特定電子メール等による電子メールの送受信上の支障の防止に資する技術の研究開発及び電子メールに係る役務を提供する電気通信事業者によるその導入の状況（概要）

別　紙

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。

※　特定電子メールの送信の適正化等に関する法律」（平成14年法律第26号）
第13条　総務大臣は、毎年少なくとも一回、特定電子メール等による電子メールの送受信上の支障の防止に資する技術の研究開発及び電子メール通信役務を提供する電気通信技術者によるその導入の状況を公表するものとする。

主な迷惑メール防止技術

【迷惑メール送信防止のための主な技術】

技術名	技術の概要
1．送信トラフィック制御	大量のメールの一括送信を阻止するために、同一アカウントからの送信量を制御する方法
2．送信者認証(SMTP-AUTH)	送信側のISPで、自社メールサーバからの送信しようとする送信者に対して認証を行う方法
3．OP25B (Outbound Port25 Blocking)	ISPのメールサーバを経由しない動的IPアドレス（インターネットに接続される度に割り当てられるIPアドレス）からのメール送信を遮断する方法

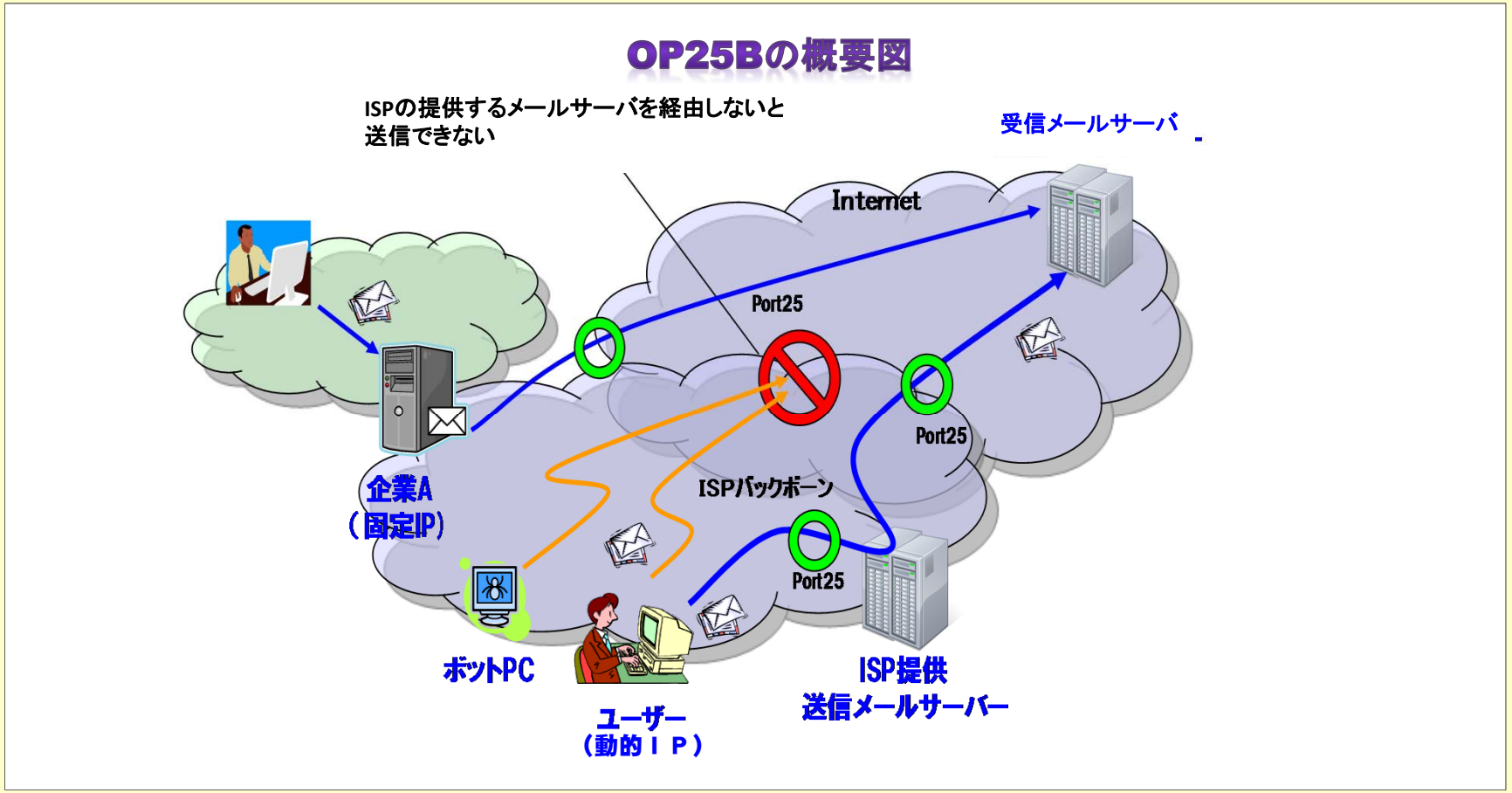
【迷惑メール受信防止のための主な技術】

技術名		技術の概要
