サイバー犯罪の総合的防止: IBM Security Trusteer 製品の概要

包括的な IBM Security Trusteer ポートフォリオを使用することで、あらゆる種類の攻撃ベクトルを検知して防止

ハイライト

- **従来のソリューションだけでは阻止できないサイバー犯罪攻撃を防止**
- **包括的な統合サイバー犯罪防止アーキテクチャーを使用することで、不正をリアルタイムに検出**
- **4 つの基本原理を活用 - 不正を効果的かつ正確に阻止、新出の脅威に適応、エンドユーザー・エクスペリエンスを合理化、および価値創出までの期間を短縮**

サイバー犯罪者は常に、金融機関、企業、e-コマース業、その他の組織を狙って、金融情報や業務情報を盗もうとしています。従来のソリューションは、脅威に関する情報に欠けており、全体的な攻撃ライフサイクルをほぼリアルタイムで識別することができないため、こうした攻撃を阻止するのは困難です。

IBM は、包括的な統合サイバー犯罪防止アーキテクチャーをいち早く開発し、世界中の何百もの組織がその導入を成功させてきました。Trusteer ソリューションは、オンライン、モバイル、チャネル間の詐欺の大半を占める、犯罪者によるエンドユーザーとアカウントの乗っ取りなど、幅広い種類の攻撃を検出、予防します。IBM のサイバー犯罪防止アーキテクチャーは、不正の防止、長期に亘る保護の持続、顧客体験の合理化、IT リソースの負担の大幅な軽減という 4 つの基本原理に基づいています:

不正を効果的かつ的確に予防
- ほとんどの不正企ての根本的原因であるマルウェアとフィッシングを予防
- アクティブな脅威をほぼリアルタイムに検出
- デバイス、ユーザー、アカウント、トランザクションに関わるリスク要因を分析して、アカウントを乗っ取ろうとする試みや高リスクのトランザクションに確実にフラグを設定

新しい脅威に適応
- 数千万ものエンドポイントからグローバルな情報をほぼリアルタイムで利用
- 様々な保護層を動的に適応させて、持続可能な保護を実現

エンドユーザー・エクスペリエンスを簡素化
- 透過的な保護を実現
- 合法的取引を行っている顧客が被る障害を大幅に軽減
- 組織のサポート、詐欺・リスク対策チームの効果をアップ

価値創出までの期間を迅速化

- 面倒な設定が不要なサービス型ソフトウェア (SaaS) ソリューションにより、迅速な導入を実現
- すべてのオンライン/モバイル・アプリケーションに即時に対応

