第5節の要旨

ブロードバンド、電子商取引、モバイルワークなど、情報通信の普及・高度化は利便性をもたらすだけでなく、情報セキュリティのリスクを増大させている。今日、情報通信にかかわるすべての者があらゆるリスクを想定した情報セキュリティの必要性と対策を認識する「セキュリティ文化」を早急に確立する必要性は高い。

第5節においては、情報セキュリティに対する意識や侵害事例の動向を概観した上で、個人及び企業の被害状況の把握と被害額の推計、情報セキュリティ対策の現状とその課題の分析を行う。また、情報通信セキュリティビジネスの動向、情報通信ネットワークの安全性・信頼性を脅かす事例、諸外国における対策を紹介する。

（情報セキュリティに対する意識と被害の状況）

○ インターネット等を利用する上で、情報セキュリティ対策が個人及び企業の双方にとって最大の課題となっている。また、使い勝手や利便性を犠牲にしてもセキュリティの確保を重視する個人、企業が半数を占めている。

○ 平成14年に約3割弱の個人（パソコン利用の場合）と4分の3の企業が情報セキュリティの被害に遭遇している。被害内容は、コンピュータウイルスによるものが最も多い。

○ 平成14年における我が国の個人ユーザの情報セキュリティ被害額は約400億円、企業の被害額は約3,500億円と推計される。

（情報セキュリティに関する対策と課題）

○ 個人では、3人に2人は何らかの情報セキュリティ対策を実施しているが、一部の利用者においては知識不足やメンテナンス不足によって情報セキュリティ対策が一時的なものにとどまっている可能性がある。

○ 企業は約98%とほとんどの企業で何らかの対策を実施しているが、対策の計画や実施に比べると、対策の効果・有効性の検証やセキュリティポリシー、対策等の見直しについては、実施できていないとする企業の割合が多い。

（情報セキュリティビジネスの動向）

○ 情報セキュリティビジネスの市場規模は、平成14年度（2002年度）の約4,600億円から平成19年度（2007年度）には約1兆9,000億円と約4倍に成長すると予想される。

（情報通信ネットワークの安全性・信頼性、諸外国における対策）

○ 平成15年1月にSQLスラマーが韓国等で過去最大規模のインターネット障害を引き起こすなど、情報通信ネットワークの安全性・信頼性を脅かす事例が発生している。

○ OECDは、2002年7月に「情報システム及びネットワークのセキュリティのためのガイドライン」を発表し、「セキュリティ文化」を提唱している。米国やEUでも情報セキュリティ対策を強化している。

1 情報セキュリティ確保の必要性

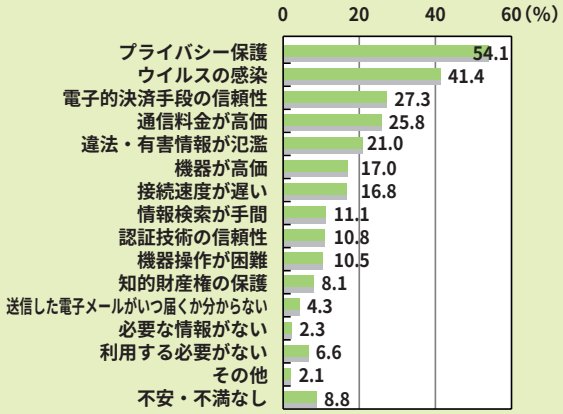
セキュリティ文化の定着が必要

インターネットや電子商取引等の情報通信の普及、ブロードバンドやモバイルワークといった情報通信の高度化は、利便性をもたらすだけでなく、情報セキュリティのリスクを増大させており、情報通信ネットワークを利用する上でセキュリティ対策が最大の課題となっている。個人がインターネットを利用する上で感じる不安・不満は、第1位が「プライバシー保護」（54.1%）であり、第2位が「ウイルスの感染」（41.4%）である（図表①）。企業の情報通信ネットワーク利用上の問題点では、第1位が「セキュリティ対策の確立が困難」（69.7%）、第2位が「ウイルス感染に不安」（63.6%）である（図表②）。また、利便性とセキュリティの優先度について、個人、企業のいずれにおいても「ある程度、使い勝手、利便性を犠牲にしてもセキュリティを重視する」割合が、半数程度を占めている（図表③、④）。

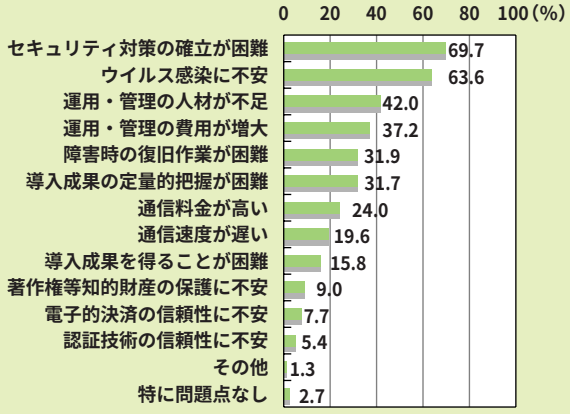
平成15年1月、韓国を中心に大規模なインターネット障害が発生し、市民生活に大きな影響を及ぼした（1-5-6(P127)参照）。この事件は、いくつかの事実を明らかにしている。第一に現代社会は情報通信ネットワークに大きく依存しており、これに障害があれば大きな社会的混乱が発生すること、第二に世界で最もブロードバンドが普及している韓国での被害が最も大きく、情報通信の進展が逆に大きな被害をもたらしたこと、第三に利用者が修正プログラムを導入することで被害は防げたはずであり、一般の被害者が自分の知らない間に大規模な事故の加害者になってしまうことである。

今後、情報通信の高度化により、情報セキュリティが侵害された場合の被害は更に甚大になる可能性がある。OECDが提唱しているように、情報通信にかかわるすべての者があらゆるリスクを想定した情報セキュリティの必要性と対応策を認識する「セキュリティ文化」を早急に定着させる必要性は高い（1-5-7(P129)参照）。

図表①　個人のインターネット利用における不安・不満（複数回答）

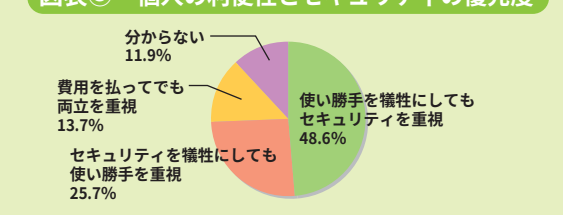


図表②　企業の情報通信ネットワーク利用における問題点（複数回答）

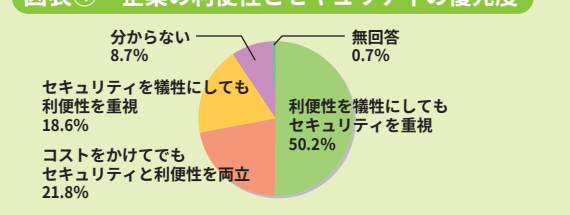


図表①、②　（出典）総務省「平成１４年通信利用動向調査」

図表③　個人の利便性とセキュリティの優先度



図表④　企業の利便性とセキュリティの優先度



図表③、④　（出典）「コンテンツとセキュリティに関する調査」（③はウェブ調査）

関連ページ ▶▶ 情報セキュリティ及びプライバシー保護対策の推進については、3-7-2（P279）参照

2 情報セキュリティ侵害等の動向

増加する情報セキュリティ侵害事例等

1 ウイルス

ウイルスによる被害発生件数について、ウイルス被害に関する届出を集計している2社(注)の発表した届出件数を合計すると、平成13年の37,622件から14年には74,001件の約2倍に増加している（図表①）。

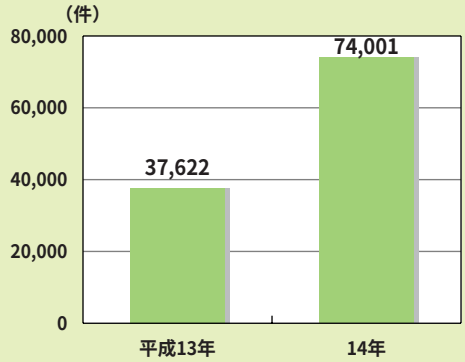
平成14年には、「Klez（クレズ）」、「Badtrans（バッドトランス）」等のワーム型ウイルス（ウイルスの一種で自己増殖する型のプログラム）が流行した（図表②）。また、感染したパソコンに保存されているアドレス帳等を使用して、送信者を詐称してウイルスを送りつけることで添付ファイルを開かせるなど、人の心理をついて感染するタイプのウイルスが多発した。

なお、ウイルスではないが、スパイウェアと呼ばれるプログラムが増加しつつある。これは、パソコン内のアクセス履歴等の個人情報を外部に送信するプログラムであるが、他のプログラムをインストールする際にパソコンに組み込まれ、利用している本人はその存在を十分認識していないことが多い。

2 不正アクセス

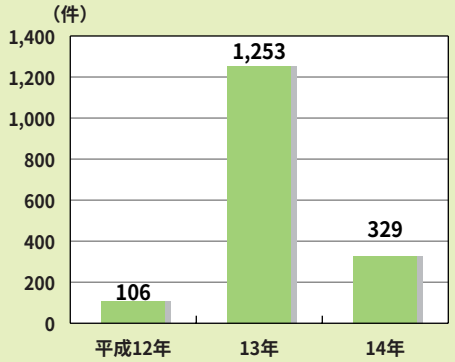
国家公安委員会・総務省・経済産業省の発表によると、平成14年における不正アクセス行為の認知件数は329件で、13年の1,253件と比べ924件の大幅減少となっている（図表③）。平成13年は、ホームページ書換プログラムによる、セキュリティホール攻撃型の事案が多発したが、最近の官民を挙げた広報活動や修正プログラムの普及等により平成14年は減少したものと考えられる。

