CISCO
SECURE

ホワイトペーパー
Cisco Public

ファイアウォールの今後

将来のビジネスとセキュリティ需要への対応に向けた架け橋を築きながら、より強力な態勢を今すぐ実現

cisco The bridge to possible

目次

概要

このホワイトペーパーでは、ネットワークセキュリティの進化と、組織の環境を将来に向けて保護するために必要なことを説明します。

ネットワークの不均一性が高まるにつれ、組織による一貫したポリシー管理とその適用、一元的な可視性の維持がますます困難になっています。相互接続されたネットワークの複雑さは、エラーや設定ミスの原因となることが多く、進化し続ける高度な脅威に対して脆弱な状態をもたらします。

組織が制御性を強化し、一貫性を維持するためにはどうすればよいでしょうか。まず、ファイアウォールに主眼を置いたセキュリティへの統合アプローチから始めます。

ファイアウォールは依然として組織のネットワークセキュリティ戦略の基盤ですが、ネットワークが進化したように、ファイアウォールも進化しなくてはなりません。以前は、ファイアウォールは、ネットワークトラフィックを許可 / 拒否するポリシー駆動型の制御ポイントとして機能する、入力 / 出力「境界」における単一のアプライアンスでした。今日のデジタル世界で成功を収めるには、組織は単一のファイアウォールにとらわれずに、「ファイアウォーリング」を採用する必要があります。これは、異種ネットワーク全体の論理制御ポイント間で高度なセキュリティ保護を戦略的に調整する、ポリシー主導型の手法です。

ファイアウォーリングは、変化するビジネスとネットワーキングのニーズに合わせて、組織がセキュリティをより良く調整する上で重要なステップとなります。シスコは、ファイアウォールを基盤とした統合セキュリティプラットフォームの構築により、企業のビジネス変革を支援しています。

> 「ファイアウォールは依然として組織のネットワークセキュリティ戦略の基盤ですが、 ネットワークの進化と同様に、ファイアウォールも進化しなくてはなりません」

デジタル変革を進めている組織は、ファイアウォーリングを導入することで、将来のビジネスとセキュリティニーズへの対応に向けた架け橋を築きながら、より強力なセキュリティ態勢を実現できます。

セクション 1：ファイアウォールの歴史

ネットワークセキュリティの進化

従来、ファイアウォールはネットワークエッジのゲートキーパーとして配備されていました。包括的な制御ポイントとして機能し、この境界を通過するネットワークトラフィックを検査してきたのです。ネットワークの入力 / 出力ポイントに位置し、通信を検証するのがファイアウォールの役目です。ここでは、ネットワークの内部トラフィックは本質的に信頼できると見なされ、外部トラフィックは本質的に信頼できないと見なされます。必要なトラフィックがネットワークに出入りすることを許可し、望ましくないトラフィックを阻止するようにルールセットとポリシーが作成され、単一の制御ポイントで適用されます。

