

**IBM Security AppScan Source**

バージョン 9.0.3.7

インストールと管理のガイド

**IBM**



**IBM Security AppScan Source**

バージョン 9.0.3.7

インストールと管理のガイド

**IBM**

(C) Copyright IBM Corp. and its licensors 2003, 2017. All Rights Reserved.

IBM、IBM ロゴおよび `ibm.com` は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、<http://www.ibm.com/legal/copytrade.shtml> をご覧ください。Linux は、Linus Torvalds の米国およびその他の国における商標です。Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。Unix は The Open Group の米国およびその他の国における登録商標です。Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

このプログラムには下記の製品が含まれています。Jacorb 2.3.0, Copyright 1997-2006 The JacORB project および XOM1.0d22, Copyright 2003 Elliotte Rusty Harold 各製品は Gnu Library General Public License (GPL) の下で使用できます。このライセンス文書は、このプログラムに付属する特記事項ファイルに含まれています。

# 目次

## 第 1 章 IBM Security AppScan Source

の概要 . . . . .	1
AppScan Source の新機能 . . . . .	2
AppScan Source バージョン 9.0.3.7 の新機能 . . . . .	3
AppScan Source バージョン 9.0.3.6 の新機能 . . . . .	3
AppScan Source バージョン 9.0.3.5 の新機能 . . . . .	4
AppScan Source バージョン 9.0.3.4 の新機能 . . . . .	4
AppScan Source バージョン 9.0.3.3 の新機能 . . . . .	7
AppScan Source バージョン 9.0.3.2 の新機能 . . . . .	9
AppScan Source バージョン 9.0.3.1 の新機能 . . . . .	10
AppScan Source バージョン 9.0.3 の新機能 . . . . .	10
現行バージョンの AppScan Source へのマイグレーション . . . . .	14
バージョン 9.0.2 からのマイグレーション . . . . .	14
バージョン 9.0 からのマイグレーション . . . . .	16
バージョン 8.7 からのマイグレーション . . . . .	16
重要な概念 . . . . .	18
分類 . . . . .	19
ワークフロー . . . . .	19
AppScan Source のデプロイメント・モデル . . . . .	20
標準デスクトップ・デプロイメント . . . . .	22
小規模ワークグループ・デプロイメント . . . . .	23
エンタープライズ・ワークグループ・デプロイメント . . . . .	25
米国政府の規制の準拠 . . . . .	27
AppScan Source とアクセシビリティ . . . . .	29
<b>第 2 章 システム要件およびインストール</b>	
<b>の前提条件 . . . . .</b>	<b>31</b>
AppScan Source の言語とフレームワークのサポート . . . . .	31
Linux での AppScan Source for Analysis および AppScan Source for Development (Eclipse プラグイン) コンポーネントの前提条件 . . . . .	34
<b>第 3 章 インストール・シナリオの例 . . . . .</b>	<b>37</b>
必要なすべてのコンポーネントを 1 台のマシンにインストールする . . . . .	38
IBM Rational License Server のインストール . . . . .	38
IBM Security AppScan Enterprise Server のインストール . . . . .	40
AppScan Source のインストール . . . . .	41
AppScan Source へのログイン . . . . .	45
複数マシン環境での AppScan Source コンポーネントのインストール . . . . .	46
マシン A への IBM Rational License Server のインストール . . . . .	46
マシン B への IBM Security AppScan Enterprise Server のインストール . . . . .	48

マシン C への AppScan Source クライアント製品のインストール . . . . .	49
マシン D への AppScan Source データベースのインストール . . . . .	52
AppScan Source へのログイン . . . . .	56
AppScan Source のインストールおよび既存の AppScan Enterprise Server との統合 . . . . .	56
AppScan Source のインストール . . . . .	57
AppScan Source へのログイン . . . . .	62

## 第 4 章 AppScan Source のアップグレード . . . . . 63

## 第 5 章 拡張インストールおよびアクティベーションのトピック . . . . . 67

インストール・ウィザードの開始 . . . . .	69
インストールとユーザー・データ・ファイルの場所 . . . . .	69
AppScan Source データ・ディレクトリーの変更 . . . . .	71
AppScan Enterprise Server の概要 . . . . .	72
データベースのインストールおよび AppScan Enterprise Server への接続の構成 . . . . .	74
solidDB のインストールおよび構成 . . . . .	74
既存の Oracle データベースへのインストール . . . . .	79
AppScan Enterprise Server への AppScan Source データベースの登録 . . . . .	86
AppScan Source データベースを、Common Access Card (CAC) 認証が有効になっている AppScan Enterprise Server に登録 . . . . .	88
AppScan Source データベースのバックアップ . . . . .	90
AppScan Source solidDB データベースのリストア . . . . .	91
macOS への AppScan Source のインストール . . . . .	91
AppScan Source for Development のインストール . . . . .	94
AppScan Source for Development (Eclipse、IBM MobileFirst Platform、および Rational Application Developer for WebSphere Software (RAD) のプラグイン) . . . . .	95
AppScan Source for Development Plug-in for Visual Studio のインストール . . . . .	100
AppScan Source for Automation のインストール . . . . .	101
構文 . . . . .	104
フィックスパック・インストール . . . . .	104
<b>第 6 章 AppScan Source インストー</b>	
<b>ルのカスタマイズ . . . . .</b>	<b>107</b>
カスタム・インストールまたはサイレント・インストールの作成 . . . . .	107
インストール構成ウィザードを起動する . . . . .	108
カスタム・インストール構成ウィザードの使用 . . . . .	109

カスタム・インストールまたはサイレント・インストールの実行 . . . . .	111
例：カスタム・インストールを介した AppScan Source のインストール . . . . .	112

**第 7 章 AppScan Source サイレント・インストーラー . . . . . 115**

カスタム・インストールまたはサイレント・インストールの作成 . . . . .	115
インストール構成ウィザードを起動する . . . . .	115
カスタム・インストール構成ウィザードの使用 . . . . .	117
カスタム・インストールまたはサイレント・インストールの実行 . . . . .	119
例：インストール・フレームワークを介した AppScan Source のサイレント・インストール . . . . .	120

**第 8 章 ソフトウェアのアクティブ化 123**

ライセンス・ファイルのインポート . . . . .	124
フローティング・ライセンスの使用 . . . . .	124
ライセンスの表示 . . . . .	125

**第 9 章 システムからの AppScan Source の削除 . . . . . 127**

Microsoft Windows プラットフォームからの削除 . . . . .	127
Linux プラットフォームからの削除 . . . . .	127
macOS プラットフォームからの削除 . . . . .	128

**第 10 章 AppScan Source の管理 . . . . . 129**

ユーザー・アカウントおよび許可 . . . . .	129
AppScan Source ユーザーの作成 . . . . .	130
AppScan Enterprise Server の認証: IBM Rational Jazz ユーザー認証コンポーネントの IBM WebSphere Liberty への置き換えに関するマイグレーションの考慮事項 . . . . .	131
AppScan Enterprise Server ユーザーの自動ログインを構成 . . . . .	132

AppScan Enterprise Server Liberty でのローカル製品管理者ユーザーの作成 . . . . .	133
Automation Server のユーザー・アカウントの作成 . . . . .	135

**第 11 章 ユーザー・アクティビティの監査. . . . . 137**

**第 12 章 AppScan Source 製品から AppScan Enterprise Server へのログイン . . . . . 139**

Common Access Card (CAC) 認証の有効化 . . . . .	141
AppScan Source ユーザー・パスワードの変更 . . . . .	144
AppScan Enterprise Server の SSL 証明書 . . . . .	144

**第 13 章 LDAP 統合 . . . . . 147**

**第 14 章 AppScan Source に公開するためのアプリケーションおよびプロジェクトの登録. . . . . 149**

**第 15 章 AppScan Source アプリケーションおよびプロジェクト・ファイル. . . . . 151**

**第 16 章 ポート構成 . . . . . 155**

デフォルトのオープン・ポート . . . . .	155
ポート転送構成 . . . . .	155
solidDB ポートの変更 . . . . .	156

**第 17 章 インストール後の solidDB ユーザー・パスワードの変更 . . . . . 157**

**特記事項. . . . . 167**

**索引 . . . . . 171**

---

## 第 1 章 IBM Security AppScan Source の概要

IBM® Security AppScan® Source は、ソフトウェア・セキュリティーに携わる組織内のすべてのユーザーに対して、最大の価値を提供します。AppScan Source 製品により、セキュリティー・アナリスト、品質保証専門家、開発者、経営幹部などの職種に関わらず、それぞれのユーザーが必要とする機能、柔軟性、処理能力がデスクトップにもたらされます。

この製品ファミリーの製品を以下に示します。

- **AppScan Source for Analysis:** アプリケーションとプロジェクトの構成、コードのスキャン、分析、トリアージ、優先度の高い脆弱性に対するアクションを実施するためのワークベンチです。
- **AppScan Source for Automation:** AppScan Source ワークフローの主要なステップを自動化し、ソフトウェア開発ライフサイクルを通じてビルド環境にセキュリティーを統合します。
- **AppScan Source for Development:** Developer Plug-in によって、AppScan Source for Analysis のさまざまな機能を Microsoft Visual Studio、Eclipse ワークベンチ、および Rational® Application Developer for WebSphere® Software (RAD) に統合します。これにより、ソフトウェア開発者は、開発プロセスで脆弱性を検出して対応することができます。Eclipse プラグインを使用することで、ソース・コードをスキャンしてセキュリティーの脆弱性を検出することができます。また、IBM MobileFirst Platform プロジェクトを Eclipse プラグインでスキャンできます。

これらの製品には、組織における AppScan Source の価値をさらに高めるための以下のコンポーネントが用意されています。

- **AppScan Source セキュリティー・ナレッジ・データベース:** 各脆弱性に関するコンテキストに沿った情報が格納されています。根本的な原因、リスクの重大度、実行可能な修復アドバイスに関する正確な説明を提供します。
- **AppScan Enterprise Server:** AppScan Source の大半の製品およびコンポーネントは、AppScan Enterprise Server と通信を行う必要があります。このコンポーネントがなくても、AppScan Source for Development をローカル・モードで使用できますが、カスタム・ルール、共有スキャン構成、および共有フィルターなどの機能は使用できません。

このサーバーは、一元的ユーザー管理機能と、AppScan Source データベースを介して評価を共有するためのメカニズムを提供します。サーバーには、オプションとして Enterprise Console コンポーネントが含まれています。管理者がこのコンポーネントをインストールしている場合は、評価を AppScan Source for Analysis、AppScan Source for Automation、および AppScan Source コマンド行インターフェース (CLI) からそのコンポーネントに公開できます。

Enterprise Console は、レポート機能、問題管理、トレンド分析、ダッシュボードなど、評価に関する作業を行うためのさまざまなツールを備えています。

**重要:** AppScan Source および AppScan Enterprise の一部のバージョンでは、AppScan Source から AppScan Enterprise Server に接続するために 2 つの製品のバージョンとリリース・レベルが一致していなければなりません。  
<http://www.ibm.com/support/docview.wss?uid=swg21975211> を参照して、どのバージョンの AppScan Source と AppScan Enterprise に互換性があるかを確認してください。

**注:**

- AppScan Enterprise Server は、macOS ではサポートされていません。
- 基本サーバー・ライセンスを保有している場合、AppScan 製品から同時にサーバーにアクセスできる接続数は最大で 10 までです。プレミアム・サーバー・ライセンスを保有している場合は、接続数に制限はありません。

**重要:** スキャン中は、AppScan Enterprise Server および AppScan Source のクライアント (AppScan Source for Development 以外) はいずれも、AppScan Source データベース (solidDB<sup>®</sup> または Oracle のいずれか) への直接接続が必要です。

このソフトウェア・オファリングは個人情報を収集するための Cookie またはその他の技術を使用していません。

## 翻訳済みの各国語

AppScan Source ユーザー・インターフェースは、次の言語で使用できます。

- 英語
- ブラジル・ポルトガル語
- 中国語 (簡体字)
- 中国語 (繁体字)
- ドイツ語
- スペイン語
- フランス語
- イタリア語
- 日本語
- 韓国語
- ロシア語

---

## AppScan Source の新機能

以下の、AppScan Source に追加された新機能と、このリリースで非推奨になった機能についての注意について説明します。

- 3 ページの『AppScan Source バージョン 9.0.3.7 の新機能』
- 3 ページの『AppScan Source バージョン 9.0.3.6 の新機能』
- 4 ページの『AppScan Source バージョン 9.0.3.5 の新機能』
- 4 ページの『AppScan Source バージョン 9.0.3.4 の新機能』
- 7 ページの『AppScan Source バージョン 9.0.3.3 の新機能』

- 9 ページの『AppScan Source バージョン 9.0.3.2 の新機能』
- 10 ページの『AppScan Source バージョン 9.0.3.1 の新機能』
- 10 ページの『AppScan Source バージョン 9.0.3 の新機能』

## AppScan Source バージョン 9.0.3.7 の新機能

- 『拡張および新規のスキャン・サポート』
- 『AppScan Source バージョン 9.0.3.7 でサポートされなくなった機能およびフィーチャー』

### 拡張および新規のスキャン・サポート

- Red Hat Enterprise Linux (RHEL) バージョン 7.3 がサポート対象のオペレーティング・システムになりました。
- Visual Studio 2015 への AppScan Source for Development Visual Studio プラグイン の適用がサポートされるようになりました。

### AppScan Source バージョン 9.0.3.7 でサポートされなくなった機能およびフィーチャー

AppScan Source バージョン 9.0.3.7 では次のような変更が行われました。

- OS X バージョン 10.10 は、サポート対象のオペレーティング・システムではなくなりました。
- Xcode バージョン 6.3 はサポートされなくなりました。このバージョンの Xcode による Objective-C プロジェクトのスキャンはサポートされなくなりました。
- Tomcat バージョン 5 および 6 はサポートされなくなりました。

## AppScan Source バージョン 9.0.3.6 の新機能

- 4 ページの『拡張および新規のスキャン・サポート』
- 『AppScan Source バージョン 9.0.3.6 でサポートされなくなった機能およびフィーチャー』

### 拡張および新規のスキャン・サポート

- Objective-C 用 Xcode 8.1 と 8.2 (iOS アプリケーションのみ) は macOS でサポートされるコンパイラになりました。Xcode のこれらのバージョンのサポートは、AppScan Source バージョン 9.0.3.5 で遡ります。

### AppScan Source バージョン 9.0.3.6 でサポートされなくなった機能およびフィーチャー

AppScan Source バージョン 9.0.3.6 では次のような変更が行われました。

- Red Hat Enterprise Linux バージョン 5 は、サポート対象のオペレーティング・システムではなくなりました。
- Oracle WebLogic サーバー バージョン 8、9、および 10 は、サポート対象のコンパイラではなくなりました。

## AppScan Source バージョン 9.0.3.5 の新機能

- 『拡張および新規のスキャン・サポート』
- 『Java ソースおよびバイトコードのより効率的かつ短時間での再スキャンを可能にする増分スキャンのサポート』

### 拡張および新規のスキャン・サポート

- macOS バージョン 10.12 がサポート対象のオペレーティング・システムになりました。 macOS バージョン 10.12 のサポートは、AppScan Source バージョン 9.0.3.4 まで遡ります。
- Objective-C 用 Xcode 8.0、8.1、および 8.2 (iOS アプリケーションのみ) は、macOS でサポートされるコンパイラになりました。

### Java ソースおよびバイトコードのより効率的かつ短時間での再スキャンを可能にする増分スキャンのサポート

バージョン 9.0.3.5 では、Windows および Linux で Java 増分スキャンのサポートを有効にできるようになりました。増分分析が有効にされている場合、AppScan Source によって分析データがキャッシュに入れられます。その後、プロジェクトあるいはアプリケーションを再スキャンすると、AppScan Source は、このデータを使用してコードの変更を判別し、その変更によって影響を受けるコードの部分のみが再度分析されます。これにより、コードの分析は完全に行われますが、時間は短縮されます。

この機能は、IBM Security AppScan Source for Analysis、AppScan Source for Development Eclipse プラグイン、IBM Security AppScan Source for Automation、または IBM Security AppScan Source コマンド行インターフェース (CLI) を使用している場合にサポートされます。

## AppScan Source バージョン 9.0.3.4 の新機能

- 5 ページの『拡張および新規のスキャン・サポート』
- 5 ページの『共通アクセス・カード (CAC) によって認証される場合、AppScan Enterprise Console への評価の公開がサポートされるようになりました。』
- 5 ページの『Payment Card Industry Data Security Standard (PCI DSS) バージョン 3.2 レポートのサポート』
- 5 ページの『AppScan Source for Analysis 製品資料』
- 6 ページの『AppScan Source for Analysis でスキャン構成を使用してすべての除外フィルターの検出結果を削除する機能』
- 7 ページの『AppScan Source for Automation および AppScan Source コマンド行インターフェース (CLI)での WAR ファイルと EAR ファイルのスキャン時のライブラリー処理の改善』
- 7 ページの『分析のためのクラウドへの AppScan Source 評価の送信』
- 7 ページの『AppScan Source バージョン 9.0.3.4 でサポートされなくなった機能およびフィーチャー』

## 拡張および新規のスキャン・サポート

PHP バージョン 7.0 は、IBM Security AppScan Source for Analysis、IBM Security AppScan Source for Automation、および IBM Security AppScan Source コマンド行インターフェース (CLI) の Windows と Linux 上でスキャンできるようになりました。

共通アクセス・カード (CAC) によって認証される場合、**AppScan Enterprise Console** への評価の公開がサポートされるようになりました。

CAC 認証を使用して AppScan Enterprise Server に接続する場合、AppScan Source ユーザー・インターフェース、AppScan Source コマンド行インターフェース (CLI)、および AppScan Source for Automation から AppScan Enterprise Console に評価を公開することができるようになりました。

## Payment Card Industry Data Security Standard (PCI DSS) バージョン 3.2 レポートのサポート

AppScan Source は、Payment Card Industry Data Security Standard (PCI DSS) バージョン 3.2 レポートをサポートするようになりました。

## AppScan Source for Analysis 製品資料

バージョン 9.0.3.4 では、AppScan Source for Analysis で「ヘルプ」 > 「ヘルプの目次」メニュー項目を使用すると、AppScan Source の IBM Knowledge Center でオンライン・ヘルプが開きます (バージョン 9.0.3.4 の場合、ヘルプは、IBM Security AppScan Source V9.0.3.4 資料を開きます)。同様に、AppScan Source for Analysis の「ようこそ」ビューのリンク先にアクセスすると、IBM Knowledge Center が開きます。

AppScan Source for Analysis は、さまざまなビュー、設定ページ、およびダイアログ・ボックスのコンテキスト・ヘルプも提供しています。コンテキスト・ヘルプへのキーボード・ショートカットは、Windows では F1、Linux では Shift+F1、macOS では command+F1 です。バージョン 9.0.3.4 では、このコンテキスト・ヘルプを使用して、AppScan Source の IBM Knowledge Center を開くこともできます。

インターネット接続なしで製品を使用している場合、以下のように、ヘルプをローカルで使用することができます。

- IBM Security AppScan Source の README およびリリース情報は、AppScan Source のインストール・ディレクトリーにある readme.html ファイルで参照することができます。
- 以下の PDF のユーザー・ガイドは、AppScan Source インストール・ディレクトリーの doc/<lang> ディレクトリーまたは doc¥<lang> ディレクトリー内にインストールされています。ここで、<lang> は、AppScan Source のインストール済み環境の各国語です。
  - Windows および Linux のみ: IBM Security AppScan Source for Analysis ユーザー・ガイド (Security\_AppScan\_Source\_Analysis.pdf)

- Windows および Linux のみ: *IBM Security AppScan Source Utilities* ユーザー・ガイド (Security\_AppScan\_Source\_Utilities.pdf)
- macOS のみ: *IBM Security AppScan Source for Analysis* ユーザー・ガイド - macOS (Security\_AppScan\_Source\_Analysis\_OSX.pdf)
- macOS のみ: *IBM Security AppScan Source Utilities* ユーザー・ガイド - macOS (Security\_AppScan\_Source\_Utilities\_OSX.pdf)
- *IBM Security AppScan Source* インストールと管理のガイド (Security\_AppScan\_Source\_Installation\_and\_Administration.pdf)

それらのファイルを表示するには Adobe Acrobat Reader が必要です。Acrobat Reader のコピーを持っていない場合は、<http://www.adobe.com/> からダウンロードすることができます。

- 一部の AppScan Source for Analysis 機能の Javadoc は、AppScan Source インストール・ディレクトリーの doc/Javadoc ディレクトリーまたは doc¥Javadoc ディレクトリーにあります。バージョン 9.0.3.4 では、以下の機能の Javadoc が使用可能です。
  - アプリケーション・サーバー・インポートのフレームワーク API クラスおよびメソッドの Javadoc は、doc/Javadoc/appserverimporter または doc¥Javadoc¥appserverimporter で入手可能です。
  - Framework for Frameworks API クラスおよびメソッドの Javadoc は、doc/Javadoc/frameworks または doc¥Javadoc¥frameworks で入手可能です。

これらのフォルダーで、index.html ファイルを開きます。

## AppScan Source for Analysis でスキャン構成を使用してすべての除外フィルターの検出結果を削除する機能

除外フィルターには、脆弱性タイプ、アプリケーション・プログラミング・インターフェース (API)、ファイル、ディレクトリー、プロジェクト、あるいはトレースを検出結果から除去する対象のルールが含まれます。スキャン構成に複数の除外フィルターを組み込んだ場合、相互に競合して、検出結果に影響する可能性があります。例えば、以下の 2 つのフィルターが提供されたとします。

- フィルター 1 は、脆弱性タイプ Validation.EncodingRequired のすべての検出結果を除去します。これは反転されないため、これらの検出結果は評価から除外されます。
- フィルター 2 は、脆弱性タイプ Validation.Required のすべての検出結果を除去します。これは反転されないため、これらの検出結果は評価から除外されません。

スキャン構成を使用してこれらのフィルターの両方が適用された場合、デフォルトでは、これらのフィルターはお互いを無視します。フィルター 1 は、Validation.EncodingRequired の検出結果を除外しますが、Validation.Required の検出結果は含めます。フィルター 2 は、Validation.Required の検出結果を除外しますが、Validation.EncodingRequired の検出結果は含めます。最終的な結果には、Validation.EncodingRequired の検出結果と Validation.Required の検出結果がすべて含まれます。

バージョン 9.0.3.4 では、スキャン構成の作成時に「任意の非反転除外フィルターを突き合わせます」を選択して指定されたすべての除外フィルターによる検出結果を除外することができます。このチェック・ボックスは、「スキャン構成」ビューの「全般」タブの「フィルター情報」セクションにあります。上記の例の場合、このチェック・ボックスを選択すると、`Validation.EncodingRequired` の検出結果および `Validation.Required` の検出結果は、すべて評価から除外されます。

## AppScan Source for Automation および AppScan Source コマンド行インターフェース (CLI)での WAR ファイルと EAR ファイルのスキャン時のライブラリー処理の改善

WAR ファイルをスキャンする際、以下の設定が使用可能になりました。

- `-include_all_lib_jars`: この設定は、スキャン時に WAR ファイル内のすべてのライブラリーを組み込むために使用します。
- `-include_lib_jars`: この設定は、スキャン時に WAR ファイル内の組み込みたいライブラリーを指定する場合に使用します。

EAR ファイルをインポートする場合、共有ライブラリーを保管するためのプロジェクトが自動的に作成されます。このプロジェクトは、共有ライブラリーが存在しない場合に作成されますが、内容は空になります。`-no_ear_project` 設定が使用可能になったので、この設定を使用すると、EAR ファイルに対してプロジェクトが作成されません。

## 分析のためのクラウドへの AppScan Source 評価の送信

IBM Cloud Marketplace での IBM Application Security on Cloud に対するサブスクリプション、あるいは Application Security on Cloud for Bluemix に対するサブスクリプションがある場合は、AppScan Source 評価を分析のために送信することができます。AppScan Source バージョン 9.0 以上からの評価がサポートされます。送信できるスキャンの数は、Application Security on Cloud サブスクリプションによって異なります。詳しくは、[http://www.ibm.com/support/knowledgecenter/SSYJFF\\_1.0.0/ApplicationSecurityonCloud/src\\_managing\\_assessments\\_cloud.html](http://www.ibm.com/support/knowledgecenter/SSYJFF_1.0.0/ApplicationSecurityonCloud/src_managing_assessments_cloud.html) を参照してください。

## AppScan Source バージョン 9.0.3.4 でサポートされなくなった機能およびフィーチャー

AppScan Source バージョン 9.0.3.4 時点:

- OS X バージョン 10.9 は、サポート対象のオペレーティング・システムではなくなりました。
- Xcode バージョン 5.x、6.0、および 6.2 はサポートされなくなりました。これらのバージョンの Xcode による Objective-C プロジェクトのスキャンはサポートされなくなりました。
- PHP バージョン 5.3 および 5.4 のスキャンのサポートは非推奨です。

## AppScan Source バージョン 9.0.3.3 の新機能

- 8 ページの『新規プラットフォームと統合ソリューションのサポート』
- 9 ページの『拡張および新規のスキャン・サポート』

- 9 ページの『Windows の新規インストール・ファイル名』
- 9 ページの『Windows での Common Access Card (CAC) サポート』
- 9 ページの『「DISA Application Security and Development STIG V3R10」レポートのサポート』

## 新規プラットフォームと統合ソリューションのサポート

AppScan Source バージョン 9.0.3.3 時点:

- Microsoft Windows 10 がサポート対象のオペレーティング・システムになりました。サポート対象には Windows 10 Education、Enterprise、および Pro の各エディションが含まれます。

注:

- Windows 10 では、AppScan Source インストーラー (AppScanSrc\_Installer.exe ファイル) を Windows 7 互換モードで実行する必要があります。Windows 10 では、AppScan Source をアンインストールする前に、AppScan\_Uninstaller.exe ファイルも Windows 7 互換モードで実行するように設定する必要があります。このファイルは、  
<install\_dir>%Uninstall\_AppScan%AppScan\_Uninstaller.exe (<install\_dir> は、AppScan Source インストール済み環境がある場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。) にあります。詳しくは、<http://www.ibm.com/support/docview.wss?uid=swg21696098> を参照してください。
- Windows 10 サポートは、<http://www.ibm.com/support/docview.wss?uid=swg21689814> に記載されている問題に影響を受けます。
- AppScan Enterprise Server バージョン 9.0.3.1 以上に接続している場合、IBM Security AppScan Source データベースは Oracle 12c データベースにインストールできます。

**重要:** Oracle 11g データベースを使用する AppScan Source の既存のインストール済み環境があり、Oracle 12c にアップグレードしたい場合、Oracle データベースをアップグレードする前に AppScan Source をアップグレードする必要があります。

- **Tomcat 8** は、AppScan Source のインストール済み環境に含まれるようになりました。
- Visual Studio 2015 ソリューションとプロジェクトのファイルは、AppScan Source for Analysis、AppScan Source for Automation、および AppScan Source コマンド行インターフェース でスキャンできるようになりました。Visual Studio 2015 で作成された .sln ファイルまたは .vcproj ファイルがある場合、そのファイルは Windows で AppScan Source for Analysis、AppScan Source for Automation、または AppScan Source コマンド行インターフェースを使用する場合にインポートおよびスキャンできます。

**重要:**

- AppScan Source for Development Visual Studio プラグイン の Visual Studio 2015 への適用はサポートされていません。

- Managed C++ プロジェクトがサポートされています。 Unmanaged C++ プロジェクトは、そのプロジェクトが Visual Studio 2013 以前の Platform Toolset (Platform Toolset V120 以前) を使用して作成された場合にはサポートされません。
- Xcode 7.3 for Objective-C (iOS アプリケーションのみ) は、macOS でサポートされるコンパイラーになりました (Xcode 7.3 のサポートは、AppScan Source バージョン 9.0.3.2 にまで遡ります)。

### 拡張および新規のスキャン・サポート

- PHP バージョン 5.5 および 5.6 は、IBM Security AppScan Source for Analysis、IBM Security AppScan Source for Automation、および IBM Security AppScan Source コマンド行インターフェース (CLI) の Windows と Linux 上でスキャンできるようになりました。
- Java™ をスキャンするために AppScan Source を使用する際は、@ValidatorMethod、@CallbackMethod、および @SuppressSecurityTrace のメソッド・レベル・アノテーションがサポートされるようになりました。

### Windows の新規インストール・ファイル名

Windows でのインストール・ファイル名が setup.exe から AppScanSrc\_Installer.exe に変更されました。

### Windows での Common Access Card (CAC) サポート

Common Access Card (<http://www.cac.mil>) は、米国で、現役の軍および政府職員、SR、国防総省職員、有資格請負業者により使用されている標準 ID です。CAC を使用することにより、建物や管理スペースへの物理的アクセスが可能になります。DoD コンピューター・ネットワークおよびシステムにアクセスすることができます。CAC は、さまざまなスマート・カード・リーダーが装備されたコンピューターおよびネットワークへのアクセスに使用できます。CAC をリーダーに挿入すると、デバイスはユーザーに PIN の入力を要求します。

AppScan Source を Windows で実行中であり、Common Access Card (CAC) 認証が有効になった AppScan Enterprise Server バージョン 9.0.3.1 iFix-001 以上に接続している場合、AppScan Source は CAC 認証をサポートするようになりました。

### 「DISA Application Security and Development STIG V3R10」レポートのサポート

AppScan Source は、Defense Information Systems Agency (DISA) Application Security and Development Security Technical Implementation Guide (STIG) V3R10 レポートをサポートするようになっています。

## AppScan Source バージョン 9.0.3.2 の新機能

### AppScan Source および AppScan Enterprise バージョン互換性

AppScan Source の一部のバージョンでは、AppScan Enterprise Server への接続時や AppScan Enterprise Console への公開時に、AppScan Source および AppScan Enterprise のバージョンとリリース・レベルを一致させる必要がなくなり

ました。 <http://www.ibm.com/support/docview.wss?uid=swg21975211> を参照して、どのバージョンの AppScan Source と AppScan Enterprise に互換性があるかを確認してください。

この変更は、AppScan Source の一部の旧バージョンにそ及的です。  
<http://www.ibm.com/support/docview.wss?uid=swg21975211> で説明されています。

## AppScan Source バージョン 9.0.3.1 の新機能

- 『新規統合ソリューションのサポート』
- 『AppScan Source for Automation および AppScan Source コマンド行インターフェース (CLI)での WAR ファイルと EAR ファイルのスキャン』

### 新規統合ソリューションのサポート

AppScan Source バージョン 9.0.3.1 では、次のようになっています。

- Tomcat 8 は、Java と JSP のコンパイルでサポートされるようになりました。

注: オペレーティング・システムのサポートは、個々のコンパイラーがサポートするオペレーティング・システムによって異なります。

- Objective-C 用 Xcode 7.0、7.1、および 7.2 (iOS アプリケーションのみ) は、macOS でサポートされるコンパイラーになりました。

### AppScan Source for Automation および AppScan Source コマンド行インターフェース (CLI)での WAR ファイルと EAR ファイルのスキャン

CLI の `openapplication (oa)` コマンドを使用して、WAR ファイルと EAR ファイルを開けるようになりました。また、これらのファイルは `ScanApplication` コマンドを使用して AppScan Source for Automation でスキャン可能です。

## AppScan Source バージョン 9.0.3 の新機能

- 『新規プラットフォームと統合ソリューションのサポート』
- 11 ページの『スキャン構成の機能拡張』
- 11 ページの『新規ルール属性によって、重大度が高いの確定セキュリティー検出結果をより正確に特定』
- 13 ページの『自動逸失シンク解決によりスキャン結果が改善』
- 13 ページの『拡張および新規のスキャン・サポート』
- 14 ページの『AppScan Source バージョン 9.0.3 でサポートされなくなった機能およびフィーチャー』

### 新規プラットフォームと統合ソリューションのサポート

AppScan Source バージョン 9.0.3 では、以下のオペレーティング・システムがサポートされています。

- Red Hat Enterprise Linux バージョン 6 アップデート 6 および 7

- OS X バージョン 10.11。OS X バージョン 10.11 のサポートは、AppScan Source バージョン 9.0.2 にまで遡りますが、制限事項が <http://www.ibm.com/support/docview.wss?uid=swg21968948> で説明されています (この制限事項は、AppScan Source バージョン 9.0.2 にのみ影響します)。

さらに、以下もサポートされるようになりました。

- Objective-C 用の Xcode 6.3 と 6.4 (iOS アプリケーションのみ) は、OS X でサポートされるコンパイラになりました (Xcode 6.3 と 6.4 のサポートは、AppScan Source バージョン 9.0.2 にまで遡ります)。Xcode 6.3 と 6.4 のサポートには、いくつかの制限事項があることにご注意ください。詳細については、<http://www.ibm.com/support/docview.wss?uid=swg21962208> を参照してください。これらの制限は、AppScan Source バージョン 9.0.3.1 以降には適用されません。
- AppScan Source for Development Eclipse プラグイン が IBM MobileFirst Platform Foundation バージョン 7.1 と統合されました。これで、IBM MobileFirst Platform バージョン 7.1 のプロジェクト、アプリケーション、環境、および HTML ファイルを AppScan Source 製品でスキャンできます。
- Rational Application Developer for WebSphere Software (RAD) バージョン 9.1.1 プロジェクト・ファイルとワークスペースをスキャンできます。また AppScan Source for Development (Eclipse プラグイン) を RAD バージョン 9.1.1 に適用できます。
- Eclipse バージョン 4.5 プロジェクト・ファイルとワークスペース (Java および IBM MobileFirst Platform のみ) をスキャンできます。また AppScan Source for Development (Eclipse プラグイン) を Eclipse バージョン 4.5 に適用できます。
- IBM WebSphere Application Server バージョン 8.5.5 は、Java と JSP のコンパイルでサポートされるようになりました。

注: オペレーティング・システムのサポートは、個々のコンパイラがサポートするオペレーティング・システムによって異なります。

## スキャン構成の機能拡張

「スキャン構成」ビューが再設計され、以下のような重要機能が提供されるようになりました。

- フィルターを指定する機能。
- スキャンで実行する分析のタイプの設定。これには、汚染フロー分析とパターン・ベース分析が含まれます。

AppScan Source には、以下の標準装備のスキャン構成が含まれるようになりました: 「Web プレビュー・スキャン」、「Webクイック・スキャン」、「Web のバランス・スキャン」、および「詳しい Web のスキャン」

## 新規ルール属性によって、重大度が高いの確定セキュリティ検出結果をより正確に特定

このリリースの AppScan Source では、Attribute.Likelihood.High 属性と Attribute.Likelihood.Low 属性が導入されます。これらの属性は、標準装備のルールに追加され、カスタム・ルールの作成時にも使用することができます。

AppScan Source では、可能性 は、セキュリティー検出結果が悪用される可能性や機会を表します。 AppScan Source は、[https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology#Step\\_2:\\_Factors\\_for\\_Estimating\\_Likelihood](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_2:_Factors_for_Estimating_Likelihood) に示された可能性の定義を取り込み、トレース・プロパティーに基づいて可能性を決定することで、その定義を詳細化します。提供された一連のトレース・プロパティー (例えば、ソース API 名、ソース API タイプ、ソース・テクノロジー、あるいはソース・メカニズムなど) によって、AppScan Source は、将来において特定の脆弱性を使用してトレースが悪用される可能性を判別します。

可能性は、トレースのソース・エレメントと結び付けられます。ソースはプログラムへの入力、ファイル、サブレット要求、コンソール入力、ソケットなどがあります。多くの入力ソースの場合、内容と長さについて制限のないデータが返されます。チェックされていない入力については、汚染のソースと見なされます。

可能性の例には、以下のものがあります。

- HTTP ソースを持つトレース (Request.getQueryString など) とクロスサイト・スクリプティング・シンク (Response.write など) が提供されると、高可能性が決定されるため、検出結果の信頼性が上昇します。
- システム・プロパティー・ソースを持つトレース (getProperty など) とクロスサイト・スクリプティング・シンク (Response.write など) が提供されると、低可能性が決定されるため、検出結果の信頼性が低下します。

可能性は、即時にアクションを実行するか修正する必要がある、優先度が高い要アクションの検出結果を識別するために使用されます。これは、悪用される可能性が高い汚染のソースと結び付けられ、検出結果を分類するためにより微細化されたアプローチを提供することができます。可能性は、汚染のソースに結び付けられた属性として、AppScan Source 脆弱性データベースに保管されます。この機能は、すぐに使用可能です。

IBM は、ソースの可能性要因を判別するための大規模な研究を実施してきています。カスタム・ルール・ウィザードを使用して、ルール・ベースに追加する新規の汚染ソースに可能性情報を追加することができます。これにより、スキャンによって生成された検出結果の分類が改善され、それによってトリアージ・ワークフロー全体の効率性が向上します。

カスタム・ルール・ウィザードには、「可能性」プロパティーに設定可能な 2 つの値 (「高」および「低」) があります。値「高」は、汚染に対してソースが非常に影響を受けやすいことを意味します。つまり、システムに侵入する汚染に対する障壁が非常に低く、攻撃者が悪意のあるデータを手動あるいは自動のいずれの方法でも容易に送信することが可能になります。値「低」は、このソースを介した悪意のあるデータの侵入に対する障壁が非常に高くなります。これは、攻撃者がソースを汚染させるには、システムの内部知識と、攻撃対象のネットワーク上で操作するための権限が必要になることを意味します。

注: これらのルール属性のために、以前のバージョンの AppScan Source で評価を生成している場合、その同じソースをバージョン 9.0.3 でスキャンすると、検出結果の分類が変更されることがあります。詳細について、またこれらのルール属性を無効にする方法については、これらの変更に関するマイグレーション考慮事項を参照してください。

## 自動逸失シンク解決によりスキャン結果が改善

AppScan Source は、getter や setter などの逸失シンク・メソッド、およびブール値を返すメソッドのマークアップを自動的に推測することで、トレース内の逸失シンクを解決しようとしています。これにより、ご使用のコードの分析がより厳密になり、逸失シンクの解決をより適切に行うことができます。

注: これらの機能のために、以前のバージョンの AppScan Source で評価を生成している場合、解決されなかった逸失シンクの検出結果に変更がある場合があります。詳細について、また自動マークアップ生成を無効にする方法については、これらの変更に関するマイグレーション考慮事項を参照してください。

## 拡張および新規のスキャン・サポート

- PHP バージョン 5.4 は、IBM Security AppScan Source for Analysis、IBM Security AppScan Source for Automation、および IBM Security AppScan Source コマンド行インターフェース (CLI) の Windows と Linux 上でスキャンできるようになりました。
- AppScan Source では、Spring MVC 4 フレームワークが標準でサポートされるようになりました。
- **Java** スキャンの最適化:
  - JavaServer Pages をスキャンする場合、スキャン中にそれらをコンパイルするのではなく、プリコンパイル済みクラス・ファイルのスキャンができるようになりました。AppScan Source for Development Eclipse プラグイン のプリコンパイル済みクラス・ファイルのスキャンするには、セキュリティー・スキャンのプロジェクトを構成 (「セキュリティー分析」 > 「スキャンの構成」 > 「セキュリティーのためのプロジェクトの構成」を選択) し、「プリコンパイル済みクラス」チェック・ボックスを選択します。IBM Security AppScan Source for Analysis のプリコンパイル済みクラス・ファイルのスキャンするには、以下のいずれかの場所にある「プリコンパイル済みクラス」チェック・ボックスを選択します。
    - プロジェクト・プロパティの「プロジェクト依存関係」タブ。
    - 新規プロジェクトまたはアプリケーションを作成する場合の「Java プロジェクト依存関係」ページ。
  - Java のスキャン中、AppScan Source は、依存関係の欠落やコンパイル・エラーについて Java ファイルや Java バイトコードをスキャンします。従属関係の欠落やコンパイル・エラーが存在する場合、その情報はログ・ファイルに書き込まれます。その情報を使用して、依存関係をプロジェクト・プロパティに追加して、再スキャンし、スキャン結果の全範囲をカバーすることができます。
- AppScan Source バージョン 9.0.3 では、Xcode プロジェクトのインポートおよびスキャン時に、ヘッダーの位置と構成オプションが、より正確に判別されます。この変更では、すべてのファイルのビルド構成を取得するために `xcodebuild -dry-run` を使用するようになったので、続行前に AppScan Source がファイルの構成を判別するとき、スキャンの開始時に一時停止する可能性があります。

## AppScan Source バージョン 9.0.3 でサポートされなくなった機能およびフィーチャー

AppScan Source バージョン 9.0.3 では次のような変更が行われました。

- OS X バージョン 10.8 は、サポート対象のオペレーティング・システムではなくなりました。
- Xcode バージョン 4.6 はサポートされなくなりました。このバージョンの Xcode による Objective-C プロジェクトのスキューンはサポートされなくなりました。
- Eclipse バージョン 3.6 および 3.7 のプロジェクト・ファイルとワークスペースはサポートされなくなり、AppScan Source for Development (Eclipse プラグイン) は Eclipse バージョン 3.6 および 3.7 に適用できなくなりました。
- Rational Application Developer for WebSphere Software (RAD) バージョン 8.0.x プロジェクト・ファイルとワークスペースはサポートされなくなり、IBM Security AppScan Source for Development プラグイン for IBM Rational Application Developer for WebSphere Software (RAD) は RAD バージョン 8.0.x に適用できなくなりました。
- IBM Rational Team Concert™ バージョン 3.0 および 3.0.1 は、障害追跡システムとしてサポートされなくなりました。
- WebSphere Application Server バージョン 6.1 は、アプリケーション・サーバーとしてサポートされなくなりました。
- PHP バージョン 4.x から 5.2 のスキューンのサポートは非推奨です。

---

## 現行バージョンの AppScan Source へのマイグレーション

このトピックには、このバージョンの AppScan Source で行われた変更についてのマイグレーション情報が記載されています。旧バージョンの AppScan Source からアップグレードしている場合は、必ず、アップグレードしている AppScan Source のバージョンと、この現行バージョンまでのすべてのバージョンにおける変更内容に注意してください。

- 『バージョン 9.0.2 からのマイグレーション』
- 16 ページの『バージョン 9.0 からのマイグレーション』
- 16 ページの『バージョン 8.7 からのマイグレーション』

