中部・東海 情報セキュリティ研修

稲石 守男
名古屋大学工学研究科技術部

はじめに

近年のインターネットの進歩には目ざましいものがあり”現代社会はコンピューターのネットワークを基礎として築かれている”と言っても過言ではない。現在文部科学省・産学官連携研究プロジェクト NAREGI（超高速コンピューター網形成プロジェクト）等も企画されつつある。このような高度情報化への趨勢に伴って情報関連のセキュリティ侵害事件も増加する傾向にある。このような情勢を踏まえて平成１５年８月２９日にＳＣＳを介した「文部科学省主催：情報セキュリティセミナー」が開催された。また更に同年１２月９日、国立情報学研究所の主催により名古屋大学シンポジオンホールにおいて「中部・東海情報セキュリティ講座」が開催された。それらのセミナーに於ける情報セキュリティについて概説する。

１．情報セキュリティポリシー [1)]

1) 一般論的情報セキュリティ

一 般にコンピューターのセキュリティについて考えるならばネットワーク全体が個々のサイトとネットワークから構成されており、コンピューターセキュリティの問題は個々のサイトの中に保存されている情報セキュリティの問題点とネットワーク自体の問題点があると考えられる。この２つについて「機密性」「正確性」「可用性」の３つの目標を要素として捉える事にポイントがある。このセキュリティに対する脅威として外部からのアタック（いわばハッカー等）だけではなく、内部からのアタックについても十分な対応をしなければならない。またネットワークにおけるセキュリティ上の問題点としては「通信傍受」「秘密性の侵害」「正確性の侵害」「使用不能攻撃」「なりすまし」「ハッキング」「コードの正確性の侵害」等が挙げられる。以上のような脅威に対してセキュリティ保護上の観点からハード面と共にソフト面での防衛策（セキュリティポリシーの構築、各セキュリティ強化的プログラムの実装、就業規則の見直し、ガイドラインの設定、法的な対応）を採らなければならない。

2) 大学における情報セキュリティポリシーの必要性

高度情報化社会において大学が学術研究・教育活動を高めようとする為には情報基盤の整備に加えて大学の情報資産のセキュリティを確保する事が不可欠である。このような方針に沿って大学の情報資産をあらゆる脅威から守る為以下のような事項を内容とする情報セキュリティポリシーを策定する事が望ましい。

* 電子・情報技術系

a) 大学の情報セキュリティに対する侵害を阻止する。
b) 学内外の情報セキュリティを損ねる加害行為を抑止する。
c) 情報資産に関して重要度に見合った管理を行う。
d) 情報セキュリティに関する情報の取得を支援する。

また情報セキュリティポリシーが対象とする範囲（人、物）は例えば以下のようなものである。

e) 学内ネットワーク及び情報機器に触れる事が可能な総ての人。例えば教職員、臨時員、非常勤職員、学生、研究生、留学生、社会人学生、聴講生、委託業者、来学者
f) 学内ネットワークに一時的にでも接続される総ての情報機器、学生が持ち込む情報機器や大学内で開催される学会等への参加者が持ち込む情報機器を含む。ここで学内ネットワークとはその大学のネットワークアドレスを持つ総てのネットワーク、バリアセグメントを経由しないで接続している総てのネットワークを指す。
g) 情報資産（研究論文、各種研究用データ、成績、人事情報等）

3) 情報セキュリティポリシーとは(1) 情報セキュリティ基本方針、(2) 情報セキュリティマニュアル (3) 情報セキュリティ対策基準から構成される。また情報セキュリティポリシー策定の流れは概ね以下のようである。

a) 適用範囲を決定する。
b) 基本方針を策定する。
c) リスクアセスメントの体系的な取り組み方法を策定する。
d) リスクアセスメント（リスク評価）を行う。
e) リスク対応を行う。
f) 管理目的と管理策を選択する。
g) 実施手順書を作成する。

2．大学における情報セキュリティと法的話題 [2)]