ネットワークの境界を城の周りの堀に例えると、ファイアウォールは要塞を出入りするすべてのトラフィックを制御する跳ね橋として機能してきたと言えます。

従来のネットワークセキュリティ

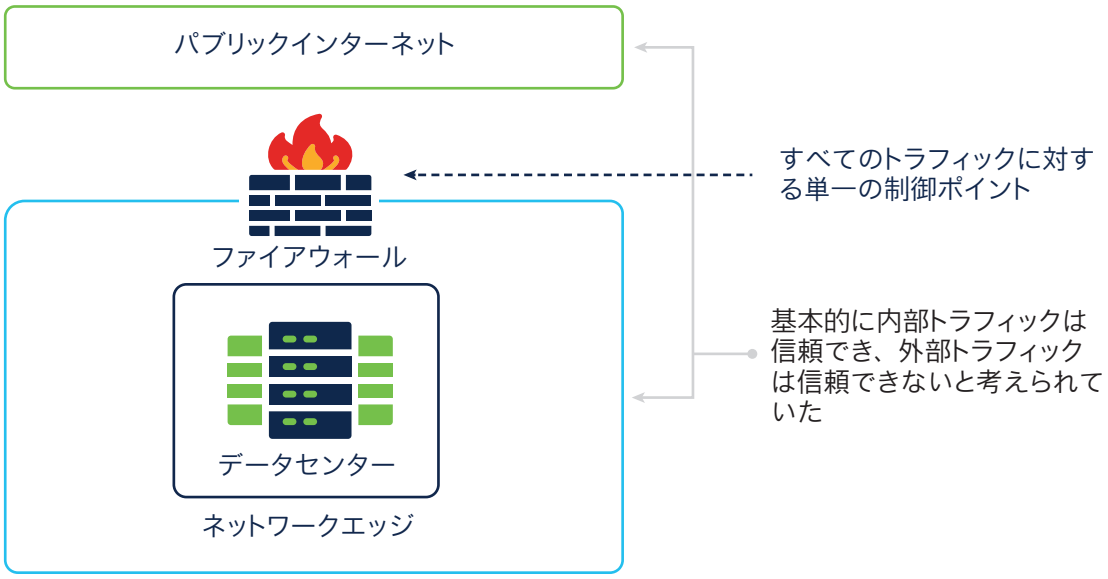


図 1. 従来のネットワーク ファイアウォールのアプローチ

クラウドが登場しました。そして、アプリケーション。

単一の制御ポイントを介してセキュリティを適用する手法が課題になるまでには、時間がかかりませんでした。まず、リモートアクセスとエンタープライズモビリティが台頭しました。次に訪れたのが、クラウドコンピューティングによる変革です。ビジネスがクラウドに移行し、デバイスとユーザは制御された内部ネットワークから外部へと一斉に移行し始めたため、「単一の制御ポイント」モデルが役立たなくなったのです。すぐに複数の境界が形成されました。それらすべてを保護しなくてはなりません。ネットワークの周りに一つの堀を配置する手法は、もはや効果的ではないのです。

現在、ブランチオフィスの場所、リモートの従業員、およびクラウドサービス利用の増加といった要因により、従来のセキュリティ制御ポイントを完全にバイパスして、これまでの「境界」から自由になるデータが増えています。さらに、多くの企業が BYOD（Bring Your Own Device）モデルを採用しており、従業員は個人のコンピュータやモバイルデバイスから機密性の高いビジネスアプリケーションにアクセスできます。実際、従業員の 67% 以上が職場で自分のデバイスを使用し、この傾向には終わりが見えません。パブリックアクセスが可能な Wi-Fi ネットワークを介して接続されたモバイルデバイスやラップトップが普及し、日々の業務にも不可欠となっています。

さらに、圧倒的多数のビジネス拠点やユーザは、クラウドベースの重要なアプリケーションやデータが増加しているインターネットへの直接的なアクセスを必要としています。企業は、複数のクラウドサービス、オペレーティングシステム、ハードウェアアプライアンス、データベースなどにわたってワークロードを展開し続けています。アプリケーションとデータの分散化がさらに進み、その結果ネットワークは多様化しています。

新たな状況

汎用的なアプローチでは、今日の状況に対応できません。

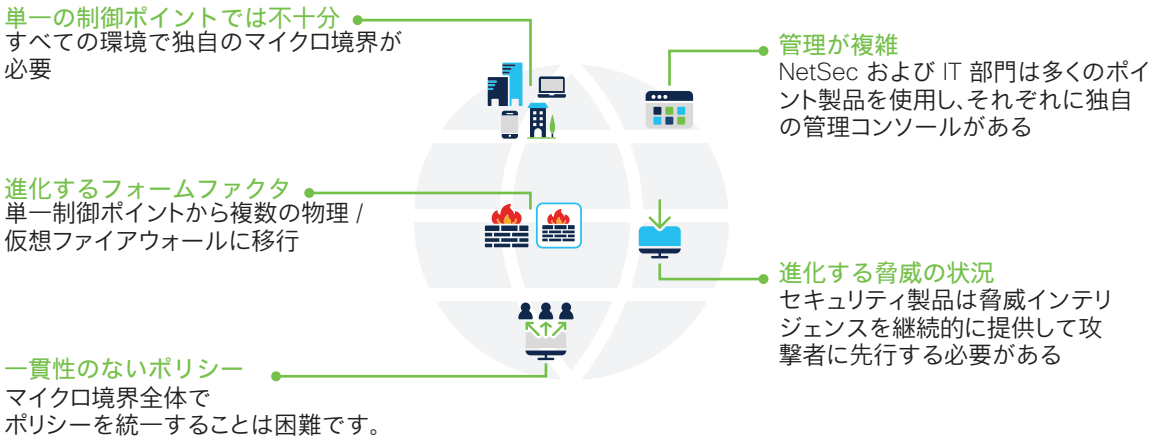
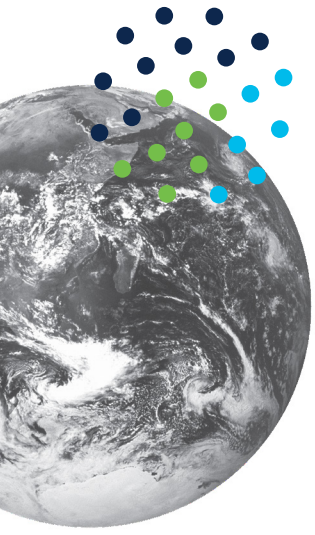


