JPCERT CC®

電子メールソフトのセキュリティ設定について

第 11 分冊

- 用語説明

一般社団法人**JPCERT**コーディネーションセンター
2011 年 **2** 月 **1** 日

本資料は、一般社団法人 JPCERT コーディネーションセンターのウエブサイトにて公開している「電子メールのセキュリティ設定」をPDFファイルにまとめたものです。
最新の情報に関しては、以下の URL を参照してください。

一般社団法人 JPCERT コーディネーションセンター
電子メールソフトのセキュリティ設定について
https://www.jpcert.or.jp/magazine/security/mail/index.html

5　用語説明

IMAP
インターネットメッセージアクセスプロトコル(Internet Message Access Protocol)は、メールサーバから電子メールを受信したり、メールサーバ上でメールを操作したりするプロトコル。主に利用される IMAP4 rev1 では、クライアントとサーバ間の通信に 143/tcp が使用され、RFC3501 にて規定されている。

MDA
メール配送エージェント(Mail Delivery Agent)は、メール転送エージェント(MTA)によって振り分けられた電子メールを別の MTA に送信したり、受信者のメールボックスに配送する機能。

MTA
メール転送エージェント(Mail Transfer Agent)は、電子メールを宛先アドレスに配送する機能のことであり、メールサーバ機能のなかで中心的な機能を持つ。

MUA
メールユーザエージェント(Mail User Agent)は、電子メールを読み書き、メールサーバへの送信、メールサーバからの受信等を行うソフトウェア。いわゆる電子メールソフト(もしくはメールクライアント)のこと。

OP25B
アウトバウンドポート 25 ブロッキング(Outbound Port 25 Blocking)は、迷惑メール送信者が増えたことに対して ISP 側で採用された対策で、ISP がユーザに割り当てた IP アドレスから ISP 外部への SMTP 通信を遮断する。SMTP 通信が TCP の 25 番ポートを利用するため、この名称が使用されている。

PGP
プリティーグッドプライバシー(Pretty Good Privacy)は、Philip Zimmermann が開発、公開した暗号ソフトウェア。公開鍵暗号方式を採用しており、電子メールの暗号化、電子署名を行うことが可能である。

POP before SMTP
ポップビフォアエスエムティーピー(POP before SMTP)は、SMTP 認証が策定される以前に策定されたメール送信者の認証に利用される仕組みで、SMTP によるメール送信の前に POP の認証機能を利用してユーザ認証を行う。

POP/POP3
ポストオフィスプロトコル(Post Office Protocol)は、メールサーバから電子メールを受信するためのプロトコル。現在は、改良された POP3（POP version3） が主に使用されている。通常、クライアントとサーバ間の通信には 110/tcp が使用され、RFC1939 にて規定されている。

S/MIME
エスマイム(Secure Multipurpose Internet Mail Extensions)は、電子メールの暗号化と電子署名に関する国際規格である。公開鍵暗号方式を採用しており、電子メールの暗号化、電子署名を行うことが可能である。

SMTP
簡易メール転送プロトコル(Simple Mail Transfer Protocol)は、電子メールを転送するプロトコル。通常、クライアントとサーバ間の通信には 25/tcp が使用され、RFC5321 にて規定されている。

SMTP 認証

SMTP 認証は、SMTP を利用したメール配送を行う際に、送信者がそのメールサーバを利用する権限があるかの認証機能を追加した仕様。

SSL/TLS

SSL はセキュアソケットレイヤー(Secure Sockets Layer)の略であり、TLS はトランスポート層セキュリティ(Transport Layer Security)の略である。
SSL 及び TLS は、安全性を要求される通信を行う場合に利用するためのプロトコルである。
SSL はもともと、Web における通信の安全性の確保のためにネットスケープコミュニケーションズ社によって開発されたものである。その後、IETF による標準化作業が行われ、SSL の後継として RFC2246 として TLS1.0 が公開された。
なお、現在では、TLS1.2(RFC5246) となっている。

開封確認

開封確認(Disposition Notification)は、送信した電子メールが受信者に届いたかどうかを確認できる機能。RFC3798 にて規定されており、この機能を利用したメールが到着しても「開封確認を送り返す必要は無い」となっている。