諸外国における不正アクセスの助長行為等を規制する
関連法令に係る調査
報告書

平成 23 年 10 月

財団法人　社会安全研究財団

はじめに

本調査は、前年度調査に引き続き、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、提供行為自体には罰則が付されているものの、他人の識別符号の譲受け行為については罰則が無く、また識別符号の不正取得を目的としたフィッシングサイトの構築行為についても、これを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可能性のある諸外国について、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、英国、イタリア、ロシア、中国の 4 カ国とした。（なお、前年度調査では米国、ドイツ、フランス、韓国の 4 カ国が調査対象国であった。）各国の関連する法制について、文献調査を行い、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 23 年 10 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

		英国	イタリア	ロシア	中国
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	コンピュータ不正使用法第1条 コンピュータ内のプログラムやデータに無権限でアクセスしたり、無権限のアクセスを可能とさせたりする行為を禁止	刑法第615条の3 セキュリティ手段により保護されているコンピュータ・システムや電気通信システムに不正に侵入する行為を禁止	刑法第272条 コンピュータ上のデータへの不正アクセスにより、データの破壊、遮断、変更若しくは複製を行い、又はコンピュータやネットワークの機能に障害を与える行為を禁止	刑法第285条 国事、国防建設、先端科学技術領域のコンピュータ・システムに侵入する行為を禁止。また、それ以外のコンピュータ・システムに侵入するか、又は他の技術手段により、当該システム内で保存、処理又は伝送しているデータを取得するか、又は当該システムに対して不法な制御を行うことを禁止
	罰則	2年以下の拘禁刑若しくは罰金刑、又はこれらの併科	1年以下の拘禁刑ほか（条件付き）	2年以下の自由刑又は20万ルーブル以下の罰金刑ほか	3年以下の拘禁刑若しくは拘留刑と罰金刑の併科か、又は罰金刑を単科ほか（条件付き）
	データの財物性（データの不正取得）に係る条文	データ保護法第55条 承諾なく個人データを取得する行為を禁止	個人データ保護法第23条 本人の明確な同意なく個人データを取得する行為を禁止	個人データの保護に関する連邦法第6条 本人の同意なく個人データを取得する行為を禁止	刑法第253条の1で、国家機関・金融機関等が保有する個人データを不正取得する行為を禁止
	罰則	罰金刑	6カ月以上18カ月以下の拘禁刑	（明文の規定はない）	3年以下の拘禁刑若しくは拘留刑と罰金刑の併科か、又は罰金刑を単科
	不正アクセス行為の予備行為の規制に係る条文	コンピュータ不正使用法第3A条 無権限アクセス行為を実行したり、実行を幇助することを目的として物品やプログラム、データを作成・提供・取得等する行為を禁止	—	—	—
	罰則	2年以下の拘禁刑若しくは罰金刑、又はこれらの併科	—	—	—
	不正アクセス行為の国外犯規定に係る条文	コンピュータ不正使用法第4条、5条 無権限アクセス犯罪（第1条）に関して、被害に遭ったコンピュータが英国外にある場合でも被告人が犯行当時英国にいる場合、また、被告人が犯行当時英国外にいる場合でも被害に遭ったコンピュータが英国内に存在する場合には、第1条が適用されると規定	刑法第9条、10条 イタリア国法で1年以上の拘禁刑に該当する犯罪で、イタリア国又はイタリア国民に被害を及ぼす犯罪を外国において犯した外国人は、イタリア国内に所在する場合、イタリア国法に従って処罰できると規定	刑法第12条 外国人がロシア国外で行った犯罪について、ロシア連邦やロシア国民の利益が侵害されており、ロシア連邦が加盟する国際条約に規定があり、かつ当該外国人が外国で有罪判決を受けていない場合に、ロシア連邦の領土内における犯罪行為の訴追を受けると規定	—
	他人の識別符号の譲渡しの規制に係る条文	コンピュータ不正使用法第3A条 無権限アクセス行為を実行したり、実行を幇助することを目的としてデータを作成・提供・取得等する行為を禁止	刑法第615条の4 自分又は他人に利益をもたらす目的や他人に損害を及ぼす目的で、セキュリティ手段により保護されているコンピュータ・システムや電気通信システムにアクセスするためのコード、パスワードその他の手段を不正に取得、複製、頒布若しくは提供する行為を禁止	—	—
	罰則	2年以下の拘禁刑若しくは罰金刑、又はこれらの併科	1年以下の拘禁刑及び5,164ユーロ以下の罰金刑ほか（条件付き）	—	—
	他人の識別符号の譲受けの規制に係る条文	コンピュータ不正使用法第3A条 無権限アクセス行為を実行したり、実行を幇助することを目的としてデータを作成・提供・取得等する行為を禁止	刑法第615条の4 自分又は他人に利益をもたらす目的や他人に損害を及ぼす目的で、セキュリティ手段により保護されているコンピュータ・システムや電気通信システムにアクセスするためのコード、パスワードその他の手段を不正に取得、複製、頒布若しくは提供する行為を禁止	—	—
	罰則	2年以下の拘禁刑若しくは罰金刑、又はこれらの併科	1年以下の拘禁刑及び5,164ユーロ以下の罰金刑ほか（条件付き）	—	—
	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	識別符号が個人データに該当する場合には、データ保護法第55条（個人データの非合法的取得その他）を適用可能 （他人の識別符号の譲渡しに関する広告や誘引行為自体を処罰する法令はない）	—	—	—
	罰則	罰金刑	—	—	—
	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	—	—	—	—

		英国	イタリア	ロシア	中国
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	コンピュータ不正使用法第3A条 無権限アクセス行為等を実行したり、実行を幇助することを目的としてプログラムやデータを作成・提供・取得等する行為を禁止	刑法第615条の5 コンピュータ・システムや電気通信システム、又はシステム内やシステムに関係するデータやプログラムを不正に損壊したり、当該システムの運用の全部若しくは一部を中断したり改変する目的で、コンピュータ・プログラムの取得、作成、複製、頒布、他者への提供等を行うことを禁止	刑法第273条 無権限での情報の破壊、遮断、変更若しくは複製、又はコンピュータ、コンピュータ・システム若しくはネットワークに対する障害を明白に目的としたプログラムの作成若しくは既存プログラムの改造、又はそのようなプログラム若しくは物理的媒体の使用若しくは頒布を禁止	刑法第286条 コンピュータ・ウィルス等の破壊型プログラムを故意に作成、頒布して、コンピュータ・システムの正常な運用に影響を及ぼす行為を禁止
	罰則	2年以下の拘禁刑若しくは罰金刑、又はこれらの併科	2年以下の拘禁刑及び10,329ユーロ以下の罰金刑	3年以下の自由刑及び20万ルーブル以下の罰金刑ほか	5年以下の拘禁刑又は拘留刑
	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	フィッシングサイト構築等については詐欺法第2条(虚偽の表明による詐欺)、詐欺法第7条(詐欺に使用するための物品の作成又は提供)を適用可能	フィッシングサイト構築等については刑法第494条(なりすまし)を適用可能	—	フィッシングサイト構築等を通じて他人の財産等を詐取する行為については、刑法第287条(コンピュータを利用して実施される各種犯罪)を適用可能 (フィッシングサイト構築自体を処罰する法令はない)
	サイバーテロ行為の規制に係る条文	コンピュータ不正使用法第3条 無権限の行為であることを認識しながら、意図的に、又は無謀さの結果として、コンピュータの運用を損ねたり、コンピュータ内のプログラムやデータへのアクセスを妨げたり、プログラムの運用やデータの信頼性を損なうような行為を禁止	刑法第635条の2～5 コンピュータのデータやプログラムを破壊、劣化、消去、改変又は削除する行為を禁止。また、そのような行為、又はデータやプログラムの入力や伝送を通じてコンピュータ・システム等を破壊、損壊若しくは使用不能(全部もしくが一部)にいたらせるか、システムの運用に重大な障害を生じさせる行為を禁止	刑法第274条 コンピュータ、コンピュータ・システム又はコンピュータ・ネットワークの使用に関する規則への違反により、法の保護の対象となるコンピュータ上の情報の破壊、遮断又は変更がなされ、重大な損害を発生させる行為を禁止	刑法第286条 コンピュータ・システムの機能を削除、変更、追加、干渉することで、当該システムの正常な運用を不可能にする行為を禁止
	罰則	10年以下の拘禁刑若しくは罰金刑、又はこれらの併科	6カ月以上3年以下の拘禁刑ほか(条件付き)	2年以下の禁固刑ほか	5年以下の拘禁刑又は拘留刑ほか(条件付き)
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	調査権限規制法第5条、6条 「重罪の予防又は探知のため」等の理由がある場合には、内務大臣が発付する令状 によって、電気通信システムによる伝送の過程における傍受が可能。傍受令状を申請できる者は、保安局長官、機密情報局長官、政府情報通信本部部長、重大組織犯罪庁長官、首都圏警察長官等に限定	刑事訴訟法第266条、267条 「終身刑又は5年超の拘禁刑が定められている、過失以外の犯罪」や「5年以上の拘禁刑が定められている、行政機関に対する犯罪」等に関係する手続きにおいて、予備捜査担当裁判官が発付する令状によって、電話又は他の通信形態の通話又は通信の傍受が可能。傍受令状は、検察官が請求可能	通信に関する連邦法第63条 権限を有する通信事業者の従業員以外の者が、電子メールを閲覧したり、添付ファイルを表示したり、通信・郵便ネットワークによって伝達される情報及び文書通信の内容を把握したりすることは、裁判所の決定によって行うことが可能	電気通信条例第66条 国家の安全又は刑事犯罪の捜査の必要から、公安機関、国家安全機関又は人民検察院が電気通信内容に対して検査を行うことが可能
	差押場所が明確でない場合の措置に係る条文	調査権限規制法第22条 警察等の関係公的機関 の官職等を保有している者は、「罪を予防若しくは探知するため、又は秩序違反を阻止するため」等の理由があるときには、電気通信事業者に対して通信データの取得、又は取得した通信データの開示を要求することが可能	個人データ保護法132条 検察官の発付する令状に基づき、公的な電気通信サービスを提供する電気通信事業者が保存しているトラフィックデータを取得することが可能	通信に関する連邦法第64条 通信事業者は、ロシア連邦の公的捜査・保安機関に対して、通信サービス利用者及び提供サービスに関する情報、並びに連邦法に規定された場合に法的任務の遂行に必要とする情報を提供する義務を負う	インターネット情報サービス管理規則第14条 インターネット接続サービス事業者は、インターネット接続に係る情報を保存し、国家の関係機関が法に基づき問い合わせる際にこれを提供しなければならない
	ログの保存に係る条文	2009年データ保存規則第5条 公的な電気通信サービスを提供する電気通信事業者はインターネットアクセス等に係る通信データを12カ月間保存しなければならない	個人データ保護法132条 公的な電気通信サービスを提供する電気通信事業者は電気通信に関するトラフィックデータを12カ月間保存しなければならない	—	インターネット情報サービス管理規則第14条 インターネット接続サービス事業者はインターネット接続に係る情報を60日間保存しなければならない

※英国・イタリア・ロシアの3カ国については、不正アクセスに関係する行為に関して未遂罪を罰する規定が存在する。

	英国	イタリア	ロシア	中国
人　口	6180万人	5930万人	1億4291万人	約13億人
インターネット普及率(2010年)	85.0%	53.7%	43.0%	34.3%
パソコン普及状況	81.2%	37.0%	13.3%	5.6%
固定電話普及率(2010年)	53.7%	35.7%	31.5%	22.0%
移動電話普及率(2010年)	130.3%	135.4%	166.3%	64.0%
1人当りGNI	4万5390ドル	3万5240ドル	9620ドル	2940ドル

人口の出典:外務省ホームページ(http://www.mofa.go.jp/mofaj/area/index.html)
インターネット普及率、固定電話普及率、移動電話普及率の出典:ITUホームページ(http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx)
パソコン普及状況、1人当りGNI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．英国における不正アクセス関連法令

２．１　英国における不正アクセス関連犯罪の現状

（１）英国企業・組織における情報セキュリティ侵害の統計

英国では、省庁等からの委託を受けて、PricewaterhouseCoopers社が2年毎に「情報セキュリティ侵害調査（Information Security Breaches Survey）」という報告書を発行している[1]。同報告書は、英国の企業・組織における情報セキュリティ侵害の実態に関する調査報告書であり、2010年の調査[2]では、539の組織（うち従業員数250人以上の大組織は53%、249人以下の中小組織は47%）が回答している。

2010年の調査では、情報セキュリティ侵害の被害に遭った企業の割合は2008年に比べて大幅に増加している（表 2参照）。

表 2　情報セキュリティ侵害の被害経験

前年1年間に被害に遭った情報セキュリティ侵害の種類	2010年調査		2008年調査[3]	
	大組織	中小組織	大組織	全体[4]
システム障害又はデータ破損	70%	58%	34%	23%
ウィルス又は悪意あるソフトウェアへの感染	62%	43%	21%	14%
コンピュータを伴う窃盗又は詐欺	49%	11%	30%	4%
従業員に起因するその他のインシデント	80%	42%	47%	16%
無権限の外部者による攻撃（ハッキングの試みを含む）	63%	49%	39%	16%

出典：PricewaterhouseCoopers「情報セキュリティ侵害調査」（2008年版、2010年版）

---

[1] 同報告書は 2006 年版までは貿易産業省（DTI）の委託、2008 年版はビジネス・企業・規制改革省（BERR）の委託、2010 年版は Infosecurity Europe（欧州で最大規模の女王セキュリティ展示会）の委託を受けて作成されている。

[2] PricewaterhouseCoopers, “Information Security Breaches Survey 2010”（http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html）。

[3] 2008 年調査（http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf）では、1007 組織が回答し、そのうち従業員数 250 人以上の大組織は 13%、249 人以下の中小組織は 87%であった。

[4] 2008 年調査には中小組織の集計値が記載されていないため、（また 2010 年調査には全体の集計値が記載されていないため）このように記載する。

情報セキュリティ侵害のうち、「コンピュータを伴う窃盗又は詐欺」、「従業員に起因するインシデント」、「無権限の外部者による攻撃」については、より詳細な調査結果が示されている（表 3、表 4、表 5参照）。

表 3　コンピュータを伴う窃盗や詐欺の種類

前年1年間に被害に遭った窃盗や詐欺の種類	2010年調査		2008年調査	
	大組織	中小組織	大組織	全体
従業員が窃盗又は詐欺を行うためにシステムを使用した	19%	5%	0%	1%
従業員がコンピュータ設備を盗んだ	29%	7%	6%	1%
外部者がコンピュータ設備を盗んだ	39%	9%	28%	3%
上記のいずれか	49%	11%	30%	4%

出典：PricewaterhouseCoopers「情報セキュリティ侵害調査」（2008年版、2010年版）

表 4　従業員に起因するインシデントの種類

前年1年間に被害に遭った従業員関連インシデントの種類	2010年調査		2008年調査	
	大組織	中小組織	大組織	全体
ウェブアクセスの不正使用・誤用	80%	34%	43%	14%
電子メールアクセスの不正使用・誤用	75%	29%	25%	7%
システム又はデータへの無権限アクセス（例えば他人のIDの使用）	58%	13%	8%	2%
データ保護法又は規則への違反	45%	10%	3%	1%
機密情報の不正使用・誤用	36%	9%	6%[5]	1%
機密情報の紛失又は漏えい	46%	16%		
上記のいずれか	80%	42%	47%	16%

出典：PricewaterhouseCoopers「情報セキュリティ侵害調査」（2008年版、2010年版）

[5] 2008 年調査では、「機密性に対する侵害（例えば知的所有権や顧客データ）」という項目であった。

表 5　無権限の外部者による攻撃の種類

前年1年間に被害に遭った無権限の外部者による攻撃の種類	2010年調査		2008年調査	
	大組織	中小組織	大組織	全体
組織のネットワークに侵入する重大な試み	61%	48%	31%	11%
組織のネットワークへの実際の侵入	15%	11%	13%	4%
インターネット又は電気通信トラフィックに対する攻撃	22%	8%	5%	2%
インターネット上での組織へのなりすまし（例えばフィッシング攻撃）	36%	12%	9%	4%
顧客へのなりすまし（例えばアイデンティティ窃盗）	27%	14%	9%	2%
DoS攻撃	25%	18%	11%	3%
上記のいずれか	63%	49%	39%	16%

出典：PricewaterhouseCoopers「情報セキュリティ侵害調査」（2008年版、2010年版）

2010年調査では、無権限の外部者による攻撃については、外部者から内部ネットワークへの侵入の試みを受けた大組織の割合は61%と、2008年に比べて約2倍に増えている。また、15%の大組織が実際に侵入を受けている。侵入を受けた主要な原因としては、従業員が技術的なコンフィギュレーションを正しく設定していなかったことや更新していなかったことが挙げられている。また、インターネット又は電気通信トラフィックに対する攻撃を受けた大組織の割合は、2008年に比べて約4倍に増えている。とりわけ、VoIPにおける通信トラフィックがハッカーにとっての魅力的な標的となっている。フィッシング（Phishing）の被害も増えており、被害を受けた大組織の割合は前回に比べて約4倍に増加している。フィッシングはより洗練されたものになってきており、特定の個人を狙うフィッシングであるスピア・フィッシング（spear-fishing）も発生している[6]。アイデンティティ窃盗やアイデンティティ詐欺[7]も増加しており、大組織の約4分の1がそのような被害を受けている。アイデンティティ窃盗や詐欺の被害経験は業種別でかなり異なっており、最も被害を受けてい

[6] 英国の大手金融サービス企業のスタッフは、スピア・フィッシング攻撃の標的にされ、ある企業を装ったサイト上で悪意あるソフトウェアをダウンロードするように促されたという。

[7] 同報告書では「不正に入手したパスワードを使って他人になりすまし詐欺的な取引を行うこと」と規定されている。

るのが小売業[8]であり、金融サービス、とりわけ銀行も被害の割合が高い。他方、製造業はほとんど被害を受けていない。また、ボットネットの増加によってDDoS攻撃を受ける企業の割合も増加しており、業種別では小売業が最も被害の割合が高く、電気通信業がそれに続く。

（２）オンラインバンクに係るフィッシングサイト等の統計

英国のFinancial Fraud Action UK（FFA）[9]では、英国における銀行関連詐欺の統計レポートとして、「詐欺の実態2011（Fraud the Facts 2011）」を発行している[10]。

同レポートによると、2005年から2010年までの英国の銀行や住宅金融組合をターゲットとしたフィッシングサイト数及びオンラインバンキング詐欺[11]による損失額の統計は、表 6 の通りである。

表 6　英国におけるフィッシングサイト数とオンラインバンキング詐欺の損失額

	2005年	2006年	2007年	2008年	2009年	2010年
英国の銀行や住民金融組合をターゲットにしたフィッシングサイト数（単位：サイト数）	1,700	14,156	25,797	43,991	51,161	61,873
オンラインバンキング詐欺による損失額（単位：万ポンド）	2,320	3,350	2,260	5,250	5,970	4,670

出典：Financial Fraud Action UK「詐欺の実態2011」

2010年のオンラインバンキング詐欺損失額は2009年に比べて約22%低減しているが、その要因として同レポートでは、業界のキャンペーン等を通じて利用者がオンラインバンキングにおけるセキュリティ意識を高めたこと、銀行業界が詐欺的な活動を監視するための高度な検出ソフトウェアを使用するようになったこと、2009年春に内務省とロンドン警視庁が共同でサイバー犯罪の重大事犯に全国的に対処するために警察中央サイバー犯罪ユニット（Police Central e-crime Unit：PCeU）を立ち上げたことを挙げている。

---

[8] 2010 年調査では、回答企業の半分以上が被害を受けている。

[9] 英国の金融サービス業界団体である UK Payments Administration が立ち上げた金融詐欺防止に向けた共同活動の名称。

[10] Financial Fraud Action UK, “Fraud the Facts 2011: The Definitive Overview of Payment Industry Fraud and the Measures to Prevent It”（http://www.financialfraudaction.org.uk/Fraud-the-Facts-2011.asp）。

[11] フィッシング詐欺のみならず悪意あるソフトウェアによる損失額も含まれている。

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[12]

（１）1990 年コンピュータ不正使用法

1990年コンピュータ不正使用法（Computer Misuse Act 1990）は1990年に制定された。同法の制定以前には、英国にはサイバー犯罪に対処するための実質的な法律が存在しなかった。同法の導入にはいくつもの要因があると考えられるが、そのうちの1つは、Regina vs. Gold & Schifreenのハッキング事犯に対処できなかったことである。同事犯は結局、1980年代終わりに貴族院控訴院（House of Lords Court of Appeal）によって棄却された。また、イングランド・スコットランド法律委員会（English and Scottish Law Commissions）による報告書の公開による法整備の勧告や、欧州評議会の法務委員会（Legal Affairs Committee）による1989年の勧告も同法の導入の一因である。同法の制定以降、いくつものコンピュータ不正使用の事犯が提訴された。

（２）2006 年警察司法法による改正

1990年コンピュータ不正使用法は、2006年11月8日にロイヤル・アセント（国王の裁可）を受けた2006年警察司法法（Police and Justice Act 2006）によって改正がなされた[13]。これは、同法を欧州評議会のサイバー犯罪条約の完全に準拠させるため、また技術進歩や近年の犯罪傾向に歩調を合わせるための改正である。

この2006年警察司法法による修正により、1990年コンピュータ不正使用法には以下の要素が追加された。

① DoS攻撃や、その他のタイプの破壊的なソフトウェアのアップロードや頒布に対処するための抑制的な手段として、コンピュータの運用を損なう犯罪に関連して、初めて「recklessness（無謀さ）」の要素を導入した（第3条）。

② 直接的な犯行者のみならず、プログラムやデータに対する無権限アクセスを可能ならしめた者にも有責性を拡大することによって、ハッキング犯罪となる行為を拡大した（第1条）。

③ コンピュータ不正使用犯罪において使用される「物品（articles）」（電子的形式で保持されるプログラム又はデータ）の作成、提供、又は取得に関する犯罪を追加した（第3A条）[14]。

---

[12] 本節の記述は、ISSA Journal の記事 “U.K. Cyber-Crime Law Changed”（2007 年 3 月）（http://www.issa.org/Library/Journals/2007/March/Austen%20-%20U.K.%20Cyber-Crime%20Law%20Changed.pdf）を参考にした。

[13] この改正法は、スコットランドでは 2007 年 10 月から、イングランドとウェールズでは 2008 年 10 月から施行されている。OUT-LAW.COM の記事（2009 年 6 月更新）（http://www.out-law.com/default.aspx?page=405）。

[14] これらの新たな犯罪の導入は、ハッキングツールや他の形態のマルウェア（これらの多

④ この種類の犯罪の広がりに対する政府の懸念を反映して、最大刑を引き上げた（第1条～第3条）。

とりわけ、既存のコンピュータ不正使用法の第3条（コンピュータ・マテリアルの改変）については、完全に書き換えがなされた。1990年当時の考えは、プログラム又はデータの内容を無権限で変更・削除・追加する問題に対処することであった。当時は、会計目的で利用される帳簿やファイルの改変が詐欺事犯の多くの割合を占めていた。1984年にロンドン警視庁刑事部（New Scotland Yard）にコンピュータ犯罪ユニット（Computer Crime Unit）が設置されたが、これは詐欺対策班（Fraud Squad）の一部であり、その主要な目的はコンピュータに関連した詐欺を捜査することであった。コンピュータウィルスも当時から存在はしていたが、その後のインターネットの急速な発展や、ワームやDoS攻撃の広がりは予想以上のものであった。

既存のコンピュータ不正使用法の第3条においては、(ⅰ)犯行者にコンピュータを改変するという明示的な意図が存在することの証明と、(ⅱ)犯行者が当該行為が無権限であることを知っていることの証明とが必要であった。このことは、2000年代に増加したDoS攻撃やDDoS攻撃、ワームを捜査したり訴追したりする際に、様々な問題をもたらした。

(ⅰ)については、犯行者はインターネットを通じてこうしたタイプのプログラムを送信する際に、自分の行為の結果や、個々のシステムへの明示的な影響を知らなかったという弁護が可能であったため、いくつもの事犯が破綻し、若しくは後年には裁判手続きにも進めなくなったりした。2006年の法改正において「無謀さ」の要素を追加することにより、そのような場合でも有罪とすることが可能となった。

(ⅱ)については、DDoS攻撃であれば踏み台とするサーバに対する無権限の行為が存在するため旧い第3条の対象になると考えられたが、単純なDoS攻撃については無権限の行為が含まれないとする考え方があった。そのため、DoS攻撃の違法性については疑義があったが、2006年のLennon事件の判決によって、最終的に旧い第3条の下でもDoS攻撃の違法性が認められることとなった[15]。

くはインターネットでダウンロードして入手することができる）の使用や拡散に対する懸念を反映するものである。

[15] 2005 年に David Lennon（当時 19 歳）は、以前の勤務先企業のサーバに対して 50 万通以上の電子メールを送信し、サーバをダウンさせた。2005 年 11 月の Magistrates 裁判所における判決では、Lennon の弁護士は、当該企業のサーバの目的は電子メールを受信することであり、それ故、当該企業は電子メールの受領及びその結果として生じるデータの改変に同意していたと主張した。同判決において裁判官は、電子メールを送信することは正当な（権限ある）行為であり、Lennon は 1990 年コンピュータ不正使用法の下では無罪だと結論付けた。しかし、上訴審では上記の論法に異議が唱えられ、確かにサーバ所持者は通常は当該サーバへの電子メールの送信に同意をしていたかもしれないが、そのような暗黙の同意は無制限のものではなく、コンピュータシステムを妨害することを目的として送信された電子メールには当該同意は当てはまらないと結論付けた。結局、2006 年 8 月の高

なお英国では、2001年4月にサイバー犯罪に対処するために、全英犯罪捜査班（National Crime Squad: NCS）の一部として全英ハイテク犯罪班（National Hi-Tech Crime Unit: NHTCU）が立ち上げられ、歳入関税庁や全英犯罪情報機関（National Criminal Intelligence Service）等の関係機関と協力して捜査活動を行っていた。2006年4月にNHTCUの機能は重大組織犯罪庁（Serious Organised Crime Agency: SOCA）に引き継がれた。また、2009年には、ロンドン警視庁に上述の警察中央サイバー犯罪ユニット（Police Central e-crime Unit：PCeU）が設置された。PCeUはSOCAに置き換わる組織ではなく、重大なサイバー犯罪事犯に対処できるように全国的な捜査能力を確保するために設立された。

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

1990年コンピュータ不正使用法第1条

「1990年コンピュータ不正使用法1条　コンピュータ・マテリアルに対する無権限のアクセス」では、コンピュータ内のプログラムやデータに無権限でアクセスしたり、無権限のアクセスを可能とさせたりすることを禁じている。

第1条の違反は、即決裁判では12カ月以下の拘禁刑若しくは罰金刑、又はこれらの併科、起訴に基づく有罪判決では2年以下の拘禁刑若しくは罰金刑、又はこれらの併科に処すことができる[16]。

以下、いくつかの補足説明を行う。

○コンピュータ内のプログラムやデータへのアクセス

1990年コンピュータ不正使用法の用語の解釈については、同法の第17条において一部規定されている。

「コンピュータ内のプログラムやデータへのアクセス」とは、第17条(2)において、「プログラムやデータを改変又は消去すること」、「プログラムやデータを、別の記憶媒体又は同

等法院の王座裁判所の判決において、Lennon は 1990 年コンピュータ不正使用法第 3 条に違反した罪で有罪を宣告された。OUT-LAW.COM の記事（2006 年 8 月）（http://www.out-law.com/default.aspx?page=7224）。

[16] 本報告書では法令原文の”summary conviction”を「即決裁判（における有罪判決）」、”conviction on indictment”を「（正式）起訴に基づく有罪判決」と訳した。「即決裁判」は治安判事裁判所で治安判事によって審理されるものであり、「起訴に基づく有罪判決」は刑事法院で陪審裁判によって審理されるものである。なお、英国における犯罪は、①治安判事裁判所で、治安判事によってのみ審理可能な略式犯罪、②治安判事裁判所・刑事法院のいずれでも審理できる中間的犯罪、③刑事法院で陪審裁判によってのみ審理できる正式起訴犯罪に分類される。司法制度改革審議会「諸外国の司法制度概要」（第 5 回審議会（1999 年 10 月 26 日）配布資料）（http://www.kantei.go.jp/jp/sihouseido/pdfs/dai5gijiroku-1.pdf）。

じ記憶媒体の別の場所にコピーや移動すること」、「プログラムやデータを使用すること」等として規定されている。

○無権限のアクセス

「無権限のアクセス」とは、第17条(5)において、「その人物が当該アクセスを制御する権限を有さない」かつ「その人物が、権限を有する人物から、当該アクセスを行う承諾を得ていない」場合に該当すると規定されている。

