メールサーバの変遷

10年間のおさらい

株式会社ブロードバンドセキュリティ
取締役CTO
安藤一憲

会社紹介

- 良く言えば「玄人向け」サービスが主体
  - SoC (24/365のセキュリティオペレーションセンター)
  - セキュアメール(90万アカウント弱)
  - 脆弱性診断
    - ソースコード診断／Webサイト診断
  - PCIDSS(カードセキュリティ標準)
  - 高度セキュリティサービス事業
    - 新サービス開発
    - フォレンジック

BBSec
BroadBand Security, Inc.

時代背景

- このセッションでは主に2007年以降のメール周りの変化を取り扱います。
- まず、2007年までにだいたいどんな動きがあったかをおさらいしておきましょう。

迷惑メール対策諸団体の設立

- 1997年
  - CAUCE(任意団体)
- 2004年
  - M³AAWG(産業界レベル)
  - London Action Plan(政府機関レベル)
    - 現在はUCEnetと改称
  - IAJapan迷惑メール対策委員会
- 2005年
  - JEAG(ISP,携帯電話事業者)

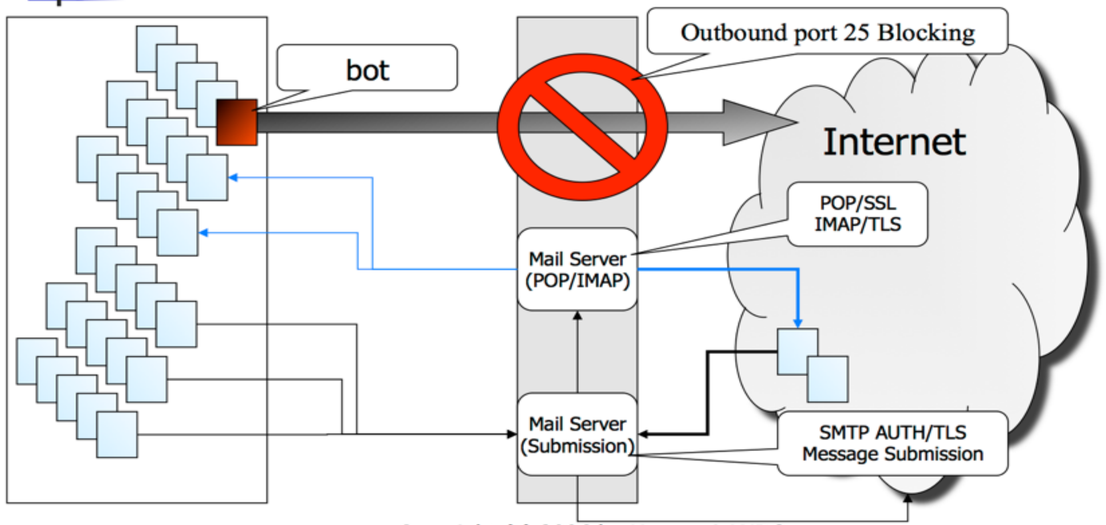
JEAG Recommendation

- 2006年2月初版発表
- 推奨したもの
  - OP25B
  - SPF Classic
  - DKIM 

2006年の安藤の講演内容

2006年12月のInternetWeekでのチュートリアル資料から

ISPによるOP25B



Copyright (c) 2006 by Kazunori ANDO
IW2006
11

認証破りへの対策

POP before SMTPの限界

- 気づかれずに感染している場合
  - POP before SMTPは危険
  - メールサーバから見えるIPアドレスを共用している場合はさらに危険
    - FW経由であるとか、PROXY経由であるとか
- 既に前世代のテクノロジ
  - 「なにもないよりはマシ」というレベル
  - パスワードもメール本文も平文で通信?
  - 早急にSMTP AUTHと経路暗号化を導入すべき

Copyright (c) 2006 by Kazunori ANDO
IW2006
15

2007年～2017年

- この10年の変化を振り返る
  - 第一部：迷惑メール対策
    - 日本とブラジルだけに普及したOP25B
      - ある意味、ガラパゴス。
    - 通信の秘密と送信ドメイン認証
      - 送信ドメイン認証が現在たどり着いたのは...
    - 特電法と各国の迷惑メール規制法
      - 海外との比較
  - 第二部：メールシステムに使われるテクノロジーの変化
    - ストレージの変化
    - アプリケーションのアーキテクチャ
    - IPv6周りの世界の掟

2012年～

- 安藤がM³AAWGに初参加
  - 最初は米国Sendmail社のCTOに誘われました
    - 初参加からRound Table Sessionで目立ちました
      - 「乗っ取りアカウント問題」のRound Table
      - ゲスト参加だったのに…
  - あれから5年、海外事情には明るいです
    - 関心の持ち方は他のM³AAWG参加者とも違うかも…
    - M³AAWGは米国大手ISP、メールとフィルタのベンダー、各国CSIRT、送信事業者等が集まったマルチステークホルダーなAnti-Abuse組織です。

