

インターネットの一般利用者の 保護及び知的財産権侵害に関する 官民連携の在り方について

平成16年度総合セキュリティ対策会議
報告書

総合セキュリティ対策会議

はじめに

近年目覚ましい発展を遂げている情報通信ネットワークは、私たちの生活の利便性を向上させるにとどまらず、社会・経済活動の根幹を支える重大なシステムとして機能するに至っている。その一方で、サイバー犯罪の検挙数の増加、コンピュータ・ウイルスの蔓延といった、情報セキュリティに対する脅威も増大していることから、情報セキュリティ対策を推進し、情報通信ネットワークの安全性・信頼性を確保することが国民の利益に直接影響を及ぼす問題となっている。

「総合セキュリティ対策会議」は、情報セキュリティに関する産業界等と政府機関との連携の在り方、特に警察との連携の在り方について検討を行うことを目的として平成13年度に設置されたものである。本会議においては、情報セキュリティに関する有識者にとどまらず、電気通信事業、コンテンツ事業、コンピュータ製造・販売業、オペレーティングシステム事業等の各種事業に関する知見を有する方々、さらには、法曹界、教育界、防犯団体、消費者団体の方々という広い分野の有識者により、幅広い議論が活発に行われており、平成13年度は報告書「情報セキュリティ対策における連携の推進について」、平成14年度は報告書「情報セキュリティに関する脅威の実態把握・分析について」、平成15年度は「官民における情報セキュリティ関連情報の共有の在り方について」をそれぞれ取りまとめた。

本年度は、「インターネットの一般利用者の保護のためにできること」及び「インターネットを利用した知的財産権侵害」について、現状の問題を明らかにし、これらの問題を解消するための官民連携の在り方について検討を行うとともに、被害の増加が懸念される「フィッシング」事案について追加検討を行った。本報告書は、本会議での成果をまとめたものである。

なお、各委員には、それぞれが有する個人的な知見に基づいて、個人の立場において自由に議論に参加していただいたものであり、本報告書の内容は、「産業界」の意見を反映したものでも、各委員が属する企業・組織の立場を反映したものでないことをお断りしておく。

本報告書が、今後の情報セキュリティの向上の一助となれば幸いである。

平成17年3月

総合セキュリティ対策会議委員長

前田 雅英

総合セキュリティ対策会議委員名簿

前田雅英 (委員長)	東京都立大学 教授
稲垣隆一	弁護士
小田啓二	特定非営利活動法人 日本ガーディアン・エンジェルス 理事長
小野田誓	(社)日本PTA全国協議会 相談役
加藤雄一	ニフティ(株) 常務取締役システム事業部長
久保田裕	(社)コンピュータソフトウェア著作権協会(ACCS) 専務理事 事務局長
桑子博行	(社)テレコムサービス協会 サービス倫理委員会 委員長 (AT&Tグローバル・サービス(株)通信渉外部長)
国分明男	(財)インターネット協会 副理事長
佐々木良一	東京電機大学 教授
下道高志	サン・マイクロシステムズ(株) システム技術統括本部 オープン・システム・センター IIアーキテクト
城内恵津子	独立行政法人国民生活センター 相談調査部 調査役
杉浦昌	日本電気(株)I基盤システム開発事業部 セキュリティ技術センター センター長

西野茂生	ボーダフォン(株) 経営企画本部 法務渉外統括部 渉外部課長
西村達之	セコムトラストネット(株) 代表取締役社長
春田真	(株)ディー・エヌ・エー 取締役 総合企画部長
東貴彦	マイクロソフト(株) 取締役経営戦略担当
廣川信彦	(社)日本クレジット産業協会 常務理事
別所直哉	ヤフー(株) 法務部部長
山口英	奈良先端科学技術大学院大学 教授
吉川誠司	WEB110 代表

(敬称略・50音順)

(オブザーバー)

内閣官房(情報セキュリティ対策推進室)
総務省
法務省
外務省
経済産業省

事務局 警察庁生活安全局情報技術犯罪対策課

目次

本編

はじめに	1
総合セキュリティ対策会議委員	2
目次	4
第1章 会議の目的	6
第2章 産業界等と政府との連携の重要性	8
1. ネットワーク化の進展	
2. 情報セキュリティに関する脅威の増大	
3. 産業界等と政府との連携	
第3章 インターネット上において人命保護等の観点から緊急の対処を必要とする事案が 発生した場合の対応の在り方に関する提言	10
1. 現状の問題点	
2. 具体的事例	
3. 対象事案の類型化	
4. 対応の在り方	
5. 今後の課題	
第4章 インターネット・オークションを利用した知的財産権侵害への対応の在り方に関 する提言	19
1. インターネット・オークションに係る現状と取組み	
2. 官民連携の在り方	
3. 今後の課題	
第5章 いわゆる「フィッシング」対策の推進について	26
1. 「フィッシング」とは	
2. 海外における被害状況と取組み	
3. 「フィッシング」対策について	
4. 今後の課題	

資料編（参考資料）

1. 平成16年中のサイバー犯罪の検挙及び相談受理状況について・・・1
2. 平成16年中の不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況について・・・9
3. 平成16年中のいわゆる出会い系サイトに関係した事件の検挙状況について・・・77
4. 警察の体制について・・・84
5. 委員発表資料
 - インターネット・オークションを利用した知的財産権侵害及び詐欺の現状とこれに対する取組み・・・87
 - インターネット・オークションを利用した知的財産権侵害の現状とこれに対する取組み・・・95
 - 不正商品対策の推進のために・・・107
 - 米国に於ける Phishing 対策へ向けた技術及び業界連携の動向・・・111
 - フィッシング詐欺・・・115
 - インターネットオークションと知的財産権の侵害・・・123

第1章 会議の目的

昨今の官民を挙げた取組みにより、情報技術の急速な進展や高度情報通信ネットワーク社会が実現されつつあり、市民生活・社会経済活動のあらゆる分野において、情報技術及び情報通信ネットワークが活用されるようになってきている。

特に、インターネットの活用による生活の利便性の向上や電子商取引の発展など、高度情報通信ネットワーク社会の光の部分が伸長する一方、これに比例するように、サイバー犯罪の検挙件数・相談件数が年々増加するなど、その陰の部分ともいえるべき、情報セキュリティに対する脅威も増大しつつある。情報通信ネットワークの安全性及び信頼性を確保し、国民がこれを安心して利用することができるようにすることは、高度情報通信ネットワーク社会の形成にとって不可欠な条件であり、情報セキュリティの確保は喫緊の課題となっている。

情報セキュリティについては、サイバー犯罪に代表される情報セキュリティに関する脅威の舞台であるインターネット等の情報通信ネットワークが社会・経済活動の根幹を担う存在であり、産業界等が発展させてきたものであること、情報セキュリティに関する脅威に有効に対処するためには速いスピードで発展している高度な技術の活用が必要であること等から、ネットワークに関わる広範な層の協力によってこそ確保されるものであると言える。

それゆえ、情報セキュリティに関する警察の活動も、産業界等多くの関係者・関係機関との連携が必要不可欠である。

情報セキュリティに関する産業界等と警察との連携については、これまで、自治体（都道府県）では「プロバイダ等連絡協議会」等を通じた各種の取組み、国レベルでは、G8等の国際的取組みへの参画等がなされてきた。国における取組みの一例である、平成13年5月に東京で開催されたG8ハイテク犯罪対策・官民合同ハイレベル会合（東京会合）においては、産業界等と法執行機関との連携を各国内でも議論することの重要性が改めて確認された。

