Cisco Secure Firewall

ネットワークと
セキュリティの統合

世界クラスの
セキュリティ制御

一貫性のあるポリシー
と可視性

現在から将来にかけてビジネスを確実に保護

ビジネスクリティカルなアプリケーションがクラウドとオンプレミスの混在環境で実行されるようになった今、ユーザーはどこからでもリソースに安全にアクセスできる必要があります。以前のネットワーク境界は単一でしたが、今や複数のマイクロ境界に分化しているため、従来のファイアウォールアプローチでは十分なセキュリティを確保できません。変化を遂げつつあるハイブリッドワーク環境では、多くの組織にとって、アプリケーションは新しい境界です。ファイアウォール環境も従来型のものから、物理アプライアンス、仮想アプライアンス、およびクラウドネイティブ アプライアンスが混在する環境へと進化しました。その結果、組織は最新のアプリケーション環境のサポートを運用するのに苦労しています。

シスコでは、最新の動的アプリケーションやますます多様化するネットワークにわたってポリシー適用を調和させるために、俊敏性に優れ、自動化された統合アプローチを可能にするネットワーク セキュリティ ビジョンを構築しています。Cisco Secure Firewall は、コアネットワーキング機能とネットワークセキュリティを最も緊密に統合し、これまでで最も安全なアーキテクチャを構築できます。その結果、中小規模の企業から企業データセンター、サービスプロバイダーまで、あらゆる場所でアプリケーションとユーザーを保護する完全なセキュリティポートフォリオが実現します。

メリット

- 統合されたワークロードとネットワークセキュリティにより、動的なアプリケーション環境全体でリアルタイムのアクセス制御を実現します。
- ネットワークセキュリティに対するプラットフォームアプローチにより、主要なソースから得られるインテリジェンスの活用と共有が可能になり、検出、対応、修復を迅速化できます。
- 時間や場所、使用デバイスを問わず、社内ネットワークへの安全性の高いアクセスを実現するとともに、組織、ユーザー、重要なアプリケーションを保護する強力な侵入防御機能を利用することで、リモートワーカーを保護できます。

Cisco Secure Firewall が選ばれる理由

Cisco Secure Firewall ポートフォリオは、進化を続ける複雑な脅威からネットワークをより強力に保護します。稼働時間を最大化して投資を保護する優れたパフォーマンスと強化されたセキュリティにより、現在から将来にかけてビジネスを確実に保護できます。シスコ製品を利用すれば、俊敏性と統合性の両方を兼ね備えたセキュリティ基盤に投資していることになります。これにより、最も強力なセキュリティ態勢を構築できます。

Cisco Secure Firewall に投資することで、暗号化されたトラフィックを検査する際のパフォーマンス低下を起こすことなく、最も高度な脅威からも確実に保護できます。さらに、他のシスコソリューションや他社製のソリューションと統合することで、セキュリティ製品の幅広い豊富なポートフォリオを活用できます。こうした製品を連携させれば、これまでばらばらだったイベントを相互に関連付け、ノイズを除去し、脅威を迅速に阻止できます。

優れた可視性と制御

脅威はより高度になり、ネットワークはより複雑になっています。常に最新の状態を維持し、絶え間なく出現し進化するあらゆる脅威を巧みに回避するためのリソースを備えた組織はほとんどありません。

脅威とネットワークがより複雑になるにつれ、データ、アプリケーション、およびネットワークを保護する適切なツールが不可欠になります。Cisco Secure Firewall は、脅威の一歩先を行くために必要な機能と柔軟性を備えています。暗号化アクセラレーション ハードウェアのおかげで、Cisco Secure Firewall は暗号化されたトラフィックを大規模に検査することができます。これにより、旧世代のアプライアンスと比較してファイアウォールのパフォーマンスが劇的に向上します。さらに、マルチスレッドの Snort 3 検査エンジンは人間が読めるルールであるため、セキュリティのシンプル化に役立ちます。Cisco Secure Workload を統合することで、動的アプリケーションの可視化と制御が可能となり、ネットワークとワークロード全体で今日の最新のアプリケーションを一貫して保護できます。