○犯行者の犯罪意思

ある行為を第1条違反として検挙するためには、以下の2つの犯罪意思（犯意）要素の証明が必要とされる[17]。

- 犯行者が当該アクセスが無権限であることを認識していること、かつ
- 犯行者がコンピュータ内のプログラム又はデータに関する情報を得ることを意図していること

すなわち、当該アクセスが無権限であるという犯行者の認識がなければならない。単なる「無謀さ（recklessness）」では不十分である。

○外部犯行と内部犯行

第1条は、外部からコンピュータをハッキングする行為のみならず、意図的に自分の権限を超えて、自分がアクセス権限を持たない他のプログラム又はデータに対してアクセスする行為（内部犯行者による行為）にも適用される[18]。

○無権限のアクセスを可能とさせる行為

また、権限のある利用者Aが無権限の人物Bのためにアカウントを作成し、Bが無権限アクセスを実行した場合、直接的な犯行者Bのみならず、Aについても「無権限のアクセスを可能とさせる」行為を行った者として、第1条違反となる[19]。

---

[17] 英国検察局の 1990 年コンピュータ不正使用法に関する法的ガイダンス（http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/）。

[18] 英国検察局の 1990 年コンピュータ不正使用法に関する法的ガイダンス（http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/）。

[19] 2006 年警察司法法によって 1990 年コンピュータ不正使用法が改正される以前は、第 1 条においてこのような行為が有罪になるか無罪になるかが不透明であった。無権限のアクセスを得ることの共同謀議の犯罪が適用されると考える人もいるが、いくつかの裁判所における解釈は不明確なものであった。この問題を明確にするために、2006 年の法改正では、「無権限のアクセスを可能とさせること」という条文が追加された。ISSA Journal の記事 “U.K. Cyber-Crime Law Changed”（2007 年 3 月）（http://www.issa.org/Library/Journals/2007/March/Austen%20-%20U.K.%20Cyber-Crime%20Law%20Changed.pdf）。

1990年コンピュータ不正使用法第2条

「1990年コンピュータ不正使用法2条　さらなる犯罪を実行する意図又はさらなる犯罪の実行を幇助する意図でなされる無権限のアクセス」では、上記第1条の犯罪を、さらなる犯罪を実行する意図又は幇助する意図をもって実行することを禁じている。

第2条の違反は、即決裁判では12カ月以下の拘禁刑若しくは罰金刑、又はこれらの併科、起訴に基づく有罪判決では5年以下の拘禁刑若しくは罰金刑、又はこれらの併科に処すことができる。

第2条は、「さらなる犯罪」が無権限アクセス行為と同じ機会に実行されるか否かに関わらず適用される。また、「さらなる犯罪」を実際に実行することが不可能であった場合でも適用されうる。

不正アクセスの未遂行為について

不正アクセスの未遂行為については、1990年コンピュータ不正使用法第8条（他の法律との関係）の第3項及び1981年犯罪未遂法第1条（犯罪実行の未遂）で規定されており、不正アクセス犯罪の実行のための単なる準備以上の行為を行った者は、当該犯罪の未遂罪で有罪とされる。

（２）データの財物性（データの不正取得）

1998年データ保護法第55条

個人データに関しては、「1998年データ保護法第55条　個人データの非合法的取得」では、データ管理者[20]の承諾なく、個人データ若しくは個人データに含まれる情報を取得（obtain）、開示（disclose）、又は他人への開示を斡旋（procure）することを禁じている。

同法の第60条(2)により、第55条の違反は、即決裁判では法令で定める限度を超えない罰金刑、起訴に基づく有罪判決では罰金刑に処すことができる[21]。

「個人データ」は、1998年データ保護法第1条（基本的な解釈規定）において、「(a)当該データ又は(b)当該データ及びデータ管理者が保有している他の情報若しくはデータ管理者が保有する可能性のある他の情報によって、識別することが可能な、生存する個人に関するデータ」と定義されている。

なお、1968年窃盗法第1条及び第4条では、窃盗罪の対象となる他人の「財産（property）」

[20] 「データ管理者」とは、個人データの処理目的や方法を決定する者であり（1998 年データ保護法第 1 条(1)）であり、日本の個人情報保護法における個人情報取扱事業者にほぼ相当する。

[21] 即決裁判における罰金の法定最高額は、1991 年刑事裁判法第 17 条によると、5,000 ポンドである。石井夏生利「個人情報の窃取・漏えいと刑事罰」（堀部政男編著『プライバシー・個人情報保護の新課題』（商事法務、2010 年）所収）p110。

について、無形財産（intangible property）も含むと規定しているが、データ一般の窃盗に関する規定はない。

（３）不正アクセス行為の予備行為

1990年コンピュータ不正使用法では、不正アクセスの予備行為として、外部からのシステム探索等に関する明示的な規定は存在しない。

ただし、後述の1990年コンピュータ不正使用法第3A条では、いわゆる「ハッキングツール」の作成・提供・取得等も対象としている[22]。「ハッキングツール」には、ポートスキャナー等のシステム探索用のツールも含まれると考えられる。

（４）不正アクセス行為の国外犯

1990年コンピュータ不正使用法の第1条や第2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。

1990年コンピュータ不正使用法第4条、第5条

1990年コンピュータ不正使用法第4条と第5条では、第1条（無権限アクセス）に違反する犯罪に関して、被害に遭ったコンピュータが英国外にある場合でも被告人が犯行当時英国にいる場合、また、被告人が犯行当時英国外にいる場合でも被害に遭ったコンピュータが英国内に存在する場合には、第1条が適用されるとしている。ただし、当該コンピュータが英国外にあり、かつ被告人が英国外にいる場合には、第1条は適用されない。

また1990年コンピュータ不正使用法第4条と第5条では、第2条（さらなる犯罪を実行・幇助する意図でなされる無権限アクセス）に違反する犯罪に関しては、（「さらなる犯罪」に英国法が適用される場合には、）被害に遭ったコンピュータが英国外にあり、かつ被告人が英国外にいる場合であっても、第2条が適用されうるとしている。

（５）他人の識別符号の譲渡し

不正アクセスの助長行為として、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、1990年コンピュータ不正使用法第3A条において規制が行われている。

1990年コンピュータ不正使用法第3A条

「1990年コンピュータ不正使用法3A条　第1条又は第3条に基づく犯罪に使用するための物品の作成、提供、又は取得」の(1)では、第1条（無権限アクセス）の犯罪を実行したり、

[22] ISSA Journal の記事 “U.K. Cyber-Crime Law Changed”（2007 年 3 月）（http://www.issa.org/Library/Journals/2007/March/Austen%20-%20U.K.%20Cyber-Crime%20Law%20Changed.pdf）及び OUT-LAW.COM の記事（2009 年 6 月更新）（http://www.out-law.com/default.aspx?page=405）。

実行を幇助したりするために、「物品（articles）」を提供することを禁じている。

「物品」にはあらゆる電子データが含まれるため、ID・パスワード等の識別符号も含まれる[23]。

第3A条の違反は、即決裁判では12カ月以下の拘禁刑若しくは罰金刑、又はこれらの併科、起訴に基づく有罪判決では2年以下の拘禁刑若しくは罰金刑、又はこれらの併科に処すことができる。

また、識別符号は通常は個人データ（又は個人データに含まれる情報）に該当しないが、識別符号が個人データ（又は個人データに含まれる情報）に該当する場合には、そのような識別符号を提供する行為については、1998年データ保護法第55条を適用することが可能である。

1998年データ保護法第55条

「1998年データ保護法第55条　個人データの非合法的取得」では、データ管理者の承諾なく個人データ又は個人データに含まれる情報を第三者に開示（disclose）することや、データ管理者の承諾なく取得した個人データ又は個人データに含まれる情報を販売することを禁じている。

ID・パスワード等の識別符号そのものは、通常はそれだけでは個人を識別できないので、1998年データ保護法第1条に言う「個人データ」に該当しない[24]が、データ管理者が他の個人を識別できるデータ（氏名等）と一緒に当該識別符号を保有している場合には、個人データの一部を構成する。すなわち、その場合には、ID・パスワード等の識別符号は「個人データに含まれる情報」に該当する。

同法の第60条(2)により、第55条の違反は、即決裁判では法令で定める限度を超えない罰金刑、起訴に基づく有罪判決では罰金刑に処すことができる。

---

[23] コンピュータ不正使用法第 3A 条は、2006 年警察司法法によって新たに追加された条項であり、この 2006 年警察司法法は欧州評議会のサイバー犯罪条約を国内法化するものでもある。コンピュータ不正使用法第 3A 条に対応するサイバー犯罪条約は第 6 条（機器の濫用）であり、第 6 条では「コンピュータ・システムの全部又は一部がアクセスされるようにするコンピュータ・パスワード、アクセス・コード又はこれに類するデータ」を不正アクセス等の目的で調達や頒布等することが禁止されている。そのため、コンピュータ不正使用法第 3A 条にいう「物品」にはパスワード等の「他人の識別符号」が含まれる。2006 年警察司法法の注釈（Explanatory Notes）第 303 項
（http://www.legislation.gov.uk/ukpga/2006/48/notes/division/5/1/5/4）。

[24] なお、参考まで、自動車のナンバーについては以下のように考えられている。「当該個人が特定される情報が個人情報であるが、例えば車のナンバーは、それだけでは個人情報ではないが、個人と関連づけられると個人情報になる。」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）。

（６）他人の識別符号の譲受け

不正アクセスの助長行為として、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、1990年コンピュータ不正使用法第3A条において規制が行われている。

1990年コンピュータ不正使用法第3A条

「1990年コンピュータ不正使用法3A条　第1条又は第3条に基づく犯罪に使用するための物品の作成、提供、又は取得」の(3)では、第1条（無権限アクセス）の犯罪を実行したり、実行を幇助したりするために、「物品（articles)」を取得することを禁じている。

上述のように「物品」にはあらゆる電子データが含まれるため、ID・パスワード等の識別符号も含まれる。

第3A条の違反は、即決裁判では12カ月以下の拘禁刑若しくは罰金刑、又はこれらの併科、起訴に基づく有罪判決では2年以下の拘禁刑若しくは罰金刑、又はこれらの併科に処すことができる。

また、識別符号は通常は個人データ（又は個人データに含まれる情報）に該当しないが、識別符号が個人データ（又は個人データに含まれる情報）に該当する場合には、そのような識別符号を不正に取得する行為については、上述の1998年データ保護法第55条を適用することが可能である。

（７）他人の識別符号の譲渡しに関する広告又は誘引行為

識別符号は通常は個人データ（又は個人データに含まれる情報）に該当しないが、識別符号が個人データ（又は個人データに含まれる情報）に該当する場合には、（不正アクセスの助長行為に限るものではないが）そのような識別符号を提供することを内容とした広告や誘引行為については、1998年データ保護法第55条を適用することが可能である。

1998年データ保護法第55条

「1998年データ保護法第55条　個人データの非合法的取得」の(5)では、データ管理者の承諾なく個人データ又は個人データに含まれる情報を第三者に開示 (disclose) することや、データ管理者の承諾なく取得した個人データ又は個人データに含まれる情報[25]の販売を申し出ることを禁じている。

同条の(6)では、個人データ又は個人データに含まれる情報が売り物であること、又は売り物である可能性があることを示唆する広告は、個人データ又は個人データに含まれる情

[25] 上述のように、ID・パスワード等の識別符号そのものは、通常はそれだけでは個人を識別できないので、1998 年データ保護法第 1 条に言う「個人データ」に該当しないが、データ管理者が他の個人を識別できるデータ（氏名等）と一緒に当該識別符号を保有している場合には、個人データの一部を構成する。すなわち、その場合には、ID・パスワード等の識別符号は「個人データに含まれる情報」に該当する。

報の販売の申し出に該当すると規定している。

同法の第60条(2)により、第55条の違反は、即決裁判では法令で定める限度を超えない罰金刑、起訴に基づく有罪判決では罰金刑に処すことができる。

（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1990年コンピュータ不正使用法や1998年データ保護法では、他人の識別符号の譲受けに関する広告や誘引行為は規制されていない。

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

1990年コンピュータ不正使用法第3A条

「1990年コンピュータ不正使用法3A条　第1条又は第3条に基づく犯罪に使用するための物品の作成、提供、又は取得」の(1)では、第1条（無権限アクセス）や第3条（コンピュータ運用の損傷）の犯罪を実行するために、又は実行を幇助するために、「物品」を作成・改造・提供等することを禁じている。また、同条の(2)では、第1条や第3条の犯罪を実行するために、又は実行を幇助するために使用されると信じて、「物品」を提供等することを禁じている。

「物品」には電子的形式のあらゆるプログラムやデータが含まれる。コンピュータウィルスも規制の対象となる[26]。

第3A条の違反は、即決裁判では12カ月以下の拘禁刑若しくは罰金刑、又はこれらの併科、起訴に基づく有罪判決では2年以下の拘禁刑若しくは罰金刑、又はこれらの併科に処すことができる。

（２）識別符号の不正取得（フィッシングサイトの構築等）

ID・パスワード等の識別符号の不正取得を目的とするものに限らないが、フィッシングサイトの構築等については、2006年詐欺法の第2条や第7条で規制することが可能である。

2006年詐欺法第2条

---

[26] OUT-LAW.COM の記事（2009 年 6 月更新）（http://www.out-law.com/default.aspx?page=405）。ただし英国検察局の 1990 年コンピュータ不正使用法に関する法的ガイダンス（http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/）では、検察官はコンピュータ・システムのセキュリティに関連してハードウェアやソフトウェアをテストしたり監査したりするためのプログラムを作成する業界の存在について認識しなければならないとされている。いくつかのプログラムはそれ故、デュアルユース（当該プログラムが正当な目的又は違法な目的の両方で使用しうること）を有する。この場合、検察官は被疑者が犯罪意図を持っているか否かを確証しなければならない。

「2006年詐欺法第2条　虚偽の表明による詐欺」では、自らが儲けたり他人に儲けさせるために虚偽の表明（false representation）を行うことを禁じている。

この虚偽の表明には、フィッシングサイトやフィッシングメールが含まれる[27]。

第2条の違反は、同法の第1条により、即決裁判では12カ月以下の拘禁刑若しくは罰金刑、又はこれらの併科、起訴に基づく有罪判決では10年以下の拘禁刑若しくは罰金刑、又はこれらの併科に処すことができる。

なお、第2条が適用されるためには、犯行者が「自らが儲ける、若しくは別の者に儲けさせる」という意図、又は「他の者に損失を招く、若しくは他の者を損失の危険に曝す」という意図を有していることが構成要件として必要である。

2006年詐欺法第7条

「2006年詐欺法第7条　詐欺に使用するための物品の作成又は提供」では、詐欺行為や詐欺行為の幇助において使用されることを意図して「物品」を作成したり提供したりすること、若しくは詐欺行為において使用される可能性を認識して「物品」を作成したり提供したりすることを禁じている。

「物品」には電子的形式のあらゆるプログラムやデータが含まれる。フィッシングサイト自体も「物品」に含まれると考えられる。また、フィッシングサイトを構築するソフトウェアや、フィッシングメールを送信するソフトウェアも規制の対象となる[28]。

第7条の違反は、即決裁判では12カ月以下の拘禁刑若しくは罰金刑、又はこれらの併科、起訴に基づく有罪判決では10年以下の拘禁刑若しくは罰金刑、又はこれらの併科に処すことができる。

なお、第7条が適用されるためには、犯行者が「それ（物品）が詐欺の過程で、若しくは詐欺との関連で使用する目的で設計若しくは改造されたことを知っている」か、又は「それが詐欺行為、若しくは詐欺行為の幇助に使用されることを意図している」ことが構成要件として必要である。「詐欺」の具体的な意味については、同法の第2条から第4条で規定されている。

（３）サイバーテロ行為

1990年コンピュータ不正使用法第3条

「1990年コンピュータ不正使用法3条　コンピュータの運用その他を損なう意図をもって、又は損なうような無謀さをもって行った無権限の行為」の(1)(2)では、それが無権限の行為であることを認識しながら、意図的にコンピュータの運用を損ねたり、コンピュータ

[27] 2006 年詐欺法の注釈（Explanatory Notes）第 16 項（http://www.legislation.gov.uk/ukpga/2006/35/notes/division/5/2）及び英国検察局の 2006 年詐欺法に関する法的ガイダンス（http://www.cps.gov.uk/legal/d_to_g/fraud_act/）。

[28] 英国検察局の 2006 年詐欺法に関する法的ガイダンス（http://www.cps.gov.uk/legal/d_to_g/fraud_act/）。

内のプログラムやデータへのアクセスを妨げたり、プログラムの運用やデータの信頼性を損なうような行為を禁じている。また同条の(3)では、意図的でなかったとしても、「無謀さ（recklessness）」によって上記のような結果を引き起こす行為も禁じている。

第3条の違反は、即決裁判では12カ月以下の拘禁刑若しくは罰金刑、又はこれらの併科、起訴に基づく有罪判決では10年以下の拘禁刑若しくは罰金刑、又はこれらの併科に処すことができる。

2006年警察司法法による法改正前は、(3)の「無謀さ」に関する規定がなかった[29]ため、DoS攻撃やDDoS攻撃に関して「コンピュータの運用を損ねる意図はなかった」との抗弁が可能であったが、2006年の法改正によりそのような場合でも(3)により有罪とすることが可能となった[30]。

また、コンピュータの運用を損ねたり、コンピュータ内のプログラムやデータへのアクセスを妨げたり、プログラムの運用やデータの信頼性を損ねたりすることには、それらを一時的に行うことも含まれる。すなわち、永続的な損傷や妨害は要件とされない。

なお、1990年コンピュータ不正使用法では、行政機関や重要インフラのシステムに対するサイバーテロ行為に係る特別な規定は存在しない。

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

2000年調査権限規制法

2000年調査権限規制法の第1条において通信傍受は一般原則として禁止されているが、同法の第5条において、「国家の安全のため」「重大な罪（重罪）の予防又は探知のため」「英国の経済的繁栄を保護するため」等の理由がある場合には、内務大臣が発付する令状[31]によ

---

[29] 1989 年にコンピュータ不正使用法が検討されていた際に「無謀さ」についても議論が持ち上がったが、当時は法律に含めることが適切とは考えられなかった。ISSA Journal の記事 “U.K. Cyber-Crime Law Changed”（2007 年 3 月）（http://www.issa.org/Library/Journals/2007/March/Austen%20-%20U.K.%20Cyber-Crime%20Law%20Changed.pdf）。

[30] 2006 年の法改正以前の第 3 条では、コンピュータの運用等を損ねるという犯行者の意図が必要とされたため、DoS 攻撃や DDoS 攻撃を捜査したり訴追したりする際に、様々な問題をもたらした。犯行者がインターネットを通じてこうした行為を行う際に、自分の行為の結果や、個々のシステムへの明示的な影響を知らなかったという弁護が可能であったため、いくつもの事犯が破綻し、若しくは後年には裁判手続きにも進めなくなったりした。ISSA Journal の記事 “U.K. Cyber-Crime Law Changed”（2007 年 3 月）（http://www.issa.org/Library/Journals/2007/March/Austen%20-%20U.K.%20Cyber-Crime%20Law%20Changed.pdf）。

[31] 傍受令状は基本的には内務大臣の署名に基づいて発付されるが、内務大臣が令状発付を明白に許可した事案であって、国際相互援助協定に基づいて外国の機関が援助を要請し、傍受の対象が国外に居ると認められるか、国外の敷地のみで行われる場合には、上級職員

って、電気通信システム（telecommunication system）[32]による伝送の過程における傍受が認められている[33]。

同法の第6条において、傍受令状を申請できる者は、保安局長官、機密情報局長官、政府情報通信本部部長、重大組織犯罪庁長官、首都圏警察長官等に限られている。

傍受の対象となる「重大な罪（重罪）」とは、同法の81条(2)と(3)において、3年以上の拘禁刑に該当すると合理的に期待できる罪である等の規定がなされている。

（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

2000年調査権限規制法

2000年調査権限規制法の第22条において、関係公的機関[34]の官職等を保有している者は、「国家の安全のため」「罪を予防若しくは探知するため、又は秩序違反を阻止するため」「英国の経済的繁栄のため」「公共の安全のため」等の理由があるときには、電気通信事業者（telecommunications operator）[35]に対して通信データ（communications data）の取得、又は取得した通信データの開示を要求することが可能である。

通信データは同法の第21条において、以下のものと規定されている。

- 通信に含まれるトラフィックデータ又は通信に付随するトラフィックデータ[36]
- 電気通信サービス（telecommunications service）[37]又は電気通信システムの利用に関係する情報
- 電気通信サービスの利用者に関して保有するその他の情報

1984年電気通信法第45条

「1984年電気通信法第45条　メッセージその他の開示」において、公的な電気通信システムの運営に従事するものは、一般的には当該システムに関係する電気通信サービスの利用に関する情報を開示することは禁止されているが、裁判所の命令や、2000年調査権限規制法の規定に基づいて発付された令状がある場合には、開示することができる。

の署名に基づいて発付することもできる（2000 年調査権限規制法第 7 条）。

[32] 「２．３（５）節　2000 年調査権限規制法」に記載の横山訳では「遠隔通信システム」と訳されているが、ここでは「電気通信システム」と表記する。

[33] なお、従来の 1985 年通信傍受法は 2000 年調査権限規制法によって改正された。

[34] 2000 年調査権限規制法の第 25 条において、警察、重大組織犯罪庁、スコットランド犯罪薬物取締庁、歳入関税庁、情報機関等と定められている。

[35] 「２．３（５）節　2000 年調査権限規制法」に記載の横山訳では「遠隔通信の管理者」と訳されているが、ここでは「電気通信事業者」と表記する。

[36] トラフィックデータには、「通信の送信先又は発信源の人、装置又は場所を特定するデータ」「通信を伝送する装置を特定するデータ」等が含まれる。

[37] 「２．３（５）節　2000 年調査権限規制法」に記載の横山訳では「遠隔通信業務」と訳されているが、ここでは「電気通信サービス」と表記する。

（３）ログの保存

2001年の米国同時多発テロ事件を受けて、英国では「2001年反テロリズム、犯罪及び安全保障法」が制定され、その中で、内務大臣が通信データの保存に関する実務綱領を作成することが規定された。内務省は2003年に自主的な実務綱領[38]を発表し、2004年1月から施行がされた。同実務綱領においては、英国で公的な電気通信サービスを提供する電気通信事業者[39]はインターネットアクセスに関するデータ（ログ）を6カ月間保存しなければならないと規定されていた[40]。

その後、2004年のマドリッドの列車爆破事件、2005年のロンドン同時テロ事件を受けて、2006年3月にEUデータ保全指令（2006/24/EC）が採択された。これを受けて、英国でも電話通信に係るデータの保存については、内務省の2007年データ保存規則（Data Retention Regulation 2007）で規定がされた。さらに2009年4月2日に、インターネットアクセス、電子メール、インターネットテレフォニー（VoIP）を包含する2009年データ保存規則（Data Retention (EC Directive) Regulation 2009）が策定され、同年の4月6日から施行されている。同規則の第5条では、英国で公的な電気通信サービスを提供する電気通信事業者のデータ保存期間を12カ月と定めている。

ただし、欧州委員会では、EUデータ保全指令（2006/24/EC）の効果を批判する2011年4月18日の同委員会による評価報告書を受けて、同指令の見直し作業に入るとのことである[41]。

---

[38] 英国内務省”RETENTION OF COMMUNICATIONS DATA UNDER Part 11: ANTI-TERRORISM, CRIME & SECURITY ACT 2001, VOLUNTARY CODE OF PRACTICE”　(http://opsi.gov.uk/si/si2003/draft/5b.pdf)。

[39] 同実務綱領では communication service provider と表記されている。

[40] その他、電話通信データ、SMS データ、電子メールデータ等の保存期間についても規定されている。

[41] 欧州委員会の同評価報告書では、データ保存義務は個人のプライバシー権を制限することや、セキュリティ侵害を防ぐための安全保護措置が必要だと述べられているとのことである。OUT-LAW.COM の記事（2011 年 4 月 19 日）（http://www.out-law.com/default.aspx?page=11877)。

２．３　不正アクセス関連法令条文集

（１）1990 年コンピュータ不正使用法

○関連する条項の抜粋訳

1990 年コンピュータ不正使用法第１条　コンピュータ・マテリアルに対する無権限のアクセス

(1) 以下の (a) から (c) に該当する場合は、有罪とする。

(a) コンピュータ内に存するプログラム又はデータへのアクセスを確保する意図で、コンピュータに何らかの機能を実行させた、又はかかるアクセスの確保を可能にさせた場合。

(b) その者が確保しようとしたアクセス、又は確保を可能にしようとしたアクセスが無権限のものである場合。及び、

(c) その者がコンピュータに当該機能を実行させた時点において、当該アクセスが無権限であることを知っていた場合。

(2) 以下のいずれに向けられたものでなくとも、本条の犯罪を構成する意図となる。

(a) 特定のプログラム若しくはデータ。

(b) 特定の種類のプログラム若しくはデータ。又は、

(c) 特定のコンピュータ内に保持されているプログラム若しくはデータ。

(3) 本条に基づいて有罪とされる者には、以下の刑が科せられる。

(a) イングランド及びウェールズにおける即決裁判では、12 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処し、又はこれを併科する。

(b) スコットランドにおける即決裁判では、6 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処し、又はこれを併科する。

(c) 起訴に基づく有罪判決では、2 年以下の拘禁刑、若しくは罰金に処し、又はこれを併科する。

1990 年コンピュータ不正使用法第２条　さらなる犯罪を実行する意図又はさらなる犯罪の実行を幇助する意図でなされる無権限のアクセス

(1) 上記第 1 条の犯罪（「無権限アクセスの犯罪」）を以下のいずれかの意図をもって実行した者は、本条に基づいて有罪とされる。

(a) 本条が適用される犯罪を実行する意図。又は、

(b) かかる犯罪の実行（自らが実行するか他の者が実行するかを問わず）を幇助する意図。

また、その者が実行若しくは幇助しようと意図した犯罪を本条の以下の項では「さらなる犯罪」とする。

(2) 本条は、以下のいずれかの犯罪に適用される。

(a) 刑罰が法律で定められている犯罪。又は、

(b) 21 歳（イングランド及びウェールズに関しては 18 歳）以上で、かつ前科を有しない者に 5 年の拘禁刑を宣告することができる（若しくはイングランド及びウェールズにおいては、1980 年 M1 治安判事裁判所法の第 33 条により課せられる制限事項を別とすればそのように宣告することができる）犯罪。

(3) 本条においては、「さらなる犯罪」が無権限アクセスの犯罪と同じ機会に実行されたか、又はその後の機会に実行されたかは、重要ではない。

(4) 「さらなる犯罪」を実行することが実際には不可能であった場合でも、本条に基づいて有罪となり得る。

(5) 本条に基づいて有罪とされる者には、以下の刑が科せられる。

(a) イングランド及びウェールズにおける即決裁判では、12 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処し、又はこれを併科する。

(b) スコットランドにおける即決裁判では、6 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処し、又はこれを併科する。

(c) 起訴に基づく有罪判決では、5 年以下の拘禁刑、若しくは罰金に処し、又はこれを併科する。

1990 年コンピュータ不正使用法第 3 条　コンピュータの運用その他を損なう意図をもって、又は損なうような無謀さをもって行った無権限の行為

(1) 以下の (a) から (c) に該当する場合は、有罪とする。

(a) コンピュータに関して無権限の行為をなした。

(b) 行為時においてそれが無権限であることを知っていた。及び、

(c) 以下の (2) 項又は (3) 項が該当する。

(2) 本項は、当該行為によって以下のことを意図した場合に適用される。

(a) コンピュータの運用を損なう。

(b) コンピュータ内に保持されているプログラム若しくはデータへのアクセスを妨げる若しくは妨害する。

(c) かかるプログラムの運用若しくはかかるデータの信頼性を損なう。又は、

(d) 上記 (a) から (c) 号に述べたいずれかがなされることを可能にする。

(3) 本項は、当該人物がかかる行為によって無謀にも (reckless) 上記 (2) 項の (a) から (d) 号に述べた事柄が生じさせた場合に適用される。

(4) 上記 (2) 項で言う意図又は上記 (3) 項で言う無謀さ (recklessness) は、以下と関連している必要がない。

(a) 特定のコンピュータ。

(b) 特定のプログラム若しくはデータ。又は、

(c) 特定の種類のプログラム若しくはデータ。

(5) 本条では、以下の (a) から (c) が該当する。

(a) 行為を実行することには、行為を引き起こすことが含まれる。

(b) 「行為」には一連の行為が含まれる。

(c) 損なう、妨げる、若しくは妨害することには、それを一時的に行うことが含まれる。

(6) 本条に基づいて有罪とされる者には、以下の刑が科せられる。

(a) イングランド及びウェールズにおける即決裁判では、12 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処し、又はこれを併科する。

(b) スコットランドにおける即決裁判では、6 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処し、又はこれを併科する。

