TANIUM

膨らむ
セキュリティ投資

減らない
セキュリティインシデント

はじめに

多くの企業では、セキュリティを維持・強化するための投資を増やしています。しかし、セキュリティインシデントの発生件数は減るどころか増えているのです。これはなぜでしょうか。

実は、セキュリティを強化してサイバー攻撃の被害を抑えるためには、セキュリティツールの導入だけでは不十分なのです。セキュリティツールに加えてサイバー・ハイジーンを実現し、システム全体の健全性を維持しなければ、十分な対策とはいえません。
なぜサイバー・ハイジーンが必要なのでしょうか。またサイバー・ハイジーンを実現するためには、企業はどのように対応すればよいのでしょうか。

この資料では、サイバー・ハイジーンが必要な理由と、サイバー・ハイジーンでは何を行うのか、また実現に必要なツールについて紹介します。

Index

セキュリティインシデントは増加の一途をたどっている

ここ数年、セキュリティインシデントの発生が増加し、質も変化してきています。

セキュリティインシデントとは

セキュリティインシデントとは、情報セキュリティインシデントともいわれます。企業や組織がセキュリティ上の脅威となる事故や攻撃などにあうことです。具体的には、次のようなものを指します。

- マルウェアの感染
- 不正アクセス、なりすまし
- 情報漏えい、情報詐取
- 悪意のない人為的な被害
- 天災による被害

セキュリティインシデントの増加と質の変化

セキュリティインシデントは、ここ数年増加を続けています。JPCERT コーディネーションセンター（JPCERT/CC）によると、2019 年には 18,070 件だったのが 2020 年には 43,823 件、さらに 2021 年では 9 月末時点で 32,372 件の発生報告がありました。

参考：JPCERT/CC セキュリティインシデント年表 | JPCERT/CC

セキュリティインシデントは、件数が増えているだけでなく、質も大きく変化してきました。
たとえば IPA（情報処理推進機構）の「情報セキュリティ 10 大脅威 2021」によると、新しく「テレワーク等のニューノーマルな働き方を狙った攻撃」がランクインしています。また「インターネット上のサービスへの不正ログイン」や「脆弱性対策情報の公開に伴う悪用増加」も大きく順位を上げているのがわかるでしょう。

参考：情報セキュリティ 10 大脅威 2021 | IPA 独立行政法人 情報処理推進機構

コロナ禍や働き方改革によるテレワークの増加で、この傾向はこれからも続くと思われます。

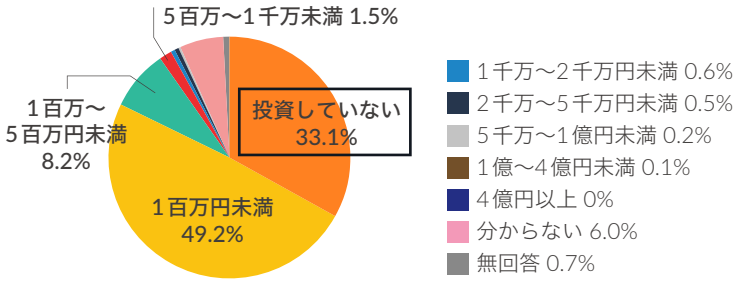
企業はセキュリティを意識していないわけではない（1）

セキュリティインシデントが増加しているといっても、企業がセキュリティ対策をしていないわけではありません。
むしろ、セキュリティ対策の重要さは多くの企業が認識しているでしょう。企業のセキュリティへの投資も進んでいます。

多くの企業がセキュリティ投資を行っている

IPA（情報処理推進機構）の「2021年度 中小企業における情報セキュリティ対策に関する実態調査」によると、過去3期において「情報セキュリティ対策投資」を行っていない企業は33.1%です。つまり、約67%の企業がセキュリティへの投資を行っています。

