

Barracuda スパムファイアーウォール ご紹介資料

株式会社富士通ソーシャルサイエンスラボラトリ

Barracuda スпамファイアウォール

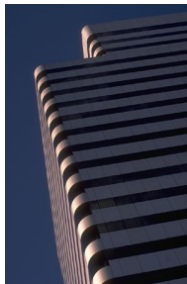
- ユーザー数毎のライセンスではなく、優れたコストパフォーマンス
- 中小規模企業からISPクラス対応までの4モデル
- オリジナル+パブリックの高精度なスパム判定
- 既存メールシステムへの組み込みが容易
- ルールやパターンファイルの自動更新機能
- スпамとウイルスの両方をブロック
- 詳細なログやレポート機能



ソフトウェアソリューションの問題

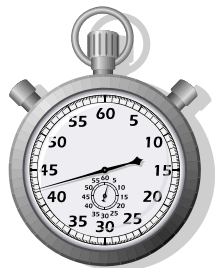


- 設計が複雑(OSなど)
- インストールが必要
- OS との互換性
- バージョンアップ運用のコスト
(ソフトだけでなく、OSも考慮が必要)
- ソフトとハードのサポート窓口は別



サービスソリューションの問題

- 電子メールがサイト外を経由する
- セキュリティの問題
- 安価とはいえない運用コスト



迷惑メール対策に猶予はありません！



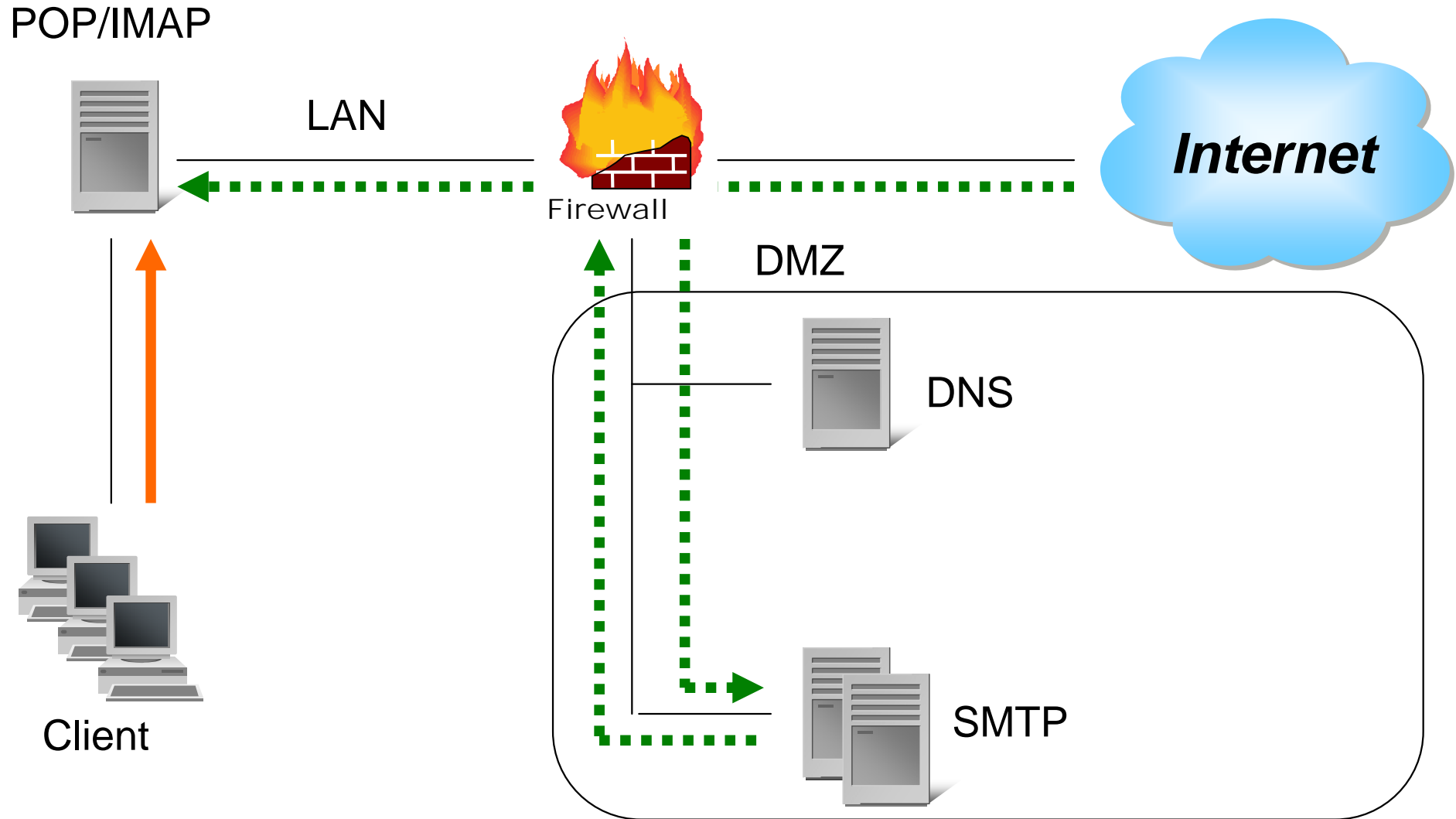
アプライアンスの優位性

- 10分間で設定完了
- メールサーバの負荷を軽減
- メールサーバを保護
- OS互換性などの問題がない

スピード

コストパフォーマンス

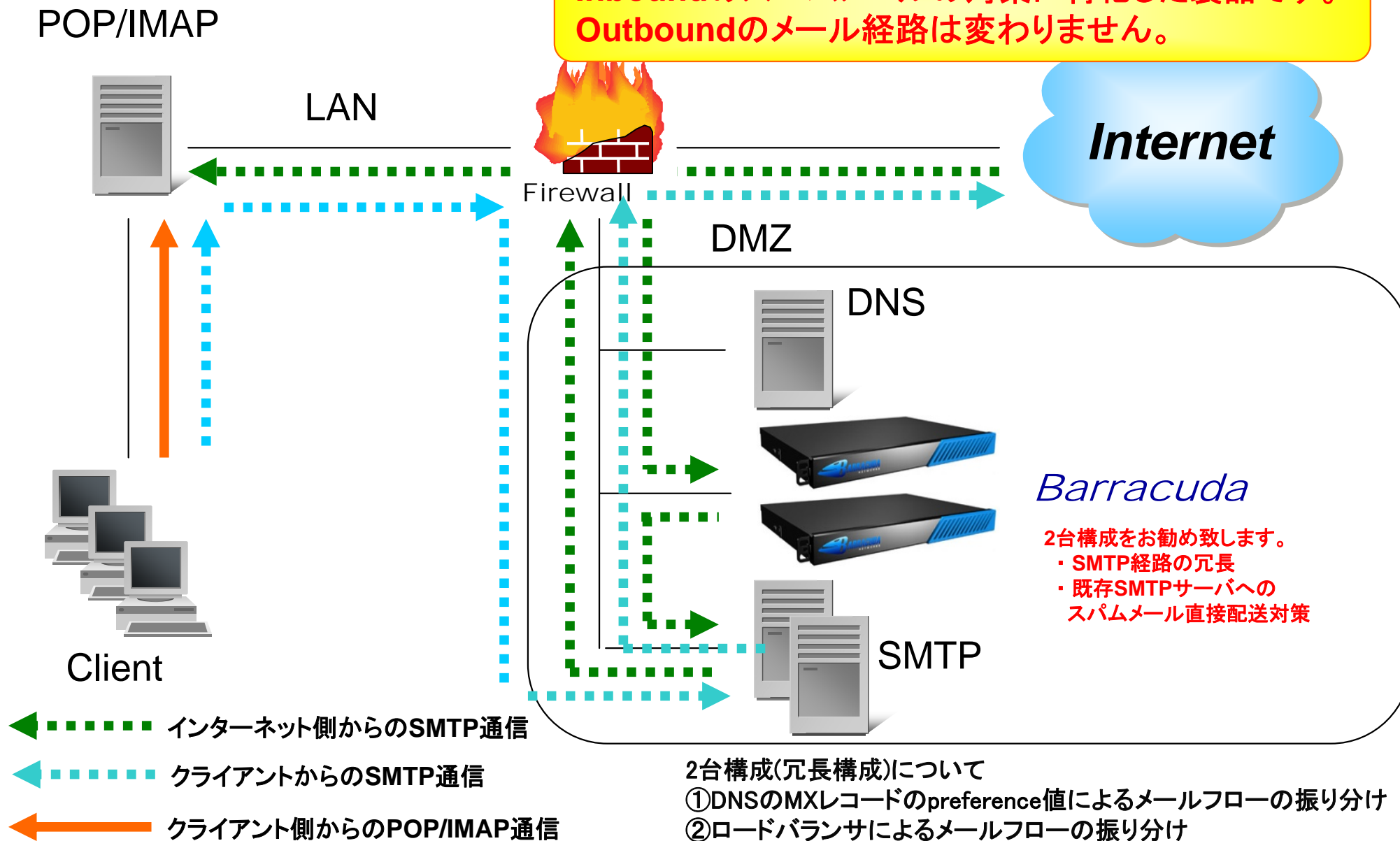
バラクーダの配置例(既存環境)



