セキュリティマネージメントWG
成果報告書

2009年1月

サイエンティフィック・システム研究会
セキュリティマネージメントWG

目次

はじめに

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る。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ある。

本WGは、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目標に、2007年1月より2009年1月まで活動してきた。活動は、準備会と計8回の会合（8回目は合宿）、メーリングリストで交換した約400通のメール、Webコンテンツマネージメントソフト POESYの利用の3本柱からなっている。2年間を第一期と第二期に分けて、各期で成果レポートを作成した。本報告書には、第二期、第一期の順番で二つの成果レポートをおさめている。両方の期で「組織・人間に関わるテーマ」、「実用的なテーマ」および「先進的なテーマ」の三つを選択し、合計で六つのテーマに取り組んだ。成果レポートでは、それぞれのテーマについての議論をレジメの文章とスライド形式にまとめている。第一期の特徴については第一期成果レポート中の「はじめに」で紹介した。ここでは第二期で選んだテーマについて簡単に紹介する。

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」をテーマに選んだ。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なにかを考えた。最初のテーマでは、情報セキュリティにおいて最も脆弱な存在である人間をどう管理するのか、セキュリティ体制をどのように良質に保っていくのか、実際にセキュリティ事故の発生に対して組織と人間はどう振る舞うべきなのか、について議論した。二つ目のテーマでは、最新のセキュリティテクノロジを実装するアプライアンスについて考察した。具体的な事例として P2P ファイル交換ソフトウェアを取り上げ、セキュリティマネージャとしての考え方をまとめた。このテーマのもと 10 の組織にセキュリティ・アンケートを実施させていただき、回答を頂いた。アンケート結果をまとめたので参照して欲しい。三つ目のテーマでは、これまで利用者側にまかされていた「エンドポイントセキュリティ」をどうマネージしていくのかについて、松竹梅の三つのソリューションを用意し議論した。それぞれの特徴を表形式で示したので、エンドポイントシステムの設計に役立てていただければ幸いである。

まとめ役
湯浅富久子

1. WG 概要

1. WG 概要

(1) 活動方針

近年インターネットの治安情勢は悪化しつづけ、情報セキュリティに関わる問題は深刻化している。攻撃は、大規模で表面化しやすいものから金銭目的の小規模なものへと変化し、研究・教育を主たる目的とする会員所属機関においてもサイバー犯罪にまきこまれる可能性がでてきている。

本 WG では、水際で奮闘するセキュリティ担当者に有用な情報を提供することを目的に、先進的なセキュリティ対策(攻めのテーマ)と実用的なセキュリティ対策(守りのテーマ)を 2 本の柱として議論を重ねていきたい。また、会員の多くをしめる大学機関においては、部局の自治を尊重しつつもセキュリティの質を低下させないマネージメント力が要求されている。本 WG では技術的な話題に閉じず、組織論などを含むセキュリティマネージメントのノウハウも共有していきたい。

(2) WG メンバー

			氏名	機関/所属
会員	担当幹事		長谷川明生*	中京大学
	推進委員	まとめ役	湯浅富久子	高エネルギー加速器研究機構計算科学センター
			吉田　和幸	大分大学総合情報処理センター
			笠原　義晃	九州大学情報基盤研究開発センター
			武蔵　泰雄	熊本大学総合情報基盤センター
			只木　進一	佐賀大学総合情報基盤センター
			長谷川明生	中京大学
富士通	推進委員	まとめ役**	三谷　修	富士通(株)計算科学ソリューション統括部
		まとめ役***	山田　久仁	富士通(株)計算科学ソリューション統括部[当時]
			吉田　真和	富士通(株)文教ソリューション統括部
			須永　知之	(株)富士通ソーシアルサイエンスラボラトリ

*推進委員兼務。 **2008 年度の推進委員。***2007 年度の推進委員。

(3) WG 活動経過

本 WG は、タイムリーな検討と会員へのフィードバックを目指し、2 年間の活動期間を第一期と第二期に分け、それぞれ 3 つの検討テーマを設定して活動した。各検討テーマは、それぞれチーム制とし、同時進行で検討を行った。

第一期テーマについては、2007 年 11 月 27 日に「第一期成果レポート」としてまとめ、SS 研 Web サイトに掲載した。

(http://www.ssken.gr.jp/MAINSITE/activity/workinggroup/securitymng/report1.html)

WG 会合の概要を表 1-1 に、検討テーマとメンバーを表 1-2 に示す。

表 1-1　WG 会合の概要

	日　時	場　所	活動内容
準備会	2006 年 10 月 14 日(土) 14:30～18:00	九州大学	・活動メンバーの確認 ・活動内容/成果物の検討 ・活動の進め方の検討
第 1 回	2007 年 2 月 7 日(水) 14:30～17:30	九州大学	・活動の進め方の検討 ・活動テーマの検討、整理 ・第一期テーマ:情報交換/意見交換
第 2 回	2007 年 6 月 10 日(日) 13:30～17:10	九州大学	・第一期テーマ:キーワードの洗い出し、整理 ・POESY の評価、改善点の検討
第 3 回	2007 年 8 月 7 日(火) 13:30～17:30	富士通本社	・第一期テーマ:情報収集、検討、報告書作成 ・POESY の評価、改善点の検討
第 4 回	2007 年 11 月 6 日(火) 13:30～17:45	富士通 九州営業本部	・第一期テーマ:報告書作成 ・第一期テーマ:成果フィードバックの検討 ・第二期テーマ:活動の検討
第 5 回	2008 年 3 月 12 日(水) 13:30～17:45	富士通 九州営業本部	・第二期テーマ:キーワード洗い出し、整理 ・第二期テーマ:フィードバック(成果物)の検討
第 6 回	2008 年 7 月 1 日(火) 13:30～17:45	富士通 九州営業本部	・第二期テーマ:情報収集、検討、報告書作成
第 7 回	2008 年 9 月 8 日(月) 13:30～17:30	富士通 九州営業本部	・全体テーマの整理 ・第二期テーマ:情報収集、検討、報告書作成 ・セキュリティ・アンケートの内容/実施方法の検討
第 8 回	2008 年 12 月 11 日(木)15:00～18:30 12 日(金) 9:00～12:00	富士通 湯布院荘	・第二期テーマ:報告書作成 ・成果報告書の検討 ・成果報告の検討 ・後継 WG の検討

表 1-2　テーマとメンバー

活動期	テーマ	メンバー（*リーダー）
第一期	セキュリティマネージメントのための組織	只木*、FJ 吉田
	Spam 対策	吉田*、笠原、長谷川
	デジタルフォレンジック	武蔵*、湯浅、FJ 山田、SSL 須永
第二期	人間・管理・インシデントハンドリング	長谷川*、湯浅、吉田
	状況認識のためのセキュリティアプライアンス	笠原*、武蔵、SSL 須永
	エンドポイントのためのセキュリティ対策	FJ 三谷*、只木、FJ 吉田

2. 第二期検討テーマ

2.1. 人間・管理・インシデントハンドリング

2.1. 人間・管理・インシデントハンドリング

はじめに

大学や研究所の IT 環境において、セキュリティの確保は重要な課題である。国立大学法人等にあっては、セキュリティポリシーおよびガイドラインのひな形が示され、ポリシー策定およびポリシーに基づいたセキュリティ体制の整備が急務となっている。

一方で、インターネットのセキュリティ状況は悪化の一途をたどっている。そのような状況で、個々の利用者の日常的行動が組織のセキュリティに大きな影響を与える。情報セキュリティにおける組織や人間の在り方について検討し整理した。

セキュリティにおける人間要因

どんなに高性能なセキュリティアプライアンスやセキュリティソフトウェアを導入したとしても、その導入による安心感に満足してしまっては、効果は限定的なものになり、かえって脆弱性を作りかねない。情報セキュリティを維持するためには、情報システムを企画、運用・管理、そして利用する人間の心構えが重要である。たとえば、ファイル共有ソフトウェアで特定のファイルのダウンロードを実行することにより（たとえば Winny や BitTorrent）、自動的に著作権等を侵害する可能性のある他のファイルの配布の中継に加担してしまうことや、ウィルス対策ソフトウェアのパターンファイルに登録されるまでの時間が長いスピア攻撃（特定少数を標的とする攻撃）への対処の方法など、利用者の高いセキュリティ意識がなければ防げない。好奇心からウィルスを実行してみるなどは言語道断である。

このためには、構成員全員に情報セキュリティ教育を行う必要がある。定期的に開催する講習会や、自分のペースで進められる e-Learning システムのコンテンツでの提供が考えられる。情報セキュリティ教育は、新たな技術の習得ではなく、セキュリティ意識の啓発であるので、何らかの形での強制力を持った義務化が必要である。

セキュリティ教育の対象は構成員全員ではあるが、大学の場合、役員、教員、事務職員、学生のそれぞれの立場での対応が必要である。役員に対しては、情報システム投資の中に情報セキュリティ投資が必須なこと、教員に対しては、成績データ等の個人情報と研究情報等のそれぞれのセキュリティレベルの認識などである。

組織のセキュリティの水準は、もっとも低いレベルに制約されることになるので、セキュリティ教育に当たっては、入門教育、初級教育を重視するべきである。小中学生向け教材はそれ以外の場面でも有用である。公開されている情報セキュリティ教材について URL をスライド形式の資料中にまとめたので参考にしてほしい。JNSA のセキュリティキャラバン、ハイパーネットワーク社会研究所の情報モラルセミナー等の無料のセミナー、講習会の利用も考えられる。

セキュリティの管理

セキュリティポリシーを作成し、ガイドライン等の整備をし、PDCA サイクルを実施することは、組織のセキュリティ確保にとって重要である。しかし、セキュリティポリシーやガイドラインを策定し、体制を用意しただけでは不十分である。誰のための何のためのセキュリティポリシーであり、セキュリティ体制であるか、組織の構成員が考え行動可能なように、組織としてセキュリティ戦略を立てて日常的に行動すべきである。

セキュリティポリシーやガイドライン策定については、「高等教育機関向けセキュリティポリシーのひな形」が参考になる。

組織のセキュリティ体制や実施状況については、セキュリティ監査が不可欠である。内部監査だけでは不十分で、第三者機関による定期的な監査と問題指摘が重要である。その際に、監査の対象や期間について十分な検討が必要になる。監査に際して、監査人の資格要件や監査結果データに関する秘密保持契約についても検討が必要である。第三者監査を実施する際の仕様書例を付録 A に添付した。

監査の成果がセキュリティ状況の改善につながらないと意味がない。第三者監査とともに、組織内の部局間での相互監査やテーマを決めての近隣大学間での相互監査は、セキュリティ意識の

向上に役立つと思われる。
組織のセキュリティ体制の外部への表明として、ISMS やプライバシーマーク等の取得以外にも、組織のセキュリティ情報を審査格付けするセキュリティ格付け会社が発足し、セキュリティ格付けのトライアルを開始している。
また、ポリシーやガイドライン遵守を個々の利用者の意識に委ねる状態では不十分で、シンクライアントシステム等のミスの発生しないシステムや不正のできないセキュアなシステムの導入整備も重要である。
CSIRT（インシデントレスポンスチーム）を整備し、インシデントハンドリング体制や連絡窓口の整備が急務であるが、今後はセキュリティを日常的に戦略的に考え行動するセキュリティオペレーションズセンター（SOC）という考えも重要である。セキュリティ管理全体を BCP(Business Contingency Plan)/BCM(Business Contingency Management)の中に取り込む考えもある。

インシデントハンドリング

セキュリティマネージメントに携わっていると、一定の割合でセキュリティインシデントの発生に遭遇する。インシデントは、ウィルス感染かもしれないし、不正侵入かもしれない。またいつ発生するのかも予想できない。しばらく発生していないなと思っていると、続いて複数のインシデントが発生してんてこ舞いになることもある。マネージメントでは、いずれのインシデントに対しても一定以上の速度で対応しなければならないが、作業の優先順位を正しく決めるためのトリアージを定めておくとずいぶんと楽になる。このトリアージという言葉は、救急医療の分野で使われている用語で、Wikipedia には「最善の救命効果を得るために多数の傷病者を重症度と緊急性によって分別し、治療の優先度を決定すること」とある。
トリアージと同じくらい大切なことに、ハンドリングにおいて中心的な役割を担う PoC（Point of Contact）という連絡窓口を決めておくことがある。PoC が車輪のハブのような役目を果たし、これによりインシデントハンドリングという車輪がまわって前に進んでいける。しかし、たとえ PoC がスキルフルな人物であったとしても、PoC が一人で全てを背負い抱えてしまわないようにマネージメントでは制御していかないといけない。それにはあらかじめ、取り扱うインシデントの範囲などを定めた規則類を整備しておくのが有効である。この規則がインシデントハンドリングの基本文書となるだろう。

文書では、最初にインシデントハンドリングの対象となる組織の構成員と取り扱うインシデントの種類をはっきりさせる。次にハンドリング手順を定めておく。事後報告のための書式も定めておき、すべての局面においてインシデントに対し個別対応することをできるだけ避ける。さらにそれらがきちんとまわっていくかどうか、イメージトレーニングや演習（サイバードリル）についても文書に書き下しておくとよい。これらの準備ができていれば、組織に重大インシデントが発生した時に必ず役に立つ。ハンドリングに関する各種の情報は、JPCERT/CC のサイト（http://www.jpcert.or.jp/csirt_material/）から得られる。また、WG 活動で大学などの場合のハンドリングの手順の例を作成したので、付録 B につけた。

まとめ

セキュリティの確保にあたって、個人の倫理やスキルに負う部分が大きいことから、組織人に対して、何をどうするか、どのような対策を実施すれば有効であるかを

- セキュリティにおける人間要因
- セキュリティの管理
- インシデントハンドリング

の観点からとりまとめた。
セキュリティ体制整備の助けになれば幸いである。

情報セキュリティ監査
仕様書

平成 XX 年 YY 月
国立大学法人 A 大学

1. 件名：情報セキュリティ監査

2. 概要

国立大学法人 A 大学（以下「本学」という。）の情報セキュリティポリシーでは、監査を実施することが決められている。監査には内部監査と外部監査の両方を実施することがセキュリティ向上に有効である。本件は、外部のセキュリティ専門業者により本学のセキュリティ監査を実施し、本学の情報セキュリティの現状分析の参考としその向上に役立てるものである。

3. 要件

1) 本学の情報セキュリティ管理が適正に行われているか、情報セキュリティポリシーおよび実施手順を点検し、点検結果を文書で報告すること。文書は電子化されたものと印刷されたものの両方を提出すること。
2) 聞き取りにより、情報セキュリティポリシーおよび実施手順の遵守状況を調査すること。調査結果を文書で報告すること。文書は電子化されたものと印刷されたものの両方を提出すること。
3) 本学と協議の上監査実施範囲を決定し監査の実施計画書を提出すること。
4) 監査実施体制を提示すること。
5) 本学と秘密保持契約を締結すること。契約書の詳細は本学と協議の上決定すること。

4. 実施内容

1) 聞き取り対象の人数は　○○名以上とすること。
2) 聞き取りの対象は、本学職員が決める。
3) 聞き取りの実施日は、業務の影響範囲などを勘案した上で本学職員と協議して決定すること。
4) 聞き取り内容を録音する場合には、聞き取りの本人から了解を得ること。

5. 請負者に必要な条件

1) 監査実施者は、複数の監査人を選任し、監査人のうちの一人を監査責任者とすること。
   ① 監査責任者は、下記資格のいずれかを取得していること。
      (ア) ISACA（情報システムコントロール協会）が認定する CISA（公認情報システム監査人）の資格
      (イ) NPO（日本システム監査人協会）が認定する公認システム監査人の資格
      (ウ) 日本規格協会マネジメントシステム審査員評価登録センターまたは国際審査員登録機構に登録された ISMS 審査員資格
   ② 監査責任者を補佐する監査人（2 名以上）は、それぞれ下記の資格のいずれかを保有していること。
      (ア) ISACA（情報システムコントロール協会）が認定する CISA（公認情報システム監査人）の資格
      (イ) NPO（日本システム監査人協会）が認定する公認システム監査人の資格
      (ウ) 独立行政法人情報処理推進機構（旧試験期間：財団法人日本情報処理開発協会）の情報セキュリティアドミニストレータ資格
      (エ) 財団法人日本情報処理開発協会のISMS審査員補資格
2) 監査実施者は、経済産業省の「システム監査企業台帳（平成〇年度）」または「セキュリティ監査企業台帳（平成〇年度）」に登録されていること。
3) 監査実施者は、平成〇年から△年の期間において情報セキュリティ監査実績を複数（5 以上）有すること。特に、国の機関、独立行政法人、あるいは国立大学法人の情報セキュリティ監査を受注した実績を有すること。
4) 監査実施者は、本件で発生する作業を外部業者に対して再委託しないこと。

6. 結果報告及び提出物

1) 監査に係わる報告書の提出及び改善策の提案について報告会を実施すること。
2) 日本語で作成した監査結果報告書
   ① 電子化された報告書(PDFファイル)　　1式
   ② ファイルリングされた報告書(印刷物)　　1式

