侵入前の攻撃の防御、侵入後の検知/対応を実現する

No.1 エンドポイントセキュリティ
Cybereason NGAV
Cybereason EDR

202１年6月

サイバーリーズン・ジャパン株式会社

cybereason

©2020 Cybereason Japan Corp. | All rights reserved

Cybereasonとは

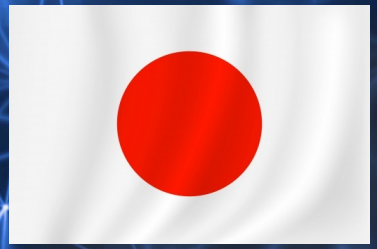
イスラエルの軍事技術から生まれたAIによるエンドポイント・セキュリティ対策を提供

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



資本金・品質

日系企業が株式の約3割を保有し筆頭株主
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700名 ※2020年10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120名 ※2020年10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 a1.100 NETWORKWORLD CYBER SECURITY EXCELLENCE AWARDS WINNER 2017
WSJ InformationWeek DARKReading BostInno WIRED CTECH Boston Business Journal

国内エンドポイントセキュリティNo.1

EPP

NEW

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) 2018年

2018 EPP No.1

出典：株式会社ミック経済研究所「エンドポイント型脅威対策編 2019年度版 サイバーセキュリティソリューション市場の現状と将来展望」

EDR／NGAV市場：
ベンダー別売上額シェア

2017
2018 EDR/NGAV No.1

出典：株式会社アイ・ティ・アール、2020年3月発行、「ITR Market View：エンドポイント／無害化／インターネット分離／CASB市場2020」

EDR

NEW

EDR市場占有率

2018
2019 EDR No.1

出典： 株式会社富士キメラ総研、2020年11月17日発行「2020 ネットワークセキュリティビジネス調査総覧《市場編》」

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) 2018年

2017
2018 EDR No.1

出典：株式会社ミック経済研究所「エンドポイント型脅威対策編 2019年度版 サイバーセキュリティソリューション市場の現状と将来展望」

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 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、2019年10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2019」

©2020 Cybereason Japan Corp. | All rights reserved

TRUSTED BY (公開を許諾いただいたお客様のみ)

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
- Beam SUNTORY
- 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)

- Belc ベルク
- 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
- NICHIBAN
- 日本マクドナルド株式会社
- nishikawa
- 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

©2020 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/

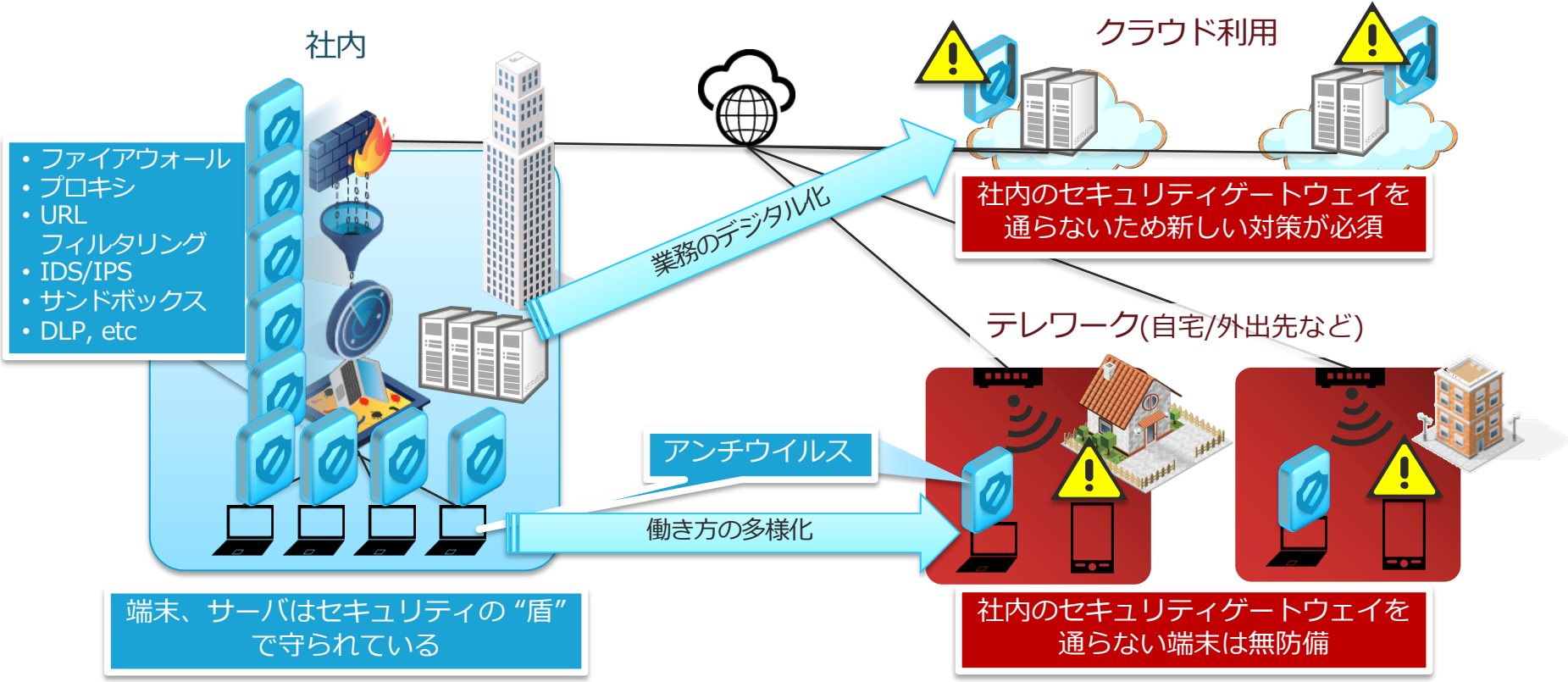
©2020 Cybereason Japan Corp. | All rights reserved

ニューノーマル時代で変化する
セキュリティ環境、対策

cybereason

©2020 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



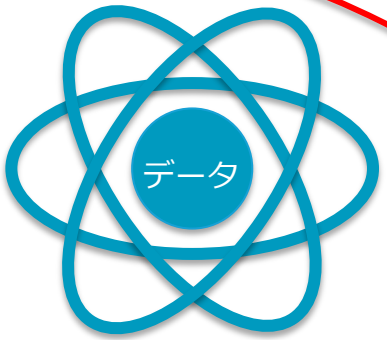
©2020 Cybereason Japan Corp. | All rights reserved

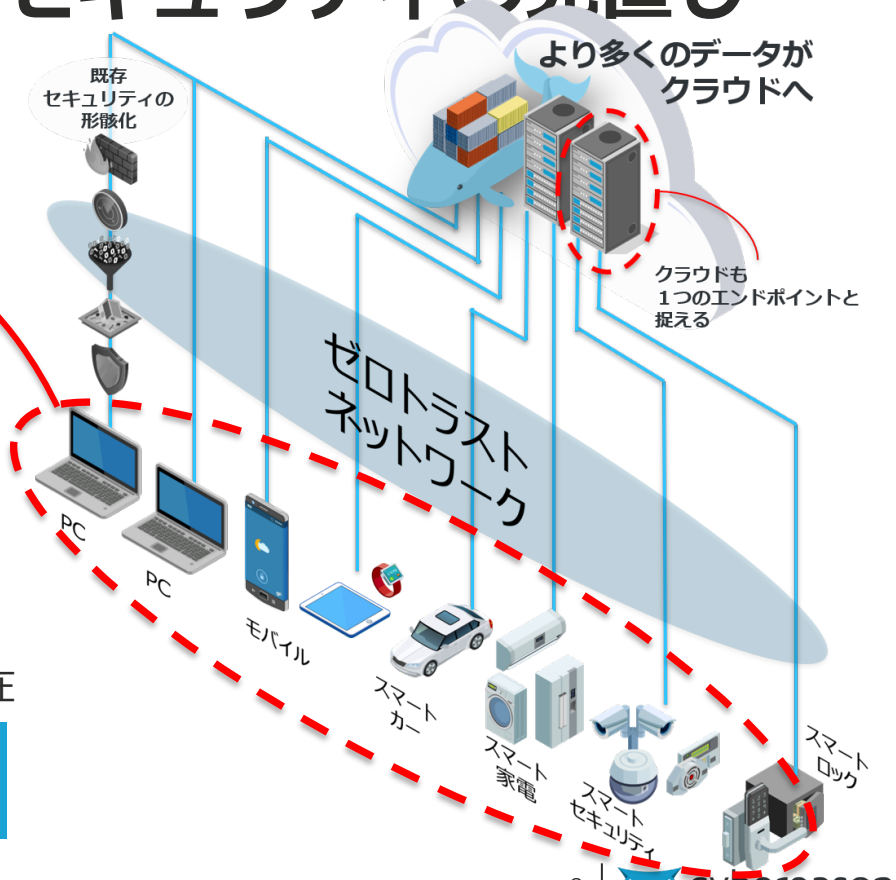
cybereason

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

©2020 Cybereason Japan Corp. | All rights reserved

サイバー脅威の現状
攻撃手法の変化

cybereason

©2020 Cybereason Japan Corp. | All rights reserved

大手企業へのサイバー攻撃相次ぐ

サイバー攻撃で関係者ら1万2
新聞社

2020.05.13 2020.05.13

NIKKEI

サイバー攻撃による社員

当社グループ従業員のパソコン１台が５月８日
一部グループ会社・団体の役員および社員・OB
員の氏名など１万 2514 人分の個人情報が流出し

流出したのは日経社内のネットワーク端末を使
レスが含まれていました。取材で得た情報や日経読者・顧客の皆様に関するデータは流出しておりません。

当社はマルウェア検知システムを導入するなど情報セキュリティー対策を講じてきましたが、当該従業員が受信したメール添付のファイルに新種のウイルスが仕込まれていたため異常の検知が遅れてしまいました。サイバー攻撃で情報が流出したとみています。

不正な送信はすでに遮断しており、新聞や電子版製作などのシステムに問題はありません。情報が流出した関係者の皆様に連絡し注意をお願いするとともに、日経グループのセキュリティー対策

日本経済新聞

トップ 速報 マネー 経済・金融 政治 ビジネス マーケット テ

新型ミサイル性能漏えいか　三菱電
衛省が全容調査

2020/5/20 18:59

保存 ま

三菱電機へのサイバー攻撃で、防衛省が研究を進める
性能に関する情報が、同社から漏えいした疑いがある
かった。防衛省はサイバー攻撃の全容について調査を

菅義偉官房長官は同日、記者会見で「流出した可能性
上の影響を精査中だ。事案の詳細についての答えは控

関係者によると、漏えいした可能性があるのは
際、企業側に求めた性能などの情報。開発過程
する「秘密」ではないが、慎重な取り扱いが必

ホンダのシステム障害、原因は産業制御システムを狙うランサムウェア「Ekans」か

セキュリティ企業によると、ホンダで発生したシステム障害は、産業制御システム（ICS）を狙うランサムウェア「Ekans」（別名「Snake」）が原因だった可能性がある。

2020年06月11日 09時45分 公開　[鈴木聖子，ITmedia]

印刷 15 Share B! 1

この記事は**会員限定**です。会員登録すると全てご覧いただけます。

本田技研工業（以下、ホンダ）の社内で発生したシステム障害に関連して、セキュリティ企業のMalwarebytesは2020年6月9日、「Ekans」（別名「Snake」）と呼ばれるランサムウェアが攻撃に使われた可能性があると伝えた。

報道によると、ホンダはサイバー攻撃を受けて6月8日に社内でシステム障害が発生し、工場の生産を停止した。米国法人の公式Twitterによれば、カスタマーサービスや金融サービスにも障害が発生して利用できなくなっている。

日本経済新聞

朝刊・夕刊 ストーリー My

トップ 速報 マネー 経済・金融 政治 ビジネス マーケット テクノロジー 国際 オピニオン スポーツ 社会

カプコン、不正アクセスで個人情報最大35万件流出

ネット・IT 関西 大阪
2020/11/16 16:38

保存 共有 印刷 その他

©2019 Cybereason Japan Corp. All rights reserved.