- ← 緑点線 インターネット側からのSMTP通信
- ← 赤実線 クライアント側からのPOP/IMAP通信

バラクーダの配置例(導入例)

Inboundのスパムメールの対策に特化した製品です。
Outboundのメール経路は変わりません。



スパムに対する3つのアクション

スパムと判断した場合に次のアクションを実施

1. タグ付配信 : タイトル(サブジェクト)に任意の文字を挿入して配信。
※ユーザーがスパムメールを管理。
2. 隔離 : *Barracuda* 内部に一時保管。
※管理者およびユーザーがスパムメールを管理。
3. ブロック : スパムメールを破棄。
※スパムメールの管理なし。

***Barracuda* なら
管理者が一括管理することも
各ユーザーが自ら管理することも可能**

※ 隔離機能については、管理者の運用負荷があがること、
ユーザーからのウェブアクセスに伴う *Barracuda* 自体の負荷があがることから、
上位モデル(モデル600、800)での利用を推奨しております。

複数技術を組み合わせることでスパムを効果的にブロック(タグ付け配信/隔離/ブロック)

■ レートコントロール

- 接続元IPアドレスと接続数の制限によりスパムを拒否。

■ IPブロックリスト

- 送信元のIPアドレスによりスパムをブロック。

■ ホワイトリスト/ブラックリスト

- 受信者、送信者が明らかなスパムをブロック。

■ インテンション解析

- 詐欺/悪質サイトのURLが記載されているスパムをブロック。リダイレクトサイトにも対応。

■ フィンガープリント

- メールデータのハッシュ値が専用DBに登録されているスパムをブロック。

■ スパムスコアリング

- Barracudaが付けたスパムらしさを表す点数(スコア)に基づきブロック。

■ スパムスコアリングに、以下の機能を組合せて使用。

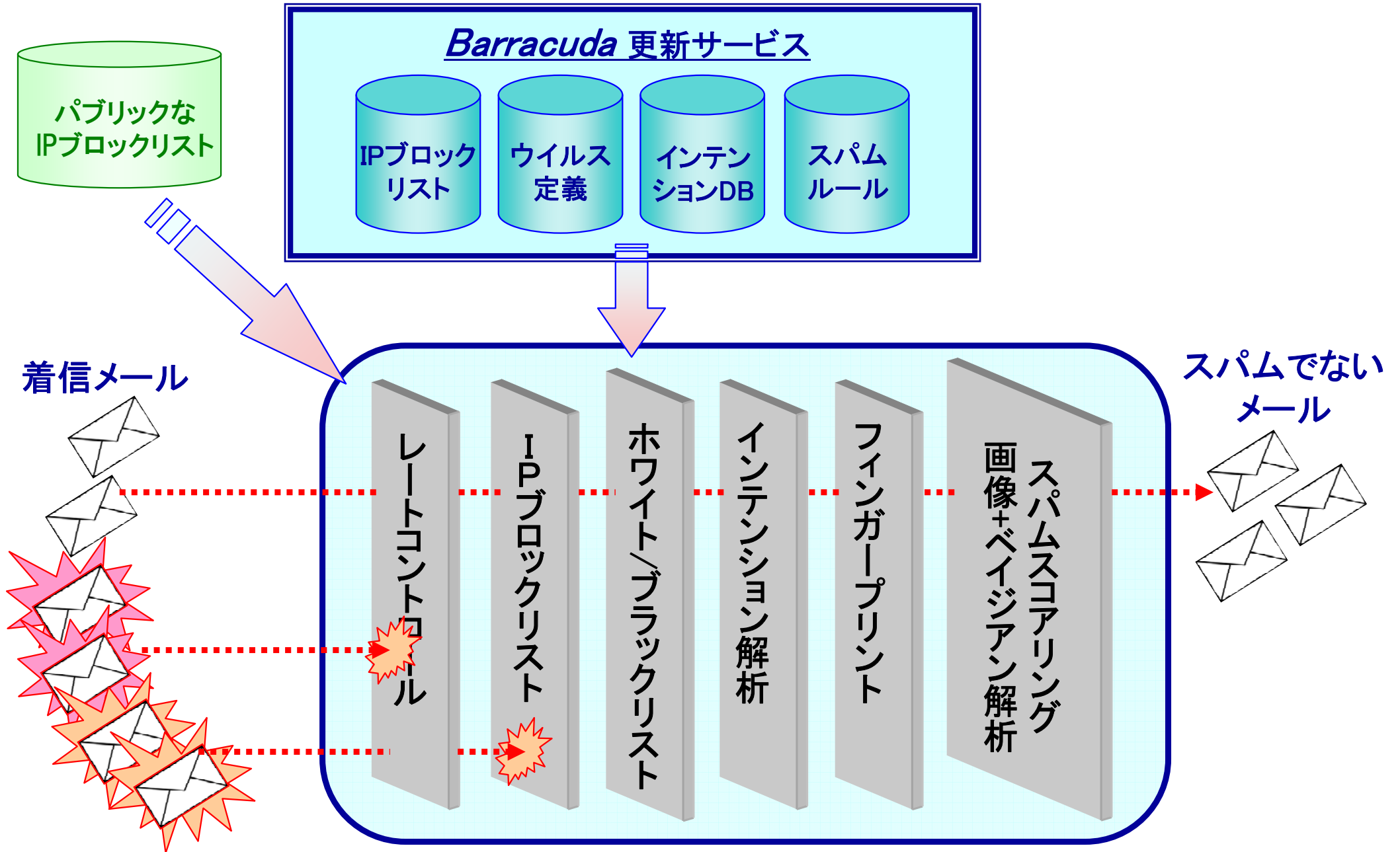
画像解析

- 高度な光学式文字認識機能(OCR)を使用して、添付された画像ファイルがスパムかどうか解析し、スパムスコアリングのスコアに10点(スパム)が加算されます。

ベイジアン機能

- ベイジアンは正常なメールとスパムメールに用いられている単語の出現頻度を計算し、受信されたメールがどちらの傾向にあるかを判断して、加点または減点(-5~+5)し、スコアリングのスコアが微調整されます。

スパムフィルタリング



各モデルの違い(1)

		製品モデル	300	400	600	800
