法務総合研究所

研究部報告

36

個人情報に関連する犯罪に関する研究

2007

法務総合研究所

はしがき

この研究部報告第36号は，法務総合研究所の研究部と国際連合研修協力部（国連アジア極東犯罪防止研修所）が平成17年度及び18年度に共同で実施した，「個人情報に関連する犯罪に関する研究」の結果を取りまとめて刊行するものである。

近時，我が国では，氏名，住所，インターネット利用時におけるID，パスワードといった個人識別情報の漏えい事件，流出した個人情報を悪用した他人の成りすましによる各種事件が報道されている。成りすましによる犯罪は，他人の成りすましと知らずに欺かれて取引・手続に応じた側にも，情報を悪用された本人にも被害を及ぼし，その内容も財産的なものから信用・名誉といった非財産的なものまで広範なものとなる。その深刻さは，国際的にも認識され，国連犯罪防止・刑事司法委員会において取り上げられ，現在，各国の状況に関する調査研究が行われている。

本研究の対象となったアメリカ合衆国は，早くから個人情報の所持・移転・使用行為を禁止するIdentity Theft罪を連邦法上の犯罪とし，被害防止のための各種対策を講じている先進国である。カナダは，上記国連での調査研究において積極的な役割を果たし，国内的にはアメリカ合衆国類似の罪の創設を検討しながら，被害防止対策を実施している。本報告は，両国において社会的に利用されている個人情報の種類・役割といった背景を踏まえて，立法的及び犯罪被害防止のための各種取組みについて取りまとめるとともに，我が国において社会的に利用されている個人情報の種類・役割と，他人の個人情報を悪用した犯罪への対策について分析を行ったものである。本報告が今後の我が国の個人情報関連犯罪対策を検討するに当たっての基礎的な資料を提供するところとなれば幸いである。

おわりに，本研究の実施に当たって御協力をいただいた調査対象諸国の関係機関及び関係者並びに在外の日本国大使館等の関係機関の方々に対し，改めて謝意を表する次第である。

平成19年3月

法務総合研究所長
松　永　榮　治

要　旨　紹　介

本報告を利用するに当たっての参考に，その要旨を紹介する。

1　アメリカ合衆国

(1)　Identity Theft 罪

アメリカ合衆国（以下「アメリカ」という。）では，1998年に成立した連邦法（Identity Theft and Assumption Deterrence Act）により，違法な目的で権限なく他人の個人識別情報を「移転」又は「使用」することを禁止する Identity Theft 罪（以下「ID Theft 罪」という。）が創設された。さらに，2005年に成立した連邦法（Identity Theft Penalty Enhancement Act）により，「所持」行為も禁止対象となったほか，加重 ID Theft 罪が新設された。

これらの連邦法は，実在の自然人(生存・死亡を問わない。)の，氏名，生年月日，社会保障番号(Social Security Number)，クレジットカード情報，指紋等の生体認証情報等の移転，所持，又は使用を禁止するものである。

また，二重主権国家であるアメリカでは，48の州法上で別途，ID Theft 罪が犯罪化されている。

(2)　個人情報関連犯罪の動向

ID Theft 罪が創設される前の1995～1997年（会計年度）に，U.S. シークレットサービスが逮捕した経済事犯のほとんど（93～94%）が，何らかの形で他人の個人識別情報を不正取得又は使用した事犯であり，事件数にも増加傾向が認められた。また，同会計年度期間中，合衆国郵政観察(U.S. Postal Inspection Service)が実施した捜査によると，他人の郵便物を勝手に転送して盗む郵便窃盗事案の大幅な増加と，郵便窃盗担当者と不正取得にかかるクレジットカード悪用者などとの犯行手口の役割分担及び組織化傾向が認められた。1997年度中，米国ビザ社（VISA U.S.A. Inc.）が提携している銀行が，クレジットカードの不正取引によって受けた損失は，4億9千万ドルにも及んだ。このような状況に対処するため，ID Theft 罪が創設された。

連邦商取引委員会（Federal Trade Commission）が把握した ID Theft の被害申告件数は，2003年は21万5,177件，2004年は24万6,847件，2005年は，25万5,565件と，年々増加している。被害態様の面では，クレジットカード関係（新規のクレジットカード口座の作成，既存のクレジットカード口座の悪用）が最も多いほか，被害者名義の冒用による携帯電話契約の締結・銀行口座の開設・就職・借財等が認められた。また，被害者名義で犯罪が行われたことによる身に覚えの無い刑事責任の追及，インターネットやEメール名義の盗用等の多様な被害が認められた。

(3)　関係機関による被害防止のための取組み

連邦商取引委員会では，電話とインターネットによる ID Theft 被害相談受付窓口を設置し，各被害者に助言を与えるほか，被害予防のための分かりやすいパンフレットを配布するなどして啓発活動を行っている。また，集積された被害申告をデータベース化し，国内外の関係機関に情報提供を行い，犯罪摘発等に役立てている。

2　カナダ

(1)　ID Theft 行為に対する法的規制

カナダでは，アメリカでいう ID Theft 罪に相当する犯罪規定はないが，個人識別情報の悪用による犯

罪に対処するため，他人の個人識別情報を取得し，移転し，所持し，使用する行為を犯罪化してはどうかという議論がある。

カナダの現行法による規制状況は，我が国のそれと類似している。すなわち，クレジットカード情報等の財産権に関する情報を除き，氏名，生年月日，住所といった非財産的情報の不正な入手，所持は，窃盗，詐欺等の既存の犯罪類型では処罰できない。非財産的情報の使用行為に関しては，旅券の偽造罪等によって処罰される場合がある。

選挙における不正行為を取り締まることを想定して作られた詐称罪（personation）は，実在する自然人（死者・生者を問わない。）に成りすます行為を禁止しているが，実際上，あまり活用されていない。

(2) 関係機関による被害防止の取組み

連邦警察とオンタリオ州警察が共同運営するフォンバスターズ（Phone Busters）は，コールセンターを設置し，ID Theftや詐欺等の被害相談を受け，助言等を行い，インターネットやパンフレットによる犯罪予防・啓蒙活動を行っているほか，データの収集，分析を行い，各法執行機関に情報提供し，犯罪摘発に役立てている。

また，連邦警察等によって，RECOL（Reporting Economic Crime On-Line）という24時間オンライン被害受付窓口も設置されている。

産業省（Industry Canada）内の消費者問題対応室（Office of Consumer Affairs）を中心に発足した各州・準州の代表が参加する消費者委員会（Consumer Measures Committee）では，立法によるID Theft規制の議論を行うほか，一般消費者向け及び企業向けに被害防止のためのパンフレットを配布するなどしている。

3 日 本

(1) 各種個人識別手段の利用の実態

我が国で個人の身元を証明する手段として広く使われ社会的信頼度の高い，自動車運転免許証，健康保険被保険者証，住民票，旅券，外国人登録証明書について，東京地方裁判所で判決のあった詐欺事案を参考に，不正使用の実態について検討したところ，これらの身分証明文書のいずれもが身元詐称による不正な入手や偽造の危険にさらされていること及びこれらの身分証明文書を用いた他人名義による預貯金口座の通帳・キャッシュカードの不正入手，消費者金融での借財，携帯電話契約が多く行われていることが認められた。

(2) 立法対策の状況

個人情報の不正な取得，所持，移転，使用という一連の行為のうち，我が国では現行法上，原則として，使用行為による法益侵害（文書偽造，詐欺，不法入国等）が発生するまで，処罰対象とはなっていない。例外的に情報そのものの取得，所持，移転等が処罰されるものとして，支払用カードに関する電磁的記録の情報の取得，提供，保管（刑法第163条の４），営業秘密の記録媒体等の複製の作成（不正競争防止法第21条第１項第５号ロ），預貯金口座キャッシュカード暗証番号，ネットバンキングのID，パスワードの授受（金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律第16条の２）等がある。

インターネットを悪用した個人情報の不正取得が行われるフィッシングに対しては，有名企業のホームページに酷似する偽のホームページを作成し公表する行為を著作権法違反として擬律し，取得した他人のID，パスワード等の個人情報を用いた不正アクセス行為が認められれば，さらに不正アクセス行為の禁止等に関する法律違反として擬律することによって対処した事案がある。

このほか，個人情報の不正な取得行為に対処するため，「住民基本台帳法の一部を改正する法律」（平成18年法律第74号）によって，従来，何人でも不特定多数の個人情報について閲覧請求が可能であった制度が改められ，閲覧可能な条件が限定されるとともに，違反に対する罰則も定められた。また，成りすまし行為に対処するため，「金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律」（平成14年法律第32号）によって，金融機関等による顧客の本人確認が義務付けられ，通帳等の不正な譲渡が罰則付きで禁止されるようになったほか，「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律」（平成17年法律第31号）によって，携帯電話事業者による顧客の本人確認が義務付けられ，本人確認を行わない携帯電話端末の授受等が罰則付きで禁止されるようになった。

現在審議中の「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」により不正指令電磁的記録等作成等の罪が新設されると，スパイウェアなどの不正プログラムを用いて他人の情報を取得する場合について，不正プログラムを実行の用に供したという形で処罰が可能になることも考えられる。

研究部長
窪　田　守　雄

個人情報に関連する犯罪に関する研究

研 究 官　太 田 玲 子
法務省矯正局付（前 教 官）　池 田 暁 子
研究官補　姫 田 卓 朗

目　　次

第1　はじめに

情報通信技術の進展・普及により，従来，書面等で物理的に管理されていた情報が電子データ化し，地理的な制約とは無関係に個々人のレベルでも世界規模での情報の受発信が可能となった。このことにより，物流や金融における効率性が高まるなどの好ましい結果も生まれているが，その反面において，犯罪者に対しても，利用主体が特定されず，証拠隠滅も容易で，かつ，外部からの可視性もない形での迅速な犯行手段を提供することとなった。

こういった，コンピュータやインターネット空間を利用する，いわゆるハイテク犯罪[1]については，本邦でも，銀行端末へのデータ不正入力によって架空名義口座へ振り込み送金をした「三和銀行事件（大阪地判昭和57・7・27判例時報1059号158頁）」など，1980年代から問題になり始めた。そして，電磁的記録の文書性についてなど，既存の法文の解釈論[2]だけでは対処しきれない新しい論点を多く提示するようになったことから，順次ハイテク犯罪に対する法整備が進められている[3]。

その中で，近時個人を特定するための名前や各種パスワードなどの情報（以下，「個人情報」という。）の漏洩事件や，流失した情報が悪用される事例が多く報道されている。また，フィッシング（phishing）と呼ばれる手口など巧妙な形態での個人情報の不正取得行為も登場しているところ，これらは犯行としての秘密性，罪証隠滅の容易性など，ハイテク犯罪特有の問題を抱えるのみならず，情報の不正取得の犯罪化の検討など，法理論上の問題点も提示する。

また他人になりすましての犯行によって発生する被害は，犯行者が提示するその主体性に関する情報を信じて取引や手続きに応じた側にも，情報を悪用された本人にも発生するという点，被害の種類が財

1　ハイテク犯罪は，①コンピュータ又は電磁的記録を対象とする犯罪，②コンピュータ・ネットワークを利用して行われる犯罪，③コンピュータ・システムへの無権限アクセス行為に大別される。

2　キャッシュカードの磁気テープ部分を「偽造」し，現金自動支払機から現金を窃取した近畿相銀事件（大阪地判昭和57・9・9判例時報1067号159頁）等。

3　昭和62年に，刑法一部改正（昭和62年法律第52号）によって電磁的記録についての不正作出・供用（刑法157条1項，158条，161条の2），電子計算機損壊等業務妨害（同法234条の2），電子計算機使用詐欺（同法246条の2）が犯罪化された。さらに，クレジットカード，プリペイドカード等の支払用カードの不正コピー被害が頻出するなどを受けて，平成13年の刑法一部改正（平成13年法律第97号）によって刑法第18章の2「支払用カード電磁的記録に関する罪」が追加され，支払用カードの電磁的記録不正作出等（同法163条の2），その準備行為としてのかかる電磁的記録の情報の取得等（同条の4），不正電磁的記録カード所持（同条の3）などが犯罪化された。

特別法においても，平成11年に一定のコンピュータの無権限使用行為等を禁止する不正アクセス行為の禁止等に関する法律（平成11年法律第128号）が，平成15年にインターネットを利用してのいわゆる援助交際斡旋などを規制するインターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律（平成15年法律第83号）が，平成16年に電気通信回線を通じての児童ポルノの提供等や，電磁的記録での児童ポルノの保管等を禁止するための，児童買春，児童ポルノに係る行為等の処罰及び児童の保護等に関する法律の一部改正（平成16年法律106号による平成11年法律第52号の一部改正）が，それぞれ制定された。

さらに，平成13年に欧州評議会で採択されたサイバー犯罪に関する条約の締結を，我が国の国会も平成16年に承認しているところ，ハイテク犯罪に対処するとともに，同条約を締結するため，いわゆるコンピュータ・ウイルスの作成等を禁止する不正指令電磁的記録作成罪等，わいせつな電磁的記録の頒布行為を禁止するわいせつ物頒布罪の処罰対象の拡充に関する刑法改正のほか，捜査機関がプロバイダ等へ業務上保管している通信記録（ログ）のうち特定のものを一定期間消去しないことを求めることを可能とすることなど，電磁的記録にかかる記録媒体に関する証拠収集手続きを整備する刑事訴訟法の改正を含む犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案が国会提出中である（平成18年10月1日現在）。

産的なもの・非財産的なものを問わないという点，また，犯罪組織による組織的犯行の場合は，不特定多数の一般大衆に向けての犯行が可能であることから，個々の被害者の被害金額が少額であったとしても最終的な合計利益が莫大なものとなり，さらなる犯罪行為を増大させる簡易な資金源となる点，いずれをとっても，法執行機関にとって看過できない問題となっている。

国際社会においても，平成16年に開かれた国連犯罪防止・刑事司法委員会（Commission on Crime Prevention and Criminal Justice）第13回会期において国際的な大規模詐欺への対策を論じている中で，かかる大規模な詐欺事案では，得てして犯人が他人の個人情報を悪用して当該他人になりすましている（criminal misuse and falsification of identity）例が少なくないことから，このなりすましの現象自体も独自の問題点として取り上げるべきだと提案された。そして，現在，同委員会の上記提案を受けた経済社会理事会の決議2004/26に基づき，政府間専門家会合が開催されており，各国における個人情報の管理状況や悪用等について，現状の把握調査が行われている。

個人情報の流通や悪用をどのように規制するべきかという問題は，どのような情報が，当該社会内でどのような役割を果たしているのか，という文化・社会の違いによる差も大きいことが予想される。そこで本研究では，個人情報の所持・移転・使用行為を禁止するIdentity Theft（以下，「ID Theft」という。）罪が連邦法上の犯罪とされているアメリカ合衆国，また，同種行為についての犯罪化を検討し，上記国連での調査研究においても積極的な役割を果たしているカナダにおける個人情報に関連する犯罪についての規制状況などを比較した上，我が国での規制状況について検討したい[4]。

4 テーマの性質上，各国の規制状況などについては，日々変化が認められるところである。本稿の記述は，原則として，アメリカ合衆国及びカナダに関しては平成18年１月にカナダ司法省，PSEPC(後述)，産業省，アメリカ合衆国司法省，IC3（後述），公正取引委員会から聴取した内容に基づいている。

第2　本稿で検討を行った範囲

表題として「個人情報に関連する犯罪」とする趣旨は，前述したID Theft，または類似の表現として用いられているIdentity fraud（以下，「ID Fraud」という。）などの用語に，国際的に確立した定義が存在しないからである。例えば，国連では，個人情報の不正取得，保管，移転，悪用までの全過程をも含めた概念としてID Fraudを暫定的に用いているが[5]，アメリカでのID Theft罪には不正取得行為が含まれていない[6]。また，日本語の「情報の不正取得」や「なりすまし」では，アメリカのID Theft罪で問題となる「保管，移転」行為まで含まないなど，比較することが困難である。

なお，「個人情報」の意味としては，我が国の「個人情報の保護に関する法律（平成15年法律第57号。以下，「個人情報保護法」という。）」が，「生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む。）」として定義づけている（同法2条1項）。これは，情報の性質を問わない網羅的な定義であり，アメリカでのID Theft罪が保護対象とする“means of identification of another person（他人の身分証明の手段，後述）”ともほぼ同視できると考える。

そこで本稿では，英語同様，何が該当するのか若干不明瞭であるとしても，概念整理のため，個人情報の不正取得，保管，移転，悪用までの全過程及び関連する行為を指す網羅的な表現として「個人情報に関連する犯罪」を用いることとし，今後の議論の発展による適切な表現の発展を待つこととしたい。後述のアメリカないしカナダの説明時点で，原語において「ID Theft」ないし「ID Fraud」という用語が用いられている場合は，用いられている個々の場面毎の定義をするよう配慮しながら検討を進めることとする。

個人情報に関連する犯罪は，その視点によって，ハイテク犯罪捜査における技術的な問題，個人情報管理のあり方を含む企業内統制の問題，プライバシー法制など，多様な論点を提示する。しかし，ハイテク犯罪としての捜査技術的な検討については，過去の研究においても取り上げられているため，本稿では，具体的事例などを検討する上で必要な程度の記述にとどめる。

また，個人情報の管理の在り方の問題については，個人情報の保護の必要性という目的においては，本稿の対象と共通する。しかし，積極的に他人の主体性に関わる情報を流通・悪用する者の責任の在り方を論じる本稿と，個人情報を管理・利用することが許されている者の管理・利用の在り方の問題とは方向性が異なる。そこで本稿では，個人情報保護法もしくは各国のプライバシー法制については詳述しない。

さらに，近時，個人使用のパソコンから，スパイウェアやファイル共有プログラムなどを通じて，個人の特定にかかる情報のみならず，写真や日記などプライバシーに関わる情報も流出させることが問題視されており，こういったプライバシーに関わる情報も「個人情報」の問題として取り上げられること

5　前出2004/26決議

6　フィッシングで情報を得る行為とは別に，得た情報を用いて「なりすます」行為をID Theftとして紹介する例として，Rachael Lininger and Russel Dean Vines, “Phishing－Cutting the Identity Theft Line,” Wiley Publishing, Inc., 2005, pp. 1-25参照。「情報の不正取得」と，「なりすまし」をID Fraudとする例としては，“Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited.” United States General Accounting Office. GAO/GGD-98-100BR. May 1998, p. 1参照。

がある。しかし，本稿では，プライバシーに関わる情報をスパイウェアなどによって流出可能な情報の一つとして理解するに留め，「個人情報」に含めないで検討する。

なお，本報告書のうち意見にわたる部分は言うまでもなく筆者の個人的見解である。

第3　アメリカ

1　連邦と州との関係

(1)　政治体制

アメリカは，50の州とコロンビア特別区で構成される連邦制国家である。1776年にイギリスから独立した際には，各州が主権国であったが，1788年に発効した連邦憲法によって単なる国家連合から連邦制へと政体が変わった。このような歴史的背景から，現在でも各州が高度な自治権を持っている。

なお，コロンビア特別区については，連邦議会が，憲法の禁止規定に触れない限り各州議会と同じ立場で立法ができるので(連邦憲法第1条8節17項)，いわば州法としての連邦法と連邦法としての連邦法が存在している[7]。ひいては，アメリカでは，連邦と50州の合計51にわかれた刑事司法制度が存在する，といえる。

(2)　立　法

連邦と州との立法権限が重なる場合は，連邦の優位性が認められる（連邦憲法第6条2項)。しかし，連邦の立法範囲は，連邦議会は，連邦憲法によって禁止されている立法ができない（例えば，言論の自由を奪う内容の法律など）ほか，連邦憲法の明文上または解釈上連邦議会に与えられた立法権の範囲内でなければ立法ができない[8]という制約があるため，完全な上下関係にはない。

(3)　捜　査

アメリカでは，各政治単位が独自の法執行機関を有することができ，連邦と州との関係はもちろん，

7　同特別区における州法レベルの多くの事項については，同特別区の立法機関としての地位を有するDC Councilが制定する条例（DC Codeもしくは DC laws）が規定している。

8　連邦憲法上，連邦議会が罰則を定めうる旨の明文規定があるのは同憲法第1条8節6項（合衆国の証券及び通貨偽造罪)，同10項（公海上の海賊行為，重罪行為その他国際法違反行為についての処罰規定）及び第3条3節2項（反逆罪）のみである。それ以外の事項に関する一般的な立法事項としては，同憲法第1条8節の18項目が中心となる。そのほかにも，第1条4節1項（連邦議会の選挙関係)，第2条1節4項，同6項（大統領選挙関係)，第3条1節，同2節2項，同3項（連邦下級裁判所の設置関係など）及び修正条項上の規定が根拠とされる。

このうち，主として第1条8節18項で「上記の権限，およびこの憲法により合衆国政府またはその各部門もしくは公務員に対し付与された他の一切の権限を執行するために，必要かつ適切な（necessary and proper）すべての法律を制定すること」等と定められていることと，第1条8節3項（州際通商条項）で「外国との通商並びに各州間およびインディアンの部族との間の通商を規制すること」と定められていることが連邦議会の権限拡大解釈の根拠となってきた。

第1条8節18項の例としては，連邦司法権が海事事件にも及ぶことから(第3条2節1項)，この権限を執行するための「必要かつ適切な」法律として，この実施に「必要かつ適切な」海事事件訴訟法や実体法の立法が可能となることがあげられる（*Askew v. American Waterways Operators*, 411 U.S.325 (1973))。州際通商条項の適用範囲は，現在相当広範囲となっている。刑事罰との関係でもっとも広範な合憲解釈とされるのは，*Perez v. United States*（402 U. S. 146 (1971)）と思われる。これは，連邦法（Consumer Credit Protection Act, Title II, 82 Stat. 159 (1968), 18 U. S.C. § 891 et seq.）が，高利貸し（loan-sharking）による恐喝的取立て行為に刑罰規制を及ぼすことの合憲性が争われた事件である。最高裁の多数意見は，たとえ問題となっている高利貸し行為そのものは，一州内の活動であったとしても，恐喝的取立て行為を伴う高利貸し業は，一般に(in a class)，州際通商に有害な影響を及ぼす組織犯罪によって支配されているとして，連邦議会の立法権を認めた。

なお，個々の業者の営業形態はさておき，連邦法規制の及ぶ業種に該当するのであれば（in a class)，当該連邦法規制に従う，という部分の論理構成は，“Class of activity”テストとして，ホテル等一定業種における人種差別を禁止した連邦法（Civil Rights Act of 1964, Pub. L. 88-352, 78 Stat. 241）の合憲判決（*Atlanta Motel v. United States*, 379 U.S. 241 (1964)）を踏襲したものである。

州と市町村レベルでも上下関係がないことから，捜査機関については，重畳的で，複雑な組織形態となっている。郡や市町村レベルでは，警察（police department），保安官（marshal），警務員（constable），執行官（sheriff）及び副執行官（deputy），州レベルではハイウェイパトロールほかの警察力が組織されている。さらに，州も市も，一般警察活動を行う組織とは別に，州立大学構内の警察組織，市営交通警察など，特定の目的の警察組織をもつことがある。連邦政府は，司法省の連邦捜査局（以下，FBIという。）が警察業務を遂行しているほか，通貨，麻薬，酒類，銃砲，タバコ，国税，関税，移民など，特別法ごとに法執行機関[9]がある。州及び連邦各法執行機関の権限が重複する場合は，基本的に最初に事件捜査に着手した機関が捜査を遂行するが，機関間の情報交換や，訴追をにらんで連邦検察等からの調整機能により，合同捜査的手法がとられることもある。

(4) 司 法

州裁判所[10]と連邦裁判所の関係も，組織として上下関係がないため，各州法上の最終判断に対しては，連邦法上の根拠[11]なくして連邦裁判所で争うことができない。連邦裁判所は，連邦裁判所が管轄を有している事件のみを扱うことができ（連邦憲法第3編第2節第1項），州裁判所は，連邦の専属管轄が認められる事項以外で，かつその州の刑罰法規に違反した者に対する公訴を扱いうる。また，一つの行為が，連邦法上の犯罪と州法上の犯罪との両方に該当する場合，連邦法上の犯罪については連邦裁判所で，州法上の犯罪については州裁判所で刑事訴追を受けることもあり得るが，これは，二重の禁止には反しないとされている（*Bartkus v. Illinois*, 359 U.S. 121 (1959); *Abbate v. United States*, 359 U.S. 187 (1959))[12]。

2 Identity Theft 罪

(1) 立法の背景

アメリカで，上記ID Theft やID Fraud を直接規制する目的でIdentity Theft and Assumption Deterrence Act[13]（以下，「ID Theft 法という。」）が立法されたのは，1998年である。同年，Money

---

9 例えば，U.S. シークレットサービスは，1865年に連邦財務省の一部門として，通貨偽造等の捜査のためにスタートした法執行機関である。1901年のウィリアム・マッキンリー第25代大統領の暗殺をきっかけに，大統領ら政府高官の警備責任も担うようになった。現在の犯罪捜査の所管としては，連邦政府の金融システムにかかる犯罪（通貨や国債など連邦政府の債務に関する証券偽造，クレジットカード詐欺，電気通信網を使った詐欺，コンピュータ詐欺，個人情報を悪用した詐欺のほか，連邦政府が保証する金融機関に影響を与える犯罪などがある。United States Secret Service, "Frequently Asked Questions," 平成18年4月12日確認（http://www.secretservice.gov/faq.shtml#crimes2/18/2006)。

10 州裁判所の構成及び名称は，州によって異なる上，かなり複雑である。例えばニューヨーク州では，包括的に第1審管轄を有する裁判所をSupreme Court（ニューヨーク市のSupreme Courtのみ民・刑事両方を扱うが，それ以外の地区のSupreme Courtは民事のみを扱う。）またはCounty Court（郡裁判所）と呼び，中間上訴審については，Supreme Court内の上訴部門，最終上訴審をCourt of Appealsと呼ぶ。

11 平等原則違反（連邦憲法修正第14条）など。

12 ただし，連邦司法省の方針として，州で訴追された事件について，重ねて連邦で訴追することは控えている。この場合，いわゆる二重の危険の問題となるのは，実際に応訴の負担を負わされたことを意味するため，起訴はされたものの，適用された法律の文面違憲によって公訴棄却となった場合など，実質審理に入っていない場合には，上記方針とは無関係に，連邦での起訴を検討することができる。

13 アメリカでは，連邦法は全て，連邦法典（U.S. Code，以下，「U.S.C.」という。）に編成されており，U.S.C. の第18編（Title 18），第1部（Part I）が，刑事実体法を規定している。ID Theft 法（Pub. L. 105-318）は，Title 18－Part I－Chapter 47－Section 1028 "Fraud and related activity in connection with identification documents, authentication features, and information（身分証明文書の偽造犯として後述）" に，Section1028(a)(7)を挿入し，その他関連規

Laundering and Financial Crimes Strategy Act of 1998[14]によってマネーロンダリング罪が立法されている。そして，犯罪によって得た資金の規制がマネーロンダリング罪であるとすれば，ID Theft 罪は，各種詐欺罪などによって犯罪組織が資金を得る前提犯罪として位置づけられている。また，連邦司法省内でも ID Theft 事件を担当するのは詐欺課である[15]。

ID Theft 法立法過程において，会計検査院（General Accounting Office，以下，「GAO」という。）が連邦議会へ基礎報告をした際にも，ID Fraud を，「他人の，個人を特定する情報，例えば社会保障番号(後述)，生年月日，母親の婚前姓等を盗み，それらの情報を，新規クレジットカードを入手する，新たな負債を作る又は既存の金融口座を乗っ取るなどの犯行に用いること」と定義しており[16]，個人情報の流通規制が，経済犯対策であることをうかがわせる。

そして，GAO の報告によると，1995会計年度中に U.S. シークレットサービスが逮捕した経済犯罪事案中，93%（9,470件中8,860件）が上にあげた意味での ID Fraud を伴っていた。この件数は，1996年度が9,220件中8,686件（94%），1997年度が10,066件中9,455件（94%）と，実数的にも増加傾向が認められていた[17]。

また，なりすまされた結果として生じた実損以外にも，なりすまし被害による信用低下がなければ得られたであろう仕事が得られなかった，ローンが組めなくなった，などといった意味での被害も重大である。また，経済的被害にとどまらず，精神的な被害や，信用歴の回復に要した時間や労力の大きさも無視できない点が指摘されている[18]。

他方，前述のとおり，本稿で個人情報に関連する犯罪について検討することとしたきっかけは，個人情報に関連する犯罪が，フィッシングなど，犯行態様のハイテク化によって，質的に変化しているのではないかという問題意識があったからである。しかし，連邦司法省刑事局詐欺課の連邦検察官によると，アメリカでは，少なくとも同法の立法時，社会の IT 化による犯罪の性質の変化ということはさほど重視されていなかった。消費者詐欺[19]事案のように，犯罪が組織化することで多大な利潤が犯罪組織に流入す

定の改正を行った法律である。

14　(Pub. L. 105-310) Title 31 - Subtitle IV - Chapter 53 - Subchapter III - Section 5340 et. seq. Title 31 は，Money and Finance（通貨・金融）に関する編である。

15　組織犯罪としては，いわゆる RICO 法を担当する組織犯罪対策課も存在するが，問題となっている犯行が専ら詐欺課の領域の犯行であれば，詐欺課の所管となり，その他の RICO 法対象犯罪も含めて，RICO 法の適用となった場合は，組織犯罪課の管轄となる。

さらに，司法省内にはコンピュータ犯罪課もあるが，コンピュータ詐欺のように，権限が競合する場合，端緒となった課が，必要に応じてもう一方の専門性からの助言を請けながら捜査指導や訴追を担当する。

16　"Identity Fraud : Information on Prevalence, Cost, and Internet Impact is Limited." United States General Accounting Office. GAO/GGD-98-100BR. May 1998, p. 1.

