

Cisco E メール セキュリティ アプライアンス (ESA)



E メールに関わる脅威を 包括的なソリューションで防御

入口対策

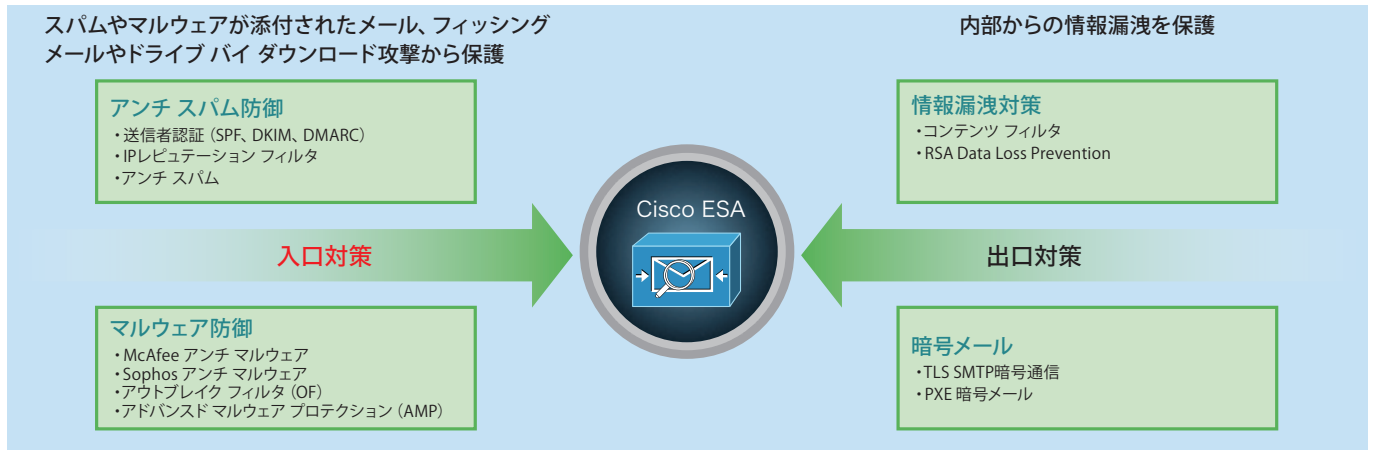
- 送信者認証機能 SPF, DKIM, DMARC
- IP レピュテーションフィルタ
- 業界をリードするアンチ スпам フィルタ
- マルウェア多重スキャン
- メール中の URL リンク脅威に対応
- サンドボックス