(c) 起訴に基づく有罪判決では、10 年以下の拘禁刑、若しくは罰金に処し、又はこれを併科する。

1990 年コンピュータ不正使用法第 3A 条　第 1 条又は第 3 条に基づく犯罪に使用するための物品の作成、提供、又は取得

(1) 第 1 条又は第 3 条に基づく犯罪を実行するために、又はかかる実行を幇助するために使用されることを意図して、物品（articles）を作成、改造、提供した、又は提供を申し出た者は、有罪とされる。

(2) 第 1 条又は第 3 条に基づく犯罪を実行するために、又はかかる実行を幇助するために使用され得ると信じて、物品を提供した、又は提供を申し出た者は、有罪とされる。

(3) 第 1 条又は第 3 条に基づく犯罪を実行するために、又はかかる実行を幇助する用途に供されることを目的として物品を取得した者は、有罪とされる。

(4) 本条では、「物品」には電子的形式で保持されるあらゆるプログラム又はデータが含まれる。

(5) 本条に基づいて有罪とされる者には、以下の刑が科せられる。

(a) イングランド及びウェールズにおける即決裁判では、12 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処し、又はこれを併科する。

(b) スコットランドにおける即決裁判では、6 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処し、又はこれを併科する。

(c) 起訴に基づく有罪判決では、2 年以下の拘禁刑、若しくは罰金に処し、又はこれを併科する。

1990 年コンピュータ不正使用法第 4 条　第 1 条から第 3 条までに基づく犯罪の地域的範囲

(1) 本条の以下の規定を除き、以下の (a) 及び (b) は上記第 1 条又は第 3 条に基づく犯罪に関して重要でない。

(a) 犯罪の有罪判決にとってその証明が必要となる行為や出来事が、関係する本国内で発生したかどうか。又は、

(b) かかる行為又は出来事の際に被告人が、関係する本国内にいたかどうか。

(2) 以下の (3) 項に従い、かかる犯罪の場合には、実行された犯罪に関して、事件の状況において国内の司法管轄との重要な関連が少なくとも 1 つは存在していなければならない。

(3) 上記第 2 条に基づく犯罪の訴訟手続きで、かかる趣旨の申し立ての証明において、上記第 1 条に基づく犯罪が成立するために、かかる関連が存在している必要はない。

(4) 以下の第 8 条では、下記の (a) 及び (b) が該当する。

(a) 上記第 1 条に基づく犯罪の場合、かかる関連が確かに存在する。及び、

(b) かかる犯罪が実行されたことが、上記第 2 条に基づく犯罪の訴訟手続きにおいて申し立てられている。

以下の第 8 条に従い、被告人が、関係する本国で発生した場合には第 2 条が適用される犯罪となるような、関係する本国以外の場所で実行又は幇助を意図した事柄が、当該の犯罪であるかのように、上記第 2 条が適用されるものとする。

(5) 本条は、本条を除いて、スコットランドの裁判所によって行使できるいかなる司法管轄をも侵害しない。

(6) この法律において、関係する本国という語が使われている場合は、以下を指している。

(a) この法律をイングランド及びウェールズに適用する場合は、イングランド及びウェールズ。

(b) この法律をスコットランドに適用する場合は、スコットランド。及び、

(c) この法律を北アイルランドに適用する場合は、北アイルランド。

1990 年コンピュータ不正使用法第 5 条　国内の司法管轄との重要な関連

(1) 本条の以下の規定は、上記第 4 条の解釈に適用される。

(2) 第 1 条に基づく犯罪に関して、以下のいずれかが国内の司法管轄との間の重要な関連となる。

(a) コンピュータに当該機能を実行させた行為を被告人が行った時に、被告人が関係する本国にいたこと。又は、

(b) 被告人が当該行為を行うことによって、無権限のアクセスを確保したか若しくは確保を意図した、又は無権限アクセスの確保を可能にしたか若しくは可能にすることを意図したプログラム若しくはデータが入っているコンピュータが、当時、関係する本国にあったこと。

(3) 第 3 条に基づく犯罪に関して、以下のいずれかが国内の司法管轄との間の重要な関連となる。

(a) 被告人が無権限の行為を行った（若しくはかかる行為を引き起こした）時に、関係する本国にいたこと。又は、

(b) 無権限の行為が、関係する本国にあるコンピュータに関して行われたこと。

1990 年コンピュータ不正使用法第 8 条　他の法律との関係

（中略）

(3) ある者が計画していたことが現行法の下での犯罪の実行を引き起こしうるものであり、当該犯罪の全部又は一部を実行することが意図されていた場合にのみ、1981 年犯罪未遂法第 1 条（1A）項又は本法第 7 条（4）項に基づいて有罪となる。

（以下略）

1990 年コンピュータ不正使用法第 17 条　解釈

(1) 本条の以下の規定は、この法律の解釈に適用される。

(2) コンピュータに何らかの機能を実行させることで以下のいずれかを行った場合、コンピュータ内に存するプログラム又はデータへのアクセスを確保したことになる。

(a) プログラム若しくはデータを改変若しくは消去する。

(b) それを保持している記憶媒体とは別の記憶媒体に、若しくはそれを保持している記憶媒体内の別の場所にコピー若しくは移動する。

(c) それを使用する。又は、

(d) それを保持しているコンピュータから出力する（表示させるか、それ以外の方法によるかは問わない）。

並びに、プログラム若しくはデータへのアクセス（及びかかるアクセスを確保する、又はかかるアクセスの確保を可能にする意図）は、しかるべく解釈されるものとする。

(3) 上記（2）項（c）号において、コンピュータに実行させる機能により、以下のいずれかが実行された場合、又は該当する場合、その者はプログラムを使用したことになる。

(a) プログラムを実行させる。又は、

(b) その機能自体がプログラムの機能である。

(4) 上記（2）項（d）号において、

(a) プログラムを構成する取扱説明が出力された場合、プログラムが出力されたことになる。及び、

(b) かかる取扱説明若しくはその他のデータが出力される形式（及び、特に、取扱説明の場合は実行可能な形式かどうか、若しくはデータの場合はコンピュータによる処理が可能な形式かどうか）は重要でない。

(5) 以下の（a）及び（b）が該当する場合、コンピュータ内に存するプログラム又はデータに誰がどんな種類のアクセスを行った場合も、無権限であるとされる。

(a) その人物が、プログラム又はデータに対する当該種類のアクセスを制御する権限を有さない。及び、

(b) その人物が、権限を有する人物から、プログラム又はデータに対する当該種類のアクセスを行う承諾を得ていない。但し、本項は第 10 条の制約を受ける。

(6) コンピュータ内に存するプログラム又はデータには、暫定的にコンピュータ内にあるリ

ムーバブル記憶媒体内に存するプログラム又はデータが含まれる。また、コンピュータは、かかる媒体内に存するプログラム又はデータを格納しているものと見なされる。
(7)　（2006 年警察司法法によって削除された）
(8) 行為者（又は当該行為を引き起こした者）が以下に該当する場合、コンピュータとの関連で行われた行為は無権限である。
(a) 自分自身がコンピュータの責任者ではなく、当該行為の実行を許可してよいかどうかを判断する権限を有する人物ではない。
(b) かかる人物から行為の承諾を得ていない。
本項で「行為」という場合には、一連の行為が含まれる。
(9) 関係する本国という場合は、上記第 4 条 (6) 項に基づいて解釈するものとする。
(10) プログラムには、プログラムの部分が含まれる。

（２）1981 年犯罪未遂法

○関連する条項の抜粋訳

1981 年犯罪未遂法第 1 条　犯罪実行の未遂
(1) 本条が適用される犯罪を行うことを意図して、当該犯罪実行のための単なる準備以上の行為（act）を行った者は、当該犯罪の未遂罪で有罪とする。
(1A) 1990 年コンピュータ不正使用法第 8 条（他の法律との関係）に従って本項がある行為（act）に適用される場合には、当該行為（act）を行った者が計画していたことは本条が適用される犯罪として扱うものとする。
(1B) 本条 (1A) 項は以下の(a)と(b)を満たす行為（act）に適用される。
(a) 当該行為が、イングランド及びウェールズで行われた。及び、
(b) 1990 年コンピュータ不正使用法第 3 条の下での犯罪を実行するための単なる準備以上の行為として本条 (1) 項に該当しうるものであり、かつ当該犯罪が達成された場合にそれがイングランド及びウェールズで審理可能な犯罪ではないという事実が存在しない。
(2) 当該犯罪の実行が不可能であったとしても、本条が適用される犯罪未遂罪で有罪となりうる。
(3) （略）
(4) 本条は、以下の場合を除き、それが達成された場合にはイングランド及びウェールズで起訴可能ないかなる犯罪にも適用される。
(a) 共同謀議（慣習法、1977 年刑法第 1 条又は他の法律におけるもの）。
(b) ある犯罪実行の幇助、扇動、助言、斡旋又は教唆。
(c) 1967 年刑法の第 4 条 (1) 項（犯行者の援助）又は第 5 条 (1) 項（逮捕可能な犯罪に

関する情報の非開示に対する対価の受領、又は受領の同意)。

1981 年犯罪未遂法第 4 条　裁判及び罰則

(1) 第 1 条の下で犯罪実行の未遂で有罪な者は、

(a) 未遂であった犯罪が殺人又は法律で刑罰が固定されているその他の犯罪の場合には、起訴に基づく有罪判決で無期拘禁刑に処すことができる。

(b) 未遂であった犯罪が起訴可能なものであるが (a) 号に該当しない場合には、起訴に基づく有罪判決で、当該犯罪の起訴に基づく有罪判決で処すことが可能ないかなる刑罰にも処すことができる。

(c) 未遂であった犯罪が即決裁判でも正式起訴でもいずれでも審理できる犯罪である場合、当該犯罪の即決裁判で処すことが可能ないかなる刑罰にも処すことができる。

(2) （以下略）

（３）1998 年データ保護法

○関連する条項の抜粋訳

1998 年データ保護法第 1 条　基本的な解釈規定

(1) この法律では、文脈上他の意味に解すべき場合を除き、

（中略）

「データ管理者」とは、(4) 項に従い、個人データが処理される、又は処理されるべき目的及び方法を（単独で、又は他の者たちと共同で）決定する者を意味する。

（中略）

「個人データ」とは、以下の (a) 又は (b) によって識別することが可能な、生存する個人に関するデータを意味する。

(a) 当該データ。又は

(b) 当該データ及び、データ管理者が保有している他の情報若しくはデータ管理者が保有する可能性のある他の情報。

また、「個人データ」には当該個人に関する意見の表出、及び当該個人に関するデータ管理者又はその他の者の意図の表示を含む。

（中略）

(4) 法令によって、又は法令に基づいて処理することが要求されている目的のみのために個人データが処理される場合、かかる法令によって、又はかかる法令に基づいてデータを処理する義務を課せられる人物が、この法律上、データ管理者とされる。

（以下略）

1998 年データ保護法第 55 条　個人データの非合法的取得、その他

(1) データ管理者の承諾（consent）なく、以下の (a) 又は (b) のいずれも故意に又は無謀に行ってはならない。

(a) 個人データ、若しくは個人データに含まれている情報を取得若しくは開示すること。又は、

(b) 個人データに含まれている情報の他人への開示を斡旋すること。

(2) 以下の (a) から (d) を示す人物には、(1) 項は適用されない。

(a) 取得、開示、若しくは斡旋が以下の (i) 又は (ii) の条件を満たしていること。

(i) 犯罪防止若しくは捜査上必要であった。又は、

(ii) 法令により若しくは法令に基づいて、法の原則により、若しくは裁判所の指図により、要求されたか、若しくは許可された。

(b) 当該人物が、データ若しくは情報を取得若しくは開示する権利、若しくは、場合に応じて、他人に情報開示を斡旋する権利を法律に基づいて有しているという合理的な信念に基づいて行動したこと。

(c) データ管理者がかかる取得、開示、若しくは斡旋について、及びその事情について知っていたならば、データ管理者の承諾が得られたであろうとの合理的な信念に基づいて行動したこと。又は、

(d) 特定の状況において、かかる取得、開示、若しくは斡旋が公益にかなうとして正当と認められたこと。

(3) (1) 項に違反する者は有罪とされる。

(4) (1) 項に違反して取得した個人データを販売した場合、個人データの販売者は有罪とされる。

(5) 以下の (a) 又は (b) に該当する場合、個人データの販売を申し出た者は有罪とされる。

(a) (1) 項に違反して当該データを取得した。又は、

(b) 後に同項に違反して当該データを取得した。

(6) (5) 項において、個人データが売り物である、又は売り物である可能性があると示唆する広告は、かかるデータを販売することの申し出である。

(7) 第 1 条 (2) 項は、本条には適用されない。また、(4) から (6) 項においては、「個人データ」には個人データから抽出された情報も含まれる。

(8) 本条における個人データには、第 28 条又は第 33 条 A によって本条から免除されている個人データは含まれない。

1998 年データ保護法第 60 条　起訴及び処罰

（中略）

(2) 第 54 条 A 及び附則 9 項 12 号を除き、この法律の規定に基づいて有罪とされる者には、

以下の (a) 又は (b) の刑が科せられる。
(a) 即決裁判では、法令で定める限度を超えない罰金。又は、
(b) 起訴に基づく有罪判決では、罰金。
（以下略）

（４）2006 年詐欺法

○関連する条項の抜粋訳

2006 年詐欺法第 1 条　詐欺

(1) 以下の (2) 項の (a)、(b) 又は (c) に違反する者は、詐欺罪で有罪とする。((2) 項は、当該犯罪を実行する異なる方法を規定する。)
(2) 以下が該当する。
(a) 第 2 条（虚偽の表明による詐欺)。
(b) 第 3 条（情報を開示しないことによる詐欺)。及び、
(c) 第 4 条（地位の濫用による詐欺)。
(3) 詐欺罪で有罪とされる者には、以下の刑が科せられる。
(a) 即決裁判では、12 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処し、又はこれを併科する。
(b) 起訴に基づく有罪判決では、10 年以下の拘禁刑、若しくは罰金に処し、又はこれを併科する。
(4) (3) 項 (a) 号は、北アイルランドに関しては、12 カ月とされている部分が 6 カ月とされているかのように読み替えて適用される。

2006 年詐欺法第 2 条　虚偽の表明による詐欺

(1) 以下の (a) 及び (b) に該当する者は、本条に違反している。
(a) 不正直に虚偽の表明を行った場合。及び、
(b) 表明を行うことにより、以下の (i) 又は (ii) を意図した場合。
(i) 自らが儲けること、若しくは別の者に儲けさせること。又は、
(ii) 他の者に損失を招くこと、若しくは他の者を損失の危険に曝すこと。
(2) 表明は、以下の (a) 及び (b) が該当する場合に虚偽である。
(a) 真実でない、又は惑わせる。及び、
(b) 表明を行う者が、その表明が真実でない、若しくは惑わせること、又は真実でない、若しくは惑わせる可能性があることを知っている。
(3) 「表明」とは、次の者の心理状態の表明を含め、事実又は法に関する表明を意味する。

(a) 表明を行う者。又は、

(b) その他の者。

(4) 表明は、明示的か黙示的かを問わない。

(5) 本条において、表明（又はそれを暗示するもの）が、通信を受ける、伝達する、又はそれに応答する（人間の介入の有無を問わない）ように設計されたシステム又は装置に対して、形式を問わず、送達された場合に、表明がなされたと見なすことができる。

2006 年詐欺法第 3 条　情報を開示しないことによる詐欺

以下の (a) 及び (b) に該当する者は、本条に違反している。

(a) 開示すべき法的義務のある情報を不正直にも他人に開示しなかった場合。及び

(b) 当該情報を開示しないことによって、以下の (i) 又は (ii) を意図した場合。

(i) 自らが儲けること、若しくは別の者に儲けさせること。又は、

(ii) 他の者に損失を招くこと、若しくは他の者を損失の危険に曝すこと。

2006 年詐欺法第 4 条　地位の濫用による詐欺

(1) 以下の (a)、(b) 及び (c) に該当する者は、本条に違反している。

(a) 他人の金銭的利益を保護すること、又は他人の金銭的利益に反して行動しないことが期待される地位に就いている場合。

(b) 不正直に当該地位を濫用した場合。

(c) 当該地位の濫用によって、以下の (i) 又は (ii) を意図した場合。

(i) 自らが儲けること、若しくは別の者に儲けさせること。又は、

(ii) 他の者に損失を招くこと、若しくは他の者を損失の危険に曝すこと。

(2) ある者の振る舞い（conduct）が行為ではなくてむしろ不作為（omission）から成る場合であっても、地位の濫用とみなすことができる。

2006 年詐欺法第 6 条　詐欺に使用するための物品の所持その他

(1) 詐欺の過程で又は詐欺との関連で使用するための物品を所持しているか、又は管理下に置いている場合、その者は有罪とされる。

(2) 本条に基づいて有罪とされる者には、以下の刑が科せられる。

(a) 即決裁判では、12 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処する（又はこれを併科する）。

(b) 起訴に基づく有罪判決では、5 年以下の拘禁刑、若しくは罰金に処する（又はこれを併科する）。

(3) (2) 項 (a) 号は、北アイルランドに関しては、12 カ月とされている部分が 6 カ月とされているかのように読み替えて適用される。

2006 年詐欺法第 7 条 詐欺に使用するための物品の作成又は提供

(1) 以下の (a) 又は (b) が該当する場合、物品を作成、改造、提供した、又は提供を申し出た者は、有罪とされる。

(a) それが詐欺の過程で、若しくは詐欺との関連で使用する目的で設計若しくは改造されたことを知っている。

(b) それが詐欺行為、若しくは詐欺行為の幇助に使用されることを意図している。

(2) 本条に基づいて有罪とされる者には、以下の刑が科せられる。

(a) 即決裁判では、12 カ月以下の拘禁刑、若しくは法令で定める限度を超えない罰金に処する（又はこれを併科する）。

(b) 起訴に基づく有罪判決では、10 年以下の拘禁刑、若しくは罰金に処する（又はこれを併科する）。

(3) (2) 項 (a) 号は、北アイルランドに関しては、12 カ月とされている部分が 6 カ月とされているかのように読み替えて適用される。

2006 年詐欺法第 8 条 「物品」

(1) 以下において、

(a) 第 6 条及び第 7 条、並びに、

(b) (2) 項に挙げられている規定、但し、詐欺の過程で、又は詐欺との関連で使用する物品に関連する限りにおいて、

「物品」には電子的形式で保持されるあらゆるプログラム又はデータが含まれる。

(2)（略）

（５）1968 年窃盗法

○関連する条項の抜粋訳

1968 年窃盗法第 1 条 窃盗の基本的定義

(1) 他人が所有する財産を恒久的に奪う意図をもって不正直に自分のものにする者は、窃盗の罪に問われる。また、「窃盗犯」及び「盗み」という語はこれに従って解釈される。

(2) かかる盗みが利益を目的に行われたか、又は窃盗犯自身の利益のために行われたかは、重要でない。

（以下略）

1968 年窃盗法第 4 条 「財産」

(1)「財産」には、金銭及び、不動産、動産の違いを問わず、債権及びその他の無形財産を

含め、その他すべての財産が含まれる。
（以下略）

（６）2000 年調査権限規制法[42]

○関連する条項の抜粋訳

2000 年調査権限規制法第 1 条　不法傍受

(1) 何人も、連合王国の場所において、次の各号の 1 により、ある者が通信の伝送の過程で、故意に、かつ合法的な許可を得ないで通信を傍受することをもって、罪とするものとする。

(a) 公的な郵便業務

(b) 公的な遠隔通信システム

(2) 何人も、連合王国の場所において、私的な遠隔通信システムによる通信の伝送の過程で、次の各号の両者により、通信を傍受することをもって、罪とする。

(a) 故意に、かつ合法的な許可を得ないで

(b) 第 6 項により、本人の行為が本条に基づく刑事責任を免れる状況にある場合を除いて

(3) 私的な遠隔通信システムの管理又は使用を規制する権利を有する者の明示又は黙示の同意により、又は同意を得ないで、連合王国の場所において行われる通信の傍受が、合法的な許可を得ておらず、かつ次の各号の 1 に該当する傍受であったときは、当該傍受は、通信の送信者、受信者又は想定受信者の告訴又は主張をもって訴追することができるものとする。

(a) 当該の私的な遠隔通信システムによる通信の伝送の過程における、通信の傍受

(b) 私的な遠隔通信システム中に含まれる装置への、又は装置からの、公的な遠隔通信システムによる通信の伝送の過程における、通信の傍受

(4) 連合王国が次の各号のすべてに該当する国際協定の当事国であるときは、合法的な許可を得た場合を除いて、連合王国外の国又は領域の権限を有する機関に対して、連合王国内に居る者に代わって当該協定に従った援助を求める要請が行われることがないことを確保することをもって、国務大臣の義務とする。

(a) 通信の傍受に関連する相互援助、又は通信の傍受の形式における相互援助の提供に関する国際協定

(b) 援助が与えられる事案において、令状、命令又はこれらに相当する文書の発付を要求する国際協定

(c) 本項の適用上、国務大臣が下した命令をもって指定された国際協定

(5) 次の各号の 1 に該当するとき、及びその場合に限って、行為は、本条の適用上、合法的

---

[42] 2000 年調査権限規制法の日本語訳については、横山潔訳「イギリス『2000 年調査権限規制法』」（横山潔「イギリス『調査権限規制法』の成立」『外国の立法 214』（2002 年 11 月））（http://www.ndl.go.jp/jp/data/publication/legis/214/21402.pdf）、p53～54、p59～61、p73～77、p128 より引用した。ただし、【 】で閉じた箇所については、左記論文掲載時点から法令条文が改定された箇所を調査実施機関にて翻訳したものである。

な許可を有するものとし、a 号又は b 号によって、本条の適用上合法的な許可を有する行為は（本条で禁止した行為であると否とを問わず)、他のすべての規定の適用上も、合法とみなすものとする。

(a) 行為が第３条又は第４条によって、又はこれらに基づいて許可されたこと

(b) 行為が第５条に基づく令状（「傍受令状」（an interception warrant））に従って行われたこと

(c) 行為が、蓄積された通信に関して、（本条とは別に）情報を取得するために執行されるか、又は文書その他の物を占有するために執行される制定法上の権限の執行中の行為であること

(6) 何人も、次の各号の１に該当するときは、私的な遠隔通信システムによる通信の伝送の過程で、通信の傍受を行った状況は、この者の行為が第２項に基づく刑事責任を免れる状況とする。

(a) 当該システムの管理又は使用を規制する権利を有する者であるとき

(b) 傍受を行うために、当該権利を有する者の明示又は黙示の同意を得ているとき

(7) 第１項又は第２項に基づく罪により有罪となった者は、次の各号の定めるところに従う。

(a) 正式起訴に基づく有罪宣告により、２年以下の拘禁若しくは罰金に処し、又は両者を併科する。

(b) 略式起訴に基づく有罪宣告により、法定上限以下の罰金に処する。

(8) 本条による罪に該当する罪の手続は、次の各号による場合を除いて、開始してはならない。

(a) イングランド及びウェールズ地方にあっては、公訴局長官の同意によるか、又は同意を得た場合

(b) 北アイルランド地方にあっては、北アイルランド公訴局長官の同意によるか、又は同意を得た場合

2000 年調査権限規制法第 5 条　令状を伴う傍受

(1) 本節の次に掲げる規定に従うことを条件にして、国務大臣は、令状の名宛人が、当該令状中に定めることができる行為によって、次の各号に定める事項の１以上を確保することを許可又は要求する令状を発付することができる。

(a) 郵便業務による、又は令状中に定める通信の遠隔通信システムによる伝送の過程における傍受

(b) 通信の傍受に関連する、又は通信の傍受の形式における、令状中に定めることができる援助の提供を求める、国際相互援助協定に従った要請

(c) 通信の傍受に関連する、又は通信の傍受の形式における、令状中に定めることができる援助の、連合王国外の国又は領域の権限を有する機関への、国際相互援助協定に従った提供

(d) 令状によって許可又は要求された傍受によって取得した被傍受資料の、令状中に定めることができる方法における開示、及び関係する通信データの、令状中に定めることができる方法における開示

(2) 国務大臣が次の各号の両者を信じなかったときは、国務大臣は、傍受令状を発付してはならない。

(a) 第３項に該当する理由により、当該令状が必要であること

(b) 当該令状によって許可された行為が、当該行為によって達成することが求められる事項に見合っていること

(3) 本条の次に掲げる規定に従うことを条件にして、次の各号の１により、令状が必要であるときは、前項 a 号中の、第３項に該当する理由により、令状が必要であるものとする。

(a) 国家の安全のため

(b) 重大な罪の予防又は探知のため

(c) 連合王国の経済的繁栄を保護するため

(d) 国務大臣が b 号によって令状を発付すると思料する状況に相当する、と自己が認める状況において、国際相互援助協定を執行するため

(4) 令状の事案において、第２項の要求が満たされているか否かを考査するに当たって考慮すべき事項には、当該令状に基づいて取得することが必要と思料される情報が、他の方法によって合理的に取得することができるか否かが含まれる。

(5) 取得することが必要と思料される情報が、イギリス諸島外の者の行為又はその意思に関係する情報でないときは、令状が、第３項 c 号に該当する理由により必要なものとして考慮してはならない。

(6) 傍受令状によって許可される行為には、次の各号に掲げる行為のすべてが含まれるものとみなされるものとする。

(a) 令状によって明白に許可又は要求される事項を行うために引き受けることが必要な（令状によって特定されない通信の傍受を含む）すべての行為

(b) 関係する通信データを取得するための行為

(c) 令状の執行を伴って援助が提供されるように令状の名宛人が課する要求、又はこの者のために課する要求を遵守した行為に該当する人の行為

2000 年調査権限規制法第 6 条　傍受令状の発付を求める申請

(1) 第２項に掲げる者又はこの者に代わる者が行う申請による場合を除いて、傍受令状を発付してはならない。

(2) 傍受令状を申請する者は次のとおり。

(a) 保安局長官（the Director-General of the Security Service）

(b) 機密情報局長官（the Chief of the Secret Intelligence Service）

(c) 政府情報通信本部部長（the Director of GCHQ）

(d) 【重大組織犯罪庁】長官（the Director General of the 【Serious Organised Crime Agency】）

【(da) スコットランド犯罪薬物取締庁長官（the Director General of the Scottish Crime and Drug Enforcement Agency）】

(e) 首都圏警察長官（the Commissioner of Police of the Metropolitan ）

(f) 王立アルスター警察隊隊長（the Chief Constable of the Royal Ulster Constabulary）

(g) 1967 年警察（スコットランド）法［1967 c.77］第１条に基づいて、又は同条によって維持される警察の警察署長

(h) 【歳入関税庁コミッショナー（the Commissioners for Her Majesty's Revenue and Customs）】

(i) 国防情報部部長（the Chief of Defence Intelligence）

(j) 国際相互援助協定の適用上、連合王国外の国又は領域の権限を有する機関に該当する者

(3) 傍受令状の発付を求める申請は、官吏の官職を保有する者が行う場合を除いて、前項【の a 号、b 号、c 号、e 号、f 号、g 号、h 号、i 号又は j 号】に掲げる者に代わって行ってはならない。

2000 年調査権限規制法第 7 条　令状の発付

(1) 傍受令状は、次の各号の１に該当する場合を除いて、発付してはならない。

(a) 国務大臣の署名に基づく場合

(b) 第２項に該当する事案において、上級職員の署名に基づく場合

(2) 前項 b 号中の、第２項に該当する事案とは、次の各号の両者に該当する事案をいう。

(a) 国務大臣自身が当該事案において令状の発付を明白に許可した緊急の事案

(b) 国際相互援助協定に基づいて、連合王国外の国又は領域の権限を有する機関が行う援助を求める要請のために、令状が関係する事案であって、かつ次の１に該当する事案

(i) 傍受の対象が連合王国外に居ると認められる事案

(ii) 令状に関係する傍受が、連合王国外の敷地のみに関して行われる事案

(3) 傍受令状は、次の各号の定めるところに従う。

(a) 第６条第２項に該当する、令状の申請を行った者、又はこの者に代わって令状の申請を行った者を、名宛人としなければならない。

(b) 上級職員の署名に基づいて発付される令状の事案にあっては、申請可能な事項に応じて、次の両者を含んでいなければならない。

(i) 第４項に掲げる表明の１

(ii) 傍受令状が第４項 b 号に掲げる表明を含んでいるときは、第５項に掲げる表明の１

(4) 前項 b 号 i にいう表明とは、次に掲げる表明をいう。

(a) 当該事案が、令状の発付を国務大臣自身が明白に許可した緊急の事案である旨の表明

(b) 国際相互援助協定に基づいて、連合王国外の国又は領域の権限を有する機関が行う、援助を求める要請のために令状が発付される旨の表明

(5) 第３項ｂ号 ii にいう表明とは、次に掲げる表明をいう。

(a) 傍受の対象が連合王国外に居ると認める旨の表明

(b) 令状に関係する傍受が連合王国外の敷地のみに関して行われる旨の表明

2000 年調査権限規制法第 21 条　通信データの合法的開示及び獲得

(1) 本節の規定は、次の各号の両者に適用する。

(a) 郵便業務又は遠隔通信システムによる通信の伝送の過程における通信の傍受中に含まれる行為を除く、通信データの取得のための当該業務又はシステムに関する行為

(b) 通信データの人への開示

(2) 次の各号の両者に該当するときは、本節の規定が適用される行為は、すべての規定の適用上合法とするものとする。

(a) 本節の規定が適用される行為が、本節に基づいて付与された許可、又は行われた通知によって、人が従事することの許可又は要求される行為であるとき

(b) 当該行為が、当該許可又は要求に従った行為又はこれを遵守した行為であるとき

(3) 何人も、次の各号の両者に該当する自己の行為について、民事責任に服さないものとする。

(a) 前項によって合法的な行為に付随する自己の行為

(b) それ自体、関係する制定法・制定法規に基づいて許可又は令状を付与することができる行為でない場合において、関係する事案にあって許可又は令状を求めることが合理的に期待されると思料される自己の行為

