Title	報告一 : 情報セキュリティの法的保護 : 刑事法的視点から
Sub Title	
Author	安冨, 潔(Yasutomi, Kiyoshi)
Publisher	慶應義塾大学法学研究会
Publication year	2015
Jtitle	法學研究 : 法律・政治・社会 (Journal of law, politics, and sociology). Vol.88, No.2 (2015. 2) ,p.73- 82
JaLC DOI	
Abstract	
Notes	特別記事 : 平成二六年度慶應法学会シンポジウム インターネット社会における法と政治
Genre	Journal Article
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=AN00224504-20150228-0073

報告一

情報セキュリティの法的保護
――刑事法的視点から――

名誉教授　安冨　潔

1　はじめに

情報通信技術は、今日の社会にとって、市民生活や社会経済活動に不可欠なインフラ・ストラクチュアとして定着し、サイバー空間は市民の日常生活を支えている。しかし、情報通信技術の発達にともなって、さまざまな情報通信技術を悪用した犯罪や不正行為も多発している。いわゆるサイバー犯罪と定義される「高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪」だけでなく、政府機関や重要インフラ事業者等の基幹システムの機能不全に陥らせるサイバーテロや情報通信技術を用いて政府機関や先端技術を有する企業から機密情報を窃取するサイバーインテリジェンスといったサイバー攻撃も世界的規模で頻発し、サイバー空間における脅威は深刻化している状況にある(1)。

警察庁の公表したところでは、二〇一三年のサイバー犯罪の検挙件数は八一一三件と、前年より七七九件（一〇・六％）増加して過去最多であった。ことに、不正アクセス行為は、認知件数二九五一件（前年比一七〇〇件増）、検挙件数九八〇件（四三七件増）であり、インターネットバンキングの不正送金が一三二五件（四四・九％）と約半数を占めていることが特徴である。また、二〇一二年五月から新たに処罰対象となった識別符号取得行為、識別符号保管行為は、それぞれ二件、フィッシング行為は一件検挙されている。

サイバー犯罪は、一般に、①犯罪の痕跡となる証拠を人の五官の作用で直接知覚することができない（不可視性）、②実行行為者はＩＤ・パスワードなどの電磁的記録によって識別される（匿名性）、③犯人性を特定する指紋、足跡などの物理的痕跡が残らず証拠隠滅が容易である（無痕跡性）、という特色がある。(2)

最近のサイバー犯罪では、高度匿名化技術を利用したり、標的型攻撃によるサイバー攻撃がみられる。

二〇一二年六月から九月にかけて発生したインターネットを利用した犯行予告・ウイルス供用事件では、被告人は、ＴＯＲ（The Onion Router）と呼ばれる高度匿名化技術を悪用してインターネット掲示板に殺害予告等の書き込みを多数行った。それ以外にも、これまで、ＴＯＲを悪用してインターネットバンキングに不正アクセスし、他人の口座から不正送金を行って、多額の現金を引き出した事案（平成二二年未検挙）や、同じくＴＯＲを悪用して出会い系サイトの掲示板に、児童を異性交際の相手方となるように誘引する書き込みを行った事案（平成二二年未検挙）も発生している。

ＴＯＲという技術は、もともと米海軍調査研究所において開発された技術で、今日では、情報統制が行われている海外の国々において国民の表現の自由の保護等、インターネット上での自由な活動と当該活動におけるプライバシーの保護等の目的で利用されている。他方、ＴＯＲは、インターネット上でフリーソフトウェアとして公開されており誰でもダウンロードが可能であることから、さまざまな事案で悪用されている。ＴＯＲは、通信履歴をそもそも残さない設定とされていることから事後的な追跡は困難である。

また、標的型攻撃によるサイバー攻撃は、攻撃対象のコンピュータに複数のコンピュータから一斉に大量のデータを送信して負荷を掛けるなどして、そのコンピュータによるサービスの提供を不可能にするＤＤｏＳ攻撃や、セキュリティ上の脆弱性を悪用してコンピュータに不正に侵入し、又は不正プログラムに感染させることなどにより、管理者や利用者の意図しない動作をコンピュータに命令する手法等がある。この不正プログラムに感染させる手口として、業務に関連した正当な電子メールを装い、市販のウイルス対策ソフトでは検知できない不正プログラムを添付した電子メール（標的型メール）を送信し、受信者のコンピュータを不正プログラムに感染させる標的型メール

