迷惑メール対策
DNSBLとどう付き合っていますか？

株式会社グローバルネットコア
青田 英雄

アジェンダ

- DNSBLのおさらい
- 当社メールサーバへの導入
- DNSBLに登録されちゃった
- ネットワーク構成の変更
- まとめ

DNSBLのおさらい

DNSBLのおさらい

- DNSBL
  - DNS(-based) Black List
    DNS(-based) Block List
    DNS(-based) Blackhole List など諸説あり

    ※当社のホームページでは
    「DNS-based Blackhole List」と記載しています

- 迷惑メール(スパムメール)の中継・発信元のIPアドレスをまとめ、メール受信サーバが参照して、受信拒否等の対策に役立てるためのリスト

- リストの公開やサーバからの問い合わせにはDNSの仕組みやプロトコルが利用されている

- メールサーバでメールを受け付けると
  - ① その送信元のIPアドレスがDNSBLに含まれているかどうかを確認
  - ② 含まれていれば接続を拒否
  - ③ 含まれていなければメールを受け取り転送する

- デメリットも
  - 正常なメールを受信できない事がある
  - 共有ホスティングサーバにて、ある1ユーザーのSPAM配信により登録されたために、そのサーバーに同居する全ユーザーに影響を与えてしまう
  - 動的IPアドレス
  - リストの信頼性
  - 運営ポリシーの不透明性 など

- 主なDNSBLサイト
  - SPAMCOP
  - spamhaus
  - Barracuda
  - RBL.JP などなど

●一度に多数のDNSBLを確認できるサイトもあります

http://www.dnsbls.com/

23のDNSBLをチェック可能

[218.223.38.126] RBL/DNSBL List Check

		http://www.spamcop.net	218.223.38.126 is not listed in bl
Not Listed	dnsbl-1.uceprotect.net	http://www.uceprotect.net/en/index.php	218.223.38.126 is not listed in dr
Not Listed	dnsbl-2.uceprotect.net	http://www.uceprotect.net/en/index.php	218.223.38.126 is not listed in dr
Not Listed	dnsbl-3.uceprotect.net	http://www.uceprotect.net/en/index.php	218.223.38.126 is not listed in dr
Not Listed	sbl.spamhaus.org	http://www.spamhaus.org	218.223.38.126 is not listed in sb
Not Listed	xbl.spamhaus.org	http://www.spamhaus.org	218.223.38.126 is not listed in xb
Not Listed	zen.spamhaus.org	http://www.spamhaus.org	218.223.38.126 is not listed in ze
Not Listed	pbl.spamhaus.org	http://www.spamhaus.org	218.223.38.126 is not listed in pb
Not Listed	dialups.mail-abuse.org	http://www.mail-abuse.org	218.223.38.126 is not listed in di
Not Listed	dnsbl.njabl.org	http://www.njabl.org	218.223.38.126 is not listed in dr
Not Listed	dnsbl.sorbs.net	http://www.sorbs.net	218.223.38.126 is not listed in dr
Not Listed	dul.dnsbl.sorbs.net	http://www.sorbs.net	218.223.38.126 is not listed in du
Not Listed	misc.dnsbl.sorbs.net	http://www.sorbs.net	218.223.38.126 is not listed in m
Not Listed	smtp.dnsbl.sorbs.net	http://www.sorbs.net	218.223.38.126 is not listed in sn

http://whatismyipaddress.com/blacklist-check

78のDNSBLをチェック可能

minute for the checks to complete.

Blacklist Status

- access.redhawk.org
- bl.shlink.org
- bl.spamcop.net
- blackholes.wirehub.net
- block.dnsbl.sorbs.net
- bogons.cymru.com
- cbl.abuseat.org
- dev.null.dk
- dialups.mail-abuse.org
- dnsbl.abuse.ch
- dnsbl.anticaptcha.net
- dnsbl.dronebl.org
- dnsbl.kempt.net
- dnsbl.tornevall.org
- duinv.aupads.org
- dnsbl-3.uceprotect.net
- dul.ru
- hil.habeas.com
- http.dnsbl.sorbs.net
- ips.backscatterer.org
- b.barracu
- bl.spamcannibal.org
- bl.tiopan.com
- blacklist.sci.kun.nl
- blocked.hilli.dk
- cart00ney.surriel.com
- cblless.anti-spam.org.cn
- dialup.blacklist.jippg.org
- dialups.visi.com
- dnsbl.ahbl.org
- dnsbl.antispam.or.id
- dnsbl.justspam.org
- dnsbl.sorbs.net
- dnsbl-1.uceprotect.net
- dnsbl-2.uceprotect.net
- dul.dnsbl.sorbs.net
- escalations.dnsbl.sorbs.net
- black.junkemailfilter.com
- intruders.docs.uu.se
- korea.services.net