(4) 本節中の「通信データ」（communication data）とは、次の各号に掲げるトラフィックデータ又は情報をいう。

(a) 郵便業務又は遠隔通信システムによって通信を伝送するか、又は伝送することができる場合における当該業務又はシステムのために（送信者によると、その他によるとを問わず）通信に含まれるトラフィックデータ又は通信に付随するトラフィックデータ

(b) （前号に該当する情報とは別に）通信の内容を含まず、かつ次の各号の１に掲げる業務又はシステムの人による利用に関係する情報

(i) 郵便業務又は遠隔通信業務

(ii) 遠隔通信業務の人への提供又は当該業務の人による利用に関連する、遠隔通信システム

(c) 郵便業務又は遠隔通信業務が提供される者に関して、当該業務を提供する者が保有又は取得する、a 号又は前号に該当しない情報

(5) 本条中の「関係する制定法・制定法規」（relevant enactment）とは、次の各号の１に掲げる制定法・制定法規をいう。

(a) 本法中に含まれる制定法・制定法規

(b) 1994 年情報機関法［1994 c.13］第５条（情報機関のための令状）

(c) 1997 年警察法［1997 c.50］第３章（警察及び【歳入関税】吏の権限）中に含まれる制定法・制定法規

(6) 通信に関して、本条中の「トラフィックデータ」（traffic date）とは、次の各号に掲げるデータのすべてをいうが、この文言には、コンピューターファイル又はコンピュータープログラムが蓄積されている装置によって当該ファイル又はプログラムが特定される範囲にのみ、当該通信によって取得又は処理される当該ファイル又はプログラムのアクセスを特定するデータが含まれる。

(a) 通信を伝送し、又は伝送することができる送信先又は発信源たる人、装置又は場所を特定し、又は特定することを目的とするデータ

(b) 通信を伝送し、又は伝送することができる装置を特定若しくは選択し、又は特定若しくは選択することを目的とするデータ

(c) 通信の伝送（の全部又は一部）を有効にする遠隔通信システムのために使用する装置を作動させるための信号を含むデータ

(d) 当該データ又はその他のデータを、特定の通信の中に含まれるデータ又は当該通信に付随するデータとして特定するデータ

(7) 本条において、次の各号の定めるところに従うものとし、かつ郵便物に関して、本条中の「データ」（data）とは、郵便物の外側に記載された事項をいう。

(a) 装置を作動させるための信号を含むトラフィックデータに関して、通信を伝送し、又は伝送することができる遠隔通信システムには、当該装置が内蔵されている遠隔通信システムが含まれる。

(b) 通信に付随するトラフィックデータには、論理的に相互に関連するデータ及び通信が含まれる。

2000 年調査権限規制法第 22 条　通信データの取得及び開示

(1) 第２項に該当する理由により通信データを取得することが必要である、と本節の適用上指名された者が信じたときは、本条の規定を適用する。

(2) 次の各号の１により通信データを取得することが必要であるときは、前項中の、第２項に該当する理由により通信データを取得することが必要であるものとする。

(a) 国家の安全のため

(b) 罪を予防若しくは探知するため、又は秩序違反を阻止するため

(c) 連合王国の経済的繁栄のため

(d) 公共の安全のため

(e) 公衆衛生を保護するため

(f) 政府部局へ支払うべき租税、関税、割当金その他の課税、分担金又は負担金を査定又

は徴収するため

(g) 非常の際に、死亡、傷害若しくは人の身体的若しくは精神的健康への危害を阻止するため、又は障害若しくは人の身体的若しくは精神的健康への危害を軽減するため

(h) 国務大臣が下した命令をもって、本条の適用上定めた（a 号から前号までの規定に該当しない）目的のため

(3) 第 5 項に従うことを条件にして、指定された者は、指定された者と同一の関係公的機関の官職、階級又は地位を保有している者が本節の規定を適用する行為に従事する許可を付与することができる。

【(3A) 以下の a 号及び b 号が該当する場合、第 3B 項が適用される。

(a) 警察の官職、階級又は地位を参考にして指定された者である

(b) その警察の警察官の長が、1996 年警察法第 23 条第 1 項に基づいて、単一又は複数の他の警察の警察官の長との間で契約を結んでいる

(3B) 指定された者は、協力部隊で官職、階級又は地位を保有している者に、本節を適用する行為に従事する許可を付与することができる。

(3C) 第 3B 項において、警察は以下の a 号及び b 号の条件が満たされる場合に協力部隊とされる。

(a) その警察の警察官の長が、第 3A 項 b 号に述べた契約の当事者である

(b) そこで官職、階級又は地位を保有している者が、契約条件によって、指定された者によって承認を受けることを許可されている

(3D) 第 3A 項から第 3C 項における警察とは、以下を指している。

(a) 1996 年警察法第 2 条に基づいて維持される警察（ロンドンを除くイングランド及びウェールズ地方の警察）

(b) 首都圏警察

(c) ロンドン市警

(3E) 以下の a 号及び b 号が該当する場合、**第** 3F 項が適用される。

(a) スコットランド警察の官職、階級又は地位を参考にして指定された者である

(b) その警察の署長が、1967 年警察（スコットランド）法第 12 条第 1 項に基づいて、単一又は複数の他のスコットランド警察の署長との間で契約を結んでいる

(3F) 指定された者は、協力部隊で官職、階級又は地位を保有している者に、本節を適用する行為に従事する許可を付与することができる。

(3G) 第 3F 項において、スコットランド警察は以下の a 号及び b 号の条件が満たされる場合に協力部隊とされる。

(a) その警察の署長が、第 3E 項 b 号に述べた契約の当事者である

(b) そこで官職、階級又は地位を保有している者が、契約条件によって、指定された者によって承認を受けることを許可されている

(3H) 第 3E 項から第 3G 項におけるスコットランド警察とは、1967 年警察（スコットラン

ド）法第 1 条に基づいて、又は同条の効力によって維持される警察である。
(3I) 第 3B 項及び第 3F 項は第 5 項に従う。】
(4) 第 5 項に従うことを条件にして、郵便又は遠隔通信の管理者が通信データを占有しているか、占有することができる、若しくは取得することができる、と指定された者が認めたときは、指定された者は、郵便又は遠隔通信の管理者に対し、この者への通知をもって、次の各号に掲げる行為の両者を要求することができる。
(a) 当該管理者が未だ当該データを占有していないときは、当該データを取得すること
(b) すべての事案において、当該管理者が占有するデータ又はその後に取得したデータのすべてを開示すること
(5) 第 3 項【、第 3 B 項若しくは第 3 F 項】に基づく許可、又は第 4 項に基づく通知をもって許可又は要求される行為により関係するデータを取得することが、当該データを取得することによって達成することが求められる事項に見合っていない、と指定された者が信じたときは、指定された者は、当該許可を付与し、又は当該通知を行ってはならない。
(6) 第 4 項に基づいて郵便又は遠隔通信の管理者へ行った通知の要求を遵守することをもって、当該管理者の義務とするものとする。
(7) 前項により義務を負担する者は、自己の負担が合理的に実施可能でない義務を遵守してある事項を行うように要求されてはならない。
(8) 第 6 項によって課せられる義務は、国務大臣による差止命令を求める民事手続、1988 年民事上級裁判所法［1988 c.36］第 45 条に基づく制定法上の義務の特別執行を求める民事手続又はその他の適切な救済を求める民事手続によって強制することができるものとする。
(9) 第 2 項 h 号に基づく命令の草案が未だ議会で提出されておらず、かつ各院の決議によって承認されなかったときは、国務大臣は、当該命令を下してはならない。

2000 年調査権限規制法第 25 条　第 2 節の解釈

(1) 本節において
「通信データ」（communications data）は、第 21 条第 4 項によって付与される意味を有する。
「指名された」（designated）は、第 2 項に従って解釈するものとする。
「郵便管理者又は遠隔通信管理者」（postal or telecommunications operator）
とは、郵便業務又は遠隔通信業務を提供する者をいう。
「関係公的機関」（relevant public authority）とは、（第 4 項に従うことを条件にして）次に掲げる機関をいう。
(a) 警察
(b) 【重大組織犯罪庁】
(c) 【スコットランド犯罪薬物取締庁】
(d) 【歳入関税庁】

(e) 情報機関

(f) 本項の適用上、国務大臣が下す命令をもって定めることができる、a 号から前号までに該当しない公的機関

(2) 第３項に従うことを条件にして、本節の適用上指名された者は、本項の適用上国務大臣が下す命令をもって定める、関係公的機関の官職、階級又は地位を保有する者とする。

(3) 国務大臣は、命令をもって、次の各号の両者に対し制限を課することができる。

(a) 所定の公的機関の官職、階級又は地位を保有する者が付与し、又は行うことができる、本節に基づく許可又は通知

(b) この者が許可を付与し、又は通知を行うことができる状況又は目的

【(3A) 本節において、重大組織犯罪庁に官職又は地位を有する個人には、当該機関の職員が含まれる。

(4) 国務大臣は、命令をもって、以下の a 号及び b 号を行うことができる。

(a) 本節の適用上、当分の間、関係公的機関に該当する者のリストからある者を排除すること

(b) 必要又は得策であるとの自身の判断により、この法令又はその他の法令に、かかる間接的修正、廃止、又は撤回を行うこと

(5) 国務大臣は、本条に基づいて以下の号又は b 号の命令を下してはならない。

(a) 本節の適用上、当分の間関係公的機関に該当する者のリストにある者を追加すること

(b) 第 4 項 b 号に基づいて、法律の条項を改正又は廃止すること

但し、かかる命令の草案が議会に提出され、両院の決議によって承認された場合はこの限りではない。】

2000 年調査権限規制法第 25 条　第 2 節の解釈

（中略）

(2) 本法において

(a) 罪は、１以上の刑事上の罪を構成する行為、又は連合王国の１地域で行われたとすれば、１以上の刑事上の罪を構成すると思料される行為に該当するか、又は当該行為に相当する行為とする。

(b) 重大な罪は、第３項 a 号又は b 号中の審査基準を満たす罪とする。

(3) 前項 b 号中の、第３項 a 号又は b 号中の審査基準とは、次の各号の両者をいう。

(a) 当該行為によって構成されるか、又は構成されると思料される罪又は複数の罪の１が、21 歳以上で、前に有罪宣告を受けたことのない者に対し、３年以上の拘禁を言い渡すことを合理的に期待することができる罪であること

(b) 当該行為が暴力の行使を含んでおり、重大な金銭的利得を生じさせ、又は共通の目的を追求する多数の者による行為であること

（以下略）

（７）1984 年電気通信法

○関連する条項の抜粋訳

1984 年電気通信法第 45 条　メッセージその他の開示

(1) 公的電気通信システムの運営に従事する者が、自身の職務中以外に以下の (a) 又は (b) を意図的に開示した場合は、有罪とされる。

(a) かかるシステムを使用して送信する過程で傍受されたメッセージの内容。又は、

(b) かかるシステムを使用して他人に提供された電気通信サービスの利用に関係する情報。

(2) 上記 (1) 項は、以下の (a) から (d) のいずれかに該当する開示には適用されない。

(a) 裁判所の命令に従って、若しくは刑事訴訟の目的でなされた開示。

(b) 2000 年調査権限規制法の規定に基づいて発行された、供与された、若しくは与えられた令状、許可、若しくは通知に従ってなされた開示。

(c) 文書若しくはその他の情報を入手する目的のために、誰によっても行使可能な法令に基づく権力を行使した結果として、課せられた（その法律を除いて）要件に従ってなされた開示。又は、

(d) 2000 年の同法、若しくは 1997 年警察法の第 III 部に基づく義務に従って、通信傍受コミッショナー（Interception of Communications Commissioner）に、若しくは 2000 年の同法の第 65 条に基づいて設定された法廷に情報を提供するか、若しくは文書を提出すること。

（以下略）

（８）2009 年データ保存規則

○関連する条項の抜粋訳

2009 年データ保存規則第 4 条　通信データを保存する義務

(1) 当規則の附則の以下の規定に定められている通信データを保存することは、公衆通信プロバイダの義務である。

(a) 第 1 部（固定ネットワーク電話）

(b) 第 2 部（携帯電話）

(c) 第 3 部（インターネットアクセス、インターネット電子メール、又はインターネット電話）

(2) 義務は、不成立となった以下の電話呼び出し（call atempts）に関するデータにも及ぶ。
(a) 電話データの場合は、英国で保存される。又は、
(b) インターネットデータの場合は、英国で記録される。
(3) 「不成立となった電話呼び出し」とは、電話呼び出しが首尾よく接続されたものの、応答がなかった、若しくはネットワーク管理の介入があった通信を意味する。
(4) 義務は、接続されなかった呼び出しにまでは及ばない。
(5) 通信の内容を明らかにするデータは、当規則に従って保存しない。

2009 年データ保存規則第 5 条　保存する期間

当規則の附則に定められているデータは、公的な通信プロバイダが当該通信日から 12 カ月間保存しなければならない。

2009 年データ保存規則第 7 条　保存されているデータへのアクセス

当規則に従って保存されているデータへのアクセスは、以下の (a) 及び (b) の場合に限り入手できる。
(a) 特定の場合。及び、
(b) データの開示が法律によって許可若しくは要求されている状況において。

2009 年データ保存規則 付表（Schedule）

第 3 部　インターネットアクセス、インターネット電子メール、又はインターネット電話

第 11 条　通信の起点を追跡し、特定するために必要なデータ

(1) 割り当てられているユーザー ID。
(2) 公衆電話網に入ってくる通信に割り当てられているユーザー ID 及び電話番号。
(3) 通信時にインターネット・プロトコル（IP）アドレス、ユーザー ID、又は電話番号が割り当てられた加入者若しくは登録ユーザーの名前及びアドレス。

第 12 条　通信の宛先を特定するために必要なデータ

(1) インターネット電話の場合は、通話の所定の受け手のユーザー ID 又は電話番号。
(2) インターネット電子メール又はインターネット電話の場合は、加入者又は登録ユーザーの名前及びアドレス、並びに通信の所定の受け手のユーザーID。

第 13 条　通信の日時及び継続時間を特定するために必要なデータ

(1) インターネットアクセスの場合―
(a) インターネットアクセスサービスとの間のログイン及びログオフの所定の時間帯（タイム・ゾーン）に基づく日時。
(b) インターネットアクセスサービスプロバイダが通信に割り当てた IP アドレス。動的

か固定かを問わない。

(c) インターネットアクセスサービスの加入者又は登録ユーザーのユーザー ID。

(2) インターネット電子メール又はインターネット電話の場合は、インターネット電子メール又はインターネット電話サービスとの間のログイン及びログオフの所定の時間帯（タイム・ゾーン）に基づく日時。

第 14 条　通信のタイプを特定するために必要なデータ

インターネット電子メール又はインターネット電話の場合は、使用しているインターネットサービス。

第 15 条　ユーザーの通信設備（又はその設備であると表明されているもの）を特定するために必要なデータ

(1) ダイアルアップアクセスの場合は、発信電話番号。

(2) その他の場合は、通信の発信元のデジタル加入者回線（DSL）又はその他のエンドポイント。

３．イタリアにおける不正アクセス関連法令

３．１　イタリアにおける不正アクセス関連犯罪の現状

イタリアにおける不正アクセス関連犯罪を含むコンピュータ犯罪の件数については、内務省が発行するレポート「イタリアのセキュリティ状況[43]」に掲載されている。2004年のレポートでは、コンピュータ犯罪の報告件数が1998年7月～2001年6月の3年間は7,957件であったのが、2001年7月～2004年6月の3年間では12,116件と約52%増加している。また、コンピュータ犯罪の検挙件数については、1998年7月～2001年6月が509件であったのが、2001年7月～2004年6月では532件と、約5%増加している。なお、2005年のレポートによると、コンピュータ犯罪の報告件数と検挙件数はそれぞれ、2004年7月～2005年6月の1年間で5,820件、238件となっている（表 7参照）[44]。

表 7　イタリアにおけるコンピュータ犯罪の報告件数と検挙件数

	1998年7月～2001年6月（3年間）	2001年7月～2004年6月（3年間）	2004年7月～2005年6月（1年間）
コンピュータ犯罪の報告件数[45]	7,957件	12,116件	5,820件
コンピュータ犯罪の検挙件数	509件	532件	238件

出典：イタリア内務省「イタリアのセキュリティ状況」（2004年版、2005年版）

また、2000 年上期から 2005 年下期にかけて、コンピュータ・システムへの無権限での侵入（いわゆるハッキング事案）について関連司法機関に報告された件数は、表 8 の通りである。

表 8　コンピュータ・システムへの侵入の報告件数

	2000年上期	2000年下期	2001年上期	2001年下期	2002年上期	2002年下期	2003年上期	2003年下期	2004年上期	2004年下期	2005年上期
コンピュータ・システムへの侵入件数[46]	22件	33件	47件	33件	17件	23件	10件	25件	41件	66件	44件

出典：イタリア内務省「イタリアのセキュリティ状況」（2005年版）

[43] Ministero dell'Interno,"Lo stato della sicurezza in Italia"。
[44] 内務省の同レポートについては、2005 年以降のレポートはインターネット上では入手できない。
[45] 関連司法機関への報告件数。
[46] 関連司法機関への報告件数。

なお、イタリアでは、サイバー犯罪の領域における捜査活動は、主に国家警察（内務省所属）の郵便・通信警察（Polizia postale e delle comunicazioni）に委ねられている。国家警察のホームページ[47]では、郵便・通信警察について以下のように記載されている。

「近年の技術的進歩によって、情報交換やデータベースへのアクセス、商取引や金融取引の実行、新たな専門的活動の実施のためのメディアとして、インターネットは必須のものとなっている。インターネット利用の急速な拡大は、ネットワーク自体の脆弱性、とりわけ情報セキュリティに関わる脆弱性を明らかにした。郵便・通信警察はあらゆる形式の通信における通信の秘密と憲法上の自由を保証し、犯罪に対処するための国家警察の専門部局である。郵便・通信警察は、最先端の犯罪に対して継続的に対応していくことを主眼としている。郵便・通信警察は、全国に州単位で20箇所の支局と、県単位で80箇所の支部を持つ。」

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[48]

（１）コンピュータ犯罪に関する 1993 年 12 月 23 日付法律

イタリアでは、1993 年 12 月 23 日付法律第 547 号「刑法及び刑事訴訟法のコンピュータ犯罪に関する規則の改正と補足」によって、初めてコンピュータ犯罪の問題への体系的な対応がなされた。同法では、保護対象を正確に絞り、コンピュータ機器やプログラム、データを対象とした犯罪（本来のコンピュータ犯罪又は電気通信犯罪）と、それらを使用した犯罪（「準」コンピュータ犯罪又は「準」電気通信犯罪）とを並置させた。

刑法第 615 条の３では、コンピュータ・システムや電気通信システムに不正にアクセスする特定の人物を想定し、「セキュリティ手段により保護されているコンピュータ・システム又は電気通信システムに不正に侵入する者、又は不正侵入を排除しうる権利を有する者の明示的若しくは暗黙の意思に反して当該システム内に存続する者」と定義している。当該犯罪は、刑法において「住居侵入罪」の節に分類されている。しかし、第 615 条の３で言うところのアクセスは、コンピュータ関係、電気通信関係のアクセスに限られ、物理的アクセス（例：入れ物を物理的に開けること）は、同条の対象外である。

また、刑法第392条や第615条の5では、コンピュータ・システムや電気通信システムの改変について規定している。1993年の法改正において、器物に対する暴力行為にコンピュータ関係の規定が追加され（第392条）、コンピュータ・データやプログラムの損壊を規制す

---

[47] イタリア国家警察のサイト（http://www.poliziadistato.it/articolo/view/982/）。

[48] 本節の記述は、Daniele Minotti,”Crimini con i bit”（イタリア国家警察機関誌”Polizia Moderna”2010 年 11 月号）（http://poliziadistato.it/poliziamoderna/articolo.php?cod_art=2126）を参考にした。

る第635条の2が新設され[49]、「悪意ある」コンピュータ・プログラム（ウィルス等）を規制する第615条の5が新設された。判例集によれば、コンピュータ関係の損壊は、当該システムへの事前の不正アクセスを通じて発生する場合が多い。不正アクセス行為の結果、当該システムに損壊が発生した場合、刑法第615条の3に基き、刑が加重される。

1993 年の法改正では、コンピュータ・プログラムの所持や作成を犯罪行為とみなすべきかどうかも問題となった。単に悪意あるプログラムの所持や作成を処罰するだけでは、ウィルス対策ソフトの製作者もが処罰されるおそれがあった。このため、第 615 条の 5 には、処罰対象を制限するために、「コンピュータ・システム若しくは電気通信システム、又は当該システム内若しくは当該システムに関係するデータやプログラムを不正に損壊する目的や、当該システムの運用の全部若しくは一部を中断したり改変する目的」という犯罪意思の要素が導入された。

（２）2008 年 3 月 18 日付法律

2008年3月18日付法律第48号では、欧州評議会のサイバー犯罪条約（2001年11月に採択）を国内法に反映させるために、刑法及び刑事訴訟法の関連条項に修正及び追加がなされた。

2008年の法改正では、従来の刑法第635条の2（コンピュータ・システム及び電気通信システムの損壊）の解釈の難しさに鑑みて、この第635条の2を4つの場合に分類した。すなわち、データやプログラムについては第635条の2と第635条の3で、コンピュータ・システムや電気通信システムについては第635条の4と第635条の5で規定した。また、国家その他の公共団体・公益団体の財については第635条の3と第635条の5で、公益性のない民間の財については第635条の2と第635条の4で規定した。

また、2008 年の法改正では、刑法第 615 条の 5 を改正し、従来はコンピュータ・システムの損壊を目的としたコンピュータ・プログラムのみが対象であったのに対し、同様なことを目的とした装置や機器（ハードウェア）についても処罰対象とされることとなった。

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

刑法第615条の3

「刑法第615条の3　コンピュータ・システム又は電気通信システムに対する不正アクセス」では、セキュリティ手段により保護されているコンピュータ・システム若しくは電気通信システムに不正に侵入した者、又はアクセスを排除しうる権利保持者の明示的若しくは暗黙の意思に反してアクセスを続けた者は、1年以下の拘禁刑に処することが規定されて

[49] 従来、第 635 条の規定は、動産又は不動産を対象としたもので、データやプログラムのような無形資産には適用できなかった。

いる[50]。

また、公務員やシステムオペレーター等が自らの権限を濫用して当該行為を犯した場合、犯行者が当該行為を犯すために器物や人間に暴力を行使した場合、当該行為によってシステムの損壊が発生した場合等には、1年以上5年以下の拘禁刑に処することが規定されている[51]。

上記の犯罪は、当該システムの使用の権限を与えられた人間によっても実行されうる。すなわち、当該システムの一部へのアクセスのみを認められた人間が、アクセスを認められていない範囲にまでアクセスを行う場合も、刑法615条の3の対象となる。

以下、補足説明を行う[52]。

○セキュリティ手段による保護

「セキュリティ手段」で保護されていないシステムは、同条の対象とならない。セキュリティ手段の範囲は非常に広く、単純なパスワードから、ICカード、生理的特徴によるバイオメトリクス（例：指紋、虹彩）、行動的特徴によるバイオメトリクス（例：声紋）、ファイアウォールまで含まれる。また、セキュリティ手段には、アクセス禁止を実効的に伝える単純な警告も含まれると考えられている[53]。

セキュリティ手段として分類されるものに共通な要素は、システム内へ侵入したりアクセスし続けることに反対する意思の表明である。換言すると、所有者の同意なしに、所有者の意思に反して行われるアクセスが処罰対象となる。

なお、コンピュータ・システムと電気通信システムとは区別する必要がある。キーボードにロックを掛ければ、当該コンピュータ・システムへのアクセスを禁止する物理的なセキュリティ手段となりうるが、必ずしもインターネット等の通信接続においてセキュリティ手段を講じていることにはならない。第615条の３の犯罪が成立するためには、犯行者がセキュリティ手段で保護されているシステムに意図的にアクセスすることが必要になるため、物理的なセキュリティ手段があると知らずに犯行者が当該システムにネットワーク経由で侵入した場合には、処罰することはできない。

不正アクセスの未遂行為について

不正アクセスの未遂行為については、刑法第56条（犯罪未遂）で規定されており、犯罪

[50] 当該行為が軍事関係のコンピュータ・システムや、公共の秩序、公安、国民の健康・保護、公益に関係するコンピュータ・システムに関わるものである場合には、1 年以上 5 年以下の拘禁刑に処せられる。

[51] 当該行為が軍事関係のコンピュータ・システムや、公共の秩序、公安、国民の健康・保護、公益に関係するコンピュータ・システムに関わるものである場合には、3 年以上 8 年以下の拘禁刑に処せられる。

[52] Daniele Minotti,”Crimini con i bit”（イタリア国家警察機関誌”Polizia Moderna”2010 年 11 月号）（http://poliziadistato.it/poliziamoderna/articolo.php?cod_art=2126）。

[53] トリノ裁判所第 4 部の 1998 年 2 月 7 日判決に基づく。

を行うことを明白に目的とした行為を行った者は、当該犯罪の未遂罪で有罪とされる。

（２）データの財物性（データの不正取得）

個人データ保護法第23条

個人データに関しては、個人データ保護法の第23条において、民間組織や営利公共団体による個人データの処理は、データ主体が明確な同意を与えた場合のみ許されると規定されている。この個人データの「処理」には、個人データの取得が含まれる。自分自身若しくは他者に利益をもたらす目的で、又は他者に損害を及ぼす目的で第23条に違反した者は、第167条において、6カ月以上18カ月以下の拘禁刑に処することが規定されている。

「個人データ」は、個人データ保護法第4条（定義）において、「他の情報を参照することによって、間接的にであれ、識別することが可能な、自然人又は法人に関する情報」と定義されている。

なお、刑法第624条に規定する窃盗罪では、動産（有体物）や、経済的価値を有する電力等のエネルギーは対象となるが、データそれ自体は対象とならないと考えられている[54]。

（３）不正アクセス行為の予備行為

イタリアの刑法には、外部からのシステム探索等の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。

（４）不正アクセス行為の国外犯

刑法において以下のように一般的な国外犯規定がなされているが、犯行者をイタリア国法にしたがって処罰するためには、犯行者がイタリア国内に所在することが必要である。したがって、被害者がイタリア以外の外国に設置しているサーバに対して、犯行者が別の外国から不正アクセスする行為等については、当該犯行者がイタリアに入国しない限り、処罰することができない。

刑法第9条、第10条

「刑法第9条　外国におけるイタリア国民の一般犯罪」では、イタリア国法により死刑[55]、終身刑又は3年以上の拘禁刑に処する旨が定められている犯罪を外国において犯したイタリア国民に関しては、イタリア国内に所在する場合に限り、イタリア国法にしたがって処罰することが規定されている。また、これ以下の拘禁刑が定められている犯罪については、犯人は、法務大臣の要請又は被害者の告訴若しくは請求を受けて処罰することが規定され

[54] Penale.it の記事（2005 年 11 月 19 日）（http://www.penale.it/page.asp?mode=1&IDPag=94）。

[55] イタリアでは、2007 年 10 月の憲法改正により、死刑は完全に廃止された。

ている。

また、「刑法第10条　外国における外国人の一般犯罪」では、イタリア国法により死刑、終身刑又は1年以上の拘禁刑に処する旨が定められている犯罪で、イタリア国又はイタリア国民に被害を及ぼす犯罪を外国において犯した外国人は、イタリア国内に所在し、法務大臣の要請又は被害者の告訴若しくは請求を受けた場合に限り、イタリア国法にしたがって処罰することが規定されている。

