




# サイバーハイジーン徹底ガイド

セキュリティ戦略を積極的に進めて  
サイバーハイジーンを実現し  
サイバー攻撃をブロック





ハイブリッドワークの増加によって攻撃対象領域が拡大する中で、サイバー犯罪はより巧妙になっています。これは、政府や民間企業のネットワークがランサムウェアの被害に遭ったことを伝えるニュースが増えていることから明らかです。

そして、脅威はますますパワフルさを増しています。

企業には自社の抱えるリスクを詳しく把握し、エンドポイントを可視化してコントロールして、脅威の検出や修復を行うためのツールが必要になっています。しかし、ツールを導入するだけでは問題は解決しません。IT リーダーたちは、企業ネットワークを維持して保護するためには、適切なツールを用意し、ハイジーンの実践と組み合わせることが重要だと考えています。

サイバーハイジーンは、企業のセキュリティとシステム管理において、基本となるものです。サイバーハイジーンを向上するには、環境全体のIT資産、リスク、脆弱性を継続的に検出し、すばやく大規模に修正するプロセスを構築する必要があります。サイバーハイジーンに注力することで、侵害や、機能停止、混乱を防止することができます。

環境の規模が拡大し複雑化するのに伴って、デバイスや業務の種類も増えています。企業は、複数のオフィスや大陸をまたがる広大な分散型ネットワークにおいて、パソコン、仮想マシン (VM) からコンテナまで、あらゆるものを管理しなくてはなりません。このような状態の中で、サイバーハイジーンは損なわれがちです。

このeBookでは、サイバーハイジーンを構成する要素を解説するとともに、さまざまなツールが改善にどのように役立つのか、あるいは妨げになるのかをご紹介します。

# すべてを把握する

サイバーハイジーンを維持し向上するためには、保有しているIT資産を把握する必要があります。社内にはコンピュータやサーバが何台あるのでしょうか？それらはどんなもので、どこにあるのでしょうか？そこでは何が稼働していて、どのようなサービスを提供しているのでしょうか？

これらの問いに対する答えとなるのが、IT資産の検出とインベントリで、サイバーハイジーンの基盤になるものです。この章では、なぜこの基盤が重要なのかを掘り下げていきます。

## 存在を把握していないものは管理できない

エンドポイントを管理するには、以下の3つのレベルの知識が必要です。

- どのようなIT資産がどこにあるのか？
- そこではどのようなソフトウェアが稼働しているか、それはライセンスがあるものか？
- ネットワーク上のマシンは互いにどのような関係にあり、どのような目的で使用されているのか？

これらの情報は、企業規模にかかわらず、すべての企業に必要なものです。そして、現代のIT環境において、この情報は常に変化しています。特に多くの企業では「BYOD (Bring Your Own Device)」が一般的になりつつあるため、ネットワーク内のIT資産は頻繁に入れ替わります。

また、ネットワーク上にたまにしか現れないものもあり、リモートワークを推奨する企業が増えていることで、ますます複雑化しています。

## 把握できていないことによる運用上のデメリット

アメリカのミュージシャンでザ・イーグルスの元メンバー、ドン・ヘンリーの言葉を借りると、「目を閉じて運転すれば、何かにぶち当たるに決まっている」のです。

最初に「ぶち当たる」可能性が高いのは、セキュリティの脆弱性です。管理できていないIT資産は、保護することはできません。そして、その存在を知らなければ管理することもできません。パッチ未適用による脆弱性など、まったく気づいていない方面から攻撃を受ける可能性もあります。

財務的な影響はどうでしょうか？どこにお金をかけているのかを大まかに把握できていますか？例えば、よく使われているMicrosoft 365のようなソフトウェアライセンスを考えてみましょう。10,000ライセンス所有しているとして、使用しているのは20,000なのか、それとも5,000だけしか使っていないのか把握できていますか？購入したライセンスを効率的に使えていますか？それとも、高額な法的措置の対象となるコンプライアンス違反をしていないでしょうか？

コンプライアンスが求められるのは、ソフトウェアのライセンスだけではありません。医療業界のケースを考えてみましょう。医療関連企業は、健康状態に関する情報やクレジットカードのデータの保護を対象とする、HIPAAやPCIの規定を遵守していることを証明する必要があります。そのデータがどこにあるか把握していますか？把握していなければ、コンプライアンスを証明することはできません。コンプライアンスを証明できなければ、法的制裁を受け、顧客の信頼を失うという2つの大きなデメリットが発生します。

