

## 背景

「特定電子メールの送信の適正化等に関する法律」第13条に基づき、年1回、研究開発等の状況について公表するもの。

## 主な迷惑メール防止技術

### ○ Outbound Port 25 Blocking (OP25B)

いわゆるボットネット等を使用した迷惑メールの送信の制限に効果的な技術。

ISPのメールサーバを経由せずに、動的IPアドレスを使用して直接メールを送信する通信を制限する。

### ○ 送信ドメイン認証技術

なりすましメールといわれる、送信者のメールアドレスを詐称したメールを受信者側で確認することができる技術。

送信元情報の中で、メールアドレスのドメイン名が正当なものであるかを技術的に認証することが出来る。

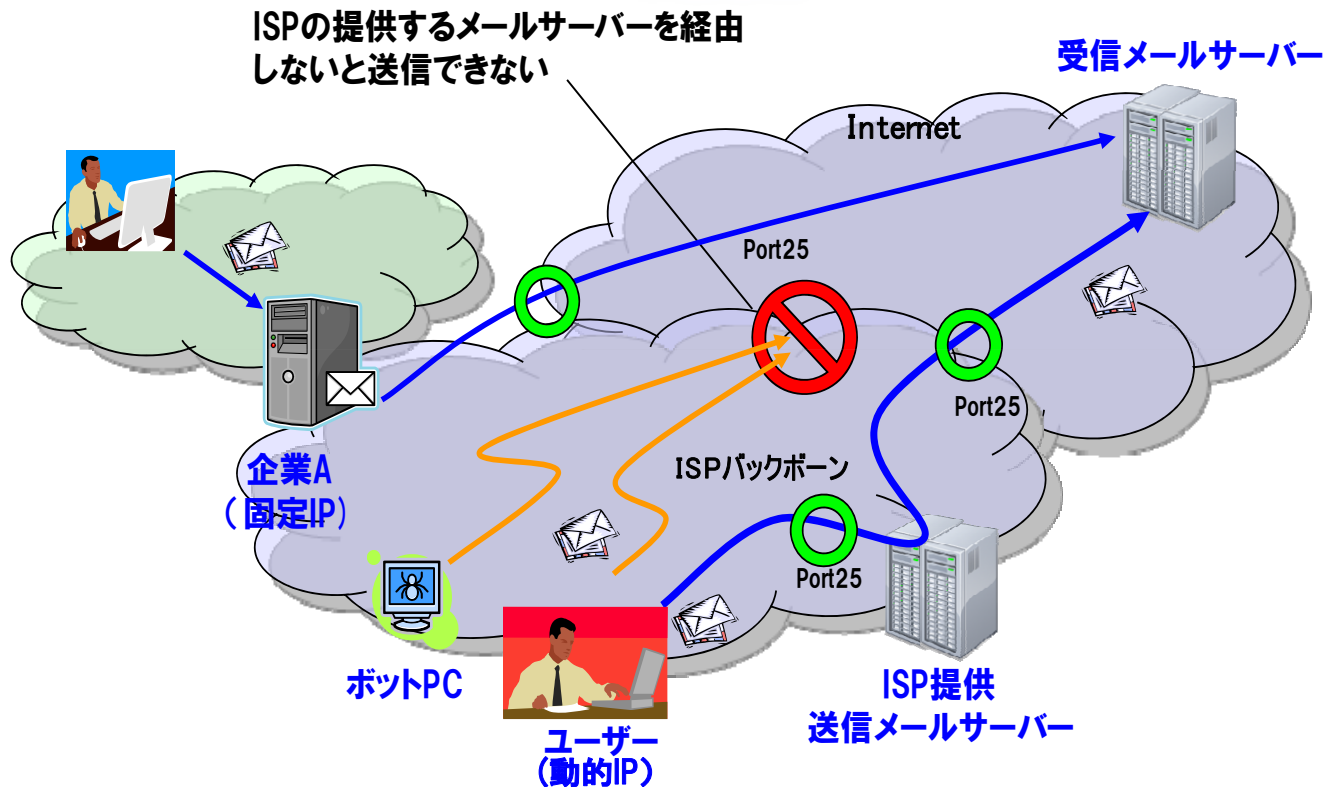
### ○ その他の技術

フィルタリング技術、受信トラフィック制御技術、指定受信・指定拒否技術、等

# Outbound Port 25 Blocking (OP25B)の概要

- 動的IPアドレスからISPのメールサーバを経由せずに直接メールを送る通信を制限する技術
- 最近増えているボットネットを利用した迷惑メールに対して、有効
- 我が国では、大手ISPに広く普及が進み、効果をあげている

