経済産業省委託調査

平成１４年度情報セキュリティ基盤整備

ブロードバンドセキュリティに関する
調　査　報　告　書

平成１５年3月

電子商取引推進協議会

財団法人日本情報処理開発協会
電子商取引推進センター

序

ブロードバンドネットワークインフラの進展は、社会のネットワーク化を一気に加速するものと想定される。ネットワーク化の進展が豊かな社会構築に寄与するためには、このような社会における安全と信頼が確保されなければならない。本調査研究は、ネットワーク社会の進展に先立ち、その安全と信頼の確保のために必要な取組みを明確化することに挑戦したものである。

まず、ネットワーク社会の安全と信頼の確保の環境を理解するため、ブロードバンドネットワークインフラの普及がもたらすネットワーク社会像についてのスケッチを行った。ネット利用技術の進展を睨みながら、社会のさまざまな分野において、新たに登場したり、爆発的に普及が想定されるネットワークの利用を、ブロードバンドネットワークの特性とユビキタスコンピューティング環境の進展がもたらすシステム技術を背景に検討した。この結果、すぐではないにしろ、近い将来、ネットワークの利用は社会の隅々まで浸透し、個人のライフスタイルも含み社会の仕組みに相当な変化が生じることが指摘された。

社会の仕組みがネットワークへの依存度を強めることにより、社会の安全と信頼について新たな課題が生じる。本調査研究では、これからの社会において想定されるネットワークの利用場面を前提に、想定される新たな脅威またはより深刻になる脅威を考慮し、今後、取組むべき課題を検討した。

これらの議論により、さまざまな課題を示唆するとともに、今後必要となる取組みについての提案も示されたが、検討の対象分野があまりにも広く、個々に課題については議論が尽くされているとは言えない。本年度の活動は、今後の本格的な議論を行うための枠組み作りにあったといえる。

次年度は、本年度の成果を踏まえ、重要とされる課題についての議論を尽くし、政策立案や技術開発についての具体的な提案に結びつけたい。

最後に、本テーマの活動にご協力いただいた関係者各位に対し、厚く御礼申し上げる次第である。

平成15年3月

財団法人日本情報処理開発協会
電子商取引推進センター
電子商取引推進協議会

目　次

1　ネットワークの利用を高度化する技術

1.1　　ネットワークの利用を高度化する技術

ブロードバンドネットワークに代表される高速大容量のネットワークの各家庭に至るまでの普及と、ネットワークインフラの普及を背景とした IT 関連機器の進化ならびにさまざまな機器のインテリジェント化とネットワーク化は、ネットワークの利用にあらたな潮流を生起すると考えられる。

ネットワーク社会の進展を加速すると見られるブロードバンドネットワークやユビキタスコンピューティングの利用技術のうち、社会のネットワーク化に大きく影響を与える代表的な基盤技術としては、以下のものがあげられる。これらは、e-コラボレーションや e-コミュニティ、e-ワーク等を実現していく上で欠くことのできない技術となる。

代表的なものとしては、以下があげられる。

- テレコンフェランスシステム（遠隔対話システム）技術
- 情報交換システム技術
- リモートモニタリングシステム（遠隔監視システム）技術
- リモートコントロールシステム（遠隔操作）技術

これらの技術は、いずれも特に新しいものではないが、これまではネットワークの容量や料金がネックとなって、広く普及するまでには至らなかったものの、ブロードバンドネットワークの持つ高速大容量性、料金を気にしなくてよい程度の低価格性、常時接続性、全国津々浦々に至るまでの各家庭に至るまでの普及によるグローバルレベルでのピアツーピア通信の実現する接続性という特性により、これらを活かした機器やシステムの提供が広まれば、爆発的に普及して行くものと思われる。

このようなネットワークの利用技術の進展は、遠隔地にありながらネットワークを介して協同作業を行うリモートコラボレーションや、同時に同じ場所にいるような深いコミュニケーションを可能とするマルチメディア・コミュニケーション、オフィスに出向かなくても業務の遂行ができるｅワーク、ネットを介して何処からでも都合の良い時に学習することを可能にするｅラーニングといった利用形態をさらに成長させる。また、さまざまな情報へのアクセスや、個人の生活においても、離れた場所からのさまざまな機器の操作の利用も広がると見られる。

今後、大きく進展すると考えられえるネットワークやユビキタスコンピューティングの象徴的な利用場面としては、以下があげられる。

- 離れた場所にいる者との、音声、画像、データを駆使したフェースツーフェースライクな対話、情報の交換、共同作業の実行（リモートコラボレーション）
- 求める情報の入手
- 行政サービスや医療サービス、金融取引等の社会サービスの利用
- ネットワークを介しての業務の実行
- 遠隔地からの自分の管轄下にあるものや特定の事象についての遠隔地からのモニタリング

- 遠隔地からの機器の操作
- 社会への情報の発信
- 離れた場所にいる者とゲーム

ネットワークやユビキタスコンピューティングの利用技術と、今後進展するこれらの利用形態との関係を、図 1-1 に示す。

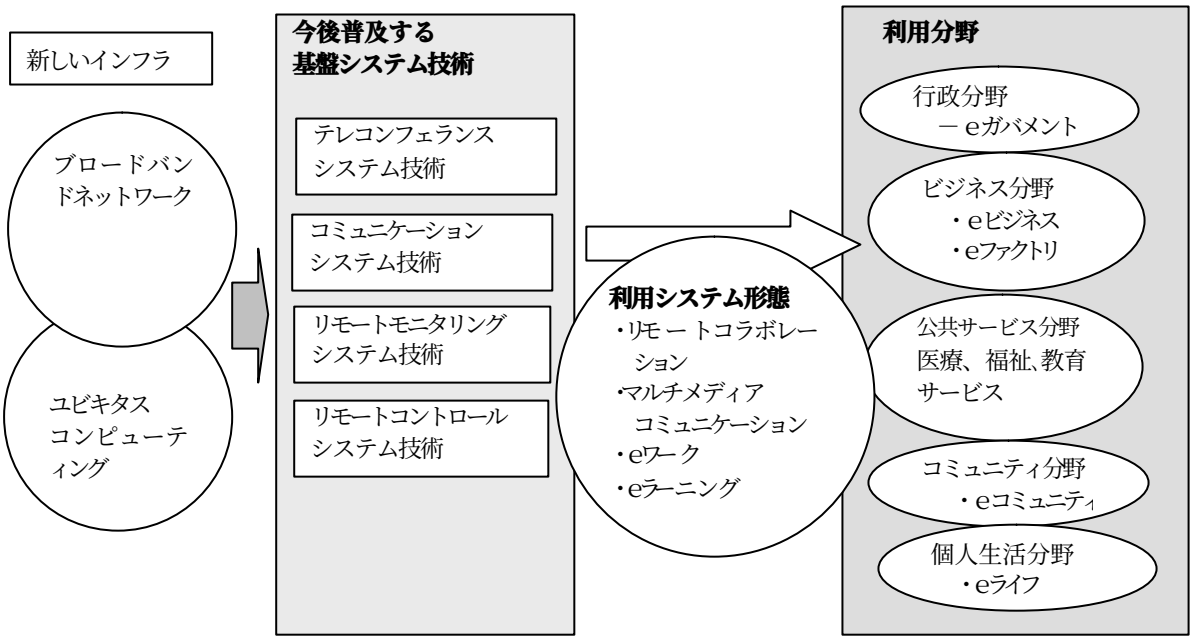


図 1-1 ブロードバンド時代の基盤技術と実社会へのインパクト

1.1.1 テレコンフェランス技術

音声、画像、映像、データ等のさまざまなメディアを同時に交換することにより、離れた場所にいる者同士のフェースツーフェースライクな対話を可能にするものである。現在の通信手段の主流である電話、FAX、メールのメディア別の通信は、徐々に、これらを統合したよりこの高機能なテレコンフェランスに吸収されて行くものと見られる。

ブロードバンドネットワークが普及した時代は、何時でも、どこからでも、どことでも、ピアツーピアまたはそれぞれが異なった場所にいる複数の者同士の対話も可能となろう。特にブロードバンドネットワークの導入によって変化すると思われるのは以下のような領域と考えられる。

- 高精細化 :物の質感を十分伝える精細な画像の利用、十分な臨場感を伴う音響の利用
- 高視野化 :対象とする人物や物だけではなく、その周辺の画像までも全てを伝達することによる環境の共有

- 同時並行利用 :複数の地点で複数の人々が周辺環境を含めて画像や音響情報の共有
- マルチメディア化 :紙上の情報、画像情報、コンピュータ上の情報、他のメディアの情報を複合的に利用することができる環境の実現
- これらの技術が活用されることにより、従来は意識して通信をしていた状態から、離れたままで環境を共有して会議ができるところまで技術を進化させることにより、同じ場所に集まっているのと変わらない対話環境を生み出すことが可能となるものと期待される。最終的には、テレコンフェレンスでの契約行為が実世界での契約行為と同じ意味を持つところまで行き着くことができれば、社会的なインパクトはさらに大きくなると考えられる。

そして、このようなシステムの普及は、社会におけるコミュニケーションのスタイルを一新させ、仕事の場においても社会におけるさまざまな人同士の交流のスタイルも変質させると考えられる。

1.1.2 コミュニケーション 情報交換）システム技術

ネットワークの普及とさまざまな機器のネットワーク化は、人同士､人とシステムとの情報の交換がますます高度かつ便利にするだけでなく､機器あるいはシステムと機器やシステム間での情報交換も自由になる。

表 1-1 に､人や機器やシステム相互間において､今後進展すると考えられる情報の交換の一例を示す。

表 1-1 高度ネットワーク社会における人や機器あるいはシステム相互間の情報交換

コミュニケーション区分	目的	効果
1 人同士のコミュニケーション	･対話、情報の交換 ･デジタルコンテンツの交換	・よりフェースツーフェースライクなリモートコミュニケーション ･情報交換の利便性の向上
2 人とシステムあるいは機器とのコミュニケーション	・さまざまな情報の検索、取得 ・リアルタイムでのシステムや機器の状況の把握や機器やシステムの提供する情報の取得 ･システムや機器に対するリモートコントロール	･機器の機能の向上 ･機器のつかい勝手の向上 ･機器使用の安全性の向上
3 機器あるいはシステム間におけるコミュニケーション	・システムや機器相互間での動作状態の把握 ・システムや機器相互間での情報の交換 ･システムや機器相互間での相互リモートコントロール	･該当設置機器殻の情報の収集 ･該当設置機器の制御 ･機器同士のコラボレーション

1.1.3 リモートモニタリングシステム技術

ブロードバンドネットワークの高速大容量の通信路が、低価格で常時接続で利用できることから、関心があるものに対する映像による観察が個人レベルでも利用可能となる。このようなネットワークの利用は、以下に示すような応用場面がある。

- 外出先からの家庭の状況の観察
- 保育所に預けた子供の様子や学校の様子の観察
- 寝たきり老人家庭に対する親族からの状況の観察
- 介護対象者がいる家庭に対する親族または介護担当者からの観察

プライバシーの問題もかかわるが、このような機能は生活の安全のためにも求められるものになろう。これを実現可能にするのが、ブロードバンドネットワークの常時接続性、ピアツーピア通信、そして観察の対象者と観察者が環境を共有していると言える程の密度の高いフェーツーフェースライクな対話環境を提供する高速大容量性という特性である。

また、このような技術はビジネスや公共、産業の分野にも大きなインパクトを与えることになろう。

1.1.4 リモートコントロールシステム技術

さまざまな装置がそのインテリジェント化の一環としてネットワークされ、その自動制御の拡大と設置場所から離れたところからのリモートコントロールの拡大も、ネットワークの利用分野の新たに普及する一つと言える。

プラントの各種装置、銀行オンラインシステムの屋外設置の ATM のような組織の敷地外に置かれた装置、各種の観測機器等に対する遠隔操作は、従来からも行なわれてきたものであるが、ブロードバンドネットワーク時代にあっては、

- 個人レベルでの使用となる家庭内に置かれた各種生活機器に対するリモートコントロール
- さまざまな街頭設置の機器のリモートコントロール
- 工場内の生産設備や装置のリモートコントロール
- 各種の装置間での自律的なコラボレーション

が、新たな対象としてクローズアップされよう。既存の遠隔操作では多くの場合、通常の操作時には問題が無くても、何か異常が起こる可能性のある場合の操作判断を下すことは難しい。これは判断をするためのデータ、例えば目、耳、におい等５感に訴える情報や、対象装置以外の周辺の情報等、人間が総合判断を下すのに必要な情報が十分ではないことが原因となっている。ブロードバンドネットワークが普及した社会においては、遠隔地にある設備や装置に対してもネットワークやセンサーを最大限活用して、操作者が現地と環境を共有することができるところまで情報量を飛躍的に増やすことにより、より高度な判断領域まで遠隔操作が可能となるものと期待される。

1.2 新たにクローズアップされるネットワークとITの利用形態

先にあげたような新しいネットワークの利用技術を駆使することにより、社会の個人の生活におけるさまざまな活動に新しい形態が登場する。ブロードバンドネットワークが普及した時代において、社会活動のベースとなるようなネットワークとITの利用形態としては、以下をあげることができる。

- リモートコラボレーション
- eワーク
- eラーニング
- eコミュニティ
- デバイスツーデバイスコラボレーション

以下に、それぞれのイメージを示す。

1.2.1 リモートコラボレーション

リモートコラボレーションとは、離れた場所にいる者あるいはチーム同士が、1.1.1 節にあげた高度テレコンフェランスシステムを用いて、データの交換や、作業の指示、意見の交換等行い、同じ場所にいるのと同じようなレベルの共同作業を行うことを言う。

(1) リモートコラボレーションのイメージ

図 1-2 に、自動車のサービスステーションにおける、故障した車両の診断や修理の実施におけるリモートコラボレーションの利用イメージを示す。

この例では、地方のサービスステーションに持ち込まれた故障車に対する、診断と修理はサービスステーションのエンジニアがあたっているが、このエンジニアはその作業を、サービスセンターの上級エンジニアから、テレコンフェランスシステムを用いフェースツーフェースライクな指導も受けながら、サービスステーションにある技術データベースや、顧客サービスセンターにあるデータベース上の当該車についての過去のメンテナンス記録等の情報を参照しつ行なっている。必要に応じては、当該車両を製造した工場の品質管理部門や設計部門の設計者も、その作業に参加させることができる。

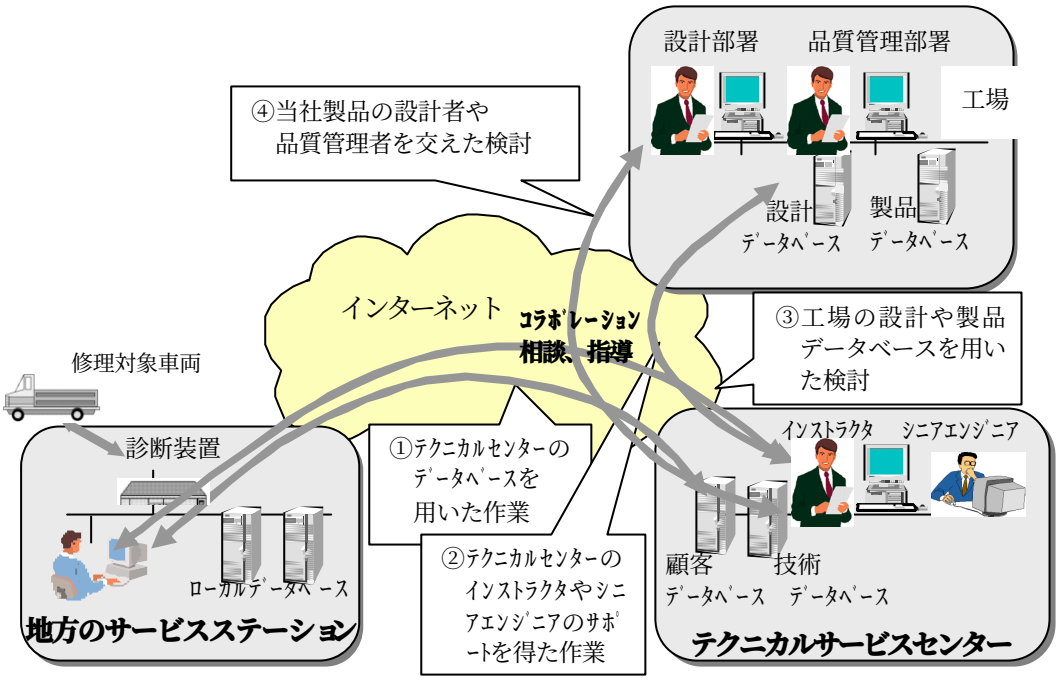


図 1-2 リモートコラボレーションの利用イメージ―車両の修理作業への利用

このような場面へのリモートコラボレーションの利用は、この作業に対し以下のような貢献ができる。

- どんな遠隔地にあっても専門的な技術支援を受けることができ、短時間で問題の解決ができる
- 場所に関係なく同じレベルの(最高の)技術支援を受けることができる
- 上級のテクニカルサポートスタッフは一箇所に集中化でき、専門家チームの有効活用ができるだけでなく、情報やスキルの集約で上級スタッフのさらなるレベルアップを図ることができる
- 情報やスキルの集約は、技術そのもののレベルアップを促進し、製品へのフィードバックもできる

(2) リモートコラボレーションのメリット

離れた場所にいる者あるいはチームが、それぞれの居場所から移動することなく、一体となって問題の解決にあたることができるこのシステムの利用は、一般に、以下のような大きな効果をもたらす。

- 問題解決のスピードアップ

  担当者で問題が解決できない場合、その場で、離れた場所にいる問題解決に必要な者を、ネットワークを利用しその場の検討や作業に参加させることと、組織の持つあらゆる情報の活用ができることにより、問題解決のスピードアップが図れる。

  問題が深刻な場合や、解決に緊急を要するような場合には、特に有効なシステムである。

- 指導員や専門家の有効活用の促進

  このようなシステムが何時でも活用できれば、指導員や専門家はどこにいても、全社的に活用できるため、一箇所への集中配置が可能となり、分散配置に比べ、専門チームの運用の効率化やレベルアップが期待できる。また、多くのケースでは、現場に出向く必要がなくなるため、指導員や専門家の移動に要する時間をなくせ、その分、研究等の活動を行なうこともできる。

- 情報の共有の促進

  上級者や専門家の集中配置を行なうことにより、これらを核とした全社的なコラボレーションの日常化する結果、情報の集中管理が進み、組織における情報の共有とその活用はより進んだものになることにつながる。

- 対象業務に対する組織全体としてのスキルアップ

  現場で問題が発生した時の問題の解決にあたり、全社レベルでの指導員や専門家のサポートの日常化は、その問題の解決を通じて、現場のその作業についてのレベルアップにつながる。また、この指導を通じ、作業マニュアルや関係要員に対する教育についても問題発掘もできる。

1.2.2 eワーク

何時どこにいても、オフィスのデータベースへのアクセス、組織のシステムへの処理の指示、組織あるいは顧客や取引先等とのフェースツーフェースライクな対話が可能となれば、外出先や自宅にあっても、オフィスにいるのと同じように業務を進めることができる。

テレコンフェランスシステムの普及等、ブロードバンドネットワークとユビキタスコンピューティング環境がもたらす、現在より一歩進んだこのようなことを可能にする環境は、勤務スタイルにも大きな変化を与える。eワークはブロードバンドネットワーク時代における、ネットワークの利用の中心の一つになろう。

1.2.3 eラーニング

電子化した教材をインターネットなどの情報メディアを通じて受講者に提供し、いつでもどこでもからでも学習できるようにしたシステムを言う。ディスタンスラーニングとも呼ばれる。そのイメージやメリット、利用分野は以下の通り。

(1) eラーニングの形態

eラーニングでは、スクール式の授業を値とを介して提供するもの、学習者の都合に応じて個別に提供される個人レッスン、学習システムにアクセスすることにより自習を行うといった形

態に分けてみることができる。

① ネットワークスクール

ネットワークスクールは１対ｎのスクール型の学習方式で、テレコンフェランスシステムが普及すれば、教える側および共に学んでいる者同士の対話や、教材への映像の活用等で、授業の質も向上すると思われる。

② オンデマンド個人レッスン

オンデマンド個人レッスンは、テレコンフェランスを利用した一対一の指導である。受験家庭における家庭教師の活用もフェースツーフェースライクな対話環境が普及すれば、ネットワークの利用が主流になる可能性もある。

③ 学習システムによる自習

ネットワーク型の教材を利用し自習するシステムで、システムによっては、テレコンフェランスシステムを用い指導員にアクセスし、フェースツーフェースライクな対話を用いた指導を受けることも可能となる。個人の都合によい時に、個々人が必要な範囲について徹底した学習ができるため、企業との組織における業務上の学習には大いに有効なシステムとなろう。

(2) ｅラーニングのメリット

受講者にとってのメリットとしては、以下があげられる。

- 時間と場所の制約から解放
- 一級の講師による講座が受講可能

また、学習指導者側から見たメリットとしては、以下があげられる。

- 教室の確保が不要
- 講師のスケジューリングが容易
- 学習状況の管理が容易

(3) ｅラーニングの応用場面

eラーニングは社会におけるさまざまな分野での適用が考えられるが、代表的なものとしては、以下があげられる。

- 学校（教室でのカリキュラムを補完）
- 企業内教育（従来の社内研修を補完）
- パートナー企業に対するトレーニング（新製品に関する情報提供）
- 業界内研修（研修者が相互に啓発）
- 生涯教育（大学等の公開講座や従来の通信教育に代わるもの）

1.2.4 eコミュニティ（ネットワークコミュニティ）

コミュニティ活動の基盤を、ネットワーク上のシステムを中心としたネットワークによるコミュニケー

ションやコラボレーションにおいたもので、その便利さとコストのかからないことから、今後は、コミュニティ活動は、このようなネットワーク型のものにシフトするものと思われる。

このことは、個々の活動をより効率化するだけでなく、真に貢献できるの者の参加を可能にするため、活動の活性化にもつながる。

コミュニティ活動におけるネットワークの利用分野としては、以下があげられる。

- 活動の案内
- 参加者の募集
- 活動成果の発信
- 会員管理
- 活動管理
- ネットワークを介しての作業
- 会員間のコミュニケーション支援

1.2.5 デバイスツーデバイス

オフィス、家庭、街頭、工場にある様々な機器はネットワークに接続されていくことになる。既に、オフィスにあるコピー機はほとんどのものがメンテナンス目的他で、ネットワークで監視されている。また、エレベーターも同様である。家庭内に目を移しても、テレビ、ゲーム機等は既にネットワークにつながれ始めており、電子レンジや冷蔵庫までもネットワーク対応を意識したものになりつつある。自動車の中も、カーナビゲーションシステムを中心にネットワーク化が進みつつある。また街頭でも、多くの自動販売機、無人駐車場システム、キオスク等がネットワークでつながっている。工場の中でも、メーカーによる保守を必要とする装置は、ネットワーク経由で監視されているものが増えてきている。

今後もこのような動きはとどまらず、ブルートゥースや無線 LAN（IEEE802.11）、IEEE1394 や電灯線ネットワーク等、家庭でも利用可能な低コストで、新たな工事が不要なネットワーク技術の浸透に伴い、様々な機器が相互につながれ、自律的なコラボレーションを行うようになると考えられる。

ブロードバンドネットワークの進展につれて、これら通信用の技術が非常な低コストで利用可能となり、利用が大きく広がっていくこととなろう。

デバイスツーデバイスの適用対象としては以下のようなものがあげられる。

- 家庭内機器（AV 関連機器、電化製品、PC、ゲーム機・・・・）
- 街頭機器（自動販売機、キオスク、掲示板、街頭カメラ、・・・・・・）
- ITS（自家用車、バス、公用車、タクシー、道路監視機器、交通信号、・・・・・）
- 工場内機器
- オフィス内機器
- 社会インフラ系設備（鉄道、バス、水道、通信、電力、ガス、・・・・・・・）

2 高度ネットワーク社会の具体像

ネットワークやユビキタスコンピューティングの利用技術がもたらす、高度ネットワーク社会の具体像を示すため、行政機関、公共機関、一般企業、社会サービス、コミュニティ活動、および個人生活分野におけるネットワークやユビキタスコンピューティングの利用イメージを示す。

2.1 行政機関におけるネットワークの利用

2.1.1 行政機関におけるネットワーク化の動き

e-Japan計画のもと電子政府構築の動きが加速してきた。政府は末端の行政機関に至るまですべてをネットで結び、行政活動の総合的なネットワーク化とIT化に積極的に取り組んでいる。

今後、行政分野におけるネットワークの利用分野は、各行政機関内部、行政機関間の連携、電子調達といった行政機関内の業務改革だけでなく、行政手続きのネットワーク化、行政サービスのネットワーク化や電子投票等に見られるような、社会のとのかかわり合いの部分にまで拡大する。

そして、これらは、政府・行政部門における業務や組織の在り方に根本的な変革を迫るものになろう。

2.1.2 行政機関におけるネットワーク化への期待

電子政府の進展は、

- 行政の効率化
- 行政サービスの向上
- 行政の質の向上

に大きく寄与するものと思われる。

(1) 行政の効率化

電子政府の狙いとして、まず、行政の効率化があげられる。行政機関内で所有している文書の電子化やデータベース化を促進することにより、文書情報の一元管理や職員間のノウハウの共有（ナレッジマネジメント）を行なわれる。また、既存業務を見直すことにより業務プロセスの再構築（BPR）を図ることで、電子決裁やワークフロー管理等の実現により、無駄のない効率的な業務を可能にする。これによって、事務処理コストのダウン、行政の生産性の向上につながる。

(2) 行政サービスの向上

電子政府の主要テーマの一つに行政サービスのワンストップ化があげられる。ワンストップ

化とは、多くの窓口業務を一つの窓口に集約することにより、サービスを一箇所で受けられるようにすることである。行政サービスのワンストップ化が実現すると、市民はその窓口に行けば、住民票や印鑑証明の交付、年金や福祉といった様々な用件を全て解決することができる。

今後、行政サービスの向上にあたり、行政のワンストップサービスを実現する上で、中央省庁、地方公共団体、政府関連機関など様々な組織に分散している行政サービスを連携させることが必要である。そのために、行政分野のネットワーク化は不可欠であり、また、ネットワークのブロードバンド化による動画や音声を使ったインタラクティブ性があるサービスの実現も期待される。

(3) 行政の質の向上

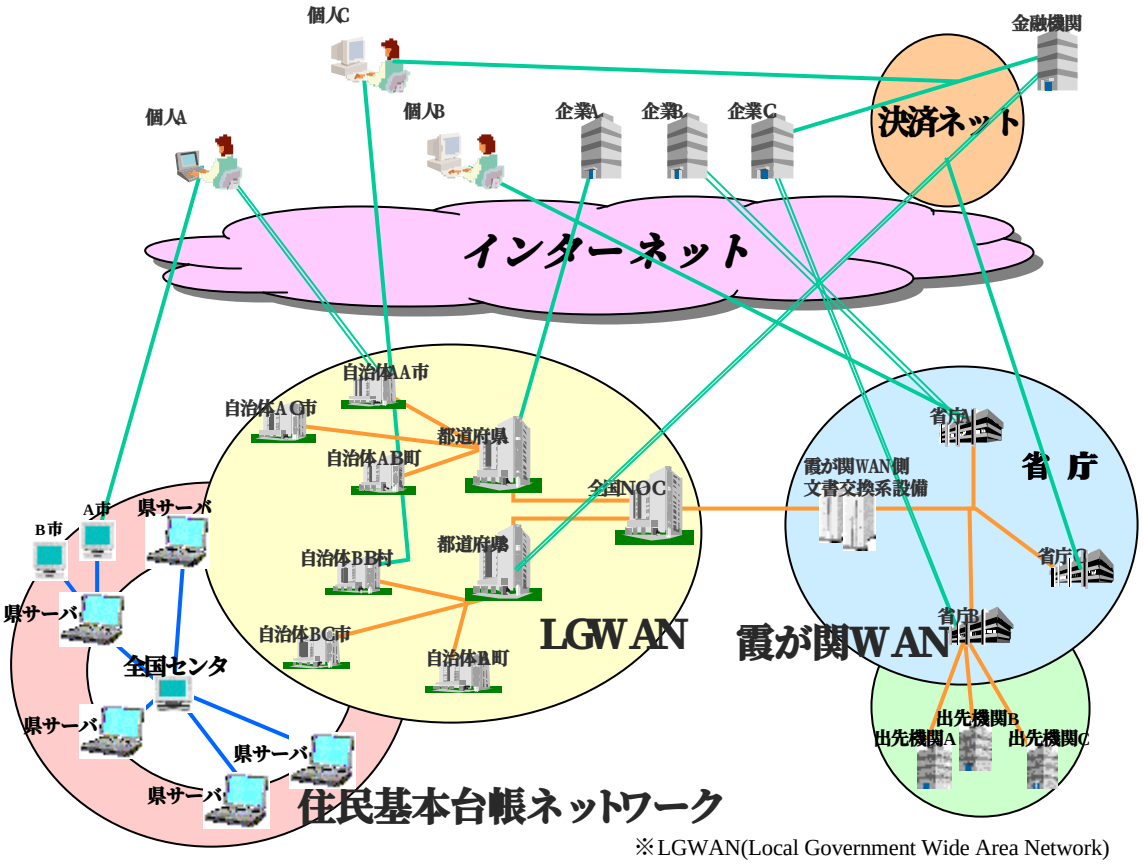
ネットを活用することによって行政自身の質の向上、すなわちデジタルデモクラシーが実現する可能性がある。例えば、インターネットを通じた選挙キャンペーンの実施、選出された議員とのコミュニケーション拡大、法制化プロセスのオープン化等にみられるように、政治家と行政、政治家と市民・企業間のコミュニケーションを密接にし、政治、行政、産業界、市民相互の距離を縮めることなどをあげることができる。

2.1.3 行政機関におけるネットワーク化の全体像

行政分野におけるネットワーク化の全体イメージを、図 2-1 に示す。

この図で示すように、中央官庁同士は霞が関 WAN で、都道府県庁や市区町村の役場は総合行政ネットワーク（LGWAN）で接続される。さらに、霞が関WANと総合行政ネットワークも相互につながれる。また、総合行政ネットワークとは別に、住民サービスの推進に向け、「住民基本台帳ネットワークシステム（住基ネット）」がある。住基ネットは、市町村を結ぶ県内ネットワークと都道府県を結ぶ全国ネットワークから構成される。また、これらの行政機関および関連機関もインターネットを介して、企業や各種機関、団体さらには一般家庭にまでネットワークでつながれる。行政機関同士だけでなく、行政機関とビジネス上で関係を持つ企業や行政のサービスを受ける国民、市民は、何時どこからでも行政機関にアクセス可能となる。

ネットワークの利用者は霞が関 WAN や LGWAN で接続されている中央官庁や地方自治体、各種行政機関を始め、行政機関にアクセスする個人や企業もネットワークを利用する。



※LGWAN(Local Government Wide Area Network)

図 2-1　行政機関のネットワーク化のイメージ

2.1.4　行政機関におけるネットワークの利用分野

行政機関の内部業務や行政サービスの提供におけるネットワークの利用分野は、大きくは①各行政機関内部業務、②行政機関間の連携、③電子調達、④行政手続き・サービスのネットワーク化、⑤電子投票、⑥ネットワークを用いた市民との対話に分けられる。

それぞれの利用分野における代表的な利用場面を表 2-1 に示す。

表 2-1 ブロードバンド時代における行政分野におけるネットワークの利用

	利用分野	代表的なネットワークの利用場面	社会的な重要性	想定される普及度合い		
				現在	5年後	10年後
1	各行政機関内部業務のBPR	業務プロセスの改革	○	△	○	◎
		データベース化とナレッジマネジメントの強化	○	＊	△	○
		業務のアウトソーシング	△		△	○
		リモートオフィス・モバイルオフィス 在宅勤務	△	＊	○	◎
2	行政機関間の業務連携の効率および質の向上	行政機関間における連携業務の業務プロセスの改革	○	＊	○	◎
		データベース化とナレッジマネジメントの進化	○		△	○
		テレコンフェランス・リモートコラボレーション	○		△	◎
3	電子調達（調達のネットワーク化）	公共調達	○		△	○
		物品調達	◎	＊	○	◎
4	行政手続き、行政サービスの質の向上と、利用者の利便性の向上（行政手続き、サービスのネットワーク化）	許認可･登録手続きのネットワーク化	◎	＊	○	◎
		各種証明書の発行	◎	＊	○	◎
		納税手続き	○		△	○
		公共施設の利用	△		◎	◎
		行政情報の提供	◎	△	◎	◎
		住民参加行事の主催	△		○	○
5	市民の政治への参加の推進（投票のネットワーク化）	選挙	△		△	○
		住民投票	△		△	○
6	行政への市民参加の拡大（ネットワークを用いた市民との対話の拡大）	各種世論調査	○	△	○	◎
		パブリックコメントの収集	○	○	◎	◎
		ネットワーク型公聴会	○		○	◎
		各種対話	△	＊	△	○

重要性
◎ 非常に重要、なくてはならないもの
○ 期待が高いもの
△ 重要性は低い、特に必要ではないが、あれば便利なもの

想定される普及の度合い
◎ ほとんどの行政機関に普及
○ 多くの行政機関に普及
△ 普及は一部に止まる
＊ 先行機関ですでに導入がみられるが、本格的な普及はこれから

また、これらのネットの利用は、その細部は別として、行政機関の種類によらず共通であると考えてよい。

2.1.5 各行政機関内部業務へのネットワークの利用

各行政機関内部のネットワーク化は従来からも推進されてきた。今後、高速・大容量のブロードバンドネットワークがインフラ化すれば、大量の情報を、どこからでもアクセスできるようになる。ブロードバンドネットワークの進展が、行政機関の業務を大きく変えるところとしては、以下があげられる。

- 業務プロセスの BPR
- データベース化とナレッジマネジメントの進化
- 業務のアウトソーシング
- リモートオフィス・モバイルオフィス

また、ネットワーク化の進展により、システム自体の共用を検討することが可能となる。たとえば、共同センターのような汎用システムを運用し、そのサービスを享受することにより行政業務が安価に実現できる。このため、資金的な理由などにより IT 化が遅れがちであった小さな地方自治体においても同質のシステムを利用することができるようになる。

(1) 業務プロセスの BPR

行政内部の業務には、複数の担当部門に責任が分担されているものもあり、各部門の担当者、責任者によって検討・決裁が行われる。時には複数の担当部門に処理を依頼する必要があり、時には、決裁のため、過去の経緯を確認する必要もある。高速大容量のネットワークが可能にする多種多様な情報の交換や、テレコンフェランスシステムは、上手に活用すれば、これらの業務における「ワンストップ化」と「スムースな決裁」を実現する行政機関内における業務のワークフロー化を進化させ、内部業務の BPR を大きく推進させる原動力の一つとなりうる。

高速・大容量のネットワークがインフラとして整備されれば、業務の処理にかかわる者の居場所を意識することなくノンストップのワークフローが実現するため、関係者が複数の場所に別れていても、それが作業に支障をきたすことは なくなる。また、例えば、決裁業務の場合、決裁判断に利用できる情報も文書情報だけでなく、画像・映像・音声といったマルチメディアファイルも取扱う事が可能となるため、より円滑な文書決裁業務の実現が期待される。

(2) データベース化とナレッジマネジメントの強化

行政機関が扱う情報としては、公開あるいは非公開の各種の報告書、行政の活動にかかわるさまざまな記録やデータ、国民や市民に関する情報、産業界に関する情報、環境に関する情報等のあらゆる分野に及ぶ。これらの情報は、これからは集中的にかつ体系的に集約さ

れ、ネットワークを活用して、何時どこからでも欲しい情報を欲しい形で瞬時にして手にすることができるようになろう。

ブロードバンドネットワークの提供する高速大容量のデータ伝送能力は、これまで、ネットワークの限界により間引いていた情報を、原情報ままの状態で送信することが可能となり、また、検索の対照をデータに限らず、画像や映像にまでその対象を拡大することができる。

検討や議論の場で即座に必要な情報を整理した形で提供できる統合行政情報バンクは、行政における判断をより迅速かつ的確なものにしてくれることが期待される。

(3) 業務のアウトソーシング

電子政府を構築していくためには、専門の業務知識や、それをシステム化するための IT利用技術、実現するための資金、期間が十分に準備されなくてはならない。本来、行政業務に携わる人々にとって IT は専門外であり、行政機関内部に IT の専門家が不足していることは、電子政府構築におけるボトルネックとなりうる。また、システム構築には、構築のコストが莫大に発生し、また、その運用にも費用が発生する。これは、予算に厳しい地方公共団体などにとっては、電子行政化推進を阻害する要因になりかねない。

この予算・人的資源の問題は、共通する汎用的なシステムの運用を外部に委託する方法で解決できる。また、行政機関と業務の委託先が安全で高速大容量のネットワークで結ばれていれば、多量の情報処理を必要とする行政業務も、庁内で処理しているのと変わらずに行うことが出来る。

また、行政機関は、住民や企業の個人機密情報を扱うことも多く、外部の業務委託先に対してこれを開示するのかという問題も発生するが、行政機関と業務委託先の間が、高速大容量ネットワークで結ばれていれば、外部の委託先に情報を預けておかなくても、必要なときに必要な情報のみを安全な形で提供する（蓄積させない）ことで、この点に関する問題に対処することも可能になろう。

(4) リモートオフィス、モバイルオフィス、在宅勤務

一つの行政機関もそのすべての活動が一箇所にあるオフィスで行なわれるわけではない。ブロードバンドネットワークの高速大容量性を活用したテレコンフェランスは、離れた場所にあるオフィス間の連携や、臨時の場外オフィスでのサービスや、外出先における業務の遂行もより円滑かつ効率的なものにするであろう。このような利用は、外部の有識者の活用も拡大できる。また、職員の自宅をネットワークで結べば在宅勤務もが可能となる。

リモートオフィス、モバイルオフィス、在宅勤務の効果的な活用は、職員の時点時点の居場所に関係かなく、常に、全職員が一体となった業務の遂行を実現するため、業務の効率化と質の向上にも大いに寄与すると考えられる。

2.1.6　行政機関間の業務連携へのネットワークの活用

行政機関相互においても省庁間、中央官庁と地方自治体、中央官庁と管轄の機関、地方自治体同士、地方自治体と警察、消防、学校、保険所等の関連機関相互間での業務の連携は多岐にわたる。これらの機関における活動においては、関連機関との間での、報告、指示、申請、認可等の行政事務上の諸手続きに加え、さまざまな協議が多くある。この分野でのネットの利用は、これらの行政機関相互間の連携のスピードアップと効率化を目指すものである。ビジネス界におけるバリューチェーンの構築と同じと考えてよい。

主な利用形態としては、以下があげられる。

- 行政機関間における連携事務の業務プロセスの改善
- データベース化とナレッジマネジメントの強化
- テレコンフェランスおよびリモートコラボレーション

(1) 行政機関間における連携事務の業務プロセスの改善

報告、指示、申請、認可等の行政事務上の諸手続きや、様々な協議など、行政は複数の行政機関の連携によることが多い。このような定型的な業務においては、それぞれの機関における内部業務のシステム化が進めば、産業界における SCM のようにワークフロー化することにより、業務のスピードアップと効率化および手続きのワンストップ化が進むことが期待される。

以下は、その先行システムの一例である。

- NACCS（厚生労働省、農林通産省、税関を結ぶ通関情報処理システム）
- MOTAS（陸運支局及び自動車検査登録事務所と国土交通省自動車登録管理室（センター）間をデータ伝送回線で結び、オンライン・リアルタイム処理方式により、自動車の登録・検査記録を一元的に管理するシステム

NACCS（Nippon Automated Cargo Clearance System の略：通関情報処理システム）は行政機関間の連携におけるネットワーク利用の代表例である。

ＮＡＣＣＳは、財務省税関、厚生労働省及び農水省と輸出入関連の民間業界（航空会社、通関業者、銀行など）をオンラインで結び、輸出入される航空貨物や海上貨物の通関に関する一連の手続き（食品関係、動物検疫、植物検疫など）及び関連民間業務を総合的に迅速かつ的確に処理する電算システムである。NACCS には、船により運搬される貨物に関する一連の手続きを処理する「Sea-NACCS」と航空機により運搬される貨物に関する一連の手続きをを処理する「Air-NACCS」がある。

ブロードバンドネットワークの普及により、各機関はデータのみならず画像や映像情報など、即座に欲しい情報を入手することができる。

ネットワークの高速大容量化とをもたらすブロードバンドネットワークの進展は、これらのシステムのさらに効果的なものにすることを促すことになろう。

(2) データベース化とナレッジマネジメントの強化

各層の行政機関が扱う情報を集中し、これらを体系化しナレッジ化した統合行政情報バンクを構築することにより、省庁間をはじめ各層の行政機関相互での情報の交流をより綿密なものにすることにより、

- 情報交換の高密度化と効率化
- 情報活用の高度化

が期待できる。ブロードバンドネットワークの高速大容量のデータ伝送能力は、データのみならず画像や映像の情報が手元になくても、欲しい時にその場で欲しい情報のすべてを入手できるため、情報バンクの役割をさらに効果的なものにしよう。ネットワークの高速性を活用すれば、この情報バンクは分散されていても一箇所に集中されたセンターと見ることができる。

統合行政情報バンクとは、各省庁・行政が発行している情報をネットワーク上にて一括管理を行い、情報の共有化を図るデータベースである。各省庁が発信している法令や通達、白書・年次報告書、基礎的統計情報その他の各省庁において利用価値の高い情報をデータベースとして、統合行政情報バンクに格納することにより、住民はネットワークを介して DB にアクセスし、各種情報を入手することが可能となる。また、オフィスや一般家庭にまで大容量通信が可能なネットワークが整備されることで、文字情報だけでなく、画像や音声などのマルチメディア情報を入手することができ、住民はより多くの情報の入手することが可能となる。

また、統合行政情報バンクは、住民に対する情報提供だけでなく、行政機関間における連携を効率的にも寄与する。現在、縦割り的に管理されている各省庁の情報を、統合行政情報バンクにて一元的に管理されることにより、各省庁をまたがる横断的な DB 化が進められ、情報を共有することが可能となる。

(3) テレコンフェランス、リモートコラボレーション

どの行政機関もその業務の遂行にあたっては、他の行政機関、外部の機関や関係者、企業等との連携も多い。情報の交換、連絡、協議等へのテレコンフェランスシステムをベースとしたリモートコラボレーションシステムの活用は、これら外部との連携をより迅速かつ効果的なものにする。

2.1.7 電子調達へのネットワークの活用

どの行政機関においても調達業務がある。電子調達は電子政府実現の主要テーマの一つとなっている。行政機関による調達は電子商取引の一環であり、

- 公共調達
- 物品調達

の大きく２つの形態がある。

(1) 公共調達

公共調達は道路や河川などに関する公共事業の調達を言う。公共調達の電子化とは、調達における公示から入札さらには契約までのプロセスにおける受発注者とのやり取りのほとんどをネット化するものである。調達手続きのネット化により、インターネットを通じて、参加条件を満たす者は、誰でも容易に入札に参加することができる。このシステムの下では、入札に参加している業者が受注者側には把握できないため、発注者側では談合による発注金額の値上げを防止することができ、また受注者側にとっても受注機会が拡大される。

ブロードバンドネットワークが整備されることにより、公示や入札段階で必要となる設計書データや建設に関する図面データ等の、大容量のデータをネット上でやり取りすることが可能となる。また、工事完成後の成果物を電子的に納品するために、CD-ROM・MOといった電子媒体ではなく、ネットを介して納品を行うことができる。

(2) 物品調達

物品調達は工事以外（行政機関内にて利用する備品を始め、コンピュータシステムそのもの）の調達のことを言う。物品調達の電子化とは、インターネットの公示から、確認申請、入札／応札、発注、契約などを、ネットを介して電子的に行えるようにするものである。

また、納入物品に関する情報も、今まで紙のカタログや電子文書で伝えていたものが、ネットワークを介して、画像データあるいは音声や映像による説明データなどをやり取りすることが可能となる。

2.1.8 行政手続き、行政サービスのネットワーク化

行政機関に対する各種の手続きや行政サービスをネットワーク経由で行おうとするもので、そのポイントは、ネットワーク経由での諸手続きの受付けとワンストップサービスであろう。

ネット化の対象としての行政手続きや行政サービスのネットワーク化の代用例としては、以下があげられる。

- 許認可手続き
- 各種証明書の発行
- 公共施設の利用
- 納税手続き
- 行政情報の提供
- 住民参加行事の運営

さまざまな行政手続き行政サービスは、さまざまな中央官庁、自治体の各機関が担当している。これまでは、これらの手続きを行ったりサービスを受けるためには、各々の機関で出向かなければならず、目的の手続きを行ったりサービスを受けるうけるには、どの機関へ行かなければならないかを知っていなければならず、利用者からは非常に不便を感じているものである。

これらの不便さを解消するしようとするのが行政ポータルサイトである。行政ポータルサイトとは総合窓口的なサイトを言い、このサイトにさえアクセスすれば、利用したいサイトへ容易にたどりつけるようにするものである。ポータルサイトの特徴としては、以下があげられる。

- ポータルを通じて行政機関をまたがり、様々な行政手続や行政サービスにアクセスできる
- 市民や企業等とネットを介した直接コミュニケートし、ネット経由での処理の完結を指向
- 提供形態

今後、ネット社会の進展にともない、市民や企業への行政の窓口は、この行政ポータルになると考えられる。

以下に、行政手続や行政サービスへのネットワークの利用イメージを示す。

(1) 許認可手続きのネットワーク化

行政機関におけるさまざまな許認可業務における申請、審査、認可のプロセスのほとんどがネットを介して行えるようにするものである。これからは、電子政府の進展と共に各行政機関が扱う許認可業務のほとんどがその対象になろう。また今後、ブロードバンドの普及に伴い、現在窓口で行なわれているサービスを、ネットワークを介した双方向通信により、窓口に出向くことなくても、窓口と同じようなサービスを受けることができる。

表 2-2 は、現在、各省庁がネット化を進めている手続き等の数を示すものである。

表 2-2 行政機関における電子化の対象となっている手続き等の数

省庁	ネット化の対象となっている手続き数	省庁	ネット化の対象となっている手続き数
内閣府	51	財務省	1,199
警察庁	138	文部科学省	472
防衛庁	36	厚生労働省	1,807
金融庁	1,257	農林水産省	960
総務省	751	経済産業省	2,162
公正取引委員会	20	国土交通省	1,793
法務省	186	環境省	222
外務省	69		

一方、地方自治体側の電子申請・届出におけるネット化の代表は、表 2-3 に示すようなものとなる。

(2) 各種証明書の発行

住民票等の行政機関が発行する各種の証明書も市民生活には欠かせないものである。これらの発行についての申請ならびに受領をネットを介して行えるようにするもので、利用者にとっては、わざわざ時間を作って出向がなくなるため大いに歓迎されるものである一方、役所のペーパレス化にも寄与する。これは、電子政府の主要テーマの一つである。

ネット化の対象となる各種証明書の発行業務の一例を、表 2-4 に示す。この表にあげたも

のはほんの一例にしか過ぎず、電子政府の進展とともに、証明書類の発行のほとんどはネット化されることになろう。

表 2-3 自治体における電子申請・届け出の区分とその例

区分	例
税金関係	相続税に関する届出、所得税に関する届出、贈与税に関する届出など
戸籍・国籍関係	死亡届、出生届、婚姻届、離婚届、帰化許可申請、戸籍・国籍関連申請・届出等
年金関係	厚生年金・国民年金に関する届出など
自動車関連関係	自動車検査証の交付申請、自動車の新規登録、変更登録、移転登録、抹消登録等
児童手当関係	児童補償手当の請求、児童補償手当の額の改定請求等
介護・福祉関係	公害医療手帳の再交付の申請、健康保険・厚生年金保険新規適用届等
生活関係	犯罪被害者等給付金又は仮給付金の支払請求、利用に関する手続（国立公文書館関係）等

表 2-4 ネットワーク化の対象となる証明書等の発行業務例

行政機関	各種証明書発行業務の対象
国税庁（税務署）	納税証明書の請求
地方自治体	住民票の写し等の交付の請求 戸籍の附票地縁による団体の告示事項の証明書の交付請求 市町村選挙の不在者投票用紙等の請求

(3) 納税手続き

住民・企業からの税金の徴収にもネットを用いることが検討されている。例えば、一般のサラリーマンが行う、還付申告などが 24 時間いつでも、都合のよい時間に行なう事が可能となり、納税者の利便性が向上する。

納税手続きにおいては、法人税や所得税といった「国税」、また自動車税といった「地方税」などの申告・税徴収にネットが利用されることとなる。

(4) 公共施設の利用

市民ホール、公民館、スポーツ施設、保養所、図書館等の公共機関が保有管理する施設の紹介や、利用状況の照会および利用予約の受付や利用許可書の発行業務等も、ネット化の対象である。利用の応募者が多い人気の公共施設の利用受付のネット化は、利用申し込みの受付は申込み手続きを便利にするだけでなく、その処理に工夫を行えばその利用をより公平なものにすることも可能となる。

(5) 行政情報の提供

従来は、公文書館や行政機関の資料閲覧室で公開したり、広報等の発行配布によって行

っていた公開の対象となる行政情報の提供が、現在でも、ネットを用いての提供が広がってきた。すべての人がネットワークの利用ができるわけではないことや、すべての情報が電子データ化されるわけでもないことから、すべての情報の提供がネット化されるわけではなく、従来の情報の提供手段に新たな手段を加えるという位置付けになろう。しかし、この新しい情報の提供手段は、

- 今後は多くの情報がもともと電子的に作成されるようになること
- これまではその対象になっていなかった画像や映像までを対象にできること
- さまざまな情報から目的に応じたものを容易に検索できること
- いつでもどこからでもアクセスできること

というところから、行政情報の提供の主流になると考えられる。そして、これらの情報のネット化は、行政情報の利用を大きく活性化することにつながろう。

グローバルネットワーク環境は、こにょうな情報の活用分野を一気に拡大することになると思われる。例えば、議会の映像をネットを介して配信することも可能になり、行政へのアクセシビリティの向上につながる。電子政府の目的は内部業務の効率化だけではなく、利用者の利便性向上も重要である。市民が意見を述べる機会が増すと、それに伴い、市民の行政への参加が容易になり、民主政治のレベルの向上に寄与することも期待される。すなわち、ネットワーク化、ブロードバンド化は、デジタルデモクラシーの進展を促すことも期待される。

ネットワークを介して提供される行政情報の一例を、表 2-5 に示す。

表 2-5　ネットワークでの提供が想定される行政情報例

行政機関	行政情報
地方自治体	白書、調査報告書、予算書、決算書 等
	地元の観光案内等を納めた広報用映像
国立・公立図書館	所蔵の音楽や映像情報
	電子図書として所蔵の（マイクロフィルム化された）新聞記事

(6) 住民参加行事の運営

行政機関主催のイベントの紹介や照会、参加者の受付等をネットワークを介して行うものである。ブロードバンドネットワークの整備により住民参加行事の受付から、ネットワーク上で行事参加することができる。例えば、生涯学習に関してなど、テレビ会議のように、情報端末の画面を通して学習を行うことができる。このような行事の例を次に示す。

表 2-6 ネットワークを介した住民参加行事の事例

主催機	行事名称
地方自治体	生涯学習、 IT講習会の案内、申込み、参加
	行事の案内、申込み、参加
各種国立機関	住民参加による展覧会の案内、申込み、参加
	住民との交流会の案内、申込み、参加

2.1.9 市民の政治参加へのネットワークの利用

現在における、市民の政治への参加はとても十分といえるものではない。政治への関心の低さ、積極的な参加へのわずらわしさ、さらには自分の意見が反映されないという無力感等が、その原因として考えられる。ネットワークインフラの進展により、さまざま形で政治に関する情報が市民に提供され、政治の動きになじむようになり、また、政党や政治家との双方向のコミュニケーションが容易にできるようになれば、市民の政治への参画は、現在に比べ数段と活性化できると期待できる。

市民の政治参加を活性化するためのネットの利用分野としては、以下があげられる。

- ネット経由での政治関係の情報の提供
- 政党、政治家との双方向コミュニケーション
- 選挙への利用
- 住民投票への利用

2.1.9.1 ネット経由での政治にかかわる情報の提供

市民の政治への参画を促す第一歩は、市民が政治にかかわる情報に多く触れることができるようにすることであろう。現在、市民が政治にかかわる情報へ接するのは、政党や政治家の発行する機関紙や文書、メデイアの報道、あるいは議会の傍聴等によっているが、議会の傍聴は仕事を持つ一般の人には限界があるし、政党や政治家発行の機関紙や文書やは受取れるものは限定されていること、報道による情報は部分的であったりメディアの主張に偏ったものであったりで、市民が政治についての自らの判断材料とすべき情報がすべてに公平に提供されているとは言い難い。

ネットを利用し、あらゆる人が都合のいい時間に、求める情報にアクセスできるようにすることができるようになることが期待される。

今後、ネットの利用が中心となってくると、考えられる政治にかかわる情報の提供の代表例としては、表 2-7 に示すようなものがあげられる。

表 2-7 ネット経由の提供が中心となる政治にかかわる情報

情報提供者	提供の対象となる情報
公共機関（国、地方自治体）	・議会情報（審議の予定、審議の経緯等） ・議会のライブ（生中継、録画配信）
政党、NPO 他の政治団体	・政党の活動状況 ・政策案件に対する政党の見解 ・政党および構成党員の紹介 ・政党の活動や政治案件の個々に対する取り組み状況に対する世論
政治活動家（議員、候補者他）	・個人のプロファイルおよび支援組織の紹介 ・政策案件に対する見解 ・議会および所属政治団体における活動および政治家個人としての活動の紹介 ・自分の見解や政治案件の個々に対する取り組み状況に対するさまざまな意見と、これらの意見に対する見解

2.1.9.2 政党、政治家との双方向のコミュニケーション

現在でも相当に普及しているメールや Web 通信を用いた政党や政治家と支援者あるいは一般市民とのコミュニケーションに加え、ブロードバンドネットワークの高速大容量の特性を活かしたテレコンフェランスの利用は、政党や政治家と市民との間でのネットを介したフェースフェースライクな対話の実現をもたらす。

今後は、市民はいつでも、議会でのやり取りの詳細の視聴できるようになることに加え、ホームページやメールマガジン等により、政党や政治家個人の考えに直接触れることができるようになるだけでなく、政党や政治家やその支援者と直接的な対話が、いつでも好きな時にできるようになる。特に、政党や政治家との政治案件を巡っての意見の交換は、市民の政治参加の意欲を高めるものとなろう。

2.1.9.3 選挙へのネットワークの利用

選挙へのネットワークの利用としては、以下のがあげられる。

- 選挙公報のネット経由での提供
- ネットを介した候補者との対話
- ネットを介した投票

現在、選挙管理委員会発行の公報やメディア等で知らされている投票についての情報や、候補者の経歴や政見を、ネット経由で提供するものである。

ブロードバンドネットワークが進展すれば、現在の限定された情報からなる候補者の経歴をさらに充実した形で提供できるようになるだけでなく、候補者の人物や日頃の活動や、候補者の政見についてのさまざまな意見の紹介も可能になろう。そして選挙民は、これらの情報に、何時でもどこからでもアクセスできるようになることに加え、前節に上げた候補者との対話が身近なものになれば、市民の選挙への関心を高め、投票率の向上に結びつけることも期待できる。

ネットを介した投票は、システムのセキュリティ上の問題等もあって、さまざまな議論があろうが、健康上の理由等で投票所に出向けない人の選挙への参加を実現する手段として、限定的なものとしては検討の対象となろう。

2.1.9.4 住民投票へのネットワークの利用

各種の住民投票に対しも、ネットワークは以下の点で利用ができる。

- ネット経由での住民投票についての公報の提供
- 投票に案件についての情報の提供
- 投票案件についてのさまざまな意見の開示、交換
- 投票所に出向けない人のネット経由での投票の実現

住民投票の場合、投票案件についての意見が割れていることが前提となるため、投票者に公平な判断材料を与えることは重要である。このため、それぞれの側の主張についての情報に加え、第三者が中心となって纏めた情報の提供も重要となる。また、一般の投票者の意見も掲示や一般の投票者同士に意見交換の場がネット上であたえられることも、住民投票への関心を高め、住民投票の結果をより民意にあったものにすることになることが期待できる。ネット上での意見の交換は、その匿名性を上手に使えば、地域社会のしがらみを離れ、本音での議論を可能にする。

2.1.10 市民の行政参加へのネットワークの利用

行政機関は市民、納税者の代行機関であり、その活動は民意を反映したものでなければならない。このため、これら各行政機関はその機関の業務あるいはサービスの対象となる者との良好なコミュニケーションができていることが求められる。従来からも、さまざまな方法で、各層の行政機関と市民との間のコミュニケーションの場も持たれてはきたが、市民にとっては手間がかかることもあり、一部の活動家層を除く一般市民の参加は低調であった。

しかし、ネットワークインフラの進展は、多くの一般市民が容易にこのコミュニケーションに参加できる環境するため、各行政機関はネットワークを活用し、自分がサービスの対象としている層との積極的な対話を図るようにし、その活動に活かすようにしなければならない。

行政機関とそのサービスの対象である市民等との対話強化のためのネットワークの利用形態とし

ては以下のようなものがあげられる。

- 各種世論調査
- パブリックコメントの収集
- ネットワーク型公聴会
- 各種市民懇談会
- オンライン相談窓口

それぞれにおけるブロードバンドネットワークの使い方は、以下のようになろう。

(1) 各種世論調査

世論調査のように多くに国民の声を集める手段としてインターネットを活用した電子投票が有効である。インターネットの活用により多くの人の意見を集めることが出来るのはもとより、インターネット上の掲示板などによるディスカッション等も可能となる。また、調査の結果を調査対象の当事者に知らせることにより住民の声を社会に反映させることとなろう。

このような世論調査は、郵送のものに比べ、回収率ならびに回答の信頼性をより向上させると考えられる。ただし、この方法は従来の郵便やメールを用いたものに比べ、相手の時間をインタビューする側の立場で拘束するため、回答内容についてのさらに突っ込んだ議論等の補助的な手段として使われることになることも想定される。ブロードバンド化が進めば、ディスカッションも文字情報主体の掲示板から、映像や動画・音声を用いたテレコンフェランス型に進化し、短時間で効果的なものになると考えられる。

(2) パブリックコメントの収集

行政機関が行うパブリックコメントの収集も、既にメールや Web を用いたものが主流になりつつあるが、ブロードバンドネットワークの進展でテレコンフェランスシステムが普及すれば、メールや Web での回答にもとづきコメントの提出者との、さらに突っ込んだ意見の交換も可能になる。コメント提言者と行政機関の担当者との対象事案についての直接の対話は、行政機関における政策立案過程におけるパブリックコメントというプロセスをより充実したものにし、それだけ行政に民意を反映できることにつながる。

これまでのパブリックコメントは、コメント発信から、意見回収までのサイクルが長かった。意見の回収に時間がかかるため、ある程度、企画を固めて、コメント化する必要があるからである。今後、ブロードバンド時代の到来によって、意見の収集が容易になる。この結果、コメント発信を企画の柔らかい段階から、複数回に渡って行なうことも可能となろう。すなわち、パブリックコメントのプロセスに、短いスパンによるスパイラル的なアプローチを可能にする。

(3) ネットワーク型公聴会

行政に関し住民の意見の集約等で公聴会が開かれることも多い。ともすれば利害関係者や特定の主張をもつ団体の者が中心であったこれらの公聴会を、真に開かれたものにするにはこれらの公聴会をネットワークを用い開かれたものにすることが必要となる。公聴会へのネットワークの利用の形態としては、以下の２つが考えられる。

