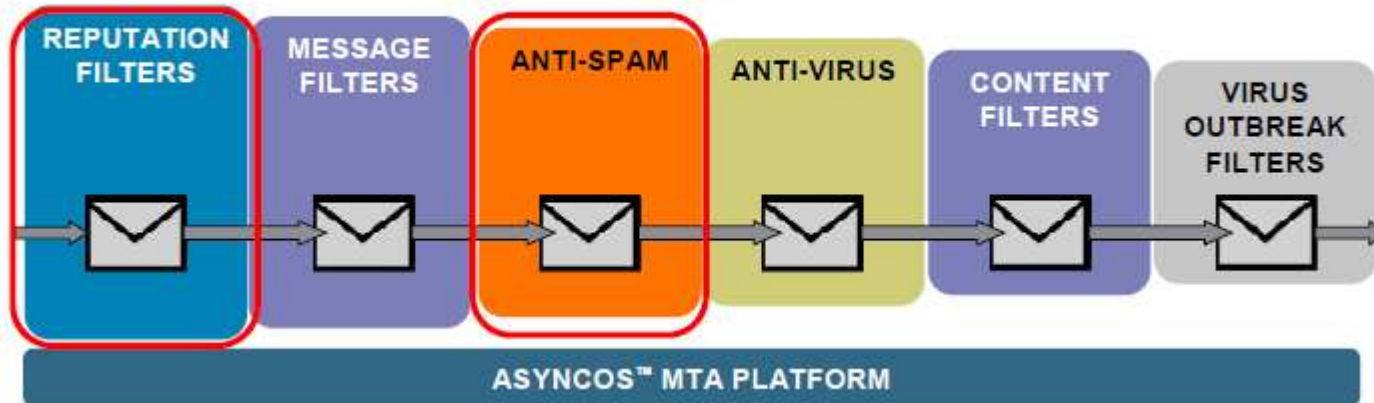


IronportにおけるSPAM対策の仕組み

2009年7月17日

株式会社ネットワークバリューコンポネンツ

アンチスパム機能の概要

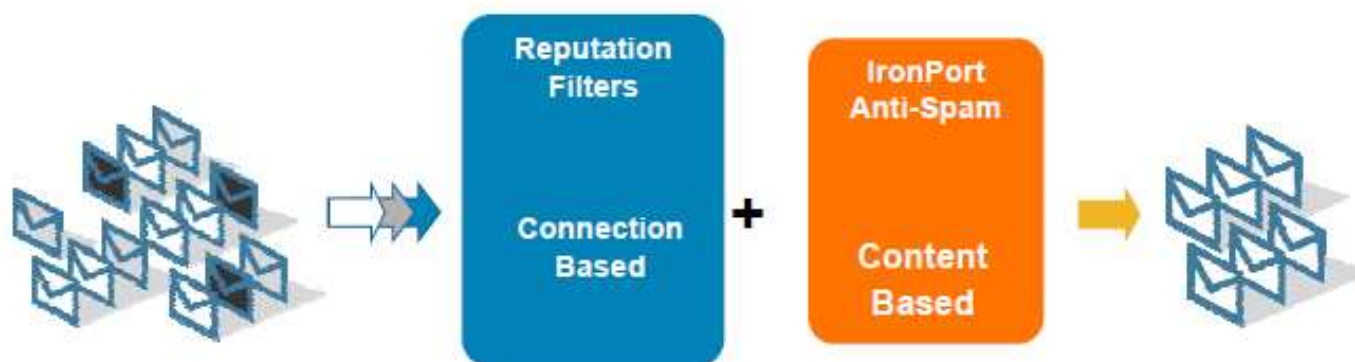


- レピュテーションフィルタは、スパムメールの受信をおこなわないようにします
 - メール送信者のクレジットレートサービス(預託)に似ています
 - 120,000を超えるISP, 企業やその他の組織に協力いただいている情報を使用しています
 - 極めて高いパフォーマンスを実現するスクリーニング機能です
- **アンチスパム**機能は、自動、もしくは隔離モードで動作します
 - 自動 – スпам判定したメールは、破棄、もしくはタグをつけて配送します
 - 隔離 – スпам判定したメールは隔離エリアに保管します
- スпам判定の閾値の設定
 - 閾値にもとづいて、スパムメールの判定を実施します(デフォルト値推奨)
 - 確実なスパム(ポジティブスパム)とスパムらしいメール(サスペクトスパム)それぞれに処理を適用できます

