LANSCOPE CPMS Cyber Protection Managed Service

金融業界の現状と不可避なセキュリティ対策

目次

金融業界の動向

■デジタライゼーションの加速的な進展を踏まえた対応

・クラウドサービス、RPAなどの活用が進んでいる。
　それに伴いセキュリティ対策もより強固な物が必要に

■2020年東京大会等への対応

・本大会実施にあたり全世界のサイバー攻撃の標的になることが予測される
　強固なセキュリティ対策とともにインシデント発生時の連携態勢を構築する必要がある

■金融機関のサイバーセキュリティ管理態勢の強化

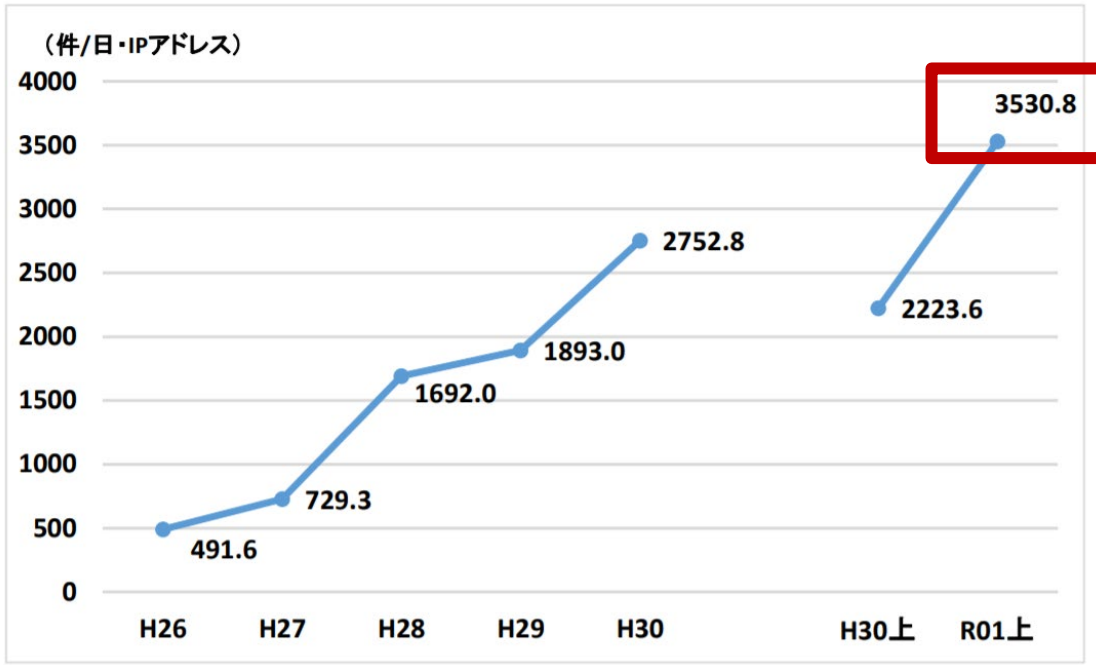
・平時のサイバー対策と有事のサイバー対策
　金融機関の規模などにより状況が異なる
　⇒金融庁は地域金融機関に対し、業務で使用するシステムや従業員のパソコンなどに
　　潜む脆弱性を診断するように促している。

出典：金融庁　「金融分野のサイバーセキュリティレポート」（2019年6月）

2020年東京オリンピック・パラリンピックへ向けた脅威の高まり

2020年の東京オリンピック・パラリンピックに向けて、大会運営の妨害および大会関係者へのサイバー攻撃や電力会社や交通機関などの重要社会インフラへのサイバー攻撃が想定され、サイバーセキュリティ対策の強化が国を挙げて推進されています。
しかし対策が必要なのは、東京2020に直接かかわる企業・組織や重要社会インフラにかかわる企業だけではありません。2020年、日本にやってくる脅威の数は間違いなく過去最大になると予測されており、すでに国内で観測された脅威の件数は過去最大となっています。
警察庁が2019年9月26日に発表した「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について」によると、2019年1月から６月末までの半年間に日本国内で確認された不審なアクセスは、１日当たり平均3530件となっており、前年と比較して約1.5倍に増えています。これは、2014年以降で最も多い件数となっており、外部脅威対策の強化が必要です。

