jamf

組織のセキュリティニーズを評価する

セキュリティニーズの評価が全般的なセキュリティ態勢にとって不可欠な理由

組織ごとに異なるセキュリティニーズを理解するには、理論的な側面と実践的な側面から絶妙にアプローチする必要があります。さらに、この二面性にもかかわらず、その基礎は論理に深く根ざしており、可視化やモニタリングを通じて得られたリスク評価や、エンドポイントテレメトリから収集される主要な脆弱性に関するデータを活用するとともに、適用される規制要件をしっかりと理解することが求められます。これらの要素をすべて組み合わせることで、セキュリティ対策ツールの設計図のようなものが完成し、コンプライアンス目標を達成（および維持）できるようになります。

組織の継続的な成功には、その状況を把握することがもっとも重要です。成功を維持する秘訣を尋ねれば、おそらくどの組織も、リスクを最小限に抑えつつ、ビジネスを前進させる機会を最大化することが鍵であると答えるはずです。つまり、組織のニーズをしっかりと理解し、その情報を実行可能なタスクに置き変えることです。このことは特に、不況や経営危機を乗り越えて経営を維持している企業や、数十年にわたってビジネスを維持してきた企業に当てはまります。

このホワイトペーパーのトピック

- リスクとは何か、そして収集されたテレメトリデータを使用してデバイスの健全性と全体的なセキュリティ態勢を可視化する方法
- リスク評価をセキュリティスタックの一部として定期的に行うべき理由
- 組織のセキュリティニーズを見極めるためだけでなく、既存または将来的なリスクから組織を守るためにデータを活用する方法
- コンプライアンス目標を達成しながら強固なセキュリティ態勢を維持するために、リスクデータをエンドポイントセキュリティソリューションと組み合わせることが大切な理由

このような考え方は、どのようなビジネスを経営しているかにかかわらず有効です。例えば、映画業界や音楽業界を見てみましょう。エンターテインメントは何世紀も前から存在しています。そして、程度の差こそあれ、視聴者が何を求めているかを見極めながら需要に合わせて提供するものを変化させることで、時代を超えて生き残ってきました。

つまり、現在進行形のプロセスなのです。

サイバーセキュリティも同じような形で進化を続けています。顧客のニーズを見極める代わりに、組織の内側に目を向け、安全でセキュアな事業運営を継続するために何が必要かを判断しなければなりません。リスク評価には、デバイスからソフトウェア、組織のインフラ、データ、プロセス、ポリシーまで、あらゆるものが含まれます。これらが組み合わさって、組織のセキュリティ態勢の全体像を作り出しているのです。

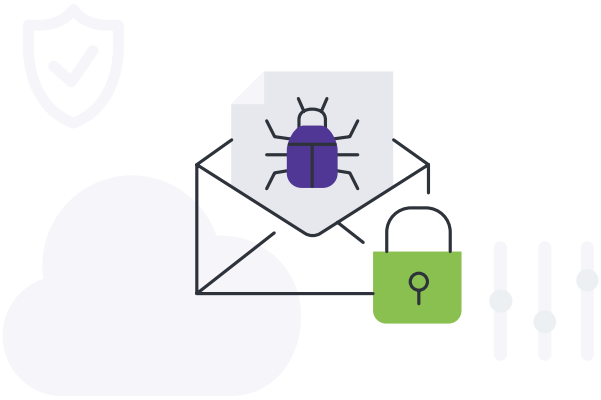
この情報を武器に、組織は既存のサイバーセキュリティ戦略のリスクや不足している点を評価し、それを是正するために必要な措置を講じることで、リスクを最小限に抑え、脅威を軽減することができます。

リスク評価は、1回行ったらそれで終わりではありません。ベストプラクティスに従って定期的に行うべきものです。テクノロジーは動的な性質を持っており、すべてが常に変化の過程にあります。このことが特に重要なのは、不具合が自然の成り行きで発生するものであり、それが脆弱性につながってセキュリティ態勢の低下を招いたり、最終的にはデバイス、ユーザ、データを侵害のリスクにさらしたりする可能性があるからです。

それだけでなく、ネットワークの防御に弱点がないか、もしくは悪用できる攻撃ベクトルがないか、徹底的に検証してくる脅威アクターの存在も忘れてはなりません。

簡単に言えば、リスク評価は包括的なサイバーセキュリティ戦略の一環として定期的に実施されるべきであり、そこで得られたデータは、セキュリティの現状を把握するためだけでなく、次のような組織の全体的な深層防御セキュリティ計画に反復的に反映されなければなりません。

- デバイスとアプリケーションのライフサイクルの各ステージ
- セキュリティソリューションの調達、構成、および導入
- 規制要件の達成とコンプライアンスの徹底
- 既存および新規の脅威の特定、および重大度や影響度レベルの割り当て
- リスク選好度とリスク軽減戦略の整合性の維持
- インシデント対応ステップの見直しと実施
- エンドユーザトレーニングなどの脅威防御戦略の見直しと実施



リスク評価

ここまでリスク評価が重要な理由について説明してきましたが、リスク評価とは実際にどのようなものなのでしょうか？そして、一体何がリスクにさらされているのでしょうか？詳細は業界や企業によって異なるものの、リスク評価とは以下の事柄を理解するためにあります。