図表①　ウイルスの届出件数の推移



シマンテック及びトレンドマイクロ資料により作成

図表③　不正アクセス行為の認知件数の推移



（出典）国家公安委員会・総務省・経済産業省報道資料

図表②　平成１４年に流行した主なウイルス

	ウイルス名	概　　要
1	Klez（クレズ）	ウェブ閲覧ソフトのセキュリティホールを悪用し、電子メールを開いたりプレビューしたりしただけで感染する。感染するとアドレス帳に登録されたメールアドレスに、自身を添付した電子メールを送信する。毎月6日に発病しハードディスクの一部のファイルを削除する
2	Badtrans（バッドトランス）	ウェブ閲覧ソフトのセキュリティホールを悪用し、電子メールを開いたりプレビューしたりしただけで感染する。感染すると未読の電子メールを探し、その返信として自身を添付した電子メールを送信する。感染したパソコンでのキー入力を記録し送信する機能があり、不正アクセスに利用されるおそれがある
3	Bugbear（バグベア）	ウェブ閲覧ソフトのセキュリティホールを悪用し、電子メールを開いたりプレビューしたりしただけで感染する。感染すると、自身を添付した電子メールを送信する。ネットワークで共有されているパソコンへの感染や、ウイルスチェックソフトの動作を終了させる、バックドア（不正侵入を行うための裏口）を仕掛けるといったことを行う
4	Nimda（ニムダ）	感染した電子メールのプレビューや、ホームページの閲覧、共有ファイル経由など、複数の感染経路を持つ。感染すると、感染を広げるためにランダムに他のコンピュータに攻撃を仕掛けるために、大量の通信を発生させ、ネットワークの混雑を生む
5	Frethem（フレゼム）	ウェブ閲覧ソフトのセキュリティホールを悪用し、電子メールをプレビューするだけで感染する。感染するとウイルスに含まれたIPアドレスへの接続を行う

（出典）「コンテンツ・セキュリティに関する調査」

（注）シマンテック及びトレンドマイクロのセキュリティセンター等へのコンピュータウイルスに関する被害の届け出件数（公表値）を合計している。届け出の内容、範囲等は事業者によって異なることに留意する必要がある

3 迷惑メール

利用者の同意を得ずに広告、宣伝、勧誘等を目的とした電子メールを送りつける、いわゆる迷惑メールが平成13年6月頃に急増し、携帯電話事業者等に寄せられた苦情・相談件数も急増した（図表④）。平成14年末に行った調査では、携帯インターネット利用者の58.0%とパソコンからのインターネット利用者の15.5%が過去1年間に迷惑メールを受け取っており、特に携帯インターネットでの被害率が高い（1-5-3(1)（P119）参照）。迷惑メールによって、電子メールの利用者はメールの配信が遅延するほか、希望しないメールの受信料を負担しなければならない場合がある。また、電気通信事業者は、設備増強等に関するコスト負担を強いられている。

迷惑メールの対策としては、平成14年7月に「特定電子メールの送信の適正化等に関する法律」及び「特定商取引に関する法律の一部を改正する法律」が施行されており、本法律の規定に違反した電子メール送信業者に対して警告メールを送信したり、措置命令を発出して是正を求めている。

4 インターネットの国際不正接続トラブル

インターネットの利用中に知らないうちに国際電話につながってしまい、高額の国際電話料金を請求されたというトラブルが問題になっている。これはダイアルアップ接続でインターネットを利用している際に、インターネット接続のアクセスポイントを自動的に変更するソフトが知らないうちにインストールされてしまうことによる。平成14年度に総務省の電気通信消費者相談センターに寄せられた苦情・相談等の件数は、2,209件となっている。また、国際電話会社にも多数の相談・苦情が寄せられている（図表⑤）。

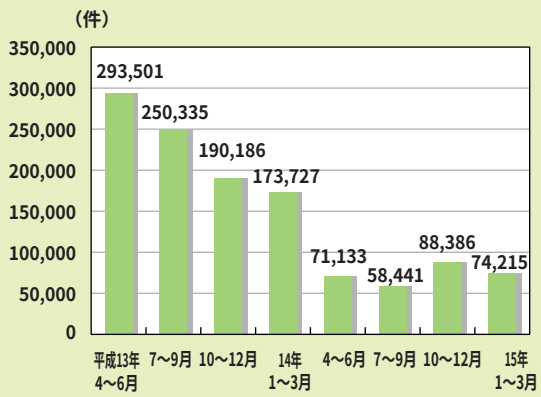
総務省及び国際電話会社では従来から注意喚起を行ってきたが、平成14年12月から国際電話会社各社は国際不正接続に関するトラブルが多発した国への通話制限を実施している。

5 ネットカフェのパソコンを悪用した犯罪

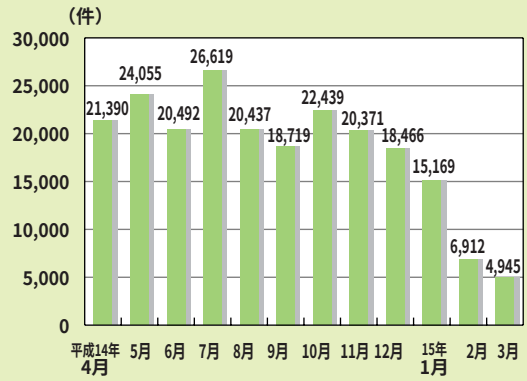
平成15年3月、他人になりすましてネットバンキングのサイトに不正アクセスし、多額の金銭を引き出すという犯罪が摘発された。ネットカフェのパソコンに、キーロガーと呼ばれるソフトを組み込んでおき、その後同じパソコンを使った別の利用者が打ち込んだ銀行口座番号とパスワードを盗み、他人になりすまして金銭を別の口座に移していた。

キーロガーとは、キーボードの入力等の操作状況を記録するプログラムであり、当初は企業において企業秘密の情報漏洩防止等のために、システム管理者がパソコンの利用状況を把握する際に利用されていた。本人の知らない間に操作状況を保存できる点を悪用したものである。

図表④　携帯電話・PHS事業者に寄せられた迷惑メールに関する苦情・相談等の件数の推移（迷惑メール対策の新サービスに関する相談等も含む）



図表⑤　国際電話会社5社に寄せられた国際不正接続に関する苦情・相談等の件数の推移



6 大規模システム障害の発生

（1）大手銀行の合併時のシステム障害

企業による情報通信ネットワークの利用が高度化し、情報システムが巨大化、複雑化する中で、大規模なシステム障害が発生している。平成14年4月、大手銀行の合併により新銀行が発足した際、システム障害により、ATM障害、口座振替処理の遅延等のトラブルが発生した。金融庁では、原因として、①システムテストや運用テストが適切に実施されていなかったなど、最低限必要な準備ができていなかったこと、②グループ内での報告・連絡体制に問題があり、十分なチェックが働かなかったこと、③大量の事務処理を支える事務インフラが不十分であったこと等を挙げている。また、このような準備ができなかった根本原因として、旧経営陣がシステム統合に係るリスクを十分認識していなかったことを指摘している。

（2）航空管制に関するシステム障害

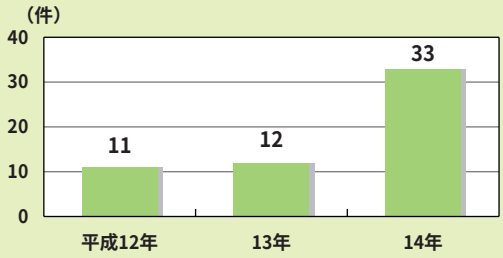
平成15年3月、国土交通省が管理しているFDP（Flight Data Processing System：飛行計画情報処理システム）に障害が発生した。FDPとは、フライトプラン、出発報等の情報をコンピュータで処理し、管制官に運行表等を自動的に配布するほか、他のシステムに対し飛行計画データを提供するシステムである。国土交通省では、今回のシステム障害は、FDPの一部のプログラム変更に伴い既存のプログラムとの間で不具合が生じたことにより発生したと発表している。また、直接的な原因はプログラムのミスであるが、受託会社の事前のチェックが不十分であったことも原因の一つであると指摘している。このシステム障害により、国際・国内線で205便が欠航し、30分以上遅延した便が1,462便あった。その影響は約30万人に及んだ。

7 個人情報の流出

個人情報のインターネット上への流出等のプライバシーの侵害事件が多発する中で、情報通信の発達によって個人情報が自分の知らない間に収集され、不正に使用されたり、流出するのではないかといった、プライバシーに関する不安が高まっている。プライバシーの保護は、インターネット利用者がインターネットを利用する際に感じる不安・不満で最大の事由となっている（1-5-1(P115)参照）。

新聞8紙の事故報道件数を集計すると、個人情報保護に関する事故件数は平成13年に12件であったものが、平成14年には33件に増加している（図表⑥）。しかしながら、企業における個人情報保護対策の実施状況では、「特に行っていない」企業が40.5%を占めている。また、実施している企業も「社内教育の充実」を行っている企業は23.9%、「必要な個人情報の絞り込み」を行っている企業は15.7%にとどまっている（図表⑦）。

