

A woman with dark hair and glasses is looking at a tablet. The background is a blurred digital interface with lines of code and a glowing blue circle.

ホワイトペーパー

サイバーリスクを 低減するための 11 のセキュリティ対策

防御力を強化し、サイバーレジリエンスを高め、
組織のリスクを低減する実践的手法

エグゼクティブサマリー

あらゆる組織の経営幹部は、セキュリティ対策の最適化が単にデータやシステムの保護にとどまらず、企業の評判や顧客の信頼、そして事業継続性に関わるリスクを総合的に低減する取り組みであることを理解しておく必要があります。ランサムウェアやビジネスメール詐欺 (BEC) などのサイバー攻撃は、業務および財務に関する重大な影響を引き起こす恐れがあります。Cyber Defense Magazine によれば、2025 年におけるサイバー犯罪による全世界の被害額は 1.2 兆ドルに達すると予測¹されています。たとえ攻撃を封じ込めることができたとしても、システムの再起動や再構築のために一時的にオフラインにしなければならない場合、大規模な業務中断が発生する恐れがあります。こうした危機を乗り越えられる組織もありますが、予期せぬ深刻な事態に直面し、存続の危機に立たされる組織も存在します。

サイバー防御力を最大化するためのセキュリティ対策の役割

セキュリティ対策は、リスクを効果的に軽減し、組織をあらゆる脅威から守るために、セキュリティチームが活用できる手段です。さまざまな種類のセキュリティ対策がありますが、その目的は共通しています。インシデントやセキュリティ侵害の発生を防止し、万が一発生した場合でも被害を最小限に抑えることです。予防に特化したセキュリティ対策や、脅威の予防、検知、対応といった各フェーズで多様なレベルの軽減効果を発揮する対策もあります。多層防御を確立するためには、すべての領域で強力なセキュリティ対策を適切に組み合わせることが不可欠です。

また、強固なセキュリティ対策は、サイバー保険を利用してリスクを管理する場合にも非常に重要となります。保険会社は、保険料や補償限度額を設定する際に、組織が導入しているセキュリティ対策の内容を重視します。

保険会社が保証の対象とする範囲は以下の通りです。

自身が支払いを受ける保険 (ファーストパーティ保険) には、サイバー攻撃やセキュリティ侵害によって自組織が直接被る損害が含まれます。これには、業務中断、データ復旧費用、データ窃取による被害、ランサムウェアによる支払いなどが該当します。

賠償責任保険 (サードパーティ保険) は、顧客、取引先、規制当局など外部関係者に対して負う責任をカバーします。これには、訴訟、損害賠償請求、政府機関や業界団体による制裁金・罰金などが含まれます。

1.2 兆米ドル

2025 年には、サイバー犯罪による世界全体の被害額が 1.2 兆米ドルに上ると予測されています。¹

重要である理由

優れたセキュリティ対策は、業務の保護にとどまらず、保険料の軽減や保険金請求の審査・支払い結果の改善にも寄与します。

11 のセキュリティ対策による サイバーリスクの低減

強固なセキュリティ対策に投資すれば、サイバーリスクの低減につながるだけでなく、サイバー保険への加入条件を満たしやすくなり、保険契約の条件も向上します。脅威の予防や影響の軽減、防御力の強化に役立つ、11 の基本的なセキュリティ対策を以下に紹介します。

これらの対策を適切に導入することで、強固なサイバーセキュリティポスチャを構築して、現在および将来の脅威に対応することが可能になります。

1

アイデンティティとアクセス管理

2

エンドポイントセキュリティ

3

多要素認証

4

脆弱性管理

5

メールセキュリティ

6

特権セッション管理 (PSM)

7

資産管理

8

セグメンテーションとアーキテクチャ

9

XDR (Extended Detection and Response)

10

バックアップと事業継続性

11

ネットワークセキュリティとトラフィック管理

1. アイデンティティとアクセス管理

アイデンティティおよびアクセス管理 (IAM) は、認可されたユーザーのみがシステムやデータへアクセスできるようにする仕組みです。特権アクセス管理 (PAM) は、IAM をさらに強化するもので、ユーザーが業務上必要な範囲の資産にのみアクセスできるように制限します。単純な仕組みのように思われるかもしれませんが、大規模な組織になると、アクセス権限の管理が非常に複雑で煩雑になりがちです。すべての企業は、入退社時のアカウント管理を厳格に行い、強固なパスワードポリシーを徹底するとともに、アクセス権限を定期的に監査する必要があります。

