要旨

第６節のポイント

インターネットは、今や欠かすことのできない重要な社会基盤として、企業活動、行政活動、国民生活等の社会全般に浸透し、インターネットを活用した電子商取引や電子政府・電子自治体の実現は、国民生活の効率性・利便性を向上し、創造性豊かな暮らしを支援するものと期待される。他方で、あらゆる情報がデジタル化されることにより、これを利用した不正行為が行われる危険性も高まりつつあり、このような不正行為による被害を最小限にするための取組が重要となってきている。そこで、第6節においては、情報セキュリティの現状と、インターネット利用者の意識について概観する。

（情報セキュリティ侵害等の現状）

○ 東証上場企業の約60%が、最近1年間に情報セキュリティに対する侵害事案が発生したと回答しており、そのうち96.0%においてウイルス・ワーム感染が起きた。

○ 平成13年における不正アクセス行為の認知件数は1,253件で、平成12年の約12倍まで増加した。

○ 携帯電話・PHSを利用した電子メールサービスを提供する事業者に寄せられた迷惑メールに関する苦情相談の合計件数は平成13年6月には14万件に達した。

（セキュリティ・プライバシーに対する意識）

○ インターネット利用者が電子商取引を行う際に感じる不安としては、「クレジットカード番号や個人情報が第三者に盗まれないか」（77.7%）が最も大きい。

○ 平成13年にコンピュータウイルスに遭遇したインターネット利用者は、5割以上であった。他方、現在行っているコンピュータウイルス対策については、ワクチンソフトを利用しパターンファイルの更新を行っている人は約半数で、15.1%の人が「特に実施していない」と回答した。

○ 企業と地方公共団体の不正アクセス対策の実施状況では、アンチウイルスツールやファイアウォールの導入は高水準にあるものの、その他の対策は必ずしも高くない状況となっている。

1 情報セキュリティ確保の必要性

ー情報通信ネットワークの安全性・信頼性を脅かす事案の概要

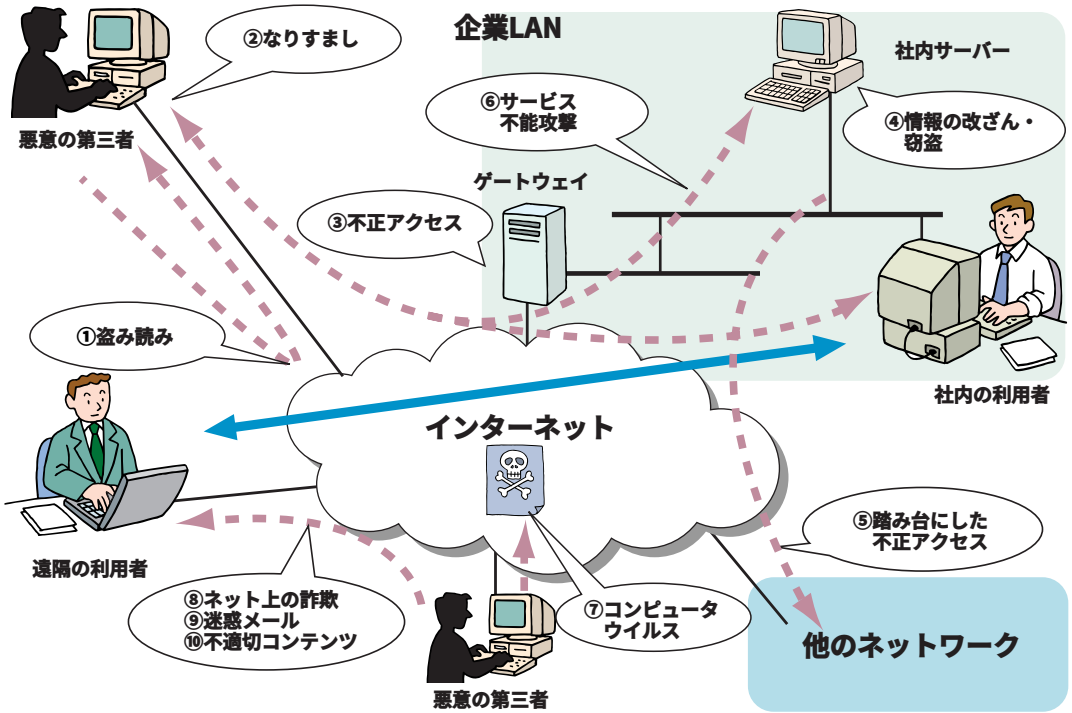
インターネットは、今や欠かすことのできない重要な社会基盤として、企業活動、行政活動、国民生活等の社会全般に浸透し、インターネットを活用した電子商取引や電子政府・電子自治体の実現は、国民生活の効率性・利便性を向上し、創造性豊かな暮らしを支援するものと期待される。

他方、あらゆる情報がデジタル化されることにより、これを利用した不正行為が行われる危険性も高まりつつある（図表）。例えばインターネットを経由して情報をやりとりする場合、暗号化が適切になされていないと、①通信途中での情報の盗み読み、②利用者へのなりすまし等の情報詐取、が行われる可能性がある。また、システムのセキュリティホール（情報セキュリティ上の不備）を悪用し、③企業ネットワーク等への不正アクセス、④機密情報や個人情報の改ざん・窃盗、⑤侵入したシステムを踏み台にした上での他のネットワークへの侵入等の不正アクセス行為、が行われるケースもある。その他、⑥大量のトラフィックを集中させて実質上機能を麻痺させるサービス不能攻撃（DoS）、⑦コンピュータウイルスの作成・配布といった迷惑行為、⑧ネットワークの匿名性を悪用した電子商取引等における詐欺行為、⑨迷惑メールの大量配信、⑩わいせつ画像等の不適切コンテンツ公開、など実社会と同様の社会問題も発生してきている。

インターネットが社会基盤として活用されている昨今、インターネットを巡るこのような問題は、企業活動、行政活動、国民生活にかかわる重大な問題を引き起こす危険性がある。そこで、上述のような被害を最小限に抑え、安全なネットワーク社会を維持するため、インターネットを利用する者一人ひとりの意識や姿勢が問われている。

