学校情報セキュリティ
ガイド

平成 16 年 3 月

神奈川県立総合教育センター

目　　次

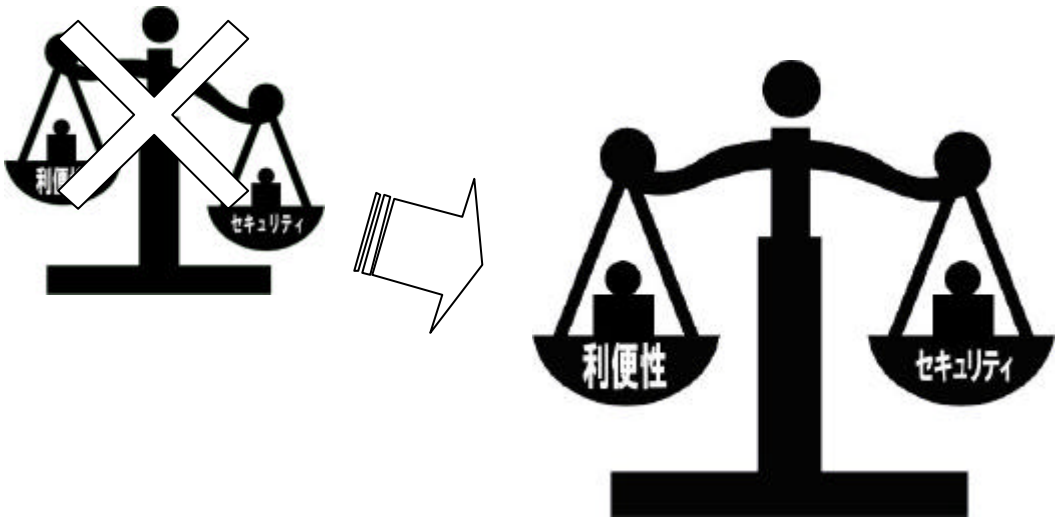
1．教育の情報化と情報セキュリティ

平成 10 年 12 月に、内閣総理大臣直属のタスクフォースとして発足した「バーチャルエージェンシー『教育の情報化プロジェクト』」では、「平成 17 年度を目標に全国の学校のすべての教室にコンピュータを整備し、すべての教室からインターネットにアクセスできる環境を実現する」という目標を明示した最終報告を平成 11 年 12 月に内閣総理大臣に提出しています。

この、バーチャルエージェンシーの報告により提言された諸施策は、「ミレニアム・プロジェクト『教育の情報化』」（平成 11 年 12 月）として内閣総理大臣決定され、「教科書」を使って行われる「各教科」の授業において、コンピュータやプロジェクタで「動画コンテンツ」などを活用することにより、「わかる授業」、「魅力ある授業」を実現することを目的に、平成 12 年度から 17 年度までの 6 年間にわたり、学校の情報環境整備を計画的に実施することとなっています。

このように「教育の情報化」が進展する一方で、インターネットの急激な普及などにより、コンピュータウイルスや不正アクセス、ネットワーク利用犯罪といった脅威が増大しており、このような背景のもと、学校においても情報セキュリティに対する関心が高くなり，注目が集まるようになっています。

ところで、情報セキュリティとは何でしょうか？用語集には、「コンピュータシステムの安全を守ること」や「通信される情報を守ること」などと書かれており、ファイアウォールやウイルス対策ソフトウェアといった技術的手段の利用から、ユーザ ID やパスワードの管理やマニュアルの整備といった運用面での注意まで含め、広い意味で情報や情報システムを守ることと考えることができます。しかしながら、単に「守る」という側面だけで情報セキュリティを捉えようとすると、「利用する」というもうひとつの側面への配慮に欠け、情報セキュリティの本質に迫ることができないという考え方もあります。例えば、利便性への配慮に欠けた規制は、形骸化を招き、その意図に反して、守りたい情報や情報システムを守ることができない危険性を負ってしまうようなケースも考えられます。つまり、情報セキュリティを考える上で重要な点は、「守る」という側面と「利用する」という側面のバランスを意識することであると考えられます。



情報漏洩などのリスクを低減することと、情報を活用するための利便性を向上することの間には、トレードオフの関係があります。そこで、このことを意識し、情報セキュリティを、次の 3 つの要素に分けて捉える考え方があります。

○ 機密性(confidentiality)
：認可されたものだけが情報にアクセスできること

○ 完全性(integrity)
：正確であること、及び完全であることを維持すること

○ 可用性(availability)
：許可されたものが必要なときに情報にアクセスすることが可能であること

これは平成 4 年に OECD が策定した「情報システムのセキュリティのためのガイドライン」（平成 14 年 8 月に全面改定）に記されているもので、一般に情報セキュリティとは、この 3 つの要素を確保し、維持することと定義されます。この 3 要素について、もう少しわかりやすく言いかえると、次のようになります。

機密性　⇒　情報を漏らさない 完全性　⇒　情報を壊さない 可用性　⇒　情報を使えるように保つ

上記の“機密性”と“完全性”は「守る」という側面に立った要素です。また、“可用性”は「利用する」という側面に立った要素ということができます。すなわち、情報セキュリティを確保するということは、これら 3 つの要素を意識し、保有する情報の重要度と存在するリスクを適切に評価し、「守る」ことと、「利用する」ことの両側面のバランスがとれた対策を行うことといえます。

参考　「教育の情報化」年次計画（ミレニアム・プロジェクトより）

年度		12	13	14	15	16	17
	校内 LAN の整備	段階的に整備【完成】(8,100 校)					
	公立学校のコンピュータ整備	全ての学級の授業でコンピュータが使える環境整備の推進					
	公立学校のインターネット接続	全ての公立学校がインターネットに接続					
	私立学校のコンピュータ整備	段階的に整備					
	教員研修の実施	すべての教員がコンピュータ操作等を習得					
	コンテンツ開発事業	開発事業の実施		成果の全国への普及			
	デジタルネットワーク化推進事業	開発事業の実施		成果の全国への普及			
	学校スポーツ･健康教育用コンテンツの制作	コンテンツの制作		成果の全国への普及			
	文化デジタルライブラリーの構築	コンテンツの制作		成果の全国への普及			
教育情報ナショナルセンター機能の整備		サイトの開設・運用・成果の全国への普及					

