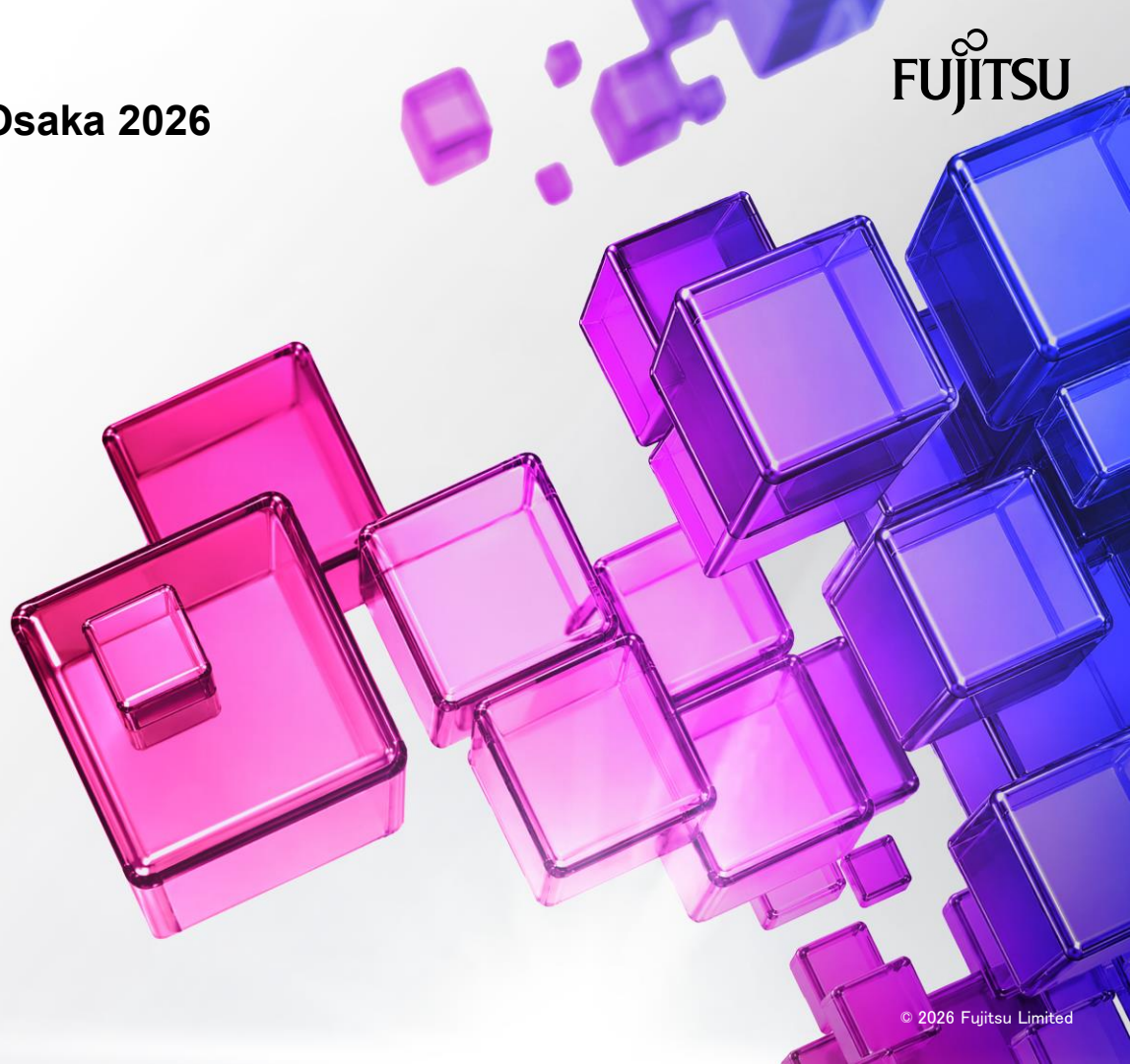


AI時代における サイバー脅威の変化と 企業が取るべき対策



AIによるサイバー脅威の変化

AIにより、「スピード」と「量」の両面でサイバー脅威が大きく変化しています。

AIによる攻撃の自律化

攻撃を検出してから人が判断する防御では、攻撃のスピードに対応できない。

急増する脆弱性報告件数

ゼロデイを含む脆弱性報告件数が急増。もはや脆弱性を個別に評価・対応するだけでは限界。

脆弱性公開後、即攻撃

脆弱性情報公開後、すぐに攻撃へ悪用されるため、人による判断・検証・パッチ適用では間に合わない。

今、すぐに求められる対応

脆弱性対応の強化

- 自組織の資産を把握して資産に存在する脆弱性を検出して評価
- パッチ適用までを完了させる一連を業務として確立することは、AIによるサイバー脅威への対策の前提であり、急務

