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事業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が、自社のネットワークの動的IPから相手方電子メールサーバの25番ポートに当てて電子メールを送信することをブロックする方法。主に、ISPの提供するメールサーバーを利用せず、自前で設置するメールサーバやボットネットを利用して、直接メール送信を行うことを防止することを目的とする。

【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. 受信メールの特徴判定	迷惑メールの特徴である「大量受信」等を検出し、受信を制御する方法
2. 受信メールの内容判定	迷惑メールを判定するため、「キーワード判定」や「迷惑メールフィルタ」等を用いる方法
(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が存在するものを迷惑メールと判定する方法
(2) 迷惑メールフィルタ	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
3. 送信元情報による判定	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
(1) 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
(2) グレーリスト	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
(3) 送信ドメイン認証	受信者が受け取ったメールについて、送信者情報が詐称されているかどうかをドメイン単位で確認する方法。ネットワークベースのSPF/Sender IDと電子署名を利用するDKIMがある。 また、これらの認証結果を利用して認証に失敗したメールを処理するための標準規格であるDMARCが策定された。
(4) 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

移動系電気通信事業者の主な迷惑メール送受信防止対策の提供状況

事業者	主な送信防止対策				主な受信防止対策					
	送信通数規制	同報送信宛先数制限	送信ドメイン認証	OP25B	指定受信・拒否	なりすまし拒否	送信ドメイン認証	ホワイトリスト	簡易設定	URL付きメール受信拒否
A社	○	－	○	○	○	○	○	○	○	○
B社	○	○(※)	○	○	○	○	○	○	○	○
C社	○	○	○	○	○	○	○	○	○	○

※B社グループ4社のうち2社が対応

用語	内容
【主な送信防止対策】	
送信通数規制	携帯電話の1日1台あたりの送信通数等を制限する。
同報送信宛先数制限	複数の宛先について、同時に送信できる件数を制限する。
送信ドメイン認証（送信側）	自社のメールドメインから発信されるメールについて、メール受信側のサーバに対し、自社サーバから送信されたメールであることを確認する手段を提供する。ネットワークベースのSPF/SenderIDと電子署名を利用するDKIMがある。
OP25B	ISPが自社のネットワークの動的IPから相手方電子メールサーバの25番ポートに電子メールを送信することをブロック方法。
【主な受信防止対策】	
指定受信・拒否	指定したメールアドレス、ドメイン等から送信された電子メールを受信／拒否する。
なりすまし拒否	PCから送信される携帯電話、PHSのドメインになりすましたメールを受信拒否する。
送信ドメイン認証（受信側）	受信したメールについてドメインが詐称されていないか送信側のサーバに問い合わせて確認する。ネットワークベースのSPF/SenderIDと電子署名を利用するDKIMがある。
ホワイトリスト	転送元のメールアドレスを登録することにより、ホワイトリストの登録前に転送により「なりすまし」と判定されて届かなかったメールを受信する。
簡易設定	メールフィルタを希望のレベルに合わせて、簡易に設定できる。
URL付きメール受信拒否	URLリンクが含まれるメールを拒否する。

固定系電気通信事業者の主な迷惑メール受信防止対策の提供状況

事業者	主な送信防止対策		主な受信防止対策									
	送信ドメイン認証	OP25B	送信ドメイン認証						メールの内容による判定			大量受信制限
			SPF/SenderID		DKIM/Domainkeys		DMARC		ﾌﾞﾗｯｸﾜｰﾄﾞ	メール容量	迷惑メールフィルタ	
			ラベリング	フィルタリング	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	○	○	―	―	―	―	―	―	○	―	○	―

用語	内容
【主な送信防止対策】	
送信ドメイン認証（送信側）	自社のメールドメインから発信されるメールについて、メール受信側のサーバに対し、認証自社サーバから送信されたメールであることを確認する手段を提供する。ドメイン詐称を防ぐSPF、アドレス詐称を防ぐSenderIDとメールの電子署名を利用するDKIMがある。また、SPFとDKIMを認証を利用して統一的に処理するDMARCがある。
OP25B	ISPが自社のネットワークの動的IPから相手方電子メールサーバの25番ポートに電子メールを送信することをブロック方法。
【主な受信防止対策】	
送信ドメイン認証（受信側）	受信したメールについてドメインが詐称されていないか送信側のサーバに問い合わせて確認する。ネットワークベースのSPF/SenderIDと、電子署名を利用するDKIMがある。また、SPFとDKIMを認証を利用して統一的に処理するDMARCがある。
ブラックワード	送信者アドレス、件名等を組み合わせて受信拒否条件を設定できる。
メール容量	受信メールのサイズによる受信拒否設定ができる。
迷惑メールフィルタ	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し、受信拒否できる
大量受信制限	大量の宛先不明のメール送信を行うサーバに対し、受信拒否等を行う。