海外のカード犯罪対策

― EUの動き ―

京藤哲久
明治学院大学大学院法務職研究科長

要 約

EUでは、クレジットカード犯罪対策の重点がカード非提示取引（CNP＝Card Not Present）におけるクレジットカード犯罪の規制に移ってきており、その規制のかなめとなるID窃盗（identity theft）をどう規制するかに関心が集まっている。本稿は、EUにおけるID窃盗対策の最近の動向についての紹介である。

現在のところ、ID窃盗に関するEU加盟国の法的規制は十分でなく、また、その規制の手法も区々である。本稿では、欧州連合条約、欧州連合運営条約に即して、EUの共有権限の対象である刑事司法協力の枠組みに触れたうえで、欧州委員会の政策決定のために用意された文書をてがかりとして、加盟国のクレジットカード犯罪対策立法に対する、条約の枠組みに従ったEUの関与の姿を明らかにしている。

【目 次】

Ⅰ．はじめに ― EU におけるクレジットカード犯罪とID窃盗 ―
Ⅱ．EUと加盟国の関係 ― クレジットカード犯罪対策立法におけるEUの権限と役割 ―
Ⅲ．EUのID窃盗対策 ― EUのID窃盗対策の具体的内容 ―

Ⅰ．はじめに
― EUにおけるクレジットカード犯罪とID窃盗 ―

1．クレジットカード犯罪対策におけるID窃盗対策の位置

クレジットカード犯罪による被害は、加盟店でクレジットカードを直接提示して行う「CP取引」（CP＝Card Present）による被害と、インターネット上の店舗でクレジットカード番号、有効期限を打ち込んで取引する、クレジットカードを提示しない「CNP取引」（CNP＝Card Not Present）による被害の二種類に分けられる。

EU加盟国では、統計上、クレジットカードを用いた国内での取引、国境をまたぐ越境型の取引のいずれにおいても、近年、CNP取引におけるクレジットカード犯罪による被害が顕著な増加を示している。そのため、EU圏では、CNP取引におけるクレジットカード犯罪の規制

のあり方に大きな関心が集まっている。そして、この関連でID窃盗の規制に向けた動きが強まっている。

他人の個人識別情報を入手して本人になりすますID犯罪、ID窃盗は昔から存在する犯罪である。しかし、近年のCNPによるクレジットカード取引の急速な普及を背景に、その利便性に伴う弱点につけ込んだクレジットカード犯罪が組織犯罪の一環として活発に行われるようになってきている。クレジットカード犯罪を行うため、様々な方法で違法に入手された個人識別情報（ID情報）がバルク単位で組織犯罪ネットワークを通じて国際的規模で活発に取引され、クレジットカード犯罪のため悪用されている。そのため、EUではID窃盗の規制は組織犯罪対策の一環として重要な政策的テーマとなっている。

なぜ、EUでID窃盗の規制に関心が集まっているのだろうか。これには、EU圏におけるクレジットカードの安全性が向上したため（主として、EMV（ユーロペイ、マスターカード、ビザのICカード統一規格）の導入という技術的要因によるものである）、クレジットカード詐欺の国際的動向が変化したことが関係している。

すなわち、EU圏内ではCP取引におけるクレジットカード詐欺の実行が難しくなってきており、CP取引によるクレジットカード詐欺は技術的理由で規制の甘いアメリカ等で行われるようになってきている。そして、EU圏内ではCNP取引によるクレジットカード詐欺の割合が著しく増えている。

このような傾向は、Europolの報告書に基づいた次のような英国BBCニュースの報道等からもうかがえる。

2011年、EU発行のカードが関係した詐欺のほとんどすべてはEU外で行われた。EUで使われているChip-and-PINの技術は未だグローバル化しておらず（その導入には、加盟店等にそれなりのコストがかかる）、その結果、海外でクレジットカードを用いた詐欺事犯が多発している。クレジットカード番号の漏洩の多くはアメリカで発生したもので、また、EU発行カードを用いた違法な対面取引（CP取引）も多くはアメリカ国内で行われている。また、インターネット上で盗まれた個人識別情報を用いた非対面取引（CNP取引）における詐欺被害は、クレジットカード詐欺による被害の60％程度になっている（BBCNews 2013年1月）。

2. ID窃盗とは

ID窃盗の問題の検討に入る前に、この犯罪現象を対象とするのに様々な用語が用いられているので（identity crime（ID犯罪）, identity theft（ID窃盗）, identity fraud（ID詐欺））、簡単に言及しておこう。

identity crime, identity theft, identity fraudはどのように使い分けられているか。文献によ

って使い方が異なることがあり、用語の使い方は統一していないが、この点をめぐっては次のような議論がなされている[1]。

identity theft という用語が普及しているのは、アメリカ、イギリス、韓国である。これに対して、多くの国では、identity crimeとidentity fraudをほぼ同義語として使用している。また、フランス語圏では、vol d'identitéとusurption d'identitéが同義の語として互換的に用いられている。

おおまかには、次の三つの考え方のあることがうかがえる。

①identity crime のなかに、identity theft, identity fraudがあるという捉え方をする方向が一つである（Europol）。identity fraudは広い意味をもつものとして使用されており、他方、identity theftは（架空人ではなく）現在する個人の情報の窃取に限定されている。このように定義することで、相互の概念を整理しているものである。

②identity theftとidentity fraudを次のように使い分ける方向が一つである（国連政府間専門家グループ）。identity theftは個人識別情報の窃取を対象とし、identity fraudは、将来、詐欺目的でこれらの個人識別情報を利用するところの、牽連犯でいう手段的位置にある犯罪を意味するものとして使われている。両者の関係がどうなるかは罪数の問題（これは国によってかなり取り扱いの異なる分野である）として処理されることになる。

③identity theftを予備罪的位置にあるものとして理解する方向が一つである（イギリス）。イギリスの、identity theftは、被害者の生死を問わず、identity fraudの予備段階に位置づけられる犯罪行為として把握されている。identity theftは詐欺に到れば捕捉されるが、予備段階の行為はよほど重大な犯罪を別として不可罰であるのが原則だから、ここでは、この段階の行為のみではまだ不可罰と考えられていることが含意されている。

3. EU内のID窃盗の現状――欧州警察機構（Europol）、European Cybercrime Center（EC3）の活動からうかがえるID窃盗の現状――

ID窃盗は昔からあった犯罪（なりすまし）である。しかし、クレジットカードが決済手段として広く利用され社会で普及すると、クレジットカード詐欺による被害が増えてきた。このクレジットカード詐欺を行うために、クレジットカードを作るのに必要な個人識別情報を窃取するID窃盗が盛んに行われるようになり、また、得られた情報が違法な取引の対象となってきた。

そして近年、インターネットの普及に伴い、クレジットカード情報を違法に入手する実に様々な手段が考案されるようになってきたことから、ID窃盗はこれまでになく深刻な問題になっている。

このような文脈で、クレジットカード犯罪を規制するためには、ID窃盗の規制が喫緊の課題となっている[2]。すなわち、CNPはクレジットカード犯罪をいっそう容易なものにしていることから、クレジットカード犯罪を抑止するためID窃盗段階での規制が切実な問題となっている。クレジットカードが登場していなかったなら、ID窃盗は今日ほど深刻にならなかったであろう。

Europolが公表している活動報告から[3]、EU地域におけるID窃盗の現状が理解できるが、本稿に関係の深い部分を、以下に要約して紹介しておきたい。

4. カード提示型カード犯罪の特徴とカード非提示型カード犯罪の特徴

Europolの2012年報告書では、カード提示型犯罪とカード非提示型犯罪に分けて、次のような分析がなされている[4]。

(1) カード提示型犯罪（CP取引に伴うカード犯罪）

EU内のATM関連の犯罪（スキミング、盗難カードや物理的な仕掛けを用いて現金を入手するもの）は増大しており、2011年には2万件強発生している。組織犯罪集団は手口を巧妙化させており、あるスキミング対策が採用されたら、今度は、その裏をかく新たな手口（キャッシュトラップ、前払いカードの不正作出、マルウェア等）を考案してくる。

組織犯罪集団の多くがその活動を国際的に展開していることから、国境を越えた国際協力こそが捜査成功の鍵となっている。

しかし、犯罪者の側は、既に警官を買収する、また有能な法律家（expensive and influential lawyers）を抱える等、犯罪捜査に対抗する強力な手段をもっており、そのような事件では捜査はいきおい難航せざるをえない。従って、捜査機関側も、技術者の助けを借りて捜査を遂行して行く必要がある。

