「米国における個人情報漏洩の現状と対策」

渡辺弘美@JETRO/IPA NY

1. はじめに

インターネットは単なる通信や表現のツールにとどまらず、実生活に必要なサービスを提供するツールへと変化した。これまで以上に、消費者はオンライン購入に対する抵抗がなくなり、大抵の品物をネットで購入する一般消費者は確実に増えている。その一方で、金融機関もオンライン・サービスを拡張し、決済サービスまでオンライン上で処理できるようになっている。

しかし、便利さとは裏腹に、ネットがもたらす様々な問題が浮上しつつある。その中でも問題になっているのが、個人情報の漏洩である。気軽に入力した個人情報がいつの間にか第３者の手に渡り、勧誘セールスに利用されたり、最悪の場合は、詐欺に悪用されたりするというケースも出てきている。米国では、このようにネット詐欺が横行し、深刻な問題となっているのが現状である。こうした状況が深刻化すれば、一般消費者がネットに対する不信感を募らせ、市場の成長を妨げる要因にもなりかねない。

また、米国民には、それぞれ社会保障番号（Social Security Number : SSN）が与えられており、年金を受け取るまでこの番号が常に必要になる。SSN は電話などでの問い合わせの時にも、本人を確認するために使われているが、これが誰かの知るところとなれば、いとも簡単に身分をすり替えられるという恐怖がある。

もちろん、政府もこうした問題に手をこまねいているわけではない。様々な法律を制定し、ID セフト（ID 盗難）に対応しようと考えている。しかし、実際には、連邦政府、州政府ともに法の整備が後手にまわっているのが現状である。

特に、本年に入って、消費者の個人情報を専門に取り扱う情報ブローカーなどからの情報漏洩問題が次々と明らかになり、何らかの規制が必要ではないかとの議論が米議会で活発になっている。

ID セフトの全貌をつかむのは難しい。最近横行しているフィッシングは ID セフトの中でも被害規模が比較的わかっている分野である。これは、フィッシングの標的となるのが企業ではなくて一般消費者であるため、詐欺事件の報告などが表面に出てくるからである。

ところが、企業は自社のイメージダウンを憚り、同様の事件が起きても外部への報告を躊躇する傾向にある。このため、大企業で ID セフトが起きても内部でもみ消されてしまい、正確な統計データとして反映されなくなってしまう。

したがって、ここで取り扱う事例はまさに氷山の一角でしかならないことを認識しておかなければならない。

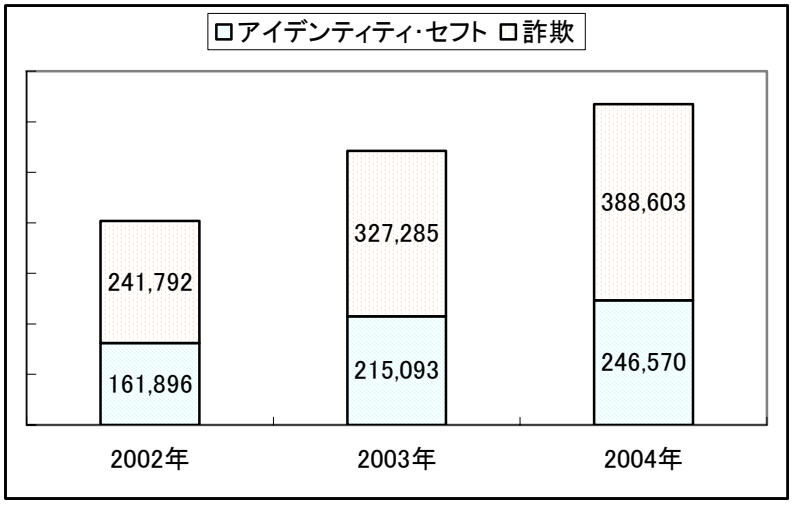
2. 個人情報漏洩の傾向

(1) 被害の状況

近年は IT の発達を背景に、SSN、生年月日、住所、クレジットカード番号や銀行口座番号といった個人情報の収集と共有が、効率的かつ簡便に行われるようになっている。こうして集められた情報は、犯罪防止や捜査活動、あるいはマーケティングの一環として個人の嗜好やニーズを把握するために活用されるなど、公共の安全や利便性向上に活用されている。その一方で、個人情報の収集の方法や取り扱いをめぐり、プライバシー侵害や悪意を持った人物や団体による情報の漏洩や盗難、そして、それらを悪用したフィッシングなどの詐欺・犯罪行為が深刻な社会問題となっている。

米連邦取引委員会（FTC）が本年２月に発表した最新の報告によると、FTC に届け出された ID セフトと詐欺に関する苦情件数は、2002 年の 40 万 4000 件から 2004 年は 63 万 5000 件に増加し、被害額は５億 4700 万ドルに達した。

ID セフトと詐欺に関する苦情件数の推移（単位：1000 件）



(2) 個人情報盗難の手口

個人情報の流出・盗難の手口は、郵便物や財布の盗難といった原始的なものから、情報が保存されたパソコンの盗難、システムへの侵入、フィッシングなど、IT の進歩を逆手に取った大掛かりなものまで多岐にわたる。

① フィッシング

フィッシングの詳細については、昨年 9 月の「ニューヨークだより」で報告しているが、最近、ますますその被害は広がっている。

フィッシング対策の団体「Anti-Phishing Working Group（APWG）」によると、本年 2 月に同団体に報告されたフィッシング・サイトの数は 2625 件で、昨年７月から 2 月までの月平均増加率は 26%である。これら偽のウェブサイトは短期間に登場と閉鎖を繰り返しており、サイトの稼動平均期間は 5.7 日、最長期間は 30 日であった。2 月に届け出されたフィッシング・メールの種類は 13,141 件で、７月からの月平均成長率は 26%となっている。

最もフィッシングの標的にされやすい業界は金融サービス業界であるが、最近では、本年 7 月 16 日に出版予定の人気小説、ハリーポッター・シリーズの最新版の電子コピー販売を騙ったサイトが登場し、ユーザに銀行口座やクレジットカード番号などを入力させる詐欺事件が発生した。この事件では筆者サイトと同小説のファンサイトのユーザが詐欺行為を発見し、サイトの早期摘発につながった。

フィッシングに対して IT ベンダーも行動を起こし始めた。本年 3 月末に、マイクロソフトはフィッシング・サイトの運営者を相手取って 117 件の訴訟を起こした。訴訟は被告名を特定しない「John Doe」形式で、ワシントン州西部地区米連邦地裁で起こされた。

また、最近では、フィッシング(Phishing)が釣り（Fishing）に基づいた造語であるのに対して、農業(Farming)をもじったファーミング(Pharming)と呼ばれる手口も現れている。これはフィッシングのようにユーザに対して偽りのメール（餌）を送って悪意あるウェブサイトに導く必要はない。DNS(ドメイン・ネーム・システム)サーバーを毒で汚染させる DNS ポイズニングを用いることで、餌なしで、ユーザが本来訪れようとしているウェブサイトから悪意あるウェブサイトへ自動的に誘導するものである。

② ハッキング

ハッキング（クラッキングとも呼ばれる）は、企業の情報システムなどにアクセスし、従業員や顧客の個人情報を不正に持ち出す手口として利用されている。大規模な情報システムがハッキングされた場合、一度に大量の情報が流出し、悪用された場合の被害が大きくなる可能性が高い。

