

2009年11月19日

関西大学法科大学院 法と社会2「法とメディア」第8回

インターネットメディア犯罪（その2）

弁護士・弁理士 近 藤 剛 史

tsuyoshi@kondolaw.jp

I 前回設問の補足説明

- 1 朝日新聞HP改ざん事件（大阪地裁平成9年10月3日判決、判タ980号285頁）
大阪朝日放送のホームページの天気予報の一部をわいせつな画像に改ざんしたとして、電子計算機損壊等業務妨害、わいせつ図画公然陳列罪に問われた事件。

「被告人は、大阪市北区大淀南二丁目二番四八号所在の朝日放送株式会社がインターネット利用者に提供するため開設したホームページ内の天気予報画像を消去してわいせつな画像等に置き換え、同会社の情報提供業務を妨害するとともに、わいせつな画像を不特定多数のインターネット利用者に閲覧させようと企て、平成九年五月一八日、埼玉県富士見市（住所略）の当時の自宅において、インターネットを利用して、右朝日放送株式会社内に設置されたサーバコンピュータの記憶装置であるハードディスク内に記憶・蔵置されていた天気予報画像のデータファイル九個を消去して損壊するとともに、女性の性器を露骨に撮影したわいせつな画像のデータファイル五個を含む画像のデータファイル九個を、消去した右天気予報画像のデータファイルと同一のファイル名を付して、右サーバコンピュータに順次送信するなどし、右ハードディスク内に記憶・蔵置させ、右サーバコンピュータが、不特定多数のインターネット利用者に対し、右天気予報画像のデータファイル九個分のデータを提供しようとした場合には、これに代えて新たに記憶・蔵置させたデータファイル九個分のデータを提供する結果となり、右利用者らが右わいせつな画像のデータファイル五個分のデータを受信してこれを再生閲覧することが可能な状況を設定し、右ホームページにアクセスしてきたAら不特定多数の者にこれを再生閲覧させ、もって、人の業務に使用する電子計算機の用に供する電磁的記録を損壊し、かつ、同電子計算機に虚偽の情報を与え、電子計算機に使用目的に反する動作をさせて、人の業務を妨害するとともにわいせつな図画を公然と陳列したものである。」

「(法令の適用) 被告人の判示所為中電子計算機損壊等業務妨害の点は刑法二三四条の二に、わいせつ図画公然陳列の点は同法一七五条前段にそれぞれ該当するが、右は一個の行為で二個の罪名に触れる場合であるから、同法五四条一項前段、一〇

条により一罪として重い電子計算機損壊等業務妨害罪の刑で処断することとし、所
定刑中懲役刑を選択し、その所定刑期の範囲内で被告人を懲役一年六月に処し、情
状により同法二五条一項を適用してこの裁判確定の日から三年間右刑の執行を猶予
することとする。」

2 FLマスク事件（大阪地裁平成11年3月19日、判タ1034号283頁）

「本件の罪における「わいせつ図画」とは、必ずしもその物自体にわいせつ性が顕
在していることを必要とするものではなく、一定の技術的操作を施すことにより、
その物に潜在するわいせつ性を外部的に認識できる程度に顕在化させることが比較
的容易であると認められる場合には、その物は本件の罪の客体である「わいせつ図
画」に該当すると解すべきであるところ、本件においては、わいせつ性の認められ
る画像データはサーバーコンピュータのディスクアレイ内に記憶、蔵置されてい
て直ちには視認できないものの、前記のとおり、インターネット利用者にとってこ
れを視認できるように顕在化させることは容易になし得ると認められるのであるか
ら、右ディスクアレイを「わいせつ図画」と解するのが相当である。」