17　Ibid., pp. 28-29

18　Ibid., pp. 48-49

19　消費者詐欺 (Consumer Fraud) とは，電話，郵便，インターネット等を通じた，不特定多数の被害者に向けられた詐欺一般を指す。欺罔内容としては，懸賞が当たったので，懸賞金受け取りに必要な手数料を払い込んでほしいなどという懸賞詐欺，ナイジェリアなどの西アフリカ諸国での独裁者などの蓄財資産を海外に移転するための振り込み口座を教えてもらいたいなどというナイジェリア詐欺（ナイジェリア刑法で詐欺罪が第419条に規定されていることから，西アフリカ詐欺，419詐欺とも呼ばれる。），低利子ローン勧誘のローン詐欺，など多様である。自動的に，機械が数理的に可能な電話番号配列に対してしらみつぶしに電話をかけ続け，反応のあったところにだけ人間が欺罔の電話をかけるなど，インターネット発生以前から，電話を通じた組織的犯行が見受けられていたため，tele-marketing fraud（電話商法詐欺）などとも言われる。日本におけるオレオレ詐欺，架空請求詐欺もこれの一種である。

る点が重視されていたとのことである[20]。GAOの調査の中でも，インターネットを使用する詐欺の増加とID Fraudの犯行とが関連しているとの直接の関連性は見つかっておらず，ただ，有効な暗号手段の開発が行われないと，インターネット経由でのID Fraud事件は増えるであろうとの予想がなされているに留まる[21]。

このように，ID TheftまたはID Fraudの犯罪化の必要性という意味では，その経済犯としての側面が重視されているのだが，その前提となっているアメリカの経済・社会システムでID Theftに関連すると思われる特色的な事項を幾つか紹介した上で，ID Theft法自体の紹介に移りたい。

(2) アメリカにおける特徴的な事項

ア 社会保障番号

本来の社会保障番号（Social Security Number。以下，「SSN」という。）は，日本で言う国民年金制度での年金番号に相当する。社会保障制度自体は，現在の就労者が納める社会保障税によって，現在の退職者，身体障害者その他に対する社会保障を賄い，現在の就労者が退職した後には，その時点での就労者からの社会保障税収入によって，それまでに納めた社会保障税の多寡等に応じた支給を受けるという制度である。したがって，初めてアメリカ国内で収入を得る機会ができた時点，あるいはそれ以前にSSNを申請・取得した後は，転職・転居如何に関わらず，以後納めている社会保障税の額が当該番号で記録・管理されることとなる。

このようにSSNは，一人につき一生涯に1回しか発行されない番号なので[22]，戸籍制度や住民登録制度がなく，州を越えると行政組織も異なってしまうアメリカでは，最も確実な個人の識別手段ともいえる。SSNがスタートした当初は，SSNを身分証明に使うことは禁止されていたが，1980年代ころから，税務処理[23]，その他の福祉的支給の申請，パスポートの取得，各州における運転免許証の発行など，社会保障関係以外の行政的分野でも，SSNが個人の特定に用いられるようになった[24]。

私的領域においても，SSNの個人識別機能の利便性から，銀行，証券会社，保険会社など，様々な場面で契約開始時にSSNを要求される[25]。さらに財産的な口座関係だけではなく，学生番号，社員番号，

---

20 平成18年1月17日インタビュー

21 前掲注16, pp. 50-51.

22 SSNは，3桁のエリア番号，2桁のグループ番号，4桁の通し番号の合計9桁の番号から構成されている。ただし，9桁全てがランダムな組み合わせなのではなく，ある程度の規則性を有している。エリア番号は，当該個人がSSNを申請した地区を表している。これは，郵便番号（zip code）を基にしており，公表もされている。Social Security Administration, "Employer Reporting Instructions & Information: Social Security Number Allocations," 平成18年3月31日確認（http://www.ssa.gov/employer/stateweb.htm）。グループ番号は，限られた組み合わせであるエリア番号をより細分化するために設けられている番号とされる。そして，このグループごとに，0001から9999までの通し番号がつけられている。

23 例えば，所得税還付申請書類上の扶養家族の存在を申請する上で，子供のSSNも必要とされるようになった。これにより，本来，当該個人としては就労するわけではないのでSSNをまだ必要としていない子供についても，生まれてすぐに親がSSNを代理申請して取得することが通常となった。また，連邦納税者番号（Federal Taxpayer Identification Number）も，SSNを用いるとされている（26 U.S.C. 6109(d)）。

24 プライバシー法（Privacy Act 1974, 5 U.S.C. 552a）に基づき，SSNを要求された者は，その根拠を行政庁等に確認することができる。

25 なお，SSNを取得するとカードが発行されるが，実際のカードは，名前とSSN，またアメリカ市民であれば，U.S. Citizenと記載されただけの簡単なものであるから，本来，そのカードを見せたからといって，提示者と真の名義人との同一性の証明にはならない。日常，SSNを求められる場面においても，実際にカードを確認するまでもなく，口頭で9桁の番号を唱え，あるいは書類上に記載すれば足りる。

銀行口座開設時など，経済活動の上でSSNを使用する場合，銀行側は，社会保障庁（Social Security Administration,

各種データベースのID番号あるいはパスワード番号などとして，あらゆる場面で用いられていた。

そして，逆にこのように様々な場所で露出しているSSNを知ることで，行為者[26]は，氏名，住所，電話番号などの，SSNに比べてもさらに社会生活の中で公表・露出度が高い情報と組み合わせ，銀行，クレジットカード，保険等，様々な場面で，容易に名義人に成り済ますことができる。このため，後述のクレジットカード契約締結の容易さも相俟って，他人名義の新規クレジットカードを取得し，限度額一杯を使った挙句，クレジットカード会社が立て替えた支払いをしない，という犯行が可能となる。

SSNの盗用であることが認められれば，この金銭的負担はクレジット会社の負担となるが，場合によっては，SSNの盗用だったことを認めさせるために名義人が法的手段を含めて係争しなければならない負担も発生する。さらに，真のSSN取得者には，直接の金銭的被害を受けなかったとしても，信用の低下という問題が生じる。信用情報管理会社（Credit Reporting AgenciesまたはCredit Bureaus。以下，「CRA」という。後述。）が管理している個人の信用評価も，SSNによって管理されているため，当該SSNに不払いクレジット記録が残っては，真の名義人の信用評価が低下し，住宅ローンを組む際などの不利益まで残る。そこでCRA 3社と交渉し，記録を削除してもらわなければいけない，また，その後の不正使用を防ぐため，そのSSNを使って勝手に預金口座を開設しようとする，あるいはローンを組もうとするなどの動きを連絡してもらうように手続きをする等という，事実上の負担が発生する。この事務手続きについての簡略化の方向については後述する。

なお，SSNの悪用に関しては，ID Theft法とは別に，詳細な刑事罰（42 U.S.C. 408, 1011, 1307(b), 1320(a)-7b(a), 1383a等）が設けられている。

イ　クレジットカード

クレジットカードによる代金決済は，クレジットカード会員（消費者）と加盟店との間での売買契約，加盟店とクレジットカード発行会社との間の加盟店契約，クレジットカード会員とクレジットカード発行会社との間の会員規約，という3面契約になっている[27]。日本では，会員規約に，さらに利用代金を銀行などの金融機関における預貯金口座から引落す契約が付随することが通常だが，アメリカでは，銀行発行のクレジットカードか，VISAなどの国際ブランドでない限り，必ずしも銀行口座との連携がない[28]。したがって，他人名義を冒用してクレジットカードを新規に入手しようとする際，銀行口座まで用意する必要がない。

さらに，ID Fraudとの関係では，pre-approved credit card（審査済みクレジットカード）の勧誘という商慣行が特徴的であろうと思われる。これは，クレジットカード発行会社がCRAにある情報等を見て，有望な顧客となりそうな者に，すでに信用審査は済んだものとしてクレジット入会申込用紙を送りつけるのである。もちろん，一方的に送られているだけなので，用紙を返送しなければクレジット契約

以下，「SSA」という。）に当該SSNと当該名義人との一致を確認するわけではなく，後述の信用情報管理会社に確認し，当該SSNの元に登録されている信用情報などを確認する。

26　ここでは，SSNを真に社会保障庁から割り当てられた人間を名義人，名義人に成り済まそうとする人間を行為者とする。

27　類似する機能のものとしてチャージカード（charge card）と呼ばれるシステムがある。基本的に，クレジットカードと同様の関係にあるが，利子を払うことを前提に，いわゆるリボルビング払いによる債務返済の先延ばしを可能とするクレジットカードと異なり，チャージカードの場合は，一月ごとの清算を要する。ただ，チャージカードも含めて，クレジットカードと通称されていることが多い。

28　なお，口座引き落としになっていないクレジットカードは，会員が，支払期日までに小切手や現金で支払う。この場合の貸し倒れのリスクは，限度額と利率に組み込まれている。

は成立しない[29]。しかし，逆を言えば，犯罪者が配達された郵便受けからこれを窃取する，あるいは受領者が不用意に捨てた申込書を用いて，書類上，カード名義人の住所を変更するなどしてから返送すると，他人名義のカードを入手することが可能となる[30]。

U.S. Postal Inspection Service（郵政監察）によると，1995年度から1997年度の3会計年度中，クレジットカードの不正申請の件数自体は横ばいないし微減状態に留まっているものの，他人の郵便物について，勝手に転送願いを出し，犯人の管理下の私書箱等へ転送させることによって郵便物を盗むという犯行による逮捕者は，1996年度の53件から，1998年度には最初の第一四半期中だけで既に54件，と大幅な増加傾向が認められた[31]。また，これら郵便窃盗及びクレジットカード詐欺事案については，郵便窃盗担当者と，続いて不正取得にかかるクレジットカード悪用者などの役割分担がなされた，組織的犯行の傾向が認められたという[32]。

さらに，米国ビザ(VISA U.S.A. Inc.)によると，1997年度中，同社が提携している銀行が，クレジットカードの不正取引によって受けた損失は，4億9千万ドルに及び，総取引高の0.097%を占める。また，この損失のうち，約5%が，虚偽のカード申し込みによるもので，約6%は，郵便窃盗などによって不正な住所変更を行って入手した既存のクレジットカードの不正使用であると疑われるとされる[33]。

ウ　信用情報管理会社（CRA）

CRAは，Credit Rating Agency，Credit Reporting Agencyまたは，Credit Bureauと呼ばれる営利目的の私企業である。法人の信用情報に関するCRAは，Moody'sやStandard & Poorsなど，いわゆる「格付け機関」として日本でも著名であるが，ここで問題とするのは，個人についての同種機関である。日本で類似する機関としては，全国銀行個人信用情報センター(KSC)，株式会社シー・アイ・シー(CIC)などがあげられるが，金融機関や与信業者間で，信用情報を共有し合う性格が強い。CRAは，SSNをインデックスとして用い，業種を越えて，債務や，その支払い状況などの情報を管理・提供しているところに違いがある。アメリカでの個人の信用情報に関する全米規模でのCRAは，Experian, Equifax, Trans Unionの3社である。

情報の使い道としては，例えば長距離電話サービス会社が，新たに契約を申し込んだ客の支払い能力を調査するのに用いたり，あるいは企業が，就職希望者の身元を調査するため，信用状況の一般的な審査方法として利用したりするなど，幅広い。また，行政機関も福祉的支給をする前の給付申請者の財産状況審査に用いるなど，その存在は公的性格を帯びている。

従来，CRAが有する信用情報の売買についての規制がなされておらず，CRA業界全体で年間数千万ドルもの収益につながっていたとの予測もあったが[34]，現在は，信用情報の開示条件，使用条件などについて，開示を承諾する名義人の文書での許可がない限り開示できない[35]などFair Credit Reporting Act

---

29　予備審査時点以後の信用事故を防ぐための第2次審査は行われている。

30　なお，SSN名義人は，各CRAに対し，pre-approvedカード勧誘目的での信用情報の閲覧をさせないよう，あらかじめ制限を加えることができるが，このようなpre-approved cardといった商慣習自体は，消費者，カード会社双方にメリットがあるとして，禁止される方向にはない。

31　ただし，逮捕件数の増加には，純粋な事件増加以外にも捜査側の体制の充実という要因も含まれる。また，このうち，審査済みカードに関する案件がどの程度含まれているのか定かではない。

32　以上，この段落について，前掲注16，pp. 32-35。

33　Ibid., pp. 42-43.

34　Ibid., p. 55

35　Pub. L. 105-347，§3による改正。

(15U.S.C. 1681 et. seq.)[36]の規制を受ける。

(3) 関連する犯罪

他人の個人情報を盗み，それらを用いて新規クレジットカードを入手し，新たな債務を負担させ又は既存の金融口座を乗っ取るなどの形態の犯行の正確な統計は存在しない。もともとアメリカ国内で詐欺犯に関する統計が取られていないことや，「○○○ fraud（詐欺）」と細分化された各種「詐欺」犯の概念の中には，欺罔のための手段を準備する行為についても含まれているため，これらの関連犯罪の発生件数中，ID Fraud と呼びうる件数のみを抽出して計上することが難しいからである。

例えば，「詐欺」の章立ての中に規定されているものを中心に関連犯罪をあげてみると；

① 身分証明文書[37]の偽造犯（18 U.S.C. 1028），

② 各種サービス等へのアクセス手段[38]に関連する詐欺等（18 U.S.C. 1029）[39]，

③ SSN または，社会保障カードの不正使用等（42 U.S.C. 408(7)[40]），

---

36 同法において，Consumer Reporting Agency との名称が用いられている。CRA は，営利目的，非営利目的を問わず，消費者信用情報その他の情報を，消費者報告（consumer report）として第三者へ提供する目的で，業務として収集し，当該報告を準備・作成するために，州際通商（interstate commerce，なお，ここでいう州際通商は，連邦法の適用が認められる根拠としての interstate commerce と同義である）の施設もしくは手段を用いている者をいう（15 U.S.C. 1681a(f)）と定義づけられている。したがって，consumer report の意義が問題となるが，これは，与信や保険，雇用（昇進などの雇用関係上の判断一般を含む）またはその他法令に規定される機会において，当該消費者の適格性を判断する目的で，消費者の（貸付に際しての）信用状況，与信格付，与信限度，人格，一般的評判，個人的特徴，生活形態などについて，CRA が提供する情報のことを意味する（15 U.S.C. 1681a(d)）。

37 身分証明文書とは，連邦政府，州政府及びその下部組織，外国政府及びその下部組織，国際機関または準国際機関発行に係る，ある人物についての情報を伴うことによって，当該人物を特定する目的で，かつ特定するものと一般に受け入れられている文書をいう（同 18 U.S.C. 1028(d)(1)）。例としては，出生証明書，運転免許証など（同脚注(A)(ii)）。

38 法文上のタイトルは Fraud and related activity in connection with access devices，と単に access devices と表現されている。定義規定（18 U.S.C. 1029(e)(1)）によれば，(A)カード，板，暗号，口座番号，ESN（携帯電話固有番号），MEID（携帯端末の製造番号），暗証番号，(B)その他の電子通信サービス，電子通信に必要な器具・設備，電子通信に用いられる機器を特定する番号等，(C)口座その他のアクセス手段，とされている。電子通信サービスそのもの，アクセスする先のサービスに限定がないため，「各種サービス等へのアクセス手段」とした。(A)の例としては，クレジットカード，銀行預金口座カード，それぞれのカード使用時に必要になってくる暗証番号等が含まれる。また，それらとは別に，(B)において，「電子通信サービス」，すなわち，かつての電話交換手的な人的設備やコンピュータ設備など，電子通信サービスを提供するに際して必要なあらゆる過程が定義されており，access devices は非常に広い概念である。

39 構成要件としても，多岐にわたる。

- 上記各種アクセス手段の偽造に用いる目的での機具等の所持・移転（18 U.S.C. 1029(a)(4)），偽造された，または，無権限なアクセス手段（正当なアクセス権者が無くした，盗まれた，期限が失効したなどの状態のアクセス手段。同(e)(3)）を15以上所持していること（同(a)(3)），アクセス手段の偽造・使用（同(a)(1)）；
- 他人のアクセス手段の無権限行使によって１年以内に1,000ドル相当以上の金品を取得（同(a)(2)，同(a)(5)）；
- アクセス手段，またはアクセス手段を入手するために必要な情報を提供するように他人を唆すこと（同(a)(6)）；
- 詐欺目的の不正アクセスを可能とする電気通信機器を製造，使用，管理，または所持すること（同(a)(7)）；
- スキマーの製造，使用，所持等（同(a)(8)）；
- 電気通信サービスへの不正アクセスを得るため，同サービスへのアクセスに用いられる機器に埋め込むなどの目的で，ハードウェアまたはソフトウェアを作成・製造，使用，管理，所持していること（同(a)(9)）；
- クレジットカードシステムの加盟者（金融機関など）に支払いをさせるために，上記アクセス手段を用いて作出した取引の証拠を，第三者が加盟者に提示するよう，仕向けるなどすること（同(a)(10)）。

なお，以上の犯罪の全てについて，未遂犯の処罰（同(b)(1)）及び共謀罪の処罰規定（同(b)(1)）がある。

40 連邦政府からの財政的支援を受けている各種支給プログラムに対し，虚偽情報を元に発行された SSN 又は SSN と思わせるような数字を用いること及び社会保障カードの偽造，変造及び売買，またはこれらの行為を目的とする所持

④ 連邦政府関係に対する不正・虚偽請求（18 U.S.C. 287），
⑤ 詐欺（18 U.S.C. 1341）[41]，
⑥ 虚偽名・虚偽住所の使用（18 U.S.C. 1342），
⑦ 電信電話，ラジオ，テレビを用いた詐欺（18 U.S.C. 1343）[42]，
⑧ 金融機関を対象とする詐欺（18 U.S.C. 1344）

などがある。このように，詐取の目的となっている利益や欺罔手段によって細分化されている。そして例えば，①の偽造犯については，法文上のタイトルは，Fraud and related activity in connection with identification documents（身分証明文書に関連する詐欺及び関連行為）とあるが，構成要件の内容としては，次のとおり，いわゆる詐欺部分自体は含まれず，いわばその準備行為である。

・18 U.S.C. 1028(a)(1) 身分証明文書の偽造；
・同(2) 偽造証明文書又は盗まれた身分証明書（以下，本罪の説明について「偽造身分証明書」という。）を，偽造文書あるいは盗品であると知りながら移転すること；
・同(3) 5つ以上の偽造身分証明書を所持・移転すること；
・同(4) 偽造身分証明書（1つでよい）を，連邦政府を騙す目的で所持・移転すること；
・同(5) 偽造身分証明書を偽造する道具であることを知りながら，当該道具を製造，移転，所持すること；
・同(6) 連邦政府による身分証明書の盗品又はかかる身分証明書の外観を有する偽造文書であることを知りながら当該文書を所持すること。

(4) ID Theft 罪の構成要件

ア 立法状況

1998年の ID Theft 法は，前述の18 U.S.C. 1028に，(a)(7)として，「州ないし地方自治体の法により重罪を構成する不法行為または連邦法違反を構成する不法行為を犯す目的で，またはかかる行為を幇助・教唆するため，故意に，権限なく，他人の身分証明の手段を移転または使用すること[43]」を犯罪として挿入し，これに連動するその他の修正[44]を加えたものである。

その後2005年には，Identity Theft Penalty Enhancement Act[45]（以下，「加重 ID Theft 法」という。）の立法により，上述の Section 1028(a)(7)の ID Theft 罪に，「移転，使用」に加えて「所持」も実行行為に加えられている。これは，情報の取得行為や，移転行為など，情報が動いている時点での認知は事実

---

41 タイトルは，単に Fraud and Swindlers（いずれも，詐欺，という意味）であるが，欺罔行為に用いるための偽の通貨，証券などを，郵便や州を跨る運送業者に渡し，宛先へ届くようにすることを内容とする。罰金または20年未満の拘禁刑に処せられうる（併科可）。金融機関に影響を与える場合は，100万ドル未満の罰金または30年未満の拘禁刑に処せられうる（併科可）。通称，mail fraud（郵便詐欺）と呼ばれる。

42 同罪は，詐欺を目的として通信設備（有線，ラジオ，テレビなど）を用いて欺罔すること自体が犯罪なので，欺罔行為として必要な著述，サイン，信号，映像や音などを発信する，または発信されるよう用意すること（transmits or causes to be transmitted）で犯罪が成立する。20年以下の禁錮による処罰が可能であり，罰金も選択または併科することができる。金融機関に影響を与える場合は，100万ドル以下の罰金と30年以下の禁錮との選択または併科することができる。

43 "Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitute a violation of Federal law, or that constitutes a felony under any applicable state or local law"

44 他人の身分証明の手段を移転・使用することの未遂（attempt）及び共謀（conspiracy）も処罰対象となった（同法第3条(e)）。

45 P.L. 108-275, sec. 2 (a), 118 Stat. 831

上困難であるから，経緯はともあれ，移動前後において，権限無く他人の情報を所持していること自体を検挙・訴追できるようにするためである。

なお，改正を経ても，個人情報の不正取得については，州法の管轄として，連邦法上のID Theftの概念には入っていない。つまり，州を跨る信用秩序への危険性が及ぶなど，連邦として取り締まる必要が出てくるのは所持以降との価値判断である。ただし，後述のとおり，個人情報の不正取得に向けた行為は，所持の未遂として評価されることもある。

イ　所持と，その他の実行行為の未遂との関係

アメリカ法における未遂行為は多義的であるが，ID Theft法との関係では，Substantial step（実質的な一歩）が基準として用いられている。すなわち，ある犯罪行為にむけられた実質的な行為があったときは，当該犯罪完成には至らなかった場合でも，当該犯罪の「未遂」が成立するとされる。例えば，クレジットカード情報を入力させるつもりでフィッシングサイトを立ち上げたものの，実際に誰かの情報を入手する前に，警察に捕まった場合などは，クレジットカード情報の所持の未遂として評価され得る。

他方，前述の通り，もともと所持罪は，移転や使用というように，個人情報が移動する前後の状態を処罰する目的で犯罪化されている。そこで，所持罪と，移転未遂罪，使用未遂罪との違いを検討するに，所持罪は，目的の如何を問わず，権限なく他人の個人情報を所持している場合に成立する。その意味で，所持自体は，移転や使用における「実質的な一歩」ではない。移転未遂などと評価できる行為とは，さらに，実際に所持していた情報を，移転させようと，電子メールや封書などで送ろうとしたが，実際に届く前に検挙されてしまったような場合など，所持を越えた「実質的な一歩」を要する。

ウ　使用とその他の詐欺行為などとの関係

「使用」という行為は，何らかの犯罪行為に向けられての使用であれば該当する。そこで，例えば，前述の各種詐欺罪における偽造行為などもID Theft罪でいう「使用」行為といえる。

例えば，犯行者Aにおいて銀行のコンピュータをハッキングし，顧客のクレジットカード番号と有効期限を盗み，これらの情報をインターネットのチャットルームを通じて，犯行者Bに売ったとする。そして，Bが，インターネット上で当該クレジットカード情報を用いて商品を購入した場合，A，Bともに，ID Theft罪の共謀罪（後述），ID Theft本体である移転罪（A）または使用罪（B），アクセス手段詐欺（18 U.S.C. 1029(a)(2)）としての移転罪（A），無権限使用罪（B）を適用しうる。

このように複数の罰条に該当するとしても，アメリカでは，日本のような観点的競合の概念がなく，法条間の択一関係を定める法律上・司法判断上の制限もない。そこで，このような場合には，担当検察官が，立証の難易に照らして最も適切と思われる罪名を選択することができる。

エ　共謀罪

共謀罪の成立要件は，①2人以上の者の間で，犯罪行為（ID Theft）を行うことを共謀し，②そのうちの誰かが，犯行に向けての何らかの行為（overt act）を行うこと，である。②の何らかの行為とは，日本で観念されるところの「実行行為」である必要はなく，例えば，他人のクレジットカード情報で不正に買い物をする，という共謀をして，盗まれたクレジットカード情報はないか，と盗品ブローカーなどに問い合わせる電子メールを送る，などでも該当する。しかし，overt act自体がID Theft行為だった場合，この場合共謀とその後のID　Theft行為とが事実関係として同一ではないため，共謀罪とID Theft罪が成立し，両罪とも訴追することができる。

ID Theftに加えて共謀罪の起訴をするメリットは，共謀のみにかかる関与者を処罰することができるほか，共謀の部分までの立証をすることにより，全体像の解明が出来る点にある。

オ 「他人の身分証明の手段」の意味

上述のとおり，ID Theft 罪の構成要件の中心的概念は「他人の身分証明の手段」であるが，この概念については，「他人の」及び「身分証明の手段」の意味が問題となる。

(ア) 「他人の」

「他人の身分証明の手段」でいうところの「他人」とは，自然人を前提としている。前述のとおり，ID Theft 罪は，個人情報自体を財産的に位置づけて保護しようとするものではない。当該情報を用いての経済犯罪の前提犯罪としての位置づけで立法されていることから，消費者保護的な視点から保護を要する範囲を把握しているからである。したがって，法人[46]や架空人の情報は含まれず，逆に，実在している限り，生存・死亡を問わない。

(イ) 「身分証明の手段」

「身分証明の手段」とは，それ単体でも，あるいは他の情報と一体に用いられることによってでも，特定の個人を識別しうる情報を全て含み，例えば，氏名，生年月日，SSN，前述の18 U.S.C. 1029と同趣旨の「アクセス手段（クレジットカード番号などを含む）」，指紋等の生体認証情報等を意味する[47]。

(5) 加重 ID 罪

2005年に成立した加重 ID Theft 法は，ID Theft 罪に所持罪を追加するほか，Section 1028A として，加重 ID Theft 罪を新設している。

① 一定の重罪（1028A(c)に列挙[48]）を犯すに際し，またはこれに関連して（during and in relation to）ID Theft を敢行した場合に，その重罪の量刑に，2年の拘禁刑を加重すること，

② テロ行為（18 U.S.C. 2332b(g)(5)(B)に列挙[49]）に関連して ID Theft を敢行した場合に，5年の拘禁刑を加重すること，

③ 刑の執行方法として；

1．保護観察に付さないこと（実刑とすること）

2．原則として，刑の同時執行[50]を認めないこと

3．当該 ID Theft が関連するとして有罪認定される重罪の量刑を減らさないこと[51]

