Cybereason セミナー

経営課題として取り組むべき サイバー脅威対策

サイバーリーズン・ジャパン株式会社
パートナー営業本部

2021年11月XX日

cybereason

©2021 Cybereason Japan Corp. | All rights reserved

経営課題として取り組むべきサイバー脅威対策

Agenda

1. サイバーリーズンについて
2. 最新のサイバー攻撃事例のご紹介
3. 経営課題として取り組むべき平時の備え
4. サイバーリーズンのセキュリティ技術のご紹介
5. デモンストレーション実施
6. Q&A

cybereason

©2021 Cybereason Japan Corp. | All rights reserved

サイバーリーズンとは

©2021 Cybereason Japan Corp. | All rights reserved

Cybereasonとは

イスラエルの軍事技術から生まれたAIによるエンドポイント・セキュリティ対策を提供

ビジネス

USボストンに本社を構え、
ワールドワイドにビジネスを
展開

テクノロジー

イスラエル軍のサイバー部隊である8200部隊の知見と実践経験に
基づく攻撃分析の
ノウハウを製品化

体制・品質

日本のお客様に寄り添った体制
日本の品質と改善を製品やサービスにフィードバック

Cybereason Inc.
設立：　2012年
事業拠点：　ボストン(本社)、 イスラエル(研究開発)、東京、ロンドン、シドニー
従業員数：　約1,000名 ※2021年9月時点

サイバーリーズン・ジャパン株式会社
設立：2016年
事業拠点：東京、大阪、名古屋
従業員数：約170名 ※2021年9月時点

最先端のエンドポイント・テクノロジとして、数々のアワードを受賞

Gartner Forbes CNNMoney CRN JMP SECURITIES a16z 100 NETWORKWORLD CYBER SECURITY EXCELLENCE AWARDS WINNER 2017
WSJ InformationWeek DARKReading BostInno WIRED CTECH Boston Business Journal

サイバーリーズンの歩み

2012.7
CYBEREASON設立

2013.5
$4.6M Series A

2015.3
- $25M Series B
- ボストン本社開業

2015.9
$59M Series C

2016.4
日本法人開業

2016.11
ロンドン支社開設

2017.6
$100M
Series D

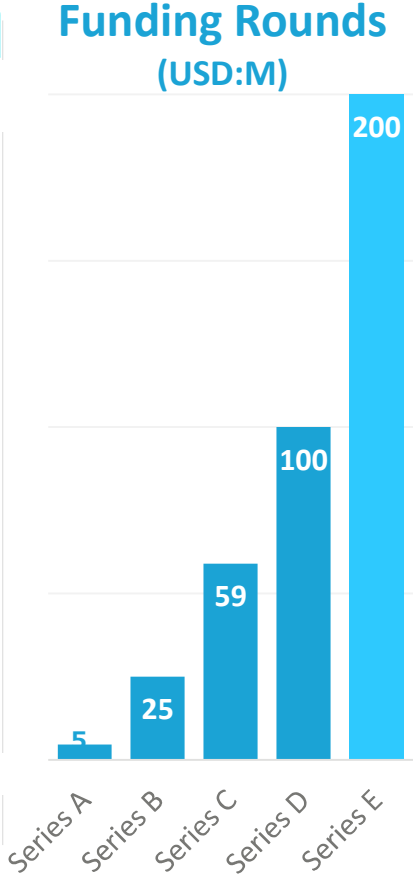
2018.1
シドニー開設

2018.10
西日本支社開設

2019.1
名古屋支店開設

2019.8
$200M
Series E

- 2012年設立以来、総額3.89億ドルの資金を調達し、急速成長
- サイバーリーズン日本法人を設立し、日本市場へコミット
  - 画面UI/レポートの完全日本語化
  - 新規パートナー開拓によるビジネスの強化
  - 日本法人従業員は2021年に170名



Protect It All | ©2021 Cybereason Japan Corp. | All rights reserved

国内エンドポイントセキュリティNo.1

EPP

国内標的型サイバー攻撃向け特化型
脅威対策(STAP)製品市場(エンドポイント製品)
ベンダー別売上額／シェア、2018 年～2019 年

2018
2019
No.1

出典：IDC Japan株式会社、2020年10月発行「国内標的型サイバー攻撃対策ソリューション市場シェア、2019 年：マネージドセキュリティサービスの進展」

次世代エンドポイント
プロテクションプラットフォーム
出荷金額(メーカー出荷) 2019年

2018
2019
EPP
No.1

出典：デロイト トーマツ ミック経済研究所株式会社「外部脅威対策ソリューション市場の現状と将来展望2020年度　サイバーセキュリティソリューション市場16版目」

EDR/NGAV市場:
ベンダー別売上金額シェア

2018
2019
EDR/
NGAV
No.1

出典： 株式会社アイ・ティ・アール、2021年5月発行、「ITR Market View：エンドポイント／無害化／Web分離／CASB／CSPM／SOAR市場2021」

EDR

NEW

EDR市場占有率

2019
2020
EDR
No.1

出典： 株式会社富士キメラ総研、2021年9月29日発行
「2020～2021 ネットワークセキュリティビジネス調査総覧(市場編)」
2019～2020年度実績

次世代エンドポイント
プロテクションプラットフォーム
出荷金額(EDRメーカー出荷)2019年

2018
2019
EDR
No.1

出典：デロイト トーマツ ミック経済研究所株式会社「外部脅威対策ソリューション市場の現状と将来展望2020年度　サイバーセキュリティソリューション市場16版目」

MDR

マネージドEDRサービス市場:
ベンダー別売上金額シェア

2018
2019
マネージド
EDRサービス
No.1

出典： 株式会社アイ・ティ・アール、2020年12月発行、「ITR Market View: エンドポイント・セキュリティ対策型/情報漏洩対策型SOCサービス市場2020」

©2020 Cybereason Japan Corp. | All rights reserved

TRUSTED BY (公開を許諾いただいたお客様のみ)

事例ホームページよりダウンロード可能
https://www.cybereason.co.jp/product-documents/

Fortune 500企業を始めとしたグローバルの導入実績

AJINOMOTO
ALMAC
AMERICAN NATIONAL BANK OF TEXAS
encore CAPITAL GROUP
FLOWSERVE
ISRACARD
LOCKHEED MARTIN
MIB MIDWEST INDEPENDENT BANK
motorola
Mount Sinai
rti surgical
Schwyzer Kantonalbank
VIZIO

日本国内実績
(幅広い業種における実績)

ダイダン
ELECOM
EXEDY 株式会社エクセディ
Kintetsu
富士製薬工業
GMO PAYMENT GATEWAY
Infcurion
J!NS
JR貨物
kanamoto ALLIANCE GROUP
九州朝日放送
muRata INNOVATOR IN ELECTRONICS
日本マクドナルド株式会社
Belc ベルク
OSAKA CITY 大阪市
SCSK
西武プロパティーズ
SoftBank
住友商事
ZOJIRUSHI
WOODONE
WORLD HOLDINGS
立命館大学
順天堂大学 JUNTENDO UNIVERSITY
宮崎大学 University of Miyazaki
獨協大学 DOKKYO UNIVERSITY

Protect It All | ©2021 Cybereason Japan Corp. | All rights reserved

導入事例

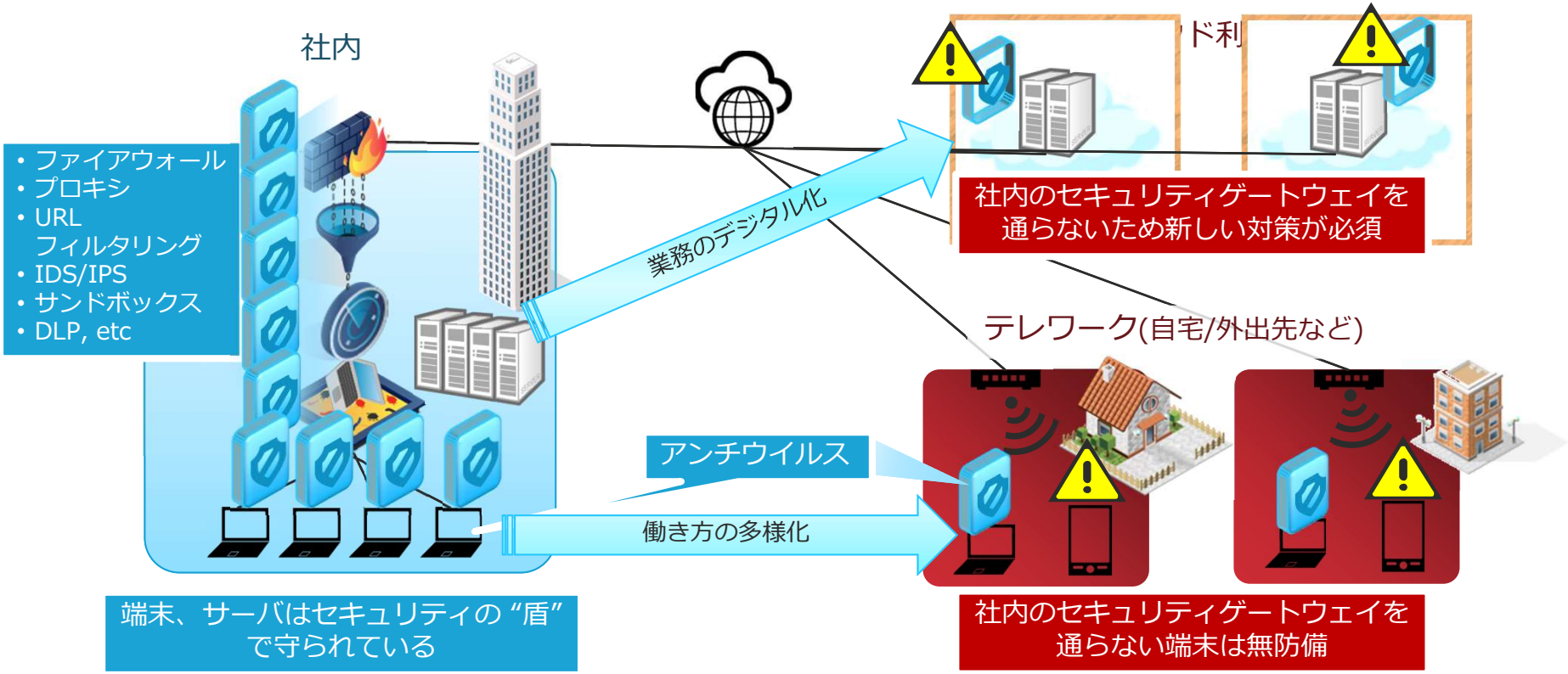
ホームページよりダウンロード可能
https://www.cybereason.co.jp/product-documents/

