

サイバー防御力検査とレジリエンス力向上サービス

最近のサイバー攻撃事例と被害の拡大(多様化と被害の急増)

サイバー攻撃の被害は、システム障害・業務停止にとどまらず、大規模・高価値な個人情報漏えいへと拡大しています。

1 アサヒグループ | 2025年9月

ランサムウェア攻撃



- ネットワーク機器から侵入し、管理者権限を奪取して内部を探索
- 複数サーバー等を暗号化し、システム障害・業務に影響



事業継続への影響

受注・出荷など広範な業務に影響

2 タイムズカー | 2026年9月

Webシステムへの不正アクセス



- 約 **660万** アカウントの情報漏えい
- 氏名、住所、生年月日、電話番号、メールアドレス、運転免許情報など
- 約 **160万** 件で運転免許証画像等の本人確認書類も漏えい



なりすましにつながる高価値情報
運転免許証等の本人確認書類が漏えい

3 焼肉きんぐ | 2026年10月

会員管理システムへの不正アクセス



- 約 **1,079万** 件の会員情報漏えい
- 会員番号、氏名、メールアドレス、電話番号
- パスワード・決済情報は漏えい対象ではない



1,000万件規模の大量漏えい
大量の連絡先情報が流出

サイバー攻撃による被害領域の拡大



システム障害・ 業務停止

- ランサムウェアによるシステム停止
- 生産・受注・出荷など業務への影響



大規模な 個人情報漏えい

- 数百万～1,000万件規模の情報漏えい
- 氏名・住所・電話番号・メールアドレスなど



本人確認情報の 流出

- 運転免許証画像など本人確認書類の漏えい
- なりすましの精度が大幅に向上



なりすまし・フィッシング等の 二次被害リスク

- フィッシング・SMS詐欺などの被害増加
- 他の漏えい情報との組合せによる標的型攻撃
- 経済的被害・信用の失墜



重要なポイント

被害評価は「攻撃を受けたか」だけでなく、

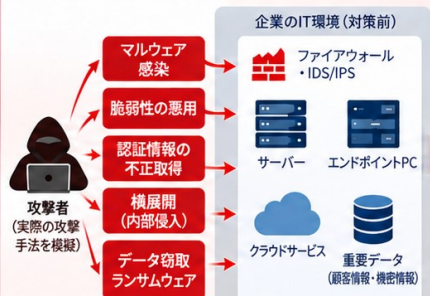
「事業への影響」「漏えい件数」「漏えい情報の重要度」「二次被害」まで評価する必要がある。

PiCUSの疑似攻撃によるペネトレーションテストで現状のリスクとAppGuardによるレジリエンス力強化の効果を検証

実際の攻撃手法を模した疑似攻撃で、「防ぐ力(現状)」「止める力(AppGuard)」「全体のレジリエンス」を可視化します。

1 現状のリスク(対策前)

