Enterprise Strategy Group | Getting to the bigger truth.™

ホワイト ペーパー

統合されたネットワーク セキュリティ アーキテクチャ：脅威に重点を置いた 次世代ファイアウォール

上級主席アナリスト、Jon Oltsik

2014 年 9 月

この ESG ホワイト ペーパーは、シスコからの委託を受けて作成され、ESG のライセンスの下に配布されています。

目次

要約

ほとんどの大企業では、ファイアウォール、VPN ゲートウェイ、IDS/IPS、ネットワーク プロキシ、マルウェア サンドボックス、Web ゲートウェイと電子メール ゲートウェイなど、多数の戦術的なポイント ツールを使用してネットワーク セキュリティに対応しています。このように別個のテクノロジーが雑然と混在する環境も 10 年前には有効であったかもしれませんが、現在では運用、ポリシー適用、モニタリングに関する重大な問題になってしまいます。さらに大きな問題は、ターゲットを絞った高度な脅威や高度なマルウェア攻撃に対して、ネットワーク セキュリティ防御の効果がますます低くなっているということです。

事態はどの程度悪くなっているのでしょうか。またこれらの問題に対処するために、CISO は何をすべきでしょうか。

- **ネットワーク セキュリティはますます困難なものになっています。**セキュリティの専門家は、ネットワーク セキュリティに関する膨大な課題と毎日戦っています。問題としては、プロセスや管理の重複、ポイント ツールの多さ、手作業のプロセスの多さ、セキュリティ スキルの不足などが挙げられます。このような新旧の問題の中で、現状のネットワーク セキュリティは企業の要求に合わなくなっているのです。
- **現在のネットワーク セキュリティ ツールだけでは不十分です。**多くの組織が、次世代ファイアウォール(NGFW)のような新しいネットワーク セキュリティ ツールを採用しています。たしかに NGFW によってセキュリティは向上しますが、NGFW ではサイバーセキュリティに対する脅威を全体的に防御するよりも、限定されたアプリケーションを管理することに集中しがちです。さらに、マルウェア分析サンドボックスなどの単一のツールは、あくまでも戦術的な対処に留まっています。ネットワーク全体またはクラウドで、保護やセキュリティの可視性の強化はできないからです。
- **大企業では相互運用可能なネットワーク セキュリティ アーキテクチャが必要です。**企業は、脅威集中型で拡張性を備え、手作業のプロセスを自動化し、ポイント ツールではなく相互運用可能なネットワーク セキュリティ サービスを提供できる、統合されたネットワーク セキュリティ アーキテクチャを必要としています。ネットワーク セキュリティ アーキテクチャには、命令と管理の一元化、分散適用、実用的なインテリジェンスの統合が求められます。