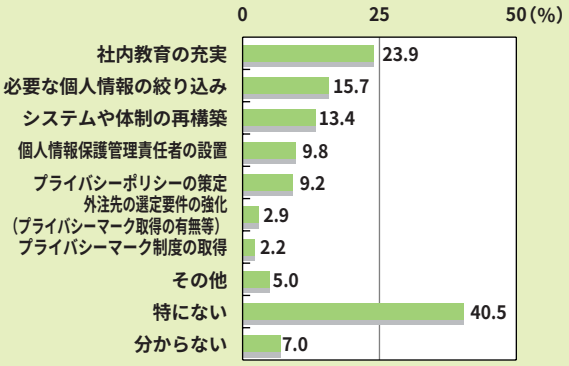
図表⑥　個人情報流出事故件数の推移（新聞8紙※の報道件数）



※　日経4紙、朝日、読売、毎日、産経の計8紙のデータベースにおいて、キーワードを設定の上調査した後、重複事件を削除した。使用キーワードは、（インターネットorホームページorメール）and（流出or漏洩or誤配信）and（情報or氏名or住所orアドレス）

（出典）「コンテンツ・セキュリティに関する調査」

図表⑦　企業における個人情報保護に関する取組（複数回答）



（出典）総務省「平成１４年通信利用動向調査」

関連ページ ▶▶ 電気通信事業分野の個人情報の保護については、3-7-2（3）（P280）参照

3 情報セキュリティ被害の状況
（1）個人の被害状況

パソコン利用者の3割弱、携帯利用者の6割弱が情報セキュリティ被害に遭遇

1 パソコンからのインターネット利用者における被害

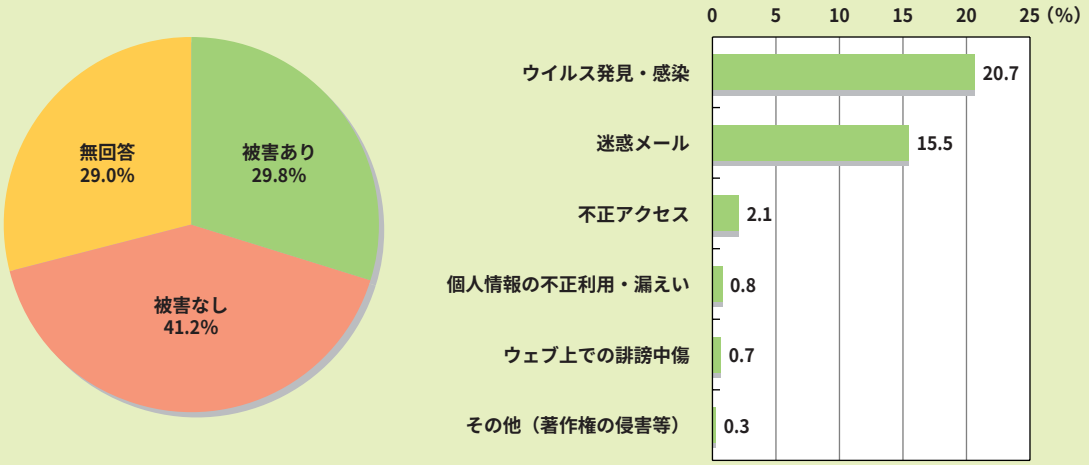
平成14年の1年間に情報セキュリティに関する被害を受けた者は、パソコンからのインターネット利用者のうち29.8%と3割弱を占める。被害の内容は、「ウイルス発見・感染」が最も多く、パソコンからのインターネット利用者のうち20.7%が被害を受けている。次いで、「迷惑メールを受信」が15.5%、「不正アクセス」が2.1%と続く。「個人情報の不正利用・漏えい」は、0.8%である（図表①）。

なお、ウイルスを発見しただけでなく、実際に感染した者は10.4%である。

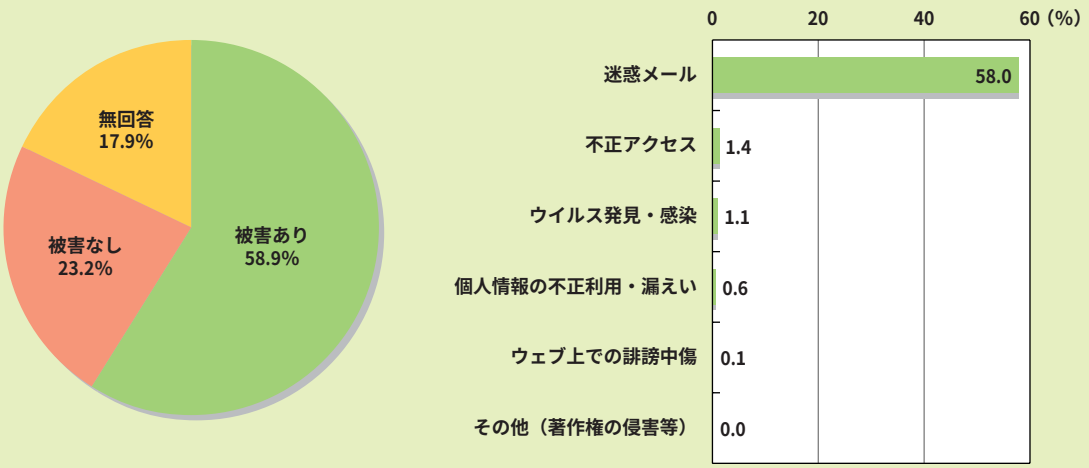
2 携帯インターネットの利用者における被害

平成14年の1年間に情報セキュリティに関する被害を受けた者は、携帯インターネット利用者のうち58.9%と6割弱を占める。受けた被害は「迷惑メール」がほとんどで、携帯インターネット利用者のうち、58.0%の利用者が被害にあっている（図表②）。

図表①　パソコンからのインターネット利用者における被害状況及び被害内容（複数回答）（過去1年間）



図表②　携帯インターネットの利用者における被害状況及び被害内容（複数回答）（過去1年間）



図表①、②　（出典）総務省「平成１４年通信利用動向調査」

3 情報セキュリティ被害の状況
（2）企業の被害状況

4分の3の企業が情報セキュリティ被害に遭遇

1 情報通信ネットワーク利用上の被害

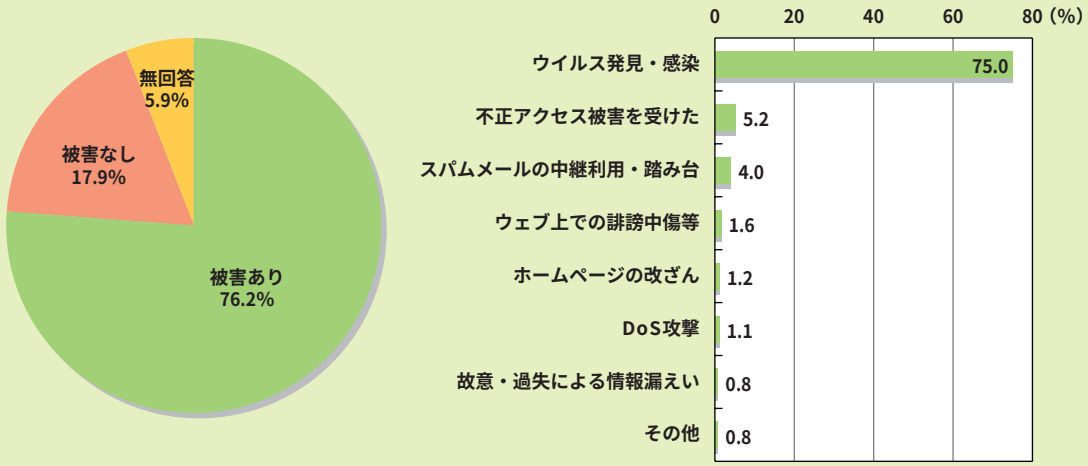
平成14年の1年間に情報通信ネットワーク（インターネットや企業通信網）の利用上、76.2%と約4分の3の企業が情報セキュリティに関する何らかの被害を受けている。被害内容は、「ウイルス発見・感染」が最も多く、企業全体のうち75.0%が被害を受けている。「不正アクセス被害を受けた」が5.2%、「スパムメールの中継利用・踏み台」が4.0%とこれに続いている。

なお、ウイルスを発見しただけでなく、実際にウイルスに感染した企業は、43.5%である。

2 内部者による被害

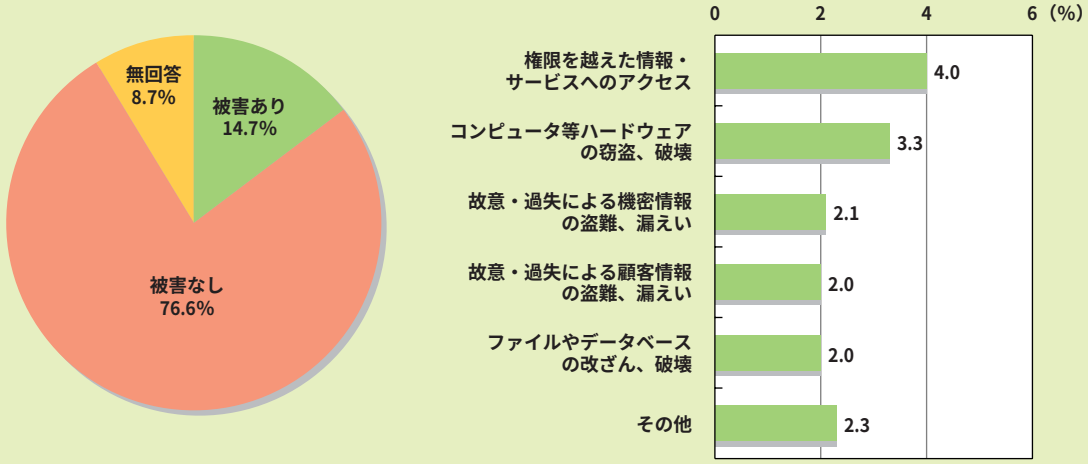
企業における情報セキュリティの脅威は、ウイルスや不正アクセス等、外部からに限らない。むしろ、内部者の故意あるいは過失による被害の方がリスクが高いとの指摘もある。そこで、内部者による被害について調査を行ったところ、内部者による情報セキュリティ関連の事件や事故が発生した企業は、14.7%であった(注)（図表②）。最も多いのは、「権限を越えた情報・サービスへのアクセス」で企業全体のうちの4.0%、次に「コンピュータ等ハードウェアの窃盗、破壊」が続く（図表②）。

