

■ メール通信が暗号化されている場合の UTM 利用上の注意点

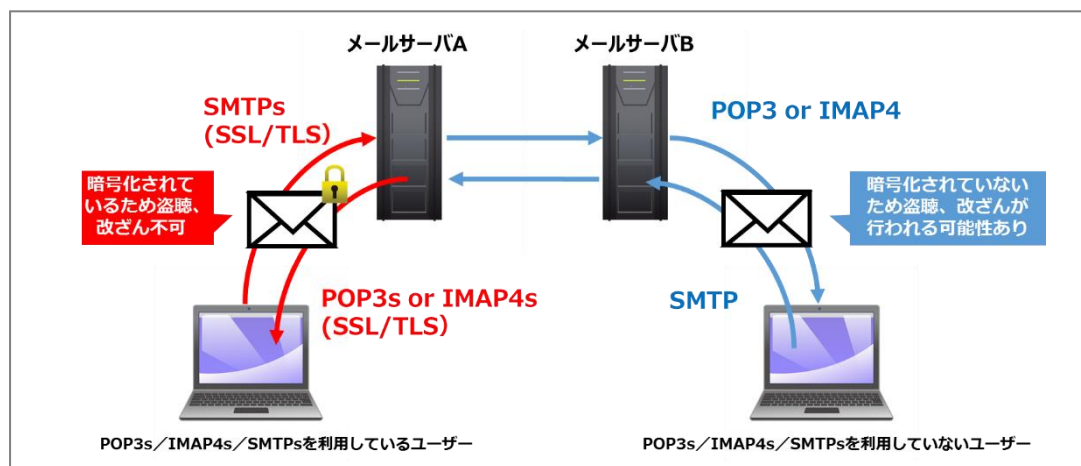
以下の技術により、メール通信が暗号化されている場合の HOME-UNIT2 及び HOMEUNIT3 利用時の注意点を以下に解説します。

- POP3s/IMAP4s/SMTPs などの暗号化プロトコルの利用
- STARTTLS などの拡張機能

◎POP3s/IMAP4s/SMTPs とは

パソコンからメールサーバまでの間の通信を SSL/TLS で暗号化する技術です。**途中経路でのメールの盗聴、改ざんに対するセキュリティ担保**を目的としています。メールサーバおよびメールソフトにて設定します。

なお、下図に記載のとおり、相手側メールサーバとパソコン間が POP3s/IMAP4s/SMTPs を利用していない場合、またメールサーバ同士が平文でのやり取りを行っている場合、当該メールの盗聴、改ざんが行われる可能性があります。



POP3s/IMAP4s/SMTPs を利用しているかどうか不明の場合は、以下の表を参考にご確認ください。

暗号化なし		暗号化あり	
プロトコル名	ポート番号※	プロトコル名	ポート番号※
POP3	110	POP3s	995
SMTP	25/587	SMTPs	465
IMAP4	143	IMAP4s	993

※デフォルトポートのため、プロバイダによって異なる場合があります。詳細はプロバイダサービスの提供元にご確認ください。

◎STARTTLS とは

パソコンからメールサーバまでの間の通信のデータ部分のみを SSL/TLS で暗号化する技術です。

POP3s/IMAP4s/SMTPs が通信の最初から暗号化が行われるのに対して、STARTTLS を利用した場合、セッション開始時は平文でやり取りが行われます。

◎POP3s／IMAP4s／SMTPs および STARTTLS 利用時の UTM 利用について

メール通信が暗号化されている場合、UTM による以下の機能をご利用いただくことができません。以下の機能をご利用になる場合は暗号化を不使用とすることをご検討ください。

- アンチスパム（迷惑メールのタグ付け）
- メールに対するウイルス検疫（ランサムウェアなどの脅威メールの検出と対策など）
- ZIP 暗号化機能
- メール誤送信防止機能（HOME-UNIT3 ご利用時に限る）

以上