EDRは本当に活用されているか

EDRの導入後の現実 – 導入したが。。。

■EDRが会社上層部が聞きつけて、EDRベンダーのハイタッチ営業で導入したが。。。

- 既存の情報システム部に丸投げされることが多いので、EDR導入後なにをすればいいのかわからない
- 情報システム部がEDRのアラートの内容がよくわからない、対応をどうするかわからない
- 社内にSoCやCISRTがないのでEDRのアラートの内容がわからない、対応もどうすればわからない
- 誤検知対応もベンダーの推奨どおりしているが誤検知が減らない
- EPPを導入していればEDRは要らないというところも多いので導入しても放置していることも
- MSSPのレベルが低いので死活監視程度のことしかできない
- 上のようなことがあるので毎年、EDRの入れ替えをしている

EDRの導入後の現実 – 導入したが。。。

■既存の情報システム部に丸投げされることが多いので、EDR導入後なにをすればいいのかわからない
  - EDR導入後、アラートをみないのでEDRは放置されることが多い
  - EDRは導入しただけでは意味がなくて導入後の運用がもっとも大切
- MSSPにおいては現在のところ安かろう悪かろうというのが現状
- MSSPが提供しているSOWの内容のよく確認して自社に適した内容なのかを要確認
- インシデントレスポンスやフォレンジックが必要な時があるので、それらサービスを提供できる会社を事前に決めておく
- Machine Learningを使うEDRは検知においてFalse Positiveがあるので、FPを減らすために、EDR製品やEDRベンダーにFP発生時のアラートの情報をもとにホワイトリストを作成できるかを要確認
- EDRの検知Alertに関して、EDRベンダーやMSSPにAlertの詳細内容を確認できるか

EDRの導入後の現実 – 導入したが。。。

■EDRを活用にするには

EDRベンダーのフルマネジドサービスの導入
　費用がかなり高い

MSSPを正しく選定すること
　費用が高い、SOWなどを明確にするには発注側にある程度知識などが必要

自社管理ができるように人材を育てるか外部から雇いいれること
　費用は上記より安いが育成時間や育成されるまでの対応方法が必要

MSSPや自社管理するにしても、EDRに付随している分析サービスなどを活用することでコストを下げて精度をあげることが可能

WithSecure Co-Monitoring service 概要

- WithSecureによる重大リスク検出の監視サービス（24時間365日または平日）
- 監視サービスにて脅威アナリストが深刻リスク検出、検証、調査を提供
- 確認された攻撃を、WithSecureからお客様へご連絡
- WithSecure脅威アナリストが迅速かつ効果的な修復のためのアドバイスを提供

Co-Monitoring 導入によるお客様のメリット

- サイバー攻撃への迅速な対応
- 24時間365日/平日 英語によるEDR マネージドサービス
- Customer trust

WithSecure による EDR 監視サービスのご提供
(2023年10月現在 英語サポートのみの提供)

WithSecure EDR / Co-Monitoring サービス比較

Feature	WithSecure EDR	WithSecure EDR + Co-Monitoring
Detection	YES	YES
攻撃検出時のお客様報告	NO	YES
深刻なリスクの検証	NO	YES
攻撃への対応、 修復ガイダンスの提供	NO	YES
Response action	NO EDRネットワーク切断手動対応など EDR の手動対応は提供外	NO EDRネットワーク切断手動対応など EDR の手動対応は提供外
Delivery	N/A	9:30-17:30 office hour or 24/365
Offering	Software only	Software + service

Co-Monitoring お客様連絡フロー

今後予想される脅威

今後、予想される脅威

■2014年に、クリミア危機が勃発

https://ja.wikipedia.org/wiki/ 2014年クリミア危機

■ロシアで猛威のPetyaで分かった、セキュリティ会社の不確かさ

https://xtech.nikkei.com/it/atcl/column/14/346926/062901039/

ウクライナやベルギーのCERTなどは当初、初期の感染原因はメール添付だったと指摘。サイランスやシマンテックなどのセキュリティ製品ベンダーも、新型Petyaのメール添付による感染を指摘した

シマンテックは当初、新型Petyaは主にメールで感染するとしていたが、6月29日にブログを更新し、ウクライナの税務・会計ソフト「MEDoc」が最初の感染の足掛かりであり、ウクライナを狙った標的型攻撃だったとした。「2016年に見つかった初期のPetyaはメール添付で広まったので、当初感染源をメールとした」（同社広報）と説明している

■サプライチェーン攻撃

会計ソフトの更新というAttack Surface

導入している日本製のソフトは大丈夫か？もちろん海外のソフトも大丈夫か？

メールやWebだけがAttack Surfaceだけではない

今ある技術ではEDRが最後の砦、しかし、EDRはDetectionするがResponseに人や組織がついてこれない現状。。。

今後、予想される脅威

- 日本の同盟国または友好関係が深い国において有事発生前後で社会インフラを担うシステムが攻撃を受ける可能性がある
- その攻撃は、PetayaのようにメールやWebのアクセスによる感染ではなく、ソフトウェアの更新などによる感染かSaaSサービス経由の感染が想定されるPetayaのようなマルウェアが感染が開始されると、亜種がメールやWebアクセスにより拡散することが予想される
- 有事の際には社会インフラ担うシステムへの攻撃は、主ではなくあくまで後方攪乱や身代金目的が考えられる
- 上記のサイバー攻撃があれば徹底して感染したPCのクリーニングとバックドアや時限式のマルウェアが仕込まれていないかを常時監視する必要がある
  何かのきっかけで再悪用される可能性がある
- 感染経路すなわちAttack Surfaceが2015年当時と比べて増えているので、考えられるAttack Surfaceに対して事前に感染しない対策を実施し、さらに端末においてEPPだけでなくEDRの導入を推奨
- **上記はクリミア危機の事例などから予測したものです**

WITH secure

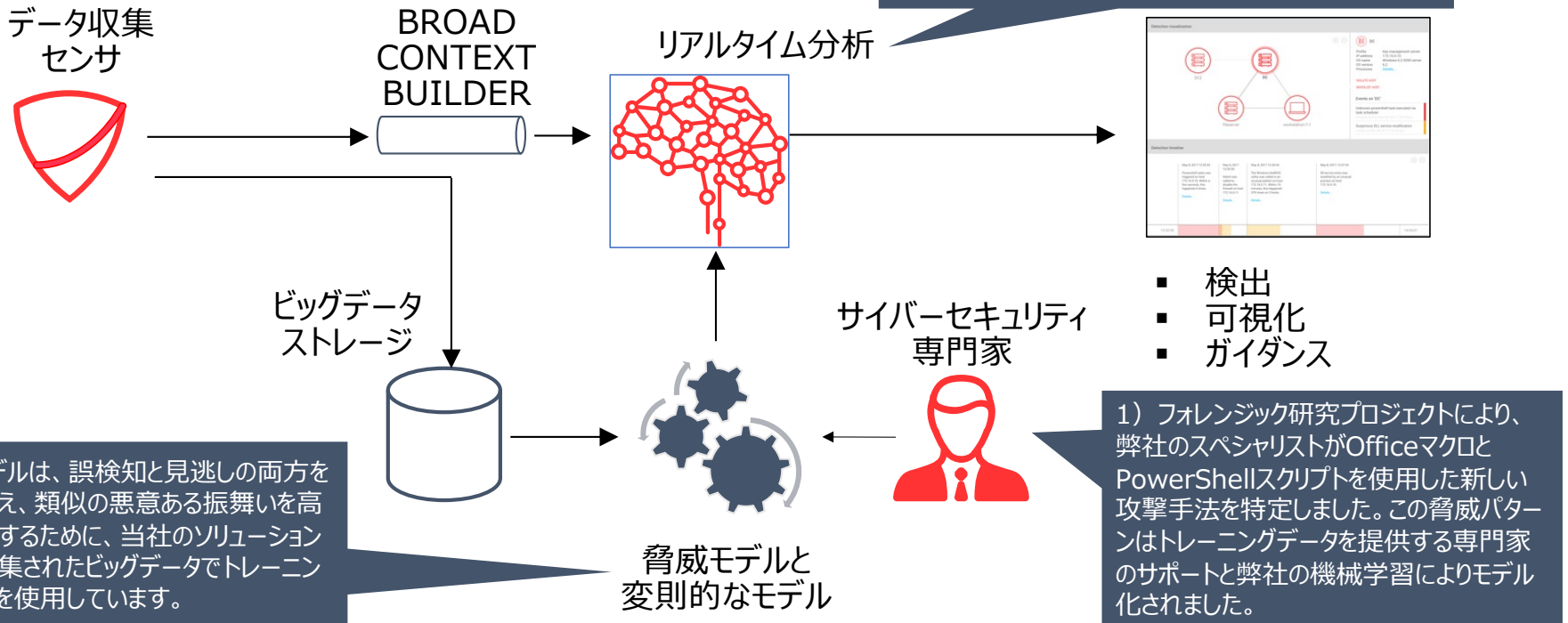
弊社のEDRとコンサルティングサービスのご紹介

WithSecure Elements EDRの概要（弊社宣伝）

EPPとEDRの違い

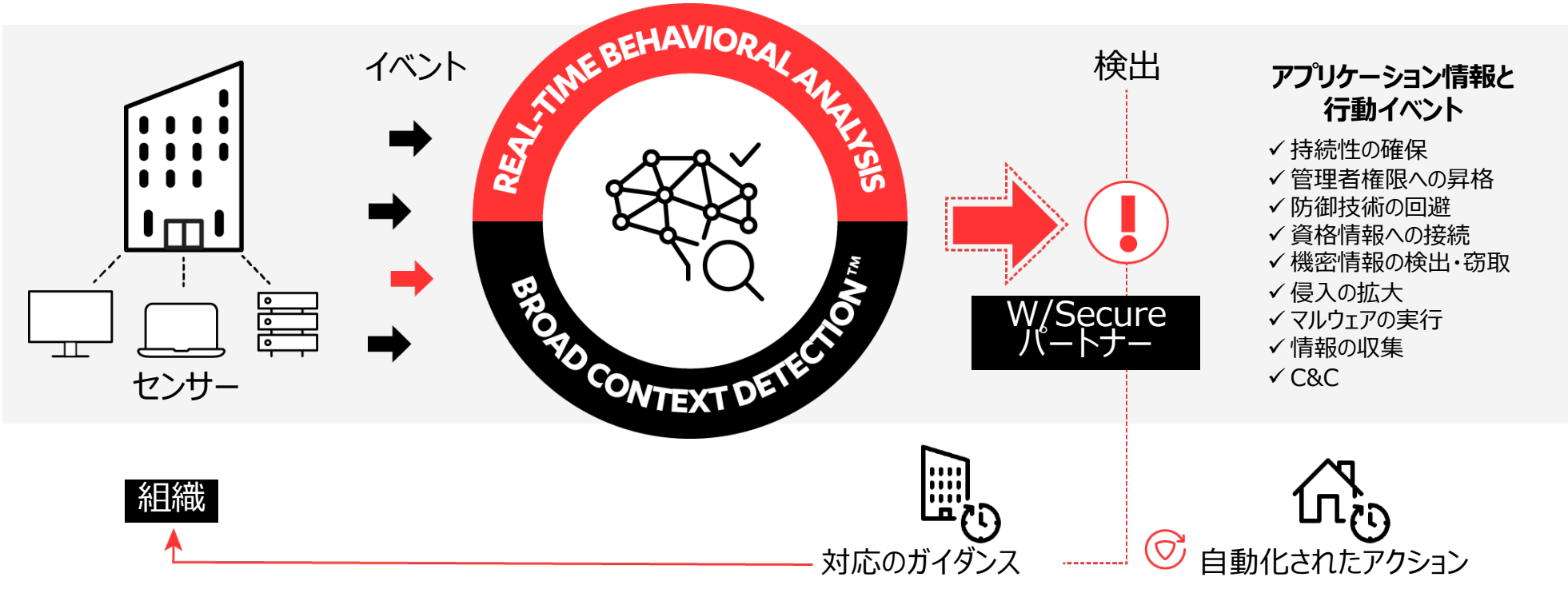
	EPP	NGEPP	EDR
対応製品	WithSecure Elements Endpoint Protection (EPP)		WithSecure Endpoint Detection and Response (EDR)
目的	既知のマルウェア対策	既知・未知のマルウェア対策	PCの操作を監視し、EPP/NGEPPをすり抜けるサイバー攻撃を検出・迅速に対処
特徴	既知のマルウェアを検知	マルウェアの振る舞いや特徴から既知・未知マルウェアを検知	・サイバー攻撃の全体像を可視化し、原因特定・影響範囲を調査 ・影響を最小化するためにPC隔離 ・マルウェア以外の脅威を検知
検知方法	パターンマッチング	・パターンマッチング ・静的な機械学習 ・振る舞い検知 ・レピュテーション ・動的解析(サンドボックス、機械学習) ・などなど	・プロセス起動 ・ネットワークアクセス ・特権昇格 ・スクリプト系 ・標準ツールの悪用 ・TTP (Tactics, Techniques, Procedures) ・などなど