今後求められる対応

AIを活用した防御

AIを活用したセキュリティ防御の高度化が必要

- 脆弱性の悪用リスク評価の高速化
- パッチ適用の自動化
- SOC運用へのAI組み込み

脆弱性対応の強化

課題



フロンティアAIの脅威

AIによる脆弱性の発見と攻撃の高速化



自社のリスクが把握できてない

IT資産・外部表出リスクの未把握



増え続ける脆弱性への対応

対策すべき脆弱性の優先度付けが難しい

解決策

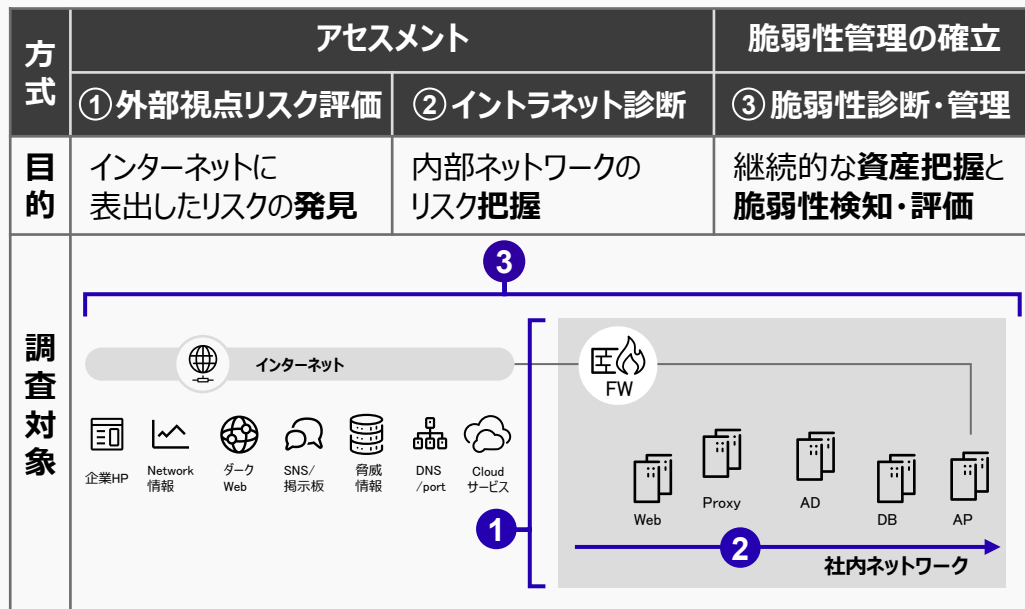
攻撃者視点での自社の状況把握

- ・ 侵入口となる外部表出リスク可視化

継続的に対処できる仕組みの導入

- ・ IT資産の継続的な把握・脆弱性検知

アセスメント（現状把握）～脆弱性管理の確立
（継続的に対処できる仕組みの導入）までご支援



「リスクを把握して先回りする」セキュリティへ

公共領域における セキュリティ対策サービス



次期ネットワークを見据えた第三期強靱化対策

課題

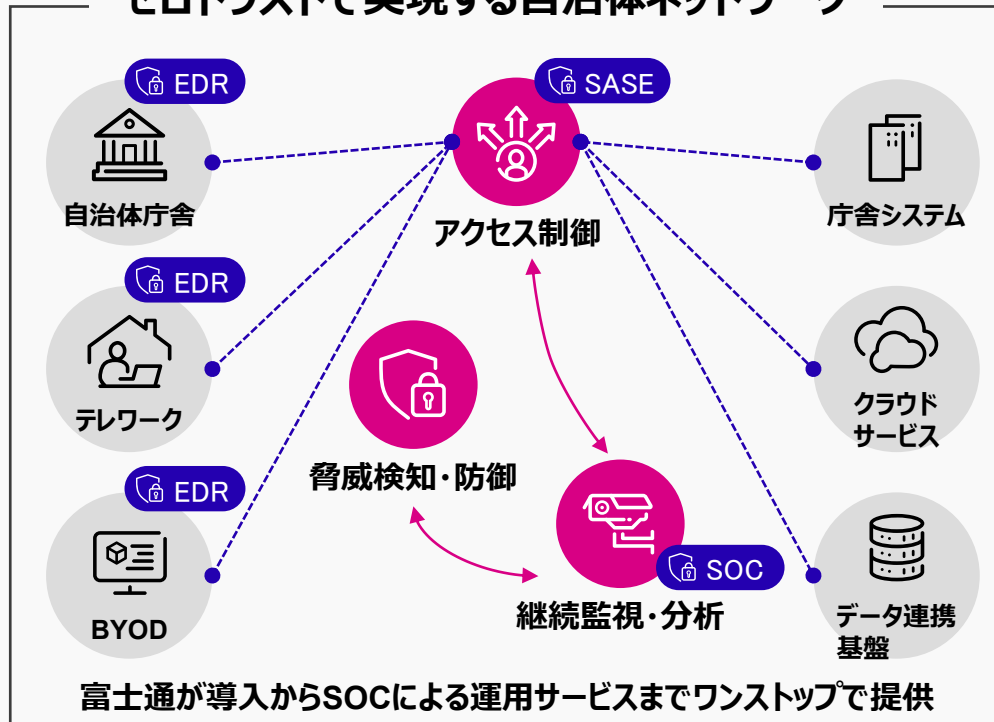
-  **M365等SaaS利用の増加**
端末セキュリティの強化が必要
-  **クラウド活用と三層分離の両立**
クラウド活用と三層分離運用の両立が必要
-  **セキュリティ運用人材の不足**
高度化する監視運用への対応

解決策

EDR・SASE・SOCの連携で、ゼロトラストと高度なセキュリティ運用を実現

- 端末でのサイバー脅威の早期検知
