経済産業省受託調査
平成18年度コンピュータセキュリティ早期警戒体制の整備事業
（インターネット安全教室及び情報セキュリティ人材育成に関する調査等）

情報セキュリティ教育の指導者向け手引書

（2007年版）

特定非営利活動法人
日本ネットワークセキュリティ協会（JNSA）

はじめに

近年では一般の人々を含め、情報セキュリティの重要性に関する認識は高まりつつあり、ソフトウェアやハードウェアにおける対策の実施、ならびにマネジメントや運用における対応も進みつつある。しかしながら、広く社会から期待されるニーズと比較して、分野的な歴史の浅い情報セキュリティの専門家は少なく、これまでその人材の不足が指摘されてきた。一方、総合的な情報セキュリティが確保されるためには、関係するすべての人々が情報セキュリティを意識した上で判断や行動を行うことが重要であり、人に依存する部分が大きいことから、すべての人々が情報セキュリティに関する学習を行うことが望ましい。こうした情報セキュリティ教育については、近年各地での取り組みが進みつつあるものの、実際には教育できる人材の不足などの理由により、十分な教育が行われているとは言えない状況にある。

本手引書はこうした背景のもとで、経済産業省が実施した平成 18 年度コンピュータセキュリティ早期警戒体制の整備事業（インターネット安全教室及び情報セキュリティ人材育成に関する調査等）による委託調査の一環として、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）が行った活動の成果をとりまとめたものである。JNSA では以前より情報セキュリティ教育に関して、会員による教育の実践や知識体系の検討等の取組みを行っていた。そこでこうした取組みで蓄積したカリキュラムやノウハウ等を、今後の情報セキュリティ教育において活用することが有効との認識のもと、後述のメンバーからなる「手引書作成ワーキンググループ（WG)」を 2006 年度に設置した。この WG による議論を通じて、本手引書の形でまとめられるに至った。

本手引書が今後の情報セキュリティ教育の一層の充実、発展に向け、関係者各位の活躍に資することとなれば幸いである。

JNSA 教育部会長　やすだなお

●JNSA 教育部会 手引書作成ワーキンググループ

リーダー	松田 剛（JNSA 研究員）
メンバー	園田 道夫（JNSA 研究員／サイバー大学）
	冨田 高樹（みずほ情報総研株式会社）
	長迫 勇樹（株式会社インターネット総合研究所）
	長谷川 長一（日本ユニシス株式会社）
	濱本 常義（株式会社エネルギア・コミュニケーションズ）
	平山 敏弘（日本アイ・ビー・エム株式会社）
	やすだ なお（株式会社ディアイティ／サイバー大学）

－ 目　　次 －

はじめに.....1
１．　この手引書のねらい.....3
　１.１　ターゲットと活用方法.....3
　１.２　情報セキュリティ教育の実施ケースの分類.....4
２．　情報セキュリティ教育のカリキュラム例.....5
　２.１　教育すべき内容の俯瞰.....5
　２.２　情報セキュリティ教育のカリキュラム例.....12
　２.３　講義数・時間・受講者に応じた調整.....21
　２.４　情報セキュリティ教育における前提知識と知識間の相互関係.....22
３．　情報セキュリティ教育の実践上のポイント.....24
　３.１　講座（講義・授業）の設計方法.....24
　３.２　講師について.....28
　３.３　情報セキュリティ教育を効果的に行うためのノウハウ.....31
　３.４　講座と教材に関するセルフチェックリスト.....36
４．　おわりに.....38
　４.１　本手引書の未完・不備事項.....38
　４.２　本内容に関連する JNSA における取り組み.....38
付録１　知識項目のリスト.....40
付録２　サンプル教材.....68
付録３　参考 URL.....129

１．この手引書のねらい

１.１ ターゲットと活用方法

はじめに本手引書の作成の意図として、本手引書が情報セキュリティ教育において、どのようなターゲットを対象として作成されているか、教育現場においてどのような活用が考えられるかなどについて説明する。

（１）手引書の利用者

本手引書は、**「情報セキュリティ教育の指導者」**に向けて作成している。この場合の「指導者」とは、**講師を担当される方のみでなく、教育現場において情報セキュリティ教育を実施したいと考えている全ての方**において役立つように意図している。

（２）想定している受講者

本手引書による講義の主たる受講者としては、**４年制大学の理工系の学部生ならびに大学院生**を想定している。こうした学生が将来的に将来のシステムエンジニアや、システムインテグレーション（SI）技術者になることを通じて、情報セキュリティ教育の成果が直接社会に反映され、社会全体の情報セキュリティの水準を高めることが期待される。学生がこうした職務に従事しない場合であっても、情報セキュリティに関する知識を得ることは、IT 依存の傾向を強める現代社会においては有用性が高いといえる。もちろん、こうした受講者以外であっても、条件の相違を加味することで対応できるように配慮している。

（３）本手引書の活用方法

本手引書は情報セキュリティ教育について「このように教えなければならない」といった強制を求めるものでなければ、「こう教えるべきである」と推奨するものでもない。利用者が本書の内容の中で、自らの用途に適用可能と思われる部分を適宜利用することで、教育に伴う負荷を軽減したり、より内容の高まった講義を行うことができれば、本手引書の目的は達成されるものと考えている。

本書の記述内容の中には、利用者の環境の中では意味をなさないものや、利用者の意見とは異なるものもあるかもしれない。情報セキュリティは比較的新しい教育分野であって、これまで様々な分野を専門としてきた人々が色々な背景知識のもとで教育を実施していることで、教育の方法論などのレベルでは異なる意見が並立していることもある。利用者においてはこうした状況を踏まえつつ、他の情報等とも比較しながら活用していただきたい。

１.２ 情報セキュリティ教育の実施ケースの分類

次章以降での紹介に先立ち、本手引書で想定している利用場面として、大学における情報セキュリティ教育の実施ケースをその特徴に応じて分類したものを示す。ただし実際の教育では、これらの複数の要素を併せ持つカリキュラムなども存在する。

（１）技術者や専門家の育成を目的とした情報セキュリティ教育

（ａ）基礎的知識の習得を目的とするもの

これから情報系分野を学ぼうとする学生等に対し、IT 関連科目の１つとして情報セキュリティに関する基礎的知識を身につけてもらうものである。カリキュラムは、情報セキュリティの関連分野を幅広く扱うような構成となるのが一般的である。

（ｂ）実践的知識の習得を目的とするもの

情報セキュリティを専門分野としようとする学生等や、情報セキュリティ対策を自ら行う必要のある情報システムの運用管理の担当者を対象に、情報セキュリティを確立するために留意すべき内容を習得してもらうものである。これは後述するように、受講者の理解度を高めるために情報システムを操作することからなる実習形式を含むことが望ましい。カリキュラムは目的・目標に応じて多様な構成をとる。

（ｃ）専門的知識の習得を目的とするもの

情報セキュリティを専門分野としようとする学生等を対象に、暗号理論やコンピュータフォレンジックスなど、情報セキュリティ分野の専門的知識を習得してもらうものである。ここに分類されるものは、一般に当該分野を専門分野とする講師によって教授されることが多い。

（２）一般向けの情報セキュリティ教育

（ｄ）実用的知識の習得を目的とするもの

大学の新入生を対象に、学内で守るべき情報セキュリティ上のルールなどを習得してもらうものである。情報倫理に関する内容を含んだカリキュラムとなることが多い。ルールの周知等が目的であるため、情報セキュリティに関する教育は必要最小限の内容となる。

（ｅ）教養的知識の習得を目的とするもの

情報系分野を専門としない学生等を対象に、一般教養の１つとして情報セキュリティに関する入門的な知識を習得してもらうものである。カリキュラムの構成は上述の（ａ）に近いが、より入門的な内容に絞ったものとなる。

２．情報セキュリティ教育のカリキュラム例

第２章では、情報セキュリティ教育の典型的な実施例について、そのシラバス情報に相当する内容を中心に紹介する。

２.１ 教育すべき内容の俯瞰

情報セキュリティ分野の技術者が不足しているといわれて久しい。この状況は、かつてのソフトウエアプログラマが不足するといわれた時代を彷彿とさせるが、情報セキュリティで望まれる人材像や育成の試みや、検討するべき内容などについて俯瞰的に考えてみる。

２.１.１ 全体を俯瞰した理解と学習目標

情報セキュリティに限ったことではないが、要素技術が大きく発展している時代においては、全体を見通して物事を判断することが難しくなってきている。しかし、重箱の隅を突くだけでは良いものにならないという経験則も、また知っている。例えば、欧米の建築物を見るときに感じるのだが、全体のデザインは素敵なのに、壁と床のつなぎ目とか、扉のねじ止めとか、細かなところの仕上げが気になったりする。一方日本の建物は内装はきれいに仕上げられているのに、景色としてみると何か溶け込んでいないというか、デザインに説得性が感じられないのも事実である。文化とか国民性に根ざすものなのかもしれないが、気になるところである。

図 1[1]は、古い東京の鳥瞰図だが、中央の円内がちょうど山手線の内側くらいのようである。この絵図で興味を引くのは、富士山を始めずっと遠くまで書き込まれていることである。図 2 に一部を拡大したものを示したが、左手を見ると渋谷から下関、台湾まで書かれている。右手の方も浅草から北海道、樺太まで見えている。いくら鳥でもこんな

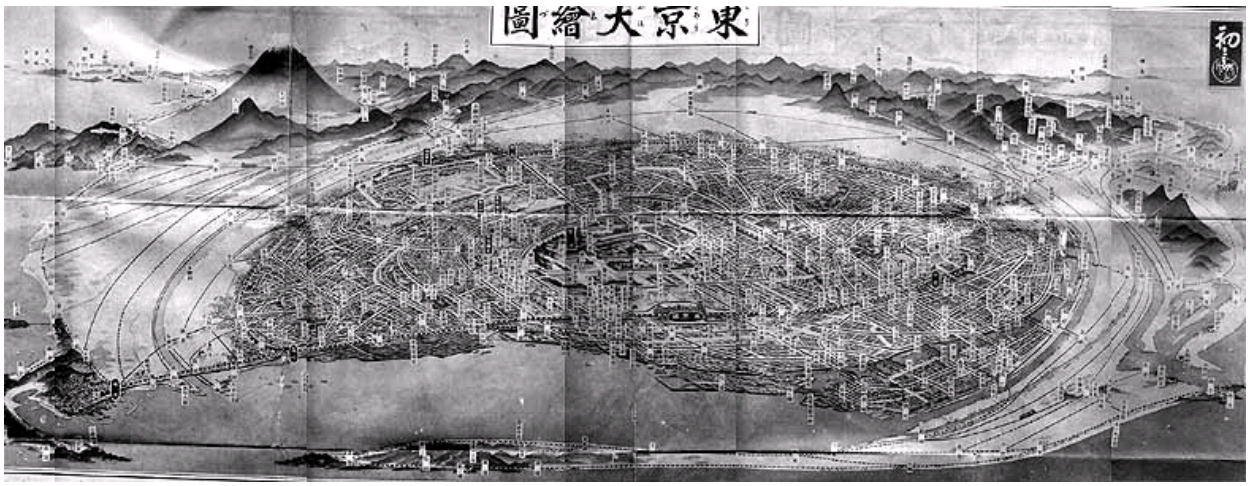


図 １　吉田初三郎版「東京鳥瞰図」[1]

1 『少年倶楽部』16 巻 11 号（1929 年）付録)「探検コム」
http://www.tanken.com/tokyocyokan.html　から引用

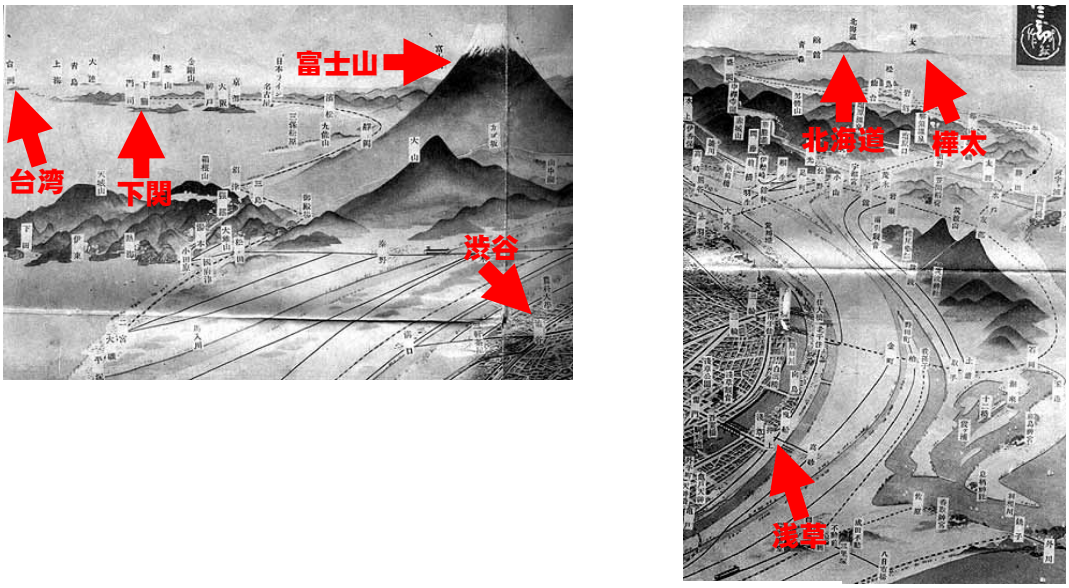


図　2　図 1 の部分拡大図

には見えないかもしれないが、いろいろな専門分野を勉強するときに、このような視点を持つことはとても大切だと思われる。情報セキュリティとしてみるとき、ファイアーウォールや暗号、認証などといった、「中央」に位置する技術だけではなく、システムデザインや仕様書の書き方、フォレンジクスや法律、運用管理や PDCA サイクル、入退室管理や作業記録、権限付与や物理セキュリティ、等々といったさまざまな関連分野があり、遠くには政治や政策、医療、初頭から高等までのいろいろな教育、一般市民への啓発などもある。どれもが視点を変えれば「中心」になるものであるが、自分の「中心」となる視点を意識し、その分野を極めるとともに、全体を見る視野は広く持っていてほしい。そのような視野を持てる人材を教育することが何より大切ではないかと考える。

２．１．２ 人材育成の根本問題

実際の開発現場で意識されている課題は、専門的視点を持ちながら、広い視野を備え、多様な問題点を理解し対応できる人材を育成することである。政府も情報セキュリティに携わる人材の育成の必要性は十分認識しており、セキュア・ジャパンのような政策目標にも書き込まれている。これはとても大切なことであるが、主に教える側や施策を行う側の視点で書かれている。

もうひとつの視点が、技術者を受け入れる社会の側の意識を変えればよいということである。これが問題解決の大きなポイントになると思うのだが、情報セキュリティの人材が不足していて、育成が急務であるのにもかかわらず、なかなか人材が輩出されないのであれば、何か本質的な原因があると考えるのが自然であろう。ではそれは何であろうか？

情報セキュリティ関係の職業は、成りたい職業だと思われていないのではないか、という懸念がある。では、なりたい職業とは何か？

（１）社会的な地位や名誉が得られる

（２）義務や責任に見合った報酬がある

（３）組織内のキャリアパスの主流である

現在の IT 関係の技術者は、待遇的にはあまり恵まれていないと自他共に認めている節がある。確かに優秀な技術者は高給で迎えられたりするが、多くの現場の技術者は３Ｋな職場だと言われたりしている。ネットワーク技術者は縁の下の力持ちで、いろいろな脅威やトラブルを未然に防ぎ、空気や水のようにネットワークをいつでもどこでも使えるよう支えている、という自負のあるエンジニアが多いと思うが、その割には評価されていないという自覚もあるように思われる。原因としては、技術者側にも、報告をしないとか、プレゼンが下手だとか、勝手に作業をして情報共有しないなどの大きな構造的な問題はあるだろうが、なりたい花形職業であれば、自然と学習・研究を希望する優秀な人たちが増え、技術者の社会的評価が上がるプラスの連鎖ができ、問題は解決するのではないだろうか。このような場合でも、単純な設置・設定の技術利用教育だけではなく、本質的な原理原則を教える基礎教育が更に重要となってくるだろう。

2.1.3 技術者教育の方法論

教育一般に当てはまるとは思うが、ここでは情報セキュリティに関する技術者教育という視点を中心に、カリキュラムを作るうえで考慮すべき点について少し整理してみよう。

まず一般的に、学習を行う手段として、大きく 3 つに分けて考えられる。

（1）座学

（2）実習

（3）ケーススタディ

一般的に「教育」というと、教室で先生が解説するタイプの(1)座学となるかもしれないが、英語でも文法だけではなく、スピーキングやヒアリングなどコミュニケーションを行うことが重要であるように、情報セキュリティの教育でも色々な学習方法を組み合わせ、学習者のモチベーションを高めながら、各個人にあった学習を実現することが必要だろう。次に、前記した 3 つの手段について、簡単に整理しておく。これらは、1955 年、ベンジャミン・ブルームが提唱したタキソノミー（taxonomy）にも教育目標の分類学の 3 つの学習領域として分類されている。

（1）認知的領域（知識と思考）

（2）精神運動的領域（物理的な動作）

（3）情意的領域（感情と態度）

この考え方は、後述するインストラクショナル・デザインにも継承されている。

2.1.3.1 座学（基礎的な原理原則を学ぶ）

いわゆる「座学」と呼ばれるものは、教室で教師と学生が向かい合って行う授業が大方のイメージであろう。初等・中等教育では、形式的に教室で行っていても、ディスカッションを取り入れたり、実習のような手を動かす作業を行わせたり、色々創意工夫がされているが、多くの高等教育では、教師が説明を行い学生が聴講するという形式が多いのではないだろうか。

IT 系の教育は、歴史が浅いだけに学問的な因果関係の確立がされておらず、どうしても製品や実際の運用に即した講義内容は主体になってしまうことが多い。これはある程度仕方が無いことではあるが、実用されている技術がどのような背景を持って作り上げられてきたのか、なぜそうなったのかという技術背景を知ることが、高等教育での重要なミッションであると考える。皮相的なものは、各メーカやベンダーが行っている製品の利用や保守に関する教育や資格制度を利用すればよく、高等教育が目指すものはその背景にある原理原則を学ぶことにある。

この座学は、科学的な興味を深め、対象分野の原理原則を身につけることが目的であるので、教える場合の教材が重要な役割を持つ。座学で教える内容は、専門家としての初学者から、自分で自立して研究や開発ができる大学院レベル以上の高度なものまであり得るが、本報告書で対象とするのは、現在一番不足していて早急に手を打ちたい初学者を対象としたものである。

JNSA の今までの調査研究で、特に地域での情報セキュリティ教育が進まないのは、

次の 2 つの理由が大きいことが指摘されている。

（1）地域で教える教員が確保できない

（2）周辺分野の教員に初期教育をやってもらいたいが適当な教材を作るのが難しい

これには、さまざまな背景となる理由があるが、このような状況を鑑み、本報告書では、主に初学者向けの座学で使う場合を想定した教材について取り上げている。

教材作成での大きなハードルのひとつが、「どのような項目を取り上げるか」という点にあることがこれまでのヒアリングなどで予想されたので、本報告書では、教える内容の項目リストアップという点に取り組んでいる。隣接分野の教員であれば、情報セキュリティについての個々の内容はそれなりに理解できると思われるが、一番不安なのが、教える内容が揃っているか、という点であろう。このような不安をチェックし確認するために、網羅的な教えるべき項目のリストアップを行っている。

2.1.3.2 実習（実験、演習）

実習や、実験、演習の類は、ある決められた条件で、実際に現象を再現させて、体験することにより理解を深める学習方法のことである。再現性がある場合とか、様々な結果が出る場合とか、いくつかのタイプに分類することはできるが、本報告書ではその点は問わないこととする。

実習は、原理原則の予備知識を持った上で、体験し確認する作業として行われるのが一般的である。もちろん体験したことへの疑問から原理原則を導く学習方法もあるだろうが、ここでは特に区別しない。両方の連係プレーが重要であることを、ここでは確認しておきたい。

情報セキュリティ分野における実習では、コンピュータやネットワークなどの機材を使うことが多いだろう。これらの環境設定や実習管理などについて、いくつかの考慮点がある。

（1）実習の初期環境を、実習を行うたびに初期化する必要がある

（2）インターネットワーク環境をそのまま使わせない方が良い場合が多い

IT 関係の実習では、使い捨ての実験装置や試薬などはほとんど無いといってよい。コンピュータは常に再利用されるので、実習のたびに実験環境を初期化する必要がある。これは簡単そうであるが、実際の実験室の準備は案外手がかかるものである。

（2）のインターネットワーク環境をそのまま使わない、というのは、実験で色々な「不正なパケット」などが出ることがあるので、実習室内に閉じられたネットワークを構築するのが安全である。これの構築や運用管理については、別途項を改めて実例等を紹介する。

このような実験専用ネットワークを構築することは、既存の教育機関では案外大変かもしれないが、インターネット環境を利用しながら、インターネットの問題点を学習する「管理された」実験ネットワークを構築し併用することはとても重要なことである。この実験環境を作ることが最大の難関かもしれないが、教育効果も高い部分であるので、ぜひ考慮していただきたい。

２．１．３．３ ケーススタディ（OJT）

ケーススタディは、仮想的な「業務」を仮定し、その仮定の中で実業務とほぼ同じ作業を行い、実際の業務を体験することである。似ているものに「OJT（On the Job Traning)」があるが、OJT では実際の業務に参加し、実業務を体験することでそれまでに得た知識や方法論などを体得するものである。どちらも目的は似たようなところにあるが、ケーススタディは仮想業務であるので、いつでも実施することができるが、OJT では実業務に依存するので、常に適切な題材の作業を行えるかどうかは不確定である。

どちらにしても、それまでに得た原理原則や、実習での体験を活かし、実際の「業務」の中でどのように生かすのかを学ぶ方法として効果がある。そのためには、適切なテーマを用意し、サポートする教員と補助教員が揃っていなくてはならない。これについては、機会を改めて検討したい。

２．１．４ 教材作成と遠隔講義

本報告書作成の予備調査で、特に地域での情報セキュリティ教育が進まないのは、次の２つの理由が大きいことが予想されている。

（１）地域で教える教員が確保できない

（２）周辺分野の既存教員に初期教育をやってもらいたいが適当な教材を作るのが難しい

これには、さまざまな背景となる理由があるだろうが、本報告書では、対策として 2 つの方法を試行してみた。

（１）東京近郊在住の技術者による遠隔講義

（２）教材作成手引書の作成

２．１．４．１ 遠隔講義についての可能性

これまでの予備調査で、「地域で教える教員の確保が難しい」という課題が示されているが、これに対する対策として「遠隔講義」の可能性が挙げられる。e-ラーニングを利用するのだが、対面せずに講義を行う制約をできるだけ回避し、非対面の長所を積極的に活用することが大切である。

最近はインストラクショナル・デザインという、より良い学習環境を総合的にデザインすることが注目されている。講師が受講者にわかりやすい説明や資料を提供することを支援することを目的とした、インストラクショナル・デザイナと呼ばれる人達との協力が、サイバー大学[2]でも始まっており 、これまでの高等教育の講師任せの講義から一歩踏み出し始めた。

また、JNSA と岡山理科大学で情報セキュリティに関する専門家育成の実証教育を行ってきたが、遠隔講義の正式講座として単位認定が行われている。

[2] http://www.cyber-u.ac.jp/

２.２ 情報セキュリティ教育のカリキュラム例

情報セキュリティ教育を実施する際の参考として、目的に応じた３種類のカリキュラム例を示す。

２.２.１ カリキュラム例（基礎編）

（１）概要

本カリキュラムは、情報セキュリティに関する基本的な技術的知識を習得することを目標とするものである。今後情報系学科における情報セキュリティ関連科目として、「情報セキュリティ基礎」等の科目を開講する際のベースとすることも想定している。なお、広義の情報セキュリティ教育には情報倫理に関する教育が含まれることもあるが、このカリキュラムでは情報倫理に関する教育については別途教育していることを前提とし、カリキュラムには含めていない。

（２）カリキュラム

カリキュラムの構成を次表に示す。

表 １　カリキュラム例（基礎編）

講義日程	タイトル	内容
第1回	情報セキュリティ概論	最近のセキュリティ事件（フィッシング詐欺、ウイルス侵入、DoS 攻撃等）とその対応手段から、セキュリティの全体像を俯瞰する
第2回	情報セキュリティマネジメント（1）	機密性、完全性、可用性、認証と識別の違いなど、セキュリティの基礎的な考え方を事例とともに紹介する
第3回	情報セキュリティマネジメント（2）	JIS Q 27000 に代表される規格の根底にある考え方、すなわち情報の分類、リスク特定、リスク評価、リスク分析、監査など）について解説する
第4回	権限とデータ管理（1）	OS や各種アプリケーションが搭載する権限構造（ユーザアカウント）とパスワード管理について解説する
第5回	権限とデータ管理（2）	ユーザアカウントが「人」の管理だとすれば、「データ」の側からの管理アプローチも存在する。そこでデータ毎の重要度分類、ファイルのアクセス制限、暗号化、バックアップ、データの破棄方法について学ぶ
第6回	ネットワークセキュリティ（1）	LAN や WAN、インターネットで活用されるルータ、スイッチなど、代表的なネットワーク装置の機能を通じて、現代ネットワークシステムを概観する
第7回	ネットワークセキュリティ（2）	ネットワークシステムシステムの安全を支えるアクセスコントロール技術、すなわちファイアウォール、侵入検知から VPN、無線 LAN の安全性などを学習する
第8回	ウイルス	ウイルス侵入事件（CodeRed、Nimda など）の被害やウイルスの仕組みを理解し、その対策技術を学ぶ
第9回	暗号・認証理論（1）	暗号の基礎用語から代表的なアルゴリズム（共通鍵暗号、公開鍵暗号）を解説する
第10回	暗号・認証理論（2）	データの改変、改ざんチェックに用いられるハッシュ関数の性質を概観したのち、代表的なアルゴリズム（MD5、SHA-1）を解説する
第11回	暗号・認証理論（3）	認証の基本的な考え方を理解したのち、PKI における認証局の構造を解説する。また SSL や S/MIME についても簡単に触れる
第12回	セキュリティ運用	ウイルス侵入など実際の事件のケーススタディを通じて、インシデントレスポンスの考え方について理解する
第13回	関連法規と規格	代表的な規格と法令について理解する。逐条的な解説よりも、法規や規格の使い方について言及する
第14回	全体まとめ	実際のセキュリティ対策は要素技術の活用だけでは不十分で、それらを統合した構築、運用が不可欠である。ここでは、これまで学んだ個別技術を復習するとともにセキュリティ分野を再度包括的に概観してみる
第15回	試験	ペーパー試験（またはレポート等）

（3）受講に際して前提となる知識・経験

本カリキュラムの受講者は、以下についての知識を習得していることが期待される。大学の情報系もしくは理工学系の学部課程の３年等での受講を想定する。

- ネットワーク技術の基礎
  TCP/IP 技術を用いたネットワークに関する主要な用語（IP アドレス、パケット、ドメイン等）について理解していることが望ましい。
- PC の利用方法
  電子メールや Web など、ネットワークを利用するアプリケーションの利用経験があることが望ましい。
- 情報倫理
  情報ネットワークや機器などを利用する際に、法律や規約の遵守の必要性や、どのようなことが他の利用者の迷惑になるかを理解した上で利用すべきことを学ぶもの。本項については入学時のガイダンス的なものでも差し支えない。

（4）実施に必要な環境

すべて座学であり、特殊な環境は必要ない。

（5）教材作成上のポイント

本カリキュラム用の教材を作成する際には、以下の事項に配慮することが望ましい。

- 情報セキュリティに関する事件・事故は受講者が実際に遭遇することが必ずしも多くないので、講義内容にリアリティが感じられないことで単調な印象を与える恐れがある。脅威の説明などを行う場合は、講義の直近に発生した事件に関する報道内容を引用するなどして、受講者の関心を高めることが必要である。
- 公開鍵暗号技術などは数学的理論に立脚しているので、その紹介の際に素因数分解などの理論的説明をすることで内容の理解を深めることができる。ただし、受講者が数学的な分野に苦手意識をもっている場合は、背景的な説明を詳しく行うことはかえって忌避感を高めることになりかねない。受講者の基礎知識や興味の状況に配慮した上で講義を行うことが望ましい。現在実用化されている暗号技術は楕円曲線理論などに立脚しているが、情報セキュリティ技術者すべてがこうした理論的背景を理解しているわけではない。技術の有効性の検証は暗号技術の専門家に委ね、一般の技術者は検証済みの技術や製品を利用するという分化が成立しているので、こうした状況をあわせて教えるのもよい。

（6）条件に応じたカリキュラムのバリエーション

受講者の特徴や目的等に応じて、以下のような調整を行うことが考えられる。

（a）文科系の受講者を対象とする場合

前述の通り、（2）のカリキュラムは主に理工学系の学部課程の学生を対象としている。しかしながら、理数系の知識が必要となるのは「暗号・認証理論」の部分のみであり、それ以外については文系・理系の違いよりもむしろ、コンピュータやイ

ンターネットの利用経験の多少によってカリキュラムの内容に関する理解の容易さに影響が生ずるといってよい。文科系の受講者を対象とする場合は、「暗号・認証理論」の内容について、原理的な説明を必要最小限とし、現在利用されている暗号化サービスや、認証手続きなどの安全性がどのように確保されているかを受講者が納得できることに主眼を置いた教材を用意することが考えられる。

（b）企業内研修などで利用する場合

前述のカリキュラムは社会人経験のない学生の受講を想定しているが、企業内研修などでこのカリキュラムをもとで「情報セキュリティ入門」などとして実施する場合は、企業内の実情に合わせて内容の調整を図ることが考えられる。（2）のカリキュラムでは、私有のパソコンについては自ら管理者としてセキュリティを確保すべきという観点から、システム管理者を対象としたカリキュラムではないにもかかわらず、管理者的視点から権限管理やセキュリティ運用などを説明している。企業内のパソコン等を集中管理し、利用者による使用の自由度を制限している場合は、こうした内容を減らす代わりに、電子メールや Web の利用における脅威とその対策などの比率を高めることが考えられる。

２.２.２ カリキュラム例（応用編１）

（１）概要

本カリキュラムは、前述の基礎編などで情報セキュリティに関する基本的な技術的知識を習得済みの学生や、企業における実務で一般的な知識を獲得している社会人を対象として、実習を中心とした実践的なセキュリティ技術の習得を目指すものである。ローカルな PC サーバの管理者などを担当する場合は事前にこのカリキュラムを学習しておくことで、実施する対策の意図や効果を有効に把握することが可能となる。

（２）カリキュラム

カリキュラムの構成を次表に示す。なお、本カリキュラムは東京電機大学と工学院大学において実際に実施した講義をもとに構成したものである。

表 ２　カリキュラム例（応用編１）

講義日程	タイトル	内容
第1回	オリエンテーション	講義の運用に関する説明
第2回	不正アクセスの理解	脅威とぜい弱性の違いなど、当該分野で使用する用語の定義と代表的な攻撃手法の説明
第3回	能動的攻撃と受動的攻撃	能動的攻撃（フットプリント、偵察、バックドアの作成など）と受動的攻撃（クロスサイトスクリプティング）の違いを実習を通じて学習する
第4回	ウイルスの理解	代表的ウイルス（CodeRed、Nimda）などの構造的理解とその被害状況について把握する
第5回	OS の要塞化（1）	物理的セキュリティ対策とファイルシステムの構造（パーミッション、UMASK、Sticky Bit、SetUID など）の理解と実習
第6回	OS の要塞化（2）	アカウントのセキュリティ（ビルトインアカウント、パスワードチェック）、OS の不要サービスの停止、パッチマネジメント等の理解と実習
第7回	DNS サーバセキュリティ（1）	ゾーン転送の制限、chroot
第8回	DNS サーバセキュリティ（2）	DNS スプーフィングによるキャッシュポイズニング、DOS/DDoS 攻撃などの理解とその対策実習
第9回	メールサーバセキュリティ（1）	プロトコルの特徴に起因する問題（SMTP：不正中継、スパムメール、フィッシングなど）の理解とその対策実習
第10回	メールサーバセキュリティ（2）	プロトコルの特徴に起因する問題（POP パスワード、APOP）から送信・受信双方の安全性確保（本文の暗号化、メッセージ認証）の理解とその実習
第11回	Web サーバセキュリティ（1）	Web サーバへの偵察、侵入（書き換え、情報漏えい）、OS コマンド、SQL インジェクションなどの脅威の理解とその対策実習
第12回	Web サーバセキュリティ（2）	盗聴・なりすまし、クロスサイトスクリプティング攻撃などの脅威の理解とその対策実習
第13回	総合演習（外部公開サーバへのセキュリティ対策（1））	セキュアな公開サーバを実際に構築する（攻撃側、防御側に分かれたグループワーク）
第14回	総合演習（外部公開サーバへのセキュリティ対策（2））	セキュアな公開サーバを実際に構築する（攻撃側、防御側に分かれたグループワーク）
第15回	全体まとめ	グループワークの報告会

（3）受講に際して前提となる知識・経験

本カリキュラムの受講者は、以下についての知識を習得するとともに、経験を積んでいることが期待される。

- 情報セキュリティの基礎
  前述の２．２．１（基礎編）に相当する内容である。
- 実習環境の OS の利用経験
  実習環境の OS を一定期間（数ヶ月）以上利用したことがあり、その利用の際に管理者（Administrator、root など）権限での簡単な設定操作を行った経験があることが望ましい。

（4）実施に必要な環境

本カリキュラムは以下の環境で実施することを想定している。

- 一人一台の実習環境
  効率的な講義を実現するために、同一環境で統一された PC 等を受講者数分用意することが望ましい。
- グループ編成
  ２人１組でのグループを作成することを前提としている。攻撃側・防御側に分かれることを想定しているが、ネットワーク上での監視などの役目を設けて 3 人 1 組とすることも可能である。

参考に、実施環境の例として本カリキュラムの原型とした講義に使用したものを次図に示す。

① ハードウエア
（受講者用）
- Web サイト等閲覧用端末：受講者人数分
- 実習用 NotePC：受講者人数分
- NotePC 収容ハブ：10 台程度
- UTP ストレートケーブル：一式

（講師用）
- サーバ機：2 台
- ネットワーク分割用ルータ：1 台
- ファイアーウォール：1 台

講師用のサーバは、ツール類の格納（受講者がこのサーバにアクセスして各人でインストール）やデモ機としての役割を有する。ネットワーク分割用ルータとは既設のネットワーク環境からこの実習環境を独立させるための装置である。その他必要に応じて CPU 切替機などの投影用装置も用意することが望ましい。

② ソフトウエア
- クライアント OS（受講者用 NotePC に搭載）：RedHat9、WindowsXP
- サーバアプリケーション（受講者用 NotePC の RedHat9 上で稼動）：sendmail、Bind、apache
- その他（第 2 回：不正アクセスの理解、第 3 回：能動的攻撃と受動的攻撃の回で使用）
  －セキュリティアナライザ
  －ポートスキャンツール
  －パスワード解析ツール

図 3　実施環境の例

（5）教材作成上のポイント

本カリキュラム用の教材を作成する際には、以下の事項に配慮することが望ましい。

- 実習で使用する OS への対応

  本カリキュラムにおける教育内容は、使用する OS の種類によって大幅に異なることになるため、あらかじめ OS を選定することが可能な場合は、教材の作成しやすさ等にも配慮して選定を行うことが重要である。

- 受講者の習熟度への対応

  実習が手際よく進行するかどうかは、受講者における OS 操作への習熟度に大きく依存する。また、操作にエディタ等を使用する場合は、その操作にも使い慣れているかどうかも影響する。受講者が不慣れと思われる場合は、講義内容のうち高度な部分を割愛し、実習時間を多く確保するなどの配慮が望ましい。

（6）実施時の留意事項

本カリキュラムの原型となった講義を実施した際の経験をもとに、実習主体の講義を実施する際の留意事項を以下に示す。

（a）講義の流れ

- 第 1 回から第 4 回までを、攻撃側手法の解説とその実習に重点を置き、第 5 回から第 12 回までを防御側すなわちセキュアサーバの構築の解説と実習を中心に据えている。
- 第 13 回以降は、これまでの学習成果を踏まえたグループワークを、攻撃側、防御側に分かれた形態で演習を展開し、最終回で構築したサーバの安全性評価を行う。攻撃とは言ってもポートスキャン等の偵察行為に留まるものだが、空いたポートの有無情報などからサーバの安全性評価が可能である。

（b）受講時間の不足への対応

- 受講者は、Unix の初歩的コマンドと TCP/IP の基礎知識を有していることが望ましいが、こうした前提知識のバラつきから実習時間が大幅に不足することが予測される。
- 環境が許すようであれば、実習に用いるセキュアサーバを管理可能なドメイン上に公開し、計算機室の既設端末やインターネット経由で自宅などからアクセス可能（TELNET、SSH などによる）な状態に据え置くことで、時間内で消化しきれなかった実習課題に対応することができる。

（c）受講者人数の上限

- 新規に用意する PC の予算的制約や、講師 1 人が実質的にフォローできる範囲を考えると、多くても 30 人が限界であり、15 人から 20 人程度が望ましい。

（7）条件に応じたカリキュラムのバリエーション

受講者の特徴や目的等に応じて、以下のような調整を行うことが考えられる。

（a）システム管理者向けの研修講座とする場合

前述のカリキュラムはシステム管理者が情報セキュリティ対策を実施する際に用

いるツールで実習を行っているが、講義の目的はあくまでネットワークセキュリティを理解することにある。そのため、このカリキュラムをそのままシステム管理者向けの研修に転用するのでは、権限設定などのアクセス制御や、ログ管理やインシデント対応などを含むセキュリティ運用に関する内容などが含まれない。システム管理者向けの研修講座とする場合は、以下のような調整を行うことが考えられる。

- セキュリティ対策に十分な知識のない受講者を対象とするときは、前述のカリキュラムにアクセス制御やセキュリティ運用に関する内容を加えることで、講義回数や期間について現状よりもボリュームを増やすことが望ましい。セキュリティ対策Ⅰ、Ⅱのように２つ以上の講座に分けてもよい。
- 反対に、すでに運用等に携わっている受講者を対象とするときなどで基礎的な部分を省きたい場合は、前述のカリキュラムにおいて１，２に分けているものを各１回に圧縮できる。これによって空いた時間でアクセス制御やセキュリティ運用に関する実習を行うことで、システム管理者が習得すべき内容を網羅することが可能となる。