もはやサイバーセキュリティは企業経営課題

IT部門だけの問題ではなく、企業経営の持続的成長を揺るがす経営リスク
- サイバー攻撃による組織の経済損失 -

6億3,767万円

日本における
侵害１件当たり平均損害賠償額

参照： https://www.jnsa.org/result/incident/data/2018incident_survey_sokuhou.pdf

約13～26億円以上

GDPRに
違反した場合の制裁金

⬇10%

サイバー攻撃を受けた後の
日本における株価下落率

⬇21%

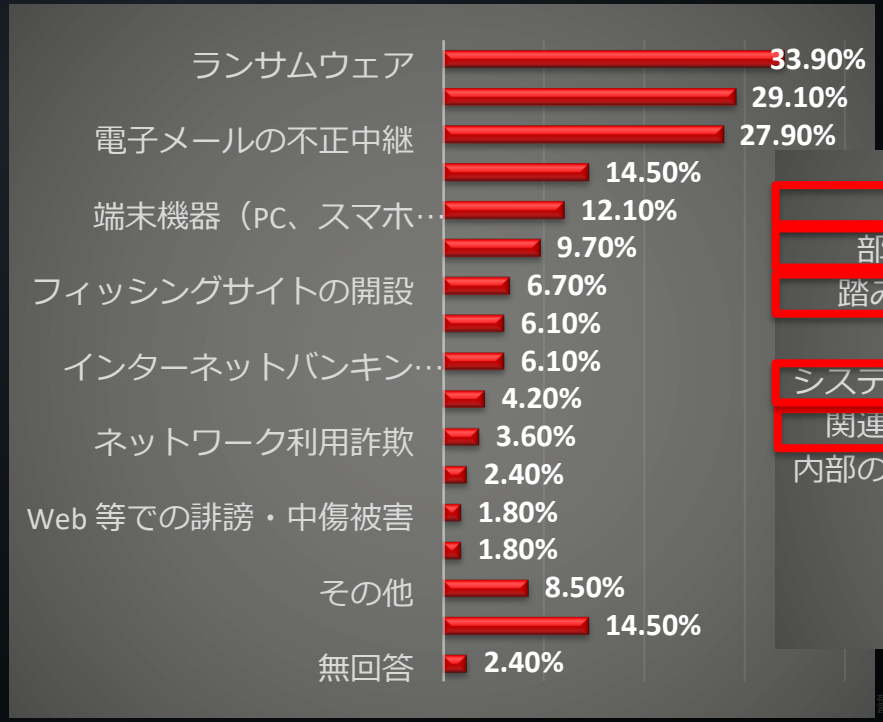
サイバー攻撃を受けた後の
日本における純利益減少率

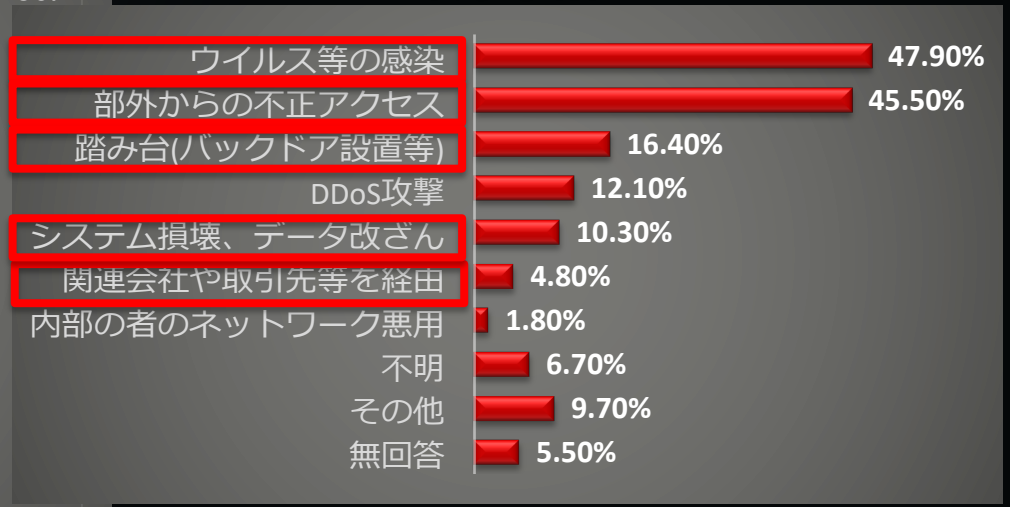
参照： https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf

©2020 Cybereason Japan Corp. | All rights reserved

巧妙な攻撃増加、100%防ぐのは困難

過去に受けたことのある被害状況





警察庁生活安全局情報技術犯罪対策課 不正アクセス行為対策等の実態調査（令和元年度）
https://www.npa.go.jp/cyber/research/r1/R1countermeasures.pdf

©2020 Cybereason Japan Corp. | All rights reserved

マルウェア感染対策の課題

技術的対策

- アンチウイルス対策
- ネットワークセキュリティ強化
- 最新パッチ適用
- 不正アクセス監視強化 など

課題

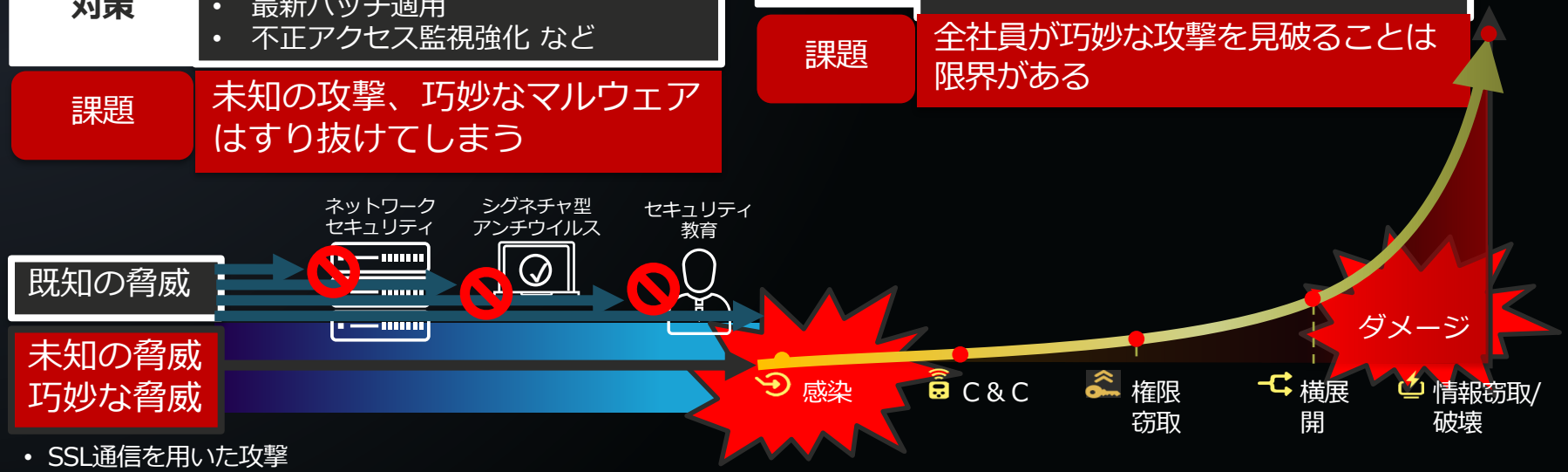
未知の攻撃、巧妙なマルウェアはすり抜けてしまう

人的対策

社員に対する継続した情報セキュリティ教育実施

課題

全社員が巧妙な攻撃を見破ることは限界がある



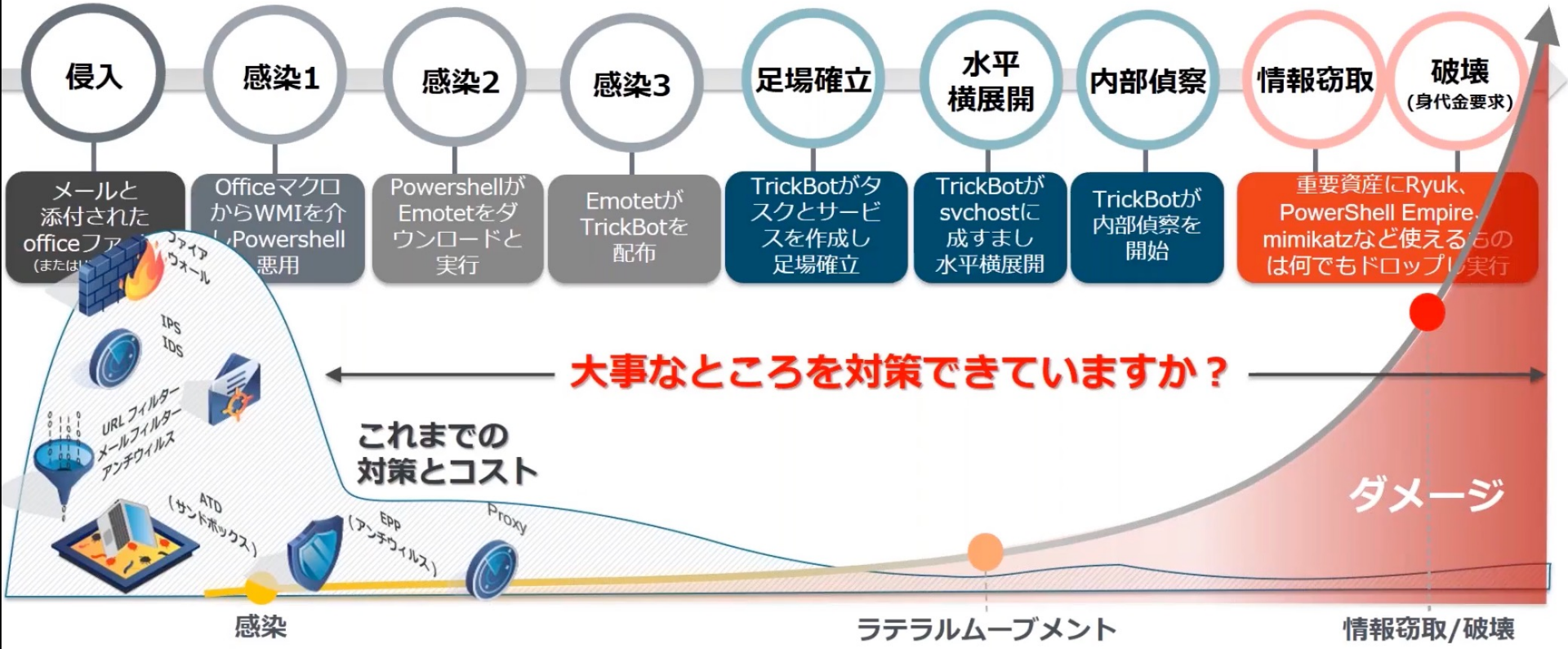
- SSL通信を用いた攻撃
- サンドボックス回避マルウェア
- シグネチャ/IOCベースでは検知できない未知/亜種のマルウェア
- ファイルを用いないマルウェア

