



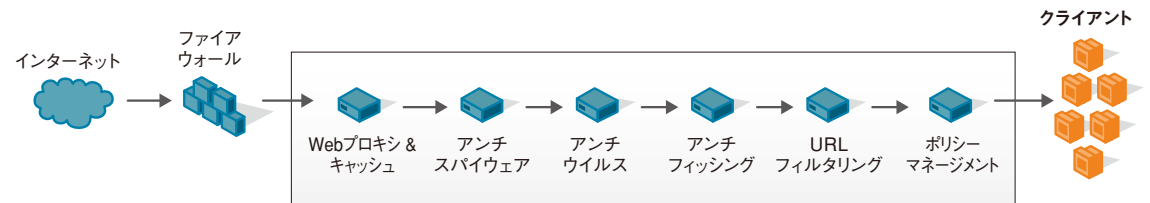
THE INDUSTRY'S BEST
WEB SECURITY GATEWAY.
PROVIDING MALWARE
PROTECTION AND HIGH
PERFORMANCE.

IronPort Sシリーズ Web セキュリティ アプライアンス

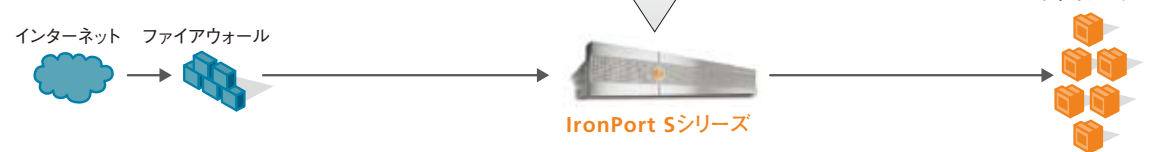
OVERVIEW

IronPort Sシリーズは、ウイルス、スパイウェアなど、Webアクセスを介した脅威からユーザを保護するWebセキュリティゲートウェイです。また、ユーザ認証やアクセス可能なWebサイトの制御機能を提供し、ITガバナンスの強化に貢献します。

<IronPort導入前>

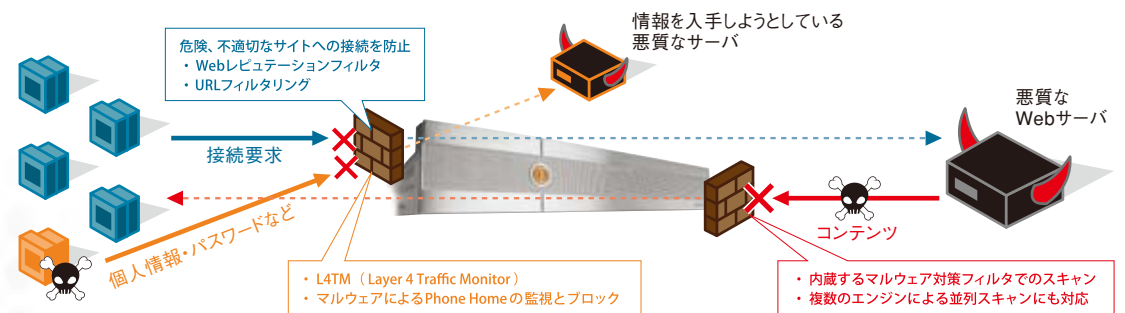


<IronPort導入後>



近年、顧客情報や個人情報など、機密情報の漏洩対策は、企業の最重要課題のひとつになっています。一方で、スパイウェアに代表されるマルウェアは巧妙化を継続しており、Webアクセスを含めたインターネットの利用がビジネスに欠かせないものとなった現代において、深刻な脅威として認識されるようになりました。マルウェアによる情報漏洩のリスクを排除して安全なWebアクセス環境を実現することは、ビジネスの継続と成長のために欠かせない要素となっているのです。また、Webアクセスを包括的に管理、監視することは、ITガバナンスの強化だけでなく、企業の生産性を向上するためにも重要な対策として位置づけられています。業務の遂行に有効なWebサイトは、企業の業態や部門、職種によって異なるほか、企業を取り巻く状況とともに変化しています。こうした環境に適応し、Webアクセスの適正な利用を実現することが求められています。IronPort Sシリーズは、統合型Webセキュリティアプライアンスとして、これらの課題に対して包括的なソリューションを提供しています。

<IronPortのマルウェア対策>



FEATURES IronPort Sシリーズの各種機能

● 高性能Webプロキシ / キャッシュ (Fast Web proxy / cache)

IronPort Sシリーズは、自社開発の高性能なプロキシ/キャッシュエンジンを搭載し、優れたパフォーマンスを実現しています。また、LDAPやActive Directoryと連携することによって多彩なユーザ認証をサポートします。

IP Spoofingや特定サイトをキャッシュ対象から除外するといったカスタマイズにも対応しています。

● L4トラフィックモニタ (Layer 4 Traffic Monitor)

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L4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、L4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。

