EDRだけでは不十分？

サイバー攻撃に備える
サイバー・ハイジーン（衛生管理）

TANIUM

はじめに

近年、企業の情報システムにおけるクラウドサービスの利用が爆発的に広まっています。これには、2つの理由があります。
1つは、クラウドサービスを利用すれば、自社内でシステムを構築するよりもスピーディーにシステムを構築できるためです。それによってビジネス環境の変化に迅速に対応できるだけでなく、コストの最適化を図ることもできます。
もう1つは、働き方改革の推進から推奨されていたものの、なかなか進まなかったテレワークが、COVID-19の蔓延により一気に広まったことです。
こういったビジネスやITシステムを取り巻く環境の変化は、企業が必要とするセキュリティのあり方にも大きな影響を及ぼしています。

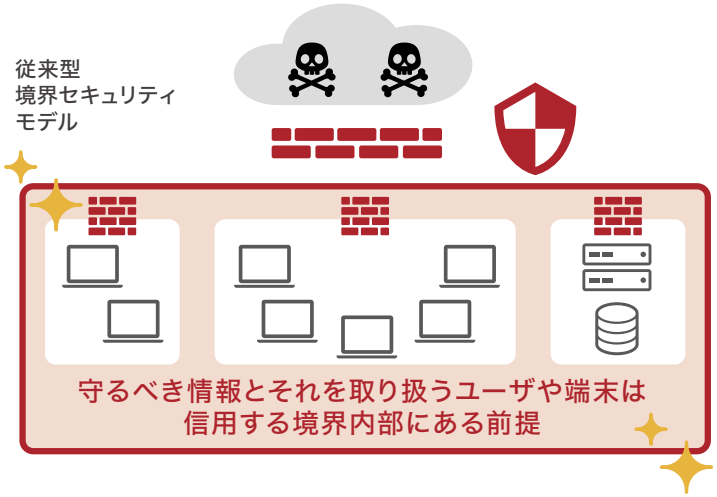
IPA（独立行政法人　情報処理推進機構）は2011年から毎年「**情報セキュリティ 10大脅威**」を発表しています。2021年はこちらに、組織にとっての脅威として初めて「テレワーク等のニューノーマルな働き方を狙った攻撃」がランクインしました。
10大脅威には、他にも「ランサムウェアによる被害」や「標的型攻撃による機密情報の窃取」などがランクインしています。これらは、ファイアウォールやIDS/IPSなどの従来型の境界型防御によるセキュリティだけでは防ぎきれません。そのため、エンドポイントで防御するEDR（Endpoint Detection and Response：エンドポイントの検知と対応）が注目を集めています。EDRはサイバー攻撃による侵入を受けることを前提に、被害を抑えるためのソリューションで、サイバー攻撃の検知から復旧に効果を発揮するものです。
侵入される前には、できる限りサイバー攻撃を防ぐことも必要になります。そのため、平時から侵入を防ぐための準備を行い、守りを固める「サイバー・ハイジーン（衛生管理）」も重要です。

このE-bookでは、従来型のセキュリティ方法である境界型防御と、現在注目されているEDR、サイバー・ハイジーン（衛生管理）についてご説明します。また、なぜサイバー・ハイジーン（衛生管理）が今後重要となるのか、これからのセキュリティにはどのような機能が必要なのかも解説していきます。さらに、最後にセキュリティについて役立つソリューションについても紹介します。

