神奈川県

KANAGAWA

学校情報セキュリティガイド 2005

平成 17 年 3 月

神奈川県立総合教育センター

はじめに

近年の急速な情報通信ネットワークの普及に伴い、教育を取り巻く環境も大きく変化してきています。教育用コンピュータの配備、県立学校同士をつなぐ教育委員会ネットワークの本格稼働といったハード面の整備、学校教育用コンテンツの開発や教育情報ナショナルセンター機能の強化といったソフト面の整備が進むとともに、各教科等の授業で、先生がプレゼンテーションしたり、子どもたちがコンピュータやインターネットで調べたり、交流したりすることによって、「わかる授業」や「魅力ある授業」を実現することが求められております。

また、常時接続化、広帯域化されたインターネットの急速な普及により、文字情報はもちろんのこと、動画や音声なども含んださまざまな情報を誰もが簡単に発信したり受信したりできるようになり、情報通信ネットワークが情報収集以外にも、他校との交流や、情報共有などに非常に大きな役割を果たしてきております。それに伴い、各学校において、情報通信ネットワークを授業や校務へ積極的に活用することが求められる一方で、情報セキュリティの確保や情報モラルの育成などの新たな問題や課題が生じ、生徒がかかわる事件等が新聞やテレビなどで取り上げられたりするようになりました。学校においても、情報漏えいなどのリスクを低減することはもちろんのこと、単に「守る」という側面だけでなく、「利用する」という側面に配慮したシステムの安全な運用が必要とされております。

本冊子は、情報セキュリティについての理解と、その運用に向けた取組について、具体的な事例を含めてまとめられております。各学校において情報システム運営上の一助として活用いただけることを願っております。

平成17年３月

神奈川県立総合教育センター

所　長　　清　水　進　一

目　次

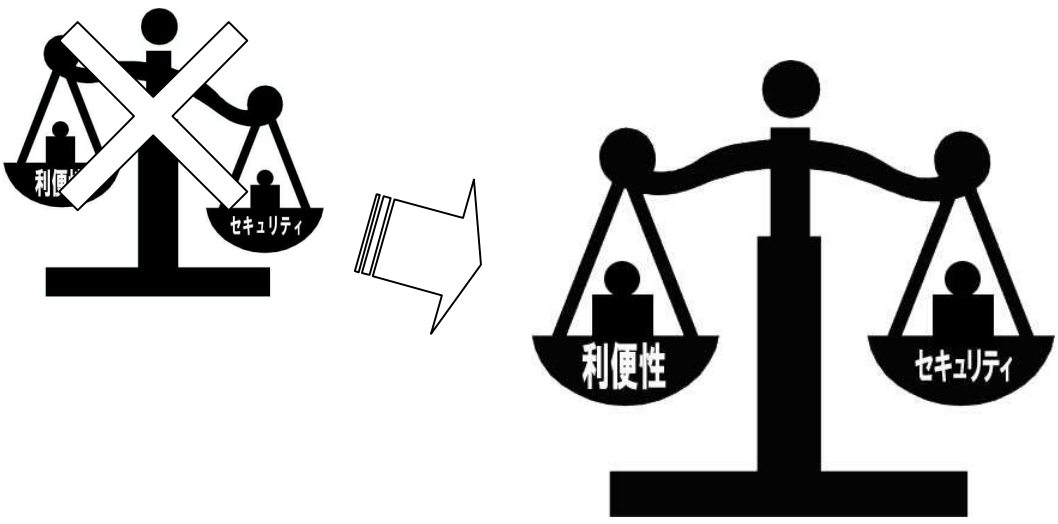
§1 教育の情報化と情報セキュリティ

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』」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」などを活用した「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、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。



情報漏えい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、もう少し詳しく説明すると次のようになります。

まず、機密性についてですが、これは、情報を取り扱うことができる者と、その利用範囲を明確にし、権限のない者による不正な利用を防ぐということになります。例えば、重要なデータが保存されているサーバへアクセスするためのパスワードが盗難にあってしまうと、サーバの正規利用者以外に、悪意ある第三者が正規利用者になりすましてサーバへアクセスすることが可能になってしまい、重要なデータが盗み出されてしまいます。この様な状況では、このサーバは機密性が保たれていないということになります。

次に、完全性についてですが、これは情報が作成されてから削除されるまでの間に、欠落や重複、改ざん等のトラブルが発生することなく、正しく処理されるようにすることということです。例えば、電子メールは、その性質上、送信してから受信するまでの間に、第三者に内容を書き換えられる可能性があります。この場合、電子メールで送信される情報は、完全性が担保されていないと言うことができます。

最後に、可用性ですが、情報システムに格納されている情報を利用したい時にいつでも利用できる状態にしておくという意味になります。可用性は、一般になじみのない言葉ですが、IT 関連用語としてはシステムの壊れにくさを表す言葉として使われます。ここでは、もう少し意味を広げて、いつでも安心して使える情報システムを指す言葉として使います。つまり、障害の発生頻度が低く、いつでも簡単に情報が取り出せる状態の情報システムは可用性が高いということができます。

情報セキュリティの 3 つの要素について、もう少し簡単に言い換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。

情報セキュリティ対策を行う上で重要なことは、場当たり的な対応ではなく、組織として統一された方針や連絡体制のもとに対応していくことです。情報セキュリティ対策は、計画・策定、導入・実施、運用・監視、評価・見直しの四つのステップを繰り返しながら、継続的に推進していくことが必要となります。

§2 情報資産に対する様々な脅威

Ⅰ　外部要因

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）

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）

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

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

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

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

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）

2 職員の故意や過失

運用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）

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

1 災害の影響

例）コンピュータや周辺機器が倒れやすい状態になっている
　　可燃物の近くにある
　　UPS（無停電電源装置）がない
　　システムが二重化されていない

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

3 不正アクセス

例）不正に入手した、他人の ID やパスワードの無断使用
　　セキュリティホールを攻撃したコンピュータへの不正侵入

Ⅱ　組織面

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

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

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

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
運用規定が周知されていない

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

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。ここでは、3 つの側面から見たセキュリティ対策について、詳しく解説します。

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侵入の早期発見
・極 小 化 ： 被害を最小限に抑え、広がらないようにすること
・復　　旧 ： セキュリティ侵害から侵害前の状態への復旧

Ⅱ　3 つの側面

1 物理面

○ハードウェアの盗難・持ち出し

・セキュリティワイヤーによるパソコンの固定



・鍵のかかるロッカーへの保管

○ハードウェアの転倒・落下

・粘着固定マットなどでパソコンを固定する
・情報を定期的にバックアップする

○廃棄パソコンや廃棄メディア

フロッピーディスクやハードディスクに記録されたデータは、「削除処理」や再フォーマットをすることにより一見消去したように見えますが、OS のもとで「呼出処理」が出来ないだけで、実データは残っている状態にあります。特殊なソフトウェアを使用することで、このデータを呼び出すことが技術的に可能な場合があります。このため悪意のある第三者により重要なデータが読みとられ、予期しない用途に利用される恐れがあります。これを避けるため、

