フォーティネットの
アンチスパムソリューション
～ FortiMail v2.0 ～

Sep/2005

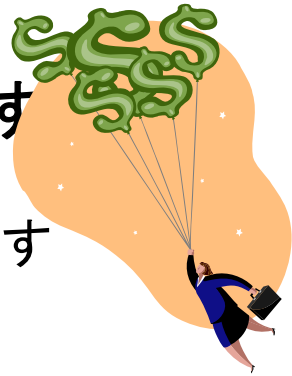
スパムによる損害！

- **生産性の低下！**
  - ・従業員はスパムメールを読んで削除するのに時間を要します
  - ・スパムによる混雑により長い応答時間を要します
- **必要なリソースの消費！**
  - スパムがシステム資源を浪費します
  - ディスク容量、ネットワーク帯域、スループット
- **スパムは多くの帯域を消費する！**
  - ・影響の大きいビジネスアプリケーション（VoIP，TV会議）
- **悪意あるコンテンツの流通手法に**
  - ・ウイルス、ワーム、トロイの木馬、スパイウェア、フィッシング
- **メールのアドレス帳はスパムに乗っ取られます！**

スパムはもはや単に迷惑なメールではありません。金銭的な目的のスパムもあり、危険性は深刻なものになってきています。

成長とスパムのコスト

- **企業電子メールでの“60-70%はスパムです！**
  - 2003-2004にかけ300%成長をとげています
  （ Source:Gartner ）
- **スパムによる悪影響！**
  - 失われた生産性は従業員１人あたり年間約24万円($2,000)と推測されます
  (Source:Nucleus Research)
- **スパムによるトラフィックは増え続けています**
  - 17,000億のスパムが毎日送られています
  - 2007年までには23,000億にまで増えると予想されます
  (Source:IDC)
- **悪意ある目的！**
  - 最高30%のスパムメッセージは、何らかのウイルスまたはスパイウェアを含んでいます
  - 攻撃は単なるいたずらから経済損失まで発展しています



代表的なスパムの発見方法

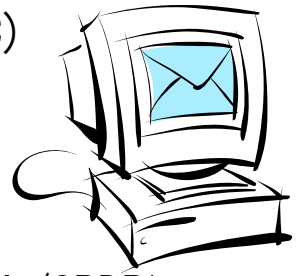
コンテンツレベルでの検出

・ブラックリスト、ホワイトリスト及びキーワードによる発見

・ベイジアン統計

- 迷惑メールの単語のパターン統計による学習型の検出

・ディストリビュート・チェックサム・クリアリングハウス(DCC)

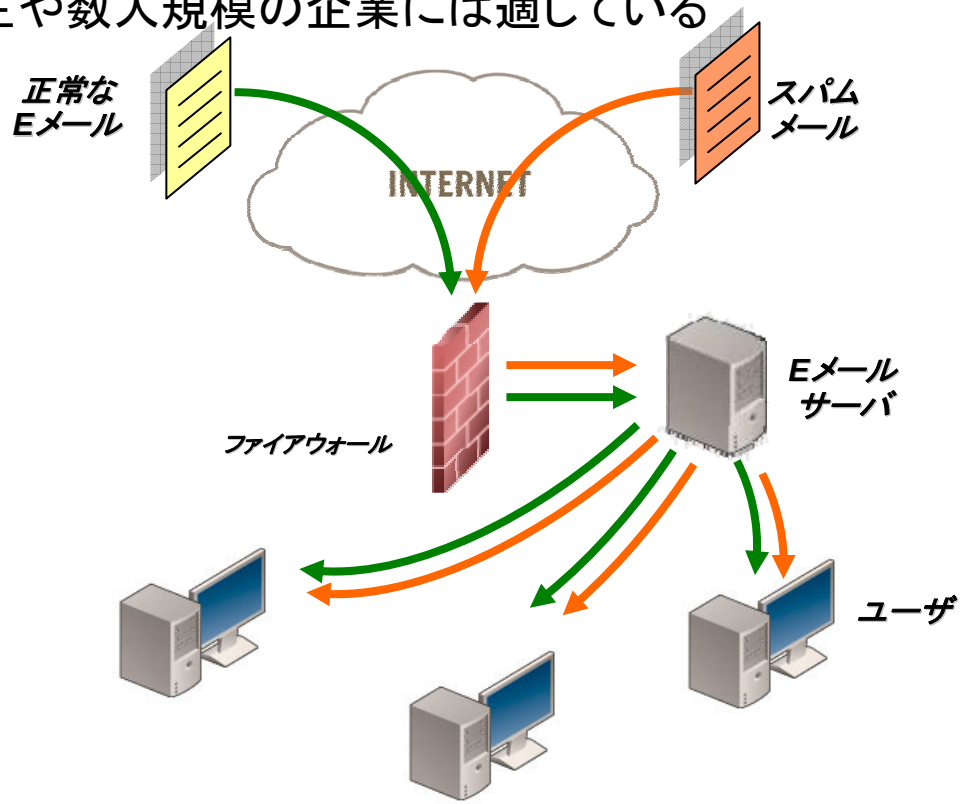


コネクションレベルでの検出

- ネットワークレベルでの検出
- ブラック/ホワイトリスト、DNS逆引き
- リアルタイムBlack hole Lists/Openリレーデータベース（RBL/ORDB）
- 送信元確認
  - 送信元のアドレスまたはドメインを確認するよう要求します
- グレイリスト
  - スパムでなかった場合は再送で受信許可
- SPAM調査
  - ダイナミックな最新アップデートの為のギャザースパマー情報

クライアントベースのアンチスパムソリューション

- アンチスパムソフトウェアをクライアントにインストール
- ユーザーによるスパムの分類設定が可能
- 精度が低い、インストールの手間が膨大、メンテナンスの工数が大きい
- 多くのリソース、帯域を必要とします（Memory , Storage , CPU）
- 個人事業主や数人規模の企業には適している



