2005－CH－67（3）
2005／7／29

コンピュータ不正アクセスの脅威

―組織における情報セキュリティ対策―

坊農　豊彦　長井　壽満　橋本　信彦
日本大学大学院総合社会情報研究科

万能薬はないが、セキュリティの必要性はこれまで以上に重要である。一定の一貫したセキュリティへの取り組みだけが、幅広い種類のサイバー攻撃でもたらされた損害を、減少させる手助けとなり得る。

この論文では、安全保障リスク管理について、その人的側面に焦点を合わせる。 危険は、技術的な対策だけでは危険を回避することはできないからである。

また能動的でも、その検出システムを設置するだけでは安全保障問題の解決にはならない。私たちは、システムを担当しているすべての人々を教育する必要がある。それら該当者は、システムセキュリティの重要性を理解しているあらゆる層からエンドユーザのレベルまで含む。

A Threat of unlawful computer access

Information security measures in enterprise

BONO Toyohiko　NAGAI Toshimitu　HASHIMOTO Nobuhiko
Nihon University, Graduate School of Social and Cultural Studies

The need for security is more important than ever. There is no panacea. Instead, only a constant and consistent security effort can help diminish the damage caused by the wide variety of cyber attacks.

This paper focuses on the human security risk management aspects. The risks cannot be prevented from the technical countermeasures only.

Just putting the active detection system is not going to solve the security issues. We also need to educate all the persons in charge of the system, and let's them understand the importance on the system security at the every level, from the top management to the end users.

はじめに

近年、インターネットの利用人口は急速に拡大し続けている。この背景にはインターネット環境の整備とパソコンの高性能化がある。それらを利用する多くの組織は、インターネットをいち早く取り入れ旧来の集中型ネットワークから低価格のパソコンを並べた分散型ネットワークに改善した。

このような分散型ネットワーク(すなわちインターネットをインフラストラクチャとしたネットワークのシステム)を導入することにより組織の業務効率は著しく向上した。その反面、インターネットの拡大にともない、不正アクセスによる弊害が深刻な問題になっている。

不正アクセスは、インターネット利用が拡大するにともない増加しており、多くの組織で不正アクセスによる被害が発生している。また不正アクセスの被害を受けたコンピュータシステムは、情報データの漏洩や破壊などが起こり、組織業務の停止や信用問題にまで発展するケースが生じている。

2005 年 6 月､4000 万人の米国マスターカードの個人情報が流出し、68,000 人分の情報が既に不正使用されている事件が発生している[i]。

現在、情報セキュリティ(以下、「セキュリティ」)対策は技術による方法が主体になっている。またセキュリティ対策の技術は日進月歩で進化しているが、同時に不正アクセスの手法も進化して新たな被害が増え続け、もはや技術だけでは防止できない状況である。

組織の情報データは、顧客・社員などの個人情報や製品データなど知的財産を保有しており、これらは重要な情報資産である。不正アクセスから情報資産を守り、組織に於いてコンピュータ業務を安全に運用する事は喫緊の課題であろう。

本論では、セキュリティ対策を技術だけで解決する方法のみでは困難であることを鑑み、一般コンピュータ利用者(以下、「ユーザ」)の意識改善に重点を置いて論述する。

第１章　不正アクセスの定義

不正アクセスとは、無断で組織のネットワークやコンピュータに侵入して攻撃する犯罪行為である。またそれら不正アクセスの形態はさまざまな手法がみられる[ii]。

本章では、実際に組織で日常発生している不正アクセスの目的と手法を示し不正アクセスの範囲を定義する。

１　不正アクセスの目的

不正アクセスの目的には、機密情報の入手、嫌がらせ、自己顕示などがある。また不正アクセス行為者で強い目的意識を持っている者ほど用意周到である。目的達成のためには手段を選ばず、重大な被害を与える可能性が高い。

２ 不正アクセスの手法

不正アクセスに対する有効なセキュリティ対策を施すためには、不正アクセス行為者が、どのような手法を使うのか知っておく必要がある。不正アクセスの手法は目的や仕組みによって表 1.1 のような分類ができる[iii]。

表 1.1 不正アクセス手法、目的別分類表

手法･目的	実態例
情報収集	ポートスキャン、ソーシャルエンジニアリング等
侵入	パスワードクラック、バッファオーバーフロー等
妨害や嫌がらせ	DoS攻撃、スパムメール等
悪意ある攻撃	コンピュータウイルス、ワーム等

