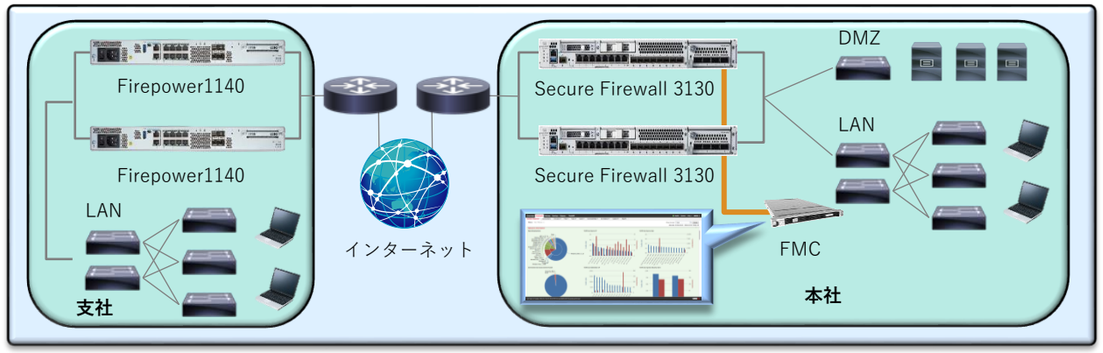
構成例

- Firepower/Secure Firewallシリーズ（FTD-OS）利用時の構成例です。
  - ・設定および監視は、専用管理製品「Cisco Secure Firewall Management Center（FMC）」を使用します。
  - ・冗長構成（Active/Stanby）が可能です。 ※性能要件に応じて幅広いラインナップの中から選択可能です。



製品ラインナップ

＜Firepower1000シリーズ / Firepower2100シリーズ＞

製品モデル		1010	1120	1140	1150	2110	2120	2130	2140
製品写真									
最大スループット	IPsec VPN	400Mbps	1.2Gbps	1.4Gbps	2.4Gbps	950Mbps	1.2Gbps	1.9Gbps	3.6Gbps
	AVC [※1]	890Mbps	2.3Gbps	3.3Gbps	5.3Gbps	2.6Gbps	3.4Gbps	5.4Gbps	10.4Gbps
	AVC + IPS	880Mbps	2.3Gbps	3.3Gbps	4.9Gbps	2.6Gbps	3.4Gbps	5.4Gbps	10.4Gbps
拠点間VPNピア数		75	150	400	800	1,500	3,500	7,500	10,000
冗長構成		Active / Standby							
二重化電源		–	–	–	–	–	–	オプション	標準搭載

＜Secure Firewall3100シリーズ / Secure Firewall4200シリーズ＞

製品モデル		3105	3110	3120	3130	3140	4215	4225	4245
製品写真									
最大スループット	IPsec VPN	5.5Gbps	8Gbps	10Gbps	17.8Gbps	22.4Gbps	45Gbps	80Gbps	140Gbps
	AVC [※1]	10Gbps	17Gbps	21Gbps	38Gbps	45Gbps	65Gbps	80Gbps	140Gbps
	AVC + IPS	10Gbps	17Gbps	21Gbps	38Gbps	45Gbps	65Gbps	80Gbps	140Gbps
拠点間VPNピア数		2,000	3,000	6,000	15,000	20,000	20,000	25,000	30,000
冗長構成		Active / Standby							
二重化電源		オプション			標準搭載		オプション	標準搭載	

安全に関するご注意　★本製品の設置/接続/使用に際しましては、取扱説明書などに記載されております注意事項や禁止事項を熟読のうえ、必ずお守り下さい。

※1 AVC：アプリケーション可視化/制御
(Application Visibility and Control)

お問い合わせは、下記のNECへ
プラットフォーム・テクノロジーサービス事業部門
URL：https://jpn.nec.com/datanet/cisco/

Specialization
- Advanced Service Provider Architecture Specialization
- Advanced Data Center Architecture Specialization
- Advanced Enterprise Networks Architecture Specialization
- Advanced Security Architecture Specialization

日本電気株式会社 〒108－8001 東京都港区芝五丁目7－1(NEC本社ビル)　2023年12月現在　Ver.9　20231227BCC592

Firepower/Secure Firewallシリーズ　Ver. 9

Orchestrating a brighter world　NEC

次世代ファイアウォールアプライアンス

Firepower/Secure Firewallシリーズ

IPS、ファイアウォール、マルウェア対策を一台に集約した
次世代ファイアウォール製品

IPS、ファイアウォール、マルウェア対策を一台に集約した次世代ファイアウォール製品。万が一の感染時にもスムーズに対応できる現実的なセキュリティを提供します。

Firepower/Secure Firewallシリーズが提供する脅威対策

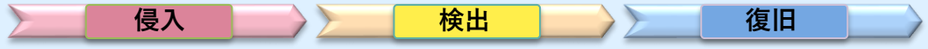
- **次世代ファイアウォールとしての高度な検知と分析力に加え、管理面でも充実した機能を提供します。**

