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.

IRONPORT

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 / オープンプロキシーリスト
     - (2) ホワイトリスト
     - (3) レピュテーション

IRONPORT

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	**MAPSPLUS**: 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/**

•同一カテゴリー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。

IRONPORT

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
  - 数少ないコマーシャル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

IRONPORT

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

IRONPORT

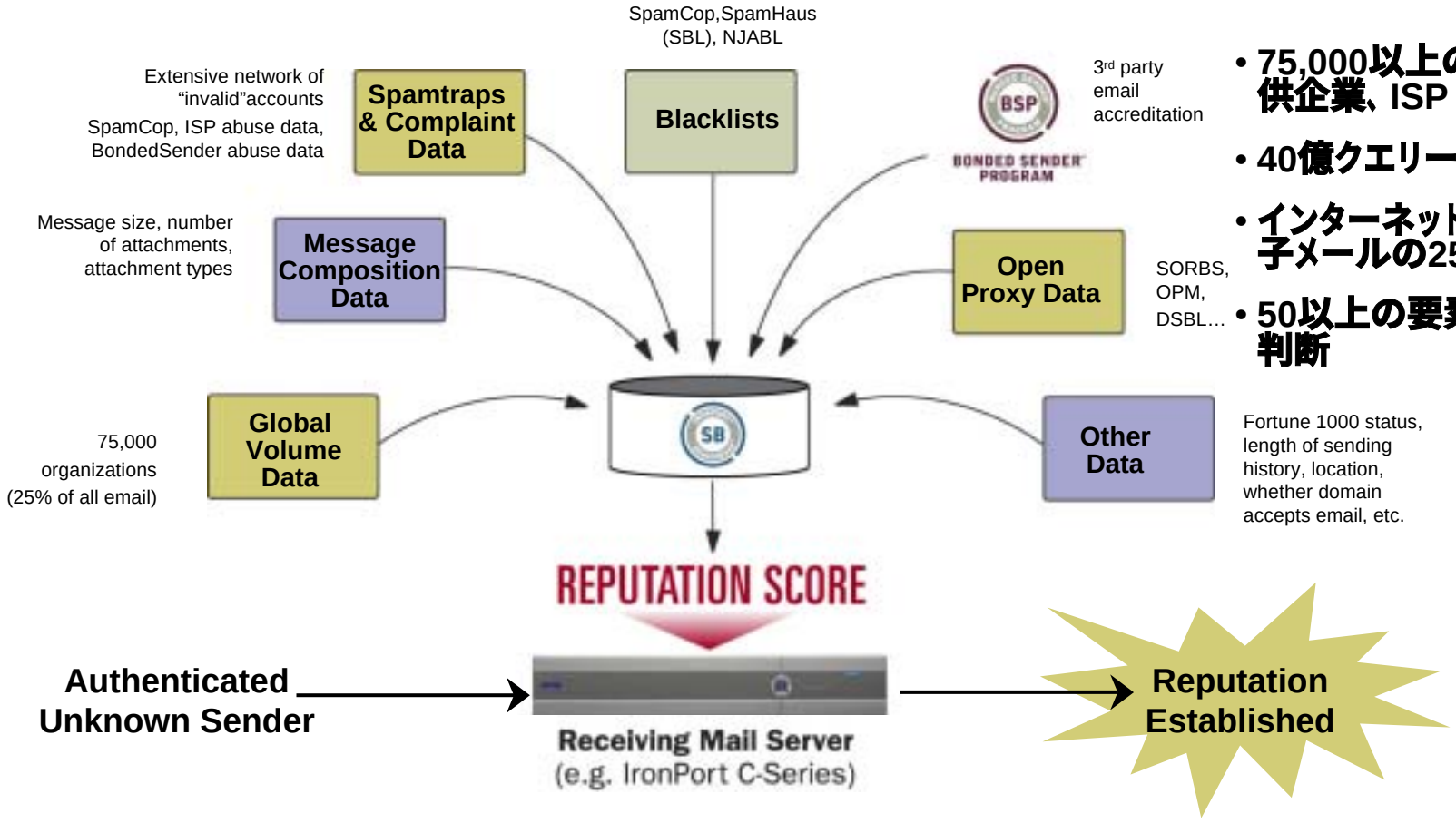
レピュテーションサービス

Reputation Service Providers	Name	Notes*
CipherTrust	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 The Immune System for Email	Cloudmark Anti-Phishing Reputation Service Claudmark Rating	Cloudmark Rating for NewsLetterはホワイトリストサービス Claudmark Rating for SenderID
IRONPORT	SenderBase	75,000社から情報を収集 40億クエリー/日
Kelkea	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.	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。