最新のサイバー攻撃事例のご紹介

cybereason

Protect It All | ©2021 Cybereason Japan Corp. | All rights reserved

テレワーク/DXによるセキュリティ環境の変化

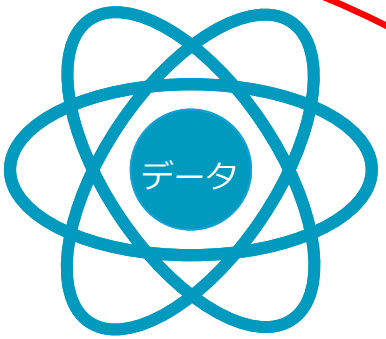


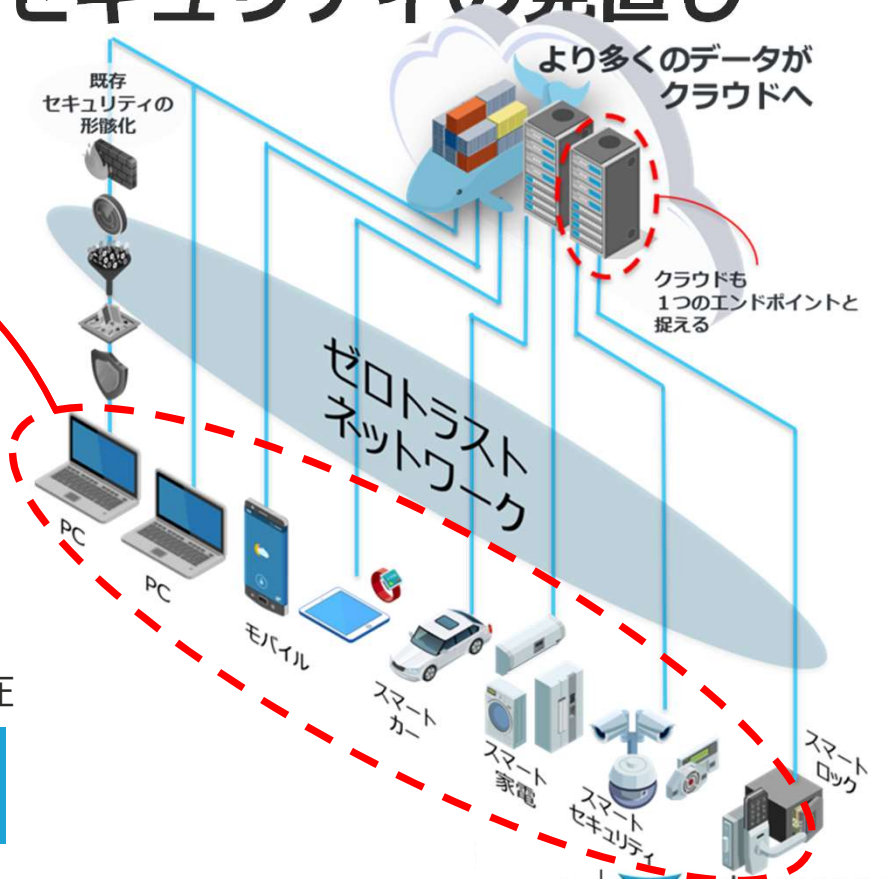
©2021 Cybereason Japan Corp. | All rights reserved

DX推進/テレワークによるセキュリティの見直し

端末や、業務システムは社外へ
(テレワーク)（SaaS/クラウド)

守るべきものは



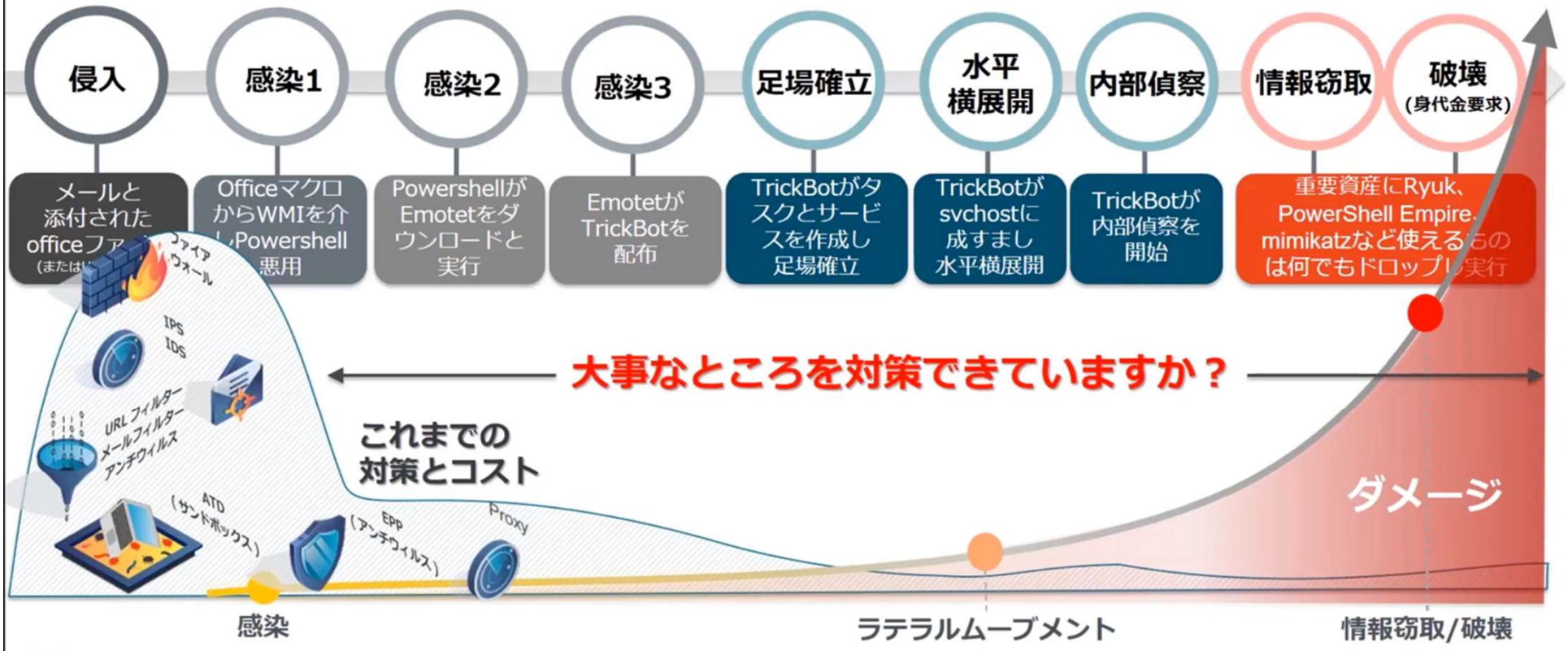


データは各エンドポイント(端末/クラウド)に存在

つまり、エンドポイントの
セキュリティ強化が必須

©2021 Cybereason Japan Corp. | All rights reserved

これまでのセキュリティ対策



©2020 Cybereason K.K. All rights reserved.

情報資産を狙った最新の脅威

https://www.nikkei.com/article/DGXZQOGN13FVQ0T10C21A5000000/
https://www.nikkei.com/article/DGXZQOGN1010J0Q1A610C2000000/
https://www.nikkei.com/article/DGXZQOUC25CMN0V20C21A5000000/
https://www.nikkei.com/article/DGXZQOUC1659T0W1A810C2000000/

cybereason

©2021 Cybereason Japan Corp. | All rights reserved
©2021 Cybereason Japan Corp. | All rights reserved

ランサムウェア被害

11秒に1回

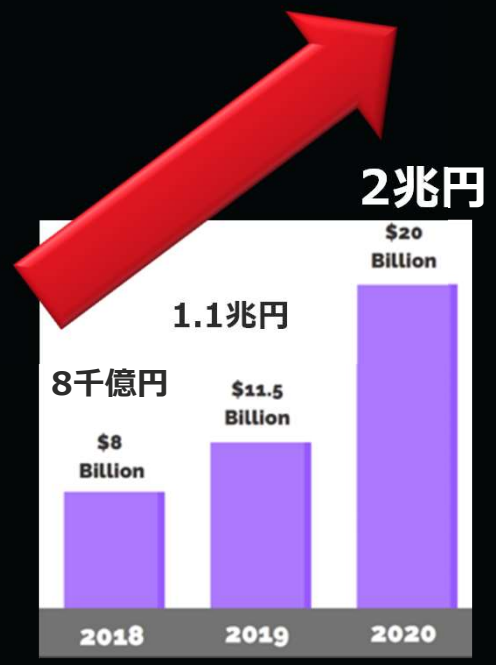
ランサムウェア攻撃 発生頻度

サイバーリーズン:【グローバル調査結果】ランサムウェア ～ビジネスにもたらす真のコスト～

約1600万円

ランサムウェア支払い平均額 2020年10-12月 ($154,108)

Coveware: Coveware Quarterly Ransomware Report
https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020



ランサムウェア総被害額

PurpleSec: 2020 Ransomware Statistics, Data, & Trends
https://purplesec.us/resources/cyber-security-statistics/ransomware/#Cost

©2021 Cybereason Japan Corp. | All rights reserved

ランサムウエアは

完全に組織化された犯行

防御する企業/組織も組織的な体制が必要

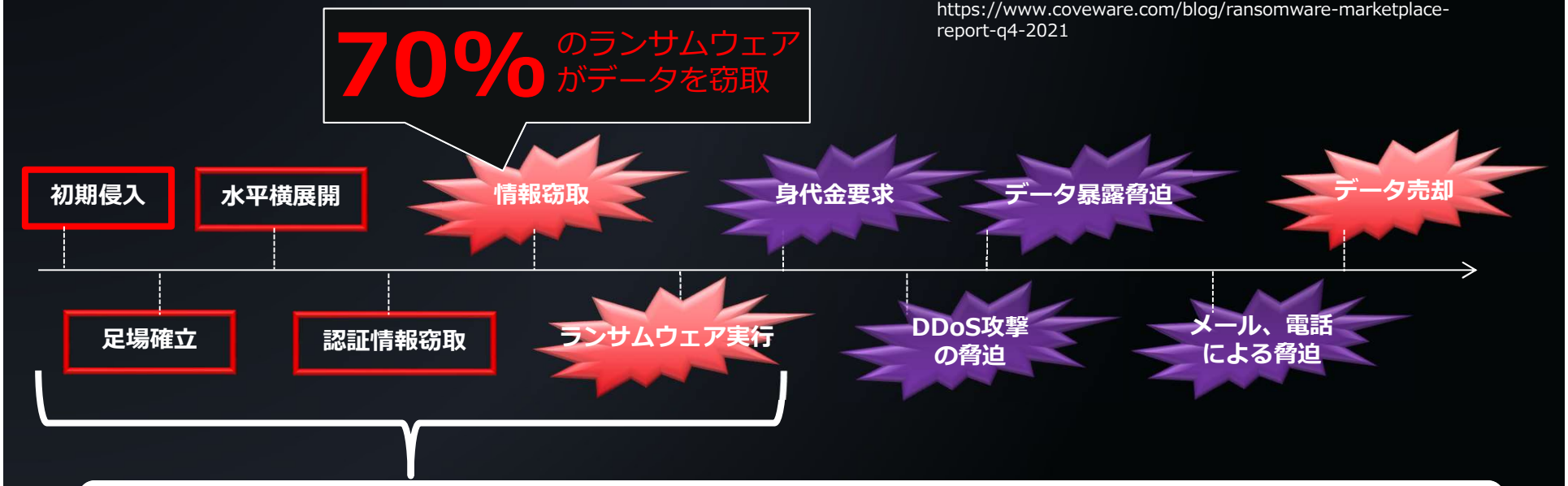
New York Times: Secret Chats Show How Cybergang Became a Ransomware Powerhouse
https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html

©2021 Cybereason Japan Corp. | All rights reserved

cybereason

最新のランサムウェアは多重脅迫型

Coveware: Coveware Quarterly Ransomware Report
https://www.coveware.com/blog/ransomware-marketplace-report-q4-2021