Eメールサーバベースのアンチスパムソリューション

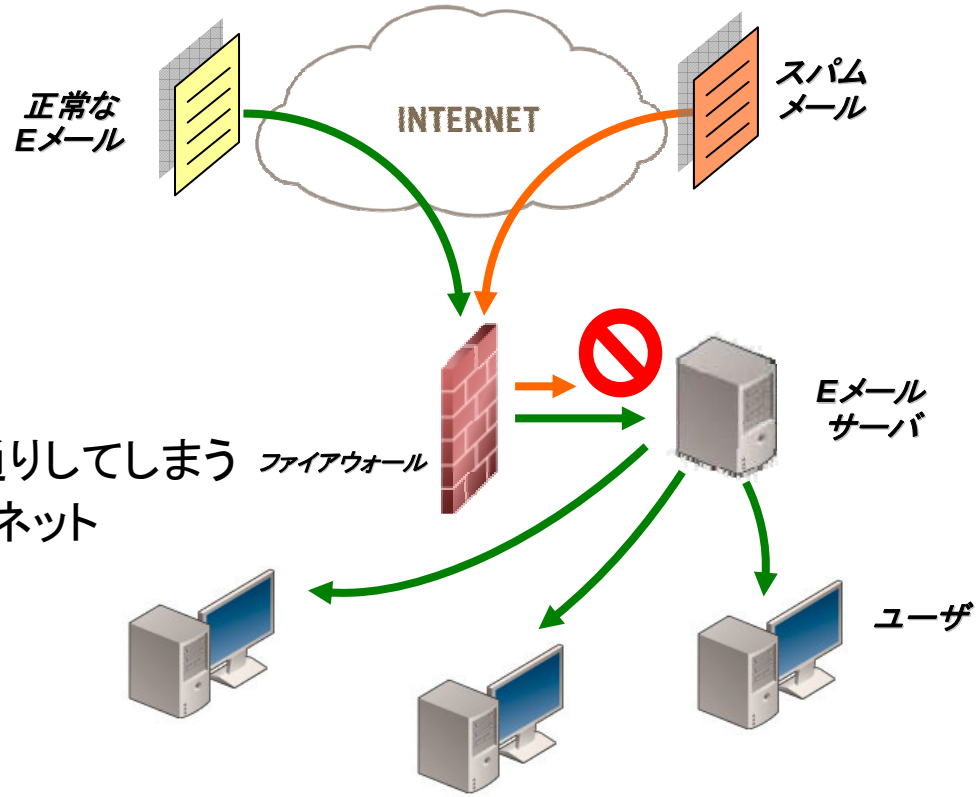
- メールサーバで動作させることにより、メール受け取り時に検査が可能
- メールサーバで高いCPU性能が必要
- 一般的なコンテンツ検出の手法が使用される

メリット:

•スパムはクライアントに送信されません
•トラフィックを無駄遣いしない
•クライアントにソフトをインストールしない

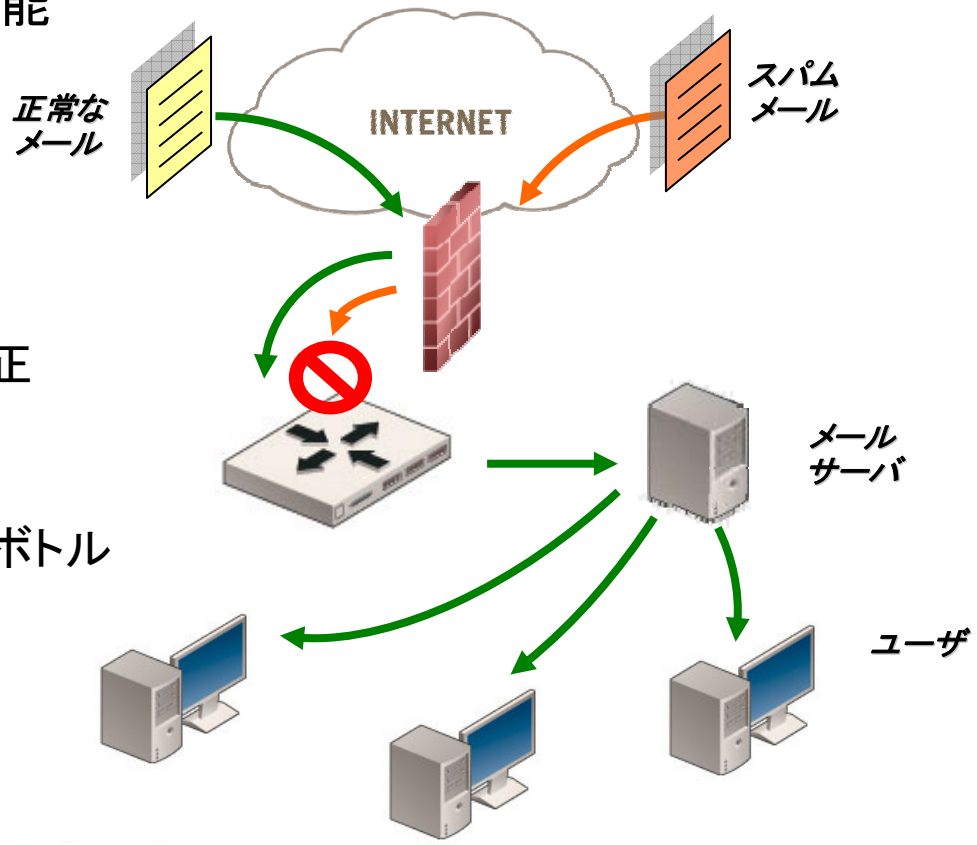
デメリット:

•スパムの大半を占めるWebリンクは素通りしてしまう
•メールサーバでは受け取ってしまうためネットワークベースの検出はできない



ゲートウェイでのアンチスパムソリューション

・インターネットゲートウェイに設置されたメールサーバプロキシィとして動作
・スパムはインターネット接続口で止められ、正常なEメールのみを通過させる
・アンチウイルスも統合可能
・全てのスパム対策手法が利用可能



