平成 19 年度内閣官房情報セキュリティセンター委託調査

サイバー空間における権利利益の保護・救済のための基盤に係る調査研究

報告書

平成 20 年 3 月

株式会社三菱総合研究所

はじめに

近年、ネットワークは企業や家庭に浸透し、社会のあらゆる場所でネットワークが利用されるに至っている。サイバー空間は、こうしたネットワーク上に出現した新たな空間であり、サイバー空間においては、実空間と同様に権利が存在するとともに、権利の侵害も日常化している。

本報告書は、サイバー空間における権利と権利侵害の実態を踏まえ、それらに対する対策について、法令を中心に述べたものである。

第 1 章では、日本国憲法を俯瞰し、サイバー空間における権利を列挙し、現状問題となっているサイバー空間における権利侵害の事例と、それらに対する対策を調査するための論点（調査の視点）を記している。

第 2 章では、論点に沿って、国内外の動向を整理している。対象とした国等は、日本、米国、英国、ドイツ、韓国、EU である。論点に対して、可能な限り表形式で各国の動向をまとめ、表の前後に解説文を付した。

第 3 章では、第 2 章の動向を整理した上、今後のサイバー空間における権利保護・救済のための検討の方向性等について総評した。

本報告書を通して、サイバー空間における権利利益の保護・救済についての課題認識や対策の方向性の示唆を示すことができれば幸いである。

なお、本報告書は、株式会社三菱総合研究所が内閣官房情報セキュリティセンターより受託した「サイバー空間における権利利益の保護・救済のための基盤に係る調査研究」の成果報告書である。

目次

本報告書に記載している URL は、すべて 2008 年 3 月 28 日現在、閲覧可能であったことを確認している。

1. サイバー空間における権利

1.1. 我が国における権利一般とサイバー空間における権利

日本国憲法及び法律で定められている権利を参照し、サイバー空間に関係する権利を明確にする。

日本国憲法においては、基本的人権が定められている。基本的人権は、人権ないし基本権などとも呼ばれ、個別的人権を総称する用語である（芦部信喜、高橋和之補訂『憲法第四版』、岩波書店を参考）。サイバー空間における様々な権利は、基本的人権から派生するものと考えられる。

日本国憲法における人権は、包括的基本権、法の下の平等、自由権、国務請求権（受益権）、参政権、社会権に分類される。このうち、法の下の平等以外の権利に関して述べる。

（1）包括的基本権

包括的基本権は、幸福追求権（憲法第 13 条）を中心とするものである。幸福追求権から導出される人権には、プライバシー権、環境権、日照権、嫌煙権等が含まれる。また、最高裁大法廷は、1986 年 6 月 11 日の判決で、名誉権を幸福追求権の一つとして認めた。このうち、名誉権とプライバシー権がサイバー空間との係わりがあり、本調査の対象は、名誉権及びプライバシー権のうち、肖像権、自己情報コントロール権[1]とする。

（2）自由権

自由権は、精神の自由、経済の自由及び人身の自由から成る。

精神の自由には、思想・良心の自由（憲法第 19 条）、信教の自由（憲法 20 条）、学問の自由（大学の自治）（憲法第 23 条）、表現の自由（憲法第 21 条）、集会・結社の自由（憲法第 21 条）、通信の秘密の確保（憲法第 21 条）等が該当する。このうち、サイバー空間においては、表現の自由（電子掲示板やホームページでの表現の自由の保障等）、通信の秘密の確保が関係する。

経済の自由は、居住・移転の自由（憲法第 22 条）、移動・国籍離脱の自由（憲法第 22 条）、職業選択の自由（憲法第 22 条）、財産権（憲法第 29 条）等から成る。このうち特にサイバー空間においては、物権、知的財産権との関係が深いと考えられる。また、電子記録債権

[1] もっとも、自己情報コントロール権はまだ確立された権利とはいえない。プライバシーの権利はもともと「私生活をみだりに公開されない法的保障ないし権利」（東京地裁昭和 39 年 9 月 28 日判決「宴のあと事件」）という自由権的なものと理解されてきたが、情報化社会の進展にともない、自由権的側面のみならず、自己の情報をコントロールする権利として、積極的に公権力に対してプライバシーの保護を請求していくという側面が重視されるようになってきている（参考：芦部信喜、高橋和之補訂『憲法第四版』、岩波書店、2007 年 3 月、pp.118-119）。

法成立により、債権もサイバー空間との関係が発生している。

人身の自由には、奴隷的拘束の禁止（憲法第 18 条)、法定手続の保障（憲法第 31 条） 、住居の不可侵（憲法第 35 条)、令状なき捜索・押収の否定（憲法第 33 条)、黙秘権（憲法第 38 条)、弁護人依頼権（憲法第 37 条）他から成る。このうち、サイバー空間においては、ログ保存に言及するため、令状なき捜索・押収の否定を本調査の対象とする。

（3）国務請求権（受益権）

国務請求権（受益権）には、請願権・陳情権（憲法第 16 条)、裁判を受ける権利（憲法第 32 条)、国家賠償・補償請求権（憲法第 17 条）等から成るとされる。本調査においては、国務請求権を調査対象としていない。

（4）参政権

選挙権（憲法第 15 条、79 条、95 条)、被選挙権 、公務員の選定・罷免の権利 、憲法改正権（憲法第 96 条)、国民審査権（憲法第 79 条 2 項）等から成る。本調査においては、参政権を調査対象としていない。

（5）社会権

社会権は、生存権（憲法第 25 条)、教育を受ける権利（憲法第 26 条)、勤労の権利（憲法第 27 条)、労働基本権（団結権・団体交渉権・団体行動権）（憲法第 28 条）等から成る。本調査においては、社会権を調査対象としていない。

以上より、本調査におけるサイバー空間における権利を表 1.1-1 に示す。

表 1.1-1　本調査におけるサイバー空間における権利

大分類	中分類	サイバー空間において関連の深い小分類
幸福追求権	人格権	プライバシー権（肖像権、自己情報コントロール権)、名誉権
自由権	精神の自由	表現の自由、通信の秘密
	経済の自由	物権、債権、財産権（知的財産権）
	人身の自由	令状なき捜索・押収の否定

1.2.　サイバー空間における権利と関連する法令

サイバー空間における権利と関連する法令を整理する。

表 1.2-1　サイバー空間における権利と関連する法令

	関連する法令	侵害の例
人格権		
プライバシー権	憲法 13 条、民法 709 条・710 条	電子掲示板で、疾病情報などのプライバシー情報を書き込まれた。
肖像権	憲法 13 条、民法 709 条・710 条	ホームページに了解なしに、顔写真を掲載された。
自己情報コントロール権	憲法 13 条、個人情報保護法	承諾なく、顧客データベースに個人情報を蓄積された。
名誉権	憲法 13 条、民法 710 条・723 条、刑法 230 条	電子掲示板で、不当に非難された。
自由権　精神の自由		
表現の自由（報道及び言論の自由、創作の自由、知る権利が含まれる）		
	憲法 21 条	電子掲示板運営者によって、了解なしに、公序良俗に反しない書き込みを消去された。
通信の秘密	憲法 21 条、電気通信事業法、不正アクセス禁止法	通信事業者によって、了解なしに検閲された。
自由権　経済の自由		
物権	憲法 14 条・29 条、不正競争防止法	従業員の Winny 等のファイル共有ソフトの使用により、営業秘密が流出した。
債権	憲法 14 条・29 条、電子記録債権法	電子債権記録に、不実な記載がなされた。
知的財産権	憲法 13 条・29 条	
特許権	特許法	インターネット上のビジネスモデルに係る特許が侵害された。
実用新案権	実用新案法	インターネット上の実用新案が侵害された。
意匠権	意匠法	承諾なしにキャラクタを利用された。
著作権（著作権は、著作権と著作近接権から成る）	著作権法	著作物を無断で引用された。
商標権	商標法	商標登録されている文言を、無断でホームページ上に掲載された。
自由権　身体の自由		
令状なき捜索・押収の否定	刑事訴訟法	通信ログに関して、当局により令状なく押収された。

1.3. サイバー空間における権利侵害の事例と論点

本節では、サイバー空間における権利に対する侵害の事例を明らかにした上で、本調査での各権利に関する調査の論点を抽出する。

サイバー空間における権利侵害の事例は、以下に例示する。

表 1.3-1 サイバー空間における権利侵害の事例

区分	権利	サイバー空間における侵害の例
人格権	プライバシー権	・ 電子掲示板で、疾病情報などのプライバシー情報を書き込まれた。 ・ 当人の了解なしに、ホームページにプライバシー情報を書き込まれた。
	肖像権	・ ホームページに了解なしに、顔写真を掲載された。 ・ 顔写真を了解なしに、P2P ソフトウエアにてファイル共有可能とされた。
	自己情報コントロール権	・ 承諾なく、顧客データベースに個人情報を蓄積された。 ・ 要求しているにも係らず、データベースから個人情報を削除されなかった。
	名誉権	・ 電子掲示板で、不当に非難された。 ・ 電子掲示板で、子どもが他の子どもをいじめる（ネットいじめ）。
自由権 精神の自由	表現の自由（報道及び言論の自由、創作の自由、知る権利、が含まれる）	・ 電子掲示板運営者によって、了解なしに、公序良俗に反しない書き込みを消去された。 ・ プロバイダ等が、当人の了解なしに、当人のホームページを他人に対して閲覧不能とした。
	通信の秘密	・ プロバイダ等が、当人の了解なく、プロバイダ責任制限法や裁判所の令状にも基づかないにも係らず第三者に発信者情報開示を行った。 ・ メールサーバに不正にアクセスし、他人のメールを閲覧した。
自由権 経済の自由	物権	・ 従業員が、Winny 等のファイル共有ソフトの使用により、営業秘密が流出した。 ・ 従業員が、企業の営業秘密を個人用パソコンにダウンロードし、第三者に提供した。
	債権	・ 電子債権記録に、不実な記載がなされた。
自由権 経済の自由のうち知的財産権	特許権	・ インターネット上のビジネスモデルに係る特許が侵害された。 ・ 公開されていた特許が閲覧され、不当に特許が利用された。
	実用新案権	・ インターネット上の実用新案が侵害された。
	意匠権	・ 承諾なしに、キャラクタを利用された。
	著作権（著作権は、著作権と著作隣接権から成る）	・ 著作物を無断で引用された。 ・ 著作権者の承諾なく、ビデオ画像をインターネット上で送信可能な状態にした。
	商標権	・ 商標登録されている文言を、無断でホームページ上に掲載された。
自由権 身体の自由	令状なき捜索・押収の否定	・ 通信ログに関して、当局により令状なく押収された。

一方、調査の論点は、諸外国の立法の動向を踏まえ、以下のとおり設定した。

（1）サイバー空間における人権と自由権（精神の自由、経済の自由）を確保するための対策に係る論点（調査の視点）

1）サイバー空間におけるプライバシー権、肖像権及び名誉権の保護に関して特別な措置がなされているか

2）プロバイダ等に対する発信者情報開示に対する特別な措置はなされているか

3）利用者が不適切なパケットの送信停止及びネット上の掲載情報の削除を要求する枠組みはあるか

4）サイバー空間での個人情報漏えいに関する特別な措置がなされているか

5）ネットいじめに関する特別な措置がなされているか

6）サイバー空間上での営業秘密の漏えいに関して特別な措置がなされているか

7）オンライン海賊版に関し特別な措置がなされているか

8）Winny 等 P2P ソフトウエアの開発者に対して、特別な措置がなされているか

（2）サイバー空間と関係する自由権（身体の自由）を確保するための対策に係る論点（調査の視点）

9）通信ログの保存に関する枠組みはあるか

（3）共通的な論点（調査の視点）

多くのサイバー空間の権利侵害の要因になる事項として、ネットワークへの匿名アクセスとウイルス製造等が存在し、これらに関しては、以下の論点で調査を行う。

１０）サイバー空間の様々な権利侵害の要因となる可能性の高いネットワークへの匿名のアクセスに関する特別な措置がなされているか

１１）ウイルス製造・保持・頒布に関する措置がなされているか

１２）情報セキュリティに関する基本法が制定されているか

表 1.3-2 に、サイバー空間における権利と論点（調査の視点）の関係を示す。

表 1.3-2　本調査における論点（調査の視点）と権利との関係

○：調査の視点と権利の関係が深いことを示す

	人格権				自由権 精神の自由		自由権 経済の自由		自由権 経済の自由のうち知的財産権					自由権 身体の自由
本調査における論点（調査の視点）	プライバシー権	肖像権	自己情報コントロール権	名誉権	表現の自由	通信の秘密	物権	債権	特許権	実用新案権	意匠権	著作権	商標権	令状なき捜索・押収の否定
サイバー空間におけるプライバシー権、肖像権及び名誉権の保護に関して措置がなされているか	○	○		○										
プロバイダ等に対する発信者情報開示に対する措置はなされているか	○	○		○										
利用者が不適切なパケットの送信停止及びネット上の掲載情報の削除を要求する枠組みはあるか	○	○	○	○										
サイバー空間での個人情報漏えいに関する措置がなされているか	○	○	○	○										
ネットいじめに関する特別な措置がなされているか				○										
サイバー空間上での営業秘密の漏えいに関して措置がなされているか							○							
オンライン海賊版に関し特別な措置がなされているか									○	○	○	○	○	
Winny 等 P2P ソフトウエアの開発者に対して、特別な措置がなされているか												○		
通信ログの保存に関する枠組みはあるか														○
ネットワークへの匿名のアクセスに関する特別な措置がなされているか	○	○	○	○	○	○	○	○	○	○	○	○	○	
ウイルス製造・保持・頒布に関する措置がなされているか	○	○	○	○	○	○	○	○	○	○	○	○	○	
情報セキュリティに関する基本法が制定されているか	○	○	○	○	○	○	○	○	○	○	○	○	○	

2. 国内外のサイバー空間における権利侵害への対策

本章では、表 1.3-2 で整理した論点（調査の視点）に沿って、国内外におけるサイバー空間における権利侵害への対策について述べる。

2.1. サイバー空間における人権と自由権（精神の自由、経済の自由）を確保するための対策に係る論点

2.1.1. サイバー空間におけるプライバシー権、肖像権及び名誉権の保護に関して措置がなされているか

サイバー空間においては、情報の仲介者に関して、電子掲示板等管理者、プロバイダ（ネットワークへの論理的な接続事業者）、通信事業者（通信回線の提供者）に分けて考えることができる。このうち、通信事業者は情報の仲介者としての責任を問われる可能性は極めて低い。

こうした状況を加味し、サイバー空間におけるプライバシー権、肖像権及び名誉権の侵害に関して、責任は以下のように分類する。

1） 発言者の刑事及び民事に係る責任
2） プロバイダの刑事及び民事に係る責任
3） 電子掲示板等管理者の刑事及び民事に係る責任

表 2.1.1-1 に、上記１）～３）それぞれに関して整理する。

表 2.1.1-1　ネットワーク上の名誉毀損に関する法的枠組み

	日本	米国	英国	ドイツ	韓国	EU
1) 発言者の刑事及び民事に係る責任	刑法 230 条及び民法 709 条の名誉毀損による。	連邦刑法、連邦民法による。	名誉毀損法（1996）による。	不法行為法と刑法による。	刑法 307 条、308 条、309 条の名誉毀損による。	なし。
2)プロバイダの刑事及び民事に係る責任	プロバイダ制限責任法にて規定。	通信品位法に規定が存在する（第 230 条）。 第三者から提供された情報の発行者とは扱われない。	名誉毀損法（1996）に規定が存在する（第 1 条(3)(e)）。 プロバイダは、文書（statement）の作者（author）、editor（編集者）又は発行者（publisher）としてみなされない。 責任なしの裁判例あり（バント対ティリー事件）。	テレメディア法第 7 条～第 10 条において、プロバイダの責任制限が規定されている。民法による損害賠償請求や刑法に基づく罰則は免責されているが、情報の除去や利用の停止を含む民法上の不作為請求権については免責を受けない。	情報通信サービス提供者は、個人の権利が侵害された者から削除又は反論内容の掲載の要請を受けた場合には遅滞なく必要な措置を取らなければならず、当該措置により賠償責任を減免される。	電子商取引の法的側面に関する EU 指令にて、プロバイダの責任に関して制限が記述されている。
3)電子掲示板等管理者の刑事及び民事に係る責任	民法 709 条に基づき、運営・管理者の損害賠償責任及び発言削除義務が認められる方向である。	責任なしの裁判例あり(ゼラン対 AOL、バレット対ローゼンタールの裁判例)。	同上。	電子掲示板等管理者は、他人の情報を仲介しているのみであるため、情報の削除義務は認められない方向である。	同上。	同上。

（参考資料）

(1) http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/tsushin_houseikikaku/pdf/071019_1_si3.pdf

(2) http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/tsushin_houseikikaku/pdf/071102_1_si4.pdf

(3) http://www.meti.go.jp/report/downloadfiles/g10903gj.pdf

(4) http://ec.europa.eu/information_society/activities/sip/programme/index_en.htm

(5) http://www.geocities.co.jp/WallStreet/9133/

.

（1）日本

1）発言者の刑事的及び民事的責任

サイバー空間においては、発言者は、リアル空間の場合と同様に、民法上又は刑法上の責任を負う。なお、名誉とは、人の社会的評価を指す。

●刑事的責任

刑法第 230 条は、「公然と事実を適示し、人の名誉を毀損した者は、その事実の有無にかかわらず、3 年以下の懲役若しくは禁錮又は 50 万円以下の罰金に処する。」と規定する。

この場合、不特定多数又は多数の者が知ることが出来る状態で「公然」と事実を示し、またその事実が「客観的に存在する社会的評価を害するおそれのある事実であることを必要とする」[2]。ただし、現実に被害者の社会的評価が下落することを要しない。

ホームページ上やメーリングリストなど、不特定多数が見ている場で公然と事実を適示した場合は、事実の有無に関わらず、刑法第 230 条の名誉毀損罪は成立する。（事実を適示しなくても、公然と人を侮辱した場合は、侮辱罪（刑法第 231 条）が成立し、拘留又は科料に処せられる。）したがって、プライバシーに関する事実は、たとえ真実であっても、名誉毀損罪が成立し得る。

ただし、①公共の利害に関する事実に係り、②その目的が専ら公益を図ることにあったと認められ、③事実の真否を判断し、真実であることの証明があったときは、名誉毀損にはならず、罰せられない（刑法第 230 条の 2）。この場合の立証責任は、当該表現の発言者側にある。

なお、真実であることの証明には、「相当の理由」基準が採用されている。「相当の理由」とは、「表現時点において、当該事実が真実であると信じたことに相当の理由があったことを表現者が立証すれば、名誉毀損は成立しない」という基準（最高裁大法廷昭和 44 年 6 月 25 日判決「夕刊和歌山時事事件」）である。

サイバー空間の場合、リアル空間と比べて表現者が立証すべき「相当の理由」は少ないとされる。この理由は、名誉を毀損されたと主張する者がサイバー空間又は他の手段で反論し、名誉の回復を図ればよいと考えられるためである（これは「対抗言論」の理論、ないし「モア・スピーチ(more speech)の理論」と呼ばれる）。東京地裁は、平成 20 年 2 月 29 日、「真実でないと知りながら発信した場合か、インターネット個人利用者に要求される水準の事実確認を行わずに発信した場合に、名誉毀損罪が成立する」と、名誉毀損の成立要件である「真実性」の要件を従来よりも引き下げ、サイバー空間上では「相当の理由」が少ないとする方向を明示した。

[2] 『法律学小辞典【新版】』有斐閣、1996 年

●民事的責任

民事上は、不法行為（民法第 709 条）が成立し、精神的損害（民法第 710 条）を含む損害賠償（民法第 709 条）のほか、名誉回復のための処分（民法第 723 条）の請求の対象となる。不法行為が成立するかどうかの判断は、上記と同様の基準が採用されている。

また、一定の要件のもとに、加害者は被害者から侵害行為の差し止めを請求され得る。

2）プロバイダ及び電子掲示板管理者の刑事及び民事に係る責任

ニフティサーブ事件（東京地裁判決平成 9 年 5 月 26 日）では、パソコン通信の電子会議室システム・オペレータが他人の名誉を棄損する発言が書き込まれたことを知った場合、被害者の名誉が不当に害されることがないよう必要な措置をとるべき作為義務があるとした。本件においては、システム・オペレータが被害者からの連絡にも係わらず、当該発言の削除等作為義務を怠ったため、作為義務違反についてシステム・オペレータが不法行為責任を負い、またパソコン通信の主催者（ニフティ）が当該システム・オペレータの不法行為につき使用者責任を負うと判断した。

これに対して、控訴審判決は、「標的とされた者が自己を守る有効な救済手段を持たない時や対策が無効な時は、管理者は条理上の削除義務を負う」とした上で、本件については、システム・オペレータ（運営責任者）は「削除義務に違反したとまではいえない」とし、運営会社のニフティについても、使用者責任を否定した[3]（東京高裁平成 13 年 9 月 5 日判決）。

この後もプロバイダの責任をめぐり、様々な判例が出たが、プロバイダは、被害者からは削除要求をされる一方、当該情報を削除すると今度は情報発信者から損害賠償を請求され、法的に不安定な立場に置かれていた。そのため、プロバイダの責任を制限する法律、すなわち「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（以下、プロバイダ責任制限法）が 2001 年 11 月 30 日に公布（翌年 5 月 27 日から施行）され、プロバイダは一定の場合にしか責任を負わないことが明確化された。

プロバイダ責任制限法では、第 3 条第 1 項で、以下の場合以外は、プロバイダは、被害者に対して損害賠償責任を負わない。

・権利を侵害した情報の不特定の者に対する送信を防止する措置を講ずることが技術的に可能な場合であり、

かつ、

---

[3]「ネット上の特許・商標権侵害についての仲介者責任の在り方」
(http://www.meti.go.jp/report/downloadfiles/g10903gj.pdf) p.1「ニフティサーブ事件」より引用。

・当該情報の流通によって他人の権利が侵害されていることを知っていたとき又は、当該情報の流通を知っていた場合であって、当該情報の流通によって他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由がある場合

また、発信者との関係では、第3条第2項で、特定電気役務提供者がとった情報送信を防止する措置が当該情報の不特定の者に対する送信を防止するために必要な限度において行われたものである場合であって、以下の場合には、発信者に対する賠償の責任はない。

・特定電気役務提供者が他人の権利が不当に侵害されていると信じるに足りる相当の理由があった場合、又は

・発信者に照会したにも関わらず、7日を経過しても、発信者から当該送信防止措置を講ずることに同意しない旨の申出がなかったとき

（2）米国

刑法典（criminal code）、民法典（civil code）に名誉毀損に係る規定が存在する。名誉毀損は、文書、図画、映像によるものと口頭によるものに区分される。名誉毀損の立証責任は、名誉を毀損されたと主張する者（原告）が負う。名誉毀損の成立は、表現者が「現実の悪意」(actual malice)を有していた場合に限定される。「現実の悪意」とは、表現内容が真実でないことを知っていた場合、又はわずかの労力による調査を行えば表現内容が真実でないことを把握できたにも係らずそうした調査を怠った場合である。

1）発言者の刑事的及び民事的責任

刑法典、民法典に名誉毀損に係る規定が存在する。「現実の悪意」の存在が名誉毀損の成立基準となる（1964年ニューヨーク・タイムズ社対サリヴァン事件最高裁判決(New York Times Co. v. Sullivan, 376 U.S. 254 (1964))。

2）プロバイダ及び電子掲示板等管理者の刑事及び民事に係る責任

名誉毀損に関して、米国では、伝統的に、情報の仲介者をその責任の度合いに応じて、①発行者（publisher、新聞社等）、②頒布者(distributor、書店・図書館等)、③コモン・キャリア(common carrier、電話会社等)に類型化してきた[4]。すなわち、「発行者」であれば、編集管理権を有するため、発言者・作者と同等の責任が課せられる。「頒布者」であれば、名誉毀損的内容について、知っていたか或いは知るべき理由のある場合にのみ責任を負い、「コモン・キャリア」であれば、責任を負わない。一般に、プロバイダと電子掲示版管理者の責任は同等である。

1995年のストラットンオークモント対プロディジー事件（Stratton Oakmont Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995),）においては、この

[4] コモン・ロー（イギリス法系の法制）の国では同様である。

発行者／頒布者基準（publisher/ distributor test）が適用され、サイト運営者は責任を負うとの判決が下された。しかし、その後、制定された 1996 年通信品位法（Communications Decency Act of 1996; CDA)の第 230 条(c)(1)（47 U.S.C. 230 (c)(1)）では、「双方向のコンピュータ・サービスにおけるプロバイダ又はユーザは、他の情報コンテンツ提供者（第三者）から提供された情報の発行者(publisher)又は発言者(speaker)とは扱われないものとする」と規定され、これにより、プロバイダが全面的に免責されることになった。これ以降のゼラン対 AOL 事件後は、プロバイダが免責される旨の判決が下された。

＜判例＞

●1997 年ゼラン対 AOL 事件（Zeran v. America Online, Inc., 129 F.3d 327, 4th Cir. 1997）

1995 年 4 月、ゼランは、ある者により、自分の名前と電話番号とともに、ビル爆破事件を称賛する標語入りの T シャツ等を宣伝する内容の掲示を数回に渡り AOL の電子掲示板に書き込まれたことに対し、プロバイダの AOL に対して削除要求を行ったが、削除要求に対する適切な対応を怠ったことに過失があったとして、プロバイダ（被告）に対して訴訟を提起した。

原告ゼランは、通信品位法第 230 条では、「発行者」と規定されているため、「頒布者」は同条で保護されないと主張した上で、原告からの通知を受けて問題の投稿について知った後も AOL が速やかに当該投稿を削除しなかったことについて、AOL の「頒布者」としての責任（情報の内容を知っている場合の責任）を主張したが、判決は、通信品位法第 230 条の免責は、発行者か頒布者かの区分は関係なく、頒布者は発行者の一類型として考えられるとし、プロバイダの AOL は免責されるとした。

●2006 年バレット対ローゼンタール事件（Barrett v. Rosenthal, 40 Cal.4th 33, 146 P.3d 510, 51 Cal. Rptr.3d 55 (Cal. Sup. Ct., Nov. 20, 2006).）[5]

電子メールで受け取った文書をインターネット上の会議室に投稿したローゼンタール（被告）に対して、当該文書が名誉を毀損するものだとして、バレットら原告が訴えた事案で、控訴審（Court of Appeal）では、通信品位法第 230 条の下でも、名誉毀損的な内容だと知って当該情報を再発行した場合は、「頒布者」の責任があるとして、伝統的な論理構成を用い、ローゼンタールに「頒布者」としての責任を認めた。

しかし、カリフォルニア最高裁判所(Supreme Court of California)は、2006 年 11 月に、控訴審判決を覆し、通信品位法第 230 条は、インターネット上の出版物

[5] http://www.eff.org/files/filenode/Barrett_v_Rosenthal/ruling.pdf

について「頒布者」の責任を禁止し、同条(c)(1)は双方向のコンピュータ・サービスの個々の「ユーザ」を免責すること及び、当該ユーザの利用が能動的か受動的かで区別されないとした上で、ローゼンタールは、「双方向のコンピュータ・サービスにおけるユーザ」であり、通信品位法第 230 条により免責されると判示した。これは、通信品位法第 230 条のプロバイダではない個々の「ユーザ」に対する免責について言及した初めての判決である。さらに、判決は、インターネット上の名誉毀損的な文書の再発行（再配信）に対して広範な免責を与えることは、多少の混乱を生じさせると認識した上で、議会が法的解決をするまでは、インターネット上の掲示で名誉が毀損されたと主張する者は、当該コンテンツの源泉元である原作者（original source）からのみ損害賠償を請求できるとした。もっとも、補足意見では、通信品位法第 230 条の免責は、オリジナルのコンテンツ提供者と名誉毀損を共謀したオンラインの発行者又は頒布者にまで拡大されないとしている。

（3）英国

英国においては、名誉毀損法（Defamation Act 1996）に名誉毀損に関する規定が存在する。米国と同様に、名誉毀損は、文書、図画、映像によるものと口頭によるものに区分される。名誉毀損の立証責任は、名誉を毀損されたと主張する者（原告）が負う。

1）表現者の刑事及び民事に係る責任

名誉毀損法に規定が存在する。既存の名誉毀損法がインターネット上においても適用されることが明らかにされた事案として、2006 年のマイケル・キース＝スミス対トレイシー・ウィリアムズ（Keith- Smith v. Tracey Williams）に係る裁判がある。

＜判例＞

●2006 年マイケル・キース＝スミス対トレイシー・ウィリアムズ事件（Michael Keith- Smith v. Tracey Williams）[6]

トレイシー・ウィリアムズ（女性）が英国独立党員のマイケル・キース＝スミス氏に対して、名誉毀損的発言をインターネット上の電子掲示板において行ったことについて、名誉毀損が認められ、損害賠償と差止めが認容された。

2）プロバイダ及び電子掲示板等管理者の刑事及び民事に係る責任

名誉毀損法では、第 1 条(3)項に、以下の規定が存在する。

いかなる者も以下の場合に、文書（statement）の作者（author）、editor（編

[6] http://www.mondaq.com/article.asp?articleid=47036&searchresults=1

集者）又は発行者（publisher）としてみなされない。

(a)～(d)略

(e)コントロールの及ばない者によって当該文書が送信され、又は入手できるようになった通信システムへのアクセスを提供するオペレータ又はプロバイダ。

プロバイダの責任について言及した初めての判決として、バント対ティリー（Bunt v. Tilly）に係る裁判がある。同判決では、プロバイダは、個人に対してインターネットへのアクセスを提供しただけで、名誉毀損的なコンテンツの発行の原因になった又は貢献した結果になったことについて知らなかった又は知る余地がなかったとしている。

●2006 年バント対ティリー事件（Bunt v Tilly & Ors [2006] EWHC 407）[7]

バント氏（原告）は、当初、名誉を毀損されたとして 3 人の個人を訴えていたが、その後、名誉毀損的な投稿を容易にさせたとして、それぞれのプロバイダである、American on Line(AOL)、British Telecom(BT)、Tiscali に対して訴えを提起した。プロバイダ側は、名誉毀損法(1996)で定義されている「無知の配布」(innocent dissemination)を主張し、高等裁判所(High Court)は原告の名誉毀損の訴えを棄却した。

（4）ドイツ

ネット上の名誉毀損は、ドイツでは不法行為法と刑法の対象となり得る。

1）発言者の刑事的及び民事的責任

情報発信者本人は、特別な免責を受けずに、不法行為法（Recht der unerlaubten Handlungen）[8]及び刑法（Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S.3322), zuletzt geändert durch Artikel 3 des Gesetzes vom 11. März 2008 (BGBl. I S.306)）の規定による責任を負う。

2）プロバイダ及び電子掲示板等管理者の刑事及び民事に係る責任

プロバイダに関しては、上記の規定による責任は一定の範囲において制限される。プロバイダの責任制限は以前、テレサービス法（Gesetz über die Nutzung von Telediensten[9]）に定められていたが（テレサービス法第 5 条では、プロバイダの責任について規定されており、第三者のコンテンツについて、当該コンテンツを知っていたか、当該コンテンツを技術的にブロックすることが合理的に期待されていな

[7] http://www.mondaq.com/article.asp?articleid=47036&searchresults=1

[8] 「不法行為法」という特定の法律があるわけではなく、主にドイツ民法に定められ、不法行為と関連する全ての規定。

[9] Gesetz über die Nutzung von Telediensten in der Fassung der Bekanntmachung vom 22. Juli 1997 (BGBl. I S.1870), zuletzt geändert durch Art. 12 Abs. 15 G vom 10. November 2006 (BGBl. I S. 2553); Außerkrafttreten am 1. März 2007 durch Art. 5 EIGVG vom 26. Februar 2007 (BGBl. I S. 179)」

い限り、責任を負わないと規定されていた[10]、テレサービス法はテレメディア法（Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179)）の施行（2007 年 3 月 1 日）とともに廃止された。よって、プロバイダに関する責任制限は現在、テレメディア法第 7 条～第 10 条に規定されている。

なお、テレサービス法のプロバイダ責任に関する規定の多くは、テレメディア法に引き継がれている。

テレメディア法第 7 条第 1 項にて、プロバイダは自己が提供する情報については不法行為法及び刑法により責任があり、第 7 条第 2 項にてこれらの情報は削除請求の対象となることが明示されている。ただし、判例は、不法行為法を適用しながらもプロバイダへの負担を考慮している[11]。

テレメディア法第 8 条によると、アクセスプロバイダ又はネットワーク・プロバイダのように、情報を純粋に伝送することに関しては、プロバイダは一定の要件の下で責任を負わない。テレメディア法第 10 条（テレサービス法第 11 条）では、ホスティングに関する責任の免除が規定され、自らが利用のために保存している他人の情報について、免責のための厳しい要件が規定されている。

システム・オペレータについては、他人の情報を保存している以上、判例はこれをテレメディア法第 10 条のプロバイダと位置付けている場合が多いようだが、これはオペレータの具体的な営業方法にもよると思われる。また前述のとおり、オペレータはテレメディア法第 7 条第 2 項第 2 文により、情報の除去や利用の停止を含む民法上の不作為請求権については免責を受けない。

＜判例＞

●2006 年 6 月 7 日付デュッセルドルフ高等裁判所判決 I-15 U21/06

（OLG Düsseldorf, Urteil vom 7.6.2006 - I-15 U21/06 (LG Düsseldorf)）

※仮処分を対象に争われたもの。

運営者が知らないところで、電子掲示板に違法な発言がなされた場合、運営者が被害者に対し当該発言を削除する責任を負うかが争われた。

事件の概要は、第三者が原告のことを被告の電子掲示板において誹謗中傷し、原告は第三者の個人情報をプロバイダから取得できないため、プロバイダを訴えたものである。デュッセルドルフ地方裁判所は、被告は電子掲示板を監視し、名誉を毀損する内容の発言を知った場合にはそれを直ちに削除する義務があるとした上で、不法行為法による削除請求を認容した。それに対し、その控訴審のデュッセルドルフ高等裁判所は、電子掲示板管理者は一般的には確認義務は負わず、当該発言について知った後に削除すれば足りるものと判断し、削除請求を認めな

[10] http://www.iuscomp.org/gla/statutes/TDG.htm#3

[11] BGH, Urteil vom 27.3.2007 – VI ZR 101/06 (OLG Düsseldorf); OLG Düsseldorf, Urteil vom 7.6.2006 – I-15 U 21/06 (LG Düsseldorf)

かった。

●2006 年 4 月 26 日付デュッセルドルフ高等裁判所判決 I-15 U180/05
（OLG Düsseldorf, Urteil vom 26.4.2006 - I-15 U180/05 (LG Düsseldorf)）
※通常の手続において争われたもの

原告は幼児ポルノ等の防止を目的とする団体、被告は幼児ポルノ等をテーマとする電子掲示板管理者である。本件では、第三者が被告の電子掲示板において、原告の活動を批判し、原告団体に所属する会員を「卑怯」「汚い」「怠け者」とし、それらの会員が「生まれてから公費に負担をかけつつ生活している」等と述べた。これを受けて、原告は名誉が毀損されたと主張し、不法行為法に基づく削除請求を行った。デュッセルドルフ地方裁判所（第一審）は不作為請求を認容した。それに対し、デュッセルドルフ高等裁判所（控訴審）は、掲示板に掲載されたコメントの場合には、メディアにおける放送・掲載と同様に、運営者は免責され情報発信者のみが責任を負うが、運営者が情報を開示しないこと等により情報発信者を特定できない場合には運営者が責任を負うものと判断した。これを踏まえて、控訴審は、特定できない情報発信者によるコメントについては請求を認容し、特定できる情報発信者によるコメントについては請求を認めなかった。

しかし、本件は上告され、連邦通常裁判所（最高裁）は不作為請求を全面的に認容した。その理由としては、裁判所は、運営者が法的にも実際にも介入し得ることをあげ、一般の確認義務がないというものの、法違反について知らされたときには削除義務を負うものと判断した。

●2005 年 5 月 28 日付ケルン高等裁判所判決 15 U 221/01
（OLG Köln, Urteil vom 28.5.2002 - 15 U 221/01 (LG Köln)）
※仮処分を対象に争われたもの

本件では、第三者が、有名人のみだらな行為を装う合成写真を作成し、それらをウェブサイトにおいて公表したため、有名人等の原告は、人格権が侵害されたと主張し、ウェブサイト管理者に対して不法行為法による削除請求を行った。ケルン地方裁判所もケルン高等裁判所も、被告の責任を認め、削除義務を肯定した。

なお、控訴審は、第三者による掲載というものの、被告は第三者による内容と自己の内容を明確に区別していないため、それらの写真を被告による内容と見なし、責任を判断するにあたって厳格な判断基準を用いた。

（5）韓国

韓国では、ネットの誹謗中傷対策で、「制限的インターネット本人確認制度」（通称：インターネット実名制）が 2007 年 7 月 27 日より導入されている。

同制度は、一日の平均アクセス数が 10 万名以上のインターネットポータルサイトと言論社サイト等の電子掲示板に利用者が文章を書き込む場合、サービス事業者に本人確認の手続きを義務化するものである。本人確認手段の導入を怠ったサイト運営企業には、最大で 3,000 万ウォン(約 376 万円)の罰金が科せられる。

インターネット実名制については以前から法制化が図られていたが、2007 年 1、2 月に連続して起きた女性タレントの自殺が彼女らに対するネット上の誹謗中傷と関係があるのではないかと社会問題となり、それが実名制導入の追い風になったと言われている。韓国・情報通信部により国会に提出され、2006 年 12 月に可決された「情報通信網利用促進及び情報保護等に関する法律」の改正案の一部として実現された。

本人と確認されれば、ペンネームや ID を使用することができる。本人確認の具体的方法までは明示されていないが、韓国で早期より導入されている 13 桁の住民登録番号を使う方法が最も現実的だと考えられている[12]。

（6）EU

EU では、2000 年 6 月に成立した「電子商取引の法的側面に関する EU 指令」（Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (“Directive on electronic commerce”)）において、一般法的な視点から仲介者の法的責任について規定している。

基本的な考え方は、以下のとおりである。

- 仲介者が第三者からの情報の単なる転送者としての受動的役割しか担っていない場合には、原則として、送信された情報に関して差止め以外の責任を負わない。
- 情報の自動的、中間的かつ一時的な蓄積が行われている場合でも、仲介者はその情報を改変していないなどの一定条件を満たしたときは、差止め以外の責任を負わない。

（http://www.meti.go.jp/report/downloadfiles/g10903gj.pdf より引用）

[12] http://itpro.nikkeibp.co.jp/article/COLUMN/20070328/266631/?ST=ep_webpluse

2.2. プロバイダ等に対する発信者情報開示に係る措置はなされているか

国内外におけるプロバイダ等における発信者情報開示に係る措置に関して述べる。

表 2.2-1 発信者情報開示に係る国内外の動向

	日本	米国	英国	ドイツ	韓国	EU
関連する法律	プロバイダ責任制限法 第 4 条において発信者情報開示請求権が規定されている。開示請求者の権利が侵害されたことが明らかであって、発信者情報の開示を受けるべき正当な理由がある場合には、電子掲示板の管理者等は任意で発信者情報の開示を行うことができる。 さらに、開示請求に電子掲示板の管理者等が応じない場合、開示請求者は裁判所に対して、電子掲示板の管理者等を被告として発信者情報開示請求訴訟を提起できる。	・通信品位法 他人の権利を侵害する情報については、身元不詳の発信者を相手方とする仮名訴訟を提起した上で、審理の前に行われる証拠開示の手続において、裁判所から文書提出命令を取得することで、訴訟外の第三者である電子掲示板の管理者等に対して発信者情報の開示を請求することができる。 ・デジタルミレニアム著作権法第 512 条 この規定に基づき、権利保有者は電子掲示板の管理者等に対して権利侵害情報の発信者情報の開示を請求するための命令を裁判所から取得できる。	Norwich Pharmacal Order 情報の流通により権利を侵害された者は、Norwich Pharmacal Order と呼ばれる第三者情報開示命令を裁判所から取得することで、審理前の段階でプロバイダに対して発信者情報の開示を請求することができる。	・刑事訴訟法第 100 条 g ・通信法第 113 条 ・差止訴訟法「発信者情報請求権」（差止訴訟法 13 条、13a 条） 2002 年から施行開始。電子メールによる広告の受信者が送信者の情報開示の請求をより実行的に行うための制度。 ・民法上の情報開示請求権も一般に認められているが、テレメディア法及び通信法が個人情報保護規定を設けているため、発信者情報の開示は特別な法的根拠がない限り許されない。	情報通信網利用促進及び情報保護等に関する法律 第 21 条 通信事業者は、通信設備によって処理される電子文書又は関連記録を、合法的手順に従わずに、又は発信者及び受信者の同意なしに公開してはならない。	電気通信分野における個人データ処理及びプライバシー保護に関する欧州議会及び欧州理事会指令 (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications))9 条 (a) 悪意、あるいは迷惑な通信があった際に、その逆探知を加入者が要請するのに応えるためには、発信者 ID の非通知を覆すことを可能とする方法に関して、透明な手続きが存在するよう確保しなければならない。
開示請求の強制力	プロバイダ制限責任法第 4 条に則った開示請求には強制力はない。裁判所から開示請求命令には強制力がある。	裁判所の開示請求命令には強制力がある。	裁判所の開示請求命令には強制力がある。	裁判所の開示請求命令には強制力がある。	裁判所の開示請求命令には強制力がある。	刑事手続の場合とは別に民事手続における開示請求については各国法に委ねられている。

（参考文献）

(1) 「情報通信の不適正利用と苦情対応の在り方に関する研究会報告書」

http://www.soumu.go.jp/joho_tsusin/pressrelease/japanese/tsusin/990201j501.html,

http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h11/press/japanese/tsusin/0201j103.htm#0205

(2) プロバイダ責任制限法発信者情報開示関係ガイドライン（2007）

http://www.telesa.or.jp/consortium/provider/pdf/provider_070226_guideline.pdf

(3) 総務省インターネット上の違法・有害情報への対応に関する研究会最終報告書

http://www.soumu.go.jp/s-news/2006/pdf/060630_11_1.pdf

(4) 通信・放送の総合的な法体系に関する研究会　第 17 回資料

http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/tsushin_houseikikaku/pdf/071019_1_si3.pdf

（1）日本

日本においては、社団法人電気通信事業者協会、社団法人テレコムサービス協会及び財団法人日本インターネット協会が、プロバイダ責任制限法対応事業者協議会を結成し、プロバイダ責任制限法発信者情報開示関係ガイドラインを策定している。このガイドラインの目的は、被害者、情報発信者、プロバイダ等のそれぞれが置かれた立場等を考慮しつつ、発信者情報開示請求の手続や判断基準等を、可能な範囲で明確化することとしており、具体的には以下の項目について言及している。

・発信者情報開示の請求の手順
・請求を受けたプロバイダの対応
・権利侵害の明白性の判断基準
・開示、不開示の手続きについて

（2）米国

通信品位法を根拠に、他人の権利を侵害する情報については、身元不詳の発信者を相手方とする仮名訴訟を提起した上で、審理の前に行われる証拠開示の手続において、裁判所から文書提出命令を取得することで、訴訟外の第三者である電子掲示板の管理者等に対して発信者情報の開示を請求することができる。

また、デジタルミレニアム著作権法（The Digital Millenium Copyright Act of 1998）第512条の規定に基づき、権利保有者は電子掲示板の管理者等に対して権利侵害情報の発信者情報の開示を請求するための命令を裁判所から取得できる。裁判所の開示請求命令には強制力がある。

（3）英国

情報の流通により権利を侵害された者は、Norwich Pharmacal Order と呼ばれる第三者情報開示命令を裁判所から取得することで、審理前の段階でプロバイダに対して発信者情報の開示を請求することができる[13]。裁判所の開示請求命令には強制力がある。

（4）ドイツ

検察は、IP アドレスを手掛かりに利用者を特定するため、刑事訴訟法（Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 2 des Gesetzes vom 11. März 2008 (BGBl. I S. 306)）第100条g、又は、通信法（Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198)；略称 Telekommunikationsgesetz 又は TKG）第113条を根拠として、プロバ

[13]インターネット上の違法・有害情報への対応に関する研究会「インターネット上の違法・有害情報への対応に関する研究会最終報告書」平成18年8月、総務省

イダに対して情報開示を請求することができる。

○法的効果について

通信法第 113 条は、いわゆる保有データを請求する場合の根拠となる。通信法第 3 条第 3 号によると、保有データとは、電気通信サービスに関する契約を締結、変更、又は終了するために収集する利用者データのこと、すなわち、名前、住所、電話番号、銀行口座、固定的な IP アドレス等を意味する。

他方、刑事訴訟法第 100 条 g を根拠とした場合には、検察はいわゆる接続データの開示も請求することができる。通信法第 3 条第 30 号によると、接続データとは、電気通信サービスの提供にあたって収集、編集又は利用したデータのことを意味し、とりわけ、接続の開始時間、終了時間、端末に関する情報を指す。

なお、インターネットにおいては、IP アドレスは固定的でなく、接続ごとに割り当てられる動的な IP アドレスによる利用もなされる。動的な IP アドレスに関する情報の開示をプロバイダに求めた場合、請求の対象は保有データとして位置づけられるのか、それとも接続データとされるのか、という点については争いがある[14]。

前述の位置付けは、手続を決めるにあたり重要である。動的アドレスを利用した者に関する情報を、保有データとし、通信法第 113 条を適用した場合には、特別な手続は不要である。

それに対し、これを接続データとして位置付けた場合には、情報開示請求を行う前に、原則として刑事訴訟法第 100 条 g 第 2 項第 1 文及び第 100 条 b 第 1 項に基づき、裁判所による事前許可を得る必要がある。

ちなみに、最近の判例で、このような裁判手続において、アップロードが 2、3 回行われたことを理由に開始された、著作権法違反に関する捜査手続に関して、検察によるプロバイダに対する情報開示請求を、相当性に欠けるとして認めなかった判例がある[15]。

○法的要件について

旧刑事訴訟法第 100 条 g 第 1 項では、法執行機関が電気通信の通信傍受を行う際の以下の要件を掲げている。

- 重大な犯罪行為の疑いがある場合(刑事訴訟法旧法第 100 条 a 第 1 文によると、殺人罪、強盗罪、恐喝罪、武器法違反罪、滞在法違反等)
- 旧通信法第 3 条第 3 号による端末による、とりわけインターネットを利用した犯罪の疑いがある場合（著作権法違反は含まれる可能性はある）
- 未遂が可罰的な犯罪の実行に着手した疑いがある場合

[14] Kitz, GRUR 2003, 1014
Forschungsstelle Recht, A. Rülke, Auskünfte an Sicherheitsbehörden, www.dfn.de
[15] AG Offenburg, Beschluss vom 20.7.2007, 4 Gs 442/07

・　予備行為が可罰的な犯罪の予備を行った疑いがある場合

上記に該当する場合、法執行機関は裁判所に通信事業者に接続データの開示命令を要求できるものとしていた。

改正後の刑事訴訟法は、この関連での適用範囲を拡張している。旧法で列挙されていた重大な犯罪行為以外にも、1）個別の場合において重大と見ることができる犯罪の場合、又は、2）電気通信を利用した犯罪の場合には、接続データの開示を命じることができるものとした。

旧法との違いは、将来的に入手する情報についても開示請求可能であること、通信事業者だけでなくドイツ国内の電気通信を行う者全てに対して適用されうることから、連邦憲法裁判所の 2008 年 3 月 11 日決定により問題視された。したがって、現在は、刑事訴訟法第 100 条 a にて列挙されている重大犯罪に関する情報開示のみが運用されている。

なお、裁判所は法執行機関から情報開示請求がなされた場合、却下することも多い。

一方、通信法第 113 条第 1 項は、通信事業者は、犯罪行為の訴追等のために、保有データを開示する義務を必要な範囲において負うものとしている。

○過去の例

コンピュータゲーム「Earth 2160」を作ったドイツのソフトウエアメーカは、2005 年の秋に違法ファイルを検索する IT 企業 Logiste 社の協力により、当該ゲームの違法な交換の利用者を著作権法違反により検察に告訴した。検察は、2 万件について捜査手続を開始したが、責任の程度が低いことから、ほとんどの案件を刑事訴訟法第 153 条により不起訴とした。

