Check Point
SOFTWARE TECHNOLOGIES LTD

セキュリティ管理 再考の勧め

セキュリティ担当者のためのガイド

ONE
STEP
AHEAD

目　次

01
はじめに

私たちは今、歴史的に見て興味深い時代に生きています。技術の進化や各種デバイスのネットワーク化、経済のグローバル化とデジタル化は、私たちの生活にさまざまなメリットをもたらしました。人々の働き方や金融取引の形態、コミュニケーションの取り方、生活様式、さらに安全を確保する方法も一変しています。さらに、サイバー・セキュリティのあり方も急激に変化しています。サイバー空間の進化は、イノベーションを促進すると同時に、未知の危険な存在を数多く生み出すことになりました。問題は、セキュリティ業界がこの危機に十分対処できているかという点です。ご存じのように、攻撃経路は増加と複雑化の一途を辿っており、脅威への対応やセキュリティ対策の管理は、年々困難になっています。

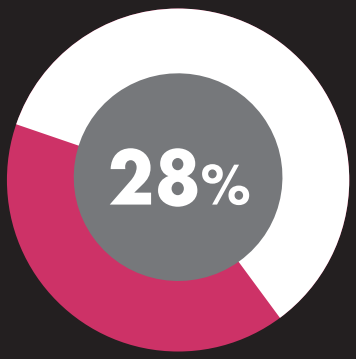
セキュリティ脅威による被害を最小限に抑えるためには、セキュリティ対策をリアルタイムで監視、管理して、発生した問題に素早く対処する必要があります。このような課題に対する解決策が、組織のデータやネットワーク、デバイスを保護するとともに、セキュリティ・リスクをリアルタイムで可視化する高度なシステムで構成された、強力なセキュリティ管理環境です。

その環境には、重要資産を保護するためのポリシーと手順の策定、文書化、適切な実装も含まれます。

従来のセキュリティ対策は、単機能型のソリューションで構成され、被害が発生してから新たなポリシーやルールを策定する事後的な対策が一般的でした。しかし、このような対策には、傷口に絆創膏を貼る程度の効果しか期待できません。従来型の対策が機能しない主な理由は、統合されたテクノロジーに基づく統一されたセキュリティ・プログラムが存在していないからです。

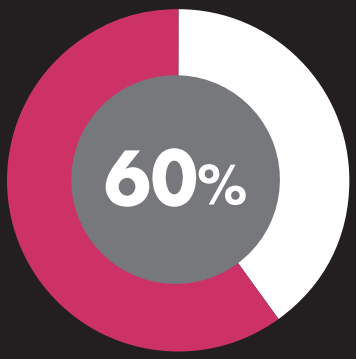
本書では、現在のセキュリティ対策を**再考**し、組織のセキュリティを強化する方法について解説します。テクノロジー、人、ポリシー、運用、管理というセキュリティを構成するすべての要素に光を当て、新たな観点から検討していきます。

セキュリティの強度は、担当者の管理性に依存する。



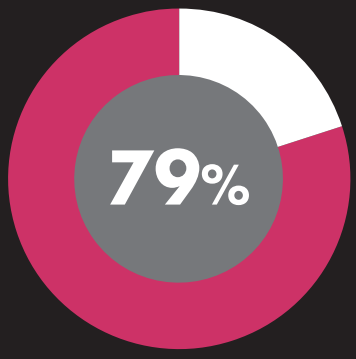
28% の組織は、管理対象や作業の重複が課題となっており、複雑なプロセスが問題発生の原因になっていると感じている。

– ESG



2017 年までには、プライベート・クラウド環境の 60% で情報セキュリティ対策のプロビジョニングが自動化される見込み。

– Gartner



組織に属する情報セキュリティ担当者の 79% は、ネットワーク・セキュリティの維持が過去 2 年間でさらに難しくなったと感じている。

– ESG

「目の前の現実と戦わなければ、変化は生まれない。何かを変えようとするなら、既存のモデルを時代遅れにする新しいモデルを作り上げる必要がある」

– リチャード・バックミンスター・フラー

02

現実の問題解決に着手する

単機能型のセキュリティ製品を寄せ集めて後は運を天に任せるというアプローチでは、昨今のセキュリティ脅威に対抗できません。各システムを緊密に統合し、ネットワークのセキュリティ・リスクを可視化できる本物のソリューションが必要です。それは、組織に戦略的・戦術的なメリットをもたらす強力なセキュリティ・プラットフォームで、ビジネスを妨げることなく潜在的な脅威に対処するセキュリティ管理環境が求められています。