---

46 1998年の立法当時は，フィッシングなどの情報取得手段は発生していなかったが，今後，架空フィッシングサイトを作られた法人の被害に鑑み，法人を加える余地はある。しかし現段階で具体的に改正議論がなされているわけではない。

47 Section 1028(d)(7)

48 ① Section 641（公金，公用財産などに関する罪），Section 656（銀行員による横領など），Section 664（企業内年金の横領など），② Section 911（アメリカ市民権があるもののように装うこと），③ Section 922(a)(6)（銃器購買時に人定等を偽ること），④ Chapter 47（ID Theft 罪を除く第47章，詐欺罪等に規定される犯罪），⑤ Chapter 63（郵便または有線通信を用いた詐欺），⑥ Chapter 69（国籍及び市民権に関する罪），⑦ Chapter 75（パスポートや査証に関する罪），⑧15 U.S.C. 6823, the Gramm-Leach-Biliey Act（虚偽の情報に基づいて顧客情報を得る罪），⑨8 U.S.C. 1253, 1306（追放処分に反してアメリカ国内で虚偽の身分証明書を作成して住み続ける罪），⑩8 U.S.C. 1321 et. seq.（移民法にかかる罪），⑪42 U.S.C. 408, 1011, 1307(b), 1320(a)-7b(a), 1383a（SSN に関連する虚偽文書作成等の罪），における重罪

49 罪名の記載は省略する。

50 アメリカでは，併合罪関係の処断刑は，各罪について判断された量刑を合算する。したがって，現実的には執行し得ない，数百年の拘禁刑ということもありうる。そこで，実際には，複数の刑を同時に（concurrently）執行する。加重 ID Theft 罪で同時執行を認めないという趣旨も，ID Theft 単体として，確実に2年ないし5年は刑に服させるという目的である。

51 これは，裁判官が，上記各規定（特に①，②及び③2）の趣旨を回避するために ID Theft 以外の罪について通常よりも軽く処断することを認めないために定められた規定である。

が，法文の概略である。

加重 ID Theft 罪の主眼は，一定の ID Theft 行為について，確実に 2 年は服役させるところにある。これは，裁判所が，ID Theft を経済犯罪の前提行為に過ぎないとして，ID Theft 単体を見た場合の量刑を，本体とみられる詐欺などの経済犯罪の量刑に吸収させる傾向が従来よく見られたことから，裁判所に ID Theft 罪が重大犯罪であるとの認識を植え付け，これを量刑にも反映させる目的で，詳細な刑の執行方法も含める立法がなされたのである[52]。

3　通報・捜査態勢

(1)　被害情報のデータベース化

ア　データベースの役割，性質

実際の ID Theft は，個人情報がなんらかの形で犯罪者の手に渡った瞬間に発覚するわけではなく，その情報が悪用されて，当該個人情報の本人に財産的被害が発生するなどし，本人から自らの人定事項が不法に他人に渡ったのではないかと通報があるなどして初めて発覚する。また，組織的な犯行の場合，一つ一つの被害は小さいことも多く，通報を受けた側の捜査機関からすれば，単発の犯罪として処理をするだけでは費用対効果が得られないことや，州を越えると管轄の問題も生じる。さらに，多数にわたる被害者の分布や被害状況を精査することで，被疑者の特定に至る場合もありうる。このような状況に対処するため，ID Theft 法では，連邦商取引委員会（Federal Trade Commission，以下，「FTC」という[53]。）によって，被害受付窓口が設置・管理されることが義務付けられた（同法 5 条）。

もともと，FTC は，他機関と共同で，消費者からの取引上の苦情を受け付けるデータベース（Consumer Sentinel[54]）を1997年から運営していた。この中に，消費者詐欺（Consumer Fraud）に関する被害申告をまとめるデータベースがあったが，FTC 自体は，個々の申告された情報に基づいての捜査を開始するわけではなく，あくまでも被害状況の集積や，そのデータ分析を通じて，捜査機関への有益な情報提供を行うためのデータベースを管理しているに過ぎない。これに加えて，ID Theft 法の要請により，FTC は ID Theft について全米中の通報を一括受付し，捜査機関への情報提供をすることとなったため，1999年11月から，ID Theft Clearinghouse（ID Theft 情報センター）として，同様のデータベースを管理することとなった。ID Theft に関するデータベースは，データ解析や提供段階では，Consumer Sentinel と一体化して扱われており，この二つのデータベースを合わせて Consumer Sentinel System と呼ば

52　一般に，司法取引の影響で，アメリカの量刑は相場としての目安が立てづらい。一例として，2003年11月に，2 件の ID theft 罪（重罪）及び不法な個人情報保持の事実で有罪判決（5 年の保護観察，350時間のコミュニティサービス，5,000ドルの賠償命令）を受けたニューヨーク州在住の20歳のフィッシング犯が，翌2004年 1 月から逮捕されるまでの10月までの間に，再度フィッシングを行っていたことで（具体的な罪名不明）受けた判決は，2 年から 4 年までの拘禁刑である。犯行で得た金額は，犯行者本人も途中で把握できなくなったとするが，フィッシングで得た他人のクレジットカード情報を使い，当該クレジット口座から犯行者管理下の口座まで電子送金する手法で，20歳までに15万ドル以上，3 時間で 2 万ドルほどの割合での利益があったとする。Tom Zeller Jr., "Stolen Lives : Identity Thief Finds Easy Money Hard to Resist," The New York Times, July 4, 2006

53　なお，FTC は，日本でいうところの独占禁止法関係に相当する不正競争防止の政策決定及び法執行以外にも，商取引全般に亘っての消費者保護，立法やその他の政策の経済波及効果の測定などを所管している。消費者保護の中では，虚偽・誇大広告の排除，消費者教育のほか，迷惑メール，本文で詳述している消費者詐欺などの被害申告受付，その解析などに従事している。また，銀行以外の与信業務への監督と，消費者情報の管理の適正化も所管している（前記 CRA の主務官庁でもある）。http://www.ftc.gov/参照。

54　http://www.consumer.gov/sentinel/

れている。

なお，FTCでのID Theftの定義とは，何者かが，個人情報を，詐欺や窃盗などを犯すに際し，盗用すること，とされている[55]。すなわち，実害を発生させている行為がどのような態様の「詐欺」であっても，その詐欺行為に用いられた名義人が，自己の個人情報が悪用されるに至った状況の認識があれば，ID Theftとして分類される。例えば「名義人」の銀行口座から犯行者口座へ金が移されるという財産的な「被害」が，日本でいうところの「詐欺行為」によって発生しているとしても，ID Theft被害者が，いつ，どのように口座決済に必要な個人情報が加害者に漏れたのか分からない，という場合はID Theftとして分類される。しかし，同じような口座間の金銭移動が，消費者詐欺，例えば通販で申し込んだ商品が届かない，といった事由に基づくのであれば，詐欺被害者から犯行者へ，口座決済に必要な情報提供がなされているので，被害者も，いつ，どのように自分の個人情報が漏れたのか，把握しているといえる。そこで後者のケースであれば，「消費者詐欺」として分類される。

イ　被害申告の受付

FTCでは，英語とスペイン語での電話受付もしており，100人弱のオペレーターによって，1週間に2万件を受け付けている。また，オンラインでの受付も，英語とスペイン語双方で行っている。

オンライン受付で入力する情報を元に，FTCで集積するデータの性質を紹介すると（**巻末資料1**参照），最初に，申告者の人定事項を入力する。これは，もし捜査が進展し，実際に訴追するなど，被害者からのより詳細な供述等が必要となった場合の連絡先を確保するためである。

次に，どのようなID Theftが問題となっているかという問いの中では，クレジットカード，銀行預金（当座・普通），融資，電話その他公共サービス（電気・ガス・水道など），証券その他の投資商品，インターネット又は電子メール，政府関係文書または福祉的支給，その他，と細目に分かれている。これは，これらのいずれのサービスまたは商品提供サービスに関して，自分の名前で(あるいは自分のSSNその他識別情報で）契約がなされたのか，ということを分類するものである。また，これらの契約を，犯行者がインターネットで締結したのか否かについて，被害者の認識の有無を確認している。

被害申告の項目の中では，被害の詳細として，被害を受けた時期及び当該問題となっている口座等が開設された時期などについて申告する。通常，実害を受けている被害者であれば，最初に地元の警察などに被害申告し，あるいは，CRAのいずれかから自分の信用状況についてのレポートを取り寄せるなどして，被害回復に努める。そうして，そういった手続きの中でFTCに被害申告窓口があるということを聞き及び，登録に至る。したがって，ここでの問は，これらの手続中に，FTCに提供できるだけの情報を申告者が入手しているということを前提にしたものである。同様に，考えられる被疑者の人定事項について答えさせる項目も，被害者が事後的に検討して，被疑者であろうと特定できる場合があることを想定しての入力項目である。

また，被害の詳細を申告する項目には，被害形態の選択肢が示されており，金銭的被害以外の選択肢としては，「なにも他には被害がない」，「民事訴訟の被告となった」，「刑事的捜査の対象となった[56]」，「逮捕された，または有罪となった」，「新たなクレジットや金融サービスを受けられなかった」，「就職口を

---

55 "Consumer Fraud and Identity Theft Complaint Data January - December 2005, Appendix B1," Federal Trade Commission, January 2006, 平成18年5月18日確認（http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf)。

56 例えば，犯人が，他人の名前で，詐欺を重ね，州を越えて逃げている，というような事案である。名前を騙られた者は，知らない間に自分に対して逮捕状が発布されている州に足を踏み入れた時に，急に逮捕される，などの被害に遭うことを指す。

得られなかった，または仕事を失った」，「厳しい債務取立てにあった」，「その他」，「時間が無駄になった」などがあげられている。

その他の申告項目に関しては，FTCの商業社会における規制機能に関する事項に関連することから，後述する。

ウ　データベースの相互補完

商業詐欺や，ID Theftについては，多様な手口が見られ，規模の大小についてもさまざまであり，影響を受ける関係機関も多いことから，民間団体も含めて，多くの団体が消費者からの苦情を受け付けている。前述のような，被害の実態を把握するという機能を高める上では，より多くの被害を確認できることが効果的であることから，FTCのデータベースとの間の情報提供関係を樹立する機関が多い。

そのうちの一つが，インターネット犯罪苦情センター[57]（the Internet Crime Complaint Center，以下，「IC3」という。）である。IC3は，2000年5月に発足したインターネット詐欺苦情センター（the Internet Fraud Complaint Center, IFCC）の名称を2003年12月に変更したものである。同センターは，FBIと，全米ホワイトカラー犯罪センター[58]（the National White Collar Crime Center）により共同運営され，実際に，勤務しているのは，FBIなどの法執行機関からの出向者のほか，産業界からの派遣や学者もおり，拡大するサイバー犯罪被害の実態を把握し，法執行機関，一般消費者及び産業界（等）に，適切な情報を提供することを目的としている。所在地は，ペンシルバニア州ピッツバーグだが，苦情相談はオンラインのみにより受け付けている。ただし，FTCが，全国のID Theft情報を集約することを義務づけられていることや，両者が収集を目的とする情報がほぼ重なる関係上，IC3とFTCの上記Consumer Sentinelのデータは，共通化されており，被害者が一方に通報すれば，両方のデータベース上に情報が登載されるようになっている。

Consumer Sentinelには，IC3のほかにも，郵政監察（U.S. Postal Inspection Service），Better Business Bureau[59]などの関連機関・団体と，カナダのフォンバスターズ（Phone Busters。後述）が情報提供している。Consumer Sentinel中のデータにおける消費者詐欺とID Theftに関する情報の2005年における提出源としては，FTCへの電話ないしインターネットによる通報が55%，IC3が28%，郵政監察が5%，Phone Bustersが5%，Better Business Bureausが4%，その他が3%となっている[60]。

エ　データベースの活用

FTCのデータベース情報を利用したい機関は，事前に，FTCとの間で秘密保持の契約を結ばなければいけない。現時点では，アメリカ国内（連邦，州，地方自治体レベル），カナダ，オーストラリアの1,000を超える法執行機関がこのデータベースを利用している[61]。

前述のように，アメリカ国内の法執行機関は，様々な行政レベルで個別に存在していることから，各執行機関側では，まず，FTCとの間で，秘密保持等に関する契約を結ばなければならない（**巻末資料2**参照）。その上で，インターネット上の検索ページへのアクセス権を得る。

法執行機関にとって，このデータベースへのアクセス権を得ることの有用性は主として3つの機能に

57　http://www.ic3.gov/

58　http://www.iir.com/nwccc.htm

59　Better Business Bureauとは，産業経済界から30万社ほどが参加している非営利目的の自主規制団体で，1912年に設立されている。ID Theft以外にも，消費者問題一般の苦情を受け付けて仲裁機能を果たすほか，企業や各種募金への投資・寄付の適格性について，問い合わせに応じるなどしている。http://www.bbb.org/参照

60　前掲注55，Appendix A2

61　参加機関についてのリストは，http://www.consumer.gov/sentinel/members.htm参照。

分けられる。

まずは，検索機能である。検索ウェブページ（**巻末資料3**参照）では，例えば，ある特定の名前の犯人，一定の住所や電話番号を連絡先とされた被害者がほかにも通報していないか，特定のSSNやクレジットカードが悪用されている事件がほかにも無いか，などと様々な条件を設定することで検索し，関連事件の調査を行うことができる。

次に，現に関連事件を捜査している法執行機関自体を特定するために，被害者が通報したであろう法執行機関名や，事件番号での検索も可能である。逆に，機関Aが検索後，他の機関が検索した際，情報共有ができるよう，未登録情報を登録して，データベースをさらに充実させることや，当該情報でAが検索をかけた，ということが分かるよう掲示しておくこともできる。（アラート機能）。

さらに，設定した検索条件に該当する情報が，後に登録された場合，自動的にeメールで連絡がくる機能もある（自動検索機能）。

オ　データの統計状況

2005年1月から12月までの1年間で，FTCのデータベースに寄せられた消費者詐欺及びID Theftの被害相談件数は，686,683件である。これを相談内容の種類別に見ると，**図1**のようになる。

相談件数のうち，約37%が，ID Theftである(255,565件)。2003年から比較すると，消費者詐欺とID Theftの割合は，6対4とほぼ安定しているが，実数としては，2003年の542,656件(このうち，ID Theftは，215,177件)，2004年の653,040件（このうち，ID Theftは246,847件），と年々伸びている。もちろん，FTCのデータベースの周知度が高まったことや，協力する関連機関の増加も影響していると思われるので，被害発生数自体が増えているとは限らない。ただし，後述するように，暗数は膨大と思われる。

次に，ID Theft中，勝手に用いられた個人情報の種別を見ると，**表2**のとおりである。

2005年は，クレジットカード関係が最も多く，約26%を占める。新規のクレジットカード口座を作成された被害が約15.6%であり，既存のクレジットカード口座を悪用された被害が約11.3%，残りがどちらか不明であった。次いで，電話や公共サービス関係の受益に関する被害が多いが(約18%)，そのうち約半数が携帯電話サービスの受益（被害者の名義で携帯電話サービスを勝手に契約する）被害であることが注目される。さらに銀行口座関係(新規口座開設，電子送金等)（約17%），他人名での就職(12%)，他人名の公的書類（運転免許証等）の交付・他人の公的利益（還付税等）の受給（9%），ローン・融資関係（約5%）と続く。

傾向としては，クレジットカード情報の盗用割合が減少している（2003年は，全体の約32%)。特に，新規クレジットカード口座の開設が減少しているが(約19.3%から約15.6%)，前述のとおり，ID Theft件数に関する通報の実数が増加していることから，通報件数実数としての大幅減少ではない。他方，そのほかの盗用態様としては，割合に大きな変化がない。しかも，255,565件の通報のうち，約20%では，一つの通報で，いくつかの盗用態様を通報しているため，実際の盗用件数は，通報数を前提とするよりもさらに増えていると言える。また，クレジットカード情報の代わりに割合で増えているのは，前述した個別態様に当てはまらない「その他」の項目のうち，刑事責任の追及(2003年約2.1%／2005年約2.2%。以下同じ。)，インターネットやEメール名義の盗用（約1.6%／約1.9%）及びさらに細分化されてもまだ「その他」と分類される項目などであり（約11.6%／約17.6%)，通報される盗用態様が，雑多になってきたことがうかがわれる[62]。

ただ，これは，前述のとおり，いずれも，何らかの形で表面化した被害内容による分類に過ぎない。

62　前掲注55，p. 13

総数　68万6，683件　　(2005年)

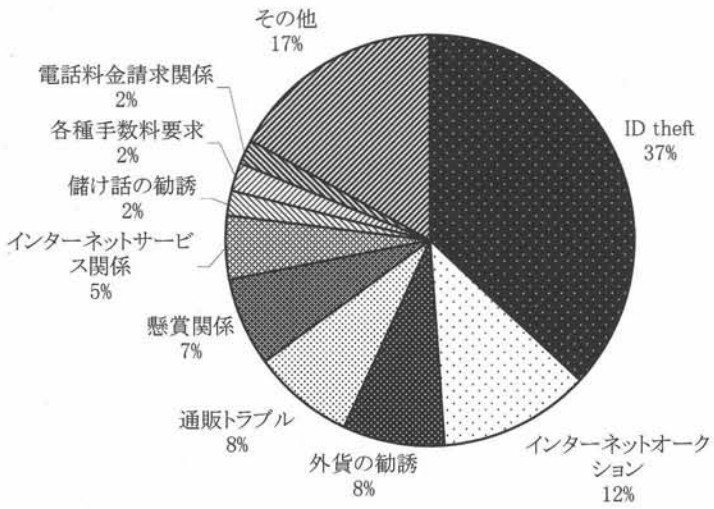


図1　苦情相談の内訳

注　1　各分類の内容は，以下のとおりである。
- ID theft；社会保障番号やクレジットカードの悪用等
- インターネットオークション：支払いをしたのに商品が届かない，注文と違う商品が届いた等
- 外貨の勧誘：外国公務員が巨額の資金を送金する分け前をもらえるので口座等を教えてほしいという勧誘
- 通販トラブル：過大な料金請求，商品が届かない，保証がない等
- 懸賞関係：当選した懸賞等の受け取りのために手数料を払って欲しい等
- インターネットサービス関係：インターネットサービスプロバイダーの試用後，解約できない，スパイウェア等
- 儲け話の勧誘：儲かる仕事があるとの勧誘，誤解を招くような仕事の勧誘等
- 各種手数料要求：融資，悪い信用情報の削除等の約束下での手数料請求
- 電話料金請求関係：架空の電話サービス料金の請求等

2　Consumer Fraud and Identity Theft Complaint Data, Federal Trade Commision, January 2006 からの抜粋による。

そもそも，被害者自身から積極的に被害を感知し，通報してきたケースだけではなく，社会保障庁や，金融機関，捜査機関などから，被害者に被害確認をすることで発覚し，FTC のデータに加算されるにいたる場合も多い[63]。しかも，結果的に，知らないうちにクレジットカードが自己名義で発行されているといっても，実際に流出していた情報は SSN だったか，被害者のパソコンから流出したものか又は被害者の SSN を保管しているその他の団体から個人情報が漏洩したものか，被害者自身には分からない。結

63　これは筆者（池田）の個人的経験であるが，アメリカで SSN を取得した後，1989年に帰国し，同年以後2001年まで日本にいてアメリカ国内での経済活動歴がないにも関わらず，2001年に再渡米し，長距離電話契約を結ぶに際して SSN を告げたところ，その SSN には債務不履行歴があると言われて契約ができなかった。そこで，SSN の不正使用が疑われるとして，社会保障庁（SSA）に相談し，さらに CRA 3社に通報した。アメリカ国内での居住者ではないことは明らかであったことから比較的単純に解決し，SSA では，おそらく，筆者の SSN と1桁違いの者が，間違えて使ったに過ぎないであろうから，今後これ以上の被害が出なければ，警察への通報も不要であると言われた。また CRA 各社とも，その債務不履行歴を削除してくれること，また，その後2年間は，筆者の SSN で新たなローンを組んだり，クレジット口座を開こうとしたりする者がいれば，CRA の方から筆者のほうへ問い合わせをするように記録を残すことを伝えられた。しかし，何度文書で問い合わせても，結局いつ，誰がどのような債務不履行歴を残していたのか，情報を得ることができなかった。また，ちなみに，約1年後，自分で，銀行口座を必要としないクレジットカード（デパート系）を申込み，これを取得して，使用もしてみたのだが，いずれの CRA からも問い合わせが来なかった。また，当時，FTC のデータベースの存在は全く知らなかった。

表２　被害者の個人情報の悪用種類別構成比

区　分	2003年	2004年	2005年
総数	215,177	246,847	255,565
クレジットカード関係	32%	28%	26%
新規カード口座作成	19.3	16.5	15.6
既存カード口座の悪用	12.0	11.9	11.3
不明	1.4	0.1	0.2
電話・公共サービス関係	20%	19%	18%
新規の携帯電話	10.5	10.0	9.0
新規の電話	5.7	6.0	5.5
新規の公共サービス	3.9	4.3	5.2
既存口座への料金転嫁	0.6	0.7	0.7
不明	0.8	0.3	0.4
銀行口座関係（電子送金，口座開設等）	17%	18%	17%
雇用関係	11%	13%	12%
ローン・融資関係	5%	5%	5%
公的書類･利益（税金還付，運転免許，社会保障カード等）	8%	8%	9%
ID THEFT の未遂	8%	6%	6%
その他	19%	22%	25%
刑事責任	2.1	2.4	2.2
インターネット，Ｅメールの名義	1.6	1.8	1.9
医療	1.8	1.8	1.8
家屋借入	0.9	0.9	0.9
保険	0.3	0.4	0.4
物の借入れ（レンタル）	0.2	0.3	0.3
破産	0.3	0.3	0.3
児童手当	0.2	0.3	0.2
雑誌購入	0.1	0.2	0.2
投資等	0.2	0.1	0.2
その他	11.6	14.4	17.6

注　1　各年の苦情総数に対する割合（%）である。ただし，2005年及び2004年は20%，2003年は19%が複数項目に該当した。

2　Consumer Fraud and Identity Theft Complaint Data, Federal Trade Commision, January 2006 からの抜粋による。

果，FTC あるいはその他の機関でも，どのような情報が，いつ，どのように流出したのか，という点についての統計をとりようがない。今後，どのような情報がどのような手法で流出・流通しているのか，個人情報自体の被害状況の実態が解明されると，予防手段を講ずる上でも，有益と思われる。

(2)　起訴における事実の選別

前述したように，アメリカでの刑事実体法の規定の仕方が，その行為態様や保護法益によって細分化されていることから，その適用関係も複雑となる。例えば，フィッシングによる詐欺目的で，他人のクレジットカード情報を入力させるためのスパムメールを発信すると，18 U.S.C. 1343（通称，wire fraud）に該当する。また，これによって入手したカード情報等を使って，無権限での買い物に及べば，アクセス手段の悪用として，18 U.S.C. 1029(a)(2)，(a)(3)または(a)(5)などの適用が考えられる。

ID Theft としての「使用」罪と，当該個人情報の名義人に成り代わっての各種詐欺犯など，複数の犯罪に該当しうる場合，いずれの犯罪によって起訴するかは，証拠の有無内容，自白の有無，司法取引の成否，刑罰の重さなどを総合考慮して検察官が選択する。また，個人情報の使用行為は，文書偽造，詐欺など他の犯罪を構成することがあるが，二重処罰を回避するため，同じ公訴事実を二つの罪名で起訴しないように事実構成を調整する。

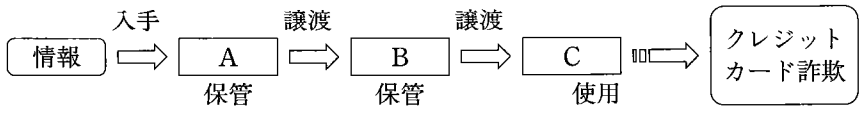
以上は，連邦での捜査・訴追判断であるが，ID Theft 罪は，州法上も48州で犯罪化されており，連邦法の適用のない多くのケースでも，州法での処罰がなされている。ただし，州法での構成要件は，連邦法と異なる場合や，重罪（felony）ではなく，軽罪（misdemeanor）に規定する場合もあり，一律化されていない。

(3) 犯罪目的の立証

ID Theft 行為は，犯罪目的で行われることを要し，その立証も必要である。

前述のとおり，個人情報を使用した場合は，同時に他の犯罪（詐欺等）を構成することが多いので，犯罪目的の立証は容易である。

個人情報の移転又は所持の場合，犯罪目的の立証は，被疑者が自白するか，あるいは，結果として個人情報が使用されたことの立証によらなければならないことが多い。例えば，被疑者 A が他人のクレジットカード情報を入手し，被疑者 B に譲渡し，B が被疑者 C にその情報を譲渡し，C がクレジットカード詐欺行為に及んだ場合，通常は，C の犯罪の発覚とその後の突き上げ捜査により，B，A という情報提供者の存在が判明することになる。A は，取得したクレジットカード情報を保管して B に移転した行為が，B は，A から取得したクレジットカード情報を保管して C に移転した行為が，それぞれ ID Theft となりうるが，A，B の犯罪目的を立証するためには，結果として C が実際に犯罪行為に及んだという客観的事実が重要な証拠となる。組織的犯行で，当該個人情報の流通過程のコマの一つにすぎない犯罪者の場合は，具体的な最終犯罪を知らないで情報を流通させていることがある。この場合にも「何らかの犯罪」という程度の立証で足りることが，ID Theft を犯罪化するメリットでもある。



(4) 具体的手口

ID Theft の元の情報がどのように盗まれるのかについては，はっきりした統計がない。しかし，組織的犯行だからといっても必ずしもフィッシング（後述）のようなハイテク手段によるばかりでなく，財布を盗んでその中のクレジットカード等を悪用する，という原始的な手法でも甚大な被害を負わせることが出来る。例えば，ある集団は，国立自然公園駐車場をターゲットにしていた。こういった施設の駐車場は，散策やキャンプに来ている者しか駐車しないため，ほぼ丸一日，どんなに少なく見積もっても，数時間は車に戻ってこないことが分かっている。また公園にもよるが，朝早くにやってきて，夕方遅くに帰っていくというように，駐車場への人の出入りのある時間帯も決まっている。さらに，散策やキャンプに不必要な財布，とりわけクレジットカードなどを，車に残したままにしていることも多い。そこで，犯行グループは，安全に車上狙いを続けることができるのである。

参考までに，ID Theft ではないが，行為地や被害発生地が複数の州にまたがっている場合に問題となる管轄の処理例として，インターネット販売の詐欺がある。代金を先に受領しておいて商品を送らない

か，宣伝した物には全く見合わない価値の商品を送りつけるといった手法だが，媒体がインターネットに代わっただけで，以前からも，カタログ販売，テレビ通販などで同様の消費者詐欺事犯が存在していた。ただ，インターネットを用いると被害者が全米に分布しているということに加え，インターネット上の通信で欺罔行為がなされているため，どこをもって行為地と理解すればよいのか，という問題も生じた。これについては結局，全ての被害者が一度は経由したことが明らかな，当該インターネット販売サイトのサーバーの所在地を管轄として起訴・公判が遂行されている。

4 その他の規制・取組み

(1) 被害者への利便性向上

連邦法（the Fair Credit Reporting Act, the Fair Credit Billing Act, the Truth in Lending Act, the Fair Debt Collection Practices Act 等）では，ID Theft の被害者である一般消費者を保護するための様々な権利を定めている。例えば，SSN 等の信用情報を悪用された被害者（名義を冒用された者）は，大手信用情報業者3社（Equifax, Experian, TransUnion）のいずれかに被害事実を伝えて「警告（fraud alert）」を発するよう要求すれば，自動的に，3社から「警告」が発せられ，「警告」が出ている名義人について取引（口座の開設等）に応じようとする事業者は，名義人本人に連絡を取る義務を負う，などである。FTC では，これらの内容を分かりやすく説明した小冊子を配布し，あるいはホームページでダウンロードできるようにして情報を提供している（**巻末資料4**参照[64]）。

