個人識別情報の不正取得・不正使用に対する刑事訴追

堀　田　周　吾

一　はじめに

2008年６月に東京で開催されたＧ８司法・内務大臣会議は，国際テロ対策や国際組織犯罪対策といった主要テーマと並んで，「ID犯罪（ID-related crime）」を議題として取り上げた。同会議の総括宣言によれば，ID犯罪とは身元の悪用にかかる不法な行為一般を広く指し，具体的には，個人識別文書／個人識別情報（以下，総じて「ID」という）の偽造・変造のほか，これらIDの不正取得，移転，所持，使用などの行為が含まれるとされる。そして，このようなID犯罪について，「緊急の全世界的課題（pressing global issue）」であるとした上で，各国政府の対応および国際的連携の必要性が説かれている(1)。

国際的には，ID犯罪またはID盗取（identity theft）が一つの犯罪事象として問題視されるようになってから久しい。アメリカ合衆国では1998年に「ID盗取・濫用防止法（Identity Theft and Assumption Deterrence Act）」が連邦法として成立した。欧州諸国においても，1995年の欧州委員会による「データ保護指令（Data Privacy Directive）」に基づき，イギリスが1998年に「データ保護法（Data Protection Act）(2)」を改正するなど，各国が対策を進めている。このような動きを受けて，国連でも2004年の経済社会理事会による決議に基づき，「詐欺及びIDの犯罪的悪用・偽造」について研究を行う専門家会合が

犯罪防止刑事司法委員会に設置された。

わが国もID犯罪と無関係ではない。例えば，近年問題となっている振り込め詐欺は，家族等の身元を偽ったり，他人名義の銀行口座に入金させたりする点で，まさに他人のIDを悪用して行う詐欺行為であるといえる。また，クレジットカード情報を機械で不正に読み取るいわゆるスキミングも，IDの不正取得行為にほかならない。

しかし，それらID犯罪への対策は十分とはいえない。平成15年に個人情報保護法制が整備され，個人情報取扱事業者や行政機関による個人情報の利用について一定の規制がされるようになったことは，ID犯罪の予防策の一環として評価できよう。他方で，刑事上は，他人のカード情報を用いてクレジットカードを偽造する行為(3)や，他人名義のクレジットカードを利用する行為(4)などの部分的な処罰にとどまっているのである。

本稿は，ID犯罪の処罰立法を早期に整えたアメリカ合衆国の状況を概観するとともに，わが国における対応の現状および今後のあり方について若干の考察を加えるものである(5)。

---

(1)　全文（仮訳および英文）は「総括宣言全文」ひろば61巻10号58頁（2008年）を参照。同会議の概要について，宇川春彦「Ｇ８司法・内務大臣会議の東京開催」ひろば61巻10号４頁（2008年）参照。

(2)　詳細については，岡田安功「イギリスの1998年データ保護法」クレジット研究21号156頁以下（1999年），木村光江＝星周一郎「イギリスのデータ保護法の概要とその運用状況――刑事規制を中心に」クレジット研究27号259頁以下（2002年）参照。

(3)　支払用カード電磁的記録不正作出罪（刑法163条の２）。

(4)　クレジットカードの名義人になりすまし同カードを利用して商品を購入する行為が詐欺罪にあたるとした最決平成16年２月９日（刑集58巻２号89頁），窃取したクレジットカードの名義人氏名等を冒用してこれらをクレジットカード決済代行業者の使用する電子計算機に入力送信して電子マネーの利用権を取得した行為が電子計算機使用詐欺罪にあたるとした最決平成18年２月14日（刑集60巻２号165頁）など。

(5)　本テーマに関連する主な文献として，吉田和彦「個人情報の不正取得等に係るサイバー犯罪等の現状と対策について」警論58巻11号135頁（2005年），太田玲子＝池田暁子＝姫田卓朗「個人情報に関連する犯罪に関する研究」法務総合研究所研究部報告36号（2007年），中川かおり「米国における個人情報保護の動向――個人情報窃盗対策を中心に――」外法231号59頁以下（2007年），宇川・前掲注(1)８頁以下，前田雅英＝堀田周吾「個人識別情報の刑事的保護――『ID犯罪』の現状――」ひ

ろば61巻10号15頁以下（2008年）参照。

二　ID犯罪の概要

1　定義

他人のIDを悪用して行われる犯罪は従来から存在するが，それが固有の犯罪類型として認識されるようになったのは，インターネットが広く普及した1990年代後半のことである。IDの悪用（identity abuse）を伴う犯罪を広く意味する用語として「ID盗取（identity theft）」が使われてきたが，IDの悪用は財産的利益の取得を目的とした場合に限られないので，「ID盗取」の語が問題状況の全てを端的に表しているとはいえない。

用語の問題について，国連の犯罪防止刑事司法委員会に設置された専門家会合が2007年に提出した報告書は，次のように整理している(6)。

すなわち，「ID盗取」とは，窃盗・詐欺等の方法により真正な他人名義のIDが取得された場合を指す。具体的には，有形の文書や無形の情報の盗取，放棄されたまたは自由に利用可能な文書・情報の取得，個人を騙して任意に文書・情報を提供させるような場合が含まれるとされている。また，「ID詐欺（identity fraud）」とは，他の犯罪を実行するためもしくは発見と訴追を免れるためにIDを使用する場合を指す(7)。

そして，これらID盗取・ID詐欺のほか，IDに関わるあらゆる形態の違法行為を表すものとして「ID犯罪（identity crime）」の用語が使われている(8)。2008年に東京で開催されたG８司法・内務大臣会議でも同様の語を用いていることは，冒頭で述べたとおりである(9)。

このように，「ID犯罪」は幅広い態様の犯罪行為を包含する概念だが，他人のIDを何らかの不正な目的で使用することに向けられるという共通点を有している。そして，その準備的・補助的段階として，IDを不正に取得したり偽造・変造したりする行為が存在するのである。

2　IDの不正取得

IDの不正取得には，ID情報が化体された有形の文書等を領得する場合と，無形のID情報そのものを取得する場合とがある。前者は，例えば，郵便物の窃取やゴミ箱漁り（dumpster diving）といった単純な手段によるものである(10)。後者は，いわゆるハイテク犯罪の類型である。中でも，クレジットカードやデビットカードに化体された磁気情報をスキマーと呼ばれる装置で不正に読み取るスキミング（skimming）の手法は，対面販売の場で行われる最も容易なID入手の手段の一つである(11)。しかし，それを除けば，この類型の大半はサイバー犯罪ないしはネットワーク利用犯罪としての性質を併せ持つのである。