○民事手続における情報開示請求

ドイツ連邦政府は、知的財産権の施行に関する EU 指令 2004/48/EC (Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights)を国内法化すべく、著作権法に関する改正案（Gesetzentwurf der Bundesregierung - BT-Drucksache 16/5048 - Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums）を 2007 年 4 月に連邦議会に提出した。この改正法案は、プロバイダ等の保持する第三者の個人情報の情報開示請求権を含むため、個人情報保護法との関係で問題視されている。

○差止訴訟法

差止訴訟法（Unterlassungsklagengesetz in der Fassung der Bekanntmachung vom 27. August 2002 (BGBl. I S. 3422, 4346), zuletzt geändert durch Artikel 19 Abs. 5 des Gesetzes vom 12. Dezember 2007 (BGBl. I S. 2840)）第 13 条 a は、①注文していない製品が配達された場合、②注文していないサービスが提供された場合、又は、③注文してい

ない広告が送付された場合の差止について、情報開示請求を定め、適用範囲は限定的である。

また、第 13 条第 2 項は、保有データのみを開示の対象としている。

2.3. 利用者が不適切なパケットの送信停止及びネット上の掲載情報の削除を要求する枠組みはあるか

迷惑メールと違法有害情報について述べる。

2.3.1. 迷惑メール対策

表 2.3.1-1 迷惑メール対策に係る国内外の動向

	日本	米国	英国	ドイツ	韓国	EU
オプトイン又はオプトアウト	オプトアウト	商業用電子メールはオプトアウト、携帯メールはオプトイン	オプトイン（ソフト・オプトイン）	オプトイン	通常の電子メールはオプトアウト、携帯メールはオプトイン	オプトイン
法的枠組み	・特定電子メールの送信の適正化等に関する法律（メール適正化法）及び特定商取引に関する法律（特定商取引法）による。 ・特定電子メール法にて、広告又は宣伝の手段としての電子メールの受信拒否の通知をした者に対する再送信が禁止されている。	・商業用電子メールは迷惑対策法（CAN-SPAM 法）による。 ・携帯メールについては FCC 規制（連邦通信委員会）による。	プライバシー及び電気通信規則（2003）（The Privacy and Electronic Communications (EC Directive) Regulations 2003）（右記の 2002 年 EU 指令 2002/58/EC を国内法化したもの）。	・不正競争防止法（2004 年 7 月 3 日に成立、同年 7 月 8 日に施行）「受忍しえない迷惑行為の規定」（7 条） ・テレメディア法	・情報通信網利用促進及び情報保護等に関する法律（電子通信網法） ・電子商取引等における消費者保護に関する法律 ・訪問販売法	電気通信分野における個人データの処理及びプライバシーの保護についての 2002 年 EU 指令（2002/58/EC）13 条 1 項による。
罰則	50 万円以下の罰	最高で 5 年間の懲役又は罰金（損害賠償額の上限は 600 万ドル）	法律には罰金額は明記されていないが、情報コミッショナー (information Commissioner)の執行通知（enforcement order）に違反すると治安判事裁判所 (magistrate‘s court) では最大 5,000 ポンド、陪審員のいる裁判所の	5,000 ユーロの罰金	1 年以下の懲役又は 1 千万ウォン(約 130 万円)以下の罰金	各国法による。

			場合、上限なしの罰金。			
民事的救済の枠組み	・プロバイダは迷惑メールの送信者に関する発信者情報の開示に応じることはできない。		明示はされていない。	あり（受け手に同意のない電話広告・ファックス広告及び電子メール広告は民法上の不法行為、受け手に損害賠償及び差止請求権がある）。		あり。

（参考文献）

(1) 「諸外国の迷惑メールに対する規制について」（総務省、平成 19 年 9 月 27 日）

http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/mail_ken/pdf/070927_2_sa1.pdf

(2) 英国 “REGULATORY IMPACT ASSESSMENT　PRIVACY AND ELECTRONIC COMMUNICATIONS (EC DIRECTIVE) REGULATIONS 2003”

http://www.berr.gov.uk/files/file23050.pdf

（1）日本

日本における主な判例を挙げる。

1）ニフティ・スパムメール送信差し止め仮処分事件

浦和地裁は、1999 年 3 月 9 日に、ニフティサーブの会員に対してわいせつビデオ販売を内容とする電子メールによるダイレクトメールを送信した被申立人に対して送信差し止めの仮処分を認める決定をした（判タ 1023 号 272 頁）。

2）NTT ドコモメール送信差し止め仮処分事件

横浜地裁は、2001 年 10 月 29 日に、NTT ドコモの携帯電話にインターネットを通じて大量の迷惑メールが送られてくる問題で、同社が横浜市内の業者に送信をやめるように求めていた仮処分申請を認める決定をした（判時 1765 号 18 頁）。

3）NTT ドコモ対有限会社スクープ事件（事件番号 平成 14(ワ)12815）

2003 年 3 月 25 日に、ｉモード利用者に大量の「迷惑メール」を送信する不法行為によって本来必要のないメール処理業務が発生したとして、NTT ドコモが、東京都内のインターネットサービス会社に損害賠償を求めた訴訟。東京地裁は、迷惑メールの損害額について「大量のあて先不明メールが送信された場合には、正常なメールがあった場合と同じ課金をし得る」と初めての判断を示し、業者側に請求どおり 656 万円の支払いを命じた。

（2）米国

米国における主な判例を挙げる。

1）コンピュサーブ社対サイバープロモーションズ社事件（CompuServe Inc. v. Cyber Promotions Inc.(No. C2-96-1070 (S. D. Oh. 1997)）)

迷惑メール送信行為が電子メール送信サービスを提供する原告の財産権の侵害行為に相当し、迷惑メールの差止めが容認された。

2）ホットスポットを用いたスパムメール送信事件

南カリフォルニア在住の男が、無防備な無線 LAN のアクセスポイント（ホットスポット）を利用してスパムメールを送信した罪を認めた。この事件は米国の迷惑メール対策法（CAN-SPAM 法(Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003)）に基づいて有罪判決が下された。量刑は 3 年間の保護観察と、半年間の勾留の範囲の刑及び 10,000 ドルの罰金となった。[16]

（3）英国

英国におけるソフト・オプトインとは、以下の 3 つの基準すべてを満たせば、個

16 http://losangeles.fbi.gov/pressrel/2004/websnare082604.htm

人の消費者に送付してよいという制度である。

a) セールス又は交渉でメールアドレスを収集した場合

b) 類似の商品サービスに関連した広告メッセージを送る場合

c) メールアドレスが収集されたときに、オプトアウトする権利を与えていたにも係わらず、当該個人がオプトアウトしなかった場合

2.3.2. 違法・有害情報対策

違法・有害情報対策に関しては、違法情報の定義、有害情報の定義、発信者の刑事的責任、プロバイダ等の刑事的及び民事的責任、法律以外の取り組みの視点で述べる。

表 2.3.2-1　違法有害情報対策に係る国内外の動向

	日本	米国	英国	ドイツ	韓国	EU
違法情報の定義 （注：主に、表下記載の参考文献(3)を参考）	わいせつ情報、薬物関連情報、振り込め詐欺等関連情報、他人の権利を侵害する情報など。	他人を不快にする等の目的で、わいせつな、淫らな、好色な、卑猥な通信、他人の権利を侵害する情報など。	わいせつ情報、児童ポルノ情報、他人の権利を侵害する情報など。	・自由民主主義的な基本法あるいは国際理解の思想に反する宣伝媒体を表すもの ・一部の民族性によって特定される集団に対する嫌悪の感情を刺激したり、暴力的な処置を誘発したりするもの ・戦争や暴力を賛美するもの ・児童ポルノグラフィティ等	・淫らな文言・音響・画像又は映像 ・恐怖心又は不安感を誘発する文言・音響・画像又は映像 ・青少年保護法による青少年有害媒体物を、相手の年齢確認、表示義務等法令による義務を履行せずに営利を目的として提供する内容の情報 ・法令により禁止される射幸行為にあたる内容の情報　等	各国法による。
有害情報の定義	青少年の健全な育成に有害である又は公序良俗に反すると考えられる情報など。		子どもの健全な育成に有害である又は人種差別を助長すると考えられる情報など。		違法情報と同様と考えられる。	各国法による。
発信者の刑事的責任	刑法 175 条 児童買春児童ポルノ禁止法　第 7 条	通信品位法 223 条(a)	わいせつ出版法 名誉毀損法 児童ポルノ法	州際協定において、不適切なコンテンツが示されている。	情報通信網利用促進及び情報保護等に関する法律	各加盟国の刑事法による。

プロバイダ等の刑事的及び民事的責任	プロバイダ制限責任法においては、以下が規定されている。 ・情報の流通を放置した場合、権利侵害情報であることについて善意、無過失であれば、責任が免除される。 ・情報を削除した場合、権利侵害情報であることについて善意、無過失又は発信者に対する照会への回答なし。	・通信品位法 230 条（c）において、情報の媒介者に過ぎないプロバイダはパブリッシャ（発行者）としての厳格な責任を負わない。 ・デジタルミレニアム著作権法において、著作権者から申立を受けた際に、あらかじめ準備されたガイドラインに基づき迅速に削除等の措置を取るならば、著作権侵害に対する責任が免除される。	違法コンテンツに関しては、わいせつ出版法、名誉毀損法、児童ポルノ法により、該当するコンテンツをシステム上で視聴可能な状態に置くことが違法とされている。 ただし、EU の電子商取引に関する法的側面指令（2000)に基づく規定が存在する。	違法コンテンツに関しては、EU の電子商取引に関する法的側面指令(2000)に基づく規定が存在する。 有害コンテンツに関しては、プロバイダに対し、児童及び青少年の人格の発育を妨げると見なされるコンテンツを頒布・公開する限り、児童又は青少年の年齢に応じて一定のアクセス禁止又は制限措置（技術的制限や時間帯制限）をとることを義務付けている。	情報通信網利用促進及び情報保護等に関する法律において、情報通信サービス提供者は、権利が侵害された個人から当該情報の削除又は反論内容の掲載の要請を受けた場合には遅滞なく必要な措置を取らなければならないとされている。また、情報通信部長官は、不法情報について、情報通信倫理委員会の審議を経て、情報通信サービス提供者に対して、その取扱いを拒否・停止・制限するように命令できる。	「電子商取引に関する法的側面指令（2000）」に以下が規定されている。 ・プロバイダは、違法なコンテンツがあることを知らない場合、又は、コンテンツの違法性を認識して速やかに削除又はアクセス不可能とした場合には、責任を負わないことを確保する ・プロバイダに対し、コンテンツを監視する一般的な義務を課さず、違法な活動を積極的に追求する一般的な義務を課さない。
法律以外の取組み	・インターネット・ホットラインセンターが利用者から情報提供を受け付け、情報を選別した上で、警察への情報提供、電子掲示板の管理者等への送信防止措置依頼を行う。	・NCMEC（National Center for Missing and Exploited Children）は、行方不明の児童及び性的搾取された児童に関する情報のクリアリングハウスである、Cybertipline を運営する。通報は、次のように処理。 ・ 国内から発信された違法情報は、管轄の州警察・地方警察に連絡。 ・ 国外から発信された違法情報は、当該国の法執行機関に情報提供。	違法コンテンツであるかどうかの判断のため、コンテンツに関する苦情はサービスプロバイダからインターネットウォッチ財団（ＩＷＦ）に転送され、ＩＷＦの違法性の判断（わいせつ、名誉毀損、児童ポルノ等）に基づき、サービスプロバイダは削除等の対応を行う。	Jugendschutz.net は、州政府が共同で設立した公共機関。ホットラインを運営しており、違法・有害コンテンツに関する通報を受け付け、次のように処理する。 ・ 国内で発信された違法情報は、ドイツ連邦刑事庁（BKA）に通報（その後 ISP にも連絡）。 ・ 国外で発信された違法情報は、INHOPE メンバーに通報（当該国に INHOPE メンバーがある場合）。	社団法人韓国サイバー監視団が、不健全情報被害申告を受け付けている。	EU では、2005 年から「より安全なインターネットプログラム」（Safer Internet programme）を行ってきたが、2008 年 2 月 27 日に、EU 委員会が新しい「より安全なインターネットプログラム」を提唱し、2009-2013 年に予算€55 million で実施することを発表した。この中で、違法・有害情報についても取り組むとしている。

（参考文献）
(1) http://www.internethotline.jp/index.html
(2) http://www.iwf.org.uk/
(3) http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/tsushin_houseikikaku/pdf/071019_1_si3.pdf
(4) http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/tsushin_houseikikaku/pdf/071102_1_si4.pdf
(5) http://www.soumu.go.jp/joho_tsusin/pressrelease/japanese/PDF/denki/001220j60101.pdf
(6) http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/shohi/pdf/060912_2_12-4.pdf

2.3.3. サイバー空間での個人情報漏えいに関する措置がなされているか

サイバー空間における個人情報漏えいに係る措置に関して、個人情報保護のための法令、サイバー空間における個人情報保護のための法令、ID 及びパスワード漏えいのための対策に関して述べる。

表 2.3.3-1 個人情報保護対策の国内外の動向

	日本	米国	英国	ドイツ	韓国	EU
個人情報保護のための法令	・ 個人情報の保護に関する法律 ・行政機関の保有する個人情報の保護に関する法律 ・独立行政法人の保有する個人情報の保護に関する法律	公的部門：プライバシー法 (Privacy Act of 1974) 民間部門：連邦法（産業別のプライバシー保護法、FTC 法第 5 条）、公正信用報告法、個人情報窃盗対策法、グラム･リーチ･ブライリ法、州法	データ保護法 (1998)	連邦情報保護法（国家機関及び民間企業に適用） 各州政府も制定	公的部門：公共機関の個人情報保護に関する法律（1994.10） 民間部門：通信秘密保護法（1993 年）、通信ビジネス法（1991 年）、医療サービス法（1973 年）、実名金融取引及び秘密法、クレジット情報の使用及び保護法（1995 年）、電子商取引に関する枠組みに関する法律（1999 年）、デジタル署名法（1999 年）、情報通信網利用促進及び情報保護等に関する法律	個人情報保護指令（指令 95/46/EC）

サイバー空間における個人情報保護のための措置	上記と同じ。	上記と同じ。	上記と同じ。	上記と同じ。	情報通信網利用促進及び情報保護等に関する法律（2001.1、2002.12 改正）において、情報通信網を利用する民間企業の個人情報保護義務が規定されている。	上記と同じ。
ID・パスワードの不正取得に対する法令（規定）	・不正アクセス禁止法	個人情報窃盗対策(1998)	データ保護法(1998) ID カード法(2006) 詐欺法(2006)	刑法第 202 条 a 第 1 項、第 202 条 b 第 1 項、第 202 条 c 第 1 項第 1 号		通知{SEC(2004) 1264}（「新 EU アクションプラン 2004-2007」）

（参考文献）

(1) http://www.ftc.gov/os/statutes/itada/itadact.htm

(2) http://www.ftc.gov/os/2000/09/idthefttest.htm

(3) http://www.ndl.go.jp/jp/data/publication/legis/231/023107.pdf

（1）米国

米国では、過去 7 年間に FTC（Federal Trade Commission：連邦取引委員会）が受理した消費者からの苦情情報のトップは ID 窃盗に関するものであり、2006 年 1 月～12 月、FTC には 670,000 件の ID 窃盗苦情が寄せられた。

米国における個人情報保護対策は、近年、個人情報窃盗対策を中心になされている。以下に、個人情報窃盗対策に関連の深い法律を挙げる。

1）公正信用報告法（Fair Credit Reporting Act；略称 FCRA）

公正信用報告法は、保険会社や雇用主に対する個人の消費者信用報告の販売を行っている機関を規制するための法律である。

公正信用報告法は、民間部門による個人情報の利用及び提供を規制する最初の連邦法である。同法は、消費者信用報告の収集、維持及び提供を規制する。消費者信用報告は、信用供与の適格性を判定するときや被用者の経歴調査を行うとき等、同法に列挙された目的のためのみに用いることができると規定されている。

個人情報保護の観点で、重要な事項は以下に示すことができる。

- 被害者が、自らの個人情報についての無権限利用の状況を知りたいと考える場合には、3 つの全米信用情報機関から、年に一度は無料で消費者信用報告を入手できることとなった
- 被害者は一定の要件の下で、自らの消費者信用報告に詐欺警告を付することを認められるようになった

2）個人情報窃盗対策法（Identity Theft and Assumption Deterrence Act of 1998）

個人情報窃盗対策法においては、個人情報窃盗それ自体が犯罪であり、20 年を上限とする拘禁刑を定めている。（連邦量刑委員会が定めた量刑ガイドラインは、被害者が金銭的被害を被っておらず、かつ、窃盗犯が犯歴を有しない場合であっても、10 か月以上 16 か月以下の拘禁刑に処することを可能とした。）

2004 年には、加重個人情報窃盗罪を新設する法改正が行われ、銀行詐欺や電気通信詐欺といった重罪により有罪とされた者が、その重罪に関連して個人情報窃盗を行った場合には、重罪の刑期にさらに 2 年を上限として加算し、また、テロ行為により有罪とされた者が、そのテロ行為に関連して個人情報窃盗を行った場合には、テロ行為による刑期にさらに 5 年を上限として加算することが可能となった。

3）グラム･リーチ･ブライリ法（Gramm-Leach-Bliley Act；GLB Act）

1999 年に制定されたグラム・リーチ・ブライリ法には、銀行、保険会社、信用情報機関等を含む金融機関に対し、系列企業との間で、非公開個人情報の共有を認める記述がある。ただし、金融機関が、系列企業ではない第三者にその情報を提供しようとする場

合には、当該個人に対し、オプトアウトを認めなければならない。

４）連邦取引委員会法（Federal Trade Commission Act；FTC Act）第 5 条

連邦取引委員会法第 5 条は、「取引における又はそれに影響を与える不公正な又は詐欺的な行為又は慣行」を禁止する。同条のもとで、委員会は、取引に参加する多様な企業及び個人による不公正な又は詐欺的な慣行を禁止するための広汎な権限を有する。禁止される慣行には、消費者情報の安全性確保についての約束が含まれる。

（２）英国

現在施行されている個人情報の取扱いに関する法律は、「1998 年データ保護法」（Data Protection Act 1998）である。これは、1995 年の EU の個人情報保護指令（指令 95/46/EC）(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)を国内法化したもので、2000 年 3 月 1 日に施行された。個人情報を保護する独立の公的機関としては、情報コミッショナー（Information Commissioner）が設置されている。

ID 窃盗及び詐欺は、英国でも深刻な問題となっており、2006 年 2 月に、英国内務省(Home Office)より発表された、英国経済に対する ID 詐欺の金額は、年間およそ 10.7 億ポンド（£1.7 billion）に及ぶ[17]。

「2006 年 ID カード法」（The Identity Cards Act 2006）は、偽の ID 文書（他人の真の ID を含む）を保持、管理、使用することを犯罪とし、2006 年 6 月 7 日に施行された。

また、「2006 年詐欺法」（The Fraud Act 2006）は、情報を開示しないことによって偽の代表を装った場合や偽の立場を乱用した場合、また、不正にサービスを得たり、詐欺を行うための道具を保持したり、詐欺で使用されるための品物を作成・提供したりした場合等を新たに詐欺罪の類型とし、2007 年 1 月 15 日に施行された。

2005 年 12 月には、ID に関連する犯罪を起訴するために、イングランド及びウェールズの警察代表、政府機関、諜報機関（intelligence agencies）から成る「Single Points of Contact (SPOC)のネットワーク」が結成された。各 SPOC は、それぞれの組織内で ID 詐欺に対処するための中心的な役割を担い、他の組織とともに、ID に関連する詐欺罪を先取りして告発したり、他の組織と情報交換したりする。

「2006 年警察及び司法の法律」（The Police and Justice Act 2006）では、死者の個人情報を悪用した詐欺を防止するために、総合登録機関（General Register Office）に、警察等に死者の個人情報を提供する権限を付与した。

（参考：Home Office Identity Fraud Steering Committee, ”Identity Theft- Don’t become a victim” (http://www.identity-theft.org.uk/what-is-being-done.html)）

[17] http://www.identity-theft.org.uk/ID%20fraud%20table.pdf

（3）ドイツ

ドイツ刑法第 242 条第 1 項は窃盗罪について有体物を対象としているため、知的財産権、債権や情報のような無体物は窃取の対象とならない。他方、ドイツ刑法第 202 条 a 第 1 項及び第 202 条 c 第 1 項は、一定の条件の下で、データの取得を処罰するものとしている。ただし、前述の規定はあくまでも故意犯を想定しており、過失犯の定めはない。

ドイツ連邦情報保護法（Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S.1970)）[18]もやはり個人情報を保護する。連邦情報保護法の適用範囲は、国家機関だけでなく民間企業にも及び、また、インターネット上の侵害行為も対象としている[19]。連邦情報保護法第 38 条は行政による監督について定め、第 43 条及び第 44 条には、故意又は過失によって個人情報が侵害された場合に関して刑罰及び過料規定が置かれている。

ID やパスワードの不正取得は、その取得行為の具体的な態様にもよるが、基本的には刑法第 202 条 a 第 1 項又は第 202 条 b 第 1 項、ならびに、第 202 条 c 第 1 項第 1 号の規定により処罰することが可能である 。

（4）韓国

韓国においては、1994 年に、公的分野における個人データの自動処理に原則として適用される（手書きの記録には適用されない）、「公共機関の個人情報保護に関する法律」が成立した。この法律は、民間機関においても、同法律のデータ保護原則を尊重するよう推奨する規定があるが、違反に対する行政又は執行的措置を伴わないため、努力義務にとどまる。民間部門における個人情報の収集、利用、開示については、分野毎に以下の法律が存在する。

通信秘密保護法（1993 年）、通信ビジネス法（1991 年）、医療サービス法（1973 年）、実名金融取引及び秘密法、クレジット情報の使用及び保護法（1995 年）、電子商取引に関する枠組みに関する法律（1999 年）、デジタル署名法（1999 年）[20]

1997 年には、民間分野における包括的な個人情報保護法が立法者や学者らによって提案されたが、政府は、より狭い、情報及び電気通信産業のみを対象とした法律「情報通信網

[18] ドイツ語の原文とその英語訳の対照表は、データ保護連邦専門委員のホームページにある：
http://www.bfdi.bund.de/cln_027/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf

[19] Ernst, Das neue Computerstrafrecht, NJW 2007, 2661, 2665 参照

[20] これら法律の名称は、
http://www.privacyinternational.org/survey/phr2003/countries/southkorea.htm に列挙されている英語名称を仮訳したものである。

利用促進及び情報保護等に関する法律」を提案、採択し、2000 年より施行された。
（参考 : http://www.privacyinternational.org/survey/phr2003/countries/southkorea.htm）
民間部門における包括的な個人情報保護法は、2008 年 3 月現在成立していない。

（５）EU

1995 年に個人情報保護指令（指令 95/46/EC）(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)が採択され、加盟国は指令に対応するために国内法を整備した。

ID 窃盗やオンライン詐欺等による支払い詐欺（payment fraud）に関しては、EU においても年間 10 億ユーロを超える損害[21]が生じており、EU 委員会は、クレジットカードや銀行送金等の非現金支払いにおける信頼度向上、国境を越えた購買や電子商取引を活発化させるために、「第 1 次詐欺防止アクションプラン(Fraud Prevention Action Plan; FPAP)」を 2001 年～2003 年に立ち上げ、続いて、非現金手段の支払いにおける詐欺を防止するための EU 委員会の通知{SEC(2004) 1264}、通称「新 EU アクションプラン 2004-2007」（Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol - A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment {SEC(2004) 1264}）に基づいて、「第 2 次 FPAP」を 2004 年～2007 年に実施した[22]。

EU の詐欺防止専門グループ(Fraud Prevention Expert Group (FPEG))は、同アクションプランの下に、非現金支払いにおける詐欺を防止することを目的として、EU 委員会によって設置された。同グループは、国内及び EU の返済機関、銀行、公的機関等の代表、ヨーロッパおよび国際法執行機関（例 : Europol、Interpol）、小売業、消費者団体、ネットワークオペレータ等の専門家から構成される。FPEG は、株主が詐欺防止に関して、効果的に情報交換できる場を提供し、国境を越えた関係者間の連携に協力する。また、EU 委員会にも助言を行っている。原則として、年に 2 度、会合が開催され、EU 委員会が議長となる。現在、FPEG には、７つの作業グループがあり、その中の一つに、「ID 窃盗・詐欺グループ」がある。2007 年 10 月に、同作業グループは、金融分野における ID 窃盗・詐欺に関するレポート[23]を公表し、主な脆弱性とリスク、防止策及び提言を行っている[24]。

---

21 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/04/1291&format=HTML&aged=0&language=EN&guiLanguage=en

22 参考：http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

23 Fraud Prevention Expert Group, “Report on Identity Theft/ Fraud“ http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf

24 参考：http://ec.europa.eu/internal_market/fpeg/about-fpeg_en.htm

2.3.4. サイバー空間上での営業秘密の漏えいに関して措置がなされているか

本節では、営業秘密漏えいに係る法令、営業秘密の定義の観点で述べる。なお、調査対象国においては、サイバー空間上での営業秘密の漏えいに関してリアル空間とは異なる措置をとっていなかった。

表 2.3.4-1 営業秘密の漏えいに係る対策の国内外の動向

	日本	米国	英国	ドイツ	韓国	EU
営業秘密漏えいに係る法令	不正競争防止法	経済スパイ法（1996 年）	秘密法（The Law of Confidentiality）	刑法	不正競争防止法	特になし。
上記法令における営業秘密の定義	秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの。	秘密性を持つ経済的価値のある全ての技術的又は経済的情報であり、かつ秘密性を保持するための合理的措置をとっていること。	秘密でかつ、当該情報を保持する者が企業と秘密契約を締結すること。	不正競争防止法に定義なし。	公然ではなく独立した経済的価値を有するもので、かつ相当の努力により秘密として維持された生産方法・販売方法その他技術上又は経営上の情報。	なし。

（1）米国

米国では、経済スパイ法(Economic Espionage Act）が 1996 年 10 月 11 日に発効している。この法律では、営業秘密を、秘密性を持つ経済的価値のある全ての技術的又は経済的情報と定義しており、さらに以下の条件に合致するものとしている。

・ 所有者がその情報の秘密性を保持するための合理的な措置をとっていること

・ その情報が公衆に一般に知られておらず、また公衆が合理的手段により容易に調べることができないもの （例：ノウハウ、特許取得に向けて開発中のもの、入札における入札予定額）

（2）英国

英国では、営業秘密は、秘密法（The Law of Confidentiality）によって保護されている。営業秘密が保護されるためには、当該情報が秘密(confidential)で、かつ、当該情報を話す者が、秘密契約を署名することが必要である。こうした措置を行った上でもなお、当該情報が署名した者から第三者に話された場合、秘密（信頼性）の違反（breach of confidence）があったとして、法的措置を実行することができる[25]。

25

http://www.ipo.gov.uk/protect/protect-should/protect-should-patent/protect-should-patent-secret.htm

（3）ドイツ

ドイツにおいては、ドイツ不正競争防止法（Gesetz gegen den unlauteren Wettbewerb vom 3. Juli 2004 (BGBl. I S. 1414), zuletzt geändert durch Artikel 5 des Gesetzes vom 21. Dezember 2006 (BGBl. I S. 3367)）第 17 条の刑罰規定は、インターネット上の情報についても営業秘密を保護する[26]。

（4）韓国

韓国では、不正競争防止法第 2 条において、営業秘密を「公然と知られておらず独立した経済的価値を有するものであって、相当な努力により秘密として維持された生産方法・販売方法その他営業活動に有用な技術上又は経営上の情報をいう。」[27]と定義されている。

2.3.5. ネットいじめに関する特別な措置がなされているか

我が国の学校現場においては、ネットいじめは深刻な問題となっている。
日本においては、ネットいじめは、名誉毀損罪の適用による運用がなされている。
各国において、ネットいじめを対象とした法整備を進めている事例は以下のとおりである。

- 米国ミズーリ州のダーデンヌプレーリー市はネットいじめ（Net harassment）を禁じるアメリカで初めての法律を 2007 年 11 月 21 日に制定した
- デラウエア州いじめ防止法には、以下の規定が存在する
  －サイバー空間におけるいじめに関する規定を置くこと
  －学校にいなくても、学校活動中でなくても、学校と密接に関係がある場合の、電子機器等を使ったいじめを処分対象とすること

ネットいじめに関する各国の状況とそれらに対する対策に関しては、参考資料 2 を参照のこと。

2.3.6. オンライン海賊版に関し特別な措置がなされているか

オンライン海賊版に関して、サーバによる配信及びファイル共有等による著作権物の違法な頒布に係る法令及びその他の対策について述べる。

---

[26] Ernst, Das neue Computerstrafrecht, NJW 2007, 2661, 2665; Köhler/Piper, UWG, 3. Aufl. 2002, §17 IV 2.a)。なお、不正競争防止法の和訳は、http://www.jetro.de/j/patent/2004Dec/%83h%83C%83c%95s%90%B3%8B%A3%91%88%96h%8E~%96@%89%FC%90%B3%96@.pdf でダウンロードすることができる。

[27] http://www.geocities.co.jp/WallStreet/9133/

表 2.3.6-1　サーバやファイル共有による頒布に係る法令及び対策の国内外の動向

	日本	米国	英国	ドイツ	韓国	EU
サーバによる著作物の公開に係る法制度	著作権法第 23 条 1 項において、著作権物の送信可能化権が認められている。インターネット上のサーバに、著作物を格納しアクセスに対し送信可能とする場合、著作権者の了解がない場合、送信可能化権の侵害となる。	米国著作権法第 106 条(Copyright Law of the United States of America; 17 USC Title 17) にて、著作権のある著作物をコピー又はレコードに複製することは、著作権者の固有の権利であるとされており、著作権の了解を得ないで公衆送信可能なサーバにコピーすることは違法とされている。	著作権法第 16 条（Copyright, Designs and Patents Act 1988 (c. 48)）第 1 項(b)により、「(b)著作物の複製物を公衆に配布すること」に関して、著作権者に排他的な権利が認められており、特に著作物の複製物の公衆への配布は 18 条で禁止されている。そのため、著作権者の同意なく著作物を公衆送信すること自体は、違法行為とされる。	著作権法第 15 条により、公衆への頒布が規定されるとともに、第 19 条 a により、公衆送信に関する権利が認められている。個人ユーザによる私的複製目的の複製については、ドイツ著作権法第 53 条第 1 項に権利制限規定を置いている。例外規定は、公衆送信が明確に違法な場合において適用されない。	デジタルコンテンツ法にて、複製及び伝送に関して、制作者の権利が認められている（同法第 2 条第 7 号、8 号）。	EU 指令 2001/29/EC (Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society) 第 5 条(2)(b)では、複製権の例外と著作権保護技術との関係について規定しており、著作権保護技術の使用の程度を考慮し、権利者が公正な補償を受けることを条件として複製権の例外を規定できることを認めている。
ファイル共有ソフトによる著作物の公開に係る法制度	ファイル共有ソフトに関しても上記と同様である。	米国著作権法第 106 条で複製権を認めているが、ファイル共有ソフトによる著作物の共有は、フェア・ユースで認められない限り、著作権侵害とされる。これについては、ナップスター訴訟において、利用者間のファイル共有はフェア・ユースにはあたらないとされた。	ファイル共有ソフトに関しても同様である。	現状、ファイル共有ソフトを用いた著作物の共有は、権利侵害とされる。	ファイル共有についても権利侵害であるとされる。	特に規定されていない。
判例等	2004 年 11 月 30 日に東京地裁は、WinMX、Winny など、ファイル共有サービスで、著作者の許諾を得ずに著作物	米国司法省（DOJ）は、2006 年に著作権保護対象作品をオンラインで違法配布している犯罪組織に対する、国際的摘	2006 年 1 月にファイル共有ソフトによる音楽データの共有を行った者に対して、英国レコード産業協会（BPI）への	e-donkey と呼ばれるファイル共有サービスを使ってテレビ番組のファイル共有をしていた者に対して、著作権侵害	ソリバダ事件は、音楽ファイルの共有サービスを行っていたソリバダが刑事訴追される（2001 年 8 月 12 日）	なし。

	をアップロードする行為は、著作権侵害（公衆送信権侵害）であるとの判決を下した。	発を行い、16か国で200余件の捜査令状が執行され、数百台のコンピュータや違法オンライン配信用ハブが押収された。	損害賠償を認める高等裁判所判決が出ている。すなわち、ファイル共有ソフトによるデータ共有を違法として認め、その際に利用者の違法性の認識は著作権侵害の成立に影響を与えないものとした。	を認める決定が出されている。	とともに、韓国音源製作者協会によりレコード複製などの禁止仮処分申立がなされた（2002年7月11日）。その後、ソリバダに対して損害賠償を認める判決が出された後、2006年2月に和解した。	

（参考文献）

(1) http://www.bunka.go.jp/chosakuken/pdf/chitekizaisan_chousakenkyu.pdf

(2) http://www.mext.go.jp/b_menu/shingi/bunka/gijiroku/020/07051108/002.pdf

(3) http://www.bunka.go.jp/chosakuken/singikai/pdf/rokuon_chuukan_1910.pdf

(4) http://www.cric.or.jp/gaikoku/england/england_c2.html#12_18

米国における主な普及啓発活動は以下のとおりである。

・MPAA（Motion Picture Association of America）が、映像に係わる権利擁護を行っている。

・BSA（Business Software Alliance）が、オンライン海賊版法規制を中心とした著作権法の整備を各国政府に対して要請している。

・EIC (Entertainment Industry Coalition for Free Trade)が普及啓発活動を行っている。

（1）日本

日本の著作権には、以下の記述がある。

「（公衆送信権等）

第二十三条　著作者は、その著作物について、公衆送信（自動公衆送信の場合にあっては、送信可能化を含む。）を行う権利を専有する。

2　著作者は、公衆送信されるその著作物を受信装置を用いて公に伝達する権利を専有する。

第七節　権利の行使

（著作物の利用の許諾）

第六十三条　著作権者は、他人に対し、その著作物の利用を許諾することができる。

2　前項の許諾を得た者は、その許諾に係る利用方法及び条件の範囲内において、その許諾に係る著作物を利用することができる。

3　第一項の許諾に係る著作物を利用する権利は、著作権者の承諾を得ない限り、譲渡することができない。」

（2）ドイツ

ドイツでは、個人ユーザによる私的複製目的の複製については、ドイツ著作権法第 53 条第 1 項で権利制限規定を置いている。同規定は、「いかなる媒体であろうと、自然人が個人利用のために行った、作品による個々の複製は、それが直接的にも間接的にも営利目的のためのものでない場合には、複製の際に明白に違法に作成された原本を利用しない限り、認められる」と規定している。

アップロード行為に関しては、個人利用目的は従来から認められておらず、そのため著作権法第条第 1 項の権利制限規定は適用されず、通説は、ファイル共有ソフトによるアップロード行為を常に違法としてきた[28]。

それに対し、ファイル共有ソフトによるダウンロード行為は原則として、個人利用のためになされるため、著作権法第 53 条第 1 項の例外規定により適法とされていた。ただし、ファイル共有ソフトがアップロードもダウンロードも同時に行う場合には、ソフトの位置付けは困難であった[29]。

アップロードに関しては故意がなかったと判断されたり、又は責任の程度が低いから捜査手続が打ち切られたりしているせいか、判例は少なく、有罪判決は一件しか見当たらない。明らかにアップロードが行われた案件について、裁判所は少額の罰金を科した[30]。

---

[28] 参考：NJW-Spezial 2008, 122
Solmecke, Filesharing – Straf- und zivilrechtliche Konsequenzen, MMR 2006, XXIV Dietrich, Rechtliche Bewältigung von netzbasiertem Datenaustausch und Verteidigungsstrategien, NJW 2006, 809, 810

[29]参考：Dietrich, Rechtliche Bewältigung von netzbasiertem Datenaustausch und Verteidigungsstrategien, NJW 2006, 809, 810 Solmecke, Filesharing – Straf- und zivilrechtliche Konsequenzen, MMR 2006, XXIV

[30] 参考：Amtsgericht Cottbus, Urteil vom 25. Mai 2004, 95 Ds 1653 Js 15556/04 (57/04)

なお、2007 年 10 月 31 日の著作権法改正（2008 年 1 月 1 日より施行）により、ファイル共有ソフトが明白に違法に（一般に向けて）アクセス可能とされたものである場合、前記の例外規定は適用されないという規定が著作権法第 53 条第 1 項に追加された。

（今回の改正で下記下線部分が追加された）
【ドイツ著作権法第５３条第１項第１文　個人又はその他自らのための複製】
いかなる媒体であろうと、自然人が個人利用のために行った、作品による個々の複製は、それが直接的にも間接的にも営利目的のためのものでない場合には、複製の際に明白に違法に作成又は一般に向けてアクセス可能とされた原本を利用しない限り、認められる。

これにより、元のファイルが個人利用のために適法にダウンロードされたものであるとしても、とりわけファイル共有ソフトに関しては、当該ファイルが明らかに（権利者による許諾がないまま）違法にアクセス可能になっていると解することができるため、第 53 条第 1 項の例外規定を適用せずにファイル共有ソフトによるダウンロード行為自体を違法とすることができるようになった。なお、立法府は、微罪について例外規定を設けるか否か検討したようだが、結局これを断念している[31]。

ただし、最近の判例では、アップロードが 2、3 回程度行われたことを理由に開始された、著作権侵害罪に関する捜査手続にあたって、検察によるプロバイダに対する情報開示請求を、相当性に欠けるとして認めなかった[32]。

（３）その他の国

- フランス政府が違法な音楽ファイル共有の抑制活動に対する支援を表明し、オンライン海賊版の抑制と合法的に音楽ファイルを提供する Web サイトの開発を促進するアクションプランを示している。
- 現行のフランス著作権法では、著作物の複製については、第 122 条の 5 第 2 号及び第 211 条の 3 第 2 号の範囲でのみ私的複製が認められている。ファイル共有ソフトによるファイル共有については、現状、「私的複製」とする裁判所の決定が出ている。
- イタリア政府は 2003 年 5 月に、違法なファイル共有を有罪とする新しい強力な法律を採用したことで、音楽業界の活動を支援している。
- 中国政府は、「2007 年は、オンラインでの海賊版コンテンツ配信を中国全土で 1,001 件摘発した。うち 832 件では海賊版コンテンツ配信を停止する命令を出し、 339 のサイトを閉鎖した。31 件は司法に委ねた。この摘発総数は 2005 年、2006 年の 2 年間の

[31] 参考：NJW-Spezial 2008, 122
連邦政府案(Gesetzentwurf der Bundesregierung zum Entwurf eines Zweiten Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft)55 頁
[32] AG Offenburg, Beschluss vom 20.7.2007, 4 Gs 442/07

摘発総数の 1.6 倍にあたる。また、あわせて 87 万 750 元（1,300 万円強）、サーバ 123 台、PC123 台を押収した」と発表している。

- 国際レコード産業連盟（IFPI）やビジネスソフトウエアアライアンス（BSA）は、各国において、オンライン海賊版の配布者を提訴している。

2.3.7. Winny 等ファイル共有ソフトウエアの開発者に対して、特別な措置がなされているか

表 2.3.7-1 P2P ソフトウエアの開発者に対する法令の国内外の動向

	日本	米国	英国	ドイツ	韓国	EU
法令	ファイル共有ソフトの開発者に関する規定はない。（著作権法第 119 条及び 123 条に規定されている著作権法違反幇助が適用された例がある。）	デジタルミレニアム著作権法では、著作権保護システムの技術的回避方法を解除することは禁じられている。しかし、ファイル共有ソフトの開発者に対する責任について明文規定は存在しない。	著作権法第 24 条第 1 項により、侵害複製物作成支援の手段を提供した者に対する責任（二次責任）が認められている。	著作権法第 97 条第 1 項で権利侵害者に対する損害賠償請求を請求できる等を規定しているが、この権利侵害者の解釈に侵害行為との相当因果関係を有する範囲で、間接侵害者も含まれるとされる。	ファイル共有ソフトの開発者に関する規定及び判例はない。	「クリエーティブコンテンツオンラインに関する通知」（EU 委員会が 2008 年 1 月 3 日に採択）で、違法なファイル共有に対抗するために、アクセス／サービスプロバイダと権利者と消費者との間で協力の仕組みを開始することが妥当であると規定されている。
判例等	京都地方裁判所　平 16（わ）第 726 号判決文より 「Winny が匿名性に優れたファイル共有ソフトであると認識したことを一つの契機としつつ、公衆送信権侵害の各実行行為に及んだことが認められるのであるから、被告人がそれらのソフトを公開して不特定多数の者が入手できるように提供した行為は、幇助犯を構成すると評価することができる。」	頒布者の責任までは認められたものの、開発者自身の責任までは踏み込んだ判断がなされていない。	ソフトウエアの開発自体がこれにあたるか否かに関する判例は、現時点では存在しない。	見当たらない。	ファイル共有ソフトの開発者に関する規定及び判例はない。	判例は特に見当たらないが、EU でも、違法なファイルのアップロード及びダウンロードは懸念事項となっている。

（1）日本

日本の著作権法には、以下の条文が存在する。

「第百十九条　著作権、出版権又は著作隣接権を侵害した者（第三十条第一項（第百二条第一項において準用する場合を含む。）に定める私的使用の目的をもつて自ら著作物若しくは実演等の複製を行った者、第百十三条第三項の規定により著作権若しくは著作隣接権（同条第四項の規定により著作隣接権とみなされる権利を含む。第百二十条の二第三号において同じ。）を侵害する行為とみなされる行為を行った者、第百十三条第五項の規定により著作権若しくは著作隣接権を侵害する行為とみなされる行為を行った者又は次項第三号若しくは第四号に掲げる者を除く。）は、十年以下の懲役若しくは千万円以下の罰金に処し、又はこれを併科する。

第百二十条の二　次の各号のいずれかに該当する者は、三年以下の懲役若しくは三百万円以下の罰金に処し、又はこれを併科する。

一　技術的保護手段の回避を行うことを専らその機能とする装置（当該装置の部品一式であって容易に組み立てることができるものを含む。）若しくは技術的保護手段の回避を行うことを専らその機能とするプログラムの複製物を公衆に譲渡し、若しくは貸与し、公衆への譲渡若しくは貸与の目的をもつて製造し、輸入し、若しくは所持し、若しくは公衆の使用に供し、又は当該プログラムを公衆送信し、若しくは送信可能化した者

二　業として公衆からの求めに応じて技術的保護手段の回避を行った者

三　営利を目的として、第百十三条第三項の規定により著作者人格権、著作権、実演家人格権又は著作隣接権を侵害する行為とみなされる行為を行った者

四　営利を目的として、第百十三条第五項の規定により著作権又は著作隣接権を侵害する行為とみなされる行為を行った者

（平十一法七七・追加、平十四法七二・三号一部改正、平十六法九二・柱書一部改正四号追加）」

（2）ドイツ

ファイル共有ソフトの開発者は、当該ソフトが違法なものとしてしか利用できない場合、ソフトウエアが違法な目的のためだけに作成されている場合、又はそのような内容でもって宣伝が行われている場合等には、著作権法第 97 条第 1 項により著作権を間接的に侵害したと判断される可能性があるとされている 。

ファイル共有ソフトの開発者に関する判例は見当たらない。

（3）EU

EU においても、違法なファイルのアップロード及びダウンロードは主要な懸念事項になっている[33]。EU 委員会が 2008 年 1 月 3 日に採択した「クリエーティブコンテンツオンラインに関する通知」（Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on creative content online in the Single Market）で、「違法なファイル共有に対抗するために、アクセス／サービスプロバイダと権利者と消費者との間で協力の仕組みを開始することが妥当である」[34]と規定されている。

（4）その他の国

フランスでは、音楽／映画配信会社、インターネット・サービス・プロバイダ及び政府との間で、2007 年 11 月 23 日に、違法にファイル共有を行った者に対して、ウェブへのアクセスを一時中断又は切断する権限を有する新しいインターネット機関を設立することを規定する、「新ネットワークにおける著作物及び文化的プログラムの発展及び保護に関する合意書」（Accord pour le développement et la protection des oeuvres et programmes culturels sur les nouveaux réseaux[35]）を締結した。[36]

[33] http://ec.europa.eu/avpolicy/other_actions/content_online/index_en.htm
[34] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0836:FIN:EN:HTML
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0836:FIN:EN:HTML
[35] http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.htm
[36] http://ec.europa.eu/avpolicy/other_actions/content_online/index_en.htm

2.4. サイバー空間と関係する自由権（身体の自由）を確保するための対策に係る論点（調査の視点）

2.4.1. 通信ログの保存に関する枠組みはあるか

表 2.4.1-1 ログ保存と利用に係る国内外の動向

ログ保存義務、機関、ログの利用	日本	米国	英国	ドイツ	韓国	EU
ログ保存義務に係る法令	電気通信事業法第二十二条に、電気通信事業者に通信量・回線数の記録を義務付けている。	連邦刑事訴訟法 2703 条（U.S.C. TITLE 18. CHAPTER 141）によると、プロバイダは、利用者の氏名、住所、通信記録、期間、サービスの種類、IP アドレス、料金支払方法の保存を義務付けている。[37]	通商産業省(DTI)[38]の規則によると、通信事業者は、トラフィックデータ自体は当該通信終了時に消去し、ログに関しては、課金、顧客からの問い合わせ、不正行為の探知、又は関連する者による電気通信サービスのマーケティングに利用することができる。	通信法第 113 条 a により、電気通信事業者に対してログ保存を義務付ける。	不明	EU 指令 2006/24/EC (2006 年 3 月 15 日、欧州ログ保存指令 2006)
法執行機関のログの利用に関する規定	刑事訴訟法第 197 条には、当局が通信事業者にログに関して問合せができる旨の記述がある。同第 218 条には裁判官の発する令状によりログの差押ができる旨の記述がある。	連邦刑事訴訟法 2703 条によると、当局が捜査の対象とされている犯罪の管轄権を有する裁判所が連邦刑事訴訟規則に定められた手続を利用して発付する令状又は州の同等の令状を取得した場合に、ログを取得できる[39]	（通信法） 裁判所の令状発付を条件として情報を提供する義務が課せられている。 （DTI の規則） DTI のトラフィックデータの扱いについて以下のとおり。 トラフィックデータは、原則として、当該通信の終了	郵政電気通信監督官庁及び安全保障官庁（裁判所・検察庁・警察等）は、電気通信事業者への通知なしに、当該電気通信事業者の有する顧客データを呼び出すことができることとされている。さらに、電気通信事業者は、顧客の承認を条件として、顧客に関するデータ	不明	第 4 条 データへのアクセス 各加盟国は、本指令にしたがって保持されたデータが国内法に沿った具体的事例において所轄国内官庁にのみ提供されるようにするための措置を取るものとする。

[37] http://www.ndl.go.jp/jp/data/publication/legis/215/21501.pdf 参照

[38] Department of Trade and Industry の略。現在は、Department for Business Entreprise & Regulatory Reform に改称されている。