➢廃棄パソコンや廃棄メディアの記録媒体を物理的に破壊する
➢ハードディスク消去サービスやハードディスク消去ツールなどを利用する

などの対策が考えられます。

2 技術面

○コンピュータウイルス

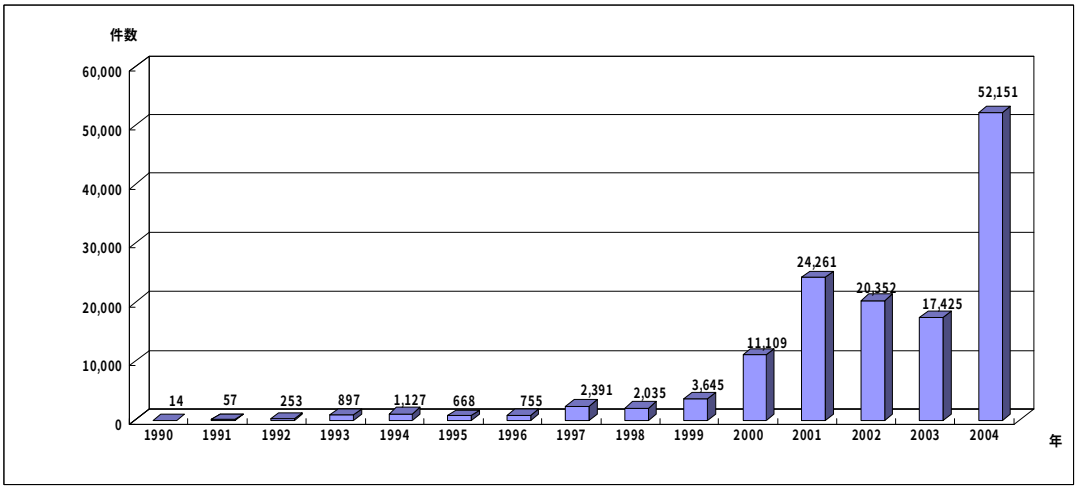
・コンピュータウイルスとは

コンピュータウイルスとは、心ない人によって意図的に作成された悪質な加害プログラムのことです。使う人の意思とは関係なく、さまざまな悪事を行います。その動作が一般のウイルスに似ているため、コンピュータウイルスと呼ばれるようになりました。

・コンピュータウイルス届出件数の推移（独立行政法人 情報処理推進機構：IPA）

IPA の調査によると、コンピュータウイルスは、2001 年を境に減少する傾向にありましたが、2004 年は年間で 52,151 件と、前年(2003 年)の 17,425 件から約 3 倍もの増加となり、史上最悪の件数となりました。しかしながら、実際にパソコンに感染した(実害があった)ケースは 2000 年から減少傾向にあり、2004 年は届け出件数に対して、わずか 1% にとどまっています。

参考 コンピュータウイルス届出件数の推移（独立行政法人 情報処理推進機構）



・コンピュータウイルスの活動

コンピュータウイルスは次のような活動を行います。

➢侵入：外部よりパソコンに入り込むこと

➢感染：ユーザが意図しない動作をコンピュータ上で行うこと

➢潜伏：PC 内にあってまだ発病していない状態

➢発病：発病条件を満たし、破壊活動を開始すること

・コンピュータウイルスの感染経路

コンピュータウイルスは主に次の経路で感染します。

➢電子メールに添付されたファイルを開くことによる感染

OS にセキュリティホールがあると、開かなくても自動的に添付ファイルを実行してしまう場合もあるので、注意が必要です。

➢Web ページからのダウンロードによる感染

便利なツールやゲームを装っていることもあるので注意が必要です。また、OS にセキュリティホールがあると、Web ページを開いただけで、自動的にファイルをダウンロードしてウイルスファイルを実行してしまうという、より悪質なものもあります。

➢インターネットや LAN 等からの直接的な感染

OS が使用するプロトコルの RPC（リモート プロシージャ コール）などに存在するセキュリティホールを悪用したりして、直接コンピュータに侵入します。

➢その他

フロッピーディスクや CD-R などのメディアを介した感染や、インターネットチャットメッセンジャー（MSN メッセンジャー等）やピアツーピア型のインターネットファイル共有システム（Kazaa 等）などを介した感染などが考えられます。

・コンピュータウイルスの例

実際のコンピュータウイルスである、Netsky、Nimda を例に、コンピュータウイルスの具体的な活動内容を示します。

➢Netsky

主な感染経路

メールの添付ファイル

主な活動

メール送信活動：

感染したコンピュータ内で、メールアドレスを収集して、取得できたアドレス宛にウイルスメールを送信します。また、差出人メールアドレスは詐称されますので、知人のメールアドレスであるということだけで添付ファイルを開くことは危険です。また、差出人メールアドレスの方のコンピュータはウイルスに感染していない場合も推測されますので、むやみにウイルスメールの差出人メールアドレスへ苦情のメールを送付することは控えるべきです。

Web サイトへのサービス妨害

特定の時間になると、特定の Web サイトへデータを大量に送信し、Web サイトのサービスを妨害します。

➢Nimda

主な感染経路

Web の閲覧時

インターネットや LAN 等からの直接的な感染

メールの添付ファイル

インターネットファイル共有システム

主な活動

メール送信活動：

メーラーのアドレス帳に登録されているアドレス等にウイルスを添付し

たメールを送信します。そのウイルス付メールを受け取ると、メールを開いたり、プレビューしたりしただけでも感染することがあります。

Web ページ改ざん：

クライアントに侵入したウイルスは、脆弱性のある Web サーバを探索し、Web ページの改ざんを行います。セキュリティホールのあるブラウザで改ざんされたホームページを見るとウイルスに感染します。

・コンピュータウイルス対策

➢ウイルス対策ソフトウェアの導入

ウイルス対策ソフトウェアを各クライアントパソコンにインストールし、自動アップデート機能などを使って、ウイルス定義ファイルやプログラムを最新の状態に保つようにします。

➢添付ファイルのウイルスチェック

IPA に届出のあったウイルスの 9 割以上がメールによって感染しています。受け取った電子メールに添付ファイルが付いている場合は、開く前にウイルス検査を行うこと、また、電子メールにファイルを添付するときは、ウイルス検査を行ってから添付することが大切です。

➢最新のセキュリティ修正プログラムの適用

メーラーが電子メールの添付ファイルを自動的に実行してしまうというセキュリティホールは、頻繁に発見されているので、使用しているソフトウェア（特に、OS、メーラー、ブラウザ）に関してベンダーの Web サイトなどの情報を定期的に確認し、最新のセキュリティ修正プログラムを適用しておくことが重要です。

➢ファイアウォール機能の活用

ファイアウォール機能とは、使用しているコンピュータに他のコンピュータから送信される情報を制限することで、利用者の許可なしにコンピュータに接続しようとするユーザ、またはウイルスやワームなどのプログラムに対する防衛線となる機能のことで、Windows XP や Mac OS X など、最近の OS に搭載されている機能の一つです。ファイアウォールは、インターネットやネットワークから送信される "トラフィック" と呼ばれる情報をチェックし、ファイアウォールの設定に応じてその情報を拒否したり、情報がコンピュータまで届くことを許可したりします。

➢復旧用バックアップの作成

ウイルス対策ソフトウェアでウイルスを駆除することはできても、ウイルスにより破壊されたデータを修復することはできません。ウイルス感染被害からの復旧のため、日頃からデータのバックアップをとる習慣をつけておことが大切です。

