資　料

西九州大学情報処理システムの現状と今後 —情報セキュリティ—

高元宗一郎[1]，古賀浩二[2]，井上千春[1]

([1]西九州大学庶務課，[2]西九州大学健康福祉学部)

(平成15年10月31日受理)

The Present Condition and Future of the Nishikyushu University Information Processing System : The Information Security

Soichiro TAKAMOTO[1], Koji KOGA[2], Chiharu INOUE[1]

([1]*Administrative Affairs Division, Nishikyushu University,*
[2]*Faculty of Health and Social Welfare Science, Nishikyushu University*)

(Accepted October 31, 2003)

Abstract

It is well known that the computer system security is composed of a balance by the reliability and cost and service. In the past, the operation failure has occurred by computer viruses and crackers,etc.. in this Univ. These problems originate for several things on the computer network system. As a method of solving these problems technically, we mention a FireWall and DMZ etc. However, Some of the most important things are the organization that manages the information system and the Security Policy. Especially Security Policy is strongly required to the university that is a scientific research organization. In this paper, we show the present information processing system of Nishikyusyu University. Furthermore, we propose the information security required in the future.

Key words : Information security 情報セキュリティ
Security Policy セキュリティポリシー

1．はじめに

近年のコンピュータの低価格化やブロードバンドの普及に伴い，誰もが高速なインターネット環境を簡単に整備出来るようになってきている。最近では，携帯情報端末と無線装置を活用することで，場所を選ばずインターネットを利用することが可能になってきており，今後ますますインターネットを手軽に利用することが出来るようになると考えられる。

本学でも，平成15年４月より第２情報処理実習室や学生ホールの情報コンセントなどの運用を開始し，学生向けの情報サービス向上に務めている。

このように，誰もがコンピュータを利用し，インターネットを活用出来る環境ではコンピュータシステムに関わる様々な問題が発生してくる。その１つに情報セキュリティに関わる問題が挙げられる。インターネットに代表されるコンピュータネットワークは，その現象が目に見えにくいため，故意，過失によらず，不正なコンピュータの使用を発見することが難しい。その結果，情報の改ざんや漏洩など好ましくない事件が発生する。今後，ますますインターネットの普及が確実となっている現在，このような事件・事故に対する備えが必要であることはいうまでもない。

本稿では情報セキュリティの基本的な考え方や技術を示し，西九州大学の現状を報告すると共に今後どのような対策が必要なのかを紹介する。

2．情報セキュリティとは

2．1　情報セキュリティとは

情報セキュリティとは，情報処理システムを事件，事故から守ることをいう。

情報処理システムとは，情報を取り扱うためのハードウェア，ソフトウェアの全てを含めたものをいう。例えば，ユーザーが所持するそれぞれのパーソナルコンピュータ（以下，PC）及びそのコンピュータに導入されているソフトウェア，通信を行うためのネットワーク機器，各種サービスを行うためのサーバ機器等は情報処理システムである。

また，情報処理システムに関わる，事件・事故とは，故意，過失によらないコンピュータシステムの不正利用，ハードウェアの故障，天災などによってもたらされる様々な不利益な現象のことをいう。特にシステムに対する悪意のあるアクセスのことを不正アクセスという。この不正アクセスを受けることで，情報の改ざんや漏洩が事件・事故として発生することは珍しいことではない。また，不正アクセスを受けたコンピュータは，次の標的となるコンピュータを探索するための踏み台として利用されることも多い。これは，自身のコンピュータだけが被害を受けるだけでなく，他人にも被害を及ぼすので，大きな問題となる。

2．2　情報セキュリティの考え方

情報セキュリティを考えるに当たっては，次の３つの項目を考慮する必要がある。１つ目は情報処理システムの安全性，２つ目はシステムで提供するサービス内容，３つ目は情報セキュリティを維持するためのコストである。一般的に，これら３項目はそれぞれトレードオフの関係である。例えば，システムの安全性を向上するためには，十分なコストが必要であるし（②），提供するサービスを制限する必要がある（④）。コストを抑えようとすれば，システムの安全性は低下し（①），提供できるサービスも制限する必要がある（⑤）。また，サービスを充実させようとした場合，安全性は低下（③）し，コストは増加（⑥）する。したがって，情報セキュリティを維持するためには，３項目を総合的に検討し，全体的な向上を図る必要がある。