組織の大小を問わず、使われなくなったアイデンティティを確実に削除する明確なルールの策定は不可欠です。放置されたアカウントは、攻撃者に悪用され、権限の昇格やネットワーク内のラテラルムーブメントにつながるリスクがあります。

2. エンドポイントセキュリティ

組織の環境に接続しているすべてのデバイスは、攻撃の潜在的な標的となります。ハイブリッドワークの普及により、アタックスurfaceが広がり、セキュリティリスクが増大しているため、エンドポイント保護の重要性はこれまで以上に高まっています。多くの攻撃は、手間をかけずに入手・使用できるマルウェアなどの「コモディティ型脅威」から始まります。しかし、高性能なエンドポイント保護ツールを導入することで、こうした脅威を迅速に検知し、無力化することが可能です。しかし、管理されていない、または放置されたエンドポイントはセキュリティ上の弱点となることがあり、**リモートランサムウェア攻撃**でも一般的に悪用される侵入経路となっています。すべてのデバイスを適切に保護する必要があります。

3. 多要素認証

多要素認証 (MFA) は、ユーザーのアイデンティティを複数の認証要素で確認する仕組みです。たとえば、パスワードなどの「知っているもの」、トークンなどの「持っているもの」、指紋などの「本人固有の要素」を組み合わせで認証を行います。漏洩した認証情報が依然として攻撃の主な原因となっており、MFA は現代の組織にとって欠かすことができないセキュリティ対策です。攻撃者による MFA 回避の手法に対する耐性を高めるために、位置情報や数字照合といった高度な MFA 手法の導入も検討すべきです。ただし、ユーザーエクスペリエンスやプライバシーとのバランスも考慮する必要があります。

重要ポイント

休眠アカウントや使用されていない特権は、攻撃者にとって格好の侵入経路となり、容易に悪用されるリスクがあります。一度侵入されると、権限を昇格させ、攻撃範囲をひそかに広げられます。

最も一般的な侵入経路は、往々にして最も見落とされやすいものです。古いエンドポイントをバックドアにさせないようにしましょう。

従業員に不要な手間をかけることなく、リスクに応じて認証を強化できる適応型多要素認証を導入してください。

4. 脆弱性管理

脆弱性管理とは、組織全体の環境に存在するセキュリティの弱点を継続的に特定および評価し、修正するプロセスです。これらのプロセスには、ソフトウェアやシステムへのパッチ適用、設定の更新、新たに公開された脆弱性の監視といった一般的な対策が含まれます。強力な脅威インテリジェンスは、新たなリスクから組織を保護するために重要な役割を果たします。

ネットワーク上のすべての資産の所在を正確に把握することは、包括的なスキャンを実施するうえで非常に重要です。このような可視性を確保することで、リスクに合わせたアプローチが可能となり、外部への公開状況、悪用される可能性、ビジネスへの影響を踏まえて、優先的に対応すべき脆弱性を判断して修正できるようになります。

5. メールセキュリティ

メールは古くからあるテクノロジーであるにもかかわらず、いまだに攻撃者にとって主要な侵入経路の 1 つになっています。特にフィッシングは最も一般的な攻撃手法であり、ランサムウェア攻撃や認証情報の窃取を目的としています。また、ビジネスメール詐欺 (BEC) は、サイバー保険の請求件数が最も多い事例の一つです。強力なメールセキュリティは、悪意あるコンテンツを受信箱に届く前にブロックできるため、欠かせない第一防衛線となります。近年、生成 AI の進化によりフィッシングメールの文法やメッセージの巧妙さが増しています。ユーザーに届く前にこれらのメールベースの攻撃を阻止するために、保護機能のさらなる進化が求められています。

しかし、メールの配信時点で保護が完了するわけではありません。受信後に、一見安全に見える URL や添付ファイルが悪意あるものに変わるケースもあります。高度なメールセキュリティソリューションには、配信後の脅威検知と対応機能が備わっており、メールコンテンツを自動的に再スキャンし、悪意のあるメッセージを回収して削除し、リスクプロファイルが変わった場合にはリンクを無効化できます。これらの対策により、脅威が初期の防御をすり抜けた場合でも迅速に対応でき、悪意あるメールがユーザーの受信箱に留まる時間を最小限に抑えることが可能になります。