- 公聴会等へのネットワーク参加の実現
- 電子掲示板やテレコンフェランスシステムを駆使したバーチャル公聴会の開催

前者の公聴会へのネットワーク参加の実現は、実際に開催されるリアルな公聴会の場にテレコンフェランスシステムを持込み、その場に来ることができない人々にその公聴会を視聴できるようにするとともに、発言の機会も与えようとするものである。このような公聴会の実現は、時間や物理的な距離の問題から公聴会の場に出向けない多くの人々に現実的な参加をさせることになり、より中立的な立場での意見の聴衆も可能とする。行政上の大きな議論案件に対する民主的な議論の推進のためには大いに期待される実施方法である。

また、後者のバーチャル公聴会もパブリックコメントの収集の一環として有効に活用すれば、個人個人の一方的なコメントの収集よりは、こなれた意見の集約となることが期待できる。大きな案件に対しては、周到な準備の下での専門家も交えたリアルな公聴会が必要で、この場合は前者の方法となろうが、地方自治体におけるさまざまな意見の交換や民意の確認については、後者のバーチャル公聴会も有効であろう。

ネットワーク参加型公聴会はネットワークを用いた市民との対話の代表例である。公聴会の場に来ることができない人が、ネットワークを活用して公聴会を視聴したり、実際に公聴会場にいる人と同じように発言したりできるようにするものである。映像や音声を扱う性質上、テレコンフェランスシステムによるリアルタイムでの公聴会参加はブロードバンドが必要とされる。

効果としては、ネットワークを利用することで物理的な距離の制約がなくなるので、今まで参加できなかったより多くの人の参加が望めること、中立的な意見が言いやすいことなどがあげられる。それによって、今まで以上に民主的な議論が進展することが期待される。

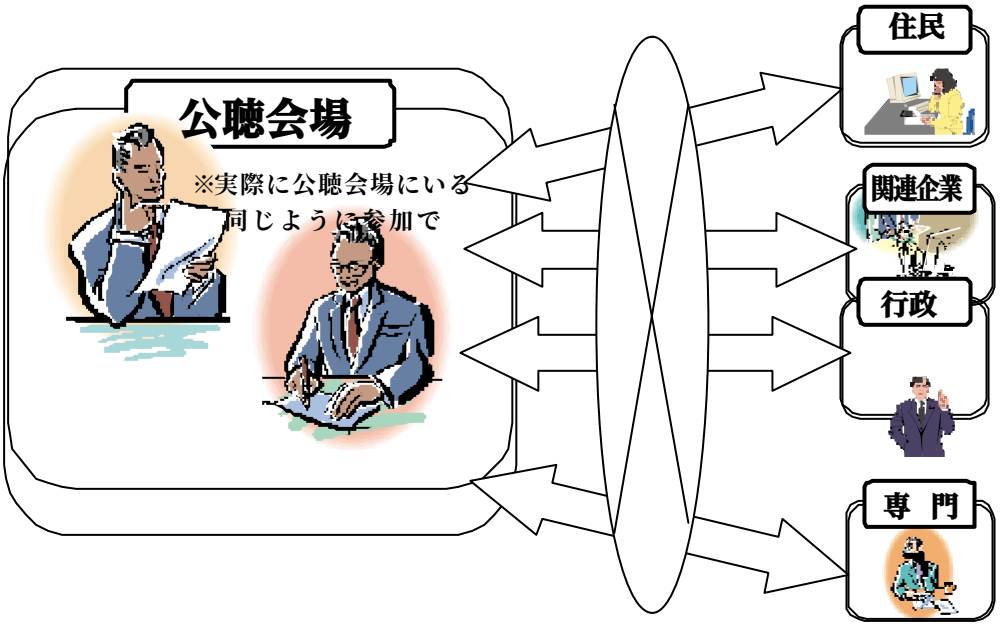


図 2-2 ネットワーク公聴会イメージ図

(4) 各種懇談会

行政機関におけるさまざまな活動においては、有識者等民間の参加を得た委員会等の活動によるところも多い。これらの活動をより活発化し効果的なものするためには、関係者が居ながらにして協議ができるテレコンフェランスシステムの活用も有効である。

参加者の時間的な負担を軽減することにより、より幅の広い層からの参画も期待できる。

(5) オンライン相談窓口

行政機関における各種の相談窓口を、テレコンフェランスシステムを導入し、相談者とのフェースツーフェースライクな対話を行うことで、相談者や相談窓口の担当者がわざわざ出向かなくても相談に応じることができるようにするものである。

過疎地域では特にきたされるネットワークの利用の一つと言える。

2.2　ビジネス分野におけるネットワークの利用

2.2.1　ビジネス分野において注目すべき今後のネットワークの利用

企業においては、そのすべての活動にネットが利用されるようになるのは論を待たないが、その中にあっても、ブロードバンドネットワークの普及により、ネットの利用に、新たに登場したり、利用が質的にも量的にも大きく拡大するところがと生じる。これらは、業務の進め方において従来の壁を破る原動力となり、経営リソースの有効活用の実現や企業の競争力確保に大きく寄与するものと考えられる。

今後、製造業企業を例に、注目すべきネットの利用場面を、表 2-8 に示す。他の業者においても、同じような考え方が当てはまると考える。

表 2-8　製造業企業における今後注目すべきネットワークの利用

	適用業務分野	代表的なネットワークの利用場面	重要性	想定される普及度合い		
				現在	5 年後	10 年後
1	経営および事業戦略	社会とのコミュニケーション	△	△	○	○
		リアルタイムでの経営情報の集約と意思決定への反映	◎	△	○	◎
		株主とのコミュニケーション	○	＊	○	○
2	研究開発	社内外の情報の活用	○	△	○	◎
		社内関連部署間および外部協力機関とのリモートコラボレーション	○	＊	○	○
		社内コンピューティングリソースや研究装置の共用	△		△	△
		社外コンピューティングリソースの利用	△		△	△
		学会等社外研究活動への参画	△		△	△
3	資材調達	電子調達の活用とリアルタイムチェインサプライマネジメント	○	△	○	◎
		調達先とのリモートコラボレーション	○	△	○	◎
4	生産（設計、製造）	ネットワーク型生産プロセス管理	◎	＊	○	◎
		生産設備、装置のリアルタイムモニタリングとリモートコントロール	○	△	△	△
		トラブル発生時のリモート支援	◎		△	○
		現場作業へのオンラインマニュアルの提供	○		○	◎
		現場要員に対するオンライン作業指導	○		△	○
		社内関連部署間およびパートナー企業とのリモートコラボレーション	◎		○	◎
5	物流	ネットワーク型物流プロセス管理	◎	＊	△	○
		在庫品および物流品のリアルタイムトレース	◎	△	○	◎
		既納品のライフサイクル管理	◎	＊	○	◎
		社内関連部署間およびパートナー企業とのリモートコラボレーション	◎		○	◎

表 2-8 製造業企業における今後注目すべきネットワークの利用

	適用業務分野	代表的なネットワークの利用場面	重要性	想定される普及度合い		
				現在	5 年後	10 年後
6	営業、販売	市場とのコミュニケーション	○	＊	○	○
		ユーザコミュニティの形成と活用	○	＊	○	○
		顧客管理と顧客とのコミュニケーション	◎	△	◎	◎
		電子商取引の拡大	◎	△	○	◎
		営業情報の活用	◎	△	○	◎
		営業マンのオンライン教育	○	＊	○	○
		社内関連部署間およびパートナー企業とのリモートコラボレーション	○		○	○
7	顧客サポート	ハイレベルで均質なサービスの提供	◎		△	○
		リモートメンテナンスサービスの提供	△	＊	△	△
		利用についてのオンラインサポート	◎	△	○	◎
		顧客に対するさまざまな情報の提供	○	△	○	◎
		リモートコンフェランスを用いた相談や苦情への対応	○		△	○
8	業務の運営	事業所間や職場間でのリモートコラボレーション	○		○	◎
		パートナー企業とのコミュニケーションおよびリモートコラボレーション	○		○	○
		アウトソーシング先とのリモートコラボレーション	◎		△	◎
		行政機関とのコミュニケーションおよびリモートコラボレーション	○	＊	○	◎
		業界団体等の各種関係機関とのコミュニケーション	○		△	○
		リモートオフィス、モバイルオフィス、在宅勤務	△		△	△
		社内生活のサポート	△	△	△	○

重要性
◎ 非常に重要、企業にとっては欠かせないところ
○ 重要、企業にとっては是非取組むべきところ
△ 重要性は低い、特に必要ではないが、あれば便利なもの

想定される普及の度合い
◎ ほとんどの企業に普及
○ 大企業はもちろん中小企業の大半にも普及
△ 普及は一部の企業に止まる
＊ 登場段階、先行ユーザで使用が始まっているが本格的な普及はこれから

2.2.2 経営および事業戦略の強化のためのネットワークの利用

(1) 社会とのコミュニケーション

事業の展開には、自社の存在や展開している事業についての社会的な認知が必須となる。企業においてパブリックリレーションといわれるこの点に関する活動にも、ネットワークの活用は有力なものとなる。すでに、従来の企業紹介のパンフレットの配布に加え、ホームページの活用は一般的なものになっている。

ブロードバンド時代においては、ネットワークと社会全体におけるPC 等の情報交換機器の普及により、ネットワークを使った市場とのコミュニケーション力は、企業ブランドの確立には欠かせないものになり、各企業はこの点にも注力するようになると考えられる。

(2) リアルタイムでの経営情報の集約と意思決定への反映

グローバルベースでの競争にさらされている現代の事業経営においては、自社の特性と市場環境にあった事業戦略の確立と適切な事業の運営は、従来に増して重要となっている。そして、これらは社会環境や市場環境の変化にも適切かつ迅速に対応できていなければならない。

このためには、事業経営に必要な情報の収集とその有効な活用、および経営にかかわる者同士の意思統一に向けた積極的なコミュニケーションが必要となる。この分野におけるネットワークとIT の利用はさらに高度化されなければならない。

(3) 株主とのコミュニケーション

企業の経営においては、株主や社会一般とのよりよきコミュニケーションが欠かせない。株主とのコミュニケーションについてのネットの利用としては、以下があげられる。

- 各種経営情報の提供
- 株主総会へのネットでの参加
- 経営についての双方向コミュニケーション

ネットを介した株主総会への参加や、株主との双方向コミュニケーションの実現は、株主の会社経営への参画を拡大することにつながる。

2.2.3 研究開発におけるネットワークの利用

(1) 社内外の情報の活用

研究開発の推進には、最新情報の入手が欠かせない。各種の情報サービスへのアクセスは、研究開発業務における基幹作業とも言える。従来に比べ、ネットワーク経由での情報の入手がより重要な位置を占めることになる。一方、情報提供側も、マルチメディアを駆使したより多様で豊富な情報の提供を行うようになろう。

また、現在においては、研究開発のスピードアップと効率化は、経営の最重要ファクターと

も言える。研究開発のスピードアップと効率化のポイントは、貴重な研究開発スタッフの効率的活用にある。研究開発活動における無駄を排除するためには、過去の研究成果や失敗事例に関する情報、ターゲットとする研究に関係する情報やデータを蓄積し、その利用が自在にできるデータベースの構築が必要となる。

(2) 社内関連部署間および外部協力機関とのリモートコラボレーション

研究開発業務においても、社内のさまざまな部署が関与する。また、業務提携先の企業や大学等の研究機関との連携も行われる。研究開発のスピードアップと効率化には、先にあげた社内外の情報の活用に加え、関係者の密度の高いコラボレーションは欠かせない。

ブロードバンドネットワークの進展が可能にする、リアルタイムでの多様な情報の交換を背景とするテレコンフェランスは、この点に大きく寄与するはずである。

(3) 社内のコンピューティングリソースや研究設備の共用

ネットワークの高速大容量化に伴い、社内におけるコンピューティングリソースや高価な研究装置の共用がより容易となる。研究開発の効率化のためには、社内コンピューティングリソースや研究装置の有効活用も重要となる。

(4) 社外コンピューティングリソースの利用

研究開発活動においては、膨大なコンピューティングパワーを必要とする場合がある。常時は必要としない大きなコンピューティングパワーを必要に応じて使えるようにするためには、社外のコンピューティングリソースを利用する方法がある。高速で大容量のネットワークは、社外のコンピューティングリソースの利用をより容易なものにする。

(5) 学会等社外研究活動への参画

研究開発スタッフは、学会等の社外の研究活動と連携を取ることが多い。これからは、これらの活動も、ネットワークを用いたものが主流になると考えられる。

2.2.4 資材調達におけるネットワークの利用

(1) 電子調達の活用とリアルタイムサプライチェインマネジメント

生産に必要な資材等をネット経由で調達するもので、必要なときに必要な物を適切な価格で調達できるようにするものである。電子調達には取引先と直接やり取りする方法と、eマーケットプレースを介して行う方法がある。すでに、普及が広まっているネットの利用形態ではあるが、まだ、先行企業においても、その利用は一部に止まっている。

電子調達がさらに信頼でき有効なものになるためには、リアルな取引の場と同じように、取引先との十分なコミュニケーションや、調達品の使用や品質の見極め等ができるようにならなければならない。ブロードバンドネットワークがもたらす、調達品についての膨大な情報のリアルタイムでの交換を背景とした、テレコンフェランスを活用すれば、担当者や責任者間でのフェースツーフェースライクな仕様の確認や指示や営業交渉が可能となり、電子調達をより便利

で信頼できるものにするはずである。このことは、電子調達の拡大に直結する。

しかしながら、経営において電子調達を効果的なものにするためには、生産から販売まで一貫してコントロールするサプライチェーンマネジメントの確立が必要となる。

(2) 調達先とのリモートコラボレーション

調達先との間では、発注品についての仕様の変更や納期の調整に加え、調達について長期的な見通しや、将来必要となると思われる調達品についての意見の交換や共同開発についての打診等もあり、調達先との効果的なコミュニケーションやコラボレーションが欠かせない。

テレコンフェランスや関係情報の共有等のブロードバンドネットワークの効果的な活用は、調達先とのコミュニケーションやコラボレーションの改善に大きく貢献するはずである。

2.2.5 生産（設計、製造）におけるネットワークの利用

(1) ネットワーク型生産プロセス管理

生産計画立案業務、部品の調達業務、半完成品の保管業務、完成品の出荷業務等が自動的に連携できれば、処理の正確性の向上とスピードアップが図られることになる。それぞれを管理するシステムのネットを介した自動連携は、今後ますます重要なものとなろう。

(2) 生産設備、装置のリアルタイムモニタリングとリモートコントロール

生産の状況や各種装置の稼動状態の細部に至る把握は、生産の自動化や適切な生産現場の管理には必須となる。従来に比べ、画像や映像データの活用がより容易に行なえるようになる分だけ、離れた場所からの現場の状況把握についての信頼性を向上させることができる。

また、生産プラントにおける装置のリモートコントロールも、生産プラントにおける生産状況や設備や装置の稼動状態の詳細についてのリアルタイムの把握を背景とすれば、それだけ信頼性を向上させることができる。

(3) トラブル発生時のリモート支援

製造現場において何かトラブルが生じた場合、テレコンフェランスシステムを用いれば、生産現場の指導者や製造装置、当該製品の設計者等の専門家が現地に赴くことなく、リアルタイムに現状を把握し、その場からの適切な指導を行うことも可能となる。

(4) 現場作業へのオンラインマニュアルの提供

生産現場における装置の取り扱いや作業を指示する電子化し、ネット経由でアクセスできるようにするものである。現場作業員は、新しい作業についてはこの電子化されたマニュアルで自習ができる。また、この自習の過程や作業中に疑問が生じた時、随時、このマニュアルにアクセスして、その指導を受けることができる。

これらが必要に応じオンラインで呼び出せ、しかもその内容が精密な映像等を駆使した対

話型のものであれば、その指示はより分かり易いものになろう。このような形態でのマニュアルの提供は、常に最新の情報や経験に基づいたメンテナンスが可能であり、その内容の充実がはかれるとともに、印刷配布の必要がないため、ベンダーにとってもコストダウンが期待できる。

(5) 現場要員に対するオンライン作業指導

テレコンフフェレンスシステムを用いて、現場従業員に対する生産現場での作業を、作業員の要求に応じ、現場の状況把握の上に立って豊富な情報を背景に上級者あるいは専門家が適切な指導を行うものである。指導レベルの向上と、問題が生じた時の場面々々に応じた指導の実施で、指導を受ける側にとってよりも身につく教育となる。また、指導要員チームのの運用の効率化も期待できる。

(6) 社内関連部署間およびパートナー企業とのリモートコラボレーション

生産現場における業務においても、社内のさまざまな組織が関与する。テレコンファレンスの有効活用により、関係者間のコミュニケーションをより効率的で密なものにすることができる。

また、生産現場においても、社外のさまざまな組織が関与する場合がある。リモートコラボレーションの有効活用により、この連携をより効率的で密なものにすることができる。

2.2.6 物流におけるネットワークの利用

(1) ネットワーク型流通プロセス管理

物流が生産や調達業務と自動的に連携できれば、流通管理の正確性の向上とスピードアップが図られることになる。それぞれを管理するシステムのネットを介した自動連携は、今後ますます重要なものなろう。

(2) 在庫品および物流品のリアルタイムトレース

在庫品や搬送中の商品の現在地の把握は、入出庫の効率化や物流の効率化が図られるだけでなく、顧客に対しその要求に応じ、納入についての情報提供が可能になるため、顧客サービスの向上にもつながる。

(3) 既納品のライフサイクル管理

既納品に対する各種のサービスや環境問題に対処するための機器等の廃棄時に必要な処置が適切な行えるようにするためには、既納品がどこにありどのような使われ方をし、またどのような状態にあるかが、正確に把握されていなければならない。このためには、納入先との連携が必要となる。すでに、多くの企業で取組みが始まっているが、今後は、既納品のその時点々々での保有者や管理者、存在場所、使用状況、整備状況等のライフサイクルに関する情報がネットを介して自動的に製造者に知らされるようなシステムの実現や、社会全体としてのこのようなシステムの運用スキームの確立も必要となる。

(4) 社内関連部署やパートナー企業とのリモートコラボレーション

流通業務においても、社内のさまざまな組織が関与する。テレコンファレンスシステムの有効活用により、関係組織間のコミュニケーションをより効率的で密なものにすることができる。

また、流通業務においても、運輸会社や保険会社等との連携が必要となる。リモートコラボレーションの有効活用により、この連携をより効率的で密なものにすることができる。

2.2.7 営業・販売におけるネットワークの利用

(1) 市場とのコミュニケーション

商品企画の立案や営業活動を戦略的で効率的に展開するためには、流動的な市場のニーズを、常に、正確に捉えていなければならない。このためには、ネットを用い、市場との双方向のコミュニケーションが不可欠となる。

この面に関する巧拙は企業の競争力を左右しかねない。ブローバンドネットワーク環境を上手に生かすための工夫が必要となる。

(2) ユーザコミュニティの形成と活用

顧客同士のコミュニティを形成し、顧客同士でのコミュニケーションをサポートすることで、顧客にさまざまな機会を与えることができる。このことは、顧客に自社と取引することについての付加的なメリットを与え、顧客満足の向上や顧客の囲い込みに役立たせることができる。

また、このコミュニティに潜在顧客も参加できるようにすることで、新たな顧客獲得のチャンスを作ることも可能となる。

ブロードバンドネットワーク環境を使いこなした、魅力あるコミュニティつくりも、今後の企業のテーマの一つになろう。

(3) 顧客管理と顧客とのコミュニケーション

顧客とのパイプの強化は営業活動の基本とも言えるものである。このためには、顧客データベースの確立による、関係者間での密度の高い顧客情報の共有と、これらの情報を背景とした、個々の顧客との密度の高いコミュニケーションの確立が必要となる。

高速ネットワーク環境は、顧客情報に映像等も含むきめの細かい情報を加えることができる。また、営業マンの訪問をベースとしていたコミュニケーションも、ネットワークを活用することにより、その効率を上げるだけでなく、顧客とのより密接な関係の構築にも寄与できる。

顧客とのコミュニケーションへのネットワークの活用としては、

- テレコンコンフェランスシステムの活用により、顧客が求めるときに営業マンが出向かなくてもフェースツーフェースライクな対話を可能とする
- 多彩で豊富な顧客情報の活用ができる
- 顧客との単純な打ち合わせ等においては、営業マンがわざわざ顧客サイドに出向く必要もなくなり、顧客要求への対応のスピードアップと、各種のデータベースをバック

にしたリアルタイムの情報提供や対話を可能とする

ブロードバンドネットワークを営業活動の有力な武器として使いこなすかどうかが、これからの企業競争の一つの要素ともなろう。

(4) 電子商取引の拡大

ネット経由での商品の販売は、すでに広く普及しているが、その適用は、商品の品質の見極めに不安がないもので、商品の確保や価格的に有利になるものに限られていたり、リアルでの取引の準備として用いられる分野に限定されているのが現状である。

取引対象の拡大やネット処理の対象となる取引プロセスを拡大するためには、商品や取引相手の信用の見極めが十分にできるようになることと、買い手と売り手での間でのリアルでの取引と同じような対話環境の提供が不可欠となる。

ブロードバンドネットワークの高速大容量という特性は、さまざまな角度からの多様な情報の提供により商品の説明力を提供するとともに、テレコンフェランスは売り手と買い手との間でのフェース-ツーフェースライクな対話を実現させる。このことにより、買い手は、

- 例えば、衣類については、その肌触りまで感じることができるような高精細な画像を、道具等についてはその動作や使用方法も見せる動画像等での商品の説明による、売り手にとっての商品の説明力、買い手にとっての商品についての理解力、判断力の増加
- 豊富な帯域を利用しての、売り手についてのデータだけでなく、オフィスや経営者像のビジネスの実態を紹介することが可能で、買い手にとっての売り手の実像の把握力の増加

をもたらす。

このため、買い手にとっては、商品とショップについてより厳密なチェックできるため、それだけ安心した取引が可能になる。ネット上での商品の展示の高度化や、売り手や買い手間でのフェースツーフェースライク名対話の実現は、オークションやネットショッピングに新たなスタイルを開き、電子商取引のさらなる発展を促すことになろう。

(5) 営業システムの活用

戦略的な営業活動の効率的な展開には、営業活動を支援する総合的な営業支援情報システムの整備が必要となる。営業情報としては、市場動向、自社の商品や技術についての情報、他社の動向や他社商品についての情報、顧客個々についての情報や、過去の取引ならびに現在進行注中の商談等が含まれる。

ブロードバンドネットワーク時代にあっては、ネットワークの特性を十分に活かす情報の蓄積とその利用法に工夫が必要となる。

(6) 営業マンのオンライン教育

営業スタッフが、販売対象となる商品やサービスおよびその販売方法についての十分な理解を得るためのマニュアルを電子化し、ネット経由でアクセス活用できるようにするものである。営業スタッフは、新しい商品とその販売方法について、自習時あるいは営業現場で疑問が生

じた時など、この電子化されたマニュアルにネットl経由でアクセスして、その指導を受けることができる。これらの教育は、自社の営業マンだけでなく、販売提携先や代理店の営業マンにも提供されなければならない。

これらが必要に応じオンラインで呼び出せ、しかもその内容が精密な画像等を駆使した対話型のものであれば、その指示はより分かり易いものになろう。このような形態でのマニュアルの提供は、常に最新の情報や経験に基づいたメンテナンスが可能であり、その内容の充実がはかれるとともに、印刷配布の必要がない分コストダウンも期待できる。

このような電子化された営業マニュアルと、テレコンフェラレンスシステムを有効に組み合わせれば、営業マン教育や販売商品に関する質の高い教育を、営業スタッフ個々の都合に応じて行なうことができる。

従来の限られた集合教育の実施に比べ、個人個人の都合に合わせ、本人が納得行くまで学習が可能となるため、達成度を確認しながら教育効果を向上させることができる。

(7) 社内関連部署間およびパートナー企業とのリモートコラボレーション

営業業務においても、社内のさまざまな組織が関与する。テレコンファレンスの有効活用により、関係組織間のコミュニケーションをより効率的で密なものにすることができる。

また、営業業務においても、提携企業や販売代理店との連携が必要となる。テレコンフェランスシステムの活用場面である。

2.2.8 顧客サポートにおけるネットワークの利用

顧客サポートの向上は、競争優位性確保の重要課題である。ネットワークの有効利用により、少ない経営資源を有効活用して、顧客サービスの向上を図ることができる。

(1) ハイレベルで均質なサービスの提供

自動車や農業機器、建設機器、あるいは家庭電化製品等にトラブルが生じた場合や、定期メンテナンス等は、各地のサービスステーションにおいて行われるのが一般である。この時、サービスステーションのエンジニアでは対応できないケースも考えられる。

このような場合、テレコンファレンスシステムを利用すれば、メンテナンス要員が現場に出向かなくても、装置の状況についてリアルタイムにデータ収集や細かい観察ができ、納入先にさまざまな指示を出しながら点検や修理の試みを行なうことも可能になる。また、サービスセンターや設計部門、製造工場、品質管理部門の上級エンジニアが対応でき、地方のサービスステーションでも最高レベルのサポートを提供できる。

指示する側は豊富な画像や映像データを用いて指示できるため、顧客側においてトラブル原因の把握や応急処置が可能となることも期待できる。深刻な状況でなければ、装置ベンダーの保守員を待たずに、修理や応急処置が可能になることで、ベンダーにとっても装置の使用者にとっても福音となる。また、修理完了に至らなくても、メンテナンス要員が現場に出向

く前にある程度の状況の把握ができていることは、現場での原因の調査や修理をよりスピードアップすることにもつながる。また、必要に応じて更なるバックアップ体制の準備も行なえる。

ブロードバンドネットワーク時代にあっては、先に上げた装置への自己診断データのネット経由での伝送機能の付加とあいまって、トラブル時におけるこのようなサービスの提供は、競合上必須のものになってこよう。

テレコンフェランスシステムのこのような活用は、メンテナンスサービスの質の向上で顧客満足度向上につなげられるだけでなく、社内専門家の有効活用と、現場のメンテナンス要員のレベルアップにつなげられるため、経営資源の有効活用にもなる。企業にとっては、早急な導入を検討すべき分野である。

(2) リモートメンテナンスサービスの提供

より良いメンテナンスサービスの提供は、商品の競争力のキーファクターの一つと言える。より良いメンテナンスサービスの提供のためには、常に、既納品の状態を正確に把握し、必要に応じたメンテナンスの実行を遅滞なく適切に提供する必要がある。

ネットを利用してリアルタイムでの既納品の状態の正確な把握や、ネットを用いたリアルタイムでのメンテナンスの実行は、今後、広く普及することになると考えられる。

プロダクトに組み込んだ自己診断データを、ネットを介して保守センターに送り、保守センターで対応装置の状況を把握し、予防保全等に必要な処置をタイムリーに行えるようにするものである。深刻な状態になる前に、必要な処置が可能となることもあって、これも期待されるネットワークの利用の一つであろう。

また、装置に組込んだ自己診断機能と保守機能を用いて、装置にトラブルが生じた場合のメンテナンスをネットを利用して、メンテナンスサービスサイトから直接行なうものである。このようなメンテナンス方法は、装置の特性やトラブルの内容にもよるが、今後増加するものと思われる。

(3) 利用についてのオンラインサポート

装置等の操作マニュアルは印刷物か電子媒体の形で提供される場合が多いが、その保管や内容のメンテナンスは利用者側にとっても発行者側にとっても負担となっている。これらが、必要に応じオンラインで呼び出せ、しかもその内容が精密な画像を駆使した対話型のものであれば、その指示はより分かり易いものになろう。このような形態でのマニュアルの提供は、常に最新の情報や経験に基づいた継続的なメンテナンスが可能であり、その内容の充実がはかれるとともに、印刷配布の必要がないため、ベンダーにとってもコストダウンが期待できる。

また、このマニュアルの理解等において疑問等があれば、テレコンフェレンスシステムを用いてインストラクターと直接対話し、理解を助けてもらうことも可能となる。

(4) 顧客に対するさまざまな情報の提供

顧客が必要とするような情報をこまめに顧客に提供すことも、顧客満足の向上に欠かせない。顧客に提供すべき情報の代表例としては、以下があげられる。

- 新しい商品、サービス、技術の紹介

- サポート体制の紹介
- 既納品の取扱い方やトラブル等の情報

ブロードバンドネットワーク環境を活かし、提供する情報の内容を豊富で使いやすいものにしたり、情報の提供方法を改善したりすることができる。

(5) テレコンフェレンスを用いた相談や苦情への対応

顧客からの相談や苦情に適切に対応することも、営業活動の一環として重要である。ネットを活用すれば、これらに対応する要員の集中が可能でとなり、対応体制の効率化と、対応のレベルの向上につなげられる。

テレコンフェランスシステムの活用により、相談や苦情への対応を、フェースツーフェースライクの対話で行うなうことを可能にする。

新しいネットワーク環境を活用した顧客からの相談や苦情への対応は、これらについての顧客の満足度を向上できる。

2.2.9 業務運営面でのネットワークの利用

(1) 事業所間や職場間でのリモートコラボレーション

一般に、企業活動は、個々の従業員やチームや部署間の協業の上になりたっている。そして、事業活動は、オフィスや工場等の複数の拠点における業務や、出張先等の社外における活動により展開されているのが一般である。事業の効率的運用には、離れた場所にいる者同士あるいはチーム間の連携が、有機的かつ効率的に行なえることが必須となる。ネットワークを利用したフェースツーフェースライクな対話を実現してくれるテレコンフェレンスシステムは、離れた場所いるチーム間の業務活動の連携や、問題解決のため共同作業は、業務の効率化と質の向上に大きく貢献するはずである。

(2) パートナー企業等とのコミュニケーションおよびリモートコラボレーション

企業の事業展開にあたっては、パートナーの存在は欠かせない。特にネットワーク時代において、事業パートナーとの垂直あるいは水平分業等の効果的な展開は、経営効率化に直結する。良きパートナーの発掘、良好で効果的な関係を維持するためには、取引上の付き合いだけでなく、事業パートナーとして総合的な立場での情報の共有と密なコミュニケーションの確立が必要となる。

ブロードバンドネットワーク環境での、テレコンファレンスの積極的利用や共通データベースの構築が想定される。

(3) アウトソーシング先とのリモートコラボレーション

最近、外部に委託できる業務は極力アウトソーシングし、自社の経営リソースは競争力の確保に重点的に配分するようにすることが経営の手法として定着してきた。業務のアウトソーシングが経営の意図どおりに機能するためには、アウトソーシング先との間でのコラボレーショ

ンが適切に行われることが前提となる。

アウトソーシング先との適切なコラボレーションの実現の要件としては、以下があげられる。

- 業務委託先における委託業務についての十分な理解
- 委託側と委託先との業務プロセスの確立
- 委託業務に関する必要な情報の共有
- 問題発生時における適切なコラボレーション
- 以上の諸事項を実現するための委託側と委託先との間での円滑なコミュニケーションの確立

一般に、離れた場所にいるアウトソーシング先との間で、これらの要件を満たすためには、ネットの効果的な活用は不可欠なものとなる。ブロードバンドネットワークの高速大容量性は、情報の共有、交換、随時のフェースツーフェースライクな対話環境を提供し、企業のアウトソーシングをより信頼できるものにするのに貢献する。

(4) 行政機関とのコミュニケーションおよびリモートコラボレーション

事業の展開にあたって、監督官庁等の関連機関への届出・申請が必要な場合が多い。電子政府の進展とともに、これら届出・申請などの事務的な処理はネット化されることになる。ブロードバンドネットワーク時代においては、これらの事務的な処理のネット化に加え、協議等が必要な場合においても、その多くはテレコンフェランスの利用で済ますことができるようになろう。

(5) 業界団体等の各種関係機関とのコミュニケーション

企業等の組織は、その事業運営上、行政機関や業界団体等さまざまな組織とコミュニケーションすることが必要となる。テレコンフェランスは、この活動をより効果的かつ効率的なものにしてくれると考えられる。

(6) リモートオフィス、モバイルオフィス、在宅勤務

会社のデータベースへのアクセス、文書の作成や送付、業務システムへの指示、社内のさまざまな部門とのフェースツーフェースライクな対話等が、何時どこからでも可能になることにより、業務の遂行に対しては、外出先でも自宅でもオフィスとの同じ環境とすることができる。

業務のスピードアップや効率化、従業員の勤務負担の低減等に効果が期待できるモバイルオフィスや在宅勤務は、これからの仕事のスタイルの中心になると想定される。

(7) 社内生活のサポート

企業等の組織にあっては、社員生活を支援するための福利厚生サービスや従業員間のコミュニケーションのサポート等が提供されるのが一般である。福利厚生施設の利用等に関する手続きや各種のイベントの案内等、企業における福利厚生サービスへのネットワークの利用も既に普及の段階にある。今後は、ネットワークの豊富な情報提供力を生かし、この分野での利用もさらに高度化しよう。

また、企業内においては、自己啓発のための勉強会やスポーツクラブ等の従業員を主体としたさまざまなコミュニティ活動がある。メンバーの管理や情報の交換もしくは活動の場として

のネットワークの利用もさらに活発化してくるものと思われる。

2.3 社会サービス分野におけるネットワーク化

ブロードバンドネットワークの普及は、医療、福祉、教育、や情報およびコンテンツの提供といった社会サービスに、ネットの利用を促す。このような分野におけるサービスのネットを利用した提供は、利用者の便を向上させるだけでなく、サービスの提供者にもサービスの提供の効率化をもたらし、結果としてサービスの質の向上をもたらす。

2.3.1 ネットワークを介しての利用が可能になる社会サービスの一覧

前節で述べた行政サーにス以外の社会サービスの分野におけるネットの利用分野を、表 2-9 に示す。

表 2-9 ブロードバンド時代における社会サービス分野におけるネットワークの利用

	サービス分野	代表的なネットワークの利用場面	重要性	想定される普及度合い		
				現在	5 年後	10 年後
1	医療サービス	医療機関間での情報の共有	◎	＊	△	○
		医療機関間でのコラボレーション	○		△	○
		在宅ヘルスケア (遠隔診断、遠隔診療)	○	△	○	○
		レセプト処理に関する関係機関間のコラボレーション	○	＊	△	○
		処方箋処理のオンライン化	△		△	△
		オンライン健康管理、健康相談	○	＊	△	○
		医療機関情報の提供	△	＊	○	◎
		医師等医療関係者に対するネットワーク教育	◎		△	○
2	介護サービスと老齢者支援	在宅ケアの支援	◎	＊	○	◎
		サービス提供機関の運営管理	△		△	△
		サービスの提供にかかわる者に対するネットワーク教育	○		○	◎

表 2-9 ブロードバンド時代における社会サービス分野におけるネットワークの利用

	サービス分野	代表的なネットワークの利用場面	重要性	想定される普及度合い		
				現在	5 年後	10 年後
3	教育サービス	ネットワーク経由での授業の提供	○	△	○	○
		ネット経由での個人レッスンの提供	○	＊	○	◎
		自習のサポート	○		○	◎
4	情報、コンテンツ提供サービス	報道情報の提供	○	△	○	○
		各種公共サービスに関する情報の提供	◎	△	◎	◎
		くらしにかかわる情報情報の提供	○	△	○	◎
		教育ライブラリの提供				
		各種の知識情報の提供	○	△	○	◎
		その他個人使用向けのデジタルコンテンツの入手	△	△	◎	◎

重要性
◎ 非常に重要、なくてはならないもの
○ 重要、是非欲しいもの
△ 重要性は低い、特に必要ではないが、あれば便利なもの

想定される普及の度合い
◎ 広く普及
○ 大半のサービスに普及
△ 普及に止まる
＊ 登場段階、先行ユーザで使用が始まっているが本格的な普及はこれから

2.3.2 医療サービスにおけるネットワークの利用

医療分野においてもネットワークを活用することにより、医療の質の向上、地域格差の解消等医療サービスの質的な向上と、病院を始めとする医療機関の運営の効率向上を図ることができる。ブロードバンドネットワークの高速大容量性は、医療にかかわる情報の交換、流通、および医療関連機関相互のコラボレーションに革命的な改善をもたらすと考えられる。

2.3.2.1 医療機関間での情報の共有

電子カルテなどの医療情報共有を実現するものである。医療情報 DB サーバを配置し、これに

地域の医療機関、検査センターなどが接続される。カルテ内容、検査結果、紹介状、退院時サマリなどの管理、蓄積を行うもので、以下に示すような効果を期待するものである。

- 電子カルテの教養による密接な医療機関連携の実現
- 急性期治療を行う期間病院と慢性安定期治療を行う医療機関との連携
- 生涯１カルテの実現、自分の病歴を参考に最適な医療を受ける。
- 大規模な電子カルテ DB に基づいた EBN（Evidence Baced Medicine）
- カルテ開示とセカンドオピニオン取得

2.3.2.2 医療機関間でのコラボレーション

医療機関同士のコラボレーションとは、図 2-3 のイメージに示すように、共同して医療行為を行ったり、情報の交換等でによりそれぞれにおける医療をより適切なものにするための情報の共有や、交換、さらには相互の助言の提供等が行うことを言う。

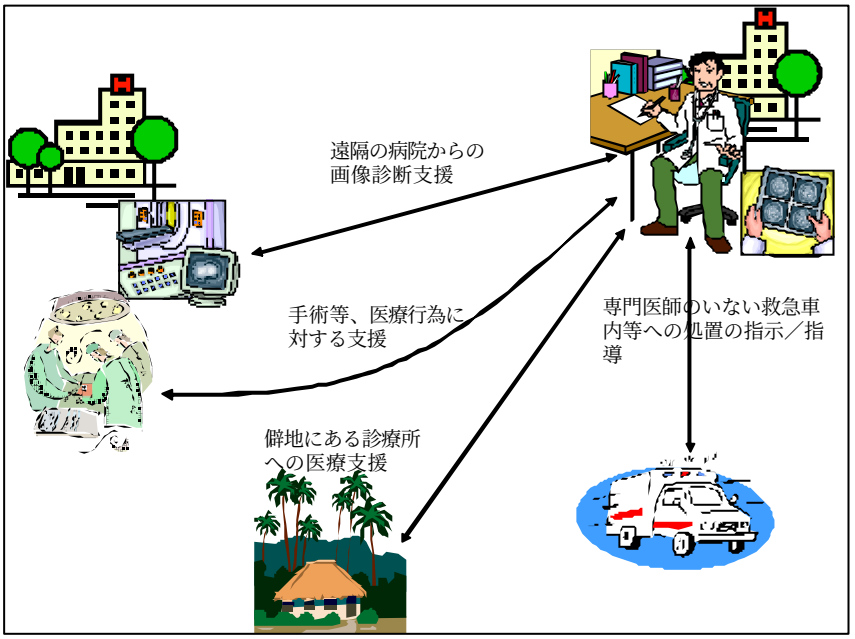


図 2-3 医療機関同士のコラボレーションイメージ

医療機関同士の リモートコラボレーションの対象としては、以下のようなものをその例としてあげることができる。

- 連携医療機関間でのグループ診療、手術等
- 専門医によるホームドクターの支援
- 医療機関による医師のいない医療関連機関に対する医療指導、医療支援

保健婦しかいない僻地診療所と中枢医療機関との間の遠隔医療、医師のいない救急車の

中に対する遠隔医療などがこれにあたる。この場合は、医師でなはないが医療従事者(コメディカル)が医療データを収集し、伝送先に送るため、上記の場合より条件がよい。

- 救急車内の救命士への救急処置の指導

このような医療機関同士のコラボレーションの進展は、以下のようなことの実現をもたらし、医療サービスの質の向上をもたらすと期待される。

- ホームドクターと大病院の連携の強化
- 医療に関する病院間あるいは地域格差の解消
- 専門医同士および専門が異なる医師によるグループ医療による高レベルの医療の実現
- 医療情報の個々の医療への反映

2.3.2.3 在宅ヘルスケアの支援 遠隔検診、遠隔診療）

在宅検診、在宅医療とは、患者は家庭に居ながらにして、血圧、心電図、尿検査データなどの生態情報を医療機関に伝送し、テレビ会議などを介して診療を受けられるサービスを言う。

以下に遠隔検診、遠隔診療のイメージを示す。

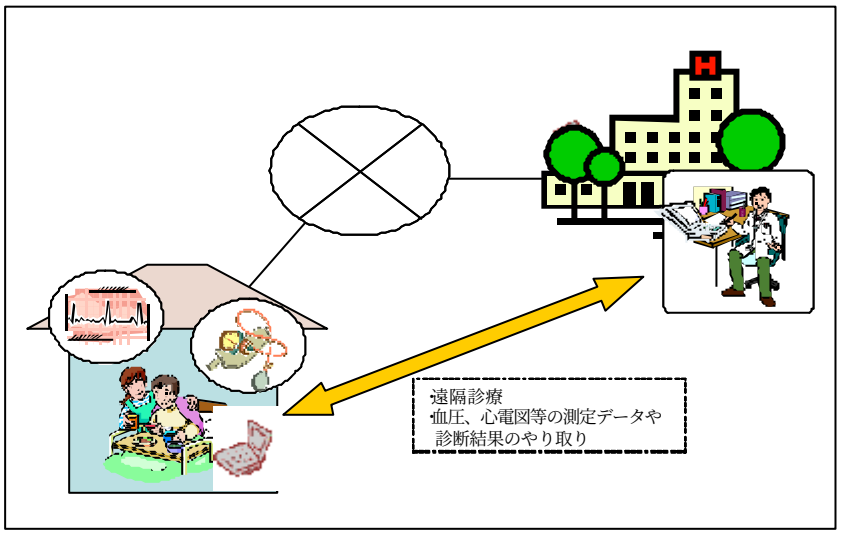


図 2-4 遠隔検診、遠隔診断のイメージ

周囲に医療機関がなく、検診あるいは診療に行くこと自体が大変であったり、時間がなくてつい行くことができないような場合に対して、オンラインで受診することができれば、距離と時間のバリアを克服することが可能となる。

遠隔診断や遠隔診療、遠隔健康相談等の適用分野としては、以下がその代表例としてあげられる。

- 慢性疾患患者の遠隔医療指導

● 在宅患者の遠隔医療機器使用指導

在宅介護支援センターの看護婦(士)と在宅患者の間で、テレビ電話のような機器を介して、機器の使い方の指導、服薬指導、栄養指導などを行う。特に機器等の使い方の指導は、例えば、在宅酸素療法、患者自身による注射の指導などを行う。

参考） 米国における在宅ヘルスケアシステム

米国で開発された在宅ヘルスケアシステムの構成を図 2-5 に示す。2000 年 8月より、米国の退役軍人協会の遠隔医療機関による実 証実験が始まり、2001 年 3 月には FDA（米国食品医薬品局）に認可された。この後、松下電器は2001 年7 月に米 CMHR 社と提携し、事業を開始している。

主な構成機器は「電子健康想定患者端末」「医師端末」「アクティブサーバ」である。

電子健康想定患者端末は、CCD カメラ、生体情報センサー（体温計、血圧計、血糖計、血中酸素飽和度計、心電計、聴診器）を搭載しており、生体情報はタッチパネル式で測定され、自動的に入力される。

一方、医師は、医師端末により患者情報を閲覧し、メールなどでアドバイスを送ることができ、アクティブサーバは、これら患者情報をインターネットを通じて蓄積、管理する機能を有する。

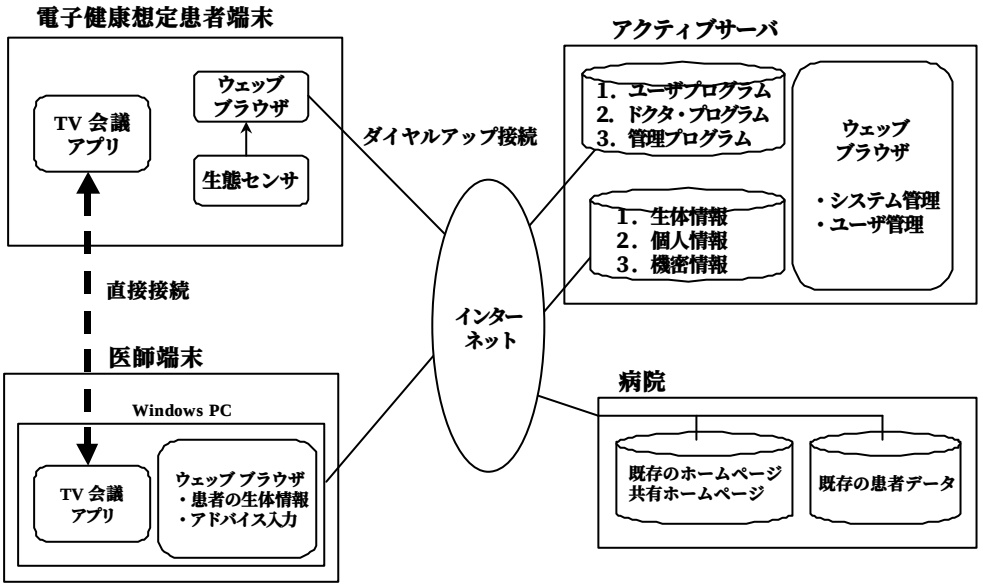


図 2-5 在宅ヘルスケアシステムの構成図

このシステムによりコールサービス、データの管理、異常値の通報などが行われると共に、医療サービスの質の向上と効率化が図られる。また、多くの医師やデータベースがネットワークで繋がることで知識の共有化が進展し、患者はよりすぐれた医療サービスを受けることができる。

また、このシステムにおいては、高齢者や障害者などコンピュータを操作できない人でも使いやすいように機器の大きさ、表示のしかたなどに工夫が凝らされている。また、患者自身による入力では、間違ったデータが入力されることがあるため、センターから自動的に記録する方式が採用されている。一画面／一操作、映像及び音声によるガイダンス機能が取り入れられている。

2.3.2.4 レセプト処理にかかる関係機関間のコラボレーション

診療報酬明細書(レセプト)の電子化に関連して、医療機関、審査機関、保険者を結ぶネットワークを構成し、診療報酬請求支払い業務のオンライン化を行うもので、以下のような効果を期待するものである。

- レセプト点検、審査業務の効率化
- 医療費用対効果分析等のためレセプトデータの DB 化
- 医療報酬回収期間の短縮
- 審査手数料の低減

2.3.2.5 処方箋処理のオンライン化

医薬分業の現行制度のもとでは、患者は医師の診察を受けた後、処方箋を受取り薬局に持参し必要な薬を受取ることになる。薬局を内部に持つ病院の場合はその問題はないが、薬局を持たない町の病院の場合は、病院を出て異なる場所にあるや薬局に出向き、ここで薬剤の準備が済むのを待たなければならない。

このため、処方箋がネットワークを介して病院から薬局へ直接届けられるようになり、この処方箋データとその処置についての薬局側の確認や、テレコンフェランスを用いた薬剤師と医師間の直接対話ができるようになれば、以下のようなことが可能となる。

- 患者が薬局に行った時にすでに薬剤が準備されていて、待ち時間を解消できる
- 必要に応じ薬剤師と処方箋を作成した医師との対話の円滑化による投与する薬剤に関する問題の未然防止
- 医師側からの投与薬剤の確認

システムイメージを、図 2-6 に示す。

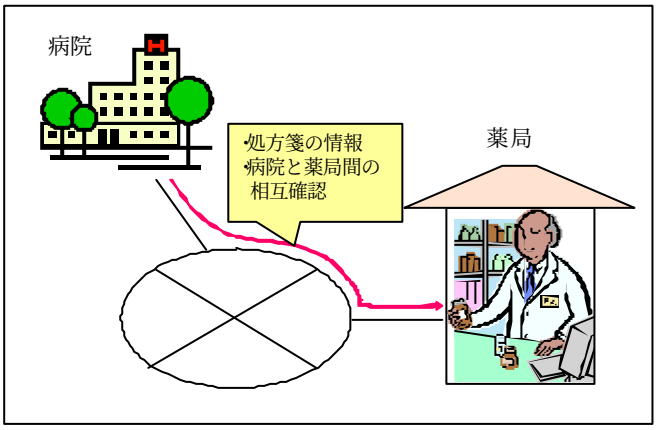


図 2-6 処方箋処理のオンライン化イメージ

ただし、このようなシステムにおいては処方箋データに改ざんは重大な結果を招くため、このようなシステムにおけるセキュリティの確保は万全でなければならない。

2.3.2.6 オンライン健康管理、健康相談

定期的な健康チェックや、健康維持のための相談や、軽い症状への対処等については、わざわざ病院まで出向かなくても、テレコンフェランスを用い健康相談員や医師とネットワークを介した対話でも用が足りることは多いと考えられる。職場や家庭に簡単な検診ツールがあり、この対話の中で健康診断員や医師が、体温や血圧等の確認や、診察カメラによる患部のチェックができれば、このような健康相談サービスの効率を上げるだけでなく、職場や家庭に居ながらにして気楽に健康相談が可能になることから、国民の健康向上にも寄与すると思われる。

2.3.2.7 医療機関情報の提供

病人やその家族にとってかかりたい病院や医師の選択も大きな問題である。また、緊急時に対応してくれる病院を探しあてることに手間がかかることも大きな問題とされている。

病気や怪我の治療を行いたいとき、その治療に適した医療機関がどこにあるのか、または医療機関の持つ方針や治療実績、医師の経歴等、医療機関の信頼に関わる情報や、医療機関の持つ施設設備に関する情報を集めることによって、患者が納得してより適した医療機関を選択することが可能となる。そのためには、医療機関に関する情報のデータベースが構築され、誰でもいつでも参照できるようになっていることが望ましい。

このようなサービスのイメージを、図 2-7 に示す。

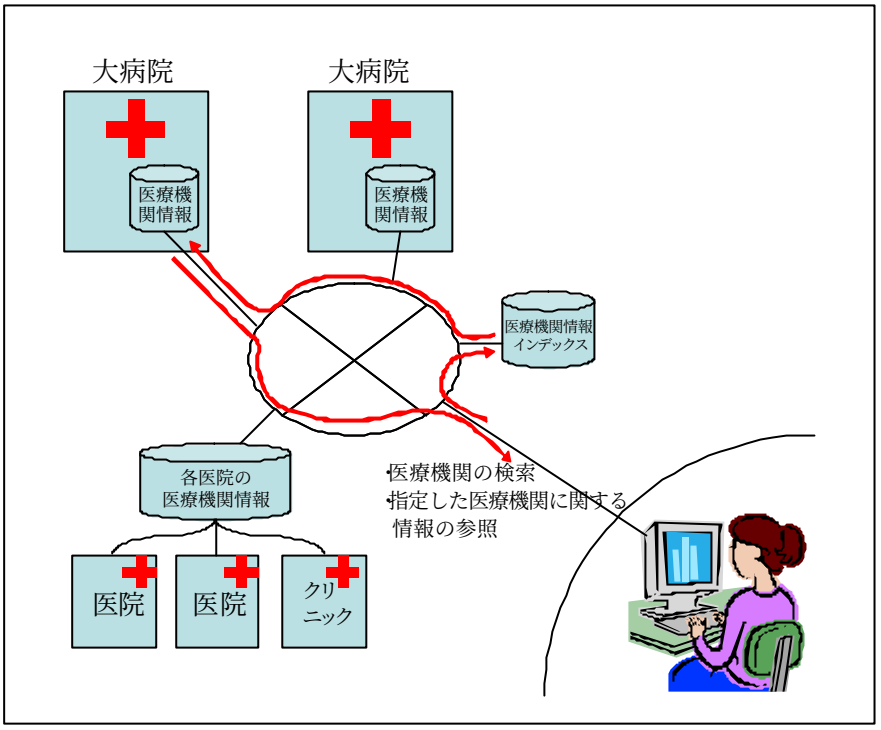


図 2-7　医療機関情報の提供・入手

参考）医療機関に関する情報提供の例－聖隷三方原病院の例

本節にあげた医療機関情報は、地域におけるあるいは他地域でも利用できる病院を網羅したものを期待したものであるが、すでに個々の医療機関で自分の病院に関する情報の提供を行っているところもある。

この病院では、収入や支出に関する情報を詳細に公表しており、手術の内容や治療の成績まで公開している。このように情報公開を積極的に行うことで、患者からの信頼も高まり、入院患者、手術件数とも増えているという。

ホームページ（http://www.seirei.or.jp/mikatabara/）では、各医師の詳しいプロフィールや、日別の専門ごとの担当医についても見ることができる。当院での医療行為に関するさまざまな統計データもかなり詳細に掲載されており、患者カルテの開示マニュアルも掲載されている。まさに“開かれた病院”であることがアピールされている例といえよう。

医療機関に関する情報の提供はの実現には、どんな情報をどのような形で提供するのか、その事業運営のスキームをどうするのかと言ったことについて、関係機関や国民の必要なる。

2.3.2.8 医師等医療関係者に対するネットワーク教育

医学／治療技術の進歩や治療薬の進歩にともない、医師等の医療関係者も、常に、新しい情

報を吸収し、スキルアップを図らねばならない。また、研修医等に対して基礎的な医療技術を体系的に教育していくことも現場では必要であると考えられる。

どちらの場合においても、医療技術、治療薬等に関わる情報が整理された状態で、どの医療機関からでも参照することができる環境が整備されることが望ましい。ブロードバンドネットワークの普及により、アクセスするための環境は整備されていくと思われるが、医療および治療薬のデータベースが整備されることが必要であろう。

また、コンテンツとしてリッチコンテンツを扱うことができるようになると、例えば治療や手術を映像で学習することも一般的なものとなる。

2.3.3 介護サービスや老齢者生活支援サービスへのネットワークの利用

ブロードバンドネットワークの特性をフルに活用することにより、老齢者だけでの暮らしや介護が必要な者を抱える家庭に対して以下のようなサービスの提供が可能となる。これらは、福祉の向上のためにも期待されるネットワークの利用形態であろう。

2.3.3.1 在宅ケアの支援

在宅ケアの支援には、要介護者自身への支援と、家族等周囲の者に対する支援がある。在宅ケアにとって大切なことの一つに、病気や障害を持っている人が気がねしないで相談でき、希望を聞いてもらえることがある。そのための環境作りの一つとして、介護機関と在宅ケアを行う本人のフェースツーフェースライクに会話できるテレコンフェランスシステムの導入がある。本人が不安に思うこと、してもらいたいことをいつでも気兼ねなく相談できる環境が必要であろう。

また、介護や老齢者の生活支援には、家族等の周囲の者に対する支援も必要となる。在宅医療機関の紹介や福祉施設の紹介、在宅ケアに関する注意事項等の情報提供サービスもこのサービスの一環である。これらのサービスがリッチコンテンツで提供されれば、家庭内で介護する者にとって、より容易に介護の方法を習得できるであろう。また、在宅医療機関とテレコンフェランスは、介護を行うための個別の指導を受けることも可能となる。

(1) サービス対象者の状態のチェックと必要な指示のオンライン化

福祉サービスの対象となる家庭に対し、サービス提供者は事前に定めた範囲で、暮らしや健康状態を常時(に近い形で)チェックし、問題が生じたと判断した場合は、テレコンフェランスを用い対象家庭とフェースツーフェース対話を行い、細かい状況の確認と必要な処置についての判断を行い、その時点で、オンラインで必要な指示をしたり、ヘルパー派遣の手当等を行う。

派遣されたヘルパーは、同じように専門家や専門医に、その場からリアルタイムに相談も可

能となる。このシステムのイメージを、図 2-8 に示す。

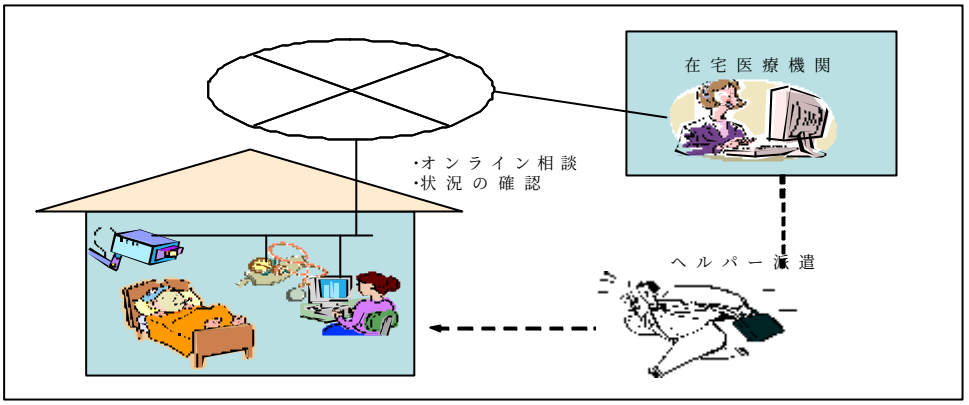


図 2-8 遠隔在宅介護サービスのイメージ

(2) 緊急時の処理のオンライン指示

ネットを介したモニタリングや家族等の通報により、緊急な対応が必要と判断された場合、テレコンフェランスを用いれば、介護の担当者はリアルタイムに状況を把握でき、必要な応急処置についての指示や助言を行うことが可能となる。

このことは、介護専門家の効率的な運用と、被介護者やその家族に大きな安心を与えるとともに、介護に携わる者にもサービスについてのゆとりを与える。

(3) オンライン相談

要介護者や老齢者だけでの暮らしにはさまざまな不安があり、家に居ながらにして気楽に専門のカウンセラー等に相談できるような環境に整備は望まれるものであろう。

それぞれの場合に応じ、相談センター等が整備され、このような家庭と相談対応者とテレコンフェランスを用いて、相談対応者が相談の背景となる状況についての判断ができるだけの観察ができ、かつ、フェースツーフェースライクな対話が可能になれば、その場で片付くものも多くなるとも考えられる。

このような環境の整備は、支援が必要な家庭にとっては大いに安心を届けるものとなろう。

2.3.3.2 サービス提供機関の運営管理

在宅介護を支援するサービスの提供を円滑に効率よく行うためには、システム的なサポートも必要となる。例えば、ホームヘルパーが決められた時間に要介護者に対して介護サービスを行っているかどうかのチェックを行うことは重要であり、介護時間管理の曖昧さが、しばしば両者の間で問題も引き起こしているともいわれている。ホームヘルパーの要介護者宅への訪問・退出時の時間チェックがその場でできることが望ましい。

ブロードバンドネットワークの特性である、“いつでも”、“どこからでも”、“安価に”繋げることが可

能となれば、訪問・退出の時刻を、要介護者宅に備え付けの端末、あるいはホームヘルパーが持参するモバイル端末からその場で入力することによって、ネットワークを通じてセンターで各ホームヘルパーの勤怠管理が一元的に行うことができ、また、こうした管理サービスにより介護保険金の請求処理もより容易となろう。

参考） 先行システム事例－ぴあラインシステム
利用社宅に通信端末を設置してホームヘルパーの訪問・退出時のチェックを行うサービスを実施している。ヘルパーは、利用者宅にて作業内容のボタンを押し、ID カードを挿入する。作業内容と時間についてのデータは、通信端末からセンターへ送信され、センターにて勤務実態の管理を行う。

2.3.3.3 サービスの提供にかかわ者に対するネットワーク教育

介護サービスが普及するにともない、介護サービスを行う者も、情報を吸収しスキルアップを図らねばならない。これは、介護センターに勤務する者ばかりではなく、家庭内で被介護者の世話をする者も対象となる。

これらの場合、介護サービスを行う上での介護方法、介護上の注意事項等に関わる情報が整理された状態で、どの介護機関あるいはどの家庭からでも参照することができる環境が整備されることが望ましい。ブロードバンドの普及により、アクセスするための環境は整備されていくと思われるが、介護サービスに関るデータベースが整備されることが必要であろう。

