

第8節 情報セキュリティの確立【要旨】

IT革命が進展し、ITの国民生活・社会経済活動への浸透が進めば進むほど、一度セキュリティに問題が生じた場合に社会経済に生じる損害が甚大となる。既に、これまでも他人のID・パスワードを窃用して企業等のネットワークやコンピュータへ侵入する不正アクセスの問題や、コンピュータウイルスによる被害が社会問題となり、政府・民間において各種対策を講じ、その防止が図られているところである。しかし、近年特定サイトのサービス提供を不能にする「DoS攻撃」(Denial of Service: サービス不能攻撃)や、電子メール添付ファイルへの「コンピュータウイルス」の混入による被害の急速・広範な拡大に見られるように、より深刻な被害を生じさせるセキュリティ侵害行為が目立つほか、国民生活や社会経済活動に重大な影響を及ぼす可能性のある攻撃、いわゆる「サイバーテロ」の脅威について指摘されているところである。

これに対して、企業や個人の対応状況をみると、平成12年度通信利用動向調査(総務省)によれば、まず不正アクセス対策については何らかの対応をしている企業の割合は77.5%に達しているが、内容的にはID・パスワードによるアクセス制御が全体の67.5%を占める一方、より実効性の高いファイアウォールの利用は39.1%にとどまっている。ウイルス対策についても、ネットワーク上の各接続端末にウイルスチェックを導入している比率は58.7%に達しているものの、外部接続の際のウイルスウォールを構築している比率は8.3%にとどまっている。いずれも、より実効性の高いファイアウォール、ウイルスウォールの一層の活用が望まれる。また、個人のコンピュータウイルス対策の状況についてみると、郵送アンケート調査結果によれば、「一応ワクチンソフトを導入している」との回答が35.2%に及んでいるが、

最近の電子メール添付ファイルによるウイルス被害の拡大に関し、「メール添付ファイル等はウイルス検査後使用」との回答は15.3%にとどまっている。個人レベルにおいても、コンピュータウイルス対策に関する意識の一層の浸透が望まれる。

他方、このように社会に重大な脅威をもたらす侵害行為のほか、わいせつ情報や個人のプライバシーを侵害する情報、いやがらせのための情報など、違法・有害情報の社会問題化や、個人情報の漏えい問題など、社会経済活動のネットワーク化にともない深刻化する問題も数多い。

違法・有害情報については、警察庁発表では平成12年中のハイテク犯罪等に関する相談受理件数のうち約26%を違法・有害情報(わいせつ画像、違法薬物販売等)が占めており、対応が喫緊の課題となっているが、違法・有害情報に対する対応としては、現在インターネット接続サービス等を提供する事業者による自主的対応が中心となっている。また、技術的な対応としては、受信者自身が違法・有害情報の受信を拒否できるよう、フィルタリング(選別)技術の開発・導入が進みつつある。

また、個人情報保護の問題については、これまで各電気通信事業者の自主的な取組を通じて取り組まれてきたところであるが、平成12年10月に政府全体の個人情報の保護・利用のあり方に対する枠組みについて「個人情報保護基本法制に関する大綱」が個人情報保護検討部会において取りまとめられ、第151回通常国会において「個人情報の保護に関する法律案」が提出されたところである。

1 不正アクセス・コンピュータウイルス

「サイバーテロ」対策が急務

インターネットの普及とともに、国民生活・社会経済活動のネットワーク化が進展する中で、ネットワークを通じて他人のID、パスワードを入力するなどしてコンピュータに不正に進入する「不正アクセス」、電子メール等を通じて感染しコンピュータに障害を引き起こす「コンピュータウイルス」といった、ネットワークに接続された情報通信システムを誤作動・停止させる行為が増加しているほか、いわゆる「サイバーテロ」の脅威が国民生活・社会経済活動に重大な影響を与える可能性が現実のものとなってきている。

不正アクセス問題

不正アクセス行為の禁止等に関し、「不正アクセス行為の禁止等に関する法律」が平成12年2月13日に施行されているが、同法に基づき国家公安委員会、総務大臣、経済産業大臣が公表した「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」(平成13年2月9日)によると、同法施行日から平成12年12月31日までの間に106件の不正アクセス行為が警察庁に報告されている。また、同期間中の不正アクセス禁止法違反の検挙状況は、31事件、37人であった(検挙事例につき図表)。不正アクセスの報告件数については、情報処理振興事業協会(IPA)に