攻撃が多発している。

標的型メール攻撃には、多数の送信先に同一の文面及び不正プログラムを添付したメールを一斉に送信する「ばらまき型」、業務等に関係する内容を装って複数回にわたりメールのやり取りを行い、標的を信用させた後に不正プログラムを添付したメールを送信する「やり取り型」がある。その他、標的が頻繁に閲覧するウェブサイトに不正プログラムを蔵置し、標的がウェブサイトの閲覧に使用したコンピュータを不正プログラムに感染させる、「水飲み場型攻撃」と呼ばれる手口もある(3)。

このように、さまざまなサイバー攻撃により、サイバー空間における脅威の深刻度はいっそう増加している。

そこで、脅威を分析し、その脆弱性に対して対策をとる必要がある。

2　情報セキュリティとその侵害

(1)　情報セキュリティの意義

「情報セキュリティ」は、情報資産の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を維持することを三要素とする理解が一般的である(4)。

ア　機密性とは、アクセスすることが許された者だけが情報にアクセスできることを確実にしておくこと。

イ　完全性とは、情報及び処理方法が、正確であること（改ざんされていない状態）及び完全であること（消去されていない状態）を確実にしておくこと。

ウ　可用性とは、アクセスが許された者が、必要なときに、情報及び関連資産にアクセスできる状態を確実にしておくこと。

である。

(2)　情報セキュリティ侵害

サイバー空間への攻撃は、情報セキュリティにおける三要素の侵害として整理される。

ア　機密性の侵害

①　不正アクセス＝コンピュータへの正規のアクセス権を持たない人が、ソフトウェアの不具合などを悪用してアクセス権を取得し、不正にコンピュータを利用する、あるいは試みること(5)。

②　情報漏洩＝企業等の保有する顧客情報や取

引情報、経営情報などの機密情報が、盗難や不注意により外部に流出すること。

イ　完全性の侵害

①　情報の改ざん＝企業等の保有する情報を書き換えること。

②　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、自己伝染機能、潜伏機能、発病機能を一つ以上有するもの。

刑法一六八条の二では、「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」と定義する。

ウ　可用性の侵害

①　サービス妨害＝ネットワークを通じた攻撃の一つ。相手のコンピュータやルータなどに不正なデータを送信して使用不能に陥らせたり、トラフィックを増大させて相手のネットワークを麻痺させる攻撃（ＤｏＳ攻撃＝ Denial of Service attack）、さらに複数のネットワークに分散する大量のコンピュータが一斉に特定のネットワークやコンピュータへ接続要求を送出し、通信容量をあふれさせて機能を停止させてしまう攻撃（ＤＤｏＳ＝ Distributed Denial of Service attack）[6]。

②　システム侵害＝情報システムを構成する機材やソフトウェアなどに問題が発生し、正常な稼働状態を維持できなくなること。また、その原因となった問題や不具合のこと。

などである。

3　情報セキュリティの刑事法的保護

情報セキュリティの保護は、技術的手段や法的手段が総合的になされる必要がある。

ここでは、法的手段、ことに刑事法的保護という観点からまとめておくこととする。

我が国では、サイバー犯罪に対する刑事法として、刑法（明治四〇年法律第四五号）、不正アクセス行為の禁止等に関する法律（平成一一年法律第一二八号）、不正競争防止法（平成五年法律第四七号）などがある。