### バージョン 9.0.2 からのマイグレーション

- 『新規ルール属性により、既存スキューンの検出結果の分類が変更される可能性があります。』
- 15 ページの『自動逸失シンク生成』

新規ルール属性により、既存スキューンの検出結果の分類が変更される可能性があります。

バージョン 9.0.2 より後のバージョンでは、Attribute.Likelihood.High と Attribute.Likelihood.Low のルール属性が導入されました。これらの属性を使用すると、AppScan Source は、検出結果が「確定」または「要確認」（あるいはその両方）かを正確に判別することができます。そのため、AppScan Source バージ

9.0.2 以前でソース・コードをスキャンした場合、その同じソース・コードを 9.0.2 より後の製品バージョンでスキャンすると、検出結果の分類が変更されることがあります。これは、悪用可能性が高い Web ソースに関連する検出結果、または悪用可能性が低いプロパティーや環境のソースにおいて最も顕著です。

これらのルール属性はデフォルトで使用可能です。以下のように無効にすることができます。

1. テキスト・エディターで `<data_dir>%config%ipva.ozsettings` を開きます (`<data_dir>` は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。)。ファイル内の `allow_likelihood` 設定を見つけます。この設定は、以下の例のようになります。

```
<Setting
  name="allow_likelihood"
  value="true"
  default_value="true"
  description="Allow the processing of the Likelihood
    attributes to help determine trace confidence based
    on the source API"
  display_name="Allow Likelihood"
  type="bool"
/>
```

この設定では、`value` 属性を変更します。属性が `true` に設定されている場合、この設定はオンになります。 `false` に設定されている場合、AppScan Source はスキャン中にこれらの属性ルールを使用しません。

2. この設定の変更後、ファイルを保存して AppScan Source を始動または再始動します。

## 自動逸失シンク生成

9.0.2 より後のバージョンでは、`getter/setter`、およびブール値を返すメソッドで終わるトレースに、自動逸失シンク解決が導入されました。これは、これらのアプリケーション・プログラミング・インターフェース (API) のマークアップを自動的に推測することで実現します。そのため、AppScan Source バージョン 9.0.2 以前でソース・コードをスキャンした場合、同じソース・コードを 9.0.2 より後の製品バージョンでスキャンすると、未解決の逸失シンクが含まれる検出結果が変更される可能性があります。

自動マークアップ生成はデフォルトでオンにされています。カスタム・ルールなど、他の手段を使用して逸失シンクを解決する場合は、生成をオフにすることができます。

1. テキスト・エディターで `<data_dir>%config%ipva.ozsettings` を開きます (`<data_dir>` は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。)。ファイル内の `automatic_lost_sink_resolution` 設定を見つけます。この設定は、以下の例のようになります。

```
<name="automatic_lost_sink_resolution"
  value="true"
  default_value="true"
  description="This setting tries to perform automatic
    lost sink resolution by assuming taint propagation
    for getters, setters and APIs which return boolean
```

```

    with no arguments."
    display_name="Auto Lost Sink Resolution"
    type="bool"
  />

```

この設定では、value 属性を変更します。属性が true に設定されている場合、この設定はオンになります。false に設定されている場合、AppScan Source はこれらのメソッドのマークアップを自動生成しません。

2. この設定の変更後、ファイルを保存して AppScan Source を始動または再始動します。

## バージョン 9.0 からのマイグレーション

### AppScan Enterprise Server の認証: IBM Rational Jazz™ ユーザー認証コンポーネントの IBM WebSphere Liberty への置き換えに関するマイグレーションの考慮事項

- ローカル Jazz ユーザーのみが含まれる Enterprise Server からのマイグレーション: このアップグレード・シナリオでは、以前の Jazz ユーザーは、AppScan Source データベースに AppScan Enterprise Server ユーザーとして表示されますが、有効ではありません。これらのユーザーをデータベースから削除できます。あるいは、<http://www.ibm.com/support/docview.wss?uid=swg21686347> の説明に従って変換を有効にする場合、これらのユーザーを AppScan Source ユーザーに変換できます。
- LDAP を使用して構成された Enterprise Server からのマイグレーション: Enterprise Server のアップグレード時に、LDAP を使用して Enterprise Server を再構成するオプションがあります。これを行う場合、既存のユーザーは引き続き AppScan Source で機能します。
- Windows 認証を使用して構成された Enterprise Server からのマイグレーション: Enterprise Server が Windows 認証を使用して構成されていた場合、新しい Enterprise Server Liberty が Windows 認証を使用するように構成されていると、既存のユーザーは AppScan Source で機能します。

## バージョン 8.7 からのマイグレーション

- 『検出結果の分類の変更』
- 17 ページの『スキャン範囲を改善するデフォルト設定の変更』
- 18 ページの『以前のバージョンからの AppScan Source 事前定義フィルターの復元』

### 検出結果の分類の変更

バージョン 8.7 以降では、検出結果の分類が変更されました。この表では、従来の分類と新しい分類の対応を示します。

表 1. 検出結果分類の変更

バージョン 8.8 より前の AppScan Source の検出結果分類	AppScan Source バージョン 8.8 での検出結果の分類
脆弱性	「確定」セキュリティ検出結果
タイプ I 例外	「要確認」セキュリティ検出結果

表 1. 検出結果分類の変更 (続き)

バージョン 8.8 より前の AppScan Source の検出結果分類	AppScan Source バージョン 8.8 での検出結果の分類
タイプ II 例外	スキャン範囲検出結果

これらの変更の例は、「脆弱性マトリックス」ビューで確認できます。

Reset	Vulnerability	Exceptions		Totals
		Type I	Type II	
High	0	51	0	51
Medium	0	12	5	17
Low	0	67	3	70
<b>Totals</b>	<b>0</b>	<b>130</b>	<b>8</b>	<b>138</b>

バージョン 8.8 では、次のようになります。

Reset	Security Findings		Scan Coverage Findings	Totals
	Definitive	Suspect		
High	0	51	0	51
Medium	0	16	5	21
Low	0	81	9	90
<b>Totals</b>	<b>0</b>	<b>148</b>	<b>14</b>	<b>162</b>

### スキャン範囲を改善するデフォルト設定の変更

AppScan Source バージョン 8.8 の場合:

- scan.ozsettings 内の show\_informational\_findings のデフォルト値が true から false に変更されました。

- ipva.ozsettings 内の waf1\_globals\_tracking のデフォルト値が false から true に変更されました。この設定により、AppScan Source がフレームワーク・ベースの各種コンポーネント間のデータ・フローを検出することが可能になります (例えば、コントローラーからビューへのデータ・フローなど)。

show\_informational\_findings に対する変更によって、重大度レベルが「情報」の検出結果は、デフォルトでは評価に組み込まれないようになります。

注: 8.8 より前のバージョンで作成されたスキャン構成があり、それらに対して値を明示的に設定していなかった場合、そのスキャン構成では新しいデフォルト値が使用されます。

## 以前のバージョンからの AppScan Source 事前定義フィルターの復元

AppScan Source バージョン 8.8 では、より有用なスキャン結果が得られるように定義済みフィルターが改善されました。AppScan Source の旧バージョンからの定義済みフィルターを引き続き使用する必要がある場合は (アーカイブ・フィルターのリストは 159 ページの『第 18 章 AppScan Source 事前定義フィルター (バージョン 8.7.x 以前)』に記載されています)、161 ページの『第 19 章 アーカイブ済みの事前定義フィルターの復元』の指示のとおりに行ってください。

---

## 重要な概念

AppScan Source の使用または管理を開始する前に、AppScan Source の基本的な概念についてよく理解しておく必要があります。このセクションでは、AppScan Source の基本的な用語と概念について定義します。これ以降の章では、こうした用語と概念の定義が繰り返して出てきます。この定義を参照することにより、これらの用語と概念が AppScan Source for Analysis ではどのような意味を持つのかを理解することができます。

AppScan Source for Analysis は、ソース・コードをスキャンして脆弱性を検出し、検出結果を生成します。検出結果とは、スキャンによって検出された脆弱性のことです。スキャンの結果は、評価と呼ばれます。バンドルは、個別の検出結果の名前付きコレクションであり、アプリケーションと共に保管されます。

アプリケーション、アプリケーションの属性、およびプロジェクトは、AppScan Source for Analysis で作成および編成されます。

- アプリケーション: アプリケーションには、1 つ以上のプロジェクトと関連する属性が格納されます。
- プロジェクト: プロジェクトは、ソース・コードを含む一連のファイルと、構成データなどの関連情報から構成されます。プロジェクトは、常にアプリケーションの一部になります。
- 属性: 属性とは、スキャンの結果を意味のあるグループ (部門別やプロジェクト・リーダー別など) に分けて整理するのに役立つアプリケーションの特性のことです。属性は AppScan Source for Analysis で定義します。

AppScan Source for Analysis の主な機能は、ソース・コードをスキャンして脆弱性を分析することです。評価データによって提供される脆弱性についてのソース・コードの分析情報には、以下のようなものがあります。

- 重大度: リスクのレベルを示すための値 (高、中、低)。
- 脆弱性タイプ: SQL 注入やバッファ・オーバーフローなどの脆弱性カテゴリ。
- ファイル: 検出結果が存在するコード・ファイル
- API/ソース: API と API に渡される引数を表示する脆弱な呼び出し。
- メソッド: 脆弱な呼び出しが作成される関数またはメソッド。
- 位置: 脆弱な API が記述されているコード・ファイル内の行番号と列番号。
- 分類: セキュリティー検出結果またはスキャン範囲検出結果のいずれか。詳しくは、『分類』を参照してください。

## 分類

検出結果は、セキュリティー検出結果かスキャン範囲検出結果のどちらであるかを示すために AppScan Source によって分類されます。セキュリティー検出結果は、実際のセキュリティーの脆弱性または疑わしいセキュリティーの脆弱性を表し、一方でスキャン範囲検出結果は、構成を改善することでスキャンの範囲がより適切となる可能性があるエリアを表します。

各検出結果には、以下のいずれかの分類 が割り当てられます。

- 「確定」セキュリティー検出結果: 本来意図されていない動作を攻撃者がアプリケーションに実行させるおそれがあることを表す、明確な設計違反、実装違反、またはポリシー違反が含まれている検出結果。

こうした攻撃は、データ、システム、リソースの無許可アクセス、盗難、破損を招く可能性があります。「確定」セキュリティー検出結果はすべて完全に明確に示され、各脆弱性条件に固有の基本パターンは識別されて記述されます。

- 「要確認」セキュリティー検出結果: 追加の情報や調査が必要な、脆弱性が発生するおそれのある疑わしい条件が存在することを示す検出結果。不正に使用されると脆弱性が発生するおそれのあるコード・エレメントまたは構造。

「要確認」検出結果は、明確に脆弱性として定義できない不明な状況が存在するという点で、「確定」検出結果とは異なります。この不明条件の例としては、ソース・コードが提供されていない動的要素やライブラリー関数を使用していることなどがあります。したがって、「要確認」検出結果が「確定」であるかどうかを断定するには、もう一段階詳しい調査が必要となります。

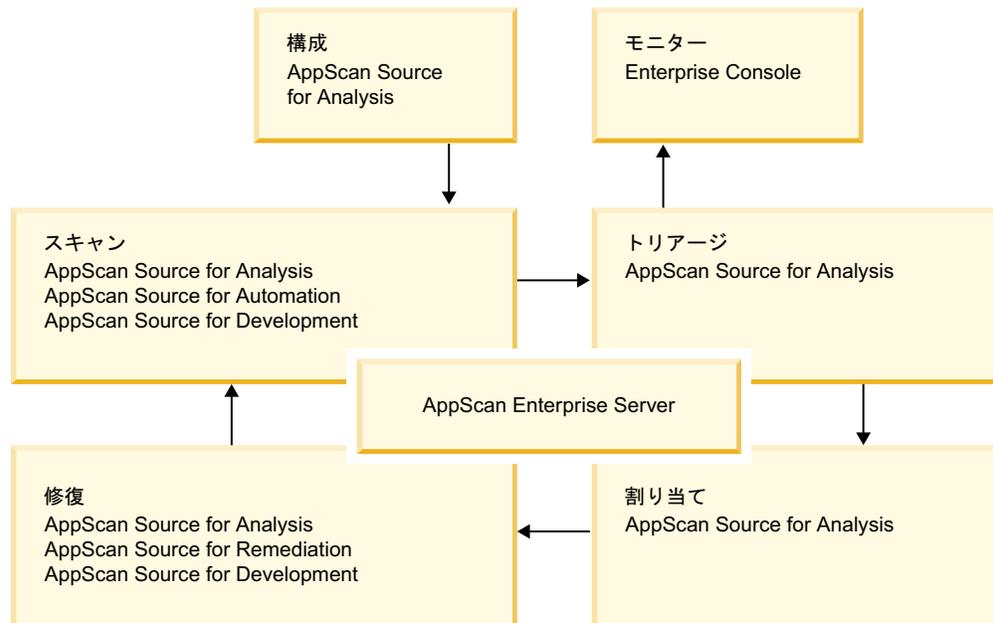
- 「スキャン範囲」検出結果: 構成の改善によって、スキャンの範囲がより適切となる可能性があるエリアを表す検出結果 (逸失シンク検出結果など)。

注: 場合によっては、「なし」の分類を使用して、セキュリティー検出結果でもスキャン範囲検出結果でもない分類が示されることがあります。

## ワークフロー

インストール、デプロイメント、ユーザー管理が完了したら、AppScan Source ワークフローの基本ステップは以下ようになります。

1. セキュリティー要求の設定: 管理者またはセキュリティーの専門家が、脆弱性と重大度の判定方法を定義します。
2. アプリケーションの構成: アプリケーションとプロジェクトを編成します。
3. スキャン: ターゲット・アプリケーションに対して分析を実行し、脆弱性を特定します。
4. 結果のトリアージおよび分析: セキュリティーを担当するスタッフが、分析結果を調査して修復ワークフローの優先順位付けを行い、実際の脆弱性と潜在的な脆弱性を切り分けます。これにより、重大な問題に関するトリアージを即座に開始することができます。この状態で、最初に修正する必要がある問題を特定します。
5. ナレッジベース・データベースのカスタマイズ: AppScan Source セキュリティー・ナレッジ・データベースをカスタマイズして、内部ポリシーに対応します。
6. スキャン結果の公開: スキャン結果を AppScan Source データベースに追加するか、または AppScan Enterprise Console に公開します。
7. 修復タスクの割り当て: 脆弱性の解決のため、開発チームに障害問題を割り当てます。
8. 問題の解決: コードの書き換え、問題部分の削除、またはセキュリティー機能の追加により、脆弱性を解消します。
9. 修正の検証: コードを再スキャンして、脆弱性が排除されたことを確認します。



## AppScan Source のデプロイメント・モデル

このセクションでは、3 種類のデプロイメント・モデルと、各モデルを構成するコンポーネントについて説明します。

AppScan Source 製品 (AppScan Enterprise Server と併用) は、さまざまな組織要件に対応するために、複数のデプロイメント・オプションをサポートします。製品ソリューションはクライアント・コンポーネントとサーバー・コンポーネントから

なり、各コンポーネントは特定の目的で使用されます。すべてのコンポーネントが必要になるデプロイメント・モデルもあれば、少数のコンポーネントのみが必要になるデプロイメント・モデルもあります。さらに、情報技術ポリシーによっては、特定のサーバー・コンポーネントを別個のコンピューターにデプロイすることが必要な場合もあれば、すべてのコンポーネントを 1 台のコンピューターにデプロイすることが必要な場合もあります。

このセクションでは、以下の 3 種類のデプロイメント・モデルについて説明します。

- 22 ページの『標準デスクトップ・デプロイメント』
- 23 ページの『小規模ワークグループ・デプロイメント』
- 25 ページの『エンタープライズ・ワークグループ・デプロイメント』

これらのモデルを組み合わせたものが、ニーズに最も適したデプロイメントである場合もあります。以下の表に、デプロイされる各 AppScan Source 製品またはコンポーネントの概要を示します。

コンポーネント	説明
AppScan Source for Analysis	優先度の高い脆弱性の分析、切り分け、処置を行うワークベンチ。セキュリティ・アナリスト、QA 管理者、開発管理者は、短時間で結果を得ることができます。AppScan Source for Analysis は AppScan Enterprise Server と通信する必要があります。
AppScan Source for Development	コード行レベルでの脆弱性の修復に重点を置いた IDE 統合型コンポーネント。AppScan Source for Development は、ソース・コードをスキャンする際に AppScan Enterprise Server のみと通信します。
AppScan Source データベース	AppScan Source セキュリティー・ナレッジ・データベースのデータ、評価データ、およびアプリケーション/プロジェクト・インベントリーが保持される、すぐに使用可能なデータベース。 <b>重要:</b> スキャン中は、AppScan Enterprise Server および AppScan Source のクライアント (AppScan Source for Development 以外) はいずれも、AppScan Source データベース (solidDB または Oracle のいずれか) への直接接続が必要です。
AppScan Source for Automation	ソフトウェア開発ライフサイクル (SDLC) において、AppScan Source ワークフローの主要な側面を自動化し、スキャンをビルド環境に統合します。Automation Server は、スキャン、評価の公開、およびレポートの生成の要求を処理します。このコンポーネントはサービス/デーモンとして動作し、AppScan Enterprise Server と通信する必要があります。

コンポーネント	説明
AppScan Source コマンド行インターフェース (CLI) クライアント	AppScan Source for Automation が提供する機能に加え、統合、自動化、およびスクリプト記述を有効にする各種の AppScan Source 機能に、コマンド行からアクセスできます。  CLI は AppScan Enterprise Server と通信する必要があります。

表内の各コンポーネントは、AppScan Enterprise Server と通信する必要があります。このサーバーは、ユーザーの集中管理機能と、AppScan Source データベースを介して評価を共有するメカニズムを提供します。さらに、管理者が AppScan Enterprise Server の Enterprise Console コンポーネントをインストールしている場合は、Enterprise Console に評価を公開することができます。Enterprise Console は、レポート機能、問題管理、トレンド分析、ダッシュボードなど、評価に関する作業を行うためのさまざまなツールを備えています。

## 標準デスクトップ・デプロイメント

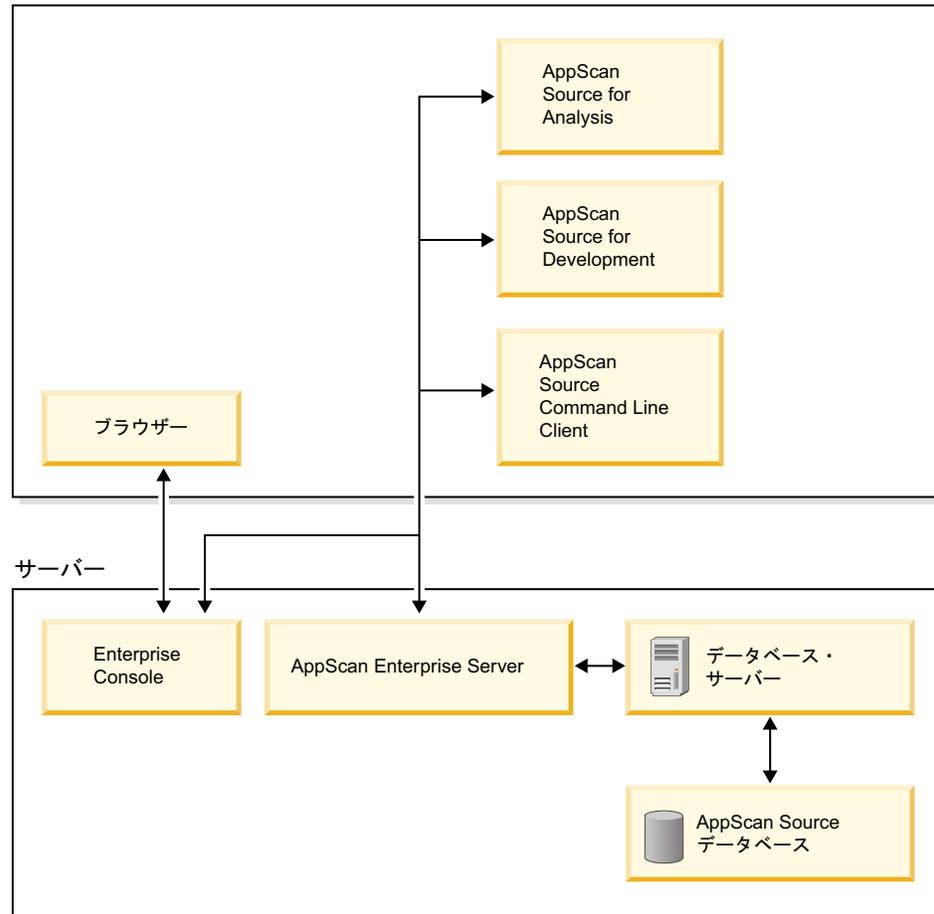
標準デスクトップ・デプロイメントは、小規模組織の AppScan Source シングル・ユーザーや、オンサイトとオフサイトの両方でセキュリティー評価を行うセキュリティー・アナリスト/監査員を対象としています。このデプロイメントでは、障害追跡システムの統合やビルド統合 (AppScan Source for Automation を使用する) がないことを前提としています。このデプロイメント・モデルは、1 台のコンピューター (ノートブックなど) にインストールされた 2 つの AppScan Source コンポーネント、つまり AppScan Source for Analysis (クライアント) と AppScan Enterprise Server で構成されます。デスクトップ・デプロイメント・モデルは、AppScan Source を多数のコンピューターにデプロイできることや、チームの作業内容に応じて最適化できることよりも、スキャン結果と個人の生産性および利便性に重点を置いています。

このモデルでは、ユーザーは AppScan Enterprise Server に対して AppScan Source の管理アカウントを使用して認証を行います。LDAP ディレクトリー・サーバーの統合は想定されていません。このモデルでは、コンピューター上のソース・コントロール管理クライアントがソース・コードにアクセスするか、コンピューターにソース・コードが格納されていることを前提としています。

標準デスクトップ・デプロイメントは、モバイルで利用する監査員に最適です。例えば、監査員がオンサイトで作業した後、一部の仕事を自宅に戻ってから、または移動中に終わらせたい場合などに適しています。AppScan Source for Analysis と AppScan Enterprise Server が稼働しているノートブックにオフサイトでログインした監査員は、ソース・コードと保存されている評価にアクセスできます。その後、監査員がオンサイトの作業に戻ったときに、ソース・コントロール・システムに再接続することで、修正したソースを社内のリポジトリーに戻すことができます。このモデルを使用すると、評価結果のすべての詳細が含まれた証跡レポートを生成できます。

以下の図に、クライアント・コンポーネントとサーバー・コンポーネントが同一のコンピュータ上にある標準デスクトップ・デプロイメントを示します。

#### ソース・コントロール管理クライアント



## 小規模ワークグループ・デプロイメント

小規模ワークグループ・デプロイメントは、アプリケーション・デプロイメントに関する IT コンプライアンス・ガイドラインが多くない、小規模から中規模のチームに最適です。

このモデルでは、AppScan Source サーバー・コンポーネントが専用のコンピューターに配置されます。このコンピューターは、一般に、AppScan Source クライアント・コンポーネントが稼働しているコンピューターと同じサブネットに配置されます。このモデルでは、ローカルの AppScan Source 管理者が AppScan Source ユーザー・アカウントを管理し、社内の LDAP ディレクトリー・サーバーが統合されていないことを想定しています。さらに、コンピューター上のソース・コントロール管理クライアントがソース・コードにアクセスするか、またはコンピューター上にソースのコピーも存在していることを前提としています。

このモデルを使用すると、デプロイメントにかかる手間や管理を最小限に抑えてチーム・コラボレーションを実現できます。このデプロイメント・モデルでは、以下のような構成になることを理解することが重要です。

- セキュリティー・アナリストと開発者は、AppScan Enterprise Server に接続します。
- 監査員/マネージャーは、Web ブラウザーを介して AppScan Enterprise Server の Enterprise Console コンポーネントに接続します。
- AppScan Source サーバー・コンポーネントは、ソース・コードにアクセスできる専用コンピューター上で稼働します。

小規模ワークグループ・デプロイメントのインストールは、ネットワーク上の複数のコンピューターで AppScan Source コンポーネントを実行するのに必要なクライアント・コンポーネントおよびサーバー・コンポーネントで構成されます。

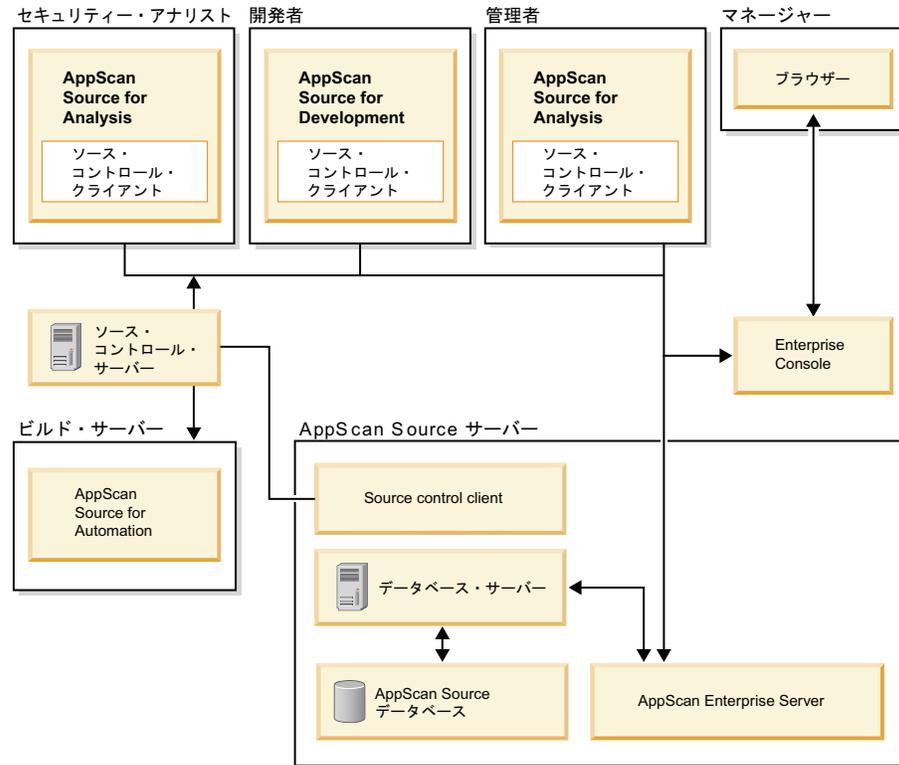
### サーバー・コンポーネント

- AppScanSource データベース
- AppScan Source for Automation

### クライアント・コンポーネント

- AppScan Source for Analysis
- AppScan Source コマンド行インターフェース
- AppScan Source for Development for Eclipse、RAD、MobileFirst (デフォルトでは未選択)
- Windows のみ: AppScan Source for Development for Visual Studio 2013(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2013 を検出した場合のみ使用可能)
- Windows のみ: AppScan Source for Development for Visual Studio 2012(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2012 を検出した場合のみ使用可能)
- Windows のみ: AppScan Source for Development for Visual Studio 2010(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2010 を検出した場合のみ使用可能)

以下の図に、AppScan Source コンポーネントの小規模ワークグループ・デプロイメントを示します。



## エンタープライズ・ワークグループ・デプロイメント

エンタープライズ・ワークグループ・デプロイメントは、組織の考慮事項に準拠する必要がある、大規模組織内の中規模から大規模のチームを対象としています。このデプロイメントは、組織に以下の要件がある場合に適しています。

- Web アプリケーションのクラスタリングやロード・バランシングなどの、IT ガバナンスおよびコンプライアンスのガイドラインに準拠する必要がある場合。
- データベースをデータ・センターに配置して自動バックアップするなど、社内リソースを最大限に活用する場合。
- いくつかのファイアウォール内でコンポーネントを実行し、何らかの形式のポート転送を必要とする場合。

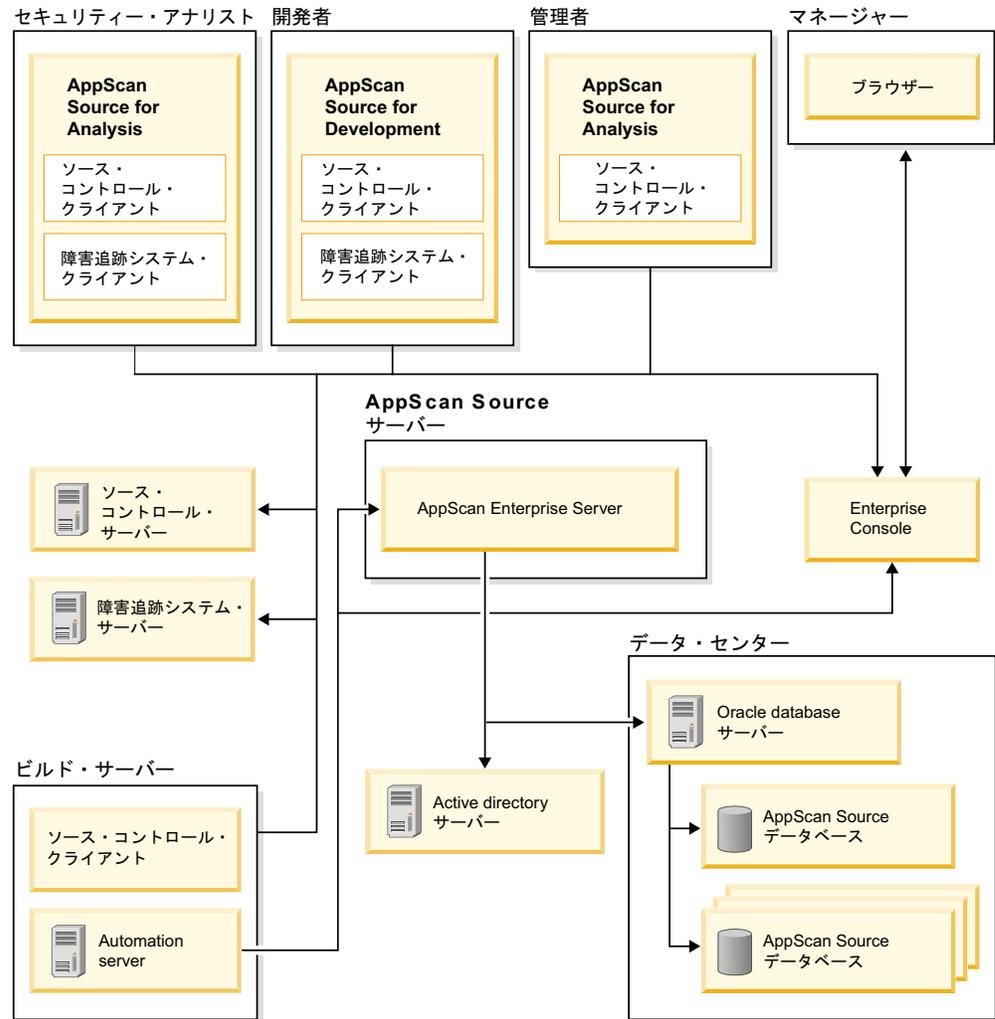
このデプロイメント・モデルでは、社内に LDAP ディレクトリー・サーバーがあることと、AppScan Source を使用するための認証で、このディレクトリー・サーバーを介した資格情報の検証が必要となることを想定しています。また、コンピューター上のソース・コントロール管理クライアントを介してソース・コードにアクセスできるか、コンピューターにソースが格納されていることと、障害追跡システムが統合されていることを前提としています。

一般に、組織はビルド・プロセスとの統合によってアプリケーションのスキャンを自動化するため、AppScan Source for Automation のデプロイメントが必要となります。このモデルでは、Oracle などのデータベース・サーバーでエンタープライズ環境が標準化されている可能性もあります。

一般的なエンタープライズ・ワークグループ・デプロイメントには、以下のような特性があります。

- セキュリティー・アナリストと開発者は、AppScan Enterprise Server に接続します。
- 監査員は、Web ブラウザーを介して AppScan Enterprise Server の Enterprise Console コンポーネントに接続します。
- AppScan Source サーバー・コンポーネントは、IT ガバナンスおよびコンプライアンスのガイドラインに従って、異なるコンピューター上で稼働します。
  - Enterprise Console はロード・バランシングされた中央の Web アプリケーション・サーバー・クラスター上に置かれ、Automation Server は 1 つ以上のビルド・サーバー上で稼働します。
  - データ・センターには Oracle Database サーバーが含まれます。
- Automation Server はビルド・システムにデプロイされます。
- AppScan Enterprise Server はユーザー認証のために LDAP ディレクトリー・サーバーと通信します。
- AppScan Enterprise Server および AppScan Source のクライアントは、データ・センターでホストされる AppScan Source データベースに接続します (また、Oracle などの特定のデータベースが必要な可能性があります)。
- ソース・コントロール・クライアントが、適切なすべてのコンピューター上のソース・コードにアクセスします。
- AppScan Source for Analysis は、同じコンピューター上の障害追跡システム・クライアントと統合されます。

以下の図に、エンタープライズ・ワークグループ環境における AppScan Source コンポーネントのデプロイメントを示します。



## 米国政府の規制の準拠

米国政府によるセキュリティーおよび情報技術の規制への準拠は、営業における障害を取り除く上で役立ちます。また、これにより IBM が自社製品を業界内で最もセキュアなものにするべく取り組んでいるというブルー・ポイント（証明）を、世界中の見込み客に提示することができます。このトピックでは、AppScan Source がサポートする規格とガイドラインについて示します。

- 『インターネット・プロトコル・バージョン 6 (IPv6)』
- 28 ページの『連邦情報処理標準 (FIPS)』
- 28 ページの『米国連邦情報・技術局 (NIST) Special Publication (SP) 800-131a』
- 29 ページの『United States Government Configuration Baseline (USGCB) を使用するように構成されている Windows 7 マシン』

### インターネット・プロトコル・バージョン 6 (IPv6)

AppScan Source は IPv6 に対して有効ですが、以下の例外があります。

- IPv6 数値アドレスの入力がサポートされておらず、代わりにホスト名を入力する必要があります。IPv4 数値アドレスの入力はサポートされています。
- Rational Team Concert に接続する場合は、IPv6 はサポートされません。

## 連邦情報処理標準 (FIPS)

AppScan Source でサポートされている Windows プラットフォームおよび Linux プラットフォーム上では、AppScan Source は、FIPS 140-2 の認定済み暗号モジュールと承認されたアルゴリズムを使用することで、FIPS 出版物 140-2 に対応しています。AppScan Source でサポートされている macOS プラットフォームの場合、FIPS 140-2 モードで操作するには、手動ステップが必要です。

AppScan Source FIPS 準拠に関する背景情報を学習し、AppScan Source FIPS 140-2 モードを有効および無効にする方法を確認するには、以下の技術情報を参照してください。

- macOS 上での FIPS 140-2 モードでの AppScan Source バージョン 8.7 以降の操作
- AppScan Source で FIPS 140-2 モードを有効化/無効化/検証する方法 (Linux および Windows)
- AppScan Source バージョン 8.7 以降の FIPS 140-2 サポートに関する背景情報

## 米国連邦情報・技術局 (NIST) Special Publication (SP) 800-131a

NIST SP 800-131A ガイドラインは、暗号鍵管理に関する指示を提供します。次のようなガイドラインが含まれます。

- 鍵管理の手順
- 暗号アルゴリズムの使用法
- 使用するアルゴリズムとそれらの最小強度
- セキュア通信のための鍵の長さ

政府機関および金融機関は、製品が指定のセキュリティー要件に準拠していることを保証するために NIST SP 800-131A ガイドラインを使用します。

NIST SP 800-131A は、AppScan Source が FIPS 140-2 モードで作動している場合のみサポートされます。AppScan Source FIPS 140-2 モードを有効および無効にする方法については、『連邦情報処理標準 (FIPS)』を参照してください。

**重要:** 接続先の AppScan Enterprise Server で NIST 800-131a コンプライアンスが有効になっている場合、AppScan Source を設定してトランスポート層セキュリティー V1.2 を強制する必要があります。トランスポート層セキュリティー V1.2 が強制されない場合、サーバーへの接続は失敗します。

- AppScan Source データベースをインストールしていない場合 (例えば、クライアント・コンポーネントのみをインストールしている場合など)、  
`<data_dir>%config%ounce.ozsettings` (`<data_dir>` は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。) を変更してトランスポート層セキュリティー V1.2 を強制することができます。このファイルで、以下の設定を見つけます。

```
<Setting
  name="tls_protocol_version"
  read_only="false"
  default_value="0"
  value="0"
  description="Minor Version of the TLS Connection Protocol"
  type="text"
  display_name="TLS Protocol Version"
  display_name_id=""
  available_values="0:1:2"
  hidden="false"
  force_upgrade="false"
/>
```

この設定で、value="0" を value="2" に変更し、ファイルを保存します。

- AppScan Source データベースをインストールしている場合は、AppScan Source と Enterprise Server の両方をインストールした後に、IBM Security AppScan Enterprise Server データベース構成ツールでトランスポート層セキュリティ V1.2 を強制します。

## United States Government Configuration Baseline (USGCB) を使用するように構成されている Windows 7 マシン

AppScan Source は、USGCB 仕様で構成されている Windows 7 マシン上のアプリケーションのスキャンをサポートしています。

注: USGCB 仕様で構成されているマシンでは、AppScan Source は、障害追跡システムと、HP Quality Center または Rational ClearQuest® との統合をサポートしていません。

---

## AppScan Source とアクセシビリティ

アクセシビリティは、動作や視界に制約があるなど、身体に障害を持つユーザーに影響します。アクセシビリティに問題があると、ソフトウェア製品の正常な使用に支障をきたすことがあります。このトピックでは、AppScan Source のアクセシビリティに関する既知の問題と、その回避策について概要を説明します。

### AppScan Source インストーラーと JAWS 画面読み上げソフトウェアの併用

AppScan Source インストーラーを実行する際に Freedom Scientific JAWS (<http://www.freedomscientific.com/products/fs/jaws-product-page.asp>) を使用するには、Java Access Bridge を AppScan Source JVM にインストールする必要があります。これにより、インストーラー・パネルのラベルとコントロールを JAWS で正しく読み上げることができるようになります。

- Java Access Bridge の詳細 (ダウンロードのリンクやインストールの説明を含む) については、<http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136191.html> を参照してください。
- Java Access Bridge をインストールするための InstallAnywhere の要件について詳しくは、<http://kb.flexerasoftware.com/selfservice/documentLink.do?externalID=Q200311> を参照してください。

## 説明テキスト付きのユーザー・インターフェース・パネルで **JAWS** 画面読み上げソフトウェアを使用する

AppScan Source ユーザー・インターフェースの多くの部分に説明テキストが表示されます。この説明テキストを読み上げられるようにするには、ほとんどの場合、JAWS で Insert+B のキー・ストロークを使用する必要があります。

---

## 第 2 章 システム要件およびインストールの前提条件

AppScan Source コンポーネントを実行するには、ご使用のコンピューターが <http://www.ibm.com/support/docview.wss?uid=swg27027486> に示す (製品ごとの) 最小要件を満たしている必要があります。

AppScan Source 言語サポートについて詳しくは、『AppScan Source の言語とフレームワークのサポート』を参照してください。

**重要:** Linux 64 ビット・システムにインストールする場合、AppScan Source を正常にインストールするには、一部の 32 ビット・ライブラリーを先にインストールしておく必要があります。これらのライブラリーは、64 ビット Linux の項目の注釈 (<http://www.ibm.com/support/docview.wss?uid=swg27027486>) にリストされています。これらのライブラリーがない場合、AppScan Source をインストールしようとするメッセージ・プロンプトが表示されます。

---

### AppScan Source の言語とフレームワークのサポート

このトピックでは、AppScan Source でスキャンできる言語のリストを示します。

- 『Windows での言語サポート』
- 32 ページの『Linux での言語サポート』
- 33 ページの『macOS での言語サポート』
- 33 ページの『Framework for Frameworks 処理 API: 標準装備フレームワーク・サポート』

#### Windows での言語サポート

IBM Security AppScan Source for Analysis、IBM Security AppScan Source for Automation、および IBM Security AppScan Source コマンド行インターフェース (CLI) は、以下の言語のスキャンをサポートします。

- C/C++
- COBOL
- ColdFusion
- Java (Android API のサポートを含む)
- JavaServer Pages (JSP)
- JavaScript
- Perl
- PHP (バージョン 5.5、5.6、および 7.0)
- PL/SQL
- T-SQL
- .NET (C#、ASP.NET、VB.NET) - Microsoft .NET Framework バージョン 2.0、3.0、3.5、4.0、4.5、および 4.6
- ASP (JavaScript/VBScript)

- Visual Basic 6

注: PHP、Visual Basic 6、および Classic ASP では、ISO-8859-1 (西ヨーロッパ)、UTF-8、および UTF-16 文字セットのみがサポートされます。

AppScan Source for Development Visual Studio プラグイン は、C/C++ および .NET (C#、ASP.NET、VB.NET) のスキャンをサポートします。

AppScan Source for Development Eclipse プラグイン ( IBM MobileFirst Platform Foundation、Eclipse または IBM Rational Application Developer for WebSphere Software (RAD) に適用可能)は、Java (Android API のサポートを含む)、JavaServer Pages (JSP)、および IBM MobileFirst Platform のプロジェクトのスキャンをサポートします。

- MobileFirst Platform プロジェクトのスキャンのサポートには、ほとんどのユーザー作成 JavaScript クライアント・サイド・コードに加えて、ネイティブ・クライアント・サイド Android および iOS ソース・コードが含まれます。MobileFirst Platform Web アプリケーションもスキャンできます。
- MobileFirst Platform プロジェクトのスキャンのサポートには、MobileFirst Platform アダプター・コードなどのサーバー・サイド JavaScript コードは含まれません。

## Linux での言語サポート

IBM Security AppScan Source for Analysis、IBM Security AppScan Source for Automation、および IBM Security AppScan Source コマンド行インターフェース (CLI) は、以下の言語のスキャンをサポートします。

- C/C++
- COBOL
- ColdFusion
- Java (Android API のサポートを含む)
- JavaServer Pages (JSP)
- JavaScript
- Perl
- PHP (バージョン 5.5、5.6、および 7.0)
- PL/SQL
- T-SQL

注: PHP では、ISO-8859-1 (西ヨーロッパ)、UTF-8、および UTF-16 の文字セットのみがサポートされます。

AppScan Source for Development Eclipse プラグイン ( IBM MobileFirst Platform Foundation、Eclipse または IBM Rational Application Developer for WebSphere Software (RAD) に適用可能)は、Java (Android API のサポートを含む)、JavaServer Pages (JSP)、および IBM MobileFirst Platform のプロジェクトのスキャンをサポートします。