対して128件、コンピュータ緊急対応センター(JPCERT/CC)に対して2,084件の届出がなされている。

また、このような不正アクセスのほか、特に近年、特定の情報システムに対して大量のデータを送りつける等の攻撃を行い、当該システムのサービス提供を不能としたり、あるいはシステムダウンを引き起こさせるいわゆる「DoS攻撃」(Denial of Service: サービス不能攻撃)の発生が問題となっている。著名な事例としては、平成12年2月に発生した、Yahoo!、buy.com、eBay、CNN.com、amazon.com等の米国の有力ポータルサイトを標的としたDDoS(Distributed Denial of Service)攻撃(注)がなされ、各サイトがいずれもサービス不能な状態に追い込まれた事例が挙げられる。また、平成13年2月には、海外のサイトに我が国のサイトに対するDDoS攻撃を行う旨の予告声明を出しているとの情報があり、これに関連すると思われる日本企業等に対するホームページ書き換え事件が発生している。平成13年3月8日の警察庁発表では、既に全国で104件の書き換えを把握し、不正プログラムの蔵置も確認されており、DDoS攻撃等の踏み台になることを防ぐよう呼びかけている。

図表 不正アクセス禁止法違反の検挙事例

件名	概要
違法薬物販売目的の他人の識別符号を使用した不正アクセス(平成12年3月検挙)	無職の男(34)が、クラッキング・ツール等を利用して入手した他人のID・パスワードを使用して不正にインターネットに接続し、ホームページを開設した上、薬物販売の広告を掲示し、薬物の購入希望者とのメールのやり取り等を行った。
レンタル・サーバー業者のウェブ・サーバーに対する不正アクセス(平成12年8月検挙)	無職の男(33)が、総当りにより探知した元勤務先の広告会社のID・パスワードを使用して同社の契約会社のウェブ・サーバーに侵入し、ホームページのデータを削除した。
iモード電話機用のウェブ・サーバーに対する不正アクセス(平成12年10月検挙)	無職の男(23)が、iモード電話機用の掲示板から入手した他人のID・パスワードを同電話機のメール・サービスを利用してハッカー仲間である会社員(25)に提供、さらに、同会社員が、同ID等をハッカー仲間である大学生(25)に提供し、同大学生が、同ID等を使用して不正にiモード電話機用のウェブ・サーバーに侵入し、掲示板の内容を書き換えるなどした。
ホームページ提供サービス業者のウェブ・サーバーに対する不正アクセス(平成12年10月検挙)	韓国関連の情報交換のためのホームページを開設する会社員(31)が、自己のホームページの掲示板に嫌がらせの書き込みをされたことに立腹し、同書き込みをした者が開設する韓国関連のホームページに係るID・パスワードを推測により探知し、不正にホームページ提供サービス業者のウェブ・サーバーに侵入し、本人に無断で退会届をすることにより同ホームページのデータを消去した。
解雇された会社の識別符号を窃取した不正アクセス(平成12年10月検挙)	情報通信関連会社の元社員(25)が、同社を解雇されたことに立腹し、同社に金銭的損害を与える目的で、在職中に知りえた同社のID・パスワードを使用して不正にインターネットに接続するとともに、同社に高額のインターネット接続料が請求されるよう契約内容を変更する旨の虚偽情報をプロバイダのサーバーに送信等した。

「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」(平成13年2月)より作成

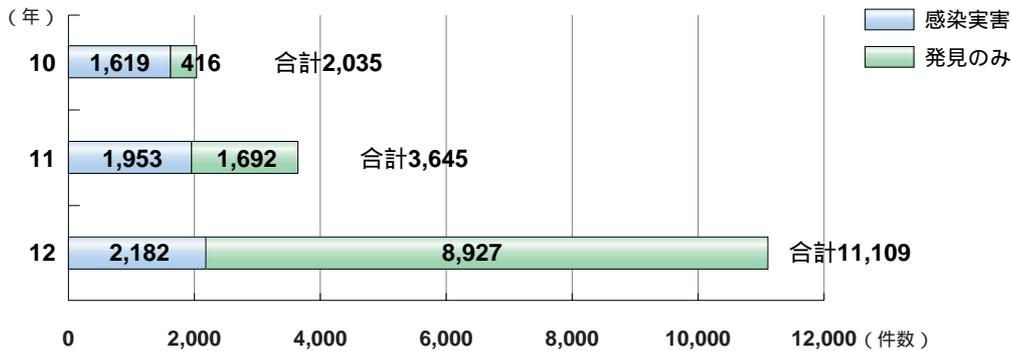
(注) DDoS攻撃とは、インターネット上の複数のコンピュータにDoS攻撃用のツールを仕掛け、攻撃者の使用するコンピュータからの命令により一斉にDoS攻撃を行い、標的となるサーバーコンピュータのサービスを妨害するものである。

コンピュータウイルス問題

コンピュータウイルスについては、IPA（情報処理振興事業協会）発表によると、平成10年から12年にかけてのIPAに対するコンピュータウイルス被害の届出件数は、平成12年は11年と比較して3倍を超える伸びを示している（図表）。また、最近の特徴としては、電子メールにファイルを添付することが一般的となり、添付ファイルにウイルスを混