導入 目安	秒間に処理可能なEメール数		2 通/秒	3.3 通/秒	6.3 通/秒	8.4 通/秒
	アクティブメールユーザー数		1,000	5,000	10,000	22,000
機能	メールサーバとの互換性		○	○	○	○
	ハード化されたセキュアOS		○	○	○	○
	ユーザー毎の設定と隔離領域		○	○	○	○
	LDAP連携によるアドレス収集攻撃対策		○	○	○	○
	Syslog サポート		○	○	○	○
	ドメイン毎の設定			○	○	○
	RAID			○	○	○
	ユーザー毎のスコア設定				○	○
	ロゴのカスタマイズ				○	○
	電源の冗長化					○

各モデルの違い (2)

各スパムフィルタリング機能が適用された際のアクション、モデル毎の機能有効範囲を下記にまとめます。

全 … システム全体に有効
 ド … ドメイン単位に有効
 ユ … ユーザー単位に有効

モデル		300	400	600	800
スパム機能	レートコントロール (ブロック)			全	
	バラクーダレピュテーション (タグ付け配信/隔離/ブロック/無効)			全	
	外部RBL (タグ付け配信/隔離/ブロック)			全	
	ホワイト/ブラックリスト (許可/タグ付け配信/隔離/ブロック)			全/ユ	
	LDAPユーザーチェック (ブロック)			全	
	添付ファイルチェック (隔離/ブロック)			全	
	ウイルスチェック (ブロック)	全		全/ド	
	キーワードチェック (許可/タグ付け配信/隔離/ブロック)			全	
	インテンション解析 (タグ付け配信/隔離/ブロック)			全	
	フィンガープリント (タグ付け配信/隔離/ブロック)			全	
	画像解析+ベイジアン+スパムスコアリング (閾値によるタグ付け配信/隔離/ブロック)	全		全/ド	全/ド/ユ
	逆引きDNSルール (タグ付け配信/隔離/ブロック)			全	
	文字セットポリシー (タグ付け配信/隔離/ブロック)			全	

統計的にスパムの状況が確認可能です。
統計グラフは時間毎、日にち毎(過去1ヶ月分)に出力されます

BARRACUDA NETWORKS
SPAM & VIRUS FIREWALL 600

guest | ログオフ | 日本語

基本設定 | 拒否許可 | ユーザ | 複数ドメイン設定 | 高度な設定

ステータス | メッセージログ | スпамチェック | ウィルスチェック | 隔離 | IP設定

管理 | レポート

メール統計 [インバウンド(受信)]