また、インターネットは基本的にベストエフォート型のネットワークであるが、情報通信インフラ全体が電話を中心としたネットワークからインターネットベースのネットワークへの転換期にあり、かつ、このような情報通信インフラへの社会的な依存度が高まっていることから、電気通信事業者側においても、これまで以上に情報通信インフラの安全性・信頼性を高め、高品質で信頼性の高いサービスの提供、非常時における重要通信の確保、消費者への積極的な情報提供等が求められている（3-6-2参照。また、非常時の重要通信確保については3-2-1、IP電話サービスの品質については3-3-1-(4)参照。）。

図表　インターネットの安全性・信頼性を脅かす事案例



2 情報セキュリティ侵害等の現状

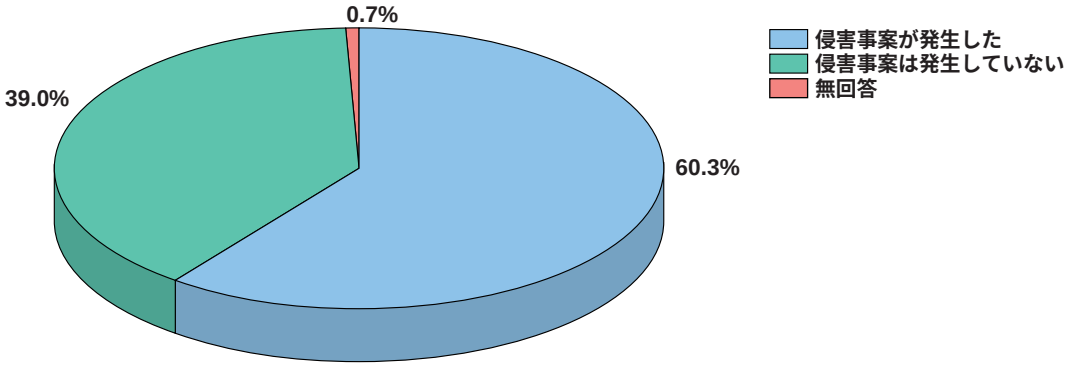
ー急速に増加するネットワークの不正事案

インターネットが急速に普及し、その利用が国民に浸透しつつある中、コンピュータウイルスや迷惑メール、電子商取引による詐欺、わいせつ画像等の不適切コンテンツ等の問題が、インターネット利用者に直接影響を及ぼす事態が生じている。

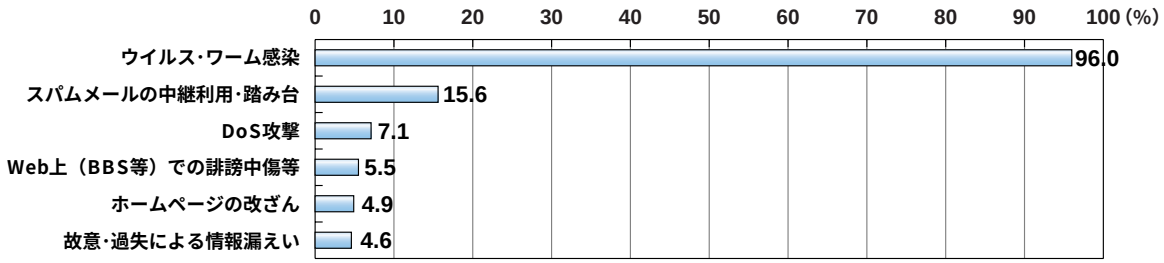
（1）コンピュータウイルス

「情報セキュリティ対策の状況調査」によれば、調査時点（平成14年2～3月）までの1年間に、東証一部・二部上場企業の約60%が情報セキュリティに対する侵害事案が発生したと回答しており（図表①）、その内容としては、ウイルス・ワーム感染が最も多く96.0%に上っている（図表②）。平成13年には、メールの添付機能を利用して自らの複製をばらまくタイプのコンピュータウイルスが大きな被害を出したことに加え、メールソフトやブラウザ等のセキュリティホールを利用して感染するタイプのコンピュータウイルスも出現した点に特徴がみられる（図表③）。

図表①　民間企業における情報セキュリティの侵害事案発生の有無



図表②　侵害事案の内容（抜粋）



※「侵害事案が発生した」と回答した企業のみを対象として集計

図表①、②（出典）　総務省「情報セキュリティ対策の状況調査」

図表③　平成１３年に流行したパソコンを標的としたコンピュータウイルスの事例

名　称	概　　要	発生時期
Sircam	・メールの添付ファイルを介して感染を拡げるコンピュータウイルス。 ・ワープロや表計算ソフトのファイルに自身をコピーし、メールに添付して自動送信する。その際、ファイルの拡張子を二重にして、普通のファイルに見せかけている。送るファイルはランダムに選ばれるため、プライバシーにかかわる情報や機密情報が他の人に漏れる可能性がある。 ・送信は自身のメーラー機能を使うため、ユーザのメーラーに送信履歴が残らない。	平成１３年７月
Nimda	・メールソフトやブラウザのセキュリティホールを悪用したコンピュータウイルス。 ・セキュリティホールのあるブラウザで改ざんされたホームページを見ると感染し、メーラーのアドレス帳に登録されているアドレス等にこのコンピュータウイルスを添付したメールを送信する。 ・さらに、メーラーによってはこのコンピュータウイルスが添付されたメールを開く又はプレビューするだけで感染することがある。	平成１３年９月
Badtrans	・メールの添付ファイルを介して感染を広げるコンピュータウイルス。 ・添付ファイルを実行すると５分後に、MAPI に対応しているメーラーの受信トレイにある未読のメールに、このコンピュータウイルスを添付したメールを返信する。 ・また、パスワードを特定のメールアドレスに送信するなど不正アクセス等を助長する機能を有する。	平成１３年１１月

（2）ウェブサーバーを標的としたコンピュータウイルス

平成13年には、ウェブサーバーを標的としたコンピュータウイルスが世界中で猛威を振るった。特に、Code Redと呼ばれるウイルスは、米国において10日間で30万台近いサーバーに感染したほか、変種であるCode RedⅡとあわせて、ブロードバンドの普及で先行する韓国をはじめとする世界各国に大きな被害をもたらした（図表④）。

