米国における個人情報保護の動向―個人情報窃盗対策を中心に―

中川　かおり

【目次】

Ⅰ　背景

1　個人情報窃盗の急増

米国では、個人情報窃盗（ID Theft）が年々大きな問題となってきている。個人情報窃盗とは、個人情報を権限なく利用することにより、その個人になりすます犯罪一般をさす。

個人情報窃盗の実例は枚挙にいとまがないが、一例として、74歳の年金生活者が被害者となった事例を示す(注1)。被害者は、メリーランド州に住んでいたが、テキサス州在住の個人情報窃盗犯が、被害者の名前を騙って、テキサスの銀行で自動車ローンを組んだ。被害者に対してこのローンの支払請求がなされたことにより、被害者は、この窃盗に気づいた。そこで、被害者は、信用情報機関（consumer reporting agencies(注2)）に対し、信用報告からこのローンの債務についての情報を削除するようかけあったが、機関は、債権者は債務が正当であると主張しているので、債権者と直接話し合うようにと回答するのみであった。結局被害者は、10以上の債権者と個別に話し合い、債務が不当であることを説得した。しかし、その後も、別の債権回収機関から債務不履行の情報が信用情報機関に提供され続けたため、被害者の信用報告には、繰り返し、その情報が掲載されることになった。このように、個人情報窃盗は、被害者に財産的被害をもたらすだけではなく、甚大な時間的・精神的な被害をもたらす犯罪である。

個人情報窃盗に何を含めるかは、人によって広狭があるが、連邦取引委員会（Federal Trade Commission、以下FTCとする。）が2003年に行った調査(注3)において「個人情報窃盗」とされたのは、⑴既存のクレジットカードを権限なく利用すること、⑵銀行口座等を権限なく利用すること、⑶請求書送付先住所を変更したり、権限のない利用者をアカウントに追加することで、既存のクレジットカードを利用すること、⑷新たなクレジットカードの取得や、新たな口座の開設等、金融関連の目的で、被害者の個人情報を権限なく利用すること、⑸犯罪の容疑で逮捕されたときに被害者の氏名を名乗る等、金融関連以外の目的で、被害者の個人情報を権限なく利用すること、の５類型であった。

漏洩個人情報のうち、個人情報窃盗につながりうる、もっとも危険な組み合わせは、氏名と社会保障番号と生年月日であることで、多くの専門家は一致している。というのも、この三つが揃えば、クレジットカード口座を作成したり、車のローンを組んだり、携帯電話を購入することができるためである(注4)。

では、個人情報窃盗の被害を定量的にみると、どのようになっているであろうか。前記の2003年調査を更新する形で行われた民間調査会社の調査(注5)によれば、2005年には、個人情報窃盗による被害者は約890万人、被害者一人当たりの被害額は6,383ドル、被害総額は、566億ドルとされている。2002年には、被害者は約1010万人、被害者一人当たりの被害額は5,249ドル、被害総額は532億ドルとされていたことと比べ、被

害者数は減ったが、被害者一人当たりの被害額・被害総額は増えていることが注目される。また、被害者が問題を解決するために費やした平均時間も、2002年の33時間から、2005年の40時間と長くなっており、被害が深刻化していることがうかがわれる。

FTCが受けた苦情の件数で見ても、個人情報窃盗が拡大傾向にあることは明白である。FTCが受けた苦情は、2000年には約3万1000件であったのが、2002年には約16万2000件、さらに、2004年には約24万7000件にまで増えたのである。(注6)

2　相次ぐ個人情報漏洩事件

2005年から2006年にかけて、米国では、大規模な個人情報漏洩事件が多数報道された。(注7)

民間企業では、2005年2月に、データブローカ（詳細後述）大手のチョイスポイント社（ChoicePoint）が、同社の顧客を装った個人情報窃盗犯に対し、約16万3000名分の個人情報を提供してしまったことが明らかになった。同年2月末には、バンク・オブ・アメリカ社（Bank of America）が、120万人分のバックアップデータを紛失したと発表した。その後も、同年4月には、投資会社のアメリトレード社（Ameritrade）が、20万人の顧客の口座番号を含むバックアップ・テープを紛失し、5月には、タイムワーナー社（Time Warner）の下請け会社が、現在及び過去の従業員60万人分の個人情報を含むテープを紛失するなど、個人情報漏洩事件が相次いでおきた。

2006年になってからは、行政機関からの個人情報漏洩事件も目立っている。比較的大きな事件としては、2月に農務省（Department of Agriculture）が、情報公開請求への回答において、本来開示すべきではない35万人分の個人の社会保障番号及び租税個人識別番号を開示するという事件をおこし、5月には、退役軍人省（Department of Veterans Affairs）が、1975年以降に任を解かれた2860万人の退役軍人につき、社会保障番号、生年月日等を含む個人情報を盗まれるという事件がおきた。後者の事件は規模も大きかったことから、これをきっかけに、下院行政改革委員会が、2003年1月以降の連邦行政機関における個人情報漏洩事件を調査した。(注8)その結果、調査対象とされた全19省庁において一度は情報漏洩事件がおきていたことや、各省庁は、どのような個人情報が漏洩したかを把握していない場合が多いことが明らかとなった。

こうした情報漏洩は個人情報窃盗につながりうるとして世論が沸騰し、これを受けて、連邦議会(注9)や州議会(注10)においても議論が高まった。

3　個人情報窃盗と個人情報漏洩の関係

もっとも、2003年に行われたFTCの調査及びそれを更新する民間調査会社の調査(注11)によれば、大々的に報道される企業や行政機関からの個人情報漏洩は、個人情報窃盗の原因として最も大きい割合を占めているわけではないことが判明している。

2006年の調査によれば、原因が判明した個人情報窃盗事件の63％は、消費者が統制可能な範囲で窃盗が起きている。すなわち、個人情報窃盗の原因の多くは、消費者の不注意や、親族・近隣住民による窃盗である。具体的には、財布、小切手帳又はクレジットカードの亡失又は盗難が30％で、個人情報窃盗の原因の第一位であり、被害額の平均も8,459ドルと、被害額平均で第二位である。この原因による被害額は、年間の被害総額の38％を占め、216億ドルに達する。また、友人や近親者が個人情報を取得できた場合が15％で、個人情報窃盗の原因の第三位であり、被害額の平均は11,411ドルと、被害額平均で第一位となっている。この原因による被害額は、年間の被害総額の23％を占め、130億ドル

に達する。これに対し、消費者の金融情報を扱う企業からの情報漏洩が原因とされる個人情報窃盗は、原因が判明した事件のうちの６％を占めるにすぎない。

Ⅱ　既存の法制・行政機関による取組み

１　法制

このように個人情報窃盗が大きな問題となっている米国で、企業や行政機関が保有する個人情報の安全性を確保し、利用・提供の範囲を定める既存の法制は、どのようになっているのであろうか。米国では、公的部門につき、1974年プライバシー法があるのに対し、民間部門については、原則的に自主規制に委ねつつ、特にセンシティブな個人情報を扱う分野について個別の法律を制定する「セクトラル方式」による保護法制を整備している(注12)。1970年代以降整備されてきたこうした個別法は､20本以上にのぼるが､本章では、個人情報窃盗と特にかかわりの深い主要な法律を概観する。

⑴　公正信用報告法

最初の主要な信用情報機関は、1899年に設立され、その後、保険会社や雇用主に対する個人の消費者信用報告の販売を拡大してきた。この信用情報機関につき、ネガティブ情報の収集や不正確な情報の収集等にかかわる、さまざまな問題が明るみとなったのを契機に、1970年に、これらの機関を統制するための公正信用報告法(注13)が制定された。

公正信用報告法は、民間部門による個人情報の利用及び提供を規制する最初の連邦法である。同法は、消費者信用報告の収集、維持及び提供を規制する。消費者信用報告は、信用供与の適格性を判定するときや被用者の経歴調査を行うとき等、同法に列挙された目的のためのみに用いることができる。信用情報機関は、個人からの保有記録へのアクセスを認め、苦情の申立てを受けるための電話番号を公表しなければならない。信用情報機関は、個人が自らの信用報告の中で誤りだと指摘した点について調査しなければならない。ある個人について、消費者信用報告に基づき不利益な取扱いをする者は、そのことを当該個人に通知しなければならず、雇用主が被用者の信用報告を調査したい場合には、まずその者の同意を得なければならない。雇用主が信用報告に基づいて不利益な取扱いをするときは、雇用主はその者に通知をし、報告の写しを入手する方法を教示しなければならない。もっとも、公正信用報告法のもとで、法執行機関は、さまざまな方法で消費者信用報告にアクセスできることが定められている。たとえば、裁判所命令若しくは大陪審召喚令状を入手した場合や、児童支援施設の要請がある場合には、完全な消費者信用報告を入手することができる。また、連邦捜査局（Federal Bureau of Investigation、以下 FBI という。）が書面により請求するときは、防諜目的で個人の口座情報及び身元特定情報へアクセスすることができる。

2003年には、個人情報窃盗対策に主眼をおいた公正信用報告法の改正(注14)が行われた。これにより、被害者が、自らの個人情報についての無権限利用の状況を知りたいと考える場合には、三つの全米信用情報機関から、年に一度は無料で消費者信用報告を入手できることとなった(注15)。また、被害者は一定の要件の下で、自らの消費者信用報告に詐欺警告(注16)を付することを認められるようになった(注17)。

