サイエンティフィック・システム研究会
システム技術分科会 2008 年度第 2 回会合資料

2009 年 1 月 29 日

セキュリティマネージメント WG 活動報告
ーアカデミック機関でのセキュリティマネージメント
BCP（ベストカレントプラクティス）ー

高エネルギー加速器研究機構
湯浅 富久子

[Abstract]

情報システムの構築にセキュリティという要素が欠かせなくなってから、ほぼ 10 年が経過しました。その間にテクノロジの進歩や規則整備の努力によりアカデミック機関における情報セキュリティ対策は一巡しました。しかし一方で、情報システムをとりまくセキュリティ情勢は厳しさを増しています。このような状況のもとでは、最新のテクノロジを理解するにとどまらず、情報セキュリティマネージメントという視点からセキュリティ対策を継続していかなければ、リスクの激しい変化や増大する業務に対応していくことは困難です。

セキュリティマネージメント WG は、現時点で実現可能なセキュリティ対策を設計、実装、検証するために役に立つマネージメント・ノウハウをわかりやすくまとめることをテーマに活動を続けてきました。2007 年 1 月からの 2 年間にわたる活動が終了しましたので、ここに報告します。

[Keyword]

情報セキュリティマネージメント、BCP（ベストカレントプラクティス、現時点における最善の実践）

1 はじめに

近年インターネットの治安情勢は悪化し続け、情報セキュリティに関わる問題は深刻化しています。研究・教育を主たる目的とするアカデミック機関でもその影響を大きく受けざるを得なくなっています。外部からの攻撃は、大規模で表面化しやすいものから小規模なものへ、面白半分のいたずらから金銭目的へと量・質ともに変化しました。情報システムが組織内で重要インフラとなった現在では、情報セキュリティ抜きのシステム構築はもはや考えられません。加えて、Web や電子メールなどの基幹アプリケーションを攻撃から保護することは当たり前のこととして IT 部門に要求されるようになりました。

しかし、IT 部門のみでは組織全体の IT 環境を安全に維持し続けることは困難になっています。例えば、ボット感染による犯罪への加担、情報漏洩や著作権侵害、Web 改ざんによるフィッシングサイトの構築などインシデントは多種多様です。被害に遭う対象者も、職員、教員、学生、研究員、非正規雇用職員、一時来訪者、外部共同研究者、退職者、卒業生など組織に関わる全ての人間へと広がっています。このようにセキュリティに関わる守備範囲は広がる一方です。情報セキュリティ対策を、掌握可能な範囲にとどめ着実に課題を解決していくには、マネージメントという考え方を持ち込んで対応します。これが本 WG が発足した理由です。

情報セキュリティマネージメントでは、技術力と効率性の追求だけでなくこれまで IT 部門にあまり蓄積されていない「モラルを高める技術」、「体制を構築する技術」、「セキュリティ監査技術」などあらたな技術が必要となります。これらの技術は裏方の技術ですが、本 WG ではこれらの技術にスポットをあてました。自分が明日からセキュリティマネージメントに従事する時にあって欲しいノウハウを提供できるよう、テーマを選択しました。いずれのテーマにおいても最終結論を模索するのではなく、現時点における最善の実践とは何か、という考え方ですすめました。

2 第一期活動

第一期には、「組織」、「spam 対策」、「デジタルフォレンジック」の三つをテーマに選びました。それぞれについての詳しい内容は、成果報告書[1]を参照してください。本発表ではこのうちの「デジタルフォレ

ンジック」について、報告書から一部抜粋して紹介します。

2.1 デジタルフォレンジック

デジタルフォレンジックは、過去に起こったインシデントを科学的に立証するための証拠を保全・収集・分析することを意味する言葉です。この言葉はまだ一般的には浸透していません。しかしアカデミック機関がサイバー犯罪に巻き込まれてしまうリスクを考えれば、フォレンジックについての知識を得ることが必要です。

刑事（民事）事件などの重大なインシデントが一旦発生すれば、IT 部門と総務部門という別々のミッションをもつ独立した部門を組織的に動かしていかないと物事がうまく進みません。これにはセキュリティマネージメントという視点が必要です。IT 部門が、IT に関する問題のよろず取締り部署とみなされてしまわないように、総務部門と所掌範囲についてセキュリティマネージメントを行う者が境界の制御やフォレンジック作業をリードしていかなければなりません。