7. 納期

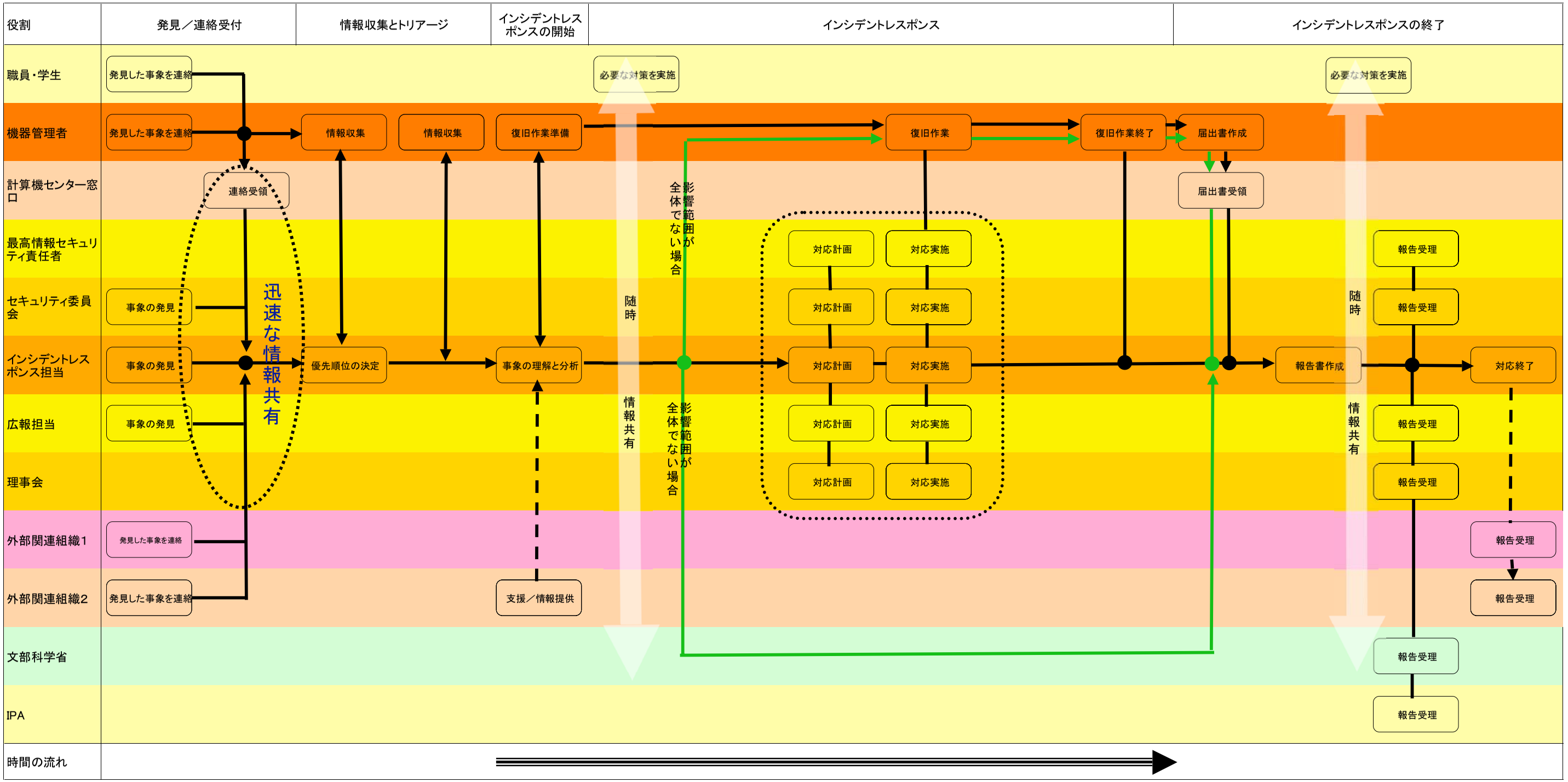
平成○○年 XX 月 XX 日

8. その他

1) 本仕様に定められていない点については、本学職員と協議の上、実施細目を決定すること。
2) 本監査に必要なもの以外は、本学に持ち込まないこと。
3) 本監査する上で請負者の責に帰すべき事由により、本学に損害を与えた場合には、請負者の責任において現状に復すること。また、請負者が被った損害は、本学の責により生じたもの以外は一切の責任を負わないものとする。
4) 本監査で作成した一切のものは、すべて本学に帰属するものであり、私権を設定してはならない。

付録B　インシデントハンドリング体制 （例）

2009.1.15　17:34



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）　*リーダー

SS研セキュリティマネジメントWG
人間・管理グループ

目次

- セキュリティにおける人間の要因
  - 懲りない人々（繰り返し感染、繰り返し侵入被害）
  - セキュリティ教育の在り方と評価
- 人間要因の管理
  - セキュリティポリシーとPDCA
  - ポリシー雛型の導入体制
- インシデントハンドリング
  - CSIRTからSOCへ(Security Operations Center)

セキュリティにおける人間的要因

- 機械やソフトの役割は限定的
  - ソフトウェアや装置の導入による安心感
  - うっかり/好奇心/出来心による受動攻撃
  - スピア攻撃（上司からのメールに見せた添付書類）
- 繰り返される感染・侵入被害
  - 同じ人、グループが複数回
- 学生や留学生の意識
  - 意識/常識/認識の差
  - 知財権侵害（不正コピー利用/配布）への認識

セキュリティ教育

- 教育とその効果
  - 機会の提供
    - 講習会
    - E-Learning＋チェックテスト（テスト内容と評価の活用）
  - 受講の義務化
    - 例外なし
    - 役員、上級者（短期の効果的教育、予算確保に重要）
  - 教育効果の検証
    - インシデントが減少しないと意味がない

セキュリティ教育の問題点

- IT用語の問題
  - わかりにくい用語や概念
  - 上級職員の理解
  - 急激な環境変化
- 人の類型化
  - セキュリティ意識の調査（適切なアンケート等）
  - 分類・教育
- セキュリティポリシーの周知
  - E-learningとチェックテスト？

セキュリティ教育教材（有償）

- 情報倫理デジタルビデオ小品集　（制作：メディア教育開発センター）
  http://www.mitomo.co.jp/online/shop01/moral.html
  http://www.mitomo.co.jp/online/shop01/moral2.html
  http://www.mitomo.co.jp/online/shop01/moral3.html
  大学生協モデルでは一部映像をインストールして販売
  2009年度以降の活動予定不明（NIME組織改変）
- INFOSS情報倫理（日本データパシフィック）
  http://www.datapacific.co.jp/e_learning/e-ichiran.htm

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：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/

セキュリティ教材（無償続き）

- 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/
- セキュリティ知識のチェック
  - セキュリティカランキング
    - 個人編と組織編があり、理解度チェックには有効

  http://www.jnsa.org/Seculiteracy/index.html

セキュリティ教材の鮮度

- 変更頻度少
  - セキュリティ基本教育用教材
- 変更頻度中
  - セキュリティポリシーとその周辺
- 変更頻度大
  - セキュリティ状況
  - IT基礎知識と応用知識

セキュリティチェックテスト

- セキュリティテキストとテスト
  - 実施基準書（部門別に作成）
  - だれが何を教え何をチェックするか
  - だれが何の権限で実施するか
  - 結果をどう日常のセキュリティに反映するか

階層別の対応

- 上級職員
- 教員
  - 事務と教育研究の境界
  - ベテラン教員のセキュリティ意識と現状把握
- 職員
  - 統一基準ベースでよい
  - ただし、機密扱いについて明確な基準必要
- 学生
  - 処分基準（ポリシーで切り分け）

階層別の対応

- 不安定短期雇用の増大
  - 産学連携、短期プロジェクト、派遣、外注
  - 組織への帰属意識の低下
  - 組織への忠誠度、信頼度の維持困難
  - セキュリティ意識の低下
- シングルサインオン等の導入
  - revokeリスト管理
  - DB管理の手間の増大

教育レベル設定

- 教育対象のレベル設定
  - 初級教育
    - 学生・教員
    - 中途半端な上級者が不満
  - 来て欲しい人がこない
    - 事務は人事記録のしばりによる効果
    - 役員、経営層
  - 教育は組織としてのアリバイ？
  - 小中学校向け教材は初級教育に有用

ポリシー遵守を助けるIT環境
ミスの発生を防ぐ環境

- ローカルに情報を残さないシステム
  - SaaS＋Web
  - Thin Client
- お仕着せ端末（余計な自由度なし）
- ICカード認証と物理的セキュリティ
- 身をまもるためのログ保全
- Cloud、SaaS,アウトソース
  - コスト削減とセキュリティリスクの移転

Cloud,SaaS,アウトソースの問題

- メール等のアウトソーシング
  - 認証データの外部提供は大丈夫？
  - データの外部保管
- データの取り扱い
  - 統計処理されてはいても大丈夫？
  - メールの紛失等
- サービスの継続性
  - サービスが消えたら（M&A等）
  - 無償から有償へ

セキュリティの管理

- セキュリティポリシーとPDCAサイクル
  - セキュリティポリシーは誰のためのものか
  - あるだけでは意味がない
  - 役に立つポリシーや手順
  - セキュリティポリシー遵守を助ける環境
    - セキュリティ機器、ソフトウェア
    - 教育、指導、援助
  - セキュリティ監査

セキュリティ監査

- 第3者監査
  - 機密保持契約（監査仕様書例は付録）
  - 監査人の資格（CISSP,JASA主任監査人）
- 内部相互監査
  - 近隣大学間や地域での情報共有
一方で地域ネット組織のあいつぐ解散
  - 近隣大学や地域でのセキュリティ相互監査
    - セキュリティ意識の向上

セキュリティ監査手順

- 監査立案
  - 実施体制
    - アウトソース/内部監査
    - 日程等
  - 実施手順書
    - 監査対象項目、監査対象者等選択
- 監査実施
- 監査レビュー

各種セキュリティ基準等

- 各種認証や証明
  - ISMS/ISO27000
    - セキュリティシステム基準への適合証明
  - プライバシーマーク
    - 名刺一枚の管理も大変（大学にとってのメリット？）
    - とりあえず学籍情報は重要だけれど
  - 事業継続/ISO25999（BCP/BCM）
  - セキュリティ格付け会社（格付けトライアル）
    - アイ・エス・レーティング（www.israting.com）
  - SOX法、JSOX法
    - 会計基準
    - 法人化した大学への適合必要？

セキュリティ体制

- CSIRT機能構築
  - セキュリティ計画
    - ポリシー策定、セキュリティシステム導入計画、インシデントハンドリング計画
  - 分析とレポート/記録
    - ぜい弱性スキャナ、ペネトレーションテスト、ログ監視
  - インシデント対応
    - インシデント拡大防止、エスカレーション、レビュー
  - トレーニング、教育
    - サイバードリル

インシデントの定義

- インシデントとは何かを明確にする
  - 部局単位？
  - ウィルスやtrojan
  - 侵入
- 外へのコンテンツ侵害はCSIRTの範囲？
  - 掲示板荒らし、内容の話への対応
    - たぶん範囲外、しかし連絡は来る！
  - ただし連絡窓口は一本化（Point of Contacts）
    - 窓口は統一しても全部はやらない

インシデントハンドリング

- 一定割合でのインシデント発生
  - ボランタリーな対応では無駄が多い
  - 担当者の無限責任にしない
  - インシデントの切り分けとエスカレーション
    - 情報トリアージ
    - インシデントの局在化
    - 事後報告

インシデントハンドリング手順

- 手順の類型化
  - インシデントハンドリングポリシー
  - 守備範囲（無限責任にならない）
- CSIRTマップ（付録PDF）
  - 早期での全組織対応か局所対応かを見極める

まとめ

- セキュリティマネージメント体制の整備
  - ポリシーとポリシーの周知徹底（教育）
  - 監査（内部、外部）と日々のセキュリティ改善
    - セキュリティ戦略→BCP/BMP
    - セキュリティ啓発活動
  - でも、完全なセキュリティはありえない
    - インシデント対応体制
    - インシデントにも学ぶ

2.2. 状況認識のためのセキュリティアプライアンス

2.2. 状況認識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、状況を認識することができず、「犯人」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。これらの機器は、通常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、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。

今回はセキュリティインシデントの状況認識のための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）について取り上げました。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。

FW はネットワーク型 FW とホスト型 FW に大別されます。ネットワーク型 FW は、パケット単位、セッション・アプリケーション単位でネットワークトラフィックを制御するもので、設置場所の観点から主として、組織とインターネットの接続点に置かれます。一方ホスト型 FW は、主として PC などのエンドポイントへ、アンチウィルスソフトウェアと共に導入され、PC をインターネットワームなどの攻撃から保護しています。

IDS も FW と同様に、ネットワーク型 IDS（NIDS）およびホスト型 IDS（HIDS）にわけられ、また検知方式によって Abuse（誤用）検知型（Signature 型）と Anomaly（異常）検知型に大別されます。例えば、Abuse 型の NIDS はネットワーク上に流れる通信パケットを捕獲し、プリプロセッサ部で前処理を行い、検知部へ入力として渡します。そして検知部では、Signature データベースと呼ばれる攻撃のパターンを集めたデータベースを利用し、攻撃パターンに一致したものを検知結果として出力します。この出力されたメッセージはアラート部でログとして記録され、更にメールなどで管理者へ通知されます。しかし NIDS によって検知された攻撃は、成功したか失敗したかはわからないという欠点があります。当然その攻撃先で、その攻撃に対する防御策が採られていれば攻撃は成功しないことになります。よって NIDS は攻撃の予兆を捕らえるためのツールと言えます。代表的な NIDS としてオープンソースの Snort が知られています。

一方 HIDS は、主としてサーバホストに導入され、プロセスの異常な動作やファイルの改ざんなどを検知することができます。また受信したパケットについて NIDS と同様に処理してネットワークから導入ホストへの攻撃そのものを検知することができます。代表的な HIDS として tripwire が知られています。HIDS は、NIDS と異なり、検知結果に基づいた次のアクションとの連携が同一ホスト内であるため容易にできるという利点があります。しかし導入するホスト自身のリソースに余裕がなければ HIDS を導入するのは難しい場合もあります。この場合、NIDS をスイッチとサーバの間に入れて監視し、攻撃の予兆を検知する方式を採用せざるを得ないことになります。

IPS は IDS 部分と動的 FW 部分から成り、IDS 部分で検知した結果を基に攻撃元 IP アドレスからの通信を動的ブロックするアプライアンスです。IDS はネットワークやホストを監視するだけで、基本的に保護や防御はしませんから、2003 年に米国で発表されたレポート[1] の影響もあって、検知して攻撃を遮断できる次のセキュリティアプライアンスとしての IPS が注目を浴びました。IPS もネットワーク型 IPS（NIPS）とホスト型 IPS（HIPS）があります。NIPS はネットワーク上

[1] http://www.sans.org/reading_room/whitepapers/detection/1028.php

の通信を監視、攻撃と見なした通信をブロックします。NIDS と NIPS が大きく異なるのは、NIPS の IDS 部分の性能が NIDS 以上に求められることです。ネットワーク帯域にも耐え得る必要があり、監視する通信を選び、確実に検知できるものに限ってブロックする必要があります。誤検知があると遮断するべきでない通信まで遮断してしまうことになるからです。

このように様々な種類のセキュリティアプライアンスが出てきたため、これらを個別に導入する場合の導入や管理コストが問題になってきました。このため、これらの機能を単一の筐体にまとめた、統合セキュリティアプライアンスが開発されました。現在このような機能や機器は UTM（Unified Threat Management: 統合脅威管理）と呼ばれています。単一の機器で多数の機能を有し、また操作が統一されているため、導入や管理コストが低いという利点があります。その一方で、全体としての処理性能や各機能の設定自由度が低かったり、耐故障性に問題があったりする場合もあります。大規模な組織には性能が見合わない場合もあるため、導入時には注意が必要です。

WAF はその名の通り、Web アプリケーションに対する攻撃を防ぎます。近年 Web を媒体としたサービスが非常に普及しており、またこれを対象とした攻撃も激しさを増しています。この際に問題になるのが、脆弱性が発見されたにもかかわらず、開発者の不在や改修コストなど様々な理由により修正が不可能な「レガシー」なアプリケーションです。WAF は、これを解決するための「外堀」として機能します。WAF は一般にウェブサービスを提供するサーバの手前に設置することにより、クライアントからの要求やサーバからの応答内容を検査し、必要なら危険な要求や応答内容を安全なものに変換することで、レガシーなアプリケーションを修正することなく防御を強化することができます。今回の報告ではネットワーク型についてだけ紹介していますが、サーバに追加で導入する形のソフトウェアもあります。

続いて、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。参加ホストに明確なサーバ・クライアントの区別が無く、両方の機能を兼ね備えた「Peer」同士によって構築されます。また、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もっとも有名ですが、それ以外にも音声通信やコンテンツ配信などで利用されています。

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交換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洩です。また、利用者による P2P ソフトウェアの多用のため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場合もあります。このため、P2P ファイル共有ソフトウェアを組織として制限・遮断したいという要求があります。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機能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、技術の悪用が問題であるため、規則や広報など人的な手段による規制も重要です。言語の問題のみならず、国によって著作権に対する意識が異なるなどの問題もあり、留学生や外国人研究者への対応には注意が必要です。

セキュリティアプライアンスの導入には、管理的な側面から、コストの問題や運用ポリシーの問題があります。導入時におけるコスト、および導入した後の維持管理のコストが挙げられるでしょう。また運用ポリシーを決めておかないと組織の構成員から「盗聴」や「検閲」ではないかと誤解を受けることがあります。またアプライアンスより生成されるログには個人情報を多く含んでいる可能性があるため、その取り扱いやアクセス権の管理などの問題が生じてきます。またセキュリティアプライアンスは廉価なものではありませんし、設置または配置される場所によって得手不得手があるため、導入場所を間違えると大きな損失を抱えることになります。通常 NIDS/NIPS や UTM などのネットワーク型セキュリティアプライアンスは、対外ルータの近傍へ設置されますし、検疫システムは L2 スイッチや統合認証システムとの連携が重要になりますので、

