「ランサムウェア対策」
製品・サービス組み合わせ例

CASE 1

cybereason

脆弱性診断　侵入防止

脆弱性がどこにあるか調べて、最低限の対策をしたい

①セキュリティ診断サービス
②次世代アンチウイルス「Cybereason NGAV」

CASE 2

侵入対策　早期復旧・データ保護

被害にあった場合を想定して早急に復旧させたい

①次世代エンドポイントセキュリティ「Cybereason EDR」
②復旧対策ーPCの復旧にかかる時間を短縮「PC復旧・代替サービス」
③復旧対策ー改ざん不可ストレージでデータ保護「イミュータブルバックアップ構築サービス」

CASE 3

脆弱性管理　侵入対策　早期復旧・データ保護

脆弱性有無やパッチ更新を定期的に管理し、万が一の感染にも備えて対策をおこないたい

①脆弱性管理「Tripwire IP360」「Rapid7」
②パッチ管理「MCore」
③サイバー攻撃の全体像を可視化「Cybereason XDR」
④復旧対策ーPCの復旧にかかる時間を短縮「PC復旧・代替サービス」
⑤復旧対策ー改ざん不可ストレージでデータ保護「イミュータブルバックアップ構築サービス」

TRIPWIRE IP360　RAPID7　MCore　EXAGRID AUTHORIZED RESELLER

まずは、脆弱性があるのか診断しませんか？
お気軽にお問い合わせください。

(LS00059)

東芝デジタルエンジニアリング株式会社
E-mail : TDEN-sales@ml.toshiba.co.jp
https://www.toshiba-tden.co.jp

商品情報2025-03

TOSHIBA

ランサムウェア攻撃の脅威に”予防”、”対策”、”復旧”で備える

ランサムウェア対策 トータルソリューション

ランサムウェア対策は進んでいるが、被害が減らないのは‥なぜ？

事実1 エンドポイント対策だけでは攻撃は防げない！？

その通りです。
近年のランサムウェア攻撃は高度化しており、エンドポイントだけでなくネットワーク機器やOSの脆弱性を狙って侵入しています。したがって、組織のIT環境全体を包括的に保護するランサムウェア対策が必要です。

事実2 ウイルス対策ソフトだけでは攻撃は防げない！？

その通りです。
新しく巧妙なウイルスが次々と生成されるため、従来のファイアウォールやアンチウイルスソフトウェアだけでは完全に防御することが困難です。侵入を防ぐだけでなく、万が一侵入された場合でも被害を最小限に抑えるための事後対策が重要です。

貴社にあったランサムウェア対策をトータルで提案します。

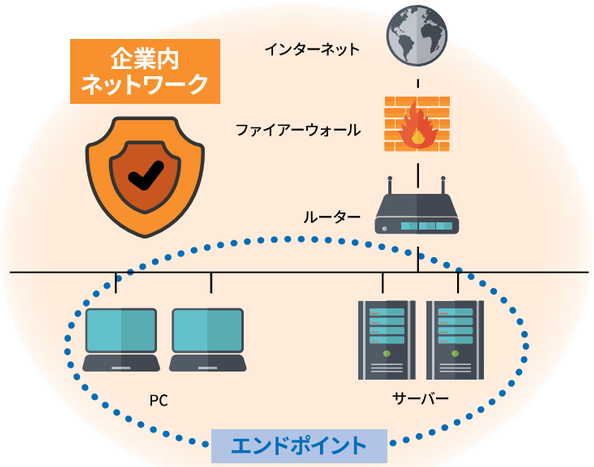
東芝デジタルエンジニアリング株式会社

ランサムウェア対策に求められる

2つの観点

Point 1 エンドポイントだけでなく 企業内ネットワーク全体の防止対策

多くの企業がインターネットに接続し、クラウドサービスなどさまざまなネットワークを利用する現代において、巧妙かつ進化を続けるランサムウェア攻撃から企業を守るためには、エンドポイントだけでなく、企業内ネットワーク全体での包括的な対策が求められます。



CHECK POINT

- 最新のネットワーク図の準備
- IT資産の全社管理
- 監視体制や報告ルートの策定

Point 2 侵入前だけでなく、侵入されても 被害を最小限にする感染対策

ランサムウェアの脅威から企業を守るためには、侵入されないための事前対策と もしも侵入されても被害を最小限におさえる事後対策、どちらも必要です。

CHECK POINT

- 攻撃後の初動対応手順の確立
- 復旧作業の優先順位方針策定
- 攻撃シミュレーション

製品・サービスラインナップ

事前対策

▶ 脆弱性管理

企業内ネットワーク

システム環境内に潜在する脆弱性や攻撃・侵入のリスクを診断し、可視化。対策の優先順位付けで管理者の負荷を軽減できます。

脆弱性診断 レポート作成 改善策の提案

- エージェントレスで企業ネットワーク全体をスキャン「Tripwire IP360」
- ITシステムの脆弱性を診断・管理「Rapid7」

どこから脆弱性対策を始めればよいかわからない！という場合には、

- 見えない脅威を見つけ出す、安心の「セキュリティ診断サービス」

をご利用ください。

TRIPWIRE® IP360
RAPID7

▶ パッチ管理

エンドポイント

- 企業のIT資産を一元管理し、セキュリティ対策やコンプライアンス遵守を強化「MCore」

MCore®

▶ 侵入防止

エンドポイント

- 8層の防御層で未知のマルウェアを未然に防止する次世代アンチウイルス「Cybereason NGAV」

侵入後の早期発見・復旧

▶侵入検知、隔離・拡散防止

企業内ネットワーク

ISMAP登録製品

- 侵入後の攻撃を振る舞いで検知する次世代エンドポイントセキュリティ「Cybereason EDR」
- IT環境全体のログを解析し、サイバー攻撃の全体像を可視化、攻撃を阻止「Cybereason XDR」

POC、構築、教育、など、サポートサービスも充実しています。

cybereason

▶ 個人情報流出対策

エンドポイント

- 個人情報などの重要情報を“探して”“暗号化”、万が一の流出時も情報を守る「Secure Protection」

▶ 復旧対策

エンドポイント

被害にあってしまった場合は感染経路の特定や被害拡大を防止するための緊急対応に時間が割かれます。業務再開を支援する復旧サービスをご利用ください。

業務中断期間の短縮

- 定期的にPCのマスターファイルを作成することで、復旧にかかる時間を短縮「PC復旧・代替サービス」
- 改ざん不可能なストレージでデータを確実に保護「イミュータブルバックアップ構築サービス」

EXAGRID AUTHORIZED RESELLER

運用監視

24時間365日体制 インシデント対応主導

- 脅威の特定と監視、脅威への対処、脅威の影響の低減を実現するアウトソーシングサービス「Cybereason MDR」

組織内にセキュリティオペレーションセンター（SOC）を設置したり、すでにあるSOCの規模やセキュリティ担当者の数を大幅に増やしたりしなくても、脅威に対処することができます。

cybereason