※Firepower/Secure Firewallシリーズでは、ASA-OS(ファイアウォール機能)とFTD-OS(次世代ファイアウォール機能)のどちらか選択可能です。本リーフレットでは、FTD-OSの機能を紹介します。

多層防御をすり抜けるサイバー攻撃に対抗する総合セキュリティ対策

- **求められるのは問題発生時の迅速な対応**
  近年、高度なマルウェアにより、情報流出などの被害が拡大しています。これらに対し、単一のセキュリティフェーズや製品だけで全ての脅威に対処することは不可能であり、感染発覚時の事後対策が必須です。

＜セキュリティ対策の流れ＞



シスコセキュリティは従来から重視されている侵入/検出フェーズだけでなく、問題発生時の原因特定と障害復旧および再発防止を迅速に行い、短期間での復旧を実現します。

★ 管理製品「Cisco Secure Firewall Management Center」利用時の機能

業界最高水準のIPSエンジン

[IDS/IPSとして実績No,1のエンジン"Snort"を採用]

すでに世界で30万以上がセンサーとして稼働中であるIPS業界の標準コアエンジンです。

Snortを使用
検知率評価NO,1
総シグネチャ数 3万以上
Windowsゼロデイ脆弱性カバー率 No1

検知率は全モデルで同等です。オープンソースであるため検知要因を管理者が明確に把握することができます。

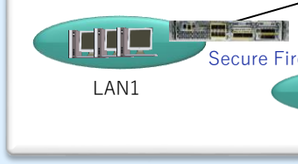
ネットワークとホストの可視化/管理

[設定/ログ解析ツール]

「Cisco Secure Firewall Management Center」は 複数のSecure Firewallの情報収集・収集データの相関分析・管理を行えます。

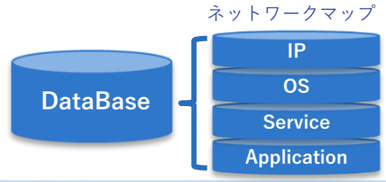
設定/管理のWebGUIは日本語対応

ログ解析で詳細な可視化



[ネットワークマップの作成] ★

監視対象ネットワーク上のホスト情報を収集し、全てをまとめたマップを作成します。



ネットワークマップでホストごとにOSや使用アプリなどの詳細情報が可視化できます。また、収集した情報はイベント解析などに利用されます。

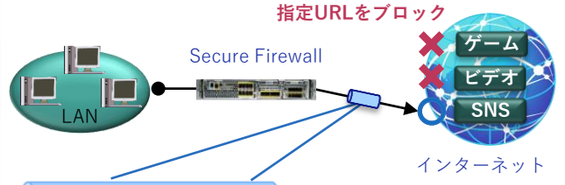
次世代ファイアウォール機能

[URLフィルタ機能]

指定したURLやカテゴリ(SNS/ゲーム/ビデオなど)ごとにWebアクセスを制御できます。

[アプリケーション制御]

通信をモニタし、アプリケーションを識別することで、個別またはカテゴリごとに動作の制御が可能です。



従来のファイアウォールより柔軟な制御が行えます。

アプリ内の動作も制御可能

かんたん設定

[推奨設定]

初期設定は「防御優先」「バランス重視」「通信優先」の推奨設定から一つを選択するだけで完了します。

複雑な初期設定が容易に行えます。

[IPSシグネチャ自動チューニング] ★

ネットワーク環境を学習し、推奨設定を自動でチューニングするので常に最適な環境で利用できます。

必要なシグネチャのみ有効化されるので誤検知が大幅に削減できます。

詳細なログ解析

[インパクト解析] ★

攻撃と対象端末情報を解析し本当に危険度の高いログを識別

必要な管理者が確認すべきログを大幅に減らせます。

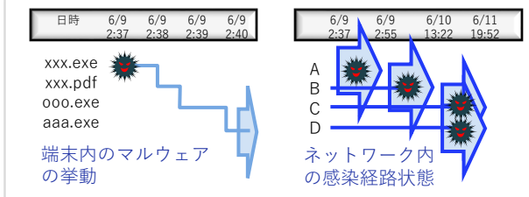
[インシデント相関分析] ★

IPS、マルウェア検知、不正通信等の異なるエンジンで検出した独立のイベントを相互に関連付けて分析します。

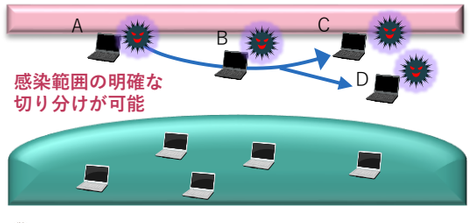
攻撃や障害の全体像を把握するのに役立ちます。

感染範囲を一目で判断

[ファイル追跡] ★



一度検査に通ったファイルでも挙動を把握しておくため、後にマルウェアだと判明した場合、即座に隔離することが可能です。
また、感染が発覚した場合、影響を受けた端末や経路を特定し、感染範囲を最小限に抑えます。



万一の感染時に原因の究明、障害復旧、再発防止が迅速に行えます。

※マルウェア検知は単体のみで動作可能(管理製品不要)
※端末内の挙動確認には別途クライアントソフトが必要