セキュリティポリシーと電子メール

CAUA FORUM 2008「大学における電子メールを再考する」

武藏 泰雄

熊本大学総合情報基盤センター・

ネットコミュニケーション研究部

アジェンダ

- セキュリティポリシーとメールに関連する話題
- 熊本大学へのセキュリティポリシーの導入
- メールサーバでのスパム対策
- スパムボットの検知と対策
- まとめ

セキュリティポリシーと電子メール（1）

- 大学におけるセキュリティポリシーについての話題：
  - 「政府機関の情報セキュリティ対策のための統一基準」への対応

    2005年12月決定 http://www.nisc.go.jp/conference/seisaku/dai2/pdf/2siryou03.pdf

    1. 政府統一基準をそのまま受け入れる？
    2. サンプル規定集を利用するかどうか？

       http://www.nii.ac.jp/kouhou/NIIPress06_09-3.pdf
    3. 大学全体としてISMS(ISO27001)取得を目指すか？

       http://cic-hp.zam.go.jp/tokyo/detail.php?pub_id=78

- 大学における電子メールに関する話題：
  - Spamメール対策
    1. Spamメールを受信しない（メールサーバ側の対策）
    2. Spamを送信しない（メールサーバ側の対策とスパムボットへの対策）

セキュリティポリシーと電子メール（2）

- 「政府機関の情報セキュリティ対策のための統一基準」への対応

  2005年12月決定 http://www.nisc.go.jp/conference/seisaku/dai2/pdf/2siryou03.pdf

1. 政府統一基準をそのまま受け入れる場合

- 長所: 非常に良くまとまっており、完成度は高いように見える
- 短所: 省庁ベースなのでそのままでは国立大学法人等へは向かないため、大学に合うように詳細に検討する必要があり、コストが高い

2. サンプル規定集を利用するかどうか？

- 長所: 詳細な検討がされており、導入コストが低いように思える
- 短所: あるのかも知れないが、今のところ導入事例が見当たらない

3. 大学全体としてISMS(ISO27001)取得を目指すか？

- 長所: ISMS認証取得を部分的にまたは大学全体として導入事例は何件かある
- 短所: これを取得しても構成員への教育周知徹底は非常に困難を伴う、取得してもセキュリティを守れないことがあり、そういう事例もある

セキュリティポリシーと電子メール（3）

- **Spamメール対策**

1. **Spamメールを受信しない、メールサーバ側での対策**

   (1) ホワイトリスト・ブラックリスト
   (2) コンテンツフィルタ
   (3) 実装の差異を利用したspam判定
   (4) 遅延・通信流量制限
   (5) 経験則による判定

2. **Spamメールを送信しない、メールサーバ側での対策**

   (1) OP25B (Outbound Port 25 Blocking)
   (2) 送信者ユーザの認証

3. **Spam Botsの検知**

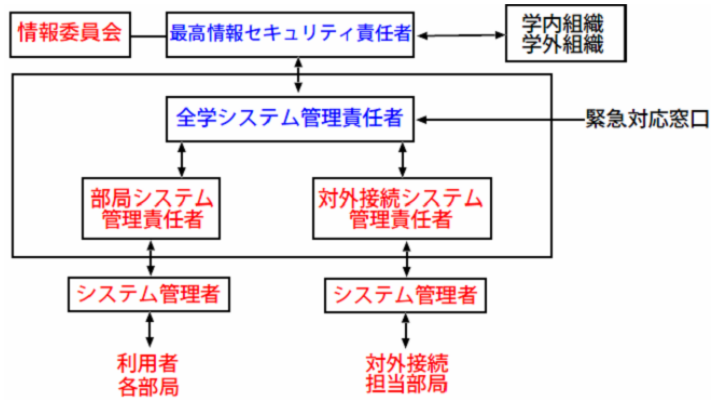
   (1) メールサーバやIDSでの検知
   (2) DNSトラフィック監視によるスパムボットの検知

熊本大学へのセキュリティポリシーの導入（1）

- 基本ポリシーとスタンダードの策定

作業期間: 2001年8月～2003年2月
雛形利用:「大学における情報セキュリティポリシーの考え方」2002年4月配布
承認委員会: 情報推進化会議・情報推進専門委員会

