TANIUM

守りのセキュリティと攻めのセキュリティ

はじめに

「2025年の崖」を間近にして、より一層DXの推進が叫ばれています。これからの時代に企業が生き残るためには、DXを推進すること、すなわちデジタルを活用してビジネスモデルを変革し、企業の競争力を強化していくことは不可欠です。
しかし、DXを推進するとセキュリティリスクも増大していきます。これは、DX推進と同時にビジネス環境が大きく変化するためです。その変化により、セキュリティリスクは量的にも質的にも対応が難しくなってきています。
そこで有効なのがEDRによる「守りのセキュリティ」とサイバー・ハイジーンによる「攻めのセキュリティ」です。この2つを組み合わせることで、ビジネス環境の変化に対応したセキュリティを確立することができます。

このEbookでは、DX時代の新しいセキュリティの課題と、そこで求められるセキュリティ対策について紹介します。また、「守りのセキュリティ」と「攻めのセキュリティ」を実現するために役立つソリューションについてもご紹介します。
貴社のDX推進やセキュリティの確立にお役立てください。

Index

DX 推進によるビジネス環境の変化

昨今、あらゆる業界・業種で、DX 推進による業務効率化・生産性向上が叫ばれています。それと同時に、ビジネス環境にも大きな変化が起こっているのです。

DX とは

ビジネスにおける DX は、経済産業省では次のように定義されています。

> **企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。**

引用元：デジタルトランスフォーメーションを推進するためのガイドライン（DX 推進ガイドライン）Ver. 1.0

つまり、次の要素を備えた企業全体におよぶ改革のことです。

- ✔ **業務やワークフローをデジタル化し、技術を活かしてビジネスモデルや企業組織を変革する**
- ✔ **顧客に新しい価値を提供し、企業の競争力を高める**

政府も DX を推進している

政府も、経済産業省を主軸に、産業界での DX 推進をあと押ししています。
経済産業省では「デジタルトランスフォーメーションに向けた研究会」を設置しました。また「DX ガイドライン」や「DX レポート」などの報告書を発表して、企業の啓蒙を行っています。

- **デジタルトランスフォーメーションを推進するためのガイドライン**（DX 推進ガイドライン）Ver. 1.0
- **DX レポート** ～ IT システム「2025 年の崖」の克服と DX の本格的な展開～
- **DX レポート 2**（中間取りまとめ）

さらに、DX 認定制度や DX 銘柄の選定、DX 人材育成サイト**「マナビ DX」**の開設、導入補助金や助成金制度の整備も行われています。

DX 時代のビジネス環境とは

DX 時代では、ビジネス環境も大きく変化してきています。

クラウドサービスの活用

ストレージや業務システムなど、クラウドサービスを業務に利用するのが当たり前になってきました。
つまり、社内ネットワークだけではなくインターネットを利用しなければ業務が成り立たなくなってきています。

リモートワークの増加

コロナ禍や働き方改革により、リモートワーク（テレワーク）やハイブリッドワークが増加しています。それによって、自宅やシェアオフィスなどオフィス以外の場所で、会社支給ではない端末で仕事をする人も増えてきました。

アクセスする端末の種類や数の激増

リモートワークやクラウドサービス、IoT などが業務に取り入れられるようになったことで、パソコンやサーバー以外の端末が業務に利用されるようになりました。
現在は、スマートフォンやタブレット、私物のパソコン、センサーのついた IoT デバイスなど、さまざまな端末がインターネット経由で社内ネットワークにアクセスしています。その数も飛躍的に増加中です。

このようにビジネス環境が大きく変化しているので、セキュリティ対策もそれに合わせて対応していかなくてはなりません。

DX時代に増加している新たなセキュリティの課題とは

ご紹介したように、ビジネス環境は大きく変化しています。それはつまり、セキュリティのリスクも変化しているということです。

セキュリティリスクの増加

デジタル技術が浸透してビジネス環境が変化したことにより、インターネットにつながっている業務用の端末が大幅に増えました。そのため、セキュリティリスクも激増しています。インターネットにつながっているということはサイバー攻撃の起点につながっているということだからです。

現在では、端末の多くは、場所や種類、業務用・私用に関わらず、いたるところでセキュリティリスクにさらされていると言ってよいでしょう。

サイバー攻撃の多様化

サイバー攻撃の種類も多様化しています。代表的なものだけでも、次のような種類があります。

攻撃の種類も、日々進化を続けています。新しい攻撃にもすぐに変種や亜種が現れ、高度化・複雑化していき、セキュリティツールが対応しきれないこともしばしばです。

企業のグローバル展開による被害拡大

現在の企業は国内でも多様な組織と連携しており、組織や国をまたいだ連携も活発です。

そのため、それらの連携の1ヵ所がサイバー攻撃を受けると、連携している他の企業・組織にも大きな影響があります。これを狙った攻撃が「サプライチェーン攻撃」です。「サプライチェーンの弱点を悪用した攻撃」は、「情報セキュリティ10大脅威2022」の第3位にも入っています。