(出典) 上原孝之『情報セキュリティアドミニストレータ』翔泳社、2003 年 4 月、P49。

第２章　　セキュリティ対策の動向

不正アクセスを防止する為のセキュリティ対策には、技術と運用ルールの両者が整合性をもって維持されている必要がある。

今までインターネットを利用している多くの組織では、技術対策さえ十分であれば安心だという誤った認識を持っているケースが多い。技術対策のポイントとしては IDS[iv]やファイアウォールなどのセキュリティ製品がある。ただし、これらを導入しただけではセキュリティの向上に結びつかない。セキュリティ機器を導入すると同時に、各自の組織形態に合った初期設定が必要である。また不正アクセスの形態は変化するので、それに合わせるようにセキュリティ機器のメンテナンスを行い、常に新しい不正アクセスに耐えられるような維持管理が重要となる。

このように技術面からのセキュリティ対策には限界がある。すなわちセキュリティを強化するには、システムを利用する際のルールが必要となる。

ルールを制定するにあたって、組織のセキュリティ管理者は行政における法制度のあり方や国際規格によるセキュリティ政策を十分理解した上で、組織のセキュリティ対策の指針を検討しなければならない。

１ 法律によるセキュリティ対策の規制

多発するネットワーク犯罪に対してセキュリティに関する国際規格の制定や政府の e-japan 構想[v]などを受け、国内においてもセキュリティに関する法律が急速に進んでいる。セキュリティ対策は組織や企業のマネジメントにおいて、その重要性

がますます高まる傾向にある[vi]。国としても情報セキュリティ政策が重要な課題となっている。わが国においては、2005 年 4 月 25 日に内閣官房情報セキュリティセンター（NISC)が発足した[vii]。

2 組織によるセキュリティ対策の現状

現状多くの組織活動に於いて情報資産の価値とセキュリティ対策にかけるコストの間にはトレードオフの関係がある。セキュリティ製品は一度導入した後も引き続きメンテナンスをしなければ効果を発揮できない。

図 2.1 にはセキュリティ機器の代表的な製品であるファイアウォール概念を示した。ファイアウォールは外部（インターネット）からのアクセスは公開サーバーにしかアクセスできない仕掛けになっている。

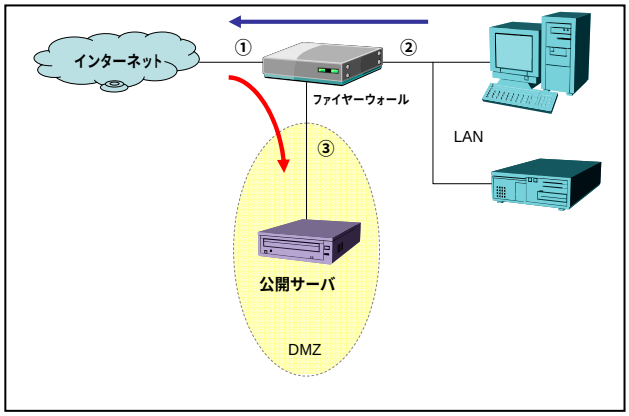

図 2.1　ファイアウォールの構成図

（出典）坊農豊彦　作成。

第３章　セキュリティマネジメントの取組み

ファイアウォールをはじめとした技術対策は、主に外部からの脅威に対しては有効に機能するが、内部の「人」の脅威に対しては限界がある。たとえば、組織のセキュリティ管理者が、悪意を持って不正アクセスをした場合などは防ぎようがない。より効果的なセキュリティ対策を行うためには、技術面での対策ばかりでなく、運用管理面での対策が必要になる。したがってセキュリティのレベルを大きく左右する要素となるのは「人」である。情報漏洩はネットワーク経由からだけではない。

情報記憶媒体であるメモリーカード、フロッピーディスクや CD 等のハードが盗難されることにより、組織の情報資産が一緒に漏洩することになる。2005 年 6 月には生徒の個人情報が入ったパソコンが盗難にあっている[viii]。ハードの盗難・紛失による情報漏洩対策も運用管理面の一環として行う必要がある。