図表①　平成１４年における企業の情報通信ネットワークの被害状況及び被害内容（複数回答）



（出典）総務省「平成１４年通信利用動向調査」

図表②　平成１４年における企業の内部要因による情報セキュリティ被害状況及び被害内容（複数回答）



（出典）「コンテンツ・セキュリティに関する調査」

（注）任意のアンケート調査であるため、実際の被害率より低い可能性がある

3 情報セキュリティ被害の状況
（3）個人及び企業の被害額推計

個人の被害額は400億円、企業の被害額は3,500億円

1 個人の被害額推計

平成14年において個人がウイルスと不正アクセスによって被った被害額を、被害率と被害額のサンプル調査結果に基づき推計すると、総額で約417億円である。このうち、「ウイルス」による被害額が約384億円、「不正アクセス」による被害額が約33億円である（図表①）。

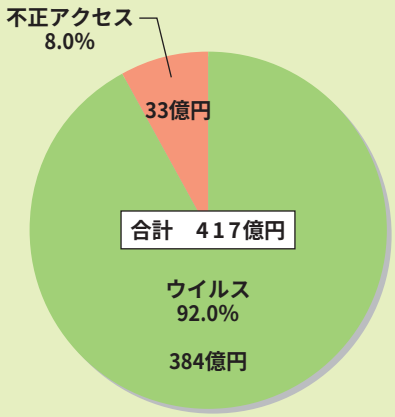
この被害額は、パソコンを対象としたウイルスと不正アクセスによる被害推計額の合計であり、ウェブ上での誹謗中傷や携帯電話による迷惑メール等による被害は含んでいない。また、故障したパソコンの修理や買い換え等のため実際に支出した金額のみを計上している。

2 我が国の企業の被害額推計

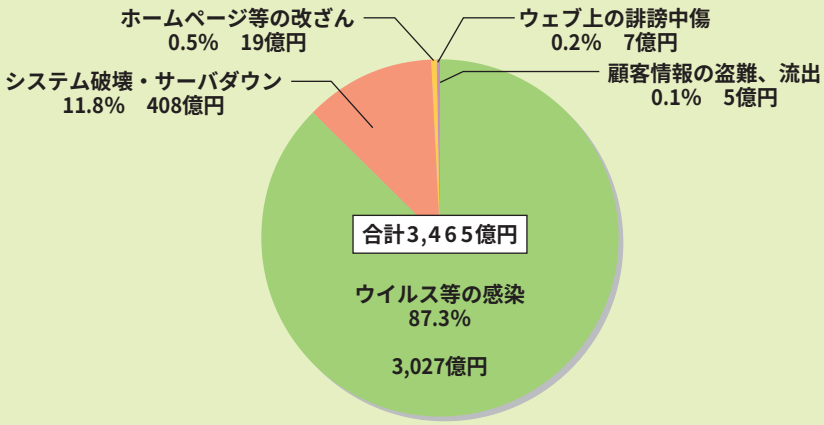
平成14年における企業の情報セキュリティ被害額を、被害率と被害額のサンプル調査結果に基づき推計すると、総額で約3,465億円である。内訳は、「ウイルス等の感染」による被害が最も多く約3,027億円であり、「システム破壊・サーバダウン」は約408億円、「ホームページ等の改ざん」は約19億円、「ウェブ上での誹謗中傷」は約7億円、「顧客情報の盗難・流出」は約5億円である（図表②）。

この被害額は、調査復旧費用及び逸失利益の被害のみを計上しており、風評被害による信用失墜等の被害額は含んでいない。

図表①　平成１４年における個人の情報セキュリティ被害額推計



図表②　平成１４年における企業の情報セキュリティ被害額推計



図表①、②　（出典）「コンテンツ・セキュリティに関する調査」

（注）個人の情報セキュリティ被害額の推計方法については、資料1-5-1（P348）参照
企業の情報セキュリティ被害額の推計方法については、資料1-5-2（P348）参照

4 情報セキュリティに関する対策と課題
（1）個人の対策と課題

知識不足等によりインターネット利用者の3分の1が情報セキュリティ対策を未実施

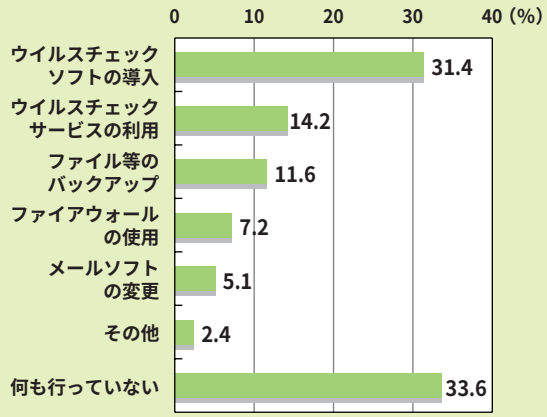
1 情報セキュリティ対策状況

インターネット利用者のウイルス・不正アクセス対策の実施率は、「ウイルスチェックソフトの導入」が31.4%と最も多く、「ウイルスチェックサービスの利用」が14.2%、「ファイル等のバックアップ」が11.6%とこれに続いている。しかしながら、「何も行っていない」者が33.6%と、約3分の1を占めている（図表①）。

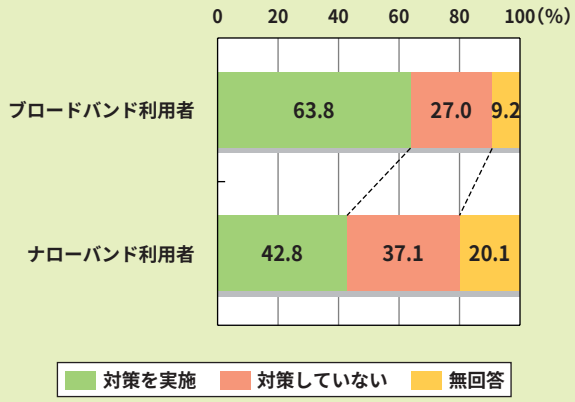
利用者の属性別には、接続回線別ではナローバンド利用者に比べ、ブロードバンド利用者の方が対策をとっている割合が高い。これは、ブロードバンド利用者は常時接続環境にあるため、外部からの攻撃を受けるリスクも高い分、情報セキュリティの意識が高いためと考えられる。ただし、ブロードバンド利用者においても対策を行っていない者は27.0%と4分の1以上となっている（図表②）。

このように、一定の割合で情報セキュリティ対策を実施していない者がいるが、情報セキュリティ対策を実施しない理由について調査したところ、情報セキュリティ対策未実施者のうち86.5%の者が「必要性は感じているが対策を行っていない」と回答している（図表③）。また、情報セキュリティ対策未実施者の65.3%が、「具体的な対策方法が分からないから」を未実施の理由として回答しており、今後、個人の情報セキュリティ対策を進めていく上で、情報セキュリティに関する知識の向上が課題となっている（図表④）。