本「総合セキュリティ対策会議」は、こうした状況を受けて、情報セキュリティに知見を有する各界の有識者による会議として開催に至ったものであり、平成13年度には報告書「情報セキュリティ対策における連携の推進について」を作成し、情報セキュリティに関する産業界等と政府機関の連携の在り方、特に警察との連携の在り方に関する全体像を提示した。また、平成14年度には報告書「情報セキュリティに関する脅威の実態把握・分析について」をとりまとめ、アンケート調査等を通じ、官民が連携して情報セキュリティ対策を講じる上で参考となるであろう脅威の実態について分析を行い、平成15年度には、情報セキュリティ上の問題を解消するため、必要となる官民連携の在り方について、具体的な事例を通じた官民の情報共有のスキームについて検討を行い、報告書「官民における情報セキュリティ関連情報の共有の在り方について」としてまとめた。

本年度（平成16年度）の会議においては、「インターネットの一般利用者の保護のためにできること」というテーマに基づき、人命保護等の観点から緊急の対処を必要とする事案が発生した場合の対応の在り方やその被害の拡大が懸念されている「フィッシング」事案に対する対策について、具体的事例に基づき、官民が連携してどのような方策を講ずることが望ましいかについて検討を行った。また、近年インターネットを利用した知的財産権侵害が社会問題となっていることから、特に最近急増しているインターネット・オークションを利用した知的財産権の侵害に関し、今後の対策の在り方についても検討を行い、提言としてまとめたものである。

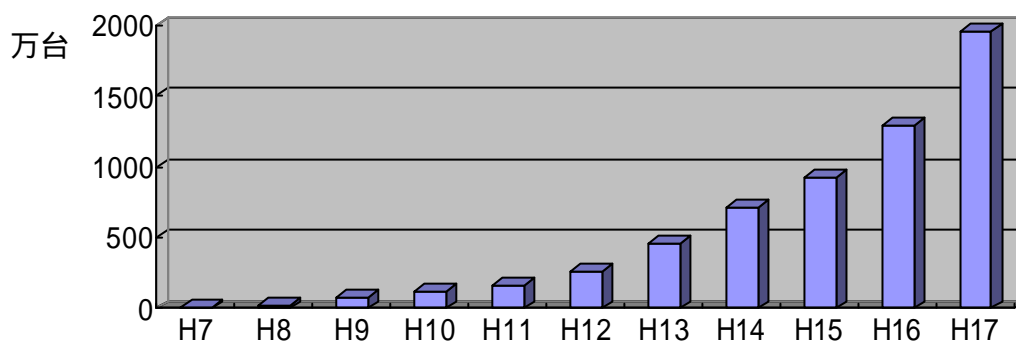
第2章 産業界等と政府との連携の重要性

高度情報通信ネットワーク社会の進展に伴って、情報セキュリティに関する脅威も増大しており、これに対処するためには、産業界等と政府が連携することが重要である。

1. ネットワーク化の進展

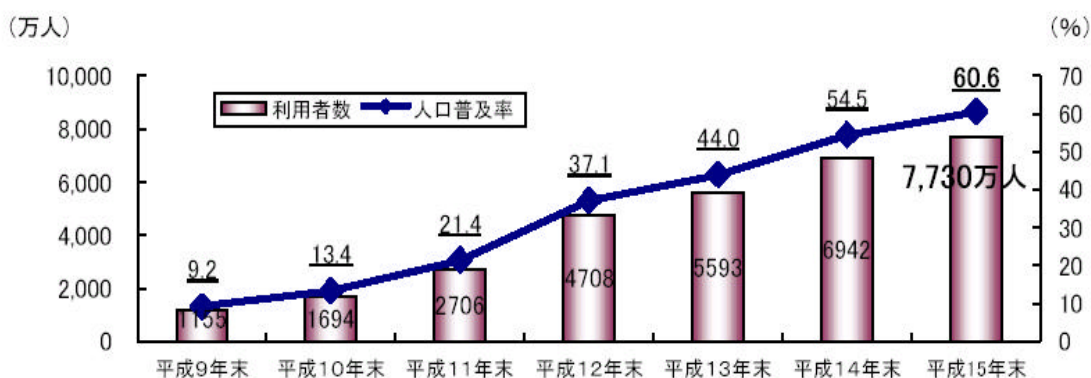
平成17年1月におけるインターネットに接続されている国内コンピュータの数は、約1954万台であり、その数は、近年急増している。

インターネットに接続されている国内コンピュータ数



ドメイン名を割り当てられている IP アドレス (.jp) から算出
Network Wizards(<http://www.nw.com>)

また、国内のインターネット利用者は、平成15年末において約7,730万人（人口普及率60.6%）であり、人口普及率は初めて6割を超えた。



平成16年情報通信白書（総務省）

2. 情報セキュリティに関する脅威の増大

このようなネットワーク利用の急増に対応し、高度情報通信ネットワーク社会の陰の部分とも言うべき情報セキュリティに関する脅威も増大しており、サイバー犯罪の検挙件数、サイバー犯罪等に関する相談件数も引き続き増加傾向にある。

3. 産業界等と政府との連携

このような状況にあって、ネットワークの安全性及び信頼性を確保し、ネットワークを安心して利用することができるようにするためには、ネットワークにおける情報セキュリティを向上させることが喫緊の課題となっているところであるが、情報セキュリティについては、次のような観点から、産業界等と政府との連携が重要であると考えられる。

(1) 社会・経済活動の根幹を担う全世界に構築された情報通信インフラ

インターネット等の情報通信ネットワーク（以下「情報通信インフラ」という。）は、電子商取引などの国民の利便性を向上させるサービスを提供するだけでなく、エネルギー供給、交通、政府・行政サービス等国民生活に大きな影響を与えるサービスをも提供するようになってきており、しかも、これらのサービスのネットワークへの依存度はますます高まっている。

このように、情報通信インフラは、社会・経済活動の根幹を担う存在となっており、その安全性及び信頼性の確保は、政府及び産業界の双方に共通の課題となっていることから、これらを効果的に実現していくために双方が協力して情報セキュリティ対策を講じていくことが必要である。

(2) 産業界等が発展させた情報通信インフラ上での事象

情報通信インフラは、国家主導で整備されたものではなく、産業界等の活動の中で発展してきたものであり、サイバー犯罪等のネットワークに関する脅威はこのようなインフラ上で生じる事象であることから、情報セキュリティに関する脅威に対して警察等の法執行機関のみで対処することは困難であり、産業界等の協力が不可欠である。

例えば、情報通信インフラ上でどのような事象が生じているのかという被害実態の把握においても、産業界等と法執行機関との連携がなければその把握は困難であり、証拠の収集等の犯罪捜査が円滑に行われるためにも産業界等の協力が不可欠である。

(3) 高度な技術を利用した事象

サイバー犯罪等のネットワークに関する脅威は、情報通信インフラをその舞台として行われるため、高度な技術を用いて犯罪等が行われることが多く、その技術は極めて速いスピードで進展している。そのため、このような脅威に対処するためには、技術に関する知識・情報を産業界等と政府とで共有することが重要であり、また、両者が協力して脅威に対処するための技術を発展させていくことも重要である。

第3章 インターネット上において人命保護等の観点から緊急の対処を必要とする事案が発生した場合の対応の在り方に関する提言

インターネット上には、違法・有害な情報も多く流通しており、これらに起因する犯罪等の未然防止のため、警察では、全国の都道府県警察にサイバー犯罪相談窓口を設置し、国民からの情報提供を受け付けている。こうした情報提供の中には、自殺の決行をほのめかす書込み、集団自殺を呼び掛ける書込み、対象が不確定な殺人予告等、人命保護の観点から緊急に対処する必要がある事案も少なくない。