IBM Security Trusteer 製品の概要と主な機能

製品	概要	主な機能
IBM® Security Trusteer Pinpoint Criminal Detection	犯罪者や、アカウント乗っ取りの企てを確実に検出	• 複合的なデバイス ID を使って、新しいなりすまし (プロキシ) の既知の犯罪デバイスを検出 • フィッシング・インシデントをほぼリアルタイムに特定 • Trusteer Pinpoint Malware Detection および Trusteer Rapport (利用している場合) の拡張マルウェアとフィッシングのリスク・インジケーターをスムースに統合 • デバイス・リスク (なりすまされた既知の犯罪デバイス) とアカウント・リスク (フィッシング・インシデントとマルウェア感染) を相互に関連付けて、犯罪とアカウント乗っ取りを確実に検出 • 世界中の数百もの組織からの情報をもとに、グローバルな犯罪デバイス・データベースを維持
IBM® Security Trusteer Pinpoint Malware Detection	活動中の MITB (Man-In-The-Browser) マルウェアに感染したデバイスを正確に、ほぼリアルタイムに検出	• PC、Mac、モバイル・デバイスで活動中の MITB 感染を検出 • マルウェア検出イベントを電子メール、バッチ・ファイル、または直接フィードによって、Trusteer Pinpoint Criminal Detection とサードパーティ製リスク・エンジンにフィード
IBM® Security Trusteer Mobile Risk Engine	感染したエンドユーザー・デバイスや犯罪者所有のデバイスから、モバイル固有の不正リスクを確実に検出	• スマートフォンやタブレットからの高リスク・モバイル・アクセスを検出 • Trusteer Mobile SDK、Trusteer Mobile App、およびサードパーティ製アプリケーションが捕捉したデバイス、セッション、およびユーザーのリスク要因に基づいてリスク分析を実行 • オンライン・チャネルのマルウェア感染やフィッシング・インシデントなど、チャネルにまたがるリスク要素を相互に関連付けて、複雑なオンライン/モバイル攻撃シナリオに対処
IBM® Security Trusteer Rapport	金融関係を標的としたマルウェアやフィッシング攻撃に対するクライアントベースのエンドポイント保護	• 活動中および休止状態の MITB マルウェアによる感染からデバイスを予防し、感染した場合は感染源を削除 • アクティブなマルウェアが存在する場合でも、セッションの閲覧を保護 • フィッシング・サイト、特定の感染アカウントの資格情報、支払いカード・データを検出 • 詐欺対策チームにマルウェア感染と削除を通知することで、ユーザーに資格情報を再び付与できるようにして、将来の脅威を排除
IBM® Security Trusteer Mobile SDK	Apple iOS プラットフォームと Google Android プラットフォーム専用セキュリティー・ライブラリーは、専用のモバイル・バンキング・アプリケーションに組み込んで、感染デバイスや脆弱なデバイスを検出して、永続的デバイス ID を生成することが可能	• 次のリスク要因を検出: – 改造/ルート化デバイス – マルウェア感染 – 不正アプリケーションのインストール – セキュリティー保護されていない WiFi 接続 – 古いオペレーティング・システム – 地理的場所 • ハードウェアとソフトウェアの属性を基に、アプリケーションの再インストールに強い永続的デバイス ID を生成
IBM® Security Trusteer Mobile Browser	モバイル・デバイスのアクセスとトランザクションのリスクベース分析	• Trusteer Mobile SDK を組み込むことで、デバイス・リスク要因と永続的デバイス ID を Web アプリケーションに提供 • 介在者攻撃を防止 (ユーザーが本当のサイトを閲覧できるように支援) • デバイス・リスク要因をユーザーにアラート通知し、改善ガイダンスを提供
IBM® Security Trusteer Apex Advanced Malware Protection	従業員のエンドポイントを高度なマルウェアから保護	• Web ブラウザー、Java、Adobe、Microsoft Office、その他のアプリケーションをゼロデイ脆弱から保護 • マルウェアによるデータの引き出しを阻止 • 消費者サイトでのスピア・フィッシングやエンタープライズ資格情報の再使用によって資格情報が盗まれるのを阻止 • 管理対象/管理対象外の従業員のエンドポイントをサポート

