日本セキュリティ・マネジメント学会
第１６回全国大会 発表要旨

技術者･管理者向け情報セキュリティ教育試案

内田 勝也 （中央大学 研究開発機構）
Katsuya Uchida uchidak@gol.com

情報システムやネットワークは、社会におけるインフラとして重要な役割を果たすようになってきた。このため、情報システムやネットワークが何らかの原因で運用が停止したり、情報の改竄、漏洩等の発生が社会問題化し、企業・組織に対して大きな影響を及ぼすようになってきた。

このような状況への対応を総合的に考える情報セキュリティに大きな関心が高まってきたが、物理的側面での情報セキュリティは比較的古い時代から検討・対応が行われてきたが、インターネット等を中心としたネットワーク・セキュリティは、新しい分野であり、また進歩が激しいため、この分野の専門家の不足が指摘されており、専門家の育成が喫緊の課題になっている。

ここでは、ネットワーク・セキュリティを中心とした技術者・管理者の情報セキュリティ教育を考察した。

1. はじめに

現状の情報システムでは、「利用者」、「システム提供者」に分けて考える必要があり、それぞれの立場で情報セキュリティ教育を考えることが必要であるが、ここでは、システム提供者側の情報セキュリティ教育について考察する。

システム提供側は、更に技術、管理･運用の2つの側面から考えてみたい。情報システムの進展と共に、情報セキュリティ分野も広範囲になり、また、情報システム、情報セキュリティ分野もますます進展しており、常に新しい知識･技術の修得を行っていく必要がある。

技術及び管理･運用に関する情報セキュリティ教育について、技術者、管理者の教育としてとらえて考察を行う。

なお、「技術者」、「管理者」は、以下とする。

技術者：企業･組織内で情報セキュリティに関して、技術的な面での対応を行う。情報セキュリティを専門とする企業･組織では、情報セキュリティの技術面でのコンサルテーションを行う能力を持った者も想定している。更に、単独で業務を遂行するだけでなく、少数の技術者を統率し、一緒に問題解決等に当たる能力を有する者もこの範疇と考える。

管理者：企業･組織内や外部にいる技術者等で構成される問題を解決のためのプロジェクトチーム等を統率し、必要に応じてトップ経営層に対して状況の報告を直接行う者を想定している。情報セキュリティについての幅広い知識はもちろんのこと、企業･組織に関連する幅広い知識･洞察力をもっており、企業･組織での CISO（Chief Information Security Officer）と考えている。但し、ここで言う CISO は必ずしも企業等の役員レベルを想定していない。

2. 情報セキュリティ教育の概観

技術者や管理者の教育をどのレベルから始めるかについては、全くコンピュータやネットワークの知識がない、情報システム分野に初めて入ってきた者を情報セキュリティ分野の専門家に育てるためのキャリアパスを考えるべきであると言った意見もあるが、ここでは一定の情報システム、ネットワークの知識を持っていることを前提に考える。もちろん、個々の技術者、管理者を考えると、今まで修得してきた教育や経験等に大きく依存するが、ここで述べている初期段階の教育で個々人の知識･技術レベルの平準化がはかれることが望ましい。

教育を考える場合、どの様な分野でも同じであるが、単にその分野における既知の知識を持つだけでなく、新しい問題が発生した場合、それらへの対応、あるいは解決方法を見いだすことができる能力が重要であるが、この点は、情報セキュリティに関しても同じである。特にシステムがますます複雑化している現状では新たな問題が日々発生していると言っても過言ではない状況を考えると、どのようにしてレベルの高い専門家を育てるかが非常に重要であると言える。

技術者･管理者に対する情報セキュリティ教育の概観を図1に示す。情報セキュリティの基礎的な内容、及び事故･事件対応のように情報セキュリティ技術、法律、広報等広範囲の専門家が対応する必要があるものについては、技術者･管理者共通で教育を行うことが考えられる。 これは技術者･管理者が一緒に教育を受けることで、それぞれの考えを知る上でも重要であると考えるためである。

3. 情報セキュリティの教育方法

(1) 講義形式

情報セキュリティを理解し、必要な知識の修得は講義形式で行うことが考えられる。 コンピュータの歴史と同じ程度にセキュリティについても遡ることが可能であるが、1970 年代のゼロックス社パルアルト研究所での実験室でのワーム作成以降のワームやコンピュータウイルス等の有害プログラムやコンピュータ犯罪等は、過去から多くを学ぶことができる。