入ることにより、被害が拡大しやすくなったことが挙げられる。平成12年度に発生した主なコンピュータウイルス被害事例（図表）をみると、共通する特徴として、電子メールの添付ファイルとして広まったことを挙げることができる。また、共通する機能としては、コンピュータウイルスが自分自身を電子メールを媒介して増殖することが挙げられ、特に特定のソフトウェア上での蔓延がみられた。

図表 コンピュータウイルスの発見件数・被害報告数等の推移



情報処理振興事業協会資料より作成

図表 平成12年度に発生したコンピュータウイルス被害事例

名称	時期	概要および特徴
ラブレターワーム VBS/LOVELETTER	平成12年4月～6月頃	「ILOVEYOU」「Mother's Day」「VBS/NewLove」等のタイトルを持つ電子メールを通じて感染・発病するウイルスが世界的に大きな被害をもたらした。感染コンピュータのファイルの破壊、ウイルスの添付されたメールの自動送信、IRC(インターネット・リレーチャット)を通じての自己増殖、ユーザーのID及びパスワードの窃盗、悪意あるプログラムの自動ダウンロード等を行うものであった。
VBS/Stages	平成12年6月～8月頃	「Funny」等のタイトルを持つ電子メールを通じて感染・発病するウイルスである。特定の文字列の表示、ウイルスの複製および関連ファイルの作成、特定実行ファイルの削除、電子メールの自動送信、IRC(インターネット・リレーチャット)を通じての自己増殖等を行うものであった。
W32/QAZ	平成12年9月～11月頃	電子メールを通じ、感染・発病するウイルスである。IPアドレスの搾取、外部からのリモートアクセスを可能にするといった、不正アクセスの支援機能も持ち合わせたトロイの木馬型ウイルスである。マイクロソフト社の不正侵入事件に利用されたとされる。
W32/MTX	平成12年9月～12月頃	メールを送信した日付による名前が異なる添付ファイルの実行により、感染・発病するウイルスである。ウイルスの複製および関連ファイルの作成、特定のファイルを改変、ウイルスが実行されるようにレジストリを変更、ウイルスによるメールの自動送信等の機能を有する。
W32/Navidad	平成12年11月～平成13年1月頃	Navidad.exeというタイトルの電子メールの添付ファイルにより、感染・発病するウイルスである。システムフォルダに、ウイルス自身をコピー、ウイルスによるメールの自動送信、exeファイルの使用不能等の機能を有する。
VBS/SST (AnnaKournikova)	平成13年1月頃	「AnnaKournikova.jpg.vbs」という電子メールの添付ファイルにより、感染・発病するウイルスである。ウイルスである添付ファイル「AnnaKournikova.jpg.vbs」を実行すると、メールソフトのアドレス帳に登録されている全てのアドレスにメールを送信する機能を有し、メールサーバーやネットワークに多大な負荷を与える。

各種資料より作成

不正アクセス及びコンピュータウイルスへの対応状況

企業における不正アクセス対策の状況については、平成12年度通信利用動向調査（総務省）によると、何らかの具体的な対応をしている企業の割合は77.5%と、平成11年と比較して9ポイント増加している（図表）。具体的な対策については、ID、パスワードによるアクセス制御のみが半数を超えている。

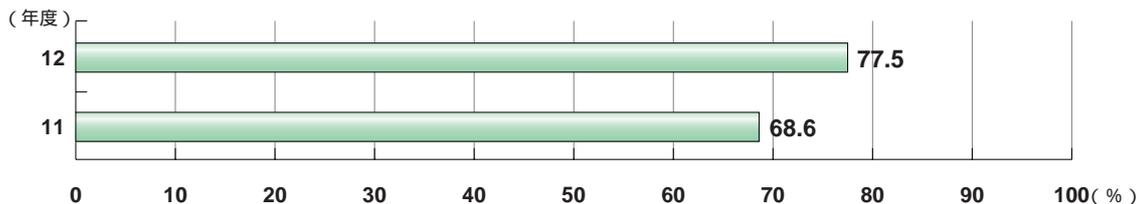
また、コンピュータウイルス対策の状況については、通信利用動向調査（総務省）によると、以下のようにになっている（図表）。平成11年と12年を比較すると、「何も行っていない」との回答が9ポイント以上減少し、全般的に企業におけるコンピュータウイルス対策は進んでいる。ただし、依然、ネットワークにおける各接続端末へのウイルスチェック

