LanScope Guard3

技術情報　Vol.4

～メール認証の仕組みと制限事項資料～

2011年4月5日

第2版

エムオーテックス株式会社

改版履歴

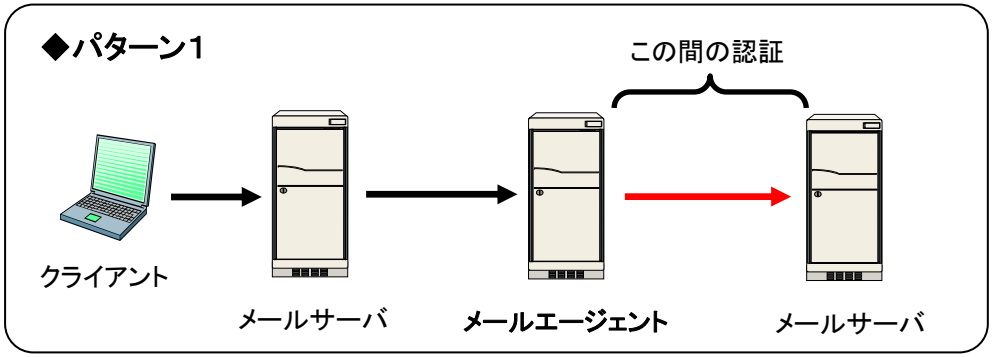
改版No	ページNo	変更内容	日時
1		制定	2009/06/29
2	3	「各認証とGuard3の関係」に追記	2011/04/05

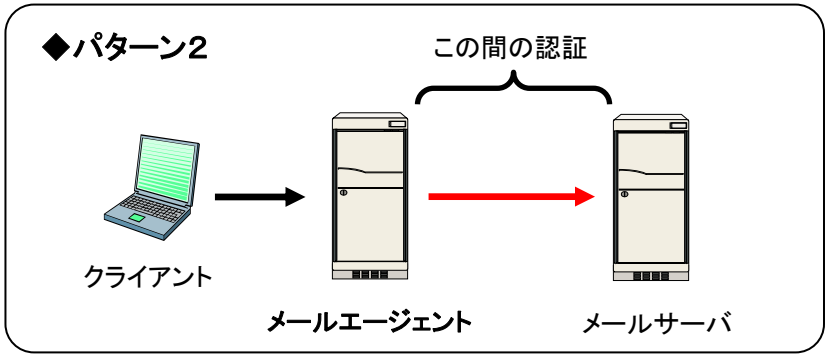
■メールの認証について

現在、迷惑メール業者などにSMTPサーバ（送信メールサーバ）を勝手に利用されないよう、ユーザ認証を行う仕組みが導入されています。
本資料では、この認証のうち代表的な2つ**「POP before SMTP」と「SMTP認証」の仕組みとGuard3運用時の注意点**について説明いたします。

