The University of Osaka
Institutional Knowledge Archive

Title	コンピュータ・ネットワーク時代の情報資産保護
Author(s)	高瀬, 宜士
Citation	大阪大学, 2001, 博士論文
Version Type	VoR
URL	https://doi.org/10.11501/3184244
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

コンピュータ・ネットワーク時代の
情報資産保護

Protecting Information Assets
in the Era of Computer Networking

平成１３年３月

大阪大学大学院　国際公共政策研究科

高 瀬　宜 士

謝　辞

この論文は, 大阪大学大学院国際公共政策研究科に学位論文として提出したものである。論文を執筆するに当たって，非常に多くの方々から暖かいご指導とご支援を頂いた。この場を借りてお礼を申し上げたい。

指導教官である真田英彦大阪大学大学院経済研究科教授の懇切なご支援なくして，この論文は成り立たなかった。また，論文作成に際しては，林敏彦大阪大学大学院国際公共政策研究科教授（元研究科長）および辻正次大阪大学大学院国際公共政策研究科教授（研究科長）より多大なるご指導を頂いた。記して深謝申しあげる。

つぎに，真田ゼミにおける諸先輩や畏友達，特に岡田定博士，松田貴典博士，上園忠弘博士，安本哲之助氏，篠原健氏，小島敏彦氏，黒目哲児氏，上杉志郎氏，水谷直樹氏，井戸田博樹氏, 岡本隆氏, 田窪美葉氏は時に暖かく時に厳しく論文の批判をしてくださった。

また，岡一文氏，猪原正敏氏，倉谷克哉氏，町田潔氏，中村大造氏，長井聡里医師からは，論文作成に際して貴重な助言を頂戴した。つぎに，田淵治樹氏，飯島邦夫氏，宮崎祥一氏，下口雄山氏，喜多村光蔵氏，野村淳二博士，稲木徹氏は情報提供を含めさまざまな援助をしてくださった。最後に，松下電工株式会社監査役室各位のご厚情に対し，深謝申し上げる。

目　次

頁

序章　　研究目的と論文構成 6

１．　問題認識 6

２．　研究の目的と本論文の論述範囲 7

３．　本論文の構成 9

第１章　情報資産保護概観 10

１．情報資産保護とは 10

２．情報資産保護の歴史 11

２．１　バッチ時代 11

２．２　オンライン時代 12

２．３　戦略情報システム時代 12

２．４　ダウンサイジング時代 13

２．５　ｅビジネス時代 13

３．　情報資産保護のための外郭団体 14

３．１　海外における外郭団体 14

３．２　日本における外郭団体 15

第２章　コンピュータウィルス被害とその対策 18

１．ウィルス被害の現状 19

１．１　日本の現状 19

１．２　Ａ社におけるウィルス被害事例分析 22

１．３　ワクチン種別からみた新種ウィルスの傾向分析 24

１．４　2000年度のウィルス被害分析 25

２．覆された「ウィルスに関する従来の常識」 26

２．１　「ワーム」機能を持った「ウィルス」の出現 27

２．２　「ワーム」機能を持った「トロイの木馬」の出現 28

２．３　添付ファイルを開かなくてもメールを見るだけで感染するウィルスの出現 29

２．４　パワーポイントファイルに感染するウィルスの出現 30

頁

２．５　リモートコントロールにより自己変化するウィルスの出現　31
２．６　「ウィルスには作成者の証拠が残らない」という常識　32
２．７　「コンピュータウィルスは空気感染しない」という常識　32
２．８　Word，Excel，Power Point のすべてに感染するウィルスの出現　33
２．９　ウィルスに感染してもワクチンで駆除できるという常識　35
２．10　パソコンの電源を入れておくだけで感染するウィルスの出現　35
３．マクロウィルス対策事例分析　36
３．１　当該企業の情報システム　36
３．２　ウィルス発見状況把握とエンドユーザーへの配慮　37
３．３　イントラネット活用による情報共有の環境整備　38
３．４　Good Times ウィルス騒ぎ　40
３．５　海外を含めたマクロウィルス対策の重要性　41
３．６　正しい情報入手の重要性　42
３．７　イントラネットで最新パターンファイルに更新する仕組みを自社開発　43
３．８　マクロウィルス大量感染防止のための事前対策の重要性　44
３．９　新発見から自社に到着するまでが対応期間　44
４．ウィルス担当の心構え　45
４．１　エンドユーザーに対して　46
４．２　ツール及び環境整備　46
４．３　教育及びリテラシーの向上　47
４．４　その他の留意点　48
５．新たなウィルス対策と今後の方向性　49
５．１　新たなウィルス対策の必要性　49
５．２　新たなウィルス対策のチェックポイント　51
５．３　グローバル・ネットワーク企業における，ウィルス対策の今後の方向性　56
５．４　ウィルスウォールの限界とその対策　57
５．５　ウィルス対策についての，新たなシステム監査のあり方　59

頁

第３章　コンピュータ不正アクセスの現状とその対策 61

１．不正アクセスの現状 61

１．１　コンピュータ不正アクセス対策基準と不正アクセス禁止法 61

１．２　不正アクセス届出件数 62

１．３　日米における不正アクセスの比較 66

１．４　大学における不正侵入被害 67

１．５　中央官庁被害事例 68

２．不正アクセス犯罪 69

２．１　不正アクセス犯罪事例分析 69

２．２　従来の犯罪とネットワーク犯罪との相違 72

２．３　不正アクセスの侵入方法とその対策 73

３．グローバル企業における不正アクセス対策モデル 76

３．１　当該企業のネットワーク概念図 76

３．２　ネットワーク構築上の留意点 77

４．不正アクセス対策の方法 78

４．１　組織的対策 79

４．２　技術的対策 80

４．３　物理的対策 82

４．４　不正アクセス対策の視点 83

第４章　違法コピーとライセンスマネジメント 86

１．違法コピーの現状分析 87

１．１　世界と日本の現状 87

１．２　学生における違法コピー実態調査 91

１．３　企業における違法コピー意識調査 93

２．ソフトウェアの違法コピーと防止活動 95

２．１　ソフトウェアの法的保護 95

２．２　違法コピーの分類 95

２．３　違法コピーを行った時の制裁 96

頁
２．４　ソフトウェア違法コピー防止活動　97
３．ライセンスの形態と使用条件　98
３．１　ライセンスの契約形態　98
３．２　ライセンスの使用条件　100
４．ＴＣＯ削減　101
４．１　マイクロソフトセレクト契約におけるＴＣＯ削減　101
４．２　同時使用によるＴＣＯ削減　103
４．３　ソフトウェア買取りによるＴＣＯ削減　104
５．ライセンスマネジメントの方法　105
５．１　ソフトウェア管理ガイドライン　105
５．２　コンピュータソフトウェア管理の手引き　105
５．３　管理方法　106
６．ライセンスマネジメントについてのシステム監査　106
６．１　ライセンスマネジメントのシステム監査の方法　107
６．２　システム監査の留意点　108
７．おわりに　110

第５章　セキュリティポリシーと国際標準化　112
１．セキュリティ標準化における世界の動向と日本の現状　113
１．１　セキュリティ標準化における世界の動向　113
１．２　セキュリティ標準化における日本の現状　114
２．セキュリティ評価の国際標準規格 ISO 15408　116
２．１　セキュリティ評価基準の国際標準化の意義　116
２．２　ISO 15408の概要　117
３．セキュリティ評価に合格するためのプロセス　118
３．１　セキュリティ基本設計書の作成　118
３．２　機能要件　118
３．３　保証要件　119
３．４　セキュリティ評価　119
３．５　ISO 15408適用に際しての注意点　120

頁
４．セキュリティポリシーのあり方 121

第６章　終 章 124
１．まとめ 124
２．情報資産保護の今後の方向性 125
３．セキュリティレベル向上のための政策提言 126
３．１　ネットワークの公衆衛生としてのセキュリティ減税 126
３．２　国家安全保障としてのセキュリティ対策と情報資産保護 132
３．３　省庁横断的セキュリティ対策部門の設置 133
４．おわりに 134

序章　研究の目的と論文構成

１．問題認識

近年，情報技術（以下，ＩＴ：information technology）の飛躍的な進歩には目を見張るものがあり，グローバル企業においては，今やＩＴ抜きには経営戦略を達成することは不可能となっている。

1950年代以降，コンピュータシステムはその最も得意とする定型業務処理を中心として，企業における業務効率化に大きく貢献してきた。コンピュータシステムは人間の処理能力を遙かに凌駕しており，現代では，コンピュータシステムの活用なくては効率的な企業経営が不可能な状況となってきている。コンピュータシステムは通信（ネットワーク）との連携により，コミュニケーションにおいてもその威力を発揮しつつある。電子メールは，インターネット技術の進歩により，日常的に利用されるようになってきており，ＩＴの進歩は今後もわれわれの想像を遙かに超えて，社会や組織に大きな恩恵をもたらすであろう。

コンピュータシステムは，電子データ処理システム（ＥＤＰＳ：electronic data processing system）から情報システム（information system）へとその呼び名が変わってきた。これはコンピュータシステムが，電子データを単に処理するだけのものから，情報を保存・加工・分析することにより，経営効率化ばかりでなく，経営戦略に組み込むべきシステムとしての機能が要求されて来ていることを意味している。

しかし，利便さが向上する一方，インターネットをはじめとするネットワークのグローバル化により，新たな脅威が発生している。グローバルネットワークは国境のないネットワークであり，国際間における法的な差異による問題発生はすでに討議されているが，運用管理的な側面での問題はまだ充分研究が進んでいない。特にソフトウェアやコンピュータに保存されている情報データ等の情報資産は，ＩＴの進展により，瞬時に消失する脅威にさらされている。即ち，機密情報の漏洩や消失により，ビジネス競争における優位性を喪失しかねない脅威が増大している。それらの脅威の中心は，ネットワークの進展と共に近年急速に被害を広げているコンピュータウィルス（以後，ウィルス）であり，不正アクセスを通じて情報資産を脅かすハッカー（クラッカー）である。

一方，ソフトウェアや情報データ等（以後，ソフトウェア等）の知的財産は，内外の不正コピーにより，ソフトウェアベンダーにとっては甚大な損害が発生している。ソフトウ

ェアの不正コピーは，知的財産保護の認識の違いにより，国や地域により大きな差異が表れている。

近年，ソフトウェア資産のマネジメントの欠如により，企業の社会的責任を問われる事件が多発し始めた。この対策には，ソフトウェアのライセンスマネジメントが急務と言えよう。システムのオープン化とネットワークのグローバル化によりパーソナルコンピュータ（以下，パソコン）やワークステーションの国際的普及は著しく，その管理はグローバル企業にとって，重要な課題である。損害賠償の請求が単なる複製物の賠償のみならず，企業の信頼を著しく低下させることになり，経済的な問題以上に打撃は大きい。

２． 研究の目的と本論分の論述範囲

本論分ではこれらの視点に立って，グローバル企業における，ネットワークを介した情報資産の脅威となるウィルス及び不正アクセスからの保護と，ライセンスマネジメントについてそのあり方を分析し，これらの基礎となるセキュリティポリシーについて論述する。

図１．１は筆者が考えるセキュリティについての概念図を表したものである。筆者はセキュリティを次の３つに分類する。まず，企業全般にかかわるセキュリティとして Corporate Security があり，その一部として，本論分で述べるコンピュータネットワークとしての Computer Network Security がある。次に，Corporate Security の一部として，情報公開や法令遵守としての Compliance Security がある。

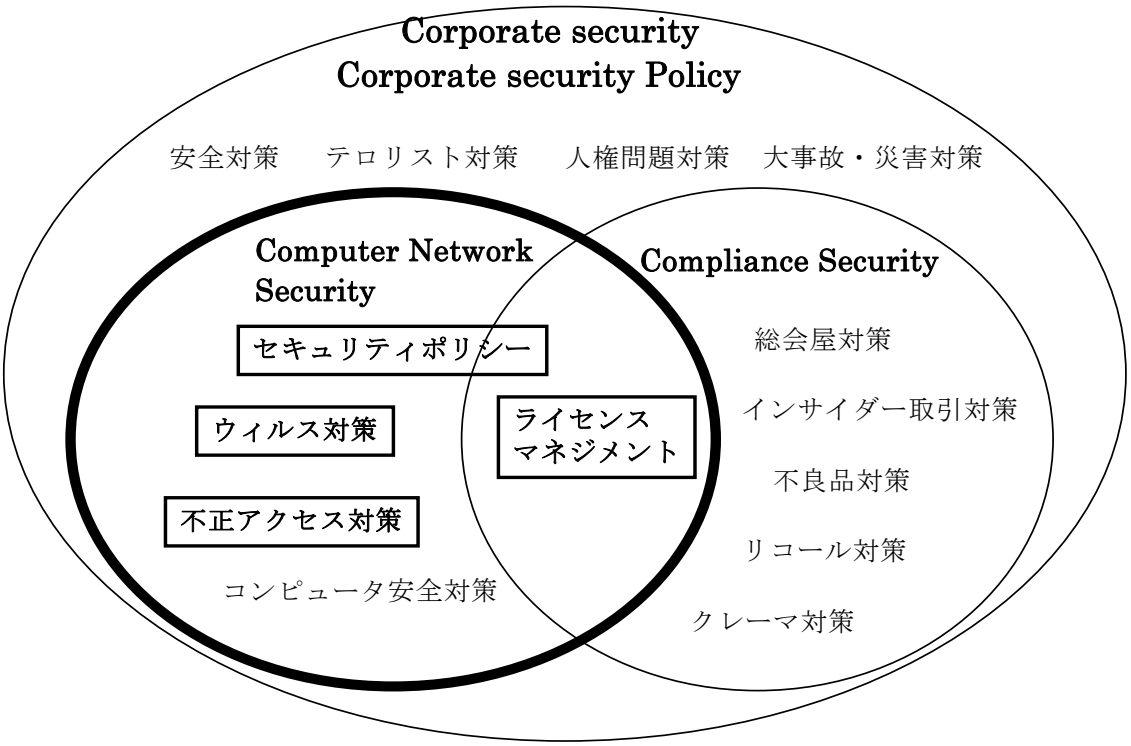
Corporate Security としては，事故防止などの安全対策，人権問題対策，テロリスト対策があり，大事故や火災・風水害など自然災害から守ための災害対策がある。次に，Computer Network Security としては，ウィルス対策，不正アクセス対策，および，データバックアップやシステムバックアップおよび回線の二重化などのコンピュータ安全対策がある。さらに，Compliance Security としては，総会屋対策，インサイダー取引対策，不良品対策，リコール対策，クレーマー対策が含まれる。次に，Computer Network Security と Compliance Security の両方に関連する部分としてライセンスマネジメントがある。

Security Policy に関しては，Corporate Security に対してCorporate Security Policy があり，Computer Network Security に対してComputer Network Security Policy が対応する。本論文ではComputer Network Security Policyのことをセキュリティポリシーと呼

ぶこととする。

本論分で述べる範囲は，図１．１の中の太線枠で囲まれた部分，すなわち，Computer Network Security についてである。具体的にはその中の，ウィルス対策，不正アクセス対策，ライセンスマネジメント，セキュリティポリシーについて論述する。

図１．１ セキュリティの概念図



本論分では，最初にウィルスの現状と対策について分析を行ない，その次に不正アクセスについて論述する。その理由は，不正アクセスにおいて，近年はウィルス技術が利用され始めており，不正アクセスの理解を深めるためにもウィルスについての問題を先に理解することが必要であるからである。

次に，ライセンスマネジメントについて論述する。近年の，乳製品の不良品問題に関する対応の誤りや，自動車でのリコール隠しが明るみに出たことによる企業業績への重大な影響などは，これらの企業に計り知れない影響を与えた。ライセンスマネジメントについてもその対応を誤ると，ブランドイメージに大きなマイナス効果が生じ，業績への影響は避けられない。それにもかかわらず，従来は，まったくといって良いほどライセンスマネ

ジメントについては研究が行なわれていなかった。本論分ではライセンスマネジメントの現状とそのあり方について研究する。

その次に，ネットワークセキュリティ全体の問題として，セキュリティポリシーについて論述する。セキュリティポリシーについては，近年急速にその必要性が指摘されており，筆者もその必要性を痛感しているところである。ネットワーク社会の健全な発展には，各企業のセキュリティレベルを上げることが必須条件であり，そのためにもセキュリティポリシーの策定が重要である。本論分では，国際標準である，IS015408との関連を含めてセキュリティポリシー策定のあり方を論述する。

そして最後に，ネットワーク社会のセキュリティレベル向上のために，公共政策的な観点からの政策提言を行う。

３． 本論文の構成

本論文では，下記のように論議を進める。

第１章「情報資産保護概観」では，情報資産保護の歴史を振り返り，情報資産保護に関連する外郭団体について述べる。

第２章「コンピュータウィルス被害とその対策」では，ウィルス被害の現状について把握し，ウィルスに関する従来の常識が覆された分析を加え，ウィルス対策の事例研究を行い，新たなウィルス対策と今後の方向性について考察する。

第３章「コンピュータ不正アクセスの現状とその対策」では，不正アクセスの現状について把握し，不正アクセスの侵入方法について分析を行い，グローバル企業における不正アクセスのモデル分析を行い，不正アクセス対策の方法について考察する。

第４章「違法コピーとライセンスマネジメント」では，違法コピーの現状について分析し，ソフトウェアの違法コピーと防止活動についてまとめ，ソフトウェアライセンスの形態を分類し，ＴＣＯ（Total Cost of Ownership）削減の観点からの分析を行い，ライセンスマネジメントの方法について考察する。

第５章「セキュリティポリシーと国際標準化」では，世界の標準化動向と日本の現状について分析し，セキュリティ評価の国際標準であるISO 15408について分析し，セキュリティポリシーのあり方について考察する。

第６章「終章」では，情報資産保護の今後の方向性を考察し，政策提言を行う。

第１章 情報資産保護概観

１．情報資産保護とは

情報資産とは何であるかについての定義はまだ定着していない。広辞苑によると，情報とは「あることがらについての知らせ」であり，「判断を下したり行動を起したりするために必要な知識」とある。しかし，情報の定義については諸説がある。例えば，サイバネティクスの創始者であるウィーナー（N. Wiener）は情報について「われわれが外界に対して自己を調整し，かつその調整行動によって外界に影響を及ぼしていく際に，外界との間で交換されるものの内容を指す言葉である」[1)] と定義している。ウィーナーの情報概念の特徴は「外界との間で交換されるもの」に限定されている点である。

マクドノウ（A. M. McDonough）は情報に価値の概念を持ち込んだ研究者の一人である。マクドノウは情報経済学の観点から，データを「評価されていないメッセージ」と定義した上で，情報を「特定の状況における価値が評価されたデータ」と定義した[2)]。さらに彼は知識を「将来の一般的な使用の可能性を評価されたデータ」と定義した[3)]。彼のデータと情報の違いは情報を受け手の解釈に委ねている点である。人間や組織において情報はなんらかの意味のあるものでなければならない。

次に，ポラット（M. U. Porat）の定義によれば「情報とは，組織化され，伝達されるデータを言う。情報活動には情報財，情報サービスの生産，処理，流通において消費されるすべての資産が含まれる」[4)] としている。

以上のことより，情報とは広い概念であるが大きな価値を持つものであり，ＩＴの進展により情報の価値が益々増大していると言える。

企業におけるさまざまな情報についても，その重要性については今後も増大することがあっても減少することはない。情報は，人・もの・カネに次ぐ第４の経営資源といわれ，その情報を保存・分析・加工するために情報システム，即ちコンピュータシステムが必要となり，現在ではインターネットの進展により，そのコンピュータがネットワークで世界中とつながっている。

そこで，本論でいう情報資産とは「コンピュータシステムに保存され，参照・分析・加工されるためのデータ，およびプログラム」のことを言い，「情報資産を円滑に利用することを阻害する要因から守ること，及び，その要因を取り除くこと」を保護と定義する。

企業経営にとっては情報資産の価値が高まる一方，インターネット利用の急激な拡大に伴い，ネットワークを経由した安全性侵害への脅威が急速に高まってきている。本論文はこれらの脅威からの防衛対策とそのあり方を述べる。

２．情報資産保護の歴史

情報資産保護については，次の５つの時代に分けて歴史を振り返る。

１．バッチ時代

２．オンライン時代

３．戦略情報システム時代

４．ダウンサイジング時代

５．ｅビジネス時代

２．１　バッチ時代

1960年代に，給与計算などの一部分の業務について，バッチ処理を中心とした単純なクローズドなシステムが，人員削減などの目的で導入された。この当時の情報システムは，ＥＤＰＳ(electronic data processing system)と呼ばれており，まさに，電子(electronic)でデータ（data）を処理（processing）するシステムと呼ばれるにふさわしいもので，プログラムやデータについてはパンチカードシステムが主流であった。コンピュータも技術計算用と業務処理用とに分けられており，それぞれ個別に運用が行われていた。

情報資産保護としては，この頃は入出力帳票の管理が中心で，プログラムもパンチカード式のものが多く，重要なプログラムについてバックアップを確保している程度のもので，コンピュータルームを守ることを中心とした対策が中心であった。

その後，プログラムについては，カードでのソースプログラムを確保するとともに，磁気テープにバックアップが取られるようになった。データについても異常終了処理に備えて，必要に応じてバックアップテープが取られていた。

しかし，トラブル発生時にはプログラマーがコンピュータルームに入って処理をするなど，オペレータとプログラマーの職務の分離は不十分であった。

２．２　オンライン時代

1970年代前半は，端末が設置されオンラインでデータ収集を行い，バッチ方式で処理するといった形態が中心であった。コンピュータシステムのネットワーク化が進展するにしたがって，コンピュータ本体だけでなく，端末やネットワークを含めた運用を行うことが必要となってきた。また，コンピュータ化の範囲も販売管理など主要業務にも広げられていった。1970年代前半は，プログラムやデータのバックアップについての確実な確保が図られ，コンピュータルームへの入出管理などが追加され，オペレータとプログラマーとの業務分離が図られた。

1970年代中頃から後半にかけては汎用コンピュータが登場し，ファイルやメモリーの大容量化とＣＰＵの高速化が実現し，オンラインリアルタイム処理が導入された。オンライン化の進展に伴い，主要な業務についてもオンラインリアルタイム方式で処理するようになっていった。コンピュータ化される業務範囲の増大に伴い，情報システムがトラブルを発生させたときの影響も広範囲になり，バックアップ体制も整備されていった。当時は端末オペレータと呼ばれる端末操作を専門とした社員により，全国でコンピュータへの入力業務が行われていた。

この時代の情報資産保護の視点としては，以前のコンピュータルームを中心としたものから，端末とネットワークを含めたものへと変わっていき，ユーザＩＤによる入力者の確認などが行われていたが，容易に類推できるレベルのものであった。

２．３　戦略的情報システム時代

1980年代になると汎用コンピュータのコストが大幅に低減し，多くの業務について効率化の面でも多くの企業がコンピュータシステムを導入するようになった。そのような中で，経営情報をオンラインでリアルタイムに処理し，戦略的に利用することにより競争優位性を確保するという戦略情報システムという考え方が登場した。

この当時の情報資産保護としては，汎用コンピュータと端末とネットワークを中心としたもので，コンピュータシステムやディスクのバックアップの強化が図られた。重要な回線については２重化が図られていたが，ネットワークとしては現在と異なり，クローズなものであり，現在と比較すると安全性は高かった。端末も専用端末だけで，パソコンはす

でに利用されてはいたが，オンライン端末としては利用されていなかった。

２．４　ダウンサイジング時代

1990年代に入ると，従来は汎用コンピュータだけで処理をしてきたものが，一部分の業務についてはパソコンとサーバを利用したシステム（クライアント／サーバシステム）を導入することが可能となった。このことにより，従来は専用線で結ばれたホストコンピュータと端末を中心としたものであったのが，クライアント／サーバーシステムを含めたものとなり，ネットワークとしてはオフィスや工場にＬＡＮ（Local Area Network）が導入された。業務面では，グループウェアが導入され，社内の電子メールや情報共有が図られた。子会社・関連会社や取引先にもネットワークが張り巡らされ，ＥＤＩ（electronic data interchange）が導入され，企業内だけの効率化から企業グループ全体としての効率化が図られるようになった。

一方，パソコンの利用により，コンピュータウィルスによる被害が発生してはいたが，フロッピーなどを経由して繁殖するタイプが大半で，被害もごく一部分であったので，業務への影響は軽微であった。

この当時の情報資産保護の視点としては，従来の汎用コンピュータを設置しているコンピュータセンターを中心としたものから，全国の主要拠点のクライアント／サーバーシステムを含めたものに保護する対象も広がるとともに，子会社・関連会社を含めたものへと拡大していった。

２．５　ｅビジネス時代

1990年代中頃になると，企業では多くのオフィースにＬＡＮが導入され，それらがネットワークで結ばれてイントラネットが構築され，先進企業では，関連企業を含めたエクストラネット網が整備されてきた。そして，インターネットの進展に伴い，従来は社内を中心としていたクローズなネットワークが，外部のオープンなネットワーク即ち，インターネットと接続されるようになってきた。

パソコンの利用が活発になり，ＥＵＣ（end user computing）が行われ，簡単な計算やプログラムについては，エンドユーザ自らが作成するようになった。そのことによりパソ

コンに保存されている情報資産の重要性が増加したが，新たにマクロウィルスが発見され，被害が拡大することとなった。

パソコンを端末として利用するためにエミュレータソフト[1]が開発された。一部の企業ではエミュレータソフトを自社開発して個別のパソコン毎に管理用No.[2]を付与することにより，外部からのアクセスを排除して安全性を高めるなどの方法でセキュリティレベルの向上が図られた。

これら一連の情報ネットワークの発展により，コンピュータネットワークを利用した新しいビジネス形態（ｅビジネス）が実現することとなった。

ｅビジネス時代には，企業の主要な戦略として情報システムとネットワークの活用が重要な位置を占めるようになった。しかし，一方，オープンネットワークであるが故の問題点として，コンピュータウィルスやハッカーによる不正侵入が発生し，コンピュータシステムやネットワークのトラブルは，事業のリスクとして認識されるようになった。ソフトウェアのライセンス問題についても，違法コピーを行った企業名が新聞で公表されるなど，企業経営としては重大な関心を払うことが必要となってきた。

現在の情報資産保護の視点としては，グローバルネットワークを対象とした世界中に対して注意を払うことが必要となってきているといえる。

３．情報資産保護のための外郭団体

情報システムの脅威に対して，米国を始めとしてさまざまな外郭団体が存在する。ここではその主なものを取り上げることとする。

３．１　海外における外郭団体

①　ＣＥＲＴ（Comuputer Emergency Response Team）

不正アクセスについての件数を始めとして，その対策方法などさまざまな情報発進を行っており，米国ばかりでなく世界中が利用している。

1　パソコンに端末機としての働きをさせるためのソフトウェアのこと

ＵＲＬ： http://www.cert.org/

② ＦＩＲＳＴ（Forum of Incident Responce and Security Teams）

1992年に設立され，1993年に11の組織で活動を開始した。2000年７月現在，84の組織が参加している。その比率は，企業が39%，民間組織が21%，大学が11%，政府関連が９%，国防関係が４%となっている。

ＵＲＬ： http://www.first.org/

③ ＣＩＡＣ（Computer Incident Advisory Capbility　U.S.Department of Energy）

米国エネルギー省の外郭団体で，コンピュータ事件の対策について広報活動を行っている。

ＵＲＬ：http://ciac.llnl.gov/

④ ＩＣＳＡ （旧称：ＮＣＳＡ： National Computer Security Association）

コンピュータセキュリティに関する情報提供を行っている。

ＵＲＬ：http://www.icsa.net

⑤ ＩＳＡＣＡ（Information Systems Audit and Control Association）

情報システムコントロール協会と呼ばれ，米国に本部を置く非営利の任意団体で，情報システムの監査やコントロールに関する情報提供を行っている。

ＵＲＬ：http://www.isaca.org/

⑥ ＢＳＡ （Business Software Alliance）

マイクロソフト等が著作権保護の推進を目ざして1988年に設立した非営利団体で，米国に本部を置きビジネスソフトウェア連合[3]と呼ばれている。全世界の違法コピーについての比率や被害額などの調査や，違法コピーに関する啓蒙活動を行っている。

ＵＲＬ：http://www.bsa.or.jp/　Business Software Alliance

３．２　日本における外郭団体

① ＪＰＣＥＲＴ／ＣＣ（Japan Computer Emergency Response Team / Coordination Center）

2　端末識別用のＩＤコード

[3] マイクロソフト等が著作権保護の推進を目ざして1988年に設立した非営利団体

1996年10月に設立され，日本におけるコンピュータ犯罪・不正アクセスに関する情報を提供する中心的存在である。公開文章としては，緊急報告，テクニカルレポート，初心者のための各種ドキュメントなどがある。それ以外の活動として，原稿の寄稿や，国内および海外での公演活動がある。

ＵＲＬ：http://www.jpcert.or.jp/

② ＩＰＡ（情報処理振興事業協会）

経済産業省の外郭団体で，「コンピュータウィルス対策基準」で定められた届出先に指定されており，日本国内におけるコンピュータウィルスなどの情報提供を行っている。

ＵＲＬ：http://www.ipa.go.jp/

③ ＪＩＰＤＥＣ（日本情報処理開発協会）

経済産業省の外郭団体で，「コンピュータ不正アクセス対策基準解説書」や「コンピュータウィルス対策基準解説書」「情報化白書」「システム監査白書」などを発行している。

ＵＲＬ：http://www.jipdec.or.jp/index.htm

④ ＩＳＡＣＡ（Information Systems Audit and Control Association）日本支部

米国に本部を置く情報システムコントロール協会の日本支部で，国内には東京，名古屋，大阪の３つの支部が有りそれぞれ連携して活動を行っている。

大阪支部ＵＲＬ：http://www.isaca-osaka.org/

⑤ コンピュータソフトウェア著作権協会（ＡＣＣＳ）

コンピュータソフトウェアの著作権を守るために設立された団体で，調査を始めとして様々な活動を行っている。

ＵＲＬ：http://www.accsjp.or.jp/

⑥ 日本パーソナルコンピュータソフトウェア協会（ＪＰＳＡ）

パーソナルコンピュータのソフトウェアに関する権利を守るために設立された団体である。

ＵＲＬ：http://www.jpsa.or.jp/

その他，これ以外にも様々な団体があるが，情報資産保護のレベルを向上させるには，これらの機関が発行する情報を的確に把握し，自社への適用および自社への影響を検討することが重要である。

参 考 文 献

１）Wiener, N.,*The Human Use of Human Beings;Cybernetics and Society* 2_{nd} *ed.*, Doubleday, p.17(1954)(鎮目恭夫・池原止戈夫訳『人間機械論　第２版』みすず書房，11頁，1979年)

２）McDonough, A. M. ,*Information Economics and Management Systems*,McGraw-Hill, p.76 (1963) (松田武彦・横山保監修 長阪精三郎訳『情報の経済学と経営システム』好学社，78頁，1965年)

３）*Ibid.*, p.76(邦訳，78頁)

４）飯沼光雄，大平号声，増田祐司 著『情報経済論』有斐閣，p.9(1992)

５）通商産業省機械情報産業局『システム監査基準解説書・改訂』日本情報処理開発協会，(1996)

６）通商産業省機械情報産業局『システム監査白書 1989』コンピュータエージ社 (1989)

第２章　コンピュータウィルス被害とその対策

コンピュータウィルス（以下，ウィルス）とは，通商産業省（現在の経済産業省）の「コンピュータウィルス対策基準[1)]」によると「第３者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムで，①自己伝染機能，②潜伏機能，③発病機能のうち１つ以上を有するもの」である。

2000年5月4日に発見されたウィルス VBS/Love Letter .worm（以下，ラブレターワーム）は，20カ国で確認され推計4500万台のコンピュータが被害を受け，26億ドル（約2800億円）もの損失が生じたと推定されている。[4]

従来筆者が危惧してきたことが，ラブレターワームの出現により現実のものとなった[2)]。1999年に発見されたメリッサウィルスを始めとして，このようにメール自動送信機能を利用した強力な感染機能を持ったウィルスの出現により，ウィルス対策としては1995年にマクロウィルスが出現した時以来の大きな転換期が来ている。

情報処理振興事業協会（以下，ＩＰＡ）の発表によると2000年のウィルス被害届出累計件数は 11,109件で，過去最高だった1999年の年間合計 3,645件の3倍以上に達しており，コンピュータウィルス被害が急速に拡大していることが分かる。企業においてウィルス対策担当者がこのような状況に応じた対策を講じていない場合は，甚大な被害をもたらす恐れが増大しており，ラブレターワームはそのことを如実に示している。

本稿では，第１節でウィルス被害の現状について，日本国内の現状とＡ社についての事例分析を行い，第２節でウィルスに関する従来の常識が覆された事例について考察を加え，その中で，どのようにウィルスが巧妙化し急速に被害の拡大が起きているかについての事例を分析する。第３節でマクロウィルス対策についての事例研究を行い，第４節でウィルス対策担当の心構えについてまとめ，第５節では，新たなウィルス対策と今後の方向性について提言を行うとともに，グローバルネットワーク企業におけるウィルス対策の今後の方向性および，システム監査のあり方を考察する。