・プログラムの導入が対策の中心であり、実効性の高いウイルスウォールの設置は1ポイント強の増加（8.3%）にとどまっている。

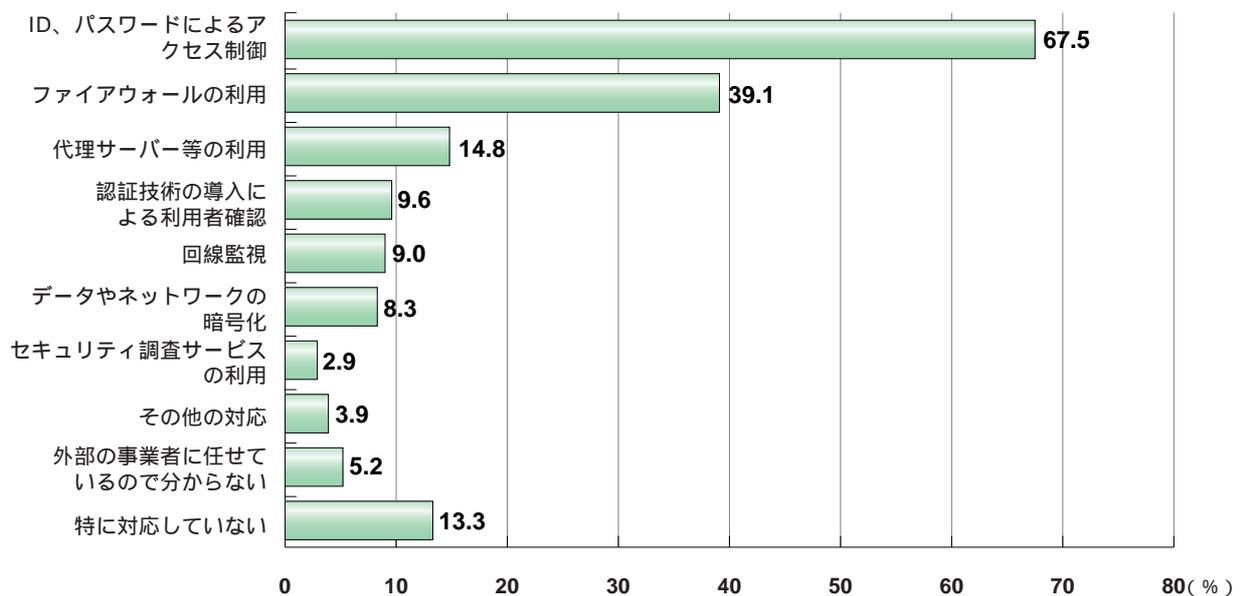
次に、個人レベルでのコンピュータウイルス対策の状況については、「インターネットに関するアンケート」によると（図表）パソコンでインターネットを利用している者のうち、「ワクチンソフトの導入」は35.2%、「データのバックアップ」は21.7%、「メール添付ファイルやダウンロードしたファイル等はウイルス検査後使用」は15.3%となっている。近年の電子メール添付ファイルを通じたコンピュータウイルスの拡大傾向を踏まえると、メール添付ファイル等へのウイルス検査の実施が求められる。

図表 企業における不正アクセス対策の現状

対応の有無



不正アクセス対策の内容（平成12年度）



「通信利用動向調査（企業編）」（総務省）より作成

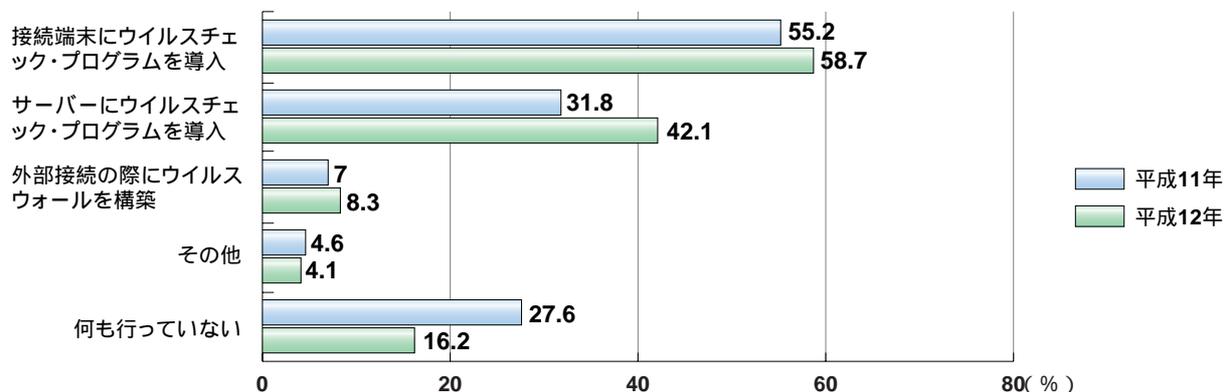
国においては、平成11年8月に「不正アクセス行為の禁止等に関する法律」が成立し、また平成12年1月には内閣において「ハッカー対策等の基盤整備に係る行動計画」が決定されたが、この行動計画に基づき政府全体として情報セキュリティ対策の取組を開始した直後に省庁等のホームページ改ざん事案が発生した。これがきっかけとなって平成12年2月に高度情報通信社会推進本部の下に設置された情報セキュリティ対策推進会議において、平成12年7月に「情報セキュリティポリシーに関するガイドライン」が決定され、各省庁において同ガイドラインを踏まえ、平成12年12月までに情報セキュリティポリシーが策定された。なお、省庁再編以降、総務省では本年2月に改めて情報セキュリティポリシーの策定を行ったところである。