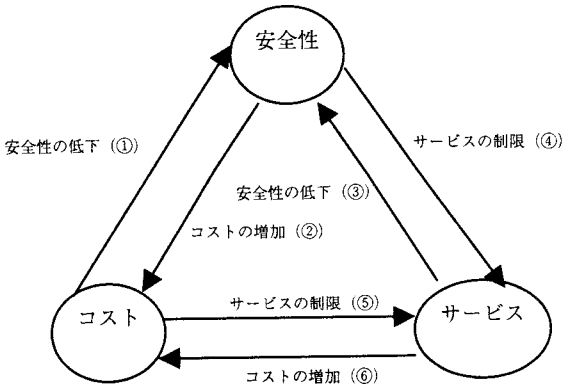

図１　安全性・コスト・サービスの関係

2．3　情報システムのセキュリティ向上のために

情報システムの安全性を向上させるためには，以下のことを検討する必要がある。

2．3．1　セキュリティポリシーの整備

セキュリティポリシーとは，組織の情報セキュリティに関する方針を示した文書のことであり，情報セキュリティを維持するための取組みについて包括的に規定した文書のことである。

セキュリティポリシーを作成する上では，システム管理者が一方的に決定するものではなく，ユーザーとシステム管理者及び組織運営者（大学運営者）が話し合いのうえ，安全性と利便性とコストのバランスをとらなければならない。

セキュリティポリシーは，組織が守るべき範囲の決定等組織（大学）全体に関わる事項から，セキュリティを維持するために必要なシステムや機器，ユーザーが利用出来なければいけないサービスなどの管理・運用を具体的に記述したものまで幅広く記述される。

セキュリティポリシーを作成する場合には「ユーザー使用条件」と「セキュリティ要件」を挙げ，必要であるものを採択していく。例えば，下記のような要件が挙げ

られると考えられる。

	要件内容
ユーザー使用要件	○ユーザーはインターネット上で電子メールの送受信が出来なければならない。 ○ユーザーはファイルサーバにドキュメントを保存できなければならない。
セキュリティ要件	○不正アクセスが内部ネットワークにアクセス出来るようになっていてはいけない。 ○ユーザーは推測が容易なパスワードを利用してはならない。

表１　ユーザー使用条件とセキュリティ要件の例

情報処理設備の整備やサービスの充実などは，このようにして作成したセキュリティポリシーに沿って計画，実行されなければならない。

情報技術の進歩，不正アクセスの技術やコンピュータウィルス等のセキュリティに対する脅威は，常に変化，高度化し，また，ユーザーの要求は，環境とともに変化するため，システムに関するルールを規定しているセキュリティポリシーは，定期的または非定期的に改良を行う必要がある。通常セキュリティポリシーは，計画（Plan），実行（Do），見直し（See）の３つのフェーズを繰り返すが，このPDSサイクルによって，変化し続けるリスクの捕捉とそのリスクへの対策を早期に実施することが出来る。

２．３．２　システムの運用・管理

情報処理システムを管理する上では，管理組織を設け，総合的に管理を行うことが必要である。

管理組織を設置する際には，まずCIO（Chief Information Officer：情報システム部門統括責任者）を配置するのが一般的であり，多くは組織の役員が務める[2)]。管理組織は，このCIOを中心に技術職員，事務職員等が配置されることが望ましい。必要であれば，アウトソーシング等を利用して外部からの技術者を配置することも検討すべきであると考える。外部からの技術者を配置することで，内部技術者では習得が困難である，より専門的なセキュリティ技術を実施することが可能になる。

管理組織の業務内容は，主に情報処理システムの安定運用を目的として行うが，その内容は、ユーザー教育，セキュリティポリシーのPDSサイクルの実施，機器の管理等，多岐にわたる。

２．３．３　物理的セキュリティ（セキュリティ維持のための必要機器）

セキュリティ方針（ポリシー）及び体制が整うと，次は実際にポリシーに沿ってコンピュータシステムを様々な脅威から守るため，専用の機器やネットワーク構成が必要となる。一般的に用いられるものを以下に示す。

(1)　FireWall（ファイヤーウォール）

組織外部ネットワーク（インターネット等）と組織内部ネットワーク（学内LAN等）のデータの出入口には，ファイヤーウォール（防火壁）といわれるシステムを設置する。ファイヤーウォールは，組織外部のネットワークと内部のネットワークが通信を行おうとするたびに，そのコネクション（通信内容）を調べ，通信の許可または拒否の判断を行うシステムである。その概略を図２に示す。

