JSSスプリングフォーラム2018

「テレワークにおける情報セキュリティとその対策」
～働き方改革がもたらす新たなIT社会と情報セキュリティ～

トレンドマイクロ株式会社
セキュリティエキスパート本部
プリセールスSE部　東日本SE課
セールスエンジニア
福井 滋隆

トレンドマイクロ株式会社 会社概要

What We Do

- IT環境のセキュリティにおけるリーダーカンパニー
- 革新的なセキュリティソリューションを提供
- ビジネス利用・個人利用双方のお客様を保護

How We Do It

世界の脅威解析の知能を集結

- 世界13ヶ所にある脅威解析センターに約1,200名のスタッフと約1,500名のR&Dエンジニアが在籍。
- TREND MICRO SMART PROTECTION NETWORK
  世界中の脅威情報を収集、分析・特定し、お客様へリアルタイムでソリューションを提供するクラウド型のセキュリティインフラ。

Who We Are

エバ・チェン
代表取締役社長
兼 CEO

大三川 彰彦
取締役副社長

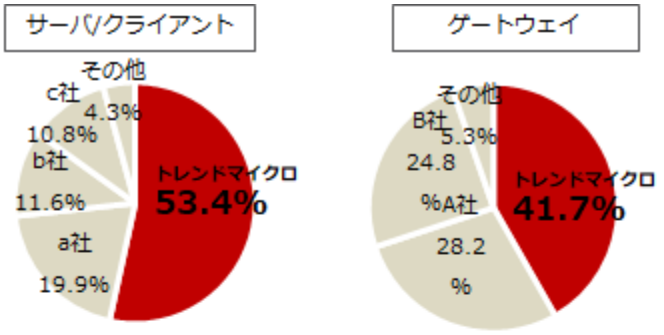
創業:	1988年
本社:	東京
従業員数（全世界）※:	5,627名
資本金※:	183億8,600万円
売上高※:	1,319億3,600万円

※2016年12月31日付

各市場における当社のマーケットシェア

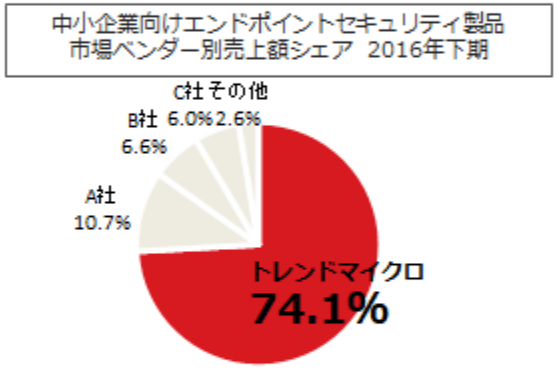
企業向け製品国内市場
13年連続シェア No.1※1

トレンドマイクロ製品は、(株)富士キメラ総研の調査で企業のサーバ/クライアント向けウイルス対策ツール、ゲートウェイにおけるウイルス対策ツールで13年連続※最も高いシェアを占めています。
※1 出典：（株）富士キメラ総研「ネットワークセキュリティビジネス調査総覧」2003～2015年度金額ベース
（グラフは2015年度金額ベース）



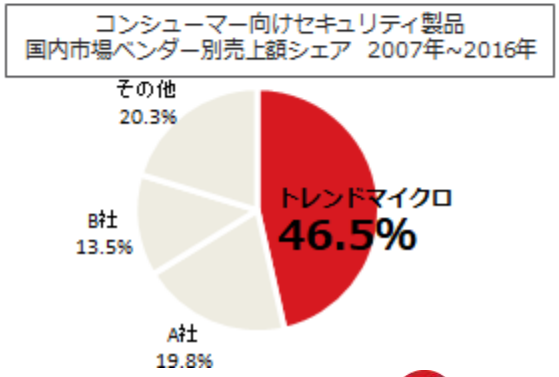
中小企業向けエンドポイントセキュリティ製品国内市場
8年連続シェア No.1※2

トレンドマイクロ製品は、IDC Japanの調査で中小企業のエンドポイントセキュリティ製品で最も高いシェアを占めています。
※2 出典： IDC Japan, Japan Semiannual Security Software Tracker 2016 H2
エンドポイントセキュリティー2009-2016年下期No.1 中小企業向け(従業員数1-99名)



コンシューマ向け製品国内市場
10年連続シェア No.1※3

ウイルスバスターなどのコンシューマ向け製品においてトレンドマイクロはお客様に長年信頼され続けている国内No.1のセキュリティベンダーです。
※3 出典： IDC Japan, Japan Semiannual Security Software Tracker 2016 H2
コンシューマ向けセキュリティー製品 ソフトウェア市場ベンダー別売上額シェア
(シェア算出全期間)



サイバー犯罪撲滅に向けた技術提供・捜査協力

インターポールを通じて加盟各国の重要機関に
セキュリティ技術のスキル向上トレーニングを提供

トレンドマイクロCEOのエバ・チェンと、インターポール（International Criminal Police Organization:ICPO、国際刑事警察機構）事務総長が会談し、サイバー犯罪対策に関するインターポールへの協力関係を築くことで合意

ネットバンキング被害の拡大防止に役立つ情報を提供し感謝状を授与

警視庁から感謝状を授与。ネットバンキングの不正送金事案に関し、被害の拡大防止に役立つ効果的な情報を提供し評価される　（2014年4月発表）

FBI 「ネットバンク利用者攻撃ツール作者が罪を認める－トレンドマイクロがFBIに捜査協力」

米連邦捜査局（FBI）に長期間に渡り捜査協力した他、犯人特定に役立つ情報を提供
（2014年1月発表）

テレワークにおける情報セキュリティ

働き方改革とICT利活用

- 労働生産性の向上・災害時の事業継続性の確保、社員・職員のワークライフバランスの確保のため、**働き方改革**の検討される法人が増加しています。
- その**働き方改革**にICTを利活用した「テレワーク」の実施が増えている状況にあります。
- インターネット接続を介したテレワークは、**情報セキュリティの課題**が存在します。
- “**利用環境**”と“**利用時**”の課題と対策案を説明します。

雇用型テレワークと自営型テレワーク

- 雇用型…企業に勤務する被雇用者が行うテレワーク

在宅勤務

モバイルワーク

施設利用型勤務

本資料では雇用型における課題と対策を説明します

- 自営型…個人事業者・小規模事業者等が行うテレワーク

SOHO・内職副業型勤務

【出典】総務省：テレワークの主な形態
http://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/18028_01.html