1) セキュリティポリシーの策定

大学内における対応の整備（大学内の規定整備、利用規定や学則その他の対応）

2) 大学におけるセキュリティの問題点（具体的な問題点と特徴について）

大学等においては以下のような問題点が存在する。

a) 経営層の理解の無い事による困難な面が存在する。
b) 大学における個性の強さ－対外接続担当部局（電子計算機センター等）の存在、学部等の独立性の存在。
c) キャンパスも分散している場合が多くネットワークの物理的存在等に問題点が存在する場合が多い。
d) 関係者の多様さ：教授、助教授、講師、大学院生、学生、技術職員、事務職員等大学の構成員に見られる多様性が存在する。
e) 情報資産の多様性：情報資産に関与する人間が多様であると同様にネットワークに関与する情報も多種多様である。例えば試験問題、研究情報、人事情報等情報資産にお

いて多様性が見られる。

3) セキュリティと法律上の問題

「営業秘密」について言えば「秘密として管理されている生産方式、販売方式その他の事業活動に有用な技術上または営業上の情報であって公然と知られていないものを言う」と定義されている（不正競争防止法 2 条 4 項）。この「秘密として管理されている」と言う要件については a）その秘密にアクセスできる人間が限定されている事。b）その秘密にアクセスする為に何等かの特別な手続きが必要である事。c）秘密にアクセスした者に当該秘密が営業秘密であると認識出来るようにしてある事」等によって認定がされる事になる。この「営業秘密」へのアクセスに関しては不正競争防止法の改正により刑事罰が課されるようになった。具体的には (1) 詐欺等行為又は管理侵害行為による媒体等の取得、複製の作成による取得行為 (2) 詐欺等行為、管理侵害行為、横領または背任行為により媒体の領得、作成による取得行為 (3) 取得した営業秘密を不正の競争の目的で使用し、または開示する行為について親告罪でありながらも３年以下の懲役、または 300 万円以下の罰金に処せられる事となっている。

4) 個人情報の保護

各個人の生年月日、住居、信条、趣味、嗜好等の個別のデータについて、これ等のデータの関連する個人をデータ主体と言えばデータ主体のデータについての利益はネットワークの爆発的な発展に伴って新らたな局面を迎えている。そのような状況の中で度重なる個人情報流出事件、またＥＵにおけるデータ保護の指令、そしてそれに対応する各国の動き等の見地から具体的な個人データ保護の法体系の整備が要求され迂余曲折を経て個人情報保護法が平成１５年５月に成立した。また関連する法律としては「行政機関の保有する個人情報の保護に関する法律案」「独立行政法人等の保有する個人情報の保護に関する法律案」等も同時期に成立している。大学については今後、独立行政法人化に伴ってかかる独立行政法人個人情報保護法の適用範囲になる可能性がある。一方、私立大学においては一般の個人情報保護法における個人情報取り扱い事業者（同法 15 条）に該当する可能性がある。その場合には具体的に (1) 利用目的の特定、利用目的による制限（15 、16 条）、(2) 適正な取得、取得に際しての利用目的の通知等（17、18 条）(3) データ内容の正確性の確保（19 条）安全管理措置、従業者・委託先の監（20 条～22 条）(5) 第三者提供の制限（23 条）(6) 公表、開示、訂正、利用停止等（24 条～27 条）(7) 苦情の処理（31 条）(8) 主務大臣の関与（32 条～35 条）主務大臣（36 条）等の規定が準備されている。最も「大学その他の学術研究を目的とする機関もしくは団体またはそれ等に属する者」が「学術研究の用に供する目的」で収集する個人情報については適用除外になっており、かかる目的の解釈とも関連して適用関係については今後も留意が必要である。

5) 不正アクセス、ウィルス製造罪

データのセキュリティに対する侵害を考える時に、そのシステムについて権限がないのにアクセスをなす事や個々のデータ等を書き換える事は極めてインテグリティの侵害の度合いが高いものと言う事が出来る。我が国ではそのようなインテグリティの高い侵害をそれ自体法益と捉えている訳ではないが無権限アクセスについては「不正アクセス禁止法」で禁止がなされている。この「不正アクセス禁止法」はセキュリティホールを

突いたり他人名義の ID/password を用いてアクセスを行ったりする事を刑事罰をもって禁じている。また現時点で法制審議会を経て国会に提案される予定であるのがウィルス製造罪である。これは「人の電子計算機における実行の用に供する目的で人の使用する計算機についてその意図に沿うべき動作をさせずに又はその意図に反する動作をさせる不正な指令に関わる電磁的記録その他の記録を作成し、又は提供した」行為を処罰しようとしするものである。