また、そのコンテンツのリッチコンテンツ化が進めば、具体的な介護の方法を映像で学習することもできるようになり、習得も容易となる。

2.3.4 教育サービス

教育には、学校教育から、学習塾、企業や機関等の組織内教育、カルチャーセンター等による生涯教育までさまざまなものがある。このうち組織内教育については、本報告書では 2.2 節に示すようにビジネス分野での問題として取扱っている。したがって、本節ではネットワーク社会において、社会サービスとしての学校教育、学習塾、および生涯教育等の教育サービスにおいて想定されるネットワークの利用形態について述べる。

ブロードバンドネットワークの進展にともなうテレコンフェランスシステム技術と利用環境の進展は、同じ場所にいなくてもフェースツーフェースライクな対話を実現できるため、発展したネットワーク社会においては、教える者と習う者が離れた場所にいても、またお互いがどこにいても、教室にいるのと同じような授業を受けることができる。ネットワークを利用した教育・学習の一般的なコンセプトやシステムのイメージは、1.2.3 節の eラーニングで述べた通りであるが、教育サービスの現場におけるネ

ットワークの利用形態としては、①ネットワーク教室（遠隔リアルタイム授業）、②オンデマンド個人レッスン、③オンデマンド自習等がある。またこれらネットワークを活用した教育サービスを支えるものとして、④教育ライブラリ、の充実も重要であるが、これについては 2.3.6 節であらためて述べる。

次図に教育サービスにおけるネットワークの利用イメージを示す。

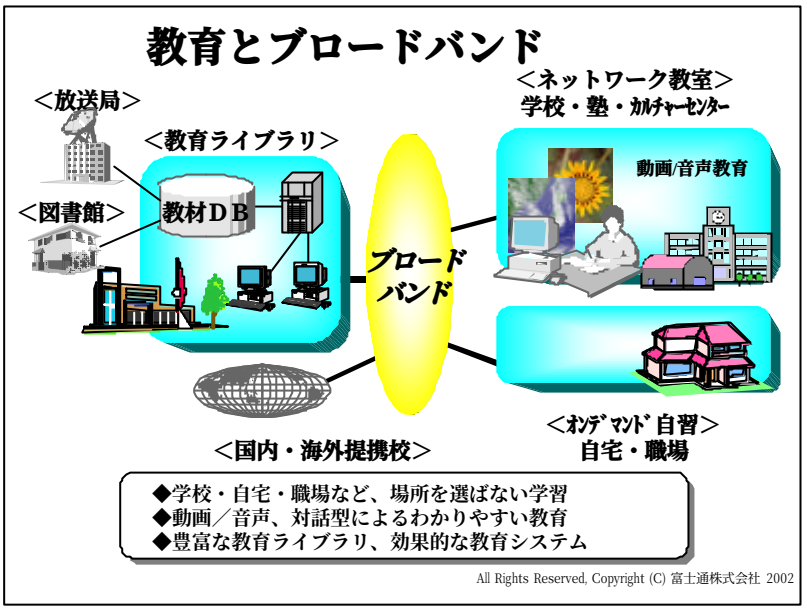


図 2-9　教育とブロードバンド

2.3.4.1 ネットワーク経由での授業

ネットワーク教室とは、教室で行われる授業をブロードバンドネットワークを介して学内または学外の離れた場所にある複数の教室や自宅等の、教育現場とは別の場所でも同時に受けることができるようにしたものである。ネットを介して行う授業は、先生と生徒が同じ教室にいた従来型の授業の補填あるいは代替するものと考えられる。ここでは双方向性を活かした講師と生徒との対話も可能であり、状況に応じて 1対N、1対 1と自由に切り替えられるなど、従来の対面教育をしのぐ効果が期待できる。最近拡大しつつある大学間の交流（相互に授業が受けられる等）もネットワークの活用で加速されると思われる。

このようなネットワーク経由での授業の利用形態や利用目的は、学校や学習塾、生涯教育等、教育機関や提供している教育により異なったものとなる。

2.3.4.2 ネット経由での個人レッスン

家庭など個人生活へのブロードバンドネットワークの普及は、教室ばかりでなく自宅からのネット

ワーク授業の利用を容易にし、個人の教育に対する選択肢を拡大する。自分の都合の良い時に、テレコンファレンスを用いて教育機関にいる講師とフェースツーフェースライクな対話により個人レッスンが受けることが可能となる。これはまず学習塾や趣味の教室等でのサービスレベルの向上手段から始まり、次第に一般の教育現場にも浸透して行くものと思われる。またここでは個人毎の学習環境の設定や学習進捗把握とそれによるきめ細かい指導も行うことが可能となる。

2.3.4.3 自習のサポート

授業のビデオ映像やさまざまな教育コンテンツをデジタル化して、メニュー化されたカリキュラムとして教育ライブラリに登録しておくことにより、個人が都合のいい時にアクセスし希望する教育を受けることができる。これは前述の「オンデマンド個人レッスン」と組み合わせて利用することにより、より効果的な学習が可能となる。また個人が必要な時にまたアクセス記録などを管理・活用することにより、学習進捗状況の把握、きめ細かい学習指導などの効果も期待できる。

2.3.5 ネット経由での教育のメリット

これまで述べてきた、ネット経由での授業、個人レッスンの提供や、自習のサポートの特徴と教育提供側と受講側それぞれの立場からのメリットを、表 2-10 に示す。

表 2-10 ネットワーク教室、オンデマンド個人レッスン／自習の特徴とメリット

項目	内容
特徴	・生徒はどこからでも都合の良い時間に、自分の求めるレッスン教材にアクセスでき、メディアを駆使した自習が可能 ・サービスによっては、疑問点等やテスト結果等について指導講師とテレコンファレンスを用い、疑念が生じた時点でフェースツーフェースライクな対話により指導を受けることが可能
教育提供側のメリット ・教育レベルの向上 ・高効率経営の実現	・適切な講師の確保と工夫した教材の作成によりレベルの高い授業を全国を対象に提供が可能 ・ビジネスの規模が拡大しても、規模に応じた教師の手配が不要（少数精鋭による事業展開が可能） ・受講者数に合わせた教室等の施設の準備が不要（ただし、オンデマンド対応するためのシステムおよびサポート体制が必要となる） ・競争優位を確保できた場合のシェアの拡大が容易（ただし、その分、教育内容やその提供にかかるサービスについての競争は激化）
受講側のメリット ・学習達成度の向上 ・利便性の向上 ・学習費用の低減	・地域的な問題に影響されずレベルの高い授業の受講が可能 ・いつでも都合の良い時間に、都合の良い場所で受講でき、勤務その他の生活との時間調整が容易 ・自分の学習進度に応じたペースでの受講が可能、場合によっては同じ授業を繰返し学ぶことも可能 ・教室や生徒数に見合った講師の手配の不要化等による授業料の低下や、交通費の不要化等による学習費用の低減への期待

2.3.5.1 教育機関別の教育サービスにおけるネットワークの利用イメージ

前節に示した教育サービスにおけるネットワーク利用は、教育機関によってその適用方法は異なったものなる。以下に各教育機関別で想定される利用方法について述べる。

(1) 小・中・高等学校におけるネットワーク教育の利用

初等ないしは基礎的な教育をおこなう小・中・高等学校においては、これまではパソコンの設置やネットワークへの接続といったインフラの整備に注力されてきたが、今後は授業等へのネットワークの活用に焦点は移って行く。下表に、小・中・高等学校において想定されるネットワークの利用場面を示す。

表 2-11　小・中・高等学校におけるネットワークの利用

利用場面と狙い	利用形態
ネットワーク教室 ・授業内容の充実 ・生徒の授業への興味の向上 ・登校できない生徒に対する受講機会の提供	・他校との合同授業 ・病欠等で教室に出席できない生徒が自宅で受講 ・自宅での補修の受講
オンデマンド個人レッスン ・生徒の習熟度の向上	・テレコンファレンスを用いた個人別の補修要求への対応 ・テレコンファレンスを用いたQ&A、宿題の指導
オンデマンド・生徒の習熟度の向上 ・生徒の学習への意欲の向上	・授業ビデオへのネットワークアクセスによる自習 ・興味ある科目、不得意科目についての自習

(2) 大学、専門学校におけるネットワークの教育利用

高等教育及び専門的な教育を行う大学や専門学校においても、ネットワークの教育利用は欧米に較べて遅れていた。しかし、近年ネットワークコースの設置などの取組みも始まるなど、ブロードバンドネットワークの環境整備に合わせて大学間合同授業が一層の進むと考えられる。

表 2-12 に、大学や専門学校において想定されるネットワークの利用場面を示す。

表 2-12　　大学および専門学校ネットワークの利用

利用場面と狙い	利用形態
ネットワーク教室 ・経営効率の向上 ・授業内容の充実 ・受講機会の拡大	・他校との交換／合同授業 ・分校舎に対しての同一授業の提供 ・教室外・遠隔地にいる講師による授業 ・教室外受講（自宅や職場） ・研究会へのリモート参加 ・バーチャルスクールの運営
オンデマンド個人レッスン ・指導効率の向上 ・社会人学生の学習機会の拡大	・テレコンファレンスを用いた研究指導
オンデマンド自習 ・学習効率の向上 ・学生の学習・研究等への意欲の向上	・授業ビデオへのネットワークアクセスによる自習 ・自己の研究テーマや興味あるテーマについての学習

(3) 学習塾におけるネットワーク教育の利用

少子化等による学習塾間の競争も一層厳しくなり、その中でネットワークを利用した教育の質の向上による差別化を図るため導入も加速すると考えられる。表 2-13 に、学習塾において想定されるネットワークの利用場面を示す。

表 2-13　学習塾におけるネットワークの利用

利用場面と狙い	利用形態
ネットワーク教室 ・経営効率の向上 ・授業内容の充実 ・受講機会の拡大	・分校舎に対しての同一授業の提供 ・教室外にいる講師による授業 ・教室外受講（自宅） ・バーチャルスクールの運営
オンデマンド個人レッスン ・指導効率の向上 ・生徒の習熟度の向上	・テレコンファレンスを用いた学習指導
オンデマンド自習 ・学習効率の向上 ・習熟度の向上	・授業ビデオへのネットワークアクセスによる自習 ・不得意科目など特定科目についての自習
教育ライブラリ例 ・授業の補足的利用 ・他塾差別化	・人気講師の授業ビデオ ・志望校別対策ビデオ等

(4) カルチャーセンターにおけるネットワーク教育の利用

カルチャーセンターとは、技能教育や生涯教育等、個人（主として社会人）の要望に応える教室であり、英会話教室や音楽教室や文学教室等を指す。表 2-14 に、カルチャーセンターにおいて想定されるネットワークの利用場面を示す。

表 2-14　カルチャーセンターにおけるネットワークの利用

利用場面と狙い	利用形態
ネットワーク教室 ・経営効率の向上 ・授業内容の充実 ・受講機会の拡大	・分校舎に対しての同一授業の提供 ・教室外にいる講師による授業 ・他校との交換あるいは合同授業 ・教室外受講（自宅など） ・研究会へのリモート参加 ・バーチャルスクールの運営
オンデマンド個人レッスン ・指導効率の向上 ・社会人学生の学習機会の拡大	・テレコンファレンスを用いた実技指導等
オンデマンド自習 ・学習効率の向上	・授業ビデオへのネットワークアクセスによる自習 ・好みのみテーマについての自習

2.3.5.2 ネットワークを利用した教育への取組み事例

表 2-15 に、ネットワークを教育に利用している事例を示す。

表 2-15 ネットワークを教育に利用している例

教育の種類	実施機関	備考
バーチャルスクール いずれも海外の学校と提携	アットマーク インターハイスクール	http://www.inter-highschool.ne.jp
	EIKOH WEB インターナショナルスクール	http://www.eikoh-internet.com
大学のインターネットコース	人間総合科学大学	http://www.human.ac.jp
	信州大学バーチャル大学院 （平成 14 年開港予定）	http://gipwm.shinshu-u.ac.jp
	WIDE大学SOI （スクールオブインターネット）	http://www.soi.wide.ad.jp 東京大学、慶応大学、奈良先端科学技術大学院大学他の大学が共同で実施しているもので、これまで個人向け遠隔リアルタイム授業実験なども行っている。（日本の大学に編入予定のマレーシアの学生向け）
その他	メディアキッズ （1994~2001. 3）	http メディアキッズ・コンソーシアムが、国公立私立の全国の小・中・高・特殊教育諸学校を対象に進めてきたプロジェクトで54校が参加。（1999 年 7 月時点）
	こねっとプラン （1996~2001. 3）	http://www.wnn.or.jp/konet 「こねっと・プラン推進協議会」が活動主体となり、教育でのマルチメディア環境の整備と活用を推進するプロジェクトで、全国の小・中・高・特殊教育諸学校におけるインターネット利用、各種プログラムを推進。約1000校が参加
	柏インターネットユニオン（KIU） 柏市	http://www.kiu.ad.jp 柏市を中心とした地域の小・中・高校、近隣センター、図書館等の公共性の高い組織のシステムを相互接続し、情報教育及び情報活用能力の向上を図る。図 2-10 に柏市教育ネットワーク構成図を示す
海外（主として北米）	ケンタッキーバーチャル高校 （米国 2000. 1~）	http://www.kvhs.org/ 成功を機に 13州でバーチャル高校が発足（フロリダ・オンラインハイスクール等）
	タコマ・パーク中学校 （米国）	数学、コンピュータ関連の英才教育を実施するマグネットスクール
	エルムウッドスクール （高校 カナダ）	http://www.elmwood.on.ca/ 全教材を学校のWEBに乗せ、インターネットを利用した授業を実施。生徒は家庭でも利用
	ウェストマウントパーク 小学校（カナダ）	32カ国の生徒が学ぶ異民族・多文化の学校で、宿題ヘルプや情報収集のためほとんどの生徒が家庭でもインターネットを利用
	大学のオンラインコース ・スタンフォード大学 ・フェニックス大学 ・サザーン電子大学	http://scpd.stanford.edu/scpd/students/onlineClass http://uoponline.com http:// www.electroniccampus.org

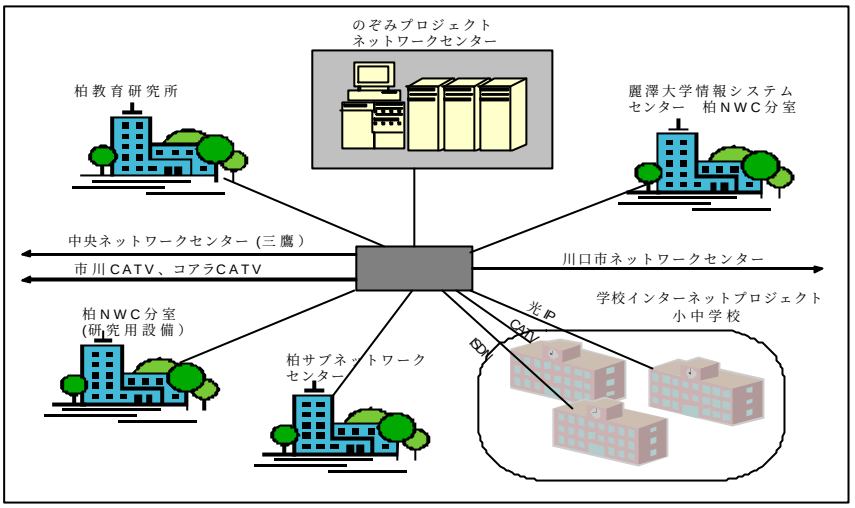


図 2-10　柏市教育ネットワーク構成

2.3.6　情報、コンテンツ提供サービス

ブロードバンドネットワークの普及にともない、家庭にいながらにしてさまざまな情報を入手することが可能となる。これまででも家庭からインターネットを通じて情報の入手は可能であったが、リッチコンテンツを扱うことが可能となることにより、映像や音声を活かした形で、利用者にとってより理解しやすいサービス提供形態へと変わってくるだろう。

2.3.6.1 報道情報のネットワーク提供

ニュース情報の提供は、現在でも画像やテキストベースで行われており、映像や音声の組み合わせについてもいくつか試みられているが、広帯域の利用が当たり前になれば、映像や音声の活用についても当たり前となるであろう。それによって、現在テレビで見られるようなニュース放送が、インターネットを通じてオンデマンドで見ることができるようなスタイルに変化してくるのではないだろうか。

2.3.6.2 各種公共サービスに関する情報の提供

各種公共施設の案内や施設利用の予約、地方自治体から住民への各種情報提供が、オンラインでいつでも見ることができるようになり、直接現地に行かなければ分からなかったことも、家庭に居ながら知ることができるようになる。

また、テレコンフェランスを用いれば、公共施設や地方自治体へ映像を通して直接相談すること

も可能となる。

【事例】

ウチダデータは、地方自治体などが行政のために保有している地図情報を、地域住民がパソコンや携帯電話を使って手軽に見ることができるようなシステムを開発している。これにより、例えば地盤が弱い危険地域情報や、病院や公衆トイレなどが簡単に分かるようになる。

2.3.6.3 暮らしにかかわる情報の提供

近くのスーパーや食料品店の販売情報や駅の時刻表、気象情報など、地域生活に密着した情報を家庭にいながら知ることができる。

このような情報提供が活用されるためには、誰でも簡単に情報発信できるような環境ができることが必要である。

気象情報提供サービスについては、気象庁やその他民間によるサービス提供も行われており、民間の予報業務認可事業者数も 40 社を超えている。民間では、例えば雷に特化した情報の提供や、局地予報を行うなど、気象庁が提供していないサービスを提供するなど、さまざまなサービス提供が試みられている。

また、食品の原産地を確認できるサービスも展開されている。これは、産地の偽装表示に対する問題に対する施策の一環であり、一例としてはインターネットで青果 1700 品目の原産地を確認できる「青果ネットカタログ」をあげることができる。これは、青果の生産者が栽培地や有機農産物の認証の有無、生産者の連絡先を登録し、生産品目に 8桁の認証番号が発行される。生産品目にはその認証番号が書かれたラベルが貼られ、流通業者や消費者がその番号を使ってインターネット上で調べるとその商品に関する情報を見ることができる。情報としては、その他栽培方法や使用した農薬、写真や音声なども扱うことができる。

2.3.6.4 教育ライブラリの提供

ネットワークを活用した教育サービスを実現する為には、教育の場で活用できるような学習素材ライブラリ、及び種々の教育支援情報を一元的に管理し学内で情報共有が図れるような学習情報システムの整備が不可欠である。このサービスは、各教育機関が独自に開発するもの、民間企業がビジネスとして提供するものの双方が考えられる。

(1) 学習素材ライブラリ（コンテンツ）

コンテンツには、教育のために先生などが作成した教材のほか、教材作成の素材や補助的な情報（例えば美術館、博物館と連携した美術、歴史に関する映像情報など）もある。

グローバル化の時代においては、他人の「文化」を理解した上で交流することが重要であ

る。その際各個人が確固たる文化的背景を持って交流を行うことが必要で、教育においても、従来の知識中心の教育から、個人の個性・感性を伸ばす教育、「文化」を学ぶ教育への変革が強く求められている。そのため教育の現場で有効に活用できるような情報を、地域の自治体、放送局、図書館、美術館等と連携して整備し、音声・映像・統計情報などさまざまな形で利用できるライブラリとして整備して行く必要がある。次表に、さまざまな機関・企業が提供するコンテンツの例を示す。

表 2-16 各機関・企業が提供する教育コンテンツの例

提供者	提供する教育コンテンツ例
学校 （小学校～大学、専門学校、塾等）	・各授業、講義のビデオ ・各教科の補助資料（科学実験、美術、歴史など）
メディア （放送局、新聞社、出版社など）	・放送番組素材の再編集（自然、歴史、伝統芸能など） ・新聞、書籍、雑誌等の記事素材の再編集
公私立の機関 （自治体、図書館、美術館、博物館等）	・地域の文化、経済などの紹介ビデオ ・美術館、博物館収蔵品などのデジタルアーカイブ情報
教育ビジネス事業者	・上記のような教育コンテンツを、学校／メディア／各機関等と連携して（または独自に）制作・販売

(2) 学習情報システム

教育サービスを支えるシステムとして、個人の学習記録、嗜好、性格、要望などを把握し、個人個人に合ったより効果的な教育が行えるような機能構築が必要となる。単なる管理情報の集積だけではなく、「教育ＣＲＭ」と言うべき考え方を導入していくことが求められる。その一環として、受講コースの選択、受講の申込み、実際の受講、教材の購入、個人に対する進路指導などをワンストップでサービスするシステムの構築は、受講者の利便性の向上と共に学校側にとっても教育事業の効率化、差別化に効果的である。

(3) 教育ライブラリの事例

現在既に提供が始まっている教育ライブラリを例示すると、表 2-17 のようになる。

表 2-17 教育ライブラリの提供例

教育ライブラリ	概 要
教育用画像素材集 www2.edu.ipa.go.jp/gz/	IPAの「教育の情報化推進事業」の一環として（財）コンピュータ教育開発センターが開発したもので、学校・教育機関が自由に使える。 日本文化（伝統工芸・芸能）、世界の地形、遺跡、歴史映像、理科実験、動物他
ThinkQuest 米国：www.thinkquest.org 日本：www.thinkquest.gr.jp	米国で開始された教育用ＷＥＢ国際コンテスト。価値あるものは教材ライブラリに登録され（約数千作品）、200万アクセス／月といわれている

表 2-17 教育ライブラリの提供例

教育ライブラリ	概　要
マルチメディア教材データベース www.gakujoken.or.jp	財)学習ソフトウエア情報教育センターが提供する有料の教材集
教育情報ナショナルセンター（文部科学省）	教育・学習に関するポータルサイト。学校教育から生涯教育までの情報化推進。次図に教育情報ナショナルセンターの構想を示す
先進学習基盤協議会（ALIC） www.alic.gr.jp	教材や教育システムに関してコンテンツ相互運用性、国際標準化の検討、及び次世代ｅラーニング研究等を行う目的で発足

参考資料」

－ネットワーク白書２００１（インターネット協会）

－第18回情報教育政策セミナー資料（日本教育工学振興会主催　2002.3.16）

－学習情報研究（学習ソフトウェア情報研究センター）

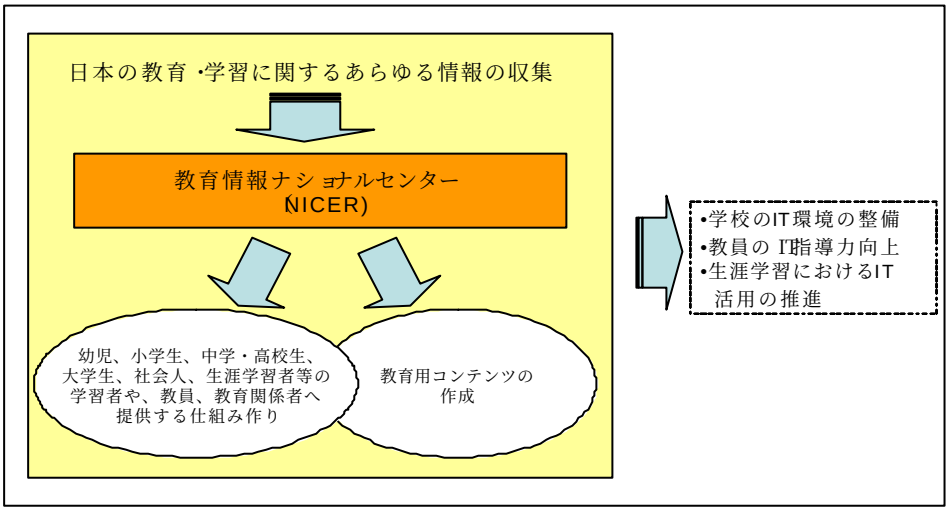


図 2-11 教育情報ナショナルセンターの構想

2.3.6.5 各種知識情報の提供

病気や薬に関する知識や、趣味や道楽に関する知識、語学に関する知識など、知りたい知識が、知りたいと思った時にいつでも入手可能となる。リッチコンテンツがネットで閲覧可能となることにより、より分かりやすく詳しい情報の提供が可能となる。

2.3.6.6 その他個人使用向けのデジタルコンテンツの提供

書籍や音楽、ビデオなど、個人で所有し楽しむための情報が、ブロードバンドネットワークの特性により、楽しみたいときに簡単に見たり聴いたりすることができるようになる。このことにより、個人生活の効率化を図ることができる。

また、テレビ放送がインターネット経由で見たいときに見ることができるようにもなってきている。例えば、楽天では、「楽天 TV ショッピング」を開設し、テレビ通販番組をネット上で見ることができるようにしている。また、エー・アイ・アイでは、インターネット上で毎日 5 時間動画番組の配信を始めている。

また、自動車向けの情報提供サービスも各自動車メーカーにより展開されている。日産自動車は、NTT ドコモと共同で、車を運転しながら店舗情報を検索したり、音楽やニュースの配信を受けたりできる情報提供サービスを行っており、トヨタ自動車も KDDI と「G-BOOK」という情報提供サービスを提供中である。

2.4 ネットワークがもたらすコミュニティ活動の活性化

コミュニティ活動は、行政機関や企業等と比べると、常勤者を中心とした組織でないため、活動参加者のほとんどは一般に本業を別に持ち、活動の参加者が一同に会することはそう簡単でないこと、多くは組織運営上の業務プロセスも十分に整備されていない等で、その運営は比較的貧弱な事務局や主宰者個人の取纏め能力に依存いることが多い。このため、組織的な活動を限られたものにしている。活動参加者や活動の周囲にいる者から見れば、活性化が望まれているものも少なくないであろう。

コミュニティ活動におけるネットワークの利用は、以下に示すように、コミュニティ活動の形態を変え、その活動をより活性化することができると考えられる。そして、ネットの利用があってこそ成立するようなコミュニティも多く形成され、さまざまな活動が展開されることが想定される。コミュニティの活性化は、社会をより良いものにするだけでなく、参加者の人生をより充実したものにすることにもつながる。

(注) ここで言うコミュニティとは、以下のようなものを指す。
各種 NGO、各種NPO、各種団体、地域コミュニティ、PTA 他の同窓会等学校周辺組織
企業 OB 会等企業周辺組織、趣味等の同好会、スポーツチーム等

2.4.1 コミュニティ活動におけるネットワークの利用場面

コミュニティ活動におけるネットの活用場面としては、

- 組織運営への利用
- 活動の場としての利用

の 2 面がある。

(1) 組織運営への利用

コミュニティの組織運営における以下に示すようなところにネットを上手に活用すれば、コミュニティ運営にかかる負担を減少するとともに、会員の募集や活動の活性化を図ることができる。

- コミュニティの存在と活動状況の紹介
- 会員の募集
- 会員や会費の管理他のコミュニティ管理業務
- 活動状況や活動成果のまとめと社会への発信
- 会員同士のコミュニケーションや活動に対する会員からの評価の収集と討議
- コミュニティと社会とのコミュニケーション
- 組織運営にかかる活動の案内等

(2) 活動の場としての活用

コミュニティ活動には、参加者の意見の集約や、情報の交換、意見の交換、機関紙や報告書の作成等のオフィス作業等もある。コミュニティによっては、これらの作業が活動のその中核と言えるものもあろう。

2.4.2 コミュニティ活動におけるネットワーク利用の効果

コミュニティ活動の組織の運営にあたって、ネットワークを上手に利用に利用することにより、コミュニティは以下のようなことが期待できる。

- コミュニティの存在とその活動の社会での認知の向上
- 参画者の拡大
- 活動の質の向上
- 活動成果の普及および活用の促進
- 参加者の活動参加にあたっての利便性の向上

(1) 社会におけるコミュニティの存在とその活動の認知の向上

コミュニティは、その存在と活動内容やその成果が社会で周知されるこは、活動の目的に

沿うものであるだけでなく、活動の活性化にもつながる。ネットを用い、コミュニティの設立主旨、会員構成、活動内容、活動状況、成果等を、社会に発信することにより、コミュニティの存在とその意義を地域や年齢層等を問わず広く社会に知らしめることが可能となる。特に、公的な役割を持つコミュニティにとっては、Web やメールを用いた情報の発信や、テレコンフェランスを用いた、社会とのコミュニケーションの充実は、、特に重要となる。ブロードバンドネットワークの進展がもたらす、より豊かな情報の発信と、テレコンフェランスによるより密度の高いコミュニケーションの実現は、コミュニティの社会での位置付けをより高いものにしてくれると考えられる。

ただし、このような活動についてのホームページへのアクセスを広げるためには、コミュニティ活動についての専門のポータルサイトの登場も必要であろう。

(2) 参画者の拡大

コミュニティの存在やその趣旨、活動メンバー、活動状況、成果等が広く認知されれば、そのような活動を知らなかった者にも活動へも参加を促すことになろう。また、ネットワークを介して活動に参加できるようになれば、コミュニティの活動拠点とは離れた場所にいる者、多忙で活動の場に出向くことが困難な者の参加も期待できる。

(3) 活動の質の向上

ネットワークの活用により、

- コミュニティ活動の主旨に賛同し、活動に貢献できる者の参加の機会の増大、組織の人的能力の向上
- テレコンフェランスシステムの活用による集会のバーチャル化による意見交換機会の拡大
- 情報の活用の能力の向上
- 運営事務の効率化による本来活動へのエネルギーの集中

等が期待でき、この結果、コミュニティ活動の質的な向上が期待できる。

(4) 活動成果の普及および活用の促進

コミュニティ活動の成果の社会での認知やその活用も、コミュニティとしては期待するところである。このため、ネットを活用し活動の成果やその利用法を広くPR することも重要となる。社会からの成果の評価やその活用の拡大は、コミュニティの活性化だけでなく、社会への貢献にも繋がる。

(5) 参加者の活動参加にあたっての利便性の向上

コミュニティ活動への参加の阻害要因は、活動参加の時間がとりにくいこと、活動の場に出向くことが面倒なこと、活動にかかる諸手続き面倒なこと等があげられる。ネットを介して行える活動を活動の中核としたり、諸手続きをネット経由で行えるようにすれば、より多くの人が活動に参加するだけでなく、大きな貢献もできるようになろう。

2.4.3　コミュニティ活動におけるネットワーク活用の事例

コミュニティ活動にネットを積極的に活用している事例を、以下に紹介する。

(1)　「ENVIROASIA」：環境問題をテーマとした情報交換の場

市民レベルで環境問題に対する情報を共有する。「ENVIROASIA」では、日本と中国、韓国にある環境 NGO が連携し、各国の環境協力を進めるために環境に絡む情報や対策を市民レベルで共有する場としている。

ENVIROASIA の URL　http://www.enviroasia/info/

(2)　「言論 NPO」：さまざまなテーマについての議論の場

特定の議題について、専門家、あるいは興味を持つ者で意見交換を行う場をネット上に提供する。例えば、「言論 NPO」では、ある議題について各界の専門家に自由な意見交換を求め、この議論の結果をもとにそれを政策提言に繋げることを狙いとしている。

言論 NPO の URL　http://www.genron-npo.net/

(3)　「ぼきんやドットコム」：NPO 活動

NPO では、ネットを通じてさまざまな情報発信や意見交換等を行っているが、その活動の 1 つとしてネットを活用した募金活動が始まっている。

例えば、財団法人オイスカが運用するサイト「ぼきんやドットコム」は、米国同時テロへの義援金やアフガニスタン難民支援募金をネット上で集めている。

ぼきんやドットコムの URL　http://www.bokinya.com/

(4)　「アスク」：地域住民コミュニティ

市町村等で、地域住民間の情報交換、あるいは意見交換を行うようなコミュニティ活動がネット上で行われている。例えば、回覧版のネット化や、地域イベントの開催案内やコミュニティペーパーの情報をネット上で提供するなどの活動である。

また、マンションでも、近隣のスーパーや食料品店、クリーニング店等の商店の情報をマンション住民に流したりマンション住民内のコミュニティを形成するのにネットが利用され始めている。

例えば、アスクでは、マンション近隣の商店の広告をマンション住民に流し、その広告料の一部をマンション内のホームページ運用に充てるといったマンション住民のコミュニティサービスの提供を開始している。

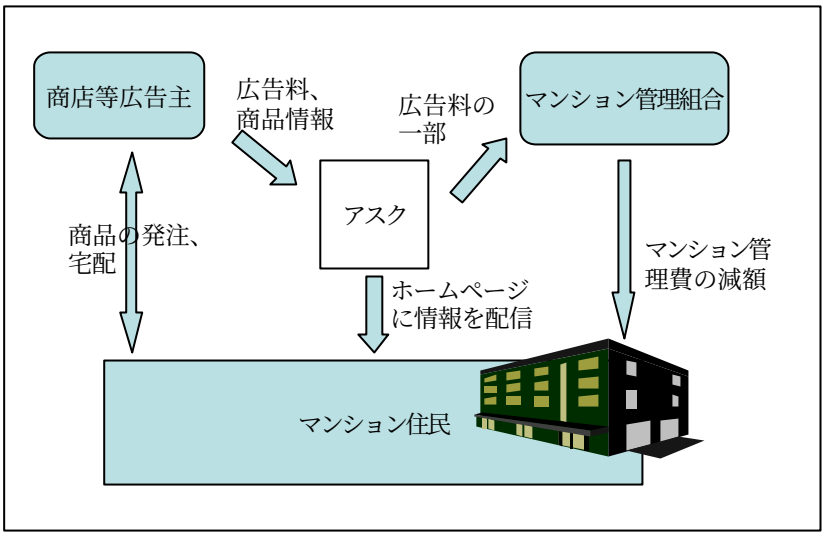


図 2-12　アスクのマンションを対象としたコミュニティサービスの仕組み

(5)　その他－政治団体

政党等の政治団体あるいは政治団体のメンバーによる政策や経歴のアピールを行うことにより、事実上の選挙活動をネット上で行う。また、選挙活動以外にも、市民からの意見を募っているケースもあり、ネット上での献金も一部始まっている。

2.5　家庭生活におけるネットワークの利用

2.5.1　家庭のネットワーク化のイメージ

家庭は、行政機関、教育機関、医療機関、福祉サービス機関等の各種の社会的なサービスを提供する機関や企業のみならず、職場、各種のコミュニティ、親戚や友人の家庭とネットワークでつながれ、さまざまなサービスの利用や、活動への参加、通信ができるようになる。家庭が社会の全体とネットワークでつながれた様子を、図 2-13 に示す。

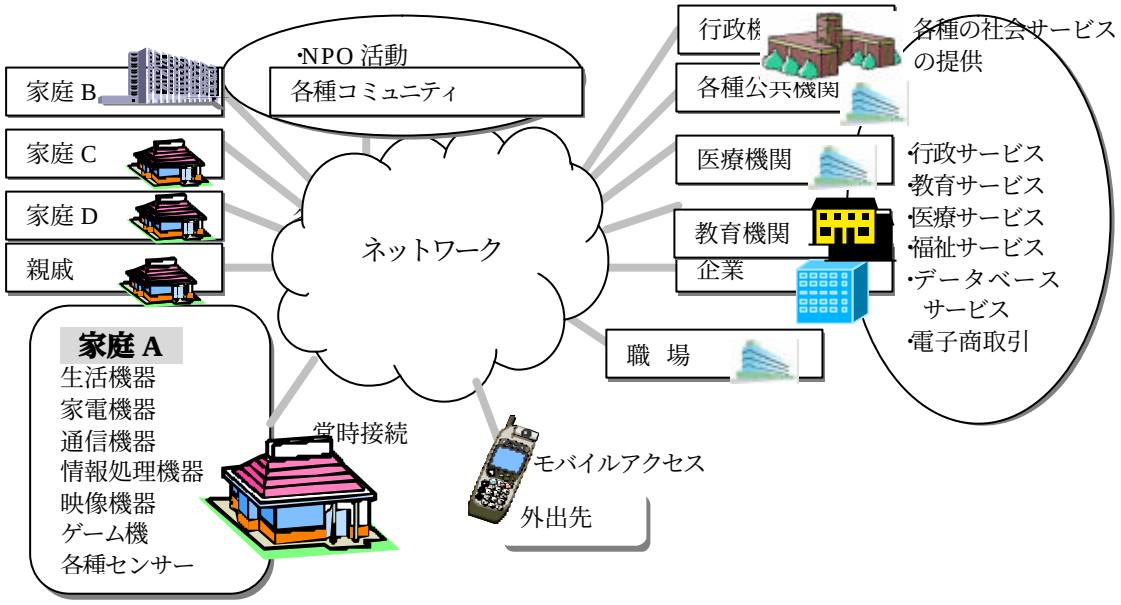


図 2-13　ネットワークによる家庭と社会のつながり

また、家庭内においても、PC 等の情報機器だけでなく、インテリジェント化した家電等の生活機器も、LAN や無線 LAN あるいは電灯線ネットワークで、相互に接続されるだけでなく、その一部はホームゲートウェイを介して、外部と接続されることになる。

2.5.2　家庭におけるネットワークの利用分野の一覧

また、家庭におけるブロードバンド時代において想定されるネットワークの利用を、表 2-18 に示す。

表 2-18 家庭におけるネットワークの利用

	利用場面	代表的なネットワークの利用形態	重要性	想定される普及度合い		
				現在	5年後	10年後
1	家庭におけるくらし	⑴家庭内機器間の自動コラボレーションと自律運用	△		＊	△
		⑵家庭の外からの家庭内機器の操作と動作状態のチェック	△		＊	△
		⑶家庭の外からの家庭状況のモニタリング	○	＊	△	○
		⑷家庭やその他の場所からの家庭の延長線上といえる場のモニタリング	○	＊	△	○
		⑸防犯、防災	◎	＊	○	◎
		⑹ホームショッピング、ホームバンキング、各種リザーベーション	○	△	○	◎
		(7) さまざまな情報の入手	△	△	○	◎
		⑻多様なデジタルコンテンツの入手	△	○	◎	◎
		⑼生活相談	○	＊	○	◎
		⑽マルチメディア・コミュニケーション	○	○	◎	◎
2	社会サービスの利用	⑴行政サービスの利用	○	＊	○	◎
		⑵教育サービスの利用	○	＊	○	○
		⑶医療サービスの利用	○	＊	○	○
		⑷福祉サービスの利用	◎	＊	○	◎
3	社会活動への参画	(1) コミュニティ活動への参画	△		○	◎
		⑵政治への参加	○		△	○
		⑶情報の発信	△	＊	△	△
4	自宅のオフィス化	⑴SOHO の運営	△	△	○	○
		⑵在宅勤務	○	＊	△	○
		⑶在宅学習	○	＊	○	○
5	趣味、娯楽	⑴ホームシアター	△	＊	○	○
		⑵ホームミュージアム	△	＊	○	○
		⑶ネット新聞、ネット雑誌	△	＊	△	△
		⑷趣味への利用	○		△	△
		⑸対戦ゲーム	△	△	○	○

重要性
◎ 非常に重要、なくてはならないもの
○ 重要、家庭によっては是非欲しいもの
△ 重要性は低い、特に必要ではないが、あれば便利なもの

想定される普及の度合い
◎ (社会の仕組みの一環として)ほとんどの家庭に普及
○ 多くの家庭に普及
△ 普及は一部の家庭に止まる
＊ 登場段階、先行ユーザで使用が始まっているが本格的な普及はこれから

2.5.3　くらし分野におけるネットワークの利用

家庭におけるくらし分野の機器のインテリジェント化とネットワーク化の進展は、日常のくらしの中におけるネットワークの依存度を高くすることになる。今後、くらし分野で広くが普及するとみられるネットワークの利用場面を以下に示す。

2.5.3.1 家庭内機器間の自動コラボレーションと自律運用

家の施錠システム、照明機器、暖房機器、浴室機器、台所の家電製品、録画装置や録音装置等のインテリジェント化がさらに進み、これらがさまざまなセンサーやＰＣ等につながれるようになると、家庭内の各機器がプログラムに従い自律的に機能するだけでなく、機器間の自動連携も行われ、現在以上に進んだホームオートメーションが実現することになる。

このようなシステムには、ハッカー等の侵入や悪意はなくともネットワーク上の問題による意図しない指示等で、システムが混乱するようなことがないような予防措置が必要となる。

2.5.3.2 家庭の外からの家庭内機器の操作と動作状態のチェック

ネットワークにつながれた各種の家庭内機器に対し、外出先等の家庭の外から動作状態の監視や操作を行うものである。このような機能を上手に利用すれば、くらしをより便利にすることができるだけでなく、消し忘れのストーブやコンロの火を外出先から消すことができる例に見られるように、くらしの安全と安心を高めることができる。

家庭内機器のほとんどは外からの遠隔操作や状態の監視の対象となりうるが、その対象としては、以下があげられる。

- 照明系統
- 暖房機器等の家庭内の環境関連機器
- コンロ、炊飯器等の台所
- 風呂、洗濯機等の水周りの機器
- 各種通信機器
- 録音、録画装置
- PC 等の IT 機器
- 施錠、防犯機器
- 家庭内の監視装置
- 給餌装置等ペット関連機器

これらは、携帯電話や PC 等のモバイル機器のみならず、このような機器を持ち合わせない場合

でも、オフィスの電話や公衆電話等からでも操作が可能になることも期待される。ただし、家人または家人に頼まれた者以外によるこのような機能への介入は、大きな事故の元になるため、このようなシステムの普及に先立っては、その利用についてのルールやシステムの安全対策が一定の水準に達していることが求められる。

2.5.3.3 家庭の外からの家庭の状況のモニタリング

外出先等の家庭の外から、ＰＣや携帯電話等のモバイル情報機器を用いて、家庭に設置された監視カメラを遠隔操作し、いつどこからでも家庭の状況をリアルタイムな映像および音声で把握できるようにするものである。監視カメラの遠隔操作により、求めるところを必要に応じクローズアップして観察することもできるようになる。

このような利用のニーズとしては、以下があげられる。

(1) 外部から支援が必要な家庭のモニタリング

ほぼ常時または随時に状態のチェックが必要な高齢者だけの家庭とか、サポートする人が家庭内にいない要介護者や自宅療養患者がいる家庭における、これらの人の暮らしや健康の状態を、遠くに離れて暮らす家族や、これらの家庭の生活を支援したり、医療サービスや健康相談を行う福祉サービス機関や医療機関等から、ネットワークを介しモニタリングすることにより、わざわざ出向かなくても、随時把握できるようにするものである。支援する方にとっても、支援される方にとっても、期待される機能である。

(2) 留守宅の監視

外出先から家庭内の状態をチェックするもので、その利用場面としては、以下のようなケースがあげられる。

- 防犯的な意味からの留守宅の監視と、問題が生じている場合の必要な対応の即時の実行
- 病人等の監視が必要な者を一人で残して外出した場合等における置いた時のこれらの者の状態のチェックと、問題がある場合の必要な対応のリアルタイムでの実施
- 小さい子供を留守番に残して外出した場合における子供の状態のチェックと、指示等の必要な対応の実行
- ペットの状態のチェック

また、このチェックによりなにか問題があれば、先にあげた関連機器を遠隔操作したり、テレビ電話等で留守宅にいる者と対話をすることにより、問題をその場で解決することができる。このような利用は、くらしをより安全に安心にするものである。

図 2-14 は、家庭状況のリモートモニタリングと家庭機器のリモートコントロールを連携させたシス

テムについての提案例を示すものである。このシステムでは、携帯電話から各種ネット家電機器がコントロールでき、宅内のモニタリングや来訪者への応対ができる。

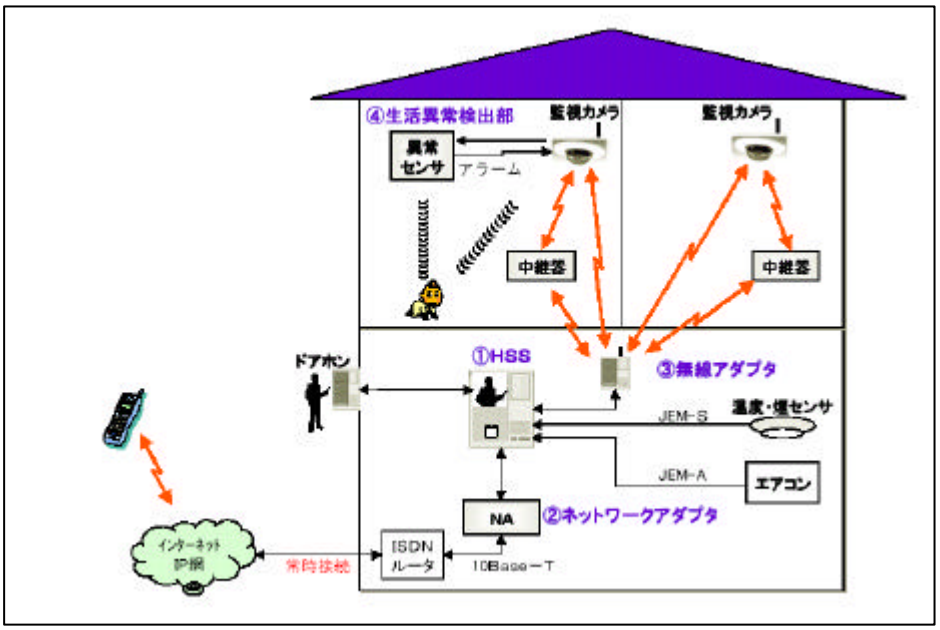


図 2-14 住宅情報盤システム構成

（IPA Technology EXPO ITX 2001 資料より）

①ホームセーフティーステーション（HSS）

監視カメラによる宅内監視機能や来訪者画像の記録（JPEG）と、センサー・家電機器（エアコン・電気錠など）の状態確認と制御を可能にするTV ドアホンの親機である。

センサーや家電機器の情報は Compact HTML で記述され、制御は CGI プログラムにより実現している。

②ネットワークアダプタ

HSS に記録されている画像や、HSS により管理されているセンサー・家電機器情報を、宅外からモニタリング、制御可能にする HTTP サーバである。ISDN を経由してインターネット網と接続されている。携帯電話に搭載されているブラウザからいつでもアクセスを可能にするため、インターネット網とは常時接続を前提としている。

③生活異常検出部

生活異常検出は、音声特徴分析、動画像情報検出、領域侵入検出、状態推論の 4つの処理部で構成され、幼児が「泣いている」または「危険な領域に侵入している」ことの認識判定を行う。判定結果は、携帯電話のブラウザ上に表示することができる。

参考） この分野での先行システム例 ： 総合警備保障の「るすメイト」

外出前に「るすメイト」をセットし、防犯センサーが侵入者を感知するとカメラで撮影、ユーザの携帯電話に直接メールで連絡が入り、外出先から画像を確認することができる。

また、留守宅内の様子が気になる場合は、外出先から「るすメイト」をコントロールして部屋を撮影し、画像を確認することもできる。ちなみに、撮影画像は契約ユーザしか見られない仕組みになっている。

このようなネットワークの利用は、プラバシーの保護との問題も絡むため、その適用にあたっては、特別な配慮が必要で、無分別な利用は避けなければならない。また、ハッカー等の悪意の第三者の介入による覗きや不正に取得した情報のネットワーク上での流布も大きな問題となる。このため、このようなネットの利用をサポートするシステムには、その利用についてのルールの確立と、許された者以外の利用を許さないようにするセキュリティ対策が十分に講じられているようにすることが求められる。

2.5.3.4 家庭やその他の場所からの家庭の延長線上といえる場のモニタリング

子供を預けている保育システムや学校、あるいは、家族が入院先の病室等における家族の状況を、家に居ながらあるいは勤務先等の外出先から、ネットワークを介してモニタリングできるようにするものである。

わざわざ出向く必要がなくなるため、他のことをしながらでも、より密度の高い観察ができるようになるため、観察の対象者とのより深いコミュニケーションや、必要に応じた支援が適切にできるようになろう。

しかし、このようなネットの利用は、プラバシーの保護との問題も絡むため、その適用にあたっては、特別な配慮が必要で、無分別な利用は避けなければならない。

参考） この分野での先行システム例 ： 映像配信システム（KDDI）

KDDIでは、ビデオカメラで撮影した映像をインターネット経由で配信するシステムを販売している。例えば、保育施設の子供の様子を家庭へ配信するなどの用途で使用することができ、映像ばかりでなく音声も聞くことができる。利用者は好みの場所にカメラを設置し、パソコンの画面上でカメラの角度や倍率を調整することが可能。

2.5.3.5 防犯、防災

近年、ピッキング等の手法による家庭への空き巣も増えてきており、家庭における防犯の重要性も高まってきている。こういった犯罪やまたは災害を防ぐための手段てとして、最近、ネットの利用がクローズアップされてきた。

(1) 防犯

家庭における防犯対策としては、自己で自衛するタイプのものと、外部からの防犯サービスを受けるタイプのものとがあるが、いずれにしても住居へ不法侵入等の犯罪を察知し、犯罪を記録し、必要な人へ犯罪発生の通知を行うと同時に犯人への威嚇を行うということが基本的な防犯対策だと考えられる。

防犯商品の中には、犯罪を察知したときに映像を記録するタイプのものがあるが、この映

像をネットワークを通じて、本人やセキュリティサービス会社へ送信することも容易となるだろう。また、本人やセキュリティサービス会社が、留守中常時住居の中を監視するようなことも可能となってくる。

参考）この分野での先行システム例

1) 防犯システム（オーデリック社）

オーデリック社では、照明器具に防犯システムを組込んだものを開発している。室内灯や玄関灯などにセンサーを組込み、侵入者を感知すると小型カメラで撮影を開始し、画像をインターネット経由で携帯電話などに配信する。なお、撮影した画像は、家庭の電気配線を通じてホームサーバへ送信し、そこからオーデリックのサーバを経由して携帯電話などに送信する仕組み。

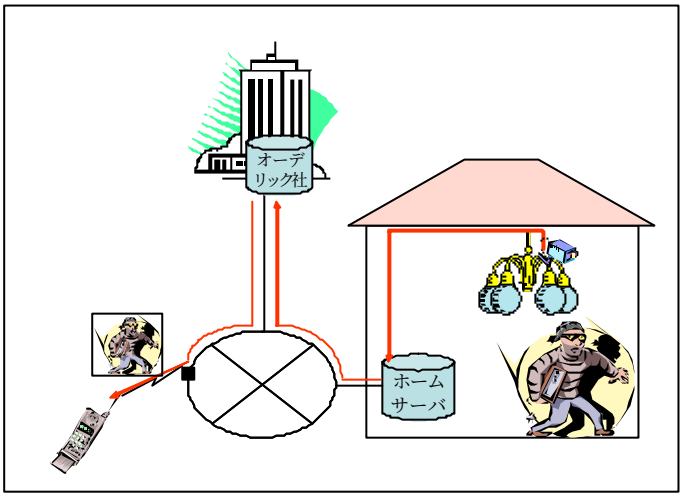


図 2-15　オーデリック社の防犯システムの仕組み

2) 自動車位置情報／異常監視サービス（ココセコム）

セコムでは、自動車の位置情報をパソコンや携帯電話へ通知するサービスを行っている。これにより、自動車が盗難された場合には自動車の位置を突き止めることができ、また緊急対処員が現場に駆けつけるサービスも用意されている。また、無理やり自動車が移動させられるなどの駐車時の自動車の異常を検知し、センターへ通報するサービスも行っている。

(2) 防災

防犯の場合と同様、火災やガス漏れが装置によって検知されることにより、それを察知し、記録し、必要な人へ発生の通知を行うことが基本的な防災対策だと考えられる。

通報先としては、本人やセキュリティサービス会社、または消防署に直接通知を行うことが考えられ、特に映像をリアルタイムで送信することができれば、より早く必要な情報を必要なところへ届けることが可能となり、被害を初期段階で食い止めることができる可能性を高めることもできよう。

2.5.3.6 ホームショッピング、ホームバンキング、各種リザーベーション

ネットを用いたショッピング、銀行取引や証券取引、チケットやホテル等のリザーベーションは、既に広く普及しているが、より豊富な情報の交換を可能にするブロードバンドネットワークの普及は、その利便性を高めるだけでなく利用の範囲も広げ、これらを一段と進化したものとし、これらの利用は従来に増して、くらしの中に定着するものとなろう。

ブロードバンドネットワークの高速大容量という特性が、ホームショッピングや、ホームバンキングや各種のリザーベーションの利用者にもたらすものとしては、以下が上げられる。

- 商品の説明力の向上による、商品についての見極めの容易化
- 売り手の実像の把握力の増加
- テレコンフェランスを用いた売り手とのフェースツーフェースライクな対話による相談や交渉の実現

これらは、買い手にとって、商品とショップについてより厳密なチェックをすることができだけでなく、対話型の交渉も可能とするため、それだけ買物や予約や取引をより満足で安心なものにしてくれる。

2.5.3.7 さまざまな情報の入手

家庭に居ながらにしてネットから入手できる情報にはさまざまなものがあり、家庭においても、すでに広く普及しているものであるが、ブロードバンドネットワークの普及は、以下の点で、このネットの利用形態をより豊かなものとする。

- 情報提供サービスの拡大による入手情報の多様化
- 映像、音声等も交えた情報のリッチコンテンツ化
- 高速化

家庭において、ネットから入手がさらに拡大すると思われる情報を、表 2-19 に示す。

表 2-19 家庭においてネットから入手の対象となる情報の例

情報区分	対象となる情報の例
報道情報	・ニュース情報 ・放映あるいは報道内容に関係する情報
各種公共サービスに関する情報	・各種公共施設の案内、施設利用の予約 ・地方自治体から住民への各種情報提供
くらしにかかわる情報	・近隣のスーパーや食料品店等の販売情報 ・駅の時刻表 ・気象情報
各種の知識情報	・病気や薬に関する知識 ・趣味や道楽に関する知識 ・語学に関する知識
娯楽用コンテンツ	・書籍、音楽、ビデオ

2.5.3.8 多様なデジタルコンテンツの入手

ブロードバンドネットワークの普及とともに、行政機関、報道機関、教育機関も含む各種団体や機関、一般企業、データベースベンダーは、こぞってさまざまな情報をネット経由で提供することになろう。このような情報の提供は、既に、広く開始されているが、ブロードバンドネットワークの普及は、コンテンツのリッチが容易になることで、新たな分野を開くことになろう。

電子商取引を始めとするネットを介したさまざまなサービスの進展により、以下のようなデジタルコンテンツは、それが販売品、非販売品にかかわらず、家庭においてもネットから入手できるようになる。ブロードバンドネットワークの普及は、ネットワークを介して流通するデジタルコンテンツの領域を、さらにリッチものへの領域へと拡大するであろう。

家庭での流通デジタルコンテンツの入手のニーズとしては、在宅勤務やSOHOの運営上での業務での使用、学習用を支援する知識に関する情報の入手、年賀状や集まりの案内上の作成やアルバムの作成等のくらしの中での使用、および趣味や娯楽のためのソフトやデータの入手があげられる。

- 音楽ソフト

  パソコンや携帯電話を使って音楽配信のポータルサイトで聞きたい曲を検索し、ほしい曲が見つかればダウンロードするサービス。

  代表的なポータルサイトとしては「レーベルゲート」(http://www.labelgate.com)がある。
- 映画・アニメ等のソフト

  サービスとしては、ストリーミング型でサービスを受けるものと、ダウンロード型でサービスを受けるものがある。ストリーミング型として普及しつつあるものに「ショートフィルム」があり、例えばパルコとフジテレビでは共同で「ショートブレイク」(http://www.shortbreak.jp)というサイトで短編映画のコンテンツを提供している。また、ソニー・ピクチャーズ・エンタテイメント等が出資するムービーリンクでは、米国内で映画の配信サービスを試験的に開始し始めている。

  また、バンダイではパソコン向けにアニメの配信サービスを手がけているが、家庭用ゲーム機経由でのアニメの配信を行うことも計画している。
- レシピだけでなく映像で示す調理手順まで含む料理ガイド
- 年賀状作成や案内文書の作成等の素材集
- 病気に関する多彩な画像や映像等によるきめの細かい自己診断用の情報
- その時点々々でのホットな観光案内や宿泊施設情報
- 地点と事項を組み合わせたピンポイントの天候情報
- さまざまなイベントの記録
- 歴史や物理現象に関する映像情報
- 困ったときの対処方法に関する情報
- 辞書・辞典
- 従来のメディアに対して情報を付加するコンテンツ

例えば、放送とインターネットを連動した番組配信を行うことで番組内の関連情報を提供するといったように、従来のメディアに文字情報等のコンテンツを付加して価値を高める方法である。

インターネット上には、既に辞典サイトはいくつも存在しており、最近では音声や画像、映像といったリッチコンテンツが充実し始めている。

2.5.3.9 生活相談

生活相談については、従来では相談窓口に直接出向いたり、電話や電子メールを用いる方法がとられていた。ブロードバンドネットワークが可能にするテレコンフェランスは、相談窓口と双方向の映像のやり取りを行うことによって、相談現地へ赴かなくても家庭から細かなニュアンスまで伝えながら相談することが可能となる。

相談分野の例としてを、表 2-20 に示す。

表 2-20 ネット利用の対象となる各種相談

区分	相談内容
法律相談	民事（金銭や借地借家に関するもの等）、人事（相続や離婚離縁、財産分与に関するもの等）ほか、商事、刑事に関する相談を弁護士と行う。
市民相談	住宅や交通機関、環境、大型ごみ、施設といった市民生活のインフラに関するものや福祉、介護、行政、教育に関する相談。
医療・健康相談	健康上の相談、治療や投薬に関する相談などを医師と行う。
交通事故相談	示談の方法，賠償問題，更生問題に関する相談を市の専門相談員と行ったり、保険に関する相談を保険会社と行う。
税務相談	税金に関する相談を税理士と行う。
消費生活相談	商品・サービスについての苦情や相談を、消費生活センターなどの消費生活相談窓口と相談を行う。
金融・保険の相談	銀行等金融機関への相談や、生命保険・火災保険への加入等に関する相談を行う。

2.5.3.10 マルチメディア・コミュニケーション

従来からあるピアツーピア型の通信であり、当面は、電話、FAX、メールといった従来のものが主流であろうが、ブロードバンドネットワークの普及と対応機器の機能の向上と低価格化による普及が進めば、ブロードバンドネットワークと高性能を活用したリアルタイムの動画像のさまざまなメディアを駆使したテレコンフェランス型が主流になってくると思われる。

2.5.4　ネットワークを介した社会サービスの利用

ブロードバンドネットワークの普及により、家庭に居ながらにして利用できるようになる社会サービスとしては、以下があげられる。

- 行政サービス
- 教育サービス
- 医療サービス
- 福祉サービス

2.5.4.1 行政サービスの利用

政府、官公庁、地方自治体、ならびに保険所等の行政機関における各種のサービスを、自宅または外出先からネット経由で利用するものである。わざわざ出かける必要もなくなるので、必要な時にはいつでも利用可能になる。

家庭生活において利用の対象になるサービスの代表的なものとしては、以下があげられる。

- 転居、結婚、出産、死亡等の市民生活に関する届出
- 住民票等の各種の証明書の取得
- パスポートや免許証の申請
- 税務関係の届け出または申請
- 介護サービス等の各種サービスへの登録

2.5.4.2 教育サービスの利用

在宅のまま、あるいは外出先から、教育サービスベンダー等が提供する教育プログラムに、ネットを介して受講や参加ができるようになるものである。

既に、英会話教室や進学予備校等でこのようなサービスが始まっているが、リアルタイムの動画像の利用や双方向性の対話を駆使したテレコンフェランスシステムが普及し、豊富な情報を駆使した一流の講師による講義を受けることが可能になれば、家庭からネット経由で利用する教育サービスは、もっと充実したものとなる。