A. 情報セキュリティポリシーの内容
・目標
情報セキュリティに対する侵害を阻止
学内外の情報セキュリティを損ねる加害行為を禁止
情報資産に関して、重要度による分類とそれに見合った管理
情報セキュリティに関する情報取得の支援
・対象・範囲
教職員、学生、来学者、外部委託事業者等
システム管理者（研究室のPCなどは教職員）
外部から持ち込まれたPCも含む
情報システムは24時間365日稼動
・対策基準
組織・体制
情報の分類と管理
物理的セキュリティ
人的セキュリティ
技術的セキュリティ
評価・見直し



熊本大学へのセキュリティポリシーの導入（2）

- プロシージャ(実施手順書）

作業期間: 2003年6月～2004年3月
雛形利用:「大学における情報セキュリティポリシーの考え方」2002年3月CD配布
承認委員会: 情報化推進会議・情報化推進専門委員会

データの分類
非公開データの管理
非公開データの消去/複製
非公開データのバックアップ

物理的セキュリティ

人的セキュリティ
PC使用時の構成員の責任
不正アクセス被害状況報告

技術的セキュリティ
サーバ等のアクセス記録の取得及び分析
アクセス制御
ウィルス対策

既存サーバ/PCのウィルス対処
新種のウィルス感染発見時の処理
新種と既知のウィルスの相違
システム脆弱性悪用型ワーム

連絡体制

既知のセキュリティインシデントは報告しなくても良い。

ウィルスも新種とシステム脆弱性悪用型に限る。

上記の構成にすることにより、当初57頁あったものが、13頁に圧縮できた。

熊本大学へのセキュリティポリシーの導入（3）

- 公開データと非公開データ

  - 公開データを、データ漏洩(流出)により該当データの作成者(管理者)、データの利用者及び大学に不利益が生じないものであり、公開可能なものと定義します。理想的には個人情報をまったく含まないデータのことですが、現実的には多少の個人情報を含んでいても公開しないといけないデータも含まれています。

  - 非公開データを、個人情報や大学の運営に関る重要な機密情報を含むものと定義します。具体的に言えば、SOSEKI等の学務情報や附属病院、保健センター等の診療に関する情報、大学の財務、経理、ネットワークIPアドレスや全学向けサーバ、メールサーバ、研究目的で知り得るところの企業秘密やログ情報、情報の非公開契約をした情報が含まれているデータということになります。

熊本大学へのセキュリティポリシーの導入（4）

- 不正アクセス被害状況報告

プロセス	手続きを行う者	手続き
（Ⅰ）連絡 ↓ （Ⅱ）報告 ↓ （Ⅲ）確認	構成員 構成員 全学システム管理責任者	・不正アクセスを発見した場合，緊急連絡としてシステム管理者及び部局システム管理責任者へ連絡し，指示を仰ぐ。 ・「不正アクセス被害状況報告書」（別紙様式4-2-1）に必要事項を記入する。 ・記入済の報告書をシステム管理者，部局システム管理責任者及び部局情報セキュリティ責任者が確認後，全学システム管理責任者に提出する。 ・提出された報告書の記入内容を確認する。

熊本大学へのセキュリティポリシーの導入（5）

- サーバ等アクセス記録の取得及び分析

プロセス	手続きを行う者	手続き
（Ⅰ）システムログ提出の依頼 ↓ （Ⅱ）ログ採取依頼 ↓ （Ⅲ）ログの採取 ↓ （Ⅳ）ログの提出 ↓ （Ⅴ）確認	全学システム管理責任者 部局情報セキュリティ責任者 システム管理者 部局情報セキュリティ責任者 全学システム管理責任者	・「サーバ及びネットワークのアクセスに関するログの提出依頼書」（別紙様式5-1-1）に必要事項を記入する。 ・記入済みの提出依頼書を部局情報セキュリティ責任者に依頼する。 ・提出依頼書に基づき当該システムを管理するシステム管理者へログの採取を依頼する。 ・ログを提出依頼形式の媒体等に採取し，部局情報セキュリティ責任者に提出する。 ・ログの記録された媒体等と提出依頼書を全学システム管理責任者に提出する。 ・提出されたログの解析を行う。