6) セキュリティの遵守義務違反の法的責任

これは自己のセキュリティを十分に保持していない場合にそれが原因で何等かの形で攻撃者の利用の「踏み台」にされた場合に被害者に対する損害賠償の責めに任じられるのではないかと言う問題である。管理者自体がシステムのセキュリティホールに対してアップデートをしていない場合には、それが原因で何等かの損害が発生すると言う事も考えられる。これ等の場合の法的責任については尚、現時点では未知数と言う事ができるが今後更にセキュリティホールに対する攻撃に対する対応の必要性と言う論点の重要性は高まるものと考えられる。

3．セキュリティプログラム

1) ネットワークのセキュリティに対する脅威に対応する為の対応策を考える時にそれをセキュリティプログラムと言う事ができる。そのセキュリティプログラムを構築する事が重要である。このセキュリティプログラムはリスク分析、プログラム・プランニング及び発展（実装及び監査）の段階を踏む事になる。

2) リスク分析

リスク分析の場合には

a) データの変造及び窃盗
b) データ破壊
c) データ正確性の喪失
d) システム乃至はネットワーク正確性の喪失
e) システム乃至はネットワークアクセスの喪失
f) 信用の喪失

等のリスクがある事が考察される。またこれ等のリスクは従来の情報漏洩と対比して考察されるべき事が説かれている。そしてこれ等のリスクを種々のアプローチを用いて評価して行くのである。

3) プログラム・プランニング

具体的なプログラムの策定に当たっては具体的なインフラストラクチャを定めて行くモジュールの決定が出され、それと同時にポリシーと手続きの発展、技術的なソリューションの選択、ユーザーの意識の向上がなされる。このインフラストラクチャを定める部分においてはインターオペラビリティ、異なるプロトコルの利用、異なるプラットフォームの利用等についての考察がなされる事になる。これ等のポリシーは「柔軟さ」「目標適合性」「適用可能性」「実装性」「適時さ」「コストパフォーマンス」「執行性」「統一性」を持たなければならない。そしてこのポリシーは構造上、経営陣が出さ

なければならないと言われる。

４．具体的なプログラムと法的な問題点

1) 大学における具体的なセキュリティ運用プログラムをカリフォルニア大学バークレー校を例に取って比較して見る。

2) インフラストラクチャの基礎

ＵＣＢのネットワーク運用は「私達は新しいＷｅｂの技術がキャンパス生活の質を改善する事が出来ると信じている。この理由から e-Berkeley は私たちの素振らしいＷｅｂの専門家を集めて総ての活動をよりスムーズにし共有社会を育むこととしている」と言う信念によるものであり、そのビジョン及びゴール（目的）ポリシーその他については以下のように述べられている。

a) ビジョン・ゴール

I．（e-Berkeley Vision）：大学をテクノロジー指向の学習、発見、従事によって変身させる事。

II．目的（e-Berkeley Goals）：学生、学部、スタッフ、同窓生の為に書類を出来る限りインターネットで利用出来るようにして摩擦なしにする事。技術を統合された共同体を通じて人間の総合作用を豊かにする事。

b) ポリシー

具体的には後述するが IT アーキテクチャー、IT 取得、IT セキュリティ、IT ポリシーの観点について触れられていると言う事が出来る。

c) 教育・トレーニング

具体的な教育やトレーニングを担当するのは他の機関、具体的には IST と言う事になる。この点についてはむしろ後述のシステムの点から触れた方が合理的に思われる。

d) システム

I．最高責任者としてのＣＩＯ（Campus Information Officer）：具体的にどのようなシステム（人員）で運営されているかと言う点についてはＣＩＯが存在し、そのＣＩＯは教育、研究、管理について責任を有するものとされており、具体的には (1) IT Vision 及びプランニング (2) IT ガバナンス (3) IT アーキテクチャ (4) IT 取得 (5) IT セキュリティ (6) ポリシーの各分野に対して責任を有するとされている。