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

スパムメール対策で絶大な効果を発揮するEmailレピュテーションの技術をWebアクセスに応用したのがWebレピュテーションフィルタです。Webレピュテーションフィルタは、IronPortが運営するレピュテーションサービスであるSenderBaseから提供される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。システム管理者は、このスコア情報を利用して、一定値以下のサイトへのアクセスは遮断、中間スコアのサイトはアンチマルウェア機能で詳細をチェック、高評価のサイトはアンチマルウェアをバイパスするという設定を行えます。システム負荷の大きいアンチマルウェアの処理を軽減することにより、突発的なトラフィック急増の場合にもパフォーマンスへの影響を抑制することが可能となります。

● HTTPS復号化 (HTTPS Decryption)

情報保護へのニーズの高まりから、Webアクセスに占めるHTTPSの割合は増加傾向にあります。しかし、その一方で、HTTPSを使用した通信は暗号化されているため、通信経路上のゲートウェイでのスキャンが行えず、マルウェア感染のリスクを高めているという現象が確認されています。この問題に対処するため、IronPort SシリーズではHTTPS復号化機能を提供しています。HTTPS復号化機能を有効にしたIronPort Sシリーズは、

HTTPS通信の"Man in the Middle"として動作します。アクセス先のサーバとIronPort Sシリーズの間、そしてIronPort Sシリーズとクライアントの間でHTTPSのセッションを確立し、サーバから受信したコンテンツを復号化してスキャンした後にクライアントに送信するのです。HTTPS復号化機能によって、HTTPS通信による情報保護と、ゲートウェイによるコンテンツスキャンの両立が可能となります。

HTTPS 復号化の流れ

スキャンする通信をポリシー (サイトの信頼度、URLフィルタのカテゴリ、各クライアントIP) でコントロール



● URLフィルタリング (IronPort URL Filters™)

2千万を超えるWebサイト、約3億5千万のWebページを登録したデータベースをもとに、アクセス先のURL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、約1万5千のURLが新規に追加されています。デフォルトではURLを52の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。

● アンチマルウェア (IronPort Anti-Malware System™)

IronPort Sシリーズは、アンチマルウェアのシステムとして、Webroot社、McAfee社のエンジンを内蔵しています。Webroot社のエンジンはスパイウェア、アドウェアの検知を専門に行う目的で開発されており、それらのマルウェアを高い精度で検出します。豊富な実績を誇るMcAfee社のアンチマルウェアエンジンは、ウイルスやワームを始めと

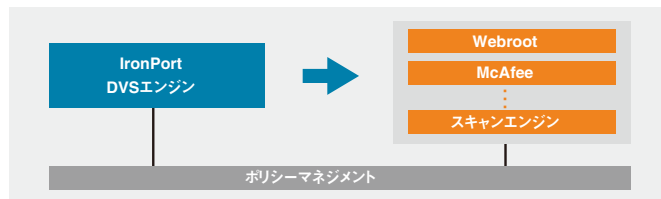
した各種マルウェアに総合的に対応しており、品質の高いスキャンを実現しています。これら二つのアンチマルウェアシステムはオプションとなっており、両方、もしくはどちらか一方を選択してご使用いただけます。IronPort Sシリーズが搭載するDVSエンジンは、両方のエンジンを使用した場合にも、低遅延で品質の高い通信を実現しています。

BENEFITS IronPort Sシリーズの特徴

●セキュリティと通信品質の両立

今日、HTTPは伝統的なWebアクセス以外にも様々な用途で使用されており、動画配信など、高度なリアルタイム性を必要とするアプリケーションも増えてきています。一方で、安全性の向上やITガバナンス強化のため、HTTPを介して通信されるコンテンツのスクランへの要望が高まり、多重のスクランによる遅延の増大など、通信品質の低下が発生しています。IronPort Sシリーズでは、コンテンツの詳細なスクランと高品質な通信を可能にするDVS (Dynamic Vectoring and Streaming™) エンジンを搭載しています。DVSエンジンは、Webroot社およびMcAfee社のアンチマルウェアエンジンや、標準機能として提供されるポリシーフィルタなど、コンテンツのスクランを実行するエンジンを統合的に制御する内部プロセスを実現しています。スクランの対象となるコンテンツのパーズやベクタリングはDVSエンジンが一元的に行い、個々のエンジンが重複して

行うことによるオーバーヘッドを解消します。コンテンツのスクランは、DVSエンジンの制御下にある複数のエンジンで並列処理を実施することで、遅延の最小化を実現し、更に、スクランの結果はDVSエンジンが管理するキャッシュに保管され、類似したコンテンツをスクランする際の高速処理を可能にしているのです。



●容易かつ綿密に設定可能なポリシー設定

HTTP/HTTPSは、インターネット上で最も多く使用されているプロトコルです。その安全かつ適正な利用を実現することは、企業の生産性を向上させ、ITガバナンスの強化に貢献します。しかし、過度なセキュリティの強化はネットワークの使い勝手を悪化させ、システム運用の硬直化はビジネスの機会を損失する危険をも有しています。IronPort Sシリーズのポリシー管理は、日々変化するビジネス環境に迅速かつ柔軟に適用