⑵　1974年プライバシー法

1974年に成立したプライバシー法(注18)は、連邦の行政機関が、ある目的のために収集した市民の個人情報を、別の目的のために利用することを禁止する。この法律は、行政機関に対し、個人情報を収集し、処理するにあたり、公正な情報慣行に従うことを要求し、国民にアクセス権、訂正権を提供すること、行政機関の特定の任務を実施するために必要な範囲にデータ収集を限

定すること、及び、一定の期間の後にデータを破棄することを義務付けている。また、この法律は、行政機関が個人のデータを第三者及び第三者機関と共有できる範囲を制限し、個人が行政機関の違反に対して訴訟を提起することを認める。

もっとも、行政機関間のデータ共有の制限は完全ではなく、当初の収集目的と「整合的な（compatible）」目的のためであれば、収集した機関とそれ以外の機関との間でデータを共有することができる。こうして、行政機関間のデータ共有が広く行われるようになったため、1988年に議会はコンピュータ・マッチング・プライバシー法[注19]を可決し、データ共有の際には、共有の理由と目的を特定しなければならないこととなった。

⑶ 個人情報窃盗に対する罰則

1998年に、連邦で最初の個人情報窃盗対策法が成立した。この「個人情報窃盗・乱用阻止法（Identity Theft and Assumption Deterrence Act of 1998[注20]）」は、個人情報窃盗それ自体を初めて犯罪とし、20年を上限とする拘禁刑を定めた。これを受けて、連邦量刑委員会が定めた量刑ガイドラインは、被害者が金銭的被害を被っておらず、かつ、窃盗犯が犯歴を有しない場合であっても、10か月以上16か月以下の拘禁刑に処することを可能とした[注21]。

2004年には、加重個人情報窃盗罪を新設する法改正が行われた[注22]。すなわち、銀行詐欺や電気通信詐欺といった重罪により有罪とされた者が、その重罪に関連して個人情報窃盗を行った場合には、重罪の刑期にさらに２年を上限として加算し、また、テロ行為により有罪とされた者が、そのテロ行為に関連して個人情報窃盗を行った場合には、テロ行為による刑期にさらに５年を上限として加算することが可能となった。

⑷ グラム･リーチ･ブライリ法

1999年に制定されたグラム・リーチ・ブライリ法[注23]は、銀行、保険会社、信用情報機関等を含む金融機関に対し、系列企業との間で、非公開個人情報の共有を認める。

もっとも、金融機関が、系列企業ではない第三者にその情報を提供しようとする場合には、当該個人に対し、オプトアウト[注24]を認めなければならない[注25]。ただし、法執行目的や裁判利用目的の場合は、このオプトアウト原則の例外とされる。この例外規定に基づき、情報を受領した機関は、自身が金融機関ではなくとも、グラム・リーチ・ブライリ法に基づくプライバシールール上の再利用及び再開示の制限に服する。

⑸ 連邦取引委員会法第5条

連邦取引委員会法第５条[注26]は、「取引における又はそれに影響を与える不公正な又は詐欺的な行為又は慣行」を禁止する。同条のもとで、委員会は、取引に参加する多様な企業及び個人による不公正な又は詐欺的な慣行を禁止するための広汎な権限を有する。禁止される慣行には、企業がプライバシーについて行う詐欺的な約束を含み、そこには、消費者情報の安全性確保についての約束が含まれる。

詐欺に加え、同条は、不公正な慣行を禁止している。企業の慣行が、消費者に対して、通常簡単に回避することもできず、相殺的給付もないような実質的な損害を与えるとき、又は、与える可能性があるときは、その慣行は不公正とされる。

２ 行政機関による取組み

1998年の会計検査院（General Accounting Office）による調査[注27]によれば、当時は、⑴個人情報窃盗事件についての包括的な管轄権を有する連邦機関はなく、⑵個人情報窃盗犯に特定して適用される法規定がなく、かつ、⑶犯罪の明確な定義がないために、個人情報窃盗を捜査する法執行機関は存在しない、という状況であっ

た。

しかし、その後、上述したように、1998年に個人情報窃盗に対する罰則が新設され、さらに、2004年には加重個人情報窃盗罪が新設される中で、FBI、合衆国シークレットサービス（United States Secret Service）、合衆国郵便監察庁（United States Postal Inspection Service）及び社会保障総局監察総監課（Social Security Administration Office of the Inspector General）が個人情報窃盗事件の捜査を行い、司法省がこうした事件の訴追を行うようになってきている。(注28)

また、司法省司法プログラム局（Office of Justice Programs）は、⑴連邦、州、地方及び部族の各層における被害者サービス・プログラム及び被害者サービス提供者に対する資金及び訓練の提供、⑵個人情報窃盗に取り組む法執行機関、訴追機関及び犯罪防止専門家に対する資金の供給、⑶国立司法研究所（National Institute of Justice）を通した個人情報窃盗に関する調査及びプログラム評価、⑷個人情報窃盗についての政策策定のためのデータ収集、などを行っている。(注29)

FTCは、個人情報窃盗についての消費者の報告を受ける情報センターとして、また、適切な対策をとらない企業に対する訴訟を提起する機関として、活動している。(注30)

まず、情報センターとしての活動については次のとおりである。FTCは、消費者からの報告のログを維持し、消費者に報告を受領した旨通知するよう求められている。(注31)これに従い、1999年11月にFTCは、個人情報窃盗データ情報センター（Identity Theft Data Clearinghouse）を設立し、個人情報窃盗についての報告を提出した消費者から情報を収集している。FTCは、この情報を、消費者監視データベース（Consumer Sentinel database）に提供しており、これが、1,000を超える法執行機関により利用されている。また、FTCは、報告を提出する消費者のために、その者が有する権利について概要を記すペーパーを作成している。(注32)

次に、訴訟を提起する機関としての活動は以下のようになっている。1998年以降、FTCは、連邦取引委員会法第5条に基づき、民事訴訟上の差止救済を求めて提訴するようになった。これは、企業が、消費者情報を保護するために適切な措置をとると明示的・黙示的に約束したにもかかわらず、適切な措置をとらないことが、連邦取引委員会法第5条の「詐欺的な行為」に該当するためである。こうした個人情報窃盗への対処に一層重点的に取り組むために、FTCは、2006年に、プライバシー・身元保護局（Division of Privacy and Identity Protection）を新設した。(注33)

さらに、現在、個人情報窃盗の広がりの中で、連邦行政機関のとるべき新たな取組みについての議論が行われている。2006年5月、ブッシュ大統領は、個人情報窃盗に関する諮問委員会を設置した。この諮問委員会は、2007年2月に大統領に提出される予定の本報告に先立ち、(注34)中間勧告を公表した。(注35)その中で、連邦行政機関による個人情報窃盗対応を強化するための措置として、⑴情報漏洩が起きた場合に連邦行政機関が行うべき被害者に対する通知についての指針の策定、⑵社会保障番号の利用の限定、⑶情報が漏洩した場合の、連邦行政機関間での被害者情報共有の推進、⑷個人情報窃盗の被害者が、自らの名声を取り戻すために費やした時間の価値を回復することができるような、刑事補償規定の改正、⑸個人情報窃盗の被害者が法執行機関に被害届を出す際の警察報告書についての、共通書式の作成等が提示されている。(注36)

Ⅲ　連邦議会が注目する主な施策

このように、個人情報の安全性を確保し、利用・提供の範囲を定める既存の法律は、多数存

在し、それに基づく行政機関の取組みも種々行われている。にもかかわらず、近年の相次ぐ情報漏洩により、センシティブな個人情報を収集・維持する企業等が、その情報が違法に提供されないよう保障するための十分な措置をとっているのか、その情報が権限のない者に取得された場合にいかなる措置をとるべきなのかについて、論議がわきおこってきている。もちろん、既存の法律を厳格に執行し、企業に対して既存の法律について教育することも、一定の範囲で、こうした疑義にこたえるものとなろう。しかし、既存の法律では不十分であるとして、新たな立法の必要性を唱える声も高まりつつある。

こうした中で、2005年から2006年にかけて、連邦議会では、８つの委員会で、個人情報窃盗に対処する方策をめぐり、審議が行われてきた。しかし、多数の委員会に審議が分散したことも一因となり、議論は収束しないまま、2006年12月、第109議会が終了した。ただ、連邦議会での議論の過程では、個人情報窃盗対策で先行する州の法律や、現在は特定の機関のみに適用される連邦規則の定める施策がモデルとして参照された。参照された主な施策には、⑴金融機関に対する個人情報保護規制、⑵個人情報が漏洩した場合の被害者への通知、⑶社会保障番号の利用制限、⑷消費者信用報告の凍結、がある[注37]。本章では、これらを順次紹介し、本稿末尾に翻訳を掲載する。

