# 情報ネットワークの情報セキュリティ対策とリスクマネジメント

杉野　隆

情報ネットワークシステムにおけるネットワーク構造，情報セキュリティに関する最近の動向を概観する．IPネットワーク化の動向は，社会経済におけるリアルタイム化，グローバル化の動向と本質において一致していることを明らかにする．情報ネットワークをめぐる危機管理，リスクマネジメントに焦点を当て，具体的に，企業情報ネットワークにおける信頼性確保対策のIPネットワーク化に対応した変化，ネットワーク社会におけるサイバーテロを紹介する．また，情報セキュリティ対策のためには，情報セキュリティマネジメントシステムの確立が必要だが，人的セキュリティ対策が最重要の課題である．

キーワード：情報ネットワーク，情報セキュリティ，危機管理，リスクマネジメント，情報セキュリティマネジメントシステム

## 1. 情報ネットワークシステムの現状

パソコンの価格対性能比が大幅に向上し，インターネットが普及したため，メインフレームコンピュータを中心とするクローズドシステムであった情報システムは，オープンシステムに置き換えられ，ネットワークを介して相互に接続され，グローバルシステムになった．インターネットは，企業，政府，自治体に至るまで，組織の情報活動を支援し，情報サービスを提供するための重要な基盤となった．個人においても，コミュニケーション活動の手段として定着しつつある．一方，1990年代になってから，ネットワークの利用形態も大きく変化した．ネットワークに接続される端末数は飛躍的に増大し，しかも，固定端末から無線/携帯端末へと拡大し，情報ネットワークの位置付け，重要性は，まったく変質してきたといえる．

情報ネットワークにおける最近の主な転換点をいくつか挙げてみよう．

- 1985年：通信自由化により，通信事業者がNTT1社から複数事業者の競争状態になった．
- 1990年：日本IBMが日本語DOS/V機を発売し，パソコンを完全にオープン化した．
- 1995年：MicrosoftのWindow 95にTCP/IPが標準装備され，インターネットが普及拡大するきっかけとなった．パソコン市場ではWindows系がde facto standardとなった．
- 2000年：中央官庁などのホームページへの不正侵入が多発し，官公庁，企業における情報セキュリティの脆弱性が露呈した．I LOVE YOUウイルスの出現により，コンピュータウイルス被害件数が過去最高となった．また，携帯電話とPHSを加えた契約数が，加入電話とISDNを加えた固定電話契約数を超えた．
- 2001年：コンピュータワームCodeRed, Nimdaが出現し，米国における同時多発テロとともに，サイバー攻撃の現実性が認識された．
- 2003年：コンピュータワームSQL Slammerが出現．広帯域ネットワークがウイルスの拡散を早めるという弱点を露呈し，またハードディスク上のファイルを検査する以外の新たなウイルス対策手法の必要性の警鐘となった．

## 2. どのように変化してきたか

フランスの都市計画研究家であり，速度の哲学者といわれるポール・ヴィリリオは，情報通信技術の急激な進展に伴う大きな社会的変化を，加速化された社会と捉えた．確かに，これまで，速度の上昇によって文明は進歩してきた．コミュニケーション技術からみると，情報を伝達（運搬）する手段は，人から馬や船，汽車というように移動速度を速めることにより，より早く伝達することを実現してきた．電話の発明により，コミュニケーションのリアルタイム化が実現したが，これは会話に限定されていた．現在では，インターネ

すぎの　たかし
国士舘大学 情報科学センター
〒154-8515 世田谷区世田谷4-28-1

ットと携帯電話の普及，マルチメディア通信技術の普及により，いつでもどこでも何でもリアルタイムに送れるようになった．ヴィリリオは，電子通信によって実現した情報通信速度を“絶対速度”（光速度）と呼んだ．あらゆる時間がリアルタイム化，グローバル化され，逆にローカルタイムは喪失された．われわれの社会，生活の“速度”は大きく変貌している．あらゆる活動が同期化し，活動範囲が拡大しつつある．企業においては，他社との競争に先んじるために，迅速な意思決定がよしとされる．迅速な意思決定は，意思決定のパターン化を促し，プロセスよりも結果を重視することになる．消費者の欲望もショートサイクルとなり，オンデマンドでないと満足しなくなっている．速度の上昇によって文明は進歩したが，逆に世界は（その速度ゆえ）相対的に矮小化されつつある．あたかも生物が老化とともに身体が萎み，手足が萎縮し，運動神経が鈍くなるように，この世界もまたどんどん萎縮していく．いわば“速度の増加”が“世界の老化”を招いているのだという[1]．