（3）不正アクセス

国家公安委員会・総務省・経済産業省の発表した「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」によれば、不正アクセス行為の認知件数は平成13年には1,253件と、平成12年の約12倍まで増加した(注1)（図表⑤）。このうち、海外から不正アクセス行為が行われたことが判明しているものは448件で、前年の約18倍となった。不正アクセス行為の内容は、ホームページ書換プログラムによるホームページ書換事案が813件と大半を占め、自己増殖型不正プログラム（いわゆるコンピュータウイルス）による事案（94件）がそれに続く。また、被害に係る特定電子計算機のアクセス管理者別にみると、一般企業が429件で、プロバイダを大幅に上回っている。これは、セキュリティホールの対策が遅れがちな企業が標的になったためと考えられる。なお、検挙数は35事件（67件）、検挙人員は51人で、このうち33事件が（52件）が識別符号（ID番号等）窃用型であり、3事件（14件）がセキュリティホール攻撃型であった。

図表④　平成１３年に流行したサーバーを標的としたコンピュータウイルスの事例

名　称	概　　要	発生時期
Code Red	・IIS サーバーのセキュリティホールより侵入し、システムを改ざんする。 ・メモリ上で動作する点が特徴で、ファイルサイズやタイムスタンプの変更を監視するソフトでは検出不可。 ・変種の「Code Red II」の場合、他の Web サーバーに感染を試み、別のバックドアを仕込んで、サーバーを外部からフルコントロール可能にする。	平成 13 年 7 月
Sadmind/ IIS	・Solaris マシンを踏み台にして IIS を攻撃するクロスプラットフォーム型のコンピュータウイルス。 ・Solaris マシンのセキュリティホールに侵入し、他の Solaris マシンの感染を試み、IIS サーバーの Web ページを改ざんする。	平成 13 年 5 月

図表⑤　不正アクセス行為の認知件数

		平成 13 年	平成 12 年	増減
認知件数	海外からのアクセス	448	25	423
	国内からのアクセス	258	73	185
	不明	547	8	539
	計	1,253	106	1,147

（出典）国家公安委員会・総務省・経済産業省「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」

（注1）平成12年の件数は、「不正アクセス行為の禁止等に関する法律」が施行された平成12年2月13日から、同年12月31日までの間の件数（3-6-2-(1)参照）

（4）ハイテク犯罪

インターネットは相手の顔が見えない匿名性を有することから、商品の受渡しや代金の支払いにおける詐欺行為等の危険性が伴う。警察庁の発表によると、インターネットを利用した詐欺事件の検挙件数は、平成12年の53件から平成13年には約2倍の103件へと急増しており、このうち約6割はインターネット・オークション(注2)の利用に関するものとなっている（図表⑥）。また、平成12年に最も検挙件数の多かったわいせつ物頒布等は、平成13年には103件（対前年比33%減）となったが、インターネットを利用した児童売春・児童ポルノ法違反は前年の約2倍に当たる245件と、急増している。

（5）迷惑メール

受信者の同意がないまま一方的に送信される、いわゆる迷惑メールの問題が大きな社会問題となっている。携帯電話・PHSを利用した電子メールサービスを提供する事業者に寄せられた迷惑メールに関する苦情相談の合計件数は平成13年6月には14万件に達したが、メールアドレスの変更や指定受信・指定拒否機能の提供等によって、同年11月時点で約6万件まで縮小している（図表⑦）。なお、NTTドコモでは、同社のメールセンターに届いた1日当たり約9.5億通の電子メールのうち、約8億通が実在しない宛先への電子メールであったとしている(注3)（3-6-1(2)参照）。

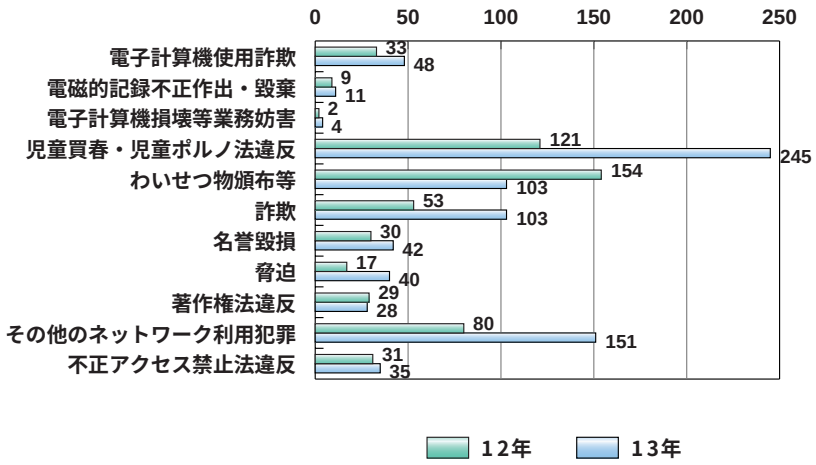
（6）インターネット上における誹謗中傷等

インターネット上の電子掲示板等において、誹謗中傷等の他人の権利を侵害する情報の流通が問題となっている。企業の信用問題にかかわる最近の事例としては、インターネット上の掲示板に自社の名誉を傷つける記載をされたとする企業が、当該掲示板管理者に対し、その記載の削除を求めて仮処分申請を行ったというものがある。本件については、東京地裁は、平成13年8月、原告側の主張を認め、管理者に対して削除を命じる決定を下している（1-6-5、3-6-1(1)参照）。

（7）個人情報保護

企業において、顧客や従業員の個人情報は重要な機密情報であるとともに、この扱い方次第では顧客等の人権を侵害することも想定され、その外部流出は企業の信用に大きなダメージをもたらす。しかし、実際には、操作ミス等の原因で、インターネットを通じそれらが外部に流出する事件が後を絶たない（図表⑧）。今後はプライバシーポリシーの策定等、問題解決のための抜本的な対応が求められる。