利用環境の課題

利用環境における課題

- 個人所有端末の**セキュリティレベルの不整合**
  - ✓ 対策ソフトやパスワードポリシーなどが**統制できない**。

- 個人所有端末のアプリなどから**情報漏えい**
  - ✓ 家族共用だと**P2Pなどからマルウェアが侵入**する

- 「情報持ちだし」した**端末の紛失**リスク
  - ✓ 紛失により**PCに保存した機密情報が漏えい**する。

- **公衆無線LANサービス**利用時に**盗聴や悪用**されるリスク
  - ✓ **スライド10で詳細を説明**

- **偽**のアクセスポイント（なりすましによる情報漏えい）
  - ✓ **スライド11で詳細を説明**

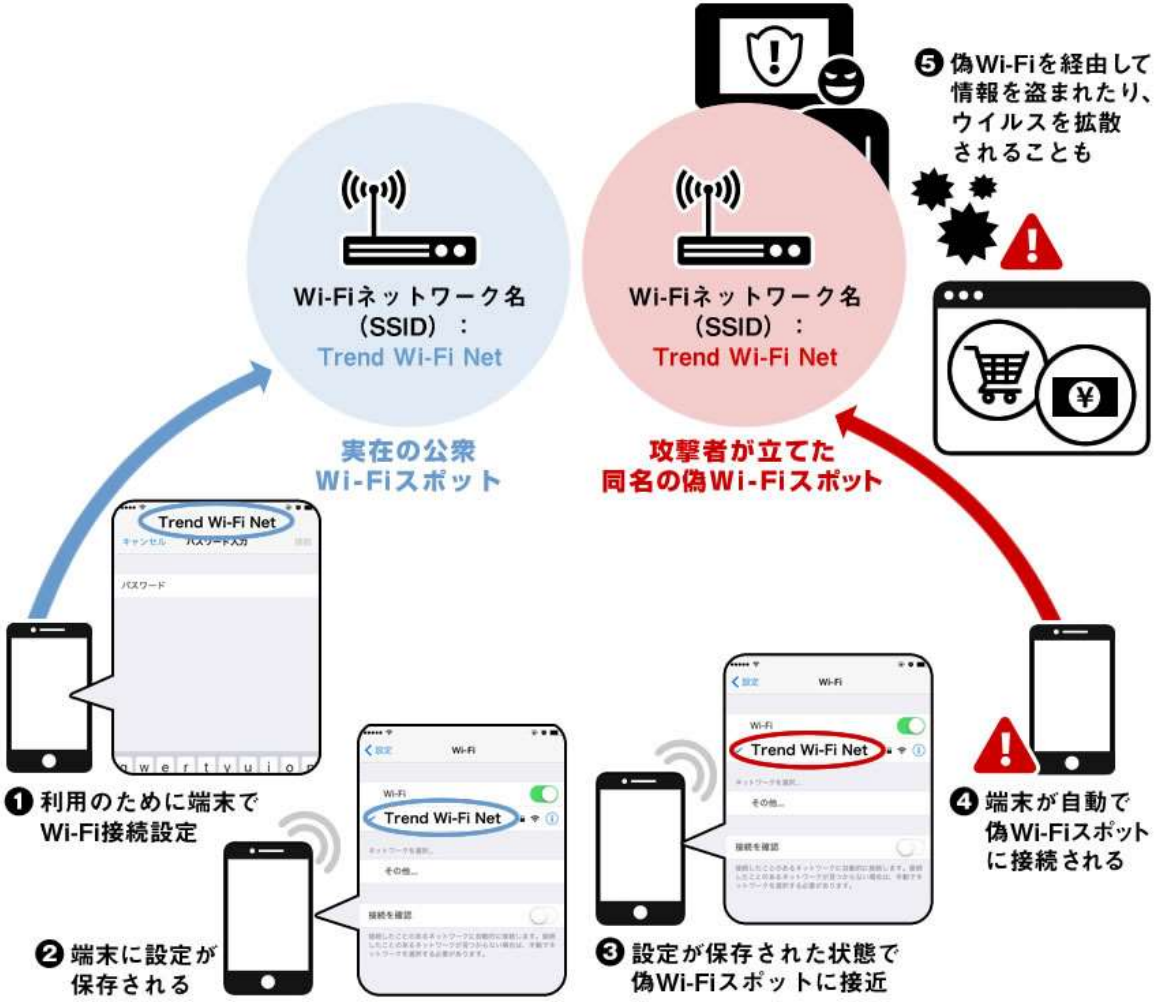
公衆無線LANサービスの課題

- 暗号化方式 WEPの問題
  - **WEPの暗号化通信を解読するツール**が出回っており、認証用ID/パスワードが判明し通信が盗聴される。
- 非暗号化通信の問題
  - 公衆無線LANサービスは**非暗号化通信の運用**が、かなり多く存在し通信が盗聴される。
- 無線LANを悪用した中間者 (MiTM) 攻撃：CoffeeMinor

上記の課題がある公衆無線LANを使用することにより、情報漏えいや攻撃者からの脅威に遭遇する可能性があります。

※ **WPAやWPA2の暗号化方式**であっても、施設で**パスコードを公開**している場合、サイバー犯罪者が悪用し**盗聴/悪用されるリスク**はあります。

偽のアクセスポイントとは



【出典】is702：偽Wi-Fiスポットの攻撃手口
https://www.is702.jp/special/2123/partner/12_t/

利用環境における課題への対策例

- **社員・職員に定期的なテレワーク利用の教育**
  - どのようなリスクが存在することの周知、かつモラル向上によって事故発生の頻度を低減する。
  - セキュリティ啓蒙を目的としたis702のWebサイトを通じて、社員・職員向けの教育への活用。
- **公衆無線LAN利用禁止のルール化（利用制限の明示）**
- **端末紛失を想定したHDD暗号化ソフトの導入**
- **モバイルルータ貸与**
  - 社員・職員が通信コスト負担を抑えようとする行動の結果、公衆無線LANを利用する。
  - モバイルルータ貸与やスマートフォンのテザリング利用許可など、社員・職員が負担しない通信手段を用意し、盗聴や悪用の機会を回避する。

