IBM Security

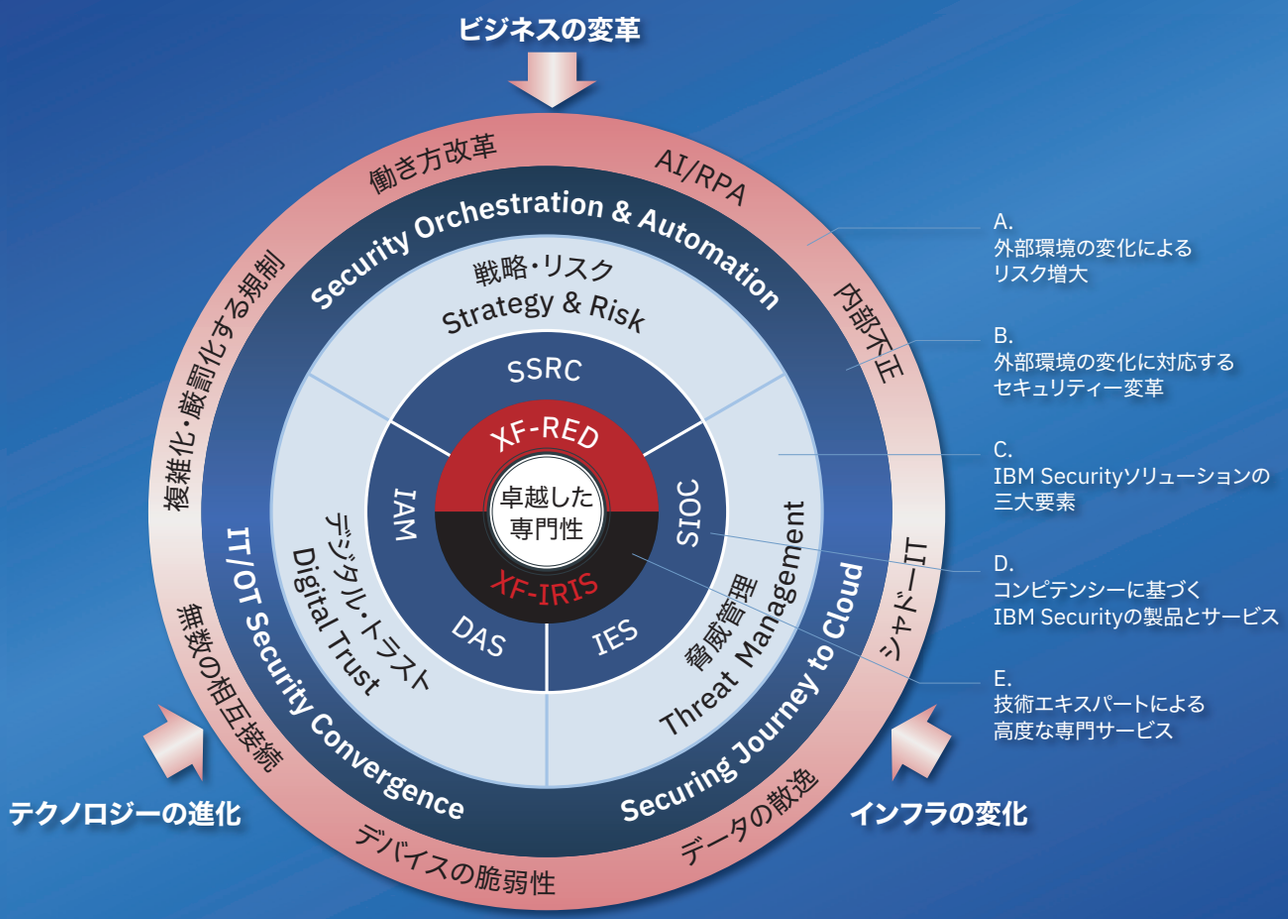
IBMセキュリティー・ソリューション
総合カタログ

IBM Securityミッション・ステートメント

We exist to protect the world, freeing you to thrive in the face of cyber uncertainty

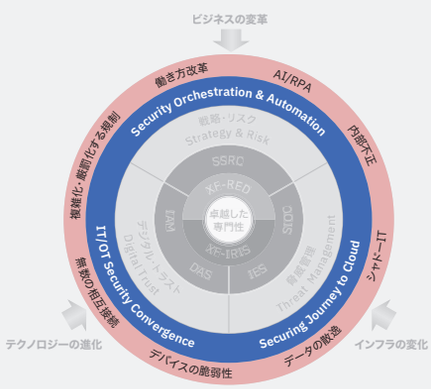
不確実なサイバー空間からお客様を保護し、ビジネスの健全な発展を支援するために

クラウド、AI、IoT、ブロックチェーンなど、テクノロジーの進化に伴い複雑で多様化するビジネスの基盤となるIT/OT環境および、それを取り巻くサイバー空間におけるリスクは深刻化しています。IBM Securityは、お客様をセキュリティー脅威から保護し、ビジネスの健全な発展と組織の持続的な運営をサポートするため、高い専門性と信頼性に基づくソリューションの提供、コンサルティング、技術的アドバイス、システム構築、運用監視などの豊富で網羅的な製品とサービスを、世界中に配置されたセキュリティー・エキスパートとともに、卓越した専門性をもってご提供します。



サイバー・トランスフォーメーション／Cyber Transformation

ビジネスの発展には革新的なテクノロジーの活用によるデジタル・トランスフォーメーションが不可欠な時代となり、それに伴って必要となる多様で柔軟なシステム、ネットワーク、アプリケーションといったインフラとそれらを運用する組織もまた、常に変化するサイバーリスクと向き合い、適切にマネジメントするための永続的な仕組みを構築することが求められます。



IBM Securityによる支援

オーケストレーションと自動化
Security Orchestration & Automation

サイロ化された単一ソリューションの集まりではなく、対策を有機的に組み合わせて効果を最大化するためのアーキテクチャー設計や、全体最適による効率化を実現するソリューションを提供します。

セキュアなクラウド導入
Securing Journey to Cloud

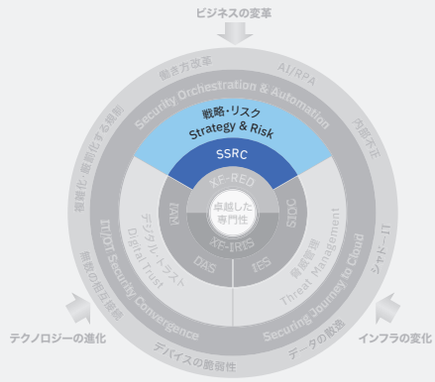
お客様が安心して安全なクラウドの導入を実現するため、計画から導入・移行、さらに運用までの各フェーズにおいて必要となる各種サービス・製品とコンサルテーションを提供します。

IT/OTの統合的なセキュリティー強化
IT/OT Security Convergence

ITのみならず、OT（制御系システム）を対象としたセキュリティー対策を強化するためのアセスメントやツールの提供、ITとOTのセキュリティーを一体となって推進するためのコンサルテーションを提供します。

戦略・リスク／Strategy & Risk

組織の経営者は、ビジネスを継続的に発展させるうえで、戦略的に経営資源を投入し、適切にリスクをマネジメントしなければなりません。さらに、ビジネスを展開する業界や当局による規制、株主や顧客、ビジネスパートナーといったさまざまなステークホルダーからの要請など、多種多様なコンプライアンス要件を満たすことも求められます。



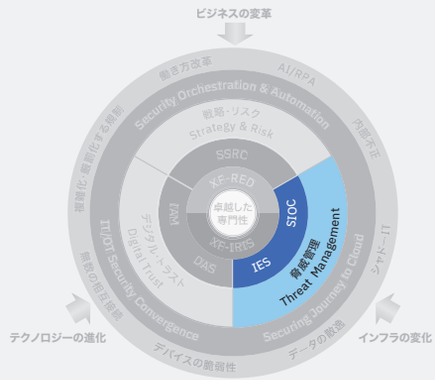
IBM Securityによる支援

セキュリティー戦略とリスクマネジメント
Security Strategy, Risk, and Compliance (SSRC)

IBMの経験豊富な専門家の知見と独自のノウハウにより、お客様のビジネス環境に即したセキュリティー要件を抽出し、最適な投資によりセキュリティー水準を向上するとともに、グローバルな組織を統制するためのコンサルテーションを提供します。

脅威管理／Threat Management

テクノロジーの進化はサイバー攻撃の大規模化、巧妙化という一面を生み出し、旧来的な対策を無力化しつつあります。セキュリティー担当者は日常的に発生する膨大なセキュリティー・イベントの対応に追われ、多くの組織が人材不足に悩まされているなか、セキュリティー脅威を迅速かつ的確に検知し、インシデントの発生や被害を極小化する取り組みが必要です。



IBM Securityによる支援

セキュリティー・オペレーションと監視
Security Intelligence and Operations Consulting (SIOC)

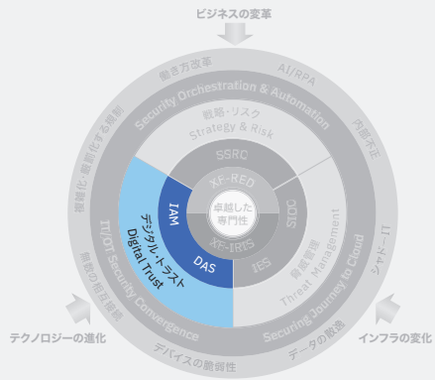
セキュリティー監視センター（SOC）の構築と運用支援、マネージド・セキュリティー・サービス（MSS）による攻撃の検知、インテリジェンス情報の活用、運用プロセスの自動化などを通じて、組織のセキュリティー脅威を可視化し、セキュリティー・オペレーション全般の高度化を支援します。

インフラとエンドポイント保護
Infrastructure and Endpoint Security (IES)

ネットワークとエンドポイントから構成されるインフラ全般のセキュリティーを強化するためのアーキテクチャー設計や各種セキュリティー・ソリューションの導入、セキュリティー・デバイスの運用監視サービスを提供します。

デジタル・トラスト／Digital Trust

デジタル・トランスフォーメーションにより、ビジネスにおけるテクノロジーと人びとの関わり合いには変化が起きています。イノベーションを実現し、健全にビジネスを発展させるためには、この新たな環境におけるリスクを理解し、特にプライバシーや知的財産などのデータとそれを扱うアプリケーションをセキュリティー脅威から保護しなければなりません。さらに、クラウドやモバイル環境の導入が進むにつれ、組織のネットワーク境界は曖昧になり、データやアプリケーションにアクセスするユーザー・アイデンティティーの識別とアクセス制御の重要性が増しています。



IBM Securityによる支援

データ保護と脆弱性管理
Data and Application Security (DAS)

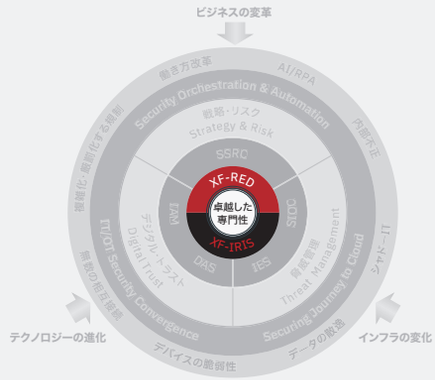
ビジネス・クリティカルなデータやセンシティブなデータを判別し、保護するためのツールやソリューションの提供、実装支援、コンサルテーションや、アプリケーションの脆弱性を適切に管理し、内外の脅威から保護するためのツールとサービスを提供します。

ID管理とアクセス制御
Identity and Access Management (IAM)

オンプレミス、クラウド、モバイルなどの多様なプラットフォームとさまざまなアプリケーションが混在し、組織内外のあらゆる経路からアクセスが生じるインフラとシステムを保護するための統合ID管理システム、認証とアクセス制御基盤となるソリューション、それらを適切に実装し、運用するためのコンサルテーションを提供します。

卓越した専門性／X-Force

興味本位やいたずら目的での不正アクセスが主流であった時代とは異なり、現代のサイバー攻撃は、相応の訓練により養成されたハッカーで構成された犯罪集団による巧妙かつ執拗なものや、国家的な支援を受けた大規模なものなど、容易に太刀打ちできる性質ではなくなってきています。こうした深刻な脅威から組織を守るためには、十分な知識と経験を有する熟練した専門家によるサポートを受けることが強く推奨されます。



IBM Securityによる支援

インシデント・レスポンス
X-Force Incident Response and Intelligence Service (XF-IRIS)

熟練したセキュリティー専門家によるインシデント対応のための準備や計画の支援、インシデント発生時の初動対応から収束までの一連のマネジメント、フォレンジック解析、実践的な訓練などを提供します。

ペネトレーション・テスト
X-Force Red (XF-RED)

業界有数の経験と技術を有するホワイトハッカーによる、確立された方法論に基づく擬似的な侵入によるセキュリティー診断（ペネトレーション・テスト）、実際の攻撃を想定したシミュレーション（REDTeaming）、ITだけでなくIoTデバイスやモバイル端末、ATMに対するセキュリティー試験などを提供します。

INDEX

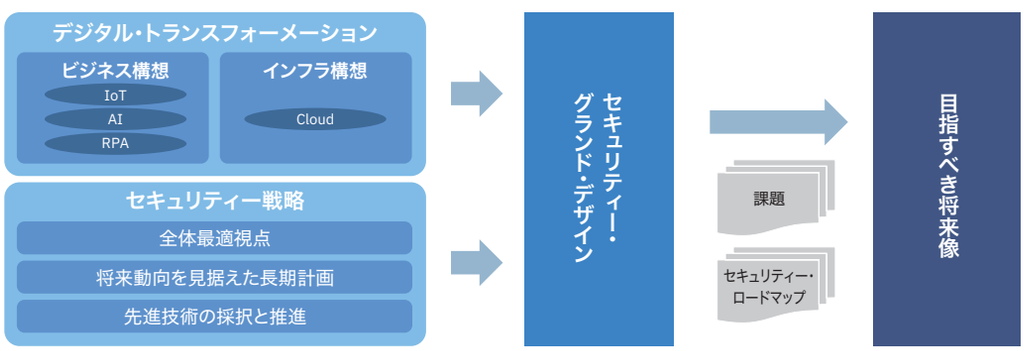
サイバー・トランスフォーメーション / Cyber Transformation

セキュリティー・グランド・デザイン策定支援サービス

セキュリティー・グランド・デザイン策定支援サービスは、IT環境の変化や高度化・複雑化するサイバー攻撃、セキュリティー脅威への対応について、部分最適ではなく、全体像と今後の見通しを踏まえた全体最適の視点で、戦略的かつ効率的なセキュリティー対策策定の実現を支援するサービスです。

お客様の課題／要望

- 個別対策によるサイロ化を改善するための全体最適視点の欠如
- サイバー攻撃の高度化・複雑化に対応するための長期計画不在
- セキュリティー対策の統合化や自動化に向けた先進的アプローチの推進

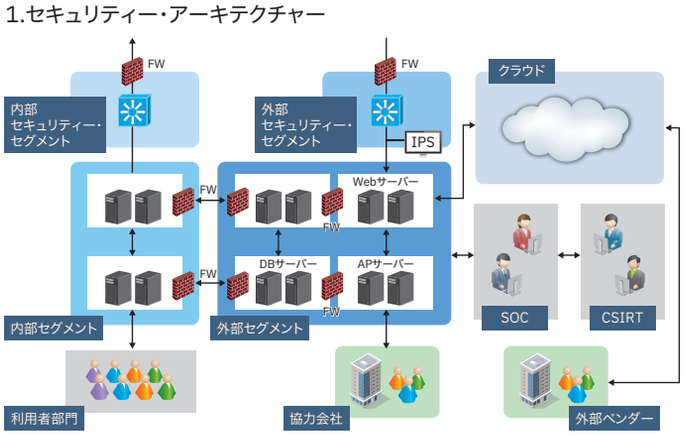


IBMがご提供する価値

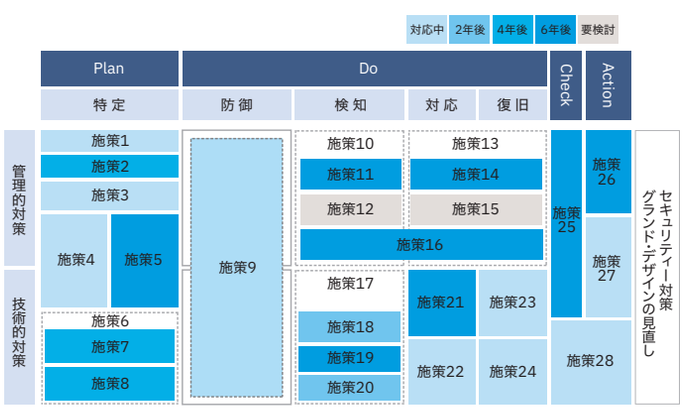
- 全体最適の視点から本来あるべき姿を構想したセキュリティー・グランド・デザインの策定
- 個別のセキュリティー対策の優先順位付けおよび重点施策の特定など、効率的かつ効果的なセキュリティー対策方針の策定
- セキュリティー・グランド・デザインにおける各施策を実施するための時系列でのロードマップ策定

■ アウトプット（例）

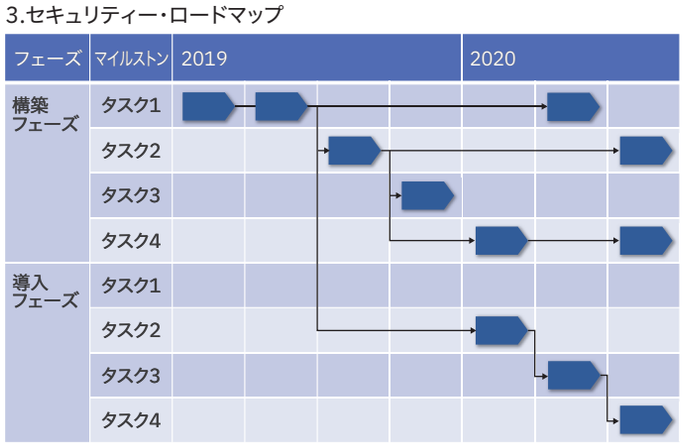
1.セキュリティー・アーキテクチャー



2.セキュリティー鳥瞰図



3.セキュリティー・ロードマップ



1. セキュリティー・アーキテクチャー

セキュリティー・グランド・デザインに基づく将来目標とするアーキテクチャーの全体像を図や絵で可視化します。

2. セキュリティー鳥瞰図

セキュリティー・グランド・デザインを重点施策単位で切り出し、全体を鳥瞰的に示します。

3. セキュリティー・ロードマップ

セキュリティー・グランド・デザインを構成する重点施策とそれぞれの関連性に基づき、ロードマップを策定します。

サイバー・トランスフォーメーション / Cyber Transformation

クラウド・セキュリティー アセスメント・サービス

IBMでは、グローバルにおけるクラウド提供事業者の実績から独自のクラウド・セキュリティー・フレームワークを開発しており、お客様のクラウド・セキュリティー対策の現状を評価して、改善案を提言することが可能です。お客様が使用または使用を検討されている複数のクラウドに対し、アセスメントを実施し、ロードマップ策定を支援します。

お客様の課題／要望

- 複数のクラウドを使用しているまたは検討しているが、一度クラウド固有のリスクに対して現状評価を行いたい
- クラウド・サービス・プロバイダーのセキュリティー状況を把握し、また、セキュリティーにおける責任範囲を明確化したい
- 複数のクラウドに対し横断的にセキュリティーを強化しつつ効率化も図りたい

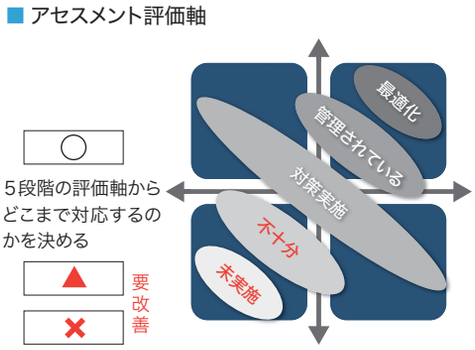
IBMのご提供する価値

- IBMがグローバルにおけるシステム設計・開発・運用を基に培ったクラウド・セキュリティー・フレームワークによりセキュリティー対策項目ごとに評価
- 課題点に対して、改善案と優先的に対応すべき項目の明確化
- アセスメント結果に基づくセキュリティー戦略、ロードマップ(計画)の策定

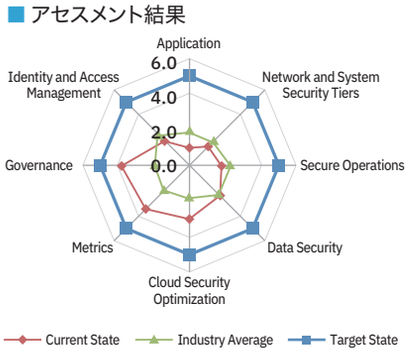
■ アセスメントのフレームワーク

セキュリティー対策項目	チェック項目
ID・アクセス管理	認証とアクセス管理
	ユーザーの認可
データ保護	シャドウ・データの有無
	暗号化
	個人情報保護
ネットワークとシステム・セキュリティー	セキュリティー・ポリシー
	ネットワーク監視
	セキュリティー脅威からの保護
アプリケーション	アプリケーション開発のセキュリティー
	脆弱性診断

■ アセスメント評価軸



■ アセスメント結果



マルチクラウド・セキュリティー戦略(ガイドライン・規定文書)

クラウドおよび情報セキュリティーの豊富な知識を持つ専門家が短期間かつ効果的にクラウド・セキュリティー強化を支援します。クラウド・セキュリティーの国際基準に基づいて現状評価を実施し、お客様が使用または使用を検討されている複数のクラウドに対し、セキュリティー計画の整備、責任範囲の明確化、ガイドラインの策定などを支援します。

お客様の課題／要望

- 社内でクラウドを利用しており、ガバナンス強化のためにクラウド利用ガイドラインなどの文書体系を整備したい
- クラウド・サービス・プロバイダーのセキュリティー状況を把握し、また、セキュリティーにおける責任範囲を明確化したい
- 国際標準やベスト・プラクティスに準拠したクラウド利用ガイドラインを作成したい

IBMのご提供する価値

- クラウド・セキュリティーの国際標準(ISO27017、NIST、CSAなど)およびベスト・プラクティスを参考とした戦略や計画作成
- クラウドの利用モデルの把握とガイドライン整備、責任範囲の明確化
- 国際標準化ガイドに基づくクラウド・セキュリティーの要件の定義

■ クラウド形態ごとのクラウド業者とご利用者間の責任範囲

	OnPremise	IaaS	PaaS	SaaS
技術的セキュリティー	データ	データ	データ	データ
	アプリケーション	アプリケーション	アプリケーション	アプリケーション
	データベース	データベース	データベース	データベース
	実行環境	実行環境	実行環境	実行環境
	ミドルウェア	ミドルウェア	ミドルウェア	ミドルウェア
	OS	OS	OS	OS
	仮想化基盤	仮想化基盤	仮想化基盤	仮想化基盤
	サーバー	サーバー	サーバー	サーバー
	ストレージ	ストレージ	ストレージ	ストレージ
	ネットワーク	ネットワーク	ネットワーク	ネットワーク
技術以外のセキュリティー	プロセス(規程類等)			
	組織・人(利用者、クラウド・プロバイダー等)			

クラウド事業者責任範囲

クラウド利用会社責任範囲

■ クラウド戦略策定におけるアプローチ(例)

ステップ	1. 現状把握とスコープ検討	2. 方針/モデルの策定	3. セキュリティー要件定義/文書策定
	• クラウド・リスク・アセスメントの実施(クラウド利用状況やクラウド・ベンダーのセキュリティー実装状況等の把握) • 対象クラウドの検討	• 利用モデルの策定(クラウド形態) • クラウド規程の文書体系の決定 • 責任範囲の明確化	• ISO27017などの標準化ガイドを利用してクラウド・セキュリティーの要件の洗い出し • 規程文書類の作成

CASB (Cloud Access Security Broker) 導入支援サービス

クラウド・サービス（Shadow IT/Sanctioned IT）を利用するユーザーに対してさまざまなセキュリティー機能を提供します。IBMはユーザーと複数のクラウド・プロバイダーの間に設けた単一のコントロール・ポイントでクラウド利用の可視化や制御を行うための一貫性のあるポリシーの適用を支援します。

お客様の課題／要望

- 無認可のクラウド・サービスの使用状況を調査し潜在的なリスクを確認したい
- クラウド内の企業情報を保護したい
- 効果的なクラウド・セキュリティー・ポリシーの策定とCASB導入を同時に実施したい

IBMのご提供する価値

- マルチクラウド環境において単一コントロール・ポイントで統制強化
- エージェントレスでDLP/脅威防止/アクセス制御/構造化データ暗号化によるセキュリティー水準向上
- 効果的なクラウド・セキュリティー・ポリシーの策定

ご参考 CASBの導入とクラウド利用ポリシー策定の流れ

CASBを導入する際に、CASBの４つの機能について、フェーズを分けて導入すると効率的です。並行して、クラウド利用ポリシーを策定し、ステップごとにポリシーを修正します。

制御系システム アセスメント・サービス / ポリシー策定支援サービス

ミッション・クリティカルな産業、社会インフラなどの制御系システム/OT を対象として、「セキュリティー・アセスメント支援」および「セキュリティー・ポリシー策定支援」サービスを提供します。2サービスともに、サービス内容はお客様の要件に基づいて調整します。

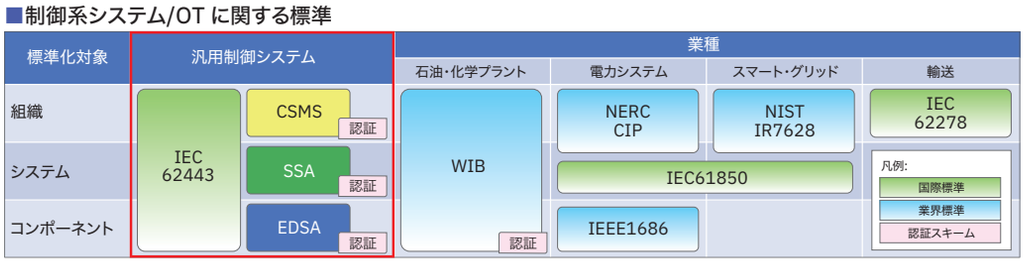
お客様の課題／要望

- 高い可用性と安全性が要求される制御系システム/OTを保有している
- 現行のITセキュリティー対応のリソースを有効活用し、制御系システム/OT領域にも効率的に横展開したい
- 専門性のある人材を確保できない