図 2. 従来のファイアウォールモデルは、ネットワークの複雑さと進化する脅威への対応を試されています。

より複雑で、新しい現実

これらのイノベーションにより、相互に接続された生産性の高い職場環境が実現するとともに、ビジネスのあり方が大きく変化しました。アプリケーションを制御し、オンプレミスのユーザを認可する時代から、企業全体にサービスとアプリケーションを提供する動的なマルチクラウドエコシステムへと転換したのです。それだけでなく、ビジネスに不可欠なサードパーティとの関係も管理対象となりました。大規模な拡張とアウトソーシングには、規模と効率性のメリットがありますが、その代償も伴います。ネットワークアーキテクチャの進化により、攻撃対象が大幅に増加し、ビジネスネットワーク、データ、およびユーザを保護する作業が著しく複雑になったことです。

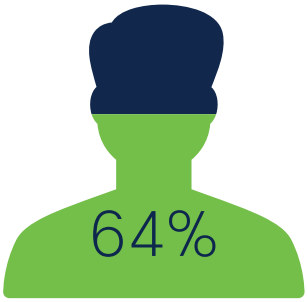


ポイント製品を使って対抗する

組織は通常、新たな問題が発生するたびに「最良」なポイント セキュリティ ソリューションを導入することで、これらの課題に対処してきました。このアプローチにより、企業は平均で 75 のセキュリティツールを使用し、非常に大きなデバイスの「スプロール」が発生しています [1]。様々なベンダーの複数のセキュリティ製品を使用すれば、ネットワーク セキュリティ チームにとって重大な管理上の問題が発生しかねません。ほとんどの場合、セキュリティデバイスとセキュリティ機能が急増すると、攻撃リスクが高まります。質問したところ、IT および情報セキュリティ専門家の 94% が、ネットワークの複雑さが増すと脆弱性が高まり、88% がより迅速にネットワーク セキュリティ ポリシーを変更したいと考えていました [2]。

2019 年 1 月から 7 月にかけて、3,800 件のデータ漏えいが明らかになり、2018 年上半期から 54% 増加しています [3]。この急上昇は、ネットワークを侵害するために、悪意ある攻撃者が、巧妙な手法を使用している証です。侵害の成功率が上昇していることは、従来のネットワークセキュリティ手法が今日の脅威に対抗できないことを示しています。

1「防御の深さ：支出を止めて、統合を開始」、CSO、2016 年 3 月 4 日。
2「ネットワークセキュリティの複雑さをナビゲーション」、ESG 調査インサイト報告、2019 年 6 月
3「ネットワークセキュリティの複雑さをナビゲーション」、ESG 調査インサイト報告、2019 年 6 月



設定ミスの主な原因は人的ミス

脅威、ノイズ、リスクの増大

電子メールから BYOD ポリシーに基づく未確認のエンドポイント、Web ポータル、IoT デバイスにいたるまで、悪意ある組織が新しいベクトルを攻撃しているため、組織は自らを保護するために他の様々なアプローチを試みています。

前述のように、ポイント製品を追加することで、組織の全体的なセキュリティ態勢は改善できません。まったく逆です。セキュリティチームが管理する「ノイズ」は増加します。セキュリティチームは、苦労しながら、避けられない新たな攻撃や、既知または未知のあらゆる脆弱性を狙うマルウェアに目を光らせ続けていますが、このように複雑さが増すことで、セキュリティポリシーの作成、管理、適用の作業がますます困難になっています。

これに対応するため、ネットワーク セキュリティ チームは、多数のクラウドリソースを個別に設定しなくてはなりません。これにより、セキュリティの設定ミスが発生し、侵害につながる可能性がさらに高まります。実装されていない、または不適切に実装されてるセキュリティ制御が最大の要因になり得ます。64% の組織が、設定ミスの主な原因は、人的ミスであると述べています[4]。このようなミスがコンプライアンス違反やサービス停止の原因になったり、攻撃者に門戸を開いてしまうと、リスクに対処する余裕はありません。

今こそファイアウォールを再検討するときです。

ネットワークセキュリティは、骨の折れるタスクです。スタッフが、大量のポイント セキュリティ ソリューション、クラウドリソース、およびアプライアンスを管理するのは難しくなっています。異なるアプローチを採るべきときです。

現在と将来のビジネスに貢献する、アジャイルで統合されたネットワーク セキュリティ プラットフォーム基盤として、今こそファイアウォールを導入すべきです。

セクション 2：ファイアウォールからファイアウォーリングへ

ファイアウォーリングを導入する理由

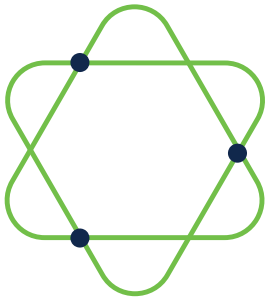
シスコのネットワークは、新しいビジネス手法に対応するため進化しており、シスコのネットワークも同様に進化しなくてはなりません。現在の分散型 IT 資産の世界では、ファイアウォールは依然として堅牢なセキュリティ態勢の中核を成しています。