１　金融機関に対する個人情報保護規制

連邦議会における議論の中で、既存の法律では規制しきれていないデータブローカについて、個人情報保護規制の対象とすべきであるという提言がなされている[注38]。

データブローカとは、消費者情報の収集・提供に特化する企業である。データブローカは、2005年に、チョイスポイント社をはじめとするいくつかの企業が、大規模な情報漏洩事件を起こしたことで注目を集めたが、もともとは、さまざまな企業及び行政機関の個人情報需要を満たすために、信用情報機関から派生した業種である。データブローカには、公的又は私的な情報源から直接に個人情報を集める者、他者が集めた個人情報を転売する者、そのいずれをも行う者とさまざまな態様が存在する。また、提供先もさまざまであり、行政機関又は大企業のみに個人情報を提供する者もいれば、中小企業又は一般市民に個人情報を提供する者もいる。データブローカにより収集・提供される個人情報は、詐欺の阻止、債権回収、法執行、法遵守確保、申請者確認、マーケットリサーチ等の目的に利用される。データブローカは、しばしばセンシティブな個人情報を収集することから、個人情報窃盗の標的とされやすい。

主なデータブローカとしては、チョイスポイント社、アクシオム社（Acxiom）、レクシス・ネクシス社（LexisNexis）等がある[注39]。たとえば、チョイスポイント社は、内国歳入庁やFBIを含む、少なくとも35の連邦行政機関との間で、何百万ドル規模の契約を締結している。また、レクシス・ネクシス社の提供する個人情報は、連邦法執行機関が、刑事捜査において、証人、被疑者、情報提供者、犯罪者及び保釈者の居所を特定するためにも用いられている。

このように、個人情報を扱う企業として目覚しい成長をみせるデータブローカであるが、公正信用報告法及び1974年プライバシー法は、この活動を有効に規制するものではない[注40]。

公正信用報告法は、消費者信用報告を提供する信用情報機関に適用される。信用情報機関とは、第三者に消費者信用報告を提供するために、消費者についての情報収集に常時携わる者と定義される。この定義によれば、公正信用報告法の適用範囲を決めるのは、「消費者信用報告」の定義となるが、公正信用報告法は、消費者信用報告をきちんと定義しておらず、結果的に公

正信用報告法の適用範囲を不当に狭めている。すなわち、消費者信用報告は、消費者の性格又は一般的な名声についての通信であって、信用評価や従業員採用を目的として用いられ又は収集されるものということになり、これら以外の目的のために用いられる個人情報には適用されないことになる。

1974年プライバシー法も、十分な実効性を有しているとはいいがたい。同法は、連邦行政機関及びそのために記録システムを管理している民間企業のみに適用される。すなわち、個人情報が政府から民間企業に提供される場合には、1974年プライバシー法の要件は民間企業に適用されるが、データブローカが収集し、提供する情報には、1974年プライバシー法の規定は適用されない。その結果、1974年プライバシー法は、データブローカに対して、行政機関が創出を禁じられている巨大なデータベースを作成することを許している。行政機関が個人情報を必要とする場合には、データブローカから入手することができるのである。もちろん、行政機関がデータブローカから個人情報を入手した時点で、その情報は1974年プライバシー法に服することにはなるが、法執行機関及び諜報機関は、同法の下で、アクセス権、正確性確保権、訂正権を制限する特別の適用除外を享受している。

このように、多くの場合、既存の法律が適用されないデータブローカに対する個人情報保護のための規制を考えるにあたり、モデルとして参照される規制のひとつに、グラム・リーチ・ブライリ法に基づくセーフガード・ルール(注41)がある（翻訳後掲）。これは、金融機関に対し、消費者情報を守るための相当の物理的、技術的及び手続的保護措置をとるよう要求している。セーフガード・ルールは、すべての機関にとって必ずしも適切ではないような、また、速やかに時代遅れとなってしまうような技術を特定し、その使用を要求するのではなく、特定のシステムについてその性質やリスクを評価し、脅威に対処するための適切な手続をとるよう要求するものである。さらに、金融機関は、定期的にデータ・セキュリティ・ポリシー及び手続を見直し、必要に応じて最新版にする必要がある。このように、セーフガード・ルールは、保有する情報の安全性を保障するために、強力であると同時に、柔軟な枠組みを、金融機関に提供している。

2　個人情報が漏洩した場合の被害者への通知

データを保護するための最善の取組みが行われたとしても、情報漏洩は依然としておこりうる。そのため、情報漏洩がおきた場合には、漏洩を起こした主体は、その事実を被害者に通知するべきであるという提言が、連邦議会における議論の中でなされている(注42)。

情報漏洩により、個人情報窃盗及び関連する被害の可能性が大きくなる場合に、迅速に消費者に通知をすれば、その被害を緩和することが期待できる。具体的には、通知を受けた消費者は、その消費者信用報告に詐欺警告が掲載されるように信用情報機関に求め、年に一度は無料で消費者信用報告の写しを受け取り、毎月口座を監視し、その他自らを守るために必要な措置をとることができる。この際、重要なのは、消費者に実際に被害が及ぶ可能性がある場合にのみ、漏洩を起こした主体に通知が義務付けられることである。

情報漏洩を起こした主体が、被害者にいつ通知を出すかを決定する方法のモデルとされうるものは、現在二つある。

第一は、金融機関規制基準である（翻訳後掲(注43)）。この基準の下で、金融機関は、センシティブな顧客情報への権限のないアクセス又は利用を含む事件に気づいた場合、直ちに連邦規制機関へ通知することが義務付けられる。加えて、金融機関が、顧客情報の悪用がおき、又はその可能

性が相当程度あると判断する場合には、顧客に対して通知を行うよう義務付けられる。

第二は、カリフォルニア州法の規定である（翻訳後掲[注44]）。企業や行政機関は、列挙されたセンシティブなデータが、消費者を特定するために用いられうる情報とともに、個人情報の安全性、秘密性又は完全性を損なう方法で、権限のない者により入手され、又はその可能性が高いと考えられる場合には、消費者に対して通知をすることが義務付けられる。

カリフォルニア州法の規定は、データベースへのすべての不適切なアクセスに対して通知を求めるものではない。むしろ、企業又は行政機関に、通知が必要な場合を判断する柔軟性を許容していると同時に、幅広い範囲の企業又は行政機関による法令遵守が可能となるような客観的な基準を定めるものである。カリフォルニア州のプライバシー保護局により発行されたガイダンスによれば、情報が「入手された」かどうかを決定するにあたり、⑴保護されたデータが権限のない人の物理的な保有のもとにあり、その統制下にあることをうかがわせる事情（コンピュータその他の機器の紛失又は盗難）、⑵保護されたデータがダウンロードされたか又はコピーされたことをうかがわせる事情、⑶保護されたデータが権限のない人により利用されたことをうかがわせる事情（新しい口座の開設）等が、考慮に入れられる。

3　社会保障番号の利用制限

社会保障番号は、国民IDが存在しない米国で、事実上国民IDと同様の役割を果たしている。連邦議会における議論の中で、この社会保障番号の利用を、制限するべきであるとの提言がなされている[注45]。

社会保障番号は、州際通商のための重要な道具である。３億人の米国消費者には、同姓同名が多いため、９桁の社会保障番号が企業にとって、主要な人物特定手段となっている。FTCの調査により、社会保障番号は、信用情報機関が、彼らに提供されたデータを正しい消費者信用報告に含めること及び消費者信用報告を正しい消費者に提供することを保障するために用いられる、主要な確認手段の一つであることが判明した。また、社会保障番号は、行方不明の受益者、潜在的証人及び法律違反者を見つけるための居所特定データベースにおいて用いられ、児童扶養費を回収するためにも用いられる。さらに、社会保障番号データベースは、個人情報窃盗の捜査のためにも用いられる。たとえば、社会保障番号が、個人情報窃盗の結果としてではなく、実際に特定のローン申請者に帰属しているかどうかを確認する場合などである。仮に、社会保障番号を、個人特定手段及び詐欺阻止手段として用いることができなくなれば、信用の供与及び他の金融サービスの提供は、よりリスクが高く、より高価で、より不便なものとなることが予想される。同時に、行政機関による、公衆衛生、刑事法執行及びテロ対策に影響を及ぼすことも懸念される。

このように、社会保障番号の合法的利用は重要な役割を果たしているが、他方で、その権限のない利用は、個人情報窃盗の横行を許す。個人情報窃盗犯は、社会保障番号を、被害者の口座等へのアクセスの鍵として用いるためである。

もちろん、現在、特定の状況において特定の種類の情報の開示に制限を加える連邦法は、いくつか存在する。たとえば、公正信用報告法は、消費者信用報告の提供を、信用評価や従業員採用の目的がある場合に限定している。グラム・リーチ・ブライリ法は、「金融機関」が、詐欺阻止又は法律遵守といった一定の適用除外の枠外で、個人情報を第三者に提供する場合には、消費者に対して、オプトアウトの機会を提供しなければならないとする。そのほかにも、情報開示を制限する法律には、保健介護サービス提

供者及び他の医療関係機関に適用される1996年医療情報保護法[注46]に基づくプライバシールールや、州の自動車局による運転免許情報の不適切な開示から消費者を守る運転者プライバシー保護法[注47]がある。

しかし、これらの法律は、それぞれの要件の範囲内で社会保障番号の提供を制限するものの、社会保障番号について包括的な保護を定めるものではない。例えば、消費者の氏名、住所及び社会保障番号の開示は、情報源が金融機関である場合にはグラム・リーチ・ブライリ法により制限されるが、多くの場合には、同じ情報を非金融機関からインターネットで購入することが可能である。

