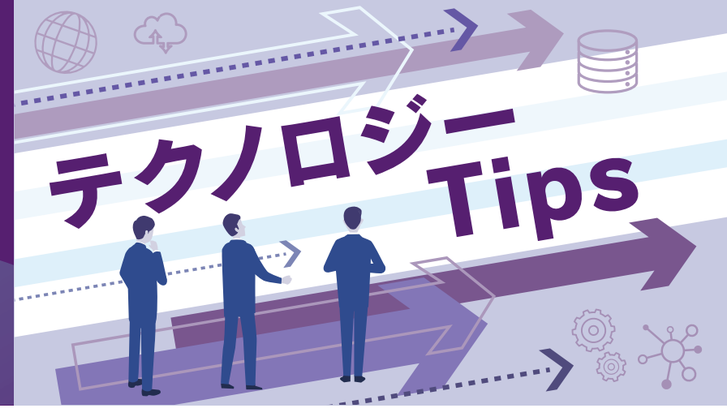
今こそ知りたい
＼ Tech Tips! ／
vol.23
(Ver2.0)

世界が大きく変わる中、さらにセキュリティ対策は重要になってきています!
対策方法やソリューション・デバイスをしっかり整理しました。

企業が講じるべきセキュリティ対策「Essential Guide」

攻撃の多様化、巧妙化、高度化、国家戦略サイバー攻撃、地政学リスクなどなど…
ICTやデジタル化が進む中、セキュリティに対するリスクは増加の一途です…



基本：その1

なぜ企業はセキュリティ対策をしなければならないのでしょうか？
当たり前のことですが、しっかり踏まえておきましょう。

❶ 事業継続そのものへのリスク	サイバー攻撃や情報漏洩は、システム停止、データ損失、風評被害を引き起こし、事業継続を困難にするため。
❷ 大切なお客様・取引先の信頼維持のため	情報漏洩はお客様や取引先の信頼を失墜させ、ビジネス関係に悪影響を与えるため。
❸ 法的義務の遵守のため	個人情報保護法や関連法規により、適切なセキュリティ対策が義務付けられているため。
❹ 経済的損失の回避のため	損害賠償、復旧費用、機会損失など、セキュリティ事故による経済的損失は甚大になるため。
❺ 企業価値の維持・向上のため	安全な事業運営は企業の評価を高め、競争優位性につながるため。

基本：その2

近年、特に企業を取り巻く環境はセキュリティの強化を迫られています。
なぜでしょうか？複合的な要因をトピックで整理してみましょう。

❶ 攻撃手口の多様化と高度化
ランサムウェア、標的型攻撃、サプライチェーン攻撃など、巧妙な手口が進化し、あらゆる企業が脅威に晒されている。

❷ AI進化による新たな脅威
攻撃の自動化、高度な標的型攻撃、セキュリティ欺瞞、ディープフェイクによる偽情報・なりすましなど、新たなリスクが増大。

❸ 地政学リスクと国家戦略としてのサイバー攻撃
国際情勢の緊張により、国家レベルの高度なサイバー攻撃リスクが増加し、企業インフラや機密情報が標的となる可能性。

❹ デジタルテクノロジー進化と情報の価値向上
クラウド、IoT、5Gなどの進化が新たな攻撃対象と脆弱性を生み出し、企業が持つ貴重な情報が攻撃者にとって魅力的な標的に。

❺ デジタルデータ量の爆発的増大
ビッグデータなどの増大によりデータ管理が複雑化し、セキュリティ上の脆弱性が生じやすい状況。

❻ 通貨・資産のデジタル化
暗号資産やデジタル資産の増加により、サイバー攻撃が直接、経済的損失に繋がるリスクが高まっている。

これらの要因が複合的に作用し、企業は事業継続、顧客信頼、法的義務、経済的損失回避、企業価値向上のため、より強固なセキュリティ対策を講じる必要に迫られています。

セキュリティ対策を強化するには、「人や組織のマネジメント・教育」と「技術的要素、つまりデバイスやソリューション」の2つの視点から対策を講じることが重要です。まずは人や組織への対策を整理しましょう。