参考：情報セキュリティ10大脅威2022 | IPA 独立行政法人 情報処理推進機構

大企業のサプライチェーンの一部である中小企業を攻撃することで、ネットワークでつながっている大企業にも大きな被害を与えることが可能です。1つの中小企業が業務停止に陥ったことでサプライチェーンが寸断され、グローバル展開している大企業の業務に大きな影響が発生することもあります。

企業は、自社のみならず、サプライチェーンを構成する企業のセキュリティ対策も考えなくてはなりません。

これらの課題に対処するセキュリティ対策とは

このように、現在ではセキュリティリスクの量が激増し、質も大きく変化しています。そのため、1つのセキュリティ対策だけでは対処できません。そこで必要となるのが「守りのセキュリティ」と「攻めのセキュリティ」の組み合わせです。

「守りのセキュリティ」とは「ゼロトラスト」を基本とした考え方でサイバー攻撃からエンドポイントを防御することです。そして「攻めのセキュリティ」とは、サイバー・ハイジーンを行い、サイバー攻撃を受けにくくすることです。

この2つを組み合わせることで、より強固なセキュリティを実現できます。

DX時代に注目されている新たな守りのセキュリティとは

DX時代の新たなセキュリティの課題をもとに注目されている「新たな守りのセキュリティ」とは、「ゼロトラスト」という考え方に基づくEDRです。

DX時代の新たなセキュリティの考え方「ゼロトラスト」とは

ゼロトラスト（Zero Trust）とは、文字通り

すべてのアクセスを信用しない、安心しない

という考え方で、これをもとにしたセキュリティが「ゼロトラスト・セキュリティ」です。
ゼロトラスト・セキュリティは、どのアクセスにも毎回厳密な認証を行い、すべての端末やユーザーの動作を監視します。一度アクセスした端末でも、インターネット経由ではなく社内ネットワーク内でのアクセスでも、毎日利用してくるユーザーでも関係ありません。どのユーザーやアクセスも平等に疑うことで、強固なセキュリティを実現します。

なぜ、ゼロトラスト・セキュリティへの備えが必要なのか

ゼロトラスト・セキュリティは、クラウドサービスへのアクセスでも厳密な認証を行い、動作を監視します。それによって、クラウドサービスを安心して使うことが可能です。
テレワークのようなオフィス以外の場所からのアクセスも、私物の端末やパソコン以外の端末からのアクセスも厳密に認証を行うことで、安心して使うことができます。すべてのエンドポイントに平等な認証を行うことで、クラウドサービスや私物の端末でも安心して使うことが可能になるのです。
そのため、DX時代のビジネス環境の変化にも対応し、セキュリティを確保することができるとして、ゼロトラスト・セキュリティが加速化しています。

EDRとは

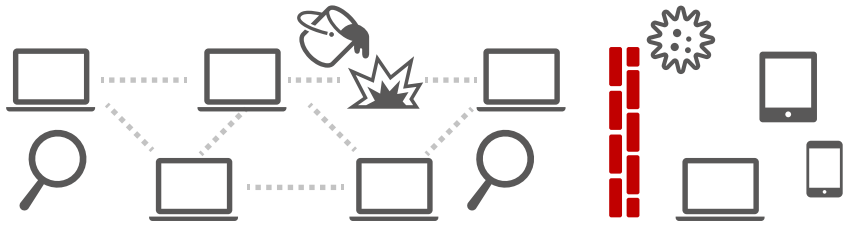
EDR（Endpoint Detection and Response）は

エンドポイントの検知と対応

とも言われます。ネットワークに接続された端末の操作や動作を監視し、トラブルが発生したら迅速な対応を行うソフトウェアです。エンドポイントとは、接続された個々の端末のことを言います。

EDRは「守りのセキュリティ」

EDRは、エンドポイント（端末）を常に監視しており、不正なアクセスやマルウェアが侵入しても、被害を最小限に抑える事が可能です。ゼロトラストの考え方とも相性がよく、ゼロトラスト・セキュリティに対応するためのセキュリティ対策としても、効果を発揮します。
また、EDRは従来の境界型セキュリティ（ペリメタセキュリティ）と組み合わせて利用するとより効果的です。境界型セキュリティとは、社内ネットワークと社外を厳密に区分し、社内ネットワークに不正なアクセスやマルウェアが侵入することを境界線で防ぐものです。



