

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

平成18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、とりわけインターネットは、私たちの生活の利便性を向上させるとどまらず、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、サイバー犯罪の増加、インターネット上の違法・有害情報の氾濫、コンピュータ・ウイルスの蔓延が社会問題となるとともに、サイバー空間に対する国民の不安感も急速に高まっており、今、正に官民が連携してより効果的な情報セキュリティ対策を検討・実施すべき時期を迎えている。

「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意見交換を行うことを目的として、平成 13 年度以降開催されているものである。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、防犯団体の方々という広い分野の有識者により、幅広い意見交換が活発に行われており、平成 13 年度以降、毎年度さまざまな内容の報告書を取りまとめてきた。そして、こうした意見交換の結果は、例えば、平成 17 年 10 月の通信事業者及び警察におけるインターネット上の自殺予告事案への対応要領の策定や、平成 18 年 6 月のインターネット・ホットラインセンターの運営開始といった施策に結び付いている。

本年度は、昨年度の議論を踏まえて設置した「インターネット・ホットラインセンター」の今後の運営の在り方について意見交換を行うとともに、インターネットカフェ等における匿名性その他の問題を取り上げ、その解消に向けた対策の在り方について意見交換を行った。各委員には、それぞれが属する企業・組織における知見を背景としつつも、個人としての立場で自由に議論に参加していただいたものである。本報告書は、これらの意見交換の結果を取りまとめたものであり、これが今後の情報セキュリティの向上及び安全・安心なインターネット社会の発展の一助となれば幸いである。

平成 19 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、市民生活や社会・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いく。

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等、高度情報通信ネットワーク社会の光の部分が増長する一方、これに比例するように、サイバー犯罪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対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対する脅威に的確に対処するためには急速に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）レベルでは「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等による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。

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意見交換の場として開催に至ったものであり、本会議における議論が産業界等と警察による情報セキュリティ対策の参考となることを期待するものである。

【これまでの議題】

平成13年度 情報セキュリティ対策における連携の推進

平成14年度 情報セキュリティに関する脅威の実態把握・分析

平成15年度 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

平成16年度 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

平成17年度 インターネット上の違法・有害情報への対応における官民の連携の在り方

総合セキュリティ対策会議委員名簿

前田 雅英 (委員長)	首都大学東京 都市教養学部長
稲垣 隆一	弁護士
江口 研一	KDDI (株) 渉外・広報本部 渉外部次長 ((社) 電気通信事業者協会 移動電話委員会部会長)
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
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 (ACCIS) 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
金野 志保	明治大学法科大学院 特任助教授
下道 高志	サン・マイクロシステムズ (株) チーフ・テクノロジスト
杉浦 昌	日本電気 (株) IT 戦略部 セキュリティ技術センター シニアマネージャー
田中 芳夫	マイクロソフト (株) 技術顧問
西村 達之	セコムトラストシステムズ (株) 代表取締役副社長

廣川 信彦 (社)日本クレジット産業協会 専務理事

別所 直哉 ヤフー(株)法務部長

松井 繁之 (社)日本PTA全国協議会 理事

安田 浩 東京大学 教授

柳沢 治通 (株)NTTドコモ モバイル社会研究所 副所長

吉川 誠司 WEB110 代表

(敬称略・50音順)

(オブザーバー)

内閣官房

総務省

法務省

外務省

文部科学省

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の目的	2
総合セキュリティ対策会議委員名簿	3
目次	5
第 1 章 インターネット・ホットラインセンターの運営状況と今後の運営の在り方	7
1. ホットラインセンターの運営状況	7
(1) 通報受理状況	7
(2) 通報選別状況	8
(3) 通報処理状況	9
(4) 警察におけるホットラインセンターからの通報の活用状況	10
2. ホットラインセンターの今後の運営の在り方	11
(1) 関係機関・団体及び企業との連携の推進	11
(2) 情報分析能力の向上等	15
第 2 章 インターネットカフェ等における匿名性その他の問題と対策	16
1. 匿名性の問題等	17
(1) 犯罪捜査における匿名性の問題	17
(2) インターネット上の自殺予告事案への対応における匿名性の問題	19
(3) インターネットカフェの現状と問題点	20
2. 匿名性その他の問題への対策の在り方	26
(1) インターネットカフェに係る対策の推進	26
(2) プリペイド式データ通信カード等に係る対策の推進	29

資料編

1. 平成 18 年のサイバー犯罪の検挙及び相談状況について	1
2. 不正アクセス行為の発生状況等の公表について	11
3. 平成 18 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	113
4. 平成 18 年中のインターネット上の自殺予告事案への対応について	120
5. 委員等発表資料	
ホットラインセンター開所までの経緯	121
ホットラインネットワークの在り方について	129
インターネット上の違法・有害情報に係る業界の取組について	142
複合カフェ業界の現状と課題	145
ネットカフェにおける利用者情報の取得と管理上の課題	151

第 1 章 インターネット・ホットラインセンターの運営状況と今後の運営の在り方

現在、インターネット上には、児童ポルノ画像、わいせつ画像、規制薬物の販売に関する情報等の違法情報が多数存在している。また、こうした違法情報のほか、爆発物の製造方法や公的証明書の偽造方法等を教示する情報、殺人等の違法行為の請負等に関する情報、他人を自殺に勧誘する情報等の有害情報も氾濫している。

こうした状況を踏まえ、本会議においては、平成 17 年度に、インターネット上の「ホットライン」の必要性及びその運営の在り方について意見交換を行い、報告書を取りまとめた。これを踏まえ、警察庁では、平成 18 年 6 月に民間委託によりインターネット・ホットラインセンター（以下「ホットラインセンター」という。）の運営を開始したところである。

平成 18 年度は、ホットラインセンターの運営状況を踏まえ、今後の運営の在り方について意見交換を行った。

1. ホットラインセンターの運営状況

平成 18 年 6 月の運用開始から同年 11 月までの 6 か月間におけるホットラインセンターの運営状況は次のとおりである。

(1) 通報受理状況

ホットラインセンターでは、ウェブサイト上に設けた通報フォームにより、インターネット利用者から 23,739 件の通報を受理した。

図 1 通報受理件数の推移

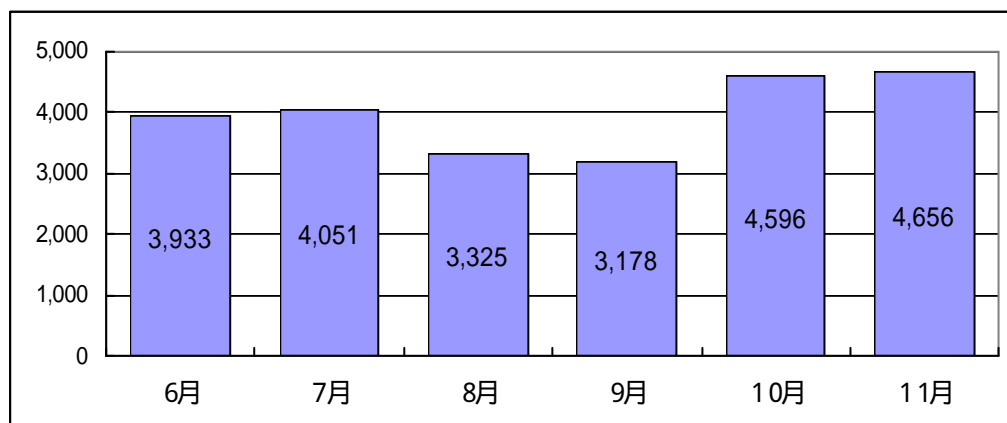


表 1 通報者が通報フォームにおいて選択した項目

違法情報として通報	
通報者が選択した項目	
わいせつ関連情報	16,764
薬物関連情報	732
振り込め詐欺等関連情報	1,699
小計 (A)	19,195
有害情報として通報	
通報者が選択した項目	
違法行為を直接的かつ明示的に請負・仲介・誘引等する情報	599
違法情報該当性が明らかであると判断することは困難であるが、その疑いが相当程度ある情報	2,717
人を自殺に誘引・勧誘する情報	244
小計 (B)	3,560
通報者が選択せずに通報	
非選択 (C)	984
総計	
(A) + (B) + (C)	23,739

