優先すべきサイバーセキュリティはどれ？

技術 組織 人

3種の脆弱性と対策

AMIYA

目次

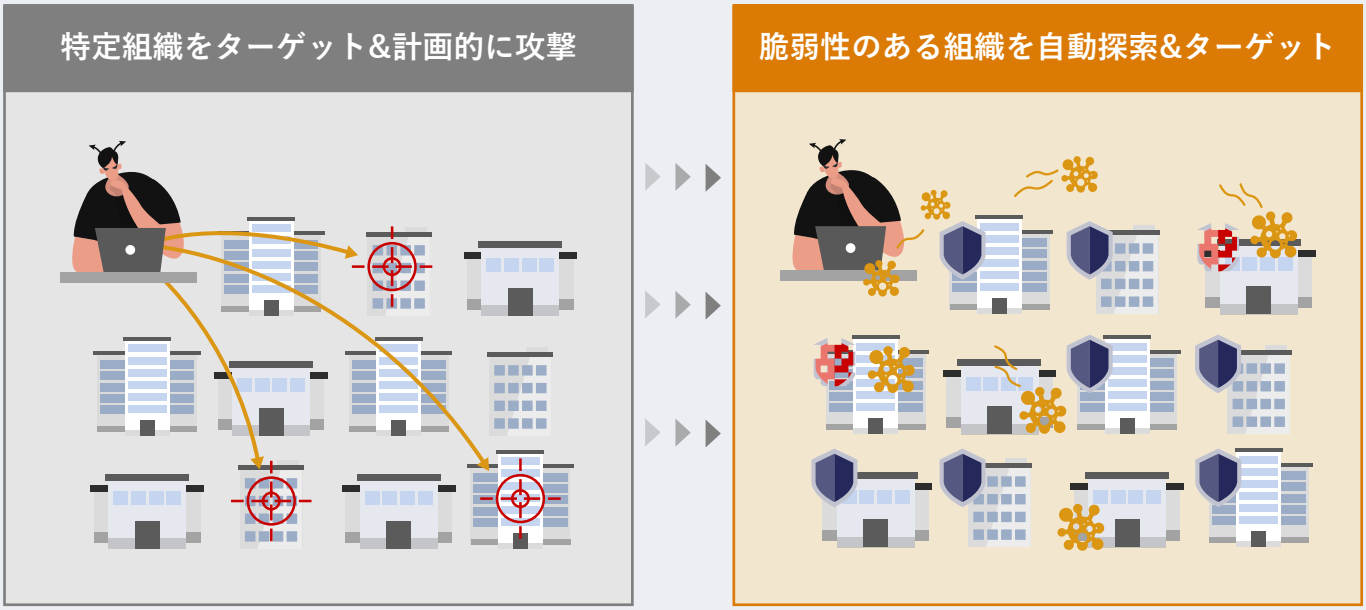
はじめに

サイバー攻撃は「脆弱性」から

01

年々激しさを増すサイバー攻撃。ランサムウェア被害件数は、２年間で5.5倍までに増加しています、（警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」）
被害件数増加の背景にあるのが、サイバー攻撃手法の変化です。かつては特定の大企業をターゲットに計画的に攻撃を行っていたサイバー攻撃ですが、現在では、「脆弱性」のある組織を自動探索し、無差別に攻撃を行うように変化してきています。

ランサムウェア被害件数は2年で5.5倍に



※ 出典：警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」

新たな攻撃手法の入口となる「脆弱性」とは、コンピュータやソフトウェア、ネットワークなどが抱えるセキュリティ上の弱点のことを指します。「脆弱性」が存在すると、サイバー攻撃者は「脆弱性」を悪用し、組織のネットワークへ不正アクセスして機密情報を盗み出したり、ランサムウェアなどのマルウェアに感染させたりします。
セキュリティ上の大きな脅威となる「脆弱性」。独立行政法人情報処理推進機構 (IPA) が発表した情報セキュリティの10大脅威のうち８つが、「脆弱性」が起因となる脅威となっています。しかし言い換えれば、適切な「脆弱性」対策を施せば、多くのセキュリティ脅威を回避することができると言えます。