DX時代に必要な攻めのセキュリティとは

もうひとつ、DX時代に必要とされている「新たな攻めのセキュリティ」とは、「サイバー・ハイジーン」という考え方です。

サイバー・ハイジーンとは

サイバー・ハイジーン（Cyber Hygiene）とは、エンドポイントの端末を常に健全な状態に保つことです。手洗い・うがいを行うかのように、IT機器を日々管理して健全なIT環境を維持することで、サイバー攻撃の被害を受けにくくします。

サイバー・ハイジーンでは何をするのか

サイバー・ハイジーンでは、具体的に次のようなことを行います。

- アクセス管理やセキュリティを適切に設定・監視する
- OS、ソフトウェア、アンチウィルスソフトなどを常に最新の状態に保ち、既知の脆弱性を解消する
- 情報システム部門の管理下にない端末を把握し、できるだけ管理下に置く
- 端末やソフトウェアのインベントリやイベントを管理し、モニタリングする
- 脆弱性に関する情報収集・診断

サイバー・ハイジーンは「攻めのセキュリティ」

このような対策を行うことで、端末の状態や脆弱性を常に可視化し、管理します。それによって

「何かあってから対処する」のではなく

「何も起こらないように未然に対策をする」のです。

そのため、サイバー・ハイジーンは「攻めのセキュリティ」なのです。

なぜサイバー・ハイジーンが必要なのか

サイバー・ハイジーンを徹底することで、既知の脆弱性をなくし、サイバー攻撃を受けても被害を受けないか、最小限にすることができます。
これは自社のためだけではありません。自社をサイバー攻撃から守ることで、サプライチェーン全体をサプライチェーン攻撃から守ることにもつながります。
被害を他の組織にまで及ぼさないためにも、サイバー・ハイジーンは重要なのです。

守りのセキュリティと攻めのセキュリティを組み合わせてDX時代を乗り越えよう

DX時代はセキュリティリスクが増大する時代でもあります。その中でセキュリティを実現するにはどうしたらよいのでしょうか。

複数のセキュリティの組み合わせが重要

サイバー攻撃の量が飛躍的に増大し、質的にも高度化・複雑化していく中で、セキュリティリスクも増大を続けています。それに対抗する新しいセキュリティとして、次の2つをご紹介してきました。

守りのセキュリティ	ゼロトラスト・セキュリティを基本にしたEDR
攻めのセキュリティ	サイバー・ハイジーン

これらはどちらか1つで安全を確保できるというものではありません。2つを組み合わせることで強固なセキュリティを確立することが可能です。EDRでサイバー攻撃に備え、サイバー・ハイジーンでサイバー攻撃の被害を受けにくくするというように、役割の異なる2つのセキュリティ対策を併用しましょう。
それによって、より安心してクラウドサービスを利用し、リモートワークで業務を行うことができます。

セキュリティ対策はコストではなく投資と考える

> 経済産業省の「サイバーセキュリティ経営ガイドライン」では、セキュリティ投資は事業継続性の確保やサイバー攻撃に対する防衛力の向上にとどまるものではなく、ITを利活用して企業の収益を生み出す上でも重要な 要素となる。セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。

と提言されており、セキュリティ対策に関する費用の考え方を根本的に変える必要があります。

つまり、企業にとってセキュリティは「コスト」ではなく「投資」と考える必要があるのです。セキュリティを強化することで「社会的信用」を得ることができるからです。

企業がセキュリティをおろそかにすれば、自社がサイバー攻撃の被害にあって損害が発生するだけではありません。顧客の情報が流出し、損害賠償が必要になることもあります。
また、サイバー攻撃の被害にあえば企業として必要なセキュリティ対策を行っていないということになり、社会的信用がなくなってしまいます。それはこれまでの顧客からの取引停止、新規顧客獲得の機会損失にもつながるでしょう。その結果、企業の経営状態にも大きな影響を及ぼすのです。

