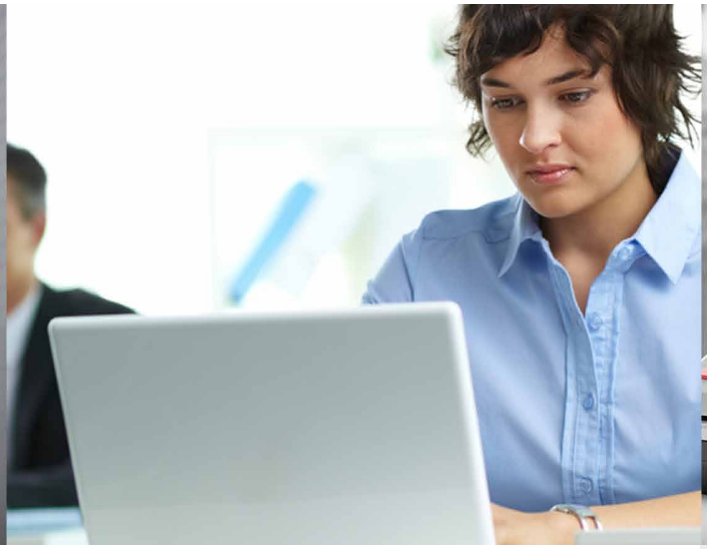
WHITE PAPER

内部ネットワークに潜む脅威からの保護

内部セグメンテーションファイアウォール（ISFW）


目次

概要

過去 10 年の間、企業組織は外部ネットワークとの境界部分にのみファイアウォールを設置することでネットワークの保護に取り組んできました。それにはインターネットエッジ、ペリメータ、エンドポイント、データセンター（DMZ を含む）などが含まれます。この「外部からの脅威の侵入を防ぐ」アプローチは、「企業は明確に定義されたエントリーポイントを制御することで、重要な資産を保護できる」という概念に基づいたものです。その目的は、可能な限り強固な境界保護を構築して、何もファイアウォールを通過させないことでした。

企業組織が成長し、モバイルやクラウドなど最新の IT テクノロジを採用するのに伴い、従来のネットワーク境界の制御やセキュリティはますます複雑になっています。これは、今日の企業ネットワークへのアクセス方法が多岐にわたっているためです。

最近まで、ファイアウォールベンダーは自社アプライアンスのポートに「外部ネットワーク」（Untrusted：信頼されていない）と「内部ネットワーク」（Trusted：信頼されている）と記し、区別していました。しかしながら、内部ネットワークに高度な脅威が侵入すると、ネットワーク内は極めてフラットでオープンであるため、その弱点を突かれることになります。一般的に、内部ネットワークはスイッチ、ルーター、ブリッジなどセキュリティ機能を備えていないデバイスで構成されています。つまり、一度、内部ネットワークにアクセス可能になったハッカー、悪意のある従業員は、あらゆる重要な資産をはじめ企業ネットワーク全体に自由にアクセスできるようになります。

このようなリスクを回避するソリューションが、内部ネットワークの極めて重要なポイントに配備される新しいクラスのファイアウォール「内部セグメンテーションファイアウォール（ISFW）」です。ISFW は、重要な知的財産が保存されている特定のサーバー、ユーザーデバイス、あるいはクラウドに配備されている Web アプリケーションの前に配備が可能です。

主な要件

- **完全な保護の実現** – 単一のセキュリティインフラストラクチャで高度な脅威に対抗する完全な保護を継続
- **ポリシーベース** – ユーザーの制御と区分化を強化し、重要なリソースに対する脅威の侵入経路を制限
- **容易な導入** – トランスペアレントモード適用により、ネットワークの再構成が不要で、一元的な導入展開と管理が可能
- **ハイパフォーマンス** – 高速なギガビットレベルのパフォーマンスにより、ワイヤースピードの East-West（水平型）トラフィックに対応

配備された ISFW は、特定のネットワーク間を出入りするトラフィックを即座に「可視化」することが求められます。ネットワークの計画と導入展開に何か月もかけることなく、直ちに可視化を実現する必要があります。

