ivanti

管理、自動化、優先順位付け（M.A.P）サイバーセキュリティジャーニー

Everywhere Workplaceのためのサイバーセキュリティを実現する包括的アプローチの6つのステップ

目次

このEブックを読むべき理由

ソフトウェアの脆弱性、マルウェア、機密情報の盗難、その他の脅威ベクトルに起因する攻撃は、頻度と巧妙さの両面において急増しています。さらに問題を深刻化させているは、リモートワークへの急速な移行に伴う、「Everywhere Workplace（場所にとらわれない働き方）」の進展や、予算とセキュリティを熟知したスタッフの数が非常に限られていることです。すべての脆弱性に対処することは、以前は困難な状況であったところ、現在では至難の業となっています。

このような状況下において、企業やIT部門では、セキュリティ体制を強化し、継続的なサイバーリスク管理を確実なものとし、混乱を減らす包括的なセキュリティ戦略が必要になっています。それはつまり、PCとデータセンターが支配する世界のために設計されたソリューションから、モバイルとクラウド技術が最も重要であるEverywhere Workplaceのために設計されたソリューションに移行することを意味します。

本Eブックは、こうしたサイバーセキュリティへの道のりを進んでいくための出発点とステップの枠組みとして役立てていただけます。このEブックの推奨事項に従うことで、Everywhere Workplaceで増え続ける脅威に対して、ユーザー、デバイス、ネットワーク、アプリケーションとデータの保護に向けて動き出すことができるのです。

はじめに

今日のサイバーセキュリティの状況

脅威は迫っているのではありません。すぐそこにあるのです。なぜこのような状況になってしまったのでしょうか？

Everywhere Workplace（場所にとらわれない働き方）の急速な普及により、脆弱性の露出ポイントが異常に増加しました。リモート環境でのデジタルビジネスへの急激なシフトは、当初は一時的なものだと思われていましたが、今もそのまま継続されています。Gartner[1]によると、82%の企業はリモートワークをある程度許可する意向であり、47%は今後フルタイムでリモートワークを許可する意向があるそうです。パンデミック前にはPCとデータベース中心のセキュリティソリューションに依存していましたが、従業員の分散や、個人のモバイルデバイスやクラウドアプリケーションの広範な使用に直面して、もはや十分ではありません。

その好例が、QRコードです。QRコードは、レストランや診療所まで、あらゆる場所に浸透しています。従業員が業務で使用しているモバイル端末でスキャンされることもあります。しかし、QRコードの普及と使いやすさは、フィッシング攻撃の理想的な手段にもなっています。電子メールによるフィッシング対策だけでは、ユーザーも企業も攻撃に対して脆弱なままです。

さらに悪いことに、あらゆる種類の脅威が巧妙化し、特にリモートワークで発生する脆弱性を標的にすることが多く、驚異的なスピードで発生しています。例えば、フィッシング攻撃は、前年比で85%増加（74%の企業が被害に遭っている）、2021年には企業の59%がランサムウェアの被害に遭ったと報告されています。世界的なセキュリティの専門家不足に加え、どの企業も予算が厳しい中、セキュリティとIT部門は、脆弱性の整理と優先順位付けという単純な作業に、大半の時間（53%[2]）を費やしているのです。

このことは、働き方が変化し、保護すべきものが多すぎるのに対し、行動するための十分なリソースがない、という最悪の事態です。現状維持という選択肢はありません。行動を起こさない企業は、ランサムウェア、フィッシング、ハッキング、社内従業員による脆弱性（故意かどうかに関わらず）など、より多くの情報漏えいに遭い、絶えず変化するコンプライアンス要件に抵触する可能性があるのです。予期せぬダウンタイム、コンプライアンスの問題、評判や顧客の損失などによって、企業ブランドへの影響は甚大です。1件のデータ漏洩につき、424万ドル（4億8000万円）のコストがかかると推定されていま[3]。ランサムウェアの攻撃は、平均22日間[4]の業務中断を引き起こします。また、コンプライアンス違反によって、企業は13億ドル（1,400億円）以上の損失を被っています。[5]