このほか、不正アクセス行為に対する技術的な対応方策と

して、現に不正アクセスが行われている際にその不正アクセスの発信源を追跡・特定し、ネットワークの安全・信頼性の向上に資する技術の研究開発（不正アクセス発信源追跡技術に関する研究開発）を実施するなど、セキュリティの高いインターネットの実現に向けた取組を推進している。

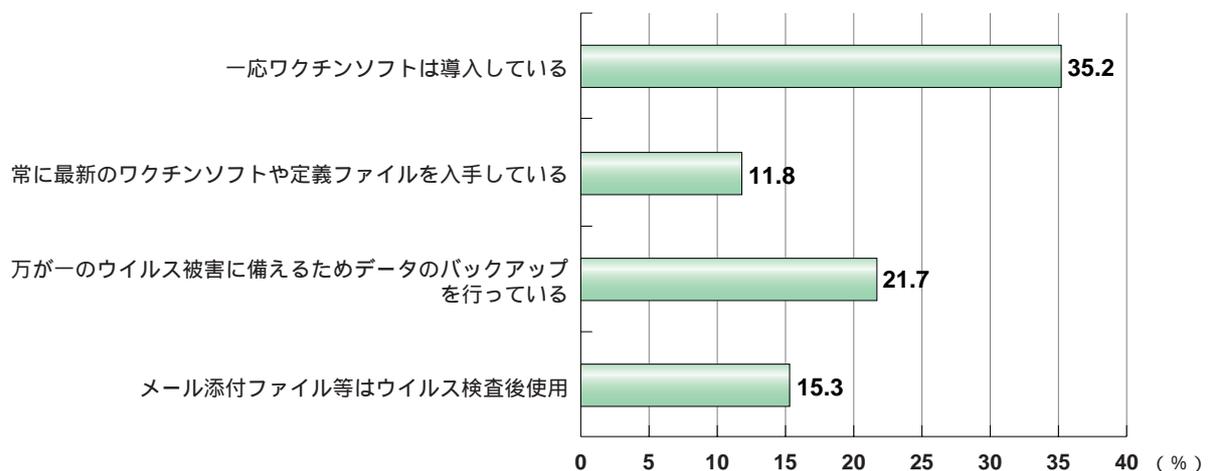
コンピュータウイルスに対しては、平成13年度予算等において、コンピュータウイルスを検知するための「コンピュータウイルス監視装置」が、電気通信基盤充実臨時措置法に基づく無利子・低利融資、税制特例措置、債務保証といった各種支援措置の対象設備として追加され、事業者におけるウイルス対策を促進するための支援が行われている。また、(財)日本データ通信協会では、ウイルスコンサルティングセンター（VCON）を設置し、インターネット利用者の不安解消を目的とした情報提供等の取組を推進している。

図表 企業におけるウイルス対策の状況



「通信利用動向調査（企業編）」（総務省）より作成

図表 個人におけるウイルス対策の状況



生活の情報化調査より作成

関連サイト：VCON（<http://www.vcon.dekyo.or.jp/>）

2 違法・有害情報

違法・有害情報の流通が社会問題化

国民生活・社会経済活動のネットワーク化にともない、インターネット上で、わいせつな情報、個人のプライバシーを侵害する情報、嫌がらせのための情報など、違法・有害情報の流通（注1）が社会問題化しつつあり、こうした情報に対する苦情・相談の件数も年々増加してきている。警察庁発表によると、平成12年中のハイテク犯罪等に関する相談受理状況（都道府県警察に寄せられた相談として警察庁に報告があったもの）では、相談件数全体（11,135件）のうち約26%（2,896件）を違法・有害情報（わいせつ画像・違法薬物販売等）（注2）の通報、取締り情報等が占めている。

違法・有害情報に対する対応は、現在インターネット接続サービス等を提供する事業者による自主的な対応により行われている。具体的には、平成10年2月に（社）テレコムサービス協会において「インターネット接続サービス等に係る

事業者の対応に関するガイドライン」を策定し、平成12年1月には、このガイドラインの趣旨を盛り込んだモデル契約約款の策定を行った。各事業者はこれらに沿って、契約約款に規定を設けた上で、違法・有害情報が発信されたことを知った場合には、その情報を発信した者に伝達、削除等の措置を要請し、さらには状況によっては削除する等の対応を行っている。また、インターネット上の情報流通に関して、ウェブページ等への情報掲載による他人の権利利益の侵害に、プロバイダ等が迅速かつ適切な対応が行えるよう責任を明確化するため、「特定電気通信による情報の流通の適正化及び円滑化に関する法律案」（仮称）を平成13年中に提出することとしている。