２.２.３ カリキュラム例（応用編２）

（１）概要

本カリキュラムは、情報系を専攻する大学院生等を対象に、暗号技術とその応用に関する講義を行うものである。

（２）カリキュラム

カリキュラムの構成を次表に示す。なお、本カリキュラムは東京電機大学において実際に実施した講義をもとに構成したものである。

表 ３　カリキュラム例（応用編２）

講義日程	タイトル	内容
第1回	イントロダクション	最近のネットワークの動向を示すとともに、セキュリティ上の脅威としてどのようなものがあるか、攻撃方法の概要について解説する
第2回	セキュリティ技術と暗号技術の概要	セキュリティへの脅威に対処するための対策技術を広く概説するとともに、暗号技術の概要を述べる
第3回	共通鍵暗号1	共通鍵暗号としてブロック暗号とストリーム暗号があることを示すとともに、ブロック暗号の例として DES の具体的処理方法を解説する
第4回	共通鍵暗号2	共通鍵暗号の適用モード、解読方法、鍵管理などについてその方法を解説する
第5回	公開鍵暗号1	公開鍵暗号のニーズと方法の概要を述べるとともに、RSA 暗号の具体的方法を示し、実際の暗号と復号の演習を行う
第6回	公開鍵暗号2	公開鍵暗号として、エルガマル暗号、楕円曲線暗号などを解説するとともに、利用形態、攻撃方法について概説する
第7回	ディジタル署名	公開鍵暗号の応用であるディジタル署名の方法について解説するとともに、そこで用いるハッシュ関数について説明する
第8回	PKI1	ディジタル署名を運用する基盤となる PKI(Public Key Infrastructure)について基本的な枠組みを解説する
第9回	PKI2	PKI の相互認証方法や、公開鍵証明書の無効化の手順を比較評価するとともに、今後の展開のために必要な事項を示す
第10回	暗号プロトコル	暗号をベースとした秘密分散法や、マルチパーティプロトコル、グループ署名、多重署名等の方法について解説する
第11回	不正コピーの防止技術	DRM 技術の概要、電子透かしなどについて解説する
第12回	全体まとめ	以上で学んだことを復習するとともに、標準化の動向や暗号技術が社会に与える影響について議論する

（３）受講に際して前提となる知識・経験

本カリキュラムの受講者は、以下についての知識を習得していることが期待される。

- 情報セキュリティの基礎

  前述の２．２．１（基礎編）に相当する内容である。

- 数学的知識

  暗号理論を理解するために、代数学系、幾何学系等の知識を習得していることが望ましい。本カリキュラムを受講するレベルであれば、大学の学部課程における一般教養の内容で十分である。

（４）実施に必要な環境

すべて座学であり、特殊な環境は必要ない。

（５）教材作成上のポイント

本カリキュラム用の教材を作成する際には、以下の事項に配慮することが望ましい。

- 最新の情報へのアップデート

  古いアルゴリズムや短い鍵の危殆化、暗号応用技術の発展などに応じ、本カリキュラムの講義内容には定期的に最新の情報に更新すべきものが多い。教材もこれを踏まえ、毎年更新の必要性を検討すべきである。

２.３ 講義数・時間・受講者に応じた調整

前項に示したカリキュラムについて、所定の講義数や時間が確保できない場合や、受講者の前提知識がカリキュラムにおける想定と異なる場合は、以下のように調整を行うことになる。

（１）講義数や実施時間が少ない場合

対策として、以下の方法が考えられる。

- 事例などを絞る。例えば、複数の OS に応じた対応の仕方を扱っている場合、特定の OS の場合のみを教えることにする。
- 後述する知識間の相互関係などを考慮した上で、応用的な要素の強い部分を省く。このように修正することで、入門的要素の強いカリキュラムとなる。
- 受講者の前提知識を考慮し、既知の分野を多く含む部分を簡略化したり、現在の前提知識では理解するのに負担が大きいと思われる部分を省くなどの調整を行う。

（２）受講者の前提知識が異なる場合

受講者の前提知識がカリキュラムにおける想定と異なる場合の調整方法の例を、条件に応じて以下に示す。

- 受講者が文系専攻等で数学的な知識に苦手意識を持っている場合、暗号理論の説明を簡略化、もしくは数学的知識を求めない形に修正することが考えられる。ただし、情報セキュリティ技術の学習に数学的な専門的知識は必要ない。基礎編については、数学的な知識として求められるのはほとんどが四則演算レベルであり、むしろ後述するネットワークに関する知識や経験の有無に依存するところが大きい。
- コンピュータネットワークに関する知識や経験が不足している場合は、受講者は講義内容を実感しにくい。受講生はここに示したカリキュラムを受講する前に、インターネットの仕組みや TCP/IP の基本に関する入門的なカリキュラムを受講していることが望ましい。こうした知識が不十分な受講者が一部含まれる場合は、そうした受講者に最初にネットワークに関する補講を行うことも考えられる。
- 情報セキュリティマネジメントに関する分野は、実務経験の有無によって理解に差が付きやすいため、受講者に実務経験のない学生と社会人が混在するような場合は配慮する必要がある。

２.４ 情報セキュリティ教育における前提知識と知識間の相互関係

情報セキュリティ教育を構成する各科目はその相互間の依存関係に基づいて有向グラフによる体系化を行うことで、下図のように整理することができる。

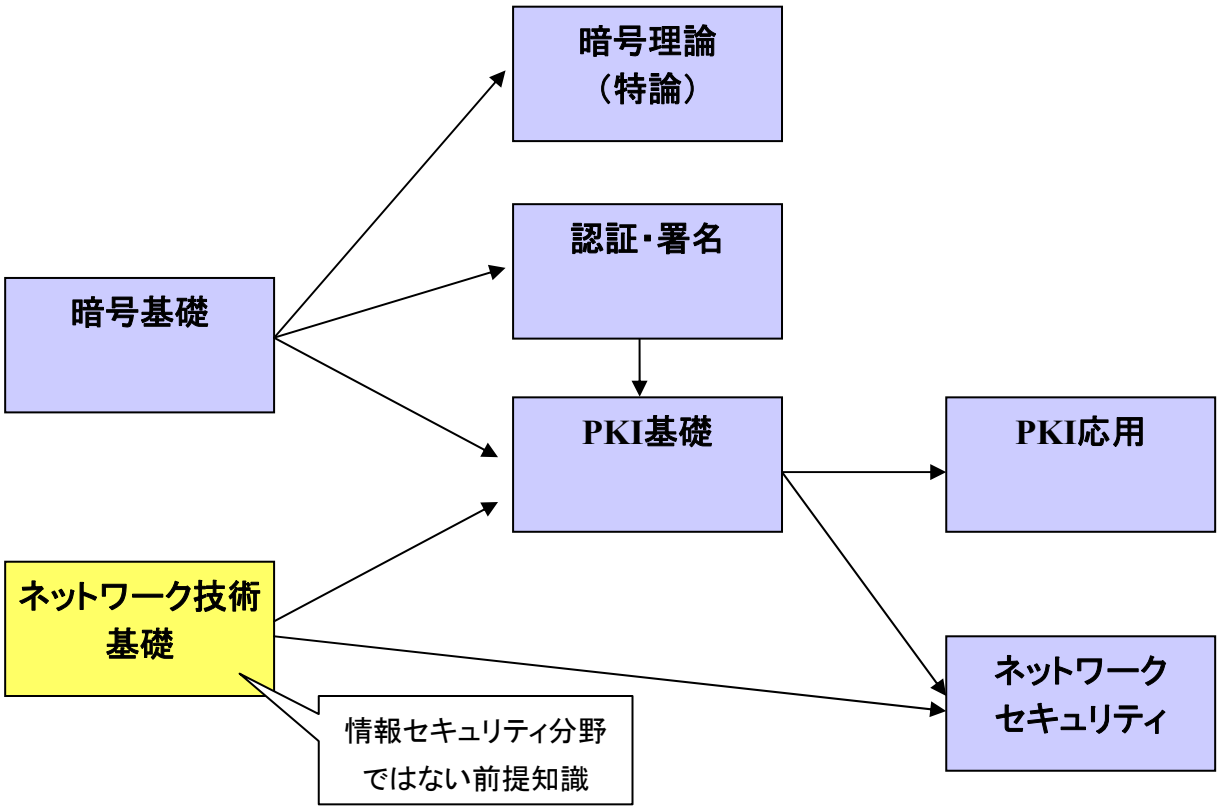


図 ４　各科目の相互間の依存関係

（１）依存関係の考え方

例えば、PKI は公開鍵暗号方式という暗号技術をもとに実現されている仕組みであるため、暗号理論の基礎を学んでいない受講者が PKI を学習しても、その学習効果は限定されたものとなる。そこで、教育による受講効果を最大限に発揮するためには、こうした科目間の依存関係を考慮してカリキュラムを構成することが望ましい。

ただし、暗号方式を応用した技術を学習する場合、その理論を受講者が完全に理解している必要ない。例えば、楕円曲線に関する関係をもとにした暗号方式が有効であることを理解するためには、一般の理系の大学卒業者の平均的な数学的知識を相当に上回るような高度な専門知識が必要である。しかしながら、現在情報セキュリティの専門家として活躍している技術者でも、その多くはこうした数学的な高度な知識を有さなくても支障なく業務を遂行している。これは、「楕円曲線を利用したアルゴリズムが適切に実装された暗号方式は実用上問題なく使用できる」ことが、情報セキュリティ分野における共通認識となっており、結果的に暗号方式をブラックボックスとして扱うことができることによる。よって、PKI に関する科目を学ぶに先立って、暗号の基礎に関する学習が済んでいる必要はあるが、暗号アルゴリズムに関する専門科目を学習しておく必要は必

ずしもないことになる。

このように、カリキュラムにおける科目間の相互関係を考える際には、各科目が立脚する理論についての相互関係だけでなく、このように実用上要求される知識の深さなどについても考慮する必要がある。

（2）情報セキュリティ以外の知識との関係

情報セキュリティ教育といっても独立した学問分野があるわけではなく、オペレーティングシステム、情報ネットワーク、暗号理論、マネジメントシステムなどの分野の中から、「情報セキュリティ」という切り口で関連する科目を集めたものと言っても差し支えない程度である。よって、情報セキュリティ教育の前提知識は、図 4で示した「ネットワーク技術基礎」のほか、「計算機システム基礎」、「システム工学基礎」といった関連分野の基礎科目が相当することになる。情報セキュリティ関連のコースを設計する場合は、こうした直接情報セキュリティを連想させない基礎科目の扱いについても配慮する必要がある。

（3）より専門的な知識との関係

高度な科目における他科目との相互関係については、２つのパターンに分類される。１つは、「暗号理論（特論）」のように、暗号技術などの１分野における高度な内容の習得を目指す科目であり、これらの科目における依存関係は、その前提となる科目が１～２科目程度と少ないのが一般的である。こうした科目については、新たに追加的に設置する場合でも、既存のカリキュラムを大きく変更するなどの必要はない。

もう１つは、「コンピュータ・フォレンジックス」のように、法学とアクセス制御技術のような複数の分野の融合により成立していたり、学際的と位置付けられるような科目である。こうした科目は、全く分野の異なる複数の科目と依存関係をもつため、既存のカリキュラムに追加する場合、受講者が事前に必要とする知識を事前に習得できるよう、場合によっては他学科との連携・調整なども行う必要が生じることがある。

３．情報セキュリティ教育の実践上のポイント

第３章では、情報セキュリティ教育を行う場合に留意すべき事項について、講座の設計方法、講師に求められる事項、実践上のノウハウなどの視点から紹介する。

３.１ 講座（講義・授業）の設計方法

情報セキュリティに関する講座（講義・授業）を設計する際に留意すべき事項を挙げる。

３.１.１ 講義時間について

講義の１回あたりの実施時間の考え方について、条件別に示す。

（１）座学の場合

通常は１回（１コマ）あたり 90 分～100 分で講義を行うのが一般的である。集中講義形式の場合、午前または午後に 2～3 コマ連続して行うこともある。有料のセミナーなど、受講者が積極的に参加している場合は集中力が持続するため、講義を連続して行ってもある程度は効果が保てるが、そうでない場合は集中力が低下するため、一度に多くの内容を長時間にわたって講義することは避けるべきである。ただし、情報セキュリティの習得には多様な科目の学習が必要であることを活かし、マネジメントに関する講義と技術に関する講義を組み合わせたり、同じ技術でも分野を変えるなどの工夫により、受講者の集中力を高めることもできる。講義の半ばで小テストを実施し、その採点をした上で次の話題に入るのもよい。

（２）実習形式の場合

講師による説明の後に受講者が自ら機器等を操作し、試行錯誤を通じて学習することを目的としているので、（１）で示した 90 分～100 分で 1 コマという単位では時間が不足する場合が多く、1 回の実習に最低 2 時間以上を確保することが望ましい。講義と実習を交互に行うことで、3～4 時間であっても比較的受講者の集中力を持続させることが容易である。反面、所定の時間内で実習を終えることができない受講者が生ずる可能性があり、講義終了後の該当者のみの時間延長なども考慮する必要がある。

（３）グループディスカッションを含む場合

講師の説明を聞いた後で、受講者をいくつかのグループに分け、グループ内での議論を通じて問題を検討し、発表を行うといった形式のものであり、受講者による問題や解決策の発見能力の向上に有効である。この場合も（２）と同様、90 分～100 分では時間が不足する場合が多く、1 回の実習に最低 2 時間以上を確保することが望ましい。

（４）遠隔講義の場合

遠隔であっても受講者と講師の間でリアルタイムの対話が可能な場合は、（１）の座

学の場合と同様と考えてよい。ただし、通常の講師と受講者が同室で行う講義に比べると遠隔での応答に時間を要するため、１回あたりの内容を少なめにするか、１回あたりの講義時間を長めに確保する必要がある。

（５）ビデオ教材、ｅラーニング教材等の場合

受講者が自分の都合のよい時間に受講するため、講義時間に関する物理的な制約は集合形式での講義と比較して少ない。しかしながら、教室での受講と異なり受講者が講師と対話したり、講師が受講者の反応を見ながら調整するといったことができず、講師からの説明に終始することになるため、受講者の集中力が続かないことになりがちである。そこで、講義の内容を 15 分～20 分程度の「章」に分割し、この章単位で内容を分け独立可能な部分として構成するのが良いと言われている。１コマは４章分程度とし、約 60 分程度で終わるようにすると、受講者の集中力を持続させやすい。章ごとにある程度完結させることによりメリハリのある講義内容になるので、これを e-ラーニングのテキストを作る際の時間や分量の目安とすべきである。

3.1.2 実習形式を取り入れる場合の留意事項

２．２．２（15ページ）で示したような、実習形式を取り入れた講義を行う場合に留意すべき事項を示す。

（1）実習にあたっての注意点

応用編１のカリキュラムは、「攻撃手法の理解を通じて、対策を強化する」ことを目的としている。このため、一部攻撃手法等の実習も含まれるが悪用に転用される恐れから、以下の対応が不可欠である。

- 民間の教育ベンダーなどでは、高度な攻撃手法をカリキュラムに組み込んでいるケースもあるが、それらの多くは法人を対象として受講者個人の身元保証や受講前に誓約書へのサインを求めていることが多い。大学の場合はこうした措置は困難であるため、高度な手法は少なくとも実習からは除外したこと、また講義の冒頭で不正アクセス禁止法など刑事罰を伴う該当法規の説明が必要である
- 実習は深刻な被害を伴うもの、例えばクロスサイトスクリプティングや SQL インジェクション、Dos 攻撃などは除外し、攻撃の前段階に見られるものに留める（例えばネットスィープ、ポートスキャンなどの偵察行為など）。
- 実害を伴う手法については、講義等で概念や危険性の解説に留め、実習では対策方法に力点を置く（セキュアサーバの構築）。
- 偵察行為などの実習でも、第三者から見れば不正パケットと思われるものが公衆回線上に流通してしまうこと、講義で使用するツールが誤解を招く恐れがあること、共有端末上では他の講義ならびに他の研究データ等の破損に結びつく懸念から、簡易な独自環境を構築することを推奨する。

（2）実習の環境

２．１．３．２（9ページ）でも述べたとおり、実習は実習室内で閉じられたネットワークを構築することが望ましい。ただし、インターネット上の情報入手など外部ネットワークにアクセスする必要も出てくることから、各大学の既存の計算機室等で講義を行うのが良いであろう。つまり外部 Web サイトへのアクセスだけであれば既存の端末を使用して、実習用のツールのインストールやその実行など他の環境に影響を与えうる操作については、新たに用意した端末からクローズドなネットワーク上で行うのが安全である。このため講座発足に際し機材の購入費用がかかるほか、機材を常時設置しておける教室を確保できない場合は講義毎に準備と撤去作業が必要となる。

学生各人がノート型の PC を所有しているような大学であれば、それらの持ち込みと数台の貸出機を用意することで費用負担は多少緩和され、また講義毎の作業についても、学生らの協力を求めることで作業負担は大幅に削減できる。ただし、学習の内容によっては学生が設定しているセキュリティ対策の変更が必要となる場合もあり、講義終了後にそれを戻すことを忘れるなどして学生に被害が及ぶことのないよう、十分に配慮する必要が生ずることを忘れてはならない。

３.１.３ 非対面的環境で教育を行う場合の留意事項

非対面で行う遠隔講義は、地域の講師不足を補い、東京地区の技術者の有効利用にもなることから、現在情報セキュリティ教育において特に大きな期待が寄せられている。ここでは、遠隔講義を行う際の考慮すべき点や、教材作成に関する注意点などをまとめる。

３.１.３.１ 非対面的環境の種類と課題点

非対面で行う遠隔講義は、実際にはいくつかのパターンに分かれる。

（１）学生の集合／非集合

学生が集合する必要性に関して、主に２パターンに分かれる。

（ａ）学生は大きなスクリーンのある教室に集まる

（ｂ）学生側は各自の回線に PC をつなぐ

（２）時間の同期

時間の同期については、次の選択肢がある

（ｃ）決められた時間に開始する

（ｄ）オン・デマンドで、学生の自由な時間に開始する

（３）学生側から講師側へのフィードバック

フィードバックがその場でできるかというパターンもある。

（ｅ）学生側から、カメラを通してその場で講師へコンタクトできる

（ｆ）学生が受講しているときには講師からの反応はない

上記（１）（２）（３）は、それぞれどちらかが選択されるが、（ａ）（ｃ）（ｅ）の場合は、大教室に学生が集まり、決められた時間に講師が授業をはじめ、その場で学生からの質問や講師からの指示を行うので、対面授業とほぼ同じ形での授業が行える。テレビ会議のような機能を持つが、一般的には、教室側に質疑など学生の発言をサポートする補助員がいることが望ましい。マイクやカメラのセッティングや教室の様子を的確に講師側に伝えることが大切だからである。

（ｂ）（ｄ）（ｆ）では、完全なビデオオンデマンド形式での e-ラーニングになる。リアルタイムでの講師側からのコンタクトはできないが、電子メールや電子掲示板などの補助的な手段で、何らかの双方向性を確保して、講義を円滑に、また知識の委譲を確実にする工夫をすることが必要である。

多くの遠隔授業は、これらの間にあるといえる。実際に利用できるパターンを確認し、その特性に合った方法を考えることにより、より効果をあげることができるだろう。

３.２ 講師について

情報セキュリティ教育を担う講師の要件として、考慮すべき事項を示す。優秀な技術者は、基本的な知識を既に持っているので、一般的に良い教師になれる可能性を持っている。実際に良い教師となるには、いくつかの要因があるようである。

（１）自分の知識を全て学生に与え、自分を凌駕することを目標としている。

（２）固定された考え方ではなく、柔軟に対応できる思考ができる。

（３）学生のレベルに合わせて、教える内容を噛み砕いて理解させる努力を行える。

これ以外にも、教育分野に精通していることなどがあるが、「研究」という役割と「教育」という役割の違いや連続性を意識していれば、良い教師となれる資質があるといえるだろう。

現在の高等教育は、「できる子をできない子にして卒業させている」と言われることがある。そうではなく、現実的には「できない子をできる子にして卒業させる」という視点も大切であろう。これはひとえに講師の教える資質と熱意と工夫がものを言う。具体的には講師一人ひとりの性格や経験などに因るが、最近このような問題を解決するために『インストラクショナル・デザイン』という考え方が広まってきている。

インストラクショナル・デザインは、もともとは第二次世界大戦のときに、戦時訓練や兵器製造を行う人員を手早く育成するためであった。前記したようにタキソロジーの分類学に基づいているが、インストラクショナル・デザインの基盤は、「学習理論（心理学）」「コミュニケーション学」「情報学」「メディア技術」であり、それらを統合した「インストラクショナルデザインの理論・モデル」である[3]。分析→設計→開発→実施→評価が代表的なプロセスであるが、一番重要なのは「より良い学習の環境を総合的にデザインする」ことであるといわれている。

このような実績を日本でも活かす試みが始められており、講師とインストラクショナルデザイナによる二人三脚の講座のコンテンツが作り始められている。当面は、講師の話し方とか、ビデオ撮りの際の目線の動き、パワーポイントなどの表示資料の作り方、文字の配分やイラストの挿入等々、同じ内容を教える場合でも、学生の感性に訴える部分の修正で効果が上がることが認識されてきているようである[4]。

[3] ウィキペディア（Wikipedia）「インストラクショナルデザイン」の項から引用。
[4] サイバー大学「安定した質の高い教育サービスの提供」
http://www.cyber-u.ac.jp/about/feature/service.html

3.2.1 講師の担当範囲の分割

ひとつの講座を全て一人で対応するのが一般的であるが、情報セキュリティのような幅広い科目の場合は、全てを一人で見るのはかなり大変である。このことが、情報セキュリティ概論のような初学者向けの講座の講師を引き受けるハードルとなっている節がある。このため、範囲の広い講座の場合は、何人かの異なる専門の講師を集めて、リレー式に講義を進めていくことも考えると良い。この場合、事前に担当範囲の調整や講座のシナリオを合わせておくことが大切である。講師チームを組んで、学生の教育という手術に対応するようなイメージだろうか。チームを組むことにより、講座内容の幅が広がり、学生を引き付ける講義が実現できる可能性がある。

3.2.2 講師に期待されるスキル

講師に求められるスキルとして、情報セキュリティに関する教育に限定されたものがあるわけではない。しかし、講義を行うに際して以下のことができると、受講者にとってより効果的かつ有益になると考えられる。

（1）つねに問題意識をもつ

情報セキュリティ上の問題は、日常の何気ない行為や状況に潜むリスクが、何らかのトラブルや犯罪者の意図によって顕在化することで生ずることが多い。過去の事故例を学んだ受講者が、日常に潜むリスクに注意を払えるようになるためには、講師自身が問題意識をもち、新しい技術やサービスに対してどのように接すればよいかをアドバイスできることが望ましい。

（2）多面的な視点の提供

情報セキュリティの確立のためにポリシーやルールの策定と遵守は欠かせないが、ルールの策定者が守る側の立場を考えずに一方的にルールを決めるようでは、守りようがないものになって有効性が発揮されないなどの問題が生じてしまう。有効なマネジメントの確立には物事を一方からだけでなく、多面的な視点から検討することが重要であることを伝えられるとよい。

（3）最新動向への関心

IT 分野の技術やサービスの変化は速く、１年前に準備した教材が講義時点では陳腐化してしまうことも珍しくない。こうした陳腐化した教材で講義をしても受講者の関心は高められないので、技術の最新動向や最近の事件等に興味をもち、トピックスとして講義の話題とできるように努めることが求められる。

（4）高い倫理性

情報セキュリティの講義で教える内容には、不正アクセス等に利用可能な技術が含まれることがある。受講者に不正目的での利用を行わないことを求めるのはもちろんであるが、受講者がそうした発想を抱かないようにするためには、講義に講師自身が

高い倫理性のもとで技術を扱っていることを示すことが重要である。

3.2.3 講座の準備方法

講座のテキスト（コンテンツ）を用意するにあたり、注意すべき点についていくつか挙げておく。対面講義では、その場で黒板等に書きながら説明をすることが多いが、e-ラーニングでは予めパワーポイントなどの資料を用意しておかなければならない。講師によっては、e-ラーニングでも黒板等を使いたいとの希望が出ることがあるが、授業の準備を十分行わずに講義を行う目的であれば、授業形態にマッチしているとは言い難い。

遠隔授業に限ったことではなく、対面授業でも同様であるが、講座の準備は十分に行うことが重要である。その場のアドリブはあまりお勧めできるものではない。特に遠隔授業では、学生側の集中力を保てる範囲で、効果的に知識を伝えなければならない。また、何度も繰り返し聴取されるため、あまり冗談や脱線を言うわけには行かない。繰り返し視聴される学習に耐えられるようなコンテンツを作らなければならない。このための準備が大切である。

３.３ 情報セキュリティ教育を効果的に行うためのノウハウ

情報セキュリティ教育に特化したものではないが、講義を効果的に行うために、いくつか考慮すると良い事項を挙げてみよう。これらは既に言い尽くされているものであるかもしれないが、インストラクショナル・デザイン上も注意点としてチェックされているものである。

３.３.１ 教材の構成上のポイント

パワーポイントなどでの教材を作る際に考慮すると効果的な点をリストアップしてみよう。

まず、**受講者のレベルの把握**が重要な項目なのであるが、受講生の母集団が社員とか特定の団体とかではなく、一般の高等教育機関での入学募集のような場合は、集まってみないと判断できないことも多い。このような場合は、ある程度の予備調査や断片的な情報から推測するしかない。一番悩ましい点であるが、講習対象が確定していない場合は、ある程度一般的なことを中心にして講座を組み立てるか、予め想定したレベル以外の学生を切り捨てるしかないだろう。初学者向けの講座であれば、前者のような一般的な内容を中心にすればよいが、設定レベルをある程度固定してしまうと、想定レベルに達しない受講生や想定レベル以上の受講生へのフォローが難しくなる。ある程度専門性の高い講座の場合は、受講生の募集方法にも工夫が必要である。

講座毎の講義内容に関する**前後関係**や**知識の依存関係を意識**して、講座を作れれば効果が高い。実際には最初に講座全体を組み立てるときに対応しなければならないので、なかなか難しいが機会があればぜひ再構築も含めて考えてみると良いだろう。この際、各講義の前後関係や相関関係を意識して、講座の内容を調整できれば、効率的な教育ができるはずである。

次に、具体的な教材を作る際の注意点として、ごく一般的な項目を挙げてみる。

（１）講座案内等に講座の目的を示す

いわゆるシラバスへの記載であるが、ここにできるだけ講座の目的や内容を簡潔に示す。受講生はこの記述を頼りに講座を選択することになるので、誇大でも過小でも不都合である。他教科との関連もあれば記載しておく。

（２）初回に全体構成を示す（鳥瞰）

初回の教材に、これから学ぶ内容についての全体構成を示し、講座が終了したときにどのような知識が得られるかを説明しておくと良い。これは、受講生の目標設定や目標管理のためにも役に立つ。

（３）毎回冒頭に今回の内容を示す

毎回の教材の冒頭に、講座での達成目標を示すと良い。これは、毎回、何を学習するのかの動機付けを行うと共に、目標達成の自己管理ができるようにするためでもある。

（4）最後に復習と予告を示す

教材の最後に、今回の学習内容のまとめや復習情報を示し、次回の予告を掲示すると良い。復習と次回予告を明示することにより、受講生が自分の進度管理のイメージを作りやすくなり、効果的な学習が可能となる。また、教材を作るときに、できるだけ全部の回の内容を予め作り、全体の進度を見直せるように、余裕を持った教材作成スケジュールを考えると良い。

（5）スライド 1 枚に内容を詰め込みすぎない

パワーポイントなどのスライドには、できるだけ完結に要点のみを記述し、細かな説明は図版や口頭で説明するようにする。スライドに沢山文字を書き込んでしまうと、読みにくいだけではなく、却って要点がぼけてしまう恐れがある。また、図版を使うと直感的にわかりやすくなることが多いので、表現方法に工夫をすると良い。このあたりの方法論については、Web などでも沢山公開されているので、参考にすると良いが、インストラクショナルデザイナの助力を得られれば楽である。

（6）FAQ の提供

講義を始めてゆくと、必ずいろいろな質問が出てくる。これらの中には説明が足りないことで必然的に出てきたものや、初学者がたいてい陥る予想される質問、受講生が新たに気が付いた問題などもあるだろう。これらをまとめて、FAQ としてまとめておき、受講生に公開すると効果が高い。同じ質問があっても「まず FAQ を見てください」という、学習を促すことも可能となる。

3.3.2 学習状況と講義内容の評価について

情報セキュリティ教育における評価に関する事項として、受講者の学習状況の評価と効果測定について示す。

（1）学習内容の評価

学習状況の評価は、受講者において講義内容を習得できたかどうかの状況を評価することを目的として実施される。前者の習得状況の評価の手段としては、講義内容に基づく試験の実施や課題・レポートの提出などが用いられることが多い。どの手段が適切かは、講義の実施目的の相違などによって異なる。主な評価手段の特徴について以下に示すが、実際には複数の手段を組み合わせて用いることも多い。

（a）択一式試験

講義内容に関する問題を出題し、選択肢の中から正解を選んで記号で回答する。遠隔講義やビデオ教材、e ラーニングなどの場合のほか、教室に学習支援システムが用意されている場合などでは、機器の画面上で回答することもある。試験に要する時間は比較的短くて済むので、各講義の最後に小テストとして実施することもできる。また、採点も容易（自動化することも可能）であるため講師側の負荷が少ないメリットもある。単純な知識習得の有無だけでなく、問題を工夫することで受講者に考えさせるようにすることはある程度可能であるが、あくまで回答を事前に用意する必要があるため、受講者に探索的、発見的な思考を促すようなことはできない。

（b）記述式試験

講義内容に関する問題を出題し、受講者は文章を記述することで回答する。回答に求める文章のボリュームは試験時間に応じて、50 字以内、400 字以内などと指定することが多い。受講者における負荷は問題の内容によって異なり、講義内容や教材の抜粋に近い形で回答する問題の場合は負荷は軽いが、講義で紹介されていない事例を挙げたり、原因を分析した上で回答をもめるような問題の負荷は重くなる。採点は回答を全て読んだ上で行う必要があるため、採点に要する時間を講義とは別に確保する必要がある。講師以外の採点者を用いることも可能であるが、採点者の違いによる不公平が生ずることがないよう、明確な採点基準を設ける必要がある。

（c）レポート提出

（b）が試験のための時間内で回答するのに対し、レポート提出は提出期限のみを定め、受講者は自分の都合のよい時間・場所でレポートを作成することが異なる。問題の内容は（b）と特に異なるところはないが、時間制限が緩い分、分量は試験よりも多めに求められることが多い。ただし、あまりボリュームが多くなると、受講者に負荷をかけるとともに、採点の負荷も増えるため、受講者の属性（社会人／学生、学科、コース）や講義の目的（専門家育成、教養科目）などに配慮することが望ましい。

（２）講義の効果測定

（１）とは別に、講義自体の有効性を評価するため、講義の効果測定が行われることもある。効果測定の手段としては、受講者に講義前後で講義内容を対象とする同じレベルの試験を解答してもらい、正解率の受講前後での変化によって測定する方法や、受講者へのアンケート調査などにより、講義の有効性等を尋ねる方法がある。

３.３.３ 教育内容の更新について

情報セキュリティ分野は教育の対象となってから日が浅く、内容が確立されているとはいえない面がある。また、情報セキュリティ分野では技術の変化が速く、他の科目と比べると、定期的な講義内容の更新の必要性が高い。ここでは、こうした情報セキュリティ教育における教育内容の更新の考え方について述べる。

（１）更新の必要性の考え方

更新の必要性の有無を判断する際には、以下のような条件を考慮する必要がある。

- 既存の教育内容は現時点でも広く利用されているか。新しい技術やサービスに置き換わっていることはないか。
- 以前は知られておらず、教育内容にも反映されていない脅威が新たに生じていることはないか。
- 対策が普及して事故が減少した結果、既存の教育内容の重要性が低下していることはないか。

（２）更新における留意事項

本項の冒頭で情報セキュリティ分野は技術の変化が速いと述べたが、情報セキュリティ分野の中でも変化の速さには違いがあり、教育内容の更新の必要性も科目によって異なってくる。

比較的更新の必要性の高い項目は以下のようなものである。

- コンピュータウイルスやマルウェア等の脅威を説明する内容を含むもの
- ファイアウォール製品、IDS（Intrusion Detection System）製品、ルータ機器などのハードウェアの運用方法を学ぶもの（実習を含む）
- アプリケーションソフトウェアの使用方法を学ぶもの（実習を含む）
- 無線 LAN 関連技術
- バイオメトリクス技術（実装関連）

反対に、更新の必要性が低いのは、理論的、原理原則的な内容を多く含む以下のようなものとなる。

- 暗号理論
- PKI の基礎
- 情報セキュリティマネジメント
- 情報セキュリティポリシーとその運用
- リスク分析技法

以上のいずれにも含まれない科目や技術については、講師が動向に関心をもち、定期的に更新の必要性を判断することが望ましい。

３.４ 講座と教材に関するセルフチェックリスト

これまで示してきた内容をもとに、講師が情報セキュリティに関する講義を設計・準備する際に留意すべき事項をセルフチェックリストとしてとりまとめた。講義に関する各種の条件（目標、受講者、期間、環境等）に応じて、最適な内容はそれぞれ異なることから、ここに示した内容を満たす必要は決してないが、検討時の見落としなどを防ぐ目的で活用してほしい。

３.４.１ 講座に関するシナリオのチェックリスト

No.	分類	確認すべき事項	チェック欄
	講義の設計	講義の目的は明確か	
		講義の目標は明確か	
		前提知識となる科目との整合性を確認したか	
	受講者	受講者の構成を把握しているか	
		受講者の専門性、前提知識を把握しているか	
		受講者数に対して教室や設備が不足することはないか	
		受講者の質問を受ける態勢が用意されているか	
	シラバス	目的・目標を満足する内容か	
		講義スケジュールは現実的か	
		受講者に無理を強いる内容ではないか	
	評価	評価方法は講義の目的・目標に比して適切か	
		正確かつ公正な評価が可能な方法か	
		採点などの負荷が現実的か	
	（遠隔講義の場合）	使用設備は講義の要件を満足するか	
		使用回線は必要な容量が確保できるか	
		教室内のアシスタント職員の体制・準備は十分か	
	（録画形式の場合）	使用設備は講義の要件を満足するか	
		受講者との質疑の態勢が用意できているか	

３．４．２ 講座で利用する教材のチェックリスト

No.	分類	確認すべき事項	チェック欄
	教材の構成	シラバスに対応した内容か	
		全体の分量は適切か	
	教材の内容	１ページあたりの情報量が多すぎることはないか	
		文字が小さすぎることはないか	
		最新動向を踏まえて更新の必要性を判断したか	
		受講者が理解できない専門用語を使用していないか	
		引用等は著作権法の定める条件を満足しているか	
		参考文献や情報源の URL など、受講者が関連学習をしたい場合の補助情報が記載されているか	
		不明な場合の問い合わせ方法が記載されているか	
	（遠隔講義の場合）	利用する設備の条件に適合した実装となっているか（アニメーションを使用しない、等）	
	（録画形式の場合）	15 分を目安に内容を分割しているか	
		繰り返しの視聴に耐えうる内容となっているか	

４．おわりに

最後に、本手引書で触れることができなかった内容と、関連する取り組みについて示す。

４.１ 本手引書の未完・不備事項

こうした取り組みが初めてであることもあり、本手引書は情報セキュリティ教育を実施するために必要な知識やノウハウをすべて網羅できているわけではない。本来は手引書に反映すべきであるが、現状では盛り込まれていない内容として以下のような例が挙げられる。

- 受講者の属性に応じた関心を引きやすいトピックスとは
- 実習の際に生ずる可能性のあるトラブル事例とその対策方法
- 受講者に対して学習内容を違法行為等に利用しない誓約を求める場合の様式例

４.２ 本内容に関連する JNSA における取り組み

本手引書の記載事項の母体となったのは、JNSA におけるこれまでの教育実践事例で得た経験と、関連ワーキンググループにおける議論の内容である。ここでは、今後の活動予定を含めた JNSA における取り組みについて紹介する。

（１）JNSA におけるこれまでの取り組み

（ａ）「情報セキュリティに関するスキルマップ」の作成・改良

2002 年度に教育部会にワーキンググループを設置し、IPA（情報処理振興事業協会（当時））からの委託調査として「情報セキュリティプロフェッショナル育成に関する調査研究」を実施した[5]。このときワーキンググループにおける議論をもとに「情報セキュリティに関するスキルマップ」を提案し、以後 3 年にわたって改良を行っている。このスキルマップの構成要素に最新の情報を反映することにより、本手引書における「知識項目のリスト」が形成されている。

（ｂ）情報セキュリティ推奨教育の検討

2005 年度の活動として、国内における情報セキュリティ教育や資格の調査を行い、ワーキンググループによる検討成果を情報セキュリティに携わる人材の効率的な育成のロードマップとして報告書にとりまとめている[6]。

（ｃ）情報セキュリティ教育の実践

東京電機大学、工学院大学、岡山理科大学のご協力を得て、2004 年度より JNSA 会員企業に所属する情報セキュリティ分野の専門技術者を講師として、大学で実践的内容の教育を行う取り組みを実施している。

---

[5] 成果は IPA（独立行政法人情報処理推進機構）の Web サイトにて公開されている。
http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html ほか参照。
[6] http://www.jnsa.org/result/2005/20060601_edu.html

（2）今後の予定

JNSA では 2007 年度より、情報セキュリティ教育を担当する講師の育成のあり方について検討を行うことを予定している。ここで得られた知見については、今後本手引書の改定の際に反映することが期待される。

（3）JNSA の連絡先

本手引書に関する問い合わせや、JNSA における最新の活動状況を知りたい場合は、以下の Web サイトにアクセスしていただきたい。

- JNSA（特定非営利活動法人日本ネットワークセキュリティ協会）Web サイト
  http://www.jnsa.org/

付録１　知識項目のリスト

情報セキュリティ教育のカリキュラムの検討時に役立てていただくため、情報セキュリティ教育において教育対象となる知識項目を分野別に整理したものを示す。なお、本知識項目は以下の調査研究において作成した「情報セキュリティ教育のためのスキルマップ」を、最新の実情を考慮して一部修正したものである。

「情報セキュリティスキルマップ構築の調査研究」（情報処理推進機構（IPA）委託事業, 2004 年）
http://www.ipa.go.jp/security/fy15/reports/skillmap/index.html