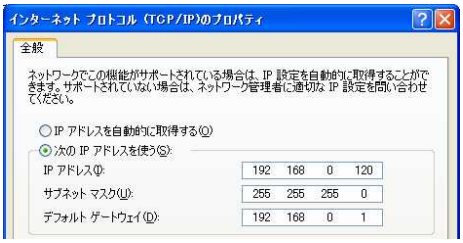
○データの紛失や盗難

データファイルを金庫などにしまって、紛失したり盗難にあったりしないように努めることは、もちろん大切なことですが、万が一に備えて、重要なデータについては暗号化をすることは効果があります。暗号化の方式は、大きく分けて「共通鍵暗号方式」と「公開鍵暗号方式」の 2 つがあります。ただし、暗号化したデータは、当然、復号化しなければ使えるようになりませんので、利便性の低下を考慮して使う必要があります。また、暗号化したデータをメールで送受信する場合は、送信側・受信側の双方で、暗号化に対応した環境が必要となりますので、その点にも注意が必要です。

○不正アクセス

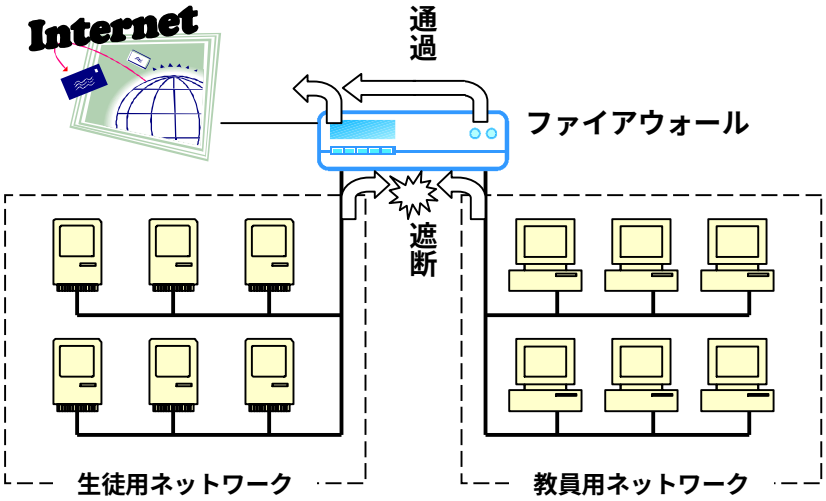
多くの場合、ネットワークに接続されたパソコンは、IP アドレスといわれる 32 ビットで表現される番号（例：192.168.0.120）で識別されます。IP アドレスの設定についてはユーザが明示的に設定する場合と DHCP と呼ばれる仕組みを使って自動的に取得する場合があります。

参考 IP アドレスの設定例

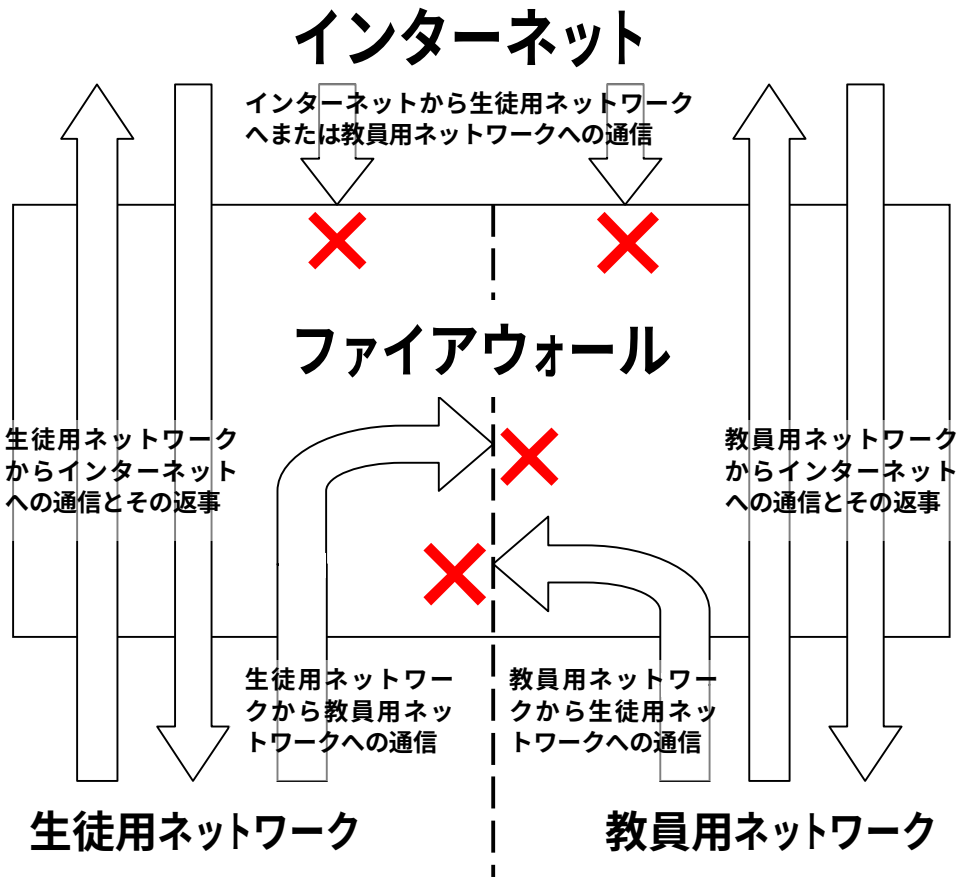


この IP アドレスをもとにパソコンが特定されて、他人に自分のデータが不正に利用される場合があります。特に、教員の使っているパソコンに生徒や外部の者がアクセスすることは、重要な情報の漏えいに繋がりますので、絶対にさけなければいけません。そこで、一般に、ファイアウォールというネットワーク中継機器を使ってネットワークを分割し、通信を制限することで、このような不正アクセスから情報を防御します。