自社に最適なファイアウォールを探す

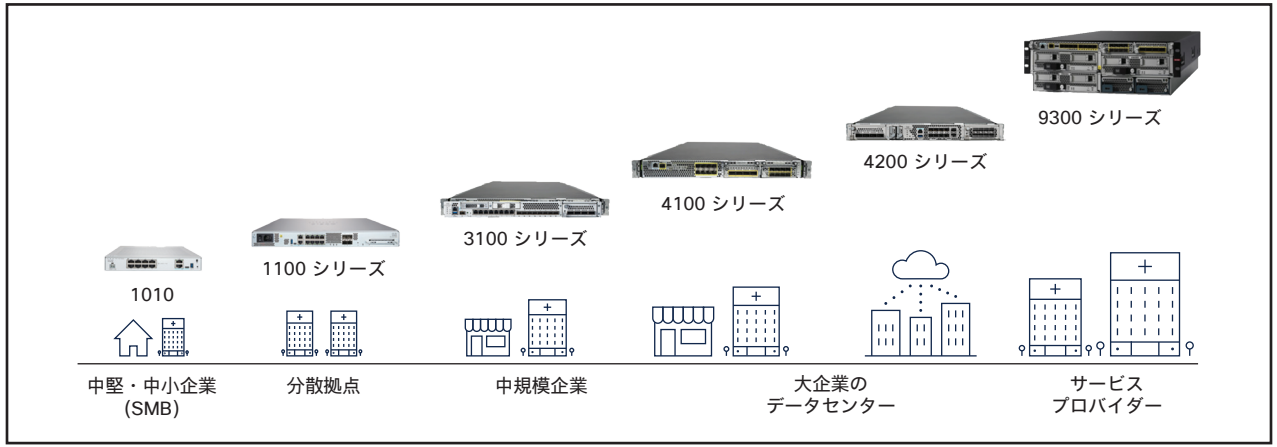

図 1. Cisco Secure Firewall ハードウェアポートフォリオ

シンプルなファイアウォール管理

Cisco Secure Firewall ポートフォリオには、数百のファイアウォールを一元的に包括的に管理するための柔軟な管理オプションがあります。オンプレミスのハードウェアを導入する場合でも、任意の仮想環境を使用する場合でも、見た目や操作感が同じなので、生産性が向上します。シスコのクラウド提供型ソリューションを利用すれば、業務効率を一歩先に進めることができます。

また、シスコは、拡張性の高いログ管理を可能にする Cisco Security Analytics and Logging も提供しています。これにより、脅威検出を強化できます。さらに、保持期間延長機能やふるまい分析機能も備わっているため、組織全体におけるコンプライアンス要件も満たせます。

