■3 群（コンピュータネットワーク）- 7 編（コンピュータネットワークセキュリティ）

1 章 コンピュータネットワークセキュリティの動向

（執筆者：安田なお）［2009 年 1 月 受領］

■概要■

本編では，情報セキュリティを考えるうえで，技術的な対応方法や考え方について説明している．第 2 章ではアクセス制御について述べている．強制アクセス制御のメカニズムについても述べられ，セキュア OS のモデルについても詳述している．第 3 章では不正侵入の手法について述べられ，クロスサイトスクリプティングや，インジェクション系の仕掛けについて詳述される．第 4 章はマルウェアについて述べられ，マルウェアの概要や動作の特徴，更に対策についても詳述されている．第 5 章は不正侵入検知について述べられ，IDS システムの基本構成や機能，関連技術との関係などを詳述している．第 6 章はセキュリティプロトコルについて述べられ，インターネットの伝送路上で実現される通信プロトコルについて詳述している．第 7 章はセキュリティシステムの構築と運用について述べられ，システム構築やセキュリティコンポーネントの設定，運用時の考慮点，更に脅威への対応についても詳述している．最後の第 8 章は，セキュリティマネジメントについて述べられ，基本的な概念やポリシー, ISMS や PDCA といった情報セキュリティを向上させるための手法，リスク分析，セキュリティ監査，認証制度などについて詳述している．

【本章の構成】

技術は，基本的な基盤を提供し，実際に動く環境を用意するが，システムは人間の考えたものなので見逃している部分も必ず存在する．このため後になってシステムの問題が発覚することがある．開発する側も利用する側も，このような背景を理解し，より良いシステムを開発し，より上手に利用することが重要である．しかし，より安全で安心なシステムは開発側でしか創ることができない．善悪の二元論だけではなく，多様な条件や環境での情報セキュリティを考えて行ければと思う．

技術的な内容を補足する専門家向けの入門書としては 3)がある．また，技術者教育についての報告書 5), 6), 7), 8)には，カリキュラムや教育方法，教材サンプルなどについての情報が含まれているので，参考にしていただきたい．

■3 群 － 7 編 － 1 章

1-1 情報セキュリティの位置づけ

（執筆者：安田なお）［2009 年 1 月 受領］

コンピュータやネットワークをターゲットとした事件や事故が注目されるようになってきている．「情報セキュリティ」の重要性がいわれるが，表面的な現象や攻撃方法は確かに新しく，日進月歩であり，巧妙になってきているが，その目的や結果については，人類の歴史をそのまま引き継いでいるともいえるだろう．つまり，情報技術（IT）は，それまでになかったまったく新しい面もあるものの，人間社会への影響という面で考えると，いにしえからの性（さが）が引き継がれている．ネットワークやコンピュータに関する問題点だけではなく，ネットワークやコンピュータを道具として利用した詐欺や誹謗中傷などの問題が注目されている．技術的な詳細については本編で記述するが，この章では技術の位置づけだけではなく，鳥瞰的な観点から見た情報セキュリティの位置づけについても若干触れておきたい．

Oxford English Dictionary によると，Secure という言葉はラテン語の securus が語源で，心配という意味の cura と「～がない」という意味の se- からなっている．心配や危険がない状態ということである．したがって，情報セキュリティ（Information Security）は，情報や情報システムの安全性を意味する．情報セキュリティの重要な三要素として，機密性（Confidentiality），完全性（Integrity），可用性（Availability）がいわれる．機密性は情報の秘密を守ることであり，機密情報やプライベート情報を権限のないアクセスから保護することである．完全性は情報の偽造や改ざんや破壊を防止することであり，情報を正しい状態に保つことである．可用性は情報を必要なときに必要な人が利用できるようにすることである．機密性，完全性，可用性の頭文字を取って「CIA」と呼ぶが，最近は機密性という情報漏えいや情報盗難だけではなく，情報が必要なとき直ちに利用できる可用性の重要性が認識されてきており，「AIC」の順で呼ぶ方が良いという意見も出ている．情報は使われてこそ活きてくる，ということだが，情報セキュリティは，情報を秘密にしておくだけではなく，正しい情報が安全に利用できなければ意味がない．そのために，技術が果たす役割は大きい．