IBM Security Trusteer 製品の概要: データ・フロー

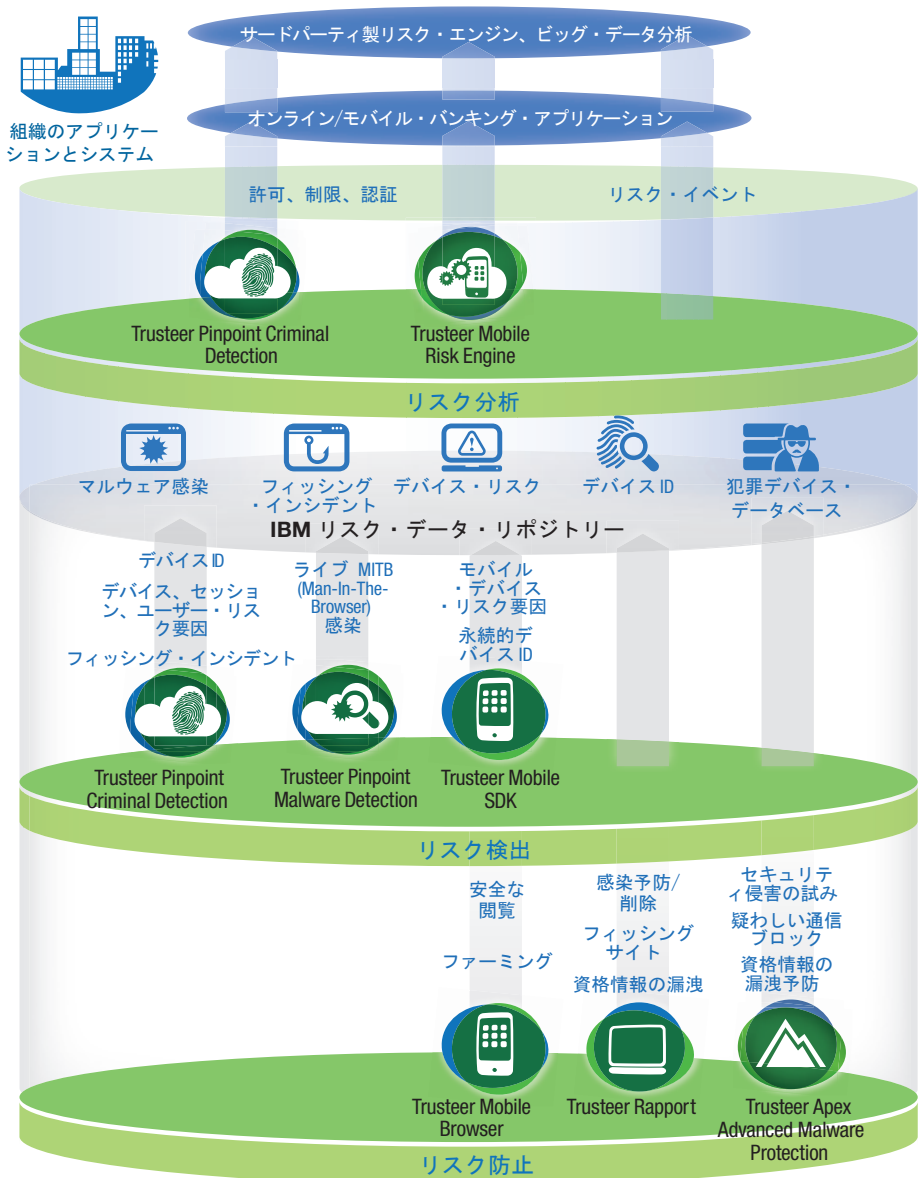

図 1: セキュリティー・アーキテクチャーへの包括的な Trusteer アプローチによって、IBM Security Trusteer 製品間でデータと情報をやり取りすることが可能

IBM 製品が選ばれる理由?

IBM Security ソリューションは、その不正防止機能、ID とアクセス管理機能で世界中の組織の信頼を得ています。これら実証済みのテクノロジーにより、組織は顧客、従業員、ビジネスに不可欠なリソースを最新のセキュリティー脅威から保護できます。新しい脅威が現れる状況の中、IBM は製品、サービス、ビジネス・パートナー・ソリューションなどの包括的なポートフォリオを提供して、組織が中核的なセキュリティー・インフラストラクチャーを構築するため支援します。IBM は、セキュリティーの脆弱性を軽減して、戦略的イニシアチブの成功に力を注げるよう、組織を強化します。

詳細情報

IBM Security Trusteer 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**/security

IBM Security ソリューションについて

IBM Security は、企業セキュリティー製品とサービスの最先端且つ包括的ポートフォリオを提供します。世界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、IBM グローバル・ファイナンシングは、ビジネスで必要とされるソフトウェア機能を、可能な限り費用対効果が高く戦略的に優れた方法でご購入いただけるようお客様を支援します。IBM は、信用審査で承認されたお客様とパートナーシップを結んで、お客様のビジネスや開発目標に見合ったファイナンシング・ソリューションをカスタマイズし、効果的な現金管理を実現し、所有総コストを改善します。お客様の主要な IT 投資にはIBM グローバル・ファイナンシングをご利用になり、ビジネスを一層推進してください。詳細については、次の URL にアクセスしてください: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

2014年8月

Trusteer は、2013 年 8 月に IBM によって買収されました。

リサイクルにご協力ください