第一部
迷惑メール対策

OP25B

10年後の真実

OP25B(国内事情)

- 主にBOTによるスパム送信への対策
  - JEAGによる推奨(2006年2月)
  - 「正当業務行為(違法性阻却事由あり)」の判断
    - 国内ISPが大挙して導入
- 一時、顕著なスパム受信減少の効果を得た
- スパム送信の手法が変化
  - 乗っ取りアカウント経由でSMTP認証を通った送信へ
    - OP25Bが効かない…
    - 徐々にスパムは元の送信レベルに戻った

OP25B(海外事情)

- 米国等では訴訟リスクのため実施できず
  - 大規模に実施したのは日本とブラジルだけ
- OP25Bが実施できなかった各国では**それ以外のスパム送信対策**に力が入れられた
- 日本と海外で「OP25B以外のスパム対策」への温度差が発生！

OP25B(成果)

- BOTからの単純なスパム送信の封じ込め
  - 知らない間に「加害者」にならない対策
  - スパムを「送信させない対策」
- SMTP認証の普及拡大
  - 送信サーバの機能分離
  - SPFやDKIM普及の土台になった
- 諸外国もOP25Bの成果は知っている

送信ドメイン認証

検証：10年でどこに到達したのか？

SPF

- **メール送信者(RFC821.From)のドメイン**の正しい**メール送信サーバのIPアドレス**をそのドメインのオーナーがDNS上に宣言する。分散型ホワイトリストの仕組み（**SPF Classic**)
- 2003年頃から議論、2006年4月にRFC4408として発行(experimental)。
- 2014年4月に**HELO/EHLOで宣言するドメイン**に対して先にSPFでの判定し、その後でRFC821.Fromの判定をするよう推奨するRFC7208(**SPFbis**)が発行されている(proposed standard)。

SPF

- メールが「送信者(RFC821-From)のドメイン、あるいは、HELO/EHLOで宣言されるドメインの正しい送信サーバのIPアドレスから送られている」とpass。
- ドメインのオーナーは認証を通らなかったメールの扱いを指定できる。
  - “+”: Pass : 通っても通らなくても配送する。
  - “-”: Fail : ドメインの使用を認めない。rejectする。
  - “~”:Softfail : FailとNeutralの中間。rejectしてはいけない。
  - “?”: Neutral : 通っても通らなくても取扱いを区別しない。

DKIM

- 公開鍵暗号技術を応用。RFC822.Fromを含むメールの内容に対して秘密鍵で署名、DNS上にある公開鍵で署名検証することで、そのドメインの正しい送信サーバから発信されたメールであることと、RFC822.Fromの改竄がないことを検証する技術。
- Yahoo Domain KeysとCISCO Idetified Internet Mailとの融合規格として2007年5月にRFC4871として発行された。
- 2009年8月にRFC5672でアップデート差分が公表された。
- 2011年9月にRFC6236がRFC4871のアップデートとして発行、さらに2013年6月に**STD76**に。
- DKIM=**D**omain**K**eys **I**dentified **M**ail

SPFとDKIMの目指したもの

- 送信者ドメインのなりすましの防止／受信側で送信サーバが確かにそのドメインの送信サーバであることが確認できる
- SPFもDKIMも厳密には「スパム対策」にはなっておらず「**なりすまし対策**」

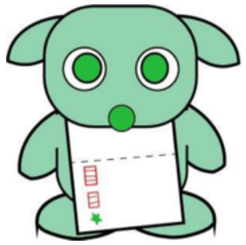
SPFとDKIM＝なりすまし対策

DKIM

ディーキいぬ

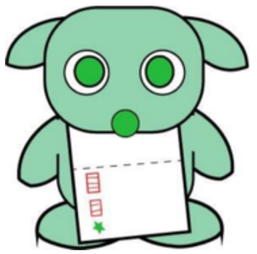
DMARC(送信側)

- 送信ドメインのオーナーは**SPFbis**もしくは**DKIM**に対応しなければならない
- 送信ドメインのオーナーはDMARCでfailしたメールの取扱いポリシーをDNS上に記述できる
  - failした割合やメールの内容をレポートしてもらうこともできる
  - いきなり p=reject とかやると従来型のメーリングリストから配送されるメールが巻き込まれる



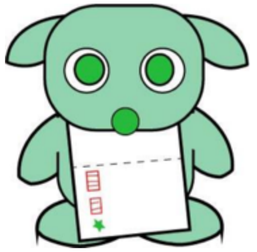
DMARC(受信側)

- 以下のいずれかが「RFC822.From」の送信者のドメインと整合すればpass
  - SPF(SPFbis)で認証された送信者のドメイン
  - DKIM(STD76)で認証された送信者のドメイン
  - Fromヘッダの送信者のドメインがサブドメインの場合は、AlignmentRuleが
    - strictだとfail
    - relaxedだとpass



DMARC(受信側)