脅威モデリングの動作

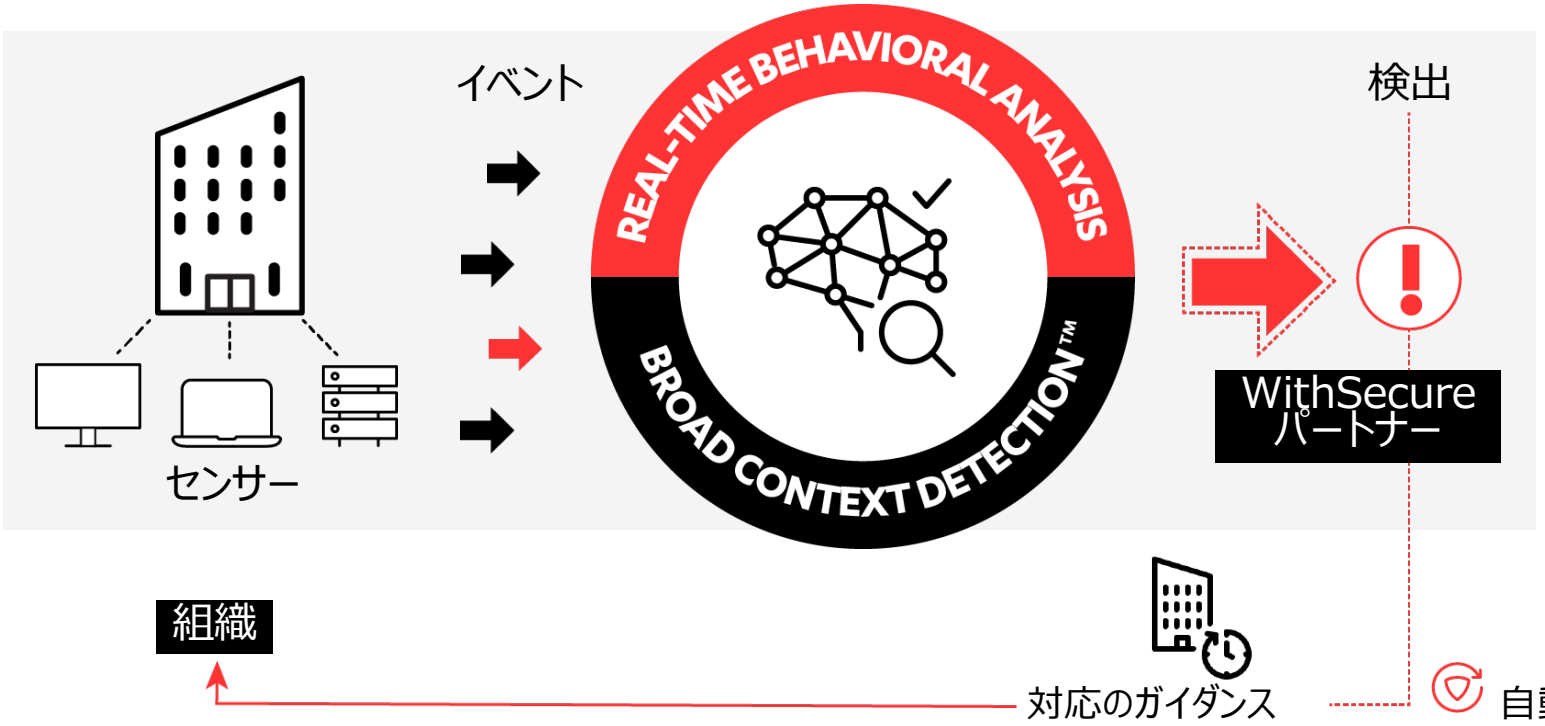


WithSecure EDRの機能

機能の概要

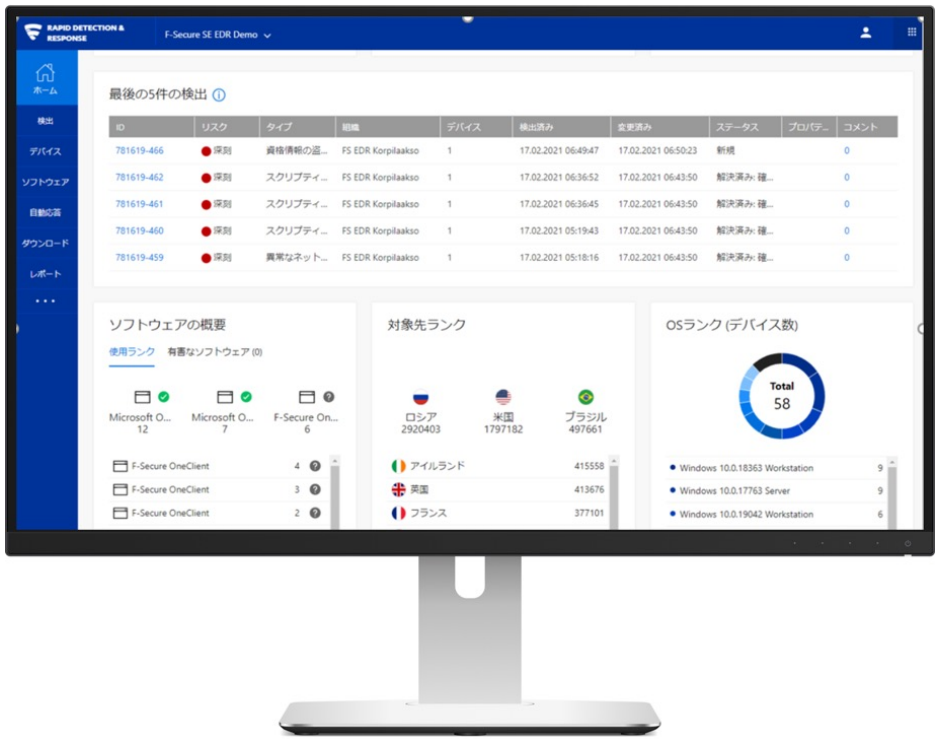


機能の概要



- 軽量なセンサーでエンドポイントを監視し、イベントデータをリアルタイムでクラウド上にアップロード
- リアルタイム行動分析とBroad Context Detection™で悪意ある行動パターンを判別し攻撃かを判断
- 警告の調査が困難な場合は弊社にエスカレートするオプションを利用可能
- 脅威を封じ込め修復するための手順を推奨アクションとして提示

機能一覧



- 振舞い分析
- BROAD CONTEXT DETECTION
- WINDOWS センサー
- アプリケーション インベントリ
- インシデント マネジメント
- 集中管理
- 専門家の ガイダンス
- MAC センサー
- スレット インテリジェンス
- ホスト隔離
- 自動対応
- API 管理統合

BROAD CONTEXT DETECTION

Broad Context Detection (BCD) により
標的型攻撃の範囲を容易に把握

機械学習によるリアルタイムの振舞いとその評価、およびデータの分析

リスクレベル、影響を受けるホストの重大度、および蔓延する脅威の状況を組み合わせて、インシデントの包括的な洞察と重大度を提供

リスクベースの多面的な対応を可視化し、関連する検出だけを提示

検出する項目

- EDRは、不審な行動を管理者に警告することにより、以下の発生し得る侵害の兆候を検出します。
  - 標準プログラムの異常動作
  - 非標準の実行可能ファイルから実行中のプロセスへの呼び出し
  - 予期しないスクリプトの実行
  - 標準プロセスから予期しないシステムツールの実行

- 検出：単一のインスタンスではインシデントにならなくとも、それが短時間で複数検出された場合、警告の重大度が高くなるため、インシデントの可能性が警告されます。

センサーが収集するデータ

- ファイルへのアクセス
- プロセスの作成
- ネットワーク接続
- レジストリの書き込み
- セキュリティ侵害の検出に関連するシステムログエントリ
- プログラム実行時に派生したスクリプト抽出

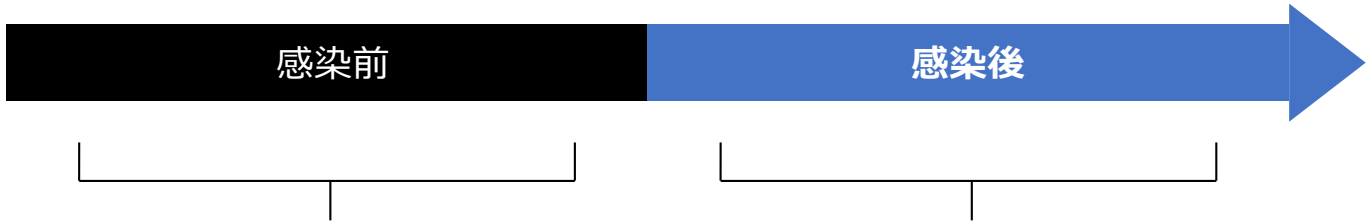
EDR（エンドポイントの検知/対応）とは

標的型攻撃などのサイバー攻撃により侵害を受けた後に、

１．攻撃者の挙動を検知してアラートを上げる（検知）
２．被害が拡大しないよう操作して収束させる（対応）

ためのソリューションです。

サイバー攻撃を**迅速に検知・対応**が重要

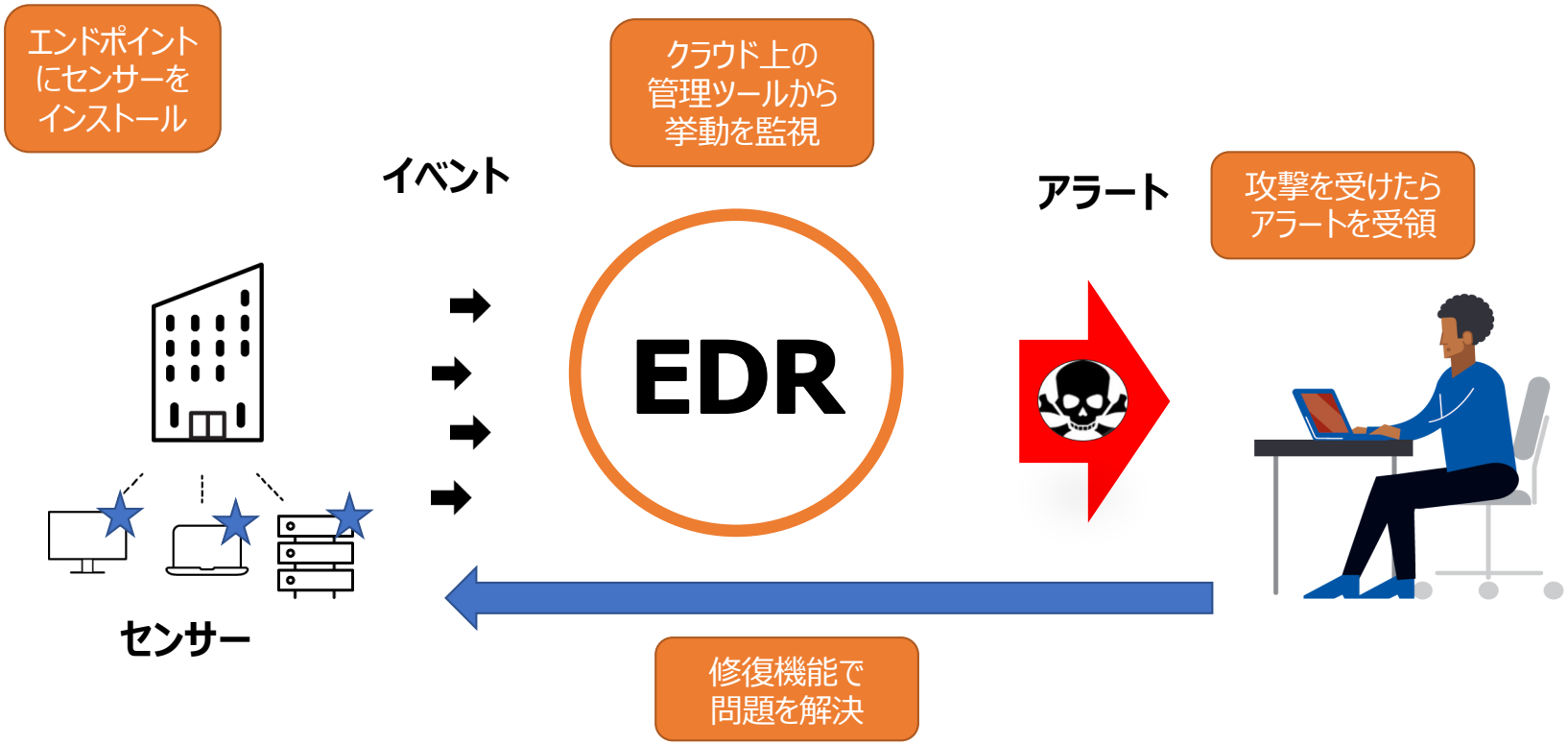


ウイルス対策

EDR (Endpoint Detection & Response)