・サイバー犯罪としてのID犯罪

無形のID情報の多くはコンピュータデータとして存在する。そして，それらデータは，個人等のコンピュータにユーザー自身の手によって保存されるだけでなく，クッキー（Cookie）などの技術の発達により，インターネットを利用する過程でユーザーの意思に関係なく，当該端末に自動的に保存されたり，ネットワークサービスの提供者によって自動的に収集されたりする(12)。ユーザーが認識し得ない形でID情報がネットワーク上に流出する可能性があるのが現在のサイバー社会の実情であり，それに乗じる形で，不正にID情報が取得されてしまう危険が存在するのである。次のような手口が問題となっている。

第一は，ハッキング／クラッキング(13)によって公共機関や企業等の保有するデータベースや内部ネットワークからID情報を取得する方法である。具体的には，データの転送時（例えばクレジットカードの加盟店が顧客のカード情報を端末機器を通じて送信する場合）にこれを傍受したり，インターネット上の商品検索などに使われるアプリケーションへ不正にアクセスしたりするのである(14)。

第二は，スパイウェア（spyware）やキーロガー（key logger）などのマルウェア（malware）を用いる方法である。スパイウェアとは，コンピュータ内のデータを盗み取るための不正なプログラムで，サイトの閲覧，メールの添付ファイルの起動，ファイルのダウンロード等によってユーザーの知らないうちにインストールされる(15)。以後，ユーザーが入力したパスワード等の情報を不

正に転送させることで，IDの取得が可能となる(16)。キーロガーとは，スパイウェアの一種で，コンピュータ端末の利用者によるキーボードへの入力信号を記録し，端末内に保存もしくは第三者に転送するためのプログラムである(17)。これらの手口は，不特定多数が利用する端末への不正なインストールを通じて行われ，インターネット利用中のID情報の送信において導入されているSSL（Secure Socket Layer）などの通信暗号化の技術に関係なく，ID情報を取得することが可能となる(18)。

第三は，フィッシング（Phishing）による方法である。フィッシングとは，第三者が公的機関・金融機関・通販サイト等を装ったメールでその受信者を偽のサイトに誘導し，そのサイト上で各種個人情報を入力させる手法であり，その容易さから，近年特に増加している(19)。類似の手口として，ファーミング（Pharming）というものもある。これは，コンピュータウィルスやクラッキング等の手段によってDNSによる再帰探索（ドメイン名に割り当てられたIPアドレスを特定する処理）を誤らせ，利用者を偽のホームページに誘導するもので，フィッシングよりさらに巧妙にIDを不正に取得することができるのである(20)。また，VoIP（Voice Over Internet Protocol＝インターネットによる音声伝送技術）を利用したIP電話などを通じて，金融機関等の電話番号を偽装して顧客へ電話をかけ，口頭でID情報を聞き出すヴィッシング（Vishing）という手法も存在する(21)。

3　IDの偽造・変造

IDの不正使用は，真正に存在する他人名義のIDを取得して用いる場合，真正なIDの一部を改変（変造）するなどして用いる場合，架空の名義によるIDを偽造してこれを用いる場合，という三つの類型に分けられる。名義人本人に何らかの被害を及ぼす犯罪を「ID犯罪」と定義するのであれば，真正なIDを用いない後二者の類型は，ここでの検討対象から外れることにもなろう。しかしながら，「ID犯罪」とはIDに関わるあらゆる形態の違法行為を包含する概念として論じられるのが一般的であるから，IDの偽造・変造も不正取得と同様，不正使用するためのIDを入手する準備行為として位置づけることができるのである。

また，偽造または変造された架空のIDを用いて，真正な他人名義のIDを不正取得する場合もある[22]。例えば，虚偽のIDで権限者を装い，相手方にID情報を提供させるようなケースである。

4　IDの不正使用

不正に取得され，または偽造・変造されたIDは，さらなる別の犯罪を行うための欺罔的手段として不正に使用されることになる。その大半は，金銭等の経済的利得を目的とした狭義の「ID詐欺」だが，他の犯罪の用に供される場合も存在する。

・ID詐欺

他人名義のIDを不正に使用して何らかの経済的利益を得る手段として最も一般的なのは，他人名義のクレジットカードや小切手などで物品等を購入し，その支払請求を他人名義の既存の口座にまわすというものである[23]。アメリカ合衆国の連邦取引委員会（Federal Trade Commision：以下，FTCという）が2006年に公表した調査結果[24]によれば，このような詐欺がID詐欺全体の８割以上を占めており[25]，クレジットカードの不正使用が全体の６割を超えるという[26]。他方，名義人本人も日常的にアクセスする可能性のある口座であるため，不正使用が発覚するまでの期間は，約７割が１ケ月以内と比較的短く[27]，被害額も約７千ドルと少額である[28]。

これに対して，他人名義のクレジットカード口座等を新設したうえで，物品購入等の支払い請求を名義人に負担させる場合，１ケ月以内の発覚は約３割に減少し，発覚が遅れることで生じる被害額も約３万ドルにのぼる。

・その他の犯罪的使用

経済的利得を目的としないIDの不正使用の態様として指摘されているのは，訴追その他の刑事処分を免れるために，法執行機関に対して他人の氏名等を詐称するものである[29]。検挙等の際の身元確認が適切に行われない場合には，このようなケースも問題となろう。また，不法入国の手段として偽造旅券を用いたり，入国先で不法に就労するために他人の社会保障番号（Social Security

Number）を使用するケースも，アメリカ合衆国では問題とされている(30)。

また，ID犯罪の背景には，資金獲得を目的とした組織的詐欺行為，架空名義人等で設けた預金口座を利用したマネー・ローンダリング，人身売買や不法移民のあっせんなどを内容とする組織的犯罪活動の存在が指摘されている(31)。さらに，特に不正な旅券を用いた不法入国をめぐって，テロ活動との関連性についても国際的な警戒感は高まっているのである(32)。

従来，個人情報の保護あるいは個人情報の適切な取扱いの問題はプライバシーとの関係で論じられることが多く，また，IDの不正使用は財産犯罪としての側面がとかく問題とされる傾向にあった。しかしながら，上記のように国家の安全保障にまで関わってくるとすれば，これはプライバシー侵害や財産侵害という以上に，深刻な問題であるといえる。

---

(6) Commission on Crime Prevention and Criminal Justice, Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity (2007), http://www.unodc.org/unodc/en/commissions/CCPCJ/session/16.html (E/CN.15/2007/8/Add.3), at paragraph 4–5 (last visited Aug. 7, 2009) [hereinafter UN Report].