このシステムにより，外部ネットワークからの不正アクセスを防止する。

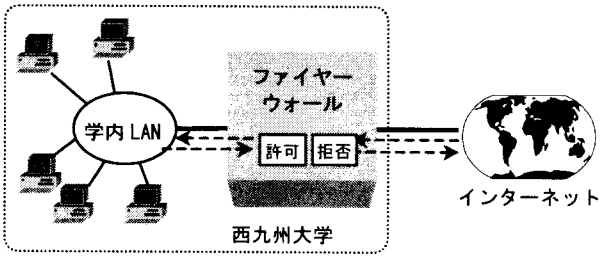

図２　ファイヤーウォールの概略

(2)　DMZ（DeMilitarized Zone：非武装地帯）

ファイヤーウォールの設置に伴いDMZと言われる領域を設けることが多い。

DMZを設定することで，Webサーバや電子メールサーバ等の外部ネットワークと直接通信する部分，つまり外部からの不正アクセスの対象となりやすいシステムと，内部ネットワークとを論理上分離することが出来る。このシステムにより，もし，DMZ内のサーバに問題が生じたとしても被害はDMZ内だけで収まり，内部ネットワーク及び外部ネットワークへの影響を最小限に抑えることが出来る。

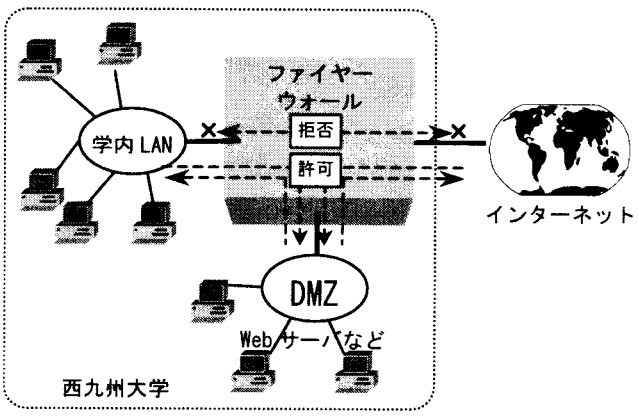

図３　ＤＭＺの概略

(3)　IDS（Intrusion Detection System：侵入検知システム）

ファイヤーウォールは，外部ネットワークからの不正アクセスを防ぐ上では有効であるが，万能ではなく，時には不正アクセスの通信を許可してしまう場合もある。また，ファイヤーウォールは一度内部ネットワークに侵入された不正アクセスには無力である。

したがって，不正アクセスでファイヤーウォールを越

えて侵入された場合の事を考え，IDSと呼ばれるシステムを導入することが一般的である。IDSは，ネットワークの様々な現象の中から，内部ネットワークへの侵入を検知するシステムである。IDSの中で最も一般的な，インスペクタと言われる種類のものは，ネットワークやコンピュータの動作を監視し，不正な処理が行われていることを示す兆候をもとに不正アクセスを判断する。

具体的には，以下のような項目に関して組み合わせによる監視を行い，その記録を作成する。

○ネットワークトラフィック（ポートスキャンなど）
○既に知られている一般的な攻撃手法の兆候
○コンピュータの使用状況（CPUなどの使用率等）
○ファイルに対する操作（システムファイルの改変等）

である。こうした兆候のさまざまな組み合わせを監視して，その記録を作成する。

このような，IDSを内部ネットワークとDMZに配置することにより，不正アクセスの内部ネットワーク侵入検知に役立てることが出来る。

3．西九州大学の現状と課題

3．1　西九州大学情報処理システムの現状

3．1．1　情報処理システム

本学の情報処理システムは，平成９年度に教育用システムとしてPC50台が導入(現第1情報処理実習室)された。平成10年度には，研究用システムとしてPCを約80台導入し各研究室に設置された。また，Ethernetを使用した学内LANを敷設し，光ファイバにより学内の各建物間を接続した。これにより学内の全てのコンピュータをネットワーク接続し，サーバによるアカウント及びファイルシステム管理の運用を開始している。学外に対するネットワークは，同じく平成10年度に九州大学を経由して学術情報ネットワーク(SINET)に128kbpsの専用線を用いたネットワーク接続を行い，インターネットの利用が可能となった。この時点で，情報公開の手段である本学ホームページならびに電子メールの運用を開始している。運用にあたっては，本学で情報処理関係の授業を担当する教員(１名)がその運用・管理等にあたった。