デジタルフォレンジックの具体的な最初の一歩はログデータの収集です。収集したログは、その完全性をなんらかの方法で維持していきます。一例としてはログの分散バックアップ保存などがあります。ログを円滑に収集するために PC やサーバ等の情報機器にログエージェントを導入することもあります。また、IT 部門で時刻配信サービスや組織全体のシスログ受信サービスを用意すれば、広く利用されることが期待されます。なおログの保存期間は判例から 3 年程度と言われています。この間は維持可能でなければなりませんので、ハードルは低くはありません。ログの取り扱いや解析手法も技術的に成熟していない部分があることが WG では指摘されました。

いずれのサービスも予算と人員の配置が必要です。ログデータの保全をアウトソーシング化する、解析をアウトソーシング化するなどを念頭におきつつ、情報設備の増強を施すことを考えなければいけません。これには組織としての判断が必要でしょう。なお、詳しいデジタルフォレンジックの解説には、[2], [3], [4] などがありますので、参考にしてください。

3 第二期活動

第二期には、「人間・管理・インシデントハンドリング」、「状況確認のためのセキュリティアプライアンス」および「エンドポイント」の三つをテーマに選びました。それぞれについての詳しい内容は、成果報告書[5]を参照してください。本発表ではこのうちの「状況確認のためのセキュリティアプライアンス」について、報告書から一部抜粋して紹介します。

3.1 状況確認のためのセキュリティアプライアンス

組織におけるセキュリティインシデントの発生状況を認識することは、組織の情報セキュリティ対策を計画するにあたって大変重要なことです。現実世界で事故や犯罪の起こりやすい地域に監視カメラや検問を設置するように、ネットワーク上にもそのような機能がなければ、状況を正しく認識することができず、「攻撃者」を捕らえたり、リスク分析に基づく次の一手を打ったりすることができません。そのような機能の技術的な解として、さまざまなセキュリティアプライアンスが開発されています。通常これらの機器は、セキュリティの強化によるインシデントの予防という側面が注目されますが、発生時の緊急対応や調査のための証拠の収集に有効であり、また逆に外部で発生したインシデントに対する身の潔白を示すために重要な役割を果たすこともあります。

代表的なセキュリティアプライアンスとして、ファイアウォール(FW)、侵入検知システム(IDS)、侵入防止システム(IPS)、統合セキュリティアプライアンスとしての UTM、および Web アプリケーションファイアウォール(WAF) があります。WG ではこれらについて、その特質をまとめました。また、セキュリティアプライアンスによって対策される具体的な事例として P2P ファイル共有の問題について取り上げています。

「P2P」とは「Peer to Peer」のことで、元々は計算機ネットワークの形態の一つを指す言葉です。この言葉は、P2P モデルを応用したソフトウェアそのものを指すこともあります。応用例としてはファイル共有が有名ですが、それ以外にも音声通信やコンテンツ配信などがあります。P2P 自体は単なる通信技術の一つですが、応用としてのファイル共有ネットワークが世界的に問題視されている現状があります。主な問題点は、違法に複製されたソフトウェアや動画の共有とウイルスなどに起因する情報漏えいです。また、P2P ソフトウェアの多用のためにネットワーク帯域が圧迫され、通常利用に差し支えるという問題が起こ

ることもあります。このため、組織としてP2P ファイル共有ソフトウェアを制限・遮断したいという要求が、経営部門からとIT部門の両方からだされることがあります。しかしP2Pではポート番号を必ずしも固定する必要がないため、単純な静的ポート遮断では対応できず、ネットワーク側で対策するにはより高性能・高機能(即ち高価な)のセキュリティアプライアンスの導入が必要となります。またセキュリティアプライアンスは、ネットワークの設計段階でその設置ポイントを考慮しなければ有効に使えません。組織内のネットワークの更新計画時にセキュリティアプライアンスの導入を前提にしたネットワーク設計を行う必要があるということになります。その際、セキュリティアプラインスを用いる理由を組織内で明確にしておくことが大切になります。