- 脅威ランドスケープ
- 組織の脆弱性
- 攻撃を受ける可能性
- 攻撃が組織に与える影響
- 組織が深刻な攻撃からどれだけ早く回復できるか

> 「敵を知り、己を知れば百戦危うからず」**孫子**

では、リスク評価によって答えを見つけることのできる質問にはどのようなものがあるのでしょうか？

組織が抱える脆弱性にはどのようなものがありますか？

攻撃者は、ハードウェア、ソフトウェア、インターフェイス、ベンダーによるネットワークインフラの利用、およびこれらの要素にアクセスできるすべてのユーザなど、多くの侵入ポイントを経由してシステムへの侵入を試みます。さらに脆弱性は、ビジネスプロセスやポリシーにも現れる可能性があります。

これらの要素を分類しインベントリ化することは、以下を含む組織のインフラの状態をしっかりと理解するために不可欠です。

- どのデバイスがネットワークにアクセスしているか
- 誰が組織データへのアクセスを許可されているか
- セキュリティのベストプラクティス（最小権限アクセス、強固なパスワードポリシーなど）を適用しているか
- ベンダーがシステムに脆弱性を持ち込む可能性はあるか
- 潜在的な脅威を認識し、適切なセキュリティ対策を実践するためのトレーニングをユーザに提供しているか

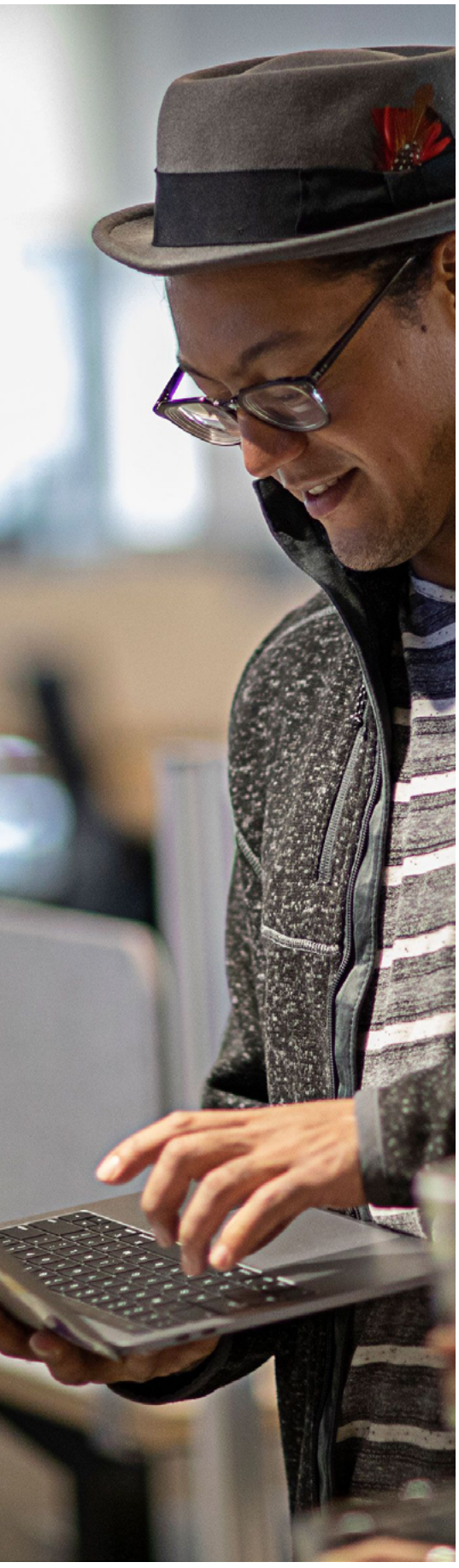
脅威にはどのようなものがありますか？

リスクを評価するということは、世の中にどのような脅威が存在し、それらがシステムにどのような影響を与えうるかを知ることでもあります。これにより、ITおよびセキュリティチームは、組織のもっとも脆弱な部分や攻撃を受ける可能性、そしてそれがビジネスに及ぼす影響について評価することができます。

例

MITRE ATT&CKフレームワークを参照することで、セキュリティチームは、脅威アクターがどのようにシステムを攻撃するかを理解するために必要な情報を得ることができます。また、未知の脅威に対しては、疑わしい行動や悪意のある行動を特定するために、AIや機械学習（ML）ソフトウェア、または脅威ハンティングの使用も検討すべきです。AIとMLは、ネットワークのベースラインから外れた異常な行動を特定してくれる縁の下の力持ちです。また、脅威インテリジェンスやパターンマッチングの膨大なデータセットを処理する能力により、サイバーセキュリティの武器として重要なツールとなっています。さらに、AIやMLから得られたデータは、より広範なセキュリティコミュニティと共有することができ、あらゆる場所で活躍するサイバーセキュリティ専門家の知識ベースをさらに強化することができます。

さらに、一般的な脅威のベクトルを知ることで、組織の防御を必要としている部分を優先順位付けすることができます。**データ侵害に関するVerizon社の2023年版調査レポート**によると、攻撃者は認証情報の盗難やフィッシング、脆弱性の悪用など多数の手段を用いて組織のシステムに侵入を企てています。一般的に、データ侵害は発生源が外部にあることが多く、少なからぬケース（40%にも上る）がパートナーソフトウェアの悪用によるものであることがわかっています。これらの脅威から組織を守るには、現在のインフラの状態やポリシーを慎重に分析する必要があります（詳細は後述）。