2．情報資産に対する様々な脅威

Ⅰ　外部要因

Ⅰ-1. 不正アクセス

正当なアクセス権を持たない者による、不正な手段を使った、内部の情報システムやコンピュータ（以下、情報システム）へのアクセス

例）個人情報や機密情報等の漏えい・改ざん・消去
学校の公式 Web ページの改ざん・消去
情報システムの破壊
なりすましによる犯罪行為（他への攻撃の踏み台など）

Ⅰ-2. 悪意ある来校者

悪意のある来校者による、情報システムへのアクセスや、机上等に置かれた機密情報や、ゴミ箱に捨てられた情報の盗難

例）個人情報や機密情報等の漏えい・改ざん・消去
情報システムの停止・破壊
情報システム機器や記録媒体の盗難
なりすましによる犯罪行為（他への攻撃の踏み台など）

Ⅰ-3. 盗聴

第三者によってネットワーク上を流れるメールやデータ等の通信内容の傍受

例）個人情報や機密情報等の漏えい

Ⅰ-4. 災害等

地震・落雷等の自然災害や停電、漏水、火災

例）情報システムの故障・停止・破壊
個人情報や機密情報等の消去

Ⅰ-5. コンピュータウイルスやワーム

情報システムがコンピュータウイルスやワームに感染

例）情報システムの停止・破壊
個人情報や機密情報等の漏えい・改ざん・消去
外部へのコンピュータウイルスの発信・感染被害の拡大

Ⅰ-6. DoS(Denial of Service)攻撃など

情報システムにかけられる不正な負荷や、セキュリティホールへの攻撃
例）情報システムの停止・破壊
個人情報や機密情報等の漏えい・改ざん・消去
学校あるいは職員になりすましての犯罪行為（他への攻撃の踏み台など）

Ⅱ　内部要因

Ⅱ-1. 生徒の故意や過失

掲示板への誹謗・中傷などの投稿、わいせつ画像や自殺の方法など不適切なサイトの閲覧や、校内のサーバへの不正アクセス
例）社会的影響（学校の信用失墜）
教育的影響
情報システムの破壊
サーバ内の情報に対しての漏えい・改ざん・消去
学校の公式 Web ページの改ざん・消去
なりすましによる犯罪行為（他への攻撃の踏み台など）

Ⅱ-2. 職員の故意や過失

規定やモラル等を無視した、個人情報や機密情報等の持ち出しや、情報システムの悪用。または、よくわからない、不得意であるなどの理由による無防備な使用や、わかっているつもりでの安易な判断による誤操作

例）個人情報や機密情報等の漏えい・改ざん・消去
学校の公式 Web ページの改ざん・消去
情報システムの停止・破壊
なりすましによる犯罪行為（他への攻撃の踏み台など）
情報システムの停止・破壊
個人情報や機密情報等の改ざん・消去

以上、様々な脅威が学校の情報システムに対して発生する可能性があり、場合によっては被害者ではなく加害者となるケースもあります。

3．脅威を引き起こす要因

なぜ、前項のような脅威が発生するのでしょうか。それは、情報資産に対するセキュリティ対策がなされていない、あるいは対策が不十分な部分（脆弱性）があるからです。具体的な脆弱性としては、次に挙げるものが考えられます。

Ⅰ　環境面

Ⅰ-1. 災害の影響

例）コンピュータが倒れやすい状態になっている
　　可燃物の近くにある
　　UPS がない
　　システムが二重化されていない

Ⅰ-2. 侵入や盗難

例）来校者が自由に出入りできる
　　記録媒体が施錠されたところに保管されていない
　　入退室管理がなされていない
　　不要の資料がシュレッダーにかけられていない

Ⅰ-3. 不正アクセス

例）不正に入手した、他人の ID やパスワードを無断で使用する。
　　セキュリティホールを攻撃してコンピュータに不正侵入する。

Ⅱ　組織面

Ⅱ-1. 管理者

例）管理や責任の所在がはっきりしていない
　　役割が明確でない

Ⅱ-2. セキュリティ教育や障害時対応訓練

例）セキュリティ研修会を実施していない
　　職員の意識が低い

Ⅱ-3. 報告や連絡体制

例）緊急時の体制が明確でない

Ⅲ　運用面

Ⅲ-1. 運用

例）定期的な監査をしていない
定期的なバックアップがない
規定が周知されていない

Ⅲ-2. 廃棄

例）媒体のライフサイクルに対する規定がない
個人情報や機密情報が再生可能な状態で捨てられている

Ⅲ-3. 機能

例）ロックアウト機能や個人認証機能などが設定されていない
暗号化されていない
アクセス権が設定されていない
パスワード管理が徹底していない

4．情報セキュリティ対策

セキュリティ対策には 4 つの段階と 3 つの側面があります。

Ⅰ　4 つの段階

・予　　防 ： セキュリティ問題の発生を未然に防ぐ対策
・発　　見 ： 不正アクセスやコンピュータウイルスの侵入をいち早く発見する
・極 小 化 ： 被害を最小限に抑え、広がらないようにする
・復　　旧 ： セキュリティ侵害から侵害前の状態に復旧させること

Ⅱ　3 つの側面

Ⅱ-1．物理面

コンピュータ室の隔離や災害対策、破壊対策などの物理面の対策

(1) 災害対策
①地震対策・設置場所・転倒防止
②水害対策・設置場所
③火災対策・出火を抑制（燃えやすい物は置かない、耐火性の素材を使用）
・出火の早期発見（火災報知器の設置）・延焼を防止する（防火壁）
・消化設備（コンピュータ機器用の消火機器により情報資産を保護）

(2) 人為的行為対策
①不正侵入対策・夜間・休日の警備体制（警備会社）
・厳重な施錠と認証技術の活用
②盗難対策・機器の机などへの固定・記録媒体の保管方法（施錠された場所で管理）
・機器の盗難を予期した対策（起動時認証）
・記録媒体の盗難を予期した対策（認証や暗号化）

(3) ハードウェア障害対策
・サーバの多重化・ディスクの多重化（RAID など）・データのバックアップ
・バックアップ電源の用意（UPS）

Ⅱ-2. 技術面

ファイアウォールやコンピュータウイルス対策ソフトウェア、OS のアップデートなどの技術面の対策

(1) **障害対策**

①システム障害対策・システムの高信頼化・資源管理（定期保守・点検の実施）
・障害の早期発見（システムの監視と状況の分析）
・システム障害時対応マニュアルの整備と訓練（障害対応手順）