PC などのエンドポイント近傍に設置されます。またインライン型の IDS/IPS などは、ルータやスイッチとサーバの間に設置されます。更に導入時のコストを下げるための方策として、導入時期を慎重に選ぶ必要があると思われます。すなわち、セキュリティアプライアンスを導入しやすいネットワークがあり、それは主要なネットワークトラフィックを容易に監視が可能であることや IDS 用のミラーポートやネットワークタップ装置が置きやすいとか、また UTM などのインライン型 IDS/IPS がそのトラフィックの速度帯域に耐えられることなどが要求されます。したがってネットワークの設計段階で、上記の導入しやすいネットワークの条件を考慮すれば良いということになります。すると組織内のネットワーク施設の更新時期が適当であり、更新計画にセキュリティアプライアンスの導入を前提にして、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。

またセキュリティアプライアンスは一般に大量のログを生成します。そしてそのログには大量の個人情報が含まれる可能性が高いことから、その管理については慎重に行われる必要があります。つまり管理ポリシーが必要になります。ログの管理ポリシーとしては、安全な保存場所の確保、アクセス権限（閲覧）規定、統計解析作業のためのリソース確保等を考慮する必要があります。

以上、「状況認識のためのセキュリティアプライアンス」と題して、ファイアウォール（FW）、侵入検知・防止システム（IDS/IPS）、Web アプリケーションファイアーウォール（WAF）、P2P アプリケーションの制御、セキュリティアプライアンス導入時のコストやネットワーク設計について検討しました。また付録として、これらセキュリティアプライアンスの導入・運用現況について 10 機関についてアンケート調査を行った結果を添付しておりますのでご覧ください。

別紙

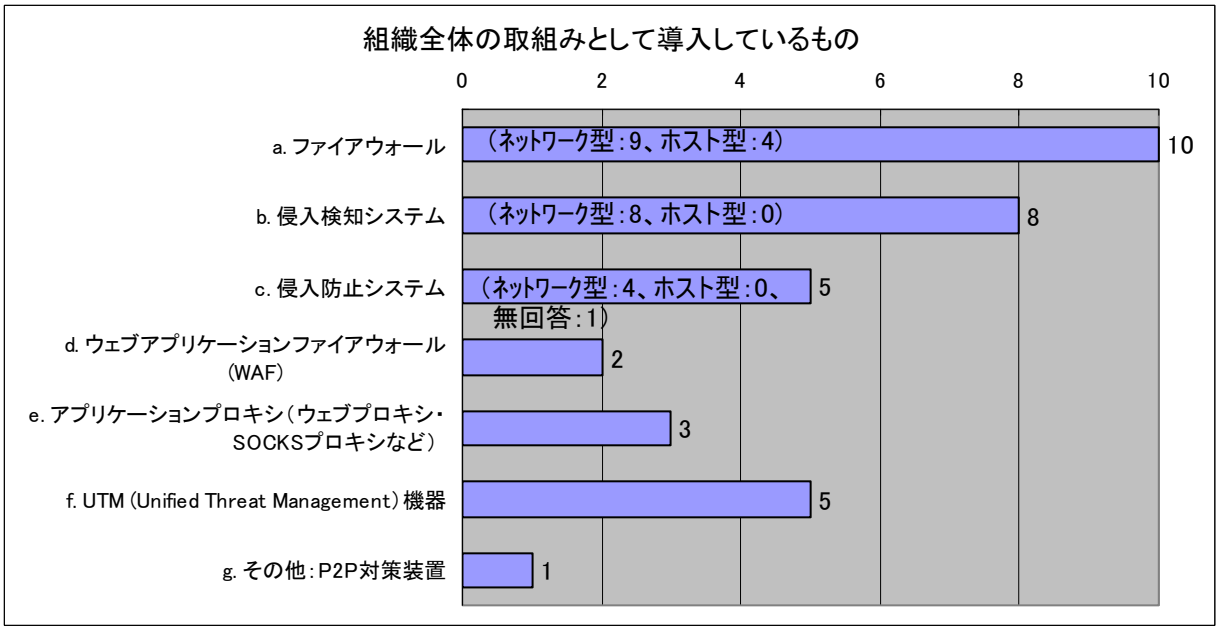
セキュリティ・アンケート 結果

SS 研会員の 10 機関が回答（機関名は A～J で記載）

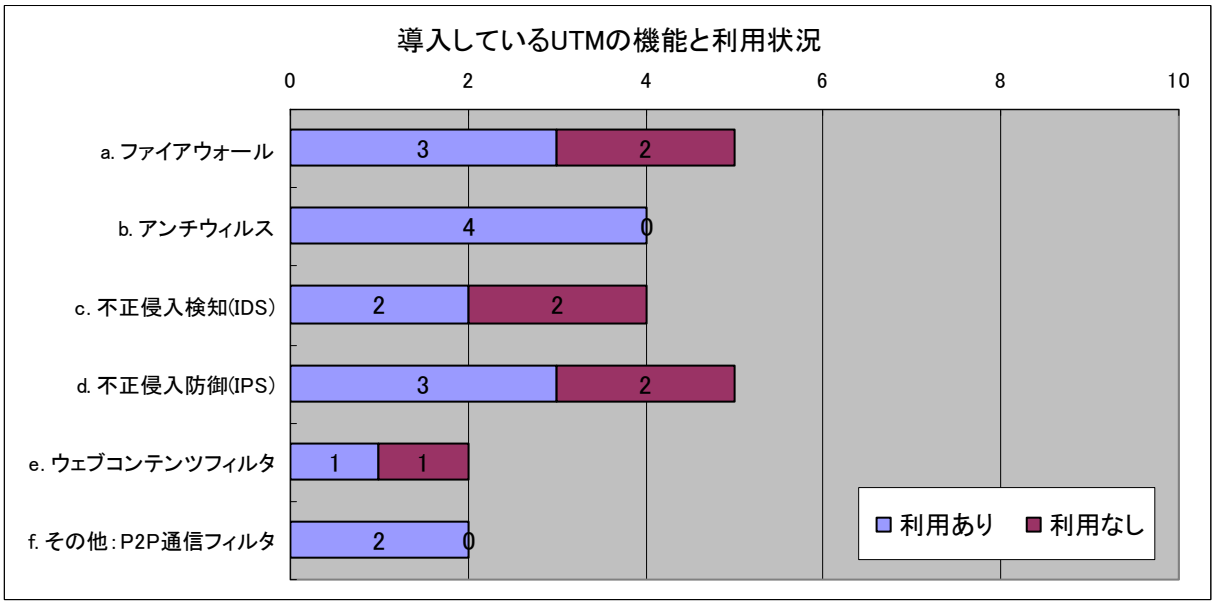
2008 年 10 月実施

Ⅰ．「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

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（複数回答可）



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（複数回答可）



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

- 増加の一途をたどり、かつ巧妙化する情報セキュリティの脅威から、当組織の情報システムを可能な限り保護するため。(A)
- 当初より必要な機器として検討。(B)
- smurf 攻撃をうけて上流のネットワークに迷惑をかけるというセキュリティインシデントが発生したことを契機に IDS を導入した（1998 年度)。続いて、補正予算などでネットワークの再構築をした時に、それまでルータで行っていたアクセス制限をファイアウォールで行うよう変更した（2002 年度頃)。Windows パソコンにウィルスが多発したので、ウィルスのネットワーク通過をできるだけ押さえられるようにウィルスブロック装置として UTM を導入した（2005 年度)。当組織が運用するネットワークに属する大学でワーム感染/不正侵入が発生したので、IDS/IPS を導入した。パーソナルファイアウォールソフトとアンチウィルスソフトをまとめて購入し申請者に無料で配布している。現在は、パソコンの OS にファイアウォール機能が含まれるようになっているので、アンチウィルスソフトのみを導入する方のほうが多い。(C)
- 外部からの侵入を伴うセキュリティインシデントが多発したことによる。(D)
- IDS については、2001 年度末頃に業者からデモ機を借りて評価する機会があった。評価の結果、様々なイベントを見ることができることが分かったため、導入することになったと記憶している。パーソナルファイアウォールは、大手製品を一括ライセンスにより構成員に安価で提供しているものである。導入は必須ではなく、詳しい導入状況は把握されていないのではないかと思う。(E)
- FW/IDS については 2002 年に組織内 LAN をギガビット化した際に、組織内的に FW/IDS 導入の要望があり導入された。FW や IDS の導入の背景については、2001 年～2002 年にかけて行われた、政府省庁に対する攻撃が直接の原因となっている。また 2002 年当時、情報セキュリティポリシーの策定時に、組織内 LAN におけるリスクを知るため IDS を導入することにした。IPS と P2P ファイル共有ネットワークの帯域制御装置として UTM が導入された。(F)
- FW はネットワーク整備時（2001 年）から導入している。P2P 対策は、対応のコストが大きくなったので、ソリューションの提案を受け、導入した。(G)
- 当初から、外部から内部へのネットワークアクセスを制限するために導入している。(H)
- 組織外からの不正アクセスを防止する為。(I)
- 外部からの攻撃が増大したため。(J)

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）

- 事案等の早期発見、早期対応が可能になるとともに、傾向分析が可能となった。(A)
- 問題ある通信や機器を的確に検知している。(B)
- IDS で数多くのセキュリティインシデントを発見できた。また、IDS によるインシデント通信のスナップショット保存機能により完全ではないが、事実関係をある程度正確に把握できるようになった。(C)
- FW を導入して DMZ を構築/運用できたこと。ルータでも可能だが、DMZ の機器毎に細かいアクセスポリシーをルータで設定するのは運用コストが高すぎる。(C)
- 無防備な wireless PC のウィルス/ワーム感染をある程度防御できた。(C)
- FW を導入して不要な通信が遮断できることが実感できたこと、外部からの侵入が減少したこと。(D)
- IDS は監視装置なので、それ自体で何かが直接守れるわけではないが、それまでトラフィック監視についてはスニッファがあるくらいで何が起こってもほとんど調べようがなかったのが、IDS の導入に伴いパケットキャプチャできる環境が整った事で、見えなかったものが見えるようになり、対処できるようになった。外からの攻撃よりも、中からの異常を検出して対処できるようになった事の方が大きいように思う。(E)
- より具体的にこれこれの攻撃を受けているとか、出しているという傾向がわかる事から、その

他のセキュリティ対策の方針決め等にも影響があったものと思う。(E)

- 具体的な攻撃事例などが集まるため、講習会等で説明する際の説得力が増したと思う。(E)
- FW や IDS を導入前後の変化は感じられなかった。IDS については多量のアラートログが得られ、その主成分がポートスキャンであることが判明した。この傾向は、現在も変わらない。P2P ファイル共有帯域制御のおかげで P2P ファイル共有絡みのインシデントはまだ経験していない。一方 IPS を導入したことで、一部サービスの提供に不具合が生じた。(F)
- セキュリティインシデントの回数が減り、コスト削減となった。(G)
- 内部にあるサーバのセキュリティ対策を緩和できる。(H)
- 組織内ネットワークが守られているという安心感。(I)
- 組織内でのウィルス感染件数が減少した。(J)

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)**

- セキュリティ関連機器がブラックボックス化され、機器の不具合対応等(事案か機器の不具合かの判別を含め)に時間を要してしまう。(A)
- マニアルが不備。マニアルにない設定をしないと、当方の構成では動作しない。(B)
- ネットワーク機器と比較すると購入価格と保守費が高い。(C)
- H.323 通信(TV 会議通信)に障害が発生しやすくきり分けが難しい。(C)
- インシデントの移り変わりもあり、常に陳腐化を心配していないといけない。(C)
- 設定ポリシーの周知が大変だった。また、IDS のログを精査する時間がとれていないこと(事後追跡に使用)。(D)
- IDS の利用方法には業務の方々にも伝えては見たものの、事実上教員が一人で見ている状態で、あまりきちんと監視できていない部分がある。(E)
- 導入から時間が経ってしまい、機器もソフトウェアも陳腐化してしまった。サポートもあって無いような状態になっているが、基幹ネットワークは 10GbE に高速化してしまっていて、それに対応した機器は高価すぎて導入できず、だましだまし使っている状態にある。(E)
- FW/IDS の導入については、情報セキュリティポリシーを策定するにあたり、それらの導入自体が必要事項であったため、ポリシー策定時に必要なリスク分析が可能となり、良かったと思われる。(F)
- 導入後多量のインシデントがあり、とにかく組織が攻撃にさらされている状況を訴えるのには良い資料提供マシンとなった。しかし組織への攻撃のポートスキャンがあまりにも多く、また IDS 設定用の GUI が不安定だったため使い勝手があまりにも悪いこともあり、ログ収集マシンとなってしまった。(F)
- 2003 年当時はログ解析技術があまり普及していなかったので高い投資になってしまった感がある。一方でログ解析技術がこれから有望であることは判ったのはよかったと思われる。(F)
- 独自ポリシーを主張する部署があり、別扱いをしなければならない。(G)
- 内部にあるサーバを外部へ公開する際に不便を感じる。(H)
- ルール定義の組織内調整。(I)
- 初期設定とその手直しが落ち着くまでしばらく大変。(J)

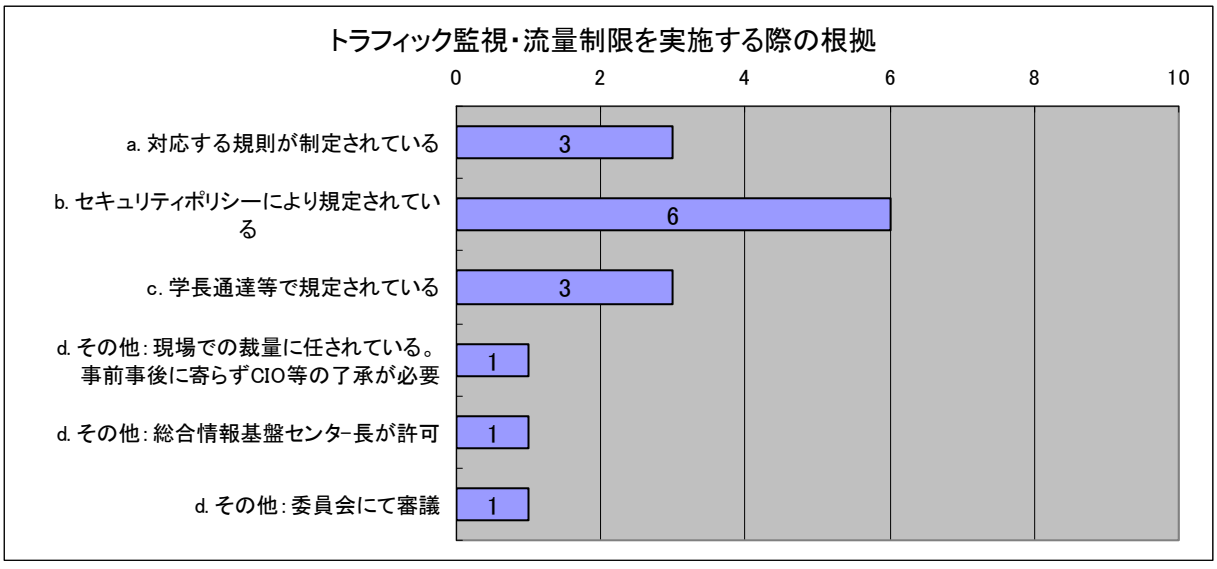
6. **ファイアウォール、IDS/IPS などのさまざまなログをどのように扱かっていますか(長期保存や閲覧規則など)**

- 保存期間はログの種別によって保存期間を定めている(最長 1 年間)。閲覧規則は対応する規程に定められた閲覧者のみ閲覧。(A)
- 現状検索が容易なように DB 化している。今後は外部解析委託を検討。保存としては、アクセス制限はしているが、暗号化などはしていない。保存期間については未決定。(B)
- IDS のログ: IDS のログ解析をアウトソースしているので、アウトソース先と VPN を構築し

常時ログを転送している。(C)

- FW のログ：　syslog サーバへ保存するとともに WLEF 形式を取り扱えるログ解析サーバへも保存し、商用の解析ソフトで解析している。ログとり用の専用のネットワークを構成している。syslog サーバへ保存したログは RAID0+1 の外部ディスクへも保存している。(C)
- 保存：　ログの保存期間は 6 ヶ月以上としている。syslog サーバへ保存したログは、センターが運用する大規模ファイルサーバへ暗号化して保存している。これはバックアップとして考えている。(C)
- 閲覧：　閲覧は、センターのセキュリティ担当者、ネットワークサポート業務受託者、IDS ログの解析のアウトソース先の会社に限定している。(C)
- アクセスが限定された syslog サーバに保存。過去は DVD-R に保存していたが、今は、ある期間後消去。(D)
- IDS はその機器の吐くフォーマットのまま、古いものは別のホストに移して長期保存している。機器固有のファイル形式だが、展開用の Perl スクリプトが提供されており、移しても検索等は可能となっている。基本的に移したものは管理している教員しか見る事ができない状態になってしまっている。(E)
- ログについては情報セキュリティポリシーにおいて記述があり、レガシーな機器を除きログが採れるようにしている。またログなどの閲覧については許可制であり、例えば新種のウィルスに感染した機器については、センター長へ申請して許可を得なければ閲覧できないようになっている。なお研究や業務などでログを常時閲覧する必要がある場合についても、新規の場合については、センター長の許可を得る必要がある。(F)
- ディスク容量の制限のため、短期間保有に限っている。インシデント発生時のみ、センター長の指示により担当者が閲覧する。(G)
- １年間保存し、管理者しかアクセスできないようにしている。(H)
- syslog サーバに送信(保存期間 1 年間)。(I)
- 一定期間保存、管理グループのみで閲覧可能。(J)