100%防ぐことは困難
従来型セキュリティの限界

©2020 Cybereason Japan Corp. | All rights reserved

cybereason

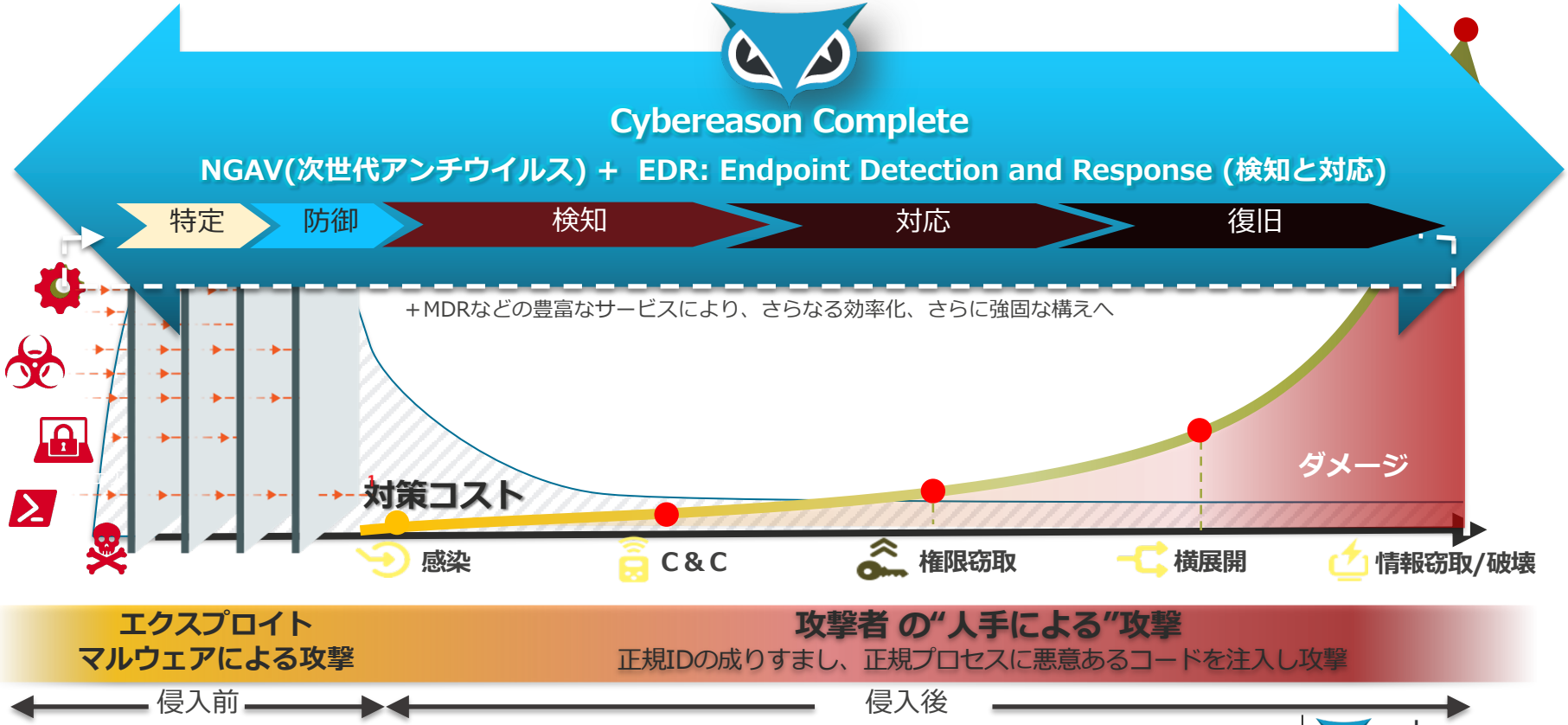
これまでのセキュリティ対策



©2020 Cybereason K.K. 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 -



©2020 Cybereason Japan Corp. | All rights reserved

cybereason

感染防御対策

次世代アンチウィルス

Cybereason Endpoint Prevention

(NGAV + Endpoint Control)

cybereason

©2020 Cybereason Japan Corp. | All rights reserved

エンドポイント防御に不可欠な機能

6つの専用防御層が必須

1. 既知の攻撃
2. 未知の攻撃
3. ファイルレス攻撃
4. ランサムウェア
5. 脆弱性を悪用した攻撃
6. スクリプトを悪用した攻撃

導入/運用が容易

- 多様で容易な導入方法
- 単一センサーでNGAVとEDRが動作
- センサーの稼働は端末に影響を与えない設計
- 単一画面で異なるソリューション、端末を管理、監視

エンドポイントコントロール

物理的な対策で端末の感染を防ぐ

- パーソナルファイアウォール
- USBデバイスコントロール
- ディスク暗号化端末の可視化

Cybereason Endpoint Prevention
(NGAV + Endpoint Control)

特定 → **防御**

©2020 Cybereason Japan Corp. | All rights reserved

Cybereason NGAV

次世代アンチウィルス 必須の6層

©2020 Cybereason Japan Corp. | All rights reserved

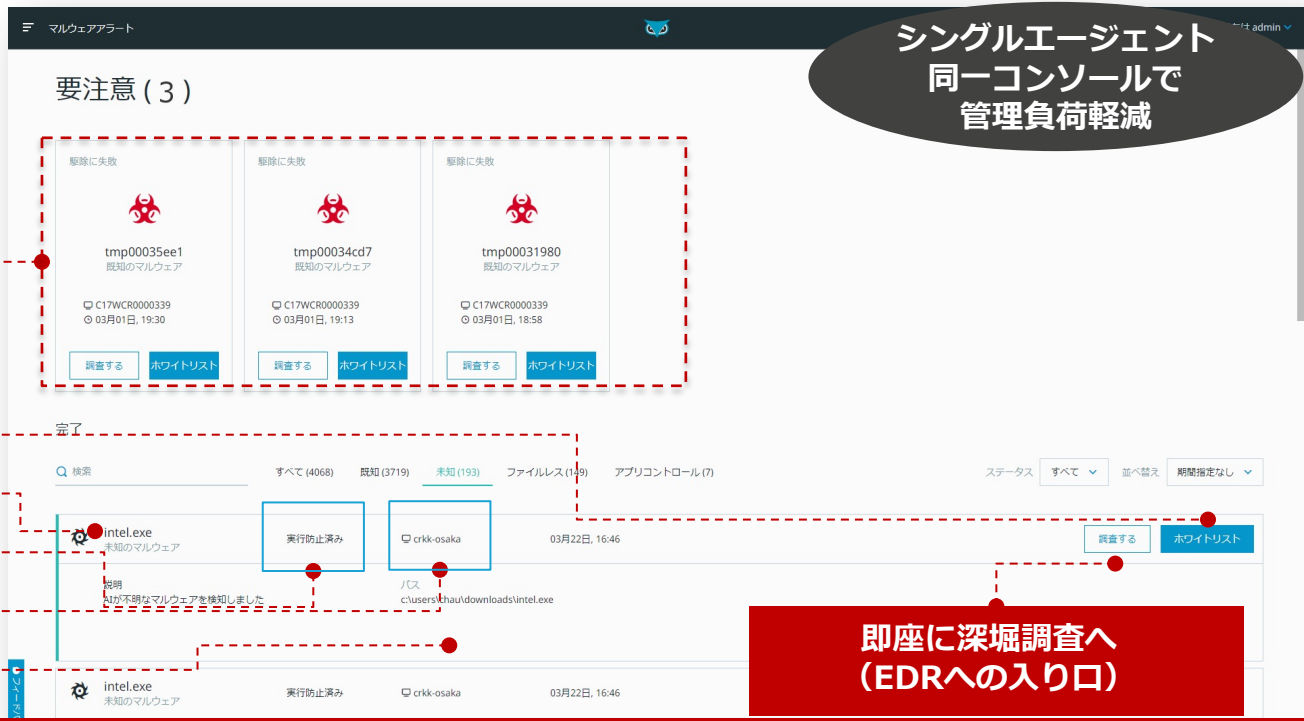
cybereason

EDRと一体になった次世代アンチウィルス（NGAV）

さまざまな脅威を
実行前に自動ブロック

既知、未知、ランサムウェア、
ファイルレス攻撃

注意が必要なアラートを視覚化
簡単にホワイトリスト登録
脅威の種別
対応の状況
影響する端末
ファイル名/コマンドなどの詳細



シングルエージェント
同一コンソールで
管理負荷軽減

即座に深堀調査へ
（EDRへの入り口）

単にプロセスを停止させるだけでなく、その状況に陥った端末/ユーザー/プロセスの素性を把握できる

©2020 Cybereason Japan Corp. | All rights reserved

cybereason

エンドポイントコントロール

デバイスコントロール

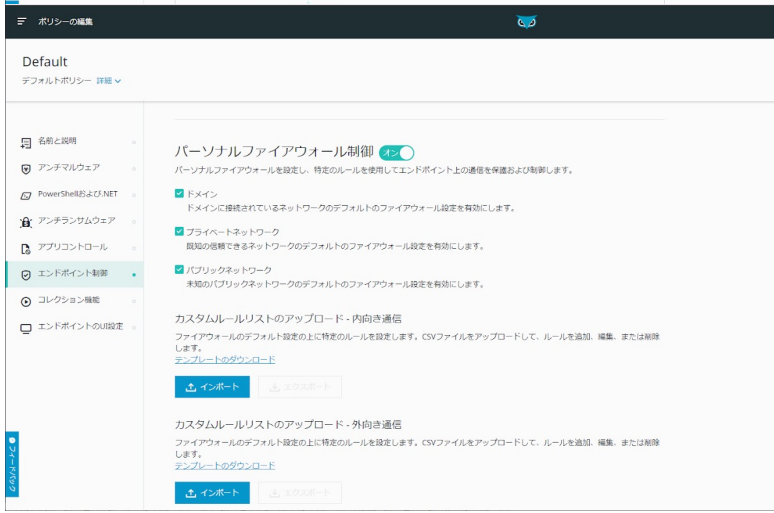
- USBデバイスの利用可否を制御可能
- ベンダー、製品、シリアル番号を指定して除外対象を指定可能