## IT資産の検出とインベントリのためのツールに必要な機能とは？

IT資産の検出とインベントリに使用するツールやプラットフォームには、これらが求められます。

- 精度
- スピード
- 大規模環境への対応
- 使いやすさ

精度、スピード、規模は密接に関係しています。インベントリの作成に2週間、1ヶ月とかかってしまうと、完成した頃には状況が変化しており、見落としが発生します。

ネットワークの規模が大きくなるほど、問題も大きくなります。そのため、大規模な環境にも対応できることが重要です。構成や操作が難しいツールはエラーが発生しやすく、ユーザーが使おうとしなくなるため、使いやすさも重要なポイントになります。

## 古いツールでは、現代のITのニーズに対応できない

10年前の資産検出ツールは、今のIT環境よりも古くに登場したもので、現代の変化のスピードに対応することはできません。しかし、企業は使い慣れたツールに固執する傾向があり、その多くは使いやすいとは言えません。

しかし、使いにくいツールを使いこなすことに誇りを感じていたり、より効果的に動作させるためにカスタムスクリプトを用意しているかもしれません。それだけでなく、そのシステムを使うために、パートナー全体でエコシステムを構築しているケースもあります。

その結果、意図せずして問題に対応するための最適な方法を考えるのではなく、使用中のツールに合わせることを目的にITポリシーやプロセスを設定してしまいます。定着したツールはITインフラの一部となりますが、最善のITポリシーはツールに依存しないものであるべきです。数十年前のツールでは柔軟性を発揮することはできません。

## エンドポイントの検出は動く標的

ネットワーク上のエンドポイントは、デスクトップ、ノートパソコン、サーバに限られません。プリンタや 電話、タブレット、そして増加の一途をたどる消費者向けや産業向けのインターネット (IoT) デバイスもあります。モバイルデバイス管理 (MDM) は成長を続ける分野で、Microsoft IntuneのようなMDMプロバイダーを利用することで、ネットワーク上のすべてのモバイル端末を追跡することができます。

しかし、なぜ消費者向けのIoTデバイスが企業ネットワークに侵入することを心配する必要があるのでしょうか。その理由はこちらです。

ある企業の社員が自宅で仕事をしていました。同社のセキュリティチームは、何かが彼女のノートパソコンに侵入しようとしているというアラートを複数受け取りました。冷蔵庫にマルウェアが忍び込み、彼女の自宅ネットワークをスキャンし、一時的に企業ネットワーク上にあった彼女のデバイスに侵入しようとしていたのです。スマート照明スイッチやスマートサーモスタット、セキュリティカメラでも同じことが起こる可能性があります。

工場にあるマシンでも同じことが言えます。多くのマシンにはセンサーが搭載され、無線ネットワークでウェブベースの製造用アプリケーションと通信しています。これはオペレーショナルテクノロジーと呼ばれており、工場にあるすべてのマシンがネットワークデバイスになります。

あらゆる種類のデバイスを識別できる資産検出ツールはないため、モバイル、タブレット、プリンタなどのデバイスを認識する補助的なアプリケーションと連携できるツールやプラットフォームを選ぶ必要があります。

## エンドポイント検出がゼロトラストの基本に

あらゆるものがネットワークデバイスである以上、すべてに潜在的なセキュリティ脆弱性が潜んでいます。そのため、エンドポイントを「管理端末」「非管理端末」「管理不可」の3つのカテゴリーに分類するポリシーと手順が必要になります。エンドポイントの検出は、ゼロトラスト（どんなデバイスやユーザーも検証なしには信頼できないことを想定したセキュリティアーキテクチャ）への重要な第一歩となります。

エンドポイントの検出が、サイバーハイジーンやセキュリティの出発点となります。まずはそこから始める必要があります。



# ドアと窓に鍵をかける

攻撃者が弱点を見つけ出す能力はますます向上しており、セキュリティチームやIT運用チームが気付く前に脆弱性や構成ミスを突いてきます。

また、侵害による評判の低下や財務上の損失への対応に苦勞する企業に対し、規制上の圧力も強まっています。

脆弱性管理と構成管理は、サイバーリスク管理戦略の中心となるものです。

## 1.優先 順位付け

企業のエンドポイント数は急増しており、すべての問題をすぐに解決することは不可能です。そのため、効率的に優先順位を設定することが重要になります。パソコン、サーバ、仮想マシン、コンテナ、その他のエンドポイントなど、IT資産の重要度を判断する必要があります。この作業は、ライフサイクルの中の検出フェーズと評価フェーズの間に行うことができます。