何よりも、「検知」はソリューションの一部分でしかないため、ISFW は「保護」を提供しなければなりません。ログやアラートの選別には数週間から数か月を要しますが、ISFW は最新のセキュリティアップデートに基づいてプロアクティブなセグメント化とリアルタイム保護を提供する必要があります。

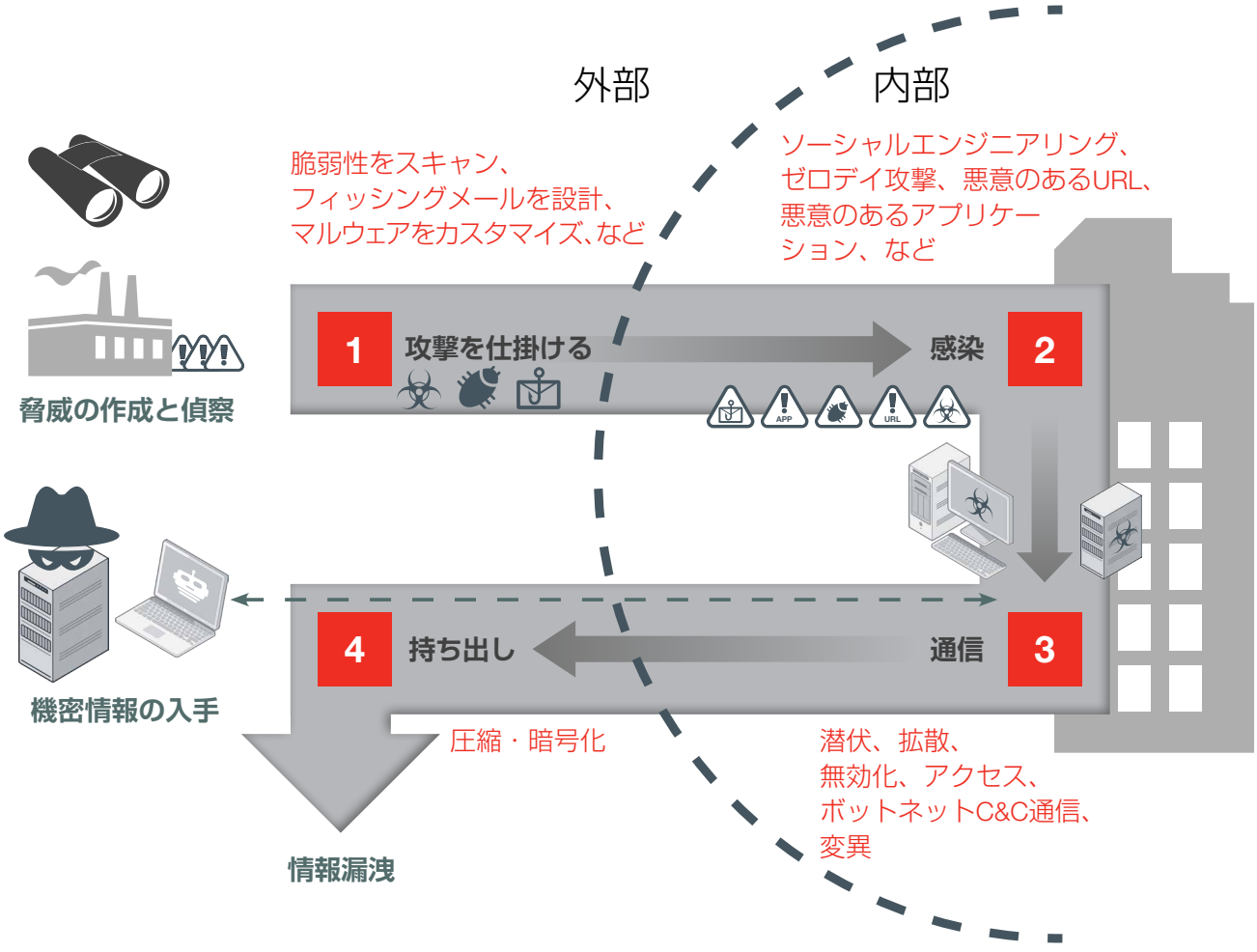
さらに、ISFW には内部ネットワークの任意の場所に配備でき、一元管理のもと企業セキュリティソリューションの他の部分と統合できるだけの柔軟性が不可欠です。他のセキュリティソリューションからも可視化や保護機能を追加で利用できます。たとえば、メールゲートウェイ、Web ゲートウェイ、境界ファイアウォール、クラウドファイアウォール、エンドポイントなどです。また、グローバルネットワーク上での導入展開が可能になるよう、ISFW は低スループットから高スループットに拡張できる必要があります。