残念ながら、現在の事件捜査の大部分はEU内で行われる犯罪のみを対象としているにすぎないから、EU外で行われた犯罪の捜査はほとんど手つかずのままである。

司法レベルでも、EU内で遂行された犯罪が起訴されるにとどまっているというのが現状である。EU内では予備行為が行われるだけで、EU内で被害が生じていない場合には、たとえ起訴にこぎつけることができたとしても、これに対する刑罰はかなり軽いものとなってしまう。そのうえ、組織犯罪集団の場合、誰かが逮捕されても、すぐに替わりの者が補充されるので、その犯罪活動は以後も継続している。

国際協力の方はどうかというと、なかなか難しい。捜査機関が国際的規模で捜査を遂行するのはまれである。国際犯罪集団をターゲットにした捜査ができるようになったら、これはEU内の支払用カードによる取引の安全の確立にとって大きな意味があるといえるだろう。例

えば、こうした国際的規模の捜査が成功した例があるが（Night Clone作戦）、この時には、実際、組織犯罪集団側の動きが数ヶ月間止まった。

(2) カード非提示型犯罪（CNP取引に伴うカード犯罪）

Europolによると、2011年には、支払い用カードの損失のほぼ6割、額にして9億ユーロが、カード非提示型（CNP）のカード詐欺により引き起こされたものである。

違法なデータは、主としてデータ漏洩により入手されたものであり、これらはインサイダーによる漏洩かマルウェアを使って入手されたものが多い。

漏洩したカード・データは大量で数十万件から数百万件にのぼっており、漏洩したデータはインターネット上でバルクで取引されている。現在のところ、EU内で悪用されるカード・データの大部分がアメリカ国内で漏洩されたものではあるが、2010年以降、EU内でのデータ漏洩によるものも増えてきている。

EUでは、データ漏洩が起きた場合の適切な報告制度が存在しないことが大きな問題である。

もちろん、こうした法制度上の欠陥だけが問題というわけではない。ほかにも、被害者である店舗側も法執行機関を信頼しておらず、また、被った損害よりも店の評判のほうを気にかける傾向も大きな問題である。その結果、カード犯罪被害の報告件数が少なく、従って、捜査の国際協力も進まないということになっている。その結果、カード非提示型のカード犯罪が急増しているのだが、これが統計に反映されないということになっている。

安全上の観点からの問題点を見るなら、カード非提示取引の保護についてのグローバル・スタンダードが欠けていることが問題である。主要企業の場合、取引の大部分は3Dプロトコールを使って行われているが、それでもこの3Dプロトコールはまだ国際的レベルで受け入れられてはいない。EUレベルですらそのような状況であるのだから、EU内のオンライン取引のすべてがこのプロトコールによりまもられているという状況にあるわけではない。

それゆえ、現時点では、情報漏洩に対する対策が喫緊の課題となっている。漏洩は大規模なスケールで行われ、そのやり口も巧妙で、関与者も多数にのぼり、しかも複数の国にまだがって行われている。

また、企業側の対策の重点は予防におかれているため、漏洩した場合、漏洩した事実が法執行機関側に報告されてこない。企業による内部調査の実施は、予防措置の強化にはつながるが、企業内調査の過程で漏洩者を特定できる場合というのはまれである。

違法なオンライン取引の捜査にあたっては、次の諸点に着目することが大切である。

すなわち、違法な高額商品の注文、運び屋等のネットワーク、違法な取引、旅行会社、航空会社等からのサービスの購入、ネットから入手したデータを用いて偽造されたクレジット

カードによる現物取引、バルト地域、東南ヨーロッパで展開する組織犯罪グループの調査、得られた情報の適切な照合の実行、データ漏洩と違法取引との関連づけ、資産没収である。

EU加盟国において法制度の整備が進んでいないため、捜査には様々な制約があり、また、実際の捜査ではロシア語に堪能な者が不足している等の語学上の問題もある。

カード非提示型取引のカード犯罪に対処するための経験もまだ不足しているから、この分野でEuropolが果たす役割は重要である。

Ⅱ．EUと加盟国の関係
― クレジットカード犯罪対策立法におけるEUの権限と役割 ―

1. 概説

EUの加盟国は、それぞれ、自前のクレジットカード犯罪対策立法を有しており、EUがクレジットカード犯罪対策立法を有しているわけではない。

2009年のリスボン条約[5]発効後も、EUの枠組みのもとでは、刑事法については加盟国に立法権限がある。しかし、加盟国の刑事立法にEUが口出しできないわけではなく、刑事法についての加盟国とEUとの立法権限の現実の関係はもう少し微妙なものである。というのは、刑事司法「協力」という角度から切り取りうる範囲内では、刑事法については加盟国とEUに「共有権限」が認められているからである[6]。

すなわち、立法権限という観点からは、加盟国にクレジットカード犯罪対策立法、ID犯罪対策立法があることを前提として、この問題が越境的性格を有する等の事情がある場合には、EU加盟国間の刑事司法協力が必要になるため、加盟国間の立法内容の接近等の調整が必要になってくる。この場合、EUは、条約の強い縛りの下に行動するとはいえ（EUの権限は、条約が権限を付与した場合に限り、しかも補完性の原則[7]、比例性の原則に従って行使することになっている（欧州連合条約5条)。)、拘束力を有する一定の立法的措置を取りうる。

こうした権限を有するEUの性格付けは複雑で興味をそそられる。EUは「それ自体は国家ではない、特異な越境的統治体制」である[8]、EU憲法を特徴付けるのは、憲法というよりは、むしろ「絶えざる憲法化のプロセス（continuous process of constitutionalisation)」である[9]という表現は、いずれも真実の一面を突くものだろう。実際、今日では、28カ国もの様々な加盟国から成る組織体であり、国家という枠組みでは捉えきれない存在である[10]。

このような組織と加盟国との権限がどのように取り扱われるのかについて、軽々な判断はできない。国家としての色彩が強いアメリカのような連邦制国家のもとですら、修正条項の解釈等をめぐって連邦主義と反連邦主義の深刻なせめぎ合いが生じるように、EUの枠組みを

決めているリスボン条約の解釈をめぐっても、EUの権限と加盟国の権限の間で紛議が生じることは想像に難くないし、また、リスボン条約自体、未だヨーロッパの統合の最終の到達点であるともいえない。

そして、リスボン条約のもとでは、消費者保護に関する問題はEUと加盟国の「共有権限」とされているが（欧州連合運営条約第4条2項）、本稿の対象であるクレジットカード犯罪対策やID窃盗対策は消費者保護の問題にも関係する。

さらに、クレジットカード犯罪対策、ID窃盗対策が越境的な性格をもつ限りでは、「共有権限」の対象だから（同条約83条1項）、EUの側に立法的介入の手がかりはある。

実際、後述のように、EUの政策的選択肢の一つして、ID窃盗について指令を出すという選択肢がありうる選択肢の一つとして検討されてもいる。また、その際、EUが介入できる根拠として、EU条約で認められるEU市民の諸基本権が参照されていることから、EUと加盟国の間の権限関係が解決済みで疑義を挟む余地のないものとはいえないことがうかがえる[11]。

このEUと加盟国との関係についての制度的枠組みを簡単に確認したうえで、Ⅲで本稿のテーマであるID窃盗に対するEUの対応について検討を加えて行きたい。

2. EUの枠組みと刑事司法協力の分野におけるEUの権限

EUの仕組みを理解するには、その沿革についての最低限の理解のあることが必要であるから、簡単に触れておく。

EUはヨーロッパの地域統合体（2013年現在28カ国）である。スイスが加盟国でないように、（我々が思い描く）ヨーロッパ＝加盟国というわけではない。EUは、マーストリヒト条約（1993年発効）により設立されたが、その後、リスボン条約（2009年発効）により、欧州議会の権限が大幅に強化されている。現実の政治的プロセスは複雑で紆余曲折は避けられないとしても、従来の、分野によって統治構造を異にしていた三本柱の統治構造（共同体型統治、政府間協同型統治、混合型統治）は廃止され（Elimination of the three-pillar system）、統合の方向に大きく進んできている。