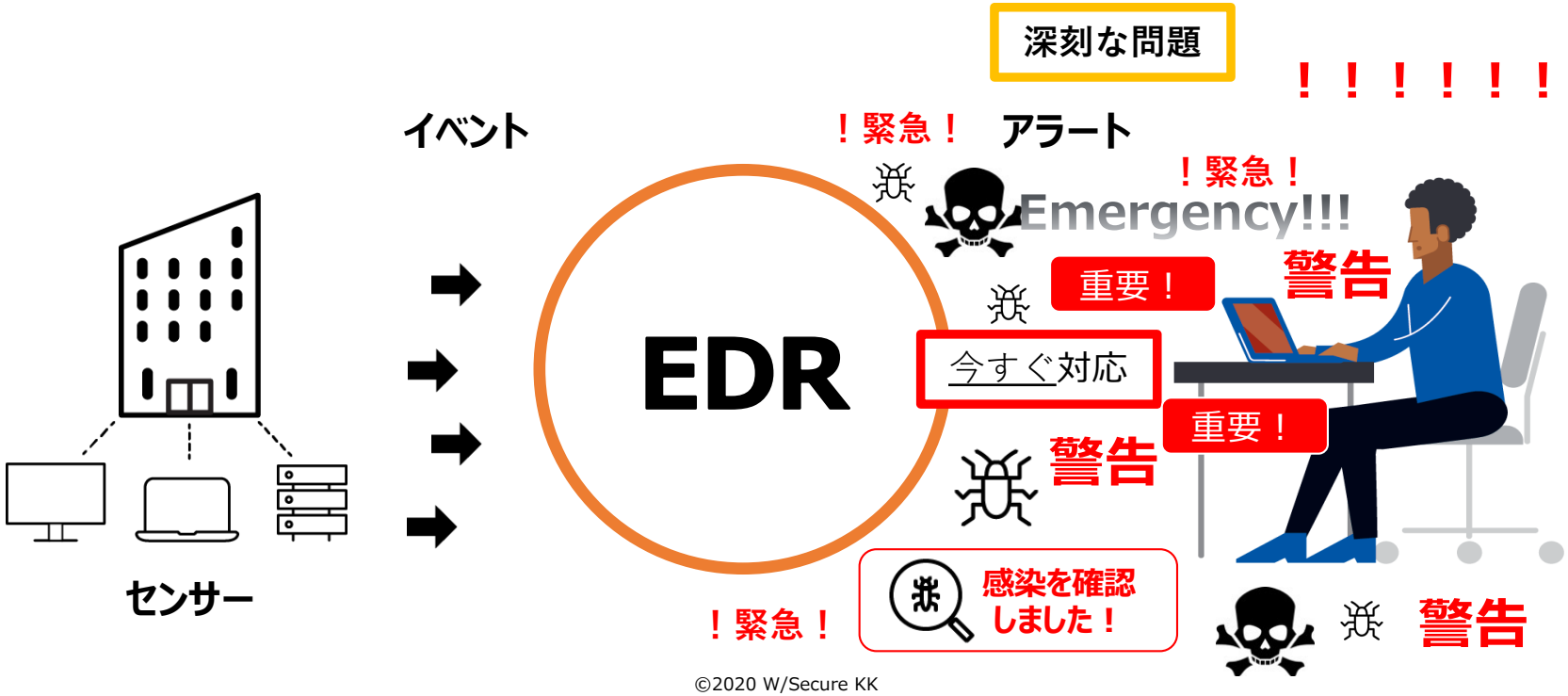
サイバー攻撃を完全に防ぐことは、もはや困難な時代です。これのセキュリティ対策は、侵害されることを前提に確立していく必要があります。ここで重要なのが、侵害されてから対処に至るまでの時間の短縮です。たとえマルウェアが感染したとしても、感染した端末をいち早く識別してネットワークから遮断し、他の端末への感染拡大を防ぐことができれば、被害を最小化できます。サイバー攻撃を受けたとしても、被害を最小化して「ビジネスを止めない」システム運用が企業価値を決めます。

EDR（エンドポイントの検知/対応）とは



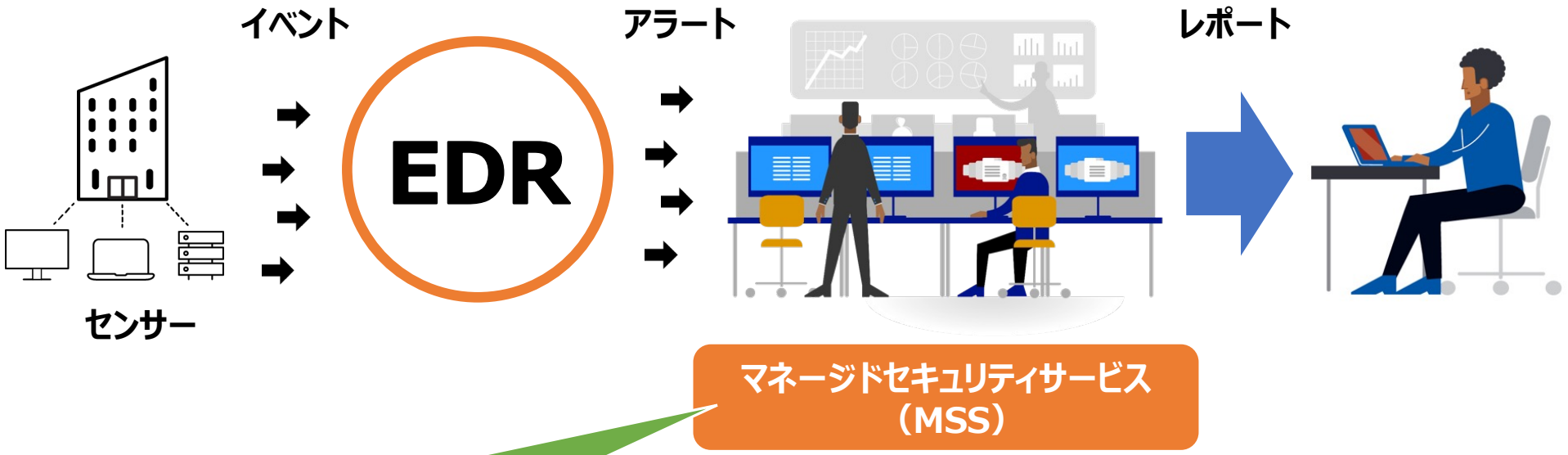
EDRの導入におけるお客様課題

EDRはアラートの分析が必要なソリューションです。



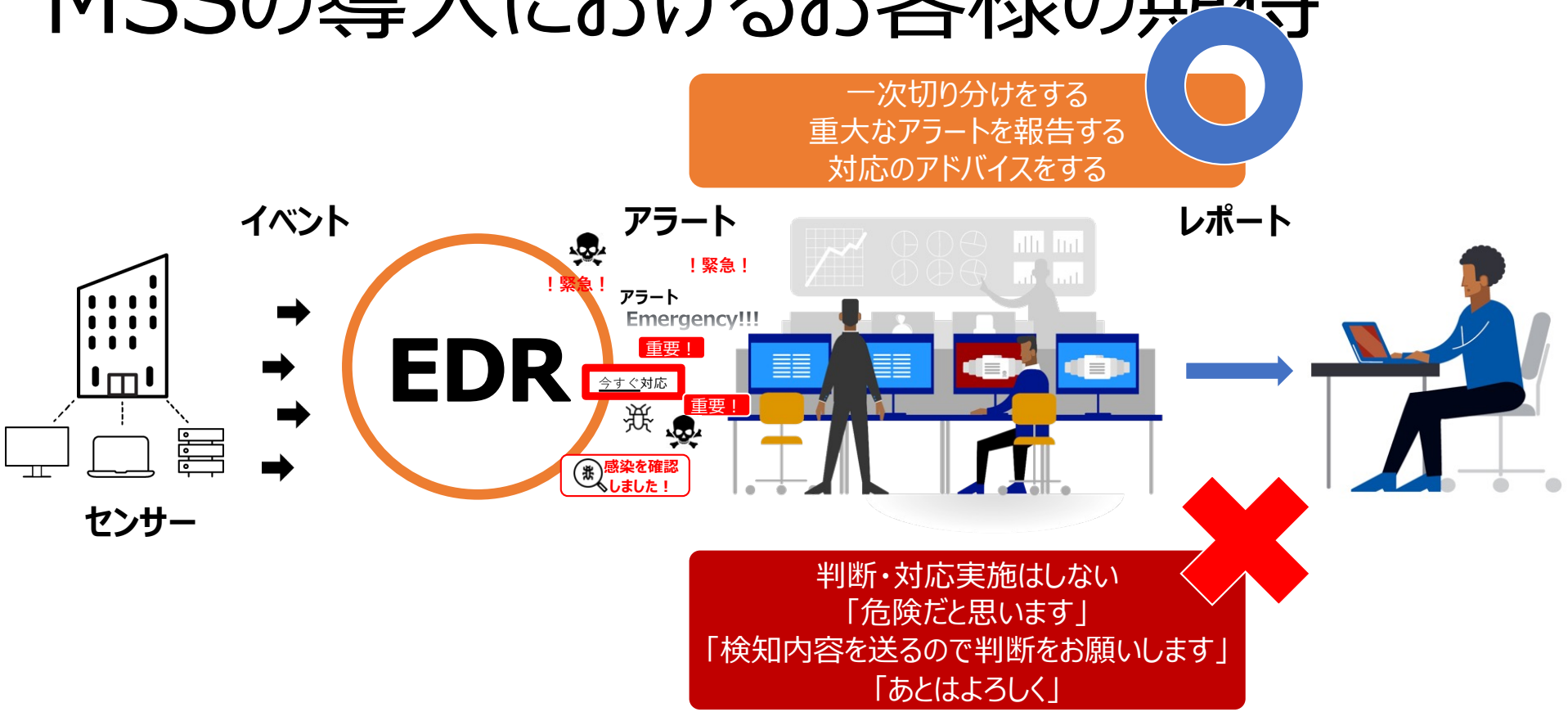
マネージドセキュリティサービス

EDR購入時にマネージドセキュリティサービス（MSS）の利用するケースが増えている



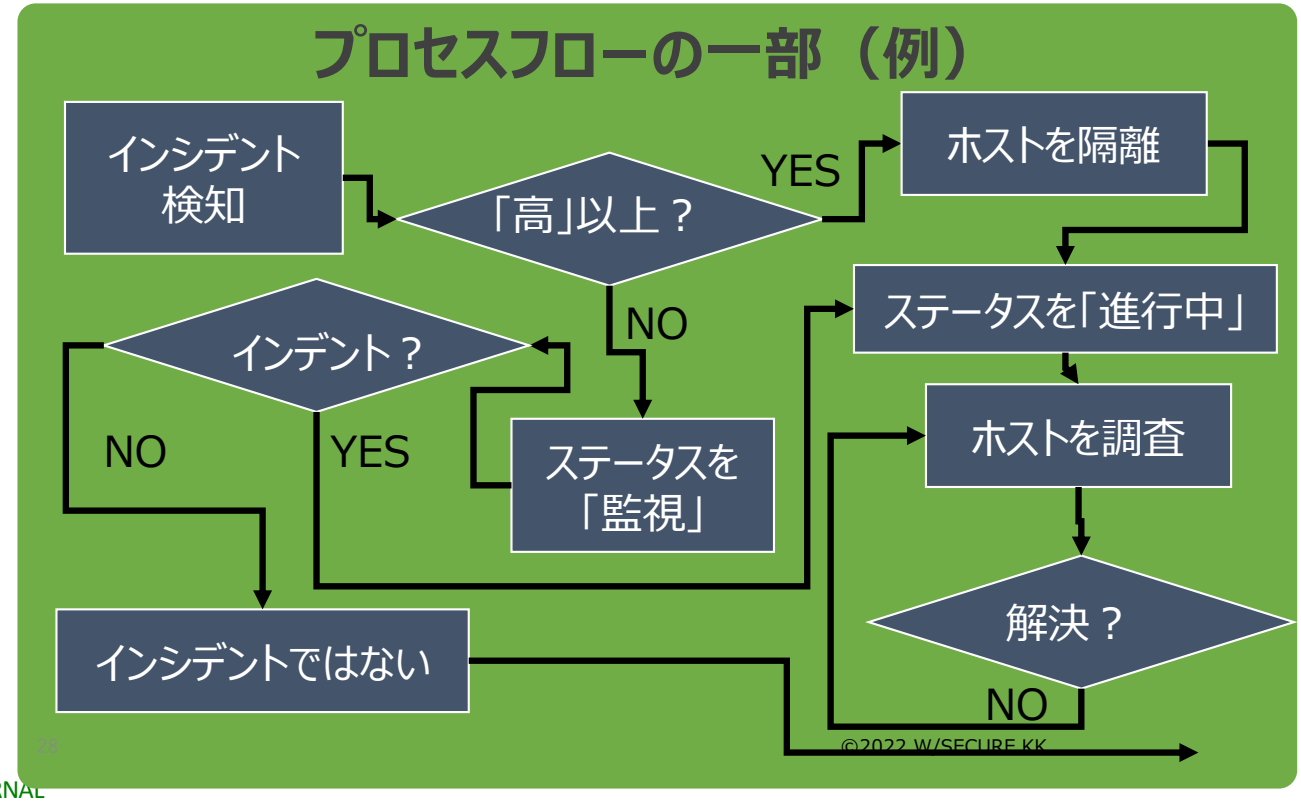
セキュリティ機器のログを外部対応組織に
転送し、イベントを監視・分析してもらう。

MSSの導入におけるお客様の期待



EDRを使った「レスポンス」フロー

対応プロセスが整備され、常にメンテナンスされている



まずは想定した攻撃に応じたプロセス一覧を作成してみる

検出結果や月次レポート等を確認し、追記・修正していく

初回の作成時は攻撃経路を中心に検討し、プロセス作成に時間をかけすぎない

インシデントの解決に支援が必要な場合

インシデントを WithSecure にエスカレーションすることができます。
分析後にインシデントを解決できない場合、インシデントを WithSecure にエスカレーションし、Broad Context Detection を解決するためのサポートと対応方法を受け取ることができます。
インシデントをエスカレーションすると、システムが WithSecure のアナリスト (専門家) に通知を送信します。アナリストは、問題を解決するためにインシデントのデータにアクセスします。