■制御系システム/OTセキュリティー推進フレームワーク

デジタル・トランスフォーメーション	セキュリティー・リスク・マネジメント	レギュレーション・コンプライアンス	セキュリティー・オーケストレーション	IT/OTセキュリティー・コンバージェンス
●動的に変化する環境の保護 ●運用プロセスへのセキュリティー統合 ●スマート・デバイスの保護 ●スマート・ファクトリーへのセキュリティー統合	●Secure byDesignの採用 ●セキュリティー・モニタリングの導入 ●セキュリティー・インテリジェンスの活用 ●ベースライン・アプローチによる異常検知	●インシデント報告義務要件の遵守 ●各種OTセキュリティー基準の参照(NIST, IEC, ISO 62443) ●センシティブ・データの保護 ●サプライチェーン・マネジメント	●セキュリティー人材の確保 ●セキュリティー管理プロセスの自動化 ●インシデント検知と対応プロセスの整備 ●エコシステム・パートナーとの連携	●IT-OT間接続のセキュリティー要件定義 ●IT-OT管理組織間でのリスク共有 ●IT-OTをまたがるセキュリティー設計 ●IT-OT間セキュリティー・モニタリング

■制御系システム/OT に関する標準



IBMがご提供する価値

●制御系システム/OT と情報系システム/IT との連携・統合
IT/OT間のセキュリティー要件、要求レベル、システム特性を認識し、統合したセキュリティー・マネジメント・サイクルを提案します

●国際標準を応用
制御セキュリティーの国際標準(IEC62443およびNIST CSF)を参照し、お客様の条件に合わせたアセスメント、ポリシー策定を実施します

●高度な専門性
多様なOS/プロトコルへの対応など、制御系システム/OTに関しての豊富な知識を持つ専門家が効果的かつ短期間に実施支援します

セキュリティー統合・自動化戦略策定支援サービス

既存または新規システムを対象に、近年セキュリティー運用の自動化として関心を集めている「SOAR(ソアー)」のコンセプトに基づくセキュリティー統合・自動化戦略を策定します。脅威インテリジェンスの収集やSOC運用、インシデント対応などのオペレーションにおいて、統合と自動化を通じた迅速化、非属人化、コスト削減の実現を支援します。

お客様の課題／要望

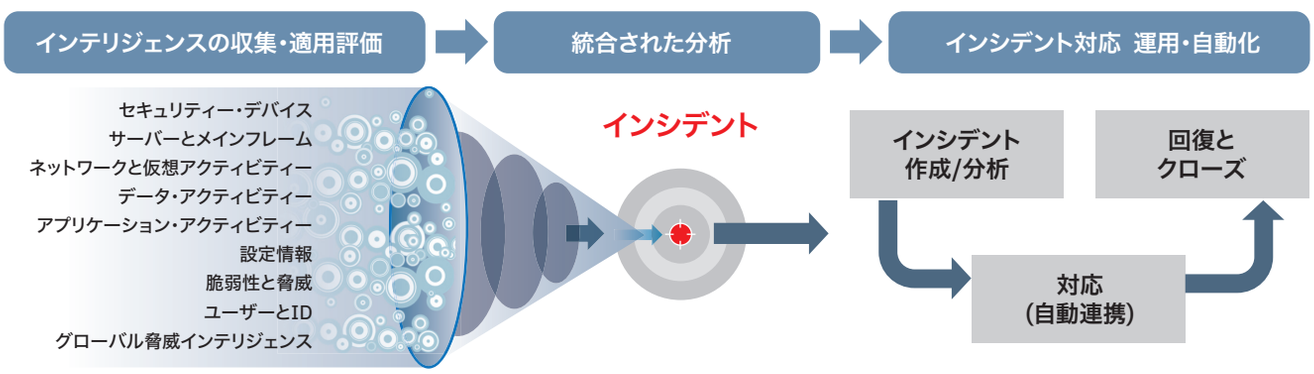
- サイロ化され、統合されていないセキュリティー製品運用
- セキュリティー製品の新規導入に起因してアラートが増加し、結果としてセキュリティー運用人材の不足が深刻化
- セキュリティー人材のスキルレベルに依存した一貫性のない属人的対応

IBMがご提供する価値

●豊富なセキュリティー・オペレーションの経験と深い知見に基づくご提案

●脅威インテリジェンス基盤、SIEMとチケッティング・システム、インシデント対応プラットフォームとレポーティング・ダッシュボードなど各種ツールを横断する統合された構想

●インシデント対応計画とツールの連携、インシデント対応の迅速化・非属人化



グローバル・セキュリティー・ポリシー策定・展開支援サービス

グローバル・セキュリティー・ポリシー策定支援サービスは、グローバルにおけるセキュリティー水準統一に向けて、セキュリティー・ポリシーを整備し、その展開および浸透に向けた取り組みを支援するサービスです。

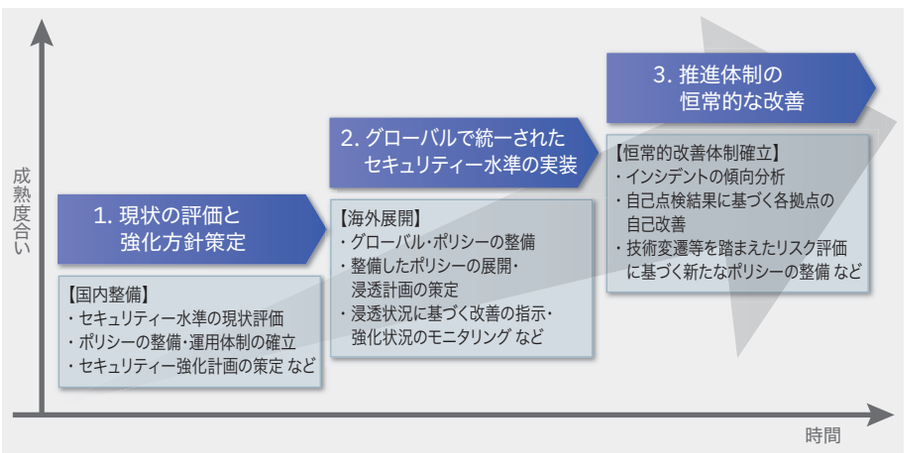
お客様の課題／要望

- 海外拠点において、セキュリティー規程類が独自の背景から各拠点別に定められ、全社統一されていない
- 各拠点において、どのようなセキュリティー水準で運用されているのか、現場のリテラシーなどの状況を把握できていない
- 現在のセキュリティー水準のばらつきを把握した上で、将来的に目指しているセキュリティー・レベルに近づけるための段階的な向上を図りたい

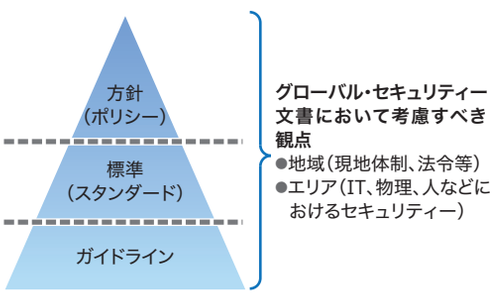
IBMがご提供する価値

- セキュリティー水準の現状把握および評価により、グローバルで展開可能なセキュリティー・ポリシーを整備
- 情報セキュリティーの国際標準（ISO27002、NISTなど）を参照したセキュリティー・ポリシーの策定
- 現状評価を踏まえた運用体制および計画の策定により、効果的なグローバル展開を実現

■グローバル・ポリシーの整備・展開とセキュリティー成熟度



■情報セキュリティー文書体系（例）



コンプライアンス準拠支援サービス

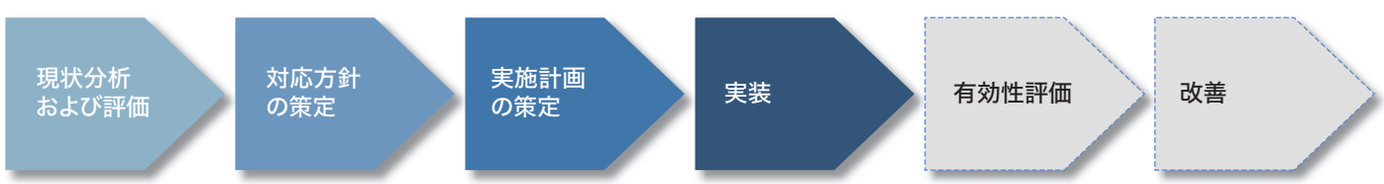
コンプライアンス準拠支援サービスは、企業内の規定やポリシー、ガイドラインなどがコンプライアンス（各国の法令や業界基準、ガイドラインなどの要求事項）を満たしているか、また各種事業プロセスが法令や業界基準に適合しているかを評価し、適合状況に不足がある場合は対応方針の決定から実装、展開、および浸透に向けた取り組みを支援するサービスです。

お客様の課題／要望

- 現在のセキュリティー対策が、法令やガイドライン（個人情報保護法、PCI DSS、GDPR、NIST、ISMSなど）に適合できているか不明
- ギャップや課題を解消するための改善策について、どの程度実施すべきかが不明確
- 専門家のアドバイスを受けながら、ビジネスを止めることなく、効率的にコンプライアンス対応を進めたい

IBMがご提供する価値

- 現状の企業内の規定、ポリシー、ガイドラインおよびプロセスが、事業遂行のために準拠が必要なコンプライアンスに適合しているか、ギャップや課題を把握することで、適切なプロセスで合理的な対応が可能
- 全体共通のセキュリティー対策により、漏れのない効率的なセキュリティー実装を実現



CSIRT設計・構築支援サービス

セキュリティー・インシデント対応の専門組織であるCSIRT(Computer Security Incident Response Team) を自社内に構築されるお客様を支援するコンサルティング・サービスです。社内統制、インシデントの早期検知および対応、被害の把握と極小化について、さまざまな状況下において柔軟に対応できるCSIRT 組織を構築します。

お客様の課題／要望

- 組織的、体系的なセキュリティー・インシデントへの対応策が急務
- 既存のCSIRT が自社に適しているか、有効に機能しているかが不安

IBMがご提供する価値

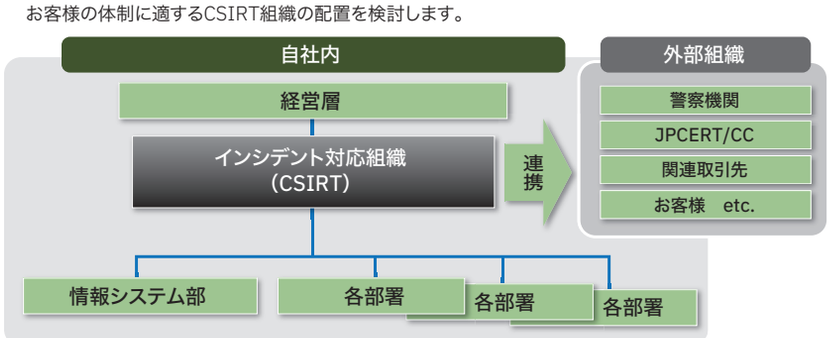
●適切なアセスメントに基づく組織設計
現状の情報セキュリティーへの取り組み、組織体制、経営層やサービス対象からの期待を調査し、お客様に必要なCSIRT 組織を設計・提案します

●ロードマップ策定
CSIRT組織のゴールに向けたロードマップを策定します

●CSIRT要員トレーニング
具体的なインシデント対応計画を立案するとともに、インシデント対応時のコアとなる要員に対し、応用力を身につけるための教育を実施します

■CSIRT組織体制の例

お客様の体制に適するCSIRT組織の配置を検討します。



■支援ステップとアウトプットの例

支援ステップは、お客様の要件に基づいて調整します。

ステップ例	Step.1 機密情報洗い出しおよびリスク・アセスメント	Step.2 情報セキュリティー対策状況アセスメント	Step.3 インシデント対応組織体制検討	Step.4 インシデント対応運用定義	Step.5 サービス・メニュー文書化	Step.6 CSIRT 要員トレーニング	Step.7 セキュリティー・ガバナンス構築支援
アウトプット例	●重要情報に対するアセスメント結果	●情報セキュリティー対策状況確認シート(調査アンケート) ●対策状況分析結果一覧 ●成熟度目標達成状況確認シート	●インシデント対応組織運用役割一覧 ●脅威およびリスク一覧表	●取得すべきログ一覧 ●インシデント対応フローおよび運用関連帳票一式	●インシデント対応組織定義書 ●残課題一覧 ●対策推進ロードマップ	●教育セミナーコンテンツ一式 ●残課題一覧(更新版)	●社内ガバナンス推進ロードマップ作成 ●インシデント対応組織年間運用計画資料作成

セキュリティー成熟度アセスメント・サービス
(IBM 10 Essential Practices)

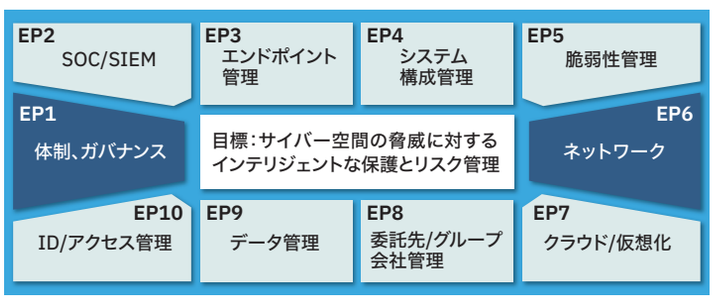
セキュリティーの重要要素を10に分解しそれぞれの現状アセスメントを実施します。現状把握から明確な目標を定め、中長期的なセキュリティーに対する戦略策定（ハイレベルな実施計画）を構築します。

お客様の課題／要望

- セキュリティー施策を進めてきているが、他社と比べてどの程度できているのか、ポジションを確認したい
- 現状のポジションを把握した上で、正しい方向に進んでいるか客観的に確認したい
- 現状把握から明確な目標を定め、中長期的なセキュリティーに対する戦略策定（ハイレベルな実施計画）を構築したい

IBMがご提供する価値

- 世界各国数百社で実績のあるIBMのフレームワーク「10 Essential Practices (10EP)」に基づく現状評価
- ベンチマーク：各EP毎にハイレベルな調査結果をグローバル業界動向と比較
- 同業他社とポジションの明確化およびハイレベルなロードマップ策定



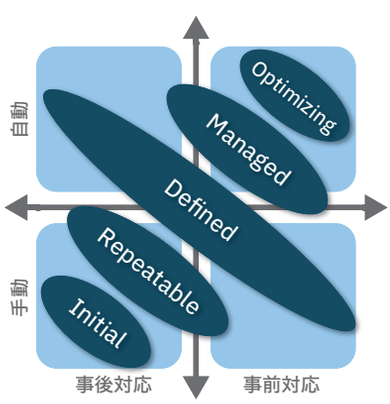
10EPアセスメント	10EP Project Insight	10EP ワークショップ	10EP コンサルテーション
	Lower ← Depth of Engagement → higher		
期間	IBM調査：3週間 ご報告と協議：2-4時間	4週間程度	4-8週間またはそれ以上 (実施内容による)
内容	IBMによるハイレベルな分析結果とご報告	分析結果をより深く掘り下げたワークショップを実施	特定のEPについて詳細な分析を実施
範囲	重要なセキュリティ課題説明と現状分析 (IBM洞察中心)	Technology, Organization, Process, Governanceの成熟度	EP領域毎の詳細な成熟度診断とアクションプラン、ロードマップの策定
成果物	・10 essential practice 分析結果のプレゼンテーション	・成熟度診断 ・ハイレベルな行動計画の策定	・成熟度診断 ・ベンチマーク診断 ・詳細行動計画 ・ロードマップ

網羅的な評価：5段階の能力成熟度モデル(Capability Maturity Model: CMM)

10EPの各要素	
EP1	体制、ガバナンス
EP2	SOC/SIEM
EP3	エンドポイント管理
EP4	システム　構成管理
EP5	脆弱性管理
EP6	ネットワーク
EP7	クラウド/仮想化
EP8	委託先/グループ会社管理
EP9	データ管理
EP10	ID/アクセス管理

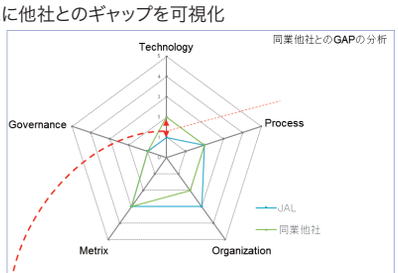
5つの観点
Technology (IT技術の活用)
Process (運用ルール)
Organization (組織の確立)
Metrics (評価基準)
Governance (全社的な仕組み)

5段階の成熟度
1 Initial (初期)
2 Repeatable (反復できる)
3 Defined (定義された)
4 Managed (管理された)
5 Optimizing (最適化された)



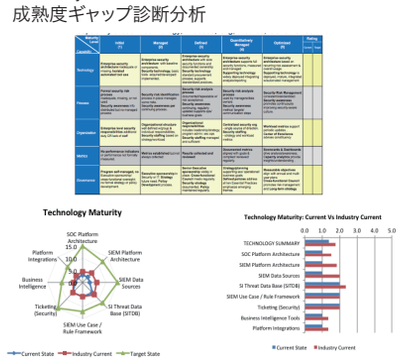
レビューと対策：他社ベンチマーク診断・成熟度診断・ロードマップ/行動計画

世界各国で100社以上のアセスメント実績をベースに他社とのギャップを可視化

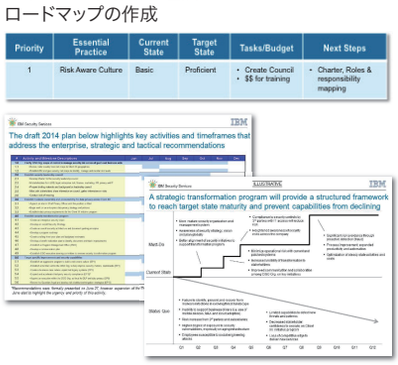


ギャップのある箇所については、課題・対応策を整理

Securityの現状のレビューと成熟度ギャップ診断分析



ハイレベルな優先順位決めとロードマップの作成



脅威管理 / Threat Management

製品

さまざまな機器から情報を収集し、脅威の早期発見を実現するセキュリティー・マネジメント・プラットフォーム

IBM QRadar

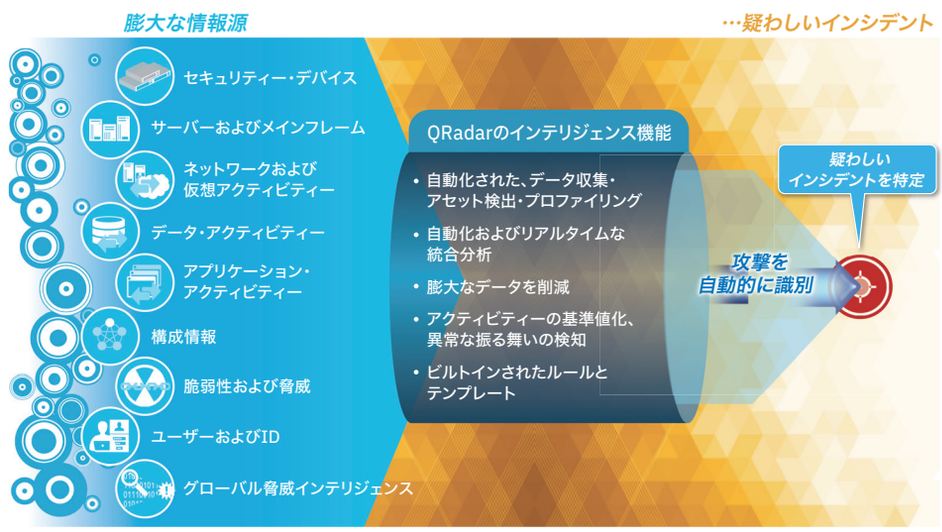
標的型攻撃を代表とする昨今の脅威は、さまざまな手法を組み合わせ、時間をかけ、少しずつ実施される攻撃のため、ネットワーク上の疑わしい事象や、OS、アプリケーションの異常を把握できず、重要とみなされる脅威を見逃しています。IBM QRadarは、企業内のセキュリティー機器や通信機器、サーバーやアプリケーションなどからの膨大な量のログやネットワーク・フローを収集し、多角的に高度な分析を行い、これまで検出が困難だった脅威までも見つけ出します。IBM QRadarは、運用の難しさや誤検知が多いこれまでのSIEM(Security Information and Event Management)とは違う次世代のセキュリティー・インテリジェンス・ソリューションです。アプライアンスもしくはソフトウェア(サードパーティーのハードウェア、仮想環境、またはIaaS環境に導入可能)、SaaS版(QRadar on Cloud)で利用可能です。

導入効果

- 予め用意された100以上のルール、1,000以上の検索パターンやレポート・テンプレートに加え、後からインストール可能なコンテンツ・パックやUBA(User Behavior Analytics/ユーザー振る舞い分析)のようなアプリケーションが提供されます。これらを活用することによって初期構成、チューニングおよび継続的管理が大幅に自動化され、短時間で本格運用を開始でき、IT環境の保護や、潜在的な脅威および違反の調査に必要な手作業が軽減されます。
- 膨大な種類のデータ(イベント、ネットワーク・フロー、アセット、トポロジー、脆弱性および外部からの脅威データ)を収集して相関付けを行い、調査が必要なアクティビティーと無害なアクティビティーとを優れた精度で判別し、脅威から守ります。
- NBAD(Network Behavior Anomaly Detection)機能により、この分野の専門知識で、ネットワーク、アプリケーションおよびユーザーの異常なアクティビティーを即時に検出し、リアルタイムな洞察を得られます。

■ IBM QRadarの特長

① 膨大なログ情報から、潜在的な脅威や不正を解析・予測



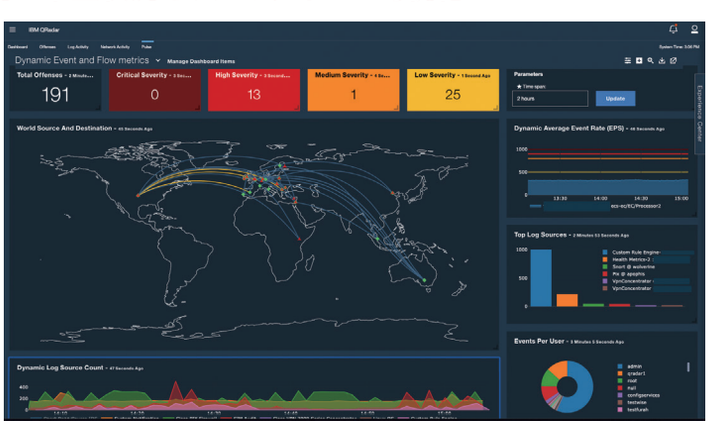
- 人手では分析が困難な、大量のログ情報から異常を検知・予測することが可能
- ネットワーク上を流れるデータとログ情報をマッチングする技術により、問題の発生源と発生範囲をリアルタイムに把握することが可能

② 社外からの攻撃や社内の不正状況をリアルタイムに可視化

可視化できる情報の一例

- 疑わしい脅威
- IPアドレス
- アプリケーション
- 認証
- ログイン失敗
- ネットワーク・トラフィック
- システム・モニタリング

など



攻撃が起きた際、攻撃の種類、誰・どこからの攻撃、アセットへの影響が瞬時にわかるため、対策を迅速に取ることが可能

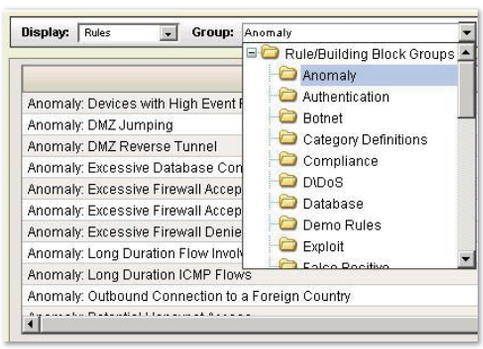
③ 知見を生かしたルールと検索パターンを製品に装備

■ 100種類以上のルールと分析（コンテンツ・パック/アプリケーションで拡張可能）

- ボットネットC&C通信の検出
- 脆弱性情報と現存する脆弱性の比較
- 複数の認証失敗後の認証成功

■ 1,000種類以上の検索パターンとレポート

- 各ログで失敗したログイン情報
- 国ごとの受信イベント情報など
- 検索、レポート、ダッシュボードに利用
- 重要な情報へのすばやいアクセスを提供



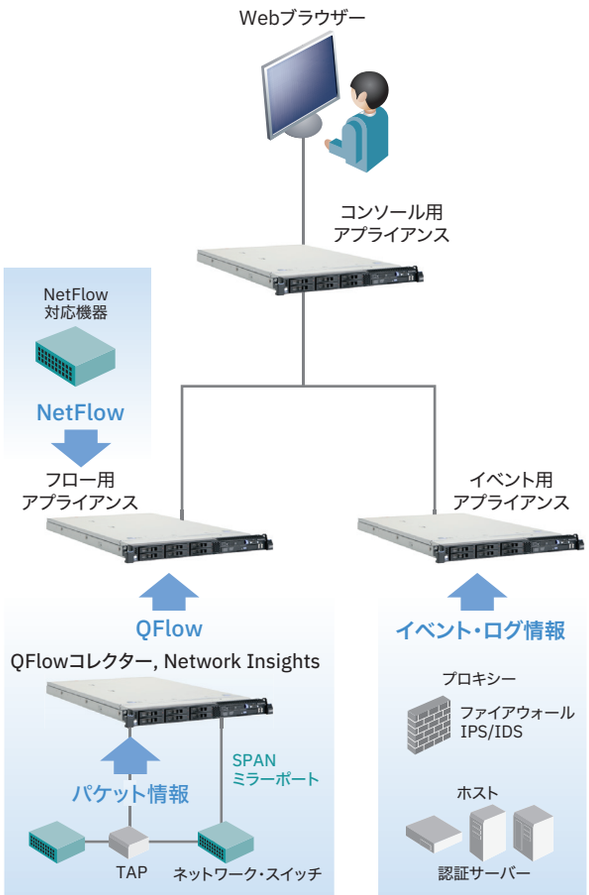
■ QRadar SIEMで活用できる相関分析ルール（主なコンテンツ・パックを含む）