出口対策

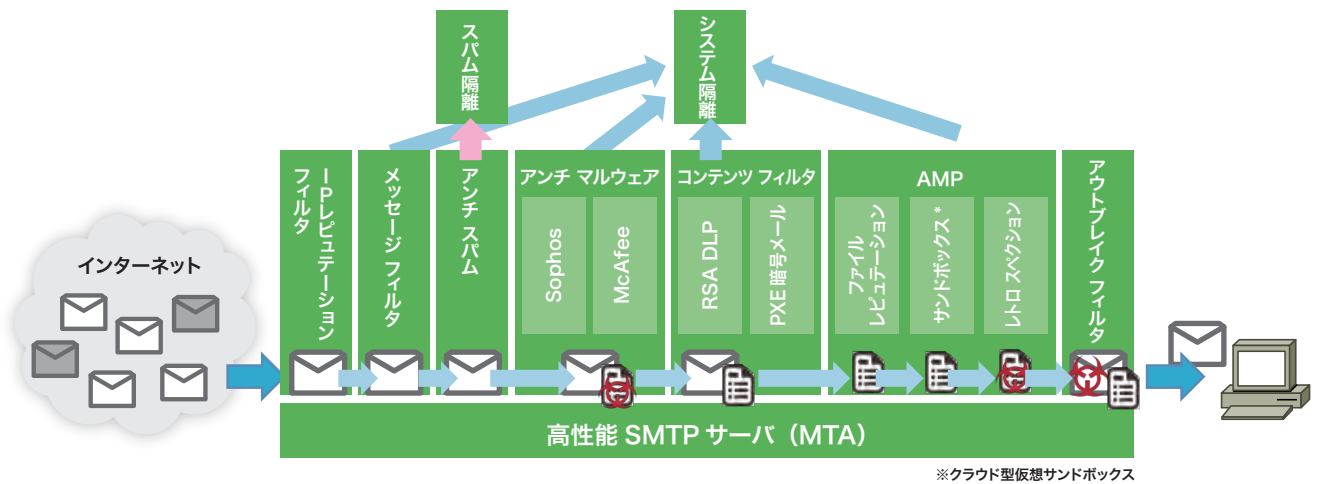
- 情報漏えい対策
- かんたん暗号メール機能

Ciscoのメール セキュリティ ソリューション

メールに関するあらゆるセキュリティ ソリューションをESA1台で提供いたします。



Cisco ESA 内部フロー

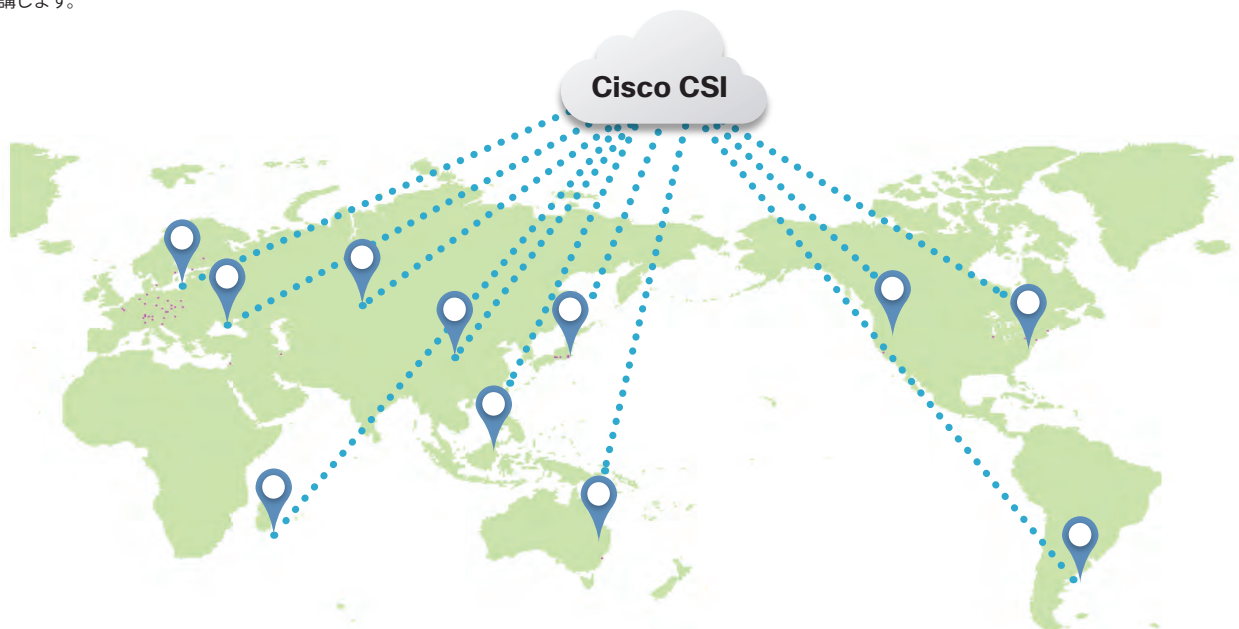


業界最大規模のセキュリティ クラウド

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。

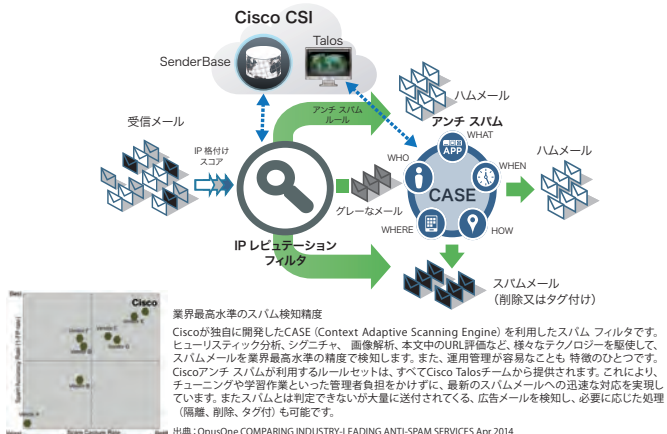
Cisco CSI の特長

- 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



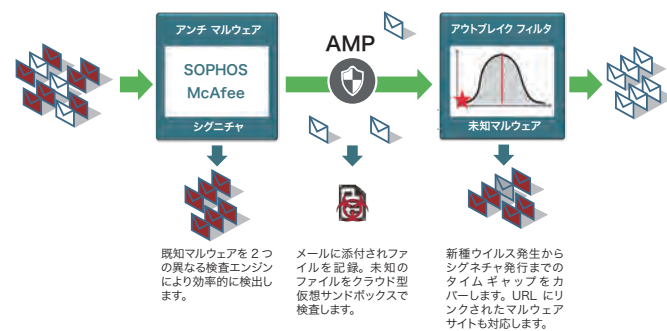
IP レピュテーション フィルタとアンチ スпам

SenderBaseが分析したメール送信元IPアドレスの評価は200段階にスコア付けされ(-10.0から+10.0) ユーザ設置のESAに提供されます。レピュテーション フィルタは、SenderBaseが提供するスコア情報をスパムメールの検知に利用し、排除もしくは受信制御を行う機能です。レピュテーション フィルタはスパムメールをコネクションレベルで排除するため、ネットワークの帯域、システムリソースの浪費を避けるとともに、メッセージング システム全体のセキュリティ レベルを向上させることが可能となります。ESAの多くは、80%を超えるスパムメールをレピュテーション フィルタによって検知しており、その効果を証明しています。