【図表１　センサーにおいて検知したアクセス件数の推移】



2019年1月から６月末までの半年間で
すでに過去最多のサイバー攻撃を観測

出典：警察庁　「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2019年9月26日）

国家規模イベントの歴史はサイバー攻撃と共に

2012年

ロンドン大会

Dos攻撃／DDos攻撃／
スパムメール／ウイルス感染

- ✓ 2週間の開催期間に**2億1,200万回のサイバー攻撃**
- ✓ **6件の重大なインシデントが発生**

2014年

ソチ大会

Dos攻撃／ゼロデイ攻撃
ハッキング

- ✓ **１日当たり最大50件**の深刻なコンピュータセキュリティインシデントの発生

2016年

リオ大会

Dos攻撃／フィッシング
Web改ざん／マルウェア

- ✓ 大会関連組織にフィッシングから不正アクセス
- ✓ **ドメインフロンティングなど手法が巧妙化**

2018年

平昌大会

Dos攻撃／マルウェア
標的型攻撃

- ✓ 2月9日開会式直前にシステム障害によるトラブル発生。Olympic Destroyerにより運営に障害

■金融業界横断的なサイバーセキュリティ演習（Delta Wall）

・平成28年10月～令和元年10月まで計4回実施

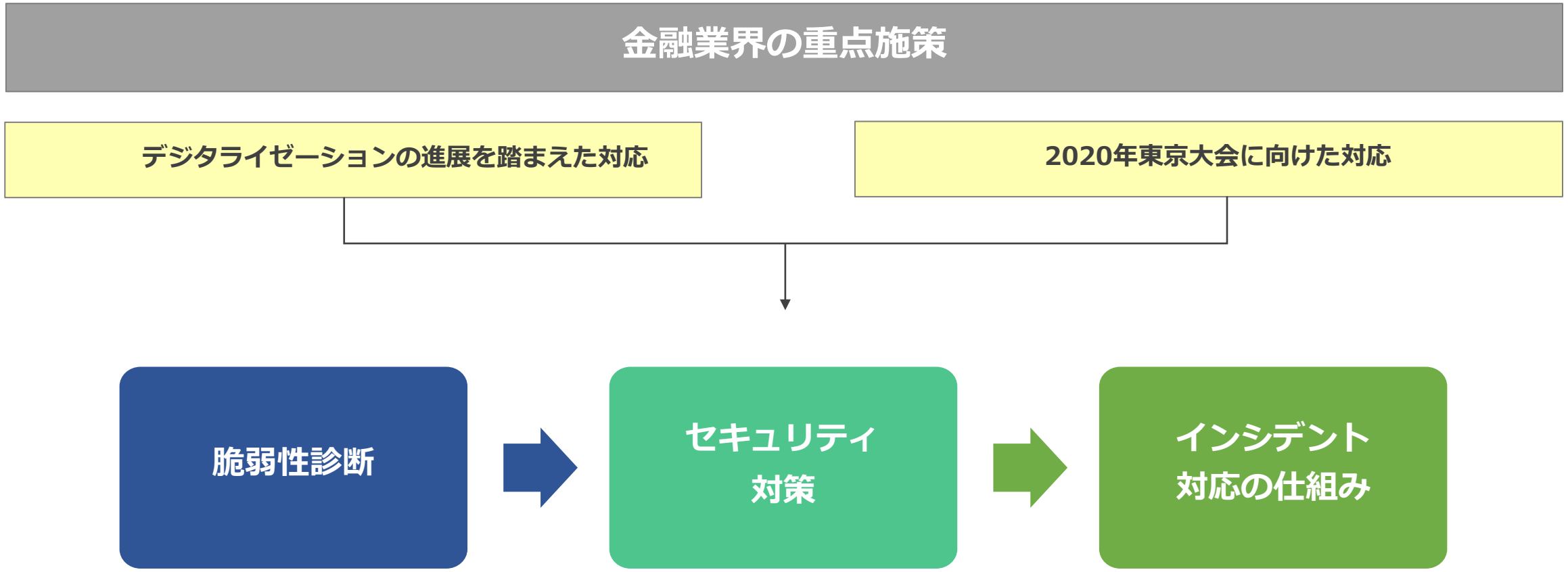
・金融機関が対象

・Delta Wall Ⅳは2020年東京オリパラ大会の開催時におけるリスク等を想定したシナリオ

・令和元年10月に実施されたDelta Wall Ⅳの結果としては多くの金融機関がコンチプラン等の見直しや社内外の情報連携強化に向けた対応を実施し、演習を通じて対応態勢を改善。
一方、インシデント対応時における委託先との連携や顧客対応等が不十分、インシデント対応に必要な人員が確保できていないなどの課題が認められ、対応能力の向上を図っていく必要あり

人員確保と共に効率的にインシデント対応ができる仕組みと
また、事前に社内に内在している脅威を察知する事が重要

金融庁における今後の取り組み



サイバーセキュリティ対策強化のために3段階の対策が必要

サイバー攻撃の動向

セキュリティ__マルウェア対策__脅威トレンド

IPA『情報セキュリティ10大脅威 2019』で「サプライチェーン攻撃」が　初めてランクイン！

順位	組織	昨年順位
1位	標的型攻撃による被害	1位
2位	ビジネスメール詐欺による被害	3位
3位	ランサムウェアによる被害	2位
4位	サプライチェーンの弱点を悪用した攻撃の高まり	**NEW**
5位	内部不正による情報漏えい	8位

[出典]IPA 情報セキュリティ10台脅威
https://www.ipa.go.jp/security/vuln/10threats2019.html

・取引先や関連企業といった中小規模で　セキュリティ対策が手薄な企業を狙い、**踏み台にして大企業を攻撃**する手法

・2017年と比べて2018年のサプラチェーン攻撃の発生件数は**178%アップ**※

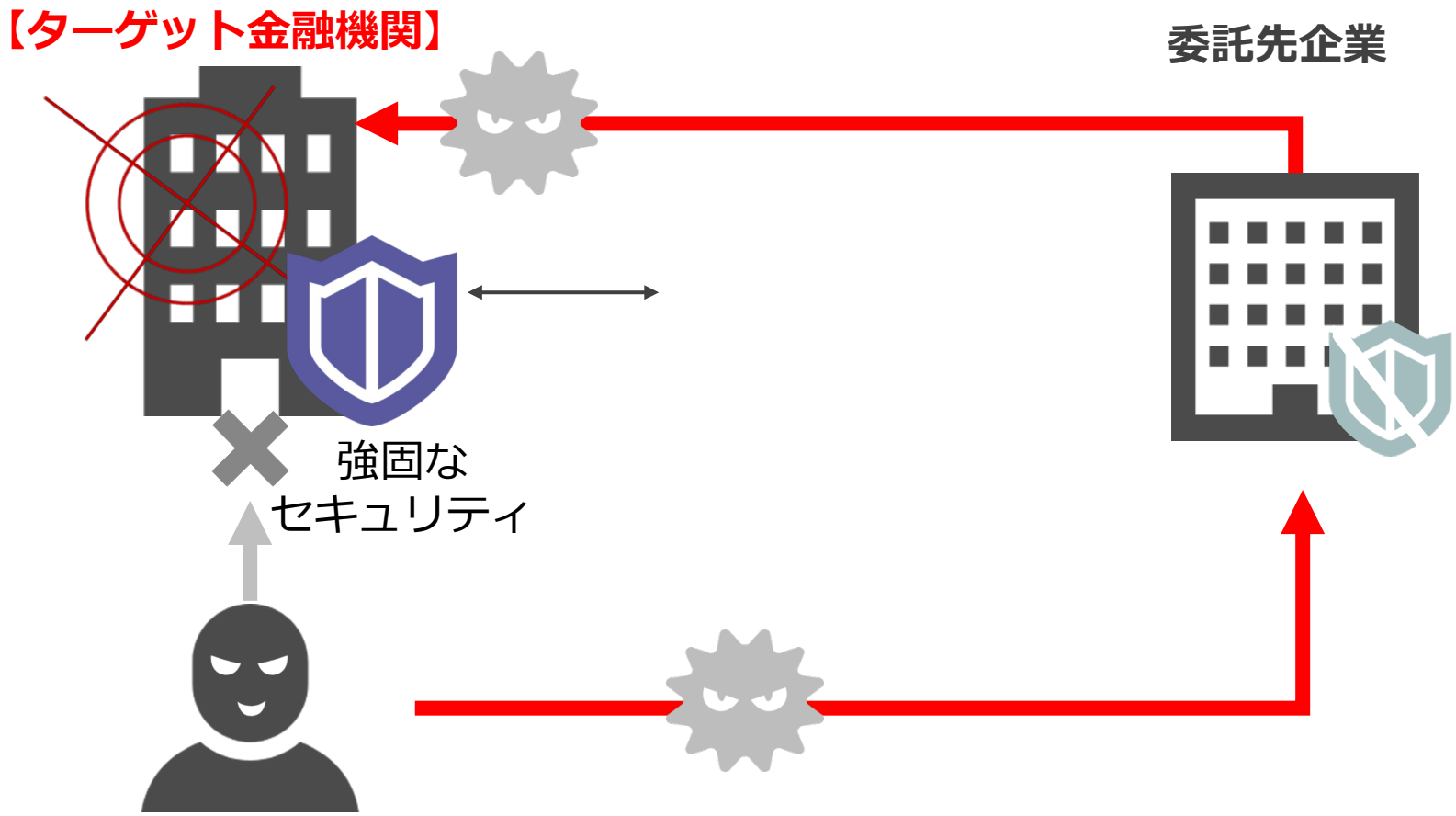
・経済産業省の「サイバーセキュリティ経営ガイドライン」でも、経営者が認識すべき事項として指摘