メリット:
•スパムトラフィックを防ぐ
•メールサーバのリソースをセーブします
•シンプルな設置:DNS&MXレコードの修正

デメリット:
•適正のアンチスパム装置を設置しないとボトルネックになる可能性がある
•他のソリューションより高額な場合がある

MSSPベースのアンチスパムソリューション

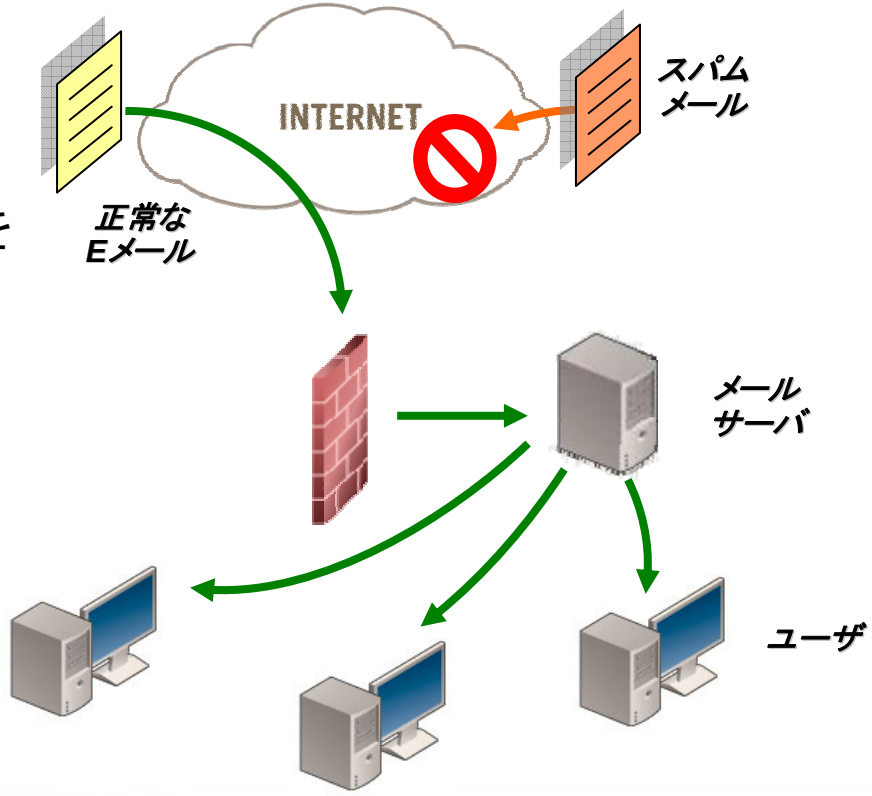
- アンチスパムはサービスとして提供される
- スパムはMSSPで除去されるのでまったく受け取ることがない
- DNSにシンプルな変更を加えるのみ
- 全てのスパム対策手法が利用可能

メリット:

- 高可用性、耐障害性に優れる
- トラフィックの浪費を防ぐ
- 複数のメールサーバとインターネット接続をサポート
- ネットワーク管理者の工数が最小限

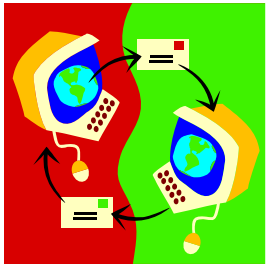
デメリット:

- 適正なチューニングがされるのが遅い
- ユーザ毎の設定に限界がある
- 自社導入に比べスパムの検出率が低い場合が多い
- サービス料がかかる



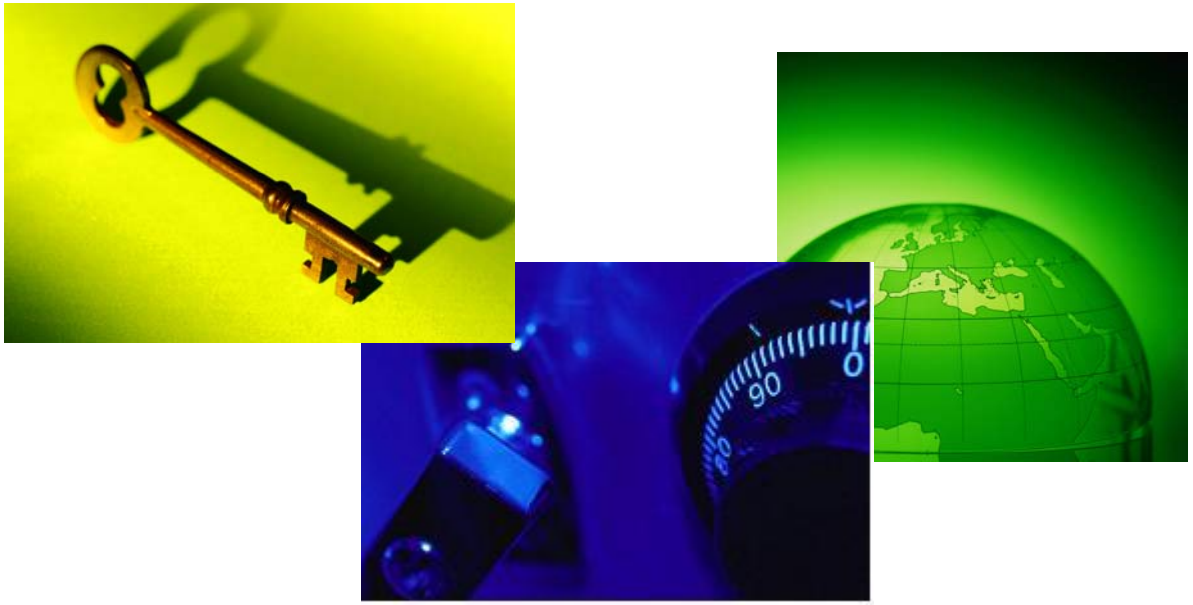
FortiMailによるアンチスパムの有効性

- MSSPとゲートウェイによるアンチスパム
  - 最も良い検出結果が得られる
  - クライアントやネットワーク内部に届く前に防ぐことが可能
- クライアントでアンチスパムを行わないことによりコストの削減
  - HDD容量、トラフィック、CPUの負荷がかからない
  - 管理者や管理工数、各ユーザでの設定の負荷を減らす
- 複合的なアプローチ
  - 複合的なメールフィルタリングの仕組みにより高い検出結果が得られる
  - エッジでのスパムフィルターにより明らかにスパムであるメールを除去
  - きめ細かいクライアント毎の設定が可能
- インターネット接続口とメールサーバの間に設置することにより、より良いコントロールと検知が可能
- FortiMail はゲートウェイ、サーバベース、MSSPの全てに設置可能です



FortiMail セキュア・メッセージ・プラットフォーム

～フォーティネットのEメールに特化した最新セキュア・プラットフォーム～



FortiMail アンチスパムソリューション

- **Hardened アンチスパムセキュリティプラットフォーム**
  - hardened OSによる専用アプライアンス
  - 脆弱性が発見されていなく、アタック成功例もない
- **2つのモデル**
  - FortiMail 400 (中規模向け)
  - FortiMail 2000 (大規模向け)
- **3つの設置モード**
  - トランスペアレント(透過型)モード, ゲートウェイモード, サーバモード
- **FortiGateシリーズとほぼ同じWebコンソール**
- **高い検知率を誇る複合型コンテンツベースとネットワークベースの検出技術**

FortiMail-400

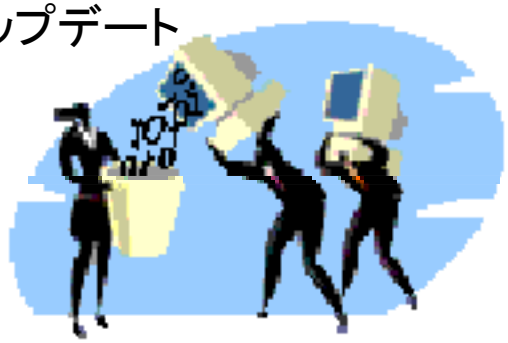
FortiMail-400

- 仕様
  - 1U 19インチ
  - 2 x Tri-Speed ギガポート
  - 4 x 10/100 イーサネットポート
  - 120GB HDD (RAID 0/1)