[39] http://www.ndl.go.jp/jp/data/publication/legis/215/21501.pdf 参照

			の時点で消去され、かつ匿名にされなければならない。また、トラフィックデータの処理は、課金、顧客からの問い合わせ、不正行為の探知、又は関連する者による電気通信サービスのマーケティングの場合に限定される。しかし、紛争処理のための権限を有する者にトラフィックデータを提供することは許される。犯罪の捜査又は防止、刑事手続、裁判所の令状への対応等では事業者に対し、義務を課すものではない。 （刑事訴訟法[警察・刑事証拠法]） 1984 年の刑事訴訟法では、捜査機関は、差押え権限の一内容として、コンピュータに記録された情報を閲読可能な状態で提出するよう命ずる権限を有する。	の収集・処理・利用を行うことができることが規定されているほか、犯罪の未然の防止又は犯罪捜査のために必要であれば、顧客への通知を行わずに当局に対してデータを開示しなければならないこととされている。 （刑事訴訟法） 差押え物一般について、それを所持している者には、捜査機関の要求に応じて、それを提示し、引き渡す義務があり、それを拒絶した場合には、裁判官が、それに対する制裁として、金銭の支払い及びそれが徴収できない場合、拘禁を命ずることができる。		
保存期間	規定はない。	180 日（連邦刑事訴訟法 2703 条）		6 ヶ月（新通信法第 113 条 a） （※旧通信法では 1 ヶ月だったが、新通信法第 113 条 a は、6 ヶ月としている。なお、新法は 2009 年 1 月 1 日に発効する。）	不明	最低 6 ヶ月、最高 2 年間（第 6 条）

（1）日本

日本の電気通信事業法及び施行規則には以下の記述が存在する。

「(電気通信事業法)

第二十二条　特定電気通信役務を提供する電気通信事業者は、総務省令で定める方法により、その提供する特定電気通信役務の通信量、回線数等を記録しておかなければならない。

(電気通信事業法施行規則)

(通信量等の記録方法)

第二十条の二　法第二十二条 の方法は、通信の距離及び速度その他の料金区分ごとに、料金の課金単位により電気通信役務の通信量、回線数その他の供給量を記録する方法により行うものとする。」

電気通信事業法上、通信事業者は、通信量と回線数を含む記録（ログ）の保存は義務付けられているが、保存期間に関しては明示されていない。

法執行機関のログの利用に関しては、刑事訴訟法にて、法執行機関が通信事業者に利用の要請を行うことが可能であると規定されているが強制力はない。裁判所の命令による場合は、強制力が発生する。

（2）ドイツ

ドイツ連邦政府は、2006 年の欧州ログ保存指令を国内法化すべく「電気通信の監視及びその他捜査方法に関する新規制のため、ならびに 2006/24/EG 指令の国内法化のための法律」（Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG；通称データ備蓄保存法（Gesetz zur Vorratsdatenspeicherung））を提案した[40]。

データ備蓄保存法は、ドイツ連邦議会により 2007 年 11 月 9 日に可決され、2008 年 1 月 1 日に施行された[41]。このデータ備蓄保存は、刑事訴訟法、電気通信法、租税通則法、刑法、信書・郵便・電信電話の秘密の制限のための法律、社団法、連邦警察庁法、裁判所組織法等の法律を幅広く改正するものであるが、この法律に対する批判は根強く、近いうちに 3 万件以上の憲法訴訟が提起されると予測されている[42]。

並行に行われている仮手続において、ドイツ連邦憲法裁判所は早速データ備蓄保存法を部分的に発効しないものとした。憲法裁判所は、2008 年 3 月 19 日の仮命令により、保存されたデータの利用に関する規定を一定の範囲において問題視した[43]。また、裁判所はドイツ連邦政府に対して、データ保存による実務上の影響について 2008 年 9 月 1 日までに

---

[40] ログ保存法連邦政府案(http://www.bmj.bund.de/files/-/2047/RegE%20TK%DC.pdf) 参照。

[41] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007, Bundesgesetzblatt Jahrgang 2007 Teil I Nr. 70, S.3198 (http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s3198.pdf 参照)

[42] http://www.dradio.de/aktuell/756694/

[43] Bundesverfassungsgericht, Pressemitteilung Nr. 37/2008 vom 19. März 2008

報告するよう命じた[44]。

なお、電気通信業者に対してログ保存の義務付けは、新しく追加された通信法第 113 条 a によってなされている。ただし、インターネットアクセス、インターネット電話及び電子メールのサービスを提供する者に対する保存義務については猶予期間が認められ、これらの者との関係においては、第 113 条 a 等の規定は 2009 年 1 月 1 日に発効する（通信法第 150 条第 12 項 b)。

（3）EU

EU においては、2006 年 3 月 15 日にログ保存義務化に係る指令（Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC）[45]が発行されている。

本指令においては、2010 年 9 月 15 日までに、委員会は当該指令の適用及び経済上の事業者及び消費者に対する影響に関する評価を出さなければならないとされている。その際、将来的な技術の発展と、各国のログの保存期間のリストを含む統計データを鑑み、指令を改正の必要性を検討することになっている。国内法化期限は、2007 年 9 月 15 日となっており、さらに 2009 年 3 月 15 日までに、各加盟国は、インターネットアクセス、インターネット電話及びインターネット電子メールに関するログの保存に関して指令の適用を延期することができる。この規定を利用すること（つまり延期）を考えている加盟国は、理事会（Council)及び委員会(Commission）に対して通知しなければならない。

次の加盟国は、適用の延期を宣言した国である：

オランダ、オーストリア、英国、エストニア、キプロス、ギリシャ、ルクセンブルグ、スロベニア、スウェーデン、リトアニア、ラトビア、チェコ共和国、ベルギー、ポーランド、フィンランド、ドイツ。

なお、各加盟国の国内法化の状況は、2008 年 3 月 28 日現在、インターネットでまだ公開されていない。

（4）その他の国

1）イタリア

（刑事訴訟法）Codice di procedura penale

刑事訴訟法第 255 条においてデータの保全に関する記述が存在する。以下に概要を示す。

- 裁判官又は検察官の書面による要請による
- 遠隔通信サービス、プロバイダ等が要請の対象となる

[44] Bundesverfassungsgericht, Pressemitteilung Nr. 37/2008 vom 19. März 2008

[45] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:EN:HTML

・ 裁判権の管轄外のデータに関しては明確になっていない
・ 裁判権の管轄外のプロバイダに対しては要請を行う旨の記述がある
・ 省庁横断的な専門家委員会が保全費用に関する基準を決定する
・ 通信事業者は、刑事的にも民事的にも免責される
・ 個人情報保護法とは、コンフリクトする
（出典）http://www.meti.go.jp/kohosys/press/0002626/1/020418cyber.pdf

２）フランス
（通信法）Le code des postes et télécommunications
刑事訴訟法典に基づく手続によるほか、電気通信担当大臣により授権を受け、又は、政令の規定により宣誓した電気通信担当行政機関・電気通信規制機関・周波数庁は、電気通信事業者に対し、郵便電気通信法又は同法規則に基づいて、必要な情報の提供又は資料の提出を求めることができることとされている（第 32 の 3 条、第 40 条）。しかし、ネットワーク事業者及びアクセス事業者には、捜査機関に提出するために通信履歴を保存しておく義務はない。
（情報処理、ファイル及び個人の諸自由に関する法律）La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
1978 年に制定された同法においては、個人情報の収集・記録・保存についての個人の権利保障、アクセス権・訂正権等の承認、コンピュータ処理のみならずマニュアル処理・機械処理についても一定の保護がなされること等が記載されている。同法の適用を監視するための独立行政機関として、「情報処理及び自由に関する国家委員会(CNIL)」が設置されている。CNIL は、その任務の遂行のため、規則制定権を有するほか、立入検査、刑事告発、苦情申立ての受理等を行うことができる。
（出典）http://www.meti.go.jp/kohosys/press/0002626/1/020418cyber.pdf

2.5. 多くのサイバー空間の権利侵害の要因の対策に係る論点

多くのサイバー空間の権利侵害の要因になる事項として、ネットワークへの匿名アクセスとウイルス製造を中心とする欧州サイバー犯罪条約の批准状況について述べる。

2.5.1. サイバー空間の様々な権利侵害の要因となる可能性の高いネットワークへの匿名でのアクセスに関する特別な措置がなされているか

国内外において、ネットワークへのアクセス時における本人確認の法的担保について調査した。

法令による対策は、日本の携帯電話不正利用防止法、韓国における情報通信網利用促進及び情報保護等に関する法律等があるが、米国、英国、ドイツ、EU において関連法令は存在しない。

以下に日本、韓国、中国、イタリア、インドにおける法令の状況と関連する動きに関して述べる。

（1）日本

プリペイド携帯電話購入時の本人確認

携帯電話不正利用防止法（総務省携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律）にて、携帯音声通信事業者（携帯電話事業者及び PHS 事業者）に対し、携帯電話等（携帯電話及び PHS）の契約締結時及び譲渡時に、契約者の本人確認を義務付けている。

（2）韓国

インターネット実名制（制限的インターネット本人確認制）

情報通信網利用促進及び情報保護等に関する法律（参考資料 3-5 参照）にて、訪問者数 10 万人以上／日のサイトは、加入契約時に本人確認が義務化され、2007 年から運用が開始された。

（3）その他

1）中国

インターネットカフェ規制[46]

[46] ChinaTech News China To Introduce New Net-Monitoring System
http://www.chinatechnews.com/2004/04/29/1221-china-to-introduce-new-net-monitoring-system/

中国文化部は2005年までに中国の110,000のインターネットカフェに監視ソフトウエアを導入するとした。このソフトウエアを導入することで、ネットカフェのユーザの個人データが保存され、さらにユーザの閲覧ページは常に監視され、有害情報にアクセスした場合は警告が発せられる。

試験的インターネット実名制[47]

2007 年 7 月、サイト上のポルノなど有害サイトを取り締まる目的で、信息産業部が北京、天津、上海、河南、広東の 5 つの省・市で「実名制」を試験的に導入し、これを基に全国に広げていく管理規定を公布している。

プリペイド携帯電話購入時の本人確認[48]

China Telecom はプリペイド携帯電話の SIM カードを購入する際に、ID によって本人確認をするシステムを北京などの都市で開始した。Ministry of Security and State Council Information Office（MII） が 2006 年に携帯電話の本人確認を求めたことに端を発しているとされている。

2）イタリア

テロ対策法（Anti-terror law）[49]

イタリアでは、2005 年 7 月のロンドンにおける爆破事件後に制定された、テロ対策法により、インターネットカフェの経営者に対して、ユーザの身元確認とログの保存を義務付けた。更に身元確認の際は、官公庁から発行された写真付き ID のコピーを店側で保管する。

3）インド

都市単位におけるインターネットカフェ規制（バンガロール、ムンバイ）[50] [51]

インターネットカフェ使用者に対して写真付きの身分証明書で本人確認を行い、更に取得した個人情報は店側で 1 年間保存することを義務付ける。

---

[47] 中国における制限付きインターネット本人確認制
http://headlines.yahoo.co.jp/hl?a=20080129-00000003-rcdc-cn
[48] CNet, “China Mobile to require ID for previously anonymous prepaid users,”http://www.cnet.com/8301-13908_1-9858125-59.html
[49]USATODAY.com, Anti-terror law forces cybercafe owners to take names (2005)
http://www.usatoday.com/tech/news/computersecurity/2005-12-08-cybercafe-law_x.htm
[50] Times of India, Going to cybercafe? ID is a must
http://timesofindia.indiatimes.com/articleshow/859224.cms
[51] Times of India, DRAG-NET ON CRIMinals?
http://timesofindia.indiatimes.com/articleshow/259995.cms

2.5.2. ウイルス製造・保持・頒布に関する措置がなされているか

現在、日本では、ウイルス製造・頒布を規制する法律はない。しかし、欧州サイバー犯罪条約を国内法化する議論の中で、現在、ウイルスの作成、提供等を禁止する刑法の一部を改正する法律案が国会で審議されている。

本節では、ウイルス製造・保持・頒布に関する措置と欧州サイバー犯罪条約の批准状況について述べる。

なお、EU を除く調査対象国のうち、欧州サイバー犯罪条約を批准した国は、2008 年 3 月現在米国のみである。

（１）ウイルス等製造に係る法令の国内外の状況

表 2.5.2-1　ウイルス等製造に係る法令の国内外の状況

	日本	米国	英国	ドイツ	韓国	EU
適用法令	なし。 2008 年 3 月現在、国会で審議中。	コンピュータ詐欺及び濫用法(Computer Fraud and Abuse Act, 18 USC. 1030)	コンピュータ不正使用法（Computer Misuse Act of 1990）	刑法 202 条 c	情報通信網利用促進及び情報保護等に関する法律第 48 条	欧州サイバー犯罪条約にて、ウイルスの製造・流通・頒布を禁止
ウイルスの定義	コンピュータやシステムに利用者の意図に反する動作をさせること 。 （参考：ウイルス製造・流通・頒布を取り締まるための刑法の改正案）[52]	プログラム、情報、コード、指令の送信によって、保護されたコンピュータに損害を与えること。	コンピュータの運用を損ねること、または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ること、またはデータの信頼性やプログラムの運用を損ねること。	データのアクセスを可能とするパスワード又は他の防護コード若しくはこれら犯罪行為を行うことを目的とするコンピュータプログラム。	正当な権限なしにネットワーク、データ、コンピュータまたはプログラムなどに損害を与える、変更する、改ざんする、またはその運用を妨害すること。	不正アクセス、不正な傍受、データの妨害、システムの妨害犯罪を主として行うため設計され又は調整された装置(コンピュータプログラムを含む。)及びそれらに関連するデータ。
裁判例等	大学院生が、アニメ画像が現れるコンピュータウイルスを作成、著作権法違反容疑で検挙された。（2008 年 1 月 25 日）	メリッサウイルス裁判（Melissa virus のときの David Smith のケース）	見当たらない	見当たらない	見当たらない	なし

[52] http://www.moj.go.jp/HOUAN/KYOUBOUZAI/refer05.pdf

（2）欧州サイバー犯罪条約の批准動向

表 2.5.2-2　欧州サイバー犯罪条約に係る国内法整備の状況

日本 ※	平成 13(2001)年 11 月 23 日、署名 2004 年 3 月 16 日、衆議院外務委員会において承認。 2004 年 3 月 30 日、衆議院本会議で承認。 2004 年 4 月 10 日、参議院の外交防衛委員会において承認。 2004 年 4 月 21 日、参議院本会議で承認。
米国 ※	2001 年 11 月 23 日署名 2006 年 9 月 29 日批准 2007 年 1 月 1 日効力発生
英国	2001 年 11 月 23 日署名
ドイツ	2001 年 11 月 23 日署名
韓国 ※	－
EU	対象外（欧州評議会として）

※欧州評議会(Council of Europe)のメンバーではない。

2008 年 2 月 1 日現在、

- 署名したが、批准していない国：21 カ国
- 批准した国：22 カ国

表 2.5.2-3　欧州評議会の加盟国における欧州サイバー犯罪条約の国内法整備の状況

国（アルファベット順）	署名	批准	施行
アルバニア	2001 年 11 月 23 日	2002 年 6 月 20 日	2004 年 7 月 1 日
アンドラ			
アルメニア	2001 年 11 月 23 日	2006 年 10 月 12 日	2007 年 2 月 1 日
オーストリア	2001 年 11 月 23 日		
アゼルバイジャン			
ベルギー	2001 年 11 月 23 日		
ボスニア・ヘルツェゴビナ	2005 年 2 月 9 日	2006 年 5 月 19 日	2006 年 9 月 1 日
ブルガリア	2001 年 11 月 23 日	2005 年 4 月 7 日	2005 年 8 月 1 日
クロアチア	2001 年 11 月 23 日	2002 年 10 月 17 日	2004 年 7 月 1 日
キプロス	2001 年 11 月 23 日	2005 年 1 月 19 日	2005 年 5 月 1 日

チェコ共和国	2005年2月9日		
デンマーク	2003年4月22日	2005年6月21日	2005年10月1日
エストニア	2001年11月23日	2003年5月12日	2004年7月1日
フィンランド	2001年11月23日	2007年5月24日	2007年9月1日
フランス	2001年11月23日	2006年1月10日	2006年5月1日
グルジア			
ドイツ	2001年11月23日		
ギリシャ	2001年11月23日		
ハンガリー	2001年11月23日	2003年12月4日	2004年7月1日
アイスランド	2001年11月30日	2007年1月29日	2007年5月1日
アイルランド	2002年2月28日		
イタリア	2001年11月23日		
ラトビア	2004年5月5日	2007年2月14日	2007年6月1日
リヒテンシュタイン			
リトアニア	2003年6月23日	2004年3月18日	2004年7月1日
ルクセンブルク	2003年1月28日		
マルタ	2002年1月17日		
モルドバ	2001年11月23日		
モナコ			
モンテネグロ	2005年4月7日		
オランダ	2001年11月23日	2006年11月16日	2007年3月1日
ノルウェー	2001年11月23日	2006年6月30日	2006年10月1日
ポーランド	2001年11月23日		
ポルトガル	2001年11月23日		
ルーマニア	2001年11月23日	2004年5月12日	2004年9月1日
ロシア			
サンマリノ			
セルビア	2005年4月7日		
スロバキア	2005年2月4日	2008年1月8日	2008年5月1日
スロベニア	2002年7月24日	2004年9月8日	2005年1月1日
スペイン	2001年11月23日		
スウェーデン	2001年11月23日		
スイス	2001年11月23日		
マケドニア旧ユーゴスラビア共和国	2001年11月23日	2004年9月15日	2005年1月1日

トルコ	2001 年 11 月 23 日		
ウクライナ	2001 年 11 月 23 日	2006 年 3 月 10 日	2006 年 7 月 1 日
英国	2001 年 11 月 23 日		

表 2.5.2-4　その他の国の欧州サイバー犯罪条約の批准動向

国（アルファベット順）	署名	批准	施行
カナダ	2001 年 11 月 23 日		
コスタリカ			
日本	2001 年 11 月 23 日		
メキシコ			
フィリピン			
南アフリカ	2001 年 11 月 23 日		
米国	2001 年 11 月 23 日	2006 年 9 月 29 日	2007 年 1 月 1 日

出典：

http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=2/1/2008&CL=ENG

http://www.nichibenren.or.jp/ja/committee/list/kokusai_keiji/kokusai_keiji_a.html

1）日本

第 163 回国会（特別会）（平成 17 年 9 月 21 日～平成 17 年 11 月 11 日）において、「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」が提出された（継続審議中）。なお、犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案の概要は、以下のとおりである。

（1）不正指令電磁的記録作成罪等の新設（刑法）

○コンピュータウイルスの作成・提供・併用〔3 年以下の懲役・50 万円以下の罰金〕、取得・保管〔2 年以下の懲役・30 万円以下の罰金〕の処罰

（2）わいせつ物頒布罪の処罰対象の拡充（刑法）

○わいせつな電磁的記録の頒布行為をも処罰

（3）電磁的記録に係る記録媒体に関する証拠収集手続等の整備（刑事訴訟法）

○電磁的記録に係る記録媒体の差押さえの執行方法の整備

○記録命令付差押さえ

○電気通信回線で接続している記録媒体からの複写

○通信履歴の電磁的記録の保全要請

２）米国

連邦レベルでは、2001 年 10 月 26 日に施行された、2001 年愛国者法（USA Patriot Act of 2001[53]）第 814 条で、コンピュータ詐欺及び濫用法(Computer Fraud and Abuse Act, 18 USC. 1030)を改正した。内容は、保護されたコンピュータに損害を与えようとした者に対する刑罰を 10 年から 20 年に引き上げたというものである。なお、犯罪の構成要件は、実害が発生したことではなく、損害を与えようとした犯意が立証されることである[54]。

州レベルでは、例えば、カリフォルニア州のスパイウエア対策法（Consumer Protection Against Computer Spyware Act (CPACSA)」第 22947.3 条(a)(1)は、権限のないユーザが、また、権限のあるユーザの許可なく、商業的電子メール又はコンピュータウイルスを消費者のコンピュータから送信したり、中継ぎしたりしてはならないと規定する。

３）英国

コンピュータ不正使用法（Computer Misuse Act of 1990）第 3 条にて、コンピュータウイルスを作成し、流通させることに対する罰則規定を設けている。

４）ドイツ

ドイツのコンピュータ犯罪防止法は 2007 年 8 月 11 日に施行された[55]。コンピュータ犯罪防止法は、2001 年 11 月 23 日に締結された欧州サイバー犯罪条約 及び 2005 年 2 月 24 日に成立した欧州理事会の「情報システムに対する非合法な攻撃に関する枠組み決定」(Framework Decision on Illegal Attacks against Information Systems)に沿って、既存のドイツ刑法を改正したものである。ドイツ刑法は従来から、ウイルス等による攻撃に関する規定を置いていた（第 202 条ａ、第 303 条ａ、第 303 条ｂ）が、今回の改正により、既存の条項の要件を変更し、また、第 202 条ｂ等の新規定を追加することにより可罰規定の範囲を拡げたものである。とりわけ、旧法ではウイルスを作成する準備行為は、データ探知（第 202 条 a）等の犯罪行為に対する幇助行為として位置づけられていたため、犯罪行為が成立しなかったときには不可罰とされていたが、今回の改正で第 202 条 c を導入したことにより、ウイルス作成のための技術情報収集等の準備行為自体を処罰することが可能となった。

---

[53] USA Patriot とは、" Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (Public Law Pub.L. 107-56)の略。

[54] http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm

[55] コンピュータ犯罪の防止のための刑法改正法律第４１号
Einundvierzigstes Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7. August 2007, BGBl. Jahrgang 2007, Teil I Nr. 38, S.1786
(http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s1786.pdf)参照。

ドイツは、サイバー犯罪条約を未だ批准していないが 、ドイツ政府は批准すべく 2007 年 11 月に法案を連邦国会に提出している[56]。

2.5.3. 抜本的な情報セキュリティ対策のための基本法は存在するか

情報セキュリティ対策を抜本的に解決するための基本法は、調査対象国には存在しない。しかし、米国における情報セキュリティ法（FISMA）、韓国における電子政府法があり、政府が電子政府における情報セキュリティの確保を行うべきである旨が定められている法律が存在する。これらは、政府自らの情報セキュリティ確保を義務化することにより、広く世の中の情報セキュリティ対策も推進することを目的としたものと考えられ、情報セキュリティ対策の推進法の側面が強い。

[56] http://dip21.bundestag.de/dip21/btd/16/072/1607218.pdf

3. まとめ

3.1. 動向

（1）ネットワーク上の名誉毀損に関する法的枠組みについて

- ネットワーク上の名誉毀損がなされた場合、発言者の刑事的及び民事的責任に関しては、米国、英国、ドイツにおいても、リアル空間での名誉毀損と同様の措置がなされる。
- ネットワーク上の名誉毀損がなされた場合、プロバイダの法的責任に関しては、韓国ではプロバイダの削除義務が規定されているが、他の国ではプロバイダに関する責任は名誉毀損発言について知り得べきときにのみ責任を負い、それ以外の場合には責任はないと考える方向が一般的となっている。
- 電子掲示板等の責任者に関しては、日本で発言の削除義務及び損害賠償を認める判例が相次いでいるが、欧米ではそのような方向にはなっていない。

（2）発信者情報開示について

- ネットワーク上で迷惑な行為を受けた者が発信者情報の開示を求めるための権利は、各国の法律で認められている場合が多い。
- 日本を含む各国の法律にて裁判所に発信者情報開示命令を下した場合は強制力を伴う。

（3）迷惑メール対策について

- 携帯メールに関しては、日本以外の調査対象国全てにおいてオプトインとなっているが日本のみがオプトアウトである。
- パソコンにて取り扱う電子メールに関しては、日本、米国、韓国がオプトアウトであるが、他はオプトインとなっている。

（4）違法・有害情報対策について

- 違法情報の定義は、韓国以外ではわいせつ情報又は児童ポルノ情報及び著作権侵害されたコンテンツその他法律に違反した情報（名誉毀損など）であるとされているが、韓国では青少年にとって有害な情報が違法情報とされている。
- 有害情報とは、韓国以外で青少年にとって有害な情報とされているが、韓国では違法情報と有害情報の定義がほぼ同じとなっている。
- 違法情報に関するプロバイダの責任は、各国にて削除義務を定めているが、責任の範囲

も明確化する方向となっており、プロバイダの努力義務を規定する方向となっている。

（5）サイバー空間における個人情報保護について

・ サイバー空間における個人情報保護とリアル空間における個人情報保護に対する立法措置は、韓国以外では同一となっている。

（6）サイバー空間での営業秘密保護について

・ 調査対象国全てにおいて、サイバー空間の営業秘密保護はリアル空間と同様に扱われている。

（7）ネットいじめについて

・ いじめ防止に関しては、米国の多くの州で立法措置が進んでいるが、国レベルでの立法には至っていない。
・ ネットいじめに特化した立法は、デラウェア州において制定されている。

（8）オンライン海賊版について

・ 調査対象国において、サーバ及び P2P ソフトの著作権物の公開に関して、著作権違反であるとの判断がなされている。

（9）Winny 等のファイル共有ソフトウエアの開発者について

・ 調査対象国において、ファイル共有ソフトウエア等の開発者を規制する明文の規定はない。
・ 日本においては、Winny 開発者に対して著作権違反幇助が適用された例があるが、諸外国においてはそうした判例は存在しない。

（１０）ログ保存について

・ ドイツ等の EU 域内の国では、ログの保存義務化に係る指令に基づき、プロバイダ等にログの保存を義務付ける立法措置が進行している。
・ 米国においては、裁判所命令がなくても当局がログを利用できるが、裁判所命令が必要であることが一般的である。

（１１）ネットワーク利用に係わる本人確認について

・ 本人確認は、イタリア、韓国、中国等では立法化されているが、日本以外の調査対象 5 カ国では立法化されていない。

（１２）（ウイルス製造罪を含む）欧州サイバー犯罪条約について

・ 日本以外の調査対象国全てにおいて、ウイルス製造に関する法律が存在する。
・ 2008 年 2 月 1 日現在、署名したが、批准していない国は 21 カ国であり、批准した国は 22 カ国となっている。

（１３）情報セキュリティに関する基本法について
・ 調査対象国全てにおいて情報セキュリティ対策を抜本的に解決するための基本法は存在しないが、政府機関に対して情報セキュリティの確保を義務づけている法律として、米国における情報セキュリティ法（FISMA）、韓国における電子政府法がある。

3.2. 提言

上記の動向を鑑み、各論点に係わる提言を述べる。

１）迷惑メール対策におけるオプトインの導入
諸外国の動向を鑑み、日本においても、携帯の電子メールおよびパソコンの電子メールを含め、オプトインとすべきである。
２）違法情報対策の徹底
違法情報に関して、プロバイダの対応方針を明確に記述するガイドライン等を策定すべきである。
３）オンライン海賊版の送信対策の徹底
P2P ソフトウエアを利用し著作権上問題のあるコンテンツを配信する行為に関して、厳密な法の運用がなされるべきである。
４）ウイルス製造罪の立法化に関する検討
諸外国の動向に鑑み、ウイルス製造に関する法律案について速やかに検討を行い、欧州サイバー犯罪条約の早期批准を目指すべきである。
５）ログの保存義務化の検討
EU 諸国の動向に鑑み、日本においても、ログの保存義務化について今後検討を実施すべきである。

6）情報セキュリティに関する基本法の検討

諸外国の動向を参考にしつつ、日本において、情報セキュリティに関する基本法の整備について検討を行うことが有益である。

また、立法および運用に係わる措置に係わる留意点を以下に挙げる。

・匿名性担保による利便性確保と、実名性による安全性向上のバランス

インターネットにおいては匿名性がサイバー空間における自由な発言やエンターテインメントを構成できる要因となっている。一方、サイバー空間における権利侵害の要因が匿名性であることも指摘されている。そのため、匿名性と実名性のバランスを取ることが重要である。

・サイバー空間における脅威に係る現実のリスク分析をベースとすること

上記の匿名性と実名性のバランスを取る際の基準として、現実の脅威に係るリスク分析をベースとすることが適当である。

参考資料

参考資料１　ネットワークへのアクセス時における本人確認の法的担保

日本

○各メーカの動き

・NTT ドコモ、ツーカー

現在、契約者名義を登録していないドコモとツーカーのプリペイド携帯電話は利用できなっている。本人確認を行うことで、利用停止を解除できる。

・日本通信（WILLCOM）

日本通信は警察庁によるデータ通信カード購入時の本人確認の要請を受け、「b-mobile」などの同社商品のデータ通信カードのユーザが、製品や更新パッケージを購入し初めて利用を開始する際、専用の電話番号に携帯電話か PHS で電話をかけ、製品固有の番号などを入力する本人確認システムを導入した。

○ネットカフェ利用における本人確認

「インターネット・ホットラインセンターの運営の在り方及びインターネットカフェ等における匿名性その他の問題と対策」

警察庁がまとめた平成 18 年度総合セキュリティ対策会議 報告書 においてインターネットカフェにおける匿名性を排除するための取組みとして以下のような対策を推奨している。

１． 少なくとも、氏名、住所、生年月日等を官公庁、企業、学校等が発行した書面等で確認し、これらの情報を適切に管理しつつ一定期間保存する。

２． 各利用者の入店時刻及び退店時刻並びに当該利用者が使用したコンピュータに関する情報を一定期間保存する

「日本複合カフェ協会運営ガイドライン」

インターネットカフェや漫画喫茶などの事業者からなる日本複合カフェ協会では犯罪防止、青少年の非行防止のために運営ガイドラインを策定しているが、同ガイドラインでは、店舗に会員制を採用して本人確認を行うように推奨している。

―日本複合カフェ協会運営ガイドラインより抜粋―

１．ネットワーク利用犯罪やその他の犯罪の抑制又は防止、及び利用客の身元を確認するため、利用客について会員制度を採用するよう努めなければならない。

参考資料 2　ネットいじめの現状と対策の動向

各国におけるネットいじめの状況

（1）日本

現在インターネット上のいじめの問題が深刻化しており、2004 年に佐世保市内の小学校において小学 6 年の女児がネット上の電子掲示板上のトラブルから同級生を殺害した事件[57]、また 2007 年には岡山県の中学 3 年生の少女が学校の仲間が情報交換する携帯電話のサイトにおける抽象が原因で自殺するなど痛ましい事件[58]が発生している。文部科学省が平成 18 年度に実施した「児童生徒の問題行動等生徒指導上の諸問題に関する調査」[59]によると、調査対象（小学校 22,878 校、中学校 11,019 校、高校 5,412 校、特殊教育諸学校 1,006 校）において「パソコンや携帯電話等で、誹謗中傷や嫌なことをされる」との回答が 4,888 件あったと報告されている。

<u>啓発活動</u>

文部科学省「子どもを守り育てる体制づくりのための有識者会議」[60]

文部科学省の同会議の中で、子どもの携帯電話・ネットの利用における「ネット上のいじめ問題」を親に注意喚起をする目的で、保護者が行うべき 4 つの取組みが提案されている。

[57]佐世保小六同級生殺害事件 http://www.nagasaki-np.co.jp/index.shtml
[58]岡山中 3 女子自殺事件
http://www.sanyo.oni.co.jp/sanyonews/2007/12/28/2007122808341615006.html
[59]文部科学省「児童生徒の問題行動等生徒指導上の諸問題に関する調査」
http://www.mext.go.jp/b_menu/toukei/001/index31.htm
[60]文部科学省「子どもを守り育てる体制づくりのための有識者会議」
http://www.mext.go.jp/b_menu/shingi/chousa/shotou/040/toushin/07030123.htm

お父さん！お母さん！ お子さんのケータイ・ネットの利用は大丈夫ですか？
「ネット上のいじめ問題」に対する喫緊の提案

ネットいじめの問題に対して保護者が行うべき 4 つの取組み：
１．知っていますか？ ～子どもが利用できる携帯電話・ネットの中身を～
教えましたか？ ～携帯電話・ネットの危険性を～
→「利用の実態」に目を向けよう！
２．約束しましたか？ ～携帯電話・ネットでしてはならないことを～
～親子で学びましたか？ ～「情報モラル」について～
→「情報モラル」についてしっかり学ぼう！
３．聞いてみましたか～お子さんが「ネット上のいじめ」で悩んでいないかを
～学校と連携して実践していますか？
～携帯電話・ネットの間違った利用をチェックする活動を
→「チェック体制」を強化しよう！
４．学校と相談していますか？
～携帯電話・ネットによるいじめにあったときにしなければいけないことを～
→「いじめられた子ども」を守り通そう！

対策：文部科学省調査開始（2008 年 1 月～3 月末）

<u>携帯各社へのフィルタリングサービス設定要請</u>

総務省は 2007 年 12 月、携帯電話各社に対し、契約者が未成年の場合に有害サイトへの接続を制限する「フィルタリングサービス」への原則加入を要請。これに対して NTT ドコモ、KDDI、ソフトバンクが原則設定を決定した。

（2）米国

米国でも SNS の普及などにより未成年の痛ましい事件が多く発生している。ミズーリ州において 2006 年に大手 SNS の My space の利用者である Megan Meier という 13 歳の少女が同サイトの中で Josh という少年から嫌がらせを受けたことで自殺した事件[61]は、米国社会に大きな波紋を投げかけ、同州のいじめ防止法の制定に繋がった。またこの事件では、後の捜査で Megan に嫌がらせをしたとする少年は実際には存在せず、数名の大人が少年に成りすまして嫌がらせを行っていたことが発覚したことで、ネットいじめ（cyber-bullying）未成年のみの問題ではなく社会の問題として

[61]ネットいじめによる少女の自殺事件--マイスペースに召喚状
http://japan.cnet.com/news/biz/story/0,2000056020,20364742,00.htm

捉えられるきっかけとなった。その他にも 2003 年にはバーモント州の 13 歳[62]の少年が数ヶ月間、校内とオンラインの両方で、ゲイとからかわれたため自殺する事件が発生している。Pew Internet & American Life Project が実施した調査レポート Cyberbullying and Online Teens[63]によると、調査対象者 866 人の内 32%が何らかのネットいじめのターゲットになった経験があると回答している。

Pew Internet & American Life Project, Cyberbullying and Online Teens レポート

・何らかの形でネットいじめのターゲットになった経験にあっている：32%
・個人的なメールを他人に転送、公開される：15%
・オンライン上で噂を流される：13%
・誹謗中傷のメールが送られてくる：13%
・承諾なしで写真をオンライン上で公開された：6%
（調査対象：866 名）

法整備

Deleting Online Predators Act (2006)[64]

未成年が My space のようなソーシャルネットワーキングサイト及び、チャットルームに学校や図書館からアクセスすることを禁じている。ペンシルベニア州議員 Mike Fitzpatrick によって提出され、2006 年 7 月 27 日に下院で可決されたが、上院での審議は行われず、109 議会の会期廃案になっている。2007 年に The Deleting Online Predators Act of 2007[65]が再び下院エネルギー商業委員会に付託され、さらに DOPA 法案を一部含んだ Protecting Children in the 21st Century Act[66]が上院に提出されている。

ネットいじめ規制[67]

上述の SNS におけるネットいじめが原因して 13 歳の少女が自殺した事件を受け、

---

[62]Bostom.com, Death by cyber-bully
http://www.boston.com/news/globe/editorial_opinion/oped/articles/2005/08/17/death_by_cyber_bully/
[63]Pew Internet & American Life Project, “Cyberbullying and Online Teens”
http://www.pewinternet.org/pdfs/PIP%20Cyberbullying%20Memo.pdf
[64] Deleting Online Predators Act (2006) http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.5319:
[65] Deleting Online Predators Act of 2007
http://www.govtrack.us/congress/bill.xpd?bill=h110-1120
[66] Protecting Children in the 21st Century Act
http://www.govtrack.us/congress/bill.xpd?bill=s110-49
[67] City of Dardenne Prairie, Cyber Harassment Ordinance
http://www.news.com/beyond-binary/8301-13860_3-9823134-56.htm
Cyber Harassment Resolution
http://www.dardenneprairie.org/forms/CyberHarassmentOrd.pdf

ミズーリ州のダーデンヌプレーリー市は、米国で初めてネットいじめ（Net harassment）を禁じる法律を制定。罰則は禁固 90 日又は罰金 500 ドルとなっている。

ネットいじめ規制（ミズーリ州ダーデンヌプレーリー市）

ネットいじめ（Cyber-harassment）の定義：

電子コミュニケーションを通じて意図的に嫌がらせや脅迫などの攻撃を行うこと。

・わいせつや卑猥な言葉、画像の使用

・身体的、所有物への損害をほのめかす脅迫行為

電子コミュニケーションの例（これらに限らない）：

① e-mail

② インターネットを介したコミュニケーション

③ ポケベル

④ テキストメッセージ（携帯などによるメール）

罰則：禁固 90 日又は罰金 500 ドル

いじめ防止法

2007 年 5 月時点で 32 の州において「いじめ防止法」が制定されている。いじめ防止法の対象者は、学校、教師、学校区など学校の関係者であり、内容としては、各学校において各学校におけるいじめ防止指針の策定をすすめることを規定している。またいじめ防止指針の策定には明確な期限を定めることで、その実効性を高めている。いじめ防止法の制定については反いじめ団体、いじめ警察（Bully Police USA）[68]が深く関与している。いじめ警察は、いじめ自殺遺族の支援に始まり、いじめ被害者の相談、各州に反いじめ法の制定を求める活動などを行っている。独自に考案している「いじめ防止法が満たすべき 11 の基準」[69]を定め、同基準をもとに、各州のいじめ防止法に対して ABC 等の評価付けを行っている。また近年のネット上のいじめの問題を受け、11 の基準以外にもいじめ防止法の中にサイバー空間上のいじめを定義するべきといったコメントを出している。実際に、いじめ警察によって最高評価 AAA を受けたデラウエア州学校いじめ防止法では、上記の 11 の基準を満たしているほか、サイバー空間におけるいじめ（Cyber bullying）についても明記している点が評価されている。いじめ警察が各州におけるいじめ防止法の制定に与える影響は大きく 2007 年 5 月時点で 11 の州がいじめ警察の基準に沿った形のいじめ防止法を制定している。

68 いじめ警察（Bully Police USA）http://www.bullypolice.org/

69 Bully Police USA 反いじめ法が満たすべき項目
http://www.bullypolice.org/ThePerfectLaw2006.pdf

（参考）デラウエア州いじめ防止法のサイバー空間におけるいじめに関する記述

サイバーいじめに関する規定を置くこと。学校にいなくても、学校活動中でなくても、学校と密接に関係がある場合の電子機器等を使ったいじめを処分対象とすること

Bully Police が示す反いじめ法が満たすべき条件[70]

1. 条文上に必ず「いじめ（bullying)」という用語を用いること。
2. 学校安全法ではなく、明確に反いじめ法とすること。
3. Bullying（いじめ）harassment（嫌がらせ）の定義をすること。
   その際にいじめの被害者を限定しないこと。
4. いじめ防止指針等の策定に関して、規定すべき内容や策定方法を明確に規定すること。
5. 規則や指針、その他の具体的な反いじめプログラムの策定及びその実施にあたっては、州教育委員会、学校区、学校、親、生徒、専門家が皆で関与し、共同して行うよう規定すること。
6. 反いじめプログラムやいじめ防止指針は強制力を有するものとして規定すること。(任意ではない点を強調、ただし罰則は規定していない)
7. 各学校区等のいじめ防止指針策定にあたっては、そのデッドラインを設けること。
8. いじめ加害者による復讐、報復や、虚偽の申立てに対して、いじめ被害者を保護する規定を置くこと。
9. **学校区が反いじめ指針を誠実に履行した場合には、教師、学校、学校区はいじめ発生に関して免責されること。**逆に、指針履行に関して誠実でなかった場合には、当然、親や生徒は、学校区等を訴える権限を有すること。
10. いじめ被害者対応について明確に言及すること。カウンセリング、セラピー等を提供する場合にも、いじめ被害者に対し、最も優先的になされるよう規定すること。
11. いじめ防止指針等の実績やいじめ発生情報等についての報告を、学校区が州議会と州教育委員長に対して行うことを義務付けること。

表 1 いじめ防止法の制定状況

州	名称	ネットいじめの定義
Delaware	AN ACT TO AMEND TITLE 14 OF THE DELAWARE CODE TO ESTABLISH THE SCHOOL BULLYING PREVENTION ACT.	有(any intentional written, **electronic**, verbal or physical act)

[70]井樋 三枝子「アメリカ合衆国におけるいじめ防止対応－連邦によるアプローチと州の反いじめ法制定の動き」（http://www.ndl.go.jp/jp/data/publication/legis/233/023301.pdf）

West Virginia	WEST'S ANNOTATED CODE OF WEST VIRGINIA　CHAPTER 18. EDUCATION　ARTICLE 2C. HARASSMENT, INTIMIDATION OR BULLYING PROHIBITION	無
Alaska	HOUSE BILL 482	無
Ohio	Am. Sub. H. B. No. 276	無
Oklahoma	§70-24-100.3. School Bullying Prevention Act	無
Oregon	Chapter 617 Oregon Laws 2001	無
Rhode Island	2003 Rhode Island Acts, Chapter 213, HB 5919	無
Washington	HOUSE BILL REPORT - SHB 1444	無
Arkansas	3 ARKANSAS ACT 681, HB 2274, 6-18-514. Antibullying policies.	無
Iowa	Senate File 61	有(any **electronic**, written, verbal, or physical act)
Idaho	HOUSE BILL NO. 750aa HOUSE BILL NO. 750, As Amended "Jared's Law"	有（An act of harassment, intimidation　or bullying may also be committed　through the use of a land line, car phone or wireless telephone or through the **use of data or computer software that is accessed through a computer, computer system, or computer network.**）
Maine	Sec. 1. 20-A MRSA §1001, sub-§15, ¶A, as enacted by PL 1999, c. 351, §2,	無
South Carolina	Safe Schools Act	有(gesture, an **electronic** communication, or a written, verbal, physical, or sexual act)
Tennessee	AN ACT to amend Tennessee Code Annotated, Title 49, Chapter 6, Part 10, relative to school curricula.	無
Virginia	VIRGINIA ACTS OF ASSEMBLY - [H 2266]	無

Vermont	House Bill H.629, entitled “AN ACT RELATING TO BULLYING PREVENTION POLICIES”	無
Indiana	SENATE ENROLLED ACT No. 285	無
New Jersey	An Act concerning the adoption of harassment and bullying prevention policies by public school districts and supplementing chapter 37 of Title 18A of the New Jersey Statutes	無
Nevada	Assembly Bill No. 202–	無
California	BILL NUMBER: SB 719 CHAPTERED BILL TEXT (Bullying Prevention for School Safety and Crime Reduction Act of 2003)	無
Colorado	CHAPTER 154 EDUCATION - PUBLIC SCHOOLS SENATE BILL 01-080	無
Georgia	1999 Georgia Laws, H.B. 84, Chap. 282 (O.C.G.A. § 20-2-751.4 and O.C.G.A. § 20-2-751.5.)	無
Kansas	HOUSE BILL No. 2310	無
Arizona	HB 2368 school policies; pupils; bullying	無
Connecticut	Public Act No. 02-119 AN ACT CONCERNING BULLYING BEHAVIOR IN SCHOOLS AND CONCERNING THE PLEDGE OF ALLEGIANCE.	無
Maryland	Safe Schools Reporting Act of 2005	無
Louisiana	HOUSE BILL NO. 364	無
Mississippi	2001 Miss. Laws, S.B. 2390 Education Chapter 371154	無
New Hampshire	AN ACT relative to school district policies on bullying	無
Illinois	HB0018　LRB095 03463 NHT 23634 b	無
Minnesota	H.F. No. 504,　as introduced - 85th Legislative Session (2007-2008)	無
Texas	H.B. No. 283	無

Stop bullying キャンペーン[71]

米国保健社会福祉省保険リソース・サービス庁(Health Resources and Services Administration, U.S. Department of Health and Human Services）によるキャンペーン。子ども、保護者、教育者、専門家に対していじめへの防止策及び対処法、更に法的手続きに関する情報を提供する。

図 1　Stop bullying キャンペーン

（3）英国

英国子供・学校・家族省（State for Children, Schools and Families）[72]が行った調査によると、英国の 12-15 歳の児童 の 34%が何らかの形で「ネットいじめ」の被害を経験と回答している。こうした事態を重く見た英国政府はネットいじめに対する啓発キャンペーン「Laugh at it and you're a part of it」[73]を実施した。は子ども向けに 6 週間にわたって行われ、ソーシャルネットワーキングサービス（SNS）や Web サイトに 5 種類のイメージ画像や短編ビデオを掲載し、自分がいじめの対象となったらどう思うか、いじめが被害者にどのような影響を及ぼすか、学校、両親、友人がいじめをどのように防げるかについて訴えた。

71 bullying キャンペーン http://stopbullyingnow.hrsa.gov/
72 State for Children, Schools and Families（DCSF）http://www.dcsf.gov.uk/bullying/
73「Laugh at it and you're a part of it」http://yp.direct.gov.uk/cyberbullying/

図 2　State for Children, Schools and Families（DCSF）
“Laugh at it and you're a part of it”

（4）ドイツ

ドイツでは、ネットいじめに関する特別な措置は講じられていない。職場におけるいじめに関しては労働法により一定の保護が与えられている（損害賠償、解雇無効等）[74]。学校のいじめは、特別な措置の対象になっていないため、通常どおりに不法行為法や刑法（名誉毀損罪、強要罪、ストーカ行為罪等）が適用される。

なお、最近、学校の教師に対するネットいじめが話題となり、2007 年 7 月にはノルトライン・ヴェストファーレン州の司法大臣と教育大臣が対策をとると発表している[75]。

[74] Benecke, „Mobbing“ im Arbeitsrecht, NZA-RR 2003, 225ff.
[75] http://www.justiz.nrw.de/Presse/PresseJM/archiv/2007_02_Archiv/04_07_07/index.php

参考資料３　各国のサイバー空間における権利利益に係る法令

3-1　アメリカ合衆国

3-1-1　アメリカ合衆国法典集犯罪及び刑事手続第 1 部犯罪
　第 47 章 詐欺及び虚偽の供述

3-1-2　アメリカ合衆国法典集犯罪及び刑事手続第 1 部犯罪
　第 119 章 有線通信及び電子的通信の傍受及び口頭の会話の傍受

3-1-3　アメリカ合衆国法典集犯罪及び刑事手続第 1 部犯罪
　第 121 章 蓄積された有線通信、電子的通信及び取引記録へのアクセス

3-1-4　米国愛国者法逐条解説

3-1-5　2002 年連邦情報セキュリティ管理法（FISMA）

3-1-6　2002 年国土安全保障法（抄）

3-1-7　デラウェア州学校いじめ防止法

3-2　EU

3-2-1　データ保持に関する EU 指令

3-3　英国

3-3-1　1990 年コンピュータ不正使用法 （抄）

3-3-2　調査権限規制法（抄）

3-3-3　2006 年テロリズム法（抄）

3-4　ドイツ

3-4-1　「情報サービスおよび情報伝達サービスの枠組条件を規定するための法律」（通称マルチメディア法）と「テレメディア法」（通称インターネット法）との関係

3-4-2　刑法（第 202 条、第 303 条）

3-4-3　通信法（第 113 条 a、第 113 条 b）

3-5　韓国

3-5-1　情報通信網利用促進及び情報保護等に関する法律（抄）

3-5-2　情報通信網利用促進及び情報保護等に関する法律の施行令（抄）

3-6　日本

3-6-1　刑法改正案（抄）

【注意】参考資料 3-1-2、3-1-3、3-1-4、3-1-6、3-1-7、3-3-2、3-3-3 の取扱いについて

3-1　アメリカ合衆国

3-1-1　アメリカ合衆国法典集犯罪及び刑事手続第 1 部犯罪第 47 章詐欺及び虚偽の供述

原文：18 USC Sec. 1029 （01/02/2006） http://uscode.house.gov/
（仮訳）

合衆国法典

第 18 編　犯罪及び刑事手続
第 1 部　犯罪
第 47 章　詐欺及び虚偽の供述

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 47--FRAUD AND FALSE STATEMENTS

第 1029 条　アクセス装置に関する詐欺及び関連行為

(a)　いかなる者も、

(1)　認識して、かつ詐欺の意図で、一以上の偽のアクセス装置において製造し、使用し、又は不正取引すること

(2)　認識して、かつ詐欺の意図で一年間に、一以上の無権限のアクセス装置において不正取引又は使用すること、及び当該行為によって、無権限で、又は付与されたアクセス権限を超過して、故意にコンピュータにアクセスし、それによって、当該期間中に 1,000 ドル以上の価値になるものを入手すること

