# 諸外国における他人の識別符号の譲受け行為等を規制する関連法令に係る調査

# 報告書

平成 22 年 12 月

財団法人　社会安全研究財団

## はじめに

本調査は、諸外国における他人の識別符号の譲受け行為等、不正アクセスに関係する行為を規制する法令やその捜査手法、当該国における不正アクセス関連犯罪の現状等の調査を行ったものである。

現在、我が国において、他人の ID・パスワード等の識別符号の譲渡しについては、不正アクセス禁止法における不正アクセスの助長行為として、提供行為自体は罰則化されているものの、他人の識別符号の譲受け行為については罰則が無く、また譲渡し・譲受けに関する広告や誘引行為についても規制する法令が無いため、これらの行為を取り締まることができない状況にある。

このような現状にあって、インターネット上で行われる犯罪を防止するためには、他人の識別符号の譲受け行為等の規制に関して法制化を検討することが喫緊の課題となっている。そのため、具体的な検討の一助とすべく、すでにこれらの行為について法規制が存在する諸外国について、当該法令の実態を把握するため、本調査を実施した。

調査対象国は、他人の識別符号の譲渡し等に関連する法規制の実態がある国として、米国、ドイツ、フランス、韓国の 4 か国である。各国の関連する法制について、文献調査及び関係者からのヒアリング調査を行い、法令条文の翻訳作業を行うとともに、比較分析を行った。

本調査が、我が国のサイバー犯罪への対応策を検討する上で活用され、より安全なインターネット社会の構築に寄与することとなれば幸いである。

平成 22 年 12 月

財団法人　社会安全研究財団

目　次

# １．各国の不正アクセス関連法令の比較表

## 表 1　諸外国における不正アクセス関連法令の比較表

| | | 米国 | ドイツ | フランス | 韓国 |
|---|---|---|---|---|---|
| 不正アクセス行為（助長行為を含む）に関する法令 | 不正アクセス行為の規制に係る条文 | 刑法典1030条(a)(2)<br>金融機関等の情報や、連邦機関の情報、保護されたコンピュータ の情報に対する無権限のアクセス、又は付与されたアクセス権限を超えたアクセスを禁止<br>(他にも関連法令あり) | 刑法典202a条<br>無権限でのアクセスに対して特別な保護がされているデータを、無権限で入手する行為を禁止 | 刑法典323-1条<br>データの自動処理システムに不正アクセス又は不正滞留する行為を禁止 | 情報通信網利用促進及び情報保護などに関する法律48条<br>正当なアクセス権限なしで、又は許されたアクセス権限を越えて情報通信網に侵入する行為を禁止<br>(他にも関連法令あり) |
| | 罰則 | 罰金又は1年以下の拘禁刑ほか(条件付き) | 3年以下の自由刑又は罰金刑 | 2年の拘禁刑及び3万ユーロの罰金ほか(条件付き) | 3年以下の懲役刑又は3千万ウォン以下の罰金刑 |
| | データの財物性（データの不正取得）に係る条文 | 刑法典1028条、1030条(a)(2)で、一定の条件下でデータの不正取得を規制 | 連邦データ保護法43条、44条において、個人データを不正に取得する行為を規制 | 刑法典226-18条<br>個人情報を不法・不当・不正な手段で収集する行為を禁止 | 情報通信網利用促進及び情報保護などに関する法律49条の2<br>情報通信網を通して騙す行為で他の人の情報を収集したり、他の人が情報を提供するように誘引する行為の禁止<br>(他にも関連法令あり) |
| | 罰則 | 刑法典1028条(a)(7)<br>罰金若しくは5年以下の拘禁刑、又はこれらの併科ほか(条件付き)<br>刑法典1030条(a)(2)<br>罰金又は1年以下の拘禁刑ほか(条件付き) | 連邦データ保護法43条<br>30万ユーロ以下の罰金刑<br>連邦データ保護法44条<br>2年以下の自由刑又は罰金刑 | 5年の拘禁刑及び30万ユーロの罰金 | 3年以下の懲役又は3千万ウォン以下の罰金 |
| | 不正アクセス行為の予備行為の規制に係る条文 | — | 刑法典202c条<br>不正アクセス行為等の準備行為として、データへのアクセスを可能とするパスワード等又はそのような行為を実行する目的を持つコンピュータ・プログラムを作成・入手・販売・譲渡・配布する行為を禁止<br>刑法典263a条<br>違法に財産上の利益を得ることを意図した不正アクセス行為等の準備行為として、コンピュータ・プログラムを作成・入手・販売・保管・譲渡する行為を禁止 | 刑法典323-3-1条<br>不正アクセス行為等を実行する目的のために作成等された装置・機械・情報処理プログラム・データを導入・所持・提供・譲渡等する行為を禁止 | — |
| | 罰則 | — | 刑法典202c条<br>1年以下の自由刑又は罰金刑<br>刑法典263a条<br>3年以下の自由刑又は罰金刑 | 当該犯罪（不正アクセス行為等）の所定刑 | — |
| | 不正アクセス行為の国外犯規定に係る条文 | 刑法典1030条(a)(2)<br>合衆国の外に設置され、合衆国の州際・国際商取引又は通信に影響を与えるコンピュータに対する不正アクセスを禁止 | 刑法典3条、9条<br>刑法典3条ではドイツ刑法は国内において実行された犯行に対して適用すると規定。また刑法典9条では、犯行は、構成要件に属する結果が生じた又は犯人自身が結果が生じることを想定していた全ての場所において実行されたものとみなす（すなわち国外犯であってもドイツ国内に影響が及ぶ場合は国内で実行されたものとみなす）と規定 | 刑法典113-6条、113-7条<br>刑法典113-6条では、フランスの刑法はフランス国外においてフランス国籍を持つ者が実行した重罪に対しても適用されると規定。また、刑法典113-7条では、フランス国外で発生した犯罪の被害者がフランス国籍を持つ者である場合、犯行者の国籍に関わらず、重罪又は拘禁刑で罰する軽罪については、フランス刑法が適用されると規定 | — |
| | 他人の識別符号の譲渡しの規制に係る条文 | 刑法典1030条(a)(6)<br>故意かつ詐欺の意図をもって、コンピュータ（対象は限定）のパスワードや類似の情報を引き渡すことを禁止<br>刑法典1028条(a)(7)<br>連邦法違反又は州法・地域法重罪を実行・幇助・教唆する意図で、又はこれらの犯罪行為に関連して、他人の個人識別手段を合法的権限なく故意に移転・所持・使用することを禁止<br>刑法典1028A条<br>一定の列挙された連邦犯罪の重罪の実行に際して、又はこれに関連して、他人の個人識別手段を故意に移転・所持・使用した事犯において、2年間の拘禁刑を加重<br>刑法典1029条(a)(1)～(3)<br>権限のないアクセス装置（個人識別番号等を含む）、又は偽造したアクセス装置を、故意かつ詐欺の意図で、製造・使用・所持・引き渡すことを禁止 | 刑法典202c条<br>不正アクセス行為等の準備行為として、データへのアクセスを可能とするパスワード等を入手・販売・譲渡・配布・その他の方法でアクセス可能とする行為を禁止 | — | 電子金融取引法6条<br>アクセス媒体（電子金融取引で使われる利用者番号、暗証番号を含む）の譲渡し・譲受け等を禁止<br>住民登録法37条<br>法律に従わずに営利の目的で他人の住民登録番号に関する情報を知らせる行為を禁止<br>（識別符号一般の譲渡しを規制する法令は無い） |
| | 罰則 | 刑法典1030条(a)(6)<br>罰金又は1年以下の拘禁刑ほか(条件付き)<br>刑法典1028条(a)(7)<br>罰金若しくは5年以下の拘禁刑、又はこれらの併科ほか(条件付き)<br>刑法典1029条(a)(1)～(3)<br>罰金若しくは10年以下の拘禁刑、又はこれらの併科ほか(条件付き) | 1年以下の自由刑又は罰金刑 | — | 電子金融取引法6条<br>1年以下の懲役刑又は1千万ウォン以下の罰金刑<br>住民登録法37条<br>3年以下の懲役刑又は1千万ウォン以下の罰金刑 |

| | | | | | |
|---|---|---|---|---|---|
| | **他人の識別符号の譲受けの規制に係る条文** | 刑法典1028条(a)(7)<br>連邦法違反又は州法・地域法重罪を実行・幇助・教唆する意図で、又はこれらの犯罪行為に関連して、他人の個人識別手段を合法的権限なく故意に移転・所持・使用することを禁止<br>刑法典1028A条<br>一定の列挙された連邦犯罪の重罪の実行に際して、又はこれに関連して、他人の個人識別手段を故意に移転・所持・使用した事犯において、2年間の拘禁刑を加重。テロリズムに関連した加重ID窃盗の事犯においては、5年間の拘禁刑を加重<br>刑法典1029条(a)(1)～(3)<br>権限のないアクセス装置(個人識別番号等を含む)、又は偽造したアクセス装置を、故意かつ詐欺の意図で、製造・使用・所持・引き渡すことを禁止 | 刑法典202c条<br>不正アクセス行為等の準備行為として、データへのアクセスを可能とするパスワード等を入手・販売・譲渡・配布・その他の方法でアクセス可能とする行為を禁止 | ― | 電子金融取引法6条<br>アクセス媒体(電子金融取引で使われる利用者番号、暗証番号を含む)の譲渡し・譲受け等を禁止<br>(識別符号一般の譲渡しを規制する法令は無い) |
| | **罰則** | 刑法典1028条(a)(7)<br>罰金若しくは5年以下の拘禁刑、又はこれらの併科ほか(条件付き)<br>刑法典1029条(a)(1)～(3)<br>罰金若しくは10年以下の拘禁刑、又はこれらの併科ほか(条件付き) | 1年以下の自由刑又は罰金刑 | ― | 3年以下の懲役刑又は1千万ウォン以下の罰金刑 |
| | **他人の識別符号の譲渡しに関する広告又は誘引行為の規制に係る条文** | 刑法典1029条(a)(6)<br>アクセス装置の発行者の承認を得ずに、アクセス装置の提供等を目的に、故意かつ詐欺の意図で、勧誘を行うことを禁止 | ― | ― | ― |
| | **罰則** | 罰金若しくは10年以下の拘禁刑、又はこれらの併科ほか(条件付き) | ― | ― | ― |
| | **他人の識別符号の譲受けに関する広告又は誘引行為の規制に係る条文** | ― | ― | ― | ― |
| | **アクセス管理者等の防御措置に係る条文** | 合衆国法典第44編3544条<br>各連邦機関の長は、当該機関により維持される情報等への不正なアクセス・使用・開示・混乱・変更・破壊によってもたらされるリスク及び被害の規模に対応した情報セキュリティ対策を整備することや、国立標準技術院(NIST)等が作成した一定の情報セキュリティ規準を遵守すること等の責任を負う | 電気通信法109条、110条<br>アクセス管理者、アクセス管理製品製造者、インターネット・アクセス・プロバイダー等に対するセキュリティ対策義務等の防御措置を規定 | 情報処理・データと自由に関する法律34条、35条<br>34条では、個人情報処理責任者のデータ安全保護のための予防措置義務を規定。35条では、下請業者における安全措置義務を規定<br>刑法典226-17条<br>安全保護のための有効な予防措置を講じずに、個人情報の処理を実施又は実施させる行為を禁止 | 情報通信網利用促進及び情報保護などに関する法45条、46条の3、47条の3<br>情報通信サービス提供者に対し、情報通信網の安全性及び情報の信頼性を確保するための保護措置や、毎年の情報保護安全診断の受診義務を規定。ソフトウェア事業者に対し、、セキュリティ脆弱性を補完するプログラムを製作した際のソフトウェア使用者への通知義務を規定<br>(他にも関連法令あり) |
| **不正アクセスにつながる可能性のある行為に関する法令** | **ウィルス作成の規制に係る条文** | 刑法典1030条(a)(5)(A)<br>プログラム・情報・コード・コマンドの送信を故意に発生させ、その結果として、保護されたコンピュータに対して無権限で故意に損害を与える行為を禁止<br>(ウィルス作成自体を規制する法令は無い) | 刑法典202c条<br>不正アクセス行為等の準備行為として、データへのアクセスを実行する目的を持つコンピュータ・プログラムを作成・入手・販売・譲渡・配布する行為を禁止<br>刑法典263a条<br>違法に財産上の利益を得ることを意図して、プログラムの不正作成等によってデータ処理プロセスの結果に影響を与え、結果として他人の財産を損なう行為を禁止。またこれらの犯罪の準備行為としてコンピュータ・プログラムを作成・入手・販売・保管・譲渡する行為を禁止 | 刑法典323-3-1条<br>不正アクセス行為等を実行する目的のために作成等された装置・機械・情報処理プログラム・データを導入・所持・提供・譲渡等する行為を禁止 | 情報通信網利用促進及び情報保護などに関する法律48条<br>正当な理由なしで、情報通信システム・データ・プログラムなどを毀損・滅失・変更・偽造したり、その運用を妨害できるプログラムを伝達・流布する行為を禁止<br>(ウィルス作成自体を規制する法令は無い) |
| | **罰則** | 罰金若しくは10年以下の拘禁刑、又はこれらの併科ほか(条件付き) | 刑法典202c条<br>1年以下の自由刑又は罰金刑<br>刑法典263a条<br>5年以下の自由刑又は罰金刑<br>(準備行為については3年以下の自由刑又は罰金刑) | 当該犯罪(不正アクセス行為等)の所定刑 | 5年以下の懲役刑又は5千万ウォン以下の罰金刑 |
| | **識別符号の不正取得(フィッシングサイトの構築等)の規制に係る条文** | 刑法典1028条(a)(7)(ID窃盗)、刑法典1028A条(ID窃盗による罪の加重)、刑法典1029条(アクセス装置詐欺)を適用可能<br>(直接フィッシングサイト構築等を処罰する法令は未制定) | 刑法典263a条(コンピュータ詐欺)を適用可能<br>(直接フィッシングサイト構築等を処罰する法令は未制定) | 知的所有権法L713 条(偽造ブランドによる商標権侵害)、刑法典226-18条(個人情報の不正取得)、刑法典323-1条(不正アクセス行為)、刑法典313-1条(詐欺的な取得)、刑法典434-23条(氏名詐称)を適用可能<br>(直接フィッシングサイト構築等を処罰する法令は未制定) | 情報通信網利用促進及び情報保護などに関する法律49の2条<br>(騙す行為による個人情報の収集禁止など)を適用可能<br>(直接フィッシングサイト構築等を処罰する法令は未制定) |

| | | | | | |
|---|---|---|---|---|---|
| | サイバーテロ行為の規制に係る条文 | 刑法典1030条(a)(5)(A)<br>プログラム・情報・コード・コマンドの送信を故意に発生させ、その結果として、保護されたコンピュータに対して無権限で故意に損害を与える行為を禁止<br>刑法典1362条<br>合衆国によって運営等されているシステム等の運用や使用を妨害する行為を禁止 | 刑法典303a条<br>不正にデータを消去、隠蔽、使用不能とするか、又は改竄する行為を禁止<br>刑法典303b条<br>他者に不利益を与える意図をもってデータを入力・中継すること等によって他者にとって重要な意義を持つデータ処理を妨害する行為を禁止 | 刑法典323－2条<br>データの自動処理システムの動作を妨害する、又は不調にする行為を禁止 | 刑法典314条<br>コンピュータなど情報処理装置又は電磁記録など特殊媒体記録を損壊したり、情報処理装置に虚偽の情報又は不正な命令を入力したり、その他方法で、情報処理に障害を発生させて人の業務を妨害する行為を禁止<br>情報通信基盤保護法12条<br>主要情報通信基盤施設の運営を邪魔する目的で、一時に大量の信号を送ったり不正な命令を処理するなどの方法で情報処理に誤りを発生させようとする行為を禁止<br>情報通信網利用促進及び情報保護などに関する法律48条<br>情報通信網の安定的運営を妨害する目的で大量の信号、又はデータを送ったり、不正な命令を処理するようにするなどの方法で情報通信網に障害を発生させようとする行為を禁止 |
| | 罰則 | 刑法典1030条(a)(5)(A)<br>罰金若しくは10年以下の拘禁刑、又はこれらの併科ほか(条件付き)<br>刑法典1362条<br>罰金若しくは10年以下の拘禁刑、又はこれらの併科 | 刑法典303a条<br>2年以下の自由刑又は罰金刑<br>刑法典303b条<br>3年以下の自由刑又は罰金刑<br>(企業・官庁等にとって重要な意義を持つデータ処理に関する妨害行為は5年以下の自由刑又は罰金刑、特に重大な事案に対しては自由刑を6か月以上10年以下に加重) | 5年の拘禁刑及び7万5千ユーロの罰金 | 刑法典314条<br>5年以下の懲役刑又は1千500万ウォン以下の罰金刑<br>情報通信基盤保護法12条<br>10年以下の懲役刑又は1億ウォン以下の罰金刑<br>情報通信網利用促進及び情報保護などに関する法律48条<br>5年以下の懲役刑又は5千万ウォン以下の罰金刑 |
| 不正アクセスに関係する行為の捜査に関する法令 | 通信傍受に係る条文 | 刑法典2511条<br>電子的通信サービスのプロバイダ等は、裁判所命令、又は合衆国司法長官等による証明書を与えられた場合は、電子的通信の傍受等を法律により授権された者に対し、情報、設備又は技術的支援を提供する権限を有する<br>刑法典2518条<br>通信傍受のための手続きを規定 | 刑事訴訟令100a条<br>裁判所の命令(危急の場合には検察官の命令)によって電気通信の監視及び記録を行うことが可能<br>刑事訴訟令100b条<br>裁判所の命令(危急の場合には検察官の命令)があった場合、電気通信サービス提供者等は裁判所、検察官、捜査員に対して電気通信の監視及び記録を可能とする情報を直ちに提供しなければならない | 1991年7月10日の法律91-646 号1条、3条<br>司法当局によって命じられる傍受、及び治安上の目的による傍受が可能<br>1991年7月10日の法律91-646 号4条<br>治安上の目的による傍受については、首相又は首相によって特別に権限を付託された2名のうちのいずれか1名による理由が記載された書面による決定で行うことが可能<br>刑事訴訟法100条<br>予審判事は電気通信手段によって発せられる通信の傍受、録音、及び転写を命ずることが可能 | ―<br>(不正アクセス行為自体は通信傍受が認められる犯罪類型ではないが、当該不正アクセス行為が通信傍受を認める犯罪類型につながる疑いがある場合には、検事は裁判所に通信傍受の許可を請求することが可能) |
| | 差押場所が明確でない場合の措置に係る条文 | 刑法典2703条<br>政府機関は電子的通信サービスのプロバイダに対して、電子的通信等の内容については、裁判所の令状又は州の同等の令状によって、その開示を要求できる | 電気通信法113条<br>事業目的の電気通信サービス提供者等は、法令の規定による要請があった場合、端末又はその内部若しくはネットワーク上に設置されているデータ保存装置へのアクセスに対する防護を行うためのデータ(パスワード等)の情報を提供しなければならない | 郵便・電子通信法典L32－4条<br>電子通信担当大臣及び電子通信郵便規制機関は、任務の遂行に関連する必要及び正当な決定に基づき、電気通信ネットワーク事業者等に対する捜査を行うことができる | 通信秘密保護法15条の2<br>電気通信事業者は、検事・司法警察官又は情報捜査機関の長が同法により執行する通信制限措置及び通信事実確認資料の提供要請に協力しなければならない<br>情報通信網利用促進及び情報保護などに関する法律48条の4<br>放送通信委員会は、不正アクセスなどの侵害事故の原因を分析するために必要と認めれば、情報通信サービス提供者等に情報通信網の接続記録などの関連資料の保全を命じることができる |
| | ログの保存に係る条文 | 刑法典2703条<br>電子的通信サービス等のプロバイダは、政府機関の要求を受けて、その専有する記録及び他の証拠を90日間保存しなければならない。保存期間は90日間延長可能<br>(ログ保存を一律に義務付ける法令は無し) | 電気通信法113a条<br>電気通信サービス提供者はログを6ヶ月間保存しなければならない | 2006 年3 月24 日のデクレ第2006-358 号<br>電子通信ネットワーク事業者はログを1年間保存しなければならない | 通信秘密保護法施行令41条<br>電気通信事業者はログを3ヶ月以上保存しなければならない |

| | 米国 | ドイツ | フランス | 韓国 |
|---|---|---|---|---|
| 人　口 | 3億880万人 | 8253万人 | 6195万人 | 4839万人 |
| インターネットユーザ数 | 2億2000万人 | 6250万人 | 3157万人 | 3748万人 |
| インターネット普及率 | 71.2% | 75.7% | 51.0% | 77.4% |
| パソコン普及状況 | 79.9% | 65.3% | 65.9% | 54.4% |
| 固定電話普及率 | 51.3% | 62.4% | 56.5% | 44.1% |
| 移動電話普及率 | 87.6% | 129.9% | 93.6% | 94.3% |
| 1人当りGNI | 4万7580ドル | 4万2440ドル | 4万2250ドル | 2万1530ドル |

(人口、インターネットユーザ数等の統計データの出典:(財)日本ITU協会『ワールドICTビジュアルデータブック2010』)

## ２．米国における不正アクセス関連法令

### ２．１　米国における不正アクセス関連犯罪の現状

#### （１）インターネット犯罪の統計

米国では、インターネット犯罪苦情センター（Internet Crime Complaint Center, IC3）が毎年、インターネット犯罪に関する統計レポートを発行している[1]。IC3 は、連邦捜査局（FBI）と全米知能犯罪センター（National White Collar Crime Center, NW3C）によって設立された組織横断的なタスクフォースである[2]。

IC3 の 2009 年の統計レポート[3]では、IC3 におけるインターネット犯罪に関する苦情受付件数は 2009 年に 336,655 件であり、2008 年の 275,284 件から約 22%増加している。インターネット犯罪類型別の内訳としては、「FBI 詐欺（FBI の名前を騙った電子メール等の詐欺）」が最も多く、全体の 16.6%を占めている。以下、「商品の未配達」が 11.9%、「料金前払い詐欺」が 9.8%、「ID 窃盗」が 8.2%で続いている（図 1 参照）[4]。

また、IC3 から法執行機関や規制機関への照会件数は、2009 年に 146,663 件であり、2008 年の 72,940 件から約 2 倍の件数に増えている。インターネット犯罪類型別の内訳は、「商品の未配達」が 19.9%で最も多く、以下、「ID 窃盗」が 14.1%、「クレジットカード詐欺」が 10.4%、「オークション詐欺」が 10.3%で続いている（図 2 参照）。

---

[1] なお、2010 年 11 月現在、米国にはサイバー犯罪の発生・検挙件数に関する全米規模の統計資料は存在しない。

[2] IC3 は、市民（被害者）からサイバー犯罪に関する苦情を受け付け、連邦・州・地方・国際レベルの法執行機関や規制機関に情報を展開（照会）する、中央的なハブとしての機能を果している。2010 年 11 月現在では、司法支援局（Bureau of Justice Assistance, BJA）も IC3 のパートナーシップに加わっている。

[3] インターネット犯罪苦情センター「2009 年インターネット犯罪レポート」、2010 年 3 月 12 日（http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf）。

[4] 2008 年の内訳は、「商品の未配達」が 32.9%、「オークション詐欺」が 25.5%、「クレジットカード詐欺」が 9.0%、「信用詐欺」が 7.9%という順になっており、1 年間でかなり傾向が変化している。2009 年にトップの「FBI 詐欺」は 2008 年にはトップ 10 に入っておらず、2009 年に急増した犯罪であることが分かる。

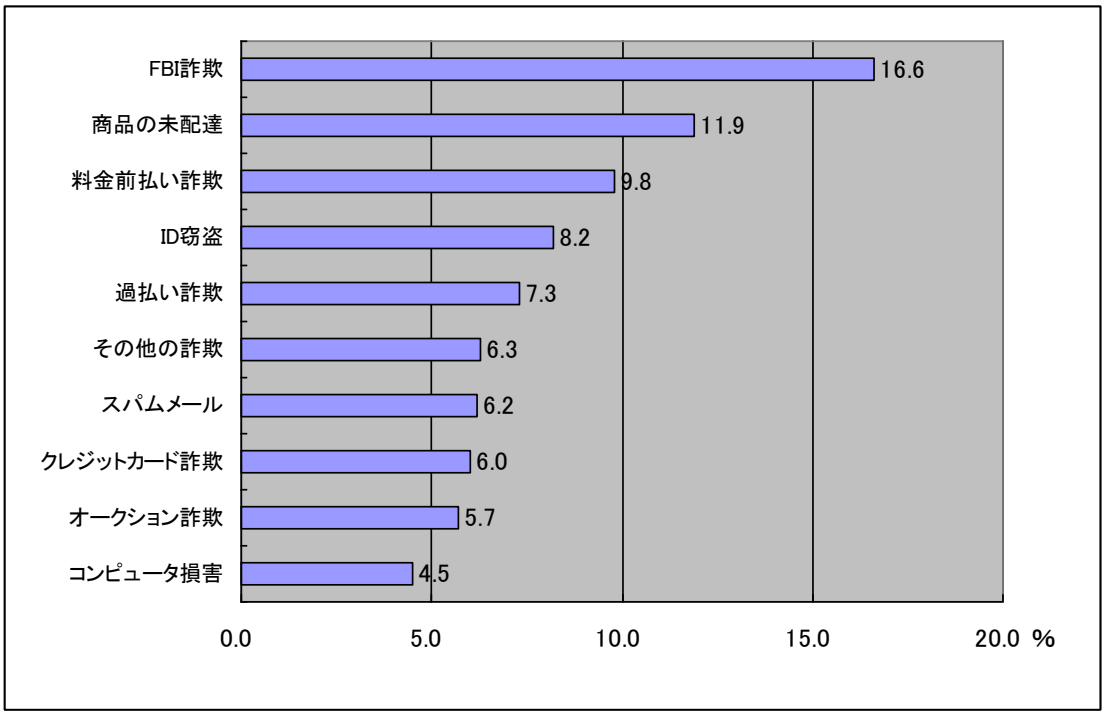


図 1　インターネット犯罪類型別の苦情受付割合（2009 年）

出典：インターネット犯罪苦情センター「2009 年インターネット犯罪レポート」

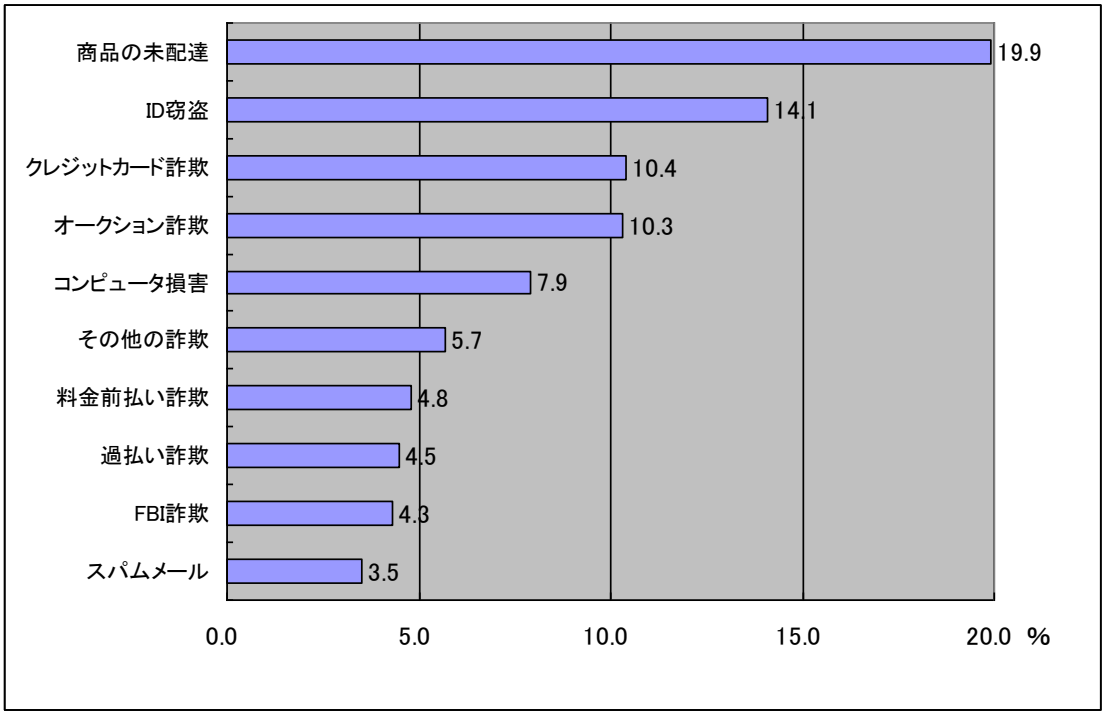


図 2　インターネット犯罪類型別の苦情照会割合（2009 年）

出典：インターネット犯罪苦情センター「2009 年インターネット犯罪レポート」

なお、同レポートにおける各インターネット犯罪類型の定義は、表 2 の通りである[5]。

**表 2　「2009 年インターネット犯罪レポート」におけるインターネット犯罪類型の定義**

| インターネット犯罪類型 | 定義 |
|---|---|
| FBI 詐欺 | FBI を騙る電子メール等によって被害者から金銭や ID 情報等を取得しようとする詐欺 |
| 料金前払い詐欺 | 被害者は何らかの褒賞を得るに先立って料金を（しばしば何回か）前払いすることを求められるが、決してその褒賞が与えられない詐欺 |
| ID 窃盗 | ID 情報等を盗んだ、又は盗もうとした事犯（クレジットカード窃盗等、他の犯罪を伴わない場合） |
| 商品の未配達 | 被害者が購買した商品が届かない事犯 |
| 過払い詐欺 | 被害者は当該取引で合意した額以上の偽の通貨代替物（monetary instrument、米国又は外国の貨幣、トラベラーズチェック、小切手など）を与えられ、合法な通貨代替物を使って過払い分を送り返すように求められる詐欺 |
| その他の詐欺 | 何も売買していないのに、被害者に金銭を送るように詐欺的に仕向ける事犯 |
| スパムメール | 受信者に望まれていない電子メール。通常は大量に送信される |
| クレジットカード詐欺 | 被害者のクレジットカード又は口座に商品やサービスの代金を課金しようとする事犯 |
| オークション詐欺 | オークションサイトで発生する詐欺的な取引や交換 |
| コンピュータ損害 | コンピュータの損害を引き起こす犯罪 |

出典：インターネット犯罪苦情センター「2009 年インターネット犯罪レポート」

### （２）ID 窃盗の統計

また、司法統計局（Bureau of Justice Statictics）では全米犯罪被害調査（National Crime Victimization Survey, NCVS）の一部として、2007 年における米国の家庭単位での ID 窃盗統計を発表している[6]。

同統計によると、2007 年には約 790 万の家庭（全米の全家庭数の 6.6%）で少なくとも 1 人の構成員が ID 窃盗の被害にあっている。2005 年の統計では、被害家庭数が約 640 万、

[5] インターネット犯罪苦情センター・前掲注 3、p2、p17。
[6] 司法統計局「家庭単位で報告された ID 窃盗：2007 年の統計表」、2010 年 6 月（http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh07st.pdf）。

被害割合が 5.5%であるので、被害家庭数・被害割合ともにかなりの増加を見せている（表 3 参照）。

2007 年の被害内訳を見ると、クレジットカードの不正利用が 3.3%、その他の既存アカウント[7]の不正利用が 1.6%、個人情報の窃盗が 0.9%となっている。2005 年から 2007 年にかけて、とりわけクレジットカードの不正利用の被害家庭数が増加している。

**表 3　ID 窃盗の被害家庭数**

| | 2005 年 | | 2007 年 | | 被害を受けた家庭数の変化（2005 年から 2007 年） |
|---|---|---|---|---|---|
| | 家庭数 | 割合（%） | 家庭数 | 割合（%） | |
| **ID 窃盗に遭った** | **6,426,200** | **5.5** | **7,928,500** | **6.6** | **23.4%** |
| 既存のクレジットカード | 2,966,500 | 2.5 | 3,894,300 | 3.3 | 31.3% |
| 他の既存アカウント | 1,586,500 | 1.4 | 1,917,000 | 1.6 | 20.8% |
| 個人情報 | 1,083,100 | 0.9 | 1,031,200 | 0.9 | -4.8% |
| 上記の組合せ | 790,200 | 0.7 | 1,086,100 | 0.9 | 37.4% |
| **ID 窃盗に遭っていない** | **109,206,700** | **93.3** | **108,197,000** | **90.5** | **-0.9%** |
| **不明** | **1,477,800** | **1.3** | **3,378,000** | **2.8** | **－** |
| **合計** | **117,110,800** | **100.0** | **119,503,500** | **100.0** | **－** |

出典：司法統計局「家庭単位で報告された ID 窃盗：2007 年の統計表」

## ２．２　不正アクセス行為関連法令の実態

### ２．２．１　不正アクセス関連法令の概要[8]

1980 年代初頭、米国の法執行機関はコンピュータ時代の幕開けに直面し、新たに発生するコンピュータ犯罪に対処するための刑法が存在しないことに対する懸念が高まっていた。連邦刑法の有線通信不正行為や郵便詐欺の条項によって、コンピュータ関連の犯罪活動の一部には対応できたが、どちらの法律も、そうした新しい犯罪への対処に必要とされる網羅的な手段は提供できなかった。

それに応えて、連邦議会は「1984 年総合犯罪規制法（Comprehensive Crime Control Act）」に、コンピュータとコンピュータ・ネットワークに対する不正アクセス・不正使用に対処する規定を導入した。コンピュータ内の機密情報への不正アクセスについては重罪とされ、金融機関に保存されている金融記録・信用履歴へのアクセス、又は政府のコンピ

[7] 銀行口座、当座預金口座、携帯電話口座等。

[8] 本節は、米国司法省刑事局コンピュータ犯罪・知的財産課「コンピュータ犯罪の訴追」、2007 年 2 月（http://www.justice.gov/criminal/cybercrime/ccmanual/index.html）、p1～2 に基づき記載した。

ュータへの不法侵入については軽罪とされた。これらの規定によって、「法の執行に携わる人々、コンピュータを使用する人々、不正アクセスによって犯罪を行う誘惑に駆られる可能性のある人々」に対して、違法行為の記述をより明瞭化することが狙いであった。連邦議会は、同法において、既存の刑法にコンピュータに関する新規定を加えるのではなく、単一の新しい制定法（「刑法典 1030 条　コンピュータに関連する詐欺及び関連行為」）の中でコンピュータ関連犯罪に対処する道を選択した。

連邦議会は刑法典 1030 条の制定後も、刑法にさらなる改正が必要か否かを判断するために、コンピュータ犯罪に関連する諸問題の調査を続けた。1985 年に上下院は、年間を通じてコンピュータ犯罪法案に関するヒアリングを開催した。その結果、1986 年に「コンピュータ詐欺と濫用に関する法律（Computer Fraud and Abuse Act, CFAA）」が制定された。これは、刑法典 1030 条を改正するものであった。

連邦議会は CFAA において、コンピュータ犯罪に対する連邦政府の関心と、そうした犯罪を禁止・処罰する各州の関心や能力の間に適切なバランスを取ろうとした。結果として連邦議会は、連邦レベルの司法管轄を、連邦政府が関心を持たざるを得ないケース、すなわち連邦政府機関や特定の金融機関のコンピュータが関係するケースや犯罪自体が本質的に州際的又は国際的であるケースに限定した。他方、各州内で発生するコンピュータ犯罪については、州レベルの司法管轄であり、各州にて法令を定めている。

CFAA によって、既存の刑法典 1030 条のいくつかの規定が明確化されたことに加えて、コンピュータ関連で犯罪とされる行為が追加された。例えば、コンピュータ経由による財産の窃盗を罰する規定（1030 条(a)(4)）や、他者に帰属するデータを故意に改変・損傷・破壊する者を罰する規定（1030 条(a)(5)）が追加された。後者の規定は、悪質なコードの配信や Dos 攻撃といった行為を網羅するために考案されたものである。パスワードその他の引渡しを犯罪とする規定（1030 条(a)(6)）も追加された。

コンピュータ犯罪がますます高度化し、検察当局が経験を積むにつれて、刑法典 1030 条に修正条項を増やす必要が生じ、議会は 1988 年、1989 年、1990 年、1994 年、1996 年、2001 年、2002 年、2008 年に修正決議を行っている。最も重要な修正は、「1996 年国家情報基盤保護法」及び 「2001 年米国愛国者法（USA PATRIOT Act of 2001）」[9]によるものである。

刑法典 1030 条では(a)(1)から(a)(7)まで 7 種類の犯罪が規定されているが、同条の(b)により、これらの犯罪の未遂も犯罪となる。また、法執行機関又は諜報機関の合法的な捜査活動・諜報活動等は、1030 条の対象から明示的に除外されている。

[9] この「2001 年米国愛国者法」では、保護されたコンピュータへの損害行為（1030 条(a)(5)）に対する罰則の 10 年から 20 年への引き上げ、国外犯規定（1030 条(e)(2)）の追加等の修正がなされた。

## ２．２．２　不正アクセス行為（助長行為を含む）に関する法令

### （１）不正アクセス行為

刑法典 1030 条(a)(2)

「刑法典 1030 条　コンピュータに関連する詐欺及び関連行為」の(a)(2)では、金融機関やカード発行者の金融記録に含まれている情報や、連邦機関の情報、その他の保護されたコンピュータ[10]の情報に対して無権限で、又は付与されたアクセス権限を超えてアクセスし、それらの情報を入手することを禁じている。

ある犯罪行為に対して 1030 条(a)(2)を適用する際に、一定の金銭的被害額が必要とされる訳ではない。ただし、侵害によって取得された情報の価値は、当該犯罪が軽罪か重罪かを決定するに当たって重要な要素となる。

1030 条(a)(2)の違反は、加重的要素がない限り、罰金又は 1 年以下の拘禁刑[11]で罰しうる軽罪である。例えば、取得した情報が 5000 ドル未満の価値[12]の場合は、軽罪である。以下の場合には、1030 条(a)(2)の違反は、重罪になる。

・商業上の利益又は私的な金銭上の利益のために行った場合
・連邦法や州法に違反する犯罪行為や不法行為を増進するために行った場合
・取得した情報が 5000 ドル以上の価値であった場合

これらの場合、罰金若しくは 5 年以下の拘禁刑、又はそれらの併科で罰しうる。

当初、刑法典 1030 条(a)(2)は、金融機関での消費者に関係した電算化情報や信用記録への不正アクセスを違法化することによって、個人のプライバシーを守るためのものであった[13]。1996 年に連邦議会は、(B)（連邦機関の情報）と(C)（保護されたコンピュータの情報）の 2 つの項目を追加することで、本条項の範囲を拡大した。

以下、いくつかの補足説明を行う[14]。

○コンピュータへの故意のアクセス

本条項を適用するには、単に被告人が他人のアクセスした情報を無権限で受領することでは不十分であり、本人があるコンピュータに無権限でアクセスしていなければならない。例えば、人物 A が 1030 条(a)(2)に違反して情報を取得し、当該情報を人物 B に送信した場合、B は本条項に違反したことにはならない[15]。

---

10 「保護されたコンピュータ」は、1030 条の(e)において、金融機関又は合衆国政府によって使用されているコンピュータや、州際若しくは国際商取引や通信に使用されるコンピュータ等と定義されている。

11 拘禁刑（imprisonment）には、懲役刑及び禁固刑が含まれる。

12 取得された情報の価値を決定する（当該情報が 5,000 ドルの価値に持つか否かを決定する）際には、いかなる合理的な方法も取りうる。例えば、調査・開発・製造コストや、「泥棒市場」での当該資産の価値などを利用することができる。

13 米国司法省刑事局コンピュータ犯罪・知的財産課・前掲注 8、 p 18。

14 米国司法省刑事局コンピュータ犯罪・知的財産課・前掲注 8、 p 16。

15 ただし、B は本条項に違反する犯罪の共同謀議に参加した事由によって訴追される可能

○無権限で、又は権限を超過して

「無権限で（without authorization）」は、1030 条の中では定義されていない。「付与されたアクセス権限を超える(exceeds authorized access)」は、1030 条(e)(6)で「権限に基づいてコンピュータにアクセスし、かかるアクセスを利用して、当該アクセス者が入手又は改変する権限を有さないコンピュータ内の情報を入手又は改変すること」と定義されている。

「無権限で」と「付与されたアクセス権限を超えて」を区分したことの意図は、外部者（あるコンピュータにアクセスする何らの権限もない個人）による行為と内部者（あるコンピュータにアクセスする何らかの権限は付与されている個人）による行為とを区別するためである。

○情報の入手

「情報の入手（obtaining information）」は、ダウンロードやコピーをすることなくオンライン上で情報を単に閲覧することをも含む、拡張的な用語である。電子的に保存された情報は、実際の物理的な窃盗によって取得されるのみならず、「単なるデータの観察」によっても取得されうる。

「情報」には、無形財も含まれる。1996 年の 1030 条の修正において、連邦議会はこの問題を明確化し、1030 条(a)(2)は「無権限でのコンピュータの利用による無形情報の窃盗についても、物理的な物品の窃盗が保護されるのと同様な仕方で、禁止されることを保証する」ものと明示した。

刑法典 1030 条(a)(1)

刑法典 1030 条の(a)(1)では、無権限で、又は付与されたアクセス権限を超えて故意にコンピュータにアクセスし、国防又は外交関係上の理由で無許可の情報開示からの保護が必要であると合衆国政府によって決定された情報等を入手し、これを通信・配信・送信等する行為を禁じている。

刑法典 1030 条(a)(3)

刑法典 1030 条の(a)(3)では、無権限で故意に、合衆国によって使用される非公開コンピュータ等にアクセスし、その行為によって合衆国政府による使用等に影響が及んだ場合、そのような行為を禁じている。

刑法典 1030 条(a)(4)

刑法典 1030 条の(a)(4)では、無権限で、又は付与されたアクセス権限を超えて、故意か

---

性はある。

つ詐欺の意図で、保護されたコンピュータにアクセスし、当該行為によって意図された詐欺を助長し、価値を持つ何かを得る行為を禁じている。

刑法典 1030 条(a)(5)

刑法典 1030 条の(a)(5)(B)及び(C)では、保護されたコンピュータに無権限で故意にアクセスし、その結果として、無謀に損害を与える行為及び過失で損害を与える行為を禁じている。

**（２）データの財物性（データの不正取得）**

連邦法において、データを不正に取得する行為自体を規制する法令は存在しない。ただし、後述の刑法典 1028 条や上述の刑法典 1030 条(a)(2)など、一定の条件の下でのデータ不正取得を規制する条文は存在する。

個人データの保護に関しては、米国では部門・分野ごとに個別に規制を行う「セクトラル方式」の法制度をとっている。行政部門については、1974 年にプライバシー法が制定されており、これは連邦機関によって保有される個人データを保護するものである。民間部門については、個別の分野（金融、医療、ビデオレンタル、運転免許等）ごとにデータ保護法が制定されている。例えば、プライバシー法[16]では、(i)(3)項において、「故意に、偽って、ある個人に関する記録を政府機関から要求したり取得した者は軽罪であり、5,000 ドル以下の罰金刑に処する」と規定されている。

**（３）不正アクセス行為の予備行為**

上記の刑法典 1030 条では、不正アクセスの予備行為自体に関する規定は存在しない[17]。ただし、不正アクセス行為など、刑法典 1030 条で規定された犯罪については、同条の(b)において、これらの未遂も同様に処罰されることが規定されている。

**（４）不正アクセス行為の国外犯**

刑法典 1030 条、及び後述の 1029 条については、不正アクセス行為等の国外犯の規制に係る規定が存在する。

---

16 合衆国法典第 5 編第 5 章 552a 条に該当。

17 ポートスキャンに関連する判例としては、以下のものがある。1999 年 12 月、IT サービス会社の社員が FBI によって逮捕され、コンピュータへの不法侵入未遂によってジョージア州のコンピュータシステム保護法及び CFAA に違反した容疑で訴追された。同社員は同社が保守をしているジョージア州チェロキー郡のサーバのセキュリティチェックをするために数回ポートスキャンし、結果として他の IT 企業が管理しているウェブサーバをポートスキャンしてしまった。裁判官はネットワークの完全性や可用性を損なういかなる損害もなかったと結論づけ、同社員は 2000 年に無罪判決を受けた。SecurityFocus 記事、2000 年 12 月 18 日（http://www.securityfocus.com/news/126）。

刑法典 1030 条(a)(2)、(e)(2)

