C3302 教育テキスト作成ガイドライン（システム管理者向け）

国立情報学研究所 学術情報ネットワーク運営・連携本部  
高等教育機関における情報セキュリティポリシー推進部会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年10月31日  A3302 | 新規作成 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2015年10月9日  C3302 | 高等教育機関の実態に合わせた内容の見直し | 金谷吉成（東北大学）  中山雅哉（東京大学）  西村浩二（広島大学） |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

　情報セキュリティ関連教育は、大学の特性を踏まえて行う必要があります。本文書では教育テキスト作成ガイドラインとして、システム管理者が踏まえるべき大学の特性と情報セキュリティ関連教育事項の関係を必要最小限の項目に絞って述べます。さらに、部局や情報センター所属のシステム管理者が情報サービスの維持・運用・管理も行う場合に必要な心構えや学習項目についても言及しています。なお部局での情報セキュリティ管理は、専門の担当部署や担当者が部局総括責任者や部局技術責任者として担当する場合と、システム管理者がこれらの役割を兼務する場合とがあります。このガイドラインの内容は部門技術責任者の役割を兼ねる可能性のあるシステム管理者を対象としたものですが、情報セキュリティ管理上の役割に応じて必要となる知識は変わってくることに留意してください。

解説：教育項目としての諸規程については、高等教育機関の情報セキュリティ対策のためのサンプル規程集（以下、本サンプル規程集：国立情報学研究所 学術情報ネットワーク運営・連携本部高等教育機関における情報セキュリティポリシー推進部会）そのものが最良のテキスト例である。必要に応じて参照願いたい。

**第１章　概論**

1.1 概要

　大学の使命は、学生に質の高い教育を提供することと、学問における未知の問題の解決に取り組むことです。その目的を果たすために、大学には多くの資産があります。ここで資産というのは、建物や実験設備に代表される物理的なもの、教員や職員といった人材、そして、大学が所有するさまざまな情報のことを指します。ここでは、情報資産について考えてみたいと思います。大学が所有する情報資産には、例えば次のようなものがあります。

● 成り立ちが大学に属するもの

　 ○ 教員、大学院学生の研究・教育内容

　 ○ 学生、教員、職員の個人情報（氏名、住所、成績、履歴、業績など）

● 購入やライセンスの取得により使用できるもの

　 ○ 情報システム（大学の情報ネットワークに接続する機器を含む）

　 ○ コンピュータルームにあるPCに内蔵されているソフトウェア

　 ○ 図書館の電子ジャーナルやオンライン・データベース

　現在、大学の情報資産の多くはコンピュータで取り扱うことができるようになっていて、その中のいくつかはインターネットを通じて外部に公開されています。しかし、公開に適さない情報資産は逆に、インターネットでは入手できないようになっています。もし、大学の情報資産を無断で消去してしまったり、外部に提供することが禁止されている情報資産を誰かが誤って提供してしまうと、大学の運営に支障を来すことがあります。このようなことは、情報資産以外の資産と同じように考えてください。大学の情報資産を不正に消したり書き換えたりすることは、大学に備え付けられている備品を破壊することと同じで、学則や就業規則に違反するときは懲戒の対象となり、法律に違反するときは犯罪になる可能性もあります。

　本学の教員および職員は、大学の就業規則にしたがって大学の資産を管理する必要があります。そこでは、大学の資産が外部に流出したり、消失したりしないように、細心の注意を怠ってはいけないといえます。

　法律や公序良俗に反する行為以外にも避けるべき行為があります。例えば、コンピュータやネットワークの正常な運用を阻害する行為を避けるべきです。ただし、個々の環境によって、避けるべき行為は様々です。

　学内に設置してある各種の電子計算機、通信回線装置および通信回線は、大学という教育・研究機関に所属するものです。また、大学から利用資格として通知されたアカウントも、本学における教育・研究目的に必要不可欠であるからこそ全員に付与されています。したがって本学の教育・研究目的に著しく反するような形で、これらを利用すべきではありません。

　近年、インターネットを始めとする情報通信技術の発達に伴い、大学が保有する情報資産の利用・流通にも変化が現われています。たとえば従来は、紙の学生証による本人確認によって交付されていたさまざまな証明書が、ICカードなどを利用した学生証によって本人宛に交付されるようになり、また、データベースの活用のおかげで、そのデータの正確性も確保されるようになりました。

　電子情報の特徴の一つとして、「複製の容易さ」と「処理のし易さ」を挙げることができます。前者は、情報漏えいや著作物の不正複製の際は「悪い特徴」として捉えられます。一方、後者は暗号などの仕組みを利用した安全な通信を成立させる「よい特徴」として捉えることができます。

　そして今後も、暗号技術、ネットワーク技術などさまざまな情報通信技術が高度に発展していくことが見込まれます。情報通信技術の発展は、システム管理者にとっては防御技術の進化に寄与しますが、一方でネットワーク犯罪者にとっては犯罪技術の進化に寄与しています。

　情報に関する技術が、他の技術ともっとも異なる様相を見せるのは、変化の速さです。情報通信技術は他の技術の数倍の速さで変化するため、われわれのライフスタイルを変えてしまうような技術が突然現れたり、新しく開発された技術がわずか数か月で陳腐化し時代遅れのものとなってしまい、変化に対応できないと成長から取り残されてしまったりすることがあります。

　システム管理者は、このように、犯罪防御も、犯罪行為も技術革新によって日々変化していて、そのなかで、安全な情報サービスの提供に努めるために何ができるかを考える必要がある、ということができます。

1.2 大学で守るべき情報

　大学にある情報資産を、事務部門と教育研究部門の２つに分けて考えてみます。

　事務部門には、教職員や学生の個人情報があります。個人情報には、氏名や住所などの基本的な個人情報の他に、研究活動・学習活動に伴う個人評価、健康状態、給与・学費の状況なども含まれます。また、大学として契約や調達に関わる情報を保有しています。

　一方、教育研究部門としては、大学が持つ研究情報資産、具体的には未公開の特許情報や、大学として企画・制作した著作物などの知的財産があります。各部門の管理責任者は、自らの部門にどのような情報資産があるかを把握しておく必要があります。

1.3 大学において守るべき事項と特徴

　研究のみを目的としている研究機関と異なり、大学の場合は、教育機関としての側面を同時に持ち合わせています。研究を行う教員と学生、教育を受ける学生、研究に参画する企業の研究者など、大学にはさまざまな立場の人間が出入りします。また、頻繁な人事異動、入学・卒業があります。そのため、大学にはさまざまな人が自由に出入りし、その状況調査も簡単ではありません。一方で、歴史的な経緯で、大学には学問の自由、自治権があり、また、大学の研究成果は広く公表されるべきだという考え方もあります。

　このような状況を前提にして、情報資産を適切に運用するには、大学情報の機密性・完全性・可用性を十分に確保する必要があります。例えば、機密性については、すでに述べたように、最新の暗号技術を利用して、多彩な情報閲覧権限・編集権限を設定する必要があります。システム管理者は、自部局の情報閲覧権限や編集権限を十分調査し、適切に設定を行う必要があります。