パーソナルファイヤーウォール

- ドメイン、プライベートネットワーク、パブリックネットワークでのアクセスルールを設定可能

フルディスク暗号化の可視化

- Windows端末でディスクの暗号化(BitLocker)を行っていないエンドポイントを特定



©2020 Cybereason Japan Corp. | All rights reserved

cybereason

Cybereason EDR

Endpoint Detection and Response
侵入後の脅威の検知と対応

©2020 Cybereason Japan Corp. | All rights reserved

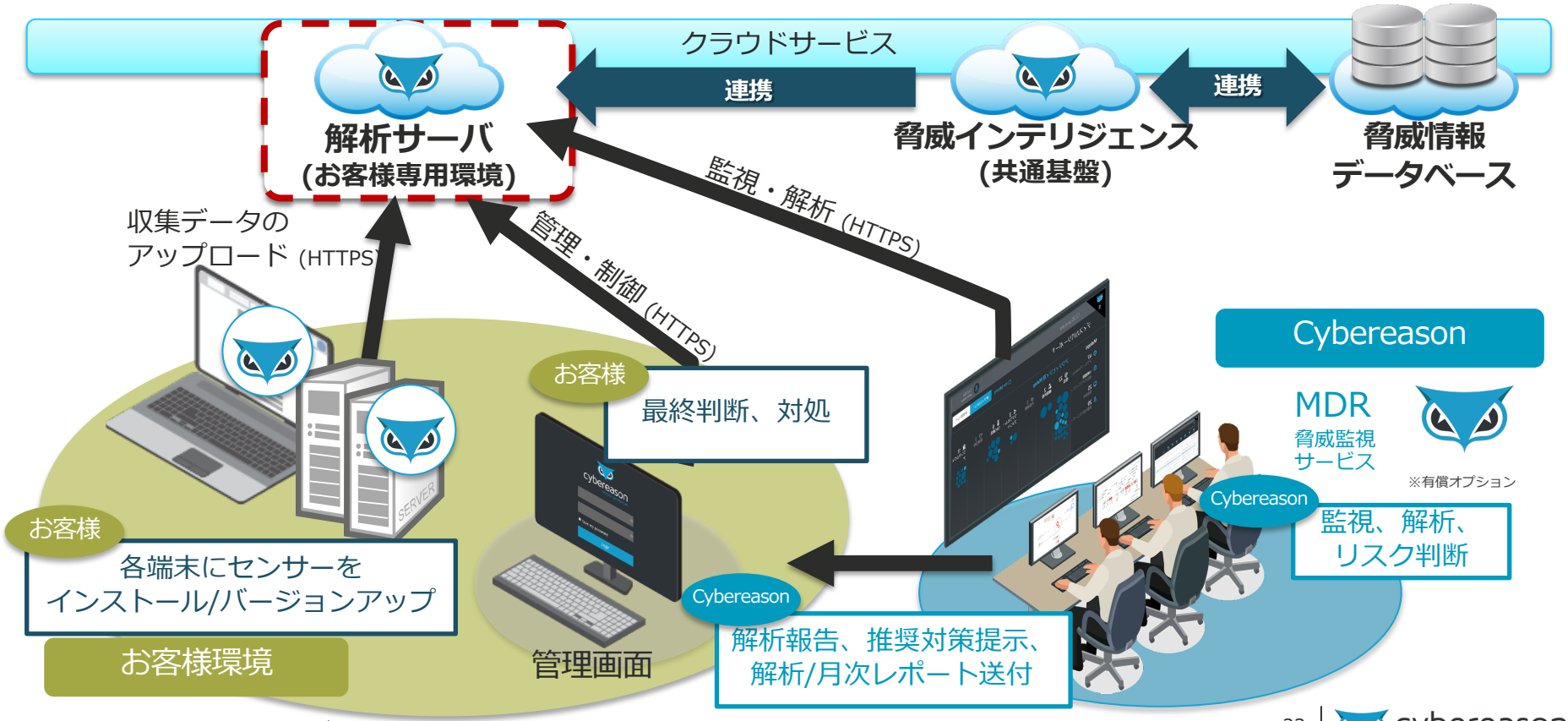
侵入後対策 “EDR” に必須の機能

複数端末にわたる相関解析	標的型攻撃を検知するには個々の攻撃を分析するのではなく、組織全体、異なるプラットフォーム(PC、サーバ、モバイル)にわたる相関解析が不可欠
振る舞い分析	従来のセキュリティソリューションでは検知できないファイルレス攻撃、ラテラルムーブメントなどの最先端の攻撃を分析が必要
リアルタイム検知	脅威を瞬時に検知するために常時毎秒800万クエリをビッグデータ解析
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、可視化することにより素早く影響範囲を把握し、対処に移ることにより被害を最小限に

迅速なインシデント対応によるセキュリティ運用負荷低減

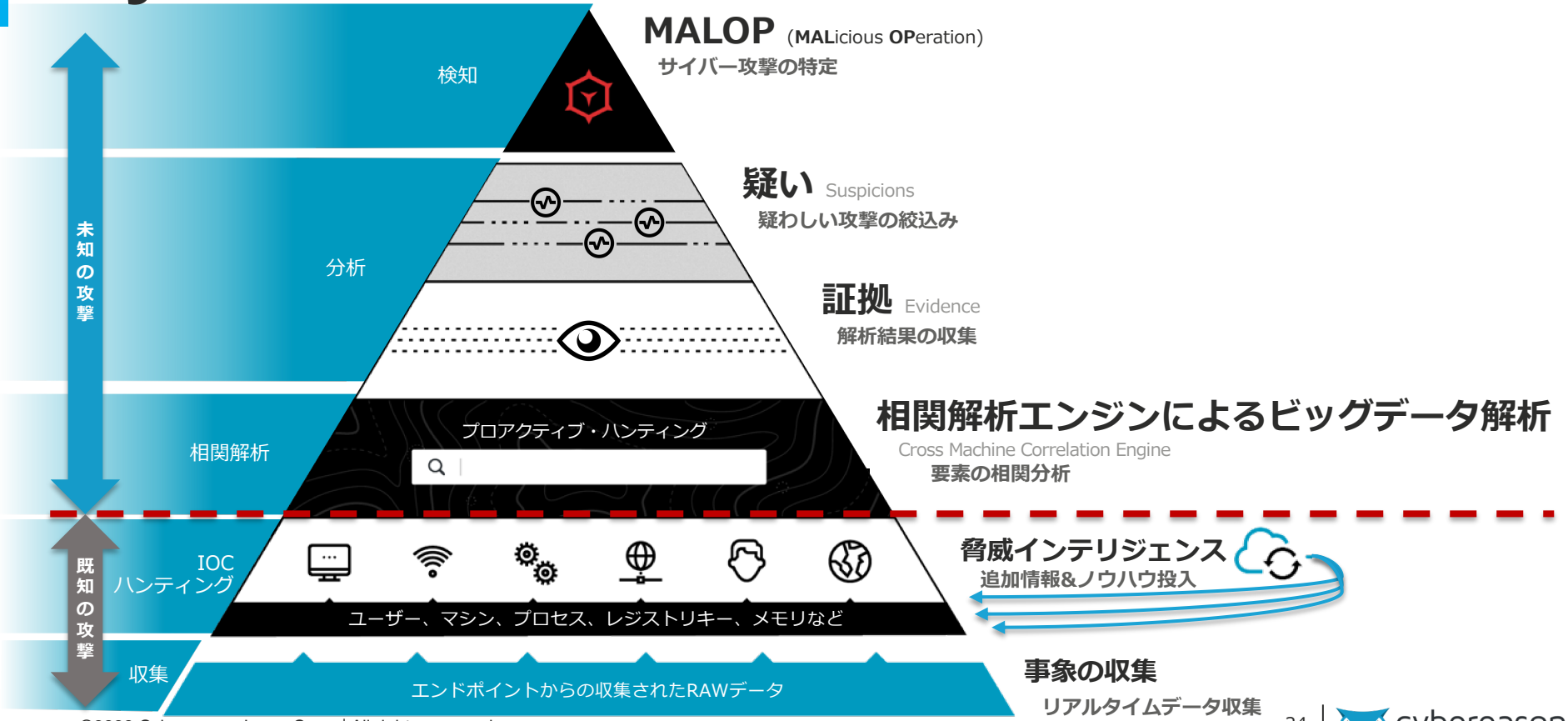
©2020 Cybereason Japan Corp. | All rights reserved

アーキテクチャ



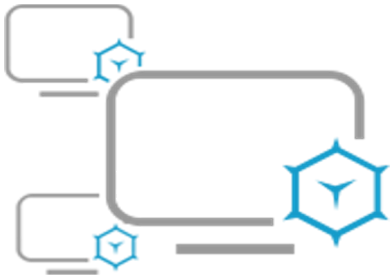
©2020 Cybereason Japan Corp. | All rights reserved