(7) *See also*, John Lyons & Greg Saville, *Resolving the Identity Document Crisis*, 2006 J. Inst. Just. Int'l Stud. 197, 198 (2006).

(8) UN Report at paragraph 4–5.

(9) *See also*, U.S. Department of Justice Office of Community Oriented Policing Services, A National Strategy to Combat Identity Theft (2006), http://www.cops.usdoj.gov/files/ric/Publications/e03062303.pdf, at 49 (last visited Aug. 7, 2009).

(10) The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan (2007), http://www.idtheft.gov/reports/StrategicPlan.pdf, at 14 (last visited Aug. 7, 2009) [hereinafter Strategic Plan]. もっとも，合衆国では，2003年の「公正・正確な信用取引に関する法（Fair and Accurate Credit Transactions Act, 15 U.S.C §1681)」により，クレジットカードおよびデビットカードを使用した際のレシートにカード番号を印字しないことを要求しており，こうした手口によるID盗取は減少したとされる。

(11) *See*, Strategic Plan at 18.

(12) IDの自動収集から生じる問題を指摘したものとして，小向太郎「ID情報の自動収集とプライバシー・個人情報保護」中央大学大学院研究年報34号391頁以下（2004年）参照。

(13) ハッキングとクラッキングはほぼ同義とされるが，厳密に区別するときには，前

者は他人のコンピュータへの単なる侵入行為を指し，後者は侵入の上データの変造・破壊・複製等を行う場合を意味する。岡田好史「ハッキング・クラッキングに対する刑事規制」現刑57号35頁（2004年）。

⑭ Strategic Plan at 15．吉田・前掲注⑸135頁。なお，ハッキングについて技術面の解説をしている国内の文献として，岡田好史『サイバー犯罪とその刑事法的規制―コンピュータ情報の不正入手・漏示に対する法的対応をめぐって』65頁以下（2004年）参照。

⑮ 吉田・前掲注⑸144頁。「トロイの木馬」がその代表例である。

⑯ Kenneth M. Siegel, *Protecting the Most Valuable Corporate Asset*: *Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 Penn St. L. Rev. 779, 785（2007）．アメリカ合衆国におけるスパイウェア対策を紹介したものとして，岡本友子「インターネット社会におけるプライバシー侵害と個人情報の保護――スパイウェア（spyware）問題を中心として――」民商133巻４・５号34頁以下（2006年）。

⑰ 吉田・前掲注⑸141頁。

⑱ 同上。

⑲ アメリカ合衆国を中心とした各国の企業，捜査当局その他によって組織されている反フィッシング団体であるAPWG（Anti-Phishing Working Group）が公表した統計によれば，2008年下半期には合計約17万３千件のフィッシング目的のＥメールが報告され，約13万７千件の新サイトが発見されている。Phishing Attack Trends Report-Second Half 2008（2009），http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf, at 4（last visited Aug. 7, 2009）. *See generally*, Jennifer Lynch, *Identity Theft in Cyberspace*: *Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 Berkeley Tech. L.J. 259, 265（2005）.

⑳ 吉田・前掲注⑸136頁以下参照。

㉑ Strategic Plan at 16. *See also*, Rasha AlMahroos, *Phishing for the Answer*: *Recent Developments in Combating Phishing*, 3 I/S: J.L. & Pol'y for Info. Soc'y 595, 598（2007）; Jonathan E. Meer, *Is the Federal Government Making VoIP Safer?*, 25-SPG Comm. Law. 9（2007）.

㉒ UN Report at paragraph 18.

㉓ インターネットを通じたオンライン販売が普及した現在，クレジットカードそのものを偽造せずとも，他人名義のクレジットカードに関する情報さえあれば，このような詐欺は可能である。Strategic Plan at 18.

㉔ 後述する1998年のID盗取・濫用防止法で，FTCは，ID犯罪の被害者からの申立てを受理した上で，それら申立てを連邦・州・地方の法執行機関で共有し，被害者の名誉を回復するための情報を提供することとされた。1999年以降，FTCは右の業務を行っており，2003年と2006年に被害実態の統計を公表している。Federal Trade Commission-2006 Identity Theft Survey Report（2007），http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf（last visited Aug. 7, 2009）.

(25) *Id*. at 13.
(26) *Id*. at 17.
(27) *Id*. at 23.
(28) *Id*. at 5.
(29) *See*, Michael W. Perl, *It's Not Always About the Money*: *Why the State Identity Theft Laws Fail to Adequately Address Criminal Identity Theft*, 94 J. Crim. L. & Criminology 169 (2003).
(30) Strategic Plan at 20. *See also*, Eduardo M. Gonzalez, *The New Arizona Data Security Breach Law*: *A Step in the Right Direction, But Unlikely to Prevent Identity Theft or Compensate Consumers*, 40 Ariz. St. L.J. 1349, 1352 (2008).
(31) UN Report at paragraph 18.
(32) UN Report at paragraph 19.

三　アメリカ合衆国の状況

1　実体法の整備

(1) 連邦法

・ID盗取罪

アメリカ合衆国でも個人情報に対する保護の必要性は早くから説かれてきたが，それは主にプライヴァシー保護の観点からのものであり，犯罪の手段として悪用される危険性を必ずしも意識したものではなかった(33)。そして，民事的保護をめぐる議論は盛んな一方で，IDの不正取得やその犯罪的利用を刑罰規定で特に抑止すべきであるという主張は，一部の州の動きを除いて，1998年の連邦法の制定までほとんど見られなかった。

しかし，ID犯罪が問題化する中で，1998年に「ID盗取・濫用防止法（Identity Theft and Assumption Deterrence Act(34)：以下，1998年法という）」が制定され，翌1999年に施行された。同法の中心的部分は，合衆国法典第18編第1028条の規定を改正して新設されたID盗取罪（identity theft）である(35)。

1028条は従来から「個人識別文書に関する詐欺および関連行為（Fraud and related activity in connection with identification documents）」として，(a)(1)項から(a)(6)項で個人識別文書（identification documents）の偽造・使用・移転

を処罰する旨を規定していた。しかし，ここでいう個人識別文書とは，合衆国政府その他の公的機関が発行した文書で，特定の個人の情報を含むまたは個人を特定するために一般的に用いられるものであるとされ(36)，偽造等の客体は限定的であった。

これに対して，新設された(a)(7)項は，「正当な権限なく，連邦法上の違反行為もしくは州法・地域法上の重罪を構成する不法活動を実行する意図で，あるいは教唆または幇助する意図で，他の個人を識別するための手段（means of identification of another person）を認識をもって移転または使用」した者を処罰するものである(37)。