組織がサイバー攻撃を受けた場合、どのような影響が考えられますか？

脅威の可能性について理解することは防衛戦略における優先順位付けに役立ちますが、実際に攻撃を受けた際に組織のビジネスにどのような影響があるかを知ることも同様に重要です。**IBMのデータ侵害のコストに関する調査**によると、2023年のデータ侵害の平均総コストは445万米ドルでした。また、データ侵害を特定し、封じ込めるまでに平均277日を要するため、時間のロスにもつながります。あるいは、データ漏洩によって評判が下がったり、2023年に被害を受けた組織の57%がそうであったように、製品やサービスを値上げせざるを得ない状況になり、顧客との関係が悪化する可能性もあります。また、適用される基準に準拠していなかった場合、関連機関から罰金が課されるのは言うまでもありません。

次のステップ

当然ながら、攻撃の影響が大きければ大きいほど、関連システムを守ることを最優先事項としなければなりません。これは可能性の高い攻撃にも当てはまります。影響度と可能性という2つの指標を組み合わせることで、特定の脅威が組織にとってどの程度のリスクがあるかを定量化することができます。リスクをしっかり理解することで、優先順位を適切につけ、次のことを判断するのに必要な知識を得ることが可能になります。

- もっとも厳重な保護を必要としているシステムはどれか（例：攻撃を受けた場合、ビジネス運用に不可欠な機能にもっとも大きな損失を与えると思われるシステム）
- 最善の防衛戦略のためにどのようなコントロールを導入すべきか
- セキュリティ態勢を強化するのに最適なソフトウェアツール
- どの程度のリスクを許容できるか（リスク選好度）

ここまで来たら、次はリスク評価から学んだことを実行に移します。次のセクションでは、ネットワークとデバイスのテレメトリデータを評価する方法や、セキュリティポリシーを策定または改訂する際に使用できるガイドラインについて説明します。

可視化とモニタリング

リスクを評価および特定し、組織の許容範囲に沿ってリスク選好度を調整しました。さらに、リスクを軽減するために、セキュリティコントロールの選択や構成に関して必要な調整も行いました。堅牢なセキュリティ態勢が確立され、既存の脅威を特定するために必要なトレーニングが関係者に提供され、見つかった脅威を報告し、対処する必要についても理解してもらいました。エンドポイントは脅威から保護され、コンプライアンス目標は達成され、すべてのデバイスにこれらが適用されています。さて、ここから何をすれば良いのでしょうか？

ITやセキュリティチームの仕事はここで終わりなのでしょうか？残念ながら、答えは「ノー」です。

繰り返しになりますが、テクノロジーの動的な性質は常に存在するものであり、今この瞬間安全だからといって、それが永遠に続くとは限りません。蔓延するセキュリティ脅威からデバイス、インフラ、そして組織の安全を守る鍵は、エンドポイントの健全性を常に把握しておくことにあります。

> 「その地に詳しい案内役がいなければ
> 地の利益をおさめることはできない」
> **孫子の兵法書**

デバイスの健全性を積極的に監視して得られたテレメトリデータには、デバイスと組織のセキュリティ態勢を維持するための豊富な情報が含まれています。それだけでなく、コンプライアンスについて言えば、テレメトリデータは、エンドポイントが規制要件を満たすように適切に設定されていることを確認し、組織のエンドポイントがどの地点においてもコンプライアンスに準拠していたことを証明する指標を提供するための重要な要素となります。特に、クレジットカード支払い手続きの安全な処理を行うための基準である**PCI-DSS**への準拠を目指す場合は、このようなコンプライアンスの証明が不可欠です。

さらに重要なのは、モニタリングによって得られる可視性が、すべてのデバイスレベルとアプリケーションライフサイクルにおける意思決定に反映されることです。モニタリングプロセスには、ITまたはセキュリティチームに、デバイスの健全性、デバイスに搭載されているソフトウェア、およびエンドユーザのアクションに関する最新情報を提供できるという性質があります。また、豊富なテレメトリデータの提供により、デバイスのコンプライアンスやユーザまたはデータの安全を維持する上で必要な調整に関して、経営陣や管理者が適切な意思決定を行えるようにします。

モニタリングではどのようなデータが収集されますか？

モニタリングによって収集されるテレメトリデータの種類について見ていく前に、まず2種類のモニタリングについて説明します。

- **パッシブ：** エンドユーザや監視対象デバイスのパフォーマンスへの影響を最小限に抑えるため、一定期間にわたって健全性データをゆっくりと収集します。データキャプチャの頻度が低いことで、テレメトリデータの収集に時間がかかり、完全な形のデバイスベースラインの構築に遅れが生じます。また、データ収集に遅れが生じると、特にデータキャプチャの間隔が数日～数ヶ月になってしまう場合、データの正確性やタイムラインに直接影響が及ぶことがあります。

- **アクティブ：** 健全性データがエンドポイントから頻繁に通信されます。エンドポイントのポーリングは定期的に行われ、多くの場合リアルタイムで一カ所のレポジトリに送信されます。

取得されるデータの種類はほぼ同じですが、両者の大きな違いは以下の通りです。

- テレメトリデータの**取得方法**
- ベースラインプロファイルの構築にかかる**時間**
- 情報の**正確性**
- テレメトリーデータの**更新頻度**