(3)　認識して、かつ詐欺の意図で、15 以上の偽の装置又は無権限のアクセス装置を所有すること

(4)　認識して、かつ詐欺の意図で、装置製造機器を製造し、不正取引し、管理若しくは保管し、又は所有すること

(5)　認識して、かつ詐欺の意図で、１年間に 1,000 ドル以上の代金又はそれに相当する価値のものを得る為に、他人に対して支給された一以上のアクセス装置における取引に対して 影響を及ぼしたこと

(6)　アクセス装置の発行者の権限なしに、認識して、かつ詐欺の意図で、以下を他人に要求すること

(A) アクセス装置の提供、又は

(B) アクセス装置を得る為に関連情報又は申請を売ること

(7) 認識して、かつ詐欺の意図で、電気通信サービスの無権限の使用を得る目的で変更された若しくは改変された電気通信機器を使用し、製造し、不正取引し、管理若しくは保管し、又は所有すること

(8) 認識して、かつ詐欺の意図で、スキャニング・レシーバを使用し、製造し、不正取引し、管理若しくは保管し、又は所有すること

(9) それが権限なしに通信サービスを入手するために使用されるかもしれない電気通信装置に関連若しくはその中に含まれる電気通信識別情報に挿入又は変更するために構成されたものであると知りながら、認識して、かつ詐欺の意図で、ハードウエア又はソフトウエアを使用し、製造し、不正取引し、管理若しくは保管し、又は所有すること

(10) クレジットカードシステム会員若しくは代理人の権限なしに、認識して、かつ詐欺の意図で、他人に、会員若しくはその代理人に対して、支払いの目的で、アクセス装置によって作成された一以上の取引の証拠又は記録を提示させた又はそのように調整すること

は、当該犯罪が州間若しくは国際取引に影響を及ぼした場合、本条の(c)項の規定するところにより処罰される。

(b)

(1) いかなる者も、本条第(a)項に基づく犯罪を実行しようと試みた者は、試みようとした犯罪に対して規定された処罰と同等の罰に処せられる。

(1) いかなる者も、本条(a)項における犯罪に 2 名以上で共謀した当事者である者は、当事者のうち誰かが当該犯罪を助長させる目的で行為に着手したときは、本条(c)項の犯罪に対する最高額の罰金を超過しない額の罰金又は本条(c)項における犯罪に対する最高拘禁刑の 1/2 の期間を超過しない期間の拘禁刑に処せられる。

(c) 罰則

(1) 総則－ 本条(a)項に基づく犯罪行為に対する処罰は、次のとおりである。

(A) 本条に基づき他の犯罪行為で有罪判決を受けた後に発生したものではない事案の場合－

(i) 当該犯罪行為が、(a)項の(1)、(2)、(3)、(6)、(7)又は(10)号に該当する場合、本編に基づく罰金刑若しくは 10 年以下の拘禁刑又はその併科、かつ

(ii) 当該犯罪行為が、(a)項の(4)、(5)、(8)又は(9)号に該当する場合、本編に基づく罰金刑若しくは 15 年以下の拘禁刑又は併科

(B) 本条に基づき他の犯罪行為で有罪判決を受けた後に発生した事案の場合、本編に基づく罰金刑若しくは 20 年以下の拘禁刑又はその併科、かつ

(C) いずれの場合においても、本条に基づき、財産の押収、処分及び関連する行政的ならびに司法的手続きを含む、財産の没収は、管理財産法(Controlled Substances Act)の 413 条が適用される。ただし、(d)項を除く。

(d) 合衆国シークレット・サービスは、捜査権限を有する他の政府機関に加え、本条にお

いて、犯罪行為を捜査するための権限を有する。当該合衆国シークレット・サービスの権限は、財務長官及び司法長官による合意にしたがって行使される。

(e) 本条において用いるときは、

(1) 「アクセス装置」という用語は、カード、プレート、コード、アカウント番号、電子的なシリアル番号、モバイル識別番号、個人識別番号その他の通信サービス、機器、道具の識別、又は、金品、サービスを得る目的でそれ自体として又は他のアクセス装置とつなぐことによって使用できるアカウントアクセスの手段、又は価値あるもの、又は資金の移動開始を着手するのに使用できるもの（紙の道具によってのみ発せられた移動以外）をいう；

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

(3) 「無権限のアクセス装置」という用語は、消滅、盗難、期限切れ、無効、取り消しになった又は詐欺の意図で得られたアクセス装置をいう

(4) 「製造された」とは、デザイン、改変、認証、複製、組み立てを含む；

(5) 「不正取引」(traffic)とは、移転若しくは他への配置、又は移転若しくは配置の意図をもって支配を得ることをいう。

(6) 「装置作成機具」(device-making equipment)とは、アクセス装置又は偽のアクセス装置を作成するためにデザインされた、若しくは一義的に使われた、機器、機械、又は痕跡のことをいう。

(7) 「クレジットカードシステム会員」(credit card system member)とは、クレジットカードシステムの会員である金融機関若しくは他の組織をいう。クレジットカードシステムの唯一の会員である発行者と提携している(affiliated with)か一致している（identical）組織を含む。

(8) 「スキャニング・レシーバ」(scanning receiver)とは、第 119 章に違反して、電話若しくは電子的通信の傍受、又は電子的シリアル番号、モバイル識別番号若しくは他の通信サービス、機器、道具の識別を傍受するために用いることができる装置若しくは器具を指す。

(9) 「通信サービス」(telecommunication service)とは、1934 年通信法第 1 編代 3 条(47 U.S.C. 153)の用語と同じ意味を有する。

(10) 「設備ベースのキャリア」(facilities-based carrier)とは、通信設備を持ち、当該設備の運営及び管理について責任を有し、1934 年通信法第 3 編に基づき、連邦通信委員会（Federal Communications Commission）から運用のライセンスの発行を受けているものを意味する。

(11) 「通信識別情報」(telecommunication identifying information)とは、特定の通信機器若しくはアカウント、又は通信機器からの特定の通信を識別する電子的シリアル番号その他の番号若しくは信号を意味する。

(f)　本条は、合衆国の法執行機関、州、州の政治部門、若しくは合衆国情報局の法執行機関の合法的な調査活動、防衛活動ないし諜報活動その他本編 224 章で認められている活動を妨げるものではない。本項において、「州」とは、合衆国の州、コロンビア特別区その他、準州及び合衆国領を含む。

(g)

(1)　設備ベースのキャリアの業務に従事する管理者、従業員若しくは代理人が、当該キャリアの財産若しくは適法な権利を守るために、(a)項(9)号で禁止されていない（不正取引以外の）行為をすることは(a)項(9)号の違反行為ではない。但し、当該行為が他の設備ベースのキャリアによって提供される通信サービスを当該キャリアの権限なしに得る目的でなされるのではないことに限る。

(2)　（製造若しくは不正取引を構成する場合を除き）(a)項(9)号違反の訴追においては、当該訴追された行為は、適法な目的を持つ調査若しくは開発のためになされたことを被告人の抗弁（被告人は立証責任を負う）とすることができる。

(h)　合衆国の管轄外の者が、合衆国の管轄内で行為に従事した場合は本条における(a)又は(b)項に定める犯罪を構成し、以下の場合、本編に規定されている罰金、刑罰、拘禁刑の対象となる。

(1)　当該犯罪が、金融機関、アカウント発行者、クレジットカードシステム会員その他合衆国の管轄内の組織によって発行、所有、経営、管理されたアクセス装置を含む場合

(2)　当該人物が合衆国の管轄内で、当該犯罪の幇助若しくは当該犯罪を助長した品物若しくはそこから派生した財産を運送、配達、運搬、移転、若しくは秘密を保管、所有した場合

原文：http://www.usdoj.gov/criminal/cybercrime/1030NEW.htm

（仮訳）

第 1030 条　コンピュータに関連する詐欺及び関連行為

(a)　いかなる者も、

(1)　無権限で、又は付与されたアクセス権限を超過していることを認識しながら、コンピュータにアクセスし、かつ、当該行為によって、合衆国の利益を侵害する目的又は外国に有利となるような目的のために入手されたと考える根拠がありながら、執行命令若しくは制定法の規定に従い合衆国政府によって国防若しくは外交関係上の理由で無権限の情報開示に対する保護すべきであると決定された情報、又は 1954 年原子力法第 11 条第 y 号に定義された機密データを入手し、それを故意に通信し、配達し、伝送し又はその通信、配達若しくは伝送されるようにし、又は通信、配達、伝送を試みた者、又はそれを受信する権限がない者に対して通信・配達・伝送されるようにした者、又は意図的に、受領権限を有する合衆国の公務員若しくは被雇用者に対して当該情報を保持しかつ

配達することを怠ったこと。

(2) 無権限で、又は付与されたアクセス権限を超過して、故意にコンピュータにアクセスし、それによって、以下を入手したこと

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

(B) 合衆国の省庁若しくは行政機関からの情報、又は、

(C) 当該行為の中に州際若しくは国際取引を含む場合には、保護されたコンピュータからの情報

(3) 故意に、合衆国の省庁若しくは行政機関の非公開コンピュータにアクセスする権限なしに、専ら合衆国政府のために利用される省庁又は機関コンピュータにアクセスしたこと、又は、そのような目的のために利用されるコンピュータでない場合には、合衆国政府により若しくは合衆国政府のために利用されるコンピュータにアクセスし、その行為によって、合衆国政府による利用若しくは合衆国政府のための利用に障害を発生させたこと

(4) 認識して、かつ、詐欺の意図で、無権限で又は権限を超過して保護されたコンピュータにアクセスし、当該行為が意図された詐欺を助長し、何らかの財産を得たこと。但し、詐欺の対象が及び入手するものがコンピュータ利用のみによって構成され、かつ、その 1 年以内の利用額が 5,000 ドルを超えない場合に限る。

(5)

(A)

(i) 認識して、プログラム、情報、コード、若しくは命令の伝送を生じさせ、当該行為の結果として、無権限で、故意に保護されるコンピュータに対し損害を発生させたこと

(ii) 無権限で、故意に保護されるコンピュータにアクセスし、当該行為の結果、無謀にも損害を発生させたこと、又は、

(iii) 無権限で、故意に、保護されるコンピュータにアクセスし、当該行為の結果、損害を発生させたこと、かつ、

(B) A 号(i)、(ii)、又は(iii)によって規定された行為によって以下のことを発生させた場合（又は、犯罪の未遂のケースでは、犯罪がなされた場合に以下のことを発生したであろう場合）

(i) 1 名以上の者に対し、1 年間に与えた損失（合衆国によってもたらされた捜査、起訴、又は他の手続、但し、1 以上の他の保護されたコンピュータに損害を与えた関連する行為から発生した損害に限る）が少なくとも 5,000 ドルの価値を生じさせる

(ii) 1 名以上の者に対し、医療行為、診断、治療若しくは手当てにおける変更若しくは加害、又は潜在的に変更、若しくは加害

(iii) 人に対する物理的な損害

(iv) 公共保健又は安全への脅威、又は

(v) 司法、国家防衛又は国家安全の行政を推進するために政府機関により利用され、若しくは政府機関のために利用されているコンピュータ・システムへの損害

(6) 無権限で、コンピュータにアクセスされることによって、パスワードその他これに類する情報におけるトラフィックを認識しながら、かつ、故意に、詐取し、以下のような場合：

(A) 当該トラフィックが州際若しくは国際取引に悪影響を及ぼした場合、又は

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

(7) 人から金銭その他の有価物を詐取する意図で、州際若しくは国際取引において、保護されたコンピュータに損害を発生させる危険を含む通信を伝送したこと

は、本条第(c)項が規定するところにより処罰される。

(b) 本条第(a)項に基づく犯罪を実行しようと試みた者は、本条(c)項に規定するところにより処罰される。

(c) 本条第(a)項又は第(b)項に基づく犯罪行為に対する処罰は、次のとおりである。

(1)

(A) 本条第(a)項 1 号に基づく犯罪であって、本条に基づき他の犯罪行為で有罪判決を受けた後に発生したものではない事案、又は、本副号に基づいて処罰し得る犯罪行為の実行の試みの事案の場合においては、本編に基づく罰金刑又は 10 年以下の拘禁刑又はその併科、及び

(B) 本条第(a)項(1)号に基づく犯罪であって、本条に基づき他の犯罪行為で有罪判決を受けた後に発生した事案、又は、本副号に基づいて処罰し得る犯罪行為の実行の試みの事案の場合においては、本項に基づく罰金刑若しくは 20 年以下の拘禁刑又はその併科、

(2)

(A) (B)副号に規定された場合を除き、本条の(a)項(2)号、第(a)項(3)号、第(a)項(5)号(A)(iii)(C)若しくは第(a)項(6)号の犯罪行為であって、本条に基づき他の犯罪行為で有罪判決を受けた後に発生したものではない事案、又は、本副号に基づいて処罰し得る犯罪行為の実行の試みの事案の場合においては、本項に基づく罰金刑若しくは 1 年以下の拘禁刑又はその併科、

(B) 第(a)項(2)号に基づく犯罪の事案において、

(i) 当該違反行為が、商業的利益若しくは私的な金銭獲得を目的として実行された場合、

(ii) 当該違反行為が、合衆国若しくは州の憲法及び法律に抵触する犯罪行為若しくは不法行為の遂行中に実行された場合、又は、

(iii) 入手された情報の価値が 5,000 ドルを超過する場合

には、本編に基づく罰金刑若しくは 5 年以下の拘禁刑又はその併科、

(C) 本条第(a)項(2)号、第(a)項(3)号、若しくは第(a)項(6)の犯罪であって、本条に基づき他の犯罪行為で有罪判決を受けた後に発生したものではない事案、又は、本副号に基づいて処罰し得る犯罪行為の実行の試みの事案の場合においては、本項に基づく罰金刑、若しくは 10 年以下の拘禁刑又はその併科、

(3)

(A) 本条第(a)項(4)号、若しくは第(a)項(7)の犯罪であって、本条に基づき他の犯罪行為で有罪判決を受けた後に発生したものではない事案、又は、本副号に基づいて処罰し得る犯罪行為の実行の試みの事案の場合においては、本項に基づく罰金刑、若しくは 5 年以下の拘禁刑、又はその併科、及び

(B) 本条第(a)項(4)号、第(a)項(5)号(A)(iii)、若しくは第(a)項(7)号の犯罪であって、本条に基づき他の犯罪行為で有罪判決を受けた後に発生した事案、又は、本副号に基づいて処罰し得る犯罪行為の実行の試みの事案の場合においては、本項に基づく罰金刑若しくは 10 年以下の拘禁刑又はその併科、及び、

(4)

(A) 本条第(a)項(5)号(A)(i)の犯罪、若しくは本項に基づいて処罰し得る犯罪行為の実行の試みの事案の場合においては、本項に基づく罰金刑若しくは 10 年以下の拘禁刑又はその併科、

(B) 本条第(a)項(5)号(A)(ii)の犯罪、若しくは本項に基づいて処罰し得る犯罪行為の実行の試みの事案の場合においては、本項に基づく罰金刑若しくは 5 年以下の拘禁刑又はその併科、

(C) 本条第(a)項(5)号(A)(i)、若しくは第(a)項(5)号(A)(ii)の犯罪であって、本条に基づき他の犯罪行為で有罪判決を受けた後に発生した事案、又は、本副号に基づいて処罰し得る犯罪行為の実行の試みの事案の場合においては、本項に基づく罰金刑若しくは 20 年以下の拘禁刑又はその併科、

(d)

(1) 合衆国シークレット・サービスは、捜査権限を有する他の政府機関に加え、本条において、犯罪行為を捜査するための権限を有する。

(2) 連邦捜査局（FBI）は、本編 3056 条(a)項に定めるところにより、合衆国シークレット・サービスの義務に悪影響を及ぼす犯罪以外の、スパイ活動、カウンターインテリジェンス、国防若しくは外交関係上の理由で無権限の情報開示に対する保護された情報、又は 1954 年原子力法第 11 条第 y 項（42 U.S.C. 2014 (y)）に定義する機密データを含む、本条第(a)項(1)号の犯罪を捜査する一次的権限を有する。

(3) 当該権限は財務長官及び司法長官による合意にしたがって行使される。

(e) 本条において用いるときは、

(1) 「コンピュータ」という用語は、論理、演算、若しくは記憶機能を実行する電子的、電磁的、光学的、電子化学的又はその他の高速データ処理装置を意味し、かつ、当該装置と関連し、若しくは結合して機能するデータ記憶装置、若しくは通信装置を含む。但し、自動タイプライタ、タイプセッタ、携帯用電卓、若しくはこれらと類似する装置を含まない。

(2) 「保護されたコンピュータ」という用語は、

(A) 金融機関、若しくは合衆国政府が専用で利用するコンピュータ、又は、そのような専用の利用にかかるコンピュータでない場合には、金融機関若しくは合衆国政府により利用され、若しくは、それらのために利用されるコンピュータであり、かつ、犯罪行為を構成する行為によって金融機関若しくは合衆国政府による利用、若しくはこれらのための利用に障害を発生させるもの、又は、

(B) 州際、若しくは海外取引又は通信において利用されるコンピュータ

を意味する。

(3) 「州」という用語は、コロンビア特別区、プエルトリコ共和国その他、準州及び合衆国領を含む。

(4) 「金融機関」という用語は、

(A) 連邦預金保険公社によって保険された預金を持つ機関

(B) 連邦準備又は連邦準備銀行を含む連邦準備委員

(C) 全米信用組合管理局によって保証された口座を持つ信用組合

(D) 連邦住宅融資銀行システムの構成員及び住宅融資銀行

(E) 1971 年農場信用法に基づく農業信用システムの機関

(F) 1934 年有価証券取引法第 15 条に基づき米国証券取引委員会に登録した販売者

(G) 有価証券投資者保護法人

(H) 1978 年国際銀行業法第 1 条第(b)項第(1)号又は第(3)号の外国銀行の支店若しくは代理店、及び、

(I) 連邦準備銀行法第 25 条又は第 25 条第(a)項に基づいて運営されている組織

を意味する。

(5) 「金融記録」という用語は、顧客と金融機関とが関係を結ぶことにより金融機関が保持した記録から得られる情報を意味する。

(6) 「付与されたアクセス権限を超過する」という用語は、権限に基づいてコンピュータにアクセスし、かつ、そのコンピュータの中にある当該アクセス者が入手する権限若しくは変更する権限を有しない情報を入手し又は変更するために、そのアクセスを利用することを意味する。

(7) 「合衆国の省庁」という用語は、政府の立法若しくは司法部門又は第 5 編第 101 条に列挙された執行部門の中の一つを意味する。

(8) 「損害」という用語は、データ、プログラム、システム、若しくは情報の完全性又は可用性に対する何らかの加害であって、

(9) 「政府の組織」という用語は、合衆国の政府、合衆国の州、若しくは政治部門、外国、並びに、外国の州、省庁、地方自治体その他の政治部門を意味する。

(10) 「有罪」という用語は、州法に基づき、1 年以下の拘禁刑によって処罰し得る犯罪行為に対する有罪判決を含む。その要素はコンピュータに対する無権限のアクセス又は付与されたアクセス権限の超過である。

(11) 「損失」とは、被害者に対する合理的な金額（犯罪行為に対するコスト、損害の算定、データ、プログラム、システム若しくは犯罪行為以前の情報を含む）及び収入の損失、サービスの妨害により引き起こされた費用その他重大な損害を意味する。

(12) 「人」とは、個人、会社、組合、教育機関、金融機関、政府機関その他法人を意味する。

(f) 本条は、合衆国の法執行機関、州、州の政治部門、若しくは合衆国情報局の法執行機関の合法的な調査活動、防衛活動ないし諜報活動を妨げるものではない。

(g) 本条の違反行為を原因として損害、若しくは損失を被った者は、加害者に対し、損害賠償請求、暫定的差止請求、又はその他の衡平法上の救済を求めるために民事訴訟を提起することができる。本条における民事訴訟は、第(a)項(5)号(B)の(i)、(ii)、(iii)、(iv)に定義する要素のうち一つ以上含まれれば定期することができる。第(a)項(5)号(B)(i)に定義されている行為のみを含む侵害行為に対する損害については、経済的損失に限られる。侵害行為であると主張する行為の日又は損害発見日から 2 年を経過したときは、本条に基づいて訴訟を提起することはできない。コンピュータのハードウエア、ソフトウエア若しくはファームウエアのデザイン若しくは製造の過失については本条に基づいて訴訟を提起することはできない。

(h) 司法長官及び財務長官は、本条の制定後の最初の 3 年間は、合衆国連邦法典集第 18 編 1030 条第(a)項(5)号に基づく調査と執行に関し、連邦議会に対し、年次報告をしなければならない。

3-1-2　アメリカ合衆国法典集犯罪及び刑事手続第 1 部犯罪第 119 章有線通信及び電子的通信の傍受及び口頭の会話の傍受

出典：「米国愛国者法（反テロ法）（下）（執筆者：平野美惠子、土屋恵司、中川かおり）」『外国の立法』No.215, 2003 年 2 月, pp.16-35（第 2510 条～第 2522 条　<http://www.ndl.go.jp/jp/data/publication/legis/215/21501.pdf>
※注釈は省略している。

合衆国法典

第 18 編　犯罪及び刑事手続
第Ⅰ部　犯罪
第 119 章　有線通信及び電子的通信の傍受及び口頭の会話の傍受
U.S.C. TITLE18. CRIMES AND CRIMINAL PROCEDURE
PART　I　CRIMES
CHAPTER119. WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

(2002 年 6 月 28 日現在)

中川かおり訳

第 2510 条　定義

この章において、次の用語が使用されるときは、当該の規定に定めるところによる。

(1)「有線通信（wire communication)」とは、音声の伝送であって、その全部又は一部が、州際の若しくは外国との通信又は州際の若しくは外国との通商に影響を与える通信の送信のために設備を提供し、又はこれを運営する者により、設置され、又は運営される、発信点と受信点の間に電話線、ケーブルその他類似の接続線（切替地点における接続線の
利用を含む。）を使った通信の送信のための設備を利用して行われるものをいう。

(2)「口頭の会話（oral communication)」とは、通信が傍受を受けないという期待を正当化する状況の下で、傍受を受けないという期待を表明する者により発される口頭の会話をいう。ただし、電子的通信は含まれない。

(3)「州（State)」とは、合衆国の各州、コロンビア特別区、プエルトリコ準州及び合衆国のその他の領土若しくは占有地をいう。

(4)「傍受（intercept)」とは、電子的、機械的その他の装置の利用を通じて、有線通信、電子的通信又は口頭の会話の内容を音声その他の形態で捕捉することをいう。

(5)「電子的、機械的その他の装置（electronic,mechanical,or other device)」とは、次の

ものを除く有線通信、口頭の会話又は電子的通信を傍受するために利用することができる装置又は機器をいう。

(a) 電話若しくは電信装置、機器若しくは設備、又はその構成要素であって、次の規定に該当するもの

(i) 有線通信サービス若しくは電子的通信サービスのプロバイダが通常の営業の過程で受信契約者若しくは利用者に提供し、通常の営業の過程で受信契約者若しくは利用者により利用されるもの又はサービス設備との接続のためにその受信契約者若しくは利用者により提供され、プロバイダが通常の営業の過程で利用するもの

(ii) 有線通信サービス若しくは電子的通信サービスのプロバイダが通常の営業の過程で利用するもの又は捜査官若しくは法執行官がその通常の職務の遂行において利用するもの

(b) 正常以下の聴覚を正常な程度に補正するために利用される補聴器又は同様の装置

(6) 「人（person）」とは、合衆国、州若しくはその行政的下部組織の被用者若しくは代理人、個人、協力者、社団、共同出資会社、信託又は法人をいう。

(7) 「捜査官又は法執行官（Investigative or law enforcement officer）」とは、この章に列挙される犯罪について、捜査を行い、又は、逮捕する権限を法律により与えられる連邦、州又はその行政的下部組織の職員及びその犯罪を訴追し、又は訴追手続に参加する権限を法律により与えられた検察官をいう。

(8) 「内容（contents）」は、有線通信、口頭の会話又は電子的通信に関して使用されるときは、通信の主旨、意図又は目的に関する情報を含む。

(9) 「管轄権を有する裁判官（Judge of competent jurisdiction）」とは、次の者をいう。

(a) 連邦地方裁判所又は連邦控訴裁判所の裁判官

(b) 有線通信、口頭の会話又は電子的通信の傍受を授権する命令を発する権限を州法により与えられる一般的刑事管轄権を有する州裁判所の裁判官

(10) 「通信についての一般通信事業者（communication common carrier）」とは、合衆国法典第 47 編第 153 条(h)による「一般通信事業者」の定義と同様の意味を有する。

(11) 「権利を侵害された者（aggrieved person）」とは、傍受された有線通信、口頭の会話又は電子的通信の一方当事者又は傍受の対象とされた者をいう。

(12) 「電子的通信（electronic communication）」とは、符号、信号、文字、画像、音、データ又はある種の情報の伝送であって、その全部又は一部が、州際の又は外国との通商に影響を与える有線、無線、電磁気、光電子変換又は光変換を用いたシステムを利用して送信されるものをいう。ただし、次のものは除く。

(A) 有線通信又は口頭の会話

(B) 信号音のみのページング装置により行われる通信

(C) 追跡装置からの通信（この編の第 3117 条の定めるところに従う。）

(D) 電子的蓄積及び資金移転に利用される通信システムにおいて、金融機関により蓄積さ

れた電子資金取引情報

(13) 「利用者（user）」とは、次の人又は団体をいう。

(A) 電子的通信サービスを利用し、かつ、

(B) そうした利用権限をサービスのプロバイダにより正当に与えられた者

(14) 「電子的通信システム（electronic communications system）」とは、有線通信又は電子的通信の送信のための有線、無線、電磁気、光変換又は光電子変換を用いた設備及びその通信の電子的蓄積のためのコンピュータ設備又は関連電子機器をいう。

(15) 「電子的通信サービス（electronic communication service）」とは、有線通信又は電子的通信を送信し、又は受信する能力を利用者に提供するサービスをいう。

(16) 「公衆が容易にアクセスできる（readily accessible to the general public）」とは、無線通信については、その通信が次のものではないことをいう。

(A) スクランブル化又は暗号化されているもの

(B) 通信の秘密を保護する意図で、基本的なパラメータが公衆に公表されていないような変調技術を利用して送信されるもの

(C) 無線通信に従属する副搬送波又は他の信号波で送信されるもの

(D) 通信が信号音のみのページングシステム通信である場合を除く、一般通信事業者により提供される通信システムにより送信されるもの

(E) 放送補助サービスに排他的に割り当てられていない連邦通信委員会規則第 74 部に基づき割り当てられる周波において送信される通信である場合に、その通信が無線による双方向音声通信であるときを除き、第 25 部、第 74 部の D 節、E 節若しくは F 節又は第 94 部に基づき割り当てられた周波により送信されるもの

(F) 削除

(17) 「電子的蓄積（electronic storage）」とは、次のものをいう。

(A) 電子的送信に伴う有線通信又は電子的通信の、暫定的、中間的な蓄積

(B) 通信のバックアップの保護の目的で、電子的通信サービスにより行われる通信の蓄積

(18) 「音声の伝送（aural transfer）」とは、発信地点と受信地点との間及びそれを含む地点での、人間の声を含む伝送をいう。

(19) この編の第 2517 条第 6 項の目的上、「外国諜報情報」とは、次のものをいう。

(A) 合衆国の人に関係するか否かを問わず、次のことに対する合衆国の防衛能力に関係する情報

(i) 外国勢力又は外国勢力のエージェントによる現実的な又は潜在的な攻撃又は他の重大な敵対行為

(ii) 外国勢力又は外国勢力のエージェントによる破壊活動又は国際テロリズム

(iii) 外国勢力の諜報機関若しくは諜報ネットワークによる、又は外国勢力のエージェントによる秘密諜報活動

(B) 合衆国の人に関係するか否かを問わず、次のいずれかに関係する外国勢力又は外国領土に関する情報

(i) 合衆国の防衛又は安全保障

(ii) 合衆国の外交の遂行

(20) 「保護されたコンピュータ（protected computer）」とは、第 1030 条に定める意味を有する。

(21) 「コンピュータへの不正アクセス者（computer trespasser）」とは、次の者をいう。

(A) 保護されたコンピュータに権限なくアクセスする者で、それゆえ、保護されたコンピュータへの通信、それを通した通信又はそれからの通信におけるプライバシーを合理的に期待できない者

(B) 保護されたコンピュータの全部又は一部へのアクセスのために保護されたコンピュータの所有者又は管理者とすでに契約関係にあることを、保護されたコンピュータの所有者又は管理者が把握している者は含まない。

第 2511 条　有線通信、口頭の会話又は電子的通信の傍受及び開示の禁止

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

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

(b) 次の場合に、口頭の会話を傍受するための電子的、機械的その他の装置を意図的に利用し、利用を試み、又は他の者を説得して利用させ、若しくは利用を試みさせる者

(i) その装置が、有線通信に利用される電話線、ケーブルその他類似の接続線に設置され、又はそれを通して信号を送信する場合

(ii) その装置が無線による通信を送信し、又はそうした通信の送信を妨害する場合

(iii) その者が、その装置又はその構成要素が、郵送され、又は州際の若しくは外国との通商により輸送されたことを知っている、又は知っている理由がある場合

(iv) その利用又は利用の試みが、(A)その営業が州際の若しくは外国との通商に影響を及ぼす営業所若しくは事業所の土地で行われる場合、又は(B)その営業が州際の若しくは外国との通商に影響を及ぼす営業所若しくは事業所の営業に関係する情報を得、若しくは得ることを目的とする場合

(v) その者がコロンビア特別区、プエルトリコ準州又は他の合衆国の領域若しくは領地において行動する場合

(c) 情報が、この項に違反して、有線通信、口頭の会話又は電子的通信の傍受により取得されたことを知り、又は知っている理由がありながら、有線通信、口頭の会話又は電子的通信の内容を、故意に他の者に開示した者又は開示を試みた者

(d) 情報が、この項に違反して、有線通信、口頭の会話又は電子的通信の傍受により取

得されたことを知り、又は知っている理由がありながら、有線通信、口頭の会話又は電子的通信の内容を、故意に利用し、又はその利用を試みた者

(e)(i) この章の第 2511 条第２ 項(a)(ii)、第 2511 条第２項(b)-(c)、第 2511 条第２項(e)、第 2516 条及び第 2518 条により授権される方法により傍受された有線通信、口頭の会話又は電子的通信の内容を他の者に対し、故意に開示し、又は開示を試みた者

(ii) 情報が犯罪捜査と関連して通信の傍受により取得されたことを知り、又は知っている理由がある者

(iii) 犯罪捜査との関連で情報を取得し、又は受領した者

(iv) 正式な権限に基づく犯罪捜査を故意に妨害する意図を持つ者

(2)(a)(i) 交換台のオペレータ又はその設備が有線通信若しくは電子的通信の送信に利用される有線通信サービス若しくは電子的通信サービスのプロバイダの職員、被用者若しくは代理人は、サービスの提供又はサービスのプロバイダの権利若しくは財産の保護に必然的に付随する活動に従事する場合には、通常の職務の過程で通信を傍受し、開示し、又は利用することは、この章の下では違法とされない。ただし、公衆向けの有線通信サービスのプロバイダは、機械又はサービスの質をコントロールするためのチェックを除き、サービス監視又はランダム監視をしてはならない。

(ii) 他の法律の定めにかかわらず、有線通信サービス若しくは電子的通信サービスのプロバイダ、その職員、被用者若しくは代理人、不動産所有者、管理者又は他の者は、次のいずれかを与えられる場合には、有線通信、口頭の会話若しくは電子的通信の傍受又は 1978 年外国諜報監視法（Foreign Intelligence Surveillance Act of 1978）第 101 条に定義された電子監視を法律により授権された者に対し、情報、設備又は技術的支援を提供する権限を有する。

(A) 授権する裁判官の署名を受けた、支援を指示する裁判所命令

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

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

判所命令又は証明書の文言に従って情報、設備又は支援を提供することは、いかなる裁判所においても訴訟原因として認められない。

(b) 連邦通信委員会の職員、被用者又は代理人が、通常の職務の過程及び合衆国法典第47編第5章に基づく委員会の監視責任の遂行において、有線通信、電子的通信若しくは無線で送信される口頭の会話を傍受すること又はそれにより取得した情報を開示し、若しくは利用することは、この章の下では違法とされない。

(c) 有線通信、口頭の会話又は電子的通信の傍受を法の外観の下で行う者は、その者が通信の当事者である場合又は通信の一方の当事者がこの傍受について事前の同意を与えた場合には、この章の下では違法とされない。

(d) 有線通信、口頭の会話又は電子的通信の傍受を法の外観によらず行う者は、その者が通信の当事者である場合又は通信の一方の当事者がこの傍受について事前の同意を与えた場合には、合衆国憲法、連邦法又は州法に違反する犯罪行為又は不法行為を行う目的で通信を傍受するのでなければ、この章の下では違法とされない。

(e) この編の別の規定又は1934年通信法（Communications Act of 1934）の第705条若しくは第706条の規定に関わらず、合衆国の職員、被用者又は代理人が、通常の公的職務の遂行過程において、1978年外国諜報監視法（Foreign Intelligence Surveillance Act of 1978）第101条の定めに従い、その授権により電子監視を行うことは、違法とされない。

(f) この編のこの章、第121章若しくは第206章又は1934年通信法第705条に含まれる規定は、1978年外国諜報監視法第101条に定める電子監視以外の方法を用いた、合衆国政府による国際通信若しくは外国との通信からの外国諜報情報の収集又は外国の電子的通信システムに適用可能な別の連邦法に従いなされる外国情報収集活動に、影響を与えるものとみなしてはならない。この編のこの章、第121章又は第206章及び1978年外国諜報監視法に定められた場合にのみ、外国諜報監視法第101条に定められた電子監視及び国内の有線通信、口頭の会話及び電子的通信の傍受を行うことができる。

(g) この編のこの章又は第121章の下で、次のことをすることは違法とされない。

(i) 電子的通信に公衆が容易にアクセスできるように設定されている電子的通信システムを通じて行われる電子的通信を傍受し、又はアクセスすること。

(ii) 次のものにより送信される無線通信を傍受すること。

(I) 公衆の利用のための放送局、すなわち、遭難した船舶、航空機、自動車又は人に関連する放送局

(II) 公衆が容易にアクセスできる政府、法執行、市民防衛、民間移動電話又は警察及び消防を含む公共保安のための通信システム

(III) アマチュア無線、市民無線又は移動無線サービスに割り当てられた帯域の許可を受けた周波数で営業する放送局

(IV) 港湾通信システム又は航空通信システム

(iii) 次の行為を行うこと。

(I) 1934 年通信法第 633 条により禁止される行為

(II) 1934 年通信法第 705 条 b 項により同法第 705 条 a 項の適用から除外される行為

(iv) 法律に従って営業する放送局又は顧客の電子機器に対し、有害な混信を引き起こす有線通信又は電子的通信の送信を、その混信の原因を特定するのに必要な限りで傍受すること。

(v) 無線通信がスクランブル化又は暗号化されていない場合に、システムを提供し、又は利用する個人が監視する周波数を利用して、そのシステムを通じてなされる通信を、同じ周波数を利用する別の利用者のために傍受すること。

(h) 次のことはこの章の下では違法とされない。

(i) ペンレジスター又はトラップ・アンド・トレース装置（この用語は、この編の第 206 章（ペンレジスター及びトラップ・アンド・トレースに関するもの）の目的のために定めるところによる。）を利用すること。

(ii) 電子的通信サービスのプロバイダが、そのプロバイダ自身、有線通信若しくは電子的通信の完遂のためのサービスを提供する別のプロバイダ又はそのサービスの利用者を、不正、違法又は乱用的なサービスの利用から保護するために、有線通信又は電子的通信が開始され、又は終了した事実を記録すること。

(i) 保護されたコンピュータに対し、それを通して、又はそれから送信されたコンピュータへの不正アクセス者の有線通信又は電子的通信を傍受するために、ある者が法の外観の下に行動することは、次のいずれをも満たす場合にはこの章の下で違法とされない。

(I) 保護されたコンピュータの所有者又は管理者が、保護されたコンピュータにおける不正アクセス者の通信の傍受を授権する場合

(II) 法の外観の下に行動する者が、合法的に捜査に従事する場合

(III) 法の外観の下に行動する者が、不正アクセス者の通信の内容が捜査に関連すると信ずる相当の理由がある場合

(IV) そうした傍受が、不正アクセス者へ、又は不正アクセス者から送信される以外の通信を収集しない場合

(3)(a) この項の(b)に定められる場合を除き、公衆に電子的通信サービスを提供する人又は団体は、そのサービスにおける送信にあたり、通信（その人若しくは団体又はその代理人に対する通信を除く。）の内容を、通信の名宛人若しくは所定の受信者以外の人若しくは団体又は名宛人若しくは所定の受信者の代理人以外の人若しくは団体に対して意図的に漏示（divulge）してはならない。

(b) 公衆に対して電子的通信サービスを提供する人又は団体は、次のいずれかの条件を満

たすときは、その通信の内容を漏示することができる。

(i) この編の第 2511 条第２ 項(a)又は第 2517 条に別に授権されるところに従うこと。

(ii) 通信の発信者、名宛人又は所定の受信者の法律に基づいた同意を得ること。

(iii) 通信を宛先に送信するために、雇われた者、権限を与えられた者又はその設備が利用される者に対するものであること。

(iv) 法執行機関へ漏示される場合には、サービス・プロバイダにより意図せずに取得され、かつ、犯罪に関係することが明らかに認められるもの

(4)(a) この項の(b)又は第５項に定められる場合を除き、この条の第１項に違反した者は、この編に基づく罰金若しくは５年以下の拘禁刑に処し、又はこれを併科する。

(b) 犯罪が、この項の(a)に基づく最初の犯罪であり、不法の若しくは違法の目的のためではない場合又は直接的若しくは間接的な商業上の利益若しくは私的な商業上の利得のためではない場合に、(a)に基づく犯罪に関連する有線通信又は電子的通信が、スクランブル化若しくは暗号化されていない無線通信であるとき又は通信の秘密を保護する意図で基本的なパラメータが公衆に公表されないような変調技術を利用して送信されていない無線通信であるときには、次のとおりに処罰する。

(i) 通信が、携帯電話通信、コードレス電話の子機と親機の間の通信、公共移動電話無線サービス通信又はページングサービス通信の無線部分ではなく、その行為が第５項に定められていないものである場合には、違反者はこの編に基づく罰金若しくは１年以下の拘禁刑に処し、又はこれを併科する。

(ii) 通信が、携帯電話通信、コードレス電話の子機と親機の間の通信、公共移動電話無線サービス通信又はページングサービス通信の無線部分である場合には、違反者にはこの編に基づく罰金を科す。

(c) 暗号化又はスクランブル化されていない衛星通信の傍受を構成し、又は関連する行為であって、次の規定に該当する、通常はこの項に基づく犯罪となる行為は、直接的若しくは間接的な商業上の利益又は私的な商業上の利得を目的としないかぎり、この項に基づく犯罪とはされない。

(i) 一般公衆への再送の目的で放送局に対して送信されるもの

(ii) 公衆に開かれた設備に再分配するために、可聴周波の副搬送波として送信されるもの（ただし、データ送信又は電話を除く。）

(5)(a)(i) 次のいずれかの場合には、その行為を行う者は、管轄権を有する裁判所において連邦政府により訴訟を提起される。

(A) 通信が、スクランブル化又は暗号化されていない民間衛星画像通信であって、この章に違反する行為が、通信の私的な鑑賞であり、かつ不法の若しくは違法な目的のためではない場合又は直接的若しくは間接的な商業上の利益若しくは私的な商業上の利得を目的としない場合

(B) 通信が、スクランブル化又は暗号化されていない、連邦通信委員会の規則第 74 部 D 節に基づき割り当てられた周波数において送信される無線通信であって、この章に違反する行為が、不法の若しくは違法な目的のためではない場合又は直接的若しくは間接的な商業上の利益若しくは私的な商業上の利得を目的としない場合

(ii) この項に基づく行為については、

(A) この章の違反が、第 4 項(a)の定める者の最初の犯罪であり、その者がこの編の第 2520 条に基づく民事訴訟において責任を負わない場合には、連邦政府は適切な差止命令による救済を得る権利を有する。

(B) この章の違反が第 4 項(a)に基づく二度目若しくはそれ以降の犯罪である場合又はその者が第 2520 条に基づく以前の民事訴訟で責任を負わされた場合には、その者は 500 ドルの民事罰を裁量の余地なく科される。

(b) 裁判所は、(ii)(A)に基づいて発せられた差止命令を執行するために権限内のいかなる方法も利用でき、差止命令の違反のそれぞれについて、500 ドル以上の民事罰を科さなければならない。

第 2512 条　有線通信、口頭の会話又は電子的通信を傍受する装置の製造、配布、所有及び広告の禁止

(1) この章に別に特に定められる場合を除き、次のことを意図的に行う者は、この編に基づく罰金若しくは 5 年以下の拘禁刑に処し、又はこれを併科する。

(a) 電子的、機械的その他の装置の設計が有線通信、口頭の会話又は電子的通信の不正な傍受の目的のために主に有用であることを知り、又は知っている理由がありながら、その装置を郵送し、又は州際の若しくは外国との通商により送付し、若しくは運搬すること。

(b) 電子的、機械的その他の装置の設計が有線通信、口頭の会話又は電子的通信の不正な傍受の目的のために主に有用であり、その装置又はその構成要素が郵送され、若しくは州際の若しくは外国との通商において輸送されたこと又はこれから郵送され、若しくは州際の若しくは外国との通商において輸送されることを知り、又は知っている理由がありながら、その装置を製造し、組み立て、所有し、又は売却すること。

(c) 新聞、雑誌、ちらしその他の印刷物に、次のいずれかの広告を、それが郵送され、又は州際の若しくは外国との通商において輸送されることを知り、又は知っている理由がありながら掲載すること。

(i) 電子的、機械的その他の装置の設計が有線通信、口頭の会話又は電子的通信の不正な傍受の目的のために主に有用であることを知り、又は知っている理由がある場合の、その広告

(ii) その他の電子的、機械的その他の装置の広告が、有線通信、口頭の会話又は電子的通信の不正な傍受の目的のための装置の利用を促進する場合の、その広告

(2) 次の者が、電子的、機械的その他の装置を、その設計が有線通信、口頭の会話又は電子的通信の不正な傍受の目的のために主に有用であること知り、又は知っている理由がありながら、郵送し、州際の若しくは外国との通商において送付し、若しくは運搬し、又は、製造し、組み立て、所有し、若しくは売却することは、この条により違法とはされない。

(a) 有線通信サービス又は電子的通信サービスを提供する通常の営業の過程における、有線通信サービス若しくは電子的通信サービスのプロバイダ、そのプロバイダの職員、代理人若しくは被用者又はそのプロバイダと契約関係にある者

(b) 連邦、州又はその行政的下部組織の通常の職務過程における、連邦、州若しくはその行政的下部組織の職員、代理人若しくは被用者又は連邦、州若しくはその行政的下部組織と契約関係にある者

(3) この条の第 1 項に定められた装置を売却するために広告することは、広告が、その装置を利用する正当な権限を有する有線通信サービス若しくは電子的通信サービスの国内プロバイダ又は連邦、州若しくはその行政的下部組織の代理人に対してのみ、郵送され、又は州際の若しくは外国との通商において送付され、若しくは運搬される場合には、この条により違法とはされない。

第 2513 条　有線通信、口頭の会話又は電子的通信を傍受する装置の没収

この章の第 2511 条又は第 2512 条に違反して、利用され、送付され、運搬され、製造され、組み立てられ、所有され、売却され、又は広告された電子的、機械的その他の装置は、合衆国に差し押さえられ、没収される。(1) 合衆国法典第 19 編に定める関税関連法に違反したことによる、船舶、車両、商品及び荷物の差押え、略式没収及び司法的没収並びに公用収用、(2) 船舶、車両、商品及び荷物の処分又はその売却の利益、(3) 没収の免除又は軽減、(4) 主張の譲歩、及び(5) 没収についての情報提供者への報償の付与、に関連するすべての法規定は、それが適用可能で、この条の規定と矛盾しないかぎりにおいて、この条の規定に基づき行われ、又は行われたと主張される差押え及び没収に適用される。ただし、合衆国法典第 19 編に定める関税関連法の規定に基づき、船舶、車両、商品及び荷物の差押え及び没収について税関長その他の者に課される職務が、この条に基づく電子的、機械的その他の傍受装置の差押さえ及び没収については、司法長官がそのために授権し、又は指名する職員、代理人その他の者により遂行される場合を除く。

第 2514 条　廃止

第 2515 条　傍受した有線通信又は口頭の会話の証拠利用の禁止

有線通信又は口頭の会話が傍受された場合に、その情報の開示がこの章に違反するときは、その通信の内容及びそれから派生する証拠を、合衆国、州若しくはその行政的下部組

織の法廷、大陪審、機関、職員、代理人、規制機関、議会の委員会又はその他の官署における公判、審理又は他の手続において、証拠として提出してはならない。

第 2516 条　有線通信、口頭の会話又は電子的通信の傍受のための権限

(1) 司法長官、司法次官、司法副次官又は司法長官により特別に指名された局長、局長代理、刑事局次長若しくは刑事局次長代理は、傍受が次の事項についての証拠を提供する可能性があり、又は実際に提供している場合には、連邦捜査局又は請求の対象となる犯罪の捜査に責任を有する連邦機関による有線通信又は口頭の会話の傍受を授権し、又は承認する命令を求めて管轄権を有する連邦裁判官に請求する権限を与えることができ、その裁判官はこの章の第 2518 条に従ってこの命令を発付することができる。

(a) 合衆国法典第 42 編第 2274 条から第 2277 条（1954 年原子力法の執行に関するもの）、合衆国法典第 42 編第 2284 条（原子力施設又は燃料の破壊活動に関するもの）又はこの編の第 37 章（諜報活動に関するもの）、第 90 章（通商の秘密の保護に関するもの）、第 105 章（破壊活動に関するもの）、第 115 章（反逆罪に関するもの）、第 102 章（騒憂罪に関するもの）、第 65 章（悪意の器物損壊に関するもの）、第 111 章（船舶の破壊に関するもの）若しくは第 81 章（海賊行為に関するもの）に基づく、死刑又は 1 年以上の拘禁刑に処せられる犯罪

(b) 合衆国法典第 29 編第 186 条若しくは第 501 条 c 項（労働組合に対する支払い及び融資の制限に関するもの）の違反又は謀殺、略取誘拐、強盗若しくは恐喝を含み、この編に基づき処罰できる犯罪

(c) この編の次の条に基づき処罰できる犯罪。第 201 条（公務員及び証人に対する賄賂）、第 215 条（銀行員の賄賂に関するもの）、第 224 条（スポーツ競技における賄賂）、第 844 条の d 項、e 項、f 項、g 項、h 項若しくは i 項（爆発物の違法な利用）、第 1032 条（資産隠匿に関するもの）、第 1084 条（賭博情報の伝達）、第 751 条（逃亡に関するもの）、第 1014 条（融資及び貸付の申請一般に関するもの；更新及び割引）、第 1503 条、第 1512 条及び第 1513 条（司法職員、陪審員若しくは証人に影響を与え、又は危害を与えること一般）、第 1510 条（犯罪捜査の妨害）、第 1511 条（州又は地方自治体の法執行の妨害）、第 1751 条（大統領及びそのスタッフの暗殺、略取誘拐及び脅迫）、第 1951 条（脅迫又は暴行による通商の妨害）、第 1952 条（ラケッティアリング活動を支援する州際の及び外国との移動又は輸送）、第 1958 条（雇われ殺人のための州際通商施設の利用に関するもの）、第 1959 条（ラケッティアリング活動を支援する暴力犯罪に関するもの）、第 1954 条（従業員福利制度の実施に影響を与えるための申込、承諾及び懇請）、第 1955 条（営業賭博の禁止）、第 1956 条（通貨代替物のロンダリング）、第 1957 条（特定の不法活動から派生する財産についての金融取引への従事に関するもの）、第 659 条（州際運搬物の窃取）、第 664 条（年金及び福祉基金からの横領）、第 1343 条（有線、無線又はテレビによる詐欺）、第 1344 条（銀行詐欺に関するもの）、第 2251 条及び第 2252 条（子どもの

