メールのエンベロープ部

●メールは、エンベロープ部とメッセージ部（ヘッダとボディ）に分かれている。

●メールの送受信においては、各機器間で TCP コネクションが確立され、確立後、例えば、メール転送においては、HELO（EHLO）、MAIL FROM、RCPT TO 等の SMTP コマンドのやり取りが行われ、このやり取りの議事録がエンベロープ部となる。

MAIL FROM や RCPT TO はエンベロープ情報（転送サーバが参照する情報）である。

●SMTP コマンドには、情報漏洩を促す以下の 2 つのコマンドがあるため、無効となるように MTA を設定する。

①VRFY（Verify）：メッセージの配信可能を調べるためにメール BOX、つまり、アカウントの存在を確認

②EXPN（Expand）：メーリングリスト（メールエイリアス）の配信アドレスの確認

メールのメッセージ部（ヘッダとボディ）

●メールボディはメール本文であり、ヘッダ情報や添付フアイルを含まない。

●ヘッダ情報としては、Return-Path、Received、From、To、Subject 等

SPF について

●SPF：受信側メールサーバは、エンベロープ情報（MAIL FROM）から、送信元メールサーバのドメインを得る。そのドメインの DNS サーバから、送信元メールサーバの IPA を知る。その IPA と何を比較するのかというと、受信側メールサーバが直接アクセスしている機器（直前の転送メールサーバ）なので、転送を繰り返していると、最初の送信元メールサーバとは異なる IPA と比較することになる。つまり、検証は困難になる。というよりできない。※もし、直前の転送メールサーバが SPF に対応しており、エンベロープ情報を自身のものに書き換えることができれば検証可能であるが、送信元サーバ以外のサーバを検証することに何の意味があるのか、わからない。

●DKIM：それに対して、DKIM は、署名（署名対象はメッセージ部）の検証に合格すればいいので、IPA は関係ない。つまり、署名と共に送信元メールサーパのドメイン情報も送られてくるので、そのドメインの DNS サーバから公開鍵を得ることができる。

●DMARC：Envelope - From（MAIL FROM のドメイン）は、Header - From（メールヘッダのドメイン）と同じドメインか、サブドメインかを確かめたうえで SPF を行うため、Header - From の詐称を見抜くことができる。

メールの暗号化

●SMTP over TLS（SMTPS）：クライアント（MUA）から自サイト内の SMTP サーバ間で TCP465。

●STARTTLS：送信側のメールサーバと受信側のメールサーバ間。受信側が SMTP サーバなら TCP25。POP3 サーバなら TCP110。IMAP4 サーバなら TCP143。つまり、暗号化又は非暗号化通信であっても、ポート番号は変わらない。

●POP3 over TLS（POP3S）：クライアント（MUA）から POP3 サーバで TCP995。POP3 サーバ内で TCP110 にポートフォワーディング。

※IMAP4 の暗号化は IMAPS であり、IMAP4S とはあまり言わない。

●上記と同じ範囲の暗号化として、

MUA → SSH クライアント → SSH サーバ（22）→ POP3 サーバ（110）

●S/MIME 証明書（S 証明書）は、メール利用者のデジタル証明書である。

①送信者は、受信者の S 証明書（公開鍵）で暗号化し、受信者は自己の秘密鍵で復号する。

②送信者は、自己の秘密鍵で署名を作成し、受信者は送信者の S 証明書（公開鍵）で検証する。

●S 証明書は、第三者機関が発行しているため、信頼できるが、PGP で使用する公開鍵は、本人以外が鍵ペアを生成することができる。そのため、正規の生成元は公開鍵のハッシュ値（フィンガプリント）を公開することで、出回っている公開鍵の正当性を利用者に確認させる方法をとる。

メールの認証

●OP25B が機能しており、サブミッションポート 587 に接続する時、MSA において、SMTP - AUTH 認証を行う。

●POP3 への接続には、認証が必要であるが、認証情報（UID と PW）やメール自体も平文で流れる。

●APOP はチャレンジレスポンス方式なので、PW は平文ではないが、メール自体は平文のまま。