ランサムウェアを阻止できたとしても手遅れになる可能性
攻撃ストーリーを把握して対処することが必須

©2020 Cybereason Japan Corp. | All rights reserved

cybereason

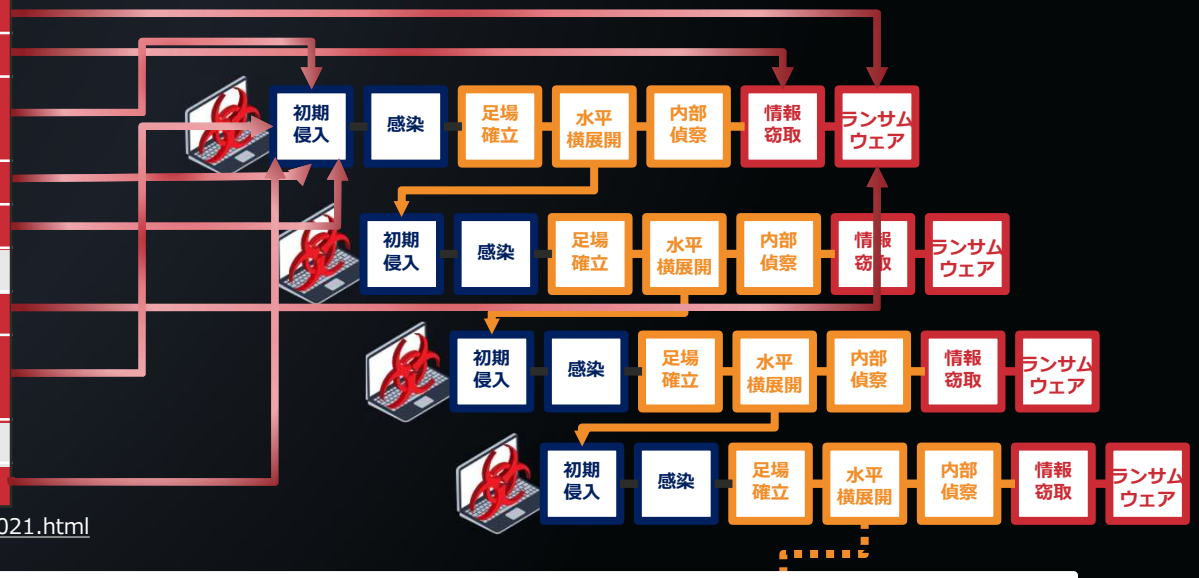
最新型のランサムウェアはあらゆる手段を駆使

情報処理推進機構（IPA）情報セキュリティ10大脅威 2021

上位8つの脅威を利用して攻撃

順位	組織向け脅威
1	ランサムウェアによる被害
2	標的型攻撃による機密情報の窃取
3	テレワーク等のニューノーマルな働き方を狙った攻撃
4	サプライチェーンの弱点を悪用した攻撃
5	ビジネスメール詐欺による金銭被害
6	内部不正による情報漏えい
7	予期せぬIT基盤の障害に伴う業務停止
8	インターネット上のサービスへの不正ログイン
9	不注意による情報漏えい等の被害
10	脆弱性対策情報の公開に伴う悪用増加

https://www.ipa.go.jp/security/vuln/10threats2021.html



導入済みのセキュリティソリューションで対応できるか見直しが必要

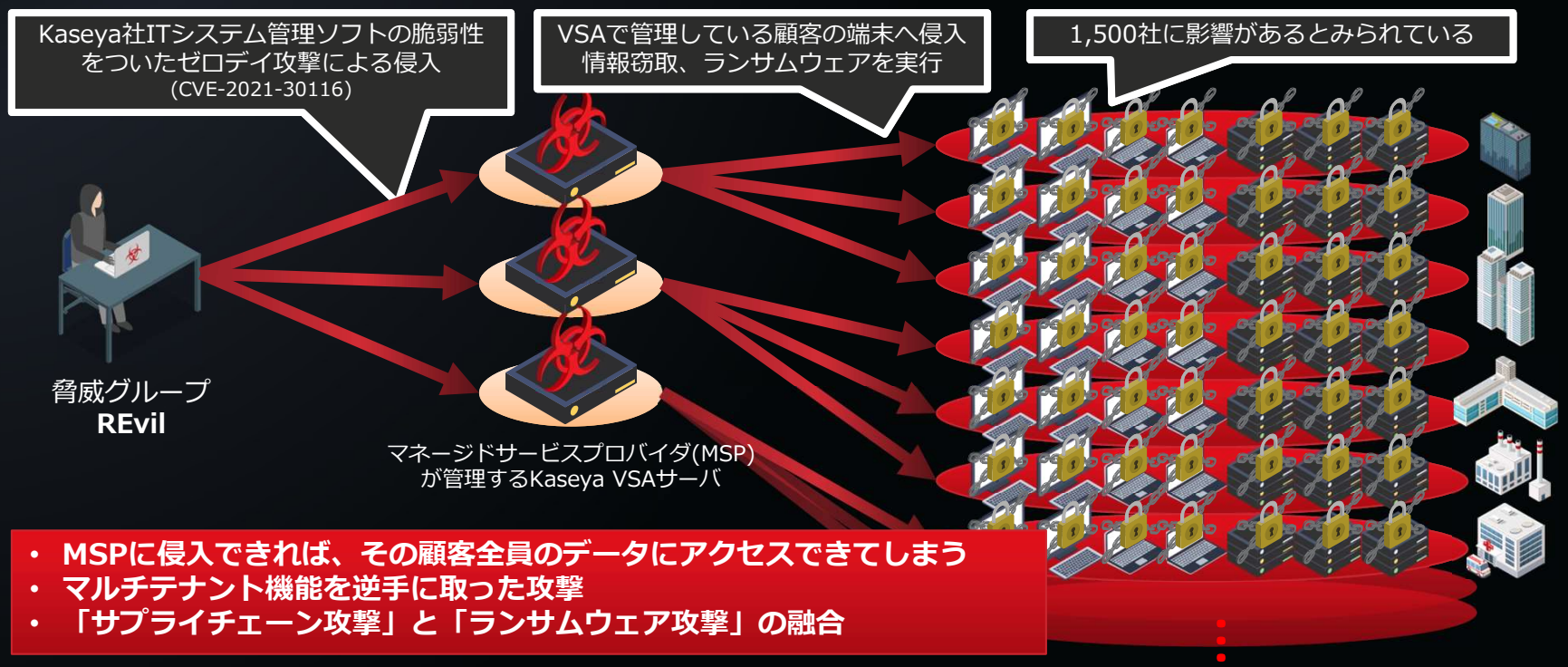
©2020 Cybereason Japan Corp. | All rights reserved

cybereason

侵入手段: サプライチェーン攻撃

ランサムウェア攻撃の侵入手段

管理ソフトを起点としたランサムウェア攻撃



- **MSPに侵入できれば、その顧客全員のデータにアクセスできてしまう**
- **マルチテナント機能を逆手に取った攻撃**
- **「サプライチェーン攻撃」と「ランサムウェア攻撃」の融合**

出典:
Kaseya Incident Overview & Technical Details
WIRED 深刻度を増すランサムウェア攻撃、今度はITサーヴィス企業の顧客もまとめて標的に

©2021 Cybereason Japan Corp. | All rights reserved

cybereason

組織に与えるランサムウェアのインパクト

32%
経営者が
解任または辞任

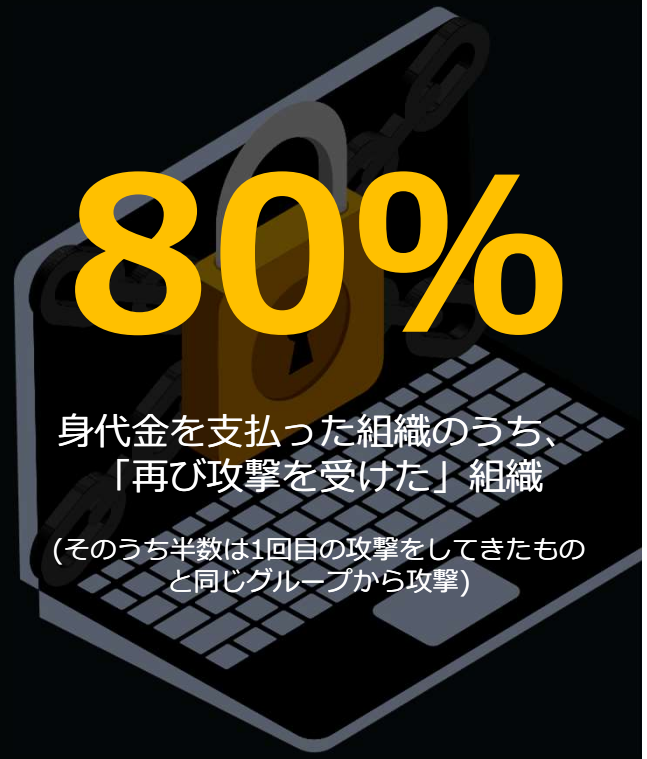
25%
営業停止

46%
身代金を支払い、
データを復号したが、
一部または全ての
データが破損

53%
ブランド
イメージ低下

66%
顕著な収益減

29%
雇用削減



80%

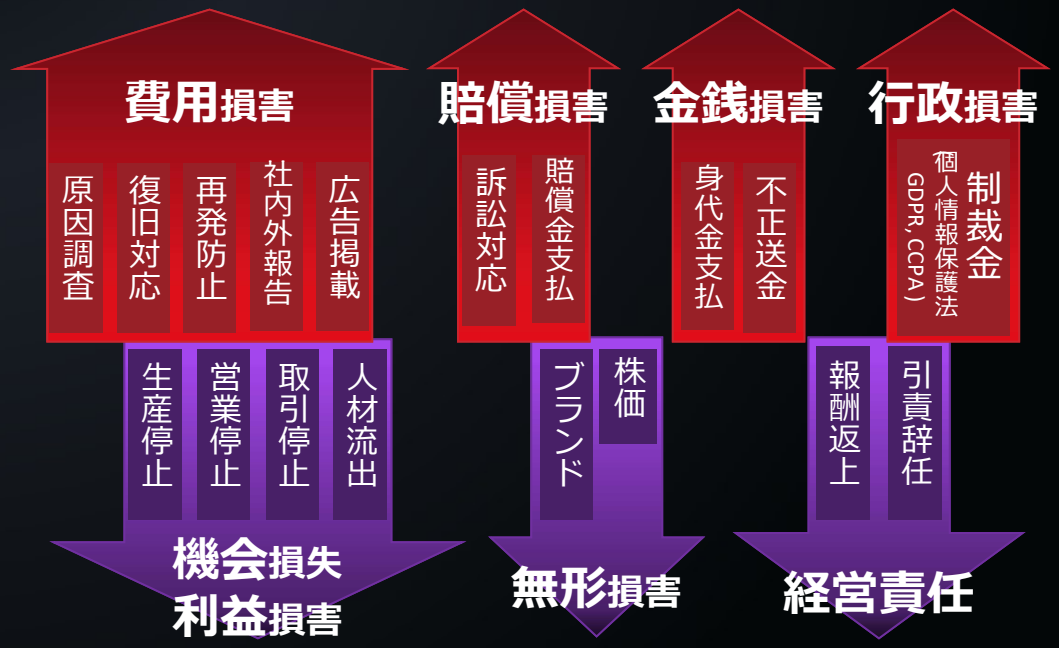
身代金を支払った組織のうち、
「再び攻撃を受けた」組織

(そのうち半数は1回目の攻撃をしてきたもの
と同じグループから攻撃)

サイバーリーズン:【グローバル調査結果】ランサムウェア ～ビジネスにもたらす真のコスト～

©2021 Cybereason Japan Corp. | All rights reserved

サイバー脅威は経営リスク



組織の事業継続に大きく影響する問題
IT/セキュリティ部門を超えた取り組みが不可欠

経済的損失額例

660万円
軽微なマルウェア感染

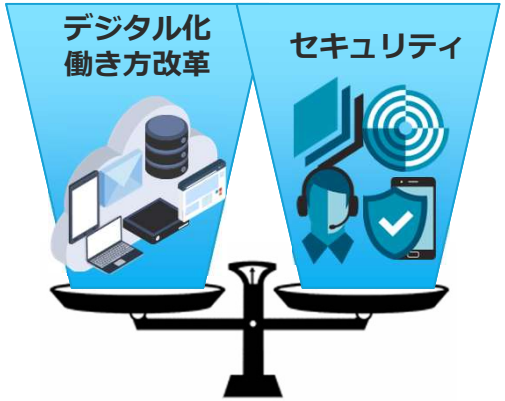
9,490万円
ECサイトからのクレジットカード情報などの漏えい

3億7,600万円
大規模なマルウェア感染

出典：JNSAインシデント損害額調査レポート2021
https://www.jnsa.org/result/incidentdamage/2021.html

©2021 Cybereason Japan Corp. | All rights reserved

攻める経営には攻めのセキュリティ対策を



セキュリティ ≠ コスト
セキュリティ ＝ 投資

サイバー脅威は組織の経営に大きく影響する問題

- DX、働き方の改革の推進とセキュリティ強化は表裏一体
- IT部門だけの問題ではなく、経営リスクとして対策に取り組む
- ビジネスのゴールを共有するだけでなく、全員が組織を守る意識を共有