(2) 通報選別状況

ホットラインセンターでは、受理した通報をホットライン運用ガイドライン^(注1) (以下「運用ガイドライン」という。)に基づいて選別し、2,226件(9.0%)を違法情報、502件(2.0%)を有害情報、22,128件(89.0%)を運用ガイドラインの対象外の情報と判断した^(注2)。

表 2 選別結果件数の内訳(違法情報)

違法情報	選別結果件数	
	国内のサーバに設置	海外のサーバに設置
わいせつ物公然陳列	471	538
児童ポルノ公然陳列	295	228
売春防止法違反の広告	1	0
出会い系サイト規制法違反の誘引行為	55	1
薬物関連情報	325	1
口座売買等の勧誘・誘引	141	16
携帯電話の匿名貸与業・無断譲渡業等の勧誘・誘引	139	15
合計	1,427	799

(注1) ホットラインセンターにおいて対象とする違法・有害情報の範囲、判断基準等について定めたガイドライン。ホットラインセンターのウェブサイト (<http://www.internethotline.jp/guideline/index.html>) 参照。

(注2) 選別の結果、1件の通報に係る情報の中に、複数の種類の違法・有害情報が含まれている場合(同一のウェブサイトにはわいせつ画像と児童ポルノ画像が存在する場合等)があり、このような場合には重複して計上しているため、通報受理件数(23,739件)と選別結果件数(2,226件+502件+22,128件=24,856件)は一致していない。

表 3 選別結果件数の内訳（有害情報）

有害情報	選別結果件数	
	国内のサーバに蔵置	海外のサーバに蔵置
違法行為を直接的かつ明示的に請負・仲介・誘引等する	251	191
違法情報該当性が明らかであると判断することは困難であるが、その疑いが相当程度ある情報	22	10
人を自殺に誘引・勧誘する情報	23	5
合計	296	206

表 4 選別結果件数の内訳（運用ガイドライン対象外の情報）

運用ガイドライン対象外の情報	選別結果件数
名誉毀損、誹謗中傷	270
殺害予告、爆破予告	131
知的財産権侵害情報	411
まんが子どもポルノ	35
一般的なポルノサイト	3,006
一般的な出会い系サイト	14,360
いずれにも入らないもの	3,915
合計	22,128

(3) 通報処理状況

ホットラインセンターでは、違法情報に係る通報のうち、1,203件について警察へ通報するとともに、そのうちの707件についてプロバイダや電子掲示板の管理者等（以下「プロバイダ等」という。）に対して削除を依頼した。その結果、572件（80.9%）の違法情報がインターネット上から削除された。

表 5 通報処理状況の内訳（違法情報）

違法情報	処理結果件数			
	通報前に削除	通報・削除依頼先		
		警察	プロバイダ等	削除
わいせつ物公然陳列	104	367	233	183
児童ポルノ公然陳列	78	217	103	70
売春防止法違反の広告	1	0	0	0
出会い系サイト規制法違反の誘引行為	7	48	32	29
薬物関連情報	25	300	93	79
口座売買等の勧誘・誘引	5	136	125	102
携帯電話の匿名貸与業・無断譲渡業等の勧誘・誘引	4	135	121	109
合計	224	1,203	707	572

また、有害情報に係る通報のうち、217件についてプロバイダ等に対して削除を依頼した。その結果、150件（69.1%）の有害情報がインターネット上から削除された。

表 6 通報処理状況の内訳（有害情報）

有害情報	処理結果件数		
	依頼前に削除	プロバイダ等に 削除を依頼	削除
違法行為を直接的かつ明示的に請負・仲介・誘引等する情報	56	179	118
違法情報該当性が明らかであると判断することは困難であるが、その疑いが相当程度ある情報	2	20	14
人を自殺に誘引・勧誘する情報	5	18	18
合計	63	217	150

さらに、運用ガイドラインの対象外の情報に係る通報のうち、名誉毀損、誹謗中傷に該当する情報に係るもの132件については法務省人権擁護局に、知的財産権侵害情報に係るもの36件については権利者団体に、まんが子どもポルノに係るもの14件についてはこれに関する国際的な活動を行っているNGOに、それぞれ情報提供を行った。

このほか、フィッシングサイトに係る通報、児童へのいたずら仲間を募集する書き込みのある電子掲示板に係る通報等、犯罪防止の観点から対応が必要と考えられる通報23件については、警察に情報提供を行った。

表 7 通報処理状況の内訳（運用ガイドライン対象外の情報）

運用ガイドライン対象外の情報	処理結果件数	
	情報提供前に 削除	関係機関への 情報提供
名誉毀損、誹謗中傷	0	132
殺害予告、爆破予告	0	0
知的財産権侵害情報	1	36
まんが子どもポルノ	3	14
一般的なポルノサイト	0	0
一般的な出会い系サイト	0	0
いずれにも入らないもの	0	23
合計	4	205

こうした措置に加えて、これらの違法・有害情報や運用ガイドラインの対象外の情報が掲載されたウェブサイトの多くについて、フィルタリング事業者に情報提供を行った。

(4) 警察におけるホットラインセンターからの通報の活用状況

ホットラインセンターが警察に通報した違法情報は、捜査に活用されており、警察では、これまでに、ホットラインセンターからの通報を端緒として

- わいせつ物公然陳列事件 2件
- 児童買春・児童ポルノ法違反事件（児童買春） 2件
- （児童ポルノ） 1件
- 出会い系サイト規制法違反事件（不正誘引） 2件

を検挙している。

【事例 1】

女子中学生(13)は、平成18年6月、携帯電話からアクセスすることのできる出会い系サイトにおいて人を児童との性交等の相手方となるように誘引した。同年9月、同女を補導するとともに、同年10月、同女に対して現金を供与することを約束し、同女と性交した会社員の男(40)を児童買春・児童ポルノ法違反(児童買春)で逮捕した(山梨県警察)。

【事例 2】

会社員の男(30)は、平成18年10月、電子掲示板にわいせつ画像及び児童ポルノ画像を公然と陳列した。平成19年1月、同人をわいせつ物公然陳列罪で逮捕するとともに、同月、児童買春・児童ポルノ法違反(児童ポルノ公然陳列)で追送致した(山口県警察)。

2. ホットラインセンターの今後の運営の在り方

上記のとおり、ホットラインセンターではインターネット利用者から多くの通報を受理しており、それらの通報が警察による事件検挙やプロバイダ等による多数の違法・有害情報の削除に結び付くなど、その活動は一定の成果を上げているとすることができる。

他方で、ホットラインセンターの存在やその活動内容は、未だ多くの国民に認知されているとは言い難い状況にある。また、ホットラインセンターで受理した通報のうち、海外に所在するウェブサーバに蔵置されている情報及び運用ガイドラインの対象外の情報に係るものについては、一部を除いて特段の対応を行っておらず、通報者の要望に十分に答え切れていない状況にある。

今後、ホットラインセンターが、国民の理解・協力の下でその機能を十分に発揮し、通報者の要望に的確に対応していくためには、次のような取組みを更に推進していく必要がある。

(1) 関係機関・団体及び企業との連携の推進

ア 「ホットラインネットワーク」の拡大

現在、ホットラインセンターでは、その存在や活動内容について国民に周知を図るとともに、運用ガイドラインの対象外の情報に係る通報にも可能な限り対応するため、関係機関・団体及び企業との連携強化に努めている。

具体的には、

ホットラインセンターの活動内容等に関する広報活動に協力する関係機関・団体及び企業を「パートナー」

運用ガイドラインの対象外の情報について対応を行う関係機関・団体を「アソシエイツ」

として位置付け、これらの関係機関・団体及び企業から構成される「ホットラインネットワーク」の拡大に努めているところである。

今後、ホットラインセンターの活動をより効果的なものとするため、「ホットラインネットワーク」を更に拡大し、次のような取組みを重点的に推進していく必要がある。

(ア) ホットラインセンターの活動内容等に関する広報活動

ホットラインセンターが十分に機能を発揮するためには、その存在が国民に認知され、その活動について理解が得られていることが前提となる。

現在、ホットラインセンターでは、ウェブサイト上で活動内容、統計資料等についての情報発信を行うとともに、インターネット利用者がホットラインセンターのウェブサイトを読覧する機会を増加させるため、「パートナー」が開設しているウェブサイト上に、ホットラインセンターのウェブサイトへのリンクを設定してもらっている。