刑法典 1030 条の(a)(2)では「保護されたコンピュータ」に対する不正アクセスが禁じられているが、この「保護されたコンピュータ」には、同条の(e)(2)において、「合衆国の外に設置され、合衆国の州際若しくは国際商取引又は通信に影響を与える方法で使用されるコンピュータ」も含まれると定義されている。この定義は、「2001 年米国愛国者法」によって追加された。

刑法典 1029 条（h）

「刑法典 1029 条　アクセス装置に関する詐欺及び関連行為」の（h）では、1029 条に規定する犯罪行為が米国の司法管轄外で行われた場合でも、当該犯罪が金融機関・アカウントの発行者・クレジットカード・システム会員等によって発行・所持・管理等されているアクセス装置に関係しており、かつ、当該人物が、当該犯罪の幇助に使用された品物や当該犯罪から得られた財産等を合衆国の司法管轄に輸送・配達・保管したり、合衆国の司法管轄を通過させたりした場合は、処罰対象になると規定している。

**（５）他人の識別符号の譲渡し**

他人の ID・パスワード等の識別符号を提供する行為については、刑法典 1030 条(a)(6)（パスワードの引渡し）、1028 条(a)(7)（ID 窃盗）、1028A 条（ID 窃盗による罪の加重）、及び 1029 条（アクセス装置詐欺）において規制がなされている。

刑法典 1030 条(a)(6)

刑法典 1030 条の(a)(6)では、故意かつ詐欺の意図をもって、コンピュータのパスワード又はこれに類する情報を引き渡し、その結果として州際又は国際商取引に悪影響を及ぼすこと、又は連邦政府で利用されるコンピュータ等について、故意かつ詐欺の意図をもって、当該コンピュータのパスワード又はこれに類する情報を引き渡すことを禁止している。

本条項の違反は、初犯の場合、罰金又は 1 年以下の拘禁刑で罰しうる軽罪である。被告人が 1030 条の前科を持つ場合は、最大で 10 年の拘禁刑で罰しうる。

連邦議会は 1986 年に、他人のコンピュータへの不正アクセスを可能にするパスワードが掲示された掲示板に関連した行為を罰することを目的として、1030 条(a)(6)を導入した[18]。

以下、いくつかの補足説明を行う[19]。

○引渡し（Trafficking）

「引き渡す（traffic）」の語は、刑法典 1029 条の定義を参照することで定義がなされている。1029 条の(e)(5)では、「引き渡す（traffic）」は、「他人に移転する、若しくは他人に

[18] 米国司法省刑事局コンピュータ犯罪・知的財産課・前掲注 8、p 48。
[19] 米国司法省刑事局コンピュータ犯罪・知的財産課・前掲注 8、p 46～48。

譲渡する、又は移転したり譲渡する意図を持って管理下に置く」ことと定義されている。それによって利益を得るという動機は、必要とされない。しかし、この定義では、被告人が当該パスワードの移転や譲渡を意図しない限り、単なるパスワードの所持は該当しない。同様に、権限のないパスワードを個人的に利用する行為も、1030 条(a)(6)の違反には当たらない。ただし、1030 条の他の条項や 1029 条の違反に当たる可能性はある。

○パスワード又はこれに類する情報

本条項は、単なるパスワードのみならず、「パスワード又はこれに類する情報」の引渡しを禁止するものである。あるユーザーがコンピュータシステムに認証されるためのパスフレーズ、記号、ユーザネーム、他の方法、あるいはそれらの方法の組合せは、1030 条(a)(6)の下で「パスワード」とみなされる可能性がある。

○他の条項との関係

1030 条(a)(6)の事犯はしばしば、1029 条のアクセス装置の事犯とオーバーラップする。パスワードは、1029 条の下ではアクセス装置でもある。

<u>刑法典 1028 条(a)(7)</u>

「刑法典 1028 条　身分証明書類、認証機能、及び情報に関する詐欺及び関連行為」の(a)(7)では、連邦法に違反する犯罪行為又は州法・地域法で重罪となる犯罪行為を行ったり幇助・教唆したりする意図で、又はこれらの犯罪行為に関連して、他人の個人識別手段を合法的権限なく故意に移転、所持、使用することを禁じている。

1028 条(a)(7)は、1998 年の「ID 窃盗・濫用防止法（Identity Theft and Assumption Deterrence Act）」の一部として採択され、2004 年の「ID 窃盗処罰推進法（Identity Theft Penalty Enhancement Act）」で修正された。2004 年の修正においては、個人識別手段の移転と使用を処罰対象とした従来の規定に対して「所持」が追加され、また、連邦法違反又は州法・地域法上の重罪を実行・幇助・教唆したりする意図がなくても、それらの犯罪「に関連して」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、主観的要件の緩和がなされた[20]。

「個人識別手段（means of identification）」は、1028 条(d)において、「単独又は他の情報との組合せで、特定個人を識別するために利用されうる、氏名又は番号」と定義されている。ここには、氏名、社会保障番号、生年月日、政府発行の運転免許証番号その他の番号、指紋・声紋・網膜・虹彩イメージ等の生体データ、ユニークな電子識別番号、アドレス、ルーティングコード、通信を識別する情報、アクセス装置（1029 条(e)の定義による）などが指定されている。

---

[20] 堀田周吾「個人識別情報の不正取得・不正使用に対する刑事訴追」駿河台法学第 23 巻第 1 号（2009 年）、p10～11。

なお、1028 条(a)(7)は、基礎となる犯罪を必要とする。1028 条(a)(7)が基礎とする犯罪の範囲は、後述の 1028A 条のものよりも広範である。1028A 条が、一定の列挙された連邦重罪にのみ基礎を置くのに対し、1028 条(a)(7)はいかなる連邦犯罪（重罪又は軽罪）、州や地域の重罪をも基礎としうる。

刑法典 1028A 条

「刑法典 1028A 条　ID 窃盗による罪の加重」では、被告人が、一定の列挙された連邦犯罪の重罪の実行に際して、又はこれに関連して、他人の個人識別手段を故意に移転、所持、又は使用した事犯において、2 年間の拘禁刑を加重する。列挙された連邦犯罪には、刑法典 1028 条（身分証明書類詐欺）（1028 条(a)(7)は除く）、1029 条（アクセス装置詐欺）、1030 条（コンピュータ詐欺）、1037 条（電子メール詐欺）、1343 条（有線通信詐欺）等がある。また、テロリズムに関連した加重 ID 窃盗の事犯においては、5 年間の拘禁刑を加重する。

刑法典 1028A 条は、2004 年の「ID 窃盗処罰推進法」において追加された。

刑法典 1029 条(a)(1)～(3)

「刑法典 1029 条　アクセス装置に関する詐欺及び関連行為」の(a)(1)～(3)では、権限のないアクセス装置、又は偽造したアクセス装置を、故意かつ詐欺の意図で、製造（作成）・使用・所持（15 個以上）・引き渡すことを禁止している。1029 条の(e)(1)において、アクセス装置は、「金品、サービス、若しくはその他の価値を有するものを入手する目的で使用できる、又は資金の移転（紙の手段のみによって開始される移転を除く）を開始するために使用できる、カード、プレート、コード、アカウント番号、電子シリアル番号、携帯電話識別番号、個人識別番号、その他の電気通信サービス・機材・機器の識別子等」を意味するものとして、広範に定義されている。ネットワーク犯罪に関連したアクセス装置には、パスワードや電子銀行口座番号、クレジットカード番号が含まれる可能性がある[21]。

上記行為に対する罰則は、罰金若しくは 10 年以下の拘禁刑、又はこれらの併科である。2 度目以降の犯行は罰金若しくは 20 年以下の拘禁刑、又はこれらの併科で罰しうる。

1029 条は、盗まれた銀行口座情報やクレジットカード情報、デビットカード情報を被告人が購買したり、販売したり、移転したりするような「カーディング[22]」事犯に適用できる

---

[21] 米国司法省刑事局コンピュータ犯罪・知的財産課・前掲注 8、p 86。「アクセス装置」には「価値のある事柄を不当に取得するためにコンピュータにアクセスするために利用される、盗まれたり不正に入手されたりしたパスワード」が含まれるという判例（United States v. Fernandez, 1993 WL 88197）がある。米国司法省刑事局コンピュータ犯罪・知的財産課・前掲注 8、p 48。

[22] 不正に入手したクレジットカード番号等により商品を購入し、それをオンライン・オークションやオンライン・ショップ等で転売する行為。

可能性がある[23]。

### （６）他人の識別符号の譲受け

他人の ID・パスワード等の識別符号を譲り受ける行為については、上述の刑法典 1028 条(a)(7)（ID 窃盗）、1028A 条（ID 窃盗による罪の加重）、1029 条（アクセス装置詐欺）において規制がなされている。

### （７）他人の識別符号の譲渡しに関する広告又は誘引行為

刑法典 1029 条(a)(6)

刑法典 1029 条の(a)(6)では、アクセス装置の発行者の承認を得ずに、アクセス装置の提供を目的に、又はアクセス装置に関する情報若しくはアクセス装置の入手申込書の販売を目的に、故意かつ詐欺の意図で、勧誘を行う（solicit）ことを禁止している。

上記行為に対する罰則は、罰金若しくは 10 年以下の拘禁刑、又はこれらの併科である。2 度目以降の犯行は罰金若しくは 20 年以下の拘禁刑、又はこれらの併科で罰しうる。

### （８）他人の識別符号の譲受けに関する広告又は誘引行為

上述の刑法典 1028 条、1028A 条、1029 条、1030 条では、他人の識別符号の譲受けに関する広告又は誘引行為は規制されていない。

### （９）アクセス管理者等の防御措置

合衆国法典第 44 編 3544 条

合衆国法典第 44 編第 35 章の「3544 条　連邦機関の責務」[24]では、各連邦機関の長は、当該機関により維持される情報や当該機関等により使用される情報システム等への不正なアクセス・使用・開示・混乱・変更・破壊によってもたらされるリスク及び被害の規模に対応した情報セキュリティ対策を整備することや、国立標準技術院（NIST）等が作成した一定の情報セキュリティ規準を遵守すること等の責任を負うことが規定されている。また、連邦機関の幹部職員には、当該情報又は情報システムに関する不正なアクセス・使用・開示等からもたらされるリスク及び被害の規模を評価することや、一定の規準に基づき当該情報及び情報システムを保護するために適切な情報セキュリティ・レベルを決定すること、定期的な検査及び評価を実施すること等の義務が規定されている。

---

[23] 米国司法省刑事局コンピュータ犯罪・知的財産課・前掲注 8、p 86。

[24] 「2002 年電子政府法（E-Government Act of 2002）」の第 3 編「連邦情報セキュリティマネジメント法（Federal Information Security Management Act of 2002, FISMA）」の一部として導入された。

## ２．２．３　不正アクセスにつながる可能性のある行為に関する法令

### （１）ウィルス作成

刑法典 1030 条の(a)(5)では故意にウィルスを送信する行為を規制しているが、ウィルスの作成行為自体を規制するものではない。

刑法典 1030 条(a)(5)(A)

刑法典 1030 条の(a)(5)(A)では、プログラム・情報・コード・コマンドの送信を故意に発生させ、その結果として、保護されたコンピュータに対して無権限で故意に損害を与える行為を禁じている。

1030 条 の(a)(5)(B)と(C)では、被告人が保護されたコンピュータにアクセスすることが該当要件となっているが、1030 条 の(a)(5) (A)では、コンピュータに損害を与えるために無権限で故意に何かを送信した証拠のみが要求される。アクセスせずにコンピュータに損害を与えることは可能であり、この(A)に該当する例としては、ウィルスの一種であるワームやトロイの木馬を送り付けるような場合が挙げられる[25]。

本条項の違反は、初犯の場合、罰金若しくは 10 年以下の拘禁、又はそれらの併科で罰しうる。被告人が 1030 条の前科を持つ場合は、罰金若しくは 20 年以下の拘禁、又はそれらの併科で罰しうる。

### （２）識別符号の不正取得（フィッシングサイトの構築等）

フィッシングサイトの構築については、上述の刑法典 1028 条、1028A 条、1029 条等によって規制することが可能である[26]。

2005 年 3 月に「アンチフィッシング法案（Anti-Phishing Act of 2005）」[27]が連邦議会に提出されたが、2010 年 11 月時点では同法案は成立していない。

刑法典 1028 条(a)(7)

刑法典 1028 条の(a)(7)では、上述のように、連邦法に違反する犯罪行為又は州法・地域法で重罪となる犯罪行為を行ったり幇助・教唆したりする意図で、又はこれらの犯罪行為に関連して、他人の個人識別手段（電子識別番号やパスワードが含まれる）を合法的権限なく故意に移転、所持、使用することを禁じている。

刑法典 1028A 条

刑法典 1028A 条では、上述のように、一定の列挙された連邦犯罪の重罪の実行に際して、

---

[25] 米国司法省刑事局コンピュータ犯罪・知的財産課・前掲注 8、 p 32。
[26] 米国司法省刑事局コンピュータ犯罪・知的財産課・前掲注 8、 p 86、p128。
[27] 同法案では、消費者を詐欺行為を働くために偽のサイトを作成したり、偽の電子メールを送った者は 5 年以下の拘禁刑若しくは 25 万ドル以下の罰金刑、又はそれらの併科に処するとしている。

又はこれに関連して、他人の個人識別手段を故意に移転、所持、又は使用した事犯において、2 年間の拘禁刑を加重するものである。

刑法典 1029 条(a)(1)～(3)

刑法典 1029 条では、上述のように、権限のないアクセス装置（個人識別番号やパスワードが含まれる）、又は偽造したアクセス装置を、故意かつ詐欺の意図で、作成・使用・所持・引き渡すことを禁止している。

### （３）サイバーテロ行為

Dos 攻撃については、刑法典 1030 条(a)(5)(A)、1362 条を適用することが可能である[28]。

刑法典 1030 条(a)(5)(A)

刑法典 1030 条の(a)(5)(A)では、上述のように、プログラム・情報・コード・コマンドの送信を故意に発生させ、その結果として、保護されたコンピュータに対して無権限で故意に損害を与える行為を禁じている。

刑法典 1362 条

「刑法典 1362 条　通信回線、通信局、又は通信システム」では、連邦機関によって運営等されているシステム等の運用や使用を妨害する者は、罰金若しくは 10 年以下の拘禁に処し、又はこれを併科すると規定されている。

## ２．２．４　不正アクセスに関係する行為の捜査に関する法令

### （１）不正アクセスに関係する行為の捜査における通信傍受

刑法典 2511 条

「刑法典 2511 条　有線通信、口頭の会話又は電子的通信の傍受及び開示の禁止」において通信傍受は一般原則として禁止されているが、その例外として、同条の(2)(a)(ⅱ)では、電子的通信サービスのプロバイダ若しくは職員等は、裁判所命令、又は刑法典 2518 条の(7)に特定された者若しくは合衆国司法長官による証明書を与えられた場合は、電子的通信の傍受等を法律により授権された者に対し、情報、設備又は技術的支援を提供する権限を有することが規定されている。

刑法典 2518 条

「刑法典 2518 条　有線通信、口頭の会話又は電子的通信の傍受のための手続き」の(1)では、電子的通信等の傍受を授権又は承認する裁判所命令の請求は、下記の情報を含む書

[28] 米国司法省刑事局コンピュータ犯罪・知的財産課・前掲注 8、ｐ127。

面によって行わなければならないと規定されている。

- 請求を行う捜査官又は法執行官の身元、及び請求の権限を与える職員の身元
- 請求者が依拠する事実及び事情
  - 当該犯罪の詳細
  - 通信傍受を行うための設備又は場所の性質及び所在地
  - 傍受しようとする通信の種類
  - 通信が傍受されるべき者の身元が分かるときは、その身元
- 別の捜査手続を試みたが失敗したか否か等についての陳述
- 傍受を要求する期間
- 同一の人物、設備又は場所の傍受に関して行われたこれまでの全ての請求、及びそれぞれの請求について裁判官が下した判断　等

また、同条の(4)では、電子的通信等の傍受を授権又は承認する裁判所命令は、下記の内容を特定しなければならないと規定されている。

- 通信が傍受される者の身元が分かるときは、その身元
- 傍受が授権された通信設備又は場所の性質及び所在地
- 傍受しようとする通信の種類及びそれに関連する犯罪の陳述
- 通信の傍受を授権された機関及び請求の権限を与えた者の身元
- 傍受が授権される期間

また同条の(4)では、裁判所命令に基づき設備又は技術的支援を提供した電子的通信サービスのプロバイダ等は、そのことにより負担した相当の費用を請求者（法執行機関等）により補償されなければならないと規定されている。

なお、同条の(7)において、人の死や重大な身体的障害の急迫の危険、国家安全保障上の利益を脅かす共同謀議又は組織犯罪に特有の共同謀議等の緊急事態が存在し、裁判所命令を取得する前に電子的通信等を傍受する必要がある場合には、司法長官・司法次官・司法副次官、又は州・行政的小区域（行政的下部組織）の主たる検察官によって特別に指名された捜査官・法執行官は、傍受が行われたとき又は着手されたときから 48 時間以内に傍受を承認する命令のための請求を行うことを条件として、電子的通信等の傍受を行うことができると規定されている。

### （２）不正アクセスに関係する行為の捜査における差押場所が明確でない場合の措置

<u>刑法典 2703 条</u>

「刑法典 2703 条　顧客の通信又は記録の要求された開示」の(a)では、政府機関は電子的通信サービスのプロバイダに対して、電子的通信システムにおいて 180 日以下の期間、電子的に蓄積されている電子的通信等の内容については、裁判所の令状又は州の同等の令状

によって、その開示を要求できると規定している。また、電子的通信システムにおいて 180 日を越えて電子的に蓄積されている電子的通信等の内容については、裁判所の令状又は州の同等の令状によるほか、同条の(d)に規定する裁判所命令等によっても、その開示を要求することができると規定している[29]。後者の裁判所命令等によって開示要求をする場合は、受信契約者（subscriber）又は顧客（customer）に対して事前に通知を行うことが必要である。

2703 条の(c)(2)において、電子的通信サービスのプロバイダが政府機関からの開示要求に従って開示する内容は、以下のものと規定されている。

- 氏名
- 住所
- 近距離及び長距離電話接続記録、又はセッション時刻及び時間の記録
- サービスの期間及び利用されるサービスの種類
- 電話番号、機器番号又は暫定的に割り当てられたネットワーク・アドレスを含む受信契約者の他の番号若しくはその識別子
- （クレジットカード番号又は銀行口座番号を含む）サービスの支払いのための方法及び財源

### （３）ログの保存

刑法典 2703 条

刑法典 2703 条の(f)では、電子的通信サービス等のプロバイダは、政府機関の要求を受けて、裁判所命令の発付又は他の手続の結果が出るまで、その専有する記録及び他の証拠を保存するために必要な全ての手続をとらなければならないと規定されている。また、その保存期間は 90 日間と規定され、その期間は政府機関の更新要求によりさらに 90 日間延長されると規定されている。

[29] 刑法典 2703 条の(b)では、遠隔コンピュータ処理サービス（remote computing service）のプロバイダに対して同様の方法で、電子的通信等の内容の開示を要求できると規定している。なお、遠隔コンピュータ処理サービスは、刑法典 2711 条において、電子的通信システムを通じてコンピュータ蓄積サービス又は処理サービスを公衆に提供することと定義されている。

## ２．３　不正アクセス関連法令条文集

### （１）刑法典（合衆国法典第 18 編）

○関連する条項の抜粋訳

**刑法典 1028 条　身分証明書類、認証機能、及び情報に関する詐欺及び関連行為**　（仮訳）

(a) 本条 (c) 項に説明されている状況において、以下の (1) から (8) 号のいずれかに該当するいかなる者も、本条 (b) 項の規定により処罰される。

(1) 故意に、かつ合法的権限を持たずに、身分証明書類、認証機能、又は虚偽の身分証明書類を発行した。

(2) 身分証明書類、認証機能、若しくは虚偽の身分証明書類が盗まれたか、又は合法的権限なしに発行されたことを知りながら、かかる文書又は機能を故意に移転した。

(3) 5 つ以上の身分証明書類（所持者が使用するために合法的に発行されたものを除く）、認証機能、又は虚偽の身分証明書類を、違法に使用する意図で故意に所持するか、又は違法に移転した。

(4) 合衆国を欺くために使用する意図で、身分証明書類（所持者が使用するために合法的に発行されたものを除く）、認証機能、又は虚偽の身分証明書類を故意に所持した。

(5) 虚偽の身分証明書類の作成、又は同様の目的で使用する別の文書作成機能若しくは認証機能の作成に使用する意図で、文書作成機能又は認証機能を故意に作成、移転、又は所持した。

(6) 合衆国の、又は全国的な重要性を持つ特別イベントとして指定されたイベントの後援団体の身分証明書類若しくは認証機能であるか、又はそのように見える身分証明書類若しくは認証機能で、盗まれたか又は合法的権限なしに発行されたものを、盗まれたか又は合法的権限なしに発行されたものであることを知りながら故意に所持した。

(7) 連邦法の違反を構成する、又はいずれかの適用される州法又は地域法の下で重罪を構成する、何らかの非合法活動を働く、又は幇助若しくは教唆する意図で、又はかかる非合法活動に関連して、他人の個人識別手段を合法的権限なしに故意に移転、所持、又は使用した。又は、

(8) 虚偽の身分証明書類、文書作成機能、又は個人識別手段において使用するために、虚偽の又は本物の認証機能を故意に引き渡した。

(b) 本条 (a) 項に基づく違法行為に対する処罰は、以下の通りである。

(1) (3) 号及び (4) 号に定めるものを除き、犯罪が以下の (A) から (D) に該当する場合は、本編に基づく罰金若しくは 15 年以下の拘禁に処し、又はこれを併科する。

(A) 以下の (i) 若しくは (ii) であるか、又はそのように見える身分証明書類、認証機能、又は虚偽の身分証明書類の作成又は移転。

(i) 合衆国によって、又は合衆国の権限下で発行された身分証明書類又は認証機能、又は、

(ii) 出生証明書、又は運転免許証若しくは個人識別カード。

(B) 5 つを超える身分証明書類, 認証機能、又は虚偽の身分証明書類の作成又は移転。

(C) 同項の (5) 号に基づく違法行為、又は、

(D) 違法行為の結果、いつの時点であれ 1 年の期間中に、犯罪を行ったいずれかの個人が総額 1,000 ドル又はそれ以上の価値を持つ何かを得た場合、1 つ又はそれ以上の個人識別手段の移転、所持、又は使用を伴う、同項の (7) 号に基づく犯罪。

(2) (3) 号及び (4) 号に定めるものを除き、犯罪が以下の (A) 又は (B) に該当する場合は、本編に基づく罰金若しくは 5 年以下の拘禁に処し、又はこれを併科する。

(A) 個人識別手段、身分証明書類、認証機能、又は虚偽の身分証明書類のその他一切の作成、移転、又は使用。又は、

(B) 同項の (3) 又は (7) 号に基づく犯罪。

(3) 犯罪が以下の (A) から (C) のいずれかに該当する場合は、本編に基づく罰金若しくは 20 年以下の拘禁に処し、又はこれを併科する。

(A) 麻薬取引犯罪の幇助（第 929 条 (a)項(2)号の定義による）。

(B) 暴力犯罪との関連（第 924 条 (c)項(3)号の定義による）又は、

(C) 本条に基づく以前の有罪判決が確定する。

(4) 国内テロ行為(本編の第 2331 条 (5) の定義による)又は国際テロ行為(本編の第 2331 条 (1) の定義による）を幇助するために犯罪が行われた場合は、本編に基づく罰金若しくは 30 年以下の拘禁に処し、又はこれを併科する。

(5) (a) 項に基づくいかなる犯罪の場合も、犯罪に使用された、又は使用が意図された一切の個人財産の合衆国による没収。及び、

(6) その他のいかなる場合においても、本編に基づく罰金若しくは 1 年以下の拘禁に処し、又はこれを併科する。

(c) 本条 (a) 項で言及されている状況は、以下の通りである。

(1) 身分証明書類、認証機能、又は虚偽の身分証明書類が、合衆国の、若しくは全国的な重要性を持つ特別イベントとして指定されたイベントの後援団体によって、若しくはその権限下で発行された、若しくはそのように見える。又は、文書作成機能が、かかる身分証明書類、認証機能、若しくは虚偽の身分証明書類の作成用に計画されている、若しくは適している。

(2) 犯罪が、本条 (a) 項 (4) 号に基づく犯罪である。又は、

(3) 以下の (A) 又は (B) が該当する。

(A) 本条によって禁じられている作成、移転、所持、又は使用が、電子的手段による文書の移転を含め、州際又は国際商取引において行われている、又はかかる商取引に影響を与えている。又は、

(B) 個人識別手段、身分証明書類、虚偽の身分証明書類、又は文書作成機能が、本条によって禁じられている作成、移転、所持、又は使用の過程で、メールにおいて送信される。

(d) 本条及び第 1028A 条において、

(1) 「認証機能（authentication feature）」という用語は、文書が偽造されているか、改変されているか、又はその他の方法で変造されているかどうかを判断するために、個別に又は別の機能との組み合わせで、発行当局によって、身分証明書類、文書作成機能、又は個人識別手段に使用される、ホログラム、透かし、証明書、記号、コード、画像、数列若しくは文字列、又は、他の機能の一切をいう。

(2) 「文書作成機能（document-making implement）」という用語は、身分証明書類、虚偽の身分証明書類、又は他の文書作成機能を作るために特に設定されている、又は主として使用される装置、インプレッション、テンプレート、コンピュータ・ファイル、コンピュータ・ディスク、電子装置、又はコンピュータ・ハードウェア若しくはソフトウェアの一切をいう。

(3) 「身分証明書類（identification document）」という用語は、合衆国政府、州、州の行政的小区域、全国的な重要性を持つ特別イベントとして指定されたイベントの後援団体、外国政府、外国政府の行政的小区域、国際政府機関若しくは国際準政府機関によって作成された、又は発行された、若しくはその権限下で発行された文書で、特定の個人に関する情報が記載されている場合は、個人の身分証明を目的とし、又は個人の身分証明として一般的に受け入れられる種類のものをいう。

(4) 「虚偽の身分証明書類（false identification document）」という用語は、個人の身分証明を目的とし、又は個人の身分証明として一般的に受け入れられる種類の文書で、以下のものをいう。

(A) 政府機関によって、若しくは政府機関の権限下で発行されていない、又は政府機関の権限下で発行されたが、その後詐欺を目的に改変された。及び、

(B) 合衆国政府、州、州の行政的小区域、全国的な重要性を持つ特別イベントとして大統領によって指定されたイベントの後援団体、外国政府、外国政府の行政的小区域、又は国際政府機関若しくは国際準政府機関によって発行された、又はその権限下で発行されたと見られる。

(5) 「虚偽の認証機能（false authentication feature）」という用語は、以下の (A) から (C) が該当する認証機能をいう。

(A) 元は本物であるが、発行当局の承認を得ずに、詐欺を目的に改ざん又は変更された。

(B) 本物であるが、発行当局の承認を得ずに、及び、それぞれの発行当局によって、かかる認証機能が添付される又は組み込まれることが意図されている、合法的に作成された身分証明書類、文書作成機能、又は個人識別手段と関係なく、配信されたか、又は配信が意図されている。又は、

(C) 本物のように見えるが実際にはそうでない。

(6) 「発行当局（issuing authority）」という用語は

(A) 身分証明書類、個人識別手段、又は認証機能を発行する権限を持つ一切の政府機関又は行政機関をいう。又、

(B) 合衆国政府、州、州の行政的小区域、全国的な重要性を持つ特別イベントとして大統領によって指定されたイベントの後援団体、外国政府、外国政府の行政的小区域、又は国際政府機関若しくは国際準政府機関を含む。

(7) 「個人識別手段（means of identification）」という用語は、以下の (A) から (D) のいずれかを含め、単独又は他の情報との組合せで、特定個人を識別するために使用される、氏名又は番号をいう。

(A) 名前、社会保障番号、生年月日、州又は政府発行の正式な運転免許証又は識別番号、外国人登録番号、政府のパスポート番号、雇用主又は納税者の識別番号。

(B) 指紋、声紋、網膜若しくは虹彩のイメージ、又は身体を一意に代表するその他のものなど、一意のバイオメトリック・データ。

(C) 一意の電子識別番号、アドレス、又はルーティングコード、又は

(D) 通信識別情報又はアクセス装置（第 1029 条 (e) 項の定義による）。

(8) 「個人識別カード（personal identification card）」という用語は、専ら識別を目的に州又は地方自治体によって発行された身分証明書類をいう。

(9) 「作成する（produce）」という用語には、改変、認証、又は組み立てるという意味が含まれる。

(10) 「移転する（transfer）」という用語には、身分証明書類、虚偽の身分証明書類、又は文書作成機能を選択し、かかる身分証明書類、虚偽の身分証明書類、又は文書作成機能を、他人が利用できるオンラインの場所に置くか、又は配置を指示することが含まれる。

(11) 「州（State）」という用語には、合衆国の一切の州、コロンビア特別区、プエルトリコ合衆国自治連邦区、及び合衆国のその他一切のコモンウェルス、所持地、又は領土が含まれる。及び、

(12) 「引き渡す（traffic）」という用語は、以下の (A) 又は (B) をいう。

(A) 価値のある何かの対価として、輸送、移転、又はその他の方法で他者に譲渡すること。又は、

(B) かかる輸送、移転、又はその他の方法による譲渡を行う意図で支配する、又は支配を得ること。

(e) 本条は、合衆国、州、若しくは州の行政的小区域の法執行機関による、又は合衆国の情報機関による、適法に認可された一切の捜査、保護、若しくは情報活動、又は本編の第 224 章に基づいて認可されるいかなる行為をも禁じるものではない。

(f) 企て及び共謀。 本条に基づきいかなる犯罪を企てる者も、又は共謀を企むいかなる者も、違反した場合に企て又は共謀の対象とされていた犯罪に対して規定されているものと同一の処罰の対象となる。
(g) 没収手続き。 本条に基づく財産の没収は、財産の一切の押収及び処分、並びに一切の関連する訴訟手続き又は行政手続きを含め、1970 年の包括的薬物乱用防止及び規制法（Comprehensive Drug Abuse Prevention and Control Act of 1970）（21 U.S.C. 853）第 413 条（同条 (d) 項を除く）の規定に準拠する。
(h) 没収、処分。 いかなる者も第 (a) 項の違反で有罪判決を受けた状況では、裁判所は、規定の処罰に加えて、違法な認証機能、身分証明書類、文書作成機能、又は個人識別手段すべての没収及び破棄又はその他の処分を命じる。
(i) 解釈のルール。 (a) 項 (7) 号において、1 つ以上の個人識別手段を含む単一の身分証明書類又は虚偽の身分証明書類は、1 つの個人識別手段として解釈される。

**刑法典 1028A 条　ID 窃盗による罪の加重**　（仮訳）

(a) 犯罪。
(1) 総則。 (c) 項に列挙されているいずれかの重大な違反中に、及びかかる違反との関連で、他人の個人識別手段を合法的権限なしに故意に移転、所持、又は使用したいかなる者も、かかる重罪について定められている処罰に加えて、拘禁 2 年に処せられる。
(2) テロによる犯罪。 第 2332b 条 (g)項(5)号(B) に列挙されているいずれかの重大な違反中に、及びかかる違反との関係で、他人の個人識別手段又は虚偽の身分証明書類を合法的権限なしに故意に移転、所持、又は使用したいかなる者も、かかる重罪について定められている処罰に加えて、拘禁 5 年に処せられる。
(b) 逐次執行の刑の宣告。 法律のその他一切の規定にかかわらず、
(1) 裁判所は、本条に対する違反で有罪判決を受けたいかなる者にも執行猶予を与えてはならない。
(2) (4) 号に規定されている場合を除き、本条に基づいて課される一切の拘禁期間は、個人識別手段を移転、所持、又は使用していた重罪に対して課される一切の拘禁の期間を含め、法律のその他一切の規定に基づいてその者に課されるその他一切の拘禁の期間と重ねて執行することができない。
(3) 個人識別手段を移転、所持、又は使用していた重罪に対して課される一切の拘禁期間の決定において、裁判所は、本条に対する違反で課された拘禁、又は課される予定の拘禁の一切の別の期間を補うために、又は別の方法で考慮に入れるために、かかる犯罪に対して課される拘禁の期間を決して短縮してはならない。及び、
(4) 本条の違反に対して課される拘禁の期間は、裁判所が本条に対する別の違反に対してその者に同時に課す拘禁の別の期間との間でのみ、裁判所の裁量において、全部又は一部を重ねて執行することができる。ただし、かかる裁量は、第 28 編の第 994 条に従っ

て量刑委員会によって発行されたいずれかの該当するガイドライン及び方針声明に従って行使する。

(c) 定義。 本条において、「(c) 項に列挙されている重大な違反」とは、以下の重大な違反である一切の違反行為をいう。

(1) 第 641 条（公金、公共財産、又は公的報酬の盗みに関して）、第 656 条（銀行の役員若しくは従業員による盗み、着服、又は不正使用に関して）、又は第 664 条（従業員福利制度からの盗みに関して）。

(2) 第 911 条（市民権の氏名詐欺に関して）

(3) 第 922 条 (a)項(6)号（銃器の取得との関連における虚偽の陳述に関して）。

(4) 本条又は第 1028 条 (a)項(7)号を除く、本章に含まれている一切の規定（詐欺及び虚偽の陳述に関して）。

(5) 第 63 章に含まれている一切の規定（メール、銀行、及び有線通信の不正行為に関して）。

(6) 第 69 章に含まれている一切の規定（国籍及び公民権に関して）。

(7) 第 75 章に含まれている一切の規定（パスポート及びビザに関して）。

(8) グラム・リーチ・ブライリー法（15 U.S.C. 6823）の第 523 条（虚偽の見せかけによる顧客情報の取得に関して）。

(9) 移民国籍法（8 U.S.C. 1253 及び 1306）の第 243 条又は第 266 条（国外追放の後に合衆国からの退去を故意に怠ること、及び外国人登録カードの偽造に関して）。

(10) 移民国籍法（8 U.S.C. 1321 以下参照）の第 II 編の第 8 章に含まれている一切の規定（さまざまな入国法違反に関して）。又は、

(11) 社会保障法（42 U.S.C. 408、1011、1307 (b)、1320a–7b (a)、及び 1383a）第 208 条、811 条、1107 条 (b) 項、1128B 条 (a) 項、又は 1632 条（同法に基づくプログラムについての虚偽の陳述に関して）。

**刑法典 1029 条　アクセス装置に関する詐欺及び関連行為**　（仮訳）

(a) いかなる者も、

(1) 故意に、かつ詐欺の意図で、1 台以上の偽造アクセス装置を製造し、使用し、又は引き渡した場合、

(2) いつの時点であれ 1 年の期間中に、故意に、かつ詐欺の意図で、1 台以上の権限のないアクセス装置を引き渡したか、又は使用し、かかる行為によってその期間中に総額 1,000 ドル又はそれ以上の価値を持つ何かを得た場合、

(3) 故意に、かつ詐欺の意図で、15 台以上の偽造又は権限のないアクセス装置を所持した場合、

(4) 故意に、かつ詐欺の意図で、装置作成機器を製造し、引き渡し、管理若しくは保管し、又は所持した場合、

(5) いつの時点であれ 1 年の期間中に、総額 1,000 ドル若しくはそれ以上の価値を持つ決済、又はその他のものを受け取るために、他人に対して発行された 1 台以上のアクセス装置によって、故意に、かつ詐欺の意図で取引を行った場合、

(6) アクセス装置の発行者の承認を得ずに、以下の (A) 又は (B) を目的に、故意に、かつ詐欺の意図で、勧誘を行った（solicit）場合、

(A) アクセス装置の提供、又は、

(B) アクセス装置に関する情報、又はアクセス装置の入手申込書の販売。

(7) 故意に、かつ詐欺の意図で、通信サービスを不正使用するために、修正又は変更された通信機器を使用し、製造し、引き渡し、管理若しくは保管し、又は所持した場合、

(8) 故意に、かつ詐欺の意図で、スキャニング・レシーバを使用し、製造し、引き渡し、管理若しくは保管し、又は所持した場合、

(9) 通信機器と関連付けられている、又は通信機器に含まれている通信識別情報を挿入又は修正するように設定済みであることを知った上で、かかる機器が無権限で通信サービスの入手に使用できるように、ハードウェア又はソフトウェアを故意に使用し、製造し、引き渡し、管理若しくは保管し、又は所持した場合、又は、

(10) クレジットカード・システム会員又はその代理店の承認を得ずに、故意に、かつ詐欺の意図で、支払いのために、アクセス装置によって行われた取引の 1 つ以上の証拠又は記録を会員又はその代理店に提示することを他人にさせるか、又はかかる行為を手配した場合、

かかる犯罪が州際又は国際商取引に影響を与える場合、本条 (c) 項の規定により処罰される。

(b)

(1) 本条 (a) 項に基づく犯罪を企てる一切の者は、企てられた犯罪に対して規定されているものと同一の処罰の対象となる。

(2) いかなる者も、本条 (a) 項に基づく犯罪を 2 名以上で共謀した当事者である者は、当事者のいずれかが当該犯罪を助長させるために何らかの行為に着手した場合、本条 (c) 項に基づく犯罪に対する最高額の罰金を超過しない額の罰金、若しくは本条 (c) 項に基づく犯罪に対する最長拘禁の 2 分の 1 の期間を超過しない期間の拘禁に処し、又はこれを併科する。

(c) 罰則

(b) 総則 本条 (a) 項に基づく犯罪に対する処罰は、以下の通りである。

(A) 本条に基づき他の犯罪で有罪判決を受けた後に発生したものではない犯罪の場合

(i) 当該犯罪が、(a) 項の (1)、(2)、(3)、(6)、(7) 又は (10) 号に該当する場合は、本編に基づく罰金若しくは 10 年以下の拘禁に処し、又はこれを併科する。及び、

(ii) 当該犯罪が、(a) 項の (4)、(5)、(8) 又は (9) 号に該当する場合は、本編に基づく罰金若しくは 15 年以下の拘禁に処し、又はこれを併科する。及び、

(B) 本条に基づき他の犯罪で有罪判決を受けた後に発生した犯罪の場合、本編に基づく罰金若しくは 20 年以下の拘禁に処し、又はこれを併科する。及び、

(C) いずれの場合においても、犯罪に使用されたか、又は使用が意図された一切の個人財産の合衆国による没収。

(2) 没収手続き　本条に基づく財産の没収は、財産の一切の押収及び処分、並びに一切の関連する行政手続き及び訴訟手続きを含め、統制薬物法（Controlled Substances Act）の第 413 条に準拠する。ただし、同条の（d）項を除く。

(d)（略）

(e) 本条において用いる場合、

(1)「アクセス装置（access device）」という用語は、単独で、又は他のアクセス装置との連携により、金品、サービス、若しくはその他の価値を有するものを入手する目的で使用できる、又は資金の移転（紙の手段のみによって開始される移転を除く）を開始するために使用できる、カード、プレート、コード、アカウント番号、電子シリアル番号、携帯電話識別番号、個人識別番号、又はその他の通信サービス・機材・機器の識別子、又はその他のアカウントアクセス手段の一切をいう。

(2)「偽造アクセス装置（counterfeit access device）」という用語は、偽造の、架空の、修正された、若しくは改変された一切のアクセス装置、又はアクセス装置若しくは偽造アクセス装置の識別可能な構成要素をいう。

(3)「権限のないアクセス装置（unauthorized access device）」という用語は、紛失した、盗難に遭った、期限切れ、無効、取り消しとなった、又は詐欺の意図で入手された一切のアクセス装置をいう。

(4)「作成する（produce）」という用語には、デザイン、改変、認証、複製、又は組み立ての意味が含まれる。

(5)「引き渡す（traffic）」という用語は、他人に移転する、若しくは他人に譲渡す、又は移転したり譲渡する意図を持って管理下に置くことをいう。

(6)「装置作成機器（device-making equipment）」という用語は、アクセス装置若しくは偽造アクセス装置を作成するために設計された、若しくはそのために主として使用される、機材、仕組み、又はインプレッションの一切をいう。

(7)「クレジットカード・システム会員（credit card system member）」という用語は、クレジットカード・システムの唯一の会員であるクレジットカード発行者と提携しているか、又はそれと同一である組織を含め、クレジットカード・システムの会員である金融機関又はその他の組織をいう。

(8)「スキャニング・レシーバ（scanning receiver）」という用語は、第 119 章に違反して有線若しくは電子通信の傍受、又は通信サービス、機材、若しくは機器の電子シリアル番号、モバイル識別番号、若しくはその他の識別子の傍受に使用できる装置又は器具をいう。

(9)「通信サービス（telecommunications service）」という用語は、1934 年通信法第 I 編第 3 条（47 U.S.C. 153）の用語と同じ意味を持つ。

(10)「設備ベースのキャリア（facilities-based carrier）」という用語は、通信設備を持ち、当該設備の運営及び維持について責任を有し、1934 年通信法第 III 編の権限下で、連邦通信委員会から発行された運用免許を有する組織をいう。及び、

(11)「通信識別情報（telecommunication identifying information）」という用語は、特定の通信機器若しくはアカウントを識別する電子シリアル番号又はその他一切の番号若しくは信号、又は通信機器から送信された特定の通信をいう。

(f)（略）

(g)（略）

(h) 合衆国の司法管轄内で犯した場合に本条 (a) 項又は (b) 項に定める犯罪を構成するいずれかの行為に合衆国の司法管轄外で携わった者は誰でも、以下の (1) 及び (2) 号が該当する場合、本編に定める罰金、刑罰、拘禁、及び没収の対象となる。

(1) 当該犯罪が、金融機関、アカウントの発行者、クレジットカード・システム会員、又は合衆国の司法管轄内のその他の組織によって発行、所有、管理、又は制御されているアクセス装置に関係している場合、及び

(2) 当該人物が、当該犯罪の幇助に使用された何らかの品物、又は当該犯罪による利益若しくはそこから得られた財産を合衆国の司法管轄に、若しくは合衆国の司法管轄を通過して、輸送、配達、運搬、移転し、又は他の方法で合衆国の司法管轄内に保管、隠匿、若しくは保管した場合。

**刑法典 1030 条　コンピュータに関連する詐欺及び関連行為**　（仮訳）

(a) いかなる者も、

(1) 無権限で、又は付与されたアクセス権限を超えて、故意にコンピュータにアクセスし、かつ、当該行為によって、かかる手段で入手された当該情報が合衆国に損害を与える目的又はいずれかの外国に有利となるような目的で使用され得ると考える理由がありながら、国防又は外交関係上の理由で無許可の情報開示からの保護が必要である旨大統領命令若しくは制定法に従い合衆国政府によって決定された情報、又は 1954 年原子力法第 11 条 y 号に定義された何らかの機密データを入手し、これを故意に通信、配信、送信し、又は通信、配信、若しくは送信されるようにし、又はこれを受信する権限を持たないいずれかの者に対して通信、配信、送信を試み、又は通信、配信、若しくは送信されるように試み、又はこれを受信する権限を持つ合衆国の公務員若しくは被雇用者に対して当該情報を故意に留保し、かつ配信を怠った場合

(2) 故意に、無権限でコンピュータにアクセスし、又は付与されたアクセス権限を超えてアクセスし、それによって以下の (A) から (C) を入手した場合

(A) 第 15 編第 1602 条 (n) 項に定義する金融機関若しくはカード発行者の金融記録に含まれている情報、又は公正信用報告法（15 U.S.C. 1681 以下参照）に定義する用語の意味における、消費者信用調査機関のファイルに含まれている情報

(B) 合衆国のいずれかの省庁若しくは行政機関からの情報、又は、

(C) いずれかの保護されたコンピュータからの情報

(3) 故意に、合衆国の省庁若しくは行政機関のいずれかの非公開コンピュータにアクセスする権限なくして、専ら合衆国政府のために使用される省庁又は行政機関のコンピュータにアクセスした場合、又は、かかる用途を専用としないコンピュータの場合は、合衆国政府によって若しくは合衆国政府のために使用されるコンピュータにアクセスした場合に、その行為によって合衆国政府による若しくは合衆国政府のための使用に影響が及んだ場合

(4) 故意に、かつ詐欺の意図で、保護されたコンピュータに無権限でアクセスし、又は付与されたアクセス権限を超えてアクセスし、当該行為によって意図された詐欺を助長し、価値を持つ何かを得た場合。ただし、詐欺の対象及び入手したものが、コンピュータの使用のみによって構成され、かつ、かかる使用の価値がいつの時点であれ 1 年の期間中に 5,000 ドルを超えない場合に限られる。