- Authentication-Resultsヘッダへの記載
  - ラベリング dmarc=pass/fail
- DMARCがfailしたメールについて
  - 送信者ドメインのDMARCポリシーによるフィルタリング
  - 規格上は送信者のドメインが指定するアドレスにレポート送信することになっている



(国内事情)通信の秘密による制限

- 送信ドメイン認証による**ラベリング**
  - 正当業務行為でありISP等によって一括で実施可能
- 送信ドメイン認証による**フィルタリング**
  - ユーザの個別同意が必要…ISP等での一括実施は不可
- DMARCのfailureレポート
  - 「レポートに元メールの内容を含まないこと」

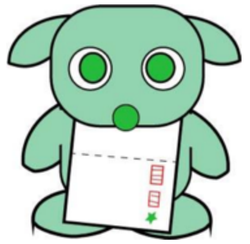
→「failした割合」のレポートはOKだけども実質的に「どのようなメールがfailしたか」のレポートは送信できない

通信の秘密

- 通信当事者以外による**通信内容の知得・窃用**を禁じている。総務省さんはこれを厳格に運用している。
- 世界的に見ると憲法で通信の秘密を規定しているのはドイツと日本くらいなのでどうしても他国と差が出る。

(海外事情)DMARCフィルタリング

- 例えば、KPN(オランダの元国営で民営化された通信会社)が送信proxyとDMARCフィルタリングを**全顧客ドメインに強制導入**し実際にフィッシングメールの劇的な削減に成功している



2013年には指摘され始めていた

https://japan.cnet.com/article/35041104/

日本では送信ドメイン認証による「フィルタリング」に個別同意が必要なため利用が促進されず、効果も実感できていない。

最近の調査結果でも...

CNET Japan ＞ ニュース ＞ 製品・サービス

「フィッシングはデータ漏えいより危険」--グーグル調査

Liam Tung （Special to ZDNet.com） 翻訳校正： 矢倉美登里 高森郁哉 （ガリレオ） 2017年11月13日 10時58分

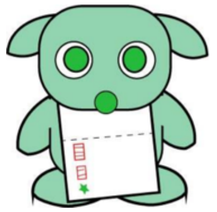
シェア 23 ツイート B! 4 Pocket 44 G+ 印刷 メール 保存 クリップ

PR | 世界４カ国の担当者が集合。なぜＳＰＡＲＣ　Ｍ１２が選ばれるのか？その理由に迫る

Googleは、「Gmail」アカウントの乗っ取りなどに関する1年間にわたる調査の結果を発表した。フィッシングはデータ漏えいよりもはるかにユーザーに対するリスクが高いことが明らかにされている。フィッシングによってより多くの情報が収集されるためだという。

https://japan.cnet.com/article/35110269/

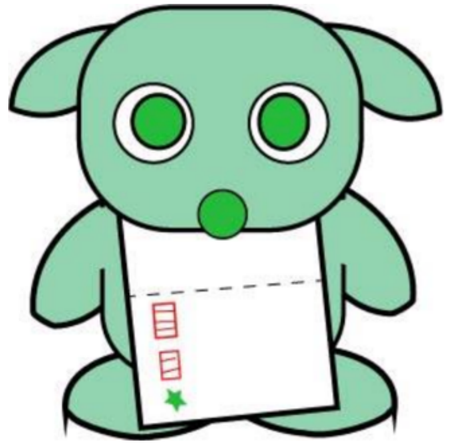
DMARCによるフィルタリングにはそれなりに利用価値はある...が、



DMARC＝フィッシングメール対策？

DMARC

ディーマーくんくん



DMARCの実装と技術詳細について

後で鈴木高彦君が喋る予定なので割愛

ARC

- 仕様議論中
- 中継MTA全てでDKIM様式の再署名とARC対象ヘッダについて再署名する、さらに各段階でARCの検証結果のヘッダを追加することで配送経過の認証のチェーンを形成する
- メーリングリストが救済される見込み
- 中継MTA全てでの実装が前提
  - 普及にはこれまでにない大きな課題がある

JIPDEC安心マークとBIMI

- 送信ドメイン認証の結果をわかりやすく表示する
  - JIPDEC安心マークはDKIMで認証されたドメインと企業実在DBを突き合わせて安心マークを表示
  - BIMIはマイクロソフトのメンバーが主導しており、DKIM/DMARCでの認証成功をその企業の小さなロゴで表示
  - 安心マークが3年先行していたので「一緒にやったら？」と提案→M³AAWGで進行中

受信フィルタの進化

- ウイルスフィルタ
  - 正当業務行為(違法性阻却事由あり)の判断
    - ISPで一斉導入・適用が可能に
    - この10年で徐々に採用するISPが増加していった
- スパムフィルタ
  - 「個別同意が必要」の判断
    - 国内ISPでの一斉導入は基本的に不可
    - 詳細な説明と「個別に有効／無効を選べる」ことが必要
    - 利用可能なサービスは増えたけれども利用は限定的