また、事業者による対応のみならず、受信者自身が違法・有害情報の受信を拒否できるよう、フィルタリング（選別）

図表 違法・有害情報事例（逮捕ないし書類送検されたもの）

分類	概要
薬物情報	平成12年4月に、ホームページを通じて覚せい剤や大麻を売買していたとして、東京都や神奈川県在住の男女合計6名が逮捕・起訴された。（客側が、平成12年2月中旬インターネット上の掲示板に「薬を売ってほしい」と書き込みを行い、これに応じた密売人から覚せい剤10袋を9万7千円で購入し、別の密売人からも覚せい剤や大麻樹脂など4袋を購入していた。）
薬物情報	平成12年9月に、北海道在住の男が逮捕・起訴された。容疑者は平成11年から、ホームページを開設し、個人輸入代行業の宣伝をし、未承認の外国製精力剤、育毛剤、ダイエット薬品、合法ドラッグなど22品目を掲載し、購入者を募り、全国の186人から計425万円の収入を得ていたとされる。
誹謗中傷（個人）	埼玉県の主婦が、平成12年3月に、当時在住していた宮城県内の隣家の女性といさかいを起こし、腹いせにインターネットの掲示板にその女性が男性を誘惑しているかのような書き込みをし、さらにその女性の自宅の電話番号を掲載する等したため、名誉毀損の疑いにより、平成12年10月に書類送検された。
誹謗中傷（企業）	平成12年11月に、千葉県在住の男が、ホームページ「最低焼き肉店のページ」を開設し、その中で以前のアルバイト先の焼肉店に「いかがわしきタレ」「干からびたカルビ」「はえだらけの注ぎ口」など虚偽情報を掲載し、偽計業務妨害容疑で逮捕された。
ポルノ情報	平成12年8月に、和歌山県在住の男が、平成11年6月頃から有料のアダルト・サイトを開設し、利用者から寄せられたわいせつな投稿写真を掲載していたとして、わいせつ図画公然陳列の疑いで逮捕された。

各種資料より作成

（注1）違法情報は、法令に違反したり、他人の権利を侵害したりするような情報をいい、有害な情報とは、公共の安全、善良な風俗や青少年の健全育成を害するような情報を指している。違法情報の例としては、覚せい剤等禁止薬物や銃器の売買情報、特定人に対する脅迫・詐欺・名誉毀損等刑法に抵触するもの、刑法上の「わいせつ」に該当するポルノ情報、児童買春、児童ポルノ法上の「児童ポルノ」に該当する情報が挙げられ、有害情報の例としては、刑法等の「わいせつ」、「児童ポルノ」に該当しないポルノ情報や暴力的な表現が挙げられる。

（注2）別掲されている名誉毀損・誹謗中傷等に関する相談（1,884件）を含めると、約43%に達する。

技術の開発・導入が進みつつある。フィルタリングには、全文検索方式、NOリスト方式、YESリスト方式、多段階レーティング（格付け）方式といった種類（図表 ）があるが、それぞれ長所・短所があり、現在きめ細かいニーズに対応できる多段階レーティング方式（図表 ）を中心としてその他の方式を組み合わせる枠組みが望まれている。

多段階レーティング方式については、レーティング情報の記述フォーマットの標準化やそれに対応したレーティング基準が提唱されている。しかし、最近ではコンテンツの内容について客観的な事実の確認にとどめるという考え方（ラベリング）が提唱され、国際的な取組が展開されている。また、通信・放送機構では、平成10年1月から横浜市の協力を得て、コンテンツのレーティングを支援する技術等、レーティング・フィルタリング技術の高度化のための研究開発を本年

3月まで実施したところであり、この研究開発の技術を活用することにより、レーティングに必要な人的負担が軽減されるほか、受信者の多様な価値観に柔軟に対応できることから、フィルタリングの機能がより発揮されることが期待できる。

図表 主なフィルタリング方式の概要

	説明	特徴
全文検索方式	コンテンツのテキスト部分を全文検索し、有害な単語が存在する場合そのコンテンツの全部または一部を閲覧させない方式	事前に設定した言葉を含むサイトへのアクセスは確実に停止。 全文検索のため効率が悪い。 画像情報には適用できない。 本来有害ではないものも閲覧不能になってしまう。
NOリスト方式	有害サイトのリストを参照し、リストに登録されたサイトへのアクセスを遮断する方式	事前に登録されたサイトへのアクセスは確実に停止。 リストから漏れている有害サイトにはアクセスが可能となるなど安全性に限界。
YESリスト方式	安全なサイトのリストを参照し、リストに登録されたサイトのみアクセスを許可する方式	安全性は高いが、新しく設置されたサイトなどリストに未登録のサイトにはアクセスできず、不便。
多段階レーティング方式	サイトの情報を発信者ないし第三者が段階別に格付けし、受信者が自らの段階を選択・設定することによりフィルタリングする方式	利用者個人のニーズにきめ細かく対応したフィルタリングをかけることが可能。 大量かつ日々変化するサイトに対するレーティング情報が必要となり、データベース作成の負荷が大きい。