（別表０）スキルマップの大分類

項番	大分類	
1	情報セキュリティマネジメント	
2	ネットワークインフラセキュリティ	
3	アプリケーションセキュリティ	Web
		電子メール
		DNS（Domain Name System）
4	OS セキュリティ	Unix
		Windows
		セキュア OS
5	ファイアーウォール	
6	侵入検知	
7	ウイルス	
8	セキュアプログラミング技法	
9	セキュリティ運用	
10	コンテンツセキュリティ	
11	認証	
12	PKI（Public Key Infrastructure）	
13	暗号	
14	電子署名	
15	不正アクセス手法	
16	法令・規格	

（別表１）情報セキュリティマネジメント

大分類	中分類	小分類	備考
情報セキュリティマネジメント	マネジメント技術	マネジメントプロセス	・セキュリティの3大要素 ・PDCA サイクル ・セキュリティポリシー
		マネジメントシステムの確立	・実施すべき項目（基本方針、リスクアセスメント等）
		マネジメントシステムの導入・運用	・実施すべき項目（対応計画、教育等）
		マネジメントシステムの監視・見直し	・実施すべき項目（有効性の見直し、内部監査等）
		マネジメントシステムの維持・改善	・実施すべき項目（改善策の実施等）
		情報セキュリティのドキュメント体系	・基本方針、対策基準、実施手順・規定類
	リスク分析技術	リスクアセスメント手法	・ベースラインアプローチ ・非形式的アプローチ ・詳細リスク分析 ・組み合わせアプローチ
		情報資産の調査・評価	・調査方法 ・評価基準
		脅威・脆弱性の調査	・脅威の分類・調査 ・脆弱性の把握・評価
		リスク評価	・定量的リスク評価 ・定性的リスク評価
		対策システムの検討・整理	・対策検討
	情報セキュリティポリシー	基本方針	・記述すべき項目（目的、適用範囲、組織と体制等）
		物理的対策	・物理的対策 ・サーバルームに関する対策 ・職場環境に関する対策 ・媒体の取り扱いに関する対策
		技術的対策	・ユーザ認証対策 ・アカウント管理対策 ・外部公開サーバに関する対策 ・サーバに関する対策 ・クライアント等に関する対策 ・ウイルス対策対策 ・ネットワーク構築対策 ・有線 LAN に関する対策 ・無線 LAN に関する対策 ・リモートアクセスサービス利用対策 ・専用線および VPN に関する対策
		人的対策	・電子メール対策対策 ・Web サービス対策対策 ・セキュリティ教育に関する対策 ・プライバシーに関する対策
		運用・管理対策	・システム維持に関する対策 ・システム監視に関する対策 ・セキュリティ情報収集及び配信対策 ・セキュリティインシデント報告・対応対策 ・監査対策 ・委託時の契約に関する対策 ・事業継続管理 ・罰則に関する対策 ・スタンダード更新手順 ・プロシージャ配布の対策

大分類	中分類	小分類	備考
	情報セキュリティ監査	情報セキュリティ監査の目的	・内部監査 ・外部監査 ・助言型監査 ・保証型監査
		情報セキュリティ監査手法	・監査の実施手順、評価方法 ・監査証跡の収集、分析手法 ・脆弱性検査手法、侵入テスト ・監査ツール
		監査報告書	・監査報告書の要件
	関連知識	情報セキュリティの関連制度	・ISMS 適合性評価制度 ・プライバシーマーク制度 ・情報セキュリティ監査制度
		情報セキュリティの標準化	・OECD セキュリティガイドライン ・JIS Q 15001 ・ISO/IEC 27001（JIS Q27001） ・ISO/IEC TR 13355（JIS Q13335）
		情報セキュリティの関連法規	大分類「法令・規格」参照
		セキュリティ監査（内部監査、外部監査）	・目的、実施手順、評価方法

（別表２）ネットワークインフラセキュリティ

大分類	中分類	小分類	備考
ネットワークインフラセキュリティ	ネットワーク設計技術	物理設計技術（物理設計時のセキュリティ対策）	・装置（HUB,Switch） ・通信経路
		論理設計技術（論理設計時のセキュリティ対策）	・ネットワークの分割・配置 ・アドレス体系
		ルーティング制御（ルーティングによるセキュリティ対策）	・スタティックルーティング ・ダイナミックルーティング
		アドレス変換（アドレス変換によるセキュリティ対策）	
		運用・管理	・IDS、IPS、SNMP、ログ等によるセキュリティ対策 ・Webアプリケーション・ファイアーウォール ・機器のセキュリティ対策
	ネットワークアクセスコントロール	パケットフィルタリング（アドレスとポート番号によるセキュリティ対策）	
		MAC(Media Access Control)アドレスフィルタリング	
		ポートベース VLAN（バーチャル LAN によるセキュリティ対策）	
	VPN(Virtual Private Network)	環境構築	・配置 ・暗号化方式 ・認証方式 ・アクセス制御
		IPSec による VPN 装置（ファイアーウォール含）	・利用形態 ・認証 ・暗号化 ・クライアント設定
		ルータによる VPN 装置	・利用形態 ・暗号化
		SSL による VPN 装置	・利用形態 ・認証 ・暗号化 ・利用サービス
	無線 LAN	認証・暗号化	・ESS-ID ・MAC アドレス ・IEEE802.1x ・WEP ・WPA ・IEEE802.11x
		その他	・ネットワーク分割 ・認証サーバとの連携
	ブルーフォース	ブルーフォースのセキュリティ	・
	セキュリティプロトコル	アプリケーション層	PGP(Pretty Good Privacy)
			S/MIME(Secure Multipurpose Internet Mail Extensions)
			SSH(Secure SHell)
		トランスポート層	SSL(Secure Socket Layer)/ TLS(Transport Layer Security)
			Socks
		ネットワーク層	IPSec
			IPinIP
		データリンク層	L2TP(Layer2 Tunneling Protocol)
			PPTP(Point-to-Point Tunneling Protocol)

大分類	中分類	小分類	備考
			L2F(Layer 2 Forwarding protocol)
			MPLS(Multi-Protocol Label Switch)
			MPOA(Multi-Protocol Over ATM)

（別表３）アプリケーションセキュリティ

大分類	中分類	小分類	備考
アプリケーション セキュリティ 【Web】	Web サーバに対する脅威	Web アプリケーションに対する攻撃	・バッファオーバーフロー ・クロスサイトスクリプティング ・パラメータ改ざん ・バックドアとデバッグオプション ・強制的ブラウズ ・セッション・ハイジャック／リプレイ ・パスの乗り越え ・SQL の挿入（SQL Injection） ・OS コマンドの挿入（OS Command Injection） ・クライアント側コメント ・エラーコード
		DoS(Denial Of Service)／DDoS (Distributed Denial Of Service)攻撃	
		ホームページの改竄	
		情報送信時の情報漏洩	
		Phishing フィッシング	
		プロキシサーバの不正利用	
	Web サーバのセキュリティ対策	アカウントの設定	・デフォルトアカウントの無効化、パスワードの設定等
		ファイル／ディレクトリのアクセス権の設定	
		ユーザ認証	・Basic 認証 ・Digest 認証 ・証明書を利用したクライアント認証
		Web アプリケーションファイアーウォール	
	Web サーバの運用	Web コンテンツのアップロード	・通信のセキュア化 ・アクセス制御の強化 ・コンテンツアップロードツール（Secure FTP、rsync、WebDAV）
		セキュリティパッチの適用	
		ログの収集と分析	
		Web サーバの監視	
		インシデント対策と体制	
	Web アプリケーション設計	クロスサイトスクリプティング対策	・入力チェック ・特殊文字のサニタイジング（無害化）
		CGI(Common Gateway Interface)	・インタプリタの格納場所 ・入力チェック ・サンプル CGI プログラムの削除
		Web のセッション管理	・乱数とハッシュによるセッション ID 生成 ・Cookie の利用の注意
	Web ブラウザのセキュリティ	Web ブラウザに対する脅威	・ウイルス感染 ・悪意あるプログラム、スクリプトのダウンロードと実行（Java、JavaScript、ActiveX 等） ・Cookie や個人情報の漏洩 ・ブラウザクラッシャー

大分類	中分類	小分類	備考
		Web ブラウザのセキュリティ対策	・OS、Web ブラウザに対するセキュリティパッチの適用 ・Web ブラウザのセキュリティ及びプライバシー設定（アクティブコンテンツ、Cookie、Java 等） ・フィッシング対策
	Web 関連プロトコルの基礎知識	HTTP(Hyper Text Transfer Protocol)	・リクエスト、レスポンスメッセージ（ヘッダ、ボディ） ・セッションレスプロトコル ・GET／POST メソッド
		SSL(Secure Socket Layer) / TLS(Transport Layer Security)	・鍵交換の仕組み ・証明書の取得 ・SSL アクセラレータの利用
		SOAP(Simple Object Access Protocol)	大分類「セキュアプログラミング技法」の中分類「XML」参照
アプリケーションセキュリティ【電子メール】	メールサーバに対する脅威	第三者不正中継（Third-Party Relay）	
		迷惑メール	
		Spam メール（UCE/UBE）	
		DoS(Denial Of Service)/DDoS (Distributed Denial Of Service)攻撃	
		盗聴	
		ユーザ情報の漏洩	
		ウイルス	
		代表的メールサーバアプリケーションの脆弱性	
	メールサーバのセキュリティ対策	第三者不正中継（Third-Party Relay）対策	・ブラックリスト（RBL）の利用 ・ブラックリスト（RBL）からの離脱 ・POP before SMTP ・SMTP Auth
		迷惑メール対策	・外部 Spam フィルタの利用
		Spam メール（UCE(Unsolicited Ccommercial E-mail)/ UBE(Unsolicited Bulk E-mail)）対策	
		ユーザ情報の漏洩	・コマンドの使用制限（VRFY/EXPN）
		代表的メールサーバアプリケーションの脆弱性対策	・セキュリティパッチの適用
	メールクライアントのセキュリティ	盗聴対策	・PGP ・S/MIME ・SSL
		ウイルス対策	
	メールサーバの運用	セキュリティパッチの適用	
		ログの収集と分析	
		メールサーバの監視	
		インシデント対策と体制	
アプリケーションセキュリティ【DNS(Domain Name System)】	DNS サーバに対する脅威	内部ネットワーク情報の漏洩	
		TCP53 番ポート（ゾーン転送）をついた攻撃	
		DNS キャッシュ攻撃（ポジションキャッシュ）	
		代表的 DNS サーバアプリケーションの脆弱性対策	・セキュリティパッチの適用
	DNS サーバセキュリティ対策と構成	内部ネットワークの隠蔽	・スプリット DNS（内部・外部 DNS の分割）

大分類	中分類	小分類	備考
		ゾーン転送対策	・ファイアーウォールでの対策 ・DNSSEC（暗号化） ・ゾーン転送を許可するサーバの登録
		DNS キャッシュ攻撃（ポジションキャッシュ）攻撃対策	・Dynamic Update による認証 ・再帰的問い合わせの制限 ・問い合わせを受けるホストの制限
	DNS サーバの運用	セキュリティパッチの適用	
		ログの収集と分析	
		メールサーバの監視	
		インシデント対策と体制	

（別表４）ＯＳセキュリティ

大分類	中分類	小分類	備考
OS セキュリティ【Unix】	ログ管理	インシデント対応	
		システムログ	
		ミドルウェアログ	
		アクセスログの解析	
		アクセスログの保管	
	イベント監視	サブジェクトイベント	・プロセスの生成/削除時などに出力
		オブジェクトイベント	・プログラムやデータ/ファイルの作成/削除時に出力
		インポート/エクスポートイベント	・プログラムやデータ/ファイルの挿入や変更および外部への書き出し時に出力
		アカウントイベント	・ユーザ追加やパスワード変更時などに出力
		セキュリティ違反イベント	・ログイン制御違反、ログイン失敗などによるユーザのロックアウト、同時ログイン数の制限違反などの際に出力
	パッチ適用管理	適切な Patch 適用状況と確認	
	サービスの管理	サービスの制限	・スーパーデーモン（inetd）と起動スクリプトによる起動の制限 ・r コマンド使用上の注意
		アクセス制御	・SSH(Secure Shell) ・TCP Wrappers によるアクセス制御 ・拡張アクセス制御
		一般ユーザでのデーモンの起動	
		ネットワークサービスとポート	
		不要なサービスの削除	
	ファイルシステム管理	ファイルシステム完全性検査	
		バックアップとリストア	
		暗号化ファイルシステム	
		デフォルトのパーミッション設定	・umask と必要に応じた権限付与の変更
		パーミッション設定ミスの検出	
		setuid/setgid ビット	
	アカウント管理	アカウント共有	・PAM（Plaggable Authentication Modules） ・NIS（Network Information Services） ・LDAP ・ディレクトリ
		シャドウファイル	・パスワードを保存する際に DES、MD5 等で暗号化する方法がある
		強いパスワード/弱いパスワード	・管理側でのパスワードポリシーの決定
		グループポリシー	
		ローカルセキュリティポリシー	
		アカウントの概念及び権限の分散	
OS セキュリティ【Windows】	構成・設定管理	Active Directory	
		CMDB(構成管理データベース)	・構成アイテム(CI)の識別
			・記録
			・追跡機能
			・レポート作成
		セキュリティポリシー	・ローカルセキュリティポリシー
			・ドメインコントローラーポリシー
			・パスワードポリシー
			・Kerberos ポリシー
			・グループポリシー
			・セキュリティテンプレート
		アクセスログの解析	

大分類	中分類	小分類	備考
		アクセスログの保管	
		アカウント毎の証明書管理	
	パッチ適用管理	Service Pack	
		Hotfix (Patch, QFE)	
		パッチ適用状況確認	・Baseline Security Analyzer
		パッチの一括・一斉配布	・Soiftware Update Services (SUS)
		WindowsUpdate	
	監査	ディレクトリアクセスの監査	
		プロセス追跡の監査	
		サービスの監査	
		ファイルとフォルダの監査	
		特権使用の監査	
		アカウント監査	・コンピュータアカウント、グループアカウント、ユーザアカウント
	ログ管理	インシデント対応	
		イベントログ	
		アクセスログの解析	
		アクセスログの保管	
	プロセス管理	ソフトウェア制限ポリシー	
	サービス管理	ネットワークサービスとポート	
		サービスのアクセス権	
		不要なサービスの削除	・管理ツール(サービス)
	ファイルシステム管理	暗号化ファイル(EFS)	
		アクセス制御リスト	
		アクセス権の継承	
		明示的な拒否権限	
		NTFS セキュリティアクセス	
	アカウント管理	強いパスワード/弱いパスワード	
		証明書認証	
		スマートカード認証	
		ActiveDirectory	
		ローカルアカウントとドメインアカウント	
		アカウントの概念及び権限の分散	
	ネットワーク保護	ポートフィルタ	
		接続元・先の制限	
		インターネット接続ファイアウィール	
OS セキュリティ【セキュア OS】	セキュア OS の基本機能	強制アクセス制御(MAC)	
		管理者特権の最小化(最小特権)	
	Trusted OS に求められる機能	ラベル式アクセス制御	・マルチレベルセキュリティ
		セキュアカーネル	・レファレンスモニタ
		デュアルロック	
	セキュア OS のアクセス制御モデル	ロールベースのアクセス制御モデル(RBAC)	
		Type Enforcement モデル	
		Bell-LaPadula モデル	
		Biba Protection モデル	
		Compartment Mode Workstation モデル	
	セキュア OS のプロテクション・プロファイル(PP)	CAPP	
		LSPP	
		SLOSPP	
		MLOSPP	

（別表５）ファイアーウォール

大分類	中分類	小分類	備考
ファイアーウォール	ファイアーウォールの導入・運用	ログ解析	・データマイニング ・侵入相関分析（対象となるイベントについて同一オブジェクトの関係、時間的関係、因果関係、社会的関係等の調査）
		侵入検知装置ログとの違い	・・採取したログの性質の違い
		DMZ 等構成の設計	・公開セグメント、非公開セグメントの区分け ・IP ルーティング
		フィルタリングルールの設計	・許可するサービス、拒否するサービス
		ゲートウエイ型とパーソナル型	・パーソナルファイアーウォール（フィルタリングと侵入検知）
	NAT(Network Address Translation)	StaticNAT	・1:1（グローバル IP:プライベート IP）の固定的アドレス変換
		DynamicNAT	・1:N（グローバル IP:プライベート IP）の動的アドレス変換
		IP マスカレード（NAPT）	・1:N（グローバル IP:プライベート IP）の動的アドレス変換
	ネットワークアクセスコントロール	Packet Filterling	・IP、TCP 層（IP、ポート番号等）でのアクセス制御
		Circuit Level Gateway	・トランスポート層でのアクセス制御
		Application Level Gateway	・アプリケーション層でのアクセス制御
		ステートフルインスペクション	・アプリケーション層でのアクセス制御

（別表６）侵入検知

大分類	中分類	小分類	備考
侵入検知	侵入検知システムの導入・運用	運用体制とインシデント対応	
		侵入検知システムの限界	・取りこぼし ・誤検知 ・FalseNegative と FalsePositive ・未知の攻撃手法（Misuse） ・検知の回避方法 ・IDS への攻撃（Stick 攻撃） ・暗号環境の未検出
		ログ解析	・データマイニング ・侵入相関分析（対象となるイベントについて同一オブジェクトの関係、時間的関係、因果関係、社会的関係等の調査）
		ファイアーウォールログとの違い	・採取したログの性質の違い
	侵入検知システムの機能	管理コンソールへの告知	
		防御機能 （TCP リセット/ルータ・ファイアーウォールでの遮断）	
		パターンマッチング方法	シグネチャ
		プロミスキャスモード	
		異常検出	・定量分析（しきい値モデル） ・統計的手法（しきい値学習モデル） ・クラスタ分析 ・ルールベースアプローチ ・ニューラルネットワーク
	検出アルゴリズム	不正検出	・パターンマッチング
		System Integrity Verifiers	
	検出方法	ログファイルモニター	
		ネットワークモニタリング	
		ホスト型	
	侵入検知システム	ネットワーク型	
		ハイブリッド型	
		ハニーポッド	
		改竄検知	
	侵入防御システム		

（別表７）ウイルス

大分類	中分類	小分類	備考
ウイルス	管理体制	報告告知体制	
	感染後のポリシー	ウイルス検出ソフトの設置管理	
		駆除方法と手順	
	予防ポリシー	社内体制	
		流行の傾向と予測	
		他アプリケーションとの連携	
		イントラネットの構築	
		システム管理	
		定義ファイル管理	
		アンチウイルスソフトの配置	
	発病	ウイルスの複合化	・感染経路の複合化（メール、共有ファイル） ・発病内容の複合化
		バックドアの作成	Root kit
		改竄	・レジストリ、データ
		情報発信	・パスワード、データのメールへの添付送信
		外部攻撃	・DoS 攻撃 ・DDoS 攻撃
		メール発信	・大量のメール発信
		破壊活動	・ファイルの破損 ・ディスクのフォーマット
	検出方法と駆除	予知検出	・亜種、ウイルスらしきプログラムの検出
		メールに対するコンテンツフィルタ	
		ウイルスの誤検知	
		駆除方法	・隔離 ・駆除 ・削除 ・アクセス拒否
		スキャン方式の種類	・オンアクセス、オンデマンド等
		定義ファイル	
		検出方法の種類	・パターンマッチング ・割り込み監視 ・ヒューリスティック ・整合性チェック ・メモリ検出 等
	感染	ウイルスの自己防衛機能	・ステルス機能 ・ポリモフィック（ミューテーション）機能
		脆弱性の利用	・Windows やその他のアプリケーションの脆弱点を利用してウイルスに感染させる。代表的なものとしては、バッファーオーバーフロー、フォーマット違反等
		兆候	・処理速度が落ちる ・関係ない情報が表示される ・ネットのトラフィックが高くなる 等

大分類	中分類	小分類	備考
		手段（媒体）	・メール ・共有フォルダ ・FD（外部記憶デバイス類） ・CD-ROM（外部メディア類） ・送り込み ・Web ・チャット ・ファイルのダウンロード ・ダイレクトアクション
		経路	・FD（外部記憶デバイス類） ・CD-ROM（外部メディア類） ・インターネット ・イントラネット
	種類	ウイルスの機能構成	・自己伝播機能 ・潜伏機能 ・発病機能
		デマウイルス	
		ジョークウイルス	
		不必要なプログラム	・Spyware、キーロガー等、コンピュータのデータを無断で入手する為のソフト ・マルウエア、アドウエア等 ・ボットネット
		マクロウイルス	
		トロイの木馬	
		ワーム	
		スクリプト	・Java スクリプト型 ・ActiveX 型 ・VBS
		ウイルス	・ファイル感染型 ・ブートセクター感染型 ・ファイルおよびブートセクター等に感染等

（別表８）セキュアプログラミング技法

大分類	中分類	小分類	備考
セキュアプログラミング技法	プログラミング言語とツール	アセンブラ、コンパイラ、インタープリタ、クロスアセンブラ、クロスコンパイラ、非手続き言語、スクリプト言語、機械語、オブジェクト指向言語	
		アプリケーションエラーハンドリング（入出力検証）	正常系、正常処理 非正常系、異常系、異常処理 デバッグ機能
		トランザクション管理	2-phase commit
			データベースのロールバック
		バックアップと冗長性の管理	
		一時ファイルのセキュリティ	
		データ辞書	
		チェックポイント/リスタート	
		バックドア	デバックオプション
		フィールドの初期設定と再利用	アプリケーションとデータベースの統合
	Web アプリケーション	クロスサイトスクリプティング	
		Web ページとユーザ認証	
		クエリストリングからの情報漏洩	
		Web フォームの選択項目の危険性	
		hidden の危険性	
		ユーザインターフェースデザイン	・2 回のパスワード入力等
	データベース	SQL 引数のチェック	
		スクリプトへの DB パスワードの埋め込み	
		データベースとアクセス権限	
		エラーメッセージの表示	・エラーSQL 文の表示等
	アプリケーション全般	パスワードの取り扱い	
		入力値のチェック方法	
		エラーメッセージからの情報漏洩	
		ログ	
		特権処理の局所化	
		ソースコードチェックツール	
		再利用と部品化	
		モジュールの分割設計	
		バッファーオーバーフロー	
		ミドルウエアの役割と利用	
	XML(Extensible Markup Language)	XML 署名	
		XML 暗号	
		XMIアクセスコントロール	
		SOAP(Simple Object Access Protocol)メッセージの取扱	
	PHP(Hypertext Preprocessor)	危険な関数	
		セキュリティホール	
		サニタイジングの対策	
	JAVA	危険なクラス	
		カプセル化	
		シリアル化と情報漏洩	
		クラス継承となりすまし	

大分類	中分類	小分類	備考
		JAVA のアサーション	
		synchronized とレースコンディション	
	Perl	ファイルオープン	
		危険な関数	
		Taint モード	
	VB/ASP	Request へのアクセス	
		仮想パスのマッピング	
		セッションタイムアウト	
	C/C++	危険な関数	
		文字列処理の際の危険	
		サブシェルの呼び出し	
		メモリリーク	
		C++デストラクタ	
	UNIX	シンボリックリンクの悪用	
		PATH 変数/子プロセスのすり替え	
		setuid	
		fork の利用	
		レースコンディション	
		core ファイルから情報漏洩	
		安全なパス名	
		テンポラリファイルからの情報漏洩	
	コンパイラ・仮想マシン	最適化による脆弱化	
		動作オプションによるオーバーフロー防止	
		出力コードの特性	
	Windows	安全なパス名	
		プロセス間通信	
		プロセス間通信オブジェクトのアクセス権	
		特権の管理	
		偽装アカウント	
		制限アカウント	
		レジストリ管理・アクセス権	
		テンポラリファイルからの情報漏洩	
		プロセス、スレッドのアクセス権	
		NTFS(New Technology File System)ストリーム	
		NTFS のセキュリティ機能	
		CORBA (Common Object Request Broker Architecture)	
		DCOM (Distributed Component Object Model)	
		EJB (Java Beans and Enterprise Java Beans)	
		SOAP (Simple Object Access Protocol)	
		カプセル化	
		オブジェクト再利用のリスク	
	データベースとデータウェア保管庫の脆弱性、リスク、防護	データベースの種類	階層型
			リレーショナル
			オブジェクト指向
		データベースとアプリケーションのインターフェース	ODBC (Open Database Connectivity)

大分類	中分類	小分類	備考
			OLE DB (Object Linking and Embedding Database)
			ADO (Active X Data Objects)
			JDBC (Java Database Connectivity)
			XML (eXtensive Markup Language)
		データベース、データマート、データ倉庫	
		メタデータ	
		DBMS (Database Management Systems)	
		ユーザーと管理者のためのアクセス制御(職務の分離)	
		バックアップと復旧	
		エラーの取り扱い	
		効率的処理	
		錠の管理	
		ACID テスト	Atomicity
			Consistency
			Isolation
			Durability
		保管された情報の防護 vs 移動中の情報の防護	
		データベースの完全性のリスク／管理	
		SQL(Structured Query Language)	

（別表９）セキュリティ運用

大分類	中分類	小分類	備考
セキュリティ運用	定常運用時のセキュリティ確保	事前設定	・ログファイルの記録／更新設定 ・制御・設定ツール(SNMP 他)
		モニタリング	・異常アカウントの有無 ・異常プロセスの有無 ・システムの負荷の状況 ・記録装置の空き容量の変化 ・構成管理 ・変更管理
		セキュリティホール対策	・セキュリティホールの影響評価 ・設定変更による被害回避 ・パッチの効果と副作用 ・パッチの適用可否の判断基準（目的、対象） ・対策の有効性の検証法
		定常作業	・バックアップ・リストアの設定／実施 ・アカウント管理 ・パスワード管理
		ユーザ対応等	・ユーザへのアナウンス ・ユーザ教育（セキュリティ啓発） ・ルール違反対策（発見、対応）
	インシデント対応（異常時対応）	異常検知	・IDS/IPS からのアラーム（大分類「IDS」参照） ・ウイルス等の検知対応 ・モニタリングによる異常検知 ・ユーザからの異常報告 ・誤検知かどうかの判断
		原因究明・トラブルシューティング	・異常要因の切り分け ・特徴の分析（再現性、影響範囲等） ・対策の実施
		緊急時対応	・緊急事態かどうかの判断（被害、影響の評価） ・運用継続の可否 ・被害の拡大防止（ネットワークの切り離し等） ・代替措置 ・関係組織への報告 ・緊急時対応の訓練
	コンピュータ・フォレンジックス	コンピュータ・フォレンジックスの成立要件	・目的 ・収集すべき証拠情報の種類 ・証拠性の担保方法 ・他のセキュリティ要件（機密性、プライバシ保護等）との整合性確保 ・RFC3227
		実装手段・ツール	・OS 機能の利用 ・商用製品、フリーソフトウェア
	運用関連情報（脆弱性情報・対策情報・攻撃情報・被害情報）	情報源の種類と特徴	・ソフトウェア、システムベンダからの情報 ・セキュリティベンダからの情報 ・公的機関からの情報
		脆弱性情報の意味と分析	・重要性、緊急性の分類 ・情報の信頼性の判断

（別表１０）コンテンツセキュリティ

大分類	中分類	小分類	備考
情報の保護	情報の格付け	格付けの基準	・機密性（Sensitivity） ・重要度（漏えい時、消失時、利用不可能時の影響の大きさ） ・個人情報、プライバシー情報
		格付けの方法	・政府機関統一基準における分類
	保護において留意すべき情報の特徴	要機密情報	・個人情報、プライバシー情報 ・内部情報、非公開情報
		要保全情報	・証跡、ログファイル
		要安定情報	・ライフラインとして提供される情報
	情報の取扱場面（ライフサイクル）	情報の作成、入手	・媒体の変換
		情報の利用	
		情報の移送	
		情報の提供	
		情報の消去	
	機密性対策	暗号化	
		アクセス制御	・情報フロー制御
		漏えい源の特定	・電子透かし技術の応用
	完全性対策	ハッシュ関数による改ざん検知	
		電子署名	
		バックアップ	
	可用性対策	サーバ多重化	
		負荷分散（ロードバランシング）	
コンテンツ利用の制御	不正コピー対策	不正コピーの脅威	
		不正コピー防止技術	
		権利管理技術の基本概念	
	権利管理技術（DRM）の要素技術	暗号技術	
		認証技術	
		鍵管理技術	
		電子透かし技術	
		リニューアル技術	
	権利記述言語の標準化	XrML（eXtensible rights Markup Language）	
		ODRL（Open Digital Rights Language）	
	法的要件	著作権法	
		不正競争防止法	
電子透かし	電子透かしの基本概念	電子透かしの埋め込みと検出	
		不可視性	
		ロバスト性	
		完全性	
	電子透かしの方式	知覚モデルの応用	
		周波数マスキング	
		周波数領域への埋め込み	
		位相への埋め込み	
		スペクトル拡散法	
		統計的方法	
	電子透かしの応用形態	著作者の識別	
		所有権の証明	
		改竄防止	
		コピー制御（機器制御）	
		フィンガープリンティング	
		コンテンツの認証	
		放送の監視	

（別表１１）認証

大分類	中分類	小分類	備考
認証	ID 管理と認証	ID 管理およびビジネスプロセスとの整合	Existence(存在) – ユニークな ID を作成し、定義、権限の割り当て、会社のリソースとサービスの使用のために、その ID を整備するプロセス。
			Context(状況) – 物理的位置、組織的位置、役割、日時などのパラメータを含む、ID の現在の動作環境を把握する。たとえば、ある人物のキャリアが変われば、レベル、権限、責任も変わる。これらの変更を把握することにより、システムはユーザのニーズの変化に対応することができる。
			Provisioning(供給) – ユーザが業務を行う上で必要とするツールを提供する。人物のデジタルコンテクストに基づき、システムはビジネスルールに則って、その人物に必要なリソースを提供する。
			Ownership(所有権) – ID 情報が組織の複数のシステムに複製されている場合に、有効とする ID 情報を決定する。
	パスワード認証	固定パスワード	
		ワンタイムパスワード	
		パスワードの暗号化	
	バイオメトリック認証	指紋	
		静脈	
		音声	
		虹彩	
		網膜	
		掌紋	
		ペンの速度、筆圧	
		顔認証	
		DNA	
		行動パターン	
	認証デバイス	IC カード	
		USB トークン	
		耐クローン	
		耐タンパ	・NIST FIPS140-1、FIPS140-2 ・耐タンパ性に対する解析法(破壊型解析法(プローブ解析)) ・非破壊型解析法(故障利用解析、タイミング解析、電力解析)
	認証プロトコル	AKE(Authenticated Key Exchange)	・PAKE(パスワード認証) ・証明書による認証
		Kerberos	
		RADIUS	
		SSH(Secure SHell)	・パスワード認証 ・秘密鍵認証
	Web 認証	Cookie	
		SSL(Secure Socket Layer)認証	・パスワード認証 ・秘密鍵認証
	システム認証	サーバ間認証	・IP アドレスによる認証 ・MAC アドレスによる認証
		クライアント認証	・
	シングルサインオン	アクセス制御	・ポリシーベース ・ロールベース
		セッション管理	
		ログ管理	

大分類	中分類	小分類	備考
		構成	・エージェント型 ・リバースプロキシ型
	その他	人間の知覚を利用	・CAPTCHA

（別表１２）PKI(Public Key Infrastructure)

大分類	中分類	小分類	備考
PKI(Public Key Infrastructure)	PKI の利用	セキュアタイムスタンプ	長期署名
		公証	
		電子 CP(コマーシャルペーパ)	
		認可機関	
		権限管理と PKI との統合	
		アプリケーションでの利用	・Web サービス ・SSL ・暗号メール ・IPSec ・コード署名 ・XML 署名
		利用方法の規格化	・暗号通信（SSL、TLS、SET、SECE、Ipsec、WAP、SSH） ・暗号メールとデジタル署名（S/MIME） ・データの暗号化とデジタル署名（Code Signing、XML、PKCS#7 と CMS） ・暗号インターフェース（PKCS#11、GSS、GSS-IDUP） ・タイムスタンプ（Time Stamp Protocol）
	証明書と認証	証明書の構造と意味	
		証明書の有効性検証	
		証明書のフォーマット	
		OID(オブジェクト識別子)	
		ポリシー機関	
		認証機関と登録機関	
		鍵と証明書のライフサイクル管理	
		属性証明書	・属性証明書の意味 ・属性証明書の利用方法
	証明書失効	CRL(証明書失効リスト)	
		ARL(認証機関失効リスト)	
		OCSP(オンライン証明書ステータスプロトコル)	・OCSP の後継として SCVP 等の標準仕様が策定されつつある
	信頼モデル	認証機関の階層構造	
		相互認証	
		ブリッジ CA	
		認証パスの構築	
		認証パスの有効性確認	
		インターオペラビリティ	
	契約モデル	クローズモデル	
		ネットワークモデル	
		オープンモデル	
	記述とデータ方式	ASN.1 と BER(Basic Encoding Rules) 、 DER(Distinguished Encoding Rules) 、PEM(Privacy Enhanced Mail)	
		Base64 エンコーディング	
	規格	公開鍵証明書の規格(RFC3280、X.509)	
		PKCS(Public Key Cryptography Standards)	
		CRL の規格	
		証明書と CRL の配布点	
		CMP(Certificate Management Protocol)	

大分類	中分類	小分類	備考
		属性証明書の規格	
	公開リポジトリ	ディレクトリサーバの利用	
	認証局(CA)の構築と運用	認証局の運用形態	
		認証局の構築	
		秘密鍵管理(HSMN、アクセラレータ)	
		認証局運用規程	
		証明書ポリシー	
	法的枠組み	電子署名及び認証業務に関する法律(電子署名・認証法)	
	PKI の要素技術	認証機関	
		証明書リポジトリ	
		証明書失効	
		鍵のバックアップと回復	
		自動鍵更新	
		鍵履歴	
		相互認証	
		否認防止と署名	
		タイムスタンプ	
	PKI が提供するサービス	認証、署名、否認防止	
		データの完全性	
		データの秘匿性	

（別表１３）暗号

大分類	中分類	小分類	備考
暗号	暗号方式概説	暗号の基礎	・基本知識と用語
		暗号方式の分類	・公開鍵暗号と共通鍵暗号 ・ブロック暗号とストリーム暗号
	公開鍵暗号	公開鍵暗号の原理	・数学的原理と暗号になる理由と強度の保障（素因数分解、離散対数問題、組み合わせ複雑性、等） ・暗号化と復号化 ・鍵生成と登録
		公開鍵暗号で実現できる機能	・秘匿 ・鍵配送 ・署名 ・親展
		共通鍵暗号のアルゴリズム	・RSA ・RSA-OAEP(Optimal Asymmetric Encryption Padding) ・ELGamal
		Diffie-Hellman 鍵配送	
		楕円曲線上の演算を利用した暗号法	主な暗号法： ・楕円 ElGamal ・楕円 Diffie-Hellman 鍵配送 ・ペアリングを使った方式
	共通鍵暗号	共通鍵暗号の原理	・置換（転置）、換字、非線形撹乱 ・ブロック暗号とその原理 ・ストリーム暗号とその原理 ・強度と脆弱性 ・ブロック暗号の利用モード
		共通鍵暗号のアルゴリズム	・DES(Data Encryption Standard ((3DES) ・AES(Advanced Encryption Standard) ・DSA(Digital Signature Algorithm) ・Misty
		非同期式ストリーム暗号	
		同期式ストリーム暗号	
	ハッシュ関数	ハッシュ関数の原理	・ハッシュ関数の定義 ・ハッシュ関数が情報セキュリティにもたらす機能
		ハッシュ関数の構成法	
		専用ハッシュ関数	主な関数例： ・MD4、MD5 ・RIPEMD128、RIPEMD160 ・SHA1 ・SHA256、SHA384、SHA512
	暗号用乱数	暗号用乱数の原理	・統計的乱数性 ・長周期性 ・線形複雑度
		真性乱数	
		擬似乱数	
	鍵管理	鍵共有方式	
		鍵生成方式	
		(公開鍵暗号方式の）秘密鍵の保管方法	
		共有鍵の保管方式	
		秘密情報分散保管法	
		鍵管理サーバ方式	

大分類	中分類	小分類	備考
		KPS(Key Predistribution System)方式	
	ゼロ知識証明	ゼロ知識証明の原理	・ゼロ知識と対話証明の定義と実現の原理 ・ゼロ知識証明のプロトコル
		ゼロ知識証明プロトコル	・プロトコルの例: ・平方剰余問題のゼロ知識対話証明 ・グラフ非同型問題のゼロ知識対話証明
		ゼロ知識証明の応用	・なりすましの脅威を排除した個人認証、等
	その他の暗号方式	MAC(Message Authentication Code)	
		量子暗号	量子揺らぎを用いた暗号 量子鍵配送方式
		秘密分散(Secret Sharing)	
	暗号解読・強度評価	暗号解読と強度評価	
		暗号解読と暗号攻撃	暗号文単独攻撃 既知平文攻撃 選択平文攻撃 選択暗号文攻撃
		全数探索型攻撃法	・鍵全数探索攻撃法 ・テーブル参照法(辞書攻撃) ・タイムメモリートレードオフ法
		ショートカット法	・差分攻撃法 ・線形攻撃法 ・高階差分攻撃法 ・SQUARE 攻撃法 ・補間攻撃法 ・中間一致攻撃法 ・関連鍵攻撃法
		サイドチャネル攻撃法	・タイミング攻撃法 ・故障利用攻撃法 ・電力攻撃法 ・電磁波解析攻撃(テンペスト)
		代数攻撃	・Berkelamp-Massey アルゴリズム
		暗号技術評価プロジェクト(CRYPTREC)	CRYPTREC「電子政府推奨暗号リスト」参照

（別表１４）電子署名

大分類	中分類	小分類	備考
電子署名	必要性と利点	秘密鍵利用による本人性の保証	・秘密鍵を利用するため、本人性を保証
		ハッシュ関数の利用	・ハッシュ値をとるため、平文そのものより暗号時間を短縮 ・ハッシュ関数利用により、入力サイズに関わらず、出力サイズが一定
		署名検証の容易さ	・署名生成者の公開鍵は公開されているため、誰でも署名検証可能、等
	電子署名の利用	コードサイニング	
		XML(Extensible Markup Language)署名(規格、利用)	
		改竄防止	
		否認防止	
	電子署名の要素技術	電子署名署名に利用される暗号アルゴリズム	・RSA ・DSA ・ESIGN ・ECDSA ・SFLASH ・ペアリング方式
		電子署名に利用されるハッシュ関数	・SHA-1、SHA-2、SHA-256、、SHA-384、SHA512 ・RIPEMD-160 ・MD2、MD5
	電子署名の仕組み	署名作成方法	
		署名検証方法	
		メッセージダイジェスト	
		デジタル封筒	

