

レピュテーション システム

メール送信者の評価

脇山弘敏 IronPort Systems, Inc.

スパム防止の為の基本的な対策

1. コンテンツ ベース

- 送られてくる内容を分析 (サブジェクト, メッセージボディ, ヘッダ, その他) してスパムをブロックする
- 例:
 - (1) ルールエンジン
 - (2) ベイジアンなどの学習型フィルター

2. アイデンティティ ベース

- 送り元が誰かを分析してスパムをブロックする
- 例:
 - (1) ブラックリスト / オープンプロキシリスト
 - (2) ホホワイトリスト
 - (3) レピュテーション

さまざまなブラックリスト

Accuracy

Blacklist

Low	@COUNTRY: Problematic Countries, http://blackholes.us/
Low	@DYNAMIC: Cable, ADSL and Dialups, http://bliab.com/
Low	@ISP: Blocked ISP's, http://www.blackholes.us/
Low	@SPAM: Spam Sources, http://bliab.com/
Low	AHBL: The Abusive Hosts Blocking List, http://ahbl.org/
Low	BLARS: Blars Block List, http://www.blars.org/errors/block.html
Low	BOGONS: completewhois.com: Bogon IP's, http://www.completewhois.com/bogons/
Low	DRBL: Distributed Realtime Blocking List, http://www.agk.nnov.ru/drbl/
Low	INTERSIL: Intersil Blackholes, http://groups.google.com/groups?scoring=d&q=blackholes.intersil.net+group:*abuse
Low	JIPPGMA: JIPPG's Relay Blackhole List, http://blacklist.jippg.org/
Low	LNSG: Leadmon SpamGuard Listings, http://www.leadmon.net/spamguard/
Low	MAPSPPLUS: Dialup Users List, http://mail-abuse.org/dul/
Low	PSS: , http://pss.spambusters.org.ar/
Low	REYNOLDS: Reynolds Boycott List, http://bl.reynolds.net.au/
Low	RFC_IPWH: Bad IP-Whois, http://www.rfc-ignorant.org/
Low	FIVETEN: Local Blackholes at Five-Ten, http://www.five-ten-sg.com/blackhole.php
Low	PSBL: Passive Spam Block List, http://psbl.surriel.com/
Low	SPAMBAG: Spambags, http://www.spambag.org/
Low	SPAMRBL: , http://spam-rbl.com/
Low	SPAMSITE: Spamware Peddler and Spamservices, http://spamsites.org/
Low	SPEWS: Spam Prevention Early Warning System, http://spews.org/
Low	UCEPROT: , http://www.uceprotect.net/en/
Medium	SORBS: Spam and Open Relay Blocking System, http://www.dnsbl.sorbs.net/FAQ.html
Medium	NJABL: Not Just Another Bogus List, http://njabl.org/
Medium	ORDB: Open Relay DataBase, http://ordb.org/
High	SPAMCOP: SpamCop, http://www.spamcop.net/
High	SBL: Spamhaus Block List, http://www.spamhaus.org/sbl/
High	CBL: Composite Blocking List, http://cbl.abuseat.org/
High	DSBL: Distributed Server Boycott List, http://dsbl.org/
High	DSBLALL: Distributed Server Boycott List, http://dsbl.org/
High	DSBLLIST: Distributed Server Boycott List, http://dsbl.org/
High	DSBLMULT: Distributed Server Boycott List, http://dsbl.org/
High	BOPM: Blitzed Open Proxy Monitor, http://opm.blitzed.org/

- 同一カテゴリ内の順序は精度順ではありません。
- あくまでIronPortの経験と評価に基づくもので、第三者、各団体の意見を反映したものではありません。

各ブラックリストの特長





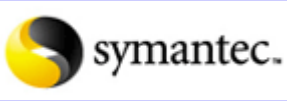
- **SPEWS**
 - 最も攻撃的なブラックリスト。一旦掲載されるとリストから外されない
- **MAPS RBL**
 - 数少ないコマースベースのブラックリスト サービス
- **SpamHaus (www.spamhaus.org)**
 - 広範に利用されており、精度も高い
 - ボランティアグループにより運営
- **SpamCop (www.spamcop.net)**
 - 非常に高い検知率
 - 自動化によりリアクションが早く新しいスパム攻撃に有効
- **Open Proxy / compromised host lists (XBL, OPM, SORBS)**
 - あまり広範には利用されていないが、スパムの特定には有効