「フラットな」内部ネットワークにつけこむ高度な脅威

サイバー犯罪者は、従来の防御対策を回避し、侵入後は検知を逃れて重要なデータを盗み出せるよう攻撃をカスタマイズしています。ネットワークに侵入してしまえば、高度な脅威を検知あるいは防御するシステムはほとんど存在しません。

図 1 に示した脅威のライフサイクルからも分かるように、大半のアクティビティは境界が侵入を受けた後にネットワーク内で行われます。実行されるアクティビティには、エンドポイント型セキュリティの無効化、ボットネット化したデバイスと C&C サーバーとの通信、感染の拡大、狙われた資産の盗み出しなどがあります。

図 1 - 高度な脅威のライフサイクル



答えは新しいクラスのファイアウォール、「内部セグメンテーションファイアウォール（ISFW）」

過去 10 年間に開発された大半のファイアウォールは、境界、インターネットエッジ、ペリメータ（ホストファイアウォール）、エンドポイント、データセンター（DMZ）、クラウドに重点が置かれていました。ステートフルファイアウォールから始まったこの流れも、現在ではファイアウォール、侵入検知、アンチウイルスが結合した分散型ネットワーク向けの統合脅威管理（UTM）が組み込まれるまでに進化しています。その後、侵入防止とインターネットエッジ向けアプリケーション制御の機能を搭載した次世代ファイアウォール（NGFW）が登場しました。最近では高速化が大幅に進み、データセンター向けファイアウォール（DCFW）のスループットは 100 Gbps を超えています。上記のファイアウォールはいずれも、外部ネットワークから侵入する脅威からネットワークを保護する、という一般的な設計になっています。

内部への迅速な導入展開と保護を実現するには、新たなクラスのファイアウォールである内部セグメンテーションファイアウォール（ISFW）が必要です。内部セグメンテーションファイアウォールには、境界ファイアウォールとは異なる特長がいくつかあります。その違いを図 2 に示しています。

ISFW の基盤

企業は、内部ネットワークの極めて重要なポイントをカバーする次世代機能を搭載した ISFW を導入して、次のようなメリットをもたらすセキュリティレイヤーを追加する必要があります。

- ポリシーベースのセグメンテーションを通じて、ユーザーにできるだけ近いところで重要なリソース / アセットへのアクセスを制御します。
- 高度なセキュリティ機能の実装によってセキュリティ対策を確立し、内部ネットワークにおける脅威やハッキングの拡散を阻止および制限します。
- ペリメータ内の脅威による被害の発生を抑制します。
- 脅威の可視性を高め、セキュリティ侵害の検出と対策を強化します。
- 企業全体のセキュリティ体制を増強します。

導入モード	ISFW	NGFW/UTM 中規模〜大規模		データセンター FW	キャリアクラス FW
もっとも重要な用途	内部セグメントの可視化と防御	外部から、もしくは内部からの脅威に対して可視化と防御	外部から、もしくは内部からの脅威に対してユーザーレベルの可視化と防御	ハイスループット、低遅延	キャリアサービス向けカスタマイズドセキュリティセット
設置レイヤー	アクセス（エッジ）レイヤー	Internet Gateway		Core Layer/DC gateway	さまざま
ネットワーク形式	L2 トランスペアレント構成 / L3 構成	L3（Route/NAT）構成		L3 構成	L3 構成
必要なポート構成	ハードウェアアクセラレーションを利用した高いポート密度	ギガビット／ 10 ギガビットポート	高密度のギガビット PoE ポート、無線 AP の統合コントロール	ハードウェアアクセラレーションを利用する高密度の 10/40/100 ギガビットポート	ハードウェアアクセラレーションを利用する高密度の 10/40/100 ギガビットポート
必要なセキュリティ機能	Firewall, IPS, ATP, Application Control	個人認証 Firewall, VPN, IPS, Application Control,	デバイス認識、個人認証を含む統合セキュリティ環境	Firewall, DDoS protection	Firewall, CGN, LTE & mobile security
その他	迅速な展開、細かく設定をする必要はないのが好ましい	ATP 向けに Sandbox を導入や LTE アップリンクを活用		高可用性重視	高可用性重視