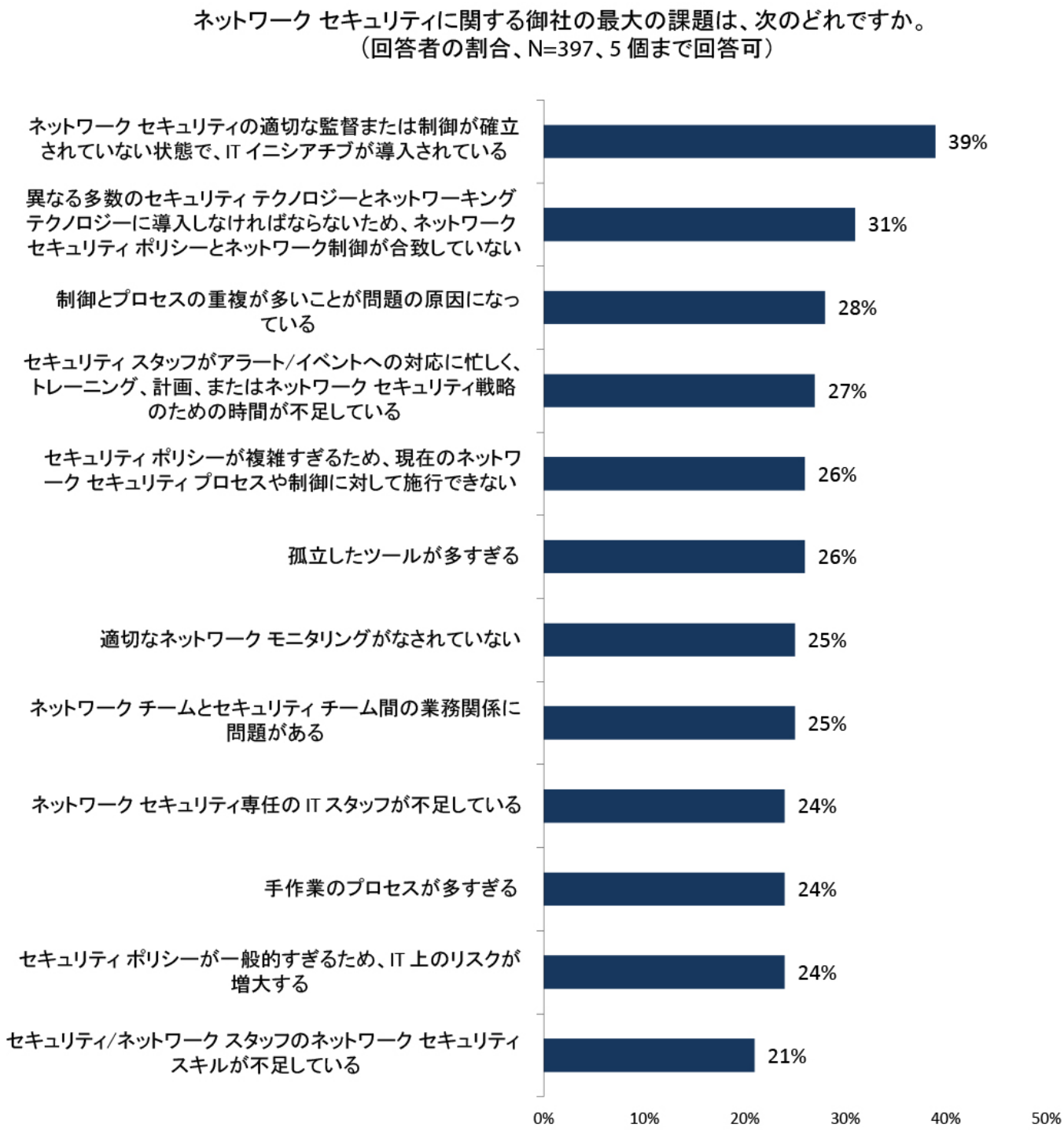
ネットワーク セキュリティに関する課題

大企業では、クラウド コンピューティング、ビッグデータ分析、モビリティ、Internet of things(IoT)アプリケーションなどの新たな取り組みによって、従来型の IT インフラストラクチャの変革を急速に進めています。このような変化によって、企業ではネットワーク セキュリティに対する多数の課題が生まれています(図 1 参照)。[1] CISO は次のような理由でネットワーク セキュリティに苦慮しています。

- **別種のソリューションとテクノロジー サイロが多すぎる。**およそ 3 分の 1(31%)の組織にネットワーク セキュリティ ポリシーと管理の不統一という問題があり、28% の組織でポリシーと管理が過度に重複しており、26% の組織が独自のツールの増大に苦慮しています。このように別種のソリューションとテクノロジー サイロによる混乱のため、セキュリティ インシデントの防止、検出、修復が困難になっています。
- **手作業のプロセスが多すぎる。**ESG のデータによれば、セキュリティ スタッフは、プロアクティブなポリシーや手順によってネットワーク セキュリティに対応するよりも、発生した問題の対処に時間を取られています。また 24% の組織が、手作業のプロセスが多すぎることが問題だと考えています。問題への対処と手作業のプロセスに時間を取られれば、現在のネットワーク セキュリティに求められるリスク管理と緊急対応を行うことができません。
- **ネットワーク セキュリティ スキルの不足。**また ESG のデータによれば、24% の組織でネットワーク セキュリティ専任のスタッフが不足しており、21% の組織にネットワーク セキュリティのための正しいスキルが欠けています。サイバーセキュリティに関するスキルが世界的に不足している状況で、これは致命的な問題です。