スパム防御の概要

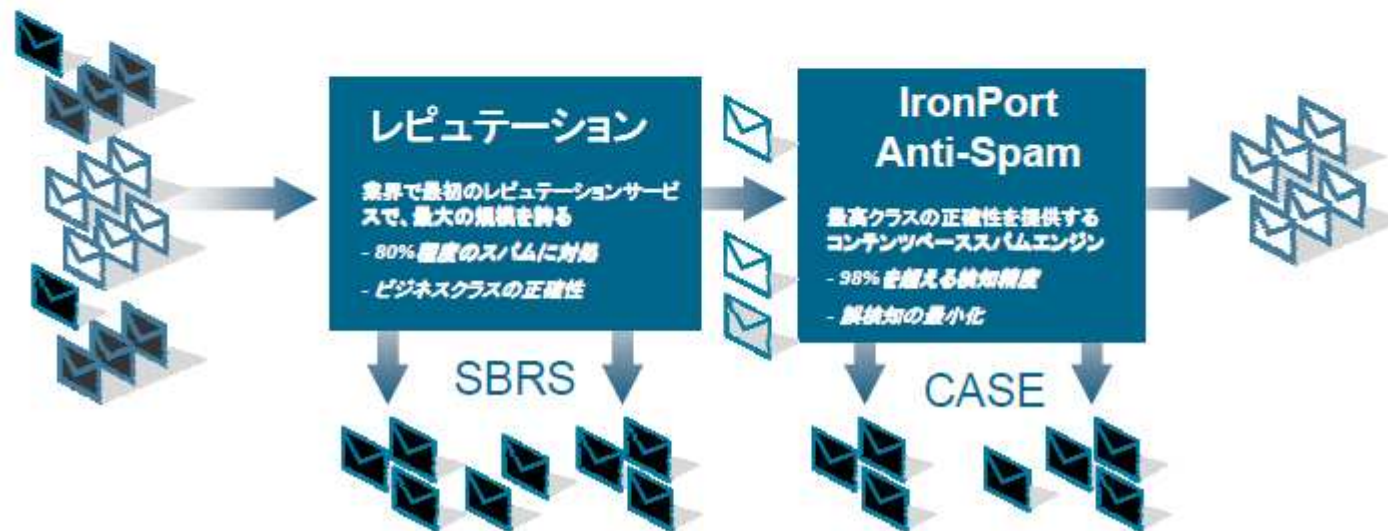
IronPort ESAのスパム対策は、ふたつの階層で構成されます:

- レピュテーションフィルタ (コネクションベース)
- IronPort Anti-Spam (コンテンツベース)