どちらのモニタリングタイプにもそれぞれメリットとデメリットがありますが、最新の脅威ランドスケープはあまりにも広大で変化が激しく、もはやアクティブモニタリング以外の方法では、デバイスの最新の健全性データを有効的に収集し、それをアクション可能なデータに変換し、セキュリティ計画のギャップを埋めることはできなくなっているのが現実です。このことは、SecurityWeekの記事である「**Active vs. Passive Monitoring: No longer an either-or proposition**」に含まれる名言「You can't protect what you can't see（目に見えないものを守ることはできない）」に表れています。

収集されるテレメトリデータの種類と、セキュリティ態勢における意味

- **OSアップデート：**オペレーティングシステム（OS）の更新レベルを判断し、デバイスが最新の機能をサポートしているか、また脆弱性を最小化するために既知の脅威に対する最新の保護機能を備えているかを把握します。
- **アプリのパッチレベル：**アプリもOSと同様、処理中のデータの保護やバグの修正、リスクを生み出す可能性のある脆弱性の対策などの目的でパッチが必要です。
- **構成設定：**デバイスの堅牢化は、セキュリティ態勢にとって極めて重要です。正しい構成がセキュリティを最大化するために大切なのはもちろんですが、エラーに関連する**データ漏洩の21%（Verizon社のデータ侵害に関する2023年の調査レポートに基づくデータ）の原因**となった構成ミスを最小化することも同じくらい重要です。
- **ネットワークアクティビティ：**デバイスがどのようなウェブコンテンツと通信しているか、信頼性が確立されていない接続は保護されているか、どのポートがデータを転送しているのかなど、ネットワーク利用をめぐるこういった質問やその他の重要な質問に対する答えは、デバイスのセキュリティ態勢を決定する上で極めて重要です。
- **行動分析：**ユーザがセキュリティチェーンの中でもっとも弱いリンクと考えられているのには理由があります。ソーシャルエンジニアリング攻撃の継続的な成功には、ユーザの異なる理解レベルが関係しています。ユーザがどのようにデバイスを利用しているかを理解することで、管理者はユーザが誘発するリスクがどのように発生するかをより明確に把握することができ、その結果、彼らをより効果的に保護する方法を知ることができます。
- **認証監査：**認証プロトコルとパスワード管理は、デバイスとその機密データのロックを解除する鍵となります。さらに大きく頑丈な鍵や、さらに複雑なパスワードがあったとしても、ユーザの認証情報が共有されていたり、アカウントが侵害されていた場合にそのことを知らせてはくれません。これは、リモートワークやハイブリッドワーク環境を持ち、様々な場所に分散したワークフォースがポリシーベースの管理を必要としている組織の場合、離れた場所にあるエンドポイントのセキュリティを確保する上でさらに重要となります。
- **悪意のあるコード：**悪意のあるコードは、さまざまな形で発生する可能性があります。正規のアプリやサイドローディングされたアプリを装ったトロイの木馬のダウンロードから、危険なサイトへの無意識の訪問、終わったと見せかけて密かにバックグラウンドで実行されている脅威まで、モバイルデバイスに関連した攻撃の普及と増加を考えると特に、これらはすべてコンプライアンスを脅かす危険を孕んでいます。
- **エラーログ：**デバイスはすべてをログに記録するため、管理者が担当するデバイスが増えれば増えるほど、ログに記録されたすべての問題に対処するのが難しくなります。これは脅威アクターにとっては素晴らしいことですが、管理者にとっては最悪です。しかし、この状況を黙って受け入れる必要はありません。きちんと適切に管理し、セキュリティ情報イベント管理（SIEM）ソリューションを活用して圧倒的なテレメトリのストリームを分類および理解することで、ログ作成や脅威検出を効果的かつ効率的に行うことが可能です。
- **システムプロセス：**エンドポイントセキュリティ管理者は、デバイス上で実行されているアプリを把握しておく必要があります。デバイス自体の平均的なベースラインに加え、データ漏えいを可能にしたりユーザプライバシーに対するリスクを増大させたりすることでセキュリティを低下させる可能性のある、承認されていない（シャドーIT）または許可されていない（制限された）ツールの使用を管理者に警告します。
- **監査コンプライアンス：**エンドポイントの健全性の可視化は、既知の事実だけでなく、未知の事実を発見する上で重要です。規制のある業界の場合、コンプライアンス目標を達成するために何が必要かを理解し、その達成の証拠を収集することで、コンプライアンスにおける組織の立ち位置を把握することができます。

テレメトリデータを使って自動的にリスクを軽減することは可能ですか？

可能です。リスク管理には、それを著しく難しくする以下のような要因があります。

- 大量のデバイスや複数のデバイスタイプの購入
- 個人所有および会社所有のデバイスから成るフリートのセキュリティ維持
- リモートワークやハイブリッドワークにより分散した従業員のサポート
- 標的に対して複雑で多面的な攻撃を行う複数の脅威の融合
- エンドポイントのコンプライアンスを維持するためのセキュリティ設定の適用

テレメトリーデータの収集、分析、分類は、各段階を手動で行うよりも自動化してしまった方が便利です。膨大な量のデータに目を通し、それぞれの作業をできるだけ手早く完了させるためには膨大な時間が必要になりますが、当然ながら人間は食事や休憩をせずに働き続けることはできません。