セキュリティは事業継続に必要な投資

- 経営観点でサイバーリスクを評価 (リスク容認の決定)
- 平時、有事の運用が回るセキュリティ投資、人材の配置
- 有事において経営者、責任者が迅速な意思決定を行える組織

©2021 Cybereason Japan Corp. | All rights reserved

経営課題として取り組むべき
平時の備え

©2021 Cybereason Japan Corp. | All rights reserved

サイバーインシデントにおける

1. リスクアセスメントの実施

組織としてセキュリティリスクを「認識」し、「容認」するかどうか判断する

資産管理のリスク評価

- 守るべき情報資産を洗い出し(データ、ソフトウェア、物理的資産、サービス)
- 侵害された場合のインパクト算出　等

脅威、脆弱性の確認

- 盗難、盗聴、通信への侵入経路がないか
- 不適切なパスワード、パッチ未適用等がないか　等

IPA:組織的取り組みと 情報セキュリティマネジメントシステム
https://www.ipa.go.jp/files/000013299.pdf

©2021 Cybereason Japan Corp. | All rights reserved

2. インシデント対応手順の策定

インシデント対応フローを予め策定することが最重要

準備 → **検知/分析** → **封じ込め・根絶・復旧** → **事後対応**

準備
- 定期的なシステムのリスク評価
- 脅威検知/分析ツールの導入

検知/分析
- 影響範囲の把握(いつ、どこで、何が、どのように起こったのか)
- 脅威のランク付け
- 優先順位付け(トリアージ)

封じ込め・根絶・復旧
- 対処を決定するための基準確立
  - 対象の情報資産
  - 意思決定者
  - 報告フロー

事後対応
- 組織内部への報告
- 外部への報告(メディア、プレスリリース、監督官庁等)
- 再発防止、改善策

時間を短縮できるポイント

インシデント対応フローを予め確認し、策定することにより迅速な対応ができ、被害を最小限に抑えることができます

コンピュータセキュリティインシデント対応ガイド(NIST SP800 61)
https://www.ipa.go.jp/files/000025341.pdf

インシデントハンドリングマニュアル
https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf

©2021 Cybereason Japan Corp. | All rights reserved

cybereason

3. セキュリティの見直し・強化

既存のセキュリティ対策の見直し

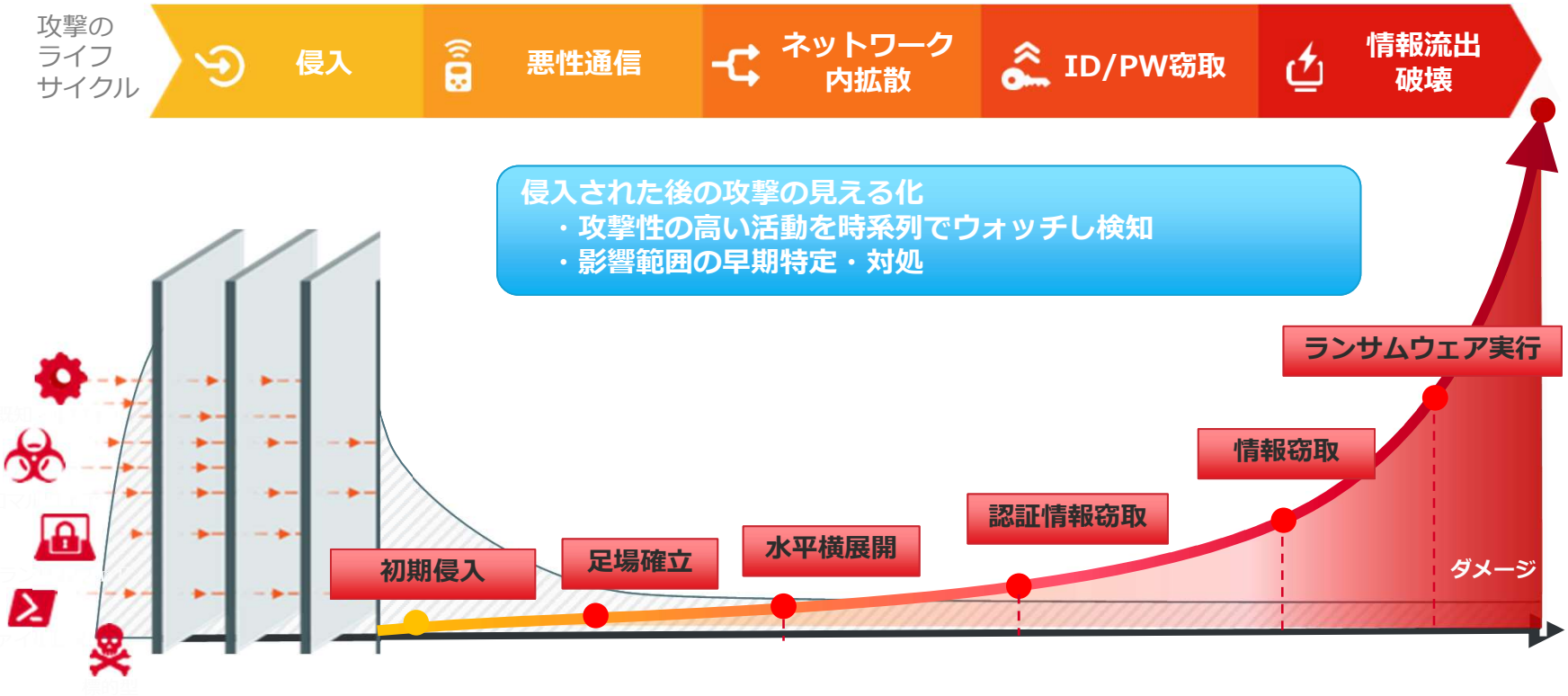
定期的なOS、パッチのアップデート
(脆弱性対策)

保護対象の端末、機器、ネットワークを監視できているか?
(テレワーク、クラウド含む)

最新の攻撃への対応ができるか?
(標的型攻撃、ランサムウェアなど)

©2021 Cybereason Japan Corp. | All rights reserved

4. 脅威の見える化



©2021 Cybereason Japan Corp. | All rights reserved

見える化に必要となる要素

複数端末にわたる相関解析	組織全体におよぶ標的型攻撃を解析し、
振る舞い分析	最先端攻撃(ファイルレス攻撃、ラテラルムーブメントなど)の振る舞いを分析を
リアルタイム検知	高速解析し、脅威を瞬時に検知することにより
攻撃の全体像を可視化	「いつどこで何が起こったか?」 を自動解析、可視化し素早く影響範囲を把握