商用スパムフィルタの性能

- 他のフィルタ以上にアップデートがきめ細かく早い
  - 秒間隔でのアップデート
  - スパム判定正解率：99.9??%の争い
  - **スパムへの対症療法としては現状最も効果がある**
- ユーザー規模の拡大（世界では…）
  - 100万のオーダー(2007年)
  - 10億のオーダー（2017年）
- SNSサービスでも利用されている

送信事業者は何をしたか？

10年間で彼らが学んだこと

実際にとある送信事業者さんがやったことをまとめて頂いて資料作成しています

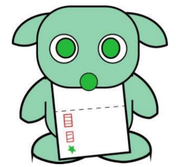
メール送信事業者の取組(1)

- 受信者にメールを受信してもらう努力
- M³AAWG Sender Best Common Practice Version 3の実装
  - 個人情報保護への対応
    - メールアドレス収集意図の透明化
    - オプトイン方式の改善
    - 登録削除方式の標準への準拠
    - データの透明化
    - データセキュリティ

メール送信事業者の取組(2)

- メール送信サービスとしての対応
  - 送信ドメイン認証への対応
    - SPF,DKIMは両方で認証が通るように整備

    - DMARC
      - » SPF,DKIM両方でpassするように整備
      - » ruaを記述しレポートメールを受信



  - STARTTLS対応

メール送信事業者の取組(3)

- メール送信する顧客の審査
- フィードバックループの整備
  - 簡易な購読解除方法の提供
  - 苦情窓口(RFC6449)と送信停止の連動
- NDR(配信不能レポート)の処理
  - アドレスリストの精査
- 全メール開封計測
  - 開封されないメールの改善
- Mailbox Provider提供ツールの利用
  - Microsoft - SNDS (Smart Network Data Service)
  - Google Postmaster Toolsの利用

メール送信事業者の取組(4)

- この10年間で
  - 現場の技術陣は「より良いメール送信事業者」になるためになまじのISPより努力してきた
  - 効果計測によって送信が多すぎると逆効果であることも把握
- 受信側からの実感
  - まともな送信事業者からのDoSのような暴力的な大量配信はほぼ見られなくなった
  - ルール・法律を守って正しく送信しましょう

この10年で世界的に最も効果があったスパム対策って何?

CASL(カナダアンチスパム法)

- 規制対象
  - **電子的に送受信されるあらゆるメッセージ**
    - テレックスやSNSのメッセージも対象
    - メール添付で送られるウイルスやマルウェアも規制
    - カナダで受信されるもの
- **厳格なオプトイン(事前承諾)**
- **超高額罰金**
  - カナダ以外の海外の送信者にも**超高額罰金**
- 2015年７月施行

スパムが37〜40%減少…世界的にもスパム減少

CAUCE

カナダは2017年もG7諸国で最高の経済成長率を維持！(広告メールに厳格なオプトインを課しても経済にマイナスにはなっていない)

特電法（特定電子メール送信の適正化等に関する法律）

- 規制対象
  - SMTPで送受信されるメール
  - 電話番号を送受信に用いるSMS
- 2002年制定(当初はオプトアウト方式)
- 2005年改正で刑事罰が規定された
- 2007年改正で**オプトイン方式**を導入
  - 特定電子メールを送るには受信者の「事前承諾」が必要
    →世界標準に沿った考え方
  - ガイドラインに**抜け道**として「名刺の授受は事前承諾とみなす」が入っている

特電法の見直しの必要性

- CASLは特電法も参考にして作られた
  - 大きなスパム削減効果を得ている
  - あんなに厳しくてもカナダ経済への悪影響は認められない
- 特電法で大きくスパムが減らなかったのはなぜか？
  - **罰金がショボい**
    - スパム送信者の儲けの方が大きい
  - **行政指導の件数も少ない**
    - 実質やったもん勝ち？
  - **事前承諾と言いながら抜け道がある**(徹底していない)
    - 名刺の授受は特定メールの事前承諾が前提とは限らない
    - 名刺の授受は自己紹介の一環なので自己紹介に弊害が出る

さらなる課題発生

- スパムは減少したが被害額は増加している
  - 直接金銭的な被害に結びつくような事例増加
  - アカウントの乗っ取り／リスト型攻撃
  - フィッシング
  - SCAM(スキャム)
  - マルウェア・ランサムウェア配布
  - 全体としては「悪質化」していると見るべき

【課題】リスト型攻撃

- 2012年終盤くらいから問題化
  - リスト型攻撃で乗っ取られたアカウントからSMTPAUTHを経てスパムが送信される
- IDの持つレピュテーションの乗っ取りとスパム配信
  - **送信ドメイン認証では配信を抑止できない**

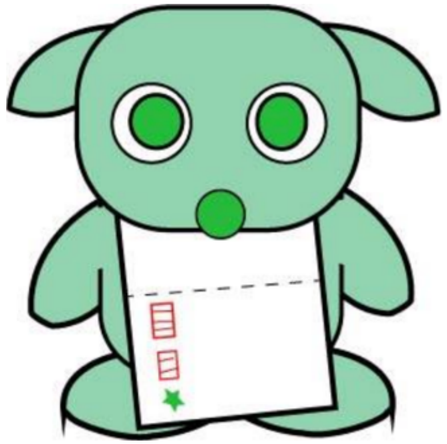
- 他のサービスやユーザ側PCからユーザ名とパスワードが漏れるケースもあり、**メールサーバでの対策だけでは解決できない**