このような制限はコンピューターには当てはまりません。

自動化を通じて「重労働」をこなすシステムを活用することで、組織は貴重な時間とコストを節約し、それを攻撃を未然に防ぐことに費やして、攻撃の後始末に奔走する事態を避けることができます。

アクティブモニタリングは、組織のセキュリティニーズを理解するためのセキュリティ計画において、リスクアセスメントに次ぐ2番目のレイヤーとして機能します。フリートを継続的にモニタリングすることによって、テレメトリーデータをリアルタイムで収集・配信することができ、ここから得られた最新のエンドポイント健全性データは、エンドポイントセキュリティソリューションによって分析・処理され、各デバイスがどのような状態にあるかを判断するために使われます。さらに、異常や怪しい動作が検出された場合は、次のステップを決定するためにITチームやセキュリティチームに自動的にアラートを送信することができます。また、このような検出機能を利用して自動的にインシデント修復ワークフローをトリガーすることも可能で、例えばデバイスから既知の疑わしいソフトウェアを自動的に削除したり、ランサムウェアに感染したエンドポイントを隔離したりできます。

さらに、エンドポイントセキュリティソリューションとその他のツール（例：アイデンティティ管理、MDMなど）を統合して、より高度な自動化機能を提供する堅牢なワークフローを作成することも可能です。

コンプライアンス

この資料では、リスクを評価するための徹底的な調査を行い、組織のセキュリティニーズをよりよく理解するための準備をする上で、ITやセキュリティ専門家の助けとなるいくつかの中心的なテーマをまとめるために、孫子の兵法から様々な引用を掲載しています。これは、それぞれのステップの独自の重要性を理解し、あらゆるギャップを埋める上で重要な教訓を提供してくれるはずです。さらに、それぞれのステップにおいて、今ある情報を次のステップに生かすことで、先に進むことができます。

セキュリティニーズを理解するということは、今現在どのようなセキュリティ問題が存在するかを知るということだけに限定されません。ここには、その組織が規制のある業界に属しているかどうかに関わらず、問題を解決するために必要なものを特定し、エンドポイントがコンプライアンス上のニーズを満たしている状態を維持するために必要な戦略を選択することが含まれます。目標は、規制要件への準拠を維持すること、規制要件を持たない企業の場合は、組織のポリシーへの準拠を維持することです。どちらも、デバイスと組織のセキュリティ態勢を強固に保つための構造化されたフレームワークを使用してリスクを軽減することで、セキュリティとユーザのプライバシーを守る役割を果たします。

> 「最高の戦術とは、戦わずして敵を制圧することである」**孫子**

この場合の「敵」とは、脅威アクターや、組織にリスクをもたらす可能性のあるあらゆるものを指します。結局のところ、リスクとは負債であり、脆弱性を悪用する、あるいはさらに悪い結果を招きかねない事態を許してしまいます。しかし、セキュリティの必要性を理解する上で、今現在のネットワークのより具体的な状態を無視して、多数の潜在的な「敵」について心配することは無駄といえます。さらに、リスクの発生源ではなく、さまざまなリスクそのものに注意を向けることも大切です。これにより、管理者は、デバイス、ユーザ、データを現在の脅威だけでなく、将来的に拡大および進化する脅威の両方から保護し、コンプライアンスの維持のための進路を見極めることにフォーカスすることができます。

さまざまなタイプのリスクを特定および最小化するのに役立つ業界別のガイダンスにはどのようなものがありますか？

本題に入る前にまずは、「ガイドライン」、「フレームワーク」、「ベースライン」の違いについて見ていきましょう。ガイドラインはベストプラクティスと近しい関係にあります。必ずしも従わなければならない厳格なルールではなく、組織が一般的な能力の範囲内で様々な形態のリスクを管理するのに役立つ実践事項を集めたものです。

一方、ベストプラクティスと似た成り立ちを持つフレームワークは、特定の組織目標やコンプライアンス目標を達成、あるいはそれ以上のレベルに到達するために必要なすべての情報、プラクティス、設定、コントロール、ワークフローを統合することを目的としています。

ベースラインは、コンプライアンスの達成と維持に果たす役割において、前者の2つのガイダンスと類似していますが、こうした目標の達成に別の角度から挑みます。ガイドラインはベストプラクティスのためのアイデアを提供し、フレームワークはそれらを構造的に整理し、特定の目標を達成するためにフォーマット化しますが、ベースラインはこれらとは異なる方法で適用されます。ベースラインは、コンプライアンスや組織の目標の達成における成功度を測るバロメーターのような役割を果たします。

これを料理に例えれば、ガイドラインは食材のようなもので、フレームワークは特定の料理を作るために異なる要素を組み合わせたものです。さらにベースラインは、この料理が正しい食材を使ってレシピ通りに作られたかどうかを判断する役目を果たします。これなら分かりやすいのではないでしょうか？

これらの違いを理解した上で、セキュリティのニーズを理解し、可能な限り正確に対処することを目的として、フレームワークとベースラインについて見ていきましょう。

セキュリティ計画でよく使われるフレームワーク

National Institite for Standards and Technology (NIST) SP800-53, Rev. 5: Security and Privacy Controls for Information Systems and Organizations：多様な脅威やリスクから組織の運営と資産を保護するために、情報システムおよび組織のためのセキュリティおよびプライバシーコントロールの一覧が掲載されています。

