



Cisco IronPort Eメールセキュリティアプライアンス

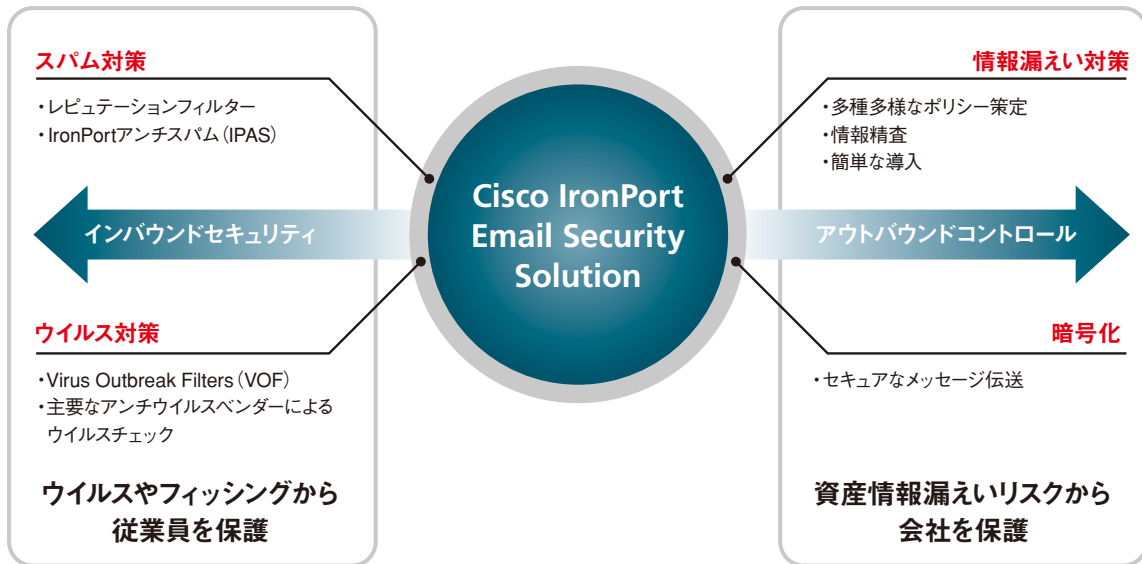


Cisco IronPort Eメールセキュリティアプライアンス
インバウンドセキュリティからアウトバウンドコントロールまで
電子メールに関わる問題に包括的なソリューションを提供

Cisco IronPort Eメールセキュリティアプライアンス

Cisco IronPort Eメールセキュリティアプライアンスは、企業の電子メールに関わるすべての問題に対する包括的なソリューションを提供します。

OVERVIEW



今日、電子メールは企業活動に不可欠なコミュニケーションツールとなると同時に、攻撃者にとって魅力的なターゲットとなり、電子メールに関わる脅威は深刻度を増しています。刻々と進化する脅威に対して、Cisco IronPort Eメールセキュリティアプライアンスは、IronPort Reputation Filters™、IronPort Anti-Spam™、Virus Outbreak Filters™ (VOF: ウイルス拡散防止フィルタ)、コンテンツフィルタ、メール暗号化、情報漏えい対策など、最新のテクノロジーを駆使し、企業の電子メールシステムを保護します。

IronPort SenderBase Network

IronPortが独自に展開するSenderBaseは、世界中の700,000台を越えるISP、大学、企業などからデータをリアルタイムに収集するとともに、200以上の異なるパラメータによってインターネット上にあるメールサーバの挙動を常時監視する、世界初、世界最大規模の電子メール監視サービスです。SenderBaseが収集するデータは、インターネット上で流通する電子メールの実に30%以上を網羅しています。これらの膨大なデータを、各Sender (送信者) ごとに、送信した電子メールの総ボリューム、DNSの設定、既知のスパム送信者やウイルスとの関係など、様々なパラメータを用いて分析することで、メール送信者の送信パターンを高い精度で捉えることが可能となります。SenderBaseの情報を利用することで、Cisco IronPort Eメールセキュリティアプライアンスは、スパムメールへの対応を飛躍的に効率化しています。今日、SenderBaseは一日に500GBを超える脅威データを1000台以上のサーバーで解析処理し、多数のお客様のスパムメール対策に貢献しています。

FEATURES

<スパム対策>

IronPort Reputation Filters™ (レピュテーションフィルタ)

