日本でもっとも選ばれている
サイバー攻撃対策

中堅企業向け 次世代エンドポイントセキュリティソリューション

— Cybereason Core Suite —

cybereason

サイバー攻撃対策はクルマの安全対策と同じです。

交通安全対策	サイバー攻撃対策
事故防止機能 ペダル踏み間違い、車線逸脱、後側方接近など	ウイルス対策、ランサムウェア対策
事故状況把握 ドライブレコーダー、イベントデータレコーダー	万が一侵入された場合、 その全体像を可視化、対処できる対策
車の正常性確認 定期点検、車検	企業・組織の安全性確認の実施
事故後の対応、交渉 コールセンター、弁護士	高度な攻撃への対応方法、体制

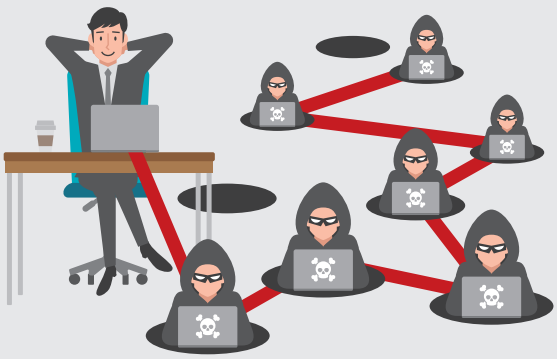
重大な事故ほど、事前の対策がカギ。
備えあれば憂いなし。
早期解決で被害が最小限に！

Before

今までのセキュリティ対策は、ひとつずつ対処する、もぐら叩き。
担当者は毎日毎日、大量のアラートと格闘。
重大な脅威を見逃し、
重大なセキュリティ事故につながる可能性も!

Cybereason

サイバーリーズンなら、
芋づる式で複数端末にわたる攻撃の全体像を可視化。
一網打尽で攻撃を最小化します。



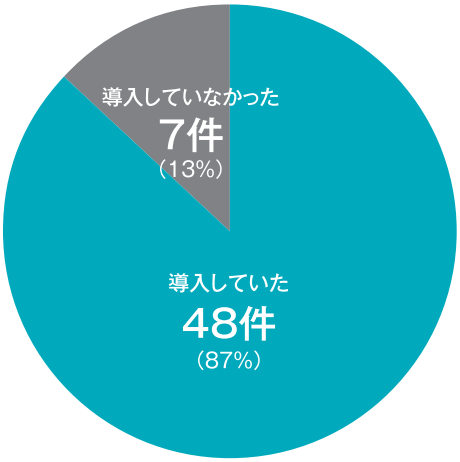
そのセキュリティ、大きな誤解!

誤解1　ファイアウォールやアンチウイルスを入れているから、侵入は防げるだろう。

ランサムウェア攻撃はアンチウイルスなどのウイルス対策ソフトでは検出が困難。

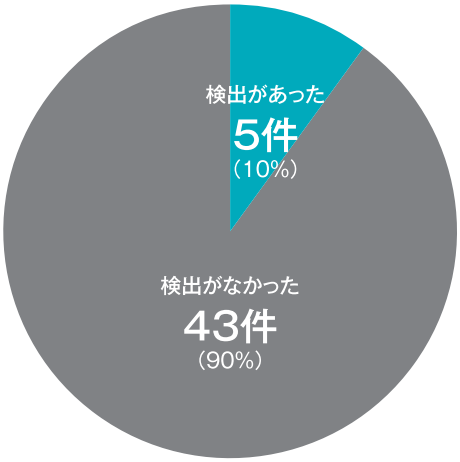
ウイルス対策ソフトの導入状況

有効回答 55件



検出の有無

対策ソフト等導入していた 48件



ランサムウェアの被害にあった企業・団体等のウイルス対策ソフト等の導入・活用状況
【出典】警察庁 令和4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　P22(4)被害企業・団体等のウイルス対策ソフト等の導入・活用状況
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