平成15年度には介護教育棟，６号館，学生ホールの新設に伴い，増設された建物間を光ケーブルで接続し，学内ネットワークを拡大している。また，第2情報処理実習室を新設し，新たに約50台のPCを導入した。

このような経緯を経て，現在本学では，情報処理担当教員１名，アシスタント(兼任)１名により，学内に約200台のPC，約10台のサーバ，25台を超えるルーティング装置を有した情報処理システムを運用している。

利用者数については，平成15年度に入って講義での実習室利用の増加，開放時間における利用者も増加している。特に，卒業論文の執筆時期などに利用者が集中している。

3．1．2　情報セキュリティ

本学における情報セキュリティへの対応は，インターネット接続が整備された平成10年に開始されており，この年に学内LANと外部ネットワークのアクセスを制御するための装置として，学内ネットワークとインターネットをつなぐ幹線にファイヤーウォールが導入されている。これにより学外からの不正アクセスを防ぐことを可能とした。しかし，当時学内ネットワークにおけるコンピュータウィルスなどへの特別な対策は取っておらず，平成11年に学内の一部のコンピュータがコンピュータウィルスに感染した。インターネットで公開されているワクチンソフトなどにより感染は限られた範囲で納まったが，継続的な対策をしなかったため，平成13年に再び同じコンピュータウィルスによる被害が学内で発生し，これを機に，全学的にコンピュータウィルス対策ソフトの導入を行っている。

平成15年３月には，学外（海外）から本学のホームページサーバへの不正アクセスにより，サーバが持つデータの一部が改ざんされた[1]。このとき改ざんされたデータはホームページとして外部に公開しているページではなかったが，そのためにデータ改ざんの発見が遅れ，対応に多くの時間と手間を強いられた。原因は，オペレーティングシステム（OS）が持つセキュリティホール（セキュリティ上の欠陥）であったため，OSを作製しているメーカーが不定期に提供する修正ソフトウェアによりOSのアップグレードを行った。

3．2　西九州大学情報処理システムの問題点

前述のようなセキュリティ上の問題が発生すると，システム管理者はその都度対策を講じているが，場当たり的な対策となっている場合も少なくない。これは，セキュリティ管理に関わる技術的な問題をはじめとしたいくつかの問題がその原因であると考えられる。以下にその問題点を示す。

(1)　物理的セキュリティ対策の不足

本学では，前述のように，外部ネットワークに対するアクセスを制限するためのファイヤーウォールという装置が導入されており，実際にコンピュータのアクセス記録を調べると，ファイヤーウォールにより失敗した不正アクセスの試みが多く見つかっている。しかし，前章で紹介したように，このような機器をもってしても学内LANに不正侵入するウィルスやクラッカーが存在しており，ネットワークセキュリティの信頼性を更に向上させるためには，DMZやIDS，高機能のロガー（通信記録装置）などセキュリティ対応機器の導入が必要である。

(2)　情報収集能力の不足

ネットワークに対する不正侵入やウィルスの侵入は，そのほとんどが新たに発見されたオペレーティングシス

テムのセキュリティホールや新種のウィルスによって発生する。これらセキュリティホールや新種のウィルスに関する情報は数が多く，また，入手した情報が本学のシステムに対して脅威となるか，どの様な対策が必要かなど多くの情報を短期間で入手し，必要に応じた対応を施さなければならないが，現状では，これらの情報の入手が遅れる場合や，入手できた場合でも必要な対応に時間を要することがあり，時間的な問題でウィルスの被害にあうことも少なくない。

(3) マンパワーの不足

前項のように，絶えず新しいコンピュータウィルスやセキュリティホールが発見されている現状では，どのように高機能のセキュリティ対策機器を導入したとしても，それが導入された時点で既に陳腐化している場合も多く，常に高い信頼性を保つためには，情報収集能力に加えて，導入した機器を絶えず調整・管理していく必要がある。そのためには，コンピュータセキュリティに対して専門知識・技術を持った技術者が絶えず気を配りシステムセキュリティを運用する必要がある。本学では，現在，教員１名，アシスタント（兼任）１名で学内の管理業務を行っているが，学内のコンピュータも200台を超える規模となり，事件・事故などの発生時には作業的なオーバーロードによる対策の遅れなどが発生している。

