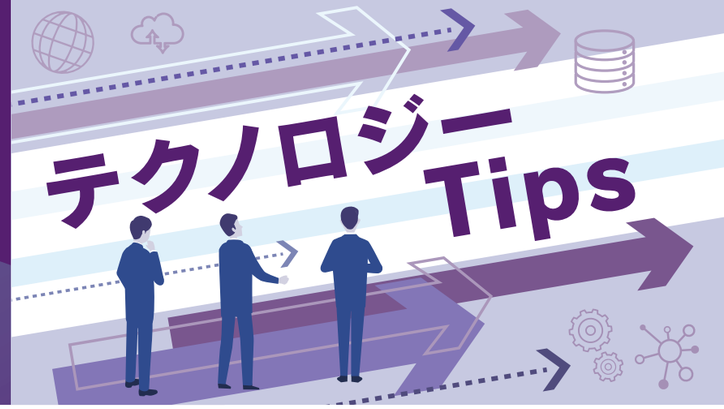
今こそ知りたい Tech Tips!

サイバー攻撃の矛先は、もはや規模を問いません。さらに境界内型セキュリティは限界。
脅威は、すでに「境界」の内外を問わず迫っています。

「何も信頼しない」から始まる、新時代の守り方。
ゼロトラストセキュリティとは?
基本概念から構築までのファーストガイド



国内大手の飲料メーカーがランサムウェア攻撃を受けた事件は記憶に新しいところです。
同社の経営トップは、弱点の点検や管理が十分ではなかった点を反省し、早期に「信頼しない前提（ゼロトラスト）」の通信環境を整えていれば防げた可能性があるとの見解を示しました。
今後はゼロトラストを軸に、VPNの廃止、クラウド移行後の対策強化、端末監視の充実、社内体制の見直しを進める方針だと報じられています。

コメントにある「ゼロトラストセキュリティ」についてあらためて詳しくご説明します。

ゼロトラストセキュリティとは？

ゼロトラストセキュリティは、**「何も信頼しない」を前提に、社内・社外を問わず、すべてのアクセスや通信を常に検証・監視する新しいセキュリティの考え方です。**従来は「社内ネットワークは安全」「外部は危険」と境界で守る発想でしたが、クラウドサービスやテレワークの普及、外部パートナーとの協業などにより、情報資産や業務システムが社外にも広がっています。

ゼロトラストの前提

- 情報資産は社内・社外に存在。
- 情報資産へのアクセスは社内・社外の両方。
- 脅威は社内NWに存在しうる。

ゼロトラストでは、

- すべてのユーザー・端末・通信を「疑う」ことから始めます。
- アクセスごとに認証・権限確認・端末の安全性チェックを行い、必要最小限の権限だけを与えます。
- 万が一侵入されても、被害の拡大を防ぐ仕組みです。

境界内型セキュリティとは？なぜ「限界」？

境界内型セキュリティとは？

境界内型セキュリティは、従来の企業IT環境で主流だった「社内ネットワーク＝安全、社外＝危険」という考え方に基づく防御モデルです。このモデルでは、社内ネットワークと外部インターネットの間に「境界（ゲート）」を設け、ファイアウォールやVPNなどの機器で外部からの不正アクセスや攻撃を遮断します。

主な特徴

- ☑ 社内ネットワークに入るためには認証やVPN接続が必要
- ☑ 社内のサーバーやデータは、外部から直接アクセスできない
- ☑ ファイアウォールやUTM（統合脅威管理）で外部からの攻撃を防御
- ☑ 社内の端末やユーザーは「安全」とみなされる

境界内型セキュリティの限界

しかし、近年のワークスタイルやテクノロジーの変化によって、この「境界で守る」考え方は限界を迎えています。

❶ ワークスタイルの変化

- テレワーク・リモートワークの普及
- モバイル端末・BYOD（私物端末の業務利用）
- 外部パートナー・協業の拡大

❷ テクノロジーの変化

- クラウドサービスの利用拡大・SaaS・Webアプリの普及
- 生成AIやIoTの導入（これらの変化により、境界型防御の前提である「社内＝安全」「社外＝危険」が成り立たなくなっています。）
- 社内ネットワークの外にも重要な情報資産が存在
- 社外からのアクセスが日常的に必要
- 社内の端末やユーザーも、ウイルス感染や不正利用のリスクがある
- 一度境界を突破されると、社内全体に被害が拡大しやすい

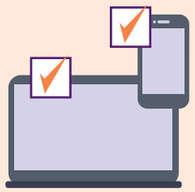
例えば

- CASE1 社員が自宅のWi-Fiから業務システムにアクセス ▶ 家庭のネットワークが安全とは限らない
- CASE2 クラウドサービスのアカウント乗っ取り ▶ 社外からでも重要データにアクセス可能
- CASE3 退職者や委託先のアカウントが残ったまま ▶ 内部からの情報漏洩リスク