ブラックリストの問題点

- そもそもどれを使用すればいいのかという選択の問題
- 1/0の判定は誤検知のもと
- チューニング作業はエンドレス
- リスト掲載、解除の時間的ギャップの問題
- 苦情情報に依存した恣意性の問題
- ダイナミックIP

ブラックリスト情報、流量、流量の変化、振る舞い、オーナー、履歴など総合的に判定をする必要がある

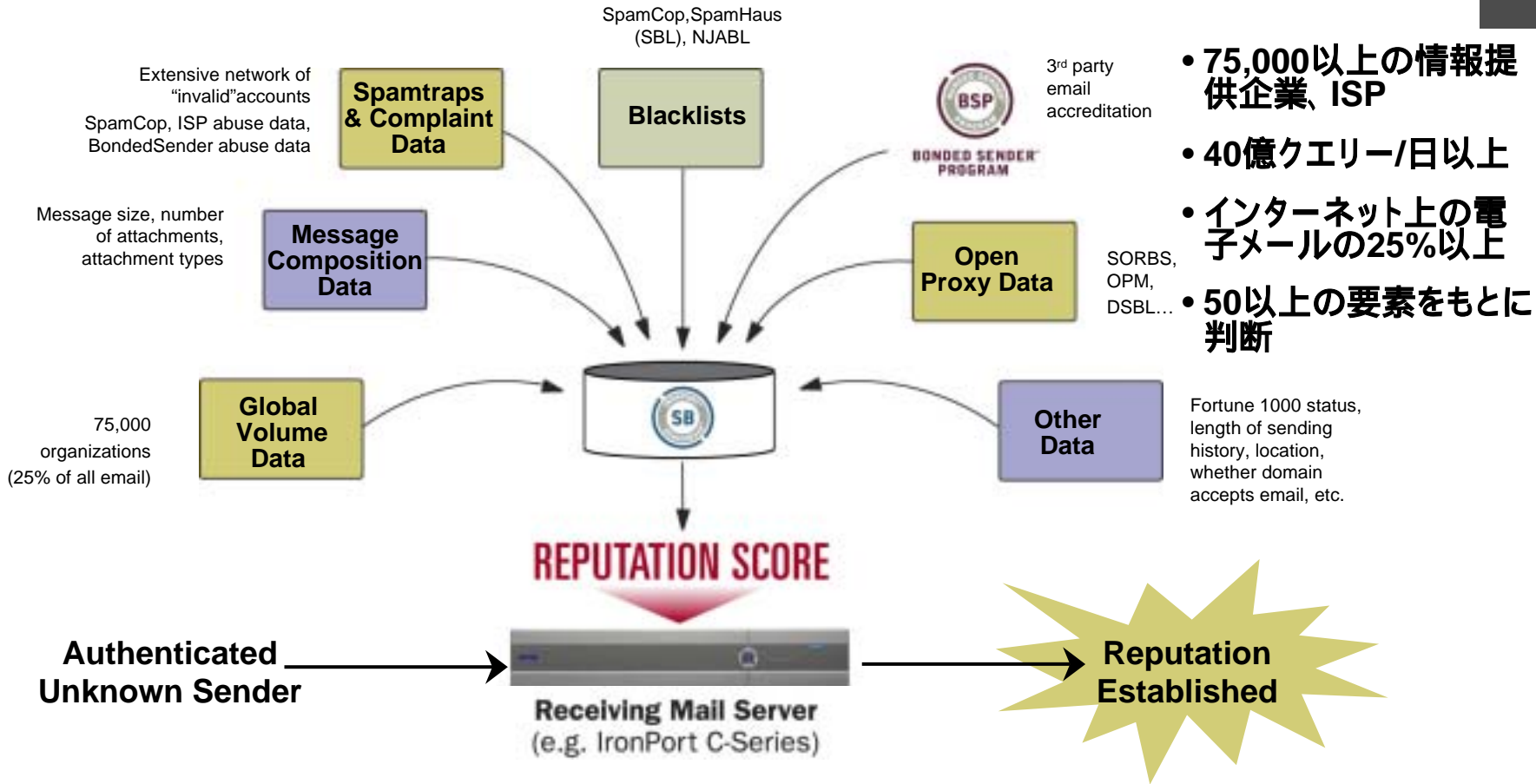
レピュテーションサービス

Reputation Service Providers	Name	Notes*
	TrustedSource	同社の顧客1400社から情報を収集 5,000万IPのデータを保持(2005/1)
	Cloudmark Anti-Phishing Reputation Service Cloudmark Rating	Cloudmark Rating for NewsLetterはホワイトリストサービス Cloudmark Rating for SenderID
	SenderBase	75,000社から情報を収集 40億クエリー/日
	Kelkea IP-based Reputation Services	15億IPのデータを保持 実体はMAPS(ブラックリスト)
	Symantec Brightmail Reputation Service	Symantec Probe Network(honeypot)からデータを収集 1000億レコード/月
GOSSiP	GOSSiP Project	OpenSource P2P メールレピュテーション まだ詳細不明

- web、その他の情報を元にまとめたもので各社を代表して掲載しているわけではありません。詳細は各社にご質問ください。
- その他未掲載のベンダーもほとんどの場合何かしらのレピュテーションを使用していると称している。

