

通常のメールが感染の疑いがあると判定される件について

平素は、ProScan をご利用頂きまして、誠にありがとうございます。掲記の件につきましてご説明申し上げます。

1. 現象

2008 年 8 月 19 日のエンジンアップデート以降、通常のメールを感染の疑いがあるメールとして判定するようになりました。(エンジンバージョン 2.1.12-61 より)これは、スキャンエンジンの機能の一つに、圧縮の多重度および MIME コンテナの入れ子状態をチェックするリミッターがあるのですが、その制限に引っかかるようになったためです。(MaxRecursion というパラメータが制限値となり、デフォルトでは 5 となっています。)本機能は、古いウイルスに基づく対処機能ですので、現在はほとんど、この機能でチェックするウイルスは出回っておりません。

お客様からの問い合わせで弊社でも現象を確認し、エンジン提供もとのドイツ Avira 社に問い合わせを行ないましたが、現時点でまだはっきりとした回答をもらえておりません。さらに強く原因の究明と対処を申し入れております。

2. 対処方法

ProScan の設定を変更することで回避可能ですので、その方法を以下にご説明いたします。

proscan.conf の[smtpscan.limits]セクションの MaxRecursion パラメータの値を 0
または 10~20 の大きな値に設定してください。(0 は無制限)

Libmilter 版をお使いの方は、proscanlm の再起動をお願いします。その他の MTA
の場合は、再起動の必要はございません。

3. 今後の対応

ドイツ Avira 社の回答によっては、このままの設定で運用して頂くか、設定を元に戻して頂く
かが変わってきます。追って、ホームページ等でご連絡致します。

以上

promark

株式会社プロマーク

サポート : support@promark-inc.com