利用時の課題

利用時の課題

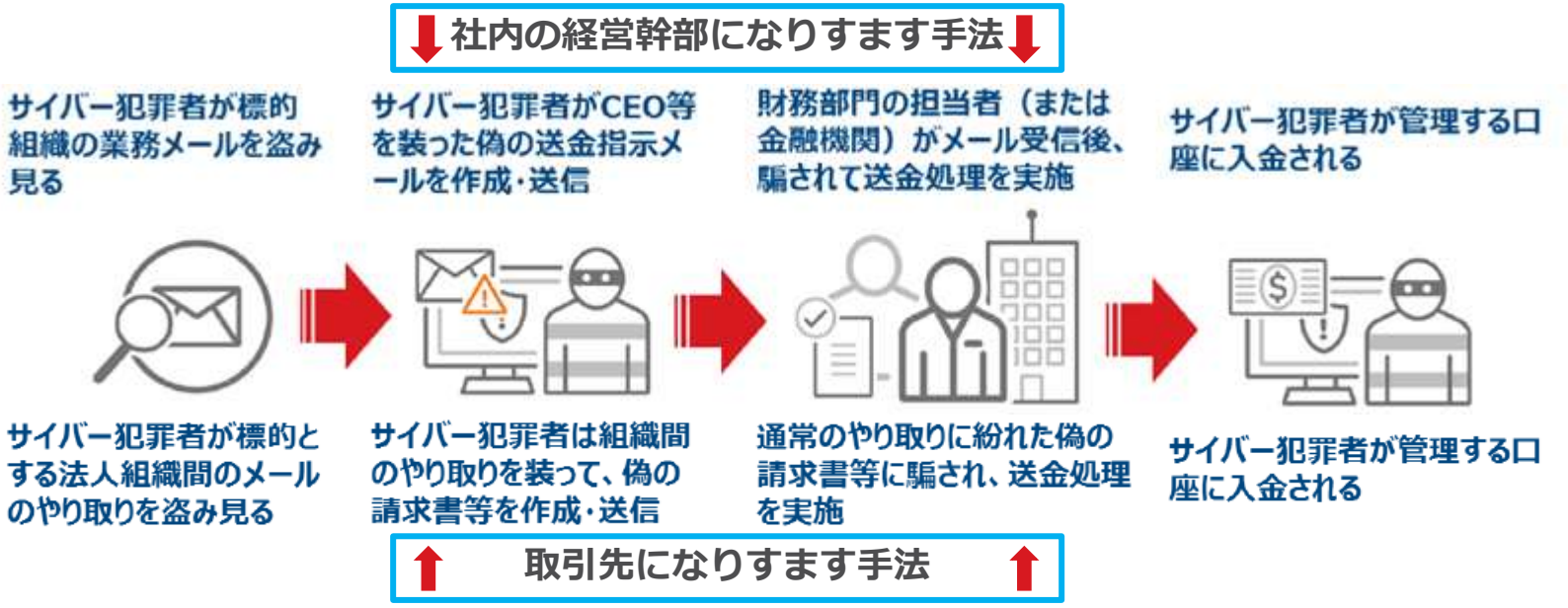
- **ビジネスメール詐欺（ BEC ）：メール利用の課題**
  - **サイバー犯罪者がメールを盗み見**から、**経営幹部や取引先に偽装したメール**で振り込み指示をする詐欺行為

- **仮想通貨発掘のコインマイナー急増：Web利用の課題**
  - サイバー犯罪者に**誘導されたWebサイト閲覧**によって、使用者の端末の**CPUリソースを過大消費**

- **外部から社内システム侵入：社内リソース利用の課題**
  - 端末感染した**ワーム型未知の不正プログラム**が**VPN**を**経由**して**脅威が組織のシステム内に侵入・拡散**
  - **公衆無線LAN**サービス経由で**端末感染**し、当該端末をLAN接続したため**脅威が組織のシステム内に侵入・拡散**

メール利用の課題

- ビジネスメール詐欺（ BEC ）
  - 企業や法人における**業務メールの盗み見を発端**に、経営幹部や取引先を偽装する**“なりすましメール”**により、偽の送金指示を送る詐欺手口



【出典】トレンドマイクロ セキュリティブログ
http://blog.trendmicro.co.jp/archives/16774

取引先を装った”ビジネスメール詐欺”被害事例

様々な組織が巧妙な詐欺手口の被害に遭遇しています。

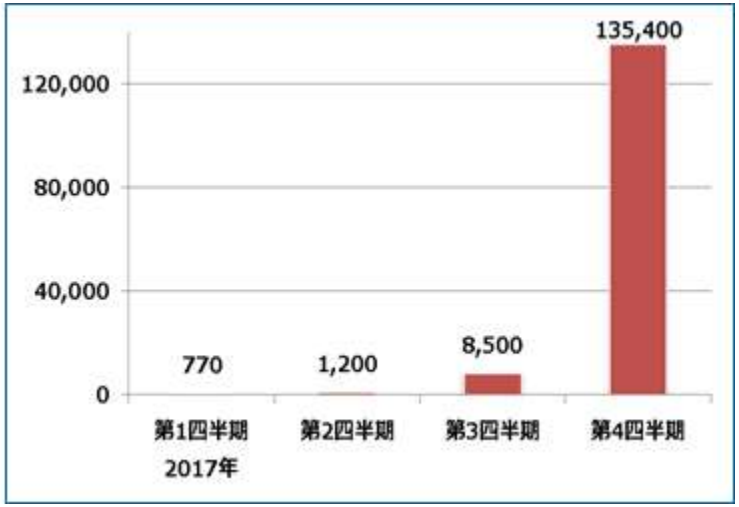
公表時期	関連組織	概要
2017年2月	国内貿易会社 海外農業用肥料販売会社	国内貿易会社が受け取るはずの取引代金580万円が国内別会社に送金、引き出したナイジェリア人を国内で逮捕
2017年3月	フランスの建築会社 米国の船舶修理会社	取引のやり取りで送金先が日本の口座に変更された4,000万円を引き出した日本人を逮捕
2017年3月	国内販売会社 海外取引先	農機具発注のやり取りで海外取引先を装った偽の送金先変更依頼に騙され、500万円の損失
2017年12月	国内航空会社 海外取引先	海外取引先を装った犯人に定期的な支払先の変更を依頼され、約3億8,000万円を騙し取られる
2017年12月	国内航空会社 海外取引先	海外取引先を装った犯人から偽の送金先変更依頼を受けたが、送金先口座が凍結されていたため被害を免れる

■国内で確認された主なビジネスメール詐欺関連事例（公表事例を元に独自に整理）

Web利用の課題

- 仮想通貨価値が上昇し、利用者が意図しない**仮想通貨の発掘を行う「コインマイナー」**の検出が増加
- マイニングサービス**「Coinhive」**が2017年9月に登場、サイバー犯罪者はその仕組みを利用して、Webページに誘導して不正なマイニングを行わせる事案が急増