「働き方が変化し、保護すべきものが多すぎるのに対し、行動するための十分なリソースがない、という最悪の事態です」

今こそM.A.P—サイバーセキュリティジャーニー

M.A.Pとは、Manage（管理）、Automate（自動化）、Prioritize（優先順位付け）の頭文字を取ったもので、Everywhere Workplaceのための包括的で拡張性の高い、フレームワークに沿ったサイバーセキュリティ戦略を構築するための3つのフェーズからなる行程です。

最初のフェーズである**Manage**（管理）は、サイバーセキュリティの基盤を確立するためのものです。この第1フェーズでは、未知の状態から既知の状態に移行することを目標にしています。つまり、どのようなユーザーがいて、どのようなデバイスやアプリケーションを使っているのかを可視化し、自社のどこに脆弱性があるのかをよりよく把握できるようにします。また、管理されていないデバイスでビジネスリソース（特にクラウドでのリソース）にアクセスしたり、最新のパッチを適用していないなど、組織を危険にさらす可能性がある慣行を排除することも意味します。

第2フェーズの**Automate**（自動化）は、負担を軽減することを目標にしています。既知の状態に到達したら、次のステップは、在庫の管理やデバイスのオンボーディング、ワークスペースやアプリケーションの展開などの反復的な手動プロセスを自動化させ、リソースを解放することです。また、自己修復およびセルフサービスのソリューションを追加することで、IT部門の介入の必要性をさらに減らすことができます。

最後の第3フェーズである**Prioritize**（優先順位付け）は、IT部門がリスクの高い領域を特定して対処するための情報と能力を備えられる状態にすることを目標としています。自動化されたとはいえ、IT部門の介入を必要とする領域は依然として存在します。優先順位付けは、IT部門にリスクに対処するために非戦略的で推測に基づくアプローチをさせるのではなく、適切なデータとリスクスコアを使用してIT部門がリスクへの対応と修復にインテリジェントで戦略的なアプローチをとることを可能にさせます。

M.A.Pは、企業ごとに異なりますが、どのような場合でも、ユーザー、デバイス、ネットワーク、アプリケーション、データという主要な柱にまたがり、次のような一貫した要素を含む必要があります：

- 検出
- 管理
- 安全な構成の実行と検証
- 最新のリスクベースのパッチ適用システム
- 認証情報の確認によるリスク低減
- アダプティブな（適応型の）制御とライフサイクル管理

このアプローチでは、すべての攻撃を防ぐことはできませんが、攻撃対象領域を最小化し、プロアクティブでインテリジェントなリスク管理を可能にすることで、できる限りの備えをすることができます。また、脅威が顕在化した場合には、迅速に対応できるよう設計された継続的なサイバーリスク管理により、セキュリティのリスクを軽減し、ビジネスの中断を最小限に抑制できます。

潜在的なメリットとしては、可視性の向上、業務システムにアクセスする非管理・非準拠デバイスの減少、パッチ適用にかかる時間の短縮、監査失敗のリスクの減少、財務的な節約などがあげられます。適切なツールを使用することで、手作業を減らすことでこれらすべてを実現できます。

ビジネスを停滞させるジレンマと、停滞を脱するための6つのステップ

先述したようなメリットは、聞こえはいいですが、実現するのは難しいと感じられることもわかります。最初は、明確な答えのないジレンマのように思えることでしょう。セキュリティの強化、脅威の低減、生産性の向上、リソースの節約が必要であるにもかかわらず、我々は非常に手薄の中、拡大する脅威の状況と攻撃に直面しているため、今すぐに新しいプログラムを実装するための余裕がありません。

だからこそ、当社は企業のセキュリティを支援する6つのステップを作成しました。それぞれが今日の効果的なサイバーセキュリティに不可欠な要素を網羅しており、これらを組み合わせることで、包括的で拡張性のあるサイバーセキュリティ管理戦略の基礎となります。