振る舞い検知	DB接続が異常に多いホスト、海外からのリモート接続、複数のFWでDenyされるホスト、高いイベント発生率
認証	連続したログイン失敗後のログイン成功、退職者のアカウントでのログイン失敗、スキャン後のログイン成功
Exploit	検出された攻撃に対して脆弱性があるホスト、攻撃の後にFW許可、攻撃後15分以内の疑わしい挙動イベント
D/DoS	一定時間に大量のパケットを送信しているローカルのホスト、数千以上の外部IPアドレスから社内への通信の発生
ボットネット	潜在的なボットネットへの接続、既知のボットネットC&Cとの通信
コンプライアンス	監査サービスへの変更、信頼度の低いネットワークから高いネットワークへの通信
データベース	複数の場所からの同時ログイン、リモート・ホストからのグループの設定変更
マルウェア	リモートへのマルウェア通信の検出、不正なDNSサーバーとの通信
ポリシー	P2Pの利用、脆弱性が残っているホストの通信、平文通信プロトコルの利用
偵察（スキャン）	リモートからのTCPスキャン、ローカル・ネットワーク内でのDNSスキャン
疑わしい挙動	コンシューマー機器検出、短時間の特定ポートによる複数ホストへの通信
VMware	VMware環境における異常性の高いゲストOSの挙動、イベントの監視（ゲストOSの作成、削除、クローン、スナップショット監視）
ワーム	一定時間内のSMTP通信、一定時間内に多数のホストとの通信
IBM X-Force	IBM X-Forceの脅威情報（IPレピュテーション）に適合するIP通信の検知（ボットネット、Anonymous Proxyなど）

■ IBM QRadarプラットフォーム・ソリューション

ログ管理	Log Manager	●難しい設定が不要なログ管理 ●中堅から大手企業までカバー ●エンタープライズSIEMへのアップグレード可能
SIEM	SIEM	●ログ、フロー、脆弱性、IDの相関分析 ●高度なアセット・プロファイリング ●脅威管理とワークフロー
ネットワークとアプリケーションの可視化	QFlow, Network Insights　VFlow	●Layer 7のアプリケーション・モニタリング ●コンテンツ・キャプチャー ●物理環境と仮想化環境
リスク管理・脆弱性管理	Risk Manager　Vulnerability Manager	●ネットワーク・セキュリティー・構成モニタリング ●脆弱性スキャンと脆弱性の優先順位付け ●予測脅威モデルとシミュレーション
スケーラビリティー		●イベント・プロセッサー ●フロー・プロセッサー ●高可用性と障害回復 ●スタック可能な拡張
ネットワーク・フォレンジック	Incident Forensics	●PCAPからネットワーク・セッションを再構成 ●データ・ピボットと可視化ツール ●「誰が、いつ、何を」をより明瞭に追跡

■ IBM QRadarの構成例（分散構成）



脅威管理 / Threat Management

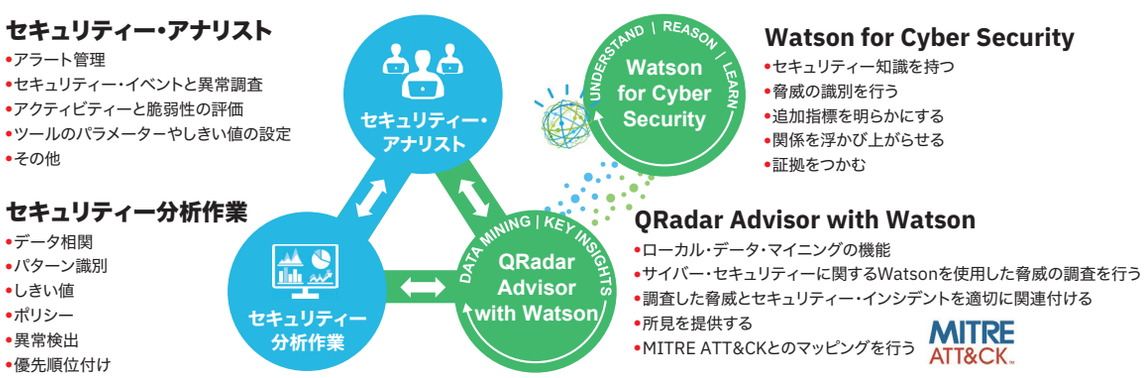
製品

Watsonを活用したセキュリティー・アナリティクス
IBM QRadar Advisor with Watson

IBM QRadar Advisor with Watsonは、WatsonにQRadarで検知したオフェンス(インシデント情報)を送信して脅威検出を実行することで、セキュリティー・アナリストが脅威を迅速に分析して対応するための支援を行います。Watson for Cyber Securityが学習している脅威情報に関する非構造化データ・ソースおよび構造化データ・ソースのコーパス(全集)を使用し、企業内のセキュリティー・インシデントと関連付けることによって、使用されたマルウェア、悪用された脆弱性、脅威の範囲など隠れた脅威を明らかにします。

導入効果

- スキル不足、膨大なアラート、インシデント対応の遅延、セキュリティー情報の拡散、対応時に起こりうるリスクなど、インシデント対応時の課題を変革します。
- 限られた時間の中で人間がアクセスできる情報源よりも、より多くの情報源を照合することができます。
- 常に最新のセキュリティー知識を維持できます。
- ヒューマン・エラーやアナリストの個人スキルへの依存を排除することができます。
- 脅威の知識、脅威アクティビティーなどの情報を活用して、正確な洞察を得ることができます。



セキュリティー・アナリスト
- アラート管理
- セキュリティー・イベントと異常調査
- アクティビティーと脆弱性の評価
- ツールのパラメーターやしきい値の設定
- その他

セキュリティー分析作業
- データ相関
- パターン識別
- しきい値
- ポリシー
- 異常検出
- 優先順位付け

Watson for Cyber Security
- セキュリティー知識を持つ
- 脅威の識別を行う
- 追加指標を明らかにする
- 関係を浮かび上がらせる
- 証拠をつかむ

QRadar Advisor with Watson
- ローカル・データ・マイニングの機能
- サイバー・セキュリティーに関するWatsonを使用した脅威の調査を行う
- 調査した脅威とセキュリティー・インシデントを適切に関連付ける
- 所見を提供する
- MITRE ATT&CKとのマッピングを行う

MITRE ATT&CK

アプリケーションのコラボレーション・プラットフォーム
IBM Security App Exchange

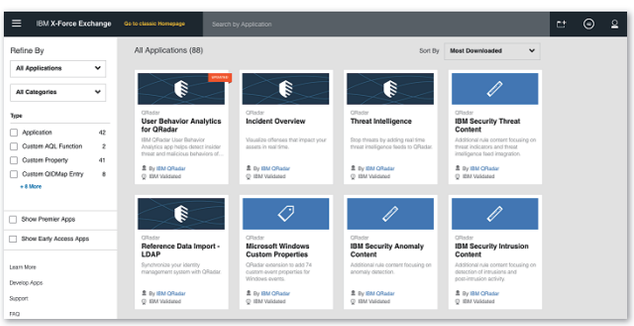
お客様、ビジネス・パートナー、開発者は、IBM Security App Exchangeのコラボレーション・プラットフォーム上で共有された高度なセキュリティー・インテリジェンス機能を利用したカスタム・アプリケーションを活用することにより、IBM QRadarをはじめとするIBMセキュリティー・ソリューションについての検知ロジック、レポート、アプリケーション連携を強化することができます。App Exchangeには多くの組織が参加しており、すでにIBMの開発者および複数のパートナーにより新しいアプリケーションが共有されています。これらの新しいアプリケーションは、サードパーティーのテクノロジーとの統合により、より多彩なデータへの高い可視性をお客様に提供するだけでなく、セキュリティーの専門家が緊急性の非常に高い脅威に集中できるようにするための新しい自動検索機能やレポート作成機能を提供します。

検証済み
セキュリティー・アプリケーション

コラボレーションの為の
シングル・プラットフォーム

パートナーの革新的な
技術へのアクセス

セキュリティー機能の
すばやい展開



導入効果

- IBMセキュリティー・ソリューションの機能を拡張するアプリケーションを簡単に入手することができます。
- ルール、レポート、検索クエリー、リファレンスセット、カスタムプロパティー、ダッシュボードなどのパッケージをアプリケーションとして利用できます。
- リアルタイムでソリューションを検索し、活用することができます。
- IBMが提供するQRadar UBA(User Behavior Analytics)アプリケーションを活用することで、早期発見が難しい不正な内部の振る舞いの可視化を実現いたします。

各種法整備やレギュレーションに対応したインシデント対応プラットフォーム

IBM Resilient SOAR (Security Orchestration, Automation and Response) Platform

セキュリティー事故や事件が発生した時に、企業としてすばやく、かつ適切で的確な対応が必須です。セキュリティー・インシデント対応に必要な、エンタープライズレベルでのプラットフォームを構築するために必要なすべての要件を兼ね備えたソリューションです。

IBM Resilientは、次世代のインシデント対応に必要なSOARの３要素（1.セキュリティーのオーケストレーションと自動化　2.セキュリティー・インシデントのケース管理および対応管理　3.セキュリティー脅威インテリジェンス）すべてを兼ね備えた、プラットフォーム構築ソリューションです。

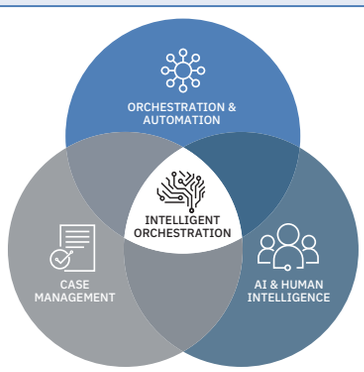
導入効果

- ●インシデント対応の属人化を排除し、SOA（標準業務手順）を遵守することによって効率的で適切な対応をチームにて実施可能
- ●「今」企業内で発生しているインシデントの対応状況やリソース状況の的確な把握と対応の検討
- ●企業によって異なる環境であってもオーケストレーションとオートメーションを実務に応じた形で実装可能。また、AppExchangeから必要な連携モジュールをダウンロードして自動化プロセスを構築可能
- ●業界のレギュレーションであるPCI DSSやHIPPA、またはGDPRなど各国の制限に応じたベストプラクティスのタスクを割り当て
- ●インシデントに対して「いつ」「どこで」「なにを」「どうしたか」をすべて記録し、対応の履歴を保持することによってコンプライアンス対応を適切に管理

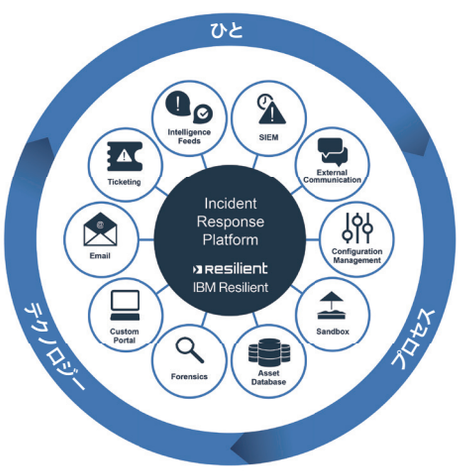
■ SOARを構成する３つの要素

オーケストレーション&自動化
- •ダイナミック・プレイブック
- •スクリプト、ルールエンジンおよびドラッグ&ドロップできるビジュアル・ワークフロー・エディター
- •インテグレーションのエコシステム、プレイブック、ベストプラクティスおよび開発者ツールキット
- •インシデントの自動エンリッチメント

ケース管理
- • インシデントのエスカレーション、作成および管理
- • コラボレーションとチーム管理
- • レポートと分析

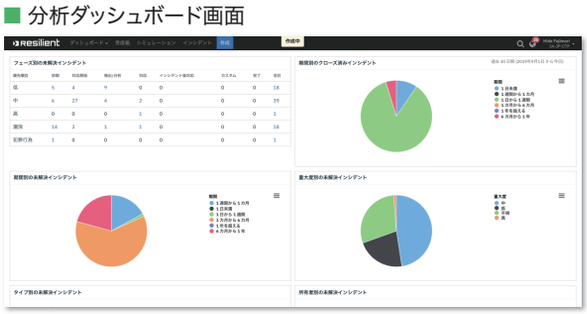


AI & 人のインテリジェンス
- •AIで強化されたインシデント・レスポンスと脅威インテリジェンスの統合
- •ベストプラクティス、IRの専門知識、およびプライバシー・ルール・エンジン



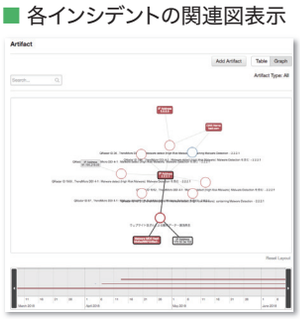
セキュリティー・インシデントを解決する為の中心となるソリューション

■ 分析ダッシュボード画面

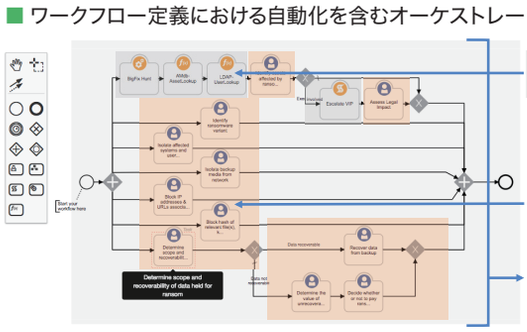


■ インシデント対応画面

■ 各インシデントの関連図表示



■ ワークフロー定義における自動化を含むオーケストレーションの例



技術的作業の自動化により、対応を迅速化

対応プロセスの重要な段階における
コンテキストや人間に よる意思決定

人、プロセス、テクノロジーの
オーケストレーション

脅威管理 / Threat Management

製品

脅威インテリジェンス情報共有プラットフォーム
IBM X-Force Exchange

IBM X-Force Exchangeは、クラウド・ベースの脅威インテリジェンス・プラットフォームです。最新のグローバルなセキュリティー脅威をすばやく調査し、対処可能なインテリジェンス情報を集めて、他の担当者と共同で作業することができます。IBM X-Force Exchangeは、世界で最も広く認められているセキュリティー調査チームの1つであるIBM X-Forceによってサポートされています。

IBMセキュリティーの技術と
パートナー・エコシステムを活用

IBM X-Forceは、世界で最も実績の高いセキュリティー研究開発チームの1つです。この研究開発のセキュリティー専門家チームは、88,000件を超えるセキュリティー脆弱性情報のデータベース、グローバルな Web クローラーおよび世界中のスパム・コレクターの情報、日々収集される何百万ものマルウェア・サンプル、150億もの日々のセキュリティー・イベントなど、世界130カ国を越えるさまざまな情報ソースをリアルタイムに監視し、セキュリティー脅威を分析しています。

オープン　膨大な脅威インテリジェンス・データに対してアクセスできる堅牢なプラットフォーム

脅威データへのすばやいアクセス

- クローラロボット、ハニーポット、ダークネット、およびスパムトラップから機械生成した700テラバイト以上のインテリジェンス情報
- 複数のサードパーティーとパートナーからのインテリジェンスな情報
- 一時間ごとに分類した数千個におよぶ悪意のあるIP情報など

実用的　脅威に対して迅速な防御を支援する統合ソリューション

タイムリーな防御のために、各製品へインテリジェンス情報を反映

- IBMセキュリティー製品とIBM X-Force Exchange情報の実用的なインテリジェンスの統合
- 自動化された脅威情報の共有に関する規格であるSTIXやTAXIIの将来的なサポートを予定している、サードパーティーとの統合を視野に入れた設計
- セキュリティー製品に脅威インテリジェンスを接続するためのAPIを活用

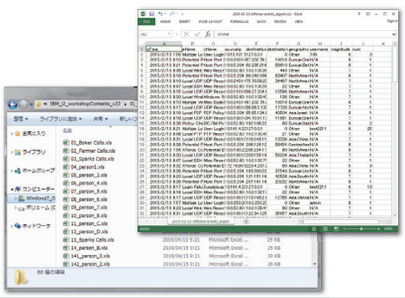
ソーシャル　脅威インテリジェンスを共有するためのコラボレーション・プラットフォーム

同業者との連携によって、脅威情報にコンテキストを追加

- 調査結果を検証するため、業界の同業他社と接続します
- フォレンジック調査を支援するため、Indicators of Compromise（IOCs）のコレクションを共有します

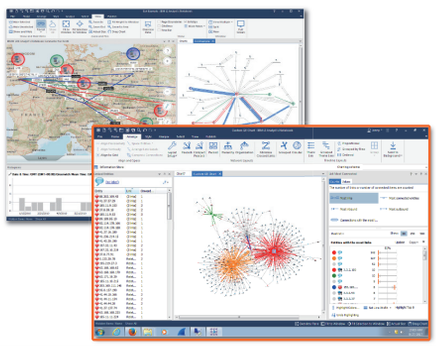
不正調査のインテリジェンス・プラットフォーム
IBM i2 Analyst's Notebook（ANB）/Analyst's Notebook Premium（ANBP）

IBM i2製品は、複雑で大量な情報や断片化情報をさまざまな視点から分析し、関係性や経緯を体系化・可視化することによって、犯罪や不正行為、疑わしい取引の識別/予測/防止/阻止を支援するツールです。



さまざまな分析の効率化を実現します
- 人と人、人と組織、人と車、人と物、人と場所などの関係性分析
- 複数事案における人や組織の関係性分析
- 広域にわたる人物、組織などの関係性分析
- 対象の背後関係の分析
- 行動パターンや発生パターンの分析
- 口座のやり取りの分析

150ケ国4500以上のお客様で利用されています



ANBPを含む上位EditionのEnterprise Insight Analysis (EIA) ではBig Dataに対応
- 100テラバイト以上の情報
- 170万の地理的エンティティー
- 100万以上の電話番号
- 120万以上のユニークなアイデンティティー
- 1日10億以上の履歴データ
- 10億以上のエンティティー
  <人、場所、車、組織、etc>
- 1兆以上の通話レコード

導入効果

- 法執行機関では調査対象者の人間関係、行動履歴、通信履歴など視覚化し犯罪、テロ、不正行為などの高度な調査・捜査を支援します。
- 金融機関においてはアンチマネー・ロンダリングなどの金融不正に対して、取引の流れ、顧客の行動履歴などをネットワーク図として視覚化し、不正行為および実行者の特定を支援します。
- サイバー・セキュリティーではQRadarなどのSIEMデータに加えて、上位Editionでは、Web/SNS、非構造化情報、オペレーショナルなビッグデータを統合し、属性を付加することによりサイバー攻撃の犯人特定を支援します。

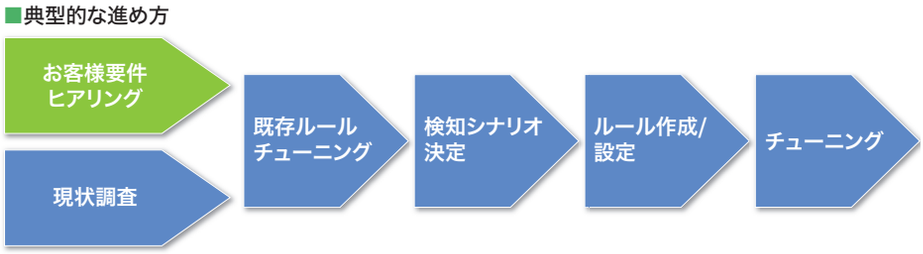
QRadarルール高度化サービス

IBM X-Force IRISの知見を集結し、お客様のQRadarを最大限に活用する検知ルール最適化を行います。「現状のルールの評価」により現在のルールの課題を洗い出し、「ルールの最適化」により最新脅威へ対応、「チューニング」により継続的に運用可能な適切な検知レベルへの調整を行います。

お客様の課題／要望

- 現在のルールで検知できている脅威、漏れている脅威を把握したい
- 最新の脅威動向に対応したい
- オフェンスが上がりすぎて運用に困っている
- こんな検知が可能か相談したい

■典型的な進め方



IBMがご提供する価値

- ●現在の検知ルールやログソースで何ができていて、何ができていないかを正確に把握できます
- ●既に設定されている検知ルールを、最適化します
- ●お客様要件や環境に合わせた最適な検知ルールを必要に応じて追加導入し、チューニングします
- ●製品提供ルール、X-Force Exchange公開ルールだけでなく、IBM知見に基づく最新の脅威動向を踏まえたオリジナル・ルールを提供します
- ●JPCERT/CCガイド類への準拠を実現します

QRadarルール高度化サービス実施の流れと検討項目の典型的な例を示します。

準備フェーズ

1. お客様要件の確認

検知に関する要望をヒアリングします
- 強化したい検知内容
- 活用したいログソース

など、を伺います

2. 現状調査

現在のQRadarのログソースやフローの取得状況およびその使用されているルールを調査しますオフェンスの生成状況も合わせて確認します
- 現在のルール一覧を提供
- 現在網羅できている検知、できていない検知を可視化
- 過剰な検知などがある場合はチューニング案を提示

3. 事前チューニング

必要に応じて既存ルールに対する事前チューニングを実施します

検討フェーズ

4. 検知シナリオの検討

ディスカッション・セッション形式にてどのような検知を行うか議論します検知シナリオ案はIBMが提示し、お客様の関係者に広く参加いただき、検知シナリオを決定します

5. 検知ルールの選定・作成

検知シナリオを具体化する検知ルールを作成します
- 製品提供ルール
- X-Force Exchange公開ルール
- IBMX-Force IRIS独自知見に基づく高度な検知ルールを提供します
- JPCERT/CCガイドへの準拠ルールを提供します

「高度サイバー攻撃への対処におけるログの活用と分析方法」
「高度サイバー攻撃(APT)への備えと対応ガイド」
「インシデント調査のための攻撃ツールなどの実行痕跡調査に関する報告書」

実行フェーズ

5. 検知ルールの設定

QRadarに検知ルールを設定します運用中のQRadarへの影響を最小化するため、オフェンスは生成させずに検知状況を確認します

6. チューニング

適切な検知件数になるようチューニングを実施します検知内容によっては、オフェンス生成ではなくレポート作成での代替など、総合的に検知の緊急度や優先度をもとに持続運用が可能となるチューニング案を提示し、合意をえたのちチューニングを実施します

脅威管理 / Threat Management

セキュリティー・オペレーションと監視 / Security Intelligence and Operations Consulting (SIOC)

360 度全方位の脅威ライフサイクルを管理するセキュリティー対策
IBM X-Force Threat Management (XFTM)

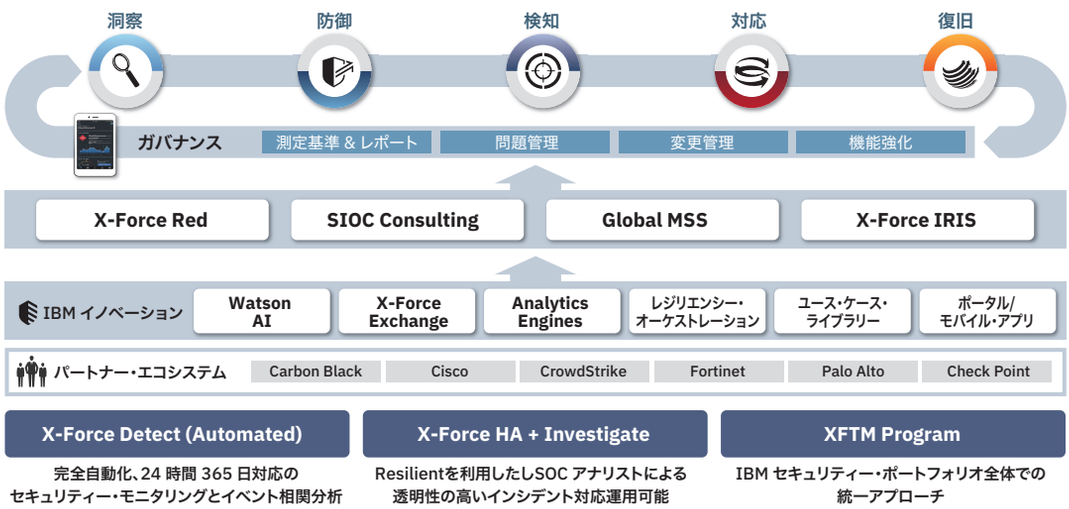
セキュリティーのビッグ・データ活用であるセキュリティー・インテリジェンスを提供するサービスとして、お客様環境やクラウド環境を対象にIBM Qradar SIEMやIBM Resilient SOAR Platformと組み合わせることで、攻撃の監視や分析のための環境の設計や構築・運用・監視を行い、次世代のセキュリティー対策の実現をご支援するサービスです。

お客様の課題／要望

- 検知、通知、調査、対応にスピードと一貫性が必要
- 高品質な調査、優れた洞察とガバナンス、継続的改善への適切な助言が必要
- 調査や洞察の情報源など助言にいたるまでの透明性が必要

IBMがご提供する価値

- **プログラムに基づいた枠組み**が規範的な統合アプローチを可能にし、よりよい成果をリード
- **信頼できるセキュリィー・パートナー**はワールド・クラスの専門家を擁し、重要な洞察や必要な規模を提供
- **よりスマートなプラットフォーム**にて、アナリティクス、AI、オーケストレーションを活用し、調査や対応を迅速化



SOC構築支援サービス

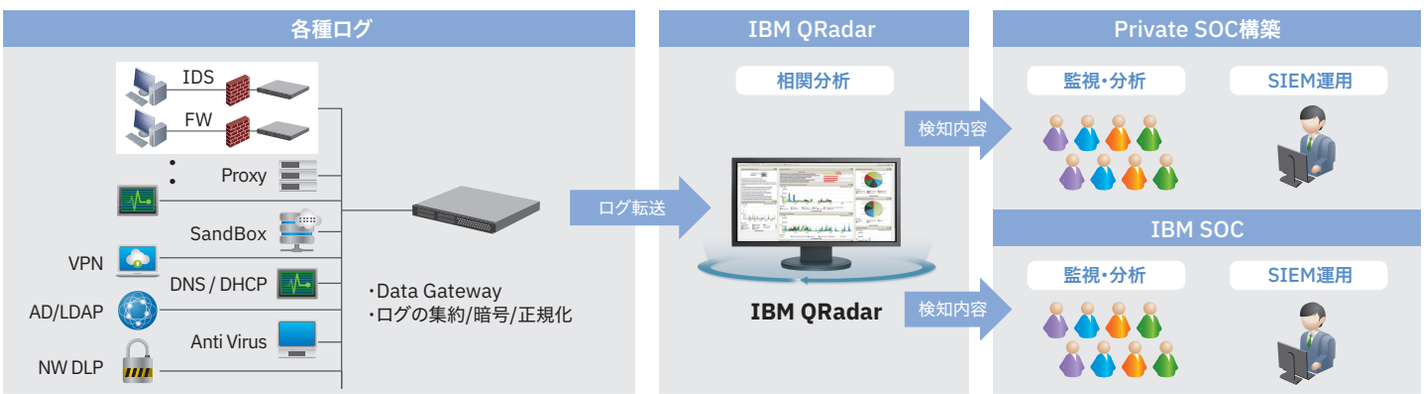
SIEMの導入およびSOCの構築を支援するサービスです。IBM QRadar SIEMによる各種ログの統合的な分析を実現するため、ログソースの選定やログの転送設定、SIEM構築、およびプライベートSOC構築を支援します。