重要ポイント

コアシステムだけでなく、サードパーティアプリやクラウドサービスの脆弱性も確認してください。

一回のクリックが、大きな被害をもたらします。フィッシング対策の最善策は、ユーザーがメールを受け取った後であっても、悪意あるリンクや添付ファイルといった「罠」を表示させないことです。

6. 特権セッション管理 (PSM)

攻撃者にとって、管理者アカウントは、最も強力な権限を有する標的です。その権限で、アイデンティティ管理システム、構成管理、セキュリティツールなどにアクセスできる場合、被害の範囲は非常に大きくなります。攻撃者が管理者レベルのアクセス権限を取得すれば、防御を無効化し、ランサムウェアを大規模に展開することも可能になります。

このようなリスクを軽減するためには、組織は特権アクセスに階層型モデルを導入し、それらのアカウントの使用状況を常に監視することが重要です。特権セッション管理 (PSM) は、管理者セッションのログ記録や録画を行い、場合によってはリアルタイムで操作を制御することで、セッションを監視します。これにより、攻撃が疑われる行動を検知し、特権の悪用を防止し、コンプライアンス要件を遵守できます。

7. 資産管理

把握していない資産を守ることはできません。組織は、デバイスなどの物理的な資産とデータ資産の両方について最新のインベントリを維持する必要があります。機密データの保管場所を正確に把握していれば、インシデント発生時に迅速かつ確かな調査が行え、正確な報告や迅速な封じ込めが可能になります。適切な資産管理は、徹底的な調査を行うために役立ち、役割や責任を明確にして対応を円滑にし、被害による影響を軽減します。

8. セグメンテーションとアーキテクチャ

サイバー攻撃者が環境へ一度侵入すると、次にラテラルムーブメントを行い、権限昇格、機密システムへのアクセス、ランサムウェアの展開を目指します。強力なネットワークセグメンテーションとアーキテクチャ設計によって、これらのラテラルムーブメントを非常に困難にすることができます。セグメンテーションによって攻撃者は目的を容易に達成できなくなり、多くの痕跡を残すようになるため、攻撃チェーンの初期段階で検知できる可能性が高まります。

システムアーキテクチャは、機密性、完全性、可用性、レジリエンスの原則に基づいて構築すべきです。具体的には、ゼロトラストモデルを採用し、システム間およびユーザーとシステム間のアクセスを制限し、すべてのトランザクションをユーザーのアイデンティティ、デバイス、権限に基づいて検証する必要があります。

重要ポイント

先週の火曜日に誰が管理者権限にアクセスし、どのような操作を実行したかを正確に把握できていますか？できていなければ、監視体制を強化すべきです。

一方で、ログや記録は必要な期間だけ保持し、不要な情報を溜め込まないことも重要です。過剰に記録を保持すると、サイバー保険の保険料が上がったり、万一の情報漏えい時に評判被害が拡大したりするリスクがあります。

ネットワークセグメンテーションを活用し、重要なシステムは通常のアクセスポイントから隔離してください。

9.XDR (Extended Detection and Response)

多くの異なるツールを煩雑に使い分けしていると、アラートの分散やトリアージの遅延、さらには脅威の見逃しを招くリスクがあります。XDR (Extended Detection and Response) は、エンドポイント、ファイアウォール、ネットワーク、メール、アイデンティティ、バックアップ、クラウドセキュリティシステムなど、複数の領域にわたる活動を統合的に可視化して、このようなリスクを軽減します。これにより、アラートのノイズを大幅に削減し、より迅速かつ確かな意思決定を支援します。これにより、アナリストが複数の分断されたツールを手動で切り替えながら脅威の調査や対応を行う煩雑な作業が解消されます。

高度な XDR システムでは、高度な分析、AI による優先度判定、詳細なデータ検索、自動的な XDR アラート相関やエスカレーションなども活用されます。これらの機能を組み合わせることで、検知精度が向上し、調査が加速します。結果として、セキュリティチームは複数の煩雑なツールに振り回されることなく、最もリスクの高い脅威に集中して対応できるようになります。