ステップ 1

アセットを完全に可視化する

理解していないものを管理することはできません。一元管理されたクラウドとアセット（ハードウェアとソフトウェア）の正確なインベントリがなければ、組織は脆弱なままとなり、セキュリティリスク、コンプライアンスの欠陥、複雑すぎるトラッキング、データの混乱を招きます。

世界的にITリソースが逼迫している今こそ、チームの力を最大限有効に活用できる自動化プラットフォームに投資すべき時なのです。包括的な検出イニシアティブは、企業所有とBYODの両方を含むネットワーク上のすべてのアセットを発見し、コンテキストに沿ってそれらをマッピングすることで、誰がどのデバイスを使用しているか、そのデバイスが貴社の組織とやり取りする場合にいつどのように使われているか、そして何のアクセス権を持っているか把握することができます。

検出には以下のようなメリットがあります：

- すべての接続されたデバイスとソフトウェアおよびそれらのコンテキストからリアルタイムで完全な可視化された情報を収集
- あらゆる場所の資産を効率的に管理、保護、サービス提供が可能
- 各ソースからのすべてのデータを合理化し整理
- ソフトウェアライセンスのトラッキングと再利用
- IT資産（ハードウェア、ソフトウェア、クラウド）の全体的な費用を最適化

検出ソリューションに求められるもの：

- ネットワーク内外の安全なデバイスの検知と管理機能。これには、クラウドサービスに接続しているデバイスが含まれます。
- 主要なハードウェアおよびソフトウェアの資産と、それらの資産に依存するサービスおよびアプリケーションとの間のつながりを自動的に検知し、M.A.Pを実行します。
- 統合エンドポイント管理（UEM）、ネットワークゲートウェイ、クラウドサービス、およびITSMなど、さまざまなシステムから情報を引き出すことができる統合アセットデータベース
- IT部門によって調達資産と、ビジネスサービスにプロアクティブに接続しているものとの間の調整
- データソースへのコネクター（ベンダー、契約データベース、ハードウェア保証など）
- ITSMおよびセキュリティプロセスとの統合により、ITの問題とセキュリティの脆弱性をプロアクティブに修正

ステップ ②

統合エンドポイント管理によるデバイス管理のモダン化

多くの企業がハイブリッド型の労働環境への移行を続ける中、エンドポイントセキュリティと管理は、ITスタッフと従業員の両方にとって、かつてないほど重要なものとなってきています。最新のデバイス管理は、ユーザーとITの生産性を向上させ、IT管理者がデバイスのプロビジョニングとソフトウェアの展開を自動化し、ユーザーの問題を迅速に解決するために必要です。

サポート時間を短縮し、すべてのデバイスを同じ基準で管理するためには、iOS、Android、Windows、macOS、Linux、ChromeOS、特殊用途のフロントワーカー用デバイス、ウェアラブル、IoTデバイスなどまざまなOSに対応し、最新のマネジメントとクライアントベースのマネジメントの両方をサポートする管理機能を備えたUEMソリューションを選択する必要があります。

統合エンドポイント管理ソリューションは、オンプレミスとSaaSの両方で利用可能で、ビジネスの展開要件を満たす必要があります。UEMは、エンドポイントでのビジネスと個人データを分離することにより、従業員のプライバシーを保護できるようにします。UEMはまた、BYODの取り組みを完全にサポートし、ユーザーのプライバシーと企業データを同時に最大限保護します。

統合エンドポイント管理のアプローチによるデバイス管理には以下のようなメリットがあります:

- 全デバイスにおける一貫した管理およびセキュリティ
- オンボーディング、アプリケーションのプロビジョニングおよびデバイス設定を大規模かつ簡単に行うことができ、ITの生産性とユーザーエクスペリエンスの両方を向上
- デバイスポスチャをモニタリングし、常にコンプライアンス遵守を徹底
- 問題を迅速にリモートで修正
- ソフトウェアアップデートおよびOSの展開を自動化
- 包括的なダッシュボードとリアルタイムの情報を提供し、ITの意思決定を向上
- OSやサードパーティ製アプリの脆弱性を検出し、修正
- エンドユーザーでの中断を減らし、シームレスなオンボーディングエクスペリエンスを提供