また，FTC は，今後の取組みとして，「ID Theft 宣誓供述書（Affidavit）」という一定の書式の，いわゆるなりすまし犯罪に関する統一被害届の使用を推進している（**巻末資料5**参照[65]）。これは，一般消費者が，複数の CRA や法執行機関に被害届出をする都度，各提出先の定める異なる様式に従わなければならないとするのは，一般消費者に過大な負担を強いるものであるため，民間企業と法執行機関で共通に使える統一規格の被害届を作り，被害者が同じ書類の必要な部分だけを提出先に応じて書き換えればすむようにしようというものである。これが官民全体で採用されれば，被害者のみならず，事業者や法執行機関も同一の書式で扱うことが可能になり事務の合理化が図られるだろうと期待されている。

(2) Real ID

2001年9月11日の同時多発テロを受け，いかに，アメリカ国民であることを確認するかについては，国家安全保障の要であるかの様相を呈してきた。現在，写真入りの身分証明手段としては，各州で発行される運転免許証が最も流通しているが，もちろん，全てのアメリカ国民が運転免許を有しているわけではなく，州によっては，運転免許証を有さない者への写真付き身分証明書の発行をしている。また，カリフォルニア州等では，不法移民でも免許証を発行していたことがあるなど，連邦としての統一性はない。そこで，2005年5月に補正予算の一部として成立し，2008年には施行されることになっている Real ID Theft 法[66]によって，運転免許証の発行要件を定め，いわば，運転免許証を国家としての身分証明書として機能させようとすることになった。

しかし，もともと不法移民にも運転免許を取得させようとした州があったのも，長い国境をメキシコと接し，絶え間ない不法移民の流れが物理的に止められない以上，真面目に生活する限り不法移民とはいえ更に社会の不安定要素としないためにも，身分証明手段を与えた方がいいのではないかという価値

64 http://www.consumer.gov/idtheft/ddd/index.html
65 http://www.consumer.gov/idtheft/pdf/affidavit.pdf
66 United States Public Law 109-13 (H. R. 1268) Division B

判断があったからである。Real ID Theft 法の施行により，アメリカ国内に安全に取り込むことができた不法移民を，再び疎外化するおそれがあるとともに，今後のアメリカの個人情報の流出問題上，第2のSSN となりかねない危険性がある。

第4 カナダ

1 連邦と州との関係

カナダは，10州(Province)[67]と3準州(Territory)[68]からなる連邦国家である。イギリスから独立する新国家が自ら憲法を制定したアメリカとは異なり，カナダは，イギリスの議会が，当時のカナダ領内の植民地を統合するために制定したThe British North America Act（The BNA Act又はThe Constitution Act of 1867，以下，「1867年憲法」という。）によって誕生している[69]。その後1982年に，形式上は1867年憲法の改正としてイギリス議会で制定されたThe Canada Actの一部であるThe Constitution Act of 1982により，カナダの憲法がカナダにおける最高法規であることが定められ，イギリスの法制度との上下関係が分断された。実際の「憲法」規範は，1867年憲法の条文も含め，30近くの法律や命令等から構成されている。

政治体制としては立憲君主制であり，英連邦の一員として英国女王を国家元首としているが，統治は，連邦においては連邦首相及び内閣，州においては州首相及び州政府によって行われている。

連邦議会は二院制であり，任命制の連邦上院（Senate）と一般有権者の投票によって選出される連邦下院（House of Commons）から構成される。議員内閣制であり，連邦首相は連邦下院の第一党の党首が任命され，内閣を構成する閣僚は議員の中から首相により選任される。

連邦と州の権限については，1867年憲法に規定されている。連邦議会は，公債発行，通商規制，郵便，軍，通貨高権等について[70]，州議会は，州の税収目的のための課税権，医療制度，地方自治体の設置権，婚姻許可等について，それぞれ権限を行使する。

刑事司法については，同憲法第91条27号により，連邦議会の権限下におかれているが，州議会は，同憲法第92条14号により州内の裁判所の設置・運営について権限を有しており，更に同条第15号により州法の執行のために必要な刑罰法規制定権が認められている。実務上の基本となるのは，実体法と手続法（一部）を規定しているCriminal Act（以下，「刑事法」という。）という連邦法である。したがって，法律体系としては，判例法によって形成されてきたイギリス法の影響を強く受けているが，制定法を前提にしての運用となる。

実際の捜査・訴追・裁判・執行を担当するのは州政府である。したがって，裁判組織も，各州によってバラエティがある。しかし，州の裁判所でも，地方裁判所レベル以上の裁判官は連邦によって任命されている点において，また，裁判所組織として，カナダ中の全ての裁判における最終的な上訴審裁判所はカナダ最高裁判所（The Supreme Court of Canada）である点において[71]，アメリカに比較すると，

---

67 Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Prince Edward, Quebec, Saskatchewan

68 Northwest, Nunavut, Yukon

69 当時，連邦に含まれていたのは，ノヴァ・スコシア，ニュー・ブランズウィック，プリンスエドワード・アイランド，ケベック及びオンタリオの5州である。もともとケベック州及びオンタリオ州東部はフランス領であったが，1774年の国王布告により，「財産権及び私権（property and civil rights）以外はイギリス法によって統治されることになり，逆を言えば，私法の分野はフランス法が残ることになった。現在は，ケベック州のみがフランス系私法を維持している。

70 1867年憲法第91条

71 カナダの裁判所は，4層構造となっている（軍裁判所，行政仲裁裁判所を除く）。

1 連邦最高裁Supreme Court of Canada

より統一されたシステムとなっているといえる。

2　現行法における個人情報に関連する犯罪の規制

以下，カナダにおける個人情報に関連する犯罪の規制について，アメリカと対比するため，窃盗，詐欺等，現行の刑罰法規での規制状況を検討するとともに，個人情報に関連する犯罪を規制する上で有効と思われる，カナダ法に独特の詐称罪についても紹介する[72]。

(1)　窃盗罪[73]

カナダにおける窃盗罪は，「権限無く，不正に『何か（anything)』を，所有者等から奪う，質入れする，履行不能な返還条件付きで手放す又は原状回復できないような形で扱う目的で，取得する又は自己ないし第三者の用に供すること」をいう[74]。判例では，この「何か」は，有体物・無体物を問わないが，①財産権の対象であること，②被害者から奪える性質のものであること，を要求されている。さらに，同判例上，当該情報が秘密情報であるからといって，窃盗の客体とはならないとされている[75]。そこで，預金債権等は，「情報」であるとしても，①財産権の対象であること，②被害者から奪えることから，もともと窃盗罪の対象に含まれていると解されているが[76]，非財産的情報，例えば氏名，住所，運転免許情報，社会保険番号（Social Insurance Number，アメリカのSSNと同様の機能を果たす。以下，「SIN」という。）などという個人「情報」については，日本と同様，窃盗罪の対象となっていない。

(2)　詐欺罪

他方，詐欺罪は，「虚偽の方法によって，公衆または個人から何らかの財産，金員，有価証券，サービスを騙し取ること」をいう[77]。客観的構成要件としては，①虚偽の方法，②それにより被害者に経済的損

2　控訴審（連邦・州）Federal/Provincial Court of Appeal

3　地方裁判所（連邦・州）Federal Trial Court/Provincial/Territorial Superior Court

4　簡易裁判所（州）Provincial Court

72　経済・社会生活上の仕組みなどは，概ねアメリカに類似していることから，別個制度としては詳述しない。

73　Theft（窃盗）との標題が付けられているが，構成要件からは，日本の横領行為を含むと思われる。

74　カナダ刑事法第322条第1項：Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything, whether animate or inanimate, with intent

(a)　to deprive, temporarily or absolutely, the owner of it, or a person who has a special property or interest in it, of the thing or of his property or interest in it;

(b)　to pledge it or deposit it as security;

(c)　to part with it under a condition with respect to its return that the person who parts with it may be unable to perform; or

(d)　to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.

75　*R. v. Stewart*, [1988]1 S.C.R. 963当該判例で問題となったのは，あるホテルの警備員に対し，報酬と引き替えに，従業員リスト（氏名，住所，電話番号等）を教えるよう唆したという事件である。警備員が，そのまま通報して発覚したことから，情報が化体した有体物の移転が全くないので，リスト（情報）が欲しい，と言ったことが窃盗（又は詐欺）教唆に該当するか，として争点となった。

76　*R. v. Stewart*, [1988] 1 S.C.R. 963。なお，クレジットカードなど支払用カード情報については，窃盗や所持，移転，使用（第三者に使用させることも含む）も処罰対象となっている（カナダ刑事法第342条第3項)。

77　カナダ刑事法第380条（被害額によって法定刑が2種類ある）：Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service…

失が生じ得ること，主観的構成要件としては，③虚偽の方法であることの認識，④当該方法によって被害者に経済的損失が生じ得ることの認識（多重債務者が，ギャンブルで金を儲けて返済するつもりで，別用途のために委託された金をギャンブルに流用する場合のように，積極的に相手に損失を被らせることを意図しない場合でも成立する。）となる。詐欺罪についても，同様に，財産的価値のない情報について「詐欺」の成立はない。従って，Aの名をBが騙ることで，Cが錯誤し，Cに財産的被害が発生した場合（主観的要件が整えば），BのCに対する詐欺が成立するが，BがAの名を用いるために，Aを欺罔し，Aから名前の使用許諾を得ていたような場合でも，Aに財産的損失が生じない限り，Aの名前に対する詐欺罪は成立しない。

そのほか，個人情報の「取得」に関連する犯罪としては，不正アクセス罪（同法第342.1条）があるが，取得に必要な行為の一部を対象とするに過ぎず，取得行為そのものを対象としているわけではない点は，日本の不正アクセス罪と同様である。

(3) 贓物所持罪

個人情報に適用可能性があるかどうか，検討される余地がある「個人情報の所持」の罪に関しては，贓物所持罪（同法第354条[78]）がある。「贓物」としたが，犯罪から派生した財産であればよく，財産犯である必要はない。ただし，物に化体していない一般的な個人情報は，property（財産）と言えないことから，純粋な情報のみの「所持」に対する適用は難しい。

(4) 偽造罪

「個人情報の使用」に関しては，一般的文書の偽造（同法第366条）及び同行使（同法第368条），パスポートの偽造（同法第57条），商標偽造（同法第405条）等が，それぞれ犯罪とされているが，偽造をするつもりでパスポート情報その他の情報を集めて持っているだけでは，何の罪にもならない。他方，偽造された身分証やパスポートを所持している場合については，前述の第354条（贓物所持罪）に該当する可能性がある。

(5) 詐称罪

カナダ刑法で特徴的なのは，詐称罪（同法第403条，personation[79]）の存在である。これは，死者・生者を問わず[80]，誰かの名前を，①自分の利益を得るため，もしくは他人を有利にさせるため，②何らかの財産を手に入れるため，又は③被詐称者又は第三者に不利益を与える目的で，詐称することをいう。ここでいう「有利」「不利」「利益」「不利益」は，財産上の利害関係のみならず，例えば逮捕を免れる目的なども含む[81]。もともと本罪は，選挙の場面で，不正に選挙人に成り代わることを処罰することを目的と

---

78 Every one commits an offence who has in his possession any property or thing or any proceeds of any property or thing knowing that all or part of the property or thing or of the proceeds was obtained by or derived directly or indirectly from
(a) the commission in Canada of an offence punishable by indictment; or
(b) an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence punishable by indictment.

79 Every one who fraudulently personates any person, living or dead,
(a) with intent to gain advantage for himself or another person,
(b) with intent to obtain any property or an interest in any property, or
(c) with intent to cause disadvantage to the person whom he personates or another person, …

80 虚無人は含まない。*R.v. Northrup* (1982), 1 C.C.C. (d) 210 (Ont. C.A.)。また，フィッシングは，自然人になりすますのではないからPersonation罪には該当しない。

81 *R.v. Rozon* (1974), 28 C.R.N.S. 232 (Que. C.A.)

したものであり，あまり活用されてこなかった。しかし，個人情報に関連する犯罪について議論が高まっていることから，今後，同罪が活用される余地がある。

(6) 共謀罪

さらに，個人情報に関連する犯罪の規制に際しては，共謀罪（同法第465条(1)(c)[82]）の適用が考えられる。「共謀」の趣旨としては，２人以上の者が，犯罪を遂行すること又は犯罪遂行によって違法な目的を達成することを合意すること，この２人以上の者の間に合意があることについての理解があること，そして，この共通の合意を実行に移す意思があることを内容とする。カナダにおいては，必ずしも共謀に基づく客観的行為（overt act）が要件とはなっていないが[83]，単に，相手方が何らかの犯罪を行うことを知っていた程度の消極的関与では足りないとされる[84]。したがって，単に一方が，犯罪に向けての何らかの準備行為を始めていたとしても，これが，共謀に基づくものかどうかは，共謀時の会話などの通信傍受記録や第三者証言が得られない限り，立証は難しいとされる。

3　立法に向けての議論

以上のように，カナダでは，アメリカでいうID Theftに相当する犯罪が法的に定義されているわけではないため，現行法上，規制対象とされていないいくつかの行為形態，特に，所持，移転行為についての犯罪化の議論がある[85]。また，カナダで議論されているID Theft罪がアメリカのそれと異なるのは，取得行為自体からの犯罪化が検討されていることである。これは，刑事実体法が連邦法で統一されていることも影響していると思われる。

犯罪化が議論されるようになったのは，アメリカと同様に，組織犯罪の資金調達手段としての大規模詐欺が見受けられるようになったことをきっかけとする。例えば，Aが個人情報を盗み，Bに売り，Bがさらにこれを Cに売り，Cがこの情報を用いて身分証明書を偽造し，Dに偽造身分証明書を売った後に，DがEに偽造身分証を渡して，詐欺に利用させた，という詐欺に向けて一連の作業が分業化され得る。その結果，前述の通り，現行のカナダ法では，最終的な詐欺行為を行ったEや，偽造犯としてのC以外を直接処罰することができず，とかげのしっぽ切りに終わる面が否めない。また，実際上も，AはBに情報を売ることは知っていても，Bが個人情報を悪用するのか，B以外の人に情報が流れるのか，それから先，どのような身分証明書に加工され，どのような犯行に用いられるのか，など，詐欺犯としての共謀を認定することも困難である。しかし，A，B，Dいずれもが，全体の事象としての詐欺に不可欠な役割を果たし，また，その行為も法的に保護されるべきではない。ID Theft罪の新設によって，A，B，Dも処罰対象とし，組織犯罪全体の抑制となることが期待されている。

また，実際の問題として，現状では犯罪とされていない以上，捜査機関の限りある資源を情報の不正取得そのものへ割り当てることが困難であることから，これら行為を犯罪化することにより，捜査機関がより早期に介入できるようになることも期待されている。

82　Every one who conspires with any one to commit an indictable offence…（なお，殺人と誣告については，別の共謀罪規定がある）

83　*R.v. O'Brien,* [1954] S.C.R. 666.

84　*R.V. McNamara* (No. 1) (1981), 56 C.C.C. (2d) 193.

85　ID Theft罪がないとしても，詐欺や偽造犯の関連犯罪であることから，捜査共助上は双罰性の観点での支障は生じていない。なお，カナダの他国との捜査共助条約の締結状態については，"Mutual Legal Assistance in Criminal Matters and Extradition," Organization of American States, Office of Legal Cooperation, 平成18年６月28日確認（http://www.oas.org/juridico/mla/en/can/en_can-mla-gen-g8iag.html）参照。

他方，カナダでは，ID Theftを犯罪化するにしても，処罰範囲を明確化し，処罰の必要のない正当な行為をどのように除外するかを更に検討する必要があると認識されている。その上で，既に犯罪化されているクレジットカード情報の移転行為等もID Theft問題として一般に認知されていることから，電子通商制度など，他の関連法との関係やそれらの改正も視野に入れながら，検討が進められている。そこで，以下，立法論以外の取組みについて紹介したい。

4 通報・その他の取組み

(1) フォンバスターズ（Phone Busters）

情報の収集という意味では，連邦警察（王立騎馬警察，Royal Canadian Mounted Police。以下，「RCMP」という。），オンタリオ州警察（Ontario Provincial Police。以下，「OPP」という。）が，フォンバスターズ(Phone Busters)と呼ばれるシステムを共同運営している。フォンバスターズは，ID Theftや消費者詐欺等，郵便や電信電話，インターネットなどを通じた詐欺的行為の被害者からの被害申告を集積するコールセンターである。フォンバスターズでは，被害者から被害申告を受け，その内容に応じた助言，被害回復のための情報提供を行うほか，データを収集，分析し，法執行機関に提供し，犯罪摘発に役立てている。

フォンバスターズ設立の契機は，1991年，OPP組織犯罪対策部がオンタリオ州北部での大規模消費者詐欺事犯に関して多数の通報を受けたことである。従来，消費者詐欺事案は，被害一件あたりの被害金額が少ないことから，警察の現場にとっては捜査対象として優先度が低かった。また，いざ，総額としての被害が甚大な大規模事案であることが判明しても，被害が広く浅く複数の警察の管轄にまたがり，摘発についても困難が伴っていた。

そこで，通報内容の集積・分析に努めたところ消費者詐欺事案はオンタリオ州のみならず，全カナダを通じて発生しているものの，特にオンタリオ州における被害が全消費者詐欺事案の約50%を占めることが判明した。また，モントリオール（ケベック州）から，オンタリオ州，さらには全カナダに向けられた消費者詐欺事案が顕著であることなども判明し，犯人の検挙・訴追にあたって，分析された情報が活用された[86]。このような経緯から，消費者詐欺事案における情報集積と，管轄を越えた捜査態勢の必要性が認識され，1993年にフォンバスターズが設立されることとなった。さらに，英語圏カナダにおいては，通商関係においてアメリカと密接な関係を有していること，相対的な経済力ではアメリカのほうが優位にあることなどの背景から，カナダ人がアメリカ人相手に詐欺スキームを仕掛ける傾向が強いため，フォンバスターズでは，1996年ころからアメリカからのマルチ商法被害者の通報も受け取るようになっている[87]。

フォンバスターズは，1997年には捜査部から独立した情報受付センターとなり，独自に犯罪予防・啓蒙活動や，捜査協力を行うようになった。体制としては，物理的にはOPP本部内に所在するが，RCMP，OPP双方の警視正の階級にある警察官が共同管理者となっている。被害通報を受けるコールセンターに42名，情報分析部署に5名配属されている。実際に被害通報の電話を受け付ける者は常勤で13名いるが，うち2名は，RECOL（後述）との兼任となっており，実働としては11名で，パートタイムの3名が交替

86 トロント市（オンタリオ州）及びモントリオール市（ケベック州）は，カナダ第1，第2の都市である。オンタリオ州とケベック州は隣り合わせに位置しており，州境にあるオタワ市（オンタリオ州）がカナダの首都である。両州は植民地時代からカナダにおける経済的，政治的な中心であったが，オンタリオ州が英語圏，ケベック州がフランス語圏ということで，よりアメリカ経済との同調性の高いオンタリオ州の方が，比較的経済水準が高い。

87 マルチ商法（Make Money Fast，MMFなどと呼ばれる）については，被害者の4割をアメリカ人が占めている。

で常勤者をサポートする[88]。これら人員の出身母体も，RCMP，OPPが中心となり，そのほか，Competition Bureau[89]（競争局。後述）から，5名参加している。

犯罪予防・啓蒙活動としては，インターネットやパンフレットなどを通じての広報活動のほか，1997年からシニアバスターというプログラムをもうけている。これは，消費者詐欺事案の被害者は高齢者であることが多いため，50歳以上のボランティア60名を用いて，高齢被害者本人やその家族の相談・支援に応じるものである。同じ年代からのアドバイスということで，サービスを受ける側からは受け入れやすい制度として好評だとのことである。

コールセンター業務としては，かけられた電話から情報を聞き出し，どのような犯罪被害の申告なのかを分類する。前述のように，受信担当者自身，捜査機関出身者なので，すでにこの受信段階で，証拠収集の要否，組織犯罪の関与の度合い，汚職の有無など，単なる被害金額の多寡以上の情報を収集する。さらにこれを情報分析部が，関連通報を集積するなどして単一ファイル化できるものはファイル化し，関係諸機関へ送る。

なお，フォンバスターズでは，犯罪の種類を電話商法詐欺，西アフリカ詐欺[90]，ID Theft及び迷惑メールに分類している。フォンバスターズでいうID Theftとは，他人が，被害者の名前や個人情報を用いて詐欺を行ったことを意味する。したがって，自分のクレジットカードで知らない間に商品を買われた，自分の名前で知らない間にローンが組まれていた，などの事案がこれに該当する。

情報分析部では，2005年中に，電話商法詐欺552件，西アフリカ詐欺101件，ID Theft 31件，迷惑メール46件，合計730件をファイル化し，このうち，電話商法詐欺453件，西アフリカ詐欺65件，ID Theft 20件，迷惑メール46件，合計584件のファイルを法執行機関などに送っている。情報の送り先は，RCMPが202件，OPPが80件，競争局が42件，その他のカナダ内の法執行機関が71件，国外の法執行機関が43件，行政規制機関が85件，民間組織が61件である。

フォンバスターズに1995年から2006年1月現在までに集められた情報によると，約21,000人のカナダ人が被害に遭い，5億カナダドル以上の損害が発生している[91]。創設以来，フォンバスターズの認知度が広まってきて，扱う件数も増えてきているところであるが，そもそも消費者詐欺事案の場合，被害者が被害に遭ったことが自らの落ち度であると思うなどして，被害申告を躊躇したり，申告をあきらめたりする者が少なからず存在するため，被害の全貌を把握できているとは言い難い。また，ID Theftは，被害者が知らない間に情報が何らかの形で漏れている事案であるため，ID Theftの元となる，当該情報が犯罪者の手に渡った経緯についての実態を把握できていない。

(2) Reporting Economic Crime On-Line[92]（以下，「RECOL」という。）

RECOLは，2003年10月に，RCMP及び当時RCMPを所管していたDepartment of Solicitor General（法務次官室）によって設立された，経済犯罪に対するオンラインのみの24時間被害受付センターであ

88　2005年1月4日から11月25日までの間に，92,307件の電話通報があった。そのうち，受信者がその場で電話に応答できたものが約60%にあたる54,986件であり，留守番電話に残されたメッセージにかけ直す形でフォローできたものが約24%にあたる22,074件，結果的に通報を受けられなかったものが約17%にあたる15,247件である。平均反応時間は，約2分と短い。

89　産業省（Industry Canada，後述）の一部局で，日本の公正取引委員会に相当する。ID Theftとの関係では，特にインターネットや，健全な通商の確保の視点から関与している。

90　注19参照

91　1995年1月時，1カナダドル＝109.1円，2006年1月時，1カナダドル＝104.1円。「日本銀行外国為替市場時系列データ」平成18年11月22日確認（http://www.boj.or.jp/type/stat/dlong/fin_stat/rate/index.htm）。

92　http://www.recol.ca/

る[93]。時間的制約や国境等を越えて広く被害申告を拾い上げることが期待されている。被害データ提供は，フォンバスターズ，カナダ詐欺被害通報センター（Canadian Anti-fraud Call Center）やアメリカのIC3からもなされており，情報の一元化が図られている。また，情報を提供する先の捜査機関としては，RCMP，OPPほか，カナダの法執行機関やアメリカのFBIなども含まれている。

(3) Department of Public Safety and Emergency Preparedness of Canada（以下，「PSEPC[94]」という。）

省名を直訳すると，公共安全・緊急事態対応省となるが，治安維持省と訳される例もある。PSEPCは，2003年に新設された省で，その前身は，RECOLの立ち上げにも関わったDepartment of Federal Solicitor Generalであり，治安維持にかかる部局を総合的に統括している。配下にあるのは，RCMP，国境警備庁(Canada Border Service Agency)，銃器センター(Canadian Firearm Centre)，矯正局(Canadian Correctional Service)，仮釈放審査会（National Parole Board）などで，必ずしも個人情報に関連する犯罪に限ってはいないが，公共の安全にかかる諸問題に対し，各部局からの報告を受けながら，施策の調整を図る立場にある。

(4) Industry Canada[95]（産業省）

産業省は，日本の経済産業省に対応し，産業界の立場からID Theft問題に関わっている。特に，その中の競争局は，マルチ商法や電話取引詐欺など，商取引を仮装した詐欺的行為の規制に関わっていることから，沿革上，フォンバスターズに参加している（前述）。

また，産業省内のOffice of Consumer Affairs（消費者問題対応室）は，消費者保護の観点で研究・分析を行っている部署であるが，ID Theftとの関わりでは，プライバシー保護や，迷惑メール規制などの視点から情勢分析を行っている。なお，同室の性質上，同室ではIdentity theftを，「他人の個人情報を，その者の知らない間に，または承諾なく，詐欺，窃盗や偽造などの犯罪に用いること及びこれら犯罪に用いるために個人情報を取得し，移転させること」と定義している[96]。

同室の分析では，迷惑メールの件数自体はそれほど増加していないが，問題なのは質的な変化であり，かつて多かった単なる嫌がらせ目的のものが減る一方，2004年ころから組織的犯罪者による金銭的利益目的のものが激増している（フィッシング，スパイウェア等）[97]。これらの手法が，インターネットや通商制度一般に与える影響も大きいことから，同室を中心に，各州・準州の代表により消費者委員会(Consumer Measures Committee, CMC）が発足されており，消費者を保護し，市場をより良いものにする

---

93 開設当時のプレスリリース "Federal Solicitor General Launches New Internet Site for Canadians to Report Economic Crimes," Office of Solicitor General of Canada，平成18年10月3日，同月7日確認（http://www.recol.ca/mediaroom/SolicitorGeneralRelease.aspx)。

94 http://www.psepc-sppcc.gc.ca/

95 http://www.ic.gc.ca/

96 "Working Together to Prevent Identity Theft-A Discussion Paper," Consumer Measures Committee (CMC), Office of Consumer Affairs，平成17年7月6日，平成18年8月14日確認，(http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00097e.html)，p. 4。このペーパー（Discussion Paper）は，CMCが，施策に関して一般からの意見を得るために，2005年7月6日から2005年9月15日までインターネット上に掲示していた試案（いわゆる叩き台）である。

97 インターネット上の，迷惑メールの発生数，ウィルスの種類など，各種研究，統計をとっている企業は多く，アメリカでは，前述のFTCのホームページなどに詳しい。そのほか，MessageLabs(ロンドン，ニューヨーク，シドニーを拠点とする国際企業で，企業向けにインターネットメッセージのセキュリティ管理を業としている。http://www.messagelabs.com/)等インターネットセキュリティ関係業種からも，活発にリサーチがなされ，情報発信がされている。

ことを目的として，定期的に話し合いの場を持つなどしている。

消費者委員会は，個人情報に関連する問題に一括して対応できる立法を目指すべきなのか，それとも，既存の刑法，個人情報保護と電子文書に関する法律（the Personal Information Protection and Electronic Documents Act, PIPEDA[98]）や施策（電子認証の方法に関するものなど）を個別に調整していくか，という点を問題点として提示すると同時に，いずれの立法方針によるにせよ，①犯人が他人の個人情報を手に入れにくくする，②ID Theftが行われたらすぐに発見できるような体制を作る，③被害の回復を速やかに行う，という3点が重視されるべきとしている[99]。

現状においては，事業者の多くはまだPIPEDAについてよく知らず，ID Theft対策を取っていないのが実情であるため，同委員会では，立法の議論と平行して，一般消費者向けと，企業向けそれぞれに対する情報発信を行っている[100]（**巻末資料6**（一般向け）及び**7**（企業向け）参照）。

さらに，同委員会がID Theft被害者保護のために導入しようとしている施策として，クレジットカード番号をレシートやクレジットカード本体等に表示させないようにする，信用情報業者[101]から信用情報を取得しようとする者の身元確認を強化する，ID Theftによって生じる被害を最小限にとどめるための措置として，被害者（名義を冒用された者）に，名義冒用者による不正な取引を被害者の信用情報に残させない権利や，他の事業者が不正取引に応じないよう信用情報業者から警告を出させる権利，名義人が身の潔白を証明できるよう，不正取引の相手方である事業者に当該取引情報を開示させる権利等を認めてはどうかといった議論もなされている。