そのため、社会保障番号の有益な利用を阻害しない形で、こうした既存の保護を強化又は拡大する方策が求められている。

社会保障番号の利用を制限するためのモデルとなりうるものとして、カリフォルニア州で2003年に制定された法律がある（翻訳後掲[注48]）。この法律は、個人や団体が、社会保障番号を公開したり、製品やサービスの提供に際して、社会保障番号の提出を要求したりすることを制限する。ただし、州法又は連邦法が定める社会保障番号の収集、利用、保持や内部的な確認又は管理目的での利用を妨げるものではない。また、州法が公表することを求めている特定の記録についても適用除外とする。

4　消費者信用報告の凍結

連邦議会における議論の中で、消費者が、自らの消費者信用報告への他者によるアクセスを原則として禁止し、必要な場合にのみ解除できるようにするべきであるという提言がなされている。

消費者が、ローンを申請するとき等には、申請を受けた者は、信用機関が保有するその者の消費者信用報告にアクセスして、信用度を調査する。現在、消費者信用報告へのアクセスに対する規制は存在しない。これを、消費者が許可した場合にのみ、その者の消費者信用報告にアクセスできるようにすれば、他者がその者になりすましてローンを組むこと等ができなくなるという理屈である。消費者が許可した場合にのみ、第三者がその消費者信用報告にアクセスできるようにすることを、消費者信用報告の「凍結」又は「セキュリティ凍結」という。

消費者信用報告の凍結のためのモデルとなりうるものとして、カリフォルニア州の2003年の法律がある（翻訳後掲[注49]）。自らの消費者信用報告を凍結するためには、消費者は、自らの記録へのアクセスを阻止するように要請する配達証明郵便を、三つの全米信用情報機関に送付する。これを受けて、信用情報機関は、消費者の要請から５営業日以内にセキュリティ凍結を行う。信用情報機関は、消費者に対して、消費者信用報告の凍結を解除するための個人識別番号（PIN）を提供する。消費者は、PIN を用いて、電話で各信用情報機関に対して、解除を認めることができるが、解除の手続きには、３営業日を要する。セキュリティ凍結は、消費者が配達証明郵便により、凍結をやめるよう請求するまで有効である。また、セキュリティ警告又はセキュリティ凍結が実施されている場合に、信用情報機関が消費者信用報告に含まれる情報に一定の変更を加えたときは、変更から30日内に消費者に書面で確認を取らなければならない。

注

＊インターネット情報は2006年11月30日現在である。

⑴ “Victims of Identity Theft Battle Creditors as Well as Crooks”, *Washington Post*, July 21, 2002.

⑵ 米国と日本では、信用情報機関のあり方は、大きく異なる。米国の信用情報機関は、利用者資格をあらゆる業態の与信業者に開放し、また収集した信用情報の蓄積・提供のほかにも、情報データベースを

もとに顧客向けのさまざまなサービスを提供する完全な営利企業である。これに対し、日本の信用情報機関は、与信業者が協同組合的に設立した会社組織として誕生し、会員相互のために情報の蓄積と交換を行う非営利組織として成長してきた。さらに、情報利用の点でも、与信目的以外の信用情報の提供は制限されている。「特集　日米比較から探る　アメリカのクレジットビューローとは　市場原理の中で発展したクレジットビューロー」『i』64号, 2006. 9, p.4.

(3) Synovate, "Federal Trade Commission -Identity Theft Survey Report", September 2003 <http://www.ftc.gov/os/2003/09/synovatereport.pdf>

(4) "Industry Seeks One Law On Data Breach Alerts", *CQ Weekly*, Vol.64, No.6, Feb.6, 2006, p.315.

(5) Javelin Strategy & Research, "2006 Identity Fraud Survey Report (consumer version)", January 2006. <http://www.javelinstrategy.com/products/AD35BA/27/delivery.pdf>

(6) "Identity Theft, Can Congress give Americans better protection?", *CQ Researcher*, Vol.15, No.22, June 10, 2005, p.530 ; Federal Trade Commission, "Consumer Fraud and Identity Theft Complaint Data January-December 2005", <http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>

(7) Privacy Rights Clearinghouse, "A Chronology of Data Breaches", <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

(8) Committee on government reform, "Staff Report, Agency Data Breaches since January 1, 2003", Oct. 13, 2006. <http://www.democrats.reform.house.gov/Documents/20061013145352-82231.pdf>

(9) 2005年には3つの公聴会が開かれ、8つの委員会に、無数の関連法案が係属していた。Gina Marie Stevens, "Data Security: Federal Legislative Approaches", *CRS Report*, RL33273, Feb 9, 2006, p.1.

(10) 2005年1月1日から4月19日の間に、35州の州議会において、個人情報窃盗を抑止することを目的として提出された法案は、124本にのぼった。*CQ Researcher*, *supra* note 6, p.527.

(11) Javelin Strategy & Research, *supra* note 5.

(12) 岡村久道・新保史生『電子ネットワークと個人情報保護―オンラインプライバシー入門―』経済産業調査会, 2002, p.121.

(13) Act of Oct.26, 1970, Pub. L. No. 91-508, 84 Stat. 1127.

(14) Act of Dec. 4, 2003 Pub. L. No. 108-159, 117 Stat. 1952. 中川かおり「公正かつ正確な信用取引のための法律－アメリカの「公正信用報告法」の改正」『外国の立法』221号, 2004. 8, pp.122-136. <http://www.ndl.go.jp/jp/data/publication/legis/221/022104.pdf>

(15) 15 U.S.C. § 1681j(a).

(16) 「詐欺警告」とは、信用情報機関が、クレジット会社等に消費者信用報告を提供する際にともに提供される情報で、消費者信用報告の主体が個人情報窃盗の被害者である可能性があることを、報告の受領者に警告するものである。

(17) 15 U.S.C. § 1681c-1.

(18) Act of Dec. 31, 1974, Pub. L. No. 93-579, 88 Stat. 1896.

(19) Act of Oct. 18, 1988, Pub. L. No. 100-503, 102 Stat. 2507.

(20) Act of Oct. 30, 1998, Pub. L. No. 105-318, 112 Stat. 3007.

(21) General Accounting Office, "IDENTITY THEFT. Prevalence and Cost Appear to be Growing", March 1, 2002, p.11. <http://www.gao.gov/cgi-bin/getrpt?GAO-02-363>

(22) Act of July 15, 2004, Pub. L. No. 108-275, 118 Stat. 831.

(23) Act of Nov. 12, 1999, Pub.L.No.106-102, 113 Stat. 1338.

(24) オプトアウトとは、本人の求めに応じて利用等の停止を認める制度全般を指す。これに対し、本人の事前同意を利用等の要件とする方式を、オプトインという。

(25) 15 U.S.C. § 6802 (a), (b).

(26) 15 U.S.C. § 45.

(27) General Accounting Office, "Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited," May 1998, pp.2. <http://www.gao.gov/cgi-bin/getrpt?GAO/GGD-98-100BR>

(28) Department of Justice, "FACT SHEET: THE WORK OF THE PRESIDENT'S IDENTITY TASK FORCE", Sep.19, 2006.

(29) *Ibid*.

(30) Government Accountability Office, "Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights Are Under Way", June 2005, pp.6-7.

(31) 18 U.S.C. § 1028 note.

(32) *Supra* note 30.

(33) Federal Trade Commission, "For Consumers: Division of Privacy and Identity Protection"<http://www.ftc.gov/bcp/bcppip.htm>

(34) Amendment to Executive Order 13402, Strengthening Federal Efforts To Protect Against Identity Theft, 71 Fed. Reg. 65365 (Nov. 8, 2006).

(35) President's Identity Theft Task Force, "Interim Recommendations", Sep.16, 2006. <http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf>

(36) 警察報告書は、連邦公正信用報告法に基づき、自らのファイルに「詐欺警告」を掲載する場合に必要となる (15 U.S.C. § 1681c-1)。

(37) その他にも、個人情報を収集する企業をFTCに登録させることで、個人が、自己情報の確認、訂正等の請求を一元的に行うことを可能にすることや、商業目的で公的記録からデータを入手することに対する制限を強化すること等が、対策として提言されている。Daniel J. Solove & Chris Jay Hoofnagle, "A Model Regime of Privacy Protection", *University of Illinois Law Review*, Feb. 2006, pp.357-403.

(38) "Prepared Statement of the Federal Trade Commission before the Committee on Commerce, Science, and Transportation, US Senate on Data Breaches and Identity Theft", June 16, 2005, pp.8-10. <http://www.ftc.gov/os/2005/06/050616databreaches.pdf>

(39) Solove & Hoofnagle, *supra* note 37, p.363.

(40) *Ibid*., pp.364-368.

(41) Federal Trade Commission, 16 CFR Part 314, Standards for Safeguarding Customer Information; Final Rule. 67 Fed. Reg. 36484 (May 23, 2002).

(42) *Supra* note 38, pp.10-13.

(43) Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005).