評価の結果を使って、資産の重要度と影響を与える脆弱性の問題に基づいて、対策の優先順位を決定します。ここでは、継続的に可視化し監視することがキーになります。

## 2.修復

攻撃者がすばやく行動し、セキュリティの抜け穴を突く能力を強化している中で、脆弱性をタイムリーに修復することが重要です。セキュリティチームの多くは頻繁にスキャンを行い、状況に応じて脆弱な箇所を認識していますが、その修正については別の問題です。人員を投入するだけでは解決できません。大規模なIT部門でさえ、問題や修復が必要なエンドポイントが次々と発生する事態に圧倒されています。

そこでワークフローを自動化することで、ライフサイクルをスムーズに進めることが可能になります。パッチの適用を自動化することで重要なシステムに支障が出るのが心配であれば、自動化したワークフローに二次評価プロセスを組み込むこともできます。このプロセスではパッチに問題がないか、それともリスクがあるのかをチェックします。

### 3.修復の頻度を追跡

修復のスピードと成果を把握することで、脆弱性管理の有効性がわかります。検証の段階では、必要な変更が行われたかどうかを確認するだけでなく、パフォーマンスの指標を評価する必要があります。

この段階では、問題をどれだけ早く特定できたか、チームがどれだけ迅速に対応できたか、サービスレベル合意書 (SLA) が守られたか、同業他社のパフォーマンスと比較してどうだったかを確認します。最新で正確なデータがあれば、このステップがより包括的なものになり、継続的な改善の文化を促進できます。

### 4.可能なものはすべて自動化

可能であれば、脆弱性管理のライフサイクル全体を自動化するのが理想的です。そうすれば、手作業によるミスやリスクを削減でき、修復までの時間を短縮し、他の業務により多くの時間を割くことが可能になります。しかし、企業によっては、実行、確認、承認、監査、検証を自動化せずに実際に作業したい、あるいは作業する必要がある場合もあります。

例えば、科学というより芸術的ともいえる最初の資産評価や、検証段階での指標分析などです。それでも、より多くのタスクを自動化できないかを定期的に確認する価値はあります。

### 5.小さいことからスタートし、変化への抵抗感をなくす

脆弱性管理の最新化を阻む最大の障壁の1つが、人と文化です。過去に自動のパッチ適用で生産停止を招いた経験から、自動修復に断固反対する人がいたり、マシンが問題の修正に使われることで、自分の業務が危うくなることを心配する人もいるでしょう。また、「こんなやり方はない」と、単純に不満を漏らす人もいるかもしれません。

変化を恐れる人もいますが、継続的に改善を続けるためには必要不可欠です。まずは、簡単にできることから手をつけましょう。そうすることで、消極的な人に対して脆弱性管理を自動化する価値や、生産性の向上を示すことができます。

例えば、ライフサイクルの検出から評価のステップを自動化するなど、無難なところから始めてみましょう。新しいIT資産を検出した後に自動スキャンを実行することで、5日かかっていたプロセスが5分に短縮されるかもしれません。

修復に関しては、本番環境で実施する前に、テスト環境で重要度が中～低の問題に対して自動でパッチ適用やソフトウェアアップデートを行い、スピードと効果を実証してみましょう。



## 6.すべてはポリシーから始まる

テクノロジーも重要ですが、基本的なことを忘れてはいけません。まずは、適切なポリシー、計画、SLAが必要です。「脆弱性管理のライフサイクルを構築し、各サイクルのSLAはこうする」といった簡単なものでもよいのです。SLAが整備されれば、目標を達成するためには、自動化ツールを活用するのが最適であることが明らかになるかもしれません。

## 7.継続的なスキャンで全体のリスクを低減

最低限のコンプライアンス要件を満たすことばかりを重視し、効果的な脆弱性管理がビジネスにとって有益であるという、大局的な視点が欠けてしまうこともよくあります。

エンドポイントのスキャンは、単に必要な規制項目をチェックするためだけではなく、総合的なリスク管理戦略の一環として実施することが重要です。

つまり、監査の前だけではなく、継続的にスキャンを実行し、問題が発生した時点で特定して優先順位をつけて対処するのです。固定資産だけでなく開発中のカスタムコードも含め、IT環境全体をカバーするようにしましょう。



# よりスピーディに対応する

データ漏洩、ランサムウェア、その他のサイバー攻撃などのセキュリティインシデントへの対応によっては、日常業務に大きな損害を与え、社会の信頼を失い、ブランド価値を低下させ、収益が大幅に減少する可能性があります。