しかし、「パートナー」の数はまだ三つにとどまるなど、広報活動は十分とは言えない状況にある。

今後、ホットラインセンターの活動内容等について更に国民に周知を図るため、「パートナー」の数の一層の増加に努める必要がある。その際には、従来のようなインターネット関連企業を中心とした協力依頼にとどまらず、広く他の業種の企業等に対しても協力を呼び掛けていく必要があり、これらの企業等においては、そのウェブサイト上にホットラインセンターのウェブサイトへのリンクを設定するなどの協力を行うことが期待される。

【参考】平成 19 年 3 月現在の「パートナー」



パートナーとは

ホットラインセンターの活動を理解して、その活動を様々な形でサポートしていただける関係機関・団体・企業等です。

ネット安全運動など、問題点について広く議論するアピールの場を設けたら、センターに通報していただき、お方への情報提供などを行ってまいります。

◆パートナー

・日本CA株式会社



安全かつ快適にインターネットをご活用いただくため、パソコンのセキュリティについてのさまざまな情報を提供中

・ヤフー株式会社



Yahoo! JAPANの社会的な取組

・財団法人 日本ユニセフ協会



ユニセフは世界で子どもと母親を中心とした社会開発活動を人道的見地から行なっています。

財団法人 日本ユニセフ協会は、日本におけるユニセフを代表する国内委員会です。

ホットラインセンターのウェブサイト (<http://www.internethotline.jp/partner/index.html>) から転載。

(イ) 運用ガイドラインの対象外の情報に係る通報に対する的確な対応

ホットラインセンターが通報者の要望に十分に答えるためには、違法・有害情報に係る通報が警察による事件検挙やプロバイダ等による当該情報の削除に確実に結びつくとともに、運用ガイドラインの対象外の情報に当たる場合であっても、他の関係機関・団体において所要の措置が講じられることが必要である。

しかし、上記 1.(2) のとおり、ホットラインセンターにおいて選別した情報の 89.0% が運用ガイドラインの対象外の情報と判断されており、そのうち「アソシエイツ」等に対応を依頼しているものは、上記 1.(3) 表 7 のとおり、ごく一部 (205 件) にとどまっている^(注3)。

このため、今後、特段の対応がとられていない通報の内容を分析した上で、当該通報に的確に対応し得る機関・団体等に対し、「アソシエイツ」としての協力を呼び掛けていく必要がある。

【参考】平成19年3月現在の「アソシエイツ」

アソシエイツ
| パートナー | アソシエイツ |

アソシエイツとは

ホットラインセンターの活動を理解して、その活動を様々な形でサポートしていただける関係機関・団体・企業等です。

ホットライン運用ガイドラインにおいて取り扱いの対象としない通報も数多く寄せられることから、これらの通報に種別に応じて的確に対応するために、センターの活動に協力していただいております。

◆ **アソシエイツ**

・社団法人コンピュータソフトウェア著作権協会



コンピュータソフトウェアの不正コピーなどの情報提供を受け付け、デジタル著作物の権利保護の活動を行っております。

・ECFAT/ストップ子ども買春の会



子ども買春、子どもポルノ、性目的の子ども的人身売買根絶をめざしています。

・ネットスター株式会社



パソコン・携帯電話向けフィルタリングや迷惑メール対策に使われる URL データベース収集・配信の専門企業です。

・有限責任中間法人ユニオン・デ・ファブリカン



知的財産権を保護するとともに、一般消費者の利益を守るため、国内に流通する偽造品・不正商品の排除を目的として活動しています。

ホットラインセンターのウェブサイト (<http://www.internethotline.jp/partner/index2.html>) から転載。

(注3) このほか、上記 1.(3) のとおり、違法・有害情報や運用ガイドラインの対象外の情報が掲載されたウェブサイトの多くについて、「アソシエイツ」であるフィルタリング事業者に情報提供を行っている。

イ 海外関係機関との連携の推進

インターネット上の違法・有害情報への対策は、各国の関係機関・団体が緊密に連携して推進することにより、初めて効果的なものとなる。

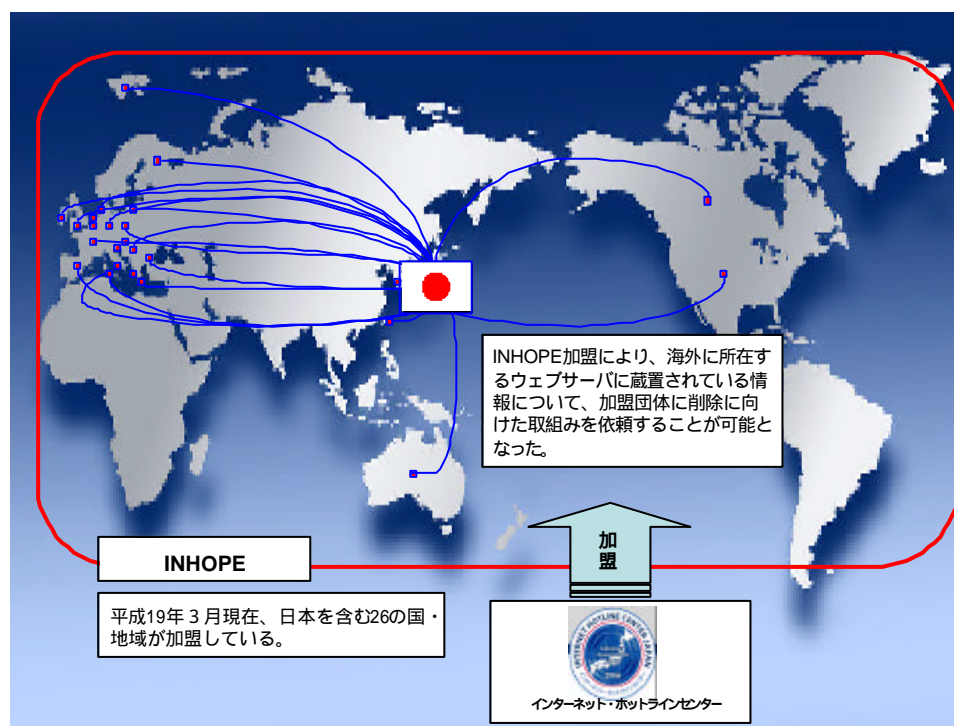
米国、英国、ドイツ、フランスを始めとする諸外国においては、既に「ホットライン」が運営されており、1999年（平成11年）には、これら諸外国の「ホットライン」相互間の連絡組織である INHOPE(Internet Hotline Providers in Europe Association)が設置されている。INHOPE 加盟団体においては、インターネット上の違法情報等が外国に所在するウェブサーバに蔵置されている場合、当該外国の INHOPE 加盟団体に対してその削除に向けた取組みを依頼するなどしているところである。

我が国においては、上記1.(2)表2及び表3のとおり、違法・有害情報の36.8%が海外に所在するウェブサーバに蔵置されている状況にあるが、ホットラインセンターは、設置当初、INHOPE に加盟していなかったことから、これらの情報について特段の対応をとることができなかった。

こうした状況を踏まえ、ホットラインセンターでは、INHOPE への加盟のための手続を進め、平成19年3月に加盟が承認されたところである。

INHOPE への加盟により、ホットラインセンターと他の INHOPE 加盟団体との間で相互に違法情報等の削除に向けた取組みの依頼を行うことが可能になったことから、ホットラインセンターにおいては、この枠組みを十分に活用し、違法・有害情報対策を一層強力に推進していく必要がある。

図2 海外関係機関との連携（イメージ）



(2) 情報分析能力の向上等

インターネット上の違法・有害情報は、絶えずその内容、傾向等が変化しているため、当該情報についての的確な対応を行うためには、その内容、傾向等を継続的に分析する必要がある。

また、上記のとおり、ホットラインセンターにおいて選別した情報の 89.0%が運用ガイドラインの対象外の情報と判断されており、当該情報に対する国民の関心の高さがうかがわれる。このため、これらの情報についても分析を行い、インターネット利用者がどのような情報について問題意識を有し、また、ホットラインセンターにどのような役割を期待しているのかを把握する必要がある。