組織内のコンピュータシステムには様々な「人」が関与している。悪意を持つユーザ、一般的なユーザ、セキュリティ意識の高いユーザ、セキュリティ意識の低いユーザなど、技術レベルや意識の違いによって、セキュリティに対する脅威のレベルは異なってくる。有効な対策を考えるためには、システムに関与する人々、すなわち組織のトップを含む経営陣からパソコンを利用している全てのメンバー（外注先・第三者も含む）にセキュリティルールの必要性を理解させ協力してもらう必要性がある。

システムに関与する人々に「何を守るのか」明確に提示できなければ協力を得られない。すなわち組織が持っている情報資産の価値をはっきりさせる必要がある。システム管理者は組織の情報資産がどの程度の資産価値を持っているのか、どのような状態にあるのか、状態によってどのようなリスクが生じるのか、といったことを分析する能力を持つが必要がある。このように、守るべきセキュリティの価値を明確にして、組織の価値を維持する環境として「人」に着目してリスクを分析することが、有効なセキュリティ対策を施すための第一歩となる。

セキュリティマネジメントとは、上述の結果を受けて対策を実施し、セキュリティを高め、運用管理を維持するための基本的な手法である。企業や組織の持つ情報資産を守るための具体的な方法や規定を明文化したルールがセキュリティポリシー(以下「セキュリティポリシー」)である[ix]。

1 リスク対応

リスクの構成要素としては、情報資産、脅威、脆弱性の 3 つが、リスクを構成する主要な要素である。リスクとは、まず社内に内在するさまざま

なリスクを定性的に分析して守るべき情報資産の価値を明確に定義する。この定義に基づいて最適なセキュリティ対策を決定する過程のプロセスが「リスクマネジメント」である。

2 セキュリティポリシーの概要

効果的なセキュリティ対策を実施するには、情報セキュリティポリシーの策定が不可欠である。セキュリティポリシーとは組織の情報資産を守るための方針や基準を明文化したものである。組織は膨大な情報を持っている。全ての情報にセキュリティという鍵をかけるのは非現実的である。守るべき情報の価値を定め、守る優先順位をつけるのがセキュリティポリシーである。セキュリティポリシーを間違えると、有効なセキュリティ体制の確立が出来なくなる。経営陣まで巻き込んだセキュリティポリシー作成が肝要である。

セキュリティポリシーは、あくまでスタートポイントである。セキュリティに関する方針や基準が明文化されたというだけで、実際のセキュリティレベルは何も変わっていない。セキュリティポリシーに書かれていることを正しく実施、導入できたときに、はじめて組織におけるセキュリティポリシーの目的が達成できるのである。

（1） セキュリティポリシーの導入計画

セキュリティポリシーを実施、運用するためには、まずセキュリティ推進担当者が計画を立案し、最高責任者は立案を精査し承認しなくてはならない。トップの理解・協力なしで、運用レベルで関係者間の協力は仰げない。セキュリティポリシー策定後の実施、運用をスムーズに進めるためには、ポリシー策定と計画の立案は並行して進めるべきである。

（2） セキュリティポリシーの運用

セキュリティを取り巻く状況は時々刻々と変化している。組織の形態に変更があれば、当然のセキュリティポリシーは見直される。管理層・セキュリティ担当部門は、このような状況の変化を的確に捉え、それに応じた新たなセキュリティ対策を施すなどの継続的な取り組みが必要となる。

一般的に情報資産の認識、保全の考え方はまだ浸透していない。この一因はセキュリティ対コストの問題がある。セキュリティとコストは比例関係にある。かつ、コストは増える傾向にある（図 3－1）。