ちょっと良くなった

DMARC＝なりすまし対策

DMARC

ディーマーくんくん



メールサーバ側で見えるのは

Brute-force攻撃と乗っ取られたアカウントの不正利用

アカウント乗っ取り対策

- 不正利用や攻撃判定のためにアクセスログ利用
  - 通信の秘密の侵害になるとされてきた
    →通信事業者の対策が及び腰になる
  - だが他に方法はない
- 2014年７月
  - 総務省「不正利用の蓋然性の高いアカウントのSMTP認証の一時停止、パスワード変更依頼」と「大量のSMTP認証失敗に対して該当IPアドレスからのSMTP認証を停止すること」について**正当業務行為(違法性阻却事由あり)**と見解を示す
  - 各ISPで対策が進む

【課題】Pervasive monitoring

- 主に各国政府機関による常時全数監視
- スノーデンの告発(2013.06)により存在が明るみに
  - 米当局がスノーデンの利用していたメールサービスに電子証明書の秘密鍵の提出を要求

    → **通信内容記録の暗号化を解くのがその目的であることは明白**
  - スノーデン以外のユーザの送受信も復号される
- 「やっぱ通信内容を記録してるんじゃんかよ！」
  - RSA方式の**鍵交換プロトコル**の限界
  - Perfect Forward Secrecyの担保できる鍵交換へ
    - **DHE/ECDHE**(鍵交換に使い捨て一時鍵を用いる方式)
  - メールサーバ間の送受信も経路暗号化する流れに

メールサーバ間の経路暗号化

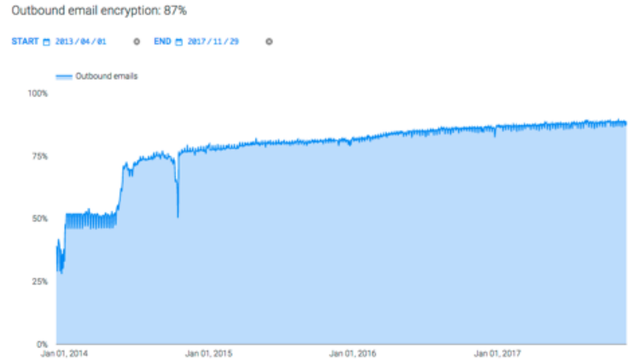
- Gmailが送受信するメールの経路暗号化率

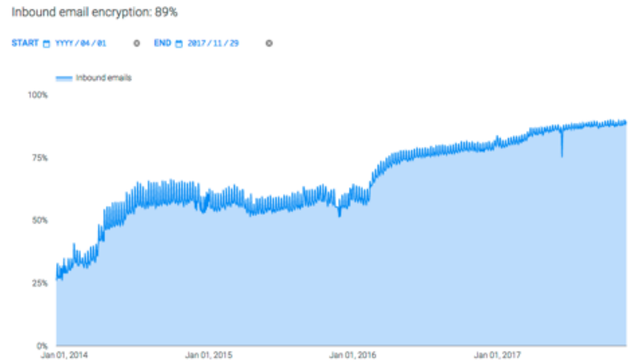
(Google透明性レポート：2014年6月)

  - 送信：65%
  - 受信：50%

(同：2017年11月現在)

  - 送信：89%
  - 受信：88%





日本では経路暗号化への関心が薄い

- 「通信の秘密」の存在
  - 日本では通信当事者以外の第三者が通信内容を知得・窃用することがそもそも違法
  - 外国で盗聴されても問題ない？
    - 多くの通信が海外を回っている事実
    - 例えばBGPが事故ったら簡単に海外回るけど？

米国だけの話？

- 日本
  - 改正通信傍受法
  - 特定の犯罪捜査に限定
  - 裁判官から傍受令状をもらう必要がある
- 英国
  - もともと盗聴を是としている国。令状なし。通信事業者は最長1年のデータ保存義務。
- オランダ
  - 法執行機関に令状なし盗聴とデータの3年保存を認める盗聴法を可決。
- 欧州の二面性
  - 一般向けには「個人情報保護は基本的人権」
  - 軍の諜報と法執行機関の犯罪対策は個人情報保護とは別枠

BGP hijacking

- 日常的に発生している
- 意図的と思われるものが含まれている
  - 盗聴目的？
  - メタデータ収集目的？
- スパム大量送信に使われるケースもある

SMTP-STS

- draft-ietf-uta-mta-sts-00
  - DNSSECの利用：DNSポイゾニング対策
  - DANE TLSAの利用：偽電子証明書の排除
  - **経路暗号化の利用を強制**することができる
    - 経路暗号化に失敗したメールはreject/report
      - 通信の秘密でこのレポートも問題になりそう
    - ポリシーはDNSで公開
- 現状ではまだ仕様が固まったとは言い難い状態
- 盗聴されたとしてもメタデータ以外渡さない