現時点でも、家庭からネットワークを介して利用できる教育サービスの一例を、以下に示す。

- 語学スクールでの遠隔授業

  英会話教室の ECC では、インターネットを通じた英会話授業を始めており、パソコン画面に写った教材と映像により、講師と生徒が 1 対 1 で授業を行うことができる。
- 通信教育

ベネッセコーポレーションでは、中学生にインターネットを通じて数学や英語を個人指導するサービスを提供している。講師と生徒が音声と筆記用ボードを使って指導を行っているが、将来的には映像も取り入れることをも計画している。

2.5.4.3 医療サービスの利用

家庭に居ながらにして、簡単な診察や治療についての指示が受けられるもので、このような形での診療で済む場合は、患者の負担を減らすだけでなく、医療機関側の負担も減らすことが可能となるため、医療サービス全体にとっては期待されるものとなる。

このサービスには、以下のタイプが考えられる。

- 在宅簡易診察
- 在宅診療
- 緊急時の応急処置

(1) 在宅簡易診察

オンデマンドでの医療機関側との テレコンフェランスによる診察と治療の指示で、風邪等の深刻でない病気等には十分利用可能であろう。

(2) 在宅診療

継続治療の患者に対する、定期的な診察で、患者側は指示された診察データを自分で取得し、医療機関に送ることと、テレコンフェランスを用いた、患者の状況のチェックによって必要な指示を行う。病状に沿った適切なデータの収集器具がネットワーク化され患者側に置くことができるようになれば、病状によっては、在宅治療が入院と同じ効果が期待でき、これも医療機関側の効率化と患者側の負担の軽減に寄与することが期待される。

(3) 緊急時の応急処置

テレコンフェランスを用いた応急処置の指示を可能にするものである。リアルな映像等を通し、状況の把握がより適切にできること、およびリアルな映像を身ながらの応急処置の指導が可能になることは、緊急時に、慣れない者でも、救急隊が到着するまでの間の現場での適せつな応急処置を可能にする。

2.5.4.4 福祉サービスの利用

福祉サービスには、一人暮らしの高齢者に対する生活支援に関するものと、介護に関するものがある。また、その形態として、在宅福祉サービスと施設福祉サービスがある。それぞれが提供しているサービスを、表 2-21 に示す。

表 2-21 福祉サービスの分類

	高齢者生活支援サービス	介護サービス
在宅福祉サービス	配食サービス 外出支援サービス 寝具の感想消毒サービス 各種相談	家族介護の指導 介護用品の支給 緊急時の通報サービス 各種相談
施設福祉サービス	養護老人ホーム 老人福祉センター	特別養護老人ホーム 老人保健施設

(1) 在宅福祉サービス

在宅福祉サービスは、ブロードバンドネットワークの活用がもっとも活かされるサービスの一つ言えよう。

先に述べたように、在宅ケアの支援や老齢者家庭・要介護者の状態のチェックと必要な指示のオンライン化、緊急時の処置のオンライン指示、オンライン相談サービス、福祉サービスの運営管理といった利用形態に対して、ブロードバンドネットワークの特性である、距離と時間の克服により、家庭に居ながらにしてさまざまなサービスを受けることができるようになるだろう。

(2) 施設福祉サービス

老人ホームや、施設／センターに入っている高齢者や被介護者も、家族・家庭とのつながりを維持していくことは重要である。例えば、テレコンフェランスを用い、入居している自室のすぐ隣に自宅内の部屋があるような環境でリアルタイムで家族との会話を楽しむことができれば、生きがいや健康増進にもつながって行くであろう。

2.5.5　ネットワークを介した社会活動への参画

さまざまなコミュニティ活動や政治に関連する活動等が、ネットワークを介しての参加ができるようになれば、家庭に居ながらにしてあるいはオフィスに居てもこれらの活動への参加が可能になる。このことは、これらの活動に参画する人口の増加、運営の効率化、および活動の質的な向上をもたらすものと考える。

2.5.5.1 コミュニティ活動への参画

コミュニティ活動への参加者は、ネットワークを利用することにより、家庭に居ながらにして以下のような形でコミュニティ活動に参加することができるようになる。

- コミュニティの活動状況に関するさまざまな情報の入手
- 意見の提示や交換
- 関係者との対話
- イベントへのネットワーク参加
- さまざまな手続きの実行

ただし、これらの機能が享受できるようになるためには、それぞれのコミュニティは十分に洗練されたシステムを準備し、必要な機能を参加者が気安く使える形で提供をしなければならない。

すでに見られるこのようネットワークの利用としては、以下のようなものがある。

2.5.5.2 政治への参加

ネットワークの利用が年齢層に関係なく広く普及し、以下のようなネットワークの利用形態が普及すれば、一般市民も話題になっている政治問題に関し、多くの人に意見に直接触れることができるようになるだけでなく、自分の意見も発信できるようになり、政治への民意の反映を期待することができる。

一般市民への政治参加につながるネットワークの利用形態としては、以下のようなものがあげられる。

- 政府や地方自治体等の行政機関と国民、県民、市民との対話
- 政党や政治団体との国民の対話
- 国会議員や地方自治体の議員他の政治家と国民、県民、市民との対話
- 政治に関する各種調査への参加
- 政治問題に関する国民、県民、市民同士の意見の交換

この点に関するネットワークの利用は最近急速に進展し、現在でも、行政機関によるホームペー

ジやメールマガジンによる情報の提供、各種の調査やパブリックコメントの収集や、政治家のホームページによる政治家としての理念や活動状況についての報告、さらにはメール等による意見の収集、報道機関による調査等は行われている。

ブロードバンドネットワークの普及は、情報提供の密度やその内容の充実に加え、テレコンフェランを駆使するとにより、ネットワークを介した国民と行政機関や政治家との直接対話や、ミニ集会を可能にする。このような利用は、国民の政治意識の向上と、政治参加への機会を大幅に向上させるもので、我国の民主政治のレベルを向上させることに繋がる。

2.5.5.3 情報の発信

ネットを利用すれば、個人またはグループでの、特定のグループあるいは社会全体を相手とした情報の発信は便利にできるようになる。これは現在でも、多くのグループまたは個人が、インターネット上にホームページを設けており、すでに一般化したものと言える。

ブロードバンドの進展は、これらの情報発信における、情報をより豊富なものにする。

2.5.6 ネットワークを利用した自宅のオフィス化

家庭をオフィス化するものであり、その形態としては、ＳＯＨＯの運営と在宅勤務、および在宅学習があげられる。

その代表的なものをあげると、以下のようになる。

- ＳＯＨＯの運営
- 在宅勤務
- 在宅学習

2.5.6.1 ＳＯＨＯの運営

家庭に情報システムを導入し、事業体としての機能するようにしたものであり、既に一般化したものである。ブロードバンドの進展により、テレコンフェランスの活用等で、その機能はさらに向上する。これは、ＳＯＨＯの拡大を促すと考えられる。

また、SOHO 運営の利用拡大に伴い、企業と SOHO のスタイルをとる家庭との間のネットワークを利用したビジネス取引も拡大され、ビジネス分野の観点からも情報の保護について対策を行う必要があると考えられる。

2.5.6.2 在宅勤務

家庭を職場の延長として、情報機器とネットワークを介して、家庭で職場の仕事を行えるようにしたものである。メールのチェック、データの分析、報告書の作成等は、現在も行われているが、これらはオフィスでの個人個人の作業にしか過ぎない。テレコンフェランスシステムが進化し、データベースアクセスも安全に行えるようになれば、グループ作業も可能になり、職場と家庭の物理的な距離の壁は取り払われることになる。

ただし、このような利用形態の進展には、組織の情報の保護についての対策が十分にとられなければならない。

また、このような状況が進展すれば、在宅勤務は現在とは少し異なったものになり、組織における勤務管理にも影響が出てくることが想定される。

2.5.6.3 在宅学習

ネットワークを利用して自宅や外出先等の自分のいる場所を学習の場とするもので、以下のような場面が想定される。

- ネットワークを介した学習の場への参加
- 個人指導の受講
- 自習

(1) ネットワークを介した学習の場への参加

ネットワークを介した学校教育やグループ学習に参加を可能にするシステムは、以下のように授業が行われる場に出席できない者に授業への参加に機会を与える。

- 病気で登校できない者
- 登校拒否等で登校が困難の者
- 遠征等で学校を離れている生徒、学生
- 登校する時間の余裕がない高等教育機関や学習塾における社会人学生

このような場の提供には、授業の映像や音声を送るだけでなく、ネット出席者からも質問ができる双方向型にし、実質的に教室で受講しているのと同じ環境を与えなければならない。

(2) 個人指導の受講

映像、画像、音声、データを駆使したテレコンフェランスを駆使すれば、実技演習を伴わないもの指導については、指導者のところに出向かなくても、ほとんど同レベルの指導を受けることが可能となろう。また、実技指導が必要なものについても、ネットで基本的なことを教え、実地で直接的に行う指導の時間はその一部にすることも可能である。

このような利用形態は、指導を受ける者にとっては、出向く時間を省くことができることで、

指導の受講をより効率的で容易なものとする。

語学教育等はネットワークを介した指導で十分と思われる。

(3) 自習

自宅や外出先等において一人で行う研究や学習にネットワークを活用するもので、普及が想定されるネットワークの利用形態としては、以下のようなものがあげられる。

- ネットワークで提供される教材による自習

  テレビ講座のような教育プログラムをオンデマンドで活用し自習する者である。現在、NHK 等で提供されているテレビ講座はその評価は高いものの、放映時間には視聴できないとか、そのすべてについて録画やアーカイブも容易ではないところから、使われなかったり十分な効果を上げていないとも見られる。このようなプログラムが、好きな時に繰返して視聴できるようになれば、一方向であるが質の高い授業を在宅で受けることができ、自習とはいえ高いレベルの学習が可能となる。

- 学習事項に関する質疑回答サービスの利用

  学習の過程で生じた疑問等に、指導者や専門家がテレコンフェランスを用い、必要なデータや映像等の情報の提供を交えながら、対談形式で回答するようなサービスも、自習による学習を質の高いものにすることができる。このようなサービスは、各種の教育機関や学習塾等の教育ビジネスを行っている事業者や教材出版社等が提供することになろう。

- ネットワークを介しての補助教材、情報、データの利用

  自習においても、さまざまな補助教材や情報やデータを必要に応じネット入手することができれば、理解が容易となり関連の知識をより確かにすることができる。

  ただし、このよう利用が誰にでも効果的にできるためには、対象となる情報が提供可能な形で整備されることと、このような情報に対する DB の整備と、利用支援システムの整備が必要となろう。

このような利用形態の先行例を、以下に示す。

- 「ドラネット」

  主に小学生を対象とした自習用のサービスであり、学習用のコンテンツ自体は CD-ROM で提供されるが、学習結果の成績表や先生への質問、オンライン上での学習もできる。学習以外にも、子供の興味をひきつけるための工夫がなされており、例えば子供でも扱いやすいメールソフトやホームページ作成もでき、コミュニケーション広場、ゲームなどもそろえている。

  (http://www.doranet.ne.jp)

2.5.7　趣味、娯楽

映画鑑賞や囲碁等、現在は映画館や碁会所等の特定の場で提供されていた娯楽も、家に居ながらにして、あるいは旅行先のホテル等の出先からでも、ネットワークを介してそのような場に居るとの同じような感覚で楽しむことができるようになろう。

その代表的なものをあげると、以下のようになる。

- ホームシアター
- ネットワークライブラリ
- 対戦ゲーム

このような場を提供するサービスが広く普及すれば、対象となるものに関しては、地域格差間は解消され、僻地に住む者も大都市に住む者と同じような場が与えられることになる。また、子育てや介護等で家から離れられない者に加え、病状に差し支えなければ、自宅療養中の者や入院患者も、このような娯楽を楽しむことが可能となり、このようなシステムは、個人々々の生活環境を越えて、多くの人により豊かな生活を送る機会を与えるものとなろう。

2.5.7.1 ホームシアター

オンデマンドで好きな時に求める映画や映像を楽しむもので、テレビ等の映像装置の高精細大画面化により、劇場に近い迫力で映画や各種の映像を楽しむことができる。

対象となるコンテンツとしては、以下をあげることができる。

- 劇場映画
- 過去のテレビ番組
- 国会、県議会、市議会、各種の公的イベントの実況記録
- スポーツ、各種集会、セミナー等の一般の放送等にはのらない身近なイベントの実況記録

発展が期待されるこのようなシステムも、その普及にはまだ以下のような課題がある。

- さまざまなコンテンツ提供を提供するメディアサービスビジネスの成長
- 家庭用映像装置の進化
- コンテンツに関する著作権の保護にかかる問題の解決

先行事例ではないが、インターネットを通じて映画を見ることができる事例をここに示す。

- 映画コンテンツの家庭への配信

  有線ブロードネットワークスと楽天が共同設立した株式会社ショウタイムでは、ストリーミングで楽しむ映像コンテンツから、動画ベースのオンラインショッピングまで、ブロードバンドならではのコンテンツを盛りだくさん用意しており、提供するコンテンツの１つとして映画コンテンツがある。

  映画の視聴は、見たいコンテンツを検索し、パソコン上で Windows Media Player を用いて

オンデマンドで行い、料金の支払体系としては、月定額料金やコンテンツごとの課金のメニューがある。(http://www.showtime.jp)

2.5.7.2 ホームミュージアム

ブロードバンドネットワークの高速大容量性を活用すれば、美術品や博物館の展示品についても、展示されている場所に出向かなくても、鑑賞あるいは観察することが可能になろう。

単に出向かなくて済むだけでなく、高精細な画像に加え解説やたの美術館や博物館が所蔵している関連する他の作品等とのリンクがサービスされれば、現場に出向く以上に奥の深い鑑賞も可能になる。また、美術館や博物館の展示スペースの問題にかかわらずすべての所蔵品を鑑賞の対象にすることができる。

このような鑑賞の仕方は、従来の現物に触れながらの鑑賞を否定するものではなく、現物の鑑賞に先立つ予習とみれば、実物の鑑賞をより億の深いものにすることも予想される。

このようなサービスは、URL の検索を行うとたくさんのサイトが見つかるが、ブロードバンドの特性を活かしたものはまだそれほどないようである。

以下に、現在提供されている事例をいくつかあげる。

- 金沢 21 世紀美術館

  コレクションより、100 点以上の美術品の写真を Web から見ることができる。各コレクションには、解説がついている。

  本美術館は、現在建設中であり、2004 年 11 月のオープンを予定しているが、オープンに先駆けコレクションを紹介する形である。

  (http://www.art.city.kanazawa.ishikawa.jp/)

- 足立美術館

  近代日本画と、陶芸、彫刻、蒔絵、童画などのコレクション を有しており、Web 上でも見ることができる。また、各コレクションの説明および作家についての経歴についても紹介している。

  (http://www.adachi-museum.or.jp)

2.5.7.3 ネット新聞、ネット雑誌

先に述べたホームシアターは、娯楽を目的とするものであるが、これは、これまで新聞、雑誌、書籍等で読んでいたニュース等の一般情報（研究や旅行の企画等の特定の目的のための情報収集とは性格が異なる）を、欲しい時にオンデマンドで、欲しいところだけ入手しようとするものである。

対象となるコンテンツとしては、以下のようなものがあげられる。

- 各種新聞

全国紙、地方紙を含め、多くの新聞社がオンラインでニュースを提供している。また、ニュースを提供しているサイトは既存の新聞メディアだけではなく、yahoo のような検索ポータルサイトでもニュースサービスを提供している。

- 一般向け雑誌

  雑誌についても新聞と同様、既存メディアによるオンライン情報提供サービスが行われている。

- 機関紙

  学会や研究会等の各種団体が発行する機関紙については、まだ案内のレベルに留まっているものが多いようであるが、一部ではオンラインで機関紙を公開しているところも見られる。

また、社会の認知度の低いコンテンツも、これらの存在を紹介し、そのコンテンツをその一部でもネットワーク経由で見たい人に提供できれば、資金力を持たない組織も、発行している機関紙等の発刊物を広い読んでもらえるチャンスも広げることができる。また、読者も思わぬ同士や考えにめぐり合える機会に恵まれるかもしれない。

2.5.7.4 趣味への利用

多くの人が趣味として楽しむものはさまざまであるが、趣味を持つ多くの人が持つ希望は、もっと上達したい、同じ趣味を持つ人との交流を増やしたい、自分の成果を見てもらいたいというところにあると言える。

ネットワークの普及と、このような趣味を持つ層におけるネットワークの利用の拡大は、趣味を持つ者に以下のような機会を与えることになる。

- ネットワークを介した指導の享受
- 同好の者との対話あるいはコミュニティの形成
- ネットを介した作品の展示

2.5.7.5 対戦ゲーム

ネットワークを介し、ゲームの場を提供するサイトでゲームを楽しんだ入り、離れた場所にいる相手と対戦ゲーム等を楽しむものである。

高精細な動画像によるゲーム画面や対戦相手の映像も写せるブロードバンドネットワークの高速大容量の特性は臨場感を増し、対戦ゲームをリアルなものに近づけることになろう。また、ピアツーピアの接続性は、対戦相手を世界に広げることになる。また、その低価格性は時間をかけた勝負を楽しむことも可能にする。

また、ネットの特性を活かし、コストをかけずに選手権大会等を開催することも可能である。

既にこのような対戦ゲームの場を提供するサービスは登場しており、その一部を下表に示す。このような利用形態は、参加者が楽しむだけでなく、対象の娯楽の普及やレベルの向上に寄与するため、関係する団体の組織的な普及活動も加速することになろう。そして、このような娯楽の参加者層にネットの利用が広がれば、在宅のまま楽しめるこのような娯楽形態は広く普及するものと考えられる。

表 2-22 対戦ゲームサービスの代表例

ゲーム種別	サービス提供元	対象ゲーム
ロールプレイング型	ｴﾚｸﾄﾛﾆｯｸ･ｱｰﾂ･ｽｸｳｪｱ カプコン セガ	ウルティマオンライン DIABLO ファンタシースターオンライン
テーブル型 （マージャン、囲碁、将棋、花札、トランプ）	サイバーフロント 日本棋院 Jgame.com	みんなで対戦（将棋、麻雀、囲碁） 囲碁 チェス、麻雀、囲碁、将棋、トランプ、ビリヤード
アクション・シューティング型	ｴﾚｸﾄﾛﾆｯｸ･ｱｰﾂ･ｽｸｳｪｱ	ｸﾞﾛｰﾊﾞﾙｵﾍﾟﾚｰｼｮﾝｽﾞ(ｻﾊﾞｲﾊﾞﾙｱｸｼｮﾝｼｭｰﾃｨﾝｸﾞ) ﾊﾞﾄﾙﾌｨｰﾙﾄﾞ 1942(戦争ｱｸｼｮﾝｼｭｰﾃｨﾝｸﾞ)
ｽﾎﾟｰﾂｼｭﾐﾚｰｼｮﾝ型	日商岩井 ｴﾚｸﾄﾛﾆｯｸ･ｱｰﾂ･ｽｸｳｪｱ コナミ	フリーゴルフ FIFA2003 ヨーロッパサッカー 実況パワフル野球オンライン対戦版
戦略シミュレーション型	マイクロソフト カプコン	エイジ オブ ミソロジー エンパイア・アース

2.6 ネットワーク社会の進展がもたらす効果

ネットワーク化の進展が、社会に変化をもたらす効果としては、以下のような典型的事例があげられる。

- 多くの場面で、物理的な距離の解消により、必要最小限の移動ですみ作業の効率化が期待される
- 離れた人、組織間のコラボレーションのスピードアップにより意思の疎通が迅速となり、創造的作業の促進や正確な判断とが可能となる
- さまざまなシステムとそれを利用する人間とのコラボレーションの向上が図られ作業の品質向上が図れる
- 情報へのアクセスの利便性の大幅な向上が図られ、作業が迅速化できる
- 文書、各種記録、音楽ソフトや各種情報のディジタルコンテンの活用が容易となる

これまであげてきたこれからのネットワークの利用場面に見られるように、上記のようなネットワーク社会の特性を生かした社会の仕組みや個々人の生活スタイルの普及は、社会に以下のような恩恵をもたらすと考えられる。

- 社会的活動における生産性の向上
- 社会的活動における機会均等の公平性の拡大
- 個人の価値感にあった生活レベルの実現
- 多様な可能性を生みだす新たな人間関係の発展

(1) 社会的生産性の向上

社会のネットワークの高度化は、表 2-23 に示すようなところから、社会生活全体での生産性の向上に大きく寄与すると言える。

表 2-23 社会的活動における生産性向上の代表的事例

区分	ネットワークの利用事例	効率向上のポイント			
		質の向上	利便性の向上	オンライン化	コスト削減
行政機関での処理やビジネス活動	・電子商取引、電子調達の進展 ・企業間や組織をまたがる処理のオンライン化		○ ○	○ ○	○ ○
各種社会サービスの提供	・利用者一人一人へのきめ細かなサービスの提供		○	○	○
業務プロセスにおけるコラボレーションの進展	・商用ビジネスにおける企業間での開発、営業、顧客サービスの共同展開 ・教育機関同士での授業や講師の交流 医療機関同士での医療活動の協力	○ ○	○	○ ○	○ ○
情報共有の進展	・各種データバンクの構築と創造的作業への活用	○	○	○	○

(2) 社会的活動における機会均等の公平性の拡大

物理的な距離の解消やさまざまな処理にかかるコストの大幅な低下をもたらすネットワーク化の進展は、地域格差や資金力の差、身体的条件の不利、などの解消をもたらす。その結果、以下に示すように、ビジネスにおいても私生活においてもすべての組織や人に同じ機会を与える可能性が期待できる。このことは、社会的な公平性の拡大と見ることができ、その結果は新たなビジネスチャンスを生み出す結果となる。

- ビジネス分野における公平性の拡大

  電子商取引や行政機関等による電子調達の進展は、ビジネスチャンスを探る事業者にその事業拠点や資金力に関係なく、公平にビジネスのチャンスを与え、健全な社会の実現に寄与する。

- 私生活面における公平性の拡大

  家庭に居ながらにしてさまざまなサービスを受けたり、社会への接点を持つことが可能になる高度ネットワーク社会は、以下のような場面において、従来は存在した生活場所に依存する地域格差を解消することにより、すべての人は均一の社会サービスを受けることが可能となり自己実現のチャンスが高まる。このことは、特に、老人、障害者、病気の人等の社会的弱者や、僻地に住む情報弱者人にとっては大きな活力となる。

表 2-24 社会のネットワーク化がもたらす機会の均等

区分	社会的公平性の事例	機会均等の背景
各種社会サービスの享受	医療サービスの利用 教育サービスの利用	ネットワーク化の進展により、どんな僻地に居ても、都会と同じレベルのサービスを受けることが可能
社会活動への参画	政治への参画 コミュニティ活動への参加参画	家庭に居ながらにして、政治やコミュニティ活動についての情報を入手し、ネットを介したこれらの活動への参加ができるため、社会的弱者や、活動拠点から離れたところに住む者に活動への参加機会を与える
文化イベントや、文物へのアクセス	ネットシアターの利用 ネットミュージアムの利用	居住地域に関係なく家庭からでも、リアルと遜色のないレベルでのネットを介した演劇の鑑賞や、美術館や博物館の展示の鑑賞が可能

(3) 個人の価値感にあった生活レベルの実現

社会の個々人にあった価値感の実現を容易にするネットワーク化が与えるものとしては、以下があげられる。

表 2-25 個人生活での価値観の多様性実現

区分	個人生活の価値観の多様性
生活様式の多様化の実現	･在宅勤務などのワークスタイルの多様性 ･生活様式の多様化を満たす行政サービスへの利用アクセスの時間的、距離的克服 ･個客主導の電子商取引の利用 ･各種ネットワークサービスの選択肢の増加 ･各種コンテンツの選択肢の増加 ・コミュニティ活動での知恵の活用
安心安全の向上	･健康生活を目指す高度の医療サービスの利用 ･元気な高齢社会を目指す福祉サービスの利用 ･リアルタイムでの家族の状況の把握 ･家庭の防犯への利用 ･各種相談サービスの利用
社会的自立の可能性向上	･政治､行政への自主的行動参画 ・コミュニティ活動への主導的参画
生活の豊かさの向上	･豊かな教育サービスの利用 ･ネットワークライブラリの利用 ･ネットシアターの利用 ･ネットミュージアムの利用 ･オンラインゲームの利用

(4) 多様な可能性を生みだす新たな人間関係の発展

社会の広い層でのネット利用の拡大は、人にさまざまな価値観を持った多様な関係での出会いを与え、多くのコミュニティが生まれることになろう。自然発生的に生じたこれらのコミュニティは、きちんと組織化されたものでなかろうと、参加する人に新たな活力を与えるとともに、これらのコミュニティが豊かな社会の創出に寄与することになろう。

2.7 高度ネットワーク社会の実現に向けた課題

ここまで整理してきたように、ブロードバンド社会の実現に向けては、第一にはまずブロードバンドネットワークが利用可能になること、つまりネットワークインフラの構築、成熟、それに対応するITの高度化が必要であり、第二にブロードバンドの活用が社会に深く浸透していくことが重要となる。

前者の課題を整理すると、以下のようなものがあげられる。

- ネットワークコスト、価格そのものの低廉化
- 大容量高速ネットワーク基盤の整備
- デバイス間通信や、現実により近づいた形で環境を共有するためのIT そのものの高度化
- 低廉なコストでネットワーク接続が可能となるセンサー/通信デバイス
- 大規模なネットワーク空間を複雑な目的に対応して管理する技術
- セキュリティ等社会の要請に対応する技術

一方、後者の例としては以下のようなものがあげられる。

- 競争優位を実現するビジネス環境の実現技術
- 多様な利用者の受入れ容易な、ユーザフレンドリーな環境の整備
- ネットワーク利用を前提とした社会システムのあり方の認識と法的整備
- ネットワーク上で安全と信頼を提供する仕組みの整備

3 ネットワーク社会における“安全と信頼”に対する脅威と必要な対応

発展したネットワーク社会にあっては、ネットワークは社会の仕組みや個人の生活に深くかかわっており、いわばエネルギーや水や交通手段と同じようなライフラインの一つと考えなければならない。このような社会環境においては、ネットワークサービスを提供しているサイトや個人の家庭のシステムに対する不正なアクセス、ウイルス、DoS 等の攻撃は、従来にはない深刻な影響を個人や社会に与えることになる。

ネットワーク社会がそれほど進展していない現在においても、ネット接続システムにおける不正アクセスやウイルスの脅威は、世界的にも猛威を振るっている。多くの官公庁や企業のホームページの改ざん事件や、SirCam、Badtrans.B、CodeRed、Nimda などのウイルスによる被害は記憶に新しいところである。

第 2 章で述べてきたような進化したネットワーク社会が、広く受入れられるようになるためには、その安全と信頼が確保されていなければならない。ネット経由の処理は、その過程や結末を自分の目で直接確かめることができないため、利用者にとっては、ネットの先の処理の相手や情報は信頼できるのか、処理は自分の意図した通りに完結したか、第三者により勝手に使われていないか、情報は保護されているかと言ったような懸念が残るのは当然であろう。また、ネット経由でのサービスを提供する事業者にとっても、悪意の者の攻撃によるサービス提供の妨害や情報の漏洩等についての脅威も無視できない。ネットワーク社会が“安心と信頼”できるものであるためには、このような懸念に対して心配することなくネットの利用にかかわるサービスの利用や提供ができる環境が実現していなければならない。

3.1 ネットワーク社会の“安全と信頼”に対する脅威

ネットワーク社会における、ネット経由でのサービスの利用や、ネットを利用するシステムの使用における安心と信頼を損なう要因としては、以下があげられる。

- サービスまたはシステムの機能の欠陥
- サービス提供またはシステムの稼動の混乱
- システム利用上の不手際
- 悪徳な事業者の存在
- 悪徳な利用者の存在
- システムに対する攻撃者の存在

(1) サービスまたはシステムの機能の欠陥

ネットを介して提供されるサービスやネットを利用するシステムに機能上の欠陥があれば、システムは利用者の意図とは異なる動きをする。その影響は、サービスやシステムにより異な

るが、行政やビジネスに深刻な影響を与えたり、システムによっては、人命や個人の財産を損ねたりすることにもなる。

サービスやシステムの機能に欠陥が残る背景としては、以下があげられる。

- 提供するサービスまたはシステムの機能の不適切な設定
- 設定した機能のシステムの実装への反映上の不備
- システムのメンテナンスの不備
- システムの運用上の不備

(2) サービスの提供またはシステムの稼動の混乱

システムにはつきものの構成機器の故障等により、ネット経由のサービスやネット利用システムを利用したいあるいは利用すべき時（もともとのサービス時間帯以外の時間を除く）に、これらが利用できなくなったり、利用できる機能が大幅に制限されたりすることも少なくない。社会の仕組みや生活の場において、そのようなサービスやシステムの存在が不可欠である場合、その影響は一時的なものにせよ、社会や個人の生活に深刻な影響を及ぼすことになる。重要なシステムにおいては、このようなことは許されるものではない。

サービスの提供やシステムの稼動に混乱をもたらすものとしては、以下があげられる。

- システムの可用性確保にかかる設計の不備
- 可用性確保のための諸施策のシステムの実装への反映の不備
- システムのメンテナンスの不備
- システムの運用上の不手際
- ハードウェアやソフトウェアやネットワーク等のシステム構成要素の欠陥または故障
- システム関連設備や施設の不備または故障
- システムを構成する機器や設備や施設に影響する災害
- 内部の者による破壊あるいは妨害行為
- 外部の者によるシステムに対する攻撃

(3) システム利用上の不手際

サービスやシステムの利用者のサービスやシステムの利用にあたっての不手際も、脅威の一つに数えられる。利用上の不手際が、サービスやシステムの利用のトラブルに繋がる要因としては、以下があげられる。

- 利用者の不注意またはスキルの不足
- サービスやシステムの提供者からの利用者へのガイドの不足
- システムの作りにおける利用者の不手際への配慮の不足

(4) 悪徳事業者の存在

ネットを介した処理では、ネットの先の相手（場合によってはシステム）が直接確認できないことを悪用して、そのサービスの提供において、最初から不当なサービスまたは商品を押し付けたり、詐欺等を企んだりする事業者も存在する。

(5) 悪徳な利用者の存在

一方、サービスの利用者側にも、他人をかたってサービスを利用したりする者も存在する。他人をかたってのサービスの利用は、サービスの提供者だけでなく、なりすましの対象となった者もトラブルに巻き込む。

(6) システムに対する攻撃者の存在

サービスを提供するシステムやネットにつながれたシステムに侵入したり、通信路上のデータを盗聴したりするハッカー等の攻撃者の存在も、ネットワーク社会において無視できない脅威である。

このような攻撃者としては、悪意を持つシステムの利用者や悪意の第三者に加え、サービスの提供者側の関係者も考慮に入れなければならない。

システムへの攻撃による被害としては、以下のようなものがある。

- システムの不正な使用によるシステムの勝手な操作や破壊
- 資格のない者によるサービスの不正な使用によるサービス提供者の権利（料金の徴収等）の侵害
- 情報の不正取得とその悪用
- 情報の改ざん等による情報の操作やシステムの処理のかく乱、妨害
- システムの改ざんや破壊等によるサービスの提供やシステムの妨害

以上のネットワーク社会における脅威と、これらの脅威が現実になった時の想定されるトラブルの関連を、図 3-1 に示す。

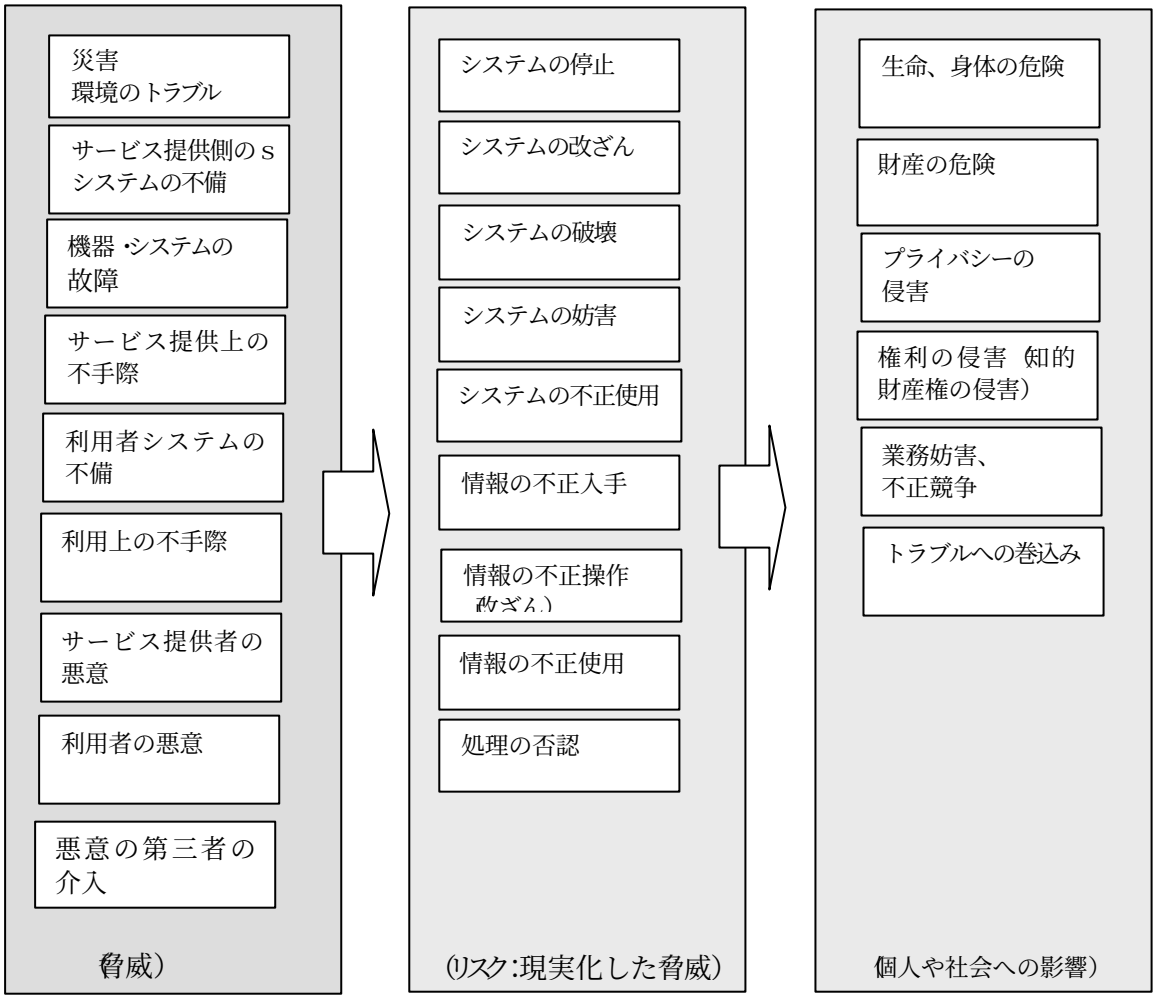


図 3-1 ネットワーク社会における脅威

3.2 ネットワーク社会における“安全と信頼”とは

ネットワーク社会を構成するさまざまなネット経由で提供されるサービスやネット接続システムに信頼がおけ安心して使えるようにするためには、これらの利用に際して、トラブルについて心配しなくてよいという環境の確立が必要となる。

このためには、それぞれのシステムが信頼できるものとしてできていることと、万一、トラブルの発生が発生しても、不便や被害は許容されるレベル以下であること、ならびに生じた紛争について納得行く解決が保証され、不当な行為から保護されていることが保証されていなければならない。

ネットワーク社会における“安心と信頼”とは、このような状態が確保された環境を言い、以下の要件が成立していなければならない。

- 自分が行ったネットを介した処理は信頼できる
- 不注意な操作が、被害に直結するようなトラブルに結びつかない

- 情報は保護されている
- サービスの提供や利用システムは必要なときには何時でも利用できる
- トラブルに起因する紛争が生じても解決の道が開かれている
- 不正行為、迷惑行為は牽制されている

以下のそれぞれの要件を詳述する。

(1) 自分が行った処理に対する信頼性

ネット経由でのサービスの提供や、その利用、電子商取引、家庭内機器のリモートコントロール等の処理が、自分の意図した通りに完結することをいう。ネット経由でのサービスの利用や処理の実行が、利用者の意図通りに完結するようにするためには、表 3-1 に示すようなことが成立していなければならない。

表 3-1 ネット経由の処理が信頼できるものにするための要件

要件	阻害要因
1 接続先は意図したあるいは意識した相手であること	・なりすましによるサービスの不正な利用あるいはシステムの不正な使用 ・接続先のすり替えによるサービス提供元や接続システムのすり替え
2 相手は悪意の者でないこと	・サービス提供者の悪意 ・利用者の悪意
3 処理に用いられた情報あるいは提供された情報は正しいものであること	・システムの誤処理 ・外部からのシステムへの侵入や内部の者の犯行による等による情報の改ざん ・ネットワーク上で情報の改ざん
4 処理は仕様通りに完了していること	・システムの仕様の欠陥 ・システムの誤処理 ・外部からのシステムへの侵入や、内部の者の犯行によるソフトウェアやシステム上の情報の改ざん等のシステムの改ざん

(2) 操作ミス等利用上の不手際に対する配慮

ネットワーク社会においては、年齢や職業やキャリァに関係なく、IT への慣れ不慣れに関係なくのすべての者が、ネットワークサービスやネットワーク経由での処理を利用することになる。この結果、システムの操作性や操作マニュアル等に十分な配慮が欠けていると、操作にミスが入り込み易い。操作ミスが、不正な処理やシステムの混乱に直結するようでは、システムは安全なものとは言えない。

表 3-2 に、操作ミスに対し求められる配慮を示す。

表 3-2 操作ミスに対し求められる配慮

要件	阻害要因
1 操作ミスが生じにくく、操作ミスがシステムの誤処理に直結しないサービスあるいはシステムの実現	・システムの操作性設計の欠陥 ・システム設計上での誤操作に対する配慮の欠如
2 サービスやシステムの使用についての適切な指導の実施	・使用マニュアルの不備 ・必要な場合におけるサービスやシステムの使用についての教育、訓練の不足
3 サービスやシステムの利用者の適切な利用	・サービスの利用者あるいはシステムの使用者の不注意 ・利用者あるいは使用者の当該サービスやシステムについての無知 ・利用者あるいは使用者に求められるスキルの不足

(3) 情報の保護

ネットワーク社会においては、さまざまな社会活動や個人の生活が、ネットを介した処理によることになるため、さまざまな情報がネット上を飛び交い、ネット経由の処理をサービスしたり仲介する事業者の多くにさまざまな情報が蓄積されることになる。これらの情報が、関係者以外に渡るようなことがあってはならない。特にプライバシーにかかわる情報や、ネットワーク社会における自社あるいは自己の認証にかかる情報等の漏洩や改ざんは, 大きな問題を誘起する。

ネットワーク社会における情報の保護が確立するためには、表 3-3 に示す要件が成立していなければならない。

(4) サービスやシステムの安定稼動の確保

ネットワーク社会においては、さまざまな社会活動や個人の生活が、ネットを介した処理によることになるため、サービスまたは使用するシステムの中断や混乱も、また、社会や個人の生活に大きな影響を与え得る。このため、サービスやシステムの性格によっては、瞬時たりともこのようなことが許されなし、そでない場合も、許容時間内に復旧することが要求される。

ネットワーク社会を支えるサービスやシステムの安定した稼動が確保されるためには、表 3-4 に示すようなことが求められる。

表 3-3 情報の保護に求められる配慮

要件	阻害要因
1 情報を取扱う者における情報保護の実践	・情報の保護に関する認識の欠如 ・実務における情報の保護に関するガイドのや指導の不足 ・ずさんな業務とその管理
2 システム上の情報の保護の徹底	・システムのセキュリティの不備 ーセキュリティポリシーの不在または欠陥 ーセキュリティ面でのシステムの欠陥 ーセキュリティ面でのシステム運用の欠陥 ・攻撃者の存在 ー外部の攻撃者 ー内部の者による犯行
3 通信路上の情報の保護の徹底	・通信路の脆弱性 ・システムのセキュリティの不備 ーセキュリティポリシーの不在または欠陥 ーセキュリティ面でのシステムの欠陥 ーセキュリティ面でのシステム運用の欠陥 ・攻撃者の存在 ー外部の攻撃者 ー内部の者による犯行

表 3-4 サービス提供の安定性に求められる要件

要件	阻害要因
1 システムの構成要素の故障への配慮	・システムの構成要素の故障 ・システムの構成要素の故障に対する配慮の欠如または不備
2 環境変化に対する適切な対応	・急激な環境の変化 ・環境変化への対応の遅れまたは不備
3 運用の不手際に対する対応	・システム運用上の不手際 ・システムにおける、システムの運用上の不手際に対する配慮の欠如または不備
4 システムの攻撃に対する配慮	・システムの攻撃者に対する配慮の不足 ーシステムのセキュリティの不備 ・攻撃者の存在

(5) 生じた紛争に対する納得の行く解決の実現

脅威に対し考えられる対策を尽くしたとしても、トラブルの発生を皆無にすることは期待できず、サービスやシステムの利用やネット処理におけるトラブルに起因して紛争も生じるうる。サービスやシステムが安心して使えるためには、生じた紛争に対し、利用者もサービスやシステムを提供した事業者もお互いに納得行く解決の道が確立していなければならない。

ネットワーク社会の進展は、行政サービスやビジネスや個人の生活のスタイルまで変更さ

せ、その結果、社会の仕組みも現在とは相当異なったものになると想定される。この結果、紛争が発生した原因等の背景や、被害の形態や、紛争の原因となったシステムに発生したトラブルに対する責任の所在の特定や責任分担等に、従来にはない形態が多くなり、現在の紛争解決の枠組みでは対処できなくなる可能性が高い。

ネットワーク社会を安心で信頼できるものにするための、重要な要素の一つである紛争の解決が円滑に行われるようにするためには、表 3-5 に示すようなことが必要となる。

表 3-5 紛争処理の円滑化のために求められる事項

紛争処理の円滑化実現のため要件	阻害要因
1 生じた問題に対する責任者の明確化	・複雑な系におけるプロセスの追跡と問題の原因追求うえの技術上の困難性 ・問題が生じた時の関係者の連携の困難性
2 責任分担（補償責任）についてのルールの確立	・複雑な系における責任分担についての基本ルールの不在 ・対応する法律の不備
3 紛争解決の支援サービスの確立	・紛争解決にかかるルールの不在 ・紛争解決機関の不備 －体制の不備 －新しい問題への不慣れ

(6) 不正行為、迷惑行為の牽制

ネットワーク社会にあっては、ネット上の行為の匿名性や追跡の困難性等のインターネットを基盤としたシステムの仕組みの弱点をついたさまざまな攻撃や迷惑行為が横行し易い。システムがこれらの行為への対抗策を講じるにしても、不正行為や迷惑行為を試みる者に対する牽制がなければ、いわば無法状態におかれていると見なければならない。

不正行為や迷惑行為の牽制を実現するためには、表 3-6 に示すようなことが必要となる。

表 3-6 不正行為や迷惑行為の牽制のために必要な事項

不正行為、迷惑行為の牽制実現の要件	阻害要因
1 不正行為、迷惑行為に対するネットワークサービスの拒否	・不正行為、迷惑行為の特定についての技術上の困難性
2 行為者の特定の実現	・ネットワーク上の処理に対するプロセスの追跡における技術上の困難性 ・行為者の追及に必要な情報の確保についての制約 ・ネットワークサービスプロバイダー等の関係者の協力の確保の困難性 ・行為者の追求体制の整備不足
3 取締りや罰則規定の確立	・新しい手口の間断ない登場 ・誰でも行為者になれる技術環境 ・罪の意識の不足

3.3　ネットワーク社会の進展に伴う新たな問題認識

3.2 節に述べたような問題は、インターネットシステムについて既に語られているがほとんどである。しかし、ブロードバンドネットワークの普及に伴い、ネットの利用に次々と新しいものが登場するとともに、ネット経由でのサービスの提供形態や、ネットを利用するシステムの形態も従来と異なったものになることが想定される。しこもこれらが、行政機関や企業等の個々の組織内に止まらず、社会のインフラとして社会の仕組み国民の多くの生活に密着したものなり、社会も個人もネットワークサービスやネットワークを介した処理への依存度が高くなれば、問題が生じた場合の影響は、従来とは比べものにならないものとなることは容易に想定される。

発展したネットワーク社会における安全と信頼を脅かす新たな環境として考慮に入れなければならないこととしては、以下があげられる。

- 機器やシステムのトラブルの影響の飛躍的な拡大
- 不注意が思わぬトラブルに発展する可能性の拡大
- サービスの提供形態やシステムの形態の複雑化によるトラブルへの対応の複雑化
- 情報保護の困難さの拡大
- 不正行為、迷惑行為の拡大

このようなことが大きな問題となるのは、第 2 章に述べたように、ネットワーク社会の進展は、在宅勤務に見られるように職場と家庭のボーダレス化、在宅診断、在宅診療に見られるような医療機関と家庭のボーダレス化、行政サービスのネットワーク化に見られるような行政機関と家庭のボーダレス化、サプライチェーンの進化による企業間のボーダレス化等、“社会活動の場 “の変質によりところが大きい。

以下に、それぞれの問題について解説する。

(1) 機器やシステムのトラブルの影響の飛躍的拡大

高度に発展したネットワーク社会では、一つのシステムのサービスの対象が、社会全体に広がる。そして、社会活動やビジネスあるいは個人の生活の多くの分野がネットワークを介した電子的な処理に依存し、いわば水や電器やガスといったエネルギーや水と同様に社会のライフライン化するため、一旦、システムにトラブルが生じると、システムのカバー範囲が個々の組織内に限定されていた時代に比べ、その影響は広範なものになるだけでなく、場合によってはその影響は深刻なものとなる。

このため、システムによっては、装置の故障や運用上の不手際によるシステムやネットワークのトラブルだけでなく、関連設備や施設のトラブルや災害等に対しても、サービスの提供への影響は、当該システムの特性からくる許容範囲内でなければならない。また、外部からの攻撃に対する十分な対策も必要となる。

(2) 不注意が思わぬトラブルに発展する可能性の拡大

ネットを介した処理は、その過程や結末を利用者が直接確認することが一般に困難であるため、誤指示等により、利用者が意図したものとはまったく異なる結果が生じることも起こりうる。

したがって、システムに対する誤指示が、社会を混乱させたり、人命に影響を与えたり、個人の財産に大きな損害を与えたりしかねないシステムにおいては、利用者の誤操作がこのような問題にむすびつかないような配慮がなされていることが要求される。

(3) サービスの提供形態の複雑化によるトラブルへの対応の複雑化

さらに考慮しなければならないことは、ネットを介したサービスは、利用者から見たら一つのシステムによりサポートしているように見えても、実際は、複数のシステムのコラボレーションにより提供されていることも少なくない。このため、ネットを介したサービスの提供にあたっては、関与者の間でのサービスの低級や利用においてトラブルが発生した場合、その責任の所在や責任分担について、事前に適切な準備がなければ、このサービスの提供に何らかのトラブルが生じた場合、トラブルの解消、生じた問題の復旧、さらには被害の補償等が円滑に行かなくなる恐れが生じる。

ネットワーク社会の安全と信頼の確保には、この点についての対応も重要となる。

(4) 情報保護の困難さの拡大

ネットワーク社会にあっては、離れた場所にいる者同士のリモートラボレーション、別な場所にある情報にアクセスしながらの業務の遂行、在宅勤務、デジタルコンテンツのネット経由の配布等は、普段に行われる。このため、情報の取扱いに関しては、現在に比べ、以下のような変化が生じる。

- 処理対象の情報のさらなる多様化
- ネットワーク上でのより多くの情報の流通
- 従来はオフィス内で厳重に保護された領域に置かれていた情報が、利用者側PCやシステムにもコピーされるようになることによる情報保管場所の拡散

これらの情報の中には、当然ながら取扱いに慎重を要するものも含まれることになる。

家庭や出先において、オフィスとような厳格な情報の保護の実践は期待することは困難であるところから、情報の保護にはこれまでとは異なる特別な努力が必要となる。

(5) 不正行為、迷惑行為の拡大

ネットワーク社会の進展は、以下のような理由から、クラッカー等によるシステムへの侵入によるシステムのかく乱や、SPAM ネール等のネットワークを用いた無差別な迷惑行為等の、不正行為や迷惑行為が拡大につながると見なければならない。

- 攻撃対象サービスあるいはシステムの拡大による不法行為や迷惑行為の場の拡大
- 攻撃者にとっての攻撃の容易化
  - －攻撃対象のソフトウェアの増加
  - －高いセキュリティレベルの確保が期待できない一般家庭が無数にネットワークに常時つながれるようになるため、攻撃者には攻撃の糸口の捕捉の容易化
  - －攻撃に必要なコストの低下

さらに、考慮しなければならないことは、一つの不正行為や、迷惑行為が多くの被害者をだすことであろう。

3.4　ネットワーク社会の安心と信頼の確保に向けて解決が求められる課題

前節までの考察により、ネットワーク社会における安心と信頼の確立のためには、以下について十分といえるような環境が整備されなければならない。

- ネット経由で提供されるサービスやネットを用いるシステムの安定稼動の実現
- これらのサービスやシステムの利用における安全性の確保
- これらのサービスやシステムの利用や提供うえでトラブルが生じた場合の責任の明確化
- プライバシーおよび個人情報の保護の確立
- 情報の保護の確立
- 電子文書の法的有効性の確立
- 不正行為、迷惑行為の牽制の確立
- ネットの利用やネットを介したサービスの提供での被害者救済の確立

3.4.1　ネットの利用をサポートするシステムの安定稼動の実現

ネットワーク社会にあっては、ネット経由して提供されるサービス他の社会活動や個人の生活を支えるシステムは、それぞれが提供している機能の特性に応じて必要な可用性が確保されなければならない。システムに求められる可用性とは、当該システムが約束している稼働時間内では、何時でも使用可能であり、かつ適切な応答特性が与えられることをいう。

システムが必要な可用性を確保するための要件としては、以下があげられる。

- システムの目的や提供する機能に応じた可用性の適切な設定と利用者への明示
- システムの可用性を阻害する要因の排除できる仕組みのシステムへの組み込み
- 適切な性能設計とシステムの性能管理の徹底
- 障害時の備えの確立

(1) システムの目的や提供する機能に応じた可用性の適切な設定と利用者への明示

ネット社会を支えるようなシステムにおいては、サービスやシステムの提供にあたっては、その可用性に関し以下のような事項を適切に設定し、それを利用者に示さなければならない。

- 稼動日および稼動時間帯
- 稼動時間帯に生じた障害（機能停止等）に対する目標とする回復までの時間
- 想定するシステムの機能停止等につながる障害の発生の頻度

これらは、当該システムの提供する機能の特性に応じて適切に決められたものでなければならない。

(2) システムの可用性を阻害する要因の排除できる仕組みのシステムへの組み込み

システムの可用性を確保するためには、システムの安定稼動を阻害する要因を封じ込めたり、機器を二重化する等して機器の故障等がシステムの機能の提供に影響を与えないように

する仕組みをシステムに組み込むことが必要となる。そのような仕組みのシステムへの組み込みの程度は、当該システムが設定した可用性による。

配慮すべきシステムの安定稼動の阻害要因としては、以下があげられる。

- 施設および設備 構成機器他）の故障やその他の要因による停止あるいは誤動作
- システムの品質管理の不備によるシステムの設計不良やソフトウェアのバグ
- システムの維持管理や運用の不手際
- システムの性能管理の不手際
- 利用者の誤操作
- 外部からの攻撃等によるシステムの運用妨害

(3) 適切な性能設計とシステムの容量管理の徹底

システムの性能設計の不備や、負荷の予測やシステムの負荷状況の把握等の容量管理の不手際も、システムを停止させたり、応答特性が利用に耐えない状態にする要因となる。

(4) 障害発生時の備えの確立

さまざまな障害の回避策を講じても、システムに障害の発生を皆無にすることは期待できない。このため、システムによっては障害の発生が利用者の被害にもたらさないようにするための手段を講じておくことが求められる。

このめに、一般に検討されるべき事項としては、以下があげられる。

- システムの運用上で想定されるさまざまな障害が、利用する者に被害を及ぼさないようなする仕組みのシステムへの組込み
- 非常時における代替手段の準備
- 非常時における利用者の処置についてのガイドの徹底

3.4.2 ネットを介したサービスやシステムの利用における安全性の確保

ネットを経由して提供されるサービス等やネットを用いたさまざまな社会活動や個人の生活を支えるシステムは、その利用にあたって、利用者がトラブルに巻き込まれたり、被害を被ったりしないことがある程度、担保されていなければならない。

このため、このようなシステムには、システムやその利用に問題が生じても利用者に被害が及ばないよう、以下のような利用の安全に脅威と要因に対し適切な対策を組み込んでおかなければならない。

- システムの誤動作や機器の故障等によるシステムの停止や機能障害
- 誤操作や利用者システムの設定不良等の利用者の不適切な使用
- 他人によるシステムの不正な利用
- 攻撃者による正常な機能提供の妨害

このことを実現するためには、以下が要求される。

- 利用に危険が伴いうるシステムにおける安全性の追求をガイドする安全性評価モデル、システムの安全対策実施基準の確立、システム種別ごとの安全対策プロフィルの確立、システムの安全性の評価認証サービスの導入等の環境整備の推進 詳細については、5.1 節参照）
- システムの利用の安全を追求するシステムの開発
- 利用に危険が伴うようなサービスやシステムにおける、利用者に対する利用上の危険の明示と利用上の注意の徹底

3.4.3 問題が生じた場合の責任の明確化

ネットワーク社会においては、さまざまなネットワークサービスやネット利用してシステムは、単一のシステムでなく複数のシステムのコラボレーションによって機能する複合システムの上に構築されているものが一般となろう。この様子を、図 3-2 に示す。また、表 3-7 は、このような形態で運転されているシステムにおいて考えられるトラブルの原因を、その責任が帰属すべき関係者のマップを示したものである。

サービスやシステムが、このように複数事業者の事業にわたって構築されている場合、サービスやシステムに問題が生じた場合、その原因の追求が困難となったり、責任の所在があいまいであったりして、被害者に対する補償の責任者があいまいなることも考えられる。

ネットワーク社会が安心で信頼できるものになるためには、このような環境にあっても、問題の発生についての責任の所在や責任の分担が特定され、被害者に対する救済のルールが確立していなければならない。

このためには、以下の課題についての解決が求められる。

- ネットワークサービスやシステムに生じたトラブルについての責任分界についての基本ルールの確立
- 責任の所在個所を特定できる仕組みの確立

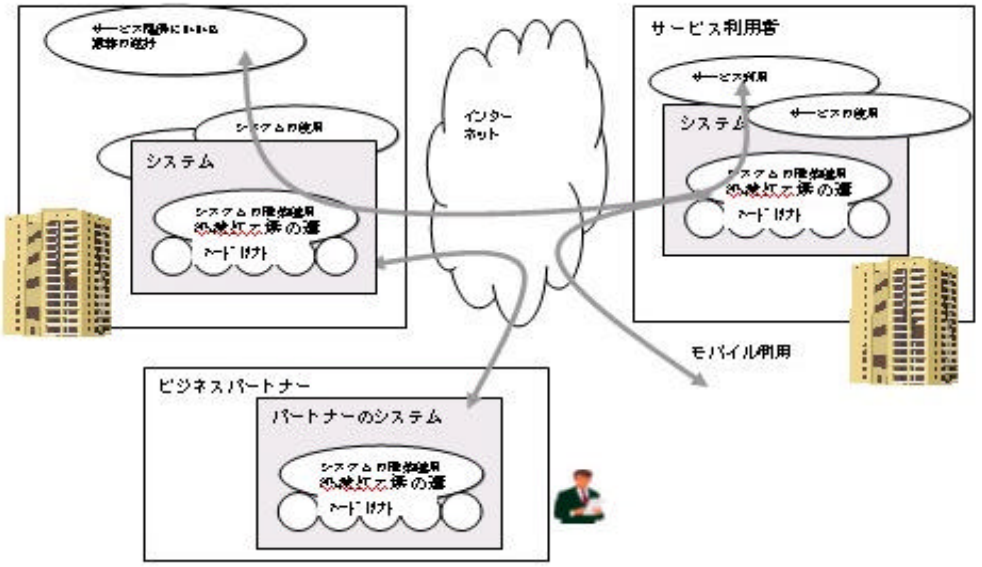


図 3-2 複数の事業者のシステムのコラボレーションのイメージ

3.4.4 プライバシーおよび個人情報の保護の確立

ネットの利用が家庭にまで広がった場合、家庭内の状況を離れた場所からモニタリングするシステムへの他人の介入による覗き見や、システムへの侵入他の手段により不正に得た個人情報のネットでの流布も考えられる。

ネットの利用が、プライバシーの保護や個人情報保護に影響を及ぼさないようにするためには、個人が安心できるレベルにするためには、以下のような課題についての解決が求められる。

- プライバシーにかかわるシステムへの第三者の介入の抑止
- 個人情報への不正なアクセスの抑止
- ネット上での個人情報の流布の抑止、牽制

表 3-7 複数の事業者によって提供されるサービスにおけるトラブルの要因

区分	関係者	事故の原因
サービス提供側	サービス提供者	業務上の不手際 システムの使用上のミス システムの不備の見逃し システムの整備、管理の不良 システム運用についての管理の不備 利用者への配慮の不足
	システム運用受託者	システム運用上の不手際
	システム構築受託者	システム構築上の不手際
	ハードソフトベンダー	通常の使用にかかわる欠陥 攻撃者に対する脆弱性 使用法についての不備
ビジネスパートナー		サービスの不備
ネットワークプロバイダー		サービスの不備
サービス利用側	利用者	サービスの不適切な使用 システム使用上のミス
	システムの提供者	通常の使用にかかわる欠陥 攻撃者に対する脆弱性 システムの使用についての指示の不備
	システム据付業者	システム据付上の不備 メンテナンスサービスの不備
	ハードソフトベンダー	通常の使用にかかわる欠陥 攻撃者に対する脆弱性 使用法についての不備

3.4.5　情報の取り扱いや情報システムでの情報の保護の確立

ネットワーク社会においては、保護されるべき情報がネット上を飛び回るだけでなく、多くのサイトや端末に分散されるため、ネットを利用したサービスの提供やネットを用いるシステムの提供や、それらの使用においては、情報の保護についての十分な配慮が求められる。

そして、これらの課題の解決のためには、以下のような施策の推進が求められる。

- 個人情報や商業秘密情報の保護に関するルールの整備
- 在宅勤務やモバイルオフィス等によりネットワーク上で拡散する情報の保護する技術の確立
- システム上の情報に対するきめ細かい保護を実現する技術の確立
- 企業等組織における個人情報や商業秘密情報の保護の徹底の推進

3.4.6　電子文書の長期にわたる有効性の維持の実現

ネットワーク社会においては、さまざまな書類は電子化され、その文書を用いる処理はネットワを介して行われるのが一般となる。しかし、電子文書は改ざんが容易であるため、電子文書が印刷物やマイクロフィルム上の文書等と同様の、真正性の検証や長期間にわたるその有効性が保証されなければ、電子文書は文書の作成、回覧、配布には便利なものではあるが、保管には適さず、業務の電子化は限られたものとなる。

ネットワーク社会を裏で支える電子文書の技術的ならびに法的効力が長期にわたって維持されるようにするためには、以下のような課題についての解決が求められる。

- 電子文書の長期見読性の確保
- 電子文書の長期間にわたる（法的）有効性の確保

そして、これらの課題の解決のためには、以下のような施策の推進が求められる。

- 電子文書の有効性についてのルールの確立
- 各種ソフトで作成された電子文書の長期見読性の確保方式および対応技術の確立
- 長期間にわたる電子文書の（法的）有効性を確保するための方式および対応技術の確立