見える化による 被害最小化

©2021 Cybereason Japan Corp. | All rights reserved

1 リスクアセスメントの実施

2 インシデント対応の策定

3 セキュリティの見直し・強化

4 脅威の見える化

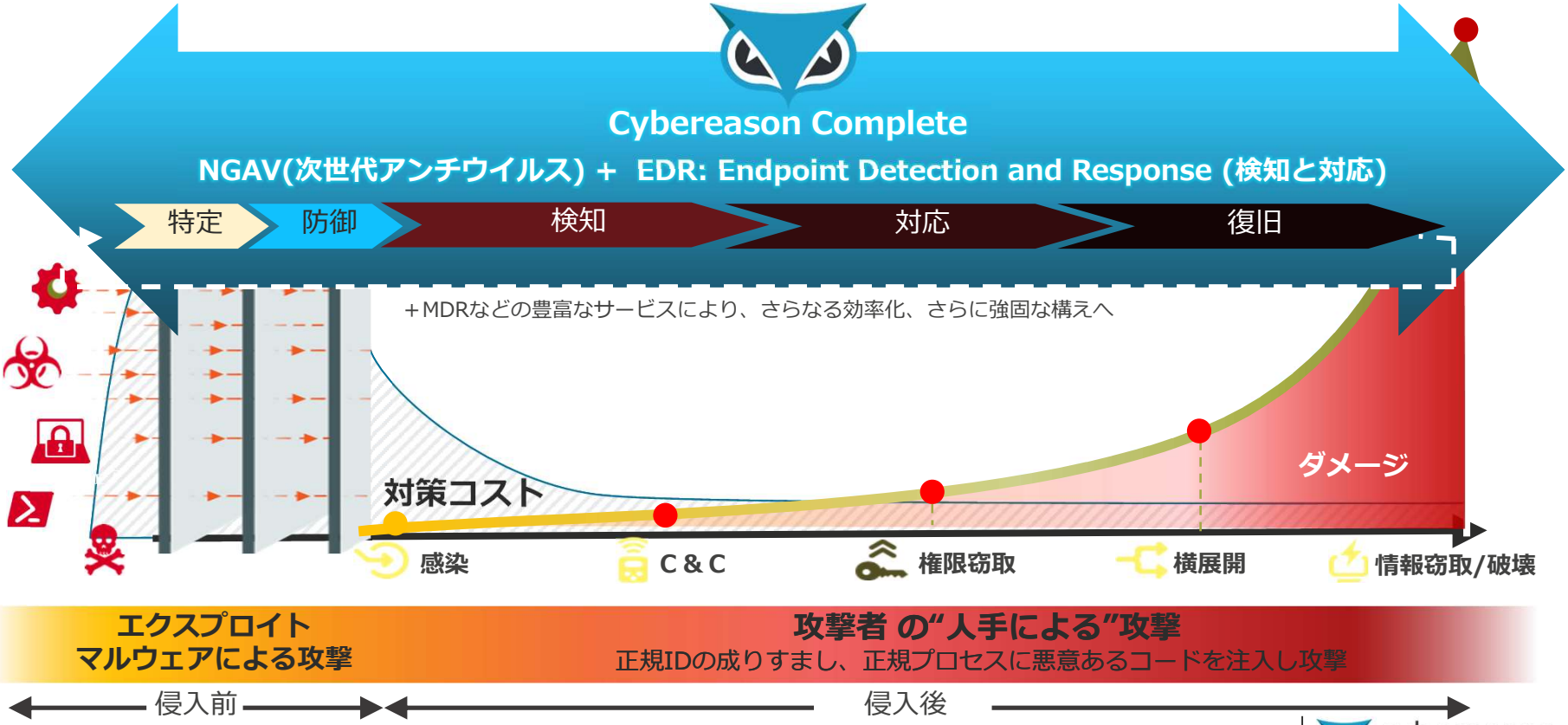
サイバーリーズンの
セキュリティ技術のご紹介

cybereason

©2021 Cybereason Japan Corp. | All rights reserved

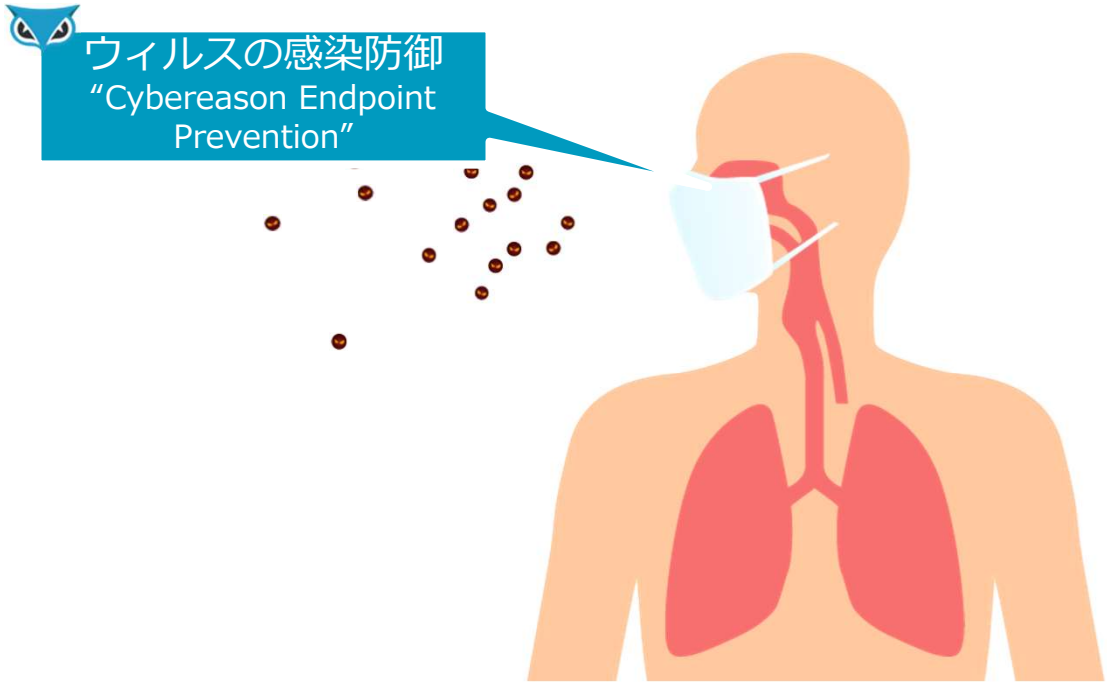
運用重視の実戦向きエンドポイント対策

- 効率よく攻撃を防御し、侵入後は攻撃者が１つでもミスをすれば検知/対応できる -



©2021 Cybereason Japan Corp. | All rights reserved

Cybereason製品/サービスイメージ



©2021 Cybereason Japan Corp. | All rights reserved

Cybereason Endpoint Prevention

次世代アンチウィルス 必須の6層

EDRで検知した攻撃のうち56%は自動対応可能な既知攻撃

Endpoint Preventionで多くの脅威を未然に排除し
EDRによる真の攻撃に対する解析、検知にリソースを集中

©2021 Cybereason Japan Corp. | All rights reserved

Cybereason Endpoint Preventionで最新の脅威を未然に阻止

Cybereasonによる ランサムウエアの継続的な調査

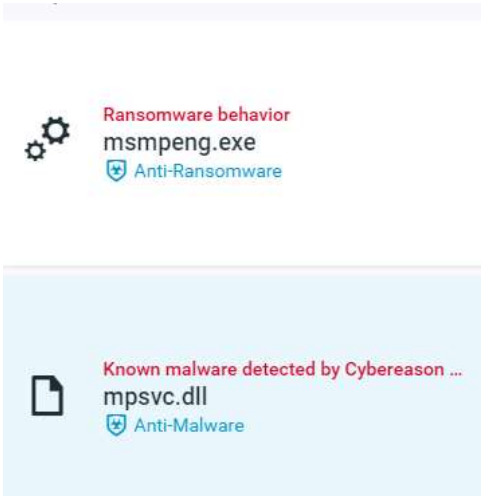
NGAVのアンチランサムウェア機能による「おとり」技術、ふるまい検知の向上

コロニアル・パイプライン社(DarkSide)、JBS社(REvil)のランサムウエア

NGAVのアンチランサムウェア機能で阻止

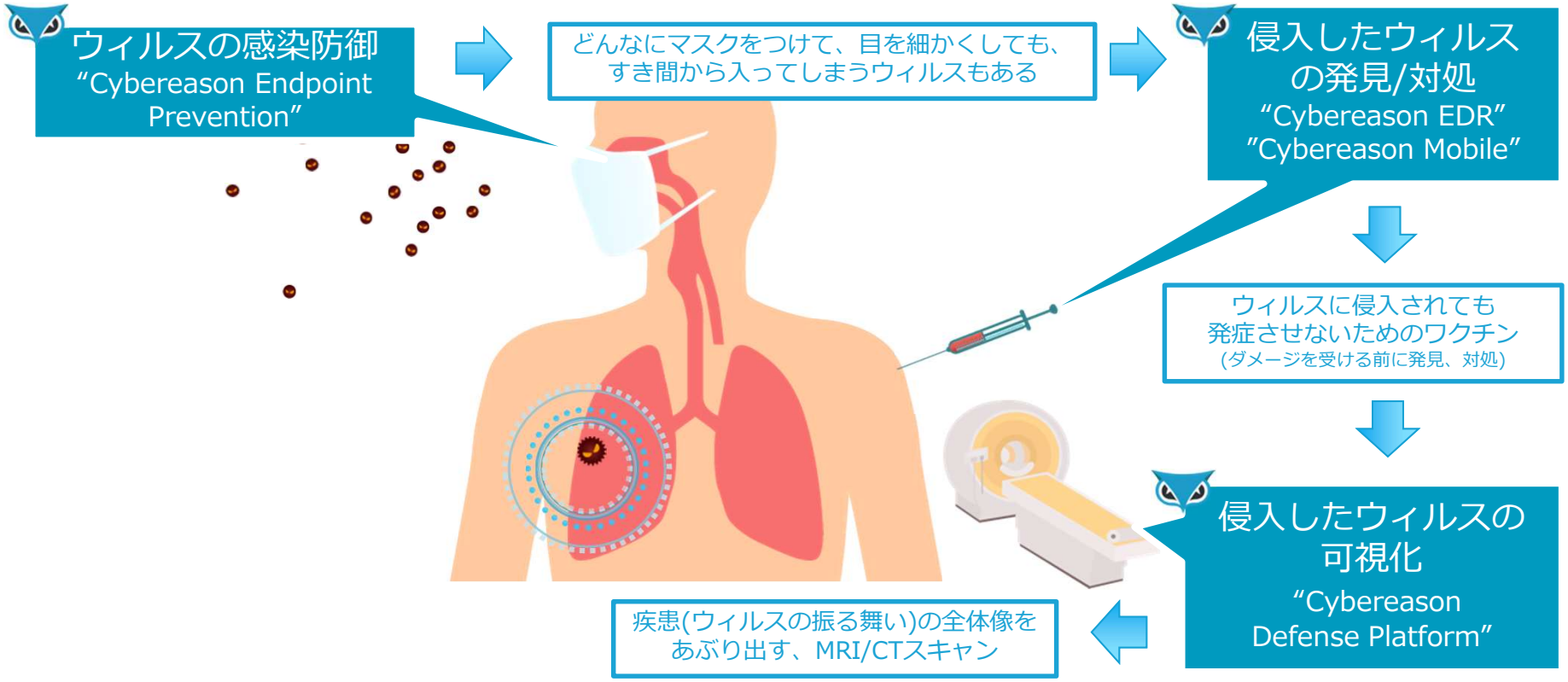
Kaseya VSAサプライチェーン攻撃で使用されたランサムウエア

NGAVのアンチランサムウェア機能で阻止



©2021 Cybereason Japan Corp. | All rights reserved

Cybereason製品/サービスイメージ



©2021 Cybereason Japan Corp. | All rights reserved

Cybereason EDR
「何が起きているか」を直感的に可視化

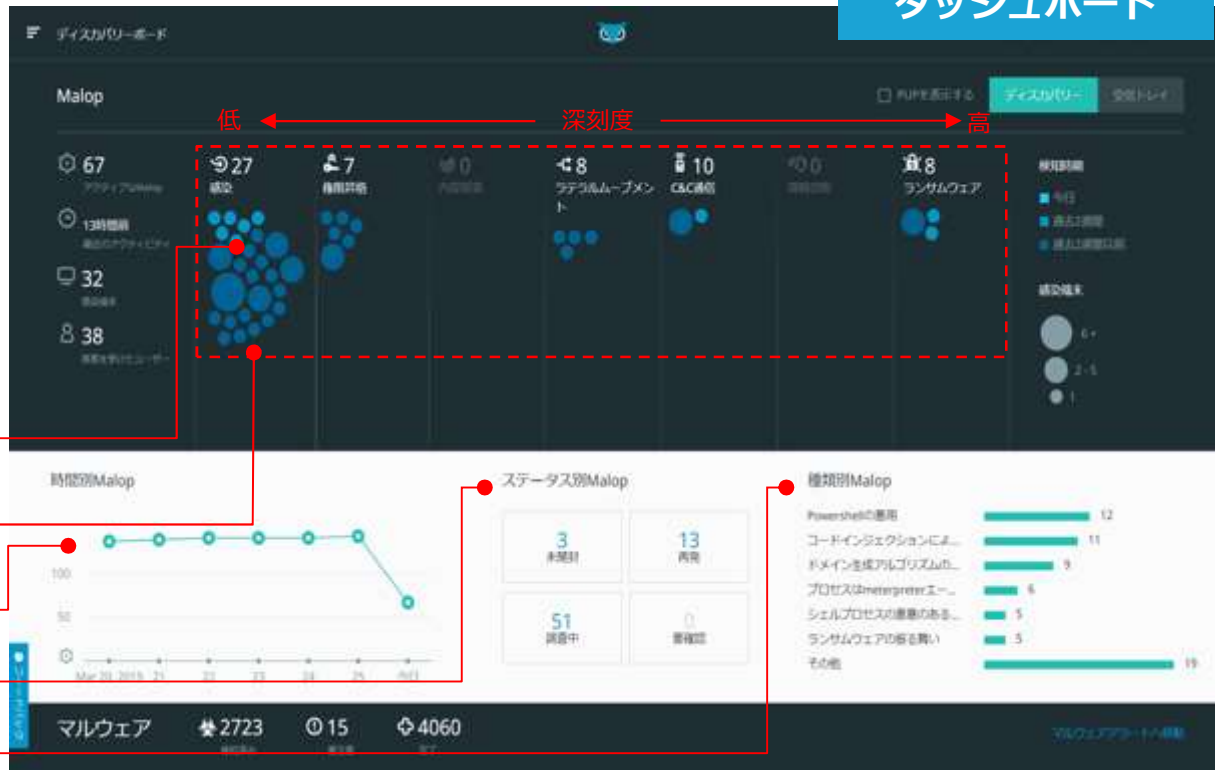
3 脅威から守るセキュリティの見直しと強化

4 脅威の見える化

ダッシュボード

朝出社したら最初に管理画面を開くことにしている。検知バブルがなければ、それで安心。すぐに画面を閉じている。

ある導入済みお客様の声



感染規模(バブルの大きさ)
感染してからの経過時間（バブルの色）

攻撃フェーズごとの感染状況

時間別統計

対応ステータス別統計

攻撃の種類別統計

©2021 Cybereason Japan Corp. | All rights reserved

Sunburst (SolarWinds)によるサプライチェーン攻撃

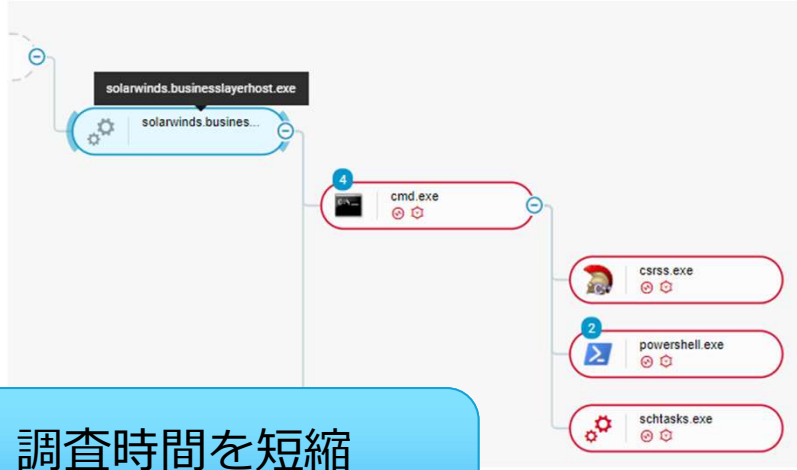
Cybereason EDRのふるまい検知機能で悪意のある行動を特定

3 脅威から守るセキュリティの見直しと強化

4 脅威の見える化

いつ、どの端末で何がどう起こったか
自動解析、イラストで図式化

プロセスの前後関係、
振る舞いの詳細を可視化

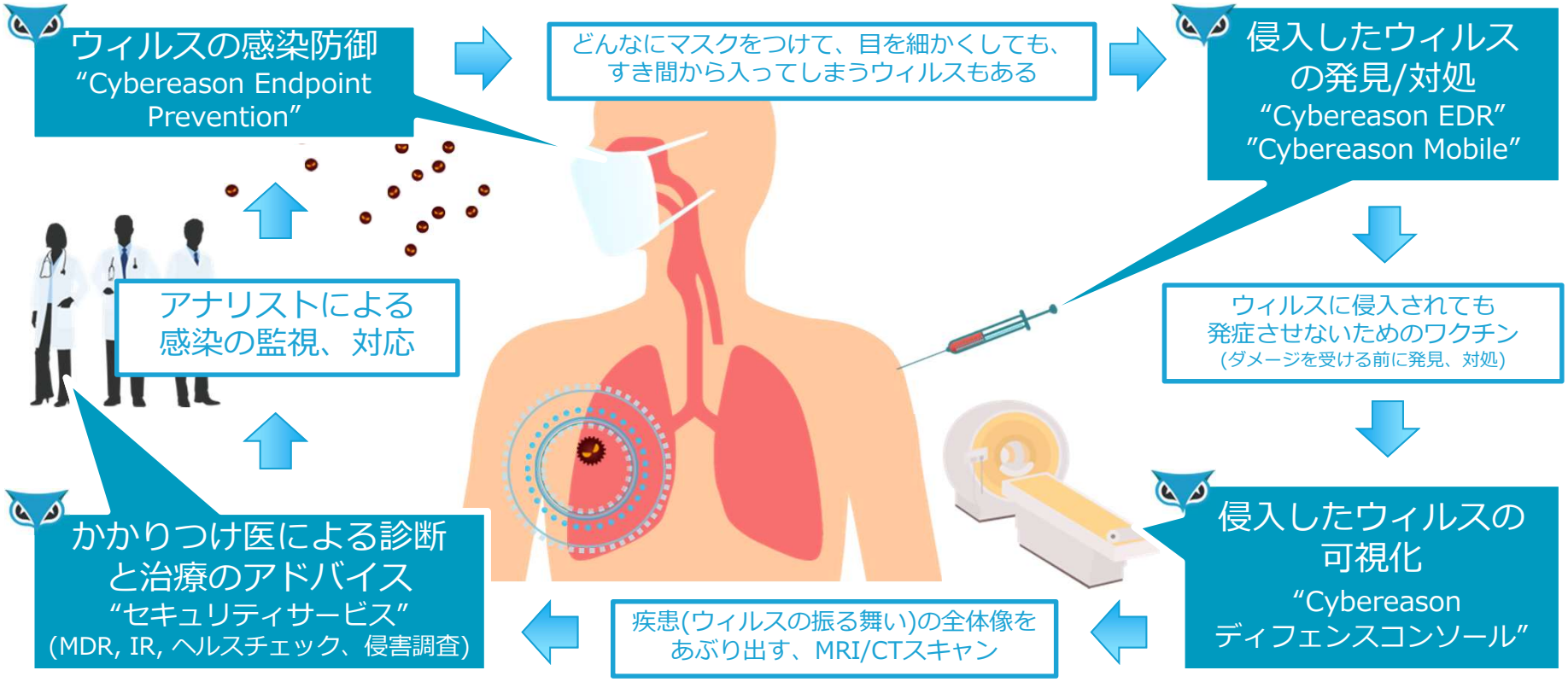


可視化によって分析、調査時間を短縮
すばやく対処し、被害を最小限に抑える

©2021 Cybereason Japan Corp. | All rights reserved

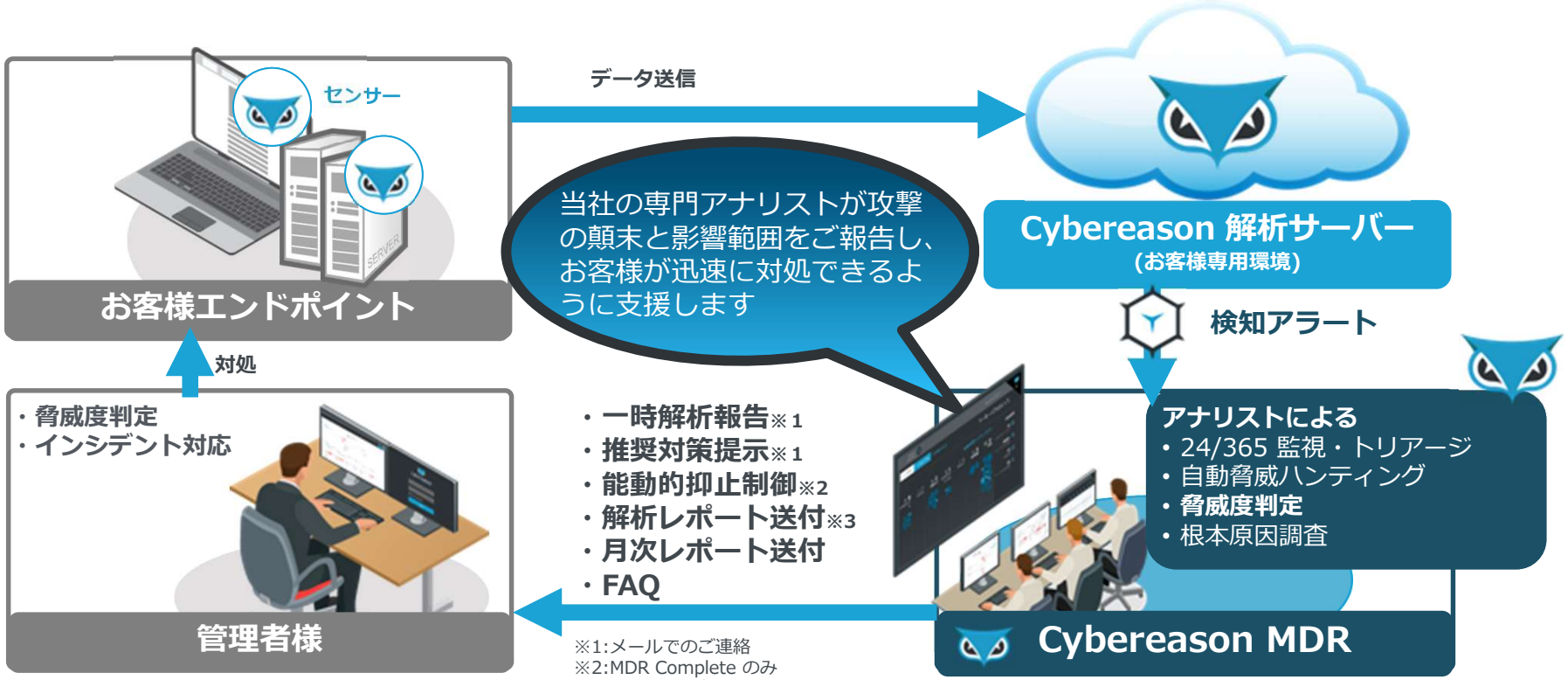
cybereason

Cybereason製品/サービスイメージ



©2021 Cybereason Japan Corp. | All rights reserved

Cybereason MDR (Managed Detection and Response = 脅威検知と対応のマネージドサービス)
専門アナリストによるエンドポイント監視・解析サービス



※1:メールでのご連絡
※2:MDR Complete のみ
※3:脅威度「緊急」の場合のみ