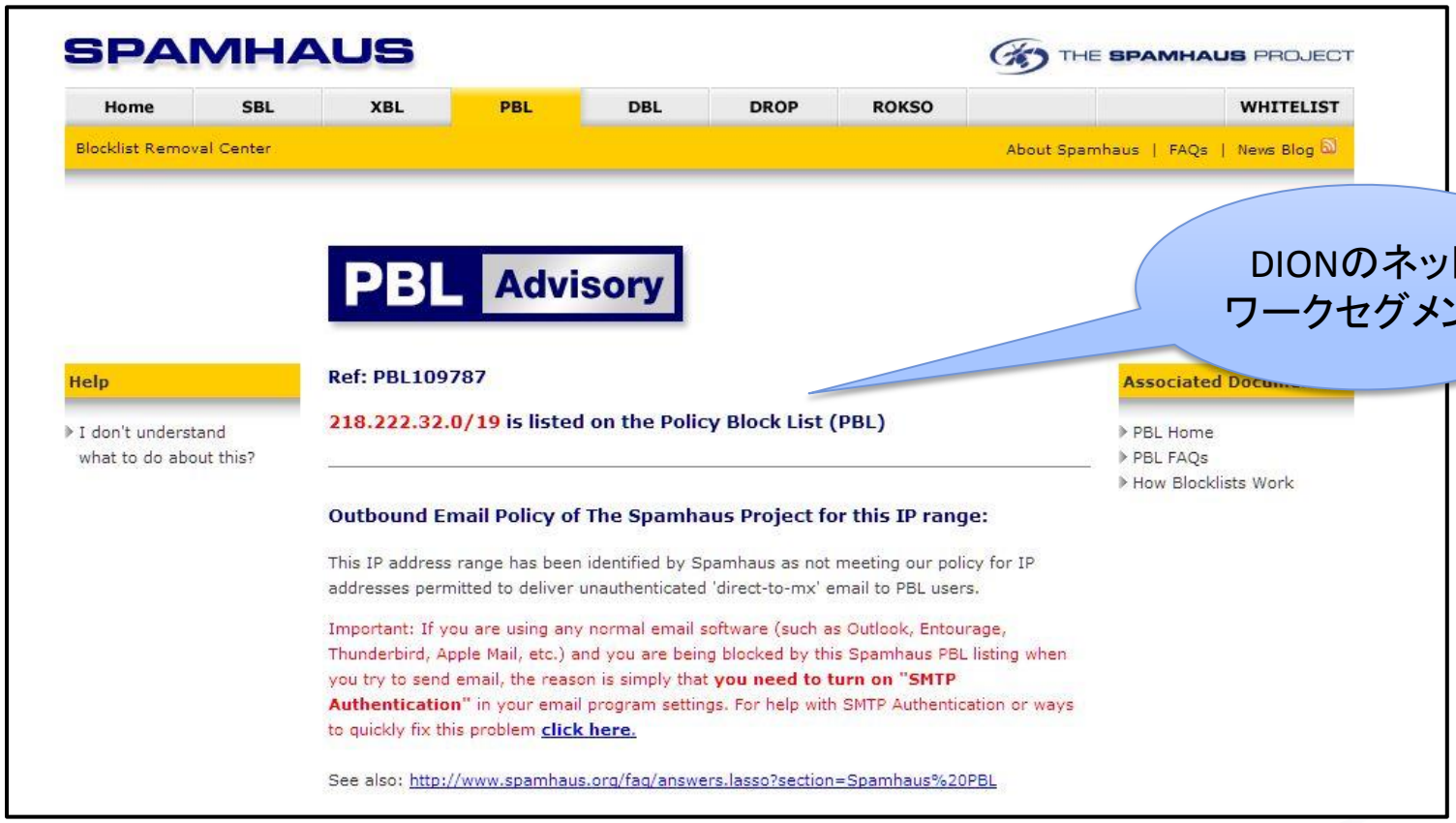
当社メールサーバへの導入

導入前の検証

- 検証方法
  - 特定のメールサーバで、各DNSBLを設定し、10分間で送信されたメール数と、DNSBLによりRejectされた数を調査

DNSBLサイト	配信数	Reject数	Reject率	特徴
sbl.spamhaus.org	2596	6	0.2%	過去にspamが配信されたIPアドレスのリスト 人の手による管理
xbl.spamhaus.org	2545	458	17.9%	管理しているメールサーバで観測されたIPアドレス
sbl-xbl.spamhaus.org	2838	623	21.9%	sblとxblを合わせたもの
pbl.spamhaus.org	2347	1224	52.1%	メールサーバで使用しているIPアドレス以外のリスト（エンドユーザIPアドレス範囲）
zen.spamhaus.org	2321	1341	57.7%	上記の全部
bl.spamcop.net	2288	140	6.1%	

●pbl.spamhaus.orgの登録例



当社メールサーバへ導入

- 迷惑メール対策として、2007/11に導入
- 当社で運用しているメールサーバ全台に一斉適用
- 参照先DNSBLは次のものに決定
  - bl.spamcop.net
  - sbl-xbl.spamhaus.org

導入後の効果

- ある運用担当者Tさん

「強力だなぁ・・・3～4割程度のセッションが落ちてる・・・・ 」
「バウンスメールも激減・・・(^^;;; 」