（別表１５）不正アクセス手法

大分類	中分類	小分類	備考
不正アクセス手法	遠隔不正侵入・操作	バッファーオーバーフローを悪用した攻撃	・リモートバッファーオーバーフロー ・ローカルバッファーオーバーフロー
		Format String Bug	
		Frame Pointer Error	
		Spyware	
		不正アクセスの隠蔽（ログ改竄）	
		クロスサイトスプリクティング	・アプリケーションセキュリティ【Web】を参照
		セッション・ハイジャック	
		パスの乗り越え	
		SQL の挿入（SQL Injection）	
		OS コマンドの挿入（OS Command Injection）	
		DNS ゾーン転送（TCP53 番）攻撃	・アプリケーションセキュリティ【DNS】を参照
		DNS キャシュポイズニング	
		バックドア	・古典的タイプ ・ファイル変更型 ・シェルポートバインド ・LKMタイプ
		ボットネット	・スパイウエア
		なりすまし	・ユーザ ID、パスワードでのなりすまし ・IP アドレスによるなりすまし
		トロイの木馬	
		ロジック爆弾	
	サービスの停止	メール爆弾	
		DoS(Denial Of Service)攻撃	
		DDoS(Distributed Denial Of Service)攻撃	
		ブラウザクラッシャー	・アプリケーションセキュリティ【Web】を参照
	盗聴行為	Sniffing	
		WireTAP	
		無線LAN（802.11 系）の傍受	・SSID の危険性 ・WEB ・ステルス機能（ビーコンの停止）
		アナログ無線の傍受	
	偵察行為	TCP(Transmission Control Protocol)スキャン	・TCP 接続スキャン ・TCP SYN スキャン ・TCP FIN スキャン ・TCP クリスマスツリースキャン ・TCP NULL スキャン
		UDP(User Datagram Protocol)スキャン	
	情報収集	パスワードクラック	
	古典的不正アクセス技法	ソーシャルエンジニアリング	
		ピギーバック	
		スーパーザップ	
		スキャベンジング	
		サラミ	

（別表１６）法令・規格

大分類	中分類	小分類	備考
法令・規格	基準・指針・ガイドライン等	情報システム安全対策基準	・経済産業省制定
		コンピュータウイルス対策基準	・経済産業省制定
		コンピュータ不正アクセス対策基準	・経済産業省制定
		システム監査基準	・経済産業省制定
		ソフトウェア管理ガイドライン	・経済産業省制定
		情報通信ネットワーク安全・信頼性基準	・総務省制定
		情報システム安全対策指針	・国家公安委員会制定
		行政情報システムの安全対策指針	・行政情報システム各省庁連絡会議幹事会了承
		情報セキュリティポリシーに関するガイドライン	・情報セキュリティ対策推進会議決定
		情報セキュリティ監査制度関連基準・ガイドライン	・経済産業省制定
		情報セキュリティマネジメントシステム(ISMS)認証基準	・Ver.2.0 を 2003 年 4 月に(財)日本情報処理開発協会制定
		政府機関統一基準	・内閣官房情報セキュリティセンター
		重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針	・内閣官房情報セキュリティセンター
	法令	電子署名及び認証業務に関する法律(電子署名・認証法)	
		特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダー責任法）	
		不正アクセス行為の禁止等に関する法律	
		電子商取引に関する準則	
		個人情報の保護に関する法律（個人情報保護法）	
		著作権法	
		高度情報通信ネットワーク社会形成基本法(IT 基本法)	
	国際標準規格	ISO(国際標準化機構)/IEC(国際電気標準会議)セキュリティ関連規格	重要な規格例: ・ISO/IEC 15408（JIS X5070） ・ISO/IEC 27001（JIS Q27001） ・ISO/IEC TR13335）
		IETF(Internet Engineering Task Force)セキュリティ関連規格	
		ITU(国際電気通信連合)セキュリティ関連規格	
		FIPS(連邦政府情報処理規格)140	
	国際ガイドライン	OECD(経済協力開発機構)セキュリティ関連ガイドライン	・情報システム及びネットワークのセキュリティのためのガイドライン ・プライバシー保護と個人データの国際流通についてのガイドライン ・暗号政策に関するガイドライン」
		欧州連合「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」	
		欧州評議会「サイバー犯罪条約」	

付録２　サンプル教材

ここに示すサンプル教材は、手引書におけるカリキュラム案【基礎編】の実施時に使用する教材を作成する際の参考として頂くため、手引書作成ワーキンググループのメンバーがこれまでに作成した教材をカリキュラムに合わせて整理したものである。

本教材の利用について

本教材は以下の条件のもとで、教材作成の参考としてご利用いただくことができます。

- 本サンプル教材の著作権は、引用部を除き、JNSA 教育部会 手引書作成ワーキンググループのメンバーであるやすだなおと園田道夫に帰属します。
- 本教材の全部又は一部を営利目的として利用することはできません。
- その他利用に関して不明な点がある場合は、以下の連絡先にご相談ください。

  特定非営利活動法人 日本ネットワークセキュリティ協会 事務局

  〒136-0075　東京都江東区新砂 1-6-35　NOF 東陽町ビル１階

  TEL：03-5633-6061　　FAX：03-5633-6062　　E-Mail：sec@jnsa.org

情報セキュリティ概論

（基礎編第１回に相当）

1

なぜ情報セキュリティを学ぶのか？

- セキュリティの確保は、情報処理の要である
- ITセキュリティは総合的な「合わせ技」なので、断片的な知識では不十分である
- 過去の知見を生かし、新しい道具や技術を使いこなすことで、次の世代のアイディアが生まれる

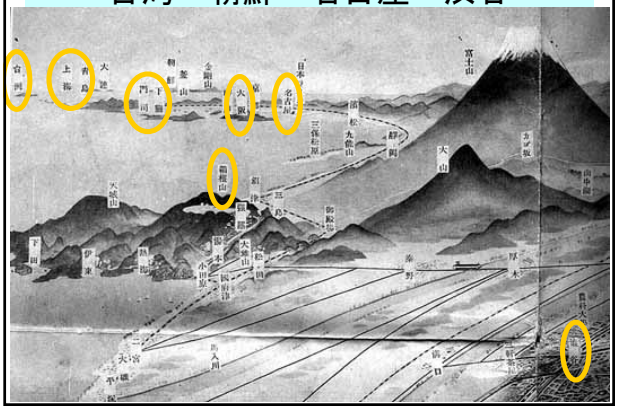
2

古い東京の鳥瞰図

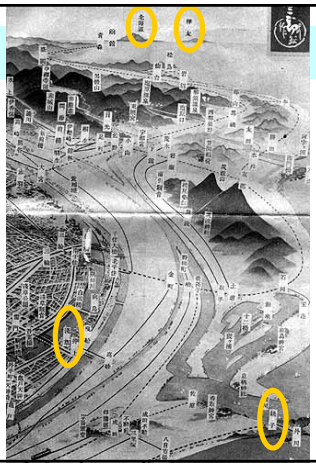
吉田初三郎版「東京鳥瞰図」（『少年倶楽部』16巻11号（1929年）付録）
「探検コム」http://www.tanken.com/tokyocyokan.html から引用

3

台湾ー朝鮮ー名古屋ー渋谷



樺太ー北海道ー銚子ー浅草

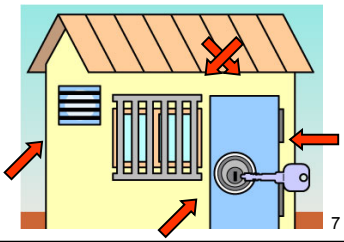


5

皇居付近

建築設計などとも考え方は同じ

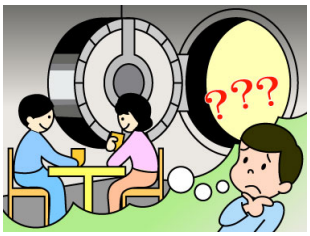
- 構造や強度に問題はないか
- 間取りや使いやすさは大丈夫か
- 全体のバランスはどうか



7

建築設計などとも考え方は同じ

- 銀行の大金庫は安全だけど…
- 手段ではなく目的が大切
- 経済的なリスク評価と管理が重要



8

技術的な攻撃

・ネットワークを使った攻撃
- 脆弱性を利用した侵入
- Bugや目的外の機能利用による副作用

・動機の変化
- 愉快犯、怨恨犯
- 誇示、警告の勇み足
- 金銭目的
- 特定の標的
- テロ、政治目的

9

脆弱性 【vulnerability】

・コンピュータやネットワークなどの情報システムにおいて、第三者が保安上の脅威となる行為(システムの乗っ取りや機密情報の漏洩など)に利用できる可能性のあるシステム上の欠陥や仕様上の問題点。
(IT用語辞典 e-Words http://e-words.jp/)

10

脆弱性 【vulnerability】

・脆弱性とは、ソフトウエア製品やウェブアプリケーション等におけるセキュリティ上の問題箇所です。コンピュータ不正アクセスやコンピュータウイルス等により、この問題の箇所が攻撃されることで、そのソフトウエア製品やウェブアプリケーションの本来の機能や性能を損なう原因となり得るものをいいます。

11

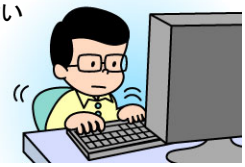
脆弱性をみつけたら

出典:IPAセキュリティセンター　脆弱性関連情報に関する届出について
http://www.jpa.go.jp/

12

攻撃する人(1)

・ Hackerクラス
  - プログラムを自分で作れる
  - 脆弱性情報を使って攻撃手法を考えられる
  - CPUやOSの特徴や弱点を理解でき知っている
  - 証拠をできるだけ残さない



13

攻撃する人(2)

・ スクリプトキディ 【script kiddy】
  - 公開されている簡単に利用できるクラッキングツールを使って、興味本位の不正アクセスをする人たち。きちんとした技術を持っていないことが多い。ほとんどのクラッカーがこれだといわれている

14

騙しの手段

・ ITが目的ではなく、手段として利用
・ 有史以前からある、人間の性(さが)
・ 基本的に金銭目的
・ オレオレ詐欺のパソコン版
・ 相手は仕事であり、生活をかけている
・ ソーシャルエンジニアリング

15

心理的な脅威

・ 人類の有史以前から存在していたはず
・ 目的は金銭の搾取(詐欺)

オレオレ詐欺
振り込め詐欺
つぎつぎ詐欺
架空請求
ワンクリック詐欺
フィッシング(ファーミング)

- 手口を知っていることで注意を喚起できる
- リテラシー教育が必要
- 普段からニュースなどを注意して聞く
- 自己防衛をするように努める

16

YAHOO と YAFOO

17

YAHOO と YAFOO

本物の「YAHOO！」サイトの代わりに「YAFOO！」という偽物サイトが作られた

検索エンジンで「ヤフー」を探して偽物サイトに誘導された人も多かったようだ

18

YAHOO と YAFOO

今までは、不審なメールを受け取った時は検索エンジン等で確認しましょうといっていた対策の裏を見事に掛かれた

大阪の会社員が著作権法違反と不正アクセス禁止法違反容疑で逮捕されたが、詐欺被害が無くても偽物サイトを作っただけで摘発されたことが注目される

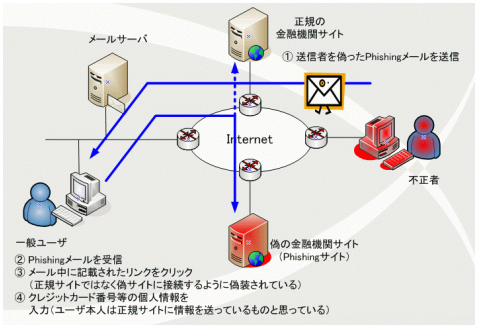
19

ワンクリック請求

- それらしいことが書いてあるけど…
- 公開情報か先方が作った情報だけ
- ISPは請求には協力しない
- でも、始めて見ると、ドキッとする！

20

フィッシングの仕掛け



出典：フィッシング対策協議会
http://www.antiphishing.jp/

21

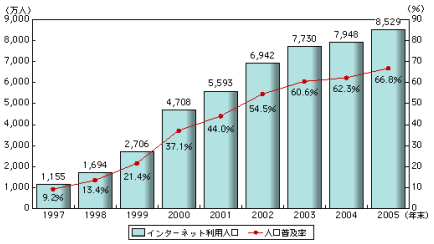
詐欺師のIT化

- 騙す方は、騙される人間が使っている道具について、より以上の知識を蓄えている
- 証拠や手口がコンピュータを使うことによって見え難くなる
- 一般の人には郵便や電話と比べ何が起こっているかが理解し難い
  - →相手の思う壺
- 愉快犯や怨恨というよりも、職業として詐欺を行っている
- 会社組織のような構造を持っていて、利益追求をしている
- 相手は本気でお金を巻き上げようとしているのである
- 「お客さん」を探すためにインターネットなどの最新技術も十分活用している

インターネットで詐欺をすることが目的というよりは、インターネットという手段を利用することにより、より簡単に目的が達成できることに目を付けられた。

22

インターネットの世帯利用人口普及率



※ インターネット利用者数（推計）は、6歳以上で、過去1年間に、インターネットを利用したことがある者を対象として行った本調査の結果からの推計値。インターネット接続機器については、パソコン、携帯電話・PHS、携帯情報端末、ゲーム機等あらゆるものを含み（当該機器を所有しているか否かは問わない。）、利用目的等についても、個人的な利用、仕事上の利用、学校での利用等あらゆるものを含む。
※ 人口普及率（推計）は、本調査で推計したインターネット利用人口8,529万人を、2005年10月の全人口推計値1億2,771万人（国立社会保障・人口問題研究所が国の将来人口推計（中位推計）値として採したもの
※ 1997～2000年末までの数値は「通信白書」から抜粋。2001～2005年末の数値は、通信利用動向調査における推計値
※ 調査対象年齢については、1999年調査までは15歳～69歳であったが、その後の高齢者及び小中学生の利用増加を踏まえ、2000年調査は15歳～79歳、2001年調査以降は6歳以上に拡大したため、これらの調査結果相互間では厳密な比較はできない

総務省「通信利用動向調査（世帯編）」により作成

出典：総務省「情報通信白書　平成18年版」

23

IT化される社会基盤

- サイバーテロ（対国家）
- 基幹産業のサーバの重要性
- 一般市民が使う業務サーバ
- 個人の情報発信
  - Winnyのように目的外の利用で問題が起こった
  - 技術での対応と、利用方法の基礎的注意

24

Winny問題

- 安部官房長官（2006/3/15当時）が記者会見で使わないよう呼びかけた
- 作者への刑事責任（裁判中）
  - 著作権侵害幇助が中心
- プロバイダによる遮断
  - 技術的に外形からの判断は難しい
  - 総務省（総合通信基盤局）が許されないと発表
- 将来の情報共有技術の先駆け
  - 問題は、制御手段が実装されていなかった

25

最近の傾向

広域・不特定多数

⇓

限定・特定狙い撃ち

多くの人に見せびらかしたい

⇓

確実に金目の物を手に入れる

26

何を思い浮かべますか？

- Winnyのこと
- 個人情報保護法のこと
- ウィルスやワームのこと
- 不正プログラムのこと
- 法律との関係のこと
- どうすればいいの？

情報漏洩の例について、
小テストを行います。

27

情報漏洩の要因

項目	主な内容
脆弱性	・管理者権限を奪取される ・リモートから認証なしで利用できる
攻撃手段	・ウイルス・ワーム、ボット、他
対策状況	・パッチなし、回避策あり
内部犯行	・権限を持っている人間の加担
盗難・遺失	・PCなどの盗難、置き忘れ
詐欺	・人間の弱みをついて情報を詐取

28

漏洩する内容

- 個人情報
  - プライベート情報、個人を特定できる情報
- 企業情報
  - 上場（経営）、特許（研究開発）、人事
- 医療情報
  - カルテ、X線写真、診療データ
- 防衛情報
  - ミサイル、配備情報、装備情報、他
- その他

29

AOL［America Online］（米国）

AOLの社員が9，300万人分の顧客情報をスパムメール送信業者に売却。（2004年）

- 米国の顧客情報漏えいとしては過去最大規模
- 顧客ID（スクリーンネーム）、電子メールアドレス、電話番号、郵便番号(ZIPコード)、クレジットカード名が含まれる。
- 信用情報は別のデータベースで管理していたため、漏えいした情報の中にクレジットカード番号やパスワードは含まれていない。
- AOLジャパンによると、日本のユーザの顧客情報は米国側で管理しており、流出した可能性を否定できないとしている。

米連邦警察は、同社のソフトウェア技術者を、個人情報を盗んだ疑いで逮捕。

- 同技術者(24才)は、すでに懲戒免職処分されている。
- 2003年にほかの社員のパスワードを用いてデータベースに侵入し、顧客情報を入手した。
- この個人情報は、2回に分けてスパムメール送信業者に、総額8万4，000ドル(約924万円)で販売された。

30

続AOL[America Online]（米国）

2006年7月末に、2000万件の検索クエリが漏洩した

- AOLを訴える集団訴訟がカリフォルニア州で起きた。
- 原告代表は、AOLが『電気通信におけるプライバシ保護法』および一連のカリフォルニア州公正事業法に違反したと主張。
- 全米規模の集団訴訟となっている
- 原告は、2004年1月1日から現在までの間に、同意なく検索クエリが公開されてしまった米国の全AOL会員と定義された。
- 賠償額は、カリフォルニア州地域の原告は4，0000ドル。それ以外の原告は1，000ドル。
- AOLに対して、検索クエリの記録を中止し、記録済みのものを全て廃棄するよう求めている。
- AOLの広報担当者は「これは完全なミスであり、この件について狼狽と腹立たしさを感じている」と述べている。

31

台湾の個人情報流出

台湾南部の高雄市の警察当局は、約1，500万人分の個人情報を違法に収集し、詐欺グループなどに売り渡していた犯罪組織を摘発、容疑者20名を逮捕した。

警察当局は、ニセの抽選券を多数の住民に送りつけていた詐欺集団を摘発、この過程で容疑者らの違法な名簿販売をつかみ、詐欺の疑いで逮捕した。容疑者らは出版物などに「個人情報買います」と広告を掲載し、金融機関や電話会社の社員から、氏名、住所や電話番号、収入などの情報を1人につき2～16円相当で購入していた。

容疑者らは、これらの個人情報を情報量に応じて1人につき3～32円で、別の詐欺グループなどに販売していた。

既に500万人分の個人情報を販売し、1億6，000万円以上の利益を得ていたという。

流出した個人情報は人口の3分の2に相当する。（2004年4月）

32

アッカの個人情報流出

アッカの顧客情報流出、元社員が名簿業者に売却していた～背任罪が確定

アッカ・ネットワークスは18日、2004年3月に公表したADSLサービスの顧客情報流出について、同社の元社員が顧客情報を名簿業者に売却していたことを明らかにした。東京簡易裁判所では3月30日、元社員に対して背任罪の判決を言い渡し、罰金50万円を科した。
アッカは2004年3月、ADSLサービスの顧客情報が流出したことを公表。これまで33万9，177人分の個人情報流出が確認されており、同年8月20日には被疑者不詳として、警視庁丸の内署に被害届を提出していた。

個人情報を売却した社員の罰金は50万円でしかない。
アッカがこの件の対策に費やした経費はどれくらいか？
直接経費、間接経費、潜在経費
情報流出事件の事前対策が重要なのは、法の裁きを受けることではなく、メディアで報道されることによる社会からの信頼を失ってしまうこと。

⇒信頼喪失を金銭に換算するとどれほどのものになるだろうか。

出典：Impress Watch 「アッカの顧客情報流出、元社員が名簿業者に売却していた」
http://internet.watch.impress.co.jp/

33

宇治市の例

宇治市住民基本台帳データ大量漏洩事件控訴審判決

本件は，控訴人がその管理に係る住民基本台帳のデータを使用して乳幼児検診システムを開発することを企図し，その開発業務を民間業者に委託したところ，再々委託先のアルバイトの従業員が上記データを不正にコピーしてこれを名簿販売業者に販売し，同業者が更に上記データを他に販売するなどしたことに関して，控訴人の住民である被控訴人らが，上記データの流出により精神的苦痛を被ったと主張して，控訴人に対し，国家賠償法1条又は民法715条（使用者責任）に基づき，損害賠償金（慰謝料及び弁護士費用）の支払を求めた事案である。
被控訴人らの慰謝料としては，1人当たり1万円と認めるのが相当である。
弁護士費用としては，被控訴人ら1人当たり5，000円と認めるのが相当である。

→実際に訴訟したのは3名

出典：Cyber Law Japan 「宇治市住民基本台帳データ大量漏洩事件控訴審判決」
http://www.law.co.jp/

34

YahooBBの例

ヤフーBB運営会社に賠償命令――個人情報流出で1人6，000円

インターネット接続サービス「ヤフーBB」の顧客情報流出問題で、大阪市の会員ら5人が「精神的被害を受けた」として、運営業者BBテクノロジー（旧ソフトバンクBB）とヤフーに損害賠償を求めた訴訟の判決で、大阪地裁の山下郁夫裁判長は19日、「不正アクセス防止の措置を怠った」としてBB社の過失を認定し、1人当たり6，000円の支払いを命じた。
BB社が全会員に金券500円を配り謝罪したことなどから、慰謝料を1人5，000円、弁護士費用を同1，000円と算定。
原告側弁護団によると、インターネットでの個人情報流出で企業の責任を認めた初の判決。同サービスの運営にかかわるヤフーについては「顧客情報はBB社とは別に管理しており、賠償責任を負わない」として、原告の請求を棄却した。
山下裁判長は争点となったBB社のセキュリティー対策について、(1)特定のコンピューター以外からのサーバーへの接続を認めない(2)定期的なパスワード変更――などの対策がとられていなかった点を指摘。「多数の個人情報を保管する事業者として注意義務違反があった」とした。

実際に訴訟したのは5名

出典：NIKKEI.NET「ヤフーBB運営会社に賠償命令」 http://www.nikkei.co.jp/

35

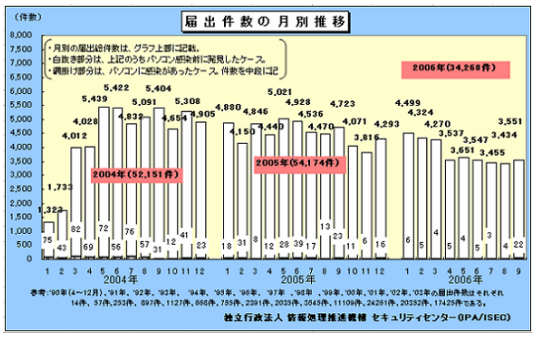
不正アクセスの分類

許可されていないアクセスを行うプログラム類

- ウイルス・ワーム類
- スパイウエア
- フィッシング
- ボットネット

36

ウイルスのIPAへの届出件数



出典： IPAセキュリティセンター 「コンピュータウイルスに関する届出について」 http://www.ipa.go.jp/

昔のウイルスは楽しめた^^)

- 音楽を演奏する。
- 異常なメッセージを表示する。
- 画面表示が崩れる。

→作者の自己顕示を目的とするものが多かった

最近のウイルスは潜伏して姿を見せない

国内初、スパイウェア作成者逮捕　ネット銀不正送金で

ジャパンネット銀行の顧客PCがスパイウェアに感染

- パスワードなどを盗み取られて不正送金の被害にあった
- 警視庁ハイテク犯罪対策総合センターは1月26日までに、不正アクセス禁止法違反と電子計算機使用詐欺の疑いで、元IT関連企業社員の31歳の男を逮捕した。
- スパイウェア開発者の逮捕は国内初。

- 同法違反で起訴されている別の男と共謀して昨年6月、ジャパンネット銀行に口座を持つ企業に、スパイウェアを添付した電子メールを送信してIDやパスワードを盗み取り、同社の口座から約21万円を自分たちの口座に送金した疑い。

出典： IT media 「国内初、スパイウェア作成者逮捕　ネット銀不正送金で」
http://www.itmedia.co.jp/news/

スパイウェアによる不正送金被害が拡大、みずほ銀行やジャパンネット銀行でも

イーバンク銀行だけでなく、みずほ銀行やジャパンネット銀行でも、顧客PCがスパイウェアに感染し、パスワードなどを盗み取られて不正送金の被害に遭う被害が生じている。

- スパイウェア(キーロガー)に感染
- パスワードなどを盗み取られて不正送金の被害
- イーバンク銀行、みずほ銀行、ジャパンネット銀行でも出ている

インターネットカフェへの仕掛けから、直接ユーザーに知られないようPCに感染し、IDやパスワードといった重要なデータを盗み取るスパイウェアに移った。
ジャパンネット銀行によると、少なくとも「数名」の顧客が身に覚えのない振込出金により被害に遭っているという。
一連の事件を踏まえて警視庁では捜査に着手している。

- 不審なソフトを安易にダウンロードしたり、心当たりのないメールおよび添付ファイルを安易に開かない
- ウイルス対策ソフトを利用する
- 口座取引明細を確認し、見に覚えのない取引が発見された場合は銀行に連絡する

出典： IT media
「スパイウェアによる不正送金被害が拡大、みずほ銀行やジャパンネット銀行でも」
http://www.itmedia.co.jp/news/

フィッシングって何？

1. 本来の設置者のWebに似せた偽Web に誘導し、ID、個人情報を入力させて、盗むもの
   ※誘導手段は、メール、検索エンジン、Web等
2. キーロガーやトロイの木馬等により、PC内のデータや入力した個人情報を盗むもの
   ※キーロガー等はできるだけ知られずに設置される
3. 不正行為を行う目的で、電子商取引を行う業者が取引を行った人の個人情報を盗む(流用する)もの

※「住民票コード占い」ってしってますか？
名前と住民票コードを入力させて占います！
というWebですが、「あなたは無防備すぎます！」
という警告が出てきたりします。

フィッシング被害

- 目的は金銭詐取
- 警察庁の発表資料によると:
  - フィッシングにより詐取したID/PWの行方
    - 全件数:　約5,800件
    - 詐欺:　約2,300件
    - 販売:　約700件
    - 未使用:　約2,800件
- フィッシングでID/PWを詐取しても行為自体を罰する法律がない
  ⇒売ったり、使えば当然犯罪

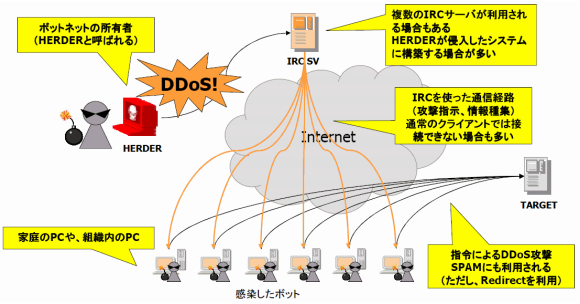
ボットネットって何？

Botnet = パソコンをロボットのように操り、ある（悪意の）目的のために一斉に動作されるインターネット上のコンピュータ群

- 感染後にウイルスなどのように決まった動きをするのではなく、攻撃者が自由に操作できる
- DoS攻撃、スパムメール、フィッシングメールの送信、パソコン内のプログラム実行やファイルの送受信等が可能
- フィッシングサイトが開設される
- IRC(Internet Relay Chat)を利用して攻撃者との交信を行う
- キーボードの入力を記録し、IDやパスワードを取得する機能を備えた種類も存在する

43

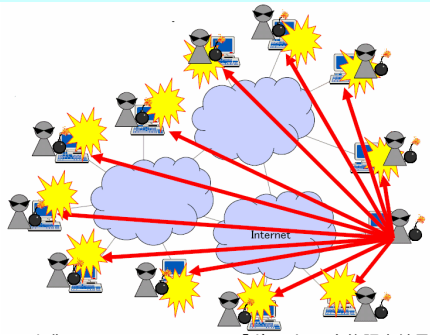
ボットネットって何？



出典： Telecom-ISAC Japan「ボットネット実態調査結果」
http://www.digitalforensic.jp/Resume2005/koyama.pdf

44

ボットネットって何？



出典： Telecom-ISAC Japan「ボットネット実態調査結果」
http://www.digitalforensic.jp/Resume2005/koyama.pdf

45

ボットネットの特徴

コントロール可能な分散型攻撃システム

- 従来のワームやウイルス等：
  - 無差別に不特定多数に対する脅威
  - 深刻な脅威が広がるまでに一定の時間を必要とする
- ボットネットを使った攻撃
  - 特定の相手を選択的に攻撃することが可能
  - 瞬時に攻撃を開始することが可能
  - ソースコードがインターネット上で容易に手に入る
  - ウイルス対策ソフトなどでは対応しきれない

2004年調査	既知		未知		合計
	数	割合	数	割合	
検体数	35,741	90.3%	3,850	9.7%	39,591
種類	1,014	23.4%	3,324	76.6%	4,338

出典： JPCERT/CC「ボットネットの概要」 http://www.jpcert.or.jp/

46

脆弱性 【vulnerability】

脆弱性とは、ソフトウエア製品やウェブアプリケーション等におけるセキュリティ上の問題箇所です。
コンピュータ不正アクセスやコンピュータウイルス等により、この問題の箇所が攻撃されることで、そのソフトウエア製品やウェブアプリケーションの本来の機能や性能を損なう原因となり得るものをいいます。

出典：IPAセキュリティセンター 「脆弱性関連情報に関する届出について」
http://www.jpa.go.jp/

47

攻撃コードが出現するまでの期間短縮が進んだ時代

MSのパッチ情報	脆弱性公開日	猶予期間	攻撃コード
MS00-078 Microsoft VMによるActiveXコンポーネントの制御	2000/4/14 (MS00-025)	17ヶ月	2001/9/18 Nimda
MS02-039 SQL server (UDP1434)	2002/7/25	6ヶ月	2003/1/25 SQLSlammer
MS03-026 RPCバッファオーバーラン	2003/7/17	1ヶ月	2003/8/11 MSBlaster
MS03-039 RPCSSバッファオーバーラン	2003/9/11	4日	2003/9/15 Welchia
MS03-049 Workstationサービスのバッファオーバーラン	2003/11/12	2日	2003/11/14 WSRShell
MS04-007 ASN.1 Library バッファオーバーフロー	2004/2/11	4ヶ月	2003/9/30 (OpenSSLで発見)

急速に短縮化

48

ゼロデイ攻撃が日常茶飯事に

ゼロデイアタック（Zero-day Attack）とは、新しいセキュリティホールの情報やセキュリティパッチが公開される前に、そのセキュリティホールに対して行われる攻撃のことです。

出典：セコムトラストシステムズのよくわかる情報セキュリティ用語辞典
http://www.secomtrust.net/secword/

49

PowerPointの未知の脆弱性狙うゼロデイ攻撃

8月の月例パッチで修復された脆弱性を狙うマルウェアが相次いで登場しているが、今度は、Microsoft PowerPointに存在する未知の脆弱性を狙ったゼロデイ攻撃が発見された。

イスラエルのBeyond Securityが運営しているセキュリティ情報サイト、SecuriTeamは8月19日、PowerPointの脆弱性を攻撃するトロイの木馬「TROJ_MDROPPER.BH」と「TROJ_SMALL.CMZ」が発見されたとブログを通じて警告を発した。

Microsoftは8月8日に、Microsoft Officeの脆弱性を修正する「MS06-048」も含む月例パッチをリリースしている。しかしSecuriTeamの情報によると、これらのトロイの木馬はMS06-048とは異なる「未知の、パッチが提供されていない脆弱性」を悪用するものだという。しかもこの脆弱性は、任意のコードの実行につながる危険性の高いものだ。

実際に発見されたトロイの木馬、TROJ_MDROPPER.BHは、PowerPoint形式の文書を装っている。このファイルを開くだけで脆 弱性が悪用され、Windowsのテンポラリフォルダに、もう1つのマルウェアであるTROJ_SMALL.CMZが作成される。TROJ_SMALL.CMZは外部のサイトにアクセスし、さらに別のマルウェアなどをダウンロードしようと試みるという。Trend Microの情報によると、Windows XPやWindows Server 2003のほか、Windows 98／ME、NT、2000などがこのトロイの木馬の影響を受けるということだ。

「このように伝えるのは残念なことだが、この脆弱性が、情報を詐取するためのターゲットを絞った攻撃に使われていたとすれば、攻撃者はすでにそうした情報を手に入れているだろう」（SecuriTeam）

Microsoftからは、この未知の脆弱性に関する情報は公開されていない。SecuriTeamでも、どのバージョンのPowerPointが影響を受けるかについては「情報がない」としている。

正式にパッチなどが提供されるまでの対処策は、ウイルス対策ソフトの定義ファイルを最新の状態に保つこと。そして、電子メールやWeb、インスタントメッセンジャーなどを通じて受け取った、出元が保証できないファイルは開かないよう注意することに尽きる。

出典：ITmedia 「PowerPointの未知の脆弱性狙うゼロデイ攻撃」
http://www.itmedia.co.jp/

ITmedia Inc. 50

Windowsの脆弱性を突く攻撃コードが公開に
―― 専門家ら、パッチの適用を呼びかけ ――

Windowsの脆弱性を突く攻撃コードがインターネットに公開され、これを悪用した攻撃が起きる可能性が高まっている。

ファイルやプリンタ共有に関するWindowsコンポーネントの脆弱性を突いた攻撃コードが公開された。
Microsoftは米国時間8月8日、セキュリティ情報MS06-40の中でこの問題に関する修正パッチを提供している。
Microsoftは8月11日のセキュリティアドバイザリで、この脆弱性はすべてのバージョンのWindowsに影響するが、公開された攻撃コードはWindows2000とWindows XP Service Pack1でのみ動くと説明した。
セキュリティ専門家は、3年前に大流行したBlasterのようなワームが出現し、この脆弱性を利用する可能性があると指摘する。
Microsoftのセキュリティプログラムマネージャー Christopher Budd氏は8月9日「今のところ、悪質な活動が広がっている兆候は見られない。普段から行っている通り、緊急対策チームでは現在も悪意ある活動の監視を 続けている」とMicrosoftのブログで述べた。

セキュリティ企業 iDefenseのRapid Response TeamディレクターKen Dunham氏は「インターネットの世界では、違法な収入を得ることを目的に、目立たないように攻撃を仕掛ける傾向がみられる。フルオートマチックの派手 な攻撃を仕掛けるワームはすたれつつある」という。
従来の攻撃に代わって、トロイの木馬やセミオートマチックの悪意あるコードによる攻撃がWindowsの脆弱性を突くことになるだろうと、同氏は予測する。
Dunham氏はインターネットに接続するコンピュータすべてに、できるだけ速やかにパッチを当てるべきだと付け加えた。

出典：シーネットネットワークスジャパン 「Windowsの脆弱性を突く攻撃コードが公開に」
http://japan.cnet.com/

51

ソーシャル・エンジニアリングって何？

- ソーシャル・エンジニアリングは、人間の心理的な隙をついて、個人が持つ秘密情報を聞き出す方法のこと。ソーシャル・ワークとも呼称される
- 元来は、コンピュータ用語で、コンピュータ本体に被害を加えることなく、パスワードを入手し不正に侵入（クラッキング）するのが目的。この意味で使用される場合はソーシャルハッキング、ソーシャルクラッキングとも言う
- フィッシングは最近の代表例

出典：フリー百科事典『ウィキペディア（Wikipedia）』
http://ja.wikipedia.org/wiki/

52

良くある手口

- システム管理者などと身分を詐称してパスワードを聞きだす
- 本体を操作する人の後ろに立ち、パスワード入力の際のキーボード（もしくは画面）を凝視する
- パスワードが書かれた紙を盗み見る
- ゴミ箱などに捨てられた書類や廃棄PC（ディスク）等を拾う
- スキミングされたコピーカードの暗証番号が、ゴルフ場のロッカーの暗証番号と同じだった［2005年1月］
- 整体院のロッカーを勝手に開けてスキミングし、会員情報から生年月日や電話番号などで暗証番号を類推した［2005年8月］
- オレオレ詐欺で、振込みをさせる
- 架空請求（ワンクリック請求）で振込ませる

53

情報セキュリティマネジメント（1）

（基礎編第2回に相当）

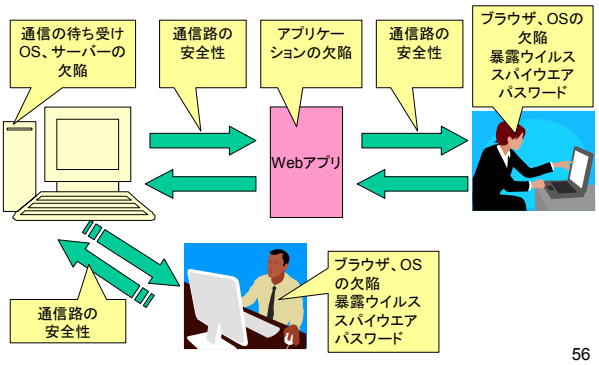
54

ライフサイクル

- 情報が生まれてから消えるまでのライフサイクル
- どこで作り出されて、どこに保管されて、どのように管理されるのか？

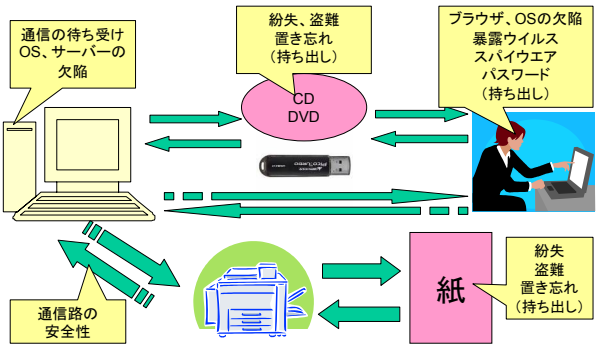
55

データベースサーバーをめぐるリスク



56

データベースサーバーをめぐるリスク



57

代表的なセキュリティ対策とカバレッジ

よくある対策	カバー範囲
ファイアウォール	①
通信の暗号化	②、④、⑥
ハードディスクの暗号化	③
パスワード強度の向上	
持ち出し手順の作成	

ライフサイクルで漏れているところは無いか？

58

「逃げる」手もある

- 保険
- 放置プレイ
- 取扱いを止める
- システムを「削除」する

最終的な目標は何か？

59

そもそも、その前に

- 資産的価値がある情報（複数）のプライオリティを考える
  - 付帯的情報をごっちゃにしない
- プライオリティのベースはビジネスインパクトがわかりやすい

60

GMITS（ISO/IEC TR13335）にあるプライオリティ付けの方法論

		リスクの程度								
	脅威の程度	低			中			高		
	脆弱性の程度	低	中	高	低	中	高	低	中	高
資源の価値	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