セキュリティアプライアンスのなかには、すべてのパケットをモニタする機能をもつものが多く、通信のプライバシに抵触する可能性があることを認識しておかなければなりません。これにもセキュリティ規則の整備や広報などマネージメント的な要素が重要です。

3.1.1 アンケート

セキュリティアプライアンスを利用できるようになったのは、ここ10年のことです。アカデミック機関でも、経済的あるいは人的なコストをかけてこれらのアプライアンスを導入し運用しています。アプライアンスは便利な箱ですが、採用するテクノロジの寿命が短いこと、やや柔軟性を欠くこと、価格が高いことなどの難点もあります。選定では、他の機関の事例を知れば大変参考になります。また、先に述べたP2Pに対してアプライアンスをどのように生かしているのかなど具体的な効能も気になることです。

そこでWGでは、現状を把握するためにアンケートを実施することにしました。アンケートは

1. 「ファイアウォール、侵入検知・防御装置、ウェブアプリケーションファイアウォールなど」の導入とそのポリシーについて
2. 「P2P」関連ソフトウェアに関する対策とそのポリシーについて

の二項目構成としました。アンケートの設問内容を表1と表2に示しました。アンケートには10機関に回答をいただきました。本発表では、アンケート結果の一部を紹介しますが、詳細は成果報告書[5]をご覧ください。

表1「ファイアウォール、侵入検知・防御装置、ウェブアプリケーションファイアウォールなど」の導入とそのポリシーについての設問

I	設問
1.	組織全体の取り組みとして導入しているものは何ですか
2.	UTMを導入している組織は、その機器の有する機能と利用している機能は何ですか
3.	1.や2.で回答した機器を導入することになった経緯を、差し支えない範囲で教えてください
4.	導入して良かったことは何ですか（セキュリティ的な観点と、運用の観点から）
5.	導入して大変だったことは何ですか（セキュリティ的な観点と、運用の観点から）
6.	ファイアウォール、IDS/IPSなどのさまざまなログをどのように扱かっていますか（長期保存や閲覧規則など）
7.	トラフィックの監視や流量制限を実施する際の根拠はどのようなものですか
8.	ログやIDSで収集された通信内容には、通信の秘密やプライバシー等のセンシティブな情報が含まれている可能性がありますが、これら情報の扱いはどのような権限で行われていますか
9.	1.であげた機器のうち、以前導入していたが運用をやめた機器があれば、その種類と理由を教えてください

表 2 「P2P」関連ソフトウェアに関する対策とそのポリシーについての設問

II	設問
1.	P2P 方式を利用したソフトウェアの制限等を実施していますか
2.	どのような種類のソフトウェアを制限していますか
3.	制限する手段はどのようなものですか
4.	制限している理由を、差し支えない範囲で教えてください
5.	制限の根拠はどのようなものですか
6.	P2P 関連ソフトウェアへの制限等を実施していない理由は何ですか
7.	P2P によるファイル交換で、外部組織から通知を受けたことがありますか
8.	どこからの通知だったか、差し支えなければ教えてください
9.	通知に、どのように対処しましたか
10.	その他 P2P に関するコメント等ありましたら、ぜひご記入ください

4 組織と人間

「組織と人間」は、第一、第二期の両期にわたって WG で最も議論されたところです。いくらやってもやまぬセキュリティ対策では、IT 部門が疲弊してしまいます。疲弊しないためには、体制作りと教育が有効です。これらは即時性はありませんが、じわっときいてきます。本発表では、WG の議論や成果報告書の内容を一部抜粋し紹介します。

4.1 マネージメント体制

情報システムや情報資源を守り、情報化による恩恵をうけるためには、組織的な対応が不可欠です。組織における情報セキュリティの基本方針を定めるセキュリティポリシーの策定、そのポリシーに基づいた安全な情報システムの構築、そしてそのポリシーの遵守状況の確認のためにも、セキュリティマネージメント体制はなくてはなりません。情報漏えいや不正侵入などのインシデントに際しても、迅速かつ的確に対応するための非常時用体制も日頃から整えておく必要があります。文部科学省からの通達もありアカデミック機関でも、セキュリティポリシーを策定しているところが殆どですが、最初のポリシー策定から時間が経過している組織もあります。ポリシーや実施手順について PDCA サイクル[1]が求められていますが、アカデミック機関の場合、「高等教育機関の情報セキュリティ対策のためのサンプル規程集[6]」を利用することで、PDCA サイクルをまわすための人的コストを下げられる可能性があります。