- MobileFirst Platform プロジェクトのスキャンのサポートには、ほとんどのユーザー作成 JavaScript クライアント・サイド・コードに加えて、ネイティブ・ク

クライアント・サイド Android および iOS ソース・コードが含まれます。  
MobileFirst Platform Web アプリケーションもスキャンできます。

- MobileFirst Platform プロジェクトのスキャンのサポートには、MobileFirst Platform アダプター・コードなどのサーバー・サイド JavaScript コードは含まれません。

## macOS での言語サポート

IBM Security AppScan Source for Analysis、IBM Security AppScan Source for Automation、および IBM Security AppScan Source コマンド行インターフェース (CLI) は、以下の言語のスキャンをサポートします。

- iOS Xcode プロジェクトおよびワークスペース内の Objective-C
- Java (Android API のサポートを含む)
- JavaServer Pages (JSP)
- JavaScript

AppScan Source for Development Eclipse プラグイン ( IBM MobileFirst Platform Foundation、Eclipse または IBM Rational Application Developer for WebSphere Software (RAD) に適用可能) は、Java (Android API のサポートを含む)、JavaServer Pages (JSP)、iOS Xcode プロジェクトでの Objective-C、および IBM MobileFirst Platform のプロジェクトのスキャンをサポートします。

- MobileFirst Platform プロジェクトのスキャンのサポートには、ほとんどのユーザー作成 JavaScript クライアント・サイド・コードに加えて、ネイティブ・クライアント・サイド Android および iOS ソース・コードが含まれます。  
MobileFirst Platform Web アプリケーションもスキャンできます。
- MobileFirst Platform プロジェクトのスキャンのサポートには、MobileFirst Platform アダプター・コードなどのサーバー・サイド JavaScript コードは含まれません。

注: CocoaPods を使用して Xcode プロジェクトを作成している場合は、AppScan Source が、生成された Xcode プロジェクト・フォーマットを読み取ることができるよう、CocoaPods の xcproj ツールをインストールする必要があります。このツールのインストールについては、<https://github.com/CocoaPods/CocoaPods/wiki/Generate-ASCII-format-xcodeproj>を参照してください。

## Framework for Frameworks 処理 API: 標準装備フレームワーク・サポート

AppScan Source には、以下のフレームワークのサポートが標準装備で含まれています。

- Apache Struts 1 および 2
- Spring MVC 2.5、3、および 4
- ASP .NET MVC 3、4、および 5 (Windows のみ)
- Enterprise JavaBeans (EJB) 2
- ASP .NET (Windows のみ)
- J2EE
- JavaServer Faces (JSF) 2

- .NET 4.5 (Windows のみ)
- Jax - RS (V1.0 および V1.1)
- Jax - WS (V2.2)

---

## Linux での AppScan Source for Analysis および AppScan Source for Development (Eclipse プラグイン) コンポーネントの前提条件

Linux 上の Eclipse では、ブラウザー・ベースのコンテンツをレンダリングするために、サード・パーティー・コンポーネントをインストールする必要があります。このコンポーネントがないと、AppScan Source for Analysis および AppScan Source for Development Eclipse プラグインは、ログイン後にハングしたり、製品使用中に障害が発生したりするなどの症状を示す可能性があります。

この前提条件についての情報は、<http://www.eclipse.org/swt/faq.php#browserwebkitgtk> で参照できます。

- 『Linux 上の AppScan Source for Analysis でブラウザー・ベースのコンテンツを使用可能にする』
- 『Linux で Eclipse バージョン 3.7 以降にインストールされている AppScan Source for Development でブラウザー・ベースのコンテンツを使用可能にする』

### Linux 上の AppScan Source for Analysis でブラウザー・ベースのコンテンツを使用可能にする

AppScan Source for Analysis は Eclipse 上に構築されているため、この問題による影響を受けます。

この問題を修正するために推奨される方法は、32 ビット版または i686 版の WebKitGTK 1.2.0 以降をインストールすることです。パッケージを入手してインストールするために適切な方法をシステム管理者に相談してください。これは、システムによっては、`yum install webkitgtk.i686` を発行するだけで行えます。

WebKitGTK をインストールできない場合、Mozilla XULRunner 1.8 の 32 ビット・バージョンをインストールできます。このオプションでは、環境変数に以下の更新を行う必要があるかもしれません。

- MOZILLA\_FIVE\_HOME を XULRunner のインストール場所に設定します。
- LD\_LIBRARY\_PATH の末尾または先頭に \$MOZILLA\_FIVE\_HOME を追加して更新します。

### Linux で Eclipse バージョン 3.7 以降にインストールされている AppScan Source for Development でブラウザー・ベースのコンテンツを使用可能にする

この問題を修正するために推奨される方法は、32 ビット版または i686 版の WebKitGTK 1.2.0 以降をインストールすることです。パッケージを入手してインストールするために適切な方法をシステム管理者に相談してください。これは、システムによっては、`yum install webkitgtk.i686` を発行するだけで行えます。

WebKitGTK をインストールできない場合、Mozilla XULRunner 1.8 の 32 ビット・バージョンをインストールできます。このオプションでは、環境変数に以下の更新を行う必要があるかもしれません。

- MOZILLA\_FIVE\_HOME を XULRunner のインストール場所に設定します。
- LD\_LIBRARY\_PATH の末尾または先頭に \$MOZILLA\_FIVE\_HOME を追加して更新します。



---

## 第 3 章 インストール・シナリオの例

AppScan Source をインストールする際には、適切なインストール・ワークフローに従う必要があります。以下のトピックでは、いくつかのインストール・シナリオ例におけるワークフローについて説明します。

重要:

- AppScan Source で必要なコンポーネントをインストールする前に、そのコンポーネントがご使用のオペレーティング・システムをサポートしていることを確認するため、コンポーネントのシステム要件を参照してください。
- これらのシナリオは、macOS には適用されません。macOS に AppScan Source をインストールする方法については、91 ページの『macOS への AppScan Source のインストール』を参照してください。

AppScan Source は以下のキー・コンポーネントで構成されます。これらのコンポーネントは、インストールすべき順序に従ってリストされています。

- Rational License Server: これは、AppScan Enterprise Server ライセンス・アプリケーションで必要とされます。また、AppScan Source フローティング・ライセンスの適用にも使用されます (ただし、AppScan Source ローカル・ライセンス・ファイルの適用には使用されません)。
- AppScan Enterprise Server: AppScan Source のすべての製品およびコンポーネントは、AppScan Enterprise Server と通信を行う必要があります。インストール後に、AppScan Enterprise Server ライセンスがインポートされた Rational License Server を指定します。
- AppScan Source 製品イメージ: これには、AppScan Source for Analysis、AppScan Source for Automation、AppScan Source for Development、および AppScan Source for Remediation が含まれます。インストール後に、AppScan Source データベース の接続先となる AppScan Enterprise Server を指定します。また、AppScan Source のフローティング・ライセンスを使用する場合には、AppScan Source ライセンスがインポートされた Rational License Server を指定します。

これらのシナリオにおける説明では、以下のことが想定されています。

- すべてのコンポーネントが Microsoft Windows にインストールされる。いくつかの説明では Linux の場合の基本的な設定および情報が提供されますが、メインのシナリオ・ワークフローは Windows についてのみ示されます。
- AppScan Source コンポーネントをインストールするマシン上での管理特権が付与されている。
- AppScan Enterprise Server のユーザー管理フィーチャーのみをインストールする。
- AppScan Source データベースとして solidDB を使用する。
- AppScan Enterprise Server のアクティブ化にはフローティング・ライセンスが使用され、AppScan Source コンポーネントのアクティブ化にはローカル・ライセンス・ファイルが使用される。

- 『必要なすべてのコンポーネントを 1 台のマシンにインストールする』
- 46 ページの『複数マシン環境での AppScan Source コンポーネントのインストール』
- 56 ページの『AppScan Source のインストールおよび既存の AppScan Enterprise Server との統合』

---

## 必要なすべてのコンポーネントを 1 台のマシンにインストールする

このシナリオでは、すべてのコンポーネントが 1 台のマシンにインストールされます。コンポーネント接続の構成時には、localhost 設定が適用されます。

### このタスクについて

このシナリオは、次の 4 つのセクションに分かれます。

- 『IBM Rational License Server のインストール』
- 40 ページの『IBM Security AppScan Enterprise Server のインストール』
- 41 ページの『AppScan Source のインストール』
- 45 ページの『AppScan Source へのログイン』

### 重要:

- AppScan Source で必要なコンポーネントをインストールする前に、そのコンポーネントがご使用のオペレーティング・システムをサポートしていることを確認するため、コンポーネントのシステム要件を参照してください。
- これらのシナリオは、macOS には適用されません。macOS に AppScan Source をインストールする方法については、91 ページの『macOS への AppScan Source のインストール』を参照してください。

## IBM Rational License Server のインストール

Rational License Server は、AppScan Enterprise Server ライセンスをホスティングするために使用されます。これは、AppScan Source フローティング・ライセンスのホスティングにも使用できますが、これについては、以下の説明では取り上げません。

### このタスクについて

サポート対象バージョンの Rational License Server が既にインストールされている場合には、Rational License Server のインストールに関する説明の部分をスキップして、「**License Key Administrator**」の起動およびライセンスのインポートに関する説明の部分に進むことができます。サポートされている Rational License Server のバージョンについては、AppScan Enterprise Server システム要件 (<http://www.ibm.com/support/docview.wss?uid=swg27027541>) および AppScan Source システム要件 (<http://www.ibm.com/support/docview.wss?uid=swg27027486>) に説明されています。

## 手順

1. Rational License Key Server イメージ (AppScan Source 製品 DVD にあるか、または IBM パスポート・アドバンテージ で AppScan Source eAssembly の一部としてダウンロードされています) を見つけます。
2. イメージをローカル・ドライブに解凍し、生成されたディレクトリーで `RLKSSERVER_SETUP%disk1%1launchpad.exe` を実行します。
3. Rational License Server インストーラーで、「**IBM Rational License Key Server** のインストールまたは更新」をクリックします。
4. IBM Installation Manager がまだシステムにインストールされていない場合には、インストール用に起動されます。
  - a. 「パッケージのインストール」ウィザードの最初のページで「**IBM Installation Manager**」チェック・ボックスとその下のすべての項目のチェック・ボックスが選択されていることを確認します。「次へ」をクリックします。
  - b. 「ライセンス」ページで、ご使用条件を読みます。ご使用条件の条項に同意するときは、「使用条件の条項に同意します」をクリックし、「次へ」をクリックします。
  - c. 「位置」ページでインストール・ディレクトリーを指定して「次へ」をクリックします。
  - d. インストールされる内容の概要が「概要」ページに表示されます。選択内容を変更する場合は、「戻る」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。
  - e. インストールが完了したら、「**Installation Manager** の再起動」をクリックします。これによって **Installation Manager** が起動し、インストールできるようになります。
5. 「パッケージのインストール」ウィザードの最初のページで、「**IBM Rational License Key Server**」チェック・ボックスとその下のすべての項目のチェック・ボックスが選択されていることを確認します。「次へ」をクリックします。
6. 「前提条件」ページで、すべてのアプリケーションを閉じてアンチウイルス・ソフトウェアを無効にするように指示されます。これらの予防タスクを完了してから「次へ」をクリックします。
7. 「ライセンス」ページで、ご使用条件を読みます。ご使用条件の条項に同意するときは、「使用条件の条項に同意します」をクリックし、「次へ」をクリックします。
8. 「位置」ページでインストール・ディレクトリーを指定して「次へ」をクリックします。
9. 必要に合わせて「パッケージ・グループ」ページへの入力を行います (例えば、**Installation Manager** を使用するのが初めてであり、既存のパッケージ・グループがない場合には、デフォルト設定のままにしてください)。「次へ」をクリックします。
10. 「翻訳」選択ページで、インストールする各国語を選択します。「次へ」をクリックします。

11. 「フィーチャー」ページで、すべてのフィーチャーが選択されていることを確認し、「次へ」をクリックします。
12. インストールされる内容の概要が「概要」ページに表示されます。 選択内容を変更する場合は、「戻る」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。
13. インストールが完了したら、「終了」をクリックして IBM Installation Manager を閉じます。
14. Windows の「スタート」メニューからIBM Rational License Key Administrator を起動します (「すべてのプログラム」メニューから「**IBM Rational**」 > 「**License Key Administrator**」を起動します)。
15. IBM Rational License Key Administrator が開始されると、「License Key Administrator」ウィザードでプロンプトが出されます (このウィザードが自動的に開かない場合には、メインメニューから「ライセンス・キー (**License Keys**)」 > 「ライセンス・キー・ウィザード (**License Key Wizard**)」を選択します)。 このウィザードで「**Rational** ライセンス・ファイルをインポート」を選択して「次へ」をクリックします。
16. 「ライセンス・ファイルのインポート」パネルで「参照」をクリックして、AppScan Enterprise Server ライセンス・ファイルにナビゲートします。 参照ダイアログ・ボックスでそのファイルを開き、「インポート」をクリックします。
17. インポートする 1 つまたは複数のライセンスを確認すると、「ライセンス・サーバーの再起動」ダイアログ・ボックスが開きます。「はい」をクリックして、ライセンス・サーバーを再始動します。 ライセンス・サーバー・サービスが開始できない場合には、Windows のサービス管理ツールを開きます。 このツールで、「**FLEXlm License Manager**」を見つけて開始します。

## IBM Security AppScan Enterprise Server のインストール

Enterprise Server のインストール方法については、「AppScan Enterprise 計画およびインストール・ガイド」または IBM Knowledge Center の対話式インストール・ガイドを参照してください。

### このタスクについて

「AppScan Enterprise 計画およびインストール・ガイド」には、IBM Security AppScan Enterprise Server のインストール・イメージに付属しています。対話式インストール・ガイドは、次の場所で参照できます: <http://www.ibm.com/support/knowledgecenter/SSW2NF/welcome> (例えば、バージョン 9.0.3 の対話式インストール・ガイドは、[http://www.ibm.com/support/knowledgecenter/SSW2NF\\_9.0.3/com.ibm.ase.help.doc/topics/roadmap\\_ase\\_install.html](http://www.ibm.com/support/knowledgecenter/SSW2NF_9.0.3/com.ibm.ase.help.doc/topics/roadmap_ase_install.html) にあります)。

### 次のタスク

Enterprise Server をインストールする前に AppScan Source がインストールされていた場合には、Enterprise Server に データベースを登録する必要があります。これを行うためのユーティリティーが AppScan Source に含まれています。これに

関する情報は、AppScan Source の「インストールと管理のガイド」の 86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』のトピックに記載されています。

Enterprise Server をアンインストールする必要がある場合は、インストールし直す前にインストール・ディレクトリーを削除する必要があります。

## AppScan Source のインストール

### 手順

1. IBM Security AppScan Source 製品の zip ファイルを見つけます (AppScan Source メディア・パックにあるか、またはIBM パスポート・アドバンテージで AppScan Source eAssembly の一部としてダウンロードした電子イメージにあります)。
2. イメージをローカル・ドライブに解凍します。そのディレクトリーは、以下の通りです。
  - Microsoft Windows: AppScanSrc\_Installer.exe を実行します
  - Linux: 32 ビット・システム上で setup.bin を実行します。64 ビット・システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180>を参照してください。
  - macOS: setup.dmg を開き、setup.command スクリプトを実行します。

インストール・ウィザードの起動に関する詳細は、「IBM Security AppScan Source インストールと管理のガイド」の 69 ページの『インストール・ウィザードの開始』のトピックに記載されています。

3. インストール・パネルに表示される各国語を選択できる画面が表示されます。言語を選択し、「OK」をクリックして続行してください。
4. インストール・ウィザードを起動すると、「ようこそ - インストール・ウィザード」パネルが開き、現在開いているアプリケーションをすべて終了することを勧めるメッセージが表示されます。「次へ」をクリックして、インストール手順を開始します。
5. 「コンポーネントの選択」インストール・パネルで、インストールするコンポーネントを選択します。AppScan Source コンポーネントは、サーバー・コンポーネントとクライアント・コンポーネントに分けられます。
  - a. AppScan Source サーバー・コンポーネントをインストールするには、「サーバー・コンポーネントの選択」を選択し、インストールするコンポーネントを選択します。
    - AppScanSource データベース
    - AppScan Source for Automation
  - b. AppScan Source クライアント・コンポーネントをインストールするには、「クライアント・コンポーネントの選択」を選択し、インストールするコンポーネントを選択します。
    - AppScan Source for Analysis
    - AppScan Source コマンド行インターフェース
    - AppScan Source for Development for Eclipse、RAD、MobileFirst (デフォルトでは未選択)

- Windows のみ: AppScan Source for Development for Visual Studio 2013(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2013 を検出した場合のみ使用可能)
- Windows のみ: AppScan Source for Development for Visual Studio 2012(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2012 を検出した場合のみ使用可能)
- Windows のみ: AppScan Source for Development for Visual Studio 2010(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2010 を検出した場合のみ使用可能)

デフォルトでは、「クライアント・コンポーネントの選択」を選択する場合、AppScan Source for Development プラグイン・コンポーネントが選択解除されて、それ以外のすべてのコンポーネントが選択されています。

インストールしたいコンポーネントを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

6. 「サーバー接続」パネルで、以下のいずれかのオプションを選択します。
  - 「**AppScan Server** インスタンスに接続する」：このオプションを選択すると、リモートの AppScan Enterprise Server をテストして、AppScan Source への接続に使用できることを確認できます。サーバー接続をテストするには、以下のフィールドにデータを入力します。
    - **AppScan Enterprise Server**: 既存の URL 形式で、ご使用のリモート AppScan Enterprise Server インスタンスのホスト名を指定します。
    - 製品管理者: AppScan Enterprise Server 管理者ユーザー ID を指定します。
    - パスワード: AppScan Enterprise Server 管理者ユーザー ID のパスワードを指定します。

サーバー設定を入力したら、「接続のテスト」をクリックして、AppScan Source との接続にそのサーバーを使用できることを確認します。

- 「サーバーを指定せずに続行する」：サーバーを指定しないで先に進む場合には、このオプションを選択します。

#### 重要:

- 接続先の Enterprise Server で NIST 800-131a 準拠が有効になっている場合は、サーバーへの接続をテストできません。この場合には、サーバーを指定せずに進んでください。AppScan Source および Enterprise Server のインストール完了後に、86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』の説明に従ってください。その際に必ず「**TLSv1.2** を強制」オプションを適用してください。
- AppScan Enterprise Server が Common Access Card (CAC) 認証を使用して設定されている場合、「サーバーを指定せずに続行する」を選択し、すべてのサーバー接続の設定とテストに appscanserverdbmgr\_cac ユーティリティを使用します。

「次へ」をクリックして、次のインストール・パネルに進みます。

7. 「インストール・ターゲットの指定」ページで、インストール・ディレクトリーを指定します。オペレーティング・システムごとのデフォルトのディレクトリーは、次のとおりです。
  - 32 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files\IBM\AppScanSource
  - 64 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource
  - Linux: root ユーザーの場合は、インストール・ウィザードによって /opt/ibm/appscansource にソフトウェアがインストールされます。 root ユーザーではない場合は、デフォルトでは <home\_directory>/AppScan\_Source にインストールされる AppScan Source for Development Eclipse プラグインをインストールできます。
  - macOS: /Applications/AppScanSource.app

**重要:**

- インストール・ディレクトリー名には、英文字のみを含めることができません。非英文字を含む名前があるフォルダーは許可されません。
- Windows にインストールする場合、AppScan Source コンポーネントをインストールするには管理者特権が付与されている必要があります。
- Linux にインストールする場合、AppScan Source サーバー・コンポーネントをインストールするには、root 特権が必要です。

「次へ」をクリックして、次のインストール・パネルに進みます。

8. 「サーバー・コンポーネントの選択」ページで IBM Security AppScan Source データベース・コンポーネントをインストール対象として選択した場合は、「データベース選択」パネルが表示されます。このページで、以下のいずれかを選択します。
  - **solidDB** のインストール
  - 既存の **Oracle 11g/12c Server** にデータベースをインストール

solidDB のインストール、または既存の Oracle データベースへのインストールについて詳しくは、「IBM Security AppScan Source インストールと管理のガイド」の 74 ページの『データベースのインストールおよび AppScan Enterprise Server への接続の構成』のトピックを参照してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

9. 「データベース選択」パネルで solidDB データベースのインストールを選択した場合は、「solidDB 管理ユーザーの構成」パネルのプロンプトが出されます。このパネルで、solidDB データベース管理者アカウントを構成します。デフォルトのデータベース管理者のユーザー名とパスワードはどちらも **dba** です。このユーザー名は変更できませんが、パスワードは変更できます。

注: 製品のインストールを完了した後にユーザー・パスワードを変更する方法については、157 ページの『第 17 章 インストール後の solidDB ユーザー・パスワードの変更』を参照してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

10. 「solidDB AppScan Source ユーザーの構成」パネルでは、solidDB AppScan Source データベースのユーザー・アカウントを構成できます。デフォルト・ユーザー名 **ounce** とデフォルト・パスワード **ounce** はそのままでも構いません。AppScan Source データベースに対して読み取り/書き込みを行うコンポーネントはすべてこのアカウントを使用します。

注:

- ユーザー名とパスワードを変更した場合は、IBM サポート担当員が AppScan Source データベースにアクセスする必要がある場合に備えて、新しい構成を記録しておいてください。
- 製品のインストールを完了した後にユーザー・パスワードを変更する方法については、157 ページの『第 17 章 インストール後の solidDB ユーザー・パスワードの変更』を参照してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

11. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つまり、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できません)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

12. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
13. 先に進む前に、インストール・オプションの概要を確認します。選択内容を変更する場合は、「前へ」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。インストーラーによって、ハード・ディスクにファイルがコピーされます。

Linux サーバー・インストールの場合のみ: ファイルをコピーしたら、デーモン・ユーザーを特定する必要があります。デフォルト・ユーザー「ounce」を作成する場合は「ユーザー '**ounce**' を作成」を選択し、既存のユーザーで実行する場合は「既存のユーザーで実行」を選択します。(インストールでこのユーザーの存在が検証されます。選択されたユーザーには有効なシェルが必要となることに注意してください。)

インストール中に「キャンセル」をクリックすると、そのタイミングにかかわらず、すべてのコンポーネントがアンインストールされます。

14. 「IBM Security AppScan Enterprise Server の構成」パネルで、solidDB データベースが AppScan Enterprise Server に接続できるようにするための設定を指定します。デフォルトでは、このインストール・パネルに、データベースとサーバーが同じマシンにデフォルト設定でインストールされていると想定した値が事前に入力されています。サーバーが Windows 認証用に構成されている場合は、「**AppScan Enterprise Server** を今すぐ構成」チェック・ボックスを選択し、サーバーにアカウントを追加したときに使用した Windows 資格情報を入力してください (ユーザー ID はフォーマット <host name>¥<user id>を使用する必要があります)。

「次へ」をクリックして、次のインストール・パネルに進みます。

注:

- 「データベース・ホスト名」フィールドの入力内容は必ず、インストーラーを実行しているマシンの完全修飾ホスト名にしてください。この値は、インストール時にこのフィールドに事前に入力されます。事前に入力された値が誤っている場合に限り変更してください。
  - Oracle データベースを使用する予定の場合は、「**AppScan Enterprise Server** を今すぐ構成」が選択されていないことを確認し、「次へ」をクリックします。このインストール・パネルは、Oracle データベースの Enterprise Server への登録に使用されません。代わりに、AppScan Source に組み込まれているユーティリティーを使用してインストール後にデータベース接続を構成できます。これに関する説明は、「IBM Security AppScan Source インストールと管理のガイド」の 86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』のトピックに記載されています。このユーティリティーを使用すると、インストール・パネルを使用する代わりに solidDB 接続を構成することもできます。
15. 「インストール完了」パネルでは、「**IBM Security AppScan Source License Manager** の起動」を選択することにより、インストール・ウィザードの終了後にただちに製品のアクティベーションを開始することができます。「完了」をクリックして標準インストールを完了し、インストール・ウィザードを終了します。
16. License Manager ユーティリティーで、以下のようになります。
- a. ライセンス・ファイルを適用するには、「インポート」をクリックしてからダウンロード済みの AppScan Source ライセンスを参照します。
  - b. フローティング・ライセンスを適用するには、「ライセンス・サーバーの構成」をクリックしてから「追加」をクリックします。フローティング・ライセンスを格納しているホスト・マシンに関する情報を入力します。
- 追加のアクティベーション手順については、123 ページの『第 8 章 ソフトウェアのアクティブ化』を参照してください。

## AppScan Source へのログイン

### このタスクについて

ログイン時に入力を求められるフィールドの説明については、下記のセクションを参照してください。詳しくは、「IBM Security AppScan Source インストールと管理のガイド」の 139 ページの『第 12 章 AppScan Source 製品から AppScan

Enterprise Server へのログイン』のトピックを参照してください。

### 手順

- **ユーザー ID:** ユーザー ID を指定します。
- **パスワード:** ご使用のユーザー ID のパスワードを指定します。
- **AppScan Enterprise Server:** 既存の URL 形式で、ご使用の AppScan Enterprise Server インスタンスのホスト名を指定します。このインストール・シナリオでは、https://localhost:9443/ase/ または localhost と指定します。

---

## 複数マシン環境での AppScan Source コンポーネントのインストール

AppScan Source コンポーネントは複数のマシンにインストールすることができます。このシナリオでは、コンポーネントは複数マシン環境にデプロイされます。Rational License Server、AppScan Enterprise Server、AppScan Source クライアント製品、および AppScan Source データベースが、すべて異なるマシンにインストールされます。

### このタスクについて

このシナリオは、以下の 5 つのセクションに分かれています。

- 『マシン A への IBM Rational License Server のインストール』
- 48 ページの『マシン B への IBM Security AppScan Enterprise Server のインストール』
- 49 ページの『マシン C への AppScan Source クライアント製品のインストール』
- 52 ページの『マシン D への AppScan Source データベースのインストール』
- 56 ページの『AppScan Source へのログイン』

### 重要:

- AppScan Source で必要なコンポーネントをインストールする前に、そのコンポーネントがご使用のオペレーティング・システムをサポートしていることを確認するため、コンポーネントのシステム要件を参照してください。
- これらのシナリオは、macOS には適用されません。macOS に AppScan Source をインストールする方法については、91 ページの『macOS への AppScan Source のインストール』を参照してください。

## マシン A への IBM Rational License Server のインストール

Rational License Server は、AppScan Enterprise Server ライセンスをホスティングするために使用されます。これは、AppScan Source フローティング・ライセンスのホスティングにも使用できますが、これについては、以下の説明では取り上げません。

### このタスクについて

サポート対象バージョンの Rational License Server が既にインストールされている場合には、Rational License Server のインストールに関する説明の部分をスキップ

プして、「**License Key Administrator**」の起動およびライセンスのインポートに関する説明の部分に進むことができます。 サポートされている Rational License Server のバージョンについては、AppScan Enterprise Server システム要件 (<http://www.ibm.com/support/docview.wss?uid=swg27027541>) および AppScan Source システム要件 (<http://www.ibm.com/support/docview.wss?uid=swg27027486>) に説明されています。

## 手順

1. Rational License Key Server イメージ (AppScan Source 製品 DVD にあるか、または IBM パスポート・アドバンテージ で AppScan Source eAssembly の一部としてダウンロードされています) を見つけます。
2. イメージをローカル・ドライブに解凍し、生成されたディレクトリーで `RLKSSERVER_SETUP¥disk1¥launchpad.exe` を実行します。
3. Rational License Server インストーラーで、「**IBM Rational License Key Server**」のインストールまたは更新をクリックします。
4. IBM Installation Manager がまだシステムにインストールされていない場合には、インストール用に起動されます。
  - a. 「パッケージのインストール」ウィザードの最初のページで「**IBM Installation Manager**」チェック・ボックスとその下のすべての項目のチェック・ボックスが選択されていることを確認します。「次へ」をクリックします。
  - b. 「ライセンス」ページで、ご使用条件を読みます。ご使用条件の条項に同意するときは、「使用条件の条項に同意します」をクリックし、「次へ」をクリックします。
  - c. 「位置」ページでインストール・ディレクトリーを指定して「次へ」をクリックします。
  - d. インストールされる内容の概要が「概要」ページに表示されます。選択内容を変更する場合は、「戻る」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。
  - e. インストールが完了したら、「**Installation Manager**」の再起動をクリックします。これによって **Installation Manager** が起動し、インストールできるようになります。
5. 「パッケージのインストール」ウィザードの最初のページで、「**IBM Rational License Key Server**」チェック・ボックスとその下のすべての項目のチェック・ボックスが選択されていることを確認します。「次へ」をクリックします。
6. 「前提条件」ページで、すべてのアプリケーションを閉じてアンチウイルス・ソフトウェアを無効にするように指示されます。これらの予防タスクを完了してから「次へ」をクリックします。
7. 「ライセンス」ページで、ご使用条件を読みます。ご使用条件の条項に同意するときは、「使用条件の条項に同意します」をクリックし、「次へ」をクリックします。
8. 「位置」ページでインストール・ディレクトリーを指定して「次へ」をクリックします。

9. 必要に合わせて「パッケージ・グループ」ページへの入力を行います (例えば、**Installation Manager** を使用するのが初めてであり、既存のパッケージ・グループがない場合には、デフォルト設定のままにしてください)。「次へ」をクリックします。
10. 「翻訳」選択ページで、インストールする各国語を選択します。「次へ」をクリックします。
11. 「フィーチャー」ページで、すべてのフィーチャーが選択されていることを確認し、「次へ」をクリックします。
12. インストールされる内容の概要が「概要」ページに表示されます。選択内容を変更する場合は、「戻る」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。
13. インストールが完了したら、「終了」をクリックして **IBM Installation Manager** を閉じます。
14. Windows の「スタート」メニューから **IBM Rational License Key Administrator** を起動します (「すべてのプログラム」メニューから「**IBM Rational**」 > 「**License Key Administrator**」を起動します)。
15. **IBM Rational License Key Administrator** が開始されると、「**License Key Administrator**」ウィザードでプロンプトが出されます (このウィザードが自動的に開かない場合には、メインメニューから「ライセンス・キー (**License Keys**)」 > 「ライセンス・キー・ウィザード (**License Key Wizard**)」を選択します)。このウィザードで「**Rational** ライセンス・ファイルをインポート」を選択して「次へ」をクリックします。
16. 「ライセンス・ファイルのインポート」パネルで「参照」をクリックして、**AppScan Enterprise Server** ライセンス・ファイルにナビゲートします。参照ダイアログ・ボックスでそのファイルを開き、「インポート」をクリックします。
17. インポートする 1 つまたは複数のライセンスを確認すると、「ライセンス・サーバーの再起動」ダイアログ・ボックスが開きます。「はい」をクリックして、ライセンス・サーバーを再始動します。ライセンス・サーバー・サービスが開始できない場合には、Windows のサービス管理ツールを開きます。このツールで、「**FLEXlm License Manager**」を見つけて開始します。

## マシン B への **IBM Security AppScan Enterprise Server** のインストール

Enterprise Server のインストール方法については、「AppScan Enterprise 計画およびインストール・ガイド」または IBM Knowledge Center の対話式インストール・ガイドを参照してください。

### このタスクについて

「AppScan Enterprise 計画およびインストール・ガイド」には、**IBM Security AppScan Enterprise Server** のインストール・イメージに付属しています。対話式インストール・ガイドは、次の場所で参照できます: <http://www.ibm.com/support/knowledgecenter/SSW2NF/welcome> (例えば、バージョン 9.0.3 の対話式インストール・ガイドは、<http://www.ibm.com/support/knowledgecenter/>

SSW2NF\_9.0.3/com.ibm.ase.help.doc/topics/roadmap\_ase\_install.html にあります)。

## 次のタスク

Enterprise Server をインストールする前に AppScan Source がインストールされていた場合には、Enterprise Server に データベースを登録する必要があります。これを行うためのユーティリティーが AppScan Source に含まれています。これに関する情報は、AppScan Source の「インストールと管理のガイド」の 86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』のトピックに記載されています。

Enterprise Server をアンインストールする必要がある場合は、インストールし直す前にインストール・ディレクトリーを削除する必要があります。

## マシン C への AppScan Source クライアント製品のインストール

### このタスクについて

AppScan Source クライアント製品および AppScan Source データベースをインストールする順序は自由です。 データベースをインストールする前にクライアント製品をインストールすることも、逆の順序でインストールすることもできます。

### 手順

1. IBM Security AppScan Source 製品の zip ファイルを見つけます (AppScan Source メディア・パックにあるか、またはIBM パスポート・アドバンテージで AppScan Source eAssembly の一部としてダウンロードした電子イメージにあります)。
2. イメージをローカル・ドライブに解凍します。 そのディレクトリーは、以下の通りです。
  - Microsoft Windows: AppScanSrc\_Installer.exe を実行します
  - Linux: 32 ビット・システム上で setup.bin を実行します。 64 ビット・システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180>を参照してください。
  - macOS: setup.dmg を開き、setup.command スクリプトを実行します。

インストール・ウィザードの起動に関する詳細は、「IBM Security AppScan Source インストールと管理のガイド」の 69 ページの『インストール・ウィザードの開始』のトピックに記載されています。

3. インストール・パネルに表示される各国語を選択できる画面が表示されます。言語を選択し、「OK」をクリックして続行してください。
4. インストール・ウィザードを起動すると、「ようこそ - インストール・ウィザード」パネルが開き、現在開いているアプリケーションをすべて終了することを勧めるメッセージが表示されます。「次へ」をクリックして、インストール手順を開始します。

5. 「コンポーネントの選択」 インストール・パネルでは、「クライアント・コンポーネントの選択」を選択してから、インストールするコンポーネントを選択します。
  - AppScan Source for Analysis
  - AppScan Source コマンド行インターフェース
  - AppScan Source for Development for Eclipse、RAD、MobileFirst (デフォルトでは未選択)
  - Windows のみ: AppScan Source for Development for Visual Studio 2013(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2013 を検出した場合のみ使用可能)
  - Windows のみ: AppScan Source for Development for Visual Studio 2012(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2012 を検出した場合のみ使用可能)
  - Windows のみ: AppScan Source for Development for Visual Studio 2010(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2010 を検出した場合のみ使用可能)

デフォルトでは、「クライアント・コンポーネントの選択」を選択する場合、AppScan Source for Development プラグイン・コンポーネントが選択解除されて、それ以外のすべてのコンポーネントが選択されています。

インストールしたいコンポーネントを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

6. 「インストール・ターゲットの指定」 ページで、インストール・ディレクトリーを指定します。オペレーティング・システムごとのデフォルトのディレクトリーは、次のとおりです。
  - 32 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files\IBM\AppScanSource
  - 64 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource
  - Linux: root ユーザーの場合は、インストール・ウィザードによって /opt/ibm/appscansource にソフトウェアがインストールされます。 root ユーザーではない場合は、デフォルトでは <home\_directory>/AppScan\_Source にインストールされる AppScan Source for Development Eclipse プラグインをインストールできます。
  - macOS: /Applications/AppScanSource.app

**重要:**

- インストール・ディレクトリー名には、英文字のみを含めることができます。非英文字を含む名前があるフォルダーは許可されません。
- Windows にインストールする場合、AppScan Source コンポーネントをインストールするには管理者特権が付与されている必要があります。
- Linux にインストールする場合、AppScan Source サーバー・コンポーネントをインストールするには、root 特権が必要です。

「次へ」をクリックして、次のインストール・パネルに進みます。

7. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つまり、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できません)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

8. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
9. 先に進む前に、インストール・オプションの概要を確認します。選択内容を変更する場合は、「前へ」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。インストーラーによって、ハード・ディスクにファイルがコピーされます。

Linux サーバー・インストールの場合のみ: ファイルをコピーしたら、デーモン・ユーザーを特定する必要があります。デフォルト・ユーザー「ounce」を作成する場合は「ユーザー 'ounce' を作成」を選択し、既存のユーザーで実行する場合は「既存のユーザーで実行」を選択します。(インストールでこのユーザーの存在が検証されます。選択されたユーザーには有効なシェルが必要となることに注意してください。)

インストール中に「キャンセル」をクリックすると、そのタイミングにかかわらず、すべてのコンポーネントがアンインストールされます。

10. 「インストール完了」パネルでは、「**IBM Security AppScan Source License Manager** の起動」を選択することにより、インストール・ウィザードの終了後にただちに製品のアクティベーションを開始することができます。「完了」をクリックして標準インストールを完了し、インストール・ウィザードを終了します。
11. License Manager ユーティリティで、以下のようにします。
  - a. ライセンス・ファイルを適用するには、「インポート」をクリックしてからダウンロード済みの AppScan Source ライセンスを参照します。
  - b. フローティング・ライセンスを適用するには、「ライセンス・サーバーの構成」をクリックしてから「追加」をクリックします。フローティング・ライセンスを格納しているホスト・マシンに関する情報を入力します。

追加のアクティベーション手順については、123 ページの『第 8 章 ソフトウェアのアクティブ化』を参照してください。

## マシン D への AppScan Source データベース のインストール このタスクについて

AppScan Source クライアント製品および AppScan Source データベースをインストールする順序は自由です。 データベースをインストールする前にクライアント製品をインストールすることも、逆の順序でインストールすることもできます。

### 手順

1. IBM Security AppScan Source 製品の zip ファイルを見つけます (AppScan Source メディア・パックにあるか、または IBM パスポート・アドバンテージで AppScan Source eAssembly の一部としてダウンロードした電子イメージにあります)。
2. イメージをローカル・ドライブに解凍します。 そのディレクトリーは、以下の通りです。
  - Microsoft Windows: AppScanSrc\_Installer.exe を実行します
  - Linux: 32 ビット・システム上で setup.bin を実行します。 64 ビット・システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180>を参照してください。
  - macOS: setup.dmg を開き、setup.command スクリプトを実行します。

インストール・ウィザードの起動に関する詳細は、「*IBM Security AppScan Source* インストールと管理のガイド」の 69 ページの『インストール・ウィザードの開始』のトピックに記載されています。

3. インストール・パネルに表示される各国語を選択できる画面が表示されます。 言語を選択し、「OK」をクリックして続行してください。
4. インストール・ウィザードを起動すると、「ようこそ - インストール・ウィザード」パネルが開き、現在開いているアプリケーションをすべて終了することを勧めるメッセージが表示されます。「次へ」をクリックして、インストール手順を開始します。
5. 「コンポーネントの選択」インストール・パネルでは、「サーバー・コンポーネントの選択」を選択してから、AppScanSource データベース が選択されていることを確認します。「次へ」をクリックして、次のインストール・パネルに進みます。
6. 「サーバー接続」パネルで、以下のいずれかのオプションを選択します。
  - 「AppScan Server インスタンスに接続する」：このオプションを選択すると、リモートの AppScan Enterprise Server をテストして、AppScan Source への接続に使用できることを確認できます。サーバー接続をテストするには、以下のフィールドにデータを入力します。
    - AppScan Enterprise Server: 既存の URL 形式で、ご使用のリモート AppScan Enterprise Server インスタンスのホスト名を指定します。
    - 製品管理者: AppScan Enterprise Server 管理者ユーザー ID を指定します。
    - パスワード: AppScan Enterprise Server 管理者ユーザー ID のパスワードを指定します。

サーバー設定を入力したら、「接続のテスト」をクリックして、AppScan Source との接続にそのサーバーを使用できることを確認します。

- 「サーバーを指定せずに続行する」：サーバーを指定しないで先に進む場合には、このオプションを選択します。

重要:

- 接続先の Enterprise Server で NIST 800-131a 準拠が有効になっている場合は、サーバーへの接続をテストできません。この場合には、サーバーを指定せずに進んでください。AppScan Source および Enterprise Server のインストール完了後に、86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』の説明に従ってください。その際に必ず「TLSv1.2 を強制」オプションを適用してください。
- AppScan Enterprise Server が Common Access Card (CAC) 認証を使用して設定されている場合、「サーバーを指定せずに続行する」を選択し、すべてのサーバー接続の設定とテストに appscanserverdbmgr\_cac ユーティリティを使用します。

「次へ」をクリックして、次のインストール・パネルに進みます。

7. 「インストール・ターゲットの指定」ページで、インストール・ディレクトリを指定します。オペレーティング・システムごとのデフォルトのディレクトリは、次のとおりです。
  - 32 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files\IBM\AppScanSource
  - 64 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource
  - Linux: root ユーザーの場合は、インストール・ウィザードによって /opt/ibm/appscansource にソフトウェアがインストールされます。root ユーザーではない場合は、デフォルトでは <home\_directory>/AppScan\_Source にインストールされる AppScan Source for Development Eclipse プラグインをインストールできます。
  - macOS: /Applications/AppScanSource.app

重要:

- インストール・ディレクトリ名には、英文字のみを含めることができます。非英文字を含む名前があるフォルダーは許可されません。
- Windows にインストールする場合、AppScan Source コンポーネントをインストールするには管理者特権が付与されている必要があります。
- Linux にインストールする場合、AppScan Source サーバー・コンポーネントをインストールするには、root 特権が必要です。

「次へ」をクリックして、次のインストール・パネルに進みます。

8. 「サーバー・コンポーネントの選択」ページで IBM Security AppScan Source データベース・コンポーネントをインストール対象として選択した場合は、「データベース選択」パネルが表示されます。このページで、「solidDB のインストール」ラジオ・ボタンを選択し、「次へ」をクリックして次のインストール・パネルに進みます。

9. 「データベース選択」パネルで solidDB データベースのインストールを選択した場合は、「solidDB 管理ユーザーの構成」パネルのプロンプトが出されます。このパネルで、solidDB データベース管理者アカウントを構成します。デフォルトのデータベース管理者のユーザー名とパスワードはどちらも **dba** です。このユーザー名は変更できませんが、パスワードは変更できます。

注: 製品のインストールを完了した後にユーザー・パスワードを変更する方法については、157 ページの『第 17 章 インストール後の solidDB ユーザー・パスワードの変更』を参照してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