　なお、インターネットに接続をして、さまざまな情報を流通させる場合には、情報セキュリティについて注意する必要があります。大学だからといって、一般企業や行政機関と比べて情報セキュリティ対策が甘くてよいということはありません。サーバ攻撃（DoS、ポートスキャン、不正侵入、ウェブページ書き換え）、ウイルス・迷惑メール、P2Pファイル交換ソフトなどの不正アプリケーション使用による情報漏えい、踏み台、物理的脅威（盗聴、侵入、操作ミス、不正）などの対策が必要です。

1.4 大学の情報セキュリティ対策の特徴

　情報セキュリティ維持の基本として大学全体の情報セキュリティポリシーが定められます。さらに大規模大学のように部局ごとに運用組織があるようなケースでは、各部局の事情に応じて部局毎に実施規程等として詳細化されることがあります。部局総括責任者にとって、情報セキュリティポリシーおよび実施規程間の矛盾に配慮することは重要です。全学のポリシーと、ある部局の実施規程等が矛盾することのないように、全学ポリシーの策定作業には全部局の部局総括責任者が参加すべきです。部局総括責任者は部局間の実施規程等の違いを部局の事情とともに理解し、それに起因する問題の解決に向けて努力すべきです。さらに、全学と各部局で実施規程等が異なる原因について検討する必要があります。多くの場合は、部局技術責任者の役割を担うシステム管理者のスキルに差が大きいため、スキルを身に付けた部局の提案が全学のポリシーに反映される傾向があります。また、附属機関として病院などがある部局と、そうでない部局では、利用者の個人情報の取扱が異なることがあります。このような情報セキュリティポリシーが適用される環境の差を認識し、全学の情報セキュリティポリシーに、部局毎の事情を矛盾なく追加できるようにしておく必要があります。

　このような努力を有効なものとするため、インシデント（情報セキュリティに関して生じる事故や事件）に対応できる全学の組織をあらかじめ整えておくことが重要です。組織を整えておかない場合にはインシデントに対する迅速な対応が困難となることもあります。  
　また、大学のように、最先端の情報通信技術を利用しようという組織の場合、潜在的な脅威となる項目を発見することが困難であり、さらに、研究開発においては、リスクのように確定していない（未知の）脅威に対する対策費用を計上することも簡単ではありません。また、セキュリティ対策には終わりがなく、どんなに高価で高性能な機器を導入しても、どれだけコストをかけても、完璧に対応できるものでもありません。システム管理者が技術者として求められるのは、情報通信技術に対する正しい理解と、技術が原因で発生した脅威には技術をもって対応するという姿勢です。

　なお、大学には学問の自由があり、教員の研究は他者から干渉されるべきではなく、自由な立場で研究が行われなければならないという考え方があります。そのため、情報セキュリティ維持に欠かせないファイアウォールによる通信の制限やパケットフィルタリングを行うことを嫌うことがあり、その結果として、管理が行き届いていないパソコンがウイルス感染や情報漏えいなどの問題を引き起こすことがあります。したがって、システム管理者は、学問の自由等の憲法上の諸権利についても考慮しながらも、情報セキュリティを十分に確保する具体的な対策を検討していく必要があります。

　ここで、情報セキュリティポリシーを作成する際に必要となる情報リスクマネジメントの注意事項を記します。

1. まず、情報セキュリティの確保を行う目的と場所を明らかにすることです。その際には、学内にある情報資産をすべて調べあげ、どのような脅威がどの程度の確率で発生するかを予想することが必要です。また、脅威に対する被害を予想することも必要です。これをアセスメントといいます。

2. 次に目的に応じた手法を計画（Plan）し、計画通りに実施（Do）し、そして実施がうまく出来ているかを監査（Check）し、改善（Act）する必要があります。この流れをPDCAと呼びます。

3. 一度PDCAを実行したら、再びPDCAを行います。これを繰り返していくことで、日々の情報セキュリティの確保を行えるようになります。

　各項目においては、制度・組織の見直し、技術的な解決、教育（研修）による対応などを同時に進める必要があります。また、予算確保や、規程・手順の作成も行う必要があります。

　規程・手順の項目を作成する場合も、

a. インシデントを防ぐための項目

例: 施錠、パスワード設定、フィルタリング

b. インシデントがあっても復旧可能にするための準備項目

例: バックアップ、暗号化、予備電源

c. インシデント発生時の対応項目

例: 緊急連絡網、バックアップからの復元、代替装置への切り替え

d. インシデント発生後の始末項目

例: 報告（お詫び）、被害算出、保険の検討、規程の改定

のすべてを考える必要があります。

　なお、近年、大学同士で図書館利用や単位互換、連合大学院、入試問題の共通利用なども行われています。また、大学においては企業との共同研究が活発化しています。そのため、情報セキュリティポリシーを作成した場合は、他機関や企業との矛盾点をうまく解決できるようにしておくべきであるといえます。

　システム管理者が情報セキュリティポリシーについて学ばなければならない項目を、別の観点で整理してみます。個人の情報をデータとして取り扱うことができるようになった現在、私たちは簡単に他人を詐称したり、架空の個人を作り出すことができるようになり、その結果として、さまざまな犯罪行為も行われるようになりました。

　しかし、社会において人々が行為の自由を権利として行使できるのは、自由が、その行為に伴う責任と不可分であるからです。ところが、他人を詐称したり、架空の個人を作り出したり、インターネットの匿名性を悪用したりすることは、行為と責任を切り離します。しかし、サイバースペースは現実社会と同じなのであって、責任をはっきりと意識しなければ、本当の意味での自由な行動を保障することはできません。情報セキュリティポリシーは、このような観点からも検討していく必要があります。具体的には、情報資産利用の目的を明らかにし、個人用アカウントの貸し借りや共用、パスワードの盗用などを禁止するとともに、アカウントのトレーサビリティを確保する事項を情報セキュリティポリシーに盛り込むべきでしょう。大学は学術研究の場所です。商業的な利益に左右されることなく、真実・科学のために活動をすることが許されている場所であるともいえます。だからこそ、おかしな商業主義や、科学的な検証をうけていない態度に惑わされることなく、活動を行うことができます。情報セキュリティ教育についても同じです。情報セキュリティ教育が目指すべき学問的な健全さを追求し、他の組織の見本となる活動を行うべきであるといえます。

　また、工学・経営学・教育学の研究者が関わることが可能ならば、その観点からも情報セキュリティ教育を評価し、改善するべきでしょう。システム管理者は、自身として教育者である場合と、自身は教育者でない場合があります。前者の場合は、自らが利用者（おもに学生）への教育に関わることになりますが、後者の場合は、自らが大学の教育課程の中で利用者教育を担当することはありません。しかし、後者の場合であっても、利用者とのやり取りの中で情報セキュリティ教育に相当する行為を行わざるを得ない場合があります。

　そこで、利用者教育を担当する人（おもに情報リテラシー系の授業担当者）と連絡をとり、大学・各部局における情報セキュリティ教育の内容に、各部局固有の事情・内容・制限を反映させることが必要となります。