Threat validation
Threat investigation

WithSecure Elevate (ウィズセキュアに報告)
当社の専門家は、困難な状況に対応し、攻撃の封じ込めと修復に関する実用的なアドバイスを提供することにより、常にお客様をバックアップします。

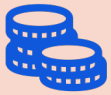
THREAT VALIDATION

過去7日間に検出されたBroad Context Detection™に関する追加情報を提供します。これには、検出の専門家が作成した概要と説明、および応答アクションが必要かどうかを判断するのに役立つその他の関連データが含まれます。

THREAT INVESTIGATION

特定のBroad Context Detection™について非常に詳細な調査を実施し、すべての直近および過去のデータを活用します。このオプションには、検出された攻撃タイプの包括的なレポートとともに、サイバーセキュリティの専門家による実用的なインシデント対応ガイダンスも含まれています。

WithSecure Elavate TOKENS



脅威の検証や調査を行う際には、そのための Token が必要です。ValidationやInvestigationには、それぞれ1つのTokenが必要です。

ウィズセキュアのパートナーは、パートナーポータルからトークンを購入することができますが、ウィズセキュアの営業からも購入することができます。Tokensの詳細については、ウィズセキュアの営業担当者にお問い合わせください。

参考：インシデント対応SLAマトリクス

事件処理の優先順位付けは、事件処理プロセス中で、おそらくもっとも重要な判断ポイントです。リソースに制限があるという理由で、起きた順に事件を処理してはいけません。代わりに、2つの要因に基づいて、処理に優先順位を付けます。

現在の影響または将来予想される影響	事件により影響を受けている、または将来影響を受ける可能性が高いリソースの重要度		
	高 (インターネット接続、公開ウェブサーバ、ファイアウォール、顧客データなど)	**中** (システム管理者のワークステーション、ファイルサーバ、プリントサーバ、アプリケーションデータ)	**低** (ユーザのワークステーション)
ルートレベルアクセス	15分	30分	1時間
データの不正な変更	15分	30分	2時間
機密データへの不正アクセス	15分	1時間	1時間
不正なユーザレベルアクセス	30分	2時間	4時間
サービス利用不可	30分	2時間	4時間
嫌がらせ※	30分	ローカルITスタッフ	ローカルITスタッフ

NIST SP 800-61「コンピュータセキュリティ インシデント対応ガイド」

※この分類は、ユーザにいやがらせをする以外の悪影響がない事件を指す。例としては、ユーザの画面に一時間に一度メッセ ージを表示するだけの悪意のコードへの感染などがある。

クラウド環境を安全に活用するために
WITHSECUREクラウドセキュリティ診断サービス(弊社宣伝)

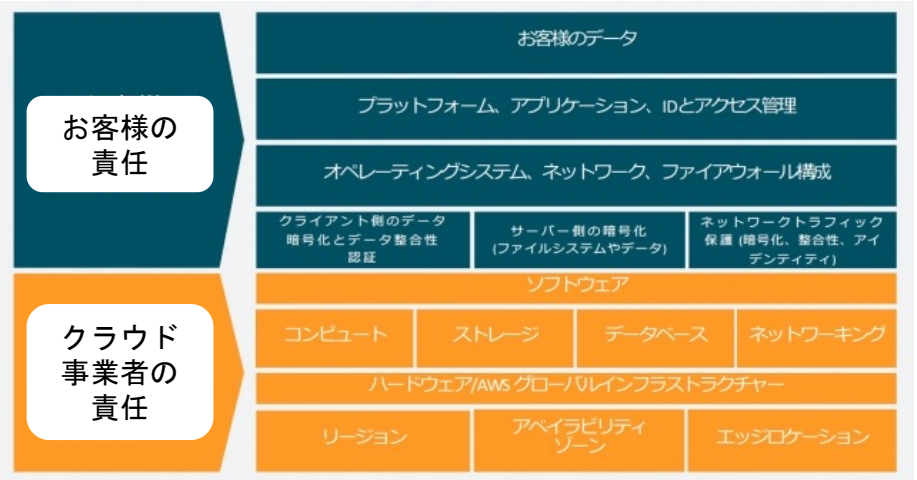
弊社の宣伝

クラウド環境診断の重要性

- クラウド環境を対象としたサイバー攻撃の約65%はユーザー側（利用者側）の設定ミスに起因している
  (WithSecure 2022)
- クラウド環境は設定箇所が多いためミスも頻発している
- 一方でユーザーがクラウド環境のセキュリティ機能やセキュリティ対策を確認するには限界がある
- 多くの企業でツールを用いたネットワークスキャンを実施しているが、それだけでは以下の理由で不十分

  - 個別のビジネスロジックに依存する問題点、たとえば一般ユーザーに管理者権限を割り当てているなどの確認はできない
  - 実際に攻撃された時にどのくらい影響があるかなど、リスクの軽重を判断することはできない
  - 診断対象の見落とし、診断のエラーや誤検出がないかを専門的な観点から確認する必要がある

クラウド環境 責任共有モデル



出典　https://aws.amazon.com/jp/compliance/shared-responsibility-model/

サイバー攻撃事例

時期	被害組織	内容
2022年12月	国内サービス業ユーザ	クラウド環境の誤設定で約1万人分の顧客データが公開された状態に
2023年5月	国内製造業ユーザ	クラウド環境の誤設定で約215万人分の顧客データが公開された状態に
2023年6月	国内報道機関	クラウド環境誤設定により約3,300人分の顧客データ (住所、生年月日、年収、金融資産額含む)が公開された状態に
2023年9月	Microsoft	GitHub上でオープンソースのAI学習モデルへAzureのSAS（Shared Access Signature）トークンを公開していたが、このトークンの設定ミスで、意図した情報以外へのアクセスが可能に。 ※38TBの内部機密情報を含む

クラウド環境の誤設定が大きな問題につながっている

WithSecure クラウド環境向けサービスの特長

多数のクラウド環境への診断実績

- 国内クラウド環境稼働基幹システムに対する、多数の提供実績
- 実施に際しては短期間でビジネスに影響があるかどうかを論理的、探究的に調査
- 多くの脆弱性・リスクを検出したことで高い評価を受領

コンサルタントの豊富な経験

- 弊社チームはレッドチーム演習の経験が豊富にあり、攻撃者が持つ最新の多様な観点を熟知
- ブルーチームの経験も同じく豊富で、実際にどのような攻撃があるかを理解し、現実的な対応方法をご提供

十分な網羅性と徹底性

- 診断対象全てに対し豊富な経験
- テスト範囲と粒度を十分に理解した上でのテスト実施

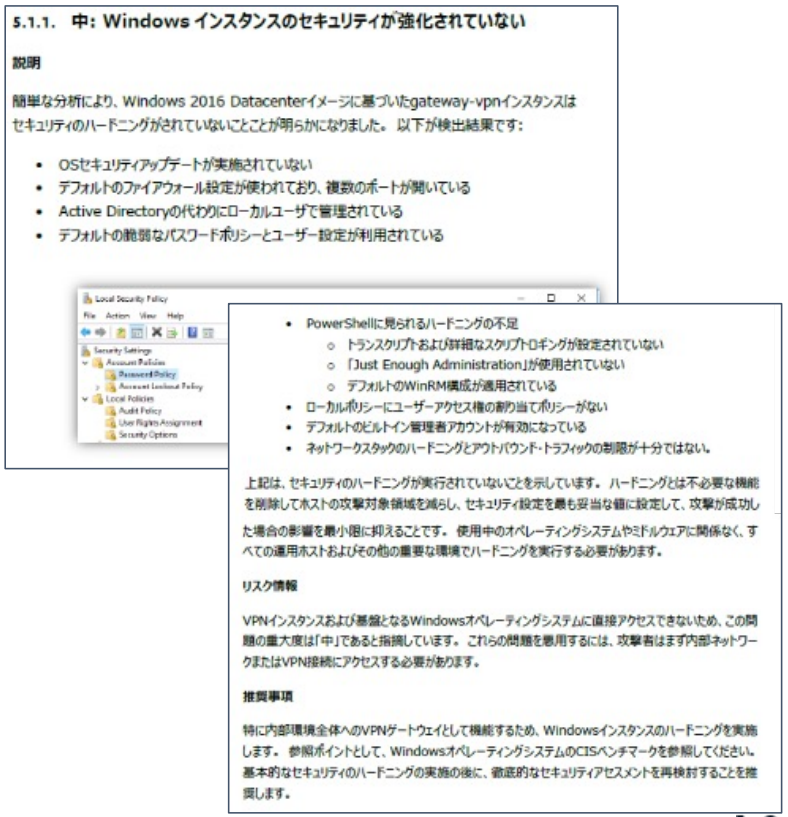
充実したフォローアップ

- 診断はレポート提出で終わりではありません
- フォローアップセッションにて、具体的で現実的な修正が可能かについて、十分な質疑応答を実施
- 対策の事例や再テストの必要性についても協議します

クラウド環境(AWS)診断

クラウド環境(AWS) 診断

- クラウド環境（例:AWS）環境に適切な設定ができているかについて、現実的かつ有効な方法を確認します。
- 設計上の問題や、設計の意図通りに AWS が設定されているかについても構成図や設計を基に確認いたします。
- 診断対象（例）
  - AWS アカウント
  - IAMアクセス
  - Amazon CloudFront
  - Amazon CloudWatch
  - Amazon Elastic Load Balancing
  - Amazon ElasticCache
  - Amazon RDS
  - AWS Cloud Trail
  - AWS Config etc….



5.1.1. 中: Windows インスタンスのセキュリティが強化されていない

説明

簡単な分析により、Windows 2016 Datacenterイメージに基づいたgateway-vpnインスタンスはセキュリティのハードニングがされていないことことが明らかになりました。 以下が検出結果です:

- OSセキュリティアップデートが実施されていない
- デフォルトのファイアウォール設定が使われており、複数のポートが開いている
- Active Directoryの代わりにローカルユーザで管理されている
- デフォルトの脆弱なパスワードポリシーとユーザー設定が利用されている

- PowerShellに見られるハードニングの不足
  - トランスクリプトおよび詳細なスクリプトロギングが設定されていない
  - 「Just Enough Administration」が使用されていない
  - デフォルトのWinRM構成が適用されている
- ローカルポリシーにユーザーアクセス権の割り当てポリシーがない
- デフォルトのビルトイン管理者アカウントが有効になっている
- ネットワークスタックのハードニングとアウトバウンド・トラフィックの制限が十分ではない。

上記は、セキュリティのハードニングが実行されていないことを示しています。 ハードニングとは不必要な機能を削除してホストの攻撃対象領域を減らし、セキュリティ設定を最も妥当な値に設定して、攻撃が成功した場合の影響を最小限に抑えることです。 使用中のオペレーティングシステムやミドルウェアに関係なく、すべての運用ホストおよびその他の重要な環境でハードニングを実行する必要があります。

リスク情報

VPNインスタンスおよび基盤となるWindowsオペレーティングシステムに直接アクセスできないため、この問題の重大度は「中」であると指摘しています。 これらの問題を悪用するには、攻撃者はまず内部ネットワークまたはVPN接続にアクセスする必要があります。

推奨事項

特に内部環境全体へのVPNゲートウェイとして機能するため、Windowsインスタンスのハードニングを実施します。 参照ポイントとして、WindowsオペレーティングシステムのCISベンチマークを参照してください。基本的なセキュリティのハードニングの実施の後に、徹底的なセキュリティアセスメントを再検討することを推奨します。

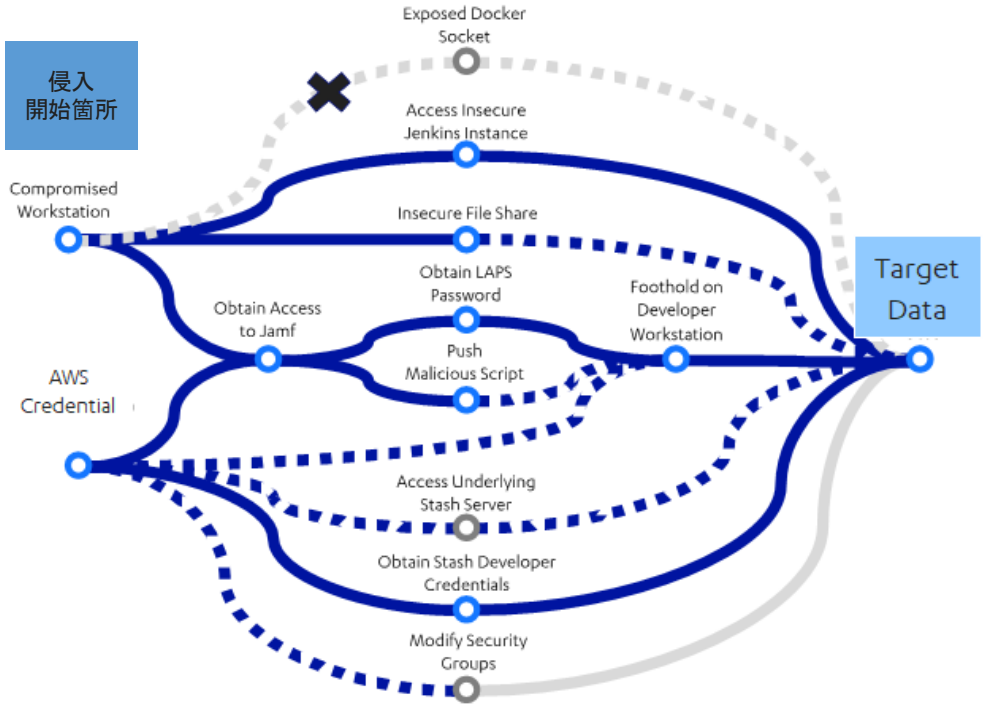
アプリケーション診断

- 対象になるアプリケーションの全体的な診断を行います。
- 診断方針は、対象システムと技術に詳しい診断者のよる手動での診断です。自動的な確認が有効な場合は、自動化のツールも使用しますが、最終的な判断と確認は手動となります。
- 技術的な脆弱性だけではなく、ビジネスロジックでの弱点や、アクセス制限の突破や、プライバシー関連の問題点や、複雑な攻撃方法まで診断します
- WithSecureの診断方法の推奨は、攻撃者観点からの手動診断とセキュリティ的に重要なソースコードと設定の部分のホワイトボックス診断です。こちらによって、診断は効率的に深くまでで き、対策案もピンポイントで提供可能です。

Category	Actions
Attack Surface 	Exercise the target using all user roles and available functionality. Examine the target to identify any artefacts. Observe the network behaviour of the target and identify protocols in use.
Business Logic 	Examine target workflows, deployment, use-cases and design.
Communication Security 	Examine the use of encryption in communications. Make use of appropriate network proxies to intercept, modify and replay messages.
Authentication 	Examine the authentication mechanism and attempt to bypass it. Examine the password policies in place.
Authorisation 	Examine the access control matrix, attempt to perform actions that are not permitted and gain access to unauthorised data.
Input Validation 	Ensure that input validation is appropriate and sufficient. This includes attempting to perform attacks including but not limited to SQL injection, CSV injection and XML entity attacks.
Data Storage 	Verify that sensitive information at rest is appropriately protected.