(4) システム使用者のセキュリティに対する意識不足

前項で示した問題点をいくら解決したとしても，システム使用者のセキュリティに対する認識が不足しているとセキュリティの信頼性は著しく低下する。例えばコンピュータの利用者が自分のパスワード管理などを怠った結果，(悪意のある) 他人にシステムアカウントを不正利用され，場合によってはデータの改ざんが行われたり，ネットワークの運用を停止しなければならなくなることは珍しくない。システムの利用者は，このように個々の使用者の認識不足がシステム全体に大きな影響を及ぼす可能性があることを念頭において，コンピュータシステムを利用しなければならない。

4．本学における情報セキュリティの今後

今後，本学ではどのような対策に取り組むべきかを検討した。

4．1　セキュリティポリシーの策定

管理組織がセキュリティ活動を行うための指針であるセキュリティポリシーの策定を行う必要がある。ポリシーの策定を行う上では，情報セキュリティの国際規格等を参考にして本学に適用可能な各種要件を挙げる方法が，現実的かつ強固なセキュリティを確保できると考える。

セキュリティポリシーは，ポリシーの策定，その方針に基づくリスク分析，各現場におけるポリシーの適用など，セキュリティポリシーの決定から各現場におけるポリシーの適用まで１～２年の期間が必要である。そのため，策定・実施に関しては，年次的な計画を立て段階的に作業を進める必要がある。

セキュリティポリシーを各現場に適用するには，現場に携わる教職員への教育が必要である。この教職員に対する教育活動は，定期的に行う機会をつくるべきである。また，教職員に限らず学生に対してもセキュリティ教育が必要であると考える。この情報セキュリティ教育で得られる技術や知識は，本学在学中だけではなく，学生の卒業後の社会生活においても十分活用できるものである。情報セキュリティの知識は，情報化の流れが激しい一般社会においても必要なものであり，一般常識として定着しつつある。したがって，大学教育においても基本的な情報セキュリティの技術や知識を学ばせる機会を作ることが必要であると考える。また，このような講習会を通じて，教職員及び学生のPCの利用技術向上も望める。

4．2　管理体制の明確化

(1) 管理組織の必要性

情報処理システムの規模によっては，管理組織が存在しなくても管理者による運用が可能である場合もある。しかし，大学のように情報処理システムの障害や事故などが，講義ばかりでなく研究・事務処理等，大学運営全体に影響を与えるような規模になると，情報処理システムの安定運用には重大な責任がある。したがって，システムの安定運用を責務とした管理組織が必要であり，システム安定運用の責任の所在を明確化し，運用規模に応じたセキュリティ対策，機器導入及びセキュリティポリシーの策定などを検討してゆく必要があると考える。

(2) 人員体制

管理組織の人員は，セキュリティポリシーの要求に応えることが可能なように配置する必要がある。また，情報処理システムから発生する諸問題に対して，迅速かつ正確に対応するためには，専任の技術者が必要であると考える。

専任の技術者を配置することで，システム環境や規模に応じたシステムの運営・管理・構築を適切に実現することが出来ると考える。また，技術者の増員を行わず，外部の業者に維持・管理を委託することや，学内のシステム全体を一元管理できるような管理システムを整備することで必要な職員数を低減出来る場合もある。

また，逆にシステム管理の業務の一部をユーザー側に依存することでも職員数の低減も可能な場合がある。例えば，ユーザーが所持するデータは各自でバックアップの作業を行うなどである。このような管理業務の分散を必要に応じて検討することも考えられる。

4．3　将来構想に応じた計画的なシステム構築

情報処理システムは，大学の規模と運営方針に準じたものでなければならない。そのためには，大学が持つ将

来構想を実現するために情報処理システムとして何を実現するべきなのかを明確にする必要がある。情報セキュリティ対策も同様であり，常に大学の将来構想を意識した上で，冒頭で紹介したようにコストと安全性，サービスのバランスを考慮しながら，セキュリティ対策を実施する必要がある。

現時点で，必要であろうと考えられるシステム及びセキュリティの対策を示す。

(1) 外部ネットワークとの通信速度の高速化

現在，本学における外部ネットワークへの通信速度は，128Kbpsである。この速度は，一般家庭での利用者が１Mbps以上の速度で利用している現状を考えると非常に低速である。また，システム管理の面から見ても改善すべき問題である。