3.4.7　不正行為、迷惑行為の牽制の確立

ネットワーク社会においては、不正行為や迷惑行為はその影響範囲が広範にわたるとともに、ケースによっては深刻な影響をもたらすことが考えられる。一方、不正行為や迷惑行為を行う者は、行為者の特定が困難なことと、不正行為や迷惑行為についての罪悪感が少ないこともあって、今

後もさらに拡大することが想定される。

このためには、以下のような課題についての解決が求められる。

- ネット上での不正行為、迷惑行為を試みる者に対する牽制
- ネット上での不正行為や迷惑行為の事前の抑止
- ネット上での不正行為や迷惑行為に対する速やかな排除処置の実行

そして、これらの課題の解決のためには、以下のような施策の推進が求められる。

- ネット上での不正行為や迷惑行為に対するルールの整備
- ネット上での不正行為や迷惑行為の早期検出技術の開発
- ネット上での不正行為や迷惑行為の実行者の追求技術の開発
- ネット上での不正行為、迷惑行為の追求体制の整備

3.4.8 ネットの利用やネットを介したサービスの提供での被害者救済の確立

ネットワーク社会を取り巻くさまざまな脅威は、ネットの利用者にもネットを介してサービスを提供する事業者にも被害を及ぼしうる。また、ネットを用いるシステムの特性から加害者の特定ができないこともありうる。

ネットワーク社会を安全で信頼できるものとするためには、万一、被害にあっても、一定の救済ができるようになっていなければならない。

このためには、以下のような施策の推進が求められる。

- ネット利用にかかる損害賠償についての基本原則の確立
- 保険の整備
- ADR 等被害の救済機関の整備

3.5 ネットワーク社会の安全と信頼の確保に向けた必要な取組み

前節に述べたような脅威の存在に対し、ネットワーク社会の安全と信頼を確保するためには、技術的な対応だけでなく、PKI や時刻認証サービス等のネットワーク社会を支える基盤サービスの整備、法制度も含むルールの見直し等による社会環境面での対応に加えて、ネット経由でサービスを提供する事業者やその利用者における自己の責任の認識と追求等が必要である。

そしてこれらのまったく別次元のともいえる分野での対応は相互に関連したものでなければならない。技術は技術でカバーできる範囲の拡大に努力しなければならないが、その限界を補うのが社会環境面での対応である。これらが一体とならなければ、社会の仕組み全体として一定の安全と信頼を担保することはできない。

それぞれの分野における必要な取組みを、表 3-8 に示す。

重点課題	技術面で必要となる対応		社会環境面で必要とな	
	開発課題	その他	基盤サービスの整備	ルールの確立、法制
⑴ システムの安定稼動の確保 システムの安全の確保 ⑵ 利用の安全の確保	・セキュリティ要素技術の強化推進 暗号技術、認証技術、通信の保護技術 タイムスタンプ技術 ・セキュリティツールの強化推進 認証ツール、OS のセキュリティの強化、侵入防止・監視ツール、ウイルス対策ツール、情報の保護ツール、ホームシステム用のセキュリティツール ・システムの安全性確保にかかるシステム技術の強化推進 セキュリティマネジメント技術、品質管理技術、信頼性確保技術、耐攻撃性確保技術、システム管理技術、システム運用技術	・システムに対する安全性基準の確立 ・システムの安全性評価モデルの確立 ・システム種別ごとのセキュリティ対策プロファイルの確立 ・情報セキュリティ専門要員の育成推進	・タイムスタンプサービス ・ネット社会全体をサポートできる認証スキームの確立 ・システムの安全性を評価認証サービスの検討 ・零細企業や家庭に対する安全支援サービスの整備 ・セキュリティについての情報提供サービスの再構築 ・ADR の整備	・認証の適用ルールの確立 ・特定のサービスに対する公的規 ・特定のサービスに対する自主規
⑶ 問題が生じた場合の責任の所在の明確化	・ネット上でのやり取りの証明方法の確立		・ネット上でのやり取りの公証サービスの整備	・サービスの提供者の責任の範囲 確立 ・複数のシステムのコラボレートス スで発生したトラブルの責任の の確立 ・責任の所在の証明についての
⑷ プライバシーの保護と 情報の保護の確保	・きめ細かく実務的な情報の保護技術の確立と必要なツールの開発		・電子情報の保護サービスの整備	・プライバシーの保護についての ・電子情報の保護についてのル ・電子情報の保護とその法的効 ールの確立 ・情報の保護の実践についての
⑸ 電子文書の有効性の確保	・長期見読性の確保 ・電子署名された文書の長期法的有効性の確保方式の確立とツールの提供		・電子文書の公証サービスの整備推進	・電子文書の法的効力の確保と の確立
⑺ 不正行為、迷惑行為の牽制の実現	・ネット上での処理の追跡技術 ・不正行為、迷惑行為の検出技術			・一般の商行為等が迷惑行為に のルールの確立 ・迷惑行為を牽制あるいは排除 立 ・不正行為や迷惑行為の存在を てのルールの確立
⑻ 被害者救済の仕組みの確立			・保険の整備 ・ADR 等救済機関の整備	・損害賠償の原則の確立

4 情報セキュリティ技術の課題についての考察

本章は、ネットワークを利用するシステムの安全を確保するための要である情報セキュリティ技術の一部について、本調査研究で議論された考察を纏めたものである。

4.1 ネットワーク社会の安全と信頼の確保に必要となる技術

ネットワーク社会の安全と信頼を実現するためには、技術の支えが必須となる。社会のネットワークへの依存がさらなる拡大に備え、開発、整備を進めるべき主な技術を、表 4-1 に示す。

表 4-1 主な技術課題

技術区分	課題となる技術
1 システムをセキュアなものするための技術	・セキュリティマネジメント技術 ・システムや機器の信頼性の確保技術 ・システムや機器の可用性の確保技術 ・システムや機器のおける耐攻撃性確保技術
2 ネット社会の安全と信頼を支えるシステム技術	・認証システム技術 ・時刻認証関係システム技術 ・電子文書の有効性保持技術 ・ネットワーク上でやり取りを証明する技術 ・ホームシステムのセキュリティ技術 ・ネットワーク処理の追跡技術 ・不法行為、迷惑行為の抑止技術
3 セキュリティツール技術	・IT プラットフォームのセキュア化技術 ・システムへの侵入防止技術 ・ウイルス対策技術 ・情報の保護技術 ・セキュリティツールとしての認証技術
4 セキュリティ基盤技術	・通信の保護技術 ・認証技術

4.2 システムをセキュアなものにするためのシステム技術の現状と課題

システムに必要なセキュリティの組み込み、そのセキュアな運用を実現するためには、システムの特性や運用環境を踏まえたセキュリティ要件の適切に定義し、定められたセキュリティ要件をシステムの作りに適切に反映するとともに、システムの運用上の不手際がシステムのセキュリティを損ねないようにしなければならない。また、システムの運用環境が変化しても、常に、求めるセキュリティのレベルが維持されるようにしなければならない。

表 4-2 は、システムをセキュアなものにするための要件と、それぞれが対応すべき脅威、および必要な施策をマップしたものである。

表 4-2 システムをセキュアなものにするためのシステム技術

セキュアなシステムの要件	対応すべき脅威	必要な施策		
		システムの品質の確保	システムにおける可用性確保対策の追求	システムの耐攻撃性の追求
1 可用性の確保の確保 必要なときにいつもシステムが利用可能であること	・施設、設備、ソフトウェアのトラブル（故障他） ・性能設計の不備、性能管理の不備 ・システム上の情報やソフトウェアの破壊や改ざん等の攻撃 ・DoS 攻撃等の外部からの運用妨害の試み	○	○ ○ ○ ○	 ○ ○
2 正確性の確保 システムの処理は信頼できる（期待通りである）こと	・システムに組み込む処理ロジック（機能）の不備 ・誤入力あるいは改ざんされた情報をもとにした処理の実行 ・システムへの不正アクセス等よるソフトウエアやシステム上の情報の改ざん	○		 ○ ○
3 秘匿性の確保 関係者以外が不正にシステムを利用したり情報を不正に取得できないこと	・システムへの不正アクセス等によるシステム上の情報の不正アクセス ・盗聴等の通信に対する攻撃 ・関係者からの情報の漏洩、流出			○ ○ ○

このことから、システムをセキュアなものにするための技術は、施設、設備、ソフトウェア等のシステムの構成要素に発生する故障等のトラブル、運用上の不手際、負荷の変動等が、システムの円滑なる運転に影響しないようにする**“システム可用性確保技術”**、システムを期待通りの処理をするものとして仕上げるための**“システムの品質確保技術”**、外部からのさまざまな攻撃や内部関係者がシステムに対して試みる攻撃の排除、およびその影響を極小化する**“システムにおける耐攻撃性確保技術”**に、これらを有効に機能するようにするために必要となる、システムに対するセキュリティ要求事項の適切な定義と、セキュリティ要求事項の実現をマネジメントするための**“情報セキュリティマネジメント技術”**を加えたの４つの技術カテゴリに分けて考えることができる。

以下に、それぞれの課題について述べる。

4.2.1 情報セキュリティマネジメント技術

情報システムのセキュリティは、技術面だけでなく、システムの構築や運用にかかわる要員にかかる人的管理面、施設や設備面での対応に加え、セ キュリティ対策の内容を決定やその実行の管理を組織的なものにする仕組み、システムの運用環境の変化によりセキュリティレベルを維持する

ための仕組みの確立も必要となる。情報セキュリティマネジメントとは、実施しているセキュリティ対策が、期待したものにするための組織の仕組みと、その仕組みを背景とした必要とされたさまざまな活動の管理活動を総称するものである。

システムが求めるセキュリティレベルを維持するためには、この情報セキュリティマネジメントを適切に行うための方法論が情報セキュリティマネジメント技術と呼ばれるものである。

4.2.1.1 情報セキュリティマネジメント技術のテーマ

情報セキュリティマネジメント技術のテーマとしては、表 4-3 に示すものがあげられる。

表 4-3 情報セキュリティマネジメント技術のテーマ

	技術区分	技術のテーマ
1	リスク分析技法	・分析すべきリスクと評価
2	セキュリティ要求事項の定義技法	・セキュリティ要求事項として定義すべき事項 ・指定した要求事項の評価
3	指定された要求事項の実践展開技法 システム構成への展開 システム運用への展開 業務運用への展開 要求事項の実行確認	・システム構成や各機器の設定への展開 ・システム構成や各機器の設置等の確認 ・システム運用への要求への展開 ・システム運用上の要求事項の実行の確認 ・業務運用への要求への展開 ・業務運用上の要求事項の実行の確認 ・施設、設備とその運用への反映とその確認
4	セキュリティ対策にかかる管理の仕組みの確立技法	・全体としてのマネジメントプロセス ・脅威分析のプロセス ・セキュリティ要求事項の定義プロセス ・指定された要求事項の実践展開プロセス ・セキュリティ要求事項の実行確認のプロセス ・実施しているセキュリティ対策の把握プロセス ・システムの運用環境の変化への対応プロセス ・脅威分析のプロセス
5	システムの安全性の評価技法	評価項目と評価 評価手順

4.2.1.2 現在の技術水準

現時点での確立している情報セキュリティマネジメント技術としては、情報セキュリティマネジメントシステム（ISMS）が存在する。また、この基準をさらに細かく定義したものとして「情報セキュリティ監査基準」が提案されている。

しかし、これらはセキュリティ要求事項として検討すべき事項の指摘と、その内容についての説明の範囲に止まっている。

4.2.1.3　取り組み状況と今後の課題

さまざまなシステムおけるセキュリティマネジメントを適切なものにするためには、表 4-3 にあげたような事項についての一般的な方法論の確立あるいは、雛型の整備が求められる。この点についての研究は、まだ緒についたばかりと言うのが現状であろう。

以下については、今後の研究が待たれる。

- リスクの分析技法
- セキュリティ要 求事項の定義技法
- 情報セキュリティにかかるマネジメントプロセス
- システムの安全性の評価技法

4.2.2　システムの品質管理技術

システムは常に期待通りに動かなければならない。このためには、システムの機能は、システムの要求に対して適切に設定されているとともに、誤処理を起こすような実装があってはならない。また、誤操作やエラーデータの入力が誤処理にむすびつかいようになっていなければならない。

このことを実現するためには、システムの構築にあたって、設計のレビューと実装についての徹底したテストを通じて、十分な品質を作りこまなければならない。システムの信頼性を確保するための技術としてハードウェアやソフトウェアの信頼性技術がる。

4.2.2.1　システムの品質管理技術のテーマ

システムが提供するサービスに対し適切のものである、かつ、期待した通りに正確に機能するようにする品質管理のテーマは、表 4-4 に示すようなものとなる。

表 4-4 システムの品質管理技術のテーマ

	システムの品質管理技術のテーマ	内容
1	要求定義技法	•システムの機能を提供するサービスに対し適切なものとしての定義と、その正確性の確認 •開発チームの正確に展開できる表現
2	システムの品質確認技法	•ハードウェアの動作の確認 ・ソフトウェアの品質の確認 ・ソフトウェアの管理

4.2.2.2　今後の課題

40 年以上にわたるシステム開発の歴史の中で、最も研究された一つがこの分野であり、要求定義技法や、要求定義をソフトウエアに展開する技術、システムの品質を管理する技術にはさまざまなものが提案され、年々進化していると言ってよい。

特に、システムの品質管理については、ISO 9000シリーズでその技術が集約され、実務にも広く展開されいてる。しかし、これらの技術については、ソフトウェア技術と連動すべきこともあって、常に、進歩する必要がある。

システムの形態も多種多様になり、システムの開発に用いられるソフトウェアもどんどん新しいものになっている。要求定義の方法や、システムの品質の確認技法は、アプリケーションの特性やシステムのアーキテクチャ、使用するソフトウェアによってまったく異なったものとなる。

メインフレームのシステムを前提に長年の研究や経験から確立されてきたこれまでのシステムの品質確保技術を、このような新しいシステム環境に適用できるようにすることは急務といえる。

現在のシステム、特にソフトウェアの品質管理技術が、新しいシステム環境に対応できているかどうかの評価の上に立った見直しが求められる。

4.2.3　システムにおける可用性確保技術

システムは多くの装置やソフトウェアの組立てに構成される。ネットワークを始めシステムを構成する装置やソフトウェアに欠陥がないことや故障が発生しないことの保証はありえない。システムが常に期待通りの機能を提供できるようにするためには、システムの構築にあたっては、これらにおける欠陥の存在や故障の発生を考慮に入れて、システムの稼動への影響を極力小さくする工夫が求められる。

代替機構の準備等で、稼動に影響がでないようにしたり、万一、停止するようなことにむすびついても、当該システムに要求される時間内に復旧できるように作られていることが求められる。

システムの可用性の確保は、コストがかかるものであるが、システムの性格によっては重要な課題となる。システムの可用性についての要求をどのように定義し、その実現を以下に図るかについては、それぞれのシステムの特性に応じて検討されなければならない。

この点に関する技術としては、システムの信頼性技術として、相当な歴史があり、すでに完成されたものと見てよく、問題は、個々のシステムにおける可用性についての取り組みにあるといえる。

4.2.3.1 システムの可用性確保技術のテーマ

システムの可用性を確保するための技術のテーマとしては、表 4-5 に示すようなものとなる。

表 4-5 システムの可用性確保技術のテーマ

	技術区分	技術のテーマ
1	必要な可用性の定義技法	・システムが実現すべき可用性の範囲の定義
2	障害対策技術	・システムに生じうるあらゆる障害（トラブル）の把握と、それぞれの障害に対する必要な対応の定義 ・必要な障害対策の組み込み確認 ・障害対策のシステムの運用環境の変更への対応
3	性能管理技法	・負荷の予測 ・システムの性能把握 ・システムへの必要な性能、容量の組み込み ・システムの容量の監視

4.2.3.2 今後の課題

障害対策技術や性能管理技術の一般論は、システムの現場ではすでに確立しているように見られるが、以下のような課題は存在する。現在、耐攻撃性についての大きな議論の影に隠れているように見えるが、今後、取り組むべき重要な課題である。

表 4-6 システムの可用性の確保にかかる技術の課題

	課題	課題の概要
1	工学的な技術としての未完成	・現場での経験的な技術は積み上げられているが、情報システムに対する障害対策の方法論や、性能計算等についての工学的な技術としては完成されていない
2	新しいアーキテキチャの登場	・新しく登場したシステムアーキテクチャにおけるシステムの性能計算技法は手探り状態が現実 ・一般的に新しいプロダクトの性能データが与えられないこと

特に、最近は、サーバや PC あるいはこれらの OS や DBMS 等のシステムのプラットフォームとなる製品の動作メカニズムや性能特性について明示されないところが多く、システムへの障害対策の設計や組み込んだ障害対策のテスト、システム性能設計や性能特性の確認を困難なものとしている。常用なシステムにおける可用性の確保のためには、この点が大きな改善が求められるところである。

このため、今後、必要となる取組みとしては以下があげられる。

- システムの障害対策技術や性能管理技術の工学的な技術体系への組み込み

- 新しく登場するアーキテクチャに対する性能管理技術の早期開発
- システムに組み込む新しいプロダクトにおける性能特性や性能データ、および障害対策に必要な情報の提供の迅速化

4.2.4 システムにおける耐攻撃性確保技術

ネットワークに接続されたシステムは、先に述べたように外部からさまざまな攻撃を受ける可能性がある。また、内部の者による内側からの犯行も無視できない。耐攻撃性とは、システムに対する攻撃に備えの総称であり、その基本要件としては、

- 攻撃を許しにくくなっている
- 被害を受けても被害範囲は限定できる
- 攻撃を許した場合、その事実を早期に発見でき、必要な処置が迅速に行える備えができているがあげられる。

4.2.4.1 システムにおける耐攻撃性確保のテーマ

システムが必要な耐攻撃性を確保するためには、当該システムのリスク分析にもとづき、想定される脅威の個々に対する予防処置と、脅威が現実になった場合の早期発見と必要な対応が、当該システムの特性の応じたレベルで当該システムに備えられていなければならない。

耐攻撃性確保技術は、このことを実現するための技術であり、表 4-7 に示すように、個々の脅威に対応する技術と、これらをシステムの構成や運用に反映する技術と、セキュリティインシデントへの備えの技術から構成される。また、個々の脅威に対応する技術は、セキュリティインシデントの予防技術と発生の早期発見技術からなる。

表 4-7 耐攻撃性確保技術の体系

	技術区分	技術のテーマ
1	脅威別対策技術 ・なりすましによるシステムの不正使用 ・システムへの不正アクセス ・セキュリティホール攻撃 ・ウイルス等の有害プログラムによる攻撃 ・情報の不正入手 ・通信の盗聴、改ざん ・DoS 攻撃	・認証技術 ・不正アクセス対策技術 ・セキュリティホール対策技術 ・ウイルス等の有害プログラム対策技術 ・システム上の情報の保護技術 ・通信の保護技術 ・DoS 攻撃排除技術
2	脅威別対策やセキュリティインシデントへの備えのシステム構成やシステム運用への反映技術	・セキュリティ要求事項のシステム構成への反映技術 ・セキュリティの要求事項のシステム運用への反映技術
3	セキュリティインシデントへの備えを確立する技術	・被害範囲の限定技術 ・被害の調査技術 ・システムの回復技術

脅威別の対策技術については、さまざまなところで議論されているので、ここでは、脅威別対策やセキュリティインシデントへの備えのシステム構成やシステム運用へ反映する技術について触れる。

(1) セキュリティ要求事項のシステム構成への反映技術

脅威別に策定した対策や被害への備えの多くは、システムに組み込まれて機能する。このため、これらをシステムの構成や個々の機器やソフトの設定に適切に反映しなければ、策定したセキュリティ対策は無意味となる。セキュリティ要求事項をシステムの構成や個々の機器やソフト設定に反映するためには、以下が求められる。

- 適切なシステム構成方針の確立と、構成方針に沿ったシステム構成の実現
- 脅威対応の対策やセキュリティ事故への備えの、個々の機器やソフトに対するセキュリティ要求事項への展開
- 個々の機器やソフトに対するセキュリティ要求事項の実装を確実にする技術
- システム環境やセキュリティ要求事項の変更を、システムの構成や個々の機器やソフトの設定に、遅滞なく確実に反映する技術

セキュリティ要求事項のシステム構成への反映技術とは、これらのことを適切に適切に行う技術を指す。

参考） システムの構成方針とは、以下のようなことについての決定することを言う。
・ゾーンの分割、サイト内での通信についてのルール、各サービスのネットワーク上での配置、情報の分散、一つのサーバにおけるサービスの同居、セキュリティサービス機能の配置、

(2) セキュリティ要求事項のシステム運用への反映技術

侵入の監視のためのログの分析やアクセス管理情報の維持等、脅威別に策定した対策や被害への備えの実現には、システムの運用に依存するところが少なくない。これらがシステムの運用に適切に反映されるようにするためには、以下が求められる。

- 脅威対応の対策やセキュリティ事故への備えの、システム運用への要求事項への展開
- その実行を確実にするための工夫

セキュリティ要求事項のシステム運用への反映技術とは、これらのことを適切に適切に行う技術を指す。

(3) セキュリティインシデント発生時の被害範囲の限定化技術

攻撃の未然に防ぐことは保証できないため、システムはいつか攻撃を受けるものと考えなければならない。この時、システムが大きな被害を受けないようにするためには、サーバや情報の配置等のシステムの構成上の工夫が必要である。被害範囲の限定化技術とは、システムに想定されるリスクやサポートしている業務等のシステムの特性を考慮し、万一、攻撃を許したとしても、被害が大きく広がらないようにする工夫を言う。

(4) 被害範囲の調査技術

攻撃等によりシステムに被害が発生した場合、影響を受けた業務の後始末やシステムの回

復のためには、被害範囲の正確な把握が要求される。セキュリティ事故発生時における被害範囲の特定のためには、以下が必要となる。

- システムの作りに応じた被害範囲の調査方式
- 被害範囲を特定を可能にする仕組みのシステムへの組み込み
- 処理履歴等の被害範囲の確認をするための情報の確保
- 被害範囲を確認するためのツールの整備

被害範囲の調査技術とは、以上のようなことをシステムに準備することを言う。

(5) 被害からの回復技術

セキュリティインシデントによる被害からシステムを迅速に確実に回復するためには、以下が必要となる。

- システムの作りに応じた被害からの回復方式
- システムの回復のためのデータの取得機能のシステムへの組み込み
- 回復用データの保護
- 被害発生時におけるシステム回復のためのツールの整備

被害からの回復技術とは、以上のようなことが確実に行われるための備えを総称するものである。

4.2.4.2 現在の技術水準

これらの技術についての現在の水準を、表 4-8 に示す。

表 4-8 耐攻撃性技術の水準

	技術区分	技術のテーマ
1	脅威別対策技術 ・認証技術 ・不正アクセス対策技術 ・セキュリティホール対策技術 ・ウイルス等の有害プログラム対策技術 ・システム上の情報の保護技術 ・通信の保護技術 ・DoS 攻撃排除技術	・DoS 攻撃への対策を除いては、毎年進化しており、必要最小限の技術は概ね確立していると見てよび、新たな攻撃手段の登場や、システム環境の変化に応じて、常に、新しいものが要求される。
2	脅威別対策や被害への備えののシステム構成やシステム運用への反映技術 ・セキュリティ要求事項のシステム構成への反映技術 ・セキュリティの要求事項のシステム運用への反映技術	・経験に依存しており、技術としては整理されていない。このため、この面で十分な対応ができているといえるシステムは多くないと見られる。
3	セキュリティインシデントへ の備えを確立する技術 ・被害範囲の限定技術 ・被害の調査技術 ・システムの回復技術	・経験に依存しており、技術としては整理されていない。このため、この面で十分な対応ができているといえるシステムは多くないと見られる。 特に、被害の調査技術は未研究領域とも言える。

4.2.4.3　技術現状と今後の課題

個々の脅威に対する対応技術は、すでにビジネスになっているところから、システム環境の進化や新たな攻撃手段への対応は、日々進んでいると考えてよい。一方、セキュリティ要求事項のシステムの構成や運用に反映する技術や、被害への備えに関する技術は、個々の脅威に対する技術ほど整備されているとはいえない。これは、これらに対する解が、システムごとに異なるため、抽象的なものにならざるをえず、ビジネスになりにくいことにも関係していると思われる。

システムの耐攻撃性の強化のための今後の課題としては、以下があげられる。

- システムアークテクチャの進化に対応した新たな攻撃を想定した攻撃予防技術の早期開発
- セキュリティ要求事項のシステム構成への反映技術の確立
- セキュリティ要求事項のシステム運営への反映技術の確立
- セキュリティインシデント発生時の被害範囲の調査技術の開発

4.3　ネット社会の安全と信頼をサポートするシステム技術の現状と課題

4.3.1　認証技術

社会の仕組み、企業等の組織の活動、家庭等における個人の生活の多くの場面でネットの利用が普及してきた場合、ネットを利用して何かを行おうとする者あるいはネット接続機器の識別、認証が重要な課題となる。

ネットでの相手の識別と認証については、すでに古い課題であり、さまざまな方式が導入され適用されてきているものの、今後のネット利用の進展は、相手確認を求めるシステム（サービス）の飛躍的拡大の点で、この問題に新たな課題としている。

4.3.1.1　高度ネットワーク社会におけるネット上での認証についての技術課題

ネットワーク社会における認証機能には、ネットへのアクセス者が利用者本人であることの確認、すなわち責任追及性の確保が第一義的に要求されるが、今後のネットワーク利用の高度化に際してはさらに以下の要件を考慮しなければならない。

- 認証の厳密さの多様性
- 認証の信頼性の確保
- 個人情報保護とのバランスの確保

(1) 認証の厳密性に関する多様な要求への対応

サービスの特性に応じて必要な責任追求性は異なる。責任追及性は認証行為に先立つ登録時の身元確認によって担保されるもので、認証を通じて得られる責任追及性はこの厳密さに依存する。認証の仕組みは責任追及性に関する要求の多様さに対応できなければならない。

(2) 認証に対する必要な信頼性の確保

当然の事であるが、脅威に対して強い認証の仕組みが利用者にネットワーク社会についての安心感をもたらす。なりすまし等の不安要素を排除できる仕組みが要求される。

(3) 個人情報保護とのバランスの確保

ネットワーク社会ではプライバシーはネット以前の社会よりはるかに深刻な危機にさらされる。利用者のあらゆる行動がデジタル情報として記録され蓄積されるからである。このようなプライバシー危機に対して、個人情報保護法に代表される制度的アプローチもあるが、それ以外に利用者個人が自衛できる手段も確保されなくてはならない。

それには本名以外に匿名（仮名）を使い分けることのできる認証の仕組みが必要である。ただし、この場合でも責任追及性は必要であり、責任追及性のある匿名（仮名）を実現する仕組みが必要である。

4.3.1.2 現在の技術水準

現在、用いられている技術には以下のものがある。

(1) パスワード

非常にポピュラーに用いられていて確立された認証技術であるが、今後の高度なネットワーク利用には、以下の点で問題があり、適しているとはいえない。

ネットワーク環境における認証に対しては、認証情報の盗聴と再利用によるなりすましの脅威がある。これは認証情報の反復性につけこむ脅威であり、毎回同じパスワードがネット上を飛んでゆくこの認証方式は本質的に弱さを持っている。ただし、この脅威はパスワードを SSL で保護すれば排除できる。

サービスが増大すると、サービスごとのパスワードは利用者の手間が大変になるだけでなく、サービス側に登録したパスワードを悪用したなりすましの脅威が発生する。特に P2P の利用環境ではその脅威は大きく、パスワード方式の認証は危険すぎる。これは、パスワード方式では登録情報と提示情報とが同じ形である事に起因していて、本質的な弱さである。

(2) ID カード、IC カード等の所有物

所有物の提示による認証は古くから使われてきた方式であるが、盗難や紛失の危険性があり、提示にあたって正当な所有者である事の確認を併用するのが普通である。紙の証明書に貼られた顔写真がこの役目を果たしている。ネット環境におけるひきんな例としては銀行の

ATM におけるキャッシュカードをあげることができるが、この場合には暗証番号を入力させることによって、正当な所有者である事を確認している。

この方式は物の認証が大前提であり、ATM のような認証する側の機器を用いる場合には適用できるが、オープンネットワークではサービス側の機器を利用者側に設置することはできないので、高度なネットワーク社会での認証の仕組みとしては用いられることはないと考えられる。次に述べる電子署名と併用される電子証明書はネットワーク利用を前提とした電子的なID カードと考える事もできる。

(3) 電子署名と電子証明書

⑴でも述べたように高度なネットワーク利用環境では認証情報の非反復性とともに登録情報と提示情報とが異なる形式である認証方式が求められる。電子署名を実現した技術であるデジタル署名は公開鍵暗号方式を利用するもので登録するのは公開鍵であり、提示するのは秘密鍵に基づく署名データである。電子証明書は登録された公開鍵を認証する側に伝える媒体としての機能を果たすもので、この利用により登録主体と認証主体（認証者）とを分離する事が可能になる。現在ある認証技術の中で高度ネットワーク利用にもっとも適した認証方式である。

電子証明書で名義者の身元以外の属性も証明させる考え方もあり、これを特に属性認証と呼ぶが、これは本人認証に付随する問題であり、この方式の導入にはまだ多くの議論が必要である。

(4) 生体認証

指紋や虹彩等のような人間の生体的特徴を利用する方式で、利用者各人に固有に属する情報を用いるので、一般的な信頼感が大きいものである。ただし、本質的にはパスワードと同じ性質を持つ方式であって、盗聴と再利用の脅威やサービス側によるなりすましの脅威を潜在的に有していることは、十分に理解されていなければならない。

4.3.1.3 取り組み状況と今後の課題

前述したように高度なネットワーク社会における認証技術としてはデジタル署名と電子証明書とを併用する方式が最も適しているとは言えない。以下ではこの方式に絞って述べる。

(1) 標準的なスキームの確立

① 認証・署名画面の標準化

デジタル署名を用いる認証方式は従来のパスワード方式と比べて普及度が低く、一般利用者にとってなじみが薄い。デジタル署名方式へ混乱なく円滑に移行するためには、利用者に見える認証操作の画面を標準化して各種サービスに実装することが重要となる。

② 証明のレベルの導入

登録時の身元確認の厳密性を示す情報を電子証明書上に表示する。これはその証明

書の証明の確かさのレベルを示す情報と考えてよい。換言すれば、高度ネットワーク社会で用いられる電子証明書の証明の確かさ（証明力）はみな同じではなく、証明力の異なるものが混在するという考え方の導入である。当然ながら電子証明書のコストは証明力のレベルによって異なる。サービス側は必要な責任追及性に応じた証明の確かさを持つ電子証明書の提示を要求する。

③　身元確認とサービス受益資格確認との分離

現在用いられている電子証明書はサービス側で発行されるのが普通である。すなわち、サービス受益資格証明書の性格を持つもので、ネット以前の社会で用いられる各種の会員証（キャッシュカード、クレジットカードなどを含む広義の会員証）の延長線上にある考え方である。

これは普及の第一ステップと言うべき姿であり、高度なネットワーク社会ではサービスの数が増大し、この方式では利用者はサービスごとの電子証明書を管理する必要が出てくるのできわめて使い勝手が悪い。

これを解消するには、身元を証明する機能だけを持つサービスとは独立な電子証明書を発行し、サービス側ではこの身元証明に基づいたサービス受益資格の登録を行い、サービス要求の受付時には身元証明書の提示を受けて登録の有無を確認する。

すなわち、登録はサービスとは独立な身元の登録とサービスごとの受益資格登録とに分けて実施され、分けて管理されることが必要である。

(2) 技術標準の確立

デジタル署名で用いられる利用者固有の秘密情報は秘密鍵であるが、これは安全性のためにはパスワードとはけた違いに長いことが必要であり、現在は 1024 ビット程度の長さが用いられている。この長さは人間の頭に記憶できる限界を超えており、実運用上は IC カードのような保管媒体に入れて常時携帯する形をとらざるを得ない。

この高度ネットワーク社会における ID カードであり、印鑑である IC カードは以下の機能が必要である。

- 秘密鍵の保管
- デジタル署名の実施

  秘密鍵の漏洩を防ぐには、この IC カードから秘密鍵を読み出してデジタル署名を生成するのではなく、署名対象データをこの IC カードに引き込んで IC カード内で署名を生成する事が必須である。
- 電子証明書の保管

  利用者が操作する PC 等の機器はこの IC カードを差し込んで利用できるインタフェースが必要であり、その標準化が必須である。また機器側のソフトからこのデバイスを使うための API の標準化も必須である。

  またこの IC カードの盗難・紛失対策も必須である。すなわち、利用時に正当な所有者であることを確認してから利用させる仕組みが必要である。現在使われている方式では PIN を設定しておき、利用時にそれで所有者確認を行うものが普通であるが、指紋等の

生体認証をここに利用するのはその特性を生かした利用法であり、今後の形をして普及が期待される。

(3) 関係基盤サービスの整備

電子証明書を発行する仕組み、その有効性を検証する仕組みの整備が必要である。

- 証明のレベル付証明書の発行

  認証局では何種類かの証明力の異なる電子証明書を発行するサービスを提供しなければならない。もちろん前述したように証明力は登録時の身元確認の厳密性に依存するから、強い証明レベルの証明書ほど発行費用は高くてよい。すなわち、認証局は多様な電子証明書とそれに応じた多様な発行費用のサービスメニューを持つ必要がある。

- 証明書の有効性確認

  電子証明書を参照する場合にはその有効性確認が必須であり、そのための仕組みの整備も必要である。有効性確認の厳密性についてもいくつかのレベルがあって良いと考える。すなわち、有効性確認の方式によって無効になった事実の反映スピードの違いが起こる可能性が大きい。換言すれば有効性確認のコストによって、その厳密性には差が生じえる。サービスに必要な責任追及性で許容し得るコストに見合う有効性確認の方式が選べる事が必要である。

(4) 法制度面での整備

- 公的個人認証の民民利用

  現在考えられている公的個人認証は公（官）によるサービスでの認証にのみ用いる前提で考えられているが、これを民によるサービスでも利用可能にする事が必須である。これは印鑑証明の利用場面を考えれば自明である。

- 証明のレベル

  サービス内容によってその責任追及性に応じた証明力を持つ電子証明書が要求される。ある種のサービスに関しては、たとえそれが民によるサービスであっても、これを法制度的に決める必要があるかも知れない。

- 法執行機関による匿名（仮名）証明書の実名の身元アクセス

  責任追及性のある匿名電子証明書とは登録時には実名による身元確認を行うが、電子証明書上の名義は匿名（仮名）を許すものである。この名義人がネットワーク社会で正直に振舞っている限りはその匿名性は守られるが、不正を働くと法執行機関は認証局（すなわち登録管理機関）にアクセスしてその実名やその身元情報を得ることのできる仕組みによる。認証局は民間の運営する場合も考えられるが、その場合でも法執行機関による、しかるべき手続きを経たアクセスは法制度的に可能にしておかなければならない。

(5) ネット接続機器への実装展開

前述した電子署名用の IC カードは利用者が扱うネット接続機器すべてで使用可能でなければならない。したがって、そのためのデバイスがすべてのネット接続機器に実装されなけれ

ばならない。

(6) 一つの提案

かなり大胆に一つの試案を以下に述べる。

- 高度ネットワーク社会の構成員（ほぼ全国民）は電子署名用 IC カードを持つ
- これには署名用秘密鍵と対応する電子証明書とが格納され、生体認証による所有者確認機能を備える
- 一人の利用者が証明力の異なる複数の IC カードを持っても良い。またその名義が匿名（仮名）であってもよい
- サービスはその必要な責任追及性に応じた証明力の電子証明書を元にして、サービス受益資格の登録を行い、サービス実施時にはこの証明書による受益資格確認を行う。匿名（仮名）の可否はサービスの性格によってサービスが決めることである
- 上記の電子証明書の発行主体は証明力の高い公的機関だけでなく、証明力は低くても簡易な手続きでの発行を可能にする民間機関もあり得る

社会の仕組み、企業等の組織の活動、家庭等における個人の生活の多くの場面でネットの利用が普及してきた場合、ネットを利用して何かを行おうとする者あるいはネット接続機器の識別、認証が重要な課題となる。

4.3.2 電子文書の有効性保持にかかる技術

4.3.2.1 電子文書の有効性保持についての課題

一般に文書は、作成⇒活用⇒保存⇒廃棄というライフサイクルを辿る。電子文書を考える場合、各過程を「紙」による情報管理からネットワークを駆使した電子化された情報の管理に移行することに伴い、3つの課題が発生する。すなわち、「完全性の確保」、「機密性の確保」、「見読性の確保」である。旧総務庁の共通課題研究会報告書では、「電子文書の原本性を確保する」とは「電子文書について、紙文書と比較した場合の保存・管理上の問題点が解決された状態にあるようにしておくこと」とし、その要件として上記3項目をあげている。

特に電子文書の長期保存を実現する場合には、基本的には、数年から数十年にわたる長期間利用される電子文書を対象としたときの、上記の３つの課題の解決が必要であるといえる。

長期の運用が短期の場合と異なるのは、電子文書をめぐる技術状況が大きく変化する可能性が高い点である。したがって技術状況の変化がおきたときの影響を踏まえて諸問題を定義し、その解決に向けた技術テーマと技術的アプローチを行い、現状の対応状況と今後の研究課題を明確にしておく必要がある。

(1)　完全性の確保」に関する課題

完全性の確保」とは、電子文書が正規の文書として確定した時点あるいは真正に成立した時点以降、そのままの状態を保持し続けることである。保持すべき対象には、文書の内容の他に、その作成者や作成時刻あるいは作成意図等を含めて考えなければならない場合が多い。

完全性の確保を妨げるのは、記憶媒体の物理的な劣化、利用者による事故または故意の改ざんなどである。記憶媒体の劣化には、記憶媒体の改良やバックアップ技術による消失・変化の防止が直接的な対策である。改ざんに対しては、アクセス管理の徹底による改ざん防止、改変履歴の管理による改ざんの回復、また、電子署名等などによる改ざん検知などが対策としてあげられる。

これらのうち、消失・変化の防止、改ざん防止、改ざんの回復については、技術状況の変化に応じて随時改良していくことによって対応可能な課題であると考えられる。改ざん検知については、現在は、暗号技術をベースとした電子署名等の技術にもとづいているため、将来的に鍵漏洩や、ベースとしている暗号技術の危殆化が起こったときには、改ざん検知が有効に働かなくなる恐れがある。これはあらかじめ技術状況の変化を見越して、事前に対策したほうがよい課題といえる。

(2)　機密性の確保」に関する課題

現在のところ、基本的に、格納された電子文書の機密性は、アクセス制御技術によって確保されている。攻撃手法の多様化、大規模化等に応じ、アクセス制御技術には解決すべき個別の課題があるが、これらのほとんどは技術状況の変化に応じて随時改良していくことによって対応すべき課題であるといえる。

また、通信路上の電子文書の機密性は第三者からアクセスされる恐れのない専用線を用いる他、暗号技術を用いた秘匿によって確保されることも多いが、短期的に機密を確保する場合は、その時点で安全性が確保されていると認識されている技術を用いればよい。

ただし、格納された電子文書の機密性の確保を、暗号技術を用いた秘匿によって行っている場合、すなわち、暗号化されたデータには攻撃者もアクセス可能な場合には、長期の運用中には、将来的に解読される可能性があるので、あらかじめ将来の技術状況の変化を見越して事前に対策すべき課題となる。

(3)　見読性の確保」に関する課題

見読性の確保」に関しては、現時点で、利用者のプラットフォームに依存せずに参照を可能とするという課題に加え、現在利用されている電子文書の格納媒体や格納フォーマット、電子文書フォーマットを、数十年先においても利用可能にするといった長期保存にかかわる課題がある。IT 技術の進歩は早いため、現在広く利用されている電子文書フォーマットであっても、数十年先に利用されているとは限らず、電子文書フォーマットを参照するためのアプリケーションやアプリケーションの動作する OS を含めたプラットフォームが存在しないために、電子データとしては保存されていても、正しく読めなくなる恐れがある。また、電子文書フォーマットの仕様が不明であるために、新たなプラットフォーム上にその電子文書フォーマットを正し

く解釈するアプリケーションを再現することができなくなるようなケースも考えられる。

(4) 「法的有効性の確保」に関する課題

以上に述べた各課題のうち、電子文書の長期保存・利用促進の観点から、特に問題となるのは、(1)完全性の確保に分類される課題である。いわゆる電子署名法の施行により、電子署名に法的裏付けが与えられたものの、有効期限切れが生じた後の電子署名に対してはなんら直接的な裏付けを与えるものではない。タイムスタンプ技術の有効活用により、技術的には電子署名文書の長期保存が可能となる見通しであるが、法的裏付けを与えるための技術や運用に関する要件整理が必要である。

4.3.2.2 技術の現状

(1) 完全性の確保

表 4-9 に、電子文書の完全性お確保にかかる技術の現状を示す。

表 4-9 電子文書の完全性の確保にかかる技術の現状

テーマ	現在使用されている技術
電子文書の消失および変化の防止	バックアップの実施により対処している。これにはバックアップ媒体の有効（保証）期間にもとづき定期的に再バックアップを実施することも含んでいる。 また、災害時への対処のため、多重バックアップや、さらに遠隔地に分散した形での多重バックアップも一部で実施されるいる。
改ざん防止	電子文書の改変のためのＡＰＩへのアクセスを限定した耐タンパな機器（装置を分解するなどして、内部の秘密情報を不正に入手あるいは改ざんしようとする行為に対する体制を持った機器）からだけに制限するなどして不正な改変を防止する。 また、追記型格納媒体を用いて記録済み文書の書き換えを防止する措置などもとられることもある。 ウイルスチェックもウイルスによる情報の改ざん防止策の一つに数えられる。
改ざん回復	電子文書への改変履歴を取得し保管する。この記録を元に改変前の状態を回復する
改ざん検知	電子文書に電子署名を付与して保存する、MAC(Message Authentication Code)を付与して保存する、電子文書のハッシュに対して電子署名を付与して電子レシート（あるいはタイムスタンプ）を生成し、電子文書とともに保存する、などの対策がとられる。 電子文書のハッシュをリンキングプロトコルにより時系列に連結させた値から生成したハッシュ値を新聞等のメディアに公開するような技術もある
長期保存にかかわる技術	電子署名の有効性をその有効期限を越えた時点で確認できるような拡張された署名フォーマット（長期署名フォーマット）が提案されている（RFC3126）。 また、署名の連鎖情報を署名履歴として保持することにより署名の偽造を困難にする「ヒステリシス署名」が提案されている。これらは、ECOM 認証・公証 WG 電子署名文書長期保存に関する中間報告（H13-認証・公証 WG-3,2002/3）」および「電子署名文書長期保存に関するガイドライン(H14-認証・公証 WG-3,2003/3)」に詳しい。 このほか、秘密鍵漏洩を前提とした署名偽造対策技術として、フォワード・セキュア署名、実行ハードウェア確認タグ付きデジタル署名、MAC 付きデジタル署名なども研究されている（宇根正志「デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策」日本銀行金融研究所、2002/10）

(2) 機密性の確保

表 4-10 に、電子文書の機密性の確保にかかる現在の技術水準を示す。

表 4-10 電子文書の機密性の確保にかかる現在の技術水準

テーマ	現在使用されている技術
アクセス制御	計算機リソースに対する一般的なアクセス制御技術を用いる
暗号技術を用いた秘匿	利用者の知識（パスワードなど）、利用者の保持するトークン（IC カード、USB トークンなど）に格納された情報、再生装置、格納媒体などに関連付けられた鍵によって暗号化して保存 鍵をいくつかに分散して保存しておき、その中のある閾値以上の個数の鍵を揃えなければ復号できないようにする技術 暗号化した電子文書をアクセス条件とともに一体化（カプセル化）しておき、利用者によって同一電子文書に対するアクセス許容範囲を変えるような技術もある

(3) 見読性の確保

表 4-11 に、電子文書の見読性の確保にかかる現在の技術水準を示す。

表 4-11 電子文書の見読性の確保にかかる現在の技術水準

テーマ	現在使用されている技術
(1) プラットフォーム非依存の参照	PDF，XMLなど標準フォーマットの使用 多くのプラットフォームで表示可能であるように標準のイメージ形式の変換
(2) 長期保存にかかわる技術	PDF、XML など、仕様が明確に公開されている標準フォーマットの使用

4.3.2.3 今後の課題

文書の中には、法的に数十年にわたって保管することが義務付けられている文書もある。このような文書を電子化した場合に、少なくとも紙と同様な安全性を確保できるようにすることが今後の中心課題である。

このためには、電子文書の真正性を証明する電子署名の有効性を法定の保存期間にわたって保持する必要がある。現在、電子署名文書長期保存のためのさまざまな技術が提案されているが、運用面まで含めて安全性に対するコンセンサスが形成されている状況にはなく、そこに向けた努力が必要である。

長期署名フォーマットを利用する場合でも、長期保存を想定した署名ポリシ (RFC3125 として標準案は提案されているものの)のプロファイルやその運用管理要件、タイムスタンプに対する技術要件および運用要件などの検討や整理が大きな課題として残されている。

暗号技術を使って機密性を長期にわたり確保することは比較的容易に解決できるであろう。暗

号技術が脆弱化してしまう前に新たな技術によ再度暗号化する、あるいは新たな技術により重畳的に暗号化する等の対策が考えられるからである。ただし、完全性の確保と機密性の確保を両立させたいような場合、複雑な問題を生じることになる。機密性確保を優先して暗号化電子文書から署名を生成するか、あるいは逆に電子署名文書を暗号化するか。いずれの手段をとるかにより、完全性の長期確保や機密性の長期確保の方法に大きな影響を与えることとなると思われる。

見読性の長期確保に関しては、議論の場があまりない状況である。OS や文書作成ツールとの関係なども含め、長期保存の観点からの調査が必要である。また、完全性確保との両立を考えた場合、電子署名の性質から、安易なフォーマット変換はできない。電子署名の添付を想定した上での対処を検討していく必要がある。

4.3.3 システム間でのやり取りを証明する技術

ネットワークを介して行う処理においては、ネットの先のシステムの不具合による処理の不成功や、処理要求の無視や、第三者の介入による身に覚えのない指示等により処理が実行されるといったようなトラブルも起こりうる。このようなトラブルに起因する紛争においては、どちらにその責任が所在するのかを証明できなければならない。一つのサービスが複数のシステムのコラボレーションにより提供されているような場合で、トラブルが生じた場合大きな問題を引き起こすようなシステムおいては、この問題は特に重要となる。

このような問題に対しては、ネット上でのシステム間でのやり取りを、法的にも効力のある形で証明する技術が必要となる。

4.3.3.1 二つのシステムのコラボレーションにおける責任の分界についての原則

二つのシステムのコラボレーションで発生したトラブルに対する責任の所在を決定するためには、コラボレーションする二つのシステム間での責任の分界について基本となる原則が確立していなければならない。この原則は、責任を証明するための技術要件の確立と、このような技術を用いた証明に対し法的な効力を与えるためのベースとなるものである。

現時点で、この点について確立した原則は存在しない。このため、ここでは、一つの提案として、その原則についての考え方を示す。

責任の分界についての基本原則としては、表 4-12 のようなものが考えられる。

表 4-12 ネットを介した二つのシステム間での責任の分界の原則

施策区分	責任を取るべき事態
(1) 処理要求側の責任 ・必要に応じ、適切な処理の要求を処理の請け負う側に届けること ・処理の結果を見届けること	・必要な時に、必要な処理の要求を行わなかった場合（処理の要求が相手に届いていない場合も含む） ・処理の要求が妥当でなかった場合 ・処理の結果のチェックを適切に行わなかった場合
(2) 処理受け持ち側の責任 ・受け付けた処理要求を適切に処理すること（含む、処理の結果を要求側に報告すること）	・処理要求の妥当性を適切にチェックしなかった場合 ・要求された処理を適切に実行できなかった場合

この原則は、処理の要求が処理を実行する側で受理された（アプリケーションレベルで受取られた）時点を、責任分界ポイントとしている。この点は、電子契約法が、契約メッセージが、受信側がそれを受取れる環境に届いたことをもって成立するとする責任分界の考え方と異なる。これは、二つのシステム間でのリアルタイムでのコラボレーションを対象としているためである。

この原則は、以下のような考えにもとづく。

表 4-13 は、図 4-1 に示すようなプロセスで示される二つのシステム間でのコラボレーションに発生するトラブルとその発生場所（責任の所在場所とは異なる）をプロセスごとに示したものである。

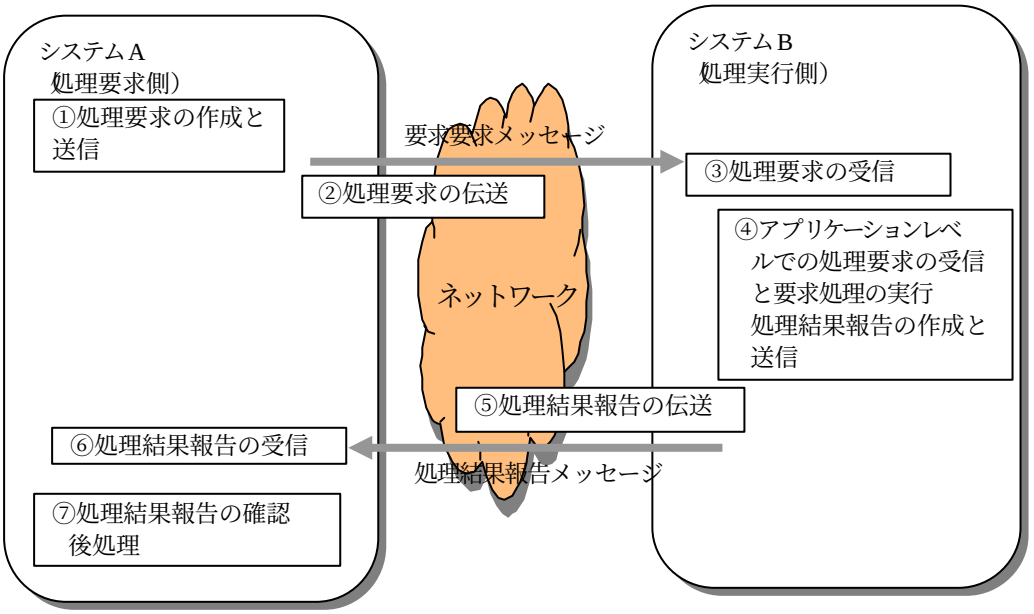


図 4-1 二つのシステム間のコラボレーションのプロセス

表 4-13 システム間のコラボレーションのプロセスに生じるトラブル

コラボレーションのプロセス	当該プロセスあるいは次のプロセスとの間で発生しうるトラブル	トラブルの発生場所		
		要求側	ネットワーク	処理側
①システムＡでの要求の作成と送信	･処理要求作成、発信上の不具合	○		
②処理要求の伝送	･伝送路上の問題による要求メッセージの不到達 ･処理要求を受けるシステム側の問題による要求メッセージの不到達		○	○
③システムＢでの要求の受信	･処理要求を受けるシステム側の問題による受信側での受信メッセージの消失 ･アプリケーションレベルで要求を受領後の処理の不実行			○ ○
④システムＢにおける受信した要求に対する処理 ･要求に対する処理 ･処理結果の報告の作成と送信	･処理要求を受けたシステム側の要求処理に対する処理の不具合			○
⑤処理結果報告の伝送	･伝送路上の問題による処理結果報告の不到達 ･システムＡ側の問題による不到達	○	○	
⑥システムＡでの処理結果報告の受信	･システムＡ側の問題による処理結果報告の消失	○		
⑦システムＡにおける処理結果報告の受け取りと後処理	･処理要求側における受信した処理結果の確認や ･後処理の不具合	○		

プロセス①で生じた不具合の責任がシステムＡにあることは論を待たない。プロセス②での通信路上のトラブルで処理要求メッセージがシステムＢに届かない場合は、システムＢは要求を知りようがないため、責任の取りようはない。また、システムＢで処理要求がネットワーク的には受信されていたとしても、システム上に発生した障害等で、このメッセージがアプリケーションで処理される前に消失することも考えられる。このような場合においても、システムＢは、システムＡからの要求を知りえないため、その責任は追求できない。このようなケースでは、システムＡは、システムＢからの処理結果報告がこない等で、システムＢに処理要求が到着していないことが類推でき、要求の不到達に対する必要な処理を取れる立場にあるため、その結果についての責任はシステムＡ側にあると考える。

一方、プロセスが③にまで至れば、システムＢは要求された処理を所期の定めの通りに完結する義務があるため、要求の真正性の確認、要求処理の仕様通りの完結、処理結果報告のシステムＢへの送信までに生じた不具合は、システムＢの責任となる。処理結果報告の未到着は、システムＢはシステムＡからの処理結果報告の受領確認メッセージの受信をもって確認できるため、システ

ムB が負うべきものである。ただし、システムA はシステムB からの処理結果報告がこないことに対して、要求処理が完結しないことから、システム A も何らかの対応もすべきであるため、システム A にも責任の一端は生じる。

また、プロセス⑦のシステム B での処理結果の確認や、処理結果に対する後処理を適切に行うことは、システムA の責任となる。

4.3.3.2 システム間でのコラボレーションで生じたトラブルに対する責任の所在の分界方法

4.3.3.1 節に述べたような責任の所在に関する原則に立った場合、実際に発生したトラブルに対し、それぞれの側は表 4-14 に示すに相手側に責任があることを指摘できることになる。

表 4-14 相手側の責任と指摘できるケース

施策区分	責任を取るべき事態
処理要求側（システム A）が責任は処理の要求先（システムB）あると指摘できるケース	・システムB は要求を確認しているのに、処理が行われず、要求が無視された場合 ・要求に沿った処理が正しく行われなかった場合 ・処理結果報告が実際に行われた処理と異なっていた場合
処理を依頼された側（システム B）が、責任は処理要求側（システム A）にあると指摘できるケース	・システムA からの処理要求が不適切であった場合 （トラブルは不適切な要求にもとづく処理が行われた結果による） ・システムA におけるシステムB からの処理結果報告に対する後処理が適切でなかった場合

このような考えにもとづいた場合、二つのシステム間でその責任の所在を明らかにするためには、以下に示すような情報が必要ということになる。

- システム A からシステムB に送信された処理要求の内容と、それをシステム B においてアプリケーションレベルで受取られている証明できる情報
- システムB における処理要求に対する処理結果を証明できる情報
- システムA からシステムB に送信された処理結果報告の内容と、それをシステムA がアプリケーションレベルで受取っていることを証明できる情報

これらの情報が揃えば、処理のプロセスをトレースすることにより、二つのシステム間で行われたコラボレーションで発生したトラブルに対する責任のある側を明らかにすることが可能となる。

4.3.3.3　責任の所在の分界のための情報を確保する方法

4.3.3.3 節にあげた二つのシステム間で行われたコラボレーションで発生したトラブルに対する責任側を明らかにするための情報の確保の方法としては、以下のような方式が考えられる。

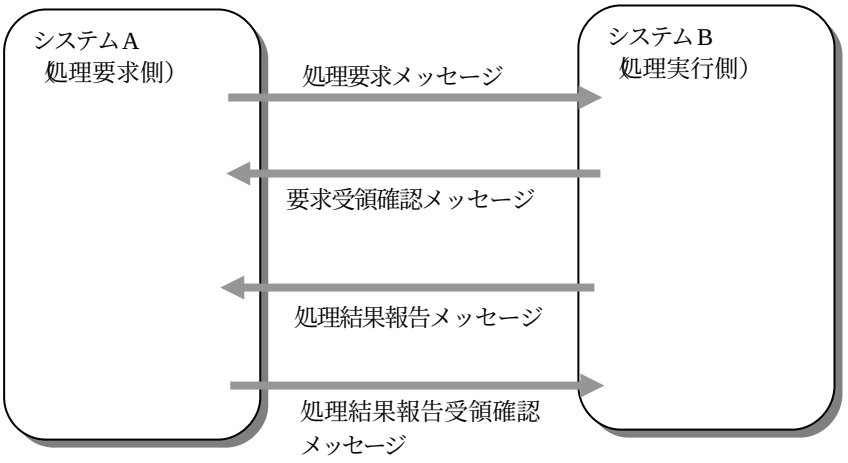


図 4-2 コラボレーションするシステム間でのやり取りを証明する情報の交換

図 4-2 は、コラボレーションするシステム間でのやり取りを証明するに必要な情報の交換のイメージを示している。要求を実行する側のシステムＢは、要求をアプリケーションレベルで受取ったことを示す要求確認メッセージを処理の要求元であるシステムＡに返す。また、システムＢは処理結果報告をシステムＡに対して行い、システムＡはシステムＢから送られてきた処理結果報告をアプリケーションレベルで受取ったことを確認する処理結果報告確認メッセージをシステムＢに返す。

それぞれの確認メッセージの役割と、取得ならびに保管要件は以下の通りとなる。

(1) 処理要求メッセージ

システムＡからの処理要求が、そもそも妥当なものであったかのを、後日確認するための情報として、システムＢが取得、保管し、必要に応じて提示できるようにするものである。このメッセージの取得、保管、提示に当たっては、その真正性が証明できなければならない。

(2) 処理要求受領確認メッセージ

システムＢにおいて、システムＡからの処理要求がアプリケーションレベルで受付けられたことを、処理要求をだしたシステムＡに伝えるものメッセージである。

システムＢがシステムＡからの処理要求をアプリケーションレベルで受付けていることは、システムＢ側の責任を追求する側のシステムＡが証明しなければならないが、このためには、システムＢがシステムＡからの処理要求を受付けたことを確認するメッセージを取得、保管し、必要な場合にこれを提示する方法が考えられる。

このとき、このメッセージは以下の要件を備えて今ければならない。

- システムＡからの要求内容を示せること
- システムＢがアプリケーションレベルで受付けたことを証明できる内容が含まれてい

ること

- システムＡからの要求内容は真正であること（改ざんされていないこと）が示せること
- システムＡが受信し、保管し、提示する受付け確認メッセージは真正であることを示せること

このため、システムＢからシステムＡに送信される要求受領確認メッセージは、システムＢにより電子署名されたものであることが要求されることになろう。

(3) 処理結果報告メッセージ

システムＢにおける処理結果をシステムＡに伝えるもので、後日、システムＢにおける実際の処理と報告された処理結果にずれがある場合等に、そのことをシステムＡが示すためのもので、システムＡが取得、保管し、必要に応じて提示できるようにするものである。このメッセージの取得、保管、提示に当たっては、その真正性が証明できなければならない。

(4) 処理結果受領確認メッセージ

システムＡがシステムＢからの処理結果報告を受取ったことをを証明するためのメッセージであり、システムＢが要求された処理を実行し、システムＡに報告したことを証明するためのものである。これは、システムＡによるシステムＢからの処理結果報告を受領していることの否認や、処理結果報告の改ざん等に備えるものである。

システムＡがシステムＢからの処理結果の報告をアプリケーションレベルで受取っていることについての証明は、トラブルはシステムＡがシステムＢからの処理結果を適切に処理しなかったことに起因していることを、システムＢが証明する場合に必要となる。

この場合、システムＡ側の責任を追求する側となるシステムＢが証明しなければならないが、このためには、システムＡがシステムＢからの処理結果報告を受取ったことを確認するメッセージを取得、保管し、必要な場合にこれを提示する。