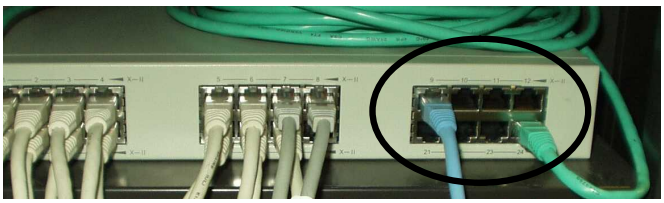
参考 ファイアウォールを使ったネットワーク分割のイメージ



参考 ファイアウォールの動作例（パケットフィルタリング）

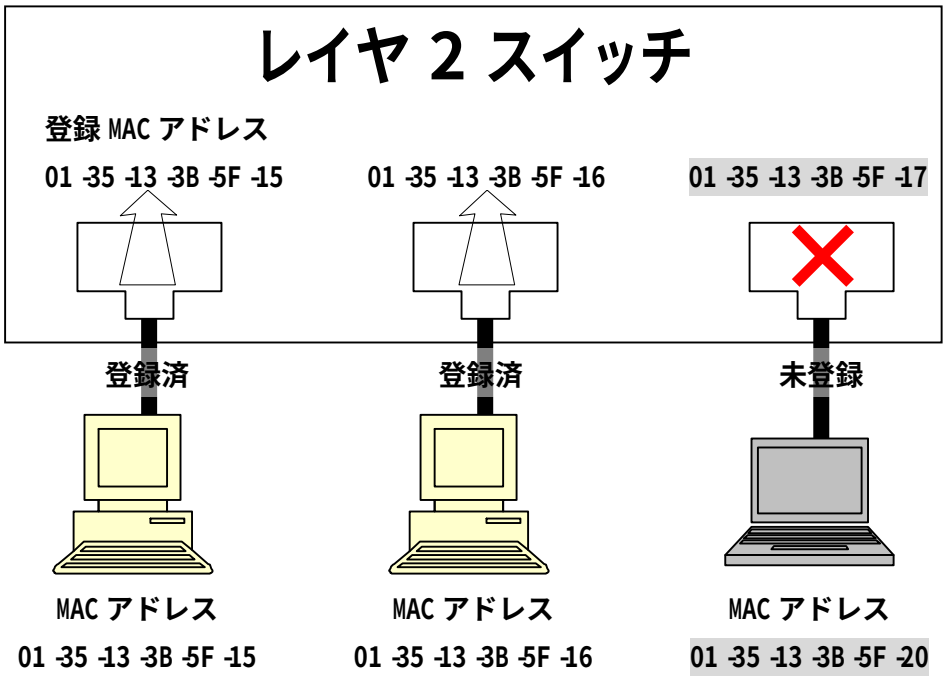


ファイアウォールでネットワークを分割しても、ハブの空きポートなどに、無許可でコンピュータを接続されてしまっては意味がありません。そこで、この様な問題への対策として、特殊な機能を持ったスイッチングハブ（一般にレイヤ 2 スイッチと呼ばれます）を使って、ネットワークに接続できる機器を物理的に制限します。



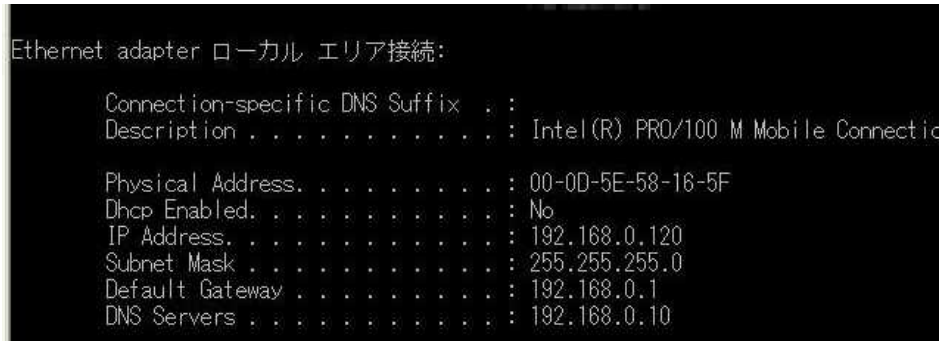
ネットワークに接続されたパソコンのネットワークインターフェースには、MAC アドレスといわれる 48 ビットで表現される番号（例：01 -35 -13 -3B -5F -15）が付与されています。IP アドレスはユーザが随意に変更することが可能であるのに対して、MAC アドレスは多くの場合、ネットワークインターフェースに対してハードウェア的に設定してあり、ユーザが変更することはほぼ不可能です。そこで、MAC アドレスがユーザによって変更できない点に着目し、機器を識別する固有の番号として MAC アドレスを使います。レイヤ 2 スイッチに接続を許可するコンピュータの MAC アドレスを登録しておくと、レイヤ 2 スイッチは登録してある MAC アドレスを持ったコンピュータからの通信を許可し、それ以外のコンピュータからの通信を遮断します。この仕組みを MAC アドレスによるフィルタリングと呼んでいます。

参考 レイヤ 2 スイッチの動作例（MAC アドレスフィルタリング）



MAC アドレスによるフィルタリングはセキュリティを強化するためには有効ですが、レイヤ 2 スイッチに全てのコンピュータの MAC アドレスを登録する必要があり、人事異動や機器の入れ替えなど、管理が煩雑になるという側面があります。無線 LAN を使ったネットワークでも同様の仕組みを使って、接続を許可されたコンピュータのみがネットワークを使えるようにすることができますが、この場合も全てのアクセスポイントに MAC アドレスを登録する必要があるので、管理が煩雑になります。

パソコンに設定されている IP アドレスや MAC アドレスは Windows XP の場合はコマンドプロンプトから ipconfig /all とすることで見ることができます。Mac OS X の場合は Apple システムプロフィールで見ることができます。



3 管理面

○パスワードの盗難

サーバへのログオンやメールの受信など、パスワードの入力を求められる場面が多くなっています。私たちは、日常的に無意識にパスワードを入力するため、その重要性を忘れがちになっていることがあります。また、当初設定したパスワードを思い出せなくなってしまったりすることなどを理由に、たやすく推測されるような文字列をパスワードにしていたり、付箋にパスワードを書いて机に貼り付けていたりするケースがよくあります。しかしながら、このような状態でパスワードが盗難にあった場合、利用者本人になりすますことが可能となり、これが原因で重要な情報が盗まれる可能性が高くなります。これを避けるため、

・紙に書き留めない。

・マシンに保存しない。

・人に教えない。

・定期的にパスワードを変更する。

といったことを心がける必要があります。また、記号(!、#等)、数字、英字を適当に織り交ぜて、他人に推測されにくく、自分が忘れにくいパスワードを設定する必要があります。

➢推測されにくいパスワードの作成例

①パスフレーズを考える

例　「奇想天外」→「ＫＩＳＯＵＴＥＮＧＡＩ」

②母音を抜き記号や数字を挿入する

例　「Ｋ＄Ｓ＆ＴＮＧ%」

○情報管理体制

・鍵のかかる保管場所の確保

・保管場所の管理者の指定

・情報を破棄するときには権限のある人が行い、記録を残す

・情報取り扱いについて意識の啓発

§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（ネットワーク上を流通する情報や、コンピュータ及びネットワ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れに対する脅威を把握・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、データ漏えい・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、生徒や職員のプライバシー等

・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。

○情報セキュリティ基本方針

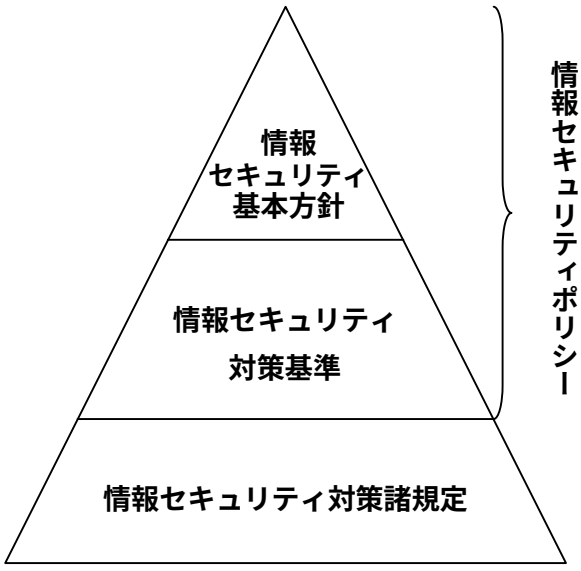
学校の情報セキュリティ対策に対する基本的な方針で、学校内でどのような情報資産を、どのような脅威から、なぜ保護しなければならないのか規定します。