アンチ マルウェア対策

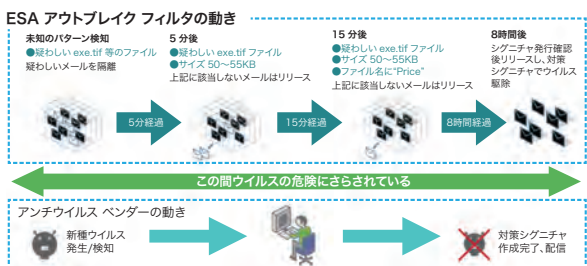
ESAは、ソフォス社とマカフィー社のアンチ ウィルス エンジンを搭載しています。お客様の判断でいずれかのエンジンを選択いただくか、または、両方を有効化してデュアルスキャンを実行することも可能です。アンチ ウィルス機能はESAに完全に統合されており、共通の管理画面から操作、設定を行っていただけます。更に新種マルウェアに対してアウトブレイク フィルタ (OF)、アドバンスド マルウェア プロテクション (AMP) をご利用いただく事でフィッシング メールやURLリンクからのドライブバイダウンロード攻撃、標的型攻撃にも対策を講じる事が出来ます。



アウトブレイク フィルタ (OF) 添付ファイル、Web リンクの両方の脅威に対処

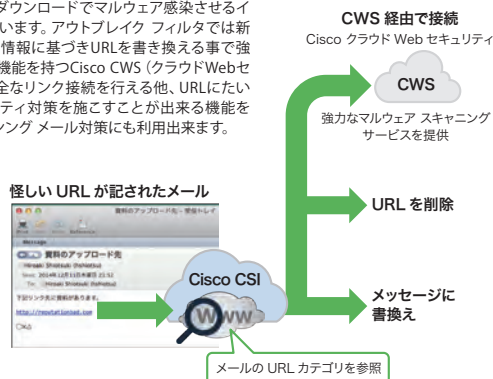
添付ファイル対策

新種マルウェアの発生後、アンチウィルス ベンダーから定義ファイルが提供されるまでの期間に、マルウェアが拡散することを防止するソリューションです。インターネット上を流通するメールを常時監視するCisco CSIが、類似したファイルが添付された電子メールの急増など、新種マルウェアの発生を早期に認識し、該当するメールを識別するルールをESAに提供します。該当するメールはESA内部に隔離され、アンチウィルス ベンダー各社から定義ファイルがリリースされたことを確認した後に開放されます。