(44) Cal. Civ. Code §§ 1798.29, 1798.82. 2005年2月に、チョイスポイント社は、35,000名のカリフォルニア州民に対して、同社の顧客を装った個人情報窃盗犯が、同社のデータベースから個人情報を入手したと通知した。同社は、カリフォルニア州法に従って同州民に対して個人情報漏洩を通知したが、この事件により影響を受けうる州外の11万人に対しては、通知は法的義務ではないとして、当初は通知せず、批判が高まって後に初めて通知した。こうした事態が二度と起こらないようにするために、ニュージャージー州をはじめとする他の州で、同様の法律の制定が相次いだ。2006年7月18日現在、少なくとも34の州で、こうした法律が制定されている。

なお、チョイスポイント社は、2001年にも、情報漏洩事件を起こしていたが、通知を義務付ける法律がなかったために、公表しなかったとされる。このことは、2005年の情報漏洩を受けて行われた連邦議会の公聴会における同社社長の証言により明らかにされた。

(45) *Supra* note 38, pp.13-16.

(46) Act of Aug. 21, 1996, Pub. L. No. 104-191, 110 Stat. 1936.

(47) Act of Sept. 13, 1994, Pub. L. No. 103-322, 108 Stat. 1796.

(48) Cal. Civ. Code §§ 1798.85, 1798.86, Cal. Fam. Code § 2024.5.

(49) Cal. Civ. Code §§ 1785.11.12, 1785.11.3.

【参考文献】

・Daniel J. Solove, "Access and Aggregation : Public Records, Privacy and the Constitution", *Minnesota Law Review*, Vol. 86, pp.1137-1218.

・Daniel J. Solove, *The Digital Person: Technology And Privacy In The Information Age*, NYU Press, 2004.

（**なかがわ　かおり**・行政法務課）

個人情報窃盗対策関係法規

【目次】

1　データブローカに対する個人情報保護規制のモデルとなる規定
連邦規則法典第16編第314部 顧客情報の保護基準

16 C.F.R. Part 314 Standards for Safeguarding Customer Information

（2006年12月７日現在）

中川　かおり訳

第314.1条　目的及び範囲

(a)　目的

グラム・リーチ・ブライリ法第501条及び第505条ｂ項(2)を実施するこの部は、顧客情報の安全性、秘密性及び完全性を保護するための相当の管理的、技術的及び物理的な保護措置を開発し、実施し、かつ維持する基準を作成する。

(b)　範囲

この部は、連邦取引委員会（「FTC」又は「委員会」）が管轄権を有するすべての金融機関による顧客情報の取扱いに適用される。この部は、そのような機関に「あなた（you）」として言及する。この部は、あなたが保有する情報が、顧客関係を有する個人に関するか、あなたに情報を提供した金融機関の顧客に関するかにかかわらず、すべてに適用される。

第314.2条　定義

(a) 一般規定

この部により改正される場合を除き、又は、別の文脈で要求されるのでない限り、この部で用いられる用語は、消費者金融情報のプライバシーを統制する委員会の規則（16 CFR part 313）に定められるのと同一の意味を有する。

(b)　顧客情報とは、金融機関の顧客について連邦規則法典第16編第313.3条ｎ項に定められる非公開個人情報を含む記録であって、あなた若しくはあなたの関連企業が取り扱い、若しくは、維持し、又は、あなた若しくはあなたの関連企業に代わって取り扱い、若しくは維持されるものをいう。紙媒体、電子媒体又は他の形式であるかを問わない。

(c)　情報セキュリティ・プログラムとは、管理的、技術的又は物理的な保護措置であって、あなたが顧客情報にアクセスし、収集し、配布し、処理し、保護し、蓄積し、利用し、送信し、処理し、又は別に取り扱うために利用するものをいう。

(d)　サービス・プロバイダとは、この部に服する金融機関に直接にサービスを提供することを通じて、顧客情報を受領し、管理し、処理し、又は他のアクセスを許容される個人又は団体をいう。

第314.3条　顧客情報の保護基準

(a)　情報セキュリティ・プログラム

あなたは、ひとつ又はそれ以上の簡単にアクセスできる部分に書かれ、あなたの活動の規模及び複雑性、性質及び範囲並びに問題となっている顧客情報のセンシティビティに適した管理的、技術的及び物理的な保護措置を含む包括的な情報セキュリティ・プログラムを作成し、実施し、かつ管理しなければならない。そうした保護措置は第314.4条に定める要素を備え、この条のｂ項に定められるこの部の目的を達成するよう合理的に計画されていなければならない。

(b)　目的

この法律の第501条ｂ項及びこの部の目的は、

以下のとおりとする。

⑴ 顧客情報の安全性及び秘密性を保障すること。

⑵ 情報の安全性又は完全性に対する予想される脅威に対して保護すること。

⑶ 顧客に対する実質的な障害又は不利益を帰結する情報への権限のないアクセス又は利用に対して保護すること。

第314.4条　要素

あなたの情報セキュリティ・プログラムを作成し、実施し、かつ管理するためには、以下のことを行わなければならない。

⑷ あなたの情報セキュリティ・プログラムを調整する被用者を一人又は複数名指名すること。

⑸ 権限のない開示、誤用、改ざん、破壊又は他の情報の損壊を帰結する顧客情報の安全性、秘密性及び完全性への、合理的に予想できる内部的及び外部的リスクを特定し、リスクを制御するために実施されている保護措置の十分性を評価する。そうしたリスク評価は、以下のものを含む、あなたの活動の関係する領域におけるリスク考慮を含まなければならない。

⑴ 被用者の訓練及び管理

⑵ 情報の処理、蓄積、転送及び廃棄だけでなく、ネットワーク及びソフトウェアの設計を含む情報システム

⑶ 攻撃、侵入又は他のシステムの失敗の検出、阻止及び応答

⑹ リスク評価を通じてあなたが特定するリスクを制御する情報の保護措置を作成し、実施すること並びに保護措置の鍵となる管理、システム及び手続きの効率性を常に検査し、又は、監視すること。

⑺ サービス・プロバイダを、次のように監視すること。

⑴ 問題となっている顧客情報のための適切な保護措置を維持することができるサービス・プロバイダを選択し、維持するための合理的な対策をとること。

⑵ 契約によりあなたのサービス・プロバイダに対し、保護措置を実施し、維持することを要求すること。

⑻ この条のｃ項により要求される検査及び監視の結果に照らして、あなたの行動若しくは業務体制に対する実質的な変更に照らして、又は、あなたの情報セキュリティ・プログラムに実質的な影響を与えうるとあなたが知り、若しくは知りうるべき事情に照らして、あなたの情報セキュリティ･プログラムを評価し、調整すること。

第314.5条　施行日

⑷ 委員会の管轄権に服する金融機関は、2003年５月23日以前には、この部に従って情報セキュリティ・プログラムを実施しなければならない。

⑸ サービス契約の二年間の延期

2002年６月24日以前に契約を締結する限り、サービス・プロバイダが適切な保護措置を維持するという要件を契約が含まなくとも、あなたのために又はあなたに代わってサービスを行う非系列の第三者と締結する契約は、2004年５月24日までは、第314.4条ｄ項の規定を満たすものとする。

（**なかがわ　かおり**・行政法務課）

2　個人情報が漏洩した場合の被害者への通知のモデルとなる規定

(1)　顧客情報への無権限アクセス及び顧客への通知のための対処プログラムについての省庁共通ガイダンス（連邦行政命令集第70巻15736頁）(抄)

Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (March 29, 2005)

（2005年３月29日現在）

中川　かおり訳

Ⅰ　背景

（略）

Ⅱ　対処プログラム

全国の何百万人の米国民が、個人情報窃盗の被害者となってきた。個人情報窃盗犯は、金融機関を含む多様な情報源から入手する個人情報を悪用し、個人情報窃盗を行う。そのため、金融機関は、情報に権限なくアクセスしようとする試みに対して顧客情報を保護するための防止的措置をとるべきである。たとえば、金融機関は、顧客情報システムについてアクセス制御を行うべきであり、顧客情報へのアクセスを許可されている被用者の身元調査を行わなければならない。しかし、それにもかかわらず生ずる顧客情報システムにおける顧客情報への権限のないアクセスの事件に取り組むためのリスクベースの対処プログラムを作成し、実施しなければならない。対処プログラムは、機関の情報セキュリティ・プログラムの主要な部分となっていなければならない。プログラムは、機関の規模及び複雑性に応じたものであって、その活動の性質及び範囲に合致したものでなければならない。

さらに、各機関は、国内外のサービス・プロバイダにより維持される顧客情報システムに含まれる顧客情報への権限のないアクセスの事件に対処できなければならない。そのため、機関とサービス・プロバイダの間の契約は、この協定に関係するガイドラインの義務及びこの論点に関して規制機関が発行している既存のガイダンスと調和する形で、サービス・プロバイダに対し、金融機関の顧客情報への権限のないアクセスの事件を扱うための適切な措置を要求するものでなければならない。そこには、機関によるこの対処プログラムの迅速な実施を可能にするように、サービス・プロバイダが、機関に対して、当該事件について直ちに通知をすることが含まれる。