○情報セキュリティ対策基準

「情報セキュリティ基本方針」を受け、遵守すべき行為と判断基準などを示します。

○情報セキュリティ対策諸規定

「情報セキュリティ対策基準」を受け、具体的な情報システムで、どのような手順で実施するのかを示します。

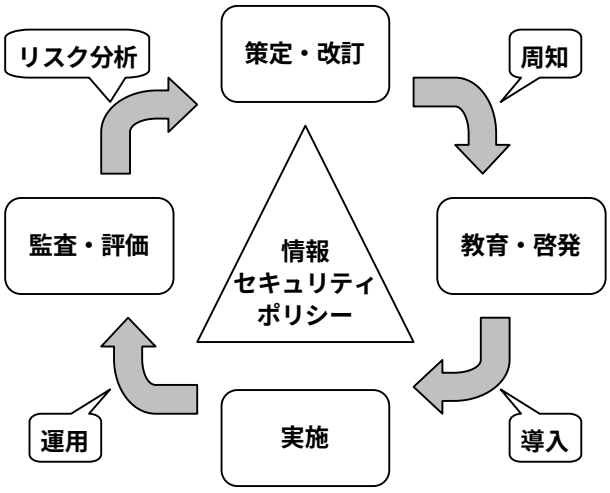


Ⅳ　情報セキュリティポリシーの運用

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、次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、セキュリティポリシーを策定し、利用者全員に周知します。
・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、その状況の直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