お客様の課題／要望

- 相関分析を含むより高度な検知を実現するためSIEMを導入したい
- SIEM導入だけでなく、SOCの体制やプロセスも合わせて構想したい
- SIEM構築にログの転送設定やSIEMルールの設計など専門家の知見が必要

IBMがご提供する価値

- SIEMを用いた統合ログ監視体制の構築
- 相関分析による高度なイベント監視・分析



セキュリティー・アーキテクチャー設計支援サービス

既存または新規システムを対象に、セキュリティー・アーキテクチャーの設計を支援します。IaaS/SaaS通信の増加への対応、安全なWebアクセスの実現、各種セキュリティー機能の最適配置、共通機能の集約を通じたコスト最適化など、さまざまな課題についてトレードオフを整理し、構成モデル・機能配置の決定を支援します。

お客様の課題／要望

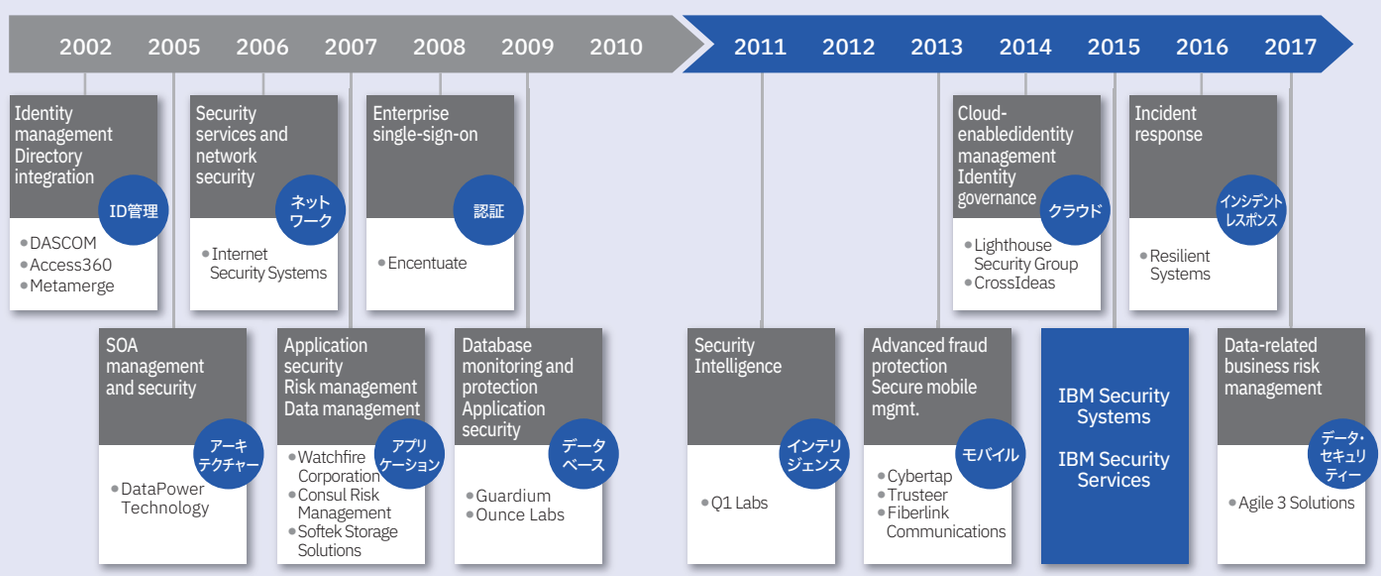
- 安全なWebアクセス実現のため、セキュリティー・アーキテクチャーを見直したい
- グループ会社間で共同のセキュリティー基盤を構築したい
- セキュリティー機能の集約・最適配置を通じたレイテンシーやコスト削減を実現したい

IBMがご提供する価値

- 安全なWebアクセスを実現するセキュリティー・アーキテクチャーの策定とエンドポイント保護水準の向上
- グループ会社間のセキュリティー基盤共同化による全体最適化と統制の強化
- 機能の集約と最適配置によるコスト削減

■ セキュリティー・アーキテクチャー設計支援

ご参考 IBM Securityの強み①-最適なソリューションをお届けするための持続的投資



“...IBM Security is making all the right moves...”
Forbes

- IT Layerの**各領域におけるLeadership Positionの企業を買収**
- **Q1 Labsによるインテグレーションとインテリジェンスの領域へ進出**
- **クラウド基盤、エンドポイント、セキュリティー運用領域へ拡大**

脅威管理 / Threat Management

インフラとエンドポイント保護 / Infrastructure and Endpoint Security (IES)

セキュリティー・システム設計・構築支援サービス

各種セキュリティー製品の導入にあたり設計支援およびシステム構築を行います。メール・セキュリティー、Webフィルタリング、サンドボックス、プロキシ、ファイアウォール、IPS/IDS、UTM、SIEMなど、さまざまなシステムの設計支援および構築により強固なセキュリティーを備えたレジリエントなネットワークとセキュリティー・システムを実現します。

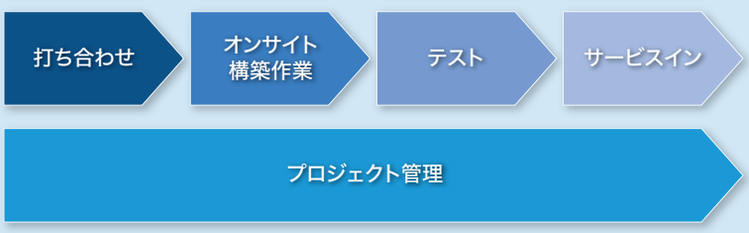
お客様の課題／要望

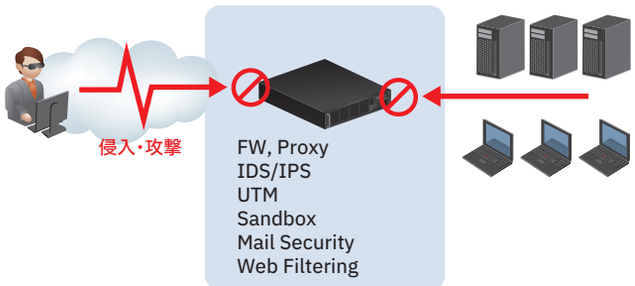
- 自社のネットワーク・セキュリティーを強化するため新システムを導入したい
- セキュリティー・システムに精通した専門家の不在
- マルチベンダーによるセキュリティー・システム連携に対する知見が不足

IBMがご提供する価値

- 製品やアプライアンスの特性を踏まえたスムーズな導入手順
- 他社での導入、運用事例に基づく利用方法の提供

構築作業の進め方(例)





IBM Managed Network Security Services (MNSS)

IBM Infrastructure Security Services - Firewall Management (ファイアウォール管理サービス)

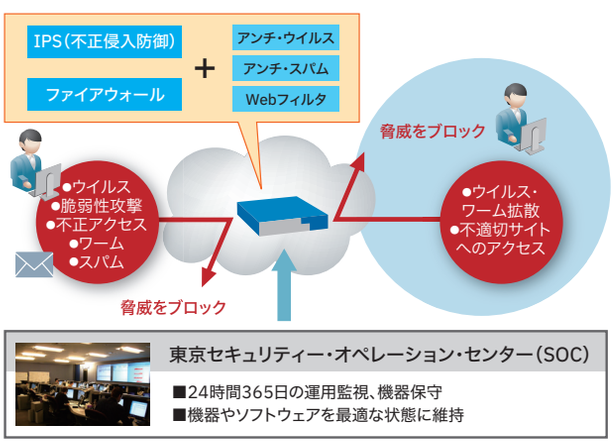
ファイアウォールはお客様のネットワークとインターネットとの境界に設置されます。そのため、その障害は多くのサービス停止の原因となり、さらには企業活動の運営に大きな損害を引き起こす可能性があります。ファイアウォール管理サービスでは、専門のエンジニアが24時間365日体制でお客様のファイアウォールを管理し、早期の障害対応、夜間・休日のバージョンアップ作業、アクセス・ルールの変更作業などの対応を実施します。

IBM Infrastructure Security Services - Intrusion Detection and Prevention System Management (IDS/IPS監視サービス)

不正侵入検知・防御システム(以下、IDS/IPS)は、ファイアウォールでは防ぎきれない、不正アクセスの兆候を検知・防御することができるシステムです。IDS/IPS監視サービスでは、専門のセキュリティー・エンジニアが24時間365日体制でお客様IDS/IPSの監視を行い、不正アクセスの兆候に合わせてIDS/IPSの設定を最適化することで攻撃を早期に発見し、お客様ネットワーク環境のリスク低減を図ります。

IBM Infrastructure Security Services - Unified Threat Management

お客様サイトに設置されたUTM(Unified Threat Management)機器をSOCから専門のセキュリティー・エンジニアがリモートで運用を行うサービスです。ファイアウォールでは防ぎきれない不正アクセスの兆候をUTMの機能であるファイアウォール、IDS/IPS、アンチ・ウイルス、アンチ・スパム、Webフィルタの設定を最適化することで攻撃を早期に発見し、お客様ネットワーク環境のリスク低減を図ります。

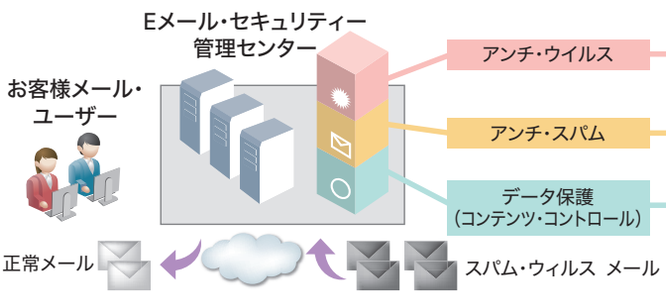


IBM Eメール・セキュリティー管理サービス

グローバル規模で24時間365日の総合的なクラウド・サービスを提供します。インターネットの上でEメールをスキャンし、お客様のネットワークに届く前に脅威を阻止し,お客様のネットワークに配信されるEメールが安全であるという安心をお届けいたします。

IBMがご提供する価値

お客様に代わって、IBMのセキュリティー・センターで24時間365日配信されるEメールのスパム、マルウエア対策を実施。最低限の初期費用で、検知精度の向上と、運用負荷およびメール・サーバー管理の負担を軽減します。また30日間の無料お試しサービスもご利用いただけます。



3種類の商用スキャナーとマルウエアのDNA分析機能を持った独自開発スキャナーを使いいち早くマルウエアを検疫し隔離します。リンク先のマルウエア分析、検知、対応可能です。

2,000以上の独自ルールにより迷惑メールを判定し隔離します。お客様によるホワイト・リスト(配信許可リスト)や、ブラック・リスト(配信拒否リスト)の設定も可能です。

お客様のメール利用方針に基づく管理が可能です。
・送信者/受信者、不適切な用語、添付ファイル、メールのサイズ

IBMクラウドWeb セキュリティー・サービス(CWSS)
(Cloud Web Security Services)

Webアクセスによる脅威防御のアウトソーシングで運用コストの最適化

お客様の課題／要望

- Webアクセスに起因するマルウェア感染
- 業務外Webアクセスが原因となる生産性低下
- 管理者不在、管理・運用スキルに不安

IBMがご提供する価値

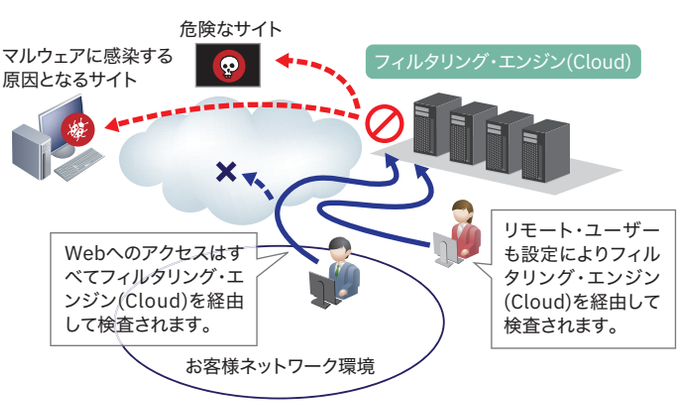
新たに機器の導入や運用管理を必要としないクラウド・サービスとして、IBMクラウドWebセキュリティー・サービスをお勧めいたします。不正サイトや改ざん済みサイトへのアクセスが原因となるマルウェア感染やスパイウェアの社内侵入を防ぎます。さらに、暗号化(SSL)通信の検査を含んでおり、業務に関係無い不適切なサイトへの制限も実現できます。

■IBMクラウドWebセキュリティー・サービスの主な機能

1 プロキシ制御
リアルタイムURL評価、詳細なポリシー制御、SSL検査、Webアプリケーション制御が可能です。

2 コンテンツ分析
ホワイト/ブラックリスト適用により既知の安全なサイトは許可、脅威サイトは遮断します。

3 レポーティング
統計情報を迅速に確認可能なレポート画面を提供し、そちらでセキュリティーに特化した各種レポートをご覧頂けます。



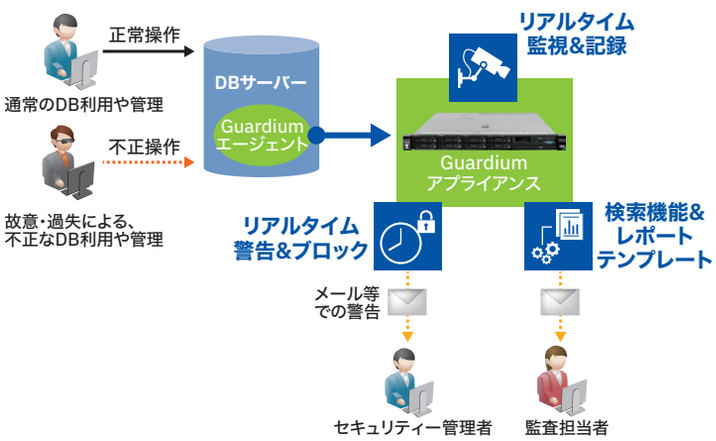
■IBM独自のヘルプデスク(Security Operation Center・24時間365日・日本語)でのお客様の支援を実施

データベースのリアルタイム監視、保護、監査

IBM Security Guardium Data Protection

不正な攻撃手段は多数存在しますが、重要データの保管先の多くがデータベース・サーバーである事実は変わりません。また記録された攻撃のうち6割が組織内でのアクセス可能な人物によって行われたという統計も出ており、特にDB特権アカウント不正操作の監視・保護は必要不可欠になっています。

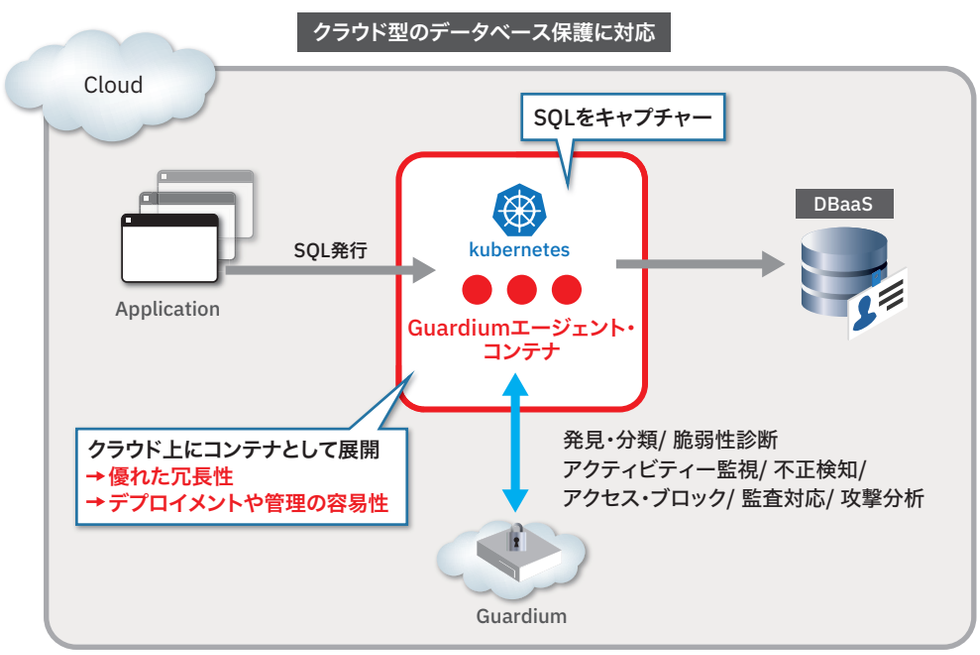
IBM Security Guardium Data Protectionは、既存データベースのパフォーマンスへの影響は最小限に抑えつつ、内部犯行を含む不正アクセスをリアルタイムで監視&防止するソリューションです。また、データベース監査ログを一元管理、ログ収集から、加工、レポート出力までの作業工数を削減します。



導入効果

- ●多数、多種類のデータベース監査ログを一元管理
- ●DBAを含むすべてのアクセスを監視しながら、データベース・パフォーマンスへの影響は最小限
- ●クイックに必要トラフィックのみを検索表示、データアクセス状況のサマリ抽出、コンプラ対応テンプレート提供など、豊富な可視化ツールを提供
- ●監査ログの収集から、加工、出力、確認までの作業をワークフローで自動化することにより、膨大な監査対応工数を削減
- ●不正アクセスをリアルタイムで通知、ブロックする事により情報漏えいの早期発見、未然防止を実現
- ●データベース・サーバーのファイル操作も監視可能
- ●取得したログを改ざん・ 不正削除されない仕組みで保管

Guardiumはクラウド型のデータベース（DBaaS）の保護に対応しています。保護のためにはエージェントをKubernetesで管理することのできるコンテナとして実装します。これにより、従来型のデータベースと同等の機能をクラウド環境に実装でき、ハイブリッド・クラウド環境のセキュリティーを強化します。また、複数のパブリック・クラウドのデータ・セキュリティーを一元管理することで運用負荷を軽減します。



<対応パブリック・クラウド>

- Oracle Cloud
- AWS
- Azure
- IBM Cloud
- Google

など

<対応クラウドDB >

- Oracle
- Postgres
- MySQL
- DB2
- SQL Server
- Amazon Aurora
- Amazon Redshift

など

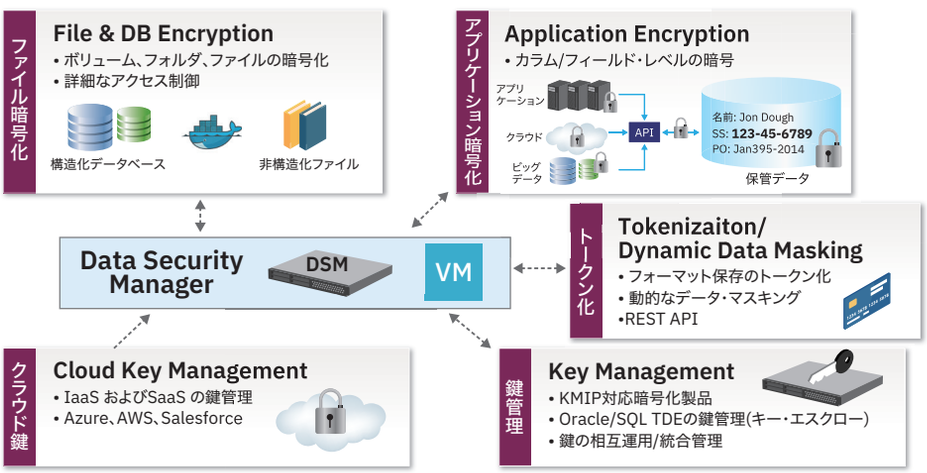
ハイブリッド・クラウド環境におけるデータ暗号化基盤

IBM Guardium Data Encryption

IBM Guardium Data Encryptionはハイブリッド・クラウド環境全体での一貫した暗号化戦略の実現を支援します。

お客様の課題／要望

- ファイルサーバー、DBサーバーに保管している重要データの漏えいや悪用を防ぎたい
- 自社の暗号鍵を用いて、データへのアクセス制御＆暗号化を実現したい
- アプリケーション側や、データベースの表に格納されるデータを暗号化したい
- 重要データをマスキングして、不適切なユーザーにはデータを見られないように値をトークン化したい



導入効果

- コンプライアンスへの準拠
  •（例：GDPR要件への対応）
- ファイルサーバー、DBサーバー、アプリケーション、コンテナ、クラウドなど、あらゆる場所でのデータ流出を防止
- KMIPやDB標準暗号化機能に対応した鍵の集中管理により、複雑性を回避し、安全な鍵管理を実現
- カード情報非保持化によるPCI DSS対応負荷軽減

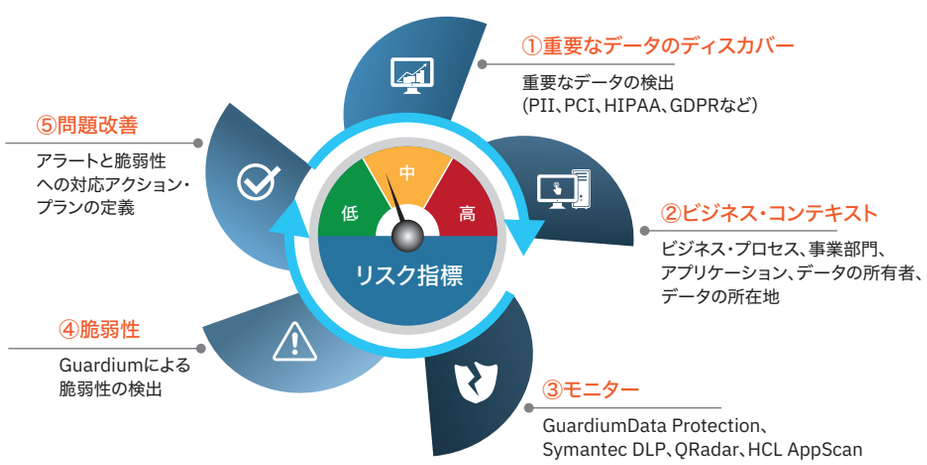
重要データのビジネス・リスクを可視化

IBM Data Risk Manager

IBM Data Risk Managerは重要データを発見し、ビジネス・リスクとしてマッピングします。それらのデータ漏えいや事後対策に至るまで、トータルでデータ・セキュリティー対策を支援するリスクマネジメント・プラットフォームです。

お客様の課題／要望

- データの所在や保存目的が不明確で何から手を付ければよいかわからない
- 重要資産を分類し、データの保管場所、アクセス権、削除権の最適化を図りたい
- データが持つリスクの状況が把握できないため有効な対策方法がわからない
- データ漏えい時に関係するステークホルダーをすぐに特定できず、初動に時間がかかる



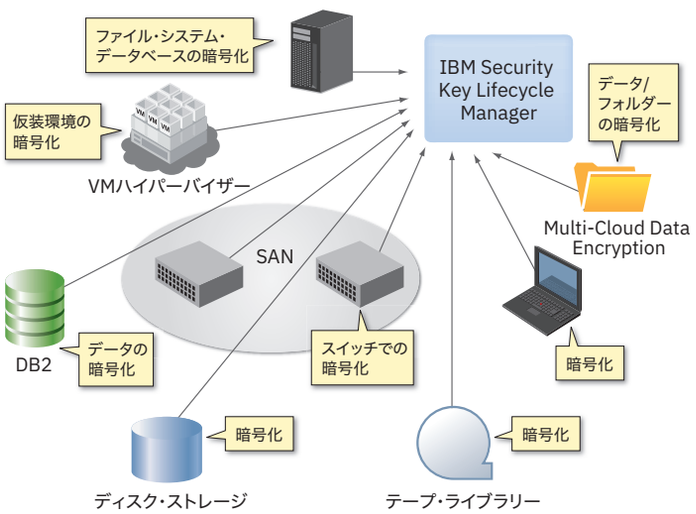
導入効果

- データカタログの作成時間短縮
- 組織全体におけるデータ・リスクとビジネス・コンテキストの可視化
- データを処理するアプリケーションやサービス、影響を受ける業務の特定時間短縮
- インシデントやデータ侵害への対応負荷軽減
- データ保護施策の有効性評価により、有るべき姿とのギャップを把握
- ギャップを修復するための行動計画を策定する負荷の軽減
- IBM製品や他社製品と連携することで、さまざまな視点からリスク分析やデータ保護対策を管理することができる統合プラットフォームとして活用可能

暗号および暗号鍵ライフサイクル管理

IBM Security Key Lifecycle Manager

IBM Security Key Lifecycle Managerは、自己暗号化機能を持ったストレージなど、暗号処理を行うさまざまなデバイスで求められる暗号鍵管理を安全に効率的に行うことを可能とします。暗号鍵管理仕様の標準であるKMIPに準拠し、IBM製品に限らず広く他ベンダー製品の暗号鍵管理を行うことができ、PCI DSSなど多くのセキュリティー標準準拠への対応施策を支援します。



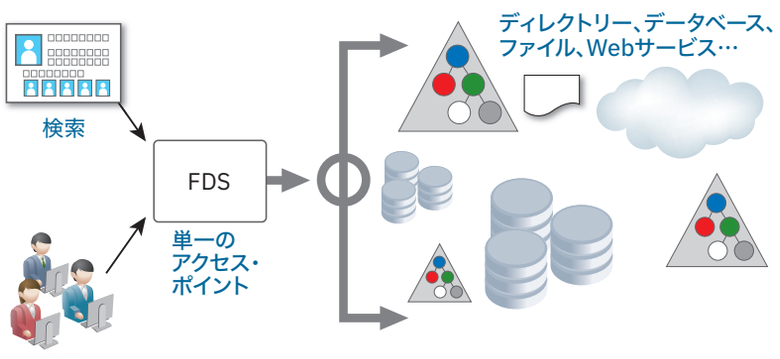
導入効果

- 暗号キー管理プロセスを集中化し、自動化する
- データ・セキュリティーを強化し、同時に暗号キーの管理にかかわるコストを大幅に削減する
- 構成と管理用に直感的に使用できるユーザー・インターフェースを使用して暗号キー管理をシンプル化
- 機密情報の損失や漏えいのリスクを最小化
- Sarbanes-Oxley や Health Insurance Portability and Accountability Act（HIPAA）などの規制標準のコンプライアンス管理を容易にする
- キー管理操作に対するロールベースのアクセス管理を提供し、セキュリティーを強化
- 暗号鍵管理仕様「KMIP」をサポートし、マルチベンダー環境での鍵管理を支援