©2021 Cybereason Japan Corp. | All rights reserved

定期的な社内環境の身体検査
(セキュリティ ヘルスチェック サービス)

1 リスクアセスメントの実施
3 セキュリティの見直し・強化

情報漏洩につながりかねないアプリの利用やグローバルIPがアサインされている端末が見つかり改善につながりました。

お客様の声

ヘルスチェックでわかる組織のセキュリティ習慣

- グローバルIPが付与されている端末
- 長期間パスワードを変更していない※
- セキュリティパッチの適用有無※
- サポートが終了したOS
- セキュリティソフトが動作していない端末
- 管理者権限アカウントによるリモート接続
- リムーバブルメディアの使用

※Windowsのみ

専門家によるセキュリティ対策のチェックを受け、レポートとして出せることは**心強く、有益**です。

センサーインストール (1週間)

調査 (1週間)

レポート (1週間)

組織内の安全性 運用体制の見直し

セキュリティ強化

対象: Windows, Mac, Linux

©2021 Cybereason Japan Corp. | All rights reserved

1 リスクアセスメントの実施

3 セキュリティの見直し・強化

Compromised Assessment /侵害調査

システムに対する侵害の証跡を調査/復旧支援

絶え間なくセキュリティ対策を改善しなければならない中、Compromised Assessment(侵害調査サービス)では、短時間で組織が攻撃を受けているかを判断。セキュリティ対策と運用の抜け穴を特定し、改善するための推奨事項を提示します。

侵入を許した侵害の発見

高度な攻撃による侵害の発見

- ✓ すり抜けたマルウェア
- ✓ 正規アカウントのなりすまし
- ✓ 隠されたバックドア

有事の際の影響分析・復旧プラン

有事の際は影響を分析し、復旧プランの策定をご支援。

セキュリティ対策・運用の盲点把握

攻撃の全フェーズにおける侵入経路、攻撃の流れを解析し、セキュリティ侵害の範囲を特定、抜け穴を根絶。

効率的なセキュリティ対策へ

増加しつづけるセキュリティ対策コストの最適化をおこなえるよう、セキュリティ対策と運用に対する改善策を提示。

実施スケジュール例(合計8週間)

2週間	2週間	2週間	2週間
事前準備	データ収集	ハンティング	報告

©2021 Cybereason Japan Corp. | All rights reserved

Cybereason IR(インシデント対応)サービス

サイバーリーズンのグローバルIRチームがワンストップで
インシデント発生時の初動から終息までに必要なインシデント対応の支援を行います。

IR実績豊富な専門部隊

CybereasonのIR専門部隊が最前線でお客様のインシデントハンドリング対応を支援します

インシデント対応における効果的な調査プロセス

徹底的な侵害調査を実施。侵害調査ライフサイクルに基づいた網羅的な影響範囲の特定を行い、封じ込め、復旧対応を支援します。

IRテクノロジーによる調査の効率化

サイバーリーズンのDefenseプラットフォームおよびIR自動化ツールを最大限に用いて調査の時間を大幅に短縮。脅威範囲を網羅的に調査し、特定します。

迅速なグローバル対応

IR専門部隊はグローバル規模。バイリンガル人材により日本と海外拠点の境界なくお客様の迅速なインシデント対応が可能です。

IRリテイナー

インシデント対応に必要な時間を事前に購入いただくことにより、実際のインシデント発生時に、インシデント対応に関するサービス契約手続き等で時間を損失することなく、迅速にインシデント対応を実施いただくことができます。
※インシデント対応に使用しなかったリテイナー時間は他のサービスに振り替え可能

©2021 Cybereason Japan Corp. | All rights reserved

Cybereasonの優位点（技術面）

1

１エージェントで防御-検知-対応-復旧までを全カバー

- ✓ １エージェントで既知、未知、ファイルレス、ランサムウェアのブロックから、侵入後の悪意ある振る舞いに対する検知、対応、復旧までをカバー
- ✓ 次世代アンチウイルスによる防御の自動化で、EDRに着弾するアラートを低減し、運用効率のよいセキュリティを提供

2

攻撃の全体像をリアルアイムに可視化

- ✓ １つの攻撃の侵入から現在までをリアルタイムに解析
- ✓ 侵入ポイント、根本原因、影響を受けた端末、影響を受けたユーザーを把握、攻撃の流れを自動分析、時系列で表示
- ✓ 短時間で攻撃の全体像を把握可能
- ✓ 影響範囲を調査コンソールから深堀でき、検知・分析からレスポンスまでの時間を短縮