※[出典]Symantec
ISTR インターネットセキュリティ脅威レポート第24号　2019年2月

攻撃者から中小企業がターゲットとされている

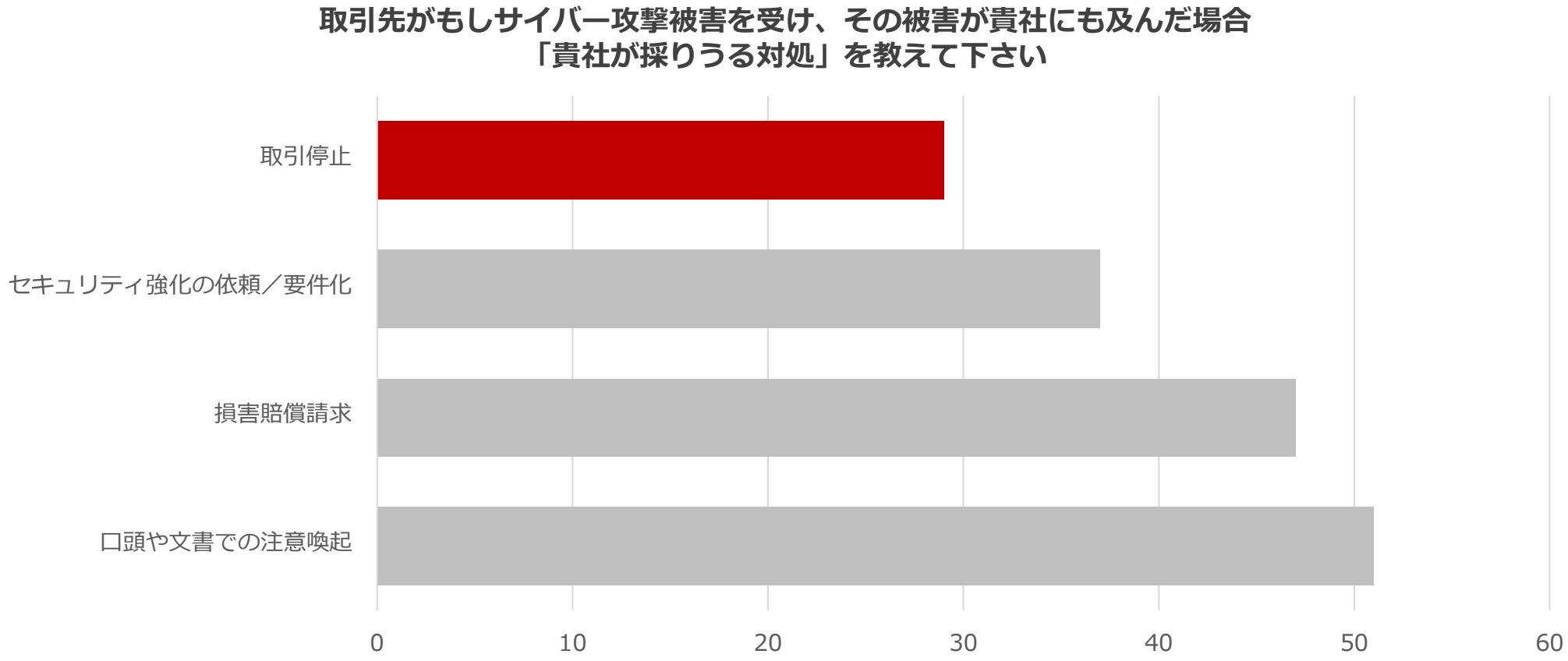
サプライチェーン攻撃の仕組み

セキュリティ強度が弱い委託先を踏み台にして、サプライチェーンをたどり最終的なターゲット企業を攻撃する手法の事を言います。また別の攻撃手法としてはソフトウェアメーカーのアップデートサーバにマルウェアを忍び込ませアップデートの配信時にマルウェアに感染させる攻撃も観測されています。強固なセキュリティで自社の対策をしていても防ぐことが難しい攻撃です。