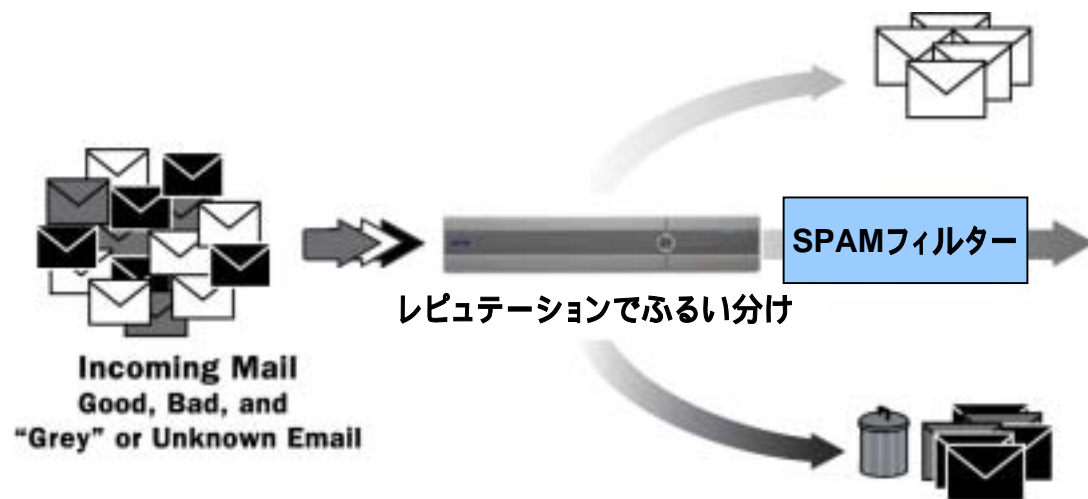


SenderBaseレピュテーションサービス



- 75,000以上の情報提供企業、ISP
- 40億クエリー/日以上
- インターネット上の電子メールの25%以上
- 50以上の要素をもとに判断

スパムをゲートウェイレベルで判断



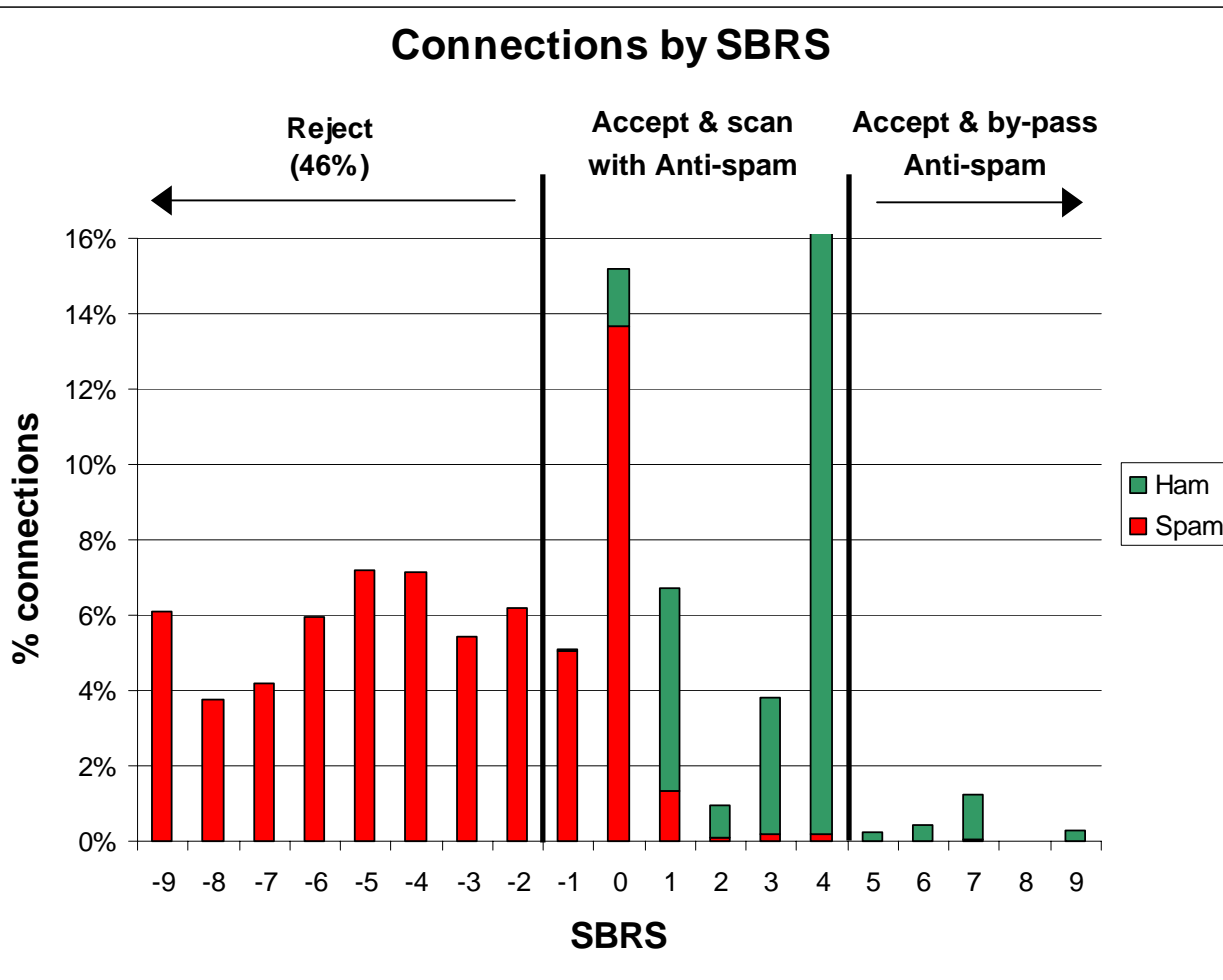
- 既知の正しいメール送信者

- 既存のスパム処理、スロットル処理

- 隔離、接続拒否、削除など

- SPAMフィルターの処理は重い
- 後段のリソース低減
- 誤検知の低減

SenderBaseスコアの実際



- SBRS eliminates need to content filter up to 70% of email
- ~ 1 / 1 million false-positive rate at -4 or below