- 安全なクラウド利用とアクセス統制
- 継続的な監視による運用負荷軽減

ゼロトラストで実現する自治体ネットワーク



2030年の自治体ネットワーク将来像に向けたゼロトラストの段階的導入を

診療を止めないためのランサムウェア対策

課題



攻撃の高度化

VPNの脆弱性悪用、横展開



医療機器やネットワークの複雑化

侵入経路の把握



監視運用の人材不足

アラートが出ても判断できない

解決策

安全なリモートアクセスを実現し、 万一の侵入後の検知・運用体制を整備

- ・ 保守接続・リモートアクセスを統制
- ・ 端末・サーバの不審な挙動を検知
- ・ 院内ネットワークの異常を検知
- ・ インシデント発生時の早期対応

安全なアクセス制御と多層防御により診療を継続

セキュアリモートアクセス



外部接続ルート統制
不正アクセスを防止

EDR | 端末・サーバ



挙動検知・端末隔離

NDR | 院内ネットワーク



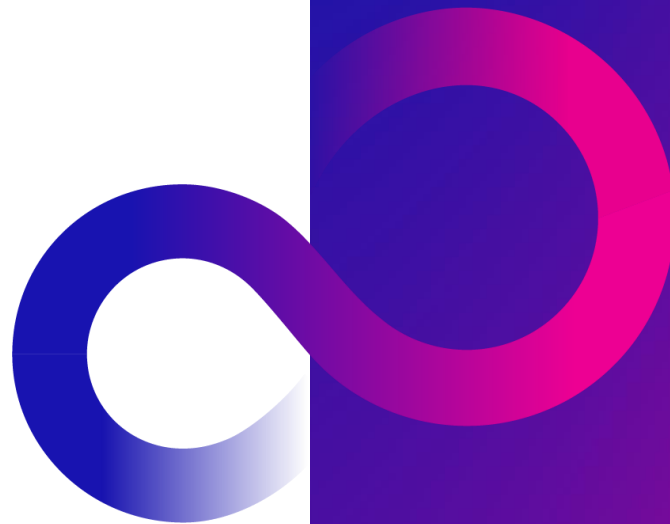
異常通信・横展開検知

SOCサービス



富士通SOCによるセキュリティ監視・
運用サービスをオールインワンで提供

もし明日、ランサムウェアに感染しても診療を継続できますか？



＜お問い合わせ先＞

セキュリティに関するお問い合わせフォーム

<https://contactline.jp.fujitsu.com/contactform/csque04701/821681/>

右記QRコードよりお問い合わせください。