図表⑥　ハイテク犯罪の検挙状況

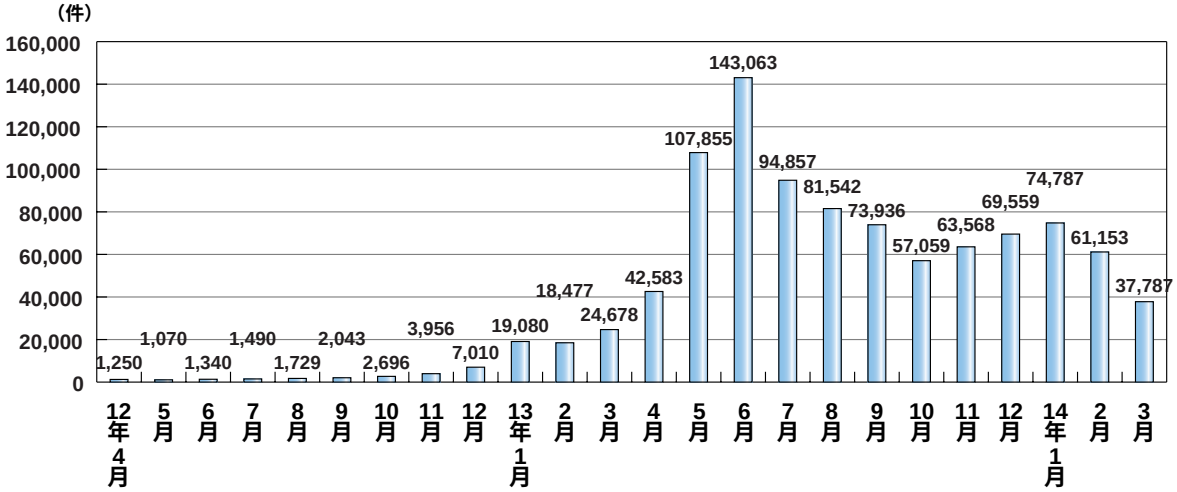


（出典）警察庁「平成13年中のハイテク犯罪の検挙及び相談受理状況等について」

（注2）ここにいうインターネット・オークションとは、インターネット上で物品の売買をしようとする者のあっせんをオークションの方法により行うサービス
（注3）平成13年10月の平均値

第６節　情報セキュリティの確保

図表⑦　迷惑メールについての利用者からの苦情・相談件数の月別推移



（出典）「迷惑メールへの対応の在り方に関する研究会」

図表⑧　平成１３年に発生したインターネット上での個人情報漏えいの事例

機　関	概　　要	原因
日用品メーカ	・自社製品のキャンペーン案内メールを顧客に配信した際、メールを返信した21人のメールアドレスが全会員約１万人に漏えい。	配信の設定ミス
旅行代理店	・航空券の案内メールを配信した際、約3,000人分のメールアドレスを流出。	配信の設定ミス
衣料品メーカ	・インターネットのショッピングサイトが保有する顧客570人分のメールアドレスを顧客全員に配信。	操作ミス
通信会社	・メールマガジンで、本文の代わりに８人分のメールアドレスを誤配信。	操作ミス
食品メーカ	・メールマガジンで、本文の代わりに読者約１万人分のメールアドレスを500人に誤配信。	操作ミス
官公庁	・メールマガジンの読者の一部に、約20人分のメールアドレスを流出。	操作ミス

3 セキュリティ・プライバシーに対する利用者のニーズ

ーネットワークにおける脅威に対する不安感

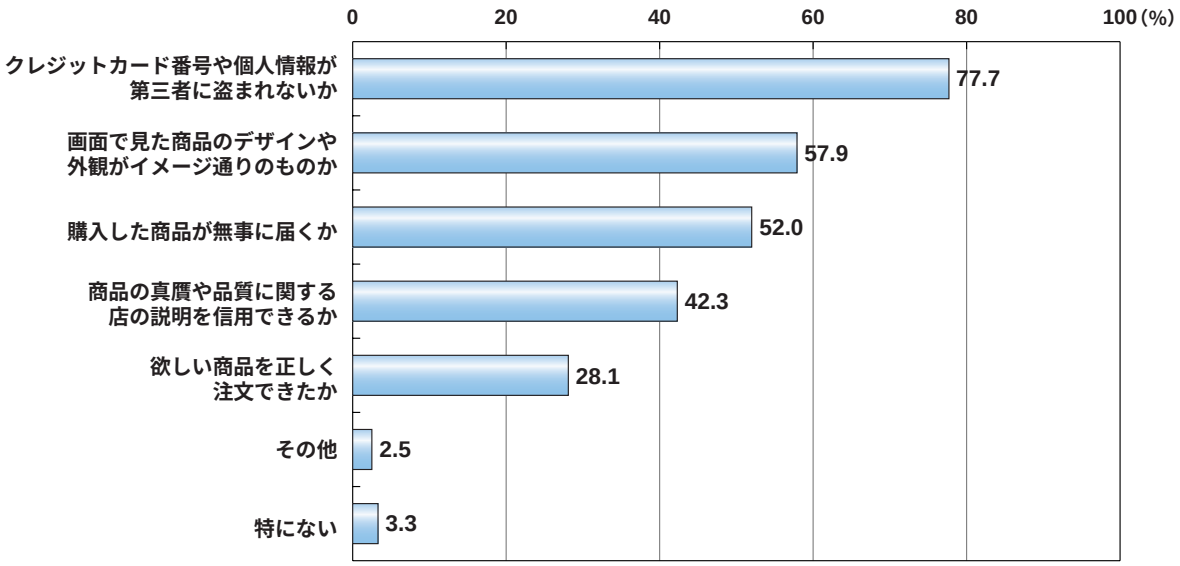
（1）利用者の不安感

インターネットの普及により国民生活は便利で豊かになるものと期待される一方、インターネット利用に対する国民の不安や不満及び知識の不足が、その発展を阻害している可能性も否定できない。ウェブアンケート調査によれば、インターネット利用者が電子商取引を行う際に感じる不安として、回答者の77.7%の人が「クレジットカード番号や個人情報が第三者に盗まれないか」を挙げており、「画面で見た商品のデザインや外観がイメージ通りのものか」「購入した商品が無事に届くか」という点についても5割以上の回答者が不安を感じている（図表①）。インターネット利用者にはネットワーク上での個人情報の送信と、取引相手の信頼性についてまだ高い不安感があることをうかがわせる。