10. 「solidDB AppScan Source ユーザーの構成」パネルでは、solidDB AppScan Source データベースのユーザー・アカウントを構成できます。デフォルト・ユーザー名 **ounce** とデフォルト・パスワード **ounce** はそのままでも構いません。AppScan Source データベースに対して読み取り/書き込みを行うコンポーネントはすべてこのアカウントを使用します。

注:

- ユーザー名とパスワードを変更した場合は、IBM サポート担当員が AppScan Source データベースにアクセスする必要がある場合に備えて、新しい構成を記録しておいてください。
- 製品のインストールを完了した後にユーザー・パスワードを変更する方法については、157 ページの『第 17 章 インストール後の solidDB ユーザー・パスワードの変更』を参照してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

11. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つまり、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できません)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

12. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
13. 先に進む前に、インストール・オプションの概要を確認します。選択内容を変更する場合は、「前へ」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。インストーラーによって、ハード・ディスクにファイルがコピーされます。

Linux サーバー・インストールの場合のみ: ファイルをコピーしたら、デーモン・ユーザーを特定する必要があります。 デフォルト・ユーザー「ounce」を作成する場合は「ユーザー 'ounce' を作成」を選択し、既存のユーザーで実行する場合は「既存のユーザーで実行」を選択します。(インストールでこのユーザーの存在が検証されます。選択されたユーザーには有効なシェルが必要となることに注意してください。)

インストール中に「キャンセル」をクリックすると、そのタイミングにかかわらず、すべてのコンポーネントがアンインストールされます。

14. 「IBM Security AppScan Enterprise Server の構成」パネルで、solidDB データベースが AppScan Enterprise Server に接続できるようにするための設定を指定します。「**AppScan Enterprise Server** を今すぐ構成」チェック・ボックスを選択して、以下の設定を行います。

- **AppScan Enterprise Server:** ご使用の AppScan Enterprise Server インスタンスの URL (例えば、<https://MachineB.mydomain.com:9443/ase>) を指定します。
- **ユーザー ID:** AppScan Enterprise Server ユーザー ID を指定します。 デフォルトでは、ユーザー ID が **ADMIN** です (この値は必要に応じて変更してください)。サーバーが Windows 認証用に構成されている場合は、サーバーにアカウントを追加したときに使用した Windows のユーザー ID を入力してください (ユーザー ID にはフォーマット <host name>%<user id> を使用する必要があります)。
- **パスワード:** AppScan Enterprise Server ユーザー ID のパスワードを指定します。
- **データベース・ホスト名:** AppScan Source データベースをインストールしたマシンの完全修飾ホスト名を指定します (例: MachineD.mydomain.com)。

注: このフィールドの入力内容は必ず、インストーラーを実行しているマシンの完全修飾ホスト名にしてください。 この値は、インストール時にこのフィールドに事前に入力されます。事前に入力された値が誤っている場合に限って変更してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

注: Oracle データベースを使用する予定の場合は、「**AppScan Enterprise Server** を今すぐ構成」が選択されていないことを確認し、「次へ」をクリックします。 このインストール・パネルは、Oracle データベースの Enterprise Server への登録に使用されません。代わりに、AppScan Source に組み込まれているユーティリティーを使用してインストール後にデータベース接続を構成できます。これに関する説明は、「IBM Security AppScan Source インストールと管理のガイド」の 86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』のトピックに記載されています。このユーティリティーを使用すると、インストール・パネルを使用する代わりに solidDB 接続を構成することもできます。

15. 「インストール完了」パネルでは、「**IBM Security AppScan Source License Manager** の起動」を選択することにより、インストール・ウィザード

の終了後にただちに製品のアクティベーションを開始することができます。  
「完了」をクリックして標準インストールを完了し、インストール・ウィザードを終了します。

16. License Manager ユーティリティーで、以下のようになります。
  - a. ライセンス・ファイルを適用するには、「インポート」をクリックしてからダウンロード済みの AppScan Source ライセンスを参照します。
  - b. フローティング・ライセンスを適用するには、「ライセンス・サーバーの構成」をクリックしてから「追加」をクリックします。フローティング・ライセンスを格納しているホスト・マシンに関する情報を入力します。

追加のアクティベーション手順については、123 ページの『第 8 章 ソフトウェアのアクティブ化』を参照してください。

## AppScan Source へのログイン

### このタスクについて

ログイン時に入力を求められるフィールドの説明については、下記のセクションを参照してください。詳しくは、「IBM Security AppScan Source インストールと管理のガイド」の 139 ページの『第 12 章 AppScan Source 製品から AppScan Enterprise Server へのログイン』のトピックを参照してください。

### 手順

- **ユーザー ID:** ユーザー ID を指定します。
- **パスワード:** ご使用のユーザー ID のパスワードを指定します。
- **AppScan Enterprise Server:** 既存の URL 形式で、ご使用の AppScan Enterprise Server インスタンスのホスト名を指定します。このインストール・シナリオでは、AppScan Enterprise Server がインストールされているマシンの完全修飾ホスト名を指定します。

ヒント: 完全修飾ホスト名を入力してもうまくいかない場合には、ホスト・マシンの IP アドレスを入力してみてください。

---

## AppScan Source のインストールおよび既存の AppScan Enterprise Server との統合

このシナリオでは、AppScan Source コンポーネントが 1 台のマシンにインストールされ、既存の AppScan Enterprise Server に接続するように構成されます。

### このタスクについて

このシナリオは、次の 2 つのセクションに分かれます。

- 57 ページの『AppScan Source のインストール』
- 62 ページの『AppScan Source へのログイン』

### 重要:

- AppScan Source で必要なコンポーネントをインストールする前に、そのコンポーネントがご使用のオペレーティング・システムをサポートしていることを確認するため、コンポーネントのシステム要件を参照してください。

- これらのシナリオは、macOS には適用されません。macOS に AppScan Source をインストールする方法については、91 ページの『macOS への AppScan Source のインストール』を参照してください。

## AppScan Source のインストール

### 手順

1. IBM Security AppScan Source 製品の zip ファイルを見つけます (AppScan Source メディア・パックにあるか、またはIBM パスポート・アドバンテージで AppScan Source eAssembly の一部としてダウンロードした電子イメージにあります)。
2. イメージをローカル・ドライブに解凍します。そのディレクトリーは、以下の通りです。
  - Microsoft Windows: AppScanSrc\_Installer.exe を実行します
  - Linux: 32 ビット・システム上で setup.bin を実行します。64 ビット・システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180>を参照してください。
  - macOS: setup.dmg を開き、setup.command スクリプトを実行します。

インストール・ウィザードの起動に関する詳細は、「IBM Security AppScan Source インストールと管理のガイド」の 69 ページの『インストール・ウィザードの開始』のトピックに記載されています。

3. インストール・パネルに表示される各国語を選択できる画面が表示されます。言語を選択し、「OK」をクリックして続行してください。
4. インストール・ウィザードを起動すると、「ようこそ - インストール・ウィザード」パネルが開き、現在開いているアプリケーションをすべて終了することを勧めるメッセージが表示されます。「次へ」をクリックして、インストール手順を開始します。
5. 「コンポーネントの選択」インストール・パネルで、インストールするコンポーネントを選択します。AppScan Source コンポーネントは、サーバー・コンポーネントとクライアント・コンポーネントに分けられます。
  - a. AppScan Source サーバー・コンポーネントをインストールするには、「サーバー・コンポーネントの選択」を選択し、インストールするコンポーネントを選択します。
    - AppScanSource データベース
    - AppScan Source for Automation
  - b. AppScan Source クライアント・コンポーネントをインストールするには、「クライアント・コンポーネントの選択」を選択し、インストールするコンポーネントを選択します。
    - AppScan Source for Analysis
    - AppScan Source コマンド行インターフェース
    - AppScan Source for Development for Eclipse, RAD, MobileFirst (デフォルトでは未選択)

- Windows のみ: AppScan Source for Development for Visual Studio 2013(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2013 を検出した場合のみ使用可能)
- Windows のみ: AppScan Source for Development for Visual Studio 2012(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2012 を検出した場合のみ使用可能)
- Windows のみ: AppScan Source for Development for Visual Studio 2010(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2010 を検出した場合のみ使用可能)

デフォルトでは、「クライアント・コンポーネントの選択」を選択する場合、AppScan Source for Development プラグイン・コンポーネントが選択解除されて、それ以外のすべてのコンポーネントが選択されています。

インストールしたいコンポーネントを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

6. 「サーバー接続」パネルで、以下のいずれかのオプションを選択します。
  - 「**AppScan Server** インスタンスに接続する」：このオプションを選択すると、リモートの AppScan Enterprise Server をテストして、AppScan Source への接続に使用できることを確認できます。サーバー接続をテストするには、以下のフィールドにデータを入力します。
    - **AppScan Enterprise Server**: 既存の URL 形式で、ご使用のリモート AppScan Enterprise Server インスタンスのホスト名を指定します。
    - 製品管理者: AppScan Enterprise Server 管理者ユーザー ID を指定します。
    - パスワード: AppScan Enterprise Server 管理者ユーザー ID のパスワードを指定します。

サーバー設定を入力したら、「接続のテスト」をクリックして、AppScan Source との接続にそのサーバーを使用できることを確認します。

- 「サーバーを指定せずに続行する」：サーバーを指定しないで先に進む場合には、このオプションを選択します。

#### 重要:

- 接続先の Enterprise Server で NIST 800-131a 準拠が有効になっている場合は、サーバーへの接続をテストできません。この場合には、サーバーを指定せずに進んでください。AppScan Source および Enterprise Server のインストール完了後に、86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』の説明に従ってください。その際に必ず「**TLSv1.2** を強制」オプションを適用してください。
- AppScan Enterprise Server が Common Access Card (CAC) 認証を使用して設定されている場合、「サーバーを指定せずに続行する」を選択し、すべてのサーバー接続の設定とテストに appscanserverdbmgr\_cac ユーティリティを使用します。

「次へ」をクリックして、次のインストール・パネルに進みます。

7. 「インストール・ターゲットの指定」ページで、インストール・ディレクトリーを指定します。オペレーティング・システムごとのデフォルトのディレクトリーは、次のとおりです。
  - 32 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files\IBM\AppScanSource
  - 64 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource
  - Linux: root ユーザーの場合は、インストール・ウィザードによって /opt/ibm/appscansource にソフトウェアがインストールされます。 root ユーザーではない場合は、デフォルトでは <home\_directory>/AppScan\_Source にインストールされる AppScan Source for Development Eclipse プラグインをインストールできます。
  - macOS: /Applications/AppScanSource.app

**重要:**

- インストール・ディレクトリー名には、英文字のみを含めることができません。非英文字を含む名前があるフォルダーは許可されません。
- Windows にインストールする場合、AppScan Source コンポーネントをインストールするには管理者特権が付与されている必要があります。
- Linux にインストールする場合、AppScan Source サーバー・コンポーネントをインストールするには、root 特権が必要です。

「次へ」をクリックして、次のインストール・パネルに進みます。

8. 「サーバー・コンポーネントの選択」ページで IBM Security AppScan Source データベース・コンポーネントをインストール対象として選択した場合は、「データベース選択」パネルが表示されます。このページで、以下のいずれかを選択します。
  - **solidDB** のインストール
  - 既存の **Oracle 11g/12c Server** にデータベースをインストール

solidDB のインストール、または既存の Oracle データベースへのインストールについては詳しくは、「IBM Security AppScan Source インストールと管理のガイド」の 74 ページの『データベースのインストールおよび AppScan Enterprise Server への接続の構成』のトピックを参照してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

9. 「データベース選択」パネルで solidDB データベースのインストールを選択した場合は、「solidDB 管理ユーザーの構成」パネルのプロンプトが出されます。このパネルで、solidDB データベース管理者アカウントを構成します。デフォルトのデータベース管理者のユーザー名とパスワードはどちらも **dba** です。このユーザー名は変更できませんが、パスワードは変更できます。

注: 製品のインストールを完了した後にユーザー・パスワードを変更する方法については、157 ページの『第 17 章 インストール後の solidDB ユーザー・パスワードの変更』を参照してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

10. 「solidDB AppScan Source ユーザーの構成」パネルでは、solidDB AppScan Source データベースのユーザー・アカウントを構成できます。デフォルト・ユーザー名 **ounce** とデフォルト・パスワード **ounce** はそのままでも構いません。AppScan Source データベースに対して読み取り/書き込みを行うコンポーネントはすべてこのアカウントを使用します。

注:

- ユーザー名とパスワードを変更した場合は、IBM サポート担当員が AppScan Source データベースにアクセスする必要がある場合に備えて、新しい構成を記録しておいてください。
- 製品のインストールを完了した後にユーザー・パスワードを変更する方法については、157 ページの『第 17 章 インストール後の solidDB ユーザー・パスワードの変更』を参照してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

11. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つまり、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できません)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

12. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
13. 先に進む前に、インストール・オプションの概要を確認します。選択内容を変更する場合は、「前へ」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。インストーラーによって、ハード・ディスクにファイルがコピーされます。

Linux サーバー・インストールの場合のみ: ファイルをコピーしたら、デーモン・ユーザーを特定する必要があります。デフォルト・ユーザー「ounce」を作成する場合は「ユーザー '**ounce**' を作成」を選択し、既存のユーザーで実行する場合は「既存のユーザーで実行」を選択します。(インストールでこのユーザーの存在が検証されます。選択されたユーザーには有効なシェルが必要となることに注意してください。)

インストール中に「キャンセル」をクリックすると、そのタイミングにかかわらず、すべてのコンポーネントがアンインストールされます。

14. 「IBM Security AppScan Enterprise Server の構成」パネルで、solidDB データベースが AppScan Enterprise Server に接続できるようにするための設定を指定します。デフォルトでは、このインストール・パネルに、データベースとサーバーが同じマシンにデフォルト設定でインストールされていると想定した値が事前に入力されています。AppScan Enterprise Server で AppScan Source データベースを構成するには、「**AppScan Enterprise Server** を今すぐ構成」チェック・ボックスを選択して、以下の設定を行います。

- **AppScan Enterprise Server:** ご使用の AppScan Enterprise Server インスタンスの URL を指定します。
- **ユーザー ID:** AppScan Enterprise Server 管理者ユーザー ID を指定します。サーバーが Windows 認証用に構成されている場合は、サーバーにアカウントを追加したときに使用した Windows のユーザー ID を入力してください (ユーザー ID にはフォーマット <host name>%<user id> を使用する必要があります)。
- **パスワード:** AppScan Enterprise Server ユーザー ID のパスワードを指定します。
- **データベース・ホスト名:** AppScan Source データベースをインストールしたマシンのホスト名を指定します。

注: このフィールドの入力内容は必ず、インストーラーを実行しているマシンの完全修飾ホスト名にしてください。この値は、インストール時にこのフィールドに事前に入力されます。事前に入力された値が誤っている場合に限って変更してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

注: Oracle データベースを使用する予定の場合は、「**AppScan Enterprise Server** を今すぐ構成」が選択されていないことを確認し、「次へ」をクリックします。このインストール・パネルは、Oracle データベースの Enterprise Server への登録に使用されません。代わりに、AppScan Source に組み込まれているユーティリティーを使用してインストール後にデータベース接続を構成できます。これに関する説明は、「*IBM Security AppScan Source* インストールと管理のガイド」の 86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』のトピックに記載されています。このユーティリティーを使用すると、インストール・パネルを使用する代わりに solidDB 接続を構成することもできます。

15. 「インストール完了」パネルでは、「**IBM Security AppScan Source License Manager** の起動」を選択することにより、インストール・ウィザードの終了後にただちに製品のアクティベーションを開始することができます。「完了」をクリックして標準インストールを完了し、インストール・ウィザードを終了します。

16. License Manager ユーティリティーで、以下のようになります。

- a. ライセンス・ファイルを適用するには、「インポート」をクリックしてからダウンロード済みの AppScan Source ライセンスを参照します。
- b. フローティング・ライセンスを適用するには、「ライセンス・サーバーの構成」をクリックしてから「追加」をクリックします。フローティング・ライセンスを格納しているホスト・マシンに関する情報を入力します。

追加のアクティベーション手順については、123 ページの『第 8 章 ソフトウェアのアクティブ化』を参照してください。

## AppScan Source へのログイン

### このタスクについて

ログイン時に入力求められるフィールドの説明については、下記のセクションを参照してください。詳しくは、「*IBM Security AppScan Source* インストールと管理のガイド」の 139 ページの『第 12 章 AppScan Source 製品から AppScan Enterprise Server へのログイン』のトピックを参照してください。

### 手順

- **ユーザー ID:** ユーザー ID を指定します。
- **パスワード:** ご使用のユーザー ID のパスワードを指定します。
- **AppScan Enterprise Server:** 既存の URL 形式で、ご使用の AppScan Enterprise Server インスタンスのホスト名を指定します。AppScan Enterprise Server が同じマシンにある場合は、`https://localhost:9443/ase/` または `localhost` を指定します。AppScan Enterprise Server がリモート・マシンにある場合は、それがインストールされているマシンの完全修飾ホスト名を指定します。

ヒント: 完全修飾ホスト名を入力してもうまくいかない場合には、ホスト・マシンの IP アドレスを入力してみてください。

---

## 第 4 章 AppScan Source のアップグレード

### 手順

1. インストールの説明に従って AppScan Enterprise Server をアップグレードします。サーバーについて詳しくは、72 ページの『AppScan Enterprise Server の概要』を参照してください。
2. IBM Security AppScan Source 製品の zip ファイルを見つけます (AppScan Source メディア・パックにあるか、または IBM パスポート・アドバンテージで AppScan Source eAssembly の一部としてダウンロードした電子イメージにあります)。
3. イメージをローカル・ドライブに解凍します。そのディレクトリーは、以下の通りです。
  - Microsoft Windows: AppScanSrc\_Installer.exe を実行します
  - Linux: 32 ビット・システム上で setup.bin を実行します。64 ビット・システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180>を参照してください。
  - macOS: setup.dmg を開き、setup.command スクリプトを実行します。

インストール・ウィザードの起動に関する詳細は、「IBM Security AppScan Source インストールと管理のガイド」の 69 ページの『インストール・ウィザードの開始』のトピックに記載されています。

4. インストール・パネルに表示される各国語を選択できる画面が表示されます。言語を選択し、「OK」をクリックして続行してください。
5. インストール・ウィザードを起動すると、「ようこそ - インストール済み環境のアップグレード・ウィザード」パネルが開き、現在開いているアプリケーションをすべて終了することを勧めるメッセージが表示されます。「次へ」をクリックして先に進みます。
6. 既存のインストール済み環境に AppScan Source データベースが存在する場合、「サーバー接続」パネルが表示され、次にデータベースのアップグレードと保守のパネルが表示されます。
7. 「サーバー接続」パネルで、以下のいずれかのオプションを選択します。
  - 「AppScan Server インスタンスに接続する」：このオプションを選択すると、リモートの AppScan Enterprise Server をテストして、AppScan Source への接続に使用できることを確認できます。サーバー接続をテストするには、以下のフィールドにデータを入力します。
    - AppScan Enterprise Server: 既存の URL 形式で、ご使用のリモート AppScan Enterprise Server インスタンスのホスト名を指定します。
    - 製品管理者: AppScan Enterprise Server 管理者ユーザー ID を指定します。
    - パスワード: AppScan Enterprise Server 管理者ユーザー ID のパスワードを指定します。

サーバー設定を入力したら、「接続のテスト」をクリックして、AppScan Source との接続にそのサーバーを使用できることを確認します。

- 「サーバーを指定せずに続行する」：サーバーを指定しないで先に進む場合には、このオプションを選択します。

**重要:**

- 接続先の Enterprise Server で NIST 800-131a 準拠が有効になっている場合は、サーバーへの接続をテストできません。この場合には、サーバーを指定せずに進んでください。AppScan Source および Enterprise Server のインストール完了後に、86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』の説明に従ってください。その際に必ず「TLSv1.2 を強制」オプションを適用してください。
- AppScan Enterprise Server が Common Access Card (CAC) 認証を使用して設定されている場合、「サーバーを指定せずに続行する」を選択し、すべてのサーバー接続の設定とテストに appscanserverdbmgr\_cac ユーティリティを使用します。

「次へ」をクリックして、次のインストール・パネルに進みます。

8. 次のインストール・パネルで、インストール中に データベース が更新されること、およびその更新に約 30 分かかる可能性があることが示されます。データベース のアップグレード中には、インストールを取り消したりコンピュータの電源を遮断したりしないでください。「次へ」をクリックします。
9. データベースの保守を容易にするために、solidDB AppScan Source データベース・ユーザー・アカウントの資格情報を入力し、データベースのアップグレードを続行する準備が整ったら「次へ」をクリックします。
10. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つまり、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できません)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

11. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
12. 先に進む前に、インストール・オプションの概要を確認します。選択内容を変更する場合は、「前へ」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。インストーラーによって、ハード・ディスクにファイルがコピーされます。

Linux サーバー・インストールの場合のみ: ファイルをコピーしたら、デモン・ユーザーを特定する必要があります。 デフォルト・ユーザー「ounce」を作成する場合は「ユーザー 'ounce' を作成」を選択し、既存のユーザーで実行する場合は「既存のユーザーで実行」を選択します。(インストールでこのユーザーの存在が検証されます。選択されたユーザーには有効なシェルが必要となることに注意してください。)

インストール中に「キャンセル」をクリックすると、そのタイミングにかかわらず、すべてのコンポーネントがアンインストールされます。

13. 「IBM Security AppScan Enterprise Server の構成」パネルで、solidDB データベースが AppScan Enterprise Server に接続できるようにするための設定を指定します。デフォルトでは、このインストール・パネルに、データベースとサーバーが同じマシンにデフォルト設定でインストールされていると想定した値が事前に入力されています。AppScan Enterprise Server で AppScan Source データベース を構成するには、「**AppScan Enterprise Server** を今すぐ構成」チェック・ボックスを選択して、以下の設定を行います。

- **AppScan Enterprise Server:** ご使用の AppScan Enterprise Server インスタンスの URL を指定します。
- **ユーザー ID:** AppScan Enterprise Server 管理者ユーザー ID を指定します。サーバーが Windows 認証用に構成されている場合は、サーバーにアカウントを追加したときに使用した Windows のユーザー ID を入力してください(ユーザー ID にはフォーマット <host name>¥<user id> を使用する必要があります)。
- **パスワード:** AppScan Enterprise Server ユーザー ID のパスワードを指定します。
- **データベース・ホスト名:** AppScan Source データベース をインストールしたマシンのホスト名を指定します。

注: このフィールドの入力内容は必ず、インストーラーを実行しているマシンの完全修飾ホスト名にしてください。この値は、インストール時にこのフィールドに事前に入力されます。事前に入力された値が誤っている場合に限って変更してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

注: Oracle データベースを使用する予定の場合は、「**AppScan Enterprise Server** を今すぐ構成」が選択されていないことを確認し、「次へ」をクリックします。このインストール・パネルは、Oracle データベースの Enterprise Server への登録に使用されません。代わりに、AppScan Source に組み込まれているユーティリティーを使用してインストール後にデータベース接続を構成できます。これに関する説明は、「IBM Security AppScan Source インストールと管理のガイド」の 86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』のトピックに記載されています。このユーティリティーを使用すると、インストール・パネルを使用する代わりに solidDB 接続を構成することもできます。

14. 「インストール完了」パネルでは、「**IBM Security AppScan Source License Manager** の起動」を選択することにより、インストール・ウィザード

の終了後にただちに製品のアクティベーションを開始することができます。  
「完了」をクリックして標準インストールを完了し、インストール・ウィザードを終了します。

15. License Manager ユーティリティーで、以下のようになります。
    - a. ライセンス・ファイルを適用するには、「インポート」をクリックしてからダウンロード済みの AppScan Source ライセンスを参照します。
    - b. フローティング・ライセンスを適用するには、「ライセンス・サーバーの構成」をクリックしてから「追加」をクリックします。フローティング・ライセンスを格納しているホスト・マシンに関する情報を入力します。
- 追加のアクティベーション手順については、123 ページの『第 8 章 ソフトウェアのアクティブ化』を参照してください。

## タスクの結果

AppScan Source バージョン 8.7 では、アプリケーション・データはインストール・ディレクトリー以外の場所に保管されます。AppScan Source バージョン 8.6.x 以前からアップグレードする場合、既存のアプリケーション・データは 70 ページの『デフォルトの AppScan Source データ・ディレクトリー』に移動されます。さらに、既存の (バージョン 8.7 より前の) アプリケーション・データのバックアップは、<data\_dir>/upgrade\_backup (<data\_dir> は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。) に保管されます。

AppScan Source バージョン 9.0 では、AppScan Source for Development Eclipse プラグイン は macOS でサポートされます。macOS 上で AppScan Source バージョン 8.8.x 以前からアップグレードする場合、アップグレードの完了後に AppScan Source for Development 機能を Eclipse 環境にインストールできるようになります (これらの機能を使用するには、適切なライセンスが必要です)。AppScan Source for Development を Eclipse 環境にインストールする方法については、97 ページの『AppScan Source for Development (Eclipse プラグイン) を Eclipse およびサポートされている Eclipse ベースの製品に適用』を参照してください。

---

## 第 5 章 拡張インストールおよびアクティベーションのトピック

このセクションでは、拡張インストール・オプションおよびアクティベーション手順について説明します。

AppScan Source ソフトウェアは、IBM パスポート・アドバンテージ からダウンロードされるか、またはメディア・パックとして購入されます。アクティベーション・ライセンスは、IBM Rational License Key Center から取得します。

Windows、Linux、および macOS では、自己解凍型インストール・ファイルが使用可能です。これらのインストール・ファイルによって、以下の設定ファイルが生成されます。

- Windows: AppScanSrc\_Installer.exe
- Linux: setup.bin
- macOS: setup.dmg

インストール・ウィザードを使用すると、その指示に従って、インストール先のオペレーティング・システムでサポートされているすべての AppScan Source コンポーネントをすぐに使用可能な状態でインストールできます。

インストールが完了したら、最後のインストール・パネルからオプションでアクティベーション License Manager を起動できます。または、後で製品をアクティブ化することもできます。

**重要:** ソフトウェアを使用するには、その前にソフトウェアをアクティブ化する必要があります。

AppScan Source コンポーネントをインストールするには、ご使用の環境およびデプロイメントの要件について十分理解していることが必要です (詳細は 20 ページの『AppScan Source のデプロイメント・モデル』を参照)。例えば、リモートの AppScan Enterprise Server に接続していないノートブック・コンピューター上で AppScan Source for Analysis を実行するには、AppScan Source for Analysis と AppScan Enterprise Server をそのノートブックにインストールする必要があります。

### 標準デスクトップ

標準デスクトップ・インストール環境は、ネットワークから切断されているときでも AppScan Source for Analysis を単一コンピューター上で実行するために必要なクライアント・コンポーネントとサーバー・コンポーネントで構成されます (このインストール・タイプは、AppScan Enterprise Server もコンピューターにインストールする必要があります)。標準デスクトップ・インストールのコンポーネント・オプションは、以下のとおりです。

- サーバー・コンポーネント:
  - AppScanSource データベース
  - AppScan Source for Automation

- クライアント・コンポーネント:
  - AppScan Source for Analysis
  - AppScan Source コマンド行インターフェース
  - AppScan Source for Development for Eclipse、RAD、MobileFirst (デフォルトでは未選択)
  - Windows のみ: AppScan Source for Development for Visual Studio 2013(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2013 を検出した場合のみ使用可能)
  - Windows のみ: AppScan Source for Development for Visual Studio 2012(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2012 を検出した場合のみ使用可能)
  - Windows のみ: AppScan Source for Development for Visual Studio 2010(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2010 を検出した場合のみ使用可能)

## サーバー

インストール対象として選択できるサーバー・コンポーネントは以下のとおりです。

- AppScanSource データベース
- AppScan Source for Automation

## クライアント

インストール対象として選択できるクライアント・コンポーネントは以下のとおりです。

- AppScan Source for Analysis
- AppScan Source コマンド行インターフェース
- AppScan Source for Development for Eclipse、RAD、MobileFirst (デフォルトでは未選択)
- Windows のみ: AppScan Source for Development for Visual Studio 2013(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2013 を検出した場合のみ使用可能)
- Windows のみ: AppScan Source for Development for Visual Studio 2012(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2012 を検出した場合のみ使用可能)
- Windows のみ: AppScan Source for Development for Visual Studio 2010(デフォルトでは未選択)(このオプションは、インストーラーがご使用のシステム上に Microsoft Visual Studio 2010 を検出した場合のみ使用可能)

---

## インストール・ウィザードの開始

AppScan Source のインストール・ウィザードは、Microsoft Windows、Linux、および macOS オペレーティング・システムで動作します。

インストールを開始するには、以下の手順を実行します。

- Microsoft Windows: AppScanSrc\_Installer.exe を実行します
- Linux: 32 ビット・システム上で setup.bin を実行します。64 ビット・システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180>を参照してください。
- macOS: setup.dmg を開き、setup.command スクリプトを実行します。

**重要:** Windows 8 以上では、インストーラーは Windows 7 互換モードで実行する必要があります。これを行うには、AppScanSrc\_Installer.exe を右クリックして、「プロパティ」を選択します。「プロパティ」ウィンドウで、「互換性」タブを選択し、「互換モードでこのプログラムを実行する」チェック・ボックスを選択して「**Windows 7**」になるようメニューを設定します。「**OK**」をクリックして変更した後、AppScanSrc\_Installer.exe を実行して AppScan Source のインストールを開始します。

ウィザードにより、ネットワーク・ポートが使用可能かどうかチェックされます。競合が検出された場合は、インストールを終了する必要があります。必要なポートについて詳しくは、155 ページの『第 16 章 ポート構成』を参照してください。

インストール・ウィザードを初めて起動すると、インストール・パネルに表示される各国語を選択できる画面が表示されます。言語を選択し、「**OK**」をクリックして続行してください。

インストール・ウィザードを起動すると、「ようこそ - インストール・ウィザード」パネルが開き、現在開いているアプリケーションをすべて終了することを勧めるメッセージが表示されます。「次へ」をクリックして、インストール手順を開始します (インストール・ファイルの場所については『インストールとユーザー・データ・ファイルの場所』を参照してください)。

---

## インストールとユーザー・データ・ファイルの場所

AppScan Source をインストールすると、ユーザー・データ・ファイルおよび構成ファイルは、インストール・ディレクトリー以外の場所に保管されます。

- 『デフォルトのインストール場所』
- 70 ページの『デフォルトの AppScan Source データ・ディレクトリー』
- 70 ページの『AppScan Source 一時ファイルの場所』

### デフォルトのインストール場所

AppScan Source をインストールすると、ソフトウェアは以下のいずれかのデフォルトの場所に配置されます。

- 32 ビット・バージョンの Microsoft Windows:  
`<SYSTEMDRIVE>:\Program Files\IBM\AppScanSource`

- 64 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource
- Linux: root ユーザーの場合は、インストール・ウィザードによって /opt/ibm/appscansource にソフトウェアがインストールされます。 root ユーザーではない場合は、デフォルトでは <home\_directory>/AppScan\_Source にインストールされる AppScan Source for Development Eclipse プラグインをインストールできます。
- macOS: /Applications/AppScanSource.app

#### 重要:

- インストール・ディレクトリー名には、英文字のみを含めることができます。非英文字を含む名前があるフォルダーは許可されません。
- Windows にインストールする場合、AppScan Source コンポーネントをインストールするには管理者特権が付与されている必要があります。
- Linux にインストールする場合、AppScan Source サーバー・コンポーネントをインストールするには、root 特権が必要です。

### デフォルトの **AppScan Source** データ・ディレクトリー

AppScan Source データは、構成ファイル、サンプル・ファイル、およびログ・ファイルなどの項目からなります。AppScan Source をインストールすると、データ・ファイルはデフォルトで以下の場所に配置されます。

- Microsoft Windows: <SYSTEMDRIVE>:\ProgramData\IBM\AppScanSource

注: ProgramData\ は隠しフォルダーです。このフォルダーを表示するには、エクスプローラーの表示設定を変更して、隠しファイルと隠しフォルダーが表示されるようにする必要があります。

- Linux: /var/opt/ibm/appscansource
- macOS: /Users/Shared/AppScanSource

AppScan Source データ・ディレクトリーの場所を変更する方法については、71 ページの『AppScan Source データ・ディレクトリーの変更』を参照してください。

### **AppScan Source** 一時ファイルの場所

AppScan Source 操作のなかには、一時ファイルが作成されるものがあります。これらの一時ファイルは、デフォルトで以下の場所に保管されます。

- Microsoft Windows: <SYSTEMDRIVE>:\ProgramData\IBM\AppScanSource\temp

注: ProgramData\ は隠しフォルダーです。このフォルダーを表示するには、エクスプローラーの表示設定を変更して、隠しファイルと隠しフォルダーが表示されるようにする必要があります。

- Linux: /var/opt/ibm/appscansource/temp
- macOS: /Users/Shared/AppScanSource/temp

一時ファイルの場所は、常に、AppScan Source データ・ディレクトリー内の temp ディレクトリーになります。データ・ディレクトリーを変更することにより、一時

ファイルの場所を変更できます。変更方法については、『AppScan Source データ・ディレクトリの変更』を参照してください。これによって、ユーザーが選択したデータ・ディレクトリに temp が配置されます。

## AppScan Source データ・ディレクトリの変更

ハード・ディスク・スペースを管理するために、AppScan Source データ・ディレクトリの場所を変更することができます。AppScan Source のインストール後に、このトピックに記載されている手順に従って、データ・ディレクトリの場所を変更できます。

### 始める前に

このタスクを実行する前に、すべての AppScan Source クライアント・アプリケーションを終了またはシャットダウンしていることを確認してください。AppScan Source クライアント・アプリケーションには、以下のものがあります。

- AppScan Source for Analysis
- AppScan Source for Development (Eclipse または Visual Studio プラグイン)(Windows および Linux でのみサポートされます)
- AppScan Source コマンド行インターフェース (CLI)
- AppScan Source for Automation

また、AppScan Source for Automation をインストールしている場合は、Automation Server が以下のようにしてシャットダウンされていることを確認してください。

- Windows の場合は、**IBM Security AppScan Source Automation** サービスを停止します。
- Linux の場合は、次のコマンドを実行します: `/etc/init.d/onceautod stop`
- macOS の場合は、コマンド `launchctl stop com.ibm.appscan.autod` を発行します。

### 手順

1. `APPSCAN_SOURCE_SHARED_DATA=<data_dir>` 環境変数を定義します。ここで、`<data_dir>` は AppScan Source データを保管する場所です。

注:

- `<data_dir>` の場所は、AppScan Source がインストールされているマシンと同じマシン上の既存の完全な絶対パスでなければなりません。
  - `<data_dir>` ディレクトリ名には、英文字のみを含めることができます。非英文字を含む名前があるフォルダーは許可されません。
2. AppScan Source のインストール時に作成されたデフォルトのデータ・ディレクトリを見つけます (データ・ディレクトリのデフォルトの場所については、70 ページの『デフォルトの AppScan Source データ・ディレクトリ』を参照してください)。
  3. デフォルト・データ・ディレクトリのコンテンツを、環境変数で指定した `<data_dir>` の場所にコピーまたは移動します。

4. **AppScan Source for Automation** を **Linux** 上にインストールしている場合のみ、以下を行います。

- a. `/etc/init.d/ounceautod` ファイルを編集します。
- b. 以下の行を見つけます。

```
su - ounce -c
'export LD_LIBRARY_PATH="/opt/IBM/AppScan_Source/bin":$LD_LIBRARY_PATH &&
cd "/opt/IBM/AppScan_Source/bin" &&
"/opt/IBM/AppScan_Source/bin/ounceautod" -s' >>
"/var/opt/ibm/appscansource/logs/ounceautod_output.log" 2>&1 &
```

この行を以下の行に置き換えます。

```
su - ounce -c
'export APPSCAN_SOURCE_SHARED_DATA=<new data directory path here> &&
export LD_LIBRARY_PATH="/opt/IBM/AppScan_Source/bin":$LD_LIBRARY_PATH &&
cd "/opt/IBM/AppScan_Source/bin" &&
"/opt/IBM/AppScan_Source/bin/ounceautod" -s' >>
"<new data directory path here>/logs/ounceautod_output.log" 2>&1 &
```

注: 上記のコマンドは、1 行で入力してください。

- c. `/etc/init.d/ounceautod` ファイルを保存します。

## 次のタスク

AppScan Source for Automation をインストールしている場合は、以下のようにして Automation Server を開始します。

- Windows の場合は、**IBM Security AppScan Source Automation** サービスを開始します。
- Linux の場合は、次のコマンドを実行します: `/etc/init.d/ounceautod start`
- macOS の場合は、コマンド `launchctl start com.ibm.appscan.autod` を発行します。

---

## AppScan Enterprise Server の概要

AppScan Enterprise Server は、別個にインストール可能なコンポーネントです。このサーバーは、ユーザーの集中管理機能と、AppScan Source データベースを介して評価を共有するメカニズムを提供します。さらに、管理者が AppScan Enterprise Server の Enterprise Console コンポーネントをインストールしている場合は、Enterprise Console に評価を公開することができます。Enterprise Console は、レポート機能、問題管理、トレンド分析、ダッシュボードなど、評価に関する作業を行うためのさまざまなツールを備えています。ほとんどの AppScan Source 製品およびコンポーネントは、AppScan Enterprise Server と通信する必要があります。このコンポーネントがなくても、AppScan Source for Development をローカル・モードで使用できますが、カスタム・ルール、共有スキャン構成、および共有フィルターなどの機能は使用できません。

重要: AppScan Source および AppScan Enterprise の一部のバージョンでは、AppScan Source から AppScan Enterprise Server に接続するために 2 つの製品のバージョンとリリース・レベルが一致していなければなりません。

<http://www.ibm.com/support/docview.wss?uid=swg21975211> を参照して、どのバージョンの AppScan Source と AppScan Enterprise に互換性があるかを確認してください。

AppScan Enterprise Server を実行するために必要なハードウェアおよびソフトウェアについては詳しくは、<http://www.ibm.com/support/docview.wss?uid=swg27027541> を参照してください。

AppScan Enterprise Server のインストールについては、「AppScan Enterprise 計画およびインストール・ガイド」または IBM Knowledge Center の AppScan Enterprise Server ユーザー・アシスタンス (<http://www.ibm.com/support/knowledgecenter/SSW2NF/welcome>) を参照してください。

AppScan Source と併用する場合、AppScan Enterprise Server には、AppScan Source インストール・ウィザードによってインストールされた solidDB データベース・サーバー、または AppScan Source インストール・ウィザードによって AppScan Source のスキーマとデータが適用された既存の Oracle データベース・サーバーが必要です。

**重要:** 接続先の AppScan Enterprise Server で NIST 800-131a コンプライアンスが有効になっている場合、AppScan Source を設定してトランスポート層セキュリティ V1.2 を強制する必要があります。トランスポート層セキュリティ V1.2 が強制されない場合、サーバーへの接続は失敗します。

- AppScan Source データベースをインストールしていない場合 (例えば、クライアント・コンポーネントのみをインストールしている場合など)、  
<data\_dir>%config%ounce.ozsettings (<data\_dir> は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。) を変更してトランスポート層セキュリティ V1.2 を強制することができます。このファイルで、以下の設定を見つけます。

```
<Setting
  name="tls_protocol_version"
  read_only="false"
  default_value="0"
  value="0"
  description="Minor Version of the TLS Connection Protocol"
  type="text"
  display_name="TLS Protocol Version"
  display_name_id=""
  available_values="0:1:2"
  hidden="false"
  force_upgrade="false"
/>
```

この設定で、value="0" を value="2" に変更し、ファイルを保存します。

- AppScan Source データベースをインストールしている場合は、AppScan Source と Enterprise Server の両方をインストールした後に、IBM Security AppScan Enterprise Server データベース構成ツールでトランスポート層セキュリティ V1.2 を強制します。

IBM Security AppScan Enterprise Server データベース構成ツールについては、86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』を参照してください。

---

## データベースのインストールおよび **AppScan Enterprise Server** への接続の構成

AppScan Source には、AppScan Source インストール・ウィザードによってインストールされた solidDB データベース・サーバーか、AppScan Source インストール・ウィザードによって AppScan Source のスキーマとデータが適用された既存の Oracle データベース・サーバーが必要です。データベースには、AppScan Source セキュリティー・ナレッジ・データベースのデータ、評価データ、およびアプリケーション/プロジェクト・インベントリが保持されます。データベース・サーバーのインストールおよび構成のオプションの概要について、このトピックで説明します。

**重要:** スキャン中は、AppScan Enterprise Server および AppScan Source のクライアント (AppScan Source for Development 以外) はいずれも、AppScan Source データベース (solidDB または Oracle のいずれか) への直接接続が必要です。

**注:** AppScan Source サーバー・コンポーネント (AppScan Source データベースなど) は、macOS でサポートされていません。

### **solidDB** のインストールおよび構成

インストール・プロセス時、データベースをインストールしてから、AppScan Enterprise Server がデータベースと接続できるように、solidDB ログイン設定を指定します。このシナリオのインストール方法については、『solidDB のインストールおよび構成』を参照してください。

### 既存の **Oracle** データベースへのインストール

AppScan Source データベースのスキーマとデータを、既存の Oracle データベースに適用します。インストール・プロセスで、Oracle データベースのログイン設定を指定して、AppScan Enterprise Server がデータベースに接続できるようにします。このシナリオのインストール方法については、79 ページの『既存の Oracle データベースへのインストール』を参照してください。

## **solidDB** のインストールおよび構成

### このタスクについて

このタスク・トピックでは、solidDB および AppScan Enterprise Server をインストールし、構成する手順について説明します。

**注:** AppScan Source サーバー・コンポーネント (AppScan Source データベースなど) は、macOS でサポートされていません。

### 手順

1. AppScan Enterprise Server に付属しているインストールの説明に従って AppScan Enterprise Server をインストールします。サーバーについては詳しくは、72 ページの『AppScan Enterprise Server の概要』を参照してください。

2. IBM Security AppScan Source 製品の zip ファイルを見つけます (AppScan Source メディア・パックにあるか、またはIBM パスポート・アドバンテージで AppScan Source eAssembly の一部としてダウンロードした電子イメージにあります)。
3. イメージをローカル・ドライブに解凍します。そのディレクトリーは、以下の通りです。
  - Microsoft Windows: AppScanSrc\_Installer.exe を実行します
  - Linux: 32 ビット・システム上で setup.bin を実行します。64 ビット・システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180>を参照してください。
  - macOS: setup.dmg を開き、setup.command スクリプトを実行します。