しかし、さまざまなネットワーク インフラストラクチャ、接続されたデバイス、およびオペレーティングシステムを高度な脅威から保護するために、ファイアウォールの要件が大幅に増えています。そのため、シスコの「従来型」ファイアウォールデバイスは、各種の物理アプライアンスと仮想アプライアンスを組み合わせて、強化を進めています。これらはネットワークに組み込まれる場合もあれば、サービスとして提供されたり、ホストベースの場合、あるいはパブリッククラウド環境に含まれる場合もあります。大規模なトラフィック要件に対応するクラスタ化されたアプライアンス、パーソナルデバイスで動作するソフトウェア、SD-WAN ルータ、安全なインターネットゲートウェイなど、新しいフォームファクタを採用している場合もあります。これらの異種ファイアウォールデバイス間で脅威インテリジェンスを共有するアクティビティは、場所を問わない、統一された脅威の可視性と強力なセキュリティ態勢に不可欠です。

今日のネットワークを完全に移行させ、セキュリティを強化するには、従来の「境界」アプローチから脱却しなくてはなりません。代わりに、保護が必要な情報やアプリケーションに近い、ネットワークファブリック全体に戦略的な適用ポイントを確立する必要があります。具体的には、物理的な制御ポイントと論理的な制御ポイントの両方で、マイクロ境界の作成が必要になります。

スタンドアロンの物理ネットワークデバイスとしてのファイアウォールではなく、ファイアウォーリングの機能について考えなくてはなりません。

4「クラウドセキュリティ違反およびヒューマン エラー」、Fugue、2019 年 2 月 7 日。



ファイアウォールとは

間違いなく、これまで以上にファイアウォールの重要性が高まっています。実際、今日のネットワークを保護するには、**あらゆる場所**にファイアウォールを追加する必要があります。ファイアウォーリングは、あらゆる場所でポリシーベースの制御を確立する方法にフォーカスしている点が異なります。

ファイアウォーリングは、俊敏性と統合性に優れたアプローチを提供し、ますます複雑化する異種ネットワーク全体で、ポリシー、高度なセキュリティ機能、一貫した適用を一元化します。包括的な保護、可視性、ポリシーの調和、より強力なユーザおよびデバイス認証を提供します。また、ファイアウォーリングは、すべての制御ポイントで脅威インテリジェンスを共有することにより、脅威の可視性と制御を統一し、脅威の検出、調査、修復に必要な時間と労力を大幅に削減します。

このように、ファイアウォーリングは今日の複雑なネットワークを保護する重要な戦略となります。ビジネスと脅威の状況が進化し続ける中、未来への架け橋となります。

どのようなものか

クラウド、オンプレミス、またはリモートの場所で資産とデータを保護する場合、ファイアウォーリングは常に高度な脅威保護、ポリシー適用、共有された脅威インテリジェンスを提供しなくてはなりません。課題は、異なるデバイスが導入され、使用されている異種環境全体で一貫性を保つことです。

セキュリティ侵害は、本社、データセンター、リモートサイト、パブリッククラウド、または従業員がリモートで作業する場所に関係なく、インターネットにアクセス可能なあらゆるデバイスから発生します。そのため、リスクを軽減するために、よりロジカルな場所に堅牢なセキュリティ コントロール ポイントを組み込むことがこれまで以上に重要です。セキュリティ制御は、必要に応じて所有環境（物理または仮想アプライアンス、ルータなどのネットワークデバイス）、非所有環境（Security as a Service（SECaaS））、ネイティブ制御、ワークロードに適用されます。

ファイアウォーリングとは

エンフォースメントポイントは、今日の異種ネットワーク全体に存在しています。

ファイアウォーリングは、一貫性のあるポリシーと脅威の可視化機能を備え、一貫した脅威防御機能を提供します。これにより、あらゆる場所で攻撃を迅速かつ正確に防止、検出、阻止できます。

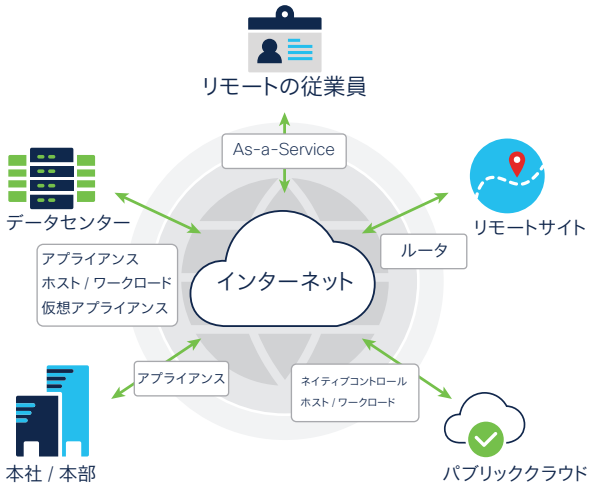


図 3. 最新ネットワークセキュリティ課題に対処する手段としての、ファイアウォーリングのコアテナント

セキュリティ制御の拡張

従来型ファイアウォールの前提では、すべての内部トラフィックと承認されたユーザは、本質的に信頼でき（外部トラフィックは信頼できず）、組織全体の保護はネットワーク境界で行われました。このネットワーク境界は、組織全体を保護する論理的なセキュリティ制御ポイントとなりました。本社、データセンター、またはリモートワーカーからのすべてのネットワークトラフィックは、この単一の制御ポイントを介して集中的に処理されました。