このリスボン条約のもとでのEU の枠組みは以下のようなものである（リスボン条約を整理した統合版欧州連合条約（Consolidated Versions of the Treaty on European Union）及び統合版欧州連合運営条約（Consolidated Versions of the Treaty on the Functioning of the European Union）により、EUの権限と加盟国の権限について、規定を引用しながら、概観しておこう（訳文は、条約集を参考にしている）。）。

3. EUの立法権限と加盟国の立法権限

(1) 連合の権限と加盟国の権限の関係

EUの立法権限の根拠は欧州連合条約4条、5条に規定されている。

欧州連合条約4条、5条でEUに権限が付与されていなければ、EUに権限はない。

欧州連合条約4条

1 第5条に従って、基本条約により連合に付与されていない権限は、引き続き加盟国に存する。

同条約5条

1. 連合の権限の限界は、権限付与の原則(principle of conferral)によって規律される。連合の権限の行使は、補完性の原則及び比例性の原則(principles of subsidiarity and proportionality)により規律される。

2. 連合は、権限付与の原則に基づいて、基本条約に定める目的を達成するために基本条約において構成国が付与した権限の範囲内においてのみ行動する。基本条約により連合に付与されていない権限は、引き続き構成国に存する。

(2) EUの権限——排他的権限、共有権限、補完権限——

また、欧州連合運営条約2条は、EU の権限を排他的権限、共有権限、補完権限の三つに整理している。

欧州連合運営条約2条

1 基本条約が特定の分野において連合に排他的権限を付与している場合、連合のみが、法的拘束力を有する法令を制定しかつ採択することができ、構成国は、連合によって権限が与えられるか連合の法令を実施する場合にのみ、法的拘束力を有する法令を制定しかつ採択することができる。

2 基本条約が特定の分野において構成国と共有される権限を連合に付与している場合、連合および構成国は当該分野において法的拘束力を有する法令を制定しかつ採択することができる。構成国は、連合が自己の権限を行使していない範囲内でその権限を行使する。構成国はまた、連合が自己の権限の行使の中止を決定した範囲内で、その権能を行使する。

・・・

5 特定の分野において、基本条約で規定された条件の下で、連合は構成国の活動を支援し、調整し、補完するための活動を行う権限を有するが、こうした権限は、この分野における構成国の権限に優先するものではない。・・・

以下略

(3) 排他的権限、共有権限、補完的権限の対象

では、EUの排他的権限、共有権限、補完権限の対象にはどのようなものが含まれているか。

排他的権限の対象は、(a) 関税同盟、(b) 域内市場の運営に必要な競争法規の設定、(c) ユーロを通貨とする構成国の金融政策、(d) 共通漁業政策に基づく海洋生物資源の保護、(e) 共通通商政策である。(欧州連合運営条約3条1項)。

共有権限の対象は、(a) 域内市場、(b) この条約で定める側面に関する社会政策、(c) 経済的、社会的および領域的な緊密化、(d) 海洋生物資源の保存を除く、農業及び漁業、(e) 環境、(f) 消費者保護、(g) 運輸、(h) 欧州横断ネットワーク、(i) エネルギー、(j) 自由、治安および司法の分野、(k) この条約で定める側面に関する公衆衛生問題における共通の安全関心事項である。(同条約4条2項)。なお、共有権限の場合、権限の競合が生じうるが、同条約第2条2項で「構成国は、連合が自己の権限を行使していない範囲内でその権限を行使する」と規定されているから、連合が共有権限を行使した場合には構成国の権限に優先するという考え方が前提になっているだろう。

補完的権限の対象は、(a) 人の健康の保護と改善、(b) 産業、(c) 文化、(d) 観光、(e) 教育、職業訓練、青少年、およびスポーツ、(f) 市民保護、(g) 行政上の協力が、その対象である (同条約6条)。

このように欧州連合運営条約4条2項 (j) 項により、「刑事司法協力」の分野 (同条約82条以下)、「警察協力」の分野 (同条約87条以下) が共有権限の対象となっている。

そして、その具体的規定の一つが、次に見る同条約82条以下の刑事司法協力である。

刑事司法協力の分野では欧州検察機構 (Eurojust) の任務が、警察協力の分野では欧州警察機構 (Europol) の任務がそれぞれ規定されている (同条約85条、88条)。

以下、刑事司法協力の分野の規定に絞って見て行くこととする。

(4) 刑事司法協力に関する規定

次に見るように、欧州連合運営条約82条以下の刑事司法協力の分野では、法律、規則を接近させることがその権限に含まれている。刑事実体法については、越境型の犯罪分野で共通の対応が必要な重大犯罪の場合、又は、調和措置が必要な分野での刑法の接近が不可欠の場合、指令で最小限の規則を制定する権限が認められている (同条約82条、83条1、2項)。他方、犯罪防止の支援については、法律規則の調和はその対象から除かれている (同条約84条)。

欧州連合運営条約82条

1 連合内の刑事事件における司法協力は判決および裁判所の決定の相互承認の原則にもとづいて行われ、また第2項および第83条に掲げる分野における法律及び規則の接近を

含む。（注　第2項は刑事手続に関する規定）

同条約第83条

1. 欧州議会及び理事会は、通常の立法手続に従って採択される指令によって、国境を越える犯罪分野において、犯罪の性質及び影響、並びに共通の基盤に基づいてそれらと戦わねばならない特別の必要性から、特に重大な犯罪の分野での犯罪の定義及び刑罰に関する最小限の規則を定めることができる。

　これらの犯罪分野は次の通りである。テロリズム、人身取引、女性及び子供の性的搾取、違法麻薬取引、違法武器取引、資金洗浄、汚職、支払手段の偽造、コンピュータ犯罪及び組織犯罪である。

　犯罪の変化にもとづいて、理事会はこの項で定められた基準を満たす他の犯罪分野を特定する決定を採択することができる。理事会は欧州議会の同意を得た後に全会一致で議決する。

2. 構成国の刑法及び刑法上の規則の接近が、調和措置を条件とする分野での連合による政策の効果的実施を確保するうえで不可欠な場合、指令によって、当該分野の犯罪及び刑罰の定義に関する最小限の規則を制定することができる。こうした指令は、第76条を害することなく、当該調和措置の採択の場合と同じく、通常の若しくは特別の立法手続により採択される。

同条約第84条

　欧州議会及び理事会は、通常の立法手続に従い、犯罪防止の分野における構成国の活動を促進し、支援する措置を確立することができる。ただし、構成国の法律及規則のいかなる調和も含まれない。

(5) EUの刑事司法協力

EUの刑事司法協力からカード犯罪に関する部分を抜き出して要約すると、次のようになる。

欧州連合運営条約83条は重大犯罪領域の刑法の最小限調和について規定しており、同条によると、EUは、「指令」[12]により、支払手段の偽造、コンピュータ犯罪、組織犯罪等の「国境を越える刑事問題において、特に重大な犯罪の領域について犯罪の定義および刑罰に関する最小限の準則」を定めることができる。また、加盟国間の法令を「接近」させることも司法協力の対象となっている（同82条、83条2項）。

ただし、犯罪防止については、支援等の措置は行うが、この犯罪防止の領域では、法令の調和は刑事司法協力の対象から除かれている（同84条）。

また、この分野の立法権限については、欧州連合運営条約上、次のような特徴がある。通常、EUの立法提案権は欧州委員会にあるが、刑事司法協力、警察協力については、加盟国群（加

盟国の4分の1）にも提案権があるので（同76条）、加盟国側にも一定の範囲で権限が留保されている。この点では、他の分野の立法権限とは異なる特徴がある（刑事司法協力、警察協力という司法・治安の分野は、マーストリヒト条約の時代には、三本柱の一つとして政府間協定型統治若しくは混合統治型統治に属していた。リスボン条約のもとでも、外交と並んで、その枠組みが完全に払拭されているわけではないということであろう。）[13]。

Ⅲ．EUのID窃盗対策 ― EUのID窃盗対策の具体的内容 ―

1．ヨーロッパにおける規制の重点　CNP取引におけるカード犯罪規制へ

Europolの分析からも、EMVカードの普及の結果、ヨーロッパにおけるクレジットカード犯罪対策の重点はカード提示型カード犯罪からカード非提示型カード犯罪に移ってきていることがうかがえる。