デバイス管理ソリューションで注目すべき機能は以下の通りです:

- ユーザーに自動デバイス登録を提供するApple Business Manager(ABM)、Google Zero-Touch Enrollment、Windows AutoPilotなどのサービスを活用することで、IT部門のオンボーディングとプロビジョニングプロセスを簡素化
- iOS、Android、macOS、Windows、Linux、ChromeOSデバイスのほか、HoloLens、OculusおよびZebraなどの没入型デバイスや堅牢なデバイスで実行されるあらゆるエンドポイントを検知、管理、保護する機能を搭載
- 複数のデバイス所有モデルをサポートし、企業所有、BYODおよび共有デバイスを管理、設定、保護
- デバイス管理を必要とせず、現場スタッフに権限を与え、それらのデバイスでビジネスアプリケーションの安全な利用が可能
- あらゆるデバイスで、データとアプリへの安全なアクセスが可能
- カスタムレポートと自動化された修正アクションにより、すべての管理対象デバイスの詳細な可視化と制御が可能

ステップ ③

デバイスハイジーンの確立

良好なデバイスハイジーンを保つには、定義されたセキュリティ要件を満たすデバイスのみがビジネスリソースへのアクセスを許可されるようにする、プロアクティブなアプローチを採用する必要があります。これには、オペレーティングシステムやアプリケーションの両方においてソフトウェアの脆弱性があるデバイスに自動的にパッチを適用するか、またはデバイスを隔離できるシステムを導入することが含まれます。良好なデバイスハイジーンを確立するには、信頼性の高いソリューションを利用し、デジタル攻撃の対象領域を縮小する必要があります。

一方で、デバイスハイジーンの状態が悪いと、組織がランサムウェアなどのサイバー攻撃にさらされやすくなります。デバイスハイジーンが不十分な組織の場合、脆弱性をアクティブに追跡し、サイバー攻撃から組織を保護するのは、専用のソリューションよりむしろ、IT部門の責任となります。

モバイルデバイスのハイジーン

従業員の71%は、モバイルデバイスが仕事には欠かせないと感じている一方で、セキュリティ部門のリーダーたちは、異口同音にリモートワーカーは、オフィスワーカーに比べ、よりリスクにさらされていると述べています。それにもかかわらず、セキュリティ専門家の4人に3人は、利便性を求める圧力に屈して、モバイルデバイスのセキュリティを犠牲にしています。[6]

これは大きな問題です。強固なモバイルデバイスハイジーンはデバイスの脆弱性(たとえばジェイルブレイク、ルート検知、脆弱なOSバージョンなど)、ネットワークの脆弱性(中間者攻撃、悪意のあるホットスポット、安全でないWi-Fiなど)、アプリケーションの脆弱性(高セキュリティリスク評価、高プライバシーリスク評価、アプリの不審な挙動、サイドロードされたアプリなど)に対処するために非常に重要です。

モバイルデバイスハイジーンの確立により、以下のメリットを享受できます:

- 自動化された実行可能なリスクに基づくインテリジェンスで、ヒューマンエラーとIT投資の両方のコントロールが可能
- ゼロデイ検出と修復により、何が起こるか推測する必要がありません
- オフになっている、または接続されていないデバイスについても問題の検出と修正が可能
- 攻撃対象領域を減らすことにより、データ、リソースおよび企業ブランドを保護

モバイル脅威対策ソリューションで注目すべき機能:

- フィッシング攻撃やデバイス、ネットワークおよびアプリケーションレベルでの攻撃を含むすべてのモバイル攻撃に対し、保護するソフトウェアの優先順位付け
- AndroidデバイスとiOSデバイスの両方を保護することが重要です。UEMクライアントにバンドルされたデバイス上の機械学習エンジンを備えた1つのアプリケーションを求めます。ユーザーは、2つ以上ではなく、1つのアプリケーションを採用する可能性がはるかに高くなります
- デバイス、ネットワーク、アプリケーションレベルの脅威、さらにフィッシングの脅威に対して、デバイスとクラウドベースの脅威検知機能を使用して多層的な保護をソリューションから探します。デバイス上の保護はインターネット接続を必要とせず、脅威を検出し、修復
- 階層化されたコンプライアンスポリシーを適用し、エンドユーザーや管理者にデバイスのコンプライアンス違反を警告できるようにすることが重要です。コンプライアンス違反には企業リソースへのアクセスブロック、隔離、デバイスの廃棄、UEMが提供するすべてのアプリケーション、コンテンツ設定の削除など、段階的な措置が適用