情報セキュリティは，独立した技術分野として存在するのではなく，**図 1･1** のように IT 分野の個々の分野や技術要素のそれぞれにセキュリティに関する項目が棘のように存在している．IT を安全に利用するために必要な要素の一つとしてセキュリティ要件が存在し，そのセキュリティ要件だけで独立した分野があるというより，技術要素や管理項目，運用手順などの個々にセキュリティ要件がかかわってくると考えた方が自然だろう．したがって，システムを作成するに当たって，要件定義，外部仕様，内部仕様，詳細設計，コーディング等々の各ステージで，それぞれのセキュリティ対応が存在することになる．

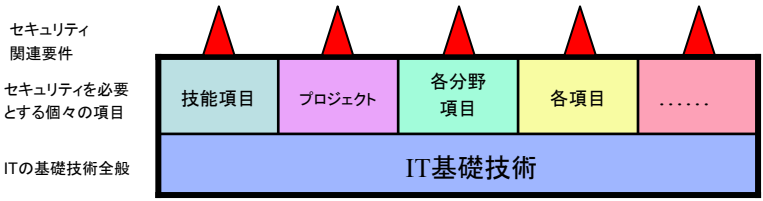

図 1・1　情報セキュリティと IT との関係

情報セキュリティは，コンピュータやネットワーク，通信機器など，更に管理者や利用者，攻撃者などの人間系を含めた広い概念で使われることが多い．必ずしもインターネットに接続されている場合だけではなく，スタンドアローンで動作しているシステムも対象になる．インターネットにつながれていなければ，確かに外部からのネットワークを経由した攻撃はないかもしれないが，可搬型デバイスにより予期しないプログラムやデータが持ち込まれる場合や，データ自身の不整合などによりシステム停止が起これば，可用性が損なわれる．セキュリティは，システムが正しく動作することが目的であると考えられる．ただし，注目する対象に分けて，コンピュータセキュリティや，ネットワークセキュリティ，インターネットセキュリティなどといわれる場合がある．コンピュータに関する安全性や，ネットワークやインターネットに関する安全性といった，コンポーネントを限定して使われる場合であるが，各分野での対応・対策を効果的に結合することが重要である．情報セキュリティとして最終的に実現するべき目的は，コンピュータやネットワークなどで構成される情報システムやそこに存在する情報そのものの安全性であり，不用意に停止しないことである．

■3 群 － 7 編 － 1 章

1-2 脅威の性質

（執筆者：安田なお）［2009 年 1 月 受領］

情報システムに対して脅威を与えるのは人間である．コンピュータが自発的に脅威を与えることはまだない．人間が直接操作するか，コンピュータにプログラムとして指令を与えて脅威をつくり出す．脅威の背景には必ず人間がいることは重要である．技術だけでは解決できない大きな理由となっている．しかし，対策を考えるとき，技術の裏づけのある対策を考えないと，自動的なセキュリティ対策を実現することが難しくなり，人間が常に張り付いた運用管理体制をとらざるを得ず，IT を使って効率化，自動化する目的と相反してしまう．

人間が背景にいるとしても，いろいろな「思い」でシステムに割り込んでくる．いくつかの例をあげてみよう．(1) 自己顕示欲や愉快犯，(2) 怨恨など，(3) 詐欺，(4) 産業スパイ，(5) テロリストなどがあげられる．このほかに人間が介在するものとして (6) 設定ミスなどの事故が考えられる．情報セキュリティに関する事件・事故では，外部から見て，システムが停止する場合と，情報が漏えいする場合が大きな脅威となる．システムが停止する場合は，外部からの攻撃と，システム内部の問題から発生するものがある．外部からの攻撃の代表例は，ネットワークに対する DoS 攻撃（Denial of Service attack：サービス不能攻撃）系があるが，これは一方的にサーバの入り口に殺到して通行不能にしてしまうようなもので，現在のインターネットのプロトコルを前提にすると，防御することはなかなか難しいといえる．一方，システム内部の問題は，システム停止に至る問題をつくり込んでしまっていたという，開発側の不備という原因が存在する．近年の話題をいくつか拾ってみても，証券取引所のシステム停止，鉄道会社の改札システムの停止や運行システムの停止，航空会社のカウンター端末の停止，火星探索機のランディングの失敗等々，たくさんの事例が報道されている．これらは必ずしもインターネットを利用しているわけではないが，情報セキュリティはインターネットを使っているものだけではないのは前記したとおりである．システムが安全に安定して動作することを実現することが「情報セキュリティ」である．これらの事件・事故の原因を探ってみると，ディジタル証明書の期限切れや，通信バッファのプログラムミス，処理能力を超えた場合の処理，データの単位系の食い違い等々，可用性を考えるときの基礎的な問題があったといえる．このような例から見ても情報セキュリティはインターネットに接続されているものだけが対象なのではないといえる．