さらに，産業省では，特にインターネット関連の規制・対策をにらみ，国際的なID Theft，情報の流出に対処するため，国際協力にも努めている（OECD，APEC等）。

98　PIPEDAは，商業活動を行っている企業に対し，個人情報の収集，使用，開示条件などを定める法律である。収集・保管されている個人情報にかかる個人に，情報の修正申し立て権や，当該企業のPIPEDA違反行為に対する不服申し立て手段を規定している。なお，行政機関に対しては，Privacy Actが適用される。

99　前掲注96，9頁

100　平成18年6月16日確認（http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00084e.html）。

101　CRAとして前述。カナダにおいては，Trans Union，Equifax，Northern Credit Bureaus，Incが大手である。

第5 日本における現状

以上のアメリカ，カナダの状況を日本の刑事規制上の参考とする上で，どのような個人情報に関連する犯罪が発生するか，ひいては，どのように刑事規制を行うべきかという問題は，社会の中でどのような個人情報がどのように管理又は流通しているのか，といった状況に影響される面が大きい。そこで，以下，日本で個々人が自己を証明する場合の証明手段とその問題点や，現行の刑事規制状況などを検討する。

1 公的証明手段

(1) 自動車運転免許証

日本においては，各都道府県公安委員会が，自動車運転免許証の発行を行っており，公的機関が発行する証明書としては，旅券以外で唯一顔写真が貼付されていることから，実取引の中での身分証明手段としての機能は高い。

しかし，各公安委員会から発行された免許証であったとしても，名義人と使用者との同一性確保は万全ではない。運転免許証の発行要件としては，申請を受け付ける際に顔写真をその場で撮影するので，手続きを行った本人の顔写真であることは担保されている。他方，氏名，生年月日など身元に関する情報は，別途公的機関（地方自治体）が発行した住民票や戸籍によって証明することになるが，実際は，住民票や戸籍上の人物と申請者が同一人物であることの確認はされていない[102]。

また，近時，パソコン，プリンター等を用いて偽造された運転免許証を使用して，消費者金融で借入れ名目で金銭を詐取したり，預貯金口座を開設し通帳等を詐取したり，携帯電話契約を締結し携帯電話機（端末）を詐取することに成功する，既遂事案も少なくないことから，偽造運転免許証の精巧さがうかがわれる。また，各取引に際して運転免許証の真偽の確認方法の徹底が求められるところである[103]。現在，運転免許証に関しても，ICカード化が進められており[104]，その成果が期待される。

(2) 健康保険被保険者証

我が国の医療保険制度は，理論上，全ての国民（一部，長期滞在外国人を含む）が，健康保険，船員保険，共済組合，国民健康保険，老人保健のいずれかの被保険者となっていることから，この被保険者証も，個人の特定機能が高く，取引社会上も身分証明手段として広く認められている。

ただし，未だに紙の被保険者証も多く，写真が貼付されていないこともあり，パソコン，プリンター，

---

102 弟になりすまして運転免許証再交付申請書を偽造し，弟名義で犯人の顔写真貼付の免許証の交付を受けている事案もある（平成17年8月16日東京地方裁判所判決）。また，知的障害者方から盗んだ郵便物を持参し，区役所で本人になりすましてこれを見せ，免許取得のためとの理由で住民票の写しの交付を受けた上，本人確認書類としては住民票の写しだけが要求されていた運転免許試験場に，不正入手した住民票の写しを持参し，名義人になりすまして原付自動車免許の試験（筆記のみ）を受け，即日，免許証の交付を受けた男が，同免許証を使って預金口座を開設し，携帯電話契約を締結するなどしていたとして逮捕された事案もある（平成19年2月8日，読売新聞）。

103 平成17年中，東京地方裁判所で判決のあった詐欺関連事案中，偽造運転免許証を用いた事件の被告人は133人である（1人で複数の犯罪を行った者を含む。）。なお，正規に発行されている（と思われる）運転免許証を用いた事件の被告人は，32人にとどまる。

104 道路交通法の一部を改正する法律（平成13年法律第51号）により，平成14年6月より，運転免許証の記載事項の一部を電磁的方法により記録できることになった。

本物に類似する紙があれば，偽造が比較的簡単にできるという問題がある[105]。平成13年2月の健康保険法施行規則及び国民健康保険法施行規則の改正を受け，愛知県豊田市などで，被保険者証のICカード化が進められているところである。このICカード化によって，偽造の困難性は勿論，資格審査が即座に行えるメリットが大きいが，カード化のコスト負担や，対応する医療機関等のインフラ整備の問題も発生し，完全移行はまだ困難な状況にある[106]。

被保険者証の最初の発行段階での本人性の確認は，少なくとも共済組合，健康保険，船員保険であれば，資格取得届の提出者は就労先であるから，不正交付を狙っての虚偽届のおそれは，国民健康保険ほど大きくない。実際，健康保険被保険者証目当ての詐欺事案は，国民健康保険被保険者証に集中している。不正交付の方法としては，住民票を異動させることで，転入に伴う新規被保険者証の発行を受ける例が多い[107]。

(3) 住民票

市町村長は，住民基本台帳法（昭和42年法律第81号）に従い，個人を単位とする住民票を世帯毎に編成して，住民基本台帳を作成しなければならない(同法第6条第1項)。住民基本台帳は，選挙人名簿の登録などの住民に関する事務処理の基礎となるほか，住所の公証制度としての機能を果たしているため，その他の身分証明手段を入手する際に要求される。

住民票の写しは，該当者の住民登録のある市町村役場で請求事由を明らかにし，それが不当でなければ誰でも有料で交付を受けることができることから，あえて偽造する必要性は乏しい。また，委任状さえあれば，届け出窓口では代理人の本人確認のみで住民票の異動届を提出できることから，届け出名義人の知らない間に住所を異動させ，転出証明を得ることも特段困難ではなく[108]，住民票の異動によって健康保険被保険者証を詐取する事案がみられることは前述のとおりである。

住民票についても，2003年8月から，ICカード(住民基本台帳カード，以下，「住基カード」という。)化[109]が図られ，運転免許を持たない者にとっての写真付き公的身分証明書としての機能が期待されているところであるが，住基カードの交付枚数は，平成18年3月末時点で約91万枚，人口比普及率で約0.7%に留まっている[110]。

また住基カードについては，ICチップ部分の偽造・変造は困難と思われるが，券面のデザインは市町村が自由にできるとされていたこともあり，既に偽造事案が発生している[111]。これを受けて，券面デザインについては，平成17年2月21日からある程度の統一性をもたせることになったが，従来の市町村レベルでのオリジナルデザインはそのままとすること，そもそも写真を載せないデザインも可能であるこ

105　平成17年中東京地方裁判所によって判決がなされた詐欺事案中，偽造被保険者証を用いた犯行は40件，正規に発行されている被保険者証を用いた犯行は30件である。

106　「ケーススタディ，CASE9：愛知県豊田市健康保険証をICカード化，」日経BPガバメントテクノロジー，平成14年5月31日，平成18年10月7日確認，(http://itpro.nikkeibp.co.jp/free/NGT/govtech/20050722/165130/?ST=govtech&P=1)。

107　平成17年中東京地方裁判所で判決のあった詐欺事案のうち，被保険者証を目的物とする事案5件全てが住民票異動によるものである。

108　代理申請の場合，通常，郵送などで届出人の意思確認が行われる。

109　住民基本台帳法第30条の44

110　「住民基本台帳カード(住基カード)の交付状況等について」，総務省，平成18年10月9日確認(http://www.soumu.go.jp/c-gyousei/daityo/pdf/050217_1.pdf)。

111　平成17年1月20日東京地方裁判所判決。偽造住基カードを身分証明書として使用した携帯電話機の詐欺未遂事案である。

となど，普及率の低さとも相まって，住基カードの，特にその外見に対する信頼を一般化するには至っていない。かえって，偽造しやすい公的証明手段の流通になりかねないため，今後普及に努める以前に，少なくとも外見の統一性は確保すべきではないかと考える。

(4) 旅　券

旅券の発給要件は旅券法（昭和26年法律第267号）によるところ，一般旅券は，原則として，旅券発給申請書のほか，戸籍謄本または抄本と申請者の写真の提出で足りることとされている（同法第３条第１項）。場合によっては，代理申請も可能だが（同条第４項），交付は申請者になされるのが原則であるから（同法第８条第１項。例外同条第３項），少なくとも交付を受ける者と，旅券上の顔写真とを見比べるなどの外形的同一性は担保できる。

しかし，旅券は，海外渡航をしない場合，氏名と生年月日程度しか人定事項が記載されていないため（同法第６条），国内での証明書としての価値は乏しく，自己名義で旅券が発給されていてもなんら国内生活上のメリットがない。そこで，名義貸しなどによる不正受給事案も散見されるところである[112]。また，旅券の偽変造事案も多発している。

そこで，平成17年の同法改正（平成17年法律第55号）により，①IC旅券の導入（同法第７条），②国際的な組織犯罪の防止に関する国際連合条約を補足する陸路，海路及び空路により移民を密入国させることの防止に関する議定書の国内実施の担保として，他人名義旅券の不正取得などの罰則の強化（同法第23条）[113]，③紛失などした旅券の悪用を防ぐため，再発行の手続きを待たずに失効させる制度の新設（同法第18条第６項）等が定められた。

(5) 外国人登録証明書

外国人登録は，外国人登録法（昭和27年法律第125号）に基づき，日本に在留する外国人の居住関係及び身分関係を明らかにするもので，外国人登録証明書については常時携帯義務がある（同法第13条，罰則は同法第18条の２第４号又は同第19条）。外国人には，旅券についても常時携帯義務がある（出入国管理及び難民認定法（昭和26年政令第319号）第23条第１項，罰則は第76条１項）が，外国政府が発行しており，用いられている言語，形式の不統一などからも，外国人登録証明書の方が，日本国内での身分証明手段として一般的と思われる。

登録事項の原票の管理・登録証の発行は，居住地の市町村が行う。登録には申請書のほか旅券，写真を要する（外国人登録法第３条第１項）だけなので，逆をいえば，旅券が真正でなければ，偽の内容の外国人登録証明書となる。また，有効な旅券を持たない，不法入国者，不法残留者のために，精巧な偽造外国人登録証明書も出回っている[114]。

2　取引上における個人の確認

平成17年中に東京地方裁判所で判決のあった詐欺事案（未遂を含む。）933件中，他人に成りすまして金品を入手し，またはしようとした事案は，預貯金口座の通帳等（キャッシュカードを含む。以下同じ。）を目的としたものが160件，消費者金融の会員カード（キャッシング機能があり，ATMで借入及び返済

112　なお，何人も，明らかに不当な目的に拠るものでない限り，戸籍謄本の交付請求をすることができる（戸籍法，昭和22年法律第224号，第10条第１項）。

113　偽造旅券などの所持，営利目的事犯の加重処罰化，未遂罪の新設などを含む。

114　平成17年９月に東京都内で摘発された外国人登録証明書などの偽造工場では，同年６月１日に導入されたホログラムシールの偽造品も押収され，また，全国の発行主体となる自治体の公印印影等が記録された電磁的記録媒体も押収されている。平成18年警察白書176頁。

ができるもの）を目的としたものが84件，携帯電話機端末を目的としたものが87件であり，近時の詐欺事案の中で，他人名義の物を入手する事案の割合の高さがうかがわれた。また，当初から第三者に譲渡する目的で，被告人名義（12件）や共犯者名義（８件）で預貯金口座通帳等を詐取し，またはしようとした事案もあった。これを譲渡先の第三者側から見れば，他人に成りすまして通帳等を手に入れる行為を被告人らを介して行ったものといえる。

銀行（インターネット専門の銀行を含む。）や消費者金融業者は，「金融機関等による顧客等の本人確認等に関する法律」（平成14年法律第32号。以下，「本人確認法」という。なお，平成16年法律第164号による改正により，題名が「金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律」と変更された。以下，これを「改正本人確認法」という。[115]）により，顧客の本人確認が義務づけられている。

すなわち，本人確認法は，金融機関等（銀行，証券会社，保険会社，郵便局，消費者金融業者等）が預貯金口座の開設，金銭貸借その他の取引[116]を行うに際し，顧客の本人特定事項を確認することを義務づけている（同法第３条第１項）。本人特定事項とは，自然人であれば，氏名，住居及び生年月日（同項第１号），法人であれば，名称，本店又は主たる事務所の所在地（同項第２号）及び法人のための取引の任に当たっている自然人についての本人確認（同条第２項）をいう。本人確認を要する場面は，取引開始時，大口現金取引（現金200万を超える）時，なりすましの疑いがあるときである。本人確認方法及び本人確認書類については，運転免許証，国民健康保険被保険者証，国民年金手帳，外国人登録証明書，住民基本台帳カード，旅券等の公的証明書の提示を受ける，または，これに加えて書留郵便等により転送不要郵便物等として郵便物を送付するといった方法によるものとされている（同法律第３条，同法律施行規則第３，第４条）。金融機関等は，本人確認を行った場合[117]，本人確認記録を作成し，上記確認を要する取引を内容とする契約終了日などから７年間保存しなければならない（同法第４条）。また，取引自体の記録は取引の日から７年間保存しなければいけない（同法第５条）。

さらに，改正本人確認法（平成16年12月30日施行）により，正当な理由なく預貯金通帳等（通帳，キャッシュカード，暗証番号，ネットバンキングのID番号やパスワード等）を授受することが禁止され，罰則が設けられるとともに，業として行った場合には刑を加重することなどが定められた（同法第16条の２）。本人名義で取得された預貯金通帳等の譲渡事案については，例えば休眠口座のように開設当初は譲渡の意思がなかった場合や，当初から第三者に譲渡する目的があったと疑われるが立証困難な場合，通帳等が転々流通し関与者の犯意が乏しいあるいはその立証が困難な場合などには，詐欺罪，盗品等譲受け罪，それらの共犯のいずれによっても従来は処罰が困難であった。しかし，改正本人確認法によりこれらの場合の処罰が可能になった。

次に，携帯電話事業者（以下，「事業者」という。）の本人確認義務については，従来，事業者にはそのような法的義務がなく，事業者の自主的取組みに委ねられていた。その結果，匿名性の高いプリペイド式携帯電話や，転々流通し誰が利用しているか分からない携帯電話が犯罪に使われ，摘発困難な状況が生じた。そこで，「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律」（平成17年法律第31号。平成18年４月１日全面施行。以下「携帯電話不正利用防

115　この後にも，本人確認法施行令及び同法施行規則の改正が行われ（平成19年９月22日公布），10万円を超える現金振込みに際し，本人確認が必要とされた。

116　本人確認法施行令（平成14年政令第261号）第３条第１項

117　金融機関は，外国為替及び外国貿易法第18条により，日本から海外へ向けての特定為替取引（200万円相当を超える額の支払い又は支払い等，外国為替令第７条の２）に関しても，同様に本人確認義務を有している。

止法」という。）により，事業者による顧客の本人確認が義務づけられるようになった。

すなわち，携帯電話不正利用防止法は，事業者に，新規契約締結時及び携帯電話端末の譲渡にともなう名義変更の際，顧客の本人特定事項を確認することを義務づけた（同法第３条）。本人特定事項とは，自然人であれば，氏名，住居及び生年月日，法人であれば，名称，本店又は主たる事務所の所在地をいい，取引の任に当たっている自然人の本人確認も必要とされた。本人確認方法及び本人確認書類については，第三者が入手できない公的証明書（運転免許証，旅券，国民健康保険被保険者証，国民年金手帳等）の原本の提示を受ける方法，又は，第三者にも入手できる公的証明書（住民票の写し，戸籍謄本，印鑑登録証明書等）の提示を受けたか若しくは第三者が入手できない公的証明書の写しの提示を受けた場合は，これに加えて書留郵便等により転送不要郵便物等として郵便物を送付する方法等によるものとされた（同法律施行規則第３乃至第５条）。事業者は，本人確認を行った場合，本人確認記録を作成し，契約終了日から３年間保存しなければならない（同法第４条）。また，顧客の連絡先（自然人は氏名，居所又は電話番号等，法人は名称，本店又は主たる事務所の所在地）を確認しないで業として行う携帯電話端末の有償貸与及び借受けの禁止（同法第10条，第22条），契約者が本人確認事項を偽ることの禁止（同法第３条第４項，第19条），事業者の承諾なき携帯電話端末の有償譲渡，譲受の禁止（同法第７条，第20条），自己が契約者でない携帯電話端末の授受の禁止（第21条）等を定め，これらの禁止事項には罰則を設けた。

このように，金融機関等，携帯電話事業者等では，公的証明書を提示させることを基本として本人確認を行うことになっている。しかし，これは公的証明書の取得の段階で本人確認が厳密に行われたはずだという前提に基づいている。そのため，公的証明書そのものを成りすましによって入手した場合は，本人確認ができないことになる。

このほか，取引開始後，本人（正規の利用者）が意図しないのに他人の手に通帳等や携帯電話端末が渡った場合の事後的被害を最小に食い止める手段として，各社が個別に導入しているものには，キャッシュカード・携帯電話端末等へのICチップ組み込み，携帯電話端末の指紋認証，ATMでの静脈認証，銀行窓口での対面取引への限定[118]，ATM操作毎の顧客へのメール通知，インターネットバンキングの際のパスワードや暗証番号の入力をバーチャルパッドのクリック操作[119]への変更（キーロガー対策。キーロガーについては後述），インターネットバンキング取引に利用するIPアドレスの事前登録[120]，口座不正利用による被害に備えた保険加入等がある。

3　個人情報に関連する犯罪の刑事的規制状況

(1)　個人情報の使用

個人情報の取得，所持，移転（売買含む），使用，という一連の行為中，日本の現行法上では，原則として，使用行為による法益侵害が発生するまで，処罰対象となっていない。使用行為としては，個人情報を用いて，①当該他人に成り済ますために用いる身分証明書の類を偽造する，②他人の権利を侵害する（詐欺罪，不正アクセス），③他人名義で行うことで犯行を隠蔽する（マネーロンダリング罪，不法入

118　銀行によっては，顧客の希望に応じて，ATMからの口座の利用を不可能にし，窓口での対面取引に限定するサービスを提供している。

119　キーボードから直接入力させるのではなく，パソコン画面上に現れるキーボードの絵をマウスでクリックすることによって入力させる方法。キーボードの入力情報を盗み取られることに対する対策である。

120　IPアドレスを指定することにより，他人が別のパソコンから正規の利用者の口座を遠隔操作することができないようにする方法である。

国）と，大雑把な分類が可能と思われる。一般的に，偽造罪の保護法益は，当該文書形式（私文書，公文書など）の名義人に対する社会の信用とされるが，犯罪の遂行過程全体で見ると，②か③の犯行の準備行為という機能を有している。例えば，偽造クレジットカードで商品を詐取する場合（②）や，偽造パスポートで不法入国する場合などである。さらに，③の犯行は，犯人にとっての利益の中心となる行為（②）の隠蔽に向けられたものであるから，実際に遂行する時間的前後関係は別として，機能としては，①→②→③という順番に，他人の個人情報が別々の機能をもって犯人に利益をもたらす関係にある。そこで，個人情報に関しては，各使用以前の行為の処罰として，又は，それ自体準備行為としての性格を有する①の行為のさらにそれ以前の準備行為に対して，どのような擬律をもって対応できるのか，あるいは，そもそもそこまで処罰範囲を広げてもいいのか，という点を検討する必要がある。

しかし，現状では，既存の個人情報の「使用罪」である，①から③の例として挙げたような犯罪とは別個に，「個人情報使用罪」を設ける実益が特にうかがえない。逆に，かかる漠然とした行為を犯罪化した場合，正当な使用行為との峻別が困難になると思われる。そこで，今後，個人情報を使用して侵害される新たな法益が問題となるとすれば，その法益侵害行為又はそれを可能とする個人情報の確認状況等に対処する立法を検討すれば足りると考える。

(2) 個人情報の取得

もともと，他人名義の預金を無断で引き出そうと企てたり，融資を受けるに際してブラックリストから免れるために他人名義の身分証明書を用意して行使するなどして他人の権利を不当に侵害したり，他人名で犯罪を行うことで自己の関与を隠蔽することは新しい現象ではない。したがって，犯罪者は，かねてから，特に科学技術的な要素がなくともなんらかの形で他人の情報を取得していた。科学技術は，この従来から存在している手法を，より効率的に，あるいはより発覚しづらい形で発展させているに過ぎない。以下，取得状況ごとに羅列する。

ア　公開情報の取得

公開されている情報を用いた場合，当然，当該情報を取得すること自体には何の犯罪性もない。しかし，過去，住民基本台帳法（昭和42年法律第82号）第７条各号に定める住民票の記載事項の内，第１号～第３号，第７号の氏名，生年月日，性別，住所に関しては，住所の公証制度として何人にも大量閲覧が可能な状態とされていたため，ダイレクトメール業者などによる営利目的利用や，悪徳商法業者などによる不正目的でのリスト作りなどにも利用されていた点が問題視されるようになってきた。さらに，近時保護者が一人しかいない女子小中学生の住所を調べ，保護者が就労中で留守番中の女児らに性的暴行を繰り返すという事件も発生した[121]。

そこで，かかる情報の原則公開制について問題が提起され，平成18年６月15日に公布された住民基本台帳法の一部を改正する法律[122]によって，何人でも不特定多数の個人情報について閲覧を請求できるという制度が廃止された。同改正法では，閲覧することが出来る場合を公益性の高い調査研究や，公共的団体の活動などに限定することや，閲覧者の氏名などの公表，目的外利用や偽りその他不正手段による閲覧の禁止とその際の罰則などが定められた。

イ　既に知っている他人の個人情報の悪用

従来から，例えば，家族間などで預貯金を無断に引き出す例などが多く見られる。また，無免許運転中に検挙された際，免許を有している兄弟・知人に成り済ますため，それらの者の氏名・生年月日など

121　平成18年３月２日名古屋地方裁判所判決，強姦致傷，住居侵入など
122　平成18年法律第74号。平成18年11月１日施行（平成18年政令第297号）

を申告して免許証不携帯罪での切符処理で免れようとする事案なども，財産的被害ではないが，悪用する個人情報源の分類としては，同じといえる。

このように，親戚・知人としてもともと持っている知識を悪用する場合，もともとの個人情報取得過程において違法はない。既に「占有している」情報を，当該情報の名義人の承諾無くして使用する行為について，犯罪の成否が問題となるにとどまる。

ウ　他人の個人情報を，当該他人に知られない間に取得する場合

次に，新たに犯罪のために他人の個人情報を手に入れる場合で，かつ，その情報の「占有者」または「所有者（名義人）」が，いつ，犯罪者に情報が渡ったのか分からない場合を検討する。

まず，情報が化体した物を取得する場合，例えば，情報が印字された紙，カード情報が入力・刻印されている各種支払用カードなどについては，その物の取得行為態様によって，窃盗，詐欺，恐喝など，財物一般に対する取得行為と同様に規制される。これらの犯罪が成立する場合は，情報が犯罪者に渡ったことについては，直ちに又は一定期間後に，被害者に知られることが多いであろう。しかし，情報が記載された紙をゴミ箱から漁って入手し情報を悪用した場合，そのゴミは財物として評価しうるのかという問題があるほか，情報を悪用された被害者は，いつ，どのようにして情報を盗まれたのかの自覚がないのが通常と考えられ，加害者の特定も困難な場合が多いであろう。

情報が物に化体されていない場合としては，他人が自己の身分を何らかの書類に記載している時に横から覗く，あるいは書き損じた書類をゴミ箱などから漁り情報のみを記憶する（ゴミ自体は拾わない）といった方法が考えられ，これは原始的な方法と言える。

これらに若干の技術的進歩を加えると，ゴルフ場などの貴重品ロッカーの暗証番号の入力状況や，銀行などのATMで使用したカードの番号及び暗証番号の入力状況などの盗撮，客が支払いに提示したクレジットカードを店員が隙を見てスキミングするといった手法となる。スキマーの性能によっては，クレジットカードとの物理的接触がなくても磁気情報を読み取ることが可能であるため，すれ違いざまにバッグ越しで情報を取得することも可能となっている。

さらに，近時話題となっているのは，コンピュータ使用者が知らない間に，当該コンピュータがスパイウェア（spyware[123]）に感染し，被害者がインターネットに接続している間中，コンピュータ内に保存

123　スパイウェアとは，コンピュータ使用者の情報（入力状況，パスワード，閲覧したウェブサイト，インストールしてあるアプリケーション・プログラム，OSのバージョン等）を，当該コンピュータ機器から集める機能をもったプログラムのことをいう。コンピュータの画面上の動きがないことから，使用者が知らない間に情報を集積し，ハードウェアに記録するか，インターネットを通じて送信している。元々は，市場調査や，企業内での従業員監視，子供が有害サイトにアクセスしないように監視する，捜査等におけるインターネット「傍受」など，有用な目的のために開発されたもので，いくつかの種類がある。

・　アドウェア（Adware）：インターネット上，無料で公開されているソフトウェア（フリーウェア）などに付随していることが多いが，スポンサーである広告も共にダウンロードし，画面上に表示させる機能を有しているソフトウェアのことを言う。このソフトウェアは，しばしば，使用者が訪れたウェブサイトのアドレスを追い，使用者の名前，メールアドレスなどの個人特定情報とリンクして，広告主へ送信されることがある。これは，広告主が，その人の関心により添った効果的な広告をするためという，マーケティング目的のソフトウェアで，基本となるフリーウェアをインストール時の初期確認時点に，かかるadwareが含まれていることの承諾を求めていることが多いので，端的に違法とまでは言い難い。まま，細かい設定条件などを読まないうちに，設定を承諾してしまっているため，有効な承諾かどうかが問題となるが，個人特定情報の流出とはいえ，マーケティング目的であることから，実害はさほどない。

・　キーロガー（key logger）：当該コンピュータでの入力作業全てを記憶するハードウェアないしソフトウェアである。つまり，通常通りにインターネット銀行の口座へログインするためのパスワードなども，キーボードなどを用

されているデータや，使用状況（入力状況や，サーバー使用状況など）が流出する形での「情報の不正取得」である。例えば，インターネットバンキングやクレジットカードのオンライン請求書確認などでの個人口座へアクセスするためのID，パスワードなどの情報も，キーボード上の入力情報としてスパイウェア（キーロガー[124]）を通じて取得できるため，ATMカードないしクレジットカードのような各種支払用カードに物理的に接触できなかったとしても，同様の情報が，より被害者に察知できない形で得られる。

日本においては，以上のような，物に化体されていない情報の窃盗は原則として処罰対象となっておらず，その情報が悪用された場合，その悪用行為が処罰対象とされるにとどまる。例えば，スパイウェアを用いてインターネットバンキングの口座ID，パスワードを「盗み」，同被害口座から，犯人の管理する口座へ送金させる，という事案については，送金指示のために各被害口座へアクセスする点を不正アクセス行為の禁止等に関する法律違反，送金指示により犯人管理口座へ送金させたことを電子計算機使用詐欺として擬律している[125]。

現在のところ，情報そのものを取得する行為を処罰の対象としているのは，支払用カード情報を窃取するスキミング罪（刑法第163条の4第1項前段[126]）や，営業秘密の記録媒体等の複製の作成（不正競争防止法第21条第1項第5号ロ）である。これら以外にも，「財物」の解釈における有体物説と管理可能性説との2説のうち，管理可能性説に立てば，電子データ化されている企業情報等についても「窃取」の

いて入力することから，後にキーロガーの記録を見直すことで簡単に入手できることになる。ハードウェア型は，わざわざ設置されないといけないので，インターネットカフェのように，不特定多数の者が使うコンピュータ以外では，知らない間に設置されるという危険性は低い。しかし，ソフトウェア型については，トロイの木馬型ソフトウェアないしは，コンピュータ・ウイルスとしてコンピュータに取り込む危険性がある。