図表 多段階レーティング方式におけるレーティング（格付け）の例（電子ネットワーク協議会）

	暴力	ヌード	セックス	言葉	その他
4	残虐	性器の強調	性行為	誹謗中傷	反社会的
3	殺人	全裸	性行為らしき描写	わいせつ表現	違法
2	殺傷	部分的なヌード	着衣のままの性的接触	悪口	公序良俗に反する
1	争い	露出的な服装	セクシャルなキス	穏やかな悪口	要注意
0	なし	なし	なし	不快感を与えない言葉	なし

図表 、 「インターネット上の情報流通の適正確保に関する研究会報告書」（平成12年12月）より作成

3 個人情報保護

個人情報の保護に関する法律案を国会提出

ITの発展により電子化された情報をネットワークを介して大量かつ迅速に処理することが可能となり、その一方で個人情報の様々な漏えい事例も発生してきていることから、個人情報保護の必要性が一層高まってきている(図表)。また、ネットワーク社会における電子商取引の発展等を促進するためには、情報の自由な流通が不可欠であることから、利用面の有用性にも配慮した個人情報保護のあり方が強く求められるようになってきている。

電気通信分野における個人情報については、郵政省(現総務省)が策定した「電気通信事業における個人情報保護に関するガイドライン」(平成3年策定、同10年改定)、「発信者情報通知サービスの利用における発信者個人情報の保護に関するガイドライン」(平成10年策定)に基づき、電気通信事業者等が自主的にその保護に努めてきている。また、(財)日本データ通信協会では、平成10年4月から、協会内に個

人情報保護登録センターを設置し、上記のガイドラインを遵守するなど、適正な個人情報保護を講じている事業者の登録及び個人情報保護マークの付与を行う「個人情報保護マーク」(図表)付与制度を運営しており、平成13年4月現在、28事業者が登録されている。しかしながら電気通信事業者の保有する顧客情報等の漏えいに関する報道等が相次ぎ、自主的な取組の限界が指摘されている。また、諸外国等においても電気通信分野における個人情報保護に関して法整備が進められてきている(図表)。

こうした状況の中、我が国では、平成11年11月に、高度情報通信社会推進本部個人情報保護検討部会において、「我が国における個人情報保護システムの在り方について(中間報告)」がとりまとめられた。この中間報告を受けて、平成12年10月に情報通信技術(IT)戦略本部個人情報保護法制

図表 我が国における平成12年度中の個人情報漏えいの主な事例

電気通信分野における個人情報の漏えい事例

平成12年10月に、大手電気通信事業者の代理店から約3万人分の顧客情報が流出している旨の報道がなされ、また、同年11月には、同社が顧客情報を代理店に提供していた旨の報道がなされた。

その他の個人情報の漏えい事例

日時	概要
平成10年7月～平成12年11月(11月に判明)	人材派遣大手企業が運営する障害者の雇用支援のサイトで行われていたオンライン署名に参加した人の名前や住所、電話番号などの個人情報が2年4ヶ月にわたり、外部から閲覧できる状態となり、105人分の個人情報が流出した可能性がある。
2月(5月に判明)	家庭用ゲーム機をインターネットにより予約した顧客の個人情報が、Web上で流出した可能性が判明した。(予約者に割り当てられた「受注番号」を入力すると、266人の顧客の氏名や届け先住所などを閲覧できる状態となっていた。)
8月	インターネット上での先物取引受託業者が、法人・個人の顧客約120カ所に一斉に電子メールを送った際、誤操作により、全送付先の顧客の名前とメールアドレスのリストを添付したことが判明した。
10月	九州のホテルが、顧客1500人に同社の新サービスを告知する電子メールを送信した際、誤って顧客の氏名と電子メールアドレスが本人を含めて全顧客にも見える形式であったことが判明した。
11月	大手教育出版企業の広告関連会社が運営している採用者向けの専用サイトを通じて応募した100人以上の実名、住所、電話番号や学歴などの個人情報がウェブサーバー上で、だれでも閲覧が可能な状態になっていた。URLが無関係な電子掲示板に掲載されたため、応募者にはいわずら電話が相次いだ。

各種資料より作成

化専門委員会において、「個人情報保護基本法制に関する大綱」が取りまとめられ、本大綱を受け、第151回通常国会において、「個人情報の保護に関する法律案」が提出された。

一方、総務省においても、電気通信分野における個人情報保護法制の在り方について検討するため、平成11年9月から「電気通信分野における個人情報保護法制の在り方に関する研究会」を開催し、平成12年12月にその最終報告書が取りまとめられた。電気通信分野においては、その公共性に加え、通信の秘密を取り扱う電気通信事業者の責務として、個人情報の保護が図られることに対する国民の期待は大きく、電気通信事業者の保有する個人情報漏えいに関わる事案が社