企業の統合されたアイデンティティー・データ・インフラストラクチャー

IBM Security Directory Suite

IBM Security Directory Suiteは、オープン・アーキテクチャーに基づく統合ソリューションであり、複数のアプリケーション、ディレクトリー、データベースにわたって情報の同期と交換を行い、アイデンティティー・データに関して企業レベルの統合されたビューを提供します。新しいIBM Security Directory Suiteは、データベース、ディレクトリー、フラット・ファイルなどのさまざまなソースをベースに、単一の情報ソース作成を支援します。ハイブリッド・アプローチを使用して一元化されたデータ・ストアを作成する一方で、元のデータソースにおけるユーザー管理と認証の機能を提供し続けることで、仮想ディレクトリー領域のさまざまなユース・ケースを解決します。またIBM Security Directory Suiteは、信頼できるアイデンティティー・データ・インフラストラクチャーを提供するのに役立つ強固なディレクトリー基盤を提供し、ミッション・クリティカルなセキュリティーと認証を実現します。柔軟でありながらスケーラビリティーの高いLDAPインフラストラクチャーであり、さまざまなオペレーティング・システムやアプリケーションと相互運用します。また、DNだけでなく電子メールや社員番号などの固有属性値で認証したり、外部のLDAPサーバーに認証をパススルーする構成も可能です。



FDS: Federated Directory Service

導入効果

- データベース、ディレクトリー、フラット・ファイルなどを統合して、単一の情報ソースを提供
- さまざまなオペレーティング・システムやアプリケーションと相互運用できる、スケーラビリティーに優れたLDAPインフラストラクチャーを実現
- 電子メールや社員番号など、DN以外の固有属性値でも認証可能
- パスワードを移行しなくても、外部のLDAPサーバーで認証できるパススルー機能

ハイブリッド/マルチ・クラウド環境のシングル・サインオン基盤

IBM Security Access Manager

IBM Security Access Managerはさまざまなユースケースにあわせ、柔軟でセキュアなアクセス管理機能を提供します。

リバースプロキシー機能

Webアプリケーションに共通のセキュリティー・ポリシーを実装し、一元的なアクセス管理を実現する製品です。ポリシー・ベースのシングル・サインオン基盤を構築することで、不正アクセスを防止しつつユーザーの利便性を向上させます。IBM Security Access Managerは完全にハードニングされた物理/仮想アプライアンスの形態で提供され、シンプルな導入/設定が可能です。既に導入設定がなされているハードウェアのほか、仮想アプライアンスはIaaS環境でも導入可能です。

Advanced Access Control Module

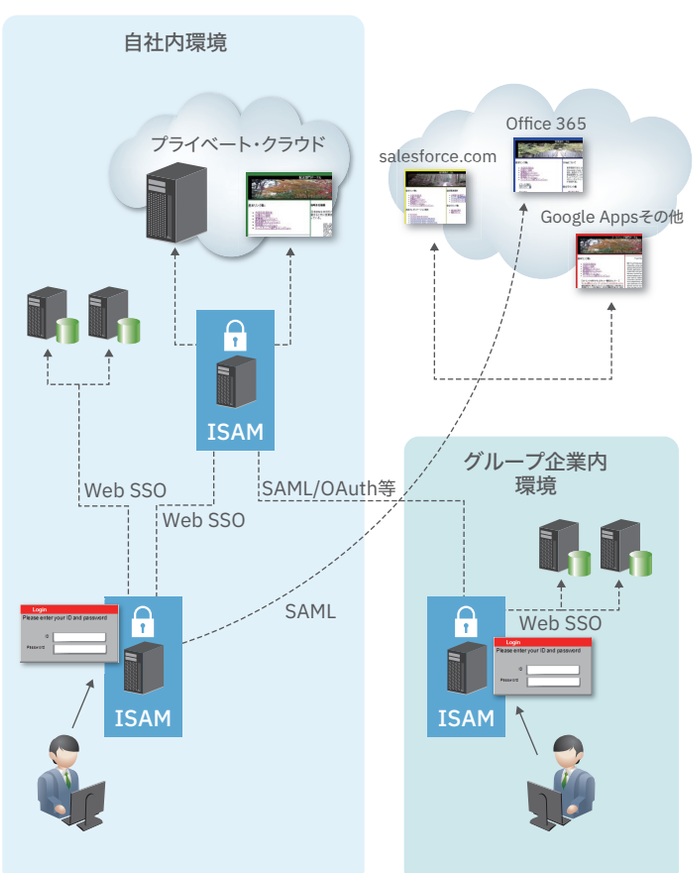
リスクベース認証や、FIDO/ワンタイム・パスワードなどの高度認証方式、またユーザー自身によるパスワード・リセットなどセルフケア機能を標準提供し、より高度なセキュリティー要件に対応します。リスクベース認証機能ではコンテキスト情報をリスク評価に利用することで、リスクが高いと判断された時のみ多要素認証を要求するなど、ユーザーの負担を増やすことなく認証強度を高めることが可能となります。さらにMaaS360、Trusteerと連携することで、より高い精度でリスク状況を判定することも可能です。

Federation Module

複数の認証ドメイン間を連携させるためのオープンな認証連携の標準技術を実装しています。既に広く展開されているSAMLやOpenID Connectをはじめとする認証連携標準を活用し、オンプレミスの企業内Webアプリケーションとクラウド・サービスなど、複数のドメインに分かれたサービスに対するシングル・サインオンを実装することができます。Federation Moduleにより、企業内Webアプリケーションの認証認可制御と共に、クラウド・サービスなどの外部ドメインのアプリケーションもその認証制御に取り込むことで、セキュリティー・ポリシーやログの一元管理など統合的なアクセス管理基盤を提供します。またIBM Security Access Managerを活用することで、クラウド・サービスなどのサービス提供者にとっても統合認証基盤として有効なソリューションとなります。

導入効果

- ●業界標準技術によりハイブリッド/マルチ・クラウド環境のさまざまなWebアプリケーションに対するシングル・サインオンを実現
- ●認証の実行点を集約することで、アクセス・ポリシーを一元管理し、多様化・複雑化するセキュリティー要件への対応が容易
- ●製品標準機能でFIDO/ワンタイム・パスワードなどの高度認証方式を容易に実装可能
- ●リスクベース認証を組み込むことで、ユーザー利便性への影響を最小化しつつ認証強化が可能
- ●認証に特化したミドルウェアとして、ブラウザからのアクセスだけでなく、API連携においても独立した機能コンポーネントして活用可能
- ●国内外で多数の実績があり、統合認証基盤に求められる高可用性/スケーラビリティーにも対応可能



■認証方式の種類と強度

What you know ユーザーの記憶情報に依存	What you have ユーザーの所有・管理物に依存	What you are ユーザー自身の特徴に依存	What you do ユーザーの振る舞いに依存 (Trusteer Pinpoint Detect連携)
・ユーザーID/パスワード ・合言葉 ・PINコード ・パスフレーズ など	・クライアント証明書 ・ICカード ・USBキー ・ワンタイム・パスワード・デバイス など	・生体認証 ・指紋 ・声紋 ・虹彩 など	・振る舞い分析 ・行動履歴 など

リスクベース・アクセス制御

デバイスのシステム環境やアクセスしてくる場所などのリアルタイム情報を使いリスクスコアを算出し、アクセスを拒否したりより追加認証を求める等の設定が可能

機器特性 / システム環境 / アクセス先のリソース / 場所 / ユーザー特性

クラウド・アプリケーションへのシングル・サインオンを実現するIDaaS基盤

Cloud Identity Connect / Cloud Identity Verify

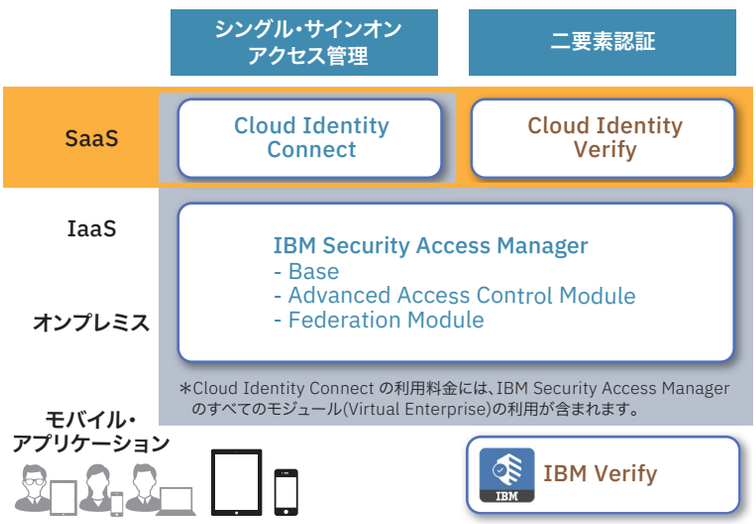
働き方改革や、デジタル・トランスフォーメーションを背景に、ユーザー・アクセスやアプリケーション基盤が多様化し、アプリケーションへのアクセス正当性を担保することが課題となっています。アプリケーション、ユーザー、利用環境、デバイスの多様化により、ユースケースは多様化しています。クラウド・アプリケーション（SaaS）におけるシングル・サインオンによるアカウントの統合や、不正アクセスを防止する二要素認証を実現します。

Cloud Identity Connect

クラウド・アプリケーション（SaaS）への認証連携（フェデレーション）によるシングル・サインオンを実現するIdentity as a Service(IDaaS)基盤です。クラウド・アプリケーション（SaaS）への連携設定（コネクター）を数多くあらかじめ用意してあり、統合環境を簡単に構成することができます。アイデンティティー・プロバイダー（IdP）として、あらかじめ定義されたテンプレートまたはカスタム・テンプレートを使用して、さまざまなアプリケーション・サービス・プロバイダー（クラウド・アプリケーション・SaaS）と統合できます。サービス・プロバイダー（SP）として、複数のアイデンティティー・プロバイダー（IBM Security Access ManagerやMicrosoft Active Directoryなど）と統合し、それらを使用してユーザーを認証できます。

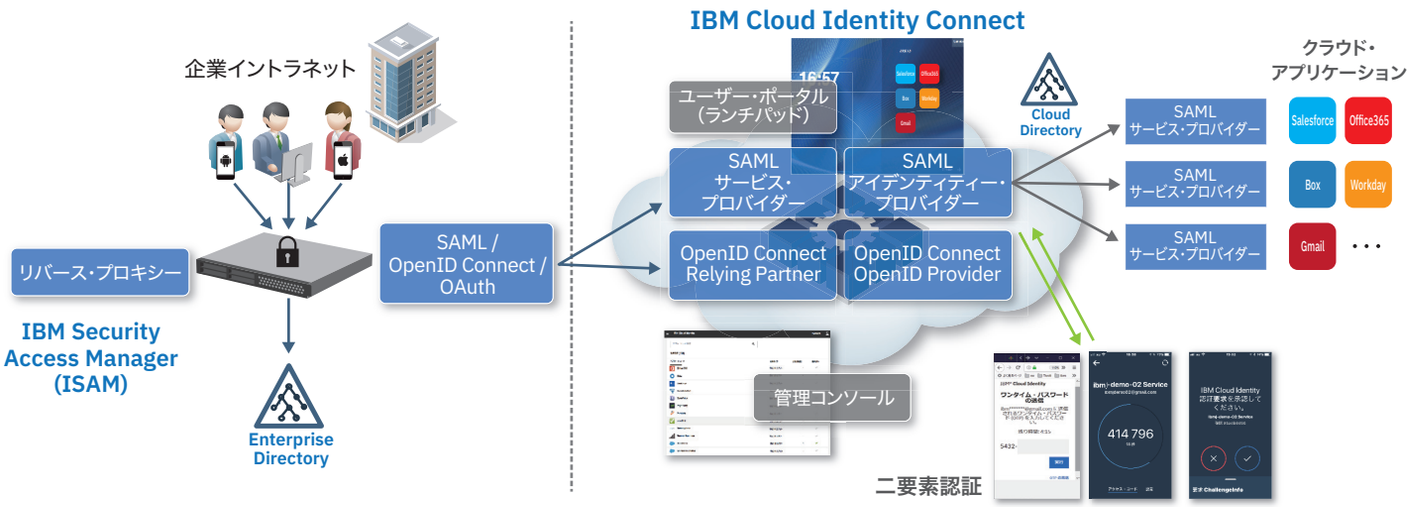
Cloud Identity Verify

Authentication as a Serviceとして、e-mailやSMSや時刻ベースのワンタイム・パスワードやデバイスによる認証を提供します。モバイル・デバイスを用いた認証のためのモバイル・アプリケーションとして、IBM Verifyを提供します。また、モバイル・デバイス管理であるIBM MaaS360と統合することにより、信頼できるデバイスおよびアプリのみがアクセスできるように構成されたシングル・サインオンを実現します。



導入効果

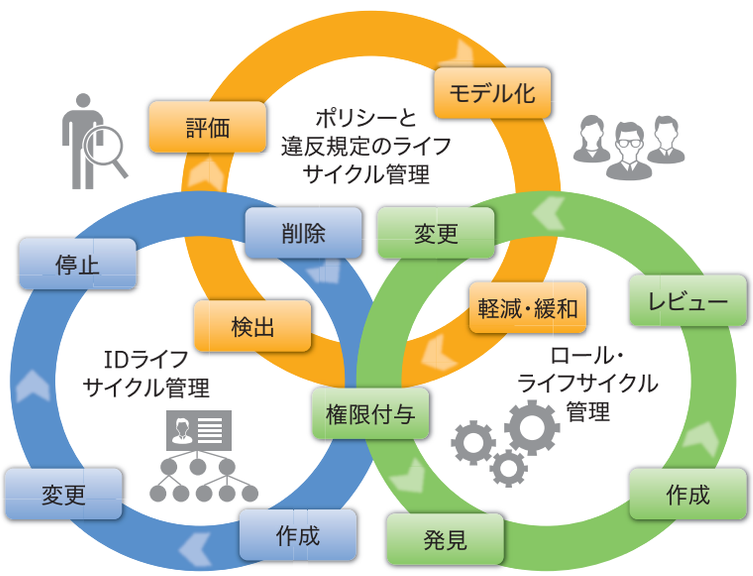
- クラウド・アプリケーション（SaaS）ごとにアクセス管理されたシングル・サインオンを設定することにより、アカウントを統合してセキュリティー要件へ対応することができます
- クラウド・アプリケーション（SaaS）ごとのセキュリティー要件に合わせた二要素認証を設定することができます
- クラウド・アプリケーション（SaaS）へのユーザーのログインを統合的に管理することができます
- REST APIを提供しています、外部アプリケーションからの管理や操作を開発することができます
- ライセンスには、IBM Security Access Managerフルライセンスが包含されており、豊富な拡張機能を使ったオンプレミスでの構築ができます



情報アクセスの権限管理とガバナンスの向上支援

IBM Security Identity Governance and Intelligence

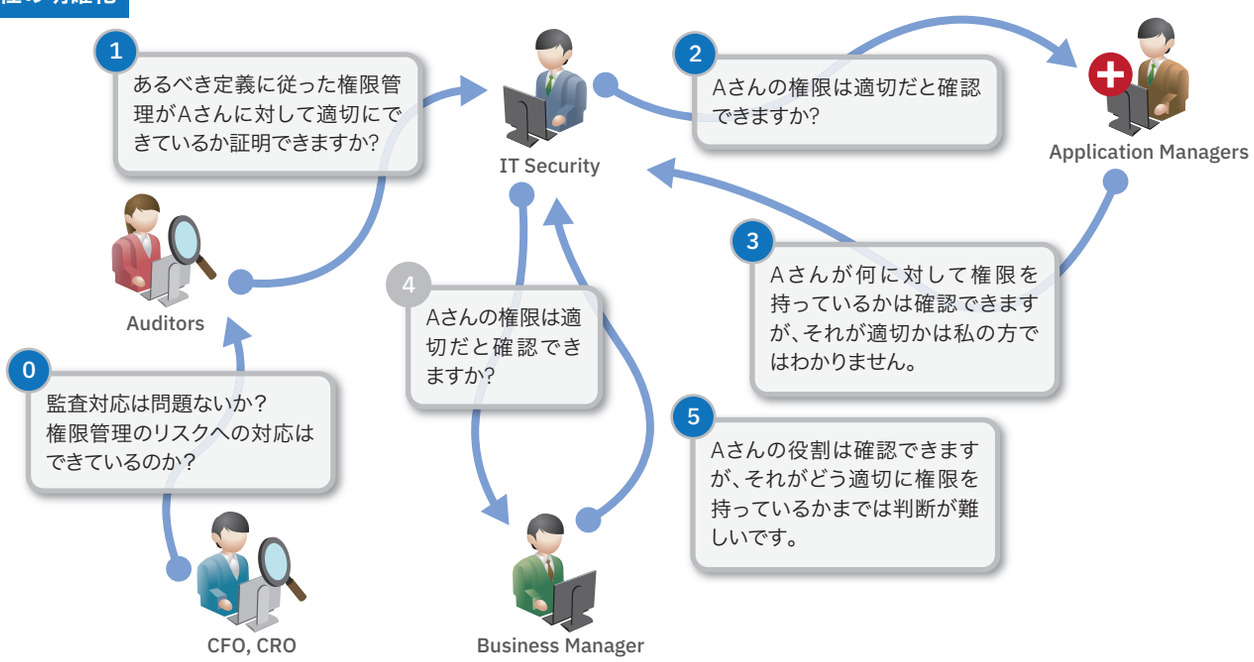
ユーザーやその権限に関わるライフサイクル管理（IDライフサイクル、ロール・ライフサイクル、ポリシーと違反規定のライフサイクル）をシステム化し、漏れのないセキュアなユーザー・アクセス環境の維持運用を実現します。
本製品にはIBM Security Identity Managerのライセンスも含まれております。



導入効果

- さまざまなシステムに散在しているID情報の不整合や不適切なアクセス権限、手作業に依存したID情報の棚卸しなど、IDライフサイクル管理の課題を解決します
- 膨大なロールのタイムリーな評価やロール設計の効率化、権限付与の妥当性判断など、ロール・ライフサイクル管理の課題を解決します
- 権限分掌の徹底や適切なアクセス権の承認、監査に対応したレポーティングなど、ポリシーと違反規定のライフサイクル管理の課題を解決します

権限責任の明確化



監査の際に問題点となる点を解決します

アクセスが承認された背景が不明確
- 誰が承認した権限なのか
- その権限は現在も有効であるべきか

アクセス権限の問題点を検知する仕組みが無い
- 一般ユーザーに認められてしまう重要データへのアクセス権
- アクセス権の不整合（SoD）

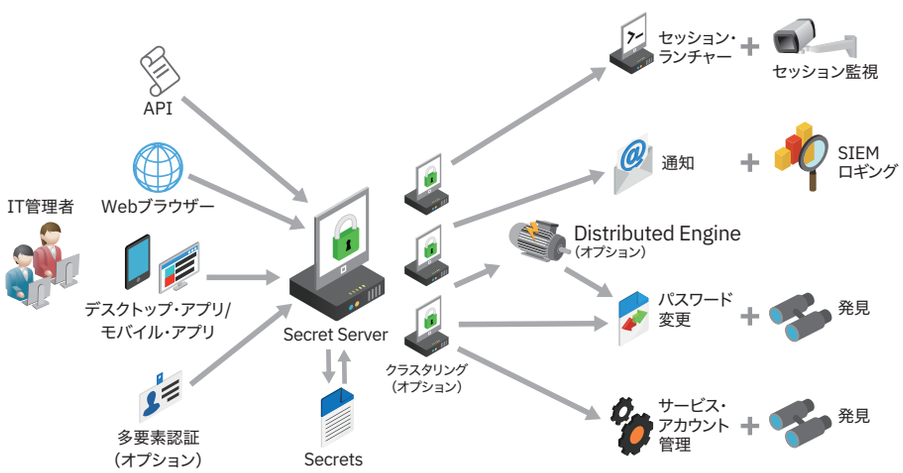
権限管理が手作業に依存してしまっている
- 作業の実施に膨大な時間がかかる
- 第三者機関に依頼する際などの費用が膨大

CEO/CFO

特権アカウントを簡単に発見・管理・監査・監視

IBM Security Secret Server

IBM Security Secret Serverは、システム全体から特権アカウントを見つけ出しセキュアに管理された状態に容易に移行します。特権アカウント利用はワークフローにより管理され、自動パスワード管理機能を通じてパスワード・リセットや要求元ユーザーに対するパスワード隠匿で不正利用のリスクを防止します。貸し出された特権アカウントによってどのような操作を実施したかを動画として記録し、管理者が後で監査やトラブル・シューティング目的で再生することができるセッション・レコーディング機能も提供します。アプリケーションやスクリプトなどのファイルに組み込まれた特権アカウントのセキュアな管理も実現します。また、要求元ユーザーが直接アクセスできないネットワークにある環境のアクセスもDistributed Engineにより実現します。さらにエンドポイント側でのマルウェアの停止やポリシー制御による最小特権の適用も実現します。(オプション)



導入効果

- 特権アカウントのチェックイン/チェックアウトの仕組みによる、セキュアな特権アカウント利用
- 特権アカウントの申請、承認などのワークフロー管理で、セキュリティー事故のリスク軽減、コンプライアンス強化を実現
- 特権アカウントの使用記録により、管理者責任の明確化、耐監査性を向上
- 特権アカウントのパスワード管理自動化で、パスワードの使い回しや漏えいを防止することでセキュリティーを向上

Discover : 発見

- システム全体から特権アカウントを検出
- 特権アカウントをセキュアに管理された状態に容易に移行
- 特権アクセスを管理するためのプロセスの導入

Manage & Audit : 管理と監査

- 特権アクセス取得のためのワークフロー確立
- 特権アカウントのパスワードとSSH鍵の安全な管理
- チェックイン/チェックアウト機能を備えたID vault機能の提供
- パスワード/SSH鍵の自動ローテーションと変更
- コンプライアンス・レポート作成のために、アクティビティーの包括的な監査証跡取得

Monitor & Control : 監視と制御

- 特権アカウントが、いつ、どのように、なぜ利用されているかの正確な把握
- 監査およびフォレンジックのための特権セッション・アクティビティーの記録と監視
- エンドポイント側でのマルウェアの停止(オプションのPrivilege Managerにより提供)

Secure and Protect : 安全と保護

- 特権アカウントの不正使用防止
- エンドポイントに対する「最小特権」ポリシー適用
  (オプションのPrivilege Managerにより提供)
- エンドポイント・ユーザーのローカル権限に関するポリシー定義/適用
  (オプションのPrivilege Managerにより提供)

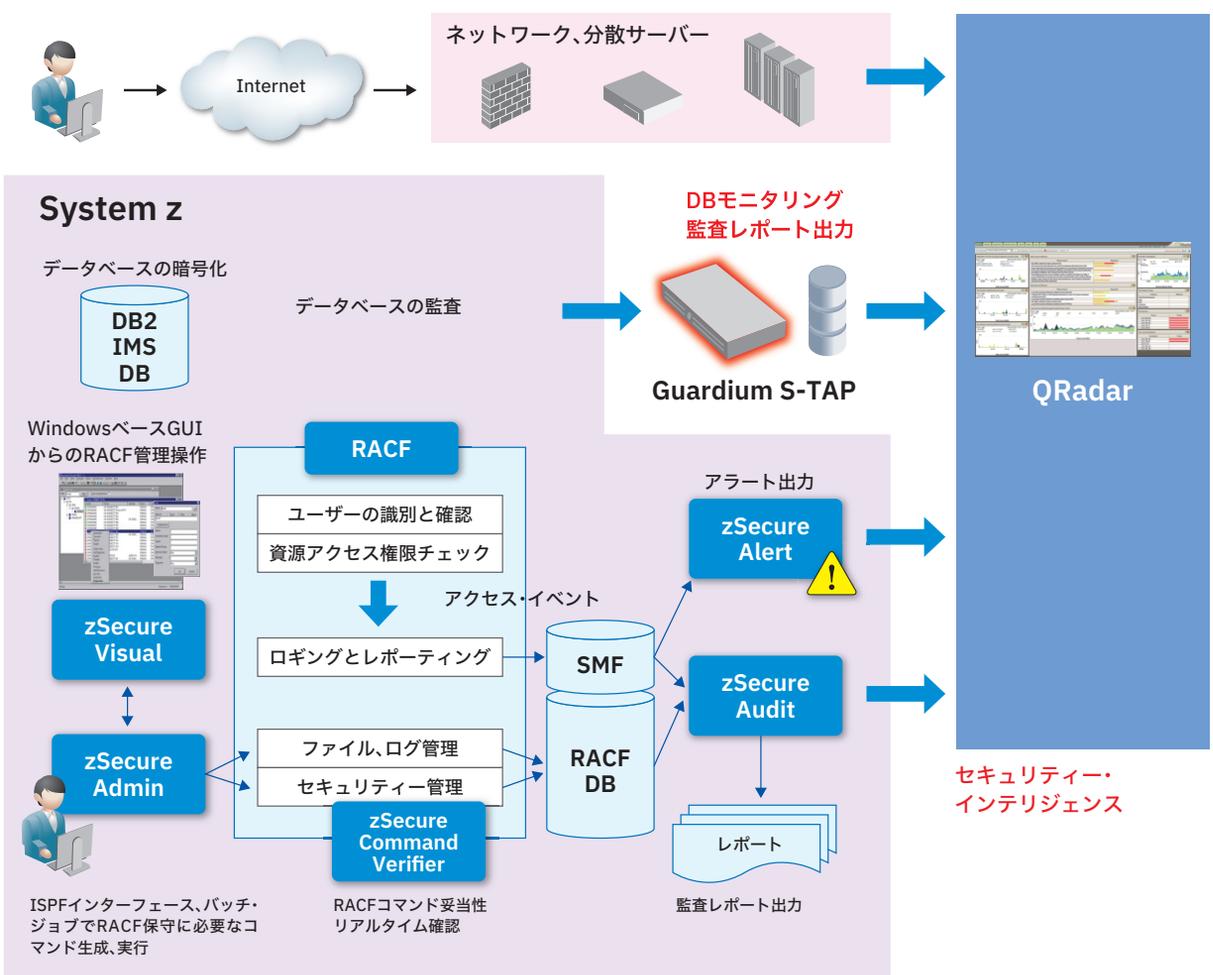
メインフレーム・セキュリティー管理

IBM Security zSecure Suite

IBM Security zSecure Suiteはメインフレームのセキュリティーの管理、脅威のモニター、ポリシー・コンプライアンスの運用、使用状況 と構成の監査、および、コンプライアンス管理と監査レポートの作成に役立つように設計された複数の個別の製品で構成されています。IBM Security zSecure Admin、IBM Security zSecure Visual は RACF 管理やプロビジョニング、IBM Security zSecure Auditは各種監査レポートの作成、IBM Security zSecure Command Verifierは特権ユーザー管理、IBM Security zSecure Alertはセキュリティー違反に至らないさまざまなインシデント発見を効率化します。これらのコンポーネントは、管理に要する時間、労力、およびコストの大幅な削減が可能で、生産性の向上、応答時間の短縮、さらに、新任管理者のトレーニングに必要な時間の削減に役立ちます。