最近、一部の攻撃者は非常に高度な技術を持っており、攻撃目標を明確に定め、いくつかの段階を経て攻撃を仕掛けてくる。いわば、企業分析を行う者が対象とする企業に対して必要な情報を収集し、手順に従って分析を行い、必要であれば対象企業トップへの面談を行い、それらの情報を基に企業の将来性等を分析する方法と同じで、攻撃方法がシステム化されている。[1]

なお、講義形式の変形として、最近はインターネット、イントラネット等を利用したｅ ラーニングがあり、教育として行う部分の一部、または全部を ｅラーニングで代替することも教育方法の1つとして検討すべきであろう。

(2) 事例による講義

サーバ、ファイアウォール、侵入検知システム等は、発生した事柄（イベント）をログとして記録しており、その内容はそれぞれの機器、ソフトウェア等でフォーマット、記録内容等が異なる。各ログにどの様な内容が含まれているかの説明だけでなく、実際に記録されたログを利用して解説を行う必要がある。[2]

(3) 実習・実技

与えられた条件や機器のセキュリティポリシーを基にセキュアなシステムを構築することで、講義で修得した知識を基に実際にソフトウェアの導入や必要機器の設定を行って、セキュアなシステムの構築体験を行う。

更に実際に構築したシステムに対し、それまでに修得したセキュリティツールや自作のプログラム、スクリプト等を利用して、自分あるいは自グループで構築したシステムや可能であれば他の人、他のグループが構築したシステムのセキュリティ強度を調べるためにシステムへの侵入を試み、構築システムの脆弱性の発見方法、結果報告書作成等を行う。これにより、構築したシステムの脆弱性の発見方法、防御方法や報告書の書き方等を体験でき、併せて、修得した理論を具現化できる。

(4) ケーススタディ、プレゼンテーション形式

私たちが言葉を話す場合、いつも文法に従った形式で話す訳でなく、主語が明確に示されなかったり、間接的な表現をしたりする。 また、話す人の話し方にも個性がある。 同様に、実際にシステムに侵入された場合、事例で示したサンプルのように単純ではないことが多い。 また、1つのログファイルだけの分析では完全に原因を突き止められるとは限らない。

かって、コンピュータウイルスが一般的でない時代には、感染経験は企業・組織の情報セキュリティ担当者でも非常にまれであった。このため、コンピュータウイルスに感染しても気がつかないことがあった。 実際に経験がないといざ事故・事件に遭遇しても、対応を十分に行えないことがある。このため、未経験の事柄を補う教育が必要になる。例えば、具体的に時間経過に基づいて、どの様な状況が発生したかを作成されたログファイルや現象を調べながら、その原因を突き止めることができれば、より実践に近い形で事故・事件を経験できる。 このため、実際に発生した事件・事故等に基づいてシナリオを作成し、その時のログファイル等を含めたデータベースを作成し、研修者は与えられた事例にあるシナリオを読んだり、ログファイルの内容を調べたりすることで、発生した事故・事件が、どの様なもので、何時、どこを経由して発生したか、また事故の発生原因を追求することで、再発生防止のための対応措置や実施すべき対策を考えさせる。このようなシナリオを1人または、グループを作って、作成したシナリオやログファイルを与えて、調査を行わせ、各人あるいは各グループの調査結果を参加者に対してプレゼンテーションを行い、講師や他の参加者等から質問・コメントを行う方法もある。[3]

更に可能であれば、実際に稼働しているシステムに対して、現場でシステム侵入ができるかを実際に経験してみることが望ましい。但し、サービスを停止に追い込む様な事柄を行うか等の取り決めを事前に行う必要があるが、現地調査、脆弱性調査、報告書作成、プレゼンテーションの一連の処理を行うことができることが望ましい。 教職に就くために必用な「教育実習」的なものと言えよう。

4. 情報セキュリティ教育の内容

図1に示した教育内容の概要等を以下に述べる。上述した教育方法等を考慮し、どの様な内容を教育すべきかを考察した。 教育は、参加者レベル、人数、テキスト等、多くの要素を含めて考慮する必要があり、これ以外にも様々な方法の教育があると考える。