一九八七年の「刑法等の一部を改正する法律」による刑法の一部改正では、「コンピュータ」に対する法

的保護が図られた。その結果、周知のとおり、電磁的記録を「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう」（七条の二）と定義するとともに、電磁的記録不正作出及び供用罪（一六一条の二）、電子計算機損壊等業務妨害罪（二三四条の二）、電子計算機使用詐欺罪（二四六条の二）が新設され、公正証書原本等不正作出罪（一五七条）、公用文書等毀棄罪（二五八条）及び私用文書等毀棄罪（二五九条）の客体に電磁的記録が追加された。その後、カード犯罪の増加に伴い、二〇〇一年の「刑法等の一部を改正する法律」による刑法一部改正により、支払用カード電磁的記録に関する罪（一六三条の二～一六三条の五）が新設された。

また、一九八七年の刑法一部改正の際には、まだインターネットが普及しているとはいえない時代背景から、法律で定められなかった不正アクセスについては、その後のネットワーク利用犯罪の脅威に対処するために、一九九九年に、不正アクセス禁止法として、新たに法整備が図られた。

このような立法状況にあって、情報セキュリティの保護という視点からは、不正アクセス禁止法が、技術的基準とは異なるものの、一定の不正アクセス行為に対してこれを規制対象としていることから、機密性の保護に機能しているといえる。そして、刑法の公正証書原本等不正作出罪、電磁的記録不正作出及び供用罪や電子計算機使用詐欺罪は、主として、完全性を保護する機能を有しているといえるし、電子計算機損壊等業務妨害罪、公用文書等毀棄罪及び私用文書等毀棄罪は、可用性の保護に機能しているといえよう。もっとも、機密性については、一九八七年の刑法一部改正の際には、保護すべき情報の範囲、保護の程度等について検討を要する問題が少なくないとして、緊急の立法的手当をするうえでは適当でないということで立法が先送りされた。その結果、いわゆる情報漏洩という機密性の保護については、刑法に新たな規定が設けられず、不正競争防止法による営業秘密の保護という範囲で保護が図られるにとどまっている。

その後、ネットワークの発達に伴い、国境を越えたさまざまなサイバー空間における脆弱性に対する攻撃がみられるようになり、二〇〇一年九月に、欧州評議会において、「サイバー犯罪に関する条約」が採択さ

れた。この条約は、サイバー犯罪と効果的に戦うための国際協力についての措置を定めた条約である。サイバー犯罪条約は、前文で「コンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの秘密性、完全性及び利用可能性に対して向けられた行為並びにコンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの濫用を抑止するために、この条約が必要である」と述べ、「秘密性、完全性及び利用可能性」という情報セキュリティの保護に関心を寄せて、実体法及び手続法の整備を求めている。

我が国も二〇〇一年一一月にこの条約に署名し、二〇〇四年に国会において承認された。しかし、条約批准のための国内での法整備が遅れ、二〇一一年になって「情報処理の高度化等に対処するための刑法等の一部を改正する法律案」が提出され、コンピュータ・ウイルス対策として不正指令電磁的記録に関する罪（一六八条の二、一六八条の三）が新設され、刑事手続きにおいてもサイバー犯罪の捜査を目的とした規定が設けられた。さらに、いわゆるフィッシング行為を禁止することを目的に不正アクセス禁止法の改正（第七条、第一二条第四号関係）もなされた(7)。

4　おわりに

我が国では、情報社会の到来を想定して、二〇〇一年に高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進することを目的として「高度情報通信ネットワーク社会形成基本法」が施行された。

情報通信技術は、今日の社会にとってのインフラストラクチュアとしてますます発展を遂げつつある。市民生活に重大な影響を与える重要インフラなどに対する巧妙なサイバー攻撃もあとを絶たない。それだけに、さまざまなサイバー攻撃に対して、適切な対策をとることが重要であることはいうまでもない。しかしながら、あらゆる起こりうる事象に対してあらかじめ対処方法を策定しておくことは現実には困難である。

そうだとしても、過去に発生した事象をふまえて、その原因を分析し、サイバー攻撃対策をできる限り実施しておくことは企業や組織体にとって社会的責任を果たすうえで必要といえよう。

サイバー攻撃への対策は、情報セキュリティの保護

を目的とする。

そのためには、構築された管理体制のもとで策定された情報セキュリティポリシーにしたがって、適切に運用していくことが求められる。とはいえ、脆弱性を悪用した、情報セキュリティへの脅威を惹起する新たなサイバー攻撃がつぎつぎと登場してきている。