図表①　インターネット利用者の情報セキュリティ対策の実施状況（複数回答）

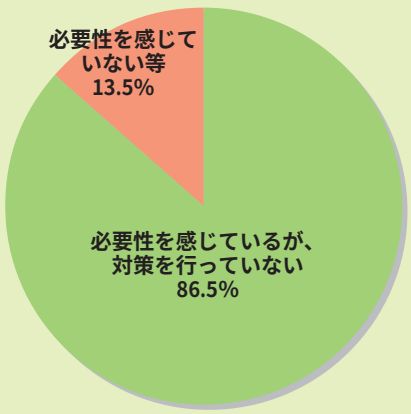


図表②　接続回線別の情報セキュリティ対策の実施状況

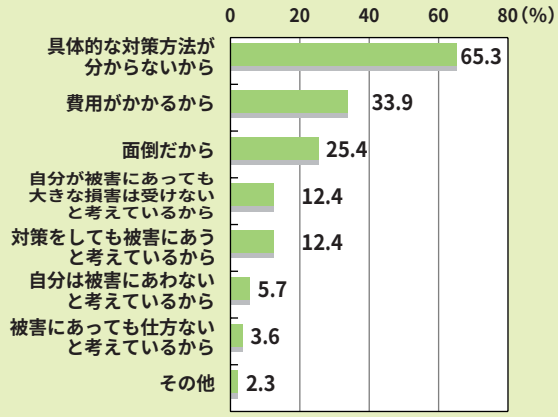


図表①、②　（出典）総務省「平成１４年情報通信利用動向調査」

図表③　情報セキュリティ対策未実施者の意識



図表④　情報セキュリティ対策に取り組まない理由（複数回答）



図表③、④　（出典）「コンテンツ・セキュリティに関する調査」（ウェブ調査）

2 情報セキュリティ対策への継続的な取組

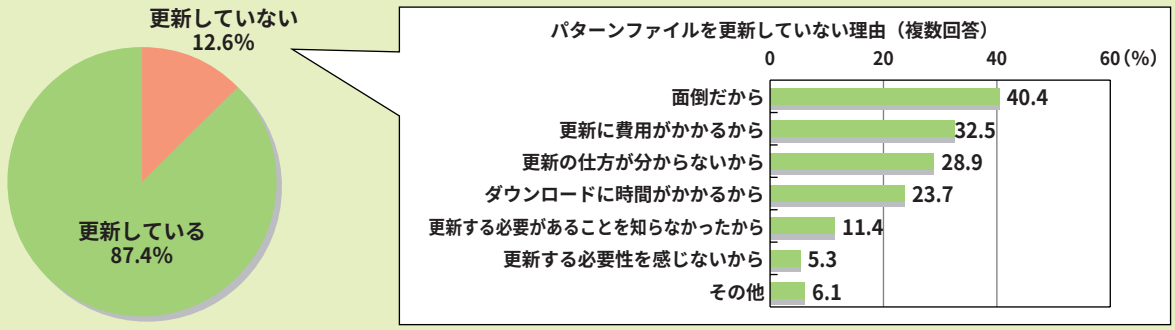
情報セキュリティを脅かすウイルスや不正アクセスの攻撃方法は常に変化しており、情報セキュリティ対策も、一度ソフトやハードを導入するだけでなく継続的に更新していく必要がある。例えば、ウイルスチェックソフトを導入した後も、パターンファイル（新しく発見されたウイルスの情報をアンチウイルスソフトに追加するための、更新情報を含んだファイル）を更新しなければ、日々新しく登場するウイルスの感染を防ぐことはできない。また、OS等へのセキュリティパッチ（セキュリティホールを修正するために、プログラムの一部分だけを書き換える修正プログラム）を適用しなければ、セキュリティホールを悪用した不正アクセスの危険にさらされる。

パターンファイルの更新状況について調査したところ、ウイルスチェックソフトの導入者のうち、87.4%はパターンファイルを更新しているが、12.6%はパターンファイルを更新していない。パターンファイルを更新していない理由としては、「面倒だから」とする者が40.4%と最も多い。その他、「更新の仕方が分からないから」を挙げる者も28.9%いる（図表⑤）。

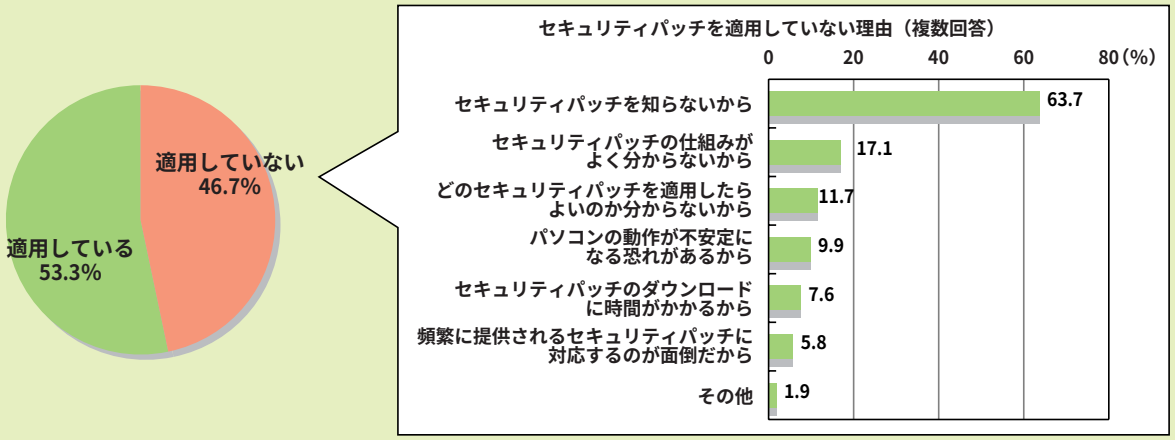
個人のセキュリティパッチの適用状況は、情報セキュリティ対策を実施している者のうちでも、適用している者が53.3%、適用していない者が46.7%であった。適用していない理由としては、「セキュリティパッチを知らない」が63.7%、「セキュリティパッチの仕組みがよく分からないから」が17.1%、「どのセキュリティパッチを適用したらよいのか分からない」が11.7%と、知識不足を理由として挙げる者が多い（図表⑥）。

このように、一部ではあるが、利用者の知識不足や日頃のメンテナンス不足によって情報セキュリティ対策が一時的なものにとどまっている。

図表⑤　個人のパターンファイルの更新状況と更新していない理由（ウイルスチェックソフトの導入者）



図表⑥　個人のセキュリティパッチの適用状況と適用していない理由（情報セキュリティ対策の実施者）



図表⑤、⑥　（出典）「コンテンツ・セキュリティに関する調査」（ウェブ調査）

4 情報セキュリティに関する対策と課題
（2）企業の対策と課題

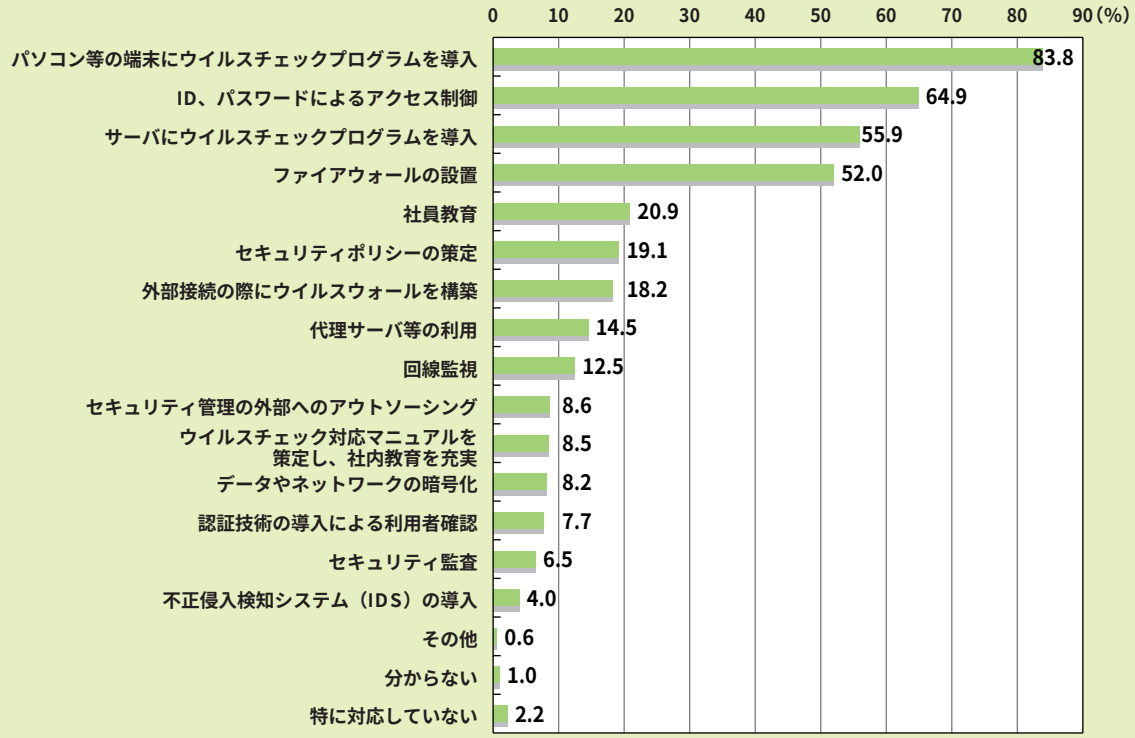
対策の効果の検証や対策の見直し等の充実が課題

1 情報セキュリティ対策状況

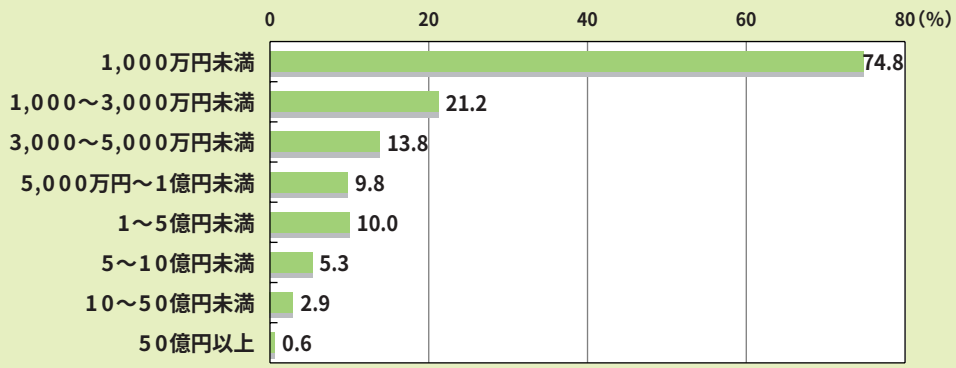
平成14年に企業が講じた情報セキュリティ対策状況としては、「パソコン等の端末にウイルスチェックプログラムを導入」が最も多く、83.8%の企業が実施している。「ファイアウォールの設置」は52.0%と、半数程度の企業が実施している。また、「特に対応していない」とする企業は2.2%にとどまり、ほとんどの企業で何らかの対策を実施している。

