PressNO.1606001

報道関係各位

2016 年 6 月 21 日

株式会社イー・ポスト

サイバー攻撃の総当たり攻撃対策を強化したメールサーバ

E-Post Mail Server シリーズの最新版を販売開始

～各サービスの認証接続時にロックアウト機能を追加～

メールサーバソフト開発・販売会社の株式会社イー・ポスト（本社；東京都新宿区、代表取締役；今西和也 http://www.e-postinc.jp/ TEL：03-5272-5386）は、この度、メールサーバソフトウェア**「E-Post Mail Server の最新版」**を 2016 年 6 月 21 日より、開始しますのでご案内申し上げます。

当社の Windows 版メールサーバソフト「E-Post Mail Server」は、高いコストパフォーマンスや安定性が評価され、一般企業や各省庁、県庁、自治体、金融、学校など多くの組織に導入が進んでおりますが、昨今のサイバー攻撃に対する機能強化の要望は高いものがありました。

サイバー攻撃の手段として、暗号や、パスワードを総当たりで割り出す総攻撃（ブルートフォース攻撃）があります。

一度ここの攻撃にさらされるとサーバの負荷が高まるだけでなく、破られるとその被害は甚大なものになる可能性があります。 そこで、SMTP 認証・POP3 認証・IMAP4 認証のそれぞれにおいて、たとえ総当たり攻撃を受けても、設定した回数でその接続をロックアウトし、その攻撃をブロック（遮断）してしまうロックアウト機能を E-Post Mail Server シリーズ、E-Post SMTP Server シリーズ、に追加いたしました。（※E-Post SMTP Server シリーズは SMTP のみ実装）

■販売製品

・メールサーバ：E-Post Mail Server シリーズ（32／64ビット対応）

・SMTP サーバ：E-Post SMTP Server シリーズ（32／64ビット対応）

・上長承認メール：E-Post BossCheck Server シリーズ （32／64ビット対応）

■価格例

E-Post Mail Server Standard シングルサーバ ： 8万円(50USER)

36 万円(500USER)

180 万円（10000USER）

（いずれも税別）

※64ビットネイティブ対応版、クラスタ版もあります。要問合せ

【背景】

E-Post の SMTP サービスにはもともと、接続時のリレー許可や拒絶などのふるまいを設定できる「中継の制限」【マシン毎の中継】機能が備わっています。【マシン毎の中継】は、【effect.dat】ファイルで設定でき、メールセキュリティの大きな中核を担っています。また、このほか、【メールフィルタ】機能も備わっており、迷惑メール対策に大きな効果をあげています。

SMTP プロトコルの利用で SMTP 認証が一般的でなかった時代には、これらの機能だけで大きな効力を発揮してきましたが、今や SMTP 認証での利用が当然な状態になってきました。外部からの不正利用を試みる者にとって、ID/パスワードを見破る必要性があり、それらが頻繁に試みられるようになりました。

今回、SMTP サービスに実装される「接続ロックアウト機能」は、既にあるこれらの機能に追加される形となり、セキュリティ的には三段構えの構成になります。「接続ロックアウト機能」が効力を発揮するのは、SMTP 認証で ID/パスワードを何千通り何万通りも試そうとする“総当たり攻撃”に対する防御として大きな力を発揮することが期待できます。

一方、POP3/IMAP4 の両プロトコルは、最初から認証ありきでした。外部から不正利用を試みる者にとっては、総当たりで POP3/IMAP4 の認証のために ID/パスワードを試みたとしても、労力が多い割には“成果”が得られなかったため、SMTP と比べて“総当たり攻撃”とは無縁でした。しかし、POP3/IMAP4 の ID/パスワードが SMTP 認証の ID/パスワードと同一に設定されているところが大部分であるとみなされたことから、ここ数年、パスワードを見破るための総当たりを POP3/IMAP4 に対しても試されることが目に見えて多くなりました。

もともと POP3/IMAP4 サービスには、認証がありますから、不正利用を防いでこれましたが、いわゆる“総当たり攻撃”には特段の対応方法もなければ、手段もありませんでした。真っ正直に認証失敗を繰り返すうち、サーバ負荷が異常に高まったりする危険性がありました。

今回、POP3/IMAP4 の両サービスにそれぞれ実装される「接続ロックアウト機能」は、特定の IP アドレスから執拗に繰り返される“総当たり攻撃”に対して、接続そのものを自動的に遮断できるようになりますので、サーバ負荷を不用意に高めたりすることなく、大きな効力を発揮することが期待できます。

【「接続ロックアウト」の基本機能】

1. SMTP 認証時・POP3 認証時・IMAP4 認証時にそれぞれ ID／パスワードが異なる理由で認証失敗し、特定の同一 IP アドレスからの接続回数が設定回数に達したとき、接続元 IP アドレスと接続時間情報を記録します。このとき各プロトコルでの情報は独立しており影響を与え合うことはありません。

2. さらに設定ロックアウト期間（時間）の間、SMTP サービス・POP3 サービス・IMAP4 サービスはそれぞれ、該当 IP アドレスからの接続を一切拒絶し、接続時に強制切断します。ここでも各プロトコルでの動きは独立しています。

3. 設定ロックアウト期間をすぎると、自動的に再度接続が可能となりますが、再び認証失敗を繰り返し設定された接続回数に達すると、再び同様の接続ロックアウト処理が繰り返されます。

4. SMTP サービス・POP3 サービス・IMAP4 サービスごとに記録された情報を管理者が編集することにより、接続回数に関わりなく、SMTP 認証時・POP3 認証時・IMAP4 認証時にそれぞれ特定の同一 IP アドレスからの接続を永続的に拒絶・切断させることが可能です。また、逆にリセットすることも可能です。

【その他の E-Post Mail Server の主な特長】

- 純国産の Windows によるソフトなので導入が容易で、簡単操作。
- 仮想 OS(VMWare、Hyper-V)導入実績多数。
- Windows Server2012 R2 対応。
- 簡易メールアーカイブ機能付き（ジャーナル機能）なので、メール消失時も復旧が容易。

- 低価格かつ、高機能、高性能の強力配送エンジン 10 万通/時間。
- ActiveDirectory 連携可能。
- LGWAN 対応オプションを用意。
- WEB によるリモート管理ツール付き。
- ログ取得用ログアナライザ付き。

詳細は、WEBページ参照ください。http://www.e-postinc.jp

【会社概要】

- 社名:　株式会社イー・ポスト
- 住所:　東京都新宿区高田馬場 1-33-14　サンフラワービル　〒169-0075

  TEL:03-5272-5386　FAX:03-5286-2610

- 設立:2000年7月19日
- 資本金:1000万円
- 代表者:今西和也
- 業務内容:

  ・コンピュータソフトウェアの開発、販売

  ・コンピュータネットワークの企画、開発、設計及びコンサルティング

  ・デジタル情報技術の開発

  ・各前号に附帯する一切の事業

記事掲載時のお問合せ及び、弊社製品に関する情報や質問は、下記へお願いします。

株式会社イー・ポスト　担当:木下

東京都新宿区高田馬場 1-33-14　サンフラワービル　〒169-0075

TEL:03-5272-5386　FAX:03-5286-2610

E-mail:　info@e-postinc.jp　　ホームページ:　http://www.e-postinc.jp/