(1) 情報セキュリティの基礎

技術者あるいは、管理者として必須であり、情報セキュリティの基礎的な教育を行う。これにより、情報セキュリティの考え方の理解、広範な知識の習得を目的とする。 図2に「情報セキュリティの基礎」で教育すべき項目について列挙した。

(2) 情報セキュリティ技術

技術者に、情報セキュリティ技術の仕組み、ツール類の利用等を通して実際の攻撃方法についても会得させる。更に、それらの攻撃に対する防御対策を実際に構築する。 以下のようなものが想定される。

- 機器・システム等のセキュリティポリシーの考え方や具体例
- 情報セキュリティの脆弱性：インターネットセキュリティ脆弱性トップ 20 (SANS) [4]、セキュリティ脆弱性トップ 14 (Hacking Exposed より) [1]
- パスワードとパスワードクラッキング
- コンピュータウイルス、ワーム、トロイの木馬等の有害プログラムやアンチウイルスソフトの仕組み
- 暗号技術 (公開鍵暗号、共通鍵暗号、ハッシュ関数、暗号強度と攻撃)
- 認証技術 (ＳＳＬ、ＰＫＩ)

(3) ネットワーク技術

ネットワークに関連する技術的な知識、及び接続するシステムを安全に構築するための知識を習得し、修得した知識を基にセキュアなシステムの構築を実際に行う。

システムに対する攻撃手法、その対策の知識を修得するとともに、システムの状況やシステムを攻撃するために必要なセキュリティツール、利用可能なツール類、その入手方法等。 更に主要なツール類を使ってシステム状況・攻撃の方法等を修得する。 セキュリティツール類については数多くあり、また市販品、フリーソフトウェア等あるので、可能な限り多くのツールを利用するとともに、主要なツールについては、自由に使いこなせるようになることが大切である。

また、実際に構築したシステムに対し、他の研修者等から攻撃を行うことにより、構築したシステムの問題点等を明確にする。

ここでは以下のものが想定される。

- ネットワーク構成、及びネットワーク関連技術
- ハブ、ルータ、ファイアウォール、侵入検知システム等の特徴
- TCP/IP セキュリティ
- ネットワーク構築実習
- ウェブセキュリティ
- 電子メールのセキュリティ
- ファイアウォール
- 侵入検知システム
- 攻撃手法とその対策
- セキュリティツールとその利用方法
- 構築したネットワークに対して攻撃を行い、侵入の可能性を確認する。
- ルータ、ファイアウォール、侵入検知システム等のログ解析

(4) Windows セキュリティ

サーバ用のソフトウェアとしては、現在、主に Windows NT、Windows 2000 が利用されているが、Windows のセキュリティに関する知識を習得するとともに、Windows の脆弱性や過去の攻撃、及びその攻撃対策等について修得する。

ここで行う教育項目としては以下のようなものが想定される。

- Windows のセキュリティ機能 (Active Directory、Kerberos 認証、暗号化ファイルシステム、PKI 等)
- インターネットインフォメーションサービス (IIS)、及び IIS のセキュリティ機能
- Internet Explorer のセキュリティ
- Windows を利用したサーバ構築の実践
- Windows に関する攻撃、及びその対策
- 構築したシステムに対して攻撃を行い、侵入の可能性を確認する。

(5) UNIX セキュリティ

UNIX や UNIX から派生したオペレーティングシステムが数多くリリースされており、UNIX を1つのオペレーティングシステムとしてとらえることは難しい部分もあるが、多くの共通点もあり、また、ネットワークＯＳとして最も古い歴史を持っており、情報セキュリティでも多くの問題点、教訓を与えた。

ここでは以下のものが想定される。

- UNIX のセキュリティ (パスワード、ファイルシステム、ログファイル等)
- 電子メールのセキュリティ
- ウェブセキュリティ
- UNIX への攻撃、及びその対応策
- 構築したシステムに対して攻撃を行い、侵入の可能性を確認する。