(5)

(A) プログラム、情報、コード、若しくはコマンドの送信を故意に発生させ、かかる行為の結果として、保護されたコンピュータに対して無権限で故意に損害を与えた場合

(B) 保護されたコンピュータに無権限で故意にアクセスし、かかる行為の結果として、無謀に損害を与えた場合、又は、

(C) 保護されたコンピュータに無権限で故意にアクセスし、かかる行為の結果として、損害と損失を与えた場合

(6) それを通じてコンピュータが無権限でアクセスされうるような、パスワード又はこれに類する情報を、故意に、かつ、詐欺の意図をもって引き渡し（第 1029 条の定義による）、

(A) 当該引渡しが州際又は国際商取引に悪影響を及ぼす場合、又は、

(B) 当該コンピュータが合衆国政府により利用され、又は合衆国政府のために利用されるものである場合

(7) いかなる者からも金銭又はその他価値あるものをゆすり取る意図で、州際又は国際商取引において、以下の (A) から (C) のいずれかを含む何らかの通信を送信した場合

(A) 保護されたコンピュータに損害を与えるおそれ

(B) 保護されたコンピュータから無権限で、若しくは付与されたアクセス権限を超えて情報を入手するおそれ、又は保護されたコンピュータから無権限で、若しくは付与されたアクセス権限を超えて入手した情報の機密性を損なうおそれ、又は、

(C) 保護されたコンピュータに対する損害との関係における金銭又はその他価値あるものの要求又は要請で、かかる損害が恐喝を助長するために引き起こされた場合、

本条 (c) 項の規定により処罰される。

(b) 本条 (a) 項に基づく犯罪を共謀するか又は犯罪を試みた（attempt to commit：訳注、「未遂」の意味）一切の者は、本条 (c) 項の規定により処罰される。

(c) 本条 (a) 項又は (b) 項に基づく違法行為に対する処罰は、以下の通りである。

(1)

(A) 本条に基づき他の犯罪で有罪判決を受けた後に発生したものではない、本条 (a) 項 (1) 号に基づく犯罪の場合、又は本サブパラグラフに基づき罰せられる犯罪を企てた場合、本編に基づく罰金若しくは 10 年以下の拘禁に処し、又はこれを併科する。及び、

(B) 本条に基づき他の犯罪で有罪判決を受けた後に発生した、本条 (a) 項 (1) 号に基づく犯罪の場合、又は本サブパラグラフに基づき罰せられる犯罪を企てた場合、本編に基づく罰金若しくは 20 年以下の拘禁に処し、又はこれを併科する。

(2)

(A) 本条に基づき他の犯罪で有罪判決を受けた後に発生したものではない、本条 (a) 項 (2) 号、(a) 項 (3) 号、又は (a) 項 (6) 号に基づく犯罪の場合、又は本サブパラグラフに基づき罰せられる犯罪を企てた場合、サブパラグラフ (B) に規定されている場合を除き、本編に基づく罰金若しくは 1 年以下の拘禁に処し、又はこれを併科する。

(B) (a) 項 (2) 号に基づく犯罪の場合、又は本サブパラグラフに基づき罰せられる犯罪を企てた場合、以下の (i) から (iii) のいずれかが該当する場合は、本編に基づく罰金若しくは 5 年以下の拘禁に処し、又はこれを併科する。

(i) 営利又は個人的な金銭的利益を目的に犯罪が行われた。

(ii) 犯罪が、合衆国又はいずれかの州の憲法又は法律に違反して、何らかの犯罪行為又は不法行為を助長するために行われた。又は、

(iii) 入手された情報の価値が 5,000 ドルを超える。及び、

(C) 本条に基づき他の犯罪で有罪判決を受けた後に発生した、本条 (a) 項 (2) 号、(a) 項 (3) 号、若しくは (a) 項 (6) 号に基づく犯罪の場合、又は本サブパラグラフに基づき罰せられる犯罪を企てた場合、本編に基づく罰金若しくは 10 年以下の拘禁に処し、又はこれを併科する。

(3)

(A) 本条に基づき他の犯罪で有罪判決を受けた後に発生したものではない、本条 (a) 項 (1) 号若しくは (a) 項 (7) 号に基づく犯罪の場合、又は本サブパラグラフに基づき罰せられる犯罪を企てた場合、本編に基づく罰金若しくは 5 年以下の拘禁に処し、又はこれを併科する。及び、

(B) 本条に基づき他の犯罪で有罪判決を受けた後に発生した、本条 (a) 項 (4) 号、又は (a) 項 (7) 号に基づく犯罪の場合、又は本サブパラグラフに基づき罰せられる犯罪

を企てた場合、本編に基づく罰金若しくは 10 年以下の拘禁に処し、又はこれを併科する。

(4)

(A) (E) 及び (F) に定めるものを除き、以下の (i) 又は (ii) に該当する場合は、本編に基づく罰金若しくは 5 年以下の拘禁に処し、又はこれを併科する。

(i) 当該犯罪が以下の (I) から (VI) のいずれかを引き起こした（又は、未遂罪の場合は、遂行されていたとしたら引き起こしたであろう）場合は、本条に基づき他の犯罪で有罪判決を受けた後に発生したものではない、(a) 項 (5) 号 (B) に基づく犯罪。

(I) いつの時点であれ 1 年の期間中に 1 人以上の人物に対する損害（及び、合衆国のみによる捜査、起訴、又はその他の手続きにおいて、1 台以上の他の保護されたコンピュータに影響を与えた、関連する行為の過程から生じた損失）で、被害額の合計が 5,000 ドル以上になるもの。

(II) 1 人以上の検診、診察、治療、又は看護の変更若しくは障害、又は潜在的な変更若しくは障害。

(III) 身体的危害。

(IV) 公衆衛生又は治安に対する脅威。

(V) 裁判、国防、又は国家安全保障の推進における合衆国政府の組織によって、又は組織のために使用されるコンピュータに影響を与える損害。又は、

(VI) いつの時点であれ 1 年の期間中に 10 台以上の保護されたコンピュータに影響を与える損害。又は、

(ii) 本サブパラグラフに基づき罰せられる犯罪の未遂。

(B) (E) 及び (F) に定めるものを除き、以下の (i) 又は (ii) に該当する場合は、本編に基づく罰金若しくは 10 年以下の拘禁に処し、又はこれを併科する。

(i) 当該犯罪がサブパラグラフ (A)(i) の (I) から (VI) に定める損害を引き起こした（又は、未遂罪の場合は、遂行されていたとしたら引き起こしたであろう）場合は、本条に基づき他の犯罪で有罪判決を受けた後に発生したものではない、(a) 項 (5) 号 (A) に基づく犯罪。又は、

(ii) 本サブパラグラフに基づき罰せられる犯罪の未遂。

(C) (E) 及び (F) に定めるものを除き、以下の (i) 又は (ii) に該当する場合は、本編に基づく罰金若しくは 20 年以下の拘禁に処し、又はこれを併科する。

(i) 本条に基づき他の犯罪で有罪判決を受けた後に発生した、(a) 項 (5) 号 (A) 又は (B) に基づく犯罪又はその未遂。又は、

(ii) 本サブパラグラフに基づき罰せられる犯罪の未遂。

(D) 以下の (i) 又は (ii) に該当する場合は、本編に基づく罰金若しくは 10 年以下の拘禁に処し、又はこれを併科する。

(i) 本条に基づき他の犯罪で有罪判決を受けた後に発生した、(a) 項 (5) 号 (C) に基づく犯罪又はその未遂。又は、

(ii) 本サブパラグラフに基づき罰せられる犯罪の未遂。

(E) 犯罪者が (a) 項 (5) 号 (A) に違反する行為により、重篤な身体的危害を故意に若しくは無謀に与えるか、又はそれを企てた場合、本編に基づく罰金若しくは 20 年以下の拘禁に処し、又はこれを併科する。

(F) 犯罪者が (a) 項 (5) 号 (A) に違反する行為により、故意に若しくは無謀に死亡させるか、又はそれを企てた場合、本編に基づく罰金、有期若しくは終身の拘禁に処し、又はこれを併科する。又は、

(G) 以下の (i) 又は (ii) に該当する場合は、本編に基づく罰金若しくは 1 年以下の拘禁に処し、又はこれを併科する。

(i) (a) 項 (5) 号に基づくその他一切の犯罪、又は、

(ii) 本サブパラグラフに基づき罰せられる犯罪の未遂。

(d) （略）

(e) 本条において用いる場合、

(1) 「コンピュータ（computer）」という用語は、論理、演算、若しくは保存機能を実行する電子的、電磁的、光学的、電子化学的、又はその他の高速データ処理装置を意味し、かつ、かかる装置と直接関連し、若しくは連動する一切のデータ記憶設備も若しくは通信設備を含む。ただし、自動タイプライター若しくはタイプセッター、携帯用電卓、又はその他同様の装置を含まない。

(2) 「保護されたコンピュータ（protected computer）」という用語は、以下の (A) 又は (B) に該当するコンピュータをいう。

(A) 金融機関、若しくは合衆国政府専用、又はかかる専用でないコンピュータの場合は、金融機関又は合衆国政府によって使用され、犯罪を構成する行為によって金融機関若しくは政府による使用、若しくはこれらのための使用に影響が及ぶもの、又は、

(B) 州際若しくは国際商取引、又は通信に使用される、又はこれらに影響を与えるもので、合衆国の外に設置され、合衆国の州際若しくは国際商取引、又は通信に影響を与える方法で使用されるコンピュータを含む。

(3) 「州（State）」という用語には、コロンビア特別区、プエルトリコ米国自治連邦区、及び米国のその他一切のコモンウェルス、所有地、又は領土が含まれる。

(4) 「金融機関（financial institution）」という用語は、以下の (A) から (I) をいう。

(A) 預金が連邦預金保険会社によって保護されている機関。

(B) 連邦準備金制度又は連邦準備金制度の会員で、一切の連邦準備銀行を含む。

(C) 口座が全米信用組合管理局（National Credit Union Administration）によって保証されている信用組合。

(D) 連邦住宅貸付銀行制度の会員及びいずれかの住宅貸付銀行。

(E) 1971 年農業信用法に基づく連邦農業信用制度の一切の機関

(F) 1934 年証券取引法第 15 条に基づき証券取引委員会に登録したブローカー・ディーラー。

(G) 証券投資家保護公社。

(H) 1978 年国際銀行法第 1 条 (b) 項 (1) 号及び (3) 号に定義されている外国銀行の支店若しくは代理店。及び、

(I) 連邦準備法第 25 条又は第 25 条 (a) 項に基づいて運営されている組織。

(5) 「金融記録（financial record）」という用語は、顧客と金融機関の関係について金融機関が保持している何らかの記録から得られる情報をいう。

(6) 「付与されたアクセス権限を超える（exceeds authorized access）」という用語は、権限に基づいてコンピュータにアクセスし、かかるアクセスを利用して、当該アクセス者が入手又は改変する権限を有さないコンピュータ内の情報を入手又は改変することをいう。

(7) 「合衆国の省庁（department of the United States）」という用語は、政府の立法部門若しくは司法機関、又は第 5 編第 101 条に列挙された行政部の一つをいう。

(8) 「損害（damage）」という用語は、データ、プログラム、システム、若しくは情報の完全性又は可用性に対する何らかの阻害を意味する。

(9) 「政府の組織（government entity）」という用語には、合衆国の政府、合衆国のいずれかの州若しくは行政的小区域、いずれかの外国、及び外国のいずれかの州、行政区分、地方自治体、又はその他の行政的小区域が含まれる。

(10) 「有罪判決（conviction）」という用語には、いずれかの州法に基づき、1 年を超える拘禁によって罰せられる犯罪に対する有罪判決が含まれる。その一要素が、コンピュータに対する不正アクセス、又は付与されたアクセス権限の超過である。

(11) 「損失（loss）」という用語は、犯罪への対処、損害判定の実施、データ、プログラム、システム、又は情報を犯行前の状態に復元するための費用、及び業務の中断によって被った一切の収入の損失、発生した費用、又はその他の間接的損害を含む、一切の被害者が被った一切の合理的な費用をいう。及び、

(12) 「人物、人、者（person）」という用語は、一切の個人、会社、企業、教育機関、金融機関、政府機関、又は法人若しくはその他の組織をいう。

(f) 本条は、合衆国、州、若しくは州の行政的小区域の法執行機関、又は合衆国の諜報機関の合法的な捜査活動、防衛活動、又は諜報活動を禁ずるものではない。

(g) （略）

(h) （略）

(i) （略）

(j) （略）

**刑法典 1362 条 通信回線、通信局、又は通信システム** （仮訳）

建設済みか建設中かに関わらず、合衆国によって運営若しくは制御されている、又は合衆国の軍事防衛若しくは民間防衛機能に使用されるか若しくは使用が意図された何らかの無線、電信、電話、若しくは有線の、回線、局、若しくはシステム、若しくはその他の通信手段の設備、所有物、若しくは機材のいずれかを故意に若しくは悪意を持って傷つけるか若しくは破壊する者、又は、かかる回線若しくはシステムのいずれかの運用若しくは使用を故意に若しくは悪意を持って何らかの方法で妨害する者、又は、かかる回線若しくはシステムのいずれかを介した通信の伝送を故意に若しくは悪意を持って妨害、阻害する、若しくは遅延させる者、又は、かかる行為を企てる若しくは共謀する者は誰でも、本編に基づく罰金若しくは 10 年以下の拘禁に処し、又はこれを併科する。

合衆国によって運営又は制御されていない設備、所有物、又は機材の場合、本条は、合衆国の軍事防衛若しくは民間防衛機能に使用されるか若しくは使用が意図された、いかなる回線若しくはシステムをも傷つけない若しくは破壊しない、集団交渉若しくはその他の相互扶助及び保護を目的とする、いかなる合法的ストライキ活動、又はその他の合法的共同行為にも適用されない。

**刑法典 2511 条　有線通信、口頭の会話又は電子的通信の傍受及び開示の禁止**[30]

(1) この章に別段の定めがある場合を除き、次の者は第４項の定めに従い処罰され、又は第５項の定めに従い訴訟を提起される。

(a) 有線通信、口頭の会話又は電子的通信を、意図的に傍受し、傍受を試み、又は他の者を説得して傍受させ、若しくは傍受を試みさせる者

(b) （略）

(c) （略）

(d) （略）

(e) （略）

(2)(a)(i) （略）

(ii) 他の法律の定めにかかわらず、有線通信サービス若しくは電子的通信サービスのプロバイダ、その職員、被用者若しくは代理人、不動産所有者、管理者又は他の者は、

---

[30] 刑法典 2511 条、2518 条、及び 2703 条の日本語訳については、中川かおり訳「合衆国法典第 18 編犯罪及び刑事手続 第Ⅰ部犯罪 第 119 章有線通信及び電子的通信の傍受及び口頭の会話の傍受」（平野美恵子、土屋恵司、中川かおり「米国愛国者法（反テロ法）（下）」『外国の立法 215』（2003 年 2 月））（http://www.ndl.go.jp/jp/data/publication/legis/215/21501.pdf）、p18～20、p27～30、p38～40 より引用した。

次のいずれかを与えられる場合には、有線通信、口頭の会話若しくは電子的通信の傍受又は 1978 年外国諜報監視法（Foreign Intelligence SurveillanceAct of 1978）第 101 条に定義された電子監視を法律により授権された者に対し、情報、設備又は技術的支援を提供する権限を有する。

(A) 授権する裁判官の署名を受けた、支援を指示する裁判所命令

(B) 法律により令状又は裁判所命令が要求されていないこと、すべての法律上の要件を満たしていること及び特定の支援が要求されていることを内容とする、この編の第 2518 条第 7 項に特定された者又は合衆国司法長官による証明書

これらは、情報、設備又は技術的支援の提供の権限が付与される期間を定め、要求されている情報、設備又は技術的支援を特定するものである。有線通信サービス若しくは電子的通信サービスのプロバイダ、その職員、被用者及び代理人、不動産所有者、管理者又は他の者は、(ii)に基づく命令又は証明書の対象とされる傍受の存在、監視の存在又は傍受若しくは監視を遂行するために利用される装置の存在を開示してはならない。ただし、訴訟手続により別段の要求があり、かつ適切な方法で司法長官又は州若しくはその行政的下部組織の主たる検察官に事前に通知する場合はこの限りではない。開示をした者に対しては、第 2520 条に定める民事賠償責任を課す。有線通信サービス若しくは電子的通信サービスのプロバイダ、その職員、被用者及び代理人、不動産所有者、管理者又は他の特定の人が、この章に基づく裁判所命令又は証明書の文言に従って情報、設備又は支援を提供することは、いかなる裁判所においても訴訟原因として認められない。

(b) ・・・（以下略）

**刑法典 2518 条　有線通信、口頭の会話又は電子的通信の傍受のための手続**

(1) この章に基づく有線通信、口頭の会話又は電子的通信の傍受を授権し、又は承認する命令の請求は、管轄権を有する裁判官への宣誓又は確約のうえで書面により行われ、請求を行うための請求者の権限を記載しなければならない。請求は、次の情報を含まなければならない。

(a) 請求を行う捜査官又は法執行官の身元、及び請求の権限を与える職員の身元

(b) 命令が発せられるべきであるとの請求者の確信を正当化するための、次のものを含む、請求者が依拠する事実及び事情の完全な陳述

(i) 行われた、行われつつあり、又は行われようとしている特定の犯罪の詳細

(ii) 第 11 項に定める場合を除き、通信傍受を行うための設備又は場所の性質及び所在地についての特定的記載

(iii) 傍受しようとする通信の種類の特定的記載

(iv) 犯罪の犯人であって、その通信が傍受されるべき者の身元が分かるときは、その身元

(c) 別段の捜査手続が試みられ、失敗したことがあるか否かについての、又は、合理的に考えて、試みたとしても成功しそうにないか、若しくは危険すぎる理由についての完全な陳述

(d) 傍受の継続を要求する期間の陳述。捜査の性質上、記載された種類の通信が最初に取得された時点で傍受権限が直ちに終了するとすべきではない場合には、その後も同種の通信が行われると信ずる相当な理由を明らかにする事実の詳細な記載

(e) 請求の権限を与えた者又は請求を行った者が知っており、請求に特定されたのと同一の人物、設備又は場所を含む有線通信、口頭の会話又は電子的通信の傍受の授権又は傍受の承認を求めて裁判官に対して行われたこれまでのすべての請求及びそれぞれの請求について裁判官が下した判断に関する事実の完全な陳述

(f) 請求が、命令の期間の延長のためである場合には、傍受によりこれまでに取得された結果の陳述又はその結果の取得に失敗したことについての相当の説明の陳述

(2) 裁判官は、請求者に対し、請求を裏付ける証言又は書面による証拠の提出を、追加して要求することができる。

(3) 請求者の提出した事実に基づいて裁判官が次のことを認定した場合には、裁判官は、その法廷の領域的管轄権の範囲内（及び、領域的管轄権の範囲内で連邦裁判所により授権された移動式通信傍受装置の場合には、合衆国国内であれば、その領域的管轄権の範囲外）で、有線通信、口頭の会話又は電子的通信の傍受を授権し、又は承認するために、請求を受けて、要求通りの又は修正した一方的命令を発することができる。

(a) 個人が、この章の第 2516 条に列挙された特定の犯罪を行った、行いつつあり、又は行おうとしていると信ずることに相当な理由があること。

(b) その犯罪についての特定の通信が傍受により取得されると信ずる相当な理由があること。

(c) 通常の捜査手続が試みられたが失敗したこと、又は、合理的に考えて、試みたとしても成功しそうにないか、若しくは危険すぎること。

(d) 第 11 項に定める場合を除き、有線通信、口頭の会話又は電子的通信が傍受される設備又は場所が、犯罪の遂行に関連して利用されつつあるか、若しくは利用されようとしており、又はその者に貸され、その者の名で登録され、若しくはその者により通常利用されていると信ずる相当な理由があること。

(4) この章に基づき有線通信、口頭の会話又は電子的通信の傍受を授権し、又は承認する命令は、次のものを特定しなければならない。

(a) その通信が傍受される者の身元が分かるときは、その身元

(b) 傍受が授権された通信設備又は場所の性質及び所在地

(c) 傍受しようとする通信の種類の特定的記載及びそれに関係する特定の犯罪の陳述

(d) 通信の傍受を授権された機関及び請求の権限を与えた者の身元

(e) 傍受が授権される期間（記載された通信が最初に取得されたときに傍受が直ちに終了

するべきか否かの陳述を含む。）

この章に基づく有線通信、口頭の会話又は電子的通信の傍受を授権する命令は、請求者の要求を受けて、有線通信サービス若しくは電子的通信サービスのプロバイダ、不動産所有者、管理者又は他の者に対して、その通信が傍受される者にサービス・プロバイダ、不動産所有者、管理者又は他の者が提供するサービスについて、控えめかつ最小限の介入で傍受を達成するために必要なすべての情報、設備及び技術支援を直ちに請求者に与えるよう指示する。その設備又は技術支援を提供する有線通信サービス若しくは電子的通信サービスのプロバイダ、不動産所有者、管理者又は他の者は、設備又は支援を提供することで負担した相当の費用を請求者により補償されなければならない。命令は、この章の第 2522 条に従い、法執行通信支援法（Communications Assistance for Law Enforcement Act）に基づく支援の能力及び適応力の要求のためにも発付することができる。

(5) この条に基づいて発付される命令は、権限の目的を達成するために必要な期間を超えて有線通信、口頭の会話又は電子的通信の傍受を授権し、又は承認することはできず、いかなるときも 30 日間以上は認められない。この 30 日間は、捜査官若しくは法執行官が命令に基づく傍受を最初に開始した日又は命令が発付されてから 10 日後のいずれか早い日から起算する。命令の延長は、この条の第 1 項に従って行われる延長の請求を受けて、裁判所がこの条の第 3 項により要求される事実認定を行う場合にのみ認められる。延長の期間は、裁判官がその授権の目的を達成するために必要と思料する期間を超えてはならず、いかなるときも 30 日間以上は認められない。すべての命令及びその延長命令は、傍受権限が、可能な限り迅速に執行されなければならないこと、この章に基づく傍受に服することのない通信の傍受を最小化する方法で行われなければならないこと及び授権された目的を達成したときに終了し、又はいかなるときも 30 日間で終了しなければならないことの定めを含まなければならない。傍受された通信が暗号又は外国語で、傍受の期間にその言語又は暗号の専門家が合理的に考えて得られない場合には、その傍受後可能な限り速やかに最小化を図ることができる。この章に基づく傍受は、その全体又は一部を、傍受を授権された捜査官若しくは法執行官の監督の下に働く政府の職員又は政府との契約に基づいて作業する者により行うことができる。

(6) この章に従い傍受を授権する命令が発付された場合には、命令は、授権された目的の達成に向けた進捗状況及び傍受の継続の必要性を示す報告書を命令を発付した裁判官に対して提出するよう求めることができる。報告書は、裁判官が要求する周期で提出されなければならない。

(7) この章の別段の定めに関わらず、次のことを合理的に認定する司法長官、司法次官、司法副次官又は州法に従って行動する州若しくはその行政的下部組織の主たる検察官により特別に指名された捜査官又は法執行官は、傍受が行われ、又は着手された時から 48 時間以内に、傍受を承認する命令のための請求をこの条に従い行うことを条件として、有線通信、口頭の会話又は電子的通信の傍受を行うことができる。

(a) 次のものを含む緊急事態が存在し、傍受を授権する命令が、適切な注意義務をもって取得される前に有線通信、口頭の会話又は電子的通信を傍受する必要があること。

(i) 人の死又は重大な身体的傷害の急迫の危険

(ii) 国家安全保障上の利益を脅かす共同謀議

(iii) 組織犯罪に特有の共同謀議

(b) この章に基づいて傍受を授権する命令を発付する根拠が存在すること。

命令が発せられない場合には、傍受は、求める通信を取得した時点又は命令の請求が却下された時点のいずれか早い時点において終了する。承認の請求が却下された場合又は命令が発付されることなく傍受が終了するその他の場合には、傍受された有線通信、口頭の会話又は電子的通信の内容はこの章に違反して取得されたものとして扱われ、請求において指名された者に対し、この条の d 項の定めに従って目録が提供されなければならない。

(8) ・・・(以下略)

**刑法典 2703 条　顧客の通信又は記録の要求された開示**

(a) 電子的に蓄積された有線通信又は電子的通信の内容

政府機関は、電子的通信サービスのプロバイダに対して、捜査の対象とされている犯罪の管轄権を有する裁判所が連邦刑事訴訟規則に定められた手続を利用して発付する令状又は州の同等の令状のみに従って、電子的通信システムにおいて 180 日以下の期間、電子的に蓄積されている有線通信又は電子的通信の内容の開示を要求することができる。政府機関は、電子的通信サービスのプロバイダに対し、電子的通信システムにおいて 180 日を超えて電子的に蓄積されている有線通信又は電子的通信の内容の開示を、この条の b 項に基づき得られる方法で要求することができる。

(b) 遠隔コンピュータ処理サービスにおける有線通信又は電子的通信の内容

(1) 政府機関は、遠隔コンピュータ処理サービスのプロバイダに対し、この項の(2)により(1)が適用される有線通信又は電子的通信の内容の開示を、次のいずれかの定めに従って要求することができる。

(A) 政府機関が、捜査の対象とされている犯罪の管轄権を有する裁判所が連邦刑事訴訟規則に定められた手続を利用して発付する令状又は州の同等の令状を取得した場合には、受信契約者又は顧客に対する通知を要求されない。

(B) 政府機関が次のことを行う場合には、この編の第 2705 条に従い通知の延期が許される場合を除き、受信契約者又は顧客に対して政府機関が事前の通知を行う。

(i) 連邦法若しくは州法により授権される行政上の罰則付召喚令状又は連邦若しくは州の大陪審若しくは公判の罰則付召喚令状を利用する場合

(ii) この条の d 項に基づく開示のための裁判所命令を取得する場合

(2) (1)の規定は、サービスについて次のように保持され、又は維持される有線通信又は電子的通信に関して適用される。

(A) 遠隔コンピュータ処理サービスの受信契約者又は顧客を代理し、その者から電子的送信により受理すること（又は、その者から電子的送信により受理した通信をコンピュータ処理して作成すること）。

(B) プロバイダが蓄積以外又はコンピュータ処理以外のサービスを提供する目的で通信内容へアクセスする権限を与えられていないときに、受信契約者又は顧客に蓄積サービス又はコンピュータ処理サービスを提供する目的だけのためにすること。

(c) 電子的通信サービス又は遠隔コンピュータ処理サービスに関する記録

(1) 政府機関は、電子的通信サービス又は遠隔コンピュータ処理サービスのプロバイダに対し、そのサービスの受信契約者又は顧客に関する記録その他の情報（ただし、通信の内容は含まない。）の開示を、次のいずれかの場合にのみ要求することができる。

(A) 捜査の対象とされている犯罪の管轄権を有する裁判所が連邦刑事訴訟規則に定められた手続を利用して発付する令状又は州の同等の令状を取得した場合

(B) この条の d 項に基づく開示のための裁判所命令を取得した場合

(C) 開示について受信契約者又は顧客の同意を得ている場合

(D) その受信契約者又は顧客が電話勧誘販売（この用語の意味は、この編の第 2325 条に定めるところに従う。）に従事しているときに、電話勧誘販売詐欺に関わる法執行捜査に関連して、プロバイダの受信契約者又は顧客の氏名、住所及び営業所について、公式の要求書面を提出する場合

(E) (2)の規定に基づく情報を求める場合

(2) 政府機関が、連邦法若しくは州法により授権される行政上の罰則付召喚令状若しくは連邦若しくは州の大陪審若しくは公判の罰則付召喚令状を利用する場合又は(1)の規定に基づき入手できるその他の手段を利用する場合には、電子的通信サービス又は遠隔コンピュータ処理サービスのプロバイダは、政府機関に対し、そのサービスの受信契約者又は顧客について次の情報を開示する。

(A) 氏名

(B) 住所

(C) 近距離及び長距離電話接続記録、又は通話の時間及び期間の記録

(D) （開始日を含む）サービスの期間及び利用されるサービスの種類

(E) 電話番号、機器番号又は暫定的に割り当てられたネットワーク・アドレスを含む受信契約者の他の番号若しくはその識別子

(F) （クレジットカード番号又は銀行口座番号を含む）サービスの支払いのための方法及び財源

(3) この項に基づき記録又は情報を受領する政府機関は、受信契約者又は顧客に対して通知を行うことを要求されない。

(d) 裁判所命令の要件

b 項又は c 項に基づく開示のための裁判所命令は、管轄権を有し、有線通信若しくは電子的

通信の内容又は捜索されている記録その他の情報が現在行われている犯罪捜査に関係し、かつ重要であると信ずる相当の根拠となる特定的かつ明確な事実を政府機関が提示した場合にのみ発付を義務づけられている裁判所が、発付することができる。この条に従って命令を発した裁判所は、要求された情報若しくは記録が性質上非常に大量である場合又は命令に従うことがプロバイダにその他の不当な負担を強いる場合には、サービス・プロバイダにより直ちになされる申立てを受けて、その命令を破棄し、又は修正することができる。

(e) この章に基づき情報を開示するプロバイダに対する訴訟原因の不存在

有線通信サービス若しくは電子的通信サービスのプロバイダ、その職員、被用者、代理人又は他の特定の人が、この章に基づく裁判所命令、令状、罰則付召喚令状又は証明書の文言に従って情報、設備又は支援を提供することは、いかなる裁判所においても訴訟原因として認められない。

(f) 証拠保存の要件

(1) 一般規定

有線通信サービス、電子的通信サービス又は遠隔コンピュータ処理サービスのプロバイダは、政府機関の要求を受けて、裁判所命令の発付又は他の手続の結果が出るまで、その占有する記録及び他の証拠を保存するために必要なすべての手続をとらなければならない。

(2) 保存期間

(1)に定める記録は、90 日間保存され、その期間は政府機関の更新要求によりさらに 90 日間延長される。

### （２）合衆国法典第 44 編（PUBLIC PRINTING AND DOCUMENTS）

○関連する条項の抜粋訳

**合衆国法典第 44 編 3544 条　連邦行政機関の責務[31]**

(a) 一般規定

各行政機関の長は、次に掲げることを行なうものとする。

(1) 次のことに責任を負うこと。

(A) 次に掲げるものへの不正なアクセス、使用、開示、混乱、変更又は破壊からもたらされる危機及び被害の規模に対応する情報セキュリティの保護を整備すること。

[31] 合衆国法典第 44 編 3544 条の日本語訳については、平野美恵子訳「2002 年電子政府法（公法律第 107－347 号）」（平野美恵子「米国の電子政府法」『外国の立法 217』（2003 年 8 月））（http://www.ndl.go.jp/jp/data/publication/legis/217/21701.pdf）、p55～57 より引用した。

（ｉ）行政機関により、又は行政機関のために収集され、又は維持される情報

（ii）行政機関により、又は行政機関の契約者若しくは行政機関を代行する他の組織により使用され、又は運用される情報システム

(B) 次に該当するものを含めて、この節の要件並びに関連の政策、手続、規準及び指針を遵守すること。

（ｉ）第 40 編第 11331 条に基づき公表された情報セキュリティの規準

（ii）法律の定めるところに従い、及び大統領の指示により発表された国家安全保障システムのための情報セキュリティの規準及び指針

(C) 情報セキュリティの管理プロセスが行政機関の戦略計画及び運用計画のプロセスと一体化されていることを保証すること。

(2) 行政機関の上級幹部職員が、自己の統制下にある業務及び資産を支える情報及び情報システムのために、次の措置を含めて情報セキュリティを整備することを保証すること。

(A) 当該情報又は当該情報システムに関する不正なアクセス、使用、開示、混乱、変更又は破壊からもたらされる危機及び被害の規模を評価すること。

(B) 情報セキュリティの分類及び関連の要件を定める第 40 編第 11331 条に基づき公表された規準に従い、当該の情報及び情報システムを保護するために適切な情報セキュリティ・レベルを決定すること。

(C) 許容しうるレベルまで危機を費用対効果的に縮減させる政策及び手続を実施すること。

(D) 情報セキュリティの制御及び技術が効果的に実施されることを保証するために定期的に検査及び評価を実施すること。

(3) 第 3506 条に基づき設置された行政機関の最高情報責任者（同条の適用対象外とされる行政機関にあっては、これに相当する幹部職員）に次のことを含め、この節に基づき行政機関に課せられた要件の遵守を確保する権限を委譲すること。

(A) 次の条件に該当する行政機関の情報セキュリティ上級担当官 1 名を指名すること。

（ｉ）この条に基づく最高情報責任者の責任を遂行すること。

（ii）この条に基づき定められた職務の遂行に必要な専門的資格を、訓練及び経験を含めて有すること。

（iii）第一の職務として、情報セキュリティの職務を負うこと。

（iv）行政機関によるこの条の遵守の確保を支援することを使命とし、そのための資源を有する部署を代表すること。

(B) (b)項により要求される行政機関全体の情報セキュリティ・プログラムを作成し、これを維持すること。

(C) この編の第 3543 条及び第 40 編第 11331 条に基づき発せられる要件を含め、すべての適用可能な要件に対応する情報セキュリティの政策、手続及び制御技術を開発し、これを維持すること。

(D) 情報セキュリティに関して重大な職責を負う職員に対し、当該の職責に関する訓練を実施し、監督すること。

(E) (2)号に基づく職責に関し、行政機関の上級職員を支援すること。

(4) 行政機関によるこの節の要件並びに関係する政策、手続、規準及び指針の遵守を十分に支援することができる要員を行政機関が訓練することを確保すること。

(5) 行政機関の最高情報責任者が、他の上級幹部職員と調整のうえ、改善措置の進捗を含めてその行政機関の情報セキュリティ・プログラムの有効性に関する年次報告を行政機関の長に対して行うことを確保すること。

(b) ・・・(以下略)

## ３．ドイツにおける不正アクセス関連法令

### ３．１　ドイツにおける不正アクセス関連犯罪の現状

#### （１）電気通信犯罪の認知件数

インターネット犯罪関連の認知件数は、連邦刑事庁（BKA）が毎年公表する警察犯罪統計に示されている。犯罪統計から、特に電気通信犯罪を取り上げたものは、「電気通信犯罪：全国情勢 2009」[32]として公表されている。この統計に含まれる犯罪はドイツ全国で告発された電気通信犯罪であって、連邦刑事庁に対して報告されたものに限定されている。2009 年に発生した電気通信犯罪の件数はドイツ全国で 50,254 件（前年比 12,354 件、33%の増加）とされている。電気通信犯罪の中ではコンピュータ詐欺が全体の約半数（22,963 件、46%。前年比では 35%の増加）を占めている（表 4 参照）。

表 4　ドイツにおける電気通信犯罪の認知件数

| 犯罪の種類 | 2008 年 | 2009 年 | 件数の変化 | 件数の変化 (%) |
|---|---|---|---|---|
| コンピュータ詐欺 | 17,006 | 22,963 | 5,957 | 35.0 |
| 通信サービスへのアクセスに係る詐欺行為 | 5,224 | 7,205 | 1,961 | 37.4 |
| データ偽造、データ処理に係る法律上の取引行為に係る詐欺 | 5,716 | 6,319 | 603 | 10.6 |
| データ改竄、妨害行為 | 2,207 | 2,276 | 69 | 3.1 |
| データの傍受・探知行為 | 7,727 | 11,491 | 3,767 | 48.7 |
| 狭義の電気通信犯罪合計 | 37,900 | 50,254 | 12,354 | 32.6 |

出典：連邦刑事庁「電気通信犯罪：全国情勢 2009」

2008 年から 2009 年にかけて犯罪件数は増加したが、被害総額は若干の減少を見せている。2009 年にドイツ全国で告発された電気通信犯罪による被害の総額は 3,690 万ユーロであり、前年の 2008 年（3,720 万ユーロ）と比較すると約 1%の減少となっている。

最近の電気通信犯罪の中で重大な変化は「フィッシング」行為及び「ボットネット」の増加である。しかし、これらの行為は表 1 で分類された異なる種類の犯罪行為にまたがって実行されているため、警察犯罪統計の中ではこのような犯罪は明示的には示されていない。

[32] 連邦刑事庁「電気通信犯罪：全国情勢 2009」（http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf）。

またコンピュータ妨害行為やデータ改竄は統計上の死角となっており、このような犯罪行為は告発の対象とならないことが多いとされる。その理由として連邦刑事庁は、①犯罪行為の実行（コンピュータシステムへの侵入）が被害者によって発見されない、②企業が被害者である場合、企業側が信用を失うことをおそれるためとしている。さらに、このような行為の未遂[33]は相当数に上るものと推定されるが、技術的防御措置の普及により物的損害が発生する率が低下し、告発されない事例が増加している。また近年の電気通信犯罪の傾向として刑事庁は、これらの行為の専門職業化の傾向を指摘している。このような高度化の指標として、不正プログラムの高度化やソーシャル・エンジニアリングの手法の適用が指摘されている。

上記のような理由から、ドイツ警察は電気通信犯罪の深刻度の判断に際して統計的指標よりも質的な傾向の変化の把握に努力している。

### （２）識別符号に係る犯罪の認知件数

インターネット上の取引や特定のデータへのアクセスを目的とした、オンライン・バンキングを含むIDの詐取は継続的に増加している。連邦刑事庁はこのような傾向を重大視して2009年にあらためて識別符号の詐取に関する統計を作成した（表 5参照）。

**表 5　ドイツにおけるID詐取に係る犯罪の認知件数**

| ID詐取のために行われた行為 | 2009年の件数 |
|---|---|
| オンライン・バンキングに関係するフィッシング行為 | 2,923 |
| カーディング[34] | 53 |
| アカウント・テイクオーバー[35] | 617 |
| 電話回線のアクセスデータの不正利用[36] | 3,207 |

出典：連邦刑事庁「電気通信犯罪：全国情勢2009」

ID詐取に際しては、通常、被害者はIDデータが不正に使用されるまで、使用するコンピュータが感染したことやIDの一部が盗難にあったことに気がつかないことが多く、また発生した金銭面の損害は金融機関により補償されることから、連邦刑事庁は判明・告発さ

[33] 刑法により、未遂も刑罰の対象となる。
[34] 不正に入手したクレジットカード番号等により商品を購入し、それをオンライン・オークションやオンライン・ショップ等で転売する行為。
[35] パスワード等識別符号の詐取行為。
[36] 電気通信サービス事業者の提供するサービスへのアクセスのために必要なアクセスデータの不正使用（例：電話回線へのアクセスデータの傍受と不正使用）。

れていない ID 詐取行為の数を上記の集計数の数倍程度はあるものと見ている。

①フィッシング

連邦刑事庁が 2009 年中に発生したことを把握したフィッシング行為の件数は 2,923 件となっている。前年（1,778 件）との比較では発生件数は 64%増加している（表 6 参照）。

**表 6　ドイツにおけるフィッシング行為の認知件数**

| | 2006 年 | 2007 年 | 2008 年 | 2009 年 |
|---|---|---|---|---|
| 発生件数 | 3,150 | 4,164 | 1,778 | 2,923 |
| 被害総額（万ユーロ） | 1,000 | 1,700 | 700 | 1,200 |

出典：BITKOM

2008 年に前年比で大幅な減少がみられるのは、この年、オンライン・バンキングに iTAN[37] が導入されたことによっている。しかしながら、その効果は長続きせず 2009 年にはドイツ市場を対象とした少なくとも 3 系統の有害ソフトが確認されている。これらの新型有害ソフトは「中間者攻撃」又は「Man-in-the-Browser[38]」攻撃と呼ばれる攻撃手段を用いている。2009 年にもフィッシングはドイツでの電気通信犯罪の中での最大の脅威ととらえられておりオンライン・バンキングを対象としたフィッシングによる 2009 年の損害額は平均で 1 件当たり 4,000 ユーロとされる。

フィッシング・プログラムの技術も進化を見せ、2009 年の段階で電子メールを媒体とするフィッシング・ソフトの割合は約 1/3 程度に低下したのに対し、「Drive-by-Infection[39]」（又は「Drive-by-Downloads[40]」）方式を採用するフィッシング・ソフトの割合は全体の 2/3 に達し、特定のウェブサイトを閲覧することでこのような有害プログラムに感染する確率は急速に高まっている。また、攻撃の対象となるウェブサイトとしては訪問者数が多いウェブサイトへの集中が進んでいる。

業界団体 BITKOM の推計によると 2010 年のフィッシング件数は 5,000 件、被害総額は 1,700 万ユーロに達するものと見られる。

②カーディング

---

37 ワンタイムパスワードの一種。

38 利用者のコンピュータに潜み込んだトロイの木馬が、利用者のオンライン取引をリアルタイムに検出し、取引を傍受して不正を実行するもの。RSA セキュリティ株式会社資料（http://www.rsa.com/japan/products/consumer_solutions/fraudaction/RDAATS_DS_0910.pdf）を参照した。

39 Web サイトを訪問しただけで利用者のコンピュータにマルウェアを感染させること。

40 利用者が意図しない場面で自動的にマルウェアをダウンロードさせること。

カーディングは通常、「Carding-on-Demand[41]」方式で実行されることが多い。カーディングに関する統計は存在していないが、連邦刑事庁は職業化した犯罪集団によるカーディングの増加を重要視している。

③ボットネット

ボットネットは様々な犯罪行為の実施手段として利用されている。連邦刑事庁の推計によれば、ドイツ国内で利用されている「ゾンビ PC」の数は 1 日平均で 35 万台、多いときには 70 万台に達するという。

### （３）電気通信犯罪の検挙件数

電気通信犯罪の検挙件数は、一部の州が公表している。以下ではドイツ最大の州であり、全国の人口の約 1/5 に相当する人口を抱えるノルトライン・ベストファーレン州の例を挙げる[42]（表 7、表 8 参照）。

**表 7　ノルトライン・ベストファーレン州における電気通信犯罪の認知件数**

| 犯罪の種類 | 2008 年 | 2009 年 |
|---|---|---|
| コンピュータ詐欺（刑法典 263a 条） | 4,024 | 5,113 |
| 証拠上重要なデータの偽造（刑法典 269 条）、間接虚偽公証（同 271 条） | 1,312 | 1,256 |
| データの改竄（刑法典 303a 条）、コンピュータ妨害（刑法典 303b 条） | 628 | 656 |
| データの探知、傍受及びその準備行為（刑法典 202a、b、c） | 1,876 | 2,695 |
| 不正に入手したデビットカード及び PIN による詐欺 | 4,975 | 5,027 |
| 通信サービスへの不正アクセスによる詐欺 | 585 | 722 |

出典：ノルトライン・ベストファーレン州刑事庁「コンピュータ犯罪：情勢レポート 2009」

**表 8　ノルトライン・ベストファーレン州における検挙件数及び検挙率（括弧内%）**

| 犯罪の種類 | 2008 年 | 2009 年 |
|---|---|---|
| コンピュータ詐欺（刑法典 263a 条） | 1,293（32.1） | 1,610（31.5） |
| 証拠上重要なデータの偽造（刑法典 269 条）、間接虚偽公証（同 271 条） | 586（44.7） | 630（50.2） |
| データの改竄（刑法 303a 条）、コンピュータ妨害（刑法典 303b | 148（23.6） | 211（32.2） |

41 犯罪者である「顧客」がカーディングに特化した犯罪者（「カーダー」）に対して特定の商品を注文する方式。

42 ノルトライン・ベストファーレン州刑事庁「コンピュータ犯罪：情勢レポート 2009」（http://www.mik.nrw.de/sch/doks/vs/Lagebild_Computer.pdf）。

| | | |
|---|---|---|
| 条) | | |
| データの探知、傍受及びその準備行為（刑法典 202a、b、c) | 483 (23.4) | 517 (19.2) |
| 不正に入手したデビットカード及び PIN による詐欺 | 1,780 (35.8) | 1,754 (34.9) |
| 通信サービスへの不正アクセスによる詐欺 | 273 (46.7) | 199 (27.6) |

出典：ノルトライン・ベストファーレン州刑事庁「コンピュータ犯罪：情勢レポート 2009」

## ３．２　不正アクセス行為関連法令の実態

### ３．２．１　不正アクセス関連法令の概要

コンピュータ犯罪に関する新規則制定の一般的背景として、刑法典 1 条及びドイツ基本法 103 条 2 項は既存の処罰規定を新たに生じた事実関係に適用することを禁じている。このため、コンピュータやインターネットの技術的特性を反映した条文の制定が必要となった。