Cybereasonの分析モデル



©2020 Cybereason Japan Corp. | All rights reserved

Cybereason センサー



Cybereason センサーは、利用ユーザーの
「端末に影響を与えない」ように設計されています。

ユーザーモードで動作
→ PCクラッシュ無し

ユーザーモードで動作。万が一、センサーに問題が発生した場合も、他のアプリケーションおよびOSには影響を与えない設計。

※実行防止ドライバ及びNGAV機能はカーネルモードを使用します。

端末へのCPU負荷が低い
→ 通常業務に影響なし

センサーは収集データのアップロード、検知サーバからの指示による軽い処理のみを実施。解析処理は検知サーバー上で実施。

通信量5-25MB/日以下
(メール数通分)
→ 社内ネットワーク影響なし

端末の振る舞いやイベント情報のメタ情報を圧縮し、サーバーへリアルタイムにアップロード。

※Cybereason EDRでの数値です。NGAVでシグネチャモードを使用する場合は、シグネチャ更新時などに通信が発生します。

©2020 Cybereason Japan Corp. | All rights reserved

ダッシュボード

組織内で進行する攻撃を直感的に可視化

インシデント時の状況把握を効率化

一目で組織に広がる攻撃状況を把握し、適切で素早い対応に導く

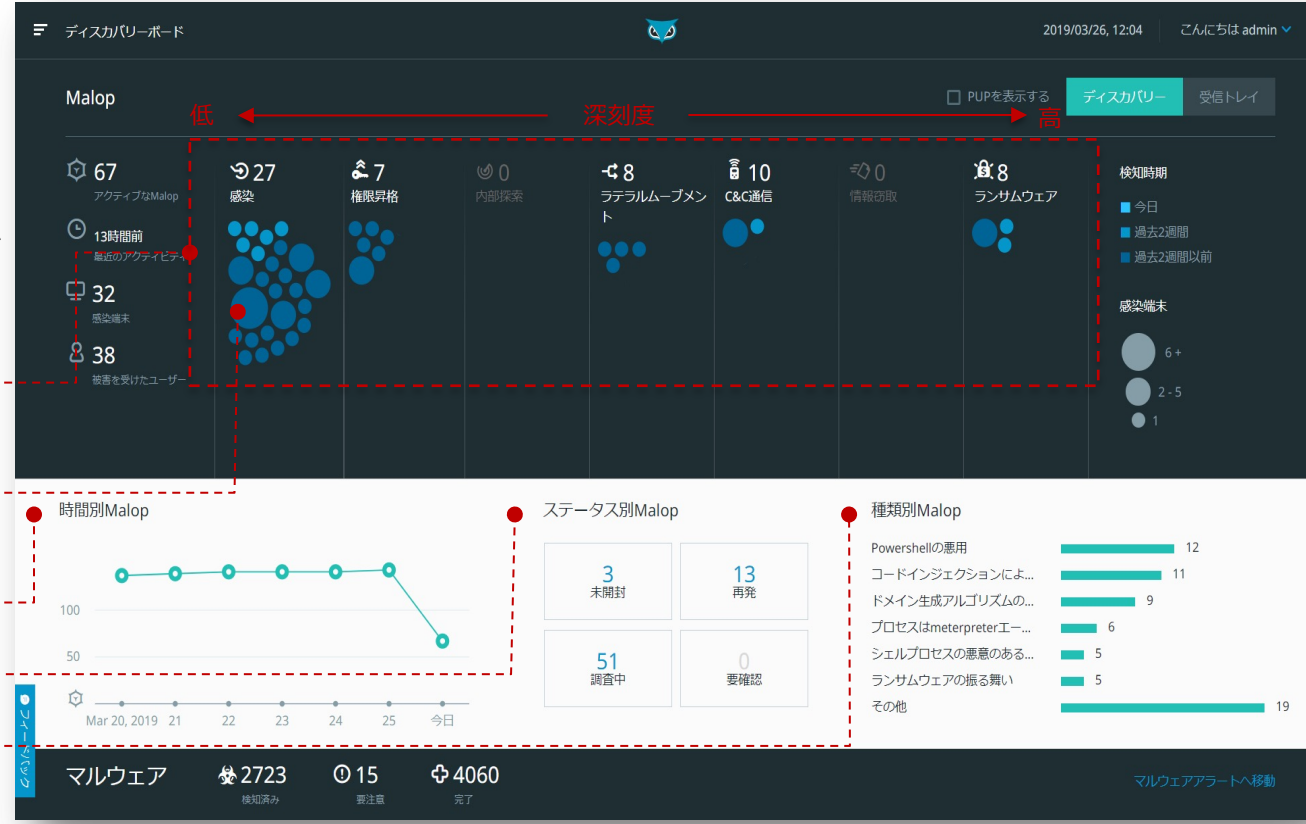
攻撃フェーズごとの感染状況

感染規模(バブルの大きさ)
経過時間（バブルの色）

時間別統計

対応ステータス別統計

攻撃の種類別統計



©2020 Cybereason Japan Corp. | All rights reserved

cybereason

MALOP詳細ビュー

インシデント解析結果の概要抽出

いつどこで何が どう起こったか 自動解析

ワンクリックで対処へ
（端末隔離、プロセス停止、レジストリ削除、ファイル隔離、リモートシェル）

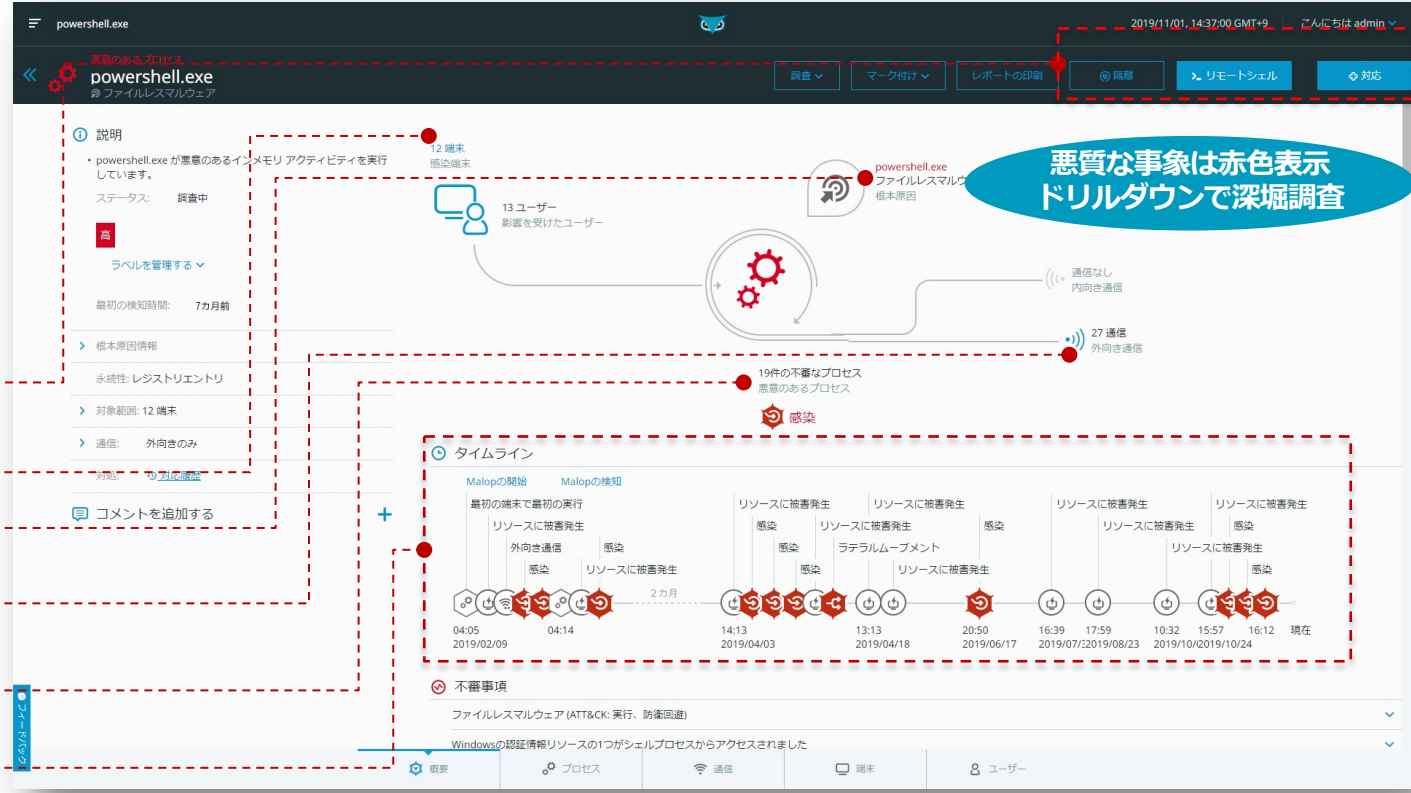
影響する端末とユーザー

検知の根本原因

悪質な通信の状況

用いられた悪質なプロセス

複数の端末にまたがる攻撃もタイムライン表示



©2020 Cybereason Japan Corp. | All rights reserved

cybereason

アタックツリー

解析結果の詳細を視覚化

インシデントの前後関係をすばやく掴む

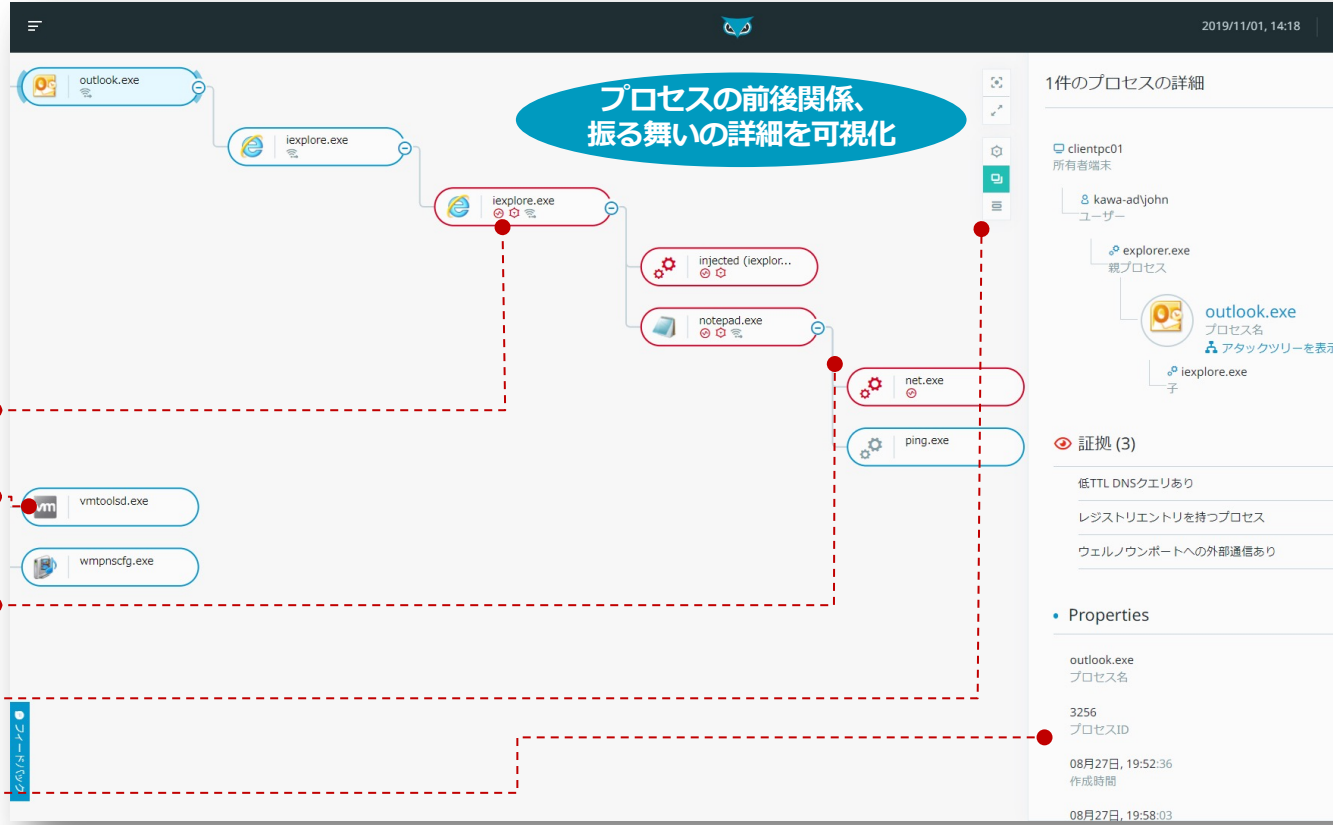
プロセスの前後関係を素早く把握

すべてのプロセスの詳細情報を表示するスケーラビリティ

ズームイン/アウト、折り畳み/展開の視覚サポート

ビュー切り替え機能で即座に必要な情報へ

疑わしい振る舞いの詳細情報



©2020 Cybereason Japan Corp. | All rights reserved

cybereason

隔離、対応機能

遠隔から、即座にワンクリック対処

複数の端末に対して一度にワンクリックで対応

ネットワークから
エンドポイントを即座に隔離

指示を出す端末の選択

プロセスの停止

ファイルの隔離

レジストリの削除

©2020 Cybereason Japan Corp. | All rights reserved

受信ボックス

効率的に対応状況を管理

対応漏れや二重対応を防ぎ
対応管理業務をラクにする
サポート機能

攻撃の一覧を確認し、適切に素早く対応

対応結果の管理（マーク付け）

一括レポート印刷

ラベル管理

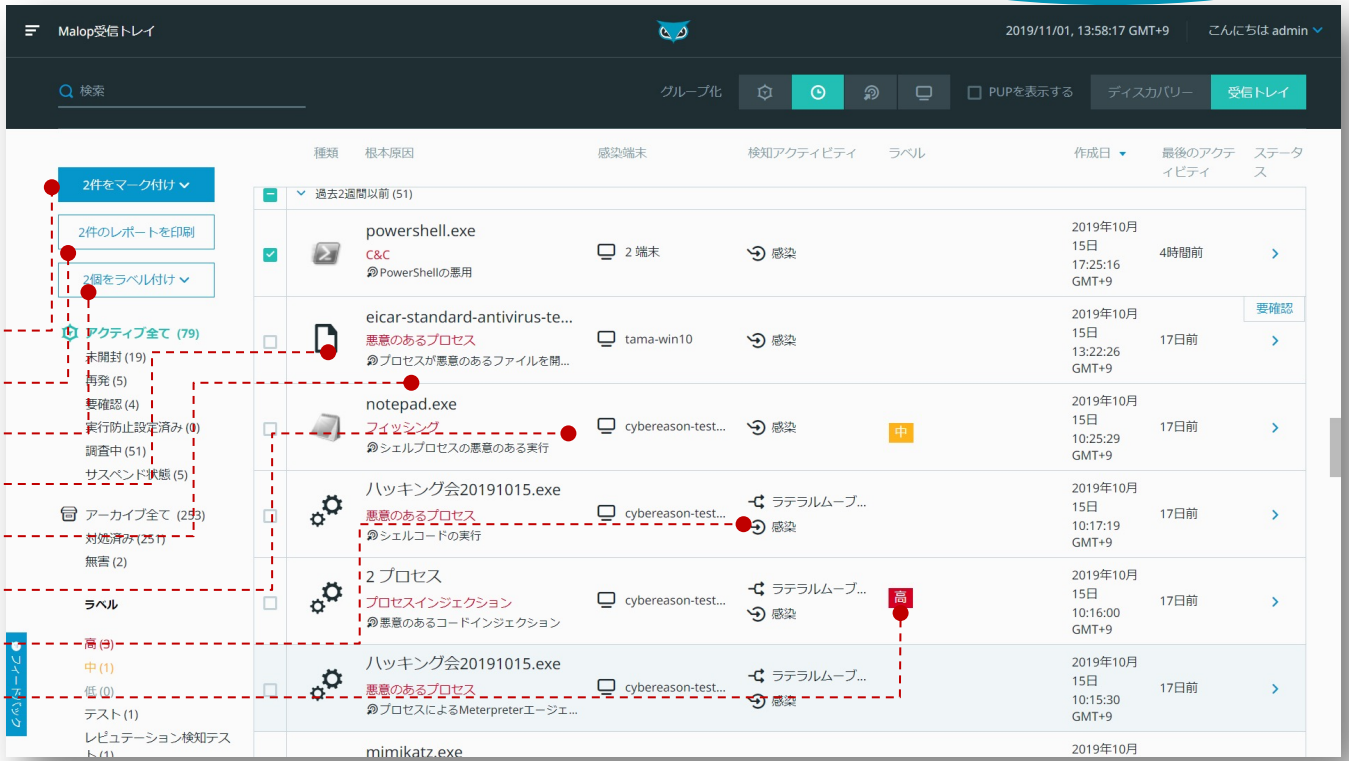
攻撃のタイプ

根本原因

感染端末、台数

攻撃フェーズ（危険度）

カスタマイズ可能なラベル管理



©2020 Cybereason Japan Corp. | All rights reserved

cybereason

調査機能

アナリスト業務を支援するスムーズな調査機能

直感的に操作でき
検索結果を素早く表示

センサーが収集した
エレメント(要素)を指定

エレメントをつなぎ合わせて
クエリを作成

エレメントに対して
フィルタで条件付け

表示された結果から
さらにドリルダウン

CSV出力

ハンティングエンジンが
フラグ付けした証拠/疑いも確認できる
迅速なアナリストによる調査を支援

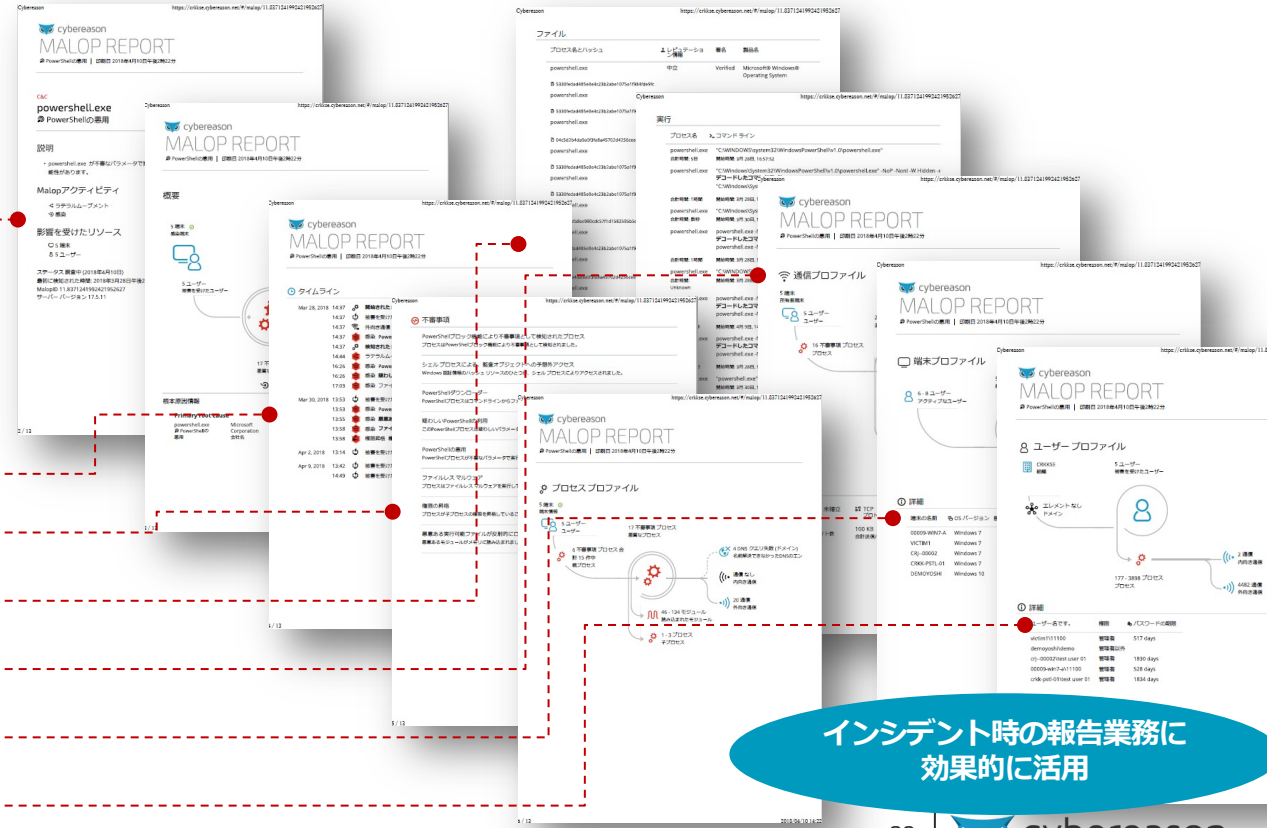
©2020 Cybereason Japan Corp. | All rights reserved

cybereason

PDFレポート自動生成機能

日本語レポートをボタンひとつで自動生成

セキュリティ業務の負荷を軽減する自動レポート生成機能



インシデント時の報告業務に効果的に活用

©2020 Cybereason Japan Corp. | All rights reserved

