Cisco WEB セキュリティ アプライアンス（WSA）

Web に関わる脅威を
包括的なソリューションで防御

入口対策

- URL フィルタリング
- Web2.0 アプリケーション可視化と制御
- 改ざん Web サイト対策
- マルウェア、スパイウェア多重スキャン
- サンドボックス

出口対策

- ボットネット通信の可視化、遮断
- ファイル レトロ スペクション

Cisco WEB セキュリティ ソリューション

Webの入口、出口対策や未知のマルウェアに対するセキュリティ ソリューションをWSA1台で提供いたします。

マルウェアやフィッシング詐欺から
情報が盗まれる脅威から従業員を保護。

不正サイト防御
・WEBレピュテーション フィルタ
・WEB Usage Control

マルウェア防御
・McAfee アンチ マルウェア
・Sophos アンチ マルウェア
・Webroot アンチ スパイウェア
・Advanced Malware Protection（AMP）

入口対策

Cisco WSA

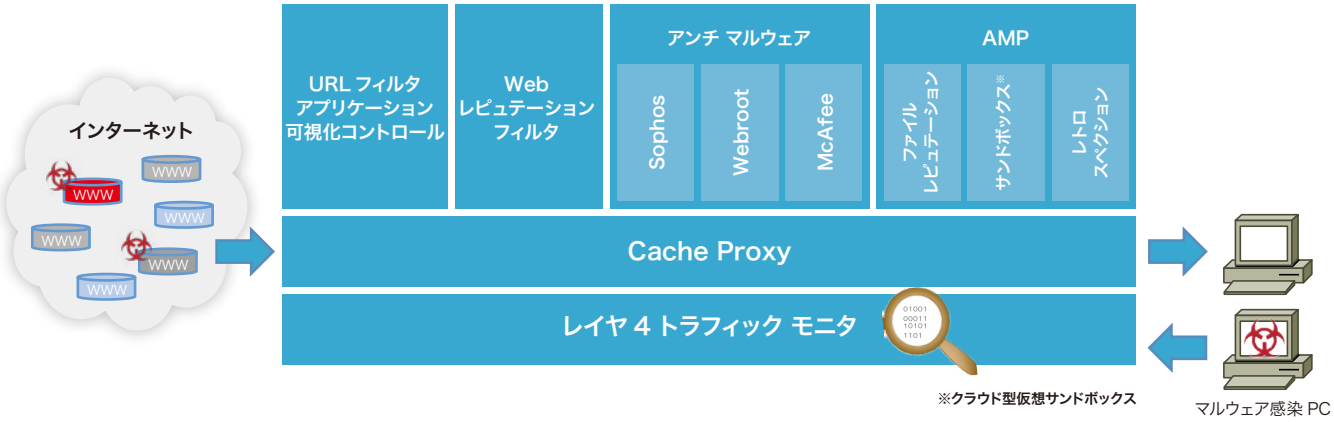
出口対策

従業員や新種マルウェアによる情報漏洩から
会社を保護

情報漏洩対策
・ポリシー フィルタ
・WEB Security Manager
・Web2.0アプリケーションの可視化と制御

マルウェア出口対策
・レイヤ4 トラフィック モニタ

Cisco WSA 内部フロー



業界最大規模のセキュリティ クラウド

Cisco Corrective Security Intelligence（CSI）は、Cisco Security Intelligence Operations（SIO）と、Sourcefire Vulnerability Research Team（VRT）を統合した世界最大級の解析力と情報提供体制を誇るクラウドベースのセキュリティ サービスです。世界中のCiscoセキュリティ製品から情報を収集して脅威を解析し、レピュテーション（危険度の格付け）情報をリアルタイムでフィードバックしています。Cisco CSIによってCisco製品は、進化を続ける最新の脅威に対してもタイムリーな対策を講じます。

Cisco CSI の特長

・全世界に設置された 160 万台の Cisco 製品からビッグデータを収集
・全世界の E メール トラフィックの 35% 以上を監視
・1 日に 100TB のデータ、180,000 のサンプル ファイルを受信
・1 日に 130 億の HTTP を解析
・600 名以上のエンジニアや専門家、研究者が 24 時間体制で解析

URL フィルタリング
ダイナミック コンテンツ解析

膨大な量のWebサイトを登録したデータベースとリアルタイムなダイナミックURLカテゴリ分類機能の組み合わせにより、アクセス先のURLカテゴリを高い精度で判別します。データベースのアップデートは毎日行われ、数万のURLが新規に追加されています。デフォルトでは78のURLカテゴリに分類していますが、カスタムURLカテゴリの追加にも対応しています。URLフィルタリング機能の管理はポリシー設定に統合されており、ソースIPアドレスや外部ディレクトリとの連携で判別されるグループごとに適用条件を変更することもできます。