「わいせつ図画を「公然と陳列した」というためには、わいせつ図画を不特定又は
多数の者にとって観覧可能な状態に置くことで足りると解するのが相当であるところ、
本件においては、被告人は、わいせつ画像データ又はマスク処理ソフトの利用、
入手に係るホームページのリンク情報とマスク処理を施してわいせつ性を隠蔽させ
た画像データをインターネット通信のプロバイダーのサーバーコンピュータに送
信して、同コンピュータのディスクアレイに記憶、蔵置させるとともに、右わい
せつ画像等をダウンロードできるホームページを作成して開設したところ、さらに、
他のホームページと相互にリンクさせたり、サーチエンジンに登録したりして、一
般ないし多数の会員に向けて公開していたとの事情も相俟って、不特定又は多数の
インターネット利用者が、右わいせつ画像データ等の存在を知り得、右わいせつ画
像データ等に容易にアクセスしてこれをダウンロードし、自己のパソコンの画面上
にて再生したり、マスクを外したりして、わいせつ画像を再生閲覧した状態が生じ
ていたものということができるから、被告人がわいせつ画像データ等をそのダウン
ロードを可能とする被告人開設のホームページのあるプロバイダーのサーバーコン
ピューターに送信し、同コンピュータのディスクアレイに記憶、蔵置させた行為
をもって、わいせつ図画を「公然と陳列した」ものと認めることができる」

「被告人が、海外プロバイダーであるユーエス・インターネットのサーバーコンピ
ューターに会員用のわいせつ画像データを送信し、同コンピュータのディスクア
レイに記憶、蔵置させた行為は、たとえ同コンピュータのディスクアレイの所在
場所が日本国外であったとしても、それ自体として刑法一七五条が保護法益とする
我が国の健全な性秩序ないし性風俗等を侵害する現実的、具体的危険性を有する行

為であって、わいせつ図画公然陳列罪の実行行為の重要部分に他ならないといえる。したがって、被告人が右のような行為を日本国内において行ったものである以上、本件については刑法一七五条を適用することができる。」

「一般に、我が国の刑法の場所的適用範囲については、犯罪構成要件の実行行為の一部が日本国内で行われ、あるいは犯罪構成要件の一部である結果が日本国内で発生した場合には、我が国の刑法典を適用しうると解すべきところ、インターネット通信においては、誰でもダウンロードすることを可能とするデータを伴うホームページの開設者が自己のパソコンからそのダウンロード用のデータをプロバイダーにあてて送信すれば、たとえそれが海外のプロバイダーに対して向けられたものであっても、瞬時にそのプロバイダーのサーバーコンピューターに記憶、蔵置され、その時点からは、日本国内からでも、右データに容易にアクセスしてダウンロードすることが可能となるものであり、本件では、被告人が、日本国内からアメリカ合衆国国内に事務所をおくプロバイダーであるユーエス・インターネットの管理するサーバーコンピューターに会員用画像データを送信して記憶、蔵置させているが、右会員用画像データに対しては、会員となってIDとパスワードを取得しさえすれば、日本国内からでも容易にアクセスし得、右会員用画像を閲覧することができるようになっていた上、ユーエス・インターネットに開設された会員用画像データを含む会員用ホームページは、日本国内のプロバイダーに開設された本件ホームページの会員用ページとして開設されたもので、その内容は日本語で構成され、本件ホームページから直接移動できるようにリンクされており、その会員も本件ホームページで募集していたものであるから、右会員用画像データは、当初から、専ら日本国内の者が閲覧することが予定され、しかも、それが容易に可能となる措置も講じられていたものといえることができ、実際にも右会員用画像データにアクセスしてこれを閲覧した者の殆どは日本国内の者であったことは、被告人自身も認めているところである。

以上に鑑みると、本件において、被告人が、海外プロバイダーであるユーエス・インターネットのサーバーコンピューターに会員用のわいせつ画像データを送信し、同コンピューターのディスクアレイに記憶、蔵置させた行為は、たとえ同コンピューターのディスクアレイの所在場所が日本国外であったとしても、それ自体として刑法一七五条が保護法益とする我が国の健全な性秩序ないし性風俗等を侵害する現実的、具体的危険性を有する行為であって、わいせつ図画公然陳列罪の実行行為の重要部分に他ならないといえる。したがって、被告人が右のような行為を日本国内において行ったものである以上、本件については刑法一七五条を適用することができる。」

