財団法人インターネット協会
第3回迷惑メール対策カンファレンス

ISPが送信ドメイン認証インバウンドチェックを行う際に考えられる手法と手順

2006年5月16日

財団法人インターネット協会　迷惑メール対策委員会
木村　孝 (ニフティ株式会社)

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

普及が進む送信ドメイン認証（送信側）

- @nifty 2005年5月11日　Sender-ID, DomainKeys
- Yahoo! Japan Yahoo!メールで2005年7月19日より　DomainKeys
- BIGLOBE 2005年11月30日より SPF
- IIJ IIJ4UとIIJmioで2005年12月21日よりSPF
- ＮＴＴドコモ　2005年12月7日よりSPF
- KDDI 、沖縄セルラー　EZweb, Dionで2005年12月よりSPF/Sender ID
- DTI　2006年2月21日より　SPF
- ウイルコム、ウイルコム沖縄　2006年3月15日よりSPF
- 関西マルチメディアサービス　ケーブルインターネットZAQ 3月22日より SPF
- ボーダフォン　2006年3月29日よりSPF

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

受信側（インバウンドチェック）の導入も進みつつある

- Yahoo! Japan　2005年9月13日　Yahoo!メールでDomainKeys認証結果を表示、検証結果を「Authentication-Results」ヘッダーに記述
- IIJ　2006年3月30日　IIJ4U、IIJmioで送信ドメイン認証フィルタ機能の提供を開始

  ユーザーが受信したメールのヘッダーに「Authentication-Results:」で始まる行が追加される。ここに送信ドメイン認証の結果がスコアとして「pass（認証成功）」「fail（認証失敗・送信元メールアドレスは詐称されている）」と いった形で記述され、メールの振り分けなどに利用できる。

  ラベリング

- 2005年12月　KDDI、沖縄セルラーは2006年度中を目処に送信ドメイン認証技術「SPF/Sender ID」を利用したメールフィルター導入を発表。

- BIGLOBEは受信対策として2006年夏までに送信ドメインが保証されていないメールを判別する機能を提供する予定。

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

おさらい

- ISPは電気通信事業者として、電気通信事業法上の義務が適用される。
- その中で最も重いのは「通信の秘密」（第4条）
- 通信の秘密の侵害には罰則が適用される。（事業法第179条、 2年以下の懲役又は百万円以下の罰金、第2項　電気通信事業に従事する者の場合は3年以下の懲役又は二百万円以下の罰金。未遂も罰）
- 機械的な処理あっても「通信の秘密」を侵害したことには変わりはない。
- 侵害とされないためには、以下の3つのいずれかの条件を満たす必要がある。
  - 当事者の同意がある
  - 業務上必要な「正当業務行為」
  - 緊急避難に該当する（刑法37条）

当事者の同意があれば秘密性はなく「違法」ではない。

これら2つを法律用語で「違法性阻却事由」と言う。

自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。

平成17年11月1日に施行された、（改正）「特定電子メールの送信の適正化等に関する法律」　（緊急避難そのものではないが、良く似た状況を表す表現の一例）
（電気通信役務の提供の拒否）
第十一条 電気通信事業者は、一時に多数の架空電子メールアドレスをそのあて先とする電子メールの送信がされた場合において自己の電子メール通信役務の円滑な提供に支障を生ずるおそれがあると認められるとき、その他電子メールの送受信上の支障を防止するため電子メール通信役務の提供を拒むことについて正当な理由があると認められる場合には、当該支障を防止するために必要な範囲内において、当該支障を生じさせるおそれのある電子メールの送信をする者に対し、電子メール通信役務の提供を拒むことができる。

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

インバウンドチェックについての従来の考え方

- 送信ドメイン認証のインバウンドチェックも広い意味でのフィルタリングに分類される。
- フィルタリングは通信の秘密に抵触するものなので、基本的に利用者（受信者）の個別※の同意（サービスの利用申込）が必要。
- 利用者の同意なしにフィルタリングを行うと違法となる。
- 常時適用されるフィルタリングには刑法37条にいう緊急避難は適用されない。
- フィルタリングをデフォルト・オンで提供するには、利用者毎に解除する機能を提供するなど、色々な条件を満たす必要がある。
- Yahoo!も認証結果を表示するだけで、認証に失敗したメールを排除している訳ではない。