もちろん、このモデルは、組織の IT インフラストラクチャが多様なフォームファクタと配信モデル（物理アプライアンス、仮想アプライアンス、ネットワーク組み込みルータまたはスイッチ（サービスとして提供される、ホストベースの、あるいはパブリッククラウドで提供されるもの））を使用する現在の複雑な環境には適用できません。

ファイアウォーリング アプローチでは、一貫したセキュリティ制御が導入され、完全な可視性、統合されたポリシー、包括的な脅威の可視性が提供されます。これらのセキュリティ制御により、ますます多様化する環境においてユーザとデバイスの認証を強化できます。ユーザ、場所、デバイスなどに関するコンテキストを収集、共有、対応して、デバイスが定義されたセキュリティ要件を満たしていることを確認します。すべてのマイクロ境界で一貫したセキュリティ制御を使用することで、セキュリティチームはタスクの自動化（コンプライアンス違反のユーザとデバイスの自動検疫、すべてのセキュリティ制御で問題のあるドメインのブロック、効果的なマイクロセグメンテーションのサポートなど）を開始できます。ファイアウォーリングでは、完全な可視性により、すべてのセキュリティアラートと侵害の兆候の全体像を把握できます。また、共有の脅威インテリジェンスにより、接続されているすべてのデバイスに対して、最新の脅威検出を行います。

クラウドベースの管理

これは単なるポイント製品ではありません。ネットワーク境界とクラウドリソースの急増により、侵害の危険性も増しています。さまざまなセキュリティ製品を管理しながら、複雑なクラウド環境でビジネスの最も貴重な資産を保護することは容易ではありません。設定ミスを減らすために、セキュリティチームには、即座に視認できる合理化された管理が必要です。

ファイアウォーリングは、一元化されたクラウドベースの管理をサポートすることで、セキュリティ態勢を強化し、セキュリティチーム業務の複雑さを解消し、組織全体でポリシーの調整が可能になります。テンプレートを使用すると、ポリシーを一度記述するだけで、ネットワーク全体で何万ものセキュリティ制御に適用でき、ポリシーの設計と一貫性が向上します。標準のポリシーテンプレートを使用し、新しいデバイスを迅速に導入すれば、設定エラーを削減できます。組織の成長に合わせて、新たに展開する際には最新のポリシーが自動的に継承されます。拡張性のあるポリシー管理システムは、複数のセキュリティ機能を一つのアクセスポリシーに統合し、セキュリティデバイス全体でポリシーを最適化して不整合を特定し、迅速に修正します。

さらに、一元化されたクラウドベースの管理ソリューションが、チームの能力を次のレベルに引き上げます。すべてのデバイスのリスクを迅速に特定し、より一貫性のある安全な状態を保つことができます。単一の管理コンソールを使用して、すべてのデバイス間でオブジェクトを比較し、不整合を検出して現在のセキュリティ態勢を最適化できます。従業員は、ポリシー管理を合理化し、効率性を高め、一貫性のあるセキュリティを実現するとともに、複雑さを軽減できます。

脅威インテリジェンスによる反撃

ネットワークの境界が拡大し、インターネットに直接接続されているデバイス数が急増すると、攻撃対象領域も拡大します。マルウェア、暗号通貨、フィッシング、ボットネットアクティビティに関連するサイバーセキュリティの脅威がエスカレートする中で、サイバー犯罪者は、既存のソフトウェアの脆弱性をエクスプロイトし、悪意ある攻撃を促進するために、機械学習と AI に注目しています。すべてのソフトウェアベンダーの脆弱性パッチを完全にテストし、認定するのに十分なリソースを備えた組織はほとんどありません。ほとんどの組織は、新たな脅威や進化する脅威の攻撃の回避という課題に直面しています。

ここで、ファイアウォールのもう一つの魅力的な側面が役立ちます。業界をリードする脅威インテリジェンスと最新の脅威調査（一部はほぼ最新の状態）を活用し、保護の更新機能にアクセスすることで、絶え間ない脅威の流れを緩和できます。脅威研究者は、侵害の兆候を迅速に特定し、脅威を即座に確認して共有します。規模の経済を活用して、脅威が発生する前に組織を保護します。相互接続されたネットワーク、エンドポイント、ワークロード、クラウド環境全体で脅威インテリジェンスを共有することで、セキュリティチームは、一見切断されたイベントを関連付け、ノイズを排除し、脅威を素早く阻止できます。