性的搾取)、第 2312 条、第 2313 条、第 2314 条及び第 2315 条（盗品の州際輸送)、第 2321 条（特定の自動車又は自動車の部品の売買に関するもの)、第 1203 条（人質行為に関するもの)、第 1029 条（銀行口座等利用手段についての詐欺その他の行為に関するもの)、第 3146 条（出頭義務違反の罰則に関するもの)、第 3521 条 b 項(3)（証人の再配置及び支援に関するもの)、第 32 条（航空機又は航空施設の破壊に関するもの)、第 38 条（航空機部品の詐欺に関するもの)、第 1963 条（ラケッティアに影響され買収された組織（RICO）に関する違反)、第 115 条（連邦職員に対する脅迫又は報復に関するもの)、第 1341 条（郵便詐欺に関するもの)、第 1030 条（コンピュータ詐欺及びコンピュータ乱用に関するもの）の重罪にあたる違反、第 351 条（議員、閣僚又は最高裁判所裁判官の暗殺、略取誘拐及び脅迫に関する違反)、第 831 条（核物質を含む禁止された取引に関するもの)、第 33 条（自動車又は自動車施設の破壊に関するもの)、第 175 条（生物兵器に関するもの)、第 1992 条（列車破壊に関するもの)、第 1028 条（身元詐称文書の作成に関するもの）の重罪にあたる違反、第 1425 条（市民権又は国籍の違法な取得に関するもの)、第 1426 条（国籍証書又は市民権証書の複製に関するもの)、第 1427 条（国籍証書又は市民権証書の販売に関するもの)、第 1541 条（権限なくしてするパスポートの発行に関するもの)、第 1542 条（パスポート申請における虚偽申告に関するもの)、第 1543 条（パスポートの偽造又は不正使用に関するもの)、第 1544 条（パスポートの悪用に関するもの）又は第 1546 条（ビザ、許可証その他の文書の詐欺または悪用に関するもの）

(d) この編の第 471 条、第 472 条又は第 473 条に基づき処罰できる偽造を含む犯罪

(e) 第 11 編に基づく事件と関係のある詐欺又は合衆国の法律に基づき処罰できる麻薬、マリファナその他の危険な薬品の製造、輸入、受領、隠匿、購入、販売その他の取扱いを含む犯罪

(f) この編の第 892 条、第 893 条又は第 894 条に基づく恐喝的信用取引きを含む犯罪

(g) 合衆国法典第 31 編第 5322 条（通貨取引報告を扱うもの）の違反

(h) この編の第 2511 条及び第 2512 条（特定の通信の傍受及び開示並びに特定の傍受装置に関するもの）についての重罪にあたる違反

(i) この編の第 71 章（わいせつ罪に関するもの）の重罪にあたる違反

(j) 第 49 編の第 60123 条 b 項（天然ガスのパイプラインの破壊に関するもの）又は第 46502 条（ハイジャックに関するもの）の違反

(k) 第 22 編第 2778 条（武器輸出規制法に関するもの）の犯罪にあたる違反

(l) この条に記述された犯罪の裁きから逃亡している者の所在

(m) 移民及び国籍法の第 274 条、第 277 条又は第 278 条（外国人の密入国に関するもの）の違反

(n) 合衆国法典第 18 編第 922 条及び第 924 条（小火器に関するもの）の重罪にあたる違反

(o) 1986 年内国歳入法典第 5861 条（小火器に関するもの）の違反

(p) この編の第 1028 条（身元詐称文書の作成に関するもの)、第 1542 条（パスポート申請における虚偽申告に関するもの）若しくは第 1546 条（ビザ、許可証その他の文書の詐欺又は悪用に関するもの）の重罪にあたる違反又は移民及び国籍法の第 274 条、第 277 条若しくは第 278 条（外国人の密入国に関するもの）の違反

(q) 第 229 条（化学兵器に関するもの）又はこの編の第 2332 条、第 2332a 条、第 2332b 条、第 2332ｄ 条、第 2332f 条、第 2339A 条、第 2339B 条若しくは第 2339C 条（テロリズムに関するもの）の犯罪にあたる違反(r) この項のいずれかの規定に記述された犯罪の共同謀議

(2) 州又はその行政的下部組織の主たる検察官は、有線通信、口頭の会話又は電子的通信の傍受を授権し、又は承認する命令について管轄権を有する州裁判官に対して請求をする権限を州法により与えられている場合には、請求の対象とされる犯罪の捜査に責任を負う捜査官又は法執行官による有線通信、口頭の会話又は電子的通信の傍受を授権し、又は承認する命令を求めて州裁判官に請求することができ、その裁判官はこの章の第 2518 条及び適用される州法に従ってこの命令を発付することができる。ただし、その傍受により、傍受を授権する州法が指定する、1 年以上の拘禁刑に処せられる謀殺、略取誘拐、賭博、強盗、収賄、恐喝若しくは麻薬若しくはマリファナその他の危険な薬品の販売に関する犯罪若しくは生命、身体若しくは財産に危害を及ぼすその他の犯罪の遂行の証拠又は上記の犯罪の遂行のための共同謀議の証拠が提供される可能性があり、又は実際に提供される場

合にかぎる。

(3) 政府の代理人（この用語が、連邦刑事訴訟規則の目的のために定義されるところに従う。）は、その傍受が連邦法上の重罪の証拠を提供する可能性があり、又は実際に提供している場合には、請求の対象となる犯罪の捜査に責任を負う捜査官又は法執行官による電子的通信の傍受を授権し、又は承認する命令を求めて管轄権を有する連邦裁判官に請求する権限を与えることができ、その裁判官はこの編の第 2518 条に従ってこの命令を発付することができる。

第 2517 条　傍受された有線通信、口頭の会話又は電子的通信の開示及び利用のための権限

(1) この章により授権された方法で、有線通信、口頭の会話若しくは電子的通信の内容又はそれから派生する証拠を取得した捜査官又は法執行官は、開示を行い、又は開示を受ける職員の公的職務の適切な遂行に該当する範囲で、その内容を他の捜査官又は法執行官に開示することができる。

(2) この章により授権された方法で、有線通信、口頭の会話若しくは電子的通信の内容又はそれから派生する証拠を取得した捜査官又は法執行官は、その利用が公的職務の適切な遂行に該当する範囲で、その内容を利用することができる。

(3) この章により授権された方法で、この章の規定に従い傍受された有線通信、口頭の会話

若しくは電子的通信に関わる情報又はそれから派生する証拠を受領する者は、連邦、州又はその行政的下部組織の権限の下で行われる手続において、宣誓又は確約のうえで証言をするときは、通信の内容又はそれから派生する証拠を開示することができる。

(4) 別段の特権を与えられた有線通信、口頭の会話又は電子的通信は、この章の規定に基づき傍受されるか、又はこれに違反して傍受されるかを問わず、その特権的性格を失わない。

(5) ここに授権される方法により有線通信、口頭の会話又は電子的通信の傍受に従事する場合に、捜査官又は法執行官が、授権命令又は承認命令に特定される以外の犯罪に関連する有線通信、口頭の会話又は電子的通信を傍受するときは、その内容及びそれから派生する証拠は、この条の第１項及び第２項の定めに従い開示され、又は利用されることができる。その後の請求において、通信の内容がこの章の規定に従って別に傍受されたと管轄権を有する裁判官が認定する場合に、その裁判官が授権し、又は承認したときは、その通信の内容及びそれから派生する証拠をこの条の第３項に基づき利用することができる。この請求は、可能な限り速やかでなければならない。

(6) この章により授権された方法で、有線通信、口頭の会話及び電子的通信の内容又はそれから派生する証拠を取得した捜査官、法執行官又は政府の代理人は、その内容が外国情報若しくは防諜情報（1947 年国家安全保障法第３条に定めるもの）又は外国諜報情報（この編の第 2510 条第 19 項に定めるもの）を含むかぎりにおいて、情報を受領することになる職員の公的職務の遂行を支援するために、その内容を連邦の他の法執行官、諜報職員、保護職員、移民担当職員、国家防衛職員又は国家安全保障職員に対して開示することができる。この定めに従って情報を受領した連邦職員は、権限のない情報開示の制限に服しつつ、その職員の公的職務の遂行に必要なかぎりで情報を利用することができる。

第 2518 条　有線通信、口頭の会話又は電子的通信の傍受のための手続

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

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

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

(i) 行われた、行われつつあり、又は行われようとしている特定の犯罪の詳細

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

(iii) 傍受しようとする通信の種類の特定的記載

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

身元

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

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

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

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

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

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

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

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

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

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

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

(a) その通信が傍受される者の身元が分かるときは、その身元

(b) 傍受が授権された通信設備又は場所の性質及び所在地

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

(d) 通信の傍受を授権された機関及び請求の権限を与えた者の身元

(e) 傍受が授権される期間（記載された通信が最初に取得されたときに傍受が直ちに終了するべきか否かの陳述を含む。）

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

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

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

(7) この章の別段の定めに関わらず、次のことを合理的に認定する司法長官、司法次官、司法副次官又は州法に従って行動する州若しくはその行政的下部組織の主たる検察官により特別に指名された捜査官又は法執行官は、傍受が行われ、又は着手された時から 48 時

間以内に、傍受を承認する命令のための請求をこの条に従い行うことを条件として、有線通信、口頭の会話又は電子的通信の傍受を行うことができる。

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

(i) 人の死又は重大な身体的傷害の急迫の危険

(ii) 国家安全保障上の利益を脅かす共同謀議

(iii) 組織犯罪に特有の共同謀議

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

(8)(a) この章に基づいて授権された方法により傍受される有線通信、口頭の会話又は電子的通信の内容は、可能であれば、磁気テープ、電信その他類似の装置に記録される。この項に基づく有線通信、口頭の会話又は電子的通信の内容の記録は、記録を編集その他の改変から保護する方法で行われる。その記録は、命令期間の終了時又はその延長期間の終了時に、直ちに命令を発した裁判官に提出され、その指示により封印されなければならない。記録の保管は、裁判官が命じた場所で行われなければならない。記録は、命令を発付した裁判官又は請求を却下した裁判官の命令による場合を除き、破棄されてはならず、いかなる場合でも 10 年間は保管される。記録の複製は、捜査のために、この章の第 2517 条第 1 項及び第 2 項の規定に従って、利用又は開示のために作成することができる。この項により定められた封印の存在又はそれがないことの十分な説明が、第 2517 条第 3 項に定める、有線通信、口頭の会話若しくは電子的通信の内容又はそこから派生する証拠の利用又は開示の前提条件である。

(b) この章に基づいて行われた請求及び発付された命令は裁判官により封印されなければならない。請求及び命令の保管は、裁判官が指示した場所で行われなければならない。請求及び命令は、管轄権を有する裁判官の前で十分な根拠を示した場合にのみ開示され、命令を発付した裁判官又は請求を却下した裁判官の命令による場合を除き破棄されず、いかなる場合でも 10 年間は保管される。

(c) この項の規定の違反は、命令を発付した裁判官又は請求を却下した裁判官に対する侮辱として処罰することができる。

(d) 却下された第 2518 条第 7 項(b)に基づく承認の命令のための請求の提出時、命令期間の終了時又はその延長期間の終了時の後、90 日以内の相当の期間に、命令を発付した裁判官又は請求を却下した裁判官は、命令又は請求において指名された者及び裁判官が正義の実現のために裁量で決定することができる傍受された通信の他の当事者に対し、次

の通知を含む目録を提供しなければならない。

(1) 命令の発付又は請求の提出の事実

(2) 授権され、承認され、若しくは承認されなかった傍受の命令の発付の日付及びその傍受の期間又は請求の却下の日付

(3) その期間に有線通信、口頭の会話又は電子的通信が傍受されたか否かの事実裁判官は、申立てを受けて、正義の実現に資すると判断した場合には、裁量により、傍受された通信、請求及び命令の一部を、その者又はその代理人の閲覧に供することができる。管轄権を有する裁判官に対する、一方当事者による十分な理由の立証により、この項に基づいて要求される目録の提供を延期することができる。

(9) この章に基づき傍受される有線通信、口頭の会話若しくは電子的通信の内容又はそこから派生する証拠は、連邦又は州の裁判所の公判、審理その他の手続において、証拠として採用され、又は他の方法で開示されてはならない。ただし、各当事者が、公判、審理その他の手続の 10 日以上前に、それに基づいて傍受が授権され、又は承認された裁判所命令及びそれに付随する請求の写しを提供された場合には、この限りではない。公判、審理その他の手続の 10 日前に上記の情報を当事者に提供することが不可能であったこと及び当事者が情報を遅れて受領することにより不利益を被らないことを裁判官が認定した場合には、この 10 日の期間は要求されない。

(10)(a) 権利を侵害された者は、合衆国、州又はその行政的下部組織の法廷、大陪審、機関、職員、代理人、規制機関、議会の委員会又はその他の官署における公判、審理その他の手続において、この章に従い傍受された有線通信若しくは口頭の会話の内容又はそこから派生する証拠につき、次の根拠に基づく証拠排除の申立てをすることができる。

(i) 通信が違法に傍受されたこと。

(ii) 傍受の根拠となる授権命令又は承認命令が、文言上不十分であること。

(iii) 傍受が授権命令又は承認命令に従って行われていないこと。

この申立ては、申立てをする機会がない場合又は申立ての根拠をその者が認識していない場合を除き、公判、審理その他の手続においてなされる。申立てが承認された場合には、傍受された有線通信若しくは口頭の会話の内容又はそこから派生する証拠は、この章に違反して取得されたものとして扱われる。裁判官は、権利を侵害された者による申立てを受けて、正義の実現に資すると判断した場合には、裁量により、傍受された通信又はそこから派生する証拠の一部を、権利を侵害された者又はその代理人の閲覧に供することができる。

(b) 合衆国の代理人が、申立てを承認し、又は請求を却下した裁判官その他の職員に対し、訴えが遅延を目的としたものではないことを証明した場合には、合衆国は、その他の訴権に加え、この項の(a)に基づく証拠排除の申立てを承認する命令について、又は承認命令のための請求の却下について上訴する権利を有する。上訴は、命令が発付された日から 30 日以内に提起され、鋭意遂行される。

(c) 電子的通信の傍受についてこの章に定められる救済及び処罰は、その通信を含むこの章の憲法に関わらない違反に対する唯一の司法的救済及び処罰とする。

(11) 通信が傍受される設備又は場所の特定に関するこの条の第 1 項(b)(ii)及び第 3 項(d)の要求は、次の場合には適用されない。

(a) 次のすべての条件を満たす口頭の会話の傍受の請求の場合

(i) 請求が連邦の捜査官又は法執行官によるものであって、司法長官、司法次官、司法副次官、局長又は局長代理により承認されているとき

(ii) 請求がその特定が現実的でない理由についての完全な陳述を含み、犯罪を行い、その通信が傍受されようとしている者を特定しているとき

(iii) 裁判官がその特定を現実的ではないと判断したとき

(b) 次のすべての条件を満たす有線通信又は電子的通信の請求の場合

(i) 請求が連邦の捜査官又は法執行官によるものであって、司法長官、司法次官、司法副次官、局長又は局長代理により承認されているとき

(ii) 請求が、犯罪を行ったとみられ、その通信が傍受されようとしている者を特定し、かつ、請求者が、その者の行為が特定の設備からの傍受を妨げる効果を持っていたことを信ずる相当な理由の存在を立証するとき

(iii) 裁判官がその立証が適切になされたことを認定するとき

(iv) 傍受を授権し、又は承認する命令が、請求において特定された者が、通信が送信されようとしている、又は送信された機器の相当直近にいる、又はいたと考えることが相当である期間の傍受に限定されているとき

(12) この条の第 11 項(a)のために、第 1　項(b)(ii)及び第 3 項(d)の要件が適用されない場合の命令に基づく通信の傍受は、傍受命令を遂行する者により通信が傍受される場所が確定されるまでは開始されない。第 11 項(b)に定められた命令を受領した有線通信サービス又は電子的通信サービスのプロバイダは、傍受のための支援が適時に又は相当な方法で遂行できないという理由に基づき、裁判所に、命令を修正し、又は破棄するよう求める申立てをすることができる。裁判所は、政府に通知したうえで、申立てを迅速に処理しなければならない。

第 2519 条　傍受された有線通信、口頭の会話又は電子的通信に関する報告書

(1) 第 2518 条に基づき発された命令（又は、それぞれの命令の延長命令）の終了又は傍受を承認する命令の却下から 30 日以内に、命令を発した裁判官又は却下した裁判官は、合衆国裁判所事務局に対して、次の内容の報告書を提出する。

(a) 命令又は延長命令が請求された事実

(b) 請求された命令又は延長命令の種類（命令が、この編の第 2518 条第 11 項のために、この編の第 2518 条第 1 項(b)(ii)及び第 2518 条第 3 項(d)の要件を適用されないものであるか否かを含む）

(c) 命令又は延長命令が、請求されたとおりに承認され、修正され、又は却下された事実
(d) 命令により授権された傍受の期間並びに命令の延長の回数及び期間
(e) 命令、請求又は命令の延長命令に特定された犯罪
(f) 捜査又は法執行の職員及び機関であって当該の請求を行った請求者並びに請求の権限を与えた者の身元
(g) 通信が傍受される設備の種類又は場所

(2) 毎年１月には、司法長官、司法長官により特別に指名された局長又は州若しくはその行政的下部組織の主たる検察官は、合衆国裁判所事務局に次の内容の報告書を提出する。
(a) それに先立つ暦年において発された命令又は延長命令のためのそれぞれの請求について、この条の第１項(a)から(g)までの規定により要求される情報
(b) 次の内容を含む、命令又は延長命令に基づき行われる傍受の一般的記載
(i) 有罪判決を招くような傍受通信のおおよその性質及び頻度
(ii) その他の傍受通信のおおよその性質及び頻度
(iii) 通信が傍受された者のおおよその人数
(iv) 暗号に到達した命令の件数及びその暗号が命令に基づく傍受通信の簡単なテキストの法執行機関による取得を妨げたか否か
(v) 傍受に利用された人員その他の資源のおおよその性質、量及び費用
(c) 命令又は延長命令に基づいて行われる傍受の結果としての逮捕の件数及び逮捕の根拠となる犯罪
(d) 傍受の結果としての公判の数
(e) 傍受に関して行われた証拠排除の申立て件数及びそれが認められた件数又は却下された件数
(f) 傍受の結果として出された有罪判決の件数及び有罪判決の取得の根拠となる犯罪並びに傍受の重要性についての一般的な評価
(g) それに先立つ暦年において取得された命令又は延長命令に関して、この項の(b)から(f)までの規定により要求される情報

(3) 毎年４月に合衆国裁判所事務局長は、議会に対し、それに先立つ暦年において、この章に従って有線通信、口頭の会話又は電子的通信の傍受を授権し、又は承認する命令のための請求の件数及びこの章に従って発付され、又は却下された命令及び延長命令の件数についての完全な報告書を提出する。報告書は、この条の第１項及び第２項により事務局に提出することを要求されたデータの要約及び分析を含まなければならない。合衆国裁判所事務局長は、この条の第１項及び第２項により提出することが要求される報告書の内容及び形式について定める拘束力のある規則を発する権限を与えられる。

第 2520 条　民事損害の回復権限

(a) 一般規定

第 2511 条第 2 項(a)(ii)に定められる場合を除き、この章に違反してその有線通信、口頭の会話又は電子的通信が傍受され、開示され又は意図的に利用された者は、違反に関わった合衆国以外の人又は団体から、民事訴訟において適切な救済を得ることができる。

(b) 救済

この条に基づく訴訟においては、適切な救済は次のものを含む。

(1) 適切な暫定的救済、エクイティ上の救済又は宣言的救済

(2) c 項に基づく損害賠償及び適切な場合には懲罰的損害賠償

(3) 相当の弁護士費用その他の訴訟費用

(c) 損害賠償額の算定

(1) この条に基づく訴訟において、この章に違反する行為がスクランブル化若しくは暗号化されていない民間衛星画像通信の私的な鑑賞である場合又は通信がスクランブル化若しくは暗号化されていない連邦通信委員会の規則第 74 部 D 節に基づき割り当てられた周波数で送信される無線通信である場合に、その行為が不法の若しくは違法な目的のためではないとき若しくは直接的若しくは間接的な商業上の収益若しくは私的な商業上の利得を目的としないときには、裁判所は損害賠償額を次のように算定する。

(A) その行為を行う者が、以前には第 2511 条第 5 項に基づき差止めを命じられず、この条に基づく以前の民事訴訟でも責任を問われなかった場合には、裁判所は原告が被った実際の損害額の総計又は 50 ドル以上 500 ドル以下の制定法上の損害賠償額のいずれか大きい方の額で算定する。

(B) その行為を行う者が、以前に第 2511 条第 5 項に基づき差止めを命じられ、又はこの条に基づく民事訴訟で責任を問われた場合には、裁判所は原告が被った実際の損害額の総計又は 100 ドル以上 1000 ドル以下の制定法上の損害賠償額のいずれか大きい方の額で算定する。

(2) この条に基づくその他の訴訟においては、裁判所は損害賠償額を次のいずれか大きい方の額で算定する。

(A) 原告の被った実際の損害額及び違反者が違反の結果として得た利益の合計

(B) 違反した日 1 日あたり 100 ドル又は 1 万ドルのいずれか大きい方の制定法上の損害賠償額

(d) 抗弁

次のいずれかへの善意の信頼は、この章又は他の法律に基づき提起される民事訴訟又は刑事訴訟に対する完全な抗弁とされる。

(1) 裁判所の令状若しくは命令、大陪審の罰則付召喚令状、立法府の委任又は制定法上の委任

(2) この編の第 2518 条第 7 項に基づく捜査官又は法執行官の要求

(3) 訴えられた行為はこの編の第 2511 条第 3 項により許されるという善意の判断

(e) 公訴期限

この条に基づく民事訴訟は、権利主張者が違反を発見することが相当とされる機会を最初に得た日から２年を経過した後は、提起することができない。

(f) 行政上の懲戒

合衆国又はその省若しくは機関がこの章の規定に違反すると裁判所又は管轄の省若しくは機関が判断し、及び違反をとりまく状況から合衆国の職員又は被用者が意図的又は故意に違反したか否かについて重大な疑念があると裁判所又は管轄の省若しくは機関が認定したときは、その省又は機関は、裁判所又は管轄の省若しくは機関の判断及び認定についての真正な写しを受け取り次第、職員又は被用者に対する懲戒処分が正当化されるか否かを判断する手続を直ちに開始する。関与した省又は機関の長が、懲戒が正当化されないと判断した場合には、関係する省又は機関を管轄する監察総監に通知し、及び監察総監に対し、その判断の理由を提出しなければならない。

(g) 不適切な開示は違法とする第 2517 条により許可される範囲を越える情報を、捜査官、法執行官又は政府機関が、故意に開示し、又は利用することは、第 2520 条 a 項の目的上、この章の違反とされる。

第 2521 条　違法な傍受に対する差止命令

人がこの章に違反して重罪を構成し、又は重罪を構成することとなる行為に従事し、又はこれから従事しようとしていることが明らかに認められる場合には、司法長官はその違反の差止めを求めて連邦地方裁判所に対して民事訴訟を提起することができる。裁判所は、可能なかぎり速やかにその訴訟の審理を行い、判決を下さなければならず、終局判決の前のいかなる時点においても、訴訟の提起による保護の対象である合衆国、個人又は特定の階級に対する継続的及び実質的な権利侵害を阻止するために正当化される一方的緊急差止命令若しくは禁止命令を発し、又は他の措置をとることができる。この条に基づく手続には、連邦民事訴訟規則が適用される。ただし、正式起訴が被告敗訴で差し戻された場合には、証拠開示手続（discovery）には連邦刑事訴訟規則が適用される。

第 2522 条　法執行通信支援法の執行

(a) 監視命令を発する裁判所による執行

この章、州法若しくは 1978 年外国諜報監視法に基づいて傍受を授権する裁判所又は第 206 章若しくは州法に基づきペンレジスター若しくはトラップ・アンド・トレース装置の利用を授権する裁判所が、電気通信事業者が法執行通信支援法の要求に従っていないと認定した場合には、裁判所は、その法律の第 108 条に基づき、事業者に対して、直ちに従うよう指示し、及び、事業者に対する支援サービスのプロバイダ又は事業者の送信装置若しくは切替装置の製造者に対して、事業者がそれに従うために必要な改善を直ちに加えるよう指示することができる。

(b) 司法長官による請求を受けた執行司法長官は、管轄の連邦地方裁判所における民事訴訟

により、法執行通信支援法第 108 条に従い、電気通信事業者、電気通信の送信装置若しくは切替装置の製造者又は電気通信支援サービスのプロバイダに対し、その法律に従うように指示する命令を得ることができる。

(c) 民事罰

(1) 一般規定

この条に基づいて命令を発する裁判所は、電気通信事業者、電気通信の送信装置若しくは切替装置の製造者又は電気通信支援サービスのプロバイダに対し、命令の発付の日以降又は裁判所が特定する将来の日以降、違反した日 1 日あたり 1 万ドルを上限とする民事罰を科すことができる。

(2) 考慮事項

民事罰を科すか否かの決定及びその額の決定において、裁判所は次のことを考慮に入れなければならない。

(A) 違反の性質、状況及び程度

(B) 違反者の支払い能力、違反者の適時に従おうとする誠実な努力、違反者が営業を続ける能力への影響、過失の程度及び従うための努力が遅れている期間

(C) 正義が要求するその他のもの

(d) 定義

この条においては、法執行通信支援法の第 102 条に定義された用語は、それぞれ、その条に定められた意味を有する。

3-1-3　アメリカ合衆国法典集犯罪及び刑事手続第 1 部犯罪第 121 章蓄積された有線通信、電子的通信及び取引記録へのアクセス

出典：「米国愛国者法（反テロ法）（下）（執筆者：平野美惠子、土屋恵司、中川かおり）」『外国の立法』No.215, 2003 年 2 月, pp.37-47（第 2701 条～第 2712 条）＜http://www.ndl.go.jp/jp/data/publication/legis/215/21501.pdf＞
※注釈は省略している。

合衆国法典

第 18 編　犯罪及び刑事手続

第Ⅰ部　犯罪

第 121 章　蓄積された有線通信、電子的通信及び取引記録へのアクセス

U.S.C. TITLE 18. CRIMES AND CRIMINAL PROCEDURE

PART　I . CRIMES

CHAPTER 121. STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

(2002 年 7 月 24 日現在)

中川かおり訳

第 2701 条蓄積された通信への違法なアクセス

(a) 犯罪

この条の c 項に定められる場合を除き、次の者はこの条の b 項の定めに従い処罰される。

(1) 電子的通信サービスを提供する設備に権限なく意図的にアクセスする者

(2) その設備にアクセスする権限を意図的に越し、有線通信又は電子的通信がシステムに電子的に蓄積されている間のその通信に対する権限に基づくアクセスを取得し、改変し、又は妨害する者

(b) 罰則

この条の a 項に基づく犯罪の処罰は、次のとおりとする。

(1) 商業上の利益、悪意の破壊若しくは加害又は私的な商業上の利得のために犯罪が行われた場合には、

(A) この規定に基づく最初の犯罪の場合には、この編に基づく罰金若しくは 1 年以下の拘禁刑に処し、又はこれを併科する。

(B) この規定に基づく二度目以降の犯罪の場合には、この編に基づく罰金若しくは 2 年以下の拘禁刑に処し、又はこれを併科する。

(2) それ以外の場合には、この編に基づく罰金若しくは 6 月以下の拘禁刑に処し、又はこれを併科する。

(c) 除外

この条の a 項は、次のものにより授権された行為には適用されない。

(1) 有線通信サービス又は電子的通信サービスを提供する人又は団体

(2) サービスの利用者自身の通信又はその利用者宛ての通信について、その利用者

(3) この編の第 2703 条、第 2704 条又は第 2518 条

第 2702 条　顧客の通信又は記録の自発的開示

(a) 禁止

b 項に定める場合を除き、次のことを禁止する。

(1) 公衆に対し電子的通信サービスを提供する人又は団体が、サービスが電子的に蓄積されている期間に、通信の内容を、人又は団体に対し、意図的に漏示すること。

(2) 公衆に遠隔コンピュータ処理サービスを提供している人又は団体が、そのサービスにおいて次のように保持され、又は維持される通信内容を、人又は団体に対して意図的に漏示すること。

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

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

(3) 公衆に対する遠隔コンピュータ処理サービス又は電子的通信サービスのプロバイダが、そのサービスの受信契約者又は顧客に関する記録又は他の情報（ただし、(1)又は(2)の対象となる情報を含まない。）を政府の機関に対して意図的に漏示すること。

(b) 通信の開示の除外

a 項に記述されたプロバイダは、次のいずれかのときに通信の内容を漏示することができる。

(1) 通信の名宛人若しくは所定の受信者又はその名宛人若しくは所定の受信者の代理人に対するとき

(2) この編の第 2517 条、第 2511 条第 2 項(a)又は第 2703 条において別に授権されるとき

(3) 通信の発信者、名宛人若しくは所定の受信者の、又は遠隔コンピュータ処理サービスの場合には受信契約者の、法律に基づいた同意を得ているとき

(4) 通信を宛先に送信するために雇われた者、権限を与えられた者又はその設備が利用される者に対するとき

(5) サービスの提供又はサービスにおけるプロバイダの権利若しくは財産の保護に必然的に付随するとき

(6) 次に該当する場合に、法執行機関に対するとき

(A) 内容が次のものである場合

(i) サービス・プロバイダにより意図せずに取得され、かつ

(ii) 犯罪の遂行に関係することが明らかに認められる場合

(B) 1990 年犯罪規制法（Crime Control Act of 1990）第 227 条により要求される場合

(C) 人の死又は重大な身体的傷害の急迫の危険に関わる緊急事態のために、遅滞なく情報を開示することが要求されているとプロバイダが合理的に信ずる場合

(c) 顧客の記録の開示の除外

a 項に定められるプロバイダは、サービスの受信契約者又は顧客に関係する記録その他の情報（ただし、a 項(1)又は a 項(2)に定める通信の内容を除く。）を次のいずれかに従って漏示することができる

(1) 第 2703 条により別に権限を与えられるところに従うこと。

(2) 顧客又は受信契約者の法律に基づいた同意によること。

(3) サービスの提供又はサービスにおけるプロバイダの権利若しくは財産の保護に必然的に付随するところに従うこと。

(4) 人の死又は重大な身体的傷害の急迫の危険に関わる緊急事態のために、情報の開示が正当化されるとプロバイダが合理的に信ずる場合に、政府機関に対してすること。

(5) 政府機関以外の者に対してすること。

第 2703 条　顧客の通信又は記録の要求された開示

(a) 電子的に蓄積された有線通信又は電子的通信の内容

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

(b) 遠隔コンピュータ処理サービスにおける有線通信又は電子的通信の内容

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

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

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

(i) 連邦法若しくは州法により授権される行政上の罰則付召喚令状又は連邦若しくは州の大陪審若しくは公判の罰則付召喚令状を利用する場合(ii) この条の d 項に基づく開示のための裁判所命令を取得する場合

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

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

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

(c) 電子的通信サービス又は遠隔コンピュータ処理サービスに関する記録

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

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

(B) この条の d 項に基づく開示のための裁判所命令を取得した場合

(C) 開示について受信契約者又は顧客の同意を得ている場合

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

(E) (2)の規定に基づく情報を求める場合

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

(A) 氏名

(B) 住所

(C) 近距離及び長距離電話接続記録、又は通話の時間及び期間の記録

(D) （開始日を含む）サービスの期間及び利用されるサービスの種類

(E) 電話番号、機器番号又は暫定的に割り当てられたネットワーク・アドレスを含む受

信契約者の他の番号若しくはその識別子

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

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

(d) 裁判所命令の要件

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

(e) この章に基づき情報を開示するプロバイダに対する訴訟原因の不存在

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

(f) 証拠保存の要件

(1) 一般規定

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

(2) 保存期間

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

第 2704 条　バックアップ保存

(a) バックアップ保存

(1) 第 2703 条 b 項(2)に基づき活動する政府機関は、要求が向けられるサービス・プロバイダに対して、捜索されている電子的通信の内容のバックアップ・コピーを通信を保存するために作成する要求を、罰則付召喚令状又は裁判所命令に含めることができる。サービス・プロバイダは、その罰則付召喚令状又は裁判所命令について受信契約者又は顧客に通知することなく、通常の営業と両立して可能な範囲で迅速にバックアップ・コピーを作成し、政府機関に対し、バックアップ・コピーを作成したことを確認する。そう

したバックアップ・コピーは、サービス・プロバイダが罰則付召喚令状又は裁判所命令を受け取ってから 2 営業日以内に作成されなければならない。

(2) 受信契約者又は顧客に対する通知は、通知が第 2705 条 a 項に従って延期される場合を除き、政府機関により、上記確認を受けてから 3 日以内に行われなければならない。

(3) サービス・プロバイダは、次のいずれか遅い時点までは、バックアップ・コピーを破壊してはならない。

(A) 情報の送付

(B) 政府の罰則付召喚令状又は裁判所命令に関する手続（その上訴を含む。）の終結

(4) サービス・プロバイダは、次のいずれをも満たすときは、政府機関が受信契約者又は顧客に対して通知をしてから 14 日を経過した後は、要求する政府機関に対し、バックアップ・コピーを開示しなければならない。

(A) 受信契約者又は顧客が政府機関の要求に異議を申し立てたとの通知を、受信契約者又は顧客から受けていないこと。

(B) 政府機関の要求に異議の申立てをする手続を始めていないこと。

(5) 政府機関は、この編の第 2703 条に基づく罰則付召喚令状又は裁判所命令の存在の通知により、証拠が破壊され、又は改変される結果となる可能性を信ずることに理由があると単独の裁量で認定する場合には、この条の a 項(1)に基づくバックアップ・コピーの作成を要求することができる。

(b) 顧客の異議の申立て

(1) この条の a 項(2)に基づく受信契約者又は顧客に対する政府機関の通知から 14 日以内に、その受信契約者又は顧客は、罰則付召喚令状の破棄又は裁判所命令の取消しを求める申立てを、政府機関に写しを送達し、及びサービス・プロバイダに対し異議の申立てを書面により通知することで、行うことができる。裁判所命令の取消しを求める申立ては、その命令を発した裁判所に対して提起されなければならない。罰則付召喚令状の破棄を求める申立ては、管轄の連邦地方裁判所又は州裁判所に提起されなければならない。この申立て又は請求は、次のことを陳述する宣誓書又は宣誓供述書を含まなければならない。

(A) 請求者が、彼のために維持された電子的通信の内容が捜索されているサービスの受信契約者又は顧客であること。

(B) 捜索されている記録が正当な法執行調査に関係がないこと又は他の点においてこの章の規定に実質的に従っていないことを信ずる請求者の理由

(2) 顧客がこの章に従って受けた通知に特定された人、職又は部局に対し、書留郵便又は配達証明郵便により、書類の写しを送付し、又は郵送することで、この条に基づく政府機関への送達が行われる。この条の目的上、「送付（delivery）」は、連邦刑事訴訟規則に定められるのと同様の意味を有する。

(3) 顧客がこの項の(1)及び(2)の規定に従っていると認定する場合には、裁判所は、政府

機関に対して宣誓応答書（sworn response）の提出を命令しなければならない。政府機関がその応答書に非公開の審理を適当とする理由を含める場合には、この宣誓応答書は、非公開で提出することができる。裁判所が当事者の当初の主張及び応答に基づき、申立て又は請求について決定を下すことができない場合には、裁判所は適切と思料するところに従いさらに訴訟指揮を行うことができる。政府機関の応答書の提出の後は、すべての訴訟手続は、可能な限り速やかに終了し、申立て及び請求に対する決定が下されなければならない。

(4) 裁判所が、請求者を、政府機関が捜索している通信がそのために維持される受信契約者若しくは顧客ではないと認定する場合又は法執行調査が正当であること及び捜索される通信が調査に関連することを信ずる理由があると認定する場合には、裁判所は申立て又は請求を却下し、その手続の執行を命じなければならない。請求者が政府機関が捜索している通信がそのために維持される受信契約者若しくは顧客であること、捜索される通信が正当な法執行調査に関連すると信ずる理由がないこと又は捜査がこの章の規定に実質的に従っていないことを裁判所が認定した場合には、裁判所はその手続の破棄を命じなければならない。

(5) この条に基づき申立て又は請求を却下する裁判所命令は、終局命令とみなされてはならず、命令に対する顧客の中間上訴は認められない。

第 2705 条　通知の延期

(a) 通知の延期

(1) この編の第 2703 条 b 項に基づき活動する政府機関は、次のことをすることができる。

(A) 裁判所命令を求める場合には、裁判所が裁判所命令の存在を通知することがこの項の(2)に定める悪影響を及ぼすと信ずる理由があると認定するときは、請求に、この編の第 2703 条 b 項に基づき要求される通知を 90 日以内の期間延期する命令の要求（この要求に裁判所は応じなければならない）を含めること。

(B) 連邦法若しくは州法により授権される行政上の罰則付召喚令状又は連邦若しくは州の大陪審の罰則付召喚令状を取得する場合には、罰則付召喚令状の存在を通知することがこの項の(2)に定める悪影響を及ぼすと信ずる理由があるとする監督職員の書面による証明の執行を受けて、この編の第 2703 条 b 項に基づき要求される通知を 90 日以内の期間延期すること。

(2) この項の(1)の目的上、悪影響とは、次のものをいう。

(A) 個人の生命又は身体的安全を危険にさらすこと。

(B) 訴追を逃れること。

(C) 証拠の破壊又は改ざん

(D) 潜在的な証人への脅迫

(E) その他捜査を著しく危険にし、又は不当に公判を遅延させること。

(3) 政府機関は、(1)(B)に定める証明書の真正な写しを保存しなければならない。

(4) 第 2703 条に定められる通知の延期期間の延長は、請求を受けた裁判所により、又は証明を用いて政府機関により、1 度につき 90 日まで認められるが、この条の b 項に従う場合に限る。

(5) この項の(1)又は(4)に基づく通知の延期期間が終了したときは、政府機関は、顧客又は受信契約者に対し、次の内容を含む通知と共に召喚令状若しくは要求の写しを送達し、又は書留郵便若しくは第一種郵便で送付しなければならない。

(A) 法執行調査の性質について相当の特定性をもった陳述

(B) 顧客又は受信契約者への次の内容の告知

(i) 召喚令状又は要求に指定されるサービス・プロバイダにより顧客又は受信契約者のために維持される情報が政府機関に提供され、又は政府機関から要求されたこと及びその提供又は要求がなされた日付

(ii) 顧客又は受信契約者への通知が延期されたこと。

(iii) 延期が行われるための条件である証明又は認定についての政府機関又は裁判所の解釈

(iv) 延期を認めるこの章の規定

(6) この項で使用される「監督職員（supervisory official)」とは、主任捜査官、主任副捜査官若しくは捜査機関の本部若しくは支部の同等の者又は主たる検察官、主たる検察官の第一補佐若しくは検察の本部若しくは支部の同等の者をいう。

(b) 政府がアクセスする対象者への通知の除外第 2703 条に基づき活動する政府機関は、第 2703 条 b 項(1)に基づき顧客又は受信契約者に通知することが求められていない場合において、又はこの条の a 項に従って通知を延期できる限りにおいて、令状、罰則付召喚令状又は裁判所命令の名宛人とされる電子的通信サービスのプロバイダ又は遠隔コンピュータ処理サービスのプロバイダに対し、裁判所が適当と思料する期間、令状、罰則付召喚令状又は裁判所命令の存在を他の者に通知しないように命ずる命令を裁判所に要求することができる。裁判所は、令状、罰則付召喚令状又は裁判所命令の存在の通知が次の結果を引き起こすと信ずる理由があると認定する場合には、命令を発付しなければならない。

(1) 個人の生命又は身体的安全を危険にさらすこと。

(2) 訴追を逃れること。

(3) 証拠の破壊又は改ざん

(4) 潜在的な証人への脅迫

(5) その他捜査を著しく危険にし、又は不当に公判を遅延させること。

第 2706 条　費用の支出

(a) 支払い

c 項に別段の定めがある場合を除き、この編の第 2702 条、第 2703 条又は第 2704 条に基

づき通信、記録その他の情報の内容を取得する政府機関は、その情報を収集し、又は提供する人又は団体に対し、合理的に必要な費用及び情報を捜索し、収集し、再生し、又は供給するにあたり、直接に生ずる費用の償還のための料金を支払う。償還が可能な費用には、情報が蓄積される電子的通信サービス又は遠隔コンピュータ処理サービスの通常の作動の必要的中断のための費用を含む。

(b) 金額

a 項により定められる料金の額は、政府機関及び情報を提供する人若しくは団体の双方が合意した額とし、又は、合意を得られない場合には、情報の作成を求める命令を発した裁判所（若しくは、情報の作成を求めて発された裁判所命令がないときは、その情報に関する刑事訴追が行われる裁判所）により決定される。

(c) 除外

この条の a 項の要求は、この編の第 2703 条に基づいて取得される、通信についての一般通信事業者が維持する電話料金記録及び電話番号リストに関する記録その他の情報には適用されない。ただし、裁判所は、要求された情報が、性質上非常に大量であり、又は、プロバイダにその他の不当な負担を強いると認定する場合には、a 項に定める支払いを命ずることができる。

第 2707 条　民事訴訟

(a) 訴訟原因

第 2703 条 e 項に定める場合を除き、違反を構成する行為がそれと知りながら、又は意図して行われるこの章の違反により権利を侵害された電子的通信サービスのプロバイダ、受信契約者その他の者は、その違反に関わった合衆国以外の人又は団体から民事訴訟において適切な救済を受けることができる。

(b) 救済

この条に基づく民事訴訟においては、適切な救済は次のものを含む。

(1) 適切な暫定的救済、その他のエクイティ上の救済又は宣言的救済

(2) c 項に基づく損害賠償

(3) 相当の弁護士費用その他の相当の訴訟費用

(c) 損害賠償額

裁判所は、この条に基づく民事訴訟の損害賠償を、原告が被った実際の損害額及び違反者が違反の結果として得た利益を合計して算定することができるが、損害賠償を回復する権利がある者が受け取る額は、いかなる事件においても合計 1000 ドルを下回ってはならない。違反が、意図的に又は故意になされた場合には、裁判所は懲罰的損害賠償を算定できる。この条に基づく責任を執行する勝訴判決の場合には、裁判所は、その認定する相当の弁護士費用と合わせて、訴訟費用を算定することができる。

(d) 行政上の懲戒

合衆国又はその省若しくは機関がこの章の規定に違反すると裁判所又は管轄の省若しくは機関が判断し、及び違反をとりまく状況から合衆国の職員又は被用者が意図的に、又は故意に違反したか否かについて重大な疑念があると、裁判所又は管轄の省若しくは機関が認定したときは、その省又は機関は、裁判所又は管轄の省若しくは機関の判断及び認定についての真正な写しを受け取り次第、職員又は被用者に対する懲戒処分が正当化されるか否かを判断する手続を直ちに開始する。関与した省又は機関の長が、懲戒が正当化されないと判断した場合には、関係する省又は機関を管轄する監察総監に通知し、及び監察総監に対し、その判断の理由を提出しなければならない。

(e) 抗弁

次のいずれかへの善意の信頼は、この章又は他の法律に基づき提起される民事訴訟又は刑事訴訟に対する完全な抗弁とされる。

(1) 裁判所の令状若しくは命令、大陪審の罰則付召喚令状、立法府の委任又は制定法上の委任（この編の第 2703 条 f 項に基づく政府機関の要求を含む。）

(2) この編の第 2518 条第 7 項に基づく捜査官又は法執行官の要求

(3) 訴えられた行為はこの編の第 2511 条第 3 項により許されるという善意の判断

(f) 公訴期限

この条に基づく民事訴訟は、権利主張者が最初に違反を発見した日又は違反を発見することが相当とされる機会を得た日から 2 年を経過した後は、提起することができない。

(g) 不適切な開示

この編の第 2703 条に従い捜査官、法執行官若しくは政府機関が取得し、又はこの編の第 3123 条若しくは第 3125 条に従い設置された装置から取得された、合衆国法典第 5 編第 552a 条 a 項に定められる意味での「記録（record）」を故意に開示することは、開示を行う職員又は政府機関の公的な職務の適切な遂行において行われる開示ではない場合には、この章に違反する。この規定は、この章に基づく民事訴訟において、連邦、州若しくは地方自治体の機関又は原告が、公衆に対し、（この章に基づく民事手続又は行政手続の開始に先立ち）以前に法律に従って開示した情報には適用されない。

第 2708 条　救済の排除

この章に定められる救済及び処罰は、この章の憲法に関わらない違反に対する唯一の司法上の救済及び処罰とする。

第 2709 条　電話料金及び取引記録への防諜目的のアクセス

(a) 提供義務

有線通信サービス又は電子的通信サービスのプロバイダは、その管理し、又は保有する受信契約者の情報、電話料金記録の情報又は電子的通信取引記録を求めて、この条の b 項に基づいて連邦捜査局長官により行われる要求に従わなければならない。

(b) 必要な証明

連邦捜査局長官、長官の指名する連邦捜査局本部の次長以上の者又は長官の指名する連邦捜査局支部の主任特別捜査官は、次のことをすることができる。

(1) 長官（又はその指名する者）が、要求先の有線通信サービス又は電子的通信サービスのプロバイダに対し、捜索されている氏名、住所、サービスの期間及び電話料金記録が、国際テロリズム又は秘密諜報活動に対抗するための授権された捜査に関連することを書面により証明する場合に、人又は団体の氏名、住所、サービスの期間並びに近距離及び長距離の電話料金記録を要求すること。ただし、合衆国の人に対するこの捜査は、合衆国憲法第１修正により保護された活動のみに基づいては行われないことを条件とする。

(2) 長官（又はその指名する者）が、要求先の有線通信サービス又は電子的通信サービスのプロバイダに対し、捜索される情報が国際テロリズム又は秘密諜報活動に対抗するための授権された捜査に関連することを書面により証明する場合に、人又は団体の氏名、住所及びサービスの期間を要求すること。ただし、合衆国の人に対するこの捜査は、合衆国憲法第１修正により保護された活動のみに基づいて行われないことを条件とする。

(c) 特定の開示の禁止

有線通信サービス若しくは電子的通信サービスのプロバイダ又はその職員、被用者若しくは代理人は、連邦捜査局がこの条に基づく情報又は記録へのアクセスを試みていること、又はアクセスしたことを他の者に開示してはならない。

(d) 連邦捜査局による情報の提供（dissemination）

連邦捜査局は、連邦捜査局により行われる外国情報収集及び外国防諜捜査のために司法長官が承認したガイドラインの定めに従う場合にのみ、この条に基づき取得された情報及び記録を提供することができ、合衆国の機関に対しては、その情報がその機関に授権された職責に明確に関連する限りで提供することができる。

(e) 特定の立法府内組織への通知要求

連邦捜査局長官は半年に１度、下院の諜報活動に関する常任特別委員会及び上院の諜報活動に関する特別委員会並びに下院の司法委員会及び上院の司法委員会に対し、この条のｂ項に基づくすべての要求について、完全な報告を行う。

第 2710 条　ビデオテープのレンタル又は売買記録の不当な開示

―略―

第 2711 条 章の定義

この章において、次の用語が使用されるときは、当該の規定に定めるところによる。

(1) この編の第 2510 条に定義される用語は、それぞれ、その条においてその用語に付与される定義を持つ。

(2) 「遠隔コンピュータ処理サービス（remote computing service）」とは、電子的通信シ

ステムの手段によるコンピュータによる蓄積サービス又は処理サービスの公衆への提供をいう。

(3) 「管轄権を有する裁判所（court of competent jurisdiction)」とは、第 3127 条により与えられた意味を有し、定義された範囲内のいかなる連邦裁判所をも地理的な限定なく含む。