1990年代からのネットワークにおけるさまざまな変化も，この社会的変化と同期していると思われる．すなわち，

① ネットワーク技術は，TCP/IP, Windows/UNIXというde facto standardが中心となる．

② 通信トラフィックは，固定通信から固定・移動混在通信に移行しつつある．電話端末数では，すでに固定より携帯が上回っている．コンテンツは，音声中心から，データとマルチメディア中心へと移行しつつある．

③ 広帯域化，ネットワーク料金の低廉化，端末機器の低廉化が急速に進んだ．

④ ネットワークサービスは，通信事業者が通信サービス品質（QoS）を保証するギャランティ型サービスからベストエフォート型サービスへと移行しつつある．

## 3. ネットワークはビジネスツール

従来，企業情報ネットワークは，企業活動のインフラストラクチャであり，さまざまな事業を支援する共有資源であると考えられていた．まず，2，3年以上にわたる音声トラフィック，データトラフィック，テレビ会議のようなマルチメディアトラフィックの予測を行い，事業所相互間の利用量を算出する．その結果に基づき，トポロジ設計，中継回線の帯域・回線設計，ノードの設計，信頼性設計といった手順を踏んでネットワーク設計を行い，費用対効果を算定する．事業形態の大きな変化が予想しにくかったことと，ネットワークに接続される端末機器（PBX，ホストコンピュータ，端末機，テレビ会議装置など）は高価であり，短期間での増設，廃止は想定されていなかったことから，このようなアプローチが可能であった．

しかし，イントラネットやeコマースの実現など，ネットワークは業務ツールの一部として使いこなさねばならない時代となった．企業間のダイナミックな提携に伴い，ネットワークの対象となる事業所，関連会社は新設，合併，廃止をダイナミックに展開する．したがって，ネットワークは，企業におけるこのような事業形態，業務形態の変化に応じて，アウトソーシングを含めて，柔軟に対応できる形態であることを要求される．IPネットワークは，そのような要請に的確に対応しているといえる．

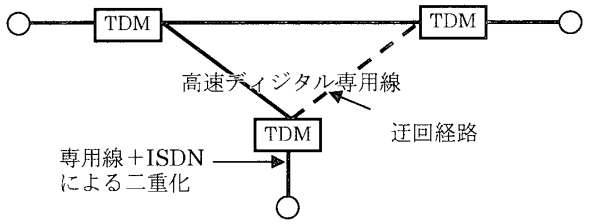
このような情報ネットワークをめぐる変化を踏まえ，企業情報ネットワークをめぐる危機管理，リスクマネジメントを中心に，最近の動向について述べたい．

## 4. 企業情報ネットワークの信頼性確保

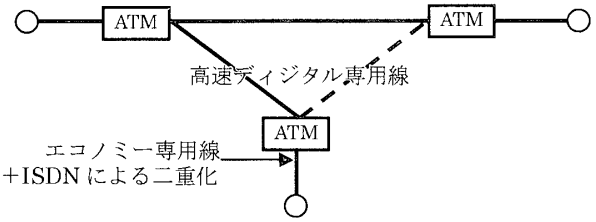
従来の大規模企業情報ネットワークは，通信事業者から高速ディジタル専用線（HSD）を借用し，時分割多重装置（TDM）で，メディアごとにチャネルを，すなわち通信速度（帯域幅とも呼ばれる）を固定的に割り当て通信サービス品質を保証する，ギャランティ型通信が中心であった．ネットワークの構築にあたっては，所要トラフィックを想定し，コスト，運用面を考慮し，最適なトポロジと回線速度，通信機器構成を決定する．ここで，ある企業が，複数の主要拠点と複数のその他事業所（関連会社でもよい）から構成されていると仮定しよう．拠点間（幹線）と拠点-事業所間（支線）ではネットワークに要求される信頼性は異なる．拠点間にはより重要なデータが流されることと，幹線には拠点間のデータばかりでなくその他事業所からのデータも流される．したがって，ネットワーク全体の信頼性の確保にとって，幹線は特に高い信頼性を要求される．そのため，次のような回線設計を行うことになる．例えば，幹線はHSDを三角網に構成して迂回化させ，支線では，HSDとISDNのような高速公衆網を組み合わせて二重化する．音声，データ，マルチメディアの各トラフィックは時分割多重装置（TDM）で多重化されてHSDに流される（図1(1)）．