この章では、インシデント対応(インシデントレスポンス、IR)計画の改善と微調整に使える6段階の「PICERLフレームワーク」を紹介します。PICERLとは、Prepare (準備)、Identify (特定)、Contain (封じ込め)、Eradicate (根絶)、Recover (回復)、Lessons Learned (教訓) の頭文字をとったものです。

## ステップ1：Prepare - 準備

まずは準備を行うことで、適切なチームの適切な人材が、それぞれの役割を理解し、インシデントが発生した際に何をすべきかを把握できるようになります。

準備段階では、インシデントレスポンス (IR) チームが実践できる計画を作成する必要があります。IR計画はどんな問題にも対処できるよう、繰り返し訓練する必要があります。訓練しておくことで、実際にインシデントが発生した際にメンバーがプレッシャー下で対応する際に役立ちます。

我々はお客様に、IRチームが訓練に参加し、自分たちの役割を理解しているかを確認します。また、誰が広報、法務、財務へ通知することになっているのかも併せて確認しています。

準備段階では、適切なツールがそろっているかを判断できます。もしそろっていない場合、それらを調達し、トレーニングを行うための資金はあるでしょうか？ IR計画と予算を作成したら、経営幹部にレビューし承認してもらいます。

## ステップ2：Identify - 特定

インシデントが発生したら、このフェーズで以下を確認します。

- パスワードや資産の盗難、フィッシングメール、ポータブルドライブからの悪意のあるコードの実行など、インシデントはいつ、どのように発生したのか？
- 侵入経路はどこか？パッチ未適用による脆弱性か？
- 誰がどのように発見したのか？
- 対象の範囲は？数人または数個のIT資産に限定されているか、それとも広範囲に及んでいるか？
- ビジネスを継続できるか？対策を講じても、どこかの事業部門に影響を及ぼすのか？

多くの場合は、漏洩した認証情報が侵入経路となります。そして、そこから悪意のある攻撃が仕掛けられます。

## ステップ3：Contain - 封じ込め

封じ込めとは、問題のある行為が拡大するのを阻止するための計画を実行することです。短期的な封じ込め戦略としては「検疫」コマンドを実行し、IT資産、アプリケーション、システムをセキュリティツール以外と通信できないようにするといった単純な方法もあります。

長期的な封じ込めは、企業全体で実施する修正のことですが、インシデントの根本原因を完全に是正するには至らない可能性もあります。また法執行機関や規制当局を支援する戦術となる場合もあります。長期的な封じ込め戦略は、データのバックアップやリカバリーシステムと連携させるのがよいでしょう。

パッチの適用やアップデートも封じ込めに含まれます。インシデントに関連するパッチ未適用の脆弱性はないでしょうか？もしある場合は、問題のアプリケーションまたはOSのパッチ適用を早めるべきでしょう。

また、どのユーザーがどのシステムに管理者としてのアクセス権を持っているのかを見直す良い機会でもあります。Active Directoryに関連する攻撃対象領域は？多要素認証は有効になっているでしょうか？これらはすべて封じ込めに関連する問題です。

## ステップ4：Eradicate - 根絶

次に、侵害の原因を「根こそぎ排除」します。例えば、マルウェアの場合、特定したすべてのインスタンスを安全に取り除きます。また、必要に応じてシステムを強化し、パッチを適用します。強化できないシステムは再構築します。そして脅威インテリジェンスを更新し、侵害に関連するアーティファクトを特定できるようにします。

このプロセスを進める間に取組みの範囲が変わることもあります。例えば、ランサムウェアの攻撃を受けた後、多くのシステムを再構築し、直近のバックアップから復元する必要があるかもしれません。攻撃に関連するアーティファクトをすべて把握できなかったり、侵入に使われた脆弱性に対処していなかったりすると、再び攻撃を受ける可能性があります。

根絶するうえでカギとなるのは徹底的に実施することです。問題が何であれ、すべてを見つけることが重要になります。多くの場合、専門知識を持つパートナーやサードパーティがクリーンアップをサポートしてくれます。

## ステップ5：Recover - 回復

損害を被ってしまった後は、回復するしかありません。自分自身に正直になりましょう。被害を受けたシステムは、いつ稼動することができるでしょうか？パッチを適用して、強化し、テストを行いましたか？レッドチーム（敵役のグループ）を使って、攻撃者と同じ手法でシステムに対して模擬攻撃を行いましたか？「これが脆弱性に対処した証拠です」と胸を張って言える状態にしたいのではありませんか。