4　http://www.asahi.com/tech/jiken/20000506c.html を参照

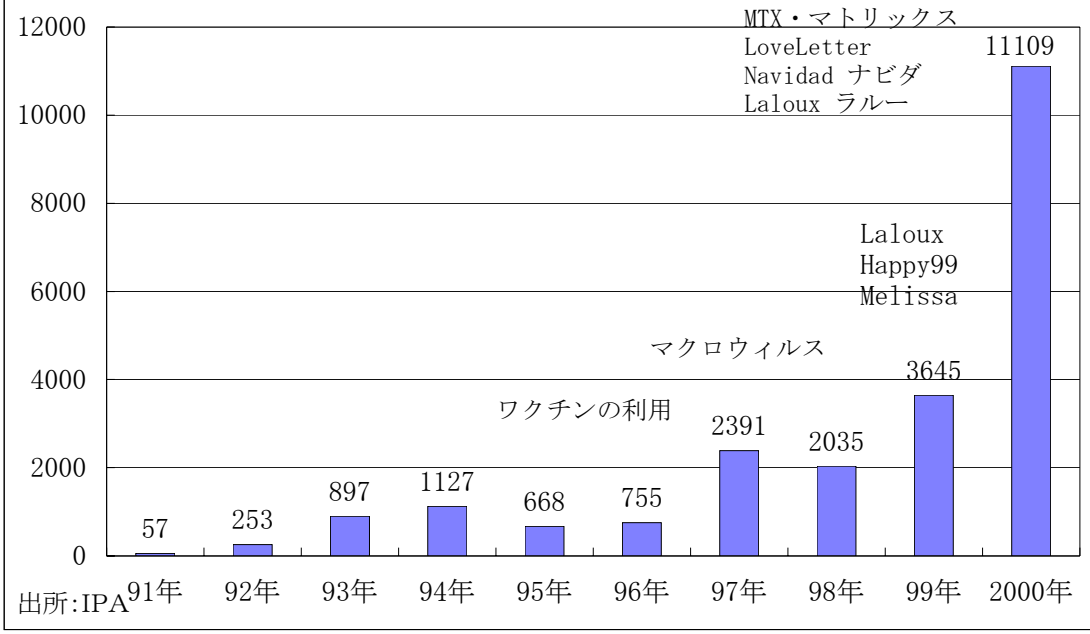
１．ウィルス被害の現状

１．１　日本の現状

日本のウィルス被害についてＩＰＡへの届出件数の推移は 図２－１の通りである[5]。

このグラフより，1994年（1127件）と，1997年（2391件）に２つの山があることが分かる。その原因は，1994年まではコンピュータウィルス駆除用ワクチン（以下，ワクチン）をパソコンにインストールしていなかったために被害に遭うケースが多かったことが原因である。ワクチンの普及により，1994年から1995年にかけて被害は減少した。次に，1997年に急増している原因は，マクロウィルスの出現によるものである。マクロウィルスへの対応については，第３節のウィルス対策の事例研究で詳しく述べる。

図2－1 日本のウィルス被害推移



出所:IPA

1998年にはマクロウィルスに対応したワクチンが広く普及し，一旦は減少傾向に向かったが， 2000年は過去最大の被害件数となり第3の大きな山が来ている。

---

[5] http://www.ipa.go.jp/　を参照。

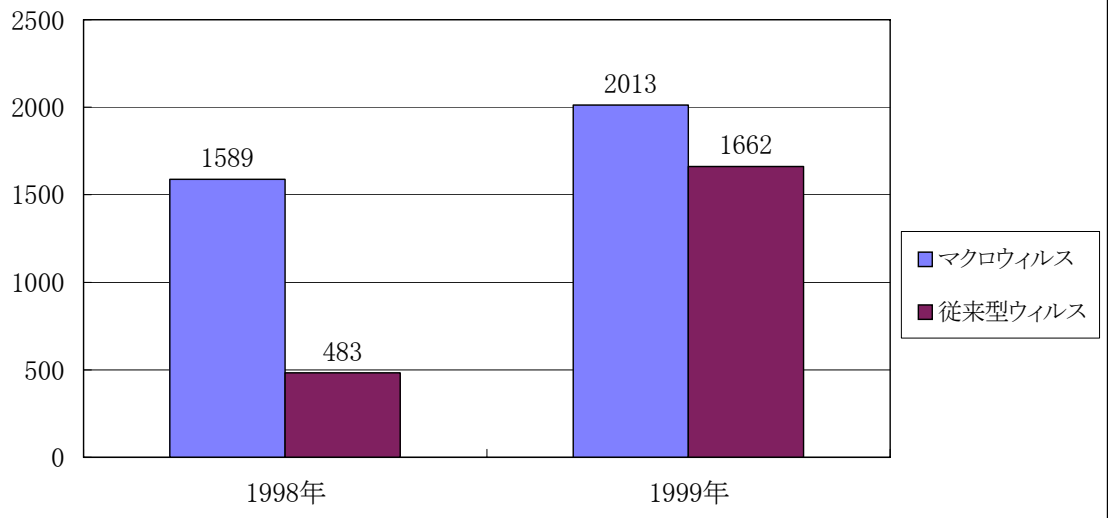
2000年の累計件数は 11,109件で，過去最高だった1999年の年間合計 3,645件を3倍以上上回っており，2000年になってからコンピュータウィルスの被害が急速に拡大していることが分かる。

2000年のウィルスによる被害届け件数が，日本全国でわずか 11,109件であることは非常に少ないと思えるが，ウィルス感染が常に身近に発生しているものであり，被害がよほど深刻な場合のみ被害届けが出されているのが実状である。実際の被害件数はもっと多い。たとえ1件の被害届けであっても，中には数千台ものパソコンが被害に遭っているケースもあり，一部の企業では甚大な損害を受けていることを認識すべきである[6]。

次に，1998年と1999年を比較したウィルス種類別推移を図２－２に示す。

これまで最も届出件数が多かったウィルスは XM/Laloux（以下，ラルー）であり，1998年が960件，1999年が998件と2年連続して最多であった。特筆すべきはHappy99が1999年に初めて発見されたウィルスであるにもかかわらず，992件もの届出があり，わずか1年間でラルーに次ぐ2番目に多いウィルスとなったことである。

図２－２ ウィルス種類別推移



出所:IPAの資料を元に筆者が作成

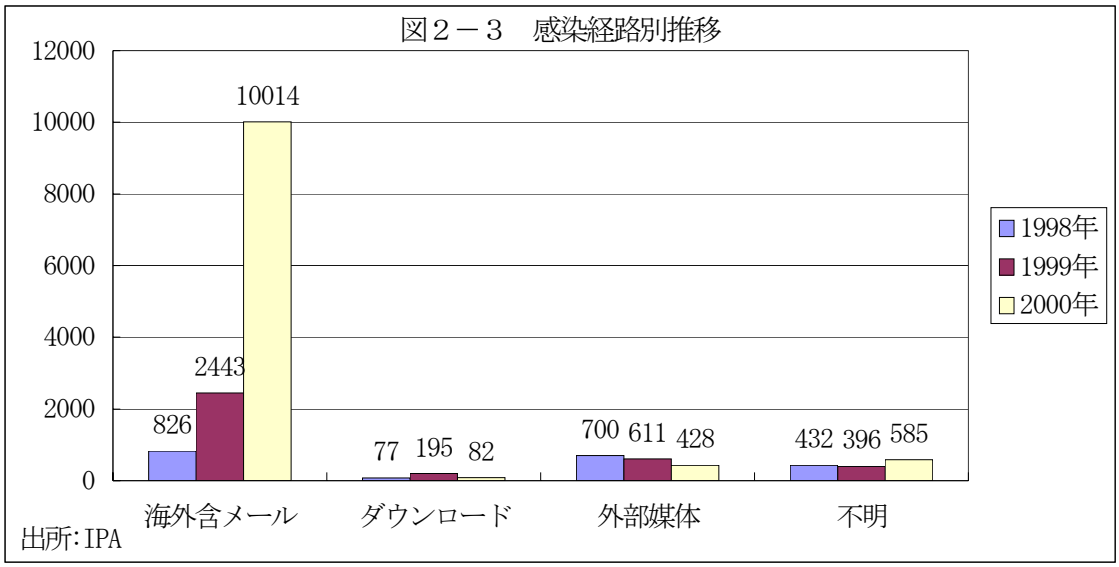
ラルーが広がった要因は，英語環境に依存するコンセプトに比べ，日本語など他の言語

6 「ウィルス被害届」は届出件数の集計であって，被害台数ではない。

バージョンでも動作したラルーの互換性の高さによる部分が大きい。Happy99で見られるようにメールソフトを利用したワーム(トロイの木馬ワーム)は，今後Outlook以外への対応が進めば急速に感染力が高まると予測される。

Happy99は図２－２のＩＰＡの分類では「従来型ウィルス」に含まれている。このタイプはインターネットを通じて感染を広げるもので，マクロウィルス以上にＥＸＥタイプのウィルスが急速に感染を広げており，ウィルスのタイプも急速に変わろうとしている。

次に，図２－３は感染経路別の推移である。件数が急増している感染経路は「海外を含むメール」である。これはインターネットの発達により世界中でメールが取り交わされ，その中にウィルスが含まれていたからである。特に感染力が強いウィルスは最新ワクチンのパターンファイルを利用していないパソコンでは発見が難しい。マトリックスウィルスやHappy99を含め，今後は「メール機能を悪用したトロイの木馬ワーム」に備えることが重要である。



ＩＰＡはウィルス対策として以下のことを警告している[7]。

（１）たとえ，友人，知人，職場の同僚から送られてきた電子メールであっても，添付ファイルは開いたり，実行したりするまえに，必ず最新のワクチンソフトでウィルス検査を行うこと。

---

[7] http://www.ipa.go.jp/SECURITY/txt/attach/2000_01-1.html を参照。

（２）ファイルに感染しないタイプの「W32/SKA」「W32/PrettyPark」のようなトロイの木馬ウィルスは，新種の場合は最新のワクチンソフトでも発見できない可能性が高いので，メールの添付ファイルでプログラムを受け取った場合は，相手先に添付ファイルの内容の問合せを行うなどにより，必ずファイルの安全性を確認してから実行すること。

１．２　Ａ社におけるウィルス被害事例分析

筆者はウィルス対策の具体的事例を調査・分析することができた。A社は日本に本社を置き，世界中に自社ネットワークを持つグローバルな製造企業である。

Ａ社の概要は，国内販売高：約1兆円，国内従業員数：約２万名，国内パソコン所有台数：一万数千台，子会社約200社（内，海外子会社約50社）で，1995年には海外を含めた関係会社や国内代理店を結ぶコンピュータネットワーク網が完成していた。Ａ社は国内受注件数のうち約６割については，Ａ社の社員を介することなく，代理店からネットワークを経由して直接Ａ社のホストコンピュータに対して受発注処理が行われており，いわゆるＢtoＢに関する先進企業である。

以下，Ａ社について筆者が行なったウィルス被害調査と分析結果である。

図２－４は，インターネット接続の際に発見された1999年12月度の「ウィルス名称別構成比」を示している[8]。

Ａ社は海外を含むエクストラネット網を完成した1995年頃からウィルスに対して組織的な防御体制を整え，すべてのパソコンにワクチンを配布してきた。

当時はブートセクター[9]に感染するウィルスが主流で，感染経路もフロッピーディスクが多く，パソコンにワクチンがインストールされていれば防御可能であった。

1996年に日本でもマクロウィルスが発見され，Ａ社でも海外を含む社内メールの中にマクロウィルスが発見された。1997年はマクロウィルスが日本国内でも猛威を振るい，社内で多くのマクロウィルスが発見された。当時は新種のウィルスが初めて発見されてからそれが該社で発見されるまでに，半年程度のタイムラグがあった。1998年になると，メール

---

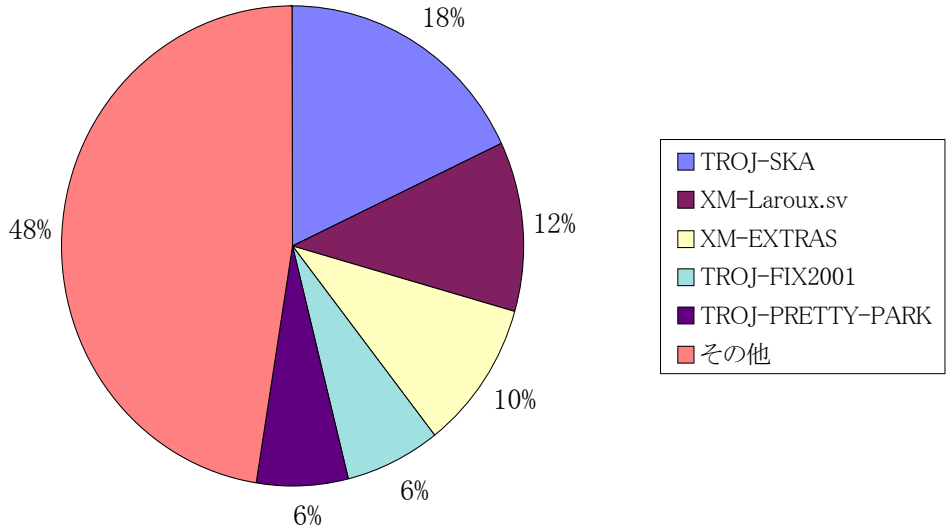
[8] ウィルスウォールで，社内と社外との間のメール送受信や，ファイルのダウンロード及びアップロードの際に発見されたウィルスの名称別構成比である。

[9] パソコンの電源を入れたときに，最初に読込む外部記憶装置の特定の場所のこと。

を経由したマクロウィルスが大量に発見されるようになり，初めて発見されてから該社で発見されるまでに要した期間は3ヶ月程度になっていた。1999年当初にはその期間が1ヶ月に短縮しており，1999年末にはわずか数日後に，新種のウィルスが該社で発見される事態になっていた。

従来はラルーが最も多く発見されていたが，1999年12月はトップがTROJ_SKA(略称：Happy99)に入れ替わった。このワームはEudoraなどOutlook以外のメーリングソフトでも繁殖できるようにプログラムされているため，これだけ急速に広がっており，ウィルスの世代交代が急速に生じていることが分かる。

図２－４ ウィルス名称別構成比

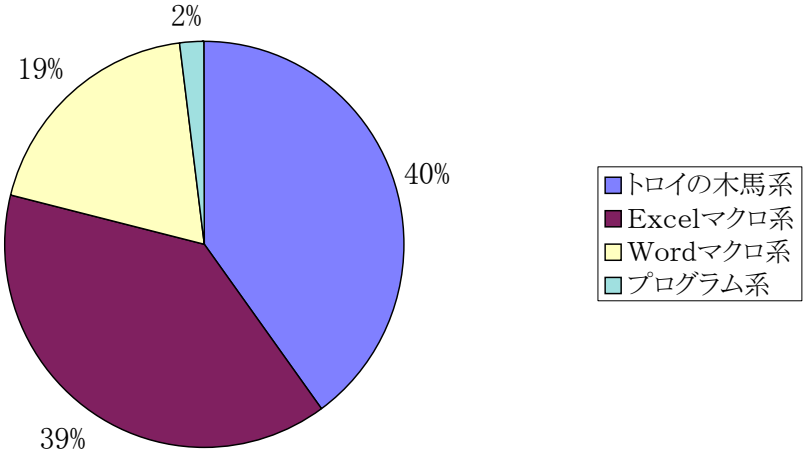


出所:A社の資料を元に筆者が作成

次に，ウィルスを種類別に分類した「ウィルス種類別構成比」（図２－５）では，「トロイの木馬」系が４０％と最も多く，続いてExcelマクロ系が３９％，Wordマクロ系１９％，その他２％，となっている。

その中で，Happy99は「トロイの木馬」に分類され，「メール機能を悪用したトロイの木馬型ワーム」が急速に感染を広げていると言える。

図 2－5 ウィルス種類別構成比



出所:A社のデータを元に筆者が作成

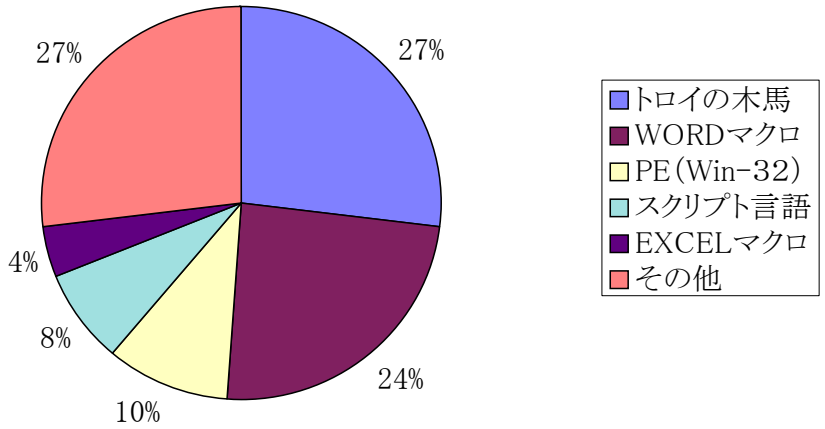
１．３　ワクチン種別からみた新種ウィルスの傾向分析

今後，どのようなウィルスが発生し,それが自社にどのように影響するかについて分析を行なうことは重要なことである。新しいウィルスが発見されれば，それに対応したワクチンが提供されているはずである。そこで，筆者はワクチンを提供している主要な2社について分析をおこなった。

次の２つの図（図２－６，図２－７）は，ワクチンメーカーＮ社とＴ社が2000年1月から3月までに配布したパターンファイルについて，筆者が種類別に分析集計したものである。それによるといずれの会社も，急速に種類を増やしているウィルスは，「トロイの木馬」タイプで，Ｎ社２７％，Ｔ社２１％である。それに加えてWordマクロウィルスも増加していることが分かる。

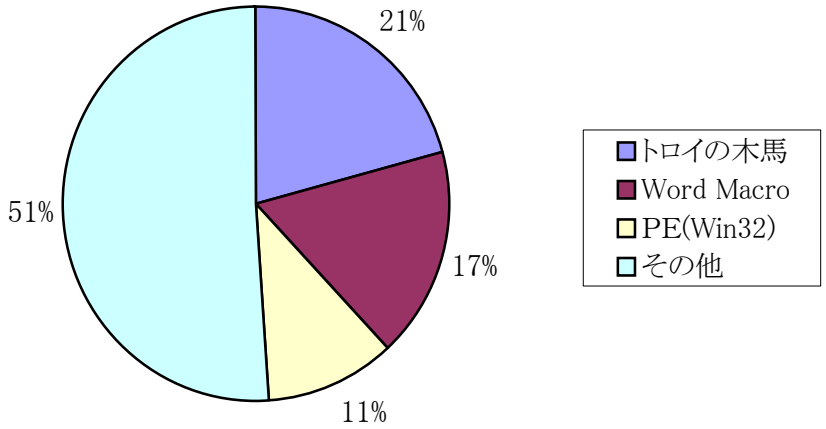
このことにより，従来はマクロウィルス対策を中心に考えていたものが，今後は「トロイの木馬」タイプを含めたメールを利用したウィルスについての対策が重要であると認識された。詳しくは次節で述べるが，この傾向は2000年度の分析を行った結果でも継続的に続いている。

図2－6　N社の事例



出所:N社のパターンファイルデータを元に筆者が作成

図2－7　T社の事例



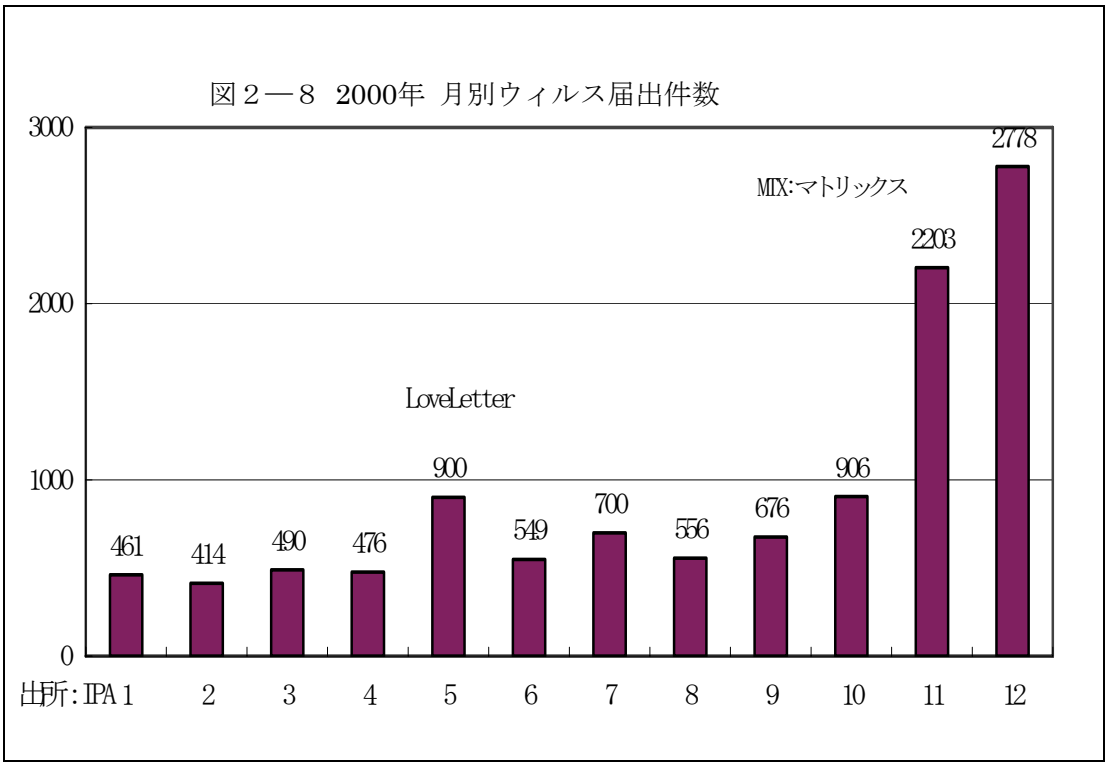
出所:T社のパターンファイルデータを元に，筆者が作成

１．４　2000年度のウィルス被害届分析

2000年度のウィルス被害届出件数の推移は図２－８のとおりである。それによると，5月にはLoveLetterウィルスの出現により 900件の被害届が出され過去最高件数となった。次に，10月 906件，11月 2203件，12月 2,778件の被害届となっており，過去最高件数を

3ヶ月間連続して更新している。このことにより，2000年の最後の３ヶ月間で，ウィルス被害が今までにないスピードで急速に拡大していることがわかる。最も届出件数が多かったウィルスは ＰＥ_ＭＴＸ（通称：マトリックス）と呼ばれるもので，11月の2203件中894件，12月の2778件中1008件を記録した。このウィルスは，2000年８月に発見され，ワクチンは９月上旬に完成しているが，発見されてからわずか３ヶ月間で最も被害届出件数が多いウィルスになった。

マトリックスウィルスの特徴及びなぜこれほど広範囲に感染が拡大したのか，その原因については，次節『２．覆されたウィルスに関する従来の常識』の『２．９　ウィルスに感染してもワクチンで駆除できるという常識』で詳しく分析する。



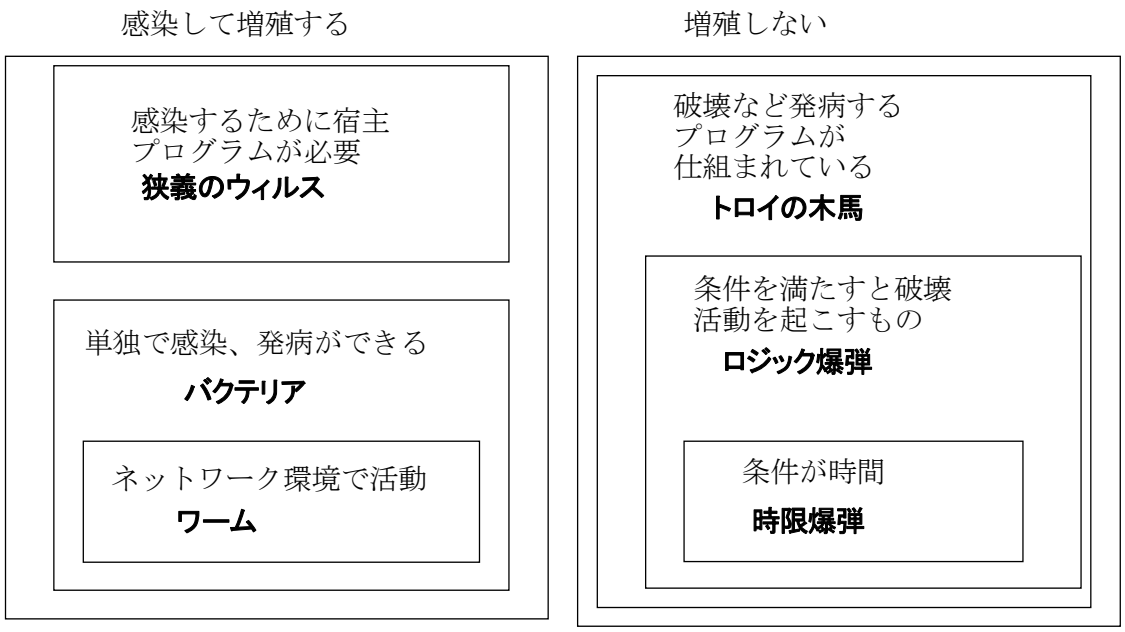
２．覆された「ウィルスに関する従来の常識」

本節では，新しいタイプのウィルスが出現してきており，そのためにウィルスに関する従来の常識が次々に破られてきた事例を分析する。

２．１　「ワーム」機能を持った「ウィルス」の出現

「コンピュータウィルス辞典[3)]」によると，ウィルスは図２－９のように分類される。しかし，以下の事例で見るように，この分類方法では分類できないウィルスが次々と現れてきている。

図２－9 ウィルスの分類図



出所：「コンピュータウィルス辞典[3)]」を加筆修正

1999年に最も話題となったウィルスであるメリッサは,マイクロソフト社のWordのマクロ機能を利用して，Outlookとの組み合わせで機能する，コンピュータ間を増殖するウィルスである。メリッサに感染したWordファイルをクリックすると，メーリングリストに登録されている最大50人分のアドレスに，自動的にメールを発信する。発信メールのタイトルには「．．からの重要なメッセージ」として，送り主の名前がタイトルに表示され，　それに加えて list.docというWordファイルが添付され，その中にはマクロ命令に加えてポルノのウェブサイトの情報が含まれている。これを受け取った人が，感染したWordファイルをクリックすると，その人を発信人としてさらに最大50人のアドレスに自動的にメールが送

られる。この課程が次々と繰り返され，急速に被害を広げていった。

メリッサは単独で感染発病ができるため「ワーム」に分類できる。しかし，感染するための宿主プログラム（MS-Word-File）を必要とするので「狭義のウィルス」ともいえる。

メリッサを開発した犯人は，このような事態を予測しており，ウィルスプログラムの中に ” Worm? Macro Virus? Word97 Virus? Word2000 Virus? You decide! ”（ワーム？ マクロウィルス？ Word97ウィルス？ Word2000ウィルス？ 勝手に決めてくれ！）と書き込んでいる。このようにメリッサは，従来のウィルスの分類方式では分類できない複数の機能を持つものである。

メリッサが発病すると，コンピュータの時計の分単位がその日の日付と同じになった時に，コンピュータ・ファイルに次の文章を挿入する。” Twenty-two points , plus triple-word-score, plus fifty points for using all my letters. Game’s over. I’m outta here, ” (22ポイント，トリプルワードスコア，私の文字をすべて利用したので50点追加。ゲームオーバー。それでは。)という文章がユーザーのWordドキュメントに，自動挿入される[10]。

メリッサの問題は，発病時の被害よりも，メール自動送信機能という強力な感染力を持ったことである。ワクチンが完成するまでに広範囲に感染が広がったこと，および電子メールサーバーに大きな負荷がかかったことによって，より深刻な被害が発生した。被害を受けた多くの企業は，ウィルスの感染をこれ以上広げないために，ワクチンが完成してウィルス駆除が出来るまでは，メールサーバーの停止を余儀なくさせられた。

メリッサのソースコードを見たり変更したりするのは比較的簡単なため，変異ウィルスも急速に登場している。Excelファイルに感染する「Papa」という変種[11] が登場しているほか，「Melissa.a」という電子メールのタイトルが空欄になる亜種[12] も登場している。

インターネットの進展に伴い，メールに添付されるウィルスの感染拡大が懸念されていたが，メリッサによってメール自動送信機能を使ったウィルスの感染力が証明され，それ以後のウィルスに大きな影響を及ぼした。

メリッサは「狭義のウィルス」であるとともに「ワーム」でもあり，「ウィルスに関する従来の常識」を覆したものである。

---

[10] http://www.hotwired.co.jp/news/news/Technology/story/2219.htmlを参照。

[11] 従来のウィルスロジックを利用して作成された，新たなウィルスのこと。

[12] 従来のウィルスの一部分を変更して出来るウィルスのこと。

２．２　［ワーム］機能を持った「トロイの木馬」の出現

自分では繁殖できない「トロイの木馬」と自分で繁殖できる「ワーム」とは，これまでは異なるものとして分類されてきた。しかし「トロイの木馬」でありながら自動繁殖機能を持つもの，即ち「ワーム」機能を持つウィルスが出現した。このウィルスはW32/SKA（以下，Happy99）とよばれるもので，このウィルスが含まれているＥＸＥＣファイルを実行すると，「 Happy New Year 1999 !! 」のメッセージとともに花火の絵が表示される。それと同時に，自分自身のプログラムを添付してメールを自動送信する。

Happy99は，ＥＸＥタイプ[13] で「トロイの木馬」の中にワーム機能が組み込まれていたもので，EudoraなどOutlook以外のメールソフトでも繁殖ができるようにプログラムされている。そのためOutlook以外のメールソフトを利用しているユーザーにも繁殖しており，このウィルスの感染は広範囲に広がっている。ある程度の知識を持つ者であれば，このウィルスプログラムを基にして，「 Happy New Year 2000 !! 」という亜種を数分間で作ることも可能である。既に2000年1月17日に，米国でこの内容と同様の亜種ウィルスが発見されている。

２．３　添付ファイルを開かなくてもメールを見るだけで感染するウィルスの出現

これまではウィルスプログラムが実行されるには，電子メールの添付ファイルがユーザーによってクリックされる必要があった。ところがメールを見るだけで活動を開始するウィルスが発見された[14]。Bubbleboy(以下，バブルボーイ)と名付けられたこのウィルスは，まだ被害報告は出ていないが今後感染が広まる可能性がある。

バブルボーイに感染すると，コンピュータの登録ユーザー名がBubbleboyという名前に変更される。このウィルスで重要な点は，添付ファイルをクリックするのではなく，電子メールを開いた直後にウィルスプログラムが実行されることである。これまでに登場したウィルスと同じように，バブルボーイはOutlookのセキュリティーホールを悪用し，被害を受けたコンピュータ上で承認されていないプログラムを実行して情報を書き換え，そのコンピュータから新たなターゲットに向けてメールを自動送信する。

---

[13] クリックすると自動実行するプログラムのタイプのこと。

バブルボーイが感染する環境は，OutlookとWindows95，98，2000， そして Internet Explorer（IE）の5.0またはそれ以降のバージョンである。バブルボーイはマイクロソフト社がすでに対処を行ったセキュリティーホールを狙ったものであるが，多くの利用者はこの修正パッチプログラム[15]による保守をしていないことが多い。

バブルボーイ自体は，電子メールによって蔓延する潜在能力があることを除けば，比較的穏やかなウィルスであるが，コンピュータからファイルやプログラムを削除するような機能を持った，急速に感染を広げる悪意のあるプログラムに作り替えることも可能である。

知らない相手から送信された電子メールでも「添付ファイルを開かなければ安全」というのがこれまでの常識であったが，今や「電子メールを使うならウィルス駆除ソフトをインストールしなければならない」という所まで来てしまっている。

バブルボーイからパソコンを防ぐためには，マイクロソフト社から提供されているパッチプログラムを使用しなければならない[16]。ウィルス駆除ソフトにこのプログラム用のパターンファイル[17]を追加すれば，インターネット・サービス・プロバイダーや企業ネットワークのウィルスウォール[18]で，このウィルスの蔓延を防ぐことが可能である。

２．４　「パワーポイントファイルに感染するウィルス」の出現

マイクロソフト社のWord，ExcelあるいはAccessで作成されたファイルに感染するウィルスはあるがPower-Pointファイルに感染するウィルスは存在しないと思われてきた。しかし，1998年12月25日にPower-Pointに感染する初めてのウィルス P97M/Vic.A が発見された。

---

[14] http//www.zdnet.co.jp/news/9911/10/b_1109_01.htmlを参照。

[15] プログラムの不具合を正すためにメーカから提供される修正プログラムのこと。

[16] http://www.microsoft.com/windows/ie_intl/ja/security/eyedog.htmlを参照。この修正プログラムを多くの利用者が実行していないということは利用者の責任のように思えるが，ソフトウェアメーカの修正パッチのリリース方法や修正情報の提供方法等，メーカにも責任があり，手続きの改善余地があるはずである。

[17] ワクチンプログラムが，ウィルスを発見するために参照するファイルのこと。

[18] ウィルスチェック機能を持ったゲートウェイのことで，出入りする全ての情報について，チェックを行うことが重要である。

このウィルスはCドライブのMy Documentsディレクトリとサブディレクトリにあるポワー・ポイントプレゼンテーションファイルに感染する。このウィルスが感染するためには，プレゼンテーションファイルにユーザーフォームが存在しなければならない。このユーザーフォームとは，Visual Basicエディターを使って作られるウィンドウやダイアログボックスのことで，実際にPower-Pointのプレゼンテーションでユーザーフォームを使うことはまれであるので，実害は少ないと推測される。ウィルス対策担当者は新しく発見されるウィルス情報を常に収集し，自分の組織における影響を考慮して，対策に反映させることが必要である。

２．５　リモートコントロールにより自己変化するウィルスの出現

ポリモフィック型ウィルスは感染するごとにウィルスが変化することが知られている。しかし，1999年12月，自己変化するまったく新しくタイプのウィルスW95/Babylonia（以下，バビロニア）が米国で発見された[19]。このウィルスはサーバーにアクセスする機能を持っている。サーバーのアドレスはウィルスの中に組み込まれており，バビロニアはこのサーバーの指示により，即ちリモートコントロールにより，自己変化を遂げるのである。

見されたウィルスをチェックすれば，どのサーバーが指示を出してウィルスを変えているかは判明する。その問題となるサーバーは日本に設置されているものであった。ウィルス作者はインターネットを経由してサーバー管理者になりすまし，このサーバーの中に必要なデータを書き込んだものである。

米国では連邦法によりウィルスの配布が禁止されており，FBIなどの厳しい取締りがあるので，米国よりも法的にも制度的にも整備が不十分な日本のサーバーを狙ったものである。インターネットに接続する場合は，サーバー管理者は必ずこのようなリスクを認識することが必要である。

バビロニアは，IRC(チャット用ソフトの一種)やWebアクセスを通じて自己繁殖していくもので，IRCを通じて，” Y2KBug-MircFix.exe ”というファイルを送信する。その意味でこのウィルスはY2K問題を悪用したウィルス(Y2Kウィルス)と言える。

---

[19] 日本経済新聞 1999年12月8日 を参照。

２．６．「ウィルスには作成者の証拠が残らない」という常識

1999年3月26日にメリッサが発見され，4月1日にFBI及び州警察がニュージャージー州在住のデビッド・スミス容疑者（30才）を逮捕した。彼はその罪を認めており，それは最大で禁固10年，罰金15万ドルといわれている[20]。その際，犯人探しの有力な情報の一つになったものがＧＵＩＤであった。