本年１月には、バージニア州のジョージ・メイソン大学がハッキング被害に遭い、学生や教授陣など３万人の氏名、写真、SSN など個人情報が持ち出された。昨年 10 月には、カリフォルニア大学バークレー校に設置されたカリフォルニア州政府のデータベースが攻撃され、州民 140 万人の個人情報が流出した可能性のあることが明らかになった。

カリフォルニア州では、2002 年４月にも同州職員 26 万 5000 人分の氏名、給与情報、SSN などが保存されていたコンピュータがハッカーの侵入を受けた。この事件は盗難規模の大きさやセキュリティ対策の不備が注目を集め、同州で

2003 年７月に施行された個人情報保護法を成立させるきっかけになった（後述）。

民間でもハッキングによる被害は出ている。たとえば、1630 万人の顧客を持つ携帯通信事業者 T モバイルは 2003 年後半にハッキングを受けた。カリフォルニア州サンタ・アナ出身のコンピュータ技術者ニコラス・リー・ジェイコブセンが７ヵ月にわたり、携帯電話大手 T モバイルのネットワークに侵入していたという。その結果、顧客 400 人の名前と SSN が盗まれた。さらに、捜査していた検察局の捜査員を含む数百人の電子メールやコンピュータ・ファイルまで盗み読みされていたことが発覚し、当局の担当者が引責辞任する事態にまで発展した。

さらに、本年２月終わりには、この T モバイルを利用していたセレブ女優のパリス・ヒルトンの携帯端末から友人である著名人たちの携帯電話番号が盗まれ、ネットに流出した。パリス・ヒルトンは以前にポルノグラフィックな映像をハッキング、流出されたことがあり、また話題を提供することになった。

また、機能がより高度化している検索エンジンも使いようによっては問題となりうる。たとえば、グーグルが提供する強力な検索機能を使って個人情報などをウェブサイトから引き出す行為は、「グーグル・ハッキング」と呼ばれている。昨年にはブッシュ政権に反対する政治活動団体、MoveOn.org の会員リストがグーグル・ハッキングによって流出した事件がある。同団体の会員専用のウェブサイトで設定が誤っていたため、メーリングリストの購読者名、電子メール・アドレス、住所などの情報が漏洩してしまった。

③ スパイウェアの悪用

ユーザのキー・ストロークを読み込んだり、ネット上の行動を監視したりすることで個人情報を収集し、第３者に送信するスパイウェアが話題となっているが、この最大の問題は、近似する「アドウェア」とどう区別するかである。両方とも機能の仕方はまったく同じだが、一方は個人情報の窃盗を目的とし、片方はオンライン広告に必要な情報を吸い上げるのが目的となっている。

アドウェアが非難を浴びるきっかけとなったのは、クラリア（Claria）社が開発したソフト「ゲイター（Gator）」である。同ソフトは、音楽ファイル交換ソフトの「カザー（Kazza）」などとバンドルされてダウンロードされる。ユーザが気づかずにダウンロードしている場合が多く、消去も非常に困難だ。これに対して、ゲイターをスパイウェアと非難するサイトなどが登場したが、これに対してクラリアが訴訟を起こして和解した経緯がある。

また、クラリア社の幹部が、国土安全保障省(DHS)内に新たに設置されたプライバシー諮問委員会のメンバーに任命されたことも話題を呼んでいる。同委員会の目的は、同省が国家安全のために情報を収集していく際に、米国市民および海外からの訪問者の個人情報に関するプライバシーを守るための提言を行っていくこととされている。委員会は 20 人のメンバーから構成されており、コンピュータ・アソシエーツ、IBM、オラクルの幹部も名を連ねている。

ネットワーク・セキュリティ・ソリューション開発の WatchGuard Technologies が全米の IT 管理者 154 人を対象に実施した調査では、回答者の 66%が、本年の最大のセキュリティ脅威として、ウイルスやフィッシング攻撃を差し置いてスパイウェアを挙げた。

また、ISP 大手のアースリンクによると、スパイウェアはネットワークに接続されたパソコンの約 90%にインストールされており、１台あたり平均 25 種類のスパイウェアが稼動しているという。2004 年は、特にスパイウェアの中でも危険度が高いとされる「システムモニタ」や「トロイの木馬」が急速に蔓延した。発見されたシステムモニタの数は第１四半期の 21 万個から第４四半期は 27 万個に増加、同じくトロイの木馬は 13 万個が 25 万個に増えたという。

民間企業もこうしたスパイウェアの浸食を防ごうと努力し始めている。調査会社フォレスター・リサーチ社によると、企業の 65%が本年、スパイウェア対策に投資を計画しているという。同社が北米 185 社の技術系投資担当者を対象に調査を行ったところ、大企業の 69%がスパイウェア防止対策への投資を計画していることがわかった。これに対して、中小規模企業では 53%にとどまった。また同社による調査では、スパイウェアの対策不備も浮き彫りになった。たとえば、回答企業の約 40%がスパイウェアの感染状況を把握していなかった。また、把握している企業のうち、システムの 17%がスパイウェアの被害に遭っていた。同社は向こう 12 ヵ月にこの割合は 25%に悪化すると予想している。

また、企業の 80%がスパイウェア対策ツールを導入しているが、未だ体系だった対策がとられていないのが実情である。スパイウェア対策ツールは、マカフィー（McAfee）とラバソフト（LavaSoft）ほか、無数のソフト会社が提供している。

マイクロソフトも１月からスパイウェア対策ソフトを試験的に配布し始めたが、同社の対策ソフトを攻撃する新たなプログラム「バンクアッシュ A トロージャン」が登場し、泥沼化しつつある。バンクアッシュ A トロージャンは、対策ソフトのファイルを削除し、警告メッセージが表示されないようにする。さらにプログラムすべてを消去してしまうという。

スパイウェアに対処するために議会も動きだした。米下院は 2004 年 10 月、スパイウェア規制法案を 399 対１の圧倒的な賛成多数で可決した。同法案では、スパイウェアを使ったパソコンユーザの行動監視活動やマーケティング活動、ウイルス駆除ソフトの無効化、ブラウザのホームページ設定改竄などの行為を違法とし、さらにスパイウェア配信会社に対し、事前にソフトウェアのインストールについてユーザの同意を得ることを義務付けた。このほか、違反者には最大 300 万ドルの罰金刑を課すことを定めた。

一方、上院では委員会レベルで上院版スパイウェア禁止法の修正法案を承認したが、昨年中の上院本会議での決議はならなかった。

年が明けて、下院エネルギー商業委員会が公聴会を開催するなど、立法化を目指す動きは続いている。しかし、オンライン広告企業などの技術系企業が法案の適用範囲は広すぎるとし、クッキーなど合法的なソフトウェアやその機能の使用

も違法になるなどと懸念を表明しており、法案提出議員らが内容の見直しを検討している。

(3) その他

これまで述べてきたような IT 技術を駆使した盗難手口が注目を集める中、個人情報が記載された書類や、保存されたパソコンを物理的に持ち出すなど、原始的な手口によって情報が漏洩するケースも相変わらず多い。

Council of Better Business Bureaus と Javelin Strategy & Research が米国人 4000 人を対象に電話アンケートを行い、個人情報の窃盗被害にあった 509 人について被害の詳細を聴取してまとめた。

両社が本年１月 26 日に発表した「2005 年個人情報詐欺調査報告（2005 Identity Fraud Survey Report）」によると、2004 年の個人情報詐欺の被害者数は 930 万人で、被害総額は 526 億ドルだった。このうち、詐欺につながる個人情報がどのような手段で盗難されたかを調べたところ、スパイウェアなどコンピュータを利用した例は全体の 11.6%にすぎなかった。最も多かったのは、盗難または拾得した財布や小切手帳、クレジットカードを悪用した例で、これに続いて個人情報にアクセスし得る立場にある友人・知人・親族経由、従業員経由、オフライン取引が続いた。