サイバー攻撃は、企業や組織体への攻撃だけではなく、その企業や組織体に関係する市民に対しても深刻な影響を与える。

企業や組織体は、攻撃に対するリスクアセスメントを行い、攻撃に対する内部要因、外部要因の分析と対応を検討するとともに、インシデントレスポンスに対する体制の整備をしておく必要があろう。すなわち、外部からの攻撃を受けないための方策、攻撃による情報漏洩や不正プログラムへの感染に対処する方策、サイバー攻撃によるデータの窃取、改ざん、破壊及びシステムの機能不全に陥らないようにするための方策が検討されるべきである。また、サイバー攻撃によるインシデントが発生した場合、被害の最小化を図り、システムの脆弱性と攻撃態様を特定し、被害の回復を図るとともに、あらかじめ定めた業務継続の手順にしたがってできるだけ迅速に対処する必要がある。

ここでは、デジタル・フォレンジック[8]が有用である。もっとも、事後的対応として用いられたデジタル・フォレンジックの成果は、サイバーセキュリティポリシーの策定に活かされなければ意味がない。

他方、企業や組織体に関係する市民も、自己のＩＴリテラシーやセキュリティ意識を向上させておく必要があろう。もっとも、サイバー空間における市民の情報格差は避けられない。政府においても市民のＩＴリテラシーやセキュリティ意識の向上を図るように努めることが望まれよう。

サイバー空間においては、ネットワークで接続されていれば、いずれかのシステムにおける機能不全は、他のシステムへの影響を避けられない。

今後は、サイバー攻撃に関する官民における情報共有体制や共同対応機関の検討を含めて総合的な情報セキュリティ対策がなされることを期待したい。

（1）二〇〇九年から二〇一三年までのサイバー犯罪の検挙状況は、別表の通りである。http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf

（2）大橋充直『ハイテク犯罪捜査入門―基礎編―』四～五頁（東京法令出版・二〇〇四）参照。

（3）【事例1】農林水産省における情報流出事案（二五年一月判明）

農林水産省のコンピュータが不正プログラムに感染し、平成二三年から二四年までの間、ＴＰＰ交渉に関係するものを含む内部文書等が外部に流出した可能性があることが、二五年一月に報じられた。その後、同年五月には、同省が設置した第三者委員会の中間報告において、二四年一月から四月までに五台のパソコンから一二四点の文書が流出した痕跡が確認されたことなどが発表されている。

【事例2】宇宙航空研究開発機構における情報流出事案（二五年四月発生）

四月、宇宙航空研究開発機構（ＪＡＸＡ）が管理するサーバが不正アクセスを受け、国際宇宙ステーション日本実験棟「きぼう」及び宇宙ステーション補給機「こうのとり」の運用準備に係る技術情報並びに関係者の個人メールアドレス等が流出したことがＪＡＸＡの調査により明らかになった。

【事例3】韓国の銀行等に対するサイバー攻撃事案（二五年三月及び六月発生）

韓国では、三月、複数の金融機関及び放送局において、不正プログラムが同時多発的に作動し、数万台に及ぶコンピュータが機能不全を起こしました。その結果、ＡＴＭやオンラインバンキングが停止したほか、ニュース原稿の作成や編集作業に影響が生じ、社会経済活動に大きな影響が生じた。また、六月には複数の政府機関等のウェブサイトが、改ざん及びＤＤｏＳ攻撃の被害を受けたほか、政府関係者等の個人情報が流出した。

（4）JIS Q 27002:2006.