最初のコンピュータ刑法となる刑法典 202a 条、263a 条、303a 条、303b 条は 1986 年に制定されたが、コンピュータ、インターネットの普及に伴う関連犯罪の多様化と急激な増加を受けて徐々に補完されている。

#### （１）第二次経済犯罪対策法

1986 年 8 月 1 日に施行された第二次経済犯罪対策法[43]はコンピュータ犯罪としてそれまでの犯罪構成要件に 4 件の犯罪を追加した。このときに新たに刑法上の犯罪と定義されたのは「コンピュータ詐欺」（コンピュータの不正操作による利得、刑法典 263a 条）、「データの探知」（データの不正取得、刑法典 202a 条）、「データの改竄」（刑法典 303a 条）及び「コンピュータ妨害」(刑法典 303b 条)である。この刑法改正は既存の詐欺罪と文書偽造を新技術に拡大するものである[44]。なおドイツ刑法では既存の法文を新規に発生した対象に拡張して適用することは認められていない。

改正の契機となったのは 1983 年 2 月に発生した信用金庫職員による不正入金事件であった[45]。この事件ではデータの不正改竄の定義が存在しなかったことから、データアクセス権

---

[43] COMPUTERWOCHE 記事、1985 年 7 月 26 日（http://www.computerwoche.de/heftarchiv/1985/30/1170137/）及び 1986 年 8 月 1 日（http://www.computerwoche.de/heftarchiv/1986/31/1165416/）。

[44] コンピュータの普及に伴い、刑法が考えられる犯罪をカバーしていないことはすでに 1970 年代に認識されており、1976 年には専門委員会が司法省に設置されていたが、その後の政権交代（1982 年）のため、刑法改正が遅れていた。

[45] コンピュータの不正操作により共犯者の口座に 130 万マルク（当時の金額で約 1 億円以上）を入金し、共犯者が 5 か所の信用金庫で現金を引き出し、1 年後に自首した事件。

限を持つ信用金庫職員に対しては著作権法及び不正競争防止法の条文が拡大解釈され適用されるという苦しい結末となった。また、1983 年 2 月には、ソフトウェア製作会社の社員が顧客データを改竄することにより、大量の解約を作り出し、同社を破産させ、直後に新会社を設立する事件が発生した。1984 年にはキール市において、特定のデータを抹消することを目的としてある企業の計算機センターが爆破される事件が発生している[46]。さらに、改正刑法施行直前の 1986 年 7 月 22 日には、ハンブルクで ATM の不正操作により現金引き出しを行おうとした人物が、既存の刑法典 263 条の対象とならないために釈放される事件が発生している。

**（２）第 41 次刑法改正法**

連邦議会は2007年8月7日、第41次刑法改正法案を可決した。その背景として、IT分野における技術の発展に伴い、国境を越えた犯罪が増加していることがある。既に欧州評議会は、このような背景のもとで、2001年に加盟各国間でサイバー犯罪条約を締結している。これは、コンピュータ犯罪の刑事訴追のための法制を欧州レベルで調和化させるためのものである。

ドイツ政府はこの刑法改正により、サイバー犯罪条約に規定されている、コンピュータ犯罪に対する最低限の刑罰規定の制定と国際的な刑事訴追及び各国の刑事訴追機関の間における相互協力に関する規則を国内法化した。さらに、欧州評議会が2005年に採択した「情報システムに対する攻撃への対策に関する評議会基本決定」[47]に示されている、情報システムに対する重大な犯罪行為の訴追についても可能とした。

第41次刑法改正法では、上記のサイバー犯罪条約及び欧州評議会決定を国内規定として具体化するため、刑法典202b条及び202c条を新たに制定したほか、同202a条、303a条及び303b条を改訂している。

### ３．２．２　不正アクセス行為（助長行為を含む）に関する法令

**（１）不正アクセス行為**

刑法典 202a 条

不正アクセス行為については、「刑法典 202a 条　データの探知」において、「自己のためではなく、さらに無権限でのアクセスに対して特別な保護がされているデータを無権限で自己若しくは他人のために入手した者は、3 年以下の自由刑[48]又は罰金刑に処する」と規定されている。

---

46 現在であればコンピュータ妨害行為の対象となる。当時は建屋の破壊による物損及び爆発物の不正使用のみを適用した。

47 英語名称は Council Framework Decision 2005/222/JHA of 24 February 2005。

48 自由刑（Freiheitsstrafe）は、日本と異なり懲役、禁固、拘留の区別がない。Wikipedia の「ドイツ法」記事（http://ja.wikipedia.org/wiki/%E3%83%89%E3%82%A4%E3%83%84%E6%B3%95）。

なお、無権限であっても刑事捜査機関によるアクセスは違法性の要件を構成しないため本条項の刑罰の対象とはならない。また、202a 条は親告罪である。

また、2007 年の第 41 次刑法改正法により構成要件が拡大され、不正なアクセスが可能となるデータそれ自体（の価値）とは関係なく、「保護」を突破すること自体が犯罪を構成することになった。

刑法典 202b 条

「刑法典 202b 条　データの傍受」においては、技術的手段を用いて、無権限で、自己のためではないデータを非公開のデータ処理設備、又はデータ処理設備の電磁放射から入手した者は、その犯行に対して他の規則によってより重い刑罰が科されていない場合には 2 年以内の自由刑又は罰金に処すると規定されている。

本条項は、インターネットによる通信の増加を反映して 2007 年の第 41 次刑法改正法により新たに追加された[49]。理論的には無権限での電話盗聴など、古典的な通信の秘密の保護に関する規定をコンピュータ犯罪にも拡大したものである。

**（２）データの財物性（データの不正取得）**

ドイツでは、刑法典 242 条 1 項において窃盗罪について有体物を対象としているため、無体物であるデーター一般については窃取の対象とならない。ただし個人データについては、連邦データ保護法において、個人データを不正に取得する行為を規制している。

連邦データ保護法 43 条、44 条

「連邦データ保護法 43 条　罰金規定」の 2 項において、一般に公開されていない個人に係るデータを無権限で収集又は処理した者は、30 万ユーロ以下の罰金刑に処すると規定されている。また、「44 条　罰則規定」において、「43 条 2 項に挙げられている行為を、対価を得て、又は自己又は他者のために不当利得を得る目的、若しくは他者に損失を与える目的で故意に行った者は 2 年以下の自由刑又は罰金刑に処する」と規定されている。

**（３）不正アクセス行為の予備行為**

刑法典 202c 条

不正アクセス行為の予備行為に対しては、「刑法典 202c 条　データの探知又は傍受の準備」で言及されている。刑法典 202a 条又は 202b 条の犯罪行為を準備するために、「1. データへのアクセスを可能とするパスワード又はその他の安全コード」又は「2. そのような行為を実行する目的を持つコンピュータ・プログラム」を作成したり、入手・販売・譲渡・配布したりした者は、1 年以下の自由刑又は罰金刑に処するとされている。

本条項は、インターネットによる通信の増加を反映して 2007 年の第 41 次刑法改正法に

[49] サイバー犯罪条約の 2 条を国内法化したもの。

より新たに追加された[50]。

刑法典 263a 条

また、「刑法典 263a 条　コンピュータ詐欺」の 3 項でも、違法に財産上の利益を得ることを意図した不正アクセス行為等の準備行為として、コンピュータ・プログラムを作成したり、入手・販売・保管・譲渡したりした者は、3 年以下の自由刑又は罰金刑に処するとしている。

**（４）不正アクセス行為の国外犯**

刑法典 3 条、9 条

ドイツ刑法の適用可能性に関する基本原則では、刑法典 3 条に「国内犯に対する適用：ドイツ刑法は国内において実行された犯行に対して適用する」としている。また刑法典 9 条では、「犯行は、犯人が犯罪を行った、又は不作為犯にあっては行為義務が生じた、若しくは構成要件に属する結果が生じた、又は犯人自身が結果が生じることを想定していた全ての場所において実行されたものとみなす」とされており、この規定によるとドイツ刑法は、遍在主義（Ubiquitätsprinzip）を採用している。このため、例えば、外国に所在する外国人がドイツ法で違法と見なされるインターネットコンテンツを公開し、ドイツ国内から呼び出すことができる場合にはドイツ刑法による処罰の対象となる。

不正アクセスの事例では、外国人がドイツ国内のサーバに対するハッキングに際してこれに損害を与えた場合にはドイツ法による処罰対象となる。また、ドイツ国内で被害を発生させたウィルスの作成者が外国に所在する場合にもドイツ刑法は適用される（I-Love-You ウィルス事件）[51]。また、ドイツのコンテンツ・プロバイダーが国外のサーバに違法コンテンツをアップロードし、ドイツ国内からダウンロードできるようにすることもドイツ刑法による処罰の対象となる[52]。過去の判例においてドイツ連邦裁判所（Bundesgerichtshof）は、国外において実行された犯罪行為によってドイツ国内の法益が侵害された場合には常にドイツ刑法典 9 条の規定を適用できると判断している。

しかし、この原則を常に適用する場合、国外に居住する外国人が、本人の居住地において法的に保証される行為を行った場合にもドイツ刑法にもとづく処罰の対象となる可能性が生じることから、国際的にはドイツ刑法の適用をここまで拡大することに対しては批判がある。

---

50 サイバー犯罪条約 6 条 1 項 a を国内法化したもの。

51 シュルツ弁護士事務所作成のオンライン・コンメンタール（http://www.mediendelikte.de/ATanwendbarkeit.htm）。

52 ただし刑法典 6 条「国際的に保護されている法益に対する国外犯」の規定により、過激なポルノ文書の公開などの違法コンテンツ提供は偏在主義を適用せずともドイツ刑法による処罰の対象となる。

### （５）他人の識別符号の譲渡し

刑法典 202c 条

他人の ID・パスワード等の識別符号を提供する行為に対しては、刑法典 202c 条「データの探知又は傍受の準備」の 1 項において、データの探知（202a 条）又はデータの傍受（202b 条）の犯罪行為の準備行為として、「データへのアクセスを可能とするパスワード又はその他の安全コード」を販売したり、譲渡したり、配布したり、その他の方法でアクセス可能とした者は、1 年以下の自由刑又は罰金刑に処することが定められている。

### （６）他人の識別符号の譲受け

刑法典 202c 条

他人の ID・パスワード等の識別符号を譲り受ける行為に対しては、刑法典 202c 条「データの探知又は傍受の準備」の 1 項において、データの探知（202a 条）又はデータの傍受（202b 条）の犯罪行為の準備行為として、「データへのアクセスを可能とするパスワード又はその他の安全コード」を「自己又は他人のために入手」した者も同様に処罰対象となっている。

### （７）他人の識別符号の譲渡しに関する広告又は誘引行為

上記の刑法典 202c 条では、他人の識別符号の譲渡しに関する広告又は誘引行為は規制されていない。

### （８）他人の識別符号の譲受けに関する広告又は誘引行為

上記の刑法典 202c 条では、他人の識別符号の譲渡しに関する広告又は誘引行為は規制されていない。

### （９）アクセス管理者等の防御措置

アクセス管理者等の防御措置については、電気通信法において、アクセス管理者（サイト管理者など）のみならず、アクセス管理製品製造者、インターネット・アクセス・プロバイダー等に対するセキュリティ対策義務等の防御措置に係る規定がされている。

電気通信法 109 条[53]

「電気通信法 109 条　技術的防御措置」では、(1)において「全てのサービス提供者は、1. 電気通信の秘密及び個人に関するデータを保護し、2. 不許可での電気通信システム及びデータ処理システムへのアクセスを防止するために適切な技術的防御措置を講じなければ

[53] 電気通信法 109 条は、2004 年に制定され、その後 2007 年及び 2009 年に、連邦の「情報技術の安全性強化に関する法律（Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14.08.2009）」の一環で改訂されている。

ならない」とされている。また、(2)において「公衆に対して電気通信サービスを提供するために電気通信設備を運用する者は、上記に加えて、その（サービス提供の）ために運用する電気通信システム及び情報処理システムに、電気通信ネットワークに重大な悪影響を及ぼす恐れのある障害や外部からの攻撃や災害の影響に対して適切な技術的措置又はその他の防御措置を講じなくてはならない」とされている。

対策を講じるにあたっては、現状の技術的進歩や自己のネットワーク設備又は共同使用する他のネットワーク運用者のネットワーク設備の収納場所についても配慮することが求められており、連邦ネットワーク庁は、連邦情報技術安全庁（BSI）及び連邦データ保護・情報公開監察官との連絡のもとに電気通信システム及び情報処理システムの運用のための安全性要件カタログを作成することとなっている。

技術的対策及びその他の防御措置は、そのために必要となる技術的・経済的負担が保護の対象となる権利と設備の価値に対して妥当である場合に、適切であるとみなされる。

電気通信法 110 条　監視措置の実施、情報の提供

「電気通信法 110 条　監視措置の実施、情報の提供」の(4)では、電気通信監視措置に用いられる技術設備を製造又は販売する者は、連邦ネットワーク庁に対して、その設備が法令にもとづく技術規定及び技術指針の法的及び技術的基準を満たしていることについての審査を求めることができると規定されている。

### ３．２．３　不正アクセスにつながる可能性のある行為に関する法令

#### （１）ウィルス作成

刑法典 202c 条

「刑法典 202c 条　データの探知又は傍受の準備」の 1 項では、データの探知やデータの傍受といった犯罪行為の準備行為として、データへのアクセスを実行する目的を持つコンピュータ・プログラムを作成したり、入手・販売・譲渡・配布したりした者には、1 年以下の自由刑又は罰金刑に処することが定められている。

刑法典 202c 条は違法行為を目的としたツールの「作成」を処罰することができると定めているが、どのようなソフトウェアがいわゆる「ハッキング・ツール」に分類されるかについては明白な規定を含んでいない。この規定には合法な使用を認める例外が設けられていないため、厳格に適用するならば他者のコンピュータに侵入するために利用（転用）可能なソフトウェアやプログラム全てが対象となる。このような指摘を受けて、連邦議会法務委員会は 2007 年 5 月 27 日に提出された報告書[54]の中で、IT 保安関係者などが違法行為を目的とせずにこのようなツールを取り扱うことは 202c 条適用の対象とはならないとして

[54] 連邦議会文書 16/5449、2007 年 5 月 23 日（http://dipbt.bundestag.de/dip21/btd/16/054/1605449.pdf）。

いる。またツプリース司法相（当時）は 2007 年 7 月にコンピュータ犯罪行為の準備行為だけを処罰することを意図していると述べている[55]。

現実にこの条文を根拠として連邦情報技術安全庁に対する告発が行われた例がある[56]。また同様にマンハイム地方検察庁も、ハッキング・ツールを作成し、本人が運営するサイトにアップロードしたことを「自首」した人物に対する捜査を中止した[57]。

ツールの作成者に係る問題としては、転用可能なプログラムがインターネット上で公開され、犯罪者によって実際に使用された場合の可罰性についても問題が指摘されており、多くのソフトウェア製作会社は販売拠点を国外のサイトに移転している[58]。

違法行為に利用可能なソフトウェアの取り扱いについては、主観的犯罪構成要件の欠如により、ほとんどが検察の判断によって不起訴となっている[59]。裁判所における判断の例としては、2009 年の連邦憲法裁判所の判例[60]が存在するが、この中では作成や配布の意図が違法性判断の基準とされている。

本条項を、善意の IT セキュリティ関係者やソフトウェア制作者に脅威を与えることなく実際に運用するためには、犯罪成立の要件を明白にする必要があるとされ、今後の条文の改正が民間団体等により要望されている[61]。

刑法典 263a 条

また、「刑法典 263a 条　コンピュータ詐欺」の 1 項では、違法に財産上の利益を得ることを意図して、プログラムの不正作成等によってデータ処理プロセスの結果に影響を与え、結果として他人の財産を損なった者は、5 年以下の自由刑又は罰金刑に処することが規定されている。

---

55 abgeordnetenwatch.de ホームページ (http://www.abgeordnetenwatch.de/brigitte_zypries-650-5639--f67757.html#frage67105)。

56 ウィルス作成ではなく、パスワード・クラッキングに使用可能なプログラム「John the Ripper」への直接リンクによる配布の疑い。2007 年 9 月 14 日に告発が行われたが、ボン地方検察庁は 2007 年 10 月 26 日に、犯罪構成要件が満たされていないとしてこの告発に関する捜査を見送った。TECCHANNEL 記事、2007 年 10 月 26 日（http://www.tecchannel.de/sicherheit/news/1737140/das_bsi_und_der_hackerparagraf_202c_keine_strafverfolgung_durch_staatsanwalt/index.html）。

57 2008 年 2 月の出来事。SPITBLOG 記事、2008 年 2 月 17 日（http://www.spitblog.de/2008/02/17/hackertoolparagraph-202c-verfahren-eingestellt/）。

58 The Hacker's Choice ホームページ（http://germany.thc.org/）。

59 heise online2009 年 3 月 10 日記事（http://www.heise.de/newsticker/meldung/Hacker-Paragraf-Verfahren-gegen-iX-Chefredakteur-eingestellt-205502.html）や、heise online2008 年 12 月 19 日記事 http://www.heise.de/security/meldung/Hacker-Paragraf-iX-Chefredakteur-zeigt-sich-selbst-an-191403.html を参照のこと。

60 MultiMedia und Recht 資料、2010 年 6 月 17 日（http://rsw.beck.de/rsw/upload/MMR/MMR_06-10_Beilage-Komplett.pdf）。

61 golem.de 記事、2008 年 7 月 21 日（http://www.golem.de/0807/61198.html）。

さらに刑法典 263a 条の 3 項では、同条の 1 条のような犯罪の準備行為としてコンピュータ・プログラムを作成したり、入手・販売・保管・譲渡したりした者についても、3 年以下の自由刑又は罰金刑に処するとしている。

### （２）識別符号の不正取得（フィッシングサイトの構築等）

刑法典 263a 条

「刑法典 263a 条　コンピュータ詐欺」の 1 項では、違法に財産上の利益を得ることを意図して、プログラムの不正な作成や不正なデータの使用等によってデータ処理プロセスの結果に影響を与え、結果として他人の財産を損なった者は、5 年以下の自由刑又は罰金刑に処することが規定されている。

なお、コンピュータ犯罪に関するオンライン・コンメンタール（法令逐条解説文書）では、フィッシングの一類型として「電子金融取引のプロセスにおいて他者に財産上の損害を与える目的でデータを不正利用」した場合、刑法典 263a 条で罰しうるとしている[62]。

### （３）サイバーテロ行為

刑法典 303a 条

「刑法典 303a 条　データの改竄」において、不正にデータを消去、隠蔽、使用不能とするか、又は改竄した者は、2 年以下の自由刑又は罰金刑に処すると規定されている。

刑法典 303 条が実体を有する物件に対する保護のみを対象としていたことから、物理的実体の無いデータを保護するため、第二次経済犯罪対策法の一部として 1986 年に制定された。また、2007 年の第 41 次刑法改正法により 3 項が追加されている[63]。

刑法典 303b 条

「刑法典 303b 条　コンピュータ妨害」においては、以下の行為によって他者にとって重要な意義を持つデータ処理を妨害した者は、3 年以下の自由刑又は罰金刑に処すると規定されている。

- 不正にデータを消去・隠蔽・使用不能・改竄すること
- 他者に不利益を与える意図をもってデータを入力・中継すること
- データ処理装置又は他のデータ保存媒体に破壊・損傷を与えたり、使用不能としたり、撤去・改造すること

また、他者の事業所・他者の企業・官庁にとって重要な意義を持つデータ処理に関する妨害行為は 5 年以下の自由刑又は罰金刑に処すると規定されている。

さらに、特に重大な事案に対しては自由刑を 6 か月以上 10 年以下にすると規定されてい

---

62 シュルツ弁護士事務所作成のオンライン・コンメンタール（http://www.mediendelikte.de/phaenomene.htm）。

63 サイバー犯罪条約の 6 条 1 項 a を国内法化したもの。

る。特に重大な事案と見なされるのは以下のような場合である。

- 犯行者が多額の財産損害を引き起こした場合
- 犯行者が職業的に、又はコンピュータ妨害の継続的な実行に関与した犯罪組織の一員として犯罪を実行した場合
- 犯行者が犯罪行為によって公衆に対する、生活基盤となる財又は役務の供給又はドイツ連邦共和国の安全を阻害した場合

303b 条も、1986 年に第二次経済犯罪対策法の一部として制定された。 これまでのところ、本条項の適用は統計上重要性を持つに至っていないが、トロイの木馬プログラムやボットネット等による犯罪が増加していることから、今後重要性の増大が予想されている。2007 年の第 41 次刑法改正法により改訂された[64]。

### ３．２．４　不正アクセスに関係する行為の捜査に関する法令

#### （１）不正アクセスに関係する行為の捜査における通信傍受

刑事訴訟令 100a 条

捜査に関する規定では、刑事訴訟令 100a 条[65]の 1 項において、下記の場合において「対象者に知らせることなしに電気通信の監視及び記録を行うことができる」としている。

> 1. ある人物が加害者又は共犯者として 2 項に記載されている重度の犯罪行為を行った場合、又は未遂が罰せられる行為の場合には、実行を試み、若しくは犯罪行為によって準備したことの疑義を根拠づける特定の事実が存在する場合
> 2. 個々の場合においてその行為が重大である場合
> 3. 事実関係の解明又は被疑者の所在捜査が他の方法によっては相当に困難であるか、不可能である場合

電気通信の監視及び記録を行うことができる対象には、重度の犯罪行為として「263a 条 2 項との関連において刑法典 263 条 3 項 2 文に挙げられている前提を満たし、かつ、263 条 5 項に該当するコンピュータ詐欺（刑法典 263a 条）」も含まれている。

電気通信の監視及び記録を行うには、検察官からの請求を受けて、裁判所が命じることが必要であるが、危急の場合には検察官の命令によって監視・記録を行うこともできるとしている。期限は、最高で 3 ヶ月とされており、延長は 3 ヶ月を超えない範囲でのみ認められる。

この刑事訴訟令 100a 条に規定する措置については、各州及び検事総長は報告対象年の翌

---

64 サイバー犯罪条約の 3 条及び 5 条を国内法化したもの。

65 刑事訴訟令 100a 条は、ロンドン及びマドリッドにおける大規模テロを受け、2009 年に、「国家に対する重大な物理的脅威の準備を訴追するための法律（Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten vom 30.07.2009）」により関連規定を整理、許可したものである。

年 6 月 30 日までに連邦法務庁に対して暦年ごとに報告しなければならず、連邦法務庁は当該の暦年に連邦全国で命令された措置の一覧を作成しこれをインターネット上で公表しなければならない。報告書には、下記の内容が含まれることとなっている。

1. 100a 条 1 項に規定する措置が命令された手続の件数
2. 100a 条 1 項に規定する監視命令の以下の分類に基づく件数
   a) 最初の命令及び延長命令
   b) 固定電話、携帯電話及びインターネット通信
3. 100a 条 2 項の分類に準拠する、（命令の）根拠となった犯罪行為

刑事訴訟令 100b 条

刑事訴訟令 100b 条[66]の 3 項では、裁判所の命令（危急の場合には検察官の命令によることもできる）があった場合、電気通信サービスを提供する者、又はこれに関与する全ての者は裁判所、検察官及びその警察業務に従事する捜査員（裁判所構成法 152 条）に対して刑事訴訟令 100a 条に規定する措置の実施を可能とする情報を直ちに提供しなければならない。このための準備の要否や、どの程度の準備が必要であるかは電気通信法及び電気通信監視令によって規定されている。

### （２）不正アクセスに関係する行為の捜査における差押場所が明確でない場合の措置

電気通信法 113 条

「電気通信法 113 条　マニュアル（個別）の情報取得手続き」において、事業目的で電気通信サービスを提供する者、又は電気通信サービスに関与する者は、法令の規定による要請があった場合、端末又はその内部若しくはネットワーク上に設置されているデータ保存装置へのアクセスに対する防護を行うためのデータ（パスワード等）の情報を提供しなければならないと規定されている。

ただし、通信の秘密に係るデータへのアクセスは、通信の秘密に関連する法規則の前提のもとでのみ許容される。また、上記の情報提供義務者（電気通信サービス事業者等）は、その顧客及び第三者に対して情報提供の事実を知らせてはならない。

さらに、情報提供義務者は、その責任領域内において情報提供に必要な措置を自らの費用負担で実施しなければならないと規定されている。

### （３）ログの保存

電気通信法 113a 条

---

66 刑事訴訟令 100b 条は、「電気通信監視及びその他の秘匿捜査措置の新規則に関する法律（Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen）」、及び EU データ保持指令（2006/24/EC）の国内法化の一環として改訂されたものである。

「電気通信法 113a 条　データ保存義務」において、データの保存期間は 6 ヶ月と規定されている。同条の 2 項から 4 項では、電気通信サービス提供者（プロバイダー）の種別ごとに保存しなければならないデータについて規定している。

電子メールサービスのプロバイダは、下記のデータを保存しなければならない。

1. メッセージの送信に際しては、電子メールボックスの識別符号及び送信者の IP アドレス、並びに全てのメッセージ受信者の電子メールボックスの識別符号
2. メッセージの、ある電子メールボックスへの着信に際しては、メッセージの送信者及び受信者の電子メールボックスの識別符号及び送信側の電気通信設備の IP アドレス
3. 電子メールボックスへのアクセスに際しては、メールボックスの識別符号及び呼び出し者の IP アドレス
4. 第 1 号から 3 号に挙げられているサービス利用の日付及び時刻並びにそのベースとなる時間帯（タイムゾーン）

また、インターネット・アクセス・プロバイダーの保存しなければならないデータは以下の通りである。

1. インターネット利用のため利用者に割り当てられた IP アドレス、
2. インターネット利用に用いられる回線の一義的な識別符号、
3. 割り当てられた IP アドレスによるインターネット利用の開始及び終了の日付及び時刻並びにそのベースとなる時間帯（タイムゾーン）

ただし、呼び出されたインターネットサイトに関する通信及びデータの内容は保存する必要がないと規定されている。

## ３．３　不正アクセス関連法令条文集

### （１）刑法典（StGB）

○関連する条項の抜粋訳（仮訳）

**刑法典 3 条 国内犯に対する適用**

ドイツ刑法は国内において実行された犯行に対して適用する。

**刑法典 9 条　犯行の場所**

（1）犯行は、犯人が犯罪を行った、又は不作為犯にあっては行為義務が生じた、若しくは構成要件に属する結果が生じた、又は犯人自身が結果が生じることを想定していた全ての場所において実行されたものとみなす。

（2）共犯は、犯行が実行された場所並びに共犯者が行為をなした全ての場所、又は不作為犯の場合にあっては共犯者に行為義務が生じた全ての場所、又は共犯者自身が行為をなすべきであったと想定する全ての場所においてなされたものとする。共犯者が国外犯に際して国内から行為をなした場合、犯行地において刑罰が適用されない行為であっても共犯行為に対してドイツ刑法が適用される。

**刑法典 40 条　日割罰金額の算定[67]**

（1）罰金刑は日割の形で科す。法律に特に定めがない限り、その最低日数は 5 日、最高で 360 日とする。

（2）日割の額は裁判所が犯行者の個人的並びに経済的事情を考慮したうえで決定する。決定に際しては通常、犯行者が一日に得る純収入の額を基準とする。日額は最低 1 ユーロ、最高で 30 ユーロとする。

（3）犯行者の収入、資産及びその他の日割の算定根拠は推定によることができる。

（4）判決には日額の日数と額が示される。

**刑法典 202a 条　データの探知**

（1）自己のためではなく、さらに無権限での アクセスに対して特別な保護がされているデータを無権限で自己若しくは他人のために入手した者は、3 年以下の自由刑 又は罰金刑に処する。

（2）1 項の「データ」とは、電子的、磁気的、その他、人間が直接には認識できない形式で保存又は中継されるもののみを意味する。

[67] 刑法典では個別の犯罪行為について罰金額を規定しておらず、40 条において罰金額の計算の基準を規定している。

**刑法典 202b 条　データの傍受**

権限なしに技術的手段を用いて自己若しくは他人のために、自己のためではないデータ（202a 条 2 項）を非公開のデータ処理設備から、又はデータ処理設備の電磁放射から入手した者は、その犯行に対して他の規則によってより重い刑罰が科されていない場合には 2 年以内の自由刑又は罰金に処する。

**刑法典 202c 条　データの探知又は傍受の準備**

（1）202a 条又は 202b 条の犯罪行為を以下によって準備した者は 1 年以下の自由刑又は罰金刑に処する。

1. データ（202a 条 2 項）へのアクセスを可能とするパスワード又はその他の安全コード

2. そのような行為を実行する目的を持つコンピュータ・プログラム

を作成、自己又は他人のために入手、販売、若しくは他者に譲渡、配布又はその他の方法によってアクセス可能すること

（2）149 条 2 項及び 3 項は準用する

**刑法典 205 条　告訴**

（1）201 条 1 項及び 2 項、並びに 201a 条以下、202 条、203 条及び 204 条の場合においては犯罪行為の訴追は、告訴があった場合にのみ行われる。 これは、刑事訴追機関がその行為の訴追に対する特別な公共の関心のため職権をもって介入することが適当であると認めた場合を除き 202a 条以下及び 202b についても同様とする。

（2）被害者が死亡した場合、告訴権は 77 条 2 項の規定に基づき近親者に移転する。これは 202a 条及び 202b 条の場合には適用されない。（以下略 ）

**刑法典 242 条　窃盗**

（1）自己若しくは第三者のために違法に私物化することを目的として、他人から他人の所有する動産を奪った者は 5 年以下の自由刑又は罰金刑に処する。

（2）未遂は、罰する。

**刑法典 263 条　詐欺**

（1）自己若しくは他者のために、財産上の利得を不正に得ることを意図して、虚偽の説明、事実をゆがめることや隠蔽によって錯誤を引き起こし又はそれを維持することによって他者の財産に損害を与えた者は 1 年以下の自由刑又は罰金刑に処する。

（2）未遂は罰する。

（3）特に重大な事案については 6 か月以上 10 年以下の自由刑に処する。通常、重大な事案と見なされるのは以下のような場合とする：

犯行者が
1. 職業的に又は犯罪集団の一員として、継続的に証書偽造又は詐欺との関連で犯罪行為を行った場合
2. 大規模の財産損害を引き起こし、又は継続的な犯行によって多数の人間に財産価値の喪失を発生させることを意図して行為を行った場合
3. 他者に経済的困窮を与えた場合
4. 公務員としての権限又は地位を濫用した場合、又は
5. 本人又は他者が保険詐欺の目的で高価な物件に放火を行い、又は放火によりその一部又は全体を破壊させ、又は船舶の沈没又は座礁を引き起こした後に保険事故と見せかけた場合、

（4）243 条 2 項及び 247 条以下、及び 248a 条は準用する。

（5）263 条から 264 条まで、又は 267 条から 269 条の犯罪行為の継続的な実行に関与した犯罪組織の一員として職業的に詐欺行為を行った者は 1 年以上 10 年以下の自由刑に処する。軽度の事案については 6 か月以上 5 年以下の自由刑に処する。

（6）裁判所は行状監督を命ずることができる（68 条 1 項）

（7）犯行者が 263 条から 264 条まで、又は 267 条から 269 条の犯罪行為の継続的な実行に関与した犯罪組織の一員として犯罪を実行した場合には 43a 条以下及び 73d 条を適用する。73d 条は犯行者が職業的に犯罪を実行した場合にも適用する。

**刑法典 263a 条　コンピュータ詐欺**

（1）自己若しくは第三者のために違法に財産上の利益を得ることを意図して、プログラムの不正な作成、不正なデータ又は不完全なデータの使用、データの無権限での使用、又は当該データ処理プロセスの過程への無権限での介入によって、データ処理プロセスの結果に影響を与えることで他人の財産を損なった者は 5 年以下の自由刑又は罰金刑に処する。

（2）263 条 2 項から 7 項は準用する。

（3）1 項の犯罪行為の実行を目的とするコンピュータ・プログラムを作成し、自己若しくは他人のために入手、販売、保管又は他人に譲渡することによりそのような行為を準備した者は 3 年以下の自由刑又は罰金刑に処する。

（4）3 項に規定する場合については 149 条 2 項及び 3 項を準用する。

**刑法典 268 条　技術的記録の偽造**

（1）法的関係における詐欺を目的に以下の行為を実行した者は 5 年以下の自由刑又は罰金刑に処する。

1. 不真正な技術的記録の作成、又は技術的記録の改竄
2. 不真正な、又は改竄された技術的記録の使用

（2）技術的記録とは技術的装置によってその全部又は一部が生成され、記録の対象を一般

人又は事情に通じた者に認識させ、法的に重要な事実を証明することが定められているデータ、測定値、計算値、状態又は事象経過の表現をいう。このことはその規定が、すでに作成の時点で存在していたか、その後定められたかには関わらない。

（3）加害者が記録プロセスへの妨害的な介入により記録の結果に影響を与えた場合、不真正な技術的記録の作成と同等と見なされる。

（4）未遂は、罰する。

（5）267 条 3 項及び 4 項は準用する。

**刑法典 269 条　証拠上重要なデータの偽造**

（1）法的関係における詐欺を目的に証拠上重要なデータを、不真正な、又は改竄された証書が存在するかのように認識させる目的で保存又は改竄し、若しくはそのように保存又は改竄したデータを使用した者は 5 年以下の自由刑又は罰金刑に処する。

（2）未遂は、罰する。

（3）267 条 3 項及び 4 項は準用する。

**刑法典 271 条　間接虚偽公証**

（1）公文書、帳簿、データ又は登録簿に記載された権利又は権利関係について重大な意思表示、弁論又は事実を、それらが全く存在しないか、事実と異なるにもかかわらず、若しくはそれらを行う資格を持たない人物又は他の人物によって行われたにもかかわらず、それらが行われたかのように証明又は保存されるように働きかけた者は、1 年以下の自由刑又は罰金刑に処する。

（2）未遂は、罰する。

**刑法典 274 条　データの隠蔽**

（1）以下の行為を行った者は 5 年以下の自由刑又は罰金刑を課す。

1. 他者に損失を与えることを意図して、本人には全く属さない、若しくは単独には属さない証書又は技術的記録を破棄、損壊、又は隠蔽すること。

2. 他者に損失を与えることを意図して、本人に属さない、若しくは単独で処分を行うことができない証拠上重要なデータ（202a 条 2 項）を消去し、隠蔽し、使用不能とすること、又は改竄すること。

3. 他者に損失を与えることを意図して境界標識又は境界や水位を表示する特定の標識を撤去、破棄、認識不能、若しくはその位置を変更又は不正に設置すること。

（2）　未遂は、罰する。

**刑法典 303a 条　データの改竄**

（1）不正に データ（202a 条 2 項）を消去、隠蔽、使用不能とするか、又は改竄した者は、

2 年以下の自由刑又は罰金刑に処する。
（2）未遂は、罰する。
（3）1 項に規定する犯罪行為の準備については 202c 条を準用する。

**刑法典 303b 条　コンピュータ妨害**

(1) 他者にとって重要な意義を持つデータ処理を以下の行為によって妨害した者は 3 年以下の自由刑又は罰金刑に処する。
1. 303a 条 1 項の行為を実行した場合
2. 他者に不利益を与える意図をもってデータ（202a 条 2 項）を入力、又は中継した場合
3. データ処理装置又は他のデータ保存媒体に破壊又は損傷を与え、若しくは使用不能とし、若しくは撤去又は改造した場合
（2）他者の事業所、他者の企業又は官庁にとって重要な意義を持つデータ処理に関する妨害行為は 5 年以下の自由刑又は罰金刑に処する。
（3）未遂は罰する。
（4）第 2 項に規定する、特に重大な事案に対する刑罰の自由刑は 6 か月以上 10 年以下とする。通常、特に重大な事案と見なされるのは以下のような場合を指す。
犯行者が
1. 多額の財産損害を引き起こした場合
2.職業的に、又はコンピュータ妨害の継続的な実行に関与した犯罪組織の一員として犯罪を実行した場合
3. 犯罪行為によって公衆に対する、生活基盤となる財又は役務の供給又はドイツ連邦共和国の安全を阻害した場合
（5）202c 条 1 項の犯罪行為の準備に対しても同様とする。

**刑法典 303c　告訴**

303 条以下、303a 条 1 項及び 2 項、並びに 303b 条 1 項から 3 項の場合においては犯罪行為の訴追は、刑事訴追機関がその行為の訴追に対する特別な公共の関心のため職権をもって介入することが適当であると認めた場合を除き告訴があった場合にのみ行われる。

### （２）刑事訴訟令（StPO）

○関連する条項の抜粋訳（仮訳）

**刑事訴訟令 94 条**

(1) 証拠資料として捜査のために重要である可能性のある物件は差押え又はその他の方法

によって確保する。
(2) 当該物件がある人物の支配に属し、当該人物が自由意思による提供を拒んだ場合には（対象物件を）押収しなければならない。
(3) （略）

**刑事訴訟令 100a 条**

(1)以下の場合には対象者に知らせることなしに電気通信の監視及び記録を行うことができる：
1. ある人物が加害者又は共犯者として 2 項に記載されている重度の犯罪行為を行った場合、又は未遂が罰せられる行為の場合には、実行を試み、若しくは犯罪行為によって準備したことの疑義を根拠づける特定の事実が存在する場合
2. 個々の場合においてその行為が重大である場合
3. 事実関係の解明又は被疑者の所在捜査が他の方法によっては相当に困難であるか、不可能である場合
(2) 1 項 1 号に定める重度の犯罪行為は以下の行為を指す：
1. 刑法典：
（中略）
n) 263 条 3 項 2 文に挙げられている前提を満たし、かつ、263 条 5 項に該当する詐欺、及び 263a 条 2 項との関連において 263 条 3 項 2 文に挙げられている前提を満たし、かつ、263 条 5 項に該当するコンピュータ詐欺
p) それぞれ 268 条 5 項又は 269 条 3 項との関連においても 267 条 3 項 2 文に挙げられている前提を満たし、かつ 267 条 4 項に該当する、又は 275 条 2 項及び 276 条 2 項に規定する文書偽造行為
（以下略）

**刑事訴訟令 100b 条**

(1) 100a 条に規定する措置は、検察官の請求があった場合にのみ、裁判所が命じることができる。（ただし）危急の場合には検察官の命令によることもできる。検察官による命令が 3 労働日以内に裁判所によって確認されない場合には命令は失効する。命令には最高で 3 カ月以下の期限を設けなければならない。得られた捜査結果を考慮したうえで命令の前提が存続している場合、（命令は）その都度 3 カ月を超えない範囲でのみ延長が認められる。
(2) 命令は文書によって行われる。判断理由には以下の内容が含まれていなければならない：
1. 判明している場合には措置の対象者の氏名
2. 電話番号又は監視対象となる回線又は、特定の事実 からその番号が同時に他の端末にも割り当てられていることが明らかでない場合には端末のその他の識別符号

3. 措置の種類、範囲及び終了時期を含む期間
(3) 命令があった場合、電気通信サービスを提供又はこれに関与する全ての者は裁判所、検察官及びその警察業務に従事する捜査員（裁判所構成法 152 条）に対して 100a 条に規定する措置の実施を可能とし必要な情報を直ちに提供しなければならない。このための準備の要否、若しくはどの程度の準備が必要であるかは電気通信法及び電気通信監視令によって規定される。95 条 2 項は準用する。
(4) 命令の前提が存在しない場合、実施された措置は命令によってただちに終了しなければならない。措置の終了後には命令を行った裁判所に対して、結果を報告する必要がある。
(5) 各州及び検事総長は報告対象年の翌年 6 月 30 日までに連邦法務庁に対して暦年ごとにその管轄領域において命令された 100a 条に規定する措置について報告しなければならない。連邦法務庁は当該の暦年に連邦全国で命令された措置の一覧を作成しこれをインターネット上で公表しなければならない。
(6) 5 項に規定する報告書には以下の内容が記載されていなければならない：
1. 100a 条 1 項に規定する措置が命令された手続の件数
2. 100a 条 1 項に規定する監視命令の以下の分類に基づく件数
a) 最初の命令及び延長命令
b) 固定電話、携帯電話及びインターネット通信
3. 100a 条 2 項の分類に準拠する、（命令の）根拠となった犯罪行為

### （３）連邦データ保護法（Bundesdatenschutzgesetz, BDSG）

○関連する条項の抜粋訳（仮訳）

**連邦データ保護法 43 条　罰金規定**
(1)（略）
(2) 故意又は過失により以下の行為を行った者は秩序違反をなした者とみなす：
1. 無権限で、一般に公開されていない個人に係る**データを収集**又は処理すること
2. 無権限で一般に公開されていない個人に係るデータを自動的呼び出しプロセス用に準備すること
3. 一般に公開されていない個人に係るデータを呼び出し、又は自己若しくは他人のために自動化された処理プロセス又は非自動化データベースから入手すること
4. 不正な申告により、一般に公開されていない個人に係る中継データを詐取すること
5. 第 16 条 4 項 1 文、28 条 5 項 1 文に反して、また 29 条 4 項、39 条 1 項 1 文又は 40 条 1 項との関連において、中継されるデータを他の目的に使用すること
（以下略）

(3) 本条 1 項の犯罪は 5,000 ユーロ以下の罰金刑、2 項の犯罪は 30 万ユーロ以下の罰金刑に処する。(以下略)

**連邦データ保護法 44 条　罰則規定**

(1) 第 43 条 2 項に挙げられている行為を、対価を得て、又は自己又は他者のために不当利得を得る目的、若しくは他者に損失を与える目的で故意に行った者は 2 年以下の自由刑又は罰金刑に処する。

(2) この行為は告訴あった場合にのみ訴追する。告訴することができるのは被害者、管轄の機関、データ保護・情報開示監察官並びに規制機関とする。

### （４）電気通信法（TKG）

○関連する条項の抜粋訳（仮訳）

**電気通信法 109 条　技術的防御措置**

(1) 全てのサービス提供者は

1. 電気通信の秘密及び個人に関するデータを保護し、

2. 不許可での電気通信システム及びデータ処理システムへのアクセスを防止

するために適切な技術的防御措置を講じなければならない。

(2) 公衆に対して電気通信サービスを提供するために電気通信設備を運用する者は上記に加えてその（サービス提供の）ために運用する電気通信システム及び情報処理システムに、電気通信ネットワークに重大な悪影響を及ぼす恐れのある障害や外部からの攻撃や災害の影響に対して適切な技術的措置又はその他の防御措置を講じなくてはならない。

対策を講じるにあたっては、現状の技術的進歩や自己のネットワーク設備又は共同使用する他のネットワーク運用者のネットワーク設備の収納場所についても配慮すること。

連邦ネットワーク庁は連邦情報技術安全庁（BSI）及び連邦データ保護・情報公開監察官との連絡のもとに電気通信システム及び情報処理システムの運用のための安全性要件カタログを作成する。

連邦ネットワーク庁は電気通信設備の製造者及び運用者に対して意見表明の機会を与える。カタログは連邦ネットワーク庁によって公開される。事業所又は技術設備が共同で使用される場合であって、特定の義務が特定の運用者に帰属させることができない場合にはそれぞれの設備運用者が 1 項及び 1 文にもとづく義務を負う。

技術的対策及びその他の防御措置は、そのために必要な技術的・経済的負担が、保護の対象となる権利と設備の価値に対して妥当である場合に適切であるとみなされる。

(3) 公共のために電気通信サービスを提供する目的で電気通信設備を運用する者は安全担

当者を選任し、以下の事項を規定する安全コンセプトを策定すること：
1. 使用される電気通信設備及び公共のために提供する電気通信サービスの種類、
2. 想定される危険
3. 1 項及び 2 項にもとづいて実施又は計画されている技術的対策又はその他の防御措置
運用者は連邦ネットワーク庁に対して電気通信サービスの提供開始後ただちに安全コンセプトを提出すること。安全コンセプトには記載されている技術的対策及びその他の防御措置が実施されている、若しくはただちに実施されることについての説明を添えること。連邦ネットワーク庁が安全コンセプト又はその実施について安全上の瑕疵を発見した場合、同庁は運用者に対して瑕疵をただちに是正するよう要求することができる。
安全コンセプトの根拠となった事実関係に変更が生じた場合、運用者はコンセプトを改訂し、連邦ネットワーク庁に対して変更箇所を明示したうえで再度提出しなければならない。
連邦ネットワーク庁は電気通信設備の重要度を考慮したうえで 1 文にもとづく義務の履行について安全コンセプトの審査を定期的に行う。1 文から 4 文は、もっぱら放送信号の受信又は配信に用いられる電気通信設備の運用者に対しては適用されない。