NISTIR 8011, Vol. 4: Automation Support for Security Control Assessments：個々の情報セキュリティ能力におけるセキュリティコントロール評価の自動化に焦点を当てると同時に、ネットワーク上のソフトウェアに存在する欠陥によって生じるリスクの管理についても言及しています。

ISO/IEC 27001: Information Security Management Systems (ISMS)：ISMSが満たすべき要件を定義するためのもっともよく知られた規格のひとつで、情報セキュリティマネジメントシステムの確立、実施、維持、および継続的な改善のための全体的な指針を提供するフレームワークを提供します。

Cyber Essentials: 英国を拠点とするイニシアチブで、組織の規模にかかわらず、もっとも一般的なサイバー攻撃全般から組織を保護する方法を案内しています。コンプライアンスを確認するための実践的かつテクニカルな検証方法を含む、様々なレベルのガイダンスが提供されています。

MITRE ATT&CK:実際に使用されたテクニックの調査から集められたサイバー攻撃者の様々な戦術をまとめたグローバル規模の知識ベース。特定の脅威モデルや方法論を開発するための基盤として、さまざまな業界、コミュニティ、エンドポイントセキュリティソリューションで使用されています。

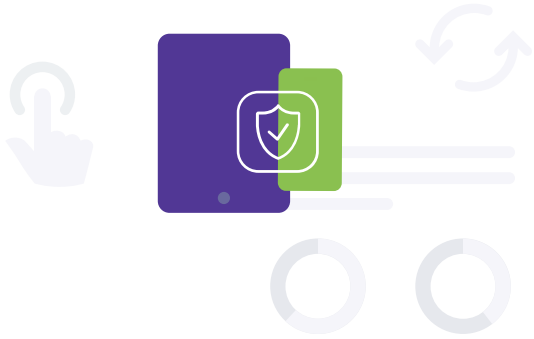
Control Objectives for Information and related Technology (COBIT) 2019: ISACAが作成したフレームワークで、IT管理のための一般的なプロセスにフォーカスおよび定義し、それらをビジネスおよびIT関連の目標に結びつけます。ここには、ISO 27001、ITIL、その他の一般的なプロジェクト管理フレームワークなど、他のフレームワークとの柔軟な連携を可能にしながらチームの責任を確保するための測定要素が含まれています。

Payment Card Industry Data Security Standard (PCI-DSS): クレジットカード決済データの取り扱いに関する技術的および運用上の要件を規定する実質的な情報セキュリティ基準で、世界中の主要なカード発行会社によって適用されています。

Cybersecurity Maturity Model Certification (CMMC) 2.0: NISTの特別刊行物（Special Publication）のセキュリティ要件に基づいた複数レベルから成るモデルで、CMMCレベルと関連する一連のプラクティスをドメイン全体で累積的に満たした組織に対して、認証レベルを提供します。

OWASPのリスク評価：OWASPによるこのフレームワークは、セキュリティテスト、リスク評価、スキャニングツールから構成され、環境のセットアッププロセスに関連する互換性や複雑さに起因する不確実性を排除し、追加のセットアップなしでコードの品質や脆弱性を分析・見直すことのできるシンプルな方法を提供することを目指しています。

macOS Security Compliance Project: NIST、米国航空宇宙局（NASA）、国防情報システム局（DISA）、ロスアラモス国立研究所（LANL）といった連邦組織のITセキュリティ担当者による共同プロジェクトで、特定の規制要件へのコンプライアンスを達成するために導入できる構成設定を含む、セキュリティガイダンスを生成するためのプログラムを通じたアプローチを提供するオープンソースの取り組みを行っています。



サイバーセキュリティにおけるベースラインの役割

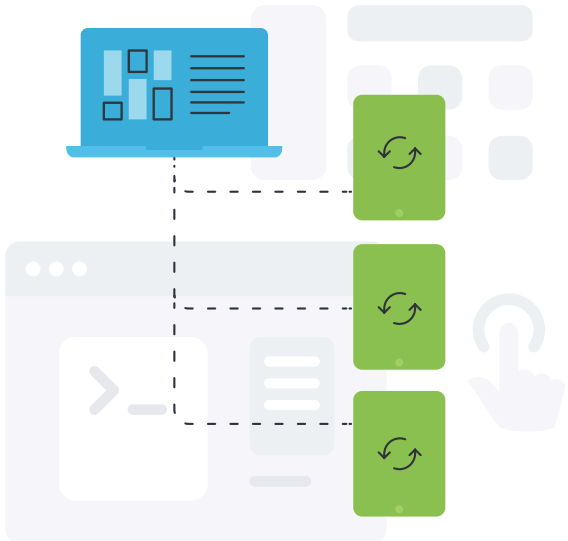
Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs): 米国国防総省（DoD）が管理する構成基準であるSTIGsには、コンピューティングシステムの安全性を確保するための具体的な要件が含まれています。論理設計やハードウェアアプライアンス上で実行されるプロトコル、およびそこで実行されるソフトウェアなどが含まれたこのガイドは、「ソフトウェア、ハードウェア、物理的および論理的アーキテクチャのセキュリティを強化し、脆弱性を減らす」ことを目的としています。