「資源の価値」とは、保護対象の資源に対するセキュリティ問題発生時の影響度合いであり、言い換えるとビジネスインパクトとでも言うべきものである。数値が4になると顧客情報や企業秘密情報などが対象となり、漏洩や破壊などされた場合には企業活動そのものに影響を及ぼすものである。
「脆弱性の程度」とは、資源に対するセキュリティ問題発生の可能性であり、どの程度保護対策がなされている状態であるか評価する。
「脅威の程度」とは脅威が発生する度合いで評価するもので、年に数回以下の場合は低いが月に数回以上発生する場合は高くなる。

61

対策の評価

- 対策はカバレッジの通りに効果を発揮するのか？

62

ルールを決めたはいいけれど

- 漏洩事件はルール違反から始まっている
- なぜ違反してしまうのか？

持ち出し、持ち込みルールの要件

①情報資産の重要度分類などに応じた「持ち出し」の制限
②「持ち出し」「持ち込み」の手順（「持ち出し」「持ち込み」の承認や記録など）
③「持ち込み」を許可する私物機器・媒体や、持ち込んだ場合の管理方法（電子ファイルを「持ち込む」場合はウイルスチェックを行う。持ち込んだ私物のパソコンは、それ単体での利用は許可するが、社内ネットワークには接続させないなど）

63

違反の背景

- 仕事だから良いだろう
- 出張なので仕方がない
- 商売取れれば文句はないだろう
- ウイルススキャンしてからなら大丈夫だろう
- 家族と別アカウントなので大丈夫だろう

64

背景の背景

- 守れるルールだったのか？
- 会社の外で仕事をしない、ということが可能なのか？
- 持ち出さない、ということが可能なのか？
- ニーズを圧殺していないか？
- 代替案を用意していないのではないか？

放置自転車の理論

65

ルールの検証

- 「承認」が必要→承認者が不在の場合？
- 持ち出し記録簿に記入→「性善説ルール」
- 使用後は即削除→「性善説ルール」
- 私物のパソコンにコピーしない→「性善説ルール」

- フィードバック？

66

代替案の検討と比較

- 持ち出し可とし、安全な環境（ノートパソコン）で使う
  - 「検疫」せずに済む環境
- コピーできなくしてしまう
- 持ち出すならファイルを暗号化（強制）
  - 暗号化ファイルシステム

67

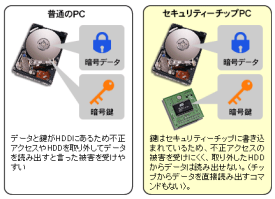
ノートパソコンのセキュリティ対策

よくある

- 指紋認証
- BIOSパスワード
- ハードディスクの暗号化
- ハードディスクパスワード
- 暗号化ファイルシステム（EFS）
- ファイルの暗号化

68

最強のノートパソコン



指紋認証＋BIOSパスワード＋ハードディスクの暗号化。

もちろんWindowsOSのログオンパスワードも。

考えられるすべてのセキュリティ機能を備えたノートパソコン。

69

最強のノートパソコンの検証

- 指紋認証
- BIOSパスワード
- ハードディスクの暗号化
- WindowsOSのパスワード

実質を伴う「セキュリティ対策」はなにか？

70

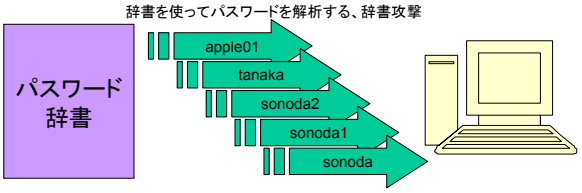
WindowsOSパスワードの問題点

- 14文字以下は脆弱な暗号化（LANMANハッシュ）
  - 大文字のみ！
  - 10文字で2の10乗（1024）倍
- ソルト（塩）が固定！
  - いつも同じ味の料理ができてしまう
- Windows でパスワードの LAN Manger ハッシュが Active Directory とローカル SAM データベースに保存されないようにする方法
  - http://support.microsoft.com/default.aspx?scid=kb;ja;299656#XSLTH4148121124120121120120

71

辞書攻撃・ブルートフォース攻撃

辞書を使ってパスワードを解析する、辞書攻撃



文字を片っ端から組み合わせる総当たり（ブルートフォース）攻撃の組み合わせ数

文字種類	10文字の場合
英字	1
英数字	23倍
英数字＋記号	10267倍

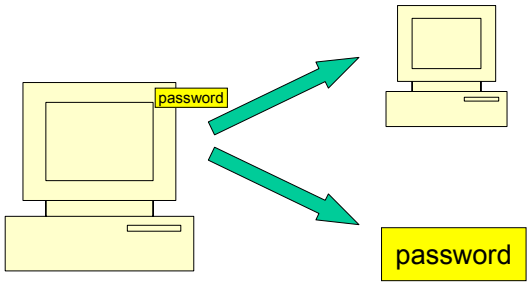
72

パスワードの理想形

- 長い
- 複雑
- 三ヶ月毎、いやもっと短いサイクルで変更することが望ましい

73

「鍵」の管理が重要



74

ノートパソコンのセキュリティ対策

実質役立つ

- ログオンしにくくする
  - WindowsOSのパスワード強化
  - USBキーによるログオン制限
- 中身を直接覗かれなくする
  - ハードディスク暗号化
  - ハードディスクパスワード

75

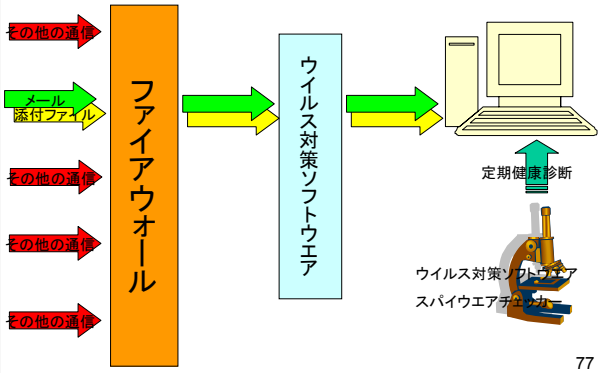
一般的なセキュリティ対策

- WindowsUpdate（OSのアップデート）
- ウイルス対策ソフトウエア
- ファイアウォール

みんな自動になっている

76

一般的なセキュリティ対策



77

ウイルス対策ソフトウエアの限界

- 「42日間の調査で収集した3705種（31864件）の検体のうち、検出できなかったものが2983種類（3537件）」
  - http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20050828/166941/
  - http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20050829/167035/

78

ウイルスの感染経路

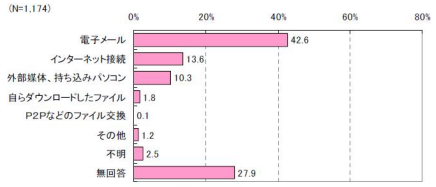


図 2.4-23 想定されるコンピュータウイルスの感染経路

IPA(情報処理推進機構)「国内におけるコンピュータウイルス被害状況調査」[2005年]より

http://www.ipa.go.jp/security/fy17/reports/virus-survey/documents/2005_virus_domestic.pdf

79

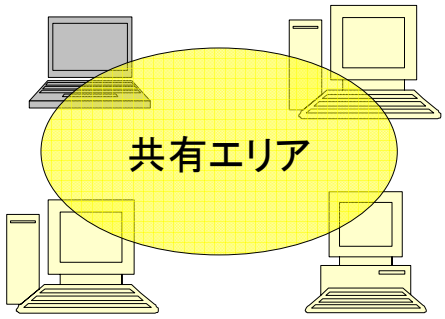
暴露ウイルスの脅威

- Webサーバーになってしまう！
- マイドキュメントなどをアーカイブ化し、Winnyネットワークにアップしてしまう！

もともとは
どんな「アクション」が問題なのか？

80

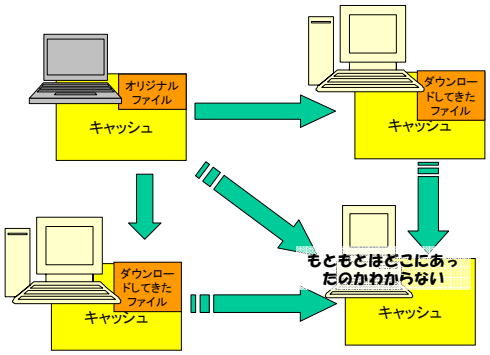
Winnyによるファイル交換とは



Winnyファイル交換ネットワークは、巨大な仮想ディスクである

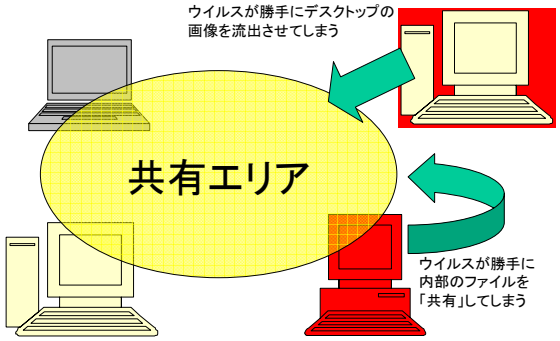
81

Winnyファイル交換ネットワークの匿名性



82

非自発的なファイルの「共有」



83

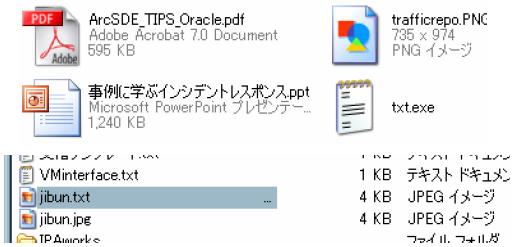
Winnyユーザーのそもそもの危険

- ウイルスチェックを行うタイミングがどこにも無い！
  - ファイル(データ)が入り込む際にチェックが行われない
- ファイルが壊れていてもおかしいと思わない
- Winnyウイルスは亜種が多い

84

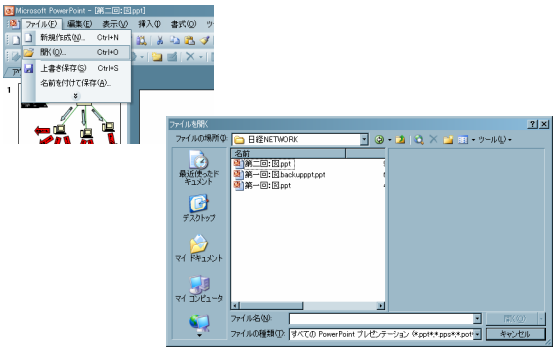
いまどきのウイルス対策

- 禁ダブルクリック。「ファイル」の「開く」で開けるようにする。
  - 拡張子偽装対策



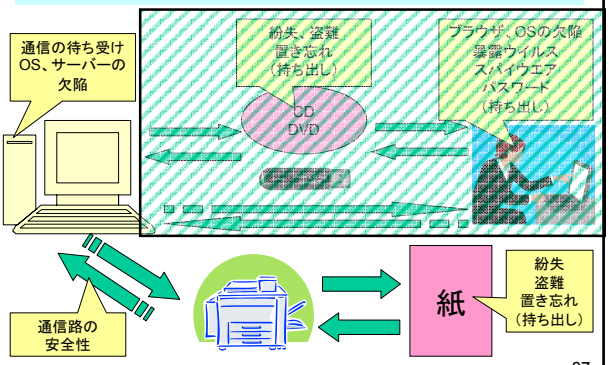
85

「ファイル」ー「開く」



86

対策の検証範囲



87

検討されていないリスク

- 意図的に持ち出すリスク
- 盗難リスク
  - 事務所荒らし、車上荒らし
- 他のルート

88

情報セキュリティマネジメント（2）

（基礎編第3回に相当）

89

脆弱性の評価

- 脆弱性定量化の目的
  - 統一した危険度の評価
  - 第三者的評価
  - パッチ対応などの判断材料
- 脆弱性評価のモデルを作ること
  - いろいろな視点がある（どれも正しい）
  - 目的に沿ったモデルはひとつではないかも

90

CVSS

Common Vulnerability Scoring System

- 提唱・賛同企業
  - Cisco Systems
  - eBay
  - Internet Security Systems
  - Qualys
  - IBM
  - Unisys
  - Microsoft
- 米国家インフラ諮問委員会（NIAC：National Infrastructure Advisory Council）の支援
- 2005年2月17日、米サンフランシスコで開催されたRSA Conferenceで発表された

91

CVSSの定量化

CIAに基づいて数値化しようとしている

- 基本評価基準 （Base Metrics）
  - 脆弱性そのものの特性を評価する基準（CIAを評価）
- 現状評価基準 （Temporal Metrics）
  - 攻撃コードの出現有無や対策情報が利用可能であるかといった脆弱性の現在の深刻度を評価する基準（時間で変化）
- 環境評価基準 （Environmental Metrics）
  - 攻撃を受けた場合の二次的な被害の大きさや、組織での対象製品の使用状況といった基準（ユーザごとに変化）

（引用：http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/ja/index.01.html）

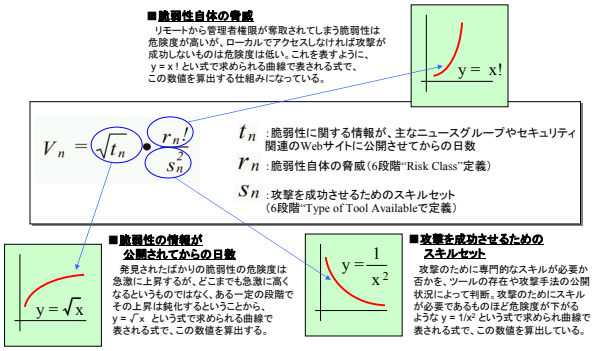
92

CVSSの計算例

http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/ja/CVSSv1.html

93

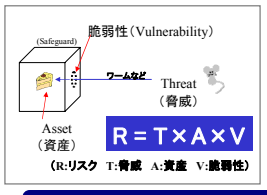
nCircleのアプローチ



参考：nCircle Network Security社

94

現場情報からの定量化



JNSA技術部会：
脆弱性定量化に向けての検討WG

パッチがリリースされた時に、即座に適用するか、次の定期保守まで待つかという判断に使える指標

純粋な「脆弱性」よりも、脅威をある程度含んだ、リスクに近い危険度を求める

「意思決定者が、対応する／しないの決定、あるいは、対応の緊急性を判断するための指標となる数値」

重み　固有値

$$d_{i \to j} = w_{i \to j}\left(\sum_a d_{a \to i} + \lambda_i\right)$$

95

Z（Triage）の構成要素

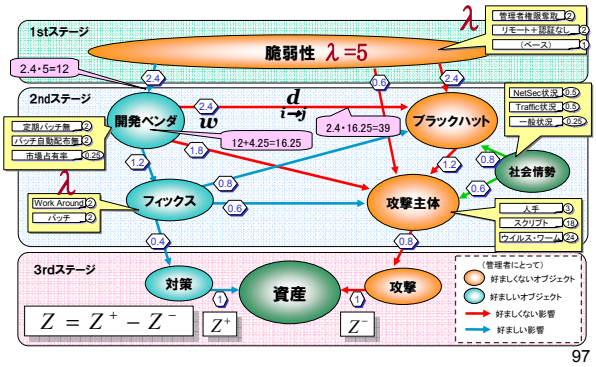
要素名	内容
手法	Exploitの存在、レースコンディション
影響	CIAの要素 v.s. 権限＋ブランド
環境	プロトコルのリモート/ローカル、認証
対策	対策をとれるか否か、それが一時的なものか 正式な対策が出ている・一時的（Workaround）・ない 副作用の話

要素名	内容
原因	仕様・コーディング・設定 パッチの作り易さ
ターゲット属性	誘引性
ソフトウェア特性	ソフトウェアのシェア、ベンダー
社会情勢	定期的、テンポラリ⇒イベント、カレンダー

現場で判断できる視点

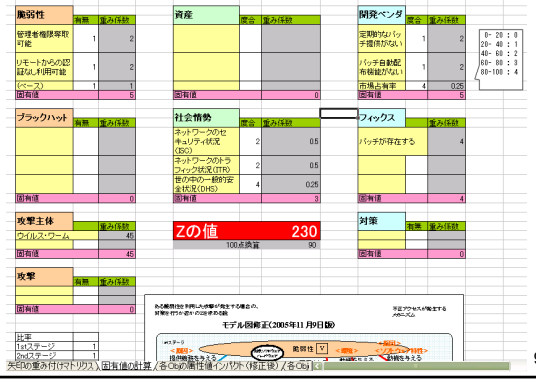
96

攻撃メカニズムの分析



97

重みを考慮した定量化



98

セキュリティ監査の目的

- システム仕様が必要な機能を網羅していることを確認する
- 脆弱性が存在せず堅牢であることを確認する
- 日々の運用が適切に行われ、各種の記録やLOGがとられていることを確認する

99

セキュリティ監査の内容

- 仕様、設計、開発について検査
- 設定等で脆弱性が存在しているか、可能性があるかどうかを検査
- 運用管理手順が決められ、適切に適用されているかどうかを検査

100

第三者機関の役割

- 当事者でない第三者が確認する
  - 開発者が自ら構築したシステムを検査し告知するのは内容の公正さに疑問が出やすい
  - 管理運用責任者が自らシステム運用の問題点を公正な目で指摘するのは難しい場合が多い
  - LOG情報を付き合わせ、適正に運用されているか確認し、トラブルがあった場合の調査を行い、証拠保全を行うのは、当事者ではないことを保障できる第三者に依頼するのが望ましい。

101

第三者と当事者

- とはいえ、第三者が監査するに当たって、システムの使用や動作について詳しい当事者の協力と情報交換が必要
- 当事者と異なる観点・視点で見るので、平常時の監査結果は、今後のシステム開発、設計、管理、運用等々に役に立たせることができる

102

セキュリティ監査の制度

- 2003年4月1日、経済産業省による「情報セキュリティ監査制度」が施行された
- 制度を着実に浸透させていく為の運営体として、「特定非営利活動法人 日本セキュリティ監査協会」が設立
  http://www.jasa.jp/
- 「公正かつ公平な情報セキュリティ監査」の確立と普及・浸透を目的

103

ITセキュリティ評価基準

- ISO/IEC 15408
  - Information technology － Security techniques － Evaluation criteria for IT security
  - ISO/IEC 15408は、欧米6ヶ国（アメリカ、カナダ、イギリス、フランス、ドイツ、オランダ）によるCCプロジェクトが1994年からISOと検討し、1999年にISO/IECとして制定された。国際的にCommon Criteria又はCCと通称されている。
- JIS X 5070
  - セキュリティ技術 － 情報技術セキュリティの評価基準
  - ISO/IEC 15408「Evaluation criteria for IT security」を技術的内容を変更することなく2000年に日本工業規格としたものである。

104

ISO15408の代表的な用語

CC：Common Criteria for Information Technology Security Evaluation
- コモンクライテリア
- 情報セキュリティ国際評価基準
- CCRA（コモンクライテリア承認アレンジメント）

PP：Protection Profile
- プロテクションプロファイル
- 製品のセキュリティ要件をまとめたセキュリティ要求仕様書（発注側作成）

ST：Security Target
- セキュリティターゲット
- 製品やシステムが備えるべきセキュリティ機能に対する要件とその仕様をまとめたセキュリティ設計仕様書（開発側作成）

TOE：Target of Evaluation
- 評価対象

EAL： Evaluation Assurance Level
- 評価保証レベル

105

セキュリティ評価の目的

- IT製品・システムの調達・構築・運用・利用に際して：
  - IT製品・システム及びPPのセキュリティ機能に関する正確で詳細な情報が入手できること
  - IT製品・システムのセキュリティ機能が間違いなく実装され、機能することに確信が持てることが必要である
  - このために、ITセキュリティ評価・認証制度が創設された

IPA「ITセキュリティ評価及び認証制度」
http://www.ipa.go.jp/security/jisec/documents/itqm24.pdf

106

EALと保証クラス

EAL（保証コンポーネント）は、セキュリティ機能の強度を示すものではなく仕様通りに実装されている確かさを

EALレベル	主な用途
1～3	一般民生用
4	政府機関等
5～7	軍用レベル、最高機密レベル

保証クラス	
構成管理 Configuration Management	ライフサイクルサポート Life cycle support
配付と運用 Delivery and operation	テスト Tests
開発 Development	脆弱性評定 Vulnerability assessment
ガイダンス文書 Guidance document	

107

EALに代わる制度

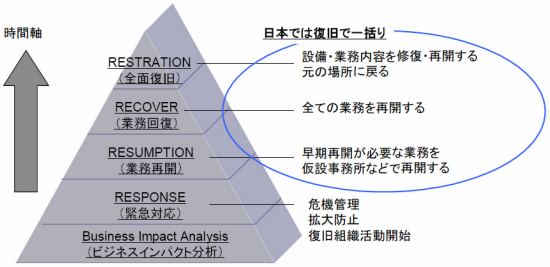
- EALの落とし穴
  - EALは数字表現なので、大きい方がセキュリティが高いと思ってしまう。
  - 保証しているのは、仕様通りに作られているかの書類確認だけ。
- パッケージ
  - 再利用可能な機能コンポーネント又は保証コンポーネントの集合。(例えば，EALは保証コンポーネントのパッケージである。)
  - セキュリティ脅威とその対策方針に関わる記載内容をパッケージ化することができる
  - IT製品やシステム固有の情報を規定の記載形式のパラメタに挿入することによって、正確なSTを作成することができる
  - EAL数値ではなく、パッケージ名で表現できる

IPA プロテクションプロファイルの登録手続
http://www.ipa.go.jp/security/fy13/evalu/event/20020328/docs/28-4Tabuchi2-plane.pdf
IPA セキュリティ脅威とその対策方針 パッケージ
http://www.ipa.go.jp/security/jisec/documents/spd_summary.pdf

108

監査と事業継続性

監査で証明するのは事業継続性の確保



（独）科学技術振興機構（RISTEX） 社会技術研究システム ミッション・プログラムⅡ
「高度情報社会の脆弱性の解明と解決（2005年3月）

109

背景にある社会要求

- BCM（Business Continuity Management）
- BCP（Business Continuity Plan）
- 情報開示（ディスクロージャー）
- 法令遵守（コンプライアンス）
- 企業の社会的責任
  （Corporate Social Responsibility：CSR）
- EC（Electronic Commerce）
- EDI（Electronic Data Interchange）
- SCM（Supply Chain Management）
- ERP（Enterprise Resource Planning）
- CRM（Customer Relationship Management）

110

フル・ディスクロージャ

- **セキュリティフォーカス**
  （http://www.securityfocus.com/）の「Bugtraq」などで提唱されている
- 本当にセキュアなシステムはプロトコルやソース・コードなど、どのようなレベルでもオープン・レビューに耐えなければならない。
- 誰に対しても，セキュリティ上の脆弱性についての詳細情報は参照可能であるべきである。
  - 初動体制、公開までの制限時間、誰のための公開か
  - METI/IPA/JPCERT-CC 情報セキュリティ早期警戒パートナーシップ

111

インシデントレスポンス

- IR（Incident Response）
- コンピュータセキュリティ・インシデントに対応すること
  - コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの（その疑いがある場合）を含む。例えば、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示や、さらにそれらに至るための行為（事象）などがある。（JPCERT/CC）

112

インシデントの種類

（JPCERT/CC）

- プローブ、スキャン、そのほか不審なアクセス（scan）
- サーバプログラムの不正中継（abuse）
- 送信ヘッダを詐称した電子メールの配送（forged）
- システムへの侵入（intrusion）
- サービス運用妨害につながる攻撃（DoS）
- その他（SPAMメール、ウイルス感染）

113

監査とフォレンジクス

前提条件

- 企画・設計・開発時のドキュメントが整備されている
- 予め事故想定の作業手順がある
- システム的にLOG情報がきちんと保管されている
- データ内容のリスク評価に従って、物理的な対策、システム的な対策、運用管理的な対策を行っている
- その上で、実行されていることを監査で確認する

事故や犯罪が起きたときの対応

- システムLOGを調査して原因や規模を追究する
- 運用管理面での証左を探す

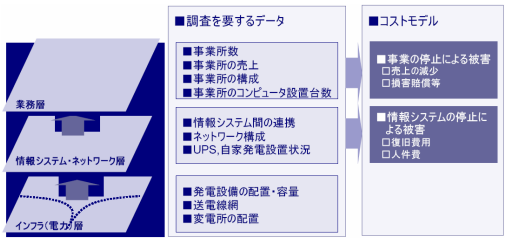
114

多重リスクコミュニケータ

- Multiplex RiskCommunicator (MRC)
- リスク対策の策定において様々な要因を考慮したリスク分析をし、関与者とのコミュニケーションを図りながら問題を解決することを支援する
- 意思決定者と関与者間で合意形成する過程
- セキュリティに対するリスクだけでなく、プライバシーや利便性、さらにはコストといった複雑に絡みあう要素、対立する利害関係を考慮してリスク対策を行う

三層ハザードマップとコストモデル

- インフラ＋IT＋業務の三層構造で相互関係とリスク連鎖を考える
- 各層での考慮点をリストアップ
- コスト算出と連携してリスク管理を行う



権限とデータ管理（1）

（基礎編第4回に相当）

データの価値

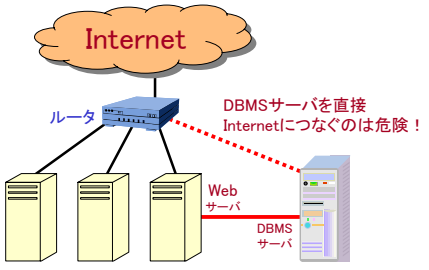
- データに価値がある
  - ハードウエアやソフトウエアは取り替えられる
  - データが個人、企業、国家にとっての財産
  - 失うと二度と回復できないことが多い
- 価値を決めるのは持ち主ではなく、情報を欲しいと思っている側である

データベースサーバ

- データベースは、DBMS（データベース管理システム）を使うだけでは作ることは出来ない。
  - ORACLE、Postgres、SQLserverなどは検索用
  - データベースは、登録項目を整理すること
    - CSV(Comma Separated Values)でもデータベース
- では、インターネットでDB検索をしたいとき、何に気をつければよいのか？

DBMSとWebとの連携

- DBMSサーバの置き方



コンピュータの守り方

- サーバを守る
  - 運用管理（設定、解析、感性）
    - OS、サーバ用ソフトに最新パッチを当てる
    - 運用管理者としての素質と研鑽
  - セキュアOS
    - Common Criteria (CC)に基づいたアクセス制御を実装
    - SELinux が有名
- クライアントを守る
  - OS等の脆弱性を塞ぐ
  - ウイルス対策ソフト
- 物理的な防御策

121

RASとCIA

- RAS：メインフレームなど高信頼マシンで使われた
  - Reliability: 信頼性
  - Availability: 可用性　システム観点
  - Serviceability: 保守性
- CIA：（第１回を参照）
  - Confidentiality 機密性
  - Integrity 完全性　情報観点
  - Availability 可用性

122

身の丈の安全性

- コンピュータを守る5W1H
  - Who（だれ）　利用者、管理者
  - Where（どこ）　設置場所
  - When（いつ）　サービス時間
  - Why（なぜ）　目的
  - What（なに）　用途
  - How（どのように）　運用・監視
- 完全性を求めると経済性が引き合わない
- 経済性だけ考えると安全性が犠牲になる

123

バランス感覚

- インターネット回線
- ネットワーク構成
  - 検疫ネットワーク、VLAN、機材、性能
- ホストマシン
  - OS、マシン、トラフィック振分、RAID disk
- データ保全
  - アーカイブ、複数コピー保管、情報漏洩対策
- 業務システム構築
  - 仕様検討、ソフト開発、継続アップデート

124

サーバを守るということ

- サーバはインターネットに接続する。（イントラネットとの違いと類似性）
- 攻撃相手は地球上のあらゆる所にいる
- インターネットは水や空気であり、水源や植物のように情報を供給するのがサーバである
- 完全に守れば良いというものではなく、最低限の対策をしつつ、経済的に見合う防衛が必要である
- サーバ管理は地味な仕事で評価も決して高くはないが、居なくては世の中がうまく動かない縁の下の力持ちでもある

125

サーバの設置方針

- 一般的なUnix/Linuxを使用
- Windowsサーバを使用
- Macintoshを使用
- セキュアOSを使用（SELinux等）

- どのような業務に使うのか？
- どのようなアプリケーションを使うのか？

126

実際の設定の考え方

- 基本は、ゼロから出発
  - 全てのサービスを止めて
  - 実現したいサービスだけを許可する
- DMZにサーバを置く
  - DMZの役割は何でしょう？
  - アクセス制限と隔離
- NGNでどのくらい解決できるのか
  - プロバイダでのサービス制限で実現
  - サービスの多様性の選択肢としては歓迎

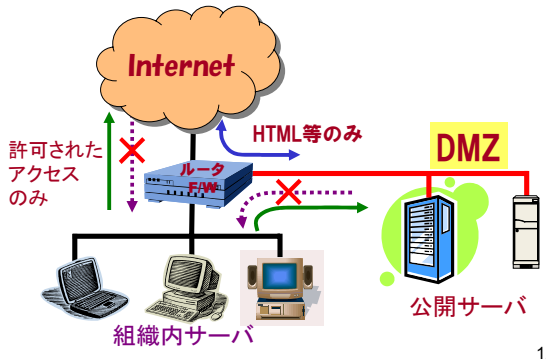
127

DMZの役割

- DeMilitarized Zone（非武装地帯）
- インターネットとはF/Wで分離
  - 外部サービスのみを通過させるアクセス制限
- 内部ネット（イントラネット）ともF/Wで分離
  - 内部ネットワークへのアクセスは原則禁止
- アクセス制限を外部と内部で独立して設定
  - 外部からの攻撃を排除
  - 外部から攻撃されてのっとられても、社内ネットワークまではすぐに影響が及ばない
- 外部サービスを行うサーバを置く場所
  - 外部サービスを行うために必要最小限のアクセスが許されたネットワークセグメント
  - NAT機能でアドレス変換を行う場合が多い

128

DMZのイメージ



129

NGNの今後

次世代通信網… Next Generation Network

- 固定電話用設備をIP対応にし、音声やデータ通信をひとつの回線で扱う
- 通信事業者が通信サービスを管理し制限する閉鎖的なネットワークを提供し、通信速度や音声品質の保証やアクセス制御等を行い、不正アクセスから守るなどの信頼性を実現しようとするもの（NTTが2008年開始で進めている）
- インターネットサービスの選択肢としては歓迎される
- サービス内容はISPごとに特徴が出ると思われる

130

一般的対策の限界

- ファイアウオールの限界
  - 不要な通信を制限するが、サービスに必要な通信は通過する
  - ファイアウオールを通過できる通信を利用した攻撃に対しては効果がない
  - Webサーバーでは、HTTPを使った攻撃はファイアウオールでは防御できない
- IDSの限界
  - 通信内容を監視し、攻撃と思われる通信を検知したら警告を発する
  - あらかじめ登録しておいた攻撃パターンを検知する
  - 未知の攻撃を検知するのは難しい
- パッチ適用の限界
  - 対策が公開されたアプリケーションはパッチを適用して対処
  - パッチが未発表の脆弱性は対応できない
  - 未知の脆弱性に対しても対処できない

131

なぜセキュアOSなのか？

- 管理者権限をとられても、全権を取られない
  ⇒全権を持つ管理者権限が存在しない
- ユーザやプロセスごとに最小権限の付与
  ⇒正常動作に必要な最小権限で実行し、
  SUIDによる権限移行や昇格を使わない
- システムセキュリティポリシーで定義と制御
  - 強制アクセス制御（MAC）
  - 最小特権（TE）

132

アクセス制御方式

- 任意アクセス制御
  - DAC: Discretionary Access Control
- 強制アクセス制御
  - MAC: Mandatory Access Control
- ロールベースアクセス制御
  - RBAC：Role-Based Access Control

133

DAC

Discretionary Access Control

- 任意アクセス制御
- ファイルやプログラムの持ち主が自由にアクセス制限を指定する
- システム管理者が設定するのではない

134

DAC　例

```
drwxr-xr-x   2 cyber  univ     4096  5 22  2006 directory
-rw-r--r--   1 cyber  univ    32485  6 30  2004 read-file
-rw-rw-rw-   1 cyber  univ    43291  1  8  2006 write-file
-rwx--x--x   1 cyber  univ   173294  8 25  2000 program
```

種類　持主　グループ　その他

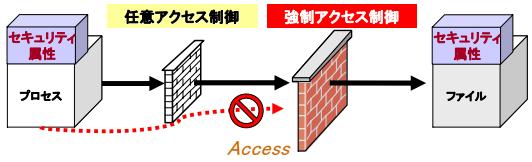
r　読み取り可能
W　書き込み可能
x　実行可能

135

強制アクセス制御（第４回）

Mandatory Access Control

- システム管理者でも予めセキュリティ属性に設定された機能しか実行できない。
- システム管理者もセキュリティ属性を回避できない。
- root権限のような全能権限がない！



rootユーザでも強制アクセス制御は回避できない

引用：　JNSA Press 第14号　特集：セキュアOSを導入せよ　http://www.jnsa.org/

136

MAC

Mandatory Access Control

- 強制アクセス制御
- セキュリティポリシーモデル
  - 「主体」Subject　と　「対象物」Object
  - 多階層（多層的）セキュリティポリシー
    Multilevel Security Policy
  - 多元的セキュリティポリシー
    Multilateral Security Policy

137

多層的セキュリティポリシー

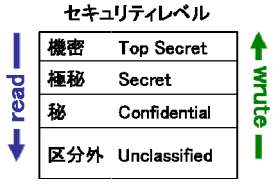
- 情報を階層に整理し、階層間のアクセスを制御する
- データが階層構造で複数の異なる重要度を持つ場合に適応
- 米国の軍などで採用されている
- Bell-LaPadulaモデル
- Biba Integrity モデル
- LOMACモデル

138

Bell-LaPadulaモデル

・1973年米国空軍の要請により
David Bell、Len LaPadulaが提案
・情報の不適切な開示の有無を検証することが可能
・情報が下へ流れない （守秘性）

- シンプルセキュリティ属性 (Simple security property)
どのサブジェクトも高位のデータを読んではならない。
NRU (no read up)
- スター属性 (*-property)
どのサブジェクトも低位にデータを書き込んではならない。
NWD (no write down)

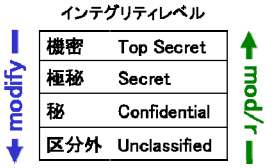


139

Biba Integrityモデル

・Low Water-Mark Model
・1975年 Bibaが情報の不適切な修正を防ぐためのモデルを提案
・情報が上へ流れない （完全性）

- シンプルインテグリティ属性 (Simple integrity property)
サブジェクトは、下位のデータに限り修正することができる。
- インテグリティ スター属性 (Integrity *-property)
もしサブジェクトが、同じインテグリティ・レベルのオブジェクトへの読み込み権限を持っていれば、そのサブジェクトは上位のオブジェクトに限り修正することができる。



140

LOMACモデル

2000年 NAIのTim Fraserによって提案

・Bibaの自己廃止問題 (Self-Revocation Problem) への対策
  - Bibaでは、高いレベルのサブジェクトがオブジェクトを作成し、低いレベルのオブジェクトを参照する場合、サブジェクトは低いレベルに「降格(demote)」させられる。
  - 低いレベルのオブジェクトを参照すると、悪意を持ったコードによって汚染される可能性がある。
  - 低いレベルにあるサブジェクトは自分で生成したオブジェクトを修正できない。
・IPC（Inter Process Communication）で生じている
・一連のプロセスをgroupとしてカプセル化してもセキュリティ強度を低下させないことを数学的に証明した

141

多元的セキュリティポリシー

・コンパートメントと呼ばれる区画で、情報へのアクセスをコントロールするモデル
・階層的な情報コントロールではなく、コンパートメント間の横方向の情報フローをコントロールする
・Clark-Wilsonモデル
・Chinese Wall モデル
・DTEモデル
・RBACモデル

142

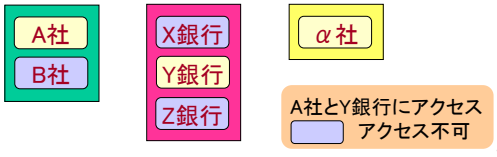
Clark-Wilsonモデル

・1987年David ClarkとDavid Wilsonが、一般の商業活動における重要な問題はデータの完全性を確保すること
・定型化されたトランザクション (well-formed transaction)
  - データの完全性を保証するためには、定型化されたトランザクションでしかデータを操作することができないようにする
・責務の分離 (separation of duty)
  - たった一人の管理者により全てのオペレーションが行える状況は、詐欺を引き起こす場合がある。
  - 権限を分割することで、例え部分的に権限が奪取されたとしても、全体としてのオペレーションは、矛盾なく実行することが可能である。

143

Chinese Wall モデル

・1989年 BrewerとNashが情報アクセスの保護のためのモデルを発表
・「関心事の衝突」を情報保護の基本としている
（守秘性にフォーカス）
・競合する会社ごとのグループに分類する
（関係協力関係ではない）
・いったん情報にアクセスすると、それ以降は競合クラス内の他のオブジェクトにはアクセスできなくなる



144

DTEモデル

- Domain Type Enforcement
- Type Enforcement (TE)の拡張
- サブジェクトがアクセス可能なオブジェクトを必要最小限に規制する
- TEはファイルとセキュリティ属性を1対1で表現する
- DTEは同じセキュリティ属性を持つファイルをファイル階層構造で表現することでアクセス制御テーブルの爆発を抑える拡張を行っている。
- プロセスは"Domain"、ファイルは"Type"を定義する。

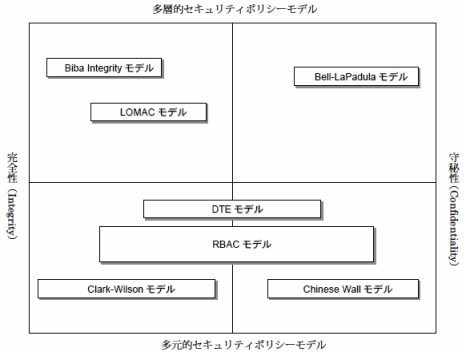
145

RBACモデル

- Role-Based Access Control
- オブジェクトへのアクセス権を役割(role)に関連付けるとともに、役割をユーザに割り当てることにより、ユーザと役割に対するパーミッションを対応させる
- root権限を持つ管理者モデルの代替
- 最小特権のセキュリティモデルとして運用できる
- 役割ごとに責任者を決め権限委譲ができる