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**

- 当組織のセキュリティ関連規程に基づき取り扱っている。(A)
- 未整備。(B)
- 「統計的な処理はするが、通常はログの詳細はみない」、「セキュリティインシデントがあれば、

詳細な内容までみる」という方針で、関係者だけがログをみることができるようにしている。(C)

- 権限は特に定義されていないが、セキュリティポリシーによりインシデント発生時にはその原因を突き止めるためにトラフィック調査をしてよい事になっている。(E)
- 研究や侵入検知業務以外の業務以外では、重要なネットワーク接続機器のログについてはセンター長の許可がなければ閲覧してはいけないことになっている。個人情報であると判断されれば、個人情報保護に関する組織内規定で対応される。(F)
- インシデント時にセンター長の示により担当者が閲覧するように制限している。また、その他の目的の場合には、文書により依頼をし、センター長が決済する。(G)
- Web ページにて、トラブルが発生した際にログデータをもとに情報取得を行う旨通知している。(H)
- 委員会からの要請のみ確認。(I)
- 通信内容はセキュリティ管理上必要な作業(トラブル原因追求)のために管理者のみが参照し、それ以外には公開しない。(J)

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**

●ホスト型の IDS （A）

理由： ・運用・管理コスト(費用)増大のため

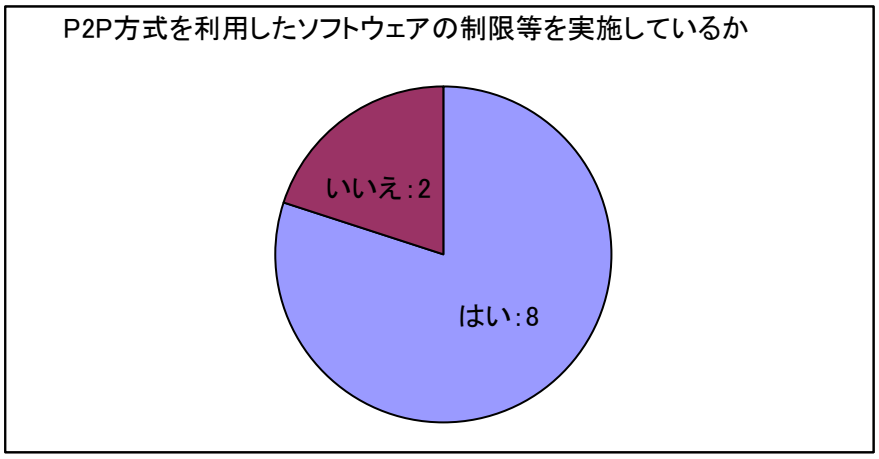
・運用・管理する人員が確保できなくなったため

●ファイウォールソフト （C）

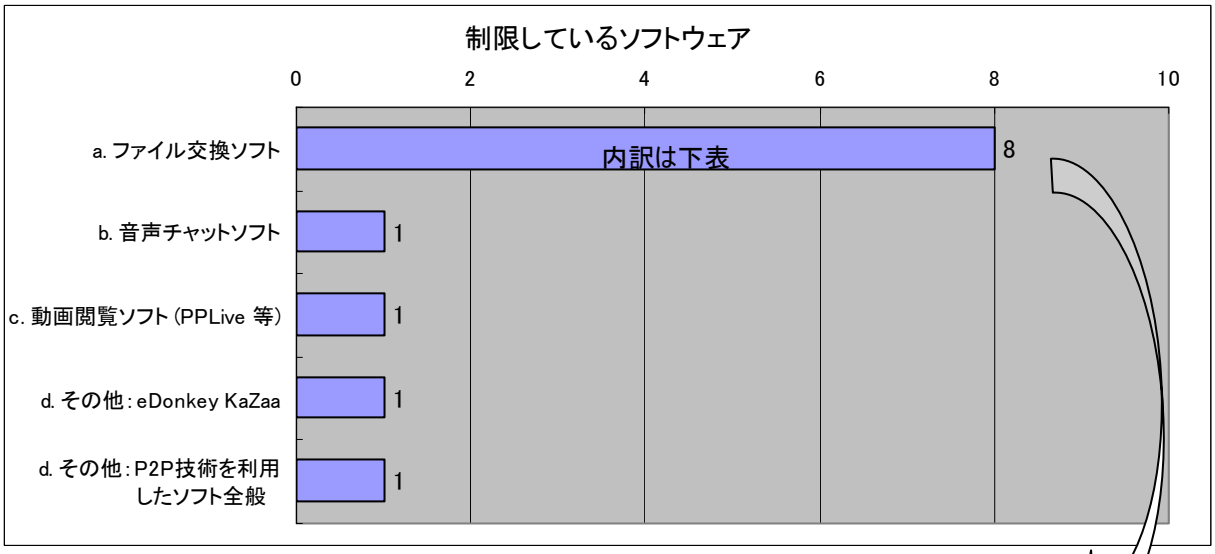
理由： ・機器のメーカーサポートが終了し保守できなくなったため

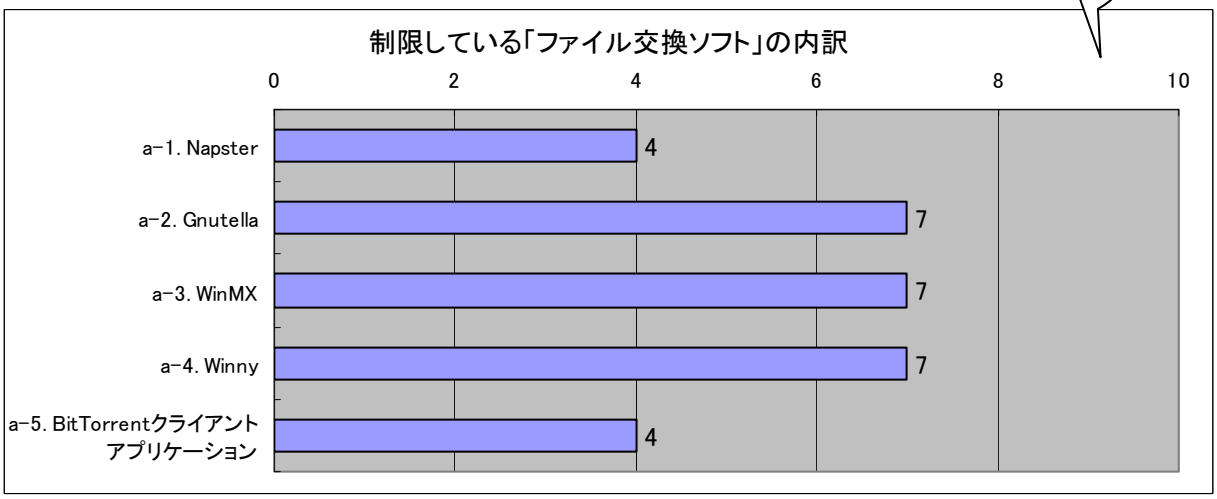
Ⅱ．「P2P」関連ソフトウェアに関する対策とそのポリシーについて

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

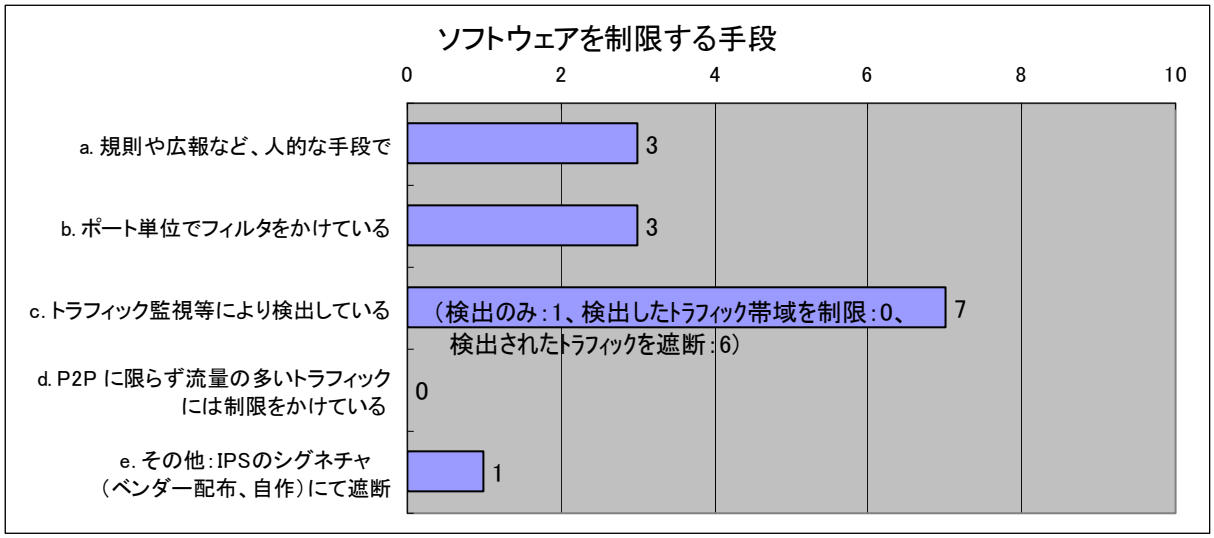


2.　どのような種類のソフトウェアを制限していますか（複数回答可）

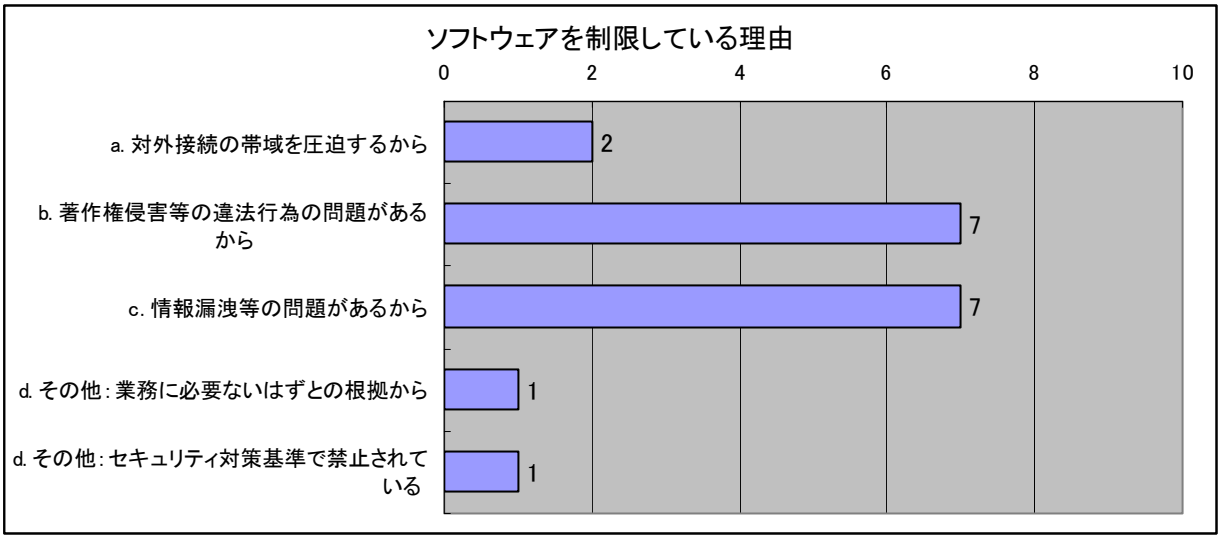




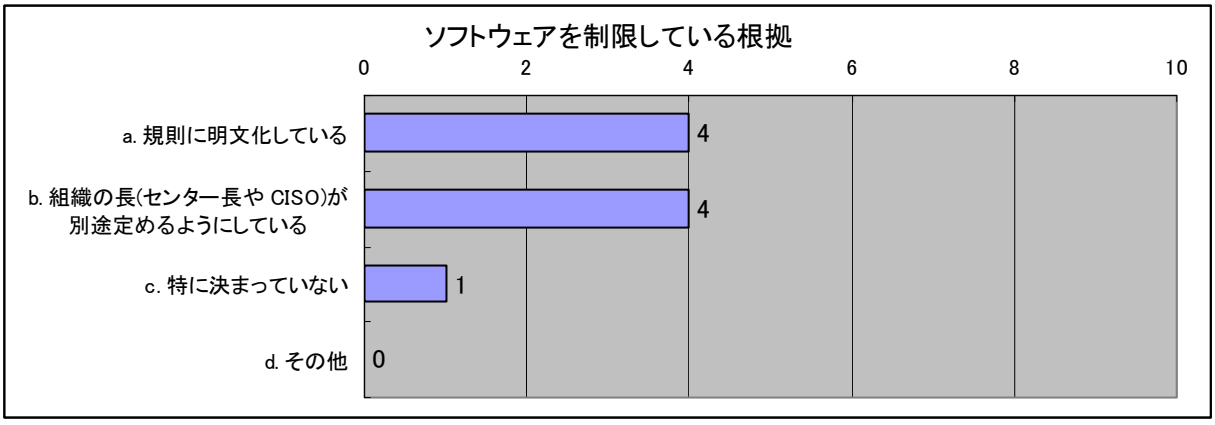
3. 制限する手段はどのようなものですか（複数回答可）



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（複数回答可）



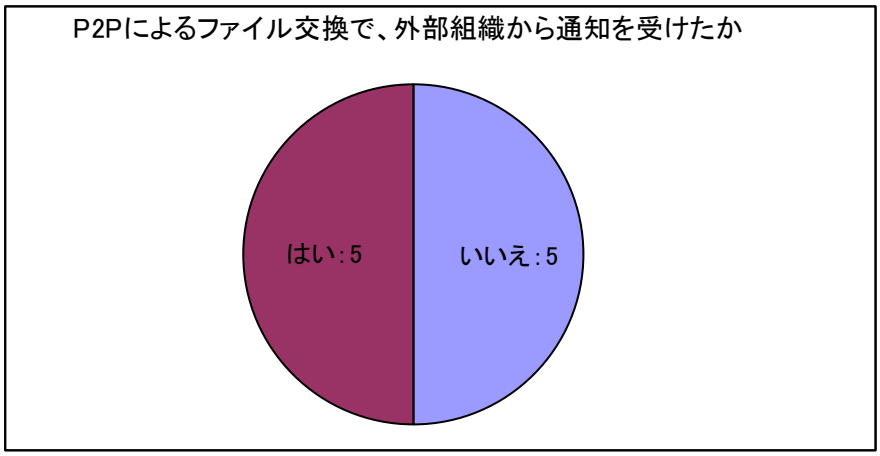
5. 制限の根拠はどのようなものですか（複数回答可）



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

a. 実施が技術的に困難だから	0
b. 制度的な整備が困難だから	1
c. 導入予算がないから	0
d. 必要性を感じないから	1
e. その他	0

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

a. 著作権団体	2
b. 著作権者自身	1
c. その他:匿名者	1
c. その他:著作権者の権利が侵害されていないか監視する会社	1

9. 通知に、どのように対処しましたか

a. 利用者を特定し、対処した	4
b. 組織のネットワーク全体で該当する P2P 通信を禁止・制限した	1
c. 特に対処はしなかった	0
d. その他:利用者の特定や技術的な補助を行ったが、具体的な対処は P2P 通信を利用していた者の属する組織でしていただいた	1

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

- 同様機能のソフトウェアが多数あり、また用途も多様でどれを規制すべきか理由が難しい。(B)
- P2P 技術を利用するアプリケーションが増えてきているが、これらの取り扱いについて組織内で規則ができていないため、個別に対応している状態ですっきりしていない。(C)
- Skype は制限していない。(C)
- 著作権侵害などが発生した場合、センターの所掌範囲をこえる。(C)
- 学術目的に限れば P2P も解放すべきだが、それ以外のものとの確証は得にくい。現時点では、BitTorrent 等を個別に解放している。(D)

- Winny WinMX Gnutella 等いくつかの著名なアプリケーションについては、検出サービスを買っている。また、BitTorrent は制限をしていなかったが、BitTorrent による著作権侵害に関する警告が来るようになったため、IDS で検知し警告するようにした。（E）
- Winny WinMX 等はキャッシュにより知らずに著作権侵害の片棒を担ぐ事があることと、情報漏洩事故の原因になりがちであるため禁止している。BitTorrent はダウンロードしているファイルを同時に他の利用者に公開もするため、違法ファイルを落とさなければ問題ないが、現実問題としてそういう利用者がいて問題となったため、特段の必要がない限り控えてもらうようにした。（E）
- 上記が禁止・制限の理由であるため、Skype や Groove のような不特定ファイル交換に関係のないアプリケーションについては制限していない。（E）
- 対応マニュアルを作成必要がある。（F）
- 著作権団体などが意図的にソーシャル攻撃をしている可能性がある。（F）
- Windows Vista に同包されている Live Messenger への対応に苦慮している。（G）

以上

状況認識のための セキュリティアプライアンス

笠原（九大）* 武蔵（熊大）
須永（富士通SSL） *リーダー

SS研セキュリティマネジメントWG
セキュリティアプライアンスグループ

目次

- セキュリティアプライアンスの必要性
- 技術的紹介
  - ファイアウォール
  - IDS/IPS（侵入検知システム・侵入防止システム）
  - WAF（Web Application Firewall）
  - 利用例としてのP2P対策
- 導入・管理・運用
- まとめ
- 付録：セキュリティアンケートについて