対策が十分でないとお客様に逃げられるかも？

取引先がサイバー攻撃被害を受け、被害が自社に及んだら…3割の企業が「取引停止」の可能性もあると回答



サイバー攻撃の被害により事業に大打撃を与える可能性も

2020年 サプライチェーン攻撃の代表格「Emotet」

サプライチェーン攻撃の中で今猛威を振るっているのが「Emotet」です。メールにマルウェアが組み込まれた添付ファイルを付けて、大量にばらまきを行います。

1 RE: ご融資につきまして

タイトルに「RE：」。過去のやり取りの続きを匂わせる

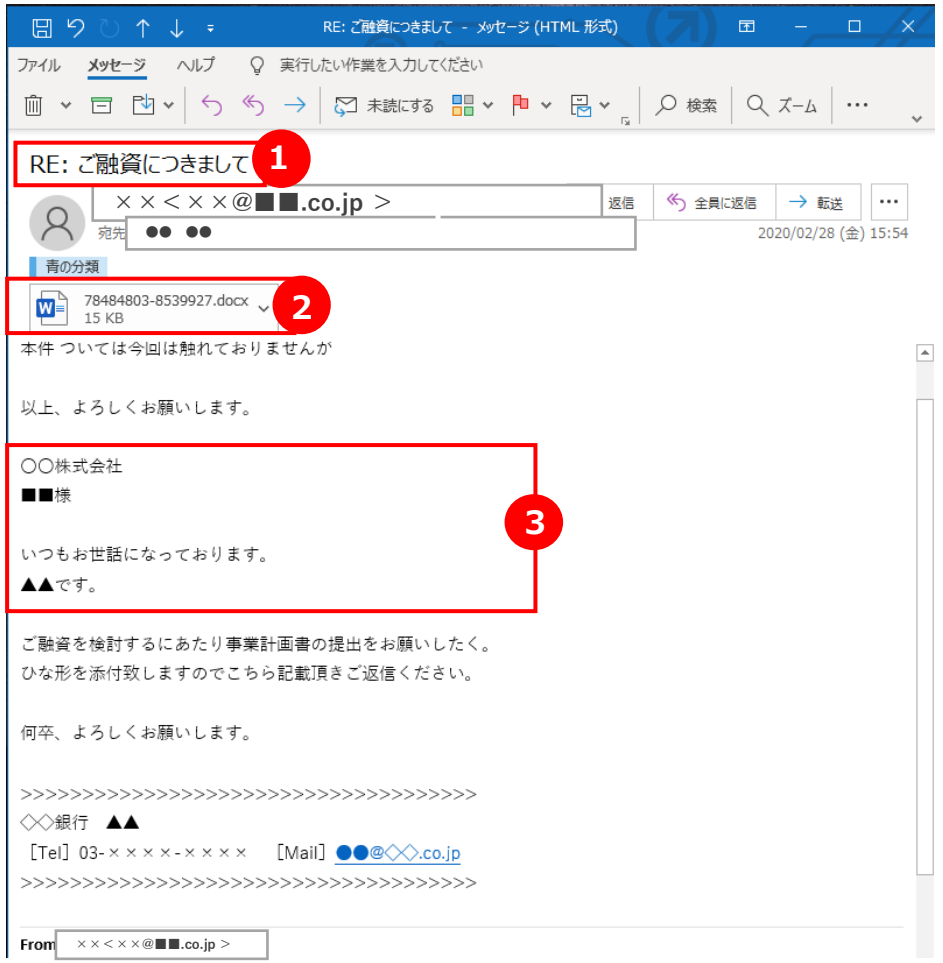
2 78484803-8539927.docx 15 KB

怪しい実行ファイルではなくWordファイルが添付

3
○○株式会社
■■様

いつもお世話になっております。
▲▲です。

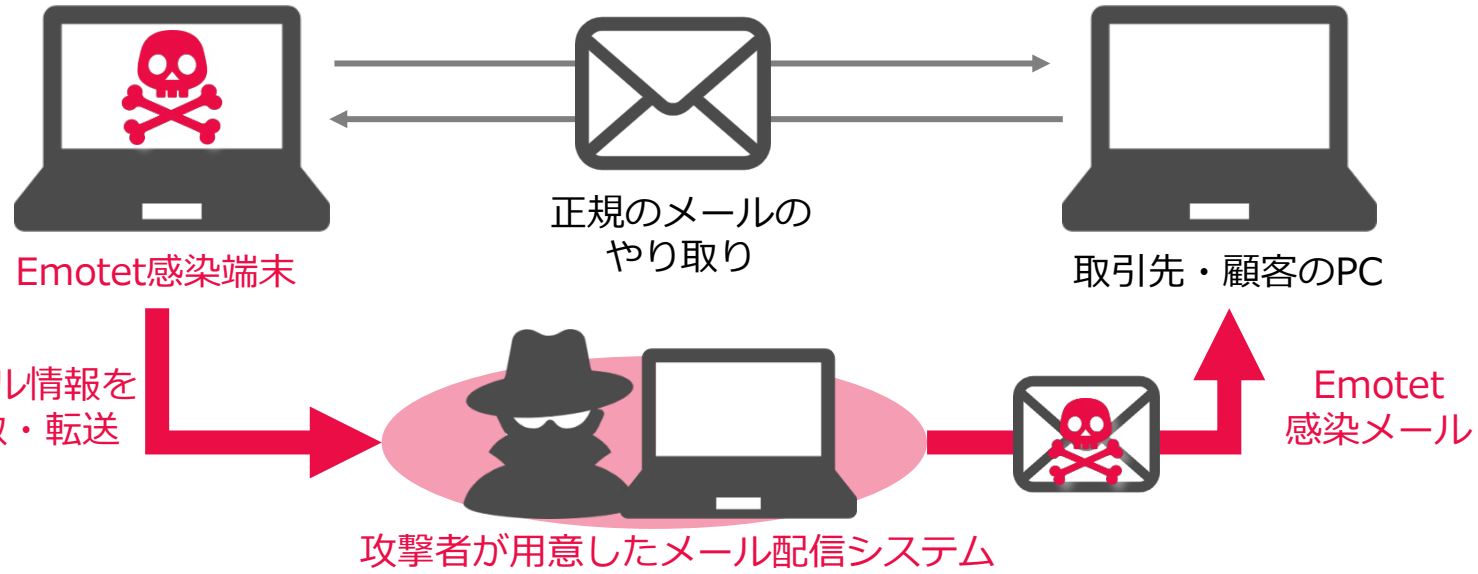
メール本文に実際の過去のやり取りの文章が引用



巧妙！Emotetばらまきメール配信の仕組み

セキュリティ対策が甘い取引先を踏み台にし情報を搾取。ターゲット企業を攻撃する手法です。窃取したメール情報を悪用し、巧妙なばらまきメールを送信し感染させようとします。