熊本大学へのセキュリティポリシーの導入（6）

- 新種のウィルス感染発見時の処理

プロセス	手続きを行う者	手続き
(Ⅱ)指示	使用機器が感染した構成員	・ネットワーク環境（ＬＡＮ）から使用機器を取り外す。
↓		
(Ⅰ)緊急連絡	システム管理者	・使用機器は電源ＯＮの状態を継続する。
↓		
(Ⅲ)対処	構成員及びシステム管理者	・システム管理者に状況を報告する。
↓		
(Ⅳ)復旧	構成員及びシステム管理者	・報告を受けたシステム管理者は，６．１．１「事案発生時の連絡」に従い，早急に事象の連絡を部局システム管理責任者に行う。又，ウィルス対処方法が全学システム管理責任者等から通知されている場合は，その指示に従う。
↓		
(Ⅴ)報告書の作成	構成員	・ウィルス駆除方法を確認後，機器使用者に適切な指示を与える。
↓		
(Ⅵ)報告書の確認	システム管理者	・全学システム管理責任者等の指示に従い，ウィルス対策を行う。
↓		
(Ⅶ)再発防止対策	全学システム管理責任者	・ウィルス対策完了後，全学システム管理責任者等の指示に従い，使用機器を復旧する。
		・「新種のウィルス感染報告書」（別紙様式5-3-3）に必要事項を記入し，システム管理者に提出する。
		・提出された報告書の記入内容を確認後，部局システム管理責任者及び部局情報セキュリティ責任者の確認を経て，全学システム管理責任者に提出する。
		・提出された報告書の記入内容を確認する。
		・再発防止策を検討し，職員に再発防止策を周知徹底する。

メールサーバでのスパム対策（1）

(1) ホワイトリスト・ブラックリスト
(2) コンテンツフィルタ
(3) 実装の差異を利用したspam判定
(4) 遅延・通信流量制限
(5) 経験則による判定

- Spamメールを受信しない、メールサーバ側での対策

(1) ホワイトリスト・ブラックリストモデル

ー アカウントや 送信元のサイトについてアクセスの可否を設定する方式である。
例えば、

- ACL(Access Control List)
- RBL(Realtime Black List)

などが知られている。

長所：利用者にも管理者にも判りやすい、説明しやすい方式。

短所： ACL方式は認証管理(IdM)システムとの連携が適切であれば問題は減少すると考えられるが、手動ではもはや考えられないし、またRBLは有効であるものの、政治的な圧力に潰されやすく、かつ良く自然消滅するためサーバの設定変更をしないといけないのに気づきにくいなどの問題がある。

メールサーバでのスパム対策（2）

(1) ホワイトリスト・ブラックリスト
(2) コンテンツフィルタ
(3) 実装の差異を利用したspam判定
(4) 遅延・通信流量制限
(5) 経験則による判定

- Spamメールを受信しない、メールサーバ側での対策

(2) コンテンツフィルタ

ーメールヘッダおよび本文の内容で spamかどうか判定する方式である。
例えば、

●キーワードによる単純なフィルタ: Spamassasin
●単語の生起確率によるベイジアン型学習フィルタ: BogofilterやBsfilte
●URI Black List (URIはほぼURLのことです): Vipul's Razor
●利用者の報告に基づく公開データベース: 手動等 Web Mailerなどに多い

などがあります。

長所: 処理が高速である。

短所:コンテンツフィルタの欠点はspam判定のファルスポジティブです。つまり誤判定によるメールの紛失問題です。この問題は大変大きな政治問題に発展することがありますので難しい問題です。また最近ではメール本文を画像化してそれを添付する画像spam を使う回避策が増加する傾向にあり、それをspamと判定できないファルスネガティブも増加しています。

メールサーバでのスパム対策（3）

(1) ホワイトリスト・ブラックリスト
(2) コンテンツフィルタ
(3) 実装の差異を利用したspam判定
(4) 遅延・通信流量制限
(5) 経験則による判定