Attack Path 概要

- お客様ご希望“Target Data”に対して
  ・ お客様からご提供頂いた侵入開始箇所から、PC, Server, Network装置など社内システムへの攻撃侵入テストを実施
  ・攻撃シナリオ、ツール、エクスプロイトなどにより社内システムへの侵入実施
  ・ 侵入成功箇所 (右図実線) から Target Data に対する侵入テストを継続
  ・ 侵入成功箇所に対する攻撃方法、利用した脆弱性および推奨変更箇所を成果物として提出致します



Red Teaming：電子鍵の診断や物理侵入を含む総合診断

- 情報システムおよび個人情報、社内機密情報の総合診断を実施
- 電子鍵、物理侵入診断はテレビ局、発電所、インフラ系で多数の実績

https://www.youtube.com/watch?v=75gIDbhYRkA&t=

クラウド環境向けセキュリティ診断 お客様事例

CASE STUDY

株式会社エウレカ 様

F-Secure

パブリッククラウドに特化した
高品質なセキュリティ診断コンサルティングサービス
リアリティあるテストシナリオが決め手に

国内最大級の恋愛・婚活マッチングサービス「Pairs」を運営している株式会社エウレカは、
サービスのベースとなるセキュリティ対策に力を入れている。
より高品質なサービスの提供を目指す同社は、パブリッククラウドを活用するうえで、
エフセキュアのセキュリティ診断コンサルティングサービスを採用。
現実的なテストシナリオに基づいて診断を実施した結果、同社は適切な対応をとることができ、多くの気づきを得ることに成功した。

eureka

株式会社エウレカ 様
「かけがえのない人との出会いを生み出し、日本やアジアにオンラインデーティングサービス文化を定着させることを定着ビジョンに、エウレカは国内最大級の恋愛・婚活マッチングサービス「Pairs」を提供・運営している。今に生きる一人ひとりの人が、自分の望む人生を手に入れられる社会を構成することが同社の目指すところだ。

所在地	東京都港区三田1-4-1 住友不動産麻布十番ビル4階
設立	2008年11月20日
資本金	1億円(2016年3月時点)
URL	https://eure.jp/

パブリッククラウドに特化したセキュリティ診断を模索

株式会社エウレカは、テクノロジーの力で今に生きる人々が自分らしい生き方ができる社会の実現を目指すインターネット企業だ。国内最大級の恋愛・婚活マッチングサービス「Pairs」を運営しており、日本や台湾、韓国で合計すでに1000万人以上が利用している。Pairsが支持されているのは、業界最高水準の安全で安心な利用環境を提供していることが要因の1つとして挙げられる。創業当時からセキュリティ対策には力を入れ、業界初で24時間365日、自社ですべてオペレーターが常駐してカスタマーサポートを行っている。

エウレカでは「巨人の肩に立つ」という考え方を重視している。これは既存のプラットフォームや知識、スキルなどを活用できるものは活用することを意味し、同社はアプリケーション提供のインフラとしてパブリッククラウドやSaaSなどを積極的に活用している。SRE(Site Reliability Engineering)部門を率いる恩田 拓也氏は次のように語る。

「サービスの成長スピードに合わせて、我々の組織規模も追従していかなければなりません。そして、お客様に対してはきちんと価値を提供していくことが重要です。そのため、自前主義に固執することなく、使えるリソースは何でも使おうと考えています」

セキュリティも例外ではない。自社のみで実施するのか、外部の力を活用するかは顧客にとっては大きな意味を持たず、結果として適切なセキュリティ対策を施せているかが大切だという。それもあって、同社では毎年プロフェッショナルからの助言を求め、セキュリティ診断を行ってきた。しかし、従来のネットワークやアプリケーションレイヤーのみを主眼とした診断だけではなく、パブリッククラウド特有の脅威へ対抗するために、外部の力を活用しより効果的なセキュリティ診断と対策を施す必要があったという。

pairs

pairs No.1 恋活・婚活 マッチングアプリ

Head of SRE Eureka,Inc.
恩田 拓也氏

F-Secure Case Study

株式会社エウレカ | F-Secure Case Study

アマゾン ウェブ サービス(AWS)環境を熟知するエフセキュアが、リアリティあるテストシナリオを提示

2018年、エウレカは外部のセキュリティ診断サービスを調査し始めた。セキュリティ専業ベンダーを含めていくつかの会社から、サービス内容をヒヤリングするとともにアウトプットされる資料を求めた。エフセキュアもそのうち1社だったという、恩田氏は選定当時の様子を次のように振り返る。

「各社には『セキュリティ診断に高いスキルセットを有しているか』『クラウド環境のWebアプリケーションを適切に診断できるか』といった観点で話を聞きました。エフセキュアは高いセキュリティ診断の技術力をもち、また実際に示してくれたテストシナリオが網羅性に富んでいるのに加えて、AWSを利用したWebアプリケーションアーキテクチャ設計指針など、我々が利用しているパブリッククラウド環境に精通しており、当初から非常にリアリティのある話をすることができました。

テストシナリオは、我々の次のアクションにつながるものでした。

またエフセキュアからは、サンプル資料としてクラウド上でホスティングされているWebアプリケーションの診断結果ももらいましたが、それもこちらの意図した内容と合致していました」

サービスの利用が決定したのは2018年6月。コミュニケーションを迅速で円滑に進めるため、同社とエフセキュアはSlackベースのコミュニケーションツールを活用した。8月のセキュリティ診断コンサルティングサービス実施に向けて、テスト環境構築など必要な準備や流れについてエフセキュアと意思の疎通を図った。

「Slackはわれわれの間ではメインのコミュニケーション手段ですが、エフセキュアと同時の呼吸で情報のやりとりができて、診断の実施までのコミュニケーションは非常に順調に進みました」(恩田氏)

次のアクションにつながるレポート脅威の可視化や「気づき」に満足

2018年8月、予定通りセキュリティ診断が実施された。エフセキュアはその結果に基づいて、対応すべき内容に優先順位をつけた詳細レポートとして提供した。エウレカのSRE部門では、これを受けてタスクリストを作成し対応を図っていったという。恩田氏は今回のセキュリティ診断サービスの利用効果を次のように語る。

「セキュリティ対策に終わりはありません。しかし今回、パブリッククラウド環境に最適化された網羅性の高いセキュリティ診断を受けたことで、効果的なセキュリティ対策を実行に移すことができました。最も恐ろしいのは脅威に気づいていないということです。それを可視化できたとともに、こういう箇所ももっと留意するべきという『気づき』も得られました。このようなセキュリティ診断を、専門人材を含め社内リソースで実現しようと思えば、膨大なコストと工数を覚悟する必要があった思います」

今後もエウレカは、セキュリティ対策に全力を注ぐ一方で、セキュリティ診断などではエフセキュアに支援を求めていく。セキュリティ診断は、人間が健康を維持するのに毎日の生活習慣に自ら留意しながらも、定期的にきちんと人間ドックを受けるようなものだと恩田氏は語る。

エフセキュア サイバーセキュリティ コンサルティングサービス

サイバー攻撃に対するビジネス資産の脆弱性をプロの視点で顕在化

エフセキュア サイバーセキュリティ コンサルティングサービスのサイバーセキュリティ診断は、システムインフラにおける設計上の欠陥や脆弱性、アプリケーション固有の弱点を明らかにするとともに、ビジネス資産および顧客データを確実に保護する方法をご提案します。

エフセキュア株式会社
〒105-0004
東京都港区新橋2-2-9 KDX新橋ビル2F
Tel. 03-4578-7710
E-mail: japan@f-secure.co.jp

お問い合わせ先

www.f-secure.com

WITH secure

クラウド環境向けセキュリティ診断 お客様事例


Case study

「WithSecure™ コンサルティング」の活用で、
サーバーレス環境でのセキュア開発を実現、
デジタルビジネスをさらに加速

「水曜どうでしょう」などで知られるバラエティ番組を制作する北海道テレビ放送株式会社は、コンテンツ配信やECサイトなど、デジタルを活用したビジネスにも積極的に取り組んでいる。そんな中、同社の課題として浮上していたのが、システム開発時におけるセキュリティの確保だった。この課題を解決するため、ウィズセキュアの「WithSecure™ コンサルティング」を利用し、セキュリティ診断、およびクラウド環境の設計レビューとガイドライン作成を実施。サーバーレス環境におけるセキュア開発を実現し、デジタルビジネスをさらに加速させるシステム基盤を構築できた。

Company
北海道テレビ放送株式会社

Country
日本

Industry
放送業

Solutions
セキュリティ脆弱診断


導入事例 | 北海道テレビ放送株式会社 2

北海道テレビ放送株式会社 様

札幌市に本社を構える北海道テレビ放送株式会社は、1968年に北海道初のUHF局として誕生した民間放送局である。「あしたへ、ユメミル、チカラ」をスローガンに、地域の基幹放送局として、ニュース・ドキュメンタリー、ドラマなど、さまざまな分野の番組制作や放送を通じて地域の未来に貢献していく。

所在地 〒060-8406 札幌市中央区北1条西1丁目6番地
創立 1967年12月1日
資本金 7億5千万円
URL https://www.htb.co.jp/

**ライブ配信やECサイト開設など
デジタル活用を積極的に推進**

1968年に放送を開始した北海道テレビ放送株式会社（以下、HTB）は、札幌に本社を構える北海道を対象とした民間放送局だ。なかでもバラエティ番組「水曜どうでしょう」は高い人気を獲得、全国47都道府県で放送された実績がある。

HTBでは番組制作だけでなく、オンデマンド放送やライブ配信のほか、番組関連グッズやDVD、マスコットキャラクターを販売するECサイトの開設など、デジタル事業にも積極的に取り組んでいる。コンテンツビジネス局ネットデジタル事業部の三浦 一朗氏は、「2022年に策定した中長期経営ビジョン「HTB2030」では、従来の番組制作やコンテンツビジネスに加え、動画配信とECサイトの融合、さらに他の地方放送局や自治体のデジタル配信を支援する「デジタルプラットフォーム」の構築など、Webメディアやデジタルを活用した地方創生ビジネス推進を掲げています」と説明する。

**サーバーレス環境でのシステム開発における
セキュリティの確保が喫緊の課題に**

HTBがデジタル事業に舵を切るなかで、課題として浮上していたのが、動画配信やECサイトを運営するプラットフォームのセキュリティだった。

「インフラは主にAWSを利用していたのですが、システム開発におけるコーディングに専念したいと考え、サーバーレス環境を採用していました。しかし、いざサーバーレス環境で開発を進めていくなかで、セキュリティを強固なものにしていくためにはどんな点に留意し、どのような対策を施せばよいのか分かりませんでした」（三浦氏）

サーバーレス環境におけるセキュリティを確保するため、HTBではAWS Well-ArchitectedやAWSのベストプラクティスを調査・参照したほか、さまざまなセキュリティベンダーに提案を依頼した。

北海道テレビ放送株式会社
コンテンツビジネス局
ネットデジタル事業部
三浦 一朗 氏


導入事例 | 北海道テレビ放送株式会社 3

たという。「しかし、ベンダー側の提案の多くは、EC2といったインフラ側でのセキュリティ対策を前提にしたもので、当社が求める要件に合致しませんでした。また市販のセキュリティ診断ツールも検討しましたが、稼働中に自動でレポートのみが出るタイプが多く、当社が抱える不安や疑問を本質的に解消できそうにありませんでした」と、三浦氏は振り返る。