　ある時にある仕組みや制度が成立しても、情報通信技術の変化は大変激しいので、その仕組み・制度が急速に陳腐化し利用されなくなる、ということがよく起こります。システム管理者は、情報通信技術に関する様々な内容を、

「技能」

時間とともに変化する、商品知識的な内容。

「技術」

時間とともに変化することは少ないが永遠の真実とはいえない内容。

「科学」

時間とともに変化することがほとんどない内容。

その知識が直接、情報セキュリティに役に立つことはないが、

情報セキュリティの根幹をなす原理・原則である。

に分類しておき、それぞれを必要に応じて点検する計画を立てる必要があります。また、その中でも技能として分類される内容は時間とともに変化するため、その詳細を学ぶことが常に必要となります。ちょうど、携帯電話の新機種を購入すると、たいていの場合は使用方法が大きく変わっていて、そのため、取り扱い説明書をよく読まなければならなくなるのと同じです。

　第１章では、情報セキュリティに関する概論を述べました。その内容は、上位（部局総括責任者や部局技術責任者）の役割を兼ねる可能性のあるシステム管理者を想定し、情報セキュリティに関して知っておくべき知識と態度について、「科学の立場・教育学の立場」から述べたものです。ここでいう「科学の立場・教育学の立場」とは、情報科学のことではなく、「情報セキュリティの学習」という作業全体を科学的に分析した結果から得られた内容ということです。すなわち、「情報セキュリティを学ぶということはどのようなことか」「情報セキュリティを身に付けるとはどのようなことか」という内容を科学的に考察したものといえます。

　個々の内容については、続く第２章以降で取り扱います。

**第２章　ネットワークサービス・システム**

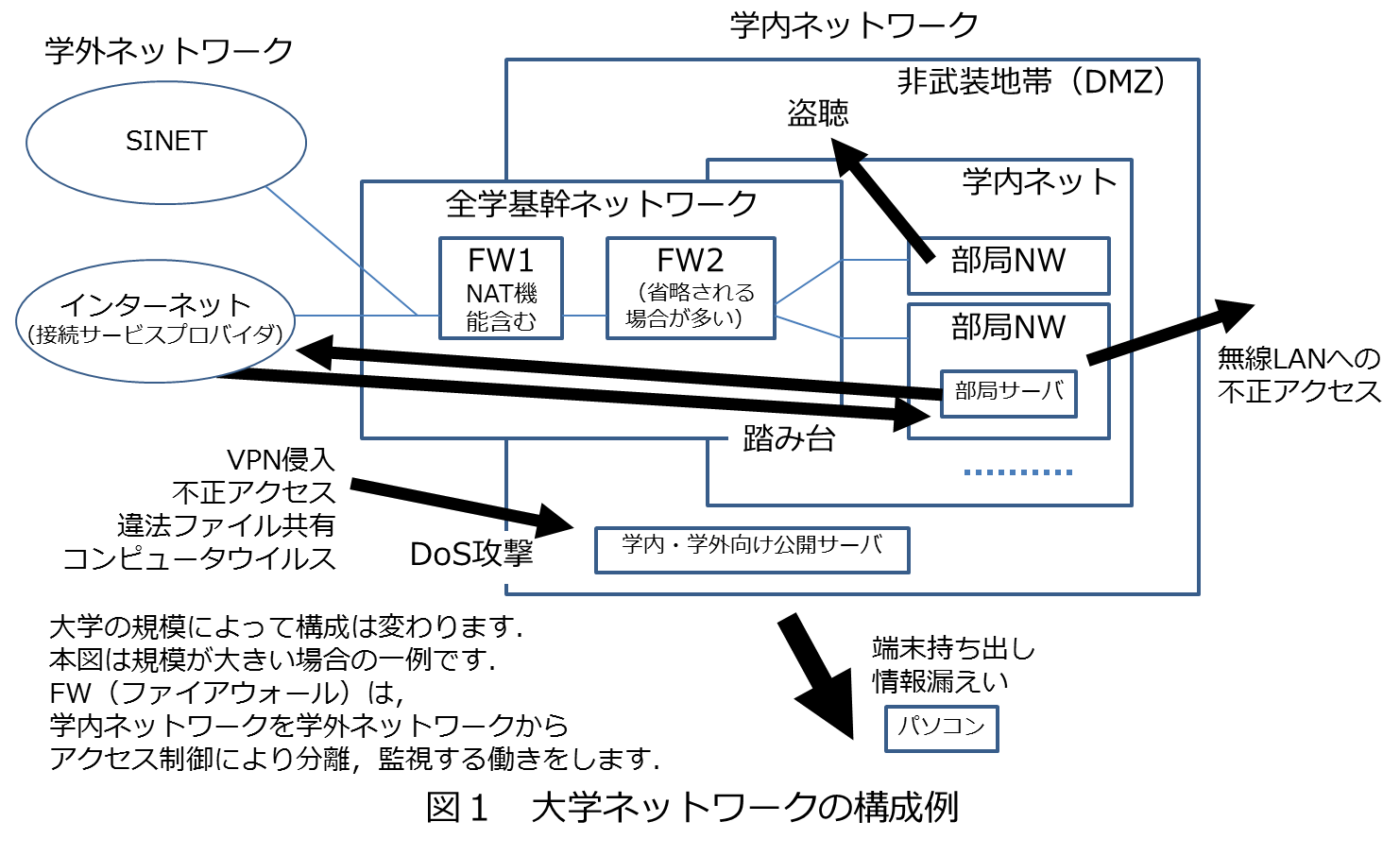


　図１に大学ネットワークの構成例を示します。図１は大規模な場合の例ですが、大学の規模によってネットワーク構成は変わってきます。小規模な場合には部局が直接インターネット（接続サービスプロバイダ）と接続する場合もあります。ある規模以上では多くの場合、部局ネットワークと全学基幹ネットワークの２階層構成になります。

　基幹ネットワーク、部局ネットワークの入り口にはセキュリティを確保するためのファイアウォールが置かれます。大学から学外への接続は、インターネット（SINETへの接続を含む）によってなされます。

　高いセキュリティレベルを保つべき学内ネットワークと学外ネットワークの間に学内・学外向け公開サーバ等をおく中間的なセキュリティレベルを設ける場合があります（非武装地帯）。中小規模の大学では十分なグローバルIPアドレスを持たないため、アドレス変換（NAT）機能を持ったファイアウォールを用いることが一般的です。

　大学ネットワークに対するセキュリティ攻撃は、例えば次のような多様な形で行われます。

- ネットワークの物理的盗聴

- 電磁的記録媒体、端末を経由した情報漏えい、ウイルス感染

- ガードの緩い無線LANへの不正アクセス

- 学外向けサーバでは簡易なパスワードの走査（スキャン）による発見とその利用

- ファイル共有ソフトによる情報漏えい

- メールに添付されたウイルスを介した攻撃

2.1 コンピュータネットワークの構成

　大学におけるコンピュータネットワークは、通常以下の要素によって構成されます。

1）LAN: 情報コンセント、無線LANアクセスポイントとそれに接続する電子計算機、周辺機器等から構成

2）部局ネットワーク: 1つ以上のLANをルータで接続したネットワーク

3）全学基幹ネットワーク: 学内の複数の部局ネットワークを接続し、さらに学外ネットワークにも接続するネットワーク

　大学ネットワークの情報セキュリティを維持するためには、ネットワークに接続する各機器において情報セキュリティを確保すると共に、ネットワークを相互に接続するルータにおいてファイアウォールにより情報セキュリティポリシーに応じたアクセス制御が必要です。