デスクトップ/ノートパソコンのハイジーン

ランサムウェア攻撃やその他のデータ漏洩が過去のものになるまで―現在までの状況からするとそんな日は来ないかもしれませんが―、組織はそれに対する防御策を講じる必要があります。共通脆弱性識別子（Common Vulnerabilities and Exposures/CVE）を修正するパッチは、ランサムウェアの攻撃に組織が対抗するための最善の方法の1つです。しかし残念ながら、Ivanti[7]の調査によると、ITおよびセキュリティ専門家の71%は、パッチ適用は過度に複雑で時間がかかると感じています。それは、存在する脆弱性の圧倒的な数によるものかもしれません。

米国の脆弱性情報データベース（NVD）には、10万件をはるかに超える脆弱性がリストアップされています。これらの脆弱性のうち、ランサムウェアと関連しているものはごく一部で、流行中/アクティブなエクスプロイトであるものの割合はさらに少ないのですが、どの脆弱性が組織にとって最もリスクが高いのかを特定することはかなり厄介です。Ivantiのレポートによると[8]、2018年から2020年の間に、CVSS v3スコアリングを使用して組織が重要な脆弱性のみにパッチを適用した場合、ランサムウェアに対するそのカバー率は、35%程度にとどまるとされています。自動化されたリスク情報に基づくパッチ適用は、デスクトップ/ラップトップデバイスのハイジーンにとって不可欠なものです。

デスクトップ/ラップトップデバイスのハイジーンの確立には、以下のメリットがあります：

- モバイルデバイスのハイジーンと同様に、自動化された、実行可能なリスクベースのインテリジェンスを使用して、ヒューマンエラーとIT投資の両方をコントロールできます
- 実際のリスクに基づいてCVEを修正するパッチを適用することにより、ランサムウェア攻撃の可能性を低減させます
- 自動化された脅威の優先順位付けを活用して、戦略的にパッチを適用し、リソースの配分を最適化できます
- パッチ適用にとどまらず、対応を自動化することにより、人が介入することなく脅威に対抗できるようになります

デスクトップ/ラップトップデバイスハイジーンのソリューションで注目すべき機能：

- デスクトップ/ラップトップデバイスについは、脆弱性を排除、または少なくとも制限するために、ソフトウェアを定期的にアップデートすることが不可欠です。パッチ適用が圧倒的な数になる可能性があるため、リスクを自動的に評価し、行動可能なインテリジェンスを提供し、最も緊急度の高い脆弱性に優先順位をつけられるソリューションは非常に有用です。
- リスクベースの優先順位付けにより、その環境の中で最もリスクの高い弱点を可視化します。これにより、組織は、最も重要なパッチの必要性に的を絞ることができます。脆弱性を現実の脅威に基づく情報にマッピングするアクティブな脅威コンテキストは、IT/セキュリティチームが最も大きなダメージを与える可能性のある脅威と戦うため、パッチ適用の優先順位を付けるのに役立ちます。

ステップ 4

ユーザーの保護

パスワードを好むのは、パスワードを武器にする脅威アクターだけのようです。加えて、ユーザーにとって負担となるパスワードベースの認証には、デバイス、アプリ、ネットワーク、脅威のコンテキストが欠けています。パスワードを入力している人が従業員なのか、それとも従業員のパスワードを入手した攻撃者なのかを知る術はありません。最も複雑なパスワードでもブルートフォース攻撃やフィッシングなどの攻撃により、比較的容易に漏洩する可能性があります。