3 参考

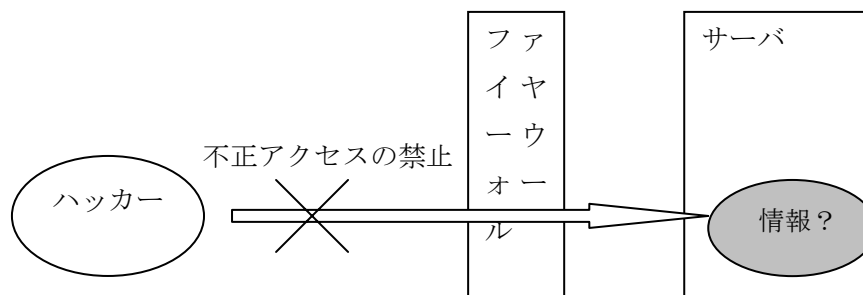
「犯罪地が日本国内であるためには、犯罪構成事実の一部が日本国内にあれば足りる」(大塚仁「刑法概説(総論)」改訂版73頁)

「電子計算機または電磁的記録の『損壊』とは、それらの物体自体を物理的に毀損することとともに、磁気ディスクなどに記録されているところを消去することも含む」(大塚仁「刑法概説(各論)」改訂版160頁)

II 不正アクセス禁止法

1 目的

電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与すること(1条)。



2 概略

「不正アクセス行為の禁止等に関する法律の概要」(警察庁)

<http://www.npa.go.jp/cyber/legislation/gaiyou/gaiyou.htm>

1) 不正アクセス行為の禁止、処罰

不正アクセス行為(アクセス制御機能を有する特定電子計算機等に電気通信回線を通じて他人の識別符号等を入力して作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為)を禁止し、その違反に対して罰則を設けた。

2) 不正アクセス行為を助長する行為の禁止、処罰

他人の識別符号を無断で提供する行為を禁止し、その違反に対して罰則を設けた。

3) アクセス管理者による防御措置

アクセス管理者は、特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとした。

4) 都道府県公安委員会による援助等

ア 都道府県公安委員会による援助等

イ 国による援助

3 識別符号 (2条2項)

特定電子計算機の特定利用をすることについてアクセス管理者の許諾を得た者及びアクセス管理者ごとに定められている符号で、アクセス管理者がその利用権者等を他の利用権者等と区別して識別するために用いるもの

- ア) アクセス管理者によって、その内容をみだりに第三者に知らせてはならないものとされている符号 (第1号) (例) ID・パスワードのうちのパスワード
- イ) 利用権者等の身体の全部若しくは一部の影像又は音声を用いてアクセス管理者が定める方法により作成される符号 (第2号) (例) 影像の例、指紋、静脈、虹彩などバイオメトリクス認証(生体認証)
- ウ) 利用権者等の署名を用いてアクセス管理者が定める方法により作成される符号 (第3号) (例) 署名の形状やその筆圧、動態等から特徴を取り出して数値化し符号化

4 アクセス制御機能 (2条3項)

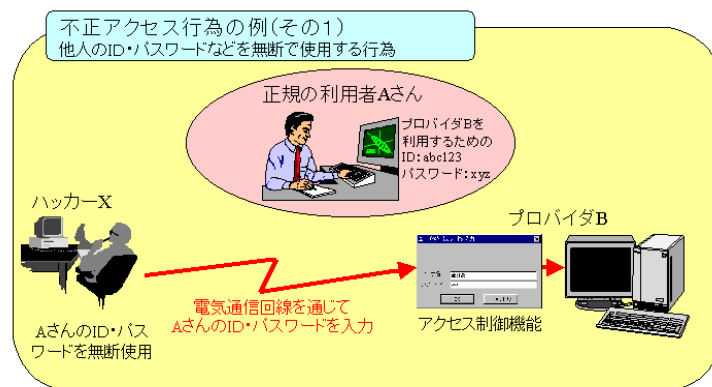
特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号 (識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。)であることを確認して、当該特定利用の制限の全部又は一部を解除するもの

5 不正アクセス行為の禁止

- ア) 他人の識別符号を無断で入力する行為 (第3条第2項第1号)