ＧＵＩＤとはGlobal Unique Identifierの略で, その中にMacアドレス(ＬＡＮカードに書き込まれた個体識別のためのユニークコード)が含まれている。ＧＵＩＤはマイクロソフト社のOffice（Word，Excel，Power-Pointなど）やその他のアプリケーションで作成された資料に，自動的に付加されており，それらの資料を詳細に調べればどのコンピュータで作られた資料であるかが判明する。メリッサの犯人は，自分が作成した文章のＧＵＩＤを消さずに残してしまっていた。

しかしＧＵＩＤのみでは決定的証拠とはなり得ない。その理由は以下の通りである。

①どのコンピュータで作成されたかが明らかになっても，必ずしもそのコンピュータの所有者が作成したとは限らない。所有者以外の者がそのコンピュータを使って作成することも可能である。

②知識のある者はＧＵＩＤのコードそのものを改ざんすることが出来る。 即ち他人のコードに変更することも可能である。

結局ＧＵＩＤは，このような知識を持たない一般ユーザーにとっては，自分の知らない間に自分の持つコンピュータ固有の情報を提供することになり，インターネット社会の恐ろしさを如実に表している。

２．７　コンピュータウィルスは空気感染しないという常識

インフルエンザウィルスは空気感染するが，コンピュータウィルスが空気感染するとは思われていなかった。しかし，現実にはすでにそのことが起きている可能性が高い。その理由は次のとおりである。

ウイルスの新たな標的は携帯端末といわれている。ウィルス作成者は常に時代の先を読

[20] 一部では，禁固40年，罰金48万ドルとも報道されている。

み，新たな機能を持ったウィルスを作成し続けている。ネット接続機能を備えたＰＤＡ[21]や携帯電話が増えるなか，2000年８月にはPalmOS上で動作する初のウイルス「PALM_LIBERTY.A」が発見され，９月にはPalmOS上で動作する初のファイル感染型ウイルス「PALM_PHAGE.A」およびトロイの木馬型「PALM_VAPOR.A」が発見されている。

一方， Bluetooth と呼ばれる無線技術は，150フィート以内の距離にあるデバイス同士が相互に通信してデータをやり取りするための技術で，すでに実用化されているいる。この技術を利用すれば，ＰＤＡからパソコンまたは，パソコンからＰＤＡにウィルスが空気感染するのは間違いなく起きることである。残念ながら，ウイルスが空気感染することを妨げる手段は見つかっていない。

２．８　Word，Excel，Power Point のすべてに感染するウィルスの出現

ウィルスは宿主となるファイルの種類によって分類されている。WMならWord Macroウィルスを意味し，ＸＭならExcel Macroウィルスを意味している。ところがWord，Excel，Power Point のすべてのファイルに感染するウィルスが出現した。そのウィルスの名前は，O97M/Tristate と呼ばれるもので，O97M 即ち Office97に感染するウィルスとして分類された。しかし，実体としてのウィルスは，Word ，Excel，Power Point のいずれかに存在するので，それぞれ，W97M/Tristate，X97M/Tristate，PP97M/Tristateと名づけられている。このように，感染時に宿主となるファイルの種類を多く持つ事により，ウィルスにとっては被害を広範囲に拡大することが可能となる。

２．９　ウィルスに感染してもワクチンで駆除できるという常識

ウィルスに感染してもワクチンで駆除できるという常識があったが，一度感染すると新しいワクチンをインストールさせないウィルスが現れた。このウィルスはＰＥ_ＭＴＸと呼ばれるもので，前述のとおり2000年11月には日本国内でのウィルス届出件数が最も多いウィルスとなった。

このウィルス（マトリックス）は大きく分けて，①感染活動 ②ハッキングツール活動

---

[21] personal digital assistants　電子手帳などの携帯用の情報端末

③ワーム活動の三種の活動を行うが，Windows95/98環境でのみ動作し,WindowsNT/2000環境では動作しない[22]。ワーム活動としては，E-Mailが送信されると同時にウイルスファイルを添付した空のメールを同じ宛て先にもう一通送信する。送信するメールにはタイトル(subject)はなく，本文もなくファイルが１つ添付されているだけである。そのファイル名が送信した日付によって３１通りに変化する。例えば，1日の場合，I_wanna_see_YOU.TXT.pif というファイル名になり，3日の場合， LOVE_LETTER_FOR_YOU.TXT.pif となり，中身を見てしまいたくなるようなファイル名が付けられている。

もしこのウィルスの感染方法に付いての知識を持たない人の場合，知人からメールが来ていて，そのメールのすぐ後に同じ知人からもう一通のメールが来ていれば，クリックして添付ファイルを見てしまう人が大半であろう。メリッサウィルスやラブレターウィルスがメーリングリストを利用して爆発的に感染を広げたことと比較すると，添付ファイルのタイトルを変えたり，一度に大量のメール発信を行わないことにより，着実に感染被害を拡大させたと言える。

このウィルスのもう一つの大きな特徴は，ワクチンのインストールを妨害することである。一般的にワクチンを有効に機能させるには，各自のパソコンに最新のウィルス情報を持ったパターンファイルをインストールすることが必須であるが，このウィルスに感染すると，そのパソコンはワクチンを供給しているサイト（ワクチン会社のＵＲＬ）にアクセスできなくしてしまう。従って，一度，感染すると最新のパターンファイルをインストールできないため，結果的にはそのパソコン自身ではウィルスを駆除できなくなる。即ち，ウィルスに感染してもワクチンで駆除できるという常識は覆された。

このウィルスは実行ファイル（ＥＸＥＣファイル）に感染し実行不能にしてしまうので，ＯＳの再インストールを行うことが必要となる。このような状況になった場合，ＯＳの再インストールの手間ばかりでなく，ファイルのバックアップを取っていなかったユーザーにとっては重要なファイルを失ってしまい，甚大な被害を受けることとなる。今後，被害が益々拡大することが懸念される。[23]

---

[22] http://inet.trendmicro.co.jp/virusinfo/default3.asp?VName=PE_MTX.A　及び http://www.jcsa.or.jp/vi-w32mtx.html　を参照

[23] トレンドマイクロ社では警戒レベルを９月11日付けでVAC4，17日付けでVAC3，としたが，10月3日には警戒レベルをVAC2に引き上げ，警告している。

このウィルスは，メールの自動発信機能を持ったワームタイプ（ウィルス名称：ＰＥ_ＭＴＸ）とトロイの木馬タイプ（ウィルス名称：ＴＲＯＪ_ＭＴＸ）も発見されている。

２．１０　パソコンの電源を入れておくだけで感染するウィルスの出現

従来はウィルスに感染するには電子メールを受け取るか，ＣＤ－ＲＯＭやフロッピーディスクなど何らかの外部記憶媒体をそのパソコンで読ませることが必要だと思われてきた。しかし，パソコンの電源を入れておくだけで感染してしまうという，新しいウィルスが出現した。[24]

そのウィルスは，2000年10月マイクロソフト社本社にハッカーが侵入する際に利用されたもので，W32.HLLW.QAZ.A（略称：QAZ.Trojan）と呼ばれ，トロイの木馬型ウィルスである。

このウィルスは，第一段階は電子メールやＷｅｂサイトからのダウンロードまたはＩＲＣチャットルームなどを経由してパソコンに感染する。第２段階として，そのパソコンからＬＡＮ内のパソコンに感染を広げる。その感染方法に特徴がある。ウィルスはまずＬＡＮ内でシステムファイル（通常はＣドライブ）の共有機能がONになっている他のパソコンを探し，そのパソコンのメモ帳をウイルスと置き換えて感染を広げる。即ち，同一ＬＡＮ内にQAZ.Trojanに感染したパソコンが1台でもあれば，Ｃドライブのファイル共有をしているパソコンは，電源をONにしているだけですべて感染してしまう。そして，このウィルスに感染すると，このウィルスの本来の目的である，ハッカーが容易に侵入するための出入り口を開けてしまう。[25]

このウィルスは2000年７月に中国で発見されたもので，ワクチンは2000年７月中旬には出来ており，チェックを行えば発見できたはづである。しかし，マイクロソフト社では社員の自宅のパソコンがまずそのウィルスに感染し，自宅のパソコンから会社のパソコンに感染した可能性が指摘されている。すべてのパソコンに最新のワクチンをインストールし，最新のパターンファイルに更新をし，確実にウィルスチェックを実施していれば防ぐこと

24　http://www.zdnet.co.jp/news/0010/30mshack3.html　を参照

25　具体的には，複数のウィルスプログラムの１つが特定のポート（ＴＣＰポート7597）を開き，ハッカーはここから侵入できる状態となる。

が出来たであろうが，全社員が確実にウィルスチェックを行うことが如何に難しいことかは容易に想像できる。一般的にインターネットとの出入り口は最新のパターンファイルに更新し，厳しいウィルスチェックを行っているが，ＬＡＮ内のウィルスチェックは比較的ゆるやかになっている場合が多い。

QAZ.Trojanは日本でもすでに発見されており，今後，被害の拡大が懸念される。このように最近の傾向として，ハッキングツールの一つとしてウィルスが利用されるようになってきており，総合的な情報資産保護対策の重要性が増加している。

QAZ.Trojan はＡ社でも10月下旬に社内で発見された。Ａ社ではこのウィルスが発見されるとすぐさま，全世界の情報担当者に「Cドライブ」のファイル共有を中止するよう緊急通達を出した。

Ａ社においてはこのように連絡体制がグローバルに構築されているが，今回のように一度，ＬＡＮ内に侵入，自動繁殖するウィルスを駆除することは非常に手間がかかり，それに伴う被害の発生が懸念されるところである。

３．マクロウィルス対策事例分析

1997年４月，ある団体から約2000台ものパソコンがウィルスに感染していたことが情報処理振興事業協会（ＩＰＡ）セキュリティセンターウイルス対策室に報告された。これは，１件で感染した台数としては1997年１月の約1,000台という記録をわずか３ヶ月で塗り替えたことになる。インターネット技術を利用した社内ネットワーク（イントラネット）の普及によりウィルスに対する脅威は従来と比較にならない程，急激に増加してきている。適切なウィルス対策を講じていない場合，イントラネットに接続されている多数のパソコンがウィルスに感染し，ある日突然発病して業務に大きな被害を及ぼす可能性が高まっている。このような状況をふまえ，イントラネットを利用したウィルス対策の実務経験をもとに，マクロウィルス対策の事例分析を行う。

３．１　当該企業の情報システム

Ａ社（概要は前述の通り）は国内外に数百拠点の事業所があり，社内の１万２千台のパ

ソコンがプロプライエタリーなネットワークとオープンネットワークとに接続されている。情報システム要員は国内外に数百人が在籍し，主要拠点に配属されてシステム開発及びエンドユーザーサポートを行なっている。情報システム要員の約半数が本社情報システム部門に所属し，主要拠点の情報システム要員と業務連携を行なっている。社内はイントラネットを利用した電子メール及びグループウェア環境が整備され，海外拠点の情報システム要員を含め，情報システム要員同士の情報交換が活発に行われている。

該社では，1995年にパソコンネットワークによる業務革新を推進するため，業務革新社長プロジェクトが発足し，向う1年間に３千台のパソコンを新規導入することが決定された。筆者は当時，本社情報システム部門に属し，情報システムの全社的企画推進及びシステム監査を担当しており，業務革新プロジェクトのメンバーでもあった。そしてパソコンネットワークの全社展開にあたり，セキュリティ重視の観点から，新規導入する全てのパソコンに全社統一の最新ウィルスチェックソフトを導入することを強く提言し承認された。その結果，筆者及び数名の要員でウィルス対策担当組織（以下ウィルス担当）が発足した。ウィルス担当としては，日々新たに発生しているウィルスに対する情報を提供し，社内のウィルス発見状況をオープンにすることで，社員全員が自分自身にも起こりうる身近な問題として認識することを目指した。そのため，情報を集中化して全社的にウィルス情報及び対策を一元化すべきと考えた。なおチェックソフトの費用は，本来は社内エンドユーザー部門が負担すべきであるが，ネットーワークセキュリティーの統一的推進の観点より，当面は全額本社情報システム部門が負担するととした。

３．２．ウィルス発見の状況把握とエンドユーザへの配慮

ウィルス対策実施には，社内でのウィルス発見状況を把握することが重要である。組織発足当初は毎月数件程度のウィルス発見報告があり，エンドユーザー部門を受け持つ各情報システム部門とウィルス担当とが連携してウィルス駆除を行なった。ウィルスが発見された時，エンドユーザーに対しては「早期発見なので発病する前であり，被害拡大を防げたこと」及び「ウィルスは誰もが感染する可能性を持っており，自分自身も他人に感染させたかも知れないこと」を強調することとした。なぜなら，初めて自分のパソコンにウィルスを発見したエンドユーザは，してはいけないことをしてしまったかのような罪悪感に陥ったり，また自分にウィルスを感染

させた個人を特定したいとの気持ちにかられる場合が多く，その気持ちを少しでも和らげることが必要と考えたからである。

エンドユーザに対しては，以下の観点での説明を心がけた。

（１）コンピュータウィルスはプログラムで出来ており，風邪のウィルスとは異なる。

（２）誰もがウィルスに感染する可能性を持っている。

（３）ウィルスを発見するには，チェックソフトが必要であり，毎日チェックソフトを実行することが被害の拡大を防ぐ。

（４）ウィルスを駆除するには，ウィルス駆除用ソフトウェア（以下，ワクチン）が必要である。

（５）毎月新しいウィルスが発生しており，ワクチンは最新のパターンファイルを使わない限り，新しいウィルスは発見できない。定期的にパターンファイルを新しいものに入れ換えることが重要である。

（６）ウィルスは，多くは感染・潜伏・発病の３つの状態があり，知らずに感染してしまった場合，その瞬間からウィルスはパソコン内に潜伏し，発病するまたは発見されるまでの間，そのパソコンがウィルス感染を広げる手助けをしていることになる。ウィルスの発病によりそのパソコン自体も被害を受けることが多い。

（７）ウィルスを発見したときや異常現象を発見した時は，必ず情報システム部門に連絡する。

ウィルス発見状況を把握するには，できる限り現場の人々が理解しやすく，ウィルス対策に協力的になるよう配慮することが重要である。

３．３　イントラネット活用による情報共有の環境整備

社内通達などで「毎月最新のチェックソフトに更新し，毎日実行すること」と連絡を出していても，実際にエンドユーザーがチェックを行わなければ，何の役にも立たない。エンドユーザー自らがウィルスにある程度の関心を持ち，実際に毎日チェックを行なように習慣づけるため，全社で導入されているグループウェアを利用することとした。グループウェア上に「ウィルス対策データベース」（以下ウィルス対策ＤＢ）を作成し，全国にその旨を連絡した。ウィルス対策ＤＢの項目と概要及び機能は，表２．１の通りである。

ウィルス対策ＤＢは，誰もが質問や意見を記入できるようにし，毎日ウィルス担当が内

容をチェックし迅速に回答を行なった。

表２．１「ウィルス対策ＤＢの項目と概要及び機能」

項 目	概要 及 び 機 能
１.ウィルス情報掲示板	緊急連絡と一般連絡とに分けられている。 緊急連絡欄：緊急を要する内容を掲載し必要に応じ内容更新する （例：経理掲示板でマクロウィルス「ラルー」発見） 一般連絡欄：以前に緊急連絡欄に掲載していた内容や，ウィルス担当からエンドユーザーに知らせたい内容を掲載する。 （例：英語版のチェックソフト導入開始。その他の言語ニーズをご連絡下さい）
２.最新版ウィルスチェックソフトの配布	ＯＳ別に掲示：Ｗｉｎｄｏｗｓ 95用／98用／ＮＴ用／ＭＡＣ用など 自動更新１：最新ソフト（パターンファイル）を定期的に（毎週月曜日の12時～1時など）自動的にダウンロードする仕組み（時刻は各パソコン毎に設定する） 自動更新２：ボタン操作で，最新ソフト（パターンファイル）を自動的にダウンロードできる仕組み
３．駆除方法・特徴	型別・ウィルス名別に掲載。発病症状等の説明を含む。 １．ブートセクター感染型 ２．ファイル感染型 ３．データ感染型（マクロウィルス） ４．心理的感染型［詳細後述］
４．被害報告	ウィルス名別・部署別に分類整理。 グループウェアで被害報告用標準フォームを作成し，入力工数の削減及び項目を統一。 様式は情報処理開発協会発行の「ウィルス対策基準」の「ウィルス被害報告基準」に準拠。 社内拠点ならどこからでも入力可能とする。

３．４　Good Timesウィルス騒ぎ

正確にはウィルスに分類されるものではないが，心理的感染型ウィルスとも言うべきものがある。当該企業でも， Good Timesウィルス騒ぎが発生したことがある。Good Timesウィルスとは以下のようなものである。

ある人から次のような電子メールが送られてきたとする。

「最近，米国でまったく新しいタイプのウィルスが発見されました。このウィルスは非常に強力な感染力を持っています。［ Good Times］というタイトルのメールが届いても決して開いては（中身を見ては）いけません。もし，そのメールを開けば，あなたのパソコンのディスクは破壊され，その上，あなたのメーリングリストに書かれている全ての人に自動的にそのメールが転送され同じような被害に遭います。このことをあなたの親しい友人･知人に，今すぐ知らせてあげてください。」

このようなメールを受け取った人はメールに書かれている通り，親しい友人や知人にこの内容を知らせてしまう。しかし，実際にはここに書かれている Good Timesというウィルスは存在しない。これは，チェーンメールの１種で悪質ないたずらに過ぎない。

海外に駐在する情報システム要員から「Good Timesという新種のウィルスが発見されたとの報告があるが，その情報は入っているか，情報は正しいか，対策はどのようにすれば良いか」との問い合わせが第１報であった。その後わずか数日の間に，社内外から Good Timesに関する情報が続々とメールで送られてきた。Good Timesのウィルス情報の信憑性に疑問を持つ人も一部にはいたが，多数の人がこれは大変だと思い込んでしまい，メールの内容に書かれている通り自分の友人・知人に急いで連絡をした。会社幹部にまで Good Timesメールを転送した社員もいた。ウィルス対策ＤＢを作成していたことにより，そのことを知っていた情報システム要員からの問い合わせは実に有効であった。インターネットで調査をし，それが全くのデマであり，悪質ないたずらであることはすぐに判明した。Good Times騒ぎは以前にも発生しており，以前からインターネットを利用していた人々の間では，なかば常識レベルの知識であることもわかった。しかし，新しくイントラネットを利用するようになった人々はそのような知識に乏しく，何処に問い合わせをすれば良いかも分からないのが実状である。ウィルス担当はウィルス対策ＤＢの「緊急連絡」欄にGood Timesウィルス情報を掲載した。その内容は「Good Timesウィルスは全くのデマなので誤った情報に惑わされないように。メールは決して転送しないこと。」であった。 ウ

ィルス発見情報は，エンドユーザから情報システム部門に必ず連絡が入っており，ウィルス対策ＤＢで正確な情報を把握している情報システム要員は，適切に対処することが出来た。その結果，１週間程で騒ぎは収まった。

以上のことをイントラネットを使わずに，従来のように，コピーして封筒で配布していたとすれば，スピードは格段に遅くなっていたであろうし，あまりに負荷がかかるため，実際には実行できなかったであろう。イントラネット時代のウィルス対策はイントラネットの有効活用による情報伝達と情報共有が重要である。この騒ぎが契機となって，エンドユーザにもウィルス対策ＤＢの重要性が認識され，参照するユーザーが増加した。正確な情報を如何に早く多数の関係者に配布できるかが，重要な要素であると認識できた。ウィルス担当としては，被害が広がる前に正しい情報提供が出来たと評価している。

2000年４月現在，ＣＩＡＣ[26]に登録されているチェーンレターとしては次の33種類がある。

PKZ300, Irina, Good Times, Good Times Spoof, Deeyenda, Ghost,E-mail Tax PENPAL GREETINGS!, Make Money Fast, Naughty Robot, AOL4FREE, Join the Crew, Death Ray, AOL V4.0 Cookie, A.I.D.S. Hoax, Internet Cleanup Day, Flesh Eating Bananas, Bill Gates Hoax, Miller's Free Beer, Netscape-AOL Giveaway Hoax, GAP Giveaway Hoax, IBM Giveaway Hoax, Disney Giveaway Hoax, Ericsson/Nokia Phone Giveaway Hoax, WIN A HOLIDAY, AOL Riot June 1 1998, E-mail or get a Virus, Bud Frogs Screen Saver, Blue Mountain Cards, Internet Access Charge, Geeks Bearing Gifts, Elf Bowling and Frogapult Hoax Chain Letter, Takes Guts to Say Jesus Hoax

日本国内ではＩＰＡがデマウィルスとして，上記の内，日本語に翻訳されているものを含め22種類を掲載し注意を促している。[27]

３．５　海外を含めたマクロウィルス対策の重要性

1996年夏，米国で発見されるウィルスの内，マクロウィルスが約半数に上るという重大

---

[26] http://ciac.llnl.gov/　Computer Incident Advisory Capability:米国エネルギー省

[27] http://www.ipa.go.jp/security/index.html　情報処理振興事業協会

な情報が入ってきた。社内でも既に数件のマクロウィルスが発見されていたが，その当時のウィルスチェックソフトでは，マクロウィルスが発見できなかった。数ヶ月後，マクロウィルス対策済みのチェックソフトが配布された。

当該企業では毎年秋に社内情報フェアーという催しをおこない，社内ユーザーを対象に新しく開発したソフトのデモや展示を行なっている。昨年の社内情報フェアーでは，ウィルスの発病デモを行ない，社内のウィルス発見状況を展示説明した。そしてウィルスが身近な問題で誰もが感染する恐れがあり，放置しておくと深刻な被害を及ぼすかも知れないこと，また新型マクロウィルスを発見するためには最新のチェックソフトに入れ替えることが重要であると訴えた。

さて，最新のチェックソフトに入れ替えを行なった部署からワードマクロウィルス WM.Ｃｏｎｃｅｐｔ（以下コンセプト）発見の連絡が入った。調査の結果，海外子会社からのメールの添付資料に感染しており，すでに数ヶ月が経過していた。しかし，コンセプトは英語環境のＭＳ－ＷＯＲＤに感染するが，感染したパソコンで日本語のＭＳ－ＷＯＲＤ文章を作成しても感染は広がらないので感染はごく一部であった。

海外子会社からのメールで，コンセプトが発見されたことはメール送信元にも連絡をしたが，数ヶ月後，同じ部門から送付されたメールに再度コンセプトが発見された。その後も海外からのメールでマクロウィルスが数回発見されている。以上のことから，海外拠点では適切なウィルス対策が取られていない状況が判明した。このことを通じてイントラネット時代には，国内だけのウィルス対策では不十分で，海外拠点・子会社を含めたグローバルな視点での対策が重要であるとの認識を深めた。

３．６　正しい情報入手の重要性

ある事業所でＮＡＣＩＴＡ（以下ナシータ）が発見されたとの連絡が入った。チェックソフトメーカに問い合わせたところ，このウィルスの発病日は「11月15日」で，古い仕組みのハードディスクに対して発病（ディスク破壊）するが，新しいハードディスクでは発病しないとのことであった。ウィルス担当に連絡が入った日から，「ウィルス発病日」まで残された時間は２日間しかなく，すぐさまウィルス担当が現場に出向き，調査し駆除を行なった。ウィルス担当はその事業所を担当している情報システム要員と共同して，事業所内の全てのパソコンを調査した結果，ナシータとアンチシーモスに事業所内のほとんど

のパソコンが感染していた。この事業所は以前からパソコン導入に積極的であったが，古いパソコンにはウィルスチェックソフトがインストールされていなかったり，インストールされていても古いバージョンのままであった。エンドユーザー全員に最新のソフトを配布することの難しさを実感した。

その数日後，ある事業部門から十数台のパソコンが急に動かなくなったとの連絡が入った。トラブル発生が11月15日からとのことなのでナシータによるディスク破壊であると推測された。担当者の話では，そのパソコンに数ヶ月前から毎回電源投入時に「ウィルス発見」のメッセージが出ていたという。担当者はすぐに「確認」ボタンを押して毎日業務を続けており，「ウィルス発見」メッセージは「確認」ボタンを押せば消えるという程度にしか考えていなかった。発病後は，ディスクは完全に破壊され，バックアップも取っていなかったため，その部門は大きな被害を受けた。エンドユーザは自分がウィルスに感染しているということはできるだけ言いたくないということ，ウィルス情報は１社だけの情報をうのみにせず他社のホームページからも情報収集すること，及びウィルスの危険性についての広報活動の重要性を認識した事例であった。

３．７　イントラネットで最新パターンファイルに更新する仕組みを自社開発

最新版パターンファイルをインストールする方法は，情報システム要員が手作業で担当するエンドユーザーのパソコン１台づつにインストールすることを前提にしていたので，当初はフロッピー方式だけであった。しかし，このことは情報システム要員に大きな負荷がかかるため，まれにしか実行されない状況であった。このような状況に鑑み，ネットワークを利用して自動的に最新版パターンファイルをインストールできる仕組みの必要性を痛感し，エンドユーザが自分自身のパソコンでボタン操作だけで簡単にダウンロードできる仕組みを自社開発した。これにより，エンドユーザーは情報システム部門に頼ることなく自らの意志で，新しいウィルスから自己防衛できるようになった。最新版パターンファイルに更新したことにより，数ヶ月間は問い合わせや被害届けが急増した。しかし潜在ウィルス駆除が完了した後，被害件数は徐々に減少した。そして，パソコン本体（ディスク）に感染する前に発見している報告事例，つまりフロッピーやメールを取り込む段階で発見している事例が増加し，日常的にウィルスチェックが行われていることが判断できるようになっていった。

３．８　マクロウィルス大量感染防止のための事前対策の重要性

社内の経理部報は全てイントラネットを経由して全経理担当者に配布されており，その添付ファイルはエクセルで作成されている。従って，ウィルス担当としてはエクセルに感染するマクロウィルスの危険性について特別な注意を払っていた。なぜなら，従来のチェックソフトには，エクセルのマクロウィルスチェック機能が組み込まれていなかったため，全国の経理担当者用の掲示版にエクセルに感染するマクロウィルス ＸＭ．Ｌａｌｏｕｘ（以下，ラルー）が感染した場合，感染被害の拡大が非常に早くかつ広範囲で，駆除に多大の工数が必要になると推察されたからである。ウィルス担当としてはその数ヶ月以前より，マニュアル（手操作）で経理担当のパソコンにラルーが感染していないこと，及び経理担当者用の全国掲示板の添付ファイルにラルーが感染していないことを確認していた。ラルーについては，社外からのメールに数件が発見されており，インターネットを始めとして色々な所からラルーに関する情報が入って来ていた。ラルー対応のチェックソフトが提供されると，すぐに全社の情報システム部門長に連絡した。その数日後，経理担当の全社掲示板の添付資料にラルーが発見された。ウィルスはすぐさま除去し，この情報は全国の経理担当者に送られ，全国の経理担当者が一斉に最新のウィルスチェックソフトを各自のパソコンにインストールしてウィルスチェックを行なった。その結果，一部の工場では，多数のパソコンがラルーに感染していた。しかし発見が早く，関係者への連絡が早かったため，全国規模での大量感染は直前で食い止められた。しかし，ラルーはその月の社内ウィルス発見件数・台数ともに，一位となった。もし，発見が１週間以上遅れていれば，感染は千台を超えていたであろう。

ラルーについては，一部の企業で大量感染が発生し，駆除に多くの負荷がかかり，業務の遂行に影響を及ぼしたことが報道された。ウィルス担当としては，事前の情報収集及び対策実施により，被害を最小限にくいとめ，早期発見，早期駆除ができたと評価している。

３．９　新発見から自社に到着するまでが対応期間

ある社外からのメールの添付ファイルにワードマクロウィルス WM．ＣＡＰ（以下キャップ）というマクロウィルスが感染していた事実が，メール発信元から連絡が入った。こ

のマクロウィルスは，ＭＳ－ＷＯＲＤのマクロ機能を使えなくするマクロ命令が組み込まれており，このウィルスに感染したパソコンは，マクロ命令が消去されマクロ命令を利用したＷＯＲＤ処理ができない。ウィルスに感染していた社外からの添付資料は，そのまま社内の全国掲示板に掲載され，すでに一日が経過していた。ログを調査した結果，全国で数名がこの掲示板を参照していたことが判明し，その旨を該当者に連絡し感染拡大を防いだ。残念なことに，当時利用していたチェックソフトでは，キャップは発見できなかった。しかし発見方法及び駆除方法についてインターネットで調査・検討した結果，数分後には対処方法を全国に情報発信することができた。このウィルスは世界で初めて発見後わずか２ヶ月で日本に上陸したことも判明した。最近では世界で初めて発見されてから，その翌日に国内で発見されている例も珍しくはなくなったが，当時としては予想をこえたスピードであった。

ウィルス担当は常に世界中に目を向けて，新たに発生している危険なウィルスに注意を払わなければならない。最近どのようなウィルスが脅威になっているかをチェックし，未然防止するよう努めなければならない。現在利用しているチェックソフトは万能ではなく，発見できない新種のウィルスもあり，それに対して注意を払い，防御策を講ずることも重要である。時には休日を返上してのパターンファイルの入替えなどの対策実施を含め，常に情報収集をすることが求められる。そして，最新の情報をできるだけ早くエンドユーザーに提供することが必要である。先ほどのラルーやキャップはその良い例である。「予防は治療にまさる」を肝に銘ずるべきである。

４．ウィルス担当の心構え

以上，事例分析を含めウィルス対策の実際を述べてきたが，ウィルス担当としての心構えを以下の4つのカテゴリーに分けて述べる。

（１）エンドユーザに対して

（２）ツール及び環境の整備

（３）教育及びリテラシーの向上

（４）その他留意点

４．１　エンドユーザーに対して

ウィルス担当としての，エンドユーザに対する心構えは表２．２のとおりである。

表２．２「ウィルス担当としての，エンドユーザに対する心構え」

ル ー ル	根拠
ウィルスの所有者を責めない	ウィルスが見つかったことは恥ずべきことではなく，誰にでも起きる可能性があるということを，多くの社員に理解させ，以後は確実に最新のワクチンを利用させることが重要である。
報告しやすい雰囲気を作る	情報共有を進めることにより，社内ユーザに被害の実態を開示し，誰もが報告しやすい雰囲気・環境を作り出すこと。
現場を知って対策を実施する	できる限り現場に出向くことにより，社内ユーザの声に耳を傾け，現場の人々の心境を察し，必要な対策を実施する。
発見後は徹底して駆除する	ウィルスが発見されればその職場の全てのパソコンはもちろん，全てのフロッピーのチェックを行なうよう指示する。ＭＯやＣＤ－Ｒ等のバックアップもチェックが必要である。

４．２　ツール及び環境整備

ウィルス担当としてのツール及び環境整備についての心構えは表２．３のとおりである。

表２．３「ウィルス担当としてのツール及び環境の整備についての心構え」

ル ー ル	根拠
ウィルス対策ＤＢを整備・活用する	ウィルスに関する情報を全社で一元化し，会社全体としてどのようなウィルスが発見されているかを把握すると共に，自らも情報発信を行なって，早期対策を実施する。

最新ウィルスチェックソフトの配布環境を整備する	イントラネットに接続している全てのパソコンに最新ウィルスチェックソフトを導入しやすい環境を提供する。（費用面・サポートデスクの充実等）
チェックソフトは容易な操作で配布する	社内エンドユーザーが最新のウィルスチェックソフトに容易に更新できるよう対策を講じる。 （例:イントラネットを活用してボタン操作だけでパソコンに最新モジュールをダウンロードする仕組みの提供）
メールサーバ・ファイルサーバーレベルでの発見を推進する	メールサーバー・ファイルサーバーにウィルスチェックプログラム導入を推進する。 （これにより，大量感染を防止できる）
自動配布ツールの導入を図る	自動配布ツールの導入を検討し，エンドユーザーが意識しなくても，最新のウィルスチェックソフトがサーバーからパソコンに配布される環境を整える。

４．３　教育及びリテラシーの向上

ウィルス担当としての教育及びリテラシーの向上についての心構えは表２．４のとおりである。

表２．４「ウィルス担当としての教育及びリテラシーの向上についての心構え」

ル ー ル	根拠
教育の実施	新しいタイプのウィルスに対する駆除方法や注意事項について，必要に応じ全国の情報システム要員を集めて教育を実施する。
サポートデスクの活用	サポートデスクと緊密に連絡を取ってサポートデスクメンバーに教育を行ない，容易に駆除できるウィルスについてはサポートデスクの指示で処理できる体制を整える。

最新ウィルス情報収集	ＩＰＡや関連するサイトの情報を収集し，また，ワクチンメーカと緊密に連絡を取ることにより，常に世界のウィルス発生状況に注意を払い，特に悪質なウィルスには早期に対策を講じる。
組織的対応を図る	日常のウィルス駆除については，サポートデスクや各現場にいる情報システム要員での対応を図る。ウィルス対策はウィルス担当だけの仕事ではない。全員で防ぐという心構えが大切である。

４．４　その他の留意点

ウィルス担当としての，その他の留意点については表２．４のとおりである。

表２．４「ウィルス担当としてのその他の留意点」

ル ー ル	根拠
一日一回ウィルス対策ＤＢのフォロー	一日一回以上はウィルス対策ＤＢを参照して質問に回答したり，全国の被害状況を把握する。ユーザーは，被害にあってからはこのＤＢを参考にしていることも多く，専門家としてのアドバイスは貴重である。
海外を含む総合的な対策の実施	海外を含め，イントラネット内の全てのパソコンに最新のチェックソフトを導入するよう体制を整える。 国内だけでなくグローバルな視点でのウィルス対策が必要である。特に海外部門は例え社内と言えども厳重な対策実施が必要である。 ファイアーウォールの構築に際して，ウィルスウォールの導入は必須であり，現代ではウィルスウォールなくしてはメールを利用した新種ウィルスの侵入を食い止めることは出来ない。

チェックソフトの限界を知る	現在利用しているチェックソフトの限界を知り，未対応の悪性ウィルスについては特に注意を払う。特にパソコンにインストールするパターンファイルを自動更新していない場合は，メールを利用した新種ウィルスに対しては，自社の環境で感染被害の可能性を把握しておくことが重要である。
現場から学ぶ	新しいタイプのウィルスが社内で発見されれば，できる限り現場に出かけて行って自らが対応し，状況を把握した上で，今後の対策を検討する。
社外との情報交換	できる限り，ウィルス対策に関係する社外の人々と情報交換を行なう。（日本国内で起きているウィルス状況の把握にはこれが重要な情報源となる。）
ウィルスを社外に配布した影響を考慮する	誤ってウィルスを社外に配布した場合の影響の大きさを考慮することが重要である。 相手に損害を与えるだけでなく，自社の社会的信用の失落，信頼回復に関わるコストの膨大さも大きな問題となる。メーリングサービスやメールの利用停止による業務の停滞等，その影響は図り知れない。
ウィルス検体を確保する	新しいチェックソフトの機能確認等に利用するため，ウィルス検体を確保しておく。ウィルス検体の保存方法については特別に厳重な注意を払う必要がある。