ファイアウォーリングを使用しない場合のリスク

ネットワーキングの進歩に伴い、組織はさまざまなポイント製品を導入して、ビジネス要件と運用をサポートしています。新しい攻撃ベクトルが公表されると、相変わらず、最新の XYZ 脅威から保護するために製品を追加しています。従来のファイアウォールを利用して複数の境界にまたがるすべての接続デバイスを保護する場合、最も貴重なデータや資産がセキュリティ侵害にさらされる危険があります。2019 年のサイバーセキュリティ年報によると、サイバー犯罪による損害は、2021 年までに世界で年間 6 兆ドルに達するとみられます [5]。

これらの脅威はネットワークに素早く侵入し、包括的なネットワークセキュリティとエンドポイントの可視性を欠くビジネスの運用を危険にさらす可能性があります。

しかし、組織のネットワーク、クラウド環境、デバイス、データを場所を問わず保護することは、セキュリティチームにとって大きな負担になります。

ファイアウォーリングは、将来を見据えたネットワークセキュリティの基盤となるファイアウォールから始まり、ファイアウォールで終わる

シスコは、このビジョンを実現するために尽力してきました。シスコは世界中のあらゆる規模のビジネスや企業と連携しています。すべての企業において、ネットワークセキュリティをより俊敏に統合し、ネットワーク自体に組み込む必要性があります。そのためシスコは、これまでで最も安全なアーキテクチャ、つまりファイアウォールを基盤とする強力で包括的なプラットフォームを提供しています。

この線に沿ってこれまでにないレベルの保護を提供することは、シスコのセキュリティ戦略の主要な要素です。シスコのセキュリティポートフォリオとシスコのファイアウォールファミリは、進化する脅威の一歩先を進みます。必要なあらゆる場所でワールドクラスのセキュリティ制御と、一貫したポリシーと可視性を提供し、セキュリティ運用を改善するイノベーションを実現します。

脅威の状況がかつてないほどダイナミックになる時代において、シスコはネットワーキングのリーダーシップと最先端のテクノロジーを統合することで、現在と将来に向けた最強のセキュリティ態勢を実現します。

5『2019 年 サイバーセキュリティ年報：100 の事実、数値、予測、および統計』、Cybercrime Magazine、2019 年 2 月 6 日。

従来のファイアウォールでは、表示範囲が限られていました。IT 部門は、脅威をより早い段階で、迅速に検出してブロックするために、脅威インテリジェンスを共有するネットワーク全体の可視性を高める必要があります。ファイアウォーリングはさらに、統合管理に基づく包括的なセキュリティ態勢と、侵入防御、URL フィルタリング、自動化と機械学習を活用した高度なマルウェア防御などの包括的なセキュリティ機能を提供し、効率性を高めます。

ファイアウォーリング戦略が導入されていない場合、ネットワークが複雑になると設定ミスが発生し、セキュリティ侵害のリスクが高まります。Gartner のレポートによると、「2022 年までに、クラウドセキュリティ障害の少なくとも 95% がお客様の過失になる」。[6] 複数の制御ポイント間でセキュリティポリシーを整合させるファイアウォーリング戦略を採用することで、組織の全体的なセキュリティ態勢が改善します。

セクション 3：ファイアウォール戦略を設定するための 4 つのステップ

ステップ 1：最新の次世代ファイアウォールで、成功するファイアウォーリング戦略の基盤を確立します。適切な Cisco Secure Firewall は、統合セキュリティソリューションのために、一貫性のあるセキュリティポリシー、可視性、および改善された脅威対応を提供します。

ステップ 2：Cisco Secure Firewall を選択したら、次は管理ソリューションを標準化します。組織に適したソリューションを決定する際には、次の要因を考慮してください。

- 優先管理場所（オンプレミスまたはクラウド）と、セキュリティ管理を担当するグループ（SecOps または NetOps）を決定します。
- 最も重要なことは、IT の現在および将来の目標に管理ソリューションを適合させることです。ワークロードをクラウドに移行する場合、ベンダーポータルを起動する場合、またはデジタル変革プロジェクトや SaaS アプリケーションに取り組む場合は、クラウドベースの管理を採用することをお勧めします。組織がモノリシックなレガシーアプリケーションに依存している場合は、オンプレミスアプリケーションがニーズに適しているかもしれません。一般的に、レガシーアプリケーションは、クラウド上で適切に実行するためにリファクタリングを行います。これらのアプリケーションをすぐにアップグレードする予定がない場合は、通常、オンプレミスの管理システムが最適です。
- クラウドベースの管理ソリューションにより、ネットワーク運用チームは、組織全体でポリシーを調整し、複雑さを軽減し、中央のダッシュボードからすべてのセキュリティ制御ポイントを管理できます。ポリシーのオーケストレーションとポリシー管理を一つの場所から一貫して簡素化し、最新の脅威から保護します。一元化されたクラウドベースのアプリケーションにより、セキュリティ管理を合理化し、テンプレートを使用して新しいデバイスを迅速に導入し、環境全体のすべての変更を追跡できます。