セキュリティアプライアンスの必要性

セキュリティアプライアンスの必要性

- 組織内のインシデントについて知る必要がある
- インシデントへの対応が必要になる

- その技術的解＝セキュリティアプライアンス
  - パケット・トラフィックに対する
    - 監視カメラ
    - 防火壁
    - 検問
  - …のようなもの

状況認識（Situation Awareness）

- 状況を認識しなければ適切に対処できない
  - SNMPによる流量記録ではおおざっぱすぎる
  - tcpdumpによる生パケットでは細かすぎる
- 機器の導入により見えてくる物がある
  - ポート番号ではわからない利用傾向
  - ウィルスの活動・踏み台の発見
  - 機器の設定ミス等々
- リスク分析が可能になり、次の一手への資料になる

インシデント予防と対応

- インシデント予防策としてのアプライアンス
  - ファイアウォールによる可能性の絞り込み
  - IDSによる傾向分析・早期発見
  - IPSによるリアルタイム遮断等
  - 「監視されている」事による利用者への抑止力
- インシデント発生時の対応
  - ファイアウォールによる緊急回避
  - IDSによる類似トラフィックの発見
  - WAFによるパッチ等
- 「アリバイ」証明
  - ログによって、組織外の事件に対する潔白を証明する
- 機器がないと、手も足も出ない場合がある

技術的紹介

ファイアウォール

ファイアウォール

- 通信を特定の基準（ポリシー）に基づき選別する仕組み
- ネットワーク型
  - ネットワーク上に設置、「内」と「外」を区別する
- ホスト型
  - ホストに導入、ネットワークからの攻撃等を防ぐ

ネットワーク型ファイアウォール

- 扱うプロトコル階層による区別
  - パケット単位
    - IPアドレス・ポート番号などヘッダ情報による選別
    - 静的フィルタ・動的フィルタ
    - ステートフル（状態保持型）
      - 主にTCPの状態遷移を認識し正当なセッションを識別
  - セッション・アプリケーション単位
    - セッションを再構築し高次プロトコルを認識して制御
      - ポート番号に依存しないアプリケーション制御
    - 例
      - ポートが固定されていないP2P通信を帯域制限
      - 特定のURLへのHTTPアクセスを遮断

NATとファイアウォール

- ここで言うNATはNAPT（Network Address Port Translation）のこと
  - 内側のプライベートアドレス空間を外側の少数のグローバルアドレスに変換し通信可能とする技術
  - 同じアドレスを使う異なる通信を区別するため、ポート番号を変換し変換表を維持する
- 変換表にない通信を遮断するため、自動的にステートフルフィルタとなる
  - 簡易的な一方通行のファイアウォール
- 高機能なファイアウォールの置き換えになるものではない

プロキシ（proxy）

- サーバとクライアントの間にあって通信を代理・仲介する仕組み
  - 通常クライアント側に置かれ、クライアントがサーバの代わりとして接続する
    - サーバからはクライアントに、クライアントからはサーバに見える
  - プロキシの両側のネットワークを不連続にできる

プロキシの種類

- トランスポート層ゲートウェイ
  - アプリケーションによらず通信を代理で仲介
    - SOCKSが代表的実装
      - プロトコルに依存しないプロキシ動作
      - クライアント側の対応が必要
- アプリケーション層ゲートウェイ
  - 特定のプロトコルに特化
    - ウェブプロキシが代表的
  - 代理だけでなく、通信内容の検査も可能
    - WAF（後述）

可用性と負荷分散

- パケット単位の静的フィルタではきめ細やかで十分な制御ができない
- 動的・ステートフルフィルタ、アプリケーション層での制御は高層になるほど負荷が高い
- 状態をもつと、障害発生時に切り替えが困難
- 負荷分散も難しい
  - セッション単位で振り分ける仕組みが必要になる

ファイアウォールの限界

- 境界線の曖昧さ
  - 可搬型PCによる物理的乗り越え
  - VPN技術による論理的乗り越え
- 許可している通信による攻撃
  - メールやウェブによるウィルス侵入等
- 記述できない制限
  - パケットフィルタではポート固定でないプロトコルを制限する記述ができない、など
- 他の防御機構と組み合わせる必要がある

アプリケーションとの相性

- ファイアウォール導入により影響を受けるアプリケーションがある
  - H.323 などのマルチメディア系
  - e-Learning 系
  - グリッド系
- 一般的でないポートを利用するもの
  - 利用者はファイアウォールで何が制限されているかわからない
  - 個別対応が必要な場合がある

ホスト型ファイアウォール

- ホストに導入し、ネットワークインターフェイスから出入りするパケットを選別
  - ホスト内部の情報を利用した細かい制御が可能
    - 接続ネットワークによるフィルタ設定の切り替え
    - プロセスの動作状況を反映したフィルタ設定
    - 実行ファイル単位でのネットワーク利用許可・不許可
  - パケットの正規化
    - プロトコル違反パケットの破棄・修正
    - プロトコル実装の差違を吸収しOS推定を妨害

主要OSでの搭載状況

- Windows
  - XP/Vista には標準搭載
    - XPはホストから出るパケットを制御できない
    - Vistaではより細かい設定が可能となった
  - 2000には機能はあるがGUIはない
- MacOS X
  - 標準搭載
- Linux
  - iptables など標準で利用可能
- 適切に設定されているかどうかという問題
  - デフォルト設定が良くないと、機能を切られたりする

IDS: Intrusion Detection System
IPS: Intrusion Prevention System
（侵入検知システム・侵入防止システム）

侵入検知システム・侵入防止システム

- ネットワーク型
  - 悪意のあると思われる通信を検出し、警報を発したり、遮断したりする仕組み
    - 誤用検知
    - 異常検知
- ホスト型
  - ホスト上で悪意のあると思われる活動を検出し、警報を発したりする仕組み
    - ファイル改ざん検出
    - ログ監視
    - プロセス挙動監視

ネットワーク型

- ネットワーク上の通信（流量・内容等）を監視し、侵入等を検知
- 誤用（abuse）検知
  - シグニチャ型とも呼ぶ
  - パケット内容を高速に走査
  - 既知のパターン（シグニチャ）に合致すると警報
  - 誤検出の多さが課題
  - 暗号化通信に無力
  - 未知の攻撃に弱い
- 異常（anomaly）検知
  - 平常の通信状態を学習
  - 平常状態からの外れ値を検知し警報
  - 平常状態の学習が難しい
  - 異常値の原因がわかりにくいことがある

IDS（侵入検知）とIPS（侵入防止）

- IDSは横で通信を見ているだけ
  - 監視カメラに相当する
  - それ自身に侵入を防御する機能はない
    - 偽のRSTパケットを送信・ファイアウォールのフィルタルールを変更するといった実装はある
- IPSは通信経路上で動作
  - ファイアウォールに類似
  - 必要に応じて通信を遮断する

実装

- Snort
  - http://www.snort.org/
  - オープンソースのIDS/IPS
  - 検知ルールの購読に有料版と無料版がある
  - Snortベースの商用アプライアンスもある

ホスト型

- ホストに導入し、システムの状態を監視・監査
  - ファイルの改ざん検出
    - 実行ファイルの置き換え
    - ログの改ざん
  - 攻撃らしい通信パケットの検知・遮断
  - ログから特定の文字列を検出
  - システムコール呼出傾向からの異常検知
  - 等々

実装

- Tripwire
  - http://sourceforge.net/projects/tripwire/
  - 主にファイルの改ざんを監視
- OSSEC
  - http://www.ossec.net/
  - ログ解析・システムの完全性チェック・レジストリ監視・rootkit検知等
- デスクトップOS用セキュリティ製品でウィルス検査・ファイアウォールとともに統合されてきている

UTM: Unified Threat Management

- 「統合脅威管理」
  - ファイアウォール・アンチウィルス・IPS・コンテンツフィルタ等のネットワークセキュリティ機能を統一管理すること、また統合された機器
- 利点
  - 低い導入・管理コスト
- 欠点
  - 低い自由度・耐故障性

WAF
（Web Application Firewall）

Web Application Firewall

- ウェブ通信に特化したファイアウォール
  - ウェブサーバの手前に設置
  - クライアントからの要求やサーバからの応答内容を検査
  - ポリシーに合致しない通信を遮断
  - 危険な要求や応答内容を安全なものに変換
- レガシーなアプリケーションを修正せずに防御
- 「リバースプロキシ」の一種
  - 通常のプロキシはクライアントの代理
  - リバースプロキシはサーバの代理

WAFの機能

- ウェブサーバ・サービスへの様々な攻撃を検出し、防止する
  - SQLインジェクション
  - クロスサイトスクリプティング
  - OSコマンドインジェクション
  - クッキー改ざん
  - 入力フォームのhidden属性改ざん
  - クレジットカード番号漏洩
  - バッファオーバーフロー
  - 不正なページ遷移
  - ディレクトリトラバーサル
  - エラーページ・HTTPヘッダからの情報漏洩
  - 表示ファイルタイプの規制
  - 文字コード変換によるフィルタ回避
  - 等々

利用例としてのP2P対策

P2Pとは

- Peer to Peer モデル
  - 計算機ネットワークの形態の一つ
  - クライアント・サーバモデルの対義語
  - ネットワークに参加するホストが明確なクライアントやサーバという区別をもたず、クライアントとサーバの両方の機能を兼ね備えた同等もしくは類似した役割を担う
- P2Pモデルを応用したソフトウェアを指すこともある

具体的な応用例

- ファイル共有
- 情報共有
- メッセンジャー
- 音声通信
- CDN（Contents Delivery Network）

何が問題か

- P2P自体は単なる通信技術
- 応用としてのファイル交換ネットワーク
- 使われ方で問題が発生している
- ポートの固定されたサーバ・クライアントモデルより通信状況を把握しにくい
- 状況把握・利用制限のためにはセキュリティアプライアンスの導入が必要な場合も

違法ファイル共有

- CDやDVDを吸い出したファイルの違法流通
  - 音楽・映画・ゲーム等々
- 効率化のための機能による問題
  - キャッシュ機能・ダウンロード中ファイルの他ホストへの公開など
    - 利用者が意識せずとも違法ファイル流通に荷担
  - 権利者から組織等に警告、法律問題に発展の危険性もある

情報漏洩

- P2Pを利用した情報漏洩ウィルスの存在
  - マイドキュメント等を固めてP2P網に放流
  - P2P網には一般にファイルを削除する手段が提供されていない
    - いったん放流されると回復が困難
- P2Pが悪いと言うより、利用者の管理が問題
  - P2Pで流通するファイルは感染危険度が高い
  - ウィルス感染の危険性が高い環境で秘密情報を扱うのが問題
- 家族の共用PCに知らないうちに入っていた、といった事例も

制限するか否か

- P2Pソフトウェアの利用自身は違法ではない
- 利用の仕方によるリスクをはらんでいる
  - 現実問題としての事件・事故
    - ウイルス感染
    - 情報漏洩
    - 権利団体からのクレーム
  - トラフィックの増大
- 最終的には組織ごとの判断になる
  - 問題が起きてから慌てないように準備
  - なぜ制限しているのかの説明根拠も必要

どう規制するか

- 規則・広報など人的な手段による努力目標
- トラフィックの監視
  - セキュリティアプライアンスによる監視
    - 流量制限等可能な製品もある
  - 商用監視サービスの利用
- フィルタ・流量制限
  - セキュリティアプライアンスによる対応
  - 主要なポートのフィルタ
    - ポート番号を変更されると抜けられる

利用者への対応

- 技術は悪くない→使う人間が悪い
  - 広報・教育に頼らざるを得ない部分
- 外国人対応
  - 国によって著作権に対する感覚が異なる
  - 単純に言葉の問題で規則が周知されない
- 規制の際に、留学生や外国人研究者によるP2Pの利用に少し注意が必要

導入・管理・運用

管理的側面について

- コストの問題
  - 初期導入コスト
  - 維持管理コスト
- 運用ポリシー
  - 「盗聴」と同等のことが可能になる
  - 内容を見ての遮断は検閲になりかねない
  - 機器そのもの、ならびに機器の生成するログへのアクセス権限が重要な問題となる

どこにどう入れるか？

- 安い物ではないため、予算とのトレードオフ
  - 導入コストと並んで維持コストが高い物が多い
- 一般的な選択肢
  - 対外ルータの近傍
    - インターネットからの防御
  - 主要なスイッチに付随
    - 内部から内部への攻撃なども監視・防御
  - 主要なサーバの近傍
  - 機密度の高いネットワークへの入り口（中への防御）
    - 事務系ネットワーク・病院系等
  - 信頼度の低いネットワークへの入り口（外への防御）
    - 学生寮・教育システム・共用ネットワークなど

ネットワーク設計との関係

- 監視しやすいネットワーク設計が必要？
  - 主要トラフィックの流れを想定し効率的なフィルタ・監視ポイントを設定
  - IDSの場合ポートミラーやスプリッタの設置を考える必要がある
    - 10GbE のミラーリングや分岐は容易でない
  - UTM等それ自体がボトルネックになりかねない
- ネットワークの更新時にまとめて設計できるといいのではないか
  - 導入後の状況把握により、新たな機器が必要とされる場合もある

更新計画

- 機器の更新を視野に入れた計画が必要
- 陳腐化
  - トラフィックの増加
  - ネットワークの更新による速度向上・インターフェイスの変化
  - 保守切れ
    - データベースの更新されないアプライアンスは無用の長物
- 互換性
  - 新種のサービス・プロトコルへの対応
    - 例: IPv6
  - 特定サービスとの非互換性
    - 例: H.323（遠隔会議の主要プロトコル）など

ログ管理

- これらの機器は通常大量のログを生成する
- 管理ポリシーが必要
  - どこに保存するか
    - syslogサーバ・外付けストレージ等
  - どれくらいの期間保存するか
    - インシデント発生時は過去にさかのぼる必要がある
    - 持っていると官憲に出さないといけなくなる可能性はある
  - 閲覧権限の規定
    - インシデント発生時のみ詳細閲覧可
    - CISOの許可等
  - 統計解析問題
    - 物量があるので人手も時間もかかる
    - アウトソースも視野に入れて検討が必要

導入前の準備（理想論？）

- 運用ポリシーを決める
  - ポリシーが決まらないとコスト計算ができない
- コストを計算する
  - これに従って導入規模等を決める
- 構成員の同意を得る
  - セキュリティポリシーに入れる
  - 雇用契約時に宣誓書で遵守させる
  - etc…
- 実際は機器を入れてから考える場合が多い

まとめ

- セキュリティアプライアンスは、組織内ネットワークの状況把握に重要な役割
- 初期コスト＋維持コストがかかる
  - お金
  - 人手
  - 手間
- 有用だが、導入には覚悟が必要
  - ただ漫然と入れると、高価な宝の持ち腐れ

付録: セキュリティアンケートについて

- セキュリティアプライアンスに関する事例調査
  - 機器の傾向
  - 導入の動機
  - 運用/管理の実情
- P2P対策の現状
- 十分な情報を得るため、一部の機関に協力をお願いした

2.3. エンドポイントのためのセキュリティ対策

2.3. エンドポイントのためのセキュリティ対策

1 人 1 台以上のパソコンの普及やネットワーク環境の充実、USB メモリ等可搬媒体の大容量化により、短時間に多くの人に情報が伝達できるようになりました。このように便利になる一方、コンピュータウィルス／スパイウェアの感染や、盗難、紛失、誤操作、P2P ファイル共有ソフトウェアによる情報漏洩の危険性も高まっています。

学内のイントラネットでは、ファイアウォールの設置やサーバのセキュリティ対策、ネットワーク／サーバの監視等、システム管理者によりセキュリティ対策がなされています。しかし、利用者側のパソコンについては、利用者依存になっている部分が多く、対策が充分できているとは言いがたい状況です。そのため、利用者パソコンが原因で、サーバ側のサービスに影響を及ぼすこともあり、システム管理者の負担を増やす要因となっています。このことから、エンドポイント（利用者側）のセキュリティ対策が重要と考え、対策を検討しました。

エンドポイントのセキュリティ対策は、対象者（教員、職員、学生、技術専門職員、その他（研究員、名誉教授、特任教授、客員教授）毎に、ソリューションを松竹梅で検討しました。以下に概要を示します。

対策レベル１：梅

エンドポイントでセキュリティ対策を実施します。具体的には、ウィルス・スパイウェア対策ソフトウェアやパーソナルファイアウォールの導入、ファイルの暗号化、重要データのファイルサーバへの集約等の対策です。

この対策の利点としては、簡単に始められる、今の利用形態と差が少ない、端末毎の多様性（OS、アプリケーション）が許容される等が挙げられます。

一方問題点としては、利用者任せのセキュリティとなる、機器の紛失、データの漏洩が防げない、事前に被害の可能性が把握できない等が挙げられます。

コストは、短期的には投資額は低く抑えられますが、インシデント発生時にコストが高くなる可能性があり、中長期的には保守コストとの兼ね合いで評価する必要があります。

また、対策レベル１.５として、梅に加え、エンドポイントをフィイアウォールや NAT で隔離することが考えられ、更にセキュリティレベルを上げることができます。

対策レベル２：竹

エンドポイントでセキュリティ対策を実施し、ネットワーク側で実施状況を確認します。具体的には、パソコン等機器をネットワーク接続時に認証や検疫、アクセスコントロールを行います。