その後，チャネルを有効利用するために，TDMでチャネルを固定割付するのではなく，データをパケット（セル）化し，専用線上に混在して転送するフレームリレー/非同期転送方式（ATM）の形態に移行した．データの発生は変動するため，TDMでは，チャネルに空きが発生するが，ATMではチャネルを共用するため，空きの発生確率が少なくなり，回線の使用効率は改善される．同じ速度の専用線であれば，同じ料金で，より大量のデータを流せることになる．あるいは，同じトラフィックを流すのであれば，より低速の専用線で十分であり，通信料金を節減できる（図1(2)）．

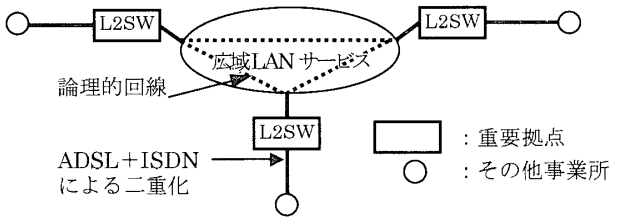
1985年の通信自由化後に出現した新規通信事業者（NCC）は，当初はNTTと同じ通信サービスを低価格で提供するのみであった．1997年にNTTが再編され，地域電話会社と長距離電話会社に分割されると，HSDにおいて，県内，県間に分けた料金形態の異なるエコノミー専用線が提供された．また，ATMをベースとした専用線サービスが提供され，回線のバックアップ形態の異なるサービスクラス，保守形態の異なる保守クラスという概念が導入された．ユーザは，ネットワークの重要度と料金に応じて，信頼性の異なる回線種別から選択できるようになった．また，支線部では，NTTのみで回線を二重化すると大きなコストがかかるが，NTTとNCC（電力系）の回線を敷設すれば，別系統の設備による二重化を容易に実現できる．




(1) 固定チャネルの割り当て，重要拠点間のみ二重化




(2) フレームリレー/ATMによる回線共有，重要拠点間のみ二重化




(3) 広域LANサービスの利用，完全メッシュ化

図1　企業情報ネットワークの形態の変遷

しかし，2000年頃から，さらにコストを削減するために，幹線にはTCP/IPによるイントラネット（自営網）の構築，又はインターネット（公衆網）の利用という形態が多くみられるようになった．前者には，広域LANサービスを利用するか，インターネットサービスプロバイダのネットワーク内でVPN（仮想私設通信網）接続するIP-VPNがある．広域LANサービスは，1G/10Gビットイーサネットの標準が制定されたことにより，長距離の拠点間でもレイヤ2スイッチ（L2SW）又はルータを簡略化したレイヤ3スイッチ（L3SW）を介してイーサネットで直接転送することが可能になったものである（図1(3)）．後者では，インターネットをファイヤウォールとVPN装置を利用して接続し，専用線的に使用する．いずれの場合も，IPネットワークである．

IPネットワークは，フレームリレー/ATMと同様の考えにより，データをパケットに分割し，通信回線上を混在して流すため，特定の端末間に固定された帯域を保証するわけではない．したがって，端末間の通信サービス品質を保証するためには，端末間の帯域制御，他の通信サービスに対する優先制御が必要となるが，これはユーザ自身の責任で設定しなければならない．また，その他事業所などを拠点に接続するための専用線は，ADSLのような安価な専用線に置き換えられ，信頼性確保のためには公衆電話網，ISDNなどとの二重化によって，コストを抑制しようとしている．しかし，ADSLには回線障害が多く，しかも，回線切替装置は確実には動作しないこともあり，ネットワーク管理者を悩ませている．

このように，TCP/IPネットワークにおいては，計画/設計に時間をかけるよりも，企業ニーズに合わせて迅速にネットワークを構築し，それをいかにうまく運用するかに重点がある．