IRONPORT

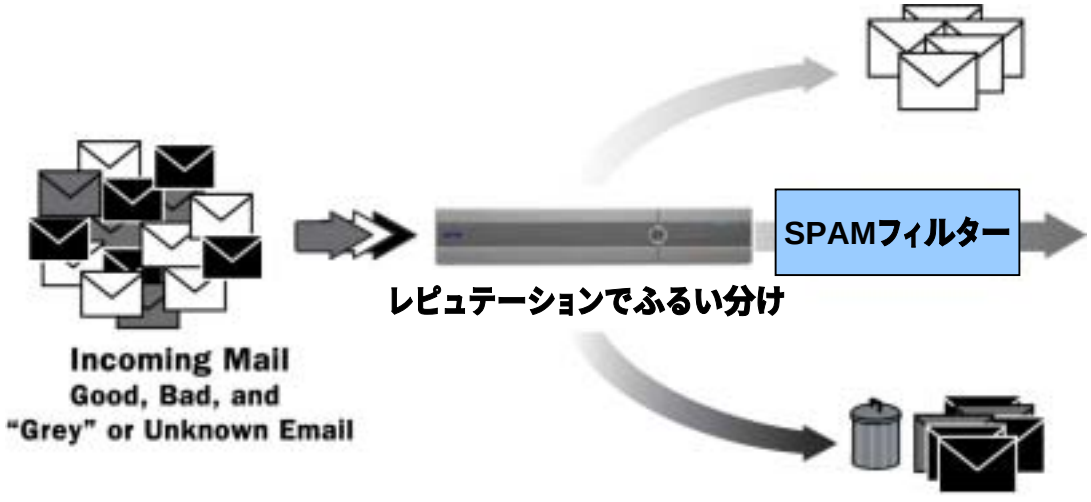
SenderBaseレピュテーションサービス



- 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

IRONPORT

スパムをゲートウェイレベルで判断

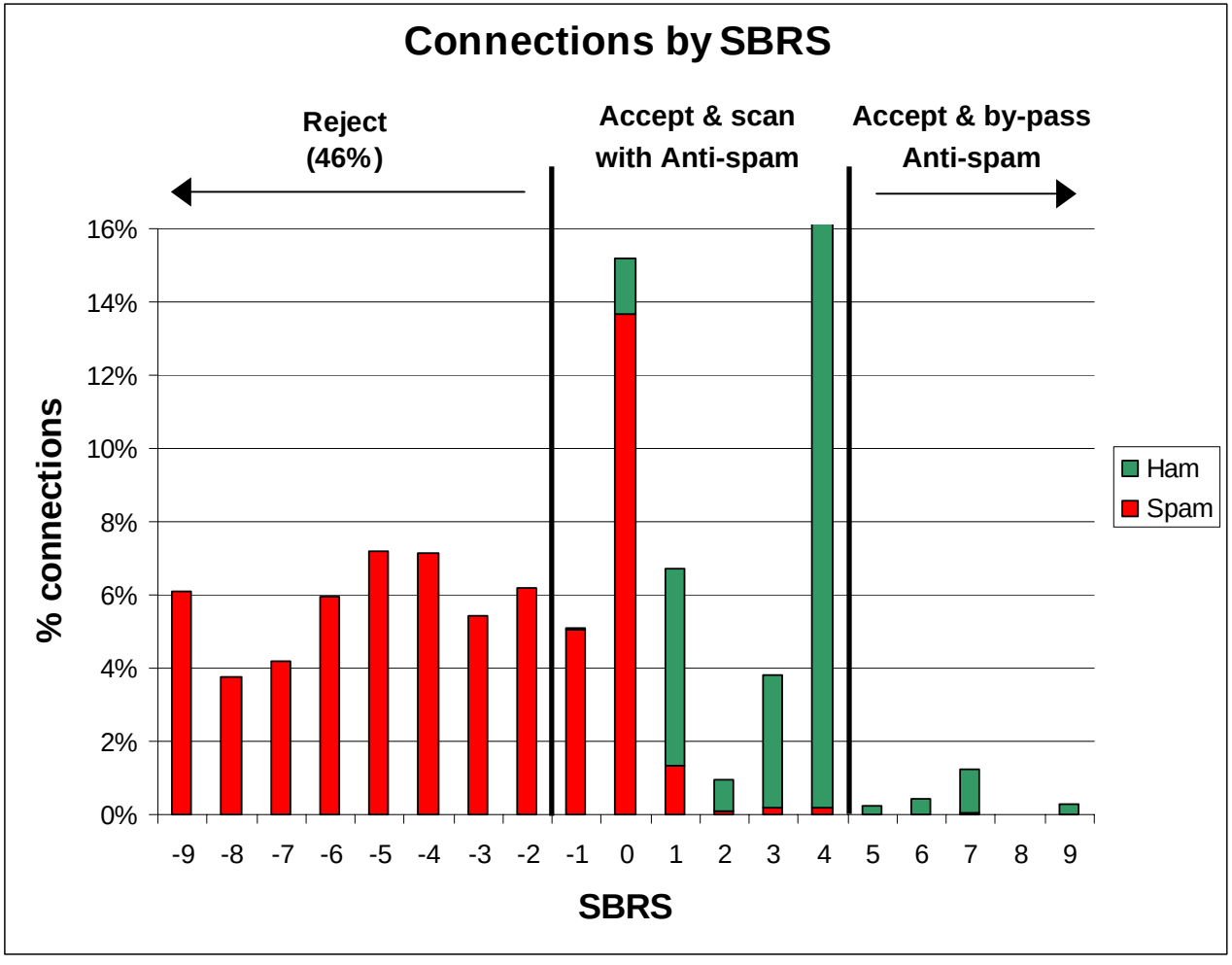


- 既知の正しいメール送信者
- 既存のスパム処理、スロットル処理
- 隔離、接続拒否、削除など

- 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

IRONPORT

SenderBaseスコアの実際

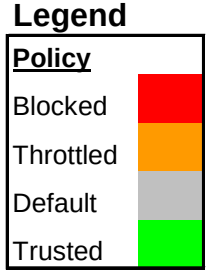


- SBRS eliminates need to content filter up to 70% of email
- ~ 1 / 1 million false-positive rate at -4 or below

IRONPORT

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:

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)																				
Moderate (Very few false-positives, high performance)																				
Aggressive (Some false-positives, max. performance)																				