正規の利用権者等である他人の識別符号を無断で入力することによって利用制限を解除し、特定利用ができる状態にする行為です。

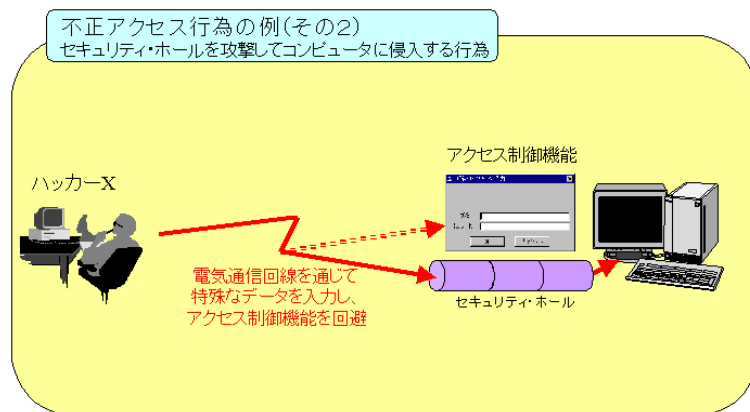
「識別符号窃用型」と呼ばれている。



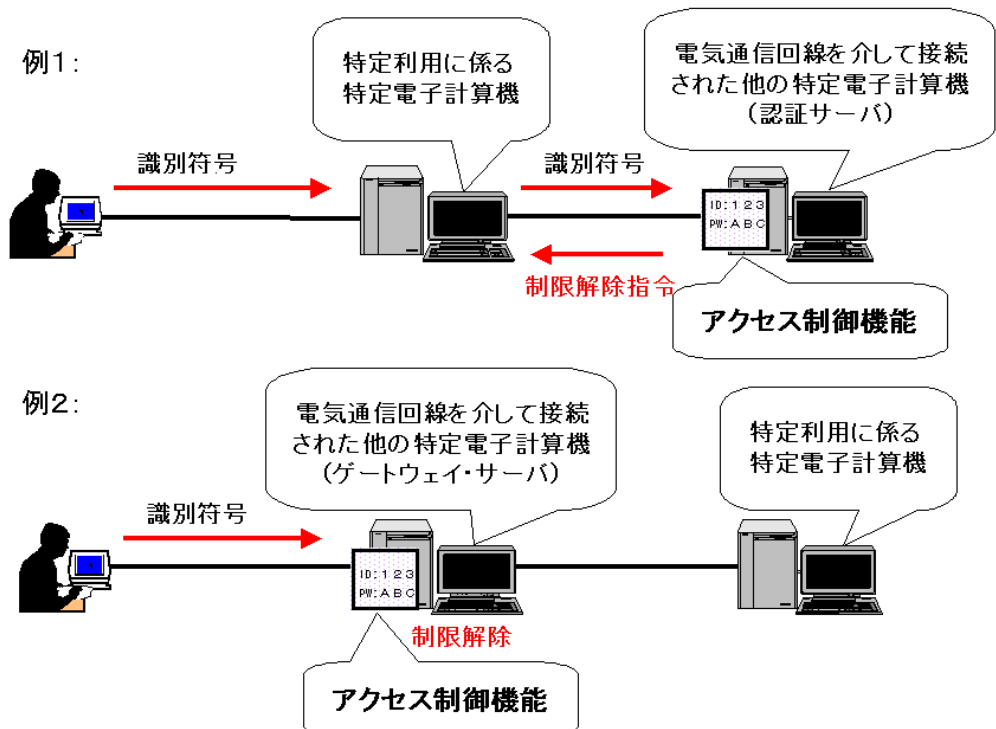
イ) アクセス制御機能による特定利用の制限を免れることができる情報又は指令を入力する行為（第3条第2項第2号、第3号）

「セキュリティ・ホール攻撃型」と呼ばれている。

- a) いわゆるセキュリティ・ホール（アクセス制御機能のプログラムの瑕疵、アクセス管理者の設定上のミス等のコンピュータ・システムにおける安全対策上の不備）を攻撃する行為



- b) 第2号、第3号の違い



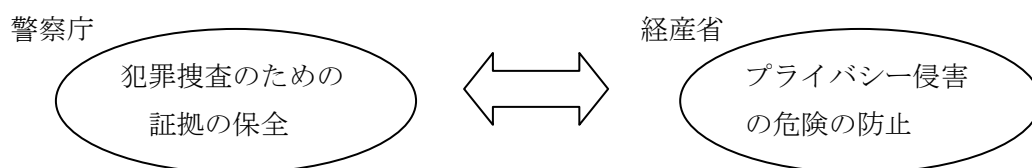
c) 退職後、自らのID、パスワードを用いた場合

利用権者等でなくなった者のID及びパスワードをアクセス管理者が消し忘れていたものは、利用権者等に付されているものではないので、識別符号には当たらず、これを侵入のために入力する行為は、1号には該当せず、2号に該当し得るだけと解されている（逐条不正アクセス禁止法40頁、75頁）。