## OP25Bの概要図



# Outbound Port 25 Blocking (OP25B)の実施状況

## 移動系電気通信事業者

事業者	提供開始時期	状況
A社	平成17年12月	平成17年6月より、インターネット接続サービスにてOP25Bを開始
		平成20年7月より、インターネット接続サービスを利用し、3G方式からアクセスポイント接続経由で25番ポートを利用して送信されるメールに対し、速度制限を開始
B社	平成18年3月	平成19年12月より、インターネット接続サービスから携帯電話宛でのOP25Bを開始 平成20年3月より、固定系ISP宛でのメール送信についてOP25Bを開始
C社	平成17年12月	平成18年6月より、インターネット接続サービスから携帯電話宛でのOP25Bを開始 平成20年9月下旬より、固定系ISP宛でのメール送信についてOP25Bを開始
T社	平成18年3月	平成18年5月より、インターネット接続サービスから携帯電話宛でOP25Bを開始 平成20年6月より、固定系ISP宛でのメール送信についてOP25Bを開始
U社	平成20年3月	平成20年3月より、携帯事業者宛でのメール送信についてOP25Bを開始 平成21年5月より、携帯事業者以外に宛てたメール送信について、OP25Bを順次開始

## 固定系電気通信事業者

事業者	携帯あて	PCあて	代替送信サーバ	port 587
D社	H17/10	H18/11	-	H17/10
E社	H17/10	H18/06	有	H18/03
F社	H17/11	H19/07	-	H17/11
G社	H18/06	H18/10	-	H18/06
H社	H18/02	H18/12	-	H17/02
I社	H17/03	H17/03	有	H17/03
J社	H17/12	H18/03	有	H17/12
K社	H18/06	H18/06	有	H18/03
L社	H18/03	H18/12	メールサーバ用 有	H18/08
M社	H18/02	H18/02	有	H17/10
N社	H17/09	H18/12	H20/6(25番ポートでのSMTP接続を自社接続のみに制限)	H18/02
O社	H18/07	H18/09	有	H17/07
P社	H17/01	H18/07	メールサーバ用 有	H18/06
Q社	H18/08	H19/01	-	H18/06
R社	H17/03	H17/03	有	H17/03
S社	H18/11	H18/11	無	H18/06

# 送信ドメイン認証技術の概要

## 概要

- ✓ 送信元情報のうちドメイン名が送信元に対して正当であるかを技術的に確認可能
- ✓ 送信元情報をドメイン単位で判断
  - ・ DNS(Domain Name System)サーバと連携
- ✓ 既存のメール配送の仕組み(SMTP)を変更することなく、上位互換的に導入可能