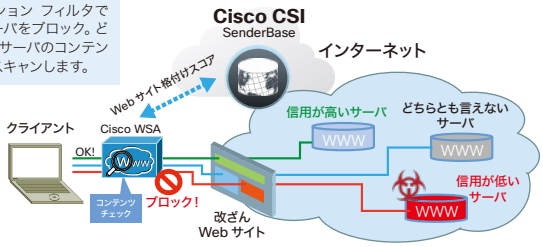
Web2.0アプリケーション可視化と制御

Cisco WSAは、ネットワーク全体のアクティビティを可視化とコントロールできます。何百もの Web 2.0 アプリケーションや150,000以上の小規模なアプリケーションの使用を簡単に制御できます。きめ細かい制御で、DropboxやFacebookなどのWeb2.0アプリケーションの使用を許可しながら、ドキュメントのアップロードや「いいね」ボタンのクリックといったアクティビティを阻止することができます。

WEB レピュテーション フィルタ

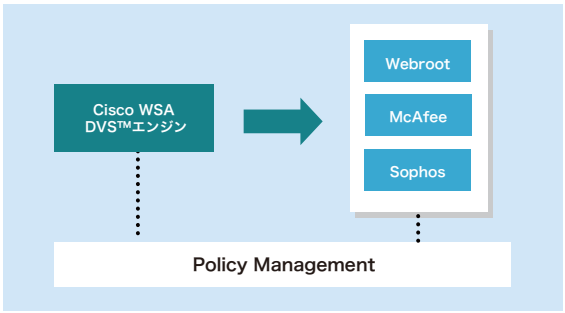
Web レピュテーション フィルタは、Cisco CSIのレピュテーション サービスであるSenderBaseから提供されるWebサイトの信用度を格付けたスコアをもとにして、Webアクセスの 制御を実施します。SenderBaseでは、WebサイトやURLに関連する様々な情報（マルウェア感染の報告やフィッシング メールでの利用、サイト管理者 の情報など）が収集され、独自のアルゴリズムにもとづいてスコア（最高評価が10.0、最低評価が-10.0で、0.1刻みの200段階）を生成します。レピュテーションにより正規サイトを改ざんした水飲み場型攻撃対策も講じる事が出来ます。

Webレピュテーション フィルタで格付けの低いサーバをブロック。どちらとも言えないサーバのコンテンツをマルウェア スキャンします。



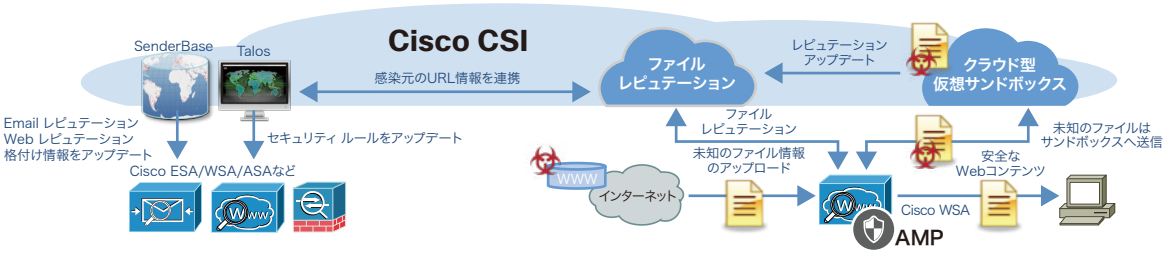
アンチ マルウェア対策

WSA1台で最大3種類のマルウェア対策エンジンを搭載し多重スキャン可能です。マルチベンダのアンチ マルウェア エンジンを組合せることでウイルス、ワーム、トロイの木馬、スパイウェア、アドウェア等多様なマルウェアの脅威を排除します。