しかし、こうした事案における現状の対応には問題点も少なくないことから、この種の事案への対応の在り方について検討を行ったものである。

1. 現状の問題点

(1) 自殺予告（集団自殺の呼び掛けを含む）の場合（図1）

自殺予告事案については、犯罪には該当しないため捜査の対象にはならないが、警察には、警察法第2条で定める個人の生命、身体及び財産の保護の責務があることから、自殺防止のため、要保護者を特定して保護するのが通常である。

警察法 第2条（警察の責務）

警察は、個人の生命、身体及び財産の保護に任じ、犯罪の予防、鎮圧及び捜査、被疑者の逮捕、交通の取締その他公共の安全と秩序の維持に当ることをもってその責務とする。

一般に、警察が自殺予告事案への対応を求められる場合の多くは、「110番通報」を契機とする場合であり、これは、ビルから飛び降りようとしている人を目撃した通行人から通報があった場合でも、また、インターネット上の掲示板等に自殺予告の書込みがあった場合でも、基本的には同じである（図1）。

しかしながら、現実には自殺を企てていると思われる人を目撃した人から通報があった場合は、通常、警察は110番通報を受けて速やかに現場に駆け付けることができるが、インターネット上の掲示板等において自殺予告の書込みを発見した旨の通報を受けた場合には、通報者も自殺を企てている人の氏名・住所や所在に関する情報を持っておらず、書込み者に関する情報としては、書込みがなされた掲示板等やIPアドレスしか判明しないことが多い。そのため警察では、要保護者を特定するため、掲示板等の管理者に対するIPアドレスの照会やインターネット接続事業者（以下「ISP」という。）等に対するIPアドレスに係る契約者情報の照会を行う必要が生じる。

ISP等については、通信の秘密を確保する義務があることから、警察からの照会については差押え令状を受けて回答するのが一般的であるが、自殺予告自体は犯罪には該当しないので差押え令状の呈示を受けられず、原則どおりの対応では警察へ回答する

ことはできない。

一方、社団法人テレコムサービス協会が公表している「インターネット接続サービス等に係る事業者の対応に関するガイドライン」(以下「ISPガイドライン」という。)によれば、「緊急避難または正当防衛」の場合の通信当事者に係る情報の開示は、通信の秘密の例外規定となっており、緊急避難の一例として「自殺予告」が挙げられている。そこで、ISP等はこれを参考に警察への照会に回答することとなるが、ISPガイドラインには、具体的例示等がないことから、自殺予告事案におけるIPアドレスやIPアドレスに係る契約者情報の開示について、各ISP等が個別にISPガイドラインに定める緊急避難への該当性を判断して回答することを迫られているのが実状である。

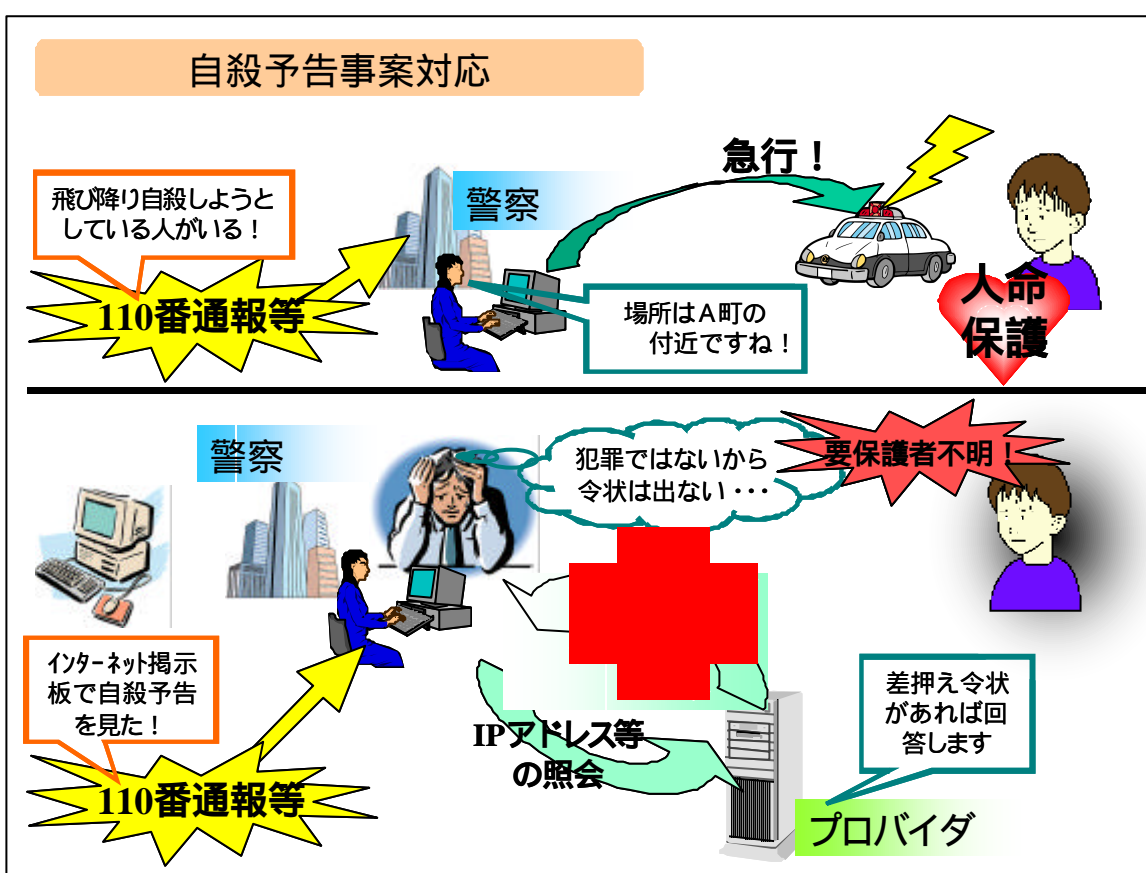


図1 自殺予告事案の場合

(2) 殺害予告の場合

殺害予告事案は、犯罪(脅迫罪等)に該当し得る事案と考えられるが、警察は、殺害予告の対象となっている者を保護するとともに、被害届を受け(図2) 裁判所から差押え令状の発付を得た上で(図2) ISP等に書込み者のIPアドレスの照会をし、契約者情報の提供を受け(図2) 書込みを行った者を特定して、被疑者を検挙することとなる。つまり警察は、自殺予告事案とは異なる対応をとることが可能である。

しかしながら、殺害予告事案の場合においても、例えば「東京の子ども」などのように殺害対象が漠然としていて具体的には絞り込むことができないような場合には、犯罪のおそれがある事案として捜査はできるものの、差押え令状の発付を得るまでの犯罪事実を構成できない場合も生じる。実際に、同種の事例で、裁判所に差押え令状を請求したが、発付されなかった事例もある。このような場合、警察としては、ISP等に対してIPアドレスやIPアドレスの契約者情報についての照会を行うこととなるが、これに対して、ISP等は個別事案に応じてガイドラインに定める緊急避難への該当性を判断して、回答せざるを得ないのが実状である。