パスワードなどの認証情報は、依然として侵害で最も狙われるデータの一つであり、データ漏洩の61%に関与しています[9]。認証情報は他のどの種類のデータよりも速く漏洩します。これは特に、標的として選択された組織へのさらなるアクセス権を獲得するために認証情報を狙うフィッシングにおいて顕著です。

SSOソリューションでは単一障害点が発生し、ハッカーがこれを悪用して企業のほとんどまたはすべてのアプリケーションにアクセスする可能性があります。調査によると[10]、42%が複数のアカウント間でパスワードを再利用しており、17%はすべてのログインに2〜5通りのパスワードを使いまわしています。つまり、職場以外でアカウントに不正アクセスされた人が、同じパスワードを職場で使っていた場合、その組織はリスクにさらされることになります。リモートワークの広がりとともに、組織はパスワードのプロトコルを厳格化すると想定されるかもしれません。しかし、Verizonによる調査[11]によれば、回答者の3分の1以上が、新型コロナウイルス関連の制約に対応し、自分の会社の認証要件は緩和されたと回答しています。

今こそ、ゼロサインオンによるパスワードレス認証を始める時です

ゼロサインオンとは、ゼロパスワードを使用する（シングルサインオンで1つのパスワードを使用するように）認証方法です。

パスワードレス認証でユーザーを保護するメリットは以下の通りです。

- パスワードなし=盗まれたり、フィッシングされる認証情報が存在しません
- パスワードなし=ログインのためのパスワードを覚える必要がなくなり、ユーザーの負担が減ります
- 企業のゼロトラストセキュリティの成熟度を上げることができます
- 従来、パスワードのリセット管理や情報漏洩の対応に費やしていたコストを節約できます

「パスワードを入力している人が従業員なのか、それとも従業員のパスワードを入手した攻撃者なのかを知る術はありません」

認証ソリューションで注目すべき機能は以下の通りです

- 理想的なソリューションは、デバイス、ビジネスアプリ、クラウドサービスにパスワードレスアクセスを提供します
- 効果的なパスワードレスアクセスは、知識要素（パスワードまたはセキュリティの質問など）の代わりに、多要素認証によって認証を確立します。多要素認証には、所有物（モバイルデバイスなど）、固有の物（指紋、FaceIDなどのバイオメトリクス）、コンテキスト（場所、時間帯など）が含まれます
- コンテキストアクセスによるゼロトラストセキュリティのアプローチでは、アクセスを許可する前にユーザー、デバイス、アプリケーション、ネットワークおよび脅威を検証する統合エンドポイント管理ソリューションと統合可能なソリューションを活用します
- IdP/IAM、MTD/XDR/EDR、SOAR、SIEMなど、既存のアイデンティティソリューションとシームレスに統合できるパスワードレス認証ソリューションを探します

ステップ 5
セキュアアクセスの提供

チームがオフィスで働いていた時に機能していたネットワークの境界は、Everywhere Workplaceでは、もはや十分ではありません。従業員がさまざまな（そしてしばしば予測不可能な）場所で働いているため、最新のネットワーク境界は、こうしたダイナミックさを反映し、制限と複雑さを取り除きながら、同時にセキュリティを確保しなければなりません。

今日のネットワークは、Software-Defined Perimeter（SDP）の原則に基づいて構築される必要があります。SPDは、マルウェア対策などの既存のセキュリティ製品では実現できない、統合されたセキュリティアーキテクチャを提供します。これは、データ暗号化、リモート認証、相互トランスポートレイヤーセキュリティ、Security Assertion Markup Languageなど、実績ある標準規格に準拠したコンポーネントを活用するよう設計されています。これら、およびその他の標準化された技術を採用することで、SDPの既存のセキュリティシステムへの統合が可能になります。

SPDはネットワーク構造ですが、メリットを最大化するためには、セキュリティのレイヤーが必要です。そこで、ゼロトラスト—具体的にはゼロトラストネットワークアクセス(ZTNA)—が登場します。GartnerはZTNAを、「アプリケーションまたはアプリケーションのセットの周辺にアイデンティティとコンテキストに基づく論理的なアクセス境界を作成する製品またはサービス」と定義しています。SDPは、ゼロトラストネットワークを実装するために使用することができます。