アドバンスド マルウェア プロテクション（AMP）

ファイル レピュテーションによる新種マルウェア検知とサンドボックスによる挙動解析、レトロ スペクションによる追跡調査

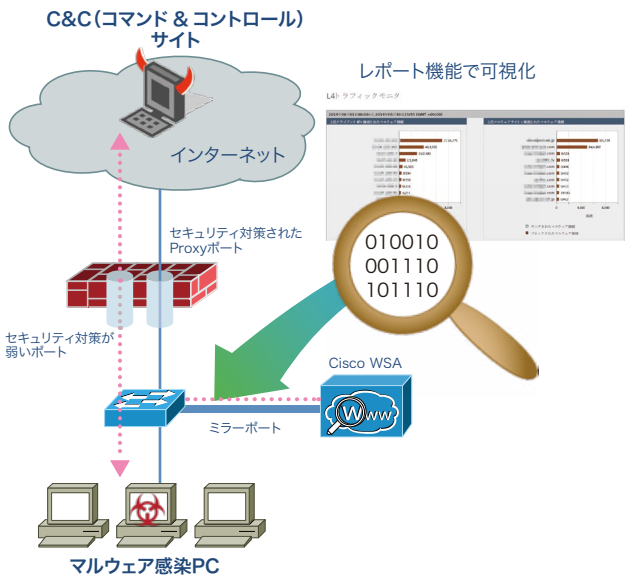


Cisco WSA/ESAは、世界最大級の解析力と情報提供能力を持つシスコのセキュリティ基盤Cisco CSIと連携し、常に最新のセキュリティ脅威に対応します。

Cisco AMPは、Webへのアクセスやメール受信時に未知の（疑わしい）ファイルを発見すると、それらの挙動を解析するCisco CSIクラウド型仮想サンドボックスへ自動的に送信します。解析結果は以後のファイル レピュテーションに反映され、セキュリティ強度を継続的に高めます。

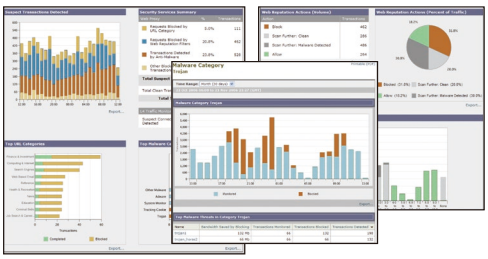
出口対策
レイヤ 4 トラフィック モニタ

キーロガーやトロイの木馬に代表されるスパイウェアは、PCに侵入して、対象となる情報を入手し、それを持ち帰ることを目的としています。スパイウェア 対策ソリューションの多くは、この中のPCへの侵入を防止する機能を提供しています。これに対してレイヤ4 トラフィック モニタは、Phone Homeと呼ばれる 不正に入手した情報を持ち帰る動きを検知する機能です。Phone Homeは、必ずしも、HTTP（TCP ポート80）を使用するわけではありません。 このため、レイヤ4 トラフィック モニタはすべてのポート番号を使用するトラフィックを監視の対象とし、自動更新されるシグニチャを使用してスキャンを 実行します。PCへの侵入を防止するソリューションと組み合わせることで、階層化された強固なスパイウェア対策を可能にします。



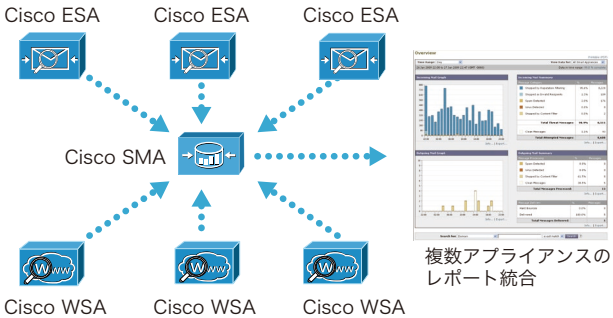
多彩なレポーティング機能

システムの状態を適切に把握することは、継続的かつ安定した運用を行うための重要な要件です。Cisco WSAでは、各クライアントのWebアクセスの利用状況やマルウェア感染状況、アクセスの多いWebサイトの一覧やURLカテゴリなど、様々なレポートの 生成機能を提供しています。これらのレポートは、GUIの操作でリアルタイムに生成できるだけでなく、定期的に生成して管理者にEmailで送付することも可能です。また、レポートの生成に使用した統計情報のエクスポートにも対応しています。



統合管理ソリューション
Cisco Security Management Appliance（SMA）

複数のWSA、ESAを統合管理致します。SMAの冗長化も可能です。



製品仕様

WSAモデル	S680	S380	S170
筐体			
筐体ユニット数	2U	2U	1U
サイズ	89.6mm (h) × 483.7mm (w) × 737.7mm (d)	89.6mm (h) × 483.7mm (w) × 737.7mm (d)	42.4mm (h) × 429.3.0mm (w) × 393.7mm (d)
重量	約29.7kg	約29.7kg	約12.2Kg
CPU	Octa Core Intel	Hexa Core Intel	Dual Core
CPU数	2	1	1
メモリ	32GB	16GB	4GB
電源ユニット	ホットスワップ対応冗長化電源、650W × 2、(90 to 264 VAC)		400W、(90 to 264 VAC)
直流電源オプション	有り		-
リモート パワー サイクル機能	有り		-
ストレージ			
RAIDレベル	RAID 10	RAID 10	RAID1
HDDサイズ	600GB × 8	600GB × 4	250GB × 2
HDDタイプ	ホットスワップ対応SFF型		ホットスワップ対応
ネットワーク インターフェース	4 Gigabit NICs, RJ-45 (10/100/1000, auto-negotiate)		2 Gigabit NICs, RJ-45 (10/100/1000, auto-negotiate)
コンソール インターフェース	1 RJ-45		
動作環境			
起動時対応温度	41 to 104˚ F (5 to 40˚ C)		23˚ F to 104˚ F (-5 to 45˚ C)
非起動時対応温度	-40 to 149˚ F (-40 to 65˚ C)		-
対応湿度 (非結露)	10% ～ 90%		20% ～ 80%