しかし、現在、ホットラインセンターの職員は、1日当たり約 130 件に上る通報を、運用ガイドラインに基づいて選別・処理することで忙殺されており、それに加えて上記のような新たな分析を行うことは不可能である。このため、早急にホットラインセンターの体制強化を図り、情報分析能力を向上させる必要がある。また、こうした情報分析能力の向上に資する調査研究、当該能力の向上のために活用し得る技術の開発・導入等にも取り組むべきである。

なお、違法・有害情報の内容、傾向等や、インターネット利用者の問題意識等に関する分析結果を踏まえ、必要があれば、運用ガイドラインの見直しも含めた業務改善措置を講じるべきである。

第 2 章 インターネットカフェ等における匿名性その他の問題と対策

サイバー犯罪は、匿名性が高い、痕跡が残りにくい、地理的・時間的制約を受けることなく、短期間のうちに不特定又は多数の者に被害を及ぼす、といった特徴を有しており、犯罪を行う者にとっては、その所在を特定されにくいなど、インターネットは極めて好都合な犯行の手段となっている。現に、サイバー犯罪は年々増加しており、平成 18 年中のサイバー犯罪の検挙件数は 4,425 件と、前年より 1,264 件（40.0%）増加し、過去最高となった。

表 1 サイバー犯罪の検挙件数の内訳（平成 13 年～18 年）

罪 名	年						増 減
	H 1 3	H 1 4	H 1 5	H 1 6	H 1 7	H 1 8	
不正アクセス禁止法違反	67	105	145	142	277	703	+ 426 (+ 153.8%)
コンピュータ・電磁的記録対象犯罪	63	30	55	55	73	129	+ 56 (+ 76.7%)
電子計算機使用詐欺	48	18	34	42	49	63	+ 14 (+ 28.6%)
電磁的記録不正作出・毀棄	11	8	12	8	17	56	+ 39 (+ 229.4%)
電子計算機損壊等業務妨害	4	4	9	5	7	10	+ 3 (+ 42.9%)
ネットワーク利用犯罪	1,209	1,471	1,649	1,884	2,811	3,593	+ 782 (+ 27.8%)
詐欺	485	514	521	542	1,408	1,597	+ 189 (+ 13.4%)
児童買春・児童ポルノ法違反（児童買春）	117	268	269	370	320	463	+ 143 (+ 44.7%)
児童買春・児童ポルノ法違反（児童ポルノ）	128	140	102	85	136	251	+ 115 (+ 84.6%)
商標法違反	31	37	95	82	109	218	+ 109 (+ 100.0%)
青少年保護育成条例違反	10	70	120	136	174	196	+ 22 (+ 12.6%)
わいせつ物頒布等	103	109	113	121	125	192	+ 67 (+ 53.6%)
著作権法違反	86	66	87	174	128	138	+ 10 (+ 7.8%)
その他	249	267	342	374	411	538	+ 127 (+ 30.9%)
合 計	1,339	1,606	1,849	2,081	3,161	4,425	+ 1,264 (+ 40.0%)

サイバー犯罪が発生した場合、警察では、当該犯罪が行われた時点のログ等から、どのコンピュータにおいて犯罪が行われたかを特定するとともに、そのコンピュータを誰が使用していたのかを明らかにし、被疑者を特定することが必要である。しかし、近年、インターネットカフェ、プリペイド式データ通信カード、フリースポット等のように、不特定の者がインターネットを利用することができる施設・サービスが増加しており、それらの中には、利用や機器購入の際に本人確認を行わないものも見られるところである。こうした利用者の匿名性の高い施設・サービスがサイバー犯罪に利用された場合には、仮にログ等から犯行に使用されたコンピュータ、プリペイド式データ通信カード、無線 LAN カード等を特定することができたとしても、これらを使用した被疑者を特定することは困難である。

また、この匿名性の問題は、犯罪捜査の分野に限られたものではない。例えば、こうした利用者の匿名性の高い施設・サービスを利用した情報発信により、特定の者の権利利益が侵害された場合には、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成 13 年法律第 137 号）に基づきプロバイダ等から発信者情報の開示を受けたとしても、被害者が加害者を特定して責任追及を行うことは困難である。さらに、当該施設・サービスを利用した自殺予告その他の緊急対応を要する事案が発生した場合に

は、プロバイダ等から発信者情報の開示を受けたとしても、警察が発信者を特定して迅速・的確に説諭等の措置を講じることは困難である。

こうした状況を踏まえ、本会議では、インターネットカフェを中心に、インターネット利用者の匿名性その他の問題を取り上げ、当該問題の解消に向けた対策の在り方について意見交換を行った。

1. 匿名性の問題等

(1) 犯罪捜査における匿名性の問題

上記のとおり、インターネット利用者の匿名性は、サイバー犯罪の捜査の大きな障壁となっている。

例えば、インターネットカフェでは、事業者が利用者の本人確認を行い、コンピュータの使用状況を記録していなければ、犯行に使用されたコンピュータが判明したとしても、それを使用した被疑者を特定することは困難である。また、不特定の者が利用することができるフリースポットや、購入時に本人確認が不要なプリペイド式データ通信カードを使用してサイバー犯罪が行われた場合、被疑者の特定は非常に困難である。現にこの匿名性を悪用した事案の発生も見られる。

平成 17 年中に警察が認知した不正アクセス行為 592 件のうち、平成 18 年 5 月末の時点で未検挙のものは 277 件であり、そのうち 212 件（認知件数の 35.8%、未検挙の件数の 76.5%）は、匿名性が障害となって捜査に進展が見られないものである。中でも、インターネットカフェのコンピュータが使用され、当該店舗又は当該コンピュータまでは判明したものの、利用者に関する情報が存在しないために捜査に進展が見られないものが 139 件（認知件数の 23.5%、未検挙の件数の 50.2%）と、多数に上っている。

図 1 インターネットカフェを利用した犯罪の捜査

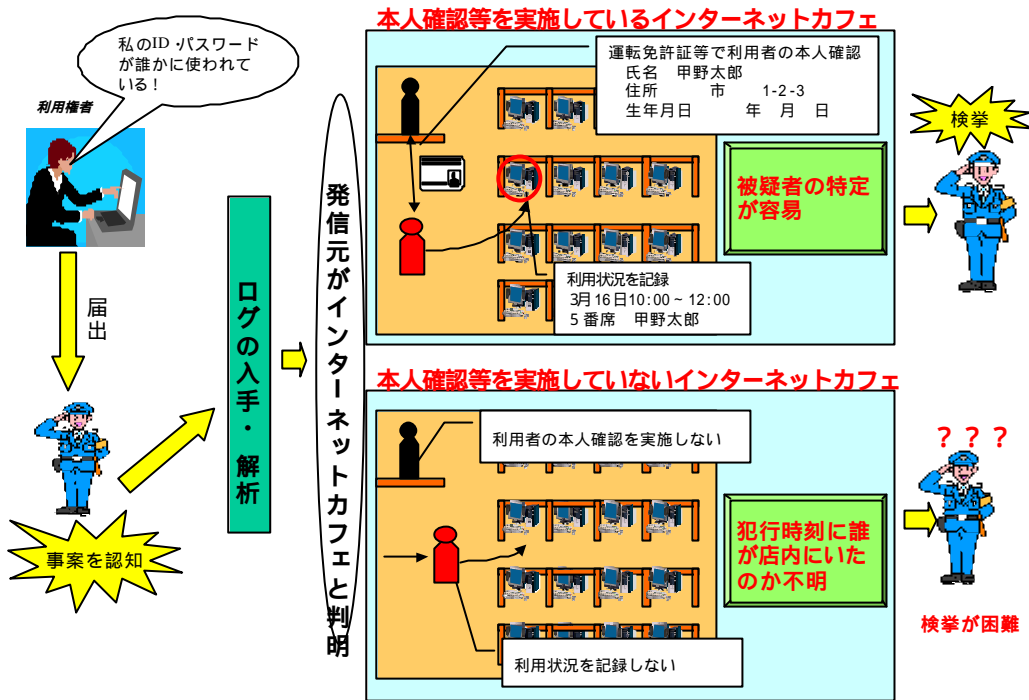
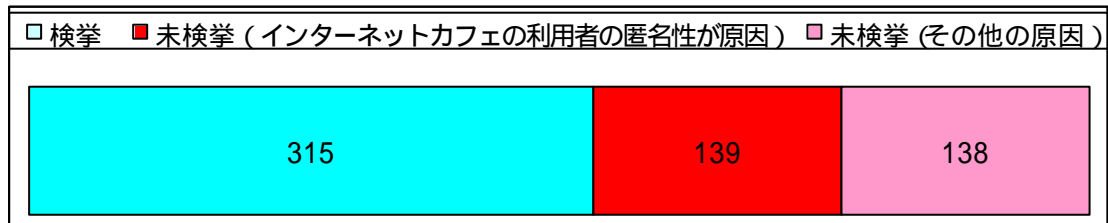
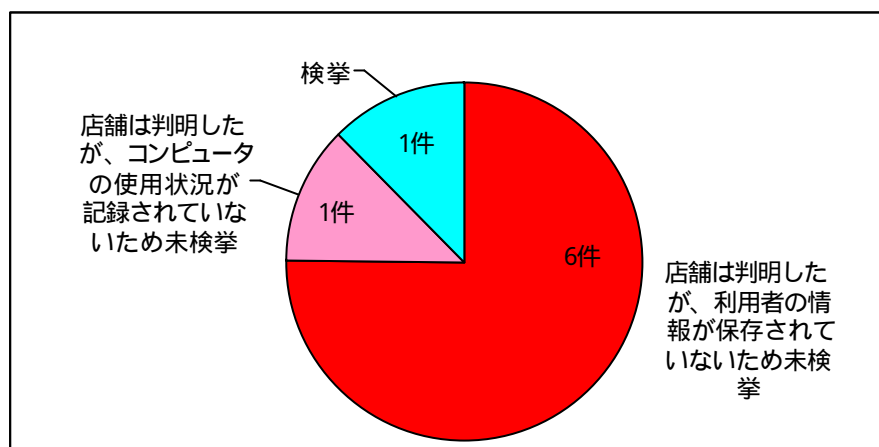