インストール・ウィザードの起動に関する詳細は、「IBM Security AppScan Source インストールと管理のガイド」の 69 ページの『インストール・ウィザードの開始』のトピックに記載されています。

4. 「コンポーネントの選択」インストール・パネルでは、「サーバー・コンポーネントの選択」を選択してから、AppScanSource データベース が選択されていることを確認します。「次へ」をクリックして、次のインストール・パネルに進みます。
5. 「サーバー接続」パネルで、以下のいずれかのオプションを選択します。
  - 「**AppScan Server** インスタンスに接続する」：このオプションを選択すると、リモートの AppScan Enterprise Server をテストして、AppScan Source への接続に使用できることを確認できます。サーバー接続をテストするには、以下のフィールドにデータを入力します。
    - **AppScan Enterprise Server**: 既存の URL 形式で、ご使用のリモート AppScan Enterprise Server インスタンスのホスト名を指定します。
    - 製品管理者: AppScan Enterprise Server 管理者ユーザー ID を指定します。
    - パスワード: AppScan Enterprise Server 管理者ユーザー ID のパスワードを指定します。

サーバー設定を入力したら、「接続のテスト」をクリックして、AppScan Source との接続にそのサーバーを使用できることを確認します。

- 「サーバーを指定せずに続行する」：サーバーを指定しないで先に進む場合には、このオプションを選択します。

**重要:**

- 接続先の Enterprise Server で NIST 800-131a 準拠が有効になっている場合は、サーバーへの接続をテストできません。この場合には、サーバーを指定せずに進んでください。AppScan Source および Enterprise Server のインストール完了後に、86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』の説明に従ってください。その際に必ず「**TLSv1.2** を強制」オプションを適用してください。

- AppScan Enterprise Server が Common Access Card (CAC) 認証を使用して設定されている場合、「サーバーを指定せずに続行する」を選択し、すべてのサーバー接続の設定とテストに appscanserverdbmgr\_cac ユーティリティを使用します。

「次へ」をクリックして、次のインストール・パネルに進みます。

6. 「インストール・ターゲットの指定」ページで、インストール・ディレクトリを指定します。オペレーティング・システムごとのデフォルトのディレクトリは、次のとおりです。
  - 32 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files\IBM\AppScanSource
  - 64 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource
  - Linux: root ユーザーの場合は、インストール・ウィザードによって /opt/ibm/appscansource にソフトウェアがインストールされます。root ユーザーではない場合は、デフォルトでは <home\_directory>/AppScan\_Source にインストールされる AppScan Source for Development Eclipse プラグインをインストールできます。
  - macOS: /Applications/AppScanSource.app

**重要:**

- インストール・ディレクトリ名には、英文字のみを含めることができます。非英文字を含む名前があるフォルダーは許可されません。
- Windows にインストールする場合、AppScan Source コンポーネントをインストールするには管理者特権が付与されている必要があります。
- Linux にインストールする場合、AppScan Source サーバー・コンポーネントをインストールするには、root 特権が必要です。

「次へ」をクリックして、次のインストール・パネルに進みます。

7. 「サーバー・コンポーネントの選択」ページで IBM Security AppScan Source データベース・コンポーネントをインストール対象として選択した場合は、「データベース選択」パネルが表示されます。このページで、「solidDB のインストール」ラジオ・ボタンを選択し、「次へ」をクリックして次のインストール・パネルに進みます。
8. 「データベース選択」パネルで solidDB データベースのインストールを選択した場合は、「solidDB 管理ユーザーの構成」パネルのプロンプトが出されます。このパネルで、solidDB データベース管理者アカウントを構成します。デフォルトのデータベース管理者のユーザー名とパスワードはどちらも **dba** です。このユーザー名は変更できませんが、パスワードは変更できます。

注: 製品のインストールを完了した後にユーザー・パスワードを変更する方法については、157 ページの『第 17 章 インストール後の solidDB ユーザー・パスワードの変更』を参照してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

9. 「solidDB AppScan Source ユーザーの構成」パネルでは、solidDB AppScan Source データベースのユーザー・アカウントを構成できます。デフォルト・

ユーザー名 **ounce** とデフォルト・パスワード **ounce** はそのままでも構いません。AppScan Source データベースに対して読み取り/書き込みを行うコンポーネントはすべてこのアカウントを使用します。

注:

- ユーザー名とパスワードを変更した場合は、IBM サポート担当員が AppScan Source データベースにアクセスする必要がある場合に備えて、新しい構成を記録しておいてください。
- 製品のインストールを完了した後にユーザー・パスワードを変更する方法については、157 ページの『第 17 章 インストール後の solidDB ユーザー・パスワードの変更』を参照してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

10. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つまり、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できません)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

11. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
12. 先に進む前に、インストール・オプションの概要を確認します。選択内容を変更する場合は、「前へ」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。インストーラーによって、ハード・ディスクにファイルがコピーされます。

Linux サーバー・インストールの場合のみ: ファイルをコピーしたら、デモン・ユーザーを特定する必要があります。デフォルト・ユーザー「ounce」を作成する場合は「ユーザー 'ounce' を作成」を選択し、既存のユーザーで実行する場合は「既存のユーザーで実行」を選択します。(インストールでこのユーザーの存在が検証されます。選択されたユーザーには有効なシェルが必要となることに注意してください。)

インストール中に「キャンセル」をクリックすると、そのタイミングにかかわらず、すべてのコンポーネントがアンインストールされます。

13. 「IBM Security AppScan Enterprise Server の構成」パネルで、solidDB データベースが AppScan Enterprise Server に接続できるようにするための設定を指定します。デフォルトでは、このインストール・パネルに、データベースとサーバーが同じマシンにデフォルト設定でインストールされていると想定した

値が事前に入力されています。AppScan Enterprise Server で AppScan Source データベースを構成するには、「**AppScan Enterprise Server** を今すぐ構成」チェック・ボックスを選択して、以下の設定を行います。

- **AppScan Enterprise Server:** ご使用の AppScan Enterprise Server インスタンスの URL を指定します。
- **ユーザー ID:** AppScan Enterprise Server 管理者ユーザー ID を指定します。サーバーが Windows 認証用に構成されている場合は、サーバーにアカウントを追加したときに使用した Windows のユーザー ID を入力してください (ユーザー ID にはフォーマット <host name>¥<user id> を使用する必要があります)。
- **パスワード:** AppScan Enterprise Server ユーザー ID のパスワードを指定します。
- **データベース・ホスト名:** AppScan Source データベースをインストールしたマシンのホスト名を指定します。

注: このフィールドの入力内容は必ず、インストーラーを実行しているマシンの完全修飾ホスト名にしてください。この値は、インストール時にこのフィールドに事前に入力されます。事前に入力された値が誤っている場合に限って変更してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

注: Oracle データベースを使用する予定の場合は、「**AppScan Enterprise Server** を今すぐ構成」が選択されていないことを確認し、「次へ」をクリックします。このインストール・パネルは、Oracle データベースの Enterprise Server への登録に使用されません。代わりに、AppScan Source に組み込まれているユーティリティーを使用してインストール後にデータベース接続を構成できます。これに関する説明は、「*IBM Security AppScan Source* インストールと管理のガイド」の 86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』のトピックに記載されています。このユーティリティーを使用すると、インストール・パネルを使用する代わりに solidDB 接続を構成することもできます。

14. 「インストール完了」パネルでは、「**IBM Security AppScan Source License Manager** の起動」を選択することにより、インストール・ウィザードの終了後にただちに製品のアクティベーションを開始することができます。「完了」をクリックして標準インストールを完了し、インストール・ウィザードを終了します。
15. License Manager ユーティリティーで、以下のようになります。
  - a. ライセンス・ファイルを適用するには、「インポート」をクリックしてからダウンロード済みの AppScan Source ライセンスを参照します。
  - b. フローティング・ライセンスを適用するには、「ライセンス・サーバーの構成」をクリックしてから「追加」をクリックします。フローティング・ライセンスを格納しているホスト・マシンに関する情報を入力します。

追加のアクティベーション手順については、123 ページの『第 8 章 ソフトウェアのアクティブ化』を参照してください。

## 既存の Oracle データベースへのインストール

このタスク・トピックでは、AppScan Source データベースのスキーマとデータを、既存の Oracle データベースにインストールする手順について説明します。Oracle スキーマを作成するには、AppScan Source インストーラーを、Oracle データベースがインストールされているマシンか、Oracle フルクライアントがインストールされているマシンで実行する必要があります (インストーラーが Oracle の sqlplus および sqlldr の各ユーティリティーにアクセスできる必要があります)。

### このタスクについて

注: AppScan Source サーバー・コンポーネント (AppScan Source データベースなど) は、macOS でサポートされていません。

### 手順

1. AppScan Enterprise Server に付属しているインストールの説明に従って AppScan Enterprise Server をインストールします。サーバーについて詳しくは、72 ページの『AppScan Enterprise Server の概要』を参照してください。
2. IBM Security AppScan Source 製品の zip ファイルを見つけます (AppScan Source メディア・パックにあるか、または IBM パスポート・アドバンテージで AppScan Source eAssembly の一部としてダウンロードした電子イメージにあります)。
3. イメージをローカル・ドライブに解凍します。そのディレクトリーは、以下の通りです。
  - Microsoft Windows: AppScanSrc\_Installer.exe を実行します
  - Linux: 32 ビット・システム上で setup.bin を実行します。64 ビット・システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180>を参照してください。
  - macOS: setup.dmg を開き、setup.command スクリプトを実行します。

インストール・ウィザードの起動に関する詳細は、「IBM Security AppScan Source インストールと管理のガイド」の 69 ページの『インストール・ウィザードの開始』のトピックに記載されています。

4. 「コンポーネントの選択」インストール・パネルでは、「サーバー・コンポーネントの選択」を選択してから、AppScanSource データベース が選択されていることを確認します。「次へ」をクリックして、次のインストール・パネルに進みます。
5. 「サーバー接続」パネルで、以下のいずれかのオプションを選択します。
  - 「AppScan Server インスタンスに接続する」: このオプションを選択すると、リモートの AppScan Enterprise Server をテストして、AppScan Source への接続に使用できることを確認できます。サーバー接続をテストするには、以下のフィールドにデータを入力します。
    - AppScan Enterprise Server: 既存の URL 形式で、ご使用のリモート AppScan Enterprise Server インスタンスのホスト名を指定します。
    - 製品管理者: AppScan Enterprise Server 管理者ユーザー ID を指定します。

- パスワード: AppScan Enterprise Server 管理者ユーザー ID のパスワードを指定します。

サーバー設定を入力したら、「接続のテスト」をクリックして、AppScan Source との接続にそのサーバーを使用できることを確認します。

- 「サーバーを指定せずに続行する」: サーバーを指定しないで先に進む場合には、このオプションを選択します。

**重要:**

- 接続先の Enterprise Server で NIST 800-131a 準拠が有効になっている場合は、サーバーへの接続をテストできません。この場合には、サーバーを指定せずに進んでください。AppScan Source および Enterprise Server のインストール完了後に、86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』の説明に従ってください。その際に必ず「**TLSv1.2** を強制」オプションを適用してください。
- AppScan Enterprise Server が Common Access Card (CAC) 認証を使用して設定されている場合、「サーバーを指定せずに続行する」を選択し、すべてのサーバー接続の設定とテストに `appscanserverdbmgr_cac` ユーティリティを使用します。

「次へ」をクリックして、次のインストール・パネルに進みます。

6. 「インストール・ターゲットの指定」ページで、インストール・ディレクトリを指定します。オペレーティング・システムごとのデフォルトのディレクトリは、次のとおりです。
  - 32 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files\IBM\AppScanSource
  - 64 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource
  - Linux: root ユーザーの場合は、インストール・ウィザードによって `/opt/ibm/appscansource` にソフトウェアがインストールされます。root ユーザーではない場合は、デフォルトでは `<home_directory>/AppScan_Source` にインストールされる AppScan Source for Development Eclipse プラグインをインストールできます。
  - macOS: `/Applications/AppScanSource.app`

**重要:**

- インストール・ディレクトリ名には、英文字のみを含めることができます。非英文字を含む名前があるフォルダーは許可されません。
- Windows にインストールする場合、AppScan Source コンポーネントをインストールするには管理者特権が付与されている必要があります。
- Linux にインストールする場合、AppScan Source サーバー・コンポーネントをインストールするには、root 特権が必要です。

「次へ」をクリックして、次のインストール・パネルに進みます。

7. 「サーバー・コンポーネントの選択」ページで IBM Security AppScan Source データベース・コンポーネントをインストール対象として選択した場合は、「データベース選択」パネルが表示されます。このページで、「既存の

**Oracle 11g/12c Server** にデータベースをインストール」ラジオ・ボタンを選択し、「次へ」をクリックして次のインストール・パネルに進みます。

8. 「サーバー・コンポーネントの選択」ページで **IBM Security AppScan Source** データベース・コンポーネントをインストール対象として選択し、「データベース選択」ページで「既存の **Oracle 11g/12c Server** へのデータベースのインストール」を選択した場合は、「Oracle Database サーバー」パネルが表示されます。このページでは、以下のことを指定します。

- 「**Oracle ホーム**」: Oracle がインストールされている場所を指定します。
- 「**Oracle TNS ロケーション**」: tnsnames.ora ファイルが存在する場所です。これは、デフォルトで <oracle\_home>%network%admin です (ここで、<oracle\_home> は Oracle がインストールされている場所です。
- 「**Oracle サービス名/SID**」: 接続文字列または TNS 別名を指定します (例えば、//<hostname>:<port>/<OracleServiceName> など)。TNS 別名を指定するには、AppScan Enterprise Server を構成する必要があります。詳しくは、86 ページの『Oracle TNS 別名の構成』を参照してください。
- 「**システム・ユーザー名**」: インストールの実行に使用する Oracle ユーザーを指定します。このユーザー名は、他のユーザーを作成する権限を持っている必要があります。デフォルト値は system です。
- 「**システム・パスワード**」: 「システム・ユーザー名」のユーザーのパスワードを指定します。
- 「**接続のテスト**」: このボタンをクリックして、指定されているデータベース設定および資格情報が正しいことを確認します。
- 「**AppScan ユーザー名**」: 作成する AppScan Source データベース ユーザーを指定します。デフォルト値は ounce です。
- 「**AppScan パスワード**」: 「AppScan ユーザー名」のユーザーのパスワードを指定します。デフォルト値は ounce です。
- 「**ダイレクト・データ・ロード**」チェック・ボックス: これを選択した場合は、初期の AppScan Source データが Oracle Direct Load によってロードされます。このチェック・ボックスはデフォルトで選択されています。
- 「**Sysdba ユーザー**」: 「ダイレクト・データ・ロード」チェック・ボックスが選択されている場合は、sysdba 特権を持つユーザーを指定します。デフォルト値は sysdba です。
- 「**Sysdba パスワード**」: 「Sysdba ユーザー」のパスワードを指定します。
- 「**SqlPlus のパス**」: ディスク上の sqlplus 実行可能ファイルのパスを指定します。これは、インストール中に sql スクリプトを実行する際に使用されます。デフォルト値は sqlplus です。sqlplus 実行可能ファイルがシステム・パス上にある場合は、絶対パスにする必要はありません。
- 「**Sqlldr のパス**」: ディスク上の sqlldr 実行可能ファイルのパスを指定します。これは、インストール中にデータをロードする際に使用されます。デフォルト値は sqlldr です。sqlldr 実行可能ファイルがシステム・パス上にある場合は、絶対パスにする必要はありません。

**重要:** これらの設定を使用してインストールを完了すると、新しいスキーマおよび AppScan Source データベース・ユーザーが、ご使用の Oracle データベ

ースに自動的にインストールされます。 AppScan Source データベース・ユーザーを手動で作成する必要はありません。

注:

- インストールの一環として、既存の Oracle データベースに AppScan Source データベース・スキーマとデータをインストールした場合は、その後、`<data_dir>%logs\core_exceptions.log` (`<data_dir>` は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。) を参照して、インストール・エラーが発生していないことを確認してください。
- AppScan Enterprise Server を Oracle データベースに接続している場合は、データベースの作成時に文字セットを UTF-8 (AL32UTF8 を含む) に設定する必要があります (通常、UTF-8 はデフォルトの文字セットではありません)。
- AppScan Source のインストールには Oracle Instant Client (OCI) ライブラリーが必要ですが、これらはインストールされません。詳しくは、84 ページの『Oracle Client (OCI) ライブラリーのインストール』を参照してください。
- 「Oracle 接続文字列」として TNS 別名を指定した場合は、`core_exceptions.log` ファイルに以下のエラーが表示される可能性があります。Unable to process the database transaction. Error: ORA-12154 (このメッセージには、Oracle データベースからのエラー・テキストが付随する場合があります)。この問題を解決するには、以下のいずれかのタスクを実行します。
  - Oracle `tnsnames.ora` ファイルを `<install_dir>%bin` (`<install_dir>` は AppScan Source インストール済み環境がある場所です) にコピーします。
  - `<data_dir>%config%ounce.ozsettings` (`<data_dir>` は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。) を開きます。このファイルで、`tns_admin` 設定を見つけて、Oracle の `tnsnames.ora` ファイルが含まれたディレクトリーを指すように値を変更します。ファイルへの変更内容を保存します。

「次へ」をクリックして、次のインストール・パネルに進みます。

9. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つまり、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できません)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

10. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
11. 先に進む前に、インストール・オプションの概要を確認します。 選択内容を変更する場合は、「前へ」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。インストーラーによって、ハード・ディスクにファイルがコピーされます。

Linux サーバー・インストールの場合のみ: ファイルをコピーしたら、デーモン・ユーザーを特定する必要があります。 デフォルト・ユーザー「ounce」を作成する場合は「ユーザー 'ounce' を作成」を選択し、既存のユーザーで実行する場合は「既存のユーザーで実行」を選択します。(インストールでこのユーザーの存在が検証されます。選択されたユーザーには有効なシェルが必要となることに注意してください。)

インストール中に「キャンセル」をクリックすると、そのタイミングにかかわらず、すべてのコンポーネントがアンインストールされます。

12. 「IBM Security AppScan Enterprise Server の構成」パネルで、solidDB データベースが AppScan Enterprise Server に接続できるようにするための設定を指定します。デフォルトでは、このインストール・パネルに、データベースとサーバーが同じマシンにデフォルト設定でインストールされていると想定した値が事前に入力されています。 AppScan Enterprise Server で AppScan Source データベース を構成するには、「**AppScan Enterprise Server** を今すぐ構成」チェック・ボックスを選択して、以下の設定を行います。

- **AppScan Enterprise Server:** ご使用の AppScan Enterprise Server インスタンスの URL を指定します。
- **ユーザー ID:** AppScan Enterprise Server 管理者ユーザー ID を指定します。サーバーが Windows 認証用に構成されている場合は、サーバーにアカウントを追加したときに使用した Windows のユーザー ID を入力してください (ユーザー ID にはフォーマット <host name>\*<user id> を使用する必要があります)。
- **パスワード:** AppScan Enterprise Server ユーザー ID のパスワードを指定します。
- **データベース・ホスト名:** AppScan Source データベース をインストールしたマシンのホスト名を指定します。

注: このフィールドの入力内容は必ず、インストーラーを実行しているマシンの完全修飾ホスト名にしてください。 この値は、インストール時にこのフィールドに事前に入力されます。事前に入力された値が誤っている場合に限って変更してください。

「次へ」をクリックして、次のインストール・パネルに進みます。

注: Oracle データベースを使用する予定の場合は、「**AppScan Enterprise Server** を今すぐ構成」が選択されていないことを確認し、「次へ」をクリックします。このインストール・パネルは、Oracle データベースの Enterprise Server への登録に使用されません。代わりに、AppScan Source に組み込まれているユーティリティーを使用してインストール後にデータベース接続を構成できます。これに関する説明は、「*IBM Security AppScan Source* インストールと管理のガイド」の 86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』のトピックに記載されています。このユーティリティーを使用すると、インストール・パネルを使用する代わりに solidDB 接続を構成することもできます。

13. 「インストール完了」パネルでは、「**IBM Security AppScan Source License Manager** の起動」を選択することにより、インストール・ウィザードの終了後にただちに製品のアクティベーションを開始することができます。「完了」をクリックして標準インストールを完了し、インストール・ウィザードを終了します。
14. License Manager ユーティリティーで、以下のようにします。
  - a. ライセンス・ファイルを適用するには、「インポート」をクリックしてからダウンロード済みの AppScan Source ライセンスを参照します。
  - b. フローティング・ライセンスを適用するには、「ライセンス・サーバーの構成」をクリックしてから「追加」をクリックします。フローティング・ライセンスを格納しているホスト・マシンに関する情報を入力します。追加のアクティベーション手順については、123 ページの『第 8 章 ソフトウェアのアクティブ化』を参照してください。

## Oracle Client (OCI) ライブラリーのインストール

AppScan Source のインストールでは、Oracle Client (OCI) ライブラリーはインストールされません。Oracle データベースを使用して AppScan Source をデプロイする場合は、データベースと通信するために、AppScan Source 製品を実行するすべてのクライアント・マシンに Oracle クライアントがインストールされている必要があります。インストール済みの Oracle クライアントを使用するには、このトピックの説明に従って、AppScan Source がクライアント・ライブラリーを検出できるようにすることが必要です。インストールが完了した後、

<data\_dir>%logs%scanner\_exceptions.log (Windows の場合) または  
<data\_dir>/logs/scanner\_exceptions.log (Linux の場合) (<data\_dir> は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。) に接続エラーが示される場合、Oracle Client ライブラリーが見つからないことが原因である可能性があります。Linux の場合は、libcIntsh.so が見つからなかったことがこのエラーで示されます。Windows の場合は、ociw32.dll が見つからなかったことが示されます。

注: AppScan Source サーバー・コンポーネント (AppScan Source データベースなど) は、macOS でサポートされていません。

Oracle クライアントがまだインストールされていない場合は、<http://www.oracle.com/> の『Downloads』セクションから Oracle Client をダウンロードできます。

Oracle スキーマを作成するには、AppScan Source インストーラーを、Oracle データベースがインストールされているマシンか、Oracle フルクライアントがインストールされているマシンのいずれかで実行する必要があります。これは、インストーラーが Oracle sqlplus ユーティリティーおよび sqlldr ユーティリティーにアクセスできるようにするために必要です。

## Linux の場合

シンボリック・リンクがシステム上に存在しない場合は、`$Oracle_Home/lib` ディレクトリー内に作成する必要があります。このリンクは `libclntsh.so` という名前にし、このファイルの特定のバージョンを指す必要があります。例:

- Oracle バージョン 12 クライアント: `lrwxrwxrwx 1 oracle oracle 69 Apr 5 15:07 libclntsh.so -> /home/oracle/app/oracle/product/12.1.0/client/lib/libclntsh.so.12.1`
- Oracle バージョン 11 クライアント: `lrwxrwxrwx 1 oracle oracle 63 Oct 2 14:16 libclntsh.so -> /u01/app/oracle/home/lib/libclntsh.so.11.1`

また、`libclntsh.so` を含むディレクトリーが、インストーラーの実行前に `$LD_LIBRARY_PATH` に含まれていなければなりません。

`NLS_LANG` および `ORA_NLS10` (または `ORA_NLS11`) 環境変数の値も設定することが必要な場合があります。例:

```
export NLS_LANG=AMERICAN_AMERICA.AL32UTF8
export ORA_NLS10=$ORACLE_HOME/nls/data
```

これらの変数については、Oracle の資料を参照してください。

**Automation Server:** AppScan Source for Automation Server を使用している場合は、`/etc/init.d/ounceautod` 開始スクリプトを編集して、`ounceautod` デーモンのユーザー・アカウントの `$LD_LIBRARY_PATH` 内に Oracle Client ライブラリーが確実に含まれるようにすることが必要な場合があります。

## Windows の場合

`%ORACLE_HOME%/bin` ディレクトリーが `PATH` 環境変数に含まれていなければなりません。

## Oracle Instant Client

Oracle Instant Client がサポートされるのは、AppScan Source スキーマが適用されている既存の Oracle データベースに接続している場合のみです。

- **Linux** の場合: `libclntsh.so` シンボリック・リンクを Oracle Instant Client ライブラリーと同じディレクトリーに作成する必要があります、そのディレクトリーが `$LD_LIBRARY_PATH` に含まれていなければなりません。

注: Oracle Instant Client の Basic Lite バージョンを使用する場合は、`ORA_NLS10` (または `ORA_NLS11`) 変数を設定してはなりません。

- **Windows** の場合: Oracle Instant Client の `.dll` ファイルが `PATH` にあることを確認してください。

## Oracle TNS 別名の構成

AppScan Source のインストール中に Oracle データベースへの接続を構成するときは、Oracle 接続文字列の代わりに TNS 別名を使用できます。そのためには、このトピックの説明に従って AppScan Enterprise Server を構成する必要があります。

### このタスクについて

詳しくは、「AppScan Enterprise Serverと連携するための AppScan Source Oracle データベースの構成」トピック (<http://www.ibm.com/support/knowledgecenter/SSW2NF/welcome>) を参照してください。

注: AppScan Source サーバー・コンポーネント (AppScan Source データベースなど) は、macOS でサポートされていません。

## AppScan Enterprise Server への AppScan Source データベースの登録

有効な設定値が入力されていれば、AppScan Source のインストール中に AppScan Source データベースが自動的にサーバーに登録されます。しかし、データベースの登録が完了しない場合や失敗する場合は、このトピックの説明に従って登録を完了してください。

注: AppScan Source サーバー・コンポーネント (AppScan Source データベースなど) は、macOS でサポートされていません。

AppScan Source には、データベースをサーバーに登録できるユーティリティーが組み込まれています。このツールは、`<install_dir>%bin%appscanserverdbmgr.bat` (`<install_dir>` は AppScan Source インストール済み環境がある場所です) または `<install_dir>/bin/appscanserverdbmgr.sh` (Linux の場合) です。データベース/サーバー接続に問題がある場合は、(サーバーおよびクライアントのコンポーネントをインストールした後に) コマンド・プロンプトで以下のパラメーターを指定してこのツールを実行できます。

表 2. `appscanserverdbmgr.bat` パラメーター

パラメーター	説明	IBM Security AppScan Enterprise Server データベース構成グラフィカル・ユーザー・インターフェースでの同等の指定
なし	以下に示されているような AppScan Enterprise Server および AppScan Source データベースの構成情報の入力および検証を行えるグラフィカル・ユーザー・インターフェースを起動します。	

表 2. appscanserverdbmgr.bat パラメーター (続き)

パラメーター	説明	IBM Security AppScan Enterprise Server データベース構成グラフィカル・ユーザー・インターフェースでの同等の指定
-s	AppScan Enterprise Server インスタンスの URL。例えば、https://localhost:9443/ase/ などです。	サーバー URL
-u	AppScan Enterprise Server および AppScan Source データベース 管理者ユーザー ID。	製品管理者
-p	AppScan Enterprise Server and AppScan Source データベース 管理者ユーザー ID のパスワード。	Password
-forceTLSv12	AppScan Enterprise Server で NIST 800-131a 準拠が有効になっている場合のみ、この設定を true に指定します (そうしないと、サーバー接続が失敗します)。AppScan Enterprise Server で NIST 800-131a 準拠が有効になっていない場合は、この設定を false に指定します。	TLSv1.2 を強制
-dbClient	ご使用の AppScan Source データベースが solidDB である場合には、1 を指定します。Oracle である場合は 2 を指定します。	IBM SolidDB または Oracle
-dbConnString	データベース接続文字列 ("Driver={IBM solidDB 7.0 32-bit - (ANSI)}" など)。Oracle データベースを実行する場合、86 ページの『Oracle TNS 別名の構成』に従ってサーバーを構成してあれば、TNS 別名を指定できます。	接続文字列

表 2. appscanserverdbmgr.bat パラメーター (続き)

パラメーター	説明	IBM Security AppScan Enterprise Server データベース構成グラフィカル・ユーザー・インターフェースでの同等の指定
-dbConnInfo	データベース接続情報 ("tcp myhostname.mydomain.com 2315" など)。 注: 完全修飾ホスト名ではなく localhost を指定すると、データベースに接続できるのはローカル・マシンのユーザーのみになります。	接続情報
-dbUserid	データベース・ユーザー・アカウントのユーザー ID。	データベース・ユーザー ID
-dbPassword	データベース・ユーザー・アカウントのユーザー ID のパスワード。	Password

グラフィカル・ユーザー・インターフェースを使用している場合は、AppScan Enterprise Server セクション内のすべての項目を入力した後、「接続の検証」をクリックします。項目を検証したら、AppScan Source データベース・セクション内の項目に入力して、「接続の検証」をクリックします。データベース項目を検証したら、「変更を適用」をクリックしてデータベースをサーバーに登録します。

## AppScan Source データベース を、Common Access Card (CAC) 認証が有効になっている AppScan Enterprise Server に登録

AppScan Enterprise Server が Common Access Card (CAC) 認証に対して有効になっている場合、このヘルプ・トピックに記載されているユーティリティですべてのサーバー設定を完了します。

注: CAC 認証が有効になっている AppScan Enterprise Server への AppScan Source データベース の登録は Windows でのみサポートされています。

AppScan Source には、CAC 認証が有効になっている AppScan Enterprise Server にデータベースを登録できる 2 つのユーティリティが含まれています。これらのユーティリティを使用できるようにするには、以下の手順を実行します。

1. <install\_dir>%appscanserverdbmgr\_cac directory (<install\_dir> は AppScan Source インストール済み環境がある場所です) を見つけます。
2. <install\_dir>%appscanserverdbmgr\_cac%bin のコンテンツを <install\_dir>%bin にコピーします。
3. <install\_dir>%appscanserverdbmgr\_cac%lib のコンテンツを <install\_dir>%lib にコピーします。
4. コマンド・プロンプトで、ディレクトリーを <install\_dir>%bin に変更し、以下のユーティリティのいずれかを起動します。

- SHA-2 クライアント証明書を使用しており、Federal Information Processing Standard (FIPS) モードを実施したい場合、`appscanserverdbmgr_cac_fips.bat` を `-client_cert_auth` 引数を指定して起動します。例えば、ディレクトリーを `C:%Program Files (x86)%IBM%AppScanSource%bin` に変更し、コマンド `appscanserverdbmgr_cac_fips.bat -client_cert_auth` を発行します。
- その他のすべてのシナリオでは、`-client_cert_auth` 引数を指定して `appscanserverdbmgr_cac.bat` を起動します。例えば、ディレクトリーを `C:%Program Files (x86)%IBM%AppScanSource%bin` に変更し、コマンド `appscanserverdbmgr_cac.bat -client_cert_auth` を発行します。

ツールは、追加のパラメーターで起動できます。

表 3. `appscanserverdbmgr.bat` パラメーター

パラメーター	説明	IBM Security AppScan Enterprise Server データベース構成グラフィカル・ユーザー・インターフェースでの同等の指定
なし	以下に示されているような AppScan Enterprise Server および AppScan Source データベースの構成情報の入力および検証を行えるグラフィカル・ユーザー・インターフェースを起動します。	
<code>-s</code>	AppScan Enterprise Server インスタンスの URL。例えば、 <code>https://localhost:9443/ase/</code> などです。	サーバー URL
<code>-u</code>	リストから管理者の CAC 共通名を選択します。	製品管理者
<code>-forceTLSv12</code>	AppScan Enterprise Server で NIST 800-131a 準拠が有効になっている場合にのみ、この設定を <code>true</code> に指定します (そうしないと、サーバー接続が失敗します)。AppScan Enterprise Server で NIST 800-131a 準拠が有効になっていない場合は、この設定を <code>false</code> に指定します。	TLSv1.2 を強制
<code>-dbClient</code>	ご使用の AppScan Source データベースが <code>solidDB</code> である場合には、1 を指定します。Oracle である場合は 2 を指定します。	IBM SolidDB または Oracle

表 3. appscanserverdbmgr.bat パラメーター (続き)

パラメーター	説明	IBM Security AppScan Enterprise Server データベース構成グラフィカル・ユーザー・インターフェースでの同等の指定
-dbConnString	データベース接続文字列 ("Driver={IBM solidDB 7.0 32-bit - (ANSI)}" など)。  Oracle データベースを実行する場合、86 ページの『Oracle TNS 別名の構成』に従ってサーバーを構成してあれば、TNS 別名を指定できます。	接続文字列
-dbConnInfo	データベース接続情報 ("tcp myhostname.mydomain.com 2315" など)。 注: 完全修飾ホスト名ではなく localhost を指定すると、データベースに接続できるのはローカル・マシンのユーザーのみになります。	接続情報
-dbUserid	データベース・ユーザー・アカウントのユーザー ID。	データベース・ユーザー ID
-dbPassword	データベース・ユーザー・アカウントのユーザー ID のパスワード。	Password

グラフィカル・ユーザー・インターフェースを使用している場合は、AppScan Enterprise Server セクション内のすべての項目を入力した後、「接続の検証」をクリックします。項目を検証したら、AppScan Source データベース・セクション内の項目に入力して、「接続の検証」をクリックします。データベース項目を検証したら、「変更を適用」をクリックしてデータベースをサーバーに登録します。

AppScan Enterprise Server が CAC 認証に対して有効になっている場合、AppScan Enterprise Server セクションで「変更の適用」または「接続の検証」をクリックすると、「Windows セキュリティ」ダイアログ・ボックスに CAC カードの PIN を入力するようにプロンプトが出されます。

## AppScan Source データベースのバックアップ

定期的なバックアップ手順に従うことにより、AppScan Source データベースのデータが失われないように保護することをお勧めします。AppScan Source の新バージョンにアップグレードする前や、旧バージョンを削除する前に AppScan Source データベース をバックアップしてください。

注: AppScan Source サーバー・コンポーネント (AppScan Source データベースなど) は、macOS でサポートされていません。

Oracle データベースをバックアップする場合は、Oracle データベース管理者にお問い合わせください。

solidDB データベースを手動でバックアップおよびリストアする方法については、<http://www.ibm.com/support/docview.wss?rs=3457&uid=swg21590980>を参照してください。

## AppScan Source solidDB データベースのリストア

バックアップした solidDB データベースをリストアするには、このタスク・トピックの説明に従ってください。

### このタスクについて

注: AppScan Source サーバー・コンポーネント (AppScan Source データベースなど) は、macOS でサポートされていません。

### 手順

1. **IBM Security AppScan Source DB** サービスを停止します。
2. `<install_dir>%soliddb%logs` (Windows の場合) または `<install_dir>/soliddb/logs` (Linux の場合) (`<install_dir>` は AppScan Source インストール済み環境がある場所です) を見つけます。そのディレクトリー内のすべてのファイルを削除します。
3. データベース・バックアップを `<install_dir>%soliddb%appscansrc` (Windows の場合) または `<install_dir>/solidDB/appscansrc` (Linux の場合) にコピーします。
4. **IBM Security AppScan Source DB** サービスを始動します。

---

## macOS への AppScan Source のインストール

このトピックでは、macOS に `setup` アプリケーションをインストールする方法を説明します。

### 手順

1. インストール・ウィザードを開始します。
2. macOS にインストールするには、管理者パスワードが必要です。認証ダイアログでプロンプトが出された場合、管理者パスワードを入力してください。
3. インストール・パネルに表示される各国語を選択できる画面が表示されます。言語を選択し、「OK」をクリックして続行してください。
4. インストール・ウィザードを起動すると、「ようこそ - インストール・ウィザード」パネルが開き、現在開いているアプリケーションをすべて終了することを勧めるメッセージが表示されます。「次へ」をクリックして、インストール手順を開始します。
5. 「コンポーネントの選択」インストール・パネルで、インストールするコンポーネントを選択します。AppScan Source コンポーネントは、サーバー・コンポーネントとクライアント・コンポーネントに分けられます。
  - a. IBM Security AppScan Source for Automationをインストールするには、「サーバー・コンポーネントの選択」を選択し、次に AppScan Source for

Automationを選択します。IBM Security AppScan Source for Automation のインストールについては、101 ページの『AppScan Source for Automation のインストール』を参照してください。

- b. AppScan Source クライアント・コンポーネントをインストールするには、「クライアント・コンポーネントの選択」を選択し、インストールするコンポーネントを選択します。

- AppScan Source for Analysis
- AppScan Source コマンド行インターフェース
- AppScan Source for Development for Eclipse、RAD、MobileFirst

デフォルトでは、「クライアント・コンポーネントの選択」を選択すると、その下に AppScan Source for Analysis と AppScan Source コマンド行インターフェース のみが選択されています。

インストールしたいコンポーネントを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

6. 「インストール・ターゲットの指定」ページで、インストール・ディレクトリーを指定します。macOS 上でのデフォルト・ディレクトリーは、/Applications/AppScanSource.app です。

重要:

- インストール・ディレクトリー名には、英文字のみを含めることができません。非英文字を含む名前があるフォルダーは許可されません。

「次へ」をクリックして、次のインストール・パネルに進みます。

7. AppScan Source for Automation コンポーネントをインストール対象として選択した場合は、「IBM Security AppScan Source for Automation の構成」パネルが表示されます。このページで、以下の手順を実行します。

AppScan Enterprise Server 認証方式がユーザー ID およびパスワードの場合、以下のようにします。

- **AppScan Enterprise Server**ホスト名: Automation Server の接続先の AppScan Enterprise Server のホスト名またはIP アドレス
- ユーザー名: Automation Server が要求を処理するために使用する AppScan Source ユーザーを入力します。
- パスワード: AppScan Source ユーザーのパスワードを入力します。
- パスワードの確認: パスワードを確認します。

「次へ」をクリックして、次のインストール・パネルに進みます。

AppScan Enterprise Server が Common Access Card (CAC) 認証に対して有効になっている場合、このページのすべてのフィールドをブランクのままにして、「次へ」をクリックして、次のインストール・パネルに進みます。

注: インストール時に IBM Security AppScan Source for Automation 構成パネルを完了しなかった場合、または AppScan Enterprise Server が Common Access Card (CAC) 認証に対して有効な場合は、インストール後に AppScan Source for Automation を構成して、コマンド・ラインでログイン資格情報を

指定して AppScan Source ユーザーとして実行する必要があります。詳しくは、*IBM Security AppScan Source Utilities* ユーザー・ガイド を参照してください。

8. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つまり、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できません)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

9. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
10. 先に進む前に、インストール・オプションの概要を確認します。選択内容を変更する場合は、「前へ」をクリックして、前のページに戻ります。インストールの選択内容に問題がなければ、「インストール」をクリックします。インストーラーによって、ハード・ディスクにファイルがコピーされます。

Linux サーバー・インストールの場合のみ: ファイルをコピーしたら、デーモン・ユーザーを特定する必要があります。デフォルト・ユーザー「ounce」を作成する場合は「ユーザー 'ounce' を作成」を選択し、既存のユーザーで実行する場合は「既存のユーザーで実行」を選択します。(インストールでこのユーザーの存在が検証されます。選択されたユーザーには有効なシェルが必要となることに注意してください。)

インストール中に「キャンセル」をクリックすると、そのタイミングにかかわらず、すべてのコンポーネントがアンインストールされます。

11. 「インストール完了」パネルでは、「**IBM Security AppScan Source License Manager** の起動」を選択することにより、インストール・ウィザードの終了後にただちに製品のアクティベーションを開始することができます。「完了」をクリックして標準インストールを完了し、インストール・ウィザードを終了します。
12. License Manager ユーティリティで、以下のようにします。
  - a. ライセンス・ファイルを適用するには、「インポート」をクリックしてからダウンロード済みの AppScan Source ライセンスを参照します。
  - b. フローティング・ライセンスを適用するには、「ライセンス・サーバーの構成」をクリックしてから「追加」をクリックします。フローティング・ライセンスを格納しているホスト・マシンに関する情報を入力します。

追加のアクティベーション手順については、123 ページの『第 8 章 ソフトウェアのアクティブ化』を参照してください。

## タスクの結果

AppScan Source for Automation をインストールしたにも関わらず、「構成」インストール・パネルに指定したユーザー・アカウントが存在しない場合、(インストール後に) AppScan Enterprise Server、AppScan Source for Analysis、または AppScan Source コマンド行インターフェース (CLI) を使用して手動でユーザー・アカウントを作成する必要があります。AppScan Source for Automation の機能に完全にアクセスできるようにするには、このユーザー・アカウントに以下の許可が必要です。

- アプリケーションおよびプロジェクトの管理
  - 登録
  - スキャン
- 評価管理
  - 評価の保存
  - 評価の公開

**重要:** macOS へのインストール後、システム・ホスト名が解決できない場合は、AppScan Source が起動できないことがあります。この場合、以下の警告を含むメッセージが表示されます。

```
WARNING: "IOP00710208: (INTERNAL) Unable to determine local  
hostname from InetAddress.getLocalHost().getHostName()"
```

これは、AppScan Source がプロセス間通信に依存しているために発生します。プロセス間通信では、localhost とご使用のシステム・ホスト名を IP アドレスに解決することが必要です。

この問題を解決するには、nslookup 端末コマンドを使用して、localhost とご使用のシステム・ホスト名を解決できることを確認してください。解決できない場合、解決できるようにするもう 1 つの方法として、/etc/hosts ファイルを変更してその localhost とホスト名を組み込む方法があります。/etc/hosts ファイルでは、以下のような操作を行います。

- ホスト名の 127.0.0.1 へのマッピングを含める
- localhost の 127.0.0.1 へのマッピングを含める

---

## AppScan Source for Development のインストール

AppScan Source for Development プラグインは、標準の AppScan Source インストール・ウィザードによりご使用のコンピューターにインストールされます。

AppScan Source 製品を新しい製品バージョンにアップグレードし、アップグレードを AppScan Source for Development Eclipse プラグインに適用する場合は、ご使用の Eclipse または Eclipse ベースの製品からプラグインを最初にアンインストールする必要があります。AppScan Source をアップグレードした後で、更新されたプラグインを Eclipse またはサポートされる Eclipse ベースの製品にインストールし直すことができます。このことについての説明は、

99 ページの『以前にインストールしたバージョンの AppScan Source for Development Eclipse プラグイン の新しい製品バージョンへのアップグレード』に記載されています。

AppScan Source 製品をフィックスパック・アップグレードの一部としてアップグレードする場合は、アップグレードの前にプラグインをアンインストールする必要はありません。フィックスパックのインストール (およびアップグレードされた AppScan Source for Development プラグインの適用) についての説明は、104 ページの『フィックスパック・インストール』に記載されています。