カリフォルニア州のデルタ血液銀行は昨年 12 月、献血者情報を保存したノートブックが盗難に遭い、献血者 10 万人に氏名、生年月日、SSN といった個人情報漏洩の恐れがあることを通知した。

これに先立つ 10 月には、金融サービス大手ウェルズファーゴの顧客情報を保存したパソコン４台が盗まれ、さらに、同年６月にはカリフォルニア大学ロサンゼルス校で献血者 14 万 5000 人の情報を保存したノートブックが、施錠した車両から盗み出されたことが明らかになるなど、大量の個人情報を所有する金融機関や血液銀行が盗難の標的とされるケースが多い。

また、昨年ハッキング被害（前述）を受けたばかりのカリフォルニア大学バークレー校では、本年 3 月に、10 万人近くの卒業生、大学院生、過去の入学志願者の個人情報が記録されていたノートパソコン１台が盗難にあった。

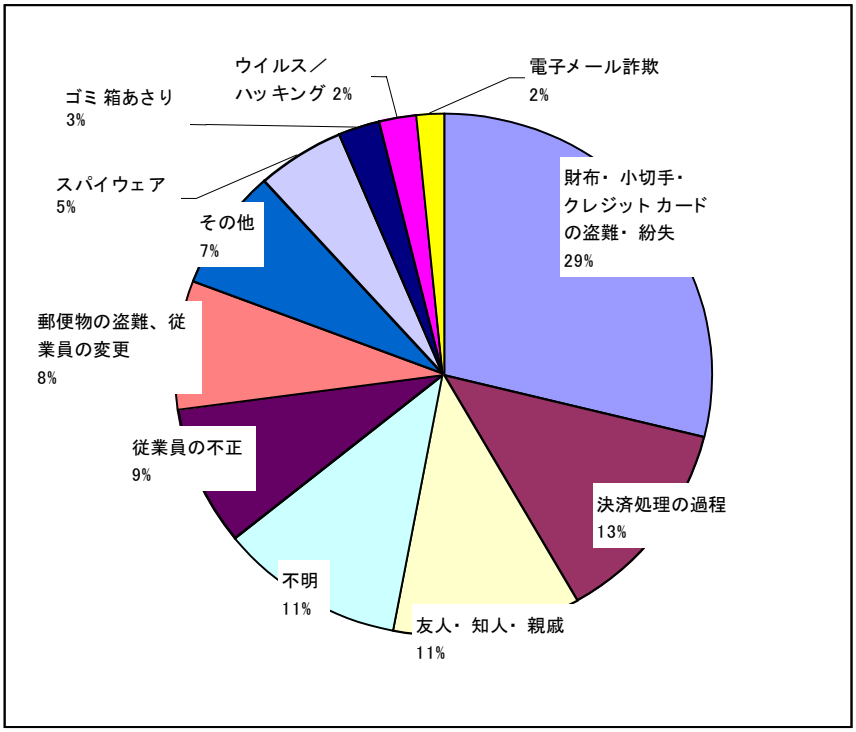
こうしたパソコンの盗難による情報漏洩は昔からあった。たとえば、2002 年 12 月には米国国防総省と契約するベンダーから兵士 50 万人強の個人情報が保存されたハードディスクが持ち去られる事件があった。

また、近年では、内部関係者が関係した情報漏洩が問題になっている。悪意を持った従業員や関係者がパスワードを使って個人情報が蓄積されたシステムにアクセスし、情報を盗み出そうとすれば、それを阻止するのは難しい。また、悪意はなくても情報セキュリティに対する認識の欠如から不用意に情報をダウンロードして複製し、携行したりすることが、情報が外部に漏洩するきっかけになることもある。

シンクタンク Ponemon Institute がフォーチュン 1000 の 163 社を対象に行った調査では、約７割の企業が内部関係者によるセキュリティ被害を報告している。

昨年 12 月には、アップルコンピュータが開発中の次世代 OS の事前公開版と楽曲プレーヤに関する情報を不当に漏洩したとして、同社は内部関係者とパートナーを相手取り２件の訴訟を起こした。アメリカ・オンライン、マイクロソフト、シスコシステムズといった IT 関係大手も、内部関係者が関与した情報漏洩を報告している。

個人情報盗難の手口



外部関係者が取引先企業や通信などサービス会社の社員になりすまして企業内に侵入し、もしくは電話や電子メールの内容を傍受してパスワードを盗み、情報ネットワークに侵入するといった事件も増えている。

こうした状況を反映し、企業では情報セキュリティ・ポリシーの徹底を急いでいるほか、不用意な情報の複製やダウンロードを防止するための技術も開発されている。

ネット社会ではこれまでなかったケースも登場している。それは、オンライン情報のずさんな管理や、システムに何らかのバグが発生することで情報が流出してしまうケースである。たとえば、電子メールでニュースを配信している会社があやまって会員のメール・アドレスを CC で出してしまうといった具合だ。これは、意図的に仕組まれたというものではなく単純な人為的ミスによるものだが、流出したメール・アドレスがスパムメールなどに悪用されてしまう。

3. 最近の個人情報漏洩事件とその行方

米国では年明けから情報ブローカーなど大手企業による大規模な個人情報漏洩事件が相次ぎ発覚し、個人情報保護対策として新たな立法措置を求める議論が活発化している。

(1) 主な事件の概要

① チョイスポイント（ChoicePoint）

消費者データを公文書や民間企業などから収集し、企業や政府機関、法執行機関などに販売する情報ブローカー大手のチョイスポイントは、昨年 10 月に同社が保管する 14 万 5000 人分の個人情報が盗難された可能性のあることを本年 2 月に明らかにした。本件では、犯人は他で盗難した情報を悪用して合法的に存在する企業になりすまして同社で約 50 件の顧客口座を開設し、個人情報を購入していた。この結果、本件に起因すると考えられる ID セフト事件が３月始め時点で 750 件報告されたという。

チョイスポイントは当初、カリフォルニア州の個人情報保護法（後述）に基づき、カリフォルニア州民３万 5000 人にクレジットカード番号や SSN などの個人情報が流出した可能性を通知した。だが、その後、他州州民への通知がなかったことが批判を受け、最終的にカリフォルニア州民を含む全米 14 万 5000 人分の情報が漏洩した可能性を明らかにした。

本件では昨年 10 月の時点で攻撃を察知したチョイスポイントが当局に事件を通報、疑わしい口座を閉鎖し、サービスサイトの認証システムを強化するなどの対策をとった。同月に 1 人が逮捕されたが全面的解決には至っていない。

事件を受けて本年３月、チョイスポイントは、「一部個人情報販売事業からの撤退」、「個人情報販売条件の厳格化」、「顧客の身元確認手続の強化」、「個人情報保護対策を専門に扱う社内組織の設置」などを柱とする個人情報保護対策を発表した。このうち販売条件の厳格化については、販売を、「保険会社や雇用主からの情報照会など、消費者が販売先企業への情報開示を承諾している場合」、「消費者とすでに何らかの取引のある大手企業顧客が口座開設時の身元確認や保険のクレーム処理または詐欺防止対策などに利用する場合」、「政府および本人から情報開示の要請があった場合」などに限定した。