❶ Plan! セキュリティ意識の向上と行動規範の明確化

経営層のコミットメントの下、基本方針を策定し全従業員に周知徹底します。
パスワード管理、情報共有、外部媒体利用に関する具体的なルールを定め、分かりやすいマニュアルを作成します。
これらは定期的に見直し更新し、グループウェアや説明会などを活用して繰り返し周知し、理解を深めます。

❷ Do! セキュリティ知識レベルの向上と適切な行動の促進

従業員の役割や職種に応じた研修プログラムを実施し、最新の脅威や対策に関する定期的な教育を行います。
標的型攻撃メールへの対策勉強会やインシデント発生への対応手順の徹底を通じて実践的なスキルを向上させ、日常的な注意喚起と研修効果の測定・改善を行います。

❶ Checkと監査 (Action) 運用状況の確認と継続的な改善

セキュリティポリシーやルールの遵守状況を内部監査し、必要に応じて外部専門家による脆弱性診断で弱点を把握します。
従業員からの意見やインシデント発生時の分析に基づき対策を見直し、その結果を経営層へ定期的に報告することで、PDCAサイクルを回し継続的な改善を図ります。

次に、中小企業が講じるべき物理的な対策を、デバイス、ソフトウェア、ソリューションの観点から整理します。ネットワーク境界防御と内部対策、エンドポイントセキュリティなど、様々な対策を紹介します。

UTM（統合脅威管理アプライアンス）

- ファイアウォール：不正な外部からのアクセスを遮断し、許可された通信のみを通過させる。
- アンチウイルス/アンチマルウェア：ネットワークを通過するファイルや通信を検査し、悪意のあるコードを検知・駆除する。
- 不正侵入防御（IPS/IDS）：ネットワーク上の不審な挙動を監視し、不正な侵入や攻撃を検知・防御する。
- Webフィルタリング：従業員がアクセスすべきでない有害なWebサイトへのアクセスを制限する。
- スパムフィルタリング：受信メールから迷惑メールやフィッシングメールを排除する。
- VPN（仮想プライベートネットワーク）：リモートワーク環境から安全に社内ネットワークへ接続するための暗号化されたトンネルを提供する。

次世代ファイアウォール（NGFW）

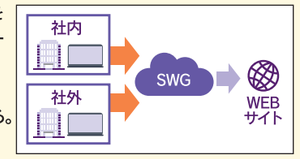
- UTMの機能に加え、アプリケーションレベルでの制御、高度な脅威インテリジェンスとの連携、サンドボックス機能などを備え、より高度な攻撃に対応する。

サンドボックスとは？

例えるなら「隔離された安全な実験室」のようなものです。危険かもしれないものを安全な場所で試したり、調べたりするための、コンピュータの中の特別な隔離空間のことです。これを使うことで、私たちは安心して新しいファイルやプログラムを扱うことができるようになります。

セキュアWebゲートウェイ（SWG）

- プロキシサーバーの機能に加え、Webアクセスにおける脅威防御、URLフィルタリング、マルウェア検査、情報漏洩対策などを包括的に行う。
- Web経由のマルウェア感染や情報漏洩リスクを低減する。
- クラウドサービスの利用状況を可視化し、セキュリティポリシーを適用する。
- リモートワーク環境におけるWebアクセスも安全に管理する。



ネットワークセキュリティ対策のためのデバイス：L2/L3スイッチ

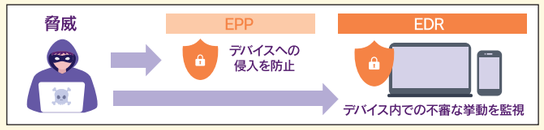
- VLAN（仮想LAN）：ネットワークを論理的に分割し、部門や役割ごとにアクセス範囲を制限することで、内部での不正アクセスやマルウェアの拡散を抑制する。
- MACアドレスフィルタリング：許可されたMACアドレスを持つデバイスのみネットワークへの接続を許可する。
- ポートセキュリティ：各ポートに接続できるMACアドレス数を制限し、不正なデバイスの接続を防ぐ。
- IEEE 802.1X認証：ポートへの接続時にユーザー認証を必須とし、未許可のデバイスの接続を防ぐ。