「COINMINER」と「WannaCry」の検出台数推移
（2017年、全世界）



「COINMINER」検出台数推移
（2017年、国内）

【出典】2017年年間セキュリティラウンドアップ
https://resources.trendmicro.com/jp-docdownload-form-m051-web-asr.html

利用時の課題への対策例（システム対策）

- **クラウドサービスと連携するセキュリティサービスを導入**
  - メール本文のURL評価や添付ファイルを動的解析を行い、**サイバー攻撃メールが利用者に到達する頻度を低減**
    - ✓**当社ソリューション：Hosted Email Security / Cloud App Security**
- **外部環境でも、端末上の脅威の検知ログを自動収集**
  - **テレワーク利用端末**が脅威を検知したことを**早期に管理者が把握**、適切な対処を迅速に実施して被害拡大を抑止
    - ✓**当社ソリューション：ウイルスバスター コーポレートエディション XG**
- **内部間通信の可視化**
  - 局所的な段階で**未知ファイルの通信のふるまい**から気づく
  - SBC方式のサーバ保護、サーバシステムの脆弱性を保護する仮想パッチ、攻撃利用されうる通信から**サーバを要塞化**
    - ✓**当社ソリューション：Deep Discovery Inspector / Deep Security**

情報セキュリティとその対策の“まとめ”

- テレワーク実施の際は、利用環境や利用時における**情報セキュリティの課題と対策案**の検討は不可欠です。
- サイバー犯罪者同士で積極的に学びを共有しており、**攻撃手法は更に洗練**され**人を弱みを狙う巧妙な攻撃**は、事故事例から見ても効果的なため継続します。
- 社員・職員への教育は欠かすことは出来ませんが、**人の弱みを補助をするシステムと組合せの防御**が有効な手段といえます。
- 特にサイバー攻撃は**システムに侵入されることを前提**に考え**有効性のある内部対策を実施**し、サイバー攻撃を**局所規模で気付くシステム**と**是正する運用体制**が必要です。

当社ソリューション

世界各地を守るエキスパートたち

脅威解析・サポートセンター　**TrendLabs（トレンドラボ）**

・本部：　フィリピン、アメリカ
・厳選された約１２００名のエキスパートが在籍
・２４時間３６５日体制で脅威を監視（アジアの夜時間にはアメリカから）
・脅威情報の収集、解析、ソリューションの提供

各地域特有の脅威にも対抗　**リージョナルトレンドラボ**

・拠点：日本、フィリピン、アメリカ、台湾、ドイツ、アイルランド、中国、フランス、ブラジル、シンガポール
・新宿オフィスのラボでは日本特有の不正プログラムの収集・解析を行い
日本のお客様へ迅速なソリューション提供を実施
・脅威情報の発信、セキュリティ啓発、ボット対策事業など

未来の脅威予測・研究

Forward-Looking Threat Research

・研究成果を２～３年後の製品開発に活かす
・リージョナルトレンドラボとも連携し、地域特有の脅威についても
研究、解析を実施。法的機関とも適宜連携。

世界に13拠点のリージョナルトレンドラボ

地域に特化した脅威におけるサンプル収集や動向調査を行い、各地域のお客さまに
迅速かつ柔軟なソリューション提供を行っています。

■ 本社：日本

■ TrendLabs（トレンドラボ）リージョナルトレンドラボ：
フィリピン（本部）、米国、日本、台湾、ドイツ、アイルランド、中国
フランス、ブラジル、シンガポール

■ 開発拠点：
日本、米国、カナダ、ドイツ、アイルランド、フランス、英国、台湾、中国、インド、オーストラリア、
ブラジル

■ 海外子会社：
米国、カナダ、アイルランド、フランス、ドイツ、イタリア、英国、スイス、オーストラリア、
中国（上海）、中国（香港）、中国（北京）、インド、韓国、マレーシア、シンガポール、台湾、タイ、
ブラジル、メキシコ、パナマ

■ 海外主要エリア：
ニュージーランド、オーストリア、ベルギー、オランダ、デンマーク、UAE（ドバイ）、ノルウェー、
ポーランド、スペイン、スウェーデン、トルコ、ロシア、インドネシア、ベトナム、フィリピン、
エジプト、サウジアラビア、南アフリカ