cybereason

Cybereason Mobile

©2020 Cybereason Japan Corp. | All rights reserved

Cybereason Mobile

Andoroid、iOS、iPadOS対応

① モバイル可視化

- ✓ BYOD端末から企業所有のデバイスまで端末のセキュリティを可視化
- ✓ PC,サーバ等の情報と統合し、包括的な可視化を実現
- ✓ インシデント発生時に網羅的な攻撃者の動きを把握

② 自律型防御

- ✓ 端末の不審な動作に基づき異常を発見
- ✓ 場所、時間を問わず常にモバイルデバイスを分析
- ✓ 端末が感染する前に自動防御

③ 検知と対処

- ✓ 実際の攻撃手順を想定した網羅的な防御と対処を支援
- ✓ 脅威に関連する全てのデバイスに対し対処を支援
- ✓ MDM/UEMとの連携により、対処を適用

©2020 Cybereason Japan Corp. | All rights reserved

お客様のセキュリティ業務を支援する充実したサービス

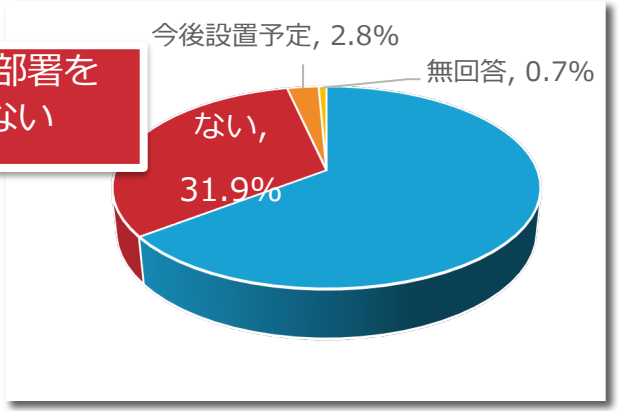
cybereason

©2020 Cybereason Japan Corp. | All rights reserved

課題: セキュリティ人材の不足

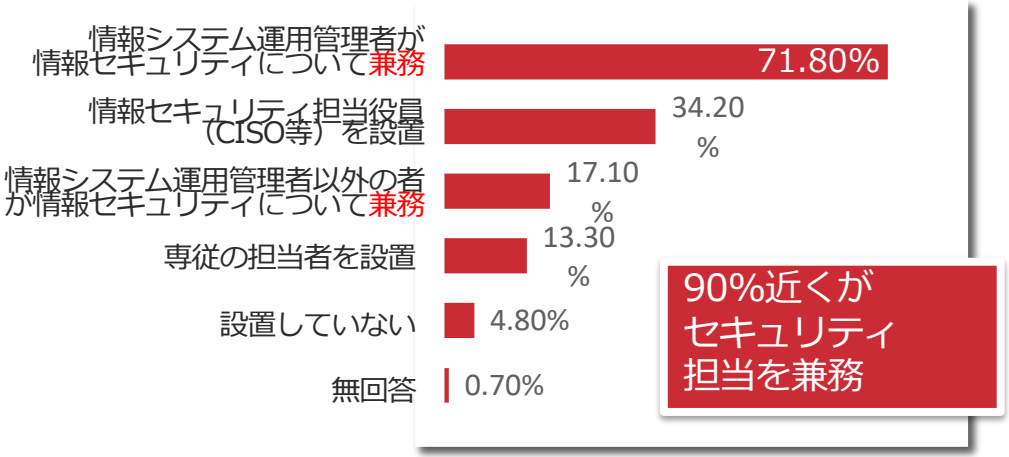
警察庁生活安全局情報技術犯罪対策課 不正アクセス行為対策等の実態調査 (令和元年度)
https://www.npa.go.jp/cyber/research/r1/R1countermeasures.pdf

情報セキュリティ運用
管理専門部署の有無



36%が専門部署を設置していない

情報セキュリティ管理体制



90%近くがセキュリティ担当を兼務

19.3万人

2020年セキュリティ人材不足数(推計)

総務省 サイバーセキュリティ人材育成分科会
我が国のサイバーセキュリティ人材の現状について
https://www.soumu.go.jp/main_content/000591470.pdf

自社で対応するのは技術的にも
マンパワー的にも難しいのが現実
高度なサイバー攻撃の解析・対応はセキュリティ専門家の知見を利用する事が一般的

©2020 Cybereason Japan Corp. | All rights reserved

cybereason

Cybereasonの高付加価値セキュリティサービス

Customer Success

カスタマー・サクセス

料金：無料

Product Support

製品サポート
契約区分：必須
料金：年額

Deployment

デプロイメント
(初期サーバー構築)
契約区分：必須
料金：初年度のみ

GSOC

MDR
脅威検知と対応の
マネージドサービス
(脅威監視解析)

契約区分：オプション
料金：年額

AST (Advanced Security Team)

Compromised Assessment
(侵害調査)

契約区分：オプション

インシデント
レスポンス
(侵害対応)

契約区分：オプション

Cyber Posture Assessment
(セキュリティ ヘルスチェック)
契約区分：オプション

Professional Services

プロフェッショナル
サービス

サイバーリーズンの
セキュリティ専門家による
高度な対応を求める
お客様向けの
アドバンスド・サービス

契約区分：オプション

©2020 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

データ収集

Cybereason 解析サーバー
(お客様専用環境)

当社の専門アナリストが攻撃の顛末と影響範囲をご報告し、お客様が迅速に対処できるように支援します

検知アラート

被疑エンドポイントの対処

- 脅威度判定
- インシデント対応

管理者様

- **一時解析報告**※1
- **推奨対策提示**※1
- **解析レポート送付**※2
- **月次レポート送付**
- **FAQ**

※1:メールでのご連絡
※2:脅威度「5」の場合のみ

アナリストによる
- 24/365 監視・トリアージ
- 自動脅威ハンティング
- **脅威度判定**
- 根本原因調査

Cybereason MDR

©2020 Cybereason Japan Corp. | All rights reserved

Cybereason MDRパッケージ

<凡例>

◎	サービス提供
○	サービス一部提供
-	サービス提供対象外

*1別途提供しているCompromised Assessment(侵害調査サービス)とは異なります。
*2インシデント対応に係る契約を事前に締結するものであり、対応時間はMDRに含まれません。インシデント対応時の実働には別途費用が必要となります。