もう一つの情報漏えいの事例を考えると，悪意をもって実行した犯罪なのか，故意ではなく不測の事故なのか，外部からの侵入によるものなのか，内部の権限のある人間が手引きをしたものかなどが考えられる．実際の情報漏えいの原因を見てみる．JNSA の 2008 年上半期の調査報告書 1), 5)によると，**図 1･2** のように上位四つが「誤操作」「紛失・置忘れ」「盗難」「管理ミス」となっている．この比率や順位は年度によって若干異なるが，この 4 項目は常に上位を占めている．誤操作，管理ミスといった不注意や知識不足と思われる原因と，紛失・置忘れ，盗難といった物理的な「物」がなくなるといった原因がほぼ同数ずつ発生している．これを見ると，実際の情報漏えいは，不正アクセスというよりは，ごく日常的な原因で起こっていることが分かる．

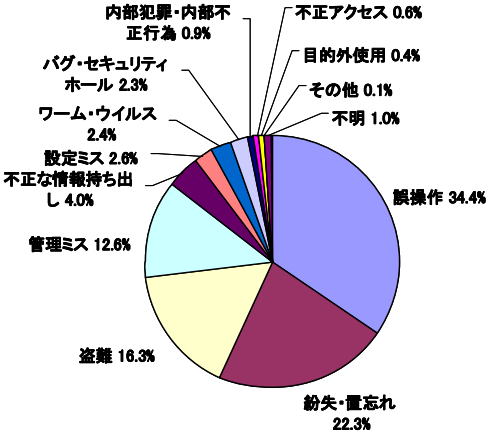

図 1・2　JNSA 調査：情報漏えいの原因（2008 年上半期）

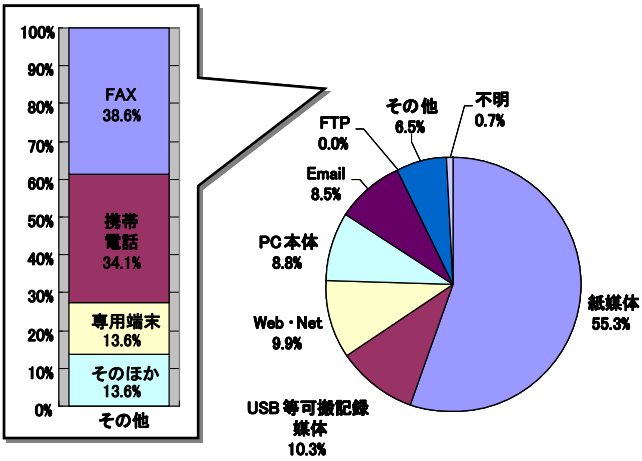

図 1・3　JNSA 調査：情報漏えいの経路

情報漏えいの経路という面から見ると，**図 1･3** のように紙媒体が 50%以上であり，この数年 50%前後ということで大きな変化がない．最大の漏えい経路は印刷物などが多数を占めているが，分類項目を変えて集計した結果を見ると，FAX が多数を占めており，紙媒体の大多数は FAX によるものであることが予想される．これは，主に金融機関などが FAX の誤送信などもすべて報告するように指導されていることとも関係があるだろう．いずれにしても，実際の情報漏えいの事件件数から見ると，決して新しくない手順や原因が多数を占めていることになる．

内部手引きがあると漏えい人数が多大になることは統計からも推測できる．**図 1･4** を見ると，1 件あたりの漏えい人数が多いグループ（業種）と漏えい人数が少ないグループがある．

