IBM Security

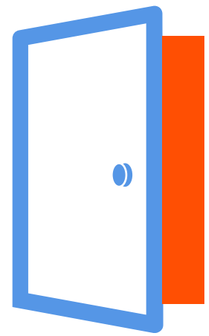
IBM

クラウド上のアプリケーション・セキュリティー・リスクを効果的に管理

シンプルな自動テストによるセキュリティー体制の合理化と強化

IBM Security ホワイト・ペーパー

なぜアプリケーション・セキュリティーが必要なのか



今までさまざまな策を講じてデータ・セキュリティーを奨励してきたと思いますが、実行中のアプリケーションが、ドアを開け放った会社の表玄関のような状態になっていませんか?組織が保有するデータのセキュリティーは、個々のファイルやレコードに鍵をかければいいというものではありません。アプリケーション レベルでもセキュリティー対策を厳重に講じる必要があります。というのは、アプリケーションはデータだけではなく、組織のモノのインターネット (IoT) インフラストラクチャーへのアクセスも制御できるからです。

多くの悪名高いセキュリティー侵害は、データ・セキュリティーの実践が不十分だったからではなく、脆弱性をはらんだアプリケーションが原因で起こっています。アプリケーション・セキュリティーを導入すれば、サイバー犯罪者が悪意ある不正なソフトウェアを使って、安全なはずのデータを吸い上げるという事態を防ぐことができます。

それでも、アプリケーション・セキュリティーはサイバーセキュリティーの中でも無視されがちな領域で、[1] セキュリティー侵害は終わりません。なぜでしょうか?一つには、アプリケーションのセキュリティーの厳格化は、ファイルの暗号化やファイアウォールによるネットワークの防御よりも複雑だという理由があります。アプリケーションの数と種類も増え、アプリ・ストア、クラウドベースのインフラストラクチャーにアクセスする専用アプリケーションも登場しました。その一方で、BYOD (個人所有機器の持ち込み可) ポリシーが広く採用された結果、十分に精査されていないアプリケーションが増え、アプリケーションに接続された IoT データ・ソースが急増しています。

アプリケーション・セキュリティーは、以下の対策を講じる上で極めて重要です。

- 評判を落とすことを防ぐ
- 顧客の信頼を維持する
- 修復コストを回避する
- ダメージが及ぶ前にセキュリティー・リスクを検知し対応する

ある調査によると、

77%

の開発者がアプリケーションを短期間でリリースしなければという圧力でがあり適切なテストをなかなか実施できないことが原因でアプリケーションに脆弱性があると回答しています。[2]

▸ デモをご覧になって、IBM Application Security on Cloud で達成できることをご確認ください。

1 “How to Make Application Security a Strategically Managed Discipline,” *Ponemon Institute*、2016 年 3 月

2 “The State of Mobile Application Insecurity,” *Ponemon Institute*、2015 年 2 月

アプリケーション・セキュリティーの実現に組織が手こずっている理由

アプリケーション・セキュリティーは、開発者、IT スタッフ、エンドユーザーなどに関わる要因で複雑化しています。さらにこれらに関係する要因が組み合わさって、組織は脆弱性の影響を受けやすくなることがあります。

リリースを急ぐ
「急いでリリース」するという空気が現場でまん延しているので、開発者がテスト要員不足に陥ることがよくあります。しかし、アプリケーション・セキュリティーは開発者だけが左右するわけではありません。ユーザーが新しいソフトウェアで達成できる効率性を早く実現したいと望んでいるため、アプリケーションのインストールも同様に大急ぎで行われます。

複雑なアプリケーション
ソフトウェアの範囲、データ要件、言語、プラットフォームは多種多様です。企業データに直結したアプリケーションが侵害されることは、同様のデータが保存されたノートパソコンを置き忘れることと同じくらい危険な事態になるおそれがあります。セキュリティー侵害に気付かなければ、ノートパソコンの紛失よりも悪いかもしれません。セキュリティーの脆弱性によって悪用が行われた場合でも、生活が脅かされるようになった場合でも、セキュリティーが万全ではないアプリケーションや悪意のあるアプリケーションによりデータが漏洩する可能性があります。