[1] 出典:ESG Research Report、*Network Security Trends in the Era of Cloud and Mobile Computing(クラウドとモバイル コンピューティングの時代におけるネットワーク セキュリティの動向)*[英語]、2014 年 8 月。

図 1. ネットワーク セキュリティに関する課題



出典:Enterprise Strategy Group、2014 年。

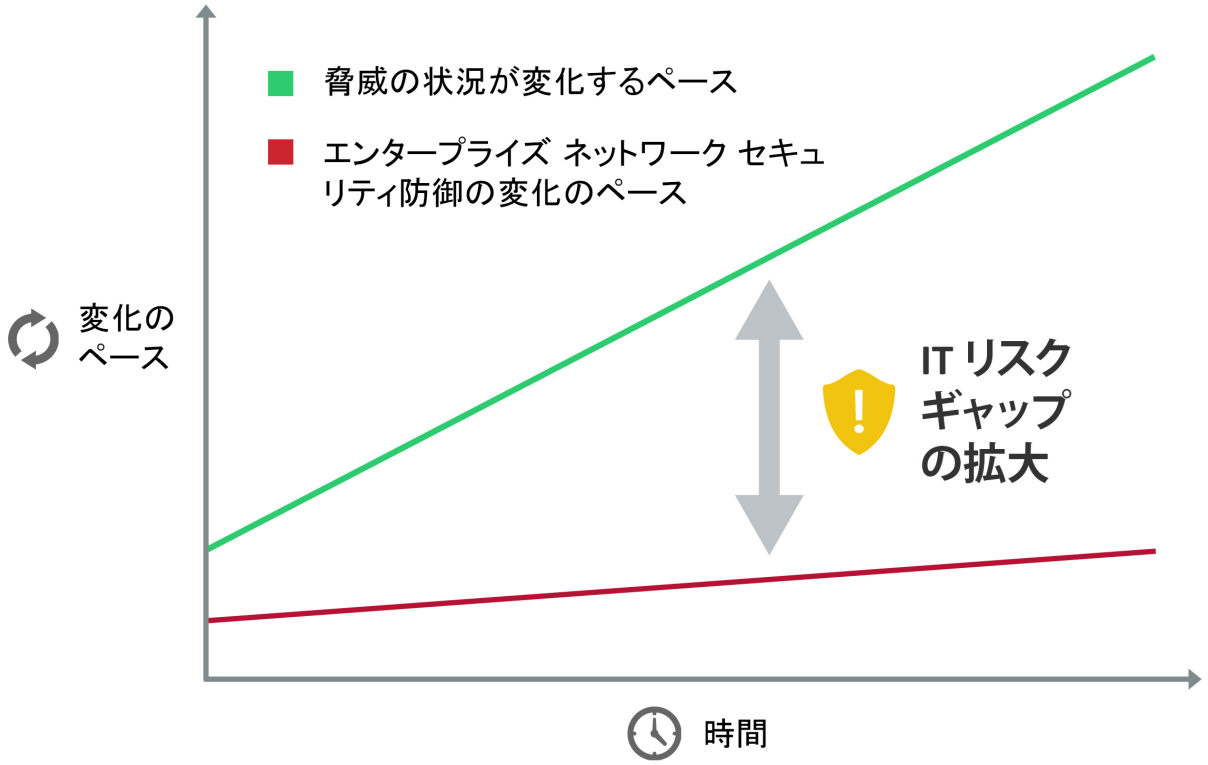
ネットワークのセキュリティ ギャップ

CEO と取締役は、ネットワーク セキュリティの課題は、サイバーセキュリティのリスク管理に関わるさらに大きな問題の一部であることを理解しなければなりません。テクノロジー サイロと手作業によるプロセスをベースにした従来型のネットワーク セキュリティを維持したまま、高度なセキュリティ スキルが不足した状態では、今日のサイバー脅威の規模、多様性、巧妙さに対応することはできません。ソリューションが連携していないと、高度な攻撃