　地域交流センター、後援会、宿舎、インキュベーションセンターなどの学外の関連者がネットワークを利用する場合、学内ネットワークとの接続にファイアウォールを設置することにより、学内利用者と異なるアクセス制御が可能となります。

2.2 ファイアウォール

　ファイアウォールはネットワークの情報セキュリティ維持に欠かせない要素です。システム管理者はファイアウォールの設置箇所、ファイアウォールのアクセス制御ルールを適切に設定しなければなりません。必要に応じて、ネットワーク間を接続するルータにファイアウォールを設定します。ファイアウォールでは、学内ネットワークへの攻撃を防ぐと共に、学外ネットワークへの意図しない通信（学外への攻撃、迷惑メールの発信、P2Pファイル共有ソフトによる通信等）を防ぐ必要があります。また、IPアドレス詐称による攻撃を防ぐために、Reverse Path Forwarding（RPF）を行うことも考慮すべきです。

解説：送信元を偽装したIPパケットの転送を防ぐ手法は、RFC2827（BCP38）ではIngress Filtering と呼ばれており、Multihomed Network 向けに改版されたRFC3704（BCP84）では、Reverse Path Forwardingという用語が用いられるようになった。どちらの用語も広く使われているが、この文書では Reverse Path Forwardingを用いている。

　Network Address Translation（NAT）は外部のグローバルIPアドレスネットワークから内部のプライベートIPアドレスネットワークへ直接通信できなくするために、簡易ファイアウォールとして機能しますが、NAT越え技術、外部への意図しない通信には対応できないため、注意が必要です。

2.3 DMZ（Demilitarized Zone: 非武装地帯）

　学内ネットワークと学外ネットワークの間にDMZを設けて、そこに学外公開サーバを設置することがあります。DMZから学内へのアクセス制御を適切に運用することで、例えば学外公開サーバが攻撃者に乗っ取られた場合においても学内ネットワークを守ることが可能となります。

2.4 VPN（Virtual Private Network）

　大学が複数拠点にあり、拠点毎のネットワークがインターネット経由で接続されている場合があります。この場合、拠点間にVPNを設定することにより、拠点間通信を拠点内通信と同様のセキュリティレベルで提供できます。また、学外にいる組織構成員がVPNを使用することにより、安全に学内サービスを利用することができます。ただし、VPNの情報セキュリティを維持するために、システム管理者はVPN接続鍵の有効期限設定、紛失時の無効化設定等を行う必要があります。

**第３章 ネットワークサービス・システムを構成する要素技術**

　情報セキュリティを維持するためには、ネットワークサービス・システムを構成する技術要素を理解することが必要です。ここでは、基礎的なネットワーク技術要素の項目を列挙します。詳細な内容については、それぞれの技術要素の文献を参照してください。ネットワーク技術は進歩の激しい分野ですので、最新技術の動向を常に把握する必要があります。

　なお、ここに示した要素技術についての教科書や文献は豊富に提供されていますので、詳細はそれぞれの教科書・参考書を参照してください。

3.1　IPアドレス体系

　IPアドレス体系を構成するための技術要素の例を以下に示します。IPアドレスの確保や管理は大学内の情報資産管理の一環として重要です。IPアドレスにおけるクラスの概念などを熟知しておく必要があります。

- IPv4 / IPv6

- グローバルIPアドレス / プライベートIPアドレス / リンクローカルアドレス

- Classless Inter-Domain Routing（CIDR） / Variable Length Subnet Masks（VLSM）

- well known port

3.2 パケットフィルタリング

　パケットフィルタリングを構成するための技術要素の例を以下に示します。パケットフィルタリングはアクセス制御に使われる重要な概念です。

- アクセスコントロールリスト（ACL）

- IPアドレスフィルタリング

- Reverse Path Forwarding（RPF）

- ICMP

- プロトコル・ポート番号フィルタリング

- IPフラグメント

- ステートレスフィルタリング / ステートフルフィルタリング

- 流量制限

3.3 NATとNAT越え（超え）

　NATを構成するための技術要素の例を以下に示します。NATは学外向けのIPアドレスであるグローバルIPアドレスと、学内向けのIPアドレスであるプライベートIPアドレスを変換する機能です。グローバルIPアドレスを持たないものが、サーバ機能を外部に提供する場合やP2P通信を行う場合などに「NAT越え」が必要となります。NAT越えは大変便利な機能ですが、情報セキュリティ上のリスクを招く恐れもあります。したがってネットワークの管理者・システム管理者は、利用実態、関連インシデントなどに気を配る必要があります。また、NATを設置する場合には、インシデント対応を容易とするためセッションログをとるようにするのが好ましいと言えます。

- Network Address Translation（NAT）

- Network Address Port Translation（NAPT） / IPマスカレード

- NAT越え

- 静的マッピングテーブル

- Universal Plug and Play（UPnP）

- TCP connection reversal

- UDP hole punching

3.4 MAC（Media Access Control）アドレス

　MACアドレスはイーサネットワークを構成する機器に付けられたユニークなアドレスであり、機器管理の基本情報の一つです。ネットワークの管理者・システム管理者は概念を熟知する必要があります。MACセキュリティの例を以下に示します。

- MACアドレス

- MACアドレス認証

3.5 無線LAN

　無線LANを構成するための技術要素の例を以下に示します。安易に無線LANを設定することは、ネットワークにおける情報セキュリティ上のリスクを生じさせる原因となります。ネットワークの管理者・システム管理者は利用実態、関連インシデントなどに注意する必要があります。

　- 無線LANの標準規格

　- 認証・暗号化

- ESS-ID

- Wired Equivalent Privacy（WEP）/ Wi-Fi Protected Access（WPA2）

- IEEE802.1x / IEEE802.1i

　- RADIUS認証

解説：WEPはすでに数秒で解読される手法が発見されており、無線LAN機器を製造するベンダ間で作るWi-Fi AllianceにおけるWi-Fi認証を受けられない状況のため、速やかにWPA2-PSK等のより安全な暗号化方式に移行することが求められている。WPA2に対応していない無線LANアクセスポイントは更新が必要である。やむを得ずWEPにしか対応していないクライアント機器を接続する場合は、複数の暗号化方式を使い分けられる機能（マルチSSID）を備えた無線LANアクセスポイントを使用し、MACアドレス認証などによるアクセス制御を併用する。