A. 対処プログラムの要素

1．機関の対処プログラムは、最低限、次の手続を含まなければならない。

ａ．事件の性質及び範囲を評価し、いかなる顧客情報システムにおける、いかなる種類の顧客情報がアクセスされ、悪用されたかを特定すること。

ｂ．機関が、下記に定義するようなセンシティブな顧客情報への権限のないアクセス又は利用を含む事件に気づいた場合には、主たる連邦規制官に可能な限り迅速に通知すること。

ｃ．規制機関の疑わしい取引報告（Agencies' Suspicious Activity Report（"SAR"））についての規則と調和させつつ、適切な法執行機関に通知すること。これは、報告できる違反が進行中であるといった緊急の注意を要する連邦刑事犯

罪に関わる状況において、時宜にかなったSARを提出するのに加えて行うべきことである。

d．記録及び他の証拠を保存する間、たとえば、影響を受けた口座を監視し、凍結し、又は閉鎖することにより、顧客情報のさらなる権限のないアクセス又は利用を阻止するために、事件を封じ込め、制御する適切な措置をとること。

e．通知すべき場合には、顧客に通知すること。

2.顧客情報への権限のないアクセス事件が、機関のサービス・プロバイダが管理する顧客情報システムと関連する場合には、機関は、その顧客及び規制官に通知することを義務付けられる。ただし、機関は、機関に代わってその顧客又は規制官に通知するよう、サービス・プロバイダに権限を与え、又は契約することができる。

Ⅲ　顧客に対する通知

金融機関は、顧客の情報を、権限のないアクセス又は利用から保護する積極的な義務を負う。義務の主要部分は､下記に定める基準に従って、顧客の情報の権限のないアクセス又は利用に関するセキュリティ事件について顧客に通知することである。顧客に対する時宜にかなった通知は、機関の名声に対するリスクを管理するためにも重要である。効果的な通知は、機関の法的リスクを減らし、顧客との良好な関係の維持を支え、機関の顧客が、個人情報窃盗に対し、自ら防衛することを可能とする。顧客に対する通知をすべき場合に、機関が自らにとって不都合であるという理由で、事件を顧客に通知しないで済ませることは許されない。

A. 通知基準

金融機関が、センシティブな顧客情報への権限のないアクセスの事件に気づいたときは、機関は、情報がすでに悪用されたか又は今後悪用される可能性があるかを迅速に判断するために、相当の調査を行わなければならない。機関が、顧客情報がすでに悪用されたか又は今後悪用されると合理的に判断するときは、可能な限り迅速に、影響を受ける顧客に通知しなければならない。顧客への通知は、法執行機関が、通知を犯罪捜査の障害となると判断し、機関に対して通知の延期を書面で要請する場合には、延期することができる。ただし、機関は、通知が犯罪捜査の障害にならなくなった時点で、直ちに、顧客に通知をしなければならない。

1．センシティブな顧客情報

機関は、ガイドラインの下で、顧客に対して実質的な障害又は不利益を帰結するような顧客情報への権限のないアクセス又は利用に対し、防衛しなければならない。センシティブな顧客情報は、個人情報窃盗において最も悪用されやすいため、実質的な障害又は不利益は、こうした種類の情報への不適切なアクセスから生じやすい。このガイダンスの目的上、センシティブな顧客情報とは、顧客の氏名、住所又は電話番号と、社会保障番号、運転免許証番号、口座番号、クレジットカード若しくはデビットカードの番号又は顧客の口座へのアクセスを許容する個人識別番号若しくはパスワードとが組み合わされたものをいう。センシティブな顧客情報には、顧客の口座に何者かがログオン又はアクセスすることを許容する顧客情報の要素の組み合わせが含まれ、これには、ユーザー名とパスワード又はパスワードと口座番号といったものがある。

2．影響を受ける顧客

金融機関が、調査により、どの顧客情報が不適切にアクセスされたかをログ又は他のデータから判断できるときは、機関は、

情報の悪用が過去におきたか又は相当に可能であると判断する顧客に対してのみに、通知を限定することができる。しかし、機関が、複数のファイルが不適切にアクセスされたと判断できるが、どの個別の顧客情報がアクセスされたかを特定することはできない場合もある。もし、権限のないアクセスの状況から、情報の悪用が相当に可能であると機関が判断する場合には、複数のファイル内のすべての顧客に通知しなければならない。

B. 顧客への通知の内容

1．顧客への通知は、明確かつ明白な方法で行われなければならない。通知は、事件を一般的な言葉で説明し、また、権限のないアクセス又は利用の対象となった顧客情報の種類を説明しなければならない。また、機関が、さらなる無権限のアクセスから顧客情報を保護するためにとる措置を、一般的に説明しなければならない。加えて、顧客がさらなる情報と支援を求めることができるように、電話番号を明記しなければならない。通知は、顧客に対し、今後12月から24月の間は、特に注意する必要があること、及び、機関に対して、個人情報窃盗が疑われる事件を迅速に報告する必要があることを伝えなければならない。通知は、そうすることが適切な場合には、次の追加事項を含まなければならない。

ａ．顧客が、預金取引明細書を審査し、機関に対して疑わしい取引を報告するべきであるという勧告

ｂ．詐欺警告の説明及び顧客が詐欺の被害者であるかもしれないということを、顧客の債権者に対して通知するために、消費者信用報告に詐欺警告を記録する方法の説明

ｃ．顧客が全米規模の信用情報機関から消費者信用報告を定期的に入手し、詐欺的取引にあたる情報を削除させることの勧告

ｄ．顧客が消費者信用報告を無料で入手する方法の説明

ｅ．消費者が個人情報窃盗に対抗するためにとるべき手続きについて、連邦取引委員会のウェブサイト上でガイダンスが入手できるという情報。通知は、顧客が個人情報窃盗事件を連邦取引委員会に報告することを推奨するものでなければならず、顧客が個人情報窃盗のガイダンスを入手し、個人情報窃盗が疑われる事件を報告するために用いる連邦取引委員会のウェブサイトの URL と無料電話番号を提供するものでなければならない。

2．規制機関は、金融機関が、信用情報機関と連絡をとるための情報を含む通知を、多数の顧客に送る前に、全米信用情報機関に通知するよう推奨する。

C. 顧客通知の送付

合理的に考えて、顧客が受領することが期待されることを保障するよう計らう方法で、顧客通知は送付されなければならない。たとえば、金融機関は、影響を受けるすべての顧客に、電話若しくは郵便により通知し、又は、有効な電子メールアドレスを有し、通信を電子的に受領することに同意する顧客に、電子メールにより通知することを選択することができる。

（**なかがわ　かおり**・行政法務課）

(2) カリフォルニア州民事法典（抄）
第３節　義務
第４部　特定の取引から生ずる義務
第1.8編　個人データ
第１款　1977年情報慣行法
第７　開示の義務

California Civil Code
Division 3. Obligations
Part 4. Obligations Arising from Particular Transactions
Title 1.8. Personal Data
Chapter 1. Information Practices Act of 1977
Article 7. Accounting of Disclosures
（2006年９月30日現在）

中川　かおり訳

第1798.29条　コンピュータ化されたデータを所有し、又は管理する機関による、セキュリティ違反の開示

(a)　個人情報を含むコンピュータ化されたデータを所有し、又は、使用を許可する機関（agency[注1]）は、暗号化されていないカリフォルニア州民の個人情報が権限のない人により取得された場合又は合理的に考えて取得されたと考えられる場合には、その州民に対して、データの安全性違反を開示し、又は通知した後に、システムの安全性違反を開示しなければならない。開示は、c項に定められる法執行の正当な必要性と矛盾せず、又は、違反の範囲を確定し、データシステムの相当の完全性を回復するために必要な措置と矛盾せずに、可能な限り最も迅速に、かつ不合理な遅延なく、行われなければならない。

(b)　自らが所有しない個人情報を含むコンピュータ化されたデータを管理する機関は、個人情報が権限のない人により取得されたとき又は合理的に考えて取得されたと考えられるときは、情報の所有者又は使用許可権者に対し、発見後迅速にデータの安全性違反を通知しなければならない。

(c)　この条により要求される通知は、法執行機関が、通知が犯罪捜査を阻害すると判断する場合には、延期されうる。この条により要求される通知は、捜査を損なわないと法執行機関が判断した後に行われる。

(d)　この条の目的上、「システムの安全性違反（breach of the security of the system）」とは、機関により管理される個人情報の安全性、秘密性又は完全性を損なうような、コンピュータ化されたデータの権限のない取得を意味する。機関の目的のために、機関の被用者又は職員が個人情報を善意で取得することは、個人情報がさらなる権限のない開示のために用いられ、又は、服することがない限り、システムの安全性違反とはされない。

(e)　この条の目的上、「個人情報（personal information）」とは、個人のファーストネーム又はファーストネームのイニシャル及び姓と、次に掲げる一又はそれ以上のデータ要素の組み合わせを意味する。ただし、姓名又はデータ要素のいずれもが暗号化されていない場合とする。

(1) 社会保障番号
(2) 運転免許証番号又はカリフォルニア身分証明書番号
(3) 口座番号又はクレジットカード若しくはデビッドカードの番号と、個人の金融口座にアクセスを許されるために必要なセキュリティ・コード、アクセスコード又はパスワードの組み合わせ

(f) この条の目的上、「個人情報（personal information）」には、連邦政府、州政府又は地方政府の記録から一般公衆が合法的に入手できる一般的な情報を含まない。