②ネットワーク障害対策・ネットワークの監視
・ネットワーク障害時対応マニュアルの整備と訓練

(2) **人為行為対策**

①過失行為（誤操作）・誤操作を起こしにくい設計・ヘルプ機能の準備・認証機能
・データチェック・警告機能

②故意行為・暗号化技術・認証技術・アクセス管理技術・セキュリティ管理技術
・コンピュータウイルス対策
・コンピュータ犯罪やネットワーク犯罪の手口の研究

Ⅱ-3. 管理面

アクセス者の管理や、ユーザ ID やパスワードの管理、データの管理など、運用・管理上の対策

(1) **不正侵入対策**

・建物内部の区画（案内）を明示しない・入退室時の記録

(2)**機密契約管理対策**

・セキュリティ監査の実施

(3) **組織内部対策**

・セキュリティ教育の実施・カウンセリング実施（不平不満の解消など）
・マニュアルや規定の整備と徹底・セキュリティ管理者の設置と監視
・特定の担当者に権限が集中しないように配慮・ログの監査

5．情報セキュリティポリシー

Ⅰ　情報セキュリティポリシーの必要性

ネットワーク環境の活用に際して現在の情報資産（ネットウーク上を流通する情報や、コンピュータ及びネットウークなどの情報システム）を調査し、その情報資産の重要度や脆弱性とその脅威を把握・評価します（リスク分析）。それを行うことによって、適切なセキュリティ対策を構築することが可能となり、適切な方針（ポリシー）に基づくネットワーク運用が行えるようになります。

またこのセキュリティ対策によって、過剰な規制を緩和し、安全なネットワーク環境の活用が可能になってきます。

Ⅱ　情報セキュリティポリシーの意義

情報セキュリティポリシーとは、セキュリティのよりどころとして

・何から　　不正アクセス、データ漏洩・改ざん・破壊、コンピュータウイルス・ワーム等

・何　を　　機密情報、個人情報、生徒や職員のフライパシー等

・どのように　システム面、環境面、管理面等

守るのかを明確にし、限られた予算の中で、生徒や職員など利用者が安心して情報システムを活用できるように、セキュリティ対策を効果的に行う方針・基準です。

また情報セキュリティポリシーは策定することが目的ではなく、導入・教育・運用・監査・評価・見直しを重ねることによって、恒久的に情報セキュリティを維持することが目的です。

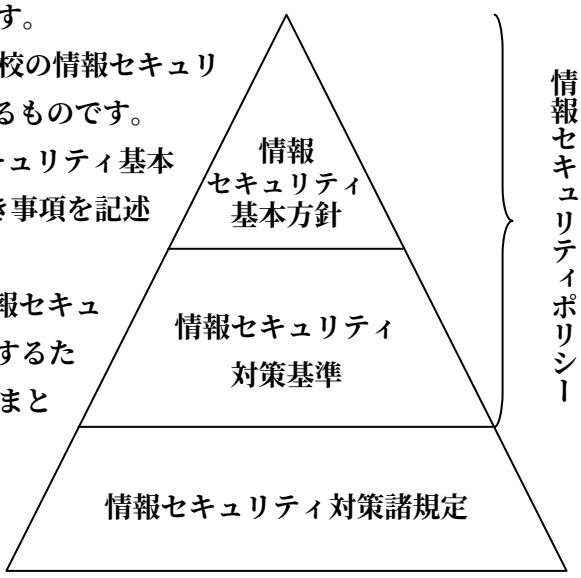
Ⅲ　情報セキュリティポリシーの構成

情報セキュリティポリシーは 3 つの階層に分けられます。

最上位に位置する「情報セキュリティ基本方針」は学校の情報セキュリティに関する方針で、学校内で守るべき情報を明確にするものです。

次の階層の「情報セキュリティ対策基準」は「情報セキュリティ基本方針」を受け、学校内の情報資産の項目ごとに遵守すべき事項を記述したものです。

最後の階層の「情報セキュリティ対策諸規定」は「情報セキュリティ対策基準」を受け、情報セキュリティ対策を実施するために、利用者（対象者）ごとに具体的な内容に編集し、まとめたものです。

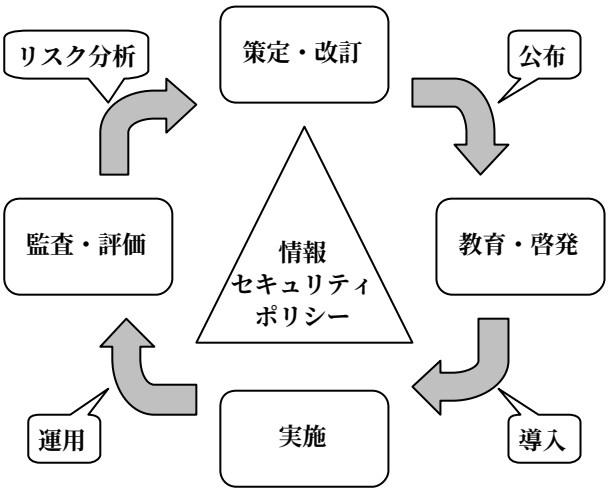


Ⅳ　情報セキュリティポリシーの運用

目標とする情報セキュリティレベルを達成するためには、導入時に研修会を実施するなど、情報セキュリティポリシーを周知することが重要となります。

また、情報セキュリティレベルを維持していくには以下のような情報セキュリティポリシーの実施サイクルを恒久的に続けていくことが必要とされています。

・策　　定：現在の情報資産に関するセキュリティを考え、策定し利用者全員に公布します。
・教育・啓発：利用者の教育と啓発が大切で必要不可欠です。情報主任が研修会を企画します。
・実　　施：情報セキュリティポリシーを実施・運用します。
・監査・評価：運用していく中で、監査・評価（監査役が実施）を必ず行います。
・改　　訂：最新のセキュリティ技術の情報を収集し、リスク分析を再度行うことによって、その状況の最前の情報セキュリティ対策を見直し、情報セキュリティポリシーを改訂します（恒常的なものではなく、運用サイクルの中で改訂し更新していきます）。