ＯＥＣＤが一九九二年に公表した「情報セキュリティに関するガイドライン」では、情報セキュリティの目的は、情報システムに依存する者を機密性、完全性、可用性の欠如に起因する危害から保護することであると定義している（OECD Guidelines for the Security of Information Systems）。

（5）代表的な不正アクセスには、ソフトウェアの保安上の弱点（セキュリティホール）を悪用してファイルを盗み見たり削除・改変する行為や、盗聴や総当たり攻撃によるパスワード窃取、メールサーバを悪用した迷惑メールのばらまきなどがある。

（6）電子掲示板（ＢＢＳ）などで参加者を募って大

サイバー犯罪の検挙状況について

罪名＼年	H21	H22	H23	H24	H25	前年比増減	
不正アクセス禁止法違反	2,534	1,601	248	543	980	+ 437	+ 80.5%
コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪	195	133	105	178	478	+ 300	+ 168.5%
電子計算機使用詐欺	169	91	79	95	388	+ 293	+ 308.4%
電磁的記録不正作出・毀棄等	22	36	17	35	56	+ 21	+ 60.0%
電子計算機損壊等業務妨害	4	6	6	7	7	± 0	−
不正指令電磁的記録作成・提供	−	−	0	4	8	+ 4	+ 100.0%
不正指令電磁的記録供用	−	−	1	34	14	− 20	− 58.8%
不正指令電磁的記録取得・保管	−	−	2	3	5	+ 2	+ 66.7%
ネットワーク利用犯罪	3,961	5,199	5,388	6,613	6,655	+ 42	+ 0.6%
詐欺	1,280	1,566	899	1,357	956	− 401	− 29.6%
うちオークション利用詐欺	522	677	389	235	158	− 77	− 32.8%
児童買春・児童ポルノ法違反（児童ポルノ）	507	783	883	1,085	1,124	+ 39	+ 3.6%
わいせつ物頒布等	140	218	699	929	781	− 148	− 15.9%
著作権法違反	188	368	409	472	731	+ 259	+ 54.9%
青少年保護育成条例違反	326	481	434	520	690	+ 170	+ 32.7%
児童買春・児童ポルノ法違反（児童買春）	416	410	444	435	492	+ 57	+ 13.1%
出会い系サイト規制法違反	349	412	464	363	339	− 24	− 6.6%
商標法違反	126	119	212	184	197	+ 13	+ 7.1%
その他	629	842	944	1,268	1,345	+ 77	+ 6.1%
合　計	6,690	6,933	5,741	7,334	8,113	+ 779	+ 10.6%

※　その他には、名誉毀損、脅迫、覚せい剤取締法違反等の薬物事犯、売春防止法、児童福祉法、犯罪収益移転防止法等の違反がある。

※　ネットワーク利用犯罪の定義

犯罪の構成要件に該当する行為についてネットワークを利用した犯罪、又は構成要件該当行為でないものの、犯罪の実行に必要不可欠な手段としてネットワークを利用した犯罪をいう。例えば、児童買春及び青少年保護育成条例違反については、ネットワーク上で連絡を取り合った者同士がネットワーク上において性交等に合意している場合に限って計上している。

勢の攻撃者が意図的に一斉に攻撃を実行する場合と、コンピュータや通信機器が攻撃者に乗っ取られ、所有者の知らないうちに攻撃に参加させられてしまう場合がある。

後者の場合、攻撃者は攻撃対象とは無関係な多数のコンピュータに侵入し、その管理者や利用者に気づかれないように攻撃実行用のプログラム（トロイの木馬など）をこっそりしかける。攻撃を開始する時には、あらかじめ仕掛けたプログラムに対して、一斉に接続要求データの送出命令を発行する。標的となったコンピュータには、乗っ取られたコンピュータから要求が送られてくるため、真の攻撃元である「黒幕」のコンピュータを割り出すことは難しい。ＤＤｏＳによる妨害アクセスは通常のアクセスと見分けがつきにくく、選択的に排除するのが難しいことが多い。このため、標的のサーバにセキュリティ上の弱点を放置するなどの管理のミスがなくても被害が発生してしまう。ＤＤｏＳを阻止するためには、攻撃者に不正なソフトウェアを仕掛けられないよう各コンピュータの管理者や利用者が注意する必要がある。

（7）二〇〇三年に出会い系サイトの利用に起因した犯罪に対する「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」が制定された。

（8）インシデントレスポンス（コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等をいう。）や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術をいう。https://digitalforensic.jp/home/what-df/