第 2712 条 合衆国に対する民事訴訟

(a) 一般規定

この編のこの章若しくは第 119 章又は 1978 年外国諜報監視法の第 106 条 a 項、第 305 条 a 項若しくは第 405 条 a 項の故意の違反により権利を侵害された者は、連邦地方裁判所において、合衆国に対して金銭的損害を回復するための訴訟を提起することができる。権利を侵害された者が、この編のこの章若しくは第 119 章又は上記の第 50 編の特定の規定に違反することの立証に成功した場合には、この訴訟において裁判所は次のものを損害として算定することができる。

(1) 実際の損害額と 1 万ドルのいずれか多い方の額

(2) 相当の訴訟費用

(b) 訴訟手続

(1) この条に基づく合衆国に対する訴訟は、合衆国法典第 28 編に定められた連邦不法行為請求権法（the Federal Tort Claims Act）の手続に基づき管轄の省又は機関に請求が提示された後に、初めて開始される。

(2) この条に基づき合衆国に対して訴訟を提起することは、請求権が生じてから 2 年以内に管轄の連邦機関に対して書面により提示されない場合又は提示を受けた機関による請求の最終的な否認の通知が配達証明郵便若しくは書留郵便により郵送された日から 6 月以内に訴訟が提起されない場合には、永久に禁止される。この請求権は、権利主張者が違反を発見する相当の機会を最初に得る日に生ずる。

(3) この条に基づく訴訟は、裁判所において陪審によらずに審理される。

(4) 法律の別段の定めに関わらず、1978 年外国諜報監視法の第 106 条 f 項、第 305 条 g 項又は第 405 条 f 項に定める手続が、この条により統制される証拠を審査するための排他的な手段とされなければならない。

(5) 関係する省又は機関は、この条に基づいて合衆国に対して裁定されたのと同一の金額を、関係する省又は機関の職務費用のために利用できる歳出、基金又は他の会計（ただし、その歳出、基金又は他の会計のうち連邦法の執行のために利用できる部分を除く。）から、合衆国法典第 31 編第 1304 条に定める基金に支出しなければならない。

(c) 行政上の懲戒

合衆国又はその省若しくは機関がこの章の規定に違反すると裁判所又は管轄の省若しくは機関が判断したとき、及び違反を取り巻く状況から合衆国の職員又は被用者が、意図的

に、又は故意に違反したか否かについて重大な疑念があると、裁判所又は管轄の省若しくは機関が認定したときは、その省又は機関は、裁判所又は管轄の省若しくは機関の判断及び認定についての真正な写しを受け取り次第、職員又は被用者に対する懲戒処分が正当化されるか否かを判断する手続を直ちに開始する。関与した省又は機関の長が、懲戒が正当化されないと判断した場合には、関係する省又は機関を管轄する監察総監に通知し、監察総監に対し、その判断の理由を提出しなければならない。

(d) 排他的救済

この項に基づく合衆国に対する訴訟は、この条の範囲内の請求については合衆国に対する排他的な救済とする。

(e) 訴訟手続の停止

(1) 合衆国の申立てを受けて、裁判所が民事上の証拠開示手続（civil discovery）につき、関係する捜査又は関係する刑事事件の訴追を行う政府の能力に悪影響を及ぼすと判断する場合には、裁判所はこの条に基づき開始された訴訟を停止する。この停止により、b 項(2)の公訴期限の進行は停止する。

(2) この項において、「関係する刑事事件（related criminal case）」及び「関係する捜査（related investigation）」の用語は、停止の要求がなされた時点又はそれに続く停止の解除の申立てがなされた時点で進行中の実際の訴追又は捜査をいう。捜査又は刑事事件がこの条に基づき提起された訴訟に関係するか否かを判断するにあたり、裁判所は、２つの訴訟手続に関係する当事者、証人、事実及び事情の類似性の程度を考慮する。ただし、一つ又はそれ以上の要因が同一であることは必要とされない。

(3) (1)に基づく停止を要求するにあたり、政府は、関係する捜査又は関係する刑事事件に悪影響を及ぼす可能性のある事柄の開示を回避するために、適切と思われる場合には、一方当事者により証拠を提出できる。政府が一方当事者による提出を行った場合には、原告は、一方当事者によらず裁判所に提出する機会を与えられ、及び裁判所は裁量によりいずれの当事者に対してもさらに情報を要求することができる。

3-1-4　米国愛国者法逐条解説（抄）

出典：「米国愛国者法逐条解説」「米国愛国者法（反テロ法）（上）（執筆者：平野美惠子、土屋恵司、中川かおり）」『外国の立法』No.214, 2002 年 11 月, pp.17-20（第 201 条～第 225 条）、pp.40-41（第 814 条、第 815 条）。
＜http://www.ndl.go.jp/jp/data/publication/legis/214/21401.pdf＞
※注釈は省略している。

米国愛国者法逐条解説

平野美惠子、土屋恵司、中川かおり

第 201 条　テロリズムに関連する有線通信、口頭の会話及び電子的通信を傍受する権限

有線通信、口頭の会話及び電子的通信の傍受のための犯罪リストに、化学兵器に関する犯罪や、テロリズムに関する犯罪を追加する。この規定は、2005 年 12 月 31 日に失効する。

第 202 条　コンピュータ詐欺及びコンピュータ濫用罪に関連する有線通信、口頭の会話及び電子的通信を傍受する権限

有線通信、口頭の会話及び電子的通信の傍受のための犯罪リストに、重罪にあたるコンピュータ詐欺及びコンピュータ濫用等を追加する。この規定は、2005 年 12 月 31 日に失効する。

第 203 条　犯罪捜査情報を共有する権限

法執行職員は、通信傍受又は大陪審により入手された外国諜報情報を、他の法執行職員、諜報職員、国家安全保障担当職員、国家防衛担当職員、移民担当職員等に対して、開示することができる。政府の代理人（an attorney for the government）は、大陪審による情報の開示の場合には、その後相当の期間内に、開示がなされたこと及び開示先の行政機関を裁判所に通知しなければならない。情報の開示を受けた者は、その情報を公的職務遂行に必要な限りで利用することができ、この制限外の情報の利用は処罰の対象となる。法執行職員が通信傍受により入手した外国諜報情報を共有する権限は、2005 年 12 月 31 日に失効する。

第 204 条　有線通信、口頭の会話及び電子的通信の傍受及び開示に対する制限からの諜報機関の除外の確認

外国諜報情報を収集する機関には、刑事捜査のための有線通信、口頭の会話及び電子的通信の傍受に適用される手続や制限は適用されない。この規定は、2005 年 12 月 31 日に失効する。

第 205 条　連邦捜査局による翻訳者の雇用

連邦捜査局（FBI）は、翻訳者を増員する権限を有する。司法長官は、FBI 及び司法省他部局のために働く翻訳者の総数を議会に報告しなければならない。

第 206 条　1978 年外国諜報監視法に基づく移動傍受の権限

FISA 捜査官は、裁判所が、被疑者の行動について従来型の監視を妨害するものであると認定するときは、移動傍受（roving wiretaps）を行うことができる。すなわち、捜査官は、電話機毎に裁判所命令を受けるのではなく、被疑者が利用するかもしれないあらゆる電話機を監視するための裁判所命令を入手できる。この規定は、2005 年 12 月 31 日に失効する。

第 207 条外国勢力のエージェントであって、合衆国の人ではない者に対する外国諜報監視法に基づく監視の期間

外国勢力のエージェントであって、合衆国の人ではない者（non-United States persons）を対象とした電子監視又は物理的捜索（physical search）のための FISA に基づく裁判所命令の期間を、90 日から 120 日に変更する。また、延長期間を 90 日以内から 1 年以内に変更する。さらに、通常の物理的捜索のための FISA に基づく裁判所命令の期間を、45 日から 90 日に変更する。この規定は、2005 年 12 月 31 日に失効する。

第 208 条　裁判官の任命

FISA 法廷のために任命される連邦地方裁判所の判事の数を 7 名から 11 名に増やす。そのうちの少なくとも 3 名がコロンビア特別区から 20 マイル以内に居住していなければならない。

第 209 条　令状によるボイスメールのメッセージの押収

捜査官は、これまで E メールに認められていたのと同等の範囲で、裁判所命令ではなく捜査令状によりボイスメールを入手できる。また、ボイスメールの入手のために、全国一円の単一捜査令状を得ることができる。さらに、プロバイダに対しボイスメールの作成を要請する場合にも、裁判所命令ではなく捜査令状で足りるとする。この規定は、2005 年 12 月 31 日に失効する。

第 210 条　電子的通信記録のための罰則付召喚令状の範囲

法執行機関が罰則付召喚令状（subpoena）に従って電子通信サービス・プロバイダから入手できる記録の範囲を拡大し、銀行口座番号又はクレジット・カード番号を含む支払いの手段及び方法の開示を求められるようにする。これまでは、法執行機関が入手できる記録は、受信契約者等の氏名、住所及び契約期間等に限られていた。

第 211 条　範囲の確認

ケーブル会社が電話会社又はインターネット・サービス・プロバイダとして行動する場合には、電話会社又はインターネット・サービス・プロバイダに適用される有線通信及び電子的通信の傍受及び開示を規制する法律に従うことを確認する。ただし、受信契約者がどの番組を選択したかについて開示することは明示的に禁止される。

第 212 条　生命及び身体を保護するための電子的通信の緊急開示

電子通信サービス・プロバイダは、人の死又は身体の重大な傷害の急迫の危険が存在すると信ずる場合には、政府機関に対し、受信契約者等の電子的通信について開示することができる。政府機関の側から、裁判所命令又は捜査令状に基づき、プロバイダに対して受信契約者等の情報の開示を請求することもできる。この規定は、2005 年 12 月 31 日に失効する。

第 213 条　令状執行通知を延期する権限

裁判所が、予め通知することが捜査に対して悪い影響を与えると認める場合には、捜査官は、裁判所命令又は令状の執行を直ちに通知することなく被疑者の財産等について捜査を行うことができる。捜査官が裁判所に対し、差押えの相当の必要性を示すことができない場合には、令状を財産又は電子的情報を入手するために利用することはできない。また、個人は、捜査が行われてから「合理的な期間内」に通知を受けなければならない。

第 214 条　外国諜報監視法に基づくペンレジスター及びトラップ・アンド・トレースの権限

FISA に基づき、捜査官がペンレジスター及びトラップ・アンド・トレースを行う場合には、裁判所に対し、通信傍受が、合衆国の人に関わらない外国諜報情報を入手するためであるか、又は、国際テロや秘密諜報活動に対抗する捜査のためであることを示さなければならない。合衆国の人に対する FISA に基づく捜査は、合衆国憲法第 1 修正により保護される自由な言論活動のみを根拠として行ってはならない。この規定は、2005 年 12 月 31 日に失効する。

第 215 条　外国諜報監視法に基づく記録及び他の情報の入手

FISA に基づき、捜査官が業務記録を裁判所命令により入手する場合には、裁判所に対し、記録の入手が、国際テロや秘密諜報活動に対抗する捜査のためであることを示さなければならない。合衆国の人に対する FISA に基づく捜査は、合衆国憲法第 1 修正により保護される自由な言論活動のみを根拠として行ってはならない。この規定は、2005 年 12 月 31 日に失効する。

第 216 条　ペンレジスター及びトラップ・アンド・トレース装置の利用権限の修正

裁判所は、全国一円で有効なペンレジスター及びトラップ・アンド・トレース装置の設置のための命令を出すことができる。この条は、ペンレジスターやトラップ・アンド・トレース装置が、電話線以外（たとえばインターネットによる）の通信にも適用されることを保障している。ただし、内容の傍受までは許されない。さらに、行政機関に対し、ペンレジスターやトラップ・アンド・トレース装置が通信の内容を傍受することのないことを保障するために最新の技術を利用することも要求した。カーニボーのような装置の利用については、事後に裁判所へ報告書を提出することを定めた。

第 217 条　不正アクセス者の行う通信の傍受

コンピュータ・サービス・プロバイダが、不正アクセス者による攻撃の被害を受けていると考える場合には、不正アクセス者を法律に基づいて監視することができる。コンピュータの不正アクセス者とは、保護されたコンピュータに権限なくアクセスするため、保護されたコンピュータとの通信においてプライバシーを保証されない者である。保護されたコンピュータの全部又は一部に対してアクセスするために、所有者又は管理者と契約関係を有する者は含まれない。この規定は、2005 年 12 月 31 日に失効する。

第 218 条　外国諜報情報

FISA に基づいて外国諜報情報を入手するには、これまではそれが捜査の「目的」であることが必要とされていた。この要件を緩和し、「重要な目的の一つ」であればよいとする。すなわち、別に主たる目的がある場合にも FISA に基づき外国諜報情報を入手できる。この規定は、2005 年 12 月 31 日に失効する。

第 219 条　テロリズムのための単一管轄の捜査令状

テロ捜査に関する令状は、テロに関係する活動が行われた可能性のあるどの地域においても入手でき、その令状は全国一円で執行することができる。

第 220 条　電子監視のための捜査令状の全国的発付

捜査対象となる犯罪を管轄する裁判所は、プロバイダの住所地の裁判所の介入を求めることなく、政府がプロバイダ等から電子的通信を入手するための捜査令状を発する権限を有する。この規定は、2005 年 12 月 31 日に失効する。

第 221 条　貿易制裁

大統領はタリバンに対する農産物、薬品又は医療機器の輸出を、単独で制限する権限を有する。

第 222 条　捜査機関への支援

この法律は、電子通信サービスプロバイダに追加の技術的要求を課すものではない。第 216 条に従い装置や技術支援を提供したプロバイダは、その経費を相当の額で補償される。

第223条　　権限に基づかない特定の開示に対する民事責任

入手した情報を権限なく開示することを含む、合衆国法典第 18 編に定められた電子監視手続の違反又は FISA の特定の条項の違反について、合衆国政府は民事責任を問われる。裁判所が、開示が違法であることを認めた場合には、政府に対し、最低 1 万ドルの罰金と訴訟費用が科される。こうした事件については、陪審審理は認められない。また、行政機関は、違法な情報の開示を行った職員に対する行政懲戒処分を検討しなければならない。この規定は、2005 年 12 月 31 日に失効する。

第 224 条　時限規定

この章の第 203 条 a 項、第 203 条 c 項、第 205 条、第 208 条、第 210 条、第 211 条、第 213 条、第 219 条、第 221 条及び第 222 条以外の規定は、2005 年 12 月 31 日に失効する。ただし、失効の日以前に、外国諜報活動の捜査が開始されていたとき、又は、犯罪が行われていたときには、その限りでこの章の規定は効力を失わない。

第 225 条　外国諜報監視法の通信傍受規定に従う者の免責

FISA に従い、情報、設備又は技術支援を提供したプロバイダが責任を問われることはない。

第 814 条サイバーテロリズムの阻止及び予防

コンピュータに関連した詐欺及び関連の行為に関する規定の一部を改正し、コンピュータ不正アクセスの刑法上の禁止規定を明確化した。
その主なものは、次のとおりである。
(1) 合衆国の国外にあるコンピュータを使って、合衆国における州際の若しくは外国との通商又は通信に影響を与えることを犯罪とする。
(2) 「損失（loss)」の定義を改め、コンピュータ不正アクセス犯罪の犠牲者の負担が完全に考慮されることが確実になるものとした。
(3) 民事責任の範囲を明確化した。
(4) 連邦の量刑基準を改正し、これまである事件については裁量の余地なく適用されることとされていた最短期間の拘禁刑の規定があっても、裁量により、適切な刑罰が科せられるようにした。

第 815 条　政府の要求に応じてした記録の保存に関する民事訴訟に対する抗弁の追加

蓄積保存された有線及び電子通信並びに暫定的記録のアクセスに係わる民事訴訟に関する規定に基づき政府が行った要請を善意で信頼した者は、その要請を受けてした記録保存が違法行為であるとして訴えられた場合に、善意の信頼に基づくことをもって抗弁とすることができるとした。

3-1-5　2002 年連邦情報セキュリティ管理法

原文：http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
（仮訳）

2002 年連邦情報セキュリティ管理法
Federal Information Security Management Act of 2002（FISMA）

III 編―　情報セキュリティ

第 301 条　情報セキュリティ

(a)　略称―　本編は、「2002 年連邦情報セキュリティ管理法」と称することができる。

(b)　情報セキュリティ―

(1) 総則―　合衆国法典第 44 編の 35 章の末尾に、以下の新しい副章を追加する。

III 副章―情報セキュリティ

第 3541 条　目的

本副章の目的は、以下のとおりである。

(1) 連邦の業務及び資産をサポートする情報資源に対する情報セキュリティ統制の有効性を確保するための包括的な枠組みを提供する。

(2) 現在の連邦のコンピューティング環境の高度にネットワーク化された性質を認識し、関連する情報セキュリティ・リスクに関する政府全体にわたる効果的な管理及び監督を提供する。これには、民間セクター、国家安全保障部門、及び司法部門にわたる情報セキュリティ活動の調整が含まれる。

(3) 連邦の情報及び情報システムを保護するために必要な最小限の統制の策定及び維持について規定する。

(4) 連邦機関の情報セキュリティ・プログラムの監督を向上させるためのメカニズムを提供する。

(5) 商業的に開発された情報セキュリティ製品が、民間セクターが設計、構築、及び運用する、国防及び国家経済安全保障にとって重要な情報インフラストラクチャの保護のための市場ソリューションを反映して、先進的、動的、堅固、及び効果的な情報セキュリティ・ソリューションを提供することを確認する。

(6) 特定の技術的なハードウエア及びソフトウエアの情報セキュリティ・ソリューションの選定は、商業的に開発された製品の中から個々の機関に委ねられるべきであることを認識する。

第 3542 条　定義

(a) 総則―　(b)項に定めるものを除き、本副章には 3502 条による定義が適用されるものと

する。

(b) 追加の定義―　本副章において、以下の用語は以下の意味を有するものとする。

(1) 「情報セキュリティ」とは、以下のものを提供するために、情報及び情報システムを無権限のアクセス、使用、開示、中断、改ざん、又は損壊から保護することを意味する。

(A) 完全性。完全性とは、不適切な情報の改ざん又は損壊から保護することを意味し、これには情報の否認不可能性及び真正性を確保することが含まれる。

(B) 機密性。機密性とは、アクセス及び開示に対する許可された制限を保持することを意味し、これには個人のプライバシー及び所有権情報を保護するための手段が含まれる。

(C) 可用性。可用性とは、適時、かつ、信頼性のある、情報へのアクセス及び使用を確保することを意味する。

(2)

(A) 「国家安全保障システム」とは、機関によって、又は機関の請負業者若しくは機関を代理するその他の組織によって使用又は運用される情報システム(電気通信システムを含む)であって、以下のいずれかに該当するものを意味する。

(i) その機能、運用、又は使用が以下のいずれかに該当するもの。

(I) 諜報活動に関与するもの。

(II) 国家安全保障に関連する暗号活動に関与するもの。

(III) 軍隊の指揮統制に関与するもの。

(IV) 兵器若しくは兵器システムの不可欠の一部である機器に関与するもの。

(V) (B)副号に定めるものに従い、軍事上若しくは諜報上の使命を直接遂行するために重要であるもの。

(ii) 大統領命令若しくは議会制定法によって確立された基準のもとで、国防又は外交政策上の利益のために機密扱いとされるべきものとして具体的に許可された情報のために確立された手順によって常に保護されているもの。

(B) (A)副号(i)(V)には、日常的な管理及び取引のアプリケーション(給与、財務、物流、及び人事管理のアプリケーションを含む)のために使用されるシステムは含まれない。

(3) 「情報技術」とは、第 40 編の 11101 条で定める意味を有する。

第 3543 条　長官の権限及び役割

(a) 総則―　長官は、以下を含む、機関の情報セキュリティポリシー及び実践の監督を行わなければならない。

(1) 情報セキュリティポリシー、原則、基準、及びガイドラインを策定し、その実施を監督する。これには、機関が第 40 編の 11331 条に基づき公布された基準を適時に導入し、これを遵守することを確実にすることを通じた監督が含まれる。

(2) 機関に、当該 11331 条に基づき公布された基準及び本副章の要件に従って、以下のい

ずれかのものへの無権限のアクセス、使用、開示、中断、改ざん、又は損壊の結果として生じる被害のリスク及び大きさに応じた情報セキュリティ保護を特定及び提供するよう義務付ける。

(A) 機関自身若しくはその代理者によって収集又は保持される情報。

(B) 機関によって、又は機関の請負業者若しくは機関を代理するその他の組織によって、使用若しくは運用される情報システム。

(3) 国家安全保障システムを運用している、又はこれに対する管理権を行使している機関及び官庁(国家安全保障局を含む)との間で、国立標準技術研究所法(15 U.S.C. 278g-3)の20 条に基づく基準及びガイドラインの策定を調整して、実現可能な最大限の程度まで、当該基準及びガイドラインが、国家安全保障システムのために策定された基準及びガイドラインに対して補完的なものとなることを確実にする。

(4) 第 40 編の 11303 条に基づいて許可された行為を通じての監督を含め、機関による本副章の要件の遵守を監督し、当該要件の遵守に関する説明責任を課す。

(5) 少なくとも年に 1 回、3544 条(b)に基づき義務付けられている、機関の情報セキュリティ・プログラムについてレビューを行い、承認又は不承認の決定を下す。

(6) 関連する情報資源管理に関する方針及び手順との間で、情報セキュリティポリシー及び手順の調整を行う。

(7) 3546 条に基づき義務付けられている、連邦の情報セキュリティ・インシデント・センターの運用を監督する。

(8) 議会に対し、毎年 3 月 1 日までに、機関による本副章の要件の遵守状況について、以下の事項を含む報告を行う。

(A) 3545 条によって義務付けられている評価の結果得られた所見の概要。

(B) 国立標準技術研究所法(15 U.S.C. 278g-3)の 20 条に基づき策定され、第 40 編の 11331 条に基づき公布された基準の策定、公布、及び導入、ならびにその遵守の査定。

(C) 機関の情報セキュリティ慣行における、重大な不備。

(D) 当該不備に対処するために計画されている是正措置。

(E) 国立標準技術研究所法(15 U.S.C. 278g-3)の 20 条(d)項(10)号に基づき国立標準技術研究所によって作成された報告書の概要、及びこれに対する長官の見解。

(b) 国家安全保障システム― (a)項の(4)号及び(8)号に定める権限を除き、本条に基づく長官の権限は、国家安全保障システムには適用されないものとする。

(c) 国防総省及び中央情報局のシステム―

(1)(a)項の(1)号及び(2)号に定める長官の権限は、(2)号に定めるシステムについては国防長官に、(3)号に定めるシステムについては中央情報局長官に委譲されるものとする。

(2) 本号に定めるシステムとは、国防総省、国防総省の請負業者、又は国防総省を代理するその他の者によって運用されているシステムであって、無権限のアクセス、使用、開示、中断、改ざん、又は損壊が起こった場合に国防総省の任務に悪影響を及ぼすであろ

う情報を処理するものをいう。

(3) 本項に定めるシステムとは、中央情報局、中央情報局の請負業者、又は中央情報局を代理するその他の者によって運用されているシステムであって、無権限のアクセス、使用、開示、中断、改ざん、又は損壊が起こった場合に中央情報局の任務に悪影響を及ぼすであろう情報を処理するものをいう。

第 3544 条　連邦機関の責任

(a) 総則―　各機関の長は、以下の義務を負う。

(1) 以下のことについて責任を負う。

(A) 以下のいずれかのものへの無権限のアクセス、使用、開示、中断、改ざん、又は損壊の結果として生じる被害のリスク及び大きさに応じた情報セキュリティ保護を提供すること。

(i) 機関自身若しくはその代理者によって収集又は保持される情報。

(ii) 機関によって、又は機関の請負業者若しくは機関を代理するその他の組織によって、使用若しくは運用される情報システム。

(B) 本副章、ならびに以下のものを含む、関連する方針、手順、基準、及びガイドラインの要件を遵守すること。

(i) 第 40 編の 11331 条に基づき公布された情報セキュリティ基準。

(ii) 法律及び大統領指令に従って発行された、国家安全保障システムのための情報セキュリティに関する基準及びガイドライン。

(C) 情報セキュリティ管理プロセスが、機関の戦略上及び運用上の計画プロセスと統合されていることを確実にすること。

(2) 機関の上級職員が、これには、以下のことを通じての提供を含め、自己の管理下にある業務及び資産をサポートする情報及び情報システムのための情報セキュリティを提供することを確実にする。

(A) 当該情報又は情報システムへの無権限のアクセス、使用、開示、中断、改ざん、又は損壊の結果として生じるおそれのある被害のリスク及び大きさを査定すること。

(B) 第 40 編の 11331 条に基づき公布された基準に従って、情報セキュリティ分類及び関連要件のために、当該情報及び情報システムを保護するために適切な情報セキュリティのレベルを決定すること。

(C) 費用効率に優れた方法でリスクを許容可能なレベルにまで軽減するための方針及び手順を導入すること。

(D) 情報セキュリティ統制及び手法の定期的なテスト及び評価を行って、それらが効果的に実施されていることを確実にすること。

(3) 3506 条に基づき確立された機関の最高情報責任者(又は当該条の対象となっていない機関については、これに相当する役職者)に、本副章に基づき機関に課された要件の遵守

を確実にする権限を委譲する。これには、以下のことが含まれる。

(A) 機関の上級情報セキュリティ責任者を任命すること。上級情報セキュリティ責任者は、以下の条件を満たさなければならない。

(i) 本条に基づく最高情報責任者の責任を実行すること。

(ii) 本条に定める役割を管理するために必要な教育及び経験を含む、職業上の適格性を有すること。

(iii) 情報セキュリティに関する職務を主要な職務とすること

(iv) 機関による本条の遵守を確実にすることを支援する任務及び資源を備えた部署を統率すること。

(B) (b)項によって義務付けられている、機関全体にわたる情報セキュリティ・プログラムを策定及び保持すること。

(C) 本編の 3543 条及び第 40 編の 11331 条に基づき発行されたものを含む、適用されるすべての要件に対処するための、情報セキュリティポリシー、手順、及び統制手法を策定及び保持すること。

(D) 情報セキュリティについて重要な責任を負っている人員を、当該責任について教育及び監督すること。

(E) (2)号に基づく責任に関して、機関の上級職員を支援すること。

(4) 機関が、機関による本副章の要件ならびに関連する方針、手順、基準、及びガイドラインの遵守を支援するために十分な、教育を受けた人員を擁していることを確実にする。

(5) 機関の最高情報責任者が、機関の他の上級職員と連携して、機関の長に対し年に 1 回、是正措置の進捗状況を含め、機関の情報セキュリティ・プログラムの有効性について報告を行うことを確実にする。

(b) 機関のプログラム―各機関は、3543 条(a)項(5)号に基づき長官の承認を受けた、機関の業務及び資産をサポートする情報及び情報システム(別の機関、請負業者、又はその他の提供元によって提供又は管理されるものを含む)のための情報セキュリティを提供する、機関全体にわたる情報セキュリティ・プログラムを策定、文書化、及び実行しなければならない。当該情報セキュリティ・プログラムには、以下のものが含まれる。

(1) 機関の業務及び資産をサポートする情報及び情報システムへの無権限アクセス、使用、開示、中断、改ざん、又は損壊の結果として生じるおそれのある被害のリスク及び大きさの定期的な査定。

(2) 以下のすべての条件を備えた方針及び手順。

(A) (1)項によって義務付けられているリスク査定に基づいていること。

(B) 費用効率に優れた方法で、情報セキュリティのリスクを許容可能なレベルにまで軽減するものであること。

(C) 各機関の情報システムのライフ・サイクル全体を通じて情報セキュリティへの対処がなされることを確実にするものであること。

(D) 以下のものの遵守を確実にするものであること。

(i) 本副章の要件。

(ii) 長官が定める方針及び手順、ならびに第 40 編の 11331 条に基づき公布された情報セキュリティ基準。

(iii) 機関が決定する、許容可能な最低限のシステム構成要件。

(iv) 法律及び大統領指令に従って発行された、国家安全保障システムのための基準及びガイドラインを含む、適用されるその他のあらゆる要件。

(3) 状況に応じてネットワーク、施設、及びシステム又は情報システム・グループに対する、十分な情報セキュリティを提供するための下位計画。

(4) 人員(請負業者、ならびに機関の業務及び資産をサポートする情報システムのその他のユーザを含む)に、以下のことを周知するセキュリティ意識向上教育。

(A) それらの人員の活動に伴う情報セキュリティのリスク。

(B) それらの人員がこれらのリスクを軽減するための方針及び手順を遵守する責任。

(5) リスクに応じた頻度で、ただし年に 1 回を下回らない頻度で実施すべき、情報セキュリティポリシー、手順、及び実践の有効性の定期的なテスト及び評価。当該テストには、以下の規定が適用される。

(A) 3505 条(c)項に基づき義務付けられている資産目録で特定されたすべての情報システムの管理上、運用上、及び技術上の統制のテストを含めなければならない。

(B) 3545 条に基づく評価において使用されるテストを含めることができる。

(6) 機関の情報セキュリティポリシー、手順、及び実践の不備に対処するための、是正措置の計画、実施、評価、及び文書化のためのプロセス。

(7) 3546 条(b)項に基づき発行された基準及びガイドラインに従った、セキュリティ・インシデントの検出、報告、及び対処のための手順。これには、以下のことが含まれる。

(A) 重大な損害が発生する前に、当該インシデントに伴うリスクを緩和すること。

(B) 3546 条参照による連邦情報セキュリティ・インシデント・センターに通知及び相談すること。

(C) 状況に応じて、以下の相手に通知及び相談すること。

(i) 司法機関及び関連する監察長官。

(ii) 国家安全保障システムに関係するインシデントについては、大統領が指定した官庁。

(iii) 法律又は大統領指令に従った、その他の機関又は官庁。

(8) 機関の業務及び資産をサポートする情報システムのための業務の継続性を確保する計画及び手順。

(c) 機関による報告―各機関は、以下のことを行わなければならない。

(1) 年に 1 回、長官、下院の政府改革委員会及び科学委員会、上院の政府活動委員会及び商業・科学・交通委員会、議会の適切な許可及び予算割当に関する委員会、ならびに会

計検査院長官に対し、情報セキュリティポリシー、手順、及び実践の十分性及び有効性、ならびに本副章の要件の遵守状況((b)項の各要件の遵守状況を含む)について報告を行う。

(2) 以下のことに関連する計画書及び報告書において、情報セキュリティポリシー、手順、及び実践の十分性及び有効性について記述する。

(A) 機関の年次予算。

(B) 本章の副章 1 に基づく情報資源管理。

(C) 第 40 編の III 副編に基づく情報技術管理。

(D) 第 31 編の 1105 条及び 1115 条から 1119 条まで、ならびに第 39 編の 2801 条及び 2805 条に基づくプログラムの遂行状況。

(E) 第 31 編の 9 章ならびに 1990 年最高財務責任者法(31 U.S.C. 501 注記、公法 101-576)(及び同法によりなされた改正)に基づく財務管理。

(F) 連邦財務管理改善法(31 U.S.C. 3512 注記)に基づく財務管理システム。

(G) 第 31 編の 3512 条(通称「連邦管理者財務保全法」)に基づく会計及び管理上の内部統制。

(3) (1)号又は(2)号に基づき検出された方針、手順、又は慣行における重大な不備を、以下の規定に従って報告しなければならない。

(A) 第 31 編の 3512 条に基づく報告において、重大な欠陥として。

(B) 財務管理システムに関連する場合には、連邦財務管理改善法(31 U.S.C. 3512 注記)に基づく、重大な遵守の欠如の事例として。

(d) 遂行計画—

(1) (c)項の要件に加えて、各機関は、長官と協議の上、第 31 編の 1115 条に基づき義務付けられている遂行計画の一部として、以下の記述を含めなければならない。

(A) 期間。

(B) (b)項に基づき義務付けられているプログラムの実施に必要な資源(予算、人員、及び教育を含む)。

(2) (1)号に基づく記述は、(b)項(2)号(1)に基づき義務付けられているリスク査定に基づくものでなければならない。

(e) 公告及び意見募集—各機関は、情報セキュリティポリシー及び手順の案について、当該方針及び手順が国民とのコミュニケーションに影響を及ぼす限りにおいて、国民に対し適時に告知し、意見を述べる機会を与えなければならない。

第 3545 条　独立した年次評価

(a) 総則—

(1) 各機関は毎年、当該機関の情報セキュリティ・プログラム及び慣行の有効性を判定すべく、当該プログラム及び慣行について、独立した評価を実施させなければならない。

(2) 本条に基づく評価には毎回、以下のことを含めなければならない。

(A) 機関の情報システムの全体を反映したサブセットの情報セキュリティポリシー、手順、及び実践の有効性のテスト。

(B) 以下のものの遵守状況の査定(テストの結果に基づいて行う)。

(i) 本副章の要件。

(ii) 関連する情報セキュリティポリシー、手順、基準、及びガイドライン。

(C) 国家安全保障システムに関連する情報セキュリティについては、状況に応じて、別個の発表。

(b) 独立した監査人―(c)項が適用される場合に従い、監査人については以下の規定が適用されるものとする。

(1) 1978 年監察長官法に基づき監察長官が任命されている各機関については、本条によって義務付けられている年次評価は、機関の監察長官の決定に従い、監察長官又は独立した外部監査人が行わなければならない。

(2) (1)項に該当しない各機関については、機関の長が、評価を実施する独立した外部監査人を任命しなければならない。

(c) 国家安全保障システム―国家安全保障システムを運用している、又はこれに対する管理権を行使している各機関については、本条によって義務付けられている評価のうち、直接国家安全保障システムに関連する部分は、以下の規定に従って行うものとする。

(1) 機関の長が指定した者のみが行う。

(2) リスクに応じて、適用されるすべての法律に従って、当該システムにおける情報セキュリティ脆弱性を伴う情報のための適切な保護を確実にするような態様で行う。

(d) 既存の評価―本条によって義務付けられている評価は、その全部又は一部を、該当する機関のプログラム又は慣行に関連する別の監査、評価、又は報告に基づくことができる。

(e) 機関による報告―

(1) 各機関の長は、毎年、長官が定める日までに、本条に基づき義務付けられている評価の結果を長官に提出しなければならない。

(2) 本条に基づき義務付けられている評価が、国家安全保障システムに直接関連するものである場合には、長官に提出する評価結果は、評価のうち、国家安全保障システムに直接関連する部分の概要及び査定のみが含まれるものでなければならない。

(f) 情報の保護― 機関及び評価者は、開示された場合に情報セキュリティに悪影響を及ぼす可能性のある情報の保護を確実にすべく適切な措置を講じなければならない。当該保護は、リスクに応じたものとし、適用されるすべての法律及び規則に準拠したものでなければならない。

(g) 議会への OMB 報告―

(1) 長官は、第 3543 条(a)項(8)号に基づき義務付けられている議会への報告書において、本条に基づき実施された評価の結果の概要を報告しなければならない。

(2) 本条に基づく議会への長官の報告書では、国家安全保障システムに関連する情報セキ

ュリティに関する情報の概要を、当該システムにおける情報セキュリティ脆弱性を伴う情報の適切な保護が確保されるような態様で、リスクに応じて、適用されるすべての法律に従って記述しなければならない。

(3) 中央情報局長官の権限及び管理の下にある情報システム、又は国防長官の権限及び管理の下にある国家外交諜報プログラム・システムに関する評価及びその他の記述は、適用される法律に従い、議会の適切な監督委員会を通じてのみ、議会に提供されるものとする。

(h) 会計検査院長官―会計検査院長官は、以下のことについて、定期的に評価を行って議会に報告しなければならない。

(1) 機関の情報セキュリティポリシー及び実践の適切性及び有効性。

(2) 本副章の要件の実施状況。

第 3546 条　連邦情報セキュリティ・インシデント・センター

(a) 総則―　長官は、連邦中央情報セキュリティ・インシデント・センターの業務が、以下の任務を果たすことを確実にしなければならない。

(1) 機関の情報システムの運用者に、セキュリティ・インシデントに関する適時の技術的支援を提供すること。これには、情報セキュリティ・インシデントの検出及び対処に関する指針が含まれる。

(2) 情報セキュリティを脅かすインシデントに関する情報を収集して分析すること。

(3) 機関の情報システムの運用者に、実際に発生した最新の、及び潜在的な情報セキュリティの脅威、ならびに脆弱性に関する情報を伝達すること。

(4) 情報セキュリティ・インシデント及び関連事項について、国立標準技術研究所、国家安全保障システムを運用している、又はこれに対する管理権を行使している機関又は官庁(国家安全保障局を含む)、及び法律又は大統領指令により指定されたその他の機関又は官庁に相談すること。

(b) 国家安全保障システム―　国家安全保障システムを運用している、又はこれに対する管理権を行使している各機関は、法律及び大統領指令に従って発行された国家安全保障システムのための基準及びガイドラインに従う範囲内で、連邦情報セキュリティ・インシデント・センターとの間で、情報セキュリティ・インシデント、脅威、及び脆弱性に関する情報を共有しなければならない。

第 3547 条　国家安全保障システム

国家安全保障システムを運用している、又はこれに対する管理権を行使している各機関の長は、機関が以下のことを行うことを確実にする責任を負うものとする。

(1) 当該システムに格納されている情報への無権限のアクセス、使用、開示、中断、改ざん、又は損壊の結果として生じる被害のリスク及び大きさに応じた情報セキュリティ保

護を提供すること。
(2) 法律及び大統領指令に従って発行された、国家安全保障システムのための基準及びガイドラインによって義務付けられている情報セキュリティポリシー及び実践を導入すること。
(3) 本副章の要件を遵守すること。

第 3548 条　予算割当の許可
本副章の規定を履行するために、2003 年度から 2007 年度までの各年度について、必要な金額の予算を割り当てることが許可されている。

第 3549 条　既存の法律に対する影響
本副章、第 40 編の第 11331 条、又は国立標準技術研究所法(15 U.S.C. 278g-3)の第 20 条のいかなる規定も、第 5 編の第 552a 条に基づく個人のプライバシーの保護、第 5 編の第 552 条に基づく情報の開示、第 44 編の 29 章、31 章、若しくは 33 章に基づく記録の管理及び処分、本編の 35 章の副章 I に基づく情報資源の管理、又は米国の議会若しくは会計検査院長官への情報の開示に関するものを含め、情報の許可された使用又は開示について、大統領、行政管理予算局若しくはその長官、国立標準技術研究所、又はいかなる機関の長の権限にも影響するものと解釈することはできない。本副章が効力を有する間は、本章の副章 II は適用されないものとする。
(2) 記述上の変更―　当該 35 章の冒頭の条目次の末尾に、以下の事項を追加する。
副章 III―情報セキュリティ

条
3541　目的
3542　定義
3543　長官の権限及び役割
3544　連邦機関の責任
3545　独立した年次評価
3546　連邦情報セキュリティ・インシデント・センター
3547　国家安全保障システム
3548　予算割当の許可
3549　既存の法律に対する影響
(c) 特定の機関の、情報セキュリティに関する責任
(1) 国家安全保障に関する責任―
(A) 本法(同法によりなされた改正を含む)におけるいかなる規定も、法律及び大統領指令により許可された、合衆国法典第 44 編の 3542 条(b)項(2)号の定義による、国家安全

保障システムの運用、統制、又は管理に関する、国防長官、中央情報局長官、又はその他の機関の長のいかなる権限にも取って代わるものではない。

(B) 合衆国法典第 10 編の 2224 条を、以下のとおり改正する。

(i) (b)項において、「(b) 目的及び最小要件−(1)」を削除し、「(b) プログラムの目的−」を挿入する。

(ii) (b) 項において、(2)号を削除する。

(iii) (c) 項における、(1)号の直前の項目において、「インフラストラクチャ」の後に、「これには、第 44 編の 35 章の副章 III の遵守を通じて行うことも含まれる」を挿入する。

(2) 1954 年原子力法―本法のいかなる規定も、1954 年原子力法(42 U.S.C. 2011 以下)によって、又はこれに基づいて定められた要件に取って代わるものではない。機密データ、又は過去に機密指定を受けていたデータについては、1954 年原子力法(42 U.S.C. 2011 以下)に従って、取り扱い、保護、分類、重要度の引き下げ、及び機密指定の解除を行うものとする。

第 302 条　情報技術の管理

(a) 総則―合衆国法典第 40 編の 11331 条は、以下のとおり読み替える。

第 11331 条　連邦情報システム基準に関する責任

(a) 基準及びガイドライン―

(1) 規定する権限―　(2)号に定める場合を除き、商務長官は、国立標準技術研究所法(15 U.S.C. 278g-3(a)) 20 条(a)項の(2)号及び(3)号により国立標準技術研究所によって策定された基準及びガイドラインに基づき、連邦情報システムに関する基準及びガイドラインを規定しなければならない。

(2) 国家安全保障システム―国家安全保障システム(本条の定義による)のための基準及びガイドラインは、別途法律及び大統領指令による許可に従って、策定、規定、執行、及び監督するものとする。

(b) 強制要件―

(1) 強制要件とする権限―(2)号に定める場合を除き、商務長官は、 (a)項(1)号に基づき規定された基準を、連邦情報システムの運用効率又はセキュリティを向上させるために商務長官が必要と判断する範囲内で、強制的で拘束力を持つものとしなければならない。

(2) 強制要件とすべき基準―

(A) (a)項(1)号に基づき規定された基準には、以下の条件を満たす情報セキュリティ基準を含めなければならない。

(i) 国立標準技術研究所法(15 U.S.C. 278g-3(b))の 20 条(b)項に基づき決定された、最低限の情報セキュリティ要件を満たすものであること。

(ii) その他、連邦の情報及び情報システムのセキュリティを向上させるために必要なものであること。

(B) (A)号参照による情報セキュリティ基準は、強制的で拘束力を持つものとしなければならない。

(c) 否認又は修正する権限― 大統領は、否認又は修正することが公共の利益に帰すると判断した場合には、(a)項(1)号参照による基準及びガイドラインを否認又は修正することができる。基準及びガイドラインを否認又は修正する大統領の権限は、委譲することができない。当該否認又は修正の告知は、速やかに官報に掲載されるものとする。商務長官は、当該否認又は修正の告知を受けてから直ちに、大統領の指令に従って、当該基準又はガイドラインを撤回又は修正しなければならない。

(d) 権限の行使― 財政上及び政策上の一貫性を確保するため、商務長官は、本条により付与された権限を、大統領の指令に従って、かつ、行政管理予算局の長官との調整のもとで行使しなければならない。

(e) より厳格な基準の適用―執行機関の長は、当該機関の監督内又は監督下にある情報システムのための費用効率に優れた情報セキュリティのための、本条に基づき商務長官が規定する基準より厳格な基準が、以下のすべての条件を満たす場合には、その厳格な基準を採用することができる。

(1) 少なくとも、商務長官によって強制的で拘束力を持つものとされている、適用される基準を含んでいる。

(2) その他、第 44 編の 3543 条に基づき発行された方針及びガイドラインに準拠している。

(f) 基準の公布に関する決定―本条に基づく基準の公布に関する商務長官の決定は、国立標準技術研究所法(15 U.S.C. 278g-3)の 20 条の定めに従い、国立標準技術研究所から商務長官に基準案が提出されてから 6 か月以内に行わなければならない。

(g) 定義―本条において、以下の用語は以下の意味を有するものとする。

(1) 連邦情報システム― 「連邦情報システム」とは、執行機関によって、又は執行機関の請負業者若しくは執行機関を代理するその他の組織によって、使用又は運用される情報システムを意味する。

(2) 情報セキュリティ― 「情報セキュリティ」とは、第 44 編の 3542 条(b)項(1)号に定める意味を有する。

(3) 国家安全保障システム―「国家安全保障システム」とは、第 44 編の 3542 節(b)項(2)号に定める意味を有する。」

(b) 記述上の変更―本編の 113 章の冒頭の条文の目次のうち 11331 条に関連する項目を、以下のとおり読み替える。

「11331 連邦情報システム基準に関する責任」

第 303 条　国立標準技術研究所

国立標準技術研究所法(15 U.S.C. 278g-3)の 20 条において、本文を削除し、以下の文言を挿入する。

(a) 総則―

国立標準技術研究所は、

(1) 情報システムのための基準、ガイドライン、ならびに関連する方法及び手法を策定する任務を有するものとする。

(2) 機関によって、又は機関の請負業者若しくは機関を代理するその他の組織によって使用又は運用される、国家安全保障システム(合衆国法典第 44 編の 3542 条(b)項(2)号の定義による)以外の情報システムに関する、基準及びガイドライン(最低要件を含む)を策定しなければならない。

(3) すべての機関の業務及び資産に十分な情報セキュリティを提供するための基準及びガイドライン(最低要件を含む)を策定しなければならない。ただし、当該基準及びガイドラインは、国家安全保障システムには適用されないものとする。

(b) 基準及びガイドラインの最低要件―　(a)項により義務付けられている基準及びガイドラインには、少なくとも以下のすべてを含めなければならない。

(1)

(A) リスク・レベルの範囲に応じた適切な情報セキュリティ・レベルを提供するという目的に基づき、各機関又はその代理者によって収集又は維持されているすべての情報及び情報システムをカテゴリーに分類するためにすべての機関が使用するべき基準。

(B) 各当該カテゴリーに含めるべき情報及び情報システムの種類を推奨するガイドライン。

(C) 各当該カテゴリーに分類された情報及び情報システムに適用される、情報セキュリティの最低要件。

(2) 情報セキュリティ・インシデントの検出及び対処についての定義及びガイドライン。

(3) 法律及び大統領指令に従って発行された、国家安全保障システムに関する適用される要件に従って、情報システムを国家安全保障システムとして特定するために、国防総省(国家安全保障局を含む)と連携して策定されたガイドライン。

(c) 基準及びガイドラインの策定―(a)項及び(b)項により義務付けられている基準及びガイドラインの策定にあたり、国立標準技術研究所は、以下のことを行わなければならない。

(1) 他の機関及び官庁ならびに民間セクター(行政管理予算局の長官、国防総省及びエネルギー省、国家安全保障局、会計検査院、ならびに国土安全保障長官を含む)と相談して、以下のことを確実にする。

(A) 情報セキュリティを向上させ、不要で費用のかかる重複作業を回避するための、情報セキュリティに関する適切な方針、手順、及び手法が使用されること。

(B) 当該基準及びガイドラインが、国家安全保障システム及び当該システム内に格納さ

れた情報の保護のために採用されている基準及びガイドラインに対して補完的なものとなること。

(2) 基準及びガイドラインの案について、国民に意見を述べる機会を与える。

(3) 以下のものを、以下の期限内に、合衆国法典第 40 編の 11331 条に基づく公布のために、商務長官に提出する。

(A) (b)項(1)号(A)に基づき義務付けられている基準を、本条の制定日から 12 か月以内に発行する。

(B)(b) 項(1)号(C)に基づき義務付けられている、各カテゴリーに適用される情報セキュリティの最低要件を、本条の制定日から 36 か月以内に発行する。

(4) (b) 項(1)号(B)に基づき義務付けられているガイドラインを、本条の制定日から 18 か月以内に発行する。

(5) 現実的に可能な最大限の範囲内において、当該基準及びガイドラインが、特定の製品(特定のハードウエア又はソフトウエアを含む)の使用又は調達を義務付けるものでないことを確実にする。

(6) 現実的に可能な最大限の範囲内において、当該基準及びガイドラインが、特定された情報セキュリティ・リスクに相当するレベルの保護を提供する代替ソリューションを認める十分な柔軟性を持ったものであることを確実にする。

(7) 現実的に可能な最大限の範囲内において、商業的に開発された市販の情報セキュリティ製品の使用を認める、成果主義に基づく柔軟な基準及びガイドラインを使用する。

(d) 情報セキュリティに関する役割―国立標準技術研究所は、以下のことを行わなければならない。

(1)

(a) 号に基づき策定した基準を、これを強制的で拘束力を持つべきものとするべき範囲の推奨事項とともに、合衆国法典第 40 編の 11331 条に基づく公布のために、商務長官に提出する。