カテゴリ	Complete提供内容	Essentials提供内容	Complete	Essentials
プレミアム **オンボーディング**	対面、またはオンラインミーティングでの検知ルールの最適化とオンボーディングコンサルテーション	オンボーディング時のご連絡・検知ルールの最適化	◎	○
プロアクティング **チューニング**	導入後のプロアクティブチューニングによる環境最適化 BWLおよびカスタムルールの作成代行	導入後のプロアクティブチューニングによる環境最適化	◎	○
脅威ハンティング*1	脅威情報ハンティング/自動相関分析	脅威情報ハンティング/自動相関分析	◎	◎
	24x7プロアクティング脅威ハンティング	-	◎	-
監視・検知・調査	24x7 のリアルタイム監視・トリアージ	24x7 のリアルタイム監視・トリアージ	◎	◎
調査支援	検知されたMalop、抑止制御策、および関連する不審な挙動に関するEmail・電話による問い合わせ対応	検知されたMalop、抑止制御策、および関連する不審な挙動に関するEmail問い合わせ対応	◎	○
	次世代アンチウィルスファイル分析（NGAV分析）	-	◎	-
抑止制御	抑止制御の推奨策の提示	抑止制御の推奨策の提示	◎	◎
	抑止制御の代行	-	◎	-
通知	Malop検知に係るメール通知	Malop検知に係るメール通知	◎	◎
	脅威度5のMalopに係る電話通知	脅威度5のMalopに係る電話通知	◎	◎
レポート	都度提供　重大なMalopに係る解析レポートの提示	都度提供　重大なMalopに係る解析レポートの提示	◎	◎
	月次提供　レポートの提示	月次提供　レポートの提示	◎	◎
	四半期提供　脅威情報レポートの提示	-	◎	-
インシデント対応*2	インシデント対応支援リテイナー	インシデント対応支援リテイナー	◎	◎

©2020 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

©2020 Cybereason Japan Corp. | All rights reserved

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

©2020 Cybereason Japan Corp. | All rights reserved

社内環境の安全性を確認

Cyber Posture Assessment (ヘルスチェック)

Cybereason EDRを用いて、約2週間で社内環境が侵害されているかどうかをチェックします。お客様にて、各エンドポイントへセンサーをインストールいただきます。

EDRの導入を検討されているお客様

既存セキュリティ対策の効果を測定したいお客様

端末の利用状況の洗い出しをしたいお客様

✓ **端末数(PC/サーバー含む)：5000台まで**

1. インストール
(2週間)

お客様がエンドポイントへCybereasonセンサーをインストールします
(サイレントインストール可)

Windows, Mac, Linux

2. 調査
(2週間)

Cybereason EDRの自動解析とアナリストクエリにて、すり抜けた侵害をあぶりだし、組織の健康状態を調査します

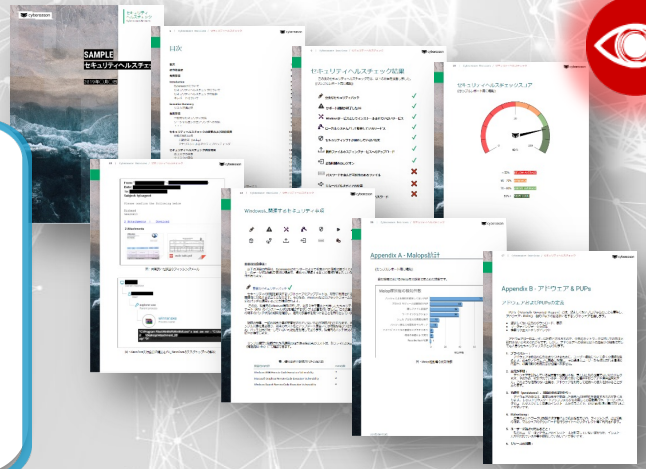
3. レポート

侵害の有無とセキュリティヘルスの診断結果を報告いたします

正規アカウント/プロセスへの成りすまし

すり抜けたウィルス/マルウェア

隠された裏口/バックドア



©2020 Cybereason Japan Corp. | All rights reserved

Cybereasonの優位性

©2020 Cybereason Japan Corp. | All rights reserved

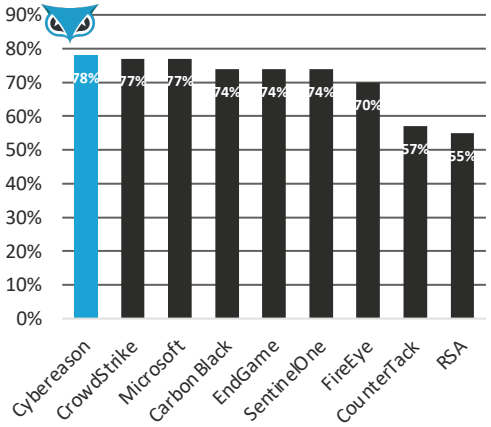
CybereasonのMITRE ATT&CK-APT3評価結果

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

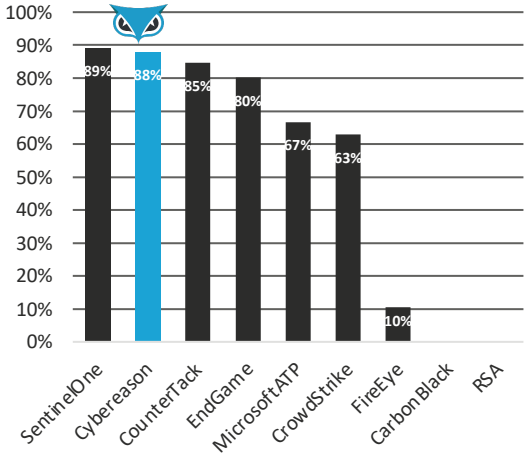
米国政府の支援を受けている非営利の研究団体MITREによるATP3攻撃テクニックを用いた完全に公平な評価結果に、Forresterが透明性の高い評価スクリプトを提供。その結果、以下のCybereasonの圧倒的な優位性が認められた。

Cybereasonは製品単体だけでも最高峰のカバレッジ

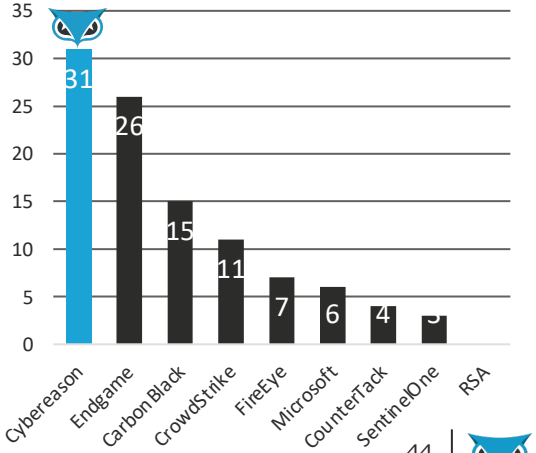
最高のカバレッジ（データ収集能力）



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

©2020 Cybereason Japan Corp. | All rights reserved

2020年4月

NSS LabsによるNGAV評価

2020年版AEPテストで最高評価を獲得

(AEP=Advanced Endpoint Protection=高度エンドポイント保護)