- ターゲット: 中規模から大規模法人、支社や支店
- 目安はメールアカウント2000以内
- パフォーマンス (1-3KBのメールで計測)
  - 7万通/1h　　168万通/日 (アンチスパム)
  - 14万通/1h　　336万通/日 (アンチウイルス)
  - 13万通/1h　　312万通/日 (ログlogging)
  - 8.5万通/1h　　204万通/日 (アーカイブarchiving)
  - 5.4万通/1h　　130万通/日 (全機能オン)

洗練されたスパム機能

- ウイルスとスパイウェアに対応した検索エンジン
  - FortiGuard Distribution Server(FDS)により自動アップデート
- Eメールを完全にスキャン
  - ヘッダ、本文、URI、メタ情報、他
- 先進的なスパム検知とフィルタリング手法:
  - アクセス・ポリシー・フィルタリング
  - コンテンツフィルタリング
  - Global and User ブラックリスト/ホワイトリストによるフィルタリング
  - リアルタイム・ブラックホール・リスト(RBL) フィルタリング
  - スパム URI RBL (SURBL)
  - FortiGuard アンチスパム (ブラックリスト & URI) フィルタリング
  - ユーザー毎のベイジアンフィルタリング
  - ヒューリスティックフィルタリング (900+ ルール)
  - ディストリビュート・チェックサム・クリアリングハウス (DCC)
- 世界中で行われるベイジアン学習DBをいち早く使用可能



先進的なアンチウイルスとDosプロテクション

- **アンチウイルス**
- SMTPをウイルススキャン
- 圧縮ファイルとNested Archive
- 感染ファイルを隔離
- Replacement Message notification
- ファイルサイズによるブロック
- 添付ファイルをフィルタリング

- **DoS攻撃(Denial-of-Service)**
- Denial of Service (メール爆弾)
- Recipient Address Attack
- Eメール制限 Rate Limiting
  - 送信者毎の受信数を制限
  - 送信者毎のSMTP同時セッションを制限
  - 除外リスト
- 送信者をDNS逆引きチェック (なりすまし防止)

自由度の高い設置方法　3モードを用意

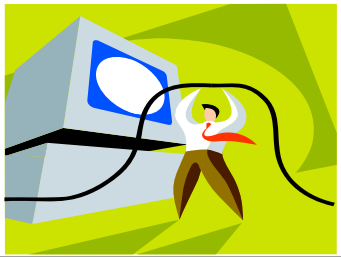
- **トランスペアレント(透過型)モード**
  - 既存のネットワークに一切の変更を加えずに設置可能。FortiMailは既存のメールサーバの手前に設置されます。

- **ゲートウェイモード**
  - 既存メールサーバのMTAプロキシとして動作。FortiMailでスキャンするためメールをFortiMailに転送するようDNSとMXレコードを設定。

- **サーバーモード**
  - アンチウイルスとアンチスパム機能を合わせ持ったメールサーバとして動作。中規模までの法人や支社/支店に最適です。

トランスペアレント(透過型)と ゲートウェイモードの特徴

- 複数メールドメイン対応
- 既存のメールサーバのSMTPゲートウェイとして動作
- DNSとMXレコードの単純な変更ですぐに設置可能(ゲートウェイモード)
- 多機能なポリシーベースのメールのルーティングとキュー管理
- 優れたメールセキュリティを実現するアウトバウンドのメールリレーとしての機能
- スパムとアンチウイルスのための細かなポリシーによる検知
- 通知の為のアンチウイルス置換えメッセージ
- スパムの隔離とタギング
- メールアドレス、IPアドレス、ドメインにわる承認、リレー、拒否、破棄の設定
- Webメール, POP3, とIMAPのメールも隔離可能
- 隔離状況のレポート
- ポリシーベースでインバウンド、アウトバウンドともアーカイブ可能
- 包括的なメールのモニタリング、ログ記録、レポートティン
- 送信失敗、遅延、未着の場合に備え、メールキューをサポート
- LDAP, RADIUS, POP3, IMAPのSMTP認証をサポート
- DNSアクセラレーション
- LDAPクエリー経由でユーザー毎にアンチウイルス/アンチウイルスの設定可能



サーバーモードの特徴

- トランスペアレント(透過型)モードとゲートウェイモードの全ての機能に加え:
  - POP3, SMTP, IMAPのメールサーバ機能
  - SMTPオーバーSSLをサポート
  - アカウント毎にディスク容量の割り当てを変更可能
  - Webメールのセキュリティも確保
  - ユーザ、グループ、エイリアスをサポート
  - ローカルアカウントとLDAP* 認証
  - スパムメール用にバルクフォルダをサポート

FortiMail ロギング&レポーティング

- 設定の変更と管理イベントログ
- アンチウイルスのログ
- アンチスパムのログ
- 外部またはネットワーク内のシスログサーバをサポート
- FortiReporterとの連携による拡張された集中管理レポートをサポート
- クリティカルなイベントとウイルスの状況によりアラート
- 7のカテゴリと140項目を超える包括的なレポート
- 複合的なレポートフォーマットをサポート
- レポート作成と発信をスケジューリング可能

FortiMailのアーカイブ機能

- 以下にもとづくポリシー設定が可能:
  - 送信者のアドレス
  - 受信者のアドレス
  - 題名中のキーワード
  - 本文中のキーワード
  - 添付ファイル名
- 禁止リスト
  - 送信者と受信者で設定可能
- 外部ストレージにアーカイブ可能　*v1.2