## AppScan Source for Development (Eclipse、IBM MobileFirst Platform、および Rational Application Developer for WebSphere Software (RAD) のプラグイン)

Eclipse、Rational Application Developer for WebSphere Software (RAD)、または IBM MobileFirst Platform 用の AppScan Source for Development プラグインをインストールする場合は、これらのプラグインをコンピューターにインストールした後、ご使用のワークベンチに適用する必要があります。

AppScan Source for Development Eclipse プラグインを適用するかどうかは、一部の Eclipse ツール (Graphical Editing Framework (GEF) および Draw2d) を適用するかどうかによって決まります。AppScan Source for Development にサポートされている Eclipse のほとんどのバージョンには、これらの機能が含まれています。含まれていない場合は、AppScan Source for Development のインストール前に、適切な eclipse.org の更新サイトを使用して、これらのコンポーネントを Eclipse 環境にインストールしてください。インストールされていないと、AppScan Source for Development プラグインの Eclipse への適用中にエラーが発生する場合があります。

AppScan Source 製品を新しい製品バージョンにアップグレードし、アップグレードを AppScan Source for Development Eclipse プラグインに適用する場合は、ご使用の Eclipse または Eclipse ベースの製品からプラグインを最初にアンインストールする必要があります。AppScan Source をアップグレードした後で、更新されたプラグインを Eclipse またはサポートされる Eclipse ベースの製品にインストールし直すことができます。このことについての説明は、99 ページの『以前にインストールしたバージョンの AppScan Source for Development Eclipse プラグインの新しい製品バージョンへのアップグレード』に記載されています。

AppScan Source 製品をフィックスパック・アップグレードの一部としてアップグレードする場合は、アップグレードの前にプラグインをアンインストールする必要はありません。フィックスパックのインストール (およびアップグレードされた AppScan Source for Development プラグインの適用) についての説明は、104 ページの『フィックスパック・インストール』に記載されています。

注:

AppScan Source for Development (Eclipse プラグイン) で何らかのアクション (例えば、スキヤンの起動や、ログインが必要なアクションの開始など) を実行しようとする、このエラー・メッセージ (またはこれに似たエラー・メッセージ) が出される場合があります。

```
Unable to link native library shared-win32-x64.dll.  
You may need to install an appropriate Microsoft Visual C++  
2010 Redistributable Package for your system.
```

64 ビット Java ランタイム環境で稼働する場合、これは通常、64 ビット Microsoft Visual C++ ランタイム・ライブラリーが使用不可であることを示します。この問題を解決するには、Microsoft Visual C++ 2010 再頒布可能パッケージ (<http://www.microsoft.com/en-ca/download/details.aspx?id=14632> で入手可能) をインストールします。

## Eclipse および Rational Application Developer for WebSphere Software (RAD) 用プラグインのインストール

### このタスクについて

AppScan Source クライアントのインストールには、Eclipse および Rational Application Developer for WebSphere Software (RAD) コンポーネント用の AppScan Source for Development プラグインも含まれます。このインストールでは、Eclipse の更新と、開発環境へのプラグインの追加も必要となります。

### 手順

1. インストール・ウィザードを開始します。
2. インストール・パネルに表示される各国語を選択できる画面が表示されます。言語を選択し、「OK」をクリックして続行してください。
3. インストール・ウィザードを起動すると、「ようこそ - インストール・ウィザード」パネルが開き、現在開いているアプリケーションをすべて終了することを勧めるメッセージが表示されます。「次へ」をクリックして、インストール手順を開始します。
4. クライアント・コンポーネントのリストから「**AppScan Source for Development for Eclipse, RAD, MobileFirst**」を選択します。

「次へ」をクリックして、次のインストール・パネルに進みます。

**重要:** AppScan Source for Development プラグインをインストールした後、Eclipse または Application Developer IDE から機能を更新する必要があります。

5. 「インストール・ターゲットの指定」ページで、インストール・ディレクトリーを指定します。オペレーティング・システムごとのデフォルトのディレクトリーは、次のとおりです。

- 32 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files\IBM\AppScanSource
- 64 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource
- Linux: root ユーザーの場合は、インストール・ウィザードによって /opt/ibm/appscansource にソフトウェアがインストールされます。root ユーザーではない場合は、デフォルトでは <home\_directory>/AppScan\_Source にインストールされる AppScan Source for Development Eclipse プラグインをインストールできます。
- macOS: /Applications/AppScanSource.app

**重要:**

- インストール・ディレクトリー名には、英文字のみを含めることができます。非英文字を含む名前があるフォルダーは許可されません。
- Windows にインストールする場合、AppScan Source コンポーネントをインストールするには管理者特権が付与されている必要があります。
- Linux にインストールする場合、AppScan Source サーバー・コンポーネントをインストールするには、root 特権が必要です。

「次へ」をクリックして、次のインストール・パネルに進みます。

6. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つまり、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できます)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

7. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
8. ファイルをコピーする前に、インストール・オプションの概要を確認します。「インストール」をクリックします。インストーラーによって、ハード・ディスクにファイルがコピーされます。

## AppScan Source for Development (Eclipse プラグイン) を Eclipse およびサポートされている Eclipse ベースの製品に適用

Eclipse および Eclipse ベースの製品には、新しいソフトウェアをインストールする機能が組み込まれています。この機能を使用すると、インストールを更新したり、インストールに追加するプラグインを参照したりすることができます。このトピックの手順は、Eclipse および Rational Application Developer for WebSphere Software (RAD) への AppScan Source for Development プラグインの適用方法を説明しています。

### 始める前に

AppScan Source でサポートされる Eclipse および Rational Application Developer for WebSphere Software (RAD) のバージョンについては、<http://www.ibm.com/support/docview.wss?uid=swg27027486> を参照してください。

### 手順

1. ワークベンチのメイン・メニュー・バーから、「ヘルプ」 > 「新規ソフトウェアのインストール」を選択します。

2. 「インストール (Install)」 ダイアログ・ボックスの「使用可能なソフトウェア」ページで、「追加」をクリックします。
3. 「サイトの追加」ダイアログ・ボックス (一部のバージョンの Eclipse では「リポジトリの追加」という名前) で、「名前」フィールドに更新サイトの名前を指定します。
4. 以下の指示に従ってサイトを追加してください。ご使用のオペレーティング・システムによって異なります。
  - a. **Windows** および **Linux** の場合: 「ローカル」をクリックします。「フォルダーの参照」ダイアログ・ボックスで、AppScan Source インストール・ディレクトリーにナビゲートします ( 69 ページの『デフォルトのインストール場所』 を参照してください)。「OK」をクリックして「サイトの追加」ダイアログ・ボックスに戻り、「OK」をクリックして更新サイトを追加します。
  - b. **macOS** の場合: 「ロケーション」フィールドで、file:/Applications/AppScanSource.app/ と入力し、「OK」をクリックして更新サイトを追加します。
5. 新しいサイトがリストに表示されます。 インストール・シナリオに応じて、次のようにこのページに入力します。
  - 完全製品インストールの後でプラグインを適用する: 「**IBM Security AppScan Source Security Analysis Feature**」ローカル・サイトの横のチェック・ボックスを選択します。

AppScan Source for Development Eclipse プラグイン を適用するかどうかは、一部の Eclipse ツール (Graphical Editing Framework (GEF) および Draw2d) を適用するかどうかによって決まります。 AppScan Source for Development にサポートされている Eclipse のほとんどのバージョンには、これらの機能が含まれています。含まれていない場合は、AppScan Source for Developmentのインストール前に、適切な eclipse.org の更新サイトを使用して、これらのコンポーネントを Eclipse 環境にインストールしてください。インストールされていないと、AppScan Source for Development プラグインの Eclipse への適用中にエラーが発生する場合があります。

- フィックスパック・インストールの後でプラグインを適用する:
  - 以前のバージョンのプラグインを既に適用している開発環境にプラグインを適用する場合は、「**IBM Security AppScan Source Security Analysis Feature**」ローカル・サイトの横のチェック・ボックスを選択します。
  - プラグインがまだ含まれていない開発環境にプラグインを適用する場合は、上記の『完全製品インストールの後でプラグインを適用する』の説明に従ってください。

注: 「**IBM Security AppScan Source Security Analysis Feature**」ローカル・サイトには、適用するフィックスパック・バージョンのクライアント・フィーチャーが含まれている必要があります。この機能がない場合、ローカル・サイトの更新または再作成が必要になることがあります。

「次へ」をクリックして、次のインストール・パネルに進みます。

6. 「インストールの詳細」ページで、インストールされる項目を確認して、「次へ」をクリックします。
7. 「ライセンスの確認」ページで、ライセンス契約に同意して「終了」をクリックします。
8. プロンプトが出されたら、Eclipse を再始動します。 インストールが完了すると、「セキュリティー分析」メニューが表示されます。初めて AppScan Source アクションを使用しようとするとき、AppScan Enterprise Server を使用するかどうかを尋ねるメッセージが開きます。サーバーを使用しない場合、フィルター、スキャン構成、およびカスタム・ルールなどの共有項目にアクセスできません。この設定は後から「全般設定」で変更できます。

## AppScan Source for Development の追加のインストール要件

AppScan Source for Development Eclipse プラグインには、追加の構成が必要です。

1. AppScan Source for Development Plug-in for Eclipse では、Java ランタイム環境 (JRE) バージョン 1.5 以上が必要です。 ご使用の環境が参照している JRE がこの要件を満たしていない場合は、Eclipse インストール・ディレクトリーにある eclipse.ini を編集して、この要件を満たす JRE を参照するようにしてください。 eclipse.ini ファイルへのこの変更については、<http://wiki.eclipse.org/Eclipse.ini> の『*Specifying the JVM*』セクションを参照してください。
2. Linux 上の AppScan Source for Development Plug-in for Eclipse (Eclipse または RAD) では、AppScan Source インストール・ディレクトリーを LD\_LIBRARY\_PATH に追加する必要があります。例えば、bash シェルを使用する場合は、~/.bashrc の初期設定に以下の行を追加します。

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/ibm/appscansource
```

## 以前にインストールしたバージョンの AppScan Source for Development Eclipse プラグイン の新しい製品バージョンへのアップグレード

AppScan Source for Development Eclipse プラグイン を製品の新規バージョンにアップグレードするには、コンピューターから現在のプラグインを削除するか無効にしてから、新規バージョンをインストールする必要があります。

### このタスクについて

このタスクでは、さまざまなレベルの Eclipse および Rational Application Developer for WebSphere Software (RAD) をアップグレードして、AppScan Source for Development Eclipse プラグイン を適用するプロセスについて説明します (完全製品インストール)。

**重要:** このトピックは、フィックスパックのアップグレードには適用されません。AppScan Source 製品をフィックスパック・アップグレードの一部としてアップグレードする場合は、アップグレードの前にプラグインをアンインストールする必要があります。フィックスパックのインストール (およびアップグレードされた AppScan Source for Development プラグインの適用) についての説明は、104 ページの『フィックスパック・インストール』に記載されています。

## Eclipse および Rational Application Developer for WebSphere Software (RAD) のアップグレード:

### 手順

1. 実行しているワークベンチに応じて、ワークベンチのメイン・メニュー・バーから「ヘルプ」 > 「<product name> について」を選択します (ここで <product name> は、アップグレードしている Eclipse ベースの製品名です)。
2. 「情報」ダイアログ・ボックスで、「インストールの詳細」をクリックします。
3. 「詳細」ダイアログ・ボックスで、以前にインストールしたバージョンの AppScan Source に対して追加したコンポーネントを複数選択します。
4. 「アンインストール」をクリックします。
5. アンインストール手順の完了時に、ワークベンチを再始動するように求めるプロンプトが出された場合は、再始動します。
6. 97 ページの『AppScan Source for Development (Eclipse プラグイン) を Eclipse およびサポートされている Eclipse ベースの製品に適用』のステップを実行して、新しい開発者用プラグインを適用します。

## AppScan Source for Development Plug-in for Visual Studio のインストール

### このタスクについて

**重要:** AppScan Source for Development Plug-in for Visual Studio をインストールする前に、Visual Studio 2010、Visual Studio 2012、または Visual Studio 2013 がコンピューターにインストールされている必要があります。AppScan Source for Development plug-in for Visual Studio は Windows でのみサポートされています。

AppScan Source のセットアップ・ウィザードによって、前に示したいずれかのバージョンの Visual Studio がインストール済みであることが検出された場合は、その Visual Studio バージョンに対応する AppScan Source for Development プラグインがインストール・オプションとして表示されます。

### 手順

1. Visual Studio が閉じられていることを確認してください。Visual Studio は、AppScan Source for Development のインストール中に稼働している場合、そのインストールが完了したら再始動する必要があります。
2. インストール・ウィザードを開始します。
3. クライアント・コンポーネントのリストから適切なバージョンのプラグインを選択します。
  - AppScan Source for Development for Visual Studio 2013
  - AppScan Source for Development for Visual Studio 2012
  - AppScan Source for Development for Visual Studio 2010

注:

- インストール・ウィザードを実行しているマシンにインストールされている Visual Studio のバージョンに対応するオプションのみ選択可能です。例えば、Visual Studio 2012 と Visual Studio 2013 はクライアント・マシン上にあるが、Visual Studio 2010 はない場合、インストール・ウィザードで選択できるのは、「AppScan Source for Development for Visual Studio 2012」および「AppScan Source for Development for Visual Studio 2013」をインストールするオプションのみです。
- インストール・ウィザードが検出した Visual Studio のバージョンが複数ある場合は、複数のバージョンに対してプラグインをインストールすることを選択できます。

「次へ」をクリックして、次のインストール・パネルに進みます。

4. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つまり、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できます)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

5. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
6. ファイルをコピーする前に、インストール・オプションの概要を確認します。「インストール」をクリックします。インストーラーによって、ハード・ディスクにファイルがコピーされます。

---

## AppScan Source for Automation のインストール

### このタスクについて

AppScan Source for Automation は、インストール・パッケージに含まれるオプション・コンポーネントです。

重要: AppScan Source for Automation をインストールするには、root/管理者特権が必要です。

### 手順

1. インストール・ウィザードを開始します。
2. 「サーバー・コンポーネントの選択」を選択し、インストールするコンポーネントとして「AppScan Source for Automation」を選択します。

「次へ」をクリックして、次のインストール・パネルに進みます。

3. インストール・ディレクトリーを指定します。
  - 32 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files\IBM\AppScanSource
  - 64 ビット・バージョンの Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource
  - Linux: root ユーザーの場合は、インストール・ウィザードによって /opt/ibm/appscansource にソフトウェアがインストールされます。 root ユーザーではない場合は、デフォルトでは <home\_directory>/AppScan\_Source にインストールされる AppScan Source for Development Eclipse プラグインをインストールできます。
  - macOS: /Applications/AppScanSource.app

「次へ」をクリックして、次のインストール・パネルに進みます。

4. 「IBM Security AppScan Source for Automation の構成」パネルで、以下のよう指定します。

AppScan Enterprise Server 認証方式がユーザー ID およびパスワードの場合、以下のようになります。

- **AppScan Enterprise Server**ホスト名: Automation Server の接続先の AppScan Enterprise Server のホスト名またはIP アドレス
- ユーザー名: Automation Server が要求を処理するために使用する AppScan Source ユーザーを入力します。
- パスワード: AppScan Source ユーザーのパスワードを入力します。
- パスワードの確認: パスワードを確認します。

「次へ」をクリックして、次のインストール・パネルに進みます。

AppScan Enterprise Server が Common Access Card (CAC) 認証に対して有効になっている場合、このページのすべてのフィールドをブランクのままにして、「次へ」をクリックして、次のインストール・パネルに進みます。

注: インストール時に IBM Security AppScan Source for Automation 構成パネルを完了しなかった場合、または AppScan Enterprise Server が Common Access Card (CAC) 認証に対して有効な場合は、インストール後に AppScan Source for Automation を構成して、コマンド・ラインでログイン資格情報を指定して AppScan Source ユーザーとして実行する必要があります。詳しくは、*IBM Security AppScan Source Utilities ユーザー・ガイド* を参照してください。

5. 言語パックの選択パネルで、インストールする言語パックを選択します。言語パックをインストールすると、AppScan Source のユーザー・インターフェースは、オペレーティング・システムがそのロケールで動作している場合、その言語で表示されます。

デフォルトでは、「英語」が選択されています (これは選択解除できません)。インストール・ウィザードが英語以外の各国語で表示されている場合 (つま

り、インストール・ウィザードの「ようこそ」パネルで英語以外の言語を選択した場合)、このパネルでその言語も選択されます (しかし、選択解除できません)。

インストールする言語パックを選択したら、「次へ」をクリックして次のインストール・パネルに進みます。

注: 特定の言語パックをインストールしない場合、インストール後にその言語を追加することはできません。

6. ご使用条件の条項を確認して同意したら、「次へ」をクリックして続行します。
7. ファイルをコピーする前に、インストール・オプションの概要を確認します。
8. インストールを行うには、以下の設定が必要です。
  - **AppScan Enterprise Server:** AppScan Source for Automation の接続先の AppScan Enterprise Server のホスト名または IP アドレス。
  - **ユーザー名:** AppScan Source for Automation が要求を処理するために使用する AppScan Source ユーザー。
  - **パスワード:** 「ユーザー名」フィールドで指定したユーザーのパスワード。
  - **パスワードの確認:** パスワードを確認します。
9. 「次へ」をクリックしてファイルをインストールし、「完了」をクリックしてインストールを完了します。
10. **macOS:** 端末装置で、<install\_dir>/bin/ ディレクトリに移動します (<install\_dir> は AppScan Source インストール済み環境がある場所です)。./automationDaemonRestart.sh (sudo は使用しない) を発行して、このディレクトリ内にある automationDaemonRestart.sh スクリプトを実行します。
11. **Linux:** 次のコマンドを発行して、AppScan Source データ・ディレクトリーおよびそのコンテンツのアクセス権を変更します。

```
sudo chmod -R a+rwx /var/opt/ibm/appscansource
```

これにより、AppScan Source for Automation ユーザーがスキャンを実行できるようになります。

## タスクの結果

AppScan Source ユーザー・アカウントがまだ存在しない場合は、それを「AppScan Source for Automation の構成」インストール・パネルで指定し、(インストール後に) AppScan Enterprise Server、AppScan Source for Analysis、または AppScan Source コマンド行インターフェース (CLI)を使用して手動で作成する必要があります。AppScan Source for Automation の機能に完全にアクセスできるようにするには、このユーザー・アカウントに以下の許可が必要です。

- アプリケーションおよびプロジェクトの管理
  - 登録
  - スキャン
- 評価管理
  - 評価の保存
  - 評価の公開

## 構文

**Windows** の場合: `<install_dir>%bin%onceautod.exe -u <user name> -p <password> --persist`

**Linux** および **macOS** の場合: `<install_dir>/bin/onceautod -u <user name> -p <password> --persist`

ここで:

- `<install_dir>` は AppScan Source インストール済み環境がある場所です。
- `-u <user name>` は、要求の処理時に Automation Server が認証に使用する AppScan Source ユーザーです。必要な許可がこのユーザーに付与されている必要があります。
- `-p <password>` は、パスワードのユーザーです。ユーザー名を指定する場合は、パスワードも指定する必要があります。
- `--persist` は、ログイン資格情報をディスクに保存します。指定したユーザー名およびパスワードを使用した暗号化鍵ファイルを作成します。

ユーザー名とパスワードを指定したら、以下のようにして Automation Server を開始できます。

- Windows の場合、**IBM Security AppScan Source for Automation** サービスを開始します。
- Linux の場合、コマンド `/etc/init.d/onceautod start` を実行してデーモンを開始します。
- macOS の場合は、コマンド `launchctl start com.ibm.appscan.autod` を発行します。

---

## フィックスパック・インストール

AppScan Source フィックスパックは、デルタ・インストーラーによって提供されます。AppScan Source フィックスパックを適用するには、このヘルプ・トピックの説明に従ってください。

### このタスクについて

**重要:** フィックスパック・インストーラーを使用してカスタム・インストールを作成することはできません。

### 手順

1. フィックスパック・インストール実行可能ファイルをダウンロードし、起動します。
  - Microsoft Windows:
    - AppScanSrc\_Installer.exe を実行し、インストール・ウィザードを起動します。
    - サイレント・インストールを実行するには、コマンド・プロンプトで `AppScanSrc_Installer.exe -i silent -D$LICENSE_ACCEPTED$="true"` を発行します。ここで、

- `-i silent` パラメーターは、サイレント・インストールの実行を指示するために使用します。
- `-D$LICENSE_ACCEPTED$="true"` パラメーターは、製品ライセンスへの同意を指示します。
- Linux: コマンド・プロンプトから以下のいずれかを発行します。
  - インストール・ウィザードを起動する場合は、`setup.bin` コマンドを発行します。
  - サイレント・インストールを実行するには、`setup.bin -i silent -D$LICENSE_ACCEPTED$="true"` を発行します。ここで、
    - `-i silent` パラメーターは、サイレント・インストールの実行を指示するために使用します。
    - `-D$LICENSE_ACCEPTED$="true"` パラメーターは、製品ライセンスへの同意を指示します。インストールの実行に使用されるシェルによっては、`-D¥$LICENSE_ACCEPTED¥$="true"` を発行して、このパラメーターをエスケープしなければならない場合があります。
- macOS: `setup.dmg` を開き、`setup` アプリケーションを実行します。

注: フィックスパックのサイレント・インストールは、macOS ではサポートされていません。

インストール・ウィザードを使用してインストールする場合は、残りのステップを完了します。

2. インストール・ウィザードを初めて起動すると、インストール・パネルに表示される各国語を選択できる画面が表示されます。言語を選択し、「OK」をクリックして続行してください。
3. 表示されている推奨事項に注意しながら、「ようこそ - インストール済み環境のアップグレード・ウィザード」パネルを読みます。「次へ」をクリックして先に進みます。
4. 「設定の確認」パネルで、先に進む前にインストール情報の概要を確認してから、「インストール」をクリックしてフィックスパックを適用します。
5. AppScan Source データベース が含まれているインストール済み環境をアップグレードする場合、データベース更新のインストール・パネルが表示されます(フィックスパックにデータベース・アップグレードが含まれている場合)。このパネルに、データベース・ユーザー・アカウントの資格情報を入力し、「開始」をクリックします。データベースのアップグレードが完了したら、「次へ」をクリックします。

注:

- solidDB のアップグレード: データベースのアップグレード中に、既存のデータベースのバックアップが作成されます。データベースのアップグレードが失敗した場合、インストーラーがバックアップに戻すため、データベースのアップグレードを再始動できます(既存のデータベースに問題がありアップグレードできない場合には、その問題を解決してから、データベースのアップグレードを再始動できます)。
- Oracle のアップグレード: データベースのアップグレードが失敗した場合、インストーラーにより、データベースのアップグレードを再始動できます

(既存のデータベースに問題がありアップグレードできない場合には、その問題を解決してから、データベースのアップグレードを再始動できます)。

6. 「インストール完了」パネルでメッセージを確認し、「完了」をクリックします。インストールの完了後には、システムを再起動することをお勧めします。

## 次のタスク

Windows または Linux の場合、ご使用の開発環境に AppScan Source for Development Eclipse プラグインが含まれている場合は、フィックスパックのインストール後にこれらのプラグインをワークベンチに適用する必要があります。このことについての説明は、以下のトピックに記載されています。

- 97 ページの『AppScan Source for Development (Eclipse プラグイン) を Eclipse およびサポートされている Eclipse ベースの製品に適用』

---

## 第 6 章 AppScan Source インストールのカスタマイズ

カスタム・インストール・ウィザードを使用するために、インストールをカスタマイズしたり、あるいは製品をサイレント・インストールするためにカスタム・インストーラーを作成することができます。

注: フィックスパックの適用時は、カスタム・インストールを作成することはできません。このセクションは、フィックスパックのインストールには適用されません。フィックスパックのサイレント・インストールを実行する方法については、104 ページの『フィックスパック・インストール』を参照してください。

全社的な導入において、AppScan Source の管理者は、特定のユーザー・クラスに合わせてインストールをカスタマイズできます。カスタム・インストールの作成では、使用できるコンポーネントの制限や選択、およびインストール属性のデフォルト値の定義などを行います。

カスタム・インストール・ウィザードを使用すると、サイレント・インストールを含めて、カスタム・インストールを必要な数だけ作成できます。組織内のすべてのユーザーが AppScan Source 製品をインストールする方法を、管理および標準化できます。

大規模な組織全体に AppScan Source を導入する場合は、まずネットワーク・サーバー上にインストールした後で、この中央の管理ポイントからインストールを開始するようにユーザーに指示するのが最も効率的です。

---

### カスタム・インストールまたはサイレント・インストールの作成

AppScan Source には、グラフィカルなインストール構成ウィザードが組み込まれています。管理者はこれを使用して、サイレント (非対話式) インストールやカスタム・グラフィカル・インストールを作成できます。

管理者がインストーラーを実行してカスタム・インストールを作成すると、新しい構成プロパティ・ファイルが生成されます。このプロパティ・ファイルを、次に AppScan Source インストーラーで使用できます。

インストール構成ウィザードでは、既存の構成ファイルを変更したり、新しい構成ファイルを作成したりすることができます。ウィザードでは、以下の事項を定義することで、インストールをカスタマイズできます。

- 対話式インストールか、サイレント・インストールか
- インストールに使用可能なコンポーネント (対話式インストールでのみ選択可能)。
- デフォルトのコンポーネントの選択 (対話式インストールでのみ選択可能)。
- 必須、すなわち自動的にインストールされるコンポーネント。
- デフォルト・インストール・フォルダー。
- インストールするデフォルト言語パック。

- 使用するライセンス・ファイルまたはライセンス・サーバー。
- AppScan Source for Automation で使用するユーザー・アカウント (これがインストール用のコンポーネントまたは使用可能コンポーネントとして選択されている場合)

注: カスタムのサイレント・インストールを作成した場合、トルコ語の言語ロケールで実行すると失敗します (例: tr および tr\_TR)。

## インストール構成ウィザードを起動する

このトピックでは、インストール構成ウィザード (カスタム・インストール・ファイルやサイレント・インストール・ファイルの作成に使用されるウィザード) の起動方法について説明します。

### このタスクについて

管理者は環境変数 `OUNCE_CONFIG_FILE` を定義し、それをインストール構成設定を保持するプロパティ・ファイルにポイントして、構成ツールを開始します。このファイルは、カスタム・インストールやサイレント・インストールの実行に使用されます。

### 手順

- Windows システムの場合は、以下のコマンドを発行します。

```
set OUNCE_CONFIG_FILE=<path>
AppScanSrc_Installer.exe
```

ここで `<path>` は、インストール設定が含まれるプロパティ・ファイルの完全修飾パスとファイル名です。例えば、`set OUNCE_CONFIG_FILE=C:\%install.properties` を発行すると、インストール設定がそのファイルに保存されます。

`setup` ファイルを含むロケーションからコマンドを実行していない場合、そのロケーションにディレクトリーを変更するか、コマンドをファイルのロケーションで修飾するようにしてください。

あるいは、Windows システム・プロパティで環境変数を設定した後、`AppScanSrc_Installer.exe` ファイルをダブルクリックするか、コマンド・ラインから起動します。

- Linux システムの場合は、次のコマンドを発行します。

```
export OUNCE_CONFIG_FILE=<path>
```

ここで `<path>` は、インストール設定が含まれるプロパティ・ファイルの完全修飾パスとファイル名です。

その後、ウィザードを起動します。32 ビット・システムの場合は、`setup.bin` を実行します。64 ビット・システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180>を参照してください。

`setup` ファイルを含むロケーションからコマンドを実行していない場合、そのロケーションにディレクトリーを変更するか、コマンドをファイルのロケーションで修飾するようにしてください。

- macOS システムの場合は、以下のコマンドを発行します。

```
export OUNCE_CONFIG_FILE=<path>
./setup.bin
```

ここで <path> は、インストール設定が含まれるプロパティ・ファイルの完全修飾パスとファイル名です。

setup ファイルを含むロケーションからコマンドを実行していない場合、そのロケーションにディレクトリーを変更するか、コマンドをファイルのロケーションで修飾するようにしてください。

重要: インストール済み環境を構成する目的で ./setup.bin コマンドを発行する場合は、コマンドの先頭に sudo を指定しないでください。

## タスクの結果

ファイル名が存在しており、有効である場合、カスタム・ウィザードはそのファイル内のプロパティをデフォルト・プロパティとして使用します。既存のファイル名または新規のファイル名を使用して構成を保存できます。ファイル名が存在しない場合、ウィザードは AppScan Source のデフォルト・プロパティを使用します。構成の保存時には、指定されたファイル名がデフォルトとして表示されます。

## カスタム・インストール構成ウィザードの使用

カスタム・インストール・ウィザードが表示され、AppScan Source インストールに使用する構成ファイルをこれから作成することが示されます。

### このタスクについて

Windows システムでカスタム・インストール・ウィザードを実行する場合は、Linux デーモンのユーザー・ステップが表示されます。Windows インストールで最終版の構成ファイルが使用される場合は、この値が無視されます。

ヒント: 既存の構成ファイルを使用してウィザードを実行する場合は、このファイルから値が読み取られ、デフォルト値として使用されます。

### 手順

1. 「サイレント・インストール・オプション」パネルで、インストールをサイレント・インストールとして実行するかどうかを指定して、インストール・タイプを構成します。対話式カスタム・インストールを作成する場合は、「いいえ」を選択してください。

注: カスタムのサイレント・インストールを作成した場合、トルコ語の言語ロケールで実行すると失敗します (例: tr および tr\_TR)。

「次へ」をクリックして、次のインストール・パネルに進みます。

2. 対話式のカスタム・インストールのみ: 対話式のカスタム・インストーラーを作成する場合 (「サイレント・インストール・オプション」パネルで「いいえ」が選択されている場合)、以下の 3 つの「コンポーネントの選択」パネルの設定を完了する必要があります。
  - a. 最初のパネルでは、対話式のカスタム・インストールで使用可能な (または表示される) AppScan Source コンポーネントを選択します。

- AppScan Source for Automation
- AppScan Source for Analysis
- AppScan Source コマンド行インターフェース
- AppScan Source for Development for Visual Studio 2013
- AppScan Source for Development for Visual Studio 2012
- AppScan Source for Development for Visual Studio 2010
- AppScan Source for Development for Eclipse、RAD、MobileFirst

注: ターゲット・オペレーティング・システムが選択したコンポーネントをサポートしていない場合や、選択したコンポーネントがシステムに存在しないソフトウェアに依存する場合は、コンポーネントを選択してもインストールでは無視されます。例えば、サポートされるバージョンの Microsoft Visual Studio がインストールされていないシステムに、カスタム・インストーラーを使用してインストールする場合、インストール対象として AppScan Source for Development for Visual Studio 2012 を選択しても、カスタム・インストーラーのデプロイ時に無視されます。

残りの「コンポーネントの選択」パネルを使用すると、インストール・パネルに表示するコンポーネントをデフォルトで選択するかどうか、有効にするかどうか (有効ではないコンポーネントはインストーラーのデプロイ時にグレー表示されて選択できません) を指定することができます。例えば、コンポーネントのインストールを強制実施するカスタム・インストーラーを希望する場合があります。これを行うには、コンポーネントをデフォルトで選択状態にする一方で、有効にはしません。

コンポーネントを使用可能に設定したにも関わらず、デフォルトで選択状態にせず有効にしない場合は、そのコンポーネントはインストールされません (グレー表示されてインストール用に選択できません)。

「次へ」をクリックして、次のインストール・パネルに進みます。

- 次の「コンポーネントの選択」パネルには、対話式的カスタム・インストーラーで使用可能になるよう選択されたコンポーネントのみ表示されます。このパネルでは、使用可能なコンポーネントのうち、どのコンポーネントをデフォルトで選択状態にするかを指定します。「次へ」をクリックして、次のインストール・パネルに進みます。
  - カスタム・インストーラーでユーザーが選択または選択解除できるコンポーネントを指定します。コンポーネントを無効にすると、そのコンポーネントのインストールが必須になります (それがデフォルトで選択状態になるよう設定されている場合に限ります)。「次へ」をクリックして、次のインストール・パネルに進みます。
- サイレント・カスタム・インストーラーのみ: サイレント・カスタム・インストーラーを作成する場合 (「サイレント・インストール・オプション」パネルで「はい」が選択されている場合)、サイレント・インストーラーがインストールする AppScan Source コンポーネントを選択します。
    - AppScan Source for Automation
    - AppScan Source for Analysis
    - AppScan Source コマンド行インターフェース

- AppScan Source for Development for Visual Studio 2013
- AppScan Source for Development for Visual Studio 2012
- AppScan Source for Development for Visual Studio 2010
- AppScan Source for Development for Eclipse、RAD、MobileFirst

注: ターゲット・オペレーティング・システムが選択したコンポーネントをサポートしていない場合や、選択したコンポーネントがシステムに存在しないソフトウェアに依存する場合は、コンポーネントを選択してもインストールでは無視されます。例えば、サポートされるバージョンの Microsoft Visual Studio がインストールされていないシステムに、カスタム・インストーラーを使用してインストールする場合、インストール対象として AppScan Source for Development for Visual Studio 2012を選択しても、カスタム・インストーラーのデプロイ時に無視されます。

4. ターゲット・インストール・ディレクトリーを選択します。サイレント・インストールの場合は、これがインストール・ディレクトリーになります。対話式インストールの場合は、これがデフォルト値になります。

「次へ」をクリックして、次のインストール・パネルに進みます。

5. 「ライセンス・ファイルの指定」パネルで、ライセンス・ファイルの場所を指定するか、ライセンス・サーバーのホスト名とポートを指定します。「次へ」をクリックして、次のインストール・パネルに進みます。
6. 「プロパティ・ファイルの指定」パネルで、ターゲット・プロパティ・ファイルの名前と場所を指定します。ウィザードが既存の構成ファイルを使用する場合は、デフォルトのパス名が表示されます。ファイル名を変更して、新しい構成ファイルを作成できます。

Linux サーバーでのインストールのみ: AppScan Source デーモンを実行する Linux ユーザーを指定します。ファイルをコピーした後に、サービス・ユーザーを指定する必要があります。デフォルト・ユーザー「ounce」を作成する場合は「ユーザー 'ounce' の作成」を選択し、既存のユーザーで実行する場合は「既存のユーザーで実行」を選択します。(インストールではこのユーザーが検証されます。選択されたユーザーには有効なシェルが必要となることに注意してください。)

「次へ」をクリックして、プロパティ・ファイルを保存します。

---

## カスタム・インストールまたはサイレント・インストールの実行

このトピックでは、コマンド行からのカスタム・インストールやサイレント・インストールの実行方法をプラットフォーム別に説明します。

### 始める前に

カスタム・インストールを作成できるウィザードを起動する場合 ( 108 ページの『インストール構成ウィザードを起動する』を参照)、OUNCE\_CONFIG\_FILE 環境変数を作成します。カスタム・インストールを実行する前に、この環境変数が削除されていることを確認してください。

## 手順

- Windows システムの場合は、以下のコマンドを発行します。

```
AppScanSrc_Installer.exe -f <configuration_properties_file>
```

ここで、<configuration\_properties\_file> は、「カスタム・インストール構成」ウィザードの実行時に作成したプロパティ・ファイルの完全パスおよびファイル名です (例えば、c:\¥install.properties)。

- Linux システムの場合は、-f <configuration\_properties\_file> を使用してウィザードを起動します。ここで、<configuration\_properties\_file> は、「カスタム・インストール構成」ウィザードの実行時に作成したプロパティ・ファイルの完全パスおよびファイル名です (例えば、/usr/local/share/my\_configs/install.properties)。

32 ビット・システムの場合は、以下を発行します。

```
setup.bin -f <configuration_properties_file>
```

64 ビット Linux システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180> の説明に従ってウィザードを起動します。ただし、起動コマンドに -f <configuration\_properties\_file> を付加してください。

- macOS システムの場合は、以下のコマンドを発行します。

```
sudo ./setup.bin -f <configuration_properties_file>
```

ここで、<configuration\_properties\_file> は、「カスタム・インストール構成」ウィザードの実行時に作成したプロパティ・ファイルの完全パスおよびファイル名です (例えば、/Users/myname/install.properties)。

---

## 例：カスタム・インストールを介した **AppScan Source** のインストール

以下の例で、カスタム・インストール・ウィザードのデプロイ方法について説明します。

### このタスクについて

情報技術 (IT) 部門が、特定のユーザーを対象としてインストール・オプションを制限または管理したいと考えています。

カスタム・インストールを作成する前に、管理者はユーザーがアクセス権を持つファイル・サーバーに AppScan Source Software インストール・ファイルを配置します。また、IT 部門では、各ユーザー・タイプで必要とされる各種の AppScan Source 製品に基づいて、いくつかの異なるインストール構成を特定する作業も行います。

カスタム・インストールで AppScan Source をインストールするには、以下の手順を実行します。

## 手順

1. IT 部門が、AppScan Source インストール CD または FTP ダウンロードから、適切なコンテンツをファイル・サーバーにコピーします。

2. IT 部門が、カスタム・インストール・ウィザードを使用して、必要なインストール・タイプ (例えば AppScan Source for Development や AppScan Source for Analysis) ごとに、必要なインストール構成ファイルを作成します。
3. IT 部門が、共有パブリック・フォルダーに構成ファイルを格納します。
4. IT 部門が、対象となるユーザーに E メールを送信します。この E メールには、クリックすると対象ユーザーに適した AppScan Source インストールが開始されるハイパーリンクが含まれています。
5. ユーザーが E メールを受信し、該当する AppScan Source 製品のインストール場所へのリンクを確認します。
6. ユーザーが、E メール内のハイパーリンクからインストールを開始します。例えば、このハイパーリンクをクリックすると、IT 部門が用意した .bat ファイルまたはスクリプトが実行されて、`setup -f install.properties` が適切に呼び出されます。
7. AppScan Source のインストールが開始されて、IT 部門のカスタム・インストール構成で定義されているデフォルトの (ただし変更可能な) オプションが表示されます。(これには、「コンポーネントの選択」ウィザード・ページが含まれます。)

## タスクの結果

このインストールが完了すると、以下のようになります。

- 適切な AppScan Source 製品がデスクトップにインストールされます。
- デフォルトのホスト・サーバーが識別されます。
- ライセンス・ファイルがターゲット・コンピューターにコピーされます (オプション)。



---

## 第 7 章 AppScan Source サイレント・インストーラー

AppScan Source カスタム・インストール・ウィザードは、サイレント・インストーラーの作成に使用されます。

AppScan Source インストールのカスタマイズについては、107 ページの『第 6 章 AppScan Source インストールのカスタマイズ』を参照してください。

注: フィックスパックの適用時は、カスタム・インストールを作成することはできません。このセクションは、フィックスパックのインストールには適用されません。フィックスパックのサイレント・インストールを実行する方法については、104 ページの『フィックスパック・インストール』を参照してください。

---

### カスタム・インストールまたはサイレント・インストールの作成

AppScan Source には、グラフィカルなインストール構成ウィザードが組み込まれています。管理者はこれを使用して、サイレント (非対話式) インストールやカスタム・グラフィカル・インストールを作成できます。

管理者がインストーラーを実行してカスタム・インストールを作成すると、新しい構成プロパティ・ファイルが生成されます。このプロパティ・ファイルを、次に AppScan Source インストーラーで使用できます。

インストール構成ウィザードでは、既存の構成ファイルを変更したり、新しい構成ファイルを作成したりすることができます。ウィザードでは、以下の事項を定義することで、インストールをカスタマイズできます。

- 対話式インストールか、サイレント・インストールか
- インストールに使用可能なコンポーネント (対話式インストールでのみ選択可能)。
- デフォルトのコンポーネントの選択 (対話式インストールでのみ選択可能)。
- 必須、すなわち自動的にインストールされるコンポーネント。
- デフォルト・インストール・フォルダー。
- インストールするデフォルト言語パック。
- 使用するライセンス・ファイルまたはライセンス・サーバー。
- AppScan Source for Automation で使用するユーザー・アカウント (これがインストール用のコンポーネントまたは使用可能コンポーネントとして選択されている場合)

注: カスタムのサイレント・インストールを作成した場合、トルコ語の言語ロケールで実行すると失敗します (例: tr および tr\_TR)。

### インストール構成ウィザードを起動する

このトピックでは、インストール構成ウィザード (カスタム・インストール・ファイルやサイレント・インストール・ファイルの作成に使用されるウィザード) の起動方法について説明します。

## このタスクについて

管理者は環境変数 `OUNCE_CONFIG_FILE` を定義し、それをインストール構成設定を保持するプロパティ・ファイルにポイントして、構成ツールを開始します。このファイルは、カスタム・インストールやサイレント・インストールの実行に使用されます。

### 手順

- Windows システムの場合は、以下のコマンドを発行します。

```
set OUNCE_CONFIG_FILE=<path>
AppScanSrc_Installer.exe
```

ここで `<path>` は、インストール設定が含まれるプロパティ・ファイルの完全修飾パスとファイル名です。例えば、`set OUNCE_CONFIG_FILE=C:\%install.properties` を発行すると、インストール設定がそのファイルに保存されます。

`setup` ファイルを含むロケーションからコマンドを実行していない場合、そのロケーションにディレクトリを変更するか、コマンドをファイルのロケーションで修飾するようにしてください。

あるいは、Windows システム・プロパティで環境変数を設定した後、`AppScanSrc_Installer.exe` ファイルをダブルクリックするか、コマンド・ラインから起動します。

- Linux システムの場合は、次のコマンドを発行します。

```
export OUNCE_CONFIG_FILE=<path>
```

ここで `<path>` は、インストール設定が含まれるプロパティ・ファイルの完全修飾パスとファイル名です。

その後、ウィザードを起動します。32 ビット・システムの場合は、`setup.bin` を実行します。64 ビット・システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180>を参照してください。

`setup` ファイルを含むロケーションからコマンドを実行していない場合、そのロケーションにディレクトリを変更するか、コマンドをファイルのロケーションで修飾するようにしてください。

- macOS システムの場合は、以下のコマンドを発行します。