【課題】SCAM

- 主に**スピア型**で経理担当者を騙してお金を振り込ませる「**経理担当狙いのオレオレ詐欺メール**」
- 社長になりすまして「今度、A社のこの事業を買ったので◯◯億円、このA社の口座に振り込むように」とやられる
- アカウントの乗っ取りを併用するケースもある
  - IMAPサーバから普段のメールを取得する
  - 送信アカウントも「ホンモノ」だったりする
  - 複数の登場人物を使った劇場型も報告されている
- 2016年に**被害額で16倍以上の増加**
- 各国が警告サイトを開設


GOV.UK

Home › Citizenship and living in the UK › Living in the UK, government and democracy

Avoid and report internet scams and phishing

Report misleading websites, emails, phone numbers, phone calls or text messages you think may be suspicious.

Don't give out private information (such as bank details or passwords), reply to text messages, download attachments or click on any links in emails if you're not sure they're genuine.

Misleading websites, emails and phone numbers

Some websites, emails or phone numbers can look like they're part of an official government service or that they provide more help than they actually do.

【課題】Technical Support SCAM

- 製品／サービスの技術サポートを装ってマルウェア感染に誘導する
  - 製品のサポートメールはその製品のユーザであれば受け取れるので文面を真似しやすい
    - 乗っ取ったアカウントの併用は必要ない
- 直接金銭被害にはならないケースがある

対策	効果	範囲	通信の秘密	
			正当業務行為	個別同意が必要
OP25B	SMTPAUTH普及・動的IPアドレスからの送信抑止	ISP/携帯事業者	○	
SPF	なりすまし防止	全ドメイン	ラベリング	フィルタリング
DKIM	なりすまし防止	全ドメイン	ラベリング	フィルタリング
DMARC	フィッシングメール防止	全ドメイン	ラベリング	フィルタリング
RBL	攻撃軽減	全ドメイン		○
スパムフィルタ		全ドメイン		○
ウイルスフィルタ		全ドメイン	○	
アカウント乗っ取り対策	なりすまし防止	全ドメイン	○(アクセス履歴の利用)	
SMTP-STS	経路暗号化利用の徹底	全ドメイン	N/A	N/A

対策	SCAM(スピア)	Tech Support SCAM(スピア)	フィッシング（バラマキ）	国家による盗聴	BGPハイジャック
OP25B	△	△	△	×	N/A
SPF	○	○	○	×	×
DKIM	○	○	○	×	○
DMARC	○	◎	◎	×	×
RBL	△	△	△	×	×
スパムフィルタ	○	◎	◎	×	○
ウイルスフィルタ	△	△	△	×	×
アカウント乗っ取り対策	◎	△	△	○	×
SMTP-STS	○	○	○	◎	◎

第２部
メールシステムに使われる
テクノロジーの変化

全体としての変化

- SMTPAUTHの普及
- POPからIMAPへ
  - ストレージ
  - サーバプログラム
- IPv6への対応
  - サーバには逆引きDNS登録が必要！

送信認証(SMTPAUTH)

- OP25B普及と同時進行
  - Digest-MD5/CRAM-MD5
    - MD5(128bit hash)はこの１０年で危殆化
    - 代わりの仕組みは作られていない
  - クライアント接続の経路暗号化が必須に
    - 日本では経路暗号化の意識低いがやらないとダメ
    - Wifiで飛ぶケースも多い(KRACKs問題)

POPからIMAPへ

- POPの場合
  - メールは逐次クライアントにダウンロード
    - そんなにストレージ容量は食わない
- IMAPの場合
  - メールはメールサーバに蓄積
  - 検索等の機能もメールサーバ側に実装
    - ストレージ容量／アクセスとCPUリソースの激増

落ちなくなったメールサーバ

- 携帯事業者
  - ここ何年か総務省への障害報告のない会社がある
- 大手クラウド事業者のメール
  - 障害は起きても人為ミスかネットワーク障害
- 裏にあるのは
  - データ喪失に対する信頼性の桁違いの向上
  - 機器障害がサービス障害に結びつかない構成

ストレージの変化

- 旧来型のエンタープライズストレージ
  - いくら高性能でもスケールに限界
    - コントローラのCPUの個数
    - キャッシュ容量の上限
  - データ消失に対する信頼性にも限界
    - RAIDでの冗長(5,6,10…)
    - RAID6で99.96%
  - SPOF(コントローラ、キャッシュメモリ)

ストレージの変化

- IMAPサーバのストレージ要件
  - POPサーバと比較にならないくらい長期間データを安全に保持できなければならない
  - 容量もPOPサーバから激増
  - アクセスも規模にスケールする必要がある
    - 単純に容量だけが増えれば良いわけではない
    - バックアップストレージとの違い