しかしながら、ハードやソフトの整備に比べると、情報セキュリティを組織的に確保する上で不可欠と考えられる「社員教育」や「セキュリティポリシーの策定」はそれぞれ20.9%、19.1%と5分の1程度であり、「セキュリティ監査」によって外部者に評価してもらっている企業も6.5%にとどまっている（図表①）。また、企業の規模別にみると、売上高の小さい企業では「特に対応していない」とする企業の率が高い（図表②）。

図表①　企業における情報セキュリティ対策状況（複数回答）



図表②　売上高別にみた情報セキュリティ未実施率



図表①、②　（出典）総務省「平成14年通信利用動向調査」

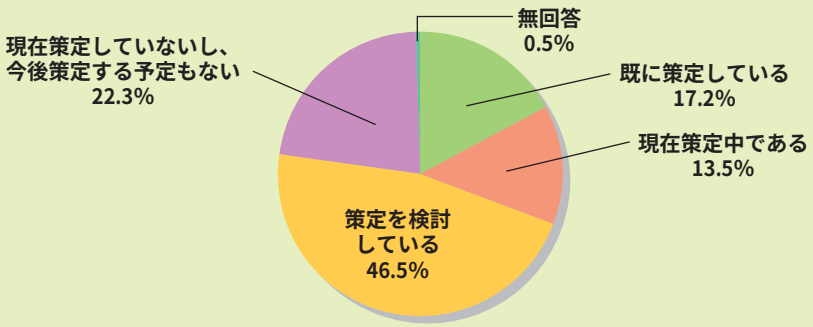
企業の危機管理に対する関心は深まっており、情報システムについて、万一の偶発事故等に備えた危機管理計画であるコンティンジェンシー・プラン(注)を既に策定している企業は17.2%であるが、策定中の企業、策定を検討している企業を加えると77.2%の企業が着手している（図表③）。

2 情報セキュリティマネジメント

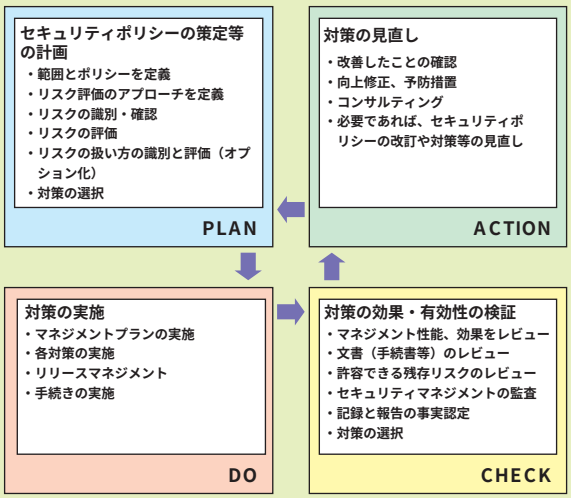
企業において情報セキュリティ対策が効果を発揮するには、情報セキュリティマネジメントとして、①セキュリティポリシーの策定等の計画（PLAN）、②対策の実施（DO）、③対策の効果・有効性の検証（CHECK）、④対策の見直し（ACTION）の4プロセスからなるPDCAサイクルを繰り返すことが必要である（図表④）。

サイクル段階毎の取組状況の自己評価について調査したところ、「おおむね実施できている」と評価する企業の比率は、実施（DO）については41.4%、計画（PLAN）については31.7%と比較的高い。これらに対し、検証（CHECK）は19.3%、見直し（ACTION）は13.9%にとどまっており低い（図表⑤）。今後、企業において情報セキュリティ対策を充実させていく上で、対策の効果の検証や対策の見直し等の充実が課題となっている。

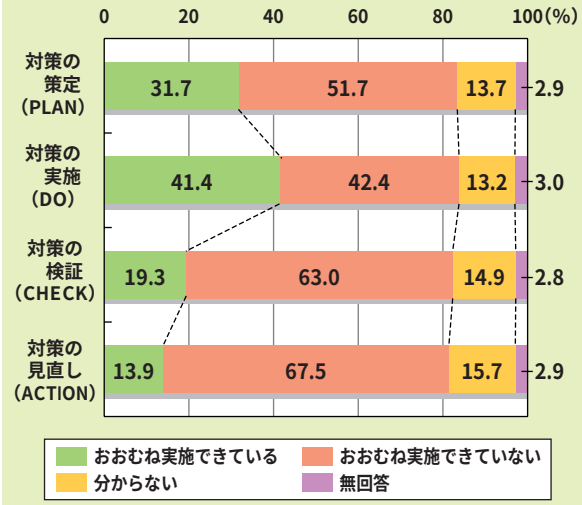
図表③　コンティンジェンシー・プランの策定状況



図表④　情報セキュリティマネジメント



図表⑤　情報セキュリティマネジメントサイクルへの取組評価



図表③～⑤　（出典）「コンテンツ・セキュリティに関する調査」

（注）コンティンジェンシー・プランとは、偶発事故や事故、不測の事態が発生した場合に、その損害を最小限に抑え、機能を迅速に復旧するための復旧計画、危機管理計画のこと

5 情報セキュリティビジネスの動向

情報セキュリティビジネス市場は2007年に1.9兆円に成長

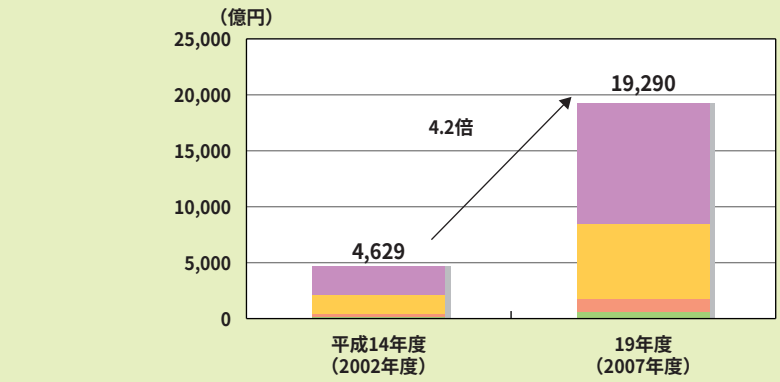
個人や企業が行う情報セキュリティ対策は、情報セキュリティ事業者が提供する機器やサービスを利用して行われることが多く、情報セキュリティビジネスは情報セキュリティを確保する上で重要な役割を果たしている。現在の情報セキュリティビジネスは、ウイルスチェックソフト等の製品提供、不正アクセス・ウイルスチェックサービス等を実施するサービス提供、セキュリティポリシーの策定やセキュリティシステムの設計を行うコンサルティング、セキュリティ監査等を行う評価に分類することが可能である（図表①）。

平成14年度における情報セキュリティビジネス市場規模を推計すると、4,629億円である。このうち、情報セキュリティ関連機器・ソフトの提供が2,595億円で全体の56.1%を占めている。次いで情報セキュリティサービスが1,618億円で35.0%を占めている。また、平成19年度（2007年度）の情報セキュリティビジネス市場規模をセキュリティ事業者の予測に基づき推計すると、1兆9,290億円と平成14年度の4.2倍に成長すると予想される（図表②）。

図表①　情報セキュリティビジネスの分類

分　類	概　要
情報セキュリティ関連製品提供	ウイルスチェックソフト、ファイアウォール、暗号関連製品、バイオメトリクス関連製品、IDS関連製品、ログ解析ツール、セキュリティ検査ツール、フィルタリングツール、セキュリティ運用管理ツール　等
情報セキュリティサービス提供	不正アクセス・ウイルスチェックサービス、電子認証サービス、ファイアウォール運用代行サービス、トラヒック監視サービス、時間情報保証サービス、データバックアップサービス、システム運用監視サービス、セキュリティ保険　等
セキュリティ確保のためのコンサルティング	セキュリティポリシー策定・コンサルティング、セキュリティシステム設計・構築、リスク評価（脆弱性検査等）、セキュリティ教育・訓練等
セキュリティの評価	セキュリティ監査、セキュリティ認証・認定　等

図表②　情報セキュリティビジネス市場規模の現状と予測



	平成14年度（2002年度）	19年度（2007年度）
情報セキュリティ関連製品提供	2,595	10,809
情報セキュリティサービス	1,618	6,764
コンサルティング	289	1,161
情報セキュリティ評価	127	556
計	4,629	19,290

図表①、②　（出典）「コンテンツ・セキュリティに関する調査」

（注）情報セキュリティビジネス市場規模の推計方法については、資料1-5-3（P348）参照

6 情報通信ネットワークの安全性・信頼性

SQLスラマーにより、韓国全土でインターネットが麻痺

近年、個人や個別企業のセキュリティ侵害だけでなく、情報通信ネットワーク全体を脅かす侵害事例が発生している。今日、社会経済全般において情報通信ネットワークへの依存度が増しており、一旦情報通信ネットワークの安全性・信頼性が損なわれた場合には甚大な被害が発生するおそれがある。

これまでも大地震等の自然災害によって情報通信ネットワークの安全性・信頼性が脅かされることは多くあった。しかし、近年、自然災害に加え、いわゆるサイバーテロなどの人為的な攻撃により、情報通信ネットワークの安全性・信頼性が実際に侵害される事例が発生している。