ヨーロッパ各国のID窃盗の概況については、欧州委員会の見解をまとめるための準備作業としてなされた、「ID窃盗およびID窃盗関係犯罪に対処するための立法的手段及び立法以外の手段に関する比較研究」（以下、「ID窃盗比較研究報告書」と略する）[14]は、各国（アメリカ、カナダ、オーストラリア、日本、中国、インド等も含んでいる）の資料を網羅的に収集しており、現状把握に便利である（報告書自体は、資料を含めると600頁以上もある大部のものである。）。

この報告書（41頁以下）から、EU加盟国の一般的傾向を掴むことができる。各国の立法状況が表になっているので、これを右に掲げておこう。

Table 11 Overall country comparision

Country	Specific ID theft law ?	Relevant provisions in criminal law ?	Case law ?	Specific dedicated reporting point ?	Public awareness campaign ?
Australia	✓	✓	×	✓	✓
Austria	×	✓	×	×	×
Belgium	×	✓	✓	×	✓
Bulgaria	×	✓	✓	×	×
Canada	✓	✓	×	×	×
China	×	✓	✓	×	×
Cyprus	×	✓	×	×	×
Czech Republic	×	✓	✓	×	×
Denmark	×	✓	✓	×	×
Estonia	✓	✓	✓	×	✓
Finland	×	✓	✓	×	×
France	✓	✓	✓	×	✓
Germany	×	✓	✓	×	✓
Greece	×	✓	✓	×	✓
Hungary	×	✓	✓	×	×
India	×	✓	✓	×	×
Ireland	×	✓	✓	✓	×
Italy	×	✓	✓	×	×
Japan	×	✓	✓	×	✓
Latvia	×	✓	×	×	×
Lithuania	×	✓	×	×	×
Luxembourg	×	✓	✓	×	✓
Malta	×	✓	✓	×	×
The Netherlands	×	✓	✓	✓	✓
Poland	×	✓	✓	×	×
Portugal	✓	✓	✓	×	×
Romania	×	✓	✓	✓	×
Russian Federation	×	✓	✓	×	×
Slovakia	×	✓	✓	×	×
Slovenia	✓	✓	✓	×	×
Spain	×	✓	✓	×	×
Sweden	×	✓	✓	×	✓
United Kingdom	×	✓	×	✓	✓
Unites States	✓	✓	✓	✓	✓

規制の現状認識についてはこの報告書が重要だが、これに対する政策提言については、この報告書の提言とこの報告書をベースに作成されたEU の政策提言との間には少しずれがある。EUの政策は、後述のように、この報告書の提言よりはEUの関与をもう少し強く認めて行きたいというニュアンスを読み取れる。

2. ID窃盗比較研究報告書の概要

「ID窃盗比較研究報告書」の結論の要約部分を以下に紹介しておこう[15]。

ID窃盗に対する規制の現状はどのようなものか。

立法について見ると、EU加盟国でID窃盗を特に処罰している国は少ない。加盟国の多くは、詐欺罪、偽造罪、サイバー犯罪立法のような伝統的刑罰法規を使ってID窃盗に対処している[16]。

判例について見ると、特別の刑罰法規がないため、困難に直面しているという事態は生じていないようである。多くの国では詐欺罪の規定を使ってID窃盗に対処しており、ID窃盗について立法に穴があるという状況ではない。

犯罪の重大性、刑罰の重さとのつり合いという点について見ると、この点については不均衡な状態であることは明白である。こうした不均衡は個別事案の特殊性により生じていると理解できる事案もあるが、しかし、基本的には、適切な刑罰がどの程度かについての選択が加盟国の判断に委ねられていることにより生じているのではないかと考えられる。もつとも、こうした不均衡は、刑事立法一般に見られる問題であり、ID窃盗に限って生じているわけではない。

従って、当報告書は、EU としてID窃盗対策のため特に行動する必要があるという考え方には与しない。ID窃盗がおよそ処罰されていないという事案は見当たらないからである。

ただし、報告制度については、加盟国の対応は非常にまちまちな状態である。越境型のID窃盗にいたっては、ほとんど報告すらなされていない。この点は改善の余地があろう。

加盟国間にID窃盗についての共通のアプローチといったものは存しないものの、詐欺、偽造、データ保護については加盟国間に類似の規制が既に存在する。これらの規制は、全体としては、ID窃盗に対する規制としても十分に機能しており、実務的な観点から、あらたな犯罪化が必要であるという要請は存しない。

弱点と提言

しかし、現在の規制が以下のような問題点を抱えていることは見落とすべきでない。

①規制に穴があるという点についての共通認識が加盟国に存しない。一カ国（フランス）は加盟国間にギャップがあると認識しているが、他方、加盟国の多くはそのような認識を有していない。

②詐欺、偽造、その他のコンピュータ関連犯罪といったID窃盗に適用可能な刑罰法規についてはどうか。これらの刑罰法規が、加盟国間で完全に調和した状態にあるとはいえない。

そうなっているのは、加盟国の刑罰法規を完全に一致させるのではなく、規制内容をできるだけ接近させるという政策手法が採用されてきた結果でもある。その副作用として、ある加盟国においては一定の段階のID窃盗が違法とされているのに、他の加盟国においてはそうでないという事態が生じている。

③データ保護規定によるセーフティ・ネットは、理論上、加盟国の執行戦略の実効性に左右される問題だが、今のところ、こうした執行戦略については、一定の標準というものが存しない。

立法

ID窃盗対策立法について加盟国間にギャップが存するかは明確ではない。この問題は、ID窃盗をどのように犯罪化するか、とくに被害者に実害が発生していない段階での介入についてどう考えるか、現行法がこの部分をカバーしていない場合にどのように対処するか、そして、どこまでを犯罪化すべきかによって結論が変わってくる性質の問題である。

フランスが採用しているような広汎な規制を導入することは（注19参照）、規定の文言の解釈が分かれることになってしまうので、他の加盟国からは支持されていない。結果として、現段階では、ID窃盗の定義と範囲について、加盟国間の合意を得ることは難しい状況にある。

判例

判例の状況はどうか。今のところ、事例は多くないものの、規制に穴があると考えるべき根拠は見当たらない。しかし、刑の重さについては、加盟国間に大きな差が出ていることは明白である。しかし、これは他の犯罪についてもいえることであるから、これだけを取り出して問題にすべきであるとはいいにくい。

報告制度

犯罪被害者等がオンラインで被害を報告する制度をもつ加盟国は多いが、他方、IDが窃取されたID窃盗の段階でも報告する制度をもつ加盟国は少ない。

すなわち、加盟国の多くは、ID犯罪にあたるという場合でなければ、あるいは、データ保護規定違反にあたるという場合でなければ、ID窃盗について報告されない。報告されている事例の多くは、ID窃盗またはプライバシー侵害も伴っていたと考えられる。

グッド・プラクティスという観点からは、最低限、ID窃盗の段階であっても報告できるオンラインの報告制度を整備することが適切である。そして、将来的には、オランダのように、報告があった場合にはその調査結果を被害者に回答するという、双方向型の仕組みを導入す

ることが検討に値する。

また、越境的な捜査の観点からは、各国の報告制度を欧州レベルの報告制度へと統合することが可能になるように仕組みを整備することが望ましい。

統計的なデータの組織的収集も望ましい。現時点では、一国のレベルでも統計データを利用できていない状況である。まして欧州レベルでの統計的データの比較となると、現時点ではほとんど絶望的な状況にある。この点は改善が望ましい。

提言

ID窃盗に対しては、「非立法的手段」による規制が優先されるべきであるし（EUの立法行為については注12参照）その必要性も高い。現時点ではID窃盗についての共通の理解は存しないから、今のところ、汎ヨーロッパ的な立法は難しく、またかりに犯罪化した場合には、他の犯罪との間で重複が生じ、かえって混乱を招いてしまう。そうした混乱を招くよりは、加盟国にあっては、ID窃盗の処罰に際しても、自国の刑法との体系的一貫性を保つほうが重要である。

3. EUの基本政策（戦略・評価センター（CSES）最終報告書）

上のⅢ-2で紹介した「ID窃盗比較研究報告書」（2011年）をもとに作成されたのが、戦略・評価センター（CSES）の「ID窃盗に関する新たな枠組みの提案の効果測定に関する研究」最終報告書（2012年）[17]（以下、「CSES最終報告書」として引用）である。