(6) 侵入テスト・セキュリティ監査

「防御の最大の武器は攻撃である」と言われているが、情報セキュリティでも同様であり、また、攻

撃者と防御者とは表裏の関係にあり、利用ツールも使用者の立場によって「諸刃の剣」となる。 攻撃者の立場から、構築してあるシステムの脆弱性を調査し、発見した脆弱性の指摘を行い、防御者の立場から、対応を考え、脆弱性やその対応について必要な報告書を作成する訓練を行う。

ツールを利用するだけでなく、物理的側面からの脆弱性、ソーシャルエンジニアリング等を含めた人的側面からの脆弱性も調査する必要があり、可能な限り、実体験ができる教育が望まれる。

- 侵入手順
- セキュリティツールの種類と利用方法、及びそれらを利用した対象システムの調査手順
- 調査結果に基づいた報告書作成手順
- 構築システムへの侵入テストを実施し、報告書作成までの手順

(7) 情報セキュリティ管理

情報セキュリティを管理・運用面から考察することは、技術面からの考察に劣らず大切な事柄であるが、情報セキュリティでは技術面が非常に強調されてきた傾向があるが、企業・組織の基幹システムの停止を避けるためにも、技術面だけでなく、管理・運用面からの対応も忘れてはならない。 管理者に対する専門的な教育として、「情報セキュリティ管理」を想定しており、このコースを受講することにより、管理・運用面の専門家の育成を行う。

なお、セキュリティポリシーや緊急時対応計画等は、その骨子の策定を行い、そのプレゼンテーションを行い、参加者間での評価を実施することも有用である。

ここでは以下のものが想定される。

- 企業・組織におけるセキュリティポリシーの作成、及びその維持のための対策
- リスク管理
- 情報システム、情報セキュリティを取り巻く法律等の詳細
- 情報セキュリティ管理システム（ISO17799、ISMS）の詳細
- 緊急時対応計画の策定と維持のための対応、及び実施訓練の実行
- 企業・組織における情報セキュリティ教育

(8) 事故・事件対応

事故・事件対応教育は、発生した事柄により、単なる被害者だけの場合と被害者、且つ、加害者の場合もある。 また、顧客情報の漏洩やコンピュータウイルスで外部企業・組織に感染を広げた場合のように外部に知られてしまったり、多額の金額的な損害を被ったため警察等への届け出を行う必要がある等の場合と企業・組織内で対応できる場合がある。

また、警察等への届け出を行うかどうかは別にして、JPCERT/CC（コンピュータ緊急対応センター）や IPA（情報処理振興事業協会）等への届け出を行うかの判断も必要になる。なお、図3は、CSI/FBI が米国内の企業・組織に対して行った調査結果であるが、実際に侵入等が発生しても警察等の法執行機関へ届けない理由を述べている。これをみると、30%前後の米国の企業・組織が届け出をしていない。 発生した事件・事故が重大なものであれば、企業・組織の存続にも関係し、企業・組織での危機管理対策として考える必要がある。

事故・事件対応は原則的にはセキュリティ技術者・管理者が中心で行うが、他の関連部門の要員も協力して事故・事件の対応を行う前提で教育を行う必要がある。

なお、実際に事故・事件が発生した場合、企業・組織としてどの様な対応を行うかを事前に十分検討し、そのための体制構築が重要になる。事故・事件発生時にどの様な体制になるかは、事件・事故の大きさにもよるが、広報部、法務部、人事部等が関係することを考える必要があり、可能な限り、多くの情報を収集し、一元的な管理が必要になるため、事前に対応組織の体制を考慮しておく必要がある。 また、色々な状況に応じた訓練を行うことにより、実際に事件・事故が発生した時に対応できる仕組み作りが大切になる。

事故・事件の大きさにより、警察、司法機関との対応も必要になり、証拠保全等も関係者が熟知している必要がある。

ここでは以下のものが想定される。

- 事件・事故対応組織（組織の目的、チーム構成、各構成員の役割）
- 事故・事件の種類（有害プログラム、ウェブ改竄、システム侵入、データ改竄・漏洩等）
- 事故・事件により、収集・保全すべきもののチェックリストの作成（参考：事件・事故への報告書様式を JPCERT/CC が記入例を示している。[5]）
- 事故・事件対応のために以下のようなステップをとるが、各ステップでどのようなことを行うかを理論面、及び実践面の両面から修得する。
  - 事前監視
  - 事件・事故の発見・識別
  - 事件・事故現状の維持、証拠保全方法