の対象となる死角が生じてしまいます。これが、多くの企業がセキュリティ違反に苦慮している理由の 1 つです。ハッカーはこのようなネットワーク セキュリティの弱点を突いて、レーダーをかいくぐってネットワークのセキュリティ コントロールを迂回し、IT 資産に不正侵入します。ハッカーは一度足がかりを掴むことに成功すると、何ヵ月も姿を隠したままネットワーク上を動き回ってから、ビジネスクリティカルなシステムにアクセスし、最終的に機密データを盗むのです。

CISO はこれまで、サイバーセキュリティの脅威には、ネットワーク セキュリティのテクノロジー、プロセス、スタッフを段階的に強化することで対応する傾向にありました。しかしこれはもう適切な戦略ではありません。簡単に言えば、テクノロジーとエクスプロイトの手法の進化によって、サイバー脅威が急激に増加しています。特に上に述べた運用上の課題を考慮すると、ネットワーク セキュリティに段階的に投資するだけではセキュリティ保護はあまり向上しません。このような状況ではネットワークにセキュリティ ギャップが生じ、IT のリスクが日々増大してしまいます（図 2 参照）。

図 2. 戦術的なネットワーク セキュリティでは IT リスクのギャップが増大する



出典:Enterprise Strategy Group、2014 年。

大企業では脅威に重点を置いた、統合されたネットワーク セキュリティ アーキテクチャが求められる

大企業では、困難な問題に直面しています。エンタープライズ ネットワークは今日の IT とビジネス プロセスを支えるために、可用性と拡張性を備え、動的かつオープンでなければなりませんが、そのようなモデルによって、サイバーセキュリティのリスクが急激に上昇しているのです。従来型のネットワーク セキュリティ コントロールでは、このような流動的な IT 環境と脅威の状況の変化には対応できません。

では何が必要なのでしょうか。ESG は、ネットワーク セキュリティには新たなアプローチが必要であると考えています。CISO は、エッジからコア、さらにクラウドに拡張できる新しいアーキテクチャ モデルに従って、ネットワーク セキュリ

ティを考慮する必要があるのです。ESG は、統合されたネットワーク セキュリティ アーキテクチャを次のように定義しています。

ネットワーク セキュリティのハードウェアとソフトウェアが統合されたシステム。内部ネットワークまたは拡張ネットワークの任意のポイントに、物理的または仮想フォーム ファクタとしてセキュリティ サービスを適用できます。ネットワーク セキュリティ アーキテクチャは、すべてのセキュリティ サービスとコンポーネントが情報をリアルタイムに共有して対応し、セキュリティ制御を微調整し、セキュリティ イベントを検出し、侵害されたシステムを修復できる、基盤となるコミュニケーションを実現します。

脅威に重点を置いた、統合されたネットワーク セキュリティ アーキテクチャは、現在使用されているものと同じタイプのファイアウォール(次世代ファイアウォールと標準のファイアウォール)、IDS/IPS、およびその他のセキュリティ テクノロジーをベースにしています。大きな違いは、個々のデバイスがネットワーク全体にわたって流動的に相互運用され、協調し、テレメトリ情報を共有することです。それによって継続的なインテリジェンスの共有がなされ、デバイスが円滑に連動します。さらに、ファイアウォールや IDS/IPS などのネットワーク セキュリティ機能はサービスとして捉えられるため、LAN、企業データセンター、または外部のクラウド プロバイダーに対していつどこでも一貫性を持って適用することができるのです。

脅威に重点を置いた統合ネットワーク セキュリティ アーキテクチャでは、統合と包括的なカバレッジ、そして相互運用性を確実に実現するために、次の 3 つの事項を満たす必要があります。

1. **命令と制御の一元化**
2. **ポリシー適用の分散化**
3. **実用的なインテリジェンスの統合**

命令と制御の一元化

従来型のネットワーク セキュリティ テクノロジーにおける課題としては、まず管理と運用に関する問題が挙げられます。ネットワーク セキュリティ デバイスにはそれぞれ独自のポリシー エンジン、プロビジョニング、構成、レポート機能があるため、運用コストや冗長タスクに関する大きな問題が生じています。さらに、戦術レベルのレポートを雑多に集めるだけでは、エンタープライズ セキュリティのステータスを把握することは可能だとしても非常に困難です。