この「CSES最終報告書」から、EUが、ID窃盗についてどのような政策で臨もうとしているのかを知ることができる。

「CSES最終報告書」は、EUレベルでID窃盗の分野における立法的手段の導入が適切か、それとも、ID窃盗に対処するため、立法以外のより効果的な手段があるかという問題について詳細な検討を加えている。同報告書では、その検討を踏まえて、欧州委員会の決定の参考に供するためいろいろな政策オプションについて効果測定を行い、その検討結果が示されている。従って、ここから、ID窃盗に対するEUの基本的姿勢とその考え方を窺うことができる。

この「CSES最終報告書」は、新たな立法的手段の採用に懐疑的であった「ID窃盗比較研究報告書」と比較すると、立法的手段の採用までは提案していないものの、立法的手段の採用にかなり好意的な立場を採っていることが、記述の端々から伝わってくる。

同報告書の概要（Executive Summary）を以下に紹介する。検討の手法には参考にすべきものが含まれているだろう。

(1) 第一次被害者（消費者）と第二次被害者（企業等）

ID犯罪については、第一次被害者（primary victim）と第二次被害者（secondary victim）を区別して問題を検討する必要がある。

悪用するために個人識別情報が盗取されると、（盗取した者自身が悪用する場合であろうと、これを譲り受けた第三者が悪用する場合であろうと）私的部門（個人、企業）、公的部門に影響を与える[18]。

ここでは、盗取された個人識別情報が濫用されることにより生じる被害について、本人である第一次被害者と、第一次被害者になりすました行為者が、詐欺その他の手段を用いて損害を与えた第三者である第二次被害者とを区別して検討する必要がある。（報告書サマリー1）

動機についてみると、犯罪者が個人識別情報を取得しようとする動機は主に金融詐欺と資金洗浄である。

その他、人身売買、個人識別情報の売買目的のためにも行われているが、これらが主たる動機で個人識別情報が取得される場合というのは、実は、それほど多くはない。それ以外にも、健康保険診療の違法な受診、組織犯罪、テロ、薬物取引、不法入国、いじめや他人の社会的評判を落とす等の犯罪目的でも個人識別情報が取得されている。（報告書サマリー1-1）

私的部門の一つである個人に対する影響について見ると、被害は、平均して、EUの人口の2％にあたる820万人がID窃盗の被害を受け、その被害額は、平均2500ユーロ、EU全体では200億ユーロにのぼっている。

個人については、こうした経済的損害だけでなく、ストレスや社会的評価の低下といった非経済的損害も被っている。従って、ここでは、EU市民の基本権侵害の問題も重要な論点となってくる。

私的部門に属する欧州企業に対する影響についての調査はほとんど行われていない。従って、その規模を見積もることは難しいが、5000億ユーロ、EUのGDPの0.4％程度にのぼるのではないかと見積もられている。欧州企業は、第一次被害者でもあり、また第二次被害者でもあるが、後者の第二次被害者としての損害の測定は比較的容易に行える。

私的部門の被害額の測定については、いくつかの加盟国には参考となる数値が存在する。

イギリスでは、2009年に、小切手詐欺（盗難にあった小切手で詐欺犯人が署名して行使した真正の小切手）の被害は195億ユーロに、プラスチックカード、オンラインまたは電話による銀行詐欺の被害は6,240億ユーロに、ID窃盗関連の詐欺による電気通信産業の被害は、8,300億ユーロにのぼっており、これが被害額の想定の手がかりとなる。

公的部門である公的機関も、違法アクセスや公文書偽造の態様で公的機関自身の個人識別情報が利用されており、ID窃盗の被害に遭っている。また、公的機関自身の個人識別情報は、

公的機関が管理する個人データを違法に取得するためにも利用されている。

調査結果の示すところでは、ID窃盗は増大し続けており、欧州全体、さらには国境を越えたレベルにまで拡大していることが明白である。

非経済的損失について、もう少し見ておこう。

個人には、次のような非経済的損失が生じている。悪用された個人識別情報をクリーンにするため、また、悪用されたため不法行為として紛争に巻き込まれてしまい、費やすことになった時間、費用といった手間もこうした非経済的損失にあたる。また、個人の心理的負担、社会的困難、信用、データやプライバシー関係の基本権の制限も非経済的損失である。(報告書サマリー2-2)

(2) 加盟国の立法状況

加盟国の立法態度

現在のところ、ID関連犯罪、ID窃盗について特別の刑罰法規をもつ加盟国は少数である。

2011年に行われた比較研究(「ID窃盗比較研究報告書」)によると、特別の刑罰法規を有しているのはエストニア、フランス、スロバニアの三国だけで[19]、同研究報告書発表後に、ポーランドであらたな立法(2011年)があったというだけである。もっとも現行法でID窃盗に十分に対処できていると自認している加盟国は少ない。(報告書サマリー2)

加盟国の多くは、詐欺罪、すなわち第二次的に行われる犯罪に対する刑罰法規により、ID窃盗に対処してきている。ベルギー、チェコ、ブルガリア、ドイツ、イギリスがそうである。従って、ID窃盗罪の規定が存しないからといって、そのような加盟国で、ID窃盗が犯罪とされていないとは言い切れず、多くの加盟国では、特別の刑罰法規を用いて処罰するのではなく、詐欺罪や偽造罪の規定により処罰しているのである。そのため、ID窃盗を処罰している場合でも、ID「窃盗」として言及されるのではなく、むしろ、詐欺罪として扱われている。

もっとも、単なる個人識別情報の「窃盗」だけでは未だ可罰的な犯罪になるとは考えられておらず、むしろ、取得された個人識別情報を違法に利用する段階ではじめて可罰的な犯罪になると考えられている。このように、ID窃盗は予備段階の行為として把握され、それ自体で犯罪に値するものとは考えられていない。

被害の回復措置

また、回答のあった18加盟国中、3加盟国(チェコ、イタリー、アイルランド)のみが、第二次的犯罪が行われる以前の段階でも第一次被害者の保護がなされていると回答している。

それ以外の加盟国の立法状況ははっきりしないが、第一次被害者については、一定の場合に損害を回復できる機会が与えられているにすぎないという状況にある。加盟国の多くは、第一次被害者が受けた損害については、盗取された個人識別情報を用いたあらたな犯罪が行われた後ではじめて被害の回復措置が行われている。

ID窃盗の定義

現在のところ、EUには、ID窃盗現象を記述する共通タームは存在しない（加盟国では、「ID窃盗」、「ID詐欺」、「ID関連犯罪」といった用語が用いられている）。従って、EU共通の法的定義も存在しない。（CSES最終報告書サマリー2-1）

ID窃盗に対するEUレベルの戦略を発展させる際、共通の定義が存在しないことが問題を錯綜させている。従って、共通の定義があることが望ましい。しかし、専門家によれば、 ID窃盗の定義の内容、範囲について、加盟国間の合意を得ることは非常に難しい状況である。従って、今の段階で可能なことは、法的拘束力をもつ規定を導入することではなく、ガイドラインを提示する程度のことである。専門家のなかには、できるだけ操作性のある、包括的な共通の定義を作ることを提案する者もいる（その専門家は、ID窃盗の共通の定義に際して、要件として「不実な意図」（dishonest intent）という文言を含むよう提案している。）。

いずれにしても、ID窃盗に関するEU全体の法的枠組みを考えるに際しては、調和のとれた一貫した枠組みを提示する必要がある。また、それにとどまらず、このID窃盗現象に対処するために採用されるべき実践的手段も考えておく必要がある。

EUの定義を作る際、次の二つの選択肢が考えられる。すなわち、ID関連犯罪についての完全に機能する共通のEUの定義をつくるか、それとも、基本原則に焦点を当てた、より柔軟な定義をつくるか、という二つの選択肢である。

最初の完全に機能する定義を作成するという第一のアプローチをとるなら、犯罪化する必要のある行為の性質を厳密にして明確化することができるし、また、行為の結果に基づくのではなく、行為そのものに着目して明確なものとすることができるから、対象の捕捉、監視も行いやすいという長所がある[20]。

第二のアプローチをとるなら、各加盟国では、自国の法制度と矛盾しないかたちでID窃盗を定義する余地が残されることになる。この報告書では、最終的に、この第二のアプローチに沿って、ID窃盗を定義している[21]。（CSES最終報告書サマリー2-2）