最近のシステム管理の作業は，ネットワーク上で行われることが多い。例えば，ソフトのセキュリティホールが発見された場合，その修正ソフトが配布されるが，その配布方法がインターネットを利用したものが多い。したがって，低速な通信回線を利用していると，セキュリティ対策の実施が遅れることになり，その間危険な状態を放置することになる。

ネットワークを利用して行われる通信が多様化，大容量化していることを考え，外部ネットワークとの回線速度の高速化は，今後実現すべきものである。

この通信速度の高速化を実現することで，将来，インターネットを利用した遠隔授業やウェブによる講義などを実施することも可能になると考える。

(2) 耐障害性の向上

現在のシステムでは，あるシステムの一部に障害が発生した時に，その障害が学内全体に影響を与え，学内のシステムを利用した業務を中断されることが考えられる。また，１台のサーバのメンテナンスを行う際には，その影響が学内全体に及ぶためサーバ停止の連絡とその周知の期間を設ける必要がり，速やかなメンテナンス作業が難しい状態である。このような状況を改善するために，システムの多重化が必要であると考える。システムを多重化し，冗長性を持たせることで，耐障害性を向上させ，速やかなメンテナンス作業も可能になる。

(3) セキュリティ機器の整備

策定されたセキュリティポリシーの要求に応じ，セキュリティ機器の整備を行う必要がある。具体的には，IDS，DMZの整備を行う必要がある。

DMZについては，平成15年度に整備を行っており，一部を除いてWebサーバ等の外部と直接通信を行うサーバは移行を完了している。今後，１～２年の間には，移行が完了していないサーバを移行する必要がある。

IDSについては，現在，サーバのログ（通信記録）から不正侵入を検知する簡易なシステムを利用しているが，本来であればさらに高度なIDS専用機器を用いてシステムの稼動状態を監視する必要があると考える。

４．４　ユーザーのセキュリティ意識向上

ユーザーのセキュリティ意識向上のためには，教育活動が重要であるが，定期的な講習会等のほかに，広報活動も重要となってくる。この広報活動は，現在のシステムが受けている脅威を知らせると共に，その脅威に対して行うべき対策を知らせることを目的として行う。

情報処理システムのセキュリティの状況は，時々刻々と変化しており，その状況にあわせてシステムを調整・整備を行う必要があるが，この状況を講習会等の定期的な教育活動で周知していくには，時間的な問題により無意味化していく可能性がある。したがって，学内の利用者がリアルタイムで現在の状況を知るための仕組みが必要になる。現在考えられる仕組みとしては，掲示物の利用，メーリングリストの利用，Webの利用が挙げられるが，必要に応じて複数の手段を講じる場合も考えられる。

５．最後に

本稿では，情報セキュリティの基本的な考え方を示し，現在の本学の現状を報告し，今後の対策案を示した。

情報セキュリティは，何事も起こらないように，または起こってもその影響を少なくするための措置であるため，その結果が見えにくい。しかし，情報処理システムが組織の重要な基盤となった現在では，情報セキュリティの取組みは組織にとって必要不可欠なものとなっていることを理解しなければならない。

また，情報セキュリティは，技術的な対策が表だって議論されることが多いが，情報を管理・利用するのは最終的に人であるため，システムの一般利用者の協力無しでは成り立たないものである。したがって，学内LANの一般の利用者（教職員及び学生）にも普段から情報セキュリティを意識してもらい，情報システムのセキュリティの維持に協力をお願いしたい。

本稿がこれからの本学の情報セキュリティ向上のきっかけとなれば幸いである。

６．参考文献

１）佐賀県警察本部生活安全部生活安全企画課ハイテク犯罪係：不正アクセス事例分析報告書，(2003)

２）情報処理振興事業協会セキュリティセンター：情報システム部門責任者のための情報セキュリティブックレット，(2001)

３）岡田庫太郎，セキュリティポリシーの策定と運用について，(2002)，(NTTデータ経営研究所)
http://www.keieiken.co.jp/monthly/repo0211/02112-1.shtml

４）内閣安全保障・危機管理室　情報セキュリティ対策

推進室：情報セキュリティポリシーに関するガイドライン，(2001)
http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html
5）Matthew Strebe著，㈱スリー・エー・システムズ訳：「ネットワークセキュリティ　ジャンプスタート」，(2003)，(技術評論社)
6）佐賀大学情報処理センター：佐賀大学情報処理センター広報　第9号，(2000)