導入効果

- セキュリティー・ポリシーの適用、監査、モニター、およびコンプライアンス管理機能を提供
- コンプライアンス監査のための負担を軽減
- コンプライアンスおよびモニターを実施する時間とコストの節減
- セキュリティーおよび問題の処理を改善し、全体的な運用効率の向上

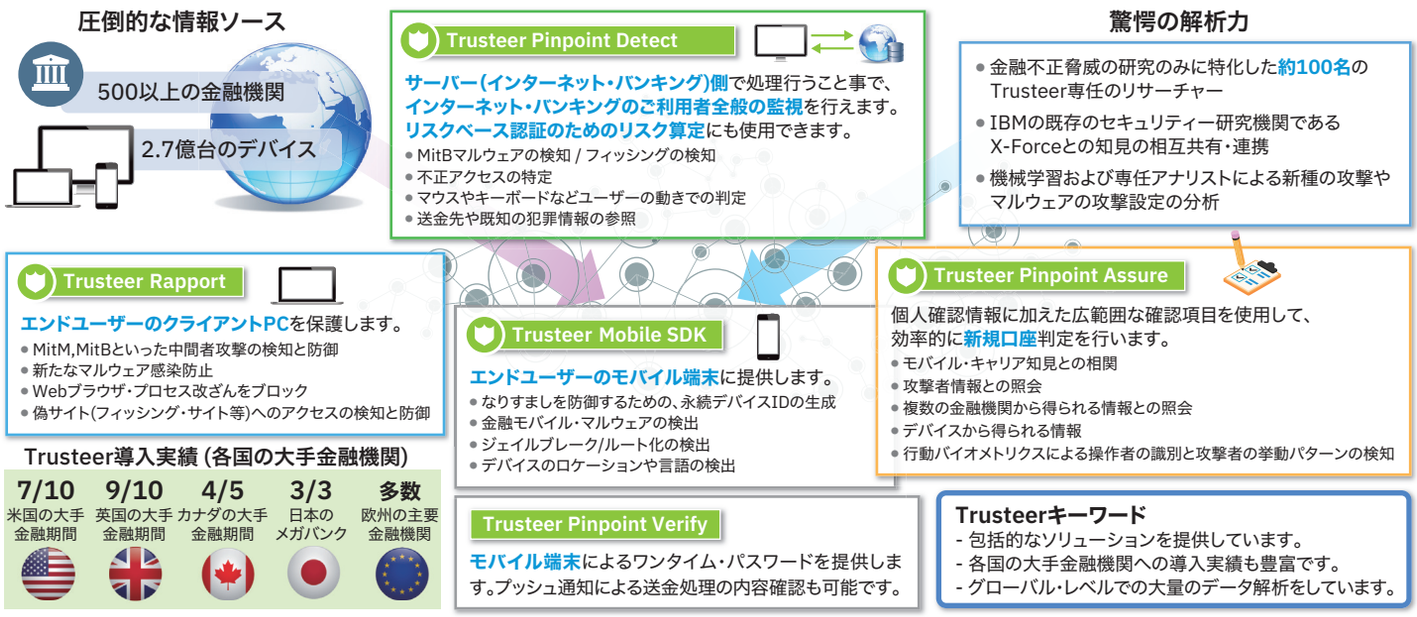


金融不正対策 / 不正アカウント検知 / リスクベース認証用分析

Trusteer Pinpointシリーズ / Trusteer Mobile SDK / Trusteer Rapport

Trusteerは、新たな犯罪ロジックを迅速に検出、分析、適応するために、エンドポイント保護技術とリアルタイム・インテリジェンスの専門的な分析を組み合わせた、ユニークなプロセスを作成しました。Trusteerのサイバー犯罪防止アーキテクチャーは、オンライン・サービスをご利用になる、法人・個人のお客様を、アカウントの乗っ取り、資格情報の窃取や不正取引から保護することを可能にします。

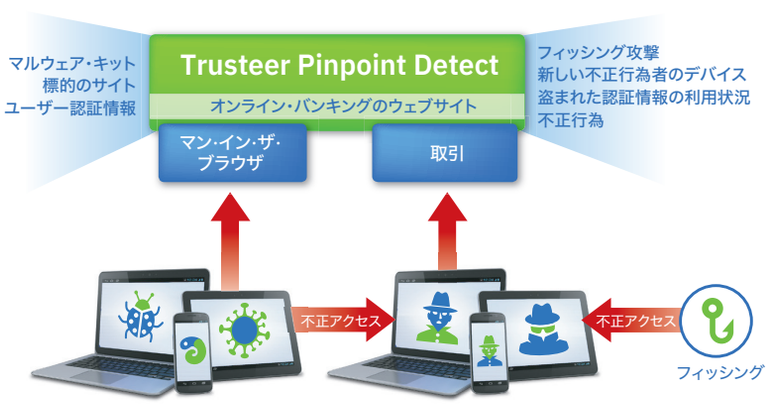
■ Trusteer の金融不正対策 / 金融不正対策 / 不正アカウント検知 / リスクベース認証用分析



Trusteer Pinpoint Detect / Trusteer Pinpoint Assure / Trusteer Pinpoint Verify

Trusteer Pinpoint Detectは、フィッシング攻撃、マルウェア感染、危険にさらされた資格情報、高度な回避手段を検出するためのさまざまな重大不正行為指標を、デバイス、地理位置情報、ユーザー・プロファイルおよびトランザクション・モデルに関連付けて、不正行為をさらに正確に検出することができます。Trusteer Pinpoint Detectが提供する行動バイオメトリクス機能は、特許取得済みのジェスチャー・モデルのコグニティブ分析によって、キーボード・タイピングや微妙なマウスの動きを識別し、複数のセッションにわたって各顧客の行動を継続的に学習し、その行動を分析します。オンラインサービスの顧客とオンラインサービス・ウェブサイト間の実際のやりとりとは異なる動作を検出することで、不正ユーザーによる盗まれた認証情報を利用したオンラインサービス・アカウントの乗っ取りを検知します。Trusteer Pinpoint Assureは、オンラインの新規不正口座開設を検知します。Trusteer Pinpoint Verifyは、スマホと連携し、電子メール、SMS、タイムベースのワンタイム・パスワード、QRコード、全体認証、プッシュ通知を使用した追加認証のためのソリューションです。

■ 不正行為のクライアントレス検出



導入効果

- マルウェア感染や不正アクセスを決定的に識別・通知し、効果的な金融機関の認証プロセスおよびアクセス制限を実現
- 特定のマルウェア・キット、標的の金融機関、攻撃の種類、および盗まれた認証情報を特定し、マルウェアの検知を実施
- リアルタイムでフィッシングやスピアフィッシング攻撃のデータを収集
- モバイル・オンライン・バンキングの不正を防止するために、デバイス・リスクスコアの活用を可能にする
- デバイスとアカウント・リスクを相関させ、アカウントの乗っ取りを検出

Trusteer Pinpoint Malware Detection

Trusteer Pinpoint Malware Detection（PPMD）はアクティブな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します。

※Trusteer Pinpoint Malware Detectionは、Trusteer Pinpoint Detectに包含されます。

導入効果

- ●マルウェア感染や不正アクセスを決定的に識別・通知し、効果的な金融機関の認証プロセスおよびアクセス制限を実現
- ●特定のマルウェア・キット、標的の金融機関、攻撃の種類、および盗まれた認証情報を特定し、マルウェアの検知を実施

Trusteer Mobile SDK

Trusteer Mobile SDKは、マルウェア感染と潜在的なセキュリティー・リスクを検出するために、デバイスをスキャンします。またTrusteerのインテリジェンス・センターは、新たな脅威を識別し、新しい犯罪ロジックを解析し、対策を作成し、新種のモバイル・マルウェアの脅威に適応します。また、Trusteer Pinpoint Detectと連携し、より高度な異状分析を実施し、Trusteer Pinpoint Detectで検知可能とします。

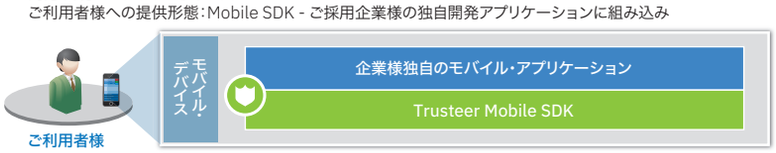
導入効果

- ●マルウェア感染やデバイスのリスクを検出・警告することで、モバイル・デバイスを保護
- ●本物のサイトに属するオンライン・バンキングのIPアドレスとSSL証明書を検証し、マン・イン・ザ・ミドル（ファーミング）の攻撃をブロック

Trusteer Mobile の概要

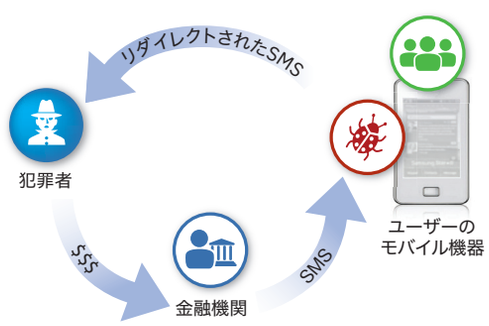
対応環境：Android および iOS

ご利用者様への提供形態：Mobile SDK - ご採用企業様の独自開発アプリケーションに組み込み



主な機能

永続デバイスIDの付与	金融モバイル・マルウェアの検知	SMS傍受など疑わしいスタートアップ・アプリケーションの検知	ジェイルブレイク/ルート化の検出	ジェイルブレイク/ルート化秘匿技術の検出
OSパッチ適用有無の検出	セキュアでないWiFi接続の検出	Google Play store公開アプリケーションのみのインストール許可設定の検出	デバイスのロケーションや言語の検出	Web管理コンソールでリスク・イベントの閲覧



犯罪者はソーシャル・エンジニアリングを用いてユーザーを騙し、彼らがモバイル機器にマルウェアをインストールするように仕向けます。
不正取引は、SMS認証をトリガーし、その認証がモバイル・マルウェアによって傍受され、犯罪者に送信されます。

Trusteer Rapport

Trusteer Rapportは、個人情報を引き渡したり、不正取引を承認するように被害者を誘うような悪意のあるWebページのインジェクションを防止するために、ブラウザをロックダウンします。またTrusteer Rapportは、正規のサイトに属するオンライン・バンキングのIPアドレスおよびSSL証明書などを検証することにより、マン・イン・ザ・ミドル攻撃をブロックします。

導入効果

- ●ブラウザとOSをロックダウンすることにより、エンドポイントを保護
- ●アカウントの乗っ取りやクロス・チャネル不正を犯すのに使用されるログイン資格情報と個人情報の盗難を防止
- ●エンドポイントから既存の金融マルウェアを除去し、ブラウザの脆弱性の悪用およびエンドポイントでのマルウェアのインストール攻撃を防御

iOS/AndroidやWindows 10/macOSなどのPCを含めた統合エンドポイント管理をWatsonが支援

IBM MaaS360 with Watson

スマートフォンやタブレット端末からWindows 10やmacOSなどのPCまで、自社のセキュリティー・ポリシーに応じ、遠隔操作(リモートロック/ワイプ)や端末管理を、異種混在の状態でも一元管理することができるソリューションです。IBM MaaS360 with Watsonは、モバイル・デバイス管理(MDM)、モバイル・コンテンツ管理(MCM)、モバイル・アプリケーション管理(MAM)を包括した、統合エンドポイント管理(UEM)を実現するソリューションだけでなく、Watsonによるコグニティブ・エンジンを用いて、エンドポイント管理における状況に応じた最適なベストプラクティスを提供し運用効率の最大化支援、最新の脅威検知対策を提供します。

導入効果

- コグニティブ・エンジンによる統合エンドポイント管理のベストプラクティス、最新の脅威対策を支援
- 迅速なモバイル・デバイス登録を実現、管理者、ユーザーそれぞれ負担を軽減
- ユーザー所有のデバイスから安全にメールやWebアクセスができるアプリケーションを提供
- SharePoint、Windowsファイル共有、企業内のリソースの認証、暗号通信によるアクセスを実現
- コンテナ向けにドキュメントを配布、認証によって使用許可を付与。データ漏えい防止機能で重要情報を保護
- モバイル・マルウェアおよびリスクのあるデバイスを検出し、迅速な対応まで実現

IBM MaaS360が提供するセキュアな統合エンドポイント管理

セキュアかつシームレスなアクセス

Secure Productivityアプリケーションによるコンテナ内でのデータ使用

クラウド・アプリケーションへのコンテキストに基づくアクセスとシングル・サインオン

複数要素による認証

先進のデータ保護

マルウェア検知

グローバルの脅威情報をもとにしたセキュアなインターネット・ブラウジング

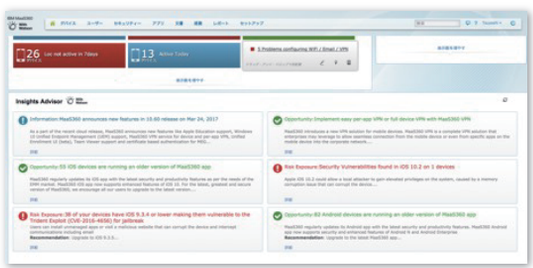
デバイスに依存しないネットワーク・ベースの保護

可視化と管理

場所に関わらずあらゆるデバイスを可視化

インテリジェントなポリシーとコンプライアンス・ルール

リスクおよび脅威を検知・対策



MaaS360の管理デバイスから収集・集計した情報とサードパーティーの構造化/非構造化データをコグニティブ・エンジンにより分析し、管理者へアクションの提案を行います。

■ 全方位をカバーする統合エンドポイント管理 (UEM)
- Editionと提供機能

Enterprise Edition
マルウェア・脅威管理と更に高度なビジネス文書の活用をされるお客様へ

Premier Edition
ビジネス文書、Webアクセス、VPNなど社内システムに積極的にアクセスされるお客様へ

Deluxe Edition
管理機能に加えてメールをセキュアに利用されるお客様へ

Essential Edition
ゴグニティブUEMのファースト・ステップ

デバイス管理 / アプリ管理 / ID管理 / With Watson® アドバイザー / セキュアコンテナー / 経費管理

セキュアメール

文書管理 / OS VPN

セキュア・ブラウザー / アプリ・セキュリティー

文書エディター / 文書同期 / マルウェア・脅威管理

重要データ保護プログラム

重要データの所在の実態を把握することは、有効なデータ保護における不可避な課題です。本サービスは、Crown Jewelと呼ばれる組織の最重要なデータを特定し、所在を把握します。それを基に、アクセス・移動の統制、データ保護、リスクの可視化と管理を実現します。

お客様の課題／要望

- 絶対に守るべきデータを特定し、その所在を把握したい
- データの取扱いに関するコンプライアンス確保と漏えいリスク低減を図りたい
- データのライフサイクルを通したデータ保護アプローチを効果的に実現したい

IBMがご提供する価値

- 企業の機密データや重要データの所在を明らかにするディスカバリー
- コンサルティングと製品が一体となったデータ保護ソリューション導入
- ライフサイクルでのデータの管理・監視
- データのアクセス・移動に対する確実な統制

Crown Jewels

組織内で最も重要かつビジネスにとってクリティカルなデータ

- 顧客データ
- 買収・売却計画
- 知的財産
- エグゼクティブや株主との審議内容 など
- 極秘の計画や手法など

- **Data discovery and classification**
  お客様のさまざまな部署や事業に分散したデータに対して、自動化されたツールを用いてディスカバリー、機密データを分類
- **Data security strategy and architecture design**
  お客様固有のビジネニーズに即したデータ保護戦略の策定、データ保護施策のロードマップ作成
- **Data loss prevention and encryption**
  データ保護のためのテクノロジーの導入
- **Data security framework and lifecycle management**
  データのライフサイクル全体を通じた保護・監視、それらにかかる計画の策定

■ 5 つのステップで持続的に ”Crown Jewels” のセキュリティーを実現

IBM Critical Data Protection Program

特定 DEFINE	発見 DISCOVER	基準 BASELINE	保護 SECURE	監視 MONITOR
Crown Jewelsを特定する •データ・セキュリティー戦略の全体像を理解 •データ保護の目的を定義 •組織のデータモデルとデータ分類方法を開発	**ITシステム内にあるCrown Jewelsを発見する** •データが存在する環境、インフラストラクチャー、ライフサイクルを理解 •反復的な発見、分析、分類	**Crown Jewelsの保護策の基準を定める** •基準となるデータ・セキュリティー要件を確立 •現在のデータ・セキュリティー・プロセスとコントロールを評価 •基準と現状とのギャップと解決策を特定	**Crown Jewelsの保護策を計画・設計・実装する** •技術やプロセス変革の計画策定と優先順位付け •重要データの保護、適正なアクセス権、ビジネスの成長目標に合わせたソリューション設計と実装	**Crown Jewelsに係るリスク状況を監視する** •データ・セキュリティー・ガバナンス・フレームワーク、リスク評価指標、プロセス監視手法を開発 •データ保護の戦略と方法論を定期的に検証

◆ DataDiscovery & Classification

◆ Data Security Strategy & Architecture Design

◆ Data Security Framework & Lifecycle Management

ソリューション(製品)
◇IBM Security Guardium　◇Symantec Data Loss Prevention
◇IBM Data Risk Manager　◇Skyhigh

◇Identity and Access Management

◇IBM Security Key Lifecycle Manager
◇z14 Hardware 暗号化

◇QRadarSIEM

※お客様の環境やご要望に応じて、
いずれのステップからでも開始できます。

Secure by Design レビュー

IBMのセキュリティー成熟度アセスメント・フレームワーク（10Essential Practices）に基づき、セキュア・アプリケーション開発について評価します。アプリケーション開発にガバナンスを確立し、技術、プロセス、組織、評価方法を包括的に改善します。また、セキュリティー要件と脅威、アプリケーションの脆弱性に体系的な管理を導入します。

IBMがご提供する価値

- アプリケーション開発に関するガバナンスを確立し、技術、プロセス、組織、評価方法を包括的に改善
- アプリケーションに対するセキュリティー要件と脅威、アプリケーションの脆弱性に体系的な管理を導入

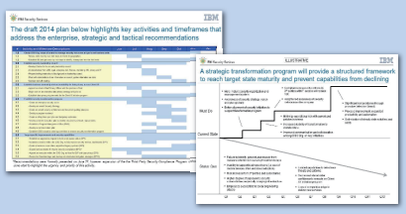
お客様の課題／要望

- アプリケーションの新規開発についてのガバナンスの確立
- アプリケーションの脆弱性の要因を早い工程で摘み取る開発スタイルの定着
- 工程が進んでから、充足されていないセキュリティー要件が発覚する事態の回避

評価のカテゴリーと評価項目（抜粋）	
Technology（IT技術の活用）	脆弱性分析ツール、コンポーネント管理能力、承認されたアプリケーション・コンポーネントのリスト...
Process（運用ルール）	ソースコード管理、共通アプリケーション開発プロセス、リスク評価と脅威分析、セキュア・コーディング...
Organization（組織の確立）	開発者・非開発者のセキュリティー教育、セキュア・ソーシング、セキュア開発の役割と責任...
Metrics（評価方法）	セキュリティー品質、サービス・インテグリティー、サービス品質、セキュア・サービサビリティー...
Governance（全社的な仕組み）	SDLCセキュリティー戦略、プログラム・ガバナンス委員会、エグゼクティブ・スポンサーシップ...

成熟度による評価

セキュア・アプリケーション開発における
- ギャップの特定
- 対策の提示
- ロードマップの策定



ご参考 IBM Securityの強み②-あらゆる産業における豊富な実績

- **98%** の世界トップの金融サービス企業・銀行
- **95%** の米国トップのヘルスケア企業
- **94%** の世界トップの製薬・バイオテクノロジー企業
- **50** の州政府と米軍の全5軍
- **70** の米国の有数のカレッジや大学
- **12** の米国トップの航空宇宙・防衛企業
- **27** の世界トップのエネルギーおよびユーティリティー企業
- **22** の米国トップの小売・消費財企業
- **10** の世界最大手の通信会社
- **8** の世界トップの航空会社
- **19** の世界トップの自動車・部品メーカー
- **43** の米国トップの製造企業

IBM は業界をリードするためにコミットしています

12 アナリストがIBMセキュリティーを「リーダー」として評価したマーケット・セグメント

- セキュリティー・アナリティクス
- エンドポイント:クライアント管理ツール
- ID ガバナンス
- アクセス管理
- Identity as a Service (IDaaS)
- ID管理
- データベース・セキュリティー
- アプリケーション・セキュリティー
- エンタープライズ・モビリティー管理(EMM)
- Webの不正検出
- マネージド・セキュリティー
- 情報セキュリティー・コンサルティング・サービス

IGAコンサルティング・構築支援サービス
(Identity Governance & Administration)

ゼロ・トラスト・セキュリティーでは、厳格な認証/認可が求められ、それらの前提となるアイデンティティー管理/ガバナンスが要求されることになります。また、働き方改革におけるRPA活用、リモート・アクセスなどにおける人以外のIDの管理も必要になってきています。当サービスでは、現状の課題だけではなく将来の要件まで取り込んで、あるべきIGAをシステム、プロセス合わせて実装、運用することを支援します。

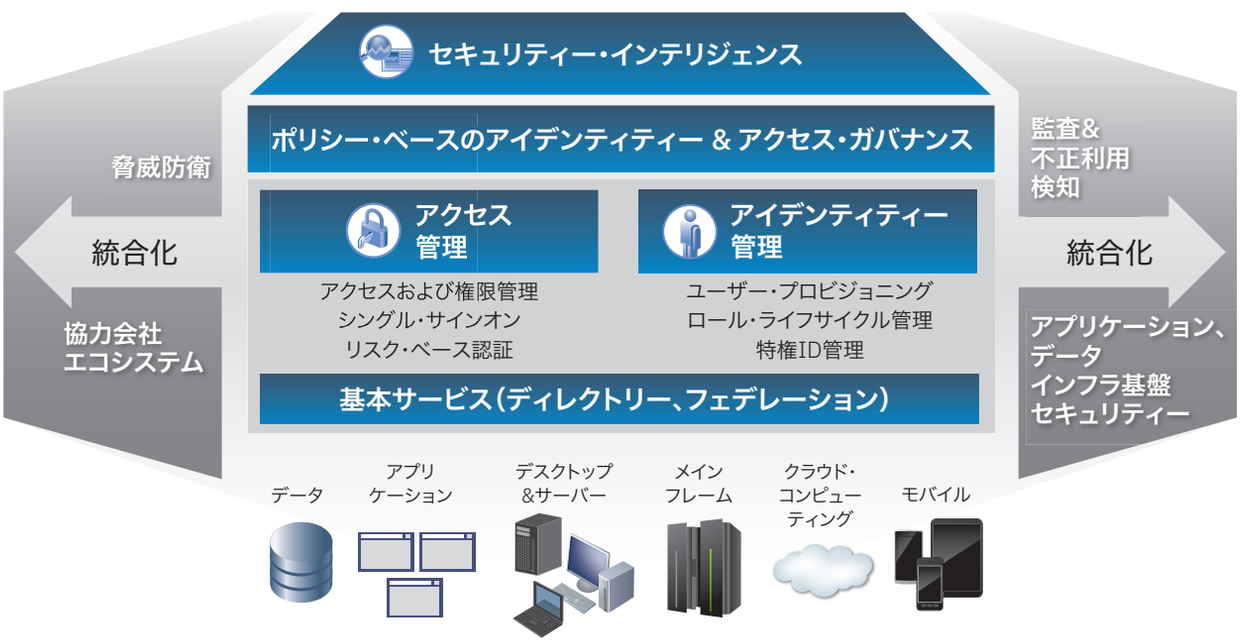
お客様の課題／要望

- クラウド活用における認証・認可をより厳格に行いたい
- RPA、リモート・アクセスをよりセキュアに実現、推進したい
- 自組織のセキュリティー管理/ガバナンスを今より一段階引き上げたい

IBMがご提供する価値

- 厳格な認証、認可を実現するためのIDライフサイクルにあった設定変更の運用工数削減および人手による設定ミスの削減
- セキュリティー監査への迅速な対応
- RPA、リモート・アクセス環境含めたIDを一元管理することによる、SIEMでの監視範囲の拡大、セキュリティー強化
- 新しいビジネス、環境変化へのIT対応速度の加速

■ IBM IGA戦略フレームワーク



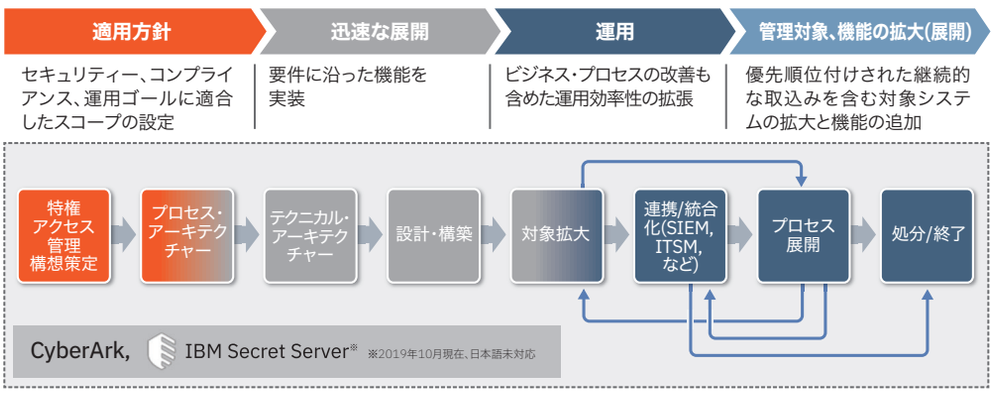
主要テーマ例		
標準IAMおよびコンプライアンス管理	**セキュア・クラウド、モバイル、ソーシャル・ネットワーク**	**内部脅威およびIAMガバナンス**
ビジネスへのアイデンティティーおよびアクセス・インテジェンスを提供するためのIAM垂直展開; データ、アプリケーション、インフラ基盤へのユーザー・アクセスの強制に対する垂直統合	証跡、確認および認証ソリューションの統合化と同様なクラウド、モバイル、SaaSアクセスに対するコンテクスト・ベースのアクセス管理	特権ID管理運用の継続的展開とID&ロール管理の展開

特権アクセス管理システム構築支援サービス

外部からの攻撃者や内部犯行者による特権アカウントの悪用防止、不正使用のリアルタイム検知、レポート作成などを可能とする、特権管理における統合的セキュリティー対策ソリューションを提供します。