セキュリティは利益を生む

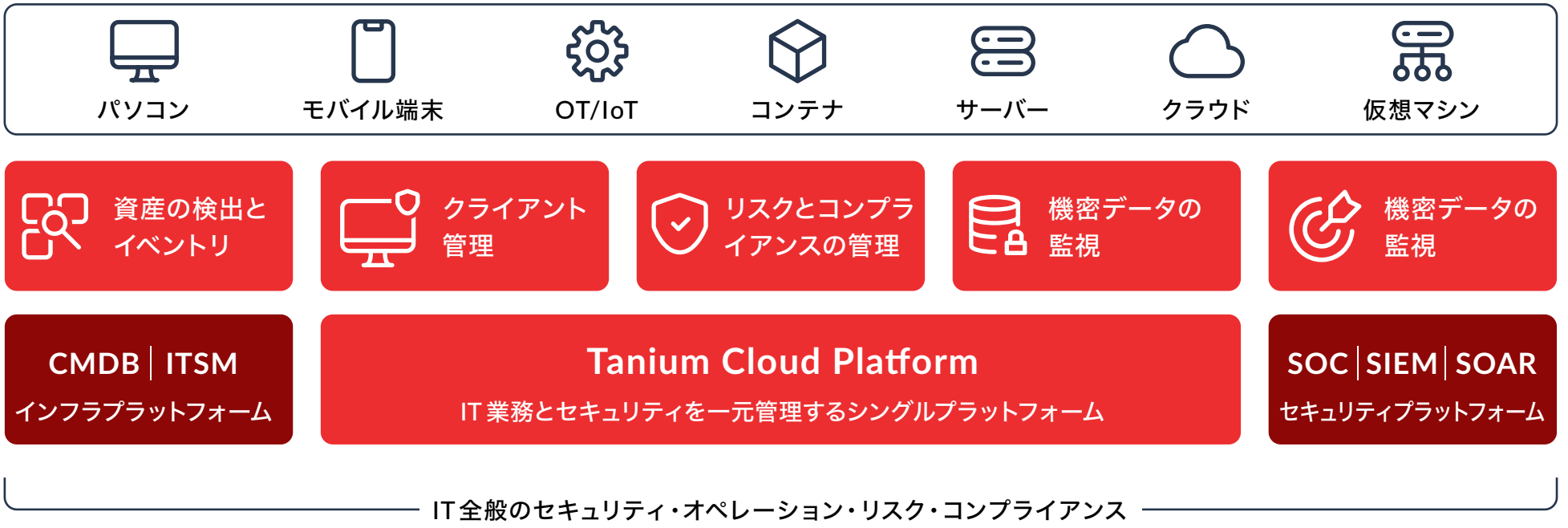
顧客や投資家の「信頼」を得ることは、企業にとって重要なことです。DXを推進し、改革を進めていくうえでは、社会的な信頼はさらに重要な意味を持ちます。企業の社会的信用は、DXを成功させる要素の1つでもあるからです。
また、十分なセキュリティ対策を行うことでサイバー攻撃にあわない、あっても被害を最小限に抑えられれば、かえって社会的な信頼を得ることもできます。それは顧客からの安心感につながり、これからの利益をもたらすからです。つまり、セキュリティ対策をしっかり行うことは将来的な利益につながる投資、「攻めのセキュリティ対策」であると言えます。
そのためにも、ゼロトラスト・セキュリティ対策をし、サイバー・ハイジーンを取り入れてシステムやネットワークを信頼できるものにしていきましょう。

守りと攻めのセキュリティを実現するためのツール

このように、セキュリティを確立するのは重要なことです。しかし、ゼロトラスト・セキュリティ対策をし、サイバー・ハイジーンを取り入れてセキュリティを確立することは容易ではありません。とくに、IT系が専門ではない企業、情報システム部門に十分な人員や予算が確保できていない企業では、かなり難しいことと言ってもいいでしょう。
その場合は、EDRやサイバー・ハイジーンを効率的に行えるツールを導入するのがおすすめです。たとえばTanium Cloud Platformを使うことで、IT機器の管理とセキュリティを一元的に管理することができます。このようなプラットフォームを使えば、情報システム部門のリソース不足を補い「守りのセキュリティ」と「攻めのセキュリティ」を実現することも可能です。
さらに、Tanium Cloud Platformはクラウドサービスとして提供されています。そのため、クラウドサービス利用やリモートワークでのセキュリティにも対応しやすいのです。DX時代のセキュリティを実現するためのプラットフォームと言えるでしょう。

現代のIT課題に対処する最新アーキテクチャ

サービスページ
Tanium Cloud Platform はこちら ▶



まとめ

DX 推進やビジネス環境の大きな変化により、セキュリティリスクも大きく変化しました。クラウドサービスやリモートワークの増加により、セキュリティリスクも激増しています。また、サイバー攻撃は日々高度化・複雑化しており、これまでのセキュリティツールでは対応できなくなってきました。

そのため、新しいセキュリティが必要とされています。

たとえば、ゼロトラスト・セキュリティを基本にした EDR による「守りのセキュリティ」や、サイバー・ハイジーンによる「攻めのセキュリティ」です。これらを併用することでセキュリティを強化し、より安全にクラウドサービスを利用したり、リモートワークを行ったりすることができます。

しかし、「守りのセキュリティ」と「攻めのセキュリティ」を併用して新しいセキュリティを確立していくことは、容易ではありません。そのため、Tanium Cloud Platform のような IT 機器の管理とセキュリティを一元的に管理できるツールを導入することをおすすめします。そうすれば、2 つのセキュリティを容易に実現し、維持することができます。