最新の攻撃は従来のセキュリティを突破。万が一の攻撃に備えた対策を。

Point
現状のセキュリティで対処できるかどうかの見直しを。
次世代エンドポイントセキュリティEDRで脅威の見える化対策を。

サイバー攻撃例	FW/UTM	プロキシ、IDPなど	アンチウイルス
既知のウイルス	○検知可能	○検知可能	○検知可能
未知/亜種のウイルス	×検知不可	×検知不可	×検知不可
暗号化通信(TLS)を用いた攻撃	△TLS復号必須	△TLS復号必須	○検知可能
ファイルを用いないマルウェア	×検知不可	×検知不可	×検知不可
OSの標準ツールを悪用した攻撃	×検知不可	×検知不可	×検知不可
マクロを悪用した攻撃	×検知不可	×検知不可	×検知不可
OSやアプリの脆弱性をついた攻撃	×検知不可	×検知不可	×検知不可

脅威の見える化 4つの必須機能

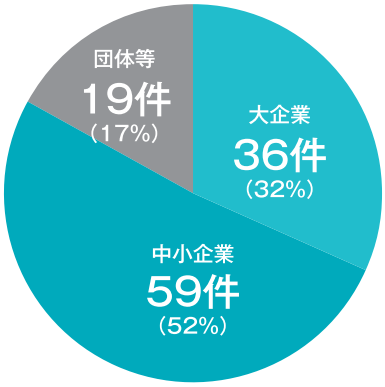
1. 巧妙な攻撃の全体像を可視化
2. すり抜けた攻撃の振る舞いを相関解析
3. リアルタイムに検知
4. 端末がどこにいても対処を実行

誤解2　中小企業だから狙われないだろう。

サイバー攻撃は組織の規模を問わず発生。

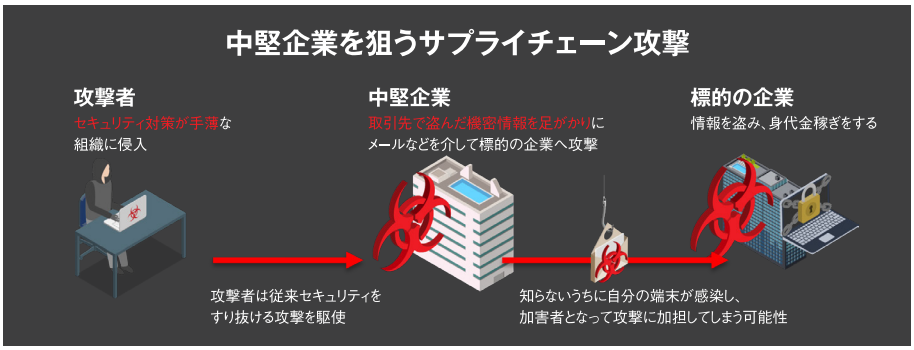
ランサムウェア被害の半数以上が中小企業。

ランサムウェア被害件数（R4上）
114件



ランサムウェアの被害にあった企業・団体等の規模
【出典】警察庁 令和4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
P4　1 令和4年上半期における脅威の動向（1）ランサムウェアの情勢と対策（ウ）被害企業・団体等の規模
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

近年、中堅企業を踏み台にするサプライチェーン攻撃が発生。特に、取引先が攻撃され個人情報が漏えいする等の被害が増加。



順位	サイバー攻撃例
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	標的型攻撃による機密情報の窃取
4	内部不正による情報漏えい
5	テレワーク等のニューノーマルな働き方を狙った攻撃
6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7	ビジネスメール詐欺による金銭被害
8	脆弱性対策情報の公開に伴う悪用増加
9	不注意による情報漏えい等の被害
10	犯罪のビジネス化（アンダーグラウンドサービス）

情報処理推進機構（IPA）情報セキュリティ10大脅威 2023 より
https://www.ipa.go.jp/security/vuln/10threats2023.html

Point
情報資産の保存されている端末、サーバーの棚卸し、セキュリティの見直しを。
サイバーリーズンでは、組織のセキュリティに対する健全性を診断し、
セキュリティ対策と運用に対する改善策を提示するサービスを提供。

誤解3　攻撃なんて頻繁にないから、セキュリティ担当は兼務で大丈夫だろう。

日本国内の企業や組織を狙ったサイバー攻撃が急増。情報資産を標的にした攻撃を封じ込めるためには エンドポイントに特化したセキュリティ専門家が必要。

Point
外部のアウトソーシングサービス活用で人材不足を解消。
サイバーリーズンでは、高度なスキルを持つサイバーセキュリティの専門家がお客様に代わり、
24時間365日体制でプロアクティブに監視。安心して日常業務に専念できる体制作りを支援。