EPP（Endpoint Protection Platform）

- PC、サーバーなどのエンドポイントにインストールするセキュリティソフトウェア。
- アンチウイルス / アンチマルウェア：ファイルやプロセスの監視、シグネチャベースおよび振る舞い検知による悪意のあるコードの検知・駆除。
- ファイアウォール：エンドポイントごとの不正な通信を制御する。
- デバイス制御：USBメモリなどの外部デバイスの利用を制限する。
- 脆弱性対策：ソフトウェアの脆弱性を悪用した攻撃を防御する。

EDR（Endpoint Detection and Response）

- EPPの機能に加え、エンドポイントの活動を継続的に監視・記録し、不審な挙動を早期に検知・分析、対応を支援する。
- 侵入後の脅威を早期に発見し、被害拡大を防ぐ。
- インシデント発生時の原因究明や復旧作業を支援する。
- リモートワーク環境のエンドポイントにおける脅威も可視化する。

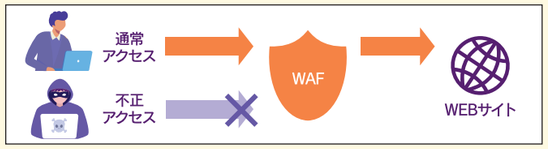


モバイルデバイス管理（MDM）/ 統合エンドポイント管理（UEM）

- スマートフォンやタブレットなどのモバイルデバイスや、PCなどのエンドポイントを一元的に管理し、セキュリティポリシーを適用する。
- リモートワークで利用されるデバイスのセキュリティを確保する（パスワードポリシー、画面ロック、データ暗号化など）。
- 紛失・盗難時のリモートロックやワイプ機能を提供する。
- 業務利用するアプリケーションの管理や配布を行う。

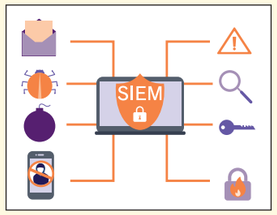
WAF（Web Application Firewall）

- Webアプリケーションに対する不正なアクセスや攻撃。（SQLインジェクション、クロスサイトスクリプティングなど）を防御する。
- WebサイトやWebアプリケーションの脆弱性を悪用した攻撃から保護する。
- 境界防御では防ぎきれないアプリケーションレベルの脅威に対応する。



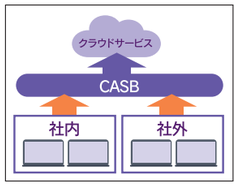
SIEM（Security Information and Event Management）

- ネットワーク機器、サーバー、アプリケーションなど、様々なシステムから出力されるログを一元的に収集・分析し、セキュリティ上の脅威を検知・可視化する。
- 複数のログを相関分析することで、高度な攻撃や内部不正の兆候を早期に発見する。
- インシデント発生時の状況把握や原因究明を支援する。



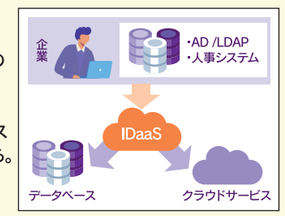
CASB（Cloud Access Security Broker）

- 従業員が利用するクラウドサービス（SaaS、IaaS、PaaS）へのアクセスを監視・制御し、セキュリティポリシーを適用する。
- シャドーIT（許可されていないクラウドサービスの利用）を可視化し、リスクを管理する。
- クラウド上のデータの保護（データ損失防止、暗号化など）を行う。
- クラウドサービス利用におけるコンプライアンスを維持する。



IDaaS（Identity as a Service）/IAM（Identity and Access Management）

- ユーザーIDとアクセス権限を一元的に管理し、適切なユーザーに適切なリソースへのアクセスを許可する。多要素認証（MFA）の導入も含む。
- 不正アクセスを防止し、情報漏洩のリスクを低減する（ゼロトラストセキュリティの重要な要素）。
- リモートワーク環境からのアクセスにおいても、安全な認証を実現する。
- アクセスログを管理し、監査に役立てる。