6．情報セキュリティ対策導入事例

Ⅰ　「教育の情報化」～鍵は校内 LAN の構築と運営

Ⅰ-1　ネットワーク事始め

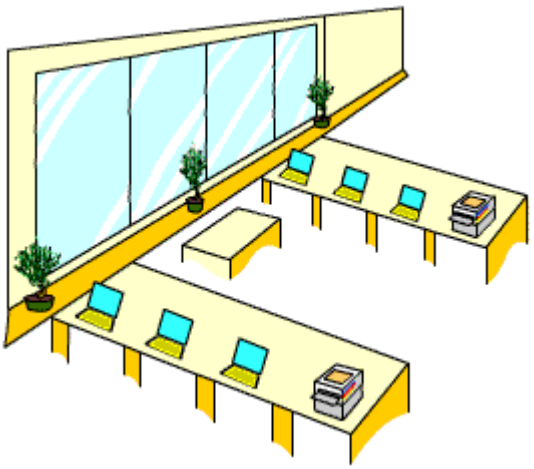
コンピュータなど、IT 機器があまり活用されていない学校で情報化を進めるためには、“ IT を活用して何が出来るのか ” ということを多くの職員に見てもらうことが大切だと思いました。

私たちはまず、コンピュータを使い勝手の良い場所に設置することから始めました。次に成績処理プログラムの作成・コンピュータ研修会の実施など、いろいろな取り組みをしてきました。最初は少人数だった輪も徐々に広がり、多くの人の理解や協力が得られるようになりました。

中でも LAN を活用することで、校務の効率化が図れることをみなさんが理解してくれたことで、本校の情報化は一気に進んだように思います。

Ⅰ-2　校内 LAN の校務活用

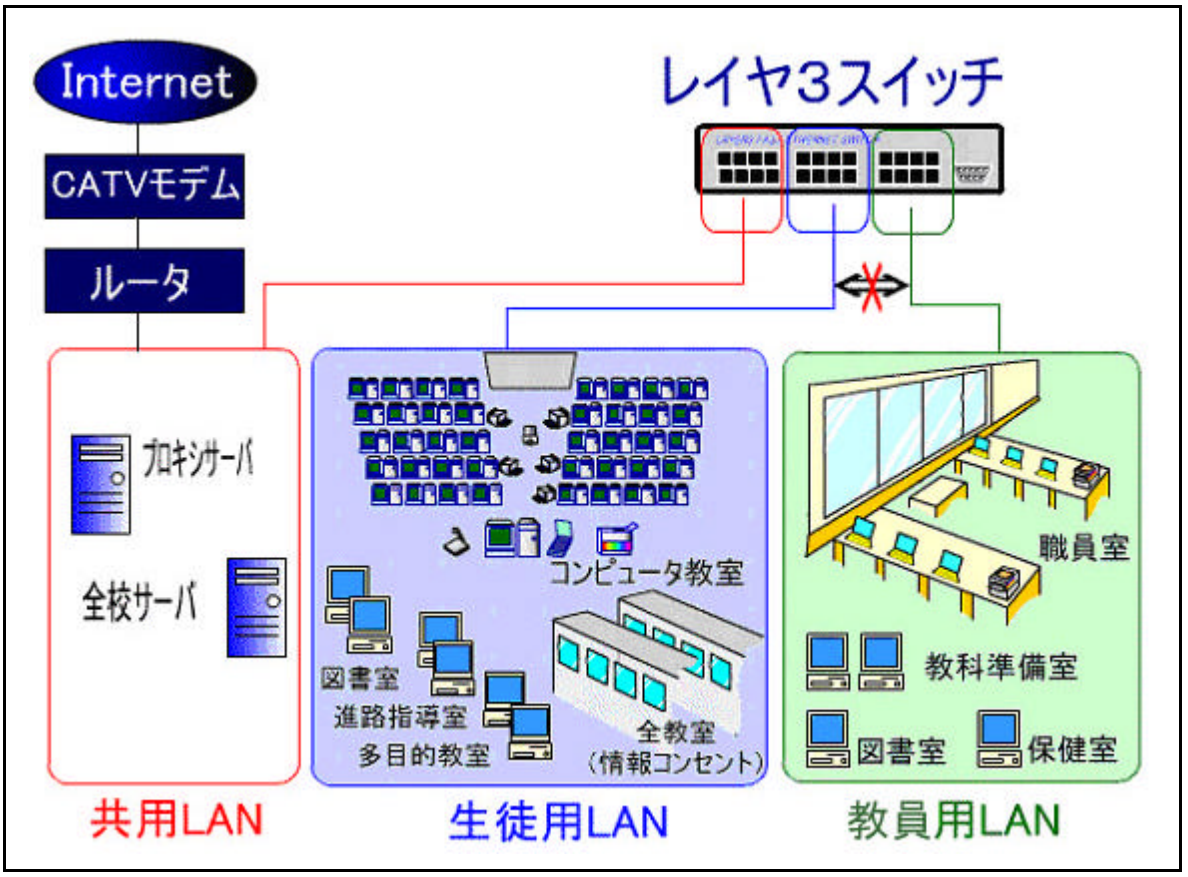
○文書ファイルは共有化し、ペーパーレスに向かっています。
○メールの活用で放課後の会議を減らしています。
○プリンタの共有化で予算やスペースの確保を図っています。
○インターネットで教材研究や他校との連携を行っています。



など、校内 LAN の活用により、校務が効率的に処理されるようになりつつあります。

Ⅱ　ネットワーク全体構成とセキュリティ確保の基本事項

Ⅱ-1　ネットワーク構成概念図



Ⅱ-2　全体構成とセキュリティ確保について

便利な LAN ですが、セキュリティ確保は最重要課題です。本校では次のように運営しています。

【全体構成】（詳細はⅡへ）

- 生徒の LAN と教員の LAN を分け、通信できないようにします。
- インターネット回線は、生徒用 LAN と教員用 LAN とで共有します。
- レイヤ 3 スイッチで LAN 間の通信を制御しています。

【コンピュータウイルス対策】（詳細はⅢへ）

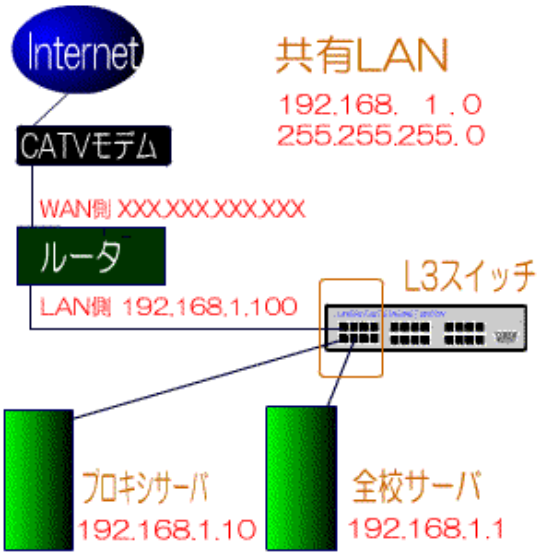
- コンピュータウイルス対策用サーバを用意し、校内すべてのコンピュータを一元管理しています。