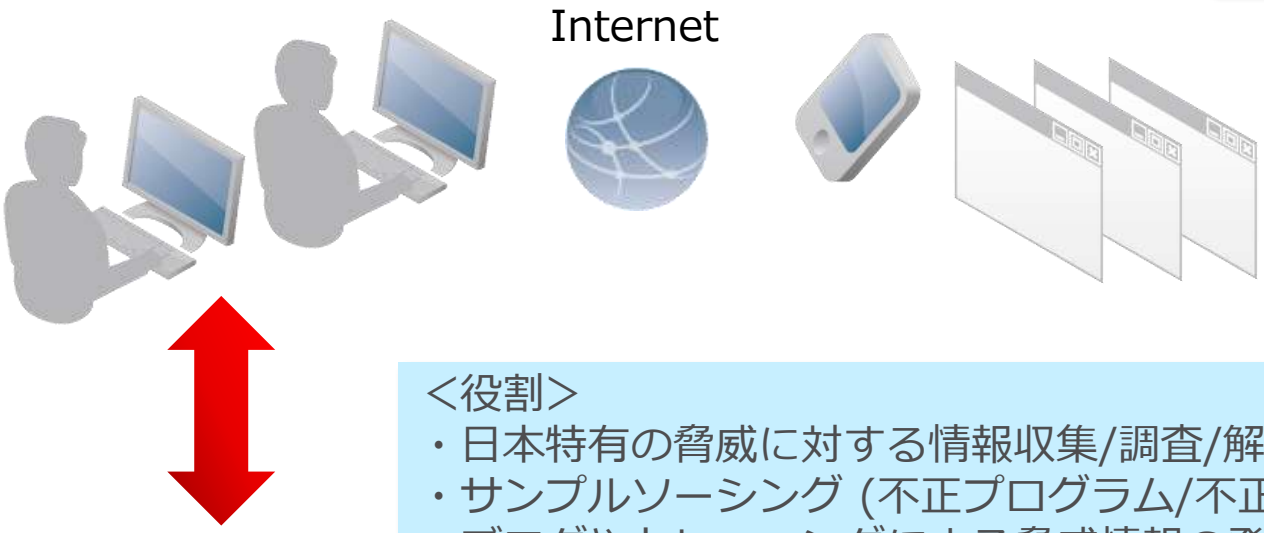
リージョナルトレンドラボ

セキュリティインテリジェンスセンターとして、
より迅速でプロアクティブなソリューション提供を実現する。

日本に特化した
脅威情報の収集

潜在する脅威・
危険性の可視化

被害拡大の予兆の
察知・警告



リージョナル
トレンドラボ

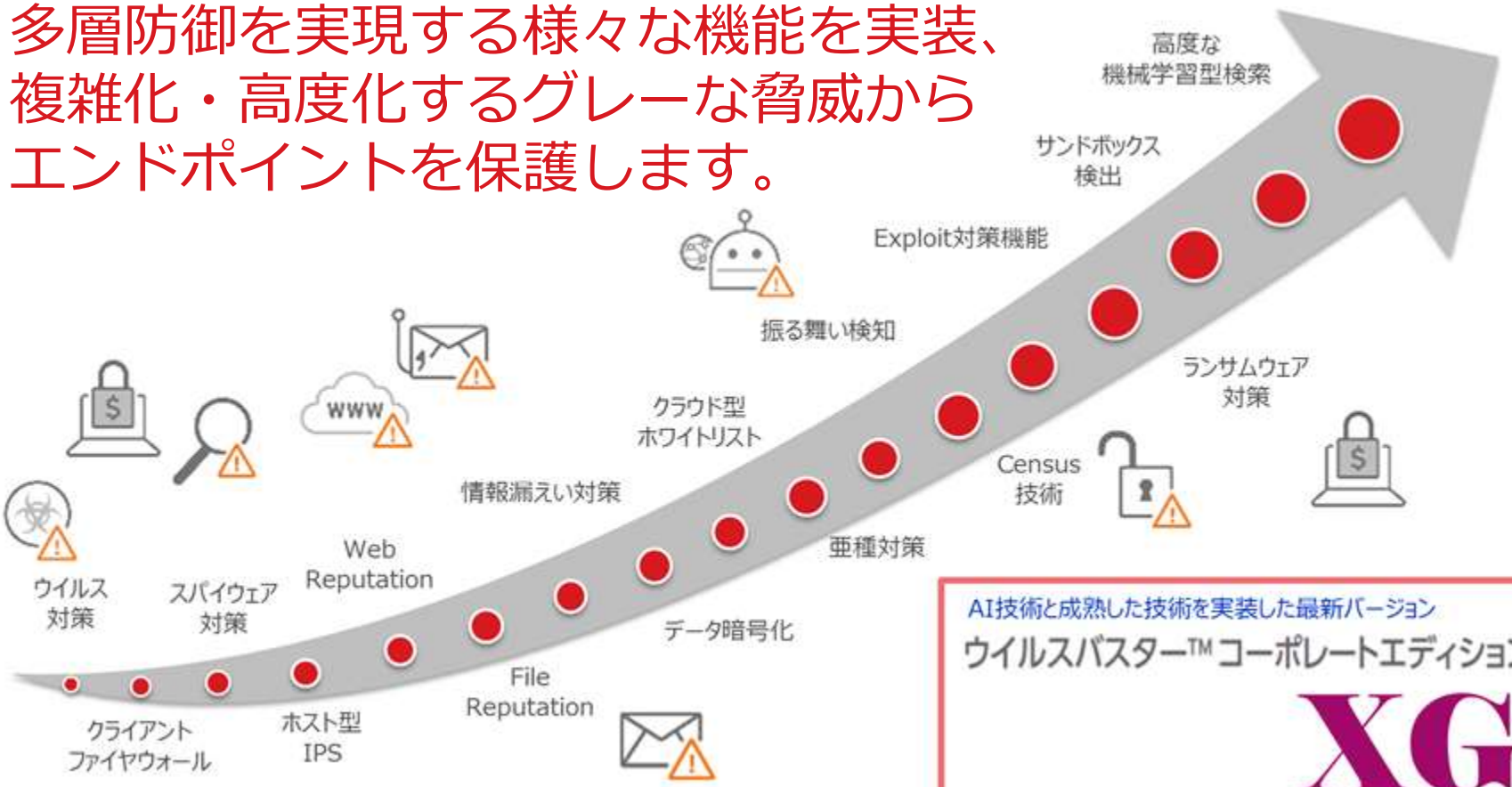
＜役割＞
・日本特有の脅威に対する情報収集/調査/解析/ソリューション提供
・サンプルソーシング (不正プログラム/不正URL/スパムメール)
・ブログやトレーニングによる脅威情報の発信とセキュリティ啓発
・日本のお客さまからのお問い合わせ対応
・政府関連機関との協業
・メディアからのお問い合わせ対応