５．新たなウィルス対策と今後の方向性

５．１　新たなウィルス対策の必要性

ウィルスはワクチンで駆除できるので，各パソコンに最新のパターンファイルワクチンをインストールしていればそれ以上に広がることはない。しかし，発見されるウィルスの

件数・種類共に増加し，グローバル企業においては，新発見のウィルスが数日後に自社で発見されるケースも発生しており，１ヶ月に１回のパターンファイル更新では遅すぎる。

マクロウィルスが出現するまでは，ウィルス作成には高度な知識が必要とされた。しかし，メリッサのような非常に感染力の強いウィルスに感染したファイルを持っている人が多数存在しており，インターネットには比較的容易にウィルスを入手できる環境がある。ウィルスの多くは発病時の症状として，現在は無害のものが多いが，現存するウィルスの内容を少し変更することにより，驚くべき破壊機能を持ち，短時間で感染・繁殖するウィルスを作ることが可能であり，メリッサ事件はそれを例証している。

一方，ウィルスが発見されてからワクチンができるまでには数日間を要している。ウィルス対策担当者はワクチンが万能ではなく，常に後追いでできており，ワクチンが完成するまでは無防備状態であることを，強く認識すべきである。ラブレターウィルスやメリッサの例で見られるように，感染力が非常に強いウィルスは，ワクチンが完成するまでにすでに広範囲に感染しており，発見・駆除をするために多大の時間と労力を要している。特に社内とインターネットとの出入り口に設置しているウィルスウォールについては，常に最新のパターンファイルに更新していることが求められている。

近年のウィルスの傾向は，①メール機能を利用して自動的に送信配布するため，感染力が強く急速に広がる。EudoraなどOutlook以外のメールソフトでも感染するケースが増加している。②メリッサなどで明らかなように，無害のウィルスを変更して有害なものを，容易に作り出すことができるなど，新たな傾向を示している。

これまで，ウィルス対策として，喜入 博[4)] は以下の点を挙げている。

１．社内ポリシーの確立と経営層の理解

２．パソコン運用管理基準の策定

３．ウィルス対策組織の設立

４．ワクチンの採用

５．社内啓蒙・訓練の実施

これまで示してきたように，これまで常識とされてきたウィルスに対する考え方が，ことごとく打ち崩されており，新たなウィルス対策が必要となってきている。それは，組織に対応した手段が必要であるが，グローバル企業においては，以下の対策を実施することが重要である。

１．ウィルスの発見・駆除はパソコン本体だけでなく，ウィルスウォールで必ずチェッ

クを行うこと。

２．ウィルスウォールは常に最新のパターンファイルに更新しておくこと。

３．パソコン本体でのウィルスチェック用パターンファイルの更新は，ユーザーの操作に依存しなくても良いように，自動更新機能を持たせること。

４．JPCERT/CC(Japan Computer Emergency Response Team / Coordination Center）のメーリングリストへの登録を含め，常に世界から情報を収集し最新のウィルス情報を入手すること[28]。

５．技術と運用の両面で対策を実施すること。技術は予防が中心となるが，運用は早期発見や被害の拡大を防ぐことになる。

以上，これまでのウィルス対策のあり方に付加して，新たな 5項目が必要であり，この対策の有効性を確認するためには，システム監査の実施が重要である。

５．２　新たなウィルス対策のチェックポイント

前項では，ウィルス対策についてその具体的対策・方法を明らかにしたが，これらの対策・方法だけでは，充分に効果があるとはいえない。情報技術は常に進化しており，情報システムを拡大化することは，新たなセキュリティホールを内在化させることになる。また，これまで充分と思われてきたところが，技術の進展により，セキュリティ機能が劣化してしまうこともある。そこで，とられてきたウィルス対策が有効なものか，及びそれが効果的に実施されているかどうかを点検し評価するには，システム監査の継続的な実施が重要である。以下，新たなウィルス対策のチェックポイントについて，グローバル企業の事例をもとに論述する。

（１）トップマネジメントのセキュリティに対する認識の向上

企業等でセキュリティが組織内に徹底されるために，最も重要なことはトップマネジメント（企業経営者等）が，セキュリティ強化に対する強い信念を持つことである。企業の情報化が進展すればするほど，組織が所有する情報資産は重要になり，その消失や漏洩は組織にとって致命的になることも考えられる。このことをトップマネジメントが強く認識

[28] メーリングリストには http://www.jpcert.or.jp/announce.html で登録できる。

しなければならない。

具体的には，次のような事項が実施されているか，確認すること。

① システム監査担当部署を内部監査部門の中に設置し，情報システム部門の技術経験者をシステム監査人に任命しているか。

② 通常の業務監査の実施とともにシステム監査も実施されているか。

③ システム監査では，まず経営者のセキュリティに対する理解レベルとセキュリティポリシーを確認する。セキュリティポリシーは企業のあらゆる資産の保護に対する基本的な方針であり，経営方針と連動しているとともに，経営会議での承認がなされていることが重要である[29]。具体的には「セキュリティポリシー」を具現化するための「セキュリティガイドライン」の中に，「コンピュータへの不正侵入及びコンピュータウィルスに対して防御策を講じる」など，ウィルス対策についての基本方針が示されているか。

④ ウィルス対策組織やウィルス対策予算について，経営者の理解が不十分な場合には，システム監査人の立場から経営者に対して強く勧告を行うことが重要である。

（２）パソコン運用管理基準の作成と遵守

社内情報資産を安全かつ効率的に守るためには，パソコン運用管理基準を作成し，それが遵守されていることが重要である。

パソコン運用管理のシステム監査では，次のような事項が実施されているか，確認すること。

① 本社情報システム部門が「推奨パソコン」を決定しているか。具体的には，社内で使用するパソコンについて，メモリーやディスク容量などのハードウェア，及びブラウザーや表計算などのソフトウェアについて，推奨機種及び推奨ソフトウェアを選定しているか[30]。「推奨パソコン」で使うワクチンソフトについても決められているか。

② パソコンの管理は各職場が行うこととし，情報システムのサポートは，子会社の場合は子会社の情報システム部門，工場の場合は各工場の情報システム部門，営

---

[29] セキュリティポリシーについて，詳しくは 高瀬[5)] を参照。

[30] ソフトウェアについてはバージョンについても，決定することが重要である。

業部門では各地区毎の情報システム部門が実施しているか。

③ 各現場で使用されているパソコンをサンプリングして，最新バージョンのワクチンソフトが導入されているか確認し，古いバージョンのままで更新されていない場合は，改善勧告を行うこと。

④ 重要なファイルについてはバックアップが確保されているか[31]。

⑤ ファイル共有機能を活用して情報共有を推進している職場では，ファイル共有に使用しているパソコンのバックアップ（MOなど）が定期的に確保され，ラベルに日付を記入した上で，火災や地震などに対して安全な場所に保管されているか。

（３）ウィルス対策組織の設置と方針の徹底

ウィルス対策について組織的な対応を取ることが重要であるが，組織の実情に応じてさまざまな対応形態が考えられる。ウィルス対策担当者は必ずしも専任である必要はないが，組織的に責任と権限が明確化されていることが必要である。

具体的には，次のようなウィルス対策が実施されているか，確認すること。

① 本社情報システム部門内にウィルス対策担当部署を設置し，ウィルス対策担当者を指名しているか。ウィルス対策担当部署は全社のウィルス対策方針を策定し，全世界の事業所，子会社に対してウィルスに関する情報提供を行うとともに，被害情報を収集しているか。

② ウィルス対策担当者は，ワクチンソフトを新しいバージョンに更新する場合は，「推奨パソコン」との整合性チェックを行うなど，システム変更に伴うトラブルの未然防止に努めているか。また，ウィルス対策担当者は，新しいワクチンソフトの選定をしているか

③ システム監査の実施に際しては，ウィルス対策担当者が名目だけで，有効なウィルス対策が実施されていない場合もあるので，実状を確認する。

④ 全世界の子会社，工場及び営業所の情報システムをサポートする情報システム部門は，ウィルスについての本社方針を受けて，ワクチンソフトのインストール及びパターンファイルの更新をしているか

⑤ 子会社などではこれらの方針が徹底されていない場合もある。システム監査人は

---

[31] ウィルス対策を実施していても，運悪く発病してディスク破壊が起きることもある。

関連するホームページやデータベースを通じて，本社情報システム部門の方針を確認し，徹底させているか。

（4）ワクチンの採用とパターンファイルの更新タイミング

ウィルス対策にワクチンソフトの採用は必須条件であるが，ウィルス感染が広がるスピードに対応して，パターンファイルの更新が実施されていることが重要である。メリッサの例で見られるように，感染力の強いウィルスは，ワクチンが出来るまでに広範囲に感染していることもあるので，必要な対策がとられているかを確認する。

そのためにはウィルスウォールでのウィルスチェックが重要である。パソコンへのパターンファイルのインストールは，出来る限り自動更新する仕組みが望ましい。体制が整備されていれば，必ずしもすべてのパソコンに最新のワクチンソフトを配布する必要はない。組織の実状に応じ，効果的な対策が取られているかどうかを確認する。

具体的には，次のようなウィルス対策が実施されているか，確認すること。

① インターネットとの接続に際してはウィルスウォールを設けて，社外とやり取りしているすべてのメール及びファイルについて，ウィルスチェックを実施しているか。

② 社内発信のメールでウィルスが発見されれば，当該者にその旨を連絡してウィルス駆除をしているか

③ ウィルスチェックログが保管され，その内容について分析及び評価されているか。

④ パソコンのワクチンソフトについては，月１回程度のパターンファイルの更新では，自動メール機能を有したウィルスには対応が不十分である。指定したパソコンを立ち上げた時に，最新のバージョンソフト及びパターンファイルがインストールされているかを確認し，古い場合は自動的にインストールを行うことも必要である。但し，新しいワクチンソフトの自動インストール，及び，インストールする毎に全ファイルをチェックするには，時間とコストを要するので，業務の効率性を勘案することが必要である。特にすべてのパソコンに自動インストール機能を待たせる場合は，ＬＡＮのトラフィックを勘案し，業務に支障の無いような方法を選択することが必要である。[32]。

---

[32] 自動インストール機能については，パソコン毎にインストール時刻を変えて設定できる

⑤　自部署で利用する情報について，ファイル共有機能を活用して，組織的に運営管理している職場の場合，重要なファイルを保存しているパソコンについて，ワクチンソフトを自動インストールしているか。

⑥　パターンファイルの更新について，フロッピーディスクやＣＤ－ＲＯＭで実施している部署あれば，サーバーからダイレクトインストールする方法を紹介し，業務効率を向上させるよう改善勧告を行う。

（５）社内啓蒙・教育の実施

ウィルス対策は，最新のワクチンソフトとエンドユーザーの協力なくしては達成し得ない。そのためには社内の啓蒙及び教育活動が必要である。ウィルス対策データベースや新人教育を通じて，ウィルスに対する防御対策を広く社内に知らしめることが重要である。

社内啓蒙及び教育については，以下の事項が実施されているか，確認すること。

①　ウィルス対策担当者は，ウィルス対策データベースを設け，全世界の社内及び子会社で発見されたウィルスについて報告させているか。ウィルスが発見された場合，連絡を受けて実際にウィルス駆除を行うのは情報システム部門の担当者である。ウィルス被害報告についても情報システム部門の担当者が入力し，世界中でどのようなウィルスが新たに発見されたかが通達される仕組みを構築しているか。

②　ウィルス対策担当者は，新たな脅威が発生すれば，ウィルス対策データベースを通じて，緊急連絡，一般連絡など緊急度を区分して，ウィルス情報を発信しているか。

③　ウィルス対策担当者は，ウィルス対策データベースを通じて，全世界から寄せられるウィルスに関する質問について，回答しているか[33]。

④　情報システム部門に配属された新入社員全員にセキュリティ教育を実施しているか。その中でウィルスの脅威と防御対策について教育しているか。ウィルスによ

機能があることが望まれる。その理由は，現状のＬＡＮ環境のままで，一斉にすべてのパソコンに自動インストールを行うと，ワクチンソフトのバージョンを上げた場合には業務開始時刻に各パソコンに数メガ単位の情報が送付され，ＬＡＮのトラフィックが急増して，業務への悪影響が懸念されるからである。

[33] 運営はウィルス対策担当者が行うが，回答は必ずしもウィルス対策担当者だけとは限らず，広く情報システム部門のだれもが回答及びアドバイスができる。

る被害は，自社内での業務への悪影響だけなく，ウィルスが入ったメールや資料を社外に送ってしまうことにより，企業の社会的な信用を傷つけることを強調した教育をしているか。

⑤ ウィルスに関する対策及び方針は，本社情報システム部門内の経営企画会議で発表され全世界の情報システム部門の責任者に通達される仕組みを構築しているか。

５．３　グローバル・ネットワーク企業における，ウィルス対策の今後の方向性

これまで，グローバル・ネットワーク企業におけるウィルス対策の今後の方向性ついて，具体的にどのような対策を立案し，実施すべきかを分析した研究は，皆無であったと言ってよい。その原因は「ウィルス対策は，パソコンに最新のワクチンソフトを導入すれば十分である」といった考え方が存在すると思われる。しかし，グローバル企業においては，ワクチンソフトに多額のライセンス費用を支払い，すべてのパソコンにパターンファイルを配布するために，多大な労力をかけている。また，パターンファイルを更新する毎に，すべてのパソコンでウィルスチェックを行うため，企業全体としては多大の時間を費やし，業務効率を低下させている。このコストと労力及び時間をミニマムにするため，今後のウィルス対策の方向性を提言する。

ウィルスに感染するには，外部からのメールやＣＤ－ＲＯＭなど，何らかのきっかけが必要である。この外部からの入り口で，ウィルスチェックを確実に実施すれば，ウィルスから防衛することが可能である。具体的には次の方法で実施する。

① インターネットとの接続に際してはウィルスウォールを設けて，社外とやり取りしているすべてのメール及びファイルについて，ウィルスチェックを行う。

② 社内でやり取りされる，すべてのメール及び添付ファイルについても，ウィルスウォールでチェックを行う。

③ ウィルスウォールについては本社ウィルス対策担当者の指示に従い，当該サーバー毎にそれを管理する各情報システム部門が，最新のパターンファイルに更新する。

④ ウィルスウォールにより，社内メールでウィルスが発見されれば，メール発信者に連絡し，当該パソコンのウィルス駆除を行う。

⑤ 各職場単位でファイル共有機能を利用して情報管理レベルを高める。具体的には職

場単位で「共有パソコン[34]」を決め，そのパソコンに重要なファイルをすべて保存し，ワクチンについてはパターンファイルの自動更新機能を組み込む。更新用パターンファイルデータは，まず本社情報システム部門のサーバーから各拠点のサーバーにダウンロードし，次に各拠点のサーバーから「共有パソコン」に自動ダウンロードする仕組みとする。パソコンへの自動ダウンロードについては，始業時刻など特定の時間帯にトラフィックが集中しないよう，パソコン毎にダウンロード時刻を変えて指定する。

⑥ フロッピーやＣＤ－ＲＯＭなど社外から外部記憶媒体を社内に持ち込む場合は，必ず「共有パソコン」でウィルスチェックを行ってから使用することとする。

以上の対策を実施することにより，「共有パソコン」など一部のパソコンにワクチンソフトをインストールするだけで，ウィルスから防御することが可能となり，大幅なコストダウンと，労力と時間が削減され，業務効率の向上が図れる。しかし，以上の対策を実施するには，まず，各職場における情報管理レベルの向上が必要であり，「共有パソコン」の確実な運用が求められる。次に，メールサーバーを含め各ウィルスウォールのワクチンが，常に最新のパターンファイルに更新されていることが必須であり，これらを担保するためにはシステム監査の実施が重要である。

５．４　ウィルスウォールの限界とその対策

マトリックスウィルスが発見からわずか２－３ヵ月間で，2000年11月と12月には最も被害届出件数の多いウィルスとなった。このようにウィルスは日々進化しており，現状分析を行うと共に，タイムリーな対策を実施することが重要である。その際，ウィルスウォールに頼りすぎず，その限界を理解してウィルス対策実施することが重要である。以下に注意点を述べる。

① 社外とのメール送受信ではウィルスウォールでチェックを行うことができるが，社内間のメールについては別途メールサーバー毎にウィルスチェックを行うことが必要である。

② Ｃドライブを共有しているパソコンに感染を広げるＱＡＺウィルスに見られるよう

[34] キーパーソンのパソコンを「共有パソコン」に指定することも可能である。

に，メール以外の手段で感染を広げるウィルスに対しては，ゲートウェイを通過しない為，ウィルスウォールは役に立たない。個別のパソコンにワクチンプログラムをインストールすることが必要である。

③ 暗号化したデータの中にウィルスが入っている場合はチェックできない。これは逆に言えば，ウィルスを暗号化すれば発見されないということである。ＬＨＡやＬＨｍｅｌｔなど一般に公開されている方法でファイル圧縮を行ったものをメールに添付した場合はその内容を容易に解読できる。しかし，Hybrisウィルス[35]に見られるように，ウィルスが自分自身を暗号化してメールを送付すればウィルスウォールはチェックできない。これを発見・阻止できるのは，復号した後にそのパソコンでウィルをチェックする方法である。

ウィルスウォールは，確かに非常に有効な手段ではあるが，以上述べてきたように，ウィルスウォールだけでは不十分であることを充分に認識して利用すべきである。即ち，各パソコン毎にワクチンを配布することにより，ウィルスウォールで補足できないウィルスに対しても有効であるということを認識することが重要である。これ以外の対策としては，パソコンをシンクイアントに変更することも有効である。シンクライアントは，外部記憶装置をもたないため，ウィルスの感染被害は格段に低下する。しかし，サーバーに対して最新のウィルス対策を実施することを忘れてはならない。

筆者は以前より，メール機能を利用した強力な感染力を持ち，発病時の被害が深刻なウィルスの出現を懸念していた者の一人である。ネットワークの健全性を確保することは，企業としての問題であるばかりでなく，インターネットが社会のインフラとして定着しつつある現在では，国家として対策を検討するとともに早急に対策を実施すべきである。その際，伝染病など病原体のウィルスを駆除するために取られた公衆衛生的な視点での国家的対策を，コンピュータウィルス対策についても取ることが可能であると考えている。すなわち，ネットワークについても公衆衛生的な視点での対策実施が必要であると考えている。

具体的対策提言については，『第６章 情報資産保護のための政策提言』『３．１ ネットワークの公衆衛生としてのセキュリティ減税』で詳しく述べる。

---

[35] 2000年9月に発見された。http://www.zdnet.co.jp/news/0011/16/e_hybris.html 参照。

５．５　ウィルス対策についての，新たなシステム監査のあり方

本稿はグローバル・ネットワークを有する企業におけるウィルス対策とシステム監査について，分析を加え具体例を含めた提言を行った。ネットワークがグローバル化することによって，従来以上のスピードでウィルスも変化し進化している。

ウィルス対策についてのシステム監査は，それだけで独立して監査しなくとも組織の実状に応じて，他のシステム監査の際に追加的に実施することも可能である。

システム監査の立場は，「システム監査基準書（平成８年１月 30 日改訂）[6)]」では，「監査対象から独立かつ客観的な立場で，情報システムを総合的に点検及び評価し，組織体の長に助言及び勧告するとともにフォローアップする」とされている。しかし，近年の情報システムが企業や組織の業務について，多くの執行機能を代替するようになり，これまでのような「客観的な立場で点検及び評価する」といった立場を踏襲するだけでは，有効なシステム監査の実施は困難になってきている。昨年，内部監査協会（ＩＩＡ）で発表された新しい内部監査の定義は，これまでの「組織内の独立した評価機能」から「独立かつ客観的な保証とコンサルティング」へと変わってきている[7)]。このことからも，システム監査も同様，情報システムの脆弱性を指摘し，そのコントロールとリスクの管理に対して，保証とコンサルティング機能を果たすべきである。ただ，この場合の保証は，情報システムのセキュリティ対策に対する実効性を担保することであろう。

これからのシステム監査は，松田 貴典[8)]が指摘するように，「情報システムを構築すれば，その情報システムの効用に反して脆弱性が内在する。脆弱性は情報技術の進展とともに変化し複雑化する。情報システムが高度化した近年のシステム監査は，システム監査人自らが技術的な指導を行う参画型システム監査が必要となる」といえよう。まさしく，ウィルス対策については，技術的なウィルス対策と，システム監査によるコンサルティングが相互に補完的に機能を果たしてこそ，効果的なウィルス対策が実現できるのである。

参 考 文 献

１）通商産業省機械情報産業局 『コンピュータウィルス対策基準解説書・改訂』 (1995)

２）高瀬 宜士「グローバルネットワーク時代のウィルス対策とシステム監査」『システム監査』Vol. 13, No. 2 , p. 13 (2000)

３）渡部 章 著 『コンピュータウィルス辞典』オーム社, p. 13 (1993)

４）喜入 博「コンピュータウィルス対策事例」『システム監査』Vol. 12, No.2 ,pp. 29-37 (1999)

５）高瀬 宜士，真田 英彦「セキュリティポリシー」『日本社会情報学会第13回全国大会予稿集』Vol. 13, No. 1 ,pp. 269-274 (1998)

６）通商産業省機械情報産業局 『システム監査基準解説書・改訂』 p. 1 (1996)

７）鈴木 英次 訳 「われわれはどこへいくのかー内部監査人協会が内部監査の本質を再定義する」『月刊監査研究』 No. 299, pp. 110-121（1999）

８）松田 貴典 著 『情報システムの脆弱性』白桃書房 p. 2, pp. 242-245 (1999)

参考ＵＲＬ

http://www.ipa.go.jp/index-j.html　IPA

http://www.cert.org/　CERT

http://www.jpcert.or.jp/　JPCERT／CC

http://ciac.llnl.gov/　CIAC

http://www.ipsj.or.jp/　IPSJ

http://www.isaca-osaka.org/　ISACA Osaka

http://www.ncsa.com/　NCSA

http://www.drsolomon.com/　Dr Solomon's

http://www.datafellows.com/vir-info/index.htm#search　Data Fellows

http://www.trendmicro.co.jp　Trendmicro

http://www.nai.com/japan/　Network Associate

http://www.symantec.com/avcenter/　Symantec Anti Virus

http://www.asia.microsoft.com/japan/　Microsoft Japan

第３章　コンピュータ不正アクセスの現状とその対策

警察庁，郵政省（現在の郵政事業庁），通商産業省（現在の経済産業省）が共同で提案した「不正アクセス行為の禁止等に関する法律」が1999年8月に成立し，2000年2月13日から施行された。コンピュータへの不正アクセス（以下，不正アクセス）については，欧米では既に法的に処罰する国が多いが，日本においては，今までは不正アクセスが犯罪とはならず，このままでは，世界中から日本を拠点として第３国に不正アクセスする懸念が持たれていた。しかし，施行直前の2000年1月，我が国の中央省庁で管理している複数のホームページが何者かによって書き換えられたことが大きく報道された。このことにより，わが国のネットワーク対策について，整備の低さが指摘されている。ネットワークを経由したシステムへの不正アクセスやデータの破壊・改ざんなどは，インターネットの進展に伴い今後ますます増加することが懸念される。企業や社会がネットワークへの依存度を強めるにしたがって，不正アクセス対策の重要性も増している。

本稿では，第１節で不正アクセスの現状について把握し，第２節で不正アクセスの侵入方法について分析を行い，第３節でグローバル企業における不正アクセスのモデル分析を行い，第４節で不正アクセス対策ついて考察する。

なお，本稿ではコンピュータへの不正アクセスを行う者に対して「ハッカー」という呼称を使用する。ハッカーとは，本来はコンピュータの持つあらゆる可能性への自由闊達な知的探求を意味している。不正アクセスを行う者に対して，本来の意味からかけ離れてしまわないように，オープンソースコミュニティーなどの団体がクラッカーやワーマーなどの呼称を考え出したが，現実には侵入者達自身が，自分たちの呼称に「ハッカー」を使っており，クラッカーやワーマーは実際にはほとんど使われていないのが実状だからである。

１．不正アクセスの現状

１．１　コンピュータ不正アクセス対策基準と不正アクセス禁止法

コンピュータへの不正アクセス対策の普及，促進を図るため「コンピュータ不正アクセス対策基準」が発表され1996年８月より施行された。これは，コンピュータへの不正アク

セスに対する予防，発見，復旧について実効性の高い対策基準として取りまとめられたものである。この基準は，ネットワークシステムの利用者，提供者者の双方を対象にして，パスワードおよびユーザーＩＤ管理，情報管理，設備管理などを実施するために対策項目を網羅したもので，「システムユーザー基準」「システム管理者基準」「ネットワークサービス事業者基準」「ハードウェア・ソフトウェア供給者基準」の４つから構成されている。

「コンピュータ不正アクセス対策基準」[1)] では，「コンピュータ不正アクセスとは，システムを利用する者が，その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと」とされている。

不正アクセス行為の禁止については，「不正アクセス行為の禁止等に関する法律」いわゆる「不正アクセス禁止法」が2000年2月13日より施行された。この法律は，不正アクセス行為の禁止・再発防止を目的としたもので，違反者には１年以下の懲役又は５０万円以下の罰金が課せられる。

しかし，日常最も多く発生している不正アクセス行為の一つである「ポートスキャン[36]」については，「不正アクセス禁止法」では違反行為であるとは断言できない。

１．２　不正アクセス届出件数

不正アクセスについては，ＪＰＣＥＲＴ／ＣＣ（Japan Computer Emergency Response Team ／ Cordination Center）に報告された件数がある。ＪＰＣＥＲＴ／ＣＣのホームページに書かれているとおり，ここにあげた件数はJPCERT/CC が受け付けた報告の件数であって，実際のアタックの発生件数や被害件数を類推できるような数値ではないし，類型ごとの実際の発生比率を示すものでもないが，現在，日本で最も利用されている数値であることは言える。

ＪＰＣＥＲＴ／ＣＣに報告された件数によると，図３．１のとおり，2000年４月－６月

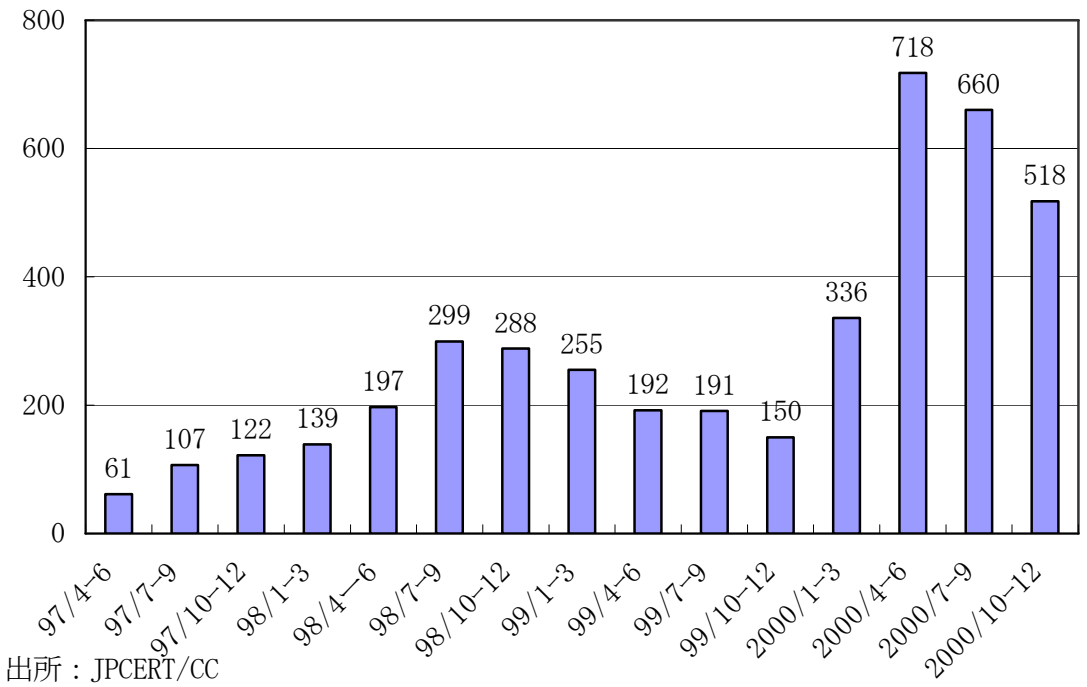
---

[36] スキャニングツールを利用してセキュリティホール（セキュリティ上の弱点）を自動検索すること。良く利用されるユーザーＩＤやパスワードを送り込む方法を始めとして，様々な手段で侵入する方法を探すこと。家の玄関や窓など，出入り口に鍵が掛かっているかどうかを確認するような行為。

の件数（３ヶ月件数）が718件と，急増している[37]。1998年から1999年にかけては徐々に減少していたものが，2000年第１・四半期（１－３月）には倍増の336件となり，第２・四半期（４-６月）には急増していることが分かる。

その原因は，従来はハッキングツールが英語など１バイト言語圏用に作成されていたものだけであったが，日本語や中国語など２バイトの言語圏に対応したハッキングツールが完成し，それがインターネットを通じて広がっていることが影響していると推測される。[38] 2000年の第３四半期，第４四半期は徐々に低下傾向となっているが，前年と比較すると高い値であることに変わりはない。今後の被害拡大が懸念される。

図３．１　届出件数



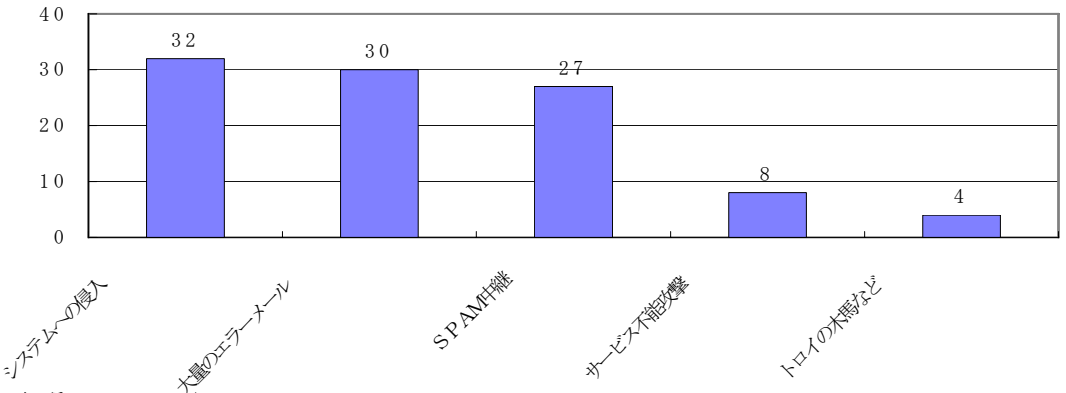
出所：JPCERT/CC

[37] http://www.jpcert.or.jp/

[38] あるハッカーの話「自分は英語だけでなく，２バイトコードのホームページでも問題はない。」これは日本語で書かれたホームページもハッキングが容易になったことを意味する。 Gartner Group Infomation Security Conference P.6　2000.6.25

筆者は被害内容について，比較的実害の少ない「ポートスキャン」と「ポートスキャン以外」とに分類した。その結果，2000年４－６月については，合計件数は７１８件で，その内「ポートスキャン」（６１７件，８６％）が大半であるが，「ポートスキャン以外」が１０１件で１４％を占めている。深刻な被害をもたらすことが多い「ポートスキャン以外」の被害について詳細を図３．２に示す。

図３．２　ポートスキャン以外の被害内容



出所：JPCERT/CC

最も件数が多いのは「システムへの侵入」であるが，この件数は被害者が気付いた件数だけであり，実際には侵入者が警告メッセージを残すなど，わざと侵入の痕跡を残していたことにより初めて気付いた場合なども含まれており，発見されていない（気付いていない）不正侵入の件数はもっと多いと推定される。

「大量のエラーメール」は実際に大量のエラーメールを送付され，被害に遭遇した件数であり，サービス継続が出来なくなったケースも考えられる。

「ＳＰＡＭ中継」はハッカーが大量のメールやデータを自社サーバーを中継して発信し，被害を受けた組織から連絡を受けて初めて気付くケースが少なくない。ハッカーの踏み台にされたケースである。

サービス不能攻撃は「DOS攻撃[39]」とも呼ばれているもので，大容量のデータやメールを送付してサーバーを能力オーバーにしてしまい，結果的にサービス提供が継続出来なくしたり，特殊なデータなどを送付してサーバーを停止させたりすることである。

---

[39] Denial of Service の略

最近ではその攻撃も1個所からだけでなく複数のサイトから同時に攻撃を仕掛ける方法が出てきており，如何に大きな処理能力を持つマシンでも，これには対抗できない[40]。

以上はいずれも深刻な被害をもたらしている。しかし，実際の被害に遭遇するまでは，多くの経営者はその問題の深刻さに気付いていない場合が多い。

「トロイの木馬」というのは，ハッカーが不正侵入を図るために仕掛けたワナの一種で，ユーザーがインターネットからサーバーやクライアントにダウンロードしたプログラムなどに仕掛けられており，勘違いをさせてパスワードを入力させたり，知らないあいだにパスワードの自動送信などを行う。

2000年10月２７日，マイクロソフト社は，本社にハッカーが侵入し，ＦＢＩが捜査を始めたことが発表された。このハッカーの手口も「トロイの木馬」型ウィルスを社内に侵入させて行ったことが判明している。この「トロイの木馬」型ウィルスはW32.HLLW.QAZ.A（略称：QAZ.Trojian）と呼ばれているものである。

一般的に，ハッカーはサーバー管理者が知らない間にネットワークを経由して密かに侵入を図り，一旦侵入できると次はサーバー管理者になりすましたり，他のサーバーの出入り口を探して入り込み，目的を果たすまで静かに潜んでいるケースが考えられる。そして，例えばホームページ改ざんや消去など，目的行動をそのサーバーを経由して実行する。サーバー管理者は，その不正行為が実行され，被害者からの連絡で初めて自社のサーバーがシステムへの不正侵入を受けていたことを知るケースも少なくない。

被害者は侵入されたマシンのＩＰアドレスなどを見て，加害者が何処か（誰か）の判断を行う。しかし，実際は，侵入を図ったサーバーはハッカーに不正侵入されている場合が多く，真の加害者はネットワークを使ってそのような行為を行った者である。