SMAモデル	M680	M380	M170
筐体			
筐体ユニット数	2U	2U	1U
サイズ	89.6mm (h) × 483.7mm (w) × 737.7mm (d)	89.6mm (h) × 483.7mm (w) × 737.7mm (d)	42.4mm (h) × 429.3.0mm (w) × 393.7mm (d)
重量	約29.7kg	約29.7kg	約12.2Kg
CPU	Hexa Core Intel	Hexa Core Intel	Dual Core
CPU数	2	2	1
メモリ	32GB	32GB	4GB
電源ユニット	ホットスワップ対応冗長化電源、650W × 2、(90 to 264 VAC)		400W、(90 to 264 VAC)
直流電源オプション	有り		-
リモート パワー サイクル機能	有り		-
ストレージ			
RAIDレベル	RAID 10	RAID 10	RAID1
HDDサイズ	600GB × 8	600GB × 4	250GB × 2
HDDタイプ	ホットスワップ対応SFF型		ホットスワップ対応
ネットワーク インターフェース	4 Gigabit NICs, RJ-45 (10/100/1000, auto-negotiate)		2 Gigabit NICs, RJ-45 (10/100/1000, auto-negotiate)
コンソール インターフェース	1 RJ-45		
動作環境			
起動時対応温度	41 to 104˚ F (5 to 40˚ C)		23˚ F to 104˚ F (-5 to 45˚ C)
非起動時対応温度	-40 to 149˚ F (-40 to 65˚ C)		-
対応湿度 (非結露)	10% ～ 90%		20% ～ 80%

WSAvモデル	S000v	S100v	S300v
CPU コア	1	2	4
メモリ	4GB	6GB	8GB
ディスク	500GB	250GB	1024GB
RAIDミラーリング	Yes (RAID10)	Yes (RAID10)	Yes (RAID1)
ユーザ数 (参考)	1,000ユーザ以下 検証用	1,000 ～ 4,999ユーザ	5,000 ～ 10,000ユーザ

SMAvモデル	M000v	M100v	M300v	M600v
CPU コア	1	2	4	8
メモリ	4GB	6GB	8GB	8GB
ディスク	250GB	250GB	1024GB	2032GB
ユーザ数 (参考)	1,000 ユーザ以下 検証用	2,000 ユーザ以下	2,000 ～ 10,000 ユーザ	10,000ユーザ以上

商品構成

WSAプラットホーム

Cisco WSA S680/S380/S170
Cisco WSAv* S300v/S100v
* サブスクリプション必須
HWサポート SMARTnet

＋

オプション1：ソフトウェア サブスクリプション

基本バンドル サブスクリプション(ソフトウェア サポート込み)

WSA用ライセンス
- Web Essential バンドル ライセンス
(Web利用制御 + Web評価)
- Anti-Malware バンドル ライセンス
(Web評価 + アンチ マルウェア(Sophos) + アンチ スパイウェア(Webroot))
- Premium Softwareバンドル ライセンス
(Web利用制御 + Web評価 + アンチ マルウェア(Sophos) + アンチ スパイウェア(Webroot))
※1/3/5年選択可能

× ユーザ数

アンチ マルウェア オプション
- アンチ マルウェア(McAfee)
- 高度なマルウェア防御(AMP)
※1/3/5年選択可能

オプション2：SMAプラットフォーム

統合管理サーバ
Cisco SMA M680/M380/M170
Csco SMAv* M600v/M300v/M100v
*サブスクリプション必須
HWサポート SMARTnet

＋

管理サブスクリプション(ソフトウェア サポート込み)

SMA用サブスクリプション
Web Management Softwareバンドル ライセンス
※1/3/5年選択可能

× ユーザ数

Cisco コンテンツ セキュリティ お貸出評価プログラム

Cisco コンテンツ セキュリティ製品を実際にお試しいただけます。
詳しくは弊社営業にお問合せください。

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

お問い合せ

1027-1502-00-PE