複合サービス事業と製造業では，事故件数はさほどではないが，漏えい人数が飛び抜けている．一方，公務と教育・学習支援業は，情報漏えいの件数に対して漏えい人数が少ないという傾向がある．大規模な漏えいは内部者の関与があったと見られる．事件件数は少ないが，ひとたび事件が起こると大規模な情報漏えいとなる特徴がある．このような大規模な事件を防止できれば，情報漏えいの人数を低く抑えることができるだろう．規模が小さい例では，印刷されている住民票などの公的書類やクラスの成績など，紙での資料などが多いので，あまり大規模な漏えいにはなっていない．

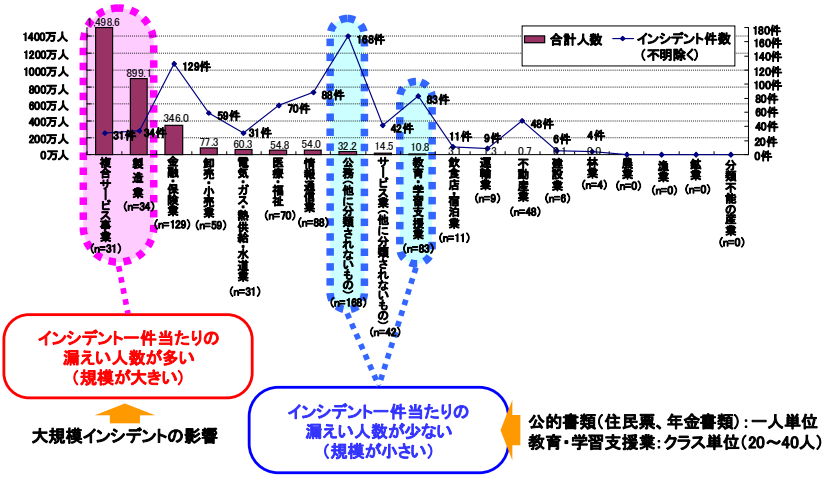

図 1・4　JNSA 調査：業種別のインシデント件数と漏えい人数

■3 群 － 7 編 － 1 章

1-3 攻撃の分類

（執筆者：安田なお）［2009 年 1 月 受領］

情報セキュリティにかかわる攻撃や防御，対策などには，既に述べたようにインターネットを媒介しないものも含まれるが，ここではインターネットが介在する場合について考える．実際の攻撃手法などの詳細は次章以降で触れるが，攻撃の手段を大雑把に分類すると，次の二つに大別することができる．

(1) **直接的攻撃**：第三者が，権限をもっていないコンピュータを直接的に操作し，通信路を経由して，ネットワークに接続されているコンピュータに侵入し，コンピュータ内のプロセスやファイルなどへコンピュータの管理者が意図しない操作を行う．悪意の第三者は，他人になりすましたり，セキュリティホールを利用して対象となるコンピュータに侵入を試みる．「不正アクセス」とも呼ばれる．

(2) 間接的攻撃：第三者が，コンピュータ管理者の意図しない不正な動作を行うソフトウェアを，対象とするコンピュータへ送りこみ，その不正ソフトウェアを介在して，コンピュータ内のプロセスやファイルなどへコンピュータの管理者が意図しない操作を行う．「コンピュータウイルス」とも呼ばれる．

直接的攻撃も間接的攻撃も，何らかの方法で対象とするコンピュータの操作権限を取得しなければならない．このため，正規ユーザの ID とパスワードを何らかのかたちで奪取するか，OS や基本的なソフトウェアのぜい弱性を利用して操作権限を奪取する．多くのシステムでは ID とパスワードが使われているが，パスワードを類推して片端から試すプログラムは多く出回っており，簡単に類推できるようなパスワードを使わないようにするのが望ましいが，人間の記憶力には限界がありなかなか難しい．特に最近は大抵の Web サービスで ID／パスワードの登録を行うようになっており，多数のパスワードを記憶するのは無理がある．このため，ID／パスワードは記憶に頼らず，何かに書いておき，コンピュータとは別の場所に保管するのが良いといわれている．また，乱数のような意味のない文字列も，常にメモを参照しなければ入力できないのでメモの管理上の危険性がかえって多くなるともいわれている．また，パスワードを聞き出す方法として，ネットワークやコンピュータを使うのではなく，人間どうしの接触による方法もある．普段は会ったこともないような上級の上司から突然電話がかかり，緊急事態が発生したので，あなたの管理している管理者権限のパスワードを今教えてほしい，というような電話が有名だが，人間心理を上手に利用して，相手が気づかないうちに必要な情報を聞き出す手段がある．「ソーシャルエンジニアリング」というが，人間の気持ちを逆手にとって利用しているので，システムではなかなか対応することが難しい．このような部分は，教育や情報共有で対応することが重要である．