このような問題を軽減するために、統合されたネットワーク セキュリティ アーキテクチャでは、まず次のような事項について、一元的な命令と制御を確立する必要があります。

- **サービス管理。**ネットワーク セキュリティ サービスのプロビジョニング、構成、変更は、直観的な GUI とワークフロー エンジンのサポートの下で、他の IT 運用ツールとの相互運用を確保しながら、一元的に管理する必要があります。たとえばネットワーク セキュリティの専門家は、ファイアウォール ルール、VLAN、ルータ/スイッチ ACL のプロビジョニングと構成を、1 つの GUI で処理できることが望ましいでしょう。これだけでも、ネットワーク セキュリティの制御が簡素化され、保護が強化され、ネットワーク セキュリティの運用が合理化されます。
- **サーバの仮想化とクラウドのオーケストレーションによる相互運用性。**VMware、Hyper-V、OpenStack、または AWS の仮想ワークロードを構成する高度なツールは、適切なネットワーク セキュリティ制御でサポートする必要があります。一元的な命令と制御の実現によって、ネットワーク セキュリティ アーキテクチャは、迅速なプロビジョニングやセルフサービスなどのクラウドの利点と、ネットワーク セキュリティ保護の該当するレイヤを関連付ける、適切な API を提供する必要があります。
- **監視とレポート。**統合されたネットワーク セキュリティ アーキテクチャでは、管理機能や運用機能とは別に、イベント管理などのアクティビティに連動した、一元的な監視とレポートが可能でなければなりません。セキュリティ アナリストは、レポートを切り替えたり、複数のレポートをすばやく関連付けたりして、ネットワーク セキュリティのステータスをより正確かつタイムリーに把握する機能を必要とします。ネットワークの盲点を減らすには、一元的な監視とレポートによって、物理的なネットワーク セキュリティ デバイスに加えて、仮想およびクラウドベースの制御も監視されなければなりません。

- **高度な可視性。**監視に加えて、セキュリティ アナリストは環境に対する高度な可視性を必要とします。それによって、多方面からの脅威を検出し、ネットワーク上にあるユーザ、アプリケーション、コンテンツ、デバイスを特定し、それぞれの動きを把握することで、効果的なセキュリティ ポリシーを適用し、脅威の検出と対応を加速することが可能になります。

ポリシー適用の分散化

CISO は一元的な命令と制御によって、グローバルなセキュリティ ポリシーを作成することができますが、これらのポリシーは、ネットワーク全体に存在するさまざまなセキュリティ サービスに適用する必要があります。統合されたネットワーク セキュリティ アーキテクチャは、このような要件に次のように対応できます。

- **あらゆる場所のフォーム ファクタをサポートします。**ネットワーク セキュリティ サービスは、場所を問わず、あらゆるフォーム ファクタで、自由に組み合わせて利用できなければなりません。それによってセキュリティ チームは、ネットワーク セグメント、フロー、アプリケーション、または特定のユーザ グループに対して、ネットワーク セキュリティ ポリシーをきめ細かく適用できます。たとえば小売企業は、物理ネットワークと仮想ネットワークのセキュリティ制御を組み合わせ、さらにファイアウォール、IDS/IPS、そして高度なマルウェア検出ツールを組み入れることで、POS システムが特定の IP アドレスを使用した場合のみ接続できるように制御できます。また企業 LAN のユーザは、パブリック ネットワークを通じて自宅で仕事をするユーザとは異なるアクセス ポリシーの適用を受けることができます。
- **ネットワーク セキュリティ サービスのポートフォリオ。**ネットワーク セキュリティ アーキテクチャは、L2-7 タスクを実行し、LAN、WAN、またはクラウドのあらゆるポイントで、あらゆるタイプのパケット フィルタリングをサポートしなければなりません。ここでは、パケット フィルタリングというカテゴリには、ウイルス、ワーム、DDoS 攻撃、SPAM、フィッシング、Web 脅威、コンテンツ漏えい、アプリケーション レイヤ攻撃などの脅威を検査することが広く含まれます。複数のフォーム ファクタと複数のサービスの組み合わせによって、企業は階層化された高度なセキュリティ スタックを作成し、異なるネットワーク フロー、ユーザ グループ、モビリティ要件に合わせて、また新しいタイプの脅威に合わせて調整することができます。
- **ネットワークとエンドポイントのセキュリティ統合。**従来、ネットワークとエンドポイントのセキュリティは多くの場合、異なるセキュリティ グループが別種のプロセスやツールを使用して管理していましたが、現在のように脅威が潜行する状況では効果を発揮できなくなっています。このギャップを埋めるために、ネットワーク セキュリティ アーキテクチャでは、ネットワークとエンドポイントの侵入防止制御と検出分析を緊密に統合する必要があります。たとえばアプリケーション制御は、ユーザが企業 LAN を通じて、または世界中のリモート パブリック ネットワークからネットワークに接続する場合に、機密資産を保護するために、NGFW とエンドポイントで一貫していなければなりません。インシデント検出を向上させるために、分析サンドボックスはエンドポイント エージェントと相互運用することで、異常で疑わしいネットワーク トラフィックを異常なシステム アクティビティに関連付けることが必要です。