ステップ 3：統合によってセキュリティ態勢を強化します。ファイアウォーリング戦略では、すべてのマイクロ境界を包括的にカバーし、接続されているすべてのデバイスとセキュリティソリューションを保護および制御する必要があります。異種混在ネットワーク全体、クラウドアプリケーションとクラウドサービス、企業の電子メール、および接続されたすべてのエンドポイントでセキュリティを統合し、拡大する脅威からビジネスを保護します。

このステップでは、より多くの脅威をブロックし、高度な脅威に迅速に対応し、ネットワーク、クラウドアプリケーション、およびエンドポイント全体に自動化を提供するようにセキュリティチームを設定します。

6「クラウドは安全か」Gartner、2018 年 3 月 27 日。

ステップ 4：最後に、ファイアウォーリング戦略に、ビジネス資産を保護するための継続的で、高度な脅威分析を組み込み、新たな脅威に対抗することが大切です。最も簡単な方法の一つは、ファイアウォールを介してネットワークに最新の脅威情報を自動的に提供するソリューションを選択することです。最新のインテリジェンスと完全な可視性により、セキュリティチームは最新の脆弱性を把握できます。脅威が侵入した場合は、その発生場所と方法を特定できます。組み込み型の次世代 IPS 機能により、リスクのランク付けと影響フラグが自動化され、優先順位が特定されるため、最も重要な資産と情報を特定して優先順位を付けることができます。セキュリティチームはただちに是正措置を講じ、脅威を修復し、「ノイズ」に圧倒されることなく、最も重要な資産に集中し、SOC 運用の安全性を高めることができます。

適切なファイアウォールを基盤にすることから始まる

今日のセキュリティチームには、以下のことが必要です。

複雑なネットワークを保護し、脅威を早期に検出して迅速に対応するための、業界トップクラスの脅威インテリジェンスに基づいた**優れたセキュリティ。**

ネットワーク全体で**セキュリティポリシーを効率的に設定、 拡張、 および調整する**方法。

統合された管理と自動化による**可視性と複雑さの軽減**により、セキュリティ運用を迅速化し、エクスペリエンスを向上させます。

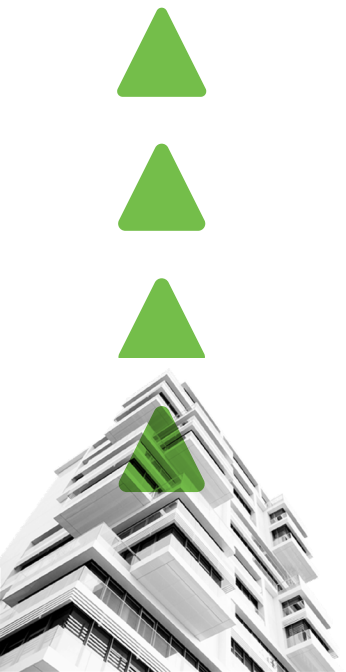
ネットワーキングとセキュリティが連携して、 既存の投資を最大化します。適切なソリューションは、あらゆる場所であらゆるものを保護する包括的なセキュリティを実現するための緊密な統合を提供します。

Cisco Secure Firewall によるファイアウォーリング戦略の利点

ネットワーク全体をセキュリティアーキテクチャの拡張に変えます。共通のポリシー、侵入防御機能、およびその他のコア機能を Cisco Secure Firewall と共有することで、スイッチとルータはセキュリティを適用し、ネットワーク インフラストラクチャを包括的なセキュリティポートフォリオに結び付けます。アーキテクチャ全体で脅威インテリジェンスを迅速に共有し、一見切断されたイベントを関連付け、ノイズを排除し、脅威を素早く阻止します。

ワールドクラスのセキュリティ制御：Cisco Secure Firewall は、脅威の有効性に優れており、ますます高度化する今日の攻撃から複雑なネットワークを保護します。業界をリードする高度な脅威インテリジェンスにより、新しいマルウェアドメインや悪意のある URL 、未知または未公開の脆弱性を検出し、脅威を早期に検出して迅速に対応できます。組み込み型の次世代 IPS は、リスクランク付けと影響フラグを自動化して、包括的な可視性を提供し、セキュリティチームの優先順位を特定し、ノイズを最小限に抑えます。レトロスペクティブ セキュリティでは、最初の検出後に脅威を継続的に分析して情報を把握し、最初は検出されない可能性のある高度なマルウェアを特定します。