※　約款や会員規約による合意は包括的合意としてみなされ、通信の秘密侵害に対する違法性阻却自由としては包括的合意では足りず、利用者個別の合意が望ましいとされている。

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

加入者の同意に基づくフィルタリングについての総務省における議論

- 電子メールの受信時期については様々な考え方があるため、今後検討を重ねていく必要がある。例えば、1)受信サーバに到達したという受信と、2)実際に受信者の端末に到達したという受信の2段階があると考えれば、受信サーバまでは届けるが、実際に受信者の端末に届くかどうかまでは保証しないといった、発信者の通信の自由の制限を2段階にわけた整理も可能と考えられる。

- フィルタリングと電気通信事業法との関係を整理する際には、電気通信事業法第4条（通信の秘密）とともに、第3条（検閲の禁止）についても検討が必要であろう。

- 電気通信事業者が、加入者の申込みを受けて行うフィルタリングは、電気通信事業者と加入者との間の回線利用契約に基づく回線利用権の一内容としての、加入者による通信選択権の行使に応じて行われるものと考えられる。

- 発信者にも、自己の発信した通信について、あて先である受信者まで送信される利益があるので、電子メールのフィルタリングサービスが正当業務行為として正当化されるには、発信者の利益の制約を最小限にする必要がある。具体的には、「受信者が受信したくないと考える範囲」と、「実際に受信されない範囲」ができるだけ同一になるような措置が講じられていなければならないと考えられる。

平成18年3月17日 電気通信事業分野におけるプライバシー情報に関する懇談会（第19回会合）議事要旨
http://www.soumu.go.jp/joho_tsusin/d_syohi/060317_1.html

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

インバウンドチェックの導入手順　1．対象

やり方次第では、従来の法的解釈でも何とかできる範囲。

1. オプションのサービスの設定者に対してのみ行う
2. 全員にサービスとして提供するが、デフォルトはオフにする。
3. 全員にデフォルト･オンで提供するが、利用者が個別に解除もできるようにする。 ※
4. 全員に一律に提供し、設定は解除できない。

更なる検討が必要

また、約款や利用規約などで送信ドメイン認証に基づくインバウンドチェックを行い、その結果によりメールを受信ないこともありうることを受信者に対し包括的な合意の形をとり、また送信者に対しては、ISPのポリシーとしてそのようなメールを受信拒否することを宣言することも必要と思われる。

※　P10の条件を満たす必要がある

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

インバウンドチェックの導入手順　2．手法

やり方次第では、従来の法的解釈でも何とかできる範囲。

1. Webメールで認証結果を表示し、ヘッダーに認証結果を挿入する。「ラベリング」※
2. 認証結果でエラーとなったものは、迷惑メールとして個別利用者のspamフォルダーに振り分ける。
3. 認証結果でエラーとなったものは、利用者のメールボックスに配送しない。

更なる検討が必要

※ユーザーが受信したメールのヘッダーに「Authentication-Results:」で始まる行 を追加する。ここに送信ドメイン認証の結果がスコアとして「pass (認証成功)」「fail (認証失敗･送信元メールアドレスは詐称されている)」と いった形で記述される。 IETFで提案中

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

従来　広い意味でフィルタリングとされていたもの

		手法		
		検証	ラベリング	(狭義の) フィルタリング
対象	全員でデフォルト･オフ	○	○	○
	全員にデフォルトオン	○	○	△　※
	全員 (強制)	○	○	×

※　P10の条件を満たす必要がある。

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

総務省の考え　電気通信事業者が行う電子メールのフィルタリングと電気通信事業法第４条（通信の秘密の保護）の関係について

＜初期設定をフィルタリングオンの状態で提供するための条件＞

1. 利用者が、いったんフィルタリングサービスの提供に同意した後も、随時、任意に同意内容を変更できる状態（設定変更できる状態）であること
2. フィルタリングサービス提供に対する同意の有無にかかわらず、その他の提供条件が同一であること
3. フィルタリングサービスの内容等が明確に限定されていること
4. 通常の利用者であれば当該サービスの提供に同意することがアンケート調査結果等の資料によって合理的に推定されること
5. 利用者に対し、フィルタリングサービスの内容等について、事前の十分な説明を実施すること（事業法第２６条に規定する重要事項説明に準じた手続により説明すること）