Federal Information Processing Standards (FIPS) 200: 同じくNISTが米国向けに開発した、米国政府や請負業者が使用する非軍事用コンピューティングデバイスやシステム向けの標準。FIPS基準がさまざまなセキュリティベースラインをカバーする一方で、FIPS 200は、連邦政府機関によって使用される、または連邦政府機関に代わって使用されるデータが、目的における各カテゴリーの最低限の情報セキュリティ要件を満たしていることを確認するための標準を提供し、**セキュリティの三原則**に基づいてセキュリティ目的に対する影響レベルを分類しながら、さまざまなリスクレベルに応じて適切なレベルの情報セキュリティを保証します。

NIST SP 800-39：包括的な企業リスク管理（ERM）ソリューションと統合する際に有用な広範なガイダンスで、他の基準やガイドライン、フレームワークと連動して継続的にリスクを評価、対応、およびモニタリングするための具体的な詳細を提供します。

Center for Internet Security (CIS): CISベンチマークは、25以上の製品ファミリーを対象とした構成の推奨事項を提供しています。世界中のサイバーセキュリティ専門家のコンセンサスに基づいて開発されたベンチマークは、セキュリティの構成ガイドとして世界中の政府や産業界で受け入れられており、いくつかのエンドポイントセキュリティソリューションの基礎基盤として統合されています。

Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Performance Goals (CPGs):CISA、NIST、および省庁間コミュニティと連携して開発されたこのCPGは、すべての重要インフラセクターに対して、広範かつ一貫性のあるサイバーセキュリティのベースラインパフォーマンス目標を提供します。特にサイバーセキュリティに着手しようとする中小規模の組織にとって有用ですが、サイバーセキュリティに関して長年の経験をもつ組織にとっても現状の見直しや改善のためのベンチマークとしての役割を果たします。



リスク評価＋継続的なモニタリング＋セキュリティガイダンス ＝ コンプライアンス管理の成功

> 「己を知れば百戦あやうからず」**孫子**

これらの要素は、単独ではある程度しか組織に貢献できませんが、組み合わせることで以下のようなメリットをもたらします。

- 負債の特定
- エンドポイントの健全性レベルの把握
- 設定の堅牢化による攻撃の最小化
- コンプライアンス目標の達成

しかし、ベースラインを確立し、積極的なモニタリングと豊富なテレメトリデータの再評価によって測定を行い、デバイスやインフラ全体のセキュリティ態勢を継続的に改善するためにこのサイクルを繰り返すことで、コンプライアンスを維持することもできます。

前述したように、これは反復的なプロセスで固定的なものではありません。目標が達成されたら終わりというものでもありません。セキュリティコントロール、プロセス、ワークフロー、要件、ポリシー、各デバイスの構成設定、エンドユーザ、そして組織の機密データについて、反復的に確認し、情報を得る必要があります。

規制の厳しい業界にある組織なのか、あるいは規制はないものの組織のポリシーに沿ったサイバーセキュリティ戦略と確実な管理コントロール（例：利用規約の強制適用）を採用したいと考える企業なのかに関わらず、上記の各構成要素は、組織のセキュリティニーズと情報について理解し、不足している部分を埋めるための部品であると考えるのがベストです。

Mac管理者の中には、組織にどのようなリスクが存在するかをすでに把握し、デバイスの健全性データも豊富に持っているものの、組織が現在置かれている状況と、実際にコンプライアンスを得るために必要な状況との間のギャップを埋めるために実際に何をしたらいいのかわからないと考える人もいるかもしれません。

Jamfにお任せください

「JamfはAppleを活用する組織を支援します」

これは単なるキャッチフレーズではなく、Jamfの使命そのものを表したフレーズです。そして、私たちはこれを実際に行なっています。JamfがAppleデバイス管理のゴールドスタンダードであることは、自他ともに認める事実です。Jamfがこのような高い評価を得ているのは、私たちが開発する業界トップクラスのソリューションが、世界中のあらゆる業界の無数の組織で数百万台ものデバイスの管理とセキュアな運用の成功に貢献しているからです。

Jamfは、Appleデバイスを使用する組織が業務においてその可能性を最大限に活用できるようサポートしています。しかし、Jamfは実際にどのようにして、それぞれの組織特有のニーズやコンプライアンス目標を特定および理解しながら、Appleフリートを包括的かつ全体的に管理するためのツールを提供しているのでしょうか？

エンドポイントの確実な検証

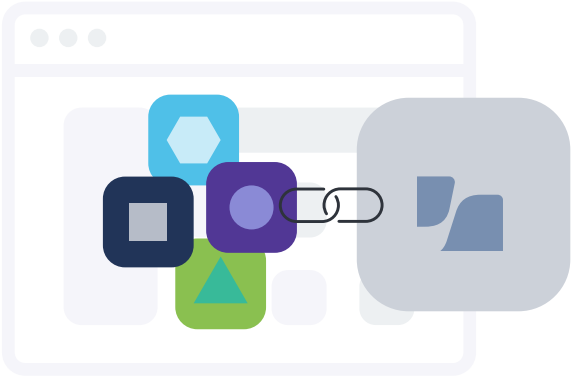
セキュリティニーズを理解するためには、組織内で使用されているエンドポイントの状況を把握することが何よりも重要です。各デバイスの健全性を確認するための豊富なテレメトリデータがなければ、管理者は推測だけで仕事をすることになり、最悪の場合、判断ミスが悲惨な結果を招く可能性があります。

管理者としては、**ただ単に知りたいのではなく、知る必要がある**のです。また、コンプライアンスに関して言えば、規制への遵守が求められる場合でも、もしくは組織のポリシーとの整合性が求められる場合でも、組織のニーズがあらゆる段階で満たされていることを確認するために、エンドポイントの健全性の状態を随時確認する必要があります。