- Spamメールを受信しない、メールサーバ側での対策

(3) 実装の差異を利用したspam判定

ースパムMTAは再送、MX RRのフォールバック、プロトコル違反による再送処理に対応できないと仮定する方式である。 例えば、

- **再送処理:** Greylisting、お馴染みさん方式、S25R方式
- **MXリソースレコード処理**：MXフォールバック判定、Unlisting、Nolisting、GION
- **プロトコル違反**：Greeting pause、EHLO、HELOへのフォールバックチェック

などがあります。

長所：**SMTP Envelope**で処理でき、単純なスパムMTAには効果が大きかった。

短所：実装が甘いがでも正当なMTAを除外する手作業があること、再送処理によって遅延が発生すること、再送処理をきちんと理解できるスパムMTAに置き換わって来たことと、組織内の脆弱性のあるローカルな正当なMTAを経由するスパムMTAの出現によってもはや単なる負荷かけ処理となっている。

メールサーバでのスパム対策(4)

(1) ホワイトリスト・ブラックリスト
(2) コンテンツフィルタ
(3) 実装の差異を利用したspam判定
(4) 遅延・通信流量制限
(5) 経験則による判定

- Spamメールを受信しない、メールサーバ側での対策

(4) 遅延・通信流量制限

一時間当たりでスパムの通信量を減らす方式である(牛歩戦術) 。
例えば、

- 時間当たりの全体の送信量を減らす:Spamd (Open BSD), Symantec Mail Security 8100
- スパムと判定されたホストに対して実行する: Spamd, Symantec Mail Security 8100

などがあります。

長所:スパムの流量を減らし、下流のサーバの負荷を軽減でき、スパム配送業者の作業効率を下げることが可能である。

短所:現在のところ対応できるMTAやOSが限られており、あるいは専用のハードウェアが必要となる。

メールサーバでのスパム対策（5）

(1) ホワイトリスト・ブラックリスト
(2) コンテンツフィルタ
(3) 実装の差異を利用したspam判定
(4) 遅延・通信流量制限
(5) 経験則による判定

- Spamメールを受信しない、メールサーバ側での対策

(5) 経験則による判定

ースパムがどこから送られて来るかを注意深く観察するなどスパム対策を講じて来た結果や経験をベースにしてスパムと判定する方式である。
例えば、

- 逆引きが不可能なMTAを拒否・制限
- 逆引きホスト名が動的IPアドレスに基づく等特定のルール に当てはまる場合を拒否・制限

する方式があります。

長所：一般的なスパムから特定のアカウントやホストを狙ったスパムに対応できる。

短所：経験則にたよるため例外がある。

メールサーバでのスパム対策（6）

- より高度なスパムメール対策

(6) DNSを経由して送信側MTAの正当性を確認する

－正当な送信側MTAのIPアドレスに関する情報をDNSサーバに登録し、受信側でそれを確認して判定する方式である。
例えば、

- **DNSサーバに正当なMTAを登録する方式:** SPF (Sender Policy Framework)
- **DNSサーバに公開鍵を登録する方式:** DKIM (DomainKey Identifier Mailed)
- **SPF方式をSMTPエンベロープではなく、メッセージヘッダで処理する方式:** Sender ID

があります。

長所：SPFやDKIMはSMTPエンベロープでチェックできる。またSender IDではどのような経路からメールが転送されて来たを知ることが可能となる利点がある。

短所：DKIMはメーリングリストサーバで再送時にDKIMを書き換える必要がある。またSPFとSender IDは似ていそうでまったく別物のため誤実装が多く有効に使えていない。またスパムが正当なMTAを介して発信された場合は、それを防ぐ方法を別に実装する必要がある。

メールサーバでのスパム対策(7)