	合計	今日	この時間
拒否	16,497,176	49,695	897
拒否:ウィルス	6,586	44	1
レートコントロール	7,441	366	36
隔離	36	0	0
許可:タグ	25,569	82	0
許可	1,084,955	5,503	112
総受信件数	17,621,762	55,680	1,046

パフォーマンス統計

IN/OUTキューサイズ: 0/3
 平均遅延時間: 2秒
 最後に受信したメール: <1分前
 メール受信者数: 163

システム負荷: 1%
 CPUファン回転数: 5870 RPM
 システムファン回転数: 5921 RPM
 CPU温度: 28°C
 ファームウェア: 41%
 ストレージ: 47%
 メール/ログストレージ: 47%
 冗長性(RAID): 正常に動作中

サービスステータス [最新表示]

エネルギー充填サービス: 有効 (有効期限: 2011-12-22)
 インスタントリブレス: 有効 (有効期限: 2011-12-22)

1時間毎のメール統計

Legend:

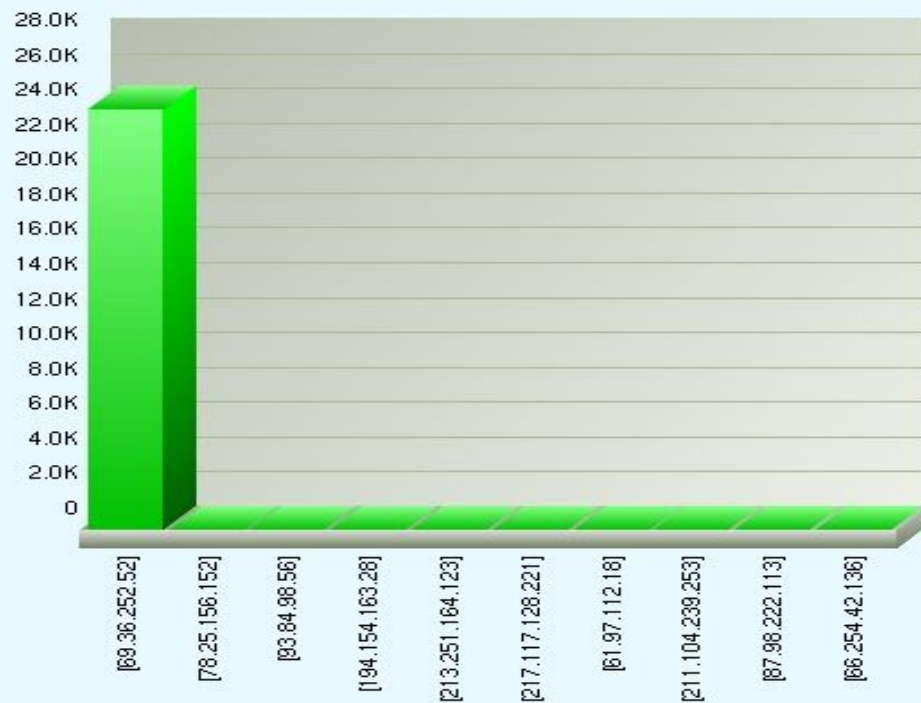
- Permitido
- Permitido: Etiqueta
- In Cuarentena
- Lista Controlada
- bloqueado: Virus
- bloqueado: Spam
- bloqueado: Autor Errorneo

HTMLベースでの
ディリーレポート出力が
可能です

デイリーレポートサンプル

Top Spam Senders Report - barracuda3.webpex.com [69.36.230.17]

From: 02/22/2010 16:00:00
To: 02/23/2010 16:00:00



トップスパム送信者

#	送信者	回数
1	unknown[69.36.252.52]	24085
2	78-25-156-152.colomna.net[78.25.156.152]	37
3	unknown[93.84.98.56]	31
4	supanames-1-28.supanames.co.uk[194.154.163.28]	24
5	ns33014.ovh.net[213.251.164.123]	22
6	fw.otohost.pl[217.117.128.221]	22
7	www.ok-net.net[61.97.112.18]	22
8	unknown[211.104.239.253]	21
9	fanfilled.com[87.98.222.113]	17
10	pppoe-qc-66-254-42.136.altaspectra.com[66.254.42.136]	16

メッセージログ

ログ表示 プリファレンス ?