図 2 平成 17 年中に認知した不正アクセス行為の検挙状況 (平成 18 年 5 月末現在)



また、首都圏及び近畿地方の二つの都道府県警察では、平成 18 年 1 月から同年 3 月までの 3 か月間に、インターネット・オークションを利用した詐欺 (以下「ネット・オークション詐欺」という。) のうちインターネットカフェのコンピュータを使用したものを 8 件認知しているが、そのうち平成 19 年 2 月 1 日までに検挙に至ったものは 1 件にとどまっている。未検挙の理由としては、ログ等から犯行に使用された店舗又はコンピュータまでは判明したものの、利用者に関する情報が存在しないために被疑者を特定することができないものが 6 件、利用者に関する情報は存在するがコンピュータの使用状況が記録されていないために被疑者を特定することができないものが 1 件となっており、インターネットカフェの利用者の匿名性が捜査の障壁となっている状況がうかがわれる。

図3 インターネットカフェのコンピュータを使用したネット・オークション詐欺の検挙状況
 (2 都道府県警察において平成 18 年 1 月から同年 3 月までに認知したもの。平成 19 年 2 月 1 日現在)



他方、匿名性を悪用したサイバー犯罪であっても、例えば数多くの関係者からの事情聴取、様々な電子データの解析等を通じて被疑者の特定に成功し、検挙に至る場合がある。しかし、その際には、膨大な捜査体制や費用を要し、かつ、捜査期間が長期にわたることが通例であり、捜査の効率は決して高いとは言い難い。また、捜査に協力する国民にとっては、数多くの照会、事情聴取等に応じる事実上の負担が大きく、さらに、納税者としての立場から見ても、捜査の効率が低いことは望ましいことではない。

こうした状況を踏まえ、サイバー犯罪の迅速かつ確実な検挙を可能にするための一つの方策として、利用者の匿名性の高い施設・サービスにおける匿名性の排除に向けた取組みを官民が連携して推進していく必要があり、特に、サイバー犯罪に悪用されやすいインターネットカフェについては、こうした取組みが急務となっている。

(2) インターネット上の自殺予告事案への対応における匿名性の問題

現在、警察がインターネット上の自殺予告事案を認知した場合において、緊急対応を要すると認められるときは、プロバイダ等から発信者情報の開示を受け、発信者やその家族に説諭等の措置を講じているところである(注1)。

(注1) 本会議では、平成 16 年度に、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応を必要とする事案が発生した場合の対応の在り方について意見交換を行い、その結果を踏まえ、平成 17 年 10 月、通信事業者団体が「インターネット上の自殺予告事案への対応に関するガイドライン」を、また、警察庁が「インターネット上での自殺予告事案に係る対処要領」を、それぞれ策定した。同ガイドラインについては社団法人テレコムサービス協会のウェブサイト (http://www.telesa.or.jp/consortium/other/guideline_suicide_051005.pdf) 参照。

図 4 インターネット上の自殺予告事案への対応状況（平成 17 年 10 月～18 年 12 月）

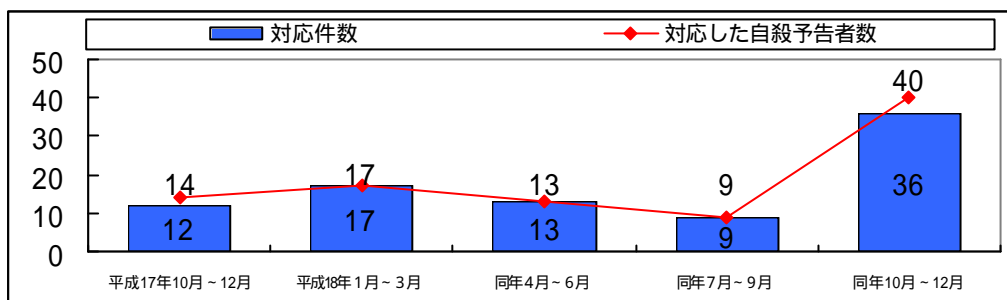
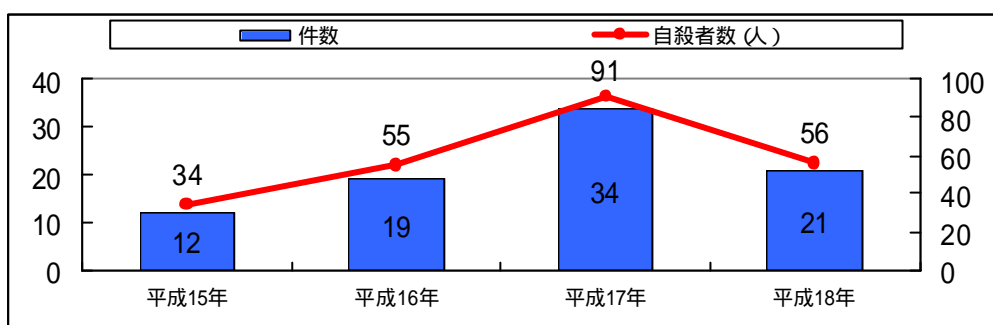


図 5 いわゆる自殺サイトで知り合った者による自殺事案の発生状況（平成 15 年～18 年）



しかし、利用者の本人確認等を行っていないインターネットカフェのコンピュータを使用して自殺予告が行われた場合には、発信者情報から自殺予告者を特定することが困難であり、人命の保護に支障を来すおそれがある。このため、インターネットカフェの利用者の匿名性の排除に向けた取組みを官民が連携して推進していく必要がある。

なお、現に、最近、インターネットカフェのコンピュータを使用して自殺予告が行われ、プロバイダ等から開示を受けた発信者情報によって当該店舗までは判明するものの、利用者の本人確認を行っていないために自殺予告者を特定することができない事案の発生が見られるところである。

【事例】

平成17年10月、インターネット上の電子掲示板への自殺を予告する書き込みに関する通報を受け、プロバイダから発信者情報の開示を受けて調査を行った結果、インターネットカフェのコンピュータからの書き込みであることが判明した。しかし、同店舗では利用者の本人確認を行っていなかったため、自殺予告者の特定には至らなかった。

(3) インターネットカフェの現状と問題点

本会議では、上記のとおり、特にインターネットカフェの利用者の匿名性の排除が急務となっていることを踏まえ、第4回会議及び第6回会議において、インターネットカフェ及びインターネット接続が可能なコンピュータを客の利用に供していない漫