サイロ化された管理がもたらすリスク

一部のセキュリティ・ベンダーは、設計や構成が複雑で、運用管理が困難な複数の管理プラットフォームを提供しています。多くの場合、各管理プラットフォームの運用には、ポリシーや設定方法の異なる複数のコンソールが必要となります。しかし、セキュリティ管理者が同じような作業をプラットフォームごとに強いられ、ビジネスの保護に必要な工程が増えるために隙が生まれやすくなり、組織のセキュリティ・リスクが高まるというデメリットが避けられません。

また多くの組織では、セキュリティ・ソリューションが変更管理プロセスに不十分のまま組み込まれており、予期しないシステム停止やプロセスの複雑化などの問題を引き起こしています。セキュリティやプライバシーを専門とする調査会社 Ponemon Institute の『2015 Global Cost of Data Breach Study』によると、組織がサイバー攻撃を発見するまでには平均 256 日、人的ミスに起因するデータ侵害を発見するまでには平均 158 日を要しています。このように問題の発見に至るまで長い時間が経過してしまう直接的な原因は、統合の不十分さが足かせとなっているためです。統合できるように設計されていない複数の管理プラットフォームを運用している場合、データ侵害の発見はさらに困難となります。

セキュリティの複雑さに対処する

ネットワーク・セキュリティの基盤は、急激な進化を遂げています。ネットワーク・セキュリティ対策は、つい最近まで独立して機能する少数の基本的なコンポーネントだけで構成されていました。この当時、ネットワーク・アーキテクトは、デバイスが単一障害点やパフォーマンス低下の原因となることを防ぐため、セキュリティが必要以上に厳格化しないよう注意する必要がありました。

一方、今日のネットワーク・セキュリティは、より動的なコンポーネントで構成されるように変化しています。多種多様なトラフィック、各種デバイスのログ、パートナーやベンダーのエコシステム、セグメント化されたネットワーク、複数の支社・支店環境、集約されたセキュリティ・アラート、コンプライアンスなど、現代のセキュリティには幅広い要素が関係しています。しかもこれらは、ただ幅広いというだけでなく、複雑に絡み合っています。

動的に変化するクラウド環境

調査会社 Gartner では、（わずか 1 年後の）2017 年までに、プライベート・クラウド環境の 60% で情報セキュリティ対策のプロビジョニングが自動化されると予測しています。クラウド環境では、ビジネスを拡大するうえで物理的な制約をほぼ受けません。市場や顧客の要請に即応して、動的にリソースを拡張できます。

また、ビジネスの成長に合わせてソフトウェアやサービスの規模を柔軟に拡大できます。その主な特徴の 1 つは、高いレベルの即応性を実現できる点です。例えば、需要や処理負荷の変動に合わせて、リソース量は自動的に調整されます。人間が介在することなく、サーバを自動的にプロビジョニング、設定、終了できるため、数分～数時間という短い単位でサーバを稼働させることも可能です。また、インターネット回線と必要な認証情報さえあれば、どこからでも、プラットフォームやアプリケーションを含むインフラストラクチャ全体を管理できる点も大きなメリットとなります。

このように、ビジネスにさまざまなメリットをもたらすクラウドですが、その利用には多大なリスクが存在する点も忘れてはなりません。従来の境界セキュリティ対策や人手を必要とするセキュリティ対策では、動的に変化するクラウドを保護し続けることは困難です。また、ネットワークを適切にセグメント化しなければ、自由にネットワーク内を動き回る攻撃者に、各システムへの侵入を許してしまいます。実際、大きく報道されたセキュリティ侵害事件の中にも、不十分なセグメント化が被害の拡大を招いた事例があります。

さらに、ほとんどの組織がそうであるように、物理環境と仮想環境が混在している場合には、その両方のセキュリティを集中管理できなければなりません。そのためにはセキュリティを自動化し、クラウド・インフラストラクチャに組み込む必要があります。

不足する人材

経験豊富なセキュリティ担当者の人材不足な状態が続いており、リソースを追加投入する解決策は現実的ではありません。仮に人材を確保できたとしても、手作業を中心とする労働集約型のセキュリティ・プロセスがそのままでは、動的なシステムの設定ミスが増えるだけで終わる可能性があります。また、目まぐるしく変化する動的な環境では、どうしてもセキュリティの死角が生まれます。