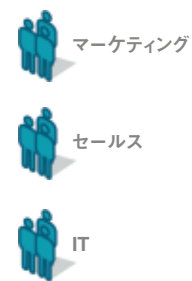
することができるように、使いやすさときめ細かさを両立した設計になっています。LDAPやActive Directoryといった外部ディレクトリや接続元のネットワークによってユーザをグループ化し、グループ単位で、許可するプロトコルやアプリケーション、接続先のWebサイトなどを簡単に設定することができます。

Webアクセスポリシー

グループ	アプリケーション	許可/拒否	カテゴリ	Webサイト/URL
1. marketing	FTP, HTTP, HTTPS	許可	Media	www.yahoo.co.jp
2. sales	FTP, HTTP, HTTPS	許可	Marketing	www.yahoo.co.jp
3. engineering	FTP, HTTP, HTTPS	許可	Marketing	www.yahoo.co.jp

グループ化 (LDAP, Active Directory, 各クライアントIP)

- 拒否：FTP通信
 - 許可：メディア関連のファイル
 - 許可：すべてのURLフィルタリングカテゴリ
- 拒否：実行形式ファイル
 - 拒否：ギャンブルサイト
 - 拒否：マルウェア
- 許可：スカイプ
 - 許可：すべてのトラフィックのモニタリング
 - 許可：実行形式ファイル
 - 許可：すべてのアプリケーション使用
 - 許可：すべてのプロトコル



●豊富なレポート生成機能

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。IronPort Sシリーズでは、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。



	IronPort S160	IronPort S360	IronPort S660
対象ユーザ規模*	～1,000	1,000～10,000	10,000～30,000
※ 使用環境によって対応可能ユーザ数は異なります。			
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	
サイズ	42.7mm(h) x 480mm(w) x 556.1mm(d)	86.4mm(h) x 482.6mm(w) x 744.3mm(d)	
CPU	Dual Core Intel Pentium x 1	Quad Core Intel Xeon x 1	Quad Core Intel Xeon x 2
メモリ	4GB	4GB	8GB
電源	345W、90-264V	ホットスワップ対応な冗長構成、750W、100-240V	
LCD	電源/ネットワーク/HD	エラーメッセージの表示やシステム状態により色調変更する正面実装LCDディスプレイ	
ストレージ			
RAID	RAID1	RAID10、バッテリー装備キャッシュ付 デュアルチャネル構成	
ドライブ	250GB SATA x 2	ホットスワップ対応300GB SAS x 4	ホットスワップ対応300GB SAS x 6
キャッシュ容量	50GB	100GB	200GB
接続			
イーサネット	10/100/1000 Base-T x 6		
シリアル	RS-232C(DB9)×1		
プロキシ/キャッシュ処理			
対応プロトコル	HTTPおよびHTTPS (FTP over HTTPを含む)		
DNS	ローカルおよびインターネット上のDNSサーバを参照可能		
認証	LDAP、NTLM Basic、NTLMSSP		
マルウェア対策、セキュリティ機能			
Web レビュー機能	オプションもしくはバンドル		
McAfeeアンチマルウェア	オプションもしくはバンドル		
Webrootアンチマルウェア	オプションもしくはバンドル		
URLフィルタリング	オプションもしくはバンドル		
HTTPS復号化	標準搭載		
Webアクセスポリシー	標準搭載		
L4トラフィックモニター	標準搭載		
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、ウィザードベースのコマンドライン入力		
ファイル転送	SCPおよびFTP		
設定ファイル	XMLベースの設定ファイル		
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)		
モニタリングと管理			
Webトラフィックモニタリング	クライアントIP、接続先サイトによるWebトラフィックデータベース		
システムモニタリング	SNMP v1/v2c/v3		
警告	アプリケーション/ファイル転送エラー/システム障害などのイベント毎のemailによるアラート		
レポート	クライアントアクティビティ、マルウェア検知数、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	シャットダウン、再起動		



アイアンポートシステムズ株式会社

<アイアンポートシステムズはシスコシステムズの一事業部門です>

〒107-0052 東京都港区赤坂2-10-12フォーシーズンズ溜池山王ビル8F
TEL 03-5573-8160 FAX 03-5573-8159

email: jp-info@ironport.com

www.ironport.com/jp

Copyright © 2000-2008 Cisco Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of Cisco Systems, Inc. All other trademarks are the property of Cisco Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, Cisco does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice. P/N 435-0120-1J 10/08

IronPort, IronPort logo, SenderBase, IronPort製品名はCisco Systems, Inc.の登録商標です。本カタログに記載されている他の会社名、製品名はそれぞれ各社の商標または登録商標です。

*本カタログ記載の内容は、予告なしに変更する場合があります。

IronPort is now
part of Cisco.