(3) EUの政策目的

EUがID窃盗の問題に介入する根拠はどこにあるか。

ID窃盗が多くのEU市民の生活に影響していること、および、これに効果的に対処するには、EUレベルでの行動が必要となっていることを挙げることができる。

この点に関するEUの政策目的を、一般目標と個別目標に分けて示すなら、次のようになる。

一般目標としては、

ID窃盗、ID関連窃盗を規制すること、より一般的には、安全を促進し、犯罪に対処することで、被害者の権利を護ることである。

個別目標としては、

①ID窃盗、ID関連窃盗を減少させること、

②公的部門、私的部門で、ID窃盗、ID関連窃盗を防止し、これに対処する能力を向上させること、

③ID関連窃盗による第一次被害者、第二次被害者に対する支援と救済を用意すること、より一般的には、次のような基本権を保障することーー(1)自由と安全に対する権利(6条)、(2)私人及び家族に対する尊敬（7条）及び個人情報の保護（8条)、(3)財産権（17条)、(4)（オンライン、オフラインのショッピングの中で取得されて濫用される結果、消費者の保護に否定的な影響を及ぼすことから、基本権でもある）消費者の保護（38条)、(5)効果的な救済と公平な裁判に対する権利（47条）ーー[22]、

④企業を保護すること、とくに大企業の保護をはかるというより、ID窃盗に弱く被害に遭いやすい中小企業の保護をはかること、

⑤ID窃盗、ID関連窃盗に関する基本的な知識を向上させること、

⑥EUにおけるID窃盗、ID窃盗関連の裁判管轄漁り（forum shopping）の危険を防止すること、である。(CSES最終報告書サマリー3-1)

(4) EUにおける政策の選択肢の検討と評価

このような問題に対処するための政策の選択肢にはどのようなものが考えられるか。それには、現状維持から、EU全体でID窃盗を犯罪化するという立法的介入まで、様々な選択肢がある[23]。

これらの選択肢を様々に組みあわせるなら、以下の四つの選択肢が考えられる。

①第1の選択肢は現状維持で、何もしないというものである。

介入するほどの問題ではないということなら、これでよいだろう。しかし、ID窃盗に対するこれまでの調査では、現状変更の必要があることは示されているし、専門家も、EUとして行動する必要があると提案している。(従って、この選択肢は採用できない。)

②第2の選択肢は、立法的手段は採らないものの、何らかの対処をするというものである。

最低限、この第2の選択肢までは採るべきだが、この選択肢には、さらに、次の5つのサブ選択肢が考えられる。

経験と知識を交流するため、被害者と専門家のためのオンラインのプラットホームを構築するという選択肢（2-1）、被害者支援のための連絡ポイントを構築するという選択肢（2-2）、共通の定義その他様々な手段について委員会として勧告するという選択肢（Commission Recommendation）（2-3）、非立法的手段である2-1と2-2とを組み合わせるという選択肢（2-4）、非立法的手段である2-1,2-2,2-3を組み合わせるという選択肢（2-5）である。

③第3の選択肢は、立法的手段による介入である。

この選択肢には、さらに、次の2つのサブ選択肢が考えられる。

第一次被害者に焦点を当てたID窃盗について指令を出すという、介入を最小限にとどめる選択肢（3-1）、第一次被害者と第二次被害者を対象とするID窃盗、ID関連犯罪について指令を出すという、介入を最大限に行うという選択肢（3-2）である。

④第4の選択肢は、第2の選択肢（2-1から2-5まで）と第3の選択肢のうち、3-1の選択肢（法的介入については最小限の介入にとどめるアプローチ）を組み合わせるという選択肢である。（CSES最終報告書サマリーとCSES最終報告書本文（118-119頁）とでは、選択肢の番号の付け方が異なっているので注意。）

これらの選択肢のどれとどれを組み合わせるかでどのような影響があるかを検討する必要がある。その検討結果を示したものが、この「CSES最終報告書」である。

上記のうち、第4の選択肢はもっとも効果的な手段であるが、EU レベルでID窃盗について共通の定義をするにはEU加盟国の合意が必要であり、残念ながら、その合意を取り付けることは難しい。そこで、「CSES最終報告書」は、現実的な選択肢である第2の選択肢を採用し、そのうえで、一歩一歩、第3の選択肢のほうに近づいて行くというアプローチが採用された[24]。

同報告書の各選択肢の政策について行われた効果測定の結果が、報告書のサマリーのなかで、表にまとめられているので次頁に示しておく（効果測定は、項目別に五段階の評価をし、そのスコアを合計するという手法で行われている。）。

(5) ID窃盗の定義の試み

これまで紹介してきた「CSES最終報告書」のなかで、議論を前進させるため、ID窃盗の定義（作業定義）などいくつの定義の試みが紹介されている。有益なので、以下に紹介し、

Summary of Key Impacts

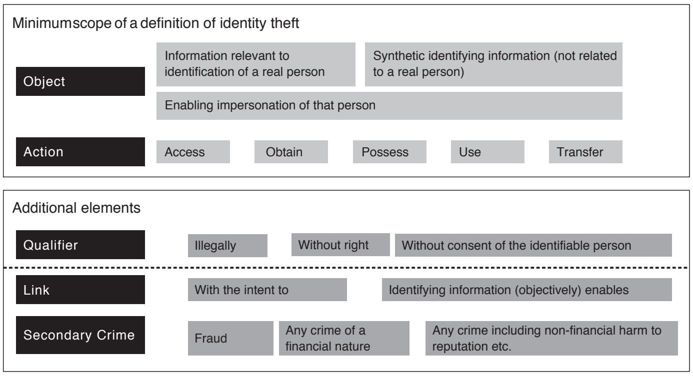
Key: ● = low score; ●●●●● = high score

Impact/Policy Options	2.1	2.2	2.3	2.4	2.5	3.1	3.2	4
Relevance	●	●●	●●	●●	●●●	●●●●	●●●●	●●●●●
Effectiveness	●	●●	●●	●●●	●●●●	●●●	●●●	●●●●●
Efficiency	●	●●	●●	●●●	●●●●	●●●	●	●●●●●
Impact and added value	●	●●	●●	●●●	●●●●	●●●	●●●	●●●●●
Feasibility	●●●●●	●●●●	●●●	●●●●	●●●	●●	●	●●

最後に同報告書の作業定義について少し詳しく紹介しておく。

ID窃盗の定義に際しては、①最低限の要件として、客体（Object）、行為（Action、具体的には、アクセス、取得、所持、利用、移転）と、②加重要件として、限定要素（Qualifier）、その他の犯罪との連関（Link,Secondary Crime）に分けて、次の図のように整理がなされている。この整理は、今後、この問題を考える際の参考になるだろう（CSES最終報告書9頁）。

Figure 2.1: Key elements in defining identity theft for the purpose of a leagal provision



Source: European Commission, January 2012

また、ID窃盗についての定義について共通の理解が存在しないことを前提としつつ、定義を作成する参考にするため、OECDの次のような定義も紹介されている（CSES最終報告書11頁）。

「詐欺その他の犯罪を遂行する意図で、または、その一環として、権限がないのに、自然

人若しくは法人の個人情報を取得、移転、所持または利用した者は、ID窃盗を行うものである。」(Identity theft occurs when a party acquires, transfers, possesses or uses personal information of a natural or legal person in an unauthorised manner with the intent to commit, or in connection with, fraud or other crimes.)