(2) 要請に応じて、以下のことに関する技術支援を機関に提供する。

(A) (a) 項に基づき策定された基準及びガイドラインの遵守。

(B) 情報セキュリティ・インシデントの検出及び対処。

(C) 情報セキュリティポリシー、手順、及び慣行。

(3) 必要に応じて、情報セキュリティの脆弱性の性質及び程度、ならびに費用効率に優れた情報セキュリティを実現するための手法を判定するための調査を実施する。

(4) 機関の情報セキュリティポリシー及び実践に関する、実績指標及び測定　基準を策定し、定期的に改訂する。

(5) 民間セクターの情報セキュリティポリシー及び実践、ならびに商業的に利用可能な情報技術を評価して、機関が情報セキュリティの強化ためにこれらを採用すべき可能性について査定する。

(6) 要求に応じて、本条に基づく活動の結果の使用及び応用について民間セクターを支援する。

(7) 国家安全保障システムのために策定された、セキュリティに関する方針及び慣行を評価して、機関が情報セキュリティの強化ためにこれらを採用すべき可能性について査定する。

(8) 本条に基づき策定された基準及びガイドラインの有効性を定期的に査定して、状況に応じて改訂を行う。

(9) (a) 項に基づき策定された基準及びガイドラインについて、21 条によって設置された情報セキュリティとプライバシーに関する顧問委員会に対し、推奨事項を諮問して、これを検討し、当該推奨事項を、商務長官に提出した当該基準とともに、商務長官に提出する。

(10) 前年度に行われた活動についての年次公開報告書を作成し、本条に基づく責任を遂行するための翌年度の計画を策定する。

(e) 定義―本条において、以下の用語は以下の意味を有するものとする。

(1) 「機関」とは、合衆国法典第 44 編の 3502 条(1)号に定める意味を有する。

(2) 「情報セキュリティ」とは、本編の 3542 条(b)項(1)号に定める意味を有する。

(3) 「情報システム」とは、本編の 3502 条(8)号に定める意味を有する。

(4) 「情報技術」とは、合衆国法典第 40 編の 11101 条に定める意味を有する。

(5) 「国家安全保障システム」とは、合衆国法典第 44 編の 3542 条(b)項(2)号に定める意味を有する。

(f) 予算割当の許可― 国立標準技術研究所が本条の規定を履行するために、2003 年度、2004 年度、2005 年度、2006 年度、及び 2007 年度の各年度についてそれぞれ 20,000,000 ドルを、商務長官に割り当てることが許可されている。

304 条 情報セキュリティとプライバシーに関する顧問委員会

国立標準技術研究所法(15 U.S.C. 278g-4)の 21 条を、以下のとおり改正する。

(1) (a) 項において、「コンピュータ・システムのセキュリティとプライバシーに関する顧問委員会」を削除し、「情報セキュリティとプライバシーに関する顧問委員会」を挿入する。

(2) (a)項(1)号において、「コンピュータ又は電気通信」を削除し、「情報技術」を挿入する。

(3) (a)項(2)号を以下のとおり改正する。

(A) 「コンピュータ又は電気通信技術」を削除し、「情報技術」を挿入する。

(B) 「コンピュータ又は電気通信機器」を削除し、「情報技術」を挿入する。

(4) (a)項(3)号を以下のとおり改正する。

(A) 「コンピュータ・システム」を削除し、「情報システム」を挿入する。

(B) 「コンピュータ・システム・セキュリティ」を削除し、「情報セキュリティ」を挿

入する。
(5) (b)項(1)号において、「コンピュータ・システム・セキュリティ」を削除し、「情報セキュリティ」を挿入する。
(6) (b)項において、(2)号を削除し、以下の文言を挿入する。
「(2) 国立標準技術研究所、商務長官、及び行政管理予算局の長官に対し、連邦政府の情報システムに関連する情報セキュリティ及びプライバシーの問題についての助言を行う。これには、20 条に基づき策定された基準及びガイドラインの案のレビューを通じての助言が含まれる。」
(7) (b)項(3)号において、「報告」の後に「年に 1 回」を追加する。
(8) (e)項の後に以下の新しい項を挿入する。
「(f) 顧問委員会は、委員会の過半数の賛成によって決定した地域、場所、及び日時において、会議を開催するものとする。」
(9) (f)項及び(g)項をそれぞれ(g)項及び(h)項とする。
(10) (9)項により変更後の(h)項を削除し、以下の文言を挿入する。
h) 本条において、「情報システム」及び「情報技術」とは、20 条に定める意味を有する。

第 305 条　技術的及び適合上の変更
(a) コンピュータ・セキュリティ法―合衆国法第 40 編の 11332 条、及び当該編の 113 章の条目次における当該条に関連する項目を廃止する。
(b) 2001 年度 Floyd D. Spence 国防認可法―2001 年度 Floyd D. Spence 国防認可法(Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001)(公法 106-398)において、1062 条(44 U.S.C. 3531 注記)を削除する。
(c) 文書業務削減法―
(1) 合衆国法典第 44 編の 3504 条(g)項を以下のとおり改正する。
(A) (1)項の末尾に「及び」を追加する。
(B) (2)項を以下のとおり改正する。
(i) 「第 40 編の 11331 条ならびに 11332 条(b)項及び(c)項」を削除し、「第 40 編の 11331 条及び本章の副章 II」を挿入する。
(ii) 「、及び」を削除し、句点を挿入する。
(C) (3)号を削除する。
(2) 当該編の 3505 条の末尾に以下の文言を追加する。
(c) 主要な情報システムの資産目録―(1) 各機関の長は、当該機関が運用する、又は当該機関の管理下にある主要な情報システム(主要な国家安全保障システムを含む)の資産目録を作成及び保持しなければならない。
(2) 本項に基づく資産目録における情報システムの識別情報には、各当該システムとその他のすべてのシステム又はネットワーク(当該機関が運用するのではない、又は当該機関

の管理下にあるのではないものを含む)の間のインタフェースの識別情報を含めなければならない。

(3) 当該資産目録は、以下のすべての条件を満たさなければならない

(A) 少なくとも年に1回、更新されること。

(B) 会計検査院長官に提供されること。

(C) 以下を含む情報資源管理のサポートに使用されること。

(i) 3506条(b)項(4)号に基づく情報資源の資産目録の作成及び保持。

(ii) 3506条(h)項、第40編の副章III、ならびに関連する法律及び指針に基づく情報技術の計画、予算管理、調達、及び管理。

(iii) 副章IIに基づく情報セキュリティ統制の監視、テスト、及び評価。

(iv) 合衆国法典第5編の552条(g)に基づき義務付けられている、主要な情報システムの索引の作成。

(v) 21章、29章、31章及び33章に基づく記録管理に必要な情報システムの資産目録の作成。

(4) 長官は、本項の要件の導入についての指針を発行し、これを監督しなければならない。

(3) 本編の3506条(g)項を以下のとおり改正する。

(A) (1)項の末尾に「及び」を追加する。

(B) (2)項を以下のとおり改正する。

(i) 「第40編の11332条」を削除し、「本章の副章II」を挿入する。

(ii)「、及び」を削除し、句点を挿入する。

(C) (3)号を削除する。

IV編― 予算割当の許可及び施行日

第401条 予算割当の許可

I編又はII編(当該編によりなされた改正を含む)において予算割当の許可について具体的に定めのある目的を除き、2003年度から2007年度までの各年度について、I編及びII編を履行するために必要な金額の予算を割り当てることが許可されている。

第402条 施行日

(a) I編及びII編―

(1) 総則― (2)号に定める場合を除き、I編及びII編ならびに本編によってなされた改正は、本法の制定日から120日後より施行されるものとする。

(2) 即時施行― 207条、214条、及び215条は、本法の制定日より施行されるものとする。

3-1-6　2002 年国土安全保障法（抄）

出典：「米国における 2002 年国土安全保障法の制定（執筆者：土屋恵司）」
『外国の立法』No.222, 2004 年 11 月, pp.42-44（第 221 条～第 225 条）
＜http://www.ndl.go.jp/jp/data/publication/legis/222/022201.pdf＞

2002 年国土安全保障法［抄］

Homeland Security Act of 2002
（Public Law No.107-296, Nov.25, 2002, 116STAT. 2135）
［extracted］

調査及び立法考査局英米法研究会訳

第Ⅱ編　情報分析及び基盤防護
C 部　情報セキュリティ

第 221 条　情報共有のための手続

長官は、この編に基づき共有される情報の使用に関する手続を次のとおり定めるものとする。

(1) 違法な目的で使用されないことを保証するために、当該情報の再提供を制限すること。

(2) 当該情報のセキュリティ及び秘密性を確保すること。

(3) 当該情報の対象である個人の憲法上及び法律上の権利を保護すること。

(4) 陳腐化し、又は誤った名称及び情報を適時に除去し、破壊することによりデータの完全性を提供すること。

第 222 条　プライバシー担当官

長官は、次に掲げる事項を含むプライバシー政策に第一次的責任を負う上級の幹部職員１名を省内で任命しなければならない。

(1) 個人情報の使用、収集及び開示に関するプライバシー保護を技術の使用により支援し、陳腐化させないことを保証すること。

(2) プライバシー法による記録システムに登載される個人情報が 1974 年プライバシー法（Privacy Act of1974）で定める公正な情報実務を完全に遵守して取り扱われること。

(3) 個人情報の収集、使用及び開示に関する連邦政府による立法上及び法規上の提案を査定すること。

(4) 省の規則案のプライバシー影響評価又は収集された個人情報の種類及びその影響が及ぶ人数を含む個人情報のプライバシーに関する省のプライバシー影響評価を実施すること。

(5) プライバシーの侵害に関する苦情、1974 年プライバシー法の実施、内部統制その他の事項を含むプライバシーに影響を及ぼす省の活動に関する連邦議会に対する年次報告を用意すること。

第 223 条　非連邦のサイバー・セキュリティの強化

第 201 条に基づく責任を果たすに当たり、情報分析・基盤防護担当次官は、以下の規定に従わなければならない。

(1) 重要情報システムを保有し、又は運用する、州及び地方政府に対しては、必要に応じ、民間部門に対しては、要請に応じ、次に掲げるサービスを提供する。

(A) 重要情報システムへの脅威及び同システムの脆弱性に関する分析及び警告

(B) 緊急事態対応担当次官と連携を図り、重要情報システムへの脅威又は攻撃に対応する危機管理の支援

(2) 民間部門及び政府の他の組織体の要請に応じ、緊急事態対応担当次官と連携を図り、重要情報システムの重大な故障に対応するための緊急の障害回復計画に関し、必要に応じて技術援助を提供すること。

第 224 条　ネット・ガード

情報分析・基盤防護担当次官は、地域社会を援助して情報システム及び通信ネットワークへの攻撃に対応し、かつ、障害回復を行うために、「ネット・ガード（Net Guard)」として周知される、科学技術の関連領域に専門知識を有する地域社会のボランティア集団からなる全国的な技術守備隊を設立することができる。

第 225 条　2002 年サイバー・セキュリティ強化法

(a) 略称

この条は、「2002 年サイバー・セキュリティ強化法（Cyber Security Enhancement Act of 2002)」として引用することができる。

(b) 特定のコンピューター犯罪に関する量刑の指針の修正

(1) 合衆国量刑委員会に対する指令

合衆国法典第 28 編第 994 条(p)に基づく権限に従い、かつこの規定に基づき、合衆国量刑委員会（United States Sentencing Commission）は、合衆国法典第 18 編第 1030 条に基づく犯罪を犯した者に適用する指針及び方針説明を見直し、適切な場合には、これらを修正する。

(2) 要件

この項を執行するに当たり、量刑委員会は、以下の規定に従う。

(A) 前号［(1)号］に規定された犯罪の重大な性格、当該犯罪の発生率の増加並びに当該犯罪の予防に効果的な抑止力及び適切な刑罰の必要性が量刑の指針及び方針説明に反映されることを保証する。

(B) 次に掲げる要因及び指針がそれらの要因について説明をすることができるか否かの範囲を考慮する。

(i) 犯罪によりもたらされる潜在的及び現実的損失

(ⅱ) 犯罪に関わる高度な知識及び計画のレベル

(iii) 犯罪が商業的利益又は個人的金融利得を目的としたものか否か。

(iv) 被告がその犯罪を実行するに当たり危害を加える悪意をもって行動したか否か。

(ⅴ) 犯罪が危害を加えられた個人のプライバシーの権利を侵害した程度

(vi) 犯罪が国防、国家安全保障又は司法運営の促進のために政府により使用されるコンピュータに関わるものか否か。

(vii) 違反行為が重要基盤を著しく妨害し、若しくは混乱させることを意図したもの又はその効果をもつものであったか否か。

(viii) 違反行為が公衆の衛生若しくは安全又は人に対する損傷を与える脅威を醸成する効果を意図し、又はその効果を持つものであったか否か。

(C) 他の関連する指令及び他の量刑の指針との合理的な整合性を確保する。

(D) 一般に適用可能な量刑範囲の例外を正当化しうる加重事由又は軽減事由について説明する。

(E) 量刑の指針に追認のために必要な修正を加える。

(F) 指針が合衆国法典第 18 編第 3553 条(a)項(2)号に定める量刑の目的に十分に合致することを保証する。

(c)～(j)［略］

3-1-7　デラウェア州学校いじめ防止法

出典：「アメリカ合衆国におけるいじめ防止対応―連邦によるアプローチと州の反いじめ法制定の動き―（執筆者：井樋三枝子）
『外国の立法』No.233, 2007 年 9 月, pp.12-15（デラウェア州学校いじめ防止法全文）＜http://www.ndl.go.jp/jp/data/publication/legis/233/023301.pdf＞

デラウェア州学校いじめ防止法

An Act of May 18, 2007, ch. 14, 76Del. Laws (2007).

井樋三枝子訳

第１条　デラウェア州法典第 14 編を、以下に掲げる新たな第 4123A 条の追加により改正する。

第 4123A 条　学校いじめ防止及び犯罪的青年ギャング発見訓練

(a) 各学校区及びチャータースクールは、デラウェア州法典第 11 編第 617 条に規定される犯罪的青年ギャング行為及びデラウェア州法典第 14 編第 4112D 条に規定されるいじめ防止の確認及び報告のために、毎年合計 1 時間の合同訓練を、公立学校の被用者が受けることを保障しなければならない。訓練のための物品は、州司法省及び州教育省により、法執行機関、デラウェア州教育協会（the Delaware State Education Association）、デラウェア州学校理事会協会（the Delaware School Boards Association）、及びデラウェア州学校運営者協会（the Delaware Association of School Administrators）の協力のもとに準備されなければならない。

(b) この条により要求されるいかなる現職教育も、この編の第 1305 条(e)項において規定される契約学校年度内に提供されることが義務付けられる。

第２条　デラウェア州法典第 14 編第 41 章を、以下に掲げる新たな第 4112D 条の追加により改正する。

第 4112D 条　学校いじめ防止

(a) いじめの定義

この条で用いられる場合、いじめとは、他の児童・生徒、学校のボランティア要員又は学校教職員に対する、書かれた、電子的な、口頭の又は身体による意図的な行為又は行動であって、当該の状況下にある通常の者が、以下に掲げる効果を有すると当然知りうるものをいう。

(1) 児童・生徒、学校ボランティア要員又は学校の被用者の精神的若しくは身体的な健康に対して実質的な危害が加えられ、又は彼らの財産に対して実質的な損傷がなされ

るかもしれないという相当な理由のある恐怖の状態に、彼らを置くこと。

(2) 行動の浸透性若しくは執拗性によって、又はいじめ加害者といじめ対象者との間の力の格差によって、敵対的、脅迫的、屈辱的又は虐待的な教育環境を作り出すこと。

(3) 教育実績、教育機会又は教育的な恩恵を促進するために必要とされる安全な学校環境を、児童・生徒が有することを妨害すること。

(4) 個人又は団体を扇動し、教唆し、又は強制することにより、他の児童・生徒、学校ボランティア要員又は学校被用者の品格を傷つけ、人間性を奪い、面目を失わせるような、又は彼らに精神的、心理的若しくは身体的危害をもたらすようないじめを繰り返すこと。

(b) いじめの禁止

(1) 各学校区及びチャータースクールは、いじめを禁止し、いじめ行為の対象者、目撃者又はいじめの行為について信頼できる情報を有する者に対する復讐、報復又は誣告を禁じなければならない。

(2) 各学校区及びチャータースクールは、少なくとも以下に掲げる要素を含む指針を策定しなければならない。

(A) 学校の所有地内若しくは学校活動においての、又は、学校区若しくはチャータースクールのコンピュータ、コンピュータシステム、コンピュータネットワーク若しくはその他の電子技術を通じて接続されるデータ若しくはコンピュータのソフトウェアを用いての、幼稚園から 12 年生までにおけるいかなる者に対するいじめも禁ずるという声明。この条でいう、学校の所有地及び学校活動とは、この編の第 4112 条におけるものと同様の定義とする。

(B) この条の(a)項と同程度に包括的ないじめの定義

(C) 学校全体でいじめ防止計画を策定するための指示

(D) 各学校が、計画の設計、承認及び監督を含む学校のいじめ防止計画の調整に責任を負う、現場ベースの委員会を設置する義務。現場ベースの委員会のメンバーの過半数は学校の専門職員でなければならず、その過半数は教員でなければならない。委員会はそのほかに、学校運営を担当する職員、支援職員、（7 年生から 12 年生までに在籍する児童・生徒のための）生徒団体、親及び始業前又は放課後活動担当の職員の代表をも含んでいなければならない。これらの代表者は、非被用者団体の代表が学校長により任命されなければならないことを除き、それぞれが、代表する集団の構成員によって選出されなければならない。委員会は 1 人 1 票の原則で運営されなければならない。現場ベースの学校規律委員会がデラウェア州法典第 14 編の第 1605 条(7)項(a)及び(b)の規定に従い、既に設立されている場合は、その委員会は、前述の責任を受け入れるかどうかについては、投票を行わなければならない。

(E) ある者がいじめ対象になっているのではないかと、通常の者ならば思うようになる信頼に足る情報を学校被用者が有する場合、それを管理者に対し迅速に報告する

義務 F 時宜を得た方法で、管理者が迅速に調査を行い、いじめが発生したか否かを判断するための執行手続きを、各学校が有する義務 G 予算措置が可能な限りにおいて、各学校が教室外の領域での監督システムのための計画を策定する義務。その計画は、教室外の領域に関する情報の審査及び交換について規定する。

(H) いじめの影響の適切な範囲の特定

(I) この編の第 202 条(f)項に規定する児童・生徒及び親、後見人若しくは親戚である保護者に対し、又は法的後見人に対し、いじめ行為についての情報を提供するための手続き。ただし、この項は、匿名の通報にのみ基づいた公式の懲戒措置を認めるものではない。

(J) この条で規定されるいじめ対象者若しくは他者をいじめる者の、この編の第 202 条(f)項に規定される親、後見人若しくは親戚である保護者又は法的後見人が通知を受ける義務

(K) 州教育省規則に従い、すべてのいじめ事件を、発生後 5 業務日以内に州教育省に報告する義務

(L) いじめの通報後の報復を禁ずる声明

(M) 学校職員の構成員及びいじめ関連の事項について児童・生徒の治療に関与する医療専門職者の間の情報伝達のための手続き

(N) 学校いじめ防止計画を年間通して実行し、かつ学校行為規律指針及びこの編の第 4112 条に統合させる義務

(c) 指針の普及及び実行責任

(1) 各学校区及びチャータースクールは、2008 年 1 月 1 日までに、この条の(b)項に一致した指針を採択し、これを 1 部デラウェア州教育省に提出しなければならない。

(2) 指針は、児童・生徒及び職員の手帳に記載されなければならず、手帳がない場合又は新たな手帳を印刷し直すことが実用的でない場合には、指針の写しを毎年すべての児童・生徒、親、教員及び職員に対して配布することもできる。

(3) 指針は、その後毎年、1 月の最初の日までにデラウェア州教育省に提出されなければならない。教育省は、指針が州法、連邦法及び州教育省の定めた規則を遵守していることを、毎年審査しなければならない。

(4) デラウェア州教育省は、年次報告書を作成する。そこには通報され及び実証されたいじめ事件の要旨を含めなければならない。

(d) 教育省の責務

(1) デラウェア州教育省はデラウェア州法務省と協力し、モデル指針を作成しなければならない。モデル指針は適宜変更が認められ、幼稚園から 12 年生までに適用される。また、州教育省は学校区及びチャータースクールを支援するため、両省のウェブサイトにこの指針を掲載しなければならない。

(2) 2009 会計年度から始まる一般予算割当法に規定される学校区及びチャータースクー

ルへの包括的学校規律改善計画基金の配分は、学校区の又はチャータースクールのいじめ防止指針を州教育省が承認することを条件とする。

(3) 予算措置が可能な限りで、デラウェア州教育省は、省が規定する基準に基づいた模範的プログラムを有する学校のための賞金制度を提供することができる。

(e) 免責

学校被用者、学校ボランティア要員、又は児童・生徒は、善意に基づき、かつ、学校区又はチャータースクールのいじめ防止指針において明記された手続きを用いて 1 人以上の適切な者に対し、いじめを報告したことから起こる損害については訴訟原因から個々に免責される。ただし、通報行為が、甚だしい不注意、無頓着又は故意若しくは意図による行為又はこれらの両方を含む場合は、このような免責は行われてはならない。

(f) 他の抗弁

(1) 技術が関係する事件における物理的位置又はアクセスの時間は、学校との関連性が十分にある場合に、この条に基づき学校区又はチャータースクールによって始められたいかなる懲戒措置においても有効な抗弁とはならない。

(2) 学校区又はチャータースクールの指針に従って、合法的な業務又はこの条の侵害に関する調査の範囲内で行われる場合は、コンピュータ、コンピュータシステム、コンピュータネットワーク若しくはその他の電子的技術を通じてアクセスされるデータ又はコンピュータソフトを用いるいかなる者に対しても、この条を適用しない。

(g) 学校犯罪報告法との連携

ある事件が、いじめの定義に加え、州法又は連邦法に基づく特定の犯罪の定義を満たす場合がある。この条、又はその結果として策定された指針におけるいかなる規定も、学校職員がデラウェア州法典第 14 編第 4112 条の報告義務のすべてを果たすこと、又は学校の所有地内若しくは学校活動において起こった、同条では報告を必要とされない犯罪の予兆を通報することを妨げてはならない。この条のいかなる規定も、デラウェア州法典第 16 編第 9 章において明記される児童の虐待若しくは性的虐待のための通報義務又は州法若しくは連邦法に基づくその他のいかなる通報要求をも廃止するものではない。

(h) 規則及び規定

この条に反する規定の有無にかかわらず、デラウェア州教育省は、この条の履行に必要な規則及び規定を制定することができる。

3-2　EU

3-2-1　データ保持に関する EU 指令

原文：

http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=2006&nu_doc=24

（仮訳）

公開電子通信サービス又は公衆通信網の提供に関連して作成又は処理されるデータ保持に関して指令 2002/58/EC を修正する欧州議会・閣僚理事会指令 2006/24/EC（2006 年 3 月 15 日）

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006

on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

欧州議会及び閣僚理事会は、

欧州共同体設立条約、特にその第 95 条に配慮し、

欧州委員会の提案に配慮し、

欧州経済社会評議会の意見[76]に配慮し、

同条約第 251 条に定められた手続き[77]にしたがい行動し、

本指令を採択した。

前文

（1）1995 年 10 月 24 日の欧州議会・閣僚理事会の個人データ処理に係る個人の保護及び当該データの自由な移動に関する指令 95/46/EC[78]は、欧州共同体内の個人情報の自由な移動を確保するため、個人データの処理、及び特にプライバシー権に関して自然人の権利及び自由を保護することを加盟国に義務付けている。

（2）2002 年 7 月 12 日の欧州議会・閣僚理事会の電子通信部門における個人データ処理及

[76] 2006 年 1 月 19 日に発表された意見（官報では未発表）

[77] 2005 年 12 月 14 日欧州議会の意見（官報では未発表）及び 2006 年 2 月 21 日の閣僚理事会決定

[78] 規則（EC）No 1882/2003（2003 年 10 月 31 日 OJ L 284、1 ページ）で修正された指令（1995 年 11 月 23 日 OJ L 281、31 ページ）

びプライバシー保護に関する指令 2002/58/EC[79]（「プライバシー及び電子通信指令」）は、指令 95/46/EC に示された原則を電子通信部門向けの詳細規制に置き換えている。

(3) 指令 2002/58/EC 第 5 条、6 条、9 条は、ネットワーク及びサービスプロバイダが電子通信サービスの利用により生じるトラフィック及びロケーション・データを処理する際に適用される規則を定めている。当該データは、課金又は相互接続料金の支払いに必要なデータを除き、通信伝送のために不要となった時点で削除か匿名化しなければならない。同意を条件に、一部のデータをマーケティング目的及び付加価値サービス提供のために処理する場合もある。

(4) 指令 2002/58/EC 第 15 条 1 項は、加盟国が同指令第 5 条、6 条、8 条 1 項、2 項、3 項、4 項、及び 9 条に規定された権利及び義務の範囲を制限する場合の条件を示す。かかる制限はいずれも、具体的な社会的秩序を目的として、すなわち国家安全保障（つまり国の安全）、防衛、公安、又は刑事犯罪若しくは電子通信システムの不正利用の防止、捜査、発見、及び起訴を目的として、民主主義社会において必要、適切、及び相応でなければならない。

(5) いくつかの加盟国は、刑事犯罪の防止、捜査、発見、起訴を目的としたサービスプロバイダによるデータ保持について規定した法律を採用している。これら国内規定には多くの相違点がある。

(6) サービスプロバイダが保持すべきトラフィック及びロケーション・データの種類ならびに保持条件及び期間についての要件は様々であるため、刑事犯罪の防止、捜査、発見、起訴を目的としたデータ保持に関する国内規定間の法的及び技術的な相違点は、電子通信の域内市場に障害をもたらす。

(7) 2002 年 12 月 19 日の法務及び内務理事会の決議は、電子通信の可能性が大幅に増加したため、電子通信の利用に関するデータが特に重要であり、そのため刑事犯罪、特に組織犯罪の防止、捜査、発見、起訴において貴重な手段であることを明確に示している。

(8) 2004 年 3 月 25 日に欧州理事会が採択したテロ対抗に関する宣言は、同理事会に対し、サービスプロバイダによる通信トラフィックデータ保持に関する規則を制定するための措置を検討するよう指示している。

(9) 欧州人権条約（ECHR）第 8 条によると、誰もが自身の私生活及び通信を尊重する権利を有している。国家の諸機関は、法に基づいた場合に限り、また民主主義社会において必要な場合、特に国家安全保障又は公安のため、混乱若しくは犯罪防止のため、又は他人の権利及び自由を保護するためであれば、その権利の行使を妨げることができる。いくつかの加盟国でデータ保持が犯罪捜査のため、とりわけ組織犯罪及びテロ行為などの重大な問題に関して必要、かつ、有効な捜査手段であることが判明しため、本指令で規定された条件にしたがって、保持されたデータを捜査当局が利用できるよ

[79] 2002 年 7 月 31 日 OJ L 201、37 ページ

うにすることが必要である。したがって、ECHR 第 8 条の要件に準拠したデータ保持に関する法律の採用が必要な措置となる。

(10) 2005 年 7 月 13 日、閣僚理事会はロンドンでのテロ攻撃を非難する宣言の中で、電気通信データ保持に関する共同措置を早急に取る必要性を再確認した。

(11) 調査及びいくつかの加盟国での実地経験から明らかなように、刑事犯罪の防止、捜査、発見、起訴におけるトラフィック及びロケーション・データの重要性を考えると、本指令で規定されている条件にしたがって、通信サービス提供の過程で公開電子通信サービス又は公衆通信網のプロバイダによって作成又は処理されるデータが、欧州レベルで必ず一定期間保持されるようにする必要性がある。

(12) 指令 2002/58/EC 第 15 条 1 項は、本指令では特に保持が義務付けられておらず、よって指令の範囲から外れる不成功の呼び出しに関連したものを含めたデータ、及び本指令の対象外となる司法などの目的のための保持に引き続き適用される。

(13) 本指令は、通信若しくは通信サービスの結果作成又は処理されるデータのみを対象とし、伝送された情報の内容であるデータは関連しない。データは複数回にわたり保持されない方法で保持される必要がある。関係のある通信サービス提供により作成又は処理されるデータとは、入手が可能なデータを意味する。特に、インターネット電子メール及びインターネット電話に関連するデータ保持については、データ保持義務はプロバイダ又はネットワーク・プロバイダ自身のサービスからのデータのみが対象となり得る。

(14) 電子通信技術は急速に変化しており、所轄官庁の正当な要請も進化する場合がある。これらの案件に関して助言を得てベスト・プラクティスの共有を促すために、欧州委員会は加盟国の捜査当局、電子通信業界の諸団体、欧州議会及び欧州データ保護監視官局などのデータ保護当局の代表で構成される団体を設立する予定である。

(15) 指令 95/46/EC 及び指令 2002/58/EC は、本指令にしたがって保持されるデータに対して全面的に適用される。指令 95/46/EC 第 30 条 1 項（c）は、同指令第 29 条に基づき設立された個人データの処理に関して個人を保護する諮問委員会の諮問を義務付けている。

(16) 指令 95/46/EC 第 6 条に基づくデータ品質を保証する措置に関してサービスプロバイダに課せられる義務、ならびに同指令第 16 条、17 条に基づくデータ処理の機密性及び安全確保の措置に関してサービスプロバイダに課せられる義務は、本指令の趣意内で保持されたデータに対して全面的に適用される。

(17) 関係者の基本的権利を全面的に尊重して国内法に準拠している場合に限っては、本指令に基づき保持されたデータが所轄国内官庁に提供されるようにするための法的措置を加盟国が取ることが不可欠である。

(18) これに関連して、指令 95/46/EC 第 24 条は、加盟国に対して同指令にしたがって採用された規定への違反に対する制裁措置を定めるよう義務付けている。指令

2002/58/EC 第 15 条 2 項は、指令 2002/58/EC にしたがって採用された国内規定に関連して同じ要件を課す。情報システムへの攻撃に関する 2005 年 2 月 24 日閣僚理事会枠組決定 2005/222/JHA[80]は、保持されたデータも含めた情報システムへの故意の不正アクセスが刑事犯罪として処罰に値すると規定している。

(19) 不正な処理操作又は指令 95/46/EC にしたがって採用された国内規定に抵触する行為により個人が損害を被った場合、同指令第 23 条に基づく損害賠償を請求する権利は、本指令にしたがった個人データの不正処理にも適用される。

(20) 2001 年欧州評議会サイバー犯罪条約及び 1981 年欧州評議会個人データの自動処理に関して個人を保護する条約もまた、本指令の趣意内で保持されたデータを対象とする。

(21) 本指令の目的、すなわち各加盟国が国内法で定義しているようにプロバイダが特定のデータを保持する義務を整合させ、これらのデータが重罪の捜査、発見、起訴のため入手可能な状態にするという目的が加盟国では十分達成できず、したがって本指令の規模及び効果を理由として共同体レベルの方がよりよく達成できることから、欧州共同体設立条約第 5 条に示される補完性の原則にしたがい、欧州共同体が措置を講じることができる。その条項に示されている比例性の原則に従い、本指令はこれらの目的を達成するために必要な措置を逸脱することはない。

(22) 本指令は基本的権利を尊重し、特に欧州連合基本権憲章によって認められた原則を遵守する。特に本指令は指令 2002/58/EC と連携して、当該憲章第 7 条、8 条に定められている国民が私生活及び通信を尊重する権利に全面的に従い、個人情報保護に努める。

(23) 電子通信サービスプロバイダの義務が比例性の原則に従う必要があることを考えると、本指令は、通信サービス提供の過程において作成又は処理されたデータのみをプロバイダが保持することを義務付けている。かかるデータがこれらのプロバイダによって作成又は処理されていない限り、データ保持義務はない。本指令はデータ保持の技術を調和させることを意図してはおらず、その選択は国レベルで解決されるべき問題である。

(24) よりよい立法についての組織間協定第 34 項[81]に基づき、自国のため、及び欧州共同体の利益のために、加盟国は本指令と国内法化した措置との相関関係をできる限り図示した独自の表を作成するとともに、これらを公開するよう奨励されている。

(25) 本指令は、加盟国が指定する国内当局によるデータへのアクセス及び使用権に関して加盟国が法的措置を取る権限を侵害しない。指令 95/46/EC 第 3 条 2 項の最初のインデントで言及されている活動に関して本指令にしたがって保持されたデータへ国

[80] 2005 年 3 月 16 日 OJ L 69、67 ページ
[81] 2003 年 12 月 31 日 OJ C 321、1 ページ

内当局がアクセスする問題は、共同体法の範囲外にあたる。しかし、これらは国内法又は欧州連合条約第 6 章に基づく行為の対象となる場合がある。かかる法律又は行為は、加盟国の共通の憲法上の伝統から生じたものであり、欧州人権条約が保証する基本的権利を全面的に尊重しなければならない。欧州人権裁判所による欧州人権条約第 8 条の解釈によれば、国家の諸機関によるプライバシー権への介入は、必要性及び比例性の要件を満たさなければならず、したがって特定の明示的、かつ、正当な目的を果たし、当該介入の目的に関連して適切、かつ、関連性があり、過度でない方法で実施されなければならない。

第 1 条

対象及び範囲

1. 本指令は、各加盟国が自国の国内法にて定義しているとおり、重罪の捜査、発見、起訴を目的としてデータが入手できる状態にするため、公開電子通信サービス又は公衆通信網のプロバイダが作成又は処理した特定のデータをこれらプロバイダに保持させる義務についての加盟国の規定を整合させることを目的とする。
2. 本指令は、法人及び自然人双方についてのトラフィック及びロケーション・データ、ならびに契約者又は登録利用者の特定に必要な関連データに適用される。本指令は、電子通信網を使って求めた情報など、電子通信の内容には適用されない。

第 2 条

定義

1. 本指令において、指令 95/46/EC、2002 年 3 月 7 日の電子通信網及びサービスに関する共通の規制枠組みに関する欧州議会・閣僚理事会指令 2002/21/EC（「枠組み指令」）[82]、ならびに指令 2002/58/EC における定義が適用される。
2. 本指令において次の通り定義される。

   (a)「データ」とは、トラフィック及びロケーション・データ、ならびに契約者又は登録利用者の特定に必要な関連データを指す。

   (b)「利用者」とは、私的又は営利目的のいずれにせよ、必ずしもサービスの契約をしていることを前提とせず公開電子通信サービスを使っている法人又は自然人を指す。

   (c)「電話サービス」とは、通話（音声、ボイスメール、会議通話、データ通話を含む）、付加サービス（無条件転送、通信中転送を含む）、ならびにメッセージング及びマルチメディア・サービス（ショート・メッセージ・サービス、拡張メディアサービス、マルチメディア・サービスを含む）を指す。

   (d)「利用者 ID」とは、インターネット接続・サービス又はインターネット通信サービスを契約する又は登録する際に割り当てられる一意の識別子を指す。

[82] 2002 年 4 月 24 日 OJ L 108、33 ページ

(e)「セル ID」とは、携帯電話による通話が発信された又は終了したセルの識別情報を指す。

(f)「不成功の呼び出し」とは、通話がうまく接続されたものの応答がない、又はネットワーク管理者による介入があった通信を指す。

第 3 条

データ保持義務

1. 指令 2002/58/EC 第 5 条、6 条、9 条の特例として、加盟国は、通信サービス提供の過程においてそれぞれの管轄権内で公開電子通信サービス又は公衆通信網のプロバイダによりこれらのデータが作成又は処理されている範囲内で、本指令第 5 条に指定されたデータが同指令の規定にしたがって保持されるようにする措置を取るものとする。
2. 第 1 項に規定されたデータ保持義務は、関係する通信サービス提供の過程において、関係する加盟国の管轄権内において公開電子通信サービス又は公衆通信網のプロバイダによりこれらのデータが作成若しくは処理され、（電話データに関しては）格納され、又は（インターネット・データに関しては）ログが取られた不成功の呼び出しに関連して、第 5 条に指定されたデータの保持を含むものとする。本指令は、呼び出しすら成功していない通話に関連するデータ保持を義務付けていない。

第 4 条

データへのアクセス

加盟国は、本指令にしたがって保持されたデータが国内法に沿った具体的な事例において所轄国内官庁にのみ提供されるようにするための措置を取るものとする。必要性及び比例性の要件にしたがって保持されたデータにアクセスするために取るべき手順及び満たすべき条件は、EU 法又は国際公法の関連規定、特に欧州人権裁判所の解釈に配慮した欧州人権条約を前提として、各加盟国がそれぞれの国内法において定義するものとする。

第 5 条

保持されるデータの種類

1. 加盟国は、次の種類のデータが本指令にしたがい保持されるようにする。

（a）通信の発信源を追跡及び特定するために必要なデータ

（1）固定通信網電話及び携帯電話について

（i）発信電話番号

（ii）契約者又は登録利用者の名前及び住所

（2）インターネット接続、インターネット電子メール、及びインターネット電話について

（i）割り当てられた利用者 ID

（ii）公衆電話網に入る通信に割り当てられた利用者 ID 及び電話番号

（iii）通信時にインターネット・プロトコル（IP）アドレス、利用者 ID、又は電話番

号が割り当てられた契約者又は登録利用者の名前及び住所

(b) 通信の着信先を特定するために必要なデータ

(1) 固定通信網及び携帯電話について

(i) ダイヤルされた番号（かけた電話番号)、及び無条件転送や通信中転送など付加サービスが伴う場合は通話の最終着信先の番号

(ii) 契約者及び登録利用者の名前及び住所

(2) インターネット電子メール及びインターネット電話について

(i) インターネット電話着信先の利用者 ID 又は電話番号

(ii) 契約者名若しくは登録利用者の名前及び住所、ならびに通話着信先の利用者 ID

(c) 通信日時及び期間を特定するために必要なデータ

(1) 固定通信網の電話及び携帯電話、通信の開始及び終了日時について

(2) インターネット接続、インターネット電子メール、及びインターネット電話について

(i) インターネット接続・サービスのプロバイダが通信に割り当てた動的・静的を問わない IP アドレスと合わせて、特定の時間帯に基づいたインターネット接続・サービスのログイン及びログオフ日時、ならびに契約者又は登録利用者の利用者 ID

(ii) 特定の時間帯に基づいた、インターネット電子メールサービス又はインターネット電話サービスのログイン及びログオフ日時

(d) 通信の種類を特定するために必要なデータ

(1) 固定通信網の電話及び携帯電話について：使用された電話サービス

(2) インターネット電子メールサービス又はインターネット電話サービスについて：使用されたインターネットサービス

(e) 利用者の通信設備又は利用者の設備と称するものを特定するために必要なデータ

(1) 固定通信網の電話、発信・着信電話番号について

(2) 携帯電話について

(i) 発信・着信電話番号

(ii) 発信者の国際移動電話加入者識別番号（IMSI）

(iii) 発信者の国際携帯電話識別番号（IMEI）

(iv) 着信者の IMSI

(v) 着信者の IMEI

(vi) 先払い匿名サービスの場合、当該サービスが初めて始動した日時及びサービスの始動元のロケーション・ラベル（セル ID）

(3) インターネット接続、インターネット電子メール、及びインターネット電話について

(i) ダイヤルアップ接続向けの発信電話番号

(ii) 発信者側のデジタル加入者線（DSL）又は他のエンドポイント

(f) 移動体通信装置の所在地を特定するために必要なデータ

(1) 通信開始におけるロケーション・ラベル（セル ID）

(2) 通信データが保持される期間にロケーション・ラベル（セル ID）を参照して地理的位置を特定するデータ

2. 通信内容を明かすデータは本指令にしたがって保持できない。

第 6 条

保持期間

加盟国は、第 5 条に指定されたデータの種類が通信日から最低 6 ヶ月、最高 2 年間保持されるようにする。

第 7 条

データの保護及びデータの安全

指令 95/46/EC 及び指令 2002/58/EC にしたがって採用された規定の実施を害することなく、各加盟国は、公開電子通信サービス又は公衆通信網のプロバイダが、本指令にしたがい保持されたデータに関して最低限次のデータ安全原則を尊重するようにするものとする。

(a) 保持されたデータはネットワーク上のデータと同じ品質で、かつ、同じ安全・保護の対象となる。

(b) 当該データは、不測の若しくは不法な破棄、不測の損失若しくは改変、又は不正な若しくは不法な保管、処理、アクセス、若しくは開示からデータを保護するため、適切な技術的・組織的措置の対象となる。

(c) 当該データは、特に認可された者しかアクセスできないようにするため、適切な技術的・組織的措置の対象となる。

(d) 当該データは、アクセス及び保存済みのものを除き、保持期間終了時には破棄されるものとする。

第 8 条

保持されたデータの保管要件

加盟国は、保持されたデータ及びかかるデータに関連する他の必要な情報が不当な遅延なく要請に応じて所轄官庁に送信できるような方法で、第 5 条に指定されたデータが本指令にしたがい保持されるようにするものとする。

第 9 条

監督官庁

1. 各加盟国は、保管されたデータの安全に関して第 7 条にしたがい加盟国が採択した規定の管轄権内での適用を監視する責任を有する国の機関を 1 つ以上指定するものとする。これら諸機関は、指令 95/46/EC 第 28 条で言及されている官庁と同一でもよい。

2. 第 1 項で言及されている官庁は、同項で言及されている監視を実施するにあたり、完全に独立して行動するものとする。

第 10 条

統計資料

1. 加盟国は、公開電子通信サービス又は公衆通信網の提供に関連して作成又は処理されたデータの保持に関する統計資料が欧州委員会に年 1 回提供されるようにするものとする。かかる統計資料には次のものが含まれる。

— 適用される国内法にしたがい所轄官庁に情報が提供された案件

— データが保持された日付から所轄官庁がデータ送信を要請した日付までの経過時間

— データ要請に応じられなかった案件

2. かかる統計資料には個人情報が含まれてはならない。

第 11 条

指令 2002/58/EC の改正

次の項を指令 2002/58/EC 第 15 項に挿入する。

「1a.公開電子通信サービス又は公衆通信網の提供に関連して作成又は処理されたデータの保持に関する 2006 年 3 月 15 日の欧州議会・閣僚理事会指令 2006/24/EC[83]によって同指令第 1 条 1 項で言及されている目的のため保持が特に義務付けられているデータには、第 1 項を適用しない。

第 12 条

今後の措置

1. 第 6 条で言及されている限定されている最大保持期間の延長を正当化する状況に直面している加盟国は、必要な措置を講じることができる。その加盟国は、すみやかに欧州委員会に報告するとともに、本条にしたがい講じられた措置の導入根拠を他の加盟国に述べるものとする。

2. 欧州委員会は、第 1 項で言及されている報告後 6 ヶ月以内に、措置が恣意的な差別をする若しくは加盟国間の貿易を制限する隠れ蓑となる手段かどうか、そして域内市場の機能への障害となるかどうかを検討したうえで、関係する国内措置を承認するか却下するものとする。その期間内に欧州委員会が判断しなかった場合、国内措置は承認されたものとみなされる。

3. 第 2 項にしたがい、本指令の規定の特例にあたる国内措置を加盟国が承認した場合、欧州委員会は本指令の修正を提案するかどうかを検討することができる。

第 13 条

救済、責任、刑罰

1. 各加盟国は、司法救済、責任、及び制裁措置を規定した指令 95/46/EC 第 III 章を履行する国内措置が、本指令に基づくデータ処理に関連して全面的に履行されるようにすべく、必要な措置を講じるものとする。

2. 各加盟国は特に、本指令にしたがって保持されたデータが本指令にしたがい採択された

[83] 2006 年 4 月 13 日 OJ L 105、54 ページ

国内法に違反し故意でアクセスされる又は転送される場合、実効的、かつ、相応で、抑止力のある行政処分又は刑事処分などの処罰の対象となるよう、必要な措置を講じるものとする。

第 14 条

評価

1. 2010 年 9 月 15 日までに、欧州委員会は、電子通信技術の将来的な発展及び第 10 条にしたがい同委員会に提供された統計資料を考慮した上で、特に第 5 条のデータのリストと第 6 条で規定されている保持期間に関して本指令の規定を修正する必要があるかどうかを検討し、本指令の適用の評価と経済事業者及び消費者への影響についての報告書を欧州議会及び閣僚理事会に提出するものとする。評価結果は公開される。
2. そのためには、同委員会は、加盟国又は指令 95/46/EC 第 29 条にしたがい設立された諮問委員会によって伝えられたすべての所見を検討するものとする。

第 15 条

国内法化

1. 2007 年 9 月 15 日までに、加盟国は、本指令の遵守に必要な法律、規則、及び行政規定を施行するものとする。加盟国は直ちに欧州委員会にその旨を通知する。加盟国がこれらの措置を取るときには、本指令への言及を含めるか、公式に刊行する際にかかる言及を伴わせるものとする。かかる言及の方法は加盟国が定める。
2. 加盟国は、本指令の対象となる分野で採択する国内法の主要規定の文言を欧州委員会に報告する。
3. 各加盟国は、本指令をインターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に適用するのを 2009 年 3 月 15 日まで延期することができる。本項を行使する予定の加盟国はいずれも、本指令の採択時点で宣言という手段で閣僚理事会と欧州委員会にその趣旨を通知する。その宣言は、EU 官報で発表されるものとする。

第 16 条

発効

本指令は、EU 官報で発表した日の 20 日後に発効する。

第 17 条

受取者

本指令は加盟国に宛てられる。

2006 年 3 月 15 日ストラスブールにて

欧州議会

議長

J. BORRELL FONTELLES

閣僚理事会

議長
H. WINKLER

指令 2006/24/EC 第 15 条 3 項によるオランダの宣言

公開電子通信サービス提供に関連して処理されたデータの保持に関して指令 2002/58/EC を修正する欧州議会・閣僚理事会の指令に関して、オランダは、本指令のインターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に対する適用を本指令発効日後 18 ヶ月を超えることなく延期するという選択権を行使する。

指令 2006/24/EC 第 15 条 3 項によるオーストリアの宣言

オーストリアは、本指令のインターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に対する適用を第 15 条 1 項に指定された日付の後 18 ヶ月間延期することを宣言する。

指令 2006/24-/EC 第 15 条 3 項によるエストニアの宣言

公開電子通信サービス又は公衆通信網提供に関連して作成又は処理されたデータ保持に関して指令 2002/58/EC を修正する欧州議会･閣僚理事会の指令第 15 条 3 項にしたがい、エストニアはここに、同項を行使し、当該指令のインターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に対する適用を当該指令の採択日から 36 ヶ月後まで延期する意図を表明する。

指令 2006/24/EC 第 15 条 3 項による英国の宣言

英国は、公開電子通信サービス又は公衆通信網提供に関連して作成又は処理されたデータ保持に関して指令 2002/58/EC を修正する指令第 15 条 3 項にしたがい、同指令のインターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に対する適用を延期することを宣言する。

指令 2006/24/EC 第 15 条 3 項によるキプロス共和国の宣言

キプロス共和国は、当該指令のインターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に対する適用を第 15 条 3 項に決められた日付まで延期することを宣言する。

指令 2006/24/EC 第 15 条 3 項によるギリシャ共和国の宣言

ギリシャは、第 15 条 3 項にしたがい、本指令のインターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に対する適用を第 15 条 1 項で規定された期間終了から 18 ヶ月後まで延期することを宣言する。

指令 2006/24/EC 第 15 条 3 項によるルクセンブルク大公国の宣言

公開電子通信サービス又は公衆通信網提供に関連して作成又は処理されたデータ保持に関して指令 2002/58/EC を修正する欧州議会･閣僚理事会の指令第 15 条 3 項にしたがい、ルクセンブルク大公国は、当該指令のインターネット接続、インターネット電話、及び

インターネット電子メールに関連した通信データの保持に対する適用を延期する選択権を持つため、当該指令第 15 条 3 項を行使する意図があることを宣言する。

指令 2006/24/EC 第 15 条 3 項によるスロベニアの宣言

スロベニアは、当該指令のインターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に対する適用を 18 ヶ月間延期することに関して、公開電子通信サービス又は公衆通信網提供に関連して作成又は処理されたデータ保持に関して指令 2002/58/EC を修正する欧州議会・閣僚理事会の指令第 15 条 3 項にしたがい宣言をした加盟国の一団に加わる。