Index

従来型セキュリティ「境界型防御」の限界

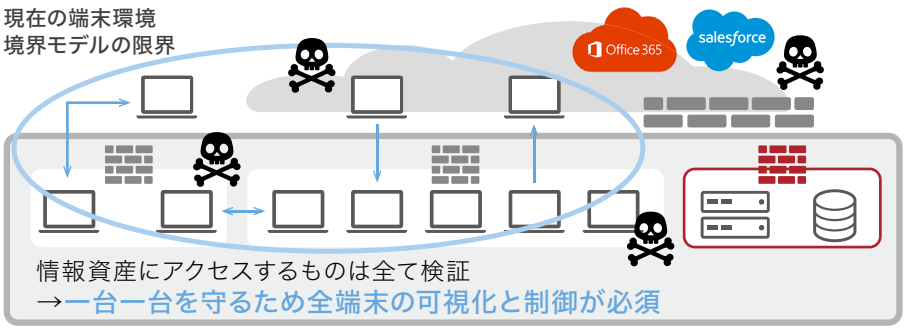
これまでの企業では、次のようなセキュリティで社内の機器やデータを守っていました。
まず、システムを大きく社内ネットワークと社外に分けます。
社員が社内から自社のサーバーにアクセスするのはイントラネットなどの内部通信であり、安全で信頼できるものと考えることが可能です。逆に社外からのアクセスは危険と見なし、ファイアウォールやアンチウイルスソフトウェアなどで内外の境界を守るという方法が取られていました。しかし現在では、この方法では安全を確保することはできません。そこには、次の２つの理由があります。



社会環境・ビジネス環境が変化している

最近は、社内ネットワークへのアクセス経路が多様化・複雑化しています。
社員が社内のPCからイントラネットで社内のサーバーにアクセスするだけではありません。業務でも、社外のネットワーク、つまりインターネットの利用が当たり前に行われています。多くの企業では、次のようなアクセスが増加しているでしょう。

- **社外にサーバーのあるクラウドサービスを利用するため、社内のPCからアクセスする**
- **テレワークで、自宅やシェアオフィスなどの社外から、イントラネット内にあるサーバーにアクセスする**



サイバー攻撃が高度化・多様化し、量も増えている

これまでは、セキュリティとしては主にファイアウォールとアンチウイルスソフトウェアが使われていました。
ファイアウォールは、外部からのサイバー攻撃から社内のネットワークを守る防護壁のようなものです。インターネットとイントラネットの境目に設置されるハードウェアやソフトウェアで、不正なアクセスからイントラネットを守ります。
また、アンチウイルスソフトウェアは、既知のウイルス（マルウェア）を検知・除去するソフトウェアです。ウイルスから作成したデータベース（シグネチャファイル、パターンファイル）をもとに、しているので、データベースはつねに最新の状態に保つ必要があります。

しかし近年は、これらの方法では防ぎきれないような高度なサイバー攻撃が増えてきました。次のページで代表的なものを紹介します。

従来型セキュリティ「境界型防御」の限界

近年における高度なサイバー攻撃の代表例

ゼロデイアタック（ゼロデイ攻撃）

新しい脆弱性が発見されたとき、修正プログラム（セキュリティパッチ）が提供される前に行われるサイバー攻撃です。脆弱性が発表される前や、ソフトウェアベンダーが脆弱性に気づく前に行われる場合もあります。修正プログラムやアンチウイルスソフトウェアのシグネチャファイルなどで対策できないので、対応が非常に難しいものです。

標的型攻撃

明確な目的を持って、特定の個人や企業などの組織を狙って行うサイバー攻撃です。業務関連の差出人になりすました標的型攻撃メール、改ざんされたWebサイトへのアクセスなどの手法があります。自治体や大企業から中小企業まで、さまざまな組織が標的です。
攻撃者は、長期間かけて計画的かつ巧妙に侵入とアカウント乗っ取りを試みます。乗っ取られたあとの内部からの犯行に対しては、境界型防御では防ぐことはできません。そのため、完全な防御は困難です。さまざまな対策を組み合わせて被害を最小限に抑える必要があります。

ランサムウェア

マルウェアの一種で、ターゲットのコンピュータやデータなどへのアクセスを制限します。その後、ターゲットにアクセス制限を解除するための身代金を要求する金銭目的のサイバー攻撃です。企業や自治体をターゲットに、多額の身代金を要求するケースが増えています。