ハッカーは最初に乗っ取ったサーバーを経由して次のサーバーを乗っ取る。その次のサーバーを経由してまた次のサーバーを乗っ取る。この過程が次々と繰り返されてゆくと，犯人の追跡はリアルタイムの追跡を除き，きわめて困難なものとなる。しかも，そのサーバーが海外に設置している場合は，言語や時間帯の関係もあり，なおさら困難を極めることとなる。ハッカーを逮捕することの難しさはここにある。

40　ＤDoS攻撃（Destributed Denial of Service Attacks）と呼ばれいる。ＡＯＬ(アメリカンオンライン)等がこの攻撃を受けて一時サービス不能に陥ったことがある。

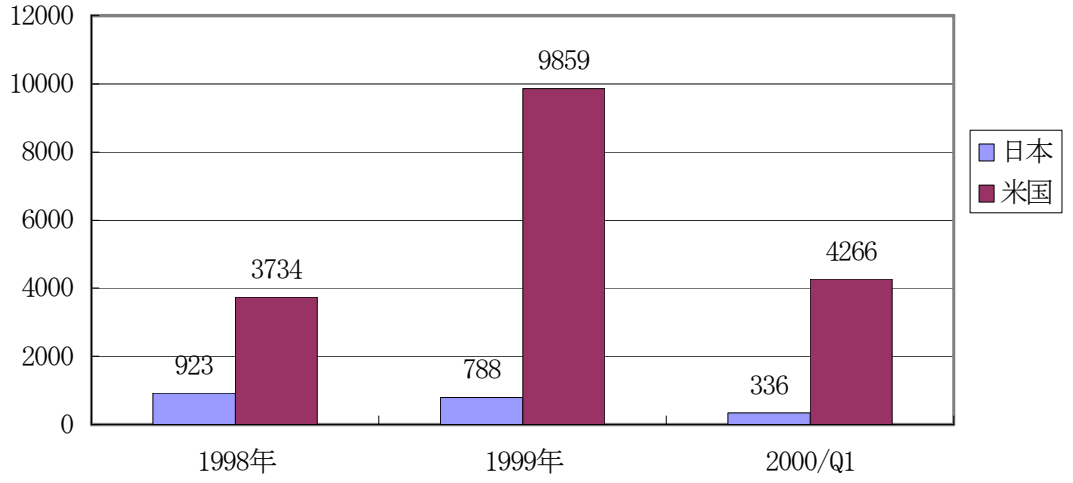
１．３　日米における不正アクセスの比較

次に，日本と米国とを比較した不正アクセス件数は図３．３のとおりである。[41]

米国では1998年の3,734件から1999年には9,858件と急増しており，その傾向は2000年の第１・四半期だけでも1999年の約半数の4,266件もあり今後も増加することと推測される。

一方，日本では1998年から1999年にかけては僅かではあるが減少しており，2000年の第１・四半期には倍増し，前述のように2000年第２・四半期には急増している。日本語対応のハッキングツールの開発が完了したことを考慮すると，今後，日本においても被害が，急増することが懸念される。

図３．３ 日米における不正アクセス件数



出所：CERTおよびJPCERT/CCのデータより筆者が作成

米国・国防省の調査によると，政府自身が自分達のシステムに対して行った20,000回以上の侵入テストの結果は以下のとおりであった。[42]

① ８８％が成功

② 成功したうちの５％のみが検知された

③ その検知されたうちの５％のみがレポートされた

---

41 ＣＥＲＴ（Comuputer Emergency Response Team） http://www.cert.org/

42 ネットワークセキュリティ・セミナー資料 P.20 2000.3.14 アシスト

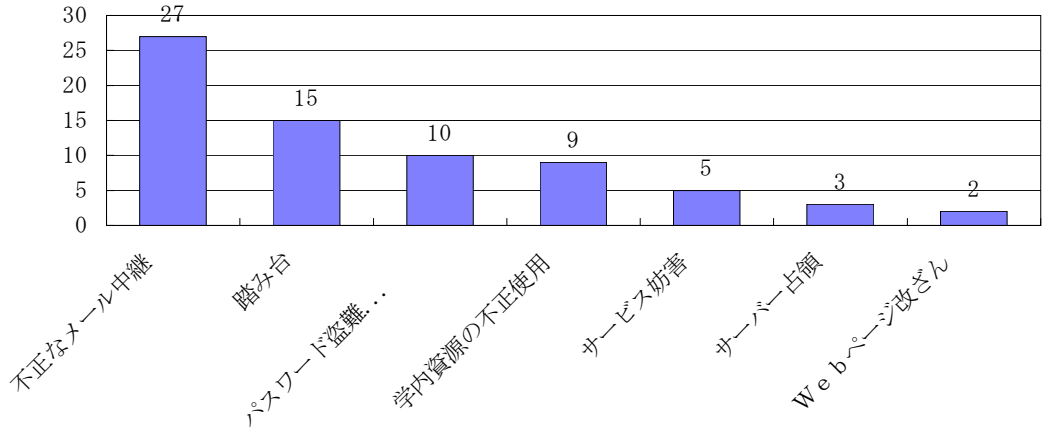
④　すなわち，１件のアタックが報告されると，その裏に　４００件が成功裡に行われていることになる。

１．４　大学における不正侵入被害

2000年９月に私立大学情報教育協会から「大学におけるネットワーク不正侵入の実状と対策」が発表された。それによると，回答をした２４５校中，７１校（２９％）が「不正侵入有り」と回答している。

具体的な被害件数の内訳をグラフに示すと，図３．４のとおりである。[43]

図３．４　大学における不正侵入



出所：私立大学情報教育協会のデータを元に作成

２４５校中７１校（２９％）が「不正侵入有り」と回答しているが，残念ながら，このアンケートには「ポートスキャン」が含まれていないので，大学に対してどの程度のポートスキャンアタックが行われているかは不明である。実際には日常的に行われていると考えるのが普通であり，あまりに頻繁に行われているのでアンケートの必要が無いとの状況判断であるなら良いのだが，実状はかなり危険な状態の大学もあろうと推測される。

大学側がファイアーウォールおよびスキャニング発見ツールで確実にセキュリティ対策を実施していれば，「ポートスキャン」の件数も把握でき，不正侵入されることは少ない

[43]　平成12度 第14回 私立大学情報教育協会大会資料 p. 1 2000.9.19-21

と思われるが，実際問題としては，ツールの導入もしていなくて，組織的対応を含めて，担当者も配置していない場合などは，現実に被害に遭ってから報告されることが多いのではないかと危惧されるところである。

１．５　中央官庁被害事例

2000年１月に発生した中央官庁の被害は以下のとおりである[44]。後で述べる1月25日に高知工科大学が自治省に不正侵入したと報道された事例研究との関連を含めて，ハッカーが攻撃を仕掛けてくれば，如何に頻繁に被害が発生していたかが分かる。

１／２４　科学技術庁のホームページ（以下，ＨＰ）を書き換え

１／２５　総務庁のＨＰを書き換え・霞ヶ関ＷＡＮに不正アクセス1万回
統計局でＨＰ用サーバーのデータとプログラムを全消去
人事院のホームページに不正アクセス1万2千回

１／２６　通産省のＨＰに不正アクセスの形跡
経済企画庁所轄の「総合研究開発機構」で書き換え

１／２７　統計局のＨＰを再び書き換え
運輸省のＨＰ書き換え：ハッカーのＨＰにリンクされる
文部省・外務省・郵政省に不正アクセスの形跡

１／２８　農林水産省で不正アクセス：１４０回
日銀ポートスキャンアクセス：１６００回
大蔵省・金融監督庁・防衛庁に不正アクセスの形跡

１／２９　最高裁判所不正アクセスが３６００回

１／３０　人事院近畿事務局のＨＰデータ　９６％が消去
沖縄郵政管理事務局に書き込み

１／３１　参議院サイトに不正アクセス１８００回＆書き換え

日本政府は，「平成12年１月に発生した一連の各省庁ホームページの改ざん事件によって，中央省庁におけるこれまでの情報セキュリティに関する取り組みが，必ずしも十分で

44　アシストネットワークセキュリティ・セミナー資料 P.8　2000/3/14

ないことが明らかになった」として，情報セキュリティ対策推進会議が[45]，2000年７月に「情報セキュリティポリシーに関するガイドライン」を策定した。各省庁はこのガイドラインをふまえ，2000年12月までに情報セキュリティポリシーを作成し，これに基づく総合的・体系的な情報セキュリティ対策を図ることになった。そして「２００３年（平成１５年）までに電子政府の基盤としてふさわしいセキュリティ水準を達成することを目標として計画的に必要な措置を順次講ずる」としている。[46]

２．不正アクセス犯罪

２．１ 不正アクセス犯罪事例分析

次に，不正アクセスの犯人特定が如何に難しいものか，具体的事例として，人事院のホームページに不正アクセスしようとしたとして，高知工科大学の名前が報道された例を分析する。

2000年１月下旬，中央省庁のホームページに対するハッカー攻撃が相次ぐ中，１月２５日に高知工科大学のコンピューターのＩＰアドレス（コンピューターのＩＤ番号）を使い，人事院のホームページに不正アクセスしようとしたハッカーがいたことが報道された。この事件は，一連の事件との関連性も含め注目された。高知工科大学のＩＰアドレスを用いたハッカーは，どうやって不正アクセスを試みたのかについて，高知新聞は次のように報道している。[47]

『人事院のホームページにハッカーが不正アクセスを試みたのは２５日午前2時半頃で，約２分半で約12,000回のアクセスが行われたが，不正アクセス防止システムが働き，侵入に失敗した。』

ところがその際，アクセス者の履歴として，高知工科大学の情報システム工学科内のサ

---

[45] 官民における情報セキュリティ対策の推進を図るため，高度情報通信社会推進本部に設置された全省庁を構成員とする会議。議長は内閣官房副長官

[46] Contorl Community Vol.4 P.33-64 2000 情報システムコントロール協会(ISACA)

[47] http://www.kochinews.co.jp/huseiac1.htm

ーバーのＩＰアドレスが残されていたことから，今回の騒ぎとなった。

上記記事によると『これまでの高知工科大学の調べでは，問題のコンピューターは事件当時，電源を切っており，部屋の施錠もされていた。情報図書館長の寺田浩詔教授は「実物は使われておらず，ＩＰアドレスだけが何者かに悪用された疑いが強い」とみている。』

一般的に，ハッカーは特殊なソフトウエア（ハッキングツール）を使って，目的のサーバーをポートスキャンし，侵入経路を探す。今回の人事院への不正アクセスとは，このポートスキャンのことで，そのアクセスが約12,000回行われたということである。グローバル企業においては日常的・頻繁に起きていることであり，今回のポートスキャンがこれほど大きな問題として高知工科大学を名指しで報道さたことは理解に苦しむ。

高知新聞によると高知工科大学の侵入手段として次の３つが考えられるとしている。

『学内で調査を進めている情報図書館長寺田浩詔教授は「三つの手口が考えられる」と説明する。

① インターネットを通じて，外部のパソコンから何者かが情報システム工学科のネットワークに入り込み，アクセスを試みた。

② 何者かが同学科内の施設に侵入し，学内から直接アクセスを試みた。

③ 手持ちのパソコンのＩＰアドレスを，問題のコンピューターのＩＰアドレスに書き換え，外部から試みた。

①は明らかに高知工科大学のネットワークに侵入しなければならない上に，問題のコンピューターの電源が切られている以上，別の稼働しているマシンを探し出し，そのマシンのＩＰアドレスを，問題のコンピューターのＩＰアドレスに書き換えるテクニックが必要である。しかも，大学側のこれまでの調査では，ネットワークに侵入された痕跡はない。

②については，事件が発生した２５日午前２時半ごろ，同学科の施設を利用して直接，不正アクセスに臨んだパターンである。この時間帯に施設内にどれだけの人がいたか，現在，大学側が調べているが，厳密には把握できそうにない。なぜなら，高知工科大学の建物は夜間は施錠されているが，昼間は部外者も自由に出入りできるので，昼間施設に入った人物が夜になるのを待ってコンピューターを悪用した可能性も否定できないからである。

③については，自分の持っているパソコンのＩＰアドレスを書き換えてアクセスを試みる手段なので，これは問題のコンピューターのＩＰアドレスさえ知っていれば，どこからでも実行できる。ＩＰアドレス自体は，インターネットを通じて比較的簡単に知ることができる。ただし，これだけでは相手側からの反応は全く把握できない。なぜなら反応はす

べて高知工科大学のコンピューターに届くからである。

いずれにせよ, 今回の人事院の事件はアクセスに失敗しているだけに, その目的は不明。また，他の省庁へのハッカー侵入事件との関連がはっきりしない以上，人物を特定することも難しい状況にある。』としている。

インターネットの世界では，こうした不正アクセスは頻繁に発生しており，しかもその行為自体は，単にサーバーへの入り口のドアを探しているだけにすぎず，犯罪性を指摘しにくい面もある。一般的にインターネットとの出入り口にはファイアーウオールが設置されており，特定の相手以外は入れないようになっている。今回，人事院もファイアーウォールで侵入を阻止した。このようにポートスキャンそのものは適切な不正アクセス対策を実施していれば阻止できるということが重要である。

ハッカーがパスワードを解読できたらサーバーの中に侵入し，データの取消し，改ざんなど様々な操作が可能となり，科学技術庁や総務庁のホームページのように，内容を書き換えることもできる。しかし，そこまでいかない行為，即ち，他人の家に鍵がかかっているかどうかをチェックする程度の行為であるポートスキャンは，ネットワーク社会では日常茶飯事に起きているだけに，今回，高知工科大学の名前が報道されたことは報道のあり方にも問題があるといえる。

最後に『高知工科大学は現在，学内関係者の関与を否定するため綿密な調査を進めているが，幹部らは「単に外部の者にＩＰアドレスを悪用されたと考えているが，それにしても，なぜうちが使われたのか…。全く分からない」と悩んでいる。』という。

前述したようにネットワーク犯罪は犯人の特定が特に難しく，もしこれが大学でなく，一般企業の名前がこういった形で公表されたなら，ブランドイメージを大きく傷つけることにつながりかねない。一度，報道されてしまうと，その企業が直接ハッキングをしているとは思われなくても，設定ミスなど何らかのミスや管理の不徹底があったのではと，一般的には思われてしまう場合が多い。今回の高知工科大学の場合も，自らが犯行を行っていないであろうということは推測されても，イメージダウンは否めない。しかし，高知工科大学は何らの過失も無く，単にそのＩＰアドレスを使われただけである可能性も否定できない。ＩＰアドレスだけで相手を特定してしまい，その名前を発表し，報道側としてもその名前を公表してしまったことの重大性を考慮すると，ネットワーク犯罪における報道の難しさを，今回の問題は提起している。

攻撃をしていると思われるサイトも実は被害を受けているサイトであり，もしかすれば

そのサイト（ＩＰアドレス）さえも確かなものでは無い，ということを今回の件は教えている。それほど不正アクセスの犯人を特定することは難しいということを肝に銘ずるべきであり，安易に組織名の公表などの報道があってはならない。日本においては社会全体として不正アクセスに対する理解が不十分であり，今後様々な事件や経験を踏まえて少しずつ進歩・成長してゆくものかも知れないが，理解不足に対する警鐘を鳴らすことを止めてはならない。

２．２　従来の犯罪とネットワーク犯罪との相違

以上見てきたように，ネットワーク犯罪には様々な特徴があり，その対策実施には犯罪の特徴を把握しておく必要がある。ネットワーク犯罪の特徴としては以下の項目が掲げられる。

１．グローバル性（国際性：無国籍性）：インターネットを利用すれば世界中のあらゆる場所からアクセス（犯行）が可能である。複数の国を経由しての犯行も起きている。

２．被害の甚大性：一瞬にして企業の信用を失墜させたり，ネットワークを麻痺させたり，社会に対して甚大な影響を及ぼす恐れがある。

３．匿名性：誰が犯罪行為を行っているのか分かりにくい。

なりすましによる侵入や，踏み台を利用しての犯罪など，複数のサーバーを経由して行われる犯行が多く，犯人の特定が非常に難しい。

４．証拠保全の困難性：瞬時にアクセスログなどの証拠を消去される可能性があり，証拠の保存が非常に難しい。

５．低リスク性：証拠となるアクセスログを消去してしまえば，犯罪を行っても発見されない可能性が高い。

６．容易性：セキュリティに関する一定レベルの専門知識があれば，ハッキングツールがインターネットで公開されているので比較的容易に犯行を行える。

７．自己アピール性（愉快犯的）：自分が行ったことで世間を驚かせたいという欲望及び自分の知識の高さを見せ付けたいという欲望。個人やグループが政府や大企業に対して挑戦できる。

８．犯罪認識の希薄性：実際に人を傷つけるのとは異なり，ネットワークを経由しての犯罪は，犯罪としての自覚が希薄となりやすい。

９．国際協力体制の未整備：国によって法律が異なる上に，国際的な協力体制が未整備なので，犯人逮捕が難しい。

10．犯罪の不明確性：犯罪と断定できるかどうか，微妙なものが増加している。例えば，会社が所有している磁気媒体などを盗めば窃盗罪が成立するが，アクセス権限を有する社員がネットワークを経由して，自らが所有している磁気媒体に顧客情報などをコピーしても，コピー行為そのものは犯罪とはならない。企業では従業員職務規定などにより情報漏洩を防止するよう努めている。

以上，ネットワーク犯罪は従来の犯罪とは異なり，その対策についても従来とは異なる対応が求められている。

２．３ 不正アクセスの侵入方法とその対策

不正アクセスの手段をあらかじめ知っておくことは重要である。この分野では技術の進歩が激しく，次々と新たな方法が発見されているが，基本的な侵入手段を理解して対策を立てることが重要である。

（１）ポートスキャン

ポートスキャンは，多くのホストのネットワークサービスポートに順次アクセスして，各ポートに対応するサービスに存在するセキュリティホールを探し出す攻撃手法で，最も多く利用されている不正アクセス手段である。ハッカーはポートスキャンなどによってシステムへの侵入を図り，次に述べる，さまざまな攻撃を実行することが可能となる。

ポートスキャンは，具体的には，自動化ツールによって実行され，TELNET，POP，HTTP，DNS など[48] のサービスへのアタックを繰り返し行う行為で，攻撃対象に指定されたドメインについてドメインネームサーバーに登録されているホスト一覧を入手し，それらホストをスキャンする手段が組み込まれているため，任意のドメインに属する全サイトやホストへの攻撃が網羅的に行われることが特徴である。

「ポートスキャンが行われた」というログは残るが，必ずしも不正侵入を受けたという

---

[48] メール送受信やファイル転送などサーバーが提供するさまざまなサービス名称

ことではない。しかし，ポートスキャンが行われると，各サイトで運用中のネットワークサービスに存在するセキュリティホールをハッカーが把握し，それに続いてさまざまな不正アクセスが行われる。例えば，パスワードファイル等，セキュリティ上重要なファイルや情報を持ち出されたり，管理者権限を不正に利用してWebページの改ざんも容易となる。さらに，侵入されたまま放置しておくと，踏み台となって，他のサイトへのサービス不能攻撃の実行など，他のサイトに大きな迷惑を与える可能性が出てくる。

この不正アクセスを未然に防止するためには次の対策が有効である。

1．不正アクセス監視用ソフトウェアをインストールして，ログにより不正アクセスの事実を確認する。

2．デフォルトでシステムに存在するアカウントの確認を行い，不要なアカウントは削除する。

3．不要なネットワークサービスが出来るようになっていないか確認し，不要なサービスがあれば停止する。

4．サーバープログラムをバージョンアップしてセキュリティホールをふさぐ。

（２）Ｗｅｂページの改ざん

2000年１月に中央省庁で多発したWebページの改ざんは，以下の方法で行われる。

① Web サーバのホストに不正侵入され，ページが改ざんされる

② FTP[49] や，CGI[50] などのネットワークサービスが不正利用され，ファイルが置き換えられる

このような不正侵入や不正利用が可能となる要因として，以下のことが考えられる。

① Web サーバのソフトウェアのバグ，設定の間違い

② CGI プログラムのバグ，設定の間違い

③ その他のネットワークアプリケーションのバグ，設定の間違い

Webページの改ざん対策として行うべき項目は，以下のとおりである。

Web サーバソフトウェアは，機能が豊富で拡張性が高い。しかし，セキュリティの観点

---

[49] File Transfer Protocol の略

[50] Common Gateway Interface の略

から，できるだけ限られた機能だけを利用することが望ましい。

① ログ機能を設定し，監視できるようにする

② 不要なネットワークサービスを停止する

③ Webサーバのソフトウェアの設定を再確認し，必要最小限の設定とする。

④ CGIプログラムを確認し，不必要な CGI プログラムを削除する。

⑤ Web サーバで利用するソフトウェア(OS, ネットワークアプリケーション)を確認し，最新のバージョンとする

Webページの改ざん被害を受けた場合の緊急対策は，以下のとおりである。

① 外部からは HTTP 以外のサービスに対するアクセスを禁止する

② Web サーバのソフトウェアを最新バージョンにする。

③ ＣＧＩを使っている場合，必要なければ，CGIの機能の停止を含めて検討する。

（３）サービス不能攻撃

DOS（Denial of Service）攻撃とも呼ばれ，システムに本来期待されているサービスが損なわれる攻撃のことを言う。

具体的な手口としては以下の方法などが考えられる。

① リモートから，処理能力を越えるパケット（リクエスト）を大量に送信し，サービスの運用を妨げる。

② リモートから，システムの弱点を攻撃するための特殊なコードを持ったパケットを送信され，サービスの運用が妨げる。

③ システムに侵入し，他のサイトに対してサービス運用妨害を行なうプログラムを実行する。

④ システムに侵入を受け，そのシステムのサービスを妨げるプログラムを実行する。

これらに対抗するには，次の方法が考えられる。

① ソフトウェアを最新のものに更新する。パッチをあてたり，リリースやバージョンを上げることでセキュリティホールをなくす。

② パケットフィルタリングによる対策，即ち，外部からサイト内部へのパケットをフィルタリングし，他の潜在的な攻撃を回避することや，内部から外界へのパケットをフィルタリングし，攻撃の中継地点としての悪用をより困難にしておく。

③ ステム構成全体を見直し，サービス不能攻撃を受けた際の影響を最小の範囲に留めるように設計し直す。

留意点としては，外界からのパケットが原因でサービス不能攻撃を受けた場合，始点アドレスが偽造されている可能性もある。また，アクセスの繰り返しは，サービス不能攻撃を意図しなくとも，アクセス元システムの設定ミス，操作ミス等々により発生する可能性もあるため，特別の配慮が必要である。

（４）新しいハッキング手段

最近使われ始めたハッキング手段としては，ウィルスを利用してパスワードを自動送信したり，バックドアを開ける方法がある。2000年10月にマイクロソフト社・本社に不正侵入したハッカーもこの手口を利用していた。[51]その他には，ポルノサイトを見ている間にパスワードを盗むなどの方法も発見されている。

なお，ＩＰＡから「セキュリティ対策セルフチャックシート」が発表されており，これらの情報も参考となる。[52]

３．グローバル企業における不正アクセス対策モデル

３．１　当該企業のネットワーク概念図

次に，グローバル企業におけるネットワーク構成についてＡ社を事例に考察する。

Ａ社におけるネットワーク構成図（概念図）は次ページの図３．５のとおりである。

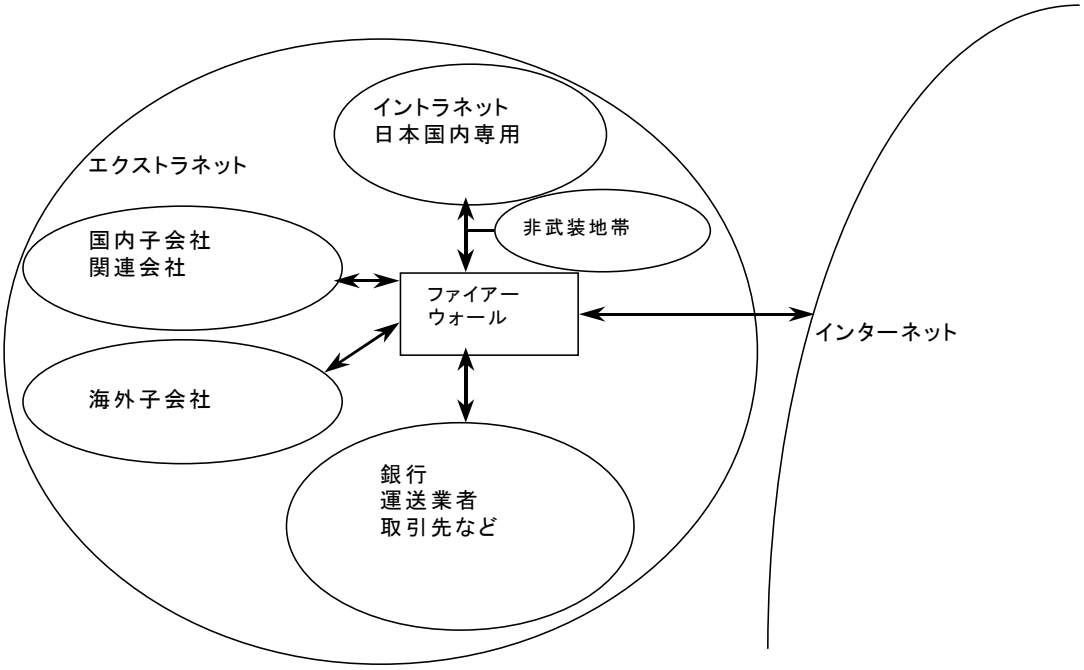
詳細なネットワーク構成図を示して説明することはセキュリティ上の観点から出来ないが，グローバル企業におけるネットワーク構成に対する基本的な考え方はこの図を元に説明することが可能である。

---

[51] 詳しくは 第２章 ２.１０「パソコンの電源を入れておくだけで感染するウィルスの出現」を参照

[52] ＵＲＬ：http://www.ipa.go.jp/security/ciadr/checksheet.html

図3．5 グローバル企業におけるネットワーク概念図



出所：A社のデータを元に筆者が独自に作成

３．２　ネットワーク構築上の留意点

インターネット網と社内との出入り口には必ずファイアーウォールを設置する。ファイアーウォールの設置に際しては，セキュリティ方針を決め，各社の環境に応じて，セキュリティ方針が満足できるレベルの商品かどうかを判断する必要がある。そして，必ずすべての設定項目について理解し，設定しておくことが必要である。社内に技術者がいない場合は，社外のコンサルタント会社に依頼することもできる。

グローバル企業では，一般的にイントラネット網とエクストラネット網とをもっている。社内と言った場合，実際の地理的な社内地域を指すこともあるが，ネットワークとしては，イントラネット網に接続されているＬＡＮ／ＷＡＮを指す場合が多い。イントラネット網の中は自由度を確保するためにセキュリティ対策のレベルは低く設定してある。それだけにハッカーが一旦ＬＡＮの中に入ると様々なことが可能となる。

イントラネット網の外側にエクストラネット網を作り，子会社や関係会社などをその中

に含める。エクストラネット網とイントラネット網との出入り口にも必ずファイアーウォールを設置すること。関係会社との接続に際しては，アクセス出来るザーバーやデータを特定するなど，きめの細かい管理が要求される。

海外拠点や海外子会社については特に注意が必要である。海外からは新型ウィルスの侵入も多く，社員の勤続年数も短いため不正アクセスの可能性が高く，また，現地でのコンピュータ技術者が実施する管理内容も不十分なことが多いので，一定レベル以上のセキュリティの確保が必要である。その意味で海外拠点は，例え組織的には社内であっても，イントラネットの中でなく，エクストラネットに含める方が安全である。

社外に公開する情報は非武装地帯と呼ばれるところに設置し，外部からのアクセスを容易にするとともに，破壊や変更されることを前提に管理体制を整備すること。特にバックアップやアクセスログについては確実に確保し，不正アクセスに備えることが重要である。また，アクセスログについては定期的に確認を行い，安全性を確認すること。

セキュリティホールについては，ソフトウェアベンダーやＪＰＣＥＲＴ／ＣＣから適宜情報を入手し，それぞれの入手情報について，自社での対応の必要性を確認し，必要に応じて対策を講じるような「業務の仕組み」を構築しておくことが重要である。これを業務の一環として実施せずに，個人のスキルだけに依存しすぎていた場合，その者が長期休暇を取ったりした場合は，当該企業は非常に危険な状態になることを肝に命じておくべきである。繰り返すが「業務の仕組み」を構築しておくことが重要である。

ハッカーとセキュリティホールは時間を待ってくれない。セキュリティ対策のモレは水漏れと一緒で，最も弱いところから発生する。ハッカーは一度侵入できると，次にはサーバー管理者になりすまし，後は思うつぼである。被害が起きてからでは遅すぎる。日頃からのたえまない準備が求められる。

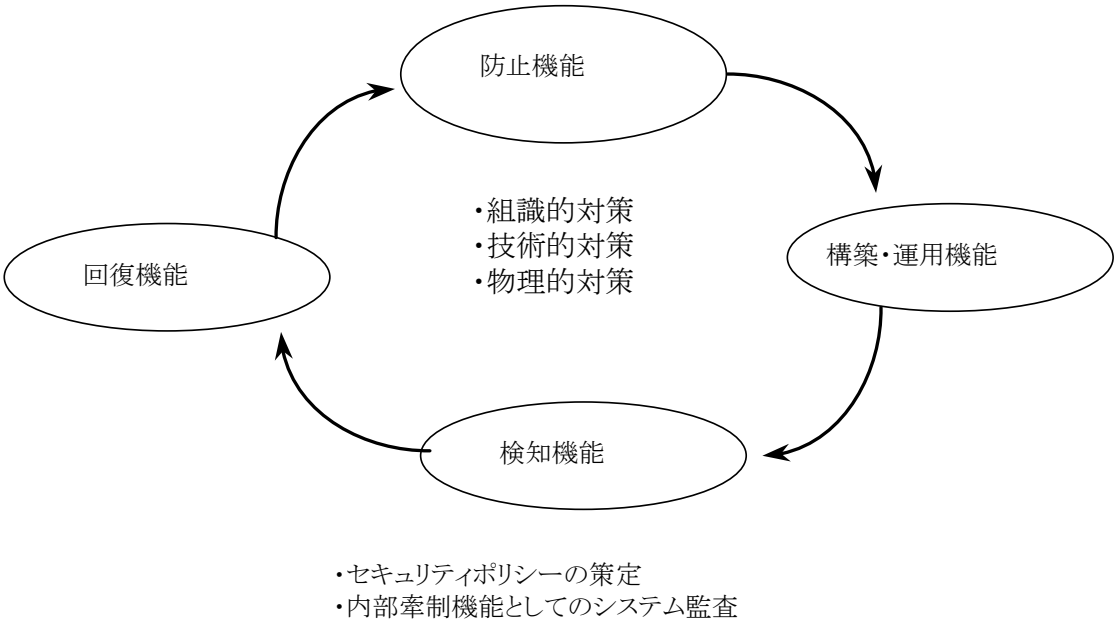
４．不正アクセス対策の方法

不正アクセス対策については，図３．６に示したように，防止機能＝＞構築・運用機能＝＞検知機能＝＞回復機能のサイクルを考慮して対策を実施することが大切である。

組織として，不正アクセスに強いネットワークを構築し，業務を分担し，日頃からの定期的かつ状況に応じた対応が，不正アクセスを防止することが出来る唯一の手段であるこ

とを忘れずに，対応することが求められる。

図3．6 不正アクセス対策のサイクル図



次に，具体的方法として，（1）組織的対策（2）技術的対策（3）物理的対策 の３つの分野について詳細を考察する。

４．１ 組織的対策（人・組織・体制面）

不正アクセスを防止するための組織的対策（人・組織・体制面）は表３．１のとおりである。

表３．１「不正アクセスを防止するための組織的対策」

No.	項　目	説　明
1	セキュリティポリシーを策定する	グローバル企業では従業員に対して，セキュリティに対する個人の責任と，会社としての姿勢を示すことが必要であり，それらを示す

		手段として，セキュリティポリシーがある。
2	不正アクセス防止のための責任者と組織を明確化する	不正アクセス防止のためにしかるべきレベルの責任者を任命し，全社横断的組織を明確にしておく
3	連絡すべき組織，部署，連絡方法について，海外を含めた連絡体制の明確化	トラブル時の連絡体制をあらかじめ決めておく。特に海外は時差があるので，それも考慮した連絡体制が必要である
4	情報管理者に対する情報伝達の構築	日常利用している情報伝達用掲示板などを非常事態には緊急用に切り替えて用いるなど，具体的な連絡方法を構築しておく。
5	不正アクセスにより被害を受けた場合の対策立案	不正アクセスにより被害を受けた場合や踏み台となった場合を想定して，ネットワークの切り離しなど，被害のレベルや内容に応じた対策をあらかじめ決めておく
6	定期的にシステム監査を実施する	構築した仕組みが正しく機能しているか，また時間とともに陳腐化していないか，内部牽制機能を含め，第3者の立場で点検評価することが必要である。

４．２ 技術的対策（ソフト・データベース・監視ツール・運用面）

不正アクセスを防止するための技術的対策（ソフト・データベース・監視ツール・運用面）は表３．２のとおりである。

表３．２「不正アクセスを防止するための技術的対策」

No.	項　目	説　明
1	セキュリティ問題に関する情報の入手	ＪＰＣＥＲＴ／ＣＣやベンダーから随時セキュリティ問題に関する情報を入手すること
2	対策実施の必要性検討	当該情報について，対策の必要性の有無を検

		討する。対策が必要な場合は速やかに関係者に連絡する
3	ソフトウェアパッチの速やかな実施	ソフトウェアの修正（パッチ）について常に最新版を速やかに該当するマシンに適用する
4	業務日誌によるミス・モレの撲滅	セキュリティーホールの内容及び発見日（ＪＰＣＥＲＴ／ＣＣの日付）と修正日（パッチをあてた日）を不正アクセス用業務日誌に記載し，ミス・モレの撲滅を図る
5	対策手順書の作成と定期的見直し	まずは対策手順書を作成することが必要であるが，この分野は技術の進歩が早く，手順書が陳腐化するのも早いので，必ず定期的に見直しを行うこと。これを怠ると実際にトラブルが発生した場合に役立たない。
6	定期的なバックアップの確保	通常の業務で使用するサーバーはもちろんのこと，特に外部公開サーバは攻撃されることを前提として，定期的にバックアップを確保する
7	パスワードの定期的な変更管理	パスワード設定に関する変更ルールを設け，ルールとおりに変更するよう関係者に徹底させる。一定期間を経過しても変更しなければ，そのままでは利用できなくすることも含めて検討する。
8	メール中継の管理	外部アドレスから外部アドレス宛てのメール転送を適切に管理する
9	ログによる監視	ファイアーウォール及びサーバーのログを定期的にチェックし，不正アクセスの形跡がないか確認する
10	パスワードの不正更新の管理	システム管理者およびユーザーのパスワードが不正に更新されていないか確認する。