II．具体的な運用担当者： (1)運用部門：これらの具体的な運営については e-Berkeley Steering Committee が実際の権限を有している。そして具体的なキャンパスにおける IT アーキテクチャの検討については ITAC が担当し、技術をデザインし、購入する際のメレームワークを設定している。 ITAC は情報の交換所として活動し、そしてキャンパス規模の標準とアーキテクチャとをコーディネートする為の中央ポイントとなっている。

e) 技術サポート部門：具体的な技術サポート部門を担当する言わば中央技術組織とでも言うべきものとして IST が準備されている。IST は情報インフラストラクチャの創設の中では３つの技術的戦略を担当する事になる。その３つとは (1) リーダーシッ

プを提供する事。(2) 情報技術インフラストラクチャを構築する事。 (3) 情報技術テクニカルサポートを拡張する事である。

f) 運用の具体的展開

I. 具体的な運用はビジョンやプランから個別のプログラムに展開される過程として把握されるものと考えられる。

II. 具体的な展開

インフラを考えた時に個別具体的な観点に展開されて行く事になる。ＵＣＢにおいてはそれが IT セキュリティ、IT ポリシーの２つの観点において展開されていると言う事が出来るであろう。キャンパスにおける IT セキュリティを担当する責任者は The Campus Information System Security Officer (CISSO) であり、このＣＩＳＳＯは直接ＣＩＯに報告し Campus System and Network Security (SNS) オフィスを運営する。ＳＮＳはポリシーの運営、コントロール、セキュアでしかもオープンなネットワークを提供する為の手続きに責任を持っている。Campus Information Security Committee (CISC) は e-Berkeley Steering Committee の常任委員会である。またセキュリティ事件の報告先として security@berkeley.edu が指定されている。このような見地から IT セキュリティに関するガイドライン（指針）及びポリシーが決定されている。これ等のガイドラインとしてはネットワークアクセスの防止のガイドライン及び手続き部門的なコンタクトのポリシー、電子情報セキュリティ、情報システムの危機管理及び回復プラン等がある。

III. IT ポリシーはミスユースの報告についてのポリシー、キャンパスにおける使用のポリシー、部門におけるポリシー群によって構成されている。ここで特に注目されるのはキャンパスにおける使用のポリシーである。これ等は更に個々のポリシーであるキャンパス・コンピューター使用ポリシー（Campus Computer Use Policy ）、カリフォルニア大学 UCElectronic Communications Policy、中間ポリシー等に展開されている。

５．ポリシー群と法律上の問題点

1) 種々の問題についてガイドラインで定めておく必要がある。ガイドラインにおいて位置付けられていなければならないと思われる法的な意味を持つ項目としては以下の事項がある。

a)「権利と責任」

ネットワークへのアクセスは特権でもあり個人の利用は責任を持って行動することが必要とされている。ユーザーは他人の権利を尊重し、システムのインテグリティや関連する資源を尊敬し、関連する総ての法律、規則、契約上の義務を遵守しなければならない。一方コンピューターのファイルにおける自己の情報については学生及び被傭者はアクセスする権利を有する。裁判所命令の下でファイルが探索される。更にシステム管理者はコンピューターシステムのインテグリティを保持する為にファイルにアクセス出来る。

b)「適用される法規等と許容されない行為の例示」

コンピューターに関するものに限らず個人的行動について一般的に適用される法律・規則総て適用される事が明らかにされている。そしてコンピューティングのミスユースに対しては利用の制限がなされている。制定法の下で訴追がなされる可能性がある。

c) ミスユースの例

ミスユースの例としては以下のものが挙げられる。無制限アクセス、無制限アクセスを得る為のキャンパスネットワークの利用、一般の妨害行為の遂行、システム乃至はネットワークに対して損害乃至は過負荷を懸けるプログラムの実行、データ保護スキームを巻き込んだりセキュリティホールを暴露したりする事。ソフトウェアのライセンス条項を違反する事等である。

2)「適正な利用」

キャンパスのネットワーク利用の際には従来のコミュニティの適切で熟慮された行動コードが生き続いているのであり、利用者にかかる行動コードの遵守を期待する事が必要となる。