このように、サイバー攻撃の種類は多様化しており、その数も大幅に増えています。そのため、境界型防御に基づいたセキュリティでは対応できなくなってきているのです。そこで、ゼロトラストという考え方に基づいたさまざまなセキュリティ対策が注目されています。ゼロトラストとは、「信頼できない」という意味で、ネットワークの内外を問わず、すべての通信は完全には信頼できないという考え方です。

ゼロトラストで注目を集める「EDR」

ゼロトラストとは特定の技術や製品を指す言葉ではなく、システムの設計や運用における基本的な考え方です。
従来のように安全なイントラネットと危険なインターネットに分けるのではありません。信頼できるもの（Trust）は何もない（Zero）ということを前提にセキュリティ対策を行わなければならないという考え方です。

NISTによるゼロトラストの考え方

NIST（National Institute of Standards and Technology、アメリカ国立標準技術研究所）では、ゼロトラストの考え方について、次のように定義しています。

1. 全てのデータソースとコンピューティングサービスは**リソースと見なす**
2. **ネットワークの場所に関係なく**、全ての通信を保護する
3. 企業リソースへのアクセスは、**セッション単位で付与する**
4. リソースへのアクセスは、クライアントID、アプリケーション、要求する資産の状態、その他の行動属性や環境属性を含めた**動的ポリシーによって決定する**
5. 企業は、全ての資産の整合性とセキュリティ動作を**監視し、測定する**
6. 全てのリソースの認証と認可は動的に行われ、**アクセスが許可される前に厳格に実施する**
7. 企業は、資産やネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、それを**セキュリティ対策の改善に利用する**

ゼロトラストの5つの機能

ゼロトラストは、情報セキュリティのなかでも特にサイバー攻撃対策に特化した内容です。ゼロトラストで求められている機能には、次の5つがあります。

特定 **防御** **検知** **対応** **復旧**

ゼロトラストでは、ネットワークセキュリティだけでなくエンドポイントセキュリティも重視しています。そのエンドポイントセキュリティでとくに注目されているのが、EDRです。

EDRの特長と機能

EDR（Endpoint Detection and Response：エンドポイントの検知と対応）は、サイバー攻撃により侵入を受ける前提で、被害を最小限に抑えるためのエンドポイントセキュリティです。EDRはゼロトラストの5つの機能のうち、検知、対応、復旧に対応できるため、エンドポイントのセキュリティとして注目されています。
EDRには、サイバー攻撃の被害を最小限に抑えるため、次のような機能があります。

- ✔ エンドポイントを常時監視する
- ✔ 振る舞い検知や機械学習を利用し、不審な動作から、サイバー攻撃の兆候を検知する
- ✔ 検知したサイバー攻撃を分析し、侵入ルートであるエンドポイントや影響範囲を調査する
- ✔ 他の端末に影響を及ぼさないように、攻撃を受けたエンドポイントを隔離する
- ✔ マルウェアを駆除したりデータを復旧したりして、エンドポイントを復旧する

EDRだけでは不十分!?　侵入を防ぐための対策が必要

しかし、EDRだけでもセキュリティ対策としては不十分と言えます。
EDRは、サイバー攻撃による侵入に対処し、被害を最小限に抑えるものです。しかし、そもそもサイバー攻撃の標的とならないための対策も必要ではないでしょうか。そのためには、サイバー攻撃を受ける前、つまり平時からサイバー攻撃を予防する対策を行うことが重要です。