【内部的な脅威に対して】（詳細はⅣへ）

- 内部的な脅威が発生しないよう定期的に教員のセキュリティ研修会を実施しています。
- LAN には管理者が許可したマシン以外は接続できないようにしています。
  （MAC アドレスセキュリティ）

Ⅲ　準備室は立入り禁止～ネットワークの要はセキュリティの要～

Ⅲ-1　共有の LAN（192.168.1.0/24）



コンピュータ準備室には共有の LAN に置くサーバ群や中継機器を設置します。
ネットワークの核となるところだけに生徒の出入りは禁止し、教員も管理者以外は使うことのないよう、機材などは施錠できる場所に置きます。

Ⅲ-2　サーバ設置の基本事項と日常のメンテナンス

本校では情報部所属の教員 3 名が管理者権限のパスワードを使いサーバの設定を行っています。年度当初のユーザアカウント作成から日常のメンテナンスまで、表には出ないけれども情報化を支える重要な仕事がたくさんあります。また、ネットワークの不具合や対処方法は必ず記録を残します。

【サーバ設置の基本事項】
- 利用できる総電源容量の確認
- データのバックアップ体制
- システムのバックアップ体制
- 停電対策としての UPS
- 物理的な地震対策/盗難対策

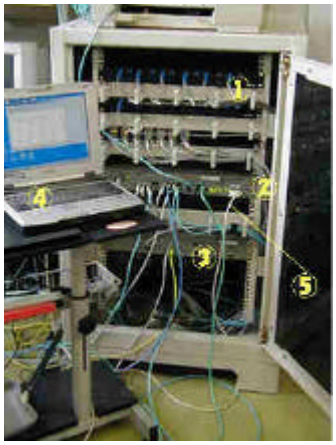
【日常的なメンテナンス】
- ユーザアカウント管理
- データ・システムのバックアップ
- 利用状況確認とログの監視
- コンピュータウイルス被害状況確認
- ウイルス対策ソフトウェアのパターンファイルのアップデート
- OS のセキュリティアップデート

Ⅲ-3　各種サーバの役割

【全校サーバの役割】
- コンピュータウイルス対策（Ⅲ-4 へ）
- コンテンツフィルタ
- ログの管理
- 利用サービスや接続台数などの規制

【プロキシサーバの役割】
- インターネット接続

Ⅲ-4　ネットワーク中継機器



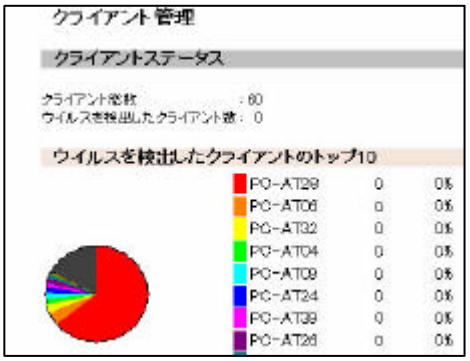
【ネットワーク中継機器】
①光ケーブルコンバータ
②レイヤ 3 スイッチ
③ギガビットレイヤ 2 スイッチ
④コンソールとして利用する PC
⑤PC とレイヤ 3 を繋ぐ RS-232C ケーブル

ネットワークの要はすべてコンピュータ準備室にあるこのラックの中に収まっています。
ここから信号は光ファイバケーブルを通って各教室の情報コンセントまで到達しているのです。
言わば校内 LAN の要にあたるわけですが、中でも②レイヤ 3 スイッチは LAN 間の通信を制御するセキュリティ上最も重要な機器と言えます。

この機器は RS-232C ケーブルを接続した他のパソコンからログインして中にあるファイルを書き換えることで、設定をしていきます。

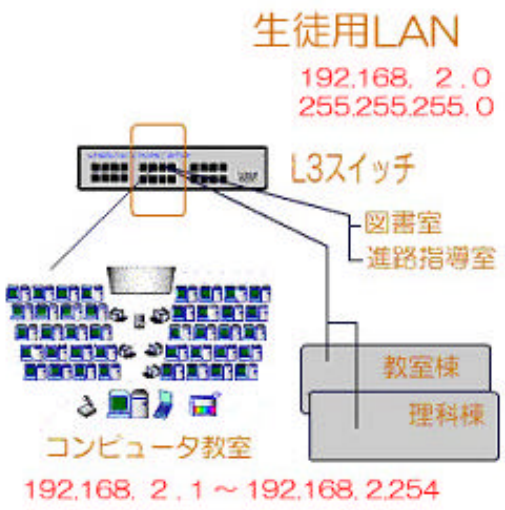
Ⅲ-4　コンピュータウイルス対策は集中管理

コンピュータウイルス対策ソフトは学校向けのパッケージを使っています。まず全校サーバにインストールし、そこから校内すべてのパソコンにインストールしました。
これによってパターンファイルの更新や被害状況の確認など全校レベルでの集中管理が可能になりました。管理・インストールともに Web ベースで簡単に行うことができます。



Ⅳ　生徒には自由に使える環境を

Ⅳ-1　生徒の LAN（192.168.2.0/24）



コンピュータ教室はじめ生徒用に設置したコンピュータは出来るだけ自由に使わせてあげたいものです。壊される、設定が変えられる、盗まれる等不安材料もありますが、本校では入学時のガイダンスを始め、利用に関する指導を十分に行い、また、生徒を信じるというスタンスで運営しています。

【生徒の使用可能 PC】
- コンピュータ教室 42 台
- 授業用ノートパソコン 2 台
- 多目的教室 4 台
- 図書室 2 台
- 進路指導室 1 台

Ⅳ-2　コンピュータ教室の利用に関して

次のようなルールや常識が守れる生徒には放課後のコンピュータ教室を開放しています。

- コンピュータ教室利用規定の内容を理解していること。
- 授業担当や担任などが発行する「利用許可証」を有していること。
- 利用目的を明らかにしていること。
- 利用時間（17 時まで）や禁止事項などルールを守れること。
- 主な禁止事項