直近過去3期の情報セキュリティ対策投資額

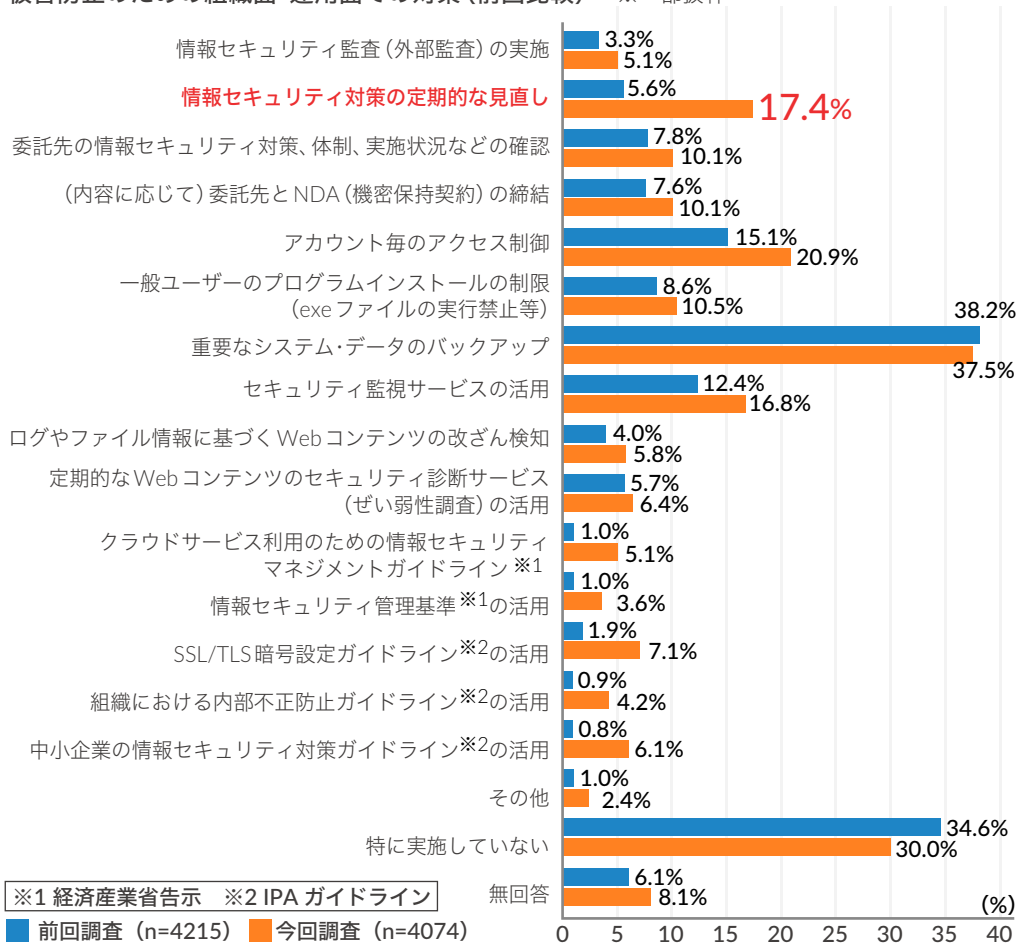


参考：「2021年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について | IPA 独立行政法人 情報処理推進機構

「情報セキュリティ対策投資」についての回答は上記のグラフに示されています。グラフからもわかるとおり、9.7%の企業が100万円から1,000万円の情報セキュリティ対策投資を行っています。
さらに、右記のグラフからわかるとおり、17.4%の企業が「情報セキュリティ対策の定期的な見直し」を行っています。

つまり、企業はある程度のセキュリティ対策を行っているのです。

被害防止のための組織面・運用面での対策（前回比較） ※一部抜粋



参考：「2021年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について | IPA 独立行政法人 情報処理推進機構

企業はセキュリティを意識していないわけではない（2）

セキュリティツールも進化している

また、セキュリティツールにも新しい技術や考え方をもとにしたツールが登場しています。たとえば、次のようなものです。

EPP（Endpoint Protection Platform）

エンドポイント保護プラットフォームともいいます。パターンマッチング方式や振る舞い検知、機械学習など、複数の検知技術を組み合わせて、マルウェアからエンドポイントを守るものです。ネットワークに入ってくるファイルを検査し、被害が出る前にマルウェアによる攻撃から端末を守ることができます。

ゼロトラスト・セキュリティ

「すべてのアクセスを信用しない、安心しない」という考え方をもとにしたセキュリティです。社内ネットワークやテレワーク、クラウドサービスなど、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。

UEM（Unified Endpoint Management）

統合エンドポイント管理ともいい、エンドポイントセキュリティを統合管理するものです。さまざまなセキュリティツールの機能を併せ持ち、管理画面からトータルに管理して現状を可視化できます。

振る舞い検知

マルウェアを検知する方法の1つで、プログラムのコードや動作・挙動から、マルウェアの特徴があるプログラムを検知する方法です。未知のマルウェアや、既存のマルウェアの変種も検出することができます。

それでも被害が減らないのはなぜか

多くの企業ではセキュリティ対策を大いに意識し、セキュリティツールを導入するなど、セキュリティに対する投資や実践も行っています。それでもセキュリティインシデントが減らないのはなぜでしょうか。