指令 2006/24/EC 第 15 条 3 項によるスウェーデンの宣言

第 15 条 3 項にしたがい、スウェーデンは、本指令のインターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に対する適用の選択権を持つことを希望する。

指令 2006/24/EC 第 15 条 3 項によるリトアニア共和国の宣言

公開電子通信サービス又は公衆通信網提供に関連して作成又は処理されたデータ保持に関して指令 2002/58/EC を修正する欧州議会・閣僚理事会の指令第 15 条 3 項（「当該指令」とする）にしたがい、リトアニア共和国は、当該指令が採択された後、インターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に対する適用を第 15 条 3 項に規定された期間延期することを宣言する。

指令 2006/24/EC 第 15 条 3 項によるラトビア共和国の宣言

公開電子通信サービス又は公衆通信網提供に関連して作成又は処理されたデータ保持に関して指令 2002/58/EC を修正する 2006 年 3 月 15 日欧州議会・閣僚理事会の指令第 15 条 3 項にしたがい、ラトビアは、インターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に本指令を適用するのを 2009 年 3 月 15 日まで延期することを表明する。

指令 2006/24/EC 第 15 条 3 項によるによるチェコ共和国の宣言

第 15 条 3 項にしたがい、チェコ共和国はここに、インターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に本指令を適用するのを指令採択日から 36 ヶ月後まで延期することを宣言する。

指令 2006/24/EC 第 15 条 3 項によるベルギーの宣言

ベルギーは、第 15 条 3 項に基づき行使できる選択権を行使し、インターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に本指令を適用するのを指令採択日から 36 ヶ月後まで延期することを宣言する。

指令 2006/24/EC 第 15 条 3 項によるポーランド共和国の宣言

ポーランドはここに、公開電子通信サービス又は公衆通信網提供に関連して作成又は処理されたデータ保持に関して指令 2002/58/EC を修正する欧州議会・閣僚理事会の指令第 15 条 3 項で規定される選択権を行使し、インターネット接続、インターネット電話、及

びインターネット電子メールに関連した通信データの保持に本指令を適用するのを第 15 条 1 項に指定された日付から 18 ヶ月間延期する意図があることを宣言する。

指令 2006/24/EC 第 15 条 3 項によるフィンランドの宣言

公開電子通信サービス又は公衆通信網提供に関連して作成又は処理されたデータ保持に関して指令 2002/58/EC を修正する欧州議会･閣僚理事会の指令第 15 条 3 項にしたがい、フィンランドは、インターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に当該指令を適用するのを延期することを宣言する。

指令 2006/24/EC 第 15 条 3 項によるドイツの宣言

ドイツは、インターネット接続、インターネット電話、及びインターネット電子メールに関連した通信データの保持に本指令を適用するのを第 15 条 1 項の第一文で指定された日付から 18 ヶ月間延期する権利を留保する。

3-3　英国

3-3-1　1990 年コンピュータ不正使用法（抄）

原文：http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
（仮訳）

1990 年コンピュータ不正使用法（抄）

Computer Misuse Act 1990 (c. 18)

1990 第 18 章

無権限のアクセス又は改変からコンピュータ・マテリアルを保護するための条項を制定する法律及び関連する目的の法律［1990 年 6 月 29 日］

女王陛下により、貴族院及び庶民院の助言と承認を得て、本国会において、本国会の権限により、以下のとおり制定された。

コンピュータ不正使用罪

第 1 条　コンピュータ・マテリアルに対する無権限アクセス

(1)　以下の行為を行なった者は、有罪とする。
(a)　コンピュータ内のプログラム又はデータにアクセスする意図で、コンピュータに何らかの機能を実行させた場合であって、
(b)　その者が得ようとしたアクセスが無権限のものであり、かつ、
(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、当該機能をコンピュータに実行させるものであることを知っていた場合

(2)　本条における犯罪を実行する行為者が有していなければならない意図は、以下に対するものであることを要しない。
(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存されているプログラム、若しくはデータ

(3)　本条で有罪である者は、略式裁判により、6 月以下の拘禁刑、若しくは標準量刑基準におけるレベル 5 以下の罰金刑、又はその併科とする。

第 2 条　犯罪を実行する又は幇助する意図でなされる無権限アクセス
(1) 第 1 条の犯罪（無権限のアクセス犯罪）を以下の目的で、意図的に実行した者は、本条において有罪とする。
(a)　本条を適用すべき犯罪行為罪を実行する目的、又は、
(b)　本条を適用すべき犯罪行為を実行すること（自身が実行する場合とそれ以外の者が実行する場合とを問わない）を幇助する目的、
また、本条の以下の条項においては、当該の者が実行、若しくは幇助しようと意図した犯罪行為を更なる犯罪として指示する。

(2)　本条は、以下に該当する罪につき適用される。
(a)　その罪の刑罰が、法律によって定められている場合、又は、
(b)　21 歳以上の者（前科を有しない）に対し 5 年の拘禁刑を宣告することができる場合（又は、イングランド及びウェールズにおいては、1980 年治安判事裁判所法（1980 年一般法律第 43 号）第 33 条により課せられる制限がなければ、そのように宣告することができる場合）。

(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時に実行されたか、又は、その後に実行されたかは、重要ではない。

(4)　さらなる犯罪を実行することが不可能であるという事実があった場合であっても、本条において、有罪となり得る。

(5)　本条の犯罪行為で有罪となった者は、以下の責任を負う。
(a)　略式裁判が行われた場合、6 月以下の拘禁刑、若しくは法定の最高額を超えない金額の罰金刑、又はその併科、又は
(b)　正式起訴(indictment)が行われた場合、5 年以内の拘禁刑、若しくは罰金刑に処し、又はその併科

第 3 条　コンピュータ・マテリアルの無権限の改変
(1)　以下の行為を行った者は、有罪とする。
(a)　コンピュータのコンテンツの無権限な改変を生じさせる一切の行為を行った場合、か

つ、
(b)　行為時において、必要な意図、及び必要な認識を有していた場合

(2)　本条第(1)項(b)における、必要な意図とは、コンピュータのコンテンツに改変を生じさせ、かつ、当該行為によって、以下のいずれかを生じさせる意図のことをいう。
(a)　コンピュータの運用を損なうこと、又は
(b)　コンピュータ内にあるプログラム、若しくはデータにアクセスすることを妨害し、又は、これを阻害すること
(c)　当該プログラムの運用、若しくは当該データの信頼性を阻害すること

(3)　この意図は、以下に対するものであることを要しない。

(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、特定の種類のプログラム、若しくはデータ、又は 、
(c)　特定の改変、若しくは特定の種類の改変

(4)　本条第(1)項(b)における、必要な認識とは、当該行為者が生じさせようとした改変が無権限のものであるという認識をいう。

(5)　本条において、本条第(2)項で規定されているような種類の無権限な改変、若しくはその意図された効果が、永久的なものか、一時的なものか、或いは永久的か一時的か意図されたものであるかは、重要ではない。

(6)　1971 年犯罪損害法（1971 年法第 48 号）においては、コンピュータのコンテンツの改変は、コンピュータ、又はコンピュータの記憶媒体に対する損害行為とみなされてはならない。但し、コンピュータ、又はコンピュータの記憶媒体への影響が、物理的な状態を害する場合はこの限りでない。

(7)　本条の犯罪行為で有罪となった者は、以下の責任を負う。
(a)　略式裁判が行われた場合、6 月以下の拘禁刑、若しくは法定の最高額を超えない金額の罰金刑、又は、その併科、又は、
(b)　正式起訴が行われた場合、5 年以内の拘禁刑、若しくは罰金刑に処し、又はその併科

3-3-2　調査権限規制法（抄）

出典：「イギリス「調査権限規制法」の成立―情報機関等による通信傍受・通信データの取得等の規制―（執筆者：横山　潔）『外国の立法』No.214, 2002 年 11 月, pp.73-77（第 21 条～第 25 条）
＜http://www.ndl.go.jp/jp/data/publication/legis/214/21402.pdf＞

イギリス「2000 年調査権限規制法」

(法律第 23 号)

Regulation of Investigatory Powers Act 2000

Chapter 23

横山潔訳

第 1 章

第 2 節通信データの獲得及び開示

第 21 条　通信データの合法的獲得及び開示

(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 date）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。

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。

(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。

第 23 条　許可及び通信の形式及び期間

(1) 前条第３項に基づく許可は、次の各号の定めるところに従う。

(a) 書面によって、又は（書面によらないときは）許可が付与された旨の記録を明示する方法によって付与されなければならない。

(b) 本節の規定が適用される、許可された行為、及び当該行為が許可されることになる通信データを記載しなければならない。

(c) 当該許可が付与されることになる、第 22 条第２項に該当する事項を定めなければならない。

(d) 当該許可を付与する者が保有する官職、階級又は地位を定めなければならない。

(2) 通信データが開示されること、及び取得され、又は開示されることを要求する、第 22 条第４項に基づく通知は、次の各号の定めるところに従う。

(a) 書面によって、又は（書面によらないときは）通知が行われた旨の記録を明示する方法によって行われなければならない。

(b) 当該通知に基づいて取得又は開示される通信データを記載しなければならない。

(c) 当該許可が付与されることになる、第 22 条第２項に該当する事項を定めなければならない。

(d) 当該通知を行う者が保有する官職、階級又は地位を定めなければならない。

(e) 当該通知によって要求される開示が行われる方法を定めなければならない。

(3) 第 22 条第４項に基づく通知によって、次の各号の１に掲げる者以外の者へのデータの開示を要求してはならないが、b 号の適用上、その者が当該通知を行う者と同一の公的機関の官職、階級又は地位を保有していないときは、その者を定め、その他特定してはならない。

(a) 当該通知を行った者

(b) 当該通知の規定中に定めることができるその他の者、その他当該通知の規定によって、若しくは当該通知の規定に従って特定することができるその他の者

(4) 第 22 条３項に基づく許可又は第 22 条第４項に基づく通知は、次の各号の定めるところに従う。

(a) 当該許可が付与され、又は当該通知が行われた日から起算して１か月の期間の終了後にデータが取得されることを許可又は要求するものであってはならない。

(b) 通知の事案において、当該期間の終了後に、当該期間中のある時点に郵便管理者又は遠隔通信管理者が占有又は取得していないデータの開示を許可又は要求するものであってはならない。

(5) 第 22 条 3 項に基づく許可又は第 22 条第 4 項に基づく通知は、（前項又は第 7 項に従って）当該許可又は通知に適用される 1 か月の期間の終了に先立って、いつでも更新することができる。
(6) 第 22 条 3 項に基づく許可の更新又は第 22 条第 4 項に基づく通知の更新は、本条に従って、再度の許可又は通知を付与し、又は行うことによるものとする。
(7) 更新された許可又は更新通知に関して、第 4 項の規定は、更新の時点に進行している許可又は通信に適用することができる 1 か月の期間の終了までに、第 4 項中に定める 1 か月の期間が開始していなかったものとして効力を有する。
(8) 第 22 条第 4 項に基づいて通知を行った者が、次の各号の 1 に該当する事項を確信したときは、この者は、当該通信を取り消すものとする。
(a) 当該通知の要求が遵守されることが、第 22 条第 2 項に該当する理由により必要でなくなったこと
(b) 当該通知によって要求される行為が、当該通知に関係する通信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こと
(9) 国務大臣は、前項によって課せられる義務を履行することができなくなった者に、当該義務が課せられる事案において、規則をもって、当該義務を履行すべき者を定めることができ、また本項に基づく規則をもって、当該義務が課せられる者を当該規則に従って任命された者とする旨を定めることができる。

第 24 条　支払いを求める取決め

(1) 国務大臣が適切と思料する事案において、第 22 条第 4 項に基づく通知を遵守するに当たって郵便管理者又は遠隔通信管理者によって生じた費用をこれらの者に適切に分担させることを要求又は許可することが適切である、と自己が思料する取決めが有効である旨を保証することをもって、国務大臣の義務とするものとする。
(2) 国務大臣は、本条に基づく自己の義務を遵守するために、議会が定める金額から支払いを行う取決めを定めることができる。

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) 国家刑事情報局
(c) 国家犯罪対策班
(d) 関税及び消費税庁委員
(e) 内国歳入庁委員
(f) 情報機関
(g) 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

(4) 国務大臣は、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ができる。

(5) 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本条に基づく命令の草案が未だ議会に提出されておらず、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。

3-3-3　2006 年テロリズム法（抄）

出典：「英国 2006 年テロリズム法（執筆者：岡久　慶）」
『外国の立法』No.229, 2006 年 8 月, pp.6-12（第 1 条～第 4 条）
＜http://www.ndl.go.jp/jp/data/publication/legis/229/022901.pdf＞
※注釈は省略している。

2006 年テロリズム法

（法律第 11 号）
Terrorism Act 2006
Chapter 11

岡久　慶訳

第 1 部　犯罪

テロリズムの奨励等

第 1 条　テロリズムの奨励

(1) この条は、その受け手である公衆によって、テロリズム活動若しくは条約犯罪の実行、準備又は扇動の直接的若しくは間接的な奨励又はその他の誘引と理解される可能性が高い声明に対して適用する。

(2) 次の各号に掲げる行為をすべて行った者は、犯罪を行ったものとする。

(a) この条が適用する声明を公表し、又は他の者に声明を公表させた場合

(b) 前掲の声明を公表し、又は公表させたとき、次の条件いずれかに該当する場合

(i) 公衆がテロリズム活動若しくは条約犯罪の実行、準備又は扇動を直接的若しくは間接的に奨励され、又はその他誘引されることを意図していること。

(ii) 公衆がテロリズム活動若しくは条約犯罪の実行、準備又は扇動を直接的若しくは間接的に奨励され又はその他誘引されるか否かに関して、結果に無思慮であること。

(3) この条の目的の上で、公衆によって、間接的にテロリズム活動若しくは条約犯罪の実行又は準備を奨励していると理解される可能性のある声明とは、次の条件のいずれにも該当するあらゆる声明を含む。

(a) これらの行為若しくは犯罪の実行又は準備（過去のものであるか、将来のものであるか又は全般に関わるか否かにかかわらず）を賛美すること。

(b) 賛美されている行為が、現在の状況において模倣されるべき行為であるとして賛美されていると、公衆が推論することが合理的に予期される声明であること。

(4) この条の目的の上で、声明がいかに理解される可能性があるか、及び公衆が声明から何を推論するかが合理的に予期されるかという問題を判断するに当たっては、次のことに留

意しなければならない。

(a) 声明全体の内容

(b) 声明が公表された状況及び態様

(5) 第 1 項から第 3 項までの規定の目的の上で、次のことは無関係である。

(a) 第 1 項から第 3 項で言及されたことが、一若しくは複数の特定のテロリズム活動若しくは条約犯罪、又は特定の名称をもったテロリズム活動若しくは条約犯罪、若しくはテロリズム活動若しくは条約犯罪一般の実行、準備又は扇動に関係しているか否か。

(b) 声明によって、これらの行為若しくは犯罪の実行、準備又は扇動を実際に奨励され、又は誘引された者がいるか否か。

(6) この条に基づく犯罪の訴追において、被告人が声明により直接的にも間接的にもテロリズム活動若しくは条約犯罪の実行、準備若しくは扇動を奨励し、又はその他誘引することを意図していたことが証明されない場合、次に掲げることを示すことは被告人の抗弁となる。

(a) 声明が、被告人の意見を表明したものでもなく、被告人の支持（第 3 条に定めるところによるものかそれとは別のものによるものかは問わない）が与えられたものでもないこと。

(b) 声明発表のすべての状況において、その声明が、被告人の意見を表明したものではなく、かつ、（第 3 条第 3 項に基づく通知を受けたものの、これに従わなかった可能性とは別に）被告人の支持が与えられたものでもなかったこと。

(7) この条に基づく犯罪の廉で有罪とされた者は、以下の刑に処する。

(a) 正式起訴による有罪宣告によって、7 年以下の拘禁刑若しくは罰金又はその併科

(b) イングランド及びウェールズにおける略式起訴による有罪宣告によって、12 月以下の拘禁刑若しくは法定最高額以下の罰金又はその併科

(c) スコットランド又は北アイルランドにおける略式起訴による有罪宣告によって、6 月以下の拘禁刑若しくは法定最高額以下の罰金又はその併科

(8) 2003 年刑事司法法（Criminal Justice Act 2003（c. 44））第 154 条第 1 項の施行の前に行われた犯罪に関しては、第 7 項(b)号の 12 月とあるのは 6 月と改める。

第 2 条　テロリスト刊行物の頒布

(1) 第 2 項に該当する行為に関与し、かつその行為の時に、次の各号いずれかに該当するかたちでこれを行った者は、犯罪を行ったものとする。

(a) 行為の効果が、テロリズム活動の実行、準備若しくは扇動の直接的若しくは間接的な奨励又はその他誘引となることを意図していること。

(b) 行為の効果が、テロリズム活動の実行又は準備についての支援の提供となることを意図していること。

(c) 行為が(a)号又は(b)号のいずれかに掲げる効果を有するかに否かに関して、無思慮であ

ること。

(2) この条の目的の上で、次に該当する行為を行う者は、この項に該当する行為を行ったものとする。

(a) テロリスト刊行物を頒布し、又は、流布させること。

(b)刊行物を贈与し、販売し、又は貸与すること。

(c) 刊行物を販売又は貸与のために提供すること。

(d) 他の者が刊行物を入手し、閲覧し、聴取し若しくは見ること、又は贈与、販売若しくは貸与によって入手することができるようにするサービスを提供すること。

(e) 刊行物の内容を電子的に伝達すること。

(f) (a)号から(e)号までの規定に該当する行為を目的として、当該刊行物を所持していること。

(3)この条の目的の上で、第 2 項に該当する行為に関連して、刊行物に含まれる内容が次の各号のいずれかに該当する可能性がある刊行物は、テロリスト刊行物とする。

(a) 当該行為の結果として、刊行物が提供されている者若しくは利用提供されうる者の内のある者若しくは全員により、テロリズム活動の実行、準備若しくは扇動の直接的若しくは間接的な奨励又はその他誘引であると理解されること。

(b) テロリズム活動の実行若しくは準備に有用であり、かつ前記の者の一部又は全員によって、全体的に若しくは主として、それらの者に役立つものであることを目的として、その刊行物に含まれ又はそれらの者の利用に供されていると理解されること。

(4) この条の目的の上で、テロリズム活動の実行又は準備の間接的な奨励であると人によって理解される可能性のある事項とは、次のものを含む。

(a)（過去のものであるか将来のものであるか又は全般的なものか否かにかかわらず）これらの行為の実行又は準備を賛美していること。

(b) 賛美される行為が、現在の状況において模倣されるべき行為として賛美されていることを、合理的に推論しうるものであること。

(5) この条の目的の上で、刊行物が特定の行為に関連したテロリスト刊行物であるか否かの問題は、次のことを考慮して決定されなければならない。

(a) 当該の行為があった時点であること。

(b) 当該の刊行物の全体としての内容及び行為があった状況という 2 つのことを考慮すること。

(6) テロリスト刊行物に関連する、ある者の行為の効果への第 1 項における言及は、当該行為の結果として刊行物を利用提供され、若しくは利用提供されるかもしれない一若しくは複数の者に及ぼす刊行物の効果への言及を含む。

(7) この条の目的の上で、第 1 項から第 4 項までに言及された事項が、一若しくは複数の特定のテロリズム活動、特定の名称を持ったテロリズム活動、又はテロリズム活動一般の実行、準備及び扇動に関連しているか否かは、無関係である。

(8) この条の目的の上で、いかなる物の内容に含まれる事項に関してであれ、次のことは同じく無関係である。

(a) 当該の事項によって、テロリズム活動の実行、準備及び扇動を実際に奨励され、又は誘引された者がいるか否か。

(b) テロリズム活動の実行又は準備のために、当該の事項を利用した者がいるか否か。

(9) 第 10 項が適用される行為に関連して、この条に基く犯罪の訴追において、次に掲げることを示すことは被告人の抗弁となる。

(a) 問題のテロリスト刊行物とされた刊行物を引証して、その内容が被告人の意見を表明したものでも被告人の支持（第 3 条の定めるところによるものかそれとは別のものによるものかにかかわらず）が与えられたものでもなかったことを立証すること。

(b) 行為のすべての状況において、その内容が被告の意見を表明したものではなく、（被告人が第 3 条第 3 項に基づく通知を受けたもののこれに従わなかったという可能性とは別に）被告人の支持が与えられたものでなかったことが明らかであったことを立証すること。

(10) この項は、次に掲げる規定に定める範囲内で人の行為に適用される。

(a) その者の行為が関連している刊行物が、引証により第 3 項(a)号に定めるテロリスト刊行物とされる内容を含むものであること。

(b) 前記の者が(1)項(a)号に明記された意図をもって当該の行為に関与したことが証明されないこと。

(11) この条に基づく犯罪の廉で有罪とされた者は、以下の刑に処する。

(a) 正式起訴による有罪宣告によって、7 年以下の拘禁刑若しくは罰金又はその併科

(b) イングランド及びウェールズにおける略式起訴による有罪宣告によって、12 月以下の拘禁刑若しくは法定最高額以下の罰金又はその併科

(c) スコットランド又は北アイルランドにおける略式起訴による有罪宣告によって、6 月以下の拘禁刑若しくは法定最高額以下の罰金又はその併科

(12) 2003 年刑事司法法第 154 条第 1 項の施行の前に行われた犯罪に関しては、第 11 項(b)号の 12 月とあるのは 6 月と改める。

(13) この条中、以下の規定に掲げる用語の解釈は、当該規定の定めるところによる。

「貸与する（lend)」とは、賃貸しを含み、「貸与（loan)」もこれに応じて解釈する。「刊行物（publication)」とは、次のいずれか　又はそれらの組み合わせを内容とする、物又は記録をいう。

(a) 読むもの

(b) 聴くもの

(c) 注視し又は観察するもの

第 3 条　インターネット上の活動に対する第 1 条及び第 2 条の適用

(1) この条は、第 1 条及び第 2 条の目的のために、次に掲げる場合において適用される。

(a) 声明が電子的に提供されるサービスの提供若しくは利用の過程で、若しくはそれとの関連で公表され、又は公表させられた場合

(b) 第 2 条第 2 項に該当する行為が、前号のサービスの提供又は利用の過程で、若しくはそれとの関連であった場合

(2) 前項の行為が関係する声明又は物若しくは記録が、いつであっても、人（以下「関係者」という。）の支持が与えられているとみなされる場合は、次に掲げる場合を含む。

(a) 警察官が第 3 項に基づき通知を関係者に与えている場合

(b) 当該の通知が行われた日の後労働日 2 日が経過している場合

(c) 関係者が、正当な理由なく、通知に従わなかった場合

(3) この項に基づく通知とは、次に掲げることを行う通知をいう。

(a) 通知を行う警察官の意見において、声明又は物若しくは記録が不法にテロリズムに関連していると表明すること。

(b) 関係者に、声明又は物若しくは記録の、前掲に関連する部分を公衆に開示しないようにし、又は関連性がなくなる修正を加えることを要請する。

(c) 関係者に対し労働日 2 日以内に通知に従わなかった場合には、声明又は物若しくは記録を支持しているものとみなされると警告する。

(d) 通知に従った後で、声明又は物若しくは記録が公衆に開示された場合、第 4 項に基づき、いかにして通知の定めるところに従い責任を問われうるかを説明する。

(4) 関係者により引き続き行われる発表の時期に関連する以下の規定に該当する場合には、第 2 項(a)号から(c)号までの条件は、再声明（(b)号中の「再声明」をいう。）の場合においては、満たされたものとみなす。

(a) 第 3 項に基づく通知が声明又は物若しくは記録に関して関係者に行われ、その者がこれに従っていること。

(b) 前号の規定にかかわらず、通知が関係する声明と同一の声明若しくはあらゆる実際的目的からいって同じ若しくは効果が同じ声明、又は通知が関係する物若しくは記録に含まれる内容と同じ声明（以下、「再声明」という。）を引き続き発表し、又は発表させること。

(5) 第 1 条又は第 2 条に基づく犯罪の廉で、ある者を訴追する際、次のいずれも示すことができれば、第 2 項(a)号から(c)号までの要件は、満たされていないものとする。

(a) その時までに再声明が公衆に利用されることを防ぐため、合理的に可能な限りの手段を講じ、かつそれが可能であるか確認していること。

(b) 当該時点で第 6 項の適用対象者であること。

(6) この項は、人が次に掲げる条件を満たす時は、いかなる時においてもその者に適用される。

(a) その者が再声明の公表を知らない場合

(b) その発表について知り、その再声明が公衆の耳目に触れなくなり、又は第 3 項(b)号に定めるように修正されることを確実なものにするための合理的に可能な限りのあらゆる措置を講じた場合

(7) この条の目的の上で、それ自体又は物若しくは記録の内容が以下のものとなるとき、声明又は物若しくは記録は、不法にテロリズムに関連しているとする。

(a) 当該公表物が利用提供された一又は複数の者に、テロリズム活動若しくは条約犯罪の実行、準備及び扇動を直接若しくは間接的に奨励し、又はその他誘引するものであると理解されうるもの

(b) 次に該当する情報

(i) 一又は複数の者にとって、テロリズム活動の実行及び準備に有用な情報

(ii) 情報が全体的に又は主として、その目的からいって非常に有用であると理解されうるような状態又は状況にある情報

(8) 第 7 項中、テロリズム活動若しくは条約犯罪の実行、準備又は扇動の間接的な奨励又はその他誘引であると理解されうるものへの言及は、次のいずれにも理解されうるものを含む。

(a)テロリズム活動の実行、準備（過去、未来又は一般的なものを問わず）の行為又は犯罪を賛美すること。

(b) 賛美対象が、現在の状況において模倣されるべき行為であるとして賛美されていると暗示していること。

(9) この条中、労働日（working day）とは次の日以外の日をいう。

(a) 土曜日又は日曜日

(b) クリスマス又は聖金曜日

(c) 連合王国内において、1971 年銀行金融取引法（Financial Dealings Act 1971（c. 80））に基づき、銀行休業日（bank holiday）である日

第 4 条　第 3 条に基づく通知

(1) 第 2 項から第 4 項までの規定が適用される場合を除き、次に掲げる態様に限定して、人に第 3 条第 3 項に基づく通知を行うことができる。

(a) 本人に交付することによる。

(b) 本人の最後に知られている住所宛に、書留郵便により送付することによる。

(2) 法人に対する通知は、次の態様で与えなければならない。

(a) 法人の事務部長に交付することによる。

(b) 法人の主たる事務所が登録された住所宛に、適切な者を受取人として、書留郵便により送付することによる。

(3) 企業に対する通知は、次の態様で与えなければならない。

(a) 企業の共同事業者に交付することによる。

(b) 共同事業の管理又は運営を執行する者に交付することによる。

(c) 共同事業の主たる事務所が登録された住所宛に、適切な者を受取人として、書留郵便により送付することによる。

(4) 法人格のない組織又は協会に対する通知は、次の態様で与えなければならない。

(a) 運営体の一員に交付することによる。

(b) 組織又は協会の主たる事務所が登録された住所宛に、適切な者を受取人として、書留郵便により送付することによる。

(5) 次の場合、この条における主たる事務所として言及されているものには、連合王国内における主たる事務所（あれば）を含む。

(a) 連合王国外で登録された企業

(b) 連合王国外で事業を営む企業

(c) 連合王国外に事務所を有する法人格のない組織又は協会

(6) この条中、「適切な人物（the appropriate person）」とは、次の者をいう。

(a) 法人の場合、組織自体又は事務部長

(b) 企業の場合、企業自体若しくは企業の共同事業者、又は共同体の管理又は運営を執行する者

(c) 法人格のない組織又は協会の場合、組織若しくは協会自体又は運営体の一員

(7) 第 3 条の目的の上で、同条第 3 項に基づく通知は、次の時間に交付されたものとみなす。

(a) 個人に交付された時は、交付された時間

(b) 書留配達を郵便送付した時は、配達時間として記録された時間

(8) この条中、「事務部長（secretary）」とは、法人に関して事務部長又はそれに相当する役職をいう。

3-4　ドイツ

3-4-1　「情報サービスおよび情報伝達サービスの枠組条件を規定するための法律」（通称マルチメディア法）と「テレメディア法」（通称インターネット法）との関係

「情報サービスおよび情報伝達サービスの枠組条件を規定するための法律」(Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste)は、1997 年 7 月 1 日に施行された。同法律は「マルチメディア法」とも称され、マルチメディア分野における法を新しい基盤におくことを目的としたものだった。上記の法律は、既存の法律（刑法、著作権法等）を改正する一方で、①「テレサービス法」（Gesetz über die Nutzung von Telediensten）、②「テレサービスに伴うデータ保護に関する法」（Gesetz über den Datenschutz bei Telediensten）、③「デジタル署名に関する法」（Gesetz zur digitalen Signatur）[84]の三法を新しく導入した。一般に向けて供されるサービスについては、「メディアサービス」として位置づけられ、当該立法権はドイツの各州にあることから、メディアサービスに関する規定は連邦法であるマルチメディア法に含まれず、その代わりにテレサービスと同様の規定を州間協定に置くこととなった。

2007 年 3 月 1 日に施行されたテレメディア法は、上記①、②の法律およびメディアサービスに関する州間協定の失効に伴い、それらの内容をほとんど変更せずに引き継いだ。（ただし、メディアサービスに関しては放送局州間協定に移行された規定もある。）従来の「テレサービス」と「メディアサービス」の語をもとに作られた、「テレメディア」という概念が新しく登場している。

これら法律の関係を図に示すと以下のようになる。

[84] 1997 年 7 月 22 日に施行、電子署名法の施行（2001 年 5 月 16 日）に伴い失効。新しい電子署名法の正式名称は、Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)。

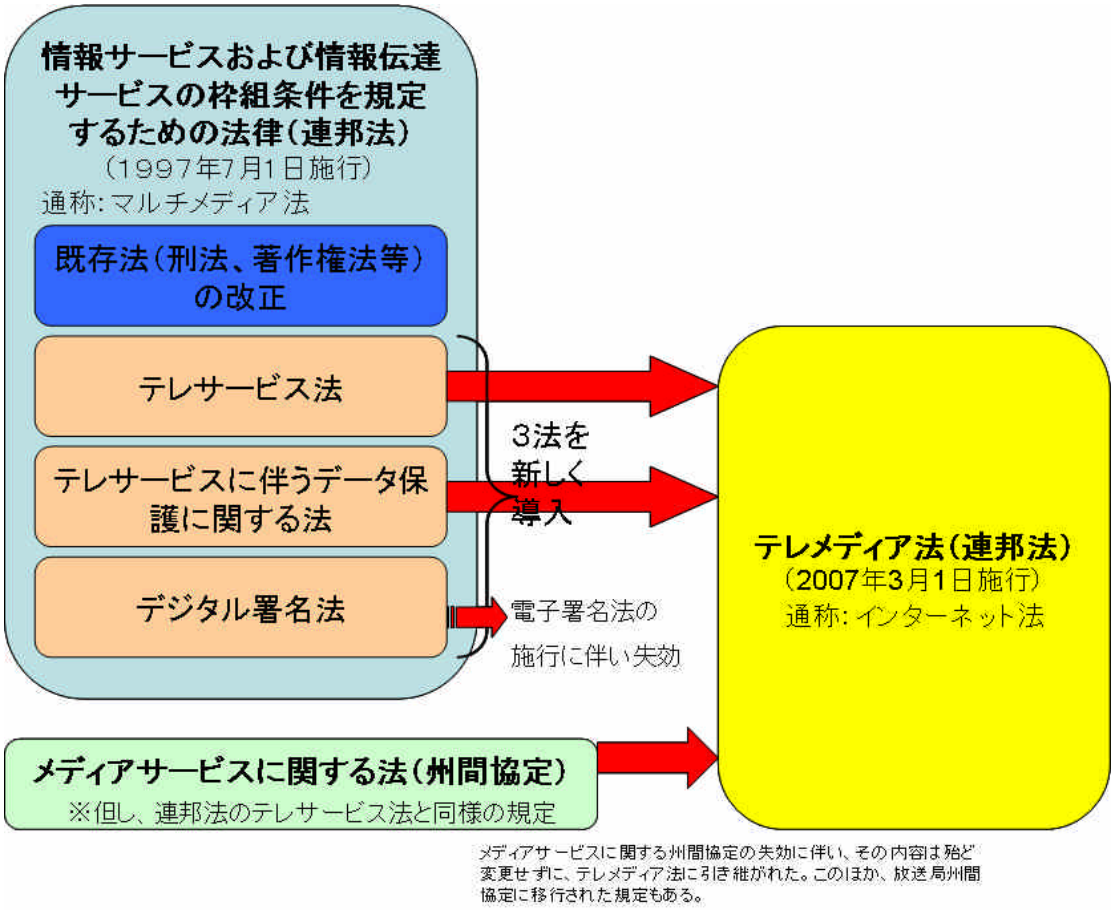

図 3　マルチメディア法とテレメディア法との関係

なお、「テレサービス」と「メディアサービス」と「テレメディア」の定義は以下のとおりである。

○「テレサービス」の定義（テレサービス法第 2 条第 1 項参照）：
「文字、画像、音等の組み合せたデータを個人利用するためのもので、かつ、テレコミュニケーションを通じた伝達を基礎とする電子情報サービスおよび電子通信サービス」

テレサービスの例（テレサービス法第 2 条第 2 項に例示列挙）：
- 個人間通信の分野におけるサービス提供（テレバンキング、情報交換等）
- 世論形成を目的とし、かつ、公衆のために編集した要素が強いものを除く（これはメディアサービスとして位置づけられる）、情報または通信に関するサービス提供（天気、交通等に関するデータサービス、製品等に関する情報の流布等）

- インターネットや他のネットワークの利用に関するサービス提供

○「メディアサービス」の定義（メディアサービス州間協定第 2 条第 1 項）：
「接続回線なしに電磁波を用いた、もしくは、回線に沿ってまたは回線を通じて伝える、文章、音、または画像による、一般に向けた情報サービスおよび通信サービス」
メディアサービスの例：
テレビや電話を通じたテレショッピング、ニュースレター、新聞のオンラインサービス、場合によっては個人の HP

メディアサービスに関しては各州が管轄を有すると判断されたため、州間協定が締結された。その内容は、テレサービス法の規定と大半一致している。

○「テレメディア」の定義（テレメディア法第 1 条第 1 項）
「通信法第 3 条第 24 号が定める通信サービス、通信法第 3 条第 25 号が定める通信に基づくサービスと、放送州間協定第 2 条が定める放送を除く、全ての電子情報サービスおよび電子通信サービス」

生ストリーミングやウェブラジオ等は未だに放送、インターネット電話等は未だに「電気通信」として位置づけられているが、このような例外を除くと、今までメディアサービスとして位置づけられていたもののほとんどはテレメディアの概念に含まれるようになった。そのため、この法律は俗称「インターネット法」と呼ばれている。

3-4-2　刑法（第 202 条、第 303 条）

（仮訳）

ドイツ刑法

Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S.3322),
zuletzt geändert durch Artikel 3 des Gesetzes vom 11.
März 2008 (BGBl. I S.306)

コンピュータ犯罪防止法が変更・追加した主な刑法規定

【刑法第 202 条 a　データの探知】

（1）権限がないのに、自己のために予定されておらず、かつ、無権限のアクセスに対して特別に保護されているデータに、アクセスに対する防護を克服した上で、自己でアクセスをした者又は他人によるアクセスを可能とした者は、3 年以下の自由刑又は罰金に処する。

（2）１項の意味におけるデータは、電子的、磁気的又はその他直接探知しえない形態で貯蔵され又は伝送されるものに限られる。

【ドイツ刑法第 202 条 b　データの傍受】

権限がないのに、自己又は他人のために、技術的方法を用いて、自己のために予定されていないデータ（第 202 a 条第 2 項）を、公開されていないデータの伝達過程又はデータ処理装置からの電磁的放射により取得した者は、2 年以下の自由刑又は罰金に処する。ただし、他の規定においてより重い刑の対象となっている場合は、この限りではない。

【ドイツ刑法第 202 条 c　データの探知及び傍受の準備】

（1） 次に揚げる行為により、第 202 条 a 及び第 202 条 b の犯罪行為の準備を行った者は、１年以下の自由刑又は罰金に処する。

1. データ（第 202 条 a 第 2 項）へのアクセスを可能とするパスワード又は他の防護コード、若しくは、
2. 前記の犯罪行為を行うことを目的とするコンピュータプログラム

を作成し、自己又は他人のために取得し、販売し、他人に譲り渡し、頒布し、又はその他アクセスを可能にすること

（2） 第 149 条第 2 項及び第 3 項の規定は、これを準用する。

【ドイツ刑法第 303 条 a　データ変更】

（1）データ（第 202 条 a 第 2 項）を違法に消去し、隠蔽し、使用不能にし、又は変更した者は、２年以下の自由刑又は罰金に処する。

（2）本条の未遂は罰する。

（3）第 202 条 c は、本条第 1 項の犯罪行為の準備について準用する。

【ドイツ刑法 303 条 b　コンピュータ妨害】

（1）次に揚げる行為により、他人にとって本質的に重要であるデータ処理を妨害した者は、3 年以下の自由刑又は罰金に処する。

1. 第 303 条 a 第 1 項の定める行為を行うこと
2. 他人に損害を与える目的をもってデータ（第 202 条 a 第 2 項）

を入力し又は伝達すること

3. データ処理装置又はデータ貯蔵媒体を破壊し、毀損し、使用不能にし、除去し又は変更すること

（2）データ処理が他人の経営体、他人の企業又は官庁にとって本質的に重要であるものの場合には、刑は5年以下の自由刑又は罰金とする。

（3）本条の未遂は罰する。

（4）本条第2項の事案が特に重大である場合、刑は6ヶ月以上10年以下の自由刑とする。特に重大な事案は、原則として、次に揚げる事案において肯定する。

1. 犯人が大規模の財産的損失をもたらした場合
2. 犯人が営利のために、又は、コンピュータ妨害を継続的に行うために結合した集団の一員として行動した場合
3. 行為によって、国民の生活にとって重要な製品又はサービスの供給、若しくは、ドイツ連邦共和国の安全を阻害した場合

（5）第202条cは、本条第1項の犯罪行為の準備について準用する。

3-4-3　通信法（第 113 条 a、第 113 条 b）

（仮訳）

通信法

Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198)

略称： Telekommunikationsgesetz 又は TKG

電気通信事業者に対するログ保存義務に関する規定

第 113 a 条[85]　データの保存義務

(1)　一般の利用に供する目的でエンドユーザのための通信サービスを提供する者は、エンドユーザがサービスを利用した際に作成または編成された通信データを、本条第 2 項から第 5 項に従い、国内または他の欧州連合の加盟国において 6 ヶ月間保存するものとする。自ら通信データを作成または編集しなくても、一般の利用に供する目的でエンドユーザのための通信サービスを提供する者は、データが本項第 1 文に従って保存されることを保障し、連邦ネット監督庁の請求に基づき、同庁にデータを保存している者を通知するものとする。

(2)　一般の利用に供する目的で電話サービスを提供する者は、次の情報を保存するものとする。

１．送信をしている接続及び送信を受けている接続の電話番号又は識別番号、そして切り換え又は伝送の場合は、その他関連する接続の電話番号又は識別番号

２．日時と時間帯による接続の開始及び終了

３．電話サービスにおいて様々なサービスの利用が可能である場合、利用されたサービスの表示

４．携帯電話サービスの場合は、さらに、

a) 携帯電話により送信をしている接続及び受信している接続の国際識別番号

b) 送信をしている及び受信している端末機器の国際識別番号

c) 送信をしている接続及び受信している接続を通じて接続開始時に使用された基地局エリアの表示

d) 前もって料金が支払われる匿名サービスの場合、時間帯、日時及び基地局エリアの表示サービスの開始

５．インターネット電話サービスの場合は、送信をしている接続及び受信してい

[85]第 113a 条は 2008 年 1 月 1 日をもって 2007 年 12 月 21 日の法律により挿入（連邦官報 I 3198 頁）

る接続の IP アドレス

本項第１文は、ショート通信、マルチメディア通信、その他同様の通信を伝送する場合に準用する。この場合は、本項第１文第 2 号の表示に代えて、メールの送信時間及び受信時間を保存するものとする。

(３)　電子郵便サービスを提供する者は、次の情報を保存するものとする。

１．　通信を送信する場合は、電子私書箱の識別番号、送信者の IP アドレス、そして通信受信者全ての電子私書箱の識別番号

２．　通信が電子私書箱に受信される場合は、送信者及び通信の受信者の電子私書箱の識別番号、そして送信した通信装置の IP アドレス

３．　電子私書箱に接続する場合は、その識別番号、及び接続者の IP アドレス

４．　日時と時間帯による接続の開始及び終了を表示する第１号から第３号に定められたサービスの利用時間

(４)　インターネットへのアクセスサービスを提供する者は、次の情報を保存するものとする。

１．　インターネット利用のために利用者に割り当てられた IP アドレス

２．　インターネットの利用が可能となる接続の明確な識別番号

３．　割り当て IP アドレスを通じたインターネット利用の開始及び終了につき、その日時及び時間帯

(５)　電話サービスを提供する者が、電話への応答がなかった場合またはネットワーク管理者の介入により電話がつながらなかった場合であっても、本条の定める通信データを第 96 条第 2 項の規定する目的のために保存または記録したときには、通信データを本条に従い保存するものとする。

(６)　通信サービスを提供し、この際に本条により保存しなければならないデータを変更した者は、変更前のデータ及び変更後のデータ、ならびに、データ変更を実行した日時及び時間帯を保存しなければならない。

(７)　一般の利用に供する目的で携帯電話網を運営する者は、本規定に従い保存された基地局エリアの表示の他に、それぞれの基地局エリアに設置された通信アンテナ及び主要な送信方向の地理的状況がわかるデータも保存しなければならない。

(８)　通信内容及び接続したインターネットサイトに関するデータは、本条を理由として保存してはならない。

(９)　本条第１項から第 7 項に基づくデータの保存は、権限を有する当局が情報の開示を請求したときは、遅滞なくこれに応えられるように行わなければならない。

(１０)　本条義務を負う者は、保存された通信データの品質と保護に関して、通信分野において通常必要とされる注意を払わなければならない。この場合、義務を負う者は、保存されたデータにアクセスできるのは本人により特別に権限を与えられた者に限定されるよう技術的かつ組織的措置をとらなければならない。

(１１) 本条義務を負う者は、本条のみを根拠として保存したデータを、本条第１項に定める期間の経過後１ヶ月以内に消去し、または消去を保障するものとする。

第 113ｂ条[86]　第 113ａ条により保存されたデータの利用

第 113ａ条の義務を負う者は、第 113ａ条に規定された保存義務のみに基づいて、保存されたデータを、

１．　犯罪行為の摘発のため、

２．　公共の安全が著しく危険にさらされることを予防するため、

３．　連邦憲法擁護庁、州憲法擁護庁、連邦情報局及び軍防諜機関が法律で定められた任務を遂行するため、

管轄当局より請求がなされたときは、第 113ａ条に関連しそれぞれの法律の規定に定めがあり、提供が個別に命じられている場合には、これらの当局に提供することができる。その他の目的には、第 113 条による情報提供を除き、これらのデータを利用してはならない。第 113 条第１項第４文の規定は、これを準用する。

[86]第 113b 条は 2008 年 1 月 1 日をもって 2007 年 12 月 21 日の法律により挿入（連邦官報Ⅰ3198 頁）

3-5　韓国

3-5-1　情報通信網利用促進及び情報保護等に関する法律（抄）

（仮訳）

情報通信網利用促進及び情報保護等に関する法律（抄）

第 44 条の 5 (掲示板利用者の本人確認)

1　以下に該当する者が掲示板を設置、運営しようとする場合には、掲示板利用者の本人確認のための方法、手続を決定する等、大統領令に定めてある必要な措置を講じなければならない。

(1) 国家機関、地方自治体、政府投資機関、政府傘下にある機関、地方公社及び地方公団

(2) 情報通信サービス事業者として提供する情報通信サービスの一日の平均利用者数 10 万人以上で、大統領令に定めてある基準に該当するもの。

2　情報通信部長官は、第 1 項第 2 号の規定による基準に該当する情報通信サービス提供者が本人確認措置をしない場合、本人確認措置をするよう命ずることができる。

3　政府は第 1 項による本人確認のために安全、かつ、信頼できるシステム開発のための施策を講じなければならない。

4　公共機関等、及び情報通信サービス事業者が善管注意義務に基づき、第 1 項の規定による本人確認措置を行った場合には、利用者名義の第三者の不正使用によって発生した損害に対する賠償責任を軽減若しくは免除することができる。

3-5-2　情報通信網利用促進及び情報保護等に関する法律の施行令（抄）

（仮訳）

情報通信網利用促進及び情報保護等に関する法律の施行令（抄）

第 22 条の 2 (本人確認措置等)

1　法第 44 条の 5 第 1 項における「大統領令が定める必要な措置」とは、以下を意味する。

(1) 公認認証機関、信用情報取扱い業者、その他本人確認サービスを提供する第三者に依頼或いは、模写電送、対面確認等を通じて掲示板利用者が本人であることを確認することのできる手続の整備

(2) 本人確認の手続、及び本人確認に関する情報の保管時に、当該本人確認情報の流出を防止できる技術の整備

2　法第 44 条の 5 第 1 項の各号に規定のある公共機関及び情報通信サービス提供者は本人確認関連の情報を 6 カ月間保存しなければならない。

第 22 条の 3(情報通信サービス提供者における本人確認措置義務者の範囲)

1　法第 44 条の 5 第 1 項第 2 号における「大統領令が定める基準に該当するもの」とは以下を意味する。

(1) 前年度末基準において、直前 3 カ月間のポータルサービス(インターネットアドレス、情報等の検索及び電子メール、通信等を提供するサービス)の、一日の平均利用者数が 30 万人以上の情報通信サービス事業者

(2) 前年度末基準で直前 3 ヶ月間のインターネット言論サービスの、一日の平均利用者数が 20 万人以上の情報通信サービス事業者

(3) 前年度末基準で直前 3 カ月間の製作物専門媒体サービス(利用者が自ら製作したデジタルコンテンツを専門職に媒体するサービス) の、一日の平均利用者数が 30 万人以上の情報通信サービス事業者

2　情報通信部長官は第 1 項の規定されている「大統領令で定める基準に該当するもの」及び本人確認措置に必要な猶予期間、適用期間等をインターネットホームページに掲示する方法によって公示する。

3-6　日本

3-6-1　刑法改正案（抄）

ウイルス製造・流通・頒布を取り締まるための刑法の改正案は、以下のとおりである。

出典：http://www.moj.go.jp/HOUAN/KEIHO5/refer02.html

犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律(案)

（該当条文のみ引用）

第十九章の二　不正指令電磁的記録に関する罪

（不正指令電磁的記録作成等）

第百六十八条の二　人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。

一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録

二　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録

2　前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。

3　前項の罪の未遂は、罰する。

（不正指令電磁的記録取得等）

第百六十八条の三　前条第一項の目的で、同項各号に掲げる電磁的記録その他の記録を取得し、又は保管した者は、二年以下の懲役又は三十万円以下の罰金に処する。

第百七十五条中「図画」の下に「、電磁的記録に係る記録媒体」を加え、「、販売し」を削り、「又は二百五十万円以下の罰金若しくは科料に処する」を「若しくは二百五十万円以下の罰金若しくは科料に処し、又は懲役及び罰金を併科する」に改め、同条後段を次のように改める。

電気通信の送信によりわいせつな電磁的記録その他の記録を頒布した者も、同様とする。

第百七十五条に次の一項を加える。

2　有償で頒布する目的で、前項の物を所持し、又は同項の電磁的記録を保管した者も、同項と同様とする。

第二百三十四条の二に次の一項を加える。

2　前項の罪の未遂は、罰する。