※あくまでこの担当者の主観によるものです。

定量的にお見せすることのできるデータは残っていませんでした

やっぱり問題点も

- 外部（他事業者）のメールサーバがDNSBLに登録されたことにより、当社のお客様が相手先からのメールを受信できないという問い合わせが増加

（2011/4～2012/7）

日付	顧客名	問い合わせ内容	登録されたドメイン名やISP
2011/4/18	株式会社	メールを送るとはじかれる	
2011/8/27	株式会社	メールがスパム扱いされる	
2011/11/28		からのメールが受信できない	
2011/12/13		スパムとなってメールが届かない	
2012/3/7		一部のメールが届かない	
2012/3/13	株式会社	メールが送れない	
2012/3/14		特定の方からメールが届かない	
2012/3/16		特定の方からメールが届かない	
2012/3/23		特定の方からメールが届かない	
2012/4/27		特定の方からメールが届かない	
2012/6/1		メールが届かない	
2012/6/12		特定の方からメールが届かない	
2012/6/29		メールが届かない	

時にはクレームになったり

お客様　「取引先からの大事なメールが届かない!!どうなっているんだ」

（調査してみると相手のメールサーバがDNSBLに登録されている）

サポート「送り元のメールサーバが、スパム関連のブラックリストに登録されていることが原因です。
お取引先様のほうから、ご利用のプロバイダーへ相談していただくようお伝え下さい。」