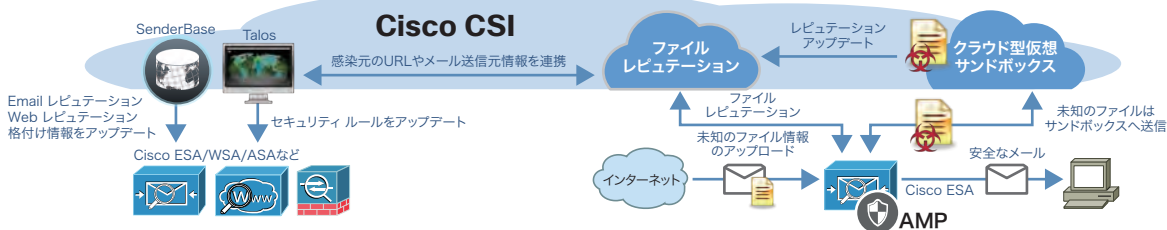
URLリンク対策

従来からあったマルウェアをスパムに添付する運搬手法から、メール本文にマルウェアがアップロードされたURLを記しておきドライブバイダウンロードでマルウェア感染させるインシデントが発生しています。アウトブレイク フィルタでは新たにURLのカテゴリ情報に基づきURLを書き換える事で強力なWebセキュリティ機能を持つCisco CWS (クラウドWebセキュリティ) 経由で安全なリネクトを行える他、URLにたいしても様々なセキュリティ対策を施すことが出来る機能を搭載しました。フィッシング メール対策にも利用出来ます。



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 ESA/WASA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。

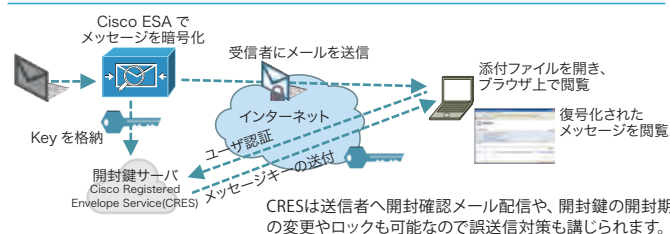
Cisco AMPは、ファイルが添付されたメール受信時に未知の(怪しい)ファイルを発見すると、それらの挙動を解析するCisco CSIクラウド型仮想サンドボックスへ自動的に送信します。解析結果は以後のファイル レピュテーションに反映され、セキュリティ強度を継続的に高めます。

暗号メール

ESAは柔軟な暗号メール機能を搭載可能でビジネスに安全なメールソリューションを提供致します。



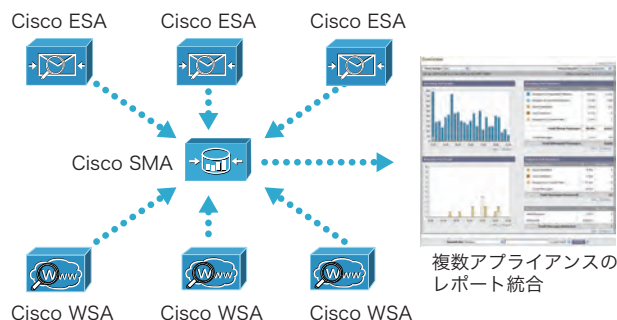
ゲートウェイ~クライアント間暗号メール (PXE)