この定義について少しコメントしておこう。ここではID窃盗について、広い定義が採用されている。それでも、詐欺その他の犯罪を遂行する意図のあることが必要とされており、この定義では、(意図のない)単なる個人識別情報の窃取のみでは犯罪を構成しないことになっているし(個人識別情報を窃取するにとどまる行為を処罰すべきか否かは難しい政策的論点である)、他方、詐欺等の第二次的な犯罪を実際に行うことが成立要件となってはいない(わが国の目的犯の立法技術を採用するアプローチといってよいだろう。)。また、この定義においては、いったいどのような場合が、権限のない取得、利用に該当するのかについて触れるところがない。

更に、「CSES最終報告書」の別の箇所では、OECDによる、別の、もう少し詳しい次のような定義も紹介されている(17頁)。

「利益を得る目的、自己が利益を得る若しくは他人に利益を得させる目的、または、他人に損害を生ぜしめる若しくは他人を損害の危険にさらす目的をもって、その他人になりすます意図で、権限がないのに、自然人若しくは法人の個人情報を取得、移転、所持または利用した者は、ID窃盗を行うものである」(Identity theft occurs when a party acquires, transfers, possesses or uses personal information of a natural or legal person in an unauthorised manner with the intent to make a false representation as to his identity in order to make a gain or acquire a benefit for himself or another or to cause loss to another or expose another to a risk of loss.)。

こうした紹介を経たうえで、「CSES最終報告書」は、次のような作業定義を提案している(丸括弧の部分は、読みやすくするため補った)。

この作業定義は要綱案のようなものであるが、例示されている部分をあわせ読めば、ID窃盗の問題の所在が的確に掴めるだろう。また、この定義の主観的要素と行為とを対比しながら読むなら、同定義は、ID窃盗行為の本体を「利用」に求めており、「取得」、「移転」、「所持」はその前段階の行為として理解されている。また、「移転」の概念は、所有権的イメージというよりむしろ利用権的イメージのもとで、その意義が捉えられている。

ID窃盗の作業定義（Working Definition）

（主体）

「[一人による場合であれ、集団で行う場合であれ］何人も、

（無権限性）

［例えば、ホテル受付の会計係が精算するために手渡されたクレジットカードのコピーを作成する場合のように］権限がないのに、

（客体）

自然人若しくは法人の［氏名、パスポート番号、生体識別情報、クレジットカード情報、利用者名及び暗証番号、社会保障番号のような］個人情報を、

（主観的要素（目的、故意））

(a)［例えば、他人のクレジットカードで商品を購入して］利得する、

(b)［例えば、高額のオンラインデータベースその他の資源にアクセスすることにより］自己が利益を得る若しくは他人に利益を得させる、

(c)［例えば、本人の口座から現金を引き出すことにより、本人の信用情報を毀損することにより、または、本人が犯罪が行われる以前の状態に戻すために相当の努力が必要になるような状況に被害者を陥れることにより］他人に、直接もしくは間接の損失を引き起こす、

(d)［例えば、他人のクレジットカード情報を第三者が濫用できるよう掲示することにより］他人に損失が生じる危険を生じさせる、

(e)［例えば、中傷的文言を掲示することにより］他人の名誉を毀損する、

(f)［上述の方法により］他人にその名誉が毀損される危険を生じさせる、または、

(g)［例えば、犯罪を行う際に、他人の個人情報を使用して警察にその者が犯罪を行ったと信じさせることにより］犯罪捜査を攪乱する目的のため、

本人になりすまして虚偽の申し出をする（make a false representation as to his identity）意図で、

（行為[25]）

(a)［例えば、コンピュータシステムに侵入する方法により、もしくは、ゴミ箱から書類を収拾する方法により］取得（acquire）、

(b)［例えば、不法に得られた個人識別情報データベースに他人が（有料で）アクセスすることを認めることにより］移転（transfer）、

(c)［例えば、クレジットカード記録を保持することにより］所持（possess）、または、

(d)［例えば、権限のある本人であることを装うことにより］利用（use）

した者は、

ID窃盗（Identity theft）を行うものである。」

さらに、「CSES最終報告書」は、続けて、ID窃盗、ID詐欺、ID関連犯罪と第一次被害者、第二次被害者との関係については、各国の立法態度が様々であることから、この点について詳細な紹介を行っている。また、ID窃盗の特別規定を有する加盟国の立法も紹介している(11-14頁)。この点について紹介する紙面の余裕がないので、言及するにとどめておく（ネット上で見ることができる)。

4. 国連（ID関連犯罪専門家会議の活動）の報告書が紹介するEUの動き

最後に、国連の専門家会議の報告を用いて、EUや国際機関の協調に触れる部分及びID関連犯罪のモデル草案についての最近の動きについて紹介したい。そうすることで、本稿で紹介してきたEUの動向についての理解の妥当性を（ほとんど紹介されたことのない領域だろう)、異なる資料を用いて裏付けておきたい。

国連の活動については、それだけでも本格的な検討が必要だが[26]、本稿の射程を超えるので、以下では、EUの活動を知る手かがりとなる部分に限って紹介しておく（報告自体は、ネットで入手できる。)。

2013年の国連犯罪防止刑事司法委員会の専門家会議（the core group of experts on identity-related crimes）の報告書では、ID関連犯罪（identity-related crimes）について次のような指摘をしている[27]。

ID関連犯罪の最近の動向としては、クレジットカード、商品やモバイル電話の購入、銀行口座の開設を対象として行うのがID関連犯罪のもっとも一般的な姿であるが、その犯行の手口はウィルスを利用するものから、ロボットサーチの弱点を突いたスキャニングを利用するものに移行してきていることに注意を促している（2013国連レポート8頁)。

また、EUや国際機関の活動が協調しながら対策の検討が進められていることが指摘されている。この点は本稿で検討してきたEUの活動の現状の理解にも資するので、以下で紹介しておこう（「2013年国連レポート」8頁)。

EU内では刑法は主として加盟国による立法に委ねられている。リスボン条約による改革は、はじめて、EUがサイバー犯罪を含む刑法の領域で単なる政府間協力にとどまらない強力な命令をなしうる余地をつくりだした。現在、児童ポルノ規制と情報システムへの攻撃に対する規制の草案作りが進んでいる。同様に、個人識別情報に関連する国境管理に関する措置も、リスボン条約（欧州連合運営条約77条）によりEUに権限が認められている。

EUの2010年から2014年までの五カ年のアクションプランを策定したストックホルム・プログラムでは、サイバー犯罪、ネット上の情報の安全を確保するためのあらたな立法提案について検討することになっている。

これに基づき、欧州委員会（EC）の政策立案のため、2011年報告書（「ID窃盗比較研究報告書」）、2012年報告書（「CSES最終報告書」）が提出された。続けて、EUとITU（国際電気通信連合）が協力して、各国のサイバー犯罪立法を調和させるための活動を行っていることが紹介されている。（「2013年国連レポート」8頁）

ID関連犯罪の規制については、ID窃盗のライフサイクルに即して、個人識別情報の取得から、その濫用を経て、被害者が損害を被る経済的利益の取得までという、ID窃盗ライフサイクルに即して戦略を立てる必要があり、予防、損失の救済、積極的な訴追処罰による抑止により、対策を強化して行くことの重要性が強調されている。（「2013年国連レポート」10頁）

同会議では、ID関連犯罪の防止、捜査、訴追、処罰のための、下記に見るようなモデル草案の骨格について検討し、さらに検討のためのチェックリストが作成されている[28]。

まず、このモデル草案の実体法部分の骨格を、以下に紹介しておく[29]。

ID関連犯罪の規定にあたっては、用語の定義が不可欠である。identity自体を定義することは措くとして、identityを特定する手段、その利用及び移転については定義しておく必要がある。

また、実体刑法部分については、オンラインのID関連犯罪とオフラインのID関連犯罪を対象とした規定が必要である。また、ID関連犯罪（computer -related crime 国連レベルでは、よくこの用語が利用される。）は、ID窃盗とID詐欺の双方を含む。特定の犯罪については加重事由を用意する必要がある。

モデル草案には、偽造パスポートの作成のためのツールの作出、販売、輸入、輸出、所持のような予備段階の行為を犯罪化することができる規定も入れておく。

さらに、実体法以外の項目として、手続法、電子証拠、緊急の際の介入手段、報告義務、個人情報の保護、統計に分け、検討されている[30]。

続けて、各国が立法に際して配慮すべきチェックリストが掲げられているが、これは、ID関連犯罪の利害関係者、実体の側面、手続の側面に分け作成されている。

実体の側面についてのチェックリストだけ以下に簡単に紹介しておくと、同報告は、以下のような諸点に配慮すべきものとしている[31]。

①犯罪がもたらす脅威の評価、②関連情報の収集と分析、③優先順位の設定及び公的部門

と私的部門の協力、④立法に関し、犯罪化、法執行、国際協力、刑罰以外の行政的手法の可能性等の問題、⑤捜査及び法執行機関の能力、⑥犯罪遂行途中で速やかに介入阻止する活動を支援する方法、⑦教育啓蒙等の社会的予防、特定の者に対する情報提供等の環境による予防（situational prevention）、セキュリティ対策等の技術的予防、⑧被害者支援、⑨捜査要員、関係する公務員、私的部門の責任者の訓練、⑩対策を講じるための公的部門、私的部門の協力。