アプリケーション・セキュリティーの優先度が低い
アプリケーション層の脆弱性はほとんどの場合、優先度が低いと見なされ、組織は通常、アプリケーションの保護の重要性を認識していません。また、アプリケーションはそのセキュリティーの責任と共に組織全体に分散していることがほとんどで、どのアプリケーションが使われていて、どのアプリケーションが最も脆弱かがほとんど把握されていません。

基準の欠落
ユーザーはセキュリティー・テストに時間をかけることはできないし、効果的なテストの実施方法も知りません。あらゆる状況に対応できる万能なアプリケーション・セキュリティー基準はないため、ガイダンスとオンサイトの知識だけでは、評価や採用が困難な場合があります。

最近の Ponemon Institute の調査によると、回答者の

47%

が、組織内のモバイル・アプリケーションのリスクが増えている、または大幅に増えていると答えました。[1]

▸ 詳細情報: リスクベースのアプリケーション・セキュリティー管理

1 “How to Make Application Security a Strategically Managed Discipline,” *Ponemon Institute*、2016 年 3 月

効果的なアプリケーションのセキュリティーとは

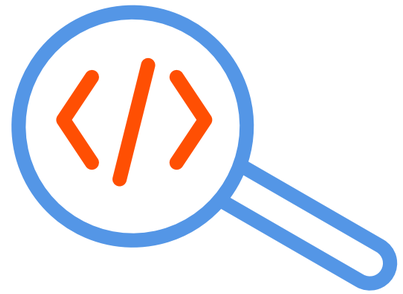
効果的なアプリケーション・セキュリティー・プラクティスからは、セキュリティーは、リストでチェックマークを付ける一連の項目ではなく、プロセスとして見るべきだということがわかります。つまり、アプリケーション・セキュリティー・テストは包括的かつ継続的に実施しなければなりません。

開発者の場合、アプリケーション・セキュリティーのテスト・プロセスは、ソース・コード分析を継続的に実施しながら、ソフトウェア開発ライフサイクルに組み込むべきです。エンドユーザー組織の場合は、導入した新しいソフトウェアをすべて検証し、すでに使用しているアプリケーションを再テストして、プロセスを継続させます。

包括的なアプリケーション・セキュリティーでは、以下の作業を実施します。

- **検出とカタログ化:** 現在使用中のアプリケーションを検出およびカタログ化
- **静的テスト:** アプリケーション・ソース・コードの脆弱性をスキャンすることは、特定のセキュリティー脆弱性の裏にある実際のコードを見つける最も直接的な方法
- **動的テスト:** 導入したときのソフトウェアの動作を評価 (たとえば、潜在的なクロスサイト・スクリプティング脆弱性と SQL インジェクション攻撃に対して脆弱かなど)
- **モバイル・アプリケーションのセキュリティー・テスト:** 市場で新しいモバイル・アプリケーションが非常に増えているため
- **導入:** 新しいアプリケーションは必ず検証してから導入

アプリケーションは定期的に再評価し、評価結果を Open Web Application Security Project (OWASP) Top Ten リストなどのソースに伝えるべきです。[1]新しい脅威によって、以前は安全だったアプリケーションがリスクにさらされる可能性があります。



2016 年 9 月時点で、

2 百万以上の

Apple iOS アプリケーションがダウンロード可能で、[2]

2.4 百万以上の

Google Android アプリケーションが存在します。[3]

▸ 詳細情報: リスクを防御するためのアプリケーション・セキュリティーの重要性

1 Paul Ionescu、"The 10 Most Common Application Attacks in Action," *IBM Security Intelligence*、2015 年 8 月 8 日

2 "Number of apps available in leading app stores as of June 2016," *Statista*、2016 年 6 月