このとき、このメッセージは以下の要件を備えて今ければならない。

- システムＢからの処理結果報告の内容を示せること
- システムＡがこの報告を、アプリケーションレベルで受取ったことを証明できる内容が含まれていること
- システムＢからの処理結果報告は真正であること（改ざんされていないこと）が示せること
- システムＢが受信し、保管し、提示する処理結果報告受領確認メッセージは真正であることを示せること

このため、システムＡからシステムＢに送信される処理結果報告受領確認メッセージは、システムＡにより電子署名されたものであることが要求されることになろう。

4.3.3.4　今後の課題

ここでで示した方法は、現時点では、まだ一つのアイデアレベルのものであるが、このコラボレーションするシステム間での責任の分界を証明する技術は、今後のシステム間のコラボレーションの拡大に備え、発生したトラブルによる紛争等の備え、さらに多くの議論を経て、一つの標準として確立されたものにならなければならない。

この課題の解決にむけては、以下についての取組みが必要となる。

- コラボレーションするシステム間で発生したトラブルの責任の所在を明らかにするための仕組みの確立

  この仕組みには、責任の分界のルールにもとづいた責任の所在の証明方法、その証明方法を実現するための証拠情報のあり方、その保管や提示の方法等を含む
- 確立した方式のシステムへの実装技術の標準化

  使用する情報の形式やシステム間でのやり取りについてのプロトコル、アプリケーションインターフェイス（API）等を含む
- 確立した標準方式によるネット上でのシステム間でのやり取りの証明の法的有効化
- 確立した標準方式のシステムへの実装を容易にするプロダクトの提供

4.3.4　ホームシステムのセキュリティ確保技術

家庭内におかれるシステムはそのほとんどが、単独で機能するものが多く、電源とアース、そして設置ないし保管場所と操作や設定をする人間を考慮するだけでよいため、セキュリティ対策というと装置の盗難や子供のいたずら操作等を抑止する程度の対策があればことは足りていた。その後、プログラム可能な製品も登場したが、プログラムをはじめとするロジックはＬＳＩ等に組み込まれメーカーにおいて出荷時に供給されていて、プラットフォーム（OS等）やプログラム（インタプリタ、ライブラリ、ランタイム等）はメーカー毎に独自であることが多く、その仕様は一般には公開されていなかったため製品利用者や第三者が介入することはまず不可能であった。ネットワーク機能という観点では、一部にホームテレホンや家庭用交換機の普及があったが、音声会話やアラームの送受信等のアナログ通信であり、その設置や設定はメーカーや専門業者によってなされていて、セキュリティ対策は(盗聴という問題はあったが)ほとんど不要であった。

その後家庭へのパーソナルコンピュータの普及が進むに従い、セキュリティ上における問題が拡大するかに思われたが、パーソナルコンピュータの仕様がメーカー毎に異なっていたことや、ネットワークの利用がモデムやカップラーを用いてアナログ電話回線経由で直接プロバイダに接続する単純なクライアントサーバ型で、セキュリティ上は機器単独でもネットワークにおいても、さほど問題にはならなかった。とりわけネットワーク利用においては、ネットワークへの接続手順が標準化されたものでなく、コマンドプロンプトから直接ターミナルコマンドを入力する必要や、プロバイダ毎に

特殊な接続用ソフトウェアの上で利用する必要があったことや、回線利用料金も高価であったため利用するたびに回線の接続と切断を繰り返していたことが原因としてあげられる。

現在では、家庭におけるパーソナルコンピュータはインターネットの普及と同時にデファクトとも言えるプラットフォームの登場、低価格化や小型化がされ、一家に一台から一人一台へと普及して行く勢いであり、他にも子供のいる家庭を中心に普及していたテレビゲーム機はゲームコンテンツにおけるインターネット利用が拡大しており、同時に大容量のネットワークが低価格で提供されるようになった結果、一般家庭でもインターネットを核としたネットワークへの常時接続環境が整いつつある。

その結果、これまで企業等でのみ利用されていたネットワーク接続を前提にしたプラットフォームやアプリケーションが、その利用頻度は別にしても一般家庭にまで導入拡大が進んでいる。これは同時に、企業で問題になるネットワークウィルスやアクセス制御が、家庭においても問題となりつつあることを予期させる。ただし、特定の企業を狙った不正アクセス等に比べると、ピンポイントで直接狙われることは少なく不特定多数としてターゲットとして踏み台的に利用される被害に留まっていることや、取り扱っている情報も限られていてその被害も比較的まだ小さく、その被害の存在すら認知されないままの場合も多く、もし気づいていたとしても企業で利用されるような高額なセキュリティ対策費用を負担できないため、パーソナルコンピュータにおいては OS や AP の再インストール、テレビゲーム機においてはリセット、家電製品に至っては電源の再投入やメーカー修理依頼といった対症療法的な対策で済まされている。

しかし近年では、一部の家庭においてホームサーバや高機能なネット家電が導入される兆しがあり、ネットワークの常時接続化が進行してきており、ネットワークセキュリティ問題は家庭生活への影響や一般家庭がインターネット社会における加害者になる恐れを生じ始めている。さらに、家電にはパーソナルコンピュータやテレビゲームのようにＬＳＩと人とのインタフェースだけでなく、100V で動作するヒーター、マイクロウェーブ発生機構やモーター等を自動制御する機能もあり、これまでに想定できない火災やけがを起こす等の物理的な危険も想定される。

4.3.4.1　ホームシステムのセキュリティにかかる技術のテーマ

まず、ホームシステムをネットワーク利用のパターンから、以下のように分類できる。ここではホームシステムの構成コンポーネントを、インターネットサービスプロバイダ（ISP）、通信機器(モデム、ブリッジ、ルータ等)と利用端末で代表させ説明する。

接続タイプ	接続形態
［タイプA］ 利用端末は1台、モデム利用したＰＰＰ接続によるインターネット接続環境	（インターネット）－（ISP）…（DialUp モデム）－（利用端末）
［タイプB］ 利用端末は複数台に増えるが、モデム利用したＰＰＰ接続によるインターネット接続環境はタイプAと同様で、インターネット接続する利用端末は 1 台に限定される環境	(インターネット）－（ISP）…（DialUp モデム）－＋－（利用端末） ……（利用端末） ……（利用端末）
［タイプC］ 回線の常時接続がされ、インターネット接続する利用端末は主に 1 台であるが、たまに他の利用端末も利用できる環境	(インターネット）－（ISP）－（ブリッジ）－＋－（利用端末） …（利用端末） …（利用端末）
［タイプD］ 利用端末間が宅内 LAN 接続され、全ての PC がルータ経由でインターネット接続が可能な環境	(インターネット）－（ISP）－（ルータ）－＋－（利用端末） ＋－（利用端末） ＋－（利用端末）

図 4-3 ホームシステムのネットワーク接続パターン

これらの環境について、端末管理者、端末利用者、ネットワーク管理者、ネットワーク利用者の分担状況とその上でのセキュリティ上の問題点について、簡単に整理する。

タイプＡでは、端末の利用と管理およびネットワークの利用と管理が、全て一人の人間が行うことが殆どであり、そのためセキュリティ上の課題や問題について一元的に認識される。さらにネットワーク回線スピードも遅く、接続時間も極めて短いので、セキュリティ問題が起きても被害の拡大は殆ど無いといってよい。これは一見、セキュリティ上ベストな環境に見えるが、一人の人間の管理手法や技術知識に頼ることになり、本人が承知していれば対策も対症療法で凌げるため、セキュリティ対策はあまり考慮されないことが多い。

タイプ B では、端末の低価格化により家庭における端末の保有台数が増加したケースである。端末利用者は増えるものの、管理者、ネットワーク利用者、ネットワーク管理者は同一であることが多い。ネットワーク利用者を単一としたのは、ネットワークを利用する際はネットワークへの接続している端末を共有するため、その利用に関してその端末の管理者の指導の下に限定的に行われるためである。ここでセキュリティ上増加する問題点は、ネットワークに接続する端末と接続していない端末間での FD やメモリカードといった可搬メディアによってデータ等の相互利用が発生することによるウィルス感染等である。さらに端末管理者が端末毎になることもあり、この場合は端末毎にセキュリティ対策が異なってくる欠点がある一方、逆に複数の利用者によって問題発見の確率が増大する利点もある。

タイプ C は、回線利用料の低価格化によりインターネットへの常時接続が可能となり、全ての端末が切替え装置や手動でのつなぎ変えによってネットワークに接続できるようになる。この場合、端

末利用者と端末管理者とネットワーク利用者が同一人物であるものの複数になる。セキュリティ上増加する問題点は、利用する人によってセキュリティ意識が異なる点がある。但し、ネットワークが必要でない場合は端末は物理的にネットワークから切り離される場合が多いので、回線は常時接続であるものの端末の常時接続はされないので、セキュリティ問題が発生する確率はまだ限定的である。

タイプDは無線アクセスポイント等により一般家庭でもLANの導入が可能となったことによりルーター経由で接続可能となっている先進的なもので、端末は物理的にはネットワークと常時接続されておりサーバー機能の導入等も可能となり企業と同等のシステム構成が可能となっているためセキュリティ上のリスクは極めて高くなる。その上、ルーターやＬANの設置や設定が家庭内のネットワーク管理者ではできないため外部業者によってなされるケースもあり、実態としてネットワーク管理者は不在の状態となり、最悪はセキュリティ上殆ど無法地帯となり得る。

個々のセキュリティ対策について整理すると、ネットワークを利用する際に必要なアクセスIDやパスワードによる認証がタイプAの頃から、まず導入されてきた。但し、これはホームシステムのセキュリティを確保するためというよりは、自らに費用が課せられるISPの不正利用を防止するためであった。次にタイプBになって、一つ屋根の下で端末を利用する能力をもつ人が増えてきたことや家の外で利用できるモバイル端末が登場してきたことで、端末自体を利用するための認証が必要となり、BIOSやOSに認証機能が取られるようになった。ただし、ネットワーク接続が限定的であったため、外部からの進入防止を目的とした認証等は、常時接続が可能となるタイプC，Dの各種機器で取られ始めることが多い。少なくとも、常時接続を前提に設計されたブリッジやルータの設定や修正には認証が必須になっている。一部のブリッジやルータでは、認証に加えて、簡単なFirewall設定ができるものも登場し始め、さらに端末においても簡便な個人向けFirewall機能が、OS内蔵や単独アプリケーション添付等と提供形態は異なるものの、バンドルされているものが登場している。ウィルス対策は、端末単位あるいはISP委託で行われている。現状では端末等にワクチンソフトや不正コンテンツ検出ソフトがバンドルされているものが殆どである。ＯＳやＡＰのパッチ適用によるバグ除去等によるセキュリティホール対策は、現在ではネットワーク経由でリアルタイムに実施できる環境が整備されつつあるものの、その実施は端末単位に利用者が意識して実施しなくてはならないのが実情である。さらに、家電機器やテレビゲーム機においては、未だ訪問修理や引取り修理の扱いでファームウエア交換がなされており、時として有料サービスとして展開されている。

最近はアプケーションの増大により、これまでのメールやWebサーフィンといった単純なインターネット活用に限られないため、パターン化されたセキュリティ対策が難しくなってきている。ゲーム専用機で近年多く利用されるようになったネットワークゲームでは、アプリケーションがグローバルIPを要求することもあり、その場合モデルの設定がインターネットとスルーになっているためセキュリティ対策がされていないことが多い。

ネットワーク家電は、外部からの録画予約や電源の投入切断等のホームコントロールや、冷蔵庫に保管されている材料を前提にレシピの情報を収集し表示する機能等を幅広く提供するため、24時間ネットワーク接続されることが多い。最近では、ホームサーバとネーミングされた情報蓄積、情

報発信機能まで提供されている場合もある。これらの組み合わせを考慮すると、企業毎における完全にカスタマイズされたシステムと同様なセキュリティ対策が、本来必要であるはずが全く施されていない場合が実態である。

最後にホームシステムと企業とのネットワークの利用形態を簡単に比較すると、①情報受信（電子メール受信、Webサーフィン、ダウンロード）→②情報発信（電子メール送信、掲示板書き込み、アップロード）→③情報管理（メールサーバ構築、Webサイト構築、FTPサイト構築）という流れに沿って利用され発展している過程は一緒だが、企業においてはその量的な配分が①＜②＜＜③であるが、家庭では①＞＞②＞③である。扱っている情報は、企業では自社の情報だけでなく、顧客情報や取引先情報まで幅広いが、家庭では主には各個人の情報程度しか扱わない（狭いコミュニテイ程度は多少増加して来ているが）。さらに、その情報を金銭に換算したときは、企業に比べて家庭では小さい額である。特にセキュリティ対策が重要となるタイプCやDにおいて、企業向けでは組織的な取り組みが行われているが、家庭では個人管理に委ねられているのが実情である

4.3.4.2 技術の現状

一般家庭を対象にしたPCやネットワーク周辺機器に実装されるプラットフォームは、その設定において、少なくともパスワードによる認証が必要になってきている。さらにそれらプラットフォームのセキュリティ対策は、各メーカーによりバグフィックスと同様にセキュリティパッチやセキュリティ情報が無償にて提供されることが増えている。家庭向けPCでは、バンドルソフトによって簡単なFirewall機能、ウィルス検出機能（一部ワクチン機能まで提供される場合もある）、ネットワークセキュリティ設定機能、リモートアシスタント機能が提供されることが多くなっており、少なくともPC購入直後は比較的にセキュリティ対策を施せる環境は整ってきている。一方、バンドルソフトウェアはお試し版的な意味合いも強く、サポート期間が短く、自ら選択して購入したのでないため、サポート期間を超過したまま、充分な機能を果たせていないのが実情である。

ホームシステムについては、企業向けに比べてセキュリティに関する技術は、技術ポテンシャルはあるものの、実装レベルでは非常に遅れているのが実態である。特に、セキュリティコンポーネントの小型化、設定・利用に必要な操作や運用の簡易化とサポートフィーを含む低価格化が、まだ充分とは言えない。

ホームシステムのPCを狙って来るハッカーは少ないとはいえ、IPアドレス空間すべてを順次（スキャン）調べて、セキュリティの甘いサイトを探すことは日常的に行われているので、そのような攻撃手法に関して言えば、その対象が企業であることや一般家庭であることは一切関係ないのである。さらに、ホームシステムのPCに重要な情報がないから侵入されても構わないと判断する人がいるかも知れない。しかし、そのPCを踏み台にして、国内外の他のサイトに攻撃を仕掛けられる可能性もあり、例えばDDoS（分散型サービス妨害）攻撃の踏み台になるリスクは決して低いとは言えないのである。攻撃されたサイトにしてみれば、相手が一般家庭であったとしても、「知らなかった」で

は済まされず、何らかの管理責任を問われるケースが出現するのもそう遠い時期ではないであろう。現状では、アクセス制御一つを例にしても、

- root や admin 権限の ID をデフォルトのまま利用（しかもインターネットに接続）
- パスワードを省略、またはログイン ID と同じに設定
- パスワードをメモ用紙に記して PC の側に貼ったり、電子メールで送信したり、
- 外部（特にフリーの）サービスのパスワードを会社で利用するものと同じにしたり、
- 外部からネットワーク共有ができたり、見えるよう設定していたりする

ことが多い。インターネット常時接続のホームシステムを対象にするのであれば、利便性の観点を犠牲にしてでも、自動的に上記の設定を拒否するプラットフォームが求められるのかも知れない。但し、覚えられないパスワードを無理に利用するのは現実的でないため、例えばメモリカードを認証用に利用できるセキュアなインタフェースを策定し、活用するのも良いかもしれない。

さらにホームシステムにおいて、比較的簡単にできるごく基本的なセキュリティ対策として、

- OS や各アプリケーションソフトウェアのバージョンアップまたはセキュリティパッチの適用（既知のセキュリティホールを排除できる）
- Directed Broadcast の禁止（DoS 攻撃の踏み台になることを防止）
- 始点アドレスを詐称したパケットの流入禁止（IP パケット偽造攻撃からの防御）
- 始点アドレスを詐称したパケットの流出禁止（外界への攻撃の抑止）
- 不要なパケットのフィルタリングと不要なネットワークサービスの停止（ネットワークサービスを介した不正アクセスの抑止）
- 電子メールサーバでの第三者中継機能の停止（メール不正中継の抑止）
- アクセスログの記録（異常の早期検出、万が一の場合の分析に備える）

があげられる。これらについても、各メーカーのサポート Web サイトで情報提供は行われているが、利用できるスキルを持つ利用者は一部であるから、メーカーによるリモートお任せアプリケーションや導入・設定自動化ツール等の提供が待たれる。証券・金融用にカスタマイズされたパーソナルコンピュータが限定顧客向けに利用されて入るものの、これらのツールはデファクトと言えるものがまだないため、利便性とのトレードオフになってしまっている。業界間のインタフェースを取ることで、利用者が様々なセキュアサイトに同一のプラットフォームからアクセス可能になることが求められている。

4.3.4.3 今後の課題

ホームシステム向けの PC に対しては、企業向けで一部利用が進んでいるセキュリティ対策を含む運用管理統合ソフトウェアや、一部のメーカーからは既に出荷が開始されているウィルス対策、Firewwall 等のセキュリティ対策パッケージソフトウェアの提供が期待される。個々の個人向けセキュリティ対策ソフトウェアパッケージは、メーカー主導で開発されていることもあり、メーカー間の混在

した利用や、その設定に関する利用者への教育については不足している。今後は、ホームシステムが加害者となりうることを想定して、利用者へのセキュリティ対策への啓蒙活動やソフトウェア更新等が義務化されるような車検のような仕組みと共に、メーカーサイドにもGUIや設定方法の共通化やパッケージソフトウェアインタフェースの公開や標準化が望まれる。

さらに、ネット家電やゲーム専用機についても、PC同様セキュリティ対策を充分に継続的に施せるような仕組みを搭載することや、様々な組み合わせで利用されることを想定したサポート体制が望まれる。但し、そのためには必要となる費用が肥大化してしまうため、セキュリティ対策の切り口から企業フォーラムや協議会を作成し、対策に必要となる費用を分担することや、第三者によるセキュリティ評価を受けられる仕組みづくりも必要となろう。

他方、ネットワークプラットフォームとして、IPレベルでセキュリティ対策が想定されているIPv6のISPやメーカーへの普及促進や、将来の主たる利用者になる子供への情報教育にセキュリティ課題や対策について追加していることも社会に望まれる。

同時に家電製品において、動作設定によっては、人はむろんのこと保有資産への物理的な危険を与え兼ねないので、パーソナルコンピュータにおけるサイバー対策だけでなく、これまで同様製造物責任の観点に立って、例えばISO15408の用にファームウエアや実装方法を含めた第三者によるセキュリティ認証を持った製品でないと、インターネットへの常時接続をできないようにする規格やルールが、技術的な検討に立脚して切望されるのは時間の問題であろう。

こうした具体的な対策だけでなく現在企業にて利用され始めている、ISMSのようなセキュリティマネジメント手法を取り入れ継続的なセキュリティ対策が、簡便なものでもよいのでとられることが望ましい。ベストなのは家庭における利用者がセキュリティ上の危険を理解したうえで使用するのが望ましいが、他にも例えば、家庭が利用するISPがチェック項目やセキュリティセッティングチェックやウィルスチェックのオプションサービスを用意し、リモートから提供されるものを利用するだけでも良い。インターネット社会は、自己責任の社会であると言われているが、個人と社会、個人のメーカー、メーカーと社会でどのように分担していくべきか、歩み寄りを前提にした対策が、リアルの社会秩序と同様、技術者だけでなく各方面の専門家や消費者団体を含めて検討されることが望ましい。

4.3.5 ネットワーク処理の追跡にかかる技術

ネットワークにおけるサービスにおいて、最大の利点であり、かつ最大の問題点は、いわゆる「顔を見せずに」サービスを利用できることにある。これは、ネットワーク上の不正行為や迷惑行為を行っている主体、すなわちコンピュータ等の端末、および行為者の特定を困難なものにしている。

以下、これらの特定を「攻撃の特定」と呼ぶ。攻撃を特定することによって、責任を明確化することが可能となり、損害賠償等の手続きを遂行することが容易になる。また攻撃の多くが過去の攻撃事例等を参考にした稚拙な模倣犯的攻撃がほとんどであり、「顔が見えない」というネットワークの安易な理解から起こされる。したがって、攻撃の特定が可能となることによって大きな抑止効果を期

待できる。

正当な利用者は、利用者自身の個人の特定されることにそうこだわるわけではなうが、攻撃では積極的に、攻撃者および利用端末の特定およびその経路を秘匿する手段をとる。したがってそれらの手段に対抗しえる技術を開発、運用することが必要となる。

具体的な技術開発テーマとしては、以下があげられる。

- サーバ、およびネットワーク上でのログ解析技術
- ネットワーク上での攻撃追跡技術
- 追跡におけるサーバおよびルータ連携技術およびその標準化

4.3.5.1 ネットワーク上での追跡にかかる技術のテーマ

攻撃者およびその利用端末を特定するためには、次の技術開発テーマとしては、以下があげられる。

(1) サーバ、およびネットワーク上でのログ解析技術

攻撃に対する認知は、CPUおよびファイル容量等の資源の不正な消費、ファイルの改ざん等であるが、閲覧権限のない攻撃者の不正なファイル閲覧、パスワード使用等を検出するためにはログの解析が重要である。またログには時間、利用した資源、コマンドおよび経路に関する情報、そして使用した権限の所有者に関する情報が記載されている。しかしながら、大量に生成されるログから、攻撃に結びつくログ、あるいは検索対象となる攻撃に関係するログを抽出することは必ずしも容易ではない。また、ログを抽出できたとしても、そのログが攻撃に関してどのような関係があるか、どのような結果を導出するか、さらに前後のログとの関係と明確化する必要がある。

(2) ネットワーク上での攻撃追跡技術

攻撃が認知された場合、その攻撃に関係するログを参考に攻撃者、および攻撃に利用した端末の特定を行う必要がある。すなわち、その攻撃を可能にした経路を特定する必要がある。また、直接ログを利用するのではなく、リアルタイムの攻撃に対して、その攻撃を可能ならしめるパケットを攻撃対象のネットワーク、さらにはサーバおよび端末が存在するLANを超えて追跡する技術が必要である。

(3) 追跡におけるサーバおよびルータ連携技術およびその標準化

上述のように、自ネットワークを超えて攻撃に関係するパケットを追跡する必要がある。その場合、各ネットワークの連携が必須である。多くの場合、自ネットワークを超えてパケットを追跡することによって、自ネットワーク外での攻撃に対する情報が不足し、効率的な追跡が不可能となる。このためネットワーク相互の連携および攻撃情報の相互共有、ならびにその標準化が必要である。

(4) 広域ネットワークにおけるセンサー構成およびその情報収集技術

LGWAN等に代表される広域ネットワークにおいては、事実上ＬＡＮの集合体を形成しているものの、その広域ネットワーク全体を統一的に管理することが可能である。したがって、サーバやルータの連携以上に、攻撃に対する情報を共有および効率的に利用することが可能となる。特に、センサと呼ばれる攻撃情報を収集する装置の開発、運用、複数のセンサーの連携技術、その情報解析等の技術がある。

4.3.5.2 現在の技術水準と取り組み状況

攻撃者を追跡し、かつ特定することは容易ではなく、悪意を持った卓越した技術を有する攻撃者に対しては、ほとんどその特定が困難である。しかしながら、研究においては着実に進歩しており、実験段階での成果も報告されつつある。

(1) サーバ、およびネットワーク上でのログ解析技術

大量のログから、探索対象となる攻撃に関するログを抽出する技術は完全ではないものの存在し、実システムとして稼動している。しかしながら、単純なパターンマッチングによる語彙検索であり、過去の攻撃事例から類推して、攻撃に関係するログを抽出する方法である。

(2) ネットワーク上での攻撃追跡技術

実験的なシステムとしてはいくつかの提案がなされ、試験運用が行われている。しかしながら、ネットワークを越えての追跡はややもすれば相手のネットワークに対する攻撃となりうる、あるいはみなされることから実現には難しい技術となっている。さらに、「ハニーポット」と呼ばれる技術が存在する。これは、攻撃者を欺き、あらかじめ攻撃に対する対策および攻撃者の情報を得るためのトラップを仕掛けた特別なサーバに誘い込み、攻撃者を特定する技術である。

(3) 追跡におけるサーバおよびルータ連携技術およびその標準化

現状では、その必要性と概念の提案はなされているものの具体的な技術開発および標準化は行われていない。しかしながら、ＩＤＳ（侵入検知装置）のシグネチャ、いわゆる攻撃パターンのデータベースについては標準化の動きがあり、ネットワークを越えてのＩＤＳの連携によって、攻撃を特定することの可能性について研究が行われようとしている。

(4) 広域ネットワークにおけるセンサ構成およびその情報収集技術

現在、研究開発段階であり、概念の提案が成されているに留まり、今後の研究成果が待たれる。

4.3.5.3　今後の課題

追跡、すなわち攻撃の特定に関しては総じて、現実的に大きな効果を有するシステムは開発段階であり、実システムとして稼動していない。厳密には、攻撃に対する追跡、特にリアルタイムでの追跡と、事後のログによる足跡の追跡は自ネットワークを超えて、情報を収集することになり、場合によっては、そのネットワークに対する不正行為と見なされる危険性がある。ネットワークを越えての攻撃に対する情報交換の枠組み作り、標準化が待たれる。また広域ネットワークでは、センサーという攻撃に対する情報を収集する機器を効率的に分散し、そのセンサーからの情報を集中管理的に解析し、攻撃の特定を行う方式が提案されている。しかしながら十分なセンサーの安全性の保証、認証、集中管理するセキュリティ管理サーバの安全性の保証等の問題が残されている。さらにログの抽出および解析は、過去の攻撃パターンを記録した攻撃データベースに基づいて、パターンマッチングによりログを抽出し、その攻撃の可能性を検証している。したがって、データベースに存在しない攻撃方法については無力である。したがって、ログから過去の攻撃方法に依存しない、すなわち未知の攻撃を類推しえる解析方法の研究開発が望まれる。また、ログについても単体のサーバのログに対する解析に留まっている。複数のサーバ間でのログを有機的に結合した解析によって攻撃およびその特定を行う技術開発が待たれる。

これからのサービスやシステムの主流となる複数のベンダーがかかわるシステムにおけるとらぶへの対応の迅速化や、責任の明確化のためには、このようなシステムにあっても、トラブルを発生させたところが特定できるようになっていなければならない。このためには、以下のような技術の整備が必要となる。

- システム構築技術の高度化
- システム構成要素個々に対するこの点に関する標準要件の確立
- ネットワーク上での処理の追跡技術

トラブルが生じたときその原因を追求し、再発の防止が図られなければならない。特に、ネットワーク社会において大きな脅威となる攻撃者に対する牽制のためには、攻撃者の特定できなければならない。このため、攻撃者の特定は、個々のシステムだけでは困難であり、ネットワーク全体としての対応が必要となる。このために、開発が求められる技術としては、以下が上げられる。

4.3.6　不法行為、迷惑行為の抑止にかかる技術

ネットワーク上では明確な不正行為には至らないが、故意の有無に依らずネットワークやサーバにとって不都合な行為、さらにその個々の利用者にとって迷惑となる行為が存在する。たとえば、ジャンクメールやスパムメールと行ったユーザが望まないメールの配信、ネットワーク、サーバへの過負荷、ならびに誹謗中傷、風説の流布等が上げられる。これらは違法か否かの判断が困難であり、積極的な排除は難しい。しかしながらネットワークや利用者にとって不快感を与えるものであり、

適切に除去、あるいは防御する必要がある。特に誹謗中傷、風説の流布は企業や組織、そして個人の信用を著しく損なう可能性があり、業務や株価等、その波及効果は小さくない。また、スパイウェアに代表されるように、コンピュータの内部の情報を許可なく特定のサイトに発信する仕組みを無意識に利用する場合もある。通常、クッキーと呼ばれるインターネットブラウザにおいての、サーバとクライアントの間での情報共有の仕組みを利用して、不正に利用者の許可なく情報をサーバ側に送ることが多い。場合によっては、利用者の個人情報が送られてしまう場合もないとは言えない。

4.3.6.1 不正行為、迷惑行為の抑止にかかる技術テーマ

(1) メール配信の拒否機能に関わる技術

何らかの方法でアドレスを収集し、不快なメールを送られる場合がある。これらはジャンクメール、あるいはスパムメールと呼ばれるが、配信先を特定し、確実に拒否することは現実問題として困難である。したがって、ユーザ自身がメールを自動的に廃棄する、もしくはメールサーバを有する組織、プロバイダがユーザの要請に応じて自動的に廃棄する技術が必要となってきている。

(2) ネットワーク、およびサーバ監視に関わる技術

ユーザの不注意やプログラムのバグ、システムの予期しない故障等によって、ネットワークやサーバに多大の負荷がかかり、正常なサービスを滞らせる場合がある。また、無意識に大量のメール、もしくは大容量の添付ファイルを含むメールを送信する場合もあり、場合によってはサーバの正常な動作を妨げる場合がある。これらの事象について事前に対策を立てるだけでなく、被害を未然に防ぐ技術、あるいは最小限に被害を止める技術が必要である。

(3) 不正情報流出に関わるクライアント監視技術

不正なクッキーの利用等、ユーザが予期しない情報流出が起こる場合もある。ID 番号やパスワード等の個人情報の流出は致命的であるが、ユーザの履歴や使用するソフトウェアのバージョン等の情報の流出も好ましいものではない。これらに対してどのような情報がどこへ流出しているかを認識することは重要である。

(4) 誹謗中傷、および風説の流布対策に関する技術

ホームページや掲示板等に誹謗中傷を書かれる事は企業や個人にとって大きなマイナスである。これらは風説の流布といわれるが、誹謗中傷に関してはいち早く発見し、対策を講じることが肝要である。誹謗中傷に関しては、それを事前に防ぐことは困難であり、いち早く発見することによって、その掲示板やホームページへの削除要求、法的処置を取ることが可能であり、特にその拡散を最小限に抑えることが出来る。

4.3.6.2 現在の技術水準

(1) メール配信の拒否機能に関わる技術

メールサーバを運用管理するレベル、たとえばプロバイダ等では、スパムメールやジャンクメールを排除する方法として、一定時間に大量のあて先に向けて送る、あるいは標題が欠如しているメール等について配送制限をする等の処置が取られる。しかしながら、スパムメールと通常のメールを判別することは難しく、厳格に運用することは不可能である。メールを送受する端末側（ユーザ）にとっては、特定のアドレス、あるいは標題に特定の語句が含まれるメールを拒否することが可能であり、ユーザからの申請によって、プロバイダ等でその処置を行うサービスも存在する。

(2) ネットワーク、およびサーバ監視に関わる技術

ネットワークの状態を常にモニターして、不正行為が行われていないかを診断することは、IDS（侵入検知装置）がその役割を担っている。また、そのモニター状況によって、サーバを停止したり、クライアントのネットワーク接続を切断することも可能である。

(3) 不正情報流出に関わるクライアント監視技術

スパイウェアによる不正なクッキー情報の流出や不正なポート使用による情報流出を検知するソフトウェアはすでに存在している。しかしながら、ユーザを欺いて、正規の通信との区別のつかない方法で情報の送受を行うプログラムを仕掛ける場合があり、その発見は難しい。

(4) 誹謗中傷、および風説の流布対策に関する技術

誹謗中傷を発見する技術は、基本的にインターネットの検索技術に負うところが大きい。すでにインターネット上に存在する企業や組織に対する誹謗中傷を発見し、通報するサービスは始まっている。しかしながら、クライアントが指定する数個のキーワードを元に、既存の検索エンジンやサービス会社がデータベースとして有している誹謗中傷が多発する掲示板やURLを定期的に巡回検索し、毎日数回にわたってその報告をメールやWEBに送る程度である。

4.3.6.3 取組み状況と今後の課題

(1) メール配信の拒否機能に関わる技術

メールサーバを運営管理する組織において、スパムメールやジャンクメールを判別、検知する技術の開発が希求される。通常、スパムメールはネットワークを超えて大量にメールが送信されることから、ネットワークを越えたメールサーバ同士が連携し、ネットワーク機能を妨害するメールについて早期に検出し、配送制限を行う等の処置をとるシステムの開発が待たれる。同様にチェーンメール（無限連鎖メール）に関しての処置も可能となる。

根本的な問題として、ジャンクメールと通常のメールの判別が問題となる。この問題は非常に難しいが、ユーザ個人に特定した場合、ユーザのメールに関する感情を自己学習し、ジャ

ンクメールを排除、あるいは目に触れさせないことも技術的には可能であろう。

(2) ネットワーク、およびサーバ監視に関わる技術

ネットワークやサーバの稼動状態の監視の問題は、ネットワークセキュリティの根本的な問題である。しかしながら、ネットワーク管理者が必ずしも容易に監視やそれに基づく適切な処理を行うシステムは開発段階である。現在ではネットワーク管理者自身のスキルに負うところが大きい。今後は必ずしもスキルの高くない管理者が容易にネットワークおよびサーバを監視、および処置を行う、いわゆる管理システムの開発、あるいは監視を外部に依頼することが可能になる標準システムの開発が待たれる。

(3) 不正情報流出に関わるクライアント監視技術

クライアント監視もネットワーク監視の一部であり、クライアントの特性に応じた監視が考えられる。クライアントが通常アクセスしないサイトへのアクセスや定期的に送信されるパケットについては注意を喚起する必要があり、クライアントの挙動を分析して、不審な行動に関しては警告をする、あるいは報告を行う等のサービスが期待される。

(4) 誹謗中傷、および風説の流布対策に関する技術

風説の流布対策に必要な技術として、従来の検索エンジンにない、リアルタイム性を重視した、すなわちインターネット上に掲載された情報を出来る限り早く検出する技術と、誹謗中傷にあたると判断される記事を識別する技術である。

4.4 システムのセキュリティを確保するためのツールの現状と課題

4.4.1 ＯＳを堅牢にする技術

現在、ＯＳのネットワークに対するセキュリティについては問題視されている反面で、脆弱なものであるとの認識が一般的であり、その脆弱性が事実上容認されているのが現実である。組織内のネットワークをインターネットと接続する際に、ファイアウォールを必須とする根拠も、そこにある。セキュアＯＳ技術は、ＯＳそのもののセキュリティを堅牢なものとするために用いる技術である。

4.4.1.1 セキュアＯＳ技術のテーマ

セキュアＯＳ技術のテーマとしては、ネットワークサービスや、アプリケーション、および操作者による故意や過失の問題に対して、ＯＳとしてその資源を保護することである。ただし、セキュアＯＳ技術が十分なものになったとしても、ファイアウォールの設置等の従来からのセキュリティ対策が不必要になるわけではない。セキュアOSは、他のセキュリティ対策を補完し、さらなる被害を食い止めることに寄与するものである。

4.4.1.2　現在の技術水準

セキュアＯＳは、３つの世代に大別できる。第１世代としての Trusted OS、第２世代としての CMW OS、第 3世代としての Secure OS である。第３世代は、まさに始まったばかりであり広く認知された呼称がないため、ここでは、総称であるセキュアＯＳと同じ呼び方で紹介する。

第 1世代の Trusted OS は、1980 年代に米国防総省がコンピュータの調達要件仕様書として制定した、TCSEC (Trusted Computer Security Evaluation Criteria :通称、オレンジブック) により定めた、コンピュータのセキュリティ強度４段階（AからD）のうち、上から２段階目である、Ｂレベル以上の強度を有すると認証されたコンピュータをいう。Trusted OS には公式の認証制度に基づく技術保証が得られる。Trusted OS については、認証制度で、公式に認証を取得している場合(certified)と、開発元がそのとおりに開発したと宣言している、準拠(compliance)とがある。当初の認証制度そのものは、1990 年代に発展解消し、現在は、Common Criteria として継承されている。また、これに基づく国際標準が、ISO/IEC 15408 であり、国内では、JIS X 5070 として JIS 化が 2001 年に完了している。Trusted OS の仕様は、スタンドアロンのコンピュータを想定したものであり、ネットワーク接続については、別の仕様（通称、レッドブック）で定めているが、ホスト型の通信装置を想定したものである。

第 2世代の CMW OS は、1990 年代に米国海軍が海軍としての調達要件仕様として策定したもので、Compartmented Mode Workstation の略である。CMW は、その中で TCSEC のＢレベルを要件のひとつとして定めている。CMW 全体としての認証制度はなく、調達により個別に検査を実施する。CMW は、Ｂレベルに加えて、ネットワークを想定した要件の他、グラフィック端末でのマルチウインドウ機能など、クライアント端末としてＯＳを実行していることを想定したものになっている。技術的にもっとも異なる点は、Trusted OS が保護する情報を重要度という縦方向の高低だけで区別するのに対して、CMW は種別という横方向の区分(compartment)を設けていることである。Unix などのオープンシステムは、TCSEC のＢレベルだけではなく、CMW の要件に合わせて開発されている。CMW による調達で最初に採用されたのは、HP 社の Trusted HP-UX であるが、応札するために、IBM 社の Trusted AIX、Sun Microsystems 社の Trusted Solaris など米国のコンピュータベンダーのほとんどが、自社のＯＳの Trusted 版を開発している。これらの CMW 仕様のＯＳを市場では、Trusted OS と呼んでいることが多いため混乱することが考えられるが、正確には CMW OS は、Trusted OS にセキュリティの追加の要件を加えたものである。

CMW OS は 1996 年まで、軍用に使われるだけであったが、米国でインターネットバンキングを開始するにあたって、インターネットからネットワークサービスを直接受け付けるＯＳとして採用されたことで、民間の商用に使われ始めた。Trusted OS ではなく、CMW OS が採用されたのは、インターネット側のコンピュータ資源と、内部ネットワーク側の資源を、横方向の区分として分離して、外部と内部を遮蔽することにより、セキュリティ侵害を防止する設計に供するためであった。そのように設計することで、本来、ＯＳが直接管理するユーザに対する情報保護技術であった機能を、サーバとして内外を分離するということにも活用できるようになった。すなわち、クライアントＯＳとしてだけ

ではなく、ネットワークにサービスを提供するサーバＯＳとしても有効活用されるようになった。

近年では、2002 年に、米国 NSA が Security Enhanced Linux を開発し、オープンソースとして公開している。こちらは、CMW 要件をすべて満たすものではないが、重要度に横方向の区分を有する Trusted OS である。

4.4.1.3 取組状況と今後の課題

セキュアＯＳを活用する場合、それがクライアントとしてのものか、サーバとしてのものかを分けて考えることが重要である。現在でも軍用などでは、すべてのワークステーションのクライアントOSをCMW OS として使用することで、情報保護を堅牢なものにしている。今後、民間でもそのような利用の仕方も考えられようが、当面は、クライアントサーバ型のアプリケーションモデルにおいて、サーバ側だけでセキュアＯＳを導入することが現実的と思われる。

また Trusted OS や CMW OS の設計は、以下を前提としている。

⑴セキュリティは最重要の課題であり厳格なセキュリティポリシーが絶対である

⑵ＯＳがユーザ管理を直接行ない、ユーザによる情報のアクセス制御を強制する

⑶セキュリティ要件に基づき、アプリケーションを独自開発する

⑷情報の漏えいを防ぐため、データフローを一方向に限定して閉じ込める

これらの設計思想について、近年、あるいは、商用で使用する場合の考察を以下に行なう。

⑴については、たとえば、ディスク装置の物理的な取り外しに備えて、当該のＯＳ以外に接続しても内容を読み取ることができないようになっている。このことは、コンピュータ本体が故障した際に、ディスク装置の内容だけを他から読み出すことができないことを意味する。データのバックアップに対して正しい運用が行なわれていないと、原本であるディスク装置があったとしても、データを復旧できないことになる。軍用の場合、重要な情報が漏えいするくらいであれば、読み出せなくなることを優先するというセキュリティポリシーでもよいが、商用においては、厳しすぎるものと考えられる。

⑵については、クライアントサーバ型のアプリケーションモデルでは、ユーザの管理は、アプリケーションが行なっておりＯＳではないため、Trusted OS による情報保護は一次的には役立たない場合が多いと考えられる。

⑶については、市販アプリケーションや既存のソフトウェアツールを多く導入する前提では、制限の多いものとなることが考えられる。

⑷情報を単に閉じ込めるだけではなく、情報を活用するという商用環境においては、情報の流れを一方向に限定するような制約を設計に与えることは、適用できるシステムを極端に少なくするものと考えられる。

以上のようなことから、セキュアＯＳ技術は、第３世代の必要に迫られている。そこでの課題としては、以下のような ものがあげられる。

- 設計者の責任において、セキュリティの要件とその他の要件とのバランスに基づいたセキュリティポリシーを採用できるような柔軟性。
- アプリケーションサーバとして用いられる場合にも活用できる、セキュリティ主体を想定した柔軟性。
- 既存のアプリケーション、ソースコードを有さないアプリケーションに対して、ＯＳがセキュリティ要件を適応できるような柔軟性。
- アプリケーションの要件を満たすような、データフローに適応しつつ、アクセス制御を堅牢にするような柔軟性。
- 標準ＯＳとの互換性をより多く保つことで、開発工数を削減し、安価に利用できるようになること。

これらの条件を満たすようなものを、第 3世代のセキュア OS として提供されることが期待される。

4.4.2 システム上の情報の保護にかかる技術

情報は、システム上に格納されていたり、ネットワーク上を流れるメッセージの上にも、CD や FD 等のリムーバブルな電磁媒体上にも存在する。また、印刷物の中にも存在する。情報を不正取得や改ざんや破壊から守る保護は、それがどこにあろうとも、保護対象となる情報の保護要件に応じて行われなければならないが、保護の具体策はその存在場所によって異なってくる。

ここでは、システムまたは電磁媒体記録上に格納された情報の保護についての技術課題についての考察を述べる。

4.4.2.1 システム上の情報の保護にかかる技術のテーマ

システム上の情報の保護と言う観点から見ると、現在、システムで一般に用いられて情報へのアクセス制御では、きめの細かい情報の保護ができないと言わざるをえない。これは、RDBMS（リレーショナルデータベース）における“表”やビュー（仮想表）“と呼ばれるシステムにおける情報のアクセス単位に異なるセキュリティ特性（保護要件の異なる）情報が混在しているため、一般に用いられているアクセス制御では、保護はセキュリティ特性の最も低いところに合わされることによる。

問題は、システム上の情報を保護する上で、認証の次の段階として問題になるのが「認可」（認証されたユーザがどの情報に対してどのような権限を持っているか）をアクセス制限要件定義に従ってどのように実行するかである。不正アクセス防止の見地から考えた場合、各ユーザがその業務において必要とする最小限の権限を付与し、不要な権限は一切与えないという“最小権限の原則”を徹底させることが必要となる。通常、同一ファイル内に格納されている各種のデータにおいてもそれぞれ情報として異なった属性や機密性を持つため、これら細分化された各情報単位での分類・

保護管理要件の策定とそれに基づいたアクセス制限の施行が重要である。

例えば、同一のファイル内に氏名・電話番号・クレジットカード番号の情報が存在した場合当然クレジットカード番号が最も高い機密性を持ち、より高いレベルで保護されていなければならない。このような状況から、保護すべき情報の単位は従来の物理ファイル単位からファイル内に格納されている各情報の単位にまで細分化していくことが必要である。

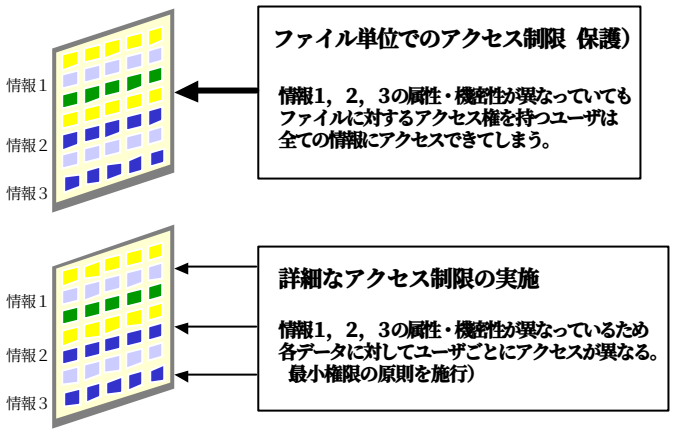


図 4-4 情報へのアクセス制限のイメージ

4.4.2.2 現在の技術水準

(1) ファイル単位でのアクセス制限技術

現在アクセス制限を施行するための技術的な手法としては①OS の機能を利用、②）アプリケーションで制御を実施、③制御用の専用ソフトウエアを導入等が存在する。現在物理的ファイルの単位では、読みとり、書き込み、削除などの基本的な操作のほか、専用ソフトウエアにおいては印刷やコピー、カット&ペーストなどを含めた詳細な制御が可能となっている。これらはファイル内部に格納された個々のデータに対しての制御は実現できていない。

(2) RDBMS における詳細なアクセス制限

RDBMS（リレーショナルデータベース）を用いてデータを格納する場合、一般的にデータを管理する単位である“表”や“ビュー”（仮想表）といった単位でユーザに対して各種のアクセス制限を施行することができる。また表・ビューの構造についても柔軟な構成が可能なため、設計段階で機密性の高いデータを隠蔽するような設計を行うこともできる。

これらの手法を用いたとしても同一の表内に格納されているデータに対しては一律に同じ権限の設定しかできないのが一般的であるが、一部の製品ではさらに詳細な権限設定・アクセス制限を施行できるような独自機能を備えたものもある。

オラクル社の Oracle9*i* Database では表を構成する“行”レベルでのアクセス制限を実現しており、さらに各データの属性・機密性を“ラベル”に置き換えて制御を行う Label Based Access Control を用いたオプション“Oracle Label Security”も用意されている。Label Based Access Control は従来セキュア OS、トラステッド OS 等におけるアクセス制御で用いられていることが多い技術であり、大規模かつ複雑なアクセス制限を行う場合に有効である。米国においてその多くは国防・政府関連組織等で使われており、近年では医療機関で使われている例もみられる。

これらの機能を用いると従来よりもデータベース内の構造を単純化しながら同時に詳細なアクセス制限を実施できる。またアプリケーションでこれらを実現した場合、当該アプリケーションを経由しないアクセスに対しては無防備となってしまう（回避される可能性が残る）のに比べ、より確実にアクセス制御を施行できるという優位性も生まれる。

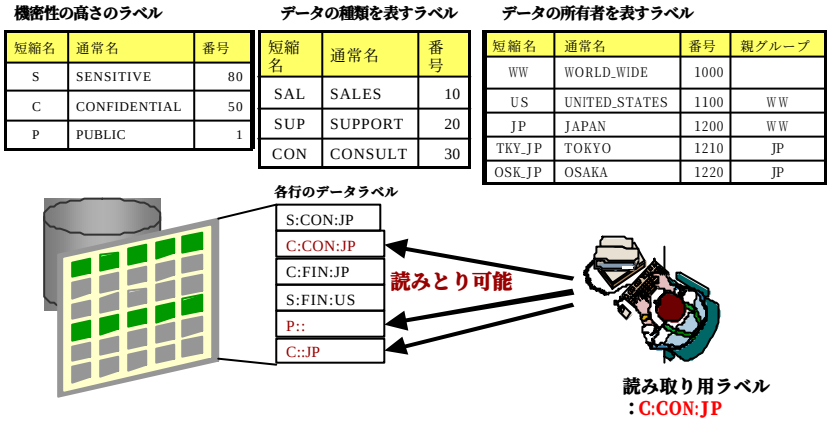


図 4-5 Label Based Access Control のイメージ

4.4.2.3 現在の取り組み状況と今後の課題

(1) 権限情報の管理方法

システムの規模が大きくなり、ユーザ数が増大するほどユーザの権限情報をどのように一元的に管理するかが大きな課題となる。従来のシステムでは権限情報が分散して存在していたため運用に大きなコストがかかる場合があり、結果的に最小権限の原則を施行できない現実的な原因にもなっている。

今後は前述の詳細なアクセス制限を実現するための管理手法として権限情報をディレクトリ・サーバに格納し一元的に管理する方法が求められていくと考えられる。

(2) さらに詳細な単位でのアクセス制限

RDBMS においては一部の製品で行レベルまでのアクセス制限を実現しているが、今後更に“列”レベルでのアクセス制御を実現し更に詳細な単位（“レコード”）でのアクセス制限を実

現する必要がある。

(3) 認証技術・シングルサインオンとの連携

近年バイオメトリクスやスマートカード等のユーザ認証技術や、Web アプリケーションに対するシングルサインオン技術は急速に進歩しているが、ここで述べたアクセス制御技術との統合・連携が実現されているシステムはまだきわめて少ない。今後はパスワード以外の認証技術によって認証されたユーザに対して一元的にシングルサインオン・詳細なアクセス制限の適用などを連携して行うシステムの構築が求められる課題と考えられる。

上記の 3点については現在各ベンダーが鋭意取り組んでいるものであり今後の製品化等が期待される。

4.5 情報セキュリティを支える基盤技術の現状と課題

4.5.1 通信の保護技術についての課題

通信の保護技術については、いろいろな観点があるが、現在問題となっているのは無線系の通信路である。有線、無線を問わず、通信の秘密を保護するための技術や運用の重要性は広く認識され、実際にも適用されているが、無線通信路は基本的に傍受ができるので、何らかの対処がされていなければ、簡単に盗聴が行えるという特性を持っている。

無線系の伝送路で実用的に利用されているものの代表として、いわゆるキャリア系の提供する携帯電話系の伝送路と、802.11 に代表される無線LAN と呼ばれるネットワーク系の伝送路がある。これらは、ステートフル/ステートレス、クローズ/オープンなどの対になるキーワードで表現できるように、まったく異なる世界を持っているが、携帯電話系もTCP/IP の世界に移行する動きもあり、ここでは主に 802.11 系の無線 LAN に関わる問題について述べる。

4.5.1.1 無線 LAN 通信の保護について

通信の保護技術のテーマとして無線系通信路で一番重要な点は、傍受に対する耐性である。何時でも誰でも盗聴ができる状況で、通信の秘密を確保することが求められる。これを実現するには、暗号技術が不可欠である。暗号技術もいろいろな対応方法が考えられる。

- 伝送路自体を暗号化する
- 伝送路上の通信プロトコルレベルで暗号化する
- 動作するアプリケーションレベルで暗号化する

これらにはそれぞれ特徴があるので、実際には利用する要求仕様によって選択されることになる。伝送路自体を暗号化する方式は、基本的にシステム全体をひとつのアルゴリズムで暗号化する集

中方式となり、電話などのキャリア系で実現されているが、システム全体が統制されて動作する必要があり、鍵の管理も基本的には集中管理となるなど、大掛かりな設備が必要になってくる。

802.11 系の無線 LAN では、通信プロトコルやアプリケーションレベルでの暗号化で対応されている。ただし、これらの標準化はまだ発展途上であり、現時点ではいろいろ問題を含んでいるのは事実である。これらをどのように回避し、早期に便利な機能を積極的に利用するとともに、今後の技術の進化や標準化の発展に対応していくかが、現時点の大きなテーマであろう。

4.5.1.2 無線 LAN の保護についての取組みの現状と課題

現時点では無線 LAN に対する安全な通信を行う手段として、次のような方法が使われている。

- WEP (Wired Equivalent Privacy)による通信の暗号化
- MAC (Media Access Control)アドレスによるクライアント機器の選択制限
- AP (Access Point)が送信するビーコンの抑制
- AP が送信するビーコン中に書かれるSSID の抑制
- SSID が ANY に設定されたクライアントからの接続禁止

一番ポピュラーなのは、WEP による方法だが、これも秘密鍵暗号方式として RC4 (Ron's Code 4)を使っており、キー長が40 ビットや 104 ビットでも、脆弱性によりそのキー長が本来持っている強度より小さい強度しか発揮できていない。ICMP パケットや IP ヘッダの IV (Initial Vector)を探してある程度の量のパケットをモニターしていると、元のキー情報を割に簡単に類推することができ、本来の暗号強度を保てないという問題点が指摘されている。

無線 LAN の安全性を高める試みとして、通信路の暗号化とともに、許可された人間だけが利用できるようにする認証技術も重要な位置づけとなる。認証に関する標準化は IEEE 802.1X (Port-Based Network Access Control)として現在検討されており、IEEE 802.11 の端末とアクセスポイント間の論理的ポート接続や、IEEE 802.1D での端末とスイッチ間相対の物理的ポート接続でのデバイス認証に関する規定している。IEEE 802.1X では、端末とアクセスポイント間での PPP 認証を拡張し、いろいろな認証方式(EAP-Type)を追加できるので、例えば RADIUS による認証が利用できるようになる。EAP は RFC2284 (PPP Extensible Authentication Protocol)で規格化されているが、PPP、IEEE 802.3、IEEE 802.5、IEEE 802.11 で EAP over LAN として代表的なものには下記のようなものがある。

- EAP-MD5
- EAP-LEAP (シスコシステムズ社の独自規格)
- EAP-TLS (Transport Layer Security) RFC2716
- EAP-TTLS (Tunneled Transport Layer Security)
- PEAP (Protected EAP Protocol) RFC2246

EAP-MD5 と EAP-LEAP ではパスワードを使った認証を行い、それ以外は公開暗号鍵方式の PKI を利用している。IEEE 801.1X を利用するには、別に RADIUS サーバが必要になる。EAP-TLS はサーバ、端末双方で電子証明書を用いた認証を行うので安全性は高いが、ユーザごとに証明書が必要になるので、証明局を用意する必要がある。TTLS、PEAP は、サーバ認証のみ証明書を使うが、園とは TLS トンネルでPAP、MS-CHAP のパスワード認証を行うので、ユーザ証明書は不要である。

この他に、IEEEE の 802.11i WG で RSN (Robust Security Network)というセキュリティ機能を強化した新しい規格が検討されている。ここでは、IEEEE 802.1X での認証に加えて、暗号化方式も追加されている。

- TKIP (Temporal Key Integrity Protocol)
- CCMP (Counter-Mode/CBC-MAC Protocol)
- WARP (Wireless Robust Authenticated Protocol)

IEEE 802.11i の標準化が遅れているのに対して、2002 年 10 月に無線 LAN ベンダー団体の WiFi Alliance が、認証 WiFi というIEEE 802.11i の TKIP とIEEE 802.1X の機能を実装する WPA (Wireless Protected Access)を発表した。TRIP は、既存の無線 LAN カードのファームウエアをアップデートすることにより対応できるとされている。WARP は AES を採用しているが、CCMP、WARP ともに既存の無線 LAN カードでは対応できない。

このように、無線 LAN を安全に使うための、技術的な開発、標準化への反映は着々と実行されて入るが、まだ統一されているわけではない。ただし、現時点での問題点を踏まえて、十分利用することができるのも事実である。賢く安全に便利に夢全 LAN を使おうという意識と知恵が今求められているといえる。

5　システムの安全性の向上に必要な取組み

ネットを介したサービスやネットを利用するシステムは、その利用が利用者にとって脅威になったり、サービスの提供が提供者にリスクを生じたりしないようなものでなければならない。このことが実現されるようにするためには、ネットを介して利用されるシステムの安全性の追求だけでなく、利用者のサービスやシステムの利用における安全の向上のためのサービスやシステムの提供についての工夫も必要となる。

システムの安全性とは、システムが当該システムに要求される正確性、可用性、秘匿性の達成度を言う。

5.1　システムの安全性の向上に向けた必要な取組み

システムの安全性は、システムの安全性確保のための諸施策が、当該システムに要求される安全性についての要求に十分に対応できているかどうかにかかる。システムの安全性を確保するための諸施策は、技術面、設備面、マネジメント面、および関与する人的側面の多くの面からの対策が必要であり、また、その一つ一つにも要求事項が多岐にわたるため、その実施に不備をなくすことはなかなか難しい。そして、この不備がシステムの安全性に思わぬ問題を生じさせることに結びつく。

このため、システムの安全性の向上には、以下のような施策が必要となる。

- システムに実施している安全性確保のための諸施策の十分性を評価し、実施上の不備の発見に結びつくようなシステムの安全性評価モデルの確立
- 実施すべき安全性の確保のための諸施策を具体的に示すシステム種別ごとのセキュリティ対策プロファイルの確立
- システム種別ごとに必要とされる安全性のレベルを示す安全性基準の確立
- 個別システムの安全性評価認証サービスの導入
- サービスやシステムを提供する事業者における情報セキュリティ対応能力の向上

5.1.1　システムの安全性評価モデルの確立

多くのシステムの安全性に欠陥が残されている主な原因の一つとして、必要なセキュリティ対策の漏れに加えて、実施しているセキュリティ対策が厳格性に欠け、実施している対策の効果が十分でないことことがあげられている。これは、システムの運営者が、自社が実施しているセキュリティ対策の十分性について評価ができていないことによると考えられる。この背景としては、これは、セキュリティ要求事項については、情報セキュリティマネジメントシステム（ISMS）や現在開発中のセキュ

リティ監査基準等で示されているものの、実施しているセキュリティ対策の十分性について客観的に評価する方法が確立していないところにその一つにあげられる。

現在、経営者や情報システムの責任者やセキュリティ対策の担当者にとって、一番悩むことは、実施しているセキュリティ対策の十分性についての評価尺度が与えられていないことであろう。セキュリティ対策にはそれなりのコストがかかるため、コストとの兼ね合いで決断した妥協が妥当なものかどうかが、当事者の心配の種になっていたり、一部に過度な手当をしているのに、必要とされるところが不十分だったりすることも多く見受けられる。

このため、セキュリティ対策にかかわる者に、実施しているセキュリティ対策について、その十分性が判断でき、対策実施上の不備が見つけられるような評価方法を確立すること、以下に示すような観点から、ネットワーク経由でのサービスやネットワーク利用システムあるいは自社の情報システムの安全性の向上に大きく貢献するはずである。

- セキュリティ対策の実施者に対し対策の目標の付与
- 実施しているセキュリティ対策の総合評価と不備の指摘による目標とする対策レベルの確保についての指針の付与

このため、本調査研究においては、実施しているセキュリティ対策の客観的な評価手法を示す“システムの安全性の評価モデル”の確立の必要性を指摘することになった。

5.1.1.1 システムの安全性評価モデルとは

システムの安全性評価モデルとは、システムの安全性を確保するための要求事項と、要求に対する実施している対策の十分性を客観的に評価する方法を示すものである。

システムの安全性は、必要なセキュリティ対策を漏れなく、かつ、その一つ一つを必要な厳格さで行うことの総和である。このため、すべてのシステムに対し、安全性の客観的な評価を実現するためには、以下のような要素が必要となる。

- セキュリティ要求事項
- セキュリティ要求事項の個々に対し実施している対策の厳格性についての標準的な評価尺度
- システム全体としてのセキュリティ対策の十分性を数値化するモデルと、数値化のためのセキュリティ要求事項に対する重み付けと、実施している対策のレベルにあたえる得点
- 結果の表現方法と評価方法

(1) 安全性評価モデルにおける評価事項

システムの安全性の評価は、当該システムに要求されているセキュリティ要求事項のすべてに対し、その実施の有無と、実施内容の評価の積み上げで行われる。

セキュリティ要求事項については、すでに、JIS 規格となっている情報セキュリティマネジメ

ントシステム（ISMS）が確立しており、このISMSの要求をさらに詳細化したものとして、セキュリティ監査基準が提案されている。

しかし、これらは、情報セキュリティにおけるマネジメント面を中心としたもので、一対となる技術面での要求の細分化には至っていない。システムのセキュリティの確保には、技術とマネジメントの融合が必須でなければならない。これらの課題に対し、本調査研究では、以下のようなことが議論された。