5. 最後に

以上、EU加盟国のクレジットカード犯罪対策において重要度を増しているID窃盗対策に対するEUの基本政策を検討してきた。

ID窃盗対策という具体的な問題についての政策の紹介であるが、その正確な理解のためには、法的枠組みとして立法的介入と非立法的介入という枠組みについて知っておく必要があるし、また、立法的介入にも、規則と指令という二種類の異なる介入の仕方があることを理解しておく必要がある。その制度的裏付けが条約に求められることから、本稿ではこの点についても紹介した。

本稿では、この特集の性格から、ID窃盗の現状を踏まえてはいるが、ID窃盗の現状の紹介は省いている。ID窃盗の現状については、Ⅰの3で紹介したEuropol、とくに2013年より活動を開始しているEC3のホームページに掲載されている諸報告書が有益である。ID犯罪の現状については、こうしたネット上の膨大な電子情報の参照が不可欠であろう。

［注］

1 OECD,Online Identity Theft,2009,p.15.,European Commission（N. Mitchison etc.）, Identity Theft A Discussion Paper, 2004.等

2 前掲（注1）Identity Theft A Discussion Paper, 2004, p.21.

3 Europolのもとに、2013年より、EC3（European Cybercrime Center）という組織が稼働している。EC3は、オンライン詐欺のような組織犯罪を対象として活動しており、EC3の活動を抜きにEUのカード犯罪対策とその実践について語ることはできない。その活動については、ホームページ等で確認できる（European Cybercrime Centre - First Year Report（2014/2））。

4 Europol Payment Card Fraud in the European Union Perspective of Law Enforcement Agencies,2012,p.7-12.

5 「欧州連合条約」、「欧州連合運営条約」の二つで、これはthe Treaties（「両条約」）と呼ばれているように（欧州連合条約1条、欧州連合運営条約1条）、「同一の」法的価値が認められている。これらに「欧州連合基本権憲章」をあわせた三つが、欧州連合の基本法である。

6 国の安全保障については加盟国の排他的責任として留保されているが（欧州連合条約4条2項）、これとは明らかに取り扱いが異なっている。

7 補完性の原則は、条約では、国家の主権から出発する説明の仕方というより、できるだけ市民に近いとこ

ろで決定が行われる（従って加盟国の権限が尊重される）という説明のされ方がなされている（欧州連合条約前文)。考え方としては興味深い。

[8] 衆議院憲法調査会事務局「欧州憲法条約—解説及び翻訳—」衆憲資第56号（委託調査報告書（中村民雄））3頁平成16年9月。

[9] Kaarlo Tuori,Klaus Tuori, “Eurozone Crisis：A Constitution”, 2013序章（Introduction）

[10] 国家と違って、EUの場合には基本政策を実現、貫徹するための担保となっているのは加盟国の実力に裏付けられた権力であって、EUのそれではない。

[11] 基本権を根拠とするなら、基本権を擁護する必要がある場合、EUの介入の口実はいくらでも考えられるだろう。立法的措置の根拠付けとして基本権への言及がなされているのは、このことを物語っている。そのこともあってか、わざわざ、欧州連合基本権憲章は「両条約に定める連合の権限をいかなる形でも拡大しない」と規定して（欧州連合条約6条)、この点に釘を刺している。(政治プロセスの問題としては興味深いが、リスボン条約は欧州連合における欧州議会の権限を強化する一方で、法的拘束力をもつものとして欧州連合基本権憲章を取り込んでいる（結果として、欧州司法裁判所は、この欧州連合基本権憲章上の人権侵害があると認めた場合、加盟国の裁判所の決定を覆しうる権限を有することになる)。)

[12] EUの立法行為には、「規則」、「指令」、「決定」がある。このうち、前二者（規則、指令）は一般に適用される規範という性質をもつている。

規則（Regulation）は、全面的な拘束力があり、すべての加盟国に適用可能な性質の立法であり、指令（Directive）は、達成されるべき結果については拘束されるが、その形式、方式の選択については構成国に委ねられている（欧州連合運営条約288条)。

両者の違いはどのようなものか。かりに指令により、ある偽造行為の処罰を求めた場合、これを詐欺罪で処罰するか、偽造罪を別罪として取り出し、両罪を牽連犯等として処罰するかの選択については加盟国に委ねられることになるということであろう。

[13] 本稿の脱稿後に刊行されたもので、末道康之「フランスにおける欧州刑法をめぐる最近の議論」『理論刑法学の探求』7号（成文堂、2014年)、275頁以下の紹介は有益である。

[14] NEIL ROBINSON, HANS GRAUX,DAVIDE MARIA PARRILLI, LISA KLAUTZER AND LORENZO VALERI, Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime：Final Report,2011.（「ID窃盗比較研究報告書」）

[15] 「ID窃盗比較研究報告書」（前注）114頁以下

[16] 個人識別情報を単に取得するという段階の行為について、それだけでも犯罪になると考えている国とそうでない国とがある。

[17] CSES, Final Report Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft,2012

[18] シナリオを用いた部門毎の未来予測として、Project 2020 Scenarios for the Future of Cybercrime - White Paper for Decision Makers, International Cyber Security Protection Alliance（ICSPA）

[19] 本稿の対象から外れるが、参考のため、フランス刑法226-4-1条を紹介しておこう（同条は、私生活、プライバシーに対する罪（De l'atteinte la vie privée）として把握されているが、個人識別情報を用いて「情報」を利用する行為が広く規制対象となっているため、結果的には、広い範囲の行為を規制できるものとなってしまっている。当初の法案では「情報」ではなく「被害者の個人情報」を対象としていた｡)。

「その者若しくはその他の者の平穏を害する目的、または、その者の名誉若しくはこれに対する配慮を侵害する目的で、その者を詐称する（usurper l'identité）行為、または、当該情報の性質がどのようなものであれ、その者の個人識別情報（l'identifier）を用いて一個若しくは数個の情報（données）を利用する行為は、1年の拘禁刑または15000ユーロの罰金刑に処する。この犯罪が公開されたオンライン通信網を用いて行われた場合も、同じ刑に処する。」

[20] EUの立法には、内容形式とも加盟国に拘束的に働く「規則」による場合と、達成すべき結果については拘束的だが、その実現方法については加盟国の選択に委ねる「指令」によるものとがある。ここでは、その違いを念頭に記述されている。(注12参照)

[21]「指令」による規制という選択が望ましいということを意味する。

[22] 基本権の保護とEUの立法権限との関係については、注11参照。

[23] 指令には達成しようという結果について拘束力がある。また、勧告（や意見）には法的拘束力は認められない。（欧州連合運営条約288条）

[24] 本文で触れたように、この最終報告書の基礎となった「ID窃盗比較研究報告書」（2011年）は、立法的対応については、この2012年の報告書より、もう少し否定的なニュアンスのものであったと思われる。

[25] 行為態様として、本文の4つの行為態様（「取得」、「移転」、「所持」、「利用」）のほかに、（取得の前に位置する行為である）「アクセス（access）」をあげる試み（3(5)に引用した図参照）もある（CSES最終報告書（注17）9頁）。

[26] この分野では、国際連合（UN）、経済協力開発機構（OECD）、国際電気通信連合（ITU）、欧州評議会（Council of Europe）の活動とEUの活動との間に緊密な協力関係のあることが認められる。特に、ITUの活動は日本ではほとんど紹介されていないが、無視できない重みがある。また、欧州評議会のサイバー犯罪条約は我が国も批准しており、同条約とID窃盗との関係も大切な問題だが、本稿は、EUの活動の検討に絞っているため、紹介を省略する。

[27] Report of the sixth meeting of the core group of experts on identity-related crime, E/CN.15/2013/25,2013（以下、「2013年国連レポート」として引用）

[28] このモデル草案の骨格は、個人識別情報の取得という早い段階の犯罪化の必要性があるという立場に立つ、ケルン大学のProf. Gerckeが用意したもので、同報告書に添付されている（Prof.Gercke,Die Strafbarkeit von Phishing und Identitätsdiebstahl,Computer und Recht,2005,S.606.）。

[29]「2013年国連レポート」（注27）18頁

[30]「2013年国連レポート」（注27）18-19頁

[31]「2013年国連レポート」（注27）20頁