**第４章　セキュリティサービス・システム**

　大学においても情報セキュリティに対する脅威が拡大し、情報システムの情報セキュリティ強化が必須となっています。情報セキュリティを危うくする原因（以下「セキュリティホール」という。）はあらゆる所に存在するため、情報セキュリティの維持はあらゆる観点から行われる必要があります。情報システムを中心に考えると、利用者の意識の低さ、利用組織・体制の不備、物理媒体を含めた情報管理の不備、組織情報システムを囲う物理環境の脆弱性、情報システムとしての論理的な脆弱性などが全て関連します。どこかにセキュリティホールがあれば、一部だけ強固な情報セキュリティを維持しても意味がありません。このことを念頭に置きつつ、以下では情報システムとしての論理的な安全性を確保することについて述べます。  
　システムとしての論理的な安全性を確保するために必要な対策（及び関連技術）は以下の通りです。それぞれの対策はそれぞれに対応する最新の技術に立脚しなければなりません。

①自己を正しく識別し正しく情報を伝え、他者を正しく識別し正しい情報を受け取るための対策  
（成りすまし防止、改ざん防止、事後否認防止、盗聴防止、電子証明書）

②迷惑を受けないための対策  
（フィッシング防止、ウイルス防止、迷惑メール防止）

③他者に迷惑をかけないための対策  
（踏み台防止、情報漏えい防止、ウイルス防止）

　これらの中で基本となる対策は、大学構成員の正しい識別（識別コード（以下「ID」という。）の管理）です。大学構成員の多様化に伴い、IDの管理が分散化する場合が見受けられます。このような分散を避け、情報インフラとしてのID管理と認証システムの確立が情報セキュリティ維持のための第一歩であるといえます。

　インシデントの大規模化に伴い、予防措置の重要性が増しています。ここでは、様々な予防措置の中から、侵入検知、監査、アンチウイルス、アンチスパムについて述べます。

4.1 大学構成員の識別

　大学構成員に付与するIDは情報システムの運用に欠かせない要素です。一般的に、学生は学籍番号、教職員は職員番号が付与されますが、これらのID体系は独立であることが多いようです。学籍番号は新学期に一括発行されます。情報システムログインのためのIDは、これらのID（またはそれから派生したID）が流用されるか、新規に付けられることになります。情報システムログインのためのIDには有効期限、再発行処理、パスワードの紛失対応などを行うシステム管理者が必要です。

解説：IDの種類ごとに管理元が分かれる場合がある。  
［構成員例（管理元例）］  
　ａ）学生（学務部）  
　ｂ）常勤職員（人事部）  
　ｃ）非常勤職員（学科）  
このため同一人物でも所属によりIDが変わる場合がある。例えば、学部生から大学院生になる時、学籍番号が更新される。  
以下にID種別例を示す。  
　ａ）管理元に対応したIDとして、組織構成員に付与するID  
　ｂ）組織横断的に個人に付与するID  
　ｃ）臨時に付与するID

4.2 ID管理の統一とIDを用いたアクセス制御

　付与したIDおよびそのIDに与えられた主体認証情報（以下「パスワード」という。）を用いて、学内サービスへのアクセス制御を行うことが広く行われています。パスワード設定ポリシーを定義しておくことにより、安易なパスワードの付与を避けることができます。

　地域交流センター、後援会、宿舎、インキュベーションセンターなどの学外の関連者にIDを付与する場合はその属性を分け、完全なアクセス管理ができるようにしておく必要があります。

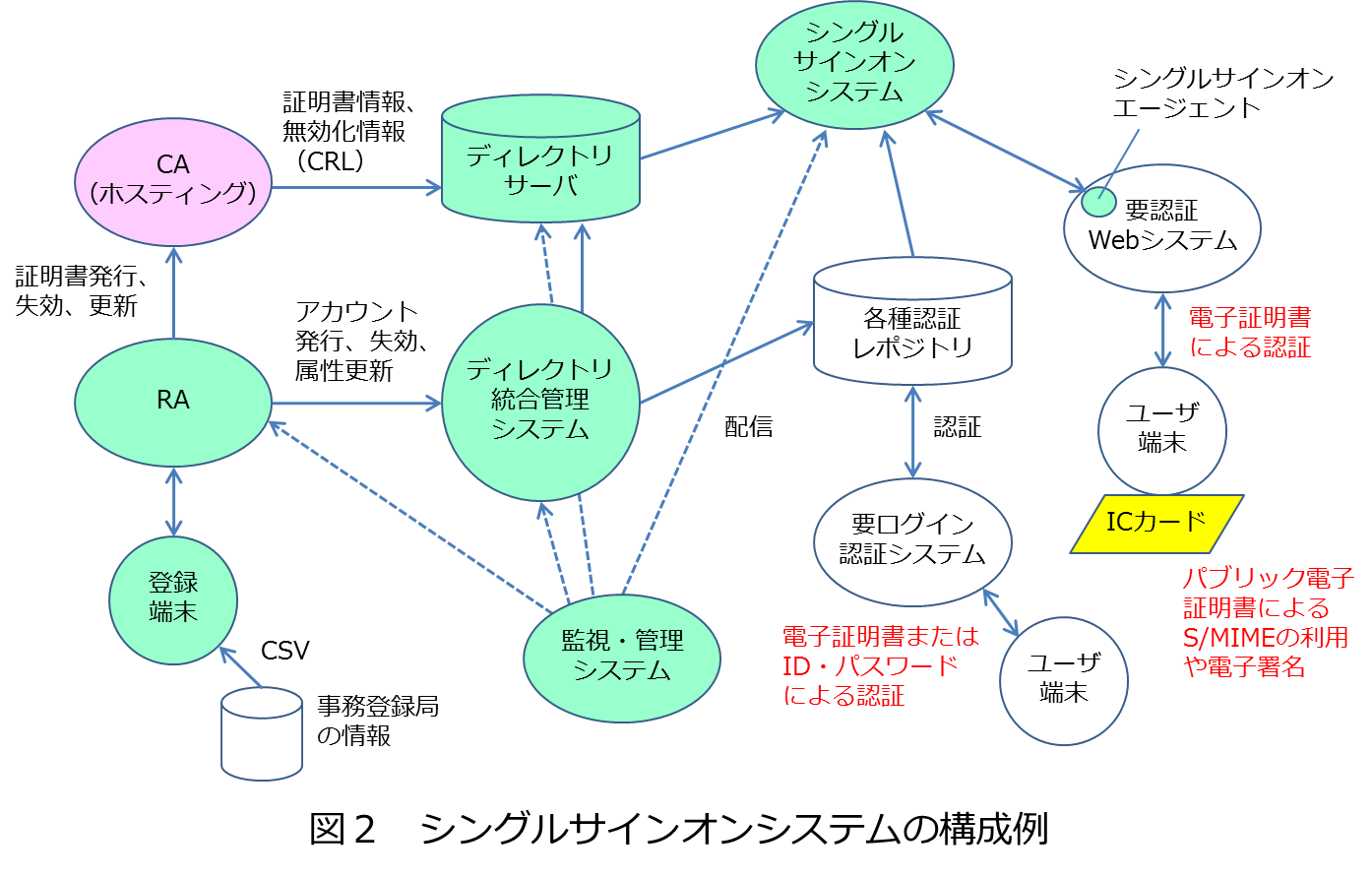
　中小規模の大学ではIDの管理元が一元化され、その結果ID付与体系の一元化に問題が起こらないのが一般的です。しかしながら大規模な大学になると、システム毎にIDが与えられることもあります。このようなIDを効率的に管理するには、統一IDを組織横断的に個人に付与し、個人の属性として所属部局、アクセス許可サービスなどを登録するようにします。ただし、情報システム毎のIDから統一IDへの移行には、情報システム毎のID付与ポリシーの統一に関する問題をクリアしなければなりません。さらに、パスワード付与ポリシーも統一する必要があります。