データ損失防止（DLP）

- 機密情報や個人情報などの重要データの利用状況を監視し、意図しない情報漏洩を防止する。
- メール、Web、ファイル共有など、様々な経路からの情報漏洩を防ぐ。
- 社内ポリシーに違反するデータの持ち出しや利用を検知・制御する。

多要素認証（MFA（Multi-Factor Authentication）

- Webサービスやシステムにログインする際に、複数の異なる認証要素を組み合わせることで、セキュリティを格段に向上させる仕組み。従来のIDとパスワードのみの認証（単一要素認証）に比べ、不正アクセスを非常に困難に。
- MFAで利用される認証要素の種類

以下の3つのカテゴリのうち、異なるカテゴリから2つ以上の要素を組み合わせて認証。

- 知識要素（Something you know）：パスワード、PIN（暗証番号）、セキュリティ質問の答え
- 所持要素（Something you have）：スマートフォン（認証アプリ、SMS）、ICカード、セキュリティトークン（物理的な鍵のようなデバイス）
- 生体要素（Something you are）：指紋認証、顔認証、虹彩認証、声紋認証

バックアップ

- 重要なデータやシステムの状態を定期的に複製し、別の場所に保管する仕組み。
- データ損失からの復旧：ランサムウェア感染、システム障害、人為的なミスなどによるデータ消失時に、バックアップデータを利用して迅速に復旧できる。
- 事業継続性の確保：主要なシステムがダウンした場合でも、バックアップデータから代替環境を立ち上げることで、事業の中断時間を最小限に抑えることができる。
- 過去の状態への復帰：誤った操作やシステム変更によって問題が発生した場合、バックアップ時点の状態にシステムやデータを戻すことができる。
- コンプライアンス要件への対応：多くの規制や業界標準において、データのバックアップと復旧体制の整備が義務付けられている。

IDS（侵入検知システム）/IPS（侵入防御システム）

- ネットワークやシステムへの不正なアクセスや攻撃を監視し、不審な活動を検知（IDS）または遮断・防御（IPS）するシステム。
- リアルタイムな脅威検知：既知の攻撃パターンや不審な挙動を監視し、早期に脅威を特定して管理者に通知する（IDS）。
- 不正アクセスの防御：不正な通信や攻撃を自動的にブロックし、ネットワークやシステムへの侵入を未然に防ぐ（IPS）。
- 攻撃ログの記録と分析：攻撃の試みや成功事例を記録し、分析することで、セキュリティ対策の改善や将来の攻撃予測に役立てることができる。
- 内部不正の監視：内部からの不正なアクセスや操作を検知し、抑止する効果も期待できる。

DDoS対策サービス

- 大量の不正なトラフィックを送りつけるDDoS（分散型サービス妨害）攻撃からWebサイトやネットワークを保護するサービス。
- 大規模トラフィックの吸収：大量の攻撃トラフィックをクラウド側の広大なインフラで吸収し、自社のサーバーへの過負荷を防ぎ、サービスダウンを回避する。
- 悪意のあるトラフィックのフィルタリング：攻撃トラフィックの特徴を分析し、正常なアクセスと不正なアクセスを識別して、不正なトラフィックのみを遮断する。
- 常に最新の攻撃手法に対応：サービスプロバイダーが常に最新の脅威情報を収集・分析し、防御機能をアップデートすることで、新たな攻撃手法にも対応する。
- 可用性の維持：DDoS攻撃によるサービス停止を防ぎ、Webサイトやオンラインサービスの継続的な可用性を確保する。

全ての企業 ～セキュリティ対策は「義務」であり「生命線」です～

デジタル社会において、セキュリティ対策はもはや当然の義務であり、企業存続のための生命線です。
それは、社会の一員としてのマナーでもあります。今こそ、貴社の情報管理、あらゆるデバイス、そしてネットワーク環境、ICTに関わる全ての領域を徹底的に見直しましょう。「人」と「組織」のマネジメントこそが、強固なセキュリティの基盤です。さらに人と組織を守るため、最適で強固、変化に柔軟に対応できるセキュリティデバイスとソリューションの導入を。時代遅れの対策では、一瞬で全てを失いかねません。

もはやセキュリティ対策はコストではなく、企業が持続的に成長するための重要な未来への投資と捉えるべき時代と言えるでしょう。