1．迷惑メールであることの判定		迷惑メールを判定する方法として、「キーワード判定」や「送信元情報参照による判定」がある
(1)キーワード（ブラックワード）判定		メールのヘッダ及び本文中の特定のキーワードに合致するものを迷惑メールと判定する方法
(2)送信元情報参照による判定		メールの送信元情報を参照し、迷惑メールであるかを判定する方法
	ブラックリスト	迷惑メール送信元として知られるIPアドレスをまとめたリストからのメールを、迷惑メールと判定する方法
	グレーリストによる判定フィルタ	受信メールサーバでメールを受信する際に、既知の送信メールサーバからの場合は正常に配信を行い、未確認のメールサーバに対してのみ配信を一時的に拒否する方法
	送信ドメイン認証	自社のメールドメインから発信されるメールに対して、メールドメインの認証を付与することで、メール受信側のサーバに対して、自社サーバから送付されたメールであることを保証する方法
2．レピュテーション		実際の迷惑メールの情報を基に構築した「信用度（レピュテーション）データ」を用いて、IPアドレス又はメールが経由してきたサーバの情報から、迷惑メール判定を行う方法。
3．内容参照による判定		主にメールの内容を検査し、流通する迷惑メールから分析した情報に基づいて迷惑メールかどうかを判定する方法
4．受信トラフィック制御		迷惑メールと判断されるメール受信のトラフィック量を制御する方法

