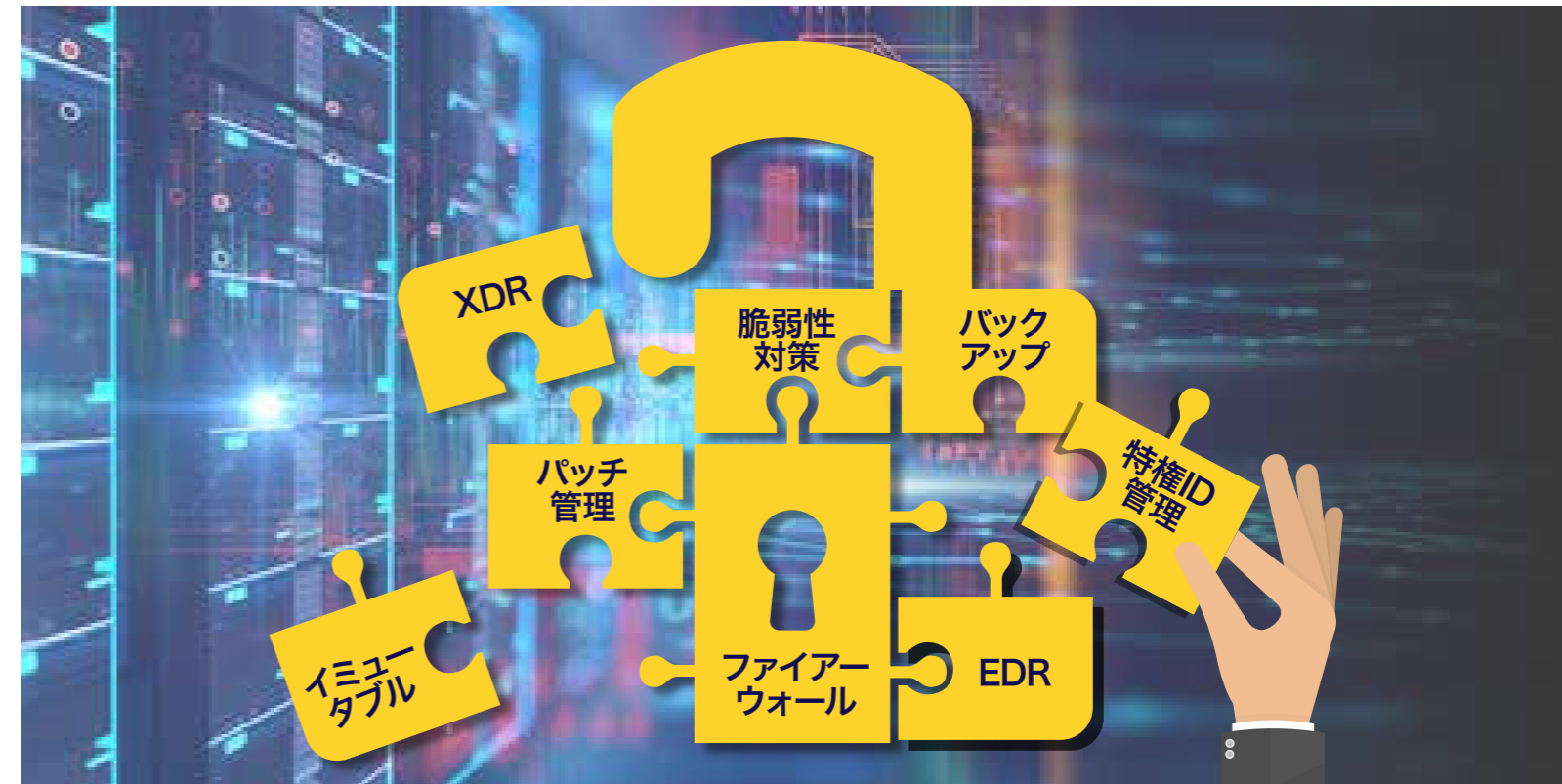


「ランサムウェア対策」 貴社が必要とする製品が必ずあります！

TOSHIBA

自社に必要なランサムウェア対策製品を選んで多層防御を実現

ランサムウェア対策ソリューションセレクト



貴社のランサムウェア対策は どこまで進んでいますか？

CASE 1 PCやサーバーのログインIDのアクセス権を管理していない

攻撃されます！
攻撃者は侵入後、IDの特権昇格して高度な操作をおこないシステム設定変更や機密情報を搾取して暗号化してしまいます。

特権ID管理ソリューションで事前対策しましょう

CASE 2 被害にあった場合が想定できていない

侵入前対策だけでは不十分です！
巧妙化するサイバー攻撃はアンチウイルスやファイアウォールなど従来の侵入対策をすり抜けて侵入し重要な情報の流出、破壊を仕掛けてきます。

今、必要とされるのは、"攻撃者は必ず侵入してくる"という前提に立った対策です

CASE 3 バックアップサーバーの攻撃対策ができていない

バックアップサーバーも暗号化されます！
毎日バックアップしていても、攻撃者によりデータ削除や書き換えなどがおこなわれてしまい、いざというときの復旧に利用できません。

イミュータブル(書き換え不可能な)機能を備えたストレージを使用したバックアップシステムを導入しましょう

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。

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。

貴社の対策を補うプラスワンの製品・サービスを提案します。

□本文中の会社名および製品名は各社が商標または登録商標として使用している場合があります。
□本資料は内容は予告なく変更される場合がありますのでご了承下さい。

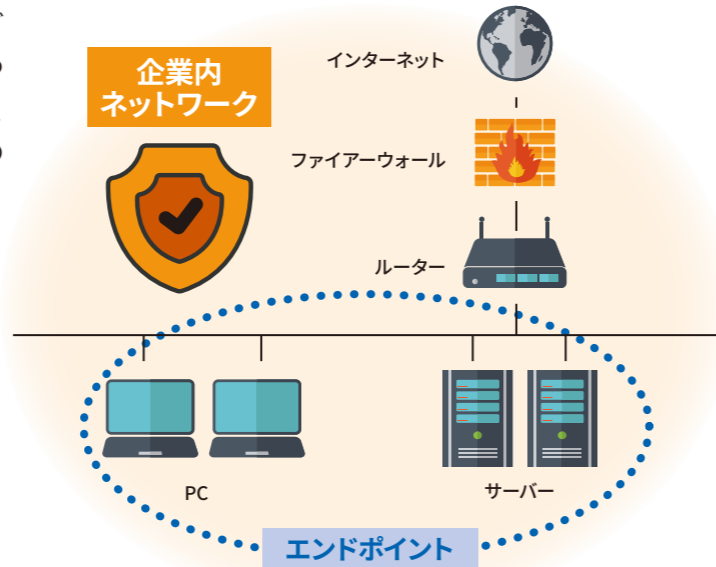
(LS00059)

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

- ・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」
- ・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」

脆弱性診断 レポート作成 改善策の提案



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」



特権ID管理

エンドポイント

- ・不正アクセス・改ざん・情報漏洩の予防に必要な特権ID管理とIT統制・監査を実現「iDoperationシリーズ製品」



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

- ・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。

ISMAP登録製品



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」
- ・改ざん不可能なバックアップでデータを確実に保護「イミュータブルストレージサービス」

運用監視

- ・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」

24時間365日体制 インシデント対応主導

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。