■Guard3に関係するパターン

Guard3環境で、この認証が関係するのは　**メールエージェントからの転送経路において**　です。



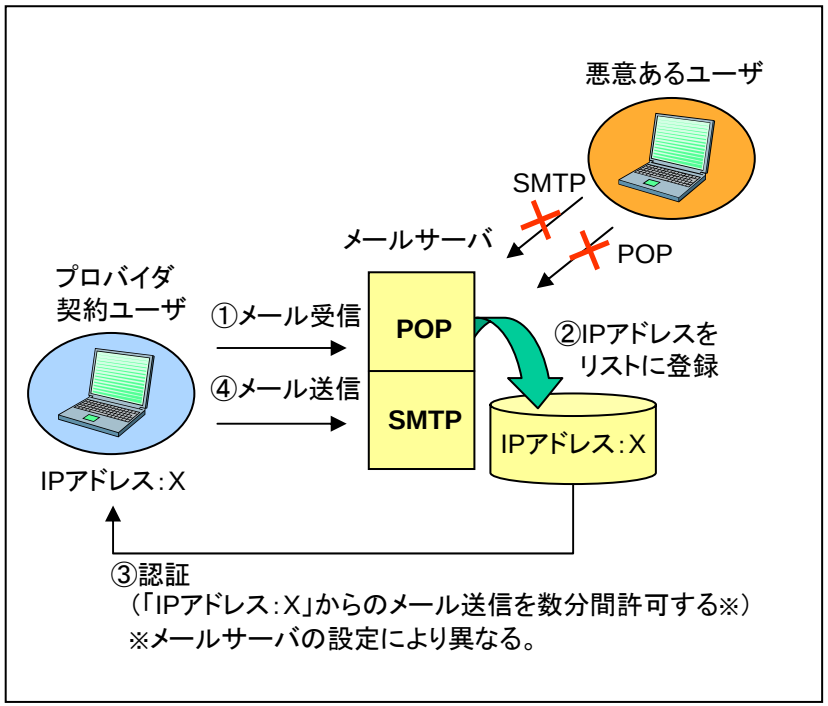


■各認証とGuard3の関係

認証タイプ	Guard3運用	制限事項
認証なし	○	問題なし。
POP before SMTP	△	クライアントにて送信前に受信処理が必要。
SMTP認証	○	問題なし。
POP3S/SMTPSなど暗号化認証	×	未対応。

■POP before SMTPについて

【仕組み】
POP before SMTPでは、ユーザ認証をPOPサーバが行います。
POPサーバとSMTPサーバを連携させ、一度POPサーバでユーザ認証（メール受信処理）を行ってからしばらくの間（設定による）は、認証を受けたコンピュータからのアクセスをSMTPサーバで許可します。
これにより、本来はユーザ認証の仕組みを持たないSMTPサーバでのユーザ認証が擬似的に可能となり、POPを通じてユーザ認証を受けていないユーザからのアクセスを拒否することになります。

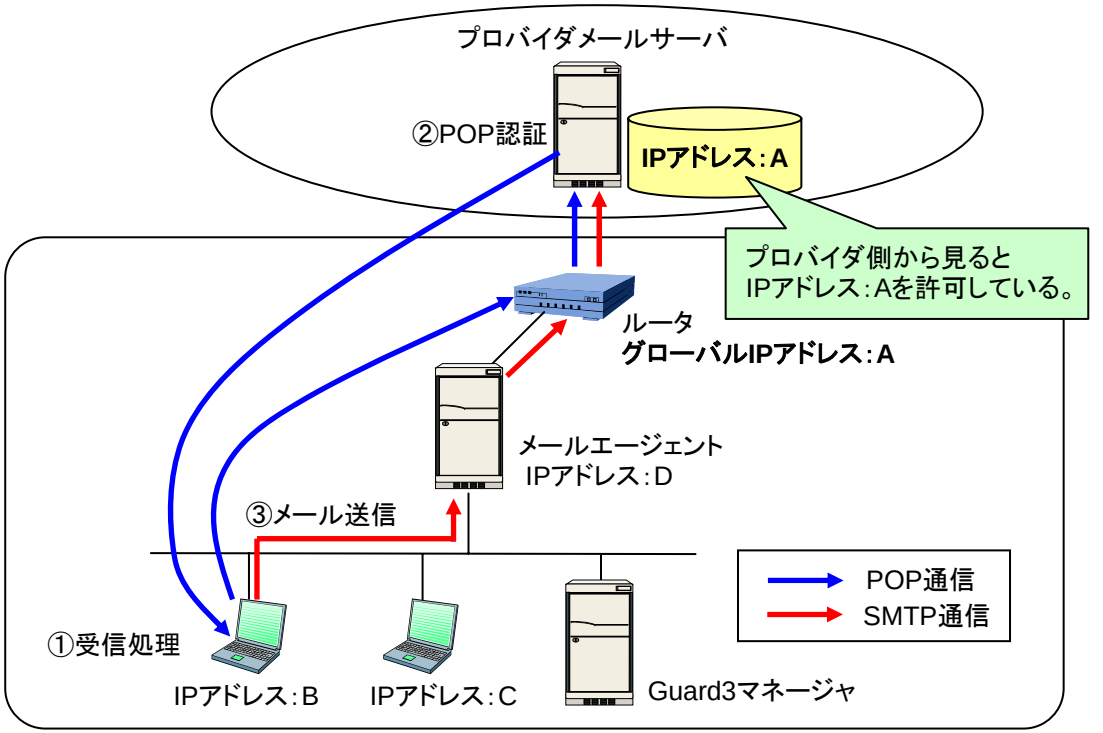


■LanScope Guard3を導入した場合

送信前に受信処理を行えば…

LanScope Guard3はPOP before SMTPでも運用可

POP before SMTP認証を設定しているメール環境の場合、リターンメール（メール送信、メール転送が失敗した場合にクライアントに送信するメール）設定で、リターンメール送信元アドレスに、実在するメールアドレスを設定する必要があります。実在しないメールアドレスの場合、ホスティングメールサーバで認証が通らず、リターンメールが送信できない場合があります。