ソーシャルエンジニアリングは脅威アクターがもっとも頻繁に利用する攻撃ベクトルであり、組織のリスク要素が悪用される可能性があります。具体的には、組織の現状のリスクを悪用し、感染したデバイスがビジネスリソースに接続する際に認証情報を盗んだり、悪意のあるコードを侵入させたりします。

ゼロトラストネットワークアクセス（ZTNA）のようなテクノロジーでは、リソースへのアクセスを許可する前にエンドポイントの健全性を一連の要件と照らし合わせてチェックし、デバイスが最低限のセキュリティレベルを満たしていることを確認することで、デバイスを保護します。**Jamf Connect**のようなZTNAを使用したソリューションは、「決して信用せず、常に検証する」をモットーに、アクセスを要求しているのが登録済みの信頼できるデバイスであることを確認することで、アイデンティティ&アクセス管理を土台にしたセキュリティ戦略を実現します。

また、**Jamf Protect**のようなエンドポイントセキュリティソリューションは、macOS、iOS、iPadOS、Android、Windowsデバイスにセーフティネットを提供し、オンデバイスおよびネットワーク内に潜む脅威の分析を通じて、脅威の迅速な検出やいち早いインシデント対応に加え、**セキュリティ、プライバシー、パフォーマンスを犠牲にしない有効かつ自動化された脅威対策および修復のワークフロー**を実現することで、デバイス（および生産性維持のためにそれを使用するユーザ）をマルウェアなどの脅威から保護します。



インフラ全体における優れたユーザ体験と信頼性

セキュリティのニーズは、デバイスが初めてビジネスリソースにアクセスする時に初めて発生する訳ではありません。

ユーザが電源を押した瞬間からすぐにデバイスを使用できるようにするプロセスのことを「ゼロタッチ導入」と呼びます。この導入ワークフローでは、Apple Business ManagerまたはApple School ManagerとJamfが自動的かつ安全に統合されます。

会社所有のデバイスであるか個人所有のデバイスであるかに関わらず、**Jamf Pro**はBYODからユーザ登録デバイスまで様々なオーナーシップモデルをサポートし、ユーザのプライバシーを守りながらセキュリティを確保します。また、セキュリティに関して言えば、JamfのMDMソリューションは**セキュリティとプライバシーの強化機能を含むすべてのApple機能に対して同日サポートを提供**しており、エンドポイントセキュリティに妥協することなく、ユーザが効率的かつ生産的に働ける環境をサポートすることができます。

アプリケーション管理もまた、セキュリティニーズの重要な部分を担っています。オペレーティングシステム（OS）やアプリケーションにアップデートを導入することは、セキュリティ計画を成功させるための重要な手段になります。

結局のところ、いくらセキュリティの必要性を理解していても、問題が発生したときに何も対処できなければ意味がありません。Jamf Proなら、OSアップデートがリリースされた時にデバイスを一括管理コマンドでアップデートすることができるので、**アプリのライフサイクル管理の簡素化**を望むMac管理者にとっても便利です。もちろん、Jamf独自のアプリカタログである**Self Service**の存在も忘れてはなりません。パワフルなAppインストーラに加え、エンドユーザが必要とするアプリが常に管理され、簡単にアクセスでき、自動的に最新バージョンに更新され、安全な状態に保たれていることを確認できます。

さらに、深層防御型の包括的なセキュリティ戦略を実現するには、アイデンティティとアクセスの効率的なプロビジョニングが不可欠です。信頼できるユーザだけがいつでもどこからでもデバイスやリソースにアクセスできるようにし、信頼できるアクセス（Trusted Access）を確立することは、特にワークフォースが分散した状態でデバイスを管理する際に大きな違いをもたらします。これにより、ゼロタッチの導入やシームレスなオンボーディング、日々の業務、ビジネスリソースへのアクセスまで、ユーザにデバイスへの簡単な認証方法を提供し、生産的に働くことのできる環境を提供することができます。さらに**Jamf Connect**によるZTNAと条件付きアクセスにより、**効果的で適応性があり柔軟なセキュリティを確実に実現**することができます。

3つの重要なセキュリティ要素を信頼できる1つのプラットフォームでまとめて提供

「チャンスは掴めば何倍にもなる」**孫子**

Trusted Accessは、様々な業界の組織が抱えるデバイス管理とセキュリティのニーズを包括的にサポートするための総合的なアプローチです。

Trusted Accessの構成要素である**デバイス管理**、**エンドポイント保護**、**可視性とコンプライアンス**は、効果的で深層なセキュリティ戦略にとって極めて重要です。これにより、デバイス、ユーザ、データに対して高度なアクセス制御とセキュアな構成を適用する一方で、テレメトリデータを活用してセキュリティ態勢やデバイス、組織の変化に対応し、セキュリティやプライバシー、コンプライアンスを維持することが可能になります。

Trusted Accessなら、いつでもどこでも、手間をかけずにAppleフリート全体を柔軟かつセキュアに運用することが可能です。

Jamfの業界トップクラスのソリューションで組織のセキュリティニーズを再評価する方法に興味のある方は、ぜひ当社までお問い合せください。

トライアルへのお申し込み

または、お近くの販売代理店までお問い合わせください。

jamf

www.jamf.com/ja/