SenderBaseが分析した送信元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Cisco IronPort Eメールセキュリティアプライアンスに提供されます。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。IronPortユーザの多くは、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。

IronPort Anti-Spam™(スパムフィルタ)

IronPortが独自に開発したCASE(Context Adaptive Scanning Engine™)を利用したスパムフィルタです。ヒューリスティック分析、シグニチャ、画像解析、本文中のURL評価など、様々なテクノロジーを駆使して、スパムメールを業界最高水準の精度で検知します。また、運用管理が容易なことも特徴のひとつです。IronPort Anti-Spam™が利用するルールセットは、すべて、IronPort Threat Operations Centerから提供されます。これにより、チューニングや学習作業といった管理者負担をかけずに、最新のスパムメールへの迅速な対応を実現しています。

広告メール対応(マーケティングメッセージ)

IronPortでは、Spamとは判定できないが大量に送付されてくる、広告メールを検知し、必要に応じた処理(隔離、削除、タグ付)を実施可能になりました。

マーケティングメール 設定

マーケティングメール スキャンを有効にする: いいえ はい

メッセージに適用するアクション: **スパム隔離**

件名ヘッダを追加: 前に付加 (Prepend) [MARKETING]

カスタムヘッダを追加(オプション):

代替の受信者に送信(オプション):

メッセージアーカイブ: いいえ はい

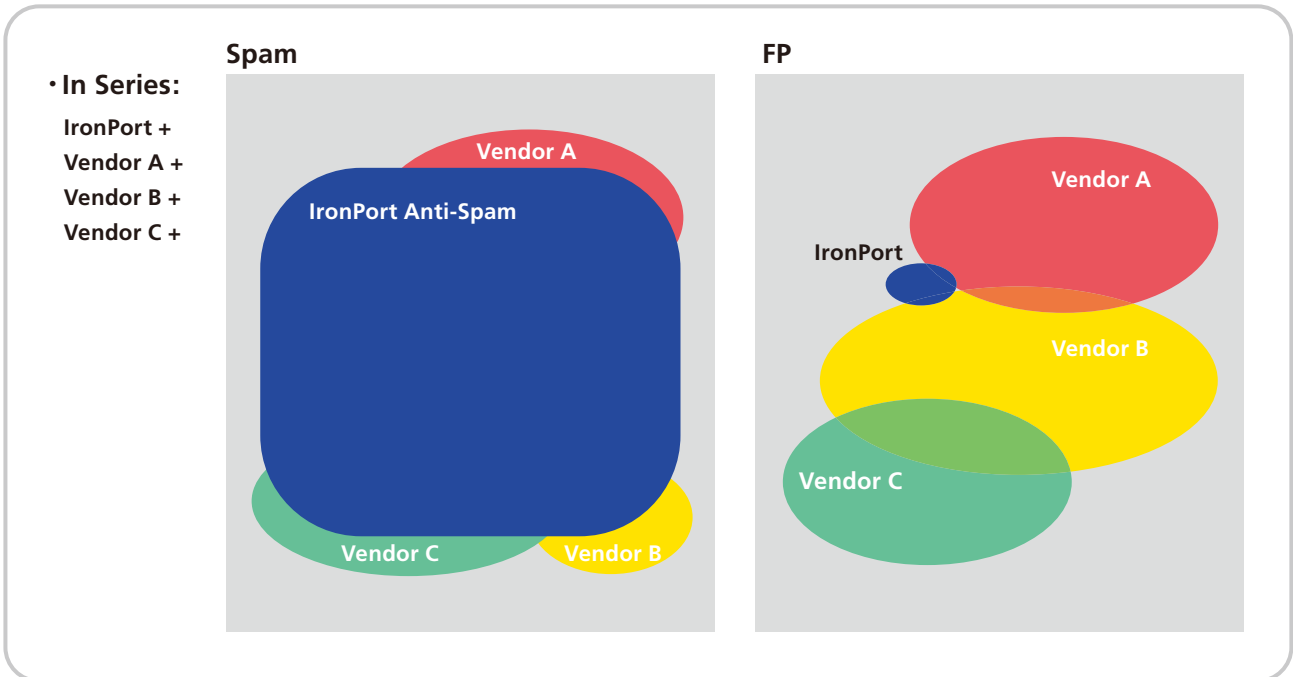
メッセージ カテゴリ	%	メッセージ
レピュテーションによるブロック	91.0%	8,916
無効な受信者としてブロック	7.8%	763
スパム検出	0.5%	53
インテリジェントマルチスキャンが他のスパムを検出しました	0.0%	3
ウイルス検出	0.0%	0
コンテンツフィルタによってブロック	0.0%	0
合計脅威メール:	99.3%	9,735
マーケティングメッセージ	0.0%	2
正常メール	0.6%	63
実行されたメッセージの合計数:		9,800