6 不正アクセス行為を助長する行為の禁止、処罰（第4条）

他人の識別符号を第三者に提供する行為、例えば、「〇〇システムを利用するためのIDは△△、パスワードは□□である。」と他人に口頭や電子メール、文書などで教えたり、電子掲示板などに掲示したりする行為は、その識別符号を利用すれば誰でも容易に不正アクセス行為を行うことが可能となる点で不正アクセス行為を助長するものですから、これを放置することは、不正アクセス行為を禁止することの実効性を著しく損なうこととなるため処罰対象とした。

7（参考）アクセスログ（通信記録）の記録・保存の要否



III ヤフーBB事件

1 事案の概要

不正アクセス行為（ハッキング）により顧客名簿が流出し、恐喝行為に用いられたものであるが、「Yahoo!BB」の会員であった原告らが、同サービスの顧客情報として保有管理されていた原告らの氏名・住所等の個人情報が外部に漏えいしたことについて、共同して同サービスを提供している被告らが個人情報の適切な管理を怠った過失等により、自己の情報をコントロールする権利が侵害されたとして、被告らに対し、共同不法行為に基づく損害賠償として慰謝料等の支払を求めた事案。

2 刑事事件（東京地裁平成16年11月19日）

a) 不正アクセス禁止法違反と恐喝未遂幫助の罪に問われた富安被告は懲役2年6カ月、執行猶予5年（求刑懲役2年6カ月）、恐喝未遂幫助の罪に問われた森被告は懲役2年、執行猶予4年（求刑懲役2年）となった。

b) 判決内容

犯罪事実

「第2 被告人bは、他人の識別符号を使用して不正アクセス行為をすることを企て、法定の除外事由がないのに、iと共謀の上、平成15年6月13日午後8時4

6分ころ、東京都新宿区<以下略>δビル×階にあるいわゆるインターネットカフェである「j」において、設置されたパーソナルコンピュータから、電気通信回線を介して、e株式会社が東京都中央区<以下略>k×階m株式会社データセンター内に設置して管理するアクセス制御機能を有する特定電子計算機である認証サーバに、e株式会社従業員nらを利用権者として付された識別符号であるログインID「○○○○○○○○」及びパスワード「○○○○○○○○」を入力して、上記特定電子計算機を作動させ、上記アクセス制御機能により制限されている特定利用をし得る状態にさせ、もって不正アクセス行為をした。」

罰条

「刑法 60 条、不正アクセス行為の禁止等に関する法律 8 条 1 号、3 条 1 項、2 項 1 号」
量刑の理由

「被告人 b は、第 2 の犯行において、平成 1 5 年 2 月ころまで e 社で派遣社員として働いていた i から、同社のコンピュータにハッキングして顧客情報を入手することができ、これを競業会社に売却したり、株価操縦に利用するなどして多額の利益を得ることができる旨を持ち掛けられて、抵抗感なくこれに応じており、動機に酌量の余地はないし、遵法精神の低下も窺われる。しかも、第 2 の犯行に続く一連のハッキング行為を通じて、約 4 6 0 万件の e 社の顧客情報の入手に成功しているところ、前記のとおり、この顧客情報は重要な情報といえる上、これが後に被告人 b から c の手に渡って、恐喝事件の直接の手段とされたのであるから、その結果も重い。」

3 民事事件における判示事項

「被告 B B テクノロジーにおけるリモートアクセスの管理体制は、ユーザー名とパスワードによる認証以外に外部からのアクセスを規制する措置がとられていない上、肝心のユーザー名及びパスワードの管理が極めて不十分であったといわざるを得ず、同被告は、多数の顧客に関する個人情報と保管する電気通信事業者として、不正アクセスを防止するための前記注意義務に違反したものと認められる」

予見可能性につき、「被告 B B テクノロジーが A に行わせていた業務の内容、与えていた権限の内容に、前記誓約書を書かせていたことを総合すれば、A が業務を終える際に同被告とトラブルがあったか否かにかかわらず、同被告は、A が業務を終えた後に、業務中に知り得たパスワード等の情報を用いたり、他人にそれらの情報を漏らしたりすることによる不正アクセスについては、予見可能であったというべきであり、本件不正取得についても予見可能であったと認められる。」