ID盗取の客体である「他の個人を識別するための手段」（以下，個人識別手段という）は，(d)(7)項で「特定の個人を識別するために用いられるあらゆる名称または数字」と定義され，氏名，社会保障番号，生年月日，運転者免許番号，移民登録番号，旅券番号，雇用主／納税者番号，（指紋，声紋，網膜等の）生体情報，電子上の識別番号・コード等，電気通信上の識別情報，1029条のアクセス手段（access device(38)）が具体的に列挙されている。ID情報が化体された公的文書に限定していた従来の規定に対して，ID盗取罪はID情報そのものを犯罪の客体とし，それがどのような有体物に化体されても，あるいは無体情報のままであっても，処罰し得るのである(39)。

また，本罪の行為は「移転」または「使用」である。一般的なセフト罪における盗取行為（窃盗，詐欺，横領）ではなく，不正取得後の行為を処罰の対象としている点が特徴的である(40)。

そして，本罪が成立するためには，連邦法上の違反もしくは州法・地域法上の重罪を構成する不法活動の実行・教唆・幇助の目的がなければならない。ID盗取の，他の犯罪の手段としての性質に着目したものであるといえよう。

1028条はその後，2004年に制定された「ID盗取処罰推進法（Identity Theft Penalty Enhancement Act(41)：以下，2004年法という）」の改正により注目すべき変更が加えられた。まず，個人識別手段の移転と使用を処罰の対象としてきた従来の規定に対して，「所持」が追加された。これにより，他人から不正に取得したIDを実際に使用したり，使用するために他に移転したりする前の「所持」の段階で検挙することが可能となったのである(42)。さらに，連邦法違反もしくは州法上の重罪を実行・教唆・幇助する目的がなくとも，それらの犯

罪に関連して（in connection with），個人識別手段の移転・所持・使用がなされていれば足りるとして，主観的要件を緩和したのである。

・加重ID盗取罪

2004年法は，1028A条に加重ID盗取罪（aggravated identity theft）を新たに規定した。一定の重罪の実行に際して，およびこれに関係して（in relation to），個人識別手段を移転・所持・使用した場合に，当該犯罪（基礎となる罪）について科される刑罰に加重するものである[43]。

基礎となる罪には二つの類型がある。第一が，同条(c)項に列挙された重罪[44]であり，この場合は，２年の刑期が加重される。第二が，および2332b条(g)(5)(B)項に列挙されたテロ犯罪[45]であり，こちらは５年の刑期が加重される。

下院議会法制委員会の報告書では，本罪が創設された背景として，ID盗取罪によって科される刑が軽すぎたという問題が指摘されている[46]。ID盗取は通常，他の連邦上の犯罪と一連のものとして行われるとして，裁判官の裁量により二つの罪に対する刑の同時執行が行われてきたためである[47]。そこで，加重ID盗取罪の刑は，基礎となる罪との必要的な逐次執行等が要求された[48]。これにより，本罪で科される２年または５年の刑が，最終的に被告人に対して科される刑期の下限を画することになるのである[49]。

・その他の処罰規定

ID盗取罪および加重ID盗取罪が主に運用されている現在も，それらの代わりに他の連邦法上の犯罪が適用されることがある。具体的には，欺罔の手段や対象ごとに設けられた各種詐欺罪[50]，IDを記載した文書に関連する罪[51]，コンピュータ／サイバー犯罪としての性質に着目した罪[52]などである。

⑵　州法

アリゾナ州は，連邦の1998年法に先立って，1996年に国内初の明文によるID盗取処罰規定を定めている。そこでは，「不法な目的で，あるいは他人に対して経済的損失を与える目的で他人のIDを入手または使用する意図で，他人の氏名・生年月日または社会保障番号を本人の承諾なく故意に取得（take）」

した者を第５級の重罪とした[53]。

他の州もこれに続き，現在，全ての州が「身元確認情報（personal identifying information）」などと総称した各種ID情報の不法取得や，これを用いた詐欺を処罰する処罰規定を置いている[54]。

2　刑事訴追の現状

⑴　捜査体制の整備

ID犯罪は，その手段の多様さと密行性から，検挙が困難であるとされる[55]。そのため，アメリカ合衆国では，各機関が連携して，ID犯罪の捜査にあたっている。1998年のID盗取・濫用防止法は，FTCに対して，ID犯罪の被害者からの申立てを受理した上で，それら申立てを連邦・州・地方の法執行機関で共有し，被害者の名誉を回復するための情報を提供することを義務づけている。現在，FTCがID犯罪事件を各機関に振り分ける業務も行っている[56]。

連邦レベルでのID犯罪の捜査は主にシークレット・サービス（U.S. Secret Service：以下，USSSという）が担当する[57]。USSSは，従来は財務省の秘密検察局として偽造貨幣等のほか，コンピュータ犯罪に関する捜査権も有していたが，2003年に新たに設立された国土安全保障省（Department of Homeland Security）の管轄に移された。USSSは金融犯罪対策本部（Financial Crimes Task Forces）を全国29ケ所に，電子犯罪対策本部（Electronic Crimes Task Forces）を24ケ所に設置し，特に他人名義のIDを用いたクレジットカード詐欺，金融詐欺，旅券詐欺などの捜査にそれぞれあたらせている[58]。

司法省の管轄である連邦捜査局（Federal Bureau of Investigation）も，全国各地に21の対策本部と80の金融犯罪対策本部を設置し，一定の成果を上げている[59]。このほかに，郵便公社（U.S. Postal Service）もID犯罪に関する捜査を行うが，郵便詐欺の場合に限定される。

⑵　ID盗取罪・加重ID盗取罪の成立要件と立証

現在，ID盗取罪および加重ID盗取罪は次のとおり規定されている。

18 U.S.C §1028

(a) 本セクション(c)項で掲げられた状況において，下記の行為を行った者は，本セクション(b)項に従い処罰する。

(7) 正当な権限なく，連邦法上の違反行為もしくは州法・地域法上の重罪を構成する不法活動を実行する意図で，あるいは教唆または幇助する意図で，またはこれに関連して，他の個人を識別するための手段を認識をもって移転，所持，または使用した場合

18 U.S.C §1028A

(a) 罪となるべき行為

(1) 一般――正当な権限なく，(c)項で列挙された重罪の実行に際してまたはこれに関係して，他の個人を識別するための手段を認識をもって移転，所持，または使用した者は，当該重罪について規定された刑罰に加えて，2年の禁錮刑に科す。