ゼロトラストの7つの柱（要素）とわかりやすい事例

① デバイス管理（端末の安全性）

会社のパソコンだけでなく、スマートフォンやタブレットなど、業務に使うすべての端末が安全かどうかを常にチェックします。ウイルス対策ソフトが入っているか、OSやアプリが最新か、勝手に改造されていないかなどを確認します。



具体的には？ 営業担当が自宅のパソコンから会社の顧客データにアクセスしようとしたとき、そのパソコンにウイルス対策ソフトが入っていなければ、アクセスできないようにします。

▶「安全な端末だけが会社の情報に触れられる」仕組みです。

② ネットワーク監視（不正侵入検知）

社内外のネットワークを24時間監視し、怪しい通信や不正な侵入をすぐに見つけて止めます。
VPNやファイアウォールだけでなく、クラウドサービスへの通信も対象です。

具体的には？ 夜中に普段使わない海外から大量のアクセスがあった場合、自動的に遮断し、管理者に通知します。

▶「怪しい動きはすぐに止める」ことで、被害を未然に防ぎます。

③ ワークロード保護（業務システムの防御）

会社の業務システム（経理、営業、顧客管理など）ごとに、誰が何を使えるか細かく決めます。
必要な人だけが必要なシステムにアクセスできるようにします。

具体的には？ 経理担当しか経理システムに入れないように設定。営業担当が経理システムにアクセスしようとすると「権限がありません」と表示されます。

▶「必要な人だけが必要な情報にアクセスできる」安心設計です。

④ データ保護（漏洩・改ざん防止）

会社の大事なデータ（顧客情報、契約書、設計図など）は暗号化して守り、
誰がいつ何をしたか記録します。外部への持ち出しや共有も厳しく管理します。

具体的には？ 夜中に普段使わない海外から大量のアクセスがあった場合、自動的に遮断し、管理者に通知します。

▶「必要な人だけが必要な情報にアクセスできる」安心設計です。

⑤ 可視化・分析（ログ監視・行動分析）

誰が、いつ、どこから、どんな操作をしたかをすべて記録し、異常な動きがあればすぐに気づけるようにします。普段と違う行動があれば、管理者にアラートが届きます。

具体的には？ 退職予定の社員が突然大量のファイルをダウンロードした場合、「通常と違う動き」として自動で管理者に通知されます。

▶「おかしな動きはすぐに見つけて対処できる」安心です。

⑥ 自動化（セキュリティ運用効率化）

ウイルス感染や不正アクセスを見つけたら、自動で端末をネットワークから切り離したり、管理者に通知したりします。定期的なセキュリティ診断やアップデートも自動で行います。

具体的には？ 社員のパソコンがウイルスに感染したら、自動で社内ネットワークから切り離し、「感染しました」と管理者にメールが届きます。

▶「人の手を使わず、すぐに対応できる」ので安心です。

⑦ ID管理（ID・認証の厳格化）

社員一人ひとりのID（アカウント）を一元管理し、必要な権限だけを与えます。パスワードだけでなく、スマホ認証など複数の方法（多要素認証）で本人確認します。退職や異動時はすぐに権限を変更・削除します。

具体的には？ 新入社員がクラウドサービスを使うとき、会社のIDで一括管理。退職したら、そのIDをすぐに削除し、会社の情報に二度とアクセスできなくします。

▶「必要な人だけが、必要な時だけ使える」安全な仕組みです。

ゼロトラストが大切なのは理解できたが…「どこから手を付ける？」

ゼロトラスト導入の最短ルートは、まず「IDaaS」で不正アクセスを防ぎ、次に「EDR」で端末の異常を監視する体制を整えることで、専門知識がなくても最小限の投資で最大限の効果を得られます。

IDaaSとは？

ひとことで言うと「クラウド上の“入館ゲート＋警備室”として、会社のログインと権限をまとめて管理する仕組み」です。

IDaaSでできること

1) 入口を一本化して、使い回しを減らす
2) 本人確認を強化して、不正ログインを防ぐ
3) 状況に応じて「通す／止める」を判断する
4) 入社・異動・退職に合わせて、権限を整える
5) 出入りの記録を残し、後から確認できる

EDRとは？

ひとことで言うと「社内PCを常に見守り、怪しい動きを見つけたら止めて、原因まで追える“端末の警備・対応”の仕組み」です。

EDRでできること

1) 端末を常に見張り、異常の兆しを早くつかむ
2) 「怪しい動き」を見つけて、注意喚起できる
3) 被害が広がる前に、その端末を止める／隔離する
4) 何が起きたかを時系列で追い、原因に近づける
5) いざという時の対応を、手順化して進めやすくする

セキュリティ対策は、もはやコストではなく「投資」です。
「社内＝安全」という境界型の前提は崩れました。
ゼロトラストの考え方を踏まえ、できるところから、そして最もリスクの高いところを優先して段階的に強化していきましょう。

当社がしっかりご提案、
導入サポートいたします！
まるっと
当社にご相談ください！