分散オブジェクトストレージ

- クラウド由来の技術
  - サービスとしてはAmazon S3が有名
  - 鍵は「**筐体間イレイジャーコーディング**」
    - データ消失に対する信頼度の劇的向上
    - スケールアウト構成が取れる
      - アクセス処理能力もスケールする
    - Geo-Redundant構成にも対応できる
    - 必要に応じて冗長方式／信頼度を選択できる
  - 大きな障害要因は「人為ミス」にほぼ集約

分散オブジェクトストレージ

- サーバが故障しても止まらない
  - 稼働させながら復旧できる
- ソフトウェアや機材のアップデートについても稼働させながらの実施が可能
  - H/Wの世代を越えてデータを保持できる
- サービスの継続稼働能力が著しく向上

初期の実装

- IMAPサーバで分散オブジェクトストレージを利用する実装が出てきた
  - 導入するにはサーバアプリケーション側で分散オブジェクトストレージに対応する必要がある
- 分散オブジェクトストレージを利用するもののアプリ側にまだSPOFを抱えた実装
  - 弊社ではそのSPOFを踏んで大障害発生
    - データ喪失はありませんでした
      - 分散オブジェクトストレージなので…
    - ご迷惑をおかけしたお客様申し訳ございませんでした
      - 新型の稼働が間に合いませんでした…

新たな実装

- 「IMAPサーバ自体にもオブジェクトストレージのこれらの特徴が欲しい！」
  - サーバが故障してもサービスが止まらない
    - 稼働させながら復旧できる
  - ソフトウェアや機材のアップデートについても稼働させながらの実施が可能
    - 世代を越えてデータを保持できる
  - サービスの継続稼働能力が著しく向上

Dovecotとは？

- 言わずと知れたIMAPサーバの世界最大手
  - フィンランドの会社
- ドイツの大手ISPでStateless構成の実績
  - ただし分散オブジェクトストレージ未対応
  - 一歩進めれば目的のものが得られる状況
- **思惑一致w**

ぽちっとな

- Dovecot Pro Stateless IMAP server
- 弊社サービスで**サーバ構築案件化**
  - テスト後サービス投入(2014年11月)
    - 分散オブジェクトストレージは2年前に導入済
  - 最初は全ユーザのうちの一部。徐々に拡大。
- ちょっと意味のある仕事ができたかも

Dovecot Proの現在

- 現在の実装ではさらにスケールが改善されている
- 世界中の巨大IMAPサーバで採用が進んでいる
  - **3000万アカウント超級**のサーバが複数稼働
  - 国内でも弊社より大規模なサーバが複数稼働
  - DovecotのIMAPサーバにおける世界シェアが75%に
- Dovecot Proを使っている世界の通信事業者との会話
  - 国内大手ISP:「わしら障害起こすと総◯省に報告だからなぁ」
  - 海外巨大ISP:「お前のとこも同じなの？」
  - 弊社：「同じ」
  - 海外巨大ISP: (それで日本の連中はこんなサーバが欲しかったのか！w)

実際に得られたもの

- 世界レベルのサービス安定性
  - クラウド由来の技術応用なので当たり前と言えば当たり前
- いままで通りのきめ細かなサービス
- 増加するmailboxユーザ数
  - GmailさんやOffice365さんがあるのに増加
    - Gmailさんは利用するのに別のメールアドレスが必要
- **定時で帰ろうと思えば帰れる運用w**

向き合おう”グローバル”インターネット

実際に世界と日本の間に
どのような齟齬が発生しているのか？

IPv6

- IP総トラフィックの20%に到達
  - ComcastやGmailなどはIPv6で受信している
  - メールはIPv6化にあたり独自に制約を追加
    - スパム対策(受け取らない対策)
  - 米国大手が先行したためIETFではなく

    M³AAWG→NISTによって「掟」が決まった

IPv6では(世界事情その1)

- 実際構築すると「メールサーバに**DNS逆引きエントリー**がないとメールを受け取ってもらえない」
- どこに書かれているか？
  - NIST SP800-177『Trustworthy email』(2016.09)
    - 「Email anti-abuse consortiums recommend that enterprises should make sure that DNS reverse trees identify the authoritative mail servers for a domain [M3AAWG].」
  - 参照先：M³AAWG Policy Issues for Receiving Email in a World with IPv6 Hosts(2014.09)

IPv6では(世界事情その2)

- IPv6のメールサーバでメールを受け取ってもらうのに必須な条件
  - メール送出サーバのDNS逆引きエントリー
  - 送出メールがSPFbisあるいはDKIMでpassすること
    - DMARCではないが、DMARCにしようという議論はある
  - WHOISで引けるドメイン
- 結果としてできるのは「スパムを受信しない」環境
  - 送信サーバの固定
    - 固定サーバでSMTPAUTHを義務化するとなお良い
  - 送信ドメイン認証フィルタの必須化

IPv6での制約(国内事情)