（５）他人の識別符号の譲渡し

不正アクセスの助長行為として、他人の識別符号を提供する行為については、刑法第615条の4で規制が行われている。

刑法第615条の4

「第615条の4　コンピュータ・システム又は電気通信システムに対するアクセスコードの不正な所持又は頒布」では、自分又は他者に利益をもたらす目的や、他者に損害を及ぼす目的で、セキュリティ手段により保護されているコンピュータ・システム若しくは電気通信システムにアクセスするためのコード、パスワード若しくはその他の手段を不正に取得、複製、頒布若しくは提供した者や、当該目的に適した情報や説明を提供した者は、1年以下の拘禁刑及び5,164ユーロ以下の罰金刑に処することが規定されている。

また、当該行為が国その他の公共機関等に対して行われたものである場合や、公務員やシステムオペレーター等が自らの権限を濫用して当該行為を犯した場合には、1年以上2年以下の拘禁刑及び5,164ユーロ以上10,329ユーロ以下の罰金刑に処することが規定されている。

（６）他人の識別符号の譲受け

上述の刑法第615条の4において、不正アクセスの助長行為として他人の識別符号を取得する行為についても規制が行われている。

なお、他人の識別符号の単なる所持は処罰対象行為にはならない。すなわち、不正アクセス未遂などの他のケースが適用されない限り、自分又は他者に利益をもたらす目的や他者に損害を及ぼす目的のない他人の識別符号の所持については、処罰対象とならない[56]。

（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明示的に規定する内容は含まれていない。

但し、上述の刑法第615条の4において、自分又は他者に利益をもたらす目的や他者に損

[56] Daniele Minotti,"Crimini con i bit"（イタリア国家警察機関誌"Polizia Moderna"2010年11月号）（http://poliziadistato.it/poliziamoderna/articolo.php?cod_art=2126）。

害を及ぼす目的で、セキュリティ手段により保護されているコンピュータ・システム等にアクセスする目的に適した情報や説明を提供した者は、1年以下の拘禁刑及び5,164ユーロ以下の罰金刑に処することが規定されている。このような「情報や説明の提供」には、他人のID・パスワード等の譲渡しに関する広告や誘引行為が含まれる可能性がある[57]。

（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。

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

刑法第615条の5

「刑法第615条の5　コンピュータ・システム又は電気通信システムの損壊又は中断を意図した情報装置、情報機器又はコンピュータ・プログラムの頒布」では、コンピュータ・システム若しくは電気通信システム、又はシステム内若しくはシステムに関係するデータやプログラムを不正に損壊する目的や、当該システムの運用の全部若しくは一部を中断したり改変する目的で、コンピュータ・プログラムの取得、作成、複製、頒布、他者への提供等を行った者は、2年以下の拘禁刑及び10,329ユーロ以下の罰金刑に処することが規定されている[58]。

（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等のフィッシング行為については、刑法第494条（なりすまし）及び刑法第640条の3（コンピュータ詐欺）で規制することが可能である[59]。

ID・パスワード等の識別符号の不正取得を目的とするものに限らないが、フィッシングサイトの構築については、刑法第494条（なりすまし）の対象となる。また、フィッシング行為[60]によって他者に損害を与えた場合は、刑法第640条の3（コンピュータ詐欺）の対象と

---

[57] イタリア国家警察機関誌の記事では、「コンピュータ・システム等へのアクセスに適した情報や説明の提供」の例として、「パスワードが記載された別のサイトへのリンク」が挙げられている。Daniele Minotti,”Crimini con i bit”（イタリア国家警察機関誌”Polizia Moderna”2010年11月号）（http://poliziadistato.it/poliziamoderna/articolo.php?cod_art=2126）。

[58] コンピュータ・プログラムには、ウィルス、ワーム、トロイの木馬、メール爆弾等が含まれる。Daniele Minotti,”Crimini con i bit”（イタリア国家警察機関誌”Polizia Moderna”2010年11月号）。

[59] Daniele Minotti,”Cybercrime”（イタリア国家警察機関誌”Polizia Moderna”2010年12月号）（http://poliziadistato.it/poliziamoderna/articolo.php?cod_art=2142）。

[60] ファーミング（DNSサーバの書き換え等により、偽のサイトに誘導する手法）のタイプのフィッシング等。

なりうる。

刑法第494条

「刑法第494条　なりすまし」では、自分又は他者に利益をもたらす目的や、他者に損害を及ぼす目的で、非合法的に自らが他者になりすました者は、1年以下の拘禁刑に処することが規定されている。

なお、第494条が適用されるためには、「自分自身若しくは他者に利益をもたらす目的、又は他者に損害を及ぼす目的」という犯行者の目的が構成要件として必要である。

刑法第640条の3

「刑法第640条の3　コンピュータ関連の詐欺」では、コンピュータ・システム若しくは電気通信システムの運用を改変したり、それらのシステム内若しくはそれらのシステムに関係するデータやプログラムを無権限で改ざんして、自分や他者に不正な利益をもたらし、他者に損害を及ぼした者は、6カ月以上3年以下の拘禁刑及び51ユーロ以上1,032ユーロ以下の罰金刑に処することが規定されている。

但し、当該行為が国その他の公共機関に対して行われたものである場合や、システムオペレーターが身分を濫用して当該行為を犯した場合には、1年以上5年以下の拘禁刑及び309ユーロ以上1,549ユーロ以下の罰金刑に処することが規定されている。

なお、第640条の3が適用されるためには、「他者に損害を与えると共に自分自身若しくは他者に不正な利益をもたらした」という行為の結果が構成要件として必要である。

（３）サイバーテロ行為

テロを目的としたDos攻撃等については、刑法第635条の2（コンピュータ・データやプログラムの損壊）、刑法第635条の3（国家等のコンピュータ・データやプログラムの損壊）、刑法第635条の4（コンピュータ・システムの損壊）、刑法第635条の5（公益用のコンピュータ・システムの損壊）及び刑法第392条（器物に対する暴力）で規制が行われている

刑法第635条の2

「刑法第635条の2　コンピュータの情報・データ、コンピュータ・プログラムの損壊」では、他者のコンピュータの情報・データ若しくはコンピュータ・プログラムを破壊、劣化、消去、改変若しくは削除した者は、被害者の告訴を受けて、6カ月以上3年以下の拘禁刑に処することが規定されている。

また、当該行為が人への暴力又は脅しをもって行われた場合や、システムオペレーターが身分を濫用して当該行為を犯した場合には、1年以上4年以下の拘禁刑に処することが規定されている。

刑法第635条の3

「刑法第635条の3　国家、その他の公共団体又は公益団体が利用しているコンピュータの情報・データ、コンピュータ・プログラムの損壊」では、国家若しくはその他の公共団体が利用している、又は当該団体に属するコンピュータの情報・データ若しくはコンピュータ・プログラムを破壊、劣化、消去、改変若しくは削除を目的とした行為を犯した者は、1年以上4年以下の拘禁刑に処することが規定されている。

また、当該行為により、コンピュータの情報・データ若しくはコンピュータ・プログラムが破壊、劣化、消去、改変若しくは削除されるにいたった場合は、3年以上8年以下の拘禁刑に処することが規定されている。

さらに、当該行為が他人への暴力又は脅しをもって行われた場合や、システムオペレーターが身分を濫用して当該行為を犯した場合には、増刑すると規定されている。

刑法第635条の4

「刑法第635条の4　コンピュータ・システム又は電気通信システムの損壊」では、第635条の2に掲げる行為又はデータ、情報若しくはプログラムの入力若しくは伝送を通じて、他者のコンピュータ・システム若しくは電気通信システムを破壊、損壊若しくは使用不能（全部もしくが一部）にいたらせるか、システムの運用に重大な障害を生じさせた者は、1年以上5年以下の拘禁刑に処することが規定されている。

また、当該行為が他人への暴力又は脅しをもって行われた場合や、システムオペレーターが身分を濫用して当該行為を犯した場合には、増刑することが規定されている。

刑法第635条の5

「刑法第635条の5　公益用のコンピュータ・システム又は電気通信システムの損壊」では、第635条の4に掲げる行為が、公益用のコンピュータ・システム又は電気通信システムを破壊、損壊、使用不能（全部若しくは一部）にいたらせるか、システムの運用に重大な障害を生じさせことを目的として行われた場合には、1年以上4年以下の拘禁刑に処することが規定されている。

また、当該行為により、公益用のコンピュータ・システム又は電気通信システムの破壊又は損壊が生じるか、システムの全部又は一部が使用不能にいたった場合には、3年以上8年以下の拘禁刑に処することが規定されている。

さらに、当該行為が他人への暴力又は脅しをもって行われた場合や、システムオペレーターが身分を濫用して当該行為を犯した場合には、増刑すると規定されている。

刑法第392条

「刑法第392条　器物に対する暴力を通じての個人的権利主張の独断的行使」では、司法に訴えることも可能であるのに、自らが主張する権利を行使するために、器物に対する暴

力を通じて個人的権利主張を認めさせた者は、被害者の告訴を受けて、516ユーロ以下の罰金刑に処することが規定されている。

「器物に対する暴力」には、コンピュータ・プログラムの全部若しくは一部が改変若しくは消去された場合又はコンピュータ・システム若しくは電気通信システムの運用が阻害若しくは妨害された場合も含まれる。

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

刑事訴訟法

刑事訴訟法の第266条において、電話又は他の通信形態の通話又は通信の傍受は、「終身刑又は5年超の拘禁刑が定められている、過失以外の犯罪」や「5年以上の拘禁刑が定められている、行政機関に対する犯罪」等に関係する手続きの中で認められている。また、同法の第266条の2では、第266条に記す犯罪であって、情報技術や電気通信技術を利用して行われた犯罪に関する手続きにおいては、コンピュータ・システムに関係する通信フローを傍受することが認められている。

同法の第267条において、検察官は予備捜査担当裁判官（giudice per le indagini preliminari）に対して、傍受のための令状（decreto motivato）を請求することができると規定されている。予備捜査担当裁判官は、犯罪の重大な兆候があり、かつ捜査の続行にとって必要な場合のみ、令状を発付する。また緊急の場合であって、捜査の遅れによって重大な侵害が生じるおそれがある場合には、検察官は自ら令状を発付できるが、検察官は予備捜査担当裁判官に対して24時間以内に当該令状を通知せねばならず、48時間以内に予備捜査担当裁判官が令状を許可しない場合は、傍受を継続したり傍受の結果を使用したりすることはできない。

（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

個人データ保護法132条

個人データ保護法132条（トラフィックデータの保存）の第3項では、公的な電気通信サービスを提供する電気通信事業者（fornitore di servizi di comunicazione elettronica）から、検察官の発付する令状に基づき、電気通信事業者が保存しているトラフィックデータを取得できることが規定されている。

また、被疑者や捜査対象者の弁護人は、当人の利用分に関するトラフィックデータを、電気通信事業者に直接請求することが可能である。

また、刑事訴訟法第254条の2では、司法機関が電気通信事業者の保有するデータを押収することを命令する際には、オリジナルデータが改変されてサービス提供に支障をきたす

ことのないように、媒体からコピーする形で押収することができると規定されている。

（３）ログの保存

個人データ保護法132条

個人データ保護法132条（トラフィックデータの保存）の第1項において、電気通信事業者は、犯罪の立証や抑制を目的として、通話に関するトラフィックデータは24カ月間、電気通信に関するトラフィックデータ（通信の内容は覗く）は12カ月間、保存することが規定されている。

３．３　不正アクセス関連法令条文集

（１）刑法

○関連する条項の抜粋訳

第１巻　犯罪全般

第１編　刑法

刑法第７条　外国における犯罪

下記のいずれかの犯罪を外国において犯したイタリア国民又は外国人は、イタリア国法にしたがって処罰する。

1）イタリア国の高官に対する犯罪。

2）国璽の偽造罪及び偽造された国璽の使用罪。

3）イタリア国内で合法的に流通している通貨又はイタリア国の収入印紙・切手若しくは公債証書の偽造罪。

4）イタリア国の国家公務員が自らの職務権限を濫用して、又は職務に関わる義務に違反して犯した犯罪。

5）法律の特別規定又は国際条約により、イタリア国の刑法を適用する旨定められているその他すべての犯罪。

刑法第８条　外国における政治犯罪

（略）

刑法第９条　外国におけるイタリア国民の一般犯罪

前 2 条に記す場合以外で、イタリア国法により死刑、終身刑又は 3 年以上の拘禁刑に処する旨が定められている犯罪を外国において犯したイタリア国民に関しては、イタリア国内に所在する場合に限り、イタリア国法にしたがって処罰する。

これより短期間人身の自由を制限する刑罰が定められている犯罪については、犯人は、法務大臣の要請又は被害者の告訴若しくは請求を受けて処罰する。

前諸規定により定められている場合で、欧州共同体、外国又は外国人が被害を被った犯罪に関しては、犯人が犯罪を犯した国の政府が犯人の身柄引き渡しを許可しないか、容認しない場合に限り、犯人は、法務大臣の要請を受けて処罰する。

刑法第 10 条　外国における外国人の一般犯罪

第 7 条及び第 8 条に記す場合以外で、イタリア国法により死刑、終身刑又は 1 年以上の拘禁刑に処する旨が定められている犯罪で、イタリア国又はイタリア国民に被害を及ぼす犯

罪を外国において犯した外国人は、イタリア国内に所在し、法務大臣の要請又は被害者の告訴若しくは請求を受けた場合に限り、イタリア国法にしたがって処罰する。
欧州共同体、外国又は外国人が被害を被った犯罪に関しては、下記の場合に限り、犯人は、法務大臣の要請を受けて、イタリア国法にしたがって処罰する。
1）犯人がイタリア国内に所在する場合。
2）死刑、終身刑又は 3 年以上の拘禁刑に処する旨が定められている犯罪。
3）犯人が犯罪を犯した国の政府又は犯人が属する国の政府が犯人の身柄引き渡しを許可しないか、容認しない場合。

第 3 編　犯罪

刑法第 56 条　犯罪未遂

犯罪を行うことを明白に目的とした行為を行ったものは、当該行為が完遂されないか、又は当該事象が発生しなかった場合には、犯罪未遂罪に該当する。罰則として死刑が規定されている犯罪の場合、犯罪未遂罪は、25 年以上 30 年以下の拘禁刑に処する。罰則として無期拘禁刑が規定されている犯罪の場合、12 年以上の拘禁刑に処する。罰則としてその他が規定されている犯罪の場合、3 分の 1 から 3 分の 2 の罰則に処する。犯行者が自発的に当該行為を止めた場合、完遂した行為が他の犯罪を構成する場合には、その完遂した行為に対する罰則のみに処せられる。犯行者が自発的に当該事象を回避した場合には、3 分の 1 から 2 分の 1 の罰則に処する。

第 2 巻　特殊犯罪

第 3 編　司法機関に対する犯罪

第 3 章　個人的権利主張の独断的保護

刑法第 392 条　器物に対する暴力を通じての個人的権利主張の独断的行使

司法に訴えることも可能であるのに、自らが主張する権利を行使するために、器物に対する暴力を通じて個人的権利主張を認めさせた者は、被害者の告訴を受けて、516 ユーロ以下の罰金刑に処する。
刑法に基き、器物の損壊若しくは改変が生じた場合又は器物の用途が変化した場合を、器物に対する暴力とみなす。
また、コンピュータ・プログラムの全部若しくは一部が改変若しくは消去された場合又はコンピュータ・システム若しくは電気通信システムの運用が阻害若しくは妨害された場合も、器物に対する暴力とみなす。

第 7 編　公的信頼に反する犯罪

第 4 章　人的虚偽

刑法第 494 条　なりすまし

自分自身若しくは他者に利益をもたらす目的、又は他者に損害を及ぼす目的で、非合法的に自らが他者に成り代わるか、自ら若しくは他者に対して偽名、虚偽の身分若しくは法律により法的効果が与えられる肩書きを付与するかした者は、当該行為が公的信頼に反する他の犯罪を構成しない場合には、1 年以下の拘禁刑に処する。

第 12 編　対人犯罪

第 3 章　個人的自由に反する犯罪

第 4 節　住居侵入罪

刑法第 615 条の 3　コンピュータ・システム又は電気通信システムに対する不正アクセス

セキュリティ手段により保護されているコンピュータ・システム若しくは電気通信システムに不正に侵入した者、又は、アクセスを排除しうる権利を有する者の明示的若しくは暗黙の意思に反してアクセスを続けた者は、1 年以下の拘禁刑に処する。

下記の場合は、1 年以上 5 年以下の拘禁刑に処する。

1）公務員若しくは公的役務担当者が、自らの職務若しくは役務に関係する権限を濫用するか、関係する義務に違反するかして当該行為を犯した場合、私立探偵の職務を遂行する者（不正遂行者も含む）が当該行為を犯した場合、又はシステムのオペレーターが、その身分を濫用して当該行為を犯した場合。

2）犯人が、当該行為を犯すために、器物若しくは人間に暴力を行使するか、明確に武装していた場合。

3）当該行為により、システムの破壊、損壊、システムの運用の全部若しくは一部の中断、又はシステムに入っていたデータ、情報若しくはプログラムの破壊、損壊が生じた場合。

第 1 段及び第 2 段に掲げる行為が、軍事関係のコンピュータ・システム若しくは電気通信システムに関わるものである場合、又は公共の秩序、公安、国民の健康若しくは保護又は公益に関係するコンピュータ・システム若しくは電気通信システムに関わるものである場合には、それぞれ、1 年以上 5 年以下、3 年以上 8 年以下の拘禁刑に処する。

第 1 段で定める場合には、被害者の告訴を受けて処罰し、他の場合は、職務上の権限に基いて手続きを行う。

刑法第 615 条の 4　コンピュータ・システム又は電気通信システムに対するアクセスコードの不正な所持又は頒布

自分自身若しくは他者に利益をもたらす目的、又は他者に損害を及ぼす目的で、セキュリティ手段により保護されているコンピュータ・システム若しくは電気通信システムにアクセスするためのコード、パスワード若しくはその他の手段を不正に取得、複製、頒布若しくは提供した者、又は当該目的に適した情報若しくは説明を提供した者は、1 年以下の拘禁刑及び 5,164 ユーロ以下の罰金刑に処する。

第 617 条の 4 の第 4 段の 1）及び 2）に掲げる事由のいずれかが生じた場合は、1 年以上 2 年以下の拘禁刑及び 5,164 ユーロ以上 10,329 ユーロ以下の罰金刑に処する。

刑法第 615 条の 5　コンピュータ・システム又は電気通信システムの損壊若しくは中断のための情報装置、情報機器若しくはコンピュータ・プログラムの頒布

コンピュータ・システム若しくは電気通信システム、当該システムに入っている、若しくは関係するコンピュータ・データ若しくはプログラムを不正に損壊する目的、又は当該システムの運用の全部若しくは一部の中断又は改変する目的で、情報装置、情報機器若しくはコンピュータ・プログラムの取得、作成、複製、輸入、配布、伝達、引渡し、若しくは他者への提供を行った者は、2 年以下の拘禁刑及び 10,329 ユーロ以下の罰金刑に処する。

第 13 編　財産侵害罪

第 1 章　対物暴力行為又は対人暴力行為による財産侵害罪

刑法第 624 条　窃盗罪

自分自身若しくは他者のために利益を得る目的で、他者から同人が所有する動産を盗み、他者の動産を奪取するにいたった者は、6 カ月以上 3 年以下の拘禁刑及び 154 ユーロ以上 516 ユーロ以下の罰金刑に処する。

刑法に基き、経済的価値を有する電力及びその他すべてのエネルギーも、動産とみなす。

第 61 条の 7）及び第 625 条に掲げる 1 つ若しくは 2 つ以上の事由が生じた場合を除き、窃盗罪は、被害者の告訴を受けて処罰する。

刑法第 635 条の 2　コンピュータの情報・データ、コンピュータ・プログラムの損壊

他者のコンピュータの情報・データ若しくはコンピュータ・プログラムを破壊、劣化、消去、改変若しくは削除した者は、被害者の告訴を受けて、6 カ月以上 3 年以下の拘禁刑に処する。ただし、当該行為がより重大な犯罪を構成する場合は、この限りではない。第 635 条第 2 段の 1）に掲げる事由（訳注：人に対する暴力又は脅迫）が生じた場合、又はシステムのオペレーターが自らの身分を濫用して当該行為を犯した場合には、1 年以上 4 年以下の拘禁刑に処し、職務上の権限に基いて手続きがとられる。

刑法第 635 条の 3　国家、その他の公共団体又は公益団体が利用しているコンピュータの情報・データ、コンピュータ・プログラムの損壊

国家若しくはその他の公共団体が利用している、又は当該団体に属するコンピュータの情報・データ若しくはコンピュータ・プログラムを破壊、劣化、消去、改変若しくは削除を目的とした行為を犯した者は、1 年以上 4 年以下の拘禁刑に処する。ただし、当該行為がより重大な犯罪を構成する場合は、この限りではない。当該行為により、コンピュータの情報・データ若しくはコンピュータ・プログラムが破壊、劣化、消去、改変若しくは削除さ

れるにいたった場合は、3 年以上 8 年以下の拘禁刑に処する。
第 635 条第 2 段の 1）に掲げる事由（訳注：人に対する暴力又は脅迫）が生じた場合、又はシステムのオペレーターが自らの身分を濫用して当該行為を犯した場合には、増刑する。

刑法第 635 条の 4　コンピュータ・システム又は電気通信システムの損壊
第 635 条の 2 に掲げる行為又はデータ、情報若しくはプログラムの入力若しくは伝送を通じて、他者のコンピュータ・システム若しくは電気通信システムを破壊、損壊若しくは使用不能（全部もしくが一部）にいたらせるか、システムの運用に重大な障害を生じさせた者は、1 年以上 5 年以下の拘禁刑に処する。ただし、当該行為がより重大な犯罪を構成する場合は、この限りではない。
第 635 条第 2 段の 1）に掲げる事由（訳注：人に対する暴力又は脅迫）が生じた場合、又はシステムのオペレーターが自らの身分を濫用して当該行為を犯した場合には、増刑する。

刑法第 635 条の 5　公益用のコンピュータ・システム又は電気通信システムの損壊
第 635 条の 4 に掲げる行為が、公益用のコンピュータ・システム又は電気通信システムを破壊、損壊、使用不能（全部若しくは一部）にいたらせるか、システムの運用に重大な障害を生じさせることを目的として行われた場合には、1 年以上 4 年以下の拘禁刑に処する。
当該行為により、公益用のコンピュータシステム又は電気通信システムの破壊又は損壊が生じるか、システムの全部又は一部が使用不能にいたった場合には、3 年以上 8 年以下の拘禁刑に処する。
第 635 条第 2 段の 1）に掲げる事由（訳注：人に対する暴力又は脅迫）が生じた場合、又はシステムのオペレーターが自らの身分を濫用して当該行為を犯した場合には、増刑する。

第 2 章　詐欺による財産侵害罪
刑法第 640 条の 3　コンピュータ関連の詐欺
コンピュータ・システム若しくは電気通信システムの運用を何らかの方法で改変するか、又はコンピュータ・システム若しくは電気通信システムに入っている、若しくは関係するデータ、情報若しくはプログラムを無権限で何らかの方法により改竄して、他者に損害を与えると共に自分自身若しくは他者に不正な利益をもたらした者は、6 カ月以上 3 年以下の拘禁刑及び 51 ユーロ以上 1032 ユーロ以下の罰金刑に処する。
第 640 条の第 2 段の 1）に掲げる事由（訳注：国家機関等に対する犯罪）のいずれかが生じた場合、又はシステムのオペレーターが、その身分を濫用して当該行為を犯した場合には、1 年以上 5 年以下の拘禁刑及び 309 ユーロ以上 1,549 ユーロ以下の罰金刑に処する。
第 2 段に掲げる事由のいずれかが生じた場合、又は他の重大な事由が生じた場合を除き、本犯罪は、被害者の告訴を受けて処罰する。

（２）刑事訴訟法

○関連する条項の抜粋訳

第１部
第３巻　証拠
第３編　証拠捜査手段
第３章　押収
刑事訴訟法第 254 条の２　情報サービス、データ処理サービス、通信サービスのプロバイダからのコンピュータ・データの押収

1. 司法機関は、情報サービス、データ処理サービス又は通信サービスのプロバイダが保有するデータ（トラフィックデータ又は所在地データを含む）を当該プロバイダから押収することを命令する際には、当該サービスの正規の提供に伴う必要性を考慮して、データは、押収データがオリジナルデータと相違することがないよう、オリジナルデータが改変されることがないような手順で、しかるべき媒体からコピーする形で押収する旨を定めることができる。いずれにせよ、この場合、オリジナルデータを適切に保存し、保護するよう、サービス・プロバイダに命令する。

第４章　通話又は通信の傍受
刑事訴訟法第 266 条　容認範囲

1. 電話又は他の通信形態の通話又は通信の傍受は、下記の犯罪に関係する手続きの中で認められる。
   a)第 4 条で定める終身刑又は 5 年超の拘禁刑が定められている、過失以外の犯罪。
   b)第 4 条で定める 5 年以上の拘禁刑が定められている、行政機関に対する犯罪。
   c)麻薬又は向精神剤に関する犯罪。
   d)武器及び爆発性物質に関する犯罪。
   e)密輸罪。
   f)名誉毀損罪、脅迫罪、暴利罪、金融事業無許可営業罪、特権情報の濫用罪、市場操作罪、電話による迷惑・妨害罪。
   f)の 2　刑法の第 600 条の 3 の第 3 段で定める犯罪。刑法の第 600 条の 4 に掲げる猥褻文書・図画に関する犯罪も含む。
2. 以上の場合、当事者間の通信の傍受が認められる。ただし、刑法の第 614 条に記す場所において通信の傍受を行う場合には、その場所で犯罪行為が行われているとみなすべき根拠ある理由が存在する場合に限り、傍受が認められる。

刑事訴訟法第 266 条の 2　コンピュータ通信又は電気通信の傍受

1. 第 266 条に記す犯罪及び情報技術若しくは電気通信技術を利用して行われた犯罪に関する手続きにおいては、コンピュータ・システム若しくは電気通信システムに関する通信のフロー又は複数のシステム間の通信のフローを傍受することが認められる。

刑事訴訟法第 267 条　措置の前提と形式

1. 察官は、予備捜査担当裁判官（giudice per le indagini preliminari）に対して、第266条で規定された傍受作業を準備するための許可を請求できる。当該許可は、犯罪の重大な兆候があり、かつ捜査の続行にとって傍受が絶対的に必要である場合に、令状（decreto motivato）として与えられる。

1の2. 犯罪の重大な兆候の評価には、第203条が適用される。

2. 緊急の場合であって、捜査の遅れによって重大な侵害が生じると信じられる合理的な根拠がある場合には、検察官は動機付けられた命令によって傍受を準備できる。令状の発付は、第1項に挙げられた予備捜査担当裁判官に対して24時間以内に直ちに通知されなければならない。予備捜査担当裁判官は当該措置の後、48時間以内に当該命令を許可する。検察官の発布した令状が期限内に許可されない場合には、傍受を継続することはできず、傍受の結果を使用することはできない。

（以下略）

刑事訴訟法第 268 条　傍受作業の実行

1. 傍受した通信は記録し、傍受作業の報告書を作成する。

2. 報告書には、傍受した通信の内容を記載する（要約でも可）。

3. 傍受作業は、もっぱらイタリア共和国の検察庁内に設置された設備により行うことができる。ただし、当該設備が不十分、又は不適切で、特別な緊急の事由が存在する場合には、検察官は、理由を付した措置により、公共サービス設備又は司法警察が備えている設備により傍受作業を行うよう命令することができる。

3 の 2. コンピュータ通信又は電気通信の傍受を行う場合には、検察官は、民間所有の設備を使って傍受作業を行うこともできる旨、命令することができる。

4. 報告書及び記録は、ただちに検察官に送られる。報告書及び記録は、傍受作業終了から 5 日以内に、傍受を命令、許可、認可若しくは延期した通達と一緒に、事務局内で登録され、検察官が定めた期間保管される。ただし、判事が、延期を必要と認めない場合は、この限りではない。

5. 登録により、捜査に重大な障害が生じる恐れがある場合には、判事は、検察官が予備捜査終了まで登録を遅らせることを許可する。

6. 当事者の弁護人に対しては、第 4 項及び第 5 項で定める期限までに、文書を検討し、登録に関して意見を聴取するか、コンピュータ通信又は電気通信の流れを把握する権利があ

る旨をただちに通知する。期限か経過した時点で、判事は、当事者が示した、明確に関連性がないとは認められないコンピュータ通信又は電気通信の流れ（フロー）若しくは通話の**取得**を命令し、職務上の権限に基く場合も含め、利用が禁止されている記録及び報告書の削除を行う。検察官及び弁護人は、削除作業に参加することができ、遅くとも 24 時間前に通知を受ける。