## メリット

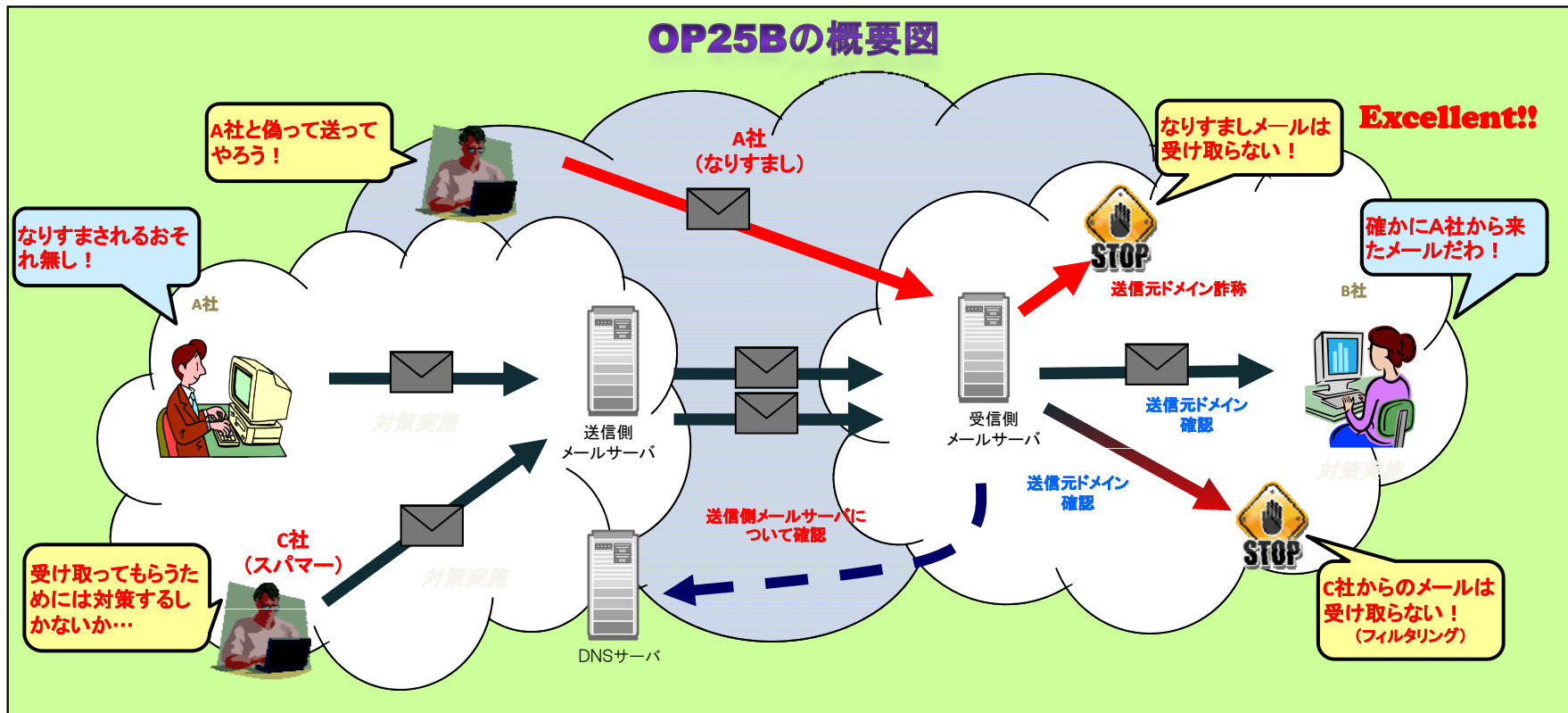
### 【送信側】送信するメールが受け取られやすく

- ・ 送信側ドメインの信頼性の確保
- ・ 受信側が送信ドメイン認証に対応していれば、受け取られやすくなる

### 【受信側】受ける電子メールを選別することが可能

- ・ 不確かなメールは、フィルタリング等で処理
- ・ 明確なものは、さらに、ドメインフィルタリング等の他の技術と組み合わせることで、信頼できる送信者が確認(効率的な迷惑メール対策)

## OP25Bの概要図



# 送信ドメイン認証技術の実施状況

## 移動系電気通信事業者

事業者	送信側の対応	受信側の対応
A社	SPFの提供済み (DNSサーバへSPFレコードの記述)	送信元情報を詐称したメールを受信拒否
B社		未実施
C社		送信元情報を詐称したメールを受信拒否
T社		未実施
U社		PCから携帯電話及びPHSドメインになりすましたメールを拒否 送信元IPアドレスとメールアドレスのドメインに対応するSPFレコードと不合致の場合に拒否

## 固定系電気通信事業者

事業者	送信側の対応	受信側の対応
D社	H17/12(S) <sup>※</sup> H21/02(D) <sup>※</sup>	○
E社	-	-
F社	H19/02(S)	○
G社	H19/05(S)	-
H社	H18/02(S)	-
I社	○	-
J社	H18/03(S)	-
K社	H18/04(S)	-
L社	H17/12(S)	-
M社	H17/05(S) H17/05(D)	-
N社	H18/05(S)	-
O社	H17/11(S) H19/09(D)	○
P社	H18/11(S)	-
Q社	H18/12(S) H17/07(D)	-
R社	H18/10(S)	-
S社	H19/11(S)	-

※ (S)はSender Policy Frameworks (SPF)、(D)はDKIM/DomainKeysと呼ばれる技術のこと

※ ○は導入した技術、導入時期は不明だが、導入は実施済