セキュリティツールだけでは届かない

セキュリティツールは強力にエンドポイントを守り、不正なアクセスの多くを防ぐことができます。しかし、セキュリティツールで届かない部分に大きなセキュリティホールがあれば、どれだけセキュリティツールが強力でも意味がありません。

セキュリティツールで届かない部分とは、防御されているシステムや端末に存在する脆弱性です。脆弱性が放置されたままであれば、セキュリティツールがあってもサイバー攻撃を防ぐことができません。

しかし、脆弱性をきちんと管理できていない企業もまだまだあります。

ビジネス環境には多くの脆弱性が残っている

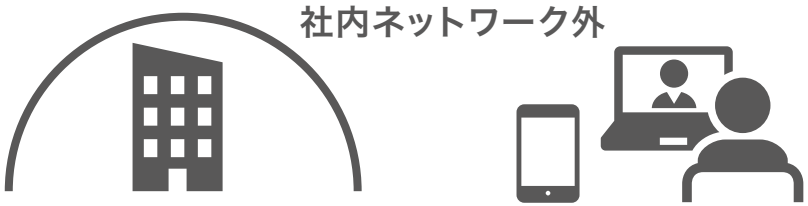
さらに、最近では脆弱性対策のしにくい端末やネットワークが増えています。原因は、クラウドサービスの業務利用やテレワーク導入の増加です。

社内ネットワークにある端末やアプリケーションなら、情報システム部門が脆弱性対策を行うことも容易です。セキュリティパッチの適用やアプリケーションの更新などを管理することで、システムの健全性を維持することができます。

しかしクラウドサービスやテレワークで使用している端末では、情報システム部門による管理がしにくいのです。クラウドサービスのセキュリティ管理は、多くの部分をクラウドサービスのベンダーが担当しています。また、テレワークで使用している端末は社内ネットワークの外にあり、私物の端末も多いため、情報システム部門の手が届きにくくなっているのです。

つまり、現在業務に利用している端末には情報システム部門で管理できない部分が多いため、まだまだ脆弱性が残っていると考えられます。

これでは、セキュリティツールだけで防御することはできません。



セキュリティには日常的な予防策も重要

セキュリティツールでは届かない部分にある脆弱性を対策するのがサイバー・ハイジーンです。

サイバー・ハイジーンとは

サイバー・ハイジーンとは、

日常的なシステム管理を行い、常に健全なIT環境を維持することです。

サイバー・ハイジーンを実現することで、脆弱性攻撃のリスクを小さくし、サイバー攻撃を受けても被害にあいにくくする、または被害を最小限に抑えることができます。それは、セキュリティの強化にもつながります。

サイバー・ハイジーンでは、具体的には次のようなことを行います。

- **セキュリティパッチの適用、アプリケーションの更新**
- **アクセス管理、アクセスログの保存**
- **端末管理、端末やソフトウェアのインベントリ管理**
- **セキュリティ設定**
- **継続的な脆弱性診断および修復**
- **脆弱性に関する情報収集**
- **イベントログの収集、監視、分析**

テレワークの端末にもサイバー・ハイジーンが必要

サイバー・ハイジーンを実現すれば、テレワークで利用している端末もより安心して使うことができます。しかし、社内ネットワークの外にある端末でサイバー・ハイジーンを実現するのは大変です。
そこで、端末の場所にかかわらずサイバー・ハイジーンを実現し、管理を容易にするツールの利用をおすすめします。

セキュリティを確保するには
セキュリティツールとサイバー・ハイジーンの両方が必要

企業がセキュリティインシデントを防ぐためには、セキュリティツールでの防御と、サイバー・ハイジーンによる健全性維持の両方を組み合わせ、死角をなくす必要があります。片方だけではサイバー攻撃を十分に防ぐことができません。

セキュリティツールは、感染症の治療薬やワクチンにあたります。さまざまな種類があり、それぞれ異なる機能や方式を持っていて、対応するサイバー攻撃から端末やデータを防御することが可能です。さまざまなサイバー攻撃からシステムを防御するためには、何種類かのセキュリティツールを組み合わせて使います。

サイバー・ハイジーンは、日常的なうがい・手洗いにあたるものです。日常的なケアでシステムや端末の健康を維持し、サイバー攻撃を受けても被害にあいにくい土台をつくることができます。

セキュリティツールでできることと、サイバー・ハイジーンでできることは異なります。そのため、両方をうまく組み合わせて相互補完することでセキュリティの死角をなくし、より安全性を高めることが可能です。