攻撃が侵入・拡大し、被害につながる可能性

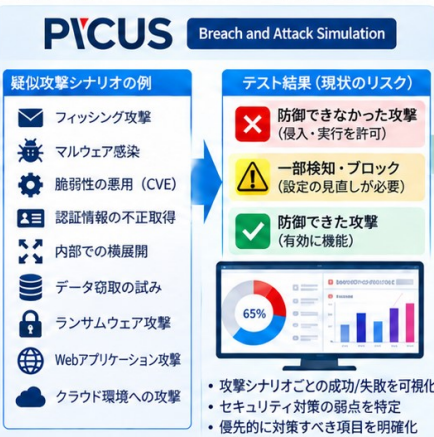


想定される被害

- システム停止・業務遅延
- 機密情報・個人情報の漏えい
- ランサムウェアによる暗号化・金銭被害
- 信頼の低下・ブランド価値の毀損

2 PiCUSによる疑似攻撃テスト

実際の攻撃シナリオを模したテストで防御状況を可視化



3 AppGuardによるレジリエンス検証

侵入・マルウェア実行時の被害拡大を防ぐ効果を検証



この取り組みで
得られる効果



現状の防御力を可視化

- 実際の攻撃手法に対する現状の防御能力を把握
- 弱点(対策すべき箇所)を特定



優先すべき対策の洗い出し

- セキュリティ対策の強化
- 設定見直し・追加対策の検討



AppGuardによる レジリエンス力強化

- 侵入後のマルウェアの実行・被害拡大の防止
- 攻撃を受けても業務継続できる環境へ



継続的な検証・改善

- 定期的なPiCUSによるテストで効果を確認
- 変化する脅威に対し、継続的にレジリエンス力を維持・向上

サイバー防御力診断

診断サービスで用いられるサイバー攻撃

CVEベースの脆弱性Exploit

ランサムウェアなど悪意のあるコード

OWASP TOP10 Webアプリの攻撃

悪意のある添付メール
悪意のあるURLが付いたメール

MITRE ATT&CK
マルウェアの振る舞い

データ漏洩

診断サービスによってわかること

セキュリティ上の弱点

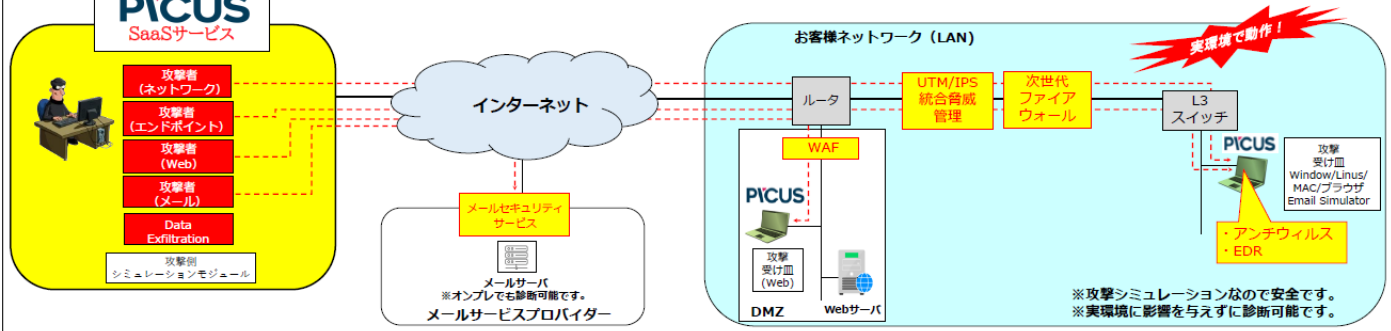
流行っているサイバー攻撃への対応度

将来どのようなセキュリティ対策へ投資すべきか

セキュリティにおける設定ミスや設定漏れ

SIEMへ統合されるセンサの妥当性

防御診断サービスイメージ図



サイバー防御力診断結果*

従来型サイバー防御とAPPGUARDによるサイバー防御の比較

セキュリティデバイス防御性能サービスレポート

【対策前】エンドポイント診断 (結果抜粋)

脆弱性診断ツール

PICUS

T社 アンチウイルス

セキュリティスコア
(防御数/総攻撃数)

総攻撃数

防御数

防御しなかった数



41% ↓ 3
SECURITY SCORE



8730 ↑ 39
TOTAL THREAT



3601 ↓ 239
BLOCKED



5129 ↑ 278
NOT BLOCKED

【対策後】エンドポイント診断 (結果)

T社アンチウイルス+次世代AV A社

セキュリティスコア
(防御数/総攻撃数)

総攻撃数

防御数

防御しなかった数



96% ↑ 96
SECURITY SCORE



9004 ↑ 9004
TOTAL THREAT



8679 ↑ 8679
BLOCKED



325 ↑ 325
NOT BLOCKED

* 2022年度防衛装備庁サイバーセキュリティ対策強化事業

侵入した脅威を発症させることなく無害化

AppGuardによる無害化例