お客様　「よく分からないから、お宅でなんとかしろ!!」

さらに身内からも・・・

担当営業「お客様からクレームになってるよ!なんとかしろ!!」

メール配信遅延障害と監視システム

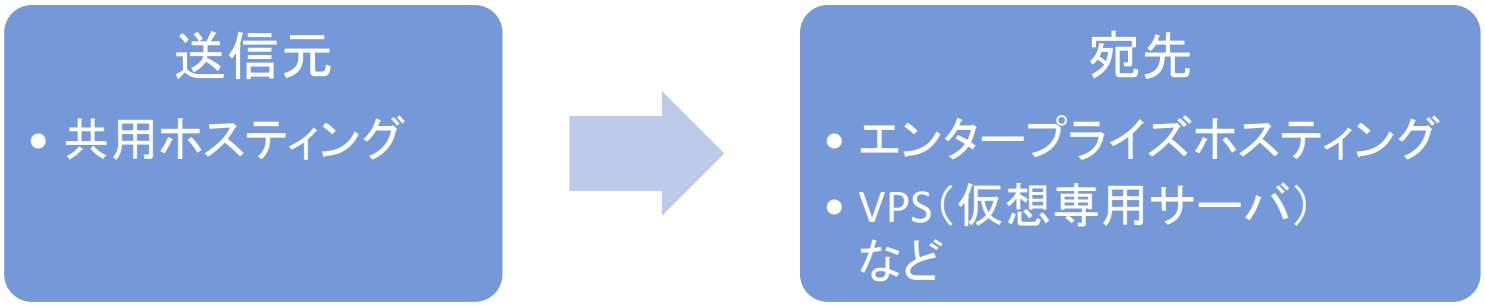
DNSBLに登録されちゃった

2012/7 大規模なメール障害発生

- 共用ホスティングで利用しているロードバランサのIPアドレスがspamhausに登録される

① spamhausを参照している外部のメールサーバにメールを送れない

② 自社の他サービスのメールサーバにもメールを送れない



障害時の対処内容

① spamhausに解除申請

申請からおよそ2時間後に解除

② 当社で管理しているすべてのメールサーバへ、ロードバランサのIPアドレスをホワイトリスト登録

自社の他サービスへの影響は即時解消

その後の対応

- 再発防止
  - 自社のメールサーバ同士への配信障害については、ホワイトリスト登録したため、再発のリスクはなし
  - 自社管理のメールサーバが、DNSBLに登録されてしまうことは防ぎきれない

DNSBLに登録された場合、いち早く検知する仕組みが必要

DNSBL監視を導入

- DNSBL監視システムを構築
  - チェック対象DNSBL
    - ✓ zen.spamhaus.org
    - ✓ bl.spamcop.net
    - ✓ short.rbl.jp
    - ✓ dnsbl.sorbs.net
    - ✓ cbl.abuseat.org
    - ✓ abuse.rfc-ignorant.org
    - ✓ barracudacentral.org
    - ✓ db.wpbl.info
    - ✓ black.junkemailfilter.com
    - ✓ bl.mailspike.net
    - ✓ psbl.surriel.com
    - ✓ ubl.unsubscore.com

DNSBL監視を導入

- 確認するIPは当社管理のメールサーバ
- チェック間隔は 10分
  - 2014/5 一部のサーバについては1日4回に変更
- DNSBL登録を検知した場合はメールとパトライトで通知
  - 夜中でも当番に連絡がはいり、対応してます・・・

DNSBL監視の運用

- DNSBLへの登録を確認したら
  - 登録の原因となったスパムメール配信が続いているのか確認
  - スパムメール配信が続いていればその対処
    - ✓メールアカウントを無効にする　等
  - 登録されたDNSBLへ解除の申請
  - 緊急時には、一時的に別のメールサーバにリレーさせたこともあります

その後DNSBLは廃止に

- DNSBLで弾かれる迷惑メールの割合が低下（導入当初の1/3以下）し、負荷軽減の効果が薄れてきた

- メールサーバの負荷軽減策として導入したが、サーバ数の増強やメールサーバソフトのパフォーマンスチューニング等により、DNSBL参照を廃止しても、障害を引き起こすような状況にはならないと思われる

- DNSBLを参照するメリットよりデメリットの方が大きくなってきた
  - メリット　　サーバ負荷軽減/メール受信総数の低減
  - デメリット　正常なメールを受信できない事がある
    クレームも相変わらず続いていた