(2) テロ犯罪――正当な権限なく，2332b条(g)(5)(B)項で列挙された重罪の実行に際してもしくはこれに関係して，他の個人を識別するための手段または虚偽の個人識別文書を認識をもって移転，所持，または使用した者は，当該重罪について規定された刑罰に加えて，5年の禁錮刑に科す。

・主観的要件

1998年に制定された当初のID盗取罪は，連邦法違反もしくは州法上の重罪を実行・教唆・幇助する目的を要求していたが，IDの不正使用により得られた金銭的利益を享受した事実がある場合などは別として，多くの場合，そのような主観面の立証は困難とされた(60)。2004年法の改正は，個人識別手段の移転・所持・使用が連邦法違反もしくは州法上の重罪に関連して行われた場合にもID盗取罪の成立を認めるものだが，この場合は，上記のような主観面の立証をすることなく他の不法活動の存在を立証することで足りるため，訴追は容易だとされる(61)。この点は，同時に新設された加重ID盗取罪の成立要件にも反映されており，個人識別手段の移転・所持・使用の事実と，所定の重罪との関連性を客観的に立証できればよいとされている。

他方，ID盗取罪および加重ID盗取罪におけるメンズ・レアの内容については，争いがある。具体的には，「認識をもって（knowingly）」に関連して，移転・所持・使用という行為の認識で足りるのか，それとも当該個人識別手段が他人のものであることの認識まで必要とするのか，という問題である。そして，これは，当該個人識別手段について被告人に正当な権限がないこと（without lawful authority）の認識を要求するか否かの問題とも重なる。

下級審裁判所は両論に分かれていたが(62)，2009年５月のFlores-Figueroaケース(63)で，連邦最高裁が初の判断を下した。本件は，不法入国のうえ他人の社会保障番号と外国人居住者証を呈示して雇用を得たメキシコ国籍の被告人に対して，不法入国の罪(64)と入国書類の不正使用の罪(65)の訴因に，加重ID盗取罪の訴因を加えて起訴したものである。被告人は，自身が所持していた社会保障番号と外国人居住者証の登録番号が他人のものであったことを知らなかった旨，そのため加重ID盗取罪の成立に必要な認識を欠く旨主張した。これに対する連邦最高裁の多数意見は，条文の文言解釈や立法過程などを検討し，当該個人識別手段が他人のものであることの認識が要求されるとしたのである(66)。

このように解した場合，被告人が当該個人識別手段の内容が不真正であることを知らなかった旨の反論をすれば主観面の立証が困難になることが懸念される。これに対して，連邦最高裁は，行為者が個人識別手段を取得する前または後に行っている他の行為から推測可能であると判示している(67)。他の犯罪に追加して訴追される加重ID盗取罪の運用が主となった現在，被告人が当該個人識別手段に関連して他の犯罪を行っている事実をもって，移転・所持・使用において正当な権限がないことの認識，さらには当該個人識別手段が他人のものであることの認識の立証が可能なのである。

・所持処罰の意義

ID盗取罪および加重ID盗取罪の特色の一つは，所持が処罰対象とされている点である。所持を処罰することには，すでに述べたように，早い段階での検挙を可能とするという意味もあるが，他方では立証上の便宜を考慮したものであるともいえる。Hurtadoケース(68)で第11巡回控訴裁判所は，他人の個人識別手段を正当な権限なく所持するに至る経緯には様々なものがあり，その経緯が何であるか（窃盗行為によるものであること）を立証する必要はないと判示し

ている。

⑶　他の連邦法規定との関係

ID盗取罪と加重ID盗取罪はいずれも，不正に取得されたIDが他の犯罪の遂行のために使用されることを想定している。IDの不正使用が他の連邦上の犯罪を構成する場合には，それらで訴追することもできる[69]。多くの場合，加重ID盗取罪との併科が可能であるため，適用可能な訴因は全て加えるのが通常である。

---

[33] *See e.g.*, Carol R. Williams, *A Proposal for Protecting Privacy During the Information Age*, 11 ALASKA L. REV. 119 (1994); Donald A. Doheny, Sr. & Graydon John Forrer, *Electronic Access to Account Information and Financial Privacy*, 109 BANKING L.J. 436 (1992); Jonathan P. Graham, Privacy, *Computers and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395 (1987). *See also*, Balaram Gupta, *Names and Logos: Protection Under Intellectual Property Laws and Consequences*, 2 SPORTS LAW. J. 245 (1995)［知的財産権の観点からのID保護について言及］. *But see*, David A. Szwak, *Data Rape: Theft of Identity*, 17-OCT PA. LAW. 16 (1995)［経済的詐欺におけるIDの使用について言及］.

[34] PL 105-318, October 30, 1998, 112 Stat 3007. ID盗取・濫用防止法について，*See*, Catherine Pastrikos, *Identity Theft Statutes: Which Will Protect Americans the Most?*, 67 ALB. L. REV. 1137, 1139 (2004); Holly K. Towle, *Identity Theft: Myths, Methods, and New Law*, 30 RUTGERS COMPUTER & TECH. L.J. 237, 264 (2004); Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1429 (2001); Kristen S. Provenza, *Identity Theft: Prevention and Liability*, 3 N.C. BANKING INST. 319, 324 (1999); Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661, 670 (1999).

[35] ID盗取罪について紹介している国内の文献として，中川・前掲注⑸62頁，太田ほか・前掲注⑸10頁以下。また，前田＝堀田・前掲注⑸15頁参照。

[36] 18 U.S.C. §1028(d)(3)（1998年当時は(d)(1)項）参照。

[37] 法定刑は，1年間以内の被害額が1,000ドルを超える場合は罰金または15年以下の禁錮，それ以外の場合は罰金または3年以下の禁錮である。18 U.S.C. §1028(b)(1)-(2). その後，2004年の改正で，後者の刑は5年以下に引き上げられた。

[38] アクセス手段とは，金銭やサービス等を得るために必要なカード，口座情報，暗証番号など有形・無形の手段をいう。18 U.S.C. §1029(e)(1)参照。

(39) Hoar, *supra* note 34, at 1429.

(40) セフト罪は，窃盗（larceny）・横領（embezzlement）・詐欺（false pretenses）の統合形式として発展したものであるが，これは財産犯にかかる立証上の困難を回避することを目的としている。*See generally*, WAYNE R. LAFAVE, CRIMINAL LAW 975–980（4th ed. 2003）; Model Penal Code § 223.1 cmt. on consolidation of theft offenses at 134–35（1980）. *See also*, Sherry A. Moore, *Nevada's Comprehensive Theft Statute*: *Consolidation or Confusion*?, 8 NEV. L.J. 672, 679（2008）; John Wesley Bartram, *Pleading for Theft Consolidation in Virginia*: *Larceny, Embezzmlement, False Pretenses and § 19.2–284*, 56 WASH. & LEE L. REV. 249, 293（1999）.