**電気通信法 110 条　監視措置の実施、情報の提供**

(1) 公共のために電気通信サービスを実施するための電気通信設備を運用する者は
1. 運用開始の時点から自己の費用負担で、法的に定められた電気通信監視措置の実施のための技術設備を維持し、その遅滞の無い実施のための組織上の準備措置を行うこと
1a. 2 か所又はそれ以上の電気通信設備の協力によってのみ監視措置が実施可能である場合、監視対象となる電気通信の捕捉及び中継のために必要な自動制御手段を自己の電気通信設備に準備し、かつそのような制御を可能としなければならない。
2. 連邦ネットワーク庁に対して運営開始後、遅滞することなく
a) 1 号に基づく準備が行われたことを届け出、さらに
b)電気通信の監視についての（法的）決定に対応する（ドイツ）国内における窓口を指定すること。
3. 1 号にもとづく技術設備と組織上の措置が 2 項にもとづく法令の規定及び 3 項にもとづく技術指針に適合することを連邦ネットワーク庁に対して無償で証明すること。このために設備の運用者は運用開始から遅くとも 1 カ月以内に、
a) 連邦ネットワーク庁に、同庁によって実施される審査に際して証明の準備に必要な文書を送付し、
b) 連邦ネットワーク庁と共に証明を行うための審査期日を決定すること;
証明に必要な審査にあたっては連邦ネットワーク庁に協力すること。
4. 根拠づけられた個々の事案に関して連邦ネットワーク庁が特に要請した場合、技術的並びに組織的な対策について無償の審査を受入れ、かつ
5. 第 10 条法の 5 条以下及び 8 条にもとづく措置の実施のための機器の、その（事業所の）

室内における設置と運転を許容し、この措置を管轄する機関の職員及び G 10 委員会の構成員(第 10 条法 1 条 2 項)に対して、その法的な任務の達成のためにこれらの装置へのアクセスを確保すること。
電気通信設備を（自ら）運用することなしに公共のために電気通信サービスを運営する者は設備運用者の選定にあたり、業務提供のために使用される電気通信設備が 2 項に規定されている法令及び 3 項に規定されている技術指針の基準による電気通信の監視の命令を遅滞なく実施できることを確認し、サービス開始後ただちに、提供される電気通信サービスの種類、その利用者に係る監視命令の実行者及び電気通信の監視命令を受ける国内の窓口について連邦ネットワーク庁に報告しなければならない。
1 文 2 号の b 及び 2 文にもとづく報告の内容に変更が生じた場合には連邦ネットワーク庁に対して遅滞なくその事実を報告しなければならない。
第 3 項にもとづく規則が制定されていない場合、義務者は 1 文 1 号及び 1a 号にもとづく技術的設備を連邦ネットワーク庁との協議のもとに構成しなければならない。連邦ネットワーク庁は権限を有する機関 の同意を得て対応する規定を定める。第 1 文から 4 文は 2 項にもとづく法令がその電気通信設備に対して例外を認めている場合には適用されない。電気通信監視の警察による犯罪予防を目的とする刑事訴訟令 100b 条 3 項 1 文、第 10 条法 2 条 1 項 3 文、連邦刑事庁法 20l 条 5 項 1 文及びそれに対応する州法上の規定に別段の定めがある場合にはその定めるところによる。
(2) 連邦政府には連邦参議院の承認を得た法令により以下の権限を付与する：
1. 以下についての規則を定める権限
a) 監視措置実施及び情報提供のための基本的な技術要件及び組織面の基本条件。これには、義務者が実施を委任した補助者による監視措置実施及び情報提供を含む。
b) 3 項に定められている技術指針による規制の枠組み
c) 1 項 1 文 3 号及び 4 号にもとづく証明及び
d) 1 項 1 文 5 号にもとづく受入れ義務の詳細
2. さらに以下について決定する権限
a) 特定の技術要件の順守を一時的に免除するケースとその条件
b) 技術的理由による個々の技術要件の順守についての例外許可に関する連邦ネットワーク庁の権限
c) 基本的な技術面の検討又は（負担の）妥当性の観点から 1 項 1 文 1 号の規定によらず技術的設備の維持及び組織面の対策の免除を認める電気通信設備並びにそれによって提供されるサービス
(3) 連邦ネットワーク庁は監視対象となる電気通信の完全な把握及び情報提供のため、並びに権限を有する機関につながる中継交換機の構成に必要な技術的詳細を、権限を有する機関との協議のうえ、関係団体及び製造者の傘下のもとに技術指針に定める。
このとき、国際的技術規格を考慮すること。技術規格からの逸脱については根拠を挙げる

こと。上記の技術指針は連邦ネットワーク庁によってホームページ上で公開される。連邦ネットワーク庁は技術指針の公開について官報により公示する。
(4) 監視措置の実施に用いられる技術設備を製造又は販売する者は連邦ネットワーク庁に対してその設備が特定の電気通信設備との組み合わせによる型式認定の枠内でその設備が2項の法令にもとづく技術規定及び3項にもとづく技術指針の法的並びに技術的基準を満たしていることについての審査を求めることができる。
連邦ネットワーク庁は、監視措置を確実に実施することができ、権限を有する機関において必要となる設備の改修が軽微である場合には羈束裁量　により技術的要件からの逸脱を暫定的に認めることができる。
連邦ネットワーク庁は製造者若しくは販売者に対して審査結果を文書によって通知しなければならない。
連邦ネットワーク庁は第 1 項 1 文 3 号 4 文にもとづいて義務者が実施する、適用技術規定への技術設備の適合に関する証明に際して上記の審査結果を考慮する。
製造者が提出した基本コンセプトに対して本規則の施行前に連邦経済技術省が与えた承認は第 3 文の通知と見なされる。
(5) 2 項にもとづく法令との関連における第 1 項による義務者は、特定の義務についてより長い期間が規定されていない限り、3 項にもとづく法令及び技術指針の要件を満たすための措置を公示から遅くとも 1 年以内に行わなければならない。
義務者によってすでに提供されている電気通信サービスを行うためにこの指針にもとづいて設計された無瑕疵の技術設備は、指針が変更された場合、その施行から遅くとも 3 年以内に変更された要件を満たさなければならない。
1 項 1 文 3 号にもとづく証明又は 1 項 1 文 4 号にもとづく再審査に際して、義務者によって実施された技術的・組織的措置に瑕疵が発見された場合、義務者は連邦ネットワーク庁の要求に応じて、この瑕疵を適切な期限内に是正しなければならない。
（設備の）運用中、特に監視措置の実施に際して瑕疵が発見された場合、義務者は遅滞なく瑕疵を是正しなければならない。
第 4 項により技術設備の型式認定が行われた場合であって瑕疵の是正に期限が定められた場合、連邦ネットワーク庁はこの期限を第 3 文にもとづく瑕疵是正の要件に考慮しなければならない。
(6) その公共への提供サービスの枠内において電気通信設備の回線接続点を他者に供与する全ての電気通信設備運用者は法的に電気通信監視の権限を有する機関の要請があった場合、当該機関に対して監視措置の枠内で発生する情報の中継のために回線接続点を遅滞なく提供する義務を負う。
上記の回線接続点の技術的構成は 2 項にもとづく法令によって規定することができる。
準備及び使用に対しては特別料金や優先的な、若しくは事前の準備、又は障害の除去に対する追加料金を除き、それぞれ（のサービス）に課せられる一般料金を適用する。

特に契約によって規定される割引に関しては第 3 文の規定の拘束を受けないものとする。
(7) 法的に権限を付与された機関によって運用され、通信の秘密に介入し、又はネットワーク運用に介入する電気通信設備は連邦ネットワーク庁の了解のもとに構築されなければならない。
連邦ネットワーク庁は設備の技術的構成について適切な期限内に意見を表明しなければならない。

**電気通信法 111 条　保安機関の情報請求のためのデータ**

(1) 事業目的で電気通信サービスを提供する者、又はそれに関与することで電話番号又は他の回線識別符号、若しくは他（の事業）者によって付与された電話番号又はその他の回線識別符号に対して電気通信回線を提供する者は、112 条及び 113 条に規定されている情報提供のため、事業の目的には不要である場合にもサービス提供開始前に以下のデータを収集し遅滞なく保存しなければならない：

1. 電話番号及びその他の識別符号、
2. 回線保持者の氏名及び住所、
3. 自然人の場合にはその生年月日、
4. 固定回線の場合には回線の所在住所、
5. 携帯電話回線のほかに携帯電話端末が供与される場合には、その端末の個体識別番号
6. 契約開始日

契約終了日はそれが判明した時点で保存すること。
第 1 文は、データが電話帳（加入者一覧）（第 104 条）に登録されていない場合にも適用される。
第 1 文に定める遅滞のない保存義務は、1 文 1 号及び 2 号のデータについて事業目的で公共のために電子メールサービスを提供し、それに際して 1 文 1 号及び 2 号のデータを収集する者にも準用される。このとき 1 文 1 号のデータは電子メールボックスの識別符号と、また 1 文 2 号の回線保持者は電子メールボックスの保持者と読み替えることとする。
第 1 文又は第 3 文に規定される義務者に変更が明らかとなった場合、義務者はデータを遅滞なく変更しなければならない。これと関連して 1 文に規定される義務者は、特に大きな負担なしにデータの収集が可能である場合、それまで収集されていなかったデータを収集、保存しなければならない。113 条に定める情報提供手続についてはデータ保存の方法は任意とする。
(2) 第 1 項 1 文又は 3 文に規定するサービス提供者が販売代理人を立てる場合、販売代理人は 1 項 1 文及び 3 文のデータをそこに規定されている前提条件のもとで収集し これらと、さらに 95 条にもとづいて収集されたデータを遅滞なくサービス提供者に伝達しなければならない。第 1 項 2 文は準用する。第 1 文は変更に関するデータが通常の業務の枠内で販売代理人の知るところとなった場合にも適用する。

(3) この規定の施行の日にすでに成立している契約関係については第1項1文又は3文に規定されているデータを事後的に収集する必要はない。
(4) データは契約関係終了に続く暦年が経過した時点で消去すること。
(5) データの収集と保存に対する補償は行われない。

**電気通信法 112 条　自動的情報取得手続**

(1) 公共のために電気通信サービスを提供する者は 111 条 1 項 1 文 3 号及び 4 号並びに 2 項にもとづいて収集されたデータを遅滞なく顧客ファイル（データベース）に保存しなければならない。顧客ファイルには電話番号及び、再販売若しくはその他の利用のために他の電気通信サービス事業者に提供される電話番号の割り当て、また、移転された 電話番号については最新のポーティング識別符号が登録される。
顧客ファイルに保存されたデータの変更及び消去には111条1項4文及び4項を準用する。移転された電話番号の場合にあっては電話番号と、それに付随するポーティング識別符号はその電話番号が本来割り当てられていたネットワーク事業者に再び返還された時点に続く年が経過したのちに消去すること。
義務者は以下の条件を確保しなければならない：
1. 連邦ネットワーク庁が顧客ファイルのデータを常に自動的に国内において呼び出せること、
2. 不完全な請求データ又は類似検索機能によってもデータの呼び出しが可能であること、
義務者は技術的・組織的対策によって義務者自身がデータの呼び出しについて知ることのできないようにしなければならない。
連邦ネットワーク庁は以下の目的のためにデータの内容を知る必要がある場合にのみ顧客ファイルのデータを呼び出すことができる。
1. 本法又は不公正競争防止法規則違反行為の訴追
2. 第 2 項に挙げられている機関の情報請求への対応
請求を行う機関は回答として受領したデータの必要性を遅滞なく審査し、不要なデータはただちに消去しなければならない。これは連邦ネットワーク庁による第 6 文 1 号にもとづくデータの呼び出しにも当てはまる。
(2) 以下の機関に対する第 1 項に定める顧客ファイルの情報は、それらの情報が法的任務の遂行に必要であり連邦ネットワーク庁に対する請求が自動手続により提出される場合、第 4 項にもとづき常に提供されなければならない：
1. 裁判所及び刑事訴追機関
2. 危険防止の目的を持つ連邦及び州の警察捜査機関
3. 刑事訴追手続きの目的を有する関税刑事局及び各関税捜査局並びに対外経済法 39 条に定められている措置の実施の目的を有する関税刑事局
4. 連邦及び州の憲法擁護機関、軍事防諜機関、連邦諜報機関

5. 第 108 条に定める緊急通報問い合わせ窓口並びに電話番号 124 124 の問い合わせ窓口
6. 連邦金融サービス監督庁
7. 不法就労対策法 2 条 1 項に挙げられている目的を有し、中央問い合わせ窓口を介する税関の諸機関
(3) 連邦経済技術省には連邦首相府、連邦内務省、連邦司法相、連邦財務省並びに連邦国防省との協議のもとに連邦参議院の承認によって以下を規定する法令を公布する権限を付与する。
1. 以下の技術プロセスに関する基本的な要件
a) 連邦ネットワーク庁に対する請求の伝達
b) 連邦ネットワーク庁による、義務者からのデータの呼び出し（呼び出しに使用されるデータの種類を含む）
c) 連邦ネットワーク庁による呼び出しの結果の、請求機関への伝達
2. 考慮すべき安全上の要件
3. 不完全な問い合わせデータによる呼び出しと類似検索機能による捜索
a) 捜索対象となる人物をできる限り正確に特定するために最低限入力すべきデータの範囲（種類）
b) 問い合わせに使用できる記号
c) 人名、道路名、地名などの異なる書き方並びに、氏名の構成部分の置き換え、脱落、追加によって生じる差異を検索に際して確実に含める言語学的プロセスの利用に対する要件
d) 連邦ネットワーク庁に伝達されるデータセットの許容量
4. 第 1 項 1 文の規定に相違して、妥当性の理由から自動情報提供手続用の顧客ファイルを維持しなくても良い者。この場合には 111 条 1 項 5 文は準用される。
このほか、法令には第 2 項 5 号から 7 号に挙げられている機関による問い合わせの可能性をこれら機関が必要とする範囲ないに制限する規定を含めることができる。
連邦ネットワーク庁は関係諸団体及び権限を有する機関の参加のもとに作成される技術指針として自動情報取得手続きの技術的詳細を定める。技術指針は必要な場合、現行の技術水準に適合させ、連邦ネットワーク庁はこれを同庁が発効する官報に公示する。
第 1 項の義務者と権限を有する機関は、技術指針の公示から 1 年以内にその要件を満たさなければならない。
この指針にもとづいて構成された瑕疵の無い技術設備は、指針が変更された場合、その施行から遅くとも 3 年以内に変更された要件に適合させなければならない。
(4) 連邦ネットワーク庁は、第 2 項に挙げられている機関の請求に対して、該当するデータセットを第 1 項の顧客ファイルから呼び出し、請求機関に伝達しなければならない。
連邦ネットワーク庁は特別な根拠がある場合に限り伝達の許容性について審査を行う。
伝達の許容性に対する責任は第 2 項に挙げられている機関が負う。
連邦ネットワーク庁はそれぞれ管轄の機関によるデータ保護監督のため、全ての呼び出し

について時刻、呼び出しのために使用されたデータ、呼び出されたデータ、呼び出しを行った者が一義的に特定するデータ及び請求機関、その文書整理番号並びに請求を行った者を一義的に特定するデータを記録する。
記録簿のデータを他の用途に使用することは認められない。記録簿のデータは 1 年後に消去しなければならない。
(5) 第 1 項に規定する義務者は本規則に基づく情報提供を行うため、その責任領域内における全ての技術的措置に係る費用を負担する。
このような技術的措置には機密保持の確保及び無権限でのアクセスに対する防護のために必要な装置の購入、適当な電気通信回線の設置及び閉鎖式のユーザシステムへの加入並びに第 3 項に定める法令及び技術指針の基準にもとづく措置の継続的な維持が含まれる。
自動情報取得手続によって提供された情報に対する補償は行われない。

**電気通信法 113 条　マニュアル（個別の）情報取得手続き**

(1) 事業の目的で電気通信サービスを提供する者、若しくはそれに関与する者は個々の（特殊な）場合であって犯罪又は秩序違反行為の訴追、公共安全又は公共の秩序に係る危険防止、連邦及び州の憲法擁護機関、連邦諜報機関、又は群防諜機関の法的任務の遂行に必要である場合、管轄の機関の要請があった場合 95 条以下及び 111 条に基づいて収集したデータについて遅滞なく情報を提供しなければならない。
第 1 項の義務者は、刑事訴訟令 161 条 1 項 1 文、163 条 1 項、連邦又は州の警察法の、公共の安全と秩序に対する危険防止のためのデータ収集規則、連邦憲法擁護庁法 8 条 1 項、これに対応する各州憲法擁護庁法の規定、連邦諜報機関法 2 条 1 項又は群防諜機関法 4 条 1 項の規定による要請があった場合、端末又はその内部若しくはネットワーク上に設置されているデータ保存装置へのアクセスに対する防護を行うためのデータ（特に PIN や PUK）についての情報を提供しなければならない。
上記以外の公共機関又は非公共機関に対してはこれらのデータを提供してはならない。
通信の秘密に係るデータへのアクセスはそれに関連する法規則の前提のもとでのみ許容される。
義務者はその顧客及び第三者に対して情報提供の事実を知らせてはならない。
(2) 第 1 項の義務者はその責任領域内において情報提供に必要な措置を自らの費用負担で実施しなければならない。

**電気通信法 113a 条　データ保存義務**[68]

(1) 末端利用者（一般消費者）向けに、一般に開かれた電気通信サービスを提供する者は、

[68] 113a 条は判決根拠によれば基本法 10 条 1 項に違反し、2010 年 3 月 2 日の連邦憲法裁判所判決（BVerfGE v. 2.3.2010　I 272 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08）により無効である。

2 項から 5 項の基準にもとづき、提供サービスの利用に際して生成又は処理された呼情報（CDR）を国内又は他の欧州連合諸国内で 6 カ月間保存する義務を負うものとする。自ら呼情報（CDR）を生成又は処理することなしに一般に開かれた電気通信サービスを提供する者はデータが第 1 文に適合する形で保存されることを保証しなければならず、連邦ネットワーク庁の要請があった場合にはデータを保存する者を通知しなければならない。

(2) 一般に開かれた電話サービスの提供者（プロバイダー）は以下のデータを保存しなければならない：

1. 発信者回線及び受信者回線の電話番号又は識別符号、並びに転送機能又は中継機能がある場合には全ての接続回線の電話番号又は識別符号

2. 回線接続の開始と終了日時とそのベースとなる時間帯（タイムゾーン）

3. 電話サービスの一環として、複数の異なるサービスを利用することができる場合には、利用されたサービスに関する記載、

4. さらに携帯電話サービスの場合には：

a) 時発信者及び受信者双方の携帯電話利用者の国際識別符号

b) 発信端末と受信端末の国際識別符号

c) die 名称 der durch den 発信者回線及び受信者回線によって回線接続の開始時点で利用された基地局の名称

d) 前払式の匿名のサービスの場合においては最初の有効化（アクティベート）の日付、時刻及び基地局の名称

5. インターネット電話サービスの場合においては発信者回線及び受信者回線の IP アドレス

第 1 文はショートメッセージ、マルチメディア・メッセージ又は類似するメッセージの中継にも適用される。この場合には第 1 文 2 号に定められた事項に代えてメッセージの送信及び受信の時刻を保存しなければならない。

(3) 電子メールサービスのプロバイダは以下のデータを保存する：

1. メッセージの送信に際しては電子メールボックスの識別符号及び送信者の IP アドレス、並びに全てのメッセージ受信者の電子メールボックスの識別符号

2. メッセージの、ある電子メールボックスへの着信に際しては、メッセージの送信者及び受信者の電子メールボックスの識別符号及び送信側の電気通信設備の IP アドレス

3. 電子メールボックスへのアクセスに際しては、メールボックスの識別符号及び呼び出し者の IP アドレス

4. 第 1 号から 3 号に挙げられているサービス利用の日付及び時刻並びにそのベースとなる時間帯（タイムゾーン）

(4) インターネット・アクセス・プロバイダーは以下のデータを保存すること：

1. インターネット利用のため利用者に割り当てられた IP アドレス、

2. インターネット利用に用いられる回線の一義的な識別符号、

3. 割り当てられた IP アドレスによるインターネット利用の開始及び終了の日付及び時刻並びにそのベースとなる時間帯（タイムゾーン）
(5) 電話サービス・プロバイダがこの規則に挙げられている呼情報（CDR）を通話が受信されない場合やネットワーク・マネジメントの介入が不成功出会った場合にも 96 条 2 項に挙げられている目的のために保存又はログ記録する場合には、呼情報（CDR）は この規定の基準に従って保存すること。
(6) 電気通信サービスを提供する者が本規定の基準によって保存の対象となる記録内容を変更する場合には元の記録内容と新規の記録内容のほか書換えの時刻及び日付並びにベースとなる時間帯（タイムゾーン）を保存する義務を負うものとする。
(7) 公共のために携帯電話ネットワークを運用する者は義務を負うものとする。zu den 本規定の基準によって保存しなければならない基地局の名称に加えて各基地局のアンテナ及び主送信方位の地理的位置を示すデータを保持しなければならない。
(8) 呼び出されたインターネットサイトに関する通信及びデータの内容はこの規定によらず保存する必要はない。
(9) 第 1 項から 7 項にもとづくデータの保存は権限を有する機関による情報請求に対して遅滞なく回答できるように行われなければならない。
(10) 本規定に定める義務者は保存された呼情報（CDR）の質と保護に関して die 電気通信分野において必要な事項に留意しなければならない。その際、義務者は技術的・組織的措置をとることによって、特に権限を付与された者だけが保存されたデータにアクセスできることを確実としなければならない。
(11) 本規定に定められた義務者は hat 本規定のみを根拠として保存されたデータを 1 項に挙げられている期限の経過後 1 カ月以内に消去、若しくは消去のために確保しなければならない。

**電気通信法 113b 条　113a 条の規定により保存されたデータの利用**

第 113a 条の義務者は権限を有する機関の要請に対して、113a 条との関連においてそれぞれの法規則に想定され、かつ、個々の（特別の）場合に伝達が命じられた場合、113a 条の保存義務だけを根拠として保存されたデータを以下の目的についてのみ、伝達することができる：
1. 犯罪行為の訴追
2. 公共の安全に対する重大な危険の防止又は
3. 連邦及び州の憲法擁護機関、連邦諜報機関及び軍事防諜機関の法的任務の法的任務の遂行
第 113 条にもとづく情報提供を除き、義務者は他の目的のためにデータを利用することはできない。113 条 1 項 4 文は準用する。

**電気通信法 149 条　罰金規定**

(1) 故意又は過失により以下の行為を行った者は規則違反行為を行ったものとみなす。

4. 以下の執行命令に違反した者

（中略）

b) （中略）第 109 条 3 項 3 文

14. 第 110 条 1 項 2 文又は 3 の規定に反して、報告を行わない、又は不正確、不完全若しくは遅延して報告を行った者

21. 第 109 条 3 項 2 号又は 4 号の規定に反して安全コンセプトを提出しなかった、又は遅延して提出した者

22. 第 110 条 2 項 21 号の a に定める法令との関連において 110 条 1 項 1 文 1 号又は 1a に反して技術設備を設置せず、又は組織的な措置を行わなかった者

23. 第 110 条 1 項 1 文 2 号の b に反してこの条文に定められている窓口を設置しなかった、又はただちに設置しなかった者

24. 第 110 条 1 項 1 文 3 号 に反して必要な証明を行わなかった、又は即時に行わなかった者

25. 第 110 条 1 項 1 文 4 号に反して検査を受け入れなかった者

26. 第 110 条 1 項 1 文 5 号に反して、この規則に定められている機器の設置又は運転を受け入れなかった、又はそのような機器へのアクセスを確保しなかった者

27. 第 110 条 5 項 3 文に反して、瑕疵を是正しなかった、若しくは期限までに是正しなかった者

28. 第 110 条 6 項 1 文に反してネットワーク・アクセスポイントを用意しなかった、規定通りに設置しなかった、又は期限までに用意しなかった者

29. 第 111 条 1 項 1 文に反して、また 2 文又は 3 文との関連において、又は第 111 条 1 項 4 文に反して、これらの条文に規定されているデータを収集しなかった、正しく収集しなかった、又は不完全に収集、若しくは期限までに収集しなかった、保管しなかった、正しく保存しなかった、又は不完全に保存、若しくは期限までに保存しなかった、又は修正しなかった、正しく修正しなかった、又は不完全に修正、若しくは期限までに修正しなかった者

30. 第 111 条 2 項 1 文に反して、また 2 文との関連において、データを収集しなかった、又は期限までに収集しなかった、若しくは伝達しなかった、正しく伝達しなかった、不完全に伝達、若しくは期限までに伝達しなかった者

30a. 第 111 条 4 項に反して、データを消去しなかった、又は期限までに消去しなかった者

31. 第 112 条 1 項 4 文に反して、連邦ネットワーク庁が顧客データベースからデータを呼び出すことができるための措置を講じなかった者

32. 第 112 条 1 項 5 文に反して、データの呼び出しを知ることができないようにするための措置を講じなかった者

33. 第 113 条 1 項 1 文又は 2 文、第 114 条 1 項 1 文又は 127 条 1 項 1 文に反して情報を提供しない、不正確又は不完全な情報を提供、若しくは期限までに情報を提供しなかった者
34. 第 113 条 1 項 2 文後半に反してデータを伝達しなかった者
35. 第 113 条 1 項 4 文に反して、また第 113b 条 2 文との関連において、守秘義務を順守しなかった者
36. 第 113a 条 1 項 1 文又は 6 項に反して、データを保存しなかった、正しく保存しなかった、又は規定されている期間保存しなかった者
37. 第 113a 条 1 項 2 文に反して、この条文に定められているデータを保存するための措置を講じなかった、若しくはデータを保管する者を報告しなかった者
38. 第 113a 条 10 項 2 文に反して 、特に権限を付与された者のみが保存されているデータにアクセスできるような措置を講じなかった者
39. 第 113a 条 11 項に反してデータを消去しなかった者、又は期限までに消去しなかった者又は期限までに消去されるような措置を講じなかった者

## ４．フランスにおける不正アクセス関連法令

### ４．１　フランスにおける不正アクセス関連犯罪の現状

情報通信技術に関連する犯罪について、情報通信技術関連犯罪対策中央局（OCLCTIC.）[69]は次のように指摘している[70]。

情報通信技術に関連する犯罪の厳密な分析が困難にぶつかっていることに留意しなくてはならないとし、とりわけ警察等に認知されていない犯罪の件数は重要であり、この数字は実施されている安全対策の影響を受けるとしている。

こういった背景の下、情報通信技術に関連する犯罪におけるいくつかの傾向を確認することができる。第一に、技術に対する挑戦ではなく、利得に対する欲望が犯罪の主な動機の一因となっており、あらゆるデジタル環境の特性を完全に使いこなし、バーチャル空間が組織犯罪の新たな現場となっていることが挙げられる。第二に、詐欺（虚偽の銀行預金口座番号の使用、あるいは法外な付加価値をつけた虚偽の物品販売）といった古典的な犯罪に対して、情報通信技術を使用する行為は、当初は「情報処理技術者」のみであったが、ますます一般的になってきていることが挙げられる。第三に、児童ポルノ画像の配信、人種差別を謳うウェブサイト、著作権を侵害する音楽のダウンロード等のコンテンツ犯罪と言われる犯罪行為が非常に増加している、といったことが挙げられる。

少々古い数字になるが、「フランスにて確認された犯罪及び非行統計資料 2004 年」では、情報通信技術に関連する犯罪は全体で 45%以上の減少が確認されおり、2003 年に比べ 525 件の犯罪が減少している。しかし、この減少はデビットカード（yescards）の偽造を可能にするための情報処理プログラムの配信に関連する犯罪のみであり、2003 年の 792 件に対し、2004 年には 64 件まで減少していることが原因である。これは、「日常生活の安全に関する 2001 年 11 月 15 日の法律」によりデビットガードの偽造に対する罪刑が決定されたため、銀行機関の安全対策が実施され、犯罪防止が行われたことが主原因である。

しかしながら、これ以外の情報通信技術に関連する犯罪行為は、全て増加している。新技術特有の犯罪（データ自動処理システムへの侵害、情報処理・データと自由に関する法律[71] に関係する犯罪、暗号理論に関係する犯罪）は、2003 年には 254 件、2004 年には 285 件が確認されている。ソフトウェア偽造件数は、2003 年の 139 件から 2004 年には 268 件に増加している。ファイル又は情報処理に起因する個人の権利を侵害する犯罪件数も 2003

---

69 OCLCTIC は、L'Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication の頭文字をとった略称となる。警察及び憲兵隊を統合して組織された省庁間連絡機関で、フランス国内での活動のほか、国際的な協力も行っている。

70 「フランスにて確認された犯罪及び非行統計資料 2004 年（Aspects de la criminalite et de la delinquance constatees en France en 2004）」を参照。

71 フランス語名称は Loi Informatique et Libertés。

年の 37 件から 2004 年には 54 件に増加している。

情報通信技術を使用した犯罪、若しくは、情報通信技術が犯罪を助けたり、あるいは情報通信技術の使用そのものに関連する犯罪件数だけは、2004 年には前年比で 3452 件、26 %減少している。その多くは前述したデビットカード番号の不法使用による詐欺行為が占めている。

しかしながら、財物又はサービスの購入のために実行される詐欺は、2003 年の 5103 件から 2004 年には 6287 件に増加している。そして携帯電話のチャージのための携帯電話を狙った詐欺も 2003 年の 1667 件から 2004 年には 1841 件に増加している。

インターネット使用が遂行を助けた重罪及び軽罪の件数はあまり変化がなく、2004 年に 431 件であったのに対し、2003 年は 428 件と横ばいとなっている。

一方、その他全ての各種犯罪件数は増加しており、とりわけ、人種憎悪及び人道に対する犯罪擁護（2003 年の 156 件から 2004 年には 333 件）、未成年が登場するポルノ画像の配信（2003 年の 464 件から 2004 年には 576 件）といった出版の自由法に対する違反が増加している現状がある。

## ４．２　不正アクセス行為関連法令の実態

### ４．２．１　不正アクセス関連法令の概要

フランスでは、2008 年 10 月に国家的なデジタル経済発展計画である「デジタル・フランス 2012（France Numérique 2012）[72]」が発表されている。フランスにおけるデジタル経済の発展のために 2012 年までに行うべき 154 のアクションが示され、超高速の情報基盤整備への約 300 億ユーロ（約 3.5 兆円）の大規模投資、全国民のブロードバンドネットワークへの接続可能化、デジタルコンテンツ制作強化等の行動計画がまとめられている。この中には、サイバー犯罪に関する行動計画も含まれ、「3.3 章　サイバー犯罪対策強化」のアクション 87 として「国内安全措置指針・計画法（LOPPSI[73]）を契機に以下を導入する。」とされ、「電子通信ネットワーク上での身元詐称罪」、「プロバイダとの同意に基づき、児童ポルノサイトのブロッキングを可能とする規定」、「処罰される、犯意のないハッカーに対する公益奉仕労働の代替刑制度」の 3 つの制度導入が言及された。

国民議会への報告書 N° 2271[74]によれば、フランスの捜査部局はすでにサイバー犯罪の取り締まり強化の手段を備えているが、国内安全措置指針・計画法（LOPPSI）は、これら

---

72 「デジタル・フランス 2012」の原文は http://www.ladocumentationfrancaise.fr/rapports-publics/084000664/index.shtml を参照のこと。

73 LOPPSI は、La loi d'Orientation Pour la Performance de la Sécurité Intérieure の頭文字をとった略称となる。

74 国民議会への報告書 N° 2271 の原文は、http://www.assemblee-nationale.fr/13/rapports/r2271.asp を参照のこと。

手段のさらなる強化を目指すものであると記述されている。国内安全措置指針・計画法（LOPPSI）の第 2 条では、「電子通信ネットワーク上での身元詐称及びハラスメントの取り締まり」を目的としており、他人の ID や個人情報の不正利用に関する条文となっている。

### ４．２．２　不正アクセス行為（助長行為を含む）に関する法令

#### （１）不正アクセス行為

刑法第 323-1 条

フランスにおける不正アクセス行為は、刑法典の第 3 章「データの自動処理システムに対する侵害」の刑法第 323-1 条に規定されている。刑法第 323-1 条では、データの自動処理システムへの「不正アクセス」又は「不正滞留」する行為に対し、2 年の拘禁刑及び 3 万ユーロの罰金で罰することが示されている。ここでの「不正アクセス」は、アクセス権限のない者が、故意にコンピュータの一部又は全部にアクセスする行為であり、パスワードを不正入手し、コンピュータにアクセスするケースが想定される。偶然や過失によって他人のコンピュータにアクセスしてしまったにも関わらず、そのアクセスを切断せずにアクセス状態を維持した場合や、アクセス権限がある者が権限の範囲を超えてアクセスする場合には、「不正滞留」となる[75]。

#### （２）データの財物性（データの不正取得）

刑法第 226-18 条

刑法第 226-18 条では、個人情報を不法、不当、不正な手段で収集する行為を禁じており、このような行為に対しては、5 年の拘禁刑及び 30 万ユーロの罰金が課せられることとなっている。

#### （３）不正アクセス行為の予備行為

刑法第 323-3-1 条

不正アクセス行為の予備行為に関しては、刑法第 323-3-1 条に規定されている。不正アクセスを禁止した刑法第 323-1 条、システムの動作妨害を禁止した刑法第 323-2 条、データを不正に消去・改変する行為を禁止した刑法第 323-3 条によって規定される犯罪を実行する目的のために作成、あるいは特別にカスタマイズされた装置、機械、情報処理プログラム、データを導入する、所持する、提供する、譲る、若しくは自由に利用できる状態にする行為は、当該犯罪の所定刑、又は最も重く罰せられる犯罪の所定刑によって処罰するとされている。

刑法第 323-3-1 条は、2004 年の「デジタル経済法（Loi n°2004-575 du 21 juin 2004 pour

[75] 独立行政法人情報処理推進機構 IPA「コンピュータ・ウイルス等有害プログラムの法的規制に関する国際動向調査」（2000 年 3 月）を参照のこと。

la confiance dans l'économie numérique）[76]」によって、新たに追加された。

**（４）不正アクセス行為の国外犯**

刑法第 113-6 条、113-7 条

刑法第 113-6 条によると、フランスの刑法は、フランス共和国の国外においてフランス国籍を持つ者が実行した重罪に対して適用されると規定している。また、フランス共和国の国外においてフランス国籍を持つ者が実行した軽罪が、犯罪が実行された国の法律の下で処罰されうる場合は、当該軽罪にも適用されることになる。この条項は、犯行者が起訴された犯罪行為の後にフランス国籍を取得した場合にも適用される。

また、刑法第 113-7 条では、犯罪の被害者がフランス国籍を持つ者である場合、フランス共和国の国外において発生したフランス国籍の者又は外国国籍の者が犯した犯罪は、重罪又は拘禁刑で罰する軽罪については、フランス刑法が適用されると規定されている。

**（５）他人の識別符号の譲渡し**

刑法第 323-1 条から刑法第 323-7 条には、他人の識別符号の譲渡しを規定する内容は含まれていない。

**（６）他人の識別符号の譲受け**

刑法第 323-1 条から刑法第 323-7 条には、他人の識別符号の譲受けを規定する内容は含まれていない。

**（７）他人の識別符号の譲渡しに関する広告又は誘引行為**

刑法第 323-1 条から刑法第 323-7 条には、他人の識別符号の譲渡しに関する広告又は誘引行為を規定する内容は含まれていない。

**（８）他人の識別符号の譲受けに関する広告又は誘引行為**

刑法第 323-1 条から刑法第 323-7 条には、他人の識別符号の譲受けに関する広告又は誘引行為を規定する内容は含まれていない。

**（９）アクセス管理者等の防御措置**

アクセス管理者等の防御措置については、1978 年に制定・施行された「情報処理・データと自由に関する法律（Loi n 。78 - 17 du 6 janvier 1978 relative à l'informatique, aux

[76] EU 電子商取引指令（2000/31/EC）や EU 電子通信プライバシー指令（2002/58/EC）、サイバー犯罪条約（2001 年）を国内法化するものである。国民議会への報告書 N° 612（http://www.assemblee-nationale.fr/12/rapports/r0612.asp）を参照のこと。

fichiers et aux libertés」[77]が大きく関わっており、公正かつ適法な収集・処理、収集目的の特定、情報の正確性・完全性、センシティブ情報の収集制限、処理に際しての本人の同意、安全保護管理義務、本人アクセス権等の個人情報の取扱いに関する規定となっている。「情報処理・データと自由に関する法律」は、1995 年の EU データ保護指令への対応等を目的とし、2004 年 8 月 6 日の法律第 2004-801 号で大きく改正されている。

本法では、第 2 条において、個人情報について「自然人に関するあらゆる情報のうち、識別番号( numérod'identification ) 又は個人に固有の一若しくは複数の要素を参照することで、直接又は間接に個人を識別し又は識別可能なもの」と定義したうえで、公的機関か民間機関かに関わらず個人情報処理責任者( responsable d'un traitement de données à caractère personnel )の安全保護管理義務を定めている（第 34 条、第 35 条)。個人情報処理責任者がフランス領内に在住しているか、あるいは、フランス領内に設置された処理手段を用いている場合に適用範囲となる[78]。

情報処理・データと自由に関する法律　第 34 条、第 35 条

第 34 条には、個人情報処理責任者がデータ安全保護のために予防措置を講じる必要があることが言及されている。また第 35 条では、下請業者においても、安全措置を行うことが求められている。

刑法典 226-17 条

刑法典 226-17 条では、情報処理・データと自由に関する法律の第 34 条に定める安全保護のための有効な予防措置を講じずに、個人情報の処理を実施又は実施させる行為に対して、5 年の拘禁及び 30 万ユーロの罰金が課せられることになっている。

### （１０）その他の ID 詐称・ID 窃盗関連法令

刑法典第 222-16-1 条

第三者の氏名を詐称することについては、刑法第 434-23 条に該当する部分がある。刑法第 434-23 条では、第三者が刑事訴追を受けた、又は受けさせうる状況で、その第三者の氏名を使用する行為は 5 年の拘禁刑及び 7 万 5 千ユーロの罰金で罰すると規定している。この量刑は、刑事訴追されている犯罪に対する量刑に追加されることになる。

しかしながら、身元詐称が被害者に対していかなる法的又は経済的被害を与えなかった場合、身元詐称の罪質を構成しないという判決が示されたこともあり、インターネット上

---

77 「情報処理・データと自由に関する法律」の原文は http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf を参照のこと。

78 内閣府「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（2008 年 3 月）（http://www.caa.go.jp/seikatsu/kojin/h21report2.pdf)。

特有の身元詐称を罰するために刑法典に新規の条を追加することが必要となった[79]。

ネットワーク上での身分詐称に関しては、2009 年 5 月 27 日に提出された LOPPSI 法案の第 2 条にて、電子通信ネットワーク上における第三者の身元又は個人情報の不正使用が犯罪として規定されている。この法案は、2010 年 2 月 16 日に下院で可決されている。

刑法典第 222-16 条は、悪意の電話発信に対しての規定であったが、LOPPSI 法案の第 2 条により、第 222-16 条「他者の平穏を乱すことを目的にした繰り返し行われる悪意の電話発信及び音による攻撃を罰する」のあとに、新しく刑法典第 222-16-1 条を追加された。そこでは、「電子通信ネットワーク上で第三者の身元又は第三者の個人情報を繰り返し使用し、その第三者あるいは他人の平穏を乱す行為は、1 年の拘禁刑及び 1 万 5 千ユーロの罰金で罰する。電子通信ネットワーク上で第三者の身元又は第三者の個人情報を使用し、名誉毀損あるいは敬意を欠く行為は、同様の刑罰を科す。」とされ、法の不備を補う。

上記の罰則は、自然人に対するものであるため、法人がこの法律に規定され犯罪で有罪になった場合には、5 倍の金額である 7 万 5 千ユーロの罰金が課せられる。

本法律により、第三者のメールアドレスの不正使用による第三者の政党又は団体への加入、あるいは第三者のメールアドレスの不正使用によるニセメールの発信といった陰険な行為への取り締まりが可能となるとしている[80]。

ここでいう「身元」という表現は、人のあらゆるログイン名、つまりその人の氏名だけではなく、ニックネーム（異名）あるいはインターネット上で使用するハンドルネームを含んでいるとみなされるべきだと考えられている。

### ４．２．３　不正アクセスにつながる可能性のある行為に関する法令

#### （１）ウィルス作成

刑法第 323-1 条、323-2 条、323-3 条

マルウェアやボットネットなどのコンピュータ・ウイルスを直接取り締まる法律は存在

---

[79] 2009 年 1 月 20 日、破毀院刑事部は、第三者のメールアドレスを使用した結果、その者に刑事訴追を受ける危険が生じた場合、その行為は刑法第 434-23 条に規定される身元詐称に該当する、という判決を確かに下した。しかし、別件の事件では、詐称が被害者に対しいかなる法的又は経済的被害を与えなかった場合、身元詐称の罪質を構成しないとされ、刑法典の新規の条はインターネット上特有の身元詐称を罰するものであることを示した。刑法典の新規の第 222-16-1 条の第 1 項は、第三者あるいは他者の平穏を乱す目的で、電子通信ネットワーク上で第三者の身元又は個人情報を繰り返し使用する行為を罰する。第 2 項は、第三者の名誉毀損あるいは敬意を欠くことを目的で、電子通信ネットワーク上で第三者の身元又は個人情報を使用する行為を、同様の刑罰をもって罰する。（国民議会への報告書 N° 2271 の p111～114、Article2 を参照（http://www.assemblee-nationale.fr/13/rapports/r2271.asp））。

[80] 国民議会への報告書 N° 2271 の p22、a）新技術の不正使用の取り締まり強化を参照（http://www.assemblee-nationale.fr/13/rapports/r2271.asp）。

していないが、不正アクセス行為の予備行為に関しては、刑法第 323-3-1 条に規定されている。不正アクセスを禁止した刑法第 323-1 条、システムの動作妨害を禁止した刑法第 323-2 条、データを不正に消去・改変する行為を禁止した刑法第 323-3 条によって規定される犯罪を実行する目的のために作成、あるいは特別にカスタマイズされた装置、機械、情報処理プログラム、データを導入する、所持する、提供する、譲る、若しくは自由に利用できる状態にする行為は、当該犯罪の所定刑、又は最も重く罰せられる犯罪の所定刑によって処罰するとされている。

直接的なコンピュータ・ウイルスの取り締まりに関しては、欧州委員会が 2010 年 9 月 30 日にサイバー攻撃に対する防衛強化策を発表している[81]。サイバー攻撃に対する防衛強化策として新たに 2 つの規則案が発表され、大規模なサイバー攻撃に見られるような新たなサイバー犯罪を取り締まるための規則、及び「欧州ネット・情報セキュリティ機関(ENISA)」の役割の強化と近代化のための規則となっている。同提案によると、サイバー攻撃者及び悪意のあるソフトウェアの製作者は起訴され、より重い刑事制裁を科されることになっており、ウィルス作成に対しても罰則が与えられることとなる。これらの提案は今後、欧州議会と欧州理事会に提出され、2012 年採択に向けて協議される予定となっている。欧州委員会で採択されれば、フランスにおいてでもそれに準じた国内法が制定されるものと考えられる。

**（２）識別符号の不正取得（フィッシングサイトの構築等）**

知的所有権法第 L713 条 1~6

刑法第 226-18 条

刑法第 323-1 条

刑法第 313-1 条

刑法第 434-23 条

フランスでは、電子メールアカウントへのログイン名とパスワードを収集する目的で MSN の Hotmail の登録ページのフィッシングサイトを作成していた犯人が、パリの第一審裁判所の 2005 年 9 月 21 日判決で有罪判決を受けた[82]。これは、フランスで初めてのフィッシング詐欺に対する有罪判決であるが、知的所有権法 L713 条による偽造ブランドによる商標権侵害によるものであった。

そのほかにも、フィッシング詐欺を取り締まるために、不正な個人情報の収集を禁止した刑法第 226-18 条、不正アクセス行為を禁止した刑法第 323-1 条、詐欺に関する刑法第

81 欧州委員会プレスリリース、2010 年 9 月 30 日
（http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1239&format=HTML&aged=0&language=EN&guiLanguage=en）。