3 "Number of Android Applications," *AppBrain*、2016 年 10 月 13日にアクセス

IBM の実績あるアプリケーション・セキュリティーのベスト・プラクティス

アプリケーションのセキュリティー・リスクを検証するに際し、組織は限りある予算、セキュリティーと IT スタッフへの重い負担がかかる状況など、さまざまな制約のもとで事業を運営しています。しかし、そのような制約でセキュリティー保護の向上が妨げられるようなことがあってはいけません。そうではなく、ベスト・プラクティスを採用するべきです。

- **監視:** 場当たり的なテストよりも、計画に沿った自動テストの方が綿密で信頼できる結果を出すことが可能
- **継続性:** アプリケーションはセキュリティーを組み込んでテストし、新たな脆弱性に対処するために再テストを実施することが必要
- **優先順位付け:** 重大度とビジネスへの潜在的影響に応じてアプリケーションのセキュリティー問題をランク付けすることで、最もビジネスの感覚に合った順序で問題解決に取り組むことが可能
- **柔軟性:** 組織で導入したアプリケーションをまんべんなく評価するには、制約のある実装要件を避けることが重要
- **適応性:** 脅威は時間と共に変化するので、柔軟なアプローチをとることで変更数を減らして、アプリケーション・セキュリティーの制御を維持
- **タイムリーな運用:** 開発プロセスの中断またはやり直しを避けるには、開発ライフサイクルの全段階においてアプリケーションをテストできる環境が必要

IBM® Application Security on Cloud などの統合アプリケーション・セキュリティー・ソリューションを使用すると、セキュリティー・ギャップを最小限に抑え、潜在的な脆弱性を特定できます。他のセキュリティー製品やプラクティスと統合すれば、包括的なセキュリティー・プログラムのアプリケーション部分のリスクを軽減でき、後手に回る事態を防げます。

58%

の組織が、セキュリティーの不安から、モバイル・セキュリティー戦略をフルに導入できないと言っています。[1]

▸ 参照先: IBM Application Security on Cloud による脆弱性の特定と修復

1 “2016 Mobile Security & Business Transformation Study,” *Information Security Media Group*、IBM Corp. 主催、2016 年

包括的なクラウドベースのアプリケーション・セキュリティー・テスト

個々のツールに頼るのではなく、統合ソリューションを実装して、アプリケーション・セキュリティーのリスク管理を支援しましょう。IBM Application Security on Cloud は Web およびモバイル・アプリケーション用の、コスト効率が高く、導入と操作が簡単なクラウドベースの包括的なソリューションで、アプリケーション・セキュリティー・テストの全段階を統合します。IBM のクラウドベース製品は、当社が長年培ってきたオンプレミス・セキュリティー・テストの専門知識をベースとし、他のセキュリティー・ツールと連携して包括的なサイバー防御を促進します。

IBM Application Security on Cloud はサブスクリプションベースの包括的なソリューションで、アプリケーションをテストし、実用的なデータを提供することでセキュリティー保護を改善できます。IBM Application Security on Cloud を使用すると、アプリケーション・リスク評価を素早く実施できるので、最も大きい脆弱性の修復に注力できます。

- クラウド上のアプリケーションである、IBM Application Security on Cloud の試用版を無料で使うことができます。または オンプレミス IBM Security AppScan® 試用版をダウンロードしてください。.