IS フィルター: なし パターン: + フィルターの適用 バラクーダセントラルに送信

配送 CSV出力 戻る 次へ

時間	送信者	受信者	件名	サイズ	アクション	理由	スコア
2010-02-23 16:46:54	zrewr13@fu-guitars.com	liban01@barracuda.c...	Acai Berry , Lose wieght feel great	2787	拒否	インテント (http://groups....	
2010-02-23 16:46:52	torvenyek@freemail.hu	sender@barracuda.c...	Èàè äðàìòñ òááæààòù è èðèèèèìààòù ñì..	21511	拒否	スコア	10.4
2010-02-23 16:46:50	Dr_marry@eze.co.za	dwssms1@barracud...	Confirm Message	40467	拒否	スコア	10.0
2010-02-23 16:46:49	culturally@interne4clas...	dawkins@bodylines...			拒否	バラクーダレピュテーシ...	



メッセージの内容確認

```
X-ASG-Debug-ID: 1266973648-2ef400020001-QwCvMU
Received: from a ( ) by bsf1. with SMTP id qNHPYD00cAU0dj for <
X-Barracuda-Envelope-From: test@
X-ASG-Orig-Subj: testa
subject: testa
X-Barracuda-Connect: UNKNOWN
X-Barracuda-Start-Time: 1266973648
X-Barracuda-URL: http:// 8000/cgi-mod/mark.cgi
X-Barracuda-Orig-Rcpt: test@
X-Virus-Scanned: by bsmtpd at
Message-Id: <20100224010904.8C0241C8B@bsf1.>
Date: Wed, 24 Feb 2010 10:09:04 +0900 (JST)
From: test@
X-Barracuda-Spam-Score: 1.58
X-Barracuda-Spam-Status: No, SCORE=1.58 using global scores of TAG_LEVEL=1000.0 QUARANTINE_LE
X-Barracuda-Spam-Report: Code version 3.2, rules version 3.2.2.23901

Rule breakdown below
pts rule name description
-----
0.00 NO_REAL_NAME From: does not include a real name
1.58 MISSING_HEADERS Missing To: header
0.00 TO_CC_NONE No To: or Cc: header
```

●メッセージログとは、Barracudaが処理したメールのログです。

➤メッセージログはディスク容量75%まで保持

※「メール/ログストレージ」で表示される容量の75%を超えると

自動的にメッセージログを削除していきます。(5分毎にチェック)

例) モデル300の場合、約90万通まで保存可能(1通10KByteを想定)。

➤メッセージ内容の確認

※ヘッダを初めとしたメール詳細を確認可能

➤メッセージログのエクスポートが可能

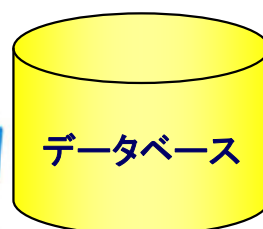
※CSVファイル形式

Barracuda 更新サービス(エネルギー充填サービス)

- 「バラクーダセントラル」が新たな攻撃を検出すると、更新データを作成しスパムDBの自動更新に対応します。
- Barracuda のスパムDBを自動更新させることで、ユーザーの負担を増加させることなく常時高精度のスパム対策として機能します。(10分～20分間隔で更新)
- 「バラクーダセントラル」は、バラクーダネットワークス社が24時間365日体制で運営するスパム防御機能の更新サービス拠点です。

Barracuda Networks Inc.

バラクーダセントラル



更新データ確認

更新データの
自動ダウンロード

Internet

■ Spam Firewall 300

- ✓ 導入目安：1,000ユーザー
- ✓ 1日のメール処理可能件数：約17万通
- ✓ 隔離ストレージ:10GByte
- ✓ 標準価格：[1,045,000円](#)
(次年度保守価格:400,000円)

■ Spam Firewall 400

- ✓ 導入目安：5,000ユーザー
- ✓ 1日のメール処理可能件数：約28万通
- ✓ 隔離ストレージ:50GByte
- ✓ 標準価格：[2,128,500円](#)
(次年度保守価格:838,500円)

■ Spam Firewall 600

- ✓ 導入目安：10,000ユーザー
- ✓ 1日のメール処理可能件数：約54万通
- ✓ 隔離ストレージ:100GByte
- ✓ 標準価格：[4,746,500円](#)
(次年度保守価格:1,846,500円)

■ Spam Firewall 800

- ✓ 導入目安：22,000ユーザー
- ✓ 1日のメール処理可能件数：約72万通
- ✓ 隔離ストレージ:200GByte
- ✓ 標準価格：[10,554,500円](#)
(次年度保守価格:4,114,500円)