3

攻撃された複数台の端末を遠隔から一度に対応可能

- ✓ 影響を受けた端末に対して、遠隔から一度に端末の隔離、プロセス停止、ファイルの隔離、レジストリの削除をおこなうことが可能。
- ✓ インシデントレスポンスにおいて対応スピードが重視される中で、同じ攻撃キャンペーンごとに、影響範囲を即座に把握し、同じ攻撃を受けた端末すべてに対して同時に対応することにより被害を最小化。

©2021 Cybereason Japan Corp. | All rights reserved

Cybereasonの優位点（運用面）

1

業務端末に影響しない

- ✓ CybereasonのEDR機能はユーザーモードで動作するためOSのアップデートのたびに影響を受けにくい。
  ブルースクリーンを引き起こさず、かつ業務アプリケーションにも影響を及ぼさない設計。
- ✓ 低CPU使用率、低メモリ使用量、低ネットワーク負荷。VDIも可。

2

日本語画面 日本語レポート

- ✓ インシデントの際には矢継ぎ早に対策をおこなう必要あり。
  日本の組織においては、画面と自動生成レポートも日本語で提供されることは対応スピードの観点からも重要。
- ✓ 管理ユーザーごとに、日本語と英語の切り替えが可能なため、状況/事象を即座に正確に把握可能。

3

日本法人による強力なサポート体制

- ✓ MDR(脅威監視対応サービス)によるセキュリティの専門家による監視/解析/報告（インシデントレポート、月次レポートあり）
- ✓ お客様担当のCS/カスタマー・サクセスによる導入/運用支援（製品トレーニング/定期ミーティング/運用に係る全般的なご相談窓口）

©2021 Cybereason Japan Corp. | All rights reserved

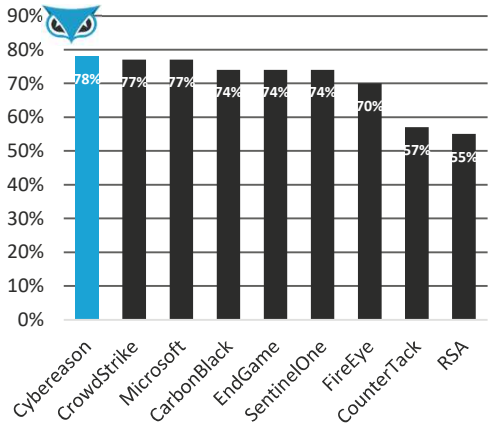
MITRE ATT&CK-APT3評価結果

Forrester提供のスクリプトcoverage.pyより作成
参照： https://github.com/joshzelonis/attack-eval-scoring

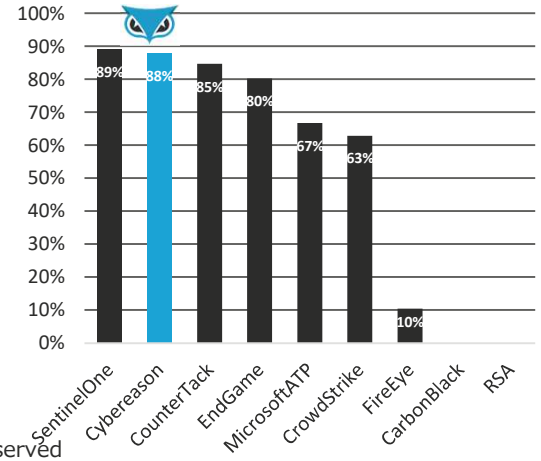
米国政府の支援を受けている非営利の研究団体MITREによるATP3攻撃テクニックを用いた完全に公平な評価結果に、Forresterが透明性の高い評価スクリプトを提供。その結果、以下のCybereasonの圧倒的な優位性が認められた。

Cybereasonは製品単体だけでも最高峰のカバレッジ

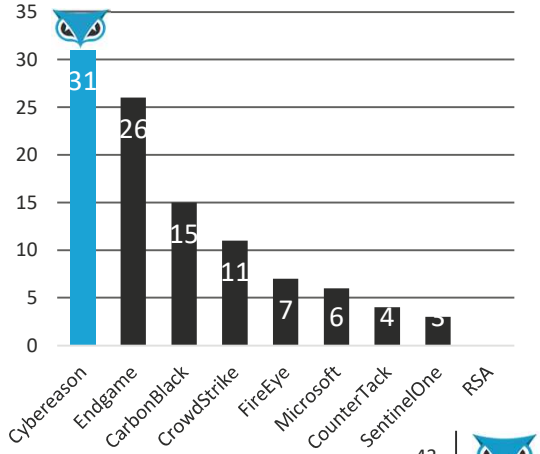
最高のカバレッジ（データ収集能力）



優秀な相関解析能力（イベントのつながり情報）



最高のリアルタイム検知率



検知遅延ゼロ

設定変更ゼロ

©2021 Cybereason Japan Corp. | All rights reserved

cybereason

経営課題として取り組むべき、サイバー脅威対策とインシデント対応

インシデント対応は時間が勝負
平時の備えが重要

		サイバーリーズンがご提供できるソリューション
1	リスクアセスメントの実施	リスク評価 脅威、脆弱性の確認
2	インシデント対応の策定	準備 封じ込め/根絶/復旧 検知/分析 事後対応
3	セキュリティ見直し・強化	保護対象端末の監視 最新の攻撃に対応
4	脅威の見える化	複数端末にわたる相関解析 振る舞い分析 攻撃の全体像を可視化

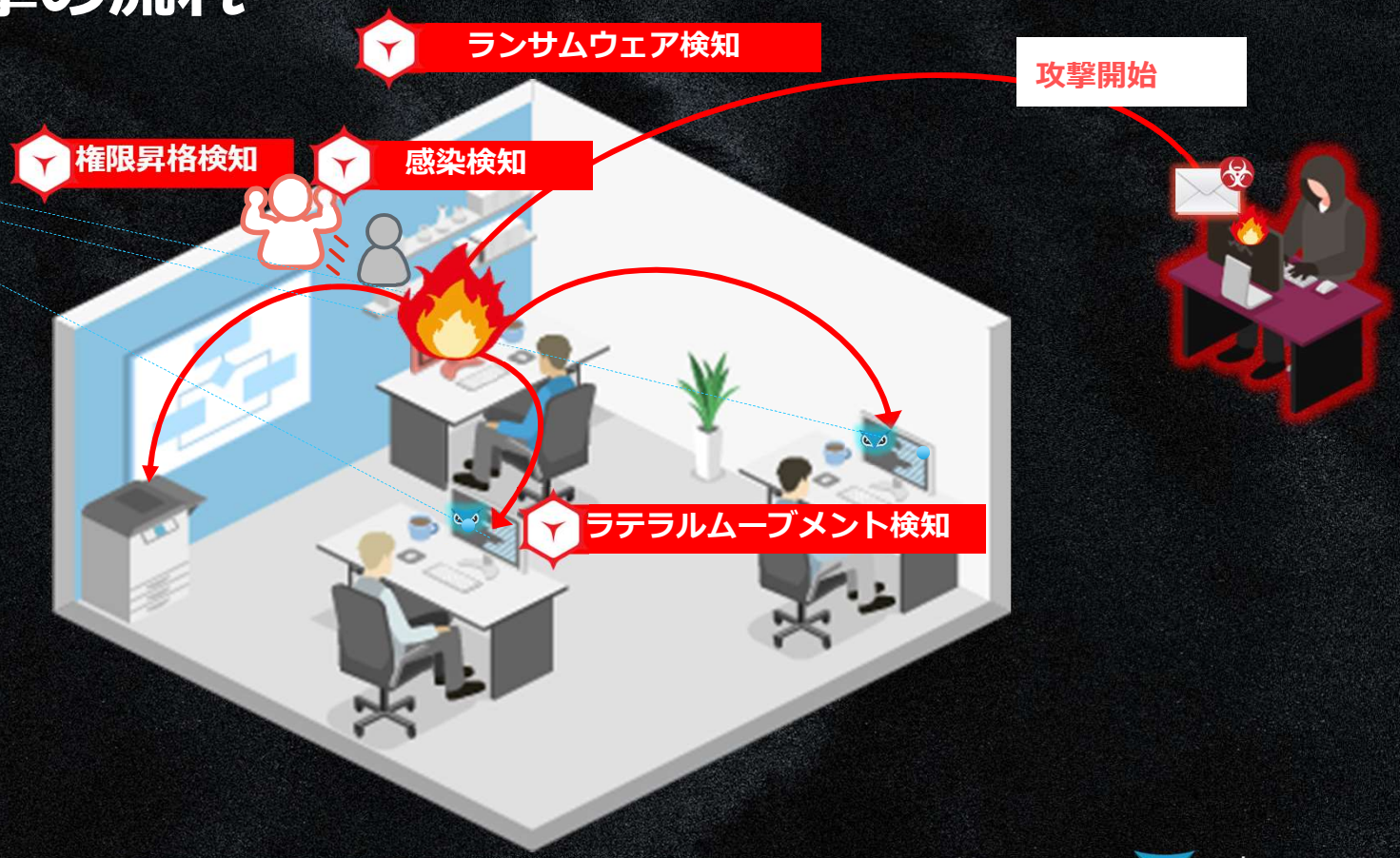
©2021 Cybereason Japan Corp. | All rights reserved

デモンストレーション実施

©2021 Cybereason Japan Corp. | All rights reserved

本日の攻撃の流れ

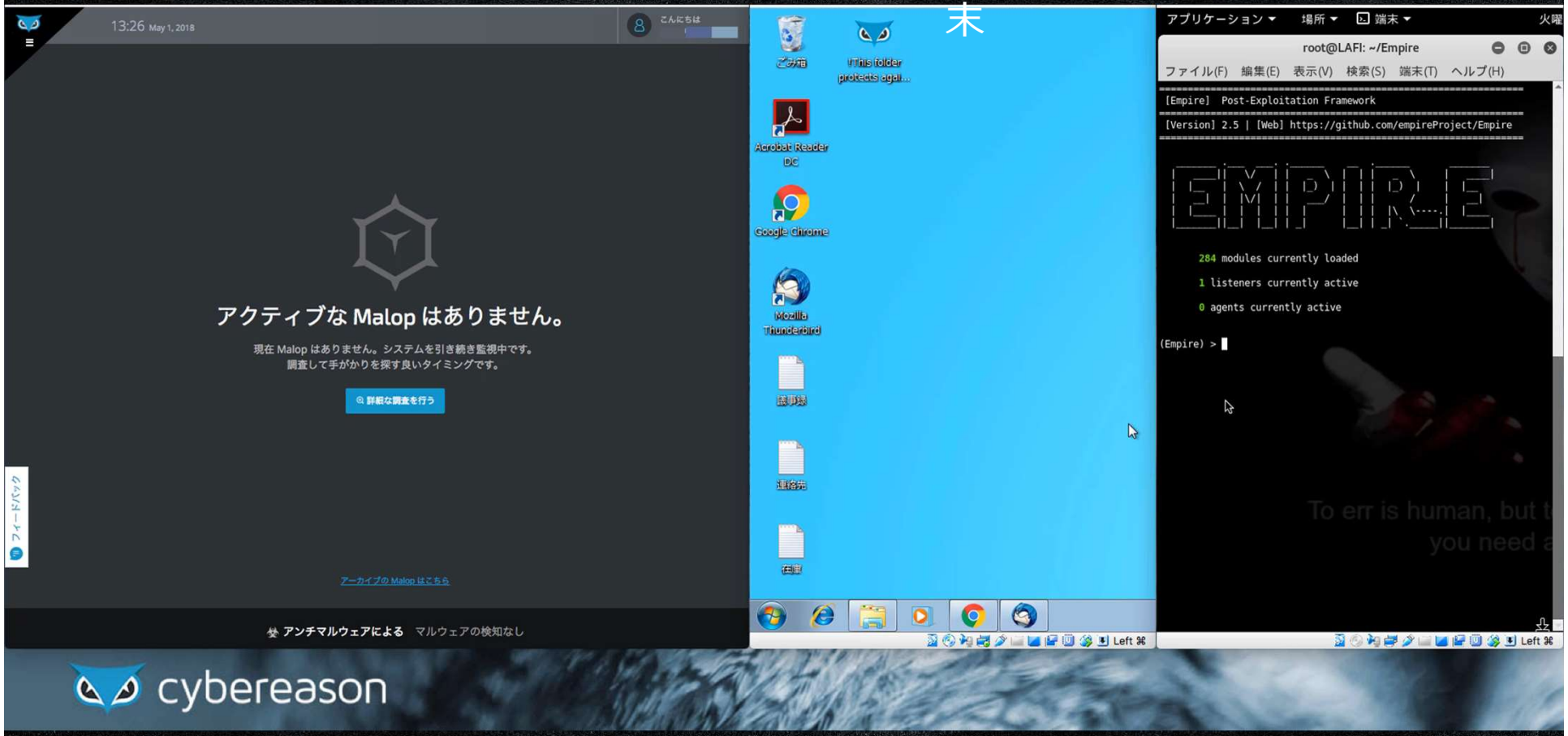
Cybereason
検知サーバー



©2020 Cybereason Japan Corp. All rights reserved.