1 パソコンをつないで使ってみましょう

(1)　２台のパソコンを別々に使っていませんか？たった２台だけでもパソコンをつないで使うのとつながないで使うのとでは大違いです。

○それぞれのパソコンにプリンタを接続する予算・スペースはありますか？

プリンタが１台でも、２台のパソコンそれぞれからプリントアウトできます。

○２台のパソコン間でのデータのやり取りはフロッピーディスクですか？

それぞれのパソコンで作ったデータを、フロッピーディスクなどを使わなくてももう１台のパソコンで使えます。

片方のパソコンのハードディスクに入っているデータを、もう一方のパソコンで利用できます。

同じデータを“共有”して同時に編集することも可能な場合があります。

(2)　職員室にあるパソコンを全部つなぎましょう。

○教材プリントなど、みんなで似たようなものをバラバラに作っていませんか？

教員同士で教材を共有することが容易になります。

いろいろな教員の作った教材を参考にプリントを作れます。

学級通信・学年便りなどを保存・再利用できます。

１年前、２年前の学年便りなどを参考にし、再利用することも容易です。

○分掌ごとの文書引継ぎは正確になされていますか？

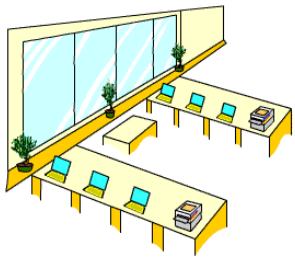
分掌ごとに一元管理しておけば、１年前、２年前のものを再利用することも容易です。

分掌ごとの年間の動きがわかり易くなります。

(3)　学校中のパソコンをつないでしまいましょう。

○どの教室からでもインターネットコンテンツにアクセスできます。

○生徒同士の討議や、教師への質問、回答 がパソコンでできます。



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

1 セキュリティの確保は重要な課題

便利なLANですが、セキュリティ確保は最重要課題です。

(1)　２台のパソコンをつないだ場合

もう１台のパソコンを使っている先生のデータを壊してはいけません。

ついうっかり、削除してはならないデータを、削除してしまう可能性があります。

自分の使っているパソコンのデータを利用している先生がいる最中に電源を切ると、作業中のデータが消えてしまう可能性があります。

→大切なデータはこまめに保存する必要があります。

(2)　職員室内のパソコンをつないだ場合

同僚とはいえ、やたらに知られたくないデータもあります。

外部に漏えいしてはいけないデータもあります。

ハードディスクが壊れることもあります。

→個人のパソコンに生徒の重要情報を保存してはいけません。

→管理者の許可無く、ソフトウェアを共用パソコンにインストールしてはいけません。

→データのバックアップは計画的・定期的に係を決めて行いましょう。

→共用パソコンの設定を勝手に変えてはいけません。

→データの入ったハードディスクや記録媒体を盗まれないようにしましょう。

(3)　生徒用のパソコンもつないだ場合

生徒に見られてはいけないデータの管理をしっかりしましょう。

生徒が先生用パソコンに侵入を試みないとは限りません。

→重要情報はハードディスクではなくMOなど可搬媒体に保存し､金庫などに保管します。

→記録媒体の置き忘れがないように注意しなければいけません。

(4)　インターネット接続している場合

ウイルス対策をしっかりとしましょう。

大事な情報が知らないうちにメールになって流出したら！

コンピュータが正常に動作しなくなったら？

→ウイルス対策ソフトを導入するだけでなく、ウイルス定義ファイルを常に最新のものにしましょう。

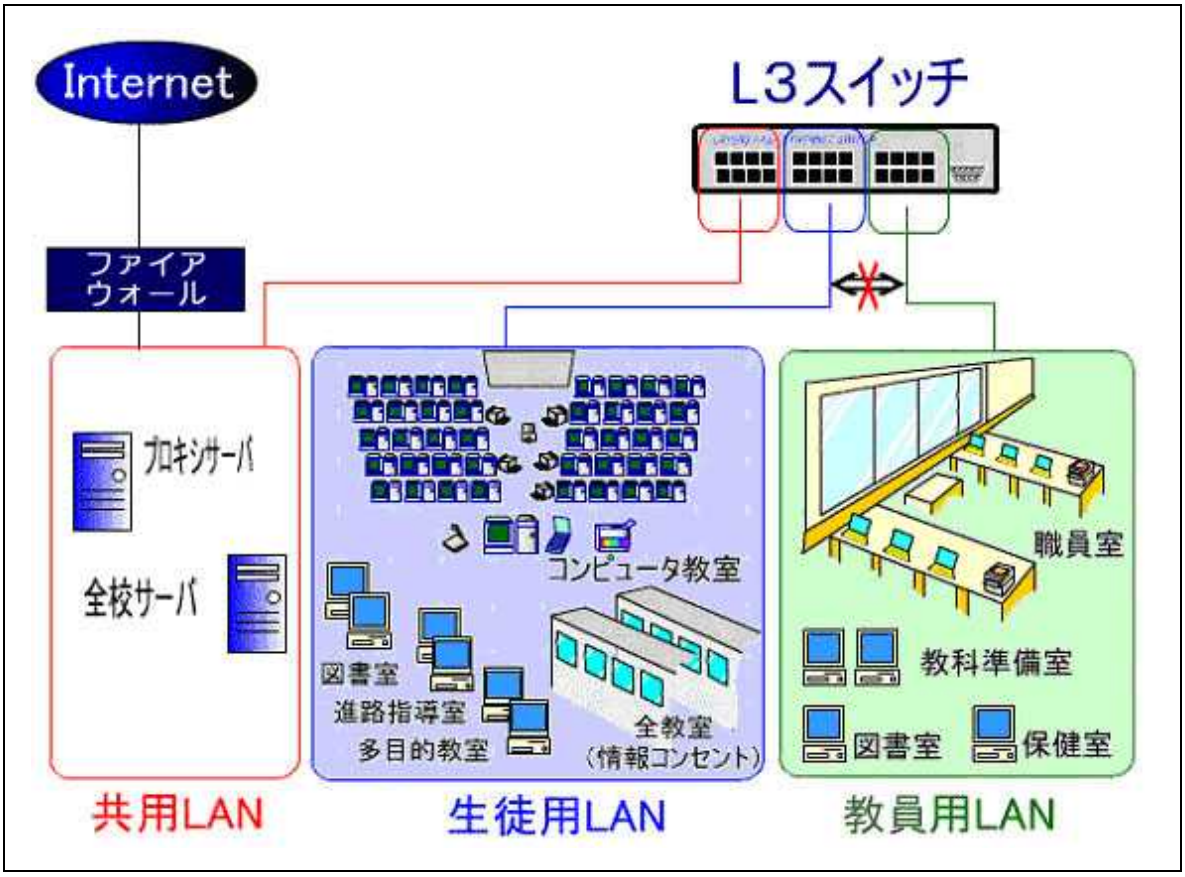
ハッカー対策をしっかりとしましょう。

大事な情報が入ったコンピュータに、第３者が勝手にアクセスしてくるかもしれません

→ＩＤとパスワードの管理に十分気を配りましょう。

→重要情報はローカルのハードディスクに保存しないようにしましょう。

2 ネットワーク構成概念図



3 全体構成とセキュリティ確保について

先に出てきた、生徒用のパソコンも全部つないだある学校では次のように運営しています。

【全体構成】（詳細はⅢ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。

・Ｌ３スイッチで LAN 間の通信を制御しています。

(Ｌ３スイッチとは、ネットワークのある種の中継機器のことです)

【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Ⅴへ）

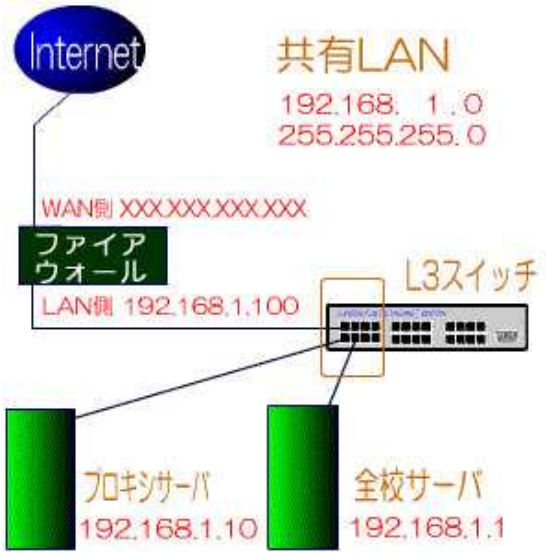
・内部的な脅威が発生しないよう定期的に教員のセキュリティ研修会を実施しています。

・LAN には管理者が許可した機器以外は接続しないようにしています。

（MAC アドレスセキュリティ）

III　サーバ室は立入り禁止～ネットワークの要はセキュリティの要～

1 共有の LAN（192.168.1.0/24）



サーバ室には共有の 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。

2 サーバ設置の基本事項と日常のメンテナンス

分掌や委員会など管理者権限を持つ係を決め、係にサーバの管理をしてもらいます。サーバの管理係には、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沢山あります。また、ネットワークの不具合やその対処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

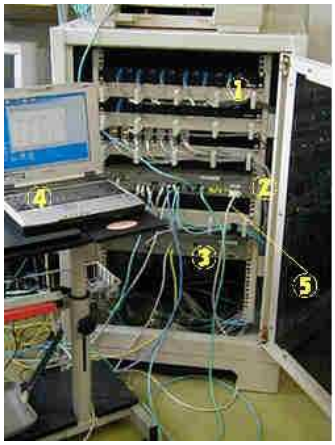
【日常的なメンテナンス】
- ユーザアカウント管理
- データ・システムのバックアップ
- 利用状況確認とログの監視
- コンピュータウイルス被害状況確認
- ウイルス対策ソフトウェアのパターンファイルのアップデート
- OS のセキュリティアップデート

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-5 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

4 ネットワーク中継機器



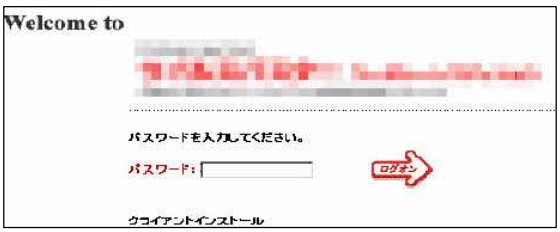
【ネットワーク中継機器】
①光ケーブルコンバータ
②Ｌ３スイッチ
③ギガビットＬ２スイッチ
④コンソールとして利用する PC
⑤PC とＬ３スイッチを繋ぐ RS-232C ケーブル

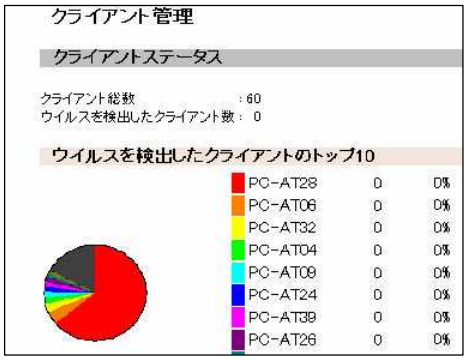
ネットワークの要はすべてサーバ室にあるこのラックの中に収まっています。
ここから信号は光ファイバケーブルを通って各教室の情報コンセントまで到達しています。
言わば校内 LAN の要にあたるわけですが、中でも②Ｌ３スイッチは LAN 間の通信を制御するセキュリティ上最も重要な機器と言えます。

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、設定をします。

5 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す。
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す。管理・インストールともに、インターネットでアンケートに答えるような要領で、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

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、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

2 コンピュータ教室の利用に関して

コンピュータ教室を生徒に開放する場合、次のような何らかのルールと指導が必要でしょう。
- 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　など

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

4 特別教室の利用に関して

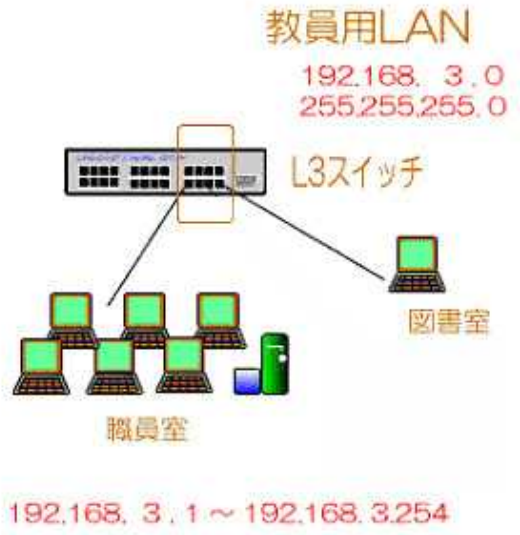
■多目的教室
教室棟の多目的教室に中古パソコン 4 台を設置
総合学習など調べ学習に利用可能

■図書室
蔵書管理システムと合わせ各検索や閲覧が可能

■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

Ⅴ　教員には理解と研修を

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。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するよう働きかけます。

【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

2 教員研修

年度の初めに着任者を交えて、ネットワークの利便性と危険性に関する研修会を実施します。

【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

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、次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？