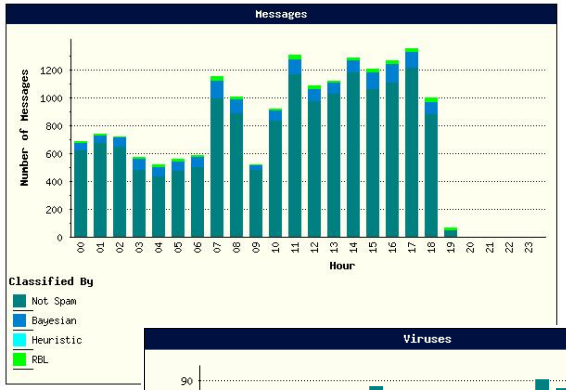
FortiMailの隔離機能とスパムのオプション機能

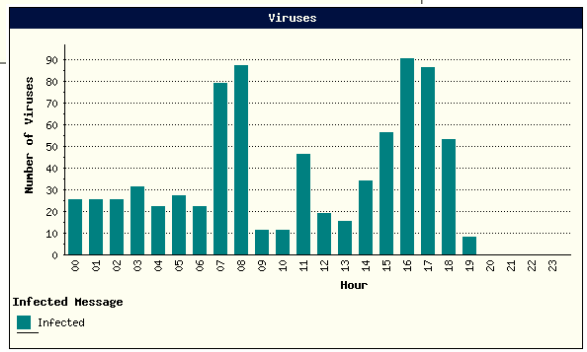
- **アクセスコントロール**
  - Eメールアドレス、IPアドレス、ドメインにより受信、リレー、拒否、破棄のコントロールが可能
- **メールキュー**
  - Failed Queue: 5日以上たった未送信メッセージを管理者が破棄か再送信可能
  - Deferred Queue: 5日以上たった未送信メッセージを自動的に再送信可能
  - Dead Mail Queue: 存在しない受信者宛や送信者のメールを保存
- **ユーザー毎にスパムを隔離しない、自動削除を設定可能(WebMailあるいはPOP3)**

わかりやすいFortiMail レポート機能

- スケジュールおよびオンデマンドのレポート
- 7つのレポートカテゴリ:
  - 高機能なブレークダウン(22レポート)
  - 送信者別(15レポート)
  - 受信者別(15レポート)
  - 送信者別のスパム(30レポート)
  - 受信者別のスパム(15レポート)
  - 送信者別のスパム(30レポート)
  - 受信者別のスパム(15レポート)

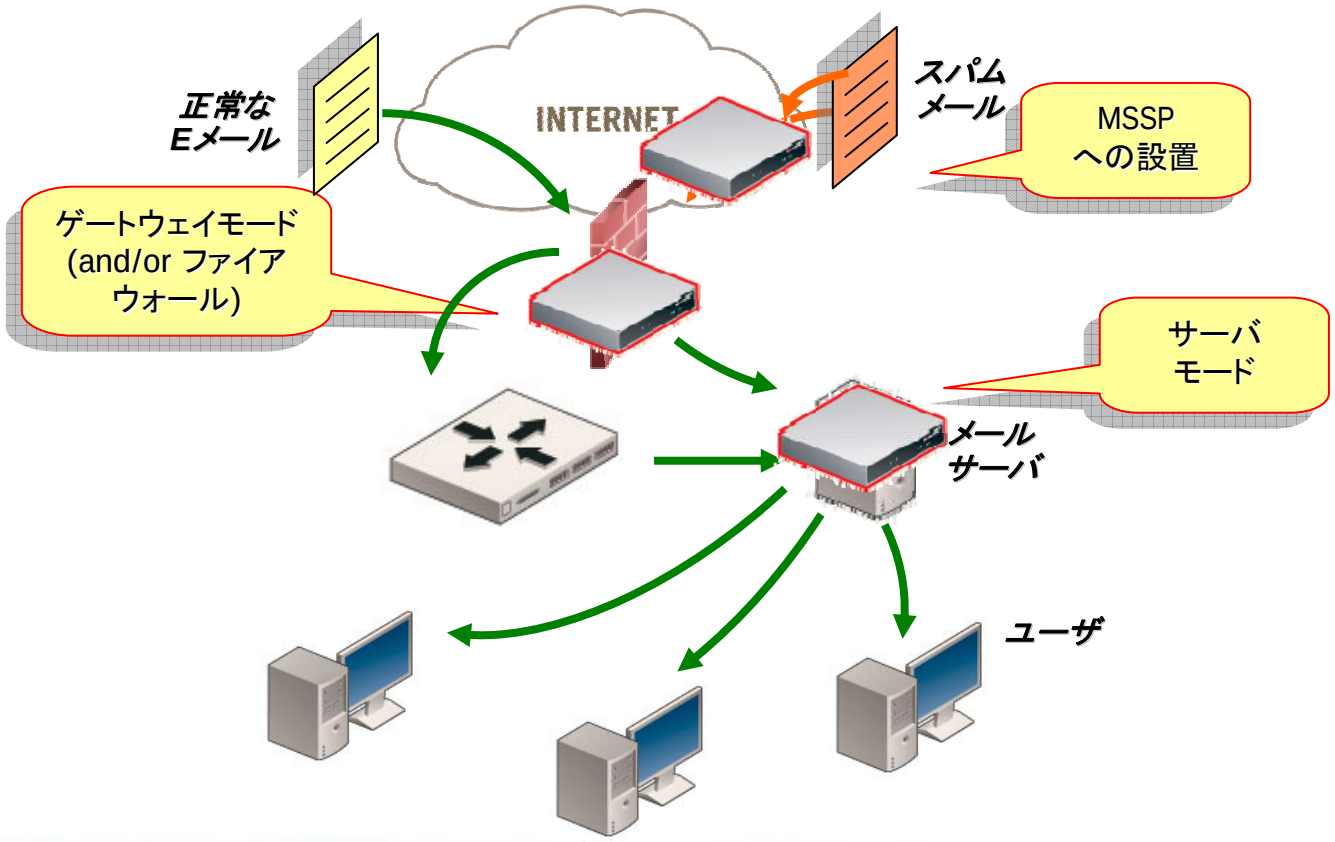
Messages		Today	This Hour
Not Spam		15742	51
Spams Classified By	Bayesian	1659	6
	Heuristic	27	0
	RBL	351	15
	Spam Subtotal	2037	21
Virus Infected		772	8
Total		17779	72