		一般的なアクセスツールで不正更新を図った場合は多数のアクセスログが残ってしまうので，これをチェックすることにより早期発見が可能となる。
11	ウィルスによる不正アクセスの排除	「トロイの木馬」によりパスワードの漏洩などを防止するため，ウィルスウォールは定期的パターンファイルを更新すると共に非常事態の場合は緊急に更新を行う。
12	ネットワーク切り離しテスト	ネットワークを切り離すに際しての手順など，技術的問題を明確にする
13	システム設定ファイルの不正な変更確認	システム設定ファイルが不正に更新されていないか確認する
14	コンテンツフィルタリング	社員のメールやインターネットでの接続先をチェックして必要な対策を講ずる
15	ネットワーク監視装置の導入	最近はステルス型ポートスキャンと呼ばれる，ＬＯＧが残らないポートスキャンが増加している。その対策として，ネットワーク監視装置を導入して，監視することが必要である。
16	管理情報のアクセス権限確認	システム管理者以外がアクセス出来ないように設定し，不信なアクセスがないか，定期的に確認する。

４．３ 物理的対策（建物・ネットワーク・ハードウェアなど）

不正アクセスを防止するための物理的対策（建物・ネットワーク・ハードウェアなど）は表３．３のとおりである。

表３．３「不正アクセスを防止するための物理的対策」

No.	項　目	説　明
1	不正アクセスに強いネットワーク構成	イントラネットとエクストタネットをゾーニングし，インターネットとはファイアーウォールを経由して接続し，外部公開サーバなどは非武装地帯に設置するなどのネットワーク構成を構築する
2	不正アクセスに強いファイアーウォールの設定	ファイアーウォールを設置し，フィルタリング設定により，未使用または不必要なポートやプロトコルを利用できなくし，不正なＩＰアドレスによる接続を排除する
3	アクセス権の設定	ファイルについては必要に応じ，格納されている場所のアクセス権を設定する
4	関連するサーバーの分離	ＦＴＰサービス，ＤＮＳサービス，メールサービスなどは，Ｗｅｂサーバーとは異なるサーバーで運用する
5	ウィルスウォールの設置	ウィルスウォール（ウィルス用ゲートウエイ）を設置して，ウィルスの侵入を防ぐと共に，社外への流出を阻止する
6	その他の留意点	実際の企業組織とネットワーク構成は同じにする必要はない，セキュリティ上の判断でネットワークを構築することが肝要である

４．４ 不正アクセス対策の視点

不正アクセス防衛の視点について，筆者が常日頃から考えていることを以下に述べる。

１．セキュリティレベルは最も弱いところで決まる。（水漏れと同じ）

２．時間と共に新たなセキュリティホールが次々と発見される。

３．ハッカーは常に新たなセキュリティーホールを探しており，対策が未実施のコンピュータを狙っている。（攻撃はプログラムの欠陥及びバックドアから行われる）

４．一旦，中に入られると非常に危険な状態になる。

５．組織的対応を図るため，最悪事態を想定したシナリオを策定しておく。

６．セキュリティ対策組織としては全社横断的組織を作り，シナリオを実施するに必要な権限を有している者を最高責任者とする。

７．ファイアーウォールは全体を把握してもれなくセットアップを行う。

８．ファイアウォールのログを詳細に確認する。

９．コンピュータウィルスを送り込む方法もある。

10. 完全なセキュリティはありあえないと心得る。

11. セキュリティにはコストがかかるのでバランスが重要。

12. 不正アクセス対策が遅滞なく実施されていることを確認するため，システム監査を実施する。

13. セキュリティについては企業トップが，自らの責任として推進を図る。

不正アクセス対策はグローバル企業としては情報資産保護のためには避けては通れない。企業のトップ自らが対策実施に積極的に取り組む姿勢を示し，組織としての対応を図り，着実な実施が望まれている。

参 考 文 献

１）通商産業省機械情報局 『コンピュータ不正アクセス対策基準解説書』（1996）

２）日本システム監査人協会編著『情報システム監査実践マニュアル』工業調査会（1998）

３）日本情報処理開発協会 『システム監査実施の手引き』日本情報処理開発協会（1989）

４）Kyas, O. *Internet Security：Risk Analysis, Strategies and Firewalls*（1997）
久保 隆之，飯倉 弘一 訳『インターネットセキュリティ』オーム社（1997）

５）Siyan, K. and H. Chris, *Internet Firewalls and Network Security*（1994）
高辻 秀興 訳『インターネットファイアーウォール』アスキー（1996）

第４章　違法コピーとライセンスマネジメント

情報社会の健全な発展のためには，著作権を含め知的財産権を保護することが必要不可欠であり，平成12年度の経済白書では「多様な付加価値を生む『知識集約型経済』への転換を提唱し，技術情報（ＩＴ）革命をそのけん引役として，知的財産の保護やインフラ整備を通じ技術革新を急ぐよう」訴えている。違法コピーは知的財産権保護のひとつの課題として，今後も重視されるべきものである。

次に，金融情報システムセンターは平成12年7月に「ＦＩＳＣ新システム監査指針」を改訂・充実させた。項目として「ソフトウェア管理」の中に「ライセンス管理」が追加され，「違法コピーなどのライセンス契約上の違法行為がないか，定期的な点検，管理が行われているか」などのチェックポイントが追加されライセンス管理を実施することを求めている。[1)]

世界に目を向けると，2000年6月27日，ＯＥＣＤ閣僚級会議においてＯＥＣＤメンバー２９カ国およびアルゼンチン，ブラジル，チリ，スロバキア共和国の政府によって「多国籍企業のためのＯＥＣＤガイドライン」が採択された。その中で「企業はビジネス活動過程において，可能ならば，知的所有権保護を当然のこととして尊重しつつ，テクノロジーおよびノウハウの移転および拡散を許すような慣行を採用する」と書かれおり，すべてのグローバル企業において，知的所有権保護を尊重することは当然のことであるとされている。

以上，国内外の状況を勘案すると，知的財産権保護はグローバル企業にとっては避けて通れない課題である。即ち，Compliance Security の一つの課題としてライセンスマネジメントをとらえるべきであり，経営課題の一つとして認識すべきである。しかし，これまでグローバル企業におけるライセンスマネジメントについて，具体的にどのような対策を立案し，実施すべきかを分析した研究は，皆無であったと言ってよい。その原因は「ライセンスマネジメントは情報システム部門に任しておけば良い」といった考え方が存在すると思われる。しかし，グローバル企業においては，多額のライセンス費用を支払い，さまざまな部門に応じて管理体制も異なり，ライセンスマネジメントを行うために多大な費用と工数が必要とされる。また，社内にも様々な部門があり管理形態も異なる。次に多くの子会社においては，情報システム部門の人員も限られており，ライセンスマネジメントが確実に実施されているとは言い難い状況である。しかしたとえ子会社であっても，ひとた

び違法コピーが発覚し，多額の損害賠償金を請求されたり，新聞への謝罪広告をしなければならない事態が発生すれば，企業グループ全体としてイメージの低下や経営への影響は避けられない。これらの事態を回避する意味で，違法コピー防止対策は情報資産保護マネジメントの1つの重要課題であると言える。

本稿はグローバル企業における違法コピー防止についての具体策を考察し，ライセンスマネジメントについてのシステム監査のあり方を分析する。

本稿では，第１節で違法コピーの現状について分析し，第2節でソフトウェアの違法コピーと防止活動についてまとめ，次に第３節でソフトウェアライセンスの形態を分類し，第４節ではＴＣＯ削減の観点からの分析を行い，第５節でライセンスマネジメントの方法について研究し，第６節でライセンスマネジメントについてのシステム監査のあり方を考察する。

１．違法コピーの現状分析

１．１　世界と日本の現状

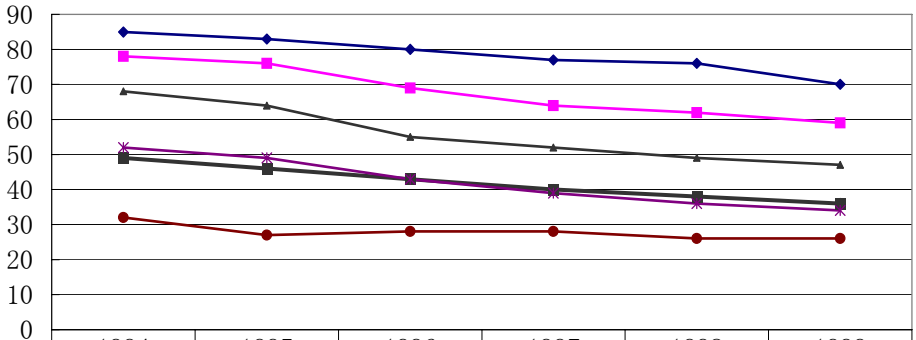
米国ビジネスソフトウェア連合[53]（Business Software Alliance ，以下 ＢＳＡ）の調査データを元に，違法コピー率推移をグラフに示した（図４．１）。それによると，世界中の違法コピー率は毎年に低下している。1999年の全世界の違法コピー率は３６％で，5年前の1994年が４９％であったことと比較すると１３％低下している。地域別に見ると，北米が２６％で最も低く，近年はほぼ横這いの状態が続いている。西欧は３４％で世界平均をやや下回っている。アジア太平洋は４７％で，東欧の５９％，ラテンアメリカの７０％に次いで高い数値である。いずれの地域においても毎年に違法コピー率は低下しており，総じて経済力の弱い地域ほど違法コピー率が高い状況である。

過去５年間の低下傾向を見ると，アジア地域が６８％から４７％に低下しており，世界中で最も顕著な低下傾向を示している。東欧圏は，８５％から７０％の低下に止まっており，世界中で最も違法コピー率が高い状態が続いている。

---

[53] マイクロソフト等が著作権保護の推進を目ざして1988年に設立した非営利団体

図4．１違法コピー率



	1994	1995	1996	1997	1998	1999
東欧	85	83	80	77	76	70
ラテンアメリカ	78	76	69	64	62	59
アジア太平洋	68	64	55	52	49	47
世界平均	49	46	43	40	38	36
西欧	52	49	43	39	36	34
北米	32	27	28	28	26	26

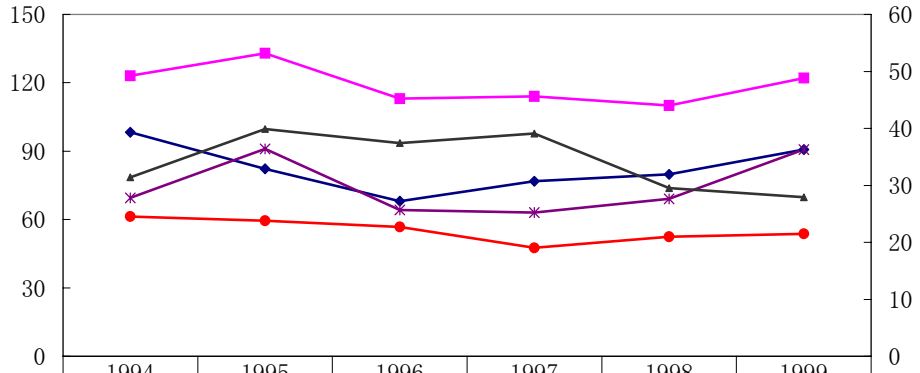
出所:BSAの資料を元に筆者が作成

次に，図４．２は違法コピーによる被害額を示したもので，1999年は122億ドルであった。過去数年間，違法コピー率は毎年低下しているが，ソフトウェア産業の広がりに伴い，1999年の被害金額は前年よりも増加している。地域別に見ると，1995年から1997年までの３年間は，アジア太平洋地域が最も大きな被害金額を出していたが，アジアで通貨危機が起きたことなどが起因し，アジアでの被害金額は低下し，1998年以降は，北米，西欧が大きくなってきている。このことは，北米，西欧地域において，ＩＴ革命の進展によりソフトウェア市場も急激に拡大していると推察される。

図４.３地域別被害比率からわかるように，1999年の地域別被害金額の割合を見ると，北米と西洋が共に３０％となっているが，アジア太平洋地域は，全世界の２３％を占めており，依然として大きな比率である。また，アジア太平洋地域は違法コピー率も世界平均と比較すると依然として高く，今後，大きな改善余地が残されている。

被害の拡大を防ぐにためには，被害金額が大きくそして今後も発展する国，地域を重点的にチェックする体制を整備することが必要である。

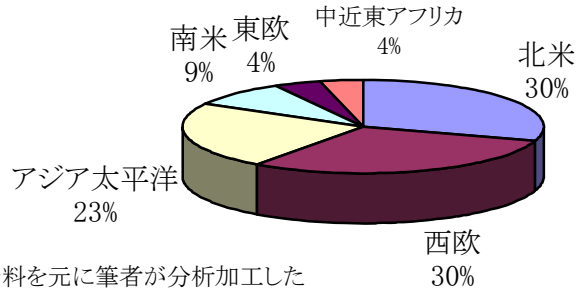
図4。2 被害額推移



	1994	1995	1996	1997	1998	1999
全世界(億ドル)	123	133	113	114	110	122
北米	39.3	32.9	27.2	30.7	31.9	36.3
西欧	27.8	36.4	25.7	25.2	27.6	36.3
アジア太平洋	31.4	39.9	37.4	39.1	29.5	27.9
その他	24.5	23.8	22.7	19.0	21.0	21.5

出所:BSAの資料を元に筆者が作成

図4．3 地域別被害比率

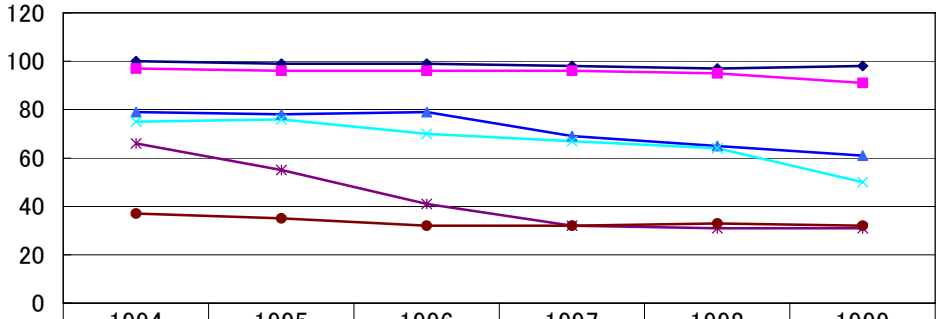


出所:BSAの資料を元に筆者が分析加工した

次に，図４．４にアジアの主な国別の違法コピー率の推移を示した。ベトナム，中国が高い比率で推移している。インドはＩＴ化の進展に伴い，違法コピー率が1994年の７９％から1999年には６１％へと減少した。韓国においても，同じく７５％から５０％へと減少した。オーストラリアにおいては，３７％から３２％に減少している。アジアの中で特筆すべきは，日本が６６％から３１％に減少したことである。

これはＢＳＡの活動が，日本では1994年に本格的に開始した事と相関があると推測される。

図4．4 アジアの違法コピー率推移



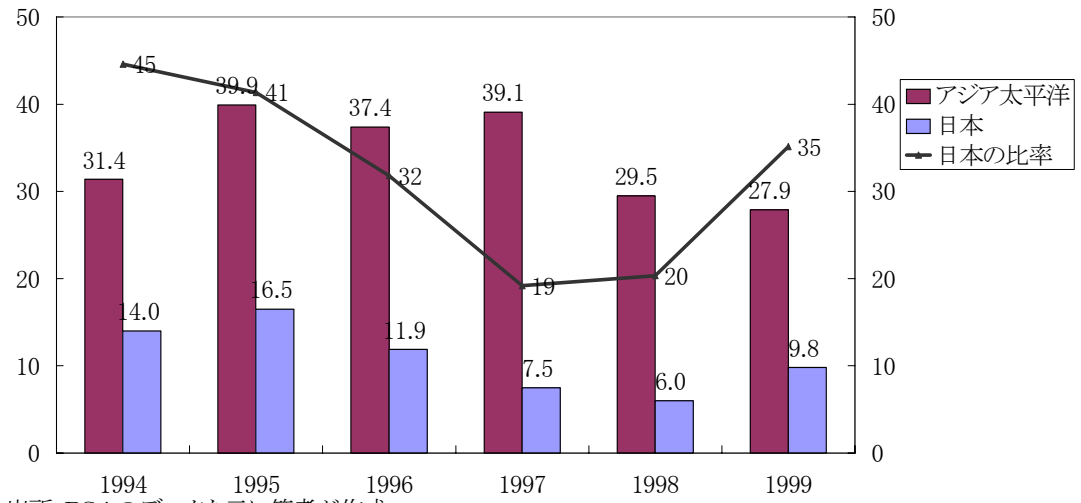
	1994	1995	1996	1997	1998	1999
ベトナム	100	99	99	98	97	98
中国	97	96	96	96	95	91
インド	79	78	79	69	65	61
韓国	75	76	70	67	64	50
日本	66	55	41	32	31	31
オーストラリア	37	35	32	32	33	32

出所：BSAの資料から筆者が作成

以上，見てきたようにアジア太平洋地域が違法コピー率が高く，なおかつ，被害金額も大きいことが分かる。ＢＳＡにとっての，アジア太平洋地域での違法コピー防止活動の重要性が理解できる。次に，アジア太平洋地域における被害金額と日本の被害金額について，図４．５に示した。アジア太平洋地域に中での日本の占める比率を分析すると，1998年には２０％であったものが，1999年には３５％に上昇しており，日本においてはＩＴ革命の進展に伴い大きな被害が発生していることが分かる。

ＢＳＡにとっては，日本で重点的に啓蒙活動を行うことが，効率的に被害拡大を防ぐための有効な手段であろう。特に，横並び意識の強い国民性は，ひとたび違法コピーを行うことは許されないことだとなれば，企業全体としてそれを着実に実施するであろう。そうするためには，情報提供者への謝礼金キャンペーンなどを含む防止活動と，報道機関への効果的な情報提供が重要であり，ＢＳＡはその方向を目指していると推察される。

図4．5 アジア太平洋地域における日本の比率



出所:BSAのデータを元に筆者が作成

１．２ 学生における違法コピー実態調査

2000年3月にコンピュータソフトウェア著作権協会（ＡＣＣＳ）より「学生における違法違法コピー実態調査」が発表された。[54]

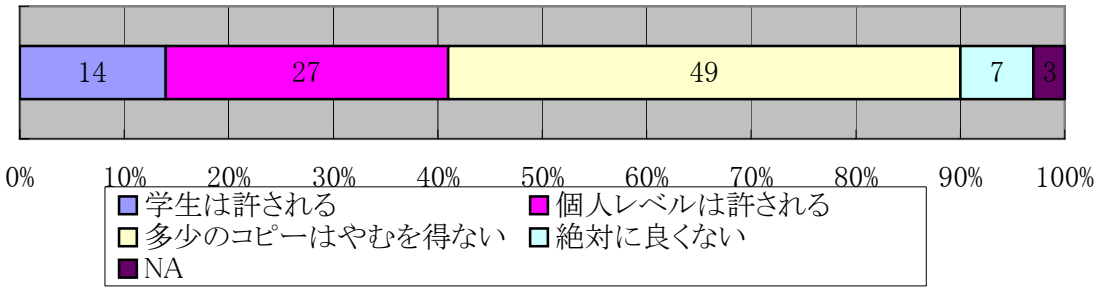
本調査研究は企業等におけるパソコンソフトウェアの管理についてその実態及び意識をアンケート調査により把握するとともに，広くソフトウェア管理の推進を図ることを目的にしたものである。ＢＳＡが調査対象としているビジネスソフトウェアとは必ずしも一致はしていないが，以下のような意識を持った学生達が企業に就職し，業務を遂行するということを理解しておくことが企業の管理者としては重要である。また，社会全体としてもこのような意識の学生が多く存在しているという事実に目を向けて，大学や専門学校における情報倫理教育の充実が望まれるところである。

（１）コピーに対する考え方については，「学生は許される」が１４％，「個人レベルは許される」が２７％，「多少のコピーはやむを得ない」が４９％となっており，合計９０％もの人が「違法コピーをしてはいけない」という認識が薄く，「コピーは

54 「学生における違法コピー実態調査」（社）コンピュータソフトウェア著作権協会2000年３月。大学生，専門学校生を対象に東京都内で実施。有効回答数：1147件

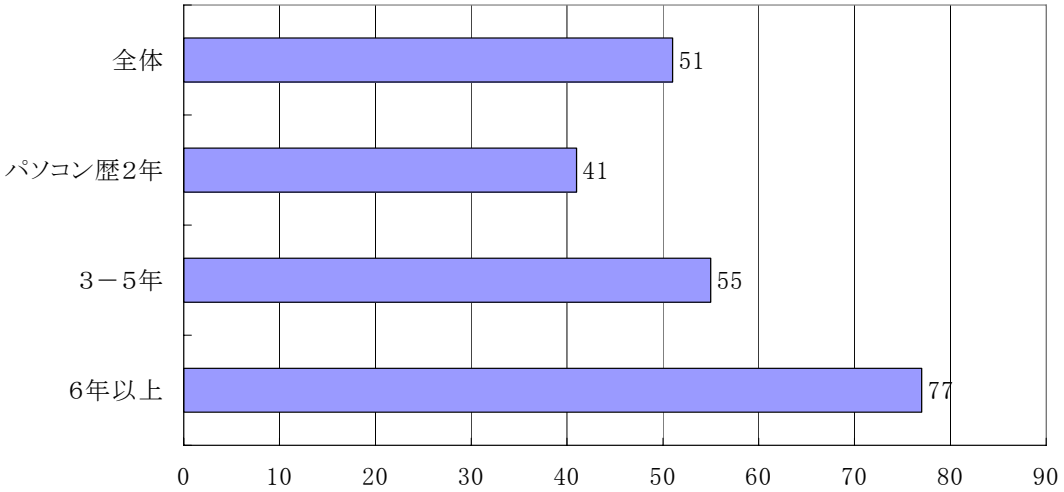
絶対に良くない」と答えた人は全体の７％にすぎない。このことからも，潜在的コピー予備軍が多数存在していることがうかがえる。

図4．6 コピーに対する考え方



出所:ACCSのデータを元に筆者が作成

図4．7 違法コピー経験の有無



出所:ACCSのデータを元に筆者が作成

（２）違法コピーを実際に行った経験者の比率は，全体平均では５１％であるが，パソコン歴３－５年では５５％，パソコン歴６年以上では７７％となっており，パソコンの使用経験が長くなるにつれて，違法コピーの使用が増加している。

（３）今後，「違法コピー」を行うか否かについて，68%もの学生が「使うと思う」と回答しており，「使わない」は4%に止まっており，27%が「わからない」と答えている。

（４）著作権者の許諾なく，インターネットやＬＡＮでソフトウェアを送受信することの

違法性については，５２％は「知っている」が，４５％もの人が「知らない」と答えており，フリーウェアやシェアウェア及びビジネスソフトウェアの著作権について，より一層の教育機会が望まれる。

以上の分析により，ソフトウェアの著作権については，従来の常識だけで判断することが難しくなってきていることが分かる。

上園 忠弘[4)]が言うように「情報社会の今日では，旧来の倫理観では律しきれない問題が多く発生している。それは人と人との関係ではなく，人と情報との関係である。すなわち，新しい犯罪の類型であるコンピュータ犯罪の問題であり，知的所有権の問題であり（中略）急速に進展するコンピュータ技術は今まで社会生活に設定されてきた種々の約束事を乗り越えていき，それに代わる『新しい』規範が求められている」といえる。

１．３ 企業における違法コピー意識調査

ライセンスマネジメントに際しては，体制の整備が肝要である。次に，日本パーソナルコンピュータソフトウェア協会（ＪＰＳＡ）がまとめた「違法コピー意識調査研究」報告書[5)]から日本企業における現状を分析する。

１．「ソフトウェアの購買部門の有無」については，６４％の企業があると答えており，企業側としての業務体制として整備されてきていることが分かる。

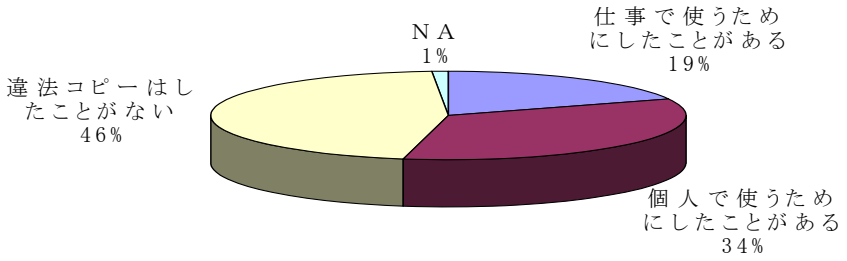
２．「ソフトウェア管理台帳の作成」については，「作成している」４３％，「作成していない」３５％，「わからない」２１％，となっており，購買部門での費用削減は図っているが，ライセンスマネジメントに対する意識はまだまだ低いことをうかがわせる。

３．「違法コピー防止通達の有無」については，「通達がある」５２％，「通達はない」２８％，「わからない」２０％，となっており，半数程度しか出されていない状況で，通達すら出していない企業では，まずは通達を出して全社員に徹底させることが求められている。

４．「違法コピー防止セミナーの実施」については，「行われている」１８％，「行われていない」６４％，「わからない」１６％，となっており，企業として積極的に違法コピー防止活動を行っているとは言えず，まだまだ不十分な状況である。

５．「違法コピー経験の有無」については図４．８のとおりである。「仕事で使うためにしたことがある」が１９％，「個人で使うためにしたことがある」３４％，「違法コピーはしたことがない」４６％，となっている。ＢＳＡの調査では日本国内では３１％が違法コピーとされており，「仕事で使うためにしたことがある」とした１９％の人は自分の分だけでなく，他人の分までライセンスをコピーしていることがうかがえる。特に情報システム部門の社員が上司の指示で違法コピーを行う場合は，違法コピー数も膨大なものとなり，企業としての責任が問われるのは当然のことである。

図４．８ 違法コピー経験の有無



出所：日本パーソナルコンピュータソフトウェア協会

６．「ソフトウェア監査の実施」については，「行われている」３３％，「行われていない」４４％，「わからない」２１％，となっており，今後より一層の実施が望まれる。企業としていくら通達を出していても，現場の責任者は利益追求や費用削減に追われ，ライセンス費用もコスト削減の一環との誤った認識に基づいて，違法コピーを指示したり，実行している可能性もある。内部牽制機能として，ソフトウェアに関するシステム監査の実施がなければ，グローバル企業の場合は違法コピーがなくなることはきわめて困難といえる。

以上，見てきたように企業においてもライセンスマネジメントについてはまだまだ不十分な状態であり，今後ともより一層のレベルアップが望まれる。

２．ソフトウェアの違法コピーと防止活動

２．１ ソフトウェアの法的保護

著作権法は著作権者に複製権，貸与権，頒布権をはじめとする種々の権利を独占的に認めている。著作者（法人を含む）は，複製権，放送権，貸与権などの「著作権」と，公表権，氏名表示権，同一性保持権などの「著作者人格権」の双方を持っている。著作権は著作者の死後50年（法人が著作者の場合は著作物の公表後，50年）まで存続する。ソフトウェアをコピーすることについては著作権の中の複製権が及び，原則として権利者の許諾を得る必要があることが著作権法に定められている。従って，権利者の許諾を得ずに無断でコピーすることが「違法コピー」となる。

ソフトウェアは使用許諾契約によって，権利者（著作権者）から使用が許諾されるもので，ユーザに認められた使用の範囲は使用許諾契約書によって規定されている。

２．２ 違法コピーの分類

違法コピーは以下のように分類することができる。

組織内違法コピー:エンドユーザによる許諾数以上のインストールやエンドユーザによる違法送信など

業者などによる違法コピー：インターネットやメールオーダーを利用した海賊版販売，販売店による違法なインストールなど

インターネットやパソコン通信を使った違法アップロード

無許諾レンタル

その他仲間内での貸し借りなど

文化庁の『コンピュータ・ソフトウェア管理の手引き［企業編］』[6)]では，以下の３つが考えられるとしている。

１．著作権の存在自体を知らずに違法コピーをしている場合。

２．著作権については何となく理解しているが，自社のしていることは「自分の会社の中でやっているのだから違法とはならない」と思って違法コピーをしている場合。

３．自分のしていることが違法だと分かっているが，予算の都合や，「どこの会社でもやっているし，自分のところでもやっても分からない」などという理由で違法コピーをしている場合。

上記のケースは，意識の違いこそあれ，いずれも違法コピーであることに変わりはない。もっとも，著作権法では，バックアップコピーを作成する場合などは，例外的に権利者から許諾を得なくてもコピー出来ることが認められている。

２．３ 違法コピーを行った時の制裁

違法コピーと知ってソフトウェアを使い続けることは，民事上，刑事上の制裁を受けるばかりでなく，テクニカルサポート，バージョンアップが受けられないという不利益を被ることでもある。また，ひとたび企業内違法コピーが明るみに出れば，社会的信用の失墜，社員のモラル低下など企業としての根幹を揺るがすことにもつながりかねない。違法コピーを行うと次のような刑事上の罰則や，民事上の損害賠償などの請求を受けることになる。

（１）刑事罰については以下のとおりである。

著作権法（第119条）違反として，3年以下の懲役又は，300万円以下の罰金が課せられる。

また，企業などの雇用者が「社員が勝手にやったことだ」と主張しても，その企業が，相応の注意及び監督を尽くしたということを証明しない限り，著作権法第124条の「両罰規定」により，企業側も刑事罰（罰金）が課される。

特に注意すべきは，平成13年1月1日より法人の罰金の上限が１億円に引き上げられことである。

（２）民事上の措置については以下のとおりである。

上記の他に，著作権者は以下の権利を有している。

1.差止請求権（著作権法第112条）

違法コピーなどの著作権を侵害する行為の停止や予防を請求する権利

2.損害賠償請求権（民法第709条）

著作権侵害により被った経済的及び精神的損害の賠償を請求する権利

3.不当利得返還請求権（民法第703条）

違法コピーを行ったために得た利益は，そのソフトウェアがなければ得られなかったはずである。違法コピーによって得た利得を請求できる権利。

4.名誉回復措置等請求権（著作権法第115条）

著作者人格権を侵害された場合に，著作者の名誉を回復するため，新聞への謝罪広告の掲載などを請求する権利。

以上，違法コピーを行った企業に対しては様々な制裁が課されるが，これらの制裁は経済的損失を与えるのみでなく，社会的信用を失墜させることとなり，経営者はライセンスマネジメントを重要課題の一つとして認識すべきである。

２．４ ソフトウェア違法コピー防止活動

マイクロソフト等は著作権保護の推進を目ざし，1988年に非営利団体の米国ビジネスソフトウェア連合（Business Software Alliance ，以下 ＢＳＡ）を発足させた。

日本における違法コピーの啓蒙活動については，1992年12月にＢＳＡ日本支部を設立し，著作権保護のパンフレットを有力企業に配布するなどして，違法コピーの監視体制を強化した。ＢＳＡ日本支部は，2年間啓蒙活動を行ったが効果が上がらないとして，1994年12月1日から違法コピー通報に謝礼金を支払うキャンペーンを開始した。これは違法コピー通報者には1件につき1万円を，訴訟になって証人として法廷で証言した場合には10万円を支払うものである。謝礼金は2000年には3万円と30万円にそれぞれ増額されている。

日本国内の動きとしては，1994年3月に日本パーソナルコンピュータソフトウェア協会が，日本監査役協会，日本内部監査役協会，日本システム監査人協会，ＥＤＰ監査人協会（現，情報システムコントロール協会）に対し，ソフトウェアの無断複製について適切な指導をするよう申し入れを行った。

もう一つの団体として，コンピュータソフトウェア著作権協会（以下，ＡＣＣＳ）がある。ＡＣＣＳはデジタル著作物の権利保護や著作権思想の普及活動を通じて，コンピュータ社会における文化の発展に寄与することを目指している。

1994年12月には労働省の外郭団体・雇用促進事業団が設立した教育訓練機関がパソコンソフトを大量に複製して使用し，コンピュータソフトウェア著作権協会から著作権法に違

反するとして改善を求められたことがマスコミに報道された。

３．ライセンスの形態と使用条件

ソフトウェアを使用するに際しては著作権者の許諾を得ることが必要であるが，著作権法では「使用権」という権利は規定されていない。「使用権」はソフトウェアを使用する際にユーザーがどのようにソフトウェアを使えるかを表す言葉として用いられており，個々の使用許諾契約によりその内容は異なる。

契約に記載されている範囲を超えて使用することは契約違反となるので，使用者は使用許諾契約を締結する際に，権利者が示した使用条件が自分の意図するソフトウェアの使用条件に適合しているかどうかを確認することが重要である。

３．１ ライセンスの契約形態

ソフトウェアの契約形態は主として次のように分類される。

（1）シュリンクラップ契約

パッケージ製品で１つのパッケージにインストール用メディアと製品マニュアルと１ユーザー分のライセンス証書が梱包されているもので，ソフトウェアを包装しているシュリンクラップ梱包を解いたときに権利者と購入者との間に使用許諾契約が成立したとみなされるのでこのように呼ばれている契約形態である。この形式は標準の使用許諾条件を定め，不特定多数のユーザーにソフトウェアを迅速かつ容易に提供するために利用されている。

（2）クリックオン契約

最近はネットワーク経由で提供されているソフトウェアも増加しており，ネットワークからダウンロードする前に契約条件を読み，同意ボタンを押すことで同意したものとみなす形態である。

（3）ライセンス契約

これは権利者とユーザーが直接使用許諾契約に署名捺印をして契約を締結するもので，ライセンスパックとボリュームライセンスに分類される。

① ライセンスパック

インストール用のメディアと製品マニュアルが各1セット含まれ,使用可能な本数が明記されたライセンス証書が発行される。

② ボリュームライセンス１

初回購入時の本数（ボリューム）により一定期間内の価格ランクが決定する。

例えば，初回100本のライセンスを一括して購入すれば，100本一括購入用の価格ランクで購入することが出来，初回購入時から2年間は，同じ価格ランクで追加購入できる，といったものである。

ボリュームライセンス１の例としてはMicrosoft Open License，Lotus Pass Port/VPO，Symantec Value license 等がある。