- 標準価格には初年度の製品保守サービスが含まれています。
- 保守価格は平日保守(平日9:00~17:00)の価格です。24H×365Dの価格については別途お問合せください。



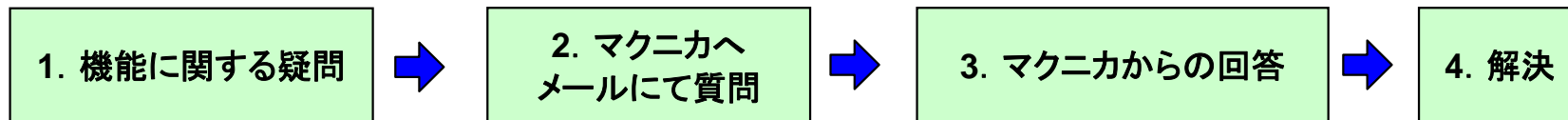
※ 1日のメール処理可能件数は、RBL,宛先不正,不正中継関連にて、ブロックした場合の各モデルの想定処理能力(1通平均10KByteのメール)となります。

トラブル対応 (製品サポート) について

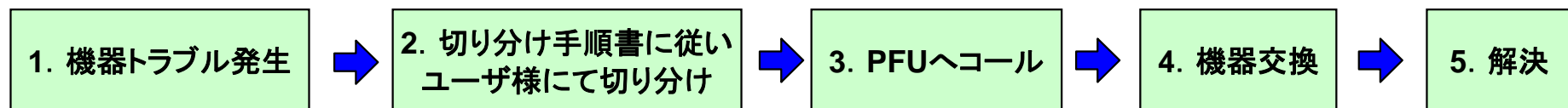
製品保守概要

- ・機能に関するメールでのQ&A
(平日9:00~17:00) 窓口: マクニカネットワークス (barracuda@cs.macnica.net)
- ・機器トラブル時のオンサイト対応
(24H365Dまたは、平日9:00~17:00) 窓口: PFU (044-520-6415)

QA対応



トラブル対応



※ 保守内容はハード交換、IPアドレスの設定、設定ファイルのリストアまで実施致します。

【ご参考】販売実績

○販売台数

現在までに富士通SSLでは約26社300台以上の販売実績。
日本国内では3,000台以上、全世界では60,000台以上の
販売実績となります。

アプライアンス出荷台数の国内シェア率は22.3%でNO.1

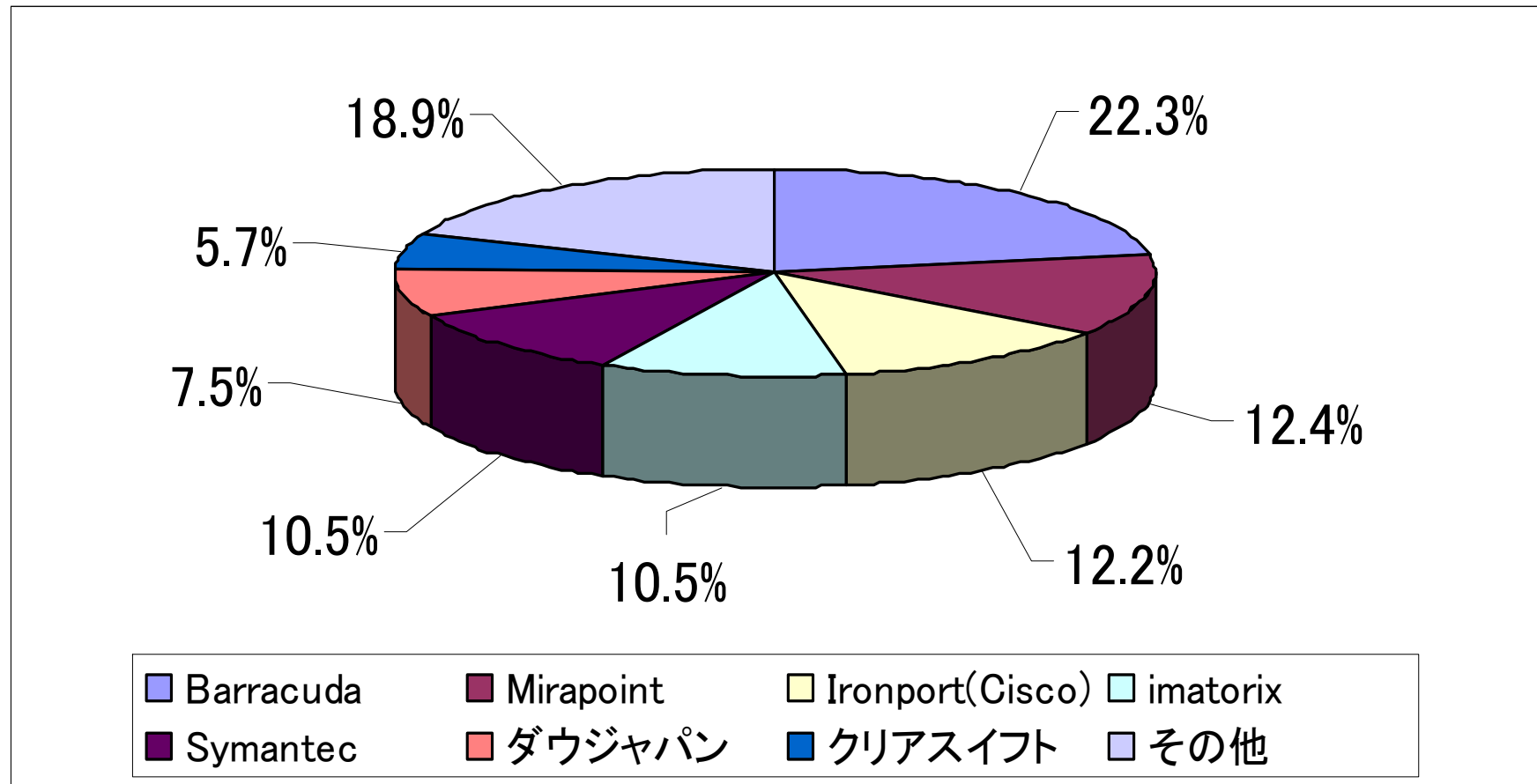
※ 富士キメラ総研調べ(2009年発表)