```
export OUNCE_CONFIG_FILE=<path>
./setup.bin
```

ここで `<path>` は、インストール設定が含まれるプロパティ・ファイルの完全修飾パスとファイル名です。

`setup` ファイルを含むロケーションからコマンドを実行していない場合、そのロケーションにディレクトリを変更するか、コマンドをファイルのロケーションで修飾するようにしてください。

**重要:** インストール済み環境を構成する目的で `./setup.bin` コマンドを発行する場合は、コマンドの先頭に `sudo` を指定しないでください。

## タスクの結果

ファイル名が存在しており、有効である場合、カスタム・ウィザードはそのファイル内のプロパティをデフォルト・プロパティとして使用します。既存のファイル名または新規のファイル名を使用して構成を保存できます。ファイル名が存在しない場合、ウィザードは AppScan Source のデフォルト・プロパティを使用します。構成の保存時には、指定されたファイル名がデフォルトとして表示されます。

## カスタム・インストール構成ウィザードの使用

カスタム・インストール・ウィザードが表示され、AppScan Source インストールに使用する構成ファイルをこれから作成することが示されます。

### このタスクについて

Windows システムでカスタム・インストール・ウィザードを実行する場合は、Linux デーモンのユーザー・ステップが表示されます。Windows インストールで最終版の構成ファイルが使用される場合は、この値が無視されます。

ヒント: 既存の構成ファイルを使用してウィザードを実行する場合は、このファイルから値が読み取られ、デフォルト値として使用されます。

### 手順

1. 「サイレント・インストール・オプション」パネルで、インストールをサイレント・インストールとして実行するかどうかを指定して、インストール・タイプを構成します。対話式カスタム・インストールを作成する場合は、「いいえ」を選択してください。

注: カスタムのサイレント・インストールを作成した場合、トルコ語の言語ロケールで実行すると失敗します (例: tr および tr\_TR)。

「次へ」をクリックして、次のインストール・パネルに進みます。

2. 対話式のカスタム・インストールのみ: 対話式のカスタム・インストーラーを作成する場合 (「サイレント・インストール・オプション」パネルで「いいえ」が選択されている場合)、以下の 3 つの「コンポーネントの選択」パネルの設定を完了する必要があります。

- a. 最初のパネルでは、対話式のカスタム・インストールで使用可能な (または表示される) AppScan Source コンポーネントを選択します。

- AppScan Source for Automation
- AppScan Source for Analysis
- AppScan Source コマンド行インターフェース
- AppScan Source for Development for Visual Studio 2013
- AppScan Source for Development for Visual Studio 2012
- AppScan Source for Development for Visual Studio 2010
- AppScan Source for Development for Eclipse, RAD, MobileFirst

注: ターゲット・オペレーティング・システムが選択したコンポーネントをサポートしていない場合や、選択したコンポーネントがシステムに存在しないソフトウェアに依存する場合は、コンポーネントを選択してもインストールでは無視されます。例えば、サポートされるバージョンの Microsoft

Visual Studio がインストールされていないシステムに、カスタム・インストーラーを使用してインストールする場合、インストール対象として AppScan Source for Development for Visual Studio 2012 を選択しても、カスタム・インストーラーのデプロイ時に無視されます。

残りの「コンポーネントの選択」パネルを使用すると、インストール・パネルに表示するコンポーネントをデフォルトで選択するかどうか、有効にするかどうか (有効ではないコンポーネントはインストーラーのデプロイ時にグレー表示されて選択できません) を指定することができます。例えば、コンポーネントのインストールを強制実施するカスタム・インストーラーを希望する場合があります。これを行うには、コンポーネントをデフォルトで選択状態にする一方で、有効にはしません。

コンポーネントを使用可能に設定したにも関わらず、デフォルトで選択状態にせず有効にしない場合は、そのコンポーネントはインストールされません (グレー表示されてインストール用に選択できません)。

「次へ」をクリックして、次のインストール・パネルに進みます。

- b. 次の「コンポーネントの選択」パネルには、対話式的カスタム・インストーラーで使用可能になるよう選択されたコンポーネントのみ表示されます。このパネルでは、使用可能なコンポーネントのうち、どのコンポーネントをデフォルトで選択状態にするかを指定します。「次へ」をクリックして、次のインストール・パネルに進みます。
  - c. カスタム・インストーラーでユーザーが選択または選択解除できるコンポーネントを指定します。コンポーネントを無効にすると、そのコンポーネントのインストールが必須になります (それがデフォルトで選択状態になるよう設定されている場合に限ります)。「次へ」をクリックして、次のインストール・パネルに進みます。
3. サイレント・カスタム・インストールのみ: サイレント・カスタム・インストーラーを作成する場合 (「サイレント・インストール・オプション」パネルで「はい」が選択されている場合)、サイレント・インストーラーがインストールする AppScan Source コンポーネントを選択します。
    - AppScan Source for Automation
    - AppScan Source for Analysis
    - AppScan Source コマンド行インターフェース
    - AppScan Source for Development for Visual Studio 2013
    - AppScan Source for Development for Visual Studio 2012
    - AppScan Source for Development for Visual Studio 2010
    - AppScan Source for Development for Eclipse、RAD、MobileFirst

注: ターゲット・オペレーティング・システムが選択したコンポーネントをサポートしていない場合や、選択したコンポーネントがシステムに存在しないソフトウェアに依存する場合は、コンポーネントを選択してもインストールでは無視されます。例えば、サポートされるバージョンの Microsoft Visual Studio がインストールされていないシステムに、カスタム・インストーラーを使用してイン

ストールする場合、インストール対象として AppScan Source for Development for Visual Studio 2012を選択しても、カスタム・インストーラーのデプロイ時に無視されます。

4. ターゲット・インストール・ディレクトリーを選択します。サイレント・インストールの場合は、これがインストール・ディレクトリーになります。対話式インストールの場合は、これがデフォルト値になります。

「次へ」をクリックして、次のインストール・パネルに進みます。

5. 「ライセンス・ファイルの指定」パネルで、ライセンス・ファイルの場所を指定するか、ライセンス・サーバーのホスト名とポートを指定します。「次へ」をクリックして、次のインストール・パネルに進みます。
6. 「プロパティ・ファイルの指定」パネルで、ターゲット・プロパティ・ファイルの名前と場所を指定します。ウィザードが既存の構成ファイルを使用する場合は、デフォルトのパス名が表示されます。ファイル名を変更して、新しい構成ファイルを作成できます。

Linux サーバーでのインストールのみ: AppScan Source デーモンを実行する Linux ユーザーを指定します。ファイルをコピーした後に、サービス・ユーザーを指定する必要があります。デフォルト・ユーザー「ounce」を作成する場合は「ユーザー 'ounce' の作成」を選択し、既存のユーザーで実行する場合は「既存のユーザーで実行」を選択します。(インストールではこのユーザーが検証されます。選択されたユーザーには有効なシェルが必要となることに注意してください。)

「次へ」をクリックして、プロパティ・ファイルを保存します。

---

## カスタム・インストールまたはサイレント・インストールの実行

このトピックでは、コマンド行からのカスタム・インストールやサイレント・インストールの実行方法をプラットフォーム別に説明します。

### 始める前に

カスタム・インストールを作成できるウィザードを起動する場合 ( 108 ページの『インストール構成ウィザードを起動する』を参照)、OUNCE\_CONFIG\_FILE 環境変数を作成します。カスタム・インストールを実行する前に、この環境変数が削除されていることを確認してください。

### 手順

- Windows システムの場合は、以下のコマンドを発行します。

```
AppScanSrc_Installer.exe -f <configuration_properties_file>
```

ここで、<configuration\_properties\_file> は、「カスタム・インストール構成」ウィザードの実行時に作成したプロパティ・ファイルの完全パスおよびファイル名です (例えば、c:%install.properties)。

- Linux システムの場合は、-f <configuration\_properties\_file> を使用してウィザードを起動します。ここで、<configuration\_properties\_file> は、「カス

タム・インストール構成」ウィザードの実行時に作成したプロパティ・ファイルの完全パスおよびファイル名です (例えば、`/usr/local/share/my_configs/install.properties`)。

32 ビット・システムの場合は、以下を発行します。

```
setup.bin -f <configuration_properties_file>
```

64 ビット Linux システムの場合は、<http://www.ibm.com/support/docview.wss?uid=swg21462180> の説明に従ってウィザードを起動します。ただし、起動コマンドに `-f <configuration_properties_file>` を付加してください。

- macOS システムの場合は、以下のコマンドを発行します。

```
sudo ./setup.bin -f <configuration_properties_file>
```

ここで、`<configuration_properties_file>` は、「カスタム・インストール構成」ウィザードの実行時に作成したプロパティ・ファイルの完全パスおよびファイル名です (例えば、`/Users/myname/install.properties`)。

---

## 例：インストール・フレームワークを介した **AppScan Source** のサイレント・インストール

以下の例で、サイレント・インストールのデプロイ方法について説明します。

### このタスクについて

情報技術 (IT) 部門が、インストール・フレームワークを介してクライアント・コンポーネントをサイレント・インストールしたいと考えています。

クライアントのカスタム・インストールを作成する前に、AppScan Source 管理者は、インストール・フレームワークがアクセス権限を持つファイル・サーバーにインストール・ファイルを配置します。また、IT 部門では、各ユーザー・タイプで必要とされる各種の AppScan Source コンポーネントに基づいて、いくつかの異なるインストール構成を特定する作業も行います。

カスタム・サイレント・インストールで AppScan Source をインストールするには、以下の手順を実行します。

### 手順

1. IT 部門が、AppScan Source インストール CD または FTP ダウンロードから、適切なコンテンツをファイル・サーバーにコピーします。
2. IT 部門が、カスタム・インストール・ウィザードを使用して、必要なインストール・タイプ (例えば AppScan Source for Development や AppScan Source for Analysis) ごとに、必要なインストール構成ファイルを作成します。
3. IT 部門が、共有パブリック・フォルダーに構成ファイルを格納します。
4. IT 部門が、AppScan Source インストールを認識するようにインストール・フレームワークを構成し、適切なコマンド行呼び出しとインストール構成 をインストール・フレームワークに関連付けます。

5. ユーザーが、(デスクトップ上で) インストール・フレームワーク・クライアントを介して更新を確認します。適切な (ユーザー固有の) AppScan Source 製品がインストール・リストに表示されます。
6. ユーザーが、インストール・フレームワーク・クライアントを介してインストールを開始します。
7. AppScan Source がユーザーのデスクトップ・コンピューターにサイレント・インストールされます。

## タスクの結果

このインストールが完了すると、以下のようになります。

- 適切な AppScan Source 製品がデスクトップにインストールされ、AppScan Enterprise Server に接続するように構成されます。
- ライセンス・ファイルがターゲット・コンピューターにコピーされます。



---

## 第 8 章 ソフトウェアのアクティブ化

AppScan Source 製品を使用する前に、ご使用のソフトウェアをアクティブ化する必要があります。AppScan Source には License Manager ユーティリティが用意されており、それを使用して、クライアント・マシン上でライセンス情報をロードおよび更新することができます。このユーティリティを使用することで、現在のライセンス状態を確認することができます。また、ライセンス・ファイルをインポートしたり、ライセンス・サーバーでフローティング・ライセンスを使用したりすることで、ユーティリティから製品をアクティブ化することもできます。License Manager を起動すると、それまでにロードされたライセンスがすべてスキャンされます。

AppScan Source 製品のインストール後、これをアクティベーションする方法は 3 とおりあります。

- 製品のインストール・ウィザードから、License Manager ユーティリティを起動します (インストールの完了後)。
- License Manager ユーティリティは、製品のインストール後に、以下のようにして起動できます。
  - Windows では、「スタート」メニューからユーティリティを起動します (「すべてのプログラム」メニューから、「**IBM Security AppScan Source**」 > 「**AppScan Source License Manager**」を起動します)。
  - Linux で、<install\_dir>/bin (<install\_dir> は AppScan Source インストール済み環境がある場所です) を見つけたら、コマンド `./licensemgr.sh` を発行することで `licensemgr.sh` を実行してください。
  - macOS で、/Applications/AppScanSource.app/bin を見つけ、コマンド `./licensemgr.sh` を発行して `licensemgr.sh` を実行します。
- 製品を起動します。製品を使用するためのライセンスがまだ適用されていない場合、製品を使用するにはライセンスを適用する必要があることを通知するメッセージが表示されます。このメッセージで「OK」をクリックすると、License Manager ユーティリティが開きます。

AppScan Source 製品のライセンスの取得、インストール、および適用に関する詳細については、<http://www.ibm.com/support/docview.wss?uid=swg21405482> および <http://www.ibm.com/support/docview.wss?uid=swg21407312> を参照してください。

注:

- コマンド行ユーザー・インターフェースを使用して製品をアクティブ化する場合、インストール・ウィザードまたは Windows の「スタート」メニューから License Manager ユーティリティを起動する必要があります。最初にソフトウェアのアクティブ化を行わずに、コマンド行インターフェースを使用して製品を使用しようとする、License Manager ユーティリティでソフトウェアをアクティブ化するよう求めるエラー・メッセージが表示されます。
- 最初にライセンスを適用せずに、AppScan Enterprise Server を実行している場合、サーバーに接続しようとしたときにエラー・メッセージが表示されます。

- AppScan Source for Development の機能を最大限に利用するには、それ自体のライセンスとともに、AppScan Source for Remediation のライセンスを適用する必要があります。

---

## ライセンス・ファイルのインポート

このタスク・トピックでは、AppScan Source のライセンス・ファイルのインポート手順について説明します。

### 手順

1. AppScan Source のライセンス・ファイルのファイル拡張子は .upd または .txt です。ローカル・ファイル・システムまたはマッピングされたドライブ上でライセンスが使用可能であることを確認してください。
2. 「ライセンスのインポート」をクリックします。
3. 「ライセンス・ファイルのインポート」ダイアログ・ボックスを使用して、ライセンス・ファイルを参照します。ライセンス・ファイルを選択して、「OK」をクリックします。

注: macOS でライセンス・ファイルを参照する場合、「ライセンス・ファイルのインポート」ダイアログ・ボックスのコンテンツが表示されなくなることがあります (フォルダーは開きますが、コンテンツは表示されません)。これを回避するには、異なるフォルダーを選択してから、表示したいコンテンツが含まれるフォルダーを再度選択してください。

4. 「ライセンス・ファイルが正常にインポートされました」というメッセージが表示されたら、「OK」をクリックしてアクティベーションを完了します。
5. License Manager を閉じます。これで、インストール済み製品の起動時に、このライセンスが使用されるようになります。

---

## フローティング・ライセンスの使用

このタスク・トピックでは、フローティング・ライセンスのアクティベーションの対象となるライセンス・サーバー (複数可) を構成する手順について説明します。

### 手順

1. 「ライセンス・サーバーの構成」をクリックして、「ライセンス・サーバーの構成」ダイアログ・ボックスを開きます。
2. 「追加」をクリックします。
3. 「ホスト名」と「ポート」にライセンス・サーバーのホスト名とポートを入力し、「変更の保存」をクリックします。複数のライセンス・サーバーを追加する場合は、このステップを繰り返します。

注: ライセンス・サーバーのデフォルト・ポートは 27000 です。別のポートでライセンス・サーバーを実行するよう設定した場合のみ、この値を編集してください。

4. ライセンス・サーバーを追加した後、そのホスト名またはポートを編集する必要がある場合は、リストから該当するサーバーを選択します。これにより、「ホ

スト名」と「ポート」フィールドに値が表示されます。これらの設定を編集したら、「変更の保存」をクリックして、ライセンス・サーバー設定に変更内容を保存します。

5. 複数のライセンス・サーバーを追加した場合は、このダイアログ・ボックス内のリストに表示される順序でライセンス・サーバーがスキャンされます。AppScan Source 機能のフローティング・ライセンスが検出された場合は、フローティング・ライセンスのスキャンが停止します。サーバーをスキャンする順序を変更するには、リスト内で移動したいサーバーを選択し、「上」または「下」をクリックします。
6. すべてのライセンス・サーバーを構成したら、「OK」をクリックします。

## タスクの結果

ダイアログ・ボックスが閉じると、構成済みのライセンス・サーバーで AppScan Source 機能のフローティング・ライセンスが検索されます。検出されたフローティング・ライセンスは、License Manager のライセンス・リストに表示されます。

ライセンス・サーバーに変更を加えた場合は、「更新」をクリックして、License Manager が現在のライセンス・サーバー情報にアクセスできるようにします。

フローティング・ライセンス・サーバーの構成が終了したら、License Manager を閉じます。これで、インストール済み製品の起動時に、これらのライセンスが使用されるようになります。

注: AppScan Source のフローティング・ライセンスは、Rational License Server のサポート対象バージョンでホストされる必要があります。それより低いレベルの Rational License Server でホストされると、License Manager にはそれらのライセンスが表示されますが、AppScan Source はそれらを使用できません。AppScan Source でサポートされる Rational License Server のバージョンについては、<http://www.ibm.com/support/docview.wss?uid=swg27027486> を参照してください。

AppScan Source for Development を使用するチームでは、フローティング・スキャン・ライセンスをユーザー・インターフェースから直接リリースできるので、他のチーム・メンバーがライセンスを必要とするときにはその獲得が可能です。ローカル・モード には、「ライセンスのスキャンの解除」アクションがあります。一方、サーバー・モード では、ライセンスは「サーバーからログアウト」アクションの一環として解除されます。ライセンスのリリース後は、スキャンの開始時に (ライセンスが使用可能な場合は) ライセンスが自動的に再度取得されます。

---

## ライセンスの表示

License Manager ユーティリティのライセンス・リストには、以下のものが表示されます。

- ライセンス (複数可) が適用される AppScan Source 製品および機能 (他の IBM 製品のライセンスは、このユーティリティには表示されません)。
- ライセンス・タイプ: フローティング・ライセンスかノードロック・ライセンス (インポートされたライセンス・ファイルを示す) のいずれかになります。

- ライセンスの有効期限: ライセンスの残り日数が表示されます。日数が 365 日を超える場合は、ライセンスの有効期限に単に「有効」と示されます。
- 指定されたすべてのサーバー上の購入済みの AppScan Source ライセンスの合計数。

注: 使用中のライセンス数を判別するには Rational License Server を使用する必要があります。この情報は、AppScan Source ライセンス管理ユーティリティでは参照できません。

---

## 第 9 章 システムからの AppScan Source の削除

AppScan Source は、Windows コントロール・パネルから削除するか、Linux または macOS のアンインストール・スクリプトを使用して削除することができます。AppScan Source のアンインストールでは、インストール済みの Oracle データベースの削除やバックアップは行われません。Oracle インスタンスから AppScan Source ユーザーを削除することは、手動のデータベース管理タスクです。

### このタスクについて

- 『Microsoft Windows プラットフォームからの削除』
- 『Linux プラットフォームからの削除』
- 128 ページの 『macOS プラットフォームからの削除』

---

### Microsoft Windows プラットフォームからの削除

#### 手順

1. プログラムの削除には、「コントロール・パネル」オプションを使用します。例えば、Windows 7 では、「コントロール パネル」の「プログラムと機能」オプションを選択します。
2. 適切なアクションを選択して、インストールされているプログラムのリストから、「IBM Security AppScan Source」を削除します。

---

### Linux プラットフォームからの削除

Linux にインストールする場合、実行すると AppScan Source を削除できるスクリプトが作成されます。

#### このタスクについて

アンインストールを行う場合は、インストール時と同じユーザーでアンインストールする必要があります。Linux 上に root としてソフトウェアをインストールした場合は、root としてアンインストールする必要があります。

#### 手順

1. `<install_dir>/Uninstall_AppScan/AppScan_Uninstaller` (`<install_dir>` は AppScan Source インストール済み環境がある場所です) というスクリプトを見つけてみます。
2. このスクリプトを実行すると、製品の削除に使用するウィザードが表示されます。

---

## macOS プラットフォームからの削除

macOS にインストールする場合、実行すると AppScan Source を削除できるスクリプトが作成されます。

### このタスクについて

アンインストールを行う場合は、インストール時と同じユーザーでアンインストールする必要があります。

### 手順

1. `<install_dir>/Uninstall_AppScan/AppScan_Uninstaller.sh` (`<install_dir>` は AppScan Source インストール済み環境がある場所です) というスクリプトを見つけてください。
2. 製品を削除するには、このスクリプトを実行します (`sudo` を使用)。

---

## 第 10 章 AppScan Source の管理

このセクションでは、ユーザー管理、許可、アプリケーションとプロジェクトの登録、およびポート構成について説明します。

AppScan Source 管理者は、AppScan Enterprise Server および AppScan Source の製品をデプロイおよびインストールし、適切な特権および許可を指定してユーザーを作成 (または AppScan Enterprise Server ユーザーの自動ログインを構成) する必要があります。これらの作業を行うためには、管理者は、各ユーザーのロールと、必要なデプロイメント・モデルについて把握していなければなりません。また、他のシステム (障害追跡システムやディレクトリー・サーバーなど) を AppScan Source および AppScan Enterprise Server と統合する必要があるかどうかについても、管理者は確認する必要があります。

AppScan Source for Analysis および AppScan Enterprise Server のインストール構成、サーバーへの接続方法、および各ユーザーが使用可能な機能を理解することも重要です。例えば、管理者は、AppScan Source アプリケーションおよびプロジェクトの構成方法や、それらの登録および公開方法について熟知している必要があります。詳細については、*IBM Security AppScan Source for Analysis ユーザー・ガイド* を参照してください。

一般に、管理者は、ユーザーが AppScan Enterprise Server の資格情報を使用して AppScan Source 製品にログインするように設定します。しかし、何らかの理由で、AppScan Enterprise Server に存在しない AppScan Source ユーザーを管理する必要がある場合、管理者はローカルの AppScan Source ユーザーを作成することができます (130 ページの『AppScan Source ユーザーの作成』を参照してください)。

---

### ユーザー・アカウントおよび許可

AppScan Source ユーザーがスキャンまたは結果のトリアージを開始するには、管理者がユーザー・アカウントを作成し、そのアカウントに許可を割り当てる必要があります。

AppScan Source ユーザー許可は AppScan Source データベース に保存されており、ユーザーが AppScan Enterprise Server にログインする時に適用されます。ローカル・モード で AppScan Source for Development を実行するユーザーは、完全な AppScan Source 許可を持っています。

ユーザーの作成時、そのユーザーにロールを設定し、そのユーザーが使用可能な許可を識別します。許可は、そのユーザーに許可される AppScan Source タスクを識別します。特に許可の一部として識別されないタスクは、すべてのユーザーが実行できます。

注: ユーザー ID は変更できません。ユーザー・アカウントを削除し、同じユーザー ID でユーザーを再作成する必要があります。

許可グループ	許可
アプリケーションおよびプロジェクトの管理	登録 (アプリケーションとプロジェクトの登録および登録抹消)
	スキャン
	登録済み内容の表示
	属性の管理
	属性の適用
評価管理	公開された評価の削除
	評価の保存
	評価の公開
	公開された評価の表示
ナレッジベース・データベース 管理	カスタム・ルールの管理
	パターンの管理
管理	ユーザーの管理
	AppScan Enterprise 設定の管理
フィルター管理	共有フィルターの管理
スキャン構成	共有構成の管理 (スキャン構成の共有および共有スキャン構成の編集/削除)

## AppScan Source ユーザーの作成

一般に、管理者は、ユーザーが AppScan Enterprise Server の資格情報を使用して AppScan Source 製品にログインするように設定します。しかし、何らかの理由で、AppScan Enterprise Server に存在しない AppScan Source ユーザーを管理する必要がある場合、管理者は、このトピックの説明に従って、ローカルの AppScan Source ユーザーを作成することができます。

### このタスクについて

ユーザーは、AppScan Source for Analysis ユーザー・インターフェース、または CLI で作成することができます (CLI でユーザーを作成する方法については、*IBM Security AppScan Source Utilities ユーザー・ガイド* を参照してください)。AppScan Source for Analysis ユーザー・インターフェースで、AppScan Enterprise Server ユーザーの自動ログインを設定することもできます (132 ページの『AppScan Enterprise Server ユーザーの自動ログインを構成』を参照してください)。

AppScan Source for Analysis のユーザー・インターフェースでユーザーを作成するには、以下の手順を実行します。

### 手順

1. ワークベンチのメインメニューで、「管理」 > 「ユーザーの管理」を選択します。
2. 「ユーザーの管理」ダイアログ・ボックスに、既存の AppScan Source ユーザーがリストされます。**AppScan Enterprise Server** ユーザー・リポジトリに存在するユーザーは、ローカルの AppScan Source データベースおよび

AppScan Enterprise Server に存在します。 **AppScan Source** リポジトリに存在するユーザーは、AppScan Source データベースのみに存在します。このダイアログ・ボックスで新規ユーザーを作成すると、そのユーザーは AppScan Source データベース内にものみ作成されます。

3. 「ユーザーの追加」をクリックして、「ユーザーの追加」ダイアログ・ボックスを開きます。
4. 「ユーザー ID」を入力した後、そのユーザーのパスワードを入力します (確認のために 2 回入力してください。パスワードは 6 文字から 16 文字までです)。これらは必須フィールドです。 オプションで、ユーザーの「名前」 (最大 255 文字) を追加することもできます。
5. 許可ツリーを展開し、ユーザーの許可を示すチェック・ボックスを選択します。
6. 「OK」をクリックして、ユーザーを作成します。

### タスクの結果

このトピックで説明した設定を使用して、ユーザーを編集することもできます。その場合は、「ユーザーの管理」ダイアログ・ボックスでユーザーを選択して「ユーザーの編集」をクリックします。同様に、ユーザーを選択して「ユーザーの削除」をクリックすることにより、ユーザーを削除できます。

注: AppScan Source for Analysis から AppScan Enterprise Server ユーザーを編集する場合は、ユーザーの AppScan Source 権限のみを変更することができます (「AppScan Enterprise 設定の管理」権限を持っている場合に限り).

## AppScan Enterprise Server の認証: IBM Rational Jazz ユーザー認証コンポーネントの IBM WebSphere Liberty への置き換えに関するマイグレーションの考慮事項

このトピックでは、旧バージョンの AppScan Enterprise Server からアップグレードする場合に考慮する必要がある、ユーザー管理に関連するマイグレーションの考慮事項について説明します。

- ローカル **Jazz** ユーザーのみが含まれる **Enterprise Server** からのマイグレーション: このアップグレード・シナリオでは、以前の Jazz ユーザーは、AppScan Source データベースに AppScan Enterprise Server ユーザーとして表示されますが、有効ではありません。これらのユーザーをデータベースから削除できます。あるいは、<http://www.ibm.com/support/docview.wss?uid=swg21686347> の説明に従って変換を有効にする場合、これらのユーザーを AppScan Source ユーザーに変換できます。
- **LDAP** を使用して構成された **Enterprise Server** からのマイグレーション: Enterprise Server のアップグレード時に、LDAP を使用して Enterprise Server を再構成するオプションがあります。これを行う場合、既存のユーザーは引き続き AppScan Source で機能します。
- **Windows** 認証を使用して構成された **Enterprise Server** からのマイグレーション: Enterprise Server が Windows 認証を使用して構成されていた場合、新しい Enterprise Server Liberty が Windows 認証を使用するように構成されていると、既存のユーザーは AppScan Source で機能します。

注: LDAP または Windows の認証を使用して構成されていた Enterprise Server からマイグレーションする場合、既存のユーザーには、AppScan Enterprise Server に割り当てられるデフォルトの権限が再割り当てされます。これらのデフォルトの権限については、『AppScan Enterprise Server ユーザーの自動ログインを構成』で説明しています。

## AppScan Enterprise Server ユーザーの自動ログインを構成

デフォルトでは、AppScan Enterprise Server ユーザーは AppScan Source にログインすることができ、自動的に AppScan Source for Analysis に追加されます (これらのユーザーは、AppScan Enterprise Server ユーザーとしてリストされます)。このトピックの説明に従い、AppScan Source for Analysis ユーザー・インターフェースで、このフィーチャーを構成することができます。

### 手順

1. AppScan Source for Analysis の「管理」メニューから、「ユーザーの管理」をクリックします。
2. 「ユーザーの管理」ダイアログ・ボックスで、「**AppScan Enterprise Server** ユーザーのログインを構成」リンクをクリックします。
3. 「AppScan Enterprise Server ユーザーのログインを構成」ダイアログ・ボックスでは、このフィーチャーを有効にして、AppScan Enterprise Server ユーザーの初期の許可を設定できます。
  - デフォルトでは、AppScan Enterprise Server ユーザーは AppScan Source にログインすることができます。このフィーチャーを無効にするには、「**AppScan Enterprise Server** ユーザーによるログインを許可」チェック・ボックスを選択解除します。
  - デフォルトでは、AppScan Enterprise Server ユーザーは AppScan Source へのログイン時には以下の許可を持っています。
    - 登録
    - スキャン
    - 登録済み項目の表示
    - 属性の管理
    - 属性の適用
    - 評価の保存

許可ツリーを展開し、AppScan Enterprise Server ユーザーに適した初期設定を示すチェック・ボックスを選択します。使用可能なすべての許可のリストについては 129 ページの『ユーザー・アカウントおよび許可』を参照してください。
4. 「OK」をクリックして、「AppScan Enterprise Server ユーザーのログインを構成」ダイアログ・ボックスを閉じてから「ユーザーの管理」ダイアログ・ボックスを閉じてください。

### タスクの結果

AppScan Enterprise Server ユーザーが初めて AppScan Source にログインすると、AppScan Enterprise Server へのログインに使用したのと同じ認証資格情報

を持つ AppScan Source ユーザー・アカウントが作成されます。このアカウントは作成後に変更できます (例えばその許可の変更など)。

この機能を無効にする場合、130 ページの『AppScan Source ユーザーの作成』の説明に従って、AppScan Enterprise Server ユーザーを手動で作成する必要があります。

## AppScan Enterprise Server Liberty でのローカル製品管理者ユーザーの作成

AppScan Enterprise Server バージョン 9.0.1 では、AppScan Source を管理するために、AppScan Enterprise Server Liberty でローカル製品管理者ユーザーを作成する機能が提供されています。ユーザーを作成した後、管理者資格情報を使用して、AppScan Source データベースを AppScan Enterprise Server に登録する必要があります。

AppScan Enterprise Server Liberty でのローカル製品管理者ユーザーの作成方法については、以下の該当するトピックの説明に従ってください。

- 『LDAP を使用して構成されている AppScan Enterprise Server のローカル製品管理者ユーザーの作成』
- 134 ページの『Windows 認証を使用して構成されている AppScan Enterprise Server のローカル製品管理者ユーザーの作成』

### LDAP を使用して構成されている AppScan Enterprise Server のローカル製品管理者ユーザーの作成

#### 手順

1. server.xml ファイルを見つけます。Windows の場合、このファイルは、ご使用の AppScan Enterprise Server インストール・ディレクトリーの Liberty\usr\servers\ase フォルダー内にあります。Linux の場合、このファイルは、ご使用の AppScan Enterprise Server インストール・ディレクトリーの Liberty/usr/servers/ase フォルダー内にあります。

このファイルを以下のように編集します。

- a. product.admins の値を管理者ユーザーの名前 (例えば、**ADMIN**) に変更します。

```
<jndiEntry jndiName="product.admins" value="ADMIN"/>
```
- b. 既存の LDAP タグ・セクションを削除して、basicRegistry セクションを追加します。

例えば、以下のセクションを削除します。

```
<ldapRegistry baseDN="o=example.com" bindDN=""
  bindPassword="" host="ldap.example.com"
  ldapType="IBM Tivoli Directory Server"
  port="389" sslEnabled="false">
  <idsFilters userFilter=
    "(&uid=%v)(objectclass=ePerson)"
    userIdMap="*:uid"/>
</ldapRegistry>
```

そして、以下のセクションを追加します (この例では、サンプル・パスワードとして ADMIN を使用しています)。

```
<basicRegistry id="basic" realm="customRealm">
  <user name="ADMIN" password="ADMIN" />
</basicRegistry>
```

注: 管理者パスワードは、135 ページの『管理者パスワードの暗号化』に記載されている説明に従って暗号化することができます。この場合、このセクションに、生成された暗号化パスワードを指定します。

2. ファイルを保存し、ase サービスを再開します。
  - Linux の場合、`/etc/init.d/ase_liberty restart` コマンドを実行します。
  - Windows の場合、以下のいずれかの作業を行います。
    - Windows の「スタート」メニューで「実行」を選択して、`services.msc` と入力します。「サービス」ウィンドウが開いたら、「**IBM Security AppScan Enterprise Server**」を右クリックして、「リスタート」を選択します。
    - コマンド・プロンプトで、ご使用の AppScan Enterprise Server インストール・ディレクトリーの `Liberty\bin` フォルダーにディレクトリーを移動します。`server stop ase` コマンドを実行して、次に `server start ase` コマンドを実行します。
3. 新しく作成した ADMIN 資格情報を使用して、AppScan Source データベースを AppScan Enterprise Server に登録します。

## Windows 認証を使用して構成されている AppScan Enterprise Server のローカル製品管理者ユーザーの作成

### 手順

1. `server.xml` ファイルを見つけます。Windows の場合、このファイルは、ご使用の AppScan Enterprise Server インストール・ディレクトリーの `Liberty\usr\servers\ase` フォルダー内にあります。Linux の場合、このファイルは、ご使用の AppScan Enterprise Server インストール・ディレクトリーの `Liberty/usr/servers/ase` フォルダー内にあります。

このファイルを以下のように編集します。

- a. 以下の行を削除します。

```
<feature>usr:WindowsRegistryFeature</feature>
```
- b. `product.admins` の値を管理者ユーザーの名前 (例えば、**ADMIN**) に変更します。

```
<jndiEntry jndiName="product.admins" value="ADMIN"/>
```
- c. 以下をファイルの最後にある `</server>` の前に追加します (この例では、サンプル・パスワードとして ADMIN を使用しています):

```
<basicRegistry id="basic" realm="customRealm">
  <user name="ADMIN" password="ADMIN" />
</basicRegistry>
```

注: 管理者パスワードは、135 ページの『管理者パスワードの暗号化』に記載されている説明に従って暗号化することができます。この場合、このセクションに、生成された暗号化パスワードを指定します。

2. ファイルを保存し、ase サービスを再開します。
  - Linux の場合、`/etc/init.d/ase_liberty restart` コマンドを実行します。
  - Windows の場合、以下のいずれかの作業を行います。
    - Windows の「スタート」メニューで「実行」を選択して、`services.msc` と入力します。「サービス」ウィンドウが開いたら、「**IBM Security AppScan Enterprise Server**」を右クリックして、「リスタート」を選択します。
    - コマンド・プロンプトで、ご使用の AppScan Enterprise Server インストール・ディレクトリーの `Liberty\bin` フォルダにディレクトリーを移動します。`server stop ase` コマンドを実行して、次に `server start ase` コマンドを実行します。
3. 新しく作成した ADMIN 資格情報を使用して、AppScan Source データベースを AppScan Enterprise Server に登録します。

## 管理者パスワードの暗号化

AppScan Enterprise Server のローカル製品管理者ユーザーを作成する場合、`server.xml` ファイルに管理者ユーザーとパスワードを追加します。このトピックの説明に従って、このパスワードを暗号化することができます。

( 133 ページの『LDAP を使用して構成されている AppScan Enterprise Server のローカル製品管理者ユーザーの作成』または 134 ページの『Windows 認証を使用して構成されている AppScan Enterprise Server のローカル製品管理者ユーザーの作成』の説明に従って) `server.xml` ファイルを編集する際に、`securityUtility` ツールを使用して、管理者ユーザーのパスワードをエンコードすることができます。Windows の場合、このツールは AppScan Enterprise Server インストール・ディレクトリー内の `Liberty\bin` にあります。Linux の場合、このツールは `Liberty/bin` にあります。`securityUtility` エンコード・コマンドを実行するときに、エンコードするパスワードをコマンド行から入力として指定します。引数が指定されていない場合、ツールはパスワードの入力を要求するプロンプトを出します。次に、ツールはエンコードされた値を出力します。例えば、値 ADMIN のパスワードをエンコードする場合は、`securityUtility encode ADMIN` コマンドを実行します。これにより、出力値 `{xor}HhsSFhE=` が生成されます。

ツールによって生成された値をコピーして、`basicRegistry` セクションを `server.xml` ファイルに追加する際に、この値をパスワードに使用します。例えば、以下をファイルに追加します。

```
<basicRegistry id="basic" realm="customRealm">
  <user name="ADMIN" password="{xor}HhsSFhE=" />
</basicRegistry>
```

## Automation Server のユーザー・アカウントの作成

Automation Server を使用するためにはユーザー・アカウントが必要です。このユーザー・アカウントは、インストール時に、またはインストール後にコマンド行を使用して、Automation Server に登録しなければなりません。対応する AppScan Source ユーザー・アカウントも、インストール後に AppScan Source for Analysis または AppScan Source コマンド行インターフェース (CLI) を使用して手動で作成する必要があります。このトピックでは、AppScan Source for Analysis を使用してこのアカウントを作成する方法を説明します。

## 手順

1. 新規ユーザーの作成方法については、130 ページの『AppScan Source ユーザーの作成』の説明に従ってください。あるいは、AppScan Enterprise Server ユーザーの自動作成を有効にしてください（132 ページの『AppScan Enterprise Server ユーザーの自動ログインを構成』を参照してください）。
2. Automation Server を使用するすべてのユーザーには、必ず Automation Server ログインに指定した同じユーザー名およびパスワードを指定してください。その他の設定（許可など）は、必要に応じて指定することができます。

---

## 第 11 章 ユーザー・アクティビティの監査

AppScan Source は、ユーザー・アクティビティを監査するための便利な機能を提供します。「監査」ビューでは、AppScan Enterprise Server に対する認証、新規ユーザーの作成、データベースでの新規ルールの作成などのイベントが記録されます。

「監査」ビューを開くには、メインメニューから「管理」 > 「監査」を選択します。

注: 「監査」ビューを使用するには「ユーザーの管理」許可が必要です。適切な許可なくビューを開くと、エラーになります。AppScan Source 許可については、129 ページの『ユーザー・アカウントおよび許可』を参照してください。



---

## 第 12 章 AppScan Source 製品から AppScan Enterprise Server へのログイン

ほとんどの AppScan Source 製品とコンポーネントでは、AppScan Enterprise Server への接続が必要です。このサーバーは、一元的ユーザー管理機能と、AppScan Source データベース を介して評価を共有するためのメカニズムを提供します。

AppScan Source for Analysis を起動すると、AppScan Enterprise Server に認証を受けるようにプロンプトが出されます。サーバー・モードで AppScan Source for Development を実行している場合、サーバーにアクセスする必要があるアクション (スキャンの起動、またはスキャン構成の表示など) を初めて開始するときに、AppScan Enterprise Server に認証を受けるようにプロンプトが出されます。

- 『AppScan Enterprise Server ユーザー ID とパスワードを使用した AppScan Source for Analysis および AppScan Source for Development からのログイン』
- 140 ページの『AppScan Source for Analysis および AppScan Source for Development からログインするための Common Access Card (CAC) 認証の使用』
- 141 ページの『AppScan Source for Automation および AppScan Source コマンド行インターフェース (CLI)からのログイン』
- 141 ページの『AppScan Enterprise Server の SSL 証明書』
- 141 ページの『AppScan Enterprise Server 証明書エラーの解決』

### AppScan Enterprise Server ユーザー ID とパスワードを使用した AppScan Source for Analysis および AppScan Source for Development からのログイン

AppScan Source for Analysis では、ログイン時に以下の情報が要求されます。

- **ユーザー ID:** ユーザー ID を指定します (アカウントがどのようにセットアップされているかに応じて、これは、AppScan Enterprise Server 上と AppScan Source データベース 内の両方に存在するユーザー ID か、AppScan Source データベース 内のみに存在するユーザー ID のいずれかです)。
  - AppScan Enterprise Server が Windows 認証を使用するように構成されている場合、Enterprise Console への接続に使用するドメイン名とユーザー名を入力します。ドメイン名とユーザー名は ¥ で区切ります (例えば、my\_domain¥my\_username)。
  - AppScan Enterprise Server が LDAP を使用して構成されている場合、Enterprise Console への接続に使用するユーザー名を入力します。
- **パスワード:** ご使用のユーザー ID のパスワードを指定します。
- **AppScan Enterprise Server:** AppScan Enterprise Server インスタンスの URL を指定します。この URL の形式は http(s)://<hostname>:<port>/ase です。ここで、<hostname> は、AppScan Enterprise Server がインストールされている

マシンの名前、<port> は、サーバーが稼働しているポートです。この URL の例は、<https://myhost.mydomain.ibm.com:9443/ase> のようになります。

AppScan Source for Development では、ログイン時に以下の情報が要求されます。

- **サーバー URL:** AppScan Enterprise Server インスタンスの URL を指定します。この URL の形式は `http(s)://<hostname>:<port>/ase` です。ここで、<hostname> は、AppScan Enterprise Server がインストールされているマシンの名前、<port> は、サーバーが稼働しているポートです。この URL の例は、<https://myhost.mydomain.ibm.com:9443/ase> のようになります。
- **ユーザー ID:** ユーザー ID を指定します (アカウントがどのようにセットアップされているかに応じて、これは、AppScan Enterprise Server 上と AppScan Source データベース 内の両方に存在するユーザー ID か、AppScan Source データベース 内のみに存在するユーザー ID のいずれかです)。
  - AppScan Enterprise Server が Windows 認証を使用するように構成されている場合、Enterprise Console への接続に使用するドメイン名とユーザー名を入力します。ドメイン名とユーザー名は ¥ で区切ります (例えば、`my_domain¥my_username`)。
  - AppScan Enterprise Server が LDAP を使用して構成されている場合、Enterprise Console への接続に使用するユーザー名を入力します。
- **パスワード:** ご使用のユーザー ID のパスワードを指定します。

### AppScan Source for Analysis および AppScan Source for Development からログインするための Common Access Card (CAC) 認証の使用

Windows の場合、CAC 認証 (<http://www.cac.mil>) を使用して AppScan Enterprise Server に接続できます。接続する前に、Common Access Card (CAC) 認証用に AppScan Enterprise Server と AppScan Source をセットアップする必要があります。Enterprise Server が CAC 認証用に設定されている場合、Enterprise Server のユーザー ID とパスワードを使用してログインすることはできません。

AppScan Source for Analysis では、ログイン時に以下の情報が要求されます。

- **ユーザー:** ご使用の CAC 共通名をリストから選択します。
- **AppScan Enterprise Server:** AppScan Enterprise Server インスタンスの URL を指定します。この URL の形式は `http(s)://<hostname>:<port>/ase` です。ここで、<hostname> は、AppScan Enterprise Server がインストールされているマシンの名前、<port> は、サーバーが稼働しているポートです。この URL の例は、<https://myhost.mydomain.ibm.com:9443/ase> のようになります。

AppScan Source for Development では、ログイン時に以下の情報が要求されます。

- **サーバー URL:** AppScan Enterprise Server インスタンスの URL を指定します。この URL の形式は `http(s)://<hostname>:<port>/ase` です。ここで、<hostname> は、AppScan Enterprise Server がインストールされているマシンの名前、<port> は、サーバーが稼働しているポートです。この URL の例は、<https://myhost.mydomain.ibm.com:9443/ase> のようになります。

- ユーザー: ご使用の CAC 共通名をリストから選択します。

「OK」のクリック後、「Windows セキュリティ」ダイアログ・ボックスに、ご使用の CAC カード PIN を入力するようにプロンプトが出されます。

ヒント:

- ログインが失敗した場合、AppScan Enterprise Server が正しくセットアップされていること、およびご使用の証明書が有効なことを確認してください。ブラウザを経由して AppScan Enterprise Server にアクセスできるかを確認してください。アクセスできる場合は、証明書を選択してログインできるはずです。
- ログイン・ダイアログ・ボックスの「ユーザー」フィールドに使用可能な証明書がリストされていない場合、JRE の `java.security` ファイルを『Common Access Card (CAC) 認証の有効化』の説明に従って変更したことを確認してください。
- 「Windows セキュリティ」ダイアログ・ボックスにより CAC カード・ピンに関するプロンプトが出されない場合、Microsoft Smart Card Resource Manager サービスが実行中であることを確認してください。一部のリモート・デスクトップ接続タイプでは、このサービスが実行されていない可能性があることにご注意ください。

## AppScan Source for Automation および AppScan Source コマンド行インターフェース (CLI)からのログイン

ログイン・アクションは、AppScan Source for Automation または AppScan Source コマンド行インターフェース (CLI) を実行する際にも必要です。詳しくは、*IBM Security AppScan Source Utilities ユーザー・ガイド* を参照してください。

## AppScan Enterprise Server の SSL 証明書

AppScan Enterprise Server の SSL 証明書について詳しくは、144 ページの『AppScan Enterprise Server の SSL 証明書』を参照してください。

## AppScan Enterprise Server 証明書エラーの解決

不明な認証局を使用して Enterprise Server にログインしようとする時、ログイン時に証明書例外またはエラーが表示される場合があります。AppScan Source には、この修正に役立つ小さなユーティリティが含まれています。このツールは、`<install_dir>\bin\certificatetool.bat` (`<install_dir>` は AppScan Source インストール済み環境がある場所です) または (Linux および macOS の場合は) `<install_dir>/bin/certificatetool.sh` です。

---

## Common Access Card (CAC) 認証の有効化

このトピックでは、Common Access Card (CAC) 認証が有効になっている AppScan Enterprise Server への接続を許可するように AppScan Source を設定する方法を示します。

## 始める前に

CAC 認証は、Windows における AppScan Enterprise Server バージョン 9.0.3.1 iFix-001 以上への接続用にのみサポートされています。

### 手順

1. AppScan Enterprise Server が CAC 認証用にまだセットアップされていないことを確認してください。
2. AppScan Source for Analysis または AppScan Source コマンド行インターフェース (CLI) に AppScan Source 管理者としてログインします。
3. すべての AppScan Enterprise Server ユーザーがすべての許可を持つように設定するために、*IBM Security AppScan Source* インストールと管理のガイドの指示に従ってください。これにより、AppScan Enterprise Server ユーザーに完全管理アクセス権を与えるための初期のデフォルト許可が設定されますが、CAC セットアップの完了後は組織のニーズに合うように、そのデフォルト許可を変更できます。
4. すべての AppScan Source クライアント・アプリケーションを終了またはシャットダウンします。
5. CAC 認証を許可するように AppScan Enterprise Server をセットアップします。
6. Common Access Card (CAC) 認証が有効になっている AppScan Enterprise Server に AppScan Source データベースを登録する場合は、*IBM Security AppScan Source* インストールと管理のガイドの指示に従います。
7. `<data_dir>%config%ounce.ozsettings` (`<data_dir>` は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。)) を開きます。このファイルで、以下の設定を見つめます。