この対策の利点としては、利用者管理が可能となり梅よりセキュリティが高い、簡単に始められる、今の利用形態と差が少ない、エージェントレスの場合、端末毎の多様性（OS、アプリケーション）が許容される等が挙げられます。

一方問題点としては、認証に時間がかかる、エージェントの場合、端末の多様性(OS)に対応できない、機器やデータが持ち出し可能であり、機器の紛失、データの漏洩が防げない、事前に被害の可能性が把握できない等が挙げられます。

コストは、短期的にはある程度投資が必要ですが、中長期的には保守コストとの兼ね合いで評価する必要があります。

また、対策レベル２.５として、ブレード PC が考えられます。ブレード PC は、PC を構成する CPU、メモリ、ハードディスクなどの主要な部品を、１枚のブレード（基盤）に集積し、マシンルームにまとめて設置します。クライアント側には画面を転送し操作します。このようにディスクレスにすることで、データの漏洩を防ぐことが可能です。一方、問題点としては、竹と同様セキュリティ対策が利用者任せになってしまう点が挙げられます。

対策レベル３：松

エンドポイントにはデータを保持せず、センター側でソフトウェアやデータを一元管理します。具体的には、端末はシンクライアントとし、アプリケーションは業務で必要なものに限定し、データはセンター側で一括管理する等、管理を徹底します。

この対策の利点としては、セキュリティ対策が一元化できる等管理が容易、利用者による情報漏洩等のリスクが低い、予防／対策が迅速にでき徹底することが可能、被害規模の想定が可能等が挙げられます。

一方問題点としては、集中管理していることから、インシデント発生時に影響が大きいことが挙げられます。

コストは、短期的には投資額が大きくなりますが、保守コストが低減できることが考えられるため、中長期的には保守コストとの兼ね合いで評価する必要があります。

上記の通り、セキュリティ対策を松竹梅のレベルに分けて提示させていただきましたが、センターのポリシーや予算に合わせて選択いただければと考えます。

その他、エンドポイントの課題として以下が考えられ、今後検討していく必要があると考えます。

USB メモリ等の可搬媒体が普及し、容易にデータ交換が可能になりました。一方可搬媒体からウィルス／スパイウェアに感染するケースが増えており、可搬媒体を PC 等の機器にさす前に、ウィルスチェックできる仕組みが必要です。

また、利用者側のセキュリティ対策が進まない原因として、ウィルススキャンのやり方が分からない、時間がかかる等利用者の負担になっていることが考えられます。これらの解決策として、USB にさせば自動的にチェックする等、容易にウィルススキャンできる仕組みが必要と考えます。

更に、P2P ファイル共有ソフトウェアによる情報漏洩も後を絶たないことから、業務に必要ないアプリケーションの使用を禁止、利用できるアプリケーションを限定できるような仕組みが必要と考えます。

別紙. 利用者別エンドポイントのセキュリティ対策（松竹梅）

利用者	利用形態	セキュリティ対策			備　　考
		松 システム的なセキュリティ対策 （端末にデータを保持しない）	竹 システム的なセキュリティ対策 （端末にデータを保持する）	梅 主に端末のセキュリティ対策	
職員	業務処理に利用	【ポリシー】 ・端末にデータを持たない（シンクライアント） 【対策】 ・画面転送型、端末型シンクライアント ・リモートアクセス型サービス	【ポリシー】 ・機器のセキュリティ対策と実施状況の管理まで実施 【対策】 ・検疫ネットワークの構築による、個別端末の監視 ・共通データの集約	【ポリシー】 ・端末のセキュリティ対策 【対策】 ・ウィルス対策、パーソナルファイアウォールなどの導入 ・ハードディスクの暗号化 ・共通データの集約	・組織的な対応が可能 ・業務の種類によっては、対応が困難な場合がある。例えば、施設系職員の業務など。
教員	教育・研究に利用 成績データの管理等業務に利用（成績情報等の重要なデータあり）	【ポリシー】 ・教育・研究用と業務用を分ける 業務用は、職員端末と同じ扱い 【対策】 1）教育・研究用 ・特殊な用途以外は、業務用と同等 ・特殊な用途のPCに対しては、「竹」、「梅」の対策 ・認証後にシンクライアント環境を仮想的に実行 2)業務用 ・画面転送型、端末型シンクライアント ・リモートアクセス型サービス	【ポリシー】 ・機器のセキュリティ対策と実施状況の管理まで実施 【対策】 ・検疫ネットワークの構築による、個別端末の監視 ・共通データの集約	【ポリシー】 ・端末のセキュリティ対策 【対策】 ・ウィルス対策、パーソナルファイアウォールなどの導入 ・ハードディスクの暗号化 ・共通データの集約	・教育/研究用と業務用を分ける ・学内からだけでなく、学外からの利用がある ・学外からのアクセス可能な情報の分離が必要 ・学外からは、重要度の応じて、画面転送、暗号化などを実施
学生	教育用PC（授業等で使用）	【ポリシー】 ・端末にデータを持たない（シンクライアント） 【対策】 ・画面転送型、端末型シンクライアント ・リモートアクセス型サービス	【ポリシー】 ・機器のセキュリティ対策と実施状況の管理まで実施 【対策】 ・ハードディスクキーパーなどによる改変阻止 ・検疫ネットワークの構築による、個別端末の監視	【ポリシー】 ・端末のセキュリティ対策 【対策】 ・ウィルス対策、パーソナルファイアウォールなどの導入	・不注意によるウィルス感染や不正侵入への対策が必要 ・被害の拡大が速い ・障害が発生すると、教育活動に支障が発生する ・学外からのアクセス可能資源の設定が必要
	持ち込みPC 研究室配属学生も同等？	【ポリシー】 ・学内では、学内用の環境を提供する 【対策】 ・認証後にシンクライアント環境を仮想的に実行	【ポリシー】 ・利用権限の確認と接続可能な端末の制限 【対策】 ・認証によって、利用権限を制限する。 ・検疫によって、ウィルス対策の実施状況などを確認する。	【ポリシー】 ・利用権限の確認 【対策】 ・認証によって、利用権限を制限する。	・端末がセキュリティレベルを決めてしまう ⇒マネジメントが必要
技術専門職員	教育・研究に利用	【ポリシー】 ・通常業務用と特殊業務用を分ける ・業務用は、職員端末と同じ扱い 【対策】 1）特殊業務 ・PCに対しては、「竹」、「梅」の対策 ・認証後にシンクライアント環境を仮想的に実行 2)通常業務 ・画面転送型、端末型シンクライアント ・リモートアクセス型サービス	【ポリシー】 ・機器のセキュリティ対策と実施状況の管理まで実施 【対策】 ・検疫ネットワークの構築による、個別端末の監視 ・共通データの集約	【ポリシー】 ・端末のセキュリティ対策 【対策】 ・ウィルス対策、パーソナルファイアウォールなどの導入 ・ハードディスクの暗号化 ・共通データの集約	・学内からだけでなく、学外からの利用がある ・技術力に大きなばらつきがある。
その他 （研究員、 名誉教授、 特任教授 客員教授）	教育・研究に利用	・研究教育用は研究室配属学生と同じ	・研究教育用は研究室配属学生と同じ	・研究教育用は研究室配属学生と同じ	・学内からだけでなく、学外からの利用がある ・業務は無いはず（業務用端末が必要ならば、事務職員と同等） ・研究室配属学生と同等
問題点と利点		〈問題点〉 ・インシデント発生時(サーバ)の影響が大 ・初期コストは大きい 〈利点〉 ・利用者によるリスクは低い ・セキュリティ管理の一元化 ・管理しやすい ・セキュリティ対策の一元化 ・予防のポイント、被害の規模が想定可能 ・対策状況を把握できる ・予防・処置の迅速性、徹底	〈問題点〉 ・利用者まかせのセキュリティ ・機器の紛失、データ持ち出しが可能 ・データ流出を防げない ・検疫に時間がかかる ・エージェントの場合、端末の多様性(OS)に対応できない ・被害の可能性が把握できない ・機器を持ち出したときに対応の必要性・データ持ち出しの危険性 ・起動が遅い(利便性の低下) 〈利点〉 ・認証を貫徹できる（利用者管理） ・ソフトウェアの管理が可能 ・今の利用形態と差が少ない ・端末ごとの多様性(Apps)を許容できる	〈問題点〉 ・利用者まかせのセキュリティ ・データ流出は防げない ・機器紛失、持ち出しが可能 ・対策が一元的にとれない ・強制が難しい ・管理が難しい ・被害の規模が把握できない 〈利点〉 ・簡単に始められる ・今の利用形態と差が少ない ・端末ごとの多様性(OS、Apps)を許容できる	
コスト		・短期的には投資額は高い ・中長期的には保守コストと効果で判断	・短期的にはある程度の投資が必要（梅のコスト+α） ・中長期的には保守コストと効果で判断	・短期的には投資額は低い ・中長期的にはは保守コストと効果で判断(高くなることもある) ・インシデント発生時のコストが高くなる可能性あり	新たな脅威に対し、継続的な投資が必要。

エンドポイントのためのセキュリティ対策

三谷/山田（富士通）*、只木(佐賀大)、
吉田（富士通）
*リーダー

SS研セキュリティマネジメントWG
エンドポイント・グループ

目　次

- 現状
- 課題
- 解決策
- 検討項目
- その他　エンドポイントで更に検討すべき課題
- ご参考　ソリューションに関するURL
- 別紙１．利用者別エンドポイトのセキュリティ対策
  （松竹梅）

現状：二つのセキュリティイシュー

- ウィルスやスパイウェア対策
- エンドポイントからの情報流出

現状：エンドポイントのロケーション

- 物理ロケーション
  - 学内LAN接続(有線)
  - 学内LAN接続(無線LAN)
  - 学外からの接続(VPN, SSH, など)
- リスクロケーション
  - 脆弱性/セキュリティホール発見時
  - 新種ウィルス発生時
  - 新型攻撃手法
  - 春夏休み空けの古いウィルスパターン・古いPatch適用レベル

課題：エンドポイントの状況は？

- エンドポイントがセキュリティホールになっている
- サーバ類は管理者が守れるが、エンドポイントはエンドユーザでは守れない
- 認証、アクセス制御、検疫で守れるか？
- 管理コストが大きくなりすぎる

課題：PCを仕事に使えるか？

- 仕事に必要な機能は何か
- 仕事に不要な機能が多すぎないか
- 「倫理」では守れない
- Vistaは移動プロファイルの展開が遅い
- リアルタイムスキャンが遅い

課題：端末がサービスの足枷になる？

- サーバのサービスに端末が対応できない（たとえばセキュリティ強度）
- 端末がサービス全体の足を引っ張る
- 一番古い端末にあわせてサービスレベルを決めるの？

解決案：検疫という解

- **検疫の頻度はどの程度が適切か？**
- **どこまで実施するのか？**
- **検疫のタイプ**

	特長	用途
エージェント	OSが限定される	持ち出し端末 固定端末
エージェントレス	検疫対象が少ない	固定端末

- コストはどうか？

解決案：シンクライアントという解

- ネットワークブート型
  - システム構成は管理できる
  - データ持ちだしをコントロールできない
  - ネットワーク帯域の問題
- 画面転送型
  - システム構成は管理できる
  - データ持ちだしをコントロールできる
  - 運用方法に検討の余地あり
- ライセンス料の契約数によってはかえって高価

解決案：リモートデスクトップという解

- Citrix
- Sun Global Secure Desktop
- MS のターミナルサービス
- データやアプリケーションの制限可能性
- コストはどうか？

検討項目：何を検討すべきか？

- 対象者（教員,職員,学生）別に検討する必要がある
- 対象者が教職員の場合、職場外からの仕事環境は？
  - VPNとリモートデスクトップ
  - 教育現場では自宅からの仕事環境が必須
- データ共有と移動方法は？
  - 安全な媒体は？
- 本当に必要なアプリケーションのセットは何か？
- 端末の世代が混じった環境で継続できるサービスを考える

➡ **対象者毎にセキュリティ対策ソリューションを松竹梅で検討する**

その他：エンドポイントで更に検討すべき課題

端末本体以外のチェックや、容易なチェックの仕組み

- 外部ストレージ（USB、メモリカード）をさす前にチェックする仕組み
- 簡単にウィルススキャンできる仕組み
  ⇒USBにさせればチェックしてくれる等
- 業務用アプリケーションセット指定
  ⇒使用禁止アプリケーションのチェック
  ⇒アプリケーションのバージョン管理

ご参考：ソリューションに関するURL

シンクライアント

・SunRay http://jp.sun.com/products/desktop/sunray/
・FMVシンクライアント
http://www.fmvworld.net/biz/fmv/product/hard/vtc0504/
・USB でシンクライアントに http://www.saslite.com/index.html
・Ardenceネットワークブート
http://www.adir.co.jp/ardence/index.html
・NTTデータ　コアブート http://www.coreboot.jp/about/index.html
・リモートアクセス環境 ・Microsoft Windows 2008サーバのTerminal Service, Remote Application
http://www.microsoft.com/japan/windowsserver2008/virtualization/client.mspx
・Citrix Presentation Server
http://www.citrix.co.jp/products/cps.html
・Sun Secure Global Desktop Software
http://jp.sun.com/products/software/sgd/

ご参考：ソリューションに関するURL

認証・検疫ネットワーク

・Opengate http://www.cc.saga-u.ac.jp/opengate/
・Ferec http://www.ferec.jp/
・アラクサラの認証スイッチ
http://www.alaxala.com/jp/solution/authentication/index.html
・富士通認証ネットワークSR-Sシリーズ
http://fenics.fujitsu.com/networksolution/oim/models/securityninshou_model.html
・PFUの検疫ネットワークiNetSec Inspection Center
http://www.pfu.fujitsu.com/inetsec/

3. 第一期検討テーマ

（第一期成果レポートより）

3. 第一期検討テーマ（第一期成果レポートより）

はじめに

近年インターネットの治安情勢は悪化しつづけ、情報セキュリティに関わる問題は深刻化している。攻撃は、大規模で表面化しやすいものから金銭目的の小規模なものへと変化し、研究・教育を主たる目的とする会員所属機関においてもサイバー犯罪にまきこまれる可能性がでてきている。SS研究会セキュリティマネージメントWGでは、水際で奮闘するセキュリティ担当者に有用な情報を提供することを目的に、先進的なセキュリティ対策（攻めのテーマ）と実用的なセキュリティ対策（守りのテーマ）を2本の柱として議論を重ねてきた。本レポートは、第一期の活動（2007年2月から11月まで）をスライド形式にまとめて報告するものである。

第一期には、「組織」、「spam対策」、「フォレンジック」の三つをテーマに選んだ。テーマの選択は、2006年10月の準備会と第一回のWG会合で我々をとりまくセキュリティ状況を概観し、活発な議論を経て絞り込んだものである。会員の多くを占める大学機関では、部局の自治を尊重しつつもセキュリティの質を低下させないマネージメント力が求められている。マネージメントにおいては、セキュリティが組織にとって過剰な負担とならないように調整することが重要である。このため、本WGでは「組織」を最重要のテーマに位置づけている。実用的なテーマとしては、「spam対策」を取り上げた。spamはメールを利用するすべての人に関わる社会的な問題となっている。所属機関の多くは社会的な責任を果たすため、人的資源と情報資産をかけてこれに取り組んでいる。我々はよく行われている対策をマネージメントの視点から分析した。三つ目のテーマである「フォレンジック」は先進性を重視して取り上げたものである。まだ一般的には浸透していないが、情報マネージメントを行う者は、これを避けて通ることができないだろう。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、いまからフォレンジックについての知識を得ることが必要である。本レポートがデジタルフォレンジック技術への入り口となれば幸いである。

WG活動は、準備会を含めて計5回の会合、メーリングリスト、Webコンテンツマネージメントソフトウェア POESYでの議論が源となっている。すべてにおいて議論がスムーズに行えたのはSS研究会事務局に負うところが多い。WGメンバー一同、事務局の諸氏に感謝する次第である。

まとめ役　湯浅富久子

3.1. セキュリティマネージメントのための組織

3.1. セキュリティマネージメントのための組織

大学における教育、研究、医療、そして組織運営の全てにわたって情報技術が不可欠な要素となっています。情報ネットワーク、情報システム、そしてその上に保有されている様々な情報は、まさしく大学の基盤を構成しています。こうした情報とシステムの有効活用は、組織の活性度や効率性を左右します。

一方で、コンピュータウィルスや情報システムへの様々な不正侵入によるセキュリティ脅威も日増しに大きく、社会問題にもなっています。コンピュータウィルスというと、コンピュータを管理する個人の問題のように矮小化されがちですが、そこで失われる、あるいは漏えいする情報が、個人情報漏えいなどとなり、組織に大きなダメージを与える場合もあります。

大学の情報システム、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。情報セキュリティの基本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、日常的な情報セキュリティマネージメント体制が必要です。情報漏えいや不正侵入などの事故に際しても、迅速かつ的確に対応するための非常時用体制を日頃から整えておく必要があります。

セキュリティポリシーは、主に日常的なセキュリティ維持・向上のための基本方針を定めるものです。セキュリティに関する責任者などの人的体制、セキュリティに関する教育体制、ポリシーの遵守状況の監査、情報の重要度を定めそれぞれの扱いを定めるための基本、情報システムの構築・運用の基本となる認証、権限管理、アクセス制限などを定めます。政府統一基準、高等教育機関向け規定集などのセキュリティポリシーの雛形が利用できます。また、雛形があれば、コンサルティングなどの手助けを受けることも可能となります。