- ハイジャック（hijacking）：ネットワーク・セキュリティへの攻撃の一種で，2つのシステムやコンピュータなど，情報のやりとりが行われている間において，一方を乗っ取ってしまうことを言う。中間経由地点を乗っ取る場合，ブラウザーを乗っ取って当初の相手とは別のサイトに導いてしまう場合，あるいは，サイト名やサイトのアドレスなどを，正当なサイトと類似する形で登録することで，検索時に入力し間違えた人を偽サイトへ取り込むなどの方法がある。日本においても，インターネットプロバイダー兼各種インターネットサービス提供社であるyahoo!（ヤフー）と類似するyafoo（ヤホー）事件が発生している（後述）。
- トロイの木馬（Trojan horse）：一件有用なプログラムを装って，システムやコンピュータに有害な機能を隠し持っているプログラムのことを言う。単に，トロージャン（Trojan）と呼ばれることもある。

  プログラムが実行されることで，その中に潜んでいたウイルス，ワームなどがシステムそのものを破壊する設定となっている場合や，スパイウェアがインストールされる設定となっている場合，クラッカー（cracker）と呼ばれるシステム侵入者が後から入ってこられるよう，システムのセキュリティに扉（back door）を開ける設定となっている場合などがある。

  さらにRAT（Remote Access Trojans）となると，仕掛けた者（釣り人）へ情報提供するだけでなく，釣り人からの指令に基づき，当該コンピュータ内のファイルを書き換えたり，そのほかのコンピュータへのスパムメールを発信させるなど，遠隔操作を可能とする設定になっていたりする。

124　キーロガー自体は，ソフトウェア型以外に，パソコンとキーボードをつなぐ端子部分に設置するハードウェア型も存在する。ハードウェア型はウィルス対策ソフトで検出することができない。個人で，自分のパソコンに設置しておけば，パソコンで作成していた文書データが何らかのトラブルで回復できないとしても，キーロガーで保存していたものから再現できる，あるいは子供が有害サイトを見ていなかったか事後的に監視できる等，有用性もある。が，インターネットカフェなどで，不特定多数の者が使用するパソコンに設置されている場合の危険性は，ソフトウェア型と同様である。

125　平成18年3月3日，東京地方裁判所判決。

126　同項後段が，支払用カードの電磁的記録の情報の提供，同条第2項が同情報の保管，同情報を使用しての支払用カード不正作出等が第163条の2各項で規定されている。

概念を認める余地がある[127]。

しかし，支払用カード情報の取得行為が，偽造罪の類型の章におかれていることからも，これらの限定的な処罰規定の本質は，当該情報の財物性を認めたというよりも，偽造罪の前提行為としての規定と解される。したがって，カナダ法と異なり，日本では限定的であっても情報の財物性は認めない立場と解される。

なお，不正指令電磁的記録等作成等の罪（刑法（案）168条の2，第168条の3）が新設されると[128]，スパイウェアなどの不正プログラムを用いて他人の情報を取得した者について，不正プログラムを実行の用に供した（同法案第168条の2第2項）として処罰しうるようになる可能性がある。

エ　個人情報を「騙し取る」行為

新たに他人の個人情報を手に入れる場合のうち，その情報の「占有者」「所有者」自身が，何らかの欺罔に基づき，自ら情報提供をしている場合を「騙し取る」として考える。国勢調査員などと権限を偽って個人情報を収集する事案[129]は，このような情報詐取事案といえる。

しかし，窃盗同様，詐取についても，一般的に虚言などで相手を欺罔して情報を取得しても，詐欺には該当しない。ただ，オンライン決済制度など，人為を介さず財産上の利益が移転しうる現状に対応するため，「財産上の不法な利益」と解釈できる電磁的記録についての詐欺は立法的手当がなされている（刑法246条の2）。但し，これは，例えば銀行口座残高の改ざんやファイルの差し替えなどによって財産上の「利益」を得ることの処罰であって，必ずしも，「情報」の詐取を処罰対象とするものではない[130]。

手口がハイテク化した情報詐取事案としては，いわゆる，フィッシング[131]またはファーミングが挙げられる。これらは，いずれも前述のスパイウェアを活用しての詐取事案である[132]。フィッシングの最も単純な流れは，以下のようなものである。

① 犯行行為者（釣り人）が詐欺を企図してスパムメール[133]を放出する。

② 被害者（魚）がスパムメールを受信する。これは，例えば，懸賞金が当たったので，金を受け取るためには，メールにあるリンクをクリックしろ，などという内容になっている。

③ 魚がリンクをクリックすると，一見正当な企業などのサイトで，懸賞金の振込先口座を入力するよう，指示がある。

---

127 大コンメンタール刑法，第2版，青林書院，171頁

128 同罪の新設を含む，犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案については，国会で継続審議中である（平成19年2月8日現在）。

129 平成17年10月上旬，同年実施の国勢調査に関する報道多数。

130 前掲注123，172頁

131 フィッシング（phishing）は，phisher（犯行行為者）が，phish（情報提供者，被害者）から個人情報を得る手法であるが，それぞれ，釣り（fishing），釣り人（fisher）及び魚（fish）と，手法として洗練されていること（sophisticated）を合体させて出来た造語である。

132 関連用語として，スプーフィング（spoofing，なりすまし）がある。フィッシングでは，個人特定情報を聞き出すに際して情報提供者を騙すために金融機関などになりすましたメールやウェブサイトを用いることから，フィッシングとスプーフィングを同義的に扱うこともあるが，他人のID番号やパスワードなどを用いてのコンピュータやシステムへの攻撃など，フィッシング以外の犯行にも用いられる。

133 スパムメール（spam mail，迷惑メール）：ジャンクメール（junk mail）ともいう。広告目的などでの大量無差別配信メールをいう。受信者側の受信費用負担となること，大量配信によってインターネット回線に負担がかかることなどが問題とされる。ちなみに「スパム」とされる由来は，迷惑メールが否応なしに届けられるメールであることから，レストランで否応なしに缶詰肉のSPAMを注文せざるを得ない状況を表したイギリスのコントから転じているとされる。

④　魚が，この指示に応じて，必要情報を与えてしまう[134]。

この例は，懸賞金詐欺であるが，同様に取引銀行を装って，あなたの口座はおかしな動きをしているので，すぐに自分の口座内容を確認してほしいなどといった内容のスパムメールの場合もある。また，スパムメールのリンク自体は，正規の銀行ウェブサイトにたどり着くとしても，スパムメールのリンクをクリックすることで，トロイの木馬などを通じてスパイウェアをインストールしてしまい，以後の口座へのアクセス状況を監視される場合もある。

他方，ファーミング（pharming）は，あらかじめスパイウェアなどによって被害者のコンピュータ上の設定を変え，銀行口座など正規のホームページアドレスを入力しても，自動的に，虚偽ホームページへと連れて行き，本来の銀行のホームページを開いているものと誤信している被害者が入力するパスワードなどを入手する，という犯行である。これも，farming（農業）とsophisticatedの造語で，あらかじめ被害者側の設定を変える「種まき」がうまくいけば，後は適宜被害者の方から虚偽サイトへやってきて当該被害者の個人情報の「収穫」ができることから，フィッシングより効率がよい面がある。

日本では，平成17年12月時点では，まだファーミング事例の報告がない。フィッシングとしては，ヤフー株式会社の携帯電話用のホームページに似せた虚偽のホームページを作成し，同社の有料コンテンツやユーザーズアカウントへアクセスするためのID番号やパスワードを入手していた事案が初摘発例となる[135]。この事案においても，虚偽のホームページを作成した点が著作権法違反（同法第119条第1号，第21条，第23条第1項）に，その後取得したID等を用いてヤフーホームページにアクセスしたことが不正アクセス行為の禁止等に関する法律違反（同法第8条第1号，第3条第1項，第2項第1号）に，それぞれ該当するとして擬律されているが，IDやパスワードを取得したこと自体は処罰対象となっていない。この点においては，情報の不正取得と同じ問題状況にある。

ただし，財産的価値を有する電子マネーや各インターネットショップにおけるクレジットポイントなどについては，「財産上の利益」と評価できれば，その「情報」の取得に電子計算機使用詐欺が適用されよう。

(3)　情報の所持・保管・移転

個人に関する情報を保管する組織に対する義務・規制については，昭和63年（1988年）の「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（以下，「1988年法」という。）」及び平成元年（1989年）に通産省（当時）から出された「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」が存在していた。しかし，1988年法は，罰則規定がなく，また，民間企業に対しては，法的拘束力をもった規制が及ぼされていなかった。さらに，平成14年に住民基本台帳ネットワークが開始されたものの，セキュリティへの不安などから導入が円滑に進まなかったことや，平成16年にADSL回線及びインターネットサービスのYahoo! BB登録者情報が内部者から漏洩されていた事件など，個人情報保護の不十分さが問題となっていた。

そこで，平成15年5月に成立した前記個人情報保護法において，情報管理の基本原則及び民間企業の責務などを定め，そのほか，個別法として「行政機関の保有する個人情報の保護に関する法律」，「独立

134　銀行口座やクレジット口座などは，既存の口座残高を引きおろしたり，限度額一杯の買い物をしたりするなどのほか，既にある情報を元に新規口座を作り，これを売却する，あるいは新規クレジット口座の限度額一杯の買い物をする，と，新旧の口座の悪用が考えられる。新規クレジット口座開設の上では，アメリカのように社会保障番号（Social Security Number，SSN，前述。）に依存した信用情報管理や，クレジット口座開設慣行の特殊性の影響もあるので，海外で問題とされているすべての手法が即日本でも利益につながるというわけではない。

135　平成17年9月12日，東京地方裁判所判決。

行政法人の保有する個人情報の保護に関する法律」,「情報公開・個人情報保護審査会設置法」,「行政機関の保有する個人情報保護法等の施行に伴う関係法律の整備等に関する法律」の4法が順次成立し，平成17年4月1日から全面施行されている。

この基本法となるのが,「個人情報の保護に関する法律（平成15年法律第57号)」であるが，個人情報保護の基本理念や国等の責務を認めた部分（第1章～第3章）は，平成15年5月30日の公布同日から施行されている。平成17年4月1日に施行されたのは，民間事業者が遵守すべき義務を定めた一般法としての部分[136]（第4章以下）である。同時に，公的部門が遵守すべき規律として,「行政機関の保有する個人情報の保護に関する法律(平成15年法律第58号)」,「独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号）も施行された。地方独立行政法人法（平成15年法律第118号）については，平成16年4月1日から施行が始まっていた。

他方，情報公開制度については，行政機関については，行政機関の保有する情報の公開に関する法律(平成11年法律第42号)，独立行政法人については，独立行政法人等の保有する情報の公開に関する法律(平成13年法律第140号）によって，情報公開審査会がそれぞれ設置され，各法に基づく不服申立ての審査を行っていた。これらは，個人情報保護各法の成立に伴い，個人情報保護各法の不服申立制度も合わせ審査する，情報公開・個人情報保護審査会に名称，機能が改められ（情報公開・個人情報保護審査会設置法，平成15年法律第60号)，プライバシーの観点から個人情報を保護することと，情報の自由な流通によってプライバシーを含めた個人の権利利益を保護することとされている。

具体的に情報を保管する上での義務としては，同法に違反した取扱いを行った事業者に罰則が科されうる。もちろん，この罰則は，そもそも正当な理由で当該情報を所持･管理していた者，しかも，5,000人分以上の個人情報を持つ個人情報取扱業者に限定された上での管理上の違反行為であるから，犯罪行為へ悪用するための準備として権限無く個人情報を所持・管理することを処罰するものではない。

なお，情報の移転については，銀行のキャッシュカードの暗証番号，ネットバンキングのID，パスワードの授受が禁止されている（改正本人確認法第16条の2。前述。)。

136 なお，個人情報の「個別法」として，医療分野，金融分野，電気通信事業分野等，業種ごとの情報管理規制が検討されている。

第6　最後に

以上，本稿では，ID Theftや，「個人情報」の問題として挙げられるような事項を脈絡なく挙げてきた。そこで，まとめとしては，北米での状況も含めて，日本で個人情報に関連する犯罪の規制の問題をどう整理できるのか，私見を述べたい。

思うに，アメリカのID Theft法や，カナダでの立法論の中でも，クレジットカード等支払用カード情報が，分かり易く財産的被害に直結するような性質の情報であるため，支払用カード等の犯罪対策と，「個人情報に関連する犯罪」対策が混乱して議論されているような印象を受けた。しかし，クレジットカード，キャッシュカード等の情報は，「個人」を識別する情報と整理するよりは，当該クレジットカード決済用口座や，銀行口座等の「財産」を識別する情報だと考えた方が，何を保護したいのか，すなわち法益を理解しやすいと思われる。「財物」についての管理可能性説と方向性が同じ考え方である。そして，このような「財産」識別情報については，前述のように，偽造の罪の間に置かれている規定であることから，財物性を認めた章立てとは言えないが，いずれにせよ，本邦では，支払用カード情報の不正取得，所持，移転，使用，いずれの段階についても既に立法上の手当が済んでいる。

この支払用カード等情報について，財産特定情報であると理解すると，インターネットアカウントのIDやパスワード，携帯電話番号など，個別的に管理可能な「サービス利用権」の識別情報の保護のため，この不正取得，所持，移転，使用についても犯罪化を検討する余地があるように思われる。これらサービス利用権は，文字どおり，クレジットカード決済用口座などと同様，アカウント（口座）として，その口座で何ができるのか，という点に価値があり，実際の利用者が誰であるかというのは，口座の側では本来重要なことではない。アメリカの連邦法を参考に考えるならば，ID Theft罪よりは，アクセス手段に関連する犯罪の規制の問題といえる。

さらにこの延長線として，ID Theft又はID Fraudとして「個人情報」の不正取得等を処罰可能にしようと考えるときの「個人」とは，利益を利用する主体としての個人ではなく，ある個人であること自体が利用価値ある客体として理解されているものと思われる。したがって，プライバシーとしての個人情報保護の問題と混同が生じないように，アクセス手段に並行して考え，ID Theftを「身分証明のための情報に関連する犯罪」と置き換えることができる[137]。なお，アメリカのID Theft罪が，身分証明文書の偽造罪の中に創設されている状況については，前述のとおりである。

そこで，身分証明情報の規制といっても，身分証明手段が実際の犯罪現象としてどのように問題となっているのかを検討したところ，平成17年中に東京地方裁判所で「詐欺罪」の有罪判決があった933人の被告人の事件のうちには，いわゆる無銭飲食（132人）や公衆接遇費詐欺事案（5人）のように，身分証明とは関係のない犯行も含まれていた。

他方，前述のとおり，いわゆる架空請求詐欺やオレオレ詐欺（87人，共犯事件含む。）のように，金員を目的とした，いわば，最終的な犯行としての架空請求詐欺等の犯行の前提と思われる，銀行預金通帳，

137　本文上，個人に関する情報として，支払用カード等の情報，アクセス手段に関する情報，身分証明に関する情報を挙げたが，そのほか，プライバシーに関わる個人の情報（前科情報や医療情報など）も存在すると考える。既に最初に述べたとおり，プライバシーの問題は本稿では直接取り上げることはしないが，本来「公表」されている情報である名前が，例えばプライバシー情報と一緒になることで，名前の部分も含めて秘匿する必要も出てくるため（行政機関の保有する個人情報の保護に関する法律第17条等），情報を管理する側の義務としては，名前など，いわば公開情報についても，実在する個人についての情報は，適切に管理される必要性があると考える。

消費者金融カード，携帯電話機端末などを目的とした詐欺事案が数多く存在する（銀行預金通帳も，携帯電話機端末も詐取したというような複数事件の被告人もいるため，人数としては一部重複している。）。また，クレジットカードを詐欺の目的物としている詐欺犯（16人）も，最終的には，そのカードでの買い物やさらに買った物の転売による利益を見込んでいるという点で，準備的犯行といえる[138]。

さらに，前述のとおり，現在，預金口座を開設する上で，窓口での本人確認がある程度徹底されていることから，預金通帳などの詐欺事犯には，身分証明書の提示も伴っている。その中では，偽造，正規発行を問わず，運転免許証を用いた者が165人と突出している。次いで健康保険被保険者証が71人[139]，そのほか偽造の外国人登録証明書（９人）等の少数例がある。そこで，こういった身分証明書を得るための詐欺犯も存在しており，被保険者証を目的とする詐欺犯が５名いる。この被保険者証を得る手段は，主として住民票を移動させて，被保険者証を再申請するというものである。

以上のように，単純に「詐欺」犯といっても，オレオレ詐欺のための銀行口座開設に伴う預金通帳詐欺があり，その預金通帳詐欺のための健康保険被保険者証詐欺があり，さらに被保険者証詐欺のための被保険者証窃取等と，重層的な犯行がうかがえる。この一連の個人情報（被保険者証）の窃取から新しい身分証の詐取，詐取した身分証を用いての詐欺まで，すべて自分ないしはオーソドックスな意味での共犯者との間で行われている場合には，何らかの時点での犯罪が成立すれば，刑事政策的意義が達せられるので，特段情報の不正取得などの議論をする必要はないであろう。

問題は，北米での議論にも顕著なように，犯罪が組織化しているために，他人の個人情報の取得，所持，移転，使用行為のすべてが犯罪となる形にしないと，使用行為，偽造行為の共犯として評価するには，関係者の関与状態が希薄になっているため，関与した鎖の一部を問責できない可能性が出てくる点である。例えば，前述の偽造運転免許証を用いて携帯電話機端末を詐取した又は詐取しようとした66名中，少なくとも10名については，インターネットで広告されていたアルバイトとして犯行に及んでおり，組織的犯行の分業化がすすんでいることがうかがえる。

しかも，この66件は，偽造公文書行使などが発覚して結局は処罰にまで至った事案であるが，検挙されるきっかけとなる事件以前に複数台の携帯電話機端末の購入に成功している者もいる。また，前述のように，キーロガーで不正入手したインターネットオークションIDやパスワードがネット上で売買されている現状を踏まえれば，その後の詐欺を未然に防ぐ上では，アクセス手段としての情報の窃盗，所持，移転，使用についても，支払用カード情報同様，犯罪化し，重層化した詐欺事犯の一環だけに関与した者も適切に処罰できるようにすることが重要と考えられる。その際，実在する自然人の情報のみを保護の対象とすると，架空人名義や法人名義を用いた犯罪を処罰できなくなるため，名義人の実在性や自然人，法人を限定する必要はないと思われる。実際，支払用カードの不正作出については，支払用カードとして機能する情報か否かという点が重要なのであり，アクセス手段についても，アクセスできるサービスがあることが重要なのであって，名義人の実在性や法人，自然人の別は問題とはなっていないであろう。

他方，身分証明にかかる情報は，氏名，住所，勤務先など，人が社会生活を営んでいれば，当然なん

---

138 ただ，クレジットカード契約は，日本では銀行口座からの引き落とし契約も伴うことから，さほど件数的に目立っているという印象はない。この点では，消費者金融のメンバーカードを目的とする詐欺犯が84人もおり，アメリカなどでクレジットカードの新規契約として問題となるような事案は，むしろ消費者金融の締結の簡便さに置き換えられていると思われる。

139 なお，消費者金融カードを目的とする詐欺犯84人中，保険証（偽造・正規発行を問わない）を用いた者が33人であるに比して，預金口座等を詐取するために保険証（偽造・正規発行を問わない）を用いた者は28人に留まっている。

らかの形で開示されている情報でもある。身分証明にかかる情報の「窃取」行為は能動的な他人の権利侵害行為であるから，本来的には情報の性質を問わずに「窃取」という行為の不法性を議論する余地もあるが，とりわけ「所持」についての処罰には，問題が大きいと思われる。有形物について「所持」のみで処罰される罪は，本来法禁物に限られているからである。例えば，融資金手数料詐欺などで悪用される可能性が非常に高く，故に処罰価値も高いと思われる多重債務者の「名簿」の所持にしても，情報の性質としては，単に氏名，連絡先の羅列であるから，持っていること自体が処罰に値する「法禁物」的な情報と位置付けることは難しい。

その意味では，カナダでの立法論の中で意見があるように，個人情報を取得し，所持し，移転し，または使用する当該行為者に，その情報が何らかの犯罪に用いられることの認識を要件とすることで処罰範囲を限定することも一つの方法であろうと思われる。ただ，必ずしも隠されていない情報の所持，移転，使用を，刑罰対象とすることの是非については，なお慎重な検討を要するであろう。実際上も，インターネット環境のセキュリティ，個人情報を保管している側の情報流出防止・不正使用防止，各種取引上，指紋認証などの本人確認証明手段の向上，公的身分証明手段の偽造防止など，予防的観点からの対策によって，その後の個人情報の不正使用による法益侵害をより効果的に防ぐことができるのではないかと考える。

巻末資料

アメリカ

1　Federal Trade Commissionへのオンライン被害申告フォーム
2　Consumer Sentinelとの秘密保持協定
3　Federal Trade Commissionの検索ウェブページ
4　一般消費者向けパンフレット（Federal Trade Commission）
5　ID Theft 宣誓供述書（Federal Trade Commission）

カナダ

6　一般消費者向けパンフレット
7　企業向けパンフレット

資料1

ID THEFT

苦情内容入力フォーム

自分がID Theftの被害を受けたと思う場合，あなたは下記のフォームを利用して，連邦商取引委員会(FTC)に苦情内容を送信することができます。提供する情報の中身は，あなたの責任で決めることです。とはいえ，あなたが自分の名前やその他の情報を提供しない限り，私たちがあなたの苦情や要請を参照し，それに対応し，その件について調査することはできません。あなたの提供した情報の利用方法については，個人情報管理方針（プライバシーポリシー）をお読みください。

FTCは，ID Theft被害者の苦情に関する連邦の情報センターとして機能しています。FTCは個々の消費者の問題を解決するわけではありませんが，あなたの苦情内容は，私たちが詐欺の調査を行う上で役立ち，法執行の措置を可能にしてくれます。FTCは，インターネット，テレマーケティング，ID Theft及びその他の詐欺関連の苦情内容をConsumer Sentinelに入力しています。これは，世界中にある数百の民事・刑事の法執行機関が利用できる安全なオンライン・データベースです。

あなたが提供する情報は，SSL(セキュアソケットレイヤー)暗号によって守られ，安全に保管されます。

あなたがID Theft以外の苦情をFTCに申告する場合は，FTCのオンライン苦情申告フォームを利用してください。

この苦情内容を印刷する。

以下のオンライン苦情申告フォームに漏れなく記入し，FTC宛に送信すると，あなたが記入した内容のほとんどを印刷することができます。ただし，社会保障番号や口座番号など秘密性が非常に高い情報は印刷されません。印刷したID Theft苦情申告書は，あなたが地元の警察に報告する際に利用できるよう，書式設定されています。以下のオンライン苦情申告フォームの記入に関する注意事項と，印刷されたID Theft苦情申告書に関する情報は，ここから参照できます。

あなたの連絡先

ファーストネーム：
ミドルネーム：
ラストネーム：
名前の接尾辞（Jr. III．等）：
所在地住所：
アパートまたは部屋の番号：
市：
州：
郵便番号：　-
国：
この住所に住み始めた時期：　（年／月）

自宅の電話：（　　）　　勤務先の電話：　　（市外局番）（番号）　　（市外局番）（番号）（内線）
（市外局番）（番号）

携帯電話：（　　）
（市外局番）（番号）

社会保障番号：　　-　　-

誕生日：　　（年／月／日）

運転免許証の発行州：

運転免許証の番号：

Eメールアドレス：　　(i.e.,anyone@myisp.com)

事件発生時の氏名住所等が上記と異なる場合は以下に記入してください。

ファーストネーム：

ミドルネーム：

ラストネーム：

名前の接尾辞：

所在地住所：

アパートまたは部屋の番号：

市：

州：

郵便番号：　　-

国：

この住所に住んでいた時期：　　（年／月）から　　（年／月）まで

あなたが抱える問題について教えてください。

1．あなたが経験したID Theftのタイプ

誰かがあなたの名前やその他の身元確認情報をその人自身の個人的利益のために利用した場合は，ID Theftが起きたことになります。あなたが被害を受けたID Theftのタイプに該当する項目をチェックしてください（該当する全ての項目をチェックしてください。）。

□クレジットカード　　□証券またはその他の投資
□当座預金または普通預金　　□インターネットまたはEメール
□融資　　□公文書または給付金
□電話または公共料金　　□その他

容疑者はアカウントを開くために，または商品やサービスを購入するために，インターネットを利用しましたか。

○はい
○いいえ
◉分からない

2．苦情の概要

ID Theftに関する情報を提供してください。たとえば，そのID Theftがどのようにして起きたのか，犯人の心当たり，ID Theftが起きてからあなたがとった措置，行動などについてです。不正なアカウントが開設され，あるいはあなたの現在のアカウントが被害を受けた会社に関して，あなたが抱えている問題を簡潔に説明してください。説明は2,000字以内にまとめてください。

3．ID Theftの詳細

あなたは，金銭，クレジット，融資，商品，またはサービスを得るために，またはその他の目的のために，自分の名前や個人情報を使用することを誰かに許可しましたか。

○はい　○いいえ

あなたは，ここに説明されている事件の結果として，何らかの利益，金銭，商品，またはサービスを受け取りましたか。

○はい　○いいえ

(該当する場合は1つをチェックする)　あなたの個人情報または身元確認資料（たとえば，クレジットカード，出生証明書，運転免許証，社会保障カードなど）は，

□（年／月／日）（頃）に，

□盗まれた　　□無くなった。

（1つをチェックする）　あなたは犯人の訴追に，

□進んで協力したい　　□あまり協力したくない。

誰があなたの個人情報や身元確認資料をあなたに断りなく，またはあなたの許可なく利用して，金銭的取引を行ったり，小切手を換金したり，預金を引き出したり，または金銭，商品，もしくはサービスを得たりしたか，知っていますか。

○はい　○いいえ

あなたがID Theftの被害に遭っているかもしれないと気付いたのは，いつですか。　□（年／月／日）

ID Theftが最初に起きたのはいつでしたか（言い換えれば，最初のアカウントが開設されたのはいつでしたか）。　□（年／月／日）

いくつのアカウント（クレジットカード，融資，銀行口座，携帯電話アカウント等）が開設され，またはアクセスされましたか。

（該当する場合） あなたはお金をいくら支払わなければならなかったのですか。
（数だけを記入）

（該当する場合） 犯人はあなたの名義で会社からお金をいくら得ましたか。
（数だけを記入）

犯人はあなたの個人情報をどのように入手しましたか。（選択肢－侵入盗，財布の紛失，電話での勧誘，インターネット上，その他等－から選ぶ）

（該当する場合） あなたはこのID Theftの結果として，他にどんな問題を抱えていますか。（選択肢－「他に被害は受けていない」「民事訴訟が提起され，または判決が下された」「強制捜査，逮捕，有罪判決が出された」「クレジットやその他の金融サービスが受けられない」「就職を断られた，または失業した」「借金の取り立てにあった」「対策のために時間をとられた」「その他（自由記入）」から選ぶ。複数選択可。）

4．ID Theftの犯人

ID Theftの犯人の心当たりについて，わかることをすべて記入してください。

ファーストネーム：
ミドルネーム：
ラストネーム：
名前の接尾辞：
所在地住所：
アパートまたは部屋の番号：
市：
州：
郵便番号：
国：
電話番号：（）（市外局番）（番号）
Eメールアドレス：
（i.e.anyone@myisp.com）
誕生日：（年／月／日）

犯人に関する追加的情報（240字）：
あなたと犯人との関係：

5．関連機関への連絡

（該当する場合） あなたがこのID Theftに対処するためにすでに講じたのは，以下のどの措置であるかを教えてください。

（該当する全ての項目をチェックする） 以下の信用調査所のうち，
あなたはこの詐欺について報告するためにどの信用調査所に連絡しましたか。
□Equifax □Experian □Trans Union □その他 □どこにも連絡していない

あなたはどの信用調査所で自分の信用報告書に「詐欺警告（fraud alert）」を載せましたか。
□Equifax □Experian □Trans Union □その他 □どこでも載せていない