このような現状に対処するには、まず、セキュリティ関連のタスクとワークフローを分析し、セキュリティ・イベントへの迅速な対処と攻撃の防御に最も大きな影響を与えるタスクを把握します。一般的によく挙がるタスクは、セキュリティ・アーキテクチャの設計やセキュリティ脅威の影響分析、セキュリティ侵害の調査などです。セキュリティ・チームはこの時点で、特定したタスクに優先的に取り組む必要があります。意識的に優先しなければ、結局はパッチ管理や資産管理、トラブルシューティング、アクセス権管理などの受け身的なルーチン・タスクに忙殺される結果に陥ってしまうからです。ルーチン・タスクの実施には、多大な時間や労力が投じられている可能性があり、ワークフローのボトルネックやプロセスの効率を分析すると、自動化または委任すべきタスクを特定できる場合があります。

不十分な監視体制

調査会社 ESG のレポートによると、セキュリティ担当者が緊急事態への対応に追われ、セキュリティ関連のトレーニングや計画・戦略の策定にほとんど時間を割けていないとする組織の割合は、調査対象全体の約 40% に上っています。実際に多くの組織で発生しているこの問題は、強力なセキュリティ管理プラットフォームを導入すべき大きな理由となります。

膨大なデータの中から、セキュリティ侵害につながるおそれのあるイベント・データを見つけ出すカギとなるのは、監視対象とする活動やシステム、そのタイミングの的確な判断です。各種システムで発生するセキュリティ・イベントの監視や情報収集は、対処すべき課題の一部に過ぎません。一見無関係と思われるイベント同士の関連性を発見できる点も重要となります。そのためには、セキュリティの状態を監視して不自然なトラフィック・パターンを探し出す相関分析ルールを作成する必要があります。

問題の解決は、早ければ早いほど、抜本的であればあるほど理想的です。ネットワーク全体のセキュリティ状況を詳細に把握できるグラフィカルなダッシュボードがセキュリティ管理プラットフォームに用意されていれば、各実施ポイントの状態を監視して、潜在的な脅威に備えることができます。また、柔軟なカスタマイズに対応したダッシュボードでは、組織にとって重要な情報だけを集中的に監視できます。セキュリティの全体像を確認しながら、数回のクリックでセキュリティ・インシデントやログ情報を素早くドリルダウンできる機能も欠かせません。さらに、関係者のニーズに合わせて異なる内容のレポートを作成し、各種 Web ブラウザで参照できる必要があります。

「多くの組織では、せっかくセキュリティ・ツールを導入しても、生成されるイベント・ログを効果的に監視、管理できていません。セキュリティの特効薬と見なされているセキュリティ情報 / セキュリティ・イベント管理（SIEM）ソリューションも、多くの組織では適切に管理、活用されていないのが実情です *」

** Avoid These "Dirty Dozen" Network Security Worst Practices. Published: January 8, 2015, Gartner, Inc.*

03

強固なセキュリティを実現するカギ

サイバー・セキュリティ対策の責任者が忘れてはならないのは、結果だけにとらわれず、大局的な観点でセキュリティ強化に取り組むという姿勢です。サイバー攻撃のリスクと潜在的な被害を軽減するためには、組織のリソースとセキュリティ戦略の足並みをそろえる必要があります。例えば、セキュリティに無頓着な人々にも、セキュリティ・ポリシーの意義や重要資産を保護する具体的な方法を理解してもらえるような文化を培っておけばセキュリティの強化につながります。

データ侵害事件の増加を受け、多くの組織は、ハッカーやサイバー犯罪者の一歩先を行くプロアクティブなソリューションの導入を模索し始めています。巧妙化の一途を辿るサイバー攻撃者とのスキル・ギャップを埋め、彼らと対等以上に戦うにはどうすればよいのか。以降では、セキュリティ管理の統合で予防的な防御を実現し、セキュリティ侵害の発生リスクを低減する方法を解説します。

統合による課題の克服

本書が提案する「セキュリティ管理の再考」とは、業界の常識にとらわれずに、課題を多角的に見直す取り組みを意味します。セキュリティの複雑さは、統合を実施する、つまりすべてのセキュリティ機能を 1 つの傘の下に集約すれば解消に至ります。セキュリティを 1 つのプラットフォームに統合すると、よりきめ細かな管理が可能になると同時に、セキュリティ状況の明確な把握とセキュリティ脅威への迅速かつ包括的な対処が実現します。

つまり、統合こそセキュリティ強化のカギと言っても過言ではありません。組織全体で統一されたセキュリティ管理プラットフォームを導入し、セキュリティのあらゆる側面を統合すると、組織としての効率が向上し、全社規模の強固な防御を実現できるようになります。

ポリシー管理の統合

通常、新たなレイヤやポリシーを追加する場合には、事前に既存のポリシーを見直し、変更や削除の必要性を確認しなければなりません。しかし、ポリシーが統合されていれば、このような手間は不要となります。