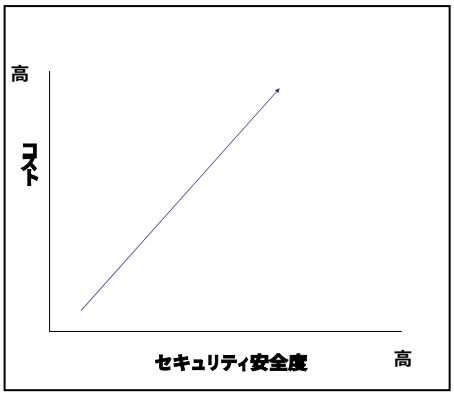

図 3.1　コストとセキュリティの関係
（出典；長井作成）

限られたコストの範囲で行うセキュリティ保全に対する一連の取り組みこそがセキュリティポリシーの運用であり、セキュリティマネジメントである。

表 3.1　セキュリティに影響を与える事象表

組織内	経営方針、事業計画、予算、組織変更、事務所の新設･移転、ネットワークの拡張、新規システムの運用開始、社員の採用･退職、関連業務のアウトソーシング内容やベンダの変更、情報セキュリティポリシーの遵守状況など
組織外	新たなウイルス･ワームの発生、新たなセキュリティホールの発見、ソフトウェアのバージョンアップ、セキュリティパッチのリリース、新製品のリリース、情報セキュリティに関する注目すべき事件の発生、情報セキュリティに関する国際標準･国内規格の発行、法律の施行、セキュリティ関連機関からの勧告　など

(出典)上原孝之『情報セキュリティアドミニストレータ』翔泳社、2003 年 4 月、P143。

第４章　セキュリティ対策の提言

近年のセキュリティ技術の進歩と普及の度合いには目覚しいものがある。例えば、ファイアウォール

や IDS の導入は数年前とは比較にならないほど普及してきている。今では個人でも、ウイルス対策ソフトのインストールは常識となっている。セキュリティ対策の大切なポイントは、各組織のセキュリティポリシーに応じた適切なセキュリティ技術や製品を導入して、それらを適切に運用することである。

加えてリスク管理として近い将来発生し得る事故備え、事故が生じた際の対応手順を事前に明確にしておくことも肝要である。日常運用・事故発生時の対応はその手順にしたがって運用を行う。本章では、外部からだけの攻撃だけでなく、内部からの情報漏洩も念頭に置いた組織のセキュリティポリシー手順にしたがったセキュリティマネジメント運用を考察する。

１．インシデントレスポンス（事故対策）

セキュリティにおけるインシデントとは、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と解釈される。つまり、不正アクセスやウイルス被害などがそれにあたる。インシデントに対応をすることをインシデントレスポンスと呼ばれている。

たとえば現在、一般に用いられているソフトウェアの多くはとても複雑に作られている。したがってソフトウェアの開発者ですら気が付かないようなセキュリティ上の弱点（脆弱性）が何かのきっかけで新たに見つかる可能性がある。想定外の不正アクセスが発生したときに対応するセキュリティポリシーとして以下のような提言を行う[x]。

（1） インシデントに対する準備

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とアクセスログ(以下、「ログ」)の取得内容の整理および取得方法の整備を行う。

（2） インシデントの発見

ログのチェック手順の整備を行いデータの改ざんや破壊が行われていないかの確認を行う。

（3） インシデントからの復旧

個々の作業において「判断」を下す責任者を明確にしておき、インシデント発見のきっかけ、インシデントの原因、具体的な復旧作業内容などの管理を行う。

（4） 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手順を作成して、JPCERT/CC などの公的機関への報告（届け出）や運用ポリシーや手順の見直しを実施する。

２ セキュリティ教育の充実

不正アクセスを防止するためのセキュリティポリシー策定を維持運用する上で、社員各自が危機感を持ちセキュリティマネジメント取り組みを行うことが重要となる。昨今、内部関係者からの情報漏洩が話題になっている。内部からの情報漏洩を念頭に置いた人材教育や社員の啓蒙活動も欠かせない。リスクマネジメントの観点からも、情報セキュリティ対策の必要性はますます高まっている。

（1） セキュリティ教育の実施

組織の不正アクセスや事故（インシデント）は内部関係者が関与している可能性があり、その大半は「故意」ではなく過失(うっかりミスや思い違い)が原因である。

セキュリティ教育は、継続と反復によって社員のリテラシーレベルを向上させることで、かなりの改善を図ることができる。一方で、効果的なセキュリティ教育や研修を実施するためには、対象となる研修者は全社員であり、職種や特性に合わせたカリキュラムを選択する必要がある（経営者向けの教育と、アルバイト社員向けの教育が同じ内容では効果が上がらない）。

セキュリティ教育は概念や理念などの内容に陥りやすいが、社員への浸透度を上げるためには、より具体的な事例情報が求められるべきである。また一般社員のセキュリティ意識を徹底する教育は、継続と反復を実施することである。特に、情報資産の価値を正確に把握し、情報漏洩が組織に与えるダメージがどれだけ大きいか、理解してもらうことが肝要である。例えば、ヤフーの情報漏洩の際、ヤフーは被害者に補償金 500 円を支払い、数十億円の損金を決算で計上している[xi]。