- Spamメールを送信しない、メールサーバ側での対策

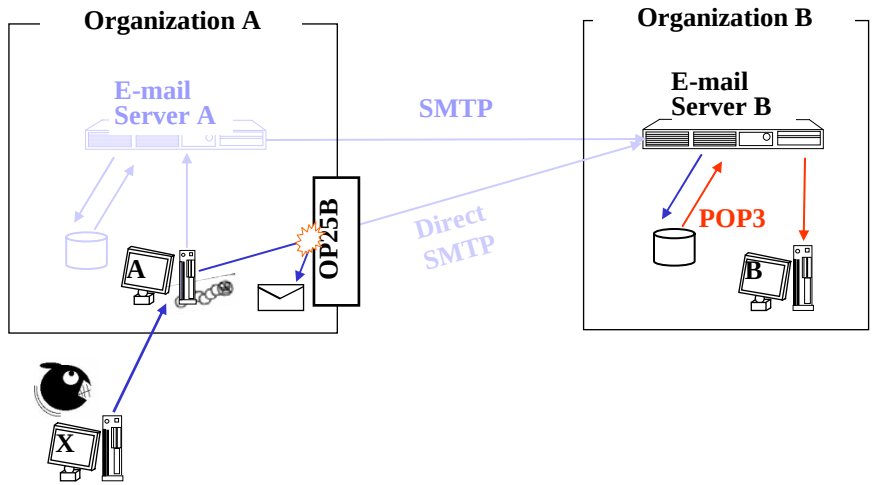
(1) OP25B (Outbound Port 25 Blocking)
(2) 送信者ユーザの認証

(1) OP25B (Outbound Port 25 Blocking)

ースパムボットからのスパム送信やメール型ウィルスの送信をブロックする方式です。
具体的には、L3スイッチ(ルータ)やFWなど指定したMTA以外からの組織外へのSMTP送信をブロックします。

長所: スパムボットなどの正当でないMTAから犠牲ホストへの直接メール送信を阻止することができる。

短所:組織内から見ればオープンリレーである。このため不要なメールサーバを整理する必要がある。組織外のメールサーバを組織内LANから利用することができなくなるため、利用者の反発が出る可能性がある。



メールサーバでのスパム対策（8）

- Spamメールを送信しない、メールサーバ側での対策

(1) OP25B (Outbound Port 25 Blocking)
(2) 送信者ユーザの認証

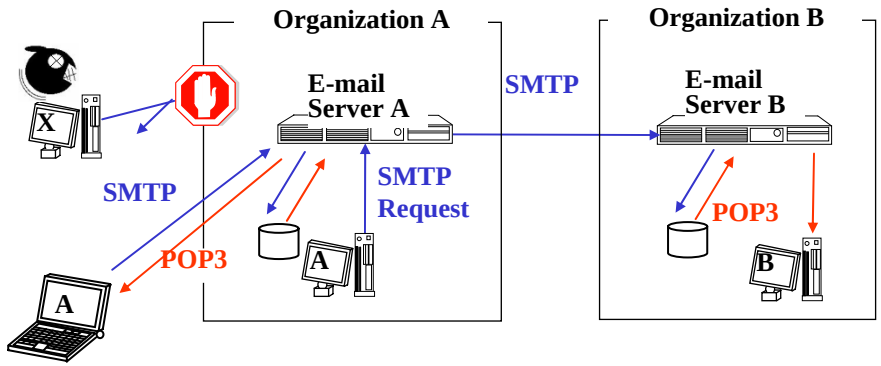
(2) 送信者ユーザの認証（SMTP AUTH）

ースパムボットからのスパム送信やメール型ウィルスの投稿をブロックする方式です。

具体的には、送信側MTAの投稿・配送ポートをTCP 25番からTCP 587番など別のポートへ変更します。また組織外からメール送信したい場合は、POP before SMTP over SSLとSMTP AUTHを行います。後者をInbound Port 25 Blocking（IP25B）と呼びます。

長所：スパムボットなどの正当でないMTAから犠牲ホストへの直接メール送信を阻止することができる。

短所：問題点は、投稿ポートの設定に対応しかつSMTP AUTHに対応できるMUAを利用者が使用していなければ意味がありません。いきなりOP25Bを導入する前に投稿ポートを利用者に周知し、OP25BやSMTP AUTHに対応していない利用者へ対応済みのMUAへの切り換えを促進していく必要があります。