図 2 – ファイアウォールの種類による違い

ISFW によるポリシーベースのセグメンテーション機能の必要性

ポリシーベースのセグメンテーション機能を使用することで、ユーザーのアイデンティティと特定のセキュリティポリシーの適用が関連付けられ、アプリケーションとリソースへのユーザーアクセスの制御と区分化が強化されます。ポリシーベースのセグメンテーションにより、ユーザーを媒介にした攻撃や脅威を制限できます。

ポリシーベースのセグメンテーションとは、ユーザーのアイデンティティと適用されるセキュリティポリシーを自動的に関連付けることであると定義できます。ユーザーのアイデンティティは、物理的な場所、ネットワークへのアクセスに使用されるデバイスのタイプ、使用されるアプリケーションなどの属性を組み合わせたものだと定義できます。ユーザーのアイデンティティは動的に変化することがあるため、適用されたセキュリティポリシーもユーザーのアイデンティティに従って動的かつ自動的に変化しなければなりません。

必須のユーザー識別および詳細なセキュリティポリシーの作成と適用に必要なパラメータを実現するには、ISFW に次の機能が不可欠です。

1. ユーザー、デバイス、アプリケーションを識別できること
2. ユーザーのアイデンティティを識別できるよう、ディレクトリサービスソリューションとの統合が可能であること
3. ユーザーのアイデンティティを特定のセキュリティポリシーおよびその適用と動的にマッピングすること

完全な保護機能が求められる ISFW

セキュリティの最初の要素は可視性です。可視性の高さは、ネットワークパケットに関する知識に比例します。パケットストリームが特定のアプリケーションではどのように見えるか、どこから送信され、どこが宛先なのか、どのアクション（ダウンロード、アップロードなど）が実行されているのか、といったことを知っている必要があります。

もう 1 つの重要な要素は保護機能です。悪意のあるアプリケーション、コンテンツ、アクションか？このタイプのトラフィックはこの資産から別の資産に通信していてよいのか？その答えを把握しておくことは、コンテンツやアプリケーションタイプが異なる場合極めて困難ですが、ISFW において不可欠な部分です。悪意のあるファイル、アプリケーション、またはエクスプロイトを検知する能力があれば、脅威に反応して阻止するための時間が企業に与えられます。上記すべての保護要素が 1 台のデバイスに組み込まれていなければ、効果は発揮されません。

可視性と保護機能は、リアルタイムで一元的に提供されるセキュリティ脅威インテリジェンスサービスに大きく依存しています。どの程度の可視性と保護機能が提供できているか、最新の脅威に対応できているか、という質問を常に投げ掛ける必要があります。だからこそ、すべてのセキュリティサービスは常に第三者機関によるテストや認定サービスで評価を受けなければなりません。

導入展開の容易さを求められる ISFW

ISFW は導入展開および管理が容易でなければなりません。簡素であれば、IT 部門は既存のネットワークを再構成することなく、最小限の構成作業だけで導入展開が可能になります。

また、ISFW には、ネットワーク内に分散しているさまざまなタイプの内部資産を保護する能力が不可欠です。重要な顧客情報が保存されているサーバー群や、最新のセキュリティ保護機能へのアップデートが不可能なエンドポイントデバイス群などを保護しなければなりません。

さらに、ISFW には企業セキュリティソリューションの他のコンポーネントと統合する機能が必要です。他のセキュリティソリューションからも可視化や保護機能を追加で利用できます。たとえば、メールゲートウェイ、Web ゲートウェイ、境界ファイアウォール、クラウドファイアウォール、エンドポイントなどです。そのすべてを一元的に管理する必要があります。管理の一元化により、境界、ネットワーク内部、さらにはネットワーク外部（クラウド）に対して一貫性のあるセキュリティポリシーが適用されます。