（飲食物持込／チャット／ゲーム／ソフトの持込やインストール／ファイルのダウンロード）

管理：情報部・情報科

Ⅳ-3　情報コンセント（全教室）の利用に関して

授業用ノートパソコンとプロジェクタ･スクリーンを運べば､情報コンセントを使ってネットワークを活用した授業も可能。

管理：情報部・情報科

Ⅳ-4　特別教室の利用に関して

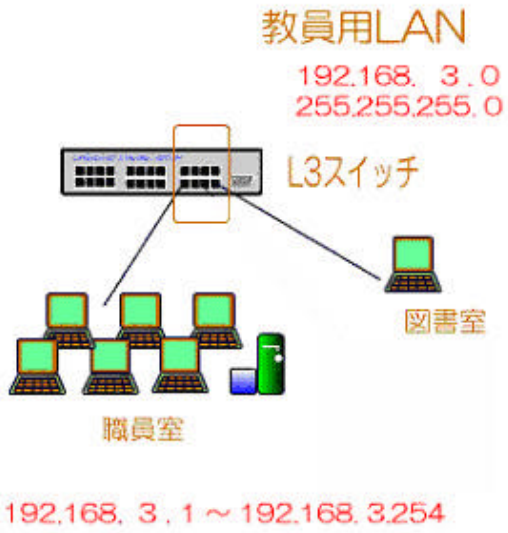
■多目的教室
教室棟の多目的教室に中古パソコン 4 台を設置。
総合学習はじめ調べ学習などに利用可能。　**管理：情報部**

■図書室
蔵書管理システムと合わせ各検索や閲覧が可能。
管理：司書教諭

■進路指導室
進路指導室に中古パソコンを設置。進路先の Web ページなど見ながら教員と相談できる。
管理：進路指導部

Ⅴ　教員には理解と研修を

Ⅴ-1　教員の LAN（192.168.3.0/24）



校務の中ですべての教員がコンピュータを使うわけですから、利便性だけでなく、危険性も知ってもらう必要があります。本校では定期的に研修会を実施するなどして、ネットワーク管理の重要性とセキュリティ確保のための基本事項を理解してくれるよう働きかけています。

【教員の使用 PC】
- 教員用ファイルサーバ
- 共用 PC 5 台
- 個人 PC 15 台

Ⅴ-2　教員研修

年度の初めに新着任者を交えて、ネットワークの利便用と危険性に関する研修会を実施しています。

【内　容】
- 学校のネットワーク構成
- LAN への接続設定
- 基本的なトラブルへの対処法
- コンピュータウイルス対策
- セキュリティに関する一般論

Ⅴ-3　個人のパソコンをどうする？

個人のパソコンをネットワークに接続する場合、以下の手順を踏んで接続を可能にしています。中でも MAC アドレスセキュリティは管理の手間はかかりますが、セキュリティを維持する上でやむを得ないと判断しています。

【LAN 接続の手順】
- 研修会に参加しましたか？
- 意識／知識チェックシートを作成しましたか？
- 利用申込書を作成しましたか？

⇒

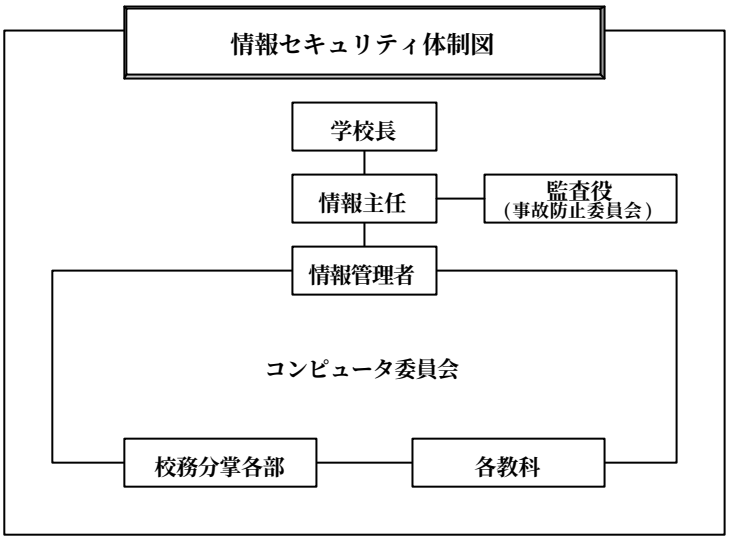
- MAC アドレスをレイヤ 3 スイッチへ登録
- 利用可能 IP アドレスを教員に配布

情報セキュリティポリシー策定事例

Ⅰ　策定前の準備

Ⅰ-1. 情報セキュリティ対策プロジェクト組織を発足

①学校長が情報セキュリティ対策プロジェクトを設置
②情報セキュリティについての情報収集
③情報セキュリティポリシーの作成・運用を方針とし準備
④情報セキュリティ管理体制の確立。（右図参照）



Ⅰ-2. リスク分析

①現在の情報セキュリティシステムと対策の把握
②「情報資産」に対する「脅威」、「脆弱性」の調査・分析、及び評価
③リスクの評価・リスクコントロールの検討

Ⅱ　情報セキュリティポリシーの策定

Ⅱ-1. 情報セキュリティ基本方針の策定

①趣　旨（目的）
②構成と位置つけ
③適用範囲
④適用者
⑤体　制
⑥公開対象者
⑦公開
⑧情報セキュリティ対策の運用
⑨情報セキュリティ侵害時の対応
⑩基本用語の定義

Ⅱ-2. 情報セキュリティ対策基準の策定

①個人情報の取り扱いに関する基準
②コンピュータ等の取り扱いに関する基準
③ソフトウェアの取り扱いに関する基準
④アカウント管理に関する基準
⑤パスウード管理に関する基準
⑥サーバの運用に関する基準
⑦ネットワークの運用に関する基準
⑧ネットウークの利用に関する基準
⑨Web サービスの利用に関する基準
⑩電子メールサービスの利用に関する基準
⑪コンピュータウイルス対策に関する基準
⑫システム維持・監視に関する基準
⑬不測事態発生時の対応に関する基準
⑭監査に関する基準
以上の基準を以下の項目で策定
・目　　的
・対象者と公開対象者
・遵守事項
・不測事態発生時