画喫茶等（以下単に「漫画喫茶等」という。）の事業者から成る日本複合カフェ協会（注 2）の出席を得て、インターネットカフェの現状と問題点について聴取した。

ア 店舗数

日本複合カフェ協会の調査によると、平成 17 年 9 月現在、インターネットカフェ及び漫画喫茶等は、全国に 2,737 店舗存在しているとされる。平成 16 年 8 月現在では、2,505 店舗存在していたとされることから、1 年強の間に 232 店舗増加したことになる。

イ 事業者団体の取組み

日本複合カフェ協会は、インターネットカフェ及び漫画喫茶等の業界における唯一の事業者団体であり、平成 18 年 10 月現在、1,322 店舗がこれに加盟している。同協会の調査によると、総店舗数に占める同協会に加盟している店舗数の割合は、平成 17 年 9 月現在、41.3%とされる。

表 2 店舗数等の推移（平成 16 年～18 年 日本複合カフェ協会調べ）

	平成16年 8月	平成17年 9月	平成18年10月
店舗数 (A)	2,505店舗	2,737店舗	-
協会加盟店舗数 (B)	697店舗	1,130店舗	1,322店舗
協会加盟率 (B ÷ A × 100)	27.8%	41.3%	-

同協会では、加盟店舗数の増加に努めるとともに、犯罪防止、青少年の非行防止、業界の健全発展等を図るため、運営ガイドライン（注 3）を策定し、これに従った店舗運営を加盟店舗に推奨している。また、同ガイドラインに従った店舗運営を行っている加盟店舗に対し、「優良店」と明記した証明書を交付しており、当該店舗ではこれを入口に掲示するなどしている。同ガイドラインの主な内容は、次のとおりである。

（注 2）平成 13 年 7 月に設立された任意団体。同協会のウェブサイト（<http://www.jcca.ne.jp>）参照。

（注 3）同協会のウェブサイト（<http://www.jcca.ne.jp/>）参照。

制定 平成 15 年 8 月 29 日
改定 平成 17 年 9 月 1 日

運営ガイドライン（抄）

日本複合カフェ協会

店舗運営

1. 会員制度の採用
ネットワーク利用犯罪やその他の犯罪の抑制または防止、及び利用客の身元を確認するため、利用客について会員制度を採用するよう努めなければならない。
 2. 防犯カメラなどの設置
防犯対策及び青少年対策をさらに効果的なものとするため、店内には防犯カメラなどを設置するよう努めなければならない。
 3. 客席の見通しの確保及び照度
客席は、周囲より見通しの確保されたオープン席と三方を囲まれたブース席とし、ブース席については通路から客席内の全体を容易に見通せる構造とし、つい立て、柵、カーテン、植木鉢等により遮蔽してはならない。（略）
- ### 青少年対策
1. 年齢の確認
利用客を入店させるに際し、未成年者または 18 歳未満の青少年等と思われる者に対して身分証明証等の提示を求め、その年齢を確認するものとする。
 2. 利用時間の制限
16 歳未満の利用客には午後 8 時以降、18 歳未満の利用客には午後 10 時以降の利用を認めないものとする。
 3. 青少年に対する措置
 - (1) 客席の取扱い
18 歳未満の利用客に対しては、オープン席を利用させるものとする。
 - (2) ~ (4) (略)
 - (5) 青少年に有害なインターネット上のコンテンツ対策
18 歳未満の利用客に対しては、有害情報等へのアクセスを制限するフィルタリングシステムを導入したパソコンを設置した客席へ案内するなどして、それらのパソコンを利用させるよう努めるものとする。（略）
 - 4・5. (略)
- ### インターネットのセキュリティ確保及びネットワーク利用犯罪の防止
1. (略)
 2. セキュリティ対策
不正アクセスやコンピュータ・ウイルス等による被害及びネットワーク利用犯罪を防止するため、利用履歴を削除するソフトやリカバリーソフトをパソコンにインストールするなどの措置をとるよう努めなければならない。また、パソコンやサーバー等の OS・ソフトの脆弱性対策、一定のプログラム（ウイルス、キーロガー等）の実行制限、不正なアクセスを防ぐシステム（ファイアーウォール）の設置、及びルータやモデム等の制御機器の初期パスワード変更、などについても、措置を講ずることが望ましい。
- ### 個人情報の取扱いについて
1. (略)
 2. プライバシーへの配慮
会員制採用の有無に拘らず、個人情報保護の精神に準じ、利用客間相互においても、それぞれの利用客の店内利用行動等のプライバシーに属する事項が他の利用客に徒に侵害されることのないよう十分な配慮をしなければならない。
- ### 管理及び雑則
1. 店舗管理者の選任
店舗ごとに管理者を置き、本ガイドラインの運用を含めた店舗における管理を徹底しなければならない。なお、店舗管理者は 20 歳以上の者とする。
 - 2 ~ 5. (略)

ウ 主な問題点

日本複合カフェ協会では、上記イのとおり、運営ガイドラインに従った店舗運営を推奨しているが、これに従うか否かはあくまで各加盟店舗の判断に委ねられている。同協会によると、インターネットカフェ及び漫画喫茶等の利用者の中には、入店時の本人確認を煩わしく感じたり、個室の利用を好んだりする者も多い

ことから、会員制度の導入や客席の見通しの確保によって利用者が減少することを懸念し、こうした措置をとることに消極的な加盟店舗が存在する。また、フィルタリング・システム等の導入についても、それにより経済的負担が増加することなどから、消極的な加盟店舗が存在する。このように、同ガイドラインに示された措置は、加盟店舗においてすら徹底されているとは言い難く、非加盟店舗においては、こうした措置がとられていない可能性が更に高いものと推察される。

(ア) 利用者の本人確認等の不徹底

日本複合カフェ協会が、平成 17 年 10 月から同年 11 月にかけて、加盟店舗にアンケート調査^(注4)を行ったところ、回答のあった 538 店舗のうち、会員制度（希望する利用者のみ会員登録を行うものを含む。）を導入していると回答したものは 71.6%であった。

このように、同アンケート調査に回答した店舗のうち 3 割弱が会員制度を導入しておらず、また、会員制度を導入している店舗の中には、会員登録を希望しない利用者についてはこれを行わないものや、会員登録時の本人確認が十分とは思われないものも混在している。さらに、同アンケート調査に回答しなかった加盟店舗や、非加盟店舗では、会員制度の導入率が更に低い可能性がある^(注5)。

こうしたことから、インターネットカフェにおいて、利用者の本人確認等が徹底されているとは到底言えない状況にある。インターネットカフェを利用してサイバー犯罪を行う場合、被疑者は、利用者の本人確認等を行わない店舗を利用する可能性が高いと考えられ、現に、上記(1)のとおり、インターネットカフェの利用者の匿名性が多くの事件において捜査の障壁となっている。また、上記(2)のとおり、インターネット上の自殺予告事案への対応においても、この匿名性が問題となっている。

(イ) 悪質な利用者による他の利用者の識別符号等の不正入手のおそれ等

インターネットカフェにおいては、違法行為等を企図する利用者が、キーロガー等のスパイウェアによって他の利用者の識別符号その他の秘密情報を不正に入手するおそれがある。そして、秘密情報の不正入手が行われた場合には、当該情報を利用して、不正アクセス行為、詐欺、脅迫等が行われる可能性がある。現に、利用者が、キーロガーにより他の利用者の識別符号を不正に入手し、

(注4) 1,130 店舗にアンケートを行い、538 店舗から回答があった（回答率 47.6%）。

(注5) 同協会は、「複合カフェ白書 2005」の中で、「このアンケート調査は JCCA 会員店舗に対して行われており、一般的な複合カフェよりも会員制の採用率が高くなっています。反対に、非会員の店舗や従来からの形態で営業を行っている店舗の中には会員制を採用していないところが多く見られます」と述べている。なお、引用文中、「JCCA」は同協会を、「複合カフェ」はインターネットカフェ及び漫画喫茶等を指す。

それを使用して不正アクセス行為等を行う事件の発生が見られる。

また、一般に、利用者が閲覧したウェブサイトやコンピュータに入力した情報の中には、当該利用者が他者に把握されることを望まないものが多々あると考えられ、それらがウェブサイトの閲覧履歴の確認、コンピュータに残存するファイルの閲覧、客席の後方からの覗き見等によって他の利用者に把握され得るとすれば、利用者にとって大きな不安となる。