2012/9　DNSBL利用を廃止

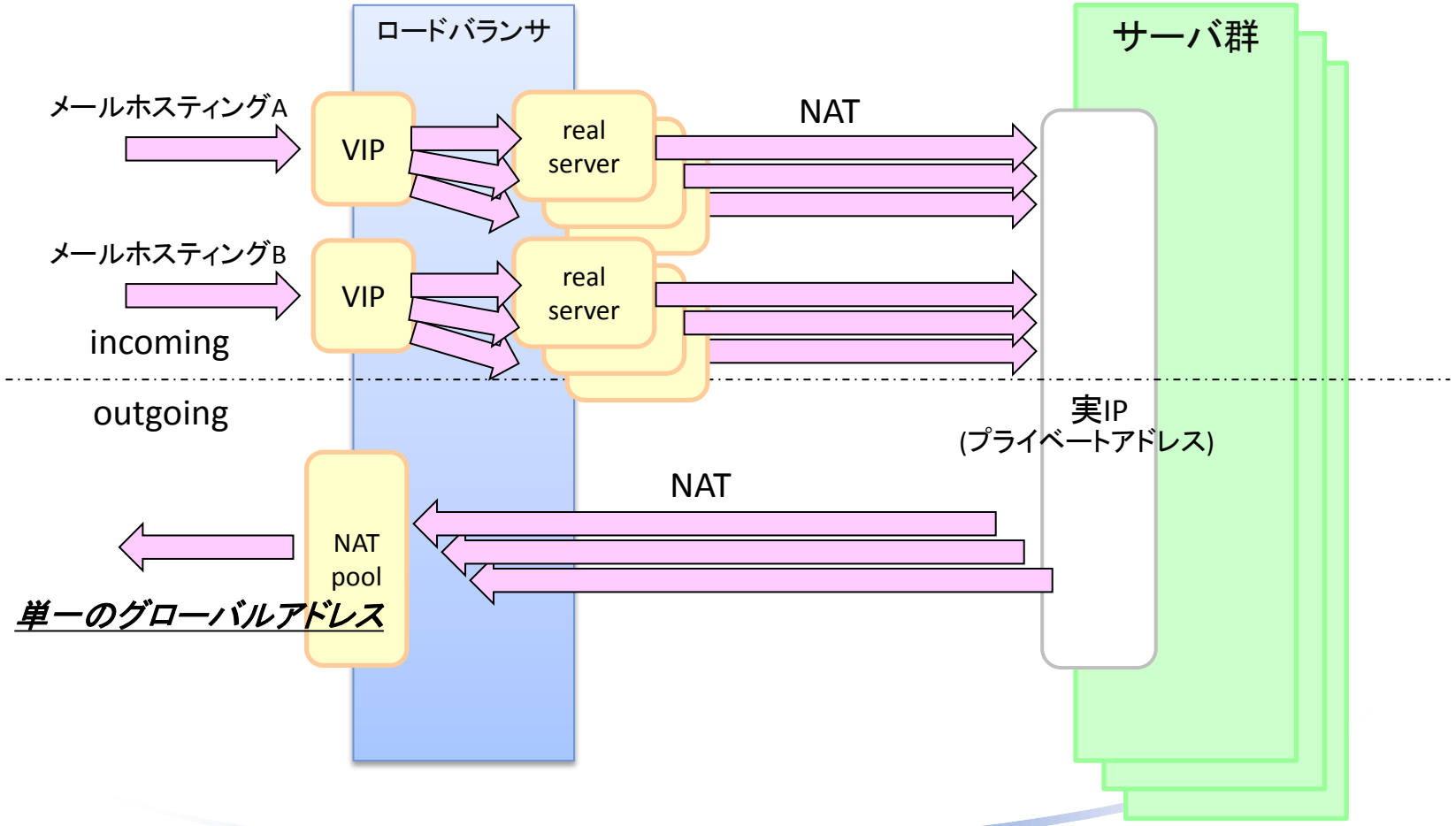
DNSBLに登録されないように

ネットワーク構成の変更

DNSBLへの登録はつづく

- 共用ホスティングを中心に、DNSBLに登録されることがたびたび続いている
- 専用サーバなら、原因と影響範囲が同じ顧客であるが、共用ホスティングでは他の顧客にも影響を与えてしまう💧
- そもそも、ネットワーク構成にも問題があり・・・
  - 共用ホスティングサーバ群は、一組のロードバランサの配下に設置