82 Legalis.net サイト、2005 年 11 月 9 日の記事
（http://www.legalis.net/spip.php?page=breves-article&id_article=1521）。

313-1 条、身分詐称に関する刑法 434-23 などが規定されている[83]が、直接フィッシングサイト構築を処罰する法律は規定されていない。

デジタル ID 盗難に関しては、上院議員の Michel Dreyfus-Schmidt 氏が上院にフィッシング詐欺等によるデジタル ID 盗難を規制する法案[84]を 2005 年 7 月に提出したが、廃案となってしまった。2008 年 12 月に同じく上院議員の Jacqueline Panis 氏が同様のデジタル ID 盗難を規制する法案[85]を提出しているが、審議はこれからとなっている。

### （３）サイバーテロ行為

刑法典第 323－2 条

サイバーテロ行為に関しては、サイバーテロ行為の結果、システムやデータベースを破壊するような行為が発生すれば、刑法典第 323－2 条「データの自動処理システムの動作を妨害する、又は不調にする行為は、5 年の拘禁刑及び 7 万 5 千ユーロの罰金で罰する。」に該当するものと考えられる。

欧州委員会では、2010 年 1 月 28 日に、CO2 排出権取引のネットに入り込み欧州 9 カ国で 300 万ユーロの被害を与えたサイバーアタッカーの出現を受け、現在のサイバーセキュリティガイドラインの見直しを行なうと表明するなど、サイバーテロ行為に対して厳しい姿勢で臨んでいる。前述した欧州委員会のサイバー攻撃に対する防衛強化策では、欧州ネット･情報セキュリティ機関(ENISA)」の役割の強化と近代化のための規則が含まれている。EU 加盟国に対してサイバー攻撃に対抗するための緊急な要請に対して迅速に行動することが義務付けられており、欧州の警察及び司法機関への協力体制をより効果的にすることを目的としている。2004 年に設立された欧州ネット・情報セキュリティ機関(ENISA)の期限は現在 2012 年と規定されているが、今回の提案ではさらに 5 年間延長し、財政及び人的資源を増加する計画だ。ENISA についてはサイバーセキュリティ確保のために、加盟国間の協力だけでなく、官民両セクターによる協力などを促進するための重要な役割を強化するという。これらの提案は今後、欧州議会と欧州理事会に提出され、2012 年採択に向けて協議される予定となっている。欧州委員会で採択されれば、フランスにおいてでもそれに準じた国内法が制定されるものと考えられる。

## ４．２．４　不正アクセスに関係する行為の捜査に関する法令

フランスでは、サイバー犯罪への取り組みのために、2000 年に情報通信技術関連犯罪対策中央局（OCLCTIC）が設立され、約 60 名のスタッフが情報通信技術に関する特別な訓

---

[83] Le Forum des droits sur l'internet サイト（http://www.foruminternet.org/）。
[84] フランス上院サイト（http://www.senat.fr/leg/ppl04-452.html）。
[85] フランス上院サイト（http://www.senat.fr/leg/ppl08-086.html）。

練を受け捜査をおこなっている。そのほとんどはサイバー犯罪捜査官の資格（CCI）を持っており、OCLCTIC の捜査官たちは、全国の警察官へもこの訓練を行い、約 260 名の警察官がサイバー犯罪捜査官と同等の資格を持つ憲兵隊のデジタルテクノロジー調査員（N'TECH）[86]へと育成されている。

### （1）不正アクセスに関係する行為の捜査における通信傍受

電気通信手段によって発せられる通信の秘密に関する 1991 年 7 月 10 日の法律 91-646 号

不正アクセスに関係する行為の捜査における通信傍受においては、「電気通信手段によって発せられる通信の秘密に関する 1991 年 7 月 10 日の法律 91-646 号」に規定されている。本法律は、全 27 条で構成されており、第 1 条において「電気通信手段によって発せられ通信の秘密は本法律によって保護される」としているが、「法律に規定された公益上の必要性がある場合に限り、また本法律によって規定された範囲内において公権力のみがこの秘密を侵害することができる」とし、司法当局によって命じられる傍受、治安上の傍受について言及している。

本法律の第 2 条では、刑事訴訟法典第 1 部第 3 編第 1 章の 3 節の表題を「電気通信手段によって発せられる通信に関する臨検、捜索、押収」とし、第 92 条から第 99 条を包括する第 1 款「臨検、捜索及び押収」が創設されることが記述されている。第 2 款「電気通信手段によって発せられる通信の傍受」として第 100 条から第 100 条の 7 を包括することになっている。

司法当局によって命じられる傍受においては、刑事訴訟法典第 100 条で、刑事事件又は軽罪事件において、刑罰が最低でも 2 年の拘禁刑である場合、審理上の必要性が認められれば、予審判事の権限・監督の下で電気通信手段によって発せられる通信の傍受、録音、転写を命じることができるとしている。刑法第 323-1 条で規定された不正アクセス行為は 2 年の拘禁刑で罰しうるため、傍受の対象となりうる。この傍受は、最大で 4 ヶ月の期間実施することができるが、期間の更新は同一形式・期間という条件でなければ認められていない。通信の傍受にあたっては、予審判事によって権限を付託された司法警察官は、電気通信担当大臣の権限・監督の下で設置された部局又は組織に属する係員、若しくは電気通信網事業又は電気通信サービス供給事業に従事する職員を動員することができる。

ただし、弁護士の事務所又はその住居に通じる回線に関しては、弁護士会の会長が予審判事から通知を受けた場合を除いて、いかなる場合も傍受できないこととなっている。

治安上の傍受に関しては、「電気通信手段によって発せられる通信の秘密に関する 1991 年 7 月 10 日の法律 91-646 号」の第 3 条において、①国家治安の維持、②テロ活動、犯罪行為、組織犯罪の予防、③私的軍隊組織及び民間傭兵に関する 1936 年 1 月 10 日の法律によって解散が命じられた集団の再組織化・存続の防止、という目的を有する場合には、電気通信手段によって発せられる通信の傍受が可能となっている。治安上の傍受に関しては、

[86] N'TECH は、Enquêteurs en technologie numérique の頭文字をとった略称となる。

首相又は首相によって特別に権限を付託された 2 名のうちのいずれか 1 名による理由が記載された書面による決定で行うことができ、司法当局によって命じられる傍受と同様に最大で 4 ヶ月の期間実施することができるが、期間の更新は同一形式・期間という条件でなければ認められていない。

治安上の傍受の場合には、決定後 48 時間以内に国家治安傍受統制委員会の委員長への通知が義務付けられている。

本法律 25 条では、法律に規定された場合を除き、通信の傍受が行われた場合や傍受した内容を利用したり公表した場合には、3 ヶ月以上の 5 ヶ月以下の拘禁刑及び 5 千フラン以上 10 万フラン以下の罰金に処されることが刑法典第 186 条の 1 として付加されることとなっている。

### （２）不正アクセスに関係する行為の捜査における差押場所が明確でない場合の措置

郵便・電子通信法典の第 L32－4 条

郵便・電子通信法典の第 L32－4 条では、電子通信担当大臣及び電子通信郵便規制機関は、任務の遂行に関連する必要及び正当な決定に基づき、①電気通信ネットワーク事業者・オンライン公衆通信サービスへのアクセスを提供するものが、郵便・電子通信法典が規定する義務を遵守しているか確認するために必要な情報・資料の収集、②電気通信ネットワーク事業者・オンライン公衆通信サービスへのアクセスを提供するものに対する捜査を行うことが認められている。

これらの捜査は、電気通信担当大臣より権限を受けて、コンセイユ・デタのデクレで定められた条件により宣誓した電子通信電子通信担当省及び電子通信郵便規制機関の係官によって行われる。係官は、事業用として使用されていた事務所、用地、輸送手段に立ち入り、必要な全事業用資料の伝達を求め、その写しをとり、召喚をして、又はその場で必要な情報及び証拠を収集することができる。

### （３）ログの保存

情報処理・データと自由に関する法律の第 28 条

ログの保存に関しては、「情報処理・データと自由に関する法律」の第 28 条において、「個人情報は、収集の際示された期限を超えて保存されない。（法令で規定のある場合、又は情報処理及び自由に関する国会委員会 CNIL の承認がある場合は適用除外）」と定めており、刑法典 226-20 条により、法令又は許可が定める期限を超えて情報を保存する行為で、統計処理や学術・歴史研究目的ではない行為に対して、5 年の拘禁及び 30 万ユーロの罰金が課せられることとなっている[87]。

---

87　内閣府「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（2008 年 3 月）（http://www.caa.go.jp/seikatsu/kojin/h21report2.pdf）。

郵便・電子通信法典の第 L34－1 条

フランスでは、2006 年 1 月に「テロとの闘いに関する、並びに安全及び国境検査に関する諸規定に係る 2006 年 1 月 23 日の法律第 2006-64 号」（以下、「テロ対策新法」と言う）が制定公布された。同法の第 5 条及び 6 条によって郵便・電子通信法典の第 L34－1 条が改正され、インターネット等の交信記録の保存を義務付けられる電子通信ネットワーク事業者の範囲が拡大された。すなわち、同法典第 L.34－ 1 条の I の第 2 項として、「それを主たる又は副次的な職業活動とし、ネットワークへのアクセスを介しオンライン通信を可能とする無償のものを含む接続を公衆に提供する者」もまた電子通信ネットワーク事業者である旨の規定が追加されたため、インターネットカフェ、Wi-Fi 接続業者、レストラン、ホテル、空港等にまで、交信記録の保存義務が課せられることとなった。ここで言う「交信記録」とは、「利用者の識別を可能にする情報、利用された通信端末装置に関するデータ、技術特性並びに各通信の日時及び長さ、要求されたか利用された補足サービスに関するデータ及びそれらサービスのプロバイダ、通信の受信者一名又は複数名の識別を可能とするデータ」のことであり、これは「電子通信データの保存に関する 2006 年 3 月 24 日のデクレ第 2006-358 号」において規定されている。郵便・電子通信法典の第 L34－1 条において、電子通信ネットワーク事業者・オンライン公衆通信サービスへのアクセスを提供するものには交信記録の消去又は匿名化の義務が課されているが、司法手続きの枠内であればこれらの義務は最長で 1 年間猶予される。上記のデクレの第 1 条によってテロ対策のため交信記録の保存期間は 1 年間と規定された。

また、欧州連合(EU)は、2006 年 2 月、プロバイダ等に対してインターネットを使ったサービス等を提供する際には IP アドレスを含む通信記録の保存を義務付ける指令を閣僚理事会において承認し、2007 年 8 月までに加盟各国に対して指令内容の実施に必要な措置を講ずるよう求めることとした。

これにより、重大犯罪の捜査に際して、EU 加盟国の各捜査当局は、各国の法律により保存が義務付けられる期間内(最低 6 か月以上 2 年まで)であれば、だれが、だれに、いつ、どこから通信を行ったのかなどについての情報を確実に入手することができるようになり、犯罪捜査が、ログの記録・保存されていないことで途切れることがなくなるものと期待されている。

## ４．３　不正アクセス関連法令条文集

### （１）刑法典

○関連する条項の抜粋訳（仮訳）

**刑法典第 113-6 条**

フランス刑法は、フランス共和国の国外においてフランス国籍を持つ者が実行した重罪に対して適用される。

また、フランス共和国の国外においてフランス国籍を持つ者が実行した犯罪が、犯罪が実行された国の法律の下で処罰されうるならば、軽罪にも適用される。

この条文は、犯罪者が起訴された罪を犯した後にフランス国籍を取得した場合にも適用される。

**刑法典第 113-7 条**

フランス刑法は、フランス共和国の国外において発生した、フランス国籍の者又は外国国籍の者が犯した、被害者がフランス国籍を持つ者である犯罪は、重罪又は拘禁刑で罰する軽罪にも適用される。

**刑法典第 226-17 条**

情報処理・データと自由に関する法律（Loi n 。78 - 17 du 6 janvier 1978）の第 34 条で要求された措置を講じずに、個人情報の処理を実施する行為又は実施させる行為は、5 年の拘禁刑及び 30 万ユーロの罰金で罰する。

**刑法典第 226-18 条**

個人情報を不法に、不当な、あるいは不正な手段で収集する行為は、5 年の拘禁刑及び 30 万ユーロの罰金で罰する。

**刑法典第 313-1 条**

詐欺は、偽名又は架空の権利能力の使用、正しい権利能力の不正使用、不正な誘導によって自然人又は法人を欺く行為であり、それによって、当人を、当人又は第三者の損害となるように資金、貴重品、若しくは財産の譲渡、サービスの提供、又は負担行為や義務履行への同意に仕向ける行為をいう。これらの行為は、5 年の拘禁刑及び 37 万 5000 ユーロの罰金で罰する。

**刑法典第 323-1 条**

不法に、データの自動処理システムの全体又は 1 部にアクセスし、又は滞留する行為は、2 年の拘禁刑及び 3 万ユーロの罰金で罰する。

前項の行為により、システム中のデータの消去若しくは改変、又はシステムの動作の悪化が生じた場合、3 年の拘禁刑及び 4 万 5 千ユーロの罰金で罰する。

**刑法典第 323-2 条**

データの自動処理システムの動作を妨害する、又は不調にする行為は、5 年の拘禁刑及び 7 万 5 千ユーロの罰金で罰する。

**刑法典第 323-3 条**

不法に自動処理システムにデータを入力する、又はそのシステム中のデータを不法に消去若しくは改変する行為は、5 年の拘禁刑及び 7 万 5 千ユーロの罰金で罰する。

**刑法典第 323-3-1 条**

第 323－1 条から第 323－3 条に規定される犯罪中の一つ又は複数を実行する目的のために作成、あるいは特別にカスタマイズされた装置、機械、情報処理プログラム、データを正当な理由なく、導入する、所持する、提供する、譲る、若しくは自由に利用できる状態にする行為は、当該犯罪の所定刑、又は最も重く罰せられる犯罪の所定刑によって処罰する。

**刑法典第 323-4 条**

第 323－1 条から第 323－3－1 条に規定される一つ又は複数の犯罪の、一件又は複数の物理的幇助の特質を帯びる準備行為を実現するために結成された団体、又は成立した共謀への参加は、当該犯罪の所定刑、又は最も重く罰せられる犯罪の所定刑によって処罰する。

**刑法典第 323-5 条**

本章に規定する違反を犯した自然人は以下の補充刑が科される：

1、第 131－26 条の条項に従い、5 年以下の期間の公民権、民法・民事上及び家族法上の権利の禁止。

2、犯罪の遂行中又は遂行の機会になされていた公務執行又は職業活動若しくは社会活動の 5 年以下の期間の禁止。

3、犯罪の実行に用いられた、又は用いようとした物、あるいは犯罪から生じた物の没収。ただし還付の対象となるものを除く。

4、非難される行為の実行に用いられた事業所一つ又は数個若しくは全部の 5 年以下の期間の閉鎖。

5、5 年以下の期間の公契約からの排除。

6、5 年以下の期間の、支払人又は証明された人物に対して振出人が元金を引き出すことを目的とする小切手以外の小切手振出しの禁止。
7、第 131－35 条に定めた条件における宣告決定の掲示又は公告。

**刑法典第 323-6 条**
第 121－2 条に定めた条件において、本章に規定する違反に関して刑法上の責任を宣告された法人は、第 131－38 条に規定される条項に従った罰金に加え、第 131－39 条に規定される刑罰が科される。
第 131－39 条の 2°に記載の禁止は、犯罪が実行された業務内、又は業務に際する活動を対象とする。

**刑法典第 323-7 条**
第 323－1 条から第 323－3－1 条に規定される犯罪の未遂は既遂と同一の刑で罰する。

**刑法典第 434-23 条**
第三者が刑事訴追を受けた、又は受けさせうる状況で、その第三者の氏名を使用する行為は 5 年の拘禁刑及び 7 万 5 千ユーロの罰金で罰する。
第 132－2 条から第 132－5 条の規定にかかわらず、当該犯罪に対して決定した刑罰は累加され、詐称の実行に際する犯罪に対して決定される刑罰と吸収されることは決してない。
第三者が刑事訴追を受けた、又は受けさせうる事態を引き起こした者には、第一項、人の民事身分に関する偽りの届出により所定される刑罰を科す。

### （２）情報処理・データと自由に関する法律

○関連する条項の抜粋訳（仮訳）

**情報処理・データと自由に関する法律第 34 条**
個人情報処理責任者は、個人情報の性質と処理のリスクに関して、個人情報の安全を保護するために、とりわけ個人情報の改変、毀損、又は無権限の第三者によるアクセスを排除するために、あらゆる有効な予防措置を講じなければならない。
（以下略）

**情報処理・データと自由に関する法律第 35 条**
下請業者、又は個人情報処理責任者の権限下で行為する者若しくは下請業者の権限下で行為する者は、個人情報処理責任者の指示に基づいてのみ個人情報の処理を行うことができ

る。
個人情報処理責任者に代行して個人情報の処理を行う者は、この法律では下請業者とみなされる。
下請業者は、第 34 条に示される安全措置および秘密保持措置を十分に講じる者でなければならない。個人情報処理責任者は、そのような措置が取られていることを監督する責任がある。
（以下略）

### （３）郵便・電子通信法典

○関連する条項の抜粋訳（仮訳）

**郵便・電子通信法典 L32-4 条**
電子通信担当大臣及び電子通信郵便規制機関は、任務の遂行に関連する必要及び正当な決定に基づき、見合った方法で以下の行為実現を認められる：

1、電子通信ネットワーク事業者又は電子通信サービスの提供者である自然人又は法人が、L32-1 条及び L32-3 条に規定された原則及び本法典又は本法典適用を規定する法文が課する義務を順守していることを確認するため、これら自然人又は法人から必要な情報あるいは資料を収集する。
2、同自然人又は法人に対し捜査を行う。

これらの捜査は、電子通信担当大臣により捜査に対する授権を受け、コンセイユ・デタの議を経たデクレにより定められた条件により宣誓した電子通信担当省及び電子通信郵便規制機関の官吏及び係官により行われ、調書が作成される。副本は 5 日以内に当事者に送付される。
前項に記載された官吏及び係官は電子通信ネットワーク事業又は電子通信サービスの提供を行う人により事業用として使用されていた事務所、用地、輸送手段に立ち入り、必要な全事業用資料の伝達を求め、その写しをとり、召喚をして、又はその場で必要な情報及び証拠を収集することができる。官吏及び係官は事務所に、8 時から 20 時の間、又はその一般の業務時間にしか立ち入ることができない。事務所が、又はその一部が住居となっている場合には、L32-5 条に規定された条件により捜索が許可される。
電子通信担当大臣及び電子通信郵便規制機関は、本条適用により収集した情報が、行政と公衆の関係の改善に係る措置並びに行政、社会保障制度及び税務手続きに係る規定に関する 1978 年 7 月 17 日の法律第 78－753 号第 6 条の対象となる秘密により保護されている場

合、それらが漏洩しないよう留意する。

**郵便・電子通信法典 L34-1 条**

Ⅰ．電子通信事業者及び特にその活動がオンライン公衆通信サービスへのアクセスを提供する者は，すべての交信記録を，以下 II, III,IV 及びⅤの規定を条件として，消去又は匿名のものとする。

それを主たる又は副次的な職業活動とし，ネットワークへのアクセスを介しオンライン通信を可能とする無償のものを含む接続を公衆に提供する者は，本条に基づき電子通信事業者に適用される規定を遵守するものとする。

Ⅱ．特定のカテゴリーの技術データを消去又は匿名のものとする作業は，刑事犯罪の捜査，確認及び訴追の必要又は知的財産法第 336-3 条に定義される義務の不履行のため，並びに，情報担当司法機関又は知的財産法第 331-12 条に記載される最高機関の用に供することを必要あれば可能とすることのみを目的として，その期間を最長で 1 年間に延長できる。「情報処理及び自由に関する全国委員会」の意見を基に採択されたコンセイユ・デタのデクレは，事業者 12)の活動及び通信の種類，並びに，政府の求めに応じて同事業者がそのためにおこなうサービス業務 13）に対する識別可能で固有の追加費用について必要ある場合の補償方式に従って，Ⅴに定める範囲内で，当該カテゴリーのデータとそれらデータの保存期間を定める。

Ⅲ．電子通信サービス業務の提供に対する請求書作成と支払いのために，事業者は，「情報処理及び自由に関する全国委員会」の意見を受けて発せられるコンセイユ・デタのデクレによって，同事業者の活動と通信の種類に基づき，Ⅴに定める範囲内で決められたカテゴリーの技術情報を，請求書に合法的に異議を唱えられる期間の最後又はその請求書の支払いを受けるために開始した訴追の最後まで，使用，保存及び，必要ある場合には，請求書作成又は取り立てによって直接に関係する第三者に伝達できる。

上記事業者はさらに，自らの固有の電子通信サービスを商品化するため，又は，付加価値サービスを提供するために，加入者がそれに明らかに一定期間について同意した場合には，交信記録の処理を実施できる。その期間は，いかなる場合にも当該サービスの提供又は商品化に必要な期間を越えることはできない。また，同事業者は自らのネットワークの安全を確保するために特定のデータを保存できる。

Ⅳ．前記ＩＩとＩＩＩの規定を損なうことなく，かつ，司法上の調査の必要ある場合を除き，利用者の端末装置の位置探知を可能とするデータは，対象となるデータの種類，処理期間，処理目的及び当該データが第三者のサービスプロバイダーに伝送されるか否かについて正式に通知された加入者の同意のある場合を除き，ルーティング以外の目的で通信中

に使用することも，通信終了後に保存し処理することもできない。加入者は，自らの同意の撤回を，その伝達に要する費用を除き無料で，いつでもできる。利用者は与られた同意の停止を，それを伝達するのに要する費用を除き，簡単にかつ無料でできる。緊急サービス用の通話はすべて，その利用者が始動させた非常用操作の帰結まで，そして，その操作の実現を可能とするためにのみ，利用者の同意の下にあるものとみなす。

V．前記 II，III 及び IV に定める条件で保存し処理されたデータは，事業者が提供するサービスの利用者の識別，同事業者がおこなう通信の技術特性及び端末装置の位置探知を専ら対象とする。
上記データは，当該通信において，交換された通信又は参照された情報の内容を，それがどのような形であれ，いかなる場合にも対象とできない。
上記データの保存と処理は，情報処理，ファイル及び自由に関する 1978 年 1 月 6 日の法律第 78-17 号の規定を遵守しておこなう。
事業者は，本条に定める以外の目的への上記データの使用を防ぐために，あらゆる措置を講ずるものとする。

### （４）電子通信データの保存に関する 2006 年 3 月 24 日のデクレ第 2006-358 号[88]

○関連する条項の抜粋訳

**第 1 条**

「電子通信ネットワークとサービスの利用者の私生活の保護」と題された郵便・電子通信法典の法規部第 2 編第 1 章第 2 節第 3 款（コンセイユ・デタの議を経たデクレ）は，以下のとおり記載された第 R10－12 条，第 R10－13 条及び第 R10－14 条を含む：

「第 R10－12 条　第 L34－1 条の II 及び III の適用に当たって，交信記録は，電子通信方式によって利用可能とされる情報であり，事業者がその伝送をおこない，法律で追求される目的から見て適切である電子通信の際に事業者によって記録され得る情報と解される。」

「第 R10－13 条

I. 第 L34－1 条の II に基づき，電子通信事業者は，刑事犯罪の捜査，確認及び訴追の必要のために，以下を保存する：

ａ）利用者の識別を可能にする情報

ｂ）利用された通信端末装置に関するデータ

ｃ）技術特性並びに各通信の日時及び長さ

ｄ）要求されたか利用された補足サービスに関するデータ及びそれらサービスのプロバイダ

ｅ）通信の受信者一名または複数名の識別を可能とするデータ

II.　事業者は，電話通信活動に当たって，I に述べられたデータ，さらに，通信の起点と位置探知を可能にするデータを保存する。

III.　本条に述べられたデータの保存期間は，記録の日から 1 年とする。

IV.　本条に述べられたカテゴリーに属するデータの提供のために司法機関からの要請によって事業者が負担する確認可能で固有の追加費用は，刑事訴訟法第 R213－1 条に定める方式に従って補償される。」

「第 R10－14 条　（略）」

---

88 同デクレの日本語訳については、社会安全研究財団「諸外国におけるインターネットカフェ関連法制に関する調査報告書」（2007 年 11 月）（http://www.syaanken.or.jp/02_goannai/08_cyber/cyber1911_01/pdf/17_29.pdf）より引用した

## （５）1991 年 7 月 10 日の法律第 91-646 号

○関連する条項の抜粋訳（仮訳）

**第 1 条**

電子通信手段によって発せられる通信の秘密は、法律によって保護される。

法律に規定された公益上の必要性がある場合に限り、また本法律に規定された範囲内において、公権力のみがこの秘密を侵害することができる。

**第 3 条**

国家治安に関連する情報を捜索し、フランスの潜在的な科学的及び経済的可能性にかかわる本質的要素を保護し、若しくはテロ行為、犯罪、組織犯罪を予防し、又は戦闘隊及び私兵団体に関する 1936 年 1 月 10 日法の適用によって解散が命じられた集団の再組織化又は存続を防止する目的を有する場合には、電子通信手段によって発せられる通信の傍受が、第 4 条に規定された条件において例外的に許可される。

**第 4 条**

許可は、首相又は彼によって特別に権限を付託された二名の者のうちいずれか一方の、理由が付記された書面による決定で認められる。決定は、国防大臣、内務大臣、税関担当大臣若しくは彼らの各々が特別に権限を付託する二名の者のうちいずれか一方の、理由が付記された書面による申請に基づいて行われる。

首相は許可された傍受の実施に関して、管理の集中化を行う。

**第 5 条**

第 4 条の適用によって傍受が同時に実施されうる場合、その最大件数は首相によって決定される。

第 4 条に規定した各大臣への割り当て数及び配分数に関する決定は、即刻、全国治安盗聴管理委員会に通知される。

**第 6 条**

第 3 条に記載された許可は、期間として最長 4 ヶ月与えられる。この期間の経過後には、傍受を実施することができなくなる。当該許可は、同一の形式及び期間という条件でなければ、更新されることがない。

## （６）刑事訴訟法典

○関連する条項の抜粋訳（仮訳）

**刑事訴訟法典　第２目：電気通信手段によって発せられる通信の傍受**

**第 100 条**

刑事事件又は軽罪事件において、科された刑罰が 2 年以上の拘禁刑である場合で、審理上の必要性があれば、予審判事は電気通信手段によって発せられる通信の傍受、録音、及び転写を命ずることができる。これらの措置は、予審判事の権限及び監督下で実施される。
傍受の決定は書面による。この決定は裁判的性格を有しないので、これについてはいかなる不服申し立ても受理されない。

**刑事訴訟法典第 100-1 条**

第 100 条を適用して行われる傍受の決定には、傍受する回線を特定する全ての要素、傍受の理由となる犯罪行為、及び傍受の期間が含まれなければならない。

**刑事訴訟法典第 100-2 条**

傍受の決定は、期間として 4 ヶ月を最長として行われる。当該許可は、同一の形式及び期間という条件でなければ、更新されることがない。

**刑事訴訟法典第 100-3 条**

予審判事又は彼によって代理権を付託された司法警察官は、傍受装置を設置するために、電気通信担当大臣の権限又は監督下で設置された部局又は機関に属する係官、若しくは許可された電気通信ネットワーク事業者又は電気通信サービス供給事業に従事する職員を動員することができる。

**刑事訴訟法典第 100-4 条**

予審判事又は彼によって代理権を付託された司法警察官は、傍受及び録音の実施につき各々調書を作成する。当該調書には、それらの開始及び終了の日時が記載される。
録音物は封印され密閉の上で保管される。

**刑事訴訟法典第 100-5 条**

予審判事又は彼によって代理権を付託された司法警察官は、真実の発見に有益な通信を転写し、調書を作成する。この転写は一件記録に添付される。
外国語による通信については、この目的のために動員される通訳の援助によりフランス語

で転写される。
無効になるため、弁護権を行使する弁護士と共に通信を転写することはできない。
無効になるため、出版の自由に関する 1881 年 7 月 29 日法第 2 条に違反する取材源を特定することができる記者と共に通信を転写することはできない。

**刑事訴訟法典第 100-6 条**
記録物は、共和国検事又は法院検事長の請求により、公訴時効期間の経過後に破棄される。
破棄の措置については、調書が作成される。

**刑事訴訟法典第 100-7 条**
国民議会議員又は元老院議員の回線に関しては、議員の属する議院の議長が予審判事から通知を受けた場合を除き、いかなる傍受も行うことができない。
弁護士の事務所又はその住居に通じる回線に関しては、弁護士会長が予審判事から通知を受けた場合を除き、いかなる傍受も行うことができない。

司法官の事務所又はその住居に通じる回線に関しては、司法官の属する裁判所の院長あるいは法院検事長が予審判事から通知を受けた場合を除き、いかなる傍受も行うことができない。
無効になるため、本条により規定された手続きは時効となる。

### （7）LOPPSI 法案

○関連する条項の抜粋訳（仮訳）

**第 2 条　刑法典は次のように改正された：**
1、第 222-16-1 条及び第 222-16-2 条はそれぞれ第 222-16-2 条及び第 222-16-3 条となる
2、第 222-16-1 条は次のように改訂する：
「第 222-16-1 条」
電子通信ネットワーク上で第三者の身元又は第三者の個人情報を繰り返し使用し、その第三者あるいは他人の平穏を乱す行為は、1 年の拘禁刑及び 1 万 5 千ユーロの罰金で罰する。
電子通信ネットワーク上で第三者の身元又は第三者の個人情報を使用し、名誉毀損あるいは敬意を欠く行為は、同様の刑罰を科す。

（８）知的所有権法[89]

○関連する条項の抜粋訳

**第 III 章 登録によって付与される権利**

**知的財産法第 L713 条 1**

標章の登録は、標章の所有者に対し、所有者が指定する商品及びサービスについての標章の所有権を付与する。

**知的財産法第 L713 条 2**

次のことは、所有者の許可がない限り禁止される。

(a) 登録において指定されているのと同一の商品又はサービスについて、標章を複製し、使用し又は付すこと(これには「formula、manner、system、imitation、type、method」等の語が付記されているものも含む)、及び複製した標章を使用すること

(b) 適法に付されている標章を隠滅又は変更すること

**知的財産法第 L713 条 3**

次のことは、公衆に混同を生じさせる虞がある場合は、所有者の許可がない限り禁止される。

(a) 登録において指定されている商品又はサービスと類似のものについて、標章を複製し、使用し又は付すこと、及び複製された標章を使用すること

(b) 登録において指定されている商品又はサービスと同一又は類似のものについて、標章を模造すること、及び模造された標章を使用すること

**知的財産法第 L713 条 4**

標章によって付与される権利は、所有者に対し、所有者又はその同意を得た者が当該標章の下に欧州経済共同体又は欧州経済地域において販売する商品に係る当該商標の使用を禁止する権原を与えるものではない。

ただし、所有者は、その後に製品の状態が変化している又は損われている等正当な理由を示すことができる場合は、更なる販売行為に反対する権能を引き続き有するものとする。

89 知的所有権法（2006 年 3 月 1 日法律第 2006-236 号による改正）の日本語訳については、特許庁サイト（http://www.jpo.go.jp/shiryou/s_sonota/fips/pdf/france/chiteki_zaisan.pdf）より引用した。

**知的財産法第 L713 条 5**

世評を享受している標章を、登録において指定されたものと類似しない商品又はサービスについて使用する者は、当該使用が標章の所有者に対して害をもたらす虞がある場合、又は当該使用が標章の不当な利用に当たる場合は、民事法上の責任を有するものとする。

前段落は、前記の工業所有権の保護に関するパリ条約第 6 条の 2 の意味において周知である標章の使用に適用される。

**知的財産法第 L713 条 6**

標章の登録は、次のものと同一又は類似の標識の使用を妨げないものとする。

(a) 会社名、商号又は看板であって、当該使用が登録の前からなされているか又は善意で自己の姓を使用する他人によってなされる場合

(b) 特に付属品又は部品等として、製品又はサービスの意図される用途を述べるために必要な言及である場合。この場合は、出所についての混同が生じないことを条件とする。

ただし、当該使用が登録の所有者の権利の侵害に当たる場合は、当該所有者は、使用の制限又は禁止を要求することができる。

## ５．韓国における不正アクセス関連法令

### ５．１　韓国における不正アクセス関連犯罪の現状

「情報通信網利用促進及び情報保護などに関する法律」では、情報通信サービス提供者と集積情報通信施設[90]事業者は、ハッキングなど不正アクセスによる侵害事故が発生すれば、直ちにその事実を放送通信委員会（KCC：Korea Communications Commission）や韓国インターネット振興院（KISA：Korea Internet & Security Agency）に通報することを義務付けている（第 48 条の 3)。放送通信委員会や韓国インターネット振興院は、事故の通報を受けたら、情報の収集・分析、伝播、予報・警報など同法で定めている必要な措置を取らなければならないとされている。

警察庁サイバーテロ―対応センター（CTRC：Cyber Terror Response Center）の統計では、サイバーテロ型犯罪[91]、一般サイバー犯罪[92]の発生件数は増加傾向にあり、合計で 2003 年度の 68,445 件に対して、2009 年度には 164,536 件と 2 倍以上の伸びをみせている。特に、一般サイバー犯罪の発生件数の伸びは、2003 年度の 54,204 件に対し、2009 年度では 147,935 件と大きく増加している。

検挙数においても、2003 年度は 51,722 件であったのに対し、2009 年度では 147,069 件とその件数は大きく伸びている（表 9 参照)。

**表 9　サイバー犯罪の発生件数及び検挙件数**

| 区分<br>年度 | 合計 | | サイバーテロ型犯罪 | | 一般サイバー犯罪 | |
|---|---|---|---|---|---|---|
| | 発生 | 検挙 | 発生 | 検挙 | 発生 | 検挙 |
| 2003 | 68,445 | 51,722 | 14,241 | 8,891 | 54,204 | 42,831 |
| 2004 | 77,099 | 63,384 | 15,390 | 10,339 | 61,709 | 52,391 |
| 2005 | 88,731 | 72,421 | 21,389 | 15,874 | 67,342 | 56,547 |
| 2006 | 82,186 | 70,545 | 20,186 | 15,979 | 62,000 | 54,566 |

90 情報通信サービスを提供するためのデータセンター等の施設。

91 サイバーテロ型犯罪には、ハッキング（単純侵入、ID 盗用、ファイル削除・変更、資料流出、爆弾メール、DOS 攻撃)、悪性プログラムといった犯罪が含まれる。

92一般サイバー犯罪には、詐欺（通信、ゲーム)、不法複製（プログラム、ポルノ)、不法・有害サイト（賭博、ポルノ、爆発物、自殺)、個人情報侵害、名誉毀損、脅迫・恐喝、サイバーストーキング、サイバー性暴力といった犯罪が含まれる。

| | | | | | | |
|---|---|---|---|---|---|---|
| 2007 | 88,847 | 78,890 | 17,671 | 14,037 | 71,176 | 64,853 |
| 2008 | 136,819 | 122,227 | 20,077 | 16,953 | 116,742 | 105,274 |
| 2009 | 164,536 | 147,069 | 16,601 | 13,152 | 147,935 | 133,917 |

出典：警察庁サイバーテロ―対応センター（CTRC：Cyber Terror Response Center）

また、サイバー犯罪の分類別にその検挙数の推移を見てみると、2003 年度ではインターネット詐欺が最も多く、2007 年度までは分類別の 1 位が続いていたが、2008 年度からは不法複製販売での検挙件数が最も多くなっている。2009 年度では、不法複製販売での検挙件数が 34,575 件となっており、インターネット詐欺 31,814 件、不法サイト運営 31,101 件の検挙件数がほぼ並んでいる。サイバー犯罪の検挙数が激増する中、その内容も大きく変化してきているといえる（表 10 参照）。

**表 10　検挙したサイバー犯罪の分類**

| 区分 | 合計 | ハッキング・ウィルス | インターネット詐欺 | サイバー暴力 | 不法サイト運営 | 不法複製販売 | その他 |
|---|---|---|---|---|---|---|---|
| 2003 | 51,722 | 8,891 | 26,875 | 4,991 | 1,719 | 677 | 8,569 |
| 2004 | 63,384 | 10,993 | 30,288 | 5,816 | 2,410 | 1,244 | 12,633 |
| 2005 | 72,421 | 15,874 | 33,112 | 9,227 | 1,850 | 1,233 | 11,125 |
| 2006 | 70,545 | 15,979 | 26,711 | 9,436 | 7,322 | 2,284 | 8,813 |
| 2007 | 78,890 | 14,037 | 28,081 | 12,905 | 5,505 | 8,167 | 10,195 |
| 2008 | 122,227 | 16,953 | 29,290 | 13,819 | 8,056 | 32,084 | 22,025 |
| 2009 | 147,069 | 13,152 | 31,814 | 10,936 | 31,101 | 34,575 | 25,491 |

出典：警察庁サイバーテロ―対応センター（CTRC：Cyber Terror Response Center）

韓国インターネット振興院の「インターネット侵害事故動向及び分析」によれば、ハッキング事故の通告・処理の件数は、2005 年度の 33,633 件に対し、2010 年度は、11,844 件と大きく減少している。特に減少が激しいのはホームページ改ざんで、2005 年度の 16,692 件から 2010 年度では 2,134 件へと大きくその通告・処理の件数を減らしている（表 11 参照)。

**表 11　民間部門ハッキング事故発生現況**

| 年度 | 合計 | 迷惑メール中継[93] | フィッシング経由サイト[94] | 単純侵入の試み[95] | その他のハッキング[96] | ホームページ改ざん[97] |
|---|---|---|---|---|---|---|
| 2005 | 33,633 | 6,334 | 1,087 | — | 9,520 | 16,692 |
| 2006 | 26,808 | 14,055 | 1,266 | 3,711 | 4,570 | 3,206 |
| 2007 | 21,732 | 11,668 | 1,095 | 4,316 | 2,360 | 2,293 |
| 2008 | 15,940 | 6,490 | 1,163 | 3,175 | 2,908 | 2,204 |
| 2009 | 21,230 | 10,148 | 988 | 2,743 | 3,031 | 4,320 |
| 2010 | 11,844 | 3,689 | 746 | 3,155 | 2,120 | 2,134 |

出典：韓国インターネット振興院「インターネット侵害事故動向及び分析」

93 他人のシステムをスパムメール発送に悪用する攻撃。
94 セキュリティ脆弱性を持つ国内のシステムが、海外のフィッシングサイトとして悪用されたケース。
95 自動化されたハッキングツールによる攻撃、ワームウィルスによる感染試みのトラフックも含む。
96 KISA が受け付けた侵害事故の中で、遠隔ターミナル接続、ウェブサービスを対象にしたハッキング、意図的なスキャン攻撃、悪性コード隠匿サイトなど。
97 ハッキングによるホームページ改ざんのみで、サービス利用に不便をもたらすものの、個人情報の漏洩などは起きていないケース。

## ５．２　不正アクセス行為関連法令の実態

### ５．２．１　不正アクセス行為（助長行為を含む）に関する法令

#### （１）不正アクセス行為

韓国では、不正アクセス行為を規制する法律は多岐に渡っている。

刑法典第 347 条の 2

「刑法第 347 条の 2 コンピュータなどを使用した詐欺」では、「コンピュータなど情報処理装置に虚偽の情報又は不正な命令を入力したり、権限なしで情報を入力・変更して、情報処理をすることによって財産上の利益を取得したり、第三者に取得させるようにした者は、10 年以下の懲役又は 2 千万ウォン以下の罰金に処する」とされている。

情報通信基盤保護法　第 12 条 1 号

国家安全保障・行政・国防・治安・金融・通信・運送・エネルギーなどの業務と関連した電子的制御・管理システム及び情報通信網に、アクセス権限を持たない者がアクセスすると、「情報通信基盤保護法第 12 条　主要情報通信基盤施設への侵害行為などの禁止」1 号により処罰される。

また、アクセス権限を持った者がその権限を超えて保存されたデータを操作・破壊・隠匿又は流出する行為をしてはならない。この規定に違反して、主要情報通信基盤施設を撹乱・麻痺又は破壊した者は、10 年以下の懲役又は 1 億ウォン以下の罰金に処し、未遂犯も処罰するとしている。

情報通信網利用促進及び情報保護などに関する法律　第 48 条

「情報通信網利用促進及び情報保護などに関する法律第 48 条　情報通信網侵害行為などの禁止」では、「正当なアクセス権限なしで、又は許されたアクセス権限を越えて情報通信網に侵入してはならない」とされている。この規定に違反した者は 3 年以下の懲役又は 3 千万ウォン以下の罰金に処される。

電子政府法　第 35 条

「電子政府法第 35 条　禁止行為」では、「行政情報を権限なしで処理したり、権限範囲を越えて処理する行為、行政情報を権限なしで、他の人に利用させるようにする行為をした者は、3 年以下の懲役又は 3 千万ウォン以下の罰金に処される」とされている。また、「偽りやその他の不正な方法で行政機関などから行政情報を提供されたり、閲覧する行為をした者は、2 年以下の懲役又は 700 万ウォン以下の罰金に処する」と定めている。

電子金融取引法　第 35 条

電子金融取引法第 35 条では、「電子金融取引のための電子的装置、又は『情報通信網利

用促進及び情報保護などに関する法律』第 2 条第 1 項第 1 号の規定にともなう情報通信網に侵入して、虚偽その他の不正な方法でアクセス媒体を獲得したり、獲得されたアクセス媒体を利用して、電子金融取引をした者は、7 年以下の懲役又は 5 千万ウォン以下の罰金に処される」とされている。ここで、アクセス媒体には、電子金融取引で使われる金融機関又は電子金融業者に登録された利用者番号、暗証番号が含まれる。

信用情報の利用及び保護に関する法律　第 50 条

信用情報の利用及び保護に関する法律第 50 条では、信用情報電算システムに対して、不正なアクセス又は権限なしで信用情報を検索・複製したり、その他の方法で利用した者は、3 年以下の懲役又は 3 千万ウォン以下の罰金に処されると規定されている。

物流政策基本法　第 71 条

物流政策基本法第 71 条では、総合物流情報網、又は国家物流統合データベースの保護措置を侵害したり、毀損した者は 3 年以下の懲役又は 5 千万ウォン以下の罰金に処されるとされている。

**（２）データの財物性（データの不正取得）**

韓国では、刑法第 329 条において窃盗罪について財物（有体物及び管理できる動力[98]）を対象としているため、無体物であるデータ一般については窃取の対象とならない。ただし個人データについては、情報通信網利用促進及び情報保護などに関する法律等において、個人データを不正に取得する行為を規制している。

情報通信網利用促進及び情報保護などに関する法律　第 49 条の 2

韓国では、個人情報データは法律で保護されており、本人又は他人の個人情報データの収集、利用、提供など、その取扱いについては、本人の同意を得るなど法律に定める規定を守らなければならない。

個人情報の定義は、「公共機関の個人情報保護に関する法律」と「情報通信網利用促進及び情報保護などに関する法律」などの関連法規では、「生存する個人に関する情報として、姓名・住民登録番号などにより特定の個人を識別できる符号・文字・音声・音響及び映像などの情報(該当情報だけでは特定個人を識別することができなくても他の情報と簡単に結合して、識別できる場合にはその情報を含む)」とされている。

同法の第 49 条の 2「騙す行為による個人情報の収集禁止など」の 1 項では、情報通信網を通して騙す行為で他の人の個人情報を収集したり、他の人が個人情報を提供するように誘引することを禁じている。これに違反して、他の人の個人情報を収集した者は、3 年以下の懲役又は 3 千万ウォン以下の罰金に処される。

98 「動力」とは、電力などのエネルギーを指す。

その他、個人情報の収集・利用・保護などに関連する条文としては、第 22 条「個人情報の収集・利用同意など」、第 23 条「個人情報の収集制限など」、第 23 条の 2「住民登録番号以外による会員加入方法」、第 24 条「個人情報の利用制限」、第 24 条の 2「個人情報の提供への同意など」、第 27 条の 2「個人情報取り扱い方針の公開」、第 28 条「個人情報の保護措置」、第 28 条の 2「個人情報の漏洩禁止」がある。

信用情報の利用及び保護に関する法律

「信用情報の利用及び保護に関する法律」では、「個人識別情報」として、同法の施行令(大統領令)において「生存する個人の姓名、住所、住民登録番号、外国人登録番号、国内居所申告番号、旅券番号、性別、国籍など個人を識別できる情報」と定めている。

個人情報の収集・利用・保護などに関連する条文は、「第 24 条　住民登録電算情報資料の利用」、「第 32 条　個人信用情報の提供・活用に対する同意」、「第 33 条　個人信用情報の利用」、「第 34 条　個人識別情報の提供・利用」、「第 35 条　信用情報提供事実の通知要求」にある。