本件では FTC や一部の州の司法長官事務局が捜査を開始したほか、米証券取引委員会（SEC）が、昨年暮れに情報漏洩事件が発覚して以降の同社幹部２名による同社株式売却を調査している。また、ロサンゼルスではある女性が消費者保護を怠ったとして業務上過失と詐欺で同社を訴えるなど、多方面に影響を及ぼしている。

② レクシスネクシス（LexisNexis）

ニュースメディアが出版した情報や公文書情報を多角的に収集、提供する情報サービス大手、レクシスネクシスは本年 3 月始め、同社が保管する顧客３万人の住所氏名、社会保障番号など個人情報が盗難された可能性があることを明らかにした。

同社によると事件は約２ヵ月前に発生し、同社のシステム監査の結果、発表の２週間ほど前に分かったという。犯人は不正に入手したパスワードを使い、個人情報を保管したファイルにアクセスしていた。

３月 10 日付けニューヨークタイムズ紙は、関係筋の話として、米連邦捜査局（FBI）や財務省が本件の捜査に乗り出したと報道している。３月半ば時点では本件に起因すると考えられる ID セフトなどの事件は報告されていない。また、パスワード流出の手口やレクシスネクシス内部関係者による犯行への関与といった具体的な情報は、一切明らかにされていない。

③ バンクオブアメリカ（Bank of America）

大手銀行のバンクオブアメリカは本年３月はじめ、連邦政府職員 120 万人の社会保障番号やクレジットカード番号を含むデータのバックアップ用テープが２月の移送中に紛失したことを明らかにした。本件についても具体的な手口などは明らかにされていない。

(2) 議会での議論

前述のように、本年は年明けから大規模な情報漏洩事件が相次ぎ明らかになったことを受け、米議会では３月になってから上院銀行委員会や下院エネルギー・商業委員会の商業・貿易・消費者保護小委員会が事件を取り上げた公聴会を開催した。また、一部議員が個人情報保護を目的とした法案を提出するなど、法整備に向けた議論が活発化している。

米国では、企業、特に情報ブローカー企業による個人情報の取り扱いを包括的に規制するような法律や、それらを監督する中央機関は存在しない。金融、医療など特定の業界や特定の状況における個人情報の取り扱いに関する規制や、カリフォルニアの個人情報保護法など州レベルの規制はあるが、焦点が極度に細分化され、さらに州によって規制の内容やレベルに差が生じている（後述）。その結果、個人情報保護対策は業界や企業の自発的努力に依存する傾向が強いというのが現状である。

これらを踏まえ、議会では主に以下の論点につき議論されている。

- 個人情報を取り扱う企業を対象とした「個人情報取り扱い基準」の制定

企業が個人情報を収集・保管・販売（個人情報販売先企業・機関の身元確認手続を含む）を行なう際に遵守されるべき規則の制定。

- 企業の個人情報保護対策を監督する中央機関の確立
  FTC に業界をまたいだ監督権限を与える意見が数案出されている。

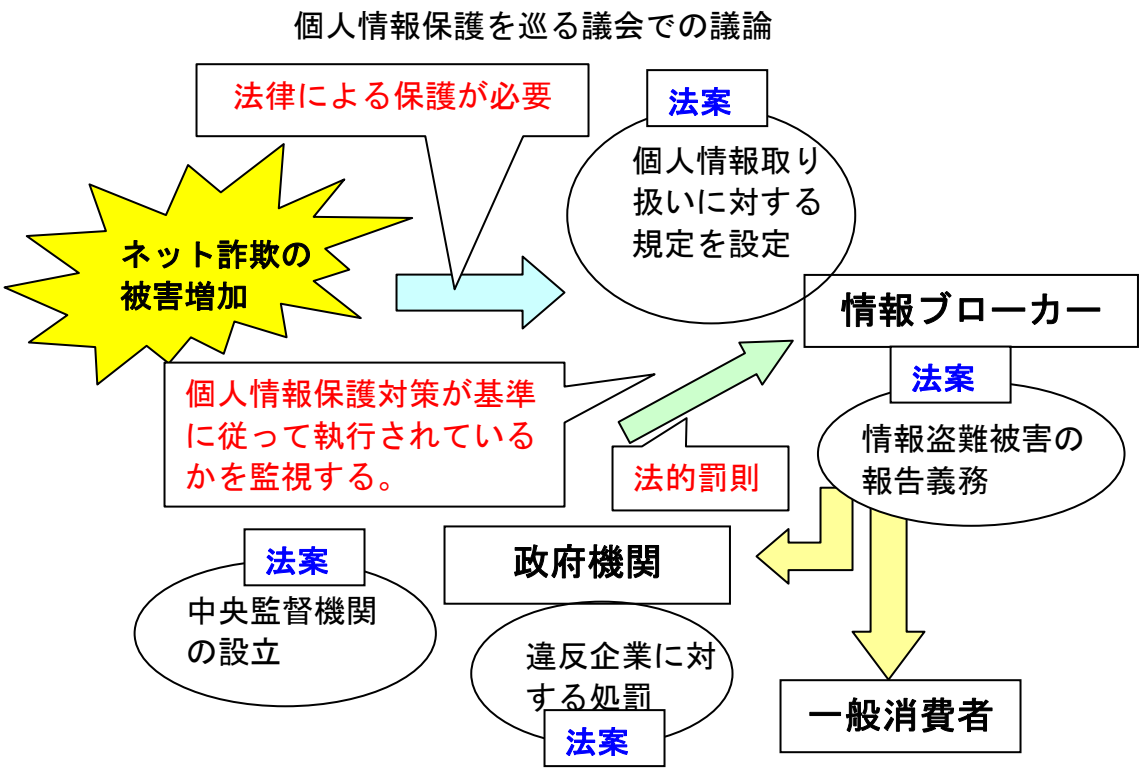
- 個人情報流出に関する個人や法執行機関への報告の義務化
  カリフォルニア州の個人情報保護法の内容を全米に適用するもので、米国で事業活動を行なう企業・団体に対し、個人情報漏洩事件の発生について被害者への通知を義務付ける。チョイスポイント事件で同社が当初、事件の通知をカリフォルニア州民に限定したことや、上記の法律が 2003 年７月に成立して以来、カリフォルニア州で個人情報盗難事件の報告が増えたことを踏まえ、事件の通知や開示を義務付けないと企業はそれらを隠蔽する可能性が高いことを危惧して提案された。通知のタイミングや方法（電子メール、HP 公開など）などが検討課題。

- 個人情報保護対策に違反した企業に対する罰則の制定
  罰則の制定や厳罰化を、企業にセキュリティ対策を急がせる動機付けとする。

中でも、個人情報を取り扱う企業を対象とした法案は注目を浴びている。法案の一部は 2003 年にも提出されたが審議見送りなどのため、これまで活発に議論されることはなかった。しかし、本議会では FTC 委員長やチョイスポイント幹部などを招聘した公聴会が開催され、さらに今後も法案提出を予定する議員もいるなど、これら法案について具体的な審議が進められるものと期待される。

一方、信用調査会社を含む情報ブローカー業界は、歴史的に情報取り扱い方法、取り扱い情報、販売先などについて政府の介入にロビー活動などを通じて強硬に反発しており、業界自主規制を重視する姿勢を一貫してとっており、今後の立法化作業も難航が予想される。

また、個人情報盗難犯や ID セフト犯に対する刑罰の厳格化を望む意見も出されている。だが、個人情報盗難や ID セフトは犯人検挙が難しく、厳罰化の効果を疑問視する声もある。業界団体 APWG によると、フィッシング・サイトのほとんどは海外のサーバで管理されていることなどが捜査の障害となっているためである。カリフォルニア州サクラメント郡検事は ID セフト事件の犯人検挙率は 11%と低く、ロサンゼルス郡では昨年報告された２万件の事件のうち、犯人起訴につながったのはわずか 220 件だったと指摘している。