セキュリティポリシー及びそれに基づく規程類を一度に完全にすることはできません。実施できないものを定めることで、かえってポリシー違反を誘発することもあります。策定、実施、そして見直しのサイクルを繰り返すことで、セキュリティ維持のレベルを上げることを考えるべきです。

情報漏えいや不正侵入などの事故は、無いにこしたことはありませんが、起きたときのための準備は必要です。発見者の通報義務、連絡網、緊急待避対策、対応体制を整備しておく必要があります。対外的な対応体制も必要です。文部科学省、IPA、警察などへの報告手順、必要に応じた記者会見、捜査への協力の基準なども定めておくべきです。また、緊急避難のためにネットワークを切断したりシステムを停止する必要があります。その時の責任体制を明確にする必要があります。特に、現場の技術担当者に過剰な責任を負わせない必要があります。IPA や JPCERT に対応マニュアルがあります。

情報セキュリティは技術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。利用者への教育だけでなく、システム管理者そしてシステム発注者への教育が必要です。IPA からの資料が利用できます。

近年、ノートブック型パーソナルコンピュータが普及しています。また、様々なタイプの外部記憶装置も活用されています。このようなものを活用して、場所を問わずに活動するユビキタス環境は確かに便利です。しかし、同時に情報セキュリティにとって大きなリスクでもあります。セキュリティ対策としては、こうしたユビキタス環境との調整行う必要があります。この問題は、働き方の問題にも踏み込む難しい問題です。

情報セキュリティ対策を考えると行うべき業務が限りなく膨らみそうです。何のための情報システムかを見失うかもしれません。そこで情報システムに対する考え方の転換が必要に思われます。私たちが必要なのは情報システムのサービス・機能であって、システムそのものでは無いはずです。箱物としてのコンピュータの数を減らす、シンクライアントなど機能を絞った端末を活用する、情報を整理して共通化する、サービスを外注するなど、積極的な方向転換が必要な時期に来ています。

セキュリティーマネジメントのための組織

只木(佐賀大)*　吉田(富士通)
*リーダー

SS研セキュリティーマネジメントWG
組織グループ

情報セキュリティ対策の必要性

- 情報システムと情報資産は大学業務の基盤
  - 情報システムの無い教育、研究、医療、大学運営は考えられない。
- 情報システムへの不正侵入や情報漏えいは大きなダメージ
  - 「ウィルス感染」のように問題を矮小化してはいけない
- 組織的対応が必要
  - 組織としての信用

組織整備の必要性

- 日常的なセキュリティマネジメント
  - セキュリティポリシーの策定
  - セキュアな情報システムの構築
  - ルールの遵守状況の監査
- インシデント時の対応
  - 現場が迅速に動けるように
  - 責任体制の明確化
  - 渉外の一本化

セキュリティポリシー (平常時)

- 日常的セキュリティ維持・向上体制
  - CISO(最高情報セキュリティ責任者)の設置、セキュリティ委員会、セキュリティ責任者、連絡網
- 情報の格付け
  - 機密性、完全性、可用性
- セキュアな情報システムの構築指針
  - 認証、証跡、権限管理、アクセス制限、セキュリティホール対策、ログ管理

セキュリティポリシー (平常時)(2)

- 利用者教育と利用者の義務
- ルールの遵守状況の監査

セキュリティポリシー (非常時)

- 通報義務
  - 職員の通報義務
- 連絡網
- 緊急待避対策
  - 情報関連部署の権限明確化
  - 技術者に責任を負わせない
- 対応体制
  - 常駐が必要
- 改善に向けた対策

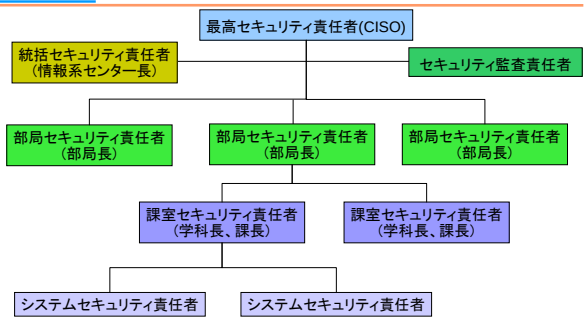
セキュリティポリシーを作る

- 無理のないポリシー
- 実情にあわせた手順
- 改善点を発見し、改善する
- セキュリティーに完全は無い
  - PDCAサイクルを回すことで徐々に改善
- ポリシー策定支援ソリューションの活用
  - 雛形があればあまり高価にならない

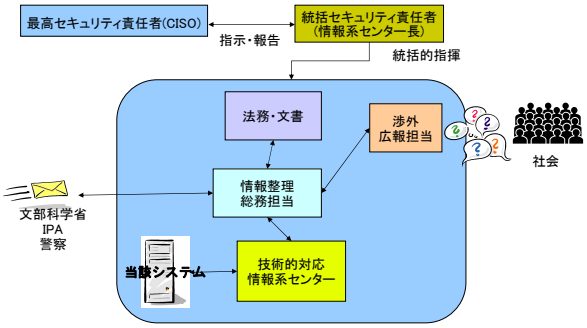
セキュリティポリシーを作るために

情報セキュリティガバナンス	http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html
政府機関の情報セキュリティ対策のための統一基準	http://www.nisc.go.jp/active/general/kijun01.html
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	http://www.nii.ac.jp/syskan/sp/
法律・ガイドライン	http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm
脆弱性関連情報取扱体制	http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
ISMS [情報セキュリティマネジメントシステム]	http://www.isms.jipdec.jp/
プライバシーマーク(R)制度	http://privacymark.jp/
組織ポリシー策定/監査ソリューション	http://segroup.fujitsu.com/secure/solution/sol1.html http://segroup.fujitsu.com/secure/service/audit.html
セキュリティ認証取得ソリューション	http://segroup.fujitsu.com/secure/service/consulting/infosecure3.html

セキュリティーマネジメント組織 (平常時)



セキュリティーマネジメント組織 (非常時)



インシデント発生時

- 迅速な対応
  - 技術的対応：システム切断
    - 電源断は要注意：証拠を残す
  - 被害拡大を防ぐ
  - 必要に応じて通報：隠さない
    - 文部科学省、IPA、警察
  - 必要に応じて記者会見

インシデント発生時(2)

- 組織内部署の役割分担
  - 平常時から組織整備
  - 技術的対応、渉外、法務、総務を分離
- 対応マニュアル
  - コンティジェンシプラン
  - データ提供手順

インシデント対応マニュアル

- 情報漏えい発生時の対応ポイント集
  - http://www.ipa.go.jp/security/awareness/johorouei/
- 組織内CSIRT構築支援マテリアル
  - 組織内のインシデント対応組織
  - http://www.jpcert.or.jp/csirt_material/

セキュリティ関連団体

- セキュリティ関連情報の取得
- インシデント発生時の対応
- セキュリティ向上・維持の方針

IPA［情報処理推進機構］	http://www.ipa.go.jp/security/
JPCERT/CC [JPCERTコーディネーションセンター]	http://www.jpcert.or.jp/
JIPDEC [財団法人 日本情報処理開発教会]	http://www.jipdec.jp/

教育

- 情報セキュリティーは技術だけでは守れない
- 利用者教育
  - 日々の情報を扱う作業
  - 情報システムの利用
- 管理者教育
  - 情報システムの管理・管理運用
- 発注者教育
  - 情報システム構築時の注意

教育(2)

情報セキュリティ読本 改訂版	http://www.ipa.go.jp/security/publications/dokuhon/2006/
情報セキュリティ教本	http://www.ipa.go.jp/security/publications/kyohon/
セキュアなWebサーバーの構築と運用	http://www.ipa.go.jp/security/awareness/administrator/secure-web/
情報システムの信頼性向上に関するガイドライン	http://www.meti.go.jp/press/20060615002/guideline.pdf
最新IT解説：セキュリティ	http://sme.fujitsu.com/tips/itnew/

CIO/CISOの役割

- CIO(最高情報統括責任者)
- CISO(最高情報セキュリティ責任者)
- 誰が行うべきか
  - CIOとCISOを必ずしも分けなくても良い
- どういう役割かを整理する

用語	http://e-words.jp/w/CISO.html
SS研講演：岐阜大 篠田先生	http://www.ssken.gr.jp/MAINSITE/download/newsletter/2006/edu/stg_edu-1/doc6.html
SS研講演：京大 上原先生	http://www.ssken.gr.jp/MAINSITE/download/newsletter/2004/stg/2/1_uehara.html

大学法人役員の役割

- セキュリティの重要性を認識する。
  - セキュリティインシデントによるダメージを知る。
- セキュリティ改善の先頭に立つ。
  - セキュリティ改善は継続的活動
  - 組織トップの姿勢は極めて重要

ユビキタスとセキュリティ

- データ持ち出し、モバイルPCへの対応
  - 便利さとセキュリティーの調整が必要
- 重要データは持ち出させない
- 持ち出し時の手順を定める
- 特に教員の場合
  - 校務と研究・教育を区分する
  - 校務は職場で行う

セキュリティが過剰な負担にならないために

- 情報・情報システムの棚卸し
  - システムの数を減らす
  - 学内のサーバをセンターに集約する
  - 仮想化
- アウトソーシング
  - SaaS、ASP
- 業務端末のあり方の検討
  - シンクライアント
- 免責の明示

セキュリティが過剰な負担にならないために(2)

- 守備範囲を定める
  - 全て、100%は不可能
- 情報・情報システムに関わるリスクを洗い出す
  - リスクの分類
    - 必ず解消、解消を努力、リスクの存在を認識
- 守るべき情報・情報システムの範囲を定める
  - セキュリティレベルの異なる情報システムを同じネットワークに混在させない

3.2. spam 対策

3.2. spam 対策

電子メールは、コミュニケーション手段の一つとして不可欠な物となっています。これに伴い spam メールに関する問題が大きな社会問題となっています。spam メールとは、受信者の意図を無視して無差別かつ大量に一括して送信される電子メールを指し、UCE（Unsolicited Commercial E-mail）、UBE（Unsolicited Bulk E-mail）とも呼ばれています。電子メールは、通常の郵便など他のコミュニケーション手段と比べると、送信者側があまりに安易に多くの相手に対して送信でき、送信者側の負担が金銭的にも時間的にも労力的にも極めて少ない、といった特徴が挙げられます。そのため spam メールの数は非常に多く、世界の spam メール送信数は一日に 550 億通、インターネットを流れる電子メールの 95%以上が spam メールであるという報告もあります。今後もインターネットの普及に伴い電子メールの流通量は増え続け、spam メールによる被害も増加の一途を辿るでしょう。

spam メールから引き起こされる具体的な被害としては、メールサーバの CPU、ディスクやネットワークリソースを浪費するため、メールの受信に時間（通信費用）がかかり、メールボックスが一杯になり、spam でないメールも受け取れなくなること、受信したメールの分類・削除に手間がかかることや、それにともない重要なメールの見落としもおこるかもしれないということがあります。また、spam メールを原因とした間接的な被害として、発信者詐称による spam メール発信者との誤解や、そのための苦情メールへの対処、詐称されたドメイン名の信頼性の低下とその後の通常メールも受信拒否される危険性等の間接的な被害もあります。詐称された発信者へのエラーメール(バウンスメール)の集中も問題になります。短期間に大量の spam によりエラーメールが同一利用者あるいは同一ドメインに送られることになれば、それは事実上のサービス不能攻撃（denial of service attack）となってしまいます。

spam 対策は、メールを受信した個人が行うもの、メールサーバを運用する会社/大学/ISP 等が行うもの、法制度等があり、それらを組み合わせて spam を減らしていく努力が続けられています。利用者個人が行う spam 対策は、メールの内容からコンテンツフィルタによる自動分類や、spam を見ても返信しない、添付の URL を開かない等、受信後の spam に対する処理や対応が中心になります。一方、メールサーバ管理者が行う対策は、spam を送らない、受け取らないという、spam が存在しにくい環境を実現する spam 予防の性格が強いものになっています。今回は、メールサーバ管理者が行う spam 対策を中心に検討し、資料にまとめました。

spam対策

吉田（大分大）* 笠原（九大）
長谷川（中京大）
*リーダー

SS研セキュリティマネージメントWG
spamグループ

背景

- 大量の迷惑メールとバックスキャッタ
- メールが届くのは幻想？
  - SMTPもbest effort
- 仕事に使えなくなるメール
  - ゴミに埋もれて見落とす
  - ゴミで細るネットワーク
- メールが必ず届くという思い込み
  - 重要な連絡は電子メール以外で！

spam対策の基本

- spamに対するポリシーの明確化
  - メール運用の方針の議論と確立
  - 対策手段はポリシー決定後
  - ポリシーと手段をごっちゃに議論しない！
- システム運用者が苦情に埋もれないこと
  - false positive問題
  - アプライアンスによる運用（責任の移転）
  - アウトソース

spam対策ポリシー(1)

- 社会的責任
  - spam受け入れはspamを助長する行為？
    - spam受信者がいなくなればspamはなくなる？
  - spamの発信源とならないこと。
    - 組織の社会的信用の失墜

spam対策ポリシー(2)

- 対策しない場合のコスト
  - ハードウェア・ソフトウェア資源
    - 対策をしないとサーバ等に過大な投資が必要
  - 人的資源の無駄（spamメール削除等）
- 対策する場合のコスト要因
  - 機器等への投資や人的投資コスト
  - false positive問題
- 現場に責任を押し付けない方針が必要

spam対策の基本選択肢

- 対策をとらない
- 自前で実現
  - ソフトウェア実装で実現
    - 現場の負担と金銭コストのトレードオフ
  - アプライアンスの導入
    - ユーザごとにオプションが選べるものがいい
- メールサービスを外部委託
  - 機密漏洩の不安

発信者確認とspam発信防止

- 発信者の身元証明
  - SPFやDKIM
    - 証明書は取得容易
  - SMTP-AUTH
- 送受信のポート制限
  - OP25B+Submission port
  - IP25B
    - 動的割り当てアドレスからの発信拒否

バックスキャッタ対策

- メールアドレスのガバナンス
  - メールアドレスをすべて把握
  - 学生証等のIC化やポータル導入がチャンス
  - 受け取ってからuser unknownは問題
    - バックスキャッタ
- 受信拒否？　受け取ってゴミ箱行き？
  - アドレスのハーベスティング防止
  - ただし、トラフィックは減らせない

メールアドレスの管理

- アドレスの一元管理
  - メールアドレスのLDAP認証
    - 認証サーバに多大の負荷？
  - 受信サーバの一元化
    - ポータルで一括（メールサーバは1台）
    - 中継サーバで管理
      - DB,LDAP等との連携
      - サブドメイン連携（受信前のアドレス存在確認）
        - » VRFYやLMTP(例　舛田、落合:FIT2007 LL-003)

受信側対策

- ●ホワイトリスト・ブラックリスト
- ●コンテンツフィルタ
- ●実装の差異を利用した判定
- ●遅延・流量制限
- ●経験則による判定

ホワイトリスト・ブラックリスト

- 送信者・送信元に○×をつける
  - 仕組み自体は単純でわかりやすい
- 問題点
  - 送信者詐称・ヘッダ改ざんに弱い
    - →発信者確認の必要性
  - 手動ではリストの管理が煩雑
  - 公開 Realtime Black List (RBL) の利用
    - DNSクエリを利用したサービスが一般的
      - 多くのMTAで設定が容易に可能
    - リストの信頼性に疑問
      - spamhaus.org と ISP の対立など

コンテンツフィルタ

- メールヘッダ・本文の内容で判断
  - NGキーワードによる単純なフィルタ
  - 単語の生起確率による学習型フィルタ
    - ベイジアンフィルタ
  - URIBL（spam本文に含まれるURIのリスト）
  - 利用者の報告に基づく公開データベース
- 問題点
  - spamかどうかの判断が100%信頼できない
    - 誤判定によるメール紛失問題
  - 画像spamなどの回避策が増加

コンテンツフィルタ/実装

- Spamassassin : http://spamassassin.apache.org/
  - キーワード・学習フィルタ・公開データベース等多数の手法からspamらしさを点数で判定
- Bogofilter : http://bogofilter.sourceforge.net/
  - ベイジアンフィルタ実装
- Bsfilter : http://bsfilter.org/
  - Ruby によるベイジアンフィルタ実装（日本語対応）
- Vipul's Razor : http://razor.sourceforge.net/
  - 公開データベース
- その他多数ある

実装の差異を利用した判定

- spam送信ソフトウェアと通常のMTAとの実装の差異を利用
  - 再送処理
  - MXレコード処理
  - その他のプロトコル違反
- 実装が甘い正当なサーバをはじく恐れ
  - ホワイトリストの管理が必要

再送処理

- 仮定: spam送信ソフトウェアは再送しない
- 初接続のMTAには一旦tempfailを応答
  - 「一時的な障害なので後で再送せよ」
- 再送してきたら受け取り、ホワイトリストに登録する
  - IPアドレスによるもの、エンベロープも利用するものなどいくつかバリエーションがある
- 単純だが効果は大きい
- 問題点
  - 再送が起こると配送遅延がかなり大きい
  - 適切に再送しない既知の実装・サービスがある
  - 適切に再送するspam実装が存在する