実施すべきセキュリティ対策を、人的セキュリティへの対応、技術面での対応、セキュアなシステム運用を実現するためのシステム運用の管理、および施設、設備の保護にセキュリティ事故への備え、法的事項への準拠、およびこれらの施策を統括するセキュリティ対策全体に対するマネジメントに分け、さらに、技術面での対応については、技術分野が異なるシステムの品質の確保、障害対策、性能確保、外部からの攻撃や内部の者による犯行に備える耐攻撃性の確保、そしてこれらをシステムの実装に反映するセキュアなシステムの確保に細分化することも必要とした。そして、セキュリティ要求事項は、個々のドメインごとに定義されるものとした。

また、セキュリティ対策は策定した施策のシステムの実装や運用への展開、システムの運用環境の変化への適切な対応がなければ機能しないことから、評価すべきは、セキュリティ要求事項に対する対象システムが定めた具体策の妥当性だけでなく、そのそれぞれについてのシステムの実装や運用への展開、その内容の妥当性の評価や、システムの実装や運用への展開を確実にするためのマネジメントププロセスの確立とその厳格な運用、および文書化等の側面からの評価も行わなければならないとした。また、個々のセキュリティ要求事項に対する対策要件の設定にあたっての当該システムでの脅威分析の十分性も評価の対象とすべきとした。

図 5-1 は、実施しているセキュリティ対策についてこの考え方を反映した評価事項の組立てを示すものである。この図は、セキュリティ対策は、技術的な対応の妥当性、業務現場やシステムの運用現場における人的セキュリティに対する対策の妥当性、システムの運営環境の変換に対するこれらの妥当性の維持、セキュリティ対策として定めたことの実行の徹底、セキュリティ対策の実施環境を整える全体としてのマネジメントを立体的に評価すべきことを示している。

ここに示したものは、ISMS や現在提案中のセキュリティ審査基準と相対するものではなく、これらの基準を、システムの現場でより的確に反映できるよう、その組立てを少し変え、それぞれの要求事項をシステムの現場におけるセキュリティ対策実施の実務により対応しやすくするための工夫を加えたものである。

システムの安全性を評価する上での評価項目の組立ては、今後、多くの専門家による議論が待たれるが、ここに示すものは、この点に関する一つの提案である。

対策ドメイン			評価事項					
			対策内容の妥当性			対策実施の管理の確立		
			脅威分析の妥当性	要件指定の妥当性	実装、運用への展開	ﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｾｽの確立	厳格な管理の実施	文書化
セキュリティ対策全体に対するマネジメント			○	○		○	○	○
人的セキュリティへの対応			○	○	○	○	○	○
技術面での対応	システムの品質の確保		○	○	○	○	○	○
	システムの耐障性の確保		○	○	○	○	○	○
	システムの性能の確保		○	○	○	○	○	○
	対攻撃性の確保	不正アクセス対策	○	○	○	○	○	○
		セキュリティホール対策	○	○	○	○	○	○
		ウイルス対策	○	○	○	○	○	○
		情報の保護	○	○	○	○	○	○
		通信の保護	○	○	○	○	○	○
		なりすましの防止	○	○	○	○	○	○
		DoS 対策	○	○	○	○	○	○
	セキュアなシステム構成の確保		○	○	○	○	○	○
セキュアなシステム運用の確保			○	○	○	○	○	○
施設、設備の保護			○	○	○	○	○	○
セキュリティ事故への備え			○	○	○	○	○	○
法的事項への準拠			○	○	○	○	○	○

(注 1) 要件指定の妥当性とは、当該対策ドメインに対する対策要件の指定の内容の妥当性を言う
(注 2) 実装、運用への展開は、セキュリティ要件として定められたことが、システムに組み込まれ、かつ、システム運用や業務運用に対する要求事項が適切に定義されていることを言う
(注 3) マネジメントプロセスの確立とは、脅威分析、要件指定、実装や運用への展開、システムの運用環境の変化に対応した対策の妥当性の維持を適切に行うためのマネジメントの仕組みの確立を指す
(注 4) 厳格の管理の実施とは定められたマネジメントプロセスに沿った定められたことの実行を徹底するため活動を指す

図 5-1 システムの安全性評価のための評価項目の組立てのイメージ

(2) 実施しているセキュリティ対策の評価尺度

セキュリティ対策では、それが技術的な要求であれ、マネジメント面での要求であれ、システムによってその実施に厳格さが異なる。セキュリティ対策の十分性は、必要なセキュリティ要求事項に対する対策の実施に漏れがないようにすることに加え、この実施上の厳格さが大きくかかわる。実施の厳格性はセキュリティ対策の十分性の評価に大きくかかわる例を、侵入監視システム（IDS）の活用による侵入監視を例に、表 5-1 に示す。

表 5-1 実施の厳格性がセキュリティ対策の効果に大きくかかわる例

実施状態	評価
・ネットワーク型 IDS とホスト方 IDS を併用しているか、障害監視をファイアウォールと連携させて監視している。 ・シグネチャコードを自分でコーディングするなどして、字サイトに適したポリシー調整を行っている ・体制を考慮したアラート方法を設計し適用している	十分、 IDS の機能をフルに活用でき大きな効果を期待できる
・各プロトコル中のシグネチャを理解し、自サイトに適したシグネチャを選択している。 ・シグネチャのしき値まで調整できている	おおむね十分、相当な効果を期待できる
・HTTP,SMTP などの監視対象のプロトコルを選択しているだけで、自サイトに適したシグネチャの選択は行われていない	不十分、ある程度の効果は期待できる
監視ポリシーは IDS 製品のデフォルトのまま稼動させている	未対策にに近く、効果はあまり期待できない
IDS による侵入監視は行っていない	未対策

このため、システムの安全性を評価するためには、要求されている実施しているセキュリティ対策の個々に対して、その実施の厳格性の評価が加わらなければならない。しかし、セキュリティ対策の実施についての厳格性を定量的に量れるものは少ない。このため、実施しているセキュリティ対策の個々い対する厳格性の評価が、評価者によって大きなばらつきがなく、ある程度、客観的にできるようにするためには、個々のセキュリティ要求事項に対し、実施の厳格性を評価する尺度を確立することが必要となる。

本調査研究で議論された、この厳格性の評価尺度定義の一つのアイディアを以下に示す。

- 評価事項ごとにその実施状態を 5 段階評価する
- 評価事項ごとに各段階に該当する標準的な状況を定義する
- 評価は、実施の状況が各段階に対し定義されている標準的な状況に最も近いものとする
- 評価項目ごとの各段階に該当する標準的な状況の定義は、実施頻度等の定量的に評価が可能なものは別とし、標準的なスタイルを準備する。このスタイルはその特性に応じ、技術的な要求とマネジメント面でその特性が反映されるようにする

こおイメージを示すものが、表 5-2、表 5-3、表 5-4 ある。

表 5-2 厳格性についての各ランク分のイメージ

ランク	ランクのイメージ	備考
A	十分（または対策不要）	考えられる対策は尽くされている
B	おおむね十分	内容的には十分であるが、わずかな隙を残す
C	一通りの対策はされている	最低限の対策は講じられているが、十分とは言えない
D	不十分ながら対策はある	対策の実施は形式的で、効果は疑わしい
E	未対策	何も対策されていない

表 5-3 定量的評価が可能な対策項目についての実施密度のランク付けのイメージ

例：セキュリティホール対策の実施

ランク	ランクのイメージ	義等する実施状況
A	十分（または対策不要）	対策の必要が生じた場合、一日以内に実施
B	おおむね十分	対策の必要が生じた場合、一週間以内に実施
C	一通りの対策はされている	対策の必要が生じた場合、二週間以内に実施
D	不十分ながら対策はある	対策は対策は月 1回未満
E	未対策	ほとんど実施していない

表 5-4 技術的要求事項に関する要件定義についてのランク付けのイメージ

例：サイト内の通信の制御ルールの指定状況

ランク	ランクのイメージ	義等する実施状況
A	十分（または対策不要）	指定内容は妥当であり、実施内容の検討やその内容の妥当性の管理も組織的に行われている
B	おおむね十分	指定内容は妥当とみられるが、実施内容の組織的な検討やその内容の妥当性の管理に不十分なところがあり、ミスがある隙も残されている
C	一通りの対策はされている	指定内容はおおむね妥当とみられるが、組織的な検討にもとづいたものではない。また、その内容の妥当性の管理も組織的には行われていなく、ミスが残されている可能性は低くない
D	不十分ながら対策はある	組織的な検討にもとづいたものではなく、重大ではないものの、指定に問題が見られる 検討に基づいた指定ではなく、問題もある
E	未対策	

注 1）指定内容が妥当とは、サイト内のネットワーク構成やサーバ配置やファイアウォールやウイルス対策ソフト等の配置に照らし、サイト全体のセキュリティポリシーを満足するものであることを言う
注 2）組織的な検討とは、指定の検討やレビューが組織として行われ、担当者ベースではないことを言う

表 5-5 マネジメントに関する要求事項についてのランク付けのイメージ

例：ログの保護の実施についての管理の状況

ランク	ランクのイメージ	義等する実施状況
A	十分（または対策不要）	実施内容は妥当であり、運用プロセスやマネジメントプロセスも確立していて、その実行も徹底している。不手際を生じる隙はほとんどない
B	おおむね十分	実施内容は妥当であり、運用プロセスやマネジメントプロセスも一応定められているが、管理の徹底さには欠ける。不手際を生じる隙も残されている
C	一通りの対策はされている	実施内容は概ね妥当であるが、担当者レベルの対応で、組織的な管理に展開されていない 運用プロセスやマネジメントプロセスが確立していない）
D	不十分ながら対策はある	実施内容は組織として決められたものでなく、担当者の実効に任されている
E	未対策	管理はされていない

ここに示したものは、システムの安全性確保のための要求に対する対策の実施状況の評価尺度についてのイメージを示したに過ぎない。セキュリティ要求事項の実施状況を客観的に評価の定義については、さまざまな議論があると考えられる。この点についての議論は、今後、セキュリティ関係者の間で、積極的な議論が行われることを期待する。

(3) 評価事項に対する重み付け

システムの安全性についての総合的な評価ができ、対策上の欠陥を把握するとともに、対策の実施にあたっての限られた予算や設備、人的リソースの有効活用を実現するためには、セキュリティ要求事項すなはち評価事項に対する重み付けが与えられ、この重みを用いた実施中あるいは計画中のセキュリティ対策全体としての評価、および 対策ドメインごとに評価を数値的に表現することも有効となる。

また、個別システムの安全性の数値表現は、ネット経由でのサービスやネット利用のシステムを利用する者が、利用するシステムの安全性を知ることができる点にも意味がある。

(4) セキュリティ対策の評価結果の表現方法

セキュリティ対策の評価結果の表現方法も、セキュリティ対策の評価モデルの重要な要素となる。これは、今後の検討に待つが、報告事項、グラフ化等の結果の表現方法は、評価結果を正しく伝えるために重要となる。

5.1.1.2　安全性評価モデルの利用方法

このような安全性評価モデルは、以下のような 利用が考えられる。

- セキュリティ対策についてのベストプラクティスの明確化
- 実施しているセキュリティ対策の十分性についての自己評価
- 実施しているセキュリティ対策の第三者による評価
- システム種別別のセキュリティ対策プロファイルの確立

(1) セキュリティ対策についてのベストプラクティスの明確化

セキュリティ対策として実施を要求する事項と、そのそれぞれに対する実施上の厳格性の評価を示すことにより、システムの運用者や構築にかかわる者は、ベストプラクティスは何かを知ることができる。このことは、目標の設定を容易にするだけでなく、セキュリティ対策に必要なリソースの有効配分の実現にも寄与することが考えられる。

(2) 実施しているセキュリティ対策の十分性についての自己評価

この評価モデルをガイドとして、システムの運用者や構築関係者は、対象システムのセキュリティ対策の欠陥と全体的なレベルを客観的に知ることができる。このことは、システムのセキュリティレベルの向上をもたらす。

また、多くのシステムの安全性が標準的な基準の下で数値表現されれば、同種のシステムが達成すべき安全性の標準を知ることができるとともに、自社のシステムの安全性を同業他社のそれと比較することも可能となる。この比較は、自社のシステムの安全性が十分かどうかの判断材料ともなる。このことは、万一、セキュリティ事故に見舞われ、外部に損害をかけた場合の責任の程度を左右することもつながる。

(3) 実施しているセキュリティ対策の十分性についての第三者評価

このモデルは、ISMS と同様に実施しているセキュリティ対策の評価サービスに一定の基準を与えるため、セキュリティ対策の評価サービスの提供や利用をより信頼の高いものにすることに寄与すると考えられる。

(4) システム種別ごとのセキュリティ対策プロファイルの確立

システムに求められるセキュリティ対策は、対象業務やシステムの運営形態等のシステムの特性によって異なるため、標準的なセキュリティ対策像であるセキュリティ対策プロフィルは、システム種別べつだけでなく、さらにその規模等別に作られなければならない。セキュリティ対策の評価モデルは、実施が要求される事項とその厳格性の評価尺度を示しているため、システムの特性が異なり、必要とするセキュリティ対策とその実施の厳格性は異なっても、その設定の妥当性を一定のものにするだけでなく、その表現も統一的にできるため、システム種別別のセキュリティ対策の開発を容易にする。

システム種別ごとのセキュリティ対策プロフィルの確立については、5.1.2 節参照。

5.1.1.3　安全性評価モデルの位置付け

安全性評価モデルと、ISMS、セキュリティ監査基準、システム種別ごとのセキュリティ対策プロファイル、およびシステムの後述の安全性評価サービスの関係を、図 5-2 に示す。

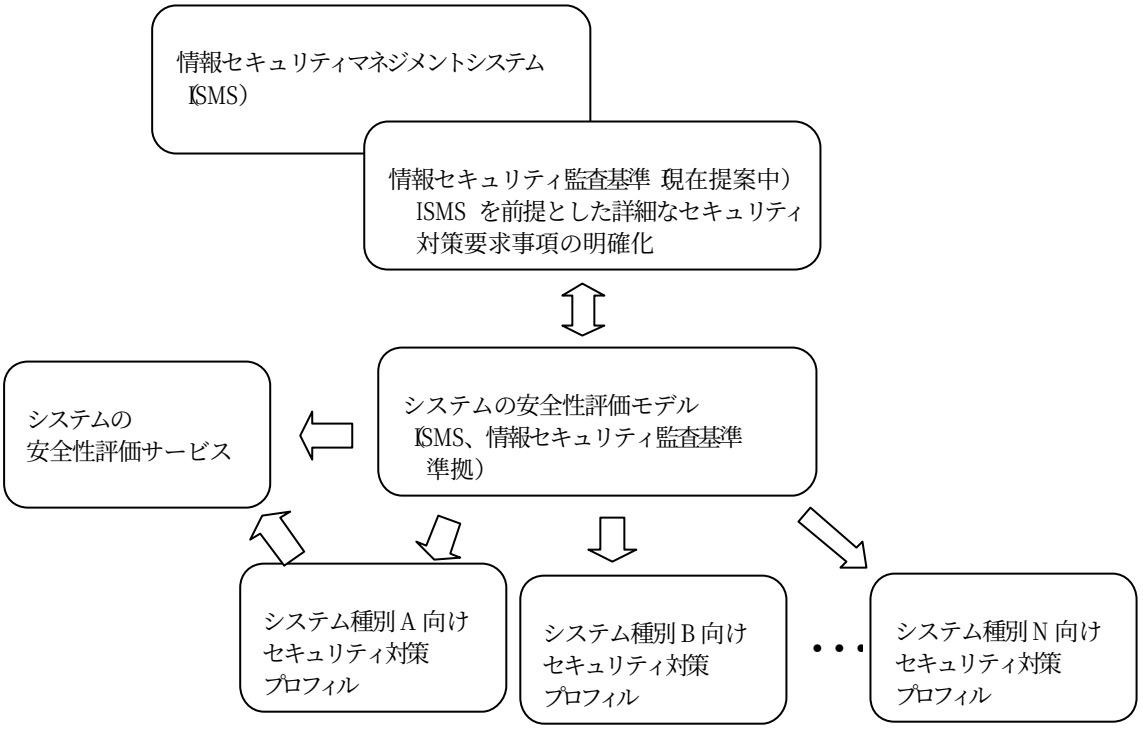


図 5-2　安全性評価モデルとシステム種別のセキュリティ対策プロファイルの位置付け

5.1.2　システム種別ごとのセキュリティ対策プロファイルの確立

求められるセキュリティ対策としての実施すべきことならびにその厳格性は、システムの特性によって異なる。これらは、個々のシステムごとに決められ実施されるべきものである。しかし、ネット社会の仕組みにかかわるシステムのすべてにおいて、その安全性に大きな欠陥がなく一定の水準に達していることを実現するようにするためには、個々のシステムの運営者に、自 社のシステムのセキュリティ対策の雛型の提示も必要と考える。

個々にシステムがその安全性を確保するために実施すべきセキュリティ対策を、システム種別およびその規模別に、一つの目標として示すのがセキュリティ対策プロファイルである。

5.1.2.1 システム種別ごとのセキュリティ対策プロファイルのイメージ

セキュリティ対策プロファイルは、システムの種別ごとに定義されるもので、表 5-6 に示すような事項を示すものと考える。

表 5-6 システム種別ごとのセキュリティ対策プロファイルでの定義事項

区分	定義事項
適用範囲	・対象となるシステムの範囲 ・セキュリティ対策上での特性
前提とする脅威	・当該システムに想定される脅威 ・想定されるセキュリティ事故の影響
セキュリティ対策についての基本方針	・脅威への対応方針 ・目標とするセキュリティ対策のレベル ・セキュリティポリシーの雛形
セキュリティ要求事項	・セキュリティ対策として実施すべき事項と、実施内容についての具体策の提示と、求められる厳格性の提示 セキュリティ対策の体系としては以下を含む －システムの品質の確保 －システムの障害対策 －システムの性能確保 －耐攻撃性の確保 －施設、設備の安全確保 －事業の継続性の確保 －人的管理、業務パートナーの管理
システム構成	・システム構成についての基本方針 ・標準的なシステム構成パターン ・システム構成上の留意点 ・システム構成の維持管理
セキュリティマネジメント―セキュリティレベルの維持管理	・セキュリティ対策内容の決定プロセス ・システムのセキュリティ対策の実態の把握方法 ・セキュリティ対策の実行を管理する仕組み ・システムの運用環境の変化に対応したセキュリティレベルの維持の仕組みの確立 ・セキュリティ監査
法的準拠	・当該システムの制約条件となる法令や業界規制および契約等 ・法的制約条件に対する対処の方針
サービスの提供上の留意点	・システムの安全性のレベルの公表 ・利用者への利用上の留意事項の明示

5.1.2.2 システム種別ごとのセキュリティ対策プロファイル確立へのアプローチ

セキュリティ対策プロファイルは、セキュリティ特性やセキュリティ対策の実現方法が異なるシステム種別およびシステム規模ごとに定義されるものであるため、当該サービスを提供する業界が研究

し開発されるのが望ましい。

先に述べたシステムの安全性評価モデルは、対応する業界ごとに定義が進められことになろうシステム種別、規模別のセキュリティ対策プロファイルの定義が、これらがシステムの安全性の確保について異なった評価尺度で作られないようにするとともに、標準的な尺度によるこれらのプロフィルに対する評価を可能にする。システムの安全性評価モデルの確立は、システム種別ごとのセキュリティ対策プロファイルの確立のベースとも言える。

5.1.2.3 セキュリティ対策プロファイルの確立が求められるシステムの例

セキュリティ対策プロファイルの確立が求められるシステム分野としては、表 5-7 に示すものがあげられる。

表 5-7 セキュリティ対策プロファイルの確立が求められるシステム分野

対象となるシステム分野	対象システム例
・ネット社会を支える基盤サービス提供システム ・行政機関の責任が問われるようなシステム ・生命財産に大きな被害を及ぼすようなシステム ・プライバシーの侵害に直結するようなシステム ・国民生活に広くかかわるシステム	・認証サービス提供システム ・電子文書の公証サービス提供システム ・各レベルの行政機関のシステム ・医療サービス関係システム ・金融機関のシステム ・電子商取引関係システム ・福祉関係サービス

5.1.3　システムの安全性対策実施基準の確立

システムの安全性対策プロファイルはシステム種別やその規模別に定義されるものであるが、これらの定義が適切であり、かつ、同じようなセキュリティ特性を持つシステム間でその安全性に大きなバラツキがでないようにするためには、ネット経由で提供されるサービスやネット利用システムに求められる安全性の高さにクラス分けを行い、それぞれのクラスごとに目標とすべき安全性確保のための対策の実施レベルを示すことも有効と考えられる。

システムの安全性対策実施基準とは、システムの安全性の強度で分けたクラス分けと、それぞれのクラスが目標とすべき安全性対策、およびさまざまなネット経由で提供されるサービスやネット利用システムが所属すべきクラスを示すものを言う。

この安全性のクラス分けと、各クラスに分類されるシステムが目標とすべき安全性の指定するこの安全性対策実施基準は、システム種別に作られる安全性対策プロファイルの定義をガイドするとともに、ネット経由でのサービスやネット利用システムの利用者にとって、対象のシステムの安全性を評価する上で大きなよりどころにもなりうる。

5.1.3.1　システムの安全性対策実施基準のイメージ

システムの安全性対策実施基準は、以下の要素で構成される。

- 安全性のクラス分け
- 各クラスが目標とする安全性対策の実施水準

  各クラスが目標とする安全性は、安全性評価モデルが指定する対策要求事項おそのそれぞれについての最低限達成しなければならない厳格性の指定で表されることになろう。
- 代表的なシステムが所属すべき目指す安全性クラス

このシステムの安全性対策基準のイメージを。表 5-8 に示す。

(注 1)表 5-8 に示す各安全性クラスに対する安全性の度合い、対策ドメインごとに要求される厳格性や、対象とするシステムの特性や該当するシステム例は、あくまでも、この安全性対策実施基準のイメージを示すためもので、個々に定義や考え方については、今後の議論とする。

(注 2)表 5-8 の中での対策ドメインごとに要求される厳格性を示す◎、○、△は、それぞれ以下を表すものとする。

◎ ：非常に重要、実施にあたっては最高の厳密さを要求

○ ：重要、実施にあたってはかなり高い厳格さを要求

△ ：最低限以上の厳格を要求

5.1.3.2　安全性対策実施基準の確立へのアプローチ

このようなシステムに対する安全性実施基準の確立に向けては、以下のようなことについての検討が必要となる。

- 安全性対策実施基準確立の要否

  本調査研究で議論の対象となったものの、その有用性についての疑問や基準の定義上の困難さ等の指摘もあり、このような基準の確立の要否については、その意義や具体的なイメージにもとづいたのさらに深い議論が求められる。
- 安全性ランクの定義
- 安全性対策実施基準の位置付け

  この基準の確立を進める場合は、ISMS やセキュリティ監査基準、安全性評価モデル、システムジャンルごとに確立が進められる安全性対策プロファイル、さらにはシステムに対する安全性評価認証制度との関係についての議論も必要となる。

クラス	安全性の度合い	対策ドメインごとに要求される強度		対象とするシステムの特性	対象となりうるシステ
クラスA	すべての要求事項について最高レベルの対策が指定され、その実施上の不備も皆無に近く、未知の攻撃手法を除いてはセキュリティ事故の発生は考えられず、かつ、セキュリティ事故は利用者の被害に結びつかないようにな工夫が行われている	全体マネジメント 人的セキュリティ 品質の確保 障害対策 性能管理 耐攻撃性 システム構成の強度 運用のセキュア度 施設、設備の保護 事故への備えのレベル 法的事項への準拠	◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎	その安全性の不備は、利用者の生命、身体に直接的な被害を生じたり、ネット社会全体の安全と信頼を揺るがしかねないようなシステム	・認証サービス ・時刻認証サービス ・電子文書公証サービス ・医療行為に直結するシステム
クラスB	すべての要求事項について相当に厳格な対策が指定され、そのシステムの実装や運用への展開も厳格に管理され、対策実施上に不備がある可能性はかなり低い。 また、セキュリティ事故が発生しても、利用者にできるだけ被害に及ばないような工夫が行われている	全体マネジメント 人的セキュリティ 品質の確保 障害対策 性能管理 耐攻撃性 システム構成の強度 運用のセキュア度 施設、設備の保護 事故への備えのレベル 法的事項への準拠	◎ ◎ ○ ○ ○ ○ ◎ ◎ ○ ○ ◎	その安全性の不備に不備があった場合、利用者に莫大な損害をもたらしたり、広範囲に利用者の身体に直接的な被害を生じたり、プライバシーの侵害等を生じ、ネット社会全体の安全と信頼にお不安を生起システム	・行政機関のシステムの一部 ・社会のインフラを提供するシステ ・社会の安全を守る機関のシステム ・金融取引をサポートするシステム ・ネット経由で提供する医療サービ ・ネット経由で福祉サービスを提供
クラスC	対象となる要求事項のすべてについて必要なレベルでの対策が指定され、そのシステムの実装や運用への展開も管理されている。また、セキュリティ事故が発生しても、被害は限定なものになるような工夫がなされている	全体マネジメント 人的セキュリティ 品質の確保 障害対策 性能管理 耐攻撃性 システム構成の強度 運用のセキュア度 施設、設備の保護 事故への備えのレベル 法的事項への準拠	○ ○ ○ ○△ △ △ ○ ○ ○ ○ ◎	ランク B ほどではないが、比較的広範囲に利用者の財産、プライバシーに少なからぬ損害を生じ得るもの	・金融取引を除く電子商取引対応シ ・行政機関のシステムの一部
クラスD	対象となる要求事項に対し必要最低限の対策が指定されており、そのシステムの実装や運用への展開についての管理もある範囲で実施されている。また、セキュリティ事故が発生しても、被害は限定なものになるような工夫も、ある程度なされている	全体マネジメント 人的セキュリティ 品質の確保 障害対策 性能管理 耐攻撃性 システム構成の強度 運用のセキュア度 施設、設備の保護 事故への備えのレベル 法的事項への準拠	△ ○ ○ △ △ △ ○ △ △ △ ◎	利用者をトラブルに巻き込む可能性はあるが、被害は限定的と見られるもの	・企業内システム ・eラーニングを提供するシステム

5.1.4　個別システムに対する安全性評価認証サービスの導入

システム種別およびその規模別に安全対策プロフィルが確立すれば、ネットを用いるサービスやシステムに個々に対し、第三者機関による、該当する安全対策プロファイルを満たしているかどうかの評価認証を行うサービスの導入も考えられる。

このようなサービスによるシステムの安全性についての評価認証は、ネット経由で提供されるサービスやネット利用システムを提供する事業者に、以下のような効果をもたらす。

- 利用者に対する当該サービスやシステムの安全性についての評価材料を与えることによる競合上の必要要件の確保
- 万一、セキュリティ事故による紛争が生じた場合における、必要な注意義務を果たしていると言う意味での）責任範囲の限定

また、利用者にとっても、該当するシステムの安全性について一定の判断が可能となる。

これは、現在、展開されている ISMS 評価認証制度に比べ、審査基準がシステムの種別やその規模によって異なるところと、セキュリティ要求事項の個々について十分性がさまざまな角度で評価されるようになるところで異なるが、安全対策上の要求事項は根本では同じで、ISMS 評価認証制度をさらに拡大するものして位置けることもできる。今後の検討課題である。

5.1.5　サービスやシステムを提供する事業者におけるセキュリティ対応力の強化

ネットワークを介して提供されるサービスやネットを用いるシステムの提供にあたって、その利用やシステムの運営についての安全の確保のために求められることが明確になっても、これらに応える能力がなければ、サービスやシステムは安全なものとはならない。

このためには、このようなサービスやシステムを提供する事業者における、システムの安全性の追求に必要な能力の向上が必要であり、その実現には、

- 経営者層に対する情報セキュリティについての啓蒙活動の推進
- 組織の責任者における情報セキュリティマネジメント対応能力の強化
- 情報セキュリティ担当者の技術レベルの向上

等が必要となる。

それぞれについての考え方を、表 5-9 に示す。

表 5-9 情報セキュリティ対応能力の向上に向けた必要な取組み

	施策区分	検討すべき施策
1	経営者層に対する情報セキュリティについての啓蒙	製品やサービスの提供にあたっての利用者の安全を阻害する脅威の存在と、利用上の安全について製品やサービスの提供者の責任についての認識の定着 ・経営者用パンフレットの整備 ・さまざまな機会を捉えたセミナーの実施 ・経営者育成コースへの情報セキュリティ問題の組み込み ・CSO（Chief Security Officer）制度導入の啓蒙
2	組織の責任者における情報セキュリティマネジメント対応能力の向上	企業等の組織の上級管理者を対象としたセキュリティ専門教育コースの整備 ・情報セキュリティを対象とした専門職大学院の新設 ・既設大学院大学における情報セキュリティマネジメントコースの強化 ・指導者の確保のための施策の展開
3	情報セキュリティ担当者の技術レベルの向上	企業における情報システムのセキュリティにかかわる担当者や、IT 製品やサービスの開発担当者の情報セキュリティについての技術力の向上を図る ・必要なスキルマップの整備 ・情報セキュリティを対象とした専門職大学院の新設 ・既設大学院大学における情報セキュリティに関するコースの再構築 ・政府による民間の教育サービス事業の支援による民間レベルでの教育サービスの強化拡大 ・指導者の確保の推進 ・有資格者の配置 ・セキュリティ技術者認定制度の強化

5.1.6 システムの安全性の評価についての米国の試み

米国においては、システムの安全性についての評価サービスがビジネスとして提供されている。サービスによって異なるが、評価の対象は、システムの技術面での脆弱性の検査と、セキュリティマネジメントの実施状況からなっており、その結果から、絶対的な総合評価と改善を要するところを可視的に示すとともに、対象システムに求められる安全性に対する（十分、普通、不十分といったような）相対的な評価も提示されるようになっている。

現在、米国内で提供されているこれらのサービスの背景となっている安全対策の評価事項の考え方は、5.1.1 節に示した安全性評価モデルにおける評価事項の組立てと、少し異なったものであるが、安全性評価モデルの確立、安全性対策実施基準の確立、およびシステムの安全性評価認証サービスの導入等の検討にあたっては、十分に参考になるものである。

米国におけるシステムの安全性評価サービスについては、巻末の参考を参照されたい。

5.2 サービスやシステムの提供に関するガイドラインの確立

利用者に、ネット経由で提供されるサービスやネットを用いるシステムの安全な利用を実現するためには、利用者にそのサービスやシステムの安全性を理解させるとともに、利用者に利用における安全確保のための利用者の選択や責任を示すとともに注意を喚起することも必要となる。

これらが該当するすべてのサービスにおいて適切に行われるようにするためには、ネット経由でのサービスの提供やネットを用いるシステムの提供にあたって、これらを提供する事業者に対する、この点に関するガイドラインの確立も必要となろう。

5.2.1 ネットを介したサービスやネットを利用するシステムの提供にかかるガイドラインのイメージ

ネットワークを用いるサービスやシステムの利用者への提供にあたって、利用者の安全の追求のためのガイドラインが要求する事項、すなはち提供事業者がサービスやシステムの提供にあたって配慮すべき事項としては、表 5-10 に示すようなものがあげられる。

表 5-10 ネットワークサービスの提供にかかるガイドラインでの要求事項

	区分	定義すべき事項
1	セキュリティのレベルに対する利用者への選択権の付与	サービスやシステムの利用にあたって、利用者に選択させるべき機能やサービスにグレードが存在する場合、その選択が可能となる仕組みの提供
2	セキュリティ面からのサービスグレードの明示	・目標とする可用性 （サービス時間帯、障害が発生した場合の回復所要時間等） ・サービスグレードが低下する場合とその範囲
3	利用上の注意事項	セキュリティ面からの利用上の注意事項
4	セキュリティ対策の限界	防ぎようのないセキュリティ事故と、それらの利用者への影響の範囲
5	IT 製品やサービス提供者の責任と利用者の責任	・サービスやシステムの提供者が追うべき責務と損害の補償の範囲 ・利用者の責任に帰するセキュリティ事故
6	相談窓口	・サービスやシステムの利用上の相談窓口 ・苦情の申し立ての窓口

5.2.2 利用者に対するセキュリティ上の担保範囲、利用者の責任の明示について

情報セキュリティについては、万全は期しがたいことから、利用者に対しその安全対策の限界と、利用にあたっての利用者側の責任と、生じたトラブルに対する提供者側の責任を明確にしておくことも必要となる。

安全対策の限界に関しては、システムのセキュリティ対策をかいくぐって発生しうるリスクと、その脅威が現実になったときに想定される利用者への影響についての説明が要求される。また、利用

者の責任の明示とは、サービスやシステムの利用にあたって、必要な装置の準備や利用上の操作上で利用者の責任で行わなければならないことのを利用説明書等で明確にすることを言う。

また、利用者側およびサービスやシステムの提供者側の責任の明確化とは、当該製品の利用においてセキュリティ上のトラブルが生じた場合における、責任の所在と責任の範囲を示すもので、このためには、製品やサービスの使用説明において、以下のような事項が明確にされることが求められる。

- 防ぎえないトラブルと想定される利用者への影響
- トラブルの原因が利用者の責任に帰属する場合の明示
- トラブルがサービスやシステムの提供者の責任に帰属する場合の明示
- トラブルが利用者またはシステムやサービス提供者以外の第三者の責任による場合の明示
- トラブル発生時におけるサービスやシステムの提供者としての支援の範囲
- それぞれの場合における生じた被害に対するサービスやシステムの提供者による補償の範囲の原則

5.2.3 利用したいサービスやシステムのセキュリティ機能についての利用者への選択権の付与について

情報セキュリティの確保にはそれなりのコストが伴う。利用者は、一般に、コストについては厳しいので、サービスやシステムの提供者が価格競合力の維持のため利用者には分かりづらいセキュリティ対策の優先度を下げてしまう傾向にあるのは当然であろう。しかし、セキュリティにかかる事故の発生についての責任問題が問われるようになると、提供者側にとっては、セキュリティレベルの確保とコストとのバランスをとることは悩みの種となる。

このため、ネットワークサービスについては、その提供者はサービスの提供にあたってさまざまなセキュリティレベルを準備し、その選択をコスト負担を前提に利用者に委ねるようにする方法を一般化すべきでなかろうか。このことは、利用者に安全の確保についての自己責任についての意識を向上することにもつながる。利用者は強度の低いセキュリティ対策を選択した場合、料金は低くなるものの、その分セキュリティ事故による被害等を、自己の責任として甘受しなければならない。

選択の対象として考えられるものとしては、以下があげられる。

- 認証方式の選択
- 通信路と通信の保護策の選択
- ネット上でのシステム間のやりとりについての証拠の確保の要否

ネットを介したサービスの利用やネットにつながるシステムの利用に対し、セキュリティ対策手段の選択権を利用者に付与する場合、サービスの提供者やシステムの提供者は、以下を明示しなければならないとするようなルールの確立も検討の対象となる。

- 選択の対象となる方式の説明とそれぞれのセキュリティのレベルについての説明
- それぞれの選択肢を選んだ場合における、当該選択にかかるセキュリティ事故における提供者側の責任版地と利用者側の責任範囲

6　ネット社会の安全と信頼を支えるインフラサービスの整備の推進

ネット社会の安全と信頼を支えるインフラサービスとしては、

- 認証サービス
- 電子文書の公証サービス
- 電子情報の公証サービス
- 電子情報の保管サービス
- 時刻認証サービス
- ネットにかかる安全支援サービス
- ネットにかかる安全と信頼に関する情報提供サービス

があげられる

認証サービスや電子文書の公証サービスはすでに提供されており、これらについての課題はさまざまな場所で論議されいるので、ここではこれから整備が求められる電子情報の公証サービス以下の新しいテーマについての考察を示す。

6.1　電子情報の公証サービスについて

電子文書については、その適用は限られているものの電子公証制度がすでに導入されている。電子化された社会においては、多くの情報は電子化されており、何かの紛争にこれらの情報が用いられるようになる自明である。

通信ログや処理のログ、あるいはある時点での DB の内容等がこれらの範疇に入るが、これらの情報についても、電子文書同様に、後日の紛争に備え法的効力をもつようにしておくことも必要になると思われる。

法的効力の持たせ方については、電子文書の公証サービスと同じスキームが考えられるが、文書と違いこのような情報は、個々の情報が大量であることに加え、その対象も多くさらに一つ一つが日々作成更新されるようなものも含まれているため、量的な側面で大いな違いがある。

このような情報に対して、電子文書の公証サービスと同じようなスキームが適用できるかどうかは疑問である。

いずれにせよ、電子文書以外の電子情報の公証サービスについては、その要否も含め、今から検討すべきテーマであると言える。

電子情報の公証サービスについて検討すべき事項としては、以下があげられる。

- 電子情報に対する公証サービスの要否
- 法的効力の付与を実現するためのルール
- 適用する技術方式
- 必要とした場合、サービス提供にかかる運用スキーム

6.2 電子情報の保管サービス

電子社会の進展に伴い、企業等ではもちろんのこと、今後は家庭においても、電子文書も含みさまざまな電子情報の保管が課題となってくる。自社内や家庭で自らこの情報の保管を行うことは、その安全上の対策の必要もあって負担となることが考えられる。このため、企業や個人の家庭が、後日の必要に備え、一部の情報の保管を外部に委託することも多くなると考えられる。

電子情報の保管サービスの利用において、保管上のトラブルによる紛争の発生を防止するとともに、紛争が生じてもその解決が円滑に行われるようにするためには、ビジネスベースで行われるものではあるが、電子情報の保管サービスににについても、そのあり方や適用する技術および運用のルールが、社会的なコンセンサス上に確立されることが必要となる。

これらについても、早急な取組みが必要となろう。

6.3 時刻認証サービス

ネット経由での処理や電子文書にかかわる紛争の処理に重要となるものに、ネット上あるいはシステム上での処理の発生時刻がある。電子文書の作成あるいは電子公証制度における文書の確定においてもその時刻が問題となる。

ネット処理や電子的な処理において事項が問題となるケースとしては、表 6-1 に示すようなものがあげられる。

表 6-1 ネット処理や電子処理における時刻問題

施策区分	時刻が問題となること
電子文書の作成時刻	・電子署名された文書の有効性
ネット（システムの）処理の実行時刻	・時刻に制限のある処理についての処理要求の有効性 ・処理要求の順序性 ・二つのシステム間でのやり取りに関する責任の切り分け

現在、文書の作成も含め、システムの処理の時刻は、それぞれのシステムの時刻が与えられているが、システムの提供する時刻の制度は十分でないことに加え、システムによってまちまちである。このため、システム間で処理が行われた時刻が問題になった場合への対処は、不可能と言わざるを居ないのが現状である。

このため、今後の文書の電子化やネット経由でのサービスの利用やシステムの操作の飛躍的拡大がもたらす、さまざまな紛争に備え、システムやネットの処理にかかる時刻の問題として、以下についての解決が必要となる。

- 標準時刻の確立

- システム時刻の標準時刻への同期化の推進
- コラボレーションするシステム間での時刻の同期化の推進
- 時刻重要となる電子文書やネット処理に対するタイムスタンプ

これらの解決のためには、ネット社会を支える基盤サービスの一つとして、以下のようなサービスの整備も必要となる。

- 標準時刻の提供サービスの整備
- 時刻重要となる電子文書やネット上でのやり取りに対するタイムスタンプサービスの整備

この時刻認証に関するサービスの整備についての検討もすでに進められているものの、早々に、ネット社会を支える基盤サービスとして整備が進められることが望ましい。このためには、これらを実現するためのアーキテキチャの確立、対応ツールの整備にくわえ、時刻認証に対する法的効力の確立等のその利用についてのルール面での検討も必要となる。

6.4 安全支援サービス

6.4.1 安全支援サービスとは

行政機関、団体、企業、家庭等に対するそれぞれの運用するシステムにおける安全確保にかかる諸サービスを提供するもので、利用者は自己システムの安全確保の一部をアウトソーシングするものである。

ネットワークの利用が一般家庭にまで広く行き渡り、しかも、それぞれが自己の責任範囲におけるシステムの安全についての責任を持つことになろうとも、技術的に対応が難しいところもあり、適切な対応をできることは期待できないことは容易に想定される。このため、これらの技術的弱者に対し、適切なサービスが提供されることが必要となる。

6.4.2 提供が求められる安全支援サービス

ネット社会の安全と信頼の確保のために、今後、充実が求められるサービスを表 6-2 に示す。企業向けとしては、これらの一部はすでに提供されているものもあるが、今後は、零細企業やSOHO、および家庭でのネットの利用の安全に重点がおかれなければならない。

表 6-2　既存ならびに今後求められるサービスの一覧

	提供する情報の内容	概要
1	安全機能のインストールサービス	各家庭や SOHO 等に対し、家庭内システムの安全の作りこみの代行するサービス
2	診断・監視サービス	家庭内や SOHO 等のシステムの脆弱性の診断や、侵入あるいはその試みの監視を代行するサービス
3	安全機能の運用代行サービス	ファイアウォールの運用等も含め安全対策の実施を全て代行するサービス

6.4.2.1　安全機能のインストールサービス

家庭内のシステムを守るためのファイアウォールやホームゲートウェイのインストールと、家庭内のネットワークやシステムをセキュアなものにするための家庭内システムの構築を代行するサービスである。

家庭内のシステムがインテリジェント化につれて、その安全対策も複雑になることから、一部の家庭を除いては、専門家の支援に頼らざるをえず、これらのサービスはネットワーク社会では不可欠なものとなろう。

(1) サービスメニュー

このサービスのメニューは、一般的に以下のようなものなろう。

- 家庭内のネットワークおよびシステム構成の設計
- 家庭内ネットワークへの機器のつなぎ込みと必要な設定
- ファイアウォールやホームゲートウェイのインストールと諸設定
- 各種認証用情報の設定の支援

(2) 想定されるサービスの提供形態

各家庭がサービスの対象となると、数もさることながら、機器の増設や、利用サービスの追加や、サービスやシステムの利用法の変更の都度サポートが必要となることを考えれば、継続的なサービスの提供が必要となり、提供者としてはそれぞれの地域に密着した事業者が対応することになろう。さまざまな業種からの参入もあるが、ある程度の技術力が求められるので、地域密着型の PC や家電の販売業者や、IT 関連産業，あるいは通信業者が中心になると考えられる。

(3) サービスの実現にあたっての課題

このようなサービスは、ネットワーク社会を裏から支えるものとして重要なものであり、社会の全体から受入れられるものでなければならない。したがって、このようなサービスのありようについては、社会的なコンセンサスが成立していなければならない。この時、議論となる事項をあげると、表 6-3 のようになる。

表 6-3　安全対策のインストールサービス提供の実現に向けての検討課題

	検討項目	検討が必要な事項	備考
1	コストと料金	・妥当とされるコスト ・設定可能な価格帯 ・課金の方式	(注 1) ものによっては製品価格に上乗せすることも考えられる。
2	サービス提供者の責任の範囲	・問題が生じた場合におけるサービス提供者の責任の範囲	
3	サービスの品質の確保	・サービス提供にあたっての標準手順の確立 ・サービス品質についてのついての基準の確立 ・サービス提供体制の確保 　－必要なスキルの定義 　－サービス要員に対する技能検定制度の検討 ・サービス提供者に対する認可制度の導入の検討	
4	サービス提供事業者のモラルの確立	・サービス提供業者における管理モデルの確立 ・サービス提供事業者に対するモラル教育	

6.4.2.2　監視サービス

監視サービスは、特に安全についてコストをかけても、安全の強化を図りたいシステムに対し、システムの脆弱性の診断や、侵入等の攻撃の検知、あるいは攻撃の試みの監視を行なうものである。事業者や一般家庭でもサービスやシステムのリッチユーザが、サービスの対象となろう。

(1) サービスメニュー

このサービスのメニューは、一般的に以下のようなものなろう。

- 対象システムの脆弱性診断
- アクセスログの分析等による攻撃の試みの監視
- 侵入等の攻撃の検知
- サイトのセキュリティ強化似ついてのコンサルテーション

(2) 想定されるサービスの提供形態

このサービスの提供には相当な技術力と高価なツールを必要とするため、当面は、セキュリティサービスベンダーやIT ソリューションベンダーが中核となると思われるが、市場の拡大によっては、地方に拠点を置くネットワーク事業者やシステムベンダーやソフトベンダーが参入することも考えられる。

(3) サービスの実現にあたっての課題

このようなサービスは、ビジネスベースで行なわれるべきものではあるが、そのサービスの提供にあたっては、以下のようなことが求められる。

- 提供されるサービスついての信頼性の確立
- 利用者におけるサービスの活用の支援
- トラブル発生時におけるサービス提供者の責任の範囲
- 低価格化を実現するビジネスモデルの確立

6.4.2.3 安全機能運用代行サービス

安全機能の運用代行サービスとは、システムの運営者に代わり、その安全対策お実施を代行するものである。システムの運用を受託している場合は、そのセキュリティの確保に関する必要な施策活動は、受託の中に含まれることになろうが、ここでは、ファイアウォール等を受託側の施設におき、ネットワーク的に見るとそのユーザは、受託者の内部ネットワークとして保護されるようなサービスを指す。

現時点では、このようなサービスは見当たらないが、ネットワーク社会の進展に伴い、特にセキュリティを厳重にすべきではあるが、自分では対応が困難な利用者から、このようなサービスのニーズが生まれてくるものと想定される。

(1) サービスメニュー

このサービスのメニューは、一般的に以下のようなものなろう。

- ネットワークの内部化サービス
- 対象システムに対するセキュリティポリシー設定コンサルテーション
- 対象システムに対するセキュリティポリシー実装サービス

(2) 想定されるサービスの提供形態

このサービスは相当な技術力と高価なツールを必要とするため、当面は、IDC サービスベンダーが対応することになると思われるが、市場の拡大によっては、地方に拠点を置くネットワーク事業者やシステムベンダーやソフトベンダー、さらにはセキュリティサービスベンダー等の参入も考えられる。

(3) サービスの実現にあたっての課題

このようなサービスは、ビジネスベースで行なわれるべきものである。このようなサービスの実現について、議論しておくべき事項としては、以下があげられる。

- サービスの品質
- 責任の範囲
- コストと料金

6.5　その他の課題－ネット上でのやり取りについての公証サービスについて

ネット経由でのサービスの利用やシステムの操作は、利用機能によっては、利用者はその結果を直接目にすることができない。また、ネットでつながれたシステム同士の連動では、リアルタイムで処理が進む。このような、環境において、処理の結果に問題が生じた場合、その結果生じた紛争の処理においては、どちらのシステムに（処理を要求した側か、処理を受け持った側か）責任があるかが焦点となる。

このため、ネット上での利用者側のシステムとサービス提供側のシステム間での、ネット上でのやり取りについての事実を、第三者が証明できるスキームも必要となる可能性もある。ネット上でのやり取りについての証明サービスとは、ネットを介して処理についてトラブルが発生した場合、トラブルの背景となった事象が発生した原因やその責任の所在を明らかにするため、当該処理にかかわる関連システム間でのやり取りの事実を第三者機関が証明するものである。

このような証明サービスは、一般には必要とはされないが、今後のネット社会の進展に伴い、システムの処理に生じたトラブルが大きな被害をもたらすようなシステムが登場した場合、そのようなシステムの運営にあたっての責任や、トラブルにより生じた紛争の解決のためには、必要となることも考えられる。このため、将来に備え、ネット上でのやり取りについての公証サービスも、ネット社会の安全と信頼を支える基盤サービスの一つとして検討の対象となろう。

このようなサービスは、コラボレーションするシステム間でのやり取りを証明する技術が背景となるが、その方式によっては、当事者間だけの問題としてすむようになることも考えられる。このような場合、当然ながらこのようなサービスは無用となる。

7 新しい社会に対応するためのルールの整備

ネットワークの利用の拡大は、社会の仕組みを従来とは異なるものに代える。このためには、ネットワーク社会の基盤となることについてのルールの確立が、社会のコンセンサスを得た形で、新たに構築されなければならない。

ネットワーク社会の登場により、社会の仕組みがこれまでと変質したものなれば、当然法律も見直されなければならない。法律を含む社会的ルールの見直しが必要となる背景としてのネットワーク社会の特徴をあげると、以下のようになる。

- 遠隔処理による非対面での行為あるいは処理の発生
- 文書の電子化
- 複数の企業のサービスが複合して、一つのサービスとして利用者に提供されるようになるサービスの提供形態の複雑化
- 職場、サービス提供の場、家庭のボーダレス化による場の概念の変質
- 一つの行為の影響範囲の飛躍的な拡大
- 不正行為、迷惑行為実行の容易性
- 問題行為の追跡の困難性

7.1 ルールの見直しが必要なところ

7.1.1 ネット処理で生じたトラブルの責任の分界

ネットワーク社会におけるさまざまなサービスは、複数の企業のサービスの組合せの上で提供される場合が多くなると想定される。このシステムに何か問題が生じた場合、直接被害を被った者に対する補償、すなわち、問題を起こした者の責任の追及は、現在の法律のままでも問題はないかどうかについての見直しも必要と考えられる。

法律の見直しが必要ないとしても、このような場合における紛争の処理についての原則は改めて明確にしておく必要があろう。

ネットを介した処理の実現は、異なる企業等の責任主体が運営する複数のシステムがかかわっている場合も多い。また、一つのシステムの運営には、システムの構成要素を提供している企業、運営を担当している企業、運営の基盤を提供している企業等が多くかかわっているのが一般である。社会のネット化の進展につれて、一つのサービスやシステムの提供に、多くの企業等の責任主体がかかわるようになる傾向はますます拡大すると考えられる。

プレイヤーの具体的な例としては、消費者、インターネットサービスプロバイダ、通信回線提供者、関係機器納入業者、ソフトウェアベンダー、ホームページ管理者、メーリングリスト管理者、ショップ、モール、アプリケーションサービスプロバイダー、CA、RA、公証業者、決済業者、政府自治体等が

考えられる。

ネット経由の処理上、発生したトラブルに関しては、トラブル発生場所の特定が困難であり、また、立証が困難であるという特徴もある。

ネットを利用するサービスやシステムの提供やその利用において、何かトラブルが生じ、利用者やサービスやシステムの提供者に被害や損害が生じた場合、その責任は誰がどのように負うべきかについてについての紛争は、複雑化することが想定される。

このような事態に備えるためには、複数の企業等の責任主体がかかわって提供されるシステムやサービスに生じるさまざまなトラブルについての、責任の所在や、責任の範囲について、当事者間で紛争にならないようにしておくこと、および発生した紛争の解決についてのルールを確立しておくことも必要となる。

このルールの確立のために検討すべき事項としては、以下があげられる。

- システムにトラブルをもたらした原因別の責任分界と責任の範囲についての一般原則
- 二つ以上のシステムのコラボレーションで生じたトラブルに対するトラブルの原因個所の明確化についてのルール

ここでの中心的問題は、システム連動にかかわる責任分界である。従来、責任分界という表現は、その領域内での注意義務を尽くすことと、その過誤により生じた損害を負担することを念頭に用いられてきたと考えられる。今後は、これにとどまらず、トラブル発生場所の特定の困難さ、かつ、立 証の困難という特徴に加え、ある意味では天災にもなぞらえられるハッカーをはじめとする第三者の介入や、プログラムのバグに関する損害に関しての責任の分担に関するルールが必要となる。当事者のいずれにも帰責事由が存しない場合であっても、いずれかが責任を負うルールという意味では、危険負担の概念に近いものを想定することが必要であるかもしれない。

(1) 関係者の責任の分界の明確化

システムにトラブルをもたらした原因別の責任分界と責任の範囲の明確化において、検討の対象とすべき場合を、表 7-1 に示す。このそれぞれの場合に対し、本来的な責任者や、責任の所在を問うべき場合、利用者に対する責任や関係者に対する損害賠償の範囲等の責任の範囲や、責任が問われる者の履行義務等が議論されなければならない。

表 7-1 責任の分界や責任の範囲を明確化すべき場面

区分	関係者	事故の原因
サービス提供側	サービス提供者	業務上の不手際 システムの使用上のミス システムの不備の見逃し システムの整備、管理の不良 システム運用についての管理の不備 利用者への配慮の不足
	システム運用受託者	システム運用上の不手際
	システム構築受託者	システム構築上の不手際
	ハードソフトベンダー	通常の使用にかかわる欠陥 攻撃者に対する脆弱性 使用法についての不備
ビジネスパートナー		サービスの不備
ネットワークプロバイダー		サービスの不備
サービス利用側	利用者	サービスの不適切な使用 システム使用上のミス
	システムの提供者	通常の使用にかかわる欠陥 攻撃者に対する脆弱性 システムの使用についての指示の不備
	システム据付業者	システム据付上の不備 メンテナンスサービスの不備
	ハードソフトベンダー	通常の使用にかかわる欠陥 攻撃者に対する脆弱性 使用法についての不備
第三者	意図的な攻撃者	セキュリティホールやシステムのセキュリティホールの不備をついた攻撃やウイルスの送り込み
	踏み台にされ攻撃に参加させられた者	セキュリティ対策の不備

(2) トラブルの原因となった場所の特定についての明確化についての

サービスが二つ以上のシステムのコラボレーションで提供されているような場合、このコラボレーションにかかわるトラブルが原因の場合、その責任の所在を確定するためには、発生したトラブルはどちらのシステムの問題に起因したのかについての証明についてもルールが必要となる。

このルールは、以下を明確にするものでなければならない。

- 証明方式
- 証明のための情報についてのルール

トラブルの発生態様により、関与したプレイヤーの個々の責任に帰される問題と、複数システムのコラボレーションの際の責任をどこに帰すべきかという問題とがある。

その他、ネット上の処理で生じたトラブルによる紛争の解決を円滑におこなうために、今後、

検討を要する課題としては、以下があげられる。

- 業務上の不手際、システム使用上のミス、システムの不備の見逃し、システムの整備管理の不良、システム運用についての管理の不備、利用者への配慮の不足等に対するサービス提供者の利用者に対する、サービス提供契約における要求事項に対する履行努力の程度
- システム運営上の不手際に対するシステム運用受託者のサービス提供者に対する、契約における要求事項に対する履行努力の程度
- システム構築上の不手際をなくすためのシステム構築受託者のサービス提供者に対する、契約における要求事項に対する履行努力の程度
- 通常使用に関わる欠陥、攻撃者に対する脆弱性、使用法についての不備をなくすための、ハード／ソフトベンダーのサービス提供者に対する、製品提供にかかる契約における要求事項に対する履行努力の程度
- 損害を生じた原因立証の困難に鑑み、立証責任、または方法の法定
- 特定できない第三者の介入により発生した被害に対する救済方法

なお、サービスやシステムの利用上、利用者に生じた被害や損害に対する責任は、サービスやシステムの提供者が負うことになるのが基本としても、システムの構成要素であるソフトの不具合に問題があっても、それが汎用品であれば、製造物責任法により当該ソフトの提供者に法的責任は及ばないとされているが、システムのソフトへ依存がさらに高まれば、今後も現在のままで良いかどうかについての議論も必要と思われる。 なお、当該ソフトウェアが個別注文により作成された固有のものである場合、開発委託にかかる契約で、瑕疵担保責任は明確にされているのが一般であるため、この問題は一般には発生しない）

7.1.2 電子文書の法的効力の拡大と法的有効性の維持

ネット社会の進展につれて、ほとんどの文書は電子的に作成されようになると考えられる。このため、法的な取り扱いの対象となる電子文書に対しても幅広く、従来の書面による文書と同様の法的有効性が確保されなければならない。

このためには、

- 電子文書の法的効力の拡大
- 電子文書の長期にわたる法的有効性の確保

7.1.2.1　電子文書の法的効力の拡大

電子文書が、通常の書面と同一の効力を法的に有するかという問題であり、既にIT書面一括法でそのような効果が認められる場面が特定されている。今後の課題は、裁判管轄の合意に書面を要するとしているような例に見られるように、IT 書面一括法が対象としていない多くの書面に対して、電子文書も書面としての法的効力をもつように拡大することが必要となる。

また、電子文書の裁判上の証拠としての提示の方法についてのルールの見直しも、この課題の一つといえる。

7.1.2.2　電子文書の法的効力の維持についてのルールの確立

電子認証・署名法の成立によって、一定の要件を満たして電子証明された電子文書は法的効力を持つとされたが、その有効性は電子文書の作成から相当な期間が経過しても維持されていなければならない。通常の債権債務で20年の長期にわたり、仮に入会権等の問題に関する場合であれば50年を越えることも考えられる。

この点については、まだ課題が多い。

電子署名された電子文書の法的効力を長期にわたり維持するためには、以下についてのルールの確立が必要となる。

- **電子文書の作成時点の確認についてのルール**
- **電子署名に使われた証明書の有効期限経過後の検証についてのルール**
- **使用された暗号が破られたとか、使用した証明書を発行した認証局の秘密鍵が漏洩したとかで、保管期間中に適用した電子署名の信頼性に問題が生じた場合の扱い**

これらの課題については、法律面での対応が必要なところが少ない。

(1) 電子文書の作成時点の特定についてのルールの確立

電子文書が法的効力を持つためには、有効な証明者による電子署名が必要であるが、証明書の失効を考えると、その有効性については署名がなされた時点の確認が必要となる。このため、電子署名については署名時刻を示すタイムスタンプが押されているが、その時刻の認証においてシステム間での整合性確保についてのルールの確立にまでは至っていない。

システム間での時刻のずれは、電子署名の有効性の確認に問題を残す余地となる。このため、時刻に認証に関し信じるべき時刻の定義や、そのシステム時刻への反映や、電子署名へのに時刻の反映する方法についてのルールの確立が必要となる。

現在、さまざまな議論が行われているが、取組みの加速が要求される。

(2) 証明書の有効期限を経過した電子署名文書の真正性の確認についてのルールの確立

電子署名された電子文書の真正性の検証には、署名に使われた証明書に対応する該当

認証局の公開鍵が必要となるが、この有効期限後に電子署名された文書の真正性をこの鍵を用い検証できるようにする環境が提供されなければならない。

技術的にはさまざまな方式が提案されているが、適用する技術やその技術を用いた検証の方法等、およびそのような検証を可能にするサービスの整備等についても、早急な解決が求められる。

(3) 保管中に電子署名の信頼性に問題が生じた場合の対応についてのルールの確立

使用された暗号が破られたとか、使用した証明書を発行した認証局の秘密鍵が漏洩したとかで、保管期間中に適用した電子署名の信頼性に問題が生じた場合、電子署名された文書の法的有効性は危ういものとなる。

したがって、このような場合、該当する電子文書の法的有効性の維持のためにはどのような対処が必要かについてのルールの確立も必要となる。

7.1.3 電子情報の保護について

システムの利用や運用にあたっては、電子文書以外にも多くの情報が用いられる。これらの文書以外の電子情報においても、その改ざんやコピーが容易であるという点や、運用上の不手際や、格納媒体の損傷からすべてを失ってしまうこともそうまれでないことから、特別の配慮が必要となる。電子情報の保護や、将来、その内容の提示が必要となった場合、その真正性が証明できるようにしておくことが必要となる。

これらを適切に行えるようにするための環境作りとして、以下のような点についてのルールの確立が必要となる。

- 電子情報の保護についてのルール
- 保管されている電子情報の法的効力の確保についのルール

7.1.3.1 電子情報の保護についてのルールの確立について

電子情報の保護は、自社の事業を守るだけでなく、事業パートナーの事業の保護、ユーザや関係者のプライバシーの保護にかかわる。情報の保護は、情報に触れたり、その管理を担当し、その保護が義務付けられている者の責任に帰する問題であるが、実務としての保護を完全にすることは難しい。