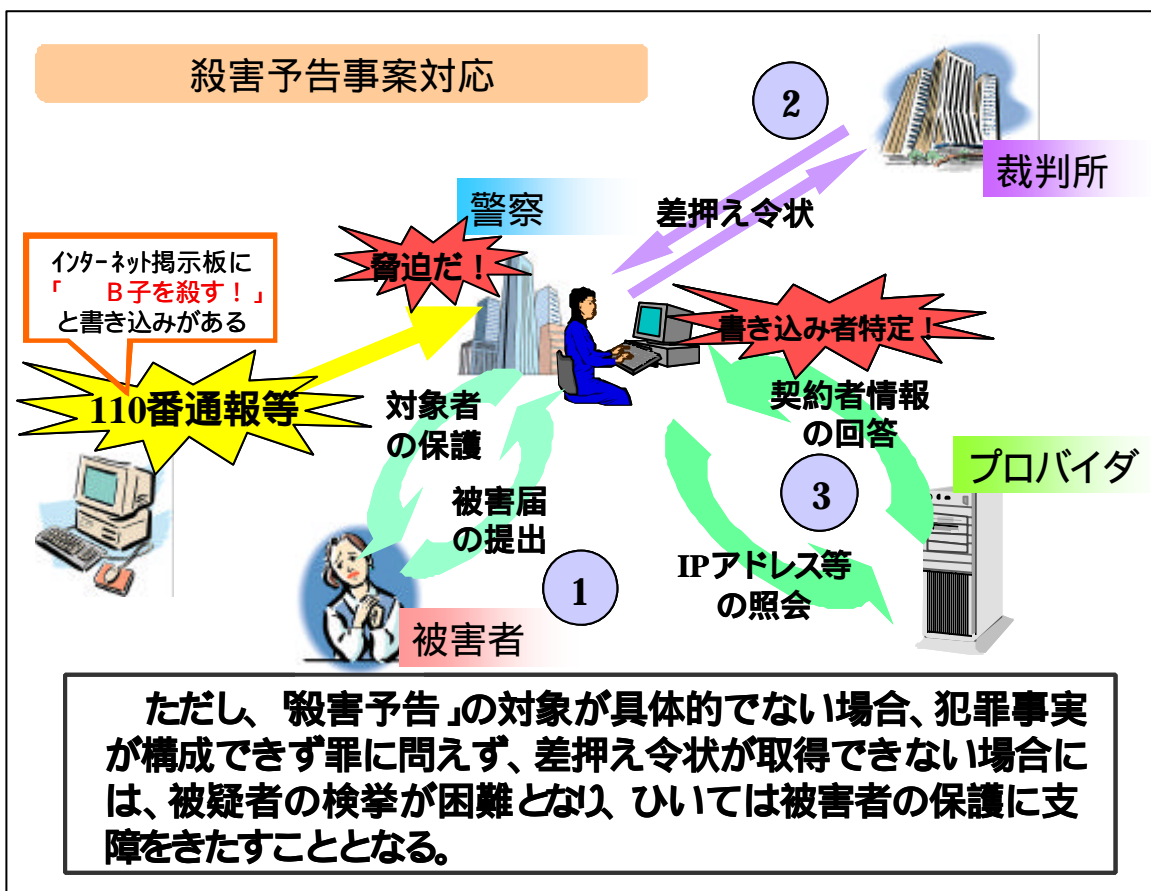


図2 殺害予告の場合

2. 具体的事例

前述のように、緊急性が求められる事案であるにもかかわらず、差押え令状の発付を受けられなかった場合の具体的事例を挙げると(表1)、どのような書き込みが緊急避難となる「自殺予告」に該当するのかについて、ISP等が自ら判断するのは困難な場合も多いと思われることから、現実には緊急避難として、任意の照会に応じて情報を開示するISP等がいる一方で、知識不足等により警察に対して差押え令状の提出を求めるISP等も存在するなど、その対応はまちまちであるのが実状である。

	内容	プロバイダ等の対応	警察の対応
1	地域別掲示板のA県のところに、「死にます」という書込みがあった旨、A県警に通報があった。	掲示板管理者から書込み者のIPアドレスについて開示を受けるも、当該IPアドレスを管理するプロバイダは、「令状がなければ個人情報を開示できない」と開示を拒否。	当該掲示板において、自殺を思いとどまるよう書き込んだ。
2	オークションの評価欄に「僕が死ねば全てが終わるのですが、・・・」と書き込まれた旨、B県警に通報があった。	オークション事業者は、緊急案件であるため、照会文書により書込み者の契約者情報を開示。	契約者に連絡したところ、書込み者はその息子と判明。息子の発作的書込みであったので説諭。
3	掲示板を管理しているプロバイダから、少女が自殺予告の書込みをしている旨、C県警に通報があった。	書込み者のIPアドレスを管理するプロバイダは、照会文書を要求。県警の説得等により、最終的には契約者情報を開示。	契約者に連絡したところ、書込み者はその娘と判明。娘が別の自殺志願者とカラオケ店にいるところを保護。
4	自殺掲示板で「本気で死ぬと考えている人いませんか？私は 市の19の男です・・・」という集団自殺の呼び掛けがある旨、D県警に通報があった。	書込み者のメールアドレスを管理するプロバイダは、協力はするが、照会文書は直接持参又は郵送に限り、回答も郵送でしか行わないと事実上の開示拒否。	「 市の19の男」との記述とメールアドレスが本名であったことから、 市を管轄する警察署において書込み者を割り出して保護。要保護者は、「本気で死ぬことを考えていた。」との言動があり説諭。
5	自殺を思いとどまらせる掲示板の管理者から、掲示板に自殺をほのめかす書込みがあった旨、E県警に通報があった。	書込み者のIPアドレスを管理するプロバイダは、「令状がなければ個人情報を開示できない」と開示を拒否。	通報者にプロバイダが照会に応じてくれない旨、回答。
6	ウェブカメラを利用したチャット中に相手が手首を切った旨、F県警に通報があった。	要保護者のIPアドレスを管理するプロバイダは、結果報告をすることを条件に、電話により契約者情報を開示。	契約者宅に急行し、瀕死の要保護者を保護。一命をとりとめた。
7	自殺掲示板で「誰か、本気で一緒に死んでください。私は何とかしてでも今年の12月までに死にたいんです。・・・」という集団自殺の呼び掛けがある旨、G県警に通報があった。	書込み者のIPアドレスを管理するプロバイダは、照会文書を要求。県警の説得等により、最終的には契約者情報を開示。	契約者は、以前に自殺未遂を図り、精神科に通院中の者であり、保護するとともに家族にも注意喚起を促した。しかし、2ヶ月後、集団自殺を決行し、死亡。
8	巨大掲示板で「明日H県のほうの小学生等を殺害します」という殺人予告の書込みがあった旨、H県警に通報があった。	書込み者のIPアドレスを管理するプロバイダは令状を要求したが、H県警の説得により6時間検討後、照会文書により回答。	書込み者が特定され、いたずらであることが判明。その後、小学校から被害届を受理し、威力業務妨害罪で検挙。

表1 人命保護等の観点から緊急の対処を必要とする事案の具体例

3. 対象事案の類型化

このような現状の問題点を解消し、適切な対応をとるため、まず、対象とする事案についての類型化を行った（表2）。

	内容	書込み表示の例
自殺予告	<p>【ホームページ又は掲示板における書込みの場合】</p> <p>総合的に判断して自殺を執行する現在の危難が認められ、自殺を防止するために書込み者の通信の秘密を侵すことがやむを得ない場合であって、その者のIPアドレス又はメールアドレスが判明しているか、判明する可能性があるとき</p> <p>【メール又はチャット等でのやりとりの場合】</p> <p>総合的に判断して自殺を執行する危難が認められる場合であって、通信の当事者からの通報であるとき</p>	<p>切迫した具体的期日・場所等を示し、「死にます」、「自殺します」、「首をつります」、「手首を切ります」など、死をほのめかしている場合（実行方法や動機が示されている場合はより緊急性が高い）</p> <p>自殺に結びつく言動が画像で確認できる場合</p>
集団自殺の呼び掛け	<p>「有害情報」として、掲示板管理者において自主的に削除等の検討がなされることが望ましいが、書込みが一定期間放置されるなどにより、それに呼応する書込み等があった場合</p>	<p>切迫した具体的期日・場所・手段（例：薬、車、練炭など）等を示し、「一緒に死んでくれる人をさがしています」「私達と一緒に逝きたい人はいませんか」など、集団自殺を呼び掛けている場合</p>
殺害予告	<p>総合的に判断して殺害を執行する現在の危難が認められる場合であって、殺害の決行防止のために殺害予告者の通信の秘密を侵すことがやむを得ない場合</p>	<p>切迫した具体的期日・場所・手段等を示し、「殺す」「刺す」「爆破する」「血の海にする」など、殺害をほのめかしている場合</p>