また、結果回避可能性につき、「本件において、後記のとおり原告らの個人情報が含まれていたと認められるのは 1 月のデータであるが、B による 1 月のデータの不正取得については、それまでに、被告 B B テクノロジーが、本件アカウントを含むユーザー名・パスワードの適切な管理等、不正アクセスを防止するための相当な措置を採っていたれば防ぎ得たといえるから、結果回避可能性も認められる。」

(大阪地裁平成 18 年 5 月 19 日、判例時報 1948 号 122 頁)

IV 三菱UFJ証券事件

1 事案の概要

2009 年 11 月 12 日、三菱UFJ証券の元社員（同社システム部長代理）であった久保英明が、顧客情報約 148 万人分や企業情報を不正に持ち出したとして、不正アクセス禁止法違反と窃盗の罪に問われた事件で、東京地裁は、懲役 2 年（求刑懲役 2 年 6 月）の実刑判決を言い渡した。

2 判決内容

判決によると、被告人は、派遣社員の ID やパスワードを使って同社サーバーに不正アクセスし、2009 年 2～3 月に、顧客情報約 148 万人分の個人情報が書き込まれた CD や、約 122 万件分の企業情報を記録した CD を盗んだ。盗んだ情報は名簿業者に約 35 万円で売却したという。「顧客情報には勤務先名や所属、推定年収など高度なプライバシーに関する情報が含まれており、企業情報も情報会社から購入した高額なもの。流出で会社は社会的信用を大きく失墜した」などと指摘している。

<http://www.nikkei.co.jp/news/shakai/20091113AT1G1201S12112009.html>

検察側は証拠の一つとして、事件の影響によるとみられる損失額の試算を提出している。三菱UFJ証券は、148 万人のうち情報が流出した約 5 万人に対して、「お詫びのしるし」として 1 万円相当のギフト券を本年 6 月下旬から発送。この費用が約 5 億円と述べた。その他、事件調査や顧客からの問い合わせ対応、顧客情報の売却先となった業者と交渉するための弁護士費用、機関投資家からの発注減少による逸失利益などを合算すると、約 70 億 3500 万円になるとした。

三菱UFJ証券の専務が意見陳述し、「一番の損害は目に見えない信用の失墜である。社会的な信用を傷つけられ、金銭では換算できない損失を被った」と強調。元社員に対して「厳重な処罰を求める」と述べた。

<http://itpro.nikkeibp.co.jp/article/NEWS/20090909/336929/>

V 違法な情報流通に対する国際的取組

1 経過

「サイバー犯罪に関する条約」(Cybercrime Convention)

平成 13 年 11 月 8 日 ストラスブール (仏) で作成

平成 16 年 4 月 21 日 国会承認

平成 16 年 7 月 1 日 効力発生

2 条約の成立経緯

情報技術分野の急速な発達、コンピュータ・ネットワークの発展によって、世界中で電子メールの幅広い利用、インターネットを通じた各種サイトへのアクセス、電子

商取引等が可能となった。このような情報技術の発展は、社会の一層の発展のための大いなる可能性を秘めているが、一方で、コンピュータ・システムを攻撃するような犯罪及びコンピュータ・システムを利用して行われる犯罪（いわゆるサイバー犯罪）が出現するようになった。

サイバー犯罪は、犯罪行為の結果が国境を越えて広範な影響を及ぼし得るという特質を備えていることから、その防止及び抑制のために国際的に協調して有効な手段をとる必要性が高く、そのために法的拘束力のある国際文書の作成が必要であるとの認識が欧州評議会において共有されるようになった。

このような状況の下、欧州評議会において、サイバー犯罪を取り扱う専門家会合が設置され、平成9年（1997年）以降、同会合においてこの条約の作成作業が行われてきた。その結果、平成13年（2001年）9月に行われた欧州評議会閣僚委員会代理会合においてこの条約の案文について合意が成立し、同年11月8日に行われた欧州評議会閣僚委員会会合において正式に採択された。