しかし、具体的に何から対策を講じるべきかわからないという方も多いでしょう。本書では、脆弱性の対策方法について、具体的に紹介します。

脆弱性が原因

順位	「組織」向け脅威
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）

出典：独立行政法人情報処理推進機構 (IPA) 情報セキュリティ 10 大脅威 2023
https://www.ipa.go.jp/files/000108838.pdf

02

技術的な脆弱性だけじゃない！

「脆弱性」の3つの種類

一般的に「脆弱性」というと、システムやプログラムなどの技術的な欠陥をイメージするのではないでしょうか。しかし、実際のセキュリティインシデントの原因は、システム的な脆弱性だけではありません。インシデントの原因となる「脆弱性」は、大きく分けると以下の３つの種類があります。

1 技術的な脆弱性

ITシステムにおいての、プログラムの不具合や設定ミスなどの技術的な欠陥です。例えば、ソフトウェアにおいて技術的な脆弱性が発見されると、開発元から修正プログラムが発表されますが、利用者が修正プログラムを適用せず脆弱性を放置すると、攻撃に悪用される恐れがあります。新たに発見される技術的な脆弱性の数は年々増加しており、脆弱性を残存させた場合のリスクは増大していると言えるでしょう。

2 組織的な脆弱性

機密情報の管理体制やセキュリティの運用プロセスなどの組織的な欠陥です。例えば、サーバ設定の検証体制が適切でなく、公開されるべきでないサーバが外部公開されている、インシデントが起こった際に適切な初動対応を実施できる体制にない、などの、適切なプロセスでITシステムを管理・運用できていな欠陥がこれに当たります。

3 人的な脆弱性

従業員の不安や焦りの感情、セキュリティ意識の欠如に起因する心理的なの欠陥を指します。例えば、不注意により従業員が不審なメールのURLにアクセスしてしまい、ランサムウェアに感染してしまう、などの脅威があります。また、ソーシャルエンジニアリングやフィッシングなどの攻撃手法にも人的な脆弱性が悪用されます。

03

脆弱性の対策方法

では、サイバー攻撃に悪用されるこれらの脆弱性の発生を抑制するには、具体的にどのような対策を施せばよいのでしょうか。ここでは、脆弱性の発生を防ぐために必要な対策をご紹介します。

技術的な脆弱性

ITシステムの脆弱性を把握し、修正プログラムを適用する

技術的な脆弱性を悪用する攻撃は、修正プログラムの公開後に増加します。日々脆弱性情報を収集・把握し、修正プログラム公開後可及的速やかに修正プログラムを適用し、脆弱性を無くしましょう。

組織的な脆弱性

ポリシーを作成し適切に運用する

適切なプロセスでITシステムを管理・運用するには、ポリシーの明文化と運用が重要です。ポリシーに沿ったセキュリティ運用により、組織全体で統制がとれたセキュリティ対応が可能になります。

CSIRT組織を設置する

インシデントの利益損失の多くは発生後に生じるため、被害の最小化には迅速な検知・復旧対応が必要不可欠です。インシデント対応が可能なCSIRTを設置して万一の事態に備えましょう。

人的な脆弱性

従業員のセキュリティ意識を向上させる

セキュリティ教育の実施により従業員の意識改革が必要です。従業員のセキュリ ティ意識向上により、人的な脆弱性に起因するサイバー攻撃を予防し、被害を抑制することが可能です。

これらの適切な脆弱性対策により、多くのセキュリティ脅威を回避することができます。しかし、自社で対策を実施するには、

- 自社で実施するノウハウがない
- 自社内で実施する時間がない
- 正しく実施できているかどうかわからない

などの課題を抱えている企業様も多いのではないでしょうか。

AMIYA

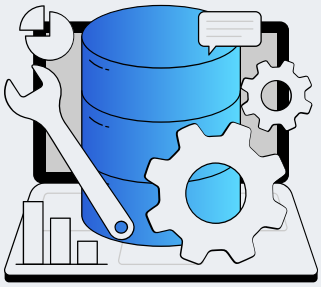
サイバーセキュリティサービス

そんな脆弱性対策の課題を解決するのが、AMIYAサイバーセキュリティサービスです。技術的・組織的・人的脆弱性の発生を防ぐ包括的なセキュリティサービスを一貫して提供。自社での対策の実施が難しい企業様のセキュリティ対策を支援いたします。