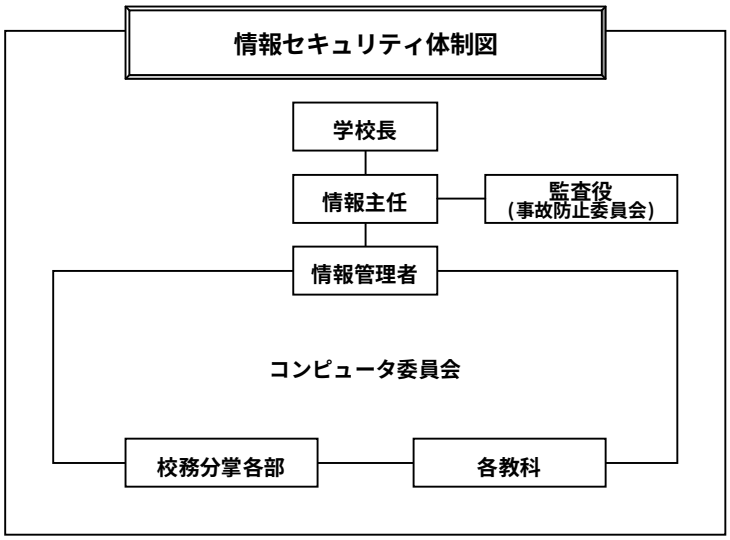
⇒
- MAC アドレスをＬ３スイッチへ登録
- 利用可能 IP アドレスを教員に配布

情報セキュリティポリシー策定事例

Ⅰ　策定前の準備

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）



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

リスク分析の例

情報資産を適切に保護するために、情報資産を把握し、リスクを定量的に評価します。ここでは ISMS などに示されている手法を使ったリスク評価の例を挙げます。

情報資産の評価

まず、情報資産の価値を機密性、完全性、可用性を考慮して設定します。次に情報資産の評価基準の例を示します。

重要度設定の例

重要度	クラス	説明
4	対策重要度Ⅰ（非公開）	個人情報
3	対策重要度Ⅱ（秘密）	特定の関係者のみに開示
2	対策重要度Ⅲ（公開）	請求があった場合開示
1	対策重要度Ⅳ（公開）	一般公開

重要度を設定したら、情報資産の一つひとつを把握し、要素ごとに、その価値を明確にします。

情報資産評価例

No	情報資産	保管場所	重要度
1	教育課程編成表	校内サーバ	2
2	生徒配付プリント	クライアント PC	1
3	学校要覧	校内サーバ	2

脅威の評価

情報資産が評価できたら、次に情報資産ごとに、それらを取り巻く環境を考慮して、関連する脅威を明らかにします。脅威の評価基準は次のように発生頻度を基に設定されます。

脅威の評価基準例

脅威の程度	内容
3	発生する可能性が高い（1 ヶ月に 1 回以上）
2	中程度の可能性で発生する。（半年に 1 回程度）
1	発生する可能性が低い。（1 年に 1 回程度）

脆弱性の評価

脆弱性とは脅威を引き起こす原因となるものを指します。脅威に対する対応策を検討し、それがすでに実施されているのか調査し、脆弱性を明らかにしていきます。次に脆弱性の評価基準例を示します。

脆弱性の評価基準例

脆弱性の程度	
3	保護対策が全く講じられていない。
2	保護策はあるが、万全ではない。
1	十分な保護対策が講じられている。

リスクの評価

リスク値は、ここまでの作業で明確になった「情報資産の価値」、「脅威」、「脆弱性」を用いて、簡易的に、次のような式で算出します。リスク値が大きいほど、リスクが高いといえます。

リスク値 = 「情報資産の価値」×「脅威」×「脆弱性」

リスク値算出例

情報資産	教育課程編成表	情報資産の重要度	2
脅威	担当者の誤操作による消去	脅威の程度	2
対策	内容の確定後はファイルの属性を読み取り専用に変更	脆弱性の程度	2
リスク値	2 × 2 × 2 = 8		

情報資産	教育課程編成表	情報資産の重要度	2
脅威	上書き保存による意図しない変更	脅威の程度	3
対策	内容を変更するときはファイルのコピーを作成する。	脆弱性の程度	2
リスク値	2 × 3 × 2 = 12		

⋮

II　情報セキュリティポリシーの策定

1 情報セキュリティ基本方針の策定

(1) 趣　旨（目的）
(2) 構成と位置づけ
(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

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) パスワ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) ネットワークの利用に関する基準
(9) Web 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

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の確保。

2 情報セキュリティシステムの実装及びテスト

(1) NT サーバの構築・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

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」の諸規程の策定

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の見直しを行う。

用語集

A～Z

DHCP

Dynamic Host Configuration Protocol の略。各クライアントに、起動時に動的に IP アドレスを割り当て、終了時に IP アドレスを回収するためのプロトコル。

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、パソコンでは左図のような項目を設定する必要がある。

ISMS

Information Security Management System の略。企業や組織が自身の情報セキュリティを確保・維持するために、セキュリティポリシーに基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのこと。ISMS をその組織が保持しているかどうかを第三者が認定する制度として「ISMS 適合性評価制度」と呼ばれる評価認定制度がある。現在、日本情報処理開発協会（JIPDEC）を中心に 2002 年より正式運用されている。

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

Uninterruptable 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～

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。

カ～

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。

サ〜

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。

タ〜

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。

ナ～

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。

ハ～

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

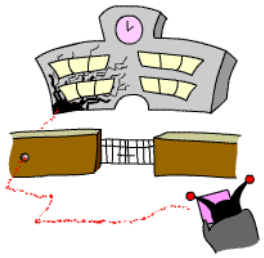
インターネットから LAN への不法な侵入を防ぐ目的で、インターネットとやり取りできるコンピュータを制限したり、LAN から利用できるインターネットのサービスを制限したりする。

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。

ラ〜

ルータ

レイヤ 3 スイッチ

ネットワーク中継機器。IP 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。

レイヤ 2 スイッチ

ネットワーク中継機器。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、次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）

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

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）

ストレージ上のデータ消去に関するガイドライン
http://it.jeita.or.jp/infosys/committee/network/guideline0407/

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**

付録

情報セキュリティ意識チェックリスト

校内研修等で、教職員の情報セキュリティ意識のチェック用にお使いください。次のページに関連項目への参照先が書いてあります。

質問事項		YES	NO
Q1	「情報セキュリティ」という言葉を知っていますか？		
Q2	「なりすまし」という言葉を知っていますか？		
Q3	「コンピュータウイルス」という言葉を知っていますか？		
Q4	Web ページの入力フォームに個人情報を記入することに不安を感じますか？		
Q5	重要なメールやファイルのバックアップをとっていますか？		
Q6	プリンタから印刷した文書をそのままプリンタに放置していることがありますか？		
Q7	パスワードには推測しにくい文字列を使っていますか？		
Q8	「IP アドレス」という言葉を知っていますか？		
Q9	「MAC アドレス」という言葉を知っていますか？		
Q10	OS やブラウザのセキュリティアップデートを知っていますか？		

解説

Q1 ⇒ 1 ページ
Q2 ⇒ 32 ページ
Q3 ⇒ 9 ページ
Q4 ⇒ 次の図のように Web ブラウザから入力した内容を Web ページの開設者へ送信できるような Web ページがあります。大変便利ですが、盗聴などの危険性もあるので、重要な情報をこの仕組みを使って送信することは避けた方が無難です。どうしても送信する必要がある場合は Web ブラウザの右下の鍵のアイコンを確認し、通信が暗号化されていることを確認しましょう。また、実在する企業の Web サイトに見せかけたサイトへユーザを誘導し、クレジットカード番号などを入力させて盗むことを目的とした Web サイト（phishing）もあるので注意が必要です。