また、従来型のファイアウォールは通常ルーティングモードで配備されます。インタフェース（ポート）は IP アドレスで明確に定義されます。その計画と導入展開には数か月を要することもあります。サイバー攻撃に即座に対応しなければならない今、そのような時間的余裕はありません。ISFW であれば、中断を最小限に抑えながら、ネットワークへの迅速な導入展開が可能です。デバイスの電源をオンにし接続するのと同じくらい単純で、ネットワークやアプリケーションに対して透過的でなければなりません。

ワイヤースピードのパフォーマンスを求められる ISFW

「内部セグメンテーションファイアウォールはネットワークゾーンに合わせて導入展開されるため、内部または水平方向のトラフィックのニーズに対応し、重要なポイントでボトルネックにならないようにするには非常に高いパフォーマンスを発揮する必要があります。広域ネットワーク（WAN）アクセスや 1 ギガビット / 秒に満たないインターネットスピードを処理する境界上のファイアウォールと異なり、内部ネットワークは数ギガビットと非常に高速です。したがって、ISFW はマルチギガビットの高速で稼働し、ネットワークの速度を低下させることなく詳細なパケット / 接続の調査を実行できなければなりません。

ISFW のテクノロジ要件

柔軟なネットワークオペレーティングシステム

ほぼすべてのファイアウォールの「導入モード」で、IP の割り当てとネットワークの再構成が必要です。これはネットワークルーティングモードと呼ばれるもので、トラフィックを可視化し、脅威防止機能を提供します。一方、構成が容易で可視化はするものの、保護機能は提供しないのがスニファーモードです。

トランスペアレントモードは、ネットワークルーティングモードとスニファーモードの長所を組み合わせたもので、迅速な導入展開と可視化を可能にするだけでなく、保護機能も提供します。これらのモードの違いの要約を図 3 に示します。

導入モード	導入の複雑さ	ネットワーク機能	高可用性	トラフィックの可視化	脅威保護
ネットワークルーティング	高	L3 ルーティング	✓	✓	✓
トレンスペアレント	低	L2 ブリッジ	✓	✓	✓
スニファー	低	X	X	✓	X

図 3 – ファイアウォールの種類による違い

拡張性に優れたハードウェアアーキテクチャ

内部ネットワークは非常に高速で稼働するため、ISFW をマルチギガビットスループットに対応した設計にする必要があります。CPU のみをベースにしたアーキテクチャは柔軟ではありますが、高スループットが求められる状況でボトルネックになります。優れたアーキテクチャでは柔軟性を高めるために現在でも CPU が使用されていますが、ネットワークトラフィックとコンテンツ調査の高速化のためにカスタム ASIC が追加されています。

ISFW はデータやデバイスにより近い場所に展開されているため、厳しい環境への対応を迫られることがあります。したがって、耐久性に優れたフォームファクターの可用性が、もう 1 つの ISFW の要件となります。