③ ボリュームライセンス２

これは一定期間内の購入ボリュームを契約開始時にコミットメントし，その購入予定量により価格ランクが決定する。購入予定量が多いほど低価格で購入することが出来る。

例えば，２年間で１万本を購入する契約を締結し，価格ランクが決定されるが，ユーザーは契約した期間内に契約した本数以上を購入することを義務付けられる。

ボリュームライセンス２の例としてはMicrosoft Select，Microsoft Enterprise Agreement，Lotus Pass Port/CO 等がある。

この契約形態では，１法人だけでなく関連会社を含む企業グループ全体まで含むものが多く，日本で契約した内容が海外を含む子会社にも適用されるものもあり，企業グループ全体としての中期情報システム戦略計画が策定されており，それに従って契約本数が決定される場合が多い。この契約形態の場合，契約締結時はもちろんのこと，締結後も十分な注意が必要である。

Microsoft Select契約の例では，２年間で１万本[55]を購入する契約を締結した場合，中間点の１年目の購入累計本数が契約本数の50%(5,000本)以上でなければならない，等の条件があり，契約締結後も契約内容に沿って適切な台数を購入しているか確認する必要がある。

[55] 正しくは「本数」ではなくソフトウェア毎に指定さている「ユニット数」の合計である。

Microsoft Select契約で購入するには，まずはマイクロソフト社[56]とMicrosoft Select基本契約を締結し，続いてマイクロソフト社とＬＡＲ[57]（Large Account Reseller）とユーザー企業との３者でMicrosoft Select加入契約を締結する。Microsoft Select契約での購入はＬＡＲ経由でなければならず，ＬＡＲはユーザー名と購入台数をMicrosoft社に報告し，ユーザは使用許諾を得る。ＬＡＲからの報告に従って後日，Microsoft社から購入部署と本数が記入されたライセンス証書が契約者に送付される。グローバル企業ではこのライセンス証書を一括して保存し，ライセンスマネジメントに利用していることが多い。

３．２ ライセンスの使用条件

使用に際しては以下の点について注意が必要である。

（１）アカデミーパック

アカデミーパックやキャンパスアグリーメント等と呼ばれるもので，学生や教育機関を対象としたライセンスで，教育用として特別価格を設定しており，一般企業では利用することができない。

（２）同時使用ライセンス

これは購入したソフトウェアについて，同時に使用する台数が契約した台数以内であれば許可するというものである。例えば，100台のパソコンを所有していても，該当するソフトウェアが同時に30台以上稼動しないように管理すれば30台分のライセンスを購入するだけで良く，大幅なコストダウンが可能となる。

しかし，マイクロソフト社を始めとして主要なソフトウェア会社では同時使用ライセンスについては許可をしていない場合が多いので，注意が必要である。

（３）個人ごとの使用許諾

コンピュータのハードウェア毎にライセンスが必要なものが多いが，電子メールやグループウェアなどの製品では，ソフトウェアを使用する個人ごとに使用許諾され

---

56 日本の場合は日本マイクロソフト社と締結する。

57 セレクト契約での購入に際して，マイクロソフト社が指定した取扱企業のこと。

るというものもあり，その場合は個人ごとの管理が必要となる。[58]

（4）モバイルユース

ソフトウェアの中には，１ライセンスで社内のコンピュータとモバイル用のコンピュータの両方にインストールして使用することを認めるものがあり，この場合は管理者は従業員にモバイル用として該当のソフトウェアの使用を許すことができる。しかし，すべてのソフトウェアがモバイルユースを許しているわけではないので注意が必要である。

４．ＴＣＯ削減

４．１ マイクロソフトセレクト契約におけるＴＣＯ削減

ボリュームライセンスとして代表的なマイクロソフトセレクト契約について，その概要とＴＣＯ削減について分析する。

（1）契約形態の概要

大手企業ではソフトウェアのコスト削減は主要テーマとしてクローズアップされている。そのような中で，子会社を含む企業グループ全体としてソフトウェア購入について一本化して契約する形態で，次の特徴を持つ。

① 購入予定量に応じて，大量のソフトウェアを低価格で購入可能。

② ２年間の購入見積りに基づき，必要なソフトウェアを計画的に導入できる。

③ 子会社を含め，企業グループ全体として低価格で購入が可能。

④ アプリケーション製品群，サーバー製品群など，同じ製品群であればさまざまなマイクロソフト製品を自由に購入できる。

⑤ アップグレードアドバテージを購入することで，バージョンアップにも柔軟に対応が可能。

---

[58] グループウェアの「ロータスノーツ」はノーツを利用する個人毎にライセンスが必要となる。

⑥　購入するのはライセンス（契約に基づく使用許諾権）であり，ＣＤ－ＲＯＭやマニュアルなどの媒体は別途購入することが必要となる。

各企業はまずマイクロソフト社とマイクロソフトセレクト基本契約を締結し，次にマイクロソフト正規取扱企業（Large Account Reseller：ＬＡＲ）と加入契約を締結する。実際の購入に際しては，ＬＡＲが受注から納入までをサポートする仕組みである。

（２）ＴＣＯ削減事例

①　モバイルパソコンのライセンス

マイクロソフトセレクト基本契約書・製品使用権説明書(June 1998)では「特段の規程のない限り以下の条項が適用される」として，「本ソフトウェアがコンピュータの固定メモリーにインストールされ，かつそのコンピュータを使用する者が特定の一人に限られている場合，そのコンピュータに組み込まれている本ソフトウェアを同時に実行しない限り，その者が専用に使用される別の携帯型コンピュータ上にて本ソフトウェアを使用することができる」とある。したがって，上記の条件を満たす従業員が，モバイル用としてもう１台のパソコンに，会社で使用しているものと同様のソフトウェアをインストールすることは許されるので，別途購入する必要はない。しかし，モバイル用パソコンにも別途ライセンスを購入しているケースがあるものと推測される。セールスマン1,000人（台）にモバイルパソコンを持たせた場合は, MS-Office Pro のライセンスだけでも ４～５千万円もの費用が発生しているはずで，コスト削減効果は大きい。

②　パソコンの入替え

古くから情報化に取り組んできた部門では, ＭＡＣを導入している部所が多いが，次第にWindows に入替えるケースが増加している。パソコンをＭａｃから Windows に入替える場合，すでにＭａｃ用のMS-Office Pro For Ｍａｃを購入している場合が多い。しかし，パソコンが替わったためにライセンスは新規購入が必要と思って，実際に新規購入しているケースが多い。しかし，ＭａｃからWindowsへの入替えの場合は，バジョンアップライセンスの購入で可能である。[59]

MS-Office Pro の場合，新規購入の場合４－５万円するものが，バジョンアップ

[59] Windows からＭＡＣに入替える場合は新規にライセンス購入が必要である。

ライセンスの場合半額程度で可能となる。

③　セレクト対象ライセンスの確認

ビジオやビジュアルベーシックなどは，マイクロソフトセレクト契約のアプリケーション群に含まれているにもかかわらず，そのことを知らずに，一般価格からの値引き交渉をしている場合が見られる。グローバル企業においては全世界に事業場が分散しており，これらの情報を各職場に的確に知らせる仕組みを構築することが重要である。

４．２ 同時使用によるＴＣＯ削減

クラリスインパクトやクラリスワークスを含め，旧クラリス社[60]は同時使用ライセンスを認めてきた。同時使用権による使用とは，所有しているライセンス数以上のパソコンにソフトウェアをインストールしても，該当するソフトウェアを同時使用できるパソコン台数をコントロールすることにより，所有しているライセンス数を超えては使えないようにする方法である。

このライセンスを利用することにより，ソフトウェアのコスト削減が可能となる。しかし現在では，マイクロソフト社を始めとして，同時使用権を認めているソフトウェア会社は非常に少なくなっている。

ソフトウェアの使用については，許諾された条件にしたがって利用することが必要であるので，使用許諾書に記載された条件を良く理解しておくことが重要である。例えば，Ｍａｃ用として購入したライセンスについてはＭａｃパソコンだけで利用するようになっているか，Windowsパソコンに使われていないか，などの注意が必要である。

クラリスインパクトでは１ライセンスで２台までの利用を認めたハイブリッドタイプと呼ばれるライセンスがあり，これはＭａｃ，Windowsいづれのパソコンであっても２台まで利用することが可能なので，Ｍａｃ，Windowsによる制限はない。

このように同時使用に際しては，様々なライセンスの使用許諾台数を合計して利用するケースが多く，それぞれのライセンスの使用条件が異なっているいることもあり，細心の

60　クラリス社は「クラリスインパクト」を始めとする大半の事業をアップル社に吸収合併され，現在，残っているのはファイルメーカ社である。

注意が必要である。

４．３ ソフトウェア買取りによるＴＣＯ削減

パソコンを購入するとハードウェアメーカがリース会社を紹介してくれることが多い。その際，リース会社はソフトウェアもハードウェアと一緒にリースにした金額を提示することが多い。しかし，ハードウェアとソフトウェアを一括でリース契約している場合，リースが完了して新機種に入替える時には，ソフトウェアライセンスはハードウェアに付帯しており，リース会社が所有していることになる。従って，新機種のハードウェアについては新たにソフトウェアのライセンス購入することが必要となる。

ハードウェアはリースで，ソフトウェアは買い取りで購入している場合，ソフトウェアの使用権は自社が所有しているので，新機種に入れるソフトウェアは同じバージョンであれば費用発生はしないし，バージョンをあげる場合でも，バージョンアップ費用だけで済む。ソフトウェアの購入について，リースアップ後のことも考慮した対策を実施することが肝要である。

このことは実に単純なことであるが，知らずに多くのソフトウェア費用を支払っている部門が実際には散見される。正しい運用で無駄なソフトウェア費用の発生を押さえるだけで大きな費用削減が可能となる。例えば, 1000台のパソコンを所有している事業所の場合，１台のパソコンのソフトウェア費用がエミュレータやMS-Officeなどのソフトウェアを含め，合計１５万円だとすると，ソフトウェア費用だけで１億5000万円となる。それをすべて買い替えるのと，そのまま使うのとでは大きな違いである。MS-Officeなどはバージョンアップする場合も有るが，特にエミュレータについては，上記のケースでは合計金額が約１億円と高額な上にバージョンアップのケースは少なく，無駄なコストを支払っているといえる。4年間リースの場合，1年間では2,500万円もの費用削減を図れることになる。

グローバル企業では，ライセンスマネジメントの専門家が実際の現場に赴き，監査を実施することが，違法コピーを無くし，なおかつ，大きな費用削減につながるケースが多いと言える。こういったことは本来は通達などにより徹底されているはずであるが，グローバル企業での現場は多岐に渡っており，部門経営者自身が自部門のことであると気付いていないケースも考えられる。

５．ライセンスマネジメントの方法

５．１ ソフトウェア管理ガイドライン

ソフトウェアの違法コピーを防止し，適正な管理の実施を促し，その具体的な取り組みの指針とするためのガイドラインとして「ソフトウェア管理ガイドライン」が1995年11月に通商産業省から公表されている [7]。その概要は以下のとおりである。

（１）法人等が実施すべき基本的事項として，次の4項目が定められている。

・ソフトウェアの管理責任者の任命及び管理体制の整備

・ソフトウェア管理体制の策定

・ソフトウェアの使用状況の監査

・ユーザへの関係法令や仕様許諾契約等の教育，啓発

（２）ソフトウェア管理者が実施すべき事項としては次の３項目が定められている。

・ソフトウェア管理台帳の整備

・違法コピーされたソフトウェアに対する速やかな措置

・関係法規，ソフトウェア管理規則，使用許諾契約の周知徹底

（３）ソフトウェアユーザが実施すべき事項としては次の２項目が定められている。

・関係法令，ソフトウェア管理規則，使用許諾契約，管理責任者の指示の遵守

・法人等の事業所における個人が保有するソフトウェアの使用について

５．２ コンピュータ・ソフトウェア管理の手引き

次に1997年３月に文化庁から「コンピュータ・ソフトウェア管理の手引き［企業編］」が公表された [8]。これは1994年に「コンピュータ・ソフトウェア管理の手引き［学校編］」を，1995年に「コンピュータ・ソフトウェア管理の手引き［大学編］」を公表したことに続くもので，企業におけるソフトウェアの違法コピーを防止するためのソフトウェアの管理のあり方について，企業の知的所有権担当部局などの法務担当者や各部署におけるソフトウェアの導入・利用の担当者を対象として作成されたものである。

これら「ソフトウェア管理ガイドライン」や「コンピュータ・ソフトウェア管理の手引［企業編］」については，情報システム部門の責任者を除けばその存在すら知らない経営

者も多い。その原因の一つは，著作権に対する意識が低く，ソフトウェアの違法コピーについての認識が希薄であるといえる。

５．３ 管理方法

グローバル企業でのライセンスマネジメントは以下の項目を実施する。

１．通達などにより，各職場（又は事業場）における情報システム管理者を任命する。

２．各職場における情報システム担当者を任命する。

３．各職場毎の情報システム担当者はライセンスマネジメント台帳を作成する。

４．情報システム部門が管理するソフトウェアと各職場が管理するソフトウェアを区分する。

５．各職場で管理するソフトウェアについてはライセンス証書を各職場で保管する。

６．情報システム部門で管理するソフトウェアについては，担当する情報システム部門がライセンス証書を管理する。ただし，実際には証書で保管するケースは少なく，本社情報システム部門が全社的に掲示している部門毎のライセンス数を比較・参照する場合が多い。セレクト契約で購入したライセンスを本社で一括管理している場合は，海外の事業所で購入したソフトウェアについても，全社掲示板にもれなく記載することが必要である。

６．ライセンスマネジメントについてのシステム監査

以上，見てきたようにライセンスマネジメントの重要性については，ひとたび新聞への謝罪広告などが出ると，今まで長年かかって築いてきた企業イメージの著しい低下など，重大な問題になりかねない。しかし，今までライセンスマネジメントについての研究は皆無といってよい。筆者はグローバル企業のおけるシステム監査部門においてライセンスマネジメントを取り上げ，実践し，ＴＣＯ削減との両輪で実施することで大きな効果を上げてきた。

ライセンスマネジメントが各事業場で正しく継続的に実施されていれば問題はないのだが，グローバル企業においては，子会社や各事業場でそれぞれに状況が異なる。子会社や

各事業所には本社部門から多数の通達類が配布されているが，ソフトウェアについては情報システム部門の問題であると思い込み，通達の内容を良く理解せずに放置している経営者もいる。このような場合を含めて，内部牽制機能としてのシステム監査が有効である。特に小規模な事業所や子会社ではシステム監査実施時に，ライセンスマネジメントについて確認することは有用である。

次に，ライセンスマネジメントのシステム監査についての方法を述べる。

６．１ ライセンスマネジメントのシステム監査の方法

グローバル企業においては，推奨パソコンを設定している場合が多い。ハードウェアの機種や，ソフトウェアについてもバージョンなども含め詳細に決められている。ソフトウェアについてもセレクト契約などを締結して全社的な費用削減を図っている。情報システムの管理体制についても，担当すべき情報システム部門が決まっており，これらの部門と連絡を取って，システム監査を実施する。

監査の実施に際しての手順は以下のとおりである。

１．各部門毎に時間を区切って実施する。

２．設計部門など，独自に情報システムを導入している部門があれば，その部門も含める。

３．部門責任者の同席を求め，ライセンスマネジメント状況を確認する。

４．利用しているソフトウェアを記載している管理台帳の有無を確認する。

５．サンプリング調査により，管理台帳の記載内容と該当するパソコンにインストールされているソフトウェアが合致していることを確認する。

６．自宅からの持ち込みパソコンなど台帳に記載されていないパソコンが設置されていないか，また，台帳に記載されていないソフトウェアがインストールされていないかを確認する。

７．台帳に記載されているライセンス証書の現物を確認する。

ライセンスマネジメントのシステム監査は，システム監査人の人数や監査日数の関係から，数千人規模の事業所の場合は，それだけで独立したテーマとして実施する必要があろうが，数百人規模の事業所においては，他のシステム監査の実施に際して同時に実施することが可能である。

システム監査の実施に際しては，ライセンス管理台帳が作成されていることが前提であるが，一部の子会社ではこれらの作成すら実施していない場合もある。システム監査人は監査の実施に先立って，被監査部門にライセンス管理台帳の作成を確認しておくことが望ましい。

６．２ システム監査の留意点

システム監査に際しては，以下の点について確認することが必要である。

（１）ハードウェアとソフトウェアの一括リース契約の確認

前述のように，このことはライセンスマネジメントをしているものにとっては当然のことであるが，グローバル企業では末端の管理においては十分に注意が払われていないことが多い。

（２）モバイルユース及びホームユース

マイクロソフトセレクト基本契約書・製品使用権説明書(June 1998)では「特段の規程のない限り以下の条項が適用される」として，「本ソフトウェアがコンピュータの固定メモリーにインストールされ，かつそのコンピュータを使用する者が特定の一人に限られている場合，そのコンピュータに組み込まれている本ソフトウェアを同時に実行しない限り，その者が専用に使用される別の携帯型コンピュータ上にて本ソフトウェアを使用することができる」とある。したがって，従業員がモバイル用としてもう１台のパソコンに，会社で使用しているものと同様のソフトウェアをインストールすることは許される。

しかし，Microsoft Office 7.0 や Microsoft Office Professional 7.0 などについては「その者が専用に使用される別の１台のコンピュータ（携帯型コンピュータ又は家庭用コンピュータ）上にて本ソフトウェアを使用することができる」となっており，バージョンによってモバイル用だけでなく家庭用のパソコンにもインストールすることが許されている。

これらの条項を知らない場合，上記の条件を満たしているにもかかわらず，携帯パソコンについても新たにライセンスを購入してしまうことが考えられる。また，携帯用でない家庭用のパソコンに，会社で利用しているソフトウェアをインストールすることについては，Microsoft Office 7.0 などであれば可能であるが，それ以降のバージョンでは許されていない。

注意すべきは，マイクロソフトセレクト基本契約書の第一条「概要」には「（中略）加

入カスタマは自己の社内使用及び甲又は甲関連会社の使用の為にライセンスを取得することが認められるが，その他の一切の個人又は法人の使用又は利益の為にライセンスを取得することはできない」となっており，たとえ社員であっても，個人へのライセンス取得は許されていない。会社のライセンスが，家庭で個人的に利用するパソコンなど，業務目的以外のパソコン用に使われていないことを確認する。

（3）サーバーへのソフトウェアのインストール

各部門毎にサーバーを設置して，情報共有を推進している事例が増加している。また，インストール用にサーバーにソフトウェアを記憶させておく例も増加している。しかし，サーバーにアプリケーションをインストールして，ソフトウェアも共有して利用すればコストダウンが図れるなどと考えても，それは契約違反となる。

マイクロソフトセレクト基本契約書・製品使用権説明書(June 1998)では「ネットワークサーバーのような記憶装置に本ソフトウェアのコピー１部を蓄積又はインストールすることができる。ただし，ライセンシーは本ソフトウェアがインストールされたコンピュータ又は記憶装置から本ソフトウェアを作動しているコンピュータのすべてについて，専用のライセンスを取得する必要がある。１つのライセンスを異なるコンピュータ間で共有したり，同時に使用することはできない」とある。

（4）発売中止されたソフトウェアの継続的利用

各職場には毎年新入社員が配属される。しかし，今まで作成していた資料がクラリスインパクトなど発売中止となったソフトウェアで作成されていた場合，新入社員のパソコンにもそのソフトウェアをインストールしていないか，確認することが必要である。

「購入したいのだが発売されていない，だからコピーすることは致し方ない」などと考えてコピーをしているケースもあり，ある者は「発売が中止されたソフトウェアはコピーフリー（無料）」などと思っていることもありえる。これらはいずれも誤りである。
発売中止となったソフトウェアについては利用できるパソコン台数を限定して，現在所有しているライセンス数の範囲で利用する方法を検討することが必要であり，根本的にはこれに替わるソフトウェアを選定し，順次移行することが求められる。

（5）組織再編成や人事異動に伴う部署名変更管理

セレクト契約で購入したライセンスについては，取得毎・職場毎に数量が登録され管理されている。しかし，組織再編成で事業部門の統廃合が行われた場合，当初に登録された部署名とは異なり，また，事務所の移転なども有り，現実に最新の部署名と合計数量を維

持管理することは多大の手間と時間とコストを要する。システム監査人は職場におけるライセンスマネジメントの実態を把握し，管理精度とその妥当性を評価することに努めることとし，管理精度を上げる為にあまりに大きなコストがかかりすぎる内容を要求することは避けなければならない。今後，ライセンスマネジメントを含めた各種の管理ツールの提供により，これらの管理コストが劇的に低減されることが望まれる。

以上，見てきたように，ソフトウェアライセンスについては，契約書を詳細に確認して，無駄なライセンス費用を支払うことのないよう，また，必要なライセンス数を正しく購入することが求められており，管理部門は充分な注意を払うことが重要である。特に，子会社や小規模の事業所においては，ソフトウェアライセンスに対する認識が薄い場合が多く，セレクト契約で安価にソフトウェアを購入できるということについても知らず，通常の市販ルートで購入しているケースも見られる。ライセンスマネジメントについては，単に担当者の知識不足と言う見方だけでなく広く教育の問題やセキュリティ対策の一環として考えるべきであろう。

７．おわりに

本稿はグローバル企業における，ライセンスマネジメントとシステム監査のあり方について，分析を加え具体例を含めた提言を行った。ライセンスマネジメントは，システム監査としては従来はあまり重視されていない分野であった。しかし，知的財産権の保護の観点から企業としても真剣に取り組む必要が出てきており，今後も重要性は増加するであろう。システム監査の実施により無駄なソフトウェアコストの削減を図ることも可能となる。企業のセキュリティ対策の一環として，また，内部牽制機能として，ライセンスマネジメントについてのシステム監査の実施が求められる。

ソフトウェアメーカーにおいては，ライセンスマネジメントが容易に実施できる安価なツールの提供と，企業全体のパソコン台数での一括管理など，より管理しやすい形態を前提とした安価な価格体系が望まれる。

参 考 文 献

１）金融情報システムセンター 「ＦＩＳＣ新システム監査指針」 (2000)

２） http://www.bsa.or.jp/ Business Software Alliance（ＢＳＡ）ホームページ

３）（社）コンピュータソフトウェア著作権協会「学生における違法コピー実態調査」(2000)

４）上園 忠弘 「企業人の情報倫理」大阪大学大学院国際公共政策研究科 博士論文 p. 31 (1999)

５）日本パーソナルコンピュータソフトウェア協会 「違法コピー意識調査研究」報告書 (2000)

６）文化庁『コンピュータ・ソフトウェア管理の手引き［企業編］』p.4 (1998)

７）通商産業省機械情報産業局「システム監査白書1999-2000」p. 285 (2000)

８）文化庁『コンピュータ・ソフトウェア管理の手引き［企業編］』 (1998)

第５章 セキュリティポリシーと国際標準化

インターネットの普及及び拡大により，不正侵入やコンピュータウイルスに感染するリスクが増加している。ファイアーウォールを設置していない企業や，設置していてもセキュリティホール対策がタイムリーに実施されていないケースもある。ウィルス用ワクチンをインストールしていてもパターンファイルが古いため新種のウィルスから防御できないケースが見られる。企業においてその対策は急務となっており，トップマネジメント自らがリスクに対する認識を深め，組織構成員にその重要性を知らせることが重要である。効果的なリスク対策を実施するには，リスクに備え組織的な対応を実施するための「セキュリティポリシー」を策定することが望まれる。

広義のセキュリティは，コンピュータセキュリティやネットワークセキュリティに限らず，組織の各種設備や人的資源，情報資源を含む全資産に対する保全行為，安全運用を指す。従って，本来コンピュータセキュリティやネットワークセキュリティは，組織資産全体のセキュリティ方針である「コーポレートセキュリティポリシー」のサブポリシーとして位置づけられるべきものである。ここでいうセキュリティポリシーとは，「利用者個人の裁量で情報セキュリティについて判断されることがないように定められた，企業・組織の情報資産を適切に保護するための，企業・組織としての安全対策に対する基本方針のこと」とする。

欧米では1980年代から情報機器の安全評価制度の整備が進んでおり，国際的な統一基準としてまとめられた「Common Criteria」と呼ばれるものがある。1996年２月にＶ1.0が，1997年12月にＶ2.0がリリースされ，1999年６月に国際標準化機構（以下，ISO）では，これがほぼそのままISO／IEC15408として制定された。これに基づいて実施すべきセキュリティ対策を決定したあと，どのようにシステムを構築・運用するかを規定したガイドラインについても，ISOで標準化が進んでいる。これは「Guidelines for Management of Information Technology Security」といわれている。ISOの「Common Criteria」とそのガイドラインは，国際的な基準として企業が実施すべきセキュリティ対策を決める指針となるものであり，今後の動向に対して十分な注意が必要である。

日本においては1998年５月に通産省が，関連団体の情報処理振興協会（ＩＰＡ）内に安全基準を作るための専門部会を設けることを発表した。従来のままでは，国境を超える電子商取引や特定の国際情報網への接続を拒否される事態が生じかねない状況であり，安全

評価制度の確立が急務となってきている。

本稿は，第１節で世界の標準化動向と日本の現状について分析し，第２節でセキュリティ評価の国際標準であるISO 15408について分析し，第３節でセキュリティ評価に合格するためのプロセスについてまとめ，第４節でセキュリティポリシーのあり方について考察する。

１．セキュリティ標準化における世界の動向と日本の現状

１．１　セキュリティ標準化における世界の動向

セキュリティのレベルを評価して認定する制度化については米国が最も早かった。1985年に軍事システム向けに政府が調達する製品に対してセキュリティレベルを評価して認定する制度を作った。この基準書が「ＴＣＳＥＣ：Trusted Computer Security Evaluation Criteria」というもので，通称「オレンジブック」と呼ばれている。古くは軍事専用であったものが現在では商用の製品についてもこの基準で評価を受けている。

ヨーロッパにおいては，英国，ドイツ，フランスで1991年よりプライバシ情報の保護を主目的にセキュリティ評価及び認証制度を作り運用している。これは「ＩＴＳＥＣ：Information Technology Security Evaluation Criteria」と呼ばれるもので，「ＴＣＳＥＣ」とは異なり，製品のみならず運用システム全体も評価の対象としている点が特徴である。

（１）国際標準化機構（ISO）の動向

インターネットが発達した今日，このように各国の基準がバラバラでは国際的なネットーワークの安全性の確保を保証しにくい。そこで1994年に，米国，カナダ，英国，フランス，ドイツ，オランダの６カ国が共同で基準書を統一するプロジェクトを発足させた。その結果「ＴＣＳＥＣ」と「ＩＴＳＥＣ」を踏まえて生まれたものが「Common Criteria V2.0」で，1997年12月に発刊された。1999年６月に国際標準化機構では，これがほぼそのままISO／IEC15408として制定されている。

（２）経済開発協力機構（ＯＥＣＤ）の動向

1992年11月に策定したセキュリティガイドライン（情報システムのセキュリティのためのガイドライン：Guidelines for the Security of Information System）は，セキュリティ

のための９つの原則（責任，周知，倫理，総合，比例，統合性，適時性，再評価，及び民主主義）を示し，ＯＥＣＤ加盟国におけるセキュリティ政策の指針となってきた。

策定後５年が経過した1997年は，同ガイドラインの見直しの年となっており，1996年にＯＥＣＤ事務局より加盟各国および関係者に対して１５項目からなる見直しに向けた質問書が送付された。その結果は，Review of the 1992 Guideline for the Security Information System (DSTI／ICCO／REG(97)／FINAL)にまとめられている。

ガイドラインの見直しには至らなかったものの，セキュリティに関する認識はこれまでの５年間で高まってきたことから，今後も継続的に啓発活動が必要であるとし，セキュリティ訓練や教育の充実，セキュリティインシデントへの対応や情報提供を行うComputer Emergency Response Center の充実の必要性が加盟国の共通認識として確認されている。

（３）米国におけるセキュリティマーク制度の動向

日本においては1998年4月から「プライバシーマーク制度」が発足したが，米国の金融機関においてはプライバシー保護を包含した「セキュリティマーク制度」の導入を検討している。これは，当該金融機関におけるセキュリティ実施レベルを示すマークであり，２～３レベルに分けることが検討されており，次のような考え方でレベル分けがなされることも考えられることを示唆している。

①ハイレベルマーク：金融機関が多くのコストをかけて，高いレベルの安全対策を実施している。または，何かがが発生した場合，金融機関がリスクをかぶる体制を整えているといった場合に付与されるプレミア的マーク。

②中間レベルマーク：ハイレベルとミニマムレベルの中間

③ミニマムレベル：最低限の安全基準に合致しており，利用者には多少リスクがあるかも知れないが手数料が安いといった金融機関に付与されるマーク

１．２　セキュリティ標準化における日本の現状

1995年に（社）日本電子工業振興協会（ＪＥＩＤＡ）が「Common Criteria」に基づいて作成したセキュリティ基本要件を記述した Protection　Profileを発表した。Protection Profileは情報システムの個々の適用領域やシステムごとに必要とされるセキュリティ要件を記述したもので，そのため個々の適用領域やシステムに対応した Protection　Profileが今後開発されることになる。

ＪＥＩＤＡの基本要件は，必要なセキュリティ機能がシステムに実現されていることを評価するための「機能要件」と，そのセキュリティ機能が実施されていることを評価するための「保証要件」で構成されており，それぞれに機能編，保証編と称している。1997年８月には機能編について「Common Criteria」第一版の要求項目を採用し，そのうえ，ＥＣＭＡ（European Computer Manufacturers Association）のＥ－ＣＯＦＣ（Extended Commercial Oriented Functionalities Class）のネットワークに関する項目を参考にして，第二版を発表した。また，ＪＥＩＤＡはセキュリティ評価技術の基礎研究プロジェクトを組織して，基本要件をベースにした評価実験を推進している。

ＪＥＩＤＡの活動は多くの成果をもたらしたが，日本には現在もセキュリティ評価基準・相互認証制度が確立していない。そのため，ＩＰＡは98年から２年間の計画でＣＣＴＦ（Common Criteria Task Force）を立ち上げて，日本におけるセキュリティ評価技術の確立などを目的に活動している。

日本政府においては，通産省が1998年５月にＩＰＡ内に安全基準を作るための専門部会を設けることを発表した。基準作りでは情報機器の種類別に利用者の識別，流通情報の暗号化，不正利用の追跡など２００項目以上の観点から７段階の評価基準を設けているISO 15408を参考にすると思われる。同時に民間団体を含めた複数の評価機関の発足を支援することとし，その評価機関は安全性について数段回で格付けを行い，日本で取得した安全評価が海外でも通用するよう，欧米の評価機関と相互認証協定を結ぶことも目指している。

日本におけるセキュリティポリシーに関する調査については，情報システムコントロール協会（ＩＳＡＣＡ）東京支部が1998年に６月に発表したものがある。その結果によると，文章化されたセキュリティポリシーが「ある」との回答は３９％，「作成中」１１％，「作成予定あり」３０％，「作成予定なし」２０％，となっている。「作成中」と「作成予定」を合わせると４１％にもなり，日本においてもセキュリティポリシーの作成が急速に進んでいることがうかがえる。

現状では多くの事業体において，簡略的な部報レベルでの作成は見られるが，包括的に明文化されたセキュリティポリシーやセキュリティ計画は存在していない場合が多い。セキュリティポリシーに対しては組織としての明確な意思表示を行うため，トップ自らの名前で周知徹底することが望まれる。これより関係者はセキュリティの必要性について具体的に認識でき，業務遂行上の各種判断や行動においてセキュリティを考慮した的確な意思決定が可能となり得る。

２．セキュリティ評価の国際標準規格 ISO 15408

1999年6月にセキュリティ評価規格についての国際規格案（DIS：Draft International Standard）が承認され，新しくISO 15408（正確にはISO/IEC15408）として発表された。これにより従来の品質保証の国際規格であるISO9000及び環境管理の国際規格であるISO14000に引き続き，ISO 15408のセキュリティ評価規格に基づいたセキュリティ対策の実施について各企業や組織体は早急に対応を迫られることになろう。

２．１　セキュリティ評価基準の国際標準化の意義

セキュリティ対策実施の問題点は，投資効果が不明であったり，どのレベルまで実施すべきかが不明確なため必要性は理解できても実施に結びつかなかないことが多い。セキュリティ対策に関する国際標準化によってどのレベルを目指すかを明確にすることが可能となる。

今後は，国際的な企業間ネットワークに接続する際に，一定レベル以上のセキュリティが確保されていることが条件になる可能性もあり，あらかじめ国際標準（ISO）に基づいたシステム企画や設計を行うことにより適合システムを構築することが可能となる。又，運用段階でもISO 15408 のチェックポイントを利用すれば効果的にセキュリティ対策を実施することが可能になる。

ユーザーは評価対象の製品またはシステムがそれぞれのセキュリティニーズを満たしているかどうかを判定する一助として，また，様々な製品またはシステムを比較する場合に評価結果を用いることができる。

どこまでプライバシー情報を管理すれば社会的な責任を果たしたことになるのか，どこまで企業秘密を管理すれば管理したことになるのか，など，従来はセキュリティについての基準が不明確であった。セキュリティ評価基準の国際標準があればそれに従った対策が可能となる。

セキュリティ対策に対してレベル付けを行うことによりリスクと対策のバランスを取ることが可能となる。民間で使われるセキュリティと軍事用のセキュリティとでは自ずとレベルが異なる。例えばISO 15408では評価を７つのレベルに分けており，民間で使用されるものとしてはレベル３～４を目指しており，軍事用はレベル６～７である。

２．２　ISO 15408の概要

ISO 15408については，具備すべきセキュリティ基本要件をコモンクライテリアで明示しているので，本稿では以後詳細はこのコモンクライテリア（Common Criteria V2.0）に記載されている内容を中心に論述する。なお，コモンクライテリアについては，ＩＰＡ（情報処理振興事業協会）セキュリティセンターが翻訳を行っている。[61]

（１）適用範囲

ISO 15408は，情報技術を用いた製品やシステムのセキュリティ機能を対象としており，ソフトウェアだけでなく，ハードウェア(PBXなど)，ファームウェア(ICカードなど)，あるいはシステム全体も評価対象となる。

製品の形態は，ファイアウォールのように，直接セキュリティに関係する機能を提供する製品ばかりでなく，ユーザに対してパスワード入力を求めるオペレーティングシステムやデータベース，業務上の役割ごとにアクセス管理を行うグループウェアなど，保護すべき資源を保有する製品やシステム全般が対象となる。規格で取扱われる内容には，セキュリティ機能の技術的な対策のみではなく，このような製品やシステムを利用するためのセキュリティ教育やセキュリティ監査といった組織的なセキュリティ運用や管理などの対策も含まれる。