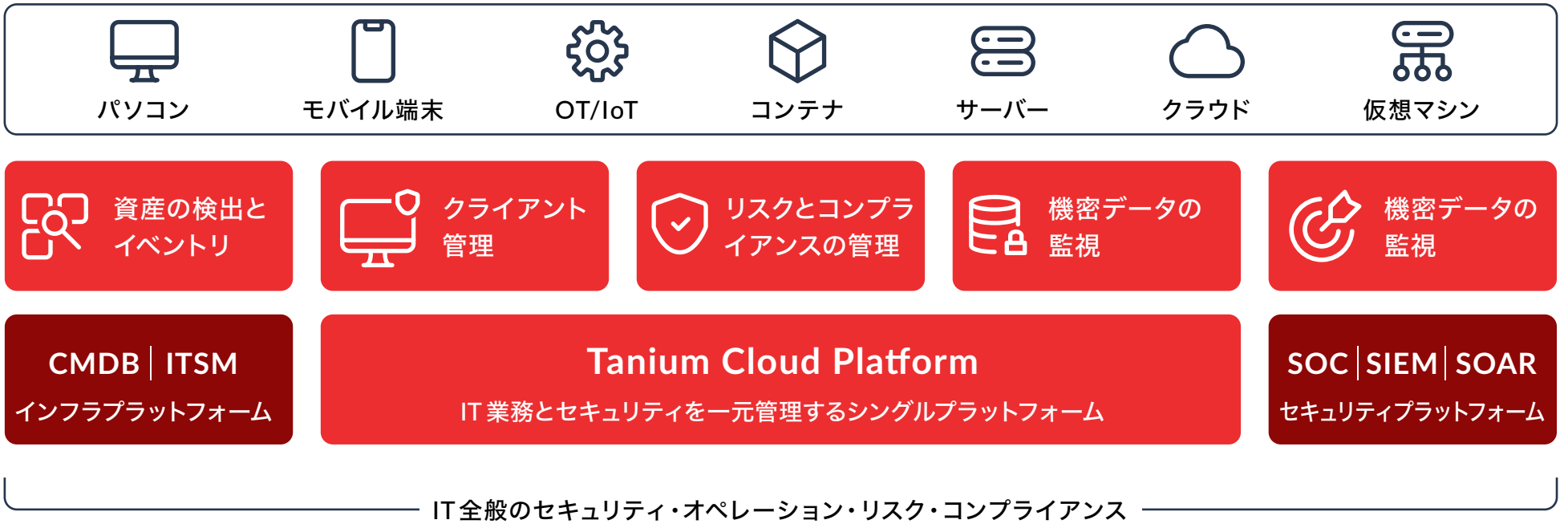
セキュリティツールとサイバー・ハイジーンを両立するためのツール

セキュリティツールとサイバー・ハイジーンを組み合わせると効果的なセキュリティを実現できるのですが、そのためには大きな手間がかかります。情報システム部門の予算や人員が少ない中小企業では、実現は厳しいというところもあるでしょう。
そこで、セキュリティツールとサイバー・ハイジーンの両方をトータルで管理できるプラットフォームを使えば、必要なセキュリティを効率的に実現することが可能です。

たとえば、Tanium Cloud Platformを使うことで、サイバー・ハイジーンとセキュリティツール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ながら強固な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テレワークでも導入しやすいのです。

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

ここ数年、企業がセキュリティ対策を意識して力を入れているにもかかわらず、セキュリティインシデントの発生は増え続けています。さらに従来にはなかった新しいセキュリティインシデントも増えてきました。それは、セキュリティツールだけでは防げない部分にまだまだ脆弱性が残っているからです。
脆弱性を減らし、サイバー攻撃にあっても被害を出しにくくするには、サイバー・ハイジーンを実現する必要があります。サイバー・ハイジーンとは、日常的に端末やネットワークの管理を行うことでシステム全体の健全性を維持し、サイバー攻撃にあっても被害を最小限に抑えるためのものです。

サイバー・ハイジーンによる健全性の維持と、セキュリティツールによる防御を併用することで、セキュリティを強化して大きな被害を防ぐことができます。しかし、これは情報システム部門に大きな負担をかけることもあります。
そのため、Tanium Cloud Platformのような、サイバー・ハイジーンとセキュリティツールを一元的に管理できるプラットフォームを導入することをおすすめします。そうすれば、システムの健全性維持とセキュリティ強化を容易に実現し、維持することが可能です。