(41) PL 108–275, July 15, 2004, 118 Stat 831．ID盗取処罰推進法について，*See*, Ian Heller, *How the Internet Has Expanded the Threat of Financial Identity Theft, and What Congress Can Do to Fix the Problem*, 17–FALL KAN. J.L. & PUB. POL'Y 84, 94（2007）.

(42) H.R. Report 108–528, 10. *See also*, CLIFF ROBERSON, IDENTITY THEFT INVESTIGATIONS 119（2008）.

(43) 18 U.S.C. §1028A(a).

(44) 公金・公的財産等の盗取（18 U.S.C. §641），銀行員による盗取等（18 U.S.C. §656），企業内基金の盗取（18 U.S.C. §664），合衆国市民の詐称（18 U.S.C. §911），銃器購入時の身分詐称（18 U.S.C. §922(a)(6)），18 U.S.C. §1028(a)(7)のID盗取罪を除く合衆国法典第18編第47章の罪（詐欺），第63章の罪（郵便詐欺・通信詐欺），第69章の罪（国籍および市民権に関する罪），第75章の罪（旅券・査証に関する罪），詐欺による顧客情報の取得（15 U.S.C. §6823），追放処分を受けた後の偽造身分証明書による滞在（8 U.S.C. §1253 and 1306），移民法にかかる罪（8 U.S.C. §1321 et seq.），社会保障番号に関連した虚偽供述等（42 U.S.C. §408, 1011, 1307(b), 1320a–7b(a), and 1383a）。

(45) 18 U.S.C. §2332b(g)(5)は，脅迫または強制により政府の活動に影響または干渉，あるいは政府の活動に対して報復する計画で，破壊，兵器の準備・使用，テロリストの蔵匿・援助，その他所定の犯罪行為を行った場合を連邦テロ犯罪（Federal crime of terrorism）として規定している。

(46) H.R. Report 108–528, 5.

(47) 同時執行（concurrent sentences）と逐次執行（consecutive sentences）について，*See generally*, WAYNE R. LAFAVE, CRIMINAL PROCEDURE 1229–30（4th ed. 2004）.

(48) 18 U.S.C. §1028A(b)．具体的には，保護観察に付してはならないこと（18 U.S.C. §1028A(b)(1)），原則として他の罪に対する刑との同時執行をしてはならないこと（18 U.S.C. §1028A(b)(2)），基礎となる重罪の刑期を決定するにあたって本罪による刑期の加重の点を考慮してはならないこと（18 U.S.C. §1028A(b)(3)）が規定された。

(49) *See*, Ian Heller, *How the Internet Has Expanded the Threat of Financial Identity Theft, and What Congress Can Do to Fix the Problem*, 17–FALL KAN. J.L. &

PUB. POL'Y 84, 96 (2007).

(50) アクセス手段に関連した詐欺（18 U.S.C. §1029），郵便詐欺（18 U.S.C. §1341），通信詐欺（18 U.S.C. §1343），金融機関詐欺（18 U.S.C. §1344），社会保障番号を用いた詐欺（18 U.S.C. §408(a)(7)(B)）など。

(51) 個人識別文書等関連詐欺（18 U.S.C. §1028(a)(1)-(6)），パスポートの申請と使用における虚偽申告（18 U.S.C. §1542），パスポートの偽造と不正使用（18 U.S.C. §1543），パスポートの悪用（18 U.S.C. §1544）など。

(52) 政府や金融機関等のコンピュータの情報の不正取得（18 U.S.C. §1030(a)(2)），コンピュータ詐欺（18 U.S.C. §1030(a)(4)）など。

(53) ARIZ. REV. STAT. ANN. §13-2708．同州の処罰規定について，*See*, David Lish, *Would the Real David Lish Please Stand Up?: A Proposed Solution to Identity Theft*, 38 ARIZ. ST. L.J. 319, 325-29 (2006); Pastrikos, *supra* note 34, at 1138.

(54) ALA. CODE § 13A-8-192; ALASKA STAT. § 11.46.290; ARIZ. REV. STAT. ANN. § 13-2008; ARK. CODE ANN. § 5-37-227; CAL. PENAL CODE ANN. § 530.5; COLO. REV. STAT. ANN. § 18-5-902; CONN. GEN. STAT. ANN. § 53A-129A; DEL. CODE ANN. TIT. 11, § 854; FLA. STAT. ANN. § 817.568; GA. CODE ANN. § 16-9-120, -132; HAW. REV. STAT. § 708-839.6; IDAHO CODE § 18-3126; 720 ILL. COMP. STAT. 6/16G; IND. STAT. ANN. § 35-43-5-3.5; IOWA CODE ANN. § 715A.8; KAN. STAT. ANN. § 21-4018; KY. REV. STAT. ANN. § 514.160; LA. REV. STAT. ANN. § 14:67.16; ME. REV. STAT. ANN., TIT. 17-A, § 905-A; MD. CODE ANN., CRIM. LAW § 8-301; MASS. GEN. LAWS ANN. CH. 266, § 37E; MICH. COMP. LAWS ANN. § 750.539k; MINN. STAT. ANN. § 609.527; MISS. CODE ANN. § 97-19-85; MO. ANN. STAT. § 570.223; MONT. CODE ANN. § 45-6-332; NEB. REV. STAT. § 28-608 ; N.H. REV. STAT. § 638:26; N.M. STAT. ANN. § 30-16-24.1; N.Y. PENAL LAW § § 190.77; N.C. GEN. STAT. § 14-113.20; N.D. CENT. CODE § 12.1-23-11; OHIO REV. CODE ANN. § 2913.49; NEV. REV. STAT. § 205.463; N.J. STAT. ANN. § § 2C:21-17; OKLA. STAT. ANN. TIT. 21, § 1533.1 ; ORE. REV. STAT. § 165.800; PA. CONS. STAT. ANN. TIT. 18, § 4120; R.I. GEN. LAWS § § 11-49.1-3 ; S.C. CODE ANN. § 16-13-510; S.D. CODIFIED LAWS § § 22-40-8; TENN. CODE ANN. § 39-14-150; TEX. PENAL CODE ANN. § 32.51; UTAH CODE ANN. § 76-6-1103; VA. CODE ANN. § 18.2-186.3; WASH. REV. CODE ANN. § 9.35.020; W. VA. CODE § 61-3-54; WIS. STAT. ANN. § 943.201; WYO. STAT. § 6-3-901.