IRONPORT

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**

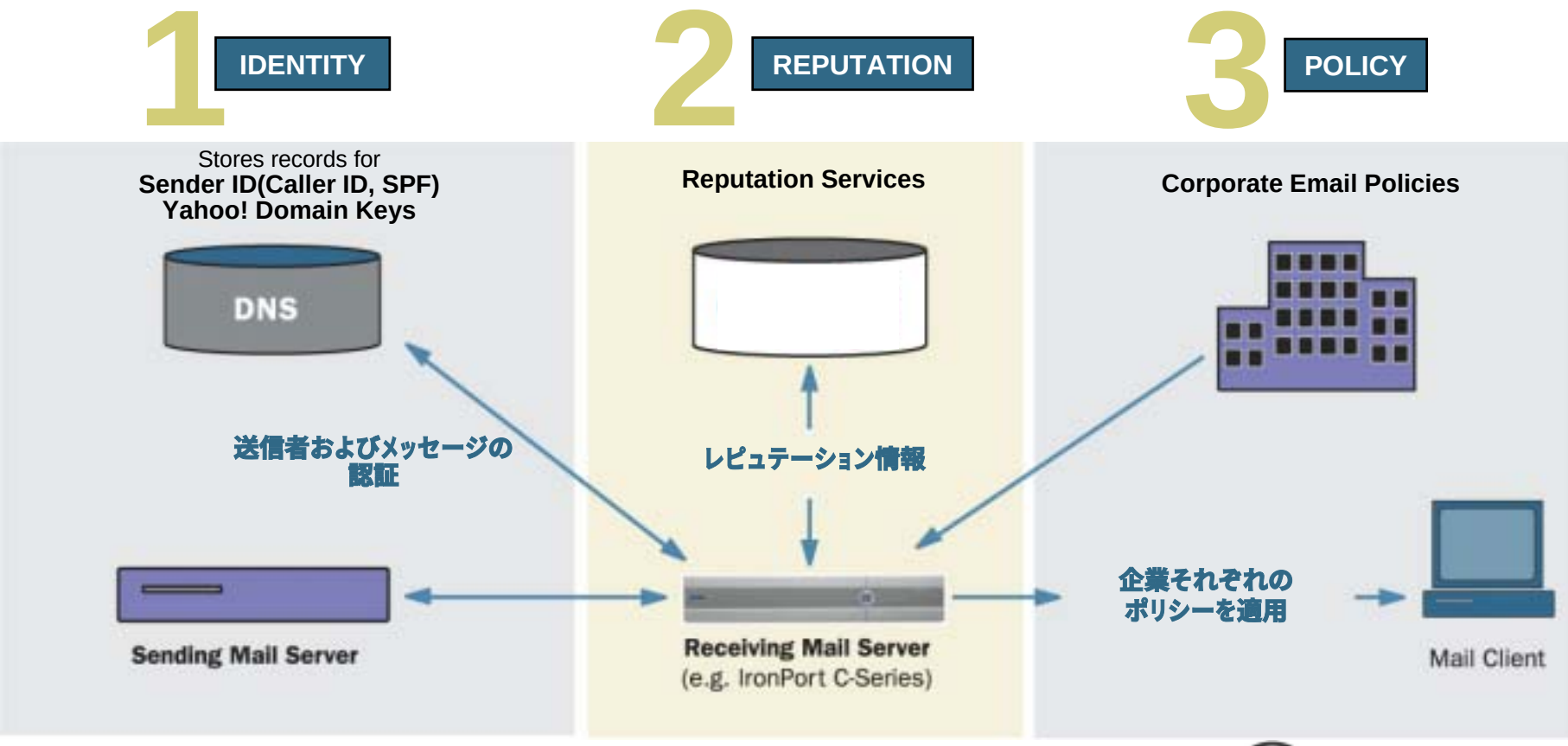
IRONPORT

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

