ウイルス防御装置の設定について

2012 年 7 月 11 日
学術情報メディアセンター

学術情報メディアセンターでは，ウイルス防御装置を設置し，学内外から送信されるメールを監視し，ウイルスの検知やウイルスと疑わしいメールの検知を行なっています．現在，ウイルス防御装置では，(1) グレイリスト処理と (2) パターンによるウイルス防御処理の 2 種類を行っています．

(1) グレイリスト処理

1. ウイルス防御装置がメールのセッション要求を受け取った際に，メールの送信元ホストが学内ネットワーク内（130.158.0.0/16, 133.51.0.0/16）かどうか確認します．
2. 学内ネットワーク以外が送信元の場合，DNSの逆引き探索を行います．
3. 逆引き情報が設定されていない，またはFQDN名の形式にXX-XX-XX-XX.example.comなどのように数字の羅列が含まれていた場合，400番台の一時エラーを応答し，メール再送の要求を行います．
4. ウイルス防御装置は再送処理を2日間受け付け，再要求があれば送信元のホストを認証されたホワイトリストに追加し，35日間セッションを受け付けます（反対に，ウイルス防御装置からの他のサーバへの再送期間は7日間に設定されています）．

(2) ウイルス防御処理

表1に従って処理を行います．この他にもマスメーリング型ウイルス（無断で大量にメール送信を行うウイルス）と疑われる送信を検出した場合には，そのメール配送の停止や遅延を行うことがあります．

表1：ウイルス防御処理の設定

	学外→学内	学内→学外または 学内→学内
ウイルス未検出の場合	そのまま配送します.	そのまま配送します.
ウイルス検出の場合	検出した旨のメッセージを追加し，ウイルスを削除して配送します. （同時にセンター側にもその事実を通知します.）	メッセージを隔離して，送信者に通知します.
ウイルスを検出したが削除に失敗した場合	添付ファイルを削除したメールにスタンプメッセージを追加し，宛先へ配送します. （同時にセンター側にもその事実を通知します.）	メッセージを隔離して，送信者に通知します.
ウイルス検出不能の場合	ウイルスチェックが行えなかった旨のメッセージを挿入して，配送します.	ウイルスチェックが行えなかった旨のメッセージを挿入して，配送します.
セキュリティ設定違反の場合	ウイルスチェックが行えなかった旨のメッセージにオリジナルメールを添付して配送します. （同時にセンター側にもその事実を通知します.）	ウイルスチェックが行えなかった旨のメッセージにオリジナルメールを添付して配送します. （同時にセンター側にもその事実を通知します.）

- 「隔離」とは，ウイルス防御装置がメールを保存し，宛先へは元のメールを配信しないことを指します.
- 「通知」とは，元のメールとは別の検出の事実を知らせるメールを配送することを指します.
- 「ウイルス検出不能」とは，メール自体が暗号化されている場合やパスワード保護された添付ファイルを含んでいる場合，または添付ファイルが破損している場合など，何らかの理由でウイルスが正しく検出できない状況を指します.

- 「セキュリティ設定違反」とは，ウイルス防御装置自体を保護するために設定された閾値を超える状況を指します．例えば，メールが圧縮された添付ファイルを含んでおり， その中のファイル数が1,000を超える状況などが該当します.

ウイルス防御装置に関する注意事項

前述のセキュリティ設定違反に加えて，ウイルス防御装置を保護するためにenvelope-from が空欄（null）となっているメールを暗黙で破棄するよう設定されています．これは，本大学のメールアドレスを詐称して第三者によって大量のメールが送信された場合に，大量のエラーメールが本学のウイルス防御装置に届き，過負荷となるのを防いでいます，しかしながら，副作用として正規のエラーメールもウイルス防御装置によって破棄される恐れがあります.

また，この文書に記載されている事項以外については，基本的にウイルス防御装置のメーカ推奨設定を採用しています.

以上