IronPort スパム隔離

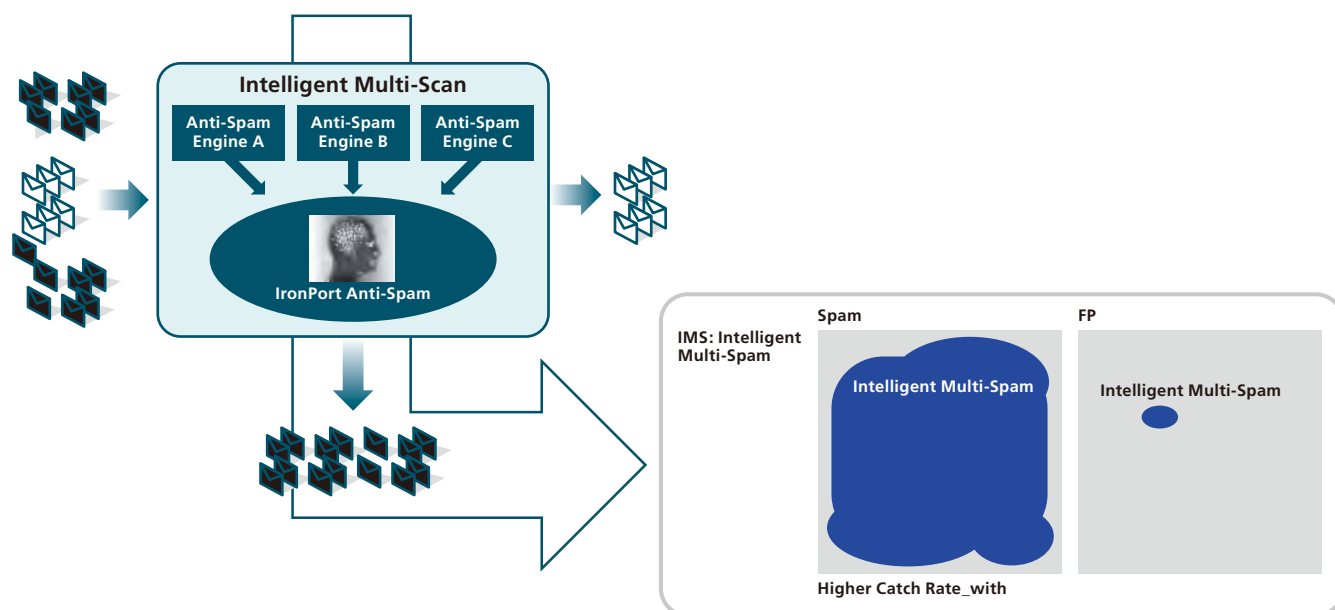
IronPort Anti-Spam™によってスパムメールと判定されたメールに対するアクションには、件名やコンテンツヘッダにタグをつけて送信する、破棄する、専用領域に隔離する、という3つの選択肢を提供しています。隔離を選択する場合の隔離領域は、Cisco IronPort Eメールセキュリティアプライアンス内部に設けるか、Cisco IronPortセキュリティマネージメントアプライアンスを外部隔離領域として設定します。エンドユーザには、隔離したスパムメールのダイジェストメールを一定期間ごとに送付することが可能で、ダイジェストメールに含まれるリンクから、隔離されたメールの内容を確認したり、リリースしたりすることができます。また、隔離メールの閲覧画面では、エンドユーザ個人によるセーフリスト、ブロックリストの設定にも対応しています。

Benefit: Catch Rate . ↑

Tradeoff: FP Rate . ↑



Cisco IronPort Eメールセキュリティプライアンスでは、Spam検知率をさらに高めるためにはIntelligent Multi-Scanを開発しました。一般的に複数Anti Spamを実装すると検知率は向上しますが、全体的な誤検知率も比例して上がってしまうため、複数のエンジンでの分析結果をIronPort Anti-Spam™が統合し、総合的に判断することでより精度の高いスパム検知率、低誤検知率を実現することが可能です。