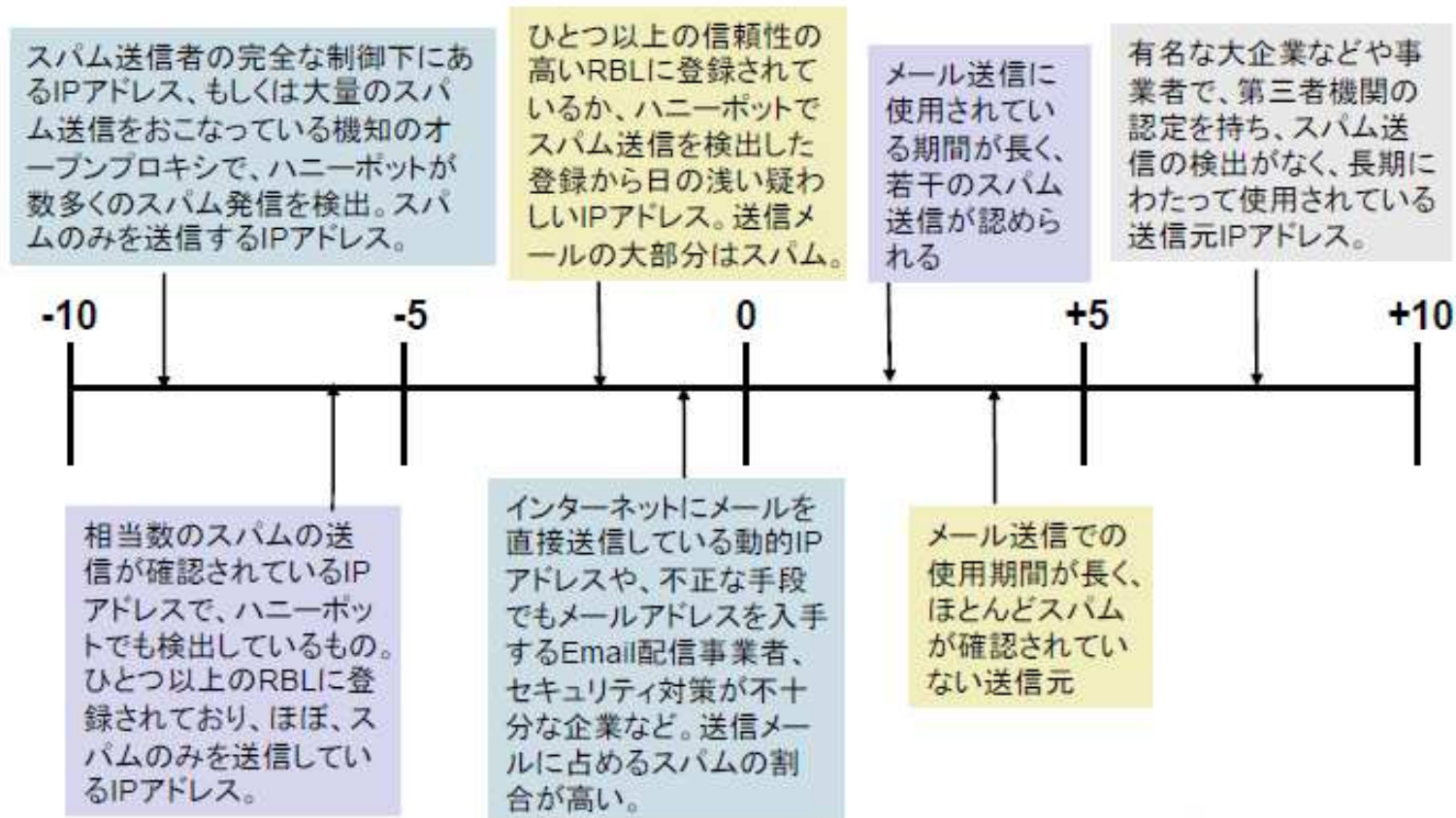


IronPort ESAのスパム対策

- 多階層 / 複数の技術を使用したスパム防御:
 - 新種のスパムにも迅速に対応
 - 正確性の向上



SBRS (SenderBase Reputation Score)



推奨構成

- HATにおけるSBRSにもとづいた送信者グループ振り分け
 - 積極的な設定では、誤検知の可能性もあり

送信者グループ	Blacklist	Suspectlist	Unknownlist	Whitelist
保守的	-10 to -7	-7 to -2	-2 to 7	7 to 10
推奨	-10 to -4	-4 to -1	-1 to 6	6 to 10
積極的	-10 to -2	-2 to -0.5	-0.4 to 4	4 to 10

実際の設定画面

IRONPORT C350

モニター | メールポリシー | セキュリティサービス | ネットワーク | システム管理

HAT 概要

送信者を検索

このテキストを含む送信者を検索

送信者グループ設定 (リスナー: IncomingMail ())

順番	送信者グループ	SenderBase™ レビュー ショウ スコア [?]											メールフローポリシー	削除
		-10	-8	-6	-4	-2	0	2	4	6	8	+10		
1	BLACKLIST	[Progress bar from -10 to -4]											BLOCKED	<input type="button" value="削除"/>
2	SUSPECTLIST	[Progress bar from -4 to 0]											THROTTLED	<input type="button" value="削除"/>
3	UNKNOWNLIST	[Progress bar from 0 to 4]											ACCEPTED	<input type="button" value="削除"/>
4	WHITELIST	[Progress bar from 4 to 8]											TRUSTED	<input type="button" value="削除"/>
	ALL												ACCEPTED	

キー:

Copyright © 2003-2008 IronPort Systems, Inc. All rights reserved.

IronPort Anti-Spam

複数の技術を駆使して、スパムメールを正確に判定