上記の各規定に違反した場合の罰則については、「第 50 条　罰則」、「第 52 条　過怠料」で定めている。

公共機関の個人情報保護に関する法律

公共機関の個人情報保護に関しては、公共機関の個人情報保護に関する法律の中で、個人情報の収集（第 4 条)、個人情報ファイルの保有範囲（第 5 条)、個人情報ファイルの保有・変更時事前協議（第 6 条)、個人情報保護方針（第 7 条の 2)、個人情報の安全性確保など（第 9 条)、インターネット上の本人確認（第 9 条の 2)、個人情報取り扱い者の義務（第 11 条）について規定している。

罰則では、公共機関の個人情報処理業務を妨害する目的で、公共機関で処理している個人情報を変更又は抹消した者は 10 年以下の懲役に処すると規定している。また、第 11 条の規定に違反して、個人情報を漏洩又は権限なしに処理したり、他人の利用に提供するなど不当な目的で使った者は、3 年以下の懲役又は 1 千万ウォン以下の罰金に処すると規定している。

位置情報の保護及び利用などに関する法律

「位置情報の保護及び利用などに関する法律」では、「個人位置情報」を、「特定個人の位置情報(位置情報だけでは特定個人の位置を識別できない場合にも他の情報と容易に結合して、特定個人の位置が識別できるものを含む)」と定義している。

この法では、「第 15 条　位置情報の収集などの禁止」、「第 16 条　位置情報の保護措置など」で個人又は所有者の同意を得なくて、該当の個人又は移動性がある物の位置情報を収集・利用又は提供してはならないと規定している。この規定に違反した場合の罰則につい

ては、「第 40 条　罰則」と「第 41 条　過怠料」で定めている。

電子取引基本法

「電子取引基本法第 12 条　個人情報保護」では、電子取引利用者の個人情報を収集・利用・提供及び管理することに関して規定されており、「情報通信網利用促進及び情報保護などに関する法律」など関連規定を遵守することとしている。

また、電子取引利用者の営業秘密を保護することについては、「第 13 条　営業秘密保護」に定めている。この規定に違反した場合の罰則に関する条文は見当たらない。

**（３）不正アクセス行為の予備行為**

刑法　第 8 条、第 28 条

刑法第 28 条には、「犯罪の陰謀又は予備行為が実行の着手に達しない場合には、法律に特別な規定がない限り罰しない」と定めている。また、刑法の総則（法の適用範囲などを規定した、第 1 条～第 86 条の条文）は、他の法令で定めている罪にも適用し、その法令に特別な規定がある場合には例外である（第 8 条）としている。したがって、不正アクセスの予備行為は、関連する法律に特別な規定が無い限り処罰されない。

上記で言及した不正アクセス行為を規制する法律でも、予備行為に対する特別な規定が無いため、システム探索等の不正アクセスの予備行為は、法律で罰せない。一方、未遂犯については、既遂犯より減軽することができるものの、罰則については、各法律で定めるとしている。

**（４）不正アクセス行為の国外犯**

刑法　第 6 条

「刑法第 6 条　大韓民国と大韓民国国民に対する国外犯」には、「第 5 条　外国人の国外犯」に記載した以外の罪を犯した外国人にも刑法の規程を適用するが、「ただし国外の場合、行為地の法律によって犯罪を構成しないか、あるいは訴追又は刑の執行を免除する場合には例外にする」としている。つまり、国際私法上の準拠法として、行為地法（問題となる行為のなされる場所の法律）に従うようにしている。

また、国際私法の「第 7 条　大韓民国法の強行的適用」により、刑法第 5 条の罪のように強制適用の規程がある法律や、国際私法第 9 条により、不法行為地での法律が大韓民国の法律を準拠法として適用する場合は、大韓民国の法律を適用することになっている。

結論的に、不正アクセス行為に対する関連法律の中には、国外犯の規制に係る明確な条文や国際私法の第 7 条「韓民国法の強行的適用」を当てるべき強制規程がないため、外国に設置しているサーバに対して犯人が別の外国から不正アクセス行為をした場合は、サーバが置かれた国の行為地法を適用することになる。もし、行為地の法律によって犯罪を構成しないか、あるいは訴追又は刑の執行を免除する場合には処罰できない。

### （５）他人の識別符号の譲渡し・譲受け

韓国では、一般の情報通信サービスにおいてID・パスワードの譲渡し・譲受け行為を直接的に規制する法律はなく、サービスの約款の中でその行為を禁止している程度である。そのため、ID・パスワードの譲渡し・譲受けをした場合は、法的な処罰を受けるのではなく、サービス利用の制限を受ける水準で止まる。状況によっては民事上の損害賠償を求められことはある。

下記は、アジア経済新聞（2010.07.27）に掲載された、2010年7月の最高裁判所の判例の記事である。

> *他人にオンラインゲームのID・パスワードを譲渡した後、そのパスワードを勝手に変えたとしても、刑事上の責任を問うことにはならないという、大法院（最高裁判所）の判断が出た。7月27日最高裁判所1部は、「情報通信網利用促進及び情報保護などに関する法律」（情報通信網法）違反の容疑で起訴されたA氏の上告審で、原審の無罪判決を確定したことを明らかにした。*
>
> *最高裁判所は、問題のオンラインゲームの利用約款が、識別符号の譲渡や売買を禁止する点、A氏が第三者に識別符号の使用を許諾したとしても原則的に第三者には正当なアクセス権限がない点などを総合すれば、A氏が暗証番号を変えたのが情報通信網法を犯して「他人の情報を毀損する行為」に該当しないと見た原審判決に法理誤解など違法がないと説明した。*
>
> *オンラインゲームの利用約款には、識別符号の譲渡や売買を禁止しているので、アクセス権は「譲り受けた者」でなく相変らず「名義者」が持っているという趣旨だ。*
>
> *A氏は2005年、「リネージュ」（韓国の人気オンラインゲーム）のアカウントをB氏に譲渡した。A氏が譲渡したアカウントは、その後も数回に亘って他人に譲渡され、最後にはC氏が直前の利用者から500万ウォンで買った。その後、A氏はあるインターネットカフェで、C氏が譲り受けたアカウントの名義者がまだ自身である点を利用して、暗証番号をむやみに変えた容疑で起訴された。*

この判決では、問題になったサービスに対して、ID・パスワードの譲渡し・譲受けや売買のその行為自体は、違法とされていない。

実際、大抵のサービスにおいては、約款で会員にID・パスワードの管理に対する義務と責任を与え、これを第三者に利用させてはならないと定めている。会員は、サービスの利用権限、その他の利用契約上の地位を他人に譲渡したり、譲受けすることはできず、これを質権の目的で使うことができないと規定している。それによって損害が発生した場合は、賠償しなければならないとしている。

下記は、韓国最大の SNS（ソーシャルネットワーキングサービス）を運営する nate.com の利用者約款の例である。

*第 24 条(会員の義務)*

*3)会員は、申請様式を記載する際、又は会員情報を変更する際には、実名で、すべての事項を事実に基づいて作成するべきで、虚偽又は他人の名義(又は情報)を使ったことが判明した場合、会員はサービス利用と関連した一切の権利を主張することができない。*

*4)会員は、サービスの利用権限、その他サービス利用の契約上の地位を、他人に譲渡し・譲受けすることはできず、これを担保に提供することはできない。*

*5)会員は、会員 ID 及び暗証番号を徹底的に管理するべきで、管理の不備による不正使用などで発生するすべての結果に対する責任は会員本人が負担し、当社はこれに対するいかなる責任も負わない。*

*6)会員は、本人の ID 及び暗証番号を第三者が利用するようにしてはならない。会員本人の ID 及び暗証番号が盗難に遭ったり、第三者に使われていることを認知した場合には、直ちに当社に通知して、当社が案内することに従わなければなりません。*

*7)会員は、利用契約を締結してから与えられた ID を変更することはできず、やむをえない理由によって変更する場合には、利用契約を解約して再加入しなければならない。*

*第 28 条(損害賠償)*

*1)会員が本約款の規定に違反したことによって当社に損害が発生した場合、この約款を違反した会員は当社に発生するすべての損害を賠償しなければならない。*

*2)会員がサービスを利用する過程で行った不法行為、又はこの約款違反行為によって当社が当該会員以外の第三者から損害賠償請求や訴訟を含む各種の異議申し出を受けた場合に、当該会員は自身の責任と費用で当社を免責させるべきで、当社が免責されることもできない場合、当該会員はそれによって当社に発生したすべての損害を賠償しなければならない。*

情報通信サービスの約款については、「情報通信網利用促進及び情報保護などに関する法律第 56 条　約款の申告など」に、通信課金サービス提供者は、通信課金サービスに関する約款を定めて、放送通信委員会に申告（変更申告を含む）しなければならない、と規定している。また、「位置情報の保護及び利用などに関する法律第 12 条　利用約款の申告など」には、位置情報事業者及び位置基盤サービス事業者がサービスの約款を放送通信委員会に申告することを義務付けている。電子金融取引法では、「第 24 条　約款の明示と変更通知など」、「第 25 条　約款の制定及び変更」には、電子金融業者又は金融機関は、サービス約

款の金融委員会に申告するように定めている。それぞれの法律で約款申告の義務を違反した場合は、1 千万ウォン以下の過怠料を賦課するとしている。

電子金融取引法　第 6 条

ID・パスワードの譲渡し・譲受け行為を規制する法律の特別な事例として、「電子金融取引法第 6 条　アクセス媒体の選定と使用及び管理」3 項の規定がある。この法では、アクセス媒体（電子金融取引で使われる利用者番号、暗証番号を含む）は、他の法律に特に規定がない限り、譲渡し・譲受けをしたり質権を設定してはならないとされている。ただし、第 18 条の規定にともなう先払い電子支給手段や電子貨幣の譲渡、又は担保提供のために必要な場合にはこの限りでない、としている。この規定に違反した者は、1 年以下の懲役又は 1 千万ウォン以下の罰金に処される。

住民登録法　第 37 条

住民登録法の第 37 条では、「法律に従わずに営利の目的で他人の住民登録番号に関する情報を知らせる者は､3年以下の懲役又は1千万ウォン以下の罰金に処する」と定めている。韓国では今まで、住民登録番号が情報通信サービスの会員登録に広く使われてきた。場合によっては、住民登録番号自体がサービスへアクセスする ID、又はパスワードの役割をすることがある。このようなサービスにおいて、ID・パスワードの譲渡し・譲受けとして住民登録番号の情報を知らせる者は処罰されることになる。

電子署名法　第 23 条

「電子署名法第 23 条　電子署名生成情報の保護など」5 項では､「行使する目的で他の人に公認証明書 を譲渡又は貸与したりすることができない」と定めている。電子証明書を譲渡し・譲受けすることには、証明書を使うためのパスワードの譲渡し・譲受けが伴う。この規定に違反した者は 1 年以下の懲役又は 1 千万ウォン以下の罰金に処される。

ゲーム産業振興に関する法律　第 32 条

「ゲーム産業振興に関する法律第 32 条　不法ゲーム物などの流通禁止など」 1 項では、「ゲーム物の利用を通して、獲得した有・無形の結果（点数、景品、ゲーム内で使われる仮想の貨幣として大統領令で定めるゲームマネー及び大統領令で決めるこれと類似しているものをいう）両替又は両替を斡旋したり再買入することを業とする行為をしてはならない」と定めている。この際は、ID・パスワードの譲渡し・譲受けの手法がよく使われているケースが多い。それを業として行う場合は、法律違反になり、5 年以下の懲役又は 5 千万ウォン以下の罰金に罰される。

### （６）他人の識別符号の譲渡し・譲受けに関する広告又は誘引行為

不正アクセスの助長行為に関しては、関連法に特別な規定が無いのが現状である。実際、インターネット上の電子掲示板などで、人気ゲームやサービスの ID・パスワードを譲渡するとの広告がしばしば見られるが、この行為は法律で処罰されるより、大抵しばらくして電子掲示板の管理者により削除されることが多い。

### （７）アクセス管理者等の防御措置

国家情報化基本法　第 37 条、第 38 条、第 39 条

「国家情報化基本法第 37 条　情報保護施策の用意」では、「国家機関と地方自治体は、情報を処理するすべての過程において、情報の安全な流通のための情報保護の施策を用意しなければならない。政府は、暗号技術の開発と利用を促進し、暗号技術を利用して情報通信サービスの安全を図る措置を用意しなければならない」と定めている。

「第 38 条　情報保護システムに関する基準告示など」では、情報保護システムの性能と信頼度に関する基準を定めて告示し、情報保護システムを製造、又は輸入する者にその基準を守ることを勧告することができるとしている。

また、「第 39 条　個人情報保護施策の用意」では、国家機関と地方自治体は、国家情報化を推進するにあたり、個人情報保護のための施策を用意しなければならないことが規定されている。

情報通信基盤保護法　第 5 条、第 6 条、第 10 条、第 11 条

情報通信基盤保護法では、国家安全保障・行政・国防・治安・金融・通信・運送・エネルギーなどの業務と関連した電子的制御・管理システム及び「情報通信網利用促進及び情報保護などに関する法律」の規定による情報通信網を、情報通信基盤施設として（第 2 条）、主要情報通信基盤施設を管理する機関の長に対して、施設保護対策（第 5 条主要情報通信基盤施設保護対策の樹立など）と、施設保護計画（第 6 条）を立てて施設のセキュリティを守ることを定めている。

また、中央行政機関の長は、所管分野の情報通信基盤施設中で電子的侵害行為からの保護が必要だと認められる情報通信基盤施設を主要情報通信基盤施設として指定し（第 8 条）、保護指針（第 10 条）を制定して保護措置の命令・勧告（第 11 条）を出すことで施設を保護することを定めている。保護措置の命令などに違反した者には、1 千万ウォン以下の過怠料に処する（第 30 条過怠料）としている。

情報通信網利用促進及び情報保護などに関する法　第 45 条、第 46 条の 3、第 47 条の 3

情報通信網利用促進及び情報保護などに関する法の「第 45 条　情報通信網の安全性確保など」1 項では、「情報通信サービス提供者は、情報通信サービスの提供に使われる情報通信網の安全性及び情報の信頼性を確保するための保護措置を取らなければならない」と定

めている。また、「第 46 条の 3　情報保護安全診断」で、「放送通信委員会が認めた安全診断を遂行することができる者(以下、「安全診断遂行機関」という)から、自身の情報通信網又は集積情報通信施設に対して、毎年情報保護指針にともなう情報保護安全診断を受けなければならない」と定めている。これに違反して、情報保護安全診断の結果を提出しなかったり、偽りで提出した者、又は改善命令を履行しない者は、1 千万ウォン以下の過怠料が賦課される。

「同法第 47 条の 3　利用者の情報保護」1 項では、政府は、利用者の情報保護に必要な基準を定めて利用者に勧告し、侵害事故の予防及び拡散防止のために、脆弱性の点検、技術支援など必要な措置を取ることができる。2 項では、主要情報通信サービス提供者は、情報通信網に重大な侵害事故が発生して自分のサービスを利用する利用者の情報システム、又は情報通信網などに深刻な障害が発生する可能性があれば、利用約款に定めるところにより、その利用者に保護措置を取るように要請し、これを履行しない場合には、該当情報通信網での接続を一時的に制限することができるとしている。3 項では、「ソフトウェア産業振興法」第 2 条にともなうソフトウェア事業者は、セキュリティに関する脆弱性を補完するプログラムを製作した時には、韓国インターネット振興院に知らせなければならなく、またそのソフトウェア使用者には、製作した日から 1 ケ月以内に 2 回以上知らせなければならないと定めている。これに違反して、ソフトウェア使用者に知らせない者は、1 千万ウォン以下の過怠料が賦課される。

信用情報の利用及び保護に関する法律　第 19 条

信用情報の利用及び保護に関する法律の「第 19 条　信用情報電算システムの安全保護」では、「信用情報会社等は、信用情報電算システム(第 25 条第 6 項にともなう信用情報共同電算網を含む)に対する第三者からの不正なアクセス、入力された情報の変更・毀損及び破壊、その他の危険に対して大統領令に定めるところにより技術的・物理的・管理的セキュリティ対策をとらなければならない」と定めている。これに違反した者には、1 千万ウォン以下の過怠金が賦課される。

物流政策基本法　第 33 条

「物流政策基本法第 33 条　電子文書及び物流情報のセキュリティ」4 項では、「総合物流情報網事業者は、又は国家物流統合データベース運営者は、電子文書及び物流情報のセキュリティに必要な保護措置を講じなければならない」と定めている。

位置情報の保護及び利用などに関する法律　第 16 条

位置情報の保護及び利用などに関する法律の「第 16 条　位置情報の保護措置など」1 項では、位置情報事業者などは、位置情報の漏洩、変造、毀損などを防止するために位置情報の取り扱い・管理指針を制定したり、アクセス権限者を指定するなどの管理的措置とフ

ァイアウォールの設置や暗号化ソフトウェアの活用などの技術的措置を取らなければならない。この場合管理的な措置と技術的な措置の具体的内容は大統領令で定めると、と定めている。これに違反した者には、1 年以下の懲役又は 2 千万ウォン以下の罰金に処される。

### ５．２．２　不正アクセスにつながる可能性のある行為に関する法令

#### （１）ウィルス作成

情報通信基盤保護法　第 12 条

情報通信基盤保護法の「第 12 条　主要情報通信基盤施設への侵害行為などの禁止」では、主要情報通信基盤施設に対し、データを破壊したり主要情報通信基盤施設の運営を邪魔する目的でコンピュータ・ウイルス・論理爆弾などのプログラムを投じる行為をしてはならないと定め、これに違反して、主要情報通信基盤施設を撹乱・麻痺又は破壊した者は、10 年以下の懲役又は 1 億ウォン以下の罰金に処される。未遂犯も処罰する、と規定している。

情報通信網利用促進及び情報保護などに関する法律　第 48 条

情報通信網利用促進及び情報保護などに関する法律の「第 48 条　情報通信網侵害行為などの禁止」2 項では、「正当な理由なしで、情報通信システム、データ又はプログラムなどを毀損・滅失・変更・偽造したり、その運用を妨害できるプログラム(以下“悪性プログラム”という)を伝達又は流布してはならない」とし、第 71 条「罰則」でこれに違反した者には、5 年以下の懲役又は 5 千万ウォン以下の罰金に処すると定めている。

現在、「(仮称)悪性プログラムの拡散防止などに関する法律案」が、国会と政府の中で審議されている。この法案では、ウィルス作成、配布に関する規程が今までよりもっと具体的に定められている。

#### （２）識別符号の不正取得（フィッシングサイトの構築等）

情報通信網利用促進及び情報保護などに関する法律　第 49 の 2 条

情報通信網利用促進及び情報保護などに関する法律の「第 49 条の 2　騙す行為による個人情報の収集禁止など」1 項では、情報通信網を通して騙す行為で他の人の情報を収集したり、他の人が情報を提供するように誘引してはならないとして、フィッシングサイトの構築等の規制している。これに違反して他人の個人情報を収集した者は、第 72 条「罰則」2 項により、2 年以下の懲役又は 1 千万ウォン以下の罰金に処される。

しかしながら、この法律の違反で起訴されて裁判を受けた判例は見当たらない。その理由は、第一に、フィッシングサイトは、殆どが海外に置かれているため犯人を逮捕することは至難であること。第二に、もし国内のフィッシングサイトを用いて犯罪が発生した場合も 2 つ以上の罪名に触れることが多く、韓国では、刑法第 40 条により複数の刑で処され

る場合は、最も重い刑で処罰されることとなっているため、「情報通信網利用促進及び情報保護などに関する法律」ではなく、別の法律で処罰されることになるという。

### （３）サイバーテロ行為

刑法　第 314 条

Dos 攻撃等の規制に係る条文として、「刑法第 314 条　業務妨害」2 項では、「コンピュータなど情報処理装置又は電磁記録など特殊媒体記録を損壊したり、情報処理装置に虚偽の情報又は不正な命令を入力したり、その他方法で、情報処理に障害を発生させて人の業務を妨害した者は、5 年以下の懲役又は 1 千 500 万ウォン以下の罰金に処する」と規定している。

情報通信基盤保護法　第 12 条

情報通信基盤保護法の「第 12 条　主要情報通信基盤施設への侵害行為などの禁止」 では、「主要情報通信基盤施設の運営を邪魔する目的で、一時に大量の信号を送ったり不正な命令を処理するなどの方法で情報処理に誤りを発生させようとする行為をしてはならない」と定め、これに違反して、主要情報通信基盤施設を撹乱・麻痺又は破壊した者は、10 年以下の懲役又は 1 億ウォン以下の罰金に処される。未遂犯も処罰すると規定している。

情報通信網利用促進及び情報保護などに関する法律　第 48 条

情報通信網利用促進及び情報保護などに関する法律の「第 48 条　情報通信網侵害行為などの禁止」3 項では、「情報通信網の安定的運営を妨害する目的で大量の信号、又はデータを送ったり、不正な命令を処理するようにするなどの方法で情報通信網に障害を発生させようとしてはならない」と定め、これを違反して、情報通信網に障害が発生させようとした者は、「第 71 条　罰則」により、5 年以下の懲役又は 5 千万ウォン以下の罰金に処すると規定している。

## ５．２．３　不正アクセスに関係する行為の捜査に関する法令

### （１）不正アクセスに関係する行為の捜査における通信傍受

通信秘密保護法　第 5 条

通信秘密保護法の第 3 条では、郵便物の検閲・電気通信の監聴（傍受）、又は通信事実確認資料の提供と、公開されない他人間の対話を録音又は聴取することができないと規定している。ただし、第 5 条において、郵便物の検閲、又は電気通信の監聴（傍受）は、犯罪捜査又は国家安全保障のために補充的な手段で利用されるべきで、国民の通信秘密に対する侵害が最小限に終わるように努力しなければならないとして、犯罪捜査のための通信制限措置（傍受）の許可要件を、法律で定めている犯罪を計画又は実行、あるいはそれを疑

うほどの十分な理由があって、他の方法ではその犯罪の実行を阻止したり、犯人の逮捕又は証拠の収集が難しい場合に限定している。

通信傍受を行うことを認める犯罪の種類では、「刑法」上の内乱の罪、外患誘致の罪、国交に関する罪、公安を害する罪、爆発物に関する罪、公務員の職務に関する罪、逃走と犯人隠匿に関する罪、放火と失火の罪、アヘンに関する罪、通貨に関する罪、有価証券などに関する罪、殺人の罪、逮捕監禁に関する罪、常習犯の脅迫の罪、常習犯の窃盗・強盗、詐欺恐喝の罪など の一部の犯罪のみである。「軍刑法」では、反乱の罪、利敵の罪、指揮権濫用の罪、逃避の罪、離脱の罪、抗命の罪など の犯罪がある。その他、「国家保安法」に規定された犯罪、「軍事機密保護法」に規定された犯罪、「麻薬類管理に関する法律」で規定された犯罪の一部、「暴力行為などの処罰に関する法律」で規定された犯罪の一部、「銃砲・刀剣・火薬類など取り締まり法」に規定された犯罪の一部、「定犯罪加重処罰などに関する法律」で規定された犯罪の一部のみである。

不正アクセスに関係する行為の捜査において、不正アクセス行為自体は通信傍受が認められる犯罪ではない。不正アクセス行為によって、上記の通信傍受を認める犯罪につながる疑いがある場合は、検事は裁判所に通信傍受の許可を請求することができる。この法律に違反した場合は、罰則として 10 年以下の懲役と 5 年以下の資格停止に処される。

### （2）不正アクセスに関係する行為の捜査における差押場所が明確でない場合の措置

通信秘密保護法　第 15 条の 2

通信秘密保護法の第 15 条の 2 では、「電気通信事業者は、検事・司法警察官又は情報捜査機関の長が同法により執行する通信制限措置及び通信事実確認資料の提供要請に協力しなければならない」と定めている。通信事実確認資料は、コンピュータ通信、又はインターネットの使用者が電気通信役務を利用した事実に関するコンピュータ通信、又はインターネットのログ記録の資料が含まれている（第 2 条)。犯罪捜査のために通信事実確認資料を提供してもらうためには、その理由、該当加入者との関連性及び必要な資料の範囲を記録した書面で、管轄地方裁判所(普通軍事裁判所を含む)、又は支所の許可を受けなければならない。ただし、管轄地方裁判所、又は支所の許可を受けられない緊急な理由がある時には、通信事実確認資料提供を要請した後、遅滞なく裁判所からその許可を受けて電気通信事業者に送付しなければならない（第 13 条)。

情報通信網利用促進及び情報保護などに関する法律　第 48 条の 4

情報通信網利用促進及び情報保護などに関する法律の第 48 条の 4 では、放送通信委員会は、不正アクセスなどの侵害事故の原因を分析するために必要と認めれば、情報通信サービス提供者と集積情報通信施設事業者に情報通信網の接続記録などの関連資料の保全を命じられる。また、情報通信サービス提供者と集積情報通信施設事業者に事故関連資料の提出を要求でき、民・官合同調査団に、関係する事業場に出入して侵害事故原因を調べるよ

うにさせることができると規定している。この際、調査のための通信事実確認資料に該当する資料の提出は、「通信秘密保護法」の定めに従う。この命令に違反して、関連資料を保全しない者は、2年以下の懲役又は1千万ウォン以下の罰金に処される。

### （3）ログの保存

通信秘密保護法　施行令第41条

通信秘密保護法の規定で電気通信事業者が保存する、コンピュータ通信又はインターネットのログ記録と、コンピュータ通信又はインターネットの使用者が情報通信網に接続するために使う情報通信機器の位置を確認できる接続地の追跡資料は、同法の施行令第41条（大統領令）で保存期間が3カ月以上となっている。

## ５．３　不正アクセス関連法令条文集

### （１）刑法典

○関連する条項の抜粋訳（仮訳）

**第１編　総則　（＊第１条～第 86 条）**

**第１条　犯罪の成立と処罰**

①犯罪の成立と処罰は、行為時の法律に依る。

**第２条　国内犯**

本法は、大韓民国領域内で罪を犯した内国人と外国人に適用する。

**第３条　内国人の国外犯**

本法は、大韓民国領域外で罪を犯した内国人に適用する。

**第４条　国外にある内国船舶等で外国人が犯した罪**

本法は、大韓民国領域外にある大韓民国の船舶、又は航空機内で罪を犯した外国人に適用する。

**第５条　外国人の国外犯**

本法は、大韓民国領域外で次に記載した罪を犯した外国人に適用する。

1.内乱の罪

2.外患の罪

3.国旗に関する罪

4.通貨に関する罪

5.有価証券、郵票と印紙に関する罪

6.文書に関する罪中の第 225 条乃至第 230 条

7.印章に関する罪中の第 238 条

**第６条　大韓民国と大韓民国国民に対する国外犯**

本法は、大韓民国領域外で大韓民国又は大韓民国国民に対して前条に記載した以外の罪を犯した外国人に適用する。ただし、行為地の法律によって犯罪を構成しなかったり、訴追又は刑の執行を免除する場合には例外にする。

**第８条　総則の適用**

本法総則は他法令に定めている罪に適用する。ただし、その法令に特別な規定がある場合には例外にする。

**第 25 条　未遂犯**

①犯罪の実行に着手して行為を終了できなかったり、結果が発生しない場合には未遂犯で処罰する。

②未遂犯の刑は既遂犯より減軽することができる。

**第 28 条　陰謀、予備**

犯罪の陰謀又は予備行為が実行の着手に達しない場合には、法律に特別な規定がない限り罰しない。

**第 29 条　未遂犯の処罰**

未遂犯を処罰する罪は、各本条に定める。

**第 141 条　公用書類等の無効、公用物の破壊**

①公務所で使う書類、その他のもの、又は電磁気録など特殊媒体記録を損傷又は隠匿したり、その他方法でその効用を害した者に対し、7 年以下の懲役又は 1 千万ウォン以下の罰金に処する。<改正 1995.12.29>

**第 226 条　資格冒用による公文書などの作成**

行使する目的で公務員又は公務所の資格を冒用して、文書又は図画を作成した者は、10 年以下の懲役に処する。<改正 1995.12.29>

**第 227 条の 2　公電子記録の偽作・変造**

事務処理を誤らせることを目的に公務員又は公務所の電磁気録など特殊媒体記録を偽作又は変造した者に対し 10 年以下の懲役に処する。

**第 232 条　資格冒用に依る私文書の作成**

行使する目的で他人の資格を冒用して、権利・義務又は事実証明に関する文書又は図画を作成した者は、5 年以下の懲役又は 1 千万ウォン以下の罰金に処する。<改正 1995.12.29>

**第 232 条の 2　私電磁記録の偽作・変作**

事務処理を誤らせることを目的に権利・義務又は事実証明に関する他人の電磁気録など特

殊媒体記録を偽作又は変造した者に対し 5 年以下の懲役又は 1 千万ウォン以下の罰金に処する。 [本条新設 1995.12.29]

**第 313 条 信用毀損**

虚偽の事実を流布したり、その他の偽計で人の信用を毀損した者は、5 年以下の懲役又は 1 千 500 万ウォン以下の罰金に処する。<改正 1995.12.29>

**第 314 条 業務妨害**

①第 313 条の方法又は威力で人の業務を妨害した者は、5 年以下の懲役又は 1 千 500 万ウォン以下の罰金に処する。<改正 1995.12.29>

②コンピュータなど情報処理装置又は電磁記録など特殊媒体記録を損壊したり、情報処理装置に虚偽の情報又は不正な命令を入力したり、その他方法で情報処理に障害を発生させて人の業務を妨害した者も、第 1 項の刑と同じである。<新設 1995.12.29>

**第 316 条 秘密侵害**

①封緘その他の秘密装置をした、人の手紙、文書、はたは図画を開封した者は、3 年以下の懲役、禁錮又は 500 万ウォン以下の罰金に処する。<改正 1995.12.29>

②封緘その他の秘密装置をした、人の便紙、文書、図画又は電磁記録など特殊媒体記録を、技術的な手段を利用して、その内容を知った者も、第 1 項の刑と同じである。<新設 1995.12.29>

**第 329 条 窃盗**

他人の財物を窃取した者は、6 年以下の懲役又は 1 千万ウォン以下の罰金に処する。<改正 1995.12.29>

**第 347 条 詐欺**

第 347 条の 2 (コンピュータなど使用詐欺)

コンピュータなど情報処理装置に虚偽の情報又は不正な命令を入力したり、権限なしで情報を入力・変更して、情報処理をすることによって財産上の利益を取得したり、第三者に取得させるようにした者は、10 年以下の懲役又は 2 千万ウォン以下の罰金に処する。[全文改正 2001.12.29]

**第 366 条 財物損壊など**

他人の財物、文書又は電磁記録など特殊媒体記録を、損壊又は隠匿、その他の方法でその効用を害した者は、3 年以下の懲役又は 700 万ウォン以下の罰金に処する。<改正 1995.12.29>

### （２）国家情報化基本法（旧　情報化促進基本法）

○関連する条項の抜粋訳（仮訳）

**第 37 条　情報保護施策の用意**

①国家機関と地方自治体は、情報を処理するすべての過程において、情報の安全な流通のための情報保護の施策を用意しなければならない。

②政府は、暗号技術の開発と利用を促進し、暗号技術を利用して情報通信サービスの安全を図る措置を用意しなければならない。

**第 38 条　情報保護システムに関する基準告示など**

①行政安全部長官は、関係機関の長と協議して、情報保護システムの性能と信頼度に関する基準を定めて告示し、情報保護システムを製造、又は輸入する者にその基準を守ることを勧告することができる。

②行政安全部長官は、流通中である情報保護システムが第 1 項にともなう基準に達してない場合に、情報保護システムの補完及びその他必要な事項を勧告することができる。

③第 1 項にともなう基準を定めるための手続きと第 2 項にともなう勧告に関する事項及びその他に必要な事項は大統領令に定める。

**第 39 条　個人情報保護施策の用意**

国家機関と地方自治体は、国家情報化を推進するにあたり、人間の尊厳と価値が保障されるように個人情報保護のための施策を用意しなければならない。

### （３）情報通信基盤保護法

○関連する条項の抜粋訳（仮訳）

**第 2 条　定義**

この法で使われている用語の定義は次のようである。<改正 2007.12.21>

1.「情報通信基盤施設」とは、国家安全保障・行政・国防・治安・金融・通信・運送・エネルギーなどの業務と関連した電子的制御・管理システム及び「情報通信網利用促進及び情報保護などに関する法律」第 2 条第 1 項第 1 号の規定による情報通信網をいう。(「情報通信網」とは、「電気通信基本法」第 2 条第 2 号にともなう電気通信設備を利用したり、電気

通信設備とコンピュータ及びコンピュータの利用技術を活用して、情報を収集・加工・保存・検索・送信又は受信する情報通信体制をいう。)
2.「電子的侵害行為」とは、情報通信基盤施設を対象に、ハッキング、コンピュータ・ウイルス、論理・メール爆弾、サービス拒否又は高出力電磁気波などによって、情報通信基盤施設を攻撃する行為をいう。
3.「侵害事故」とは、電子的侵害行為によって発生した事態をいう。

**第 12 条　主要情報通信基盤施設への侵害行為などの禁止**
誰でも次の各号の 1 に該当する行為をしてはならない。
1.アクセス権限を持たない者が、主要情報通信基盤施設に寄りついたり、アクセス権限を持った者が、その権限を超えて保存されたデータを操作・破壊・隠匿又は流出する行為
2.主要情報通信基盤施設に対し、データを破壊したり主要情報通信基盤施設の運営を邪魔する目的でコンピュータ・ウイルス・論理爆弾などのプログラムを投じる行為
3.主要情報通信基盤施設の運営を邪魔する目的で、一時に大量の信号を送ったり不正な命令を処理するなどの方法で情報処理に誤りを発生させようとする行為

**第 28 条　罰則**
①第 12 条の規定に違反して、主要情報通信基盤施設を撹乱・麻痺又は破壊した者は、10 年以下の懲役又は 1 億ウォン以下の罰金に処する。
②第 1 項の未遂犯は処罰する。

### （４）通信秘密保護法

○関連する条項の抜粋訳（仮訳）

**第 2 条　定義**
この法で使う用語の定義は次のようである。<改正 2005.1.27>
1.「通信」とは、郵便物及び電気通信をいう。
3.「電気通信」とは、電話・電子メール・会員制情報サービス・模写電送・無線呼び出し等と同様に、有無線・光線及びその他の電子的方式によって、すべての種類の音響・文言・符号又は映像を送信したり受信することをいう。
8.「監聴（傍受）設備」とは、対話又は電気通信の監聴（傍受）に使われる電子装置・機械装置その他設備をいう。　ただし、電気通信機器・機構又はその部品として一般的に使われるもの及び聴覚校正のための補聴器、又はこれと類似の用途で一般的に使われるもの中で、大統領令が決めるものを除く。

10.「会員制情報サービス」とは、特定の会員や契約者に提供する情報サービス、又はそのようなネットワークの方式をいう。
11.「通信事実確認資料」とは、次の各目のいずれか一つに該当する電気通信事実に関する資料をいう。
ア.加入者の電気通信の日時
イ.電気通信の開始・終了時間
オ.コンピュータ通信、又はインターネットの使用者が電気通信役務を利用した事実に関するコンピュータ通信、又はインターネットのログ記録の資料
カ.情報通信網に接続された情報通信機器の位置を確認できる発信機支局の位置追跡資料
キ.コンピュータ通信又はインターネットの使用者が情報通信網に接続するために使う情報通信機器の位置を確認できる接続地の追跡資料

**第 3 条　通信及び対話秘密の保護**

①誰でもこの法と刑事訴訟法又は軍事裁判法の規定によらなくては郵便物の検閲・電気通信の監聴（傍受)、又は通信事実確認資料の提供をしたり、公開されない他人間の対話を録音又は聴取することができない。ただし、次の各号の場合には、当該の法律が決めることに従う。<改正 2009.11.2>
②郵便物の検閲、又は電気通信の監聴（傍受）(以下「通信制限措置」という)は、犯罪捜査又は国家安全保障のために補充的な手段で利用されるべきで、国民の通信秘密に対する侵害が最小限に終わるように努力しなければならない。<新設 2001.12.29>

**第 5 条　犯罪捜査のための通信制限措置の許可要件**

①通信制限措置は、次の各号の犯罪を計画又は実行していたり実行したと疑うほどの十分な理由があって、他の方法ではその犯罪の実行を阻止したり犯人の逮捕又は証拠の収集が難しい場合に限って、許可することができる。<改正 2007.12.21>
－（詳細は省略）－；　(刑法上の一部犯罪)、(軍刑法上の一部犯罪)、(国家保安法に規定された犯罪)、(軍事機密保護法に規定された犯罪)、(麻薬類管理に関する法律で規定された犯罪中の一部)、(暴力行為などの処罰に関する法律で規定された犯罪中の一部)、(銃砲・刀剣・火薬類など取り締まり法に規定された犯罪中の一部)、(特定犯罪加重処罰などに関する法律で規定された犯罪中の一部)
②通信制限措置は、第 1 項の要件に該当する者が発送・受取したり、送・受信する特定の郵便物や電気通信、又はその該当者が一定の期間にわたって、発送・受取したり送・受信する郵便物や電気通信を対象に許可される。

**第 13 条　犯罪捜査のための通信事実確認資料提供の手続き<改正 2005.5.26>**

①検事又は司法警察官は、捜査又は刑の執行のために必要な場合、電気通信事業法による電気通信事業者(以下"電気通信事業者"という)に通信事実確認資料の閲覧や提出(以下"通信事実確認資料提供"という)を要請することができる。
②第 1 項の規定による通信事実確認資料提供を要請する場合には、要請理由、該当加入者との関連性及び必要な資料の範囲を記録した書面で、管轄地方裁判所(普通軍事裁判所を含む)、又は支所の許可を受けなければならない。ただし、管轄地方裁判所、又は支所の許可を受けられない緊急な理由がある時には、通信事実確認資料提供を要請した後、遅滞なくその許可を受けて電気通信事業者に送付しなければならない。<改正 2005.5.26>

**第 15 条の 2　電気通信事業者の協力義務**

①電気通信事業者は、検事・司法警察官又は情報捜査機関の長がこの法により執行する通信制限措置及び通信事実確認資料提供の要請に協力しなければならない。
②第 1 項の規定により通信制限措置の執行のために電気通信事業者が協力する事項、通信事実確認資料の保管期間、その他電気通信事業者の協力に関して必要な事項は、大統領令に定める。[本条新設 2005.5.26]

**第 16 条　罰則**

①次の各号の 1 に該当する者は 10 年以下の懲役と 5 年以下の資格停止に処する。
1.第 3 条の規定に違反して、郵便物の検閲又は電気通信の監聴（傍受）をしたり、公開されない他人間の対話を録音又は聴取した者
2.第 1 号の規定によって、知得した通信又は対話の内容を公開したり漏洩した者

**通信秘密保護法施行令（大統領令）**

**第 41 条　電気通信事業者の協力義務など**

①法第 15 条の 2 により、電気通信事業者は、殺人・人質強盗など個人の生命・身体に差し迫った危険が現存する場合には、通信制限措置、または通信事実確認資料の提供要請が遅滞なく行われるように協力しなければならない。
②法第 15 条の 2 第 2 項にともなう電気通信事業者の通信事実確認資料の保管期間は次の各号の区分に従う期間以上とする。
1.法第 2 条第 11 号ア目からカ目まで、およびク目で定めた通信事実確認資料：　12 カ月.
　ただし,市外・市内電話の役務と関連した資料の場合には 6 カ月とする。
2.法第 2 条第 11 号オ目、およびキ目で定めた通信事実確認資料：　3 カ月

### （５）情報通信網利用促進及び情報保護などに関する法律

○関連する条項の抜粋訳（仮訳）

**第 4 条　情報通信網利用促進及び情報保護などに関する施策の用意**

①行政安全部長官、知識経済部長官、又は放送通信委員会は、情報通信網の利用促進及び安定的管理・運営と利用者の個人情報保護など(以下「情報通信網利用促進及び情報保護など」という)を通じて、情報社会の基盤を作るための施策を用意しなければならない。

②第 1 項にともなう施策には次の各号の事項が含まれなければならない。

6.情報通信網を通して、収集・処理・保管・利用される個人情報の保護及びそれと関連した技術の開発・普及

**第 22 条　個人情報の収集・利用同意など**

①情報通信サービス提供者は、利用者の個人情報を利用しようとして収集する場合には、次の各号のすべての事項を利用者に知らせて同意を受けなければならない。

次の各号のいずれか一つの事項を変更しようとする場合にもまた同じである。

1.個人情報の収集・利用目的

2.収集する個人情報の項目

3.個人情報の保有・利用期間

②情報通信サービス提供者は、次の各号のいずれか一つに該当する場合には第 1 項にともなう同意なしで利用者の個人情報を収集・利用することができる。

1.情報通信サービスの提供に関する契約を履行するために必要な個人情報として経済的･技術的な理由で通常の同意を受けるのが明確に困難な場合

2.情報通信サービスの提供にともなう料金精算のために必要な場合

3.この法、又は他の法律で特別な規定がある場合　[全文改正 2008.6.13]

**第 23 条　個人情報の収集制限など**

①情報通信サービス提供者は、思想、信念、過去の病歴など、個人の権利・利益や私生活を明確に侵害する恐れがある個人情報を収集してはならない。ただし、第 22 条第 1 項にともなう利用者の同意を受けたり、他の法律により特別な収集対象の個人情報として許された場合には、その個人情報を収集することができる。

②情報通信サービス提供者は、利用者の個人情報を収集する場合には情報通信サービスの提供のために必要な最小限の情報を収集するべきで、必要最小限の情報以外の個人情報を提供しないという理由でそのサービスの提供を拒否してはならない。[全文改正 2008.6.13]

**第 23 条の 2　住民登録番号以外による会員加入方法**

①情報通信サービス提供者として提供する情報通信サービスの類型別の一日平均利用者数が大統領令に定める基準に該当する者は、利用者が情報通信網を通して会員に加入する場合に、住民登録番号を使わなくて会員に加入できる方法を提供しなければならない。
②第 1 項に該当する情報通信サービス提供者は、住民登録番号を使う会員加入方法を別途提供して、利用者が会員加入方法を選択するようにすることができる。[本条新設 2008.6.13]

**第 24 条　個人情報の利用制限**

情報通信サービス提供者は第 22 条及び第 23 条第 1 項のただし書きにより収集した個人情報を、利用者から同意受けた目的や第 22 条第 2 項各号で定めた目的と異なる目的で利用してはならない。[全文改正 2008.6.13]

**第 24 条の 2　個人情報の提供への同意など**

①情報通信サービス提供者は、利用者の個人情報を第三者に提供しようとする場合、第 22 条第 2 項第 2 号及び第 3 号に該当する場合他には、次の各号のすべての事項を利用者に知らせて同意を受けなければならない。
次の各号のいずれか一つの事項が変更される場合にもまた同じである。
1.個人情報の提供を受ける者
2.個人情報の提供を受ける者の個人情報の利用目的
3.提供する個人情報の項目
4.個人情報の提供を受ける者の個人情報保有及び利用の期間
②第 1 項により情報通信サービス提供者から利用者の個人情報の提供を受ける者は、その利用者の同意があるか、他の法律に特別な規定がある場合の他に、個人情報を第三者に提供したり、目的以外の用途で利用してはならない。　[全文改正 2008.6.13]

**第 27 条の 2　個人情報取り扱い方針の公開**

①情報通信サービス提供者などは、利用者の個人情報を取り扱う場合、個人情報取り扱い方針を定め、利用者がいつでも簡単に確認できるように大統領令に定める方法により公開しなければならない。
②第 1 項にともなう個人情報取り扱い方針には、次の各号の事項が全て含まれなければならない。
1.個人情報の収集・利用目的、収集する個人情報の項目及び収集方法
2.個人情報を第三者に提供する場合、提供を受ける者の姓名(法人の場合には法人の名称)、提供を受ける者の利用目的と提供される個人情報の項目
3.個人情報の保有及び利用期間、個人情報の破棄手続き及び破棄方法(第 29 条各号以外の部分のただし書きにより個人情報を保存しなければならない場合には、その保存根拠と保存する個人情報項目を含む)

4.個人情報取り扱いの委託をする業務の内容及び受託者(該当する場合のみ、取り扱い方針に含む)
5.利用者及び法定代理人の権利とその行事方法
6.インターネット接続情報ファイルなど個人情報を自動で収集する装置の設置・運営及びその拒否に関する事項
7.個人情報管理責任者の姓名又は個人情報保護業務及び関連の苦情事項を処理する部署の名称と、その電話番号などの連絡先
③情報通信サービス提供者などは、第 1 項にともなう個人情報取り扱い方針を変更する場合には、その理由及び変更内容を大統領令に定める方法により遅滞なしで公示し、利用者がいつでも変更された事項を簡単に調べてみられるように措置しなければならない。 [全文改正 2008.6.13]