また、同調査結果によれば、平成13年の1年間にコンピュータウイルスに遭遇した回答者の割合は、インターネットを週20時間以上利用する人の約7割、週20時間未満の人でも約5割に達している（図表②）。他方、現在行っているコンピュータウイルス対策については、ワクチンソフトを利用している人（57.2%）やパターンファイルの更新を行っている人（45.0%）が多いものの、15.1%の人が「特に実施していない」と回答しており、コンピュータウイルスに関するリスクは依然として大きいものと推察される(注)（図表③）。

そのほか、何らかの迷惑メールを受信した経験がある人は回答者のうち、およそ4人中3人に達することが明らかになった。迷惑メールの内容としては、特に出会い系サイトの広告を挙げる回答が多くなっている（図表④）。

図表①　電子商取引における不安

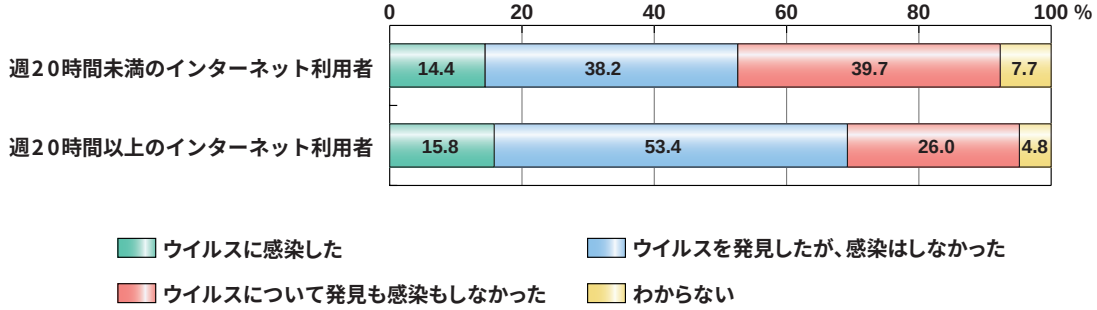


（出典）「情報通信分野の安全性と将来技術に関する調査」

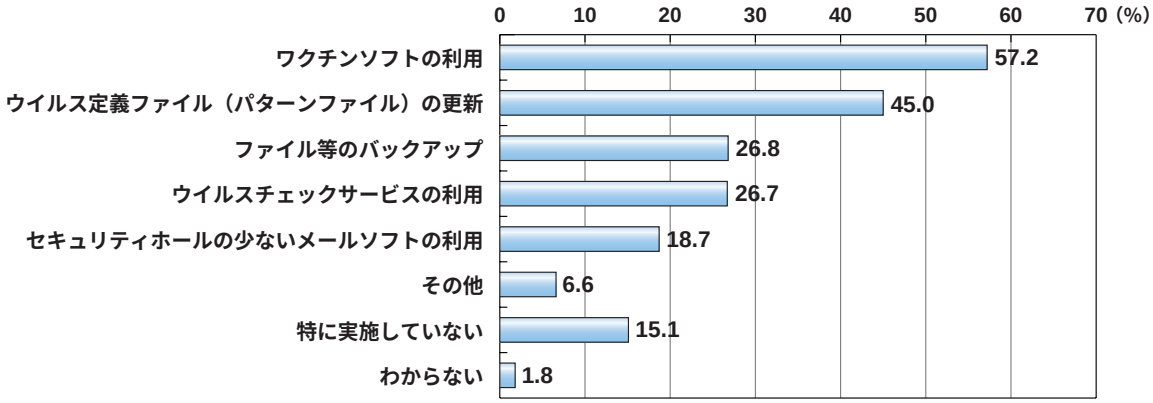
（注）本調査はウェブアンケートを用いているため、分析に当たり、アンケート回答者はインターネットを利用する頻度が比較的高い傾向があることに注意を要する

第６節　情報セキュリティの確保

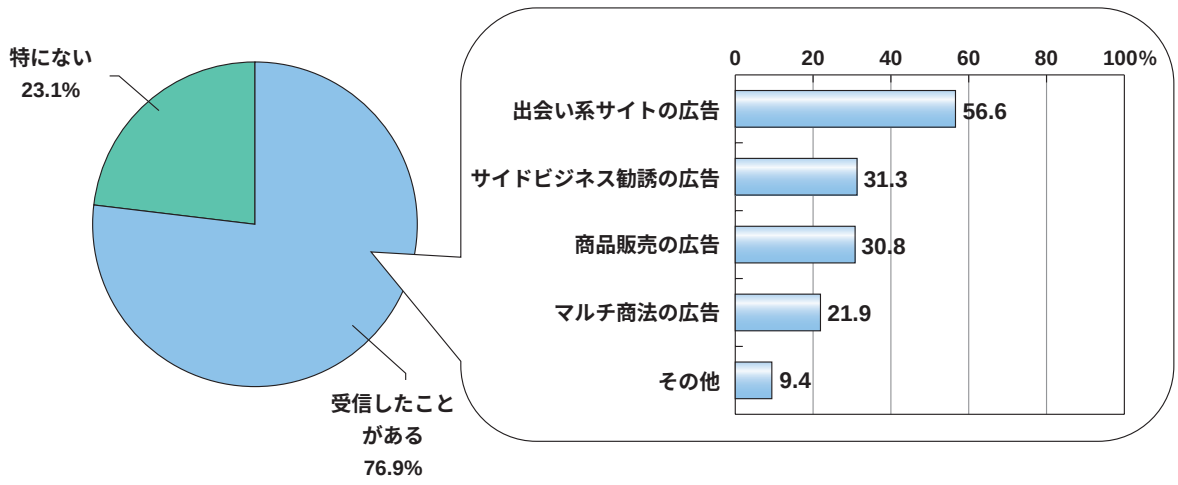
図表②　平成１３年のコンピュータウイルス被害経験（インターネットの週当たり利用時間別）