## 5．危機管理とリスクマネジメント

Crisis Management（危機管理）とRisk Management（危険管理）は区別して論じられるべきであろう．危機とは，時と場所を選ばず発生する異常事態によって政治経済活動，企業活動，社会生活が混乱し，

社会不安を引き起こすような緊急事態をいう．例えば，国家間の紛争が核戦争のような危険に発展しないように，事前に危機を回避するための了解や規則の体系をつくろうとする政策が危機管理といわれる．危機管理の考え方は，1962年10月のキューバ危機ののち，米ソ間で本格的に定着するようになった．最近では，2001年9月の同時多発テロ，2003年3月のイラン戦争がある．日本では，1977年に近藤三千男の『危機戦略』で最初に使用されたようであるが，一般には，1995年1月の阪神淡路大震災，同年3月の地下鉄サリン事件などを契機に，危機管理ブームともいうべき現象が生じた．その後，2001年のハワイ沖の実習船えひめ丸沈没事故において政府の危機管理が問題となった．

一方，リスクは，災害，自然災害による損失，従業員の死亡，障害などによる人的損失，賠償責任損失といった損失が発生する可能性をいう．ビジネスチャンスも，果敢に挑戦して失敗すれば損失を蒙ることになるからリスクである．企業経営におけるリスクマネジメントのルーツには，1920年代のドイツにおける悪性インフレに対する企業防衛のための経営政策，1930年代のアメリカにおける大恐慌に対して企業防衛のために登場した保険管理などがある．リスクとは，このように，企業などの倒産，著しい業績不振を招来する事態などを意味することが多い．日本では，1970年代に，技術革新，新製品の開発，経済の国際化，多国籍企業の登場に伴う企業の管理リスク，海外進出リスク，各種戦略リスクを的確に処理するための経営戦略として，リスクマネジメントが要請されるようになった．最近では，2000年夏に大規模な食中毒事件を起こした企業の目に余る詐欺事件があり，極めて優良であったこの企業は，ほぼ解体された．いったん事件や事故を起こし，そのリスク対応を誤ると企業イメージや信頼を取り戻すことが不可能になる，典型的な例であった．したがって，危機管理は，国家，社会レベルでのリスクマネジメントということもできるが，二つのマネジメントは混同して使われることが多い．

1990年代前半までは，企業におけるリスクマネジメントは，主として保険あるいは財務的リスクへの対応策であった．1995年の阪神淡路大震災を契機の一つとして，業務，環境，情報などに領域が拡大された．日本規格協会の中に「危機管理システム規格検討委員会」(1998年9月にリスクマネジメントシステム規格委員会として再編成された）が設置され，危機管理システムの標準化を目指した検討が始まった．そのころISOでもRisk Management Systemの規格化が検討され，日本からの提案とする狙いもあった．2001年に，「リスクマネジメントシステム構築のための指針」(JIS Q 2001）がJIS化され，いわばリスクマネジメントは制度化された．

危機管理にしろ，リスクマネジメントにしろ，管理のための手段には，回避（リスク発生源との断絶)，低減（損失発生の抑制（予防)，発生源の分散，発生した損失の局限化・拡大防止（防護))，移転（損害保険の利用等）がある．

コンピュータウイルスを例に，これらの手段を例示しよう．ウイルス被害を回避するためには，例えば，パソコンをインターネットに接続しないという対策があるが，これでは明らかに業務の遂行を著しく損なうことになろう．低減策には，予防，軽減，分散などの方策がある．ウイルス対策ソフトを各パソコンにインストールすることは，被害の予防策として有効であるが，定期的にウイルス定義ファイルを更新しないと，効果が発揮できない．社員教育によって更新の重要性を認識させる，あるいは更新ファイルを自動配布する仕組みを導入するといった防止策との併用が重要である．また，分散策としては，Windows系パソコンばかりでなく，Mac, LinuxなどOSを分散する対策が考えられる．最近，電子政府関連のプロジェクトでもLinuxの採用が相次いでいる．さらに，リスクの移転方策として，ウイルス被害による損失を補償する情報化保険がある[2]．もっとも，失われた情報そのものを保証するものではないが．

このように，損失を免れるための手段には種々あるが，その企業にとって，情報セキュリティ確保のためにどの手段がもっとも適切であるかを判断する基準が必要となる．そのために，情報セキュリティポリシーを策定し，企業の情報セキュリティへの取り組み方針を明確にし，行動規範として提示する必要がある．