(55) *See*, ROBERSON, *supra* note 41, at 74-75.

(56) *Id*. at 101-102.

(57) *Id*. at 101.

(58) USSS Homepage, http://www.ustreas.gov/usss/criminal.shtml (last visited Aug. 7, 2009).

(59) ROBERSON, *supra* note 41, at 105.

(60) H.R. Report 108-528, 10-11.

(61) *Id*.

⑹ 「他人の」個人識別手段であることの認識を必要としたものとして，United States v. Godin, 534 F.3d 51（1st Cir. 2008）; United States v. Miranda-Lopez, 532 F.3d 1034（9th Cir. 2008）; United States v. Villanueva-Sotelo, 515 F.3d 1234（D.C. Cir. 2008）. 不要としたものとして，United States v. Mendoza-Gonzalez, 520 F.3d 912,（8th Cir. 2008）, United States v. Hurtado, 508 F.3d 603（11th Cir. 2007）; United States v. Montejo, 442 F.3d 213（4th Cir. 2006）. *See also*, Roberson, *supra* note 41, at 122-125; Lori J. Parker, *Legal and Procedural Issues in Prosecutions Under Federal Statutes Relating to Offense of Identity Theft*, 4 A.L.R. Fed. 2d 365, at § 31.2-31.3（2005）

⑹ Flores-Figueroa v. United States, 129 S.Ct. 1886（2009）.

⑹ 8 U.S.C. § 1325.

⑹ 18 U.S.C. § 1546.

⑹ Flores-Figueroa v. United States, 129 S.Ct. 1886, 1888（2009）.

⑹ *Id*. at 1893.

⑹ United States v. Hurtado, 508 F.3d 603（11th Cir. 2007）.

⑹ Strategic Plan at Append. N.

四　わが国の現状と課題

１　ID犯罪への対応の現状

冒頭で述べたように，わが国ではIDの不正取得および不正使用を「ID犯罪」という枠組みで扱ってはこなかった。しかし，国際的にはID犯罪の一類型として問題視されている種々の犯罪の実態は存在するのである。そこでまずは，わが国におけるID犯罪の現状を概観しながら，既存の法適用について整理することにしたい。

⑴　不正アクセスおよびフィッシング

現在，ネットワークを通じて行われるID犯罪の大半は，不正アクセス禁止法で対応されている。

IDを不正に取得するための手段としてハッキングやマルウェアの使用があることは前述のとおりであるが，ハッキングは，セキュリティ・ホール攻撃型

の不正アクセス行為として，不正アクセス禁止法３条２項２号ないし３号が適用可能である(70)。これに対して，後者にかかるスパイウェアやキーロガーの使用については，それらの手口によって入手したIDを使用する段階を待って，識別情報盗用型の不正アクセス行為として同法３条２項１号を適用することになる(71)。

他方，IDの不正使用にかかる行為としては，インターネット・オークションの不正操作やオンラインゲームの不正操作，インターネットバンキングの不正送金などが挙げられるが(72)，いずれも，その前提に存在する識別情報盗用型の不正アクセス行為について処罰されている。

ところで，不正アクセスの手段として使用するためのID情報をフィッシングにより入手する手口の横行も深刻である(73)。しかしながら，フィッシング等，利用者によるネットワーク等へのアクセスを誤らせて不正にそのID情報を取得する行為を直接処罰する規定は存在しない。そのため，正規のホームページに体裁が酷似したサイトを作成した行為に対する著作権法違反，そこで入手したID情報を使用して不正アクセスした行為に対する不正アクセス禁止法違反などで対応せざるを得ないのが現状である(74)。

⑵　カード犯罪

クレジットカード，デビットカード，プリペイドカード等の支払用カード（以下，カードという）を悪用する犯罪は「カード犯罪」と呼ばれる。周知のとおりその被害は深刻で，クレジットカードの不正使用による被害額は，1989年から1999年までの10年間で２倍以上増加し，300億円を超えた2000年をピークに減少しているものの，2008年も100億円余りと依然として大きな被害をもたらしている(75)。このうち約５割は偽造カードの使用によるものであるが，カード偽造の手口として代表的なものが，前述のスキミングである(76)。わが国でも，加盟店の信用照会端末に不正に取り付けられたスキマー等を通じて，他人名義のカードを偽造するために必要な情報を得る手法が社会問題となった。

最広義では，支払の能力と意思を欠いて自己名義のカードを使用する詐欺もこれに含まれることになろうが(77)，特に問題なのは他人名義のカードを用いて行う詐欺である。具体的には，窃取・拾得等により得られた真正の他人名義の

カードを用いて詐欺・窃盗等を行う場合と，他人名義のカードを偽造した上でこれを詐欺・窃盗等に用いる場合であり[78]，いずれもIDの不正使用にかかる犯罪である。また，スキミングは，IDの不正使用の前段階にあたる不正取得の類型である。

2001年の刑法改正では，以上の状況に対応するため，支払用カード電磁的記録不正作出等の罪（163条の２），不正電磁的記録カード所持の罪（163条の３），支払用カード電磁的記録不正作出準備の罪（163条の４）が新たに設けられた。このうち，支払用カード電磁的記録不正作出準備の罪は，電磁的記録の不正作出の用に供する目的で，支払用カードを構成する電磁的記録の情報を取得，提供，または保管した場合を処罰する。スキミング等，カード偽造の準備行為を禁止する趣旨である。

２　今後の課題

ここまでみたように，わが国においても，IDの不正取得・不正使用に関して，一定の対応がされてきた。しかし，現状に問題が全くないわけではない。

⑴　不正アクセス罪の意義

ID犯罪の多くがネットワークを介在して行われるという実情に鑑みたとき，不正アクセス罪の積極的な運用は，既存の規定を用いた現実的な対応として評価できる。他方，ID犯罪への対策を総合的に考えるならば，現状が必ずしも望ましいものではない。

不正アクセス罪の保護法益ないし罪質をめぐっては議論があるが[79]，住居侵入罪との対比でこれを捉える見解が有力である[80]。すなわち，同罪において保護されるのは，アクセス制御機能を有する特定電子計算機の内部で行われるデータ処理およびそのデータ処理の確実性に対する信頼を保護するために構築されたアクセス制御システムそれ自体であり，アクセス制御システムを不正に突破する行為を住居侵入類似の行為と考えるのである[81]。