クライアント端末を多層防御で脅威から保護する

ウイルスバスター コーポレートエディション

ウイルスバスター コーポレートエディション

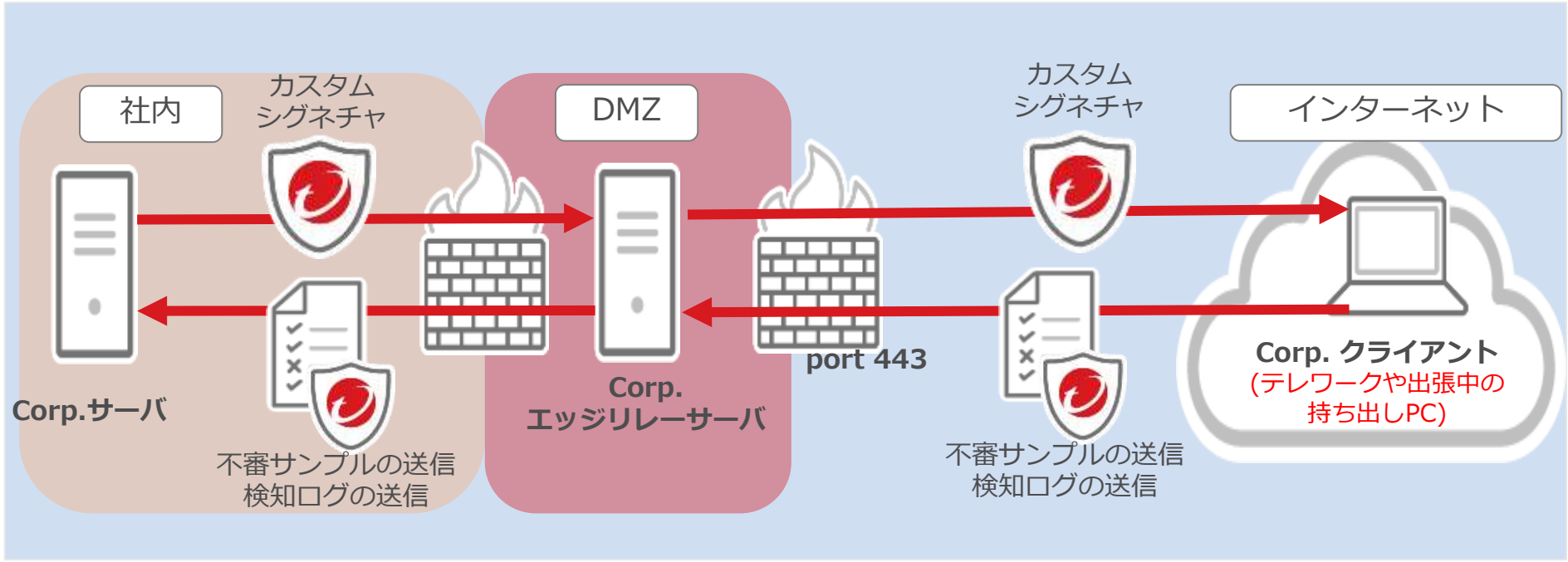
ウイルスバスター コーポレートエディションは、
多層防御を実現する様々な機能を実装、
複雑化・高度化するグレーな脅威から
エンドポイントを保護します。



ウイルスバスター コーポレートエディション XG：
テレワーク中の端末の脅威検知を自動収集

エッジリレーサーバを利用すると、Corpサーバと直接接続できないテレワークで利用している場合であっても、インターネット接続すると検索機能で脅威を検出したログを自動的に受信することが可能です。エッジリレーサーバはDMZ上に配置し、インターネットから接続できる必要があります。

後述のDDIが未知の高リスクファイルを検知した場合、製品間連携機能で端末で同ファイルを検知するカスタムシグネチャを配布可能にします。



クラウドメールサービスのメールを多層防御を実現する

Trend Micro Hosted Email Security

Trend Micro Hosted Email Security 概要

Trend Micro Hosted Email Security(以下、HES)はSaaS型メールセキュリティサービスです。

• 導入メリット

クラウド型サービスで初期投資費用削減

お客さま側で管理サーバを構築する必要がなく、導入時の初期投資や構築に関わる時間を抑えることができます(※)。
※お客さまには、DNSサーバのMXレコードを変更していただく必要がございます。

最新鋭のクラウドサンドボックス

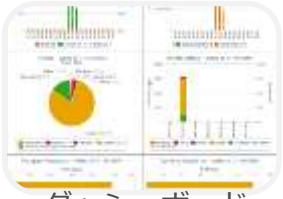
お客さまのメールボックスがオンプレミスの場合やクラウドサービスを利用されている場合(Microsoft Office 365やGoogle Apps)でも、最新鋭のクラウドサンドボックスや検索技術を使った対策が可能です。

ランサムウェア対策機能搭載

ランサムウェアや標的型メールを検知しブロックする対策機能を備えたクラウド型セキュリティサービスです。

ウイルス対策　スパイウェア対策　コンテンツフィルタ　スパム対策　フィッシング対策

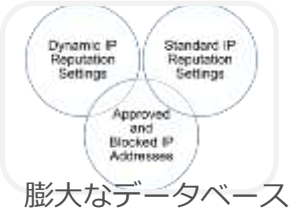
• 機能一覧



ダッシュボード

柔軟なポリシー設定

グループごとのフィルター設定



膨大なデータベースによる脅威検出

メールの隔離機能

メールの追跡機能

わかりやすい管理機能

HESが提供するセキュリティ機能

ウイルス対策
スパイウェア対策

- 不正プログラムなどのセキュリティリスクを含むメールの検知/処理を行います。
- 検知にはSPN、高度な脅威検索、クラウドサンドボックス、機械学習を使った検索などの最新技術が使われます。