<ウイルス対策>

Virus Outbreak Filters™(VOF:ウイルス拡散防止フィルタ)

新種のウイルスの発生後、アンチウイルスベンダから定義ファイルが提供されるまでの期間に、ウイルス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SenderBase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、新種のウイルスの発生を早期に認識し、該当するメールを識別するシグニチャをCisco IronPort Eメールセキュリティプライアンスに提供します。シグニチャに該当するメールはCisco IronPort Eメールセキュリティプライアンス内部に隔離され、アンチウイルスベンダ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。

アンチウイルス

Cisco IronPort Eメールセキュリティプライアンスは、ソフォス社とマカフィー社のアンチウイ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。アンチウイルス機能はCisco IronPort Eメールセキュリティプライアンス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。

<メール暗号化>

暗号化機能

IronPort PXE™暗号化技術はIronPort独自のメールの暗号化方式で容易にメールの暗号化を実現します。共通鍵方式を採用することで、送信者、受信者ともに鍵を意識させることなくメールの暗号化、復号化を実施できます。

Key Server(キーサーバ)

IronPort PXE™暗号化技術利用時に必要となるKey Serverは、独自で構築する事も可能ですが、IronPort/Ciscoが提供するASPサービスを利用する事も可能です。ASPサービスは暗号化ライセンスを購入していただくことで利用可能になります。現在、ASPサービスは8ヶ国語に対応しています。

専用のクライアントソフト/アプリケーション不要

クライアント側にアプリケーションソフトをインストールする必要がなく、Webブラウザを用いて暗号化メールの復号化が行えます。暗号化されたコンテンツは、html形式の添付ファイルとして届けられ、受信者はブラウザから開くことで復号化を実施します。

暗号化対象メッセージの識別

件名、ヘッダ、送信元、送信先などの条件を、コンテンツフィルタで組み合わせることにより、組織のポリシーに沿った様々な条件で暗号化の対象となるメールの識別をすることが出来ます。

あらゆるメールクライアントに対応

AOL、Yahoo!、Gmail、HotmailといったWebベースクライアントを始めOutlook、Lotus Notes、GroupWiseといったデスクトップクライアントに至るまでさまざまなメールクライアントをサポートしている事で、あらゆるユーザが暗号化メールを閲覧できます。

TLS(Transport Layer Security)による暗号化機能の提供TLSを採用することで、コンテンツではなくパス自体の暗号化をサポートします。宛先単位で、有効・無効の設定が可能です。

IronPort Encryption Applianceと組み合わせることで、S/MIMEやOpenPGPなど、さらに暗号化機能のサポート範囲が広がります。さまざまな環境に対応できるように、2回目以降のオフラインエンベロープ用鍵のメッセージ有効期限の設定、パスワード無しエンベロープ、開封プログラム添付無しエンベロープ、オフラインエンベロープといった機能拡張を行っている。

<マネージメント機能>

電子メールセキュリティマネージャ

スパム対策やウイルス対策、コンテンツフィルタなど、Cisco IronPort Eメールセキュリティアプライアンスの提供するセキュリティサービスの適用方針を、ポリシーとして、ユーザ単位やグループ単位で制御する機能を提供します。この機能を利用することで、部門や役職ごとに異なるセキュリティサービスの運用をおこなうことが可能になります。ポリシーの分類には、メールアドレスやドメイン名を利用するほか、LDAPサーバと連携することもできます。

集中管理 (クラスタリング)

複数のCisco IronPort Eメールセキュリティアプライアンスを導入されるお客様向けの機能で、Cisco IronPort Eメールセキュリティアプライアンスのクラスタリングを可能にします。クラスターを構成した場合、クラスター中の1台に実施された設定は、クラスターメンバーのアプライアンスに同期されます。複数のCisco IronPort Eメールセキュリティアプライアンスに

ログインして同じ設定を実行する必要がなくなり、管理者負担を軽減し、運用コストの削減に貢献します。

モニター機能

送信メール、受信メールの状況など、10種類以上のレポート生成に対応しています。レポートの生成はGUIから実行できるだけでなく、定期的に生成したレポートを管理者の方にメールで送付することも可能です。また、レポートの生成に使用する統計情報をCSVフォーマットでエクスポートすることもできますので、外部ツールを利用した管理にもご利用いただけます。