【窃取される恐れのある情報】
- 端末やブラウザに保存されたパスワード等の認証情報
- メールアカウントとパスワード
- メール本文とアドレス帳の情報



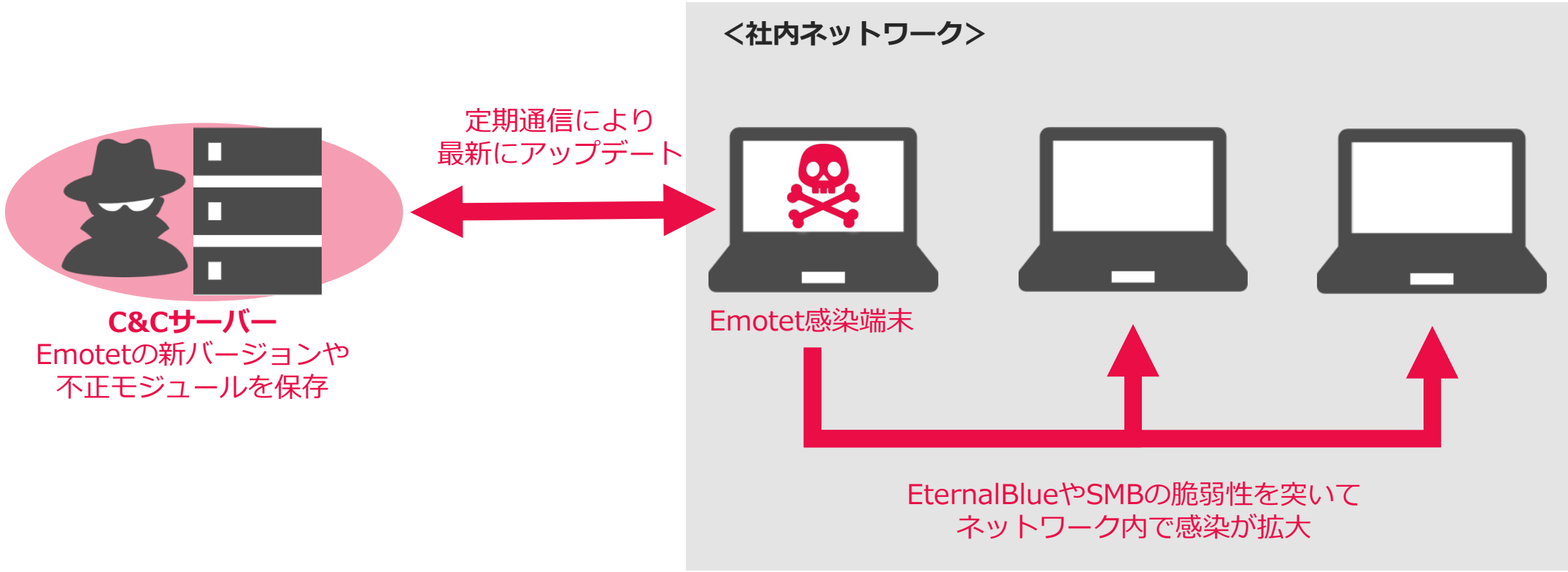
Emotetの被害が拡大

ブランドイメージの低下

損害賠償・取引停止

感染拡大を虎視眈々と狙い潜伏

自己増殖能力を持ち、潜伏しながら頻繁にアップデートを行います。新たな脆弱性の発見が感染拡大の引き金につながる恐れがあるのもEmotetの恐ろしいポイントです。



Emotet感染端末の末路

情報窃取が完了したらランサムウェアを呼び寄せ、自身の活動の痕跡を隠して調査不能させてしまいます。感染したら最後、フォレンジックも困難な状態になります。

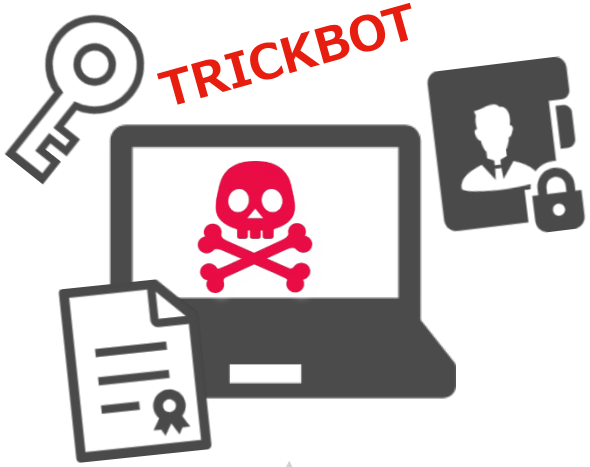
Emotetに感染

EMOTET

ばらまきメールに添付したMicrosoft Word ドキュメントのマクロが実行され、EmotetがPCに侵入、感染する。
メール情報を窃取し次の感染に悪用

情報窃取などの不正行為

TRICKBOT



PCに潜伏したEmotetが様々な不正モジュールをダウンロードし、認証情報の窃取や他の組織内PCへの侵入を試みる。

ランサムウェアで痕跡抹消

RYUK（Ransom）

PCのデータが暗号化され、使用不可に。データを復元できないため、Emotetが原因なのか、どんな情報が窃取されたのか、調べることすらできない。

Emotet への有効な対策とは？

Emotetは変化を繰り返しているマルウェアです。今後攻撃手法が変わる可能性もあるので、どんな手法で侵入されても検知・防御できる体制構築が必要です。

【現時点でのEmotetへの対応策】

Emotetの特徴	対応策
メール添付したMicrosoft Wordドキュメントのマクロを利用してEmotetの本体ファイルをダウンロードし、感染する。	・マクロの自動実行の無効化 ・マクロの利用に対してセキュリティ製品で制御を行う
情報窃取などの活動を行う際には、専用のモジュールをダウンロードし、メモリ上で動作させる。	メモリ上の不審な動作に対して対策ができるセキュリティ製品を活用する
ワーム機能を有しており、ネットワーク内で自己増殖し、感染端末を増加させる。	境界型ではなくエンドポイントでのマルウェア対策（アンチウイルス）を強化する

前提として基本的な対策が行われていることも非常に重要となります。
Emotet への対策の基本として、JPCERTコーディネーションセンターでは以下の対策を推奨しています。

- 組織内への注意喚起の実施
- マクロの自動実行の無効化（事前にセキュリティセンターのマクロの設定で「警告を表示してすべてのマクロを無効にする」を選択しておく）
- メールセキュリティ製品の導入によるマルウェア付きメールの検知
- メールの監査ログの有効化
- OSに定期的にパッチを適用（SMBの脆弱性を突く感染拡大に対する対策）
- 定期的なオフラインバックアップの取得（標的型ランサムウエア攻撃に対する対策）

出典：JPCERT/CC マルウエア Emotet の感染に関する注意喚起(2019/11/27)　https://www.jpcert.or.jp/at/2019/at190044.html

エンドポイント侵害診断

セキュリティ＿マルウェア対策について

エンドポイント侵害診断とは

ありとあらゆるサイバー脅威のリスクを分析・改善方法までご提案します

【情報分析】

- 過去もしくは現在、サイバー攻撃が行われている痕跡がないか？
- 社内に危険なプログラムは無いか？
- その他サイバー脅威に対するリスクが存在しないか？

【対応策の提案】

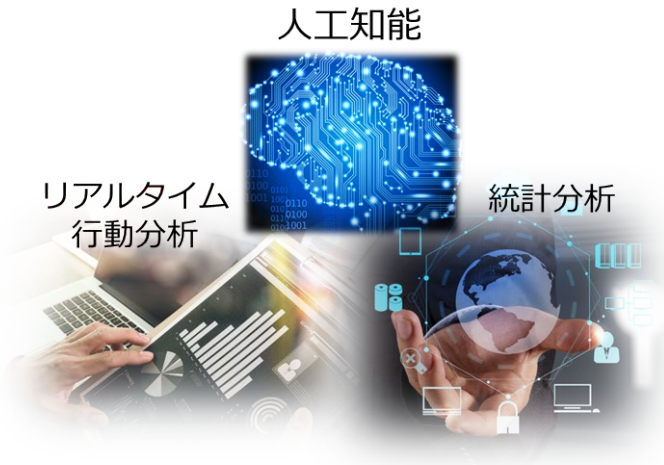
スクリプトで必要な情報を自動収集！複数のアプローチで解析し リスクを発見
初回打ち合わせから2～3カ月で完結できます！