図　入力フォームの例

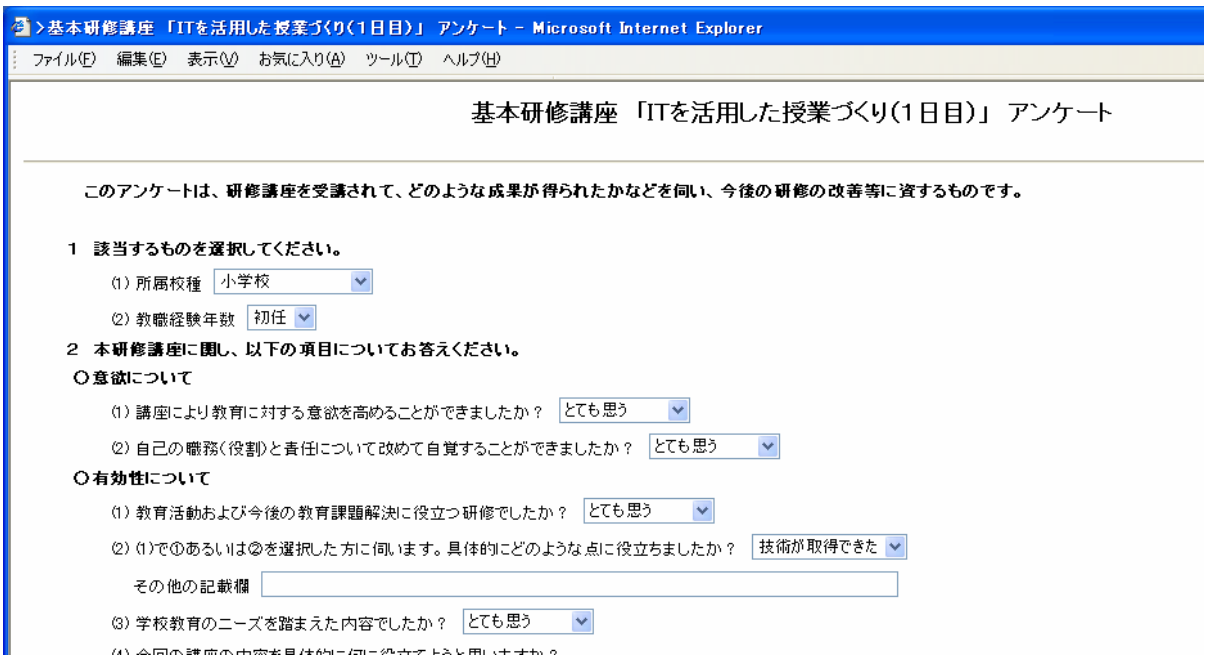
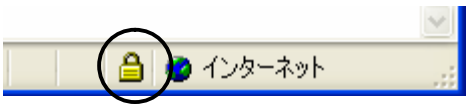


図　暗号化通信時に表示されるアイコンの例



Q5 ⇒ 11 ページ
Q6 ⇒ ネットワークを使ったプリンタ共有の普及により、プリントアウトした書類は自席を離れて、プリンタ設置場所へ取りに行かなければいけないことが増えました。この様な環境では、重要書類をプリンタに放置したままの紛失に注意する必要があります。
Q7 ⇒ 15 ページ
Q8 ⇒ 12 ページ
Q9 ⇒ 13 ページ
Q10 ⇒ 11 ページ

リスク評価シート

26 ページの例で紹介したような、リスク分析を行うときにお使いください。次のページに記入例があります。

情報資産

内容	重要度	備考

脅威

番号	内容	程度	備考
T1			
T2			
T3			
T4			
T5			

対策

番号	内容	対策済	程度	備考
P1		□ (済の場合■)		
P2		□		
P3		□		
P4		□		
P5		□		

リスク

番号	脅威	対策	内容	リスク値	備考
1					
2					
3					
4					
5					

ISMS ガイド（財団法人日本情報処理開発協会）を参考に作成

リスク評価シート（記入例）

情報資産

内容	重要度	備考
教育課程編成表	2	

脅威

番号	内容	程度	備考
T1	担当者の誤操作による消去	2	
T2	上書き保存による意図しない変更	3	

対策

番号	内容	対策済	程度	備考
P1	内容の確定後はファイルの属性を読み取り専用に変更	■	2	
P2	内容を変更するときはファイルのコピーを作成する	□	2	まだ徹底されていない

リスク

番号	脅威	対策	内容	リスク値	備考
1	T1	P1	当該電子データの消失	2 × 2 × 2 = 8	
2	T2	P2	オリジナルデータの改ざん	2 × 3 × 2 = 12	

重要度設定の例

重要度	クラス	説明
4	対策重要度Ⅰ（非公開）	個人情報
3	対策重要度Ⅱ（秘密）	特定の関係者のみに開示
2	対策重要度Ⅲ（公開）	請求があった場合開示
1	対策重要度Ⅳ（公開）	一般公開

脅威の評価基準例

脅威の程度	内容
3	発生する可能性が高い（1ヶ月に1回以上）
2	中程度の可能性で発生する。（半年に1回程度）
1	発生する可能性が低い。（1年に1回程度）

脆弱性の評価基準例

脆弱性の程度	
3	保護対策が全く講じられていない。
2	保護策はあるが、万全ではない。
1	十分な保護対策が講じられている。

『学校情報セキュリティガイド 2005』の作成関係者

<調査研究協力員>

所属	職名	氏名	備考
大和市立文ヶ岡小学校	教諭	山口　亮二	平成 15 年度
大和市立引地台小学校	教諭	鎌田　達雄	平成 16 年度
大磯町立大磯中学校	教諭	伊藤　努	平成 15、16 年度
県立津久井浜高等学校	教諭	深瀬　誠	平成 16 年度
県立高浜高等学校	教諭	間辺　広樹	平成 15 年度
県立大船高等学校	教諭	内藤　哲也	平成 16 年度
県立新磯高等学校	教諭	大河原広行	平成 15 年度

<神奈川県立総合教育センター>

所属	職名	氏名	備考
情報交流課	教育専門員	長塚　正義	
情報交流課	研修指導主事	柏木　隆良	
情報交流課	教育指導員	村山　孝夫	

学校情報セキュリティガイド 2005

発行日　平成 17 年 3 月 31 日
発行者　清水　進一
発行所　神奈川県立総合教育センター
〒251-0871　藤沢市善行 7-1-1
TEL (0466)81-1679（情報交流課　直通）
ホームページ　http://www.edu-ctr.pref.kanagawa.jp/

古紙配合率 100%再生紙を使用しています。

神奈川県

神奈川県立総合教育センター
カリキュラムセンター（善行庁舎）
〒251-0871　藤沢市善行 7-1-1
TEL (0466)81-0188
FAX (0466)84-2040

教育相談センター（亀井野庁舎）
〒252-0813　藤沢市亀井野 2547-4
TEL (0466)81-8521
FAX (0466)83-4500

ホームページ　http://www.edu-ctr.pref.kanagawa.jp/