```
<Setting
  name="client_cert_auth"
  value="false"
  default_value="false"
  description="Uses client certificate authentication"
  display_name="Uses client certificate authentication"
  type="boolean"
  read_only="true"
  hidden="true"
/>
```

8. この設定で、`value="false"` を `value="true"` に変更し、ファイルを保存します。
9. AppScan Source for Analysis または AppScan Source for Development Eclipse プラグイン から AppScan Enterprise Server にログインする場合は、以下のようにします。
  - a. Java インストール・ディレクトリーで、`jre/lib/security/java.security` を見つけます。AppScan Source for Analysis の場合、`jre` フォルダは AppScan Source インストール・ディレクトリー内にあります。このファイルのバックアップ・コピーを作成します。
  - b. `java.security` を編集します。

- c. プロバイダーとその優先順位のリストに、1 番目のセキュリティー・プロバイダーとして `com.ibm.security.capi.IBMCAC` を追加します。例えば、AppScan Source for Analysis 使用のために `java.security` を編集している場合、変更対象箇所は以下のとおりです。

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.cert.IBMCertPath
security.provider.5=sun.security.provider.Sun
```

以下のように編集します。

```
security.provider.1=com.ibm.security.capi.IBMCAC
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.crypto.provider.IBMJCE
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=sun.security.provider.Sun
```

- d. `java.security` ファイルを保存して閉じます。
10. CAC 認証を使用して、AppScan Source 管理者として AppScan Source for Analysis または AppScan Source コマンド行インターフェース (CLI) にログインします。
  11. AppScan Enterprise Server ユーザーのデフォルト許可を組織のニーズに合うように変更します。

## 次のタスク

連邦情報処理標準 (FIPS) モードを実施したい場合は、証明書を SHA-1 に設定することはできません。SHA-2 証明書を使用し、`appscanserverdbmgr_cac_fips.bat` ツールを実行して FIPS モードを実施できます。その方法は *IBM Security AppScan Source* インストールと管理のガイド に説明されています。このガイドでは、Common Access Card (CAC) 認証が有効になっている AppScan Enterprise Server に AppScan Source データベース を登録するためのヘルプを見つけてください。

所有している Web 証明書の種類を判別するには、以下のようになります。

1. Windows 証明書マネージャーを開きます。Windows の「スタート」メニューの検索ボックスで `certmgr.msc` と入力し、Enter を押します。管理者パスワードまたは確認のプロンプトが表示されたら、パスワードまたは確認の入力をします。
2. ダブルクリックするか、ユーザー・インターフェースの「開く」アクションで証明書を開きます。
3. 証明書の「詳細」タブを選択します。
4. 「署名ハッシュ アルゴリズム」フィールドを見つけます。このフィールドの値が証明書のタイプを示しています。

---

## AppScan Source ユーザー・パスワードの変更

AppScan Sourceユーザー・パスワードを変更するには、「ユーザーの管理」権限が必要です。また、AppScan Source for Analysis で変更を行う必要があります。この権限がない場合は、代わりに管理者にこのトピックの説明に従ってパスワードを変更してもらってください。LDAP 認証または Windows 認証を使用するように AppScan Enterprise Server が構成されている場合、このトピックは適用されません。

### 手順

1. AppScan Source for Analysis で、メイン・ワークベンチ・メニューから「管理」 > 「ユーザーの管理」を選択します。
2. 「ユーザーの管理」ダイアログ・ボックスに、既存の AppScan Source ユーザーがリストされます。いずれかのユーザーのパスワードを変更するには、以下のいずれかのタスクを実行してユーザー情報を編集します。
  - ユーザーをダブルクリックします。
  - ユーザーを右クリックして、「ユーザーの編集」を選択します。
  - ユーザーを選択して、「ユーザーの編集」ボタンをクリックします。

注: AppScan Enterprise Server ユーザーのパスワードを AppScan Source から変更することはできません。

3. 「ユーザーの編集」ダイアログ・ボックスで、新規パスワードを入力してから、「パスワードの確認」フィールドにパスワードを再び入力します。
4. 「OK」をクリックして、パスワードを変更します。

---

## AppScan Enterprise Server の SSL 証明書

AppScan Enterprise Server をインストールしたら、有効な SSL 証明書を使用するように構成する必要があります。これを行わないと、AppScan Source for Analysis または AppScan Source コマンド行インターフェース (CLI) - あるいは Windows および Linux 上の AppScan Source for Development からサーバーにログインするとき、「信頼できない接続」というメッセージが表示されます。

### SSL 証明書の保管場所

永続的に受け入れられた証明書は、`<data_dir>%config%cacertspersonal` と `<data_dir>%config%cacertspersonal.pem` (`<data_dir>` は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。) に保管されます。証明書を永続的に保管する必要がなくなった場合は、これらの 2 つのファイルを削除してください。

### AppScan Source for Automation と SSL 証明書の検証

デフォルトでは、AppScan Source for Automation を使用すると、証明書が自動的に受け入れられます。この動作は、Automation Server 構成ファイル (`<data_dir>%config%ounceautod.ozsettings` (`<data_dir>` は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。)) の

ounceautod\_accept\_ssl 設定によって決まります。この設定を編集して value="true" を value="false" に設定すると、SSL 検証が試行され、無効な証明書が検出された場合は、AppScan Enterprise Console へのログインまたは公開が失敗します。

## **AppScan Source コマンド行インターフェース (CLI) と SSL 証明書の検証**

デフォルトでは、CLI login コマンドを使用すると、SSL 検証が試行され、無効な証明書が検出された場合 (別の AppScan Source クライアント製品でログインしたときに、証明書を永続的に受け入れていない場合) は AppScan Enterprise Console へのログインまたは公開がエラーとなって失敗します。この動作は、login コマンドの実行時にオプションの -acceptssl パラメーターを使用することにより変更できます。このパラメーターを使用すると、SSL 証明書が自動的に受け入れられます。



---

## 第 13 章 LDAP 統合

LDAP を介して認証される AppScan Source ユーザーを追加するには、LDAP リポジトリを使用するように AppScan Enterprise Server ユーザー・リポジトリを構成しておく必要があります。

LDAP リポジトリを使用するように AppScan Enterprise Server ユーザー・リポジトリを構成する方法については、「AppScan Enterprise 計画およびインストール・ガイド」または IBM Knowledge Center の AppScan Enterprise Server ユーザー・アシスタンス (<http://www.ibm.com/support/knowledgecenter/SSW2NF/welcome>) を参照してください。

LDAP 認証を使用していて、LDAP ユーザー・グループに属していない AppScan Source ユーザーを追加するときは、「ユーザーの追加」ダイアログ・ボックスで「**AppScan Source** リポジトリへのユーザーの保管」チェック・ボックスを選択することにより、ローカルの AppScan Source ユーザー・リポジトリにユーザーを作成します。作成手順については、130 ページの『AppScan Source ユーザーの作成』を参照してください。



---

## 第 14 章 AppScan Source に公開するためのアプリケーションおよびプロジェクトの登録

アプリケーション/プロジェクトの登録および評価結果の公開を行うことで、重要なセキュリティー・データをチーム内で共有できるようになります (評価は AppScan Source データベースに公開されます)。適切な特権および許可を持つユーザーは、AppScan Source for Analysis を使用して、これらの評価結果にアクセスできます。一部の実装環境では、アプリケーション/プロジェクトの登録および評価結果の公開は、管理者の責任で行うタスクです。その他の実装環境では、これらはプロジェクト・リーダー/セキュリティー・アナリストの責任で行うタスクです。これらのタスクを実施する必要がある担当者のみ限定して許可を与えることをお勧めします。



---

## 第 15 章 AppScan Source アプリケーションおよびプロジェクト・ファイル

AppScan Source のアプリケーションおよびプロジェクトには、スキャンおよびトリアージのカスタマイズに必要な構成情報を保守する対応ファイルがあります。プロジェクトをビルドするために必要な構成情報 (依存関係やコンパイラ・オプションなど) は、AppScan Source がプロジェクトを正常にスキャンするために必要な構成情報と非常に似ているため、これらのファイルはソース・コードと同じディレクトリーに配置することをお勧めします。ベスト・プラクティスとしては、これらのファイルをソース・コントロール・システムで管理する方法が挙げられます。

AppScan Source for Analysis で作成されたアプリケーションおよびプロジェクトには、それぞれ `.paf` および `.ppf` という拡張子が付けられます。これらのファイルは、AppScan Source for Analysis、AppScan Source for Automation、および AppScan Source コマンド行インターフェース でアプリケーションまたはプロジェクトを手動で作成および構成するときに生成されます。

Windows では、Visual Studio ソリューションとプロジェクトを AppScan Source for Analysis、AppScan Source for Automation、および AppScan Source コマンド行インターフェース にインポートすると、そのファイル (拡張子は `.sln.gaf` および `.vcproj.gpf`) が作成されます。

macOS では、Xcode ディレクトリーおよびプロジェクトをインポートすると、そのファイル (拡張子は `.xcodeproj.gaf` および `.xcodeproj.gpf`) が作成されます。同様に、Xcode ワークスペースをインポートすると、`.xcworkspace.gaf` 拡張子を持つファイルが作成されます。

注: Eclipse Importer を Eclipse または Rational Application Developer for WebSphere Software (RAD) ワークスペースで実行すると、AppScan Source は、`.ewf` および `.epf` という拡張子の中間ファイルを作成します。これらのファイルは、AppScan Source for Analysis への初回インポート時、および後でスキャンを実行するときに必要です。

重要: 開発環境内に依存関係を持つ AppScan Source プロジェクト (例えば、IBM MobileFirst Platform プロジェクト) を処理する場合は、必ず、プロジェクトをインポートする前に開発環境でビルドしてください。プロジェクトをインポートした後、その中のファイルを変更した場合は、AppScan Source でスキャンする前に開発環境で再ビルドしてください (そうしないと、ファイルに対する変更は AppScan Source によって無視されます)。

表 4. AppScan Source ファイル

AppScan Source ファイル拡張子	説明
ppf	<ul style="list-style-type: none"> <li>• AppScan Source プロジェクト・ファイル</li> <li>• AppScan Source for Analysis またはサポートされている AppScan Source ユーティリティでプロジェクトを作成するときに生成されます。</li> <li>• 名前はユーザー指定</li> </ul>
paf	<ul style="list-style-type: none"> <li>• AppScan Source アプリケーション・ファイル</li> <li>• AppScan Source for Analysis またはサポートされている AppScan Source ユーティリティでアプリケーションを作成するときに生成されます。</li> <li>• 名前はユーザー指定</li> </ul>
sln.gaf	<ul style="list-style-type: none"> <li>• Visual Studio ソリューションをインポートするときに生成される AppScan Source アプリケーション・ファイル</li> <li>• カスタム・アプリケーション情報 (除外設定やバンドルなど) を保持するために使用されます。</li> <li>• インポートするワークスペースまたはソリューションの名前が採用されます。例:  d:%my_apps%myapp.sln  d:%my_apps%myapp.sln.gaf</li> </ul>
vcproj.gpf	<ul style="list-style-type: none"> <li>• Visual Studio プロジェクトをインポートするときに生成される AppScan Source プロジェクト・ファイル</li> <li>• カスタム・プロジェクト情報 (パターンや除外設定など) を保持するために使用されます。</li> <li>• インポートするプロジェクトの名前が採用されます。例:  d:%my_projects%myproject.vcproj  d:%my_projects%myproject.vcproj.gpf</li> </ul>

表 4. AppScan Source ファイル (続き)

AppScan Source ファイル拡張子	説明
xcodeproj.gaf	<ul style="list-style-type: none"> <li>• Xcode ディレクトリーをインポートする場合に生成される AppScan Source アプリケーション・ファイル</li> <li>• カスタム・アプリケーション情報 (除外設定やバンドルなど) を保持するために使用されます。</li> <li>• インポートするワークスペースまたはソリューションの名前が採用されます。例: /Users/myUser/myProject.xcodeproj /Users/myUser/myProject.xcodeproj.gaf</li> </ul>
xcodeproj.gpf	<ul style="list-style-type: none"> <li>• Xcode プロジェクトをインポートする場合に生成される AppScan Source プロジェクト・ファイル</li> <li>• カスタム・プロジェクト情報 (パターンや除外設定など) を保持するために使用されます。</li> <li>• インポートするプロジェクトの名前が採用されます。例: /Users/myUser/myProject.xcodeproj /Users/myUser/myProject.xcodeproj.gpf</li> </ul>
xcworkspace.gaf	<ul style="list-style-type: none"> <li>• Xcode ワークスペースをインポートする場合に生成される AppScan Source アプリケーション・ファイル</li> <li>• カスタム・アプリケーション情報 (除外設定やバンドルなど) を保持するために使用されます。</li> <li>• インポートするワークスペースの名前が採用されます。例: /Users/myUser/myProj.xcworkspace.gaf</li> </ul>
ewf	<ul style="list-style-type: none"> <li>• Eclipse ワークスペース・ファイル</li> <li>• Eclipse ワークスペースを AppScan Source にインポートするときに生成されます。</li> <li>• Eclipse エクスポーターが Eclipse ワークスペース内の情報に基づいてファイルを作成し、AppScan Source がそのファイルをインポートします。</li> </ul>

表 4. AppScan Source ファイル (続き)

AppScan Source ファイル拡張子	説明
epf	<ul style="list-style-type: none"> <li>• Eclipse プロジェクト・ファイル</li> <li>• Eclipse プロジェクトを AppScan Source にインポートするときに生成されます。</li> <li>• Eclipse エクスポーターが Eclipse プロジェクト内の情報に基づいてファイルを作成し、AppScan Source がそのファイルをインポートします。</li> </ul>

ヒント: サポートされているビルド統合ツール (Ounce/Ant または Ounce/Maven など) を使用して AppScan Source アプリケーション・ファイルおよびプロジェクト・ファイルを作成する場合、これらを開発チーム間で共有できるように、ビルド自動化処理の一環としてソース・コントロール・システムでこれらのファイルを更新することをお勧めします。開発者が、ソース・コントロール・システムでファイルのローカル・ビューを更新すると、AppScan Source のアプリケーション・ファイルおよびプロジェクト・ファイルも更新されます。これにより、チーム全体が一貫性のあるファイル・セットを使用して作業できます。

注: AppScan Source for Analysis、AppScan Source for Automation、および AppScan Source コマンド行インターフェース でサポートされているインポート・ファイルのバージョンを確認するには、<http://www.ibm.com/support/docview.wss?uid=swg27027486>を参照してください。このページで、使用している AppScan Source のバージョンのタブを選択してから、使用している AppScan Source コンポーネントを選択します。AppScan Source が他の開発環境からのファイルのオープンおよびスキャンをサポートする場合、そのサポートは、「Supported Software」タブの「Compilers and Languages」セクションにリストされています。

---

## 第 16 章 ポート構成

AppScan Source 製品を導入するには、これらのコンポーネントがインストールされるコンピューター上で特定のポートが開かれている必要があります。『デフォルトのオープン・ポート』の表は、ポートの使用法に関する情報を示しています。各ポートを構成可能です。

---

### デフォルトのオープン・ポート

#### リモート通信用のデフォルトのオープン・ポート

ポート	コンポーネント	プロトコル
443 および 9443	AppScan Enterprise Server	HTTPS
2315	solidDB	solidDB

#### ローカル・ホスト・アクセス用のデフォルトのオープン・ポート

ポート	コンポーネント	プロトコル
443 および 9443	AppScan Enterprise Server	HTTPS
13194-13294 (この範囲内の 1 つのポートのみ使用)	AppScan Source for Analysis	IIOIP
13205	AppScan Source for Automation	IIOIP

#### ライセンス・サーバーのポート

AppScan Source に対するフローティング・ライセンスのサービス提供は、Rational License Key Server を使用して行われます。ファイアウォールを介して、または別のネットワークから AppScan Source フローティング・ライセンスを使用するには、多少の手動構成が必要です。Rational License Key Server 上で lmgrd および ibmratl ベンダー・デーモン用に License Manager ポートを構成し、次に、AppScan Source ポートに加えてこれらの両方のポートをオープン/転送する必要があります。詳しくは、Rational License Key Server の資料を参照してください。デフォルトでは、lmgrd ポートは 27000 に設定され、ibmratl ベンダー・デーモン・ポートは動的に割り振られます。

---

### ポート転送構成

ポート転送環境で作動させるには、AppScan Source システム・プロパティの構成を変更する必要があります。該当する設定の変更方法について詳しくは、IBM サポート担当員にお問い合わせください。

---

## solidDB ポートの変更

### このタスクについて

solidDB 通信ポート番号を変更するには、AppScan Source データベース をインストールしたマシンにアクセスし、このトピックの手順に従ってください。

**重要:** solidDB ポートを変更する場合は、appscanserverdbmgr ツールを実行して、更新後のデータベースの場所をサーバーに登録する必要があります。このツールについては、86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』を参照してください。

### 手順

1. `<install_dir>%solidDB%appscansrc%solid.ini` (Windows の場合) または `<install_dir>/soliddb/appscansrc/solid.ini` (Linux の場合) (`<install_dir>` は AppScan Source インストール済み環境がある場所です) を開きます。このファイルで、NETWORK NAME 設定を見つけてそのポート番号値を変更します。例えば、Windows 上にデータベースがインストールされていて、そのポート番号を 12345 に変更したい場合は、`Listen=tcPIP 2315, nmpipe SOLID ; Windows` (Windows 上の設定のデフォルト値) を見つけて、その値を `Listen=tcPIP 12345, nmpipe SOLID ; Windows` に変更します。ファイルへの変更内容を保存します。
2. `<data_dir>%config%database.ozsettings` (Windows の場合) または `<data_dir>/config/database.ozsettings` (Linux の場合) (`<data_dir>` は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。) を開きます。このファイルで、`db_connection_information` 設定を見つけてそのポート番号値を変更します。例えば、ポート番号を 12345 に変更する場合は、`value="tcp localhost 2315"` を見つけて、その値を `value="tcp localhost 12345"` に変更します。ファイルへの変更内容を保存します。
3. **IBM Security AppScan Source DB** サービスを再始動します。

---

## 第 17 章 インストール後の solidDB ユーザー・パスワードの変更

製品のインストール時に solidDB データベースをインストールする場合は、solidDB のユーザーおよび管理ユーザーの資格情報を構成する必要があります。デフォルトで、solidDB ユーザーの設定は、ユーザー名が **ounce**、パスワードが **ounce** です。デフォルトのデータベース管理者のユーザー名とパスワードはどちらも **dba** です。

### このタスクについて

これら 2 つのユーザー・アカウントのいずれかのパスワードを変更するには、このトピックで紹介している以下の手順に従います。

**重要:** solidDB ポートを変更する場合は、`appscanserverdbmgr` ツールを実行して、更新後のデータベースの場所をサーバーに登録する必要があります。このツールについては、86 ページの『AppScan Enterprise Server への AppScan Source データベースの登録』を参照してください。

### 手順

1. コマンド・プロンプトで、`<install_dir>%solidDB%bin (<install_dir> は AppScan Source インストール済み環境がある場所です)` にディレクトリーを移動します。
2. コマンド `solsql.exe "tcp 2315"` (Windows の場合) または `solsql "tcp 2315"` (Linux の場合) を発行します。
3. Username の入力を求めるプロンプトが出されたら、現在構成されている solidDB 管理ユーザー名を入力します。これは、デフォルトでは `dba` です。
4. Password の入力を求めるプロンプトが出されたら、現在構成されている solidDB 管理パスワードを入力します。これは、デフォルトでは `dba` です。
5. コマンド `alter user <db_username> identified by <new_password>;` を発行します。このコマンドの説明は以下のとおりです。
  - `<db_username>` は、パスワードを変更する solidDB ユーザーです。solidDB ユーザー・パスワードを変更することも、solidDB 管理ユーザー・パスワードを変更することもできます。
  - `<new_password>` は、`<db_username>` に対して設定する新しいパスワードです。

例えば、デフォルトの管理ユーザー・パスワードを `newpassword123` に変更する場合は、コマンド `alter user dba identified by newpassword123;` を発行します。

6. solidDB ユーザーのパスワード変更を完了させるために、コマンド `commit work;` を発行してから、コマンド `exit;` を発行します。
7. オプション: このステップは、solidDB ユーザー・パスワードを変更した場合のみ、実行する必要があります。solidDB 管理ユーザー・パスワードを変更す

る場合は、このステップは実行しないでください。 solidDB ユーザー・パスワードを変更したら、AppScan Source データベースに登録されているパスワードを変更する必要があります。

- a. コマンド・プロンプトを開き、ディレクトリーを `<install_dir>%bin` (`<install_dir>` は AppScan Source インストール済み環境がある場所です) に移動します。
- b. Windows の場合は、コマンド `0unceServer.exe -a <new_password>` を発行します。 Linux の場合は、コマンド `ounceserverd -a <new_password>` を発行します。 いずれの場合も、`<new_password>` は、上記の手順で solidDB ユーザー・パスワードを変更したときに指定した新しいパスワードです。

---

## 第 18 章 AppScan Source 事前定義フィルター (バージョン 8.7.x 以前)

このトピックでは、AppScan Source バージョン 8.7.x 以前に組み込まれていた事前定義フィルターをリストします。

以下のフィルターにアクセスする必要がある場合、161 ページの『第 19 章 アーカイブ済みの事前定義フィルターの復元』の説明に従ってください。

### ! - 厳選テスト

このフィルターは、最も危険な脆弱性カテゴリーの一部からの検出結果と一致します。外部ネットワーク通信ソースに起因する検出結果のみが含まれます。このフィルターは、高リスクの検出結果を得るための開始点を正確に示します。このフィルターに含まれる具体的なカテゴリーは、以下のとおりです。

```
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.PathTraversal
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.SQL
Vulnerability.Injection.OS
Vulnerability.Injection.XML
Vulnerability.Injection.XPath
```

### 高優先度 - 外部通信 (High Priority - External Communications)

このフィルターは、アプリケーション外部の、ネットワークから得られる検出結果を一致させます。このフィルターは、Technology.Communications ソースに起因する検出結果を一致させます。

### 高優先度 - 重要なタイプ (High Priority - Important Types)

このフィルターには、最も危険な脆弱性カテゴリー (例えば、CrossSiteScripting や Injection.SQL など) の一部からの検出結果が含まれます。このフィルターに含まれる具体的なカテゴリーは、以下のとおりです。

```
Vulnerability.AppDOS
Vulnerability.Authentication.Credentials.Unprotected
Vulnerability.Authentication.Entity
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.OS
Vulnerability.Injection.SQL
Vulnerability.Injection.XML
Vulnerability.Injection.XPath
Vulnerability.PathTraversal
```

## 低優先度 - テスト・コード (Low Priority - Test Code)

このフィルターには、テスト・コードからの検出結果が含まれます。このフィルターの具体的なタイプは、以下のとおりです。

Vulnerability.Quality.TestCode

## ノイズ - コピーに類似した操作 (Noise - Copy-like Operations)

このフィルターには、コピーに類似した操作に関連する検出結果が含まれます。データの取得元のソースが信頼できるかどうかにかかわらず、ソースから取得されたデータに対して実行されるアクションが信頼できる場合に、コピーに類似した操作が発生します。

以下のパターンが検索されます。

Technology.Database --> Vulnerability.Injection.SQL  
Mechanism.SessionManagement --> Mechanism.SessionManagement  
Technology.XML, Technology.XML.DOM, Technology.XML.Schema,  
Technology.XML.XPath --> Vulnerability.AppDOS.XML,  
Vulnerability.Injection.XML

## ノイズ - 問題のロギング (Noise - Logging Issues)

このフィルターには、エラー処理に関連した検出結果が含まれます。検出結果は、エラー処理ルーチンからロギング・メカニズムにまでわたります。以下のパターンが一致します。

Mechanism.ErrorHandling -->  
Vulnerability.Logging, Vulnerability.Logging.Forge, Vulnerability.Logging.Required

## ノイズ - 低重大度 (Noise - Low Severity)

このフィルターには、重大度が「低」の検出結果が含まれます。すべての分類が含まれます。

## ノイズ - 信頼できるソース (Noise - Trusted Source)

このフィルターには、信頼できるソースから得られる検出結果が含まれます。`java.lang.System.getProperty.*` をソースとする検出結果だけがこのフィルターに組み込まれます。

---

## 第 19 章 アーカイブ済みの事前定義フィルターの復元

このタスクの手順に従うと、バージョン 8.8 より前の AppScan Source で提供されていた事前定義フィルターを製品に再び追加することができます。それらの事前定義フィルターは、いったん 1 台のマシンに復元すると、ユーザーが作成するフィルターと同じ方法で管理することができます (例えば、フィルターを複数のクライアントで共有できます)。

### このタスクについて

アーカイブ済みの事前定義フィルターは、`<data_dir>%archive%filters` (`<data_dir>` は、ご使用の AppScan Source プログラム・データの場所です。詳しくは、69 ページの『インストールとユーザー・データ・ファイルの場所』を参照してください。) にあります。

### 手順

1. `<data_dir>%archive%filters` で、復元するフィルターを見つけます (AppScan Source フィルターには `.off` ファイル拡張子が付いています)。
2. フィルターを `<data_dir>%scanner_filters` にコピーします。
3. AppScan Source を再始動します。

### 次のタスク

フィルター (復元したアーカイブ済みフィルターを含む) の管理方法を確認するには、163 ページの『第 20 章 「フィルター・エディター」ビューでのフィルターの作成および管理』を参照してください。



---

## 第 20 章 「フィルター・エディター」ビューでのフィルターの作成および管理

このビューでは、フィルターの作成、編集、保存、削除、および管理を行えます。AppScan Source for Analysis を使用している場合、フィルターを共有して、他のユーザーによって共有されているフィルターにアクセスすることができます。AppScan Source for Development では、サーバー・モードを使用している AppScan Enterprise Server にログインしている場合、共有フィルターにアクセスできます。

### 手順

1. 165 ページの『第 21 章 「フィルター・エディター」ビュー』のツールバーで、「新規」をクリックします。新規フィルターにつく名前は Untitled<-number> (最初のタイトルのない新規フィルターは Untitled、次のタイトルのない新規フィルターは Untitled-1、以下同様) です。

注: AppScan Source for Development (Visual Studio プラグイン) では、このビューは「フィルターの編集」ウィンドウの一部です。

2. カテゴリーを展開し、必要なフィルター基準を選択します。
3. 「保存」または「名前を付けて保存」をクリックします。
4. フィルターに名前を付け、「OK」をクリックします。フィルターのリストで、Untitled<-number> が新規フィルター名に置き換えられます。

### 次のタスク

フィルターを適用するには、「フィルター・エディター」ビューのドロップダウン・メニューでフィルターを選択します。

注: 「脆弱性マトリックス」ビューの外部で適用されるフィルターは、「脆弱性マトリックス」ビューに作用しない可能性があります。フィルターが「脆弱性マトリックス」ビューに反映されるようにするには、「脆弱性マトリックス」ビューの「フィルターに掛けた検出結果の数を表示」ツールバー・ボタンを選択する必要があります。

フィルターは、リスト内でフィルターを選択してから操作することによって、「フィルター・エディター」ビュー内で直接管理できます。あるいは、「フィルターの管理」をクリックして「フィルターの管理」ダイアログ・ボックスを開くことができ、このダイアログ・ボックスに、保存されたフィルターのリストが表示されます。

- フィルターの変更: 「フィルター・エディター」ビューまたは「フィルターの管理」ダイアログ・ボックスでフィルターを選択し、そのフィルター・ルールを変更して、変更内容を保存します。

注: 標準装備フィルターは、変更も削除もできません。

- フィルターの削除: 「フィルター・エディター」ビューまたは「フィルターの管理」ダイアログ・ボックスでフィルターを選択し、「削除」をクリックします。「フィルターの管理」ダイアログ・ボックスで、複数のフィルターを選択し、「削除」をクリックしてそれらを一度に削除することができます。
- 別のフィルターからのフィルターの作成: フィルターを変更し、「名前を付けて保存」をクリックして、新しい名前のフィルターとして保存することができます。こうすることで、既存のフィルターの設定をベースとして新規フィルターを作成できます。この操作は、「フィルター・エディター」ビューおよび「フィルターの管理」ダイアログ・ボックスの両方で実行できます。

ヒント: フィルターを開き、「名前を付けて保存」アクションを使用して新規名で保存することでも、同じ内容を実行できます。これで、新規フィルターを開いて変更できます。この方法を選択すると、標準装備フィルターの 1 つから新規フィルターを作成できます。

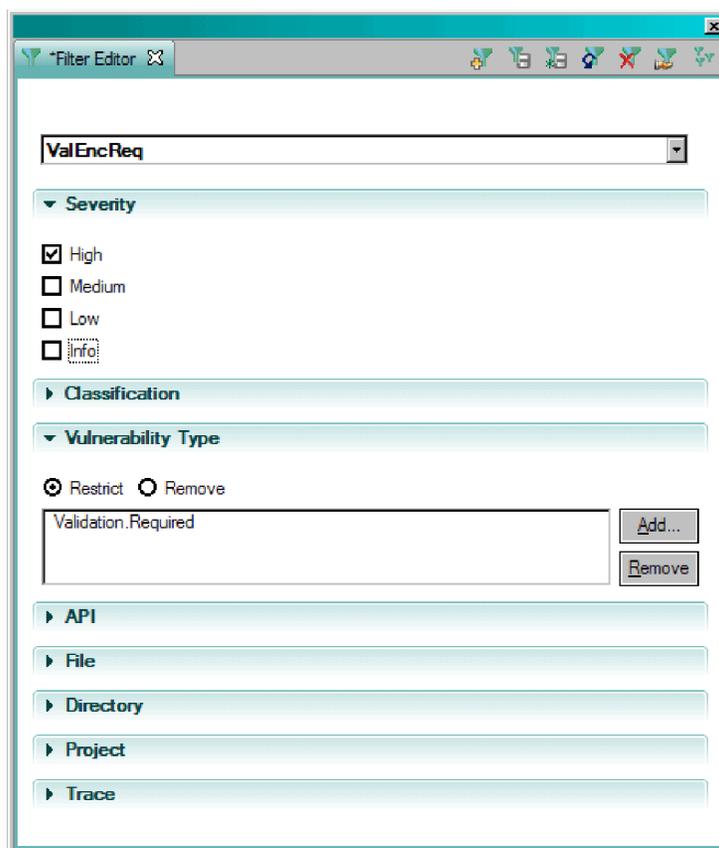
- フィルター設定の復帰: フィルターのプロパティを変更したが、それらの変更を元に戻したい場合は、「復帰」をクリックして、フィルターを最後に保存された設定に戻します。このアクションは、「フィルター・エディター」ビューおよび「フィルターの管理」ダイアログ・ボックスの両方で実行できます。ダイアログ・ボックスで、変更が保存されていないフィルターが複数ある場合、「復帰」をクリックすると、変更が保存されていないすべての選択されたフィルターが、保存された設定に戻されます。
- フィルターの共有 (AppScan Source for Analysis のみ): 共有フィルターを作成するには、フィルター・エディターでフィルターを開き、「フィルター・エディター」ビューのツールバーで「フィルターの共有」をクリックします。

注: 共有フィルターを変更、削除、または作成するには、「共有フィルターの管理」権限が必要です。権限の設定について詳しくは、「*IBM Security AppScan Source* インストールと管理のガイド」を参照してください。

## 第 21 章 「フィルター・エディター」ビュー

「フィルター・エディター」ビューでは、現在選択されているフィルターを、AppScan Source ビューよりもきめ細かく操作することができます。このビューは、フィルタリングが可能なすべての基準で構成されています。

注: AppScan Source for Development (Visual Studio プラグイン) では、このビューは「フィルターの編集」ウィンドウの一部です。



ヒント: 「フィルター・エディター」ビューの「トレース」セクションで、トレース項目の上にマウスを移動すると、項目に関する詳細が表示されます。



---

## 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510  
東京都中央区日本橋箱崎町19番21号  
日本アイ・ビー・エム株式会社  
法務・知的財産  
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。

国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については検証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラット

フォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年).このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. \_年を入れる\_ All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

## 商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、<http://www.ibm.com/legal/copytrade.shtml> をご覧ください。

Adobe、PostScript は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

IT Infrastructure Library は英国 Office of Government Commerce の一部である the Central Computer and Telecommunications Agency の登録商標です。

インテル、Intel、Intel ロゴ、Intel Inside、Intel Inside ロゴ、Intel Centrino、Intel Centrino ロゴ、Celeron、Intel Xeon、Intel SpeedStep、Itanium、および Pentium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

ITIL は英国 Office of Government Commerce の登録商標および共同体登録商標であって、米国特許商標庁にて登録されています。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Cell Broadband Engine は、Sony Computer Entertainment, Inc.の米国およびその他の国における商標であり、同社の許諾を受けて使用しています。

Linear Tape-Open、LTO、LTO ロゴ、Ultrium、および Ultrium ロゴは、HP、IBM Corp. および Quantum の米国およびその他の国における商標です。

# 索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

## [ア行]

アクティブ化 123  
アプリケーション (application)  
 定義 18  
アプリケーションおよびプロジェクトの登録 149  
アンインストール 127  
一般的なインストール・シナリオ 37  
 既存の AppScan Enterprise Server との統合 56  
 すべてのコンポーネントを 1 台のマシンにインストール 38  
 複数マシン環境での AppScan Source コンポーネントのインストール 46  
インストール  
 カスタム 107  
 既存の Oracle データベース 79  
 構成 129  
 サイレント 107, 115  
 データの場所 34, 69  
 変更 71  
 ファイルの場所 34, 69  
 AppScan Enterprise Server 72, 74  
 AppScan Source  
 フィックスパック 104  
 AppScan Source for Automation 101  
 AppScan Source for Development 94  
 AppScan Source for Development Plug-in for Eclipse 96  
 AppScan Source for Development Plug-in for Visual Studio 100  
 AppScan Source データベース 74  
 CAC の登録 88  
 register 86  
 AppScanSrc\_Installer.exe 67  
 Developer Plug-in 97, 99  
 Eclipse プラグイン 95, 99  
 Linux サーバー 109, 117  
 macOS 91  
 Microsoft Windows 69  
 setup.bin 67  
 setup.bin.gz 67  
 solidDB パスワードの変更 157  
 solidDB ポートの変更 156

インストール (続き)  
 Visual Studio Plug-in 100  
 インターネット・プロトコル・バージョン 6 27

## [カ行]

カスタム・インストール 107  
カスタム・インストール・ウィザード 107, 109, 115, 117  
共有フィルター 163  
権限 129, 130  
検出結果  
 分類 19  
コマンド行  
 カスタム・インストール 111, 119  
 ounceautod 101

## [サ行]

サイレント・インストール 107, 115  
システム要件 31  
新機能 2  
脆弱性 (vulnerability)  
 定義 18  
製品 1  
属性  
 定義 18

## [タ行]

デフォルトのインストール・ディレクトリ 34, 69  
デプロイメント 20, 112, 120  
 エンタープライズ・ワークグループ 25  
 小規模ワークグループ 23  
 標準デスクトップ 22

## [ナ行]

ナレッジベース・データベース 1

## [ハ行]

バンドル 18  
ビュー  
 フィルター・エディター 165  
評価 18  
フィルター  
 共有 163

フィルター (続き)  
 作成  
 「フィルター・エディター」ビューでの 163  
 事前定義アーカイブ 159  
 アクセス権限 161  
 フィルターの作成  
 フィルター・エディター 163  
 「フィルター・エディター」ビュー 165  
プロジェクト  
 定義 18  
分類  
 確定 19  
 スキャン範囲 19  
 要確認 19  
米国連邦情報・技術局 27  
ポート 155  
 デフォルト 155  
 転送 155

## [マ行]

マイグレーション 14

## [ヤ行]

ユーザー  
 監査 137  
ユーザーの管理 130  
 AppScan Enterprise Server ユーザーの自動ログイン 132  
 Automation Server ユーザー 136  
ユーザー名 130  
ユーザー・アカウント 129  
 Liberty のマイグレーション 131

## [ラ行]

連邦情報処理標準 27

## [ワ行]

ワークフロー 19

## A

AppScan Enterprise Server  
 パスワード変更 144  
 SSL 証明書 144

AppScan Enterprise Server Liberty での  
ローカル製品 ADMIN ユーザーの作成  
暗号化パスワード 135

AppScan Enterprise Server Liberty での  
ローカル製品管理者ユーザーの作成 133

LDAP 133

Windows 認証 134

AppScan Source

- アクセシビリティの問題 29
- 製品ファミリー 1

AppScan Enterprise Server へのログ  
イン 139

- パスワード変更 144
- CAC 142
- SSL 証明書 144

for Analysis 1

- 概念 18

for Automation 1

for Development 1

AppScan Source for Automation 101

- インストール 101
- 構文 (syntax) 104

AppScan Source for Development プラ  
グイン 96

AppScan Source solidDB 90, 91

AppScan Source インストール・ウィザ  
ード 67

AppScan Source 製品 1

AppScan Source セキュリティー・ナレ  
ッジ・データベース 1

AppScan Source データベースのバック  
アップ 90

AppScan Source データベースのリスト  
ア 91

AppScan Source ファイル

- epf 151
- ewf 151
- gaf 151
- gpf 151
- paf 151
- ppf 151

## F

FIPS 27

## I

IPv6 27

## J

JRE バージョン 1.5 の要件 95, 99

## L

LDAP 147

License Manager 123

ライセンス

インポート (import) 124

表示 125

フローティング 124

Linux

アンインストール 127

Eclipse プラグインのインストール 95,  
99

setup.sh 69, 96

Linux インストール

setup.bin.gz 67

## M

macOS

アンインストール 128

Microsoft Windows 31

アンインストール 127

## N

NIST 27

## O

OCI ライブラリー 84

Oracle 90

Oracle Client ライブラリー 84

ounceautod 101

Ounce/Ant 151

Ounce/Make 151

Ounce/Maven Plug-in 151

OUNCE\_CONFIG\_FILE 108, 111, 116,  
119

## P

password 130

## S

setup.sh 69, 96

## V

Visual Studio

サポート対象システム 100

Visual Studio のサポート対象システム  
100





Printed in Japan