お客様の課題／要望

- 法令、監査などで特権アクセス管理についてより厳格な管理が求められている
- 特権アクセス管理の労力を減らしたい
- クラウドの管理コンソールのセキュリティーを強化したい
- スクリプトやプログラムに記述(ハードコード)されたID/パスワードを管理したい



IBMがご提供する価値

- 特権管理について、運用プロセスの最適化とシステム化による特権管理運用業務の効率化、省力化
- オンプレ、クラウド含めた特権アカウントの一元管理化することによる特権アカウントと利用者を可視化、統合管理が可能
- 特権アカウントのパスワードの秘匿化やパスワード自動変更機能により、攻撃者含む利用者が特権アカウントを悪用するリスクの最小化
- 特権アカウントの作業はすべて記録され、事後検証だけでなく、異常行動をリアルタイムに検知、アラート、監視、強制停止などが可能
- スクリプト、プログラムの組込み特権アカウントに対する、パスワード秘匿化によるセキュリティー確保

統合認証基盤構築 / 認証連携・多要素認証実装支援サービス

ITインフラ、サービスのクラウド化に伴い、シングル・サインオンの範囲もオンプレだけですまなくなってきました。また、ID/パスワードだけの認証からよりセキュリティー強度の強い認証が求められています。当サービスでは、運用・展開まで考えた認証基盤構築、実装支援を提供いたします。

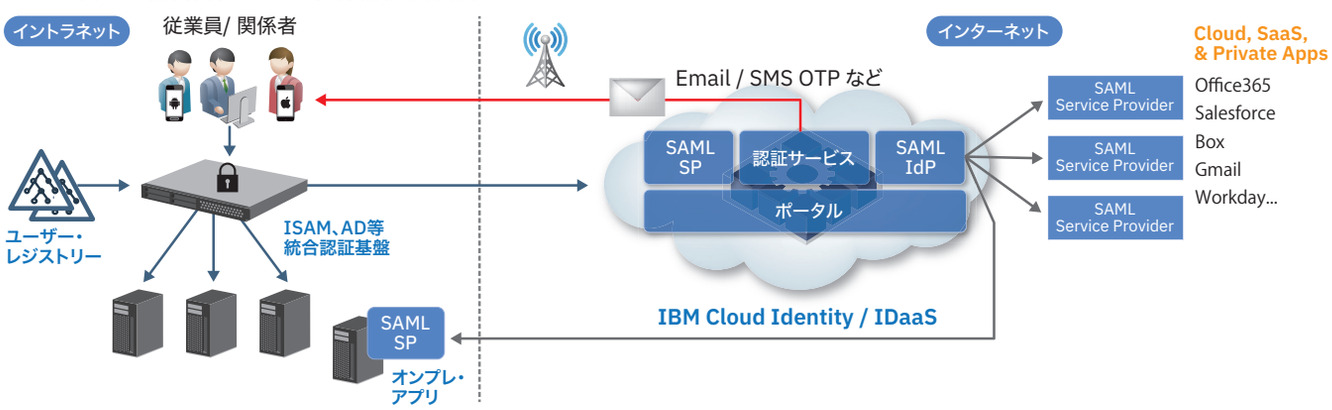
お客様の課題／要望

- オンプレだけでなくSaaSなどのクラウド環境まで含めたシングル・サインオンを実装したい
- ゼロ・トラスト実現、サイバー攻撃に向けたセキュリティー強度の高い認証をユーザーに提供したい
- 認証にかかる運用を効率化したい

IBMがご提供する価値

- サービスがどこにあるかを意識しないで利用できる利便性の向上
- 多要素認証による、確実な本人確認による、サイバー攻撃への確実な対抗策
- 認証運用における作業効率の向上
- お客様のIT環境、運用要件に最適な認証(認証連携方式、認証トークン、運用プロセスなど)実装による認証業務負荷軽減

■ クラウド含めた統合認証基盤・多様認証実装例



卓越した専門性 / X-Force

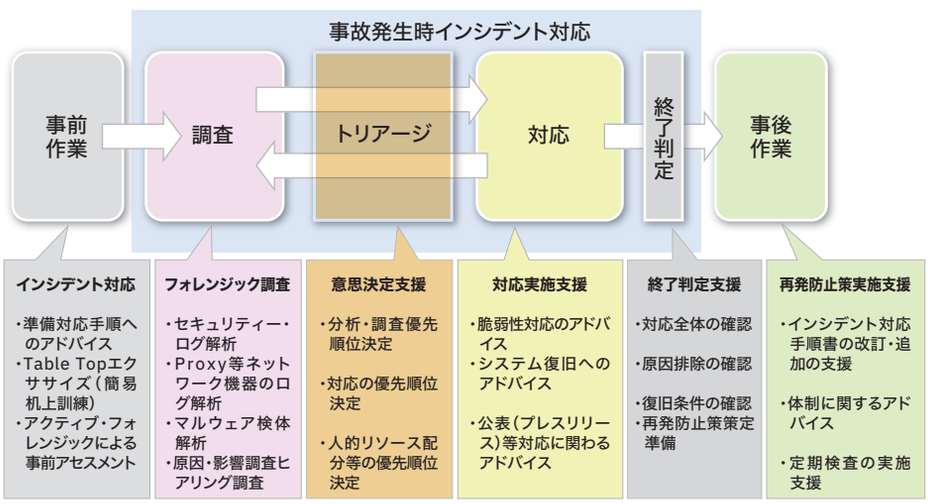
インシデント・レスポンス / X-Force Incident Response and Intelligence Services (XF-IRIS)

IBM X-Force IRIS Vision Retainer (インシデント対応サービス)

X-Force IRISインシデント対応サービスは、インシデント対応全体をサポートする総合インシデント対応サービスです。不正アクセスや情報漏えいなどの各種技術解析だけではなく、公表などの経営陣が取るべき判断なども含めたアドバイスを提供します。

X-Force IRISインシデント対応サービスの特徴

- インシデント終了判定基準、公表、広報のアドバイスも実施
- 年間対応時間が含まれたサブスクリプション型サービス(対応時間は契約により異なります)
- インシデントの兆候発見時のアドバイスなど早期の対応が可能
- 対応時間をテーブル・トップ・エクササイズなどのオプション・サービスに転用することが可能
- グローバル対応オプションを用意



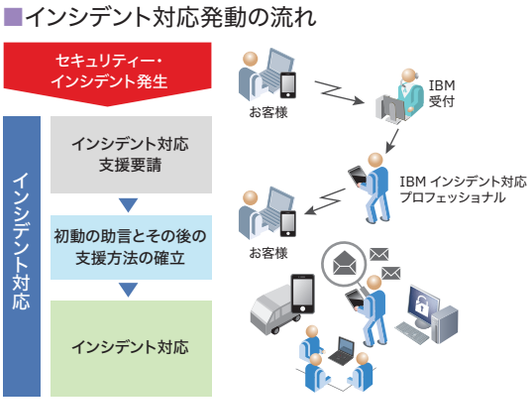
IBMがご提供する価値

- インシデント発生原因の解明、緩和策および恒久策などの策定サポートが得られます
- 公表やメディア対応を実施する場合のサポートを得られます
- インシデント対応を進める上でインシデント全体管理のサポートを得られます
- 分析すべきログの提案を得られます
- インシデント初期対応に必要な技術支援を得られます
- 世界各国で発生したインシデントへの対応サポートが得られます
- WindowsやLinuxを搭載したPCやサーバー、IBMの汎用機、IoT機器やスマートフォンなど多種類の調査が可能です
- 定例会、技術セッションなどを通じ事例共有や技術取得が可能です
- 未使用のインシデント対応時間を転用することでさまざまなオプション・サービスを利用可能です

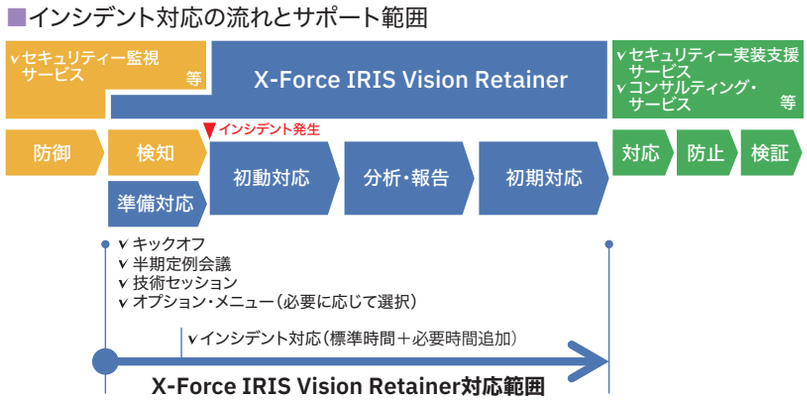
■ インシデント対応範囲の例

マルウェア感染事故	マルウェア感染事故 ● フォレンジック調査 ● ログ解析 ● 原因、影響調査 ● マルウェア検体分析	不正アクセス対応 ● 防止のための緊急措置 ● 原因、影響調査 ● フォレンジック調査 ● 再発防止策提言	情報漏えい対応 ● 原因、影響調査 ● フォレンジック調査 ● 公表や報告のサポート ● 施設立ち入り調査 ● 当事者ヒアリング
不正アクセス対応			
内部犯行、内部事故	内部犯行、内部事故 ● 原因、影響調査 ● フォレンジック調査 ● ログ解析 ● 当事者ヒアリング	Web改ざん対応 ● 状況確認と緊急措置 ● 原因、影響調査 ● フォレンジック調査 ● 再発防止策提言	DDoS対応 ● 状況確認 ● 原因、影響調査 ● 対応アドバイス ● 再発防止策提言
情報漏えい対応			
Web改ざん対応			
DDoS対応			

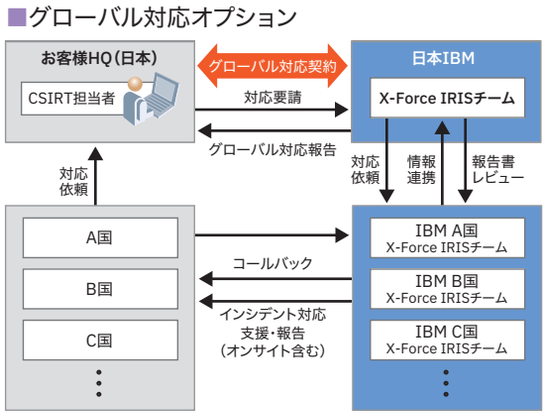
■インシデント対応発動の流れ



■インシデント対応の流れとサポート範囲



■グローバル対応オプション



卓越した専門性 / X-Force

インシデント・レスポンス / X-Force Incident Response and Intelligence Services (XF-IRIS)

IBM MDRサービス
IBM Managed Detection & Response Services

近年のサイバー攻撃は手口が極めて巧妙化しており、侵入を100%防ぐのはもはや不可能とされています。ネットワークの入り口で侵入を防ぐだけでなく、侵入を許してしまった後のすばやい検知と対応が重要です。本サービスでは、既にネットワーク内に侵入した脅威をいち早く検知し、迅速に対応するマネージド・サービスを提供します。

お客様の課題／要望

- 自社のセキュリティー対策は非暗号化通信が前提の境界防御が主体となっており、現在主流の暗号化通信への対応とエンドポイントにおける監視・対応体制は不十分
- 自社にはインシデント・レスポンスの要員を抱えておらず、侵入を許してしまった後のすばやい検知と対応について、技術面/運用面の懸念
- プロアクティブな脅威ハンティングの未実施

IBMがご提供する価値

- マルウェアの存在時間を短縮し、封じ込め速度を加速
- SOCチームおよびCSIRT脅威管理プロセスと統合
- 脅威+インシデント+推奨事項までの明確なコミュニケーション・パス

Detect & Respond
24時間365日にて監視を行い(Monitor)、特定された脅威(Detect)に対してプログラマティックな対応(Respond)をします。

Threat Hunting
プロアクティブな脅威ハンティングを実施し、悪意のあるアクティビティー、脆弱性、設定ミスを発見します。

Prevention(ポリシー管理)
ポリシーを定義、管理、最適化し、カスタマイズされた高レベルのアクティブな「予防」を実現します。

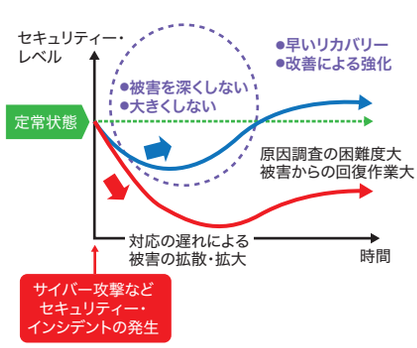
Sensor and Console Management
センサーの活動内容を管理し、各種レポーティングやヘルスチェックを実施。コンソール機能を用いて、全体システムを管理します。

インシデント・レスポンス研修

セキュリティー・インシデントが発生した際に迅速な初動対応、被害の最少化、適切な再発防止策の立案などを実施できる人材を養成します。セキュリティー・インシデントの発生を想定し、初動対応からリスク判定、調査、対策、クローズまでのCSIRTに求められる活動内容を、実例をベースにした題材を使用し参加者と講師間のディスカッション形式で学習します。

インシデント・レスポンス研修の特徴

- 教室での講義、グループ単位のワークショップ、実習の混在カリキュラム式
- 講習時間は30時間/4日間
- セキュリティー・インシデント対応の全体指揮・管理に携わる方、専門家によるインシデント・レスポンス・サービスを受ける場合の担当の方を対象とし、フォレンジック調査などの技術的スキルは前提としていません



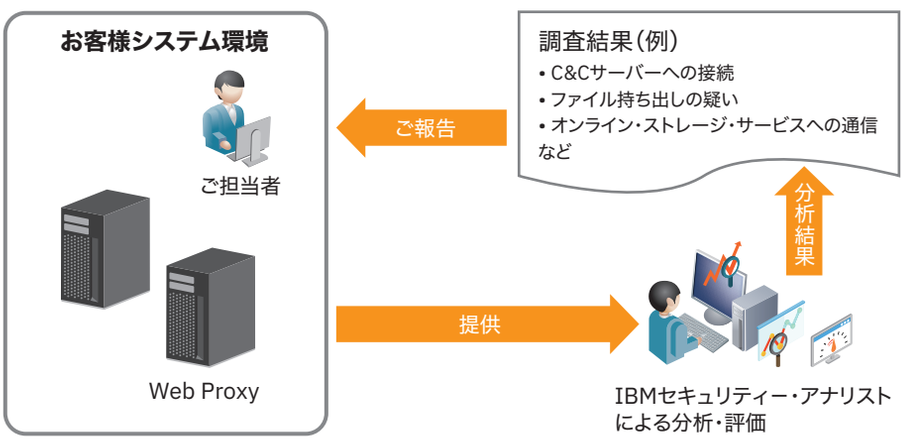
	1日目: CSIRTの活動実践	2日目: インシデント・ハンドリング	3日目: 内部インシデントの対応	4日目: 公表などの考え方
9:30	オープニング	【講義】インシデント・ハンドリング・プロシージャー	【講義】情報漏えい内部インシデント事例	【講義】セキュリティー組織成熟度調査
11:00	【講義】CSIRT概要			【講義】インシデント公表事例
12:00	〈休憩〉			
13:00	【講義】インシデント対応基礎	【実習】インシデント解析解説	【講義&実習】①初動調査 ②ヒアリングと証拠保全	東京SOC見学
14:00	【実習】事例解析	【実習】IDSログ解析実習①		【実習】実習説明
15:00			【講義&実習】③本格調査以降の対応	【実習】総合演習
16:00		【実習】IDSログ解析実習②	【講義】インシデント・情報の読み方	
17:30				

IBMがご提供する価値

- 実例を元にしたケースを利用するため、セキュリティー・インシデントが生じた際の対応をリアルに体験することができます
- 次のことを学べます
  - セキュリティー・インシデントのリスク判定
  - 原因究明、影響範囲、被害状況の特定
  - フォレンジック調査概要
  - セキュリティー対策、再発防止策の実施
  - セキュリティー・インシデントのクローズ方法
  - 経営層への報告
  - 公表の考え方
  - 顧客への対応の考え方
  - 顧客対応コールセンターの設置

アクティブ・スレット・アセスメント（プロキシ）

セキュリティー・インシデント対応の経験で培われた知見を基にC&Cサーバーとの通信や情報持ち出しの可能性を調査します。
Proxyログを対象として不正なアクティビティー（C&Cサーバーへの接続、ファイル持ち出しの可能性など）の痕跡がないか調査します。



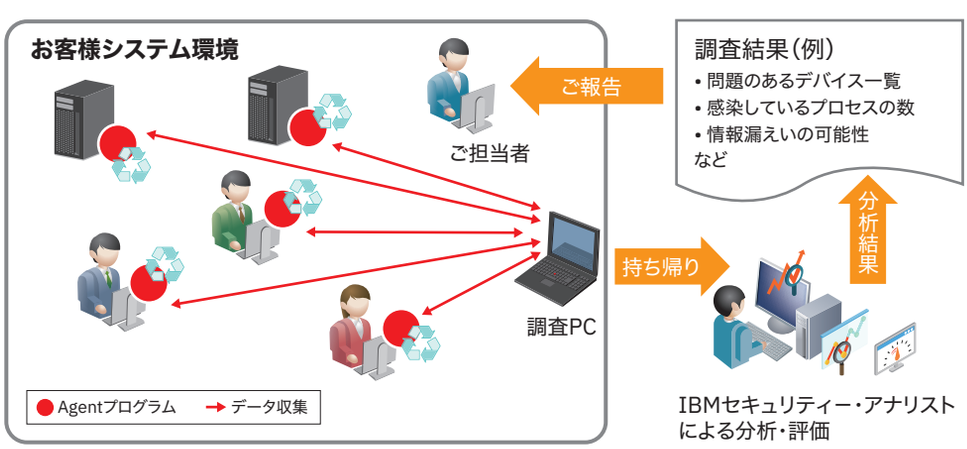
IBMがご提供する価値

- ●C&Cサーバーへの接続有無を確認することが可能です
- ●ファイル持ち出しの有無を確認することが可能です
- ●オンライン・ストレージ・サービスなど社内規定違反の有無を調査することが可能です

報告書イメージ

アクティブ・スレット・アセスメント（エンドポイント）

セキュリティー・インシデント対応の経験で培われた知見を基にPCやサーバーを対象に潜在的なリスクや脅威が存在しないか調査します。
各種ログ（セキュリティー・ログ、イベント・ログ、など）、ファイルシステム、レジストリ、設定内容などを調査し、さまざまな観点から分析・評価を実施します。



IBMがご提供する価値

- ●隠れたセキュリティー・インシデントを発見することができます
- ●PCやサーバーの潜在的なリスクや脅威を発見することが可能です
- ●短期間に大量のPCとサーバーに対して調査することが可能です

【調査の流れ】

1. Agentプログラムを調査対象のPCにインストールし実行
2. Agentプログラムが収集した調査データを調査PCで受け取る
3. IBM施設内に調査PCを持ち帰りデータの解析を実施
4. 調査報告を作成して報告

卓越した専門性 / X-Force

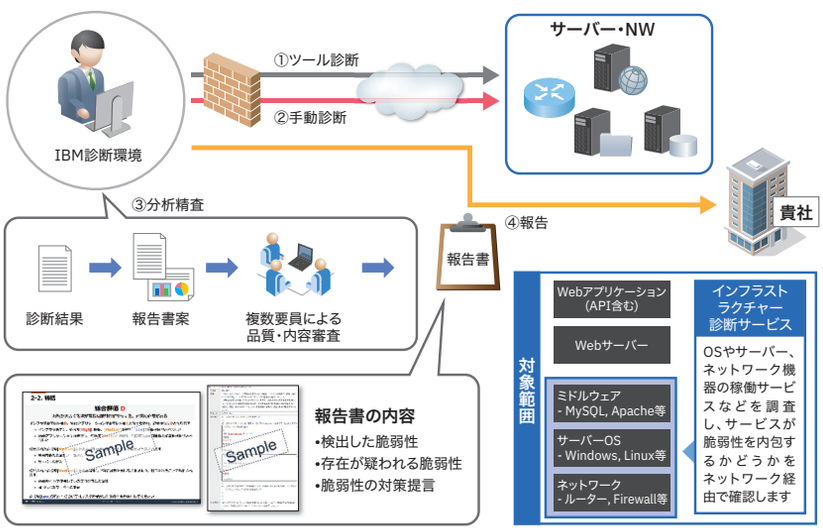
ペネトレーション・テスト / X-Force Red (XF-RED)

インフラストラクチャー診断サービス

お客様のサーバーやNW機器などに内包するセキュリティーの問題（脆弱性）を調査し、脆弱性が検出された場合には内容と対策を報告します。

お客様の課題／要望

- サーバーやNW機器などが内包する脆弱性を調べたい
- 公開システムに問題が無いか調べたい
- 簡易的ツールでの調査結果だけでは不安がある



IBMがご提供する価値

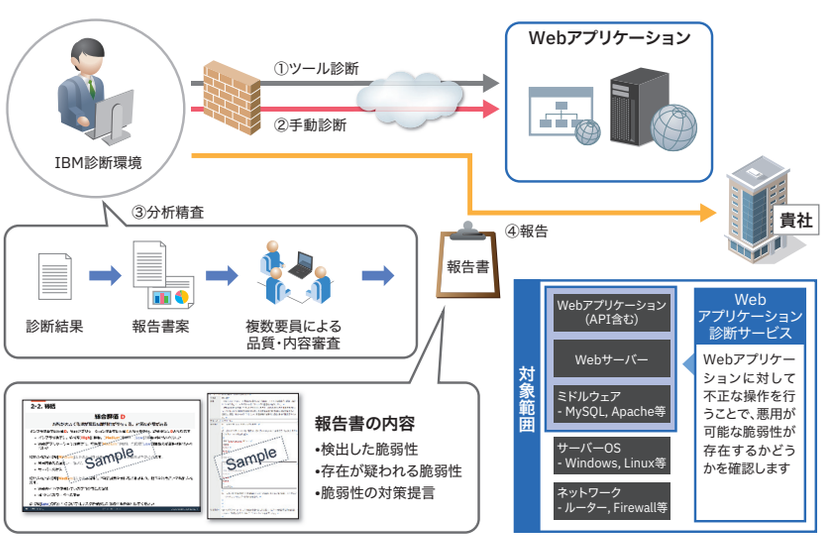
- 複数の脆弱性診断ツールによる検査と経験豊富なセキュリティー専門技術者の手動調査を組み合わせたハイブリット診断手法により、網羅的かつきめ細かい検査を行うことができます。脆弱性診断ツールのみに頼った診断では発見できない脆弱性を検出すること、複数の脆弱性診断ツールを使用することで誤検知や検出漏れを排除した調査結果を報告する事が可能です
- 3段階の危険度、4段階の対象評価で要約した経営層向け報告書と技術的な観点で記載した技術者向け報告書の2種類を提供します

Webアプリケーション診断サービス

お客様のWebアプリケーションに内包するセキュリティーの問題（脆弱性）を調査し、脆弱性が検出された場合には内容と対策を報告します。

お客様の課題／要望

- Webアプリケーションが内包する脆弱性を調べたい
- 公開システムに問題が無いか調べたい
- 簡易的ツールでの調査結果だけでは不安がある

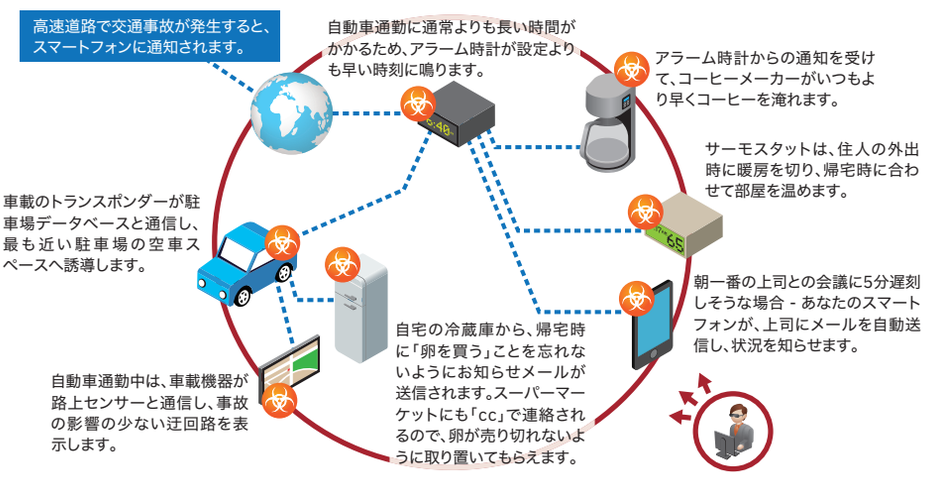


IBMがご提供する価値

- 複数の脆弱性診断ツールによる検査と経験豊富なセキュリティー専門技術者の手動調査を組み合わせたハイブリット診断手法により、網羅的かつきめ細かい検査を行うことができます。脆弱性診断ツールのみに頼った診断では発見できない脆弱性を検出すること、複数の脆弱性診断ツールを使用することで誤検知や検出漏れを排除した調査結果を報告する事が可能です
- 3段階の危険度、4段階の対象評価で要約した経営層向け報告書と技術的な観点で記載した技術者向け報告書の2種類を提供します

IBM X-Force Redペネトレーション・テスト・サービス

最先端の技術を持つセキュリティー・テスト専門家によるペネトレーション・テスト・サービスです。
ネットワーク、アプリケーション、シミュレーションを含むHuman、ハードウェア/組み込み機器などを対象に最新の攻撃手法を利用した侵入テストを試み、その結果について報告します。調査は社外(インターネット)または社内からの実施が可能です。



IBMがご提供する価値

- 既知と未知の脆弱性を利用して侵入可能かどうかを確認できます
- 侵入成功した状況や、発見された社内機密情報のレベルに基づき、セキュリティー状態の評価をします
- ネットワーク、アプリケーション、シミュレーションを含むHuman、ハードウェア/ 組み込み機器などさまざまな対象に対しペネトレーション・テストを行うことが可能です

X-Force Red IBM

IBM X-Force Redペネトレーション・テスト・サービスが提供する4つの分野にわたるお客様資産の評価と可視化

ネットワーク

- ペネトレーション・テスト
- すべてのネットワークの脆弱性診断
  - 内部
  - 外部
  - Wi-Fiおよびその他の無線
  - SCADA、PCI DSS

アプリケーション

- ペネトレーション・テスト
- すべてのプラットフォームのコードレビューと脆弱性診断
  - Web
  - モバイル
  - クライアント・サーバー
  - ターミナル
  - メインフレーム
  - ミドルウェア