電子情報の保護に対して、現実的な取組みを推進するための環境作りとして、以下が求められる。

- 電子情報の保護についての責任範囲
- 電子情報の不正入手や改ざん、破壊等の抑止につながる罰則の制定

保管された電子情報の真正性の検証を行うためには、以下に示すようなことが確立していなければならない。

(1) 電子情報の保護についての責任範囲

情報の保護に関して紛争が生じた場合、何処までその保護に努力していたかが問われることになるが、電子情報の保護は、システムに対するセキュリティ対策の組込みだけでなく、システムの運用や業務の運用もかかわり、保護のために行うべきことが多く、そのすべてに完全を求めることは難しい。

このため、一般に求められる保護策のレベルを示す電子情報の保護についてのガイドラインの確立も求められる。

(2) 電子情報の保護を侵害する行為を牽制するための罰則規定の制定

不正入手とその不正な使用の対象が個人情報の場合は、現在審議中の個人情報保護法が、その不正入手の手段がシステムへの不正アクセスのよる場合は、不正アクセス防止法が適用できる。また、企業等の機密情報の不正入手やその流布は、不正競争防止法が適用できる場合がある。

しかし、この両法律の適用ができない場合も少なくない。このため、電子情報全体を対象とした、不正入手や改ざんや破壊行為に対しても、法により行為者を処罰できるようにすることも必要となる。

また、情報漏洩による損害賠償請求が認められるとした場合には、いかなる範囲の損害に賠償を認めるかについても検討する必要があろう。

7.1.3.2 電子情報の法的効力の確保についてのルールの確立

作成時点から法的効力の確保を必要とする文書以外にも、長期にわたり、その内容の真正性の確保が必要とされる電子情報は多い。将来、これらの参照が必要になった場合、その真正性について疑義がでないようににしなければならない。

このためには、将来の参照時に、その真正性の検証が問われるような電子情報の作成や保管方法や、真正性の検証についてのルールが確立されていることが必要となる。

- 電子情報の真正性の検証方法の確立
- 電子情報の保管を自ら行う場合における保管についてのルール
- 電子情報を公証人等への預託についてのルール

また、これらについて法的な効力を与えるため、法律面での対応も必要となる。

(1) 電子情報の真正性の検証方法の確立について

保管された電子情報の真正性の検証を行うためには、以下に示すようなことが確立してい

なければならない。

- 適切な技術に裏付けられた検証方式の確立
- 適用される検証方式の法的な有効性の付与

電子文書と同等な扱いをするようにすることもできるが、文書と違い、保管の対象となる情報が数的に多いことと、形態が多岐にわたること、および個々の保管対象の情報量が圧倒的に大きいこと等で、その方式には工夫が必要となろう。

電子文書と同じ扱いにする場合は、先に示した課題が存在する。

(2) 電子情報の保管を自ら行う場合における保管についてのルール

電子情報の特性から、その管理には、いくつかの側面から留意する必要がある。保存方法については、まず、保存媒体ごとに、物理的な脆弱性がありたとえば、磁気、高温、力など)、それぞれの媒体ごとの管理基準ルールが必要となる。また、媒体間のデータの伝送の際のエラーの可能性を検証する手続ルールや、バックアップをとる基準ルールも必要である。

適用される方式にあわせ、その作成や保管について、真正性の検証に耐えられるようにするためのルールを決める必要もでてくる。

(3) 電子情報を公証人等へ預託する場合のルールの確立について

電子情報の真正性を署名する手段として、第三者に預託する方法もある。このような方法を有効なものとするためには、電子情報の第三者への預託に関し、以下のようなことについての検討が必要となる。

- 第三者への預託による真正性の検証の有効性についての合意の形成
- 適用される検証に対する法的効力の付与

第三者への預託による電子情報の真正性の検証を有効なものとして確立するためには、電子情報に対する技術的な要件を示す検討適用する技術の妥当性に加え、電子情報作成側での情報の作成や保管、第三者への預託の方法、第三者機関での情報の保管等についてのルールも確立していなければならない。

データ預託等の場合には、受託者の関わりの程度 例えば、データ内容を公証するか、データ内容には関わらないかなど)、運用管理基準などを明らかにするルールも必要となる。

また、データ保存が長期にわたるような場合に、特定のアプリケーションに依存するデータの場合には、見読性の確保も重要であり、アプリケーション確保、またはデータ・コンバートのルールも必要となる。

7.1.4 プライバシーの保護および個人情報の確保について

ネットワーク社会にあっては、ネット上のシステムの多くに個人情報が多く存在しているため、個人情報の漏洩が起こりやすいことや、ブロードバンドネットワークの普及により、リモートモニタリングの私的使用が拡大することもあって、なりすましによりこの機能にアクセスすれば簡単に他人の生

活を覗き見ることができる。また、ネット上の掲示板の使用やメールの配布等により、プライバシーにかかわる情報の流布も容易となる。

このため、プラバシーの保護はについては、現在以上に厳しい対応が必要となる。このような環境にあっても、最近、重要視されてきたプライバシーの保護を実現するためには、以下がその課題としてあげられる。

- ネットの利用におけるプライバシーの侵害となる行為の明確化
- ネット上でのプライバシーの侵害行為を処罰または牽制するためのルールの確立
- システム上の個人情報の保護の実務についてのルールの確立

参考 1)

プライバシー保護の問題と、前節であげた情報保護の問題は次元が異なる。前者は、自己の私的な情報内容が公にされることに関する支配権の問題であるのに対して、後者は、自己の情報それ自体に関する管理権の問題である。

プライバシーの保護は、一般に我が国では憲法13条幸福追求権を根拠として、論じられる問題である。一方、情報保護の問題という場合には、単に情報それ自体が盗まれる、またはそれに不法にアクセスされたことが問題である。不正に取得された情報が個人にかかわる情報で、漏洩された情報が公にされた場合にはプライバシーの問題にもなる。

参考 2) 現在、国会で審議中の個人情報保護法における個人情報の保護にかかる原則

内容は、利用目的による制限（4条）、適正な取得（5条）、正確性の確保（6条）、安全性の確保（7条）、透明性の確保（8条）に関して、国、地方自治体、および個人情報取扱事業者にそれぞれ一定の義務を課すものとなっており、監視機関の命令に従わない場合には、懲役または罰金が科される。

(1) ネットの利用におけるプライバシーの侵害となる行為の明確化

例えば、社員の受発信したメールの管理者による閲覧がなされている場合がある。自社内システムの利用を業務関連に限定するなどの就業規則の有無や、管理者による検閲を予め公にしているかなど、取り決めの態様によっては、プライバシー侵害になることもある。これは一例であるが、今後登場してくるネットのさまざまな利用場面ごとに、どのような行為がネット上でのプライバシーの侵害に当たるかを明確にすることも必要となる。

(2) ネット上でのプライバシーの侵害行為を処罰または牽制するためのルールの確立

法的なレベルでの刑事上の処罰や、民事責任を課すことによる侵害行為の牽制は、現在のところ基本的には、リアルな世界と変わらない。具体的には例えば、名誉毀損や不法行為などである。ただ、ネット上のプライバシーの侵害は、放送や出版と比べて、安価、即時、かつ広範に情報が配布拡散する点という特性があり、差し止めや謝罪広告といった救済方法がリアルな世界と比べてどれだけ有効かは疑わしい。従って、ネット上でのプライバシー保護を法的なルールで徹底しようとする場合には、一般抑止効果を重視して一層重い責任を規定する方向に進むことになると想定され、侵害行為の定義を前提としたルールの確立が必要となる。

(3) システム上の個人情報の保護の実務についてのルールの確立

意図的なプライバシー侵害を行う者のみならず、結果としてプライバシーの侵害になる行

為をしてしまった者や、個人情報の漏洩や配布に関わるシステム管理者もプライバシー侵害に重大な関わりがある場合が多いと想定される。その不手際がプライバシーの侵害につながるシステム上の個人情報や業務上での個人情報の保護についての原則は、現在国会審議中の個人情報保護法で示されるものの、実務において何処までの努力が要求されるのかについては、事業者や当事者の判断に任されている。

個人情報の保護は、その実務上の努力に大きく依存するため、実務上の努力の目標を示すガイドラインの確立も必要となる。個人情報保護の実務の厳格性についての要求は、扱う個人情報の内容や量によって異なるため、このガイドラインは業界単位に作られることが望ましい。

7.1.5 ネット上での不正行為や迷惑行為に対する課題

ここでいう不正行為は、犯罪行為や禁制品の売買等を意味するもので、法的に民事責任を問う不法行為とは、区別される。また迷惑行為とは、刑事罰や行政罰の適用にまでは至らないが、さまざまな手段を通じて行われる迷惑な行為を指す。ネットワークにおいては、迷惑行為や不正行為が影響範囲が広範かつ安価に行われ、かつ一般に加害者の痕跡をたどることが困難であるという特徴を有するが、その被害は場合により非常に深刻なものになる可能性がある。

このような行為の例としては、以下があげられる。

- 禁制品の販売等、法律で禁止されていることのネット上での実行
- システムへの不正なアクセスによるシステム上の情報の不正な取得や改ざん、破壊、プログラムの改ざん、破壊、システム機能の不正な使用、システム運用の妨害
- ウイルスの作成、配布によるシステム上の情報の不正な取得や改ざん、破壊、プログラムの改ざん、破壊、システム機能の不正な使用、システム運用の妨害
- DoS 攻撃によるシステム運用の妨害
- スパムメールの送りつけ
- ネット上の掲示板や無差別に多くのあて先にメールを送るなどして、他人の誹謗、中傷を行うこと、流言飛語を拡散すること
- ネット上の掲示板や無差別に多くのあて先にメールを送るなどして、攻撃方法を教示し、情報の不正取得や第三者のシステムに対する攻撃を誘うこと

このような行為が蔓延するのを防ぐためには、行為者を牽制したり、ネットワークプロバイダー等においてこのような行為の場を与えないようしたり、行為者を処罰できるようにすることが必要となる。

これらの行為の抑止のためには、技術的な対応も必要であるが、技術以外に関しても以下にあげるような課題がある。

- 一般の商行為等が、迷惑行為にならないようにするためのルール

- 不正行為や迷惑行為を行った者を特定することを可能にするルールの確立
- 迷惑行為の実行者の処罰を可能にするルールの確立
- 不正行為や迷惑行為の原因を作ったり、実行を助長した者の処罰を可能にするルールの確立
- 不正行為や迷惑行為の実行の場を提供している者に対する、行われている不正行為や迷惑行為への対応についてのルール

(1) 迷惑行為の実行者の処罰を可能にするルールの確立

発信者の特定を含む必要事項の記載やオプトアウト条項を義務付けた「特定電子メールの送信の適正化等に関する法律」は、スパムメールとそうでない広告メールの線引きを示したものである。このように、何が迷惑行為として禁止されるべきものであり、かつ、該当する行為を取り締まれるようにするためのルールは、迷惑行為のさまざまに対して準備されなければならない。

今後、このようなルールを検討すべき迷惑行為としては、以下があげられる。

- ネット上の掲示板や無差別に多くのあて先にメールを送るなどして、他人の誹謗、中傷を行うこと、流言飛語を拡散するような行為

(2) 不正行為や迷惑行為を行った者を特定することを可能にするルールの確立

ネット上での不正行為や迷惑行為の実行者を特定するためには、ネットワークプロバイダーの協力が欠かせない。プラバシーの保護とからみ、そのルール作りは容易ではないが、早々に、ガイドラインの確立や、必要な法律の整備について一定の答えをだすことが必要となろう。

(3) 不正行為や迷惑行為の原因を作ったり、実行を助長した者の処罰を可能にするルールの確立

現時点では、ウイルスの作成者や、セキュリティホールの存在を示しその攻撃方法を示したり、特定のシステムの脆弱性をネット上で公表したりする行為自体を直接取り締まる法律はない。ウイルスの作成、保持、配布については取締りができるための法整備について、現在、検討中ということであるが、ウイルスの作成等に関するだけでなく、広くこのような行為を取り締まれるようにしなければならない。

(4) 不正行為や迷惑行為の実行の場を提供している者に対する、行われている不正行為や迷惑行為への対応についてのルール

特定のシステムをターゲットとしたDoS攻撃や、掲示板サービスを用いた誹謗、中傷、流言の流布等は、ネットワークプロバイダーがそのような行為に場を提供していることが多い。したがって、このような行為の抑止にもネットワークプロバイダーの協力が必要となる。このような場合における、ネットワークプロバイダーの協力を得るためには、表 7-2 に示すようなことについての検討が必要となる。

表 7-2 迷惑行為等に対するネットワークプロバイダーの義務についてのルール

検討対象	要検討事項
提供しているサービスの上でこのような行為を予防するために必要な手段の組込みについてのルール	・抑止に効果的な技術が存在している場合におけるそのような技術のシステムへの組込みにを義務つけるようなルール
提供しているサービスの上でこのような行為が行われていることが発見された場合、取るべき処置についてのルール	・行為の差し止めについてのルール ・行為者の公表に関するルール

(5) 不正行為や迷惑行為の存在を知ったときの対処についてのルール

ネット上で、不正行為や迷惑行為、プライバシーの侵害行為、不正に取得されたと思われる情報の流布、明らかにデジタルコンテンツの権利保護を侵害しているような行為を発見した者についての義務等についても、何らかのルール化がなされることも望ましい。

また、このような行為を知った者が、関係当局や被害の対象者に通知することを奨励する制度の導入も検討の対象となろう。

7.2　ネットを利用するサービスやシステムの提供に対する規制の適用について

問題が生じた場合、社会的な不安を惹起するような取り扱いに慎重を要するサービスやシステムについては、その安全性が一定の水準に達していることが求められる。このことを確実にするためには、安全性の確保についての努力目標を示し、その実現を指導するだけに止まらず、特定のサービスやシステムに対しては、その提供を制限する規制の適用も検討する必要もある。

この規制は、そのトラブルがネット社会の安全と信頼に影響を与えるようなシステムにおける、

- ネット社会の安全と信頼全体に影響を与えたり、トラブルが利用者の生命、身体、財産に直接的な被害をもたらすようなシステムにおける事故の予防
- ネットを利用するサービスやシステムの提供者の責任の明確化

を目的とするもので、対象となるサービスやシステムが必要とされる安全対策が講じられていることを前提に提供を認められるようにするものである。

これは、原子力プラント、薬品、航空機、自動車、電車、民間航空サービスも、経済産業省や総務省の認可を必要としている考え方を、ネットワークサービスにおいても、必要なものに対しては同じような考え方を適用すべきという考え方による。

7.2.1　検討すべき公的な規制の枠組み

ネットを用いるサービスやシステムの提供を制限する規制としては、以下の３つのレベルが考えられる。

- 提供にあたっては、個々のサービスやシステムごとに、指定された要件が満たされていることを、公的あるいは公的機関に準ずる機関による安全性についての厳格な審査に合格しなければならないとする規制
- 運用にあまり依存しないパッケージ的なシステムの販売は、公的あるいは公的機関に準ずる機関による安全審査に合格しなければならないとする規制
- 事業者が一定の資格を有することを前提にサービスの提供が認められるとする規制

それぞれのタイプについての基本的な考え方を、表 7-3 に示す。

規制のタイプ	規制の大枠義	対象となるサービスの特性と対象となるサービス例	
サービスの提供やシステムの運用にあたっては、対象サービスやシステムの個々に公的機関あるいは公的機関に準ずる機関、あるいは業界団体等によるその安全性についての審査に合格を条件とする規制	・その提供にあたっては当該システムに要求される安全性の確保についての取組みが十分であることが、公的機関あるいは公的機関に準ずる機関による審査で認証されること ・サービス提供の認可は審査の有効期間内に限られる ・サービス提供の認可は、有効期間内に再審査に合格すれが延長できる ・再審査に合格しないまま、有効期間が経過した場合は、認可は取り消せる ・認可期間内においても、サービスやシステムの安全性に著しい欠陥がある場合、サービスの提供やシステムの利用を、一時停止にしたり、認可を取り消したりできる	その安全対策上の不備は、ネットワーク社会の安全と信頼に対する不安を醸成したり、トラブルが広範囲に広がる可能性のあるサービスおよびシステム ・ネット社会の安全と信頼を支える基盤サービス 検討の対象となるサービスやシステムとして考えられるもの： 認証サービス、電子文書の公証サービス、時刻認証サービス他） ・その安全対策上の不備は、利用者の生命、身体､財産に直接的に被害を及ぼしたり、プライバシーの侵害に直結するようなサービスやシステム 検討の対象となるサービスやシステムとして考えられるもの： 遠隔医療サービス、医療機関システムの一部、行政機関のシステムの一部、大量の個人情報を扱うシステム他）	当 項 ・ ・ ・
提供にあたってシステムの型式単位に公的機関あるいは公的機関に準ずる機関、あるいは業界団体等による安全性についての審査に合格することを条件とする規制	・審査および認可は、システムの型式単位に行われる ・その提供にあたっては当該システムに要求される安全性の確保についての取組みが十分であることが、公的機関あるいは公的機関に準ずる機関による審査で認証されること ・認可後に安全性に著しい欠陥がある場合、改善の指示や使用の停止指示、認可の取り消しができる	汎用に販売提供されるパッケージ的なシステムで、その安全対策上の不備は、利用者の財産に損害を与えたり、プライバシーの侵害につながるようなもの ・家庭用のリモートモニタリングシステム ・リモートコントロールができる家庭用機器 ・家庭用のセキュリティゲートウェイ ・認証ツールの一部	当 項 ・ ・ ・
サービスの提供にあたっては事業者が必要な資格を有することを条件とする規制	・審査は事業者単位 ・有効期間が過ぎた場合再審査を必要とする	サービスを提供する事業者の信用が問われるサービス ・安全支援サービス	当 が ・ ・ ・ 有

7.2.2 規制の適用について検討すべき事項

このような規制の導入について、その必要性の是非も含め検討すべき事項としては、表 7-4 に示すようなことがあげられる。

表 7-4 導入にあたって検討を要する事項

表 7-4 規制の導入についての検討事項

検討項目区分	検討が必要な事項
規制の要否とその適用範囲	・このような規制の要否 ・提供する規制のタイプ ・対象とすべきシステムについての考え方と適用範囲の原則
認可の条件	規制の対象となるサービスやシステムごとの審査基準 審査の方法
運用スキーム	・認可機関とその責任 ・審査機関の条件およびその責任 ・審査料、審査機関のビジネスモデルと事業性 ・申請から審査、認定、認定サービスやシステムの管理の手順
法的な裏づけ等の規制実施のための環境の整備	・対象システムの提供を規制する法律の整備 （サービスやシステムの提供の条件、問題が生じた場合の責任他を規定） ・審査基準のベースとなる対象システム種別に対する安全対策プロファイルの確立

7.2.3 規制の導入についてのアプローチについて

特に、規制の要否については十分な検討が必要となる。ネットを用いるサービスやシステムの安全性は、提供する事業者の自主努力に任せるのが本来であり、このような規制は必要最低限に止めなければならない。このため、このような規制の導入にあたっては、関係する業界だけでなく、社会全体としてのコンセンサスの確立が必要となる。

特に、検討の対象となるサービスやシステムを提供する業界との間では、以下についての詰めが必要となる。

- 個々の事業者の自主努力の実態や業界での自主規制の適用も配慮した公的規制の要否
- 規制を行う場合の規制の大枠
  －対象システムにおける適用範囲、審査事項、審査基準、有効期間、事業者の責任の範囲等
- 審査手続き等の運用形態

8 その他の課題

ネット社会の安全と信頼の構築のために検討が必要なその他の課題としては、以下があげられる。

- 脅威や脅威への対応についての情報の提供形態の改善
- 利用者のネット社会における脅威についての認識の醸成と自己責任能力の向上
- トラブルが生じた場合の被害者ならびに知らないうちに加害者になってしまった者に対し一定の救済を行えるようにする保険の整備や救済機関の整備

8.1 脅威および脅威への対応に関する情報の提供形態の改善

ネットワーク社会を支えるシステムのまわりの脅威は、日々進化して言っても過言ではない。また、技術や使用できるツールの進化と共に求められる安全対策も継続的に変化しているとみなければならない。この結果、昨日までの対策は通用しなくなることも珍しくない。

このような環境にあって、ネットの利用を安全で信頼できるものにするためには、新たな脅威の出現や、これらへの脅威への対応について助言となる情報は、ネット経由でのサービスを提供する事業者、ネット利用システムを提供する事業者、システムのセキュリティを支援する事業者だけでなく、利用者にとっても不可欠のものとなる。

現在においても、さまざまなところからさまざまな情報の提供が行われているが、これらの情報を利用する立場からは改善が求められるところが少なくなく、今後、このような情報の提供形態の改善についての議論が必要と考える。

8.1.1 提供が求められる情報

ネットワーク社会における安全と信頼の向上のために、提供が求められる情報をあげると、表 8-1 のようになる。

表 8-1 ネットワーク社会の安全と信頼の向上のための情報

	情報区分	情報の内容等
1	一般情報、脅威情報	・セキュリティ一般情報、トピックス ・脅威情報 －蔓延しているトロイの木馬やワーム、ウイルス情報等の一般脅威情報 －被害が広がっている拡散しているワーム、ウイルス、DoS 攻撃等についての情報等の警報情報
2	制度関係情報 （注）	・制度の紹介、変更等の紹介 ・制度の利用に関する情報
3	製品情報	・製品の使用方法に関する情報 ・セキュリティホール等の汎用製品における安全上の問題に関する情報
4	各種信用情報	・事業者としての信用についての情報 －オンラインマーク、プライバシーマーク ・製品・サービスに対する認証情報 －CCの取得、ISMSの取得

（注）オンライントラストマーク制度やプライバシーマーク制度や ISMS 評価認証制度等の、ネット社会における安全と信頼の確保に関係する評価認証制度

8.1.2 情報の提供についての課題

このような情報の提供にあたっては、その情報の利用者が適切に利用できる形で提供されることが望ましい。情報の洪水では、情報の利用者は自分が必要な情報を見逃すことになる。これらの情報は該当するシステムにおける対策に結びつくものでなければならない。

このため、ネット利用の脅威についての情報の提供においては、さまざまな利用者の技術レベルを意識した対策に結びつく情報の提供の実現が求められる。

このことの実現に向けて検討すべき課題としては、以下があげられる。

- 情報提供を統合的に行う体制の整備
- 利用しやすい情報としての提供の実現

(1) 情報提供を統合的に行う体制の整備

現在、セキュリティに関する情報の提供は、IPA や JPCERT/CC 等の公的機関や、プラットフォームベンダーやセキュリティサービスベンダー、情報セキュリティ関係団体の多くから、さまざまな形で行われている。

ビジネスベースでユーザに特化した情報の提供が行われているケースも含め、ユーザは多くの情報の洪水にさらされているものの、それらの活用は低調であると見られている。このような現状を打開するためには、ユーザは一つの提供元だけをウオッチしていれば済むようになることが期待される。このためには、セキュリティについての情報提供を統括的に行う体制の

確立も検討の対象となる。

このような体制の確立には、現在、セキュリティ情報を提供している公的機関、企業、団体、研究機関等の多くの組織の協力が必要となる。このような体制の整備には、表 8-2 に示すような事項についての検討が必要となる。

表 8-2 情報セキュリティに関する情報提供に体制の整備についての検討課題

	情報区分	情報の内容等
1	情報する情報と提供についての工夫	提供する情報・・・・提供する情報の体系とレベル分けと利用者セグメント別の提供内容 情報の提供形態・・・どんなチャネルを用いてどのような方法で提供するか（使用チャネル、提供手段あるいはアクセス手段他）
2	提供体制	提供機関のタスクと位置付け 協力機関と提供機関の関係 情報の管理元・・誰が情報を提供するのか 情報の責任元・・だれが情報内容に責任を持つのか コスト負担の原則
3	利用条件	利用条件（含むコスト負担） 基本情報については無料とし、情報のレベルに応じ有料とすることも考えられる。

(2) 利用できる情報とての提供の実現

提供される情報は、利用者の技術レベルにかかわらず、当該情報が対象とする利用者に有効に使用されなければならない。このためには、以下の課題についての解決が求められる。

- 提供情報の利用者セグメント別の作成

  ネットの利用者の技術レベルはさまざまである。このため、提供される情報は、利用者のセグメントごとに利用できる形に工夫されたものでなければならない。

- 情報提供方法の工夫

  必要とする者に必要な情報を遅滞なく届けるためには、利用者への情報の提供方法についての工夫も重要となる。工夫すべき事項としては、以下があげられる。

  ・情報のクラス分け（緊急、普通、注意、警告、指示等）

  ・利用チャネル（メール、Web 利用等）

  ・提供手段あるいはアクセス手段（プッシュ型かプル型か等）

(3) 提供情報についての相談サービスの整備

情報の利用者が IT に不慣れな層に拡大することを考えると、提供情報の有効な活用のためには、利用者に対する、内容の説明や対処についての指導を行うサービスの提供も必要となる。このことの実現には、必要な体制の確保が必要となるため、上記の情報提供機関だけでは対応が難しく、6.4 節に述べたような安全支援サービスの提供機関がその一部を分担することも含め、その実現のスキームを検討しなければならない。

8.2 利用者の自己責任能力の向上

生活やさまざまな社会的な活動の中におけるネット経由のサービスの利用やネット利用システムの使用においては、これらの利用にかかるリスクに対し、利用者も応分の責任を持たなければならない。

すべての責任を製品やサービスの提供者に課することは、健全なネット社会進展の阻害要因の一つともなろう。このため、ともすれば利用者の責任をあいまいにしがちな日本の社会においても、社会のネットワーク化の進展に対応して、利用者側にこれらの使用におけるリスクについての認識と、利用上生じるトラブルについての自らの責任の範囲についての認識を十分に植付けなければならない。

8.2.1 利用者が認識すべき事項

ネット社会を構成するさまざまな仕組みを利用するにあたって、その安全と信頼に関し利用者が認識すべきことをあげると、表 8-3 のようになる。

表 8-3 利用者がネット社会の安全と信頼に関し認識すべき事項

項目	備考
ネット経由のサービスの利用やネット利用システムの使用にかかわる脅威の存在	・システムへの不正なアクセス、侵入、コンピュータウイルス、通信の盗聴等、ネットワークシステムを脅かすものの存在とその概要 ・脅威が利用者にもたらすトラブルや被害の概要
ネット経由のサービスの利用やネット利用システムの使用にあたっての自らの責任の範囲	・ネット経由のサービスの利用やネット利用システムの使用にかかわる利用者の責任についての原則 ・用いる装置の設置や諸設定にかかる責任の範囲 ・使用する装置や利用環境の維持管理についての責任 ・トラブルが生じたときの必要な処置
被害にあった時に行うべき処置	・被害に対し適用される救済の大枠 ・被害救済のための必要な手続きの大枠

8.2.2 利用者の責任の範囲

ネット経由のサービスの利用やネット利用システムの使用上で生じたトラブルのうち、その原因が以下のものについては、利用者がその責任を取らなければならないと思われるが、これらについても専門家の議論を通じたコンセンサスの確立が必要となろう。

表 8-4 IT 製品やネットワークサービスの利用上生じたトラブルのうちその責任が利用者側にあると考えるべき場合

利用者の責任に帰すると考えられる場合	備考
システムを使用したりサービスの提供を受けるにあたって利用者の責任で導入でしなければならない装置等の不備 ・ 装置の設置ならびに諸設定の不備（メンテナンスの不備も含む） ・ セキュリティ対策上の要求事項についての必要な機能や必要なパラメータの設定の不備	ただし、一般的に考えられる装置の故障や誤動作や、よくあるセキュリティ対策上の要求事項についての違反の一部については、製品やサービス提供側のシステムで事故に結びつかないようにすべき課題であるため、利用者の責任に帰するのは、提供者側として十分な配慮を施したものを、利用者がないがしろにするような範囲に限定される。
利用上の留意事項についての違反があった場合 ・ 利用上の注意事項の重大な違反 ・ セキュリティ対策上要求されている装置の維持管理上の重大な不手際	ただし、一般的に考えられる操作上のミスや、利用装置の維持管理にかかる不手際は、製品やサービス提供側のシステムで事故に結びつかないようにすべき課題であるため、利用者の責任に帰するのは、提供者側として十分な配慮を施したものをないがしろにするような範囲に限定される。

利用者の責任の範囲についての一般原則は、上記のようになろうが、その責任の範囲は個々の製品やサービス毎に明示されるべきものである。

8.2.3 必要な施策

IT に縁遠い老齢者、家庭の主婦、子供等も含み、ネットワーク社会におけるさまざまな仕組みの利用者に広く、その利用にあたっての脅威と、自らの責任についての認識を浸透させるためには、表 8-5 に示すような施策も必要となろう。

表 8-5 利用者の啓蒙に必要な施策

啓蒙手段	教育すべき内容
公的機関による公法、宣伝 各種サークル活動の場での教育 学校等の教育の場での教育	基本認識の醸成 ・ IT 機器やネットワーク経由でのサービスの利用における脅威の存在 ・ 利用者の責任に関する原則 ・ 利用にあたっての安全対策上の基本事項 ・ トラブルに遭遇した場合のおける対処の基本
ネット経由でのサービスやネットワーク利用システムを提供する事業者等による教育	個別サービスやシステムの利用についての教育 ・ IT 機器やネットワーク経由でのサービスの利用における脅威の存在 ・ 利用にあたっての安全対策上の留意事項 ・ 利用にあたっての利用者の責任の範囲 ・ 生じたトラブルについての提供者の責任の範囲 ・ トラブルに遭遇した場合における対処の方法

8.3 保険の整備

ネット経由のサービスの利用やネット利用システムの使用、あるいはその提供において生じた被害の救済のための保険の整備も、また、ネットワーク社会の安全と信頼を構築するためには必要となる。

整備が求められる新しい保険としては、に示すようなものが考えられる。

表 8-6 検討の対象となるセキュリティインシデントに対する保険

区分	保険の対象となる被害等
利用者に対する、ネット経由のサービスの利用やネット利用システムの使用にかかる保険	・外部からの攻撃による事故でシステムに生じた被害 ・外部からの攻撃によるシステムの意図しない動作で生じた被害 ・外部からの攻撃により他社サイト他の攻撃の踏み台とされ外部に与えた損害の補償 ・利用者の不手際が原因の事故によりシステムに生じた被害 ・利用者の不手際が原因で生じたシステムの意図しない動作により生じた被害 ・利用者の不手際が原因で外部に与えた損害の補償
事業者に対する、ネット経由のサービスやネット利用システムの提供にかかる保険	・外部からの攻撃による事故でシステムに生じた被害 ・外部からの攻撃によるシステムの意図しない動作で利用者に生じた被害 ・外部からの攻撃により他社サイト他の攻撃の踏み台とされ外部に与えた損害の補償 ・自社の不手際が原因の事故によりシステムに生じた被害 ・自社の不手際が原因で生じたシステムの意図しない動作により生じた被害 ・自社の不手際が原因で外部に与えた損害の補償

これらの保険の整備にあたっては、以下のような事項についての検討や市場のコンセンサスの確立が必要となる。

- 保険の対象となる損害とその原因の範囲
- 被害を生じさせ事故の責任社区分の特定ルール
- 事故の責任区分を特定するためにシステムに求められる技術的事項
- 被害者の責任の範囲の判断についてのルール
- 間接的加害者になった場合の責任の範囲の判断ルール
- 保険料の設定ルール

8.4 紛争処理機関の整備

ネット経由のサービスの利用やネット利用システムの使用において生じたさまざまなトラブルによる被害者と関係者の間の紛争は、ネットワーク社会の進展と共にその件数は急激に増加するものと思われる。これらの紛争の一部は、保険の整備により保険会社の手で対処されることになろうが、

その一部は法廷に持ち込まれることになろう。

これらの紛争の特徴としては、

- 被害額の認定が難しい
- 件数が多く、事象は多岐に渡る
- 責任の所在の明確化が難しい
- 責任の分担について専門的な知識が必要とされる

このため、被害額が比較的低い事案については、一般市民が気楽に相談できるような ADR（法廷外紛争処理機関）を整備し、この機関での処理が行えるにすることが望ましい。

これらについては、現在、実証実験中である電子商取引にかかる ADR をベースに、この機関の処理の対象を電子商取引からネットワーク社会のさまざまな事象に広げることにより対応することも検討の対象になる。

紛争処理機関の整備の推進のために、今後、検討すべきこととしては、以下があげられる。

表 8-7 ネット社会対応紛争処理機関整備の課題

項目	概要
紛争処理機関の運営スキーム	・対象とするトラブルとサービスの範囲 ・紛争処理の基本原則 ・運営体制と事業性の確保
対応専門家の育成	・ネット社会に特有なトラブルに対応できる専門家の確保、育成 ・業務に必要な教育の継続的な実施

8.5 サイバーセキュリティについての統合機関の設立

ネットワーク社会の安全と信頼の確保の基盤となるサイバーセキュリティについては、多くの分野にわたる活動が必要となる。現在これらについては、多くの国家機関や民間の団体がさまざまな活動を行っているが、ネットワーク社会の進展に伴い、これらの活動をより効果的活効率的なものにするためには、これらの活動を統括することも必要である。

民間の活動を制約するわけではないが、表 8-8 に示すような機能、活動については、国家レベルでの統括が必要と思われる。

表 8-8 統合が必要なサイバーセキュリティについての機能

機能・活動区分	保険の対象となる被害等
サイバーセキュリティに関する政策の提言	・ネットワーク社会の安全と信頼に関する課題の整理 （課題マップの作成とその維持） ・ネットワーク社会の安全と信頼の構築に必要な政策の提言
関係する基準の制定	・IT 機器当に対するセキュリティ基準の制定と維持 ・ネットワークサービスに求められるセキュリティ基準の制定と維持
関係する制度の運用と、その維持	・装置、システム、サービスについてのセキュリティ評価認証制度の運用とその維持管理 ・ISMS 評価認証制度の運用とその維持管理（ISO/IEC17799 準拠） ・IT 製品のセキュリティ評価認証制度のうんようとその維持管理 （ISO/IEC15408 準拠）
サイバーセキュリティに関する情報の提供	・注意勧告の発令 ・脅威情報の提供 ・事故事例と教訓の提供 ・新しい技術に関する情報の提供
サイバーセキュリティの向上のための技術開発の促進	・開発課題と取組み状況についての情報の整理と提供 ・共同開発の場の提供 ・開発費の支援
サイバーセキュリティに関する啓蒙 教育の推進	・利用者の啓蒙のための資料の作成配布およびセミナー等の開催 ・セキュリティ担当者向けのセミナーの開催 ・専門家向けのセミナーの開催
サイバーセキュリティに関するさまざまな議論の場の提供	・関係する専門家による合同シンポジュームの開催 ・各種研究会の主宰

これらの機能、活動を担当する機関の設立の検討にあたっては、以下にあげる事項についての議論が必要となる。

- このような統合機関の必要性
- 設立するとした場合の機関の形態と位置付け－既存機関との関係
- 事業内容
- 体制と運営の方法

8.6 ネットワーク社会の安全と信頼の確保にかかわる教育の充実

ネットワーク社会の安全と信頼の向上のためには、まず、ネットワーク社会の仕組みを提供する事業者やネットワークサービスを提供する事業者における経営者や当事者、さらにこれらを管理する機関の当事者が、ネットワークの利用システムにおける脅威とこれらの脅威への対応について十分な認識とスキルを持っていることが必要となる。

さらに、利用者にもサイバー社会における脅威の存在と自己の責任についての認識とこれらの

利用にあたって必要となるスキルの習得が必要となる。

これらを実現するためには、表 8-9 に示すような教育の充実が求められる。

表 8-9 サイバーセキュリティについての充実が必要となる教育

教育対象者区分	主たる教育内容	主たる教育機関
セキュリティ専門家（含もう予定者） ・研究者 ・セキュリティ技術、製品開発者 ・セキュリティコンサルタント ・セキュリティサービス提供者	・情報セキュリティ技術一般 ・情報システム構築、運用管理論 ・サイバーセキュリティ関連法制ならびに制度	・一般大学 ・専門高等教育機関（注）
IT 製品、システム、ネットワークサービスの提供事業者の経営者および管理者	・IT 製品やネットワークサービスの提供にかかる脅威と事業者としての責任 ・関係する法規等の事業上準拠すべきルール	・専門高等教育機関
IT 製品、システム、ネットワークサービスの開発および運用担当者	・サイバーセキュリティにかかる基本スキル ・担当する業務に必要な専門的なスキル	・一般大学 ・専門高等教育機関
利用者	・ネットワーク社会における脅威 ・IT 機器やネットワークサービスの利用上の留意事項と自己の責任 ・トラブルが生じた場合の対処の基本	・公的機関での市民教育活動の中での教育 ・各種市民運動の中での啓蒙、教育 ・小、中、高等学校

(注) ここで言う高等専門教育機関とは、後述の大学卒業生や社会人を対象とした大学院レベルのサーバセキュリティを専門とする専門家育成機関構をさす。このような教育機関は、現在、存在せず、一部でその構想についての議論が行われている段階である。

これらの教育の充実に関し、教育機関別の課題をあげると、表 8-10 のようになる。

表 8-10 教育機関別の課題

教育対象者区分	課題
情報セキュリティ専門高等教育機関	・ このような教育機関構想の位置付けとその必要性 ・ 教育対象者とカリキュラム ・ 事業性の見通し ・ 必要な教官の確保
一般大学、大学院 ・ 情報セキュリティの実務家の育成	・ 専門課程でのカリキュラムの再構築 ・ 大学院でのカリキュラムの再構築 ・ 実務家育成のための教官の確保
小、中、高等学校 ・ネットワーク社会の仕組み ・サイバーセキュリティにおけるの脅威の存在 ・ネットワーク社会での安心の確保についての自己の責任	・教育内容の確立 ・教員への必要な教育の実施
公的機関や市民団体等 ・自分で守るネットワーク社会での安全の確保のための	・ネットワーク社会における脅威 ・IT 機器やネットワークサービスの利用上の留意事項と自己の責任 ・トラブルが生じた場合の対処の基本

9　高度ネットワーク社会における“安心と信頼”の確保に向けた提言

以上の考察より、ネットワーク社会の進展に備え、その安全と信頼の確保にのために、今からと組むべき重要課題としては、以下があげられる。

⑴ ネットワーク経由で提供されるサービスやネットワークを使用するシステムの安全性を評価できるスキームの確立

この課題に関するテーマとしては、以下があげられる。

- 安全性評価モデルの確立
- 安全対策実施基準の確立
- システム種別ごとの全性対策プロファイルの整備
- システムの安全性評価認証サービスの導入

⑵ ネットワーク社会の安全と信頼を支える仕組みの整備推進

この課題についてのテーマとしては、以下があげられる。

- ネット上での認証スキーム
- 時刻認証のスキーム
- 電子文書の法的効力の確保の仕組み
- 電子情報の法的効力の確保の仕組み
- 技術的弱者である一般利用者等の安全を支援するスキーム

⑶ システム間のコラボレーションで生じたトラブルの責任の所在を明確にするスキームの確立

この課題についてのテーマとしては、以下があげられる。

- 責任の所在の分界と責任の範囲についてのルールの確立
- 責任の切分けを実現する技術的方式の確立と対応ツールの整備推進

ここでは、重要と思われるもののみを取り上げた。いずれも難解な問題であるが、官民一体となって、技術とその適用環境およびルール等が一体となった有効な対策の確立に向けて、官民一体となった取組みが期待される。

参考

米国における情報システムの安全性評価・格付けサービスの現状

本調査研究において、その主要テーマの一つであったシステムの安全性評価モデルや、この評価モデルをベースとした安全性の評価サービスに関する米国の状況について調査を行った。本参考は、この調査で得た、このテーマにかかる米国の状況を纏めたものである。

米国における情報システムのセキュリティ評価・格付けサービスの現状

1. はじめに

現時点では米国においても、現状は人的、技術的、管理的なセキュリティ対策を網羅した情報セキュリティマネジメントシステムを総合的に評価し、格付けするような標準（Rating Standard）や、格付けサービス（Rating Service）は存在しない。だたし、情報システムのセキュリティを総合的に評価し、評価結果を納得のいくランク付け（Rating）で表現することに対するニーズは低くない。

また、Rating Standard を策定しようという試みが、数年前から始まっている。しかし、Rating Standard を作り上げるには、調査・検討・考慮すべきことがあまりにも多く、課題は広範囲にわたっており、この試み自体がまだ端緒についた段階と言える。

また、情報セキュリティシステムを格付けするという試みは、政府主導で行われているのではなく、情報セキュリティシステムの安全性評価のニーズを痛感している金融や保険、医療など民間側のアプローチが主である。情報システムの安全性評価のニーズは様々であり、そのニーズに応じたセキュリティ評価（Security Assessment）サービスは、すでにビジネスベースで展開されている。

2. 政府主導での情報システムのセキュリティに対する評価・格付け標準の策定について

政府主導で情報システムセキュリティに対する標準的な格付け基準を策定しようという動きに対しては、民間からの抵抗、反発が大きく、政府自体もこの分野は能動的に動いていない。セキュリティポリシーやセキュリティプロシジャー、セキュリティ対策は、政府に規定されて実施するものではなく、あくまでも個々の会社のビジネスモデルに適合した施策を、自社のリスクを見据えて選ぶべきという意見が大勢を占めている。

これは、以下のような問題が大きく立ちはだかっていることにもよる。ある会社の情報システムのセキュリティレベルが E（未対策）と格付けされたとすると、その会社はビジネスがたちゆかなくなる可能性がある。上位ランクに格付けされるためには、相当のセキュリティ対策コストが見込まれるが、対策コストの投資効果（ROI= Return Of Investment）が測定不可能なため、政府の標準に従い、セキュリティ対策を施し、ランク付けされるということに対しては、大変な抵抗がある。また、セキュリティをめぐる環境はダイナミックに動いており、例えば一旦 A ランクに格付けされたとしても、新しい脆弱性が発見されたり、ネットワークに新しいサーバが設置されたりするだけでセキュリティ環境は変化し、そのランク付けがいつまで有効性を保てるか見定めが難しいという問題もある。

現在情報セキュリティに関して米国政府が主導的に動いている分野は、個人情報保護に関する分野で、しかも①金融関係、②ヘルスケアの 2 分野に限られている。この分野は個人情報が漏洩した場合、個人が蒙る被害が甚大であるため、特別に政府が個人情報の保護に関する規定を設け

ている。

なお、政府の情報セキュリティシステムの調達に関しては、ISO/IEC15408 の Common Criteria に則った製品・システムの調達方式が採用されている。但し、政府のオーダを受けるためにセキュリティシステムの格付けサービスを受けなければならないという規定は存在しないし、そのような格付けサービスも存在しない。

3. 重要インフラの情報セキュリティに対する米国政府の取組み

1998 年、当時のクリントン大統領主導の下、"Presidential Decision Directives - PDD63"という指令が策定された。これは、通信、エネルギー、金融、交通等々の重要インフラの事業継続性、実行可能性を確保するために、重要インフラの情報システムの脆弱性を削減するために官民一体となって取り組むように指示した文書であり、情報セキュリティにおける初期の安全保障体制を作り上げるのは 2000 年までを達成目標とし、国家の重要インフラを守る情報セキュリティの安全保障体制を稼働させ、またそれを維持する体制の確立は 2003 年を目標としている。また、重要インフラの情報システムに潜在する脆弱性に対処するための基本ガイドラインも定められている。

この指令の下、官民一体となった努力が続けられ、2003 年 2 月に"The National Strategy to Secure Cyberspace"という文書が策定された。これは、サイバースペースにおいて国の経済や国民の生命を守るための基本戦略を纏めたものである。サイバースペースの特性に始まり、サイバースペースの安全保障のための本質的事項が網羅的に記載されている。この中に記載されているサイバースペースの安全保障のために民間がとるべきアクションは、法的に遵守すべき事項（規定）ではなく、推奨事項(recommendation)という位置づけである。

4．システムの安全性評価のニーズ

システムの安全性の評価が必要であるというニーズは高いが、そのニーズの内容は業態により異なっている。現在、米国で提供されているシステムの安全性の評価・格付けサービスは、個々のニーズに対応したものとなっており、サービスの組み立ても多様である。

米国におけるこれらのサービスへのニーズの背景としては、以下についての期待があげられる。

- セキュリティインシデント発生時における免責効果
- 企業自体や提供するサービスや製品の信頼性の向上
- セキュリティインシデントに 対する保険の適用

1）セキュリティインシデント発生時における免責効果への期待

金融業界やヘルスケア（医療サービス）業界に対しては、個人情報保護に関する規制が厳

しいと記載したが、個人情報が漏洩した場合、訴訟される事態は十分に考えられる。訴訟の際の罪状をできるだけ軽微にするため、ベストプラクティスという考え方が導入されている。すなはち、セキュリティ対策に最善を尽くした（ベストプラクティス）にもかかわらずシステムへの侵入等により個人情報が漏洩した場合、その企業の罪は、ベストプラクティスの無い、またはセキュリティレベルの低い（未対策の）企業より軽微ですむという考え方である。このために、セキュリティレベルを評価する民間のサービスはあるが、それは人的、技術的、管理的なセキュリティ対策の必要項目を網羅し、情報セキュリティマネジメントシステムを総合的に評価し、格付けするようなものではなく、脆弱性検査やペネトレーションテストによる検査、各社のスキャンツールによるサービス等、各社各様である。

2）企業自体や提供するサービスや製品に対する市場での信頼の向上

政府や金融機関、大企業など、自社の情報セキュリティシステムの安全性について、第三者の認定を受けたいというニーズはある。金融関係の取引にしろ、企業間取引にしろ、政府調達にしろ、取引の電子化は加速度的に進展している。その際、電子商取引の安全性を担保する何等かの証明書が有効な場合がある。また、様々な会社と取引をする時、その会社のセキュリティレベルはどうなのかを把握した上で取引をしたいというニーズがある。例えば顧客が取引銀行を選定する場合、その銀行がどれだけのセキュリティ対策をしているかは重要なファクターとなる。そのため、信頼できる第三者より認定証を得られれば、少なくともそれが無い他行よりは、有利に顧客獲得を進められる。

このようなニーズを反映して、様々な認定サービスが提供されている。これらのサービスは、セキュリティ対策の度合い、脆弱性対策の度合いをスコアで示し、ある一定の基準に達すれば認定マークを発行するというものである。認定証は、WEB に掲載してその安全性を自社のホームページで公表することができるようにすることから"Web Site Seal Program"とも呼ばれており、主要なサービスとして、表 1 に示すようなものがあげられる。

表 1 米国における代表的な安全性評価と認定マークサービス

サービス名	サービスの概要
FoundSecure FoundScore Risk Rating	セキュリティ対策の度合い、脆弱性対策の度合いをスコアで示し、ある一定の基準に達すれば FoundSecure 認定マークをホームページに掲載できる。後述の項目6を参照
Trusecure	セキュリティ評価を実施し、一定レベルに達すれば、TruSecure 認定マークをホームページに掲載できる。後述の③E-Risk Insurance を参照
WebTrust	米国の公認会計士協会が運営する、会計監査のフレームワークに沿った Web サイトの安全性保証サービス 。業務開示、取引完全性、情報保護の 3つの観点から Web サイトの安全性を保証しており、認定を受けた事業者は WebTrust マークをホームページに掲載できる。
VeriSign	Secure Site 認定シール

3）セキュリティインシデントに対する保険の適用（Risk Insurance）

保険業界では、サイバーアタックやサイバーインシデントの被害を補償する保険がある。この場合、セキュリティ対策を施している会社に対しても、施さない会社に対しても一律にサイバーアタックやサイバーインシデントの被害額に応じた保険を支払うことは不可能である。そこで、セキュリティ対策の度合いに応じて保険を支払うという考え方が導入されている。そのためにセキュリティ評価のシステムが必要であり、TruSecure 社という会社は保険会社から委託を受けて情報システムセキュリティの安全性評価を実施している。評価結果が一定のスコア以上の会社は、TruSecure 認定マークをホームページに掲載できる。

5. 金融業界における情報システムの安全性評価基準策定の動き

金融業界における情報システムの安全性確保についての取組みを示すものに、The World Bank (世界銀行)のセキュリティ専門家によって纏められた下記文書がある。この文書は、金融業界での情報システムの安全性評価基準策定の動きを示すものである。

文書名：Risk Mitigation in Financial Transactions – Public Policy Issue

著者： Thomas Glaessner, Lead Financial Economist in the financial Sector Operations and Policy Department of the World Bank

Tom Kellermann Data Risk Management Specialist

Valerie McNevin Security Information Officer and Privacy Officer for the State of Colorado

決済の電子化が進んでいる金融業界においては、デジタルマネーをサイバースペースに存在する脅威からいかに守るか、また、金融機関の情報セキュリティシステムの安全性をいかに評価するかが大きな課題になっている。この文書では、表 2 が示すように、健全な電子セキュリティ基盤を構築するための柱となる、8つの主要ドメイン（eight key pillars）を設定し、その 8 番目のドメインで、電子セキュリティ（E-Security）を守るための 12 の施策（12 Layer of E-Security）について述べている。

この提言は金融業界からのアプローチとはいえ、他の業界にも敷衍できる性格のものであり、例えばシンガポール政府はこのフレームワークを採用している。

この研究を始めるにあたって、ISO/IEC17799 をベースとして考察を進めたが、本書で述べられているセキュリティ対策・評価のアプローチは、ISO/IEC17799 と異なったものになっている。これは、この研究チームの ISO/IEC17799 に対する評価が、ISO/IEC17799 は原理原則であり、例えば現実の脅威となっている数千から数万とも言われる脆弱性・脅威に対する対応や、VoIP、その他の新技術に対するセキュリティに関しても触れられていないように、現実のサイバースペースの安全を守るための具体的なセキュリティ施策については触れられていなく、システムの安全性を客観的に評価するには不十分であるというとこらからきている。

表 2　"Risk Mitigation in Financial Transactions"のフレームワーク

施策ドメイン	内容
Pillar I	Legal Framework and Enforcement　(法的フレームワークと規制)
Pillar II	Electronic Security of Payment Systems　(決済における電子セキュリティ)
Pillar III	Supervision and Prevention Challenges　(監督及び防御の試み)
Pillar IV	The Role of Private Insurance as a Complementary Monitoring Mechanism (モニタリングメカニズムを補完するものとしての民間保険会社の役割)
Pillar V	Certification, Standards, and the Roles of the Public and Private Sectors (証明書、スタンダード及び官民の役割)
Pillar VI	Accuracy of Information on E-Security Incidents and Public-Private Sector Cooperation　(電子セキュリティ事故における情報の正確さと官民セクターの協力)
Pillar VII	Education and Prevention of E-Security Incidents (教育と電子セキュリティ事故防止)
Pillar VIII	The 12 Layers E-Security　(12 の電子セキュリティ対策要求事項) **電子セキュリティを守るための12 の施策** 1. Information Security Officer 2. Risk Management 3. Access Controls/Authentication The first line of defense is access controls; these can be divided into passwords, tokens, biometrics, and public key infrastructure (PKI). 4. Firewalls 5. Active content filtering 6. Intrusion detection system (IDS) 7. Virus scanners 8. Encryption 9. Vulnerability testing 10. Proper systems administration 11. Policy Management Software 12. Business Continuity/Incident response plan (IRP)

6. FoundSecure 社の評価･格付けサービス－"FoundScore Risk Rating サービス"

Foundstone 社は、大手監査系会社の情報セキュリティグループ出身者が中心となって 1999 年に設立された会社で、業務の中心はネットワーク診断、セキュリティコンサルティング、教育訓練、FoundScan (ネットワーク診断ツール)の販売、FoundSecure プログラム等々である。今回の訪問調査では、Rating Service の一形態としての FoundSecure プログラム (FoundScore Risk Rating)について、その評価プロセス、脅威の度合いに応じた脆弱性の分類、スコア計算方法、ランク付け、FoundSecure 認定マーク、価格、市場等について説明を受けた。

1）FoundSecure プログラムにおける安全性評価プロセスと認定マーク

Step#1(第一段階)　— コンサルティング

第一段階の評価事項を、表 3 に示す。

表 3 第一段階での評価事項

評価事項	内容
Penetration Test	擬似ハッキングによるネットワーク診断 （ネットワークの規模によるが平均 2 週間位の期間がかかる）
Recommendation	ネットワークの脆弱性を削減するためのセキュリティ対策を推奨
Fix Recommendation	推奨されたセキュリティ対策の実施
Verify Fix	セキュリティ対策が有効に機能しているかを確認

上記に要する期間　– 平均 1～2ヶ月間

第一段階の実施費用　– ネットワーク環境により異なり、都度見積。

Step#2 (第ニ段階)　— 脆弱性診断と認定マーク

① FoundScan MVAS（Managed Vulnerability Assessment Service）の Subscription

第一段階が完了すると、FoundScan（脆弱性診断ツール）を使ったオンライン脆弱性診断を行う。この脆弱性診断は、主にカリフォルニアの本社の専門チームが FoundScan ツールを用いてオンライスキャニングをすることにより行われる。脆弱性診断サービスを定期的に受けるために顧客が加入するサービスが FoundScan MVAS（FoundScan 脆弱性評価サービス）である。年間加入費用はネットワークの規模により異なり、例えば最低料金として、32IP アドレスに対する脆弱性診断サービスの費用は 1 年間で約$25,000 である。価格はネットワークの規模に依存し、脆弱性診断の回数には依存しないため、1 年間で何回脆弱性診断を受けても費用は同じである。診断は外部からのエクスターナルスキャン、内部からのインターナルスキャンの両方が可能。

脆弱性診断は診断の要請を受けてからおよそ 72 時間後に行われる。この時間は、診断を要請されたIP アドレスが確かに要請した会社に属するものであり、競争相手のIP アドレスなどではないことを事前に確認するために必要な時間である。

② 脆弱性診断の対象範囲、規模、精度、速度、レポート

システムの規模、複雑さネットワークの数にかかわらず脆弱性診断が可能で、独自の技術と言語（FASL）により高速で精度の高い診断が可能。例えば、255IP アドレスの脆弱性診断の所要時間は約 20 分。診断内容は GUI より診断項目をチェックすることにより選べる。複数のネットワークの診断結果（スコア）の一覧表示や、個々のネットワーク診断結果の詳細表示もできる。

③ FoundSecure 認定マーク

この診断によりスコア（Found Score）が 90 点以上の会社は FoundSecure 認定マークをホ

ームページに掲載できる。但し、次の評価でスコアが 90 点に満たない場合、認定マークは取り消されるというダイナミックなシステムである。

② スコア（Found Score）の計算方法

スコアは 100 点満点からの減点方式で採点され、Vulnerability の観点から 4 項目、Exposure の観点から4 項目について検査した結果がVulnerability の数や Exposure の数、または Yes/No で示され、各々の項目に重み付けをした結果得られた点数を減点していくことにより総得点（Total Score）が計算される。表 4 にスコアの計算イメージを示す。

なお、以下は一般的なサンプルであり、何をハイリスクとするかは、個々の会社のポリシにより異なることがあるため、コンサルティングにより、重み付けや脅威レベルをカスタマイズすることがある。

③）ランキング

スコアに応じてネットワークの安全度がランク付けされる。スコアとランク付けの関係を、表 4 に示す。

表 4 スコアの範囲　ランキング

スコア	ランキング
0 – 25	Poor
26 – 50	Below Average
51 – 70	Average
71 – 85	Above Average
86 – 100	Excellent

④）診断結果の対策と管理 – VulnTrank

ネットワーク環境の弱点を FoundScan により発見した後に、必要なセキュリティ対策の実施をトレースするVulnTrank というシステムを導入。これにより、「診断の実行―対策担当者の任命―対策作業―対策の検証」という作業が確実に行われたかどうかをトレースできる。対策実行後に再度脆弱性検査を行い、スコアとランキングを決定し、このサイクルによりネットワークのセキュリティを向上し、90 点以上のスコア以上を獲得した会社・機関には FoundSecure の認定証が与えられる（FoundSecure 認定マークをホームページに掲載できる）。

⑤）セキュリティ環境変化の把握 － Trending

セキュリティ評価結果が出ても、セキュリティ環境は日々変化している。その変化をスコアの推移により図示し、時系列でセキュリティ環境の変化を見られるようにするのが Trending（トレンドの把握）である。これにより、セキュリティ管理者は、セキュリティレベルの推移を視覚的に理解することができ、セキュリティレベルが下降傾向にあれば、それを上昇させるような対策を取るのである。

表 5　評価におけるスコアリングのイメージ

満点　　**100 点**

FoundScore:　Vulnerabilities	結果	重み付け	減点数	減点後のスコア	減点の上限
High Risk Vulnerabilities ルートなどの権限が奪取される可能性のある脆弱性の数	20	2.5	50	50	50 points
Medium Risk Vulnerabilities 非特権ユーザなどの権限が奪取される可能性のある脆弱性の数	7	0	0	0	10 points
Low Risk Vulnerabilities 他の情報と組合せた場合に脅威となる可能性のある脆弱性の数	34	0	0	0	5 points
Vulnerabilities の各項目の点数を減じた後のスコア				**50**	
FoundScore:　Exposure	結果	重み付け	減点数	減点後のスコア	減点の上限
Number of Non-Essential Services DNS, FTP, HTTP, HTTPS(SSL), SMTP, SSH 以外のサービスの数	6	1	6	44	20 points
Number of Machines with No-Essential Services 非特権ユーザなどの権限が奪取される可能性のある脆弱性の数	4	1	4	40	15 points
UDP Permitted 53(DNS)以外の UDP サービス(inbound)が許可されているか？	Yes	-	10	30	10 points
ICMP Permitted ICMP サービス(inbound)が許可されているか？	Yes	-	5	25	5 points
Vulnerabilities/Exposure の各項目の点数を減じたトータルスコア				**25 点**	
ランキング				**Poor**	

注：Vulnerabilities の得点は 50 点満点からの減点法。High Risk Vulnerabilities で
すでに 50 点減点されたため、Medium とLow で減点項目があっても減点数は 0である。

6）FoundSecure プログラムの顧客

顧客は政府や金融機関、連邦航空局（FAA- Federal Aviation Administration）、大企業等のミッションクリティカルなユーザ。現在保険会社にE-Risk Insurance の損害賠償額決定のための基準として FoundScore プログラムを採用するように働きかけている。

7）市場と将来の見込み

セキュリティ評価により情報システムの安全性を評価し、ネットワークの安全性向上に努め、また変化するセキュリティ環境に動的に対応したいというニーズはミッションクリティカルなユーザに根強く、このビジネスは始まったばかりとはいえ、将来の大幅な成長が見込めるとの見解。

メンバーリスト

本調査研究参加メンバー

チーム１　高度ネットワーク社会像のスケッチ）

前川　　徹	早稲田大学	大学院国際情報通信研究科
相原　憲一	名古屋商科大学	経営情報学部
新保　　豊	株式会社日本総合研究所	研究事業部

チーム２　高度ネットワーク社会における安心と信頼の確保についての課題）

井上　陽一	株式会社ヒューコム	代表取締役社長
石橋　泰博	株式会社東芝	コアテクノロジーセンター
浦山　清治	株式会社ヒューコム	e-Government 推進室
木村　道弘	日本電気株式会社	IT 基盤システム開発事業部
佐藤　慶浩	日本ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ株式会社	コンサルティング統括部
下村　正洋	株式会社ディアイティ	代表取締役社長
菅　　知之	関西大学	総合情報学部
宮崎　一哉	三菱電機株式会社	情報総合研究所
安田　直義	株式会社ディアイティ	営業本部
山崎　文明	ｸﾞﾛｰﾊﾞﾙｾｷｭﾘﾃｨｴｷｽﾊﾟｰﾄ株式会社	代表取締役社長
土井　悦生	翔国際法律事務所	弁護士
吉田　一雄	清和大学	法学部

事務局

重松　孝明	電子商取引推進センター
川村　尚哉	電子商取引推進センター