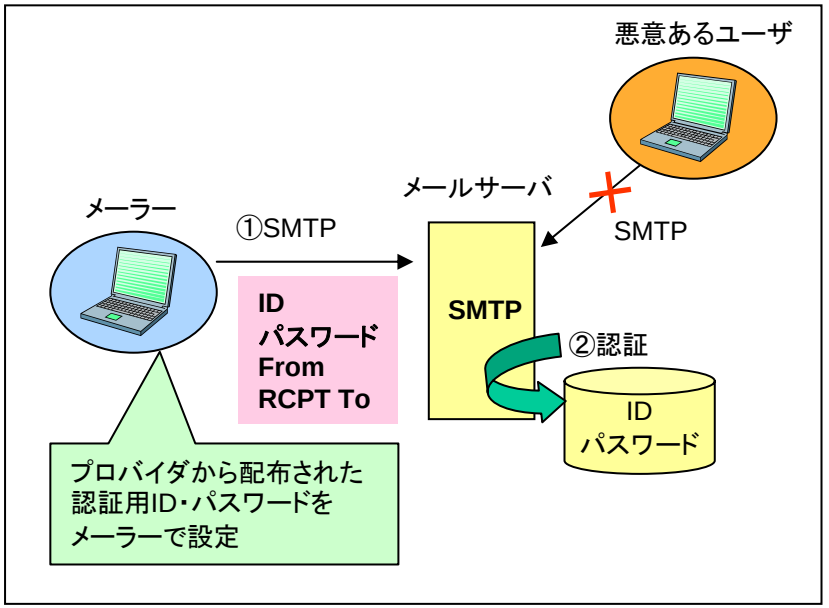


【上図例】IPアドレス「B」のPCがメールを受信すると、グローバルIPアドレス「A」がプロバイダメールサーバの許可リストに登録され、メールエージェントからのメール送信も許可される。