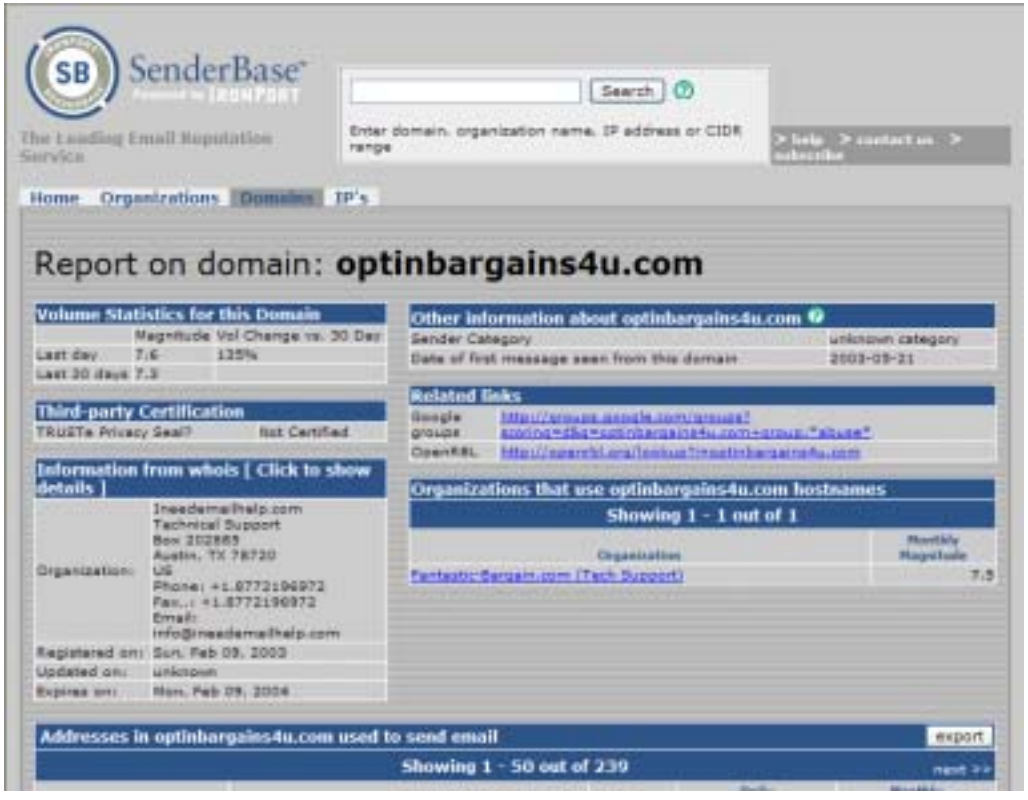
Identity, Reputation, Policy



IRONPORT

SenderBaseのデモ

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



IRONPORT