2008年電子メールセキュリティアプライアンスにおける市場占有率



【ご参考】製品シェア

スパム対策アプライアンス製品の導入台数



引用元: 2009ネットワークセキュリティビジネス調査総覧(富士キメラ総研)

● 検知精度の評価方法

[評価方法]

- スпамルールの拒否動作を無効し、タグ付け配信に変更する。

[評価内容]

- メッセージログより、どのメールが、スパム判定されたか確認し、誤検知されていないことを確認します。

[評価環境]

- 実際に配送されるメールにて、確認しなければ、評価できないため、本番導入構成で導入します。

※ サンプルドメインなどを擬似環境を構築しても、環境差異(流れるメール)があるため、正確な検知精度の評価にはなりません。

[コメント]

拒否動作なしに、評価したいというお客様にお勧めです。

無償のBarracuda評価貸し出し(2週間)を行っておりますので、ご活用下さい。

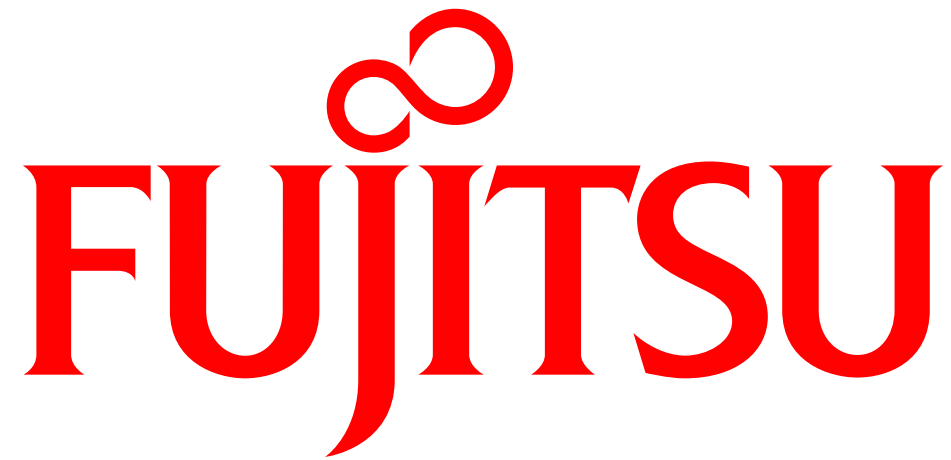
※ 導入のための設定は、別途有償となります。

株式会社 **富士通** ソーシャルサイエンスラボラトリ
(富士通SSL)

<http://www.ssl.fujitsu.com>

E-mail : ssl-info@cs.jp.fujitsu.com

TEL : 044-739-1251



shaping tomorrow with you