146

セキュリティポリシーモデルの位置づけ



引用:IPA「オペレーティングシステムのアクセスコントロール機能におけるセキュリティポリシーモデル」
http://www.ipa.go.jp/security/awareness/administrator/security-model.pdf

147

セキュアOSの例(第4回)

- SELinux
  - Security Enhanced Linux
  - 米国家安全保障局　2001年1月2日に公開 NSA (National Security Agency)
  - Linuxカーネル用セキュリティ拡張モジュール
  - 強制アクセス制御 (MAC)、最小特権の実装
- LIDS
  - Linux Intruder Detection System
  - Xie Huagang氏とPhilippe Biondi氏により，1999年10月15日に公開　オープンソフト
  - アクセス制御リスト(ACL)に基づいた権限制御

148

セキュアOSの例(第4回)

Trusted OS	Trusted Solaris
	PitBull Foundation Suite
セキュアOS (カーネル型)	SELinux
	PitBull LX
	Hp Compartment Guard
セキュアOS (ドライバ型)	MIRACLE HiZARD
	PitBull Protector Plus
	Secure TOS

149

権限とデータ管理(2)

(基礎編第5回に相当)

150

クライアントPC対策

- ウイルス等に感染した場合の対策
- ウイルス対策ソフトによるクリーンアップ
- 最後は再インストール（初期化）を行うのが確実
- Windowsなどでは、追加インストールしたソフトの再インストールが必要
- ユーザデータは定期的にバックアップを作っておくと安心

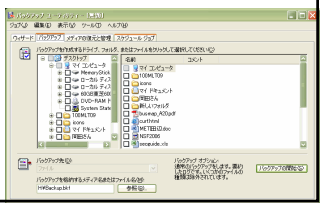
151

バックアップ方法

サーバは当然。クライアントも必要

- Unix/Linux コマンド
  - dump / restore
  - cpio
  - tar
- Windows/ Macintosh
  - バックアップツール
  - 製品類

{ 全部
{ 差分
元に戻すときの速度や操作



Windowsでのバックアップのコツ

- C: にはOS関係のみとする
  - インストール直後のまま
- ユーザデータは全てD: に置く
  - 「マイドキュメント」も D: に変更
- 再インストールは C: だけにする
  - 追加されたプログラム類は再インストール
  - ユーザデータはそのまま温存できる
- C: のディスクイメージを取るとよい
  - 再インストールはディスクイメージから行う
  - 追加プログラムも回復できる

153

バックアップの保管

- 外付けディスク
- DVD/CD-R
- 磁気テープは…

ユーザデータの扱いはPCと同様

思わぬ情報漏洩を起こさないように…

154

シンクライアントの背景

- パソコンの高速化
  - 20年前のスーパーコンピュータ
  - 10年前のパソコンの10倍以上（CPU）
  - CPUは早くなっているけど、周辺はそこそこ
- パソコンの大容量化
  - 20年前の汎用機・ミニコンの1000倍
  - 10年前のパソコンの100倍以上（ディスク）
  - 画像・音声データが爆発を推進している
- ノートPCの普及
  - 軽量高性能なノートPCが安価に手に入る
  - 盗難・紛失しやすく、しかも大量のデータが漏洩し易い

155

高機能パソコンの問題点

- Rich Client / Fat Client
- 大量の情報を保管している
- いろいろなソフトをインストールしている（Winnyなども含まれると危険）
- 外部記憶装置（USB等）の大容量化
- ノートPCの管理ポリシーが必要
- 持ち出し・持ち込み制限だけで良いのか？

156

クライアントPC管理の課題

- 重要な情報が分散保管される
  - コピーデータの管理と版管理が大変
- クライアントPCの管理が困難
  - OSやソフトのパッチ管理、版管理が大変
- セキュリティ対策のコストが増大
  - 情報システム部門の作業管理コストの負担
- クライアントPCのリスク管理
  - クライアント環境の一括管理によるリスク対策

157

シンクライアントへの道

時代 →

	メインフレーム ミニコン時代 (1970年代～1990年前後)		クライアントサーバ(CS)時代 (1980年代～)				
	TSS端末	インテリジェント端末	ワークステーション	X端末	パソコン	シンクライアント	Sun Ray
プログラム	ホスト	ホスト	端末	ホスト	端末	ホスト	ホスト
データ	ホスト	ホスト	端末	ホスト	端末	ホスト	ホスト
実行	ホスト	端末	端末	端末	端末	ホスト	端末
表示	端末	端末	端末	端末	端末	端末	端末

158

Thin client

サーバベースコンピューティング

- ダム(Dumb)端末
  無手順端末
- X端末
- Sun Ray
- 先祖帰り？
- 振り子の法則

159

シンクライアント端末の種類

1. キーボードやマウスなどの入力制御や画面表示を行うために最小限の機能を持つプログラムを、EEPROMやFlashメモリにインストールした組込型の汎用OS(Windows XP Embeddedや Embedded Linuxなど)上から起動する
2. ネットワーク上のマスターから汎用OSをダウンロードしてPC同様に起動する
3. 表示や入力処理に必要な機能を実現する専用ソフトを直接ファームウェアで実行する(Ultra Thin Client)

160

ネットワークセキュリティ(1)

(基礎編第6回に相当)

161

データ自身を守る方法

- 暗号化
  - 通信の暗号化(IPsec, VPN, SSL, SSH等)
  - 記憶媒体の暗号化(HDD, CD, USBメモリ等)
  - 情報漏洩対策(盗難、遺失、オペミス)
- データ保全
  - バックアップ(コピーの作成)
  - システム障害対策
  - 複数地域での保管(BCP、自然災害対策)
    - Business Continuity Plan
  - 誤操作によるデータ回復

162

データのバックアップ

データの何を守るのか？
- 改竄、不正操作
  - 悪意の操作を回復する
- 事故があった場合の迅速な復旧
  - 不可抗力や人為的過失を回復する
  - 自然災害
  - システム障害
  - オペレーションミス（誤操作）

一番大切なのはデータのバックアップ
★リスク管理の一環として考える

163

ネットワークセキュリティ（2）

（基礎編第7回に相当）

164

ファイアーウォール

- Fire Wall （F/W）
- 防火壁（飛び火や不正侵入を防ぐ壁）
- 不正なアクセスをブロックする
- 基本機能
  - パケットフィルタリング
  - アドレス変換（NAT）
- アプリケーションゲートウェイ
- DMZ （第11回）
- パーソナルファイアウォール

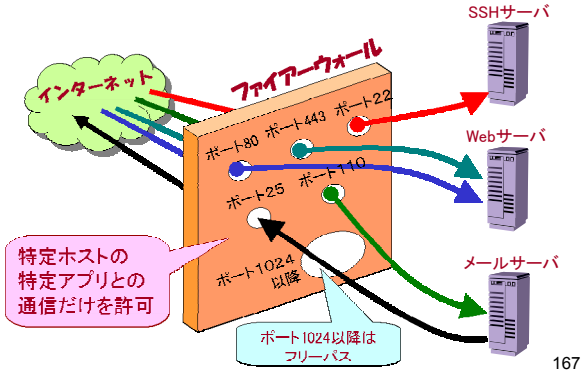
165

パケットフィルタリング

- パケットのヘッダ情報や内容（ペイロード）を見て、通過させるか破棄するかを決める
- ルータやファイアーウォールで実現
- ヘッダのアドレス情報
  - IPアドレス　第3層　ネットワーク層
  - ポート番号　第4層　トランスポート層
- 基本はホストとアプリで選別する

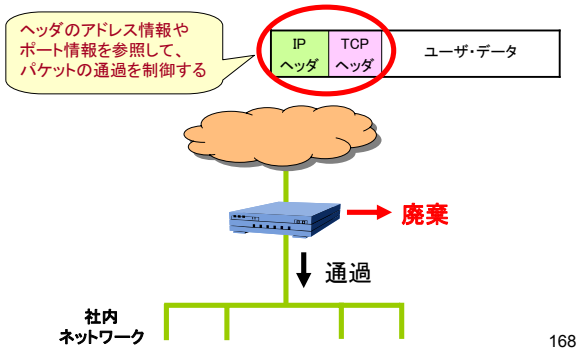
166

ファイアーウォールのイメージ



167

フィルタリング

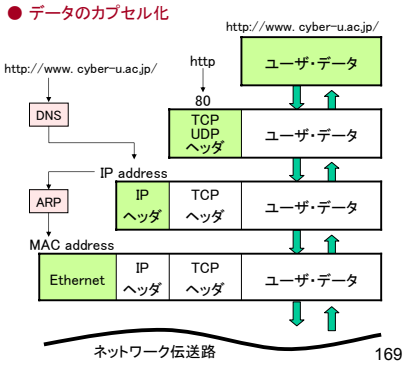


168

ヘッダの構成とカプセル化（第9回参照）

● OSI参照モデル　● データのカプセル化

7	アプリケーション層
6	プレゼンテーション層
5	セッション層
4	トランスポート層
3	ネットワーク層
2	データリンク層
1	物理層



169

3層ヘッダ情報

IPヘッダ　(Internet Protocol)

VER: バージョン	IHL: ヘッダ長	TOS: サービスタイプ	TL: パケット長
ID:識別子		FL: フラグ	FO : フラグメントオフセット
TTL: 生存時間	PROT: プロトコル	HC: ヘッダ・チェックサム	
SA: 送信元IPアドレス			
DA: 送信先IPアドレス			
OPT: オプション（不定長）			PAD: パディング
DATA: 上位層データ			

20オクテット

32ビット(4オクテット)

170

4層ヘッダ情報（TCPヘッダ）

TCPヘッダ　(Transmission Control Protocol)

SRC: 送信元ポート番号			DEST: 送信先ポート番号
SEQ: 送信シーケンス番号			
ACK: 応答確認番号			
DO: データオフセット	RES: リザーブ	CB: 制御ビット	WINDOW: ウインドウ
CS: チェックサム			URGPTR: 緊急ポインタ
OPT: オプション			
DATA: 上位層データ			

20オクテット

32ビット(4オクテット)

171

4層ヘッダ情報（UDPヘッダ）

UDPヘッダ　(User Datagram Protocol)

SRC: 送信元ポート番号	DEST: 送信先ポート番号
LEN: データ長	CS: チェックサム
DATA: 上位層データ	

32ビット(4オクテット)

172

F/Wの限界

- 1024以降のポート番号は空いている
- P2Pなどサーバを使わないアプリでは、クライアント同士で自由なポート番号を使える
  - ➢パケットフィルタリングができない
- SkypeやSoftetherなどhttp/httpsを利用するものは区別がつかない
  - ➢パケットフィルタリングができない

173

F/Wの対策

ステートフル・パケット・インスペクション

- 外部からのパケットに「ACK」があると、F/Wは通過させる（F/Wの攻撃方法）
- 要求パケットと応答パケットの順序をチェックし、正当なパケットのみを通過させる

CB (Control Bits): 制御ビット

URG (Urgent)	緊急ポインタが設定されている
ACK (Acknowledgment)	応答確認番号が設定されている
PSH (Push)	プッシュ機能
RST (Reset)	接続をリセットする
SYN (Synchronize)	送信シーケンス番号を同期させることを通知
FIN (Final)	送信元からのデータが最後であることを通知する

TCPヘッダ　(Transmission Control Protocol)

174

アプリケーション・ゲートウェイ

- アプリケーションごとにプロキシサーバ(Proxy server：代理サーバ)を立て、ここでデータの内容のチェックを行う。
- 例えばHTTPのペイロードに書かれているコマンド(GET、POST、PUT、URL記述等)をチェックできる。
- 例えばFTPのダウンロード（受信）を許可し、アップロード（送信）は禁止するなどの方向性制御ができる。
- 解析時間が必要なため、パフォーマンスが低下する。

175

NATの機能

- Network Address Translator
- 主に、内部ネットでプライベートアドレスを利用するために、インターネット側のグローバルアドレスとプライベートアドレスを相互変換する。
  - GlobalとPrivateアドレスは1対1に対応づく
  - 複数のホストがある場合、同数のGlobalアドレスが必要になる。
  - Globalアドレスの枯渇対策にはならない
- ポート番号を置き換え、ひとつのGlobalアドレスで複数のPrivateアドレスのPCからのアクセスを可能にする。
  - IPマスカレード（masquerade：仮面舞踏会）
  - NAPT（Network Address Port Translation）。

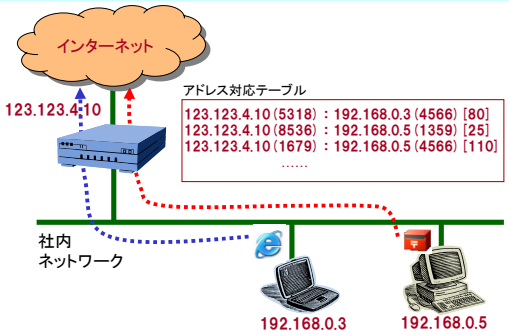
176

NATの副作用効果

- 最初に内部からのアクセスで変換テーブルを設定する必要があることから、外部から内部のプライベートアドレスのPCを特定するのが困難なので、外部からの不要アクセスを制限できる。
- IPsec、FTP、SIP、VoIP、P2Pなどが動作しないことがある。

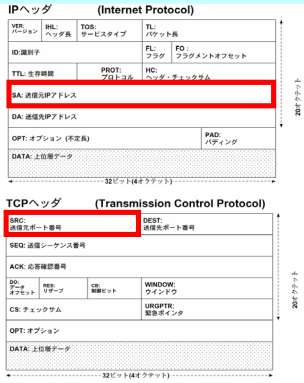
177

NAPTの動作イメージ



178

ヘッダ情報の書き換え



送信元のアドレスをNAT機器のIPアドレスに書き換える
送信元ポート番号をユニークに書き換える

パケット改竄による成りすましと同じ操作をしている

179

IDS/IDP

- Intrusion Detection System
- Intrusion Detection Prevention
  Intrusion Prevention System (IPS)
  Intrusion Protection System
- 侵入検知システム
- 侵入防御システム
- ネットワークやコンピュータに対する不正アクセスを検出し報告、防御する
- 不正アクセス
  ＝許可されていないアクセス

180

検出方式(1)

- シグネチャ・マッチング方式
  ミスユース検知方式
- 不正検出
  - 「シグネチャ」として記録されている既知の攻撃パターンと比較する
  - 既知の攻撃パターンと比較する
  - 一致したとき、攻撃を受けていると判断する。
  - ウイルス対策ソフトのパターンファイルと同様

181

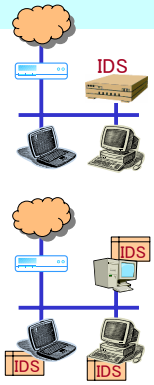
検出方式(2)

- アノマリー検出方式
  - 正常(通常)なプロトコルの遣り取りや振る舞いと異なることを検出する
  - 決められたパターンでなければ攻撃者がいると判断する。
  - 期待される動作以外を検出するので、未知の攻撃方法にも対応できる。
  - プロトコル異常検出方式
    - HTTP、SMTP、FTPなどのプロトコルがRFC標準に基づいているかどうかを検査する
  - トラフィック異常検出方式
    - 統計的に分析された正常時のトラフィックからのずれを検出する

182

監視対象

- ネットワーク型(NIDS)
  - ネットワークを流れるデータを監視する
  - プロミスキャスモードのNIC
- ホスト型(HIDS)
  - ホスト上のシステムコールの使用やログデータの内容等を監視する
- ハイブリッド型
  - 複合型



183

IDSの課題

- IDSで検出されない攻撃方法が論文として公開された。(1998)
- IDSを回避する攻撃ツールが出た
- IDSの内部動作をメーカーはほとんど公開しなかった
- IDS導入の目的が曖昧
- 誤検知、過剰検知が多い
- トラフィックを取りこぼしてしまう
- 検出しても防御をしない

184

IPSへの拡張

- 侵入防止システム
- 異常を検知すると、パケット破棄などの自動防御を行う
- F/Wと連動させて、検知ルールの自動修正や改竄検出などを行うものもある
- パケットのユーザデータ部分(ペイロード)を見るので、通信の秘密に触れるのではないかという議論もある。

185

ハニーポット

Honey Pot (蜜壷) 囮サーバ

攻撃者を引付け対策の時間稼ぎをする

攻撃パターンを監視し、不正アクセスの手法を研究する

セキュリティ設定が甘いように見せかける罠を仕掛ける

186

ハニーポットのタイプ

特定サーバの機能をエミュレート
- HTTPサーバ、SSHサーバ、FTPサーバ、等々
- 該当サーバと同じレスポンスを返すが、本来の機能が全て実行されるわけではない

各種OSをエミューレート
- SSH、SSLなどの暗号化通信でも復号した情報を記録できる
- キーストロークやOSの応答なども記録できる
- ハニーポットを踏み台にされないようにする

187

ハニーポットの情報

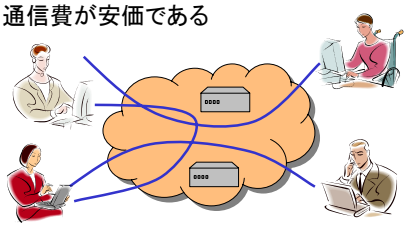
The Honeynet Project
http://www.honeynet.org/
- ハニーポットなどの最新技術やテクニックを研究・情報交換することが目的

ハニーポットの技術
- ネットワーク型IDS
- ホスト型IDS（ログ監視、プロセス監視等）
- アクセス制御
- ログ制御
- コンピュータ・フォレンジクス（プロセス、ファイル、ネットワーク）

188

インターネット

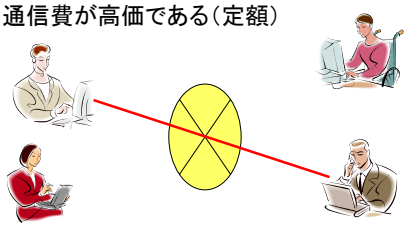
- インターネットは経路途中での通信データは原則オープン
  - 盗聴が可能
  - 通信速度は必ずしも保障できない
  - 通信費が安価である



189

専用線

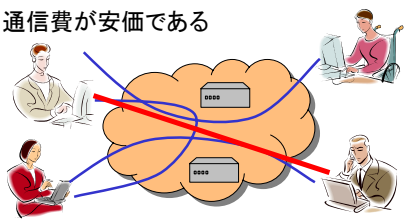
- 専用線は、他人の通信内容は傍受できない（ことになっている）
  - 盗聴が困難
  - 通信速度が確保できる
  - 通信費が高価である（定額）



190

Virtual Private Network

- VPNはインターネットで専用線並みの安全性を確保する技術
  - 盗聴が困難
  - 通信速度は必ずしも保障できない
  - 通信費が安価である



191

VPNって？

なぜVPNが必要なの？

- インターネットを使って、専用線と同じような安全な通信をしたい！

どんな技術を使うの？

- 暗号化と認証、それに諸々…

192

利点

- インターネットが利用できる
  - 全てインターネットの世界で解決できる
  - 接続先を迅速・柔軟に変更できる
- 盗聴されても通信内容の安全性が保てる
  - 暗号通信で実現される
- 許可された相手としか通信しない
  - 認証を行う

193

欠点

- 帯域確保などは保証し難い
  - インターネットの制限は変わらない
  - ISPによっては、独自回線を使ったIP-VPNと呼ばれるサービスを提供している場合もある
- 安全性はVPNアルゴリズムに依存
  - VPNは皆同じではない
- VPN用の機材を追加しなければならない
  - 価格、機能は多種多様
  - 固定IPアドレスを取るのが良い

194

VPNの用途

- それほど高い安定性は必要ないけど、そこそこの通信速度が欲しい。
  - 専用線で通信速度を確保するのはコストがかかる。
  - ファイル共有、データベース検索、TV会議等。
- 個人情報など盗聴されたくない情報を扱う場合
  - 専用線を使っていても、暗号化しない通信は、危険な場合がある。
- 回線が切れてしまった時、アプリケーションで回復処理を行うコスト増と、専用線をインターネットに変更するコスト減との比較

195

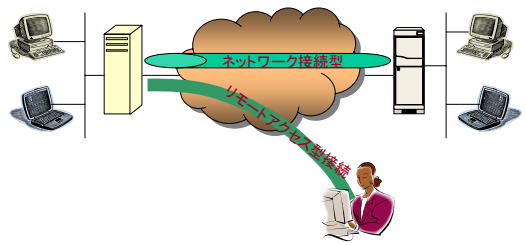
VPNの接続形態

- ネットワーク接続型
  - サイト間接続
  - ネットワークをリモートに延長
  - 両ネットワークがひとつに見える
- リモートアクセス型
  - リモートからクライアントを遠隔接続
  - 外部から暗号通信で接続
  - 組織内ネットワークに外部から接続

196

VPNの接続形態概要

2つの形態に求められる機能はかなり異なる



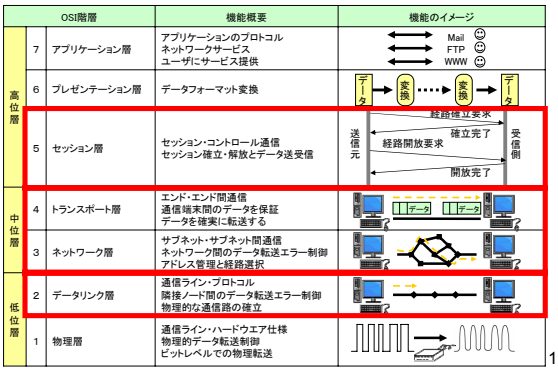
197

VPNが実装される部分

- 対応する層
  - アプリ層　5層：セッション層
  - TCP/UDP層　4層：トランスポート層
  - IP層　3層：ネットワーク層
  - レイヤ2　2層：データリンク層
- IPパケットのカプセル化
  - トランスポート・モード
  - トンネル・モード
- カプセル化したパケットを仮想トンネルで運ぶ
  - データリンク層をトンネリング ⇒ 「レイヤ2トンネリング・プロトコル」 **PPTP、L2F、L2TP**
  - ネットワーク層をトンネリング ⇒ 「レイヤ3トンネリング・プロトコル」 **IPSec**
  - セッション層で対応 **SSL-VPN、SSH-VPN**

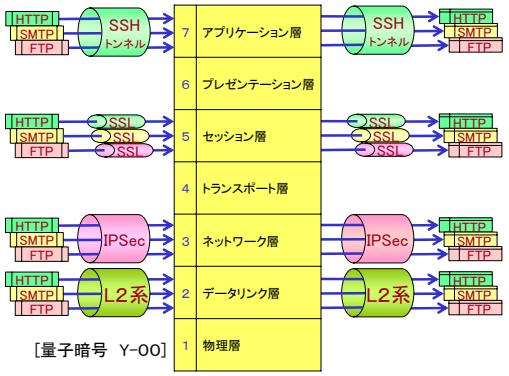
198

OSI 7階層モデル（第3回）



199

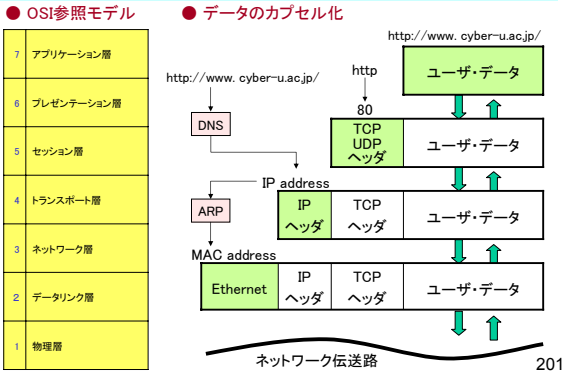
VPNの通過対象レイヤ



［量子暗号 Y-00］

200

ヘッダの構成とカプセル化



201

PPTP（Point to Point Tunneling Protocol）

- Microsoft、Ascend Communications（現Lucent Technologies）、US.Robotics（現3Com）等が開発
- レイヤ2トンネリング・プロトコル（RFC 2637）
- 発信元をPAC（PPTP Access Concentrator）と接続を受けるPNS（PPTP Network Server）からなる
- PAC-PNS間で仮想トンネルを構築する。
- Windows クライアント系ではPACが標準実装されている。
- Windowsサーバー系ではPNSが実装されている。

202

L2F（Layer 2 Forwarding）

- Cisco SystemsやNorthern Telecom（現Nortel Networks）等が開発
- レイヤ2トンネリング・プロトコル（RFC 2341）
- 現在はL2TPに統合
- 制御チャンネルとトンネルにUDP（ポート1701）を使用する
  - PPTPでは、制御コネクションにTCP、トンネルに拡張GREプロトコルを使用する

203

L2TP（Layer 2 Tunneling Protocol）

- レイヤ2トンネリング・プロトコル（RFC 2661）
- PPTPとL2Fを統合したもの
  - PPTPのトンネル制御部分とL2Fのフレーム構造を組合せた感じ
- PPTPのPACとPNSに相当するLAC（L2TP Access Concentrator）とLNS（L2TP Network Server）の間に仮想トンネルを構築する。
- 制御チャンネルとトンネルは、L2Fと同様にUDP（ポート1701）を使う。
- ATMやフレーム・リレー上での利用も可能
  - PPTPは、IPネットワーク上でのみ利用可能
- 1つの仮想トンネルで複数のユーザー・セッションを作れる
- 通信データを暗号化する機能を持たない
  - PPPやIPSecの暗号化機能を利用する

204

IPSec（Internet Protocol Security）

- IPの拡張プロトコル
- RFC 2401～2412、2451、3948、4308等
- Ipv6では実装が必須となった。
- 暗号化をIP（Internet Protocol）プロトコルレベルで行う。
  - 上位のアプリケーションでは暗号化のことを特に意識する必要はない。
  - SSLはアプリケーション層で暗号化を行う。

205

IPSecの手順

- 暗号アルゴリズムと鍵の交換
  - フェーズ1、フェーズ2でネゴシエーション
- SA（Security Association）
  - 暗号化アルゴリズムや暗号鍵に関する合意
- SPI（Security Pointer Index）
  - SAに関係づけられた32ビット値。
  - パケットに書かれ、SAを指定する。
- プロトコル
  - IKE（Internet Key Exchange）
  - ESP（Encapsulating Security Payload）
  - AH（Authentication Header）

206

IKEによる鍵交換

- 自動的にSAの合意を取る
- IPSecによる暗号化以前なので、IKE自身で暗号化を行う。
  - Phase1：Diffie-Hellmanによって、Phase2で使う共有鍵を決める。
  - Phase2：Phase1の鍵でIPSecによる暗号化通信のためのネゴシエーションを行う。
  - ESPによる暗号化データ転送

207

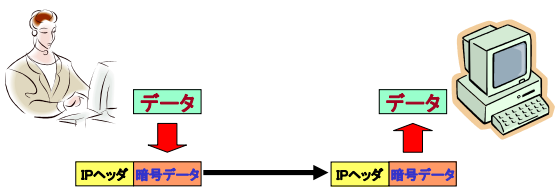
接続手順

IKEでの鍵交換が味噌

208

トランスポート・モード

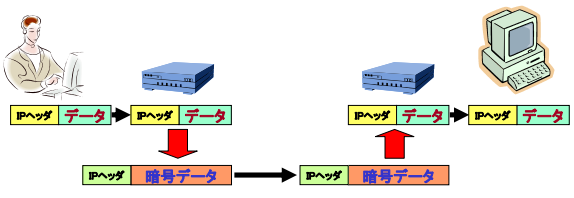
- データ部を暗号化
- 送信先のIPヘッダをつけて直送



209

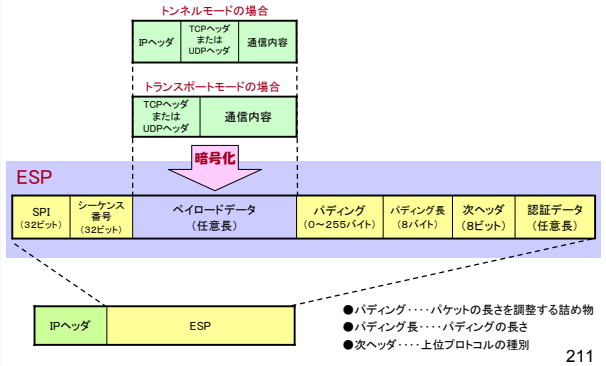
トンネル・モード

- データ＋送信先のIPヘッダをGWで暗号化
- 受信側GWで復号したIPヘッダへ送出



210

IPSecパケットの構造

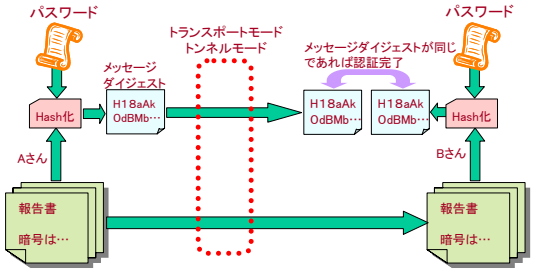


211

認証と完全性

MAC（Message Authentication Code）

通信内容と共有しているパスワードを
ハッシュ化してメッセージダイジェストを生成



212

暗号化が定義されているポート番号

プロトコル	暗号	通常	プロトコル名
https	443	80	http protocol over TLS/SSL
nntps	563	119	nntp protocol over TLS/SSL
ldaps	636	389	ldap protocol over TLS/SSL
ftps-data	989	20	ftp protocol, data, over TLS/SSL
ftps	990	21	ftp protocol, control, over TLS/SSL
telnets	992	23	telnet protocol over TLS/SSL
imaps	993	143	imap4 protocol over TLS/SSL
ircs	994	194	irc protocol over TLS/SSL
pop3s	995	110	pop3 protocol over TLS/SSL

213

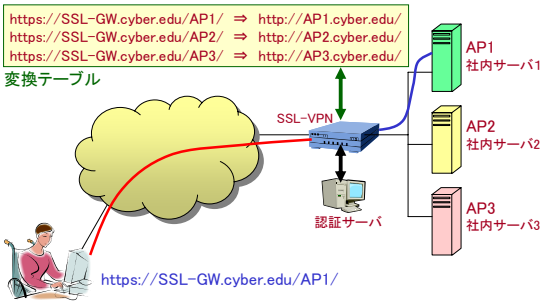
SSL-VPN

- Netscape Communicatinos社が提唱
- リバースプロキシ＋SSL技術
- リモートアクセス型VPN
- IETFでRFC化されている
- SSL-VPN装置で、URLを読替え変換して社内ネットワークをアクセスする。
- 基本的にWebベースのアプリケーションが対象となる。

214

SSL-VPNの動作概要

社内サーバはWebベースで動作することが条件



215

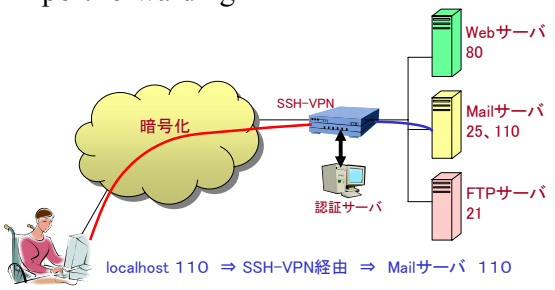
Webに対応していないアプリは？

- SSL対応のクライアントアプリを使用
  - MSのOutlook ExpressはSSL-VPN機能を持つ
- SSL-VPN用のJavaアプレットを使う
  - HTTP以外のプロトコルをJavaアプレットで処理する。
  - SSLをトンネルとして利用する
- SSL-VPN専用アプリを使用
  - ブラウザの代わりに専用アプリを用意する。
  - SSLをトンネルとして利用する
- いずれも必要とするポートを開ける

216

SSH-VPN

- ポートフォワーディング技術
  port forwarding



217

SSH-VPNの特徴

- SSHをサポートしていればそのまま使える
- クライアントとSSH-VPN間の通信はSSHにより暗号化される
- クライアントの localhost 宛の指定されたポートへの通信を、SSH-VPNのGWを経由して、指定されたホストの指定されたポートへ転送する。
- クライアント側のアプリケーションは、社内ネットと同じものが使える。

218

ウイルス

（基礎編第8回に相当）

219

ウイルスの定義

「コンピュータウイルス対策基準」（通商産業省（当時）が告示）
『第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの』

1. 自己伝染機能
   自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能
2. 潜伏機能
   発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、条件が満たされるまで症状を出さない機能
3. 発病機能
   プログラムやデータ等のファイルの破壊を行ったり、コンピュータに異常な動作をさせる等の機能

引用：IPA「ウイルス対策スクール」
http://www.ipa.go.jp/security/y2k/virus/cdrom/basic/basic_f.html

220

ウイルスの分類

- メール機能悪用型
  - メール添付ファイルを介して感染拡大する
- セキュリティホール悪用型
  - OSや広く使われているソフトウエアの脆弱性を悪用するウイルス。メールを開いたりプレビューしたり、Webを閲覧するだけで感染することもある。
- ネットワーク感染型
  - 脆弱性を悪用し、ネットワークにつないだだけで感染する。セキュリティホール悪用型の一種。
- ファイル感染型
  - 感染したプログラムファイルを実行すると感染する。
- マクロ感染型
  - WordやExcelなどの文書ファイルのマクロプログラムに感染し、文書を開くと感染が広がる。
- ブートセクタ感染型
  - パソコンの起動を行う時、最初に参照するデータ領域をブートセクタと呼び、ブートセクタに感染しているFDDなどでパソコンを起動するとHDDにも感染する。

221

ウイルスの分類

- メール機能悪用型
  - メール添付ファイルを介して感染拡大する
- セキュリティホール悪用型
  - OSや広く使われているソフトウエアの脆弱性を悪用するウイルス。メールを開いたりプレビューしたり、Webを閲覧するだけで感染することもある。
- ネットワーク感染型
  - 脆弱性を悪用し、ネットワークにつないだだけで感染する。セキュリティホール悪用型の一種。
- ファイル感染型
  - 感染したプログラムファイルを実行すると感染する。
- マクロ感染型
  - WordやExcelなどの文書ファイルのマクロプログラムに感染し、文書を開くと感染が広がる。
- ブートセクタ感染型
  - パソコンの起動を行う時、最初に参照するデータ領域をブートセクタと呼び、ブートセクタに感染しているFDDなどでパソコンを起動するとHDDにも感染する。

222

ワームとトロイの木馬

【ワーム】
- ウイルスのように寄生せずに、自分自身のコピーを送り込む。
- ネットワーク上をウロウロするのがミミズが這うようなイメージ

【トロイの木馬】
- 普段は有益なプログラムの装い、ある条件で不正な動作を行う。
- ギリシア神話のトロイア戦争において、オデッセウスが送り込んだ木馬にちなむ

ウイルス類も「合せ技」が進んできているので、最近は敢て分類しない場合も多い。

223

ウイルス対策ソフトの例

社名	代表製品	URL
アラジンジャパン	eSafe	http://www.aladdin.co.jp/
イーフロンティア	ウイルスキラー、 ウイルスキラー北斗の拳	http://www.viruskiller.jp/
シマンテック	Norton Internet Security、 NortonAntiVirus、	http://www.symantec.com/region/jp/
ソフォス	Sophos Anti-Virus	http://www.sophos.co.jp/
トレンドマイクロ	ウイルスバスター、Inter Scan	http://www.trendmicro.co.jp/
日本エフ・セキュア	F-Secure アンチウィルス	http://www.f-secure.co.jp/
マカフィー	VirusScan 、GroupShield	http://www.mcafee.com/jp/
ソースネクスト	ウイルスセキュリティ ウイルスセキュリティZERO	http://sec.sourcenext.info/
CANONシステムソリューション	NOD32 アンチウイルス	http://canon-sol.jp/product/nd/
Grisoft	AVG Anti-Virus	http://www1.grisoft.com/doc/1/lng/jp/
ALWIL Software	avast! Home Edition	http://www.avast.com/index_jpn.html

224

スパイウエア Spy Ware

- 『利用者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集し、利用者以外のものに自動的に送信するソフトウェア』

  引用：IPA　http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html
- 似た意味の用語
  - マルウエア　(Malware)　不正プログラムの総称
  - アドウェア　(Adware)　広告用途の情報収集

225

不正プログラムの種類

ウイルス	メールや記憶媒体等の宿主を介して自己感染を繰り返すプログラム
ワーム	ネットワーク経由で自己増殖を繰り返すプログラム。受動的攻撃によって攻撃を仕掛ける、あるいは感染するプログラム
受動的攻撃	攻撃される側のアクション(Webを閲覧する等)によって感染するプログラム
トロイの木馬	普通のプログラムを装って侵入するプログラム
バックドア	PCを外部から操作できるようにするプログラム。デバッグ用に作りこまれることもある
ルートキット	バックドアなどの存在を隠蔽する仕掛けやプログラム
スパイウエア	PCの情報を勝手にメール等で攻撃者へ送付するプログラム
アドウエア	広告用の情報を収集し、ユーザの嗜好に合わせた広告を表示するプログラム
キーロガー	ユーザーのキー入力などを記録するプログラム。スパイウエアで盗聴に使われる
フラッダ(Flooder)	DoS/DDoS攻撃を行うためのプログラム。トロイの木馬型で感染するものが多い
ドロッパ(Dropper)	ゲーム等を装い他のマルウエアをダウンロードするトロイの木馬型マルウエア
ボットネット	ボットと呼ばれるマルウエアに感染したPCで構成されるネットワーク。IRC等を経由して、感染活動やDDoS攻撃、情報収集、スパムの送信などを行う
フィッシング	銀行などを騙ったメールに書かれたURLをアクセスするなどすると、個人情報が盗み出だされる仕掛け。特定の組織や個人をピンポイントで狙うスフィア型フィッシングもある。
暴露型ウイルス	破壊型ウイルスと異なり、PCのデータを不特定多数に漏洩させるマルウエア
ゾンビ	感染すると、ネットワーク上の他のPCにも攻撃を仕掛ける。DDoS攻撃等に使われる。

