サイバー犯罪捜査における事後追跡可能性の確保に向けた対策について

平成23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

本　　編

平成23年度総合セキュリティ対策会議

はじめに

近年めざ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・ウィ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・実施する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。当会議においては、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、ソフトウェア産業等の各種事業に関する知見を有する方々、さらに、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、様々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、平成20年５月のファイル共有ソフトを悪用した著作権侵害対策協議会の発足、平成21年６月の児童ポルノ流通防止協議会の発足、平成24年の不正アクセス禁止法の改正等の取組に結び付いている。

本年度は、「サイバー犯罪捜査における事後追跡可能性の確保」をテーマに選定し、事後追跡上の障害となっている事項について議論を行い、サイバー犯罪捜査における事後追跡可能性の確保に向けた対策についてまとめた。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、中立的な立場で、各テーマに関して関係者が講じるべき具体的な取組等について議論を行っていただいた。本報告書は、これらの議論の結果を取りまとめたものであり、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24年３月

総合セキュリティ対策会議委員長

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る。

特に、インターネット等の活用により生活の利便性が向上するなど、高度情報通信ネットワーク社会の光の部分が拡大する一方、サイバー犯罪が年々増加するなど、その陰の部分とも言うべき、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、①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、②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、情報通信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、産業界を始めとする多くの関係者・関係機関との連携が不可欠である。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、都道府県レベルでは「プロバイダ連絡協議会」等を通じた各種の取組がなされていたものの、国レベルではかかる広範な官民連携の場が設けられていなかったところ、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、当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の連携の在り方
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
平成18年度	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19年度	Winny等ファイル共有ソフトを用いた著作権侵害とその対応策
平成20年度	インターネット上での児童ポルノの流通に関する問題とその対策
平成21年度	インターネット・オークションにおける盗品の流通防止対策
平成22年度	安全・安心で責任あるサイバー市民社会を実現に向けた対策

平成23年度総合セキュリティ対策会議

目　次

～　本　　編　～

平成23年度総合セキュリティ対策会議

～　資　料　編　～

委員発表資料

平成 23 年度総合セキュリティ対策会議

サイバー犯罪捜査における事後追跡可能性の確保に向けた対策について

昨今、パーソナルコンピュータや携帯電話を中心としたインターネット端末が年齢を問わず幅広く普及し、インターネットが社会・経済活動の根幹を支える重要なインフラとして必要不可欠なものとなる一方で、インターネットバンキングへの不正アクセス等により国民の財産が侵害されるなど、国民生活を脅かすサイバー犯罪が多発しており、サイバー空間をめぐる情勢は深刻な状況にある。こうした状況を打開し、国民の生命、身体及び財産を守り、また、国民の誰もが安心してインターネットを利用することができるような社会を実現するためには、サイバー犯罪の発生を抑止することが必要である。

サイバー犯罪の発生を抑止するためには、発生した犯罪を確実に検挙し、犯罪企図者に「サイバー犯罪を行えば必ず捕まる」という意識を抱かせることが重要であるが、確実な取締りを実現するためには、現実空間と同様、捜査機関が捜査を進めるに当たって犯人の特定及び検挙が可能な捜査環境が整備されていなければならない。しかし、実際の捜査においては、犯人は捜査機関の追跡を免れるために、あらゆる手段を用いて捜査機関の捜査をかく乱させ、これにより捜査が円滑に行われないことがしばしばある。このような手段としては、広く国民に普及している通信機器やサービス、すなわち通信手段・環境の構造を巧妙に利用したものが多く、それらの構造自体が、まさに犯罪捜査における事後追跡上の障害となっている場合がある。新たな通信機器やサービスが短期間のうちに次々に開発され、瞬く間に普及する現代社会において、それぞれの通信手段・環境において事後追跡上の障害について検討することは、現在だけでなく、将来にわたって、サイバー犯罪の十分な取締り機能を確保する上で、必要不可欠であるといえる。

そこで、平成 23 年度総合セキュリティ対策会議では、「サイバー犯罪捜査における事後追跡可能性の確保」をテーマとして選定し、議論を行った。サイバー犯罪捜査における事後追跡上障害となっている通信手段・環境の中で犯人側の匿名化手段として用いられているものを具体的に選定し、これらの事後追跡上の障害の現状と問題点、改善に向けた今後の在り方について議論を重ねる中で、急激に増加しているサイバー犯罪の発生を抑止するのに十分な取締活動の水準を確保するためには、それぞれの匿名化手段について事後追跡可能性が開かれるとともに、新しい通信手段・環境に対して、サイバー犯罪の事後追跡可能性の確保についての検討がなされていることが重要であるとの認識に至った。

本報告書では、これらの議論の結果を踏まえ、まず始めに、事後追跡可能性の確保がサイバー犯罪の発生抑止とどのような関係を持つかについて言及した後、データ通信カード・無線ＬＡＮ、インターネットカフェ及びインターネット上の高度匿名化技術における事後追跡上の障害の現状や問題点を明らかにした上で、それぞれの障害に係る改善に向けた今後の在り方について、さらに、本年度の検討テーマの結論として、サイバー犯罪の事後追跡可能性の確保について取りまとめた。

第１章　サイバー犯罪の現状と事後追跡可能性について

１　サイバー犯罪[1]の現状

現実空間における治安情勢の指標の一つとなっている刑法犯の検挙件数は減少傾向にある一方で、サイバー空間における治安情勢の指標の一つとなっているサイバー犯罪の検挙件数は高水準で推移しており、極めて深刻な状況にある。

刑法犯検挙件数の 10 年間の推移をみると、平成 16 年の約 67 万件をピークにそれ以降は年々減少傾向にあり、平成 23 年は約 46 万件と平成 16 年に比べて約 31%減少している状況にある（図１－１）。その一方で、サイバー犯罪検挙件数の 10 年間の推移をみると、平成 14 年は 1,606 件で年々増加傾向にあり、平成 23 年には 5,741 件と前年に比べて約 17%減少したものの、平成 14 年に比べて約 3.6 倍となっている（図１－２）。中でも、詐欺、児童買春・児童ポルノ法違反（児童ポルノ）、青少年保護育成条例違反を始めとするネットワーク利用犯罪[2]が大幅に増加しており（平成 14 年に 1,471 件であったものが平成 23 年には 5,388 件と約 3.7 倍）、サイバー空間を悪用した身近な犯罪が急増している状況がうかがえる。

また、インターネット接続のブロードバンド化や情報利用端末としての携帯電話の利用拡大等を背景に、インターネットを利用した取引が日常的になるなど、インターネットは社会・経済活動の根幹