記憶やメモに頼る ID とパスワードの限界を回避するために，IC カードや生体認証への期待も高いが，これらにも考慮すべき点がある．IC カードは，認証自体は電子署名を使い暗号解読に関する安全性も定量的な評価ができるが，物理的な IC カードに格納されているので，カード自体の盗難などには効果がない．「鍵管理」ともいわれるが，暗号アルゴリズムの安全性と，システムとしての安全性は別に考える必要がある．生体認証も指紋や掌紋，虹彩等々，他人と同じものはほぼないことが経験的に確認されていることから，なりすましや盗難など

からの安全性に期待があるが，生体自身には異なった刻印がされていても，それを読み取り判断するのは認証システムである．認証システムは，生体情報をアナログ的に読み取り，そこから特徴データを抽出するのだが，ここでアナログ→ディジタル変換が入る．このため，本人なのに本人と認識されない，あるいは，別人が本人と認識されてしまうという誤判断が起きる可能性がある．このため，パスワードなどの代替認証が用意されていることがあるが，結局このパスワードの強度までシステムの安全性が後退してしまう恐れがある．

攻撃には，コンピュータ内部に侵入して何がしかの操作を行うのではなく，ネットワークの外部から大量のアクセスを行うことにより，該当コンピュータの能力を使い切るか，ネットワークの帯域幅を使い尽くすことにより，正当な利用者がコンピュータを使えないようにする攻撃方法もある．DoS（Denial of Service）攻撃や DDoS（Distributed DoS）攻撃と呼ばれるが，該当コンピュータのデータを直接漏えいさせたり改ざんしたりするものではないが，コンピュータが利用できなくなることにより，経済的なダメージや社会的な影響が発生することがある．

■3 群 － 7 編 － 1 章

1-4 対策の概要

（執筆者：安田なお）［2009 年 1 月 受領］

セキュリティ対策を考えるとき，敷地の周りの塀の高さの比喩がいわれることがある．一部でも低いところがあれば，そこから侵入されてしまうので，どこも基準以上の高さの塀をつくらなければならないと．これは現実世界でも同じであるが，実際には地形を利用して闇雲に高い塀をつくらなくても済む場合がある．例えば，崖があったり，堀があったりすれば，その部分の塀は低くても全体としては機能するという議論である．何かを守るときに，一つの対策だけではなく，幾重にも重ねた階層防御モデルが重要である．更に階層がブロック化されていれば，組み合わせた強度が一定以上であれば，効果があるといえる．このような考え方によるシステムデザインやシステム設計手法もあるはずである．一律ではなく，必要な部分に必要な対策を取る，といった今までの経験則を利用することにより，守るべき情報の価値やリスクを評価し，必要最小限の対策や，更に余裕をもった対策を取るなどの判断と選択ができる．一律な対策は，一番安全な住まいは銀行の大金庫であるとか，パソコンを安全に保つには金庫に入れておけばよい，というような飛躍した論理に陥りがちである．

ぜい弱性（vulnerability）は新しい脅威のように感じられるかもしれないが，その原因はソフトウェアの Bug そのものといえる．そもそも Bug は自然にできるものではなく，設計者やプログラマという人間がつくり込んでしまうものである．たまたま露見していなかったものが，何かの拍子で発覚し，システム管理者の権限を取ってしまったり，権限外のデータ参照ができてしまったりすると，ぜい弱性と呼ばれる．Bug を根絶するのは極めて困難だが，今までも工業製品の安全性を確保するための考え方がいくつかある．

- フェールセーフ
  - 誤作動，障害時も常に安全側に動作する．
  - エンジンがオーバーヒートすると自動的にブレーキがかかる
- フールプルーフ
  - 操作ミスをしても安全側に動作する
  - 電子レンジのドアを開けると停止する
  - 乾電池ケースがプラス極の出っ張りと合っていて電池が反対側に入らない