図表③　現在行っているコンピュータウイルス対策



図表④　迷惑メールの受信経験とその内容



図表②～④　（出典）「情報通信分野の安全性と将来技術に関する調査」

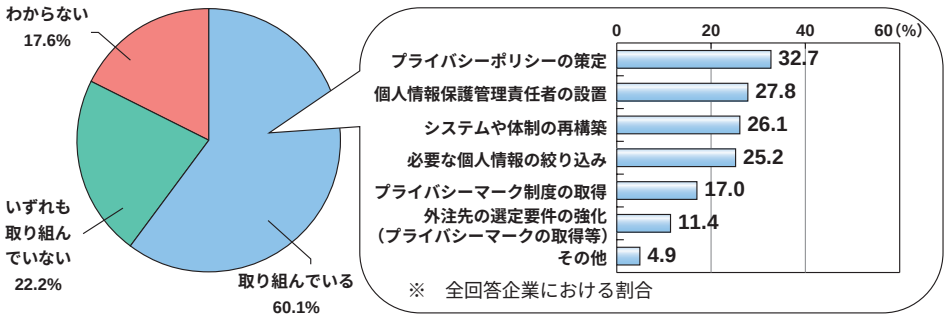
（2）企業利用者の意識

企業では、不正アクセス等の脅威にさらされてきた経験から、セキュリティ対策に様々なアプローチで取り組んでいると考えられる。他方、電子商取引、個人情報利用、広告メールなどの企業活動が社会的問題をもたらすことのないよう配慮する必要も生じている。

個人情報保護に対する取組については、消費者向けビジネス（電子商取引を含む。）を行っている回答企業の約6割が何らかの取組に着手していることが明らかになった（図表⑤）。その具体的な施策としては、「プライバシーポリシーの策定」、「個人情報保護管理責任者の設置」、「システムや体制の再構築」「必要な個人情報の絞り込み」が比較的上位の項目となっているが、いずれも3割以下の実施率にとどまっている。

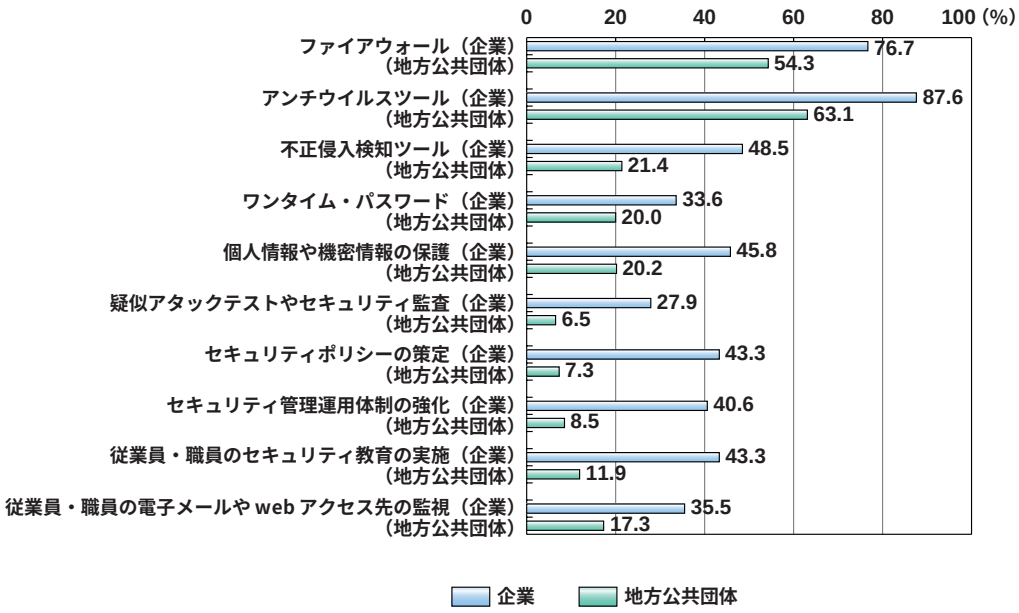
また、企業と地方公共団体の不正アクセス対策の実施状況を調べたところ、地方公共団体では、企業に比べ不正アクセス対策の実施が遅れていることが明らかになった（図表⑥）。対策別の導入状況をみると、アンチウイルスツールやファイアウォールは高水準にあるが、それ以外は企業で3～4割、地方公共団体で1～2割にとどまる。特に、「セキュリティポリシーの策定」については、企業では「実施済・実施中」が43.3%であるのに対し、地方公共団体では7.3%に過ぎない状況となっている。

図表⑤　個人情報保護への取組状況



（出典）「情報通信分野の安全性と将来技術に関する調査」

図表⑥　企業・地方公共団体における不正アクセス・ウイルス対策の実施状況



※　本調査は企業の情報システム部署担当者を対象としたウェブアンケートを用いているため、分析に当たり、比較的規模の大きな企業の回答率が高いことに注意を要する（従業員規模３００人以上／年間売上高１０億円以上の企業がそれぞれ約５割）

（出典）「情報通信分野の安全性と将来技術に関する調査」／「電子自治体の動向に関する調査」

4 健全なネットワーク環境の確保に向けた課題

－ユーザー意識の向上と技術・サービスによる対応

（1）セキュリティ技術／サービス

情報セキュリティを確保し健全なネットワーク社会を育成するためには、これらに対応した技術やサービスの開発が急務となっている。以下では、現在取り組まれている主な技術やサービスの開発状況等について、その概要をみていくこととする。

①不正アクセス等に対する技術

（ｉ）ファイアウォール

外部からのアクセスを制御するファイアウォールは、ネットワークセキュリティの基本技術として広く普及している。従来のゲートウェイ型に加え、サーバーごとに組み込むホストベース型のものが普及しつつあり、効果を高めるためこれらを組み合わせるケースもみられる（図表①）。

（ii）アンチウイルスツール

コンピュータウイルスを検出・駆除するツールは、最新のウイルス情報が組み込まれたパターンファイルを頻繁に更新する必要がある。そこで、管理者の負担を軽減するため、統合的な管理技術やサービスの開発が進んでいる。また、未知のウイルスの検出等についても研究が進められている。