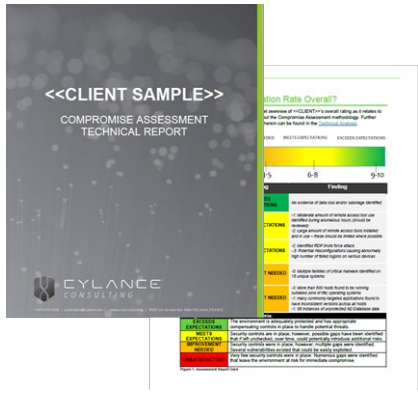
情報収集 ▶▶ **詳細分析** ▶▶ **レポート報告**

スクリプトの実行でカンタンに
分析に必要な情報を転送

人工知能／機械学習をコア技術とし
複数のアプローチで解析

分析結果だけでなく
対処策までを提案





こんなお客様におすすめです

弊社の商品を導入されていない方にもご利用いただけます
社内リスクの状況把握にピッタリです！

安全であるかどうか確認したい

現在のセキュリティ対策では気づけない脅威が潜在していないかを調査します。

サイバー攻撃を受けたことがある

サイバー攻撃の原因や脅威の残留がないかを調査し、再発防止策をご提案します。

サイバー攻撃対策の強化を検討している

現状のリスクを洗い出し、検討している対策の妥当性の判断を支援します。

今世紀最強のアンチウイルス？！『プロテクトキャット（BlackBerry Protect）』

セキュリティ__マルウェア対策__最強のアンチウイルス『BlackBerry Protect』

未知・亜種のマルウェアもマシンラーニングで99%検知！次世代のアンチウイルス

次世代型AIアンチウイルス

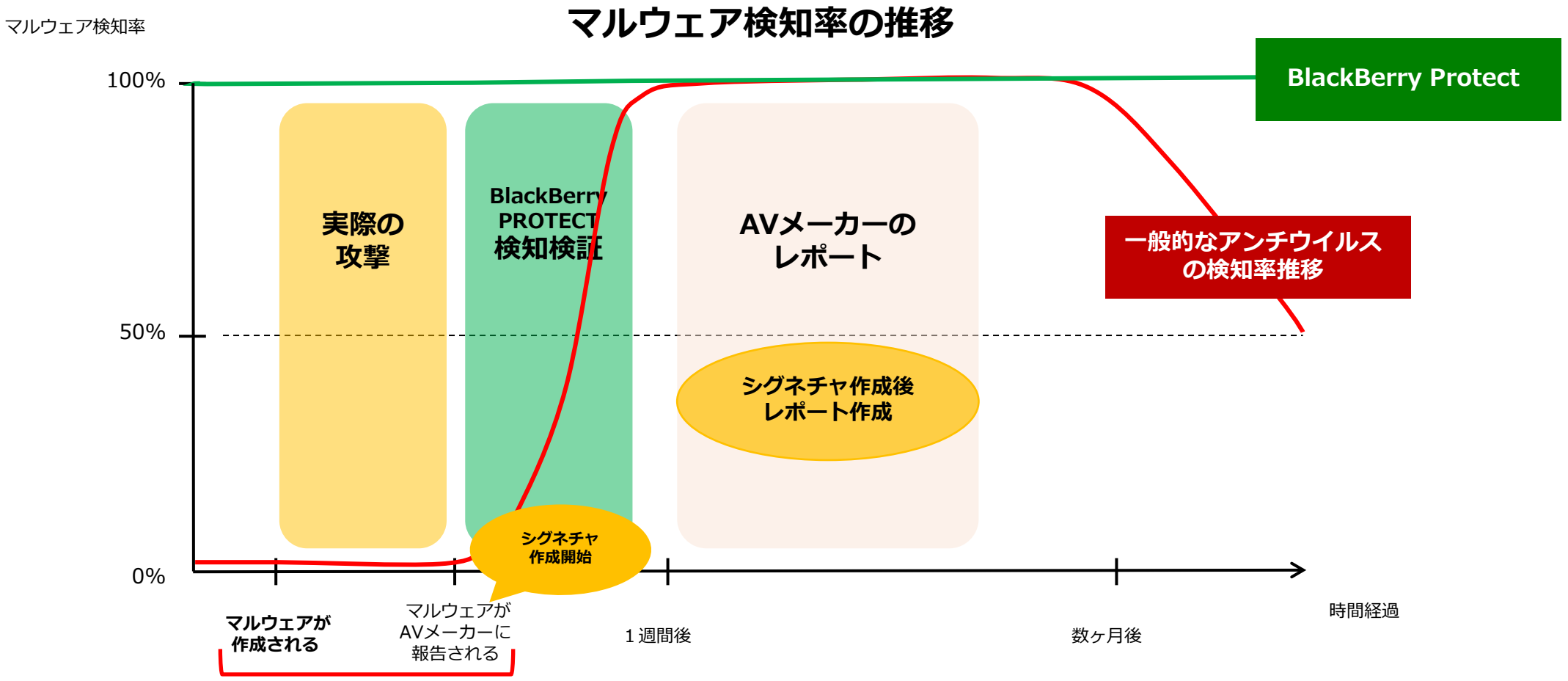
BlackBerry Protect

AIを活用したマシンラーニングによる予測検知が可能で、未知・亜種のマルウェアも99%の高検知が実現。LANSCOPE連携で簡易EDR、オプションのOpticsによるDERが可能