表2 人命保護等の観点から緊急の対処を必要とする場合

4. 対応の在り方

表2で類型化したインターネット上において人命保護等の観点から緊急の対処を必要とする事案（以下「緊急事案」という。）が発生した場合には、現状の問題点を解決し、警察及びISP等は相互に連携し、人命保護等の観点から、対象者の保護に努めることが必要である。

具体的には、警察が、110番通報等により緊急事案の発生を認知し、ISP等に通信の秘密に係る情報の開示を求める場合には、差押え令状等に基づくことが原則となるが、表2の自殺予告事案等のように犯罪に該当しない場合や殺害予告事案のうち対象が漠然としており具体的に絞り込むことができず差押え令状の発付が得られないような場合で

あっても ISP 等が緊急避難に該当すると判断できるときには、照会文書（別紙様式 1 ～ 2 参照）等により ISP 等に協力を依頼するなど、事前に定められた手続に則り、人命保護に努めることが重要である。

よって、書込み者の IP アドレスが判明していない場合は、警察は、照会文書（別紙様式 1 参照）により、掲示板やチャットの管理者等に対し、書込み者の IP アドレスを照会することが考えられる。また、IP アドレスやメールアドレスが判明した場合には、警察は、当該 IP アドレスやメールアドレスを管理する ISP 等に対し照会文書（別紙様式 2 参照）による照会を実施し、書込み者を特定することが考えられる。

なお、書込み者の特定にあたっては、書込み者の住所・氏名のほか、迅速に書込み者と連絡を取るため、連絡先（電話番号、FAX、メールアドレス等）が必要であるほか、住所・連絡先が登録時と変わっていたなどの理由により連絡がつかない場合に、住民票等により書込み者の所在地を特定する際に必要となる生年月日についても把握する必要がある。

その際、警察は、ISP 等が緊急避難に該当すると判断ができるよう十分な情報及び警察としての判断を ISP 等に提供するよう努めるほか、消防を始めとする地方公共団体の機関とも連携し、迅速に対応すべきである。

ISP 等は、前述の緊急事案について警察からの要請があった場合には、緊急避難に該当する事案については、差押え令状がなくとも対応できることなどにかんがみ、緊急避難該当性を適切に判断した上、関係機関と連携して人命保護に努めるべきである。とりわけ、緊急事案のうち、複数の者に対する殺害予告等、特に複数の者に被害が及ぶおそれがあるような場合は、緊急性が高いことから迅速な対応が必要である。ISP 等においては、本提言を踏まえ、この種の事案への適切な対処についての周知徹底及び確実な実行が望まれる。

5. 今後の課題

前述のような緊急事案は、今後も発生するおそれが高く、人命保護については、社会全体として最善を尽くすことが重要である。最近の報道によれば、オーストラリアでは、日本のインターネット上での集団自殺を呼び掛ける事案の報道をきっかけに、インターネット上で自殺を呼び掛ける者に罰金を科す法律が成立する見込みであるなど、この種の事案は、諸外国においても対応が急がれている問題であることから、今後とも、法制度も含め、検討をしていく必要がある。

自殺サイト運営 罰金4500万円

【シドニー＝橋口椰子】オーストラリアの連邦政府はこのほど、インターネット上の自殺関連サイトの管理者に対し、最高55万豪ドル（約4500万円）の罰金を科す法案の導入を決めた。

日本で相次ぐネット心中事件がオーストラリアで大きく報道されたのがきっかけ。ネット上で自殺をおおったり、自殺方法を公開した場合が処罰の対象になる。

ただ、安楽死に関するサイトや、ネット上の安楽死議論は除外される。

法案は今週、議会に提案されるが、最大野党・労働党は賛成しており、可決・成立する見込み。

オーストラリアでは自殺関連サイトは大きな社会問題とはなっていないが、エリソン司法・税関相は日米の例をあげた上で、「ネット上の破壊的な意図から無防備な個人を守るため」と述べ、法案の意図が集団自殺の予防であることを強調した。

豪、日本の「ネット心中」報道受け

平成17年3月11日（金）読売新聞夕刊での報道

別紙様式 1 (書込み者の IP アドレス等の特定に係る照会)

通知 (.) 第 号
平成 年 月 日

株式会社
部 御中 (殿)

県 警察署長



要保護者の所在確認に関する協力要請について (照会)
下記の事案に関し、要保護者の所在等を緊急に確認する必要があるため協力願いたい。

記

1 事案概要

インターネット上の電子掲示板「 」に、 月 日付で「今から死ぬ」旨の意思表示 (以下、書込みという。) があったもの。実際の書込みの内容は別紙のとおり。

2 端緒

月 日、当該書込みを閲覧した者が警察に通報した (又は家族から相談があった等) ことによる。

3 要保護者の書込みについての詳細

(1) 書込みの場所

[掲示板等の呼称及び URL]・[項目 (スレッド) の名称]・[書込み番号] 等

(2) 書込みの日時

平成 年 月 日 時 分

4 所在確認を必要とする理由

自殺予告に関する事項を調査の上、所要の措置を講じることが必要である。

5 要請事項

(1) 3 の書込みをした者の IP アドレス

(2) 書込みをした者の住所、氏名、生年月日、電話番号、連絡先 (電話番号、FAX、メールアドレス等) についての情報を有する場合は、当該情報

6 問い合わせ先

取扱責任者 生活安全課長 (宿直責任者) 警部

担当者 係 警部補

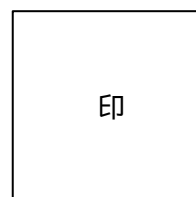
電話 - - FAX - - 以上

別紙様式 2 (書込み者の特定に係る照会)

通知 (.) 第 号
平成 年 月 日

株式会社
部 御中 (殿)

県 警察署長



要保護者の所在確認に関する協力要請について (照会)
下記の事案に関し、要保護者の所在等を緊急に確認する必要があるため協力願いたい。

記

1 事案概要

インターネット上の電子掲示板「 」に、月 日付で「今から死ぬ」旨の意思表示 (以下、書込みという。) があったもの。実際の書込みの内容は別紙のとおり。

2 端緒

月 日、当該書込みを閲覧した者が警察に通報した (又は家族から相談があった等) ことによる。

3 要保護者の使用 IP アドレス (又はメールアドレス) 及び書込みの日時

IP アドレス (又はメールアドレス) 平成 年 月 日 時 分

4 所在確認を必要とする理由

自殺予告に関する事項を調査の上、所要の措置を講じることが必要である。

5 要請事項

3の IP アドレス (又はメールアドレス) を有する者の住所、氏名、生年月日、連絡先 (電話番号、FAX、メールアドレス等)