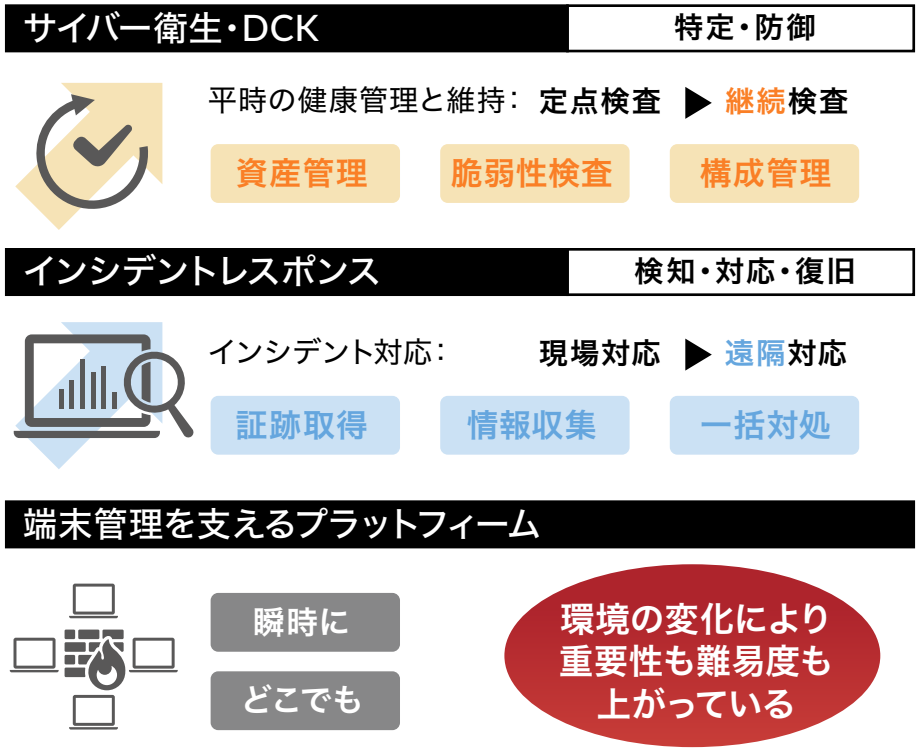
サイバー攻撃を予防する対策とは、定期的に検査を行い、修正プログラムを更新し、つねにシステムを健全な状態に保つことです。それによってシステムの脆弱性を排除し、サイバー攻撃をある程度予防して、セキュリティの強化につなげることが可能です。これをサイバー・ハイジーン（衛生管理）といいます。
このサイバー・ハイジーン（衛生管理）により、エンドポイントやネットワークの現状を可視化することができます。状況を可視化することで、今後どのような対策を行えばよいかを明確にすることが可能です。そのため、サイバー・ハイジーン（衛生管理）はセキュリティにとってとても重要なのです。

サイバー・ハイジーンでは、常時、次のような項目を管理します。

- ✔ **資産管理**（IT資産、ハードウェアの管理）
- ✔ **ソフトウェア管理**（ライセンス、バージョンなどの管理）
- ✔ **パッチ管理**
  （アプリケーションの修正プログラムを随時更新することで脆弱性を排除）

環境変化に対応する端末管理の要件

機能要件と実現の形



エンドポイントセキュリティのためには、サイバー・ハイジーン（衛生管理）が必要

サイバー・ハイジーン（衛生管理）では、平時からサーバーや端末などのIT資産を管理し、サイバー攻撃に対する予防策を実行します。
サイバー・ハイジーン（衛生管理）がしっかり行われていれば、脆弱性の多くが排除されるため、セキュリティ対策としても非常に有効です。

サイバー・ハイジーン（衛生管理）により、次のようなことも可能になります。

- つねに最新の修正プログラムがインストールされた状態を保つことで、脆弱性を利用した未知の攻撃を防ぐ
- パフォーマンスを常時監視することで、速やかに異常を検出する
- 許可されていないデバイスが接続されたことを検出して、デバイスを経由した攻撃を防ぐ

しかし、サイバー・ハイジーン（衛生管理）をしっかり実行するには、手間がかかります。情報システム部門だけでは人手が足りないということも出てくるかもしれません。
情報システム部門がセキュリティチームと運用チームが分かれている場合は、運用チームが担当するなど、部門全体で取り組むといいでしょう。