平成18年1月23日電気通信事業分野におけるプライバシー情報に関する懇談会（第１８回会合）議事要旨
http://www.soumu.go.jp/joho_tsusin/d_syohi/060123_1.html

Copyright (c) 2006 Internet Association
Japan & Takashi Kimura

ラベリングが効果を表すためにはフィルタ設定、メーラーの対応などが必要

メールのヘッダーのAuthentication-Results:情報を反映する

- サーバー上で提供される（狭義の）spamメールフィルタリング
- Webメールにおける表示（Yahoo!メール）
- クライアントPC上のメールソフトウェアで表示、振り分け
- クライアントPC上のウイルス対策ソフトの迷惑メールフィルタ機能での振り分け

現在、マイクロソフト社、トレンドマイクロ社、シマンテック社などに次期バージョンでの対応を呼びかけている

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

(主張) 将来的に誤判定の問題が解決されれば、送信ドメイン認証の検証結果に基づくメールの廃棄は全ユーザー対象に一律に行っても良いのではないか？

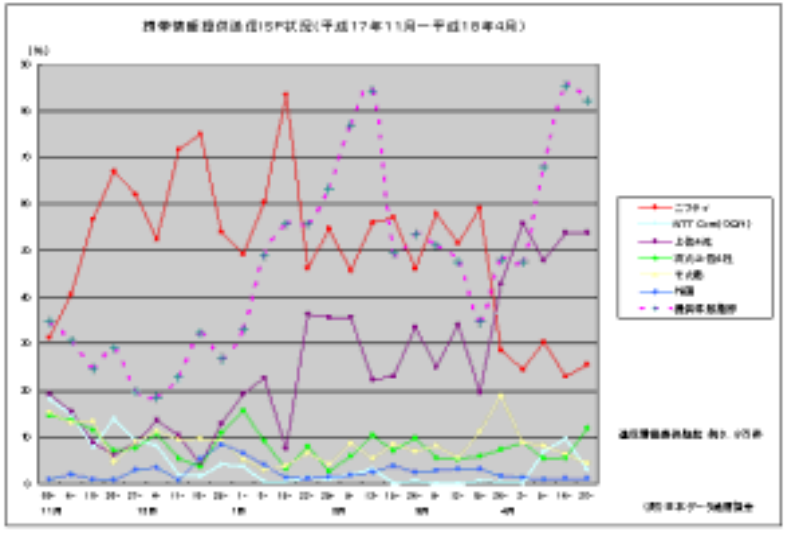
根拠

- 他のフィルタリング手法とは異なり、送信ドメイン認証には論理的に誤判定の問題は生じ得ず、一部の問題が生じると分かっているケースについては技術的に対応が可能である。
- 送信ドメイン認証の検証結果はじかれたメールを廃棄しても、正当なメールの送受信に支障が生じたり、送信者や受信者が不利益を被ることはない。
- 送信ドメイン認証の検証でメールを廃棄することで、フィッシング詐欺のメールが届かないならば、個人情報の流出や詐欺を未然に防ぐなどの利用者保護に効果が期待できる。
- 受信者が送信ドメインを詐称しているメールの受信を希望するというのは、通常ありえない。

ちなみに、改正特電法では第6条で送信元情報の詐称が直罰規定つきで禁止されたが、法律で禁止されていることと、それを電気通信事業者がフィルタリングしてよいか、ということとは別問題とされている。

Copyright (c) 2006 Internet Association Japan & Takashi Kimura

(ご紹介)
財団法人データ通信協会迷惑メール相談センターのサイトがリニューアル　http://www.dekyo.or.jp/soudan/top.htm



Copyright (c) 2006 Internet Association Japan & Takashi Kimura