**高度な知見とグローバルでの実績
親身な対応を評価しウィズセキュアを選択**

そうしたHTBの悩みを解消してくれたのが、ウィズセキュアの「WithSecure™ コンサルティング」だった。ウィズセキュアの専任のコンサルタントが顧客企業のあらゆる環境やシステムに応じた脅威分析やセキュリティ診断のほか、設計レビューやガイドライン作成を行うものだ。

「AWS環境で数多くのセキュリティ診断の実績があること、バックエンドからフロントエンドまで総合的な対応が可能なこと、そして、唯一サーバーレス環境のセキュリティについても高度な知見を持っていることがウィズセキュア選定の決め手となりました。また、勉強会後のコミュニケーションの場でも気軽に相談に乗ってくれたことや、運営としていたセキュリティの不安にも丁寧に説明してもらえました」（三浦氏）

**ウィズセキュアの脅威分析レポートを
セキュリティガイドラインとして活用**

ウィズセキュアによるコンサルティングは2021年2月から約1ヶ月かけて実施された。今回はバックエンド側のシステムを中心に脅威診断や分析が行われ、その結果が脅威分析レポートとして提示された。三浦氏は、「レポートには想定しうる脅威や攻撃による影響範囲、セキュリティを確保するために必要な対策などが具体的に提示されていてとても分かりやすいものでした。加えて、ウィズセキュアによる対面での説明や質疑応答といったフォローアップによって不明点がさらに明確化されたことも大きな評価ポイントです」と話す。脅威分析レポートは、HTBのシステム開発におけるセキュリティガイドラインとして活用されているという。

WithSecure™コンサルティングの効果は、セキュアな開発の促進にとどまらない。社内のセキュリティ意識にも変革をもたらしているという。三浦氏は、「一般にセキュリティはコストと捉えられがちですが、私はインフラやシステムに投資するのと一緒と考えています。

WithSecure™ コンサルティングの利用前後で、社内のセキュリティ対する危機感や投資意識にも変化が生じているように感じています」と語る。

**デジタルビジネスのさらなる拡大に向け
ウィズセキュアの支援に期待**

WithSecure™ コンサルティングにより、セキュアな開発を実現できたHTB。三浦氏は、「運用フェーズがメインになった現在でも、フロントエンドシステムをはじめ、データの取り扱いやセキュリティ面で考慮すべき項目は多岐にわたります。また、現在のシステムがきちんとセキュリティが確保された状態になっているのか「答え合わせ」もしてみたいと考えています」と語る。最後に三浦氏は、次のようにセキュリティ対策に悩んでいるシステム担当者にメッセージを寄せてくれた。

「ウィズセキュアのサービスを通じて、セキュリティ対策も『今すぐやるべきこと、今後やらないといけないこと』を選別すれば、スモールスタートができることに気づかされました。企業ごとに異なるセキュリティ要件に対しても、ウィズセキュアは適切な提案を寄せてくれます。セキュリティ対策に悩んでいるのならば、一度ウィズセキュアに相談して、『はじめの一歩』を踏み出してみてはいかがでしょうか」（三浦氏）

"レポートは、想定される脅威や攻撃による影響範囲、セキュリティを確保するために必要な対策などが具体的に提示されています。また、ウィズセキュアによる対面での説明や質疑応答といったフォローアップしてもらった点も大きな評価ポイントです。"

北海道テレビ放送株式会社
コンテンツビジネス局
ネットデジタル事業部
三浦 一朗氏

クラウド環境における Serverless 環境 へのセキュリティ診断実施例

Salesforce環境における セキュリティリスクと対策

リスク 1　Salesforceの設定ミスに起因する情報流出

リスク 1　Salesforceの設定ミスに起因する情報流出

年　月	事例
2020年12月	金融庁の注意喚起で金融機関が対応急ぐ、セールスフォース製品への不正アクセスで | 日経クロステック（xTECH） https://xtech.nikkei.com/atcl/nxt/news/18/09416/
2021年1月	イオンでも不正アクセス、セールスフォース製品の設定不備で | 日経クロステック（xTECH） https://xtech.nikkei.com/atcl/nxt/news/18/09526/
2021年2月	クラウド型システムへの第三者からのアクセスについて | 両備システムズ https://www.ryobi.co.jp/news/notification20210210
2021年3月	クラウド型口座開設システムへの第三者のアクセスについて - 株式会社SMBC信託銀行 https://www.smbctb.co.jp/contents/aboutus/news/pdf/j_pr_210308_01.pdf

Salesforce からの情報流出リスクへの対策

- Salesforceの推奨設定に合わせた対応の実施
- Salesforceリリースノートを確認し、ビジネスや業界の要件に沿った設定を実施
- 第三者による診断サービスの利用

WITH secure

Salesforce 環境 セキュリティ ご相談例
国内金融機関様

Salesforce 環境 サイバーセキュリティ診断

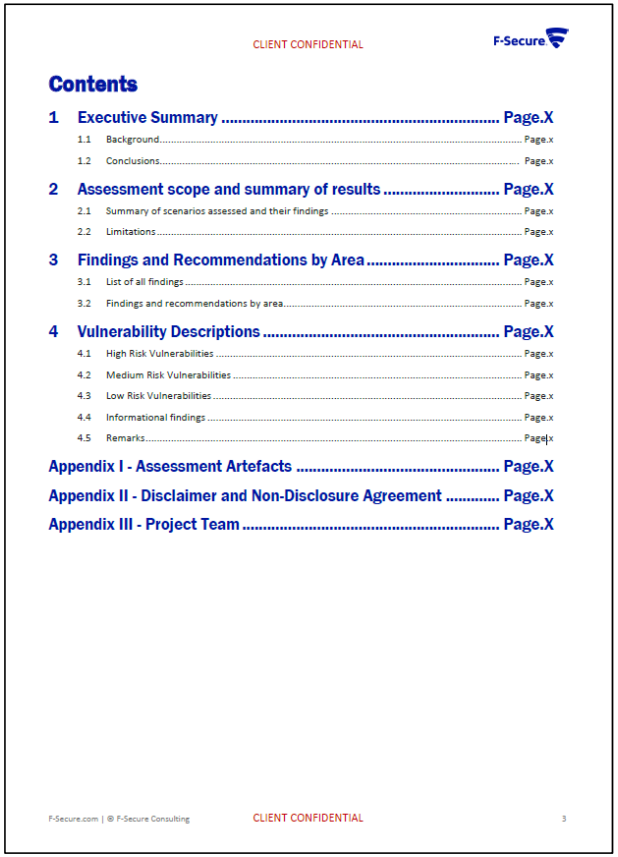
既に複数年にわたり Salesforce 環境を利用しており、顧客情報および社内情報が Salesforce環境に保存されているため下記の対策を講じたい。

1) Salesforce環境の設定ミスによる外部情報流出対策
2) Salesforce環境に保存ファイルのマルウェア、ランサムウェア対策

WithSecure™ Salesforce環境診断の特長

10年以上にわたる Salesforce 環境に対する設定診断の実績および、過去のサイバー攻撃対策事例を元に、Salesforce 環境に対する:

- お客様 Salesforce Sandbox 環境に対する、Whitebox 形式による網羅的セキュリティ診断(初回診断)
- 1年間 4回の継続的 Security Alert Review をご提供します



CLIENT CONFIDENTIAL

F-Secure

Contents

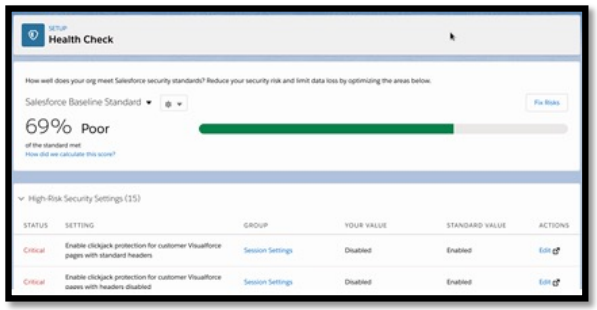
ご提案の概要 1/2

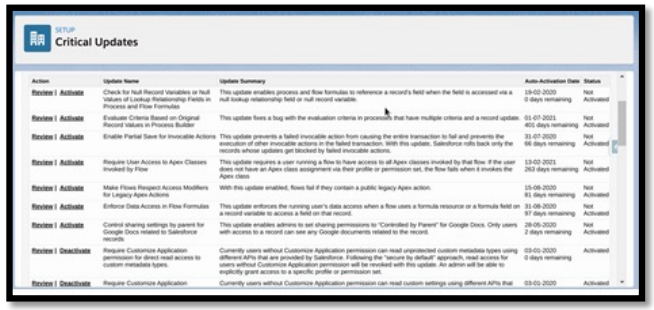
1. Salesforce 環境 セキュリティ設定, ハードニング（ 初回実施 ）
   - WithSecure™ セキュリティコンサルティング 提供実績あり
   - 特定の Salesforce 環境 Org IDを対象に実施
   - Authentication, Access control, Network/boundary security controls, Data security and encryption, Secrets management, Detective controls などの設定確認、ハードニングレビューを実施致します
   - 指摘点に関するサンプルレポートを打ち合わせにてご説明させていただきます。

ご提案の概要 2/2

2. お客様 Salesforce 環境の定期的なアップデート, セキュリティアラートレビュー
   - 毎月/四半期ごとの実施
   - お客様環境セキュリティアラート/ベースラインステータス/アップデートのレビュー
   - セキュリティ上の対策が必要かの分析と提案

   ご提案(1) にてハードニングを実施した環境を対象に、Health Check , Critical Updates内容等を確認の上、WithSecureから セキュリティ対策を分析、ご提案 いたします





リスク 2

Salesforce 環境に対する マルウェア、悪意あるURLの送付による攻撃

投影のみ

Cloud Protection for Salesforce Q2/2023

スキャンされたファイルの数
20,950,361
+7% QTQ

スキャンされたURLの数
2,387,733
+4% QTQ

平均スキャン時間
0.784s

平均ファイルサイズ
423 kB

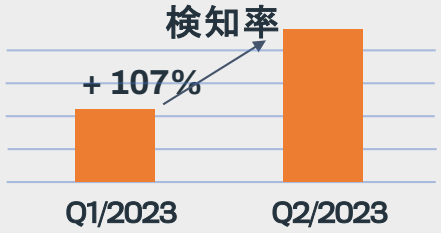
Top 10 スキャンしたファイルタイプ

1. PDF 11,690,117
2. Jpeg 1,935,055
3. PNG 1,645,974
4. Word 1,158,135
5. html 1,093,367
6. Json 615,348
7. CDFV2 573,617
8. Excel 530,905
9. Text 441,452
10. Zip 220,666

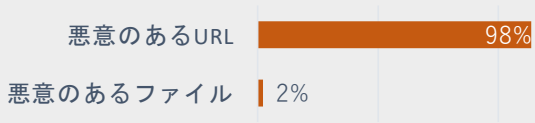
Top 10 マルウェア

1. HTML/Phish.SBH
2. TR/Inject.Gen
3. JS/Phish.G7
4. HTML/Phish.PATB
5. HTML/Infected.WebPage.Gen2
6. Trojan:HTML/Phishing.C
7. HTML/Phish.SBG
8. JS/Phish.G10
9. Trojan:W32/Generic.relch!fsmin
10. HTML/Phish.kjh

検知率

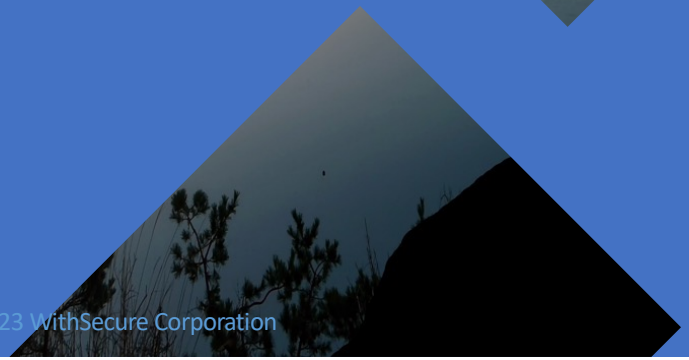


見つかった悪意のあるファイル/URL



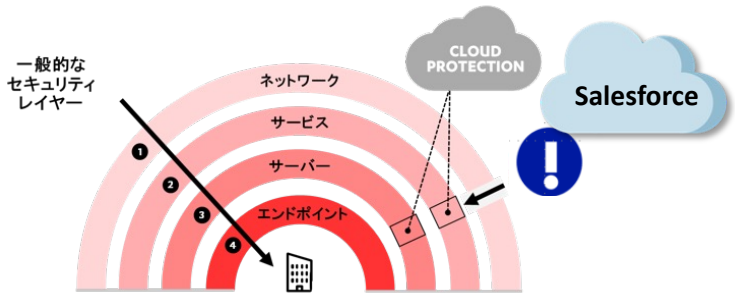
データは1000以上の保護されたSalesforce組織から収集される

Salesforce 環境へのマルウェア対策
国内ユーザ様 採用事例



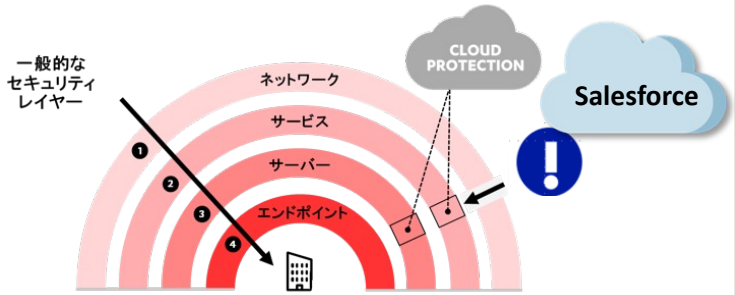
INTERNAL

クラウドプラットフォーム上にセキュリティを導入する理由



- クラウド上 コンテンツの安全性確保はユーザ側の責任です
- 企業の社内端末は、エンドポイントセキュリティにより保護されますが、Salesforceはパートナーやエンドユーザとコンテンツを共有する場としても使用されます
- このような場所を通じてマルウェアが拡散されてしまうと、
企業のイメージダウンにもつながります
- クラウドプラットフォーム上にセキュリティ機能を導入することで、組織の内外に関わらず、安全性を確保することが可能になります