## 6. ネットワーク社会における危機管理対応

米国で1990年に発表された報告書は，初めてサイバー脅威が将来拡大する可能性を明確に指摘し，「明日のテロリストは，キーボードを使って，爆破以上の活動をすることができるかも知れない」[3]と述べている．もっとも，サイバーテロリズムの定義はさまざまである．Dorothy Denningは下院軍事委員会におけ

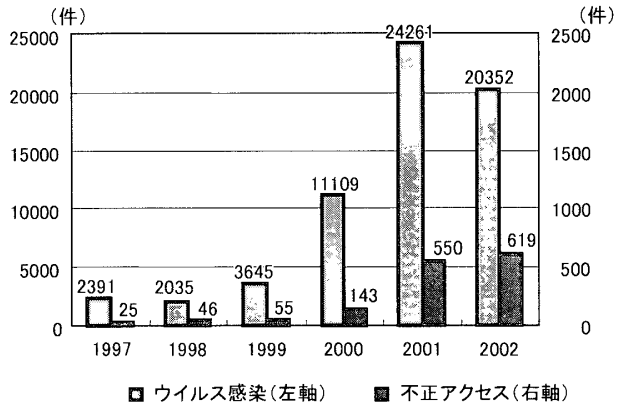



図2　コンピュータウイルス，不正アクセスの届け出件数[5]

る証言で，「政治的又は社会的な目標の推進を目的として，政府あるいは一般市民を脅迫，強制するために，コンピュータ，ネットワークとそこに保管された情報に対する不法な攻撃及び攻撃の脅し」[4]と定義したが，幸いなことに，今までのところこの規模のサイバーテロリズムの攻撃は顕在化していない．しかし，9.11同時多発テロのようなリアル攻撃の影響で，サイバー攻撃が顕在化することが懸念されている．

一方，国家，社会ほどの規模ではないが，企業レベルでは，ネットワークを利用した情報盗難，詐欺，システム破壊といったセキュリティ被害件数は，急激に増加している．図2に，コンピュータウイルス及びコンピュータ不正アクセスの被害届け出があった件数を示す．2000年には，中央官庁などでのホームページ書き換え事件が頻発し，情報セキュリティ対策の不備がもたらす被害について，改めて認識された．また，その直後には不正アクセス禁止法が施行され，情報セキュリティ対策への関心が喚起されたはずだが，不正アクセス届け出件数は逆に増え続けていることが分かる．インターネットに接続されたサーバには1日当たり数百件のポートスキャンが日常茶飯事のように行われ，脆弱性をもった攻撃対象を探す偵察行動が行われているという．このような実害のない不正アクセスは統計に含まれていない．実際には，被害届の出されていない情報セキュリティ被害が多いわけで，総務省の調査によると，民間企業の場合，78.8%の事故が関連機関・団体に届けられていないという[6]．

ウイルス被害がネットワーク経由で大きく猛威を振るった理由には，ADSLによるインターネットの常時接続環境の普及が背景にある．また，電子メールに添付されたファイル中にウイルスが潜んでいて，メールソフトに内蔵されるアドレス帳を参照して自動的に多数のアドレスにウイルスを転送するという，メール機能を悪用するウイルスが次々に作成されている．これは，添付ファイルの利用が増えたことと，特定のメールソフトが多数のパソコンにプレインストールされていることがウイルスを拡散させたといえる．その上，インターネット利用者がウイルス対策ソフトを導入していない，また，ウイルス対策ソフトを導入しているユーザであっても，適切にパターン定義ファイルを更新していないなど，インターネット利用者のウイルス対策に対する意識が乏しいことが原因である．

企業活動の情報化，ネットワーク化はさらに加速化されていく．この傾向は，エネルギー，交通，金融のような社会経済活動，国民生活に不可欠なサービスを提供する重要インフラにおいても，進行している．これまでさまざまな規制により保護されていた重要インフラにおいては，規制緩和の波の中で，競争力強化，コスト削減を至上命題としつつ安定供給を確保するために，情報ネットワーク，情報システムにさらに依存するようになってきた．それだけに，情報ネットワークの障害は，重要インフラのサービスを必須とする企業活動にとって重大な影響をもたらすことになる．これらのネットワークもTCP/IP化されつつある．