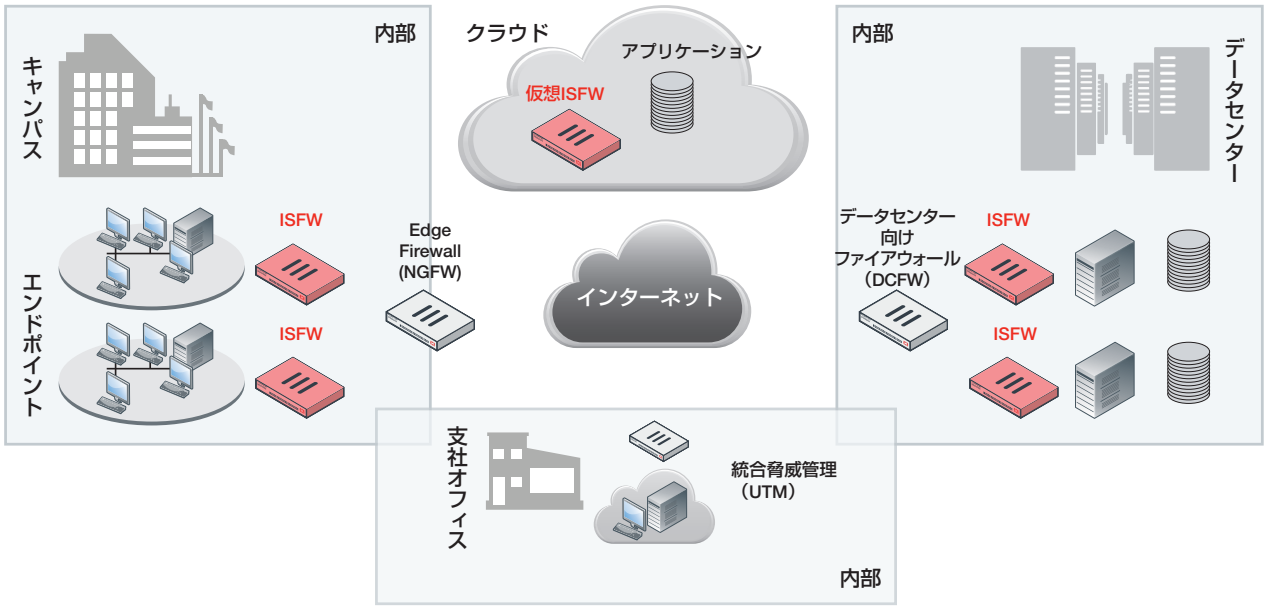


図 4 – 内部セグメンテーションファイアウォール（ISFW）の導入

ネットワークのセグメント化 - 高速統合スイッチ

トランスペアレントモードでは、スイッチを介してサブネットワークとサーバーを物理的に分離する機能が進化しています。現在市場では、アプライアンス内にフル機能の統合型スイッチを搭載した製品としてファイアウォールは認識され始めています。多数の 10 GbE ポートインタフェースを搭載したこのような新しいファイアウォールは、データセンターの理想的なトップオブラック（ToR）ソリューションであり、サーバーを物理的にも仮想的にも保護します。また、1 GbE インタフェースを高密度実装した同様のスイッチ統合型ファイアウォールは、LAN セグメントの分離に最適です。ISFW はその両方の役割を果たす必要があります。また、そのためにはフル機能の統合スイッチ機能を備えているのが理想的です。

リアルタイムセキュリティ

内部セグメンテーションファイアウォールは、IPS、アプリケーションの可視化、アンチウイルス、アンチスパム、クラウドベースのサンドボックス機能との統合など、高度なセキュリティサービスをすべて提供し、標準的な境界ファイアウォールを補完するポリシーの適用を可能にしなければなりません。このリアルタイムで提供される可視化と保護機能は、ネットワーク内部でのマルウェア拡散を抑制するうえで非常に重要です。

ネットワーク全体への ISFW の導入例

大部分の企業はこれまで、境界の保護にファイアウォール、NGFW、UTM を配備してきました。これらは確かにネットワークの保護に重要な要素ですが、内部セグメンテーションファイアウォールをネットワーク内部に計画的に導入することで、セキュリティ対策を強化できます。知的財産が保存されていてセキュリティやサーバーのアップデートが容易でない場所に、特別なエンドポイントセキュリティとして導入が可能です。

セグメントへの ISFW の導入例

ISFW は通常アクセスレイヤーに導入展開され、特定の資産を保護します。導入環境は当初ディストリビューションスイッチとアクセススイッチの間で透過的です。この場合、統合スイッチがアクセススイッチとディストリビューションスイッチに取って代わり、物理的な保護機能を追加するまでの時間が長くなる可能性があります。