Ⅲ　情報セキュリティシステムの実装

Ⅲ-1. 情報セキュリティシステムの設計

①ファイルサーバを構築（教員全員にアカウントを配布し、アクセス制御を行う）。
②サーバ一式、情報処理室整備の為の予算を確保。

Ⅲ-1. 情報セキュリティシステムの実装およびテスト

①NT サーバを構築・情報処理室の整備、ルータの再設定、ファイアウォールの設定確認、等
②アカウント登録、アクセス権限の登録、他
③情報セキュリティシステムの運用・管理
④情報セキュリティシステムの分析

Ⅳ　情報セキュリティ対策諸規程を策定

Ⅳ-1. 情報セキュリティ対策諸規程を策定

①情報セキュリティ対策基準を元に、「教員対象」「生徒対象」の諸規程を策定

Ⅳ-2. 情報セキュリティポリシーの見直し

①情報セキュリティシステムの運用・管理・分析により、情報セキュリティポリシーを見直し

用語集

CATV モデム

ケーブルテレビの回線を使ってインターネットに接続するための装置。

DoS 攻撃

Denial of Services の略。ネットワークを通じた攻撃の一つ。相手のコンピュータやルータなどに不正なデータを送信して使用不能に陥らせたり、トラフィックを増大させたりして相手のネットワークを麻痺させる攻撃。

IP アドレス

インターネットの標準プロトコルである TCP/IP プロトコルにおいて、ネットワーク上のコンピュータを一意に識別するために、32 ビットの 2 進数で表したアドレス。ただし、2 進数は人間にはわかりにくいので、通常は 8 ビットずつ.（ドット）で区切った 10 進数表記を用い、192.168.1.15 といった形式で表される。IP は Internet Protocol の略。LAN にコンピュータを接続するために、パソコンでは右図のような項目を設定する必要がある。

LAN

Local Area Network の略。学校内などの限定された場所でのコンピュータネットワーク。

MAC アドレス

Ethernet カードなどに固有で付けられている 48 ビットの 2 進数で表したアドレス。ただし、2 進数は人間にはわかりにくいので、通常は 8 ビットずつ：（コロン）で区切った 16 進数表記を用い、00:11:22:AA:BB:CC といった形式で表される。MAC は Media Access Control の略。同じ MAC アドレスを持つ Ethernet アダプタは本来存在せず、すべて異なるアドレスが割り当てられている。変更が可能な IP アドレスに比べて、MAC アドレスは変更不可能なので、MAC アドレスで接続制限をかけるとセキュリティは高くなる。

OECD

経済協力開発機構（Organisation for Economic Co-operation and Development）

RAID

Redundant Array of Independent Disks の略。複数のハードディスクを並べて 1 台のディスクのように使用し、信頼性や処理速度を高める方法。ディスクアレイともいう。

UPS

Uninterruptible Power Supply（無停電電源装置）の略。バックアップ用の電池（または発電機）を内部に持ち、停電時でもシステムをそのまま稼働できるようにする装置。小容量のものでは、システムを数分稼働できる程度の容量の電池を持ち、この間にシステムを安全にシャットダウンさせられるようにする。一方、大容量のものでは、内部に発電機を持ち、システムを数日にわたって稼働できるものもある。

アカウント

コンピュータやネットワーク上の資源を利用できる権利のこと、または利用する際に必要な ID のこと。メールアカウントやファイルサーバのアカウントなどがある。通常、ユーザはパスワードを設定し、本人以外の不正な利用を防止する。

アクセス権限

ネットワーク上にあるファイルなどのデータを読んだり利用したりするための権利。段階的に制限を設けることができる。たとえば、重要なファイルを特定のユーザにしか利用できないように規制することで、権利のないユーザに機密ファイルを見られたり、削除されたりしないようにする。

アクセス制御

各ユーザに対してあらかじめ許可された以上のアクセスを禁止するための技術的措置。

暗号化

情報の表現を組み替えて第三者が利用できないようにすること。ネットワーク上でのセキュリティ保護などで重要な役割をもつ。暗号化された文を暗号文といい、暗号化されずに、そのままの状態にあるデータを平文という。データを暗号化せず、平文でやり取りした場合、データの内容を簡単に覗き見ることができる。

コンティンジェンシプラン

緊急事態が発生した際の業務の復旧や継続についての対応方針、対応要領をあらかじめ定めた総合的な計画のこと(緊急時対応計画)。

コンテンツフィルタ

教育・倫理上の問題や行動規範の問題を背景として、好ましくない Web サイトなどが閲覧できないように、クライアントもしくは内部サーバで動作するソフトウェアによって、閲覧内容に一定の規制をかける仕組み。

コンピュータウイルス

自己伝染機能・潜伏機能・発病機能のいずれかをもつ加害プログラム。広義の定義と狭義の定義があり、広義の定義では「ワーム」や「トロイの木馬」を含むが、狭義の定義ではこれらを含まない。

脆弱性

システム上のセキュリティに関する欠陥や、企業・組織・個人に対する行動規範の不徹底や未整備など。

セキュリティホール

ソフトウェアの設計ミスなどによって生じた、システムのセキュリティ上の弱点。セキュリティホールを放置しておくと、悪意のあるユーザに不正にコンピュータを操作されてしまう可能性がある。ソフトウェアにセキュリティホールが発見された場合は、対策のための修正プログラムが無償で配布されるので、該当するソフトウェアのユーザは、出来る限り早く修正プログラムをインストールする必要がある。

チャット

コンピュータネットワークを通じてリアルタイムに文字ベースの会話を行なうシステム。1 対 1 で行なうものや、同時に多人数が参加して行なうものがある。

トロイの木馬

善意のユーザが期待する動作とは異なる動作をする悪意あるプログラム。例えば、ユーザが入力するパスワードを取得するプログラムなどがある。トロイの木馬は他のファイルに寄生したりはせず、自分自身での増殖活動も行わない。

トレードオフ

複数の要素が関連を持ち、ひとつの要素を改善すると、他の要素が悪化するような状態。

なりすまし

他人のユーザ ID やパスワードを盗用し、その人のふりをしてネットワーク上で活動すること。本来その人しか見ることができない機密情報を、その人のふりをして盗み出したりする。

パターンファイル

コンピュータウイルスに感染したファイルや、ネットワーク上で自己複製を繰り返すワームプログラムの特徴を収録したファイル。ウイルス対策ソフトウェアがコンピュータウイルスやワームを検出するのに使う。「ウイルス定義ファイル」などとも呼ばれる。ウイルス対策ソフトウェアごとに専用のパターンファイルが必要である。