再送処理/実装

- greylisting: http://www.greylisting.org/
  - ポータルサイト
  - 各種MTAの実装がまとめられている
- 「お馴染さん」方式:
  http://moin.qmail.jp/_a4_aa_c6_eb_c0_f7_a4_b5_a4_f3_ca_fd_bc_b0
  - 初接続ホストは遅延通信後tempfailする
- S25R: http://www.gabacho-net.jp/anti-spam/
  - 逆引きしたホスト名を経験則で分類しtempfail 対象とする
  - Starpit・Rgrey・taRgrey等のバリエーションがある

MXレコード処理

- MXレコードの優先順位処理の差異を利用
- ダミーMX・SMTPリセット
  - 優先度最高のMXでメールを受け取らない
  - 通常は次のMXへ即時再送する
  - MXを正しく処理しないspam送信ソフトは次のMXに再送できない

MXレコード処理/実装

- MXフォールバック判定:
  http://moin.qmail.jp/MX_20fallback_20_c8_bd_c4_ea
  - 最優先MXでは接続を受け付けず、接続履歴だけ取る
  - 次のMXでは最優先MXに接続履歴があるホストからだけメールを受け取る
- Unlisting: http://unlisting.org/
  - MXフォールバック判定とほぼ同様
- Nolisting: http://nolisting.org/
  - 接続履歴の検証を省略したもの
- GION: http://www.reflection.co.jp/spam/
  - 次MXでtempfailや遅延応答・逆引きチェックも実施

受信側対策

その他のプロトコル違反

- greet pause
  - sendmail 8.13 の設定項目名に由来
  - 接続時の最初の応答（greeting）を一定時間遅らせる
    - 正しい実装はgreetingを待つ
    - 待たずにメールを流し込むspammerを拒否
- プロトコルの検査
  - HELOの形式チェック
  - EHLOからHELOへのフォールバック

受信側対策

遅延・流量制限

- spammerからの通信を遅延させたり流量を絞る
  - 時間当たりの総送信量を減らす
  - 他の判定方法でspammerと判定されたホストに対して実行
  - spamの流量を減らし下流のサーバ負荷低減
  - spammerの作業効率を低下
- tarpitting・トラフィックシェーパ等

受信側対策

遅延・流量制限/実装

- OpenBSD spamd: http://www.openbsd.org/spamd/
  - 遅延通信とgreylisting機能
  - pf（OpenBSD/FreeeBSD のパケットフィルタ）と組み合わせて使用
- Symantec Mail Security 8100 シリーズ: http://www.symantec.com/ja/jp/enterprise/products/overview.jsp?pcid=1011&pvid=852_1
  - メールの通過パスを元にspam判定
  - spamは流量制限（最大50%減）

受信側対策

経験則による判定

- 逆引きのできないサーバを拒否・制限
- 逆引きしたホスト名が特定のルールに合致するものを拒否・制限
  - 動的アドレスらしいものを判定など
- 問題点
  - 経験則なので必ず例外がある

受信側対策

アプライアンス・ソリューション

- 個々の対策には異なる特徴がある
  - それぞれの利点と欠点
- 現場の管理者が組織のサーバに対し自力で対策した場合、欠点や設定ミスによるメール紛失等の責任問題が発生する
- 既存の製品を導入することでこれを回避する方が得策かもしれない
  - 採用している技術が異なる
  - 可能なら複数の製品を試用して比較するべき
  - コストとの兼ね合い

受信側対策

代表的な製品（網羅的でない）

- Barracuda SPAM Firewall
  - http://www.barracudanetworks.com/ns/index.php?L=jp
- IronPort Mail Security Appliance
  - http://www.ironport.com/jp/
- McAfee SpamKiller for WebShield
  - http://www.mcafee.com/japan/products/mcafee/spamkiller_ws.asp
- Symantec Mail Security 8200
  - http://www.symantec.com/ja/jp/enterprise/products/overview.jsp?pcid=1008&pvid=849_1
- Trend Micro Spam Prevention Solution
  - http://jp.trendmicro.com/jp/products/enterprise/sps/index.html

送信側対策

- OP25B(Outbound Port 25 Blocking)
  - Bot(ゾンビ)等からのspam送信をブロックする
- 送信者メールアドレスの詐称防止
  - 送信ユーザの認証
    - SMTP AUTH
  - ドメイン認証
    - SPF (Sender Policy Framework)
    - DKIM (DomainKeys Identified Mail)

OP25BとSMTP AUTH(1)

- Outbound port 25 blocking
- 受信側での対策はたいへん(法的・技術的)
- 送信側のルータで止めることが効果的
- 「spamを送らない」
  - Bot(ゾンビ)や、無線LAN不正使用によるspam送信を止めることができる

OP25BとSMTP AUTH(2)

- 配送ポート(25)と投稿ポート(587)との分離
- 投稿ポートでは、smtp authによるユーザ認証
- 利用者には、ユーザ認証が必要な投稿ポート(587)のみを提供する
- 配送ポート(25)は、投稿目的での利用は不可
- 現実的には、
  - 同一ドメイン内: 配送ポートでの投稿もOK
  - ドメイン外から: 投稿ポートからのみ受け付ける

OP25BとSMTP AUTH(3)

- MTA(Mail Transfer Agent)のみが配送ポートを使って外部へメールを配送する
- 一般端末から配送ポート(25)で、直接外部へのメール配送は禁止
- レート制御
  - 同一送信者、同一IPから

レート制御

- 同一送信者、同一IPから短時間に大量のメール(spam)が送られることを禁止する
- OP25Bにより配送サーバを限定することで、そのサーバの中で対応できる。

SPF

- POBOX.COMが提唱
- 送信サーバをDNSに登録

  [例] - example.jp IN TXT “v=spf1 +ip4:10.1.2.3 –all”
  - example.jp IN TXT “v=spf1 +mx ~all”
  - 「+」pass, 「?」neutral, 「~」softfail, 「-」fail
  - 「ip4:」ipv4アドレス, 「mx」mxレコード
- 受信側
  - SMTPコネクションから送信元MTAのIPアドレスを得る
  - 送信者メールアドレスを取り出す(envelope from:)
  - そのドメイン部をDNSで検索し、SPFレコードを得る
  - 送信元MTAのIPアドレスとSPFレコードを比較する

送信側対策

DKIM

- YahooとCiscoが提唱
- 送信者は、公開鍵をDNSに登録
  - 認証局(CA)は不要
- 秘密鍵を使ってメールに署名
  - 署名はヘッダに挿入される
- 受信側
  - メールを受信する
  - 送信元アドレスを取り出す
  - そのドメイン部からDNSを検索し公開鍵を得る
  - 公開鍵を使って署名を検証する

送信側対策

メールの転送

- SPF
  - 送信MTAが変わるので認証に失敗する
- DKIM
  - 送信MTAのIPアドレスに依存しないので問題なし

送信側対策

メーリングリスト

- SPF
  - MLサーバにSPFのための機能追加をする必要なし
- DKIM
  - メールの書き換え等のため、署名を作り直す必要あり（MLサーバに機能追加）

送信側対策

SenderID

- SPF＋CallerID(Microsoft)
- DNSへ登録するSPFレコードは、共通
- 送信元アドレスとしてエンベロープFROMではなく、ヘッダ中からPRA(purported responsible address)を抽出し、用いる。

3.3. デジタルフォレンジック

3.3. 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。この言葉が重要になって来た背景には最近の ICT 技術の進化とインターネット利用の目覚しい発展によって犯罪そのものが主として PC やサーバ等のコンピュータを介して行われるようになって来たためです。それで犯罪捜査においても ICT 技術を駆使して、その捜査能力の向上が必要と言えます。また情報内部統制や 2007 年 9 月 30 日までに完全施行された JSOX の存在もそれに大きく関連しています。

例えば、Web アクセスや E-mail のやり取りそのものが捜査対象になるということです。それらのやり取り、すなわち通信内容などを追跡するためには、サーバや PC 等の情報機器のログやシステムの状態が記録されたメディアを詳細に調査解析を行う技術が必要となります。大学が関係している事例としては、ネットワークストーカーの犯罪捜査への協力としてメール送信元に関するログを提出依頼されたケースや大学内のフィッシングサイトによって被害が発生したため Web サーバのログを提出し犯罪捜査へ協力、個人情報漏洩時のアクセスログの提出等が事例としてあがっています。

さてデジタルフォレンジックにスムーズに対応するためには、Web や E-mail などのメジャーな通信内容はすべてある一定期間保存するということになります。膨大なメールや Web アクセスを記録するとなるとそれなり資源が必要となります。例えば米国の企業においては、上記の E-mail などの保全収集とそのデータベース化「電子情報開示(e-Discovery)」に関連する規則が、2006 年 12 月 1 日に連邦民事訴訟規則（Fed. Ro Civil Proc.）発効したため、大きな負担となりつつあります。

大学でも恐らく例外なく、同様の事情が発生するかも知れません。あまり喜ばしくないシナリオとして、情報セキュリティに関する事件（セキュリティインシデント）が発生すれば、ICT 部門と総務部門などがその対応（証拠保全・解析・報告）を引き受けざるを得ない状況が発生し、そのような場合ログの部分提出が必要である、ということがありえそうです。しかしそれは、膨大なデータ処理や多様な文字コードへの対応が必要となります。たとえ 1 件でも大変なのに、同時多発的事態となれば恐らくほとんど対応できないと考えられます。

なにはともあれデジタルフォレンジックに対応するためには、情報機器の追跡可能性（トレーサビリティ）を維持しなければなりません。そうすると機関におけるログの保全は必須であり、その期間は判例から 3 年程度と言われています。またログの完全性(Integrity)をなんらかの形で維持する必要があります。例えばログの分散バックアップ保存などが挙げられます。また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し、ログ収集サーバへログを集中保全管理させます。ログエージェントシステムが導入できない場合は、NIDS などのパケット収集に基づいたセキュリティアプライアンスの導入が考えられます。そして大量のストレージが必要です。

ログの保全技術としては、時系列データであるため時間認証局を使って時間の正当性を確保し、更にログは個人に関する情報やプライバシーを含むため機密性の高い情報資産と考えられるので、保存時に暗号化する必要があります。また既存のサーバや PC などの情報機器のログの完全性の保持も必要です。大学の ICT 部門では、組織全体のシスログ受信サービスも必要かと思われます。いずれにしても膨大なストレージを必要とするものと考えられます。

最後にセキュリティマネージメントの観点から、アウトソーシング化も選択肢の一つかも知れません。デジタルフォレンジックに耐えうるためには、外部評価の視点から大学でそのシステムを持たず、または大学のインフラ的施設の一部として考え、予算と人員を配置して施設部や設備課などにまかせる、ログデータの保全をアウトソーシング化する、解析のアウトソーシング化を念頭におきこれからの ICT 化や設備増強を施すことを考えなければいけません。セキュリティベンダーもアウトソーシングを受け入れる体制を確立すること、新しいビジネスモデルへの転換の必要に迫られていると思われます。

デジタルフォレンジック

武蔵(熊本大)*、湯浅(高エネ研)、
山田(富士通)、須永(富士通SSL)
*リーダー

SS研セキュリティマネージメントWG
フォレンジック・グループ

背景

- 個人情報漏洩
- 情報内部統制
- ソフトウェアライセンス管理
- ECサイトの事例
- 警察捜査等への協力(ログ提出)

定義: フォレンジック(法科学)

- フォレンジック(Forensics: 法科学)
- メディカルフォレンジック(法医学)
- デジタル鑑識:ICTを利用した鑑識
- デジタルフォレンジック:
  - コンピュータフォレンジック
  - ネットワークフォレンジック

デジタルフォレンジックとは何か

- 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
- サーバ等の情報機器のログやシステムの状態が記録されたメディアについて詳細に調査解析を行う手法および技術を含む

刑事(民事)事件で警察へのログ提出の具体例

- A大学でネットワークストーカの犯罪捜査としてメールサーバのシステムログを提出
- B大学でたてられたフィッシングサイトに関連して被害が発生、Webサーバのログを提出し捜査に協力
- テロ予告など犯罪性の強い書き込みに関する警察への捜査協力
- 個人情報漏洩時のアクセスログ

e-Discovery

- e-ディスカバリとは:電磁的な証拠開示
- セキュリティインシデントに関連する訴訟では、IT部門と総務部門がその対応を引き受けざるを得ない
- そんな場合でも、ログをすべて提出する必要はなく、必要な範囲を適切に提出すればよいが、
  - 必要な三要素:証拠保存、解析、報告
  - 課題: 膨大なデータの取り扱い、多様な文字コードへの対応
- 多くの機関では、経験がなく急な事態に適切に対応できる体制になっていない

情報機器のトレーサビリティ

- ログの保全は必須である
  - 期間は？
    - 判例では3年がある
  - 完全性はどう保護するか
    - ログの分散バックアップ保存
- 収集の方法の一例
  - PCログエージェントとログ収集サーバ
  - メールサーバアプライアンスのログのフォレンジック解析

パケットキャプチャリングの技術

- ネットワークタップ（UTPタップ、ファイバタップ）やミラーポートの利用
- libpcapライブラリを利用したパケットダンプ
  - tcpdump
  - snort
    - https://www.ssken.gr.jp/lib/nl/2004/stg/2/3_watanabePPT.pdf
- フルロギングあるいはヘッダロギング(フロー)
- ターゲットロギング(ARGUS)
  - http://www.qosient.com/argus/index.htm
  - http://www.hawkeye.ac/micky/SA/AuditTrail.files/frame.htm
- 課題
  - 大量のストレージが必要
  - 雇用契約との整合性

ログの保全技術

- 時間認証局の採用？
- 暗号化
- ログデータのハッシュ化
- サーバサイドの完全性の保持
- ユーザクライアント側の完全性の保持
- 組織ワイドのシスログ受信サービスの必要性
- UDP/TCP通信で十分か、あるいはSSL化が必要か

フォレンジックで使われる技術

- キャプチャリングツール
  Gigabitネットワークでの確実な保存への期待
- ネットワーク
  メール(SMTP)アーカイバ
  Web(HTTP)アーカイバ
  KVMやRDP,VNC経由でのPC操作画面保全
- サーバ(改ざんされないログ)
  アクセス権(特権)の分離：SecureOS
- クライアント
  画面キャプチャ
  キーロガー
- 調査、解析ツール
  ハードディスクのイメージファイルの作成(取得)
  取得ファイルからの調査、解析
  調査結果レポート

フォレンジック製品例

- キャプチャリングツール
  SwiftWing SIRIUS LCS
  GigaProve
- ネットワーク
  NetEvidence, MSIESER, Net Detector, PBH
  NetEnrich
- サーバ(改ざんされないログ)
  SHieldWARE
- クライアント
  ESS REC
- 調査、解析ツール
  EnCase

マネージメントの視点から

- アウトソーシング化
  - 大学でシステムを持たない
  - 施設部や設備課に委譲
  - ログデータの保存をアウトソーシング
  - 解析のアウトソーシング
    - アウトソーシング先の技術レベルが問題となる
- 将来、新しいビジネスモデルへと成長する可能性がある

参考文献・参考リンク

- 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)
- 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
- 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/

4. セキュリティマネージメントWGを終えて

4. セキュリティマネージメント WG 活動を終えて

（WG メンバーからのコメント）

私が、情報セキュリティ関連のテーマで SS 研究会の WG 活動に参加させていただくのは今回で 2 度目になります。前回はメンバーの一員としての活動でしたが、今回はまとめ役をとのお話をいただき、最後までやり遂げられるのか不安でした。しかし、実際に活動のふたを開けてみると、準備会から話が沸き、どの会合においても時間が足りないと感じるほど活気のある活動となりました。つまりこれは、「情報セキュリティマネージメントが、現場の研究者や技術者にとって、いま正に必要なものである」ということを意味しているのではないでしょうか。2 年間にわたりそんな気持ちを持ち続けられたことや WG メンバーのなかからわきでる発想や知見を共有できたことは私にとって大きな収穫でした。

最初から最後まで SS 研究会事務局の諸氏に活動を支えていただきました。ありがとうございました。最後になりましたが、セキュリティ・アンケートにご協力くださった機関の皆様に深く御礼申し上げます。

（湯浅富久子）

WGメンバーとの議論の中で現在のセキュリティ状況を再認識しました。

昨年くらいから、TCP/IPプロトコルやDNSプロトコル等のインターネットの根幹に関わる問題点の発覚と、それらに対する攻撃が続出しています。そんな中、どのような活動が次に必要か考えています。

（長谷川明生）

私のSS研究会におけるセキュリティに関連する活動としては、以前に講演会などでの発表はありましたが、WG活動はこれが初めてになります。普段学内のセキュリティ対策に追われて内側ばかり見ている事もあり、今回の活動を通してWGメンバーとさまざまな側面からセキュリティ問題について議論できたことは大変よい経験になりました。セキュリティ・アンケートについては、報告をまとめるにあたり自分達の知識と経験では不十分そうだと感じてのアイデアでしたが、微妙な質問にもかかわらず望外の御協力により興味深い情報が得られました。

御協力いただいた機関の皆様に深く御礼申し上げます。

（笠原義晃）

SS 研 セキュリティマネージメント WG (2007/2-2009/2) 成果報告書

【発行】 サイエンティフィック・システム研究会

【編集/著者】 セキュリティマネージメント WG

＜連絡先＞サイエンティフィック・システム研究会（SS 研） 事務局
〒105-7123 東京都港区東新橋 1-5-2 汐留シティセンター
富士通株式会社 カスタマーリレーション部内
TEL：03-6252-2582 FAX：03-6252-2934
Email：ssken@ssken.gr.jp
Web：http://www.ssken.gr.jp/MAINSITE/index.html

2009 年 1 月 20 日作成