226

マルウエアの分類

感染・侵入形態に対する呼び方	**狭義のウイルス** メールやメディアを使って感染する 何らかのアクションで感染するもの	**トロイの木馬型感染** 実行を行わないと感染しないもの 実行ファイルの添付など	**ワーム** プログラムの脆弱性を使ってネットワークから感染する 利用者のアクションが無くても感染する	**受動型感染** WEBなどにアクセスすることで感染する	その他
動作に対する呼び方	**感染活動** 感染/拡散活動を行う 必ずしも自動的とは限らない	**バックドア** 外部からの操作を有効にする機能を持つプログラムの総称 **ルートキット** バックドアの存在を隠蔽する手法・ツールの総称	**スパイウェア** バックドアの一種 利用者の行為やデータを盗み出す **アドウエア(の一部)** スパイウエア的な活動をする。	**破壊活動** ディスクの破壊など **DoS攻撃(Flooder)** DDoS攻撃を行う **ドロッパ(Dropper)** 他のマルウエアのダウンロードを行う	その他
ネットワーク形態に対する呼び方	**(単独：名称なし)** 特に連携をとらないもの DDoS機能をもつウイルスも、特に連携はとらない場合、このカテゴリ	**殻なネットワーク** **(特に名称なし)** バックドア機能を持つウイルスを利用するための、アドホックなネットワーク	**DDoSネットワーク** DDoS Zombieによって構成される、DDoSを目的としたネットワーク	**ボットネット** **(ゾンビクラスタ)** 多数のノードを分散システム的に管理できる仕組みを持つもの	その他
手法に対する呼び方	**(特に名称なし)** 一般に言うところのウイルス活動手法	**スピアフィッシング** 特定の組織に侵入することを目的とした手法	**暴露型ウイルス** 情報を盗み出し、公開することを目的とした手法	**DDoS攻撃** 多数のFlooderによって実施される、分散型のDoS攻撃	その他
目的に対する呼び方	**愉快犯**	**情報の盗難**	**詐欺行為**	**商売行為**	その他

出展：日経BP「ITpro」http://itpro.nikkeibp.co.jp/article/COLUMN/20060421/235970/
マイクロソフト　高橋 正和氏

227

最近の攻撃傾向

- スピア攻撃
- 無作為攻撃から特定攻撃へ
- 不特定多数を狙わないので、ウイルス対策ソフトやスパイウエア対策ソフトなどではチェックできない。
- 検体数がある程度多くないと、対策ソフトに反映されない。

228

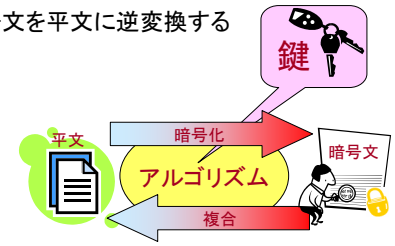
暗号・認証理論（1）

（基礎編第9回に相当）

229

暗号の基本

平文（人間が読める文書）を
アルゴリズムを使って
暗号文に変換する
暗号文を平文に逆変換する



230

共有鍵暗号方式

- 共有鍵暗号 secret key cryptosystem
- 対称鍵暗号 symmetric key cryptosystem
- 共有鍵暗号 shared key encryptosystem
- 共通鍵暗号 common key encryptosystem
- 秘密鍵暗号 Private key encryption system
- 慣用暗号 conventional encryption system

- ひとつの「鍵」を送り手と受け手で持っていることで、暗号化と複合を行う。
- あらかじめ「鍵」をお互いに知っておく必要がある。

231

公開鍵暗号方式

- 公開鍵暗号 public key cryptosystem
- 非対称鍵暗号 asymmetric key cryptosystem
- 2つ以上の鍵を暗号化・復号化に使い分ける暗号化アルゴリズム。

232

公開鍵暗号の「鍵」

- 公開鍵（Public Key）
  - 他人に広く公開される鍵
- 私有鍵（Private Key）
  - 秘密鍵 、プライベート鍵
  - 本人だけが使えるように厳重に管理される

233

公開鍵と私有鍵の関係

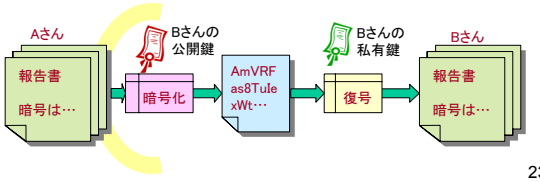
- 公開鍵で暗号化されたデータは対応する秘密鍵でしか復号できない
  ⇒相手を特定できる
- 私有鍵で暗号化されたデータは対応する公開鍵でしか復号できない
  ⇒不特定の相手
  ⇒著名者を特定できる

234

公開鍵の使い方（暗号）

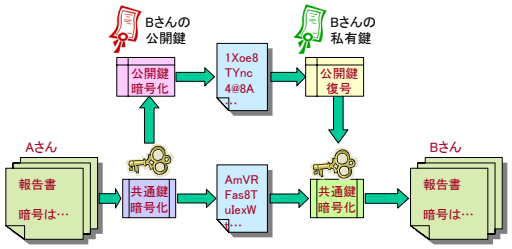
・暗号としての利用：
- 受取者の公開鍵で暗号化
- 受取者の私有鍵で復号

【原理】



235

暗号化データの実例



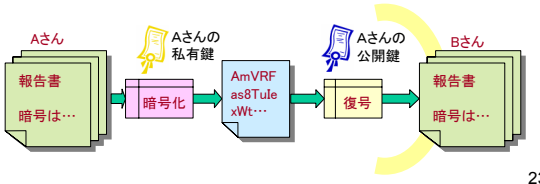
・ 公開鍵方式は処理速度が遅い（3桁）
⇒本文には共通鍵暗号方式を使う
・ 共通鍵を送るのに公開鍵方式を使う

236

公開鍵の使い方（署名）

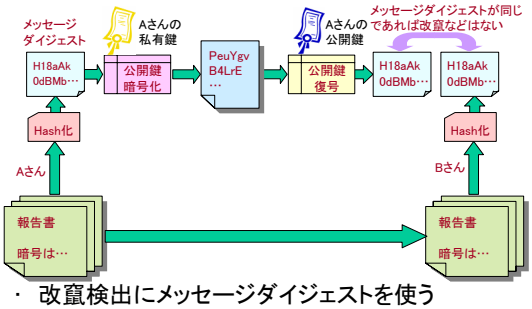
・署名としての利用：
- 署名者の私有鍵で署名
- 署名者の公開鍵で複合

【原理】



237

署名データの実例



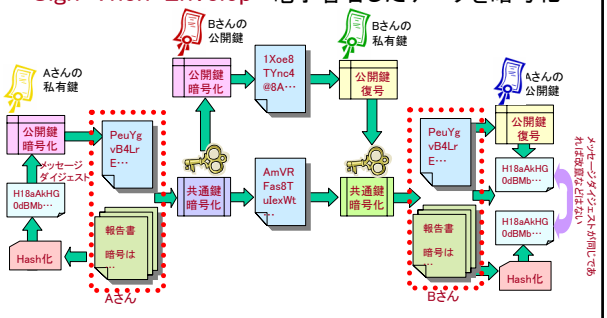
・ 改竄検出にメッセージダイジェストを使う
- Hash関数で任意長の平文を固定長のメッセージダイジェストに変換する。

・ 平文はそのまま相手に送る

238

電子署名＋暗号化(1)

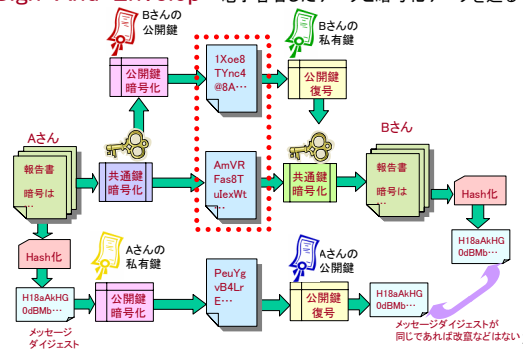
Sign-Then-Envelop　電子署名したデータを暗号化



239

電子署名＋暗号化(2)

Sign-And-Envelop　電子署名したデータと暗号化データを送る



240

暗号を使う目的（1）

(1)機密性 (Confidentiality)
第三者に「盗聴」されないこと
盗聴された場合は、大規模な漏洩が起こる可能性がある。（第5回参照）
盗聴されている側は、事故が起こるまで、盗聴されている事に気付かない

241

暗号を使う目的（2）

(2)完全性 (Integrity)
インターネットを流れるデータを盗聴し、データの内容を「改竄」することも簡単
「改竄」が巧妙であれば、発見は難しい
10万円でパソコンを買ったのに、100万円が引き落とされていたら気付くだろうが、11万円の引き落としだったら、気付かないかも知れない。

242

暗号を使う目的（3）

(3)認証 (Authentication)
通信を横取りし、他人への「成りすまし」を行うことも可能。
相手が「本人」かどうかを判断するのが難しくなっている。
「成りすまし」を防ぎ、相手が「本人」かどうかを確認するために「認証」という考え方が必要になる。
本人性の確認が絶対ではない。匿名性を保持したまま、支払い可能性など必要な条件を確認できれば社会基盤としては十分な場合が多い。

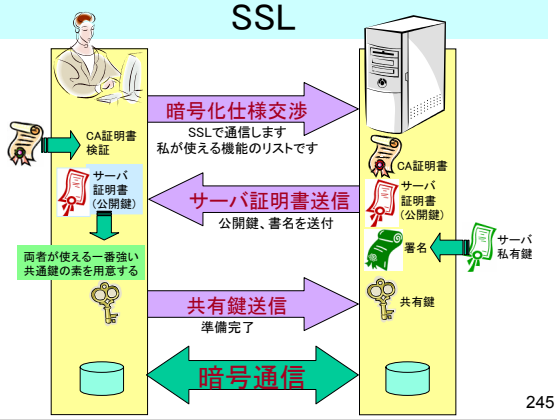
243

暗号を使う目的（4）

(4)否認防止 (Non Repudiation)
ある情報を送ったことを「否認」出来ないことを保障。
実際には送ったのに「送っていない」、「知らない」と言うことを防止する。
インターネット上での取引を行う上で重要な条件
注文側が「私はそんな注文していない」
受注側が「そんな注文は受けていない」という。

244

SSL



245

暗号方式の歴史

ヒエログラフ　古代エジプトの象形文字　BC19世紀頃の石碑
ステガノグラフィフィ（Steganography）
- 木は森に隠せ（目立たないところに隠す）
- 秘匿式（電子透かし）

サイファ形式（Cipher）
- 約束に従って文字やビットを1対1で置き換える
- 換字式（シーザー暗号：数文字ずらす）
- 置換式（出現位置を変換する）
- 転置式（逆さ言葉等）
- 分置式（ためき）
- 混合形式（DES等）

コード形式（Code）
- 文字列のまとまりを予め決められた言葉や記号で置き換える
- 隠字式（あぶりだし等）
- 隠語式（符丁・符牒等）
- 比喩式（古文における歌等）

共有鍵暗号（Shared Key Encryption）
- RC4

公開鍵暗号（Public Key Encryption）
- RSA暗号

量子暗号（Quantum cryptography）

246

Cipher Disc

暗号文:

平文:

C Y B E R

鍵:

S E C U R I T Y

暗号文:

U C D Y I

多表式換字暗号(シーザー暗号)

・決められた文字数分シフトする
・例えば3文字毎に区切る

平文(情報セキュリティ)	jou	hou	sec	uri	ty
鍵(ずらす文字数)	753	753	753	753	753
暗号文	qtx	otx	yjf	bwl	ad

・16世紀ヨーロッパで考案。アンリー4世の家臣のフランソワ・ヴィエト
・同じ文字でも別の文字に変換され解読困難。

平文(情報セキュリティ)	jouhousecurity
鍵(ずらす文字数)	08033654396
暗号文	jwukrcxifdxiby

・鍵が長くなればなるほど解読困難
・電話番号を鍵にする

248

アトバシュ暗号

旧約聖書にあるヘブライ語の換字方式暗号
アルファベット順を途中で折り返し対応表にする
ダヴィンチコードでも使われていた

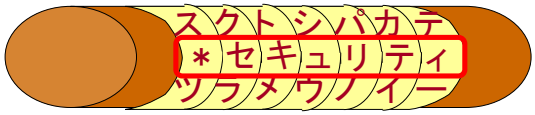
A	B	G	D	H	V	Z	Ch	T	Y	K
Th	Sh	R	Q	Tz	P	O	S	N	M	L

B a P V o M e Th (母音は表記されない)
Sh V P Y A (pはfと同じ、vは母音のoになる)
S…o…f…y…a

引用:「ダ・ヴィンチ・コード」ダン・ブラウン著 越前敏弥訳 角川書店 249

置換方式

スキュタレー



暗号文:

…ス＊ツ…クセラ…トキメ…シュウ…パリノ…カテイ…ティー…

鍵: 棒の太さといえる。

250

いろは歌の暗号

「咎無くて死す」
かきのもとのひとまろ(柿本人麿)

い	ろ	は	に	ほ	へ	と
ち	り	ぬ	る	を	わ	か
よ	た	れ	そ	つ	ね	な
ら	む	う	ゐ	の	お	く
や	ま	け	ふ	こ	え	て
あ	さ	き	ゆ	め	み	し
ゑ	ひ	も	せ	す		ま

251

転置式

文字の並べ替えを行い、意味がない状態、あるいは別の意味の文にする。

O, Draconian devil!
Oh, lame saint!

13 3 2 21 1 1 8 5
1 1 2 3 5 8 13 21

Leonardo da Vinci!
The Mona Lisa!

引用:「ダ・ヴィンチ・コード」ダン・ブラウン著 越前敏弥訳 角川書店 252

近代の暗号方式

- 共有鍵暗号・対称暗号 (Shared Key Encryption)
- 公開鍵暗号・非対称暗号 (Public Key Encription)
- ハイブリッド暗号
- ストリーム暗号 (Stream cipher)
  - 平文をビット毎に逐次暗号化する
    - 平文の量が予測不可能な場合に適している
  - 平文のサイズと暗号文のサイズが同じ
  - RC4、バーナム暗号(Vernam cipher)
- ブロック暗号 (Block cipher)
  - 平文を一定の量(ブロック)単位でまとめて暗号化する
  - 平文が全て揃わないと暗号化処理を開始することができない
  - DES, AESShar

253

準備運動(ブール代数)

論理演算

- 論理和 or＋∨
- 論理積 and・∧
- 論理否定 not^ ¬

真理値表

0 + 0 = 0
1 + 0 = 1
0 + 1 = 1
1 + 1 = 1

+	0	1
0	0	1
1	1	1

0 ・ 0 = 0
1 ・ 0 = 0
0 ・ 1 = 0
1 ・ 1 = 1

・	0	1
0	0	0
1	0	1

^0 = 1
^1 = 0

^	
0	1
1	0

排他的論理和
exclusive-or
⊕

0 ⊕ 0 = 0
1 ⊕ 0 = 1
0 ⊕ 1 = 1
1 ⊕ 1 = 0

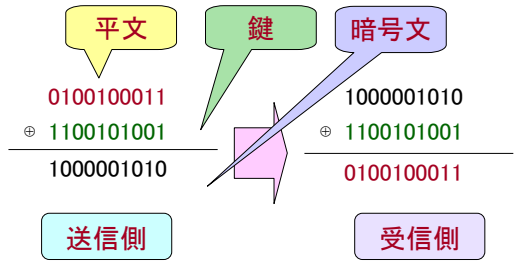
⊕	0	1
0	0	1
1	1	0

254

共有鍵方式の原理

暗号化と複合に同じ鍵を使う
- 送信者と受信者があらかじめ鍵を共有する

XORを2回行うと元に戻る



255

公開鍵方式の原理

- 1976年アイディアが発表
  Whitfield Diffie, Martin Hellman
- 共有鍵の配送問題が解決できる
- RSA暗号
  - Ron Rivest, Adi Shamir, Leonard Adeleman
  - 大きな数の素因数分解は困難である


Adi Shamir

256

RSA公開鍵方式の原理

暗号化と複合はべき乗して剰余を取る

暗号文 $C=M^e \pmod n$

平文 $M=C^d \pmod n$

鍵の生成

p, q : 素数(実際には大きな素数)

n = p・q (これを「法」とする)

e = 任意の数(暗号鍵)

$$d = \frac{(p-1)*(q-1)+1}{e}$$ (複合鍵)

257

暗号／複合の例

素数:p=3, q=11, n=33

暗号鍵: e=3

復号鍵: d=((3−1)(11−1)＋1)/3

=(2・10＋1)/3 = 21/3 = 7

平文: 13 4

暗号化: $13^3 \pmod{33} = 19$ 暗号文

$4^3 \pmod{33} = 31$

復号: $19^7 \pmod{33} = 13$

$31^7 \pmod{33} = 4$ 平文

258

量子暗号

- Quantum cryptography
- 現在の暗号は「計算量的安全性 」に基づく
- 秘密鍵暗号方式で利用する鍵を量子力学的原理によって安全に配布する。
- 情報そのものを量子力学的に暗号化して盗聴を不可能にする。

259

BB-84方式

- 1970年 Wiesnerが発表
- 1984年 C. BennettとG. Brassardが実装
- 量子鍵配送（Quantum Key Distribution：QKD）
- 量子テレポーテーション
  - 光子レベルの状態を利用する
- 暗号カギの生成速度：100Kbps程度
- B92(1992年Bennet)
  E91(1991年Ekert)

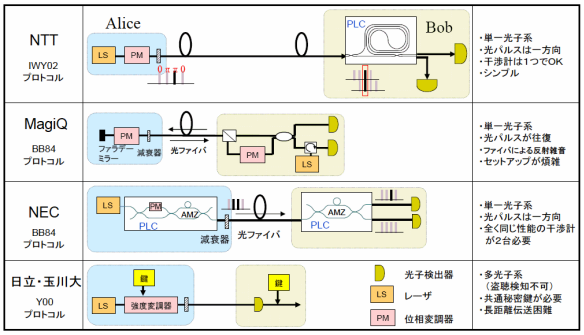
260

Y-00方式

- 2000年H・P・ユエン教授（米ノースウエスタン大学）
- 「量子ゆらぎ」を利用
  - 強度変調
  - 量子揺らぎに基づいて設定された複数のレベルで01の判定レベルを決め、更に判定レベル自体をアルゴリズムにしたがってダイナミックに変化させる方式
- 高速暗号化通信：数Gbps
- 計算量的安全性を超えるかについて賛否両論がある

261

量子暗号技術の対外比較



http://www.rcast.u-tokyo.ac.jp/ja/research/meeting/2005/0413/pdf/01.pdf
出典：「量子暗号」2007年　東京大学先端科学技術研究センター　高柳英明氏

262

暗号アルゴリズム

代表的なもの

AES	**A**dvanced **E**ncryption **S**tandardとしてNISTによってFIPSに上げられたブロック暗号
Blowfish	Bruce Schneier設計によるブロック暗号
DES	Data Encryption Standard.　FIPS PUB 46-2で定義されているブロック暗号
トリプルDES/DESede	DESを3重に使用するブロック暗号
PBEWith<digest>And<encryption>	パスワードベースの暗号化アルゴリズム
RC2, RC4, RC5	RSA Data Security社が策定したブロック暗号。鍵長/段数を可変に出来るのが特徴
RSA	PKCS#1で定義されている公開鍵暗号

263

電子政府推奨暗号リスト（1）

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS#1 v1.5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS#1-v1.5
	鍵共有	DH
		ECDH
		PSEC-KEM

出典：IPA/NICT “CRYPTREC Report 2005”

264

電子政府推奨暗号リスト（2）

技術分類		名称
共通鍵暗号	64ビットブロック暗号	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES
	128ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4

出典：IPA/NICT “CRYPTREC Report 2005”

265

電子政府推奨暗号リスト（3）

技術分類		名称
その他	ハッシュ関数	RIPEMD-160
		SHA-1
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+change notice 1) revised Appendix 3.1

出典：IPA/NICT “CRYPTREC Report 2005”

266

公開鍵暗号の歴史

1976年 Diffie, Hellmanが秘密鍵の交換方法を発表する

1977年 Rivest, Shamir, AdlemanがRSA暗号を発表する

1979年 RabinがRabin暗号を発表する

1982年 ElGamalがElGamal暗号を発表する

1985年 KoblitzとMillerがほぼ同時に楕円曲線暗号を発表する

1991年 Koyama, Maurer, Okamoto and Vanstoneが楕円曲線を用いたRSA暗号及びRabin暗号を発表する。

267

公開鍵暗号の具体的なアルゴリズム

- RSA暗号
- 楕円曲線暗号
- ElGamal暗号

268

CRYPTREC

- Cryptography Research and Evaluation Committees
- 電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクト
- 暗号技術検討会
  - 座長：今井秀樹東京大学教授
  - 総務省及び経済産業省が共同で開催
- 暗号技術監視委員会
  - 委員長：今井秀樹東京大学教授
  - 独立行政法人情報通信研究機構（NICT）
  - 独立行政法人情報処理推進機構（IPA）が共同で開催
- 暗号モジュール委員会
  - 委員長：松本勉横浜国立大学教授

269

暗号・認証理論（2）

（基礎編第10回に相当）

270

ハッシュ関数の概要

- ハッシュ関数
  - 任意長のデータを入力として固定長のデータ（ハッシュ値）を出力する機能
  - 一方向性と衝突困難性
- 代表的なハッシュ関数
  - MD5
    - 1991年にRivestが開発。
    - 128ビット
  - SHA-1
    - **1995年**に、NSAが開発。
    - 160ビット
    - 後継としてSHA-2ファミリと呼ばれるSHA-224, SHA-256、SHA-384、SHA-512がある

271

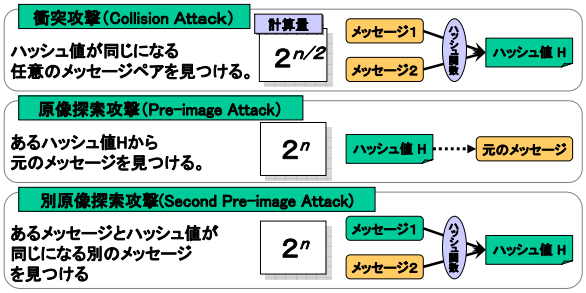
ハッシュ関数に関する危殆化の報告

- MD5
  - 2004年、X. Wangらにより、Collisionが2^{-37}で発見できることが発表される。
  - 2005年、A. Lensta、X. Wangらにより、ハッシュ値が衝突した2つの証明書ペアが作成される。
  - 2005年、V. Klimaがより高速にCollisionを発見する手法を提示。

- SHA-1
  - 2005年2月、X. WangさんによりCollisionが2^{-69}で発見できることが発表される。
  - 2005年10月、同じくCollisionが2^{-63}で発見できると発表される。

272

ハッシュ関数への攻撃手段



273

IETFでのHash対応の方向性

- SHA-256などSHA2ファミリーへの移行
  - 移行負荷が大きい。時間もかかる。
  - 運用だけでなく**関連アプリケーションとの相互運用性**についても配慮の必要あり
- SHA-1互換の安全な実装検討
  - 上記のような関連アプリケーションとの相互運用性問題を回避するため、現行SHA-1とできるだけ互換性の高い改善案の検討
    - IETF Hash BOFの3つの提案(63rd IETF ミーティング（パリ）)
- 新しいハッシュ関数を組み込んだTLS 1.2の検討
  - Eric Rescorla(TLS WG Chair)とSteve Bellovin(IETFセキュリティエリアの元ディレクタ)の見解
  - RFC化に2年、ベンダが設計・開発・テストするのにもう1、2年展開に3～5年

274

ソフトウェア実装性能(cycles/byte)

アルゴリズム	PIII/Win98（系列1）	PIII/Linux（系列2）	PIII/Win00（系列3）	P4/Linux（系列4）
MD4	–	4.7	4.5	6.4
MD5	3.66	7.2	6.8	9.4
RIPEMD-128	6.64	–	–	–
RIPEMD-160	11.34	18	16	26
SHA (SHA-0)	–	15	12	23
SHA-1	8.30	15	13	25
SHA-256	20.59	39	39	40
SHA-384	–	83	74	122
SHA-512	40.18	83	74	122
Whirlpool	36.52	46	73	60

PIII/Win98: Pentium III (800MHz, 256MB RAM), Windows 98, Visual C++, MASM 6.15. 文献 [NM03] に示されている様々な実装方法のうち、最速のものを引用.
PIII/Linux: Pentium III (450MHz, 256MB RAM), Linux 2.4.17, gcc 3.1.1 など. 測定環境は何種類かあるが、サイクル数はほぼ同一 [NESSIE03].
PIII/Win00: Pentium III (850MHz, 256MB RAM), Windows 2000, gcc 2.95.3 など. 測定環境は何種類かあるが、サイクル数はほぼ同一 [NESSIE03].
P4/Linux: Pentium 4 (1.8GHz), Linux 2.4.0, gcc 2.95.2 など. 測定環境は何種類かあるが、サイクル数はほぼ同一 [NESSIE03].

出典：IPA/NICT "CRYPTREC Report 2005"

275

暗号・認証理論（3）

（基礎編第11回に相当）

276

認証の種類

Authentication

- 真正性の確認
- 正当な本人であることを確認する

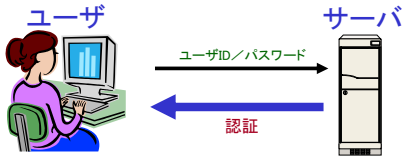
Certification

- 証明書により何らかの権威者が何事かを証明する
  - 会社が社員を。自治体が市民を。カード会社が利用者を。

277

二者間認証

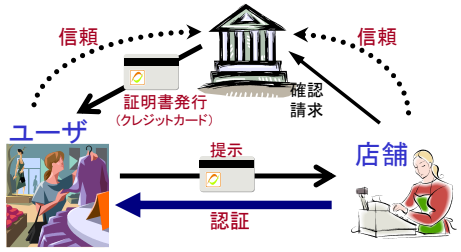
- 認証される側とする側が予め共有している情報を使って確認すること



278

第三者認証

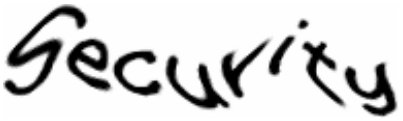
- 信頼できる第三者機関（認証局）が発行した証明書を基にして、「持ち主」の正当性を確認すること



279

Captcha（キャプチャ）

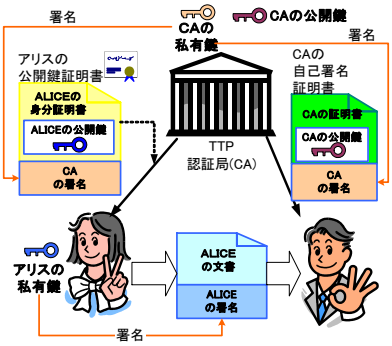
- Carnegie Mellon Universityが商標登録
- 相手が人間であることを確認したい
  - 自動認識し難い画像でも人間は理解できる
  - ID/PWなどの情報を搾取しようとする場合は、画像自体を盗聴すればよいので、万能ではない。



280

信頼できる第三者機関による署名での認証

Aさん（アリス：Alice）の公開鍵をどのように信頼するか



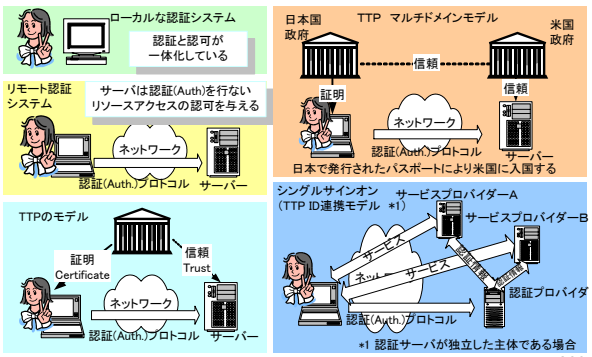
281

TTP（Trusted Third Party）

- 信頼できる第三者機関
- TTPによって署名されたデータは信用できるものとする
- 代表的な例はCA（Certification Authority：認証局）
- CAは印鑑証明を発行してくれる役所のイメージ
- 公的個人認証サービスでは、都道府県CAが市民のための証明書を発行する。

282

認証のモデル



283

生体認証

- 生体情報の条件は、全ての人が持つ特徴であること、同じ特徴を持つ他人がいないこと、時間によって特徴が変化しないこと、が挙げられる。
- 生体情報は、基本的にアナログ長方であり、パターンマッチング技術が基礎になっている

指紋	犯罪捜査にも用いられ、信頼性の高い認証方式であるが、利用者の心理的抵抗が大きい。更には指紋のコピー法も作られてしまっている。
網膜	目の網膜の毛細血管のパターンを認識する方法。
虹彩	虹彩パターンの濃淡値のヒストグラムを用いる認証方式。双子でも正確な認証を行えることから、高い認証精度を有している。
顔	虹彩パターンの濃淡値のヒストグラムを用いる認証方式。双子でも正確な認証を行えることから、高い認証精度を有している。
血管	近赤外光を手のひら、手の甲、指に透過させて得られる静脈パターンを用いる技術が実用化されている。
音声	声紋 を利用したものが良く知られている。
筆跡	有効な認証方法のひとつとして考えられているが、筆跡は、似せようと思えば、似せ得るもの。したがって、決して確実な方法ではない。
DNA	最も確実な究極的な生体認証の手段であるが、確認のためには(血液や、唾液などの)サンプルの提出を必要とし、現時点においては瞬時に相手を見極める装置は開発されていない。

出典: フリー百科事典『ウィキペディア(Wikipedia)』

284

PKI

- Public Key Infrastructure
- 公開鍵暗号技術と電子署名を使って、インターネット上で安全な通信ができるようにするための環境のこと
- なりすましやデータの盗聴、改竄を防ぐ
- インターネット上で、目的に応じた通信の安全性を確保できる有力な方法。
- 証明書の確認に掛かる手数が一番コストが掛かることが多い
- 各国の電子政府の認証方式として利用されている。
- 日本でも、電子政府、医療関係、教育関係、等々で普及促進がされている。

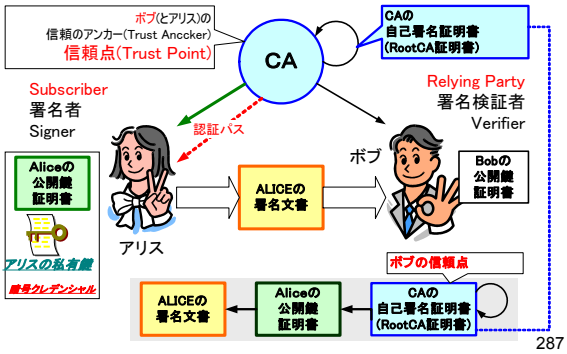
285

デジタル(電子)証明書 X.509

version	証明書バージョン番号(V3)
serialNumber	認証局が割当てるシリアル番号
signature	公開鍵証明書の署名アルゴリズム
issuer	発行認証局のX.500識別名
validity	有効期間(開始/終了日時)
subject	所有者のX.500識別名
subjectPublicKeyInfo	証明する公開鍵の値
issuerUniqueIdentifier	認証局の固有識別子
subjectUniqueIdentifier	所有者の固有識別子
extensions	V3の拡張フィールド
extnId	拡張型
extnValue	拡張値
critical	クリティカルビット

286

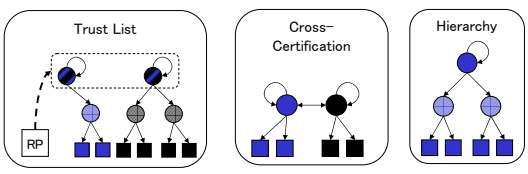
単純なPKIのモデル



287

認証局 (CA) 同士の相互信頼

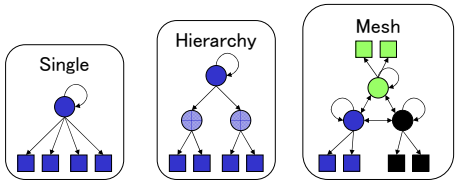
- 信頼リストを共有する
- 相互認証を行う
- 階層的に認証を行う



288

シングルドメインPKI

シングルドメインでのPKIモデル
- シングルPKIモデル
- 階層PKIモデル
- メッシュPKIモデル

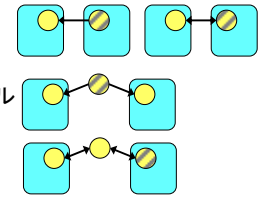


289

マルチドメインPKI

マルチトラストポイントモデル
- トラストリストモデル

シングルトラストポイントモデル
- ピアツーピアモデル
  - 片方向相互認証
  - 双方向相互認証
- ユニファイドドメインモデル
- ブリッジモデル



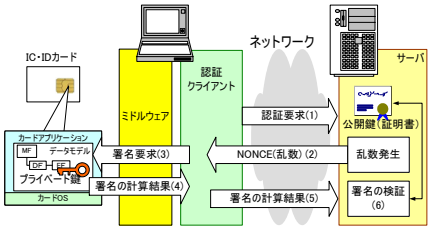
290

PKIを用いた認証（Authentication）

チャレンジ・レスポンス認証

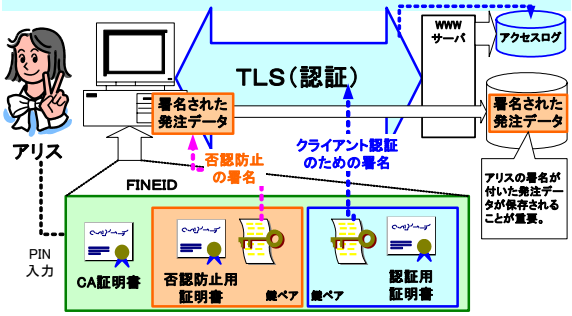
アリスの秘密情報（私有鍵）はハードウェアトークンから出ない
- もちろんネットワークにも流れない

アリスの秘密情報は、サーバには、格納されない
- サーバは、アリスの秘密情報（例えばパスワード）を預かる必要がない
- これは、アリスとっても、サーバの運用者にとってもメリット



291

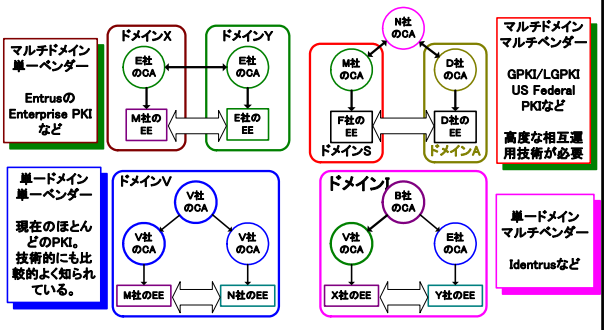
電子認証(Auth.)と電子署名の違い



電子政府などでは、**文書に署名**され、**署名された文書が保存**されることが重要。欧州の市民カードは、**2種類の証明書**を使っている。

292

マルチベンダ、マルチドメインPKI



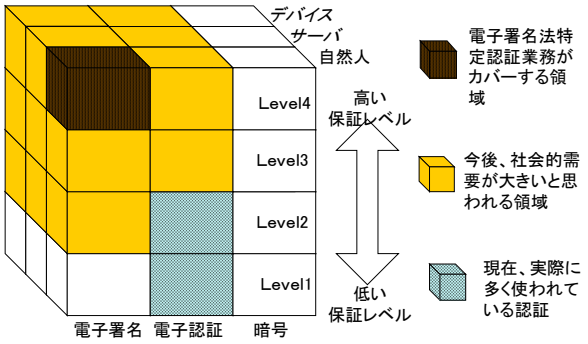
293

各国の認証サービス

IC・ID カード	カード保有者の証明書とプライベート鍵の種類	説明
FINEID フィンランド	認証、暗号用の証明書	（認証のための）署名操作と暗号文からの復号に使用。PIN 1によるカード保有者の認証。
	否認防止の署名用証明書	署名操作のみ。署名操作毎にPIN2によるカード保有者の認証が必要。
BELPIC ベルギー	認証用の証明書 PrK#2	（認証のための）署名操作に使用。復号できない（暗号には利用できない）。PINによるカード保有者の認証。
	否認防止の署名用証明書 PrK#3	署名操作のみ。署名操作毎にPINによるカード保有者の認証が必要。否認防止の署名用証明書は、18歳以上に発行される。
PIV 米国	PIV認証鍵 証明書	個人識別番号（PIN）を使用してカードおよびカード保有者を識別する際には、FIPS 201で定義されているPIV認証鍵を使用する。
	ディジタル署名鍵 証明書（オプション）	この鍵と認証は、文書に署名するためのディジタル署名の使用をサポートする。「常にPIN」というアクセス規則によって保護される。これには、鍵を使用してディジタル署名を生成するたびに、カード保有者が関与する必要がある。
	鍵管理鍵 証明書（オプション）	この鍵ペアは、鍵復元のために発行者がエスクローする。「PIN」アクセス規則によって保護される。
公的個人認証サービス	否認防止の署名用証明書	否認防止用の証明書のみ。

294

署名・認証・暗号と社会との関係



セコム IS研究所　松本泰氏の資料より引用

署名(Signature) と認証(Authentication)

- 自然人による否認防止(Non Repudiation)の署名
  - 自分の意志で文書に対して内容を確認した上で署名　－自署名
- **透明性**がありかつ**効率的**な社会の構築のためには**電子署名**は非常に重要な意味を持つ
  - これには**変革**も伴う。しかし、**電子署名**がなされた**電子データ**は、これまでITの普及が困難だった業務を劇的に改善する可能性を秘めている。
- 電子認証(Authentication)を普段から利用しているセキュリティ技術者ほど、意外に「電子署名」への理解が難しいような気がする。

電子署名の基本

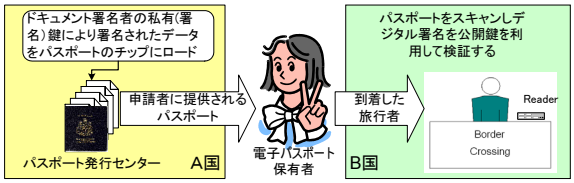
- ブラインド署名 (Blind signature)
- 電子透かし (electronic watermarking)
- リング署名 (Ring signature)
- グループ署名 (Group signature)
- 検証者指定署名 (Designated verifier signature)
- 否認不可署名 (Undeniable signature)

S/MIMEメール

- Secure MIME
  電子メールの暗号化と電子署名に関する国際規格。
- 暗号化:
  - 受信者の公開鍵で暗号化
  - 受信者の私有鍵で複合
- 署名:
  - 本文のダイジェスト(ハッシュ)を送信者の私有鍵で暗号化
  - 送信者の公開鍵で複合しダイジェストを確認