タニウムが提供する機能　NISTサイバーセキュリティフレームワーク（CSF）との関連

特定	防御	検知	対応	復旧
未然対策：サイバー衛生・CDM		事後対策：インシデントレスポンス		
シャドーIT管理 資産管理 脆弱性対策	パッチ適用 アプリケーション管理	モニタリング 攻撃検知	インシデント対応 侵害調査・分析	復旧業務

ベースライン全て

TANIUM

端末に求める要件にプラットフィーム・単一エージェントで対応
数千数万台「**全ての端末**」の可視化や制御を「**瞬時**」に、かつ「**一括**」して実現

今後のセキュリティで必要とされる機能はなにか

適切なセキュリティ対策を行うためには、リアルタイムでエンドポイントの状態を可視化して把握し、管理する必要があります。
現状把握は、一度情報を取得したら終わりではありません。定期的に情報を取得するとしても、週に一度のレポートでは感覚が空きすぎてしまいます。
サイバー攻撃に気づいた時にはもう手遅れかもしれません。重要なのは、リアルタイムで状況を把握できること、攻撃を受けたら迅速に対処できることの2つです。ゼロトラスト時代の情報セキュリティでは、以下のような機能が必須と言えるでしょう。

エンドポイント管理

リアルタイムに端末の状態を可視化し、管理する

資産の検出とインベントリ

管理されていないエンドポイントの自動検出、IT資産目録の作成・管理

構成管理

システムを構成するハードウェアやソフトウェアの管理

パッチ管理

エンドポイントのOSやアプリケーションの修正プログラム配布・管理

パフォーマンス監視

システムおよびシステムのリソースごとのパフォーマンスを監視

ソフトウェア管理（SAM）

ソフトウェア、ライセンス、ソフトウェアがインストールされた
端末などの情報管理

デバイスとアプリケーションの可視化

デバイスやアプリケーションの種類などセキュリティ管理に
必要な情報を可視化

EDR

エンドポイントである端末を一括して制御する

資産の検出とインベントリ

ネットワーク全体から管理 / 非管理のデバイスを自動的に可視化し管理

データリスクとプライバシー

機密情報や個人情報など、エンドポイントにあるデータを包括的に管理

インシデントレスポンス

サイバー攻撃にどのように対応するかを定義し準備

脆弱性と構成管理

脆弱性と構成を評価し、リスクを特定・測定

サイバー・ハイジーン（衛生管理）と EDRを組み合わせることでセキュリティを強化

ゼロトラストの5つの機能のうち、サイバー・ハイジーン（衛生管理）は「特定」「防御」をカバーし、残りの「検知」「対応」「復旧」はEDRでカバーします。
つまり、この2つを組み合わせることで、ゼロトラストに必要な5つの機能を網羅することが可能となります。