7. 判事は、記録の全面記載又は取得すべきコンピュータ通信又は電気通信の流れに含まれる情報を理解しうる形式でプリントすることを命令する。この際、鑑定実施のために定められた形式、方法、保証を順守する。記載文又はプリントは、公判のために分冊に挿入する。

8. 弁護人は、記載文の写しをとり、記録を磁気テープに転写させることができる。コンピュータ通信又は電気通信の流れの傍受が行われた場合には、弁護人は、傍受された流れをしかるべき媒体にコピーするか、第 7 項で定めるプリントをコピーすることを請求することができる。

（３）個人データ保護法

○関連する条項の抜粋訳

個人データ保護法第 4 条　定義

1. 本法の目的にとって、

a) 「処理」は、電子的又は自動的手段によって実行されるか否かに関わらず、また当該データがデータベース内に格納されているか否かにかかわらず、データの取得、記録、組織化、保持、問合せ、加工、修正、選択、検索、比較、利用、接続、社団、通信、頒布、消去及び破壊に関わる運用、又は一連の運用を意味するものとする。

個人データ保護法第 23 条　同意

1. 民間組織又は営利公共団体による個人データの処理は、データ主体が明確な同意を与えた場合のみ許されるものとする。

2. データ主体の同意は、当該処理全体に対してのものであっても、当該処理の 1 つ以上の運用に対してのものであってもよい。

3. データ主体の同意は、明確に特定された処理の運用に関して、自由かつ明示的に与えられたものであり、書面に記載されたものであり、かつデータ主体が第 13 条に挙げる情報を提供された場合にのみ、実効的なものとみなされるものとする。

4. 機微なデータに関わる処理の場合には、同意は書面で与えられるものとする。

個人データ保護法第 132 条　その他の目的のためのトラフィックデータの保存

1. 第 123 条第 2 項の規定はそのまま有効とし、プロバイダは、犯罪の立証、抑制を目的として、通話日から 24 カ月間、通話に関するトラフィックデータを保存するものとする。一方、プロバイダは、同じ目的のために、通信日から 12 ヶ月間、電気通信に関するトラフィックデータ（通信の内容は除く）を保存するものとする。

1 の 2. 公的な電気通信サービス又は公的な通信ネットワークのプロバイダは、一時的に処理され不成立となった電話呼び出しに関する当該データについては、30 日間保存するものとする。

2.（削除された）

3. 被疑者の弁護人、捜査対象者、被害者及び他の個人当事者から請求があった場合も含め、第 1 項に掲げる期限内に、検察官の発布する令状に基き、プロバイダから当該データを取得することができる。被疑者又は捜査対象者の弁護人は、刑事訴訟法の第 391 条の 4 に記した方法により、当人名義の利用分に関するデータを、プロバイダに直接請求することができる。ただし、電話の受信に関しては、第 8 条第 2 項の f）に掲げる条件はそのまま有効とする。

（以下略）

個人データ保護法第 167 条　違法なデータ処理

1. 自分自身若しくは他者に利益をもたらす目的で、又は他者に損害を及ぼす目的で、第 18 条、第 19 条、第 23 条、第 123 条、第 126 条及び第 130 条、又は第 129 条に違反して個人データを処理した者は、被害が発生した場合には、当該犯行がより重大なものでない限り、6 カ月以上 18 カ月以下の拘禁刑に処する。また、当該犯行がデータの通信又は頒布である場合には、当該犯行がより重大なものでない限り、6 カ月以上 24 カ月以下の拘禁刑に処する。

（以下略）

４．ロシアにおける不正アクセス関連法令

４．１　ロシアにおける不正アクセス関連犯罪の現状

ロシアにおけるコンピュータ犯罪の認知件数については、ロシア連邦内務省中央情報分析センターの統計[61]が存在する（表 9 参照）。不正アクセス行為等の検挙件数は、刑法典にコンピュータ犯罪に関する条項（刑法典第 28 章第 272 条～第 274 条）が制定された後の 1996 年以降、急激に増加した。2006 年には不正アクセス行為等の検挙件数が減少しているが、同年に施行された『個人データの保護に関する連邦法』の効果によるものかどうかは不明である。

表 9　ロシアにおけるコンピュータ犯罪の認知件数

	1997 年	1998 年	1999 年	2000 年	2001 年	2002 年	2003 年	2004 年	2005 年	2006 年
電子データへの不正アクセス（刑法典第 272 条違反）	6	53	209	608	1,619	3,782	7,053	8,002	8,682	7,704
有害プログラムの作成･使用･配布（刑法典第 273 条違反）	1	12	85	191	327	330	728	1,079	1,928	1,625
コンピュータ、システム及びネットワークに関する犯罪（刑法典第 274 条）	0	1	0	44	120	10	1	11	2	4
詐欺行為、地位の濫用による財産損害。特に個人のパスワード等識別符号の不正使用による財産上の侵害行為（刑法典第 165 条及び第 272 条違反）	—	—	423	275	721	1,494	2,321	2,892	2,496	1,421
電話回線及びコンピュータを使用した通信、商業、課税、銀行データの不正な傍受及び配布（刑法典第 183 条違反）	—	—	—	—	48	58	242	480	396	188

出典：Cybernetic Police サイト

[61] Cybernetic Police サイト（http://www.cyberpol.ru/statcrime.shtml#p_00）に掲載されている。なお、同サイトには 2007 年以降のデータは掲載されていない。

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

（１）不正アクセス関連法令の制定経緯

ロシアには、1992 年まで不正アクセス行為を禁止する法制度が皆無であった。1992 年 9 月 23 日、ロシア政府は『コンピュータ用ソフトウェア及びデータベースの法的保護に関する法律』を制定した[62]。同法の基本的な目的はソフトウェア及びハードウェア開発者[63]の権利保護であり、データの保護（又は不正アクセスの禁止）それ自体が目的ではなかったが、この法律によりロシアでは初めてデータ保護に必要な用語[64]が整備されることとなった。

1996 年には刑法典の改正により、第 28 章にコンピュータ情報の領域における犯罪に関する条項が追加された。具体的には、第 272 条（不正アクセス）、第 273 条（有害プログラムの作成・使用・頒布）、第 274 条（コンピュータ・システムの運用規定への違反）が追加された。

さらに、個人データの取り扱いに関しては、2006 年 7 月 27 日に、『個人データの保護に関する連邦法』が制定された。制定の背景は、コンピュータにより処理されるデータが増加し、個人データの不正取得が増加したことであった。

（２）ロシアにおける不正アクセス関連法令と運用の特徴

ロシアの不正アクセス関連犯罪では、コンピュータの不正使用や不正アクセス、データ不正取得といった手段としての行為ではなく、それらの行為がもたらした結果に対して起訴が行われることが多い。法令の規定自体が、犯行者の行為が何らかの被害を及ぼしたことを前提としており、さらに起訴便宜主義のため、該当する犯罪行為が必ず起訴につながる必然性はない[65]。そのため、相当の被害が発生していないと、起訴が行われない。

ロシアの不正アクセス関連法令の運用については、同一の行為であっても必ずしも同じ条文が適用されておらず、また必ずしも条文に明記されていない行為であっても類似の行為の罰則が適用されるなどの事例が見られる。

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

刑法典第 272 条

「刑法典第 272 条　コンピュータ情報への不正アクセス」の第 1 項では、刑法典により

---

[62] 同法は 2008 年 1 月 1 日、ロシア連邦民法典第 4 編の改正により廃止された。その後は民法典第 4 編が適用されることとなった。

[63] 同時に制定された『集積回路の構成の保護に関する法律』は、集積回路の設計に関する著作権保護を目的としている。

[64] この法律以前にはロシアの法体系にはソフトウェア、プログラムの変更、データベースなどの用語が定義されていなかった。

[65] Cybernetic Police サイト（http://www.cyberpol.ru/cybercrime.shtml）。

保護の対象と規定されるコンピュータ上のデータ（物理的媒体、並びにコンピュータ、コンピュータ・システム及びネットワーク上のデータ）への不正アクセスにより、データの破壊、遮断、変更若しくは複製を行い、又はコンピュータ若しくはネットワークの機能に損害を与えた場合には、20 万ルーブル以下若しくは犯行者の給与その他の収入の 18 カ月以下に相当する額の罰金刑、120 時間以上 180 時間以下の奉仕活動[66]若しくは 1 年以下の更生労働[67]、又は 2 年以下の自由刑[68]に処することが規定されている。

また、同条の第 2 項では、内部犯行者による不正アクセス行為を禁止している。コンピュータ･システム等へのアクセス権限を持つ者が第 1 項と同様の行為を行った場合には、10 万ルーブル以上 30 万ルーブル以下若しくは給与その他の収入の 1 年以上 2 年以下に相当する額の罰金刑、180 時間以上 240 時間以下の奉仕活動若しくは 2 年以下の更生労働、又は 3 カ月以上 6 カ月以下の禁固刑[69]若しくは 5 年以下の自由刑に処することが規定されている。

不正アクセスの未遂行為について

不正アクセスの未遂行為については、刑法典第 29 条で規制されており、不正アクセス犯罪を準備したり、不正アクセス犯罪の実行を試みることは、当該犯罪の未遂罪で有罪とされる。

（２）データの財物性（データの不正取得）

ロシア刑法典及び通信関連法令においては、データの財物性を定義する条項は存在しない。

ただし個人データに関しては、個人データの保護に関する連邦法において、本人の同意なく個人データを取得することを禁じている。

個人データの保護に関する連邦法第 6 条

個人データの保護に関する連邦法第 6 条において、行政機関や民間企業等による個人データの処理は、一定の例外の場合を除き、個人データの主体の同意の下でなされなければならないと規定されている。この個人データの「処理」には、個人データの取得が含まれる

「個人データ」は、個人データの保護に関する連邦法第 3 条において、「特定の個人に関する情報、又は当該情報によって識別される個人（「個人データの主体」）に関する情報であり、氏名、生年月日、出生地、住所、家族・社会・財産の状況、教育、職業、収入その他の情報が含まれる。」と定義されている。

---

[66] 職業又は勉学の余暇時間に指定された労務を行うことを指す（刑法典第 49 条）。
[67] 犯罪者の居住地域において自治体が司法機関の同意を得て指定する場所における労働を指す（刑法典第 50 条）。
[68] 更正・矯正機関、矯正コロニー（収容所）、又は刑務所への隔離を指す（刑法典第 56 条）。
[69] 社会からの厳重な隔離を指す（刑法典第 54 条）。

また、刑法典第 183 条の第 1 項では、商業・税務・銀行の秘密を構成する情報の不正取得を禁じている。刑法典第 183 条が他人の識別符号の不正取得に適用された判例も存在する[70]。

刑法典第 183 条

「刑法典第183条　商業、税務、銀行の秘密を構成する情報の違法な取得と開示」の第1項では、商業・税務・銀行業務の秘密を構成する情報を、文書の窃盗、賄賂、又は脅迫その他の違法行為により取得した場合には、1万8000ルーブル以下若しくは犯行者の給与その他の収入の1カ月以上6カ月以下に相当する額の罰金刑、1年以下の更生労働、又は2年以下の自由刑に処することが規定されている。

（３）不正アクセス行為の予備行為

不正アクセスの予備行為として、外部からのシステム探索等に関する明示的な規定は存在しない。

ただし、秘密裏に情報を取得することを目的とする特殊な技術的装置の違法な作成、販売、又は販売目的での購入については、刑法典第 138 条第 3 項で規制されている。

刑法典第 138 条

「刑法典第 138 条　信書、通話、郵便その他の通信の秘密の侵害」の第 3 項では、秘密裏に情報を取得することを目的とした特殊な技術的装置を違法な作成、販売、又は販売目的で購入した場合には、20 万ルーブル以下若しくは給与その他の収入の 18 カ月以下に相当する額の罰金刑、3 年以下の自由の制限[71]、又は 3 年以下の特定の官職に就く権利若しくは特定の活動を行う権利の剥奪を伴う 3 年以下の自由刑に処することが規定されている。

（４）不正アクセス行為の国外犯

不正アクセス行為に限るものではないが、国外犯の訴追に関しては、刑法典第12条で規定されている。

刑法典第12条

「刑法典第12条　ロシア連邦の国境外で犯罪を行った者の刑法上の取扱い」第3項では、

---

[70] 1999 年 6 月 23 日のバシコルトスタン共和国における判例。インターネットサービスへの不正アクセスと利用の疑いから 2 名に対して刑法典第 158 条（窃盗）による捜査が開始された。捜査は途中で第 183 条への違反ならびに第 272 条（不正アクセス）への違反の疑いに切り替えられた。犯人らは特殊なプログラムを用いてパスワードを収集し、他のコンピュータへの侵入に使用していた。刑法典 183 条が識別符号の不正取得に適用された。SecurityWiki サイトの記事（http://securitywiki.ru/NovostnyeSoobshhenija）。

[71] 特定の時間帯の外出禁止や集会等への参加禁止等を指す（刑法典第 53 条）。

外国人がロシア国外で行った犯罪については、ロシア連邦やロシア国民の利益が侵害されており、ロシア連邦が加盟する国際条約に規定があり、かつ当該外国人が外国で有害判決を受けていない場合に、ロシア連邦の領土内における犯罪行為の訴追を受けると規定している。

したがって、被害に遭ったコンピュータがロシア国外にあり、かつ犯行者がロシア国外から当該犯罪を行った場合でも、ロシア連邦やロシア国民の利益が侵害されていれば、国外犯が適用されうる。

（５）他人の識別符号の譲渡し

ロシア刑法典では、他人の識別符号の譲渡しは直接的には規制されていない。

ただし、刑法典第 183 条の第 2 項において、商業・税務・銀行の秘密を構成する情報の不正な開示が禁じられている。上述のように、刑法典第 183 条第 1 項が他人の識別符号の不正取得に適用された判例が存在するため、第 2 項が他人の識別符号の譲渡しに適用される可能性はある。

（６）他人の識別符号の譲受け

ロシア刑法典では、他人の識別符号の譲受けは規制されていない。

（７）他人の識別符号の譲渡しに関する広告又は誘引行為

ロシア刑法典では、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

ロシア刑法典では、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。

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

ID・パスワード等の識別符号を不正取得することを目的とするものに限らないが、ウィルス作成については、刑法典第 273 条で規制されている。

刑法典第 273 条

「刑法典第 273 条　有害プログラムの作成、使用と頒布」の第 1 項では、無権限での情報の破壊、遮断、変更若しくは複製、又はコンピュータ、コンピュータ・システム若しくはネットワークに対する障害を明白に目的としたプログラムの作成若しくは既存プログラ

ムの改造、又はそのようなプログラム若しくは物理的媒体の使用若しくは頒布に対して、3年以下の自由刑及び20万ルーブル以下若しくは給与その他の収入の18カ月以下に相当する額の罰金刑に処することが規定されている。

（２）識別符号の不正取得（フィッシングサイトの構築等）

ロシア刑法典では、（識別符号の不正取得を目的とした）フィッシングサイトの構築自体を規制する条項は存在しない。

（３）サイバーテロ行為

刑法典第274条

「刑法典第274条　コンピュータ、コンピュータ・システム又はコンピュータ・ネットワークの運用規定への違反」の第1項では、コンピュータ、コンピュータ・システム又はコンピュータ・ネットワークの使用に関する規則への違反により、法の保護の対象となるコンピュータ上の情報の破壊、遮断又は変更が行われ、重大な損害が発生した場合には、5年以下の特定の官職に就く権利若しくは特定の活動を行う権利の剥奪、180時間以上240時間以下の奉仕活動、又は2年以下の禁固刑に処することが規定されている。

なお、刑法典では、行政機関や重要インフラのシステムに対するサイバーテロ行為に係る特別な規定は存在しない[72]。

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

（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

通信に関する連邦法第63条

「通信に関する連邦法第63条　通信の秘密」の第3項において、権限を有する通信事業者の従業員以外の者が、電子メールを閲覧したり、添付ファイルを表示したり、通信・郵便ネットワークによって伝達される情報及び文書通信の内容を把握したりすることは、連邦法に定められている場合を除き、裁判所の決定によってのみ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

通信に関する連邦法第64条

「通信に関する連邦法第64条　捜査活動に際しての通信事業者の義務及び利用者の権利の制限」の第1項において、通信事業者はロシア連邦の公的な捜査機関や保安機関に対し

[72] ロシアの法学者の間では、刑法典第205条（テロ行為）を政治的動機に基づく妨害行為すべてに適用できるとする見解があり、そのような見解を示している法学者は、刑法典を改正し第205条にコンピュータを利用して同様の被害をもたらした場合を明記すべきと主張している。Nauka-xxiサイトの記事（http://naukaxxi.ru/materials/298/）。

て、通信サービス利用者及び提供された通信サービスに関する情報、並びに公的捜査や保安機関が連邦法に定められた場合に法的任務の遂行に必要とする情報を提供する義務を負うことが規定されている。

（３）ログの保存

通信に関する連邦法や個人データの保護に関する連邦法には、通信事業者のログの保存期間を規定する条文は含まれていない。

４．３　不正アクセス関連法令条文集

（１）ロシア刑法典

○関連する条項の抜粋訳

第 1 編　刑法

第 2 章　刑事法への時間と空間の影響

第 12 条　ロシア連邦の国境外で犯罪を行った者の刑法上の取扱い

第 1 項　ロシア連邦の国境外で、本法による保護の下にある法益に対する犯罪を行ったロシア国民及びロシア連邦に定住している無国籍者は、当該犯行者に対して外国の法廷による訴追が行われない場合、本法の規定に基づく刑事訴追の対象となる。

第 2 項　（外国に駐留するロシア軍将兵に関する規定、略）

第 3 項　ロシア連邦内に定住していない外国人及び無国籍者がロシア連邦の国境外で犯罪を行った場合、当該犯罪によってロシア連邦、ロシア国民又はロシアに定住する無国籍者の利益が侵害されており、ロシア連邦が加盟する国際条約に規定があり、かつロシア連邦内に定住していない外国人及び無国籍者が外国で有罪判決を受けておらず、ロシア連邦の領土内で訴追を受けていない場合には、本法の規定に基づく刑事訴追の対象となる。

第 6 章　未遂犯

第 29 条　既遂犯と未遂犯

第 1 項　ある犯罪は、犯行者の行為に本法に規定されているすべての犯罪構成要素が含まれている場合に、遂行されたと見なされる。

第 2 項　犯罪の準備及び犯罪の実行を試みることは、未遂犯罪と見なされる。

第 3 項　未遂犯罪に対する刑事訴追は、第 30 条を考慮したうえで既遂犯に対する刑罰に対する条文を適用する。

第 30 条　犯罪の準備と犯罪の試み

第 1 項　犯罪を行う目的で、その手段若しくは機材を探索、作成若しくは改造したり、共犯者を募ったり、犯罪実行のために共謀したり、その他意図的に犯罪実行のための条件を創出することは、当該人物の統制外の状況下において犯罪が実行された場合を除き、犯罪の準備と見なされる。

第 2 項　犯罪の準備に対する刑事訴追は重大な、又は特に重大な犯罪行為に対してのみ行われる。

第 3 項　犯罪を行うことを明白に意図した行為（完遂しなかったもの）は、当該人物の統制外の状況下において犯罪が実行された場合を除き、犯罪の試みと見なされる。

第 19 章　人間と市民の憲法上の権利と自由に対する犯罪

第 138 条　信書、通話、郵便その他の通信の秘密の侵害

第 1 項　信書、通話、郵便、電報その他の個人が使用する通信手段の秘密の侵害に対しては、8 万ルーブル以下若しくは犯行者の給与その他の収入の 6 カ月以下に相当する額の罰金刑、又は 120 時間以上 180 時間以下の奉仕活動若しくは 1 年以下の更生労働を科す。

第2項　上記の行為を職権を濫用して行った者に対しては、10万ルーブル以上30万ルーブル以下若しくは犯行者の給与その他の収入の1年以上2年以下に相当する額の罰金刑、2年以上5年以下の特定の官職に就く権利若しくは特定の活動を行う権利の剥奪、又は6か月以下の禁固刑、若しくは特定の官職に就く権利若しくは特定の活動を行う権利の剥奪を伴う4年以下の自由刑を科す。

第 3 項　秘密裏に情報を取得することを目的とした特殊な技術的装置の違法な作成、販売、又は販売目的での購入は、20 万ルーブル以下若しくは犯行者の給与その他の収入の 18 カ月以下に相当する額の罰金刑、3 年以下の自由の制限、又は 3 年以下の特定の官職に就く権利若しくは特定の活動を行う権利の剥奪を伴う 3 年以下の自由刑に科す。

第 183 条　商業、税務、銀行の秘密を構成する情報の違法な取得と開示

第 1 項　商業、税務、銀行業務の秘密を構成する情報を、文書の窃盗、賄賂、又は脅迫その他の違法行為により取得した場合には、1 万 8,000 ルーブル以下若しくは犯行者の給与その他の収入の 1 カ月以上 6 カ月以下に相当する額の罰金刑、又は 1 年以下の奉仕活動若しくは 2 年以下の自由刑を科す。

第 2 項　所有者、代理権を有する者、又は作業若しくは業務のために認められている者の同意を得ずに、商業、税務、銀行業務の秘密を構成する情報を違法に使用したり開示したりした場合には、12 万ルーブル以下若しくは犯行者の給与その他の収入の 1 年以下に相当する額の罰金刑、特定の官職に就く権利若しくは特定の活動を行う権利の剥奪、2 年以下の更生労働、又は 3 年以下の自由刑を科す。

第 3 項　上記の行為により大規模の被害が生じた場合又は利己的な理由によってそのような行為を行った場合には、20 万ルーブル以下又は犯行者の給与その他の収入の 18 カ月以下に相当する額の罰金、及び 3 年以下の特定の官職に就く権利若しくは特定の活動を行う権利の剥奪又は 5 年以下の自由刑を科す。

第 4 項　本条第 2 項又は第 3 項の行為により重大な結果が生じた場合には、10 年以下の自由刑を科す。

第 9 編　公共の安全と秩序に対する犯罪

第 28 章　コンピュータ情報に対する犯罪

第 272 条　コンピュータ情報への不正アクセス

第1項　本法により保護の対象とされる規定されるコンピュータ上のデータ(物理的媒体、並びにコンピュータ、コンピュータ・システム及びネットワーク上のデータ）への不正アクセスによりデータの破壊、遮断、変更若しくは複製を行い、又はコンピュータ若しくはネットワークの機能に障害を与えた場合には20万ルーブル以下若しくは犯行者の給与その他の収入の18カ月以下に相当する額の罰金刑、120時間以上180時間以下の奉仕活動若しくは1年以下の更生労働、又は2年以下の自由刑を科す。
第 2 項　事前に共謀した個人の集団、犯罪組織、又は官職に在る者が同様の行為を行った場合、又はコンピュータ・システム若しくはコンピュータ・ネットワークへのアクセス権限を持つものが同様の行為を行った場合には､10万ルーブル以上30万ルーブル以下若しくは給与その他の収入の1年以上2年以下に相当する額の罰金刑、180時間以上240時間以下の奉仕活動若しくは2年以下の更生労働､又は3カ月以上6カ月以下の禁固刑若しくは5年以下の自由刑を科す。

第273条　有害プログラムの作成、使用と頒布

第 1 項　無権限での情報の破壊、遮断、変更若しくは複製、又はコンピュータ、コンピュータ・システム若しくはネットワークに対する障害を明白に目的としたプログラムの作成又は既存プログラムの改造、又はそのようなプログラム若しくは物理的媒体の使用若しくは頒布は、3年以下の自由刑、及び20万ルーブル以下若しくは給与その他の収入の18カ月以下に相当する額の罰金刑を科する。
第2項　同様な行為が、過失によって重大な結果をもたらした場合には、7年以下の自由刑を科す。

第274条　コンピュータ、コンピュータ・システム又はコンピュータ・ネットワークの運用規定への違反

第 1 項　コンピュータ、コンピュータ・システム又はコンピュータ・ネットワークの使用に関する規則への個人の違反により、法の保護の対象となるコンピュータ上の情報の破壊、遮断又は変更が行われ、重大な損害が発生した場合には、5年以下の特定の官職に就く権利若しくは特定の活動を行う権利の剥奪、180時間以上240時間以下の奉仕活動、又は2年以下の禁固刑を科す。
第2項　同様の行為が、過失によって重大な結果をもたらした場合には、4年以下の自由刑を科す。

（２）個人データの保護に関する連邦法（2006 年 7 月 27 日制定）

○関連する条項の抜粋訳

第 1 条　本連邦法の対象領域

第 1 項　本法は自動処理を用いた又は自動処理手段を用いなくとも業務の性質が自動化処理に相当する手段の使用を要求する、連邦機関、連邦の地方出先機関、及びその他の公的機関、自治体、法人、個人による個人データの取り扱いを規定する。

第 2 項　（略）

第 2 条　本連邦法の目的

本法は個人データの処理に際しての、プライバシー及び個人的・家族の秘密を含む個人の自由権を保護することを目的とする。

第 3 条　本連邦法の基本用語

本法では、以下の用語が使われる。

第 1 項　個人データ

特定の個人に関する情報、又は当該情報によって識別される個人（「個人データの主体」）に関する情報であり、氏名、生年月日、出生地、住所、家族・社会・財産の状況、教育、職業、収入その他の情報が含まれる。

第 2 項　管理者

個人データを組織化及び／又は処理し、かつ個人データの処理の目的及び範囲を決定する国の機関、自治体の機関、法人又は個人を意味する。

第 3 項　個人データの処理

個人データに対する行為（操作）であり、個人データの取得、整理、蓄積、保存、精緻化（更新、変更）、利用、頒布（移転を含む）、匿名化、遮断及び破壊が含まれる。

第 4 項　（以下略）

第 6 条　個人データの処理の条件

第 1 項　管理者による個人データの処理は、本条の第 2 項で記述される例外を除いて、個人データの主体の同意の下でなされなければならない。

第 2 項　（以下略）

第 24 条　本連邦法の要件に対する違反の際の（刑事）責任

本連邦法に違反した者は民法、刑法、行政法、秩序法その他の連邦法により訴追される。

（３）通信に関する連邦法（2003 年 6 月 25 日制定）

○関連する条項の抜粋訳

第 53 条　契約者に関する通信事業者のデータベース

第 1 項　通信サービス契約の履行のために事業者が知り得た、契約者及び契約者に提供された通信サービスに関するすべての情報は秘密であるとみなされ、ロシアの法規にもとづく保護の対象となる。

契約者に関する情報には、氏名、父称 、ユーザー名、法人契約者名（会社名）、経営者及び被用者の氏名、契約者の住所、端末の所在地、契約者番号、並びに、サービスの提供に対する課金のためのデータベースのデータ、接続データ、トラフィックデータ及び支払いデータ等、契約者又は端末の特定を可能とするその他のデータが含まれる。

第 2 項　（中略）

個人契約者に関する情報の第三者への提供は、連邦法に定められている場合を除き、契約者本人の書面による同意がある場合にのみ可能である。

第 63 条　通信の秘密

第 3 項　権限を有する通信事業者の従業員以外の者による、電子メールの閲覧、添付ファイルの表示、通信・郵便ネットワークによって伝達される情報及び文書通信の内容の把握は、連邦法に定められている場合を除き裁判所の決定によってのみ行うことができる。

第 64 条　捜査活動に際しての通信事業者の義務及び利用者の権利の制限

第 1 項　通信事業者はロシア連邦の公的な捜査機関又は保安機関に対して、通信サービス利用者及び提供された通信サービスに関する情報、並びに上記の機関が連邦法に規定された場合に法的任務の遂行に必要とする情報を提供する義務を負う。

第 2 項　通信事業者は、通信分野を管轄する連邦行政機関がロシア連邦の公的な捜査機関又は保安機関と協力して作成した、連邦法に規定された場合の通信ネットワーク及び通信設備に関する要求事項を実施すると共に、その組織的及び戦術的手法が明るみに出ないよう必要な対策を実行しなければならない。

第 3 項　自然人又は法人に対する通信サービスの停止は、連邦法に規定されている場合に、根拠を記載したロシア連邦の公的な捜査機関又は保安機関の責任者の文書による決定にもとづいて実施される。

通信事業者は、裁判所の命令、又はロシア連邦の公的な捜査機関若しくは保安機関における通信サービスの停止を決定した責任者の根拠を記した書面による決定に基づき、サービスの提供を再開しなければならない。