10. バックアップと事業継続性

サイバーインシデントによって業務が停止したりシステムが破損したりした場合、迅速に復旧できるか、あるいは長期にわたるダウンタイムを余儀なくされるかを決定付ける、適切に管理されたバックアップと堅牢な事業継続計画です。すべてのバックアップが同じように効果を発揮するとは限りません。検証と定期的なテストが行われ、システムやデータを完全かつ確実に復元できることが、効果的なバックアップの条件です。

よくある失敗は、バックアップの設定です。バックアップがシステムを部分的にしか復元できなかったり、重要なデータが含まれていなかったりする問題に気づくのが遅れると、本来は短期間で済むはずの業務中断が、数週間に及ぶ混乱へと拡大してしまうケースもあります。

同様に重要なのは、バックアップデータを通常とは異なる経路の認証方法で保護することです。そうしなければ、攻撃者が広範なアクセス権限を入手した場合、攻撃の一環としてバックアップデータが無効化または削除される恐れがあります。

重要ポイント

XDR は分断されたアラートを統合し、迅速な調査と効果的な対応を可能にします。

可能な限りバックアップは分割し、オフラインで保管してください。複数の方法で復旧できる体制を整えてください。

11. ネットワークセキュリティとトラフィック管理

ネットワークは単なる接続レイヤーではなく、企業環境全体にわたるトラフィックを検査、フィルタリング、管理するための戦略的な制御ポイントです。ファイアウォール、侵入防止システム (IPS)、DNS フィルタリング、セキュア Web ゲートウェイは、多層防御の中核をなす重要な機能です。

しかし、すべてのファイアウォールが同じわけではありません。ファイアウォールが旧式であったり、設定ミスがあったり、十分に活用されていないと、悪用されるギャップを生む可能性があります。防御策を定期的に評価し、パッチを適用して最新の状態に維持するとともに、現在の脅威環境に合わせて調整することが、レジリエンスを維持するために不可欠です。

ゼロトラストネットワークアクセス (ZTNA) のような最新の対策は、詳細でコンテキストアウェアなアクセス制御を提供します。このような最新の対策に従来型の防御策を組み合わせることで、アタックサーフェスの縮小、ラテラルムーブメントの防止、ハイブリッドおよびクラウド環境における情報流出の阻止が可能となります。

全体像を把握して、 包括的なアプローチを実行する

単に適切なツールを導入するだけでは、サイバーセキュリティを向上することはできません。人、プロセス、テクノロジーを統合した戦略を推進することが重要です。本書で紹介した 11 のセキュリティ対策を、慎重に導入して継続的に実施することで、組織のサイバーリスクを大幅に低減できます。

レジリエンスを長期的に強化するためには、再現性と適応性を備え、責任の所在が明確に定められたサイバーセキュリティプログラムの構築から始めることが不可欠です。テクノロジーは強力な武器となりますが、それを効果的に活用するには熟達したチームと体系化されたプロセスが不可欠です。

脅威は進化し、テクノロジーも変化します。また、企業のかたちも変わり続けます。脅威の影響を未然に防ぐためには、全体的な視点で捉え、環境の変化に応じて継続的に適応していくことが不可欠です。セキュリティ対策は単なる形式的なチェックリストではなく、ビジネスの中核を支える文化として根付かせることが求められます。

重要ポイント

ネットワークテレメトリを検知システムに統合し、可視性を高め、調査を迅速化するとともに、特にラテラルムーブメントやコマンド & コントロールサーバーとの通信などの異常なアクティビティを検知してください。

¹ Cyber Defense Magazine : The True Cost of Cybercrime: Why Global Damages Could Reach \$1.2-\$1.5 Trillion by End of Year 2025 (サイバー犯罪のコスト：2025 年末までに全世界の被害額は 1.2 ～ 1.5 兆ドルに達すると予測)

² ソフォスの年次脅威レポート 2025 年版

³ Dark Reading, 「Email-Based Attacks Top Cyber-Insurance Claims (サイバー保険の申請の最多の要因はメールベースの攻撃)」、2025 年 5 月 8 日

サイバーセキュリティプログラムの 評価を始めましょう

ソフォスの専門家にご相談ください。

ソフォス株式会社

Email: sales@sophos.co.jp