FortiMailの設置方法

- **MSSPにおける設置**
- **ゲートウェイモードの設置**
- **サーバーモードの設置**

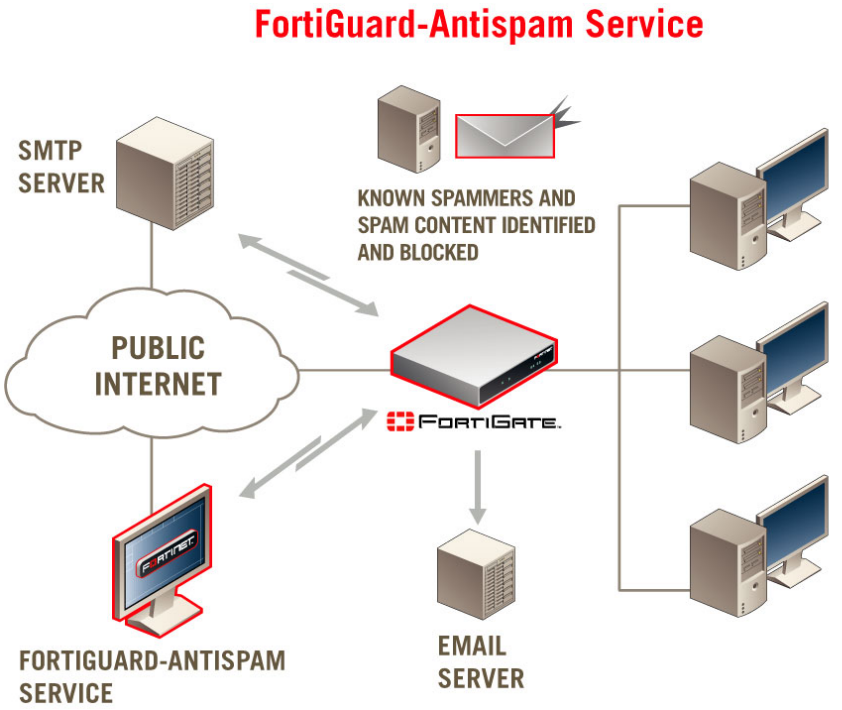


FortiGuard-アンチスパムサービス

～ フォーティネットの最新アンチスパム・マネジメントサービス ～

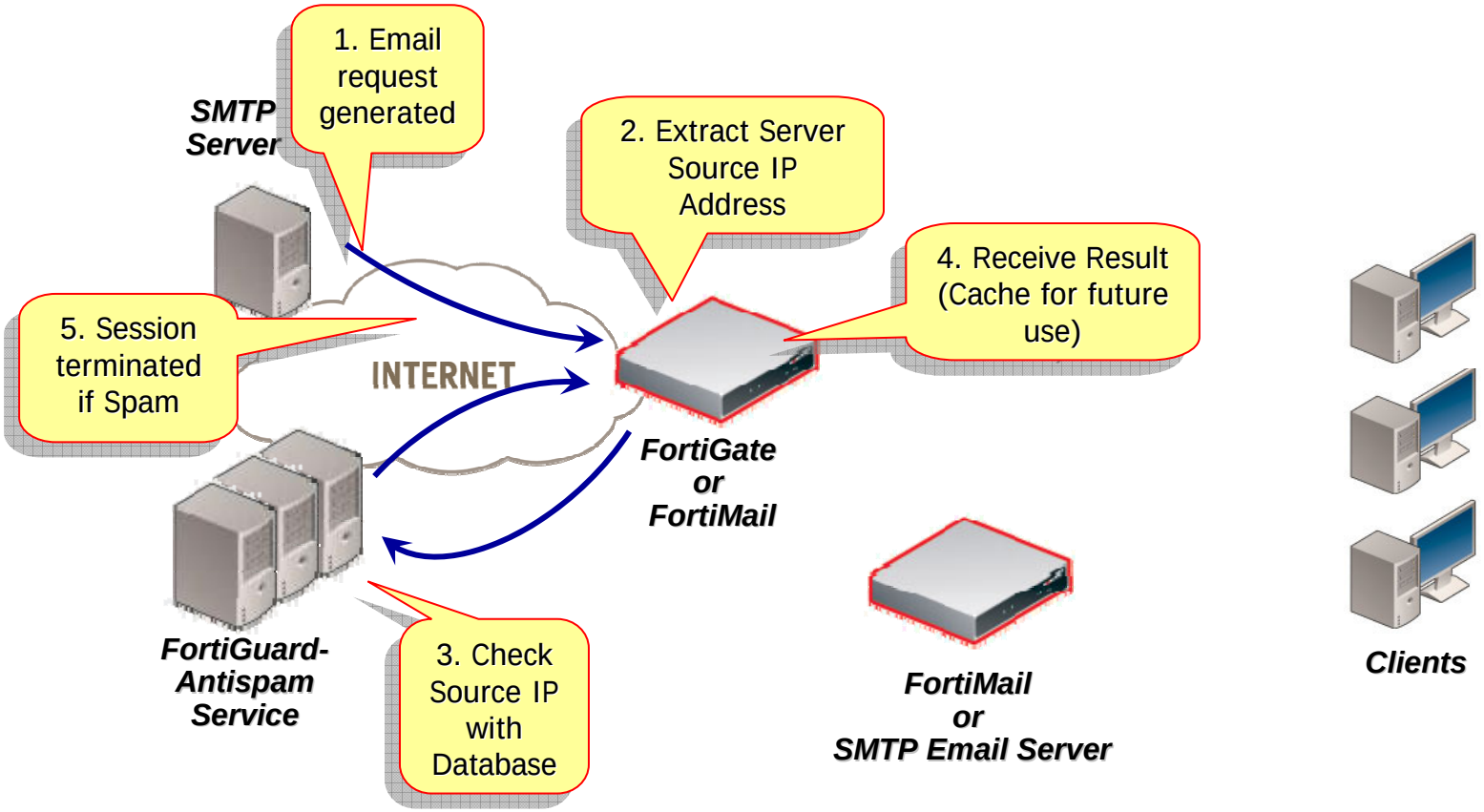
FortiGuard アンチスパムサービス

- 明らかなスパムによる被害を減らすマネジメントサービス
- フォーティネットは世界規模で調査しスパム情報を提供します
- アンチスパムのデータベースは毎日更新されます
- FortiGate及びFortiMailのプラットフォームで利用可能です
- デュアルパス・スキャニング・テクノロジーはRBLサービスでの検知率をさらに向上させます
  - 1st：名の知られたIPアドレスを使用します
  - 2nd：URLのコンテンツを使用します