Salesforce 社 のコメント



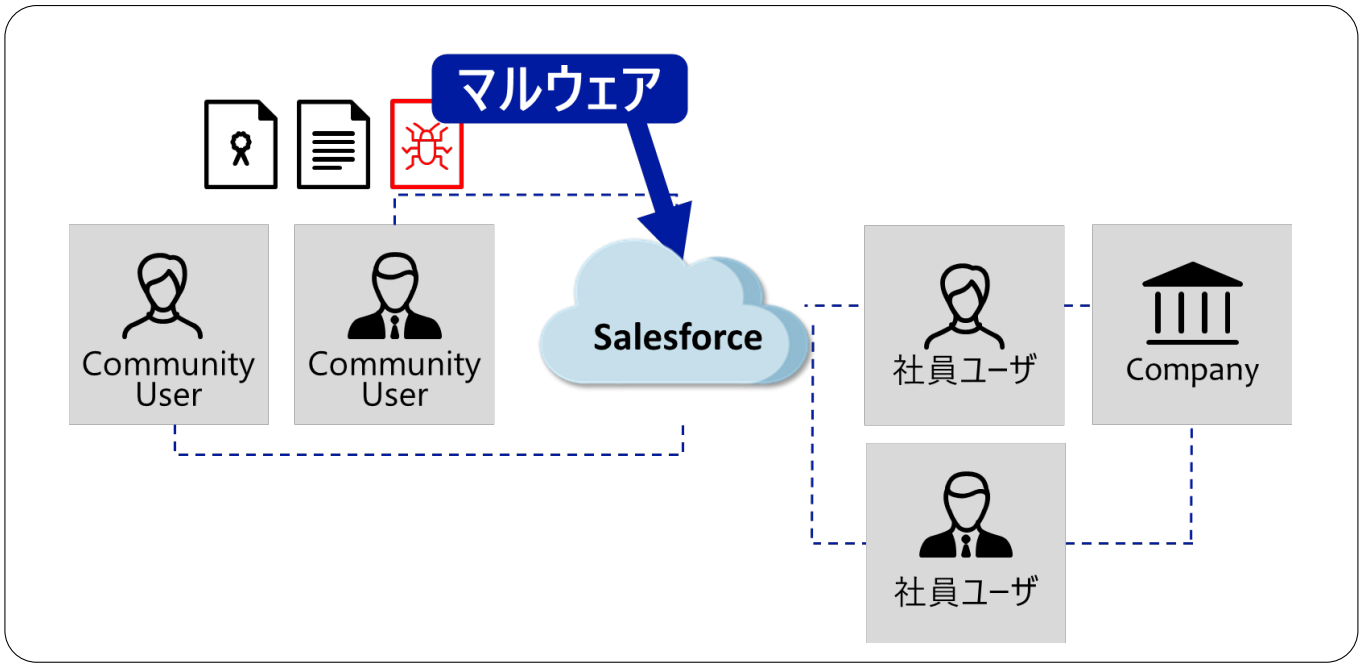
Salesforce サービスではデータプライバシー保護の観点から、ウイルススキャンまたは検疫はお客様データをファイルデータとして取り扱うため実施しません。システムはお客様より受領したデータをデータベースにエンコードされた形式のまま格納しており、そのデータを解釈し実行することはありません。

したがってウイルスに感染したファイルを格納しても他のファイルやシステムに感染することはありません。マルウェアに関する脅威を低減するための施策として、お客様側で最新のウイルス対策またはマルウェア対策ソリューションを実行いただくことを推奨しています。

Salesforceご利用ユーザ様が(自社で)必要なセキュリティ対策

お客様 ご相談例

- 外部Community Userによるファイルアップロード
- Mail to Case, Chat botなどによるメール内でのURL送付
- Salesforce と外部システム連携に伴うファイル受信



**Salesforce へアップロードするファイルの安全性は
エンドユーザ様の側でチェックする必要があります**

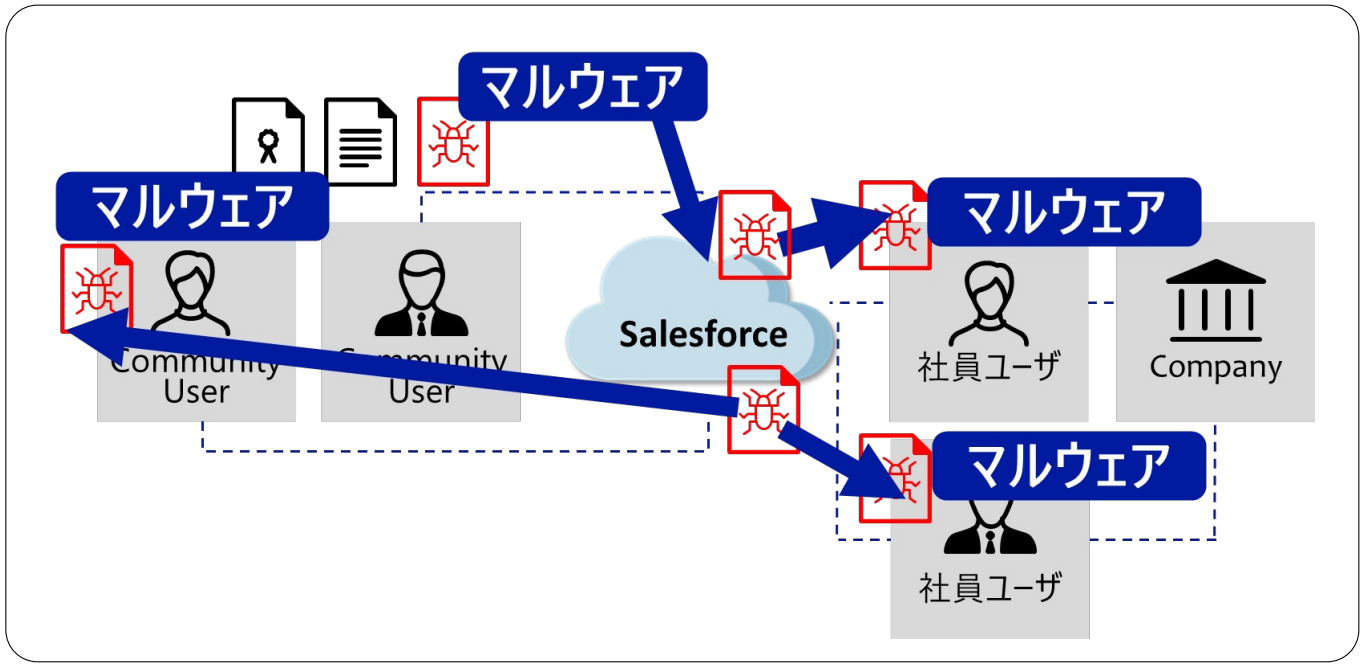
Salesforceご利用ユーザ様が(自社で)必要なセキュリティ対策

お客様 ご相談例

・外部Community Userによるファイルアップロード

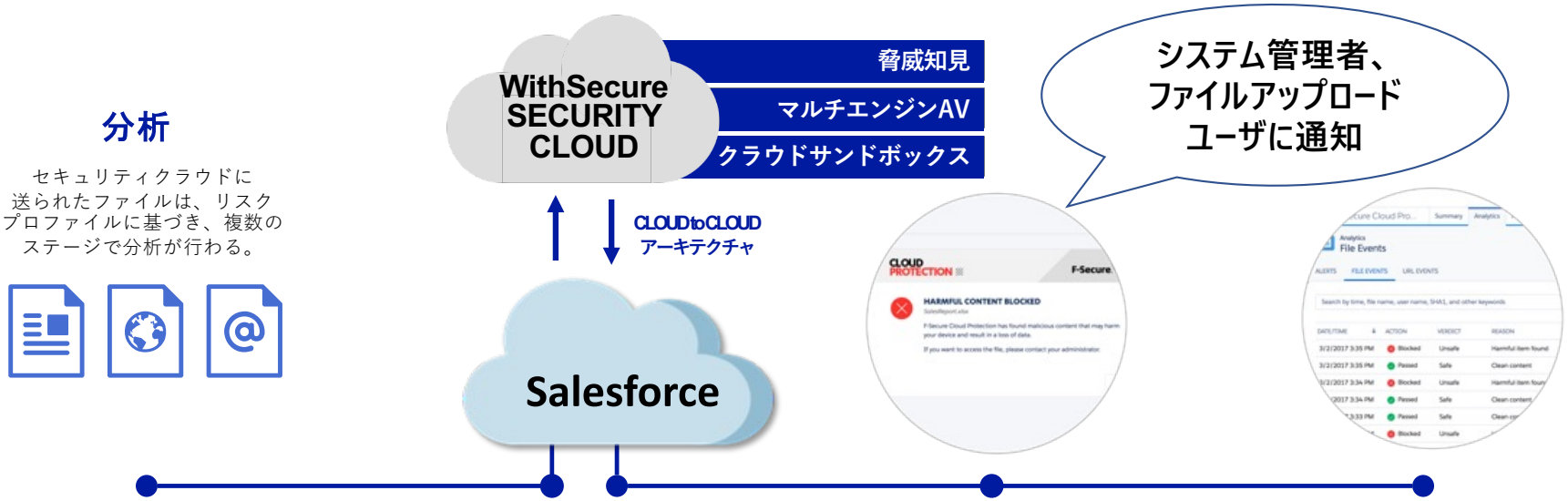
・Mail to Case, Chat botなどによるメール内でのURL送付

・Salesforce と外部システム連携に伴うファイル受信



外部 Community User アップロードコンテンツへの
セキュリティ対策 ご希望案件が、急速に増加しています

Cloud Protection for Salesforce 動作概要



お客様ファイル

Salesforce社と共同で、Salesforceプラットフォームのネイティブなセキュリティ機能を補完するために開発されました。Salesforce 環境にアップロードされたすべてのファイルやURLを介したランサムウェアなどの高度なマルウェアからリアルタイムに保護します。

Salesforce 環境

ユーザがアップロード/ダウンロードするコンテンツやURLを、セキュリティ検査を実施
クラウドツークラウドの技術により、ミドルウエアや追加の設備は不要。

検出

危険なコンテンツが検知された場合、ユーザに検知画面を表示。
何故ブロックされたのか
を明示することで、
次のアクションを容易に。

対応

危険なコンテンツが検知されると、管理者に自動的に警告を送信。
豊富なレポートとセキュリティ分析、追跡情報により管理者はインシデントに効果的に対応。

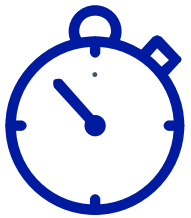
WITH secure

CLOUD to CLOUD
アーキテクチャ

ミドルウェアのインストールや
新規サーバの導入は不要

※ Salesforce AppExchange からの導入するため
お客様PC環境への
ソフトウェアインストールや
ネットワークの設定変更は必要ありません

数分間で
インストール完了



AppExchange
「今すぐ入手」で導入は完了

※エンドユーザ様向け
30日間 無償評価ライセンスを使用した
テストも実施可能です

WITH secure

国内の主な採用事例

金融機関様	銀行口座開設ポータル	個人ユーザ 申込書類 アップロード
金融機関様	法人融資申込・受付ポータル	法人ユーザ 申込書類 アップロード
金融機関様	保険商品申込ポータル	法人ユーザ 申込書類 アップロード
金融機関様	保険金 申請Webサイト	個人ユーザ 保険金申請書類・関連書類ファイル アップロード
官公庁様	給付金電子申請Webサイト	個人ユーザ 申請書類・個人情報書類ファイルアップロード
官公庁様	検査実施登録Webサイト	個人ユーザ 申請書類・個人情報書類ファイルアップロード
地方自治体様	検査申込・申請Webサイト	個人ユーザ 申請書類・個人情報書類ファイルアップロード
地方自治体様	検査実施登録Webサイト	個人ユーザ 申請書類・個人情報書類ファイルアップロード
製造業様	B2B 購買システム	法人ユーザ 注文書・納品書・請求 ファイルアップロード
製造業様	コールセンターシステム	個人ユーザ お問合せ受付・画像ファイルアップロード
流通ユーザ様	転職・就職情報Webシステム	個人ユーザ 申込書類・個人情報書類ファイルアップロード

サービス提供実績多数

ヤフー株式会社様 CPSF ご採用事例

WITH secure

ヤフー株式会社様 CPSF ご採用事例

ヤフー株式会社 様

創業以来、国内初のポータルサイト「Yahoo! JAPAN」をはじめとした多種多様なインターネットサービスを展開しながら、常に時代の真ん中でインターネットの可能性を追求し続けている。2018年10月にはソフトバンクと連携しスマートフォン決済サービス「PayPay」の提供を開始し、政府が推進する「日本のキャッシュレス化」を牽引するための中心的な役割も担っている。