ポリシーの設定ミスは、深刻な結果を引き起こすおそれがあります。ミスによって各ネットワーク・セグメントの保護や監視が手薄になり、組織全体がサイバー攻撃にさらされる危険性が生じるからです。高い運用効率を備えるセキュリティ管理プラットフォームは、このような課題を克服する強固なセキュリティ・アーキテクチャを実現するための切り札となります。

従来のポリシー管理

従来のセキュリティ製品は、ネットワークや重要資産を保護する際に、多数のポリシーを強引に束ねるという失敗を犯していました。

セキュリティの複雑化という問題について、責任の一端は私たちベンダーにもあります。製品が統合されていない点や、それに伴うポリシーの設定ミスといった人的エラーの増加によって、セキュリティの死角が大きくなっていったのです。問題の所在を的確に把握するためには、デバイスやベンダーの種類を問わず、すべてのセキュリティ・ポリシーを単一の統合コンソールから把握できることが何よりも重要となります。

ポリシーが統合されていると、アクセス制御と脅威対策の管理が効率化されます。ただし、複雑な環境下では、ポリシーの容易な分割が求められます。ポリシーを分割すれば、保護対象とするユーザ、ホスト、アプリケーションの追加権限をヘルプ・デスク・チームに付与するなど、セキュリティ管理の権限を別のチームに安全に委譲できるからです。さらに一歩踏み込んで、セキュリティ管理プラットフォームとチケット発行システムを直接統合すると、このプロセスを一層効率化できます。

このように、セキュリティ担当でないチームや外部のパートナーにルーチン・タスクを委譲すると、セキュリティ・チームは、高度な専門知識が必要となる作業に専念できるようになります。これは、セキュリティをビジネスの阻害要因から推進要因へと転換することにつながります。

脅威管理の統合

オックスフォード英語辞典によれば、「Visibility」（可視性）とは、「物事が見える状態、見られる状態」を指します。この定義をサイバー・セキュリティ、特にセキュリティ管理に当てはめると、「セキュリティの可視性」は、「セキュリティ状況を細部まで見通し、必要な情報をすぐに参照、管理できる能力」と定義できるでしょう。

セキュリティ管理で重要なポイントは、包括的な可視化の実現、つまり組織のセキュリティ状況の全体像を把握できるようにすることです。高度な脅威管理ソリューションには高機能でグラフィカルなダッシュボードが統合されており、デバイスの設定状況や、進行中の攻撃、攻撃の兆候、ポリシー違反などのさまざまなセキュリティ・リスクを把握できます。

存在が把握されていないデバイスは、監視、保護の対象になり得ません。可視化は、インシデントの検出や対応に不可欠な能力であり、可視化が不十分な場合、さまざまなセキュリティ管理の課題に直面することになります。ネットワーク・アクティビティを記録してインシデントの検出に役立てる（38%）、不正な活動のネットワーク・フローを追跡する（35%）、ネットワーク・デバイスやセキュリティ・デバイスのログを収集、分析する（29%）、平時におけるネットワーク・アクティビティの基準値を策定する（27%）など、いずれもセキュリティ状況の全体像が不透明な場合は容易に達成できません。

グラフィカルな統合ダッシュボードが必要な理由は、このような課題に対処するためです。統合ダッシュボードでは、ネットワークの境界にとどまらず、組織全体のセキュリティ状況を包括的に可視化して、イベント解析や脅威の監視、対処を実施できます。効果的なリスク管理には、概要レベルのアラートを参照して詳細レベルにドリルダウンし、ネットワークに導入した各セキュリティ・ツールやセンサーのデータを相関分析できるダッシュボードが求められているのです。

セキュリティ管理の自動化

セキュリティ管理の自動化を掲げた過去のソリューションが大きな成果を上げなかったのは事実です。しかし、最近のソリューションは、より効果的に自動化を実現できるよう進化を遂げています。特に、最も先進的なセキュリティ管理プラットフォームでは、実施可能な処理を厳格に制御しながら、セキュリティ関連のワークフローやタスクを自動化することが可能です。ちなみに、実現できる自動化および統合のレベルは、制御機能の優劣に依存します。

自動化を導入すると、各システムのアクセス先や処理内容を厳密に制限しながら、チケット発行やネットワーク管理、クラウド連携など、システムの安全な統合を実現できます。クラウド環境やアウトソーシング環境との統合の際に、特に重要となるのが安全という要素です。例えば、クラウド連携プラットフォームにセキュリティ機能が組み込まれていれば、仮想マシンのプロビジョニングと同時にセキュリティを自動適用する、その逆に、マルウェアに感染した仮想マシンを直ちに隔離するなどの処理が可能となります。