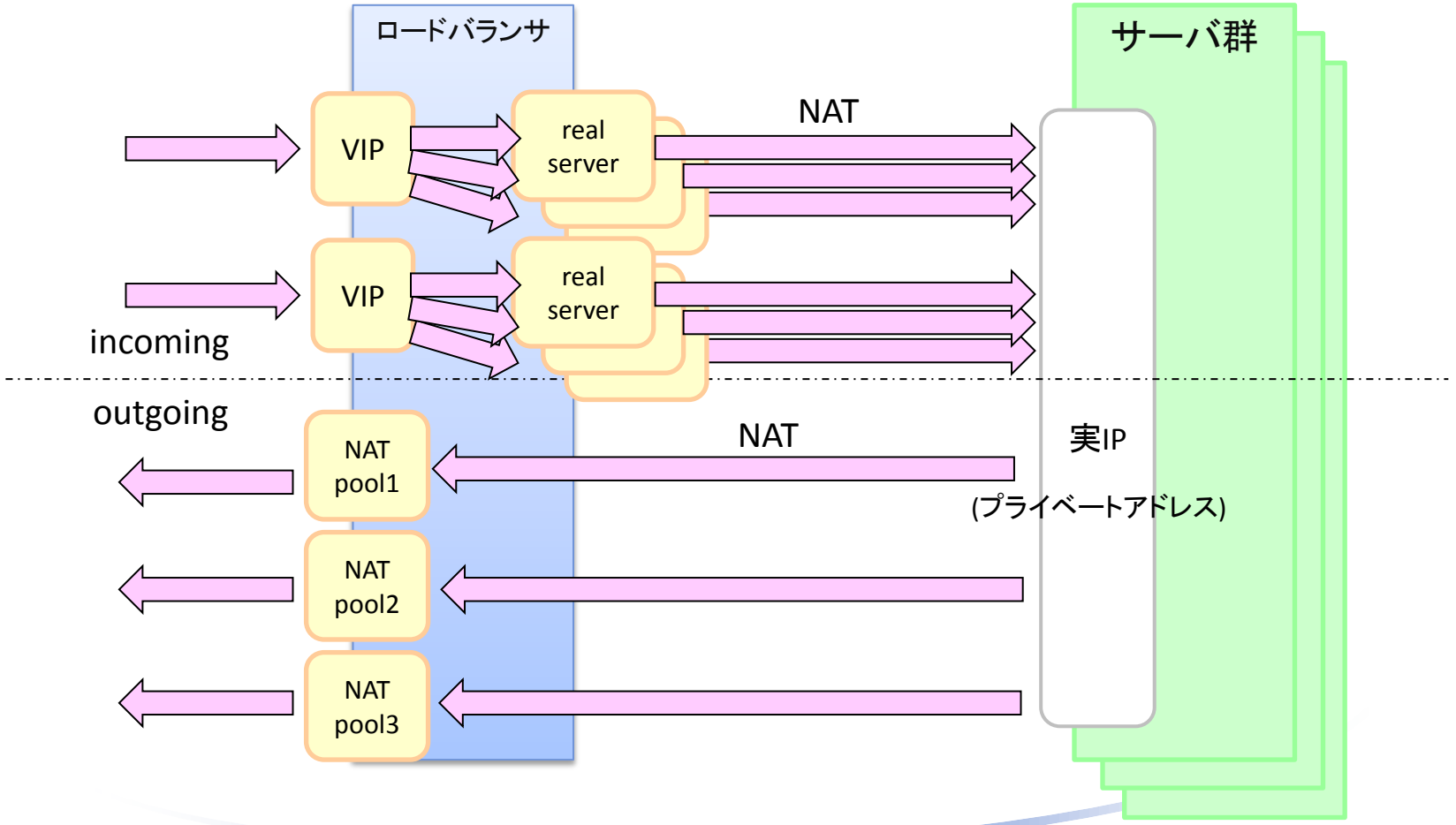
これまでのネットワーク構成



それなのでちょっとだけ構成を変えました

小手先の対応ですけど(^^;;

変更後のネットワーク構成



- この対応により
  - ① DNSBL登録リスクを分散
  - ② 影響範囲の局所化
  - ③ 原因の特定が今までより容易に

まとめ

まとめ

- 迷惑メール対策に使ってみたけど、弊害も多い
- 自分達が運用しているサーバが登録されちゃうことも
  - 登録されちゃった時どーしてます！？
    解除申請する/しない
    解除にお金が掛かるところもあります・・・
  - 登録されたかの監視までしているのって
    当社だけですか！？


Q&A