メッセージトラッキング

送信メールや受信メールの配送状況確認は、電子メールシステム管理者への問い合わせの中で、最も多いもののひとつだと言われています。Cisco IronPort Eメールセキュリティアプライアンスが提供するメッセージトラッキング機能は、送信者や受信者のメールアドレス、件名、日付および時間の範囲などを指定した検索に対応し、当該メールの処理状況の迅速な確認を可能にしています。

IronProt Cシリーズは日本語を始め、各国の言語に対応したウェブベースのGUIのほか、CLI、SNMPサポートなど、お客様の要望に柔軟に対応するマネージメントツールを提供しています。

■アウトバウンドコントロール

情報漏洩対策

RSA DLP

企業において、今や情報漏洩対策は必須となってきており、送信メッセージを何もせずに送信することが不可な状況にあります。Cisco IronPort EメールセキュリティアプライアンスのAsyncOSに業界No.1 RSAのDLPを搭載既に法令化されているUSのCriteriaを中心に101からなるポリシーを搭載。RSAセキュリティ独自アルゴリズムを用い、0-100点を5段階にレベル分けします(無視・低・中・高クリティカル)。無視できるスコア以外の4つ(低・中・高クリティカル)に分類されたメッセージに対し、隔離、削除、タグ付送信をおこなうことが可能になります。

TLS

一通信の機密を守る

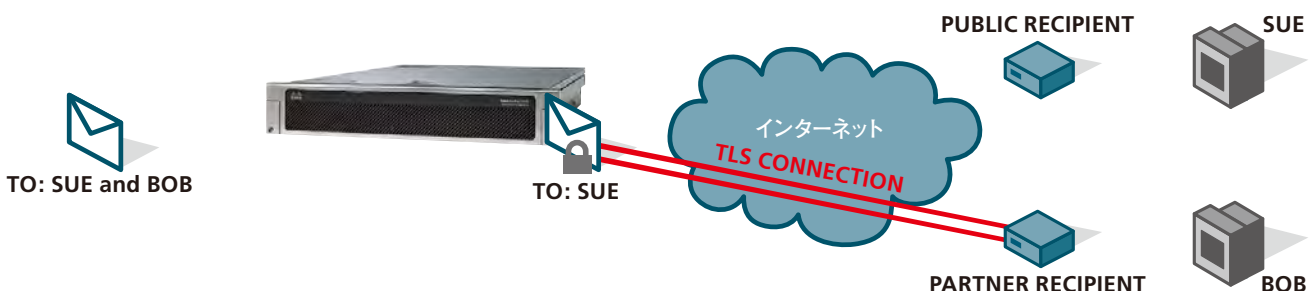
メッセージを暗号化する目的は情報を安全に伝達することです。TLSは情報伝達するパスを安全にするための機能です。Cisco IronPort Eメールセキュリティアプライアンス上での暗号化技術では、コンテンツの暗号化だけではなくパスの暗号化も組み合わせて利用することでより強固な暗号化をご提供いたします。たとえば、下記のように既知の顧客に対しTLS環境が確立されている通信ではコンテンツの暗号化を行う必要ありませんがTLSが確立できない顧客に対してはコンテンツを暗号化するという手法が有効になります。

DLPポリシーマネージャ:DLPポリシーの追加

テンプレートから DLP ポリシーを追加	
表示設定: すべてのカテゴリを展開 ポリシー説明を表示	
Regulatory Compliance	
追加	Payment Card Industry Data Security Standard (PCI-DSS)
追加	PIPEDA (Personal Information Protection and Electronic Documents Act)
追加	FERPA (Family Educational Rights and Privacy Act) <small>カスタマイズをお勧めします。</small>
追加	GLBA (Gramm-Leach Bliley Act) <small>カスタマイズをお勧めします。</small>
追加	HIPAA (Health Insurance Portability and Accountability Act) <small>カスタマイズをお勧めします。</small>
追加	SOX (Sarbanes-Oxley)
US State Regulatory Compliance	
Acceptable Use	
Privacy Protection	
Intellectual Property Protection	
Company Confidential	
Custom Policy	