1 SQLスラマーによるインターネット障害

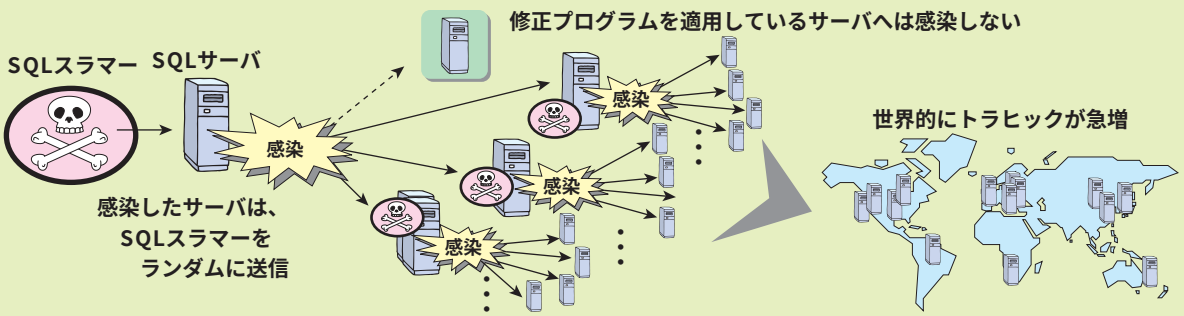
平成15年1月、SQLスラマー（Slammer）と呼ばれるワーム型ウイルスが猛威を振るい、過去最大規模のインターネット障害が発生した。SQLスラマーは、SQLサーバというデータベースサーバ用プログラムの欠陥（セキュリティホール）を突くワームである。メモリー上でのみ活動し、ハードディスクにファイルを作成しないため、ウイルスチェックソフトでは検出できない。感染したサーバは、他のサーバに向け極めて高速でワームのコピーの送信を繰り返すため、トラヒックが急増し、ひいてはインターネット接続ができなくなるなどの障害に至った（図表①）。我が国においては一部を除き、特に目立った被害はなかったものの、米国、韓国、中国等で被害が発生した。特に韓国では、全土で約9時間にわたってインターネットが麻痺し、社会的混乱をもたらした。

韓国で被害が大きかった理由として、韓国情報通信部では、ブロードバンド等を通じて急速に拡散したことや一部利用者がセキュリティパッチを当てていなかったことなどを挙げている。実際、今回のプログラムの脆弱性については半年以上前から危険性が警告されており、既に無償で配布されていたセキュリティパッチを当てていれば、このワーム感染は防止できていた。韓国政府では、今回の障害を踏まえ、総合的な「情報セキュリティ強化対策」を策定し実施する方針である。

2 ルートネームサーバへの攻撃

平成14年10月、インターネットの基盤システムを脅かしかねない事件が発生した。インターネット上で接続されているコンピュータ等の端末は、IPアドレス（例えば「211.133.250.131」）によって識別される仕組みとなっており、さらに、IPアドレスに対応して、人間がわかりやすいように、ドメイン名（例えば、「www.soumu.go.jp」）というアルファベット等を用いた標記が使用されている。このドメイン名とIPアドレスを対応させるシステムがDNS（Domain Name System）であり、我が国を含む全世界13か所にその根幹をなすルートネームサーバが置かれている（図表②）。このルートネームサーバが、一斉にDDoS攻撃（Distributed Denial of Service：分散型サービス不能攻撃。システムをダウンさせることを目的として多数のサーバを踏み台にして大量のデータを同時に送りつける攻撃）を受けた。一般利用者に実害はなかったが、日米など9か所のルートネームサーバで、処理能力が若干低下するなどの障害が発生した（図表③）。

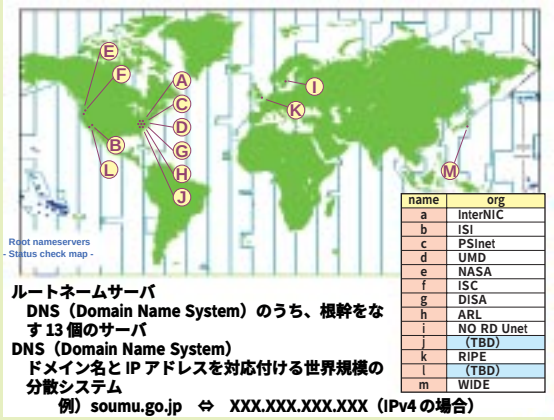
図表①　SQLスラマーによるインターネット障害のイメージ図



3 ワン切りによる電気通信ネットワークの機能障害

情報通信ネットワークに対する意図的な攻撃だけでなく、情報通信の不適切な利用に伴い情報通信ネットワークの安全性・信頼性が損なわれる事故も発生している。平成13年11月頃から、いわゆる「ワン切り」の被害が急増した。ワン切りとは、携帯電話端末等の着信履歴表示機能を悪用した迷惑電話であり、着信履歴に残された電話番号にコールバックさせて有料の音声サービス等を聞かせることを目的に、ワンコール（1回程度の呼び出し）だけで電話を切る行為である。平成14年7月には、NTT西日本において、大量のワン切りが原因となり、大阪府及び兵庫県の一部で輻そうが生じ、約500万回線の電話の利用に支障が生じる事態が発生した（図表④）。ワン切りについては、処罰規定を設ける有線電気通信法の一部を改正する法律が、平成14年12月に施行されている(3-7-1(1)(P274)参照)。

図表②　ルートネームサーバの配置

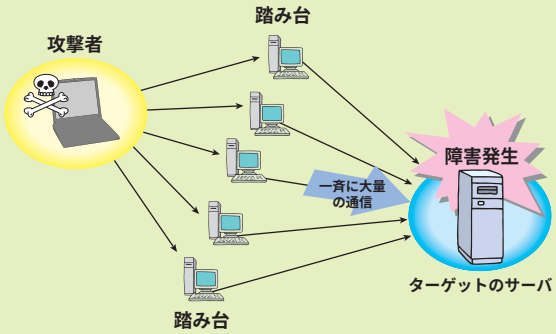


ルートネームサーバ
DNS（Domain Name System）のうち、根幹をなす13個のサーバ
DNS（Domain Name System）
ドメイン名とIPアドレスを対応付ける世界規模の分散システム
例）soumu.go.jp　⇔　XXX.XXX.XXX.XXX（IPv4の場合）

（注）XXXは0～255までの数字

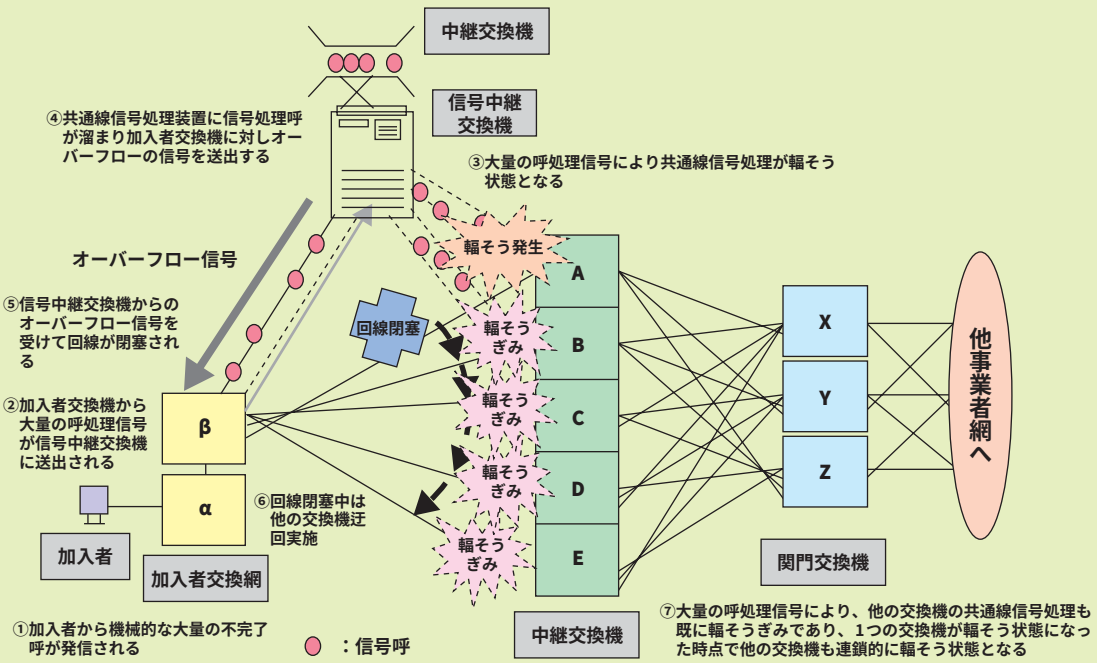
（出典）「WIDE資料より総務省作成」

図表③　DDoS攻撃



（出典）「コンテンツ・セキュリティに関する調査」

図表④　平成14年7月に起きた大阪における輻そうのメカニズム



NTT西日本資料により作成

7 諸外国における対策

OECD、欧米等で情報セキュリティ政策を強化

情報セキュリティや情報通信ネットワークに対する危機に対処するため、我が国では、IT戦略本部に、「情報セキュリティ対策推進会議」及び「情報セキュリティ専門家調査会」を設置し、各種の措置を講じてきた。総務省においても、「有線電気通信法」の改正、「電気通信事業における重要通信の在り方に関する研究会」の開催、関係技術開発等の取組を行ってきた（3-7-2(P277)参照）。国際機関や米国、EUにおいても、2001年9月11日の米国同時多発テロ等を契機に国の安全確保に対する意識が高まっており、情報セキュリティ政策が強化されている。

1 OECDによる新しい情報セキュリティ・ガイドラインの策定

OECDは、2001年から、各国の情報セキュリティ確保の指針として1992年に定めた「OECD情報システムのセキュリティ・ガイドライン」を見直し、2002年8月に「情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて（Guideline for the Security of Information Systems and Networks： Towards a Culture of Security)」を発表した。新ガイドラインにおいては、「セキュリティ文化」を提唱し、情報システムやネットワークの利用や開発に際してセキュリティ意識を高める必要性を強調している。また、ネットワークの観点から情報セキュリティをとりあげ、情報セキュリティ確保に関する9原則を打ち出している(図表①)。