解説：認証を要求される通信（高信頼な情報交換）には2者間の認証を用いることもできるが、多くの利用者種別とサービスが存在する場合には、公開鍵基盤（PKI: Public Key Infrastructure）による電子証明書を使うことにより、認証コストを削減できる。電子証明書では信頼のおける機関（以下「信頼点」という。）を介して認証する。信頼点として、学外に開かれた公的なレベル（パブリック）と学内に閉じる私的なレベル（プライベート）がある。ブラウザには信頼できる認証局（パブリック）の電子証明書（ルート証明書）が組み込まれている。  
大学におけるパブリックな証明書の利用シーンは、  
①大学情報公開時のサーバ認証、  
②電子商取引における個人認証、  
③大学間で交換する情報の認証、  
④物理トークンを用いたVPNへのアクセス制御  
などである。  
IDとパスワードの併用に比較したPKIの利点は、見破りやすいパスワード利用の害がない（セキュリティレベルが高い）、リアルシーンでの利用を含め多く応用シーンがある等であるが、サービス開始時のコストは高い。  
大学間のPKI利用を促進する動きとして、大学間連携のための全国共同認証基盤（UPKI）がある。UPKIイニシアティブが推進する。用途、目的、特徴は以下の通りである。  
　用途：大学間相互認証、ネットワークローミング、  
　　　　グリッドコンピューティング　  
　目的：学生・教員流動化への対応、導入・開発コストの削減、  
　　　　国際連携への展開  
　特徴：パブリックとも連携

4.3 統一IDとその応用（SSOアクセス制御管理）

　IDを使ったアクセス制御方式には、情報システム毎に設計する個別アクセス制御方式と一回の認証で多くのサービスへのアクセスを可能とするSSO（シングルサインオン）アクセス制御方式とがあります。SSOアクセス制御方式は利用者にとっては便利ですが、高度な機能（SSOアプリケーション）が必要になります。SSOアプリケーションがサービス毎のIDとパスワードを記憶しておく方式もありますが、情報システム間で統一したIDを用いると、SSOアクセス制御を大幅に効率化できます。学内の情報サービスが多様化すると、統一ID（ID管理ポリシーの統一を含む。）を用いたSSOアクセス制御による管理コストの節約とサービス性の向上が有効になると考えられます。

解説：統一IDを用いた情報システム構成例を図２（シングルサインオンシステムの構成例）に示す。SSOサーバの機能は、①利用者のアクセス制御を個別サーバ（サービス）に代わって行い、②必要とする利用者属性を個別サーバに渡す。さらに、③オンラインによるSSOアクセス制御を行わないサーバ（サービス）のために、IDとその利用者属性を供給する役目も果たす、場合もある。  
利用者属性を納めるデータベースをディレクトリデータベースと称す。ディレクトリデータベースにアクセスするプロトコルの一種にLDAP（Lightweight Directory Access Protocol）がある。  
なお、学外のクラウドサービスと認証連携を行うことによって、学内サービスで利用している統一IDをそのままクラウドサービスの認証に用いることが可能であるが、クラウド事業者に利用者属性を供給することにもなるため、特に注意が必要である。クラウドサービスのセキュリティについては、第7章で述べる。



4.4 インシデントの予防措置

大規模化するインシデント、複雑化する情報セキュリティ攻撃に対して、予防措置の重要性が高まっています。予防は物理・論理的にインシデントを防ぐだけではなく、利用者の意識向上ももたらします。

１）トラヒックパターンによるネットワーク侵入検知  
　特定のIPアドレス・ポートに対する集中的なアクセスなどトラヒックパターンの観察によりネットワークに対する侵入を検知する情報セキュリティサービスです。特徴的なトラヒックパターンを伴う侵入の試みを検知することができます。攻撃を受ける場合にも、踏み台となって学外サーバを攻撃してしまう場合にも有効です。ただし、攻撃を受ける場合はファイアウォールで防御しておき、学外または学内への意図しない攻撃の検知に用いられる場合が一般的です。欠点は誤認識があることです。

　大学では侵入検知後のアクションをあらかじめ確立しておくことが重要です。例えば、大学のサーバが踏み台となって学外サーバを攻撃してしまった場合、踏み台とされたサーバの管理者による迅速な分析・対応が不可欠です。アクションをあらかじめ確立しておかないと、迅速な対応ができません。

　コストはかかりますが、大学の情報システム維持に有効なサービスといえるでしょう。

２）サーバ監査（脆弱性評価）

　サーバの管理者の了解のもと、仮想的なアタックやサーバの分析（セキュリティホールの発見）を行います。評価コストを抑えるため、対象サーバが主要なサーバに限定されることもあります。セキュリティホールの種類としては、①OS、アプリケーションの既知の脆弱性、②見破られやすいパスワードの存在、③通信回線、サーバ装置の物理的状態など多岐にわたります。実施頻度は実情に応じて設定されます。評価結果はリスクのランクとともにサーバの管理者に通知され、対処が求められます。運用なども含めた総合的評価を行うことが一般的です。  
　安易に設定されたパスワードによるインシデントが後を絶たないなかで、その抑止力ともなります。

３）ウイルスとアンチウイルス処理

他のソフトウェア（宿主）の一部として自己を複製し、拡散させていくソフトウェアのことをウイルスと呼びます。これに対して、独立したソフトウェアの形態をとるのがワームです。特定の条件が揃うまで活動を抑制する場合があり、被害を拡大する一因となります。情報システムに様々な悪影響を及ぼしますが、具体的には、システム不安定・停止、バックドア、踏み台などの原因になります。利用者が気づかないうちに感染が広がることがあるので、他者にも多大な迷惑（損害）をかけることになります。

　こうしたウイルスやワームに対しては、しっかりした知識に基づき、感染予防、拡散予防に努めなければなりません。ウイルス発生に関する情報を常にチェックし、必要な対策をとることが重要です。不審なページへのアクセスや不審なソフトウェアをダウンロードしないなどの日常オペレーションにおける注意、ネットワークの入り口での対策、汚染された端末を持ち込まないなどの物理的対策が同時に必要となります。アンチウイルスソフトウェア（ウイルス対策ソフトウェア）を用いることも重要な対策であり、利用促進指導が必要です。また、キャンパス全体で対応しないと感染が収束しにくいものです。

解説：ウイルスの種類  
ワーム型：単独で活動できるプログラムを指す。宿主のファイルが必要な場合のみをウイルスと定義する場合もある。  
トロイの木馬型：見たくなるような画像やおもしろそうな文書になりすまし、電子メールに添付されたり悪意あるウェブサーバにアクセスすることで利用者に気づかれないように感染し、感染後に外部から遠隔操作できる機能を持っていたり、利用者情報の消去や不正持ち出し、システムを破壊するなどの動作を行うことがある。  
ボット型：ロボットに因んだ命名。侵入後、端末が第三者の意思のままに動作するようになる。このようになると悪意の集団行動に知らぬうちに加担させられてしまう。