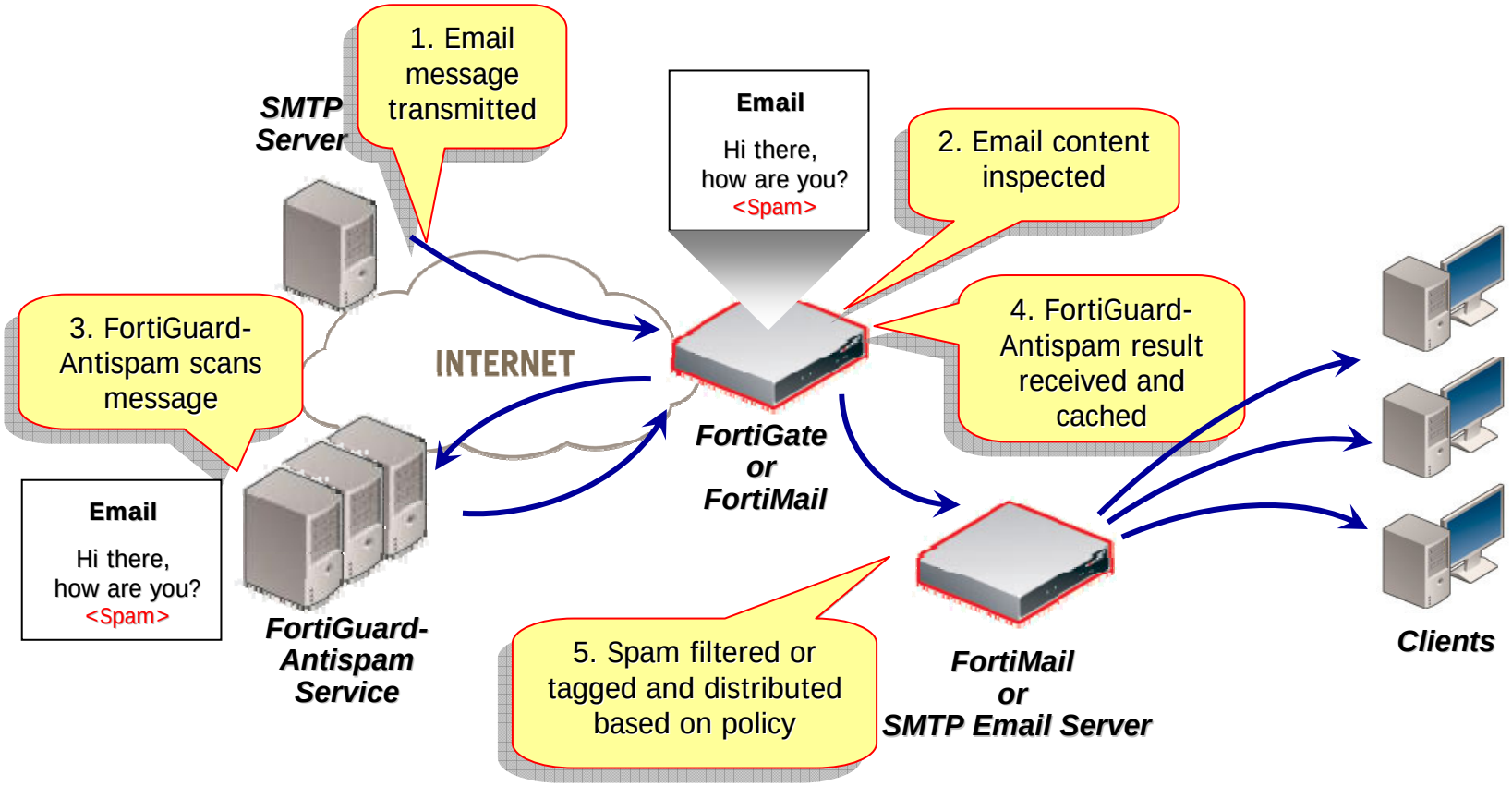
FortiGuard-Antispam Overview – First Pass Scan

- IP Black List Check



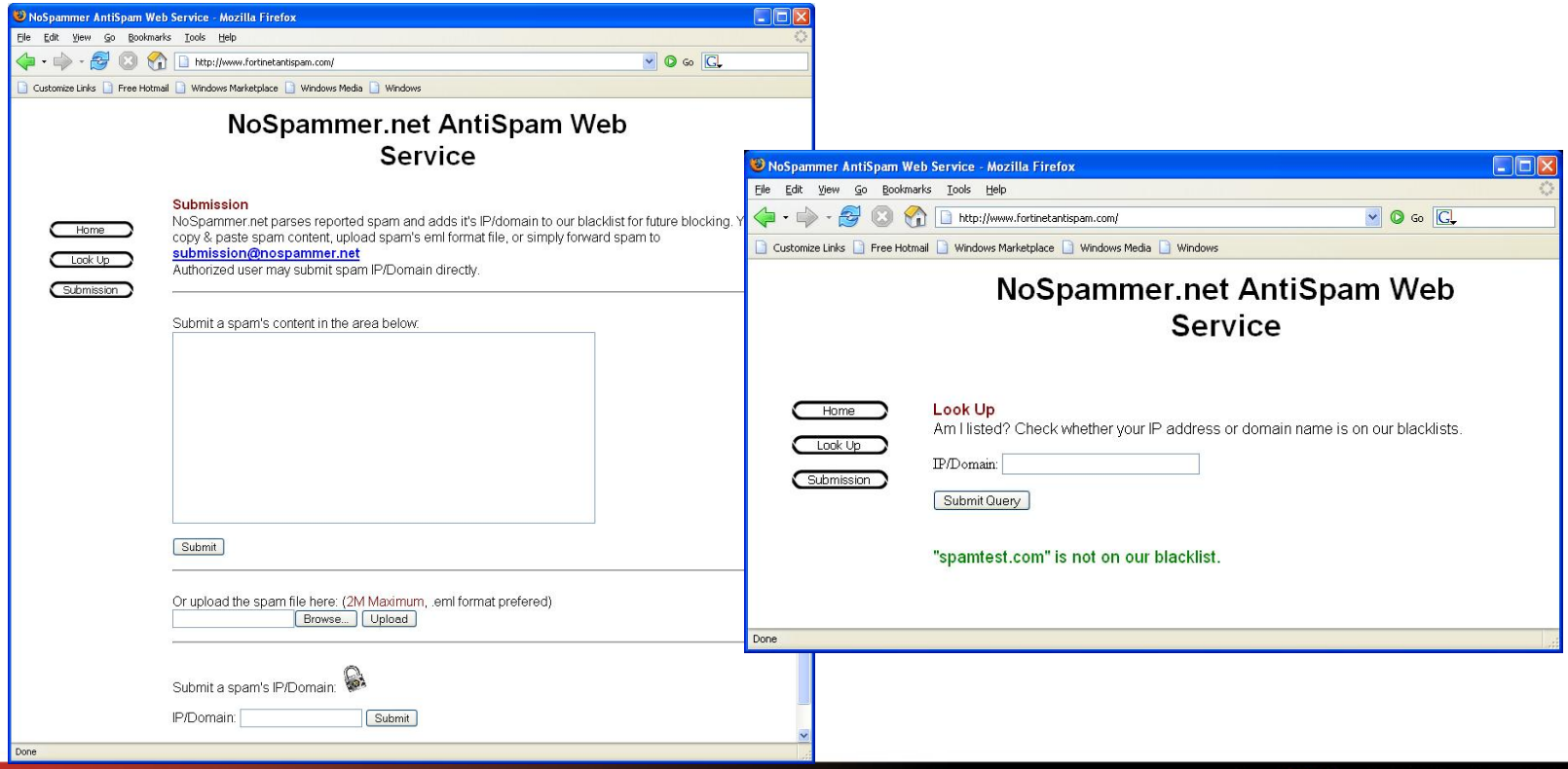
FortiGuard-Antispam Overview – Second Pass Scan