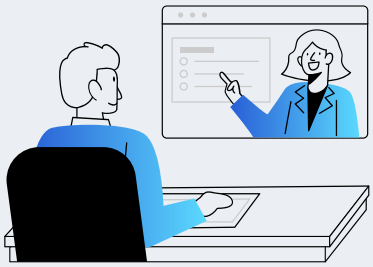
サイバーセキュリティサービス

AMIYA Security

コンサルティング



セキュリティ診断



教育・トレーニング

特定	防御	検知	対応	復旧
アタック サーフェイス調査	EDR導入	ALog MDRサービス		フォレンジック サービス
脆弱性調査	ゼロトラスト コンサル/導入/運用	EDR運用サービス	インシデントレスポンス コンサルサービス	
セキュリティ監査	セキュリティ トレーニング			ランサムウェア 対策バックアップ
セキュリティ 設定診断	標的型攻撃 メール訓練			
CSIRT構築 コンサルサービス				

何から対策すればよいかわかる！

サービスラインナップ

05

技術的な脆弱性　Level 1　ITシステムの脆弱性の把握と対策

概要資料を無料 DL

脆弱性診断サービス

ITシステムの脆弱性調査とその対策案を提供するプラットフォーム脆弱性診断サービス。
専任のエンジニアが脆弱性を洗い出し、アフターフォローまでを一貫して提供。
対策すべき脆弱性を発見し、技術的な脆弱性を悪用するサイバー攻撃のリスクを低減します。

専任のエンジニア

サイバー攻撃者と同じ目線で
お客様環境を診断

レポート / 報告会

組織的な脆弱性　Level 2　ポリシーの作成と適切な運用

概要資料を無料 DL

セキュリティ監査サービス

公的資格を有するセキュリティスペシャリストが、ポリシーやレギュレーションへの対応状況をチェック。セキュリティリスクの洗い出しから実際の対策へ繋げることで、組織のセキュリティレベルが向上します。

公的資格を有する
セキュリティスペシャリスト

- CISA（公認情報システム監査人）
- 情報処理安全確保支援士

ギャップ分析 / 評価

- セキュリティポリシー
- 各種ガイドライン（ISO/IEC 27001 等）
- 対応の実態

レポート / 報告会

- 監査チェックリスト
- 監査計画書 / 報告書
- ポリシー改定案

何から対策すればよいかわかる！

サービスラインナップ

組織的な脆弱性　Level 3　CSIRT組織の設置

概要資料を無料 DL

CSIRT構築支援サービス

お客様それぞれに最適なCSIRTを構築するCSIRT構築支援サービス。
構築プロジェクトの立ち上げから運用・評価まで一貫してご支援。
万が一の際に”動ける”組織へと導きます。

サービス範囲

プロジェクトの立上げ	• 目的の明確化（CSIRT構築のきっかけ） • プロジェクト構成メンバーのアサイン • スケジューリングや運用ルールの明確化、意思決定フローの確認
現状・問題把握	• 現状の情報を収集（既存の体制や守るべき資産、脅威等の把握） • 問題の洗い出し（提供すべきサービスや CSIRTの配置組織、規模感等）
CSIRT構築計画・構築	• CSIRT構築計画書の作成 • 経営層 / 意思決定層の承認とリソースの確保 • CSIRT体制整備と必要文章の作成、社内説明
CSIRT運用前準備・開始	• インシデントシナリオの作成と机上シミュレーション • 社内 / 社外への周知、CSIRTサービスの提供開始 • 社外連携体制の確立
再検討	• CSIRT 活動の分析 • ポリシーやマニュアル、提供サービスの見直し