3)「執行もしくは制裁」

「執行」の項目の下で制裁について触れる。例えば前述のＵＣＢの例では大学の規則、キャンパスの規則、カリフォルニア州法、合衆国法に基づいて制裁が課せられる事が触れられている。具体的にはさ細なもの、乃至は偶発的なものであれば電子メール乃至は個人的な注意で非公式的に処理される。一方より深刻な侵害であれば正式な手続きを通じて処理され、調査がなされる間、特権を停止される事となる。

６．最近のウィルス事情と技術的解説 [3)]

1) ウィルスによる被害状況

近年のウィルスによる被害状況は２年間で被害件数が約４倍に増加している。

2) ウィルスの変化

現在 MX, CODERED, SIRCAM, NIMDA, Badtrans.b, MSBLAST.A と言ったウィルスが検出されている。またセキュリティホールを悪用したウィルスは全体の 2% 程度でありメール機能を悪用したウィルスは 78% に上っている。またマクロウィルスは 15% その他が 5% となっている。

3) 昨年８月に猛威を振るった MSBLAST.A はワームに分類されるトロイの木馬型不正プログラムでありMS-Windows のセキュリティホール（MS03-026）への攻撃を行っている。これはメール感染ではなく TFTP を利用している。感染すると自分自身が攻撃者に変身する。ウィルス駆除のパターンファイルだけでは防御出来ない等の性質を備えている。トレンドマイクロサポートセンターの調査によれば１日の感染では 200 件と過去最速の感染報告がなされている。MSBLAST.A は 2003 年 7 月17 日にマイクロソフトが公開したセキュリティホール［MS03-026］RPC インターフェースのバッファオーバーランによりコードが実行される。この問題により TCP/IP port 135, 139, 445, 593 を経由して応答する基本の DCOM インターフェースに影響が及び攻撃者は不正な RPC メッセージを送信する事によりコンピューター上の RPC サービスを異常終了させ任意のコードが実行

されるメカニズムとなっている。

4) MSBLAST.A が利用するポート

MSBLAST.A は Windows の RPC (Remote Procesure Call)を利用するポート 135 番をアタックする。一般的にはファイアウォールにより外部から 135 番ポートへのアクセスをブロックしても問題はないが各種 Windows のサービスに使用されており問題が発生する可能性が高いので注意が必要となる。

5) ウィルスの侵入経路

一般にはインターネットに直接接続した場合に感染する。前述以外の例では感染したノートＰＣ等を内部ネットワークに接続した場合、想定していない外部との接続ルートが利用されていたケース等により感染している。

6) 一般的なウィルス検知の仕組み

a) パターンマッチング方式

パターンマッチング方式では、ウィルス定義ファイルを用いてプログラム内に含まれる文字列やバイナリコードが既知のウィルスのパターンと同一かどうかを判断する。既知のウィルスであればほぼ確実に検知するがウィルス定義ファイルに登録されていないパターンは検知出来ない。従って常にウィルス定義ファイルを更新する必要がある。

b) チェックサム方式

感染していない状態の時に検索対象となる実行可能なプログラムやライブラリの情報をデータベース化しておき現在の状態と比較する事でウィルスを検知するのがチェックサム方式である。パッチを適用したりソフトウェアをアップデートするとファイルの状態が変化するのでデータベース更新の必要がある。

c) ルールベース方式

ウィルスの活動を分析してルール化するのがルールベース方式である。例えばシステム領域の書き換え及び実行ファイルやライブラリへの書き込み等一般的な操作では発生しない挙動を監視しルールと合致する動作を行ったプログラムをウィルスと判断する方式である。

7) ウィルスを防御する場所

現在はウィルスの感染経路がネットワークに移行し電子メールがターゲットとされている。その為、メール受信時にウィルスチェックを行えば感染する確率は低くなる。従ってゲートウェイ、ファイアーウォールにウィルス対策ソフトウェアを導入するのが効果的である。

参考資料

1) 文部科学省主催：ＳＣＳによる情報セキュリティセミナー：インターナショナル・ネットワークセキュリティ（株）石井宏幸「ポリシー策定の流れとリスク分析」
2) 平成１５年１２月９日「情報学研究所による情報セキュリティセミナー」資料
3) トレンドマイクロ株式会社提供資料