(3) 主な法案

上記の情報ブローカー企業に対する法案を含め、今議会に提出された情報漏洩に関する主な法案のポイントを紹介する。

① 包括的プライバシー法案（Comprehensive Privacy Act）

カリフォルニア州選出のダイアン･ファインスタイン上院議員（民主党）が提出。個人情報を保護し、SSN と運転免許証番号の販売と開示を規制する全米レベルの法律を制定する内容。具体的に、SSN など機密性の高い個人情報の販売にあたり消費者から事前承認を得る（オプトイン）ことと、機密性の低い情報については消費者に販売禁止を選択できる権利を与える（オプトアウト）ことを企業に義務付ける。

② SSN 悪用防止法案（Social Security Number Misuse Prevention Act）

カリフォルニア州選出のダイアン･ファインスタイン上院議員（民主党）が提出。個人の同意を得ない SSN の不特定多数への販売と開示を規制する。

③ 個人情報漏洩リスク通知法案（Notification of Risk to Personal Data Act）

カリフォルニア州選出のダイアン･ファインスタイン上院議員（民主党）が提出。企業や政府機関に対し、データベースが外部から攻撃され、SSN や運転免許証番号、クレジットカード番号などの個人情報が盗難された可能性を個人に通知することを義務付ける。

④ ID セフト防止と被害者救済法案（Identity Theft Prevention and Victim Recovery Act）

ニュージャージー州選出のジョー･コーザイン上院議員（民主党）が提出。被害者への事件発生の通知に加え、FTC に情報収集およびブローカー企業を監督する権限を与え、これら企業が遵守すべきシステムのセキュリティ要項や個人情報取り扱い基準などの指針や規制案を作成させる。また、企業の最高責任者（CEO）または最高コンプライアンス責任者（CCO）に、これら規制へ遵守していることを証明させる。

⑤ 情報保護・セキュリティ法案（Information Protection and Security Act）

フロリダ州選出のビル・ネルソン上院議員（民主党）、マサチューセッツ州選出のエド・マーキー下院議員（民主党）らが提出。FTC に情報ブローカー企業を監督させ、それら企業が保有する個人情報を保護、非承認の情報アクセスや使用などを防止するための規制を作成する権限を与える。また、消費者が自分についての誤情報を修正できるようにする。

⑥ 反フィッシング法案（Anti-Phishing Act of 2005）

バーモント州選出のパトリック・リーヒー上院議員（民主党）が提出。犯罪目的でフィッシング・サイトへのリンクが貼られた電子メールを意図的に送信することと、フィシングサイトそのものの設置を違法とする。

(4) 州レベルの動き

最近の一連の事件発生を受け、州レベルでも個人情報保護対策が進められている。たとえば、消費者にクレジットヒストリー（過去の金融機関の利用履歴）の公開を禁止する権利を与える「セキュリティ凍結」について議論されている地域が多い（既にカリフォルニア州、テキサス州ではセキュリティ凍結は法律で認められている）。いったんセキュリティ凍結が発効されると、金融機関の口座開設審査などで必要とされるクレジットヒストリーの公開が禁止される。この結果、たとえば ID セフト犯が金融機関などで盗難した情報を悪用して口座を開設しようとしても口座を開くことができず、盗んだ情報の使い道が無くなる。ウォール・ストリート・ジャーナルによると、本年はイリノイ州、コロラド州など約 20 州がセキュリティ凍結の導入を検討、または検討中であるという。

セキュリティ凍結は個人が合法的に口座を開く際の妨げにもなるが、時間と手間はかかるが必要に応じて凍結と解除を繰り返すことは可能である。消費者団体はセキュリティ凍結について、ID セフト事件による被害発生を防止するための最も有効な対策の 1 つと評価している。

4. 個人情報保護に関するこれまでの連邦政府、州政府の取り組み

個人情報の盗難と、それを悪用した犯罪の被害は、FTC が当局に寄せられた苦情などを基に状況を発表しているが、その全貌は正確には把握されていない。これは、米国には個人情報盗難に起因する詐欺行為などの犯罪を、一括して扱う機関が存在しないためである。また、米国には包括的なプライバシー保護法はなく、代わりに連邦および州レベルで金融、医療などの分野別にプライバシー保護に関する法律が制定され、様々な機関がそれらを監督、実施している。

この結果、同分野の法制は詐欺や犯罪行為の内容や、発生した場所などによって様々な法執行機関が関わり複雑な構造となっている。ここでは個人情報保護に関わる連邦および州レベルの主な法律を分野別に紹介する。

⑴ 連邦政府の取り組み

① 一般分野

＜FTC Act Section 5＞

市場における不公正または詐欺的な行為や慣行を禁止する連邦法である FTC 法の条項の 1 つ。個人情報の保護や取り扱いなどを定めた企業のプライバシー規約について、同法に照らし合わせて違反を摘発する権限を FTC に与えた。

同法に基づき、たとえば、ペット用品大手のペトコ・アニマル・サプライズが、同社のウェブサイト上で「顧客情報の保護は我々の最優先項目であり、同サイトでのクレジットカード番号の入力は安全で、全ての情報は暗号化され守られてい

る」などと宣言していたにも係わらず、プライバシー規約に反して十分なセキュリティ対策を講じていなかったとして、FTC は同社を同法違反で摘発した。両者は 2004 年 11 月、ペトコが同社ウェブサイトに包括的なセキュリティプログラムを導入することで和解している。

また、2001 年には消費者擁護団体「エレクトロニック・プライバシー・インフォメーション・センター（EPIC）」の訴えを受けて、マイクロソフトのウェブサービス「パスポート」を経由して収集された個人情報のプライバシー保護とセキュリティ対策に関する調査に着手した。この件では、2002 年にマイクロソフトが包括的セキュリティ対策を導入することで和解している。

＜電気通信プライバシー法（Electronic Communications Privacy Act of 1986）＞

1968 年に制定された連邦通信傍受法を修正したもの。電子メール、携帯電話、コンピュータ通信といった特定の電気通信にまでプライバシー保護の適用範囲を拡大した。通話履歴へのアクセスにも制限を設けた。

＜コンピュータ詐欺と悪用禁止法（Computer Fraud and Abuse Act of 1984）＞

「保護されたコンピュータ」への権限のないアクセスを違法とした法律。保護されたコンピュータには、政府所有のコンピュータ、州間商取引や金融機関によって使用されるコンピュータが含まれる。また、コンピュータ・パスワードの不正取引と、保護されたコンピュータの破壊も禁止した。

② オンライン関係

＜ID セフト防止法（Identity Theft and Assumption Deterrence Act、Identity Theft Act）＞

ID セフトに関する問題の増加を受けて、1998 年に制定された法律。法的権限がないにも関わらず、意図的に連邦法や州・地方法に違反する行為を行う、またはそれらを助長する目的で他人の個人情報を利用・譲渡する行為を連邦犯罪に指定し、さらに個人情報の窃盗に対する罰則を強化した。これにより、同法の違反はシークレットサービスや FBI といった連邦捜査機関の捜査対象となり、司法省による起訴対象とされた。