**第 28 条　個人情報の保護措置**

①情報通信サービス提供者などが個人情報を取り扱う時には、個人情報の紛失・盗難・漏洩・変造、又は毀損を防止するために、大統領令に定める基準により次の各号の技術的・管理的な措置を取らなければならない。
1.個人情報を安全に取り扱うための内部管理計画の樹立・施行
2.個人情報に対する不法なアクセスを遮断するための侵入遮断システムなどアクセス統制装置の設置・運営
3.接続記録の偽造・変造防止のための措置
4.個人情報を安全に保存・送信できる、暗号化技術などを利用したセキュリティ措置
5.ワクチンソフトウェアの設置・運営などコンピュータ・ウイルスによる侵害防止措置
6.その他、個人情報の安全性確保のために必要な保護措置
②情報通信サービス提供者などは、利用者の個人情報を取り扱う者を最小限に制限しなければならない。[全文改正 2008.6.13]

**第 28 条の 2　個人情報の漏洩禁止**

①利用者の個人情報を取り扱っているか、取り扱ったことがある者は、職務上で知った個人情報を毀損・侵害又は漏洩してはならない。
②誰でもその個人情報が漏洩した事を知りながら、営利又は不正な目的で個人情報の提供を受けてはならない。[全文改正 2008.6.13]

**第 44 条の 7　不法情報の流通禁止など**

①誰でも情報通信網を通して、次の各号のいずれか一つに該当する情報を流通してはならない。
4.正当な理由なしで情報通信システム、データ、又はプログラムなどを毀損・滅失・変更・

偽造したり、その運用を妨害する内容の情報

**第 45 条　情報通信網の安全性確保など**

①情報通信サービス提供者は、情報通信サービスの提供に使われる情報通信網の安全性及び情報の信頼性を確保するための保護措置を取らなければならない。

②放送通信委員会は、第 1 項にともなう保護措置の具体的内容を定めた情報保護措置及び安全診断の方法・手続き・手数料に関する指針(以下“情報保護指針”という)を決めて告示し、情報通信サービス提供者にこれを守るように勧告することができる。

③情報保護指針には次の各号の事項が含まれなければならない。

1.正当な権限がない者が情報通信網にアクセス･侵入するのを防止して対応するための情報保護システムの設置・運営など技術的・物理的な保護措置

2.情報の不法流出・変造・削除などを防止するための技術的な保護措置

3.情報通信網の持続的な利用が可能な状態を確保するための技術的・物理的な保護措置

**第 46 条の 3　情報保護安全診断**

①次の各号のいずれか一つに該当する者は、放送通信委員会が認めた、安全診断を遂行することができる者(以下"安全診断遂行機関"という)から、自身の情報通信網又は集積情報通信施設に対して、毎年情報保護指針にともなう情報保護安全診断を受けなければならない。この場合、安全診断遂行機関は 15 人以上の情報保護技術人材を保有して最近 3 年以内に情報保護コンサルティングを遂行した実績がある法人でなければならない。<改正 2010.3.22>

**第 47 条の 3　利用者の情報保護**

①政府は、利用者の情報保護に必要な基準を定めて利用者に勧告し、侵害事故の予防及び拡散防止のために、脆弱性の点検、技術支援など必要な措置を取ることができる。

②主要情報通信サービス提供者は、情報通信網に重大な侵害事故が発生して自分のサービスを利用する利用者の情報システム、又は情報通信網などに深刻な障害が発生する可能性があれば、利用約款に定めるところにより、その利用者に保護措置を取るように要請し、これを履行しない場合には、該当情報通信網での接続を一時的に制限することができる。

③「ソフトウェア産業振興法」第 2 条にともなうソフトウェア事業者は、セキュリティに関する脆弱性を補完するプログラムを製作した時には、韓国インターネット振興院に知らせなければならなく、またそのソフトウェア使用者には、製作した日から 1 ケ月以内に 2 回以上知らせなければならない。　<改正 2009.4.22>

④第 2 項にともなう保護措置の要請などに関して、利用約款に定めなければならない具体的な事項は大統領令に定める。　[全文改正 2008.6.13]

**第 48 条　情報通信網侵害行為などの禁止**

①誰でも正当なアクセス権限なしで、又は許されたアクセス権限を越えて情報通信網に侵

入してはならない。
②誰でも正当な理由なしで、情報通信システム、データ又はプログラムなどを毀損・滅失・変更・偽造したり、その運用を妨害できるプログラム(以下“悪性プログラム”という)を伝達又は流布してはならない。
③誰でも情報通信網の安定的運営を妨害する目的で大量の信号、又はデータを送ったり、不正な命令を処理するようにするなどの方法で情報通信網に障害を発生させようとしてはならない。[全文改正 2008.6.13]

**第 48 条の 3　侵害事故の通報など**

①次の各号のいずれか一つに該当する者は、侵害事故が発生すれば直ちにその事実を放送通信委員会や韓国インターネット振興院に通報しなければならない。この場合「情報通信基盤保護法」第 13 条第 1 項にともなう通知があれば前段にしたがう通報として見なされる。<改正 2009.4.22>
1.情報通信サービス提供者
2.集積情報通信施設事業者
②放送通信委員会や韓国インターネット振興院は、第 1 項により侵害事故の通報を受けたり、侵害事故を知るようになれば、第 48 条の 2 第 1 項各号にともなう必要な措置を取らなければならない。<改正 2009.4.22>　[全文改正 2008.6.13]

**第 48 条の 4　侵害事故の原因分析など**

①情報通信サービス提供者など情報通信網を運営する者は、侵害事故が発生すれば侵害事故の原因を分析して被害の拡散を防止しなければならない。
②放送通信委員会は、情報通信サービス提供者の情報通信網に重大な侵害事故が発生すれば被害拡散防止、事故対応、復旧及び再発防止のためで、情報保護に専門性を揃えた民・官合同調査団を構成して、その侵害事故の原因分析することができる。
③放送通信委員会は､第 2 項にともなう侵害事故の原因を分析するために必要と認めれば、情報通信サービス提供者と集積情報通信施設事業者に情報通信網の接続記録などの関連資料の保全を命じられる。
④放送通信委員会は、侵害事故の原因を分析するために必要ならば、情報通信サービス提供者と集積情報通信施設事業者に侵害事故関連資料の提出を要求できて、第 2 項にともなう民・官合同調査団に、関係する事業場に出入して侵害事故原因を調べるようにすることができる。ただし、「通信秘密保護法」第 2 条第 11 号にともなう通信事実確認資料に該当する資料の提出はその法の定めに従う。
⑤放送通信委員会や民・官合同調査団は、第 4 項により提出させた資料と調査を通して知るようになった情報を侵害事故の原因分析及び対策用意以外の目的では使用できなくて、原因分析が終わった後には直ちに破棄しなければならない。

⑥第 2 項にともなう民・官合同調査団の構成と第 4 項により提出された侵害事故関連資料の保護などに必要な事項は大統領令に定める。[全文改正 2008.6.13]

**第 49 条　秘密などの保護**

誰でも情報通信網によって、処理・保管又は転送される他人の情報を傷つけたり他人の秘密を侵害・盗用又は漏洩してはならない。

[全文改正 2008.6.13]

**第 49 条の 2　騙す行為による個人情報の収集禁止など**

①誰でも情報通信網を通して騙す行為で他の人の情報を収集したり、他の人が情報を提供するように誘引してはならない。

②情報通信サービス提供者は、第 1 項を違反した事実を発見すれば直ちに放送通信委員会や韓国インターネット振興院に通報しなければならない。<改正 2009.4.22>

③放送通信委員会や韓国インターネット振興院は第 2 項にともなう通報を受けたり、第 1 項を違反した事実を知るようになれば、次の各号の必要な措置を取らなければならない。<改正 2009.4.22>

1.違反事実に関する情報の収集・伝播

2.類似する被害に対する予報・警報

3.情報通信サービス提供者に対する接続経路の遮断要請など被害拡散を防止するための緊急措置　[全文改正 2008.6.13]

**第 56 条　約款の申告など**

①通信課金サービス提供者は、通信課金サービスに関する約款を定めて、放送通信委員会に申告(変更申告を含む)しなければならない。<改正 2008.2.29>

②放送通信委員会は第 1 項にともなう約款が、通信課金サービス利用者の利益を侵害する恐れがあると判断される場合には通信課金サービス提供者に約款の変更を勧告することができる。　<改正 2008.2.29>

[本条新設 2007.12.21]

**第 71 条　罰則**

次の各号のいずれか一つに該当する者は 5 年以下の懲役又は 5 千万ウォン以下の罰金に処する。

1.第 22 条第 1 項(第 67 条により準用される場合を含む)を違反して、利用者の同意を受けなくて個人情報を収集した者

2.第 23 条第 1 項(第 67 条により準用される場合を含む)を違反して、利用者の同意を受けなくて個人の権利・利益や私生活を明確に侵害する恐れがある個人情報を収集した者

3.第 24 条、第 24 条の 2 第 1 項及び第 2 項又は第 26 条第 3 項(第 67 条により準用される場合を含む)を違反して、個人情報を利用したり、第三者に提供した者及びその事情を知りながらも、営利又は不正な目的で個人情報の提供を受ける者
5.第 28 条の 2 第 1 項(第 67 条により準用される場合を含む)を違反して、利用者の個人情報を毀損・侵害又は漏洩した者
6.第 28 条の 2 第 2 項を違反して、その個人情報が漏洩した事情を知りながらも、営利又は不正な目的で個人情報の提供を受ける者
7.第 30 条第 5 項(第 30 条第 7 項、第 31 条第 3 項及び第 67 条により準用される場合を含む)を違反して、必要な措置をしなくて個人情報を提供したり利用した者
9.第 48 条第 2 項を違反して、悪性プログラムを伝達又は流布した者
10.第 48 条第 3 項を違反して、情報通信網に障害が発生させようとした者

**第 72 条　罰則**

①次の各号のいずれか一つに該当する者は 3 年以下の懲役又は 3 千万ウォン以下の罰金に処する。
1.第 48 条第 1 項を違反して、情報通信網に侵入した者
2.第 49 条の 2 第 1 項を違反して、他の人の個人情報を収集した者
②第 1 項第 1 号の未遂犯は処罰する。[全文改正 2008.6.13]

**第 73 条　罰則**

次の各号のいずれか一つに該当する者は、2 年以下の懲役又は 1 千万ウォン以下の罰金に処する。
1.第 28 条第 1 項第 2 号から第 5 号まで(第 67 条により準用される場合を含む)の規定にともなう技術的・管理的措置をしなくて利用者の個人情報を紛失・盗難・漏洩・変造又は傷つけた者
6.第 48 条の 4 第 3 項にともなう命令を違反して、関連資料を保全しない者
7.第 49 条の 2 第 1 項を違反して、個人情報の提供を誘引した者
[全文改正 2008.6.13]

**第 76 条　過怠料**

①次の各号のいずれか一つに該当する者と第 7 号から第 11 号までのケースに該当する行為をするようにした者には 3 千万ウォン以下の過怠料を賦課する。
1.第 23 条第 2 項(第 67 条により準用される場合を含む)を違反して、サービスの提供を拒否した者
2.第 23 条の 2 を違反して必要な措置をしない者
3.第 28 条第 1 項第 1 号及び第 6 号(第 67 条により準用される場合を含む)にともなう技術

的・管理的措置をしない者
②次の各号のいずれか一つに該当する者には 2 千万ウォン以下の過怠料を賦課する。
4.第 27 条の 2 第 1 項(第 67 条により準用される場合を含む)を違反して、個人情報取り扱い方針を公開しない者
③次の各号のいずれか一つに該当する者には 1 千万ウォン以下の過怠料を賦課する。 <改正 2009.4.22>
4.第 43 条を違反して、情報を保管しない者
6.第 46 条の 3 第 1 項を違反して、情報保護安全診断を受けない者
7.第 46 条の 3 第 2 項を違反して、情報保護安全診断の結果を提出しなかったり、偽りで提出した者
8.第 46 条の 3 第 5 項にともなう勧告内容、又は処理結果を偽りで通知した者
9.第 46 条の 3 第 6 項にともなう改善命令を履行しない者
10.第 47 条の 3 第 3 項を違反して、ソフトウェア使用者に知らせない者
11.第 48 条の 2 第 4 項にともなう是正命令を履行しない者
12.第 48 条の 4 第 4 項にともなう事業場出入及び調査を妨害したり、拒否又は忌避した者
15.第 56 条第 1 項を違反して、約款を申告しない者

### （６）住民登録法

○関連する条項の抜粋訳（仮訳）

**第 37 条　罰則**
次の各号のいずれかか一つに該当する者は、3 年以下の懲役又は 1 千万ウォン以下の罰金に処する。<改正 2009.4.1>
9.法律に従わずに営利の目的で他人の住民登録番号に関する情報を知らせる者
10.他の人の住民登録番号を不正に使用した者。 ただし、直系血族・配偶者・同居親族又はその配偶者の間には、被害者が明示した意思に反して、控訴を提起することができない。

### （７）電子取引基本法

○関連する条項の抜粋訳（仮訳）

**第 2 条　定義**
この法で使う用語の定義は次の通りである。<改正 2005.3.31>

1.「電子文書」とは、情報処理システムによって電子的な形態で作成、送信・受信又は保存された情報をいう。
2.「情報処理システム」とは、電子文の作成、送信・受信又は保存のために利用される情報処理能力を持った電子的装置又は体系をいう。
5.「電子取引」とは、財貨や用役（サービス）を取引することにおいてその全部又は一部が電子文書によって処理される取引をいう。
8.「公認電子文書保管所」とは、第 31 条の 2 第 1 項の規定により指定を受けて、他人のために電子文書を保管又は証明したり、その他電子文書と関連した業務(以下"電子文書保管など"という)を遂行する法人をいう。

**第 12 条　個人情報保護**

①政府は、電子取引の安全性及び信頼性を確保するために、電子取引利用者の個人情報を保護するための施策を樹立・施行しなければならない。
②電子取引会社業者は、電子取引利用者の個人情報を収集・利用・提供及び管理することにおいて「情報通信網利用促進及び情報保護などに関する法律」など関連規定を遵守しなければならない。<改正 2007.5.17>

**第 13 条　営業秘密保護**

①政府は、電子取引の安全性及び信頼性を確保するために電子取引利用者の営業秘密を保護するための施策を樹立して施行しなければならない。
②電子取引会社業者(情報処理システムの運営を委託受けた者を含む)は、電子取引利用者の営業秘密を保護するための措置を講じなければならない。
③電子取引会社業者は、電子取引利用者の同意を得なくては当該の利用者の営業秘密を他人に提供したり漏洩してはならない。
④第 1 項ないし第 3 項の規定による営業秘密の範囲、保護措置などに関して必要な事項は大統領令に定める。

**第 31 条の 12　電子文書など関連情報のセキュリティ**

①誰も公認電子文書保管所に保管された電子文書その他の関連情報を偽造又は変造したり、偽造又は変造した情報を行使してはならない。
②誰も公認電子文書保管所の情報処理システムに偽り情報や不正な命令を入力するなどの方法で第 31 条の 7 第 2 項の規定による証明書が偽りで発給されるようにしてはならない。
③誰も公認電子文書保管所に保管された電子文書、その他の関連情報を滅失又は毀損したりその秘密を侵害してはならない。

**第 43 条　罰則**

①次の各号のいずれか一つに該当する者は10年以下の懲役又は1億ウォン以下の罰金に処する。<改正 2007.5.17>

1.第 31 条の 12 第 1 項を違反して、公認電子文書保管所に保管された電子文書、その他の関連情報を偽造又は変造したり、偽造又は変造した情報を行使した者

2.第 31 条の 12 第 2 項を違反して、公認電子文書保管所の情報処理システムに偽り情報や不正な命令を入力するなどの方法で第31条の7第2項の規定による証明書が偽りで発給されるようにした者

②第1項の未遂犯は処罰する。 [本条新設 2005.3.31]

**第 44 条 罰則**

次の各号のいずれか一つに該当する者は 5 年以下の懲役又は 5 千万ウォン以下の罰金に処する。<改正 2007.5.17>

1.第 31 条の 12 第 3 項を違反して、公認電子文書保管所に保管された電子文書、その他の関連情報を滅失又は毀損したたり、その秘密を侵害した者

### （８）電子政府法

○関連する条項の抜粋訳（仮訳）

**第 2 条　定義**

この法で使う用語の意は次のようである。

6.「行政情報」とは、行政機関などが職務上作成したり取得して、管理している資料として電子的方式で処理されて、符号、文字、音声、音響、映像などと表現されたことをいう。

**第 35 条　禁止行為**

誰でも行政情報を取り扱い・利用する時、次の各号の行為をしてはならない。

1.行政情報の処理業務を妨害する目的で行政情報を偽造・変更・毀損したり抹消する行為

2.行政情報共同利用のための情報システムを正当な理由なしで、偽造・変更・毀損したり利用する行為

3.行政情報を変更したり抹消する方法やプログラムを公開・流布する行為

5.行政情報を権限なしで処理したり、権限範囲を越えて、処理する行為

6.行政情報を権限なしで他の人に利用させるようにする行為

8.偽りやその他の不正な方法で行政機関などから行政情報を提供させたり、閲覧する行為

**第 76 条　罰則**

①第 35 条第 1 号を違反して、行政情報を偽造・変更・毀損したり抹消する行為をした者は 10 年以下の懲役に処する。

②次の各号のいずれか一つに該当する者は 5 年以下の懲役又は 5 千万ウォン以下の罰金に処する。

1.第 35 条第 2 号を違反して､行政情報共同利用のための情報システムを正当な理由なしで、偽造・変更・毀損したり利用した者

2.第 35 条第 3 号を違反して、行政情報を変更したり抹消する方法及びプログラムを公開・流布する行為をした者

③次の各号のいずれか一つに該当する者は 3 年以下の懲役又は 3 千万ウォン以下の罰金に処する。

2.第 35 条第 5 号を違反して、行政情報を権限なしで処理したり権限範囲を越えて、処理する行為をした者

3.第 35 条第 6 号を違反して、行政情報を権限なしで他の人に利用させるようにする行為をした者

④第 35 条第 8 号を違反して、偽りやその他の不正な方法で行政機関などから行政情報を提供させたり閲覧する行為をした者は 2 年以下の懲役又は 700 万ウォン以下の罰金に処する。

## （９）電子署名法

○関連する条項の抜粋訳（仮訳）

**第 23 条　電子署名生成情報の保護など**

①誰でも他人の電子署名生成情報を盗用又は漏洩してはならない。<改正 2001.12.31>

②誰でも他人の名義で公認証明書の発給を受けたり、発給を受けられるようにしてはならない。<改正 2001.12.31>

⑤誰でも行使する目的で他人に公認証明書を譲渡又は貸与したり、行使する目的で他の人の公認証明書を譲り受け、又は貸与を受けてはならない。<新設 2005.12.30>

**第 24 条　個人情報の保護**

①公認認証機関は、認証業務の遂行と関連して、個人情報を保護しなければならない。

②第 1 項の個人情報保護に関しては「情報通信網利用促進及び情報保護などに関する法律」第 22 条ないし第 32 条、第 36 条第 1 項、第 54 条、第 55 条、第 62 条、第 66 条及び第 67 条の個人情報に関する規定を準用する。この場合、"情報通信サービス提供者"は"公認認証機関"に、"利用者"は"加入者"とする。<改正 2005.12.30>

**第 31 条　罰則**

次の各号の 1 に該当する者は 3 年以下の懲役又は 3 千万ウォン以下の罰金に処する。<改正 2001.12.31>

2.第 23 条第 1 項の規定に違反して、他人の電子署名生成情報を盗用又は漏洩した者

3.第 23 条第 2 項の規定に違反して、他人の名義で公認証明書の発給を受けたり発給を受けられるようにした者

**第 32 条　罰則**

次の各号のいずれか一つに該当する者は 1 年以下の懲役又は 1 千万ウォン以下の罰金に処する。<改正 2005.12.30>

4.第 23 条第 5 項の規定に違反して、行使する目的で他人に公認証明書を譲渡又は貸与したり、行使する目的で他人の公認証明書を譲り受け、又は貸与を受けた者

## （１０）電子金融取引法

○関連する条項の抜粋訳（仮訳）

**第 2 条　定義**

1.「電子金融取引」とは。金融機関又は電子金融業者が電子的装置を通して、金融商品及びサービスを提供(以下「電子金融業務」という)と、利用者が金融機関又は電子金融業者の従事者と直接対面してのコミュニケーションをしなくて、自動化された方式でこれを利用する取引をいう。

10.「アクセス媒体」とは、電子金融取引において取引指示をしたり、利用者及び取引内容の真実性と正確性を確保するために使われる次に各項目のいずれか一つに該当する手段又は情報をいう。

ア、電子式カード及びこれに準ずる電子的情報

イ、「電子署名法」第 2 条第 4 号の電子署名の生成情報及び同組第 7 号の認証書

ウ、金融機関又は電子金融業者に登録された利用者番号

エ、利用者の生体情報

オ、ア又は、イの手段あるいは情報を使うために必要な暗証番号

**第 4 条　相互主義**

外国人又は外国法人に対しもこの法を適用する。ただし、大韓民国国民又は、大韓民国法人に対してこの法に準ずる保護をしない国家の外国人又は外国法人に対しては、それに相応して、この法又は大韓民国が加入したり、締結した条約にともなう保護を制限することができる。

**第 6 条　アクセス媒体の選定と使用及び管理**

③アクセス媒体は、他の法律に特に規定がない限り、譲渡し・譲受けたり質権を設定してはならない。ただし、第 18 条の規定にともなう先払い電子支給手段や電子貨幣の譲渡し又は担保提供のために必要な場合には、この限りでない。

**第 22 条　電子金融取引記録の生成及び保存**

①金融機関などは、電子金融取引の内容を追跡・検索したり、その内容に誤りがあった場合にこれを確認したり訂正できる記録を生成して、5 年の範囲の中で大統領令が決める期間の間保存しなければならない。

②第 1 項の規定により、金融機関などが保存しなければならない記録の種類及び保存方法は大統領令に定める。

**第 26 条　電子金融取引情報の提供など**

電子金融取引と関連した業務を遂行することにおいて、次の各号のいずれか一つに該当する事項を知るようになった者は、利用者の同意を得なくてこれを他人に提供・漏洩したり業務上目的の他に使ってはならない。ただし、「金融実名取引及び秘密保障に関する法律」第 4 条第 1 項のただし書きの規定にともなう場合、その他の法律で決める場合には、この限りでない。

1.利用者の個人的事項

2.利用者の口座、アクセス媒体及び電子金融取引の内容と実績に関する情報又は資料

**第 49 条　罰則**

①次の各号のいずれか一つに該当する者は、7 年以下の懲役又は 5 千万ウォン以下の罰金に処する。

1.アクセス媒体を偽造したり変造した者

2.偽造されたり変調したアクセス媒体を販売斡旋・販売・輸出又は輸入したり使用する者

3.紛失又は盗難されたアクセス媒体を販売斡旋・販売・輸出又は輸入したり使用する者

4.電子金融取引のための電子的装置又は、「情報通信網利用促進及び情報保護などに関する法律」第 2 条第 1 項第 1 号の規定にともなう情報通信網に侵入して、虚偽その他の不正な方法でアクセス媒体を獲得したり獲得されたアクセス媒体を利用して、電子金融取引をした者

5.強制的に奪ったり、横領したり、人をだましたり恐喝して、獲得したアクセス媒体を販売斡旋・販売・輸出又は輸入したり使用した者

③第 26 条の規定に違反して、電子金融取引情報を提供したり、漏洩したり、業務上目的の以外に使った者(第 28 条第 4 項の規定によりこれを準用する先払い電子支給手段を発行する者を含む)は、5 年以下の懲役又は 3 千万ウォン以下の罰金に処する。

⑤次の各号のいずれか一つに該当する者は 1 年以下の懲役又は 1 千万ウォン以下の罰金に処する。

1.第 6 条第 3 項の規定に違反して、アクセス媒体を譲渡し・譲受けたり、質権を設定した者

**第 51 条　過怠料**

①次の各号のいずれか一つに該当する者(第 1 号、第 3 号、第 4 号、第 5 号及び第 6 号の場合には、第 28 条第 4 項の規定によりこれを準用する先払い電子支給手段を発行する者を含む)は 1 千万ウォン以下の過怠料に処する。

3.第 22 条第 1 項(第 29 条第 2 項で準用する場合を含む)の規定に違反して、記録を生成したり保存しない者

## （１１）電子商取引等における消費者保護に関する法律

○関連する条項の抜粋訳（仮訳）

**第 6 条　取引記録の保存など**

①事業者は、電子商取引及び通信販売での表示・広告、契約内容及びその履行など取引に関する記録を相当な期間保存しなければならない。この場合、消費者が簡単に取引記録を閲覧・保存できる方法を提供しなければならない。

③第 1 項の規定によって、事業者が保存する取引記録の対象・範囲・期間及び消費者に提供する閲覧・保存の方法などに関して必要な事項は大統領令に定める。

**第 21 条　禁止行為**

①電子商取引を行う事業者、又は通信販売業者は次の各号の 1 に該当する行為をしてはならない。　<改正 2005.3.31>

・・・

6.本人の同意なしに、又は同意を得た範囲を越えて、消費者に関する情報を利用する行為. ただし、次の各目の 1 に該当する場合を除く。

ア.財貨などの配送等で消費者との契約の履行に避けられない場合として大統領令が決める場合

イ.財貨などの取引にともなう代金精算のために必要な場合

ウ.盗用防止のためで、本人確認に必要な場合として大統領令が決める場合

エ.法律の規定又は法律によって必要な避けられない理由がある場合

**第 45 条　過怠料**

②次の各号の 1 に該当する者は 500 万ウォン以下の過怠料に処する。<改正 2005.3.31>

1.第 6 条の規定に違反して、取引記録を保存しなかったり、消費者に記録保存及び閲覧の方法を提供しない者

## （１２）電子貿易促進に関する法律

○関連する条項の抜粋訳（仮訳）

**第 20 条　電子貿易文書及び貿易情報に関するセキュリティ**

①誰も電子貿易基盤事業者、第 22 条の規定による電子貿易専門サービス業者、貿易業者と

貿易関連機関のコンピュータ・ファイルに記録された電子貿易文書、又はデータベースに入力された貿易情報を偽造又は変造したり、偽造又は変造した電子貿易文書又は貿易情報を行使してはならない
②誰でも電子貿易基盤事業者のコンピュータなど情報処理装置に、偽り情報又は不正な命令を入力して、情報処理ができるようにするなどの方法で、第 17 条第 1 項の証明書を発給しようとしてはならない
③誰でも電子貿易基盤事業者、第 22 条の規定による電子貿易専門サービス業者、貿易業者と貿易関連機関のコンピュータ・ファイルに記録された電子貿易文書又はデータベースに入力された貿易情報を毀損したり、その秘密を侵害してはならない

**第 30 条　罰則**
①次の各号のいずれか一つに該当する者は、1 年以上 10 年以下の懲役、又は 1 億ウォン以下の罰金に処する。
1.第 20 条第 1 項の規定に違反して、電子貿易基盤事業者、電子貿易専門サービス業者、貿易業者、貿易関連機関のコンピュータ・ファイルに記録された電子貿易文書又はデータベースに入力された貿易情報を偽造又は変造したり、偽造又は変造した電子貿易文書又は貿易情報を行使した者
2.第 20 条第 2 項の規定に違反して、電子貿易基盤事業者のコンピュータなど情報処理装置に偽り情報又は不正な命令を入力して、情報処理を行うなどの方法で第 17 条第 1 項の証明書が発給されるようにした者
②第 1 項の未遂犯は処罰する。

### （１３）信用情報の利用及び保護に関する法律

○関連する条項の抜粋訳（仮訳）

**第 2 条　定義**
この法で使われている用語の意味は次のようである。
1.「信用情報」とは、金融取引など商取引において、取引相手方の信用度と信用取引能力などを判断する際に必要な情報として大統領令に定める情報をいう。
2.「個人信用情報」とは、信用情報の中で、個人の信用度と信用取引能力などを判断する際に必要な情報として大統領令に定める情報をいう。
3.「信用情報主体」とは、処理された信用情報で識別される者として、その信用情報の主体になる者をいう。
4.「信用情報業」とは、第 4 条第 1 項各号にともなう業務の全部又は一部を業とすることを

いう。
5.「信用情報会社」とは、信用情報業をする目的で第 4 条により金融委員会の許可を受けた者をいう。
6.「信用情報集中機関」という信用情報を集中して、管理・活用する者として第 25 条第 1 項により金融委員会に登録した者をいう。
7.「信用情報提供・利用者」とは、顧客との金融取引など商取引のために、本人の営業に関連して得たり作り出した信用情報を他人に提供したり、他人から信用情報をされて本人の営業に利用する者と、その他にこれに準ずる者として大統領令に定める者をいう。
8.「信用照会業務」とは、信用情報を収集・処理する行為、信用情報主体の信用度・信用取引能力などを現わす信用情報を作り出す行為、及び依頼人の照会により信用情報を提供する行為をいう。
9.「信用調査業務」とは、他人の依頼を受けて、信用情報を調べて、その信用情報をその依頼人に提供する行為をいう。

**第 19 条　信用情報電算システムの安全保護**

①信用情報会社等は、信用情報電算システム(第 25 条第 6 項にともなう信用情報共同電算網を含む)に対する第三者からの不正なアクセス、入力された情報の変更・毀損及び破壊、その他の危険に対して大統領令に定めるところにより技術的・物理的・管理的セキュリティ対策をとらなければならない。

**第 20 条　信用情報管理責任の明確化及び業務処理記録の保存**

①信用情報会社などは、信用情報の収集・処理及び利用などに対して金融委員会が決めるところにより内部管理規定を用意しなければならない。
②信用情報会社などは、次の各号の事項に対する記録を 3 年間保存しなければならない。
1.依頼人の住所と声明又は情報提供・交換機観の住所と名前
2.依頼受けた業務内容及び依頼受けた日
3.依頼受けた業務の処理内容又は提供した信用情報の内容と提供した日
4.その他に大統領令に定める事項

**第 24 条　住民登録電算情報資料の利用**

①信用情報集中機関及び大統領令に定める信用情報提供・利用者は、次の各号のいずれか一つに該当する場合には、行政安全部長官に「住民登録法」第 30 条第 1 項にともなう住民登録電算情報資料の提供を要請することができる。この場合要請を受けた行政安全部長官は特別な理由がなければその要請に従わなければならない。
1.「商法」第 64 条など他の法律により消滅時効が完了された預金及び保険金などの支給のための場合として、該当預金及び保険金などの元の権利者に関連事項を知らせるための場

合
2.金融取引契約の満期到来、失効、解約など、契約の変更理由の発生など、取引相手方の権利・義務に影響を及ぼす事項を知らせるための場合
②第 1 項により住民登録電算情報資料を要請する場合には金融委員会委員長の審査を受けなければならない。
③第 2 項により金融委員会委員長の審査を受けた場合には「住民登録法」第 30 条第 1 項にともなう関係中央行政機関の長の審査を経たとみなす。処理手続き、使用料又は手数料などに関する事項は「住民登録法」に従う。

**第 32 条　個人信用情報の提供・活用に対する同意**
①信用情報提供・利用者が貸し出し、保証に関する情報など大統領令に定める個人信用情報を他人に提供しようとする場合には、大統領令に定めるところにより該当個人から次の各号のいずれか一つに該当する方式であらかじめ同意を受けなければならない。

**第 33 条　個人信用情報の利用**
個人信用情報は該当信用情報主体が申請した金融取引など商取引関係（雇用関係は除く。以下同様である)の設定、及び維持有無などを判断するための目的にのみ利用しなければならない。ただし、次の各号のいずれか一つに該当する場合にはこの限りでない。

**第 34 条　個人識別情報の提供・利用**
①信用情報提供・利用者が個人を識別するために必要とする情報として大統領令に定める情報(以下"個人識別情報"という)を、信用情報会社などに提供しようとする場合には該当個人の同意を受けなければならない。
②個人識別情報は、該当個人が同意した目的又は、該当個人から直接提供された場合にはその提供の目的範囲内でのみ利用されなければならない。

**第 35 条　信用情報提供事実の通知要求**
信用情報主体は、信用情報会社などが本人に関する信用情報(以下"本人情報"という)を提供する場合大統領令に定めるところにより提供を受けた者、その利用目的、提供した日、提供した本人情報の主要内容などを知らせるように要求したり、インターネット ホームページを通して問い合わせできることを要求することができる。この場合、信用情報会社などは特別な理由がなければその要求に従わなければならない

**第 42 条　業務目的外の漏洩禁止など**
①信用情報会社などと、第 17 条第 2 項により信用情報の処理を委託受けた会社の役職員又は役職員だった者(以下"信用情報業関連者"という)は、業務上知った他人の信用情報及び私

生活など個人的な秘密(以下"個人秘密"という)を業務目的外に漏洩したり利用してはならない。
②信用情報会社などと信用情報業関連者が、この法により信用情報会社などに信用情報を提供する行為は、第 1 項にともなう業務目的以外の漏洩や利用と見なされない。
③第 1 項を違反して漏洩した個人秘密を取得した者(それから漏洩した個人秘密をまた取得した者を含む)は、その個人秘密が第 1 項を違反して漏洩したことを知るようになった場合、その個人秘密を他人に提供したり利用してはならない。
④信用情報会社などと信用情報業関連者から個人信用情報を提供された者は、その個人信用情報を他人に提供してはならない。ただし、この法又は他の法律により提供が許される場合にはこの限りでない。

**第 50 条　罰則**

①次の各号のいずれか一つに該当する者は 5 年以下の懲役又は 5 千万ウォン以下の罰金に処する。
4.第 32 条第 1 項又は第 2 項を違反した者
5.第 33 条を違反した者
6.第 42 条第 1 項・第 3 項又は第 4 項を違反した者
②次の各号のいずれか一つに該当する者は、3 年以下の懲役又は 3 千万ウォン以下の罰金に処する。
3.権限なしで第 19 条第 1 項にともなう信用情報電算システムの情報を変更・削除したり、その他の方法で利用できなくした者、又は権限なしで信用情報を検索・複製したり、その他の方法で利用した者
③次の各号のいずれか一つに該当する者は 1 年以下の懲役又は 1 千万ウォン以下の罰金に処する。
5.第 20 条第 2 項を違反した者

**第 52 条　過怠金**

③次の各号のいずれか一つに該当する者には、1 千万ウォン以下の過怠金を賦課する。
5.第 19 条を違反した者

**信用情報の利用及び保護に関する法律施行令(大統領令) [施行 2010.7.6]**

**第 29 条　個人識別情報の提供・利用**

法第 34 条第 1 項で"大統領令に定める情報"とは、生存する個人の声明、住所、住民登録番号、外国人登録番号、国内居所申告番号、旅券番号、性別、国籍など個人を識別できる情報をいう。

## （１４）物流政策基本法

○関連する条項の抜粋訳（仮訳）

**第 2 条　定義**

この法で使う用語の定義は次の通りである。

9.「総合物流情報網」とは、単位物流情報網を総合的に連係して構成した物流情報体系をいう。

第 33 条(電子文書及び物流情報のセキュリティ)

①誰も総合物流情報網又は第 32 条第 1 項の電子文書を偽作又は変作したり、偽作又は変作した電子文書を行使してはならない。

②誰も総合物流情報網又は国家物流統合データベースにより処理・保管又は転送される物流情報を毀損したり、その秘密を侵害・盗用又は漏洩してはならない。

③総合物流情報網事業者は、電子文書及び情報処理装置のファイルに記録されている物流情報を大統領令に定める期間の間保管しなければならない。

④総合物流情報網事業者は、又は国家物流統合データベース運営者は、第 1 項から第 3 項までの規定にともなう電子文書及び物流情報のセキュリティに必要な保護措置を講じなければならない。

⑤誰も不法又は不当な方法で第 4 項にともなう保護措置を侵害したり、毀損してはならない。

**第 71 条　罰則**

①第 33 条第 1 項を違反して,電子文書を偽作又は変作したり、その事情を知りながら、偽作又は変作した電子文書を行使した者は、10 年以下の懲役又は 2 億ウォン以下の罰金に処する。

この場合、未遂犯は本罪に準じて処罰する。

②第 33 条第 2 項を違反して,総合物流情報網又は国家物流統合データベースによって,処理・保管又は転送される物流情報を毀損したり、その秘密を侵害・盗用又は漏洩した者は、5 年以下の懲役又は 1 億ウォン以下の罰金に処する。

③第 33 条第 5 項を違反して、総合物流情報網又は国家物流統合データベースの保護措置を侵害したり、毀損し者は 3 年以下の懲役又は 5 千万ウォン以下の罰金に処する。

④次の各号のいずれか一つに該当する者は 1 年以下の懲役又は 3 千万ウォン以下の罰金に処する。

1.第 33 条第 3 項を違反して、電子文書又は物流情報を大統領令に定める期間の間保管しない者

## （１５）インターネットアドレス資源に関する法律

○関連する条項の抜粋訳（仮訳）

**第 15 条　個人情報の保護**

①インターネットアドレス管理機関などは、インターネットアドレス使用者の個人情報を保護しなければならない。

②第 1 項にともなう個人情報保護に関しては「情報通信網利用促進及び情報保護などに関する法律」第 22 条、第 23 条、・・・　－（省略)-　の個人情報に関する規定を準用する。この場合、"情報通信サービス提供者"は"インターネットアドレス管理機関など"で、"利用者"は"インターネットアドレスの使用者"と見なされる。　[全文改正 2009.6.9]

(*　この条項に対する罰則条項はない。)

## （１６）ゲーム産業振興に関する法律

○関連する条項の抜粋訳（仮訳）

**第 32 条　不法ゲーム物などの流通禁止など**

①誰でもゲーム物の流通秩序を阻害する次に各号の行為をしてはならない。ただし、第 4 号の場合「射倖行為など規制及び処罰特例法」により射倖行為営業をする者を除く。<改正 2007.1.19>

7.誰でもゲーム物の利用を通して、獲得した有・無形の結果(点数、景品、ゲーム内で使われる仮想の貨幣として大統領令で定めるゲームマネー及び大統領令で決めるこれと類似しているものをいう)を両替又は両替を斡旋したり再買入することを業とする行為。

第 44 条(罰則)

(1)次の各号のいずれか一つに該当する者は 5 年以下の懲役又は 5 千万ウォン以下の罰金に処する。　<改正 2007.1.19>

2.第 32 条第 1 項第 1 号・第 4 号又は第 7 号に該当する行為をした者

**ゲーム産業振興に関する法律施行令　(大統領令)**

**第 18 条の 3　ゲームマネーなど**

法第 32 条第 1 項第 7 号で「大統領令で定めるゲームマネー及び大統領令で決めるこれと類似しているもの」というとは、次の各号のいずれか一つに該当することをいう。

1.ゲーム物を利用する時、ベッティング（賭け）又は配当の手段になったり偶然的な方法で

獲得されたゲームマネー
2.第 1 号で決めるゲームマネーの代替交換対象になったゲームマネー、又はゲームアイテム(ゲームの進行のためにゲーム内で使われる道具をいう。以下同様)等のデータ
3.ゲーム製作業者のコンピュータ・プログラムを複製、改作、ハッキングなどをしたり、ゲーム物の非正常的な使い方を通じて、生産・獲得したゲームマネー又はゲームアイテムなどのデータ[本条新設 2007.5.16]

## （１７）位置情報の保護及び利用などに関する法律

○関連する条項の抜粋訳（仮訳）

**第 2 条　定義**
この法で使う用語の定義は次のようである。<改正 2010.3.22>
1.「位置情報」とは、移動性がある物又は個人が特定の時間に存在した場所に関する情報として「電気通信事業法」第 2 条第 2 号及び第 3 号にともなう電気通信設備及び電気通信回線設備を利用して収集されたものをいう。
2.「個人位置情報」とは、特定個人の位置情報(位置情報だけでは特定個人の位置を分からない場合にも他の情報と容易に結合して、特定個人の位置が分かるものを含む)をいう。
3.「個人位置情報主体」とは、個人位置情報によって、識別される者をいう。
4.「位置情報収集事実確認資料」とは、位置情報の収集要請人、収集日時及び収集方法に関する資料(位置情報を除く)をいう。
5.「位置情報利用・提供事実確認資料」とは、位置情報の提供を受ける者、取得経路、利用・提供日時及び利用・提供方法に関する資料(位置情報を除く)をいう。
6.「位置情報事業」とは、位置情報を収集して、位置基盤サービス事業者に提供するのを事業として営むことをいう。
7.「位置基盤サービス事業」とは、位置情報を利用したサービス(以下"位置基盤サービス"という)を提供するのを事業として営むことをいう。
8.「位置情報システム」とは、位置情報事業及び位置基盤サービス事業のために、「情報通信網利用促進及び情報保護などに関する法律」第 2 条第 1 項第 1 号の規定による情報通信網を通して、位置情報を収集・保存・分析・利用及び提供することができるように互いに有機的に関連したコンピュータのハードウェア、ソフトウェア、データベース及び人的資源の結合体をいう。

**第 12 条　利用約款の申告など**
①位置情報事業者及び位置基盤サービス事業者(以下"位置情報事業者など"という)は、提供

しようとする位置情報の収集、利用及び提供に関する料金、またその条件など(以下"利用約款"という)を決めて、放送通信委員会に申告しなければならない。これを変更しようとする時にもまた同じである。<改正 2008.2.29>
②放送通信委員会は、位置情報事業者などの利用約款が個人位置情報の保護、公正競争又は公共利益を侵害する恐れがあると判断される場合には位置情報事業者などに利用約款の変更を命じられる。<改正 2008.2.29>

**第 15 条　位置情報の収集などの禁止**
①誰でも個人又は所有者の同意を得なくて、該当の個人又は移動性がある物の位置情報を収集・利用又は提供してはならない。　ただし、第 29 条の規定による緊急救助機関の緊急救助又は警報発送の要請があったり、他の法律に特別な規定がある場合にはこの限りでない。
②誰でも他人の情報通信機器を複製したり、情報を盗用するなどの方法で位置情報事業者などをだまして、他人の個人位置情報を受け取ってはならない。
③位置情報を収集できる装置が付着した物を貸与する者は、位置情報収集装置が付着した事実を、その装置を借りる者に告知しなければならない。

**第 16 条　位置情報の保護措置など**
①位置情報事業者などは、位置情報の漏洩、変造、毀損などを防止するために位置情報の取り扱い・管理指針を制定したり、アクセス権限者を指定するなどの管理的措置とファイアウォールの設置や暗号化ソフトウェアの活用などの技術的措置を取らなければならない。この場合管理的な措置と技術的な措置の具体的内容は大統領令で定める。
②位置情報事業者などは、位置情報収集・利用・提供事実確認資料を位置情報システムに自動で記録して保存されるようにしなければならない。

**第 40 条　罰則**
次の各号の 1 に該当する者は、3 年以下の懲役又は 3 千万ウォン以下の罰金に処する。<改正 2007.12.21>
4.第 15 条第 1 項の規定に違反して、個人の同意を得なくて、該当の個人の位置情報を収集・利用、又は提供した者

**第 41 条　罰則**
次の各号の 1 に該当する者は、1 年以下の懲役又は 2 千万ウォン以下の罰金に処する。
・・・
4.第 16 条第 1 項の規定に違反して、技術的・管理的な措置を取らなかったり、第 16 条第 2

項の規定に違反して、位置情報収集・利用・提供の事実確認資料が位置情報システムに自動で記録・保存されるようにしない者

**第 43 条　過怠料**

②次の各号の 1 に該当する者は 1 千万ウォン以下の過怠料に処する。

3.第 12 条第 1 項の規定に違反して、利用約款の申告又は変更申告をしなかったり、第 12 条第 2 項の規定による利用約款変更命令を違反した者

**諸外国における他人の識別符号の譲受け行為等を規制する**
**関連法令に係る調査**
**報告書**

**平成 22(2010)年 12 月**

**発　行:**　　**財団法人 社会安全研究財団**
〒101-0047 東京都千代田区内神田 1-7-8 大手町佐野ビル
Tel: 03-3219-5177　Fax: 03-3219-2338
**調査実施・編集:株式会社 国際社会経済研究所**
〒108-0073 東京都港区三田 1-4-28 三田国際ビル
Tel: 03-3798-9711　Fax: 03-3798-9719