シミュレーションを含むHuman

- フィッシング・キャンペーン
- ソーシャル・エンジニアリング
- ランサムウェア
- 物理的なセキュリティー違反

ハードウェア/組み込み機器

- Internet of Things (IoT)
- ウェアラブル・デバイス
- POS (point-of-sale) およびセルフ・チェックアウト・システム
- ATM
- 自動車、MFP、ビデオ会議システム、その他のシステム

IBM X-Force Redの強み

IBM X-Force Redは、大規模かつ複雑なシステムに対する豊富な実績を有し、最新のグローバル・セキュリティー・インテリジェンスと高い技術力を誇るホワイトハッカー集団です。

インテリジェンス

世界最大級のセキュリティー・インテリジェンスを活用

- 専門研究機関X–Force
- 研究所10拠点12ラボ保有
- 特許取得件数3,500件以上
- 年間投資額15億ドル以上
- 全世界専門家数約8,000名

ホワイトハッカー集団

高い技術力を誇るホワイトハッカーによる攻撃者目線の演習

- 国際的セキュリティー・コンテストへの豊富な登壇経験有(Black hat、DEFCONなど)
- CREST USAボードメンバーやOSCP資格保有者を含む
- 日本語を理解可能なホワイトハッカーを含む

豊富な実績

ミッション・クリティカルな大規模システムにおける実績

- 金融機関、電力会社、製造業などミッション・クリティカルな社会基盤システムを対象としたペネトレーション・テストを実施
- 複雑なシステムを持つグローバル金融機関にて高評価を頂く攻撃演習を実施

卓越した専門性 / X-Force

ペネトレーション・テスト / X-Force Red (XF-RED)

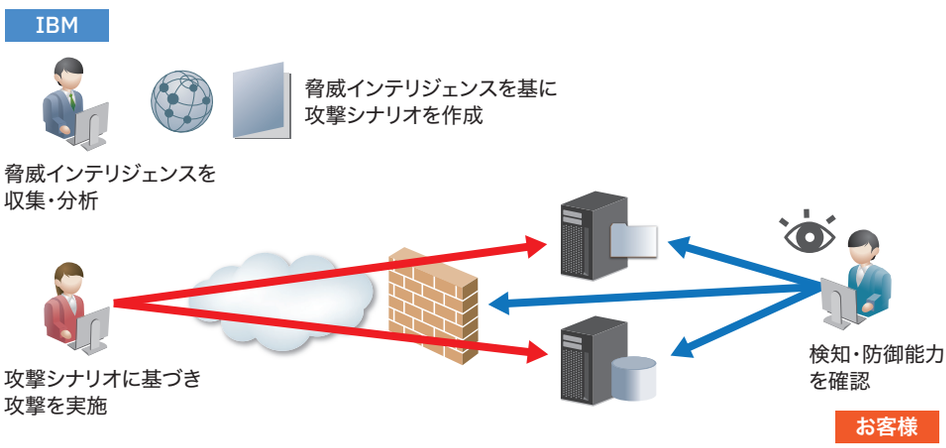
脅威ベースのペネトレーション・テスト・サービス
(TLPT: Threat-led Penetration Test)

金融分野におけるサイバー・セキュリティー強化にむけて、TLPTのレッドチームとして攻撃シナリオを作成し、ペネトレーション・テストを実施します。

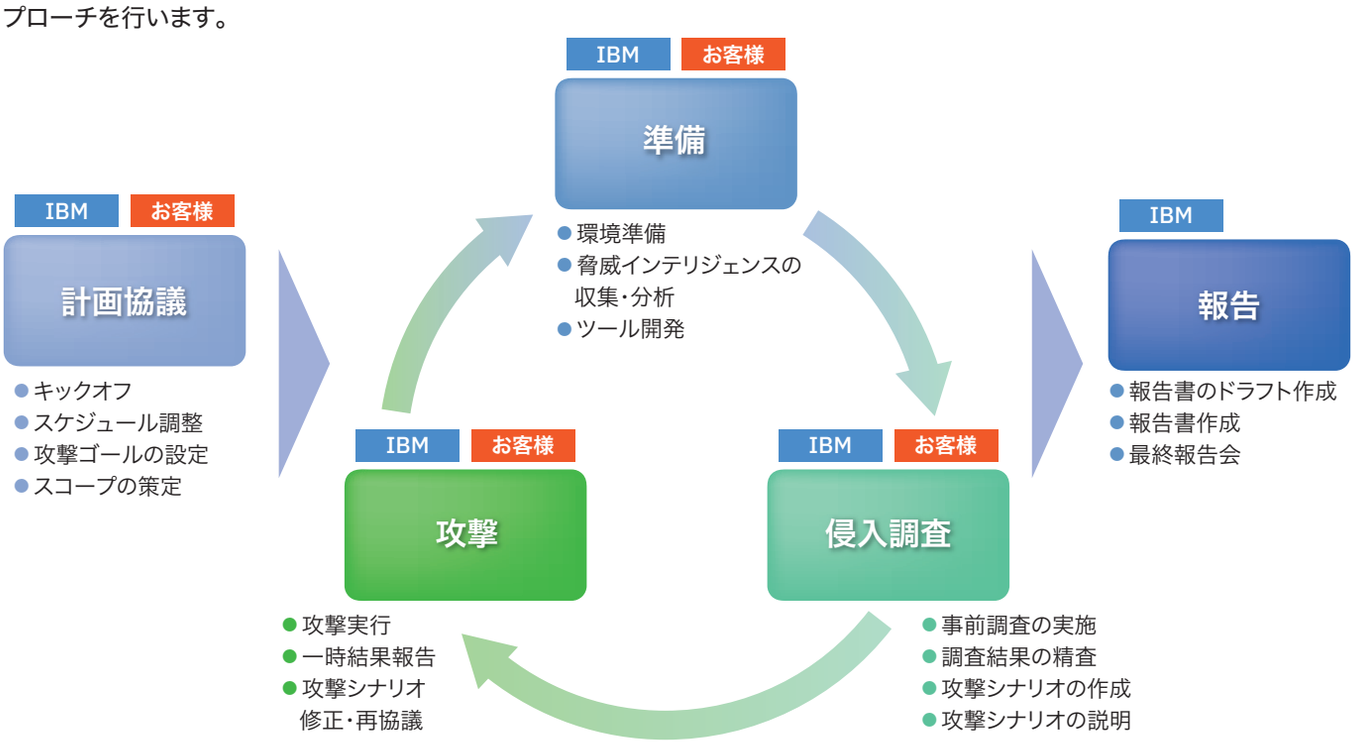
- 脅威インテリジェンスを収集し、お客様の特性を加味した脅威を分析します。
- 経験豊富なセキュリティー専門技術者が収集・分析した脅威インテリジェンスを基に攻撃シナリオを作成します。
- 攻撃シナリオを基にペネトレーション・テストを実施し、結果を報告書にまとめ報告します。

IBMがご提供する価値

- 金融庁のガイドラインに沿った脅威ベースのペネトレーション・テストを実施
- 自社が現在どのような脅威にさらされており、どのような攻撃を受ける可能性があるのかを把握することが可能
- 脅威に基づいた攻撃を受けることで、お客様が自社のサイバー攻撃に対する防御能力を確認することが可能



脅威ベースのペネトレーション・テストは、「計画協議」「準備」「侵入調査」「攻撃」「報告」の5つのフェーズで提供します。「準備」「侵入調査」「攻撃」の3つのフェーズは調査・攻撃の結果やお客様との協議結果を反映し適宜更新を行うため、繰り返しを前提としたアプローチを行います。



IBM X-Force Red ATMペネトレーション・テスト・サービス

金融機関ATMを対象としたサイバー攻撃に備え、IBM X-Force Redのホワイトハッカーがオンサイトにてペネトレーション・テストを実施するサービスです。

お客様の課題／要望

- 日本においては海外と比較してATM関連システム全般に求められるサービス品質が非常に高い。ATMが停止した場合には社会問題となり、銀行の信頼に甚大な悪影響を及ぼす。

IBMがご提供する価値

- 効果的な投資でATMのセキュリティー・リスクを評価し、対策の立案が可能
- グローバル最先端のセキュリティー専門家によるテスト実施
- 日本語サポートの提供

ATMへの攻撃手法の例

物理的攻撃
- ATM機器の不正改造
- メンテナンス用特権ユーザーの悪用

マルウェア攻撃
- 直接またはリモート操作によるインストール
- 単体の機器、またはATMネットワーク全体を標的とする
- 目的の達成後、マルウェアは消去し証拠を隠滅

旧型のATMを狙った攻撃
- 旧型ATMが意図しない場所に残存
- セキュリティー・パッチが適用されていない

想定される攻撃被害

- 情報流出（口座情報・暗証番号）
- 現金の盗難
- ATMネットワークへの侵入
- ネットワーク上の他のシステム/資産への攻撃

作業内容（例） ※お客様の要件に基づいて調整します。

- テスト・スコープの決定
- 事前準備・Kick-off ミーティングの実施
- テスト実施
- 中間・最終報告
- テスト実施報告書、Executive Summary 作成
- 日本語サポート・オンサイト作業の準備支援、お客様拠点におけるエスコート、各種会議、報告書作成

IBM X-Force Red IoTデバイス ペネトレーション・テスト・サービス

2016年に話題になったマルウェア“Mirai”をはじめとして、ボットネットは多くのマルウェアをIoTデバイスに拡散し攻撃に利用しており、またIoTに関する脆弱性は直近5年で50倍以上に増加しています。こうした脅威に対処するため、最先端のスキルと知識を持つホワイトハッカー集団 IBM X-Force RedがIoTデバイスに対して、ペネトレーション・テストを行うサービスです。

お客様の課題／要望

- 自社でIoTデバイスを活用しているがセキュリティーに不安がある
- 自社でIoTビジネスの展開を計画しているが事前にセキュリティー・リスクを把握したい
- 一般のセキュリティー対策は実施しているが、IoTデバイスについては知見が不足

IBMがご提供する価値

- IoTデバイスに関連した自社のセキュリティー・リスクを把握
- IoTビジネスの市場展開前にセキュリティーの影響を把握
- リスク対象、脆弱性の詳細、エクスプロイト（実際に試行された攻撃）など詳細な発見事項の報告と洞察

X-Force Red IBM

報告書の例

- 診断概要
- 発見されたリスク一覧
- 有効範囲
- テスト方法・手法
- リスクレベル（評価基準）
- 各発見事項の詳細
- 診断実施者

卓越した専門性 / X-Force

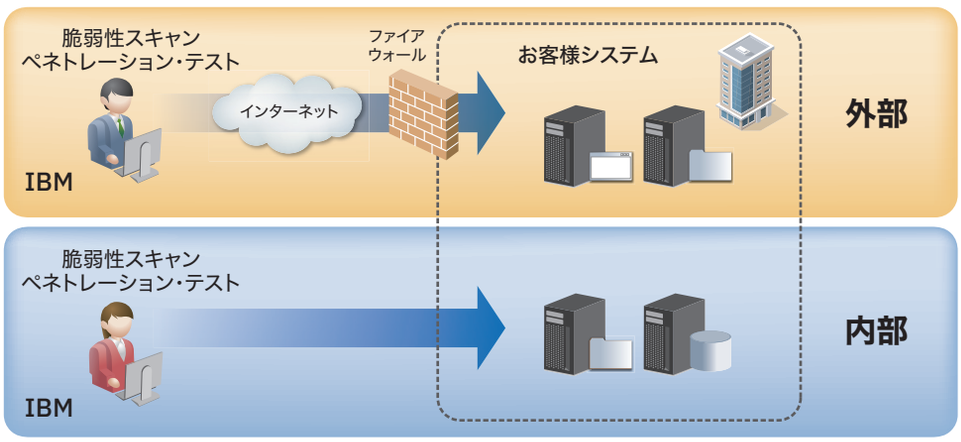
ペネトレーション・テスト / X-Force Red (XF-RED)

PCI DSS スキャン・サービス

PCI DSS認定取得のためASV(認定スキャンベンダー)として、PCI DSS要件11.2「脆弱性スキャン」およびPCI DSS要件11.3「ペネトレーション・テスト」の要件を満たすスキャンおよびテストを提供します。

お客様の課題／要望

- 金融庁のガイドラインに沿ったテストを実施したい
- サイバー攻撃に対する自社の対策について評価をしたい
- 自社にどのような脅威があるのかを調査したい

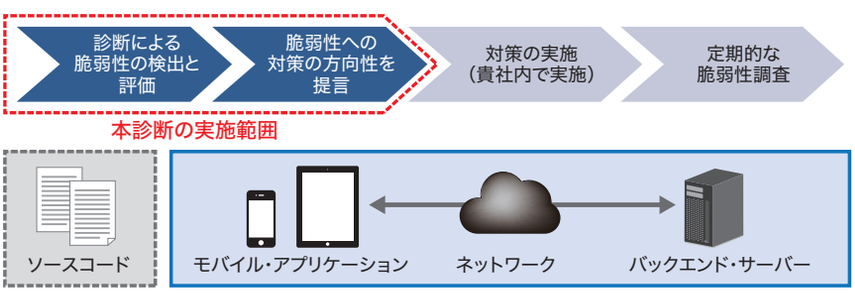


IBMがご提供する価値

- 脅威インテリジェンス情報を分析し、対象システムの脅威を分析します
- 経験豊富なセキュリティー専門技術者が脅威インテリジェンスを分析し対象システムに有効な攻撃シナリオを作成、テストを実施します
- ペネトレーション・テストを実施するレッドチームのテスト結果を報告するとともに、防御チームであるブルーチームの防御記録を最終報告書にまとめる支援をします

モバイル・アプリケーション診断サービス

モバイル・アプリケーション自体やバックエンド・サーバーとの通信において、セキュリティー上の問題(脆弱性)の有無を調査し、脆弱性が検出された場合にはその内容および対策方法を報告します。
モバイル・アプリケーション診断では、クライアント側である「モバイル・アプリケーション」とサーバー側である「バックエンド・サーバー」の双方を対象とすることで、アプリケーション全体をひとつのシステムと捉えた総合的な診断を実施し、システム内にセキュリティー上の問題が存在しないか調査を行います。



※モバイル・アプリケーション診断のソースコード解析は本サービスの対象外となります。
※対象となるモバイル・アプリケーションはiOSもしくはAndroidのみとなります。

IBMがご提供する価値

- モバイル・アプリケーションに存在する脆弱性を発見し、脆弱性を悪用される前に修正・対策を講じることが可能です
- 脆弱性が検出された経緯を知ることで、今後同様の脆弱性が再発するリスクを軽減できます

【モバイル・アプリケーション診断の流れ】

1. 診断対象やスケジュール、連絡体制、確認・依頼事項などを確認
2. 関係各位への報知や診断に必要な情報を提供(お客様)
3. IBM内の診断環境を使用しモバイル・アプリケーションの脆弱性を調査
4. 診断の結果を複数人にて精査し診断の結果をまとめた報告書を作成
5. 報告書を使用して検出された脆弱性の内容や対策の方針について説明を実施

サイバー攻撃対応訓練サービス

安定稼働が不可欠な情報システムを対象として、サイバー攻撃対応訓練を提供するサービスです。お客様のご要望、課題と目的に合わせて、日本IBMのプロジェクト・チームがオリジナルのサービス内容と訓練内容をデザインし、ご提供します。IBM X-Force Redと連携した訓練の計画・実施、主に経営層を対象とした米IBMの訓練施設IBM X-Force Command Centerの利用、およびTable Top Exercise（机上演習）形式もご選択いただけます。

お客様の課題／要望

- 安定稼働が不可欠な情報システムを保有している。
- セキュリティー対策を講じるとともに、サイバー攻撃対応の体制整備とスタッフのスキルアップが必要

IBMがご提供する価値

- 課題と目的に合わせて、最新かつ高度な技術力を反映した攻撃を実施
- 実演習形式と机上演習形式の選択が可能
- サイバー攻撃対応力を複数の観点から評価

■ サービス内容の一例（作業内容、成果物はお客様の要件に基づき調整します。）

計画立案フェーズ

現状調査
ネットワーク、システム、組織体制、セキュリティー対策・施策、インシデント対応策などの現状を調査します

攻撃目標の設定・シナリオの作成
攻撃対象のシステムを定め、想定される脅威を整理し、攻撃シナリオを立案します

- 現状調査結果
- 訓練シナリオ

訓練実施フェーズ

攻撃準備
攻撃プログラムやツールの開発、環境準備などを行います

訓練実施
攻撃を実施します
お客様担当者はインシデント対応を実施します

- 訓練実施結果

評価フェーズ

評価
関係者を集めて訓練後の振り返りを実施し、サイバー攻撃対応力の評価を実施し、課題を共有します

報告書作成
報告書を作成します

- 訓練実施結果報告書

■ IBM X-Force Red との連携

IBM X-Force Redが、お客様の要件に基づき環境調査、攻撃計画、および攻撃実施に参画します。
お客様との連絡、調整、日本語サポートは日本IBMのプロジェクト・チームが行います。

■ IBM X-Force Command Centerの利用

米IBMのサイバー攻撃対応訓練施設IBM X-Force Command Centerを利用し、主に経営層のお客様を対象として、「顧客や監督官庁への連絡」「サービス、ネットワークの遮断」「公表の判断」など実践的な意思決定と評価の訓練を実施することも可能です。

IBMハイブリッド／マルチクラウド・セキュリティー戦略

IBMは、グローバル規模のクラウドサービス事業者としての技術的知見と豊富なノウハウを活かし、お客様がセキュアにハイブリッド／マルチクラウド環境の導入・移行を実現するために、包括的なソリューションとサービスを提供します。

IBMハイブリッド／マルチクラウド向けソリューション・フレームワーク

サービス	Advise	Move	Build	Manage		
プラットフォームに統合されたCloud Pakオファリング	Cloud Pak for Applications	Cloud Pak for Data	Cloud Pak for Integration	Cloud Pak for Automation	Cloud Pak for Multicloud Mgmt.	Cloud Pak for Security
基盤（Red Hat OpenShiftなど）	Open Hybrid / Multi Cloud Platform					
インフラ	IBM Cloud	AWS	Azure	GCP	Edge	Private Cloud	On Premise

IBMハイブリッド／マルチクラウド・セキュリティー基本方針

1. Securing Journey to Cloud

IBMのクラウド・セキュリティー・エキスパートがお客様のクラウド移行をセキュリティーの面から包括的にご支援

2. Cloud Pak for Security

オープンなハイブリッド/マルチクラウド・プラットフォームRed Hat OpenShift向けに予め統合されたセキュリティー・ソリューションを提供

3. Security for IBM Cloud

セキュリティーを維持したままIBM Cloud上へのワークロード移行を実現するための基盤を提供

“Securing Journey to Cloud”

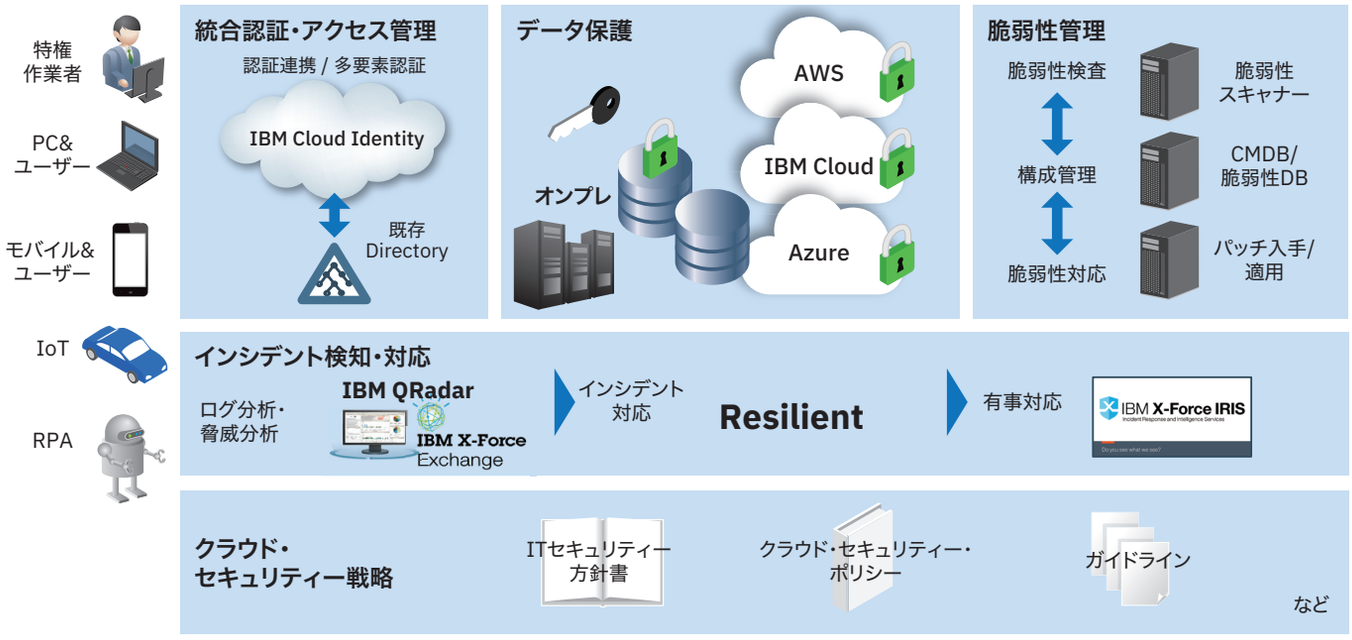
IBMは、お客様のハイブリッド／マルチクラウド導入と移行（”Journey to Cloud”）をセキュアに実現するため、4つのフェーズと14の主要ソリューション（”14 in 4”）で構成される一連の支援を提供します。

Advise on Cloud	Move to Cloud	Build for Cloud	Manage on Cloud	
IBM Services for Cloud Strategy	IBM Services for Cloud Migration	IBM Services for Cloud Development	IBM Services for Cloud Management	
Enterprise Cloud Strategy	Cloud Migration	Cloud Application Developm ent and DevOps	DevOps Monitoring and Management	Multicloud Management Services
Cloud Architecture Design	Cloud Modernization	Multicloud Infrastructure Development	Enterprise Application Management	Managed Infrastructure-as-a-service
Cloud Security and Compliance Strategy		Enterprise Application Integration	Managed Multicloud Services Platform	Cloud Security and Resiliency

Shift Left セキュリティーに基づくソリューション・モデル

■ セキュリティーが関連するソリューション　Security セキュリティーを主体とするソリューション

IBM Securityが推奨するハイブリッド／マルチクラウド・セキュリティー・アーキテクチャー基本構成



世界に誇るIBM Securityの専門性とファシリティー

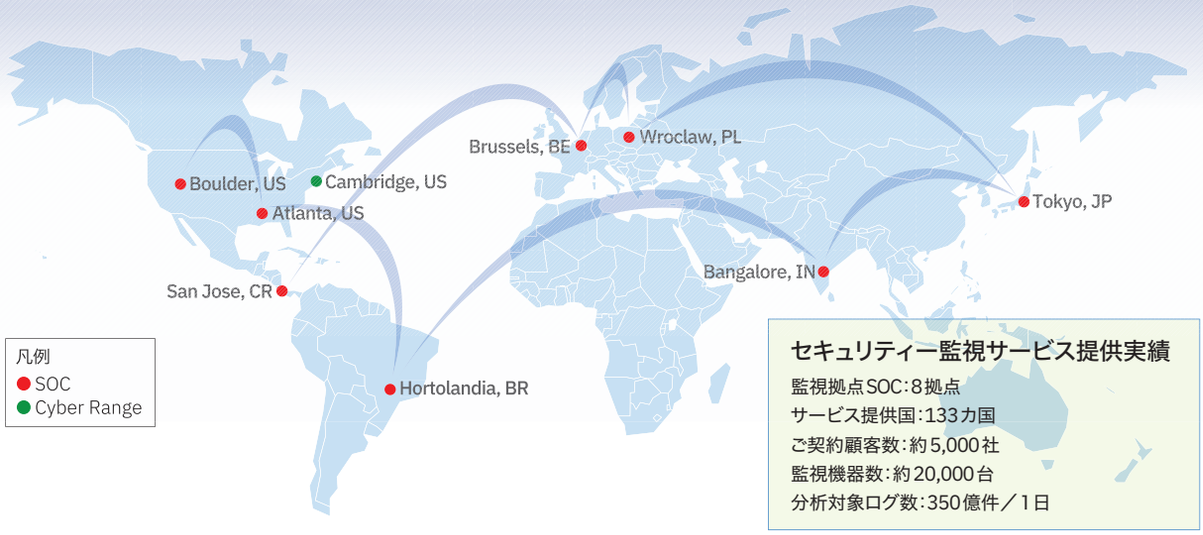
X-Force

世界最大規模の セキュリティー・エキスパート集団

- 世界8,000名を超える専門家
- 世界10拠点の研究開発拠点
- 特許取得件数：3,500件以上
- 年間投資額：1,500億円以上
- ATMや自動車の脆弱性テストも可能
- 金融マルウェア特化の研究所

IBMセキュリティー・オペレーション・センター（SOC）

世界8箇所のセキュリティー・オペレーション・センターが連携し、Follow the sunオペレーションにより24時間365日体制でセキュリティー監視サービスを提供しています。



セキュリティー監視サービス提供実績

監視拠点SOC：8拠点
サービス提供国：133カ国
ご契約顧客数：約5,000社
監視機器数：約20,000台
分析対象ログ数：350億件／1日

最新鋭設備 IBM X-Force Command Center

IBMは業界で先駆けて約2億ドルを投資し、2016年に商用のCyber Range（サイバー訓練場）としてマサチューセッツ州ケンブリッジのIBMセキュリティー本部内に「IBM X-Force Command Center」を設置し、企業のサイバー・セキュリティーへの意識向上の重要性と、日々直面する脅威に対する啓発に取り組んでいます。

この施設では、外部から隔離されたネットワーク環境において架空のサイバー攻撃を体験し、インシデントに即時対応するために必要なトレーニングを提供しており、参加者は実際のセキュリティー・ツールを操作して感染状況を調査し、内部／外部のインシデントに対応するための危機管理の方法、意思決定をシミュレーションできます。

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19番21号

10-19 Printed in Japan

このカタログに掲載されている製品、サービスは2019年10月のもので事前の予告なしに変更することがあります。

お問い合わせは、IBMビジネスパートナー、製品販売店、弊社営業担当員または、IBMアクセスセンターへ。
●IBMアクセスセンター
電話番号: 0120-550-210(フリーダイヤル)
受付時間: 平日 9:00～12:00、13:00～17:00
(土曜、日曜、祝日、12月30日～1月3日を除く)

■ IBMセキュリティー
ibm.biz/security_jp

■ Security Intelligence Blog
ibm.biz/security_blog

■ メール・フォームでのお問い合わせ
ibm.biz/security_contact