(3) スパムボットの検知

スパムボットの検知と対策（1）

(1) メールサーバやIDSでの検知
(2) DNSトラフィック監視によるスパムボットの検知

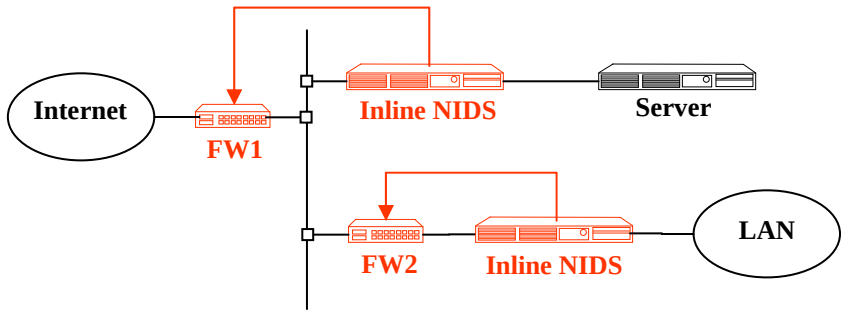
- スパムボットの検知と対策

(1) メールサーバやIDSでの検知

－メールサーバのログやIDS/IPS等でSMTP関連のチェックを行い検知を行います。
具体的にはメールサーバの/var/log/maillogなどからスパム関連の行を抜き出して統計を取り、組織内が送信元になっているものを探します。IDS/IPSなどでも同様の作業を行います。

長所：比較的小規模な組織内のメールサーバを経由するスパムメールやIDSの検知ログを調査することでスパムボットのIPアドレスが判る。

短所：メールサーバを経由しないスパムメールは検知できない。またIDSで採取されるログは、ポートスキャンだけで一日あたり400MB以上であり、それにSMTPまで設定すると、データの取りこぼしなど性能低下が起こり、中・大規模な組織では現実的に不可能である。



スパムボットの検知と対策（2）

(1) メールサーバやIDSでの検知
(2) DNSトラフィック監視によるスパムボットの検知

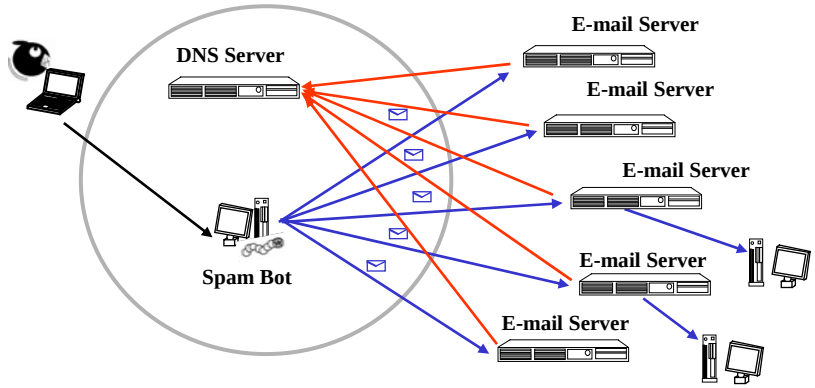
- スパムボットの検知と対策

(2) DNSベースのスパムボットの検知

ー組織内のPC端末や組織外のC&Cサーバ やIDSセンサーからのDNSサーバへのDNSクエリパケット流量を監視して、組織内のセキュリティインシデントを検知する方式である。特にスパムボット活動を行っているPC端末等のIPアドレス候補を検出するのに有用である。

長所：中・大規模組織内の新種のトロイ等スパムボット活動を行っているのPC端末の早期発見が可能であり、迅速に対策を打つことが可能である。

短所：あくまでも疑わしいIPアドレス候補であるため、可能な限り状況証拠や組織外での接続点や該当IPアドレスを持つPC端末とLAN間のパケットキャプチャリングが必要である場合があり、該当者PC所有者または利用者から協力を得る必要があること。



まとめ

今回は、「セキュリティポリシーと電子メール」と題し、下記の項目について説明させていただきました。

(1) 熊本大学への情報セキュリティポリシーの導入について、基本ポリシー・対策基準および実施手順書の策定について

(2) メールサーバにおけるスパム受信および送信対策について

(3) スパムボットの検知・対策について

実際スパムボットの検知を行っているのですが、利用者からの反発もなくほぼ問題なく調査できております。これも情報セキュリティポリシーの実施手順書に、「不正アクセスの被害状況の報告」、「サーバ等アクセス記録の取得及び分析」、および「新種のウィルス感染発見時の処理」の三つの項目を設定していたおかげであると考えています。