何から対策すればよいかわかる！

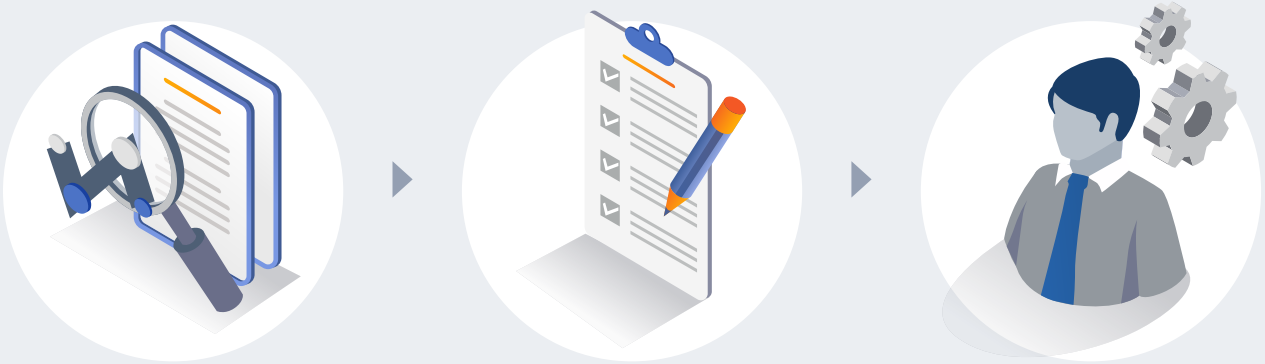
サービスラインナップ

人的な脆弱性 Level 2 セキュリティ意識の向上

概要資料を無料 DL

情報セキュリティ教育

セキュリティ教育に必要な三つのステップを一貫して提供する、
フルラインナップのセキュリティ教育プログラム。
社員のセキュリティ意識を最大化し、セキュリティの強い組織へと導きます。



知る　実践する　自ら考える

人的な脆弱性 Level 2 セキュリティ意識の向上

概要資料を無料 DL

標的型攻撃メール訓練

猛威を振るう「標的型メール攻撃」を疑似体験する標的型攻撃メール訓練。
AMIYAのトレーニングでは、攻撃メールを送信してリアクションを確認するのみならず、
その後のセキュリティ教育までをセットで実施し、訓練の効果を最大化します。

セキュリティ講習とセットで効果を最大化

安全な標的型攻撃メールを送信 ▶ 対象者のリアクション ▶ 結果を確認（報告書） ▶ セキュリティ講習 ▶ 理解度テスト

06

おわりに

サイバー攻撃対策は脆弱性対策から

多くのセキュリティ脅威の入口となる「脆弱性」。多くの脅威の入口となるからこそ、技術的な脆弱性だけでなく、組織的・人的脆弱性も含めたあらゆる脆弱性に適切な対策を施せば、セキュリティ被害に遭うリスクを大きく低減することができます。
AMIYAは、長年お客様のセキュリティ課題をコンサルティング・解決してきたノウハウを生かし、「今抱えているセキュリティ課題を相談したい」「自社に必要なセキュリティ対策がわからない」といった、セキュリティのお悩み相談も無料で受け付けております。
お気軽にお問い合わせください。

AMIYA

お問い合わせ

お申し込みや詳しいサービスのご紹介をご希望の方は以下にお問い合わせください

電話でのお問い合わせ
03-6822-9996

メールでのお問い合わせ
bv-sales@amiya.co.jp

株式会社網屋 データセキュリティ事業部

Secure the Success.

網屋の事業は、セキュリティ。

セキュリティ製品やサービスを自ら開発・製造・販売する、セキュリティの総合プロバイダです。

サイバー攻撃は、経済的余裕度に関係なく、全ての事業法人がターゲットになります。

サイバー攻撃の脅威を「セキュリティの自動化」で解決し、

高水準のセキュリティを誰でも享受できる社会を創りたい。

それが私たちのアイデンティティです。

AMIYA

株式会社 網屋

https://www.amiya.co.jp/

〒103-0007
東京都中央区日本橋浜町3-3-2
トルナーレ日本橋浜町 11F
TEL: 03-6822-9999
FAX: 03-6822-9998