Outbound Port 25 Blocking（OP25B）の概要

○　我が国の大手電気通信事業者での普及が進み、迷惑メール送信の削減に大きな効果をあげている技術。

○　ＩＳＰのメールサーバを経由しない動的ＩＰアドレス（インターネットに接続される度に割り当てられるＩＰアドレス）からのメール送信を遮断する方法。



Outbound Port 25 Blocking (OP25B)の実施状況

移動系電気通信事業者

事業者	提供状況
A社	○
B社	○
C社	○
T社	○
U社	○

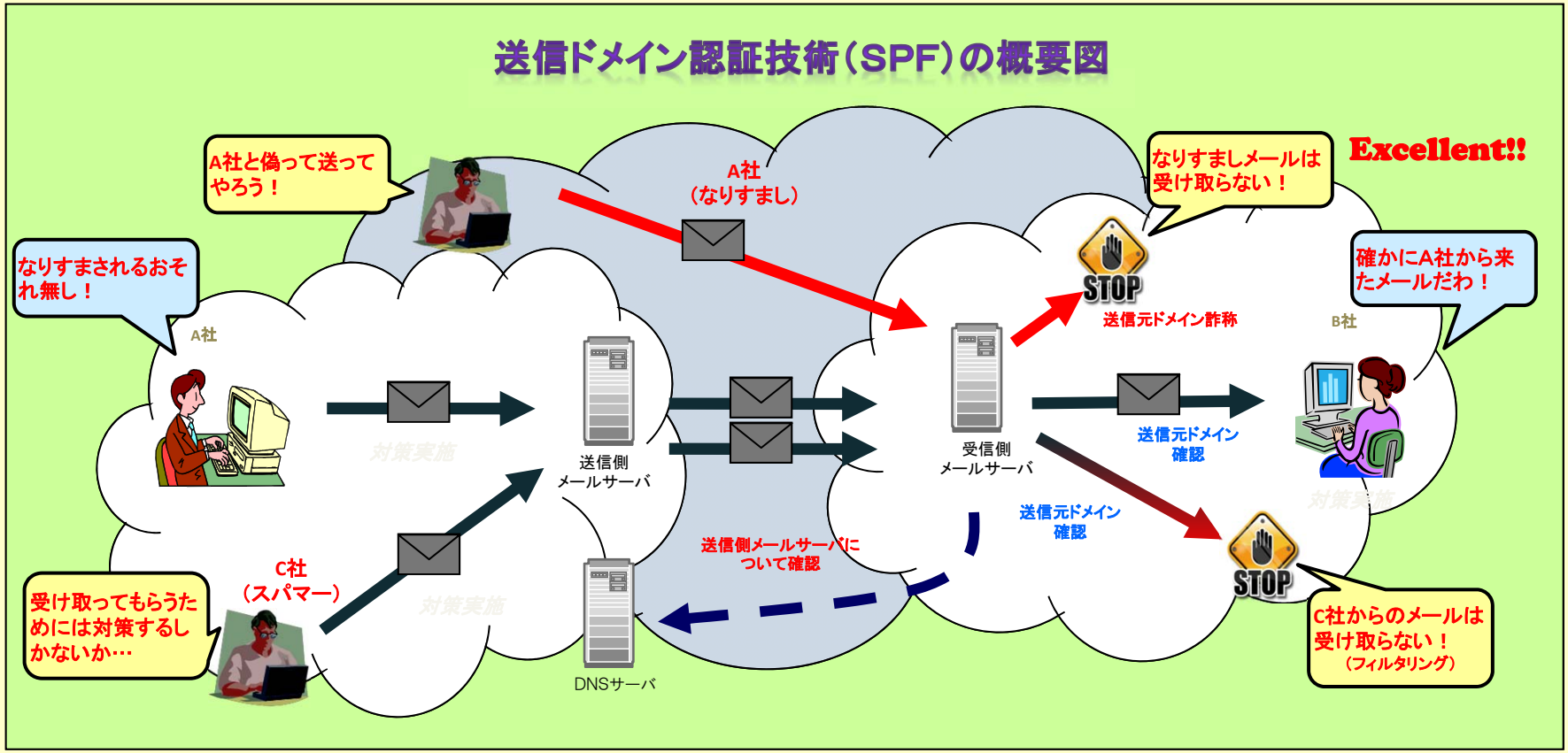
固定系電気通信事業者

事業者	携帯宛て	PC宛て	port 587
D社	○	○	○
E社	○	○	○
F社	○	○	○
G社	○	○	○
H社	○	○	○
I社	○	○	○
J社	○	○	○
K社	○	○	○
L社	○	○	○
M社	○	○	○
N社	○	○	○
O社	○	○	○
P社	○	○	○
Q社	○	○	○
R社	○	○	○
S社	○	○	○

送信ドメイン認証技術の概要

○　いわゆる「なりすまし」による迷惑メール送信の対策として有効な技術。今後の普及が期待されている。

○　自社のメールドメインから発信されるメールに対して、メールドメインの認証を付与することで、メール受信側のサーバに対して、自社サーバから送付されたメールであることを保証する方法。



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可能
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可能
Ｔ社		未実施
Ｕ社		未実施

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			
	Sender Policy Frameworks（SPF)	DKIM/DomainKeys	Sender Policy Frameworks（SPF)		DKIM/DomainKeys	
			ラベリング	フィルタリング	ラベリング	フィルタリング
Ｄ社	○	○	○	○	○	―
Ｅ社	―	―	―	―	―	―
Ｆ社	○	―	○	―	―	―
Ｇ社	○	―	―	―	―	―
Ｈ社	○	―	―	―	―	―
Ｉ社	○	―	―	―	―	―
Ｊ社	○	―	―	―	―	―
Ｋ社	○	―				
Ｌ社	○	―	○※	―	―	―
Ｍ社	○	○	○※	―	○※	―
Ｎ社	○	―	―	―	―	―
Ｏ社	○	○	○	―	○	―
Ｐ社	○	―	―	―	―	―
Ｑ社	○	○	○※	○※	○※	○※
Ｒ社	○	―	―	―	―	―
Ｓ社	○	―				

（注1）※印は、今回の調査で新しく導入されたことが判明したもの。
（注2）ラベリング：送信ドメイン認証結果を電子メールに記録する。　フィルタリング：ラベリングの結果を用いてフィルタリングを行う。