注意すべきはこれらの製品やシステムが評価の対象であり, ISO9000やISO14000のように組織を評価するための基準ではない点である。

（２）セキュリティ評価基準の構成

セキュリティー評価基準は三部で構成されており，第一部は「概説と一般モデル」第二部は「セキュリティ機能要件」第三部は「セキュリティ保証要件」となっている。

第一部「概説と一般モデル」は概説で，IT（Information Technology）セキュリティ評価の一般的概念と原則を定義し，評価の一般モデルを示している。セキュリティ環境，セキュリティ要件，評価の種類，保証維持，評価結果等について書かれている。

第二部「セキュリティ機能要件」は，評価対象の機能要件を表現する標準的な手段として，機能コンポーネントのセットを規定している。セキュリティ監査，通信，暗号，ユーザーデータ保護，識別と認証，セキュリティ管理，プライバシー，セキュリティ機能の保

---

[61] http://www.ipa.go.jp/SECURITY/ccj/index-j.html　Common Criteria ホームページ

護，資源利用，アクセス管理，信頼通信路などについて書かれている。

第三部「セキュリティ保証要件」では，評価対象の保証要件を表現する標準的な手段として，保証コンポーネントのセットを規定している。構成管理，配布と運用，開発，ガイダンス文章，ライフサイクル，テスト，脆弱性分析，等について書かれており，保証レベルを７段階に規定している。

３．セキュリティ評価に合格するためのプロセス

３．１　セキュリティ基本設計書の作成

個々の評価対象単位毎に「セキュリティ基本設計書」（Security Target）を作成し，最低限必要なセキュリティ事項を規定する。その作成プロセスは以下の通りである。

まず保護対象コンピュータ資源を特定し，保護対象に対する脅威を分析する。次に，脅威に対するセキュリティ方針を決定し，対策方針実現のためのセキュリティ要件について抽出を行う。そして要件を満足する機能使用及び開発手法を決定し，最後に検証を行うこととなっている。

３．２　機能要件

第２部「セキュリティ機能要件」では，評価対象の機能要件を表している。その概要は以下の通りである。

１．セキュリティ監査：監査データの収集，収集データの内容・タイミング，及びデータ分析についての要件。

２．暗号サポート：暗号鍵管理及び暗号操作についての要件。

３．ユーザデータ保護（アクセス管理）：利用者とアクセス権限（規則，操作，許可／禁止）と資源（利用最小単位）の管理ルールに関する要件。

４．識別と認証：ユーザ認証と識別に関する要件。

５．セキュリティ管理：セキュリティ属性管理，属性の解除，属性の期限切れに関する要件。

６．セキュリティ機能の保護：フェールセキュア，ドメイン分離，タイムスタンプの要件。

３．３　保証要件

第３部「セキュリティ保証要件」では，評価対象の保証要件を表している。その概要は以下の通りである。

１．構成管理：自動管理ツールによるソースコード／オブジェクトコードの管理，設計書，テスト関連ドキュメント，マニュアルのログ管理の要件。

２．開発：セキュリティポリシーモデルの完備（機能との関連，規則／特徴，無矛盾性／完全性）に関する要件。

３．ガイダンス：システム管理者向け（安全な運用方法）ユーザ向け（安全な利用方法）の要件。

４．テスト：テストドキュメントの完備（計画，手順，期待効果，実施結果），機能テスト，独立テスト，インターフェーステストの実施要件。

５．脆弱性評価：利用環境分析からの対策の完備性，セキュリティ機能の強度分析の実施，侵入テストの実施，脆弱性分析と評価に関する要件。

脆弱性評価の方法について：内在のセキュリティ問題が運用では問題とならないことを侵入テストを実施して確認する。一つは誤使用についての分析で，関連するハード／ソフトの動作異常，運用上の操作ミス，利用者のミス，システム構成上のミス，などによって正常に動作しない場合への対応を確認する。次に暗号秘密鍵やパスワードなどの秘密情報の強度の十分性を確認する。

６．ライフサイクルサポート：設計や作成時の物理・運用・人の管理，障害修正管理の要件。

３．４　セキュリティ評価

最終的には下記の項目について評価を行いレベルが決められる。

１．セキュリティ基本設計書評価

２．開発評価

３．脆弱性分析評価

４．ガイダンス文章

５．構成管理評価

６．配布と運用評価

７．ライフサイクル評価

８．保守評価

３．５　ISO 15408適用に際しての注意点

ISO 15408は合理的な安全対策の実施が可能になるという点で評価できるが，この基準を適用するに際しては，以下の点に十分な注意を払わねばならない。

一つには，ISO 15408はこれらの製品やシステムが評価の対象であり，ISO9000やISO14000のように組織を評価するための基準ではない点である。即ち認証を受けた商品やシステムであってもその使用や運営については各組織体で十分な管理体制を構築することが必要である。このことは，個別の製品やシステムについてのセキュリティは確保できていてもシステム全体としてのセキュリティレベルが確保できていることを保証するものではない。セキュリティ機能を適切に維持していくためには一定レベル以上の組織的な対応が不可欠である。

次に，安本 哲之助[1)]がいうように機能要件の中で「セキュリティ監査」機能がうたわれているが，ここでいう「セキュリティ監査」は監査データの収集，収集データの内容・タイミング，データ分析であって，システム監査でいう安全性監査とは異なる機能であることに留意が必要である。

アクセス制御については，外部からの侵入テストは規定されているが，内部の者の犯行については考慮されていない。これは，ISO 15408が組織や運営を認定するものではないので当然のことではあるが，実際の運営に際しては十分な留意が必要であり，システム監査等で定期的に信頼性を確認することが望まれる。

また，地震や水害・火災など自然災害等に対しても保証しているものではない。セキュリティ全体の中でISO 15408を適用できる場面は限られた分野であると認識をすることが大切である。即ちまず全体のセキュリティポリシーを確立し，その中でISO 15408を適用できる部分を明確にし，安全対策を含めた運用レベルの対策実施が必要である。

４．セキュリティポリシーのあり方

広義のセキュリティは，コンピュータセキュリティやネットワークセキュリティに限らず，組織の各種設備や人的資源，情報資源を含む全資産に対する保全行為，安全運用を指す。従って，本来情報セキュリティポリシーやネットワークセキュリティは，組織資産全体のセキュリティ方針である「コーポレイトセキュリティポリシー」のサブポリシーとして位置づけられるべきものである。セキュリティポリシーは，利用者個人の裁量で情報セキュリティについて判断されることがないようにと定められた，組織全体としてのセキュリティに対する基本方針のことをいう。

セキュリティといっても，組織全体のセキュリティ，次に部門単位のセキュリティ，そしてコンピュータシステム単体のセキュリティというように様々なレベルがある。本論文で言うセキュリティポリシーとは，図１．１で言う Computer Network について，組織全体のセキュリティについて共通の価値観を持つために定めるためのものである。部門単位やコンピュータシステム単体でのセキュリティについては，セキュリティガイドラインやセキュリティ管理規定などと呼ばれるもので規定されるべきものである。セキュリティの組織化については，全社レベルのセキュリティを管理するグループ，部門単位でのセキュリティを管理するグループ，といったように範囲と責任を明確にし，組織全体として統制の取れたセキュリティを確保することが望まれる。

セキュリティポリシーの目的は次の３つに集約される。

１．機密性（Confidentiality）の確保：情報漏洩の防止

２．一貫性（Integrity）の確保：情報改ざんの防止

３．可用性（Availability）の確保：情報の積極的活用の場の提供

セキュリティポリシーには詳細な技術的項目は含めずに，普遍的な考え方について記述することが望ましい。セキュリティポリシーに類するものとしてセキュリティガイドラインやセキュリティ管理規定等と呼ばれるものがあるが，セキュリティポリシーが最上位に位置する。

セキュリティ対策については通常は発生費用のみに目が行きがちであるが，一旦，事件や事故が発生すればセキュリティ対策はどうなっていたのかと問題になる。しかし，セキュリティ対策は費用対効果が把握しにくいこともあり，その必要性は認識されていても，実際の対策についてどのレベルまで実施すべきかが理解されていないことが多い。このよ

うな場合，ISO 15408 は国際的な標準として企業が最低限実施すべき対策を決める指針となる。

今後は，国際的な企業間ネットワークに接続する際に，セキュリティ認定を受けていることが条件になる可能性もある。あらかじめISO 15408 やガイドラインに基づいてシステム企画や設計を行っておけば，セキュリティ認定に適合できるシステムを構築することができる。ユーザーは評価対象の製品またはシステムがそれぞれのセキュリティニーズを満たしているかどうかを判定する一助として，また，様々な製品またはシステムを比較する場合に評価結果を用いることができる。次に，運用段階でもISO 15408 のチェックポイントを利用すれば効果的にセキュリティ対策を実施することが可能になる。

しかし，ISO 15408は情報技術を用いた製品やシステムのセキュリティ機能を対象としており，ISO9000やISO14000のように組織を評価するための基準ではないし，管理者による犯行に対しては考慮されていないことを認識しておくべきである。

日本では田舎にいけば家に鍵はなかった。小さな島では泥棒の侵入など考えてもいなかった。我が国においても近年はナイフ等による殺傷事件が増加してきているが，米国では古くから安全のためには一般市民が拳銃を持つことが必要と考えられている。セキュリティ意識は国や社会の風土に大きく影響される。ナイフや拳銃が人を殺傷する武器であることは認識されているが，インターネットの普及により情報技術（ＩＴ）が人の心を傷つけ企業システムを混乱させる武器となり得るとの認識は薄い。

インターネットが発達した今日，現実には様々な新しいリスクが発生し始めており，社内だけ，日本国内だけでは十分なセキュリティを確保できない状況になってきている。欧米諸国では，既に法的制度化も着々と進み，自主規制のガイドラインもできつつある。日本においても，ISOによる標準化の動向をいち早く捉え，各企業や自治体において速やかに適切なセキュリティ対策を実施することが望まれている。

セキュリティー機能を維持するには組織的な対応が不可欠であり，自然災害などを含む安全対策に充分な注意を払い，システム監査などを含めた総合的な対策実施が重要である。

ある日突然，重要な情報システムが使用不能に陥ることも考えられる。企業のトップ自らがその重要性を認識し，継続的に着実な対策をとることが望まれており「セキュリティポリシー」の策定がその第一歩である。

参 考 文 献

１）安本 哲之助 「経営情報システムの安全性に関する国際セキュリティ評価基準の適用の効果と限界」p. ３ システム監査学会近畿地区研究会資料（1999.7.24）

２）田淵 治樹 「国際セキュリティ評価基準－ISO 15408のすべて」日経ＢＰ（1999）

３）田淵 治樹「国際セキュリティ評価基準の意義」ISACA大阪支部研究会資料（1999.6.5）

４）田淵 治樹「セキュリティ国際標準の活用法」日経コミュニケーション（1998.4.20）

５）松田 貴典 著 「情報システムの脆弱性」白桃書房（1999）

６）Common Criteria V2.0（Final Committee Draft）
http://csrc.nist.gov/cc/ccv20/ccv2list.html

７）情報システムコントロール協会 Control Community 編集委
「コントロール・コミュニティ」Vol. ３ （1998.6）

８）岡田 仁志 「個人データ保護の立法政策」電子情報通信学会発表資料（1998.5.28）

９）金融情報システム安全対策部「ネットワークセキュリティについて」No.200 (1998.4)

10）金融情報システム安全対策部「セキュリティポリシーについて」No.193 (1997.11)

11）安全対策に関する情報開示研究会報告書の参考資料「米国における金融情報システムに関する安全対策実施状況の情報開示に対する考え方」金融情報システム N0.202 (1998.6)

12）日本情報処理開発協会「情報化白書１９９８」コンピュータエージ社（1998）

13）日本情報処理開発協会「情報化白書１９９９」コンピュータエージ社（1999）

14）Barbara Y. Fraser 宮川 寧夫 訳「サイトセキュリティハンドブック」(1997)

第６章　終 章

１．まとめ

本論文では，第一章で情報資産保護の歴史について論述し，情報資産保護の重要性が高まることを示した。

第二章では，ウィルスの現状について，ウィルス被害届出件数が2000年には新たなウィルスの出現により過去最高となり，多数の被害届が出されている現状を分析した。マクロウィルスの脅威に加えて，従来型ウィルスにより，次々に覆されてきた「ウィルスに関する従来の常識」の分析を行った。その結果，ネットワークを利用したメール自動送信型ウィルスの危険性について言及した。

インターネットが社会のインフラとなっている現在では，ウィルス対策は民間企業としての問題だけではなく，国家としての問題となりつつあることを示した。そして，新たなウィルス対策のあり方と今後の方向性について考察を行った。

第三章では，不正アクセスの現状について把握し，2000年４－６月および７－９月における日本での不正アクセス急増の原因が，日本語対応の不正アクセスツールの開発によるもので，日本においても今後ますます不正アクセスが増加する危険性について言及した。

そして，具体的な侵入方法についての分析を行い，グローバル企業における不正アクセスのモデル分析を元に，不正アクセスに対する具体的対策についての考察を行った。

第四章では，ライセンスマネジメントについての重要性について言及し，違法コピーの現状について分析を行い，ソフトウェアの違法コピーと防止活動についてまとめた。そして，ＴＣＯ削減の観点からのシステム監査を実施することにより，ライセンスマネジメントにおいて大幅なコストダウンが図れることを事例で示した。

第五章では，セキュリティについて世界標準化の動向と日本の現状について論述し，セキュリティ評価の国際標準であるISO 15408について分析し，その適用に際しての問題点を整理し，セキュリティポリシーのあり方について考察を行った。

以上，見てきたように情報資産保護はもはや，一企業だけの問題として捉えるべきではなく，情報システムのあり方を含め，社会全体として対策を検討すべきテーマでもある。

次に，情報資産保護の今後の方向性について述べた後，情報資産保護レベル向上のための政策提言について述べる。

２．情報資産保護の今後の方向性

第１章 第２節 「情報資産保護の歴史」 で見てきたように，戦略情報システムより前，即ち1980年台までは，集中処理で効率化を図っていたが，1990年頃から現在までは，ＬＡＮ環境が整備され，各人がパソコンで様々な処理を行うという分散方式で処理を行ってきた。今後の方向性としては，現在パソコンで処理している内容をすべてサーバーで処理し，パソコン側はブラウザーだけがあれば処理できるようになるであろう。いわゆるシンクライアント方式である。

近い将来，ネットワークコストは大幅に低下し，大量のデータ伝送が可能となり，３次元ＣＡＤＡＭなど大容量のデータをリアルタイムで受信する場合などを除いて，ネットワークスピードは大きな問題とはならなくなるであろう。シンクライアント方式により，データは全てサーバー側で保存管理され，バックアップも確保され，安全性についても大きく向上するであろう。

シンクライアント方式では，ウィルスチェック用ソフトもサーバー側でチェックするだけで可能となるばかりでなく，パターンファイル更新もサーバーだけで済むこととなる。

ライセンス管理についても，サーバー側に全てのソフトウェアを準備しているので容易に管理ができようになり，ソフトウェアのバージョンアップについても，サーバー側だけで済むので大きな効率化につながるとともに，新しいソフトウェアの導入が容易となる。

ライセンスについては，今後は「購入」という形態ばかりでなく，「レンタル方式」といった形態が増加するであろう。マイクロソフト社では，従来のセレクト契約に加えて，ＥＳＬ契約（Enterprise Subscription Agreement Licence）と呼ばれる，ソフトウェアを年間レンタルする契約方式を新たに提案している。これは，企業グループ単位で，必要な台数分を１年間レンタルする方式で，契約した台数よりも実際に使用する台数が増加した場合は，従来の台数分に加えて追加台数分のレンタル費用を加算して支払う方式である。米国においては，ＷＯＲＤやＥＸＣＥＬＬなどのソフトウェアについても，週単位や月単位でのレンタル方式で貸し出す企業（サイト）も出てきている[62]。

例えば，新規にプロジェクトを立ち上げた場合，必要な期間，必要なユーザー分だけソフトウェアをレンタルすることが可能となる。それも，ユーザー側（クライアント側）は

---

[62] http://www.personable.com/ を参照

ＷＥＢ用ブラウザーさえあれば事足りて，必要なアプリケーションは全てサーバー側で準備されワークスペースもサーバ側に確保されている。現在のように買取りの場合は，不要となったライセンスを必要としている他のパソコンに移し替えれば良いのだが，実際問題としては，あまり活用されていない例が多い。また，他の職場で利用するとなるとバージョンが異なるなど，利用する場合の問題点も発生する。

シンクライアント方式のパソコンについては，現状では市場にコストパフォーマンスの良いマシンが登場していないこと，及びコスト面でネットワーク環境が整備されていないことなどの理由で普及が遅れているが，今後，急速に導入する企業が増加する可能性が高い。

３．セキュリティレベル向上のための政策提言

筆者は情報資産保護を推進する上で以下のことを提言する。これらの政策実行により日本におけるセキュリティレベルは確実に向上するであろう。

３．１　ネットワークの公衆衛生としてのセキュリティ減税

ウィルス被害は2000年10月・11月・12月の3ヶ月間，連続して過去最高の被害届出件数を更新した。ネットワークがグローバル化し，日本においても2000年になって不正アクセス件数が急激に増加しており，ハッカーなどネットワーク犯罪が今後急速に増加するのではないかと危惧される。それに伴い，ネットワーク犯罪による社会的損失は今後益々増加すると思われる。

インターネットが社会のインフラとして定着しつつある現在では，国家としてネットワークの安全性を確保するための対策を検討し，早急に実施すべきである。その際，参考とすべきものが，伝染病など病原体のウィルスを駆除するために取られた公衆衛生的な視点での国家的対策である。コンピュータウィルス対策についても同様の対策を実施することにより経済的効果を上げることが可能であろう。すなわち，ネットワークについても公衆衛生的な視点での対策実施が必要であると考えている。

悪意をもって作成されたプログラムがコンピュータウィルスと呼ばれて久しいが，この

コンピュータウィルスというネーミングは実にその動きを如実に表していると言える。病原体であるウィルスと，プログラムであるコンピュータウィルスとは，まったく異なるものであるにもかかわらず実に共通点が多い。病原体のウィルスと同様に，多くのコンピュータウィルスにも感染・潜伏・発病の状態がある。インフルエンザウィルスのように，感染力は強いが発病時の被害は比較的小さい場合が多いコンピュータウィルスとしては，ラルーやメリッサおよびラブレターウィルス等があげられるであろう。メリッサやラブレターウィルスは発病時の被害は大きくはないが，あまりに感染力が強く，ワクチンソフトの配布が遅れてしまったため，サーバー停止などによる被害が発生した例といえる。エイズウィルスに似て感染力はさほど強くないが発病時の被害が大きいものとしては，マトリックスウィルスなどがあげられる。このウィルスに感染すると駆除するためのパターンファイルをホームページからインストールことができなくなり，結果的にＯＳの再インストールが必要になるケースが多く，バックアップを確保していない場合はすべての情報が消えることもあり，被害は甚大である。

まったく新しいウィルスよりも，従来あるコンピュータウィルスが変化して新たなコンピュータウィルスができる場合が多いことなども，病原体のウィルスと似ている。多くのコンピュータウィルスは，過去に発見されたウィルスのロジックを参考にして，新たな機能が追加されて新種のウィルスが作られている。メリッサやラブレター，マトリックスウィルス等に見られたように，従来にない強い感染力や破壊力を持ったウィルスも現れるが，これらのウィルスもまったく新しいというよりは従来の技術と人間心理をたくみに利用したウィルスであるといえる。

インフルエンザウィルスに感染しないためには，出来るだけ人の多いところに出かけないこと，時々うがいをすることなどであろう。これをコンピュータウィルスに適用すると，できるだけ危険なサイトは出かけないこと（見ないこと），週に一度はワクチンのパターンファイルを更新すること，と言い替えられる。しかも，一度感染してしまったら，今度は自分が感染源となって，知らない間に他人に感染させてしまうところも病原体のウィルスと類似している。

このように病原体のウィルスとコンピュータウィルスとは非常に共通点があり，コンピュータウィルス対策の一つのアプローチとして，公衆衛生的なアプローチは有効となるであろう。唯一異なる点は，コンピュータウィルスは人間が作り出したものであるので，法律によってこのような悪意のあるプログラム作成者を厳罰に処することであろう。しかし，

現実にはネットワークの安全性はすでに大きく脅かされており，法律だけでの対策では不十分であり，セキュリティ減税などを含めた総合的な対策が必要となる。その際に参考となるのが公衆衛生的なアプローチである。

「保険医療プログラムの経済的評価法」[1)] の著者である武藤 孝司はその著書の中で「経済的評価の対象となる保険医療プログラム」として予防のステージ毎に以下の項目を掲げている。（表５．１ 参照）

表 ５．１ 経済的評価の対象となる保険医療プログラム

予防のステージ	プログラム		
	大分類	中分類	小分類
１次予防	健康教育プログラム		禁煙，エイズ教育
２次予防	スクリーニングプログラム	診断手技・機器	乳がん検診 胃がん検診
３次予防	診断プログラム 治療プログラム	診断手技・機器 内科的治療 外科的治療 患者教育プログラム	ＣＴ，ＭＲＩ， 超音波検査， 高血圧， 高コレステロール， 冠動脈バイパス手術， 糖尿病
４次予防	リハビリテーションプログラム		脳卒中リハビリテーション

この考え方を筆者がコンピュータウィルスに適用したものが，表 ５．２ 「経済的評価の対象となるネットワークの安全性プログラム」である。このようにコンピュータウィルスに対しても病原体のウィルス対策と同じようなレベルでの対策が有効であり，そのアプローチ方法は参考となる。すなわち企業や学校においてもネットワークの安全性の教育が必要であり，個人がワクチンソフト無しでインターネットに接続することがいかに危険なことであるかを教えることが必要である。また，たとえワクチンソフトを利用していても，古いバージョンのままでは新たなウィルスは発見できないということを十分に教育すべきである。

表 5．2 経済的評価の対象となるネットワークの安全性プログラム

予防のステージ	プログラム		
	大分類	中分類	小分類
１次予防	ネットワーク教育プログラム	バックアップの確保	不信なメールはクリックしない・怪しげなサイトにはアクセスしないなどのコンピュータウィルス対策教育およびハッカー対策教育
２次予防	スクリーニングプログラム	防衛対策及び発見方法	ワクチン，ウィルスウォール，ファイアーウォールの必要性教育及びそれらの使用方法と留意点
３次予防	診断プログラム 治療プログラム	発見用及び駆除用ソフトの利用	ワクチン，ウィルスウォール，ファイアーウォールによる発見及び駆除
４次予防	リハビリテーションプログラム	バックアップによる回復	不幸にしてシステムやデータが破壊された場合には，バックアップから再インストールを行う なぜ被害に遭ったかを分析し反省する

「日本医師会雑誌（小特集・予防接種）」[2)]で武内 可尚が，インフルエンザワクチンの経済的効果について分析している。その中で多くの諸外国においては，ワクチン投与の費用負担については国又は社会保険が負担している現状を示すとともに，日本においてもワクチン投与が結果的に医療費抑制につながるということを，川崎市立川崎病院小児科のレセプトを元に分析している。筆者はインフルエンザワクチンの経済的有効性と，コンピュータウィルスの経済的有効性を同義に論ずることが出来ないことは十分に理解している。

しかし，ワクチンソフトやファイアーウォールを購入することにより，ネットワークの安全性を高める努力をしている個人や企業に対しては税制面で優遇し，結果的に社会全体としての経済的効果を高めることが有効となるであろう。

経済的分析を始めるときにチェックすべき事項として，武藤 孝司は以下の事項を上げている。[3)]

１．誰がこの評価を必要としており，なぜ必要なのか

２．代替案をどのように選ぶか

３．提案された代替案の効果について，どのようなことが分かっているのか

４．対案された代替案にかかる費用と資金運用の見込みはどの程度判明しているのか

５．経済的評価をどのように行うか

日本におけるウィルス被害やハッカー被害については，データ破壊に伴う修復やウィルス駆除に要した直接的なコストだけでも大きなものになると推定されるが，現実にはそれらの基礎となる日本国内での被害金額が把握出来ていない。したがって，今回提言するコンピュータワクチンに関する減税についての経済性評価については今後の課題とし，本稿では提言のみを行うこととする。

平成１３年度予算として，文部省は「私学助成関係概算要求」で，「私立大学等研究設備整備等補助」の中で，２億１千万円を「セキュリティ対策分」として要求している。[4)] 大学におけるセキュリティ対策はまだ緒に就いたばかりであろうと推測され，人材の育成を含め，迅速な実施が望まれるところである。ネットワークはそれぞれが，安心して稼動して初めて効果を発揮するものであるが，グローバル化の進展に伴い，日本におけるハッカー脅威が日増しに増大しているにもかかわらず，一般企業の意識も低いのが実状である。

このような状況を鑑み，ネットワークセキュリティ対策費に対しての特別減税を実施する方法が考えられる。2000年12月現在，これに関連して実施中の減税としては，いわゆるパソコン減税とファイアーウォール減税がある。

いわゆるパソコン減税とは，企業が本体及び付属品の取得合計金額が100万円未満のパソコンを購入した場合，11年4月1日から13年3月31日までは，１年間での償却が可能となるものである。しかしこの特別減税は計画期間の終了と共に廃止される。

次に，いわゆるファイアーウォール減税が実施されている。これは本体及び付属品の取得合計金額が180万円以上のファイアーウォール製品を購入した場合は，12年4月1日から14年3月31日までは，1年間で取得価格の20%の特別償却ができるというものである。しか

し，この中にウィルスウォールは含まれていない。ウィルス技術を利用したハッキングツールが開発されている現在，ファイアーウォール製品ばかりでなくウィルスウォールについても減税対象に含めるべきであろう。次に，取得価格の20%の特別償却ではなく，１年間での全額特別償却を認めることが望まれる。それほどウィルス対策面での変化は激しいものがあり，税制面でのバックアップが必要である。

次に，インターネットサービスプロバイダーについては，顧客のメールの全てについてウィルスチェックを実施することが望まれる。各プロバイダー側でのウィルスチェックは，最新のパターンファイルに更新しておくことにより，マトリックスウィルスのように感染力が強く，発病時の被害が大きなウィルスについても各プロバイダー側でチェックすることが可能となる。ユーザーもウィルスチェックサービスのレベルが低いプロバイダーからは脱退するなどといったことが考えられ，ウィルス感染防止に大きな威力を発揮する。

インターネットサービスプロバイダーがウィルスウォールでチェックをするに際しては，ゲートウェイサーバーでチェックすることが必要となる。そのためのハードウェアやソフトウェアについては，１年間で償却できるように税制面で特別の配慮することが必要である。この政策によりウィルス被害は劇的に減少するであろう。

ウィルスウォールを含めたファイアーウォール減税により，一般企業におけるセキュリティ意識の高揚につながり，ネットワークに接続されている各企業がこぞってハッカーやウィルスに対して強いネットワークを構成しそれを維持すれば，ハッカー人口の減少も見込める。というのは，現在のネットワークではあまりに容易にハッキングができるので興味半分に実行しているハッカー[63]も相当数いると推定されるが，そういった興味半分のハッカーは，成功率があまりに低いと時間の無駄となり，ハッキングを止めることも期待できる。こういったハッカー予備軍を減少させることも大切なことである。

インターネットは国境の無いネットワークである。それにもかかわらず，日本国内でのセキュリティ減税はおかしいのではないかという意見もあるかもしれない。しかし，日本国内だけでも，以上の対策を実施すれば十分な効果が見込めるばかりでなく，結果的には世界中のネットワークのセキュリティレベルを向上させることにつながるであろう。

日本では安全と水はタダという風潮があったが，インターネットにより世界中につながったために，これからは自分の家には鍵をかけることが必要であり，企業も同様である。

---

[63] キッズハッカーなどと呼ばれており，インターネットからハッキングツールをダウンロードしてハッキングを楽しむ初心者ハッカーのこと

３．２　国家安全保証としてのセキュリティ対策と情報資産保護

国家安全保証の面で情報資産保護を考慮すると，ネットワークのグローバル化に伴い，サイバーテロの危険性が増大している。サイバーテロにより有効な情報を破壊するこことが可能となった現在，従来はミサイルなどの武力による攻撃が中心であったものが，これに加えて，ネットワークを利用したサイバーテロによる同時に攻撃を行なうことで，その効果は倍増する。

2000年10月，ハッカーがトロイの木馬を利用して，マイクロソフト社内の超機密データを盗み出した可能性について，ＦＢＩが調査に乗り出したことが明らかになった[64]。2000年１月の中央省庁の連続ホームページ改ざん事件により，日本国家のセキュリティレベルの低さを露呈したことからも分かるように，日本の中央省庁にトロイの木馬を送り込むことが大きな困難であるとは思われない。

現在の霞ヶ関は，省庁がそれぞれバラバラにセキュリティ対策を実施しているので，セキュリティレベルの低い省庁へは容易に侵入することが可能であろう。しかも，一旦霞ヶ関ＬＡＮに侵入すれば，そこから他の省庁への侵入は比較的容易になるであろう。というのは，省庁間でのデータ交換など，省庁間の情報流通を容易にするため，霞ヶ関ＬＡＮ内のセキュリティレベルは低く設定されていると推測され，また，霞ヶ関ＬＡＮのサーバー情報も比較的容易に入手できると想像される。[65]

もう一つ，重要な視点がある。従来は，国家でなければ国家は攻撃できなかった。しかし，現在は個人が国家を攻撃することが可能となっている。ミサイルは打ち込めなくても，サイバーテロは個人が実行することが可能な状況になってきている。例えば，一部の者が日本国家に戴して敵意を持ち，国家混乱を企てるとすれば，サイバーテロは被害が甚大となる可能性の高い手段の一つであろう。

このような状況をかんがみ，我が国においても，国家安全保証としてのセキュリティ対策と情報資産保護を真剣に検討すべきであるといえる。政府は，従来のようなミサイル攻撃に備えるばかりでなく，サイバーテロに備え，政官民すべてにおける情報資産保護につ

64　http://www.asahi.com/1027/news/business27020.html

65　縦割り行政の弊害（この場合は長所）で，他省庁のサーバー情報がほとんどない，という可能性も否定はできないが。

いても検討すべきである。ネットワーク社会の進展により，我々はネットワークなくしては社会生活を維持できなくなっている事実を認識し，それを守るための政策を検討すべきである。2000年１月の中央省庁ホームページ改ざん事件をサイバーテロの警鐘として真剣に受け止め，今後の政策を検討すべきである。

３．３　省庁横断的セキュリティ対策部門の設置

日本政府は，「平成12年１月に発生した一連の各省庁ホームページの改ざん事件によって，中央省庁におけるこれまでの情報セキュリティに関する取り組みが，必ずしも十分でないことが明らかになった」として，情報セキュリティ対策推進会議[66]が，2000年７月に「情報セキュリティポリシーに関するガイドライン」を策定した。各省庁はこのガイドラインをふまえ，2000年12月までに情報セキュリティポリシーを作成し，これに基づく総合的・体系的な情報セキュリティ対策を図ることになった。そして「２００３年（平成１５年）までに電子政府の基盤としてふさわしいセキュリティ水準を達成することを目標として計画的に必要な措置を順次講ずる」としている。[5)]

１月にハッカー侵入事件が発生して，その対策ガイドラインが作成されたのが７月で，その年の12月末までにセキュリティポリシーを策定して，３年後に「総合的・体系的な情報セキュリティ対策を図る」などという，そのようなスピードで良いのだろうか。それも，従来と同じ縦通しの組織毎にセキュリティポリシーを立案して本当に効率化を図った対応と言えるであろうか。

グローバル企業が子会社毎にセキュリティ対策を立案していればコストは膨らみ，子会社間での情報連携では不便な面が多発することとなり，通常は本社部門が基本的な枠組みを決定して実施に移すケースが大半であろうと考えられる。

日本政府においても，従来のような対応では，導入費用，運営費用共に大きなものとならざるをえない。また，対策立案についても各省庁が立案するので，セキュリティの専門家も分散されハイレベルの対策が実施出来ないのではと危惧される。

霞ヶ関ＬＡＮ等と言われているが，実際には各省庁毎にバラバラのセキュリティ対策状

66　官民における情報セキュリティ対策の推進を図るため，高度情報通信社会推進本部に設

態であり，今回の事件がそれを示している。この際，日本の各省庁をすべて束ねたセキュリティ対策室を立案できないものであろうか。それを実行に移すのは政治力である。セキュリティ対策を省庁毎に行う従来の方法を反省し，日本政府としての統合されたセキュリティ対策の実現を目指すべきである。

米国政府においては，すでにＣＩＡＯ（Critical Infrastructure Assurance Office : チャオ）と呼ばれる対策組織を作っている。この組織はインターネット犯罪に対して，現在のような縦割り組織では対応できないとして，各省庁の枠を超えた総合的な対策を練るために設置されたものである[67]。2000年１月，ＣＩＡＯがまとめた計画では ①各省庁に専門家を育成するために25億ドル　②ハッカーの侵入を検知するシステムに10億ドル ③現在のシステムの弱点分析に５億ドル ④研究所の設立に50億ドル の予算を計上している。我が国においてもこのような省庁横断的なサイバーテロ対応組織を早急に設立すべきである。

４．おわりに

本論文においては，情報資産の保護の観点から，ウィルス対策，不正アクセス，ライセンスマネジメント，およびセキュリティポリシーについて調査分析しそのあり方を研究し，最後に公共政策的な観点からの政策提言を行った。

情報資産保護は，知的財産権の保護や自らの資産を守るというだけでなく，ネットワーク社会を守るという大きな意義があり，公共政策の一環としてそのあり方を考えるべきであろう。情報セキュリティが弱い社会は即ち，脅威に弱い社会である。ネットワークセキュリティは企業だけの問題ではなく，国家政策としてのありようが問われていると言える。

ＩＴ革命が進展するにしたがって，情報資産保護の重要性は今後も益々増大する。今後ともこれらについての研究が活発に行われることを願うものである。

置された全省庁を構成員とする会議。議長は内閣官房副長官

[67] ＮＨＫ・ＢＳ１「見えざる敵・アメリカーサイバーテロの脅威」11月12日PM10-11放映

参 考 文 献

１）武藤 孝司 著『保険医療プログラムの経済的評価法』篠原出版 p. 2 (1998)

２）『日本医師会雑』第118巻・第6号 日本医師会 pp. 825-829 (1997.9.15)

３）武藤 孝司 著『保険医療プログラムの経済的評価法』篠原出版 p. 18 (1998)

４）平成12度 第14回 私立大学情報教育協会大会資料 pp. 10-12 (2000.9.19-21)

５）Contorl Community Vol.4 情報システムコントロール協会(ISACA) pp.33-64 (2000)