スパムメール対策
フィッシング対策

- ビジネス詐欺メール(BEC)、スパムメール、フィッシングメール、グレーメール、ソーシャルエンジニアリング攻撃などに対し、検知/処理を行います。

コンテンツフィルタ

- キーワード、用語集、添付ファイルの特性、およびその他のフィルタルールに基づいて、メールメッセージと添付ファイルをフィルタできます。

Web管理コンソールにて設定が可能

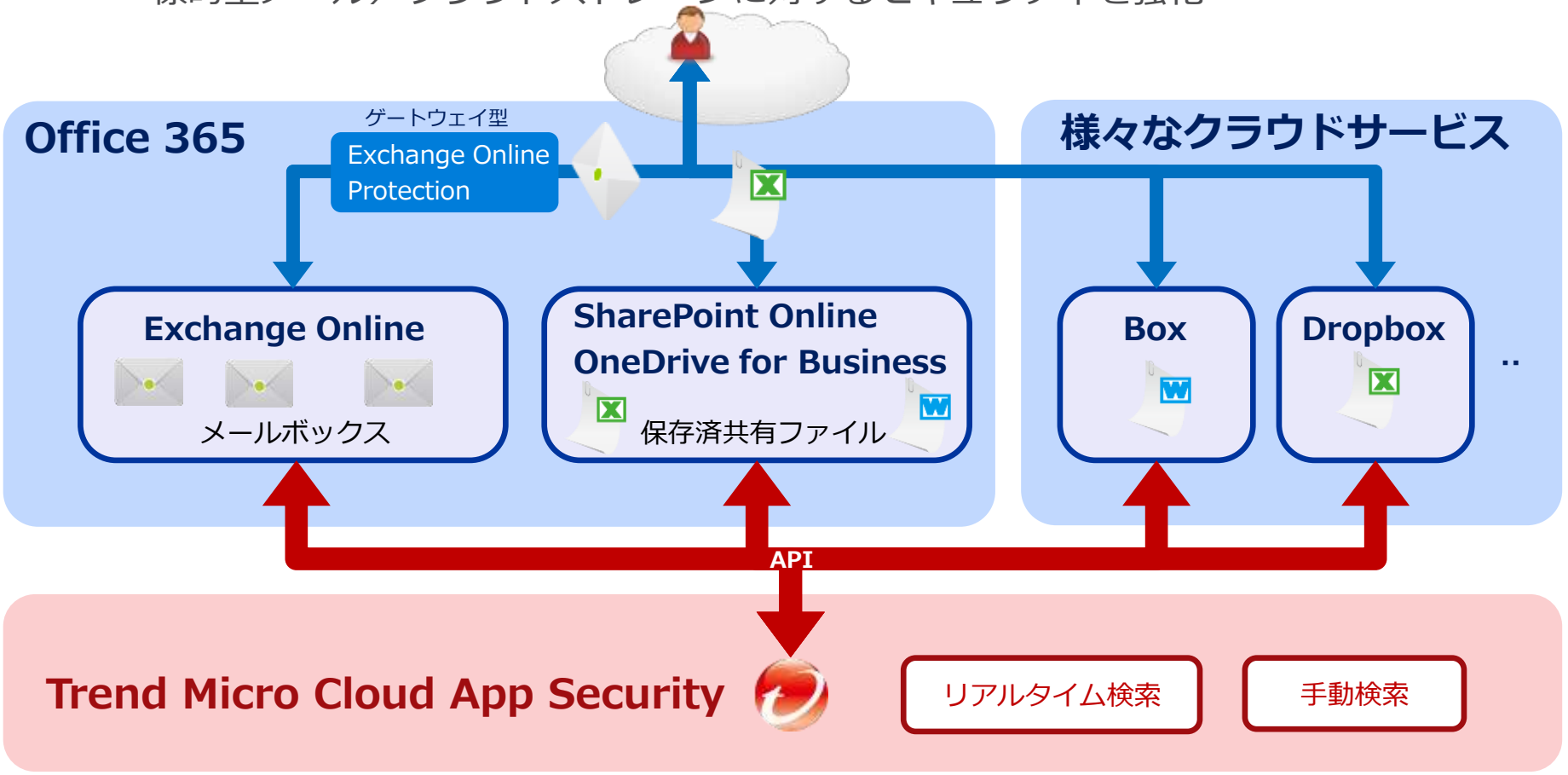
Office 365やDropboxなどのセキュリティを高める

Trend Micro Cloud App Security

Office 365のメール/ファイルをリアルタイム検索：

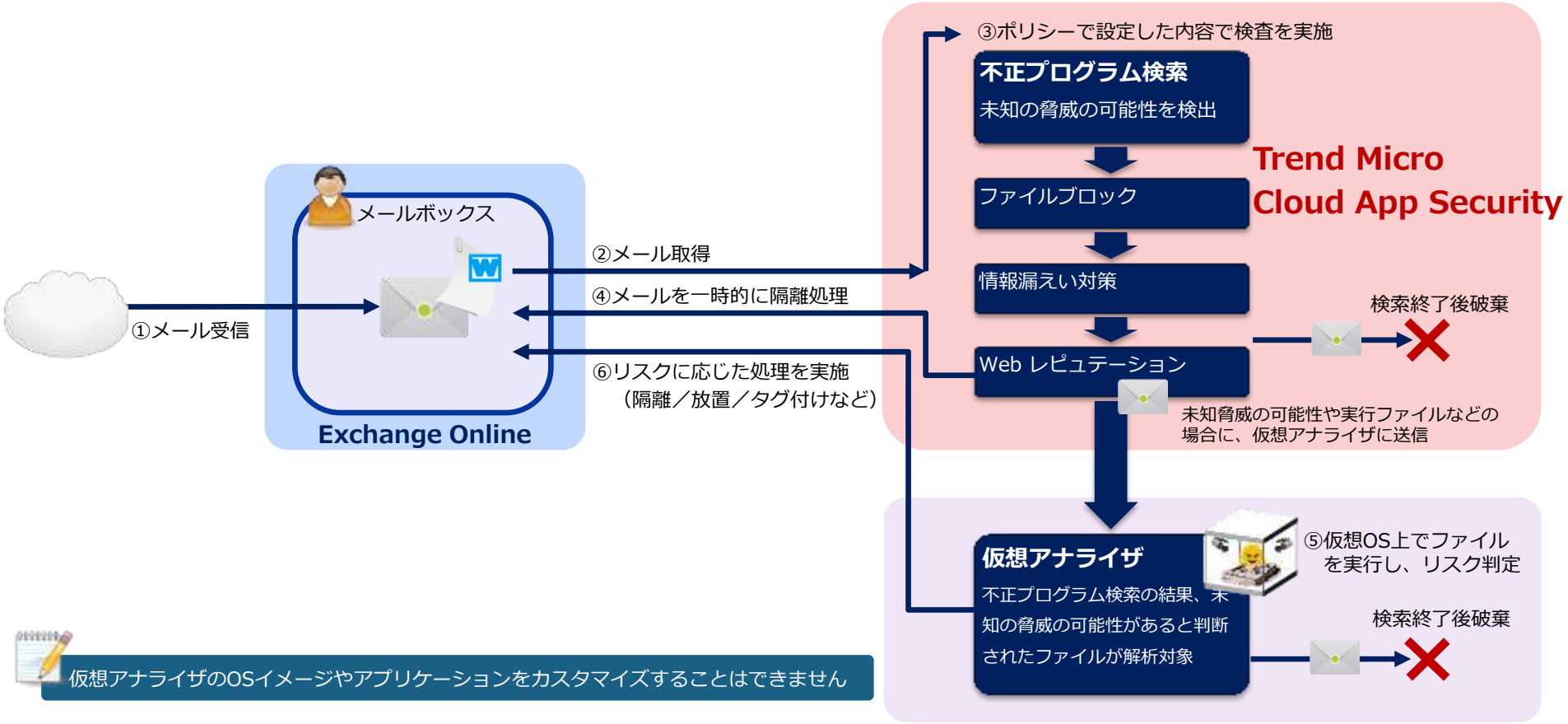
Trend Micro Cloud App Security 概要

- Office 365／Box／Dropboxとクラウド上で接続するクラウドサービス
  - Office 365はExchange Online/SharePoint Online/OneDrive for Businessが対象
- 標的型メール／クラウドストレージに対するセキュリティを強化



CAS 製品概要

CASはAPIを利用することで、メールサービス（Exchange Online）や、クラウドアプリケーション（OneDrive for Business／SharePoint Online／Box／Dropbox）上のファイルをポリシーで設定した内容で検索し、処理を行うことができます。