大企業が選んだその実績。
シェアNo.1の機能そのまま、リーズナブルに。

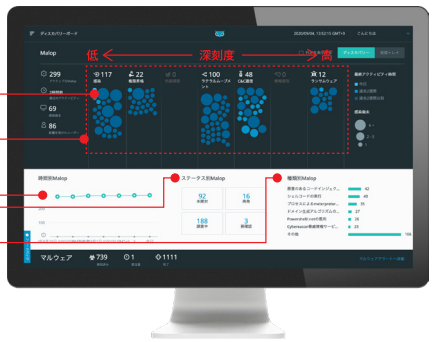
サイバーリーズンから、中堅企業向け 次世代エンドポイントセキュリティソリューションが誕生しました。

Cybereason Core Suite
Cybereason EDR Core

特徴1 「何が起きているか」を直感的に可視化

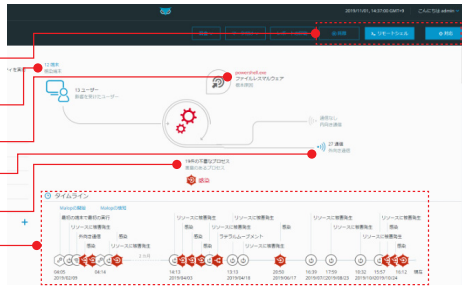
出社後まず
管理画面を開き、
検知バブルがなければ、
それで安心。

- 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



特徴2 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



特徴3 遠隔でも複数の端末に、ワンクリックで対応

遠隔から影響ある端末を
確実に即座に隔離。
業務上隔離できない端末には
個別の対応も可能。

- 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

特徴4 AIと相関解析で攻撃の全体像をあぶりだす

- 複数端末の相関解析
- 異常な振る舞いを絞り込み、検知
- AIによる異常検知と振る舞い分析
- 常時毎秒800万クエリをビッグデータ解析

Cybereason Core Suite

Cybereason Dual Core

あらゆるタイプのマルウェアに対応できる専用の防御層で情報資産を保護する真の次世代アンチウイルス
「Cybereason Endpoint Prevention Core（NGAV & Endpoint Control）」と
「Cybereason EDR Core」をセットでご提供。

Cybereason Endpoint Prevention Core
（NGAV & Endpoint Control）

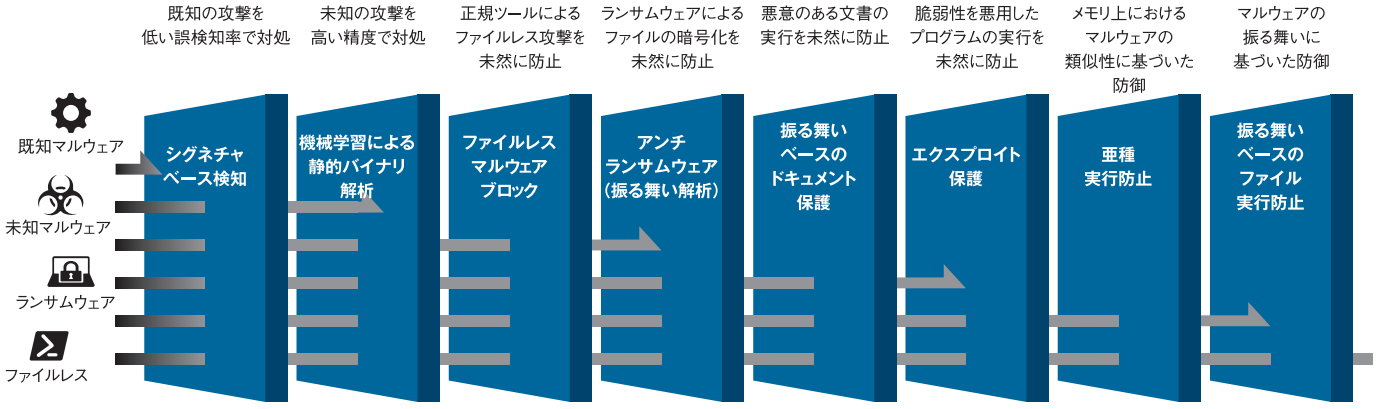
＋

Cybereason EDR Core

Cybereason Endpoint Prevention Core

次世代アンチウイルス 必須の8層

巧妙な攻撃を専用防御層でブロック



エンドポイントコントロール

組織内のすべてのエンドポイントを安全に管理

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
パーソナルファイアウォール	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	ディスクの暗号化を行っていない エンドポイント（Windows端末）を特定