＜児童オンライン・プライバシー法（The Children’s Online Privacy Protection Act、COPPA）＞

オンライン上で児童から収集される情報や、こうして収集された情報の取り扱いについて保護者に監督権や決定権を与える目的で 1998 年に制定・公布され、2000 年４月に施行された。13 歳未満の児童から個人情報を収集するウェブサイトの運営会社に対し、「ウェブサイトにプライバシーポリシーを掲載する」、「児童からの情報収集について保護者の同意を得る」、「収集した情報を第３者に開示するにあたり、保護者の同意を得ること」、「保護者に児童の個人情報に

アクセスさせ、必要に応じて情報削除や将来の情報収集について事前拒否できるようにする」ことなどを義務付けた。

③ 金融関係

＜金融制度改革法（Gramm-Leach-Bliley Act, GLBA）＞

1999 年に議会で可決された金融サービス関連法。その中で、銀行、証券会社、保険会社、その他金融製品やサービス提供会社など金融機関が守るべき、包括的な個人情報取り扱い規制を定めた。

内容は、「金融プライバシー規制（金融機関による個人情報の収集と開示について）」、「セーフガード規制（顧客情報保護を目的とした、管理的・技術的・物理的セーフガードの設計・導入・運用について）」、「プリテクスティング条項（プリテクスティングとして知られる、身元を偽った個人情報の収集について）」の３つに大別される。このうち金融プライバシー規制、セーフガード規制について、８つの連邦機関と州政府に施行に関する権限を与えた。

具体的には、金融業界団体に対し、顧客情報保護に関するガイドラインの策定を義務付け、金融機関に対しては、顧客に第３者との個人情報の共有に関する事前拒否権（オプトアウト）を与えることと、プライバシーポリシーを最低年に一度開示することを義務付けた。また、プリテクスティングを犯罪行為とした。

＜公正・正確信用取引法（The Fair and Accurate Credit Transactions Act of 2003、FACTA）＞

1970 年に成立した公正信用取引法（Fair Credit Reporting Act、FCRA）の修正法案として 2003 年に可決された。FCRA はクレジット・ビューローに代表される信用情報機関（Consumer Reporting Agencies、CRA）や、ここで収集し、販売される個人信用情報（コンシューマー・レポート）の取り扱いについて主に規定したもので、具体的には、「収集された情報の開示を、合法的な必要性がある使途に厳しく制限する」、「不正確または不完全な情報について、個人に内容の再調査や修正を請求する権利を認める」などを定めた。

一方、ID セフトによる被害の増加を受けて、FACTA では、ID セフトの防止と被害者救済を目的とした条項が追加された。具体的には、CRA に対し、「詐欺によって生じた（傷が付いた）信用情報の開示を拒否する権利」、「詐欺を行うために利用された文書のコピーを請求する権利」などについて被害者に通知することを義務付けた。

④ 医療関係

＜患者プライバシー法（Standards for Privacy of Individually Identifiable Health Information）＞

患者のプライバシー保護に関する全米基準を策定し、さらに患者による医療記録へのアクセスを改善する目的で、1996 年に成立した医療保険の相互運用性と説明責任法（Health Insurance Portability and Accountability Act of 1996、HIPAA）によって制定された法律。2001 年４月に発効した。

保険会社、ヘルスケア・クリアリングハウス、医療従事者による医療記録の取り扱いに制限を設けたほか、患者のプライバシー保護を目的に、患者の医療記録の閲覧や使用目的を治療、医療従事者・機関への支払い処理、公衆衛生保護及び公安機関への提出に限定し、さらに、上記以外の人物や機関との情報開示には患者の書面による承諾が必要とした。

⑤ その他

＜リアル ID 法（Real ID Act）＞

2004 年２月に米下院で可決した法案。州政府に対し、連邦政府が認めた電子 ID カードを成人に発行することを義務付ける内容で、運転免許証やその他 ID カードに対してデジタル写真と偽造防止機能を義務づける。今後は、国土安全保障省が規制の詳細を起案する予定。

同法案が制定されれば、州政府は個人に SSN の証拠提示を求め、それらを社会保障庁と確認することになる。さらに、生年月日や身元確認を示す文書などの個人情報を電子的に共有可能な規格で保存することも義務付けられる。

同法案では、連邦補助金の交付条件として、個人情報を関係機関で共有できるようにするために、州の車両管理局（Department of Motor Vehicles、DMV）のデータベースを連携することも定められている。

今のところ、ブッシュ政権が法案の成立を強く進めているが、プライバシー擁護団体からの激しい反発は必至と見られている。

＜運転者プライバシー保護法（Driver’s Privacy Protection Act of 1994）＞

州の DMV が管理する運転者の個人情報の開示と利用に制限を設けた法律。DMV の職員や下請け業者が故意に個人情報を開示・譲渡することを禁止した。

＜家庭教育の権利とプライバシー法（Family Educational Rights and Privacy Act of 1974）＞

連邦政府の資金援助を受けた教育機関が保有する教育関連の個人情報の開示に制限を設けた法律。開示可能な情報や、開示する場合の手続きなどを定めた。

⑵ 州政府の取り組み（カリフォルニア州の場合）

米国では、ほとんどの州で医療、通信など分野別に個人情報保護関連の法律が制定されている。ここでは、個人情報保護について先進的な取り組みで知られる

カリフォルニア州を例に取り、同州で施行された主な法律を紹介する。同州は、個人情報の盗難防止に積極的に取り組む州として注目を集めている。特に、個人情報保護法（後述）を成立させたことは、他州からも評価されている。しかし、その一方で全米で一番被害が大きいという事実もある。FTC によると、2004 年に米国で唯一、ID セフトの被害者数が 100 万人を超えたのが同州だった。言い換えると、昨年に個人情報を盗まれた被害者の 10 人に１人がカリフォルニア州の住民という計算になる。

同州がこれだけの盗難件数を抱えるのは、覚醒剤利用者が他州に比べて多く、売買に盗まれた ID が利用されていることが理由として指摘されている。また、個人情報保護法によって、企業が情報漏洩を州民に通知する義務が発生したため、事件の報告件数が増加したことも一因と見られている。

カリフォルニア州は、深刻化する ID セフトに対して、法的整備を進める一方で、全米で初めてサミットを開催している。

① 一般分野

＜個人情報保護法（civil code 1798.82）＞

カリフォルニア州で事業を行う個人または企業に対し、ハッカー攻撃などによって個人情報が盗難、または盗難された可能性があることが判明した場合に、それを迅速に公開するか、または住民に個別に通知することを義務付けた法律。氏名、および SSN、運転免許証番号、州 ID カード番号、クレジットカード番号などのいずれか 1 つが盗難された、または盗難された可能性がある場合に適用される。2003 年７月に施行された。

企業は従来、企業信用の低下などを懸念して個人情報の盗難を隠蔽、もしくは公開を遅らせる傾向があった。同法は被害者保護を優先したもので、施行を受けて大規模な情報漏洩や盗難が次々と明らかになった。また、同法では通知を怠ったり遅延させたりした企業に対する民間の訴訟を認めている。

＜電子盗聴法（Electronic Eavesdropping）＞

電話や携帯電話、ケーブルなどを利用したプライベートなコミュニケーションの電子的盗聴や記録を禁止した。違反者には最大１万ドルの罰金と最高１年の禁固刑が科せられる。また、ケーブル TV や衛星 TV 会社による加入者の自宅内で行われた会話の監視・記録、および加入者の視聴嗜好やその他個人情報を、加入者の書面による同意なしに第３者と共有することを禁止した。