また、回復では、インシデントによって監視の範囲がどう変わるかを定義する必要があります。侵害の原因となった行為はどの程度の期間監視したらよいでしょうか？30日、3ヶ月、それとも半年でしょうか？そして何を注視すべきでしょうか？ここではレッドチームを使ったテストや、封じ込めの際に収集したアーティファクトが役に立ちます。

### 平均修復時間

平均修復時間 (MTTR, Mean Time to Remediate) とは、IR計画の中で特定、封じ込め、根絶のフェーズにかかる時間です。

2018年のVerizonのデータ漏洩レポートによると、パフォーマンスの高い企業のMTTRは14～30日でした。しかし、セキュリティの専門家の間では、IR計画が成熟しチームの実践力が高まるにつれて、日数が短縮する傾向にあります。

## ステップ6：Lessons learned - 教訓

このステップではまず、IT、コンプライアンス、法務、広報などインシデントレスポンスチーム全員が参加するミーティングを行いましょう。

ここでは、侵害について学んだことを振り返り、文書化します。

- IR計画でうまくいった部分といかなかった部分はどこでしょうか？
- 追加人員が必要になる場面はありましたか？リストにない第三者や社内の部門に連絡を取る必要がありましたか？
- 今回のインシデントを基に運用方法を変更する必要がありますか？手持ちのツールを効果的に利用できましたか？ツールは適切に構成されていましたか？
- チーム間のコミュニケーションはどうでしたか？改善すべき点はありませんか？
- フィッシング攻撃や不適切なデータ処理など、社員側の問題はありましたか？それはトレーニングで改善できますか？
- 悪用された脆弱性は、特定の事業部門だけのものでしたか、それとも社内全体に存在するものでしたか？運用体制やプロセスを変更することで、その脆弱性に対処することはできますか？

IR計画は柔軟性が高いほど、侵害が発生した際に多くの教訓を得ることができます。学んだことはすべて準備のステップに反映し、常に改良・改善を行っていきましょう。



## まとめ

ランサムウェアをはじめとするサイバー脅威は、今後もなくなり、標的とされやすいネットワークや重要インフラは常に狙われ続けることになります。このeBookはサイバーハイジーンを幅広く理解し、IT部門が管理するエンドポイントをより効果的に保護するためのハイジーンガイドライン、ベストプラクティス、見識を提供することを目的としています。

計画から行動に移す過程で、サイバーハイジーンが破綻することが多々あります。断片化したツールやチーム間で情報が失われてしまうのです。

パッチやソフトウェアの導入を環境全体で効率的に進めるためには、IT運用チームとセキュリティチームが足並みをそろえて協力し、説明責任を果たさなければなりません。そのためには、システムを整備し、ワークフローを明確に定義する必要があります。



業界唯一の統合型エンドポイント管理 (XEM) プロバイダであるタニウムは、複雑なセキュリティとテクノロジー環境を管理するための従来のアプローチにおけるパラダイムシフトをリードしています。デバイス間の包括的な可視性、統一されたコントロールセット、そして「機密情報と大規模インフラの保護」という単一の共有目的に向けた共通のタクソノミを提供する単一のプラットフォーム内にIT、コンプライアンス、セキュリティ、リスクを統合することで、タニウムは、すべてのチーム、エンドポイント、ワークフローをサイバー脅威から保護します。タニウムは、「Fortune 100 Best Companies to Work For」に含まれ、6年連続で「Forbes Cloud 100」に選ばれています。実際、Fortune 100の半数以上と米軍は、タニウムが人々を保護し、データを守り、システムを保護し、あらゆる場所のあらゆるエンドポイントを監視して制御することを信頼しています。これが“The Power of Certainty”です。

[www.tanium.jp](http://www.tanium.jp)をご覧ください、[Facebook](#)と[Twitter](#)でフォローしてください。

サイバーハイジーンのアセスメントを実施することで、IT環境の健全性を可視化してエンドポイントの状態を把握できるようになります。そして、重要な問題を特定し、サイバーハイジーンを改善する方法を理解することで、大きな問題を起こさないための体制を整えることができます。タニウムがそのお手伝いをいたします。

エンドポイント管理やサイバーハイジーンによるセキュリティの強化については、ぜひタニウムにご相談ください。**お問合せ**はこちらから。

精度の高いリアルタイムのエンドポイントデータや制御機能を提供するTanium Platformの詳細については、[tanium.jp](http://tanium.jp)でご確認ください。