（iii）IDS（Intrusion Detection System：侵入検知システム）

IDSは、ホストへのアクセスやネットワーク上の通信を監視し、不正侵入を検知した場合に警報を発するツールである。そのシステムの存在を侵入者に隠すためのIPアドレスを付与しないステルス接続の実用化、性能の評価基準の確立等といった課題が検討されている。

（iv）不正アクセス発信源追跡

インターネットを介した不正アクセスの抑止を徹底するためには、その発信源を追跡し、突き止めることが有効である。そこで、パケットの発信源の特定を可能にするIPトレースパック技術の研究開発が進められている。

②ネットワーク環境の健全性確保に向けた技術

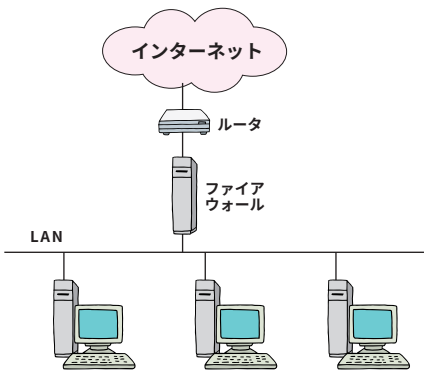
（ｉ）バイオメトリクス

バイオメトリクスとは、指紋や瞳の光彩、声紋、筆跡等、利用者個人に固有の生体情報を用いて本人認証を行う技術であり、入退室管理やネットワークへのログインの認証等、実利用も進んでいる。

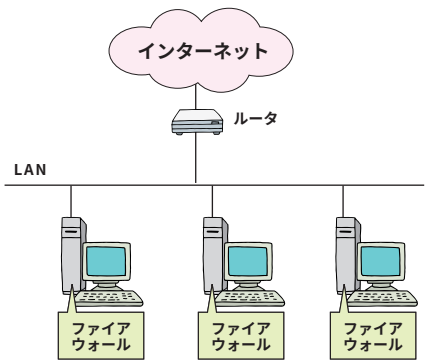
（ii）コンテンツ・フィルタリング

コンテンツ・フィルタリングとは、子供が閲覧するのに不適切なサイト等を、事前にその程度や内容に応じてリスト化（レイティング）しておき、必要に応じてこれらへのアクセスを制御する目的で利用されるツールである。現在は、サイトに記載された文章から検索ロボットでキーワードを抽出し、不適切なキーワードを含むサイトを選び出した上で、管理者がレイティングを行っているが、今後は画像や文章の意味理解を組み込んで、省力化・自動化を図る技術が期待されている。