cybereason

Cybereason管理画面　被害者端末　攻撃者



cybereason

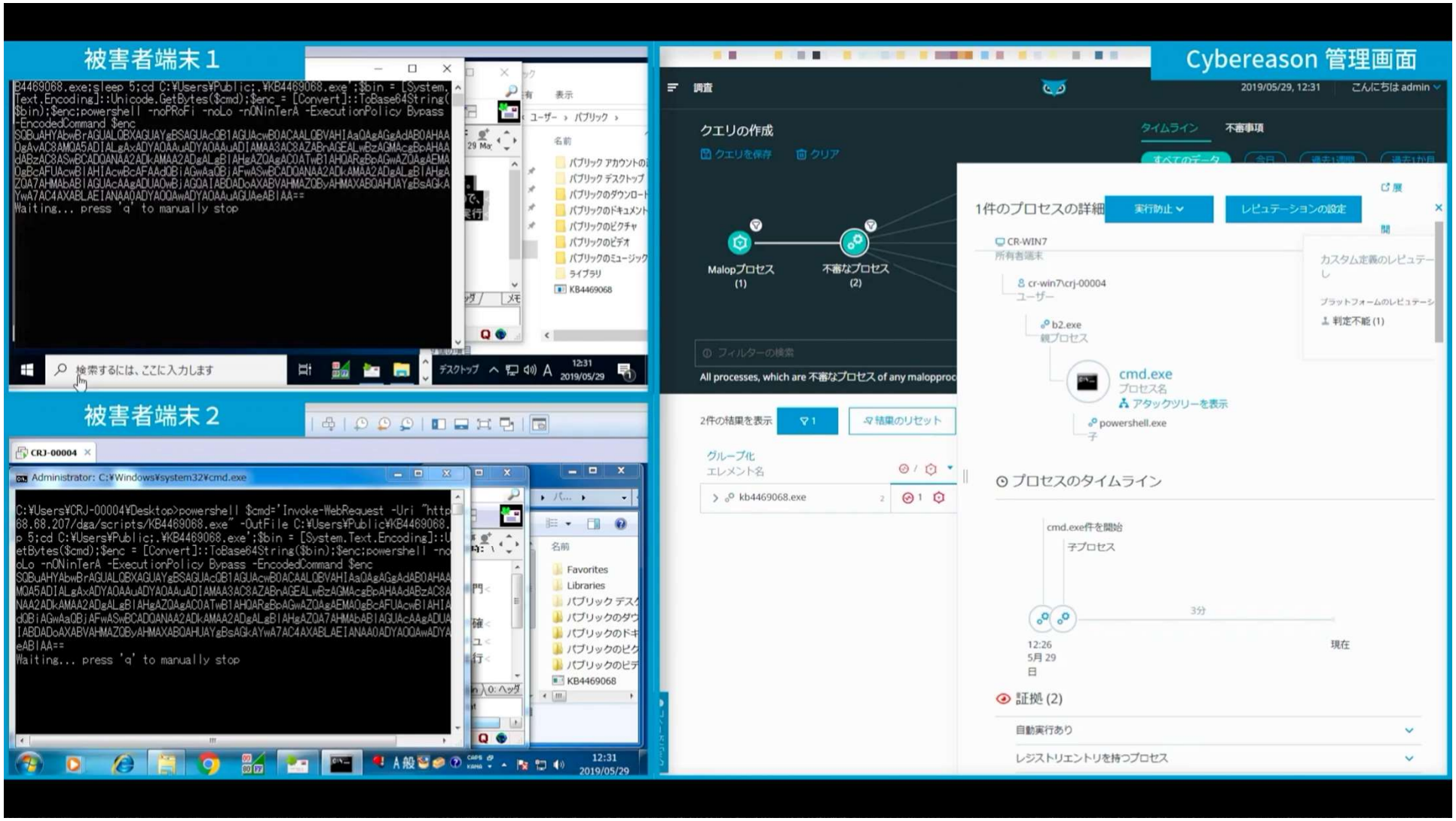
©2020 Cybereason Japan Corp. All rights reserved.
cybereason

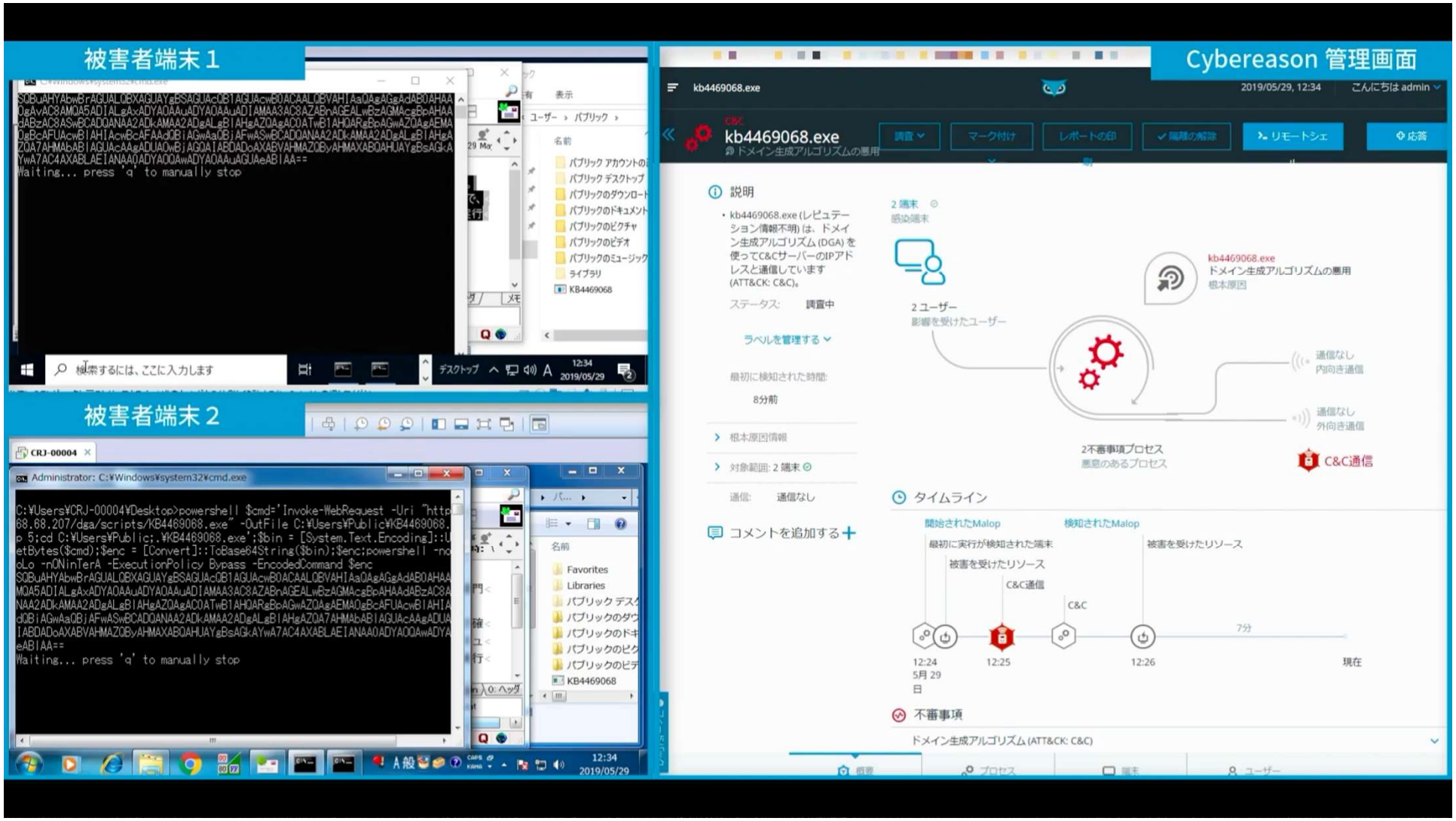
検知後に対応可能な処理

侵入された端末に対し、遠隔からまとめて
「封じ込め、根絶・復旧」

- 端末隔離・復旧
- マルウェア隔離
- プロセス停止
- レジストリ削除

©2020 Cybereason Japan Corp. All rights reserved.
cybereason


被害者端末 1
Waiting... press 'q' to manually stop
被害者端末 2
Administrator: C:¥Windows¥system32¥cmd.exe
Waiting... press 'q' to manually stop
Cybereason 管理画面
調査
クエリの作成
クエリを保存
クリア
Malopプロセス
(1)
不審なプロセス
(2)
All processes, which are 不審なプロセス of any malopproc
2件の結果を表示
結果のリセット
グループ化
エレメント名
kb4469068.exe
1件のプロセスの詳細
実行防止
レピュテーションの設定
CR-WIN7
所有者端末
cr-win7\crj-00004
ユーザー
b2.exe
親プロセス
cmd.exe
プロセス名
アタックツリーを表示
powershell.exe
子
プロセスのタイムライン
cmd.exe件を開始
子プロセス
3分
12:26
5月 29
日
現在
証拠 (2)
自動実行あり
レジストリエントリを持つプロセス
タイムライン
不審事項
2019/05/29, 12:31
こんにちは admin


被害者端末１
Waiting... press 'q' to manually stop
被害者端末２
Administrator: C:¥Windows¥system32¥cmd.exe
Waiting... press 'q' to manually stop
Cybereason 管理画面
kb4469068.exe
2019/05/29, 12:34
こんにちは admin
C&C
kb4469068.exe
ドメイン生成アルゴリズムの悪用
調査
マーク付け
レポートの印
隔離の解除
リモートシェ
応答
説明
kb4469068.exe (レピュテーション情報不明) は、ドメイン生成アルゴリズム (DGA) を使ってC&Cサーバーの IPアドレスと通信しています (ATT&CK: C&C)。
ステータス: 調査中
ラベルを管理する
最初に検知された時間:
8分前
根本原因情報
対象範囲: 2 端末
通信: 通信なし
コメントを追加する
2 端末
感染端末
2 ユーザー
影響を受けたユーザー
kb4469068.exe
ドメイン生成アルゴリズムの悪用
根本原因
通信なし
内向き通信
通信なし
外向き通信
2不審事項プロセス
悪意のあるプロセス
C&C通信
タイムライン
開始されたMalop
検知されたMalop
最初に実行が検知された端末
被害を受けたリソース
被害を受けたリソース
C&C通信
C&C
7分
12:24
5月 29
日
12:25
12:26
現在
不審事項
ドメイン生成アルゴリズム (ATT&CK: C&C)

ENTER IF YOU DARE

cybereason

サイバーリーズン・ジャパン株式会社
www.cybereason.co.jp