6 問い合わせ先

取扱責任者 生活安全課長 (宿直責任者) 警部

担当者 係 警部補

電話 - - FAX - - 以上

第4章 インターネット・オークションを利用した知的財産権侵害への対応の 在り方に関する提言

知的財産の創造・保護及び活用については、平成14年7月に取りまとめられた知的財産戦略大綱を受けて、同年11月に知的財産基本法が制定された。平成15年3月には、同法に基づき、内閣総理大臣を本部長とし、全閣僚を構成員とする知的財産戦略本部が設置され、「知的財産立国」の実現を目指した新たな取組みが、進められてきたところである。具体的には、知的財産戦略本部は、平成15年7月に「知的財産の創造、保護及び活用に関する推進計画」を策定し、その後、我が国の知的財産を取り巻く環境の変化に対応するため、平成16年5月、同計画を改訂し、「知的財産推進計画2004」^(*)を策定し、知的財産の保護に係る施策を推進してきた。

「知的財産推進計画2004」は、「創造分野」、「保護分野」、「活用分野」、「コンテンツビジネスの飛躍的拡大」及び「人材の育成と国民意識の向上」の5章から成り、そのうち第2章の「保護分野」については「知的財産の保護」と「模倣品・海賊版対策」から構成されている。

さらに、「模倣品・海賊版対策」は、「1.外国市場対策を強化する」、「2.水際での取締りを強化する」、「3.国内での取締りを強化する」、「4.中小企業・ベンチャー企業の支援と啓発を強化する」、「5.官民の体制を強化する」及び「6.模倣品・海賊版対策を集中的に処理する」の6項目から構成されている。とりわけ、「3.国内での取締りを強化する」の中においては、「(1)インターネットを利用した侵害の取締りを強化する」として(表3)主に警察に対し、「インターネット・オークションを利用した知的財産権侵害事犯の取締りの強化」が求められている。具体的には、「インターネット・オークションサイト等の管理者による出品者の本人確認の徹底、権利を侵害している出品物のサイトからの削除等を円滑にする方策等取締りの強化の方策」については、警察庁が中心となって検討することとされていることから、これについて、本会議において検討を行うこととした。

(*) 全文については、首相官邸ホームページを参照のこと。

<http://www.kantei.go.jp/jp/singi/titeki2/kettei/040527f.html>

3. 国内での取締りを強化する

(1) インターネットを利用した侵害の取締りを強化する

) インターネットオークションサイト等を通じた多量の模倣品・海賊版の売買及びファイル交換ソフトや技術的保護手段を回避する機器による著作権侵害の問題の深刻さにかんがみ、それに対する取締りを強化するため、以下の項目を含め、2004年度中に、取締方策について幅広く検討を行い、必要に応じ法改正等制度整備を行う。

a) インターネットオークションサイト等の管理者による出品者の本人確認の徹底、権利を侵害している出品物のサイトからの削除等を円滑にする方策等取締りの強化の方策 (警察庁、総務省、経済産業省)

b) 商標法、意匠法等における取締りの強化の方策 (経済産業省)

c) ファイル交換ソフトを用いた著作権侵害に対する取締りの強化等の方策 (文部科学省)

d) 古物営業法における取締り及び犯罪抑止対策の強化の方策 (警察庁)

e) 特定商取引法における消費者の混同を招く表示の取締りの強化の方策 (経済産業省)

) 2004年度以降、オークションサイト等を通じた模倣品・海賊版の売買、映画ファイル等の無許諾アップロード(送信可能可)の警察による取締りを一層強化するとともに、オークションサイト等を通じて発注される模倣品・海賊版の輸入を税関が積極的に取り締まる。(警察庁、財務省)

) 2004年度以降も引き続き、インターネット上の違法コンテンツを常時・自動的に監視するシステムの活用を支援する。(総務省、経済産業省)

表3 「知的財産推進計画2004」からの抜粋

1. インターネット・オークションに係る現状と取組み

インターネット・オークションを利用した知的財産権侵害等の現状及びそれに対する官民の取組み状況は次のとおりである。

(1) 現状

平成 16 年中のサイバー犯罪の検挙件数^(*)のうち、インターネット・オークションを利用した著作権法違反の検挙件数は 105 件で、前年の約 2.4 倍に増加し、ネットワークを利用した著作権法違反に占めるインターネット・オークション利用の著作権法違反の検挙件数の割合も約 6 割を超えている。

一方、インターネット・オークションを利用した商標法違反の検挙件数は 65 件で、前年より 20 件減少した(表 4)。

	H15			H16		
	全体	オークション利用	割合	全体	オークション利用	割合
著作権法違反	87	43	49.4%	174	105	60.3%
商標法違反	95	85	89.5%	82	65	79.3%

【事例 1】無職の男らが、無断で複製した人気アニメーション映画の DVD をインターネット・オークションを利用して販売した。平成 16 年 10 月、著作権法違反で検挙(富山)。
【事例 2】会社役員の男らが、外国有名ブランドに類似する商標を付した腕時計を、インターネット・オークションを利用して販売した。平成 16 年 6 月、商標法違反で検挙(宮城)。

表 4 インターネット・オークションを利用した著作権法違反及び商標法違反の検挙件数

また、平成 16 年中に都道府県警察のサイバー犯罪相談窓口等が受理した相談受理件数 70,614 件のうち、インターネット・オークションに関する相談は 13,535 件であり、前年の約 2.3 倍に増加している(表 5)。代表的な相談は、代金を振り込んでも、品物を送ってこないというものであるが、そのほかにも、インターネット・オークションでコンピュータ・ソフトウェアや音楽 CD を落札したが、送られてきた品が違法コピー品であったなどの相談も寄せられている。

	H15	H16	増減
インターネット・オークションに関する相談	5,999	13,535	+7,536
サイバー犯罪等に関する相談(全体)	41,754	70,614	+28,860

表 5 サイバー犯罪等に関する相談受理件数

(*) 全文については、警察庁サイバー犯罪対策ホームページの統計欄を参照のこと。

<http://www.npa.go.jp/cyber/statics/index.html>

(2) 法整備

インターネット・オークション事業については、古物営業法において、インターネット・オークション事業者に係る盗品等の売買防止等のための規定が整備されているほか、インターネット・オークション事業者に関して、営業の届出、遵守事項（盗品等の疑いがある場合の申告義務、出品者の確認及び取引の記録に関する努力義務）、競りの中止の命令、業務の実施の方法に関する認定制度等が規定されている。

(3) 取組み

ア インターネット・オークション事業者及び ISP 等の取組み

インターネット・オークションを利用した知的財産権侵害事犯については、インターネット・オークション事業者としても自主的な取組みを進めており、具体的には、知的財産権侵害品の出品についての常時監視、情報提供窓口の設置及び利用者への普及啓発等の対策を進めている。また、インターネット・オークション事業者は、知的財産権侵害のおそれのある出品を確認した場合には、自主的な判断により出品の取消しを行っているほか、権利者及び権利者団体（以下「権利者等」という。）からの要請に応じ、速やかに出品を取り消す措置を講ずるなど、権利者等との連携を進めている。

また、テレコムサービス協会等の電気通信事業者団体及び権利者団体、インターネット・オークション事業者等から構成される「プロバイダ責任制限法ガイドライン等検討協議会」では、商標権侵害の書込み等を迅速に削除するため、プロバイダ責任制限法の枠組みの中でのガイドラインの策定について、検討を進めているところである。

イ 権利者団体の取組み

権利者団体では、インターネット・オークションに知的財産権侵害品を出品している者に対する警告や、インターネット・オークション事業者と連携した知的財産権侵害品の出品取消し等に取り組んでいるほか、積極的な捜査協力を実施し、検挙結果について広く消費者に広報啓発することにより、知的財産権侵害事犯の抑止を図っている。