高信頼性設計とも呼ばれているが，ほかにも主に冗長化で実現するフォルトトレラントなどがある．これは，主に可用性の確保が主な目的となっている．

ソフトウェアを設計するとき，対象となる業務の処理内容を整理し，どのように処理するかを決めて仕様書をつくるが，このような業務に基づく流れの中核になる仕様を「正常系」とか「機能要件」と呼ぶ．工業製品や業務アプリケーションを開発する際には重要な仕様であるが，設計・開発を行うときには，これだけでは十分ではない．入力項目と保存されたデータどうしの不整合があったときなどに行わなければならないリカバリ処理は，正常系の仕様や機能要件には明記されないことがよくある．このような機能仕様に明記されていない部分を「非正常系」「異常系」「非機能要件」などというが，多くはプログラマの実装手腕に依存しているのが現実である．このため，想定されていなかった入力が指定されたり，内部データとの不整合があった場合に，想定されていなかった副作用が起こる可能性がある．正常

系や機能要件で想定していない状態から正常系へ復旧するリカバリ処理によって，新たに想定外の状態が発生することもある．このような副作用も考慮しなければならない．経験と知識のあるプログラマであれば，想定外の状態を予想して，できるだけほかの機能に影響のないような回復処置をつくるように努力するが，かなり神経を使い手間もかかるのは事実である．これがぜい弱性の元となる Bug をつくり込む大きな要因の一つになっている．

「非正常系」や「非機能要件」の仕様は，本来は発注側で考える問題ではあるが，ソフトウェアの実行上の不整合対策は業務として考えるのは難しい部分もある．したがって，業務の専門家と設計・開発・実装の専門家が逐一検討を行い，副作用もセキュリティ要件と考え，脅威への対策を行うことが大切である．そもそもぜい弱性をつくり込まないようにする，ということである．このためにも，正常系／非正常系，機能要件／非機能要件のすべてに対して検討を加えることが大切である．重要なのはステークホルダのコミュニケーションであり，問題を事前に把握し，対策を考えることである．

設計・開発時にセキュアなシステムデザインを実現するために，第三者にも説明できる対策として，「脅威分析」を実施することが推奨されている．脅威分析は，STRIDE 分析と呼ばれる項目で行うのが一般的である．S：Spoofing（なりすまし），T：Tempering（改ざん），R：Repudiation（否認），I：Information Disclosure（情報漏えい），D：DoS（サービス不能），E：Elevation of Privilege（特権昇格）の分析を中心に確認してゆくもので，設計段階で想定される攻撃や脅威を想定して，あらかじめ適切な防御策を用意しておくための分析モデルとして知られている．

■参考文献

1) セキュリティ被害調査ワーキンググループ，NPO日本ネットワークセキュリティ協会（JNSA）
【速報版】2008 年上半期 情報セキュリティインシデントに関する調査報告書Ver. 1.0, 2008.12.
http://www.jnsa.org/result/2008/pol/incident/ , Dec. 2008.
2) セキュリティ被害調査ワーキンググループ，NPO日本ネットワークセキュリティ協会（JNSA）
2007 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Ver.1.5, 2008.12.
http://www.jnsa.org/result/2007/pol/incident/ , Dec. 2008.
3) 情報セキュリティ教科書執筆者 WG，“情報セキュリティプロフェッショナル教科書，”
アスキー・メディアワークス，Feb. 2009.
4) NPO 日本ネットワークセキュリティ協会（JNSA），NPO ネットワークリスクマネジメント協会（NRA），
“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，”
http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html, http://www.meti.go.jp/kohosys/press/0003929/, Apr. 2003.
5) NPO日本ネットワークセキュリティ協会（JNSA），“情報セキュリティスキルマップ構築の調査研究，”
http://www.ipa.go.jp/security/fy15/reports/skillmap/, Apr. 2004.
6) 安田直義，佐久間敦，松田剛，“知識の尺度「スキルマップ」と能力の評価について
－スキル評価の一側面の考察－，”電子情報通信学会 技術研究報告，vol.103, no.378,
http://db.ieice.org/gakkai/show.php?id=150376, Oct. 23th. 2003.
7) 経済産業省，“情報セキュリティ教育研究会報告書，”
http://www.meti.go.jp/policy/netsecurity/edu_report.html, Jun. 2004.
8) 情報セキュリティ教育の指導者向け手引書（2007 年版），
教育部会情報セキュリティ教育実証実験プロジェクト．
http://www.jnsa.org/result/2007/edu/materials/071111/