実用的なインテリジェンスの統合

Web 脅威デバイス、IDS/IPS、ウイルス対策ゲートウェイなどのネットワーク セキュリティ テクノロジーは、署名やクラウドからのインテリジェンスの更新に依存していますが、他のネットワーク セキュリティ テクノロジーの多くは、構成変更やネットワーク接続をブロックする新しいルールの作成について、セキュリティ担当者に依存しています。これに対して統合されたネットワーク セキュリティ アーキテクチャは、最初から次のように「インテリジェンス主導」を考慮して設計されています。

- **多様なデータ ソースをベースにする。**SIEM システムは一般的にログ イベントに基づいてセキュリティ分析を実行しますが、ネットワーク セキュリティ アーキテクチャは、その他のタイプの多様なデータを分析に使用します。多様なデータには、NetFlow などのネットワーク ステープルやフルパケット キャプチャの他に、エンドポイントの調査やプロファイリングに関する詳細なデータ、ユーザ/デバイスのアクセス パターン、クラウド アプリケーションの監査なども含まれています。このような新しいデータを適切に組み合わせて関連付け、分析することで、組織のリスク管理が改善され、インシデントの検出と対応が加速されます。

- **クラウドベースの脅威インテリジェンスと統合する。**ネットワーク セキュリティ アーキテクチャは、クラウドベースの脅威インテリジェンスにまで拡張し、ソフトウェアの脆弱性、不良な IP アドレス、不正な URL、既知の C&C チャネル、悪意のあるファイル、Indicators of Compromise(IoC)、急速に変化する攻撃パターンなどの詳細を把握する必要があります。
- **自動化を前提に構築する。**ネットワーク セキュリティ アーキテクチャは最終的に、内部および外部のセキュリティ インテリジェンスを利用して、組織のネットワークのセキュリティ防御を自動化します。たとえば、データセンターに異常なトラフィックがあれば、自動化されたファイアウォール ルールがトリガーされ、ソース IP、ポート、プロトコル、DNS アクティビティなどの要因の組み合わせに基づいてフローが停止されます。あるいはマルウェアが検出されると、ネットワークはファイルのダウンロードを確認し、特定の URL から疑わしいファイルをダウンロードしたエンドポイントを遡って検出して、修復することができます。このような自動修復アクティビティによって、ネットワークのセキュリティ制御が継続的に改善され、セキュリティ調査がシステム化されて、より迅速な対応が可能になります。

つまりネットワーク セキュリティ アーキテクチャは、既存の課題に対応できるだけでなく、ビジネス、IT、そしてセキュリティにとっても利点をもたらすのです(表 1 参照)。