- AIによる高精度な予測検知
- シグニチャレスで日々のアップデート不要
- 過検知が少なく低負荷

既存アンチウイルスとの違い

構造的な問題でシグネチャでは実際の攻撃を止められない



（事前対策）この期間に端末が保護できるかが重要

平均25か月前に、未来に発生するマルウェアを予測して検知
あらゆる未知・亜種のマルウェアから組織を守ります

MyWebSearch
26か月前に予測

Emotet
27か月前に予測

PolyRansom
28か月前に予測

GandCrab
26か月前に予測

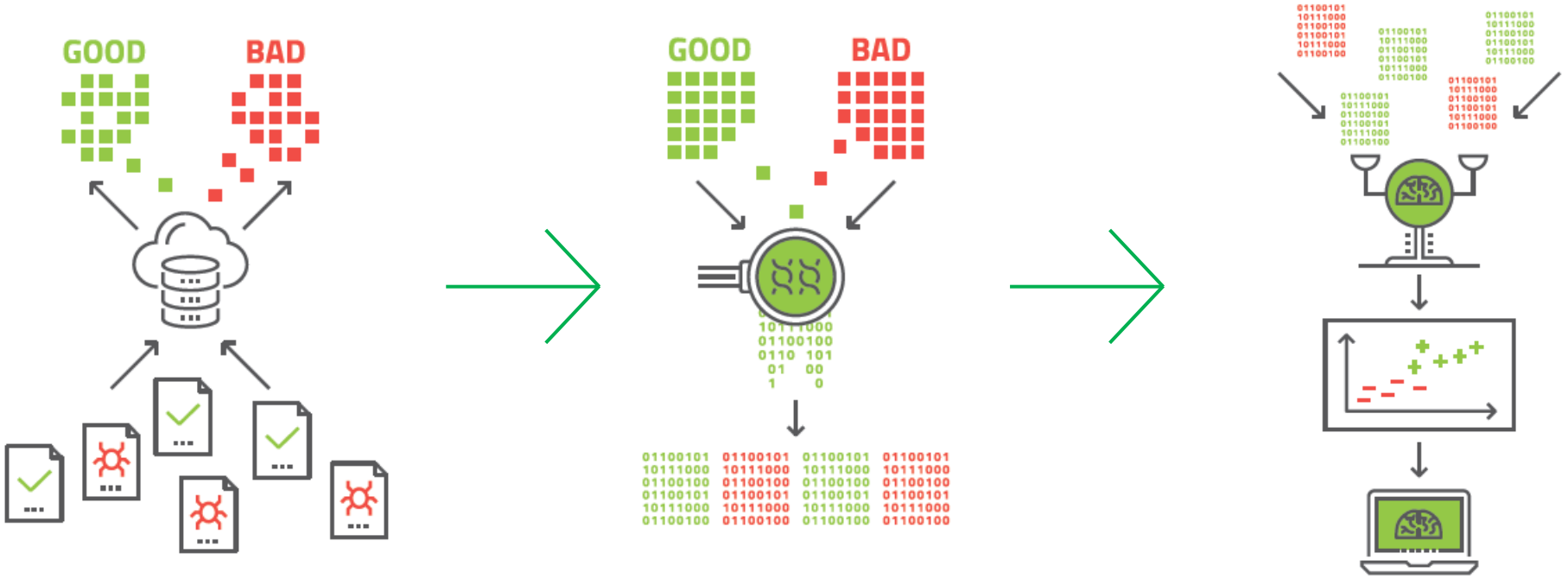
installCore
27か月前に予測

Petya-Like
20か月前に予測

GoldenEye
13か月前に予測

WannaCry
19か月前に予測

マシンラーニングの特許技術を活用した「予測脅威防御」



収集と学習

正常なファイルとマルウェアを10億以上収集し、クラウド上のAIに教師データとして学習させる

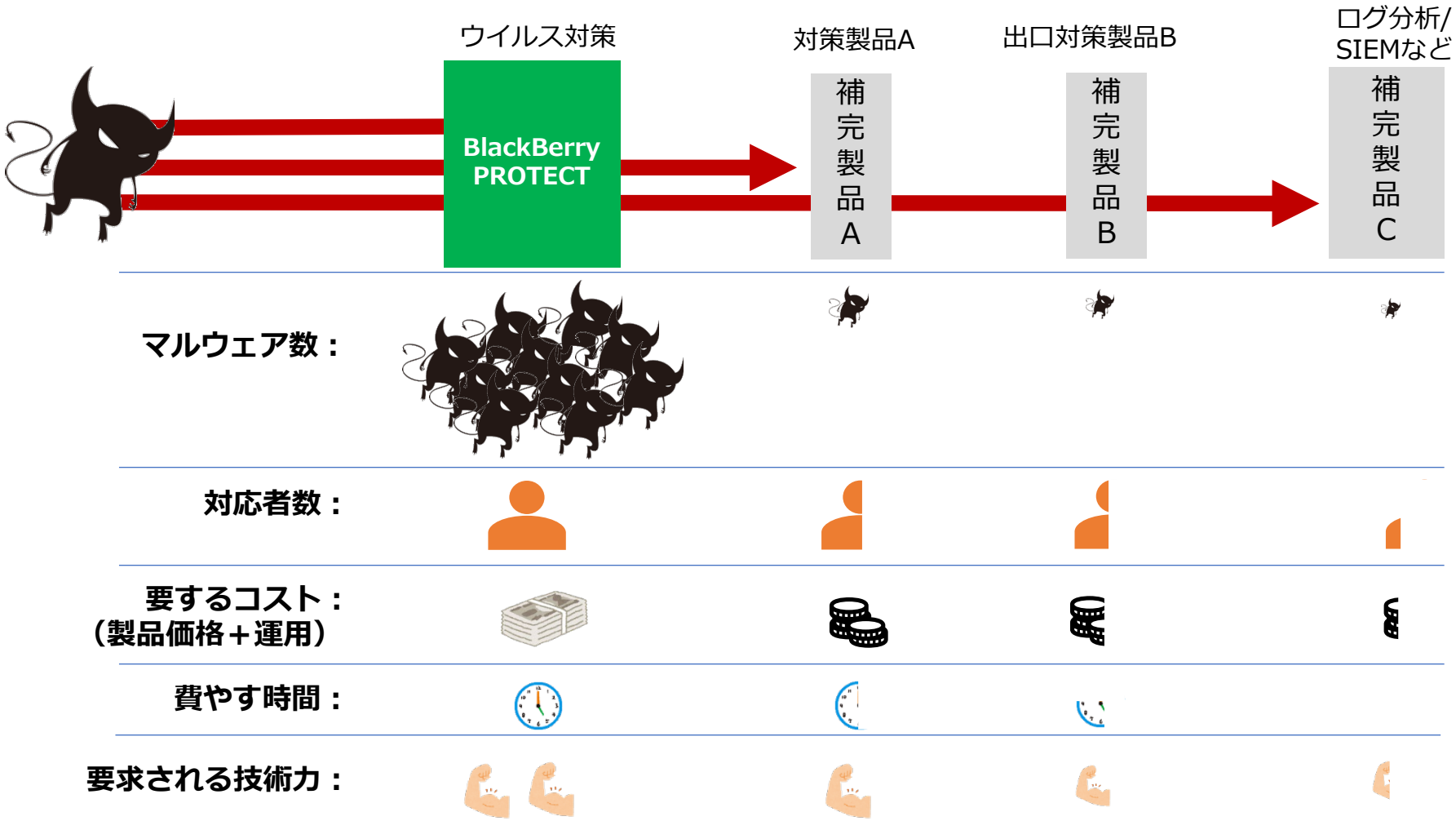
特徴抽出・数値化

教師データの特徴点を抽出（1ファイルあたり最大700万の特徴点）、各ファイルのマルウェアらしさを数値化

数理モデル作成

数学者やアナリストのチューニング後、膨大なノウハウを反映した数理モデルを作成。端末上は数理モデルのみ稼動

事前に止める。だから事後対策に掛かるコスト・工数・技術力が抑えられる



一度の漏洩が億単位の賠償になるコストよりもセキュリティの担保を優先

・多層防御を実施しているが万が一のマルウェアの**すり抜け**を懸念。

・従来型のパターンマッチングのアンチウイルスでは、**未知には十分な対策とは言えない。**

・振る舞い検知は**マルウェア実行リスク**を懸念。

・最終的に守る部分は**エンドポイント**である。

・**運用・PC負荷**を上げたくなかった。

沖縄銀行 システム部 システム企画管理グループ
上席調査役　上原 慶典 氏

導入の決め手は「事前検証テスト」実行前検知、検知率の高さ、低い運用負荷

株式会社おきぎんエス・ピー・オー　システム開発部 金融システム開発課 チーフ　上原 浩輝 氏

・テスト時、オフラインでも**高い検知率**

・パターンファイルアップデートによる
トラブルを過去経験、AIモデルの更新は
頻度が少なく**管理負担の軽減になる**。

・PC側の**定期スキャンも無く**ユーザが快適。

・LANSCOPEのログ連携でWebコンソールによる
原因特定が容易になった。

MOTEXだからこその付加価値

最強のアンチウイルスがさらに便利になるポイント

MOTEXは『BlackBerry Protect』をLANSCOPEのマルウェア対策ツールとして販売

①PC操作ログでマルウェア侵入の流入経路を特定

②インターネット非接続環境の統合管理

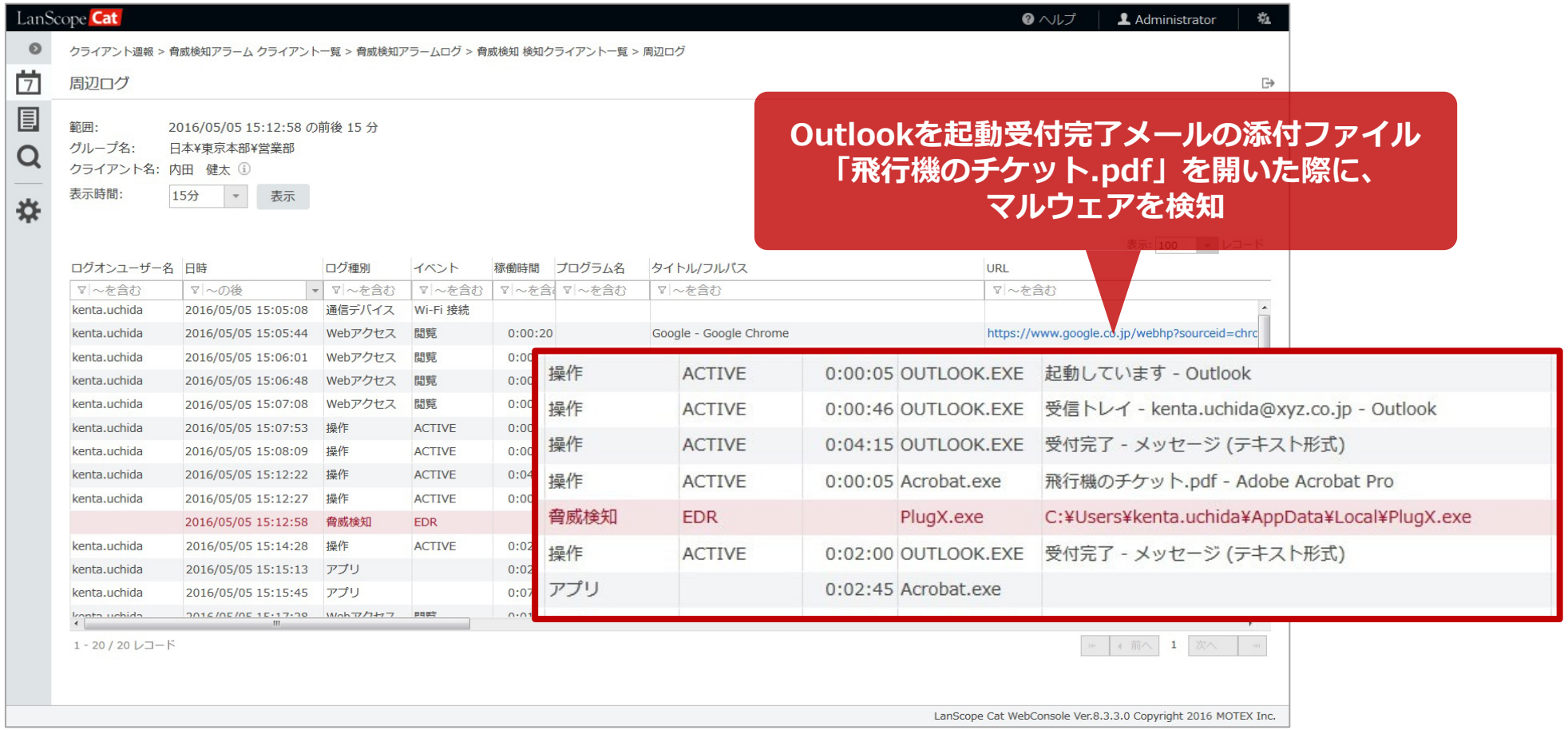
③マルウェア検知時に即時管理者へメール通知

OEMパートナーならではの インシデント対応での便利な3つのポイント

ポイント①__操作ログで “流入経路” の特定

どんなマルウェアになぜ感染したかをクリックだけで追跡
流入経路を操作ログで確認し再発防止

【周辺ログ】



インターネット非接続のクローズド環境の統合管理

BlackBerry Protect

【クローズド環境における運用】

・クローズド環境においても数理モデルで、非常に高い防御率を実現します。