■SMTP認証について

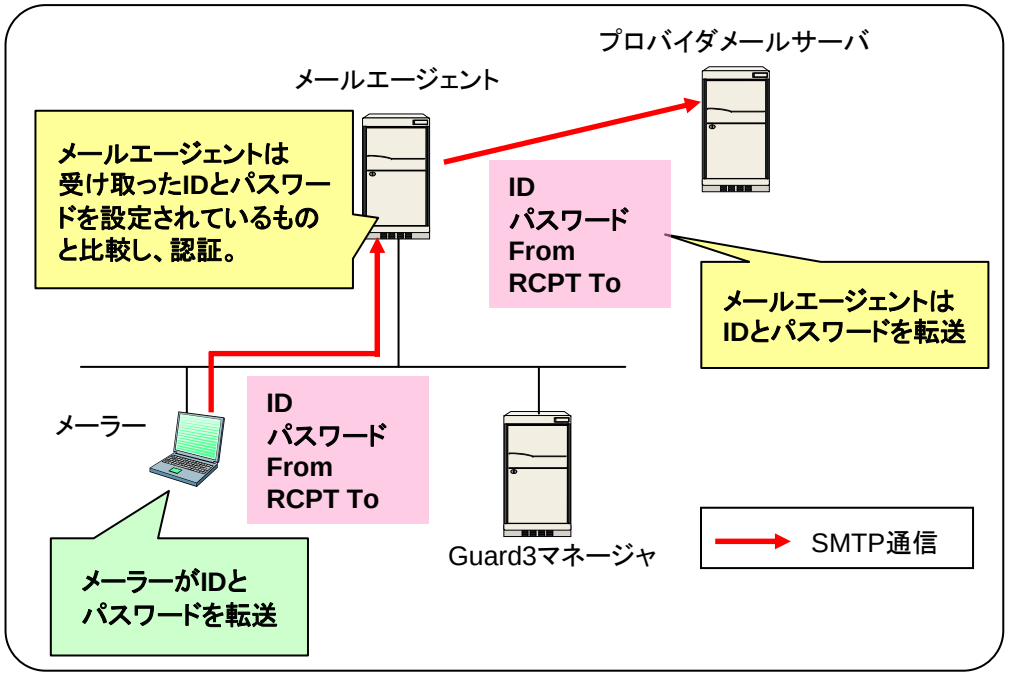
【仕組み】

SMTP認証とは、メール送信プロトコルであるSMTPにユーザー認証機能を持たせたもので、SMTP Authentication、SMTP-AUTHとも呼ばれます。
メールの送受信には、送信にSMTP、受信にPOPとそれぞれ異なるプロトコルを利用します。この場合ユーザー認証が求められるのはPOP（受信時）のみであったため、ユーザー認証のないSMTPを悪用して、スパムメール送信のためにSMTPサーバーが不正利用される、という問題が発生していました。
そのような問題を解決するために、メール送信時にユーザー認証を行なうようにしたのがSMTP認証です。
ただし、SMTP認証を使うには、メールサーバとメールクライアント（メーラー）の双方がSMTP認証に対応している必要があります。
SMTPサーバそのもので認証を行えば、前述のPOP before SMTPを使う必要はありません。



■LanScope Guard3を導入した場合

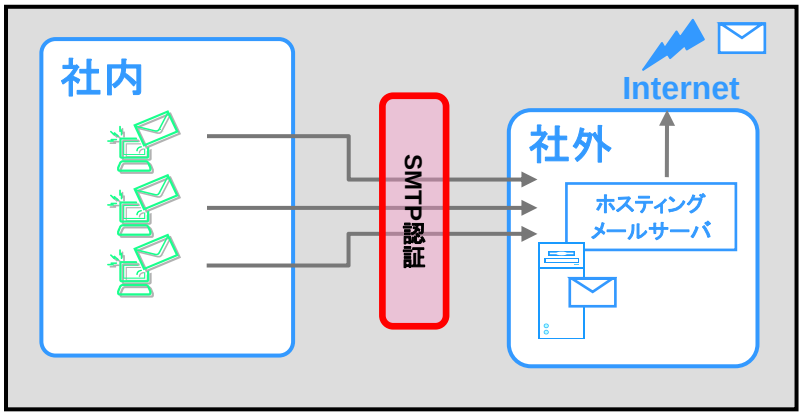
メールの送信が可能



【上図例】メールエージェント（以下MA）はメールに付加されたID・パスワードを転送する仕組みに対応しています。
MAはIDとパスワードの情報をもち、その情報を使用してメールの送受信を行います。
（MAの設定画面より、IDとパスワードを設定する必要があります。）

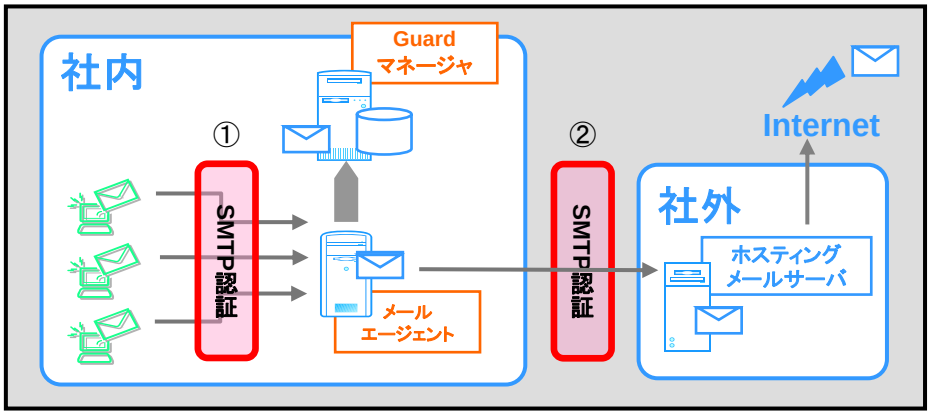
■SMTP認証を行うメールサーバが社外（ホスティング環境等）にある場合の導入例

【Guard3導入前】



導入例

【Guard3導入後】



※1000ライセンス以下のユーザ様ではGuardマネージャとメールエージェントの同居が可能なためサーバは1台で運用可能です。

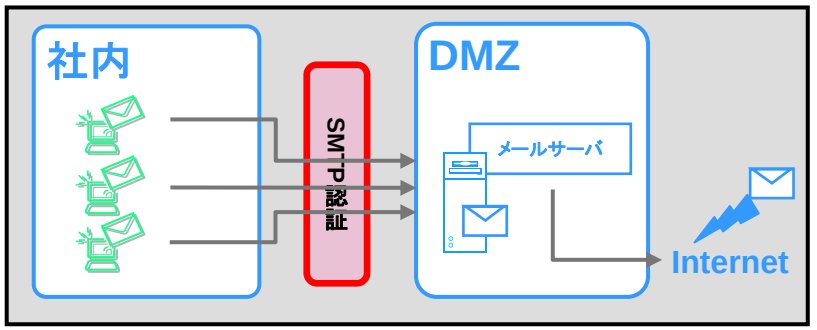
【導入に必要な設定】

①メールエージェントを社内に設置する。
②メーラのメール送信先をメールエージェントのIPアドレスに変更する。
③メールエージェントのメール転送先をホスティングサーバのIPアドレスに変更する。
④メールエージェントにSMTP認証のアカウントとパスワードを設定する。