※Endpoint Prevention Coreは、EDR Coreとセットになった「Cybereason Dual Core」で提供します。
※Cybereason Endpoint Prevention Core（次世代アンチウイルス）単体の販売はございません。

中堅企業向け 次世代エンドポイントセキュリティソリューション

Cybereason Core Suite製品ラインアップ

Cybereason EDR Core
アンチウイルスをすり抜けた攻撃を検知、対応

Cybereason Dual Core
Endpoint Prevention+EDR（次世代アンチウイルス）

IRリテイナー
インシデント対応代行

セキュリティヘルスチェック
組織内環境の検査

1 導入コスト 運用負荷を軽減

- シェアNo.1EDR機能をリーズナブルな価格で提供
- シェアNo.1の「Cybereason MDR」を中堅企業様向けに最適化、コストを押さえて提供
- 社内外の端末を一括監視
- 管理サーバーはクラウドなのでシステム構築は不要
- 日本語管理画面、レポート対応
- 「今攻撃を受けているか?」がひと目で分かる直感的な管理画面

2 専任者がいなくても 簡単に運用

- インシデント発生時、推奨対応方法をご案内
- ひと目で状況を把握でき、直感的に操作できる管理コンソール
- クリックするだけで深掘り調査が可能（SQLライクなクエリの習得不要）
- 封じ込め、端末隔離などの対処もワンクリックで遠隔から実行可能
- MSSPのSOCサービスがお客様のセキュリティチームの一部として機能し24/365監視

3 情報資産を保護する 運用重視のセキュリティ

- 第三者機関で高い検知率、可視性、リアルタイム性を実証
- 最先端の攻撃をふるまいベースで検出
- 「いつどこで何が起こったか?」を自動相関解析、可視化
- リアルタイムに攻撃の全体像を可視化
- 厳しいエンタープライズ環境で実績多数

Cybereasonの優位点

技術面

- 1エージェントで防御-検知-対応-復旧までを全カバー
- 攻撃の全体像をリアルアイムに可視化
- 攻撃された複数台の端末を遠隔から一度に対応可能

運用面

- 業務端末に影響しない
- 日本語画面とレポートで即座に把握
- 日本法人による強力なサポート体制

信頼の証。シェアNo.1を獲得

数々の強みを評価いただいている、サイバーリーズンのセキュリティソリューション。エンドポイントセキュリティにおいて国内No.1のシェアを獲得するなど、その卓越した機能やサービス品質の高さは、多くの企業・組織の皆様から信頼をいただいています。

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2022年度
サイバーセキュリティソリューション市場18版目」
https://mic-r.co.jp/mr/02630/

出典:IDC Japan株式会社
2022年12月発行「国内標的型
サイバー攻撃対策製品市場シェア、
2021年:SIEM 市場の成長」

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2022年度
サイバーセキュリティソリューション市場18版目」
https://mic-r.co.jp/mr/02630/

出典:株式会社アイ・ティ・アール
2023年1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2022」

出典:株式会社富士キメラ総研
2022年11月17日発行
「2022 ネットワークセキュリティビジネス
調査総覧（市場編）」 2021年度実績

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」

cybereason

Defend the Future

お問い合わせ

サイバーリーズン合同会社

本社　〒104-0031 東京都中央区京橋1-17-10 住友商事京橋ビル8F
西日本支社　〒530-0011 大阪府大阪市北区大深町1-1 LINKS UMEDA 8F
名古屋支店　〒453-6111 愛知県名古屋市中村区平池町4-60-12 グローバルゲート11F

www.cybereason.co.jp

取扱代理店