次々と現れる新種のウイルスに対応するため、各ソフトメーカーは頻繁に自社ソフト向けの新しいパターンファイルをインターネットなどで配布している。

ファイアウォール

インターネットから LAN への不法な侵入を防ぐ目的で、インターネットとやり取りできるコンピュータを制限したり、LAN から利用できるインターネットのサービスを制限したりする。

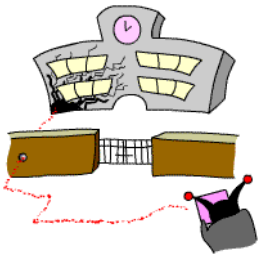
ファイルサーバ

ネットワーク上で他のマシンとデータをやり取りするために、ファイルを蓄積しておく専用機。

不正アクセス

あるコンピュータへの正規のアクセス権を持たない人が、ソフトウェアの不具合などを悪用してアクセス権を取得し、不正にコンピュータを利用する、あるいは試みること。

代表的な不正アクセスには、セキュリティホールを悪用してファイルを盗み見たり削除・改変したりする行為や、盗聴や総当たり攻撃によるパスワード窃取、メールサーバを悪用した迷惑メールのばらまきなどがある。



踏み台

セキュリティ対策の甘いサイトに不正侵入し、他サイトの攻撃の中継サイトとして利用すること。一般的な不正アクセスでは、攻撃元の特定を困難にするため、複数のサイトを踏み台にするのが普通。

プロキシサーバ

ファイアウォールなどの内側のネットワークから、インターネット接続を行う際、セキュリティ確保と高速アクセスを実現するために設置されるサーバ。プロキシとは「代理」の意味。

プロトコル

コンピュータ同士のデータ通信の際の規約や約束事。インターネットでは TCP/IP プロトコルが標準プロトコルとして普及している。

ルータ

レイヤ 3 スイッチ

レイヤ 2 スイッチ

ネットワーク中継機器。一般に、ルータとレイヤ 3 スイッチは IP アドレスを使い、レイヤ 2 スイッチは MAC アドレスを使って中継を行う。必要によって、通過させるデータやプロトコルの種類を制限できるものもある。

ログ

コンピュータの利用状況やデータ通信の記録を取ること。また、その記録。操作やデータの送受信が行われた日時や行われた操作の内容などが記録される。

ロックアウト機能

一定回数以上ログオン操作に失敗したとき、そこで使われたアカウントを一定時間無効にしてしまう機能。

ワーム

通常のコンピュータウイルスは感染するときに、媒介となるファイルが必要になるが、そのようなファイルを必要とせずに、自力で多くのパソコンに感染するコンピュータウイルスのことをワームと呼ぶ。ワームは自分自身の力でネットワークを経由して、パソコンの間を移動し、他のパソコンに感染していく。

参考文献

このハンドブックを作成する上で、以下の文献を参考にさせて頂きました。

Web ページ

教育の情報化

バーチャルエージェンシーについて

http://www.kantei.go.jp/jp/it/vragency/991221saisyuu.html **（首相官邸）**

ミレニアム・プロジェクトについて

http://www.kantei.go.jp/jp/mille/index.html **（首相官邸）**

高度情報通信ネットワーク社会推進戦略本部

http://www.kantei.go.jp/jp/singi/it2/index.html **（首相官邸）**

情報化への対応

http://www.mext.go.jp/a_menu/shotou/zyouhou/index.htm **（文部科学省）**

法律関係

個人情報の保護に関する法律について

http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/ **（首相官邸）**

ＩＴ関連法律リンク集

http://www.kantei.go.jp/jp/singi/it2/hourei/link.html **（首相官邸）**

成立した主要なサイバー関連立法（2003 年 2 月現在）

http://www.law.co.jp/link/cyberlawjp.htm **（英知法律事務所）**

わが国における情報ネットワーク関連判例の動向

http://www.law.co.jp/cases/netcase.htm **（英知法律事務所）**

用語集

IT 用語辞典 e-Words

http://e-words.jp/**（株式会社インセプト）**

アスキーデジタル用語辞典

http://yougo.ascii24.com/**（株式会社アスキー）**

ネットワークセキュリティ関連用語集

http://www.ipa.go.jp/security/glossary/glossary.html**（情報処理振興事業協会）**

セキュリティ全般

IPA **セキュリティセンター**

http://www.ipa.go.jp/security/ **（情報処理振興事業協会）**

JPCERT **コーディネーションセンター**

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

日本ネットワークセキュリティ協会

http://www.jnsa.org/

国民のための情報セキュリティサイト

http://www.soumu.go.jp/joho_tsusin/security/index.htm **（総務省）**

情報セキュリティマネジメントシステム(ISMS)適合性評価制度

http://www.isms.jipdec.jp/ **（財団法人日本情報処理開発協会）**

情報セキュリティに関する政策、緊急情報

http://www.meti.go.jp/policy/netsecurity/ **（経済産業省）**

2002 **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/active1a.html **（日本ネットワークセキュリティ協会）**

@police

http://www.cyberpolice.go.jp/ **（警察庁）**

ハイテク犯罪対策

http://www.npa.go.jp/hightech/ **（警察庁）**

情報通信白書

http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm **（総務省）**

OECD **情報セキュリティガイドラインに関する調査**

http://www.ipa.go.jp/security/fy13/report/oecd-guideline/oecd-guideline.pdf**（情報処理振興事業協会）**

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セキュリティ文化の普及に向けて

http://www.meti.go.jp/policy/netsecurity/oecd2002.htm**（経済産業省）**

書籍

田渕治樹　2003　**「ISMS 構築のための情報セキュリティポリシーとリスク管理」オーム社**

田渕治樹　2000　**「国際セキュリティ標準　ISO/IEC17799 入門」オーム社**

相戸浩志　2003　**「図解入門 よくわかる最新 情報セキュリティ技術の基本と仕組み」秀和システム**

中野　明　2003　**「図解入門 よくわかる最新 ISMS Ver.2 の基本と仕組み」秀和システム**

森　慎一・塩谷　幸治・新川　晃太郎

2000　**「セキュリティポリシーの考え方～BS7799 照準～」SCC**

調査研究協力員

大和市立文ヶ岡小学校	山口　亮二
大磯町立大磯中学校	伊藤　努
県立高浜高等学校	間辺　広樹
県立新磯高等学校	大河原広行