図表①　ファイアウォールのタイプ



ゲートウェイ型ファイアウォール

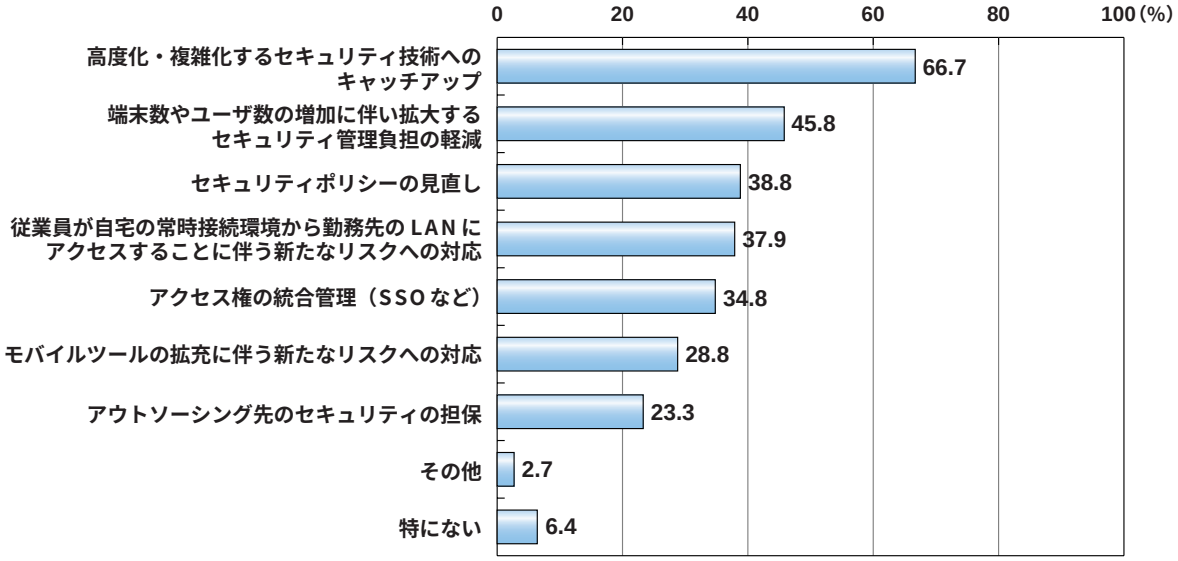


ホストベース型ファイアウォール

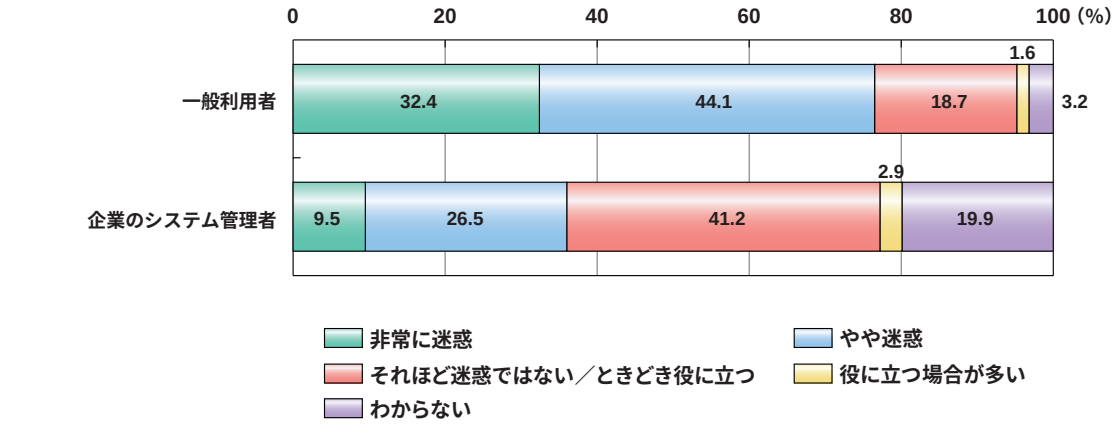
（2）ネットワーク環境に関するユーザ意識

健全なネットワーク環境を確保するため、上述のように様々な技術・サービスの開発が進んでいるものの、最終的にはネットワーク利用者それぞれが果たすべき役割の認識や意識向上が重要である。「情報通信分野の安全性と将来技術に関する調査」によると、企業の情報システム管理者のうち、およそ3人に2人が「高度化・複雑化するセキュリティ技術へのキャッチアップ」が今後の課題であると回答している（図表②）。また、広告メールを「非常に迷惑」「やや迷惑」とする割合は、企業側の認識では36.0%であったが、インターネット利用者側では4人に3人にも及んでおり、広告メールの発信者側と受信者側の意識の乖離がみられる（図表③）。これらから、健全なネットワーク社会の構築のためには、上述の技術やサービスの開発とともに、ネットワーク社会を適切に動かすための技術者の育成や、利用者の不安や不満を改善するためのルール作りなども今後の課題であると考えられる。

図表②　不正アクセス対策において今後重要となる課題



図表③　インターネット利用者の広告メールに対する考えと企業が想定する顧客の考え



図表②、③　（出典）「情報通信分野の安全性と将来技術に関する調査」

5 健全なネットワーク社会形成に向けた制度の整備

ー健全なネットワーク社会の実現に向けた政府・電気通信事業者の取組

情報セキュリティを確保するためには、技術等による対策だけではなく、ネットワーク社会における新たな制度／ルールの確立も必要となってきている。このような状況に対応するため、現在政府として、主に次のような制度整備を行っているところである。

（1）電子署名法

電子署名に手書きの署名や押印と同等の法的根拠を与えるなど、電子認証基盤の整備を図るため、平成13年4月に「電子署名及び認証業務に関する法律」が施行された（3-6-1-(4)参照、認証ビジネスの動向については1-2-3-(2)参照）。

（2）プロバイダ責任制限法

特定電気通信による情報の流通により他人の権利が侵害されたときに、関係するプロバイダ等が、これによって生じた損害について賠償の責めに任じない場合の規定と、自己の権利を侵害されたとする者が、関係するプロバイダ等に対し、当該プロバイダ等が保有する発信者の情報の開示を請求できる規定を設けることを目的として、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」が、平成14年5月より施行された（3-6-1(1)参照）。

（3）個人情報保護法

公的機関及び民間企業等の有する個人情報の保護に関する法案として「個人情報の保護に関する法律案」が国会に提出されているところである（3-6-1(3)参照）。

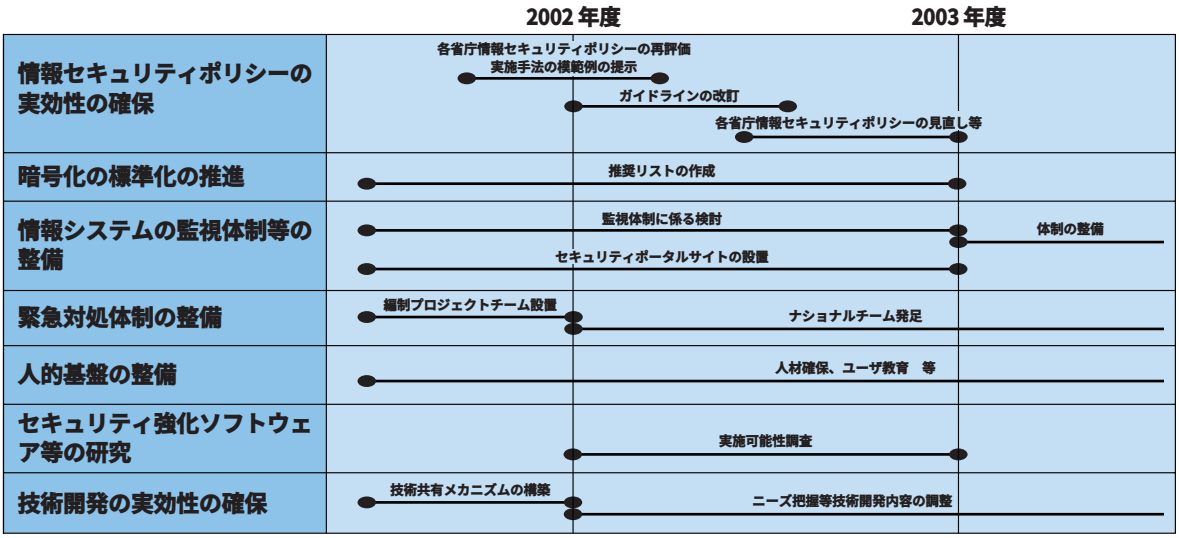
（4）迷惑メール対策

迷惑メールについては、各電気通信事業者においても対応策が採られているものの、現在のところ根本的な解決には至っていない。そこで、「特定電子メールの送信の適正化等に関する法律案」が第154回通常国会において成立するなど、対応が進められているところである（3-6-1(2)参照）。

（5）電子政府の情報セキュリティ確保のためのアクションプラン

IT戦略本部の下に設置されている情報セキュリティ対策推進会議においては、平成15（2003）年度までに予定されている電子政府の実現に向けて、国際的な連携や地方自治体との連携にも配意しつつ、政府の情報セキュリティ確保に万全を尽くすための7つの具体的な方策とその施策展開のスケジュールを示した「電子政府の情報セキュリティ確保のためのアクションプラン」を平成13年10月に策定した（図表）。

図表　電子政府の情報セキュリティ確保のためのアクションプラン（日程表）



（出典）「電子政府の情報セキュリティ確保のためのアクションプラン」（平成 13 年 10 月 10 日情報セキュリティ対策推進会議決定）

関連サイト：IT戦略本部・情報セキュリティ対策
（http://www.kantei.go.jp/jp/it/security/index.html）