3 社員意識の改善

社員の中では、社内にてコンピュータを私用に使ったことがあるかという問いに自信を持って「NO」と答えられる人は、恐らく 10%にも満たないのではないだろ。ほとんどの社員が、「許可はされていない認識はあるが、常識の範囲なら私用しても何もいわれない」、「たぶん禁止されていると思うので、よくないとは思うがたまにはよいであろう」と答えている。

多くの組織では社員のコンピュータ利用の最終判断は「個人のモラルに任せる」というところが大勢を占めているのが現実である。

外部からの攻撃を避けるという意味で、アダルトサイトやオークションサイトなどをあらかじめ閲覧禁止サイトとして設定し、ユーザがアクセスした場合には「警告」の 2 文字をページ一面に表示するなどの対策を施している組織も有る。社員のインターネットの私用を制限する理由は、安全でないホームページ閲覧によるウイルス感染や、不正侵入などの外部からの攻撃の脅威にさらされるということである。

少し前までは、社内コンピュータシステムを利用するうえで、ユーザが注意しなければならないことは、メールに添付されるウイルスに感染することくらいであった。しかし、ここ数年の間に、不正アクセス行為者はセキュリティホールを悪用して、ユーザがある特定のサイトにアクセスした際に自動的に悪意のあるプログラムを実行させられたりする、いわゆる能動的な被害が急激に増加している。

この被害を避けるためには、ユーザに外部攻撃の危険性を理解してもらう必要がある。そのうえで、セキュリティホール情報を常にチェックし、何らかの対策か、修正プログラムが公開されたらすぐに、社内ネットワークに接続するすべてのコンピュータに適用する [xii]。

日立製作所では、社員の使用しているパソコンを自由に持ち出せないようなシステムを提供している[xiii]。組織によっては PC を自宅持ち帰り厳禁、社外持ち出し履歴管理とルールを定めている。セキュリティポリシーを管理していくためのルールは厳しく煩雑なものが多いのも事実である。しかし、あまりにも煩雑なルールを管理者からトップダウンで押し付けると、社員のセキュリティ意識は却って疲労しインターネット・IT 化の利便性を享受する意識に水を差すことになり、仕事の効率に影響を与えることになる。このような事態を避けるためには、まずは何を守るのか、守るもの価値を明確に定義しなくてはならない。

理解できない価値を守らせる事は不可能である。手段としては講義形式の教育ばかりではなく、グループディスカッション式の教育研修により社員の問題意識や改善提案を吸い上げる等息の長い活動が必要である。㈱日立情報システムズは情報媒体である「紙」のセキュリティ保全システム構築（ハードとソフトを含む）に 1987 年～1999 年の長い年月をかけている[xiv]。守るべきセキュリティの明確化と社員の理解がなければ、いくら社内運動・教育を行っても砂上の楼閣である。その上で、情報セキュリティ教育の内容をしっかりと守った組織へのインセンティブ、守らなかった組織へのペナルティなどの信賞必罰を教育プログラムと連動して導入するこが有効である。[xv]

おわりに

本論では不正アクセスの実態を説明して組織における不正アクセスのセキュリティ対策として現状の問題について明らかにした。セキュリティの最後の砦は「人」である。どんなに厳格なルールや強固なシステムを導入しても、それを実行する「人」の意識が低ければ組織の個人情報や知的財産である情報資産を守ることはできない。組織におけるセキュリティ対策の根幹をなすものは、ユーザーレベルのセキュリティ管理の発想である。

今後、ネットワークの分散化は、IT やインターネットの発展によって、さらに進むと予想される。組織におけるインターネットの利用は情報の共有化が目的であり、情報の共有が機能すれば大きな富を得ることが可能である。しかし、同時に、インターネットの発展は不正アクセスによって脅威をもたらしている。不正アクセスは毎年増え続けてそれらの技