(g) この条の目的上、「通知（notice）」は次のいずれかの方法で行われうる。
(1) 書面による通知
(2) 提供される通知が、合衆国法典第15編第7001条に定められる電子記録及び電子署名に関する規定と矛盾しない場合には、電子的通知
(3) 機関が、通知を行う費用が250,000ドルを超えること、通知を受けるべき影響を受ける対象者の集団が500,000名を超えること又は機関が連絡のための十分な情報を有していないことを証明する場合には、代替的通知。代替的通知とは、次のものをいう。
(a) 機関が対象者の電子メール・アドレスを有するときは電子メールによる通知
(b) 機関がウェブサイトを有する場合には、そのウェブサイトにおける明白な通知の掲示
(c) 主要な全州規模のメディアに対する通知

(h) g項にかかわらず、個人情報の取扱いのために情報セキュリティ・ポリシーの一部として通知手続きを維持し、それ以外の点ではこの部に定める時期の要件に従っている機関は、システムの安全性違反がおきたときにそのポリシーに従って対象者に通知する場合には、この条の通知要件に従っているものとみなされる。

(1)「機関（agency）」とは、州の省庁、職員、部、局、委員会又は他の州の機関をいう。ただし、立法府、司法府、州保障保険基金、カウンティ等の地方機関は含まれない。（Cal. Civ. Code § 1798.3）

（**なかがわ　かおり**・行政法務課）

カリフォルニア州民事法典（抄）
第３節　義務
第４部　特定の取引から生ずる義務
第1.81編　顧客の記録

California Civil Code
Division 3. Obligations
Part 4. Obligations Arising from Particular Transactions
Title 1.81. Customer Records
（2006年９月30日現在）

中川　かおり訳

第1798.82条　個人情報を含むコンピュータ化されたデータを維持する企業による漏洩の危険性の開示

(a)　個人情報を含むコンピュータ化されたデータを所有し、又は、使用を許可する個人又は企業は、権限のない人により暗号化されていないカリフォルニア州民の個人情報が取得された場合又は合理的に考えて取得されたと考えられる場合には、その州民に対して、データの安全性違反を開示し、又は通知した後に、システムの安全性違反を開示しなければならない。開示は、c 項に定められる法執行の正当な必要性と矛盾せず、又は、違反の範囲を確定し、データ・システムの相当の完全性を回復するために必要な措置と矛盾せずに、可能な限り最も迅速に、かつ不合理な遅延なく、行われなければならない。

(b)　自らが所有しない個人情報を含むコンピュータ化されたデータを管理する個人又は企業は、個人情報が権限のない人により取得されたとき又は合理的に考えて取得されたと考えられるときは、情報の所有者又は使用許可権者に対し、発見後速やかにデータの安全性違反を通知しなければならない。

(c)　この条により要求される通知は、法執行機関が、通知が犯罪捜査を阻害すると判断する場合には、延期されうる。この条により要求される通知は、捜査を損なわないと法執行機関が判断した後に行われる。

(d)　この条の目的上、「システムの安全性違反（breach of the security of the system）」とは、個人又は企業により管理される個人情報の安全性、秘密性又は完全性を損なうような、コンピュータ化されたデータの権限のない取得を意味する。個人又は企業の目的のために、個人又は企業の被用者又は職員が個人情報を善意で取得することは、個人情報がさらなる権限のない開示のために用いられ、又は、服することがない限り、システムの安全性違反とはされない。

(e)　この条の目的上、「個人情報（personal information）」とは、個人のファーストネーム又はファーストネームのイニシャル及び姓と、次に掲げる一又はそれ以上のデータ要素の組み合わせを意味する。ただし、姓名又はデータ要素のいずれかが暗号化されていない場合とする。

(1)　社会保障番号

(2)　運転免許証番号又はカリフォルニア身分証明書番号

(3)　口座番号又はクレジットカード若しくはデビッドカードの番号と、個人の金融口座

にアクセスを許されるために必要なセキュリティ・コード、アクセス・コード又はパスワードの組み合わせ

(f) この条の目的上、「個人情報（personal information）」には、連邦政府、州政府又は地方政府の記録から一般公衆が合法的に入手できる一般的な情報を含まない。

(g) この条の目的上、「通知（notice）」は次のいずれかの方法で行われうる。

(1) 書面による通知

(2) 提供される通知が合衆国法典第15編第7001条に定められる電子記録及び電子署名に関する規定と矛盾しない場合には、電子的通知

(3) 個人又は企業が、通知を行う費用が250,000ドルを超えること、通知を受けるべき影響を受ける対象者の集団が500,000名を超えること又は個人若しくは企業が連絡のための十分な情報を有していないことを証明する場合には、代替的通知。代替的通知は、次のものをいう。

(A) 個人又は企業が対象者の電子メール・アドレスを有するときは電子メールによる通知

(B) 個人又は企業がウェブサイトを有する場合には、そのウェブサイトにおける明白な通知の掲示

(C) 主要な全州規模のメディアに対する通知

(h) g項にかかわらず、個人情報の取扱いのために情報セキュリティ・ポリシーの一部として通知手続きを維持し、それ以外の点ではこの部に定める時期の要件に従っている個人又は企業は、システムの安全性違反がおきたときにそのポリシーに従って対象者に通知する場合には、この条の通知要件に従っているものとみなされる。

（**なかがわ　かおり**・行政法務課）

3　社会保障番号の利用制限のモデルとなる規定
(1)　カリフォルニア州民事法典（抄）
第3節　義務
第4部　特定の取引から生ずる義務
第1.81.1編　社会保障番号の秘密保持

California Civil Code
Division 3. Obligations
Part 4. Obligations Arising from Particular Transactions
Title 1.81.1. Confidentiality of Social Security Numbers
（2006年9月30日現在）

中川　かおり訳

第1798.85条　社会保障番号の特定の利用の禁止；例外；条の適用可能性

(a) この条に定めのある場合を除き、個人又は団体は、次のことを行ってはならない。

(1) 個人の社会保障番号を公衆掲示又は公衆表示すること。「公衆掲示（publicly post）」又は「公衆表示（publicly display）」とは、一般公衆に対して、故意に伝えること又は入手可能とすることをいう。

⑵　個人又は団体により提供される製品又はサービスに個人がアクセスするために必要とされるカードに、個人の社会保障番号を印字すること。
⑶　通信が安全である場合又は社会保障番号が暗号化されている場合を除き、インターネットを通じて個人に社会保障番号を送信するよう求めること。
⑷　インターネットのウェブサイトにアクセスするときに、社会保障番号だけでなく、パスワード又は固有の個人識別番号又は他の認証手段もまた要求される場合を除き、インターネット・ウェブサイトにアクセスするために社会保障番号を利用するよう個人に求めること。
⑸　州又は連邦の法律が郵送文書に社会保障番号を印字すること求める場合を除き、個人に郵送される資料に、個人の社会保障番号を印字すること。この号にかかわらず、社会保障番号は、申請過程又は登録過程において送付される文書、口座、契約又は保険証書を創設し、変更し、又は終了させるために送付される文書、又は、社会保障番号の正確性を確認するために送付される文書を含む、郵送される申請書及び書式に印字することができる。この条の下で郵送することが許される社会保障番号は、その全部若しくは一部が、はがき若しくは封筒を必要としない他の郵送手段に印字されてはならず、又は、封筒上に印字され、若しくは封筒を開封することなしに見ることが可能であってはならない。
⑹　この条は、州法若しくは連邦法により要求される社会保障番号の収集、利用若しくは提示又は内部的な確認若しくは管理目的での社会保障番号の利用を阻止しない。
⑹　政府法典の第１編第７節の第3.5款（第6250条以下）、第14款（第7150条以下）若しくは第14.5款（第7220条以下）、第２編第３節第１部第１款の第９章（第11120条以下）又は第５編第２節第１部第９款（第54950条以下）に従って記録され、又は、公衆に開かれた形で保存することが要求される文書には、この条は適用されない。この条は、カリフォルニア憲法Ⅵ節のために定められた機関により一般公衆に入手可能であることを、法律、判例又はカリフォルニア法廷規則により要求される記録にも適用されない。
⑹⑹　略
⑹　個人又は団体は、この条に要求されるところに従って、社会保障番号を除去するかわりに、バーコード、チップ、マグネティック・ストリップ又は他の技術を用いること等により、カード又は書面に社会保障番号をコード化したり、埋め込んだりしてはならない。
⑹－⑹　略

第1798.86条　この編の規定の免除の無効性

この編の規定の免除は、公共政策に反し、無効であり、執行できない。

（**なかがわ　かおり**・行政法務課）

(2) カリフォルニア州家族法典（抄）
第６節　無効、解消及び法律上の別離
第１部　一般規定
第３款　手続規定

Family Code
Division 6. Nullity, Dissolution, and Legal Separation
Part 1. General Provisions
Chapter 3. Procedural Provisions
（2006年９月30日現在）