この条約の署名式典は、平成13年（2001年）11月23日にハンガリーのブダペストにおいて開催され、我が国は、この条約に署名した。

3 条約締結の意義

この条約は、サイバー犯罪から社会を保護することを目的として、コンピュータ・システムに対する違法なアクセス等一定の行為の犯罪化、コンピュータ・データの迅速な保全等に係る刑事手続の整備、犯罪人引渡し等に関する国際協力等につき規定するものである。我が国がこの条約を締結することは、サイバー犯罪に効果的に対処するための国際的な取組に寄与するとの見地から有意義であると認められる。

4 条約の締結により我が国が負うこととなる義務

この条約の締結により我が国が負うこととなる主要な義務の概要は、次のとおりである。

コンピュータ・システムに対する違法なアクセス、コンピュータ・データの違法な傍受、コンピュータ・ウィルスの製造、児童ポルノのコンピュータ・システムを通じた頒布等一定の行為を犯罪として定め、その犯罪についての裁判権を設定すること。

自国の権限のある当局が、蔵置されたコンピュータ・データの迅速な保全、捜索及び押収並びに提出命令、通信記録のリアルタイム収集並びに通信内容の傍受を行うことが可能となるよう、必要な立法その他の措置をとること。

コンピュータに関連する一定の刑事手続、犯罪人引渡し等において国際協力を促進すること。

5 条約の内容

http://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4b.pdf

国内法で担保されているもの◎、条件付きで担保されているもの○、担保されていない可能性が高いもの△、担保されていないもの×

- 不正アクセス（第 2 条）
不正アクセス禁止法では、「アクセス制御機能を有する」「電気通信回線に接続している」場合に限定されている。
- 不正傍受（第 3 条）
電気通信事業法(179 条 1 項)、有線電機通信法（9 条、14 条 1 項）により、秘密を犯す行為が処罰される。
- ◎ データ妨害（第 4 条）
公用文書等毀棄罪（刑法 258 条）、私用文書等毀棄罪（259 条）、電磁的記録不正作出罪（161 条の 2）、電子計算機損害等業務妨害罪（234 条の 2）
- ◎ システム障害（第 5 条）
電子計算機損害等業務妨害罪（刑法 234 条の 2）、信用毀損罪・業務妨害罪（233 条）、威力業務妨害罪（234 条）
- ×、○ 装置の濫用（第 6 条）
ハッキングツール等の不正プログラムの製造、頒布行為についての規制は我が国には存在しない。ただし、不正アクセス禁止法 4 条の規定あり。
- ◎ コンピュータに関連する偽造及び詐欺（第 7 条及び第 8 条）
電磁的記録不正作出罪（刑法 161 条の 2）、詐欺罪（246 条）、電子計算機使用詐欺罪（246 条の 2）、背任罪（247 条）
- 児童ポルノに関連する犯罪（第 9 条）
児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律。ただし、提供目的のない場合の児童ポルノの取得、保有に関する処罰規定はない。
- ◎ 著作権及び関連する権利の侵害に関連する犯罪（第 10 条）
著作権法（著作隣接権を含む）
- 未遂及びほう助又は教唆（第 11 条）
- 手続規定の適用範囲（第 14 条）
- 条件及び保障措置（第 15 条）
- △ 蔵置されたコンピュータ・データの迅速な保全（第 16 条）
刑事訴訟法による捜索差押えの運用を迅速に行うことで対応可能？
- △ 提出命令（第 18 条）
公務所等（公私の団体を含む）に対する照会請求（刑事訴訟法 197 条 2 項）。ただし、個人に対して行えないことや通信の秘密の保護による制限等あり。
- △ コンピュータ・データの捜索及び押収（19 条）
刑事訴訟法による捜索差押えは、有体物を前提しており、データ自体の差押えについては疑義がある。
- △ 通信記録のリアルタイム収集（20 条）
我が国では、通信傍受法による傍受が限定的な場合にのみ認められている。従っ

て、通信記録（トラフィック・データ）のリアルタイム収集は、現行の検証令状によることは不可能（刑事訴訟法 222 条の 2）

△ 通信内容の傍受（第 20 条及び第 21 条）

重大犯罪に関しては、通信傍受法による傍受が可能。

（参考）「サイバー刑事法研究会報告書」（平成 14 年 4 月 18 日 経産省）

<http://www.meti.go.jp/policy/netsecurity/Cybercriminallawcom.htm>

以 上