AAA

検知回避への耐性

攻撃を100%ブロック

AA

メール経由のマルウェア

攻撃を99.9%ブロック

AA

HTTP経由のマルウェア

攻撃を98.3%ブロック

AA

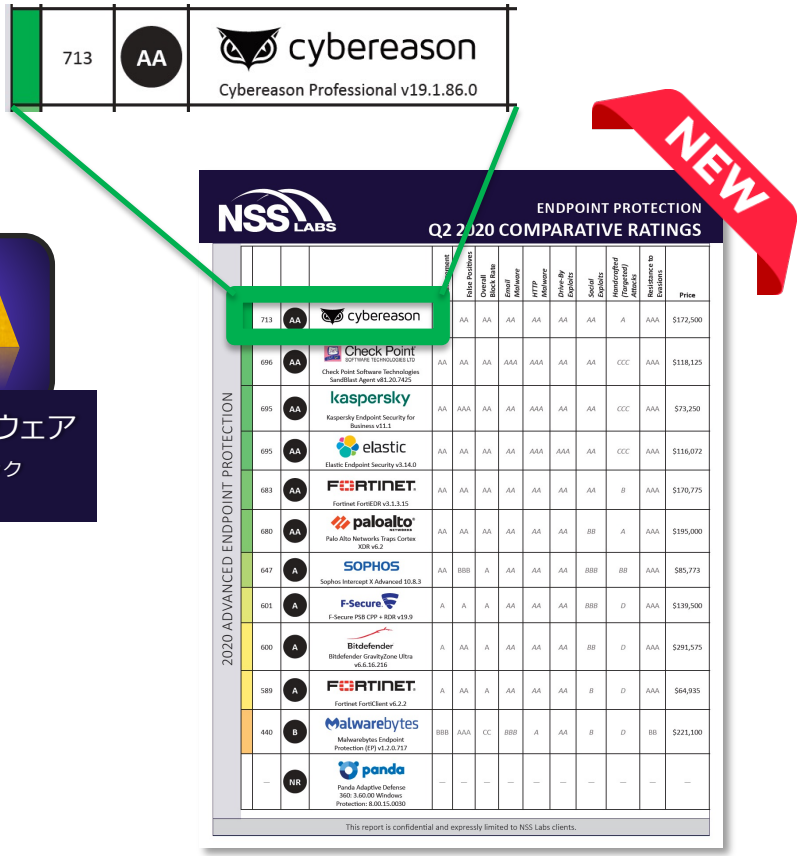
チューニングと誤検知

誤検知率1%未満

AA

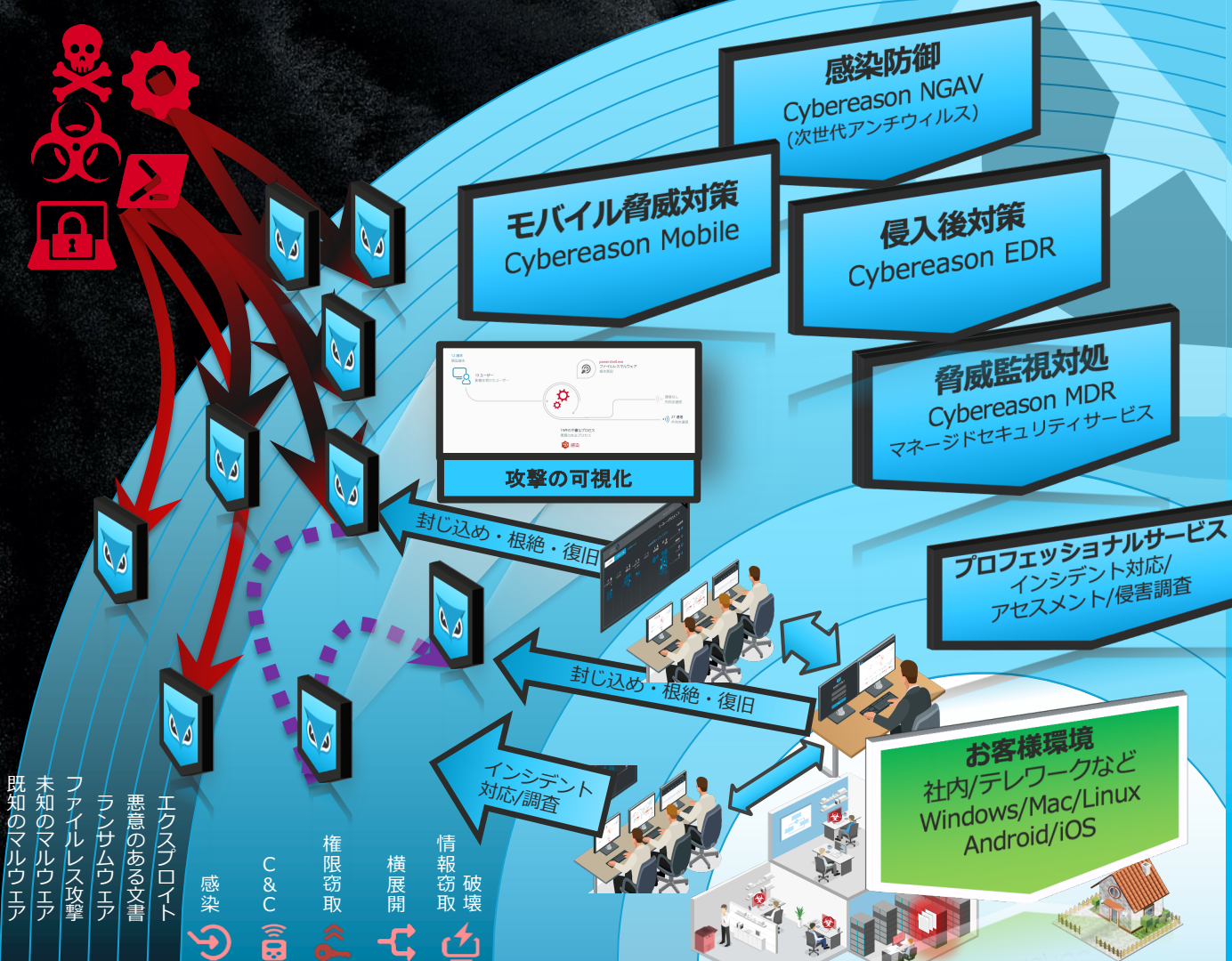
ドライブバイエクスプロイト

攻撃を98%ブロック



©2020 Cybereason Japan Corp. | All rights reserved

cybereason



“感染防御”
“侵入後対策”
“脅威監視対処”
をワンストップ
で提供

cybereason®

真の
エンドポイント保護
プラットフォーム

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。

©2020 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）

©2020 Cybereason Japan Corp. | All rights reserved

Cybereason NGAVとEDRの併用によるさらなる効率化

他社製 AV/NGAVとの組み合わせ

センサー/エージェントは個別に動作

他社製 AV/NGAV

- シグネチャベースではなくAIのみに依存した分析
- ランサムウェア、ファイルレス攻撃、エクスプロイト攻撃などの高度な攻撃に対する専用の防御機能なし
- AIに依存する検知防御のため処理効率に劣る

Cybereason EDR

- 他社 AV/NGAVで検知した攻撃の共有不可
- 可視性に劣る
- 他社NGAVをすり抜けた攻撃の解析処理が増加することにより、アラートの増加
- 運用上、真の脅威を見落とす可能性

Cybereason NGAV、EDRとの組み合わせ

✓ 単一センサーでNGAV、EDRが動作

Cybereason NGAV

✓ 次世代アンチウィルス必須の専用防御6層に対応

✓ NGAV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

Cybereason EDR

✓ EDRとNGAVから収集されたデータを相互に相関させることが可能

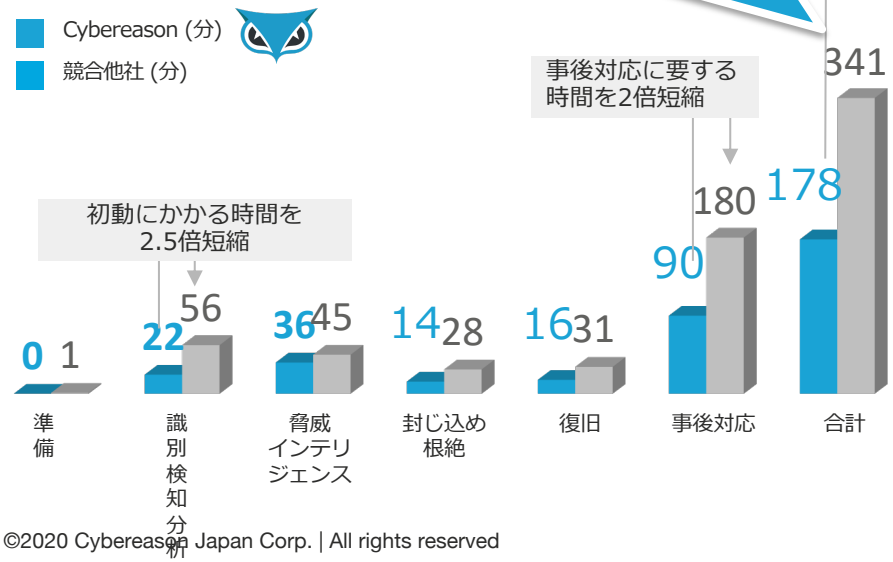
✓ より高度な可視性を提供

©2020 Cybereason Japan Corp. | All rights reserved

Cybereasonでインシデント対応時間を半減

あるMSSPによるCybereasonと他社ソリューションとの比較
準備から事後対応までのインシデント対応に要した時間を評価

Cybereasonの高いデータ収集能力、相関解析、可視化機能によって全体の対応時間を2倍短縮



単位: 分

	サイバーリーズン	競合他社	SIEM	オープンソース
準備	0	1	15	45
識別 検知 分析	22	56	240	720
脅威インテリジェンス	36	45	195	2085
封じ込め、根絶	14	28	240	240
復旧	16	31	2405	2430
事後対応	90	180	1200	4800
合計	178分 (3時間)	341分 (6時間)	4295分 (72時間)	10320分 (172時間)

セキュリティチームの作業負荷を軽減
早期対応でビジネスの影響を最小限に

©2020 Cybereason Japan Corp. | All rights reserved

cybereason

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

Appendix

cybereason

©2020 Cybereason Japan Corp. | All rights reserved

センサーシステム要件

v20.1

©2020 Cybereason Japan Corp. | All rights reserved

センサーの対応OS

Cybereason OS 20.1

Microsoft Windows

OPERATING SYSTEM (PC)	OPERATING SYSTEM (SERVER)
Windows 10 (Windows 10バージョン20H2 (October 2020 Update)まで)	Windows Server 2019
Windows 8.1	Windows Server 2016
Windows 8	Windows Server 2012 R2
Windows 7 SP1	Windows Server 2012
	Windows Server 2008 R2 SP1

KB要件

OS	REQUIRES KB	NOTES
WWindows Server 2012 R2 Windows 8.1 Windows Server 2012 Windows 8 Windows Server 2008 R2 Service Pack 1 (SP1) Windows 7 SP1	KB2999226	センサーが機能するために必要。
Windows 7 SP1, Windows Server 2008 R2 SP1	KB3033929 または KB4474419	SHA256署名をサポートするために必要。他のMicrosoftパッチもこの機能を提供している可能性があります。

Mac OS

オペレーティングシステム
MacOS Big Sur (11) [1]
macOS Catalina (10.15) [2]
macOS Mojave (10.14)
macOS High Sierra (10.13)
macOS Sierra (10.12)

[1] Sensors running macOS Big Surのセンサーは Signatures modeおよびDNSリクエストのデータ収集はサポートしていません。 [2] Service Pack (Nov. 12, 2019)が必要です

Linux

オペレーティングシステム	フルサポート	限定サポート[1]
CentOS 6, 7 and 8	✓	
Red Hat Enterprise Linux 6 and 7	✓	
Red Hat Enterprise Linux 8	✓	
Oracle Linux 6 and 7	✓	
Ubuntu 14 LTS and 16 LTS	✓	
Ubuntu 18.04		✓
SLES 12		✓
Debian 8 and 9	✓	
Amazon Linux AMI 2017.03 [2]	✓	

注: すべての*Linux*オペレーティングシステムは、*Python 2.6*以降または*Python 3.0*以降がインストールされている必要があります。*Linux 32*ビットオペレーティングシステムはサポートされていません。

[1] 限定サポートとは、当該オペレーティングシステムでセンサーのアップグレードとインストール/アンインストールが可能であり、基本的な機能がサポートされていることを意味します。基本的な機能とは、Cybereasonサーバーとの通信、プロセスと静的端末情報の収集などです (インターフェイスなど)。他の収集アクションと対処アクションはサポートされません。 [2] ARMプロセッサは未サポートです。Amazon Linux 2は未サポートです。

©2020 Cybereason Japan Corp. | All rights reserved

古いOSへの対応

以下の表は、古いオペレーティングシステムでサポートされる最新のセンサーバージョンを示します。

OS	バージョン	サポートされる最新のセンサーバージョン
Windows	XP SP3	18.0
Windows	Vista	18.0
Windows	Server 2003	18.0
Windows	Server 2003 R2	18.0
Windows	Server 2008	18.0
Windows	Server 2008 R2	18.0
Mac	Yosemite (10.10)	18.0
Mac	El Capitan (10.11)	18.0
Amazon Linux	2017より前のすべてのバージョン	18.0

古いオペレーティングシステムの場合、特定のセンサーバージョンまでのセンサーがサポートされます。このバージョンより後のセンサーをインストールする前に、エンドポイントをサポートされているオペレーティングシステムにアップグレードすることをお勧めします。これを行わないと、センサーの完全な機能が保証されません。

©2020 Cybereason Japan Corp. | All rights reserved

OSごとの対応機能

機能	WINDOWS 7SP1、8、8.1、10、WINDOWS SERVER 2008 R2 SP1、2012、2012 R2、2016、2019	MAC （すべてのバージョン）	LINUX （すべてのバージョン）
ファイルのダウンロード	✓	✓	✓
ファイル検索	✓		
端末の隔離	✓	✓	
プロセスの終了	✓	✓	✓
実行防止	✓		
ファイルの隔離	✓	✓ [1]	✓
リモートシェル	✓		
レジストリの削除	✓		
ランサムウェアのサスペンド/サスペンド解除	✓		

[1]Mac用センサーの場合、DMGファイル、およびOSXオペレーティングシステムでインターネットからダウンロードしたファイルの隔離はサポートされていません

©2020 Cybereason Japan Corp. | All rights reserved

センサーのシステム要件と管理UI接続ブラウザ

センサー：ハードウェア要件

EDRのみ利用 (NGAV機能無効)

コンポーネント	要件
RAM	1GB
CPU	デュアルコア2GHz、コアi3以上か同等
ディスク容量	150MB以上
ネットワーク接続	イーサネットまたはWi-Fi

EDR/NGAV機能を併用 (Windowsのみ)

コンポーネント	要件
端末のRAM	2GB
CPU	デュアルコア2GHz、コアi3以上か同等
ディスク容量	1.5GB以上
ネットワーク接続	イーサネットまたはWi-Fi

その他要件

Windows
- 「TLS通信」の記載要件を満たしている必要があります (TLS1.2対応など、詳細はお問い合わせください)
- エンドポイント上でCybereasonのシステムトレイアイコンと通知を表示するには、.NET Framework 4.0を有効にする必要があります
- センサーのKB要件を満たしていることが必要です
- DPIコレクションを有効にすると、さらに30MBのRAMが使用 (または部分的に使用) されます

Linux
- エンドポイントでは、端末にglibcをインストールする必要があります。

Cybereason UI(管理画面）のサポートブラウザ

- Cybereason UIは、最新バージョンのChromeをサポートします

©2020 Cybereason Japan Corp. | All rights reserved