このため、インターネットカフェのコンピュータに、スパイウェアを発見・駆除する機能や、コンピュータの使用後に残存している情報を消去する機能を付加することなどが必要であるが、こうした措置がとられていない店舗が依然として存在している。

【事例 1】

利用者が、インターネットカフェのコンピュータにキーロガーを仕掛け、他の利用者の識別符号（700件以上）を不正に入手し、インターネットカフェから当該識別符号を使用してインターネットバンキングシステムにアクセスし、他人の銀行口座から自己の管理する銀行口座に送金するなどした。平成15年3月、不正アクセス禁止法違反、電子計算機使用詐欺等で逮捕した（警視庁）。

【事例 2】

利用者が、インターネットカフェのコンピュータにキーロガーを仕掛け、当該コンピュータに入力された情報が数時間おきに自己のメールアドレスに転送されるようにして、他の利用者の識別符号を不正に入手し、当該識別符号を使用してインターネットバンキングシステムにアクセスし、他人の銀行口座から自己の管理する銀行口座に送金するなどした。平成16年10月、不正アクセス禁止法違反及び電子計算機使用詐欺で逮捕した（警視庁）。

(ウ) 悪質な従業員等による利用者の識別符号等の不正入手のおそれ等

違法行為等を企図する者がインターネットカフェの経営者や従業員となった場合においても、上記(イ)と同様の問題が生じる。この場合、当該店舗のコンピュータに、スパイウェアを発見・駆除する機能や、コンピュータの使用後に残存している情報を消去する機能が付加されていたとしても、経営者や従業員であれば当該機能を停止させる方法を知っている可能性があるため、秘密情報の不正入手やプライバシー侵害の危険性はより高いと言える。現に、インターネットカフェの従業員が、当該店舗のコンピュータにキーロガーを仕掛け、利用者の識別符号を不正に入手し、それを使用して不正アクセス行為等を行う事件の発生が見られる。

現在、こうした悪質な経営者や従業員を排除する仕組みはなく、また、日本複合カフェ協会では店舗ごとに管理者を置いて業務管理を徹底するよう推奨しているが、こうした措置がとられていない店舗も存在している。

【事例 1】

従業員が、自己の勤務するインターネットカフェのコンピュータのうち、使用後に残存している情報を消去する機能が付加されていないものにキーロガーを仕掛け、利用者の識別符号を不正に入手し、当該店舗から当該識別符号を使用してオンラインゲームにアクセスした。平成18年5月、不正アクセス禁止法違反で逮捕した（岡山）。

【事例 2】

従業員が、自己の勤務するインターネットカフェのコンピュータにキーロガーを仕掛け、利用者の識別符号を不正に入手し、当該店舗での勤務を辞めた後に、自宅等から当該識別符号を使用してインターネットオークションに参加し、出品物を落札した。平成18年5月、不正アクセス禁止法違反で逮捕した（詐欺は未遂。警視庁）。

(I) 子どもによる違法・有害情報の閲覧を防止する措置の不徹底

子どもがインターネットカフェを利用した場合、当該子どもが保護者の知らない間にインターネット上の違法・有害情報にさらされるおそれがある。

平成 18 年 12 月 1 日現在、21 都府県^(注6)では、いわゆる青少年保護育成条例により、インターネット接続が可能なコンピュータを公衆の利用に供する事業者に対し、フィルタリングソフトの活用等によりインターネット上の有害情報を青少年に閲覧させないように努力する義務を課している。また、日本複合カフェ協会も、運営ガイドラインの中で、18 歳未満の利用者に対してフィルタリング機能を付加したコンピュータを使用させるよう努力する義務を定めている。

しかし、東京都青少年・治安対策本部が平成 18 年 2 月から同年 3 月にかけて実施した調査によると、都内のインターネットカフェ 63 店舗のうち、フィルタリングサービスを提供していると回答したものは 12 店舗（19.0%）に過ぎなかった^(注7)。

このように、東京都内のインターネットカフェでは、子どもが使用するコンピュータへのフィルタリング機能の付加が徹底されておらず、他の道府県においても同様の状況である可能性がある。

(注6) 宮城県、福島県、東京都、神奈川県、岐阜県、愛知県、三重県、京都府、大阪府、兵庫県、和歌山県、岡山県、広島県、徳島県、香川県、愛媛県、福岡県、大分県、宮崎県、鹿児島県及び沖縄県。

(注7) 東京都青少年・治安対策本部「フィルタリングに関する実態調査」（平成 18 年 3 月）。インターネットカフェ及び漫画喫茶等 408 店舗に対して調査を実施し、67 店舗から回答があった。なお、フィルタリングサービスの提供に関する問いに回答したのは 63 店舗のインターネットカフェである。東京都のウェブサイト（<http://www.metro.tokyo.jp/INET/CHOUSA/2006/05/60g5o100.htm>）参照。

2. 匿名性その他の問題への対策の在り方

(1) インターネットカフェに係る対策の推進

ア サイバー犯罪の防止・検挙、人命保護等に向けた取組み

(ア) 利用者の匿名性の排除

インターネットカフェのコンピュータを使用したサイバー犯罪の防止を図るとともに、当該犯罪の発生時にはこれを確実に検挙し、また、当該コンピュータを使用した自殺予告事案等の発生時に迅速・的確に人命保護等のための措置をとるためには、インターネットカフェの利用者の匿名性を排除する取組みが不可欠である。

具体的には、第一に、インターネットカフェにおいて、利用者の本人確認を確実に行うとともに、当該利用者の特定に資する情報を一定期間保存する必要がある。上記 1.(3)ウ(ア)のとおり、インターネットカフェの中には、利用者の本人確認を行わずにコンピュータの使用を認めているものも依然として多く、会員制度の導入率の向上が急務である。また、会員制度を導入している場合であっても、例えば、顔写真や住所その他の連絡先が掲載・記載されておらず、かつ、作成者の如何を問わない身分証明書を掲示するのみで利用を認めるなど、本人確認が十分とは思われない店舗も存在する。金融機関、携帯電話会社等と同様の厳格な本人確認^(注8)まで行うべきか否かは別として、少なくとも、氏名、住所、生年月日等を官公庁、企業、学校等が発行した書面等で確認し、これらの情報を適切に管理しつつ一定期間保存するべきである。

第二に、インターネットカフェにおいて、各利用者の入店時刻及び退店時刻並びに当該利用者が使用したコンピュータに関する情報を一定期間保存する必要がある。これらの情報が保存されていなければ、仮に、サイバー犯罪、自殺予告等が行われた時刻及び当該行為に使用された店舗又はコンピュータが判明し、かつ、当該店舗で利用者の本人確認が行われていたとしても、どの利用者が当該行為を行ったのかを特定することが困難である。このため、各利用者が、いつからいつまで当該店舗を利用したのか、どの客席を使用したのか、途中で客席を変更した場合にはいつどの客席に移動したのかなどに関する情報を、適切に管理しつつ一定期間保存するべきである。

上記の利用者の匿名性を排除する取組みについては、まず、インターネットカ

(注8) 金融機関、携帯電話会社等においては、金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律(平成14年法律第32号)や携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律(平成17年法律第31号)に基づき、顧客、契約者等について、その氏名、住居及び生年月日の記載のある官公庁の発行した書面を提示させるなどして本人確認を行うとともに、本人確認記録を一定期間保存している。

フェの事業者が自主的に推進する必要がある。日本複合カフェ協会は会員制度の導入を推奨しているが、同協会への加盟率は平成 17 年 9 月現在で 41.3%に過ぎず、また、加盟店舗の中でも会員制度が徹底されているとは言い難い状況にある。サイバー犯罪が急激に増加し、その手口も高度化する中、現にインターネットカフェを悪用したサイバー犯罪が発生しており、サイバー空間に対する国民の不安感も急速に高まっていることなどを踏まえると、現時点において事業者の取組みは不十分と言わざるを得ず、格段の努力が求められる。今後、事業者による自主的な取組みが進展せず、かつ、インターネットカフェを利用したサイバー犯罪、自殺予告等を巡る状況に改善が見られないようであれば、より強力な対策についての検討が必要となるものと考えられる。