同見解は，不正アクセス行為の性質を端的に表すものとして妥当であろう。しかし，このように考えたとき，不正アクセス罪によって侵害される法益（ア

クセス制御システム）と，不正アクセス行為によって不正に得られてしまうデータやサービスが保護されるべき利益とは，切り離されることになる。データやサービスへの不正アクセスと，それらの不正取得を区別するのであれば，前者に対する刑罰規定である不正アクセス罪をして後者への刑事的対応とすることはできない。不正アクセス禁止法の効果的な運用をもって，データの不正取得それ自体を処罰するための立法的手当が不要とまではいえないのである。

⑵　詐欺罪による対応の限界

IDの不正使用にかかる行為は多岐にわたるが，わが国の現行法上は，その大半の処罰を詐欺罪に委ねざるを得ない。最決平成14年10月21日（刑集56巻８号670頁）は，被告人が不正に入手した他人名義の国民健康保険被保険者証等を使用して開設した同人名義の預金口座にかかる預金通帳を交付させた行為について，詐欺罪の成立を認めた。また，最決平成19年７月17日（刑集61巻５号521頁）は，第三者に譲渡する意図であることを秘して自己名義の預金口座を開設し，銀行に預金通帳とキャッシュカード交付させた行為について詐欺罪の成立を認めている。

これらの行為は，口座名義が有する身元確認機能を害するという意味において，IDの不正利用に該当するものである。そして，振り込め詐欺における振込先口座としての犯罪的利用やマネー・ローンダリングへの悪用の危険性を考えれば，自己名義・他人名義にかかわらず，不正な目的で預金通帳を騙取する行為の当罰性について異論はないだろう。

しかし，たとえ詐欺罪が個別財産に対する罪であるとしても実質的な損害の発生が必要であるとする実質的個別財産説[82]が有力な現在，預金通帳を交付しても銀行に財産上の損害は発生しないとして，上記二判例は学説の批判にさらされている[83]。IDをめぐる新たな問題に対応するために詐欺罪の本来の処罰範囲を今後も拡げざるを得ないとすれば[84]，IDの不正使用を何らかの形で捕捉する立法を模索する必要が生じることになろう。

⑺⓪　岡田・前掲注⑬36頁。

(71)　吉田・前掲注(5)146頁。

(72)　警察庁の統計を参照。［http://www.npa.go.jp/hakusyo/h20/toukei/t1-20.pdf］（最終確認日：2009年８月７日）

(73)　警察庁の統計によれば，平成19年の不正アクセス事犯のうち識別符号盗用型にかかる手口の約８割がフィッシングによるものである。［http://www.npa.go.jp/hakusyo/h20/toukei/t1-22.pdf］（最終確認日：2009年８月７日）参照。

(74)　吉田・前掲注(5)138頁。

(75)　日本クレジット産業協会「クレジットカード犯罪の現状」ジュリ1209号24頁（2001年）。日本クレジット協会HPで公開されている統計も併せて参照。［http://www.j-credit.or.jp/information/statistics/download/inv_05_01.pdf］（最終確認日：2009年８月７日）。

(76)　刑法改正当時の被害状況について，日本クレジット産業協会「クレジットカード犯罪の現状」ジュリ1209号24頁以下（2001年），前田雅英「カード犯罪対策の現状と課題」ジュリ1203号106頁（2001年）参照。

(77)　野村稔「カード犯罪について」現刑20号96頁以下（2000年），山口厚「クレジットカードの不正使用と詐欺罪の成否」法教297号88頁以下（2005年）。

(78)　前田・前掲注(75)106頁，岡谷晃治・林秀典「カード犯罪をめぐる捜査上の問題点と今後の対策について」警論58巻10号144頁（2005年）。

(79)　岡田・前掲注(14)112頁以下，今井猛嘉「ネットワーク犯罪」法教303号50頁以下（2005年）参照。

(80)　佐伯仁志「無権限アクセス規制に関する覚書」研修602号４頁（1998年），岡田・前掲注(14)114頁，今井猛嘉「『不正アクセス』の意義をめぐって」研修719号８頁（2008年）。

(81)　今井・前掲注(79)８頁。

(82)　佐伯仁志「詐欺罪の理論的構造」山口・井田・佐伯『理論刑法学の最前線Ⅱ』104頁（2006年），西田典之『刑法各論〔第４版〕』189頁（2007年），前田雅英『刑法各論講義〔第４版〕』287頁（2007年）。

(83)　松原芳博「判批」法教274号139頁（2003年），松宮孝明「判批」法セミ48巻３号107頁（2003年）など。これに対して，木村光江「詐欺罪における損害概念と処罰範囲の変化」曹時60巻４号27頁以下（2008年）は，処罰範囲を拡大する傾向があるとはいえ，それは無限定なものではないとする。

(84)　なお，詐欺罪と，平成19年に成立した犯罪収益移転防止法における罰則との関係も，今後の検討課題となろう。これに関連して，木村・前掲注(83)13頁以下参照。

五　おわりに

以上，本稿では，「ID犯罪」という従来から存在する各種犯罪問題を性格づ

ける新しい枠組みについて，アメリカ合衆国の状況を概観したのち，わが国における現状とその問題点を検討した。

国民生活において個人識別情報が有する重要性の度合いに，日米で温度差があることも事実である。とりわけ，戸籍制度や住民登録制度などを持たないアメリカ合衆国において，国民に必ず発行される社会保障番号への依存度は非常に高く，これを他人に冒用されることで生じ得る被害は多岐にわたるのである(85)。

したがって，そのように汎用的なIDに依存する仕組みを持たないわが国において(86)，他人に不正使用される危険性のあるIDは預金口座や支払用カードの番号およびパスワードなどに限定されており，アメリカ合衆国のように切迫した問題状況に現在直面しているとまではいえない。

もっとも，情報技術は日々発展を遂げており，将来わが国においても深刻な問題が生じないとも限らない。不正アクセス罪と詐欺罪を中心とした現在の運用では対応しきれないおそれがある以上，この問題は今後さらなる議論を要する領域なのである。その際，訴追および立証上の便宜を最大限に考慮してなされているアメリカ合衆国の立法例は，一つの参考となろう。

---

(85)　同国では，ID犯罪の被害に鑑み，社会保障番号を必要以上に活用しない方針が提言されているほどである。Strategic Plan at 25.

(86)　国民背番号制度の問題点について検討した文献として，平松毅「IDカード及び国民背番号制度の導入に伴う個人情報保護」比較憲法学研究 9 号53頁以下（1997年）参照。