第 4 項　通信事業者とロシア連邦の公的な捜査機関又は保安機関の協働の手続は連邦政府

によって規定される。
第 5 項　捜査機関による捜査活動に際して、通信事業者は刑事訴訟法の定める要件に従い当該機関に対する支援を提供しなければならない。

５．中国における不正アクセス関連法令

５．１　中国における不正アクセス関連犯罪の現状

（１）中国におけるサイバー犯罪の急増

中国のコンピュータ・ネットワークは 1970 年代に構築され、1994 年から国際インターネットへのアクセスを本格的に開始した。その後、中国において国際インターネットは凄まじい勢いで発展し、インターネット人口の規模も急速に拡大していった。中国インターネット・ネットワーク情報センター（China Internet Network Information Center、CNNIC）の『中国インターネット発展状況統計報告』によると、中国のインターネット・ユーザー数は 2008 年にすでに米国を抜いて世界第 1 位になったという。また、当該センターが 2011 年 7 月に公表した『第 28 回中国インターネット発展状況統計報告』によると、2011 年 6 月 30 日現在、中国のインターネット・ユーザー総数はすでに 4.85 億人に達し、普及率は 36.2%に上昇した。そのうち、携帯電話によるインターネット・ユーザーは 3.18 億人で、インターネット人口全体に占める割合は 65.5%となっている。また、自宅のパソコンによるブロードバンド・インターネット接続による利用者の規模も 3.9 億人に達し、自宅パソコンによるインターネット人口の実に 98.8%を占めている。

コンピュータとインターネットの国内普及率が日増しに高まるにつれ、中国もまた世界的ネットワークでの違法・犯罪行為の主要な被害国の一つになっている。

コンピュータ・ネットワークを利用した中国初の犯罪事件は 1986 年 7 月 22 日に発生した。香港の利用者が深センのある銀行で預金を引き出した時、口座から 2 万元が消えていることを発見した。さらに 2 カ月後、同様に深センで、別の利用者が銀行に預けていた 3 万香港ドルも口座から消えていた。後に、この 2 件の事犯は同一犯罪者がコンピュータの知識を利用して詐取したものであることが判明した。

今後中国ではコンピュータ・ネットワークに係る犯罪が大幅に増加すると見られる。各種の従来型犯罪とサイバー犯罪とが組み合わさって実行される傾向が日増しに顕著になっており、インターネット詐欺やインターネット窃盗等といった他人の財産を侵害する犯罪、コンピュータ・ウィルスの作成・頒布、コンピュータとネットワークへの侵入・攻撃といった犯罪が急速に増え、インターネットを利用してのわいせつ・アダルト画像の頒布、賭博等の不正行為も依然として非常に多い。統計[73]によると、1998 年に中国の公安局の処理した各種サイバー犯罪検挙件数は 142 件であったが、2008 年には 3.5 万件と激増、この 10 年間で 250 倍近くに増え、2010 年には更に 4.9 万件に達した。注意すべきなのは、サイバー犯罪の実際の発生件数は、公安局が受理した件数よりはるかに多いということである。

[73] 2010 年 6 月 8 日に国務院新聞弁公室の発表した『中国インターネット状況白書』。

（２）中国におけるサイバー犯罪の主な特徴

第一の特徴として、サイバー犯罪では異なるグループにより役割分担、利益分配の利益チェーンが徐々に形成され、各種サイバー犯罪が相互に融合浸透しているという点が挙げられる。サイバー犯罪者はトロイの木馬型ウィルス、インターネット詐欺等の手口で不正に金銭を得ており、次第に一つの「産業」に発展、さらに一本の完全な「闇産業チェーン」が形成されている。ウィルスの作成者も従来は単独で行動していたのが、細かい役割分担をする集団化運営を展開するようになっている。現在中国ではすでに、ウィルスの作成・頒布により不法に金銭を収奪する闇組織「ウィルス集団」が横行する傾向にある。その内部の役割分担は明確で、リーダーが指令を下し、ハッカープログラマーがウィルスの「作成」を担当し、その後エンジニアがウィルスを埋め込むウェブサイトとウェブページを構築し、最後に「ネット水軍」が掲示板でインターネット・ユーザーを騙しておびき寄せる。報道によると､現在国内インターネットで暗躍しているウィルス集団は少なくとも 30 あり、大半のウィルス頒布経路は、黄飛虎集団、HYC 集団、HY 集団、老蛇集団、192 集団、GZWZ 集団、CL 集団、張峰集団、WG 集団、安妮（アニー）集団という 10 の超巨大なウィルス集団によって握られている。これら「ウィルス集団」の行動は徹底して隠蔽され、IP アドレスも頻繁に変更される。ウィルス頒布の主要な行為には、商業サイト（主に中小規模のナビゲーションサイト、悪質サイト、動画ダウンロードサイト）のためにアクセス量を引き上げることや、商用ソフトウェア（これらソフトウェアにはしばしば各種プラグイン・ソフトウェアがバンドルされており、ブラウザ起動時に接続するページを改ざんし、奇妙なポップアップ広告を出現させる）の促進、フィッシングサイトの推進により感染者を騙すこと、その他ウィルス（主にオンラインゲームを攻撃するパスワード盗用型トロイの木馬）の推進が含まれる。この 10 大ウィルス集団はインターネット上の約 80%のウィルスダウンロードルートをすでにその支配下においており、またこれにより巨額な違法収益を得ている。毎年の収益が数億元に達するウィルス集団もある。

第二の特徴は、サイバー犯罪者による海外ネットワーク資源を利用した犯罪行為が目立っている点である。特に中国のインターネット賭博、インターネット詐欺の犯罪行為は、主に海外の犯罪集団に制御されており、中国のサイバー犯罪者が構築しているフィッシングサイト、アダルトサイト等の違法サイト及び使用する電子メールボックス等のネットワーク資源は、主に米国等の国々にある。前出の統計によると、中国で調査されたサイバー犯罪事件のうち、90%超の詐欺、フィッシング、アダルト、賭博等の違法サイト及び 70%超のゾンビ・ネットワークの制御側は海外にある。2010 年、国家コンピュータ・ネットワーク応急技術処理協調センター（CNCERT）の監視の結果、約 48 万個のトロイの木馬制御側 IP のうち、22.1 万個が海外にあることがわかった（そのうち最も多かったのが米国（14.7%）、次がインド（8.0%）、3 番目が台湾（4.8%）だった)。また計 13,782 個のゾンビ・ネットワークの制御側 IP のうち 6,531 個が海外にあることも発見された（最も多かったのは米国（21.7%）、次がインド（7.2%）、3 番目がトルコ（5.7%）だった)。2010 年、

中国で行われたドライブ・バイ・ダウンロード[74]、インターネット上のフィッシング等、不法行為により利用された悪意のあるドメイン名の半数以上は海外で登録されたものであった。

第三の特徴は、中国の重要なネッワーク情報システムと公共ネットワークがサイバー犯罪者の重要なターゲットとなっている点である。CNCERT が 2011 年 4 月に発表した『2010 中国インターネット・ネットワーク・セキュリティ・レポート』では、中国の重要なネットワーク情報システムと公共ネットワークのセキュリティが緊迫した状況にあることが指摘されている。これについて、主に以下のような説明がある。

1. 政府機関のウェブサイトのセキュリティ保護に脆弱性が生じている。2010 年、中国で約 3.5 万ヵ所のウェブサイトがハッカーに改ざんされた。その数は 2009 年より 21.5%減少したが、そのうち改ざんされた政府機関のウェブサイトは 4,635 ヵ所に達し、2009 年比で 67.6%増加した。中央や省レベルの政府機関ウェブサイトのセキュリティ状況は、地方都市以下の政府機関ウェブサイトより明らかに優れているが、依然として約 60%の部・委員会レベルのウェブサイトにさまざまな程度のセキュリティ・ホールが存在している。
2. 金融業のウェブサイトは、サイバー犯罪者にとって金銭を詐取しプライバシーを盗み取る格好のターゲットとなっている。金銭目的のサイバー犯罪行為が顕著になり、大型電子商取引、金融機関、第三者オンライン決済サイトがフィッシングの主要ターゲットとなっている。ハッカーはこうしたウェブサイトを模倣したりショッピングサイトを偽造してユーザーがログインし取引するよう誘い込み、そのアカウントとパスワードを盗み取ってユーザーに経済的損失を被らせている。2010 年に CNCERT が受理したフィッシング事件の通報件数は 1,597 件、2009 年比 33.1%増だった。また同年に「中国アンチフィッシングサイト連合会」が処理したフィッシングサイト事件は 20570 件、2009 年比 140%増加した。
3. 産業の制御システム上のセキュリティも深刻な問題に直面している。2010 年 9 月、イランのブシェール原子力発電所が Stuxnet というウィルスによるサイバー攻撃に遭い、原発施設の始動遅延が起きた。セキュリティ業界では、これが仮想世界から現実世界への初のネットワーク攻撃であると一般的に認識されている。
4. トロイの木馬とゾンビ・ネットワークは、依然としてネットワークのセキュリティにとって直接的な脅威となっている。2010 年、監視範囲を広げたところ、CNCERT では年間計 500 万個近い国内ホストの IP アドレスがトロイの木馬とゾンビプロセスに感染し、2009 年よりも大幅に増加していることが発見された。監視結果からは、2009 年データに比べて遠隔操作の類によりトロイの木馬とゾンビ・ネットワークに操作されるホスト数は 25%減少したため、管理作業が一定の効果をあげたことがわ

[74] 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。

かる。しかしながら、ハッカーも絶え間なく技術的な対抗能力を高めている。2010年に検挙された悪質なコードの件数、特にトロイの木馬の件数は、2009年に比べ明らかに増加している。またCNNICのデータも、2011年の上半期、ウィルス又はトロイの木馬攻撃を受けたインターネット・ユーザーが2.17億人に達したことを示している。

5. 携帯電話向けのマルウェアがますます頒布されるようになっている。モバイル・インターネットが利用できるスマート端末の普及に伴い、携帯電話向けのマルウェアが出現し、急速に蔓延しつつある。サイバー犯罪者は携帯電話向けのマルウェアを利用してユーザーのプライバシー情報を盗み取り、悪意をもって各種付加価値サービスを注文したり大量の迷惑メールを送信し、ユーザーの利益とネットワーク・セキュリティに危害を及ぼしている。「中国インターネット協会アンチネットワーク・ウィルス連合会（ANVA）」の監視データによると、2010年に新たに検挙した携帯電話向けのマルウェアは1,600個余りあり、感染したスマート端末の総数は計800万台以上に上った。そのうち、“AVK.DuMusic”（中国語は「毒媒」）プログラムに感染したユーザー携帯電話は年間累計で約200万台余りあり、「携帯ドクロ」プログラムに感染したユーザーの携帯電話も累計83万台余りあった。その他、携帯電話のプラットホームについて見ると、Symbianプラットホームが携帯電話向けマルウェア感染の主要なターゲットとなっており、約69%のマルウェアが当該プラットホームの携帯電話向けであり、次いでJ2MEプラットホーム（27%）、Androidプラットホーム（3%）の順となっている。

6. DDoS攻撃がネットワーク・セキュリティに危害を及ぼしている。2010年は、DDoS攻撃としてファーミング攻撃とフラッディング攻撃に特徴があった。同年にある政府機関ウェブサイトでトラフィック異常事件が発生、また騰訊（Tencent）の業務システムが何度も攻撃に遭ったのは、遊戯私服（ゲーム名）の4つのウェブサイトが攻撃され、そのウェブドメインから騰訊の業務システムに悪意を持ってトラフィックが差し向けられたためである。また、DDoS攻撃のトラフィックはますます大きくなっており、“456 ゲーム”ウェブサイトに対する攻撃トラフィックのピークが100Gbpsを超えるなど、公共インターネットの安全性に大きな衝撃を与えている。攻撃トラフィックのソースの多くには虚偽IPアドレスが使われており、攻撃行為の追跡や応急処置作業が難航している。

（3）中国におけるサイバー犯罪の被害

CNNICとCNCERTが2010年3月に連名で発表した『2009年中国インターネット・ユーザーネットワーク情報セキュリティ状況調査報告書』によると、2009 年に 52%のネット・ユーザーが、ネットワーク・セキュリティ事件に遭ったことがあるという。ユーザーが遭ったネットワーク・セキュリティ事件のうち、ウィルス、トロイの木馬等の悪質なコ

ードがコンピュータに侵入する事件が大半を占めた。調査結果からは、インターネット上からのダウンロードとウェブサイトの閲覧がウィルスとトロイの木馬頒布の主要経路となっており、77.5%のインターネット・ユーザーがインターネット上からのダウンロードやウェブサイト閲覧時にウィルスやトロイの木馬の攻撃を受けたことがわかった。次に多かったのが、USB メモリ、ポータブルハードディスク、光ディスクなどのリムーバブル記録媒体がウィルス若しくはトロイの木馬頒布の二次経路となるケースで、26.9%のインターネット・ユーザーがこれによって攻撃を受けていた。

2009 年、ネットワーク・セキュリティ事件によりインターネット・ユーザーが被った最も直接的な損失は、事件を処理するために費やした時間的コストだった。77.3%のネット・ユーザーが、ネットワーク・セキュリティ事件に遭遇した際、多くの時間を費やして対処しなければならなかったとしている。統計によると、1 人当たり平均約 10 時間かけてセキュリティ事件を処理していた。

2009 年にネットワーク・セキュリティ事件により国内の 21.2%のインターネット・ユーザーが受けた直接的経済の損失には、インスタント・メッセンジャー、オンラインゲーム等のアカウントが盗まれたことによる仮想財産の損失、オンラインバンクのパスワードやアカウントが盗まれたことによる財産損失、さらにネットワークシステムや OS のフリーズ、データ・ドキュメントなどの紛失又は損壊により、回復・修復に生じた費用等があった。ネット・ユーザーがネットワーク・セキュリティ事件を処理するために支出した費用について統計したところ、2009 年にユーザーがセキュリティ事件処理のために支出した費用は総額 153 億元であった。また、費用が発生したユーザーの一人当たり費用は約 588.9 元であった。

（4）中国におけるサイバー犯罪の取締

中国は法に基づきネットワークを利用した違法・犯罪行為を取り締まることを極めて重視しており、立法、法令の遵守、司法、技術等各方面により対策を通じ、サイバー犯罪全体を取り締まってきた。近年では中国の公安局によるサイバー犯罪に対する特別の取締活動が不断に展開されている。それと同時に、他の関係部署、地方自治体、関連企業も、サイバー犯罪行為取締活動に積極的に参加している。中国では特に以下の取締に力を入れている。

- ネット上でのわいせつ・アダルト物頒布
- ネット上の治安問題
- ネット賭博の違法・犯罪行為
- ネット上の権利侵害行為
- ネット上での偽証明書作成・販売の違法情報
- ハッカー攻撃・破壊行為
- 知的財産権侵害と偽造・粗悪品製造・販売犯罪

・ ネットワークの闇ウィルス産業チェーン

５．２　不正アクセス行為関連法令の実態

５．２．１　不正アクセス関連法令の概要

中国ではサイバー犯罪規制関連の法令は、主に 2 つの面から構成されている。一つはネットワークを利用してのわいせつ・アダルト物頒布、賭博、詐欺、禁制品の違法販売、知的財産権侵害等に対して従来型犯罪の法令に基づいて処罰することである。二つ目はハッカー攻撃・破壊行為に対して刑法の中で独立した犯罪として処罰することである。現在のところ、中国ではネットワークに関係した法令（法律・法規・規則）を計 200 余り公布・施行しており、ネットワーク・セキュリティ、ネットワーク運営の秩序、電子商取引、個人情報保護及びネットワークの知的財産権等の領域をカバーするネットワーク法律体系を形成している。このうち、不正アクセス行為や不正アクセスの助長行為等を規制する関連法令については、以下のものが挙げられる。

（１）コンピュータ・ネットワークの安全を保障する法令

インターネットの安全を守るため、「中華人民共和国刑法（2011 年最終改正）」、「（全国人民代表大会常務委員会の）インターネットの安全維持に関する決定（2000 年可決）」、「中華人民共和国治安管理処罰法（2005 年可決）」、「中華人民共和国電気通信条例[75]（2000 年公布）」、「中華人民共和国コンピュータ情報システム安全保護条例（1994 年公布）」、「インターネット情報サービス管理規則（2000 年公布）」、「コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則（1997 年公布）」等の法令でコンピュータ・ネットワークの安全に危害を及ぼす違法・犯罪行為について関連規定を制定することで、中国のインターネットの健全な発展を促進し、国家の安全と社会の公共利益を守り、個人・法人及び他の組織の合法的権益を保護している。

---

[75] 中国では「条例」は地方的法規を指すこともあれば全国的法規を指すこともあるが、本条例は国務院が定めた全国的法規である。なお、中国の実定法源は、憲法を頂点として、以下、「中華人民共和国立法法」において概ね下記のものが定められている。(1) 法律：全国人民代表大会、全国人民代表大会常務委員会が制定、全国に適用する。(2) 行政法規（条例、規則等）：国務院が憲法と法律に基づいて国務院が制定、全国に適用する。(3) 地方性法規（条例）：省・自治区・直轄市の人民代表大会及びその常務委員会が制定する。又は、大きな市（省・自治区の人民政府が所在、経済特区が所在等）の人民代表大会及びその常務委員会が制定し行政区域内で適用する。(4) 部門規章（規則等）：国務院の各部や委員会、中国人民銀行、審計署と行政管理職能を備えた国務院直属の機構が法律と国務院の行政法規・決定・命令に基づき、当該部門の権限の範囲において制定、全国に適用する。(5) 地方政府規章：省・自治区・直轄市と大きな市の人民政府が法律、行政法規と当該省・自治区・直轄市の地方性法規に基づいて制定し、行政区域内において適用する。

（２）コンピュータ資産を保護する法令

コンピュータ資産を保護する法令として、「中華人民共和国コンピュータ・ソフトウェア保護条例（1991 年公布）」や「中華人民共和国刑法」第 287 条（1997 年改正）がある。後者では、コンピュータを利用しての金融詐欺、窃盗、汚職、公金着服、国家機密の盗取又はその他犯罪を行った場合、刑法の関係規定に従い処罰すると規定されている。

（３）コンピュータ・ネットワーク上の個人情報の保護する法令

コンピュータ・ネットワーク上の個人情報を保護する法令として、「中華人民共和国刑法改正案（2009 年）」や、「ウェブサイトでのニュース掲載業務従事管理暫定規定（2000 年公布）」、「インターネット電子公告サービス管理規定（2000 年公布）」がある。「中華人民共和国刑法改正案（2009 年）」では、個人情報の販売や不正取得、提供に対する罪を規定した。また、「中華人民共和国権利侵害責任法（2010 年 7 月 1 日施行）」において、国民個人のプライバシー権保護を明確に規定した。その他、「中華人民共和国電気通信条例」等の法令にも個人情報を保護する規定が盛り込まれている。

５．２．２　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

中国では、国事等に関係するコンピュータ・システムへの侵入行為については、刑法第 285 条第 1 項において規制が行われている。また、それ以外のコンピュータ・システムに侵入等をして、その結果として当該システム内のデータを取得したり、不法な制御を行ったりすることについては、刑法第 285 条第 2 項において規制が行われている。

また、コンピュータ・システム一般に侵入し危害を及ぼす行為については、中華人民共和国治安管理処罰法第 29 条においても規制が行われている。

なお、上記のような犯罪行為や、治安管理に対する違反行為に至らない場合でも、「コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則」において、公安局は警告を与えたり、罰金等の処分を下したりできることが規定されている。

刑法第 285 条

刑法第 285 条第 1 項（コンピュータ・システムへの不法侵入罪）では、国家の規定に違反し、国事、国防建設、先端科学技術領域のコンピュータ・システムに侵入した場合、3 年以下の拘禁刑又は拘留刑に処することが規定されている。

刑法第 285 条第 2 項（コンピュータ・システム・データの不正取得、コンピュータ・システムの不法制御罪）では、国家の規定に違反し、前項規定以外のコンピュータ・システムに侵入するか、又は他の技術手段により、当該システム内で保存、処理又は伝送しているデータを取得するか、又は当該システムに対して不法な制御を行い、その状況が深刻な

場合、3 年以下の拘禁刑又は拘留刑に処し、罰金を併科又は単科することが規定されている。また、状況が特に深刻な場合は、3 年以上 7 年以下の拘禁刑に処し、また罰金も併科することが規定されている。

中華人民共和国治安管理処罰法第 29 条

中華人民共和国治安管理処罰法第 29 条では、国家の規定に違反し、コンピュータ情報システムに侵入して危害を及ぼした場合、5 日以下の勾留に処することが規定されている。また、状況が特に深刻な場合、5 日以上 10 日以下の勾留に処することが規定されている。

コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則第 6 条

コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則第 6 条では、許可を得ることなくコンピュータ・ネットワークにアクセスしたり、コンピュータ・ネットワークの資源を使用する行為等を禁止している。同規則の第 20 条では、第 6 条で禁止された行為がある場合、公安局は警告を与え、個人に対しては 5,000 元以下の罰金を、企業・団体に対しては 15,000 元以下の罰金を科せることが規定されている。また、状況が特に深刻な場合は、6 カ月以内のインターネット接続中止、コンピュータ作動停止の処分を下すことができる。さらに、治安管理に対する違反行為を構成する場合、治安管理処罰条例の規定に基づき処罰し、犯罪を構成する場合は、法に基づき刑事責任を追及することが規定されている。

不正アクセスの未遂行為について

中国の刑法等では、不正アクセスの未遂罪については規定されていない。

（２）データの財物性（データの不正取得）

個人情報データを不正に取得する行為については、刑法第 253 条の 1 で規制されている。また、コンピュータ・システムに侵入等をして、その結果として当該システム内のデータを取得することについては、上述のように刑法第 285 条第 2 項で規制が行われている。

また、電気通信ネットワークを利用して他人の情報を窃盗し、他人の合法的権益に損害を与える行為については、中華人民共和国電気通信条例第 58 条で規制が行われている。

刑法第 253 条の 1

刑法第 253 条の 1 では、国家機関又は金融、通信、交通、教育、医療等の組織が職場において職責を履行する、又はサービスを提供する過程において取得した公民の個人情報を窃盗又はその他の非合法な手段で取得した場合、3 年以下の拘禁刑又は拘留刑に処し、罰金を併科又は単科することが規定されている。

個人情報の定義については、法律の規定は存在しないが、氏名、性別、生年月日、民族、

身分証番号、血液型、指紋、戸籍、婚姻状況、家庭状況、教育的背景（学歴）、職歴、健康情報、財務状況など、単独で、又はその他の情報と照合して個人を識別するために用いることができるあらゆる情報が含まれるということが基本的コンセンサスとして形成されている。

中華人民共和国電気通信条例第 58 条

中華人民共和国電気通信条例第 58 条では、電気通信ネットワークを利用して他人の情報を窃盗又は破壊し、他人の合法的権益に損害を与える行為を禁じている。

なお、刑法第264条では財物に対する窃盗罪について規定しているが、データ一般は窃盗罪の対象となる財物とはみなされていない。

（３）不正アクセス行為の予備行為

中国の法令には、外部からのシステム探索（セキュリティ・ホールのスキャン）等の不正アクセスの予備行為を規制する条文はない。

（４）不正アクセス行為の国外犯

中国の法令には、不正アクセスする行為等の国外犯の規制に係る条文はない。

（５）他人の識別符号の譲渡し

識別符号は通常は個人情報に該当しないが、識別符号が個人情報に該当する場合には、そのような識別符号を提供する行為については、刑法第 253 条の 1 を適用することが可能である。

刑法第 253 条の 1

刑法第253条の1の第1項では、国家機関又は金融、通信、交通、教育、医療等の組織職員が国家規定に違反し、職場において職責を履行する、又はサービスを提供する過程において取得した公民の個人情報を第三者に販売、又は非合法的に提供することを禁じている。

ID・パスワード等の識別符号そのものは、通常はそれだけでは個人を識別できないので個人情報に該当しないと考えられるが、他の情報（氏名等）と照合して個人を識別することができる場合には、個人情報に該当しうる。

第253条の1の第1項の違反は、3年以下の拘禁刑又は拘留刑に処し、罰金を併科又は単科することが規定されている。

（６）他人の識別符号の譲受け

識別符号は通常は個人情報に該当しないが、識別符号が個人情報に該当する場合には、

そのような識別符号を不正に取得する行為については、刑法第 253 条の 1 を適用することが可能である。

刑法第 253 条の 1

刑法第253条の1の第2項では、国家機関又は金融、通信、交通、教育、医療等の組織が職場において職責を履行する、又はサービスを提供する過程において取得した公民の個人情報を窃盗又はその他の非合法な手段で取得した公民の個人情報を非合法的な手段で取得することを禁じている。

ID・パスワード等の識別符号そのものは、通常はそれだけでは個人を識別できないので個人情報に該当しないと考えられるが、他の情報（氏名等）と照合して個人を識別することができる場合には、個人情報に該当しうる。

第253条の1の第2項の違反は、3年以下の拘禁刑又は拘留刑に処し、罰金を併科又は単科することが規定されている。

（７）他人の識別符号の譲渡しに関する広告又は誘引行為

中国の法令には、他人の識別符号を提供することを内容とした広告や誘引行為を規制する条文はない。

（８）他人の識別符号の譲受けに関する広告又は誘引行為

中国の法令には、他人の識別符号を譲り受けることを内容とした広告や誘引行為を規制する条文はない。

５．２．３　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

コンピュータ・ウィルス等の破壊型プログラムを故意に作成、頒布して、コンピュータ・システムの正常な運用に影響を及ぼす行為については、刑法第 286 条第 3 項及び中華人民共和国治安管理処罰法第 29 条において規制が行われている。

なお、上記のような犯罪行為や、治安管理に対する違反行為に至らない場合でも、「コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則」において、公安局は警告を与えたり、罰金等の処分を下したりできることが規定されている。同様の趣旨は、中華人民共和国電気通信条例においても規定されている。

刑法第 286 条

刑法第 286 条（コンピュータ情報システム損壊罪）の第 3 項では、コンピュータ・ウィルス等の破壊型プログラムを故意に作成、頒布して、コンピュータ・システムの正常な運

用に影響を及ぼし、重大な結果を引き起こした場合、5 年以下の拘禁刑又は拘留刑に処することが規定されている。

中華人民共和国治安管理処罰法第 29 条

中華人民共和国治安管理処罰法第 29 条では、コンピュータ・ウィルス等の破壊型プログラムを故意に作成、頒布し、コンピュータ情報システムの正常な運用に影響を及ぼした場合、5 日以下の勾留に処することが規定されている。また、状況が特に深刻な場合、5 日以上 10 日以下の勾留に処することが規定されている。

コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則第 6 条

コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則第 6 条では、コンピュータ・ウィルス等の破壊型プログラムを故意に作成、頒布する行為等を禁止している。同規則の第 20 条では、第 6 条で禁止された行為がある場合、公安局は警告を与え、個人に対しては 5,000 元以下の罰金を、企業・団体に対しては 15,000 元以下の罰金を科せることが規定されている。また、状況が特に深刻な場合は、6 カ月以内のインターネット接続中止、コンピュータ作動停止の処分を下すことができる。さらに、治安管理に対する違反行為を構成する場合、治安管理処罰条例の規定に基づき処罰し、犯罪を構成する場合は、法に基づき刑事責任を追及することが規定されている。

中華人民共和国電気通信条例

中華人民共和国電気通信条例第 58 条では、コンピュータ・ウィルスを故意に作成、複製、頒布する行為等を禁じている。

第 58 条の違反は、当該行為が犯罪を構成する場合は法に基づいて刑事責任を追及し、犯罪を構成しない場合は公安局や国家安全局[76]が関係の法律や行政法規の規定に基づき処罰する旨が、第 67 条において規定されている。

（２）識別符号の不正取得（フィッシングサイトの構築等）

中国の法令には、（ID・パスワード等の識別符号の不正取得を目的として）フィッシングサイトの構築自体を規制する条文は存在しない。ただし、フィッシングサイトの構築等を通じて他人の財産等を詐取する行為については、刑法第 287 条や、「インターネットの安全維持に関する決定」の第 4 条で規制が行われていると考えられる。

刑法第 287 条

刑法第 287 条（コンピュータを利用して実施される各種犯罪）では、コンピュータを利用して金融詐欺、窃盗等を行った場合、この法律の関係規定に基づき罪を決定して処罰す

[76] 中国における情報機関。

ることが規定されている。

インターネットの安全維持に関する決定（2000 年）

インターネットの安全維持に関する決定の第 4 条では、インターネットを利用して窃盗、詐欺、恐喝を行い、当該行為が犯罪を構成する場合、刑法の関係規定に基づき刑事責任を追及することが規定されている。

なお、中国では「詐欺」とは、不法に占有することを目的として、事実の虚構又は真相の隠蔽の方法を用いて、比較的多額の公的又は私的財産を騙し取る行為を指す。詐欺罪が成立するためには、不法に公的又は私的財産を占有する犯行者の目的が構成要件として必要である。

詐欺罪に対する罰則は、刑法第 266 条において、3 年以下の拘禁刑、拘留刑又は管制[77]に処し、罰金を併科又は単科することが規定されている。また占有した財産額が巨額であるか、又はその他状況が深刻であるものは、3 年以上 10 年以下の拘禁刑に処し、罰金を併科すること、さらに金額が特に莫大であるか、又はその他状況が特に深刻であるものは、10 年以上の拘禁刑又は無期拘禁刑に処すとともに、罰金を科すか、又は財産を没収することが規定されている。