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

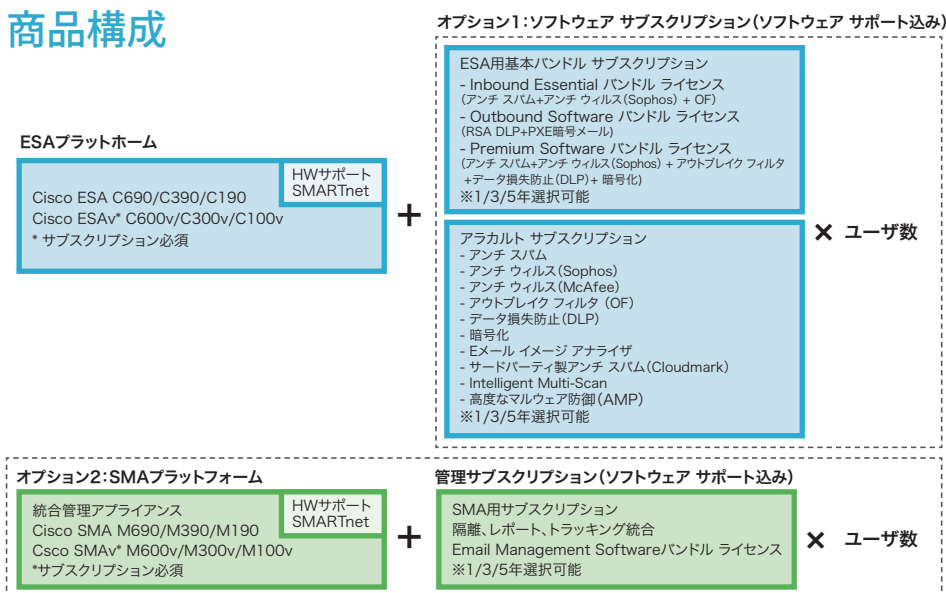
ESAモデル	C690	C390	C190
筐体			
筐体ユニット数	2U	1U	
サイズ	8.6cm (h) × 48.3cm (w) × 73.7cm (d)	4.3cm (h) × 48.3cm (w) × 78.7cm (d)	
重量	約23.6kg	約16.6kg	
CPU	2.4GHz, 6Core		1.9GHz, 6Core
CPU数	2	1	
メモリ	32GB DDR4	16GB DDR4	8GB DDR4
電源ユニット	AC650W × 2 ホットスワップ対応	AC770W × 2 ホットスワップ対応	AC770W × 1 (オプションで追加可能) ホットスワップ対応 (電源追加時のみ)
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 1		
RAIDレベル	RAID 10	RAID 1	
HDDサイズ	600GB SAS 10K rpm × 4	600GB SAS 10K rpm × 2	
HDDタイプ	ホットスワップ対応SFF型		
ネットワーク インターフェース	6 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: 5~35℃		
非起動時対応温度	-40~65℃		
対応湿度 (非結露)	10% ~ 90%		

SMAモデル	M690	M390	M190
筐体			
筐体ユニット数	2U	1U	
サイズ	8.6cm (h) × 48.3cm (w) × 73.7cm (d)	4.3cm (h) × 48.3cm (w) × 78.7cm (d)	
重量	約24.2kg	約17.0kg	約16.6kg
CPU	2.4GHz, 6Core		1.9GHz, 6Core
CPU数	2		1
メモリ	32GB DDR4	16GB DDR4	8GB DDR4
電源ユニット	AC650W × 2 ホットスワップ対応	AC770W × 2 ホットスワップ対応	AC770W × 1 (オプションで追加可能) ホットスワップ対応 (電源追加時のみ)
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 1		
RAIDレベル	RAID 10		RAID 1
HDDサイズ	600GB SAS 10K rpm × 10	600GB SAS 10K rpm × 6	600GB SAS 10K rpm × 2
HDDタイプ	ホットスワップ対応SFF型		
ネットワーク インターフェース	6 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: 5~35℃		
非起動時対応温度	-40~65℃		
対応湿度 (非結露)	10% ~ 90%		

ESAモデル	C000v	C100v	C300v	C600v
CPU コア	1	2	4	8
メモリ	4GB	6GB	8GB	8GB
キャッシュ	10GB	10GB	70GB	70GB
ディスク	200GB	200GB	500GB	500GB
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 ~ 20,000ユーザ	20,000ユーザ以上

SMA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



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。

安全に関するご注意 正しく安全にお使いいただくために、ご使用前に必ず「取扱説明書」をお読みください。



株式会社ソリトンシステムズ <http://www.soliton.co.jp>

〒160-0022 東京都新宿区新宿 2-4-3

TEL 03-5360-3811 netsales@soliton.co.jp

大阪営業所 06-6821-6777 福岡営業所 092-263-0400

名古屋営業所 052-217-9091 東北営業所 022-716-0766

札幌営業所 011-242-6111