② オンライン関係

＜オンライン・プライバシー保護法（Online Privacy Protection Act of 2003）＞

カリフォルニア州の住民に関する個人情報を収集するオンライン・サービスおよびウェブサイトの運営会社に対し、サイト上でのプライバシーポリシー開示と遵守を義務付けた。プライバシーポリシーでは、サイト訪問者から収集する情報と、こうして収集された情報をどのような第３者（カテゴリー）と共有するかを開示することが定められた。同法に違反したサイト運営会社は、民事裁判で訴えられる可能性がある。2004 年７月に発効した。

＜スパイウェア禁止法（Consumer Protection Against Computer Spyware Act）＞

カリフォルニア州内にあるコンピュータを対象に、権限を持たない人物が故意に特定のソフトウェアをインストールしたり、提供したりすることを禁止した。特定のソフトには、コンピュータを乗っ取る、あるいは個人情報を収集するような機能を持ったソフトが該当する。

③ 金融関係

＜金融情報プライバシー法（Financial Information Privacy Act）＞

金融機関が個人の非公開情報を、本人の同意を得ること無しに第３者と共有・販売することを禁止した。さらに、金融機関に対し、「個人情報を第３者と共有するにあたり、顧客から事前に承諾を得る（オプトイン）こと」、「提携先との情報共有について、顧客に拒否権（オプトアウト）を与えること」などを定めた。2004 年７月に施行された。

5. 民間団体・NPO の動き

個人情報保護に関する民間団体や NPO としては、昨年 9 月の「ニューヨークだより」で触れたフィッシング対策の団体「Anti-Phishing Working Group（APWG）」以外にも様々な活動を行っている組織がある。

⑴ トラスト e（TRUSTe）

ネットワーク社会における消費者権利の擁護団体、エレクトロニック・フロンティア・ファンデーション（EFT）と Commerce.Net が設立した 1997 年に設立した非営利団体。独立した第３者機関として、オンライン、ネットワーク上のプライバシー保護に焦点を当て、ウェブサイトの個人情報保護の開示・管理状況を審査・認証している。

同団体の認証を受けたサイトは本年１月１日現在で 1413 サイトに達し、フォーチュン 500 企業 28 社が同認証プログラムに参加している。認証を受けたサイトには、それを示すための「TRUSTe」のロゴマークが掲示される。

⑵ デジタル・フィッシュネット（Digital Phishnet）

2004 年に設立。AOL やアースリンクなどの ISP、マイクロソフトやベリサインなどの IT 関連企業、大手９銀行、オンライン競売会社などの民間団体に加えて、FBI や FTC などの政府機関が加わった団体。フィッシングの防止を目的に設立された。具体的な活動内容としては、フィッシング詐欺の関連情報を民間と政府機関が共有し、当局の捜査および起訴を支援していく。

⑶ 電子フロンティア財団（EFA）

1990 年に設立された非営利団体。個人のプライバシーが司法当局の捜査行為などによって不当に侵害された場合に、コンサルティングや援助を行っている。P2P ファイル交換が問題視されている中、大手ソフトウェア開発会社で構成される業界団体 BSA（ビジネス・ソフトウェア・アライアンス）が ISP に対して個人情報の開示を求めた行為に対して、EFA は「ネットの匿名性を軽んじた行為」として反論を掲げている。EFA のサイトには、これまでのケーススタディが紹介されているほか、会員向けのホットラインなども用意している。また、FTC や連邦通信委員会（FCC）など政府の主要機関へのアドバイスもかねている。

⑷ 信用電子通信フォーラム（Trusted Electronic Communications Forum）

IBM、フィデリティ・インベストメンツ、チャールズ・シュワブ、E トレード、テネット・ヘルスケア、AT&T ワイヤレス・サービシズ、Best Buy など、金融および小売業界などの大手が結成した。ネット上における銀行口座番号やパスワードといった個人情報を守るのが目的。対策技術の標準化を進めるとともに、訴訟支援なども手がけている。

⑸ 全米市民自由連合（ACLU）

米国市民の人権擁護保護を掲げる同団体は 1920 年に設立された老舗。最近では、オンラインの人権擁護問題も取り上げ、積極的な活動を展開している。2004 年６月には、FBI が ISP に対して顧客情報の開示を求めた件で訴訟を起こしている。

FBI は、テロやスパイ活動の捜査に際して、裁判所の承認を受けずに「国家安全書簡」を発行し、電話会社、ISP、銀行、信用調査会社などに顧客情報の開示

を要求できる。また、同書簡を受理した側はその事実を他言できない。問題の争点となっているのは、テロやスパイ活動に関与していない者の個人情報の開示を求められるのかという点である。
　さらに、米政府が本年央に発効を予定しているバイオメトリクス・パスポートについて ACLU は反対運動を行っている。

⑹ VOIP セキュリティ・アライアンス（VOIPSA）

　日本に遅れることながら、ようやく米国内で普及のめどがついてきた IP 電話のセキュリティ問題に関して、本年２月に 20 社以上の技術企業およびコンピュータ・セキュリティ団体などが結成して設立された。
　同団体には、3Com、アルカテル、アバヤ、シーメンス、シマンテックおよびアーンスト＆ヤングなどの企業に加えて、米国標準技術局（NIST）、SANS 研究所、大学が参加している。活動目的としては、技術をめぐるセキュリティ面での問題点を明らかにしていくこと、ハッカーなどによる攻撃に対する広報活動を行うこと、既存の電話並の信頼性を確立していくこととされている。

⑺ 全米サイバー・セキュリティ連合（National Cyber Security Alliance）

　ネット利用者に対するネット犯罪の実態と対処の仕方を啓蒙していくのを目的に産学官が協力して結成した団体。FTC や国土安全保障省などが参加している。また、同協会のサイトでは、一般ユーザ、企業ユーザそれぞれ向けにセキュリティに関する様々な情報を提供している。主な協賛企業には、シスコ、e ベイ、マイクロソフト、デル、AOL が名を連ねている。

6. 個人情報関連ビジネスに取り組む IT 企業

　個人情報保護をビジネスチャンスと捉え、個人情報保護にまつわる分野毎に各種サービスや商品を提供しているユニークな IT 企業がある。

⑴ フィッシング対策

　マークモニタ（MarkMonitor）社とシヨタ（Cyota）社は、フィッシングを特定し、顧客企業の損害を最小限に抑える法人向けサービスを提供している。
　マークモニタは、法人向けにドメインネーム登録サービスを提供していたが、新たにフィッシング防止サービス「Fraud Protection」を開始した。これは、企業

に関する情報をウェブ上で自動収集しながら、顧客企業の関連情報を選別する。不審な点が見つかれば、即座に調査スタッフが発信源となるウェブサイトを追跡して、該当サイトを遮断する仕組みとなっている。

シヨタはこれまで、金融機関などにセキュリティ・サービスを提供してきたが、新たにウェブサイトを監視するサービス「FraudAction」を提供している。顧客企業に対しては、警告を発して対応を促す一方、フィッシング攻撃の規模や、これによる損害と深刻度の査定も行う。さらに、損害を 70−80%軽減し、フィッシングを仕掛けた犯人の捕獲率を高める対抗措置も提供する。

⑵電子メール監視サービス

電子メールのウイルス感染に関する従来のアプローチは、新しいウイルスを個別に分析し、アンチウイルス・ソフトに新ウイルスの定義を被害者に配信する方法であった。しかし、電子メール監視サービスを行う企業は、大量のネットワークを監視し、ウイルスなどによる異常を探知すると、配信を遅らせたりブロックしたりするアプローチを採用している。