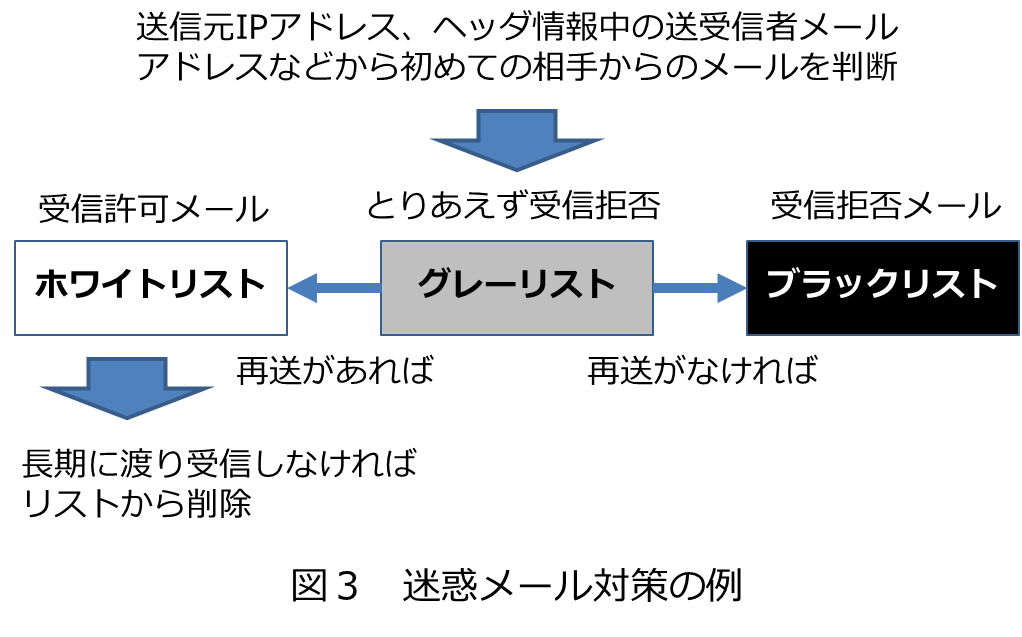
解説：感染経路と対策  
ウイルスの特徴を表すデータ（パターンデータ）を用いて検出するのが一般的である。新しいウイルスの出現に対して、パターンデータをいち早く更新することが重要である。メールの添付ファイルなどネットワーク経由で侵入する場合が多い。このため、大学ネットワークの入り口でウイルス侵入を防ぐ必要があるが、媒体経由、持ち込みPC経由などでも感染するため、端末毎の対策も不可欠である。ウェブ閲覧中にセキュリティホールを突かれて感染する場合もある。

解説：予防措置と対応組織の確立  
予防措置の実施においては異常時に即応できるよう、対応する大学の組織を整えることが重要である。政府機関の情報セキュリティ対策のための統一基準（内閣官房情報セキュリティセンター）や本サンプル規程集に従うことで、しっかりした組織を整備することができる。

4.5 迷惑メールと対策

　各大学とも迷惑メールが急激に増加しており、対応に苦慮しているのが現状です。完全な対応方法はありませんが、①メールアドレスの使い分け、②メールアドレスの公開を制限、③簡単に見破られないメールアドレスの利用などがあります。ネットワーク入り口での対処と、端末における対処を併用する場合もあります。

解説：迷惑メール対策には、ホワイトリスト方式、グレーリスト方式、ブラックリスト方式がある。図３（迷惑メール対策の例）に各方式の概要を示す。ホワイトリストは非迷惑メールのリスト、ブラックリストは迷惑メールのリストである。グレーリストは初めて受信するメールをリスト化したもので、このメールはいったん受信拒否される。ランダムに送りつけられる迷惑メールはほとんどの場合は再送されないが、非迷惑メールは再送される。再送されたメールは正常受信させホワイトリストに移行させる。メールの識別は送信元IPアドレス、ヘッダ情報中の送受信者メールアドレスなどを使って行われる。



このほかの迷惑メールを受け取らなくするための対策としては、送信元IPアドレスが正規なものであることを証明・確認する送信ドメイン認証、送信元IPアドレスの危険度評価に基づいてフィルタリングを行うE-mailレピュテーションなどがある。ただしこれらは送信側、受信側双方で対応する必要がある、危険度評価データベースの精度により誤判定のリスクがあるなど、解決すべき課題も残されている。

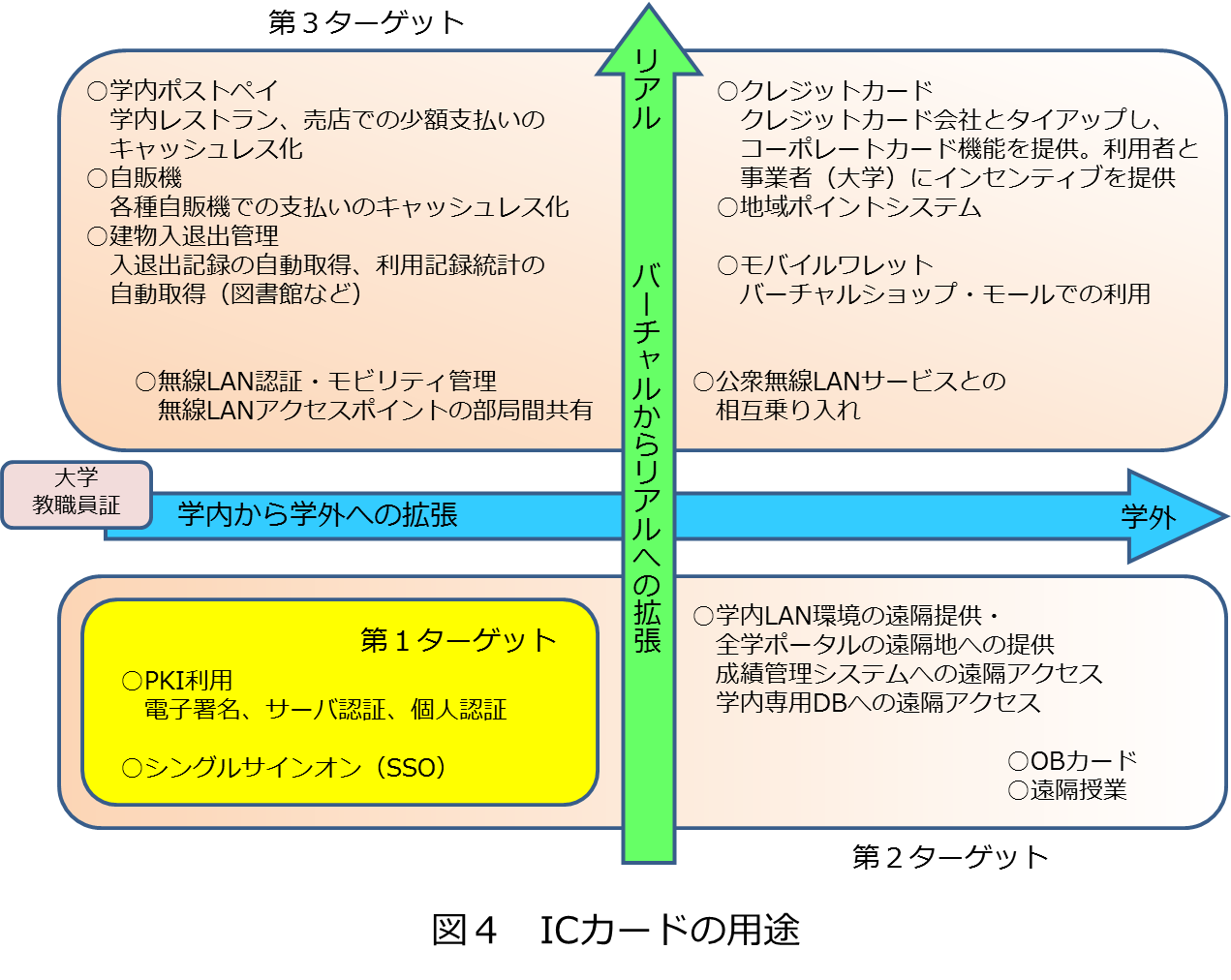
一方迷惑メールを送信しないようにするための対策としては、あらかじめ許可されたメールサーバ以外からの送信をブロックするOP25B（Outbound Port 25 Blocking）などがある。