中川　かおり訳

第2024.5条　法廷記録における社会保障番号の省略

(a)　b項に定められる場合を除き、原告又は被告は、婚姻の解消、婚姻の無効又は法律上の別離のための申請に従って裁判所に提出される訴答文、付属文書、書面又は他の文書から、社会保障番号を省略することができる。訴状又は答弁書を提出するために用いられる司法委員会の書式は、裁判所に提出される訴答文、付属文書、書面又は他の資料から、当事者が社会保障番号を省略することができるとする通知を含まなければならない。

(b)　扶養費に関する判決の要約、第4014条b項に従って要求される書式又は児童若しくは配偶者の扶養費を徴収する目的で作成される同様の書式は、a項に従って社会保障番号を省略してはならない。

（**なかがわ　かおり**・行政法務課）

4　消費者信用報告の凍結のモデルとなる規定
カリフォルニア州民事法典（抄）
第３節　義務
第４部　特定の取引から生ずる義務
第1.6編　信用情報機関法
第２款　信用情報機関の義務

California Civil Code
Division 3. Obligations
Part 4. Obligations Arising from Particular Transactions
Title 1.6. Consumer Credit Reporting Agencies Act
Chapter 2. Obligations of Consumer Credit Reporting Agencies
（2006年９月30日現在）

中川　かおり訳

第1785.11.2条　消費者の請求を受けた信用報告のセキュリティ凍結；凍結措置の除去又は一時的解除；手続；期間；適用可能性；料金

(a)　消費者は、信用情報機関に配達証明郵便により書面で請求することにより、信用報告に、セキュリティ凍結を記録することを選択することができる。「セキュリティ凍結（security freeze）」とは、消費者の請求により行い、かつ、一定の例外に服する、消費者信用報告に記録される通知をいい、消費者の明確な授権なしに、消費者の信用報告その他の情報を開示することを信用情報機関に禁止するものである。セキュリティ凍結が記録される場合には、消費者信用報告の情報は、消費者から事前に明確な授権がなされないかぎりは、第三者に提供されることはない。この項は、信用情報機関が、消費者の信用報告につき、セキュリティ凍結が実施されていることを第三者に通知することを禁止するものではない。

(b)　信用情報機関は、消費者から書面による請求を受け取ってから５営業日内に消費者の信用報告に、セキュリティ凍結を記録しなければならない。

(c)　信用情報機関は、消費者に対して10営業日以内にセキュリティ凍結に関する書面による確認を送付し、消費者が、特定の団体に対して、又は特定の期間において、信用情報を提供することを授権する場合に、消費者が利用する個人識別番号又はパスワードを提供しなければならない。

(d)　消費者が、その信用報告に対する凍結が記録されている間に、特定の団体に対して、又は特定の期間において、信用報告へのアクセスを許容したい場合には、信用情報機関に連絡し、凍結を一時的に解除するよう要請し、次の情報を提供する。

(1)　第1785.15条ｃ項に定める適切な身元情報[注2]

(2)　ｃ項に従って信用情報機関が提供する個人識別番号又はパスワード

(3)　信用報告を受け取る第三者又は信用報告の利用者が信用報告を利用できる期間についての適切な情報

(e)　ｄ項に従って信用報告の凍結を一時的に解除するよう、消費者から請求を受けた信用情報機関は、請求を受けてから３営業日内に請

求に従わなければならない。

(f) 信用情報機関は、d 項に従って信用報告の凍結を一時的に解除するようにとの消費者からの請求を、迅速に受理し、処理するために、電話、ファクス、インターネットその他の電子的メディアの利用を含む手続きを作成することができる。

(g) 信用情報機関は、次の場合にのみ、消費者の信用報告に記録された凍結を除去し、又は一時的に解除しなければならない。

(1) 消費者の請求を受けて、d 項又は j 項にしたがう場合。

(2) 消費者の信用報告が、消費者による重大な事実の詐称のために凍結された場合。信用情報機関がこのパラグラフに従って消費者の報告に対する凍結を除去しようと意図するときは、信用情報機関は、消費者信用報告の凍結を除去する前に、書面で消費者に対して通知しなければならない。

(h) 第三者が、セキュリティ凍結が実施されている消費者信用報告へのアクセスを請求し、この請求がクレジット又は他の利用のための申請にかかわるものであって、その特定の第三者に対して又は期間において消費者が信用報告へのアクセスを許容しないときは、第三者は、その申請を不完全なものとして扱うことができる。

(i) 消費者がセキュリティ凍結を請求する場合には、信用情報機関は、凍結の記録又は一時的解除の手続について、及び凍結が記録されている間に、特定の団体又は期間について、消費者の信用報告情報へのアクセスを許容する手続について、開示しなければならない。

(j) セキュリティ凍結は、消費者が、セキュリティ凍結の除去を請求するまで、記録される。信用情報機関は、次の双方を提供する消費者から除去の請求を受けてから 3 営業日内にセキュリティ凍結を除去しなければならない。

(1) 第1785.15条 c 項に定める適切な身元情報

(2) c 項に従って信用情報機関が提供する個人識別番号又はパスワード

(k) 信用情報機関は、セキュリティ凍結の記録又は除去を請求する人につき、第1785.15条 c 項に定める適切な身元情報を請求しなければならない。

(l) この条の規定は、次のいずれかの者による消費者信用報告の利用には適用されない。

(1) 金融債務について消費者が、義務履行以前から当座預金口座を含む口座若しくは契約を有する若しくは有していた場合に、その債権の購入提案に関わる個人若しくは団体若しくはその個人若しくは団体の補助者、補助員若しくは代理人、その個人若しくは団体に対して消費者が負う金融債務の指定者、若しくは、その個人若しくは団体に対して消費者が負う金融債務の指定予定者、又は、口座を審査する目的若しくは口座、契約若しくは流通証券について負う金融債権を回収する目的で、消費者が流通証券を発行する相手方たる個人若しくは団体若しくはその個人若しくは団体の補助者、補助員若しくは代理人、その個人若しくは団体に対して消費者が負う金融債務の指定者、若しくは、その個人若しくは団体に対して消費者が負う金融債務の指定予定者。この号の目的上、「口座を審査する」とは、口座の維持、監視、貸出限度額の引上げ並びに口座の格上げ及び強化に関する行為を含む。

(2) 信用の拡大又は他の許容される利用を促進する目的で、第1785.11.2条 d 項に基づきアクセスが認められる者の補助者、補助員、代理人、指定者又は指定予定者

(3) 裁判所命令、令状又は罰則付召喚令状に従う州若しくは地方の機関、法執行機関、事実審裁判所又は民間債権回収機関

⑷ 家族法典第17節第２款又は社会保障法IV-D編（42 U.S.C. et.seq）に従う児童支援機関
⑸ カリフォルニア州医療保障プログラム（Medi-Cal）の詐欺を調べるために行動する州の保健福祉サービス省又はその代理人若しくはその受託者
⑹ 未回収の税若しくは未払いの裁判所命令を調査し、若しくは回収するため、又は、他の法的な責任を執行するために行動する税委員会（Franchise Tax Board）又はその代理人若しくは受託者
⑺ 連邦公正信用報告法により定められるプレスクリーニング(注3)の目的のための信用情報の利用
⑻ 消費者が契約した信用ファイル監視契約サービスを運営する個人又は団体
⑼ 消費者の請求を受けて信用報告の写しを消費者に提供する目的を有する個人又は団体

⒨ この法律は、信用情報機関が、消費者に対して、凍結、凍結の除去若しくは一定期間の一時的な凍結の解除のために10ドル以下の料金を課すること又は消費者信用報告へのアクセスに関して、特定の団体のための一時的な凍結の解除のために12ドル以下の料金を課することを禁止するものではない。ただし、信用情報機関は、有効な警察報告書又は刑法典第530.5条の違反を主張する有効な自動車省による捜査報告書を提出する個人情報窃盗の被害者に対して、料金を課してはならない。

第1785.11.3条　セキュリティ凍結が記録されている場合の信用情報機関の義務

⒜ セキュリティ凍結が記録されているときは、信用情報機関は、変更が消費者ファイルに掲示されてから30日内に、消費者に対し、変更につき、書面による確認を送付することなしに、消費者信用報告における氏名、生年月日、社会保障番号及び住所といった公的情報を変更してはならない。書面による確認は、氏名及び住所の省略、綴り又は数字若しくは文字の転置を含む消費者の公的情報の技術的修正については、不要とする。住所の変更の場合には、書面による確認は、新住所と旧住所の双方に送付される。
⒝ 消費者が、セキュリティ警告を記録する場合には、信用情報機関は、その消費者の要請を受けて、90日間のセキュリティ警告の期間が終了するときに、その信用報告の無料の写しを提供しなければならない。

⑵「b項でいう「適切な身元情報」とは、一般に人を特定するのに十分であるとみなされる情報をいう。（以下略）」（Cal. Civ. Code § 1785.15(c)）
⑶「プレスクリーニング（prescreening）」とは、信用情報機関が、一定の基準を満たす消費者のリストを編集・作成し、提供するプロセスをいう。作成された消費者リストは、その依頼人または（ダイレクト・メール業者のような）依頼人にかわる第三者に提供され、リスト上の消費者に対して依頼人の製品やサービスの購入を勧誘するために利用される。「特集：アメリカ『公正信用報告法』の全容」『クレジット研究』20号，1998. 9，p.139.

（**なかがわ　かおり**・行政法務課）