（3）サイバーテロ行為

コンピュータ・システムに干渉することで、当該システムの正常な運用を不可能にする行為については、刑法第 286 条第 2 項及び中華人民共和国治安管理処罰法第 29 条において規制が行われている。

なお、上記のような犯罪行為や、治安管理に対する違反行為に至らない場合でも、「コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則」において、コンピュータ情報ネットワークのセキュリティに危害を及ぼす行為について、公安局は警告を与えたり、罰金等の処分を下したりできることが規定されている。同様の趣旨は、中華人民共和国電気通信条例においても規定されている。

刑法第 286 条

刑法第 286 条（コンピュータ情報システム損壊罪）の第 2 項では、国家の規定に違反して、コンピュータ・システムの機能を削除、変更、追加、干渉することで、当該システムの正常な運用を不可能にし、重大な結果を引き起こした場合、5 年以下の拘禁刑又は拘留刑に処することが規定されている。また、その結果が特に重大な場合は、5 年以上の拘禁刑に処することが規定されている。

[77] 3 カ月から 2 年以下の期間内に公安局の監督の下、一定の自由を制限しながら社会生活を送らせる刑罰。

「重大な結果を引き起こした場合」や「その結果が特に重大な場合」の具体的な解釈については、「コンピュータ情報システムの安全に危害を加える刑事案件の処理に応用される法律の若干の問題に関する解釈」の第 4 条において規定されており、「国家機関又は金融、電気通信、交通、教育、医療、エネルギー等の分野において公共サービスを提供しているコンピュータ情報システムの機能、データ又はアプリケーション・プログラムを破壊し、生産、生活に重大な影響を与えたか、又は劣悪な社会的影響を引き起こした場合」については、「その結果が特に重大な場合」に該当する旨が規定されている。

中華人民共和国治安管理処罰法第 29 条

中華人民共和国治安管理処罰法第 29 条では、国家の規定に違反し、コンピュータ・システムの機能を削除、修正、追加、干渉することで、当該システムの正常な運用を不可能にした場合、5 日以下の勾留に処することが規定されている。また、状況が特に深刻な場合、5 日以上 10 日以下の勾留に処することが規定されている。

コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則第 6 条

コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則第 6 条では、コンピュータ情報ネットワークのセキュリティに危害を及ぼす行為等を禁止している。同規則の第 20 条では、第 6 条で禁止された行為がある場合、公安局は警告を与え、個人に対しては 5,000 元以下の罰金を、企業・団体に対しては 15,000 元以下の罰金を科せることが規定されている。また、状況が特に深刻な場合は、6 カ月以内のインターネット接続中止、コンピュータ作動停止の処分を下すことができる。さらに、治安管理に対する違反行為を構成する場合、治安管理処罰条例の規定に基づき処罰し、犯罪を構成する場合は、法に基づき刑事責任を追及することが規定されている。

中華人民共和国電気通信条例

中華人民共和国電気通信条例第 58 条では、他人の電気通信ネットワーク等の電気通信施設を攻撃する行為等を禁じている。

第 58 条の違反は、当該行為が犯罪を構成する場合は法に基づいて刑事責任を追及し、犯罪を構成しない場合は公安局や国家安全局が関係の法律や行政法規の規定に基づき処罰する旨が、第 67 条において規定されている。

５．２．４　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

中華人民共和国電気通信条例第 66 条

中華人民共和国電気通信条例の第 66 条において、何らかの組織や個人が電気通信内容を

検査することは一般原則として禁止されているが、国家の安全又は刑事犯罪の捜査の必要から、公安局、国家安全局又は人民検察院が法に定めるプロセスに基づき電気通信内容に対して検査を行うことは認められている。

また、中華人民共和国コンピュータ情報システム安全保護条例の第 17 条では、公安局は、コンピュータ情報システムの保護作業に対し、コンピュータ情報システムの安全に危害を及ぼす違法犯罪事件の調査に関する監督職権を行使できることが規定されている。

（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

インターネット情報サービス管理規則第 14 条

インターネット情報サービス管理規則の第 14 条において、インターネット接続サービス事業者は、ネット・ユーザーのアクセス時間、ユーザー・アカウント、インターネット・アドレス（URL）若しくはドメイン名、発信者電話番号等の情報を記録しなければならず、国家の関係機関が法に基づき問い合わせる際にこれを提供することが規定されている。

第 14 条に定める義務が履行されない場合には、省、自治区、直轄市の電気通信管理機関が是正を命じ、状況が深刻な場合は、営業停止又はウェブサイトの一時閉鎖を命ずることが、第 21 条において規定されている。

（３）ログの保存

インターネット情報サービス管理規則第 14 条

インターネット情報サービス管理規則の第 14 条において、インターネット接続サービス事業者の上記記録のバックアップは 60 日間保存することが規定されている。

第 14 条に定める義務が履行されない場合には、省、自治区、直轄市の電気通信管理機関が是正を命じ、状況が深刻な場合は、営業停止又はウェブサイトの一時閉鎖を命ずることが、第 21 条において規定されている。

５．３　不正アクセス関連法令条文集

（１）中華人民共和国刑法（1979 年 7 月 1 日可決、2011 年 2 月 25 日最終改正）

○関連する条項の抜粋訳

第 253 条の 1

第 1 項　国家機関又は金融、通信、交通、教育、医療等の組織職員が国家規定に違反し、職場において職責を履行する、又はサービスを提供する過程において取得した公民の個人情報を第三者に販売、又は非合法的に提供して、その状況が深刻である場合、3 年以下の拘禁刑又は拘留刑に処し、罰金を併科又は単科する。

第 2 項　前出情報を窃取又はその他の非合法な手段で取得し、その状況が深刻な場合は、前項の規定に基づいて処罰するものとする。

第 3 項　組織が前二項の罪を犯した場合、組織に罰金を科す。直接責任を負う責任者及びその他の直接担当者を各該当号の規定に基づいて処罰するものとする。

第 264 条

公私の財物を窃盗し、窃盗物件が多い若しくは複数回にわたって窃盗した場合、住宅に侵入して窃盗した場合、凶器を携帯して窃盗した場合、すり取った場合は 3 年以下の拘禁刑、拘留刑又は管制に処し、罰金を併科又は単科する。窃盗物件が膨大である若しくは状況が深刻である場合は 3 年以上 10 年以下の拘禁刑に処し、罰金を併科する。窃盗物件が特に膨大である又は状況が特に深刻である場合は 10 年以上の拘禁刑又は無期拘禁刑に処し、罰金を併科又は財産を没収する。

第 266 条

公的又は私的財産を騙し取った場合、金額が大きな場合は、3 年以下の拘禁刑、拘留刑又は管制に処し、罰金を併科又は単科する。巨額であるか、又はその他状況が深刻であるものは、3 年以上 10 年以下の拘禁刑に処し、罰金を併科する。。金額が特に特に莫大であるか、又はその他状況が特に深刻であるものは、10 年以上の拘禁刑又は無期拘禁刑に処すとともに、罰金を科すか、又は財産を没収する。本法に別の規定がある場合には、当該規定に従う。

第 285 条

第 1 項　国家の規定に違反し、国事、国防建設、先端科学技術領域のコンピュータ情報システムに侵入した場合、3 年以下の拘禁刑又は拘留刑に処す。

第 2 項　国家の規定に違反し、前項規定以外のコンピュータ情報システムに侵入するか、又は他の技術手段により、当該コンピュータ情報システム内で保存、処理又は伝送しているデータを取得するか、又は当該コンピュータ情報システムに対して不法な制御を行い、その状況が深刻な場合、3 年以下の拘禁刑又は拘留刑に処し、罰金を併科又は単科する。状況が特に深刻な場合は、3 年以上 7 年以下の拘禁刑に処し、また罰金も併科する。
第 3 項　コンピュータ情報システムへの侵入用や不法な制御用のプログラム及びツールを提供し、又は、他人がコンピュータ情報システムへ侵入したり不法に制御するといった違法・犯罪行為を行うことを明確に認識しているにもかかわらず、プログラムやツールを提供し、その状況が深刻な場合、前項の規定に基づき処罰する。

第 286 条
第 1 項　国家の規定に違反して、コンピュータ情報システムの機能を削除、変更、追加、干渉することで、コンピュータ情報システムの正常な運用を不可能にし、重大な結果を引き起こした場合、5 年以下の拘禁刑又は拘留刑に処す。
第 2 項　また、その結果が特に重大な場合は、5 年以上の拘禁刑に処す。国家の規定に違反し、コンピュータ情報システム内で保存、処理又は伝送しているデータとアプリケーション・プログラムを削除、修正、追加し、重大な結果を引き起こした場合、前項の規定に基づき処罰する。
第 3 項　コンピュータ・ウィルス等の破壊型プログラムを故意に作成、頒布して、コンピュータ・システムの正常な運用に影響を及ぼし、重大な結果を引き起こした場合、第 1 項の規定に基づき処罰する。

第 287 条
コンピュータを利用して金融詐欺、窃盗、汚職、公金着服、国家機密の盗取又はその他犯罪を行った場合、この法律の関係規定に基づき罪を決定して処罰する。

（2）中華人民共和国治安管理処罰法（2005 年 8 月 28 日可決・公布、2006 年 3 月 1 日施行）

○関連する条項の抜粋訳

第 29 条
下記のいずれかの行為に該当する場合、5 日以下の勾留に処す。状況が特に深刻な場合、5 日以上 10 日以下の勾留に処す。
（一）国家の規定に違反し、コンピュータ情報システムに侵入して危害を及ぼした場合。

（二）国家の規定に違反し、コンピュータ情報システムの機能を削除、修正、追加、干渉することで、コンピュータ情報システムの正常な運用を不可能にした場合。
（三）国家の規定に違反し、コンピュータ情報システム内で保存、処理、伝送しているデータ及びアプリケーション・プログラムを削除、修正、追加した場合。
（四）コンピュータ・ウィルス等の破壊型プログラムを故意に作成、頒布し、コンピュータ情報システムの正常運用に影響を及ぼした場合。

（３）全国人民代表大会常務委員会「インターネットの安全維持に関する決定」（2000 年 12 月 28 日可決）

○関連する条項の抜粋訳

第 1 条
インターネットの運用における安全を保障するため、下記のいずれかの行為に該当し、犯罪を構成する場合、刑法の関係規定に基づき刑事責任を追及する。
（一）国事、国防建設、先端科学技術の領域のコンピュータ情報システムに侵入した場合。
（二）コンピュータ・ウィルス等の破壊型プログラムを故意に作成、頒布し、コンピュータ・システム及び通信ネットワークを攻撃することで、コンピュータ・システム及び通信ネットワークに損害を与えた場合。
（三）国家の規定に違反し、無断でコンピュータ・ネットワーク又は通信サービスを中断し、コンピュータ・ネットワーク又は通信システムの正常な運用を不可能にした場合。

第 4 条
個人、法人及びその他組織の人身、財産等の合法的権益を保護するため、下記のいずれかの行為に該当し、犯罪を構成する場合、刑法の関係規定に基づき刑事責任を追及する。
（一）インターネットを利用して他人を侮辱したり事実を捏造して他人を誹謗した場合。
（二）他人の電子メール又は他のデータ資料を不正に取得、改ざん、削除し、国民の通信の自由と通信の秘密を侵害した場合。
（三）インターネットを利用して窃盗、詐欺、恐喝を行った場合。

（４）コンピュータ情報ネットワークの国際ネットワーク接続安全保護管理規則（1997 年 12 月 11 日国務院承認、同年 12 月 30 日公安部公布・施行）

○関連する条項の抜粋訳

第 6 条

いかなる事業者も個人も、下記のようなコンピュータ情報ネットワークの安全に危害を及ぼす行為を行ってはならない。

（一）許可を得ることなく、コンピュータ情報ネットワークにアクセスしたり、コンピュータ情報ネットワークの資源を使用する行為。

（二）許可を得ることなく、コンピュータ情報ネットワークの機能を削除、修正又は追加する行為。

（三）許可を得ることなく、コンピュータ情報ネットワーク内に保存、処理又は送信しているデータ及びアプリケーション・プログラムを削除、修正又は追加する行為。

（四）コンピュータ・ウィルス等の破壊型プログラムを故意に作成、頒布する行為。

（五）その他コンピュータ情報ネットワークのセキュリティに危害を及ぼす行為。

第 20 条

法律、行政法規に違反し、本規則の第 5 条、第 6 条に掲げられるいずれかの行為がある場合、公安局は警告を与え、また違法所得があった場合はこれを没収し、個人に対しては 5,000 元以下の罰金を、企業・団体に対しては 15,000 元以下の罰金を併科することができる。状況が特に深刻な場合は、6 カ月以内のインターネット接続中止、コンピュータ作動停止の処分を下すことができる。また必要な場合は、原承認書発給・承認機関に経営許可証の返上又はネットワーク接続資格を取り消すようアドバイスすることもできる。治安管理に対する違反行為を構成する場合、治安管理処罰条例の規定に基づき処罰する。犯罪を構成する場合は、法に基づき刑事責任を追及する。

（５）中華人民共和国コンピュータ情報システム安全保護条例（1994 年 2 月 18 日国務院公布・施行）

○関連する条項の抜粋訳

第 17 条

公安局は、コンピュータ情報システムの保護作業に対し下記の監督職権を行使する。

（一）コンピュータ情報システムの安全保護作業の監督、検査、指導。

（二）コンピュータ情報システムの安全に危害を及ぼす違法犯罪事件の調査。

（三）コンピュータ情報システムの安全保護作業のその他監督職責の履行。

第 23 条

コンピュータ・ウィルス及びその他有害データを故意に入力してコンピュータ情報システ

ムの安全に危害を及ぼした場合、又は許可を得ることなくコンピュータ情報システムのセキュリティ専用製品を販売した場合、公安局は警告するか、又はその個人に対し 5,000 元以下の罰金を、企業・団体に対しては 15,000 元以下の罰金を科す。違法所得があった場合は、これを没収するほか、違法所得の 2～3 倍の罰金を科すことができる。

第 28 条

本条例における用語の意味は以下のとおりである。

コンピュータ・ウィルスとは、コンピュータ機能を破壊又はデータを毀損して、コンピュータの使用に影響を与える目的で作成され、コンピュータ・プログラム内に入り込んで自己増殖することもできるコンピュータ・コマンド若しくはプログラム・コードのことをいう。

コンピュータ情報システムのセキュリティ専用製品とは、コンピュータ情報システムの安全を保護するために用いる専用のハードウェアとソフトウェア製品をいう。

（６）中華人民共和国電気通信条例（2000 年 9 月 20 日国務院可決、同年 9 月 25 日国務院公布・施行）

<u>○関連する条項の抜粋訳</u>

第 58 条

いかなる組織又は個人も、下記の電気通信ネットワークの安全と情報の安全に危害を及ぼす行為があってはならない。

（一）電気通信ネットワークの機能若しくは保存、処理、伝送するデータとアプリケーション・プログラムを削除又は修正する行為。

（二）電気通信ネットワークを利用して他人の情報を窃盗又は破壊し、他人の合法的権益に損害を与える行為。

（三）コンピュータ・ウィルスを故意に作成、複製、頒布するか、又は他の方式で他人の電気通信ネットワーク等の電気通信施設を攻撃する行為。

（四）電気通信ネットワークの安全と情報の安全に危害を及ぼすその他の行為。

第 66 条

電気通信ユーザーが法に基づいて電気通信を利用する自由と通信の秘密は、法律によって保護される。国家の安全又は刑事犯罪の捜査の必要から、公安局、国家安全局又は人民検察院が法に定めるプロセスに基づき電気通信内容に対して検査を行う場合を除き、いかなる組織又は個人も、なんらかの理由で電気通信内容を検査することはできない。

電気通信事業者及びその従業者は、電気通信ユーザーが電気通信ネットワークを利用して伝送した情報内容を、無断で他人に提供してはならない。

第 67 条

本条例第 57 条、第 58 条の規定に違反し、犯罪を構成する場合、法に基づいて刑事責任を追及する。犯罪を構成しない場合は、公安局、国家安全局が関係の法律、行政法規の規定に基づき処罰する。

（7）インターネット情報サービス管理規則（2000 年 9 月 20 日国務院可決、同年 9 月 25 日国務院公布・施行）

○関連する条項の抜粋訳

第 14 条

ニュース、出版及び電子公告等のサービス項目に従事するインターネット情報サービス・プロバイダは、提供した情報内容及びその発表時間、インターネット・アドレス（URL）若しくはドメイン名を記録しなければならない。インターネット接続サービス事業者は、ネット・ユーザーのアクセス時間、ユーザー・アカウント、インターネット・アドレス（URL）若しくはドメイン名、発信者電話番号等の情報を記録しなければならない。
インターネット情報サービス・プロバイダとインターネット接続サービス事業者の記録のバックアップは 60 日間保存するとともに、国家の関係機関が法に基づき問い合わせる際にこれを提供すること。

第 21 条

本規則第 14 条に定める義務を履行しない場合、省、自治区、直轄市の電気通信管理機関が是正を命ずる。状況が深刻な場合は、営業停止又はウェブサイトの一時閉鎖を命ずる。

（８）コンピュータ情報システムの安全に危害を加える刑事案件の処理に応用される法律の若干の問題に関する解釈[78]**（2011 年 6 月 20 日最高人民法院審判委員会第 1524 回会議、2011 年 7 月 11 日最高人民検察院第 11 期検察委員会第 63 回会議で可決、2011 年 9 月 1 日より施行）**

○法令の全文訳

法に基づきコンピュータ情報システムの安全に危害を加える犯罪活動を懲治するため、『中華人民共和国刑法』、『全国人民代表大会常務委員会のインターネット・セキュリティ保護に関する決定』の規定を根拠として、現在このような刑事案件の処理に応用される法律についての若干の問題に関する解釈は次の通りである。

第 1 条

第 1 項　コンピュータ情報システムのデータの不法取得、又はコンピュータ情報システムの不法制御において、次のいずれかの状況がある場合、刑法第 285 条第 2 項に規定する「状況が深刻」であると認定する。

（一）支払決済、証券取引、先物取引等のネットワーク金融サービスの ID 認証情報を 10 組以上取得した場合。

（二）第（一）号以外の ID 認証情報を 500 組以上取得した場合。

（三）コンピュータ情報システムを 20 台以上不法制御した場合。

（四）5,000 元以上を違法に取得したか、又は 10,000 元以上の経済損失を引き起こした場合。

（五）その他状況が深刻な場合。

第 2 項　前項に規定する行為の実行において、次のいずれかの状況がある場合、刑法第 285 条第 2 項に規定する「状況が特に深刻」であると認定する。

（一）数量又は金額が前項第（一）号から第（四）号に規定する標準の 5 倍以上に達する場合。

（二）その他状況が特に深刻な場合。

第 3 項　他人が不法に制御するコンピュータ情報システムであると知っていながら、そのコンピュータ情報システムに対する制御権を利用した場合、前 2 項の規定に従い罪を定めて処罰する。

第 2 条

[78] 正式名称は、「最高人民法院最高人民検察院の、コンピュータ情報システムの安全に危害を加える刑事案件の処理に応用される法律の若干の問題に関する解釈」。

次の状況のいずれかに該当するプログラム、ツールは、刑法第 285 条第 3 項に規定する「コンピュータ情報システムへの侵入用や不法な制御用のプログラム及びツール」であると認定する。

（一）コンピュータ情報システムのセキュリティ保護措置を回避又は突破し、権限付与を経ないで、又は認められた権限を超過して、コンピュータ情報システムのデータを取得する機能を備えたもの。

（二）コンピュータ情報システムのセキュリティ保護措置を回避又は突破し、権限付与を経ないで、又は認められた権限を超過して、コンピュータ情報システムに対し制御を実施する機能を備えたもの。

（三）その他コンピュータ情報システムへの侵入、不法制御、コンピュータ情報システムのデータの不法取得に用いるために専門的に設計されたプログラム、ツール。

第 3 条

第 1 項　コンピュータ情報システムに対する侵入、不法制御を行うプログラム、ツールの提供において、次の状況のいずれかに該当するものは、刑法第 285 条第 3 項に規定する「状況が深刻」であると認定する。

（一）支払決済、証券取引、先物取引等のネットワーク金融サービス ID 認証情報を不法に取得するために用いることができる専門的なプログラム、ツールを延べ 5 人以上に提供した場合。

（二）第（一）号以外に、コンピュータ情報システムの侵入、不法制御に専門的に用いられるプログラム、ツールを延べ 20 人以上に提供した場合。

（三）他人が支払決済、証券取引、先物取引等のネットワーク金融サービス ID 認証情報を不法に取得する違法犯罪行為を実行すると知っていながら、それに対して延べ 5 人以上にプログラム、ツールを提供した場合。

（四）他人が第（三）号以外に、コンピュータ情報システムに対する侵入、不法制御の違法犯罪行為を実行すると知っていながら、それに対して延べ 20 人以上にプログラム、ツールを提供した場合。

（五）5,000 元以上を違法に取得したか、又は 10,000 元以上の経済損失を引き起こした場合。

（六）その他状況が深刻な場合。

第 2 項　前項に規定する行為の実行において、次の状況のいずれかに該当する場合、コンピュータ情報システムに対する侵入、不法制御を行うプログラム、ツールの提供の「状況が特に深刻」であると認定する。

（一）数量又は金額が前項第（一）号から第（五）号の規定する標準の 5 倍以上に達する場合。

（二）その他状況が特に深刻な場合。

第 4 条

第 1 項　コンピュータ情報システムの機能、データ又はアプリケーション・プログラムの破壊において、次の状況のいずれかに該当する場合、刑法第 286 条第 1 項と第 2 項に規定する「重大な結果」であると認定する。

（一）10 台以上のコンピュータ情報システムの主要ソフトウェア又はハードウェアの正常な運用を不可能にした場合。

（二）20 台以上のコンピュータ情報システム中において保存、処理、又は伝送されたデータに対して削除、変更、操作の追加を行った場合。

（三）5,000 元以上を違法に取得したか、又は 10,000 元以上の経済損失を引き起こした場合。

（四）100 台以上のコンピュータ情報システムに対してドメイン名の解析、ID 認証、料金計算等の基礎サービスを提供している、又は 10,000 以上のユーザーに対してサービスを提供しているコンピュータ情報システムの正常な運用を、累計 1 時間以上にわたって不可能にした場合。

（五）その他の重大な結果を引き起こした場合。

第 2 項　前項に規定する行為の実行において、次の状況のいずれかに該当する場合、コンピュータ情報システム破壊の「結果が特に重大」であると認定する。

（一）数量又は金額が前項第（一）号から第（三）号に規定する標準の 5 倍以上に達する場合。

（二）500 台以上のコンピュータ情報システムに対してドメイン名の解析、ID 認証、料金計算等の基礎サービスを提供している、又は 50,000 以上のユーザーに対してサービスを提供しているコンピュータ情報システムの正常な運用を、累計 1 時間以上にわたって不可能にした場合。

（三）国家機関又は金融、電気通信、交通、教育、医療、エネルギー等の分野において公共サービスを提供しているコンピュータ情報システムの機能、データ又はアプリケーション・プログラムを破壊し、生産、生活に重大な影響を与えたか、又は劣悪な社会的影響を引き起こした場合。

（四）その他の特に重大な結果を引き起こした場合。

第 5 条

次の状況のいずれかに該当するプログラムは、刑法第 286 条第 3 項に規定する「コンピュータ・ウィルス等の破壊的プログラム」であると認定する。

（一）ネットワーク、ストレージ・メディア、ファイル等のメディアを通じて、そのプログラム自身の一部、全部、又は変種の複製、頒布を行うことができるとともに、コンピュータ・システムの機能、データ、又はアプリケーション・プログラムを破壊できるもの。

（二）あらかじめ設定された条件下で自動的にトリガーできるとともに、コンピュータ・システムの機能、データ又はアプリケーション・プログラムを破壊できるもの。

（三）その他コンピュータ・システムの機能、データ又はアプリケーション・プログラムの破壊に用いるために専門的に設計されたプログラム。

第 6 条

第 1 項　コンピュータ・ウィルス等の破壊的プログラムを故意に製作、頒布し、コンピュータ・システムの正常な運用に影響を与え、次の状況のいずれかに該当する場合、刑法第 286 条第 3 項に規定する「結果が重大」であると認定する。

（一）第 5 条第（一）号の規定するプログラムを製作、提供、伝送し、そのプログラムがネットワーク、ストレージ・メディア、ファイル等のメディアを通じて頒布された場合。

（二）20 台以上のコンピュータ・システムに対し、第 5 条第（二）、（三）号に規定するプログラムの埋め込みを引き起こした場合。

（三）コンピュータ・ウィルス等の破壊的なプログラムを延べ 10 人以上に提供した場合。

（四）5,000 元以上を違法に取得した、又は 10,000 元以上の経済損失を引き起こした場合。

（五）その他の重大な結果を引き起こした場合。

第 2 項　前項に規定する行為の実行において、次の状況のいずれかに該当する場合、コンピュータ情報システム破壊の「結果が特に重大」であると認定する。

（一）第 5 条第（一）号に規定するプログラムを製作、提供、伝送し、そのプログラムがネットワーク、ストレージ・メディア、ファイル等のメディアを通じて頒布され、生産、生活に重大な影響を与えたか、又は劣悪な社会的影響を引き起こした場合。

（二）数量又は金額が前項第（二）号から第（四）号の規定する標準の 5 倍以上に達する場合。

（三）その他の特に重大な結果を引き起こした場合。

第 7 条

第 1 項　コンピュータ情報システム・データの不法取得犯罪により取得されたデータであること、コンピュータ情報システムの不法制御犯罪により取得されたコンピュータ情報システムの制御権であることを知っていながら、移転、買取、代理販売、又はその他の方法で粉飾、隠蔽し、5,000 元以上を違法に取得した場合、刑法第 312 条第 1 項の規定に従い、犯罪所得の粉飾、隠蔽罪で有罪として処罰する。

第 2 項　前項の規定する行為を実行し、50,000 元以上を違法に取得した場合、刑法第 312 条第 1 項の規定する「状況が深刻」であると認定する。

第 3 項　組織が第 1 項の規定する行為を実行した場合、有罪量刑基準は第 1 項、第 2 項の規定に従い実行する。

第 8 条

組織名義又は組織の形式でコンピュータ情報システムの安全に危害を加える犯罪を実行し、本解釈の規定する有罪量刑基準を満たす場合、刑法第 285 条、第 286 条の規定に従い、直接責任を負う管理者とその他直接責任者の刑事責任を追究する。

第 9 条

第 1 項　他人が刑法第 285 条、第 286 条に規定する行為を実行すると知っており、次の状況のいずれかに該当する場合、共同犯罪と認定し、刑法第 285 条、第 286 条の規定に従い処罰する。

（一）その他人に対してコンピュータ情報システムの機能、データ又はアプリケーション・プログラムの破壊に用いるプログラム、ツールを提供し、5,000 元以上を違法に取得したか、又は延べ 10 人以上に提供した場合。

（二）その他人に対してインターネット・アクセス、サーバー・コロケーション、ネットワーク・ストレージ空間、通信伝送チャネル、費用清算、取引サービス、広告サービス、技術トレーニング、技術支援等の支援を提供し、5,000 元以上を違法に取得した場合。

（三）ソフトウェアの普及委託、広告掲載等の方法を通じて、その他人に対して 5,000 元以上の資金を提供した場合。

第 2 項　前項の規定する行為を実行し、数量又は金額が前項に規定する標準の 5 倍以上に達する場合、刑法第 285 条、第 286 条の規定する「状況が特に深刻」又は「結果が特に重大」であると認定する。

第 10 条

刑法第 285 条、第 286 条の規定する「国家事務、国防建設、先端科学技術分野のコンピュータ情報システム」、「コンピュータ情報システムの侵入、不法制御に専門的に用いられるプログラム、ツール」、「コンピュータ・ウィルス等の破壊的プログラム」に属するかどうかの確定が困難な場合、省級以上のコンピュータ情報システム・セキュリティ保護管理作業を担当する部門に検査を委託する。司法機関は検査の結論を根拠にするとともに、案件の具体的な状況と結びつけて認定する。

第 11 条

第 1 項　本解釈にいう「コンピュータ情報システム」と「コンピュータ・システム」とは、コンピュータ、ネットワーク設備、通信設備、自動化制御設備等を含む、データ自

動処理機能を備えたシステムを指す。
第 2 項　本解釈のいう「ID 認証情報」とは、アカウント、パスワード、デジタル証明書等を含む、ユーザーがコンピュータ情報システム上で操作アクセス権を確認するために用いるデータを指す。
第 3 項　本解釈にいう「経済損失」とは、コンピュータ情報システムに危害を加える犯罪行為によりユーザーが直接被った経済損失、及びユーザーがデータ、機能を回復するために支払った必要な費用を含む。

諸外国における不正アクセスの助長行為等を規制する
関連法令に係る調査
報告書

平成 23(2011)年 10 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