※1　全ての未知の脅威に対応するものではありません
※2　全てのアプリケーションの動作を保証するものではありません

未知のサイバー攻撃に気づく内部対策を実現する

Deep Discovery Inspector

未知脅威の通信を監視する内部対策製品：

Deep Discovery Inspector 概要

■未知の脅威に気付く、標的型サイバー攻撃対策製品■

お客様環境に合わせたラインアップ

- Deep Discovery Inspector 4100
- Deep Discovery Inspector 1100
- Deep Discovery Inspector 250

隠れた脅威のありかを、相関分析を駆使して可視化！

- **日本の環境に対応**したカスタムサンドボックスによる動的解析
- ルールやパターンを用いて**通信やファイルの振る舞い**から脅威を解析
- URL/IPの情報から**不正Webサイト(C&Cサーバ)**への接続を検知
- 約**100種**の多様なプロトコルをモニタリング
- **正規の通信にまぎれた**不正に関わる通信を検出

Deep Discovery Inspectorの検知ロジック

パケットモニタリング　スイッチのミラーポートからパケットをモニタリング

静的解析

セッション情報解析

ヘッダ等の情報の取得

パケット内からヘッダ等の情報を取得

挙動分析

①ネットワーク上の不審なふるまい
④要注意アプリケーションの検出

ネットワーク経由の脆弱性コード

ネットワークレベルでOSの脆弱性を狙った攻撃を検出

URL判定

③不正Webサイト（C&Cサーバ）への接続検知

ファイル解析

ファイルの構築

パケット内からファイル構造のみを取得

パターンマッチング

既知の不正ファイルを検出

脆弱性コードの確認

②ドキュメントファイルの脆弱性を検出

動的解析

Sandboxを用いた動的解析

⑤動的解析の実施

伊勢志摩サミットのサイバーテロ対策に協力

～三重県警察、愛知県警察より感謝状を授与～

トレンドマイクロは、2016年5月26、27日に三重県で開催された伊勢志摩サミットのサイバーテロ対策に協力、期間中サイバーテロによる被害はありませんでした。本協力により、三重県警察、愛知県警察より感謝状を授与されました。

◆サイバーテロの監視

- 伊勢志摩サミットの関連拠点にネットワーク型脅威対策製品「**Deep Discovery Inspector**」を設置し、サイバーテロの兆候を24時間体制で監視。警察組織内に当社のサイバークライムアナリストが常駐しサイバーテロの調査活動を支援

◆サイバーテロ対策の演習

- 警察組織内に設置されたサイバーテロ対策を担う部門に対し、サイバー攻撃の演習を実施

◆重要インフラ事業者に対するセキュリティ啓発活動

- 「サイバーテロ対策協議会」で鉄道、電力、水道などの重要インフラ事業者のシステム管理者向けに、最新のサイバーセキュリティに関する講演を実施
- 一部事業者に対し、警察組織とともに現地に訪問し、セキュリティ対策の助言や啓発活動を実施

Deep Discovery InspectorとウイルスバスターコーポレートエディションのConnected Threat Defense概要

Connected Threat Defense概要

※ 設定により複数のアクションを選択することが可能

エンタープライズ製品であるDeep Discoveryファミリー製品から

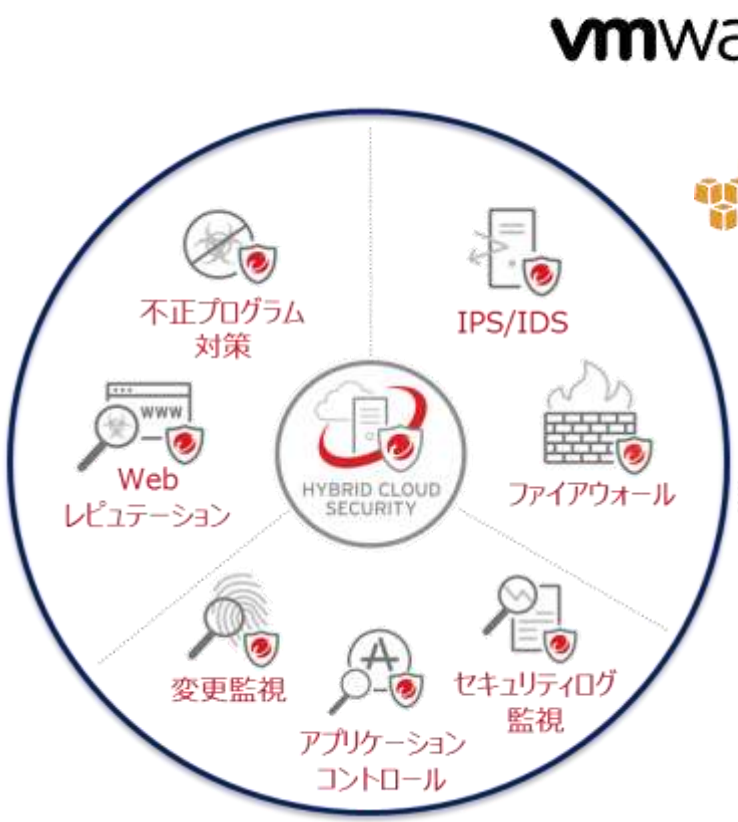
未知の不審ファイルの解析情報を取得し、

従来のエンドポイント・サーバ製品で検出・防御できるソリューション

Trend Micro Deep Security 概要

- Trend Micro Deep Securityは、サーバセキュリティに必要な複数の機能を１つの保護モジュールに実装した総合サーバセキュリティ対策製品です。

- サーバ管理者、セキュリティ担当者が抱えているセキュリティ課題を物理・仮想・クラウド環境にまたがって、トータルに解決します。



Trend Micro Deep Security 対応環境

- 「多層防御」を実現するセキュリティ機能を「All in One」で提供
- 「ホスト型」のセキュリティ対策でIT環境に依存しない柔軟な対策が可能
- 管理コンソールにより、複数のサーバ、セキュリティイベントを「集中管理」

物理環境

エージェント型ソフトによるサーバー単位の保護

- 基本的な構成
- OS・機能ともにもっとも制限なく広範囲でカバー

クラウド環境

エージェント型又は**Virtual Appliance型**による保護

- Amazon Web Serviceと連携
- Microsoft Azureとの連携
- IBM SoftLayer との連携
- vCloud Director、vCloud Airと連携
- クラウドホストのDSaaSも登場

仮想環境

Virtual Appliance型によるESXi単位での保護

- VDIで特に効果的なエージェントレスタイプ
- vSphere環境と連携

※OS・機能など環境には一定の制限があります。

ご清聴ありがとうございます。