サイバー・セキュリティで忘れてはならない点は、単にセキュリティ脅威をブロックするだけでなく、ビジネス・プロセスを保護することです。ポリシーの設定ミスが頻発したり、各ネットワーク・セグメントを確実に可視化、保護できないと、組織全体がセキュリティ・リスクにさらされます。

このため、セキュリティ・ソリューションの選定時には、必ず管理機能を評価項目に含めるべきです。セキュリティ・ソリューションの管理性と運用効率は、強固なセキュリティ・アーキテクチャのまさにカギであり、現代のセキュリティ課題を克服できるかどうかを大きく左右します。

「統合」がカギを握る

結論

「私たちがここにいるのは、未来の設計者となるためである。未来の犠牲者になるためではない」

– リチャード・バックミンスター・フラー

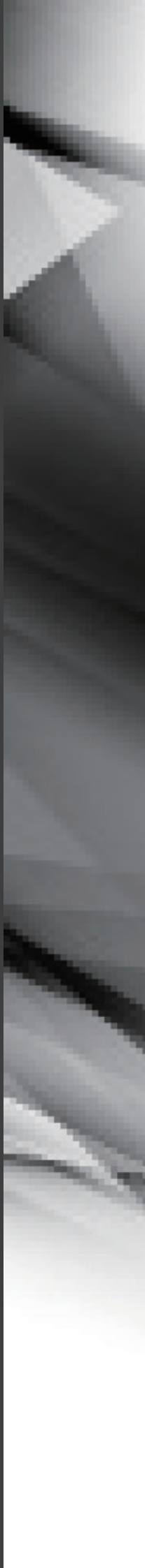
現代の CISO は、拡大と複雑化の一途を辿るネットワークを管理しながら、頻発するセキュリティ侵害に備えるという難題に直面しています。先見の明に秀でた CISO は、次々と新たな手口を編み出すサイバー攻撃者に対抗しながら、技術的な要件とビジネス上の要件の最適なバランスを模索しています。事後対応に徹する受け身のセキュリティ対策では、被害を未然に防ぐことはもはや不可能です。予防を重視するプロアクティブなセキュリティ対策を導入し、各所との協調・連携を強化する必要があります。

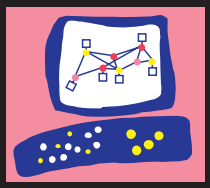
ビジネスを妨げずに、効率的な運用が可能な強固なセキュリティ対策の実現が求められています。では、具体的にどのような選択肢があるのでしょうか。それは、脅威動向の変化に対応できるインテリジェントなテクノロジー、つまり既知および未知の脅威を検出・防御しながら、各種規制に対応し、組織のセキュリティ状況を包括的に可視化できるテクノロジーです。

セキュリティ対策を回避する攻撃側の技術は、さらなる進化と巧妙化を遂げています。防御側も、それに合わせてセキュリティ技術をレベルアップしなければ、ビジネスを継続的に保護することはできません。強力なセキュリティ管理プラットフォームは、問題が起きてから対応するのではなく、問題の発生を未然に防ぐプロアクティブなセキュリティの実現を支援します。事後対応型のアプローチでは、問題発生のたびに時間と労力、金銭を費やす結果を招きますが、予防型のアプローチでは、このようなコストを最小限に抑えることができます。

ポイントはセキュリティの最適化

セキュリティ管理プラットフォームを選定する際には、セキュリティに関するすべての設定を一元的に把握すると同時に、ネットワーク・トラフィック、アプリケーション、イベント、セキュリティ脅威を包括的に可視化できる統合型のプラットフォームに注目してください。また、組織固有のニーズに合わせてカスタマイズできる機能も重要となります。セキュアかつ信頼の置ける API アーキテクチャと、Web およびコマンドライン経由の管理に対応しているプラットフォームにより、この柔軟な運用とカスタマイズが可能になります。運用効率の向上とリスクの可視化、管理権限の委譲を可能にし、真の統合セキュリティ管理を実現するプラットフォームこそ、今日のセキュリティ対策に相応しいソリューションと言えるでしょう。





Check Point®
SOFTWARE TECHNOLOGIES LTD

ONE STEP AHEAD

チェック・ポイントのセキュリティ管理ソリューションの詳細については、
http://www.checkpoint.co.jp/products-solutions/security-management/index.html
をご覧ください。

製品に関するお問い合わせ
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿 5-5-3 建成新宿ビル 6F　Tel：03（5367）2500　E-mail：info_jp@checkpoint.com

August 2016
P/N WD47L0 2016.8