4.2 情報セキュリティ教育

情報セキュリティは担当者の技術力だけでは守れません。情報システムの利用者の一人一人が注意しなくてはなりません。そのため、情報セキュリティに関する教育が重要となります。教育は講習会や E-Learning システムで行いますが、経営部門などの上級職員、教員、一般職員、学生など職位別あるいは階層別に教材を準備しないと効果がでにくくかえってコストがかかります。エンドユーザ、システム管理者、システム発注者およびアプリケーション開発者などを区別した教育も必要です。こうなるとセキュリティ教材を IT 部門が独自にすべて用意することは不可能です。有償・無償のセキュリティ教材[7]を活用してコストをさげることが大事です。

アカデミック機関の場合、職員向けのセキュリティ講習会を開催してもその効果をチェックすることが十分にされていないことが有ります。講習後は、チェックテストを必ず行うようにします。講習会の教材を機関間で共有したり、教材の内容を相互に評価したりするなどしてお互いにコストを減らしていくことも考えられます。

1 PDCA cycle：Plan（計画）, Do（実行）, Check（評価）, and Act（改善）のサイクル

5　おわりに

セキュリティマネージメントWGはマネージメントに関連する六つのテーマを選択し、ノウハウをまとめ成果報告書に納めました。本発表では、「spam 対策」や「エンドポイントのためのセキュリティ対策」など実用性に富むテーマについては内容を紹介できませんでしたので、これらについては成果報告書をご覧くださることをお願いします。最後になりましたが、WGメンバーを紹介して本発表を終わります。

第一期	テーマタイトル	メンバー
1	セキュリティマネージメントのための組織	只木（佐賀大）、吉田（FJ）
2	spam 対策	吉田（大分大）、笠原（九大）、長谷川（中京大）
3	デジタルフォレンジック	武蔵（熊本大）、湯浅（KEK）、山田（FJ）、須永（SSL）
第二期	テーマタイトル	メンバー
1	人間・管理・インシデントハンドリング	長谷川（中京大）、湯浅（KEK）、吉田（大分大）
2	状況確認のためのセキュリティアプライアンス	笠原（九大）、武蔵（熊本大）、須永（SSL）
3	エンドポイント	三谷（FJ）、只木（佐賀大）、吉田（FJ）

参考文献

[1] http://www.ssken.gr.jp/MAINSITE/activity/workinggroup/securitymng/report1.html
[2] 上原哲太郎, “ ディジタルフォレンジック”, IPSJ Magazine Vol.48, No.9, pp.889-898 (2007)
[3] 辻井重男監修, “ デジタル・フォレンジック事典”, 日科技連出版社, ISBN4-8171-9208-9
[4] 特定非営利活動法人デジタル・フォレンジック研究会, http://www.digitalforensic.jp/
[5] http://www.ssken.gr.jp/MAINSITE/download/wg_report/securitymng/index.html
[6] http://www.nii.ac.jp/csi/sp/
[7] セキュリティ教材（無償）
15 分でわかるウィルスの脅威(IPA)：http://www.ipa.go.jp/security/y2k/virus/cdrom2/index.html，
警察庁サイバー犯罪対策の情報セキュリティ対策ビデオ：
http://www.npa.go.jp/cyber/video/index.html ，
情報モラル啓発ビデオ（ハイパーネットワーク社会研究所）：
http://www.hyper.or.jp/staticpages/index.php/moral#moral_video ，
インターネット社会を安全に暮らすために（人工知能研究振興財団）：
https://www.tokai-ic.or.jp/selfdefense/ ，
日本セキュリティ協会(JNSA) の無償セキュリティ教育：http://www.jnsa.org/ ，
セキュリティ力ランキング：http://www.jnsa.org/Seculiteracy/index.html