あなたはどの信用調査所で自分の信用報告書を請求しましたか。
□Equifax □Experian □Trans Union □その他 □どこにも請求していない

あなたはどの信用調査所との間に問題を抱えていますか。
□Equifax □Experian □Trans Union □その他

信用報告書に記載されている不正確な情報
個人情報（名前，社会保障番号，誕生日など）
(A)
(B)
(C)
(D)
あなたに無断であなたの信用報告書を請求した会社
会社名：
会社名：
会社名：

あなたは警察に連絡しましたか。 ○はい ○いいえ
連絡した場合，その警察署名を教えてください。
警察署の属する州：
被害届の番号はありますか。 ○はい ○いいえ
「はい」の場合，その番号を教えてください。

6．会社

不正なアカウントが開設され，あるいはあなたの現在のアカウントが被害を受けた会社または組織を明らかにしてください。できる限り具体的に情報を提供してください。

会社名 1

会社名：

アカウントの種類（※）：

新規のアカウントですか。 ○はい ○いいえ

発行または悪用された日： （年／月／日）

犯人が得た金額（$）： （数だけを記入）

信用限度額（$）： （数だけを記入）

交渉担当者：

連絡先： （市外局番） （番号） （内線）

あなたはこの会社に通知しましたか。 ○はい ○いいえ

あなたはこの会社に書面で通知しましたか。 ○はい ○いいえ

※ アカウントの種類は，選択肢－クレジットカード，当座または預金口座，融資，電話又は公共料金，証券または投資商品，インターネットまたはメール，公的書類や公的な受益，その他－から選ぶ。

会社 2

上記と同様（省略）

会社 3

上記と同様（省略）

7．証拠資料

法執行機関やあなたが通知した会社に提供できる証拠資料を明らかにしてください（一方または両方をチェックする）。

□政府発行の身元確認情報：

（選択肢－自動車運転免許証，旅券，運転免許証以外の州発行による身分証，軍の身分証明書，社員証，学生証，等－から選ぶ）

□事件が起きた時期の居住の証拠となるもの（たとえば，あなたの名義での賃貸借契約書，公共料金支払書のコピー，保険証書のコピーなど）

苦情内容を送信する リセットする

資料2

Consumer Sentinel Network 秘密保持協定

本協定は，連邦商取引委員会（以下「FTC」という）の消費者保護局（以下「保護局」という）と＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿との間で，同様の協定を結んでいる他の全ての国内外の機関及びその他の事業体との協力の下に締結された。本協定の目的は，インターネット，ダイレクトメール，テレマーケティング，又はその他の媒体を通じて以下に規定された条件下で遂行される消費者詐欺・欺罔に関する情報を含む，消費者の苦情情報の秘密保持下での交換を促進することにある。

Consumer Sentinel Network

1．FTCは，全国司法長官協会（National Association of Attorneys General），Canshare，及びフォンバスターズ（PhoneBusters）と共同で，参加している法執行機関及びその他の消費者詐欺に関する貢献者から提供された調査情報を保管するための自動データベースであるConsumer Sentinelを開発した。FTCはまた，1998年ID Theft防止法（Identity Theft and Assumption Deterrence Act）18 U.S.C. §1028に基づき，消費者，関係する法執行機関及びその他のID Theftに関する貢献者から提供された調査情報を保管するための自動データベースであるIdentity Theft Data Clearinghouseも開発した。FTCは，Consumer Sentinel及びIdentity Theft Data Clearinghouseに含まれる情報を，Consumer Sentinel Networkを通じて利用できるようにしている。双方のデータベースに含まれる情報を併せて「Consumer Sentinel Network」情報と呼ぶ。この情報交換プログラムは，連邦商取引委員会法（Federal Trade Commission Act）第6条(f)，15 U.S.C. §46(f)，委員会規則（Commission Rules）4.6，4.10，及び4.11(c)(d)，16 C.F.R. §§4.6，4.10，及び4.11(c)(d)（2000），並びに改正1974年プライバシー法（Privacy Act）5 U.S.C. §552aに準拠している。57 FR 45678，45700（1992），64 FR 57887(1999)（システム記録の通常の使用について規定した，全般的な消費者苦情システムと具体的なID Theft苦情システムに関するFTCプライバシー法のシステム上の通知）も参照のこと。

2．Consumer Sentinel Networkに保管される情報は，商業的な機密資料を含まず，主として消費者から寄せられた苦情から得られた情報と，ID Theft，詐欺及びその他の消費者保護に関する調査を通じて収集された情報に限定される。かかる情報には，何よりもまず，会社及びその代表者の名前，関連する製品又はサービスの実体，進行中の法執行措置の状況及び担当するスタッフの名前と電話番号を含めることができる。

参加者からのデータ提供

3．参加している団体及びその他のデータ提供者は，自ら事務所に設置されたコンピュータ端末を用いて，又はシステムにデータを入力する他の者に情報を提供することにより，関連情報を一方若しくは双方のデータベースに入力することができる。必要な場合，FTCは続いてかかる情報を，FTCが管理する自動データベースに登載する。

Consumer Sentinel Network 情報へのアクセス

4．Consumer Sentinel Network 内の情報は，以下の仕方で利用可能にされるものとする。

a．Consumer Sentinel データベース内の情報は，FTC と，Consumer Sentinel Network 秘密保持協定を結んでいる国内外の関係する法執行機関に対してのみ利用可能にされる。外国の法執行機関に対する開示の形式，内容及び程度は，FTC とその外国の法執行機関の双方の合意に基づき，FTC の裁量に従うものとする。

b．Identity Theft Data Clearinghouse 内の情報は，FTC と，Consumer Sentinel Network 秘密保持協定を結んでいる国内外の関係する法執行機関に対して利用可能にされる。外国の法執行機関に対する開示の形式，内容及び程度は，FTC とその外国の法執行機関の双方の合意に基づき，FTC の裁量に従うものとする。Identity Theft Data Clearinghouse から引き出される限定的情報は，1998年 ID Theft 防止法，18 U.S.C. §1028及びプライバシー法，5 U.S.C. 552a に準じる程度において，本協定を結んでいるその他の関係する国内の政府機関，信用調査機関，及び民間事業体に対しても利用可能にされる。それらの関係する国内の政府機関，信用調査機関及び民間事業体に対する開示の形式と内容は，FTC の裁量に従うものとする。

Consumer Sentinel Network 情報の秘密保持と利用

5．この情報交換システムに参加している全ての当事者は，全ての Consumer Sentinel Network 情報－Consumer Sentinel Network の限定的ウェブサイトで利用できる全ての情報を含む－が秘密を保持されなければならないとの了解の下に参加している。特に，本協定を締結する当事者は，本協定の拘束を受け当該情報を知る必要のある，その従業員，コンサルタント，契約者又は誠実な法執行機関職員以外に対しては，当該情報を開示しないことに同意する。FTC は，本協定の条件に違反した全ての関係する機関若しくはその他の団体による当該情報へのアクセスを制限し，又は取り消す権利を保持する。

6．本協定を結んでいる当事者は，Consumer Sentinel Network に含まれている情報を以下の仕方で利用することに同意する（いずれか一方の規定だけを選択する）。

a．本協定を結んでいる当事者_____は，国内又は外国の法執行機関であり，本協定の第 4 項に基づいてアクセスできる Consumer Sentinel Network 情報を，法執行の諸目的に関連する限りでのみ利用することに同意する。

又は，

b．本協定を結んでいる当事者_____は，関係する国内の政府機関，信用調査機関，又は民間事業体であり，当該当事者に開示される限定的な Identity Theft Data Clearinghouse 情報を，FTC が定める追加的条件に従い，18 U.S.C. §1028(a)に規定された詐欺を防止又は調査する目的のためにのみ利用することに同意する。

7．法律により認可される場合を除き，保護局は，Consumer Sentinel Network に含まれる情報が，本協定に定められている関係機関及びその他の事業体，並びにかかる団体及び FTC の従業員，コンサルタント，または契約者であって当該情報を知る必要のある者を除いては，何人に対しても開示されないことに同意する。ただし，FTC が他の連邦の法執行機関または議会[1]から公式の要求を受けた場合，あるいは FTC が Consumer Sentinel Network 内の情報を非参加者に提出するよう，かかる命令を出

す司法権を有する裁判所から命じられた場合は，FTCは自らの裁量において，法に定められた該当する制限に従い，当該情報の秘密保持の必要に応じ，当該情報を提出することができる。加えて，FTCは，要求があった場合は総統計を参加者に利用できるようにし，また傾向データを一般公衆に開示し続けるものとする。

8．参加当事者は，Consumer Sentinel Networkに含まれる資料の照会を受け，又はその情報が強制的手続に従うことになった場合は，FTCの交渉担当者にかかる事実を即座に通知し，照会のあった情報を提出するか否かについて，また当該情報を提出しなければならない場合はその秘密を保持できるような提出の仕方について，時宜にかなった決定を行いうるよう協力することに同意する。

9．FTCは，消費者保護局の計画・情報部門の副部長を，国内の機関及びその他の事業体に関連するこの情報交換プログラムの諸目的に関する交渉担当者に任命した。この担当者は，Consumer Sentinel Networkに含まれる情報の秘密保持を保証する責任を有し，また適切な状況下では，参加者が照会や強制的手続に対応するため情報の追加的開示を行うことについて認可する責任を有する。当該副部長はまた，消費者詐欺に関連するFTCの証拠資料へのアクセスを求める国内の法執行機関からの要望に対応する権限も，委員会から委任されている。かかる要望は委員会規則4.11(c)，16 C.F.R. §4.11(c)に定められた手続に基づいて処理されるが，その際，要望を出した当事者は，当該資料が法執行の目的に利用され，その秘密が保持されることを保証する証明書を提出しなければならない。委員会は，国際消費者保護部門の副部長に対し，委員会若しくは委員会代表によって情報へのアクセスがすでに認可された又は今後認可される外国の法執行機関との間でConsumer Sentinel Network秘密保持協定を締結する権限を委任した。委員会はまた，国際消費者保護部門の副部長に対し，若干の非公開の情報を外国の法執行機関に開示する権限も委任した。外国の法執行機関とのかかる秘密保持協定の締結及び外国の法執行機関へのかかる開示は，67 FR 45738(2002)又は委員会が公表したその他の連邦行政命令集（Federal Register）の通知若しくは規則に準拠するものとする。消費者保護局の局長は，62 FR 15185(1997)に定められた委任権に基づき，再委任の手続を踏むことにより，消費者保護に関する若干の情報への外国からのアクセスの要望に対応することもできる。

_____は上記の条件に同意する。

署名_____

名前_____

肩書_____

日付_____

郵便先住所_____

電話番号_____

Eメールアドレス_____

David M. Torok

消費者保護局，計画・情報部門，副部長

1　FTCは情報の秘密保持を維持するよう要求するものではあるが，公式の要求があった場合は議会に情報を提供するのがFTCの方針である。

日付＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Hugh G. Stevenson

消費者保護局，国際消費者保護部門，副部長

日付＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Consumer Sentinel ウェブサイトへのアクセスの申請書		
記載漏れがある場合，申請手続が遅れることがあります。お問い合わせは，Consumer Sentinel Support, sentinel@ftc.gov または（877）701-9595までご連絡ください。		
1A．申請者の名前（ラストネーム，ファーストネーム，ミドルネームのイニシャル）（印字）	2．誕生日（年／月／日）	4．ファックス番号
1B．申請者の肩書	3．電話番号	5．電子メールアドレス
6．機関名		8．ウェブブラウザ（名称とバージョン）
7．機関の所在国		8A．あなたのウェブブラウザは128ビット暗号化をサポートしていますか。はい＿＿いいえ＿＿
9．郵便先住所		10．組織コード（FTCによって記入される）
以下の証明書は申請を行う機関により記入すること。		
私は，承認された政府の目的のためにのみConsumer Sentinelを利用することを保証します。私は，認可されていないアクセスや開示を含む他のいかなる目的のための利用も，FTC法第10条及びConsumer Sentinel秘密保持協定への違反を構成しうることを了解します。		
11．申請者の署名		12．日付
13．認可担当者の署名／日付		14．認可担当者の名前（印字）
15．認可担当者の肩書		
ファックス番号：01＋（202）326-3392	郵便宛先：Consumer Sentinel Project Manager Federal Trade Commission 600 Pennsylvania Avenue, NW H-292 Washington, DC 20580	

FTCの使用欄			
16．消費者保護局の承認			17．日付
18．認証局	19．証明書	20．署名	21．日付

資料 3

IDENTITY THEFT
情報処理センター

Help Identity Theft 情報処理センター　DataMart

・少ない情報でも，たくさんの情報でも，入力して検索できます。１つのフィールドに最低１文字入力して検索してください。「%」をワイルドカードとして使用することができます(例 J%Doe で検索すると，Joe Doe という結果が得られる)。ワイルドカードは被疑者の会社名の１文字目としては使用できません。また，検索文字列の後ろには自動的に%が追加されます（例 MILLION で検索すると，MILLIONARES CLUB という結果が得られる。）

・注：要約検索で得られる検索結果は最大で1,000件までです。

レポートのタイプを選択　　作成された日（年／月／日）

質問数	○	始　期：	
要約検索	○	終　期：	

被疑者

名前［姓，名］			
住所：		市：	
州：		郵便番号：	
国名：			
電話番号：		E メール：	

消費者

名前［姓，名］		住所：	
市：			
州：		郵便番号：	
国名：			
SSN		誕生日（年／月／日）	～
ID Theft タイプ別		被害額	～
インターネット関連		法執行機関名	
事業体の名前		法執行機関州	
事業体の種類			
会社と問題あり			
言語		レポート番号	
参照番号			
組織			

検索実行　クリア

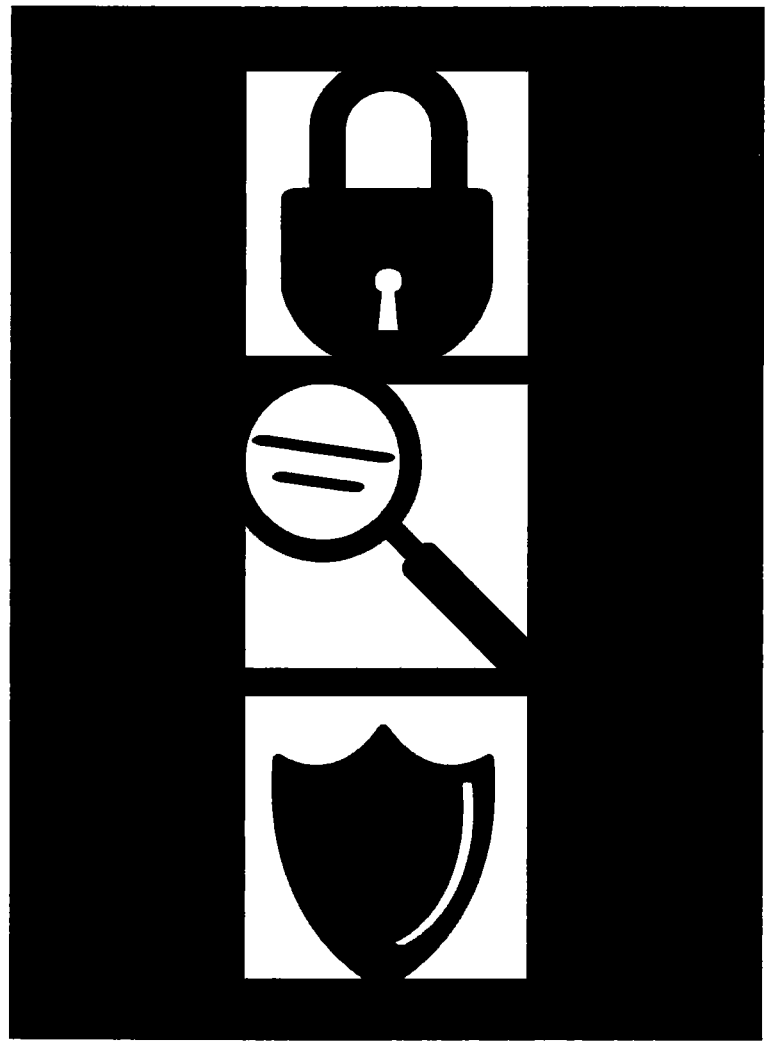
資料4

（パンフレット表紙）

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft



FIGHTING BACK AGAINST

IDENTITY THEFT

FEDERAL TRADE COMMISSION

（パンフレット内容）

ID Theft のよくある手口

巧妙な ID Theft 犯は，あなたの個人情報を盗むために様々な手口を使います。例えば……

1．**ごみばこ漁り**

彼らはごみをかき分けて，あなたの個人情報の載った請求書などの書類を捜します。

2．**スキミング**

彼らはあなたのクレジットカードやデビットカードを処理する際に特殊な記憶装置を使ってカード番号を盗みます。

3．**フィッシング**

彼らは金融機関や会社を装ってスパムメッセージやポップアップメッセージを送りつけ，あなたが自分の個人情報を明かすように仕向けます。

4．**あなたの住所を変更する**

彼らは「住所変更」用紙に記入することにより，請求明細書を別の場所に転送させます。

5．**「従来型の」盗み**

彼らは，財布，バンクカードやクレジットカードの明細書の入った郵便物，事前承認されたクレジットカードの提供書，新しい小切手，税金の情報を盗みます。彼らは雇用者から個人記録を盗み，標的に接近できる従業員を買収します。

阻止する

ID Theft は重大な犯罪です。それは，あなたの個人情報が盗まれ，知らないうちに利用され，詐欺その他の犯罪が行われるときに起こるのです。この犯罪は，あなたから時間とお金を奪い，あなたの信用と評判を台無しにするのです。

あなたの情報を守り，ID Theft 犯を阻止してください。

■個人情報の載った金融明細書や書類を捨てる前に**シュレッダーにかけて**ください。

■あなたの社会保障番号を**知られないようにして**ください。財布の中に社会保障カードを入れて持ち歩いたり，小切手に社会保障番号を記入したりしてはいけません。絶対必要な時にだけ使うようにし，他の方法で本人確認してもらいましょう。

■相手が誰であるかが分からない限り，電話，郵便，インターネットを通じて個人情報を**他人に明かさないで**ください。

■勝手に送られてきたＥメールに貼られているリンクを**決してクリックしないで**ください。自分の知っているウェブアドレスを打ち込むようにしてください。自宅のコンピュータを守るために，ファイアウォール，スパイウェア対策ソフト，ウイルス対策ソフトを利用し，常にアップデートしてください。さらに詳しい情報を知りたい方は，OnGuardOnline. gov を参照してください。

■自分の誕生日，母親の旧姓，自分の社会保障番号の下４桁などの，簡単に分かるパスワードを**使わな**

いでください。

■自分の個人情報を自宅内の安全な場所に**保管して**ください。ルームメイトがいたり，外部のヘルパーを雇っていたり，自宅内を仕事場にしている方は，特に要注意です。

見破る

自分の金融口座と請求明細書を日常的に点検し，疑わしい活動を見破ってください。

すぐに気づかなければならないサインに注意してください。

■届くはずの請求書が届かない。

■クレジットカードや預金取引の明細書が予想外の内容になっている。

■明白な理由がないのに信用取引を拒否される。

■したはずのない購入をめぐって電話や郵便物が来る。

以下のものを点検してください。

■自分の信用報告書

信用報告書には，あなたが所有する口座やあなたの請求書支払の履歴など，あなたに関する情報が記載されています。

□主要な全国規模の信用調査会社－Equifax，Experian，TransUnion－は，あなたが要望すれば，信用報告書のコピーを，毎年，無料で，あなたに交付することを法律によって義務づけられています。

□自分の無料の信用報告書を毎年注文する場合は，www.AnnualCreditReport.com を参照するか，1-877-322-8228に電話してみてください。これは上記の３つの会社が新設したサービスです。以下の宛先に郵送で請求することもできます。

Annual Credit Report Request Service,

P.O. Box 105281, Atlanta, GA 30348-5281

■自分の金融明細書

金融口座と請求明細書を定期的に見直し，身におぼえのない請求がないか調べてください。

防御する

ID Theft の疑いがある場合は，直ちに防御策を講じてください。

■自分の信用報告書に「詐欺警告」を載せ，報告書を注意深く見直してください。

この警告は債権者に対し，彼らがあなたの名義で新しいアカウントを開設したりあなたの現在のアカウントを変更したりする前に，一定の手続に従うよう通告するものです。全国規模の３つの信用調査会社が，最初の90日間の詐欺警告を載せるための無料電話番号を設けています。どれか１つの会社に電話すれば十分です。

□ Equifax：1-800-525-6285

□ Experian：1-888-EXPERIAN（397-3742）

□ TransUnion：1-800-680-7289

詐欺警告を載せると，あなたは自分の信用報告書のコピーを無料で入手できます。あなたが接触したことのない会社からの照会，あなたが開設したのではないアカウント，あなたのアカウントに記載

された説明できない負債，これらのものがないか調べてください。

■アカウントを閉鎖してください。

不正に変更されたり開設されたりした全てのアカウントを閉鎖してください。

□あなたの承諾なしにアカウントの開設や変更がなされた場合は，各会社のセキュリティまたは詐欺の部門に電話してください。次いで，証拠資料のコピーと合わせて書面で報告してください。

□書面での報告には，ftc.gov/idtheft で入手できる「ID Theft 宣誓供述書」を利用してください。

□問題のアカウントが閉鎖され，不正な債務が取消されたことを確認するよう依頼してください。

□ ID Theft に関する資料のコピーとあなたの会話記録は保存しておいてください。

■警察に被害届出してください。

捜査当局者に被害届をしてください。あなたが債権者から，犯罪被害に遭ったことを証明するよう求められたときに役に立ちます。

■連邦商取引委員会（FTC）に報告してください。

あなたの報告は捜査活動に従事する全国の捜査当局者にとって役立ちます。

□インターネット：ftc.gov/idtheft

□電話番号：1-877-ID-THEFT（438-4338）または TTY，1-866-653-4261

□郵便宛先：Identity Theft Clearinghouse,
Federal Trade Commission, Washington, DC 20580

資料5

名前____________________電話番号____________________ページ1

ID Theft 宣誓供述書

被害者の情報

(1) 私の氏名は__________________________________です。

（ファースト）　（ミドル）　（ラスト）　(Jr., Sr., III)

(2) (上記と異なる場合)本供述書に記された事件が起きた時には，私は以下の氏名で知られていました。

____

（ファースト）　（ミドル）　（ラスト）　(Jr., Sr., III)

(3) 私の誕生日は_______________です。

（年／月／日）

(4) 私の社会保障番号は_______________です。

(5) 私の運転免許証と身分証明書の州及び番号は___________________です。

(6) 私の現住所は____

市__________州____________郵便番号___________です。

(7) 私は上記の住所に______________から住んでいます。

（年／月）

(8) (上記と異なる場合) 本供述書に記された事件が起きた時には，私の住所は以下のとおりでした。

____

市__________州____________郵便番号___________

(9) 私は(8)の住所に____________から____________まで住んでいました。

（年／月）　（年／月）

(10) 私の昼間の電話番号は(　　)________________です。

私の夜間の電話番号は(　　)________________です。

宣誓供述書はFTCその他のいかなる政府機関にも送付しないでください。

名前____________________電話番号____________________ページ2

どのようにして詐欺が起きたか

(11)～(16)のうち該当する全ての項目をチェックしてください。

(11)□私は本供述書に記されている金銭，クレジット，融資，商品，またはサービスを得るために私の名前や個人情報を利用する許可を誰にも与えませんでした。

(12)□私は本供述書に記されている事件の結果として，いかなる利益，金銭，商品，またはサービスも受け取りませんでした。

(13)□私の身分証明書（クレジットカード，出生証明書，運転免許証，社会保障カード等）は

______________（頃）に　□盗まれました　　□なくなりました。

（年／月／日）

(14)□私の知りかつ信じる限り，以下の人（々）は，金銭，クレジット，融資，商品，またはサービスを得るために，私に断りなく，または私の許可なく，私の情報（たとえば，私の名前，住所，誕生日，現在のアカウント番号，社会保障番号，母親の旧姓等）または身分証明書を利用しました。

______________________	______________________
名前（知っている場合）	名前（知っている場合）
______________________	______________________
住所（知っている場合）	住所（知っている場合）
______________________	______________________
電話番号（知っている場合）	電話番号（知っている場合）
______________________	______________________
追加情報（知っている場合）	追加情報（知っている場合）

(15)□私は，金銭，クレジット，融資，商品，またはサービスを得るために，私に断りなく，または私の許可なく，私の情報または身分証明書を利用したのが誰であるかを知りません。

(16)□追加的コメント：（たとえば，詐欺の内容，どの情報や身分証明書が利用されたか，または ID Theft 犯がどうやってあなたの情報を知り得たのか。）

____

____

____

____

（必要ならページを追加添付してください。）

宣誓供述書は FTC その他のいかなる政府機関にも送付しないでください。

名前______________________電話番号______________________ページ 3

被害者の法執行活動

(17)（１つをチェックしてください）私はこの詐欺を犯した人（々）の訴追に

□進んで協力したい　　□あまり協力したくない。

(18)（１つをチェックしてください）私はこの詐欺を犯した人（々）の捜査と訴追を行う法執行当局者を助けるために，この情報を法執行当局者に開示することを

□許可するつもりである　　□許可するつもりはない。

(19)（該当するもの全てをチェックしてください）私は本供述書に記された事件を警察その他の法執行機関に　□報告した，□報告していない。警察は，報告書（被害届）を　□作成した，□作成しなかった。あなたが警察またはその他の法執行機関に連絡を取った場合は，以下に記入してください。

______________	______________________
（機関#１）	（報告書・被害届を作成した警察官／担当職員）

(報告日)	(報告書・被害届の番号（わかる場合))
(電話番号)	(E メールアドレス（わかる場合))
(機関# 2)	(報告書・被害届を作成した警察官／担当職員)
(報告日)	(調書番号（わかる場合))
(電話番号)	(E メールアドレス（わかる場合))

証拠資料のチェックリスト

あなたが通知しようと考えている会社に提出できる証拠資料を明らかにしてください。会社にそれを送付する前に，本供述書にその（現物ではなく）コピーを添付してください。

⑳□有効な政府発行の写真付き身分証明書(たとえば，あなたの運転免許証，州発行の ID カード，またはあなたのパスポート）のコピー。あなたが16歳未満で，写真付き身分証明書を持っていない場合は，あなたの出生証明書のコピー，またはあなたの登録事実と住所が分かる正式な学校記録のコピーを提出することもできます。

㉑□問題となった請求書が発生し，融資が行われ，またはその他の事件が起きた時期の住居を証明するもの（たとえば，あなたの名義での賃貸借契約書，公共料金支払書のコピー，または保険証書のコピー)。

名前＿＿＿＿＿＿＿＿＿＿＿＿＿＿電話番号＿＿＿＿＿＿＿＿＿＿＿＿＿＿ページ 4

㉒□あなたが警察または保安官事務所に提出した被害届のコピー。コピーや被害届（報告書）の番号を警察から入手できない場合は，⑲にその旨を記してください。一部の会社は，被害届等の番号だけ判ればよいのです。あなたはその点について各会社に確認することができます。

署名

私の知りかつ信じる限り，私は，本供述書に記載され添付された全ての情報が真実であり，正しく，完全であり，また誠意を持って記入されたことを保証します。私はまた，本供述書またはそれに含まれる情報が，連邦，州，及び／または地方の法執行機関に対し，彼らがその管轄区内で適当と見なす措置のために利用される場合があることを了解します。私は，政府に対して虚偽または不正の供述や説明を故意に行った場合は，18 U.S.C. §1001またはその他の連邦，州，若しくは地方の刑法違反になりうること，またその結果として罰金若しくは懲役またはそれらの併科に処せられうることを了解します。

(署名)	(日付)

（公証人）

［各会社について内容をチェックしてください。債権者は時々公証を要求することがあります。彼らがそれを要求しない場合は，あなたが本供述書に記入し署名したことの証しとして，１人の証人（親戚以外の人）が以下に署名を行ってください。］

証人：

（署名）　（印字での名前）

（日付）　（電話番号）

宣誓供述書はFTCその他のいかなる政府機関にも送付しないでください。

名前＿＿＿＿＿＿＿＿＿＿電話番号＿＿＿＿＿＿＿＿＿＿ページ5

不正アカウント明細書

本明細書を仕上げるに当たって

●このページを必要なだけコピーしてください。**あなたが通知しようとする各会社について別個のコピーを使って完全に記入し，それらは各々対応する会社だけに送付してください。**あなたの署名入りの宣誓供述書のコピーも１部同封してください。