※設定方法の詳細については、標準操作ガイド及び構築設定説明書をご参照ください。

■SMTP認証を行うメールサーバが社内（DMZ内等）にある場合の導入例

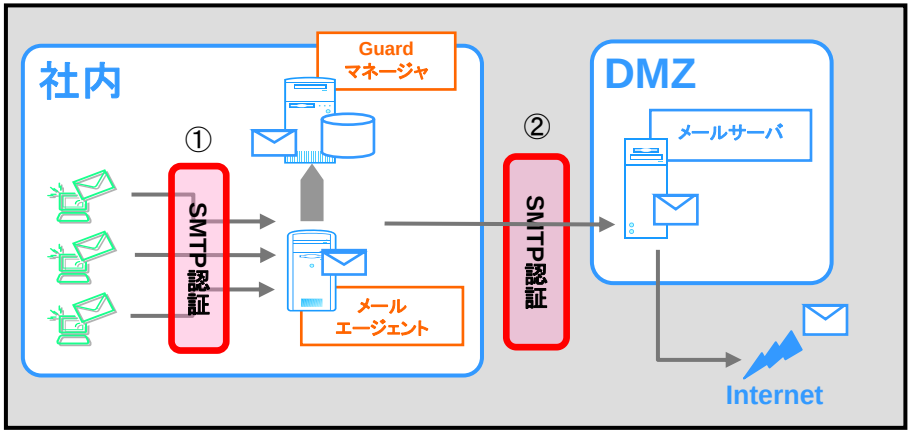
【Guard3導入前】



導入例1

導入例2

【Guard3導入後1】



※1000ライセンス以下のユーザ様ではGuardマネージャとメールエージェントの同居が可能なためサーバは1台で運用可能です。

【導入に必要な設定】

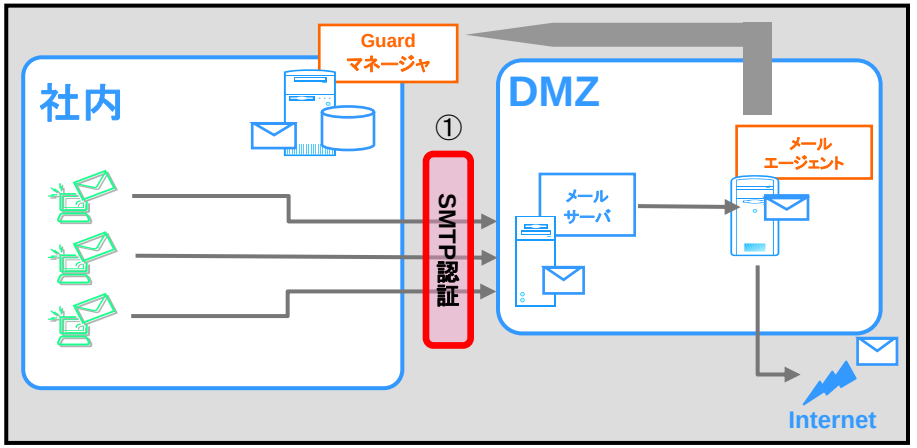
【Guard3導入後1】の場合：
①メールエージェントを社内に設置する。
②メーラのメール送信先をメールエージェントのIPアドレスに変更する。
③メールエージェントのメール転送先をメールサーバのIPアドレスに設定する。
④メールエージェントにSMTP認証のアカウントとパスワードを設定する。

【Guard3導入後2】の場合：
①メールエージェントをDMZ内に設置する。
②メールサーバのメール転送先をメールエージェントのIPアドレスに変更する。

※この場合、メーラのメール送信先を変更する必要がありません。

※設定方法の詳細については、標準操作ガイド及び構築設定説明書をご参照ください。

【Guard3導入後2】



※上記の環境ではGuard3用のサーバが2台必要になります。