SBRS利用の推奨値

- 危険IPからの接続拒否で不要トラフィックを激減
- 2以下ではほとんど誤検知がみられない、-4以下だと100万分の1
- 世界中の送信者情報

SBRS推奨値:

Legend

Policy	
Blocked	Red
Throttled	Orange
Default	Grey
Trusted	Green

Customer Profile	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10
Conservative (Near-zero false-positives, better performance)	Blocked	Blocked	Blocked	Throttled	Throttled	Throttled	Throttled	Throttled	Default	Default	Default	Default	Default	Default	Default	Trusted	Trusted	Trusted	Trusted	Trusted
Moderate (Very few false-positives, high performance)	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Throttled	Throttled	Throttled	Default	Default	Default	Default	Default	Default	Trusted	Trusted	Trusted	Trusted	Trusted
Aggressive (Some false-positives, max. performance)	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Throttled	Default	Default	Default	Default	Trusted	Trusted	Trusted	Trusted	Trusted	Trusted	Trusted

レピュテーション利用の効果例

- **某大手企業:**
 - 1日に2600万メッセージを受信
 - 約150万メッセージが正しいメッセージ(残りはスパム)
 - Spam Assassinを68台のゲートウェイ上で動作
 - 高い誤検知率
- **レピュテーション導入後:**
 - レピュテーションだけで1900万メッセージ/日をブロック
 - 550万メッセージを後段のコンテンツベースのフィルターでスキャン、ブロック
 - ゲートウェイ数を68台から 8台に削減
- **精度向上(検知率、誤検知率)**
- **サーバの負荷を低減**
- **運用コストの削減**

ドメイン認証との連携

1. 認証されたIPをどう評価するか？

- SenderBaseではspfレコードのある送信者を + 側に評価する
- ただし、身元を明らかにしているという意味で

2. IPベースのレピュテーションからドメインベースに拡張

- 現時点ではIPベース
- ドメインに対するレピュテーション

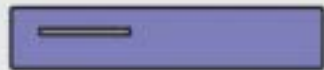
Identity, Reputation, Policy

1 IDENTITY

Stores records for
Sender ID(Caller ID, SPF)
Yahoo! Domain Keys



送信者およびメッセージの
認証



Sending Mail Server

2 REPUTATION

Reputation Services



レピュテーション情報

Receiving Mail Server
(e.g. IronPort C-Series)

3 POLICY

Corporate Email Policies



企業それぞれの
ポリシーを適用



Mail Client

SenderBaseのデモ

- 時間があれば....
- なければ、www.senderbase.org

The screenshot displays the SenderBase website interface. At the top left is the SenderBase logo, featuring a circular emblem with 'SB' and 'IRONPORT' text. Below the logo, it reads 'The Leading Email Reputation Service'. A search bar is located to the right of the logo, with a 'Search' button and a green checkmark icon. Below the search bar, there is a prompt: 'Enter domain, organization name, IP address or CIDR range'. To the right of the search bar are links for 'help', 'contact us', and 'subscribe'.

The main content area is titled 'Report on domain: optinbargains4u.com'. It is divided into several sections:

- Volume Statistics for this Domain:** A table showing 'Magnitude Vol Change vs. 30 Day' for 'Last day' (7.6, 135%) and 'Last 30 days' (7.3).
- Third-party Certification:** A section for 'TRUSTe Privacy Seal?' with a 'Not Certified' status.
- Information from whois [Click to show details]:** A table listing contact information for 'Ineedemailhelp.com', including address, phone, fax, email, and registration dates.
- Other information about optinbargains4u.com:** A table showing 'Sender Category' as 'unknown category' and 'Date of first message seen from this domain' as '2003-09-21'.
- Related links:** A list of links including Google groups and OpenURL.
- Organizations that use optinbargains4u.com hostnames:** A table showing 'Showing 1 - 1 out of 1' with one entry for 'contact@optin.com (Tech Support)' with a 'Monthly Magnitude' of '7.3'.
- Addresses in optinbargains4u.com used to send email:** A section at the bottom with an 'export' button and a status 'Showing 1 - 50 out of 239'.