2 欧州評議会（Council of Europe）(注)における「サイバー犯罪に関する条約」の採択

欧州評議会は、2001年11月、閣僚委員会において「サイバー犯罪に関する条約（Convention on Cybercrime)」を採択した。2003年2月末現在、我が国も含め35か国が署名、そのうち2か国が締結している。「サイバー犯罪に関する条約」では、不正アクセスや不正な傍受等についてこれを犯罪として処罰することや、コンピュータ・データの迅速な保全等の刑事手続について、締約各国においてこれらを立法化すること等を求めている。

我が国においては、総務省を含め関係省庁において、締結に向けた関係国内法の整備等を進めている。平成15年3月には、刑事の実体法及び手続法の整備のため、法務大臣が法制審議会に対し、「ハイテク犯罪に対処するための刑事法の整備に関する諮問」を行っている。

図表①　OECDの新情報セキュリティ・ガイドラインの9原則

9原則	概　要
①認識の原則	情報システム及びネットワークの開発、サービス提供等をする政府、企業、その他の組織及び個人利用者（以下、参加者）は、情報システム及びネットワークのセキュリティの必要性並びにセキュリティを強化するために自分達にできることについて認識すべきである
②責任の原則	すべての参加者は、情報システム及びネットワークのセキュリティに責任を負う
③対応の原則	参加者は、セキュリティの事件に対する予防、検出及び対応のために、時宜を得た、かつ協力的な方法で行動すべきである
④倫理の原則	参加者は、他者の正当な利益を尊重すべきである
⑤民主主義の原則	情報システム及びネットワークのセキュリティは、民主主義社会の本質的な価値に適合すべきである
⑥リスクアセスメントの原則	参加者は、リスクアセスメントを行うべきである
⑦セキュリティの設計及び実装の原則	参加者は、情報システム及びネットワークの本質的な要素としてセキュリティを組み込むべきである
⑧セキュリティマネジメントの原則	参加者は、セキュリティマネジメントへの包括的アプローチを採用すべきである
⑨再評価の原則	参加者は、情報システム及びネットワークのセキュリティのレビュー及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである

（注）欧州評議会は、西欧10か国が人権、民主主義、法の支配という価値観を実現するために設置した国際機関であり、我が国は米国、カナダ等とともにオブザーバ国となっている

3 米国における情報セキュリティ対策

（1）「国土安全保障省」の創設

2002年11月、「2002年国土安全保障法（Homeland Security Act of 2002）」が成立し、米国内の安全保障を総括する「国土安全保障省（The Department of Homeland Security）」が新設されることとなった。「国土安全保障省」は、安全保障に関連する22の政府機関を統合し、約18万人の職員と約360億ドルの予算を擁する予定である。「国土安全保障省」の設置により、通信インフラを含む重要インフラのセキュリティ関連組織の一元化、サイバーセキュリティ対策の強化、研究開発体制の強化が図られることとなっている（図表②）。

（2）「サイバースペースの安全性を確保するための国家戦略」の策定

2003年2月、大統領直属のインフラ保護委員会（CIPB：Critical Infrastructure Protection Board）は、「サイバースペースの安全性を確保するための国家戦略（The National Strategy to Secure Cyberspace）」を発表した。この戦略は、民間と協力して重要インフラに対する攻撃を未然に防ぐこと、脅威に対する脆弱性を少なくすること、攻撃された場合の被害と復旧時間を最小限にすることを目標としており、重点5項目について取り組むべき対策や勧告が示されている。本戦略では、情報セキュリティの確保は、連邦政府だけでなく、州、地方自治体、民間セクター、国民など米国全体で取り組むべき問題であるとしている。

（3）「サイバーセキュリティ研究開発法」の成立

2002年11月、情報セキュリティに向けた「サイバーセキュリティ研究開発法」（Cyber Security Research and Development Act）が成立した。本法に基づき、全米科学財団（NSF：National Science Foundation）は、情報セキュリティの研究センターを設置し、奨学金制度及び特別研究員制度を設ける。米国立標準技術研究所（NIST：National Institute of Standards and Technology）は、産学連携等を助成する制度や他分野の研究者がセキュリティ研究を促すプログラムを設ける。また、情報セキュリティの研究開発には、2003年度～2007年度の5年間において約8億7,700万ドルの予算を割り当てられる。

4 EU（欧州連合：European Union）における情報セキュリティ対策

ＥＵにおいては、2002年6月に採択された「eEUROPE 2005アクションプラン」の中で、2005年までに達成する4つの目標の一つに「安全な情報インフラ」を掲げ、①サイバーセキュリティ・タスクフォースの設置、②セキュリティ文化の実現、③行政情報交換のための安全な通信環境の調査を推進していくこととしている（図表③）。また、欧州委員会では、EU諸機関及び加盟国に対し情報セキュリティに関する助言等を行う「ネットワーク情報セキュリティ庁（Network and Information Security Agency）」を設立する規則案を2003年2月に提出した。

図表②　米国「国土安全保障省」の情報セキュリティ確保に関する任務

- 米国の重要インフラ及び重要資源の安全確保に関する包括的な計画の策定
- 重要インフラに対する攻撃への対応における危機管理の実施
- 民間セクターや他の政府機関に対する、重要システムの障害からの緊急復旧時の技術支援提供
- 州や地方自治体、民間セクターや教育機関、国民に対して、警告発信や予防措置／対抗措置に関し助言
- 安全保障につながる研究開発、技術開発の実施や財政的措置

図表③　EUのeEUROPE 2005アクションプランにおける「安全な情報インフラ」実現に向けた行動案

- 2003年半ばまでにサイバーセキュリティ・タスクフォースを立ち上げる。サイバーセキュリティ・タスクフォースは、セキュリティ問題の専門研究センターとなるべきである
- 2005年末までに情報通信機器の設計や実装における“セキュリティ文化”を確立する。2003年末に進展状況についての中間報告を発表し、2005年末までに最終的な評価を発表する
- 2003年末までに行政機密情報を交換するための安全な通信環境の実現可能性について調査を行う

コラム2

オープンソースソフトウェア

ー各国の政府調達でも採用が進む

情報通信システムの導入に当たり、オープンソースソフトウェア（Open Source Software）の利用が進んでいる。オープンソースソフトウェアとは、ソフトウェアの設計図に該当するソースコードを、インターネット等を通じて無償で公開し、誰でも改良、再配布することができるようにしたソフトウェアをいう。商用のソフトウェアの場合、ソースコードがオープンにされることは少なく、他社に供与する場合はライセンス料を取ることが一般的である。これに対し、ソースコードを公開することで、誰もがソフトウェアの開発に参加可能にし、その結果、改良、開発が推進されるという考え方から作られたソフトウェアが、オープンソースソフトウェアである。

非営利の民間団体であるFSF（Free Software Foundation）は、オープンソースの考え方に基づき、GPL（General Public License）というライセンス体系を定めている。GPLにおいては、ソースコードの公開を原則とし、オープンソースソフトウェアを改変した者は、自ら改変したソフトウェアを他人が再配布や改変することを妨げてはならない。

代表的なオープンソースソフトウェアとしては、OS（Operating System：コンピュータシステム全体を管理する基本的なソフトウェア）であるLinux（リナックス）やウェブサーバであるApache（アパッチ）が挙げられる。Linuxは、当時フィンランドの大学院生であったリーナス・トーバルズ氏が開発したOSで、GPLに基づいて公開され、誰でも自由に改変・再配布することができる。現在では全世界の開発者によって改良が重ねられている。

オープンソースソフトウェアは、ソースコードが公開されているため、開発・利用段階において多くの技術者によるチェックが行われ、不具合の発生するおそれのある箇所がすばやく発見される可能性がある。また、ユーザ自身がリスクをある程度把握し、対応策を講じることが可能である。ただし、オープンソースソフトウェアがセキュリティ面で必ずしも優れているわけではなく、また、一般にセキュリティは保証されておらず、自己責任で利用しなければならない。

諸外国の政府調達においても、オープンソースソフトウェアの採用が進んでいる（図表）。その背景には、①機能性・信頼性の向上、②導入運用コストの削減、③特定のソフトウェアへの依存の回避等があると指摘されている。

総務省では、平成15年に学者や業界関係者らで構成する調査研究会を開催し、オープンソースOS及び非オープンソースOSについて、セキュリティ面や運用面等におけるメリット・デメリットを客観的・中立的に評価する予定である（3-7-2（1）（P227）参照）。

図表　オープンソースソフトウェア導入に関する諸外国の動向

国・地域	概　要
米国	2003年2月　国防総省が高セキュリティ用途向けの調達品認定リストにオープンソースソフトウェアを追加した
EU	2002年7月　欧州委員会は、公共機関でオープンソースソフトウェアを共有し、IT費用を削減するよう各国政府に求めた
フランス	2001年8月　行政機関のフリーソフトウェアとオープンな規格の採用を奨励するために、行政関連情報通信技術庁（ATICA）を設立した
ドイツ	2002年6月　政府はオープンソースソフトウェアの利用を促進するために民間企業と包括的な契約を結んだ
中国	2002年12月　中国政府は公共機関向けのオープンソースソフトウェアを開発し、北京市がこれを数千台採用した

（出典）三菱総合研究所資料により作成