統合されたポリシーと脅威の可視性：セキュリティチームは、ネットワークアプライアンスからホスト、クラウドに至るまで、すべてのデバイスでセキュリティ制御を標準化し、推進することで、ポリシーの一貫性と整合性を実現できます。シスコの柔軟で一元化された管理機能により、チームは、拡張性のある制御を多数のデバイスに迅速かつ簡単に適用し、一貫したポリシーを維持できます。アプリケーション ファイアウォーリング、NGIPS 、AMP などの緊密に統合されたセキュリティ機能全体で、一元管理と自動化した脅威の関連付けを実施し、複雑さを低減します。広範なネットワーク全体でセキュリティポリシーとデバイス管理を効率化し、検知、調査、および修復など、主なセキュリティ運用に要する時間を短縮します。



セクション 4：将来に対応するセキュリティソリューション

ワークスタイルは変化しました。シスコのビジネスとネットワークは変革を遂げ、ネットワークセキュリティのルールを変化させました。この発展により、ファイアウォールを再考し、ファイアウォーリングを採用する必要性が高まっています。

シスコは、業界トップクラスの脅威インテリジェンスに裏付けられた、一貫性のあるセキュリティポリシーと可視性により、必要な場所に世界クラスのセキュリティ制御を提供するセキュリティプラットフォームを実現し、こうしたトレンドに対応するイノベーションを推進しています。最新世代の Cisco Secure Firewall は、緊密に統合された製品ポートフォリオの基盤となっています。

シスコの主力クラウド管理ソリューションである Cisco Defense Orchestrator は、さまざまなシスコ セキュリティ製品全体でポリシーを統一します。

すべてのシスコセキュリティ製品には、セキュリティアーキテクチャ全体で対抗策を自動的に共有して展開することで、新しいサイバー攻撃に対応する自動脅威対応ソリューションである Secure Threat Response が含まれています。

Secure Endpoint は、グローバルな脅威インテリジェンス、高度なサンドボックス、リアルタイムのマルウェアブロッキングを提供します。AMP では拡張ネットワーク全体のファイル アクティビティを継続的に分析します。これにより、高度なマルウェアがすばやく検出され、封じ込められ、除去されます。

Talos Threat Intelligence は、現在および進化する脅威の情報を収集する、フルタイムの脅威研究者、データ科学者やエンジニアで構成された世界的に有名なチームです。Talos は、シスコのセキュリティエコシステム全体を支え、攻撃やマルウェアから保護します。Talos は、最新のグローバルな脅威に対する可視性、防御と緩和に関する実用的なインテリジェンス、およびシスコのすべてのお客様を積極的に保護するための集合的な対応を提供します。

SNORT Next-Generation Intrusion Prevention System（SNORT NGIPS）は、トラフィック分析、パケットスニッフィング / ロギング、およびプロトコル分析を実行する、業界トップクラスのオープンソース NGIPS です。SNORT NGIPS は Talos の脅威インテリジェンスを活用し、脅威の発生を防ぐポリシーを共有することでセキュリティコミュニティ全体を支援します。

Identity Services Engine（ISE）では、コンテキストに基づき、あらゆる場所で適応可能な信頼できるアクセスを利用できます。インテントベースのポリシーおよびコンプライアンス ソリューションにより、インテリジェントな統合保護を提供します。

Secure Access by Duo は、多要素認証、エンドポイントの可視性、適応認証、およびリモートアクセスとシングルサインオンによるポリシー適用を提供し、アプリケーションへのアクセスをプロアクティブに保護します。

Secure Network Analytics、Secure Workload、および Application Centric Infrastructure（ACI）が連携し、あらゆる場所にいるユーザや、そのアプリケーションのワークロードを把握し、機械学習、動作モデリング、ネットワーク インフラストラクチャ テレメトリ、セグメンテーションを使用して、新たな脅威を回避します。

シスコのセキュリティプラットフォームと Cisco Secure Firewall に投資することで、将来に対応するファイアウォーリング戦略を実装できます。現在利用できる最も強力なセキュリティ態勢を手に入れて、将来に備えることができます。

セクション 5：今すぐファイアウォールの未来を構築する

シスコは、ネットワーキングのリーダーシップと最先端のセキュリティテクノロジーを組み合わせて、これまでで最も安全なアーキテクチャを実現します。既存の投資を最適化することでネットワークセキュリティを強化する場合でも、ルータをファイアウォールに変換する場合でも、シスコは常に刷新しています。

Cisco Secure Firewall は、ネットワークを構築した企業を起点とする、デジタル変革ビジネス向けに設計されたネットワークセキュリティです。

Cisco Secure Firewall の詳細をご覧いただき、未来のファイアウォーリングへの対応を今すぐ始めましょう。また、2020 年グローバル ネットワーキング トレンド レポートでは、将来のネットワークを形づくる最新のトレンドについて詳しく説明しています。