●この明細書を受け取る会社との間で問題になっているアカウントだけをリストアップしてください。**下記の例を参照してください。**

●取立代理会社がその不正アカウントに関する明細書，証書，または通知をあなたに送付してきた場合は，その文書の（現物**ではなく**）コピーを添付してください。

（該当する項目を全てチェックしてください）私は，

□ ID Theft 宣誓供述書に記された事件の結果として，私に断りなく，または私の許可もしくは認可なく，私の個人情報または身分証明書を利用して，私の名義で，以下のアカウントが開設されたことを申告します。

債権者の名称／住所（アカウントを開設した，または商品やサービスを提供した会社）	**アカウント番号**	**債権者によって提供された許可されていないクレジット／商品／サービスの種類**（知っている場合）	**発行または開設された日付**（知っている場合）	**提供された金額／価格**（請求された金額，または商品／サービスの代価）
（例） Example National Bank 22 Main Street Columbus, Ohio 22722	012345 67-89	自動車ローン	2002年5月1日	$25,500.00

□上記アカウントが存在した間，私は貴社に以下のアカウントを開設していました。

請求先名称＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

請求先住所＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

アカウント番号＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

宣誓供述書はFTCその他のいかなる政府機関にも送付しないでください。

ID Theft宣誓供述書の作成に当たっての説明

ID Theft犯によって被った負債の責任を負わないためには，あなたの名義でアカウントが開設されたり利用されたりした各会社に対し，負債を作ったのはあなたではないことを証明しなければなりません。

与信者，消費者保護団体，及び連邦商取引委員会（FTC）は，共同で，詐欺の被害者がもっと簡単に被害に被害申告できるようにと考え，ID Theft宣誓供述書を作りました。多くの会社がこの供述書を受け入れていますが，追加的な書類や異なる形式の書類を提出するよう要求する会社もあります。この供述書を送付する前に，各会社と連絡を取って，彼らがこの供述書を受け入れるかどうかを確認してください。

この供述書に含まれる情報は，あなたの名義で**新しい**アカウントが開設された全ての会社に提供する必要があるでしょう。それらの情報のおかげで，会社は詐欺に関する調査を行い，あなたの主張について決定を下すことが可能になるでしょう。また，誰かが**既存の**アカウントに権限なく請求を行った場合は，会社に電話して説明を求めてください。

この宣誓供述書は2つの部分から出来ています。

- **第1部**－ID Theft宣誓供述書－は，あなたが自分自身と窃盗に関する一般的な情報を報告する箇所です。
- **第2部**－不正アカウント明細書－は，あなたの名義で開設された不正なアカウントについて説明する箇所です。通知する必要のある会社ごとに別個の不正アカウント明細書を使用してください。

この宣誓供述書を会社に送付する際には，全ての証拠資料（たとえば運転免許証や警察への被害届）の（**現物ではなく**）コピーを添付してください。あなたの供述書を提出する前に，家族や友人と一緒に，問題になったアカウントを見直し，何か関係する情報を知らないか確かめてください。

この供述書はできるだけ早く仕上げてください。多くの債権者は供述書を2週間以内に送付するよう頼んできます。あなたの側でのもたつきが，調査の進行を遅らせることになるかもしれません。

できる限り正確かつ完全なものに仕上げてください。あなたは要求されている情報の一部を提供しないという選択もできます。しかし，不正確で不完全な情報は，あなたの主張に関する調査と債務取消のプロセスを遅らせることになるでしょう。印刷は鮮明になるように行ってください。

供述書を記入し終えたら，あなたが記した，クレジット，商品，またはサービスを犯人に提供した各債権者，銀行，会社のそれぞれに，コピーを1通ずつ郵送してください。送付先ごとに，関係する不正アカウント明細書のコピーも1部添付し，同時にあなたが提供できる他の全ての証拠書類も同封してください。

相手が受領したことをあなたが証明できるよう，受領通知のある配達証明付き郵便で，適切な書類を

送付してください。会社側はあなたの主張について検討し，彼らの調査結果を告げる書面をあなたに送ってくるでしょう。あなたが提出した書類は全てコピーを保存しておいてください。

あなたがこの供述書を作成できない場合は，法定後見人や代理権を持つ誰かに代わりに作ってもらうこともできます。注記されている場合を除き，あなたが提出した情報は，あなたの宣誓供述書を処理し，あなたが報告した事象について調査し，それ以上の詐欺の発生を食い止めることに役立てる目的のためにのみ，会社側で利用されることになるでしょう。この供述書が訴訟の中で請求された場合は，会社はそれを請求した当事者に提供しなければならないかもしれません。この供述書を作成したからといって，ID Theft の犯人が訴追され，あるいは負債が取消されることが保証されるわけではありません。

宣誓供述書は FTC その他のいかなる政府機関にも送付しないでください。

あなたが詐欺の被害を以下の組織に対してまだ申告していないのなら，……

1．あなたの信用報告書に詐欺警告を載せるために，次のいずれかの信用調査会社に連絡してください。

詐欺警告は，ID Theft 犯があなたの名義でこれ以上アカウントを開設するのを阻止する上で役立ちます。あなたが連絡した会社は，他の 2 社に連絡することを義務づけられており，それらの会社でもあなたの信用報告書に警告を載せる措置をとるでしょう。

- Equifax：1-800-525-6285
  www.equifax.com
- Experian：1-888-EXPERIAN
  (397-3742)；www.experian.com
- TransUnion：1-800-680-7289
  www.transunion.com

詐欺警告の掲載に加えて，これら 3 社は，あなたの信用報告書の無料コピーをくれます。また，あなたが要請すれば，あなたの信用報告書には社会保障番号の下 4 桁だけしか表示されないようにできます。

2．そこでのアカウントが不正に変更または開設されたことをあなたが知っている，またはそのように信じている各会社のセキュリティもしくは詐欺の部門に連絡してください。

そして，アカウントを閉鎖してください。さらに，書面を作成し，証拠書類の(**現物ではなく**)コピーを同封して送ってください。クレジットカード会社と銀行に書面で通知することは重要です。会社側がいつ，何を受領したかをあなたが文書で証明できるよう，関連書類は，受領通知のある配達証明付き郵便で送付してください。あなたが送付した書類及び同封物のファイルは保存しておいてください。

あなたが新規にアカウントを開設する際には，新しい個人識別番号とパスワードを使用してください。母親の旧姓，あなたの誕生日，あなたの社会保障番号や電話番号や同種の通し番号の下 4 桁など，簡単にわかる情報を利用するのは避けてください。

3．あなたの地元の警察か，またはID Theftが起きた地域の警察に被害届をして下さい。

被害届のコピーか，または少なくとも被害届番号を入手してください。それはあなたが債権者に対して，犯罪被害に遭ったことを証明する上で役立ちます。もし，警察が被害届の受理に消極的であれば，「雑事件」報告として受理してくれるよう依頼するか，または州警察など別の管区に当たってみてください。あなたの州の検察庁で，州法が警察にID Theftの被害届受理を義務付けているかどうかを調べることもできます。電話番号は電話帳の官公庁の部で，州検察庁のリストはwww.naag.orgで調べてみてください。

4．連邦商取引委員会（FTC）に報告してください。

ID Theftに関する苦情をFTCと共有することにより，あなたは重要な情報を提供することになり，その情報は法執行当局者が全国でID Theft犯を探し出し，犯行を阻止する上で役立ちます。FTCはまた，追加的措置のため被害者の苦情内容を他の政府機関や会社側に参照させることもでき，FTCが監視している法律違反に関して会社を調査することもできます。

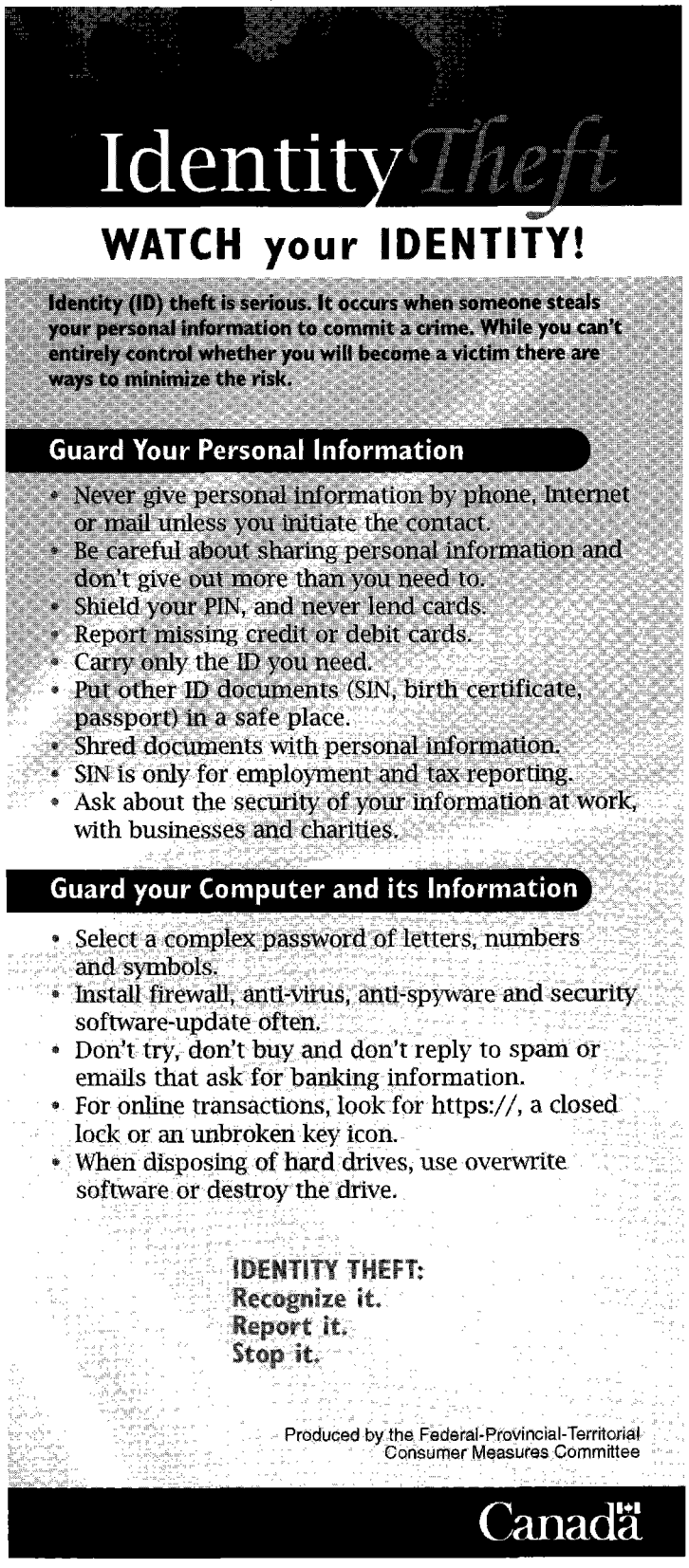
苦情の申告は，オンラインwww.consumer.gov/idtheftからできます。インターネットが使えない場合は，無料のFTC ID Theftホットライン：1-877-IDTHEFT（438-4338）；TTY：1-866-653-4261に電話するか，または以下の宛先に書状を送ってください。

Identity Theft Clearinghouse, Federal Trade Commission,
600 Pennsylvania Avenue, NW, Washington, DC 20580.

宣誓供述書はFTCその他のいかなる政府機関にも送付しないでください。

資料 6

（パンフレット表）



Identity Theft

WATCH your IDENTITY!

Identity (ID) theft is serious. It occurs when someone steals your personal information to commit a crime. While you can't entirely control whether you will become a victim there are ways to minimize the risk.

Guard Your Personal Information

- Never give personal information by phone, Internet or mail unless you initiate the contact.
- Be careful about sharing personal information and don't give out more than you need to.
- Shield your PIN, and never lend cards.
- Report missing credit or debit cards.
- Carry only the ID you need.
- Put other ID documents (SIN, birth certificate, passport) in a safe place.
- Shred documents with personal information.
- SIN is only for employment and tax reporting.
- Ask about the security of your information at work, with businesses and charities.

Guard your Computer and its Information

- Select a complex password of letters, numbers and symbols.
- Install firewall, anti-virus, anti-spyware and security software-update often.
- Don't try, don't buy and don't reply to spam or emails that ask for banking information.
- For online transactions, look for https://, a closed lock or an unbroken key icon.
- When disposing of hard drives, use overwrite software or destroy the drive.

IDENTITY THEFT:
Recognize it.
Report it.
Stop it.

Produced by the Federal-Provincial-Territorial Consumer Measures Committee

Canada

(パンフレット表)

Identity Theft
あなたのIDに注意!

ID Theftは深刻な問題です。それは，誰かが犯罪を実行するためにあなたの個人情報を盗み出すときに起こります。あなたが被害者にならないよう状況を完全にコントロールすることはできませんが，リスクを最小限に抑える方法はあります。

あなたの個人情報を守ってください

●あなたから連絡したのではないのなら，電話，インターネット，郵便で他人に個人情報を知らせてはいけません。
●個人情報の共有には注意を払い，必要以上に他人に明かさないでください。
●暗証番号は秘密にし，IDカードは決して他人に貸さないでください。
●クレジットカードやデビットカードを紛失した場合は報告してください。
●必要とするIDだけを携行するようにしてください。
●その他のID文書（社会保険番号，誕生日，パスポート）を安全な場所にしまってください。
●個人情報の載った書類はシュレッダーにかけてください。
●社会保険番号は就職と税の申告のためにのみ用いてください。
●商業活動や慈善事業を伴う仕事場でのあなたの情報のセキュリティについて調べてみてください。

あなたのコンピュータとその情報を守ってください

●パスワードは，文字，数字，記号を用いた複雑なものを選んでください。
●ファイアウォール，ウイルス対策ソフト，スパイウェア対策ソフトをインストールし，セキュリティソフトの更新を頻繁に行ってください。
●スパムメールや銀行情報について尋ねてくるEメールに対しては，試したり購入したり返答したりしないでください。
●オンライン取引を行う場合は，閉鎖したロックや破られないキーを意味するhttps://の表示を探してください。
●ハードドライブを処分する際は，上書きソフトを使うか，ドライブを破壊してください。

IDENTITY THEFT：
この犯罪を理解し，
報告し，
阻止してください。

連邦・州・準州の消費者対策委員会による作成

（パンフレット裏）

Identity Theft

ARE YOU a VICTIM?

With your identity, thieves can open new bank accounts, order cell phones, take out a mortgage on your property and buy cars or furniture.

Signs of ID Theft

- Purchases not made by you appear on your monthly bills.
- Bills arrive on accounts you don't own.
- Collection agency calls about unknown debt.
- Credit card/bank statements don't arrive.
- Your credit report shows mystery debts.

What to Do

- ✔ Call financial institutions and local police.
- ✔ Put a fraud alert on your credit report by contacting
  Equifax: 1-800-465-7166 and
  Trans Union: 1-877-525-3823
  (Quebec residents: 1-877-713-3393).
- ✔ To replace ID cards like health, driver's licence, SIN call 1 800 O-Canada
- ✔ Contact Canada Post if your mail is missing.
- ✔ Keep records of steps taken to clear your name and re-establish your credit.
- ✔ Help stop fraud. Contact PhoneBusters at 1-888-495-8501 or phonebusters.com

For more information on Identity Theft visit

www.ConsumerInformation.ca

Cat. No. lu23-5/2006E
ISBN 0-662-42652-5
54405E

PHONEBUSTERS™
The Canadian Anti-fraud Call Centre

Canada

(パンフレット裏)

Identity Theft
あなたは被害者ですか？

あなたのIDを悪用して，犯人たちは新規の銀行口座を開設し，携帯電話を購入し，あなたの財産に抵当権を設定し，自動車や家具を購入してしまうのです。

ID Theftのサイン

●毎月の請求書に，したはずのない購入が記載されている。
●あなたが持っていないアカウントに関する請求書が届く。
●取立代理会社から，自分の知らない債務の取り立てがある。
●クレジットカード／銀行の明細書が届かない。
●あなたの信用報告書に不可解な負債が記載されている。

何をすべきか

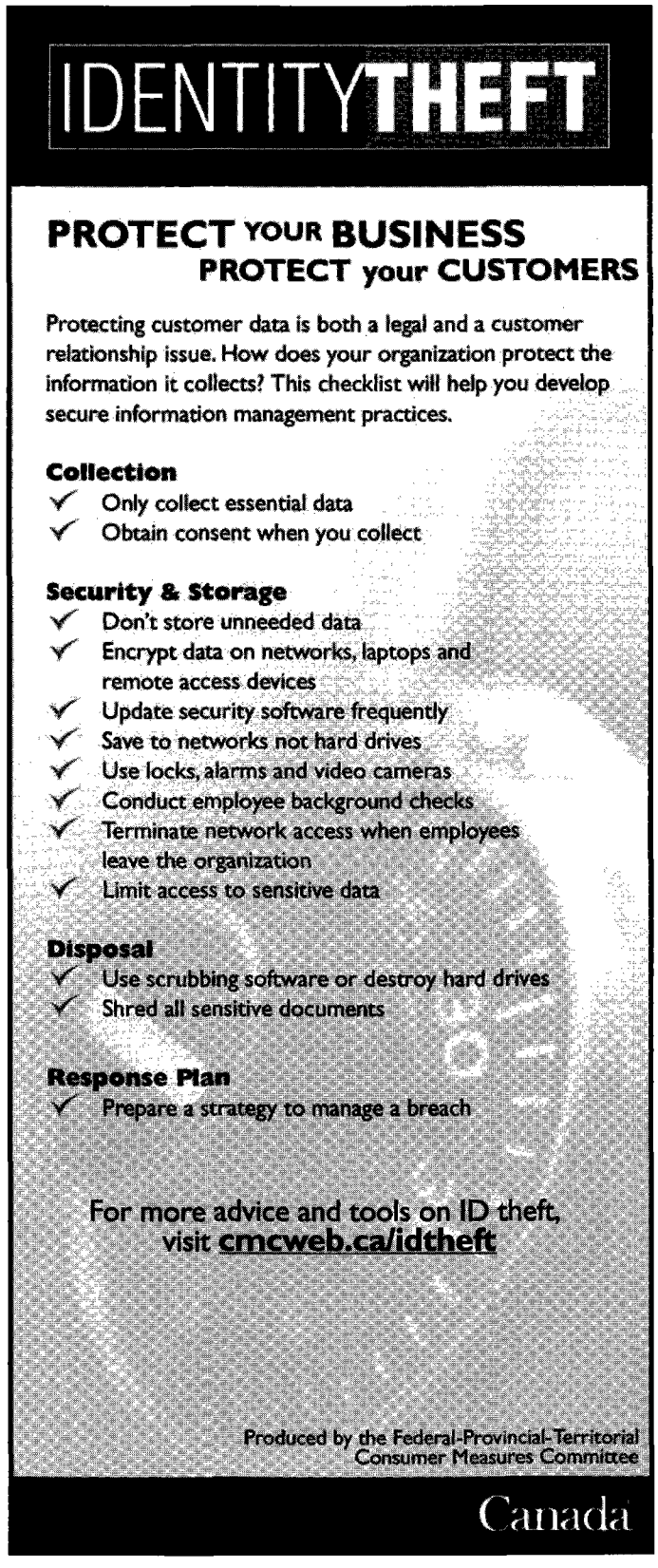
✓金融機関と地元の警察に連絡してください。
✓以下に連絡してあなたの信用報告書に詐欺警告を載せてください。
Equifax：1-800-465-7166
TransUnion：1-877-525-3823
(ケベック在住者の場合：1-877-713-3393)
✓健康保険証，運転免許証，社会保険番号などの身分証明書を取り替えるため，1 800 O-Canadaに電話してください。
✓あなたの郵便物の行方が分からないときには，カナダ郵政省に連絡してください。
✓あなたの名義をはっきりさせ，信用を回復させるために取った措置を記録し保管してください。
✓詐欺を阻止する活動に協力してください。フォンバスターズ－1-888-495-8501またはphonebusters.com－にご連絡ください。

ID Theftについてさらに詳しい情報を知りたい方は，www. ConsumerInformation. caをご覧ください。

フォンバスターズ
カナダ詐欺対策コールセンター

資料 7

（パンフレット表）


IDENTITYTHEFT
PROTECT YOUR BUSINESS
PROTECT your CUSTOMERS
Protecting customer data is both a legal and a customer relationship issue. How does your organization protect the information it collects? This checklist will help you develop secure information management practices.
Collection
Only collect essential data
Obtain consent when you collect
Security & Storage
Don't store unneeded data
Encrypt data on networks, laptops and remote access devices
Update security software frequently
Save to networks not hard drives
Use locks, alarms and video cameras
Conduct employee background checks
Terminate network access when employees leave the organization
Limit access to sensitive data
Disposal
Use scrubbing software or destroy hard drives
Shred all sensitive documents
Response Plan
Prepare a strategy to manage a breach
For more advice and tools on ID theft, visit cmcweb.ca/idtheft
Produced by the Federal-Provincial-Territorial Consumer Measures Committee
Canada

(パンフレット表)

IDENTITY THEFT

あなたのビジネスを守ってください
あなたの顧客を守ってください

顧客のデータを守ることは，法的な問題であると同時に，顧客との関係に関わる問題でもあります。あなたの会社は収集した情報をどのように保護していますか。このチェックリストは，あなたが安全な情報管理習慣を身につける上で役立つでしょう。

収集

√必要不可欠なデータだけを収集してください。
√収集する際に本人の同意を得てください。

セキュリティと保管

√不必要なデータを保管しないでください。
√ネットワーク，ラップトップ，及びリモート・アクセス装置上にあるデータを暗号化してください。
√セキュリティソフトを頻繁に更新してください。
√ハードドライブにではなくネットワークに保存してください。
√ロック，警報器，ビデオカメラを利用してください。
√従業員の身元調査を行ってください。
√従業員が会社の外に出る際にはネットワークへのアクセスを終了してください。
√機密データへのアクセスを制限してください。

処分

√除去ソフトを使うか，ハードドライブを破壊してください。
√全ての機密文書をシュレッダーにかけてください。

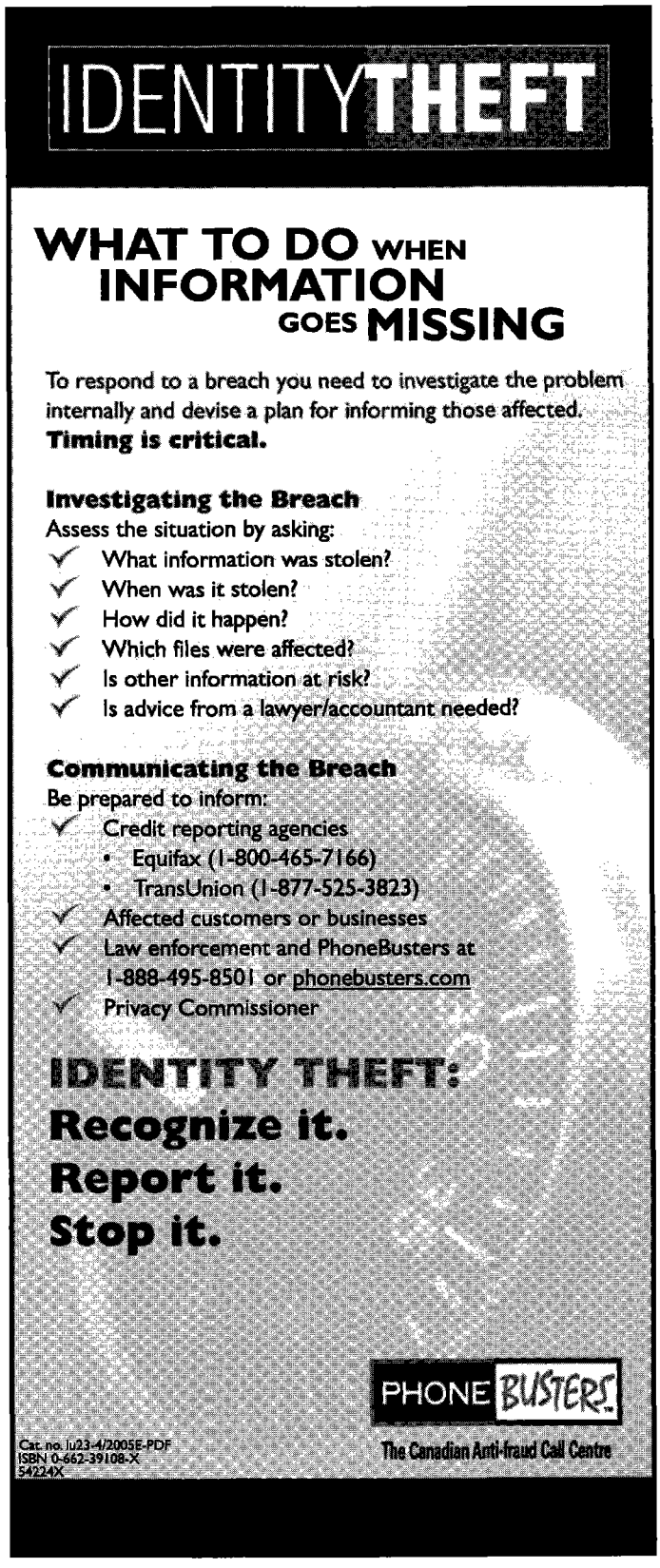
対策計画

√情報が盗まれた時に備えて，戦略を立ててください。

ID Theft に関する追加的なアドバイスとツールについては，cmcweb.ca/idtheft をご覧ください。

連邦・州・準州の消費者対策委員会による作成

(パンフレット裏)



IDENTITY THEFT

WHAT TO DO WHEN INFORMATION GOES MISSING

To respond to a breach you need to investigate the problem internally and devise a plan for informing those affected. **Timing is critical.**

Investigating the Breach

Assess the situation by asking:

- ✓ What information was stolen?
- ✓ When was it stolen?
- ✓ How did it happen?
- ✓ Which files were affected?
- ✓ Is other information at risk?
- ✓ Is advice from a lawyer/accountant needed?

Communicating the Breach

Be prepared to inform:

- ✓ Credit reporting agencies
  - Equifax (1-800-465-7166)
  - TransUnion (1-877-525-3823)
- ✓ Affected customers or businesses
- ✓ Law enforcement and PhoneBusters at 1-888-495-8501 or phonebusters.com
- ✓ Privacy Commissioner

IDENTITY THEFT:
Recognize it.
Report it.
Stop it.

PHONE BUSTERS!
The Canadian Anti-fraud Call Centre

Cat. no. Iu23-4/2005E-PDF
ISBN 0-662-39108-X
54224X

（パンフレット裏）

IDENTITY THEFT

情報が盗まれたら，どうするべきか

情報が盗まれる事件が起きたら，内部調査を行い，影響を受ける人々への通知について計画を立てる必要があります。**時機を逸さず行動することがきわめて重要です。**

事件調査

以下の点を調べることにより，状況を評価してください。

√どんな情報が盗まれたか。
√いつ盗まれたか。
√それはどのようにして起きたか。
√どのファイルが影響を受けたか。
√他の情報は危険にさらされているか。
√弁護士や会計士のアドバイスが必要か。

事件の通知

以下の組織や人々に通知する準備を行ってください。

√信用調査会社
- Equifax（1-800-465-7166）
- TransUnion（1-877-525-3823）

√影響を受ける顧客や企業
√法執行機関とフォンバスターズ－1-888-495-8501または phonebusters.com
√プライバシー監督官（Privacy Commissioner）

IDENTITY THEFT：
この犯罪を理解し，
報告し，
阻止してください。

フォンバスターズ
カナダ詐欺対策コールセンター

法務総合研究所研究部報告　36

平成19年3月印刷
平成19年3月発行

東京都千代田区霞が関1－1－1
編集兼
発行人　法務総合研究所
印刷所　ヨシダ印刷両国工場