- Email Screening



FortiGuard-Antispam Service Controls

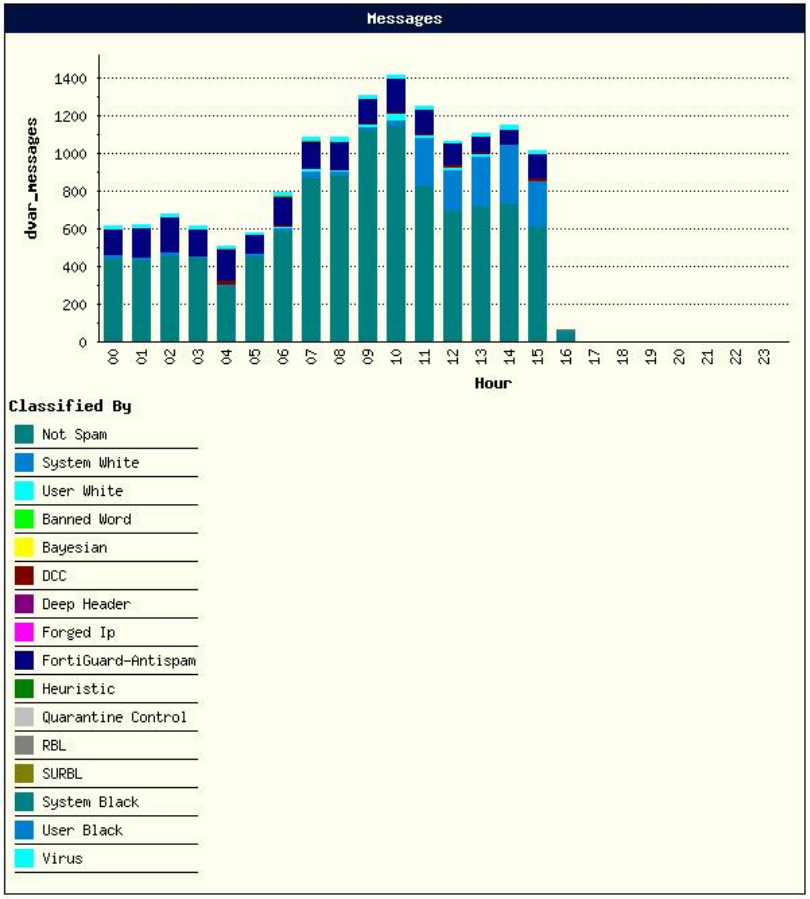
- FortiGuard-Antispam はウェブサービスを提供します
  - 名の知られたスパマーをサーチします
  - 新しいスパマーをレポートします
  - スパマーリストから取り除くリクエストをします



FortiGuard アンチスパムの有効性 – Live Customer Production Network

- 3カ国においてスパム検知でFortiMailを使用しているお客様のデータ

Messages		Today	This Hour
Not Spam Classified By	Not Spam	10769	49
	System White	1590	18
	User White	165	0
	Subtotal	**12524**	**67**
Spam Classified By	DCC	141	0
	FortiGuard-Antispam	2235	7
	RBL	67	1
	SURBL	38	1
	Virus	286	0
	Subtotal	**2767**	**9**
Virus Infected		285	0
Total		15291	76



集計結果:

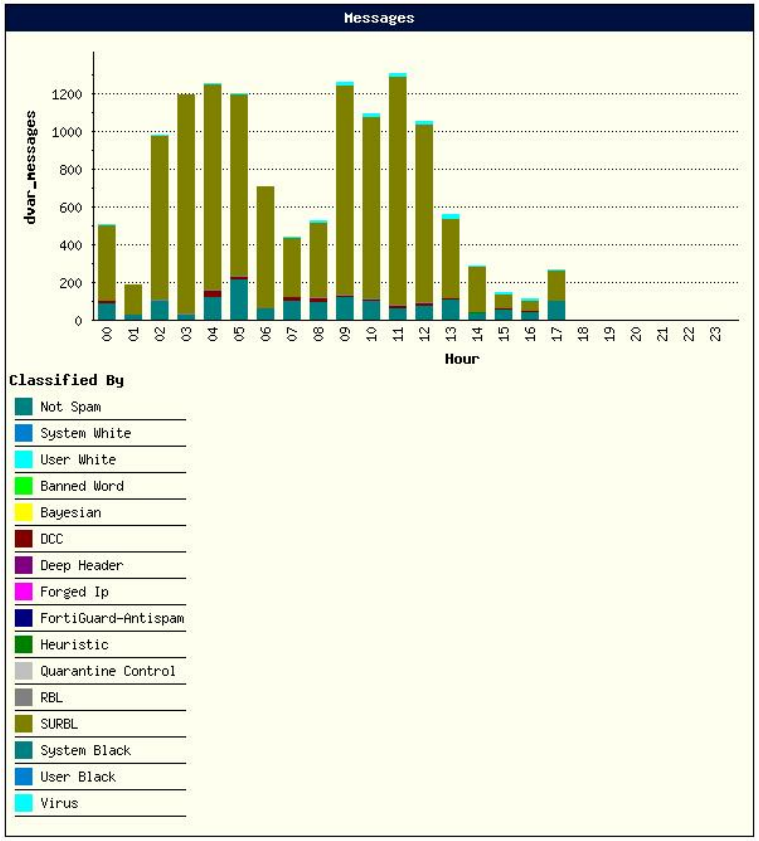
FortiGuardアンチスパムが80.8%と最も高い検出率であった

検知手法	**スパム**	**パーセント**	
DCC:	141	5.1%	
FortiGuard-AS:	**2235**	**80.8%**	
RBL:		67	2.4%
SURBL	38	1.4%	
AV Engine:	286	10.3%	

FortiMailの有効性は？
Live Customer Production Network

- リアルタイムでスパムの検出率を表示(図はラテンアメリカの物)
  FortiMail-400ユーザでアンチウイルスも使用のユーザの集計

Messages		Today	This Hour
Not Spam Classified By	Not Spam	1567	103
	Subtotal	**1567**	**103**
Spam Classified By	DCC	220	3
	Heuristic	45	2
	RBL	108	4
	SURBL	11177	162
	Virus	135	2
	Subtotal	**11685**	**173**
Virus Infected		129	2
Total		13252	276



集計結果:

17時までにあるお客様は以下のメールを受信:

非スパム:	1567
スパム:	11685
トータル:	13252
スパム%:	**88.2%**
ウイルス感染%:	1.1%


FORTINET
REAL TIME NETWORK PROTECTION
ありがとうございました。
Mydoom
Bagle
Alcaul
SDBot
RBot
Annil
Evaman
M/Opey