IBM Application Security on Cloud のダッシュボードの表示。

多数のプログラミング言語で開発されたアプリケーション・コードの静的セキュリティー・テストを実行し、実働前および実働中のソフトウェア Web アプリケーションを動的に分析し、Android アプリケーションと iOS アプリケーションを導入前にテストできます。IBM Application Security on Cloud はセキュリティーの問題を特定および報告し、それらを漏洩の危険度と重大度に応じてランク付けし、修復ステップを推奨します。結果はすべて多数の DevOps システムと統合開発環境 (IDE) に統合できます。

また、提携先の幅広いコンサルティング・サービスも利用できるので、セキュリティー・チームは IBM Security が提供可能なオファーをフルに活用できます。

IBM Application Security on Cloud を実際に使用したユースケース

IBM のアプリケーション・セキュリティー・ソリューションを導入している組織は、アプリケーションを開発・展開の際に、総合セキュリティー戦略の一部として統合と自動化の価値を実現しています。

ソフトウェア開発ライフサイクル全体を通じてコードを保護

- Concur Technologies of Bellevue (ワシントン州) は企業の経費管理を専門としているので、機密財務情報を日常的に管理しています。その情報を保護することは最重要事項ですが、簡単に達成できるものでもありません。自社製モバイル・アプリケーションなどを含む、モバイルを大規模に利用している組織であるConcur は、IBM Application Security on Cloud でクラウドサービスとして提供されているものと同じ脆弱性テスト・テクノロジーを搭載した AppScan を導入しました。AppScan により、Concur はアプリケーションを開発するごとにセキュリティー・リスクをテストし、便利な方法でコードを分析できます。

急成長中の企業におけるリスク軽減

- 国内外で急成長を遂げているトルコの大手小売業者、Migros は、保護を必要とする大規模なインフラストラクチャーを抱えており、約 1,500 店舗、10 万台のインターネット接続エンドポイント・デバイスを含むネットワーク経由でアプリケーションから在庫情報と決済情報を送信しています。自社の成長に伴い BYOD ポリシーを実施し、クラウドへの移行作業で課題に直面しました。しかしMigros は IBM アプリケーション・セキュリティー・ソリューションを利用することで、リスクを最小限に抑えながらビジネスを拡大できています。

IBM は、製造業 から金融業までさまざまな分野の大手企業で使われている[1]アプリケーション・セキュリティーテストツールの

包括的なポートフォリオ

を提供して[2]、アプリケーション、デバイス、データの保護を支援しています。

- サインアップ: IBM Application Security on Cloud の無料トライアルにお申し込みください。

1 “Large global automaker:Protecting the Connected Car Ecosystem,” *IBM Corp.*、2016 年 7 月.

2 “Progressive Insurance:Proactively Protecting Data by Creating Appropriate Controls,” *IBM Corp.*、2016 年 5 月

詳細情報

IBM Security ソリューションの詳細については、日本 IBM 営業担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。**ibm.com**/applicationsecurity

IBM Security ソリューションについて
IBM Security は、最先端の企業セキュリティー製品・サービスを包括的ポートフォリオにて提供します。世界中で高い評価を受けている IBM X-Force® 研究開発がサポートするこのポートフォリオは、ID とアクセス管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、ネットワーク・セキュリティーなどのソリューションを提供して、組織が人材、インフラストラクチャー、データおよびアプリケーションを包括的に保護するためのセキュリティー・インテリジェンスを提供します。これらのソリューションにより、組織はリスクを効果的に管理できると共に、モバイル、クラウド、ソーシャル・メディア、他企業のビジネス・アーキテクチャーに対応する統合セキュリティーを実装できます。IBM は世界で最も幅広くセキュリティーの研究、開発、提供組織を運営しており、130 か国で一日当たり 150 億ものセキュリティー・イベントを監視し、3,000 以上のセキュリティー特許を保持しています。

また、アプリケーション・セキュリティー・プログラムを構築、実行しながら、進化する組織のニーズに合わせて IBM Security Services を利用することもできます。IBM Security Services を利用することで、いつでもどこでも必要なときに、必要な期間、アプリケーション・セキュリティーの専門知識にアクセスできます。チームの作業を迅速化するために素早く契約を決める必要がある場合でも、綿密なコンサルティング・サービスが必要な場合でも、倫理的ハッカーにアプリケーションの手動調査を依頼したい場合でも、あるいはその中間にあるニーズでも、IBM が支援いたします。

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
October 2017

WGW03254-JPJA-02