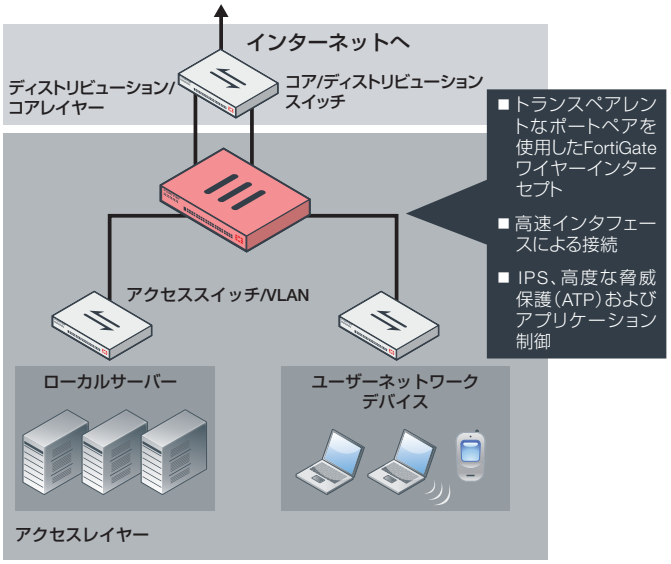


図 5 – 内部セグメンテーションファイアウォール（ISFW）の導入

高度な脅威保護（ATP）を強化する内部の可視化

高度な脅威を緩和する適切なアプローチの 1 つとして、防御、検知、減災というサイクルの継続を検討してください。一般的には、次世代ファイアウォール（NGFW）は防御コンポーネントの主な基盤として機能することで L2/L3 ファイアウォール、侵入防止、アプリケーション制御などを実現し、リスクの高い未知のアイテムをサンドボックスに隔離して検知に役立てる一方で、既知の脅威をブロックします。しかし、NGFW は従来ネットワークエッジに導入配備され、主に出入りを監視するため、攻撃ライフサイクルの一部しか可視化されません。

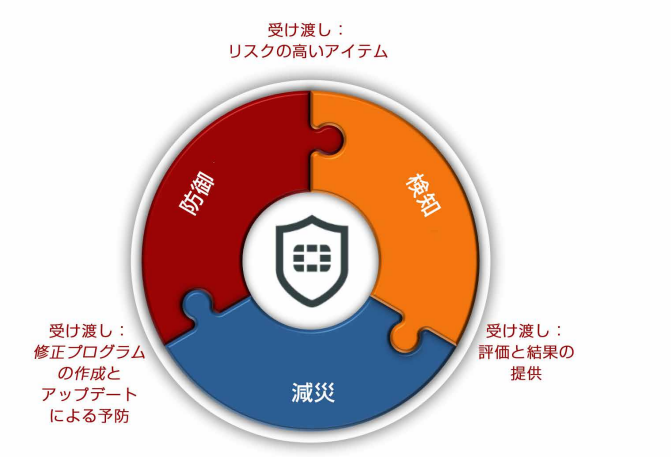


図 5 – 高度な脅威保護（ATP）のフレームワーク

ISFW を導入展開することで、ネットワーク境界に侵入したハッカーによる内部でのアクティビティをさらに完全に可視化できます。水平方向の動きがあれば、ハッカーが重要な資産の特定と情報の持ち出しを試みていることを意味します。また、内部および境界でのアクティビティが完全に可視化されれば、高度な脅威保護（ATP）フレームワークの全フェーズが強化されます。内部ネットワークのトラフィックは境界トラフィックの帯域幅の数倍になることも珍しくないため、ISFW を導入することで、既知の手法によるセキュリティ侵害の拡大を抑止する機会が大幅に増えます。また、より多くの高リスクアイテムがサンドボックスに隔離され、詳細な調査の対象になります。

まとめ

フラットな内部ネットワークは高度な脅威によって悪用されています。境界の防御線を通過してしまえば、拡散とその後に続く重要な資産の流出を阻止する手段はほぼありません。従来型ファイアウォールは低速なインターネットエッジに合わせて設計されているため、このようなセキュリティデバイスの内部への導入展開は困難です。ファイアウォールネットワークの再構成には、長い時間を要します。

内部セグメンテーションファイアウォールは新しいクラスのファイアウォールであり、サービスの中断を最小限に抑え、内部ネットワークを高速なギガビットレベルに維持しながら、迅速に導入展開することが可能です。内部ネットワークの特定の部分を瞬時に可視化し、保護機能を適用できます。

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.co.jp/contact

お問い合わせ