表 1. ネットワーク セキュリティ アーキテクチャの特性

ネットワーク セキュリティ アーキテクチャのプロパティ	詳細	機能	利点
命令と制御の一元化	サービス管理、クラウド/サーバ仮想化オーケストレーションの相互運用、一元的な監視とレポート	ポリシー管理、プロビジョニング、構成管理、変更管理、イベント管理などが一元化される	セキュリティ運用の合理化、使いやすさ、場所やフォーム ファクタを問わずすべてのネットワーク セキュリティ要素にわたる一元的な制御と可視性
ポリシー適用の分散化	すべてのネットワーク セキュリティ サービス、すべての場所、すべてのフォーム ファクタ、ネットワークとエンドポイントのセキュリティ統合	ネットワーク サービス間の協調、クラウドに及ぶセキュリティ ポリシー適用の拡張	多様なユース ケースに対応する階層化されたセキュリティにより、ユーザ、デバイス、アプリケーションを保護。新しいタイプの脅威に対応して簡単に拡張または変更が可能
実用的なインテリジェンスの統合	組み込みのクラウドベースの脅威インテリジェンスなどの多様なデータ ソース	アプリケーション トラフィック、ネットワーク トラフィック、エンドポイント アクティビティ、最新の脅威インテリジェンスを提供	セキュリティ チームはリアルタイムのインテリジェンスに基づいて意思決定ができ、修復プロセスが自動化される

出典:Enterprise Strategy Group、2014 年。

シスコ ネットワーク セキュリティ アーキテクチャ:脅威に重点を置いた次世代ファイアウォール

シスコはネットワーク セキュリティ製品で知られてきましたが、その一方で、急増する企業の要求と危険性を増す脅威の状況に対応するために、テクノロジーに関するビジョンを進化させてきました。シスコはこの目標を達成するために、2013 年にネットワーク セキュリティ分野のイノベーターである Sourcefire の買収に踏み切りました。

シスコと Sourcefire の合併によって、ネットワーク セキュリティ分野の大手企業 2 社が 1 つになりましたが、テクノロジーを統合してエンタープライズクラスのネットワーク セキュリティ アーキテクチャを構築するには、まだ多くの取り組みが必要でした。この努力が実を結んで、Cisco ASA with Firepower Services の発表に至りました。Cisco ASA ファイアウォールと Sourcefire の次世代 IPS、そして高度なマルウェア防御が 1 つのデバイスに統合されることで、シスコは次のような特徴を持った包括的なネットワーク セキュリティ サービスを提供できるようになりました。

- **アプリケーションのきめ細かな把握と管理。**他の NGFW と同様に、シスコではアプリケーション接続を検出してレポートし、ユーザ、グループ、デバイスなどに応じてきめ細かい制御ポリシーを適用できます。FirePOWER ではさらに、アプリケーションの可視性と制御をネットワーク全体に拡張し、各種の機能を TrustSec と Identity Services Engine(ISE)などシスコの他の資産と統合しようとしています。
- **ネットワークとエンドポイントにわたる、脅威に重点を置いた保護。**シスコのネットワーク セキュリティ アーキテクチャには、包括的脅威防御機能と、高度なマルウェア検出/防止機能が含まれています。ネットワーク保護には FirePOWER が、エンドポイントのセキュリティには FireAMP が使用されています。脅威の検出と防止は、FirePOWER NGIPS、レピュテーション/カテゴリベース URL フィルタリング、広範な脅威インテリジェンスによってさらに強化されています。FireAMP では、エンドポイントのアクティビティを追跡して履歴分析を行うこともできます。新たなマルウェア ファイルが発見されると、FireAMP ではレトロスペクティブなセキュリティ ポリシーを適用して、それまでにそのファイルに遭遇したエンドポイントを特定して修復することが可能です。シスコでは最終的に、IPS イベント、脅威インテリジェンス、およびマルウェア イベントを組み合わせて、詳細な IoC を提供します。それによってセキュリティ チームは、セキュリティ調査と修復プロセスを改善または自動化することができます。
- **複数のセキュリティ サービスでエンドツーエンドの可視性を確保。**シスコは、ファイアウォール、アプリケーション制御、IDS/IPS、URL フィルタリング、高度なマルウェアの検出と防止などを行う、物理および仮想のセキュリティ サービスの完全なポートフォリオを提供しています。それによって企業は、複数のフォーム ファクタを使用してネットワーク上のあらゆる場所を対象に、ユーザ、アプリケーション、ネットワーク セグメント、ネットワーク フローに応じて階層化された保護をカスタマイズできるようになります。シスコはこれらすべてのサービスと場所を包含する監視と可視性を実現し、盲点をなくします。
- **影響評価。**シスコのネットワーク セキュリティ アーキテクチャは、侵入イベントと、特定のターゲットに対する攻撃が及ぼす影響を関連付けるように設計されています。シスコでは、このような関連性を 5 つの異なる「影響フラグ」で示しています。1 番目の影響フラグは、特定のホストに関連付けられた、迅速な対処が要求される脆弱性に対応するイベントを示します。その他の影響フラグは、これよりも優先度が低くなります。この方法によって、セキュリティ専門家は限られたリソースを適用する箇所を決定できるようにするため、セキュリティ保護と運用効率の向上につながります。