一TLS拡張機能

- ・ 証明書管理: 信頼できる公開証明書や自己署名証明書の登録を行ったり、自己署名証明書の発行のリクエストが可能です。
- ・ 認証局管理: 信頼できる証明書認証局を登録、管理することが可能
- ・ リスナー毎のTLS設定: 個々のリスナーに対し、個別の証明書を指定することが可能です。また、IPインターフェース、LDAPインターフェース、外部TLSインターフェースそれぞれのHTTPSに対する証明書を割り当てすることも可能です。



Cisco IronPort Eメールセキュリティアプライアンス 仕様

	C160	C370	C670
	中堅、小規模企業向けのエントリーモデル 低価格ながら、上位機種と同等の機能を提供	大企業から中堅企業の幅広い層に対応するモデル 優れたコストパフォーマンスを提供	サービスプロバイダや大企業向けの上位モデル 高度な耐障害性と優れたパフォーマンスを提供
対象ユーザ規模※	～1,000	1,000～5,000	5,000～20,000
筐体プロセッサ			
筐体	19インチラック、1U	19インチラック、2U	19インチラック、2U
サイズ	42.7mm(h) × 480.0mm(w) × 556.1mm(d)	86.4mm(h) × 443.0mm(w) × 680.7mm(d)	86.4mm(h) × 443.0mm(w) × 680.7mm(d)
質量	9.7kg	22.2kg	24.67kg
CPU	Dual Core Intel Pentium × 1	Quad Core Intel Xeon × 1	Quad Core Intel Xeon × 2
メモリ	4GB		
電源	345W、90-264V	ホットスワップ対応な冗長構成 870W、100-240V	ホットスワップ対応な冗長構成 870W、100-240V
ストレージ			
RAID	RAID1	RAID1	RAID10
ドライブ	250GB SATA × 2	ホットスワップ対応300GB SAS × 2	ホットスワップ対応300GB SAS × 4
容量			
キュー	15GB	35GB	70GB
ログ、各種データ、隔離、トラッキング、レポート	210GB	210GB	460GB
(最大スラム隔離領域)	5GB	15GB	30GB
接続			
イーサネット	10/100/1000 Base-T × 2	10/100/1000 Base-T × 4	10/100/1000 Base-T × 4
シリアル	RS-232C(DB9) × 1		
アンチスパム、アンチウイルス			
SenderBaseRとの連携	標準搭載		
送信ドメイン認証(SPF、DKIM、ドメインキー)	標準搭載		
VOF(ウイルス拡散防止フィルター)	オプション もしくは バンドル	オプション もしくは バンドル	オプション
DOS/DHA攻撃防御	標準搭載		
Sophos アンチウイルス	オプション もしくは バンドル	オプション もしくは バンドル	オプション
McAfee アンチウイルス	オプション		
IronPort アンチスパム	オプション もしくは バンドル	オプション もしくは バンドル	オプション
メールスキャン、メッセージアーカイブ	標準搭載		
仮想ゲートウェイ	32		
インターフェイス/設定			
GUI(Webインターフェイス)	HTTPおよびHTTPS		
コマンドライン	SSHおよびTelnet		
プログラム可能な監視機能	XML over HTTP(S)		
設定情報	XMLベースの設定ファイル、Centralized Management機能(オプション)による設定情報の同期		
ログ			
ログ設定	ユーザ設定可能なログサービス、FTPあるいはSCPで外部収集、アップロード/ダウンロード、一定時間毎(固定)/ファイルサイズによるローテート		
外部転送方法	FTP、SCP(アップロード/ダウンロード)、Syslog		
モニタリングと管理			
メールモニタリング	ソースIP、ドメイン、組織名によるメールフローデータベース		
システムモニタリング	SNMP v1/ v2c/v3、MIBII、プライベートMIB		
警告	アプリケーション/キュー/ファイル転送エラーなどのイベント毎のemailによるアラート		
レポート	送受信数、ウイルス検知数、スパム検知数、システム状態などの定期レポート		
メンテナンスのスケジュール	オフライン(配信/インジェクション)の停止、配信一時停止、シャットダウン、再起動		

※使用環境によって対応可能ユーザ数は異なります。

©2010 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2010年8月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。

[開発元]



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

[発売元]



株式会社ソリトンシステムズ

〒160-0022 東京都新宿区新宿2-4-3
Tel. 03-5360-3811 Fax. 03-5360-3880
email: netsales@soliton.co.jp

http://www.soliton.co.jp