

送信ドメイン認証技術 導入マニュアル

第2版 2011年8月

迷惑メール対策推進協議会



目次

第1章 はじめに	1
1.1 メールの普及と送信者情報偽装の問題	2
1.2 送信ドメイン認証技術による対応	2
1.3 本マニュアルの目的	2
第2章 メールの仕組みと課題	5
2.1 メールシステムの概要	6
2.2 メール配送の手順	8
2.3 メール本体の構造	9
2.4 メールの送信者情報	9
2.4.1 概要	9
2.4.2 メール配送時に指定される送信者情報	9
2.4.3 ヘッダ領域に記述される送信者情報	10
2.5 送信者情報詐称の問題	11
2.5.1 送信者情報詐称を判断する仕組み	11
2.5.2 送信者情報詐称の問題点	12
2.5.3 送信ドメイン認証技術	13
第3章 送信ドメイン認証技術	15
3.1 送信ドメイン認証技術による対応	16
3.2 Sender Policy Framework (SPF)	17
3.2.1 概要	17
3.2.2 SPFの仕組み	17
3.2.3 送信側の設定	17
3.2.4 SPFレコードの記述法	18
3.3 Sender ID	22
3.3.1 概要	22
3.3.2 Puported Resposible Adress(PRA)	22
3.3.3 SPFレコードのバージョン	23
3.4 Domainkeys Identified Mail (DKIM)	25
3.4.1 概要	25
3.4.2 公開鍵の提供	26
3.4.3 送信側での電子署名の作成	27
3.4.4 受信側での処理	29
3.4.5 認証結果の扱い	29
3.4.6 DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)	29
3.5 認証結果のヘッダへの表示	32
3.5.1 Authentication-Results	32
3.5.2 ヘッダの詐称	32
3.5.3 認証方法ごとの結果表示	32

第4章 送信ドメイン認証技術導入手順 **37**

- 4.1 事前準備 38
 - 4.1.1 導入する送信ドメイン認証技術の決定 39
 - 4.1.2 ドメイン名の把握 40
 - 4.1.3 メールの利用方法の確認 42
 - 4.1.4 導入計画の作成 45
- 4.2 一般的な導入手順 48
 - 4.2.1 SPF/Sender ID 48
 - 4.2.2 DKIM 51
- 4.3 運用 54
 - 4.3.1 メールサーバの運用 54
 - 4.3.2 DNS の運用 54

第5章 ISP での対応 **57**

- 5.1 ISP のメールサービスの概要 58
- 5.2 送信側の対応 59
 - 5.2.1 概要 59
 - 5.2.2 送信ドメイン認証技術の導入 59
 - 5.2.3 迷惑メールの管理 62
- 5.3 メール受信側としての検討 65
 - 5.3.1 概要 65
 - 5.3.2 利用する送信ドメイン認証技術の選定 65
 - 5.3.3 メールの配送制御 65
- 5.4 ユーザ周知 67
 - 5.4.1 送信側の対応 67
 - 5.4.2 受信側の対応 67

第6章 ホスティングサービスでの対応 **69**

- 6.1 ホスティングサービスの分類 70
 - 6.1.1 メールサーバによる分類 70
 - 6.1.2 DNS サーバによる分類 73
- 6.2 送信側の対応 74
 - 6.2.1 SPF / Sender ID の対応 74
 - 6.2.2 DKIM の対応 76
- 6.3 受信側の対応 79
 - 6.3.1 認証結果の解説と利用方法の提示 79
 - 6.3.2 認証結果によるフィルタリング実施 79

第7章 配信サービスでの対応 **81**

- 7.1 配信サービスとは 82
 - 7.1.1 配信サービスと送信ドメイン認証技術 82
 - 7.1.2 From ヘッダアドレスの管理主体 83
- 7.2 送信ドメイン認証技術の導入 84
 - 7.2.1 SPF 84
 - 7.2.2 SenderID 84
 - 7.2.3 DKIM 86
- 7.3 配信サービスによる利用者への周知 88

8.1	送信ドメイン認証技術とは	90
8.2	送信時の注意事項	91
8.3	受信時の注意事項	92
8.4	メール転送時の注意事項	93
Appendix 1.	SPF レコードの記述例	95
Appendix 2.	DKIM レコードの記述例	103
Appendix 3.	関連 RFC	109
Appendix 4.	用語集	111