あらゆる場所でのセキュアアクセスの確立によるメリットは以下の通りです：

- 信頼され、承認されたユーザーのみがリソースにアクセスできることを認証します
- ネットワークの外側の境界を曖昧にし、エンドユーザーにより柔軟な展開とより容易なワークフローを許可します
- ネットワークのサブセクションへの余分で不必要なアクセスの開放を含む、ハードな境界の制限と複雑さを回避します
- セキュリティと可視性を保証しつつ、アクセスを容易にします

ゼロトラストネットワークで注目すべき機能は以下の通りです：

- データ主権：アプリケーションデータはベンダーネットワークを経由せず、インターネットにも公開されません。このダイレクトパスは、パフォーマンスとユーザーエクスペリエンスを最大化します
- 包括的な可視性：ユーザーごと、デバイスごと、およびアプリケーションごとのアクティビティ（SaaSで展開されたリソースを含む）
- クライアントのセキュリティ状態の継続的かつ適応的な評価と、行動や場所などさまざまに変化するコンテキスト要素に基づくポリシーの自動適用

ステップ 6

コンプライアンスとリスクの管理

コンプライアンスを維持し、脅威を軽減するためには、ガバナンス、リスク、コンプライアンス（GRC）マネジメントを、把握することが不可欠です。

信じる信じないにかかわらず、コンプライアンスをスプレッドシートなどの手動で管理している企業が多すぎます。こうした企業はまた、セキュリティ製品の統合や活用についてきちんと理解しないまま、膨大な費用を断片的にセキュリティ製品に費やしてしまいがちです。それは言うなれば、「壁にスパゲッティを投げつける（試行錯誤）」アプローチです。

リスクの影響度に関して、全体像を描くことが非常に重要です。セキュリティポスチャの評価のほとんどは、攻撃の後に行われるもので、攻撃ベクトルに特化したものになります。この後手後手のアプローチは、空席が多すぎるITの役割と相まって、大きな問題になっています。

「信じる信じないにかかわらず、コンプライアンスをスプレッドシートなどの手動で管理している企業が多すぎます」

コンプライアンスとリスクを理解することのメリットは以下の通りです：

- 手動で行っていた作業を、自動化されたコンプライアンスプロセスに置き換えます
- よりスムーズな監査のためのステージを設定します
- プロアクティブにリスクを軽減します
- 予算を実際のリスクと整合させ、推測を排除します
- より戦略的で信頼性の高いコンプライアンスのフレームワークを構築します
- 進化し続ける要件変更に開発者なしで対応できます
- 人的リソースを解放し、より戦略的な仕事に集中できるようにします