(1) ネット・オークション詐欺の防止

インターネットカフェを利用したネット・オークション詐欺については、上記 1.(1) のとおり、首都圏及び近畿地方の二つの都道府県警察で、平成 18 年 1 月から同年 3 月までの 3 か月間だけでも 8 件認知しており、しかもそのうち平成 19 年 2 月 1 日までに検挙に至ったものは 1 件に過ぎない。これは当該詐欺の捜査の困難さを物語っており、上記(ア) の取組みと併せて、そもそもインターネットカフェをネット・オークション詐欺に悪用させないための取組みが求められる。

具体的には、インターネットカフェの事業者とインターネット・オークション事業者が連携し、インターネットカフェのコンピュータからはインターネット・オークションに出品できないようにすることが考えられる。そのためには、インターネットカフェのコンピュータに固定の IP アドレスを割り当て、又は一定の範囲の IP アドレスのみがインターネットカフェのコンピュータに割り当てられるようにした上で、当該 IP アドレスをインターネット・オークション事業者に通知する必要があり、これにより経済的負担が増加するという問題があるものの、インターネットカフェの事業者とインターネット・オークション事業者において、こうした取組みを推進するべきである。

なお、ネット・オークション詐欺では、落札者（被害者）が、出品者（被疑者）から依頼を受け、先行して代金を出品者（被疑者）に送金するという形態が典型的であることから、落札物の送付と代金の送金の同時履行を実質的に担保すれば、ネット・オークション詐欺のほとんどは防止することが可能と考えられる。こうした観点から、インターネット・オークション事業者等の中には、エスクロー（注

(注⁹) 中立な第三者（エスクローサービス提供会社等）が落札者から代金を預かり、その後出品者が落札者に落札物を送付し、落札者が落札物を確認した後に、第三者が出品者に代金を送金する取引。なお、エスクローサービスについては、出資の受入れ、預り金及び金利等の取締りに関する法律（昭和 29 年法律第 195 号）、銀行法（昭和 56 年法律第 59 号）等との関係について、関係機関等において更なる議論が行われることが期待される。

9) サービスや商品代金引換を徹底又は推奨しているものがある。これらは、現在、インターネット・オークション事業者等が講じているネット・オークション詐欺の防止対策の中では極めて有効なものと考えられる。このため、インターネットカフェを利用した場合に限らず、インターネット・オークション全般について、エスクローサービスや商品代金引換の徹底又は更なる普及に向けた取組みをインターネット・オークション事業者等が推進することが期待される。

イ 利用者が安心して利用できる環境の構築に向けた取組み

(ア) 利用者の識別符号等及びプライバシーの保護

インターネットカフェにおいては、利用者の識別符号その他の秘密情報が他者に不正に入手されることを防ぐとともに、利用者が閲覧したウェブサイトやコンピュータに入力した情報に関するプライバシーを保護することにより、利用者が犯罪等に巻き込まれることなく安心して利用できる環境を構築することが重要である。

このため、インターネットカフェの事業者において、当該店舗のコンピュータに対し、キーロガーを始めとするスパイウェアを発見・駆除する機能や、コンピュータの使用後に残存している情報を消去する機能の付加を推進するべきである。また、客席の後方からの覗き見等を防ぐため、従業員の巡回や防犯カメラでの確認により挙動不審者の発見に努めるとともに、コンピュータの向きに配慮するなどの取組みも有用である。

なお、こうした取組みは、サイバー犯罪の発生状況や最新の手口等を踏まえながら、情報セキュリティに関する十分な知識を持った者の下で推進することが効果的である。このため、少なくとも事業者や店舗管理者については、定期的に警察から防犯指導を受けるなどして、こうした知識の維持・向上に努めるべきである。

(イ) 優良店舗の明示等

インターネットカフェの中には、日本複合カフェ協会の運営ガイドラインに従うなど、優良な店舗運営を行っているものがある一方、上記 1 . (3) ウ(ウ) のとおり、従業員が利用者の識別符号を不正に入手し、それを使用して不正アクセス行為等を行うようなものも存在する。利用者は、一般に、情報セキュリティ対策、従業員の管理等が的確に行われている店舗の利用を希望するものと考えられ、特に会員制度を導入している店舗の利用に際しては、自己の個人情報の厳格な管理を期待するのが通常である。このため、優良な店舗運営を行っている店舗が利用者に分かるようにすることが重要である。

現在、同協会では、上記 1 . (3) イのとおり、同ガイドラインに従った店舗運営を行っている加盟店舗に対して「優良店」と明記した証明書を交付し、当該店舗ではこれを入口に掲示するなどしている。今後、事業者において、当該

証明書の交付・掲示を引き続き推進するとともに、例えば当該証明書に有効期限を設けるなどして同ガイドラインの遵守状況の定期的な確認を行い、当該証明書の交付・更新は警察による防犯指導への対応状況等を踏まえてより厳格に行うこととするなどの取組みを推進するべきである。

なお、こうした事業者の自主的な取組みを通じて、優良な店舗運営を行う店舗が増加することが期待されるが、今後、仮にこうした取組みが十分に機能せず、かつ、インターネットカフェの事業者や従業員による犯罪が増加するようであれば、不適切な事業者の排除に向けた新たな対策についての検討が必要となるものと考えられる。

(ウ) 利用者に対する注意喚起

インターネットカフェのコンピュータを始めとする不特定の者が使用するコンピュータに識別符号等を入力する場合、スパイウェア等により当該識別符号等が他者に不正に入手される危険が伴う。しかし、警察庁が平成 18 年 3 月に行ったインターネット利用者を対象とする意識調査^(注10)では、スパイウェアについて「よく分からない」又は「そのような言葉は聞いたことがない」とする者が 57.6%と過半数を占めるなど、コンピュータに入力した情報が他者に不正に入手される危険に対する認知度は低い状況にある。

このため、警察においては、引き続き広報啓発活動を推進し、不特定の者が使用するコンピュータに識別符号等を入力しないよう注意喚起を行う必要がある。また、インターネットカフェの事業者においても、個々の利用者に対し、受付における従業員からの口頭説明等を通じて確実に同様の注意喚起を行うべきである。

ウ 子どもによる違法・有害情報の閲覧を防止するための取組み

インターネットカフェにおいては、子どもが保護者の知らない間にインターネット上の違法・有害情報にさらされるおそれがあるため、事業者においてこれを防止する措置を徹底する必要がある。

具体的には、各店舗において、子どもの来店状況を踏まえ、コンピュータにフィルタリング機能を付加するとともに、身分証明書等により利用者の年齢確認を確実にを行い、子どもについては当該機能を付加したコンピュータを使用させるべきである。また、フィルタリング機能を付加したコンピュータが不足した場合には、子どもに見通しのよい客席を使用させるとともに、従業員が適宜巡回するなどの取組みを推進することが望ましい。

(注10) 全国のインターネット利用者男女 1,000 名を対象に、調査を委託した民間事業者のウェブサイト上に警察庁において作成した質問票を掲示して回答を求める形式で実施した。

(2) プリペイド式データ通信カード等に係る対策の推進

上記 1 . (1) のとおり、平成 17 年中に警察が認知した不正アクセス行為 592 件のうち、匿名性が障害となって捜査に進展が見られないものは 212 件存在するが、この中には、購入時に本人確認が不要なプリペイド式データ通信カードを使用した事件や、セキュリティ対策がなされていない無線 LAN を悪用（ただ乗り）した事件等が含まれている。

プリペイド式データ通信カードについては、これを悪用したサイバー犯罪の防止等のため、事業者において、購入者の本人確認を確実に行うとともに、当該購入者の特定に資する情報を一定期間保存することが期待される。また、無線 LAN については、官民が連携し、利用者に対して、ただ乗りを防ぐための十分なセキュリティ対策を講じるよう広報啓発を推進する必要がある。

なお、インターネット・オークション事業者の中には、購入時に本人確認が不要なプリペイド式データ通信カードを使用する者による出品を認めていないものもある。こうした取組みは、ネット・オークション詐欺の防止に有効であるとともに、当該カードを製造・販売する事業者に購入者の本人確認を促す効果を持つことから、当該取組みがインターネット・オークション事業者の間で普及することが期待される。