UNIXサーバー構築 Ⅱ

第6章　MAILサーバーの設定Ⅱ（SSL/TLS）

メールの暗号化（SSL/TLS）

メールの暗号化

メールは暗号化せずに送受信されています。SSL/TLSを使用することで暗号化されたメールを送ることができるようになります。また、クライアントとの通信はすべて暗号化し、デフォルトとのポート番号でのアクセスを禁止します(OP25B：Outbound Port 25 Blocking(SMTP の 25 番ポートでの通信をブロックする))。

＊暗号化する前

暗号化するために証明書や鍵を事前に作成しておく必要があります。
以前に使用したものを作成します。

暗号化の設定手順

クライアントとメールボックス間は暗号化し、OBP25Bを設定します。

暗号化の設定手順は以下の通りに行います。

①証明書と鍵の作成・・・今回は省略します

②Dovecotの設定（POP3用）

③Postfixの設定（SMTP用）

④構文チェック

⑤Postfix、Dovecotの再起動

⑥動作確認

暗号化の設定②

②Dovecotの設定（**/etc/dovecot/conf.d/10-ssl.conf**）

Dovecotでは**10-ssl.conf**ファイルを変更します。SSLを有効にし、使用する鍵と証明書の指定を行います。

ssl = yes　・・・ no から yes に変更します。

ssl_cert = <証明書のパス　・・・証明書の指定

ssl_key = <鍵のパス　・・・鍵の指定

<例>

ssl_cert = </ca/server.pem

ssl_key = </ca/private/server.key

暗号化の設定③

③Postfixの設定

PostfixではMain.cfとmaster.cfの2つのファイルを変更します。

・master.cf（/etc/postfix/mater.cf）の設定

2か所のコメントを解除します。

・17行目付近

submission inet n - y - - smtpd

-o syslog_name=postfix/submission

・33行目付近

smtps inet n - y - - smtpd

・main.cf（/etc/postfix/main.cf）の設定

以下の内容を最終行に追加します。

smtpd_use_tls = yes ・・・ SMTP で TLS を使用

smtp_tls_mandatory_protocols = !SSLv2, !SSLv3 ・・・ プロトコル指定

smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3

smtpd_tls_cert_file = /ca/server.pem ・・・ 証明書の指定

smtpd_tls_key_file = /ca/private/server.key ・・・ 鍵の指定

smtpd_tls_session_cache_database = btree:${data_directory}/

smtpd_scache ・・・1行で記述

暗号化設定④

④構文チェック

Postfixとdovecotの構文チェックを行います。

sudo postfix check

sudo dovecont -n

⑤再起動

sudo systemctl restart postfix dovecot

暗号化の設定⑤

⑥動作確認

動作確認は **openssl コマンド**を使用して行います。設定したポート番号で送受信ができるか検証します。**POP3s は 995、SMTP のサブミッションポート は 587、SMTPs は 465** のポート番号を使用します。

・POP3s（dovecot）の確認

sudo openssl s_client -connect　メールサーバー:995

＊ログインやメールの確認コマンドはtelnetと同じです。

<例>

sudo openssl s_client -connect mail.ecccomp.ac.jp:995

・SMTPs（Postfix）の確認

sudo openssl s_client -connect　メールサーバー:475

＊ログインやメールの確認コマンドはtelnetと同じです。

・動作ポートでの確認

sudo netstat -nat

＊netstatコマンドを使用する場合、インストールが必要

sudo apt -y install net-tools

・SMTP（サブミッションポート）の確認

sudo telnet メールサーバー 587

ログインなど多くの入力が必要となります。

helo　メールサーバー ・・・ セッションの始まりを伝えます

ehlo　メールサーバー ・・・ 拡張サービス対応

mail from:送信元メールアドレス ・・・ 送信元メールアドレス

rcpt to:宛先のメールアドレス ・・・ 宛先メールアドレス

data ・・・ メールの本文です

. ・・・ ドット(本文を終了するためのものです)

quit ・・・ 終了