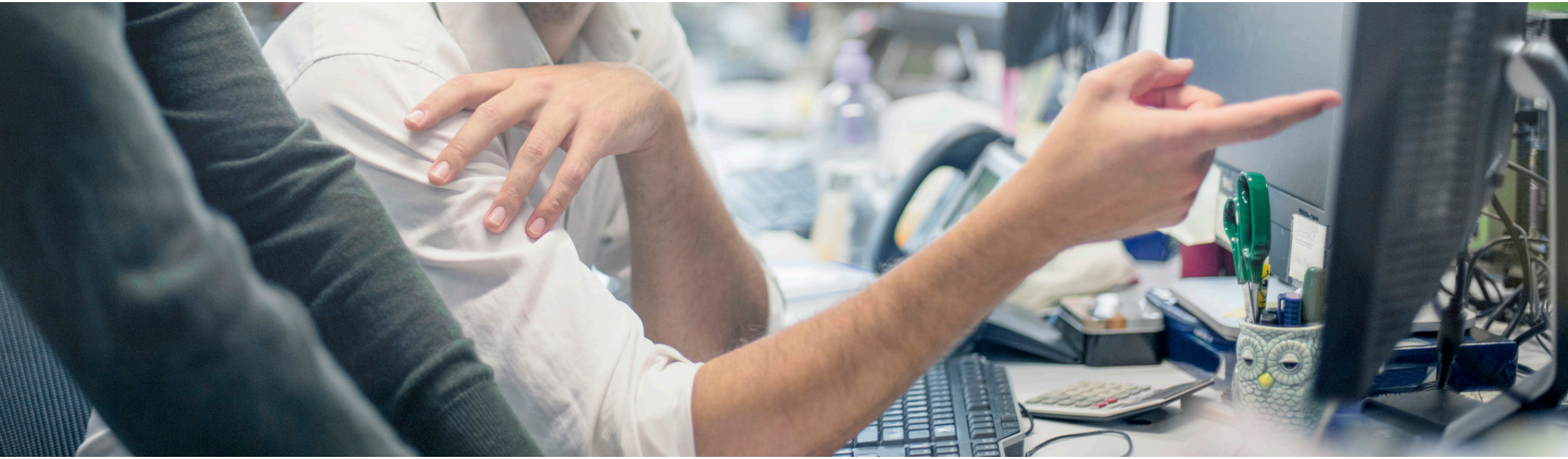
コンプライアンスソリューションで注目すべき機能は以下の通りです：

- 強力なソリューションは、セキュリティとコンプライアンスコントロールを備えたM.A.P.参照への迅速で簡単な規制文書インポートにより、コンプライアンスの負担を軽減します。
- プロアクティブなリスクマネジメントの能力とは、適切なタイミングで適切な場所に集中的に注意を払うことを意味します
- 手動タスクを自動化され繰り返し行われるガバナンス活動に置き換え、コンプライアンスが円滑に機能するようにします
- プロセス成熟度管理とは、重要なセキュリティプロセスとコントロールの成熟度を評価し、優先度とリスクに基づいて最適化できることを意味します
- 効率的で正確な結果を得るためには、リスクアセスメントの作業全体を自動化するガイダンスを備えたソリューションを探します

M.A.Pでサイバーセキュリティジャーニー

これらのステップはそれぞれ、サイバーセキュリティへの取り組みを管理、自動化、優先順位付けするための不可欠な要素なのです。気後れしてしまう？ どこから手をつければいいのかわからない？ セキュリティへの取り組みをサポートしてくれるパートナーを得て、ソリューションを活用することが重要です。適切なソリューションは、包括的かつ統合的で、ITスタッフの負担を軽減するものです。最適なソリューションはまた、従業員が働く場所と時間、手段を問わず完全性を維持する直感的で生産性の高いユーザーエクスペリエンスを保ちます。

どこでも働ける。どこでも安全。



Ivantiについて

Ivantiは「Everywhere Workplace（場所にとらわれない働き方）」を実現します。場所にとらわれない働き方により、従業員は多種多様なデバイスでさまざまなネットワークからITアプリケーションやデータにアクセスし、高い生産性を保つことができます。Ivanti Neurons自動化プラットフォームは、業界をリードする統合エンドポイント管理、ゼロトラストセキュリティと、エンタープライズサービス管理のソリューションをつなぎ、デバイスの自己修復および自己保護、またエンドユーザーのセルフサービスを可能にする統合ITプラットフォームを提供します。Fortune 100の96社を含む40,000社以上の顧客が、クラウドからエッジまでIT資産の管理、検出、保護、サービスのためにIvantiを選択し、従業員があらゆる場所にいても作業できる優れたユーザー体験を提供しています。詳細については、www.ivanti.co.jpをご参照ください。

ivanti

ivanti.co.jp
+81 (0)3-6432-4180
contact@ivanti.co.jp

1. Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time
2. Ivanti: Patch Management Challenges. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges
3. Statista: Global average cost of a data breach 2021.
4. Statista: Average https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/ length of downtime after a ransomware attack 2021.
5. The biggest data breach fines, penalties, and settlements so far | CSO Online
6. 2021 Data Breach Investigations Report | Verizon
7. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges
8. https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensecsw?_ga=2.114312003.538830105.1638796042-898995573.1638285247
9. 2021 Data Breach Investigations Report | Verizon
10. Best Password Managers 2021 | The Strategist (nymag.com)
11. People and behaviors | Verizon