お客様事例

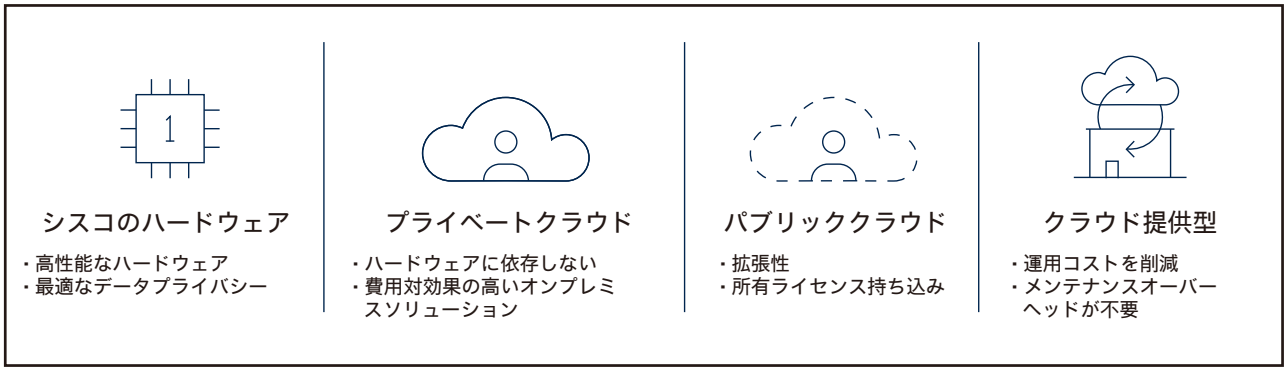

図 2. 多様なファイアウォール管理であらゆるフォームファクタをサポートし、お客様のユースケースに独自の価値を提供

Cisco Secure Firewall の先進的な機能：

先進的な機能	詳細
シンプルなファイアウォール管理	・ Cisco Secure Firewall Management Center（FMC）は、ファイアウォール、アプリケーション制御、侵入防御、URL フィルタリング、マルウェア防御のポリシーを包括的に管理します。
侵入防御システム	・ Secure Firewall は、業界をリードする Snort 3 侵入検知防御システム（IDS/IPS）により、より高速な脅威防御を提供します。
脅威インテリジェンスの更新	・ 世界最大級の民間の脅威インテリジェンスチームである Cisco Talos Intelligence Group は、シスコをご利用のお客様に実用的な脅威インテリジェンスを定期的に提供しています。 ・ また、Talos は、Snort.org と ClamAV.net の公式ルールセットの保守も行っています。

先進的な機能	詳細
動的ポリシーのサポート	・動的属性は、静的 IP アドレスを利用できない場合に VMware、AWS、Azure タグをサポートします。 ・シスコはタグベースのポリシーにおけるパイオニアであり、セキュリティグループタグ（SGT）と Cisco Identity Services Engine（ISE）の属性サポートを提供しています。
Encrypted Visibility Engine (EVE)	・暗号化されたトラフィックを復号せずに制御できるため、パフォーマンスのボトルネックを解消し、コンプライアンス要件を満たすことができます。 ・Encrypted Visibility Engine は、機械学習と人工知能を使用して、暗号化されたトラフィック内の悪意のあるアプリケーションを復号せずにブロックします。
AI Assistant for Security	・ファイアウォールとの連携：ポリシーの特定とレポート作成を支援し、トラブルシューティングと脅威防御を強化し、設定不備、重複するルール、レガシールールの修正を自動化します。
TLS サーバーアイデンティティと検出	・暗号化された Transport Layer Security（TLS）1.3 トラフィックに対し、レイヤ 7 のポリシーを維持できます。 ・すべてのトラフィックフローを復号して検査することが現実的ではない暗号化された環境でも、可視性と制御を維持します。
SD-WAN 機能	・ダイナミック仮想トンネルインターフェイス（DVTI）により、分散拠点から本社へのセキュリティ運用を簡素化します。 ・トラフィックのきめ細かな可視化と制御を実現しながら、ハイブリッドワーカーとリモートワーカーのエクスペリエンスを向上させます。
ゼロトラスト アプリケーション アクセス（ZTAA）	・「承認した後は確認しない」という従来の ZTNA モデルの枠を超えて、個々のアプリケーション別の完全な脅威検出とポリシーを追加します。
Cisco Secure Firewall Cloud Native	・Kubernetes で構築され、AWS で初めて利用可能になった Cisco Secure Firewall Cloud Native は、開発者向けの使いやすいアプリケーション アクセス ソリューションであり、柔軟性の高いクラウドネイティブなインフラストラクチャを構築できます。
クラウド提供型管理	・クラウド提供型のファイアウォール管理ソリューションである Cisco Defense Orchestrator を使用すると、見た目や操作感が同じなので一貫したポリシー管理が可能になるため、運用コストを削減できます。
Security Analytics and Logging	・拡張性に優れたオンプレミスベースおよびクラウドベースのファイアウォールのログ管理機能とふるまい分析機能により、リアルタイムの脅威検出が可能になり、対応時間が短縮されます。 ・すべてのシスコ ファイアウォールのログを集約することで、コンプライアンスのニーズに対応できます。 ・ファイアウォールマネージャとの緊密な統合によって、ロギングと分析を拡張し、ファイアウォールのログデータを単一の直観的なビューに集約します。
Cisco Secure Workload の統合	・Cisco Secure Workload（旧 Tetration）を統合することで、ネットワークとワークロード全体で最新の分散アプリケーションと動的アプリケーションを包括的に可視化し、拡張可能な方法で一貫性のあるポリシーを適用できます。
Cisco XDR	・Cisco XDR プラットフォームを活用すれば、脅威検出と修復を迅速化できます。Firewall Management Center により、セキュリティチームは即座に Cisco XDR のオープンなプラットフォームに切り替えられるようになったため、インシデント対応を迅速化できます。

次のステップ

Cisco Secure Firewall の詳細については、https://www.cisco.com/site/jp/ja/products/security/firewalls/index.html を参照してください。購入オプションの詳しい情報やシスコのセールス担当者への問い合わせをご希望の場合は、cisco.com/c/ja_jp/buy.html をご覧ください。