術も洗練されるにつれて、不正アクセスの被害は組織に限らず、社会全体に広げ深刻な状況を及ぼしている。

現在、多くの組織でリスクマネジメントの一環として IT セキュリティ対策を急務に進めている。しかし、セキュリティ対策として、いくら技術的に堅固なセキュリティ製品やセキュリティポリシーを策定しても組織内のコンピュータを使うユーザがセキュリティについての意識を持たない限り、組織におけるセキュリティ対策は効果が出ない。

つまりセキュリティの対策のポイントは、社員各自に IT セキュリティの意識を持たせる事が喫緊の課題である。

外部から組織にウイルスが進入したら瞬時にして全コンピュータに感染するのである。もはや「自分は大丈夫であろう」という意識は通用しない。同時に内部からの情報漏洩対策も必須である。外部と内部対策は、車の両輪であり、一つが欠けたら動かないのである。そのためには、全社員へのセキュリティ啓蒙運動が重要な位置付けとなる。

今後の課題として組織毎に守るべき情報価値を明確にして組織の情報資産と見合ったセキュリティ対策と社員のコンピュータ利用者の意識を改めさせる一元管理された総合セキュリティマネジメントシステムの構築が必要急務である。とくにスモールビジネスにも適合できる手法の開発が必要である。現在、技術の動向としてはネットワークにアクセスするユーザ生体認証技術利用して、すべて記録に残し、セキュリティを確保する方向で進んでいる。しかし、日進月歩で進む IT 業界で絶対と言える対策はありえないであろう。最終的にはシステムを扱う(人)の問題を避けては通れない課題である。

---

[i] http://www.asahi.com/business/update/0620/001.html (2005 年 6 月 20 日)。

ii ドナルド･ペプキン『企業･ユーザのための情報セキュリティ戦略』久下哲夫･矢野達男･星野秀明訳、ピアソンエデュケーション、2002 年、1 月、213 頁。

iii 上原孝之『情報セキュリティアドミニストレータ』翔泳社、2003 年 4 月、48-59 頁。

iv IDS とは不正アクセスを検知するプログラムである。

v 2000 年 9 月 21 日に森首相(当時)が所信表明演説の中で掲げた、全ての国民が情報通信技術を活用できる日本型 IT を実現するための構想。

vi 上原孝之『情報セキュリティアドミニストレータ』翔泳社、2003 年 4 月、229 頁。

[vii] 内閣官房情報セキュリティセンター、http://www.bits.go.jp/ (2005 年 6 月 19 日)。

[viii] 日本経済新聞社、http://kensaku.nikkei.co.jp/cgi-bin/common.cgi (2005 年 6 月 19 日)。

ix 上原孝之『ネットワーク危機管理入門』翔泳社、2000 年 7 月、44-45 頁。

x アットマーク･アイティ、http://www.atmarkit.co.jp/fsecurity/rensai/inci01/inci01.html (2005 年1月 3 日)。

[xi] 週刊！木村剛 powered by ココログ、http://kimuratakeshi.cocolog-nifty.com/blog/2004/03/_5.html (2005 年 6 月 20 日)。

xii アットマーク･アイティ、http://www.atmarkit.co.jp/fsecurity/rensai/policy11/policy01.html (2005 年 1 月3日)。

[xiii] アットマーク･アイティ、http://www.atmarkit.co.jp/news/200502/16/hitachi.html (2005 年 6 月 20 日)

[xiv] 関谷紀雄『ハイセキュリティ紙資源循環システムの開発と普及』、日本セキュリティマネジメント学会第 19 回全国大会発表要旨、2005 年 6 月 18 日、89 頁～95 頁

xv インフォセック、http://www.infosec.co.jp/counsel/d2.html (2005 年 1 月 2 日)

参考文献

(1) 板倉正俊『インターネット・セキユリィとは何か』日経 BP 社、2002 年 5 月

(2) 上原孝之『ネットワーク危機管理入門』翔泳社、2000 年 7 月

(3) 上原孝之『情報セキュリティアドミニストレータ』翔泳社、2003 年 4 月

(4) 岡村久道『インターネット訴訟 2000』ソフトバンクパブリッシング、2000 年 7 月

(5) 田渕治樹『国際セキュリティ標準 ISO/IEC17799 入門』オーム社、2001 年 5 月

(6) ドナルド・ペプキン『企業・ユーザのための情報セキュリティ戦略』久下哲夫・矢野達男・星野秀明訳、ピアソン、エデュケーション、2002 年、1 月