会的に大きな注目を集めたことは、その期待への裏返しであると考えられる。本報告書においては、電気通信分野における個人情報保護に関する「個別法」整備の要否や内容などについて検討し、その必要性を確認するとともに、現時点での方向性として、電気通信事業者に対する規制、個人（行為者）に対する規制、の2点を具体的イメージとして挙げている。今後、総務省では、「個別法」の整備に向けて、更に具体的な検討を深めていくこととしている。

図表 個人情報保護マーク



図表 諸外国等における法整備の現状

国名	規定	内容
米国	電気通信法（1996年）	電気通信事業者の守秘義務、サービスの提供上知り得た情報の利用制限、顧客のアクセス権、集計顧客情報の取扱い、加入者リスト情報の取扱い等について規定
EU	電気通信個人データ保護指令（1997年）	EU「個人データ保護指令」を具体化し補完するものとして、通信の秘密の保護、トラヒック・データ及び課金データの取扱い、通話明細、電話番号情報等の取扱いについて規定
イギリス	電気通信（データ保護及びプライバシー）規則（1999年）	トラヒック・データ及び課金データの取扱い、電話番号情報の取扱い、通話明細、発信電話番号通知サービスの提供のための条件等について規定
ドイツ	電気通信事業者データ保護令（TDSV）（1996年）	通信履歴の収集・処理・利用制限、発信電話番号通知サービスの提供のための条件、電話番号情報の取扱い等について規定
フランス	電気通信規則法及び関連デクレ（政令）（1996年）	通信内容の秘密の保護、電話番号情報の取扱い、発信番号通知サービス提供のための条件、その他データの収集・利用・外部提供に関する事項について規定

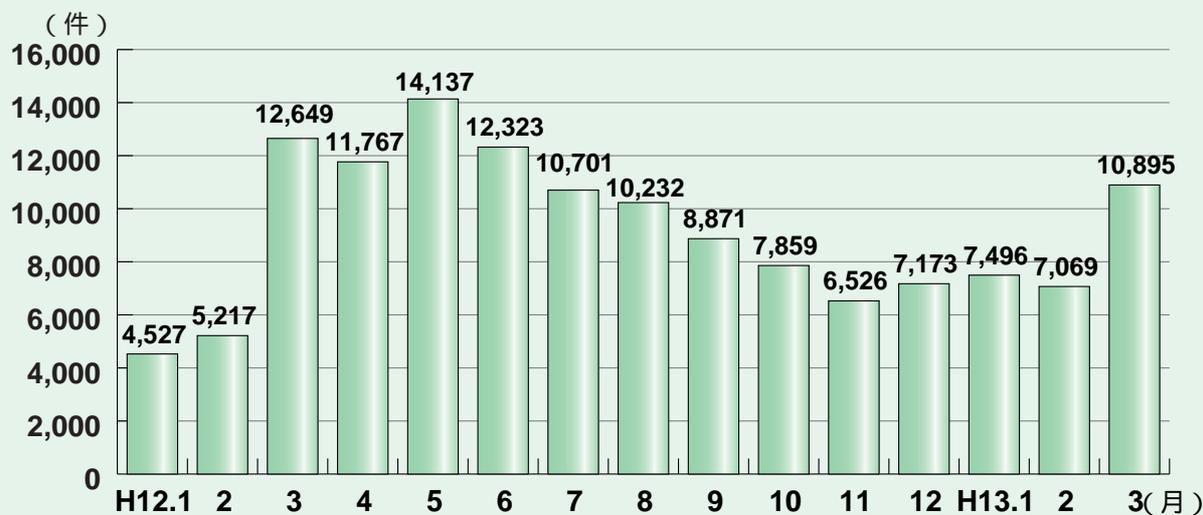
総務省資料より作成

コラム4 国際情報提供サービスに関するトラブル

平成12年初頭から夏にかけて、ホームページの閲覧中において、国際通話に自動的につながるよう設定されてしまうソフトウェアをダウンロードさせられ、多額の国際電話料金を請求される等の被害が続出した(図表)。国民生活センターには、「インターネットを始めたら、利用した覚えのない高額な国際電話の通話料金を請求された。」「インターネットで無料アダルトサイトをダウンロードして利用したところ、国際電話の通話料金を請求された。」等の相談が寄せられているとの報告がある。

これに対して、郵政省(現総務省)では、同年10月に、国際電気通信事業者7社に対し利用者周知等の対応を要請する等の対策を講じるとともに、パンフレットを作成・配布し、利用者に対し注意喚起を行っている。各事業者もそれぞれ対策を講じており、例えばKDDIでは、音声ガイダンスの導入、利用額が一定額に達した時点で随時請求書の送付、国際電話につながろうとすると警告を発してくれるチェックソフトの無料配布及び注意喚起のリーフレットを請求書に同封する等の対策を講じている。

図表 インターネットを利用した国際情報提供サービスに関する苦情・相談の発生件数(各社合計)



総務省資料より作成