## 7. 情報セキュリティマネジメントの重要性

個人であれ，企業であれ，将来の出来事には必ずリスクが存在する．リスクが顕在化する決定要因には，管理の欠如，情報の欠如，時間の欠如，感性の欠如がある[7]．われわれが，取り巻く状況や環境を完全に管理できるならば，リスクは存在しない．完全な情報をもつならば，最適な選択や対策が可能である．さらに，選択のための意思決定や決断に十分な時間が与えられるならばリスクは激減する．リスク感性とは，直感や経験によってリスクの存在を感じ取る能力である．事故として顕在化した事象の背後にはヒヤリ・ハット事故に対する感性が鈍ると，大きな事故につながるといわれる．情報セキュリティ事故にも，同様のメカニズムが存在する．

OECDの情報セキュリティガイドラインは，1992年に採択され，OECD加盟各国における情報セキュリティ政策の立案に影響力をもっている．このガイド

[1] 名称も，「情報システムのセキュリティのためのガイドライン」から「情報システム及びネットワークのセキュリティのためのガイドライン」に変更された．

ラインは，5年ごとに見直すことになっている．1997年には見送られたが，その後のインターネットの普及によって状況が大きく変質したことと，9.11同時多発テロ後のテロリズムへの対応を明確にする必要性を踏まえ，2002年7月に改正された．今回は，ネットワーク社会におけるセキュリティの重要性を広く認識し，個人を含むすべてのネットワーク社会への参加者は，セキュリティ確保に責任をもつべきであるとし，「セキュリティ文化」と「情報セキュリティマネジメント（ISM）」概念の導入を狙いとされた[1]．ISM概念は，管理，情報の欠如に関する対策として提唱されたもので，情報セキュリティマネジメントシステム（ISMS）の制度化を狙いとしている．

また，企業におけるセキュリティ被害には，内部者の関与が大きいともいわれている．これまでの日本企業では，終身雇用，年功序列を軸としていたため，中途採用による人材の調達は少なかった．しかし，特に情報システム部門では技術革新が急激に進展しており，自社内で人材を育成するだけでは間に合わない．このため，中途採用が定着しており，人材の流動化はかなり進展している．また，定期採用の社員も含めて，価値観が多様化している時代でもあり，組織全体への企業文化の浸透を図るために，社員への入念な情報セキュリティ教育が必要である．

企業として情報セキュリティ確保のための取り組みを情報セキュリティポリシとして制定し，それにもとづく物的，技術的，人的な情報セキュリティ管理活動を遂行することが必要である[8]．

セキュリティ文化を担うのも人間である．情報ネットワークのセキュリティを高め，危機管理対応を全うするためには，人間的側面を忘れてはならない．これは，感性の欠如に対する対策といえる．

## 8. おわりに

冒頭に述べたように，通信事業者間の競争の激化，ベストエフォート型サービスの利用による料金の低廉化と，企業のコスト削減努力の相乗効果により，企業情報ネットワークは安価にはなった．このことは，企業の必須経営要素であるネットワークのセキュリティを確保するために，企業自身が相応のコストを負担すべきであることを意味する．しかし，現実には，経営層の情報セキュリティ意識が十分ではないこと，企業体力の弱体化などにより，情報セキュリティ確保のための施策は後回しにされている．人的セキュリティへの配慮も必要である．企業経営者にその認識がないような企業は淘汰されるかもしれない．

### 参考文献


[1] ポール・ヴィリリオ（本間邦雄訳），電脳世界—最悪のシナリオへの対応，産業図書，1998.

[2] http://www.jisa.or.jp/insurance/index-j.html

[3] Computer Science and Telecommunications Board Computers at Risk, Washington D. C., 1991.

[4] Dorothy E. Denning, “Cyberterrorism”, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Servoces, U. S. house of Representatives (May 23,2000), http://www.terrorism.com/documents/denning-testimony.shtml

[5] IPAの発表する統計をもとに作成した．http://www.ipa.go.jp/security/

[6] 総務省，情報セキュリティ調査2002.

[7] 亀井利明，危機管理とリスクマネジメント 改訂増補版，同文館出版，2001.

[8] JIS X 5070 情報技術—情報セキュリティマネジメントの実践のための規範.