学内向け（受信用）メールゲートウェイの設定について

2013 年 7 月 16 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メールゲートウェイを設置し，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，メールゲートウェイでは，(1) SenderBase 評価スコア(SBRS)に基づく送信元ホストの確認，(2) アンチウィルススキャン (3) アンチスパムスキャンの 3 種類の処理を行っています.

(1) SenderBase評価スコア(SBRS)に基づく送信元ホストの確認

1. メールゲートウェイ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のIPアドレスに基づき，評価スコア(-10～10)を判定します.
2. 評価スコアと，手動で設定したブラックリスト・ホワイトリスト，DNSが逆引きできるかのテストによって，以下の処理を行います.

表1: SBRSに基づく送信元ホストの確認処理ポリシー

	条件（３つの条件はORで働きます）			
送信グループ	①送信元IP	②SBRSスコア	③DNS逆引き	処理
WHITE	特定のリストに登録済み	7.0以上		配信
UNKNOWN		-2.0以上7.0未満		配信
SUSPECT		-6.0以上-2.0未満		200通/1時間までに制限
DARK		-8.0以上-6.0未満	逆引き失敗	20通/1時間までに制限
BLACK	特定のリストに登録済み	-8.0未満		着信拒否

表1のポリシーは，ベンダー推薦のポリシー設定のうちで，誤って着信を拒否してしまうfalse positiveがほぼ皆無とされているConservativeポリシーよりも，さらにfalse positiveの可能性が少ない，極めて保守的な設定となっています．

（参考）

http://www.cisco.com/cisco/web/support/JP/docs/SEC/EmailSecur/IronPortEmailSecurApplian/UG/001/reputationfiltering.html?bid=0900e4b1827e1445#pgfId-1110553

http://www.senderbase.org/home

それでも万一，特定の送信元からのメールが受け取れない場合はご連絡ください．

(2) アンチウィルススキャン

受信メールゲートウェイを通過したメールについて，表2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2：アンチウィルススキャンの処理ポリシー

ウイルス未検出の場合	そのまま配送します．
ウイルスを検出した場合（ウィルス削除に成功した場合）	添付ファイルからウイルスのみを削除して配送します．（同時に，センターの管理者にもその事実を通知※1します．） メールの件名に[WARNING: VIRUS REPAIRED]という文字列を挿入し，本文にもウィルスを検出した旨の警告文を挿入します．
ウイルスを検出したがウイルスのみの削除に失敗した場合	添付ファイルを全て削除したメールを宛先へ配送します．（同時に，センターの管理者にもその事実を通知※1します．）メールの件名に[WARNING: VIRUS REMOVED]という文字列を挿入し，本文にも警告文を挿入します．
ウイルス検査不能※2の場合	メールの件名に[WARNING: MESSAGE ENCRYPTED]という文字列を挿入し，本文にもウ

	イルスの検査が行えなかった旨の警告文を挿入して，配送します.
セキュリティ設定違反※3の場合	メールの件名に[WARNING: A/V UNSCANNABLE]という文字列を挿入し，本文にもウイルスの検査が行えなかった旨のメッセージを挿入して，配送します．（同時に，センターの管理者にもその事実を通知※1します．）

※1 「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.

※2 「ウイルス検査不能」とは，添付ファイルに暗号化されたファイルやパスワード保護付きのファイルを含んでいる場合，または圧縮された添付ファイルが破損しており，正しく解凍できない場合など，何らかの技術的な理由でウイルス検査ができない状況を指します． 現在の仕様では，書き込み保護されたPDFファイルなど一部のセキュリティ保護されたファイルは検査不能と判定され，検査しないまま開くことができてしまいますのでご注意下さい.

※3 「セキュリティ設定違反」とは，ウイルス防御装置の負荷を高める不自然なメール等を指 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、その中に多数のファイ ルが存在する、何重にも圧縮がかけられたファイル、そのような添付ファイル付きメール が該当します。ウイルス防御装置自体を過度の負荷から保護するための措置です。

(3) アンチスパムスキャン

スパム(あるいは疑わしい)と判定したメールについては，次の情報が付加されます.

- 件名に[Spam]あるいは[Suspected Spam]
- ヘッダ情報に X-Ironport: Positive あるいは X-Ironport: Suspected

スパムと判定したメールもすべて配送しますが，この付加情報を用いれば，利用者がフィルタする事が可能です.

以上