- 分析
- 報告

- 具体的な事例を利用して、どの様な事故･事件が発生し、それに対してどの様な対応をすべきかを策定した対応計画に基づいて実施し、問題点、改良点等があれば、それらに基づいて必要な資料、体制等の見直しを行う。

参考文献

[1] Stuart McClure, Joel Scambray, George Kurtz: *Hacking Exposed: Network Security Secrets and Solutions, Third Edition*, 2001, Osbone/McGraw-Hill

[2] Stephen Northcutt, Mark Cooper, Matthew Fearnow, Karen Frederick, 武田圭史監修: ネットワーク侵入解析ガイド（*Intrusion Signatures and Analysis*），2001，ピアソン・エデュケーション

[3] Mike Schiffman: Hacker ’s Challenge: Test Your Incident Response Skills Using 20 Scenarios, 2001, Osbone/McGraw-Hill

[4] The Twenty Most Critical Internet Security Vulnerabilities (Updated) The Experts ’ Consensus 、http://www.sans.org/top20.htm

[5] JPCERT/CC インシデント報告の手引 http://www.jpcert.or.jp/form/HOWTO

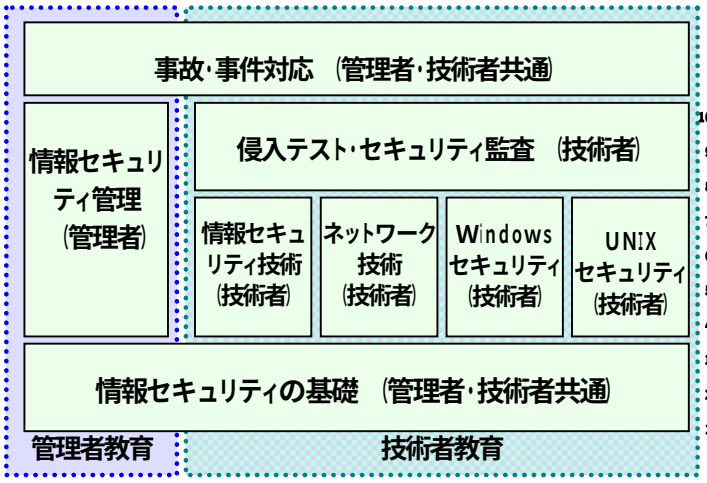

図1 管理者や技術者への情報セキュリティ教育概観図

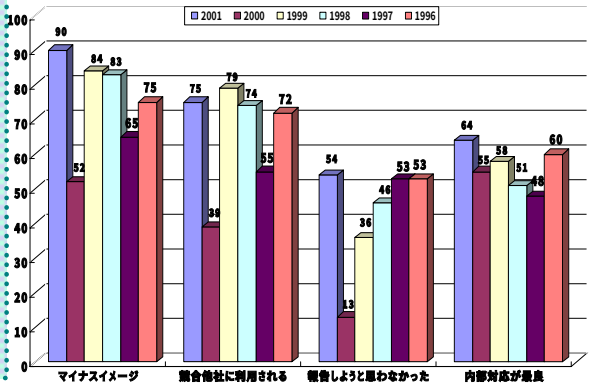

図3 警察等への届け出をしない理由

情報セキュリティの基礎

（1）情報セキュリティ
（2）ハイテク犯罪
（3）アクセス制御
（4）リスク分析
（5）ネットワーク及びネットワークセキュリティ
（6）コンピュータウイルス・ワーム等
（7）暗号
（8）ウェブセキュリティ(スクリプト、CGI、SSL 等)
（9）デジタル署名と PKI
(10）ファイアウォール、侵入検知システム
(11）一般的なハッカー攻撃
(12）Windows セキュリティ
(13）UNIX セキュリティ
(14）ブラウザーのセキュリティ
(15）セキュリティツール
(16）侵入テスト・セキュリティ監査
(17）アプリケーション、システム開発のセキュリティ
(18）情報セキュリティ標準（IS017799、15408 等）
(19）情報セキュリティ関連法制及び倫理
(20）業務継続計画
(21）物理的セキュリティ
(22）セキュリティポリシー
(23）参考文献、情報収集方法

図2 情報セキュリティの基礎の教育内容