シスコでは、ASA と FirePOWER を組み合わせることで、攻撃前、攻撃中、そして攻撃後も、セキュリティが向上すると考えています。攻撃前のフェーズでは、シスコのネットワーク セキュリティ アーキテクチャによってネットワーク資産を検出し、セキュリティ ポリシーを適用し、制御を強化することで保護を向上させます。攻撃中は、ASA と FirePOWER を使用することで、悪意のあるまたは疑わしいアクティビティを(ネットワークとエンドポイントで)検出し、ネットワーク接続をブロックし、ネットワーク全体を防御します。そして、シスコのネットワーク セキュリティ アーキテクチャでは攻撃後にも価値が得られます。セキュリティ アナリストはセキュリティ違反の影響を評価し、制御を変更して封じ込めを行い、調査データを活用して修復プロセスを加速することができます。

シスコではさらに機能の向上に取り組んでおり、12 ～ 18 ヵ月のロードマップで多数のアーキテクチャ機能を追加する予定です。またシスコは多くの CISO が、現行のネットワーク セキュリティ防御を評価して、ネットワーク セキュリティ アーキテクチャを構築する計画を策定する支援を求めていることを認識しています。この分野でも、シスコは組織をサポートするさまざまなサービスを用意しています。

結論

サイバーセキュリティについては、次のような現実が広く認識されています。

1. 仮想化、モビリティ、クラウド コンピューティングによって、IT の複雑性がさらに高まっています。
2. 脅威の状況は危険度を増し、ターゲット攻撃は特に防止、検出、修復が困難です。
3. 従来型のネットワーク セキュリティ防御は、現在では効果が低下しています。
4. 多くの組織では、いくつもの分野でネットワーク セキュリティ スキルが不足しています。

全体として、サイバーセキュリティ リスクが日々増大するという、非常に危険な様相を示しています。

かつてアインシュタインは、「狂気とは、同じことを何度も繰り返して行い、異なる結果を期待することである」と述べました。賢明なアドバイスであり、これはネットワーク セキュリティについて多くの CISO が行っていることとぴったり重なります。ビジネス、IT、そしてセキュリティ部門のリーダーは、不毛な戦いを行っていたことを認識しなければなりません。サイバー犯罪者は新しいタイプの武器や戦術を利用しているので、企業も、保護、検出、対応を向上させる新しいタイプの防御によってこの攻撃に対抗しなければなりません。

ESG では、このような強化は、従来型のネットワーク セキュリティ防御の戦術を段階的に変更する方法では達成されないと考えています。それよりも企業は、エンドツーエンドで統合されたネットワーク セキュリティ アーキテクチャによって、より戦略的な変革を進める必要があります。2013 年にシスコと Sourcefire が合併したことで、大きな可能性が生まれました。ASA ファイアウォール、FirePOWER NGIPS、高度なマルウェア防御、そして総合的な脅威インテリジェンスの最良の部分を統合したことで、シスコは統合されたネットワーク セキュリティ アーキテクチャを生み出し、新たなリーダーシップを確立することになります。

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | 電話:508.482.0188 Fax:508.482.0218 | www.esg-global.com