タニウムプラットフォームの紹介

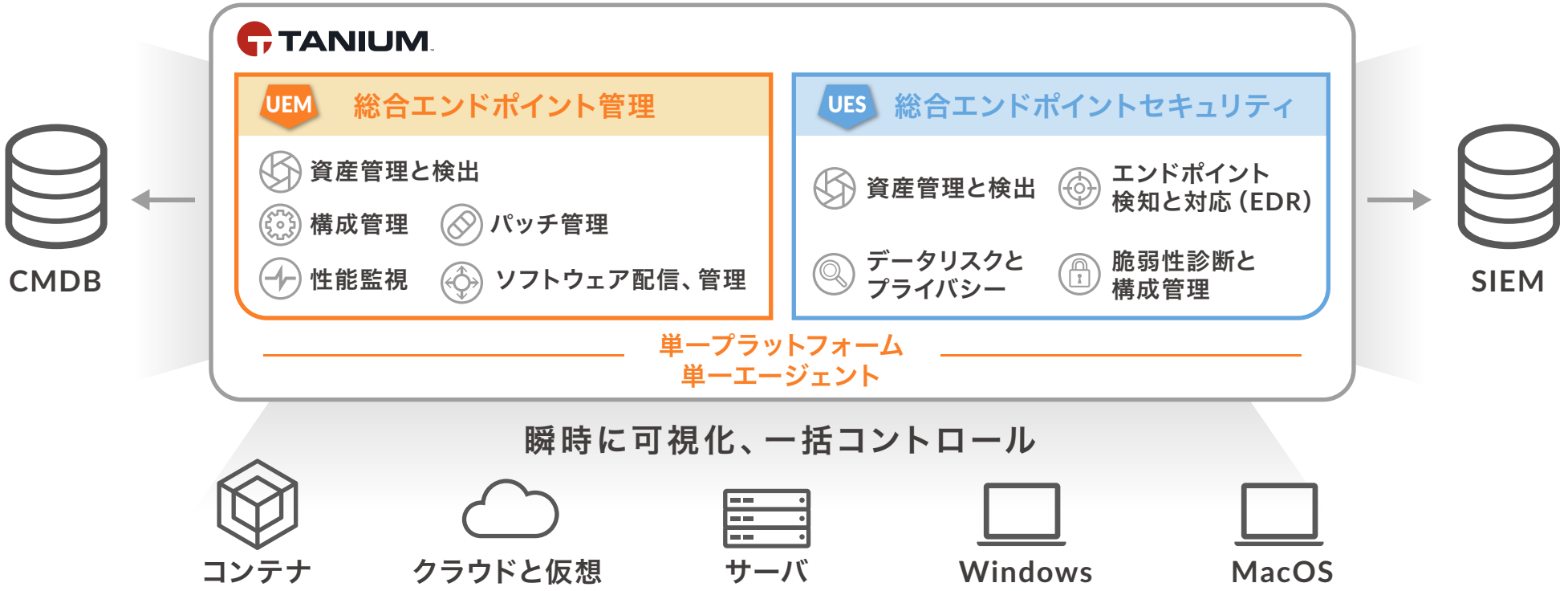
タニウムでは、ゼロトラストの5つの機能を統合エンドポイント管理（UEM）と統合エンドポイントセキュリティ（UES）の2つのプラットフォームで提供しています。

統合エンドポイント管理（UEM）ではサイバー・ハイジーン（衛生管理）の観点からエンドポイントを管理・保護します。また、統合エンドポイントセキュリティ（UES）はEDRを実現する方向でエンドユーザやサーバ、クラウドのエンドポイントを管理・保護するものです。どちらのプラットフォームも、オンプレミス、もしくはSaaSの2種類の形態で提供しています。

タニウムプラットフォーム

統合エンドポイント管理とエンドポイントセキュリティ

サービスページ
タニウムプラットフォーム はこちら ▶



まとめ

従来の境界型防御によるセキュリティだけでは、近年のサイバー攻撃は防ぎきれません。そこで注目を集めているのが、サイバー攻撃を受けたときの被害を最小限に抑える「EDR」です。
ただし、EDRはサイバー攻撃による侵入を受けることを前提として検知から復旧を行います。そのため、侵入を防いでサイバー攻撃を予防しなければなりません。そこで重要となるのが平時の衛生管理「サイバー・ハイジーン（衛生管理）」です。

タニウムでは、プラットフォームとしてEDRとサイバー・ハイジーン（衛生管理）の両方を提供しています。それによって、ゼロトラストで求められる5つの機能に対応し、セキュリティの強化に貢献しているのです。

EDRとサイバー・ハイジーン（衛生管理）、さらに包括的にセキュリティを実現するプラットフォームについては、右記までお問い合わせください。

TANIUM™

タニウム公式サイト

https://www.tanium.jp/

お問い合わせ