電子パスポート

- **電子署名**を施したパスポート
- 国際民間航空機関(ICAO)のNTWG (New Technology Working Group) PKIによるパスポートのデジタル署名の案
  - 機械可読な旅行文書(MRTD)のための**PKI電子署名**
    - **電子署名** -> **不正**を防ぐ　**署名の意味=内容の証明**
- 「不正を防ぐ=**Big Brother**」とならない情報公開、透明性が必要
  - 透明性の確保自体にも電子署名が重要



匿名証明書

- anonymous certificate
- 匿名性 (**Anonymity**)
- 自分の実名を隠して知らせないこと(広辞苑)
- 何らかの行動をとった人物が誰であるのかが分からない状態をさす。自分の実名・正体を明かさない事を目的とする。
  (ウィキペディア日本語版)
- 選挙・投票(日本国憲法第15条4項)
- ペンネーム(偽名、通称名)

セキュリティ運用

（基礎編第12回に相当）

301

インシデント対応のPDCA

（1）リスク分析
- 事業への寄与度や資産価値、再投資コストなどを評価
- インシデントがあったときの影響度を様々な角度から評価

（2）正常時対応
- 緊急時の連絡体制および連絡手順
- データのバックアップ手順
  - 頻度、バックアップするデータの内容、システムの二重化
- ログの取得内容の整理および取得方法

（3）インシデントの発見
- ログのチェック手順
  - チェックするログファイル、ログの読み方
- データの改ざんや破壊が行われていないかの確認手順
  - 署名による比較
  - 汚染されていないことが確実に保証されている同じシステムとの比較

302

インシデント対応のPDCA

（4）インシデントからの仮復旧
- 復旧作業の責任者
  - 個々の作業において「判断」を下すのはだれか？
- 作業記録の作成手順（記録すべき項目など）
  - インシデント発見のきっかけ、インシデントの原因
  - 具体的な作業内容
  - パッチの適用などの再発防止策の内容
- 復旧作業の手順
  - 事実の再確認、スナップショットの保存、
  - ネットワークの遮断もしくはシステムの停止
  - バックアップ機などによる運用の切り替え、
  - 影響範囲の特定
  - 復旧に掛かる時間などのコストの見積もり、
  - 復旧見込み時刻のアナウンス
  - インシデントに関係するサイトへの協力依頼、
  - インシデントの原因の特定
  - バックアップメディアからのデータの復旧
  - パッチの適用などの再発防止策の検討および実施

303

LOGの効果

- 事故が起こったときの原因調査と対策方法の手掛かり
- 正規の権限を持った人間の不正操作の防止と記録

失敗ログ…不正アクセス
成功ログ…内部犯行

- デジタルフォレンジクス（証拠保全）
  - きちんとしたLOGがあれば心証が良くなる

304

LOG解析（1）

日々の自動解析レポート（LogWatch）

```
vsftpd:
   Unknown Entries:
      check pass; user unknown: 1 Time(s)
      authentication failure; logname= uid=0 euid=0 tty= ruser= rhost=▒▒▒▒9.136 : 1 Time(s)

Unknown users:
   asec@jnsa.org
      from [▒▒▒▒▒190.186]    26 time(s).
   ctujq@jnsa.org
      from [▒▒▒▒▒190.186]    1 time(s).
   day@jnsa.org
      from [▒▒▒▒▒190.186]    12 time(s).

Unknown hosts:
   mail.xyz.xyz.: 2 Times(s)
   1x1y4u.net.: 1 Times(s)
   webvacancy.com.: 1 Times(s)
```

305

LOG解析（2）

日々の自動解析レポート（LogWatch）

```
sshd:
   Invalid Users:
      Unknown Account: 74 Time(s)
   Authentication Failures:
      sshd (▒▒▒▒.176.14 ): 1 Time(s)
      ftp (▒▒▒▒.176.14 ): 1 Time(s)
      unknown (▒▒▒▒.176.14 ): 72 Time(s)
      squid (▒▒▒▒176.14 ): 1 Time(s)
      unknown (▒▒▒▒65.233 ): 2 Time(s)

   Failed logins from these:
      adam/password from▒▒▒▒176.14: 1 Time(s)
      alex/password from▒▒▒▒176.14: 1 Time(s)
      alfred/password from▒▒▒▒176.14: 1 Time(s)
      ali/password from ▒▒▒▒176.14: 1 Time(s)
       ...
      webmaster/password from▒▒▒▒176.14: 1 Time(s)
      will/password from▒▒▒▒176.14: 1 Time(s)
      willie/password from▒▒▒▒176.14: 1 Time(s)
      win/password from▒▒▒▒176.14: 1 Time(s)
      work/password from▒▒▒▒176.14: 1 Time(s)
      www/password from ▒▒▒▒176.14: 1 Time(s)
```

306

サーバの運用・管理

サーバー管理のA to Z

- サーバーのシステム設計
- サーバーの初期設定
- サーバーの更新・修正
- サーバーの監視・IRT
- サーバーの監査
- サーバールームの管理

307

情報を手に入れる早道

【問題】

あなたは悪の組織に入っています。
某組織の秘密データを手に入れろとの指令が出ました。予算は1000万円です。あなたはどのような作戦を立てますか？

【回答】

某組織の秘密データを見ることができる人間を買収する。

308

権限のある人間の犯罪防止

業務以外での操作の監視

- 入退室記録（認証）
- 作業内容の記録
- 複数人での作業
- 業務ごとの権限管理
- 契約・業務規約
- モラル、リテラシーの涵養・教育
- 業務評価、報酬

309

サーバーを守る「要」

- 技術で守る
  - なんといっても基本
- 技術だけでは守れない
  - 正しい通信の中に潜む不正
  - 人間が判断するしかない
    （あなたと私は同じ判断をするか？）
- 技術の背景がないと解決できない
  - 精神論の運用管理手法では通用しない
  - どんなデータを守りたいのかが根本

310

インシデント対応のPDCA

（5）仮復旧後の対応

- ➢ インシデントに関係していると思われるサイトへの連絡
  - JPCERT/CCなどの公的機関への報告（届け出）手順
  - 運用ポリシーや手順の見直し

（6）完全復旧の段取り

- ➢ 応急処置等を行った場合の後処理
  - 建物、マシン、ネットワーク、ソフトウエア等々の定常運用化

311

デジタルフォレンジック

- forensic は、「法廷の」「鑑識」の意味
- 基本は、事故が起こった時の調査に使えるLOG情報を保存すること
- 事故があった時、LOG情報を解析し、証拠提出する

技術や運用管理、知恵で対応できなかった時の「最後の拠り所」

312

守りたいもの（目的）

企業など組織体 ⇒ 情報資産の保護

国家・社会 ⇒ 重要インフラの保護

■ 情報セキュリティの3つの要素 ■

・機密性（Confidentiality）
- 情報および処理方法が正確で完全であること

・完全性（Integrity）
- 権限を持ち許可されたものだけがアクセスできること

・可用性（Availability）
- 許可された者が必要な時に確実にアクセスできること

313

最後の砦の保険

お金で解決できることは保険で対応できる
- サイバーアタック保障保険
- 個人情報漏えい保障保険
- ネットワーク総合保険
- e-リスク保険
- eBANKセキュリティ保険
- 等々その他多数

診断や監査などと組み合わせてソリューションとして提供されることも多い

314

JNSA調査報告書

「2005年度 情報セキュリティインシデントに関する調査報告書」

http://www.jnsa.org/result/2005/20060803_pol01/

JNSA セキュリティ被害調査ワーキンググループ

情報漏えいによる被害想定と考察
（賠償額および株価影響額）

315

個人情報漏洩事件数（公開情報）

調査対象事業者数（1月1日～12月31日に公開された情報からリストアップ）

2005年度	2004年度	2003年度	2002年度
1032件	366件	57件	62件

被害者数

2005年度	2004年度	2003年度	2002年度
8,814,568人	10,435,061人	1,554,592人	418,716人

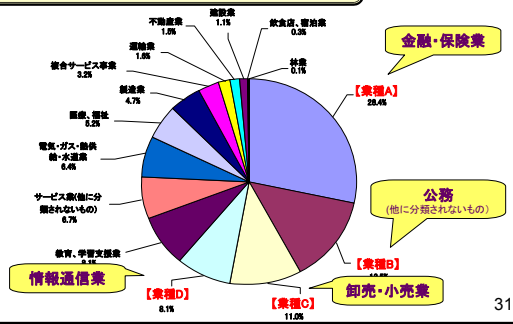
1 件当たりの平均被害者数（※但し、被害者数が不明な事件を除く988件を母数とする）

2005年度	2004年度	2003年度	2002年度
8,922人	31,057人	30,482人	7,613人

316

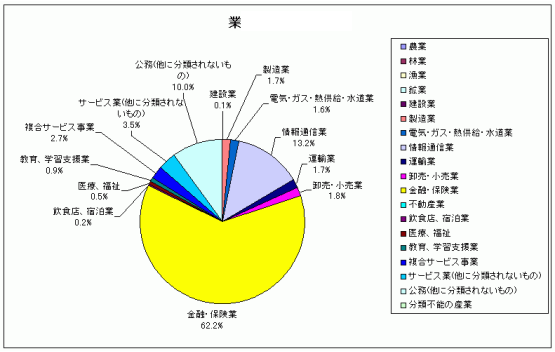
2005年 個人情報漏洩事件数の業種別分類

Q:【業種A～D】には、以下の業種のどれが当てはまるでしょうか？
・金融・保険業　・卸売・小売業
・情報通信業　・公務(他に分類されないもの)



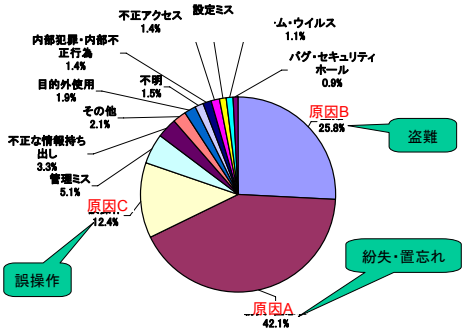
317

2005年 業種別被害者数



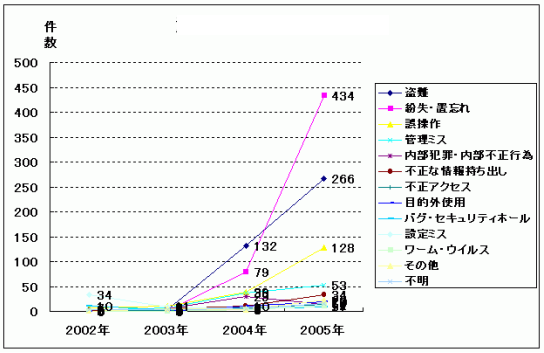
318

2005年 漏洩原因(件数)



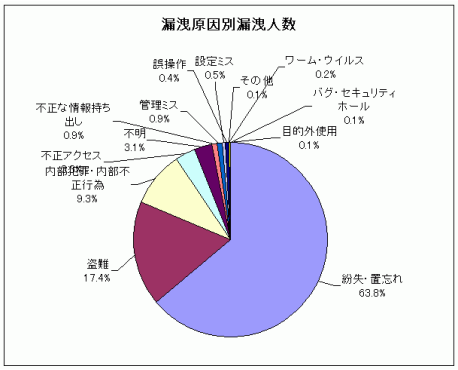
319

情報漏洩原因の経年変化



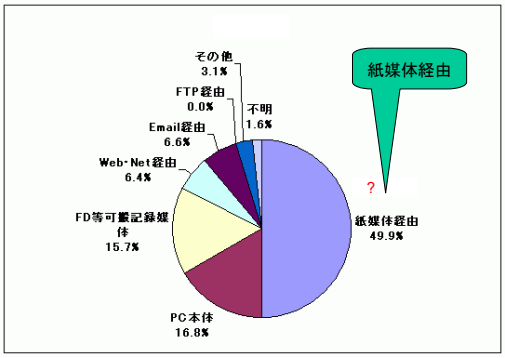
320

2005年 漏洩原因別漏洩人数



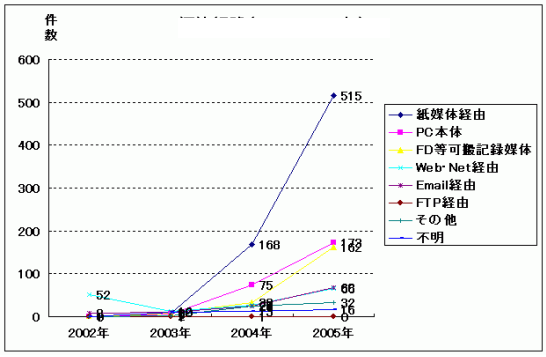
321

2005年 情報漏洩経路



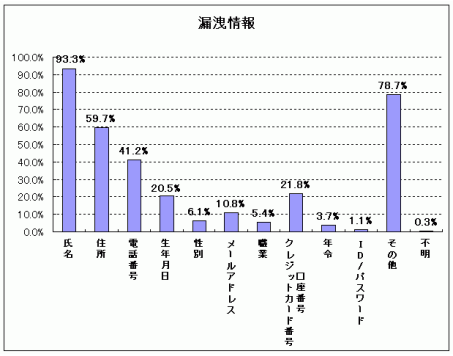
322

情報経路の経年変化



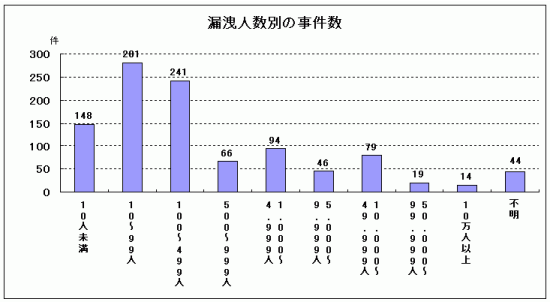
323

2005年漏洩情報の項目



324

2005年漏洩人数別事件数



325

内閣府国民生活審議会

「平成17年度 個人情報の保護に関する法律施行状況の概要」（平成18年6月）
http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20060630kojin6.pdf
から引用

個人情報の保護に関する法律（平成15年法律第57号）第53条第1項の規定に基づき、内閣総理大臣は、関係する行政機関の長に対し、この法律の施行の状況について報告を求めることができることとされています。
また、同条第2項の規定に基づき、内閣総理大臣は、毎年度、同条第1項の報告を取りまとめ、その概要を公表することとされています。
今回、平成17年度における施行状況の報告について取りまとめましたので、その概要を公表します。

326

漏洩人数の増加

表８　漏えいした人数（平成 17 年度）

漏えいした人数	17 年度	
	件数	割合
500 人　以下	1, 114	71. 6%
501　～　5, 000 人	220	14. 1%
5, 001　～　50, 000 人	167	10. 7%
50, 001 人　以上	37	2. 4%
不明	18	1. 2%
合計	1, 556	100. 0%

（注）「割合」は、漏えい事案全体（1, 556 件）に対する割合。

327

漏洩情報の種類

表９　漏えいした情報の種類（平成 17 年度）

漏えいした情報の種類	件数		うち基本情報のみ	
顧客情報	1, 531	(98. 4%)	112	(7. 2%)
従業員情報	51	(3. 3%)	3	(0. 2%)
その他の情報	22	(1. 4%)	1	(0. 1%)
合計（重複分除く）	1, 556	(100. 0%)	112	(7. 2%)

（注）１．（ ）内は、漏えい事案全体（1, 556 件）に対する割合。
２．表中の「うち基本情報のみ」は、基本情報のみ漏えいした事案の件数（内数）及び漏えい事案全体（1, 556 件）に対する割合。

328

暗号化保護の有無

表１０　暗号化等の情報保護措置（平成 17 年度）

情報保護措置の有無	件数	
措置有	105	(11. 8%)
うち一部のみ措置有	17	(1. 9%)
措置無	459	(51. 7%)
不明	323	(36. 4%)
合計（重複分除く）	887	(100. 0%)

（注）１．（ ）内は、漏えい事案全体（887 件）に対する割合。（一部の省庁は平成 17 年度下半期分のみ集計しているため、全体の件数は、他の項目のものと異なる。）
２．暗号化等の情報保護措置とは、情報の暗号化や紛失したパソコンへのパスワードによるアクセス制限等、情報保護のために講じられた措置をいう。

329

漏洩元と漏洩した者

表１１　漏えい元・漏えいした者（平成 17 年度）

漏えいした者 / 漏えい元		不明	第三者 意図的	第三者 不明	第三者 計	その他	不明	合計
事業者		24 (1. 5%)	182 (11. 7%)	29 (1. 9%)	211 (13. 6%)	8 (0. 5%)	29 (1. 9%)	1, 186 (76. 2%)
委託先		7 (0. 4%)	53 (3. 4%)	4 (0. 3%)	57 (3. 7%)	1 (0. 1%)	13 (0. 8%)	358 (23. 0%)
不明		－	－	－	－	－	－	12 (0. 8%)
合計		31 (2. 0%)	235 (15. 1%)	33 (2. 1%)	268 (17. 2%)	9 (0. 6%)	42 (2. 7%)	1, 556 (100. 0%)

（注）（ ）内は、漏えい事案全体（1, 556 件）に対する割合。

330

漏洩後の改善処置

表１２　漏えい後の改善措置状況（平成 17 年度）

期間	合計	事業			その他の対応	改善措置実施せず	不明
17 年度	1,556 (100.0%)	1,553 (99.8%)	1,501 (96.5%)		1,497 (96.2%)	2 (0.1%)	1 (0.1%)

（注）１．表中の「組織的」安全管理対策とは、安全管理責任者の設置、社内規定の整備、教育・研修の実施、監査の実施等を指す。
「技術的」安全管理対策とは、ファイアウォールの構築、情報漏えい防止ソフトウェアの導入、個人データへのアクセス状況の監視等を指す。
「その他の対応」とは、詫び状の送付、専用窓口の設置、カードの差し替え等を指す。
２．「安全管理対策」と「その他の対応」は複数回答。
３．（）内は、漏えい事案全体（1,556 件）に対する割合。

331

情報資産のリスク評価試算モデル

NPO日本ネットワークセキュリティ協会(JNSA)
技術部会　セキュリティ被害調査WG

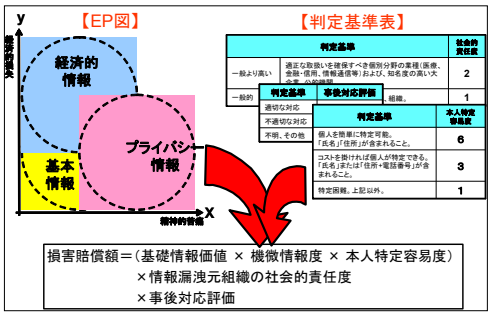
「2005年度情報セキュリティインシデントに関する調査報告」
http://www.jnsa.org/result/2005/20060803_pol01/

本報告書は、2005年1年間に公表された国内の個人情報漏えい事件・事故（以降 便宜上 個人情報漏えい事件と表記する）の調査分析結果をまとめたものである。
なお、2005年度中の大きな漏えい事件であるカードシステムソリューションズ社の事例は、米国での事例という理由から、それに起因するインシデントについては集計から除いたことをご承知いただきたい。

332

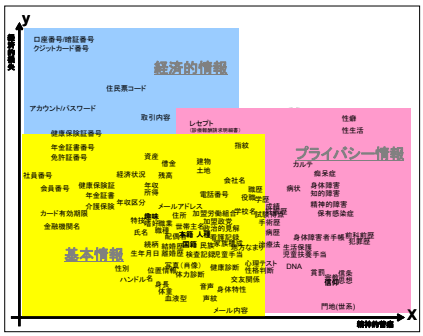
情報資産のリスク評価試算モデル

2003年「プライバシー面」「経済面」の2要素で、事故が起こり訴訟が行われた場合の損害賠償額を試算するモデルを試行



333

情報の価値基準の検討 (Entity Processing図)

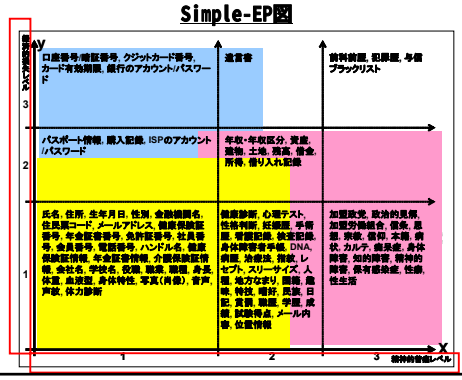


個人情報の配置例（EP図）

334

情報の価値基準の検討 (Entity Processing図)

Simple-EP図



335

個人情報価値評価のモデル式

損害賠償額 ＝ 漏洩個人情報価値
×社会的責任度
×事後対応評価

＝（基礎情報価値×機微情報度×本人特定容易度）
×情報漏洩元組織の社会的責任度
×事後対応評価

＝ 基礎情報価値　[500]
×機微情報度　[Max（$10^{x-1}+5^{y-1}$）]
×本人特定容易度 [6, 3, 1]
×社会的責任度　[2, 1]
×事後対応評価　[2, 1]

機微情報度＝（$10^{x-1}+5^{y-1}$）
x＝漏洩した情報の精神的苦痛レベルの最大値
y＝〃　経済的損失レベルの最大値

判定基準	本人特定容易度
個人を簡単に特定可能。「氏名」「住所」が含まれること。	6
コストを掛ければ個人が特定できる。「氏名」または「住所+電話番号」が含まれること。	3
特定困難。上記以外。	1

判定基準	社会的責任度
一般より高い	適正な取扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信等）および、知名度の高い大企業、公的機関。	2
一般的	その他一般的な企業および団体、組織。	1

判定基準	事後対応評価
適切な対応	1
不適切な対応	2
不明、その他	1

336

宇治市の例

損害賠償額＝ 基礎情報価値[500]
× 機微情報度[Max（10^0+5^0）=2]
× 本人特定容易度[6]
× 社会的責任度[2]
× 事後対応評価[1]
＝ 12,000円

実際は慰謝料10,000円＋訴訟費用5,000円

217,617件×15,000円＝約32.6億円
（原告は3人）

337

YahooBBの例

損害賠償額＝ 基礎情報価値[500]
× 機微情報度[Max（10^0+5^0）=2]
× 本人特定容易度[6]
× 社会的責任度[2]
× 事後対応評価[1]
＝ 12,000円

実際は慰謝料5,000円＋訴訟費用1,000円

社会的責任度を情状酌量して[1]とすれば損害賠償額は6,000円となり、実際の判決と合う。

約450万件×6,000円＝約270億円
（原告は5人）

338

インシデント被害額算出モデル

＝表面化被害＋潜在化被害
＝直接被害＋間接被害＋潜在化被害
＝逸失利益（直接的な被害）
＋復旧に要したコスト（ハードウエア、ソフトウエア、工数）
＋営業継続費用＋喪失情報資産＋機会損失
＋補償、補填、損害賠償など(間接的な被害)
＋（固定費（人件費）×インシデントによる影響を受けた人数
×IT 感応度（業務依存度）×停止時間）
＋業務外の潜在化被害(風評被害など)

339

関連法規と規格

（基礎編第13回に相当）

340

個人情報保護法の課題

- **個人情報保護法の「そもそも」の目的は？**
  - 自分の情報は自分でコントロールできる。
  - アンケートや検証募集で事業者としては対価を払って手に入れた個人情報も、預かっているに過ぎない。自由に使えるわけではない。

個人情報保護法は、だれもが安心してIT社会の便益を享受するための制度的基盤として、平成15年5月に成立し、公布され、17年4月に全面施行されました。
この法律は、個人情報の有用性に配慮しながら、個人の権利利益を保護することを目的として、民間事業者の皆様が、個人情報を取り扱う上でのルールを定めています。

内閣府「個人情報の保護」 http://www5.cao.go.jp/seikatsu/kojin/

341

個人情報保護法の課題

- 内閣府もパブリックコメントを出した
  - 国民生活審議会個人情報保護部会「個人情報保護に関する主な検討課題」に関する意見募集について
  - http://search.e-gov.go.jp/servlet/Public?CLASSNAME=Pcm1010&BID=095060570&OBJCD=100095&GROUP=

342

「過剰反応」の背景及び対応

(2)いわゆる「過剰反応」について

- 個人情報の第三者への提供に当たって、法律上、本人の同意を得る必要がないにもかかわらず、法律を誤解し、提供を控えるような場合については、内閣府の解釈や運用基準を明確化し、また、関係省庁は分野ごとのガイドラインやその解説等の必要に応じた見直し等を行うとともに、その周知徹底を図る必要がある。
- 自治会や同窓会の名簿等について、プライバシー意識の高まり等を背景に、本人が掲載を拒否するケースが見られる。また、このような名簿については、本人の同意を得ること又はオプトアウトの仕組みを活用することにより名簿の作成・配布ができるが、このような手続きが負担に感じられること等から名簿の作成を取りやめる場合がある。個人情報を利用するかしないかは当事者の意思に委ねられているが、こうした問題をどのように考えるか。
- 法律の有無にかかわらず、個人情報保護意識の高まりによって起きている問題もあるのではないか。

なお、自治会名簿の作成が中止される等の背景には、個人情報保護法とは別に住民が地域活動と距離を置きたい等の事情も考えられる。個人情報保護法が、そのような活動から距離を置くことの口実になっている側面もある。一方、地域によっては防災、防犯、地域福祉等の分野で、地域活動への理解を深めている場合もある。個人情報保護法との関連性を論じる場合は、個々のケースを慎重に検討する必要があるのではないか。

343

全体まとめ

（基礎編第14回に相当）

344

グーグル革命

- 全てはGoogle等の検索エンジンから…
- 巨大ビジネスに育っている
  - 検索結果の上位15位に入らなければ会社は存続できない
- 生活のあらゆる部分に入り込んでいる
  - 買い物、恋人探し、仕事、等々
- 社会との関係が興味深い
  - 「検索」の効力はどこまで及ぶのか？
  - 国際的なグローバルスタンダードができるのか？
  - セキュリティ問題

345

検索エンジンの威力

- TBCの漏洩原因となった
- Webサーバーに置かれているファイルの一覧表示を許しているサイトが探せる。
- しかもCGI出力のCSVファイルがHTMLファイルを置く場所に置いたりすると…
- 更に誰でも読めるパーミッションになっていると…

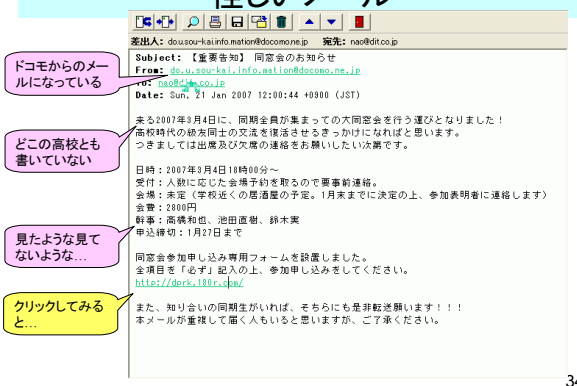
346

問題点は何？

- Webサーバで不用意にIndexのリストをさせるのは危険
- CGI等の書込みファイルを、htmlファイルと同じ場所においてはいけない
- 書込みファイルのパーミッション設定は細心の注意で行う

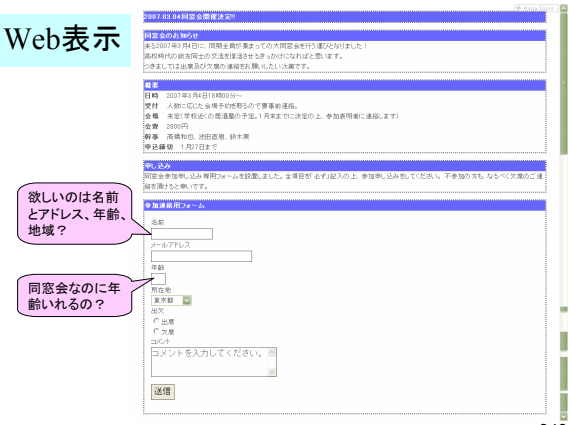
347

怪しいメール



348

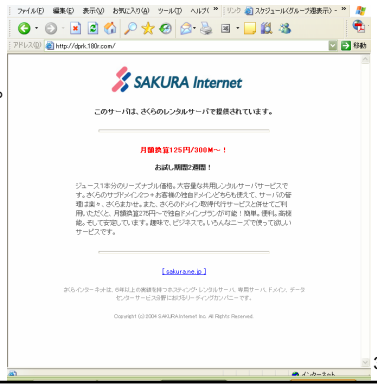
Web表示



349

数日後…

CGIファイルが
消されていました。



350

ヘッダ情報を確認

- 発信者のFrom:アドレスのドメインがReceivedと合っていない

⇒リレー(3rd Party Relay)か詐称されている可能性が高い

⇒発信されているホスト名が怪しさいっぱい…

中国のプロバイダらしい

Received: from [redacted]) by xxx.yyy.co.jp (8.12.11/3.7W-0607251930) with ESMTP id l0L30nl8000850 for <nao@yyyco.jp>; Sun, 21 Jan 2007 12:00:50 +0900 (JST)

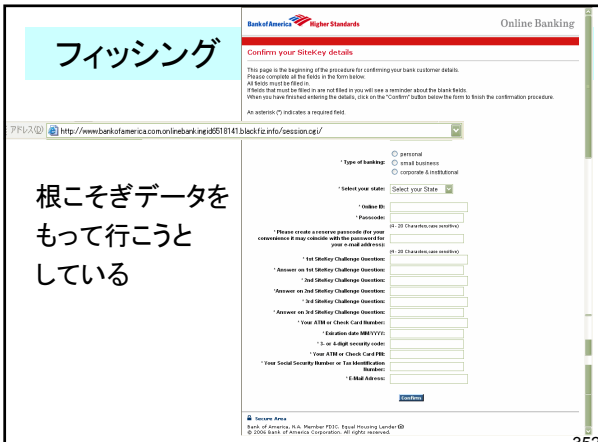
Subject:【重要告知】同窓会のお知らせ

From: [redacted]

351

フィッシング

根こそぎデータを
もって行こうと
している



352

メールヘッダの見方

Delivered-To: nnnnnnn@gmail.com
Received: by 10.78.25.19 with SMTP id 19cs149902huy; Sun, 7 Jan 2007 00:52:12 -0800 (PST)
Received: by 10.67.91.6 with SMTP id t6mr16623572ugl.1168159932334;
Sun, 07 Jan 2007 00:52:12 -0800 (PST) Return-Path: <XXX
Received: from ares.XXX.co.jp (ares.XXX.co.jp [000.166.249.2]) by mx.
id x33si31622552ugc.2007.01.07.00.52.10; Sun, 07 Jan 200
Received-SPF: pass (google.com: best guess record for domain of XX
designates 000.166.249.2 as permitted sender)
Received: from venus.XXX.co.jp ([000.16.32.19]) by [redacted]XXX.co.jp (8.12.11/3.7W-0607251930) with ESMTP
id l078q9Da001420 for <nnnnnnn@gmail.com>; Sun, 7 Jan 2007 17:52:09 +0900 (JST)
Received: from venus.XXX.co.jp (localhost [127.0.0.1]) by localhost.XXX.co.jp (Postfix) with ESMTP
id 466DEBB36 for <nnnnnnn@gmail.com>; Sun, 7 Jan 2007 17:52:04 +0900 (JST)
Received: from [redacted] (aratin.XXX.co.jp [000.16.64.6]) by venus.XXX.co.jp (Postfix) with SMTP
id 1348BBB33 for <nnnnnnn@gmail.com>; Sun, 7 Jan 2007 17:52:04 +0900 (JST)
Message-Id: <200701070851.AA06077@sarah.jnsa.
Date: Sun, 07 Jan 2007 17:51:42 +0900
To: nnnnnnn@gmail.com
From: XXX@cyber-u.ac.jp
Subject: =?ISO-2022-JP?B?GyRCQC4kaiQ5JF4
MIME-Version: 1.0
X-Mailer: AL-Mail32 Version 1.13
Content-Type: text/plain; charset=iso-2022-jp

成りすましメールです。代理投稿とも言います。
直接使っているメールサーバは、XXX@XXX.
From: には、XXX@cyber-u.ac.jp としています。

---やすだ

メーラが自由に設定できる場合が多いので、当てにならない。

From: は、"cyber-u.ac.jp" となっているが、最後の Received: の fromは "XXX.co.jp" となっているので、3rd Partyを許しているメールサーバあるいはSMTPで直接任意のFrom:アドレスで発信された「成りすましメール」の可能性が高い。

353

PWの作り方

- 忘れるのならメモしなさい！
  - 最近のWebサービスなどを考えると、メモしない使い方は人間業ではない…
- メモとパソコンは別々に！
  - 銀行の通帳と印鑑は別々に保管
- 長い文字列にする
  - 許される最大長を有効に活用
- 辞書にあるような文字列は避ける
  - アイドル名などは危ない…

354

情報の扱い方

- 個人情報は誰のもの？
- 誰が情報を見たかを本人が調べられる（エストニア）

【前提】
- 紙の時代
  - 役所は不正をしないことが拠り所
- 電子の時代
  - 役所でも不正は起こる

355

セキュリティの標語

- 技術的に出来ることと、やったほうが良いことは、別の場合が多い。
- やり過ぎ、過剰反応は、何にしても後ろ向きな反応を呼ぶ。
- 危ない！という説得理由は、リフォーム詐欺と同類になりやすい。

356

ソーシャルエンジニアリング

- 手段は本当に千差万別
- 人間の知恵の多彩さに感心する
- エレベータから情報漏洩
  - 機密情報について会話してませんか？
- 会社近くの呑み屋さんや喫茶店
  - 結構メーター上がって大声でお話ししてますね
- IT技術以前の問題です
  - 人間の特徴を逆手に取られると簡単です

357

ヒヤリ・ハット

- 事故が起きる寸前、または起きてもおかしくない状態で済んだ経験のこと
- 失敗は非難・隠蔽するものではなく、そこから学ぶために活用すべきもの
- 「ヒヤリ・ハット」の報告は褒めるのが原則。セキュリティ関係は責められることが多いのは問題

358

ルールの作り方

～してはいけない　×

～しなさい　○

情報セキュリティの目的
- 安全・安心・快適に使える
- 決められた操作のみが許可される

本人の協力がなければ成立しない

359

まとめ

- 情報セキュリティの守備範囲は広い
  - ネットワーク環境設計・構築
  - サービス環境・マシンの設計・設定
  - 業務アプリケーションの設計・開発
  - 運用・管理・保守・オペレーション
  - トラブルシューティング
  - 法制度、法律問題の準備・チェック・対応
  - それぞれが正しく機能しているかの監査
  - サーバルームの入退室管理、作業管理
  - 権限許可、監視、記録管理
  - 企業経営、事業継続、インシデント対策
  - 等々
- すべて一人ではできない
  - 全体を見通した総合技術が安全を確保する

360

付録３　参考 URL

講義で使用するもの、講師が参照するもの、学生が学習用に参照するもの、全てに有益なインターネット上の Web サイトを以下に紹介する。

① IPA(情報処理推進機構セキュリティセンター)

http://www.ipa.go.jp/security/index.html

情報セキュリティに関係する情報を幅広く提供。利用者にとって最も重要なウイルス情報も豊富に掲載。

② JPCERT/CC（Japan Computer Emergency Response Team / Coordination Center）

http://www.jpcert.or.jp/

JPCERT は、インターネット上で発生しているインシデント（事件）の収集と情報提供を行っている。影響度の高いウイルス発生等をタイムリーに報告してくれるため、アラート代わりにメーリングリストへの登録をしておくと便利。

③ 警察庁セキュリティポータルサイト@Police

http://www.cyberpolice.go.jp/

情報セキュリティ初心者から、技術者まで幅広い種類の情報が入手可能。

ただし比較的利用者向けの内容となっているため、技術的には初級レベルのものが多い。

④ インターネット定点観測(@Police)

http://www.cyberpolice.go.jp/detect/observation.html

警察庁の@Police 内のコンテンツで、インターネット上に配置されている侵入検知システム（IDS)のサマリをグラフで報告している。攻撃手法の流行や傾向が分かる。

⑤ マイクロソフト TechNet セキュリティセンター

http://www.microsoft.com/japan/technet/security/default.mspx

マイクロソフト製品の関係するツール、情報を入手できる管理者向けサイト。

重要度の高い情報がアップされた場合、メールでのアナウンスが行われるためメーリングリストを活用した方が便利。

⑥ 日本 DNS オペレータグループ

http://dnsops.jp/index.html

2006 年に KDDI の石田氏を中心に設立。DNS の運用に関する話題を提供している。比較的 DNS の安全性というより安定性に関する議論が多い。メーリングリストによる情報提供も行っている。

http://dnsops.jp/ml.html

⑦ セキュリティホール memo

http://www.st.ryukoku.ac.jp/~kjm/security/memo/

情報セキュリティのみならず、時事等の話題も含めた情報が掲載されている。散らばっているセキュリティ関連の情報を手早く確認することができる。

⑧セキュリティホール memo-定番情報源

http://www.st.ryukoku.ac.jp/%7Ekjm/security/memo/teiban.html

上記サイトの開設者である、龍谷大学小島氏のリンク集。

⑨ セキュリティのポータルサイト

http://www.packetstormsecurity.org/

セキュリティの総合サイト。最新の情報から OS、パケット解析、暗号などの話題が豊富。

⑩ フットプリントで使用されるサイト

（DNS）http://www.dusstuff.com/

（Web）http://uptime.netcraft.com/

（GoogleHack）http://johnny.ihackstuff.com/

⑪ 電子メール（第三者不正中継など）

（第三者中継のチェックツールの提供）http://www.rbl.jp/svcheck.php

（不正中継ホストのデータベース）http://www.ordb.org

（スパムメールのヘッダ解析などの話題が豊富）http://www.gabacho-net.jp/anti-spam/

⑫ その他メーリングリストなど

JPCERT/CC メーリングリスト

http://www.jpcert.or.jp/announce.html

マイクロソフト プロダクト セキュリティ 警告サービス

http://www.microsoft.com/japan/technet/security/bulletin/notify.asp

この冊子は、経済産業省が実施した平成 18 年度コンピュータセキュリティ早期警戒体制の整備事業（インターネット安全教室及び情報セキュリティ人材育成に関する調査等）による委託調査の一環として、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）が行った活動の成果をとりまとめたものである。

公開 URL：　http://www.jnsa.org/

情報セキュリティ教育の指導者向け手引書（2007 年版）

2007 年 10 月　初版公開

特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）

お問合せ先（JNSA 事務局）
〒136-0075 東京都江東区新砂 1-6-35 NOF 東陽町ビル 1 階
TEL：03-5633-6061 FAX：03-5633-6062
E-Mail：sec@jnsa.org