・マルウェアの検知状況を各端末上で確認できます。

・クラウドにある管理サーバーとの通信が出来ない為、プログラムのアップデート、ポリシーの更新、検知状況の把握ができる仕組みを別途用意する必要があります。

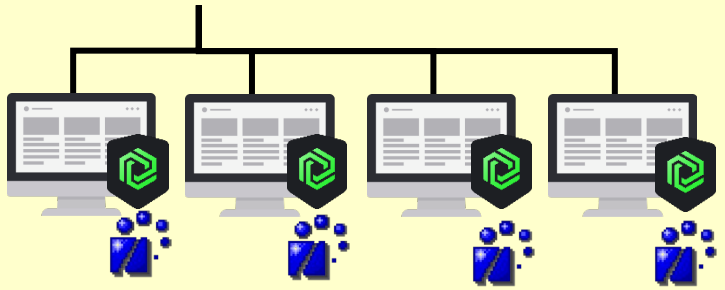
BlackBerry Protect×LANSCOPE

（Ver.8.4.0.0）

【クローズド環境における運用】

・LANSCOPEマネージャーからBlackBerry Protectのプログラムやポリシーの更新が可能です。

・マルウェア検知状況ログをリアルタイムにLANSCOPEマネージャーに送信しレポート及び、メール通知、定期的なCSV出力が可能です。



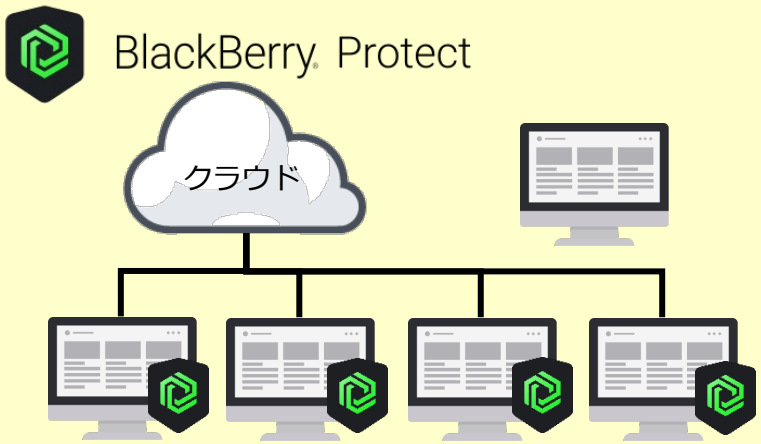
※BlackBerry Protect Managed Service for LASCOPE ご利用時は
条件付きでインターネット接続可能な環境が必要

検知状況をリアルタイムにメール通知

BlackBerry Protect

【メール通知機能】

マルウェアを自動隔離した場合、
安全なのでメール通知をしない。

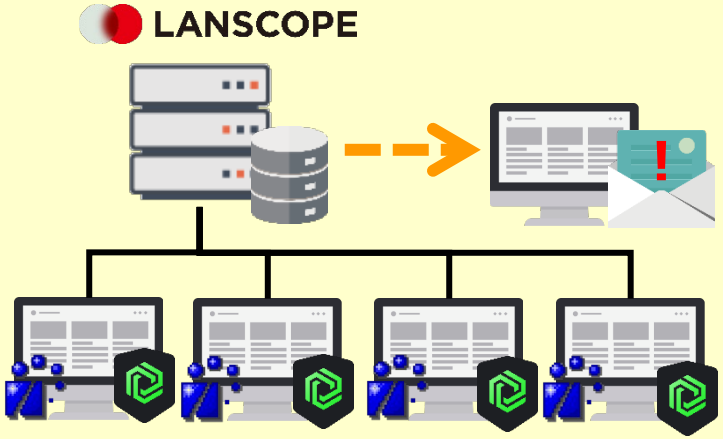


BlackBerry Protect×LANSCOPE

(Ver.8.4.0.0)

【メール通知機能】

マルウェア発見時は、部門ごとの管理
者にメールで通知できます。



まとめ

BlackBerry Protect国内販売４年連続No.1獲得！国内唯一のOEM連携製品

次世代型マルウェア対策製品としてLANSCOPEにOEM連携、2020年以降CPMSスタートで多彩なプランが登場

CYLANCE
2019 Japan Partner of the Year

BlackBerry Japan
「2019 Japan Partner of the Year」
国内販売実績 4年連続NO.1

まずは①[現状把握]で、社内脅威状況の現状把握が第1歩！！

①[脆弱性診断] 脅威リスクの洗い出し、改善方法の提案

**エンドポイント
侵害診断サービス**

**AIアンチウイルス
無料体験キャンペーン**

②[セキュリティ対策] AIで事前検知、事後対策の工数削減

③[インシデント対応の仕組み]

＿流入経路の特定、メール通知にてインシデント対応をスムーズに

BlackBerry Protect　×　LANSCOPE

BlackBerry Protect

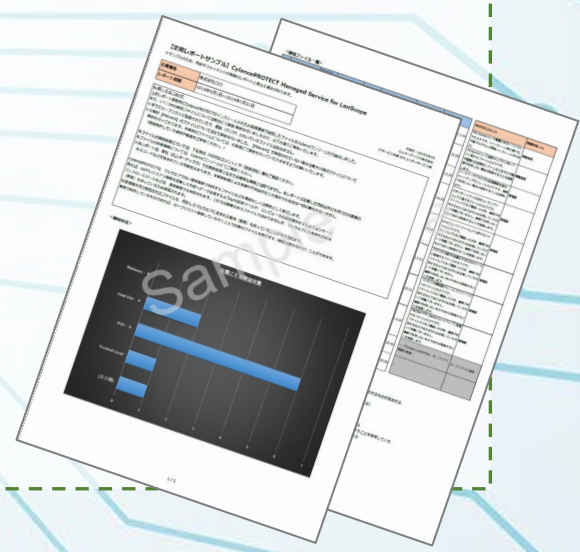
AIアンチウイルス無料体験キャンペーン

～BlackBerry Protectを気軽に使ってみよう～

最新AIを活用した新技術で超高精度の検知率を誇る「BlackBerry Protect」を**1ヶ月無料**で**何台でも体験**できるキャンペーンがスタートしました。実際に自社のPCにBlackBerry Protectをインストールし、コンソールの操作方法や検知力の高さを体験いただけます。

体験終了後、エムオーテックスにて**検知結果のサマリーレポートをご提供**します。
AIを活用した最新鋭のアンチウイルス製品を、この機会にお気軽にご体験ください！

●お申し込みはこちらから
https://go.motex.co.jp/l/320351/2019-06-27/2fv6jr?re



https://www.lanscope.jp/cpms/