- IPv6メールの世界との差異
  - 世界で実施されているのは「受け取らない」施策
  - 「通信の秘密」の制約
    - 国内ではOP25Bで「送信させない」を実現
    - 一方、通信事業者は送信ドメイン認証で「受け取らない」ためのフィルタリングは一斉実施できない
    - 海外・国内で送受の対策がバランスしていない
      - 「送れないけど受け取る」→加害者にはならないが被害者にはなりやすい

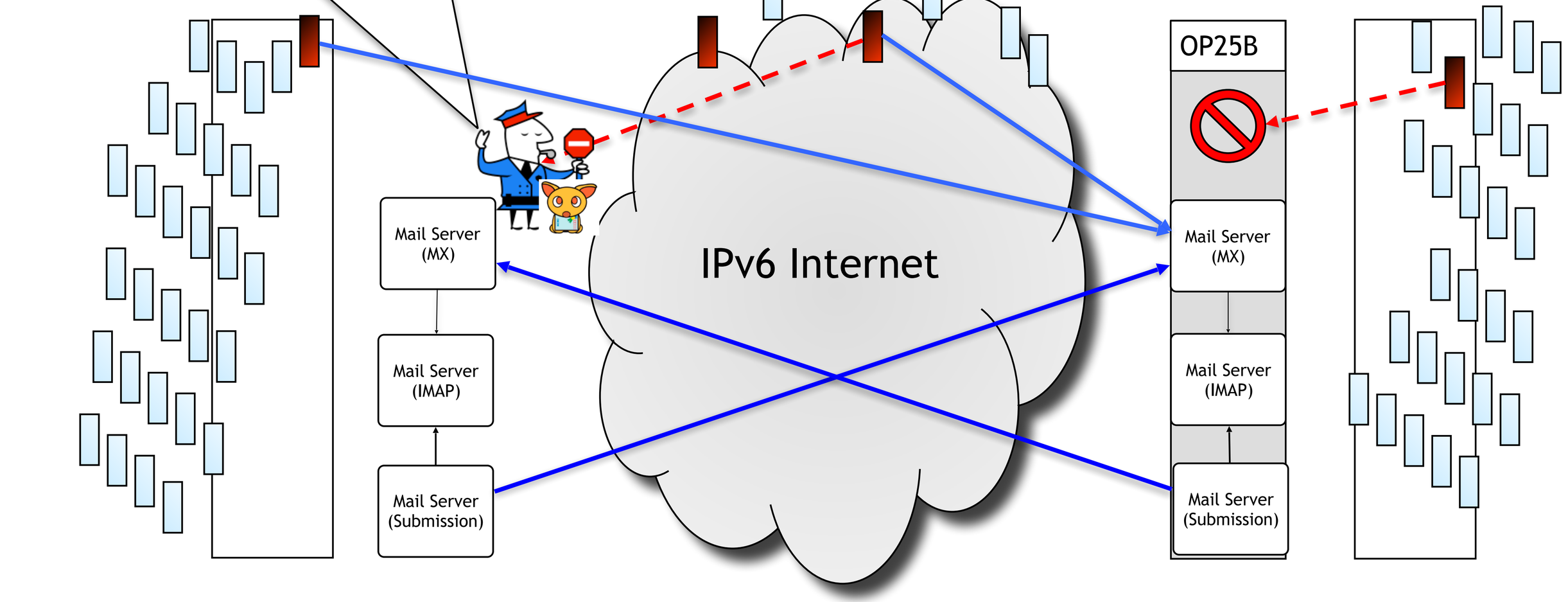
IPv6での状況

米国/NIST SP800-177

DNS逆引きと送信ドメイン認証でフィルタ

日本/総務省規制

送信ドメイン認証フィルタは個別同意が必要



GDPRとWHOIS

GDPR(欧州一般データ保護規則)

- 来年5月25日施行予定
- PIIを保護
- WHOISで得られる情報はPIIだらけ
  - 現時点での観測では使えなくなる公算大
  - メール周りでもAbuse対策に使われているので産業界は使用継続を要望
- ICANNの調整能力不足？

世界との齟齬のまとめ

- 「インターネットはひとつ」という理念と各地域／各国の法律との間の齟齬が目立ってきている
  - GDPRとwhoisの問題などが典型
- 国内事情の最たるものは「通信の秘密」
  - 「出させない対策」の漏れは「ホスティング」
    - 通信事業者以外はOP25Bに参加しなかった
    - 海外から見てスパム発信源になっている可能性がある
  - 「受け取らない対策」の不備はIPv6で不利に
    - 世界のIPv6メールサーバでは送信ドメイン認証によるフィルタリングがデフォルトになっているが…

まとめ

- SPFは**某大手のSPFフィルタリング実施**で書かないとメールが通らないので普及
  - 変なことさえしなければDMARCまでpassできる状態に
- 弊社は他に方法がなかったので**2012年7月に乗っ取りアカウント対策**開始
  - 総務省の判断を待っているだけでは被害は防げない
- **「迷惑メール対策」はどれも銀の弾丸ではない**
  - むしろ、ひとつずつ問題を解決して行っていると見るべき