所在地	東京都千代田区紀尾井町1-3 東京ガーデンテラス紀尾井町 紀尾井タワー
資本金	300百万円（2019年10月1日現在）
URL	https://about.yahoo.co.jp/

ヤフオク!やYahoo!ショッピングの問い合わせファイルのマルウェア混入リスクへの対策

ヤフー株式会社は、日本最大級のポータルサイト「Yahoo! JAPAN」を筆頭に、「ヤフオク!」や「Yahoo!ショッピング」といったEC事業、コンテンツ配信サービスなど、質量ともに充実した数多くのインターネットサービスと幅広いユーザーを誇る。

8,000万ものユーザーを抱える同社だけに、問い合わせ件数も膨大であり、各サービスを合算した1日の問い合わせ件数は数千件にものぼる。そうした問い合わせ受付サービスのプラットフォームとしてヤフーが採用しているのがSalesforceだ。このSalesforce上で日々の問い合わせ対応をするなかで、ヤフーでは更なるセキュリティ強化を目指すこととなった。

そのポイントは、一般ユーザーからの問い合わせメールなどに添付されるファイルやURLの安全性の確保だった。カスタマーサポートのためのシステムの運用管理を担う、ヤフー株式会社 CS本部 クラウドオペレーション リーダーの徳山 敦氏はこう振り返る。

「お問い合わせをいただくお客様側のクライアント環境は把握できませんので、パソコンやスマートフォンにアンチウイルスソフトを入れていなかったり、OSのアップデートが行われていなかったりといったことも考えられます。そうなると添付ファイルにマルウェアなどが混入されているリスクも考慮しなければいけません。しかし、Salesforce側では添付ファイルの中身をセキュリティチェックする機能は提供されていないため、マルウェア混入ファイルが保存・外部転送されるリスクが想定されます。このためヤフー側で何らかの対策をすることが急務であると考えました[注]」

ヤフー株式会社 CS本部
クラウドオペレーション リーダー
徳山 敦 氏

注：セールスフォースサービスではデータプライバシー保護の観点から、ウイルススキャンまたは検疫はお客様データをファイルデータとして取り扱うため実施しません。システムはお客様より受信したデータをデータベースにエンコードされた形式のまま格納しており、そのデータを解釈し実行するようなことはありません。したがってウイルスに感染したファイルを格納しても他のファイルやシステムに感染することはありません。マルウェアに関する脅威を低減するための施策として、お客様側で最新のウイルス対策またはマルウェア対策ソリューションを実行いただくことを推奨しています。

ポイントはクラウド連携！導入はわずか数分で完了

Salesforce上でやり取りされる添付ファイルへのマルウェア混入や危険なURLの脅威にどう対処すべきか――解決策の模索は2020年に入ってからスタートした。ヤフーが求めたのは、セキュリティアプライアンスを物理的に設置したり、問い合わせを受け付けるコミュニケーター（オペレーターの呼称）のPCなどに特定のアンチウイルスソフトをインストールせずとも、マルウェアが排除されたファイルやリンクの安全性が確保できるようなソリューションだった。なぜなら、これらの方法では、不特定の場所からのファイル送付や、コミュニケーターのミスなどに十分に対処することが難しいからである。

このような条件でソリューションの検討を行ったヤフーだったが、CISO室の迅速な判断により2月にはウィズセキュアの「WithSecure™ Cloud Protection for Salesforce（以下、CPSF）」の導入が決定したのである。CPSFは、WithSecure™ Security Cloud（セキュリティクラウド）とSalesforceのクラウドとの間をAPI連携することで、Salesforceのプラットフォームのパフォーマンスを低下させることなく、クラウド上で共有されているファイルとURLリンクの安全性を検証することができるソリューションだ。

「一般的に言えば、1日数千件もの問い合わせメールをチェックできるソリューションの導入となると、インストールや設備導入などにかなりの時間と手間を要するはずです。しかし、CPSFはクラウド間連携のソリューションなので、ネットワークの設定変更やクライアント端末へのソフトウェアのインストールなども必要ありません。ウィズセキュアの触れ込み通り、本当に数分で導入できてしまったのは驚きでしたね」と徳山氏はコメントする。

徳山氏のチームでは、まず無償ライセンスのCPSFの動作をサンドボックス上で確認。Salesforce側のパフォーマンスが低下しないことなど、さまざまなヤフー側の要件を満たしていることが確認できると、一気に導入を進めたのだった。

わかりやすいUIやスキャン時のタイムラグのなさも評価

ヤフーがカスタマーサポートのSalesforceにおいてCPSFの利用を開始したのは3月のこと。これまで数百人のコミュニケーターが利用しているが、特別問題などは生じていないようだ。

「管理画面や通知のデザインが明瞭で、ITに強くないユーザーでもわかりやすいと感じています。また、スキャン時のタイムラグなどもほぼ生じないので、コミュニケーターに存在を意識させることもありません。さらに、従来は添付ファイルの閲覧を禁止していたのですが、CPSF導入後は開けるようになったのでコミュニケーター側のメリットは大きいはずです」と、徳山氏は評価する。

当初の懸念事項でもあった、自社で作成しているカスタム要素やSalesforceの標準機能とのバッティングなどによる、予期せぬ動作や機能制限なども発生していないという。

徳山氏は、「日々お客様から送られてくる添付ファイルなどをチェックしている中で、その内容がリアルタイムに通知されるので、しっかり保護されているのだと安心することができています」と笑顔を見せる。

そして今後も、CPSFのように自動化できる部分はシステムに任せながら、セキュリティ対策に力を入れていく構えだ。

「いまや情報セキュリティの確保は非常に大事であり疎かにしてはいけません。これに加えてCPSFのようなソリューションは、セキュリティ面の不安を払拭することで、それ以外の面にリソースを集中することができる土台を支えるものであるとも考えています」と徳山氏は力強く語った。

> “WithSecure™ Cloud Protection for Salesforceは、WithSecure™ Security CloudとSalesforceのクラウドとの間をAPI連携することで、Salesforceのプラットフォームのパフォーマンスを低下させることなく、クラウド上で共有されているファイルとURLリンクの安全性を検証し、確保することができるソリューションです。CPSFは、Salesforce社と共同で設計・開発されているため、シームレスな統合を実現しています。”

ヤフー株式会社 CS本部
クラウドオペレーション リーダー
徳山 敦 氏

大阪府様 CPSF ご採用事例

大阪府様 CPSF ご採用事例

大阪府 様

人口880万人を超える西日本の中心的都市である大阪府。大阪府は、コロナ対策およびコロナ禍からの回復に向けて、「命を守る最大限の感染症対策の推進」「コロナ禍で打撃を受けた経済・産業の回復、雇用を支える取り組みの推進」「くらしを支えるセーフティネットの充実」を重点的に取り組んでいる。

所 在 地 | 〒540-8570　大阪市中央区大手前2丁目1
U R L | https://www.pref.osaka.lg.jp

公共システムにアップロードされる画像に潜むマルウェア対策が急務

新型コロナウイルス感染症に対して、常に先駆的に対策を重ねている大阪府。感染拡大や医療提供体制のひっ迫状況を示す指標である「大阪モデル」など独自の施策に加え、ICTを効果的に活用しながら対策に取り組んでいる。

その一例が「大阪府療養者情報システム（Osaka-Covid19-Information-System）」（以下、O-CIS）だ。新型コロナウイルス患者の療養先となる宿泊や入院調整などを行うため、保健所や宿泊療養施設をはじめとする関係者と、申請内容や患者情報などの共有を図るシステムである。

従来は表計算ソフトとメール、電話・FAXで情報を共有していたが、O-CISの導入によって、情報の一元化とリアルタイムで情報の共有ができるようになるとともに、事務処理の簡素化も実現した。O-CISの導入前は、陽性者の宿泊の手続きには最短でも2日要していたが、導入後は最短でその日のうちに手続きが完了するようになった。また、各医療機関において、リアルタイムで病床稼働状況を把握できるようになり、データの見える化にも大きく貢献している。このシステムのプラットフォームとして、大阪府が採用しているのがSalesforceだ。

一方、2022年9月12日、政府の発生届の全数把握見直し表明を受け、大阪府はO-CIS上に新たに「大阪府陽性者登録センター」を開設し、陽性者が直接登録することができるシステムを構築した。陽性者は登録の際、運転免許証などの本人確認書類と検査結果資料の画像をアップロードする必要がある。そのため、ポイントとなったのは、アップロードされる画像に起因するサイバー攻撃のリスクを軽減する機能の追加による安全性の確保だった。

大阪府
健康医療部
保健医療室感染症対策支援課
総括主査
寺岡 新司 氏

大阪府 健康医療部 保健医療室感染症対策支援課 総括主査 寺岡 新司 氏は「府民の皆様を装って、マルウェアが仕込まれた画像がアップロードされた場合、O-CISが甚大な被害を受けてしまいます。また、これまでO-CIS上での画像アップロードは、医療機関の中で限られたメンバーに対して活用されていましたが、陽性者本人に登録していただく場合は、マルウェア対策によるさらなるセキュリティ確保は必須でした。そして、なるべく早い時期から陽性者登録を行えるよう、短い期間で導入できることも優先度の高い要件として求められていました」と振り返る。

短期間でCPSFによるマルウェア対策を実装した陽性者登録システムを開設

こうした要件を踏まえ、大阪府が導入支援企業の提案を受けながら採用に至ったのが、ウィズセキュアの「WithSecure™ Cloud Protection for Salesforce」（以下、CPSF）だ。Salesforce環境にアップロードされる悪意のあるファイルやURLを使ったサイバー攻撃から、利用企業やユーザーを保護するクラウド型セキュリティソリューションである。CPSFは、Salesforce社と共同で設計・開発されており、Salesforce環境とのシームレスな統合と信頼性を確保している。SalesforceとのCloud-to-Cloudでのネイティブな統合によって、ミドルウェアを必要とせず簡単に導入できる。CPSFは、Salesforce環境のネイティブセキュリティ機能を補完するために設計されており、ユーザーが感じる遅延を最小限に抑え、Salesforce本来の使い勝手を維持できるように設計されている。

寺岡氏はCPSFの採用理由を「アップロードされた画像に起因したサイバーリスクを軽減することは重要な要件でした。それに加えて、限られた時間の中で、短期間で確実にシステムを開設することが絶対条件でした。その点、CPSFは私たちの要望に最適なソリューションでした」と話す。

O-CISの改修が完了し、大阪府陽性者登録センターでの登録を開始し、運用がスタートしたのは9月30日で、短期間での導入・稼働を実現した。CPSF自体は通常、数分間でSalesforceに導入できるため、確認も含めて1日で検収が完了したという。

また、運用の容易さも高く評価されている。陽性登録の際、府民がアップロードするすべての画像ファイルは、自動的にスキャンされてマルウェアの検知が行われる。O-CIS担当の府職員も、特別なトレーニングなどは一切不要であり、仮に有害と評価された画像は、自動的に削除またはブロックされるため、運用管理負荷は低い。

「府民も府職員もCPSFを意識せずに使えて、セキュリティを担保できる点を高く評価しています。大きなトラブルもなく運用できており、2023年1月末の時点で約48万人の陽性者登録を終えています」（寺岡氏）

今後も府民による画像アップロードの仕組みのもとで、CPSFを用いたマルウェア対策を継続していく。加えて、画像アップロードに関するさらなる機能追加をCPSFに期待しているという。

「画像にマルウェアは含まれていないものの、本人確認書類や検査結果資料とは無関係な画像がアップロードされる可能性があります。そのような画像を削除するため、現在は目視で中身を確認していますが、画像認識AIによって自動で検出・削除する仕組みがCPSFで実装されると、O-CIS以外でも活用の場面が増えそうだと考えています」（寺岡氏）

O-CIS全体についても、必要な機能追加などの改修を迅速に実施し、新型コロナウイルスから府民を守るための体制を強化していく。そしてさらに、DX（デジタルトランスフォーメーション）を推進しながらO-CISのさらなる有効活用を図っていくつもりだ。

大阪府の陽性者登録フォーム。本人確認書類や検査結果の画像がアップロードされた際、マルウェア検出にCPSFが採用されている。

※本事例は、2023年2月9日時点の情報をもとに作成しています。

CPSFケーススタディ:国内銀行ユーザ様

用 途	• 銀行の口座開設･融資申込の電子申請システム
解決したい課題	• 銀行と顧客間でやり取りされる口座開設に伴う本人確認書類や融資申込書類は、顧客の個人的な財務に関する機密情報を含むデータを扱うため、このデータを保護し、同時に悪意のあるコードからデータの安全性を保つこと
導入の結果	• １カ月にアップロードされる顧客からの口座開設時の本人確認書類や融資申込書の安全性確認を実視
導入スケジュール	• 導入検討　　～ 本番稼働 6ヶ月

CPSFケーススタディ:国内保険会社様

用 途	• 保険申込/申請のための電子申請システム
解決したい課題	• 保険会社と顧客間でやり取りされる口座開設時の本人確認書類や融資申込書類は、顧客の個人的な財務に関する機密情報を含むデータを扱うため、このデータを保護し、同時に悪意のあるコードからデータの安全性を保つこと。
導入の結果	• １カ月にアップロードされる顧客からの口座開設時の本人確認書類や融資申込書の安全性確認を実視
導入スケジュール	• 導入検討～ 本番稼働 2ヶ月