その１社、アイアンポート・システムズ（IronPort Systems）社は、２万 8000 以上の商業 ISP や企業・大学ネットワークを監視しており、その量は世界の電子メール・トラフィックの約 25%に上るという。同社の提供する「ウイルス・アウトブレーク・フィルターズ」は、専門のハードを用いて企業ネットワークなどへのメール配信を管理する。配信パターンからウイルスを探知し、顧客のメールを処理しているアイアンポートのシステムに自動警告を送る仕組み。さらに、疑わしいメールは、差し止めにし破壊する。サイファートラスト（CipherTrust）社も同様のアプローチを採用している。

⑶個人情報管理サービス

ネット上に出回る個人情報を管理するユニークなサービスも登場している。スタートアップのズームインフォ（ZoomInfo）社は、ネットに公開された個人に関する情報を収集し、本人に内容を管理させるサービスを開発した。

たとえば、検索エンジンを使って自分の名前でキーワード検索すると、いくつかのサイトで情報が掲載されている場合がある。そこで、同サービスは、ウェブ上に散在する公開情報を収集し、個人のプロフィールを作成する。後は、登録会員が自らのプロファイルを見ながら誤った情報などを修正するほか、プロフィール自体を削除できる。

変更されるのはプロフィールの内容だけで、変更後に情報を収集した他のサイトが更新されることはない。ところが、同社によると、検索エンジンで個人名検索した場合に、最も関係のある結果が先頭に表示される。このため、必然的に同

社プロフィールが先頭グループに表示され、結果的に本人が「公開したい」情報だけが閲覧される可能性が高くなるという仕組みだ。
　ズームインフォの根幹の事業は、ネットを使った求人応募者のスクリーニング情報を企業に提供することとなっている。これは有償で、年間数千～数十万ドル。マイクロソフトなどを含むフォーチュン 500 社の 20%が同社サービスを利用しているという。

⑷ 内部犯行対策

　ボンツ（Vontu）社は、社内のネットワークから外部に送信される情報を監視し、内部関係者による機密情報や顧客情報（SSN、口座情報など）の不正持ち出しや漏洩を防ぐためのソリューションを開発している。
　「ボンツ・モニター（Vontu Monitor）」は自動コンテンツ監視ソフトで、電子メール、インスタント・メッセージング（AOL、MSN、ヤフー）、ウェブメール、ウェブポスティング、FTP、電子メールの添付文書など、企業内ネットワークを使ってやり取りされる全トラフィックを監視し、文脈分析技術や不信な事象を発見する独自技術「エグザクト・データ・マッチング（Exact Data Matching）」などを使って、セキュリティ・ポリシーに違反した機密情報などを含んだ通信内容を発見し、管理者に通知する。
　「ボンツ・プリベント（Vontu Prevent）」は、データ、コンテンツ、送信者、受信者、物理的所在地などのパラメータを用い、企業のセキュリティポリシーに違反した、社内から社外への電子メールを発見し、送信を阻止する。

⑸ リスク管理ソフトとサービス

　リスク管理ソフトおよびサービスを提供するウォッチファイアー（Watchfire）社は、オンラインのセキュリティを管理するプラットフォーム「ウェブ XM4.0」を提供している。同システムは、企業のウェブサイトをスキャンして、フィッシング攻撃や ID セフトにつながるシステムの弱点を分析する。同製品は様々なモジュールから構成されているため、金融機関を含む多様な業界に対応している。
　同社はまた、IBM と提携して、企業がプライバシー保護やデータの取り扱いに関して、社内基準や法的規制に従えるよう支援するオンライン・サービス「オンライン・ビジネス・マネジメントサービス（Online Business Management Services）」を提供している。同サービスの料金は、中規模程度のサイトだと初期評価に４万ドルかかる。また、モニタリングを継続する場合は、月額１万ドルの費用が必要。
　IBM が米国上位 200 社の金融機関のサイトを調査したところ、記入した個人情報を送信する際に暗号化を行わないページを持つサイトが全体の 66%に達し

ている。また３分の１のサイトが顧客の了承を得ずに広告主のようなサードパーティが顧客のパソコンにクッキーを設定することを許可していたという。こうした中、同サービスのニーズは増えていくと期待されている。

⑹ 電子カード

ベリファイド・アイデンティティ・パス（Verified Identity Pass）社は、顧客に対し、当人の名前が政府のテロリスト・リストに掲載されていないことや過去に重犯罪暦がないことを証明するデータを記録した電子カードを提供している。

ビジネス企業や空港、政府機関などがベリファイドと契約し、カード読み取り機をセキュリティ・チェックに置く。また、カードには保持者の指紋情報が入っている。実際に保持者が通過する際に指紋をスキャンしてカードと照合する。

提携企業にはリーマン・ブラザーズほか、電子通行料金支払いシステムのイージーパス（E-ZPass）を開発したトランスコア（TransCore）、利用者のスクリーニング技術を提供するチョイスポイント（ChoicePoint）などがある。

また、利用者の名前が政府機関のテロリスト・リストに掲載されている場合は、速やかに当局へ通報する方針を打ち出している。

⑺ ネット犯罪調査機関

スパマー、元社員、詐欺師などを含むネット犯罪者の追跡捜査を専門とする民間調査機関として、クロール・オントラック（Kroll On-track）社、ICG 社、デシジョン・ストラテジーズ（Decision Strategies）社、サイベイランス（Cyveillance）社などがある。

たとえば、ICG が手がけた通信大手エリクソンの事例は、同社のサーバにテレフォンセックスを売込む大量の電子メールが押し寄せたため、システムに支障を来したものである。ICG は、スパムメールを検索エンジンにかけて同じメッセージが現れるウェブサイトを捜し出した。そして、そこにあった電子メール・アドレスから発信源をつきとめ、そのレジストリーからスパマーの名前を割り出した。犯人は、数週間後には訴えられ、最終的に民事和解で 10 万ドルの支払いに合意したという。犯人の割り出しはケースによって異なるため、あらゆる手段を講じて追跡するという。

(参考資料)

http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf
http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf
http://news.com.com/Cookie+fans+chip+away+at+spyware+bill/2100-1028_3-5562748.html
http://www.watchguard.com/press/releases/wg299.asp
http://www.earthlink.net/spyaudit/press/
http://www.bbb.org/alerts/article.asp?ID=565
http://news.com.com/2100-7349_3-5584691.html
http://news.com.com/Securing+data+from+the+threat+within/2100-7347_3-5520016.html?tag=st.rn
http://www.MoveOn.org/
http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-03-02-calif-idtheft-summit_x.htm
http://corzine.senate.gov/
http://billnelson.senate.gov/
http://leahy.senate.gov/
http://www.consumer.gov/idtheft/federallaws.html#credit
http://www.hhs.gov/ocr/hipaa/consumer_summary.pdf
http://www.privacyprotection.ca.gov/
http://www.hppub.com/colpa.htm
http://www.privacyalliance.org/
http://www.eff.org/
http://www.digitalphishnet.org/
http://www.tecf.org/
http://www.aclu.org/
http://www.voipsa.org/
http://www.staysafeonline.info/
http://www.markmonitor.com/
http://www.cyota.com/
http://www.ironport.com/
http://www.ciphertrust.com/
http://www.vontu.com/
http://www.watchfire.com/
http://www.verifiedidpass.com/who.html
http://www.krollontrack.com/
http://www.icginc.com/
http://www.dsijobs.com/
http://www.cyveillance.com/

このレポートに対するご質問、ご意見、ご要望がありましたら、
hiroyoshi_watanabe@jetro.go.jpまでお願いします。