受信者が行う迷惑メール対策としては、ベイズフィルタを応用して本文中に存在する特定の単語群をもとに迷惑メールの確率を予想し、振り分けを行う方法がある。本文の内容に基づく判断が可能であり、学習により判断精度を向上させることができる。プロバイダの中には極めて優秀な迷惑メールフィルタ機能を提供しているものもあるため、受信したメールをプロバイダに転送して振り分けを行う方法も考えられる。しかし、所属組織の情報セキュリティポリシーによっては組織外へのメールの自動転送が禁止されている場合や、プロバイダによってはこのような方法は利用規約に反していたり、大量のメールが転送されることにより組織全体が迷惑サイト判定されて受信拒否されたりする場合があるため、利用に当たっては注意が必要である。

4.6 主体認証情報格納装置

　実験室の入退出、図書館の入退館・貸出しなど、多くのカードがアプリケーション毎に使われていることがあります。アプリケーション毎に使われるカードは個別に管理されますが、主体認証情報格納装置（以下「ICカード」という。）を用いることにより、個別管理のコストを削減することができます。さらに、ICカードを応用した高度なサービスを提供できるようになります。即ち、ICカードは高度に情報化された大学の情報インフラとなることが期待されます。

解説： ICカードの用途を図４（ICカードの用途）に示す。その用途は、職員証、学生証、パブリック証明書（PKI）格納などが想定されている。



**第５章　セキュリティサービス・システムを構成する要素技術**

　セキュリティサービス・システムを構成するための要素技術の例を以下に示します。教科書や文献の豊富な分野です。詳細はそれぞれの教科書・参考書を参照してください。

１）公開鍵暗号による電子署名

２）認証・認可

３）暗号（秘匿）

４）改ざん検出

５）セキュリティプロトコル

**第６章　サーバ（アプリケーション、OS）のセキュリティ**

　サーバ（アプリケーション、OS）のセキュリティの例を以下に示します。教科書や文献の豊富な分野です。詳細はそれぞれの教科書・参考書を参照してください。

１）電子メールサーバ

２）ウェブサーバ

３）DNSサーバ

４）OSのセキュリティ

UNIX®

Linux®

Windows®

**第７章　クラウドサービスのセキュリティ**

　クラウドサービスはサーバ管理の煩雑さを軽減し、サービスの構築を迅速かつ低コストに行えることから注目を集めています。しかしその一方で、クラウドサービスはその運用の大部分がクラウド事業者の管理下で行われ、運用コスト最適化のため他の利用者とコンピュータ資源を共用する運用が行われるのが一般的です。そのため、データの保護・インシデントの管理など情報セキュリティに関する懸念が指摘されています。

　大学等においても、管理運用業務の効率化の観点からクラウドサービスの積極的な活用が望まれますが、クラウドサービスの利用にあたっては、事業者の選定、サービス内容の確認、責任体制の構築等を慎重に行う必要があります。また大学が所有する情報資産については、情報格付け基準等によりそれぞれの区分に応じた取扱いを定めて、提供されるサービスとの整合性を確認する必要があります。

　クラウドサービスのセキュリティを構成する要素の例を以下に示します。

１）情報の格付けとの整合性

取扱制限との整合性

利用組織の体制（責任者、担当者）

２）利用範囲の明確化

サービスの質（SLA）

機能とコスト

サポート体制

業務の継続性

３）事業者の選定

物理的セキュリティ

サービスの継続性

インシデントの管理

４）契約条件の確認

責任範囲の明確化

準拠法と管轄裁判所

データの所有権と返却・消去

解説：クラウドサービスのセキュリティを構成する要素は、一例に過ぎない。それぞれの大学およびクラウド事業者の実情に合わせて、詳細を検討していく必要がある。  
例えば、クラウドサービスを利用するにあたっては、情報の格付けだけでなく取扱制限にも注意が必要である。クラウド事業者が海外の場合は、外国法が適用されたり、外国の裁判所で裁判が行われる可能性があり、契約時（約款による契約の場合を含む。）に注意を要する。

**第８章　法令・基準**

　情報セキュリティに関連する法令として、内閣官房情報セキュリティセンター（<http://www.nisc.go.jp/law/index.html>）では、下記の概要と本文が紹介されています。

1. 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
2. 電子署名及び認証業務に関する法律（平成12年法律第102号）
3. 高度情報通信ネットワーク社会形成基本法（IT基本法）（平成12年法律第144号）

この他に、

1. 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダ責任制限法）（平成13年法律第137号）
2. 個人情報の保護に関する法律（平成15年法律第57号）、行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）、独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号）
3. 著作権法（昭和45年法律第48号）
4. 特定電子メールの送信の適正化等に関する法律（平成14年法律第26号）

などが、情報セキュリティ周辺に関係する法令として重要です。

　システム管理者は一通りの知識を持つことが望まれます。

解説：個人情報保護については、その法体系に注意する必要がある。すなわち、個人情報保護法の基本法的部分（第１章から第３章）は、私立大学・国立研究機関・国立大学・公立大学等のすべての学校・機関に適用されるが、個人情報取扱事業者の義務に関しては、私立大学には個人情報保護法の第４章以下、国立研究機関には行政機関個人情報保護法、国立大学には独立行政法人個人情報保護法、公立大学には地方公共団体が制定する個人情報保護に関する条例が適用される。  
著作権については、ウェブによって情報を公開する際に利用者が注意すべき事項を示すものとして、サンプル規程集の中に「B3254 情報発信ガイドライン」があり、その中で著作権法との関係についても触れられている。