ウ 公的機関の取組み

警察では、知的財産権侵害事犯の取締りを強化するとともに、サイバー犯罪相談窓口での端緒情報の受付や学校等教育機関と連携した広報啓発活動を推進している。また、特許庁では、「模倣品の個人輸入及びインターネット取引に関する事例集」^(*)を公表し、事例の中で、インターネット・オークションサイトでの取引について、

^(*) 全文については、特許庁ホームページの模倣品対策欄を参照のこと。

http://www.jpo.go.jp/torikumi/mohouhin/mohouhin2/jirei/inet_trans_jirei.html

偽ブランドの出品が商標権侵害に該当するおそれがあることを示し、模倣品対策についての周知徹底を図っている。さらに、全国の消費生活センター等においては、インターネット・オークション上のトラブルについての相談を受け付けている。

(4) 問題点

インターネット・オークションを利用した知的財産権侵害に対しては、前述のような取組みが進められているが、現状では次のような問題が指摘されている。

犯罪が発生した場合、一般に、警察は被害者による被害の届出により犯罪を認知し、捜査活動を行うこととなる。しかし、インターネット・オークションを利用した知的財産権侵害事犯の場合は、権利者等による知的財産権侵害品の出品者に対する警告により実際に出品を取り消した者の割合が約 20%であった^(*)ことから分かるように、知的財産権侵害品の出品者は知的財産権侵害の事実を認識しつつ出品を行い、かつ、落札者においても出品物が知的財産権侵害品であることを知りながら落札している場合が多いため、通報が期待されず、結果的に警察が知的財産権侵害事犯として認知できないことが多くなっていると考えられる。

また、出品者も落札者も知的財産権侵害品であることを承知で取引していることから、本人確認の徹底という対策では同種事犯を防止する効果が期待できないという問題もある。

さらに、現在、権利者等とインターネット・オークション事業者が連携して、知的財産権侵害品の出品の取消し及び ID の利用停止措置を講じているが、ID の変更等により反復・継続して出品する悪質な違反者に対しては、いたちごっこになっているのが現状であり、結局のところ、違反出品の取消しをするだけでは十分な解決策にはならないという問題も生じている。

2. 官民連携の在り方

このような現状を踏まえ、インターネット・オークションを利用した知的財産権侵害事犯に対し、政府、事業者及び権利者等による各自の取組みに加え、官民が連携し、犯罪被害の実態やその効果的な防止策について情報交換を行い、実態に即した犯罪被害の防止に努める必要がある。

(*) 社団法人コンピュータソフトウェア著作権協会調べ（資料編 P 95 参照のこと。）

そこで、インターネット・オークションを利用した知的財産権侵害品の効果的な取締り及び同種事犯の効果的な防止を図ることにより、知的財産権の保護を確かなものとするため、権利者等、インターネット・オークション事業者及び捜査機関等が情報を共有し、インターネット・オークション事業者による出品の取消し及び警察による取締りに効果的に活用できるスキームを構築する必要がある（図3）。

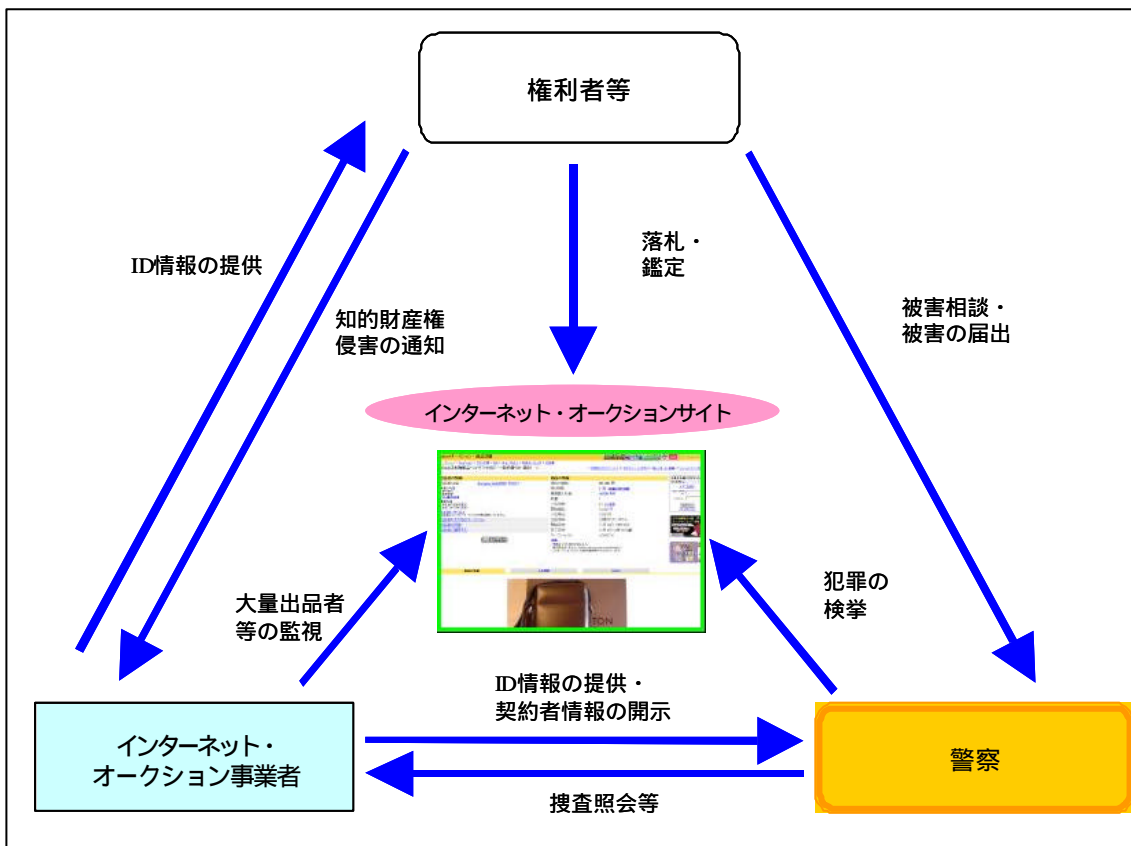


図3 情報共有のスキーム

具体的には、インターネット・オークション事業者は、インターネット・オークションサイトにおける知的財産権侵害品の出品についての監視を行い、知的財産権侵害のお

それのある出品を発見したときには、権利者等に通告する。通告を受けた権利者等は、この情報に基づき出品物が知的財産権侵害品かどうかの鑑定を行い、知的財産権侵害事犯と認められる場合、インターネット・オークション事業者に出品の取消しを求めるとともに、警察に被害の届出を行う。この場合、インターネット・オークション事業者は知的財産権侵害品の出品を取り消し、警察はインターネット・オークション事業者に対して出品者に係る契約者情報を照会し、出品者を特定することにより、当該知的財産権侵害事犯を検挙する、という流れになるのが望ましい。

なお、ここでいう警察による照会とは、契約者情報の開示についての照会であり、捜査関係事項照会書等による照会を想定している。

また、権利者等がインターネット・オークションの利用者からの通告等により知的財産権侵害品のおそれのある出品を発見し、鑑定の上、知的財産権侵害事犯と認めた場合も、同様のスキームにより、インターネット・オークション事業者による出品の取消し及び警察による取締りが円滑に行われることが望ましい。

3. 今後の課題

情報共有のスキームの構築により、インターネット・オークションを利用した知的財産権侵害に対する取組みの強化が期待される一方で、本会議において、この種の問題への対応として検討すべき提案がなされた。

例えば、この種の事犯についても国境を越えて行われる場合があるなど国際連携が不可欠であることから、今後、インターネット・オークションを利用した知的財産権侵害事犯に対する各国の取組みについて各国の産業政策を踏まえつつ検討を進めていく必要があると思われる。

また、この種の事犯の根絶のためには、知的財産権侵害品を利用することが悪質な犯罪を助長する行為であるという点について、初等中等教育の段階から、情報教育の中で積極的に取り上げていくこと等により、利用者の規範意識を向上させることが重要である。

さらに、インターネット社会の特徴である匿名性を悪用した犯罪が他にも後を絶たないことから、匿名性を確保しつつも、追跡性との両立について、今後、検討を進めていくことが必要と考えられる。

第5章 いわゆる「フィッシング」対策の推進について

いわゆる「フィッシング」により入手した情報を利用した詐欺等については、欧米を中心として多額の被害が発生している。我が国においても有名企業を装った偽のホームページが開設され、平成16年末には国内初の金銭的被害が確認されるなど、今後、被害の拡大が懸念されている状況にある。

こうした状況において、「フィッシング」による被害の拡大防止対策を迅速に推進する必要があることから、官民においてどのような連携が必要かについて、本会議の場で緊急に検討を行ったものである。

1. 「フィッシング」とは

「フィッシング」(Phishing)とは、銀行等の企業からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいて個人の金融情報(口座番号、クレジットカード番号、ID、パスワード等)を入力させるなどして個人の金融情報を不正に入手するような行為である(図4)。

フィッシングにより窃取された個人の金融情報は、例えば、インターネット・バンキングの口座から不正にお金を引き出したり、インターネット・ショッピングの商品購入の支払いにクレジットカードを使用したり、偽造カードの作成に利用したりすることにより、不正アクセス行為、電子計算機使用詐欺、詐欺等の犯罪が行われるおそれがある。

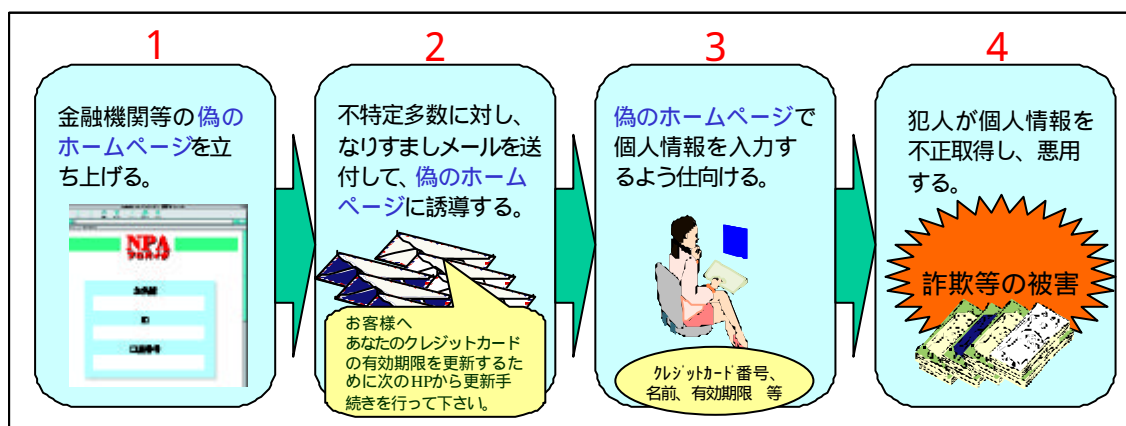


図4 フィッシング事案の流れ

2. 海外における被害状況と取組み

(1) 被害状況

例えば、米国では「フィッシング」による被害が急速に拡大しており、米 Gartner

社の推計^{(*)5}によると、2003 年中に銀行やクレジット会社が受けた損害額は約 12 億ドルとも言われている。他にも、ブラジルでは、フィッシングにより入手した情報を基に、インターネット・バンキングから約 3 千万ドルを搾取した組織犯罪グループが逮捕されるなど、国境のないインターネットの世界で、被害は世界規模の広がりを見せている。

(2) 取組み

こうした状況にかんがみ、米国では、法執行機関、金融機関、ISP、ソフトウェアベンダー、電子商取引事業者、消費者団体等が連携し、APWG (Anti-Phishing Working Group)^{(*)6}を設立して、フィッシング事案の把握及び情報共有を行っている。

3. 「フィッシング」対策について

(1) 政府における取組み

ア 警察の取組み

このようなフィッシングによる被害を未然に防止するためには、偽のホームページが開設されるなどの詐欺に至らない段階で早期に防止、検挙することが不可欠であることから、警察としては、フィッシング行為の早期把握及び被害防止を図るほか、フィッシング行為自体の取締りに努めている。

(ア) 「フィッシング 110 番」の設置及び取締りの強化等

全国の都道府県警察においては、フィッシング事案に関する情報提供を受け付ける「フィッシング 110 番」を設置し、フィッシング事案の早期把握に努めており、平成 17 年 2 月末までに、「フィッシング 110 番」等により全国の警察が把握したフィッシング事案は 43 件である。

また、「フィッシング 110 番」に寄せられた情報等を基に、例えば、なりすましを受けた企業のホームページについての問い合わせが集中することにより、通常業務に支障をきたすような場合は、業務妨害罪の適用を検討するほか、既存の企業のホームページにそっくりな偽のホームページを立ち上げている場合には、著作権法違反の適用を検討するなどによるフィッシング行為自体の取締りを強化している。

(イ) 関係業界団体への要請

関係業界団体に対しては、フィッシング事案を認知した場合等における「フィッシング 110 番」の積極的な活用による迅速な情報提供及び被害拡大防止のた

(*)5 米 Gartner 社の推計については、ホームページを参照のこと。

http://www4.gartner.com/press_releases/asset_71087_11.html

(*)6 詳細についてはホームページを参照のこと。

<http://www.antiphishing.org/>

めの協力について要請を行っている。

また、各企業等に対して、利用者に対するフィッシングに関する広報啓発を推進すること、インターネット上において個人の金融情報等を安易に回答しないような注意喚起を行うこと、フィッシングに関する社員教育を行い、利用者からの相談への適切な対応やフィッシング発生時の迅速な対応による被害の拡大防止に努めることなどについて要請を行っている。

イ 総務省の取組み

インターネット接続サービスを提供する電気通信事業者を中心とする「フィッシング対策推進連絡会」を立ち上げ、情報共有を図るとともに、効果的な対策について検討している。

ウ 経済産業省の取組み

「フィッシング・メール対策連絡会議」の開催による関係者との検討の結果、「フィッシング対策協議会」を設立し、情報収集と広報啓発を積極的に行うこととしている。

(2) 民間分野における取組み

ISPでは、電子署名技術等の技術的対策についての検討を進めているほか、広報啓発や情報共有を進めている。また、フィッシングによりなりすましの対象となるおそれ強い金融業界においても、フィッシング事案について利用者への周知徹底を図っているほか、被害者の救済に向けた取組みも進めている。

4. 今後の課題

官民によるフィッシング対策が推進されつつあるが、現在のところ、フィッシングによる被害の発生を完全に防止するのは困難であるという実状を踏まえ、例えば、各企業等において、そもそもフィッシングページを作られないようなホームページ作りを進めることや、フィッシング対策について欠かせない国際連携を今後強化すべきであることが挙げられる。

また、フィッシングに関する取締りの強化を前提にした上で、インターネット上における追跡性の確保など現行の法制で対応できない点については、新しい枠組みを検討することも重要である。

さらに、フィッシングは、インターネット利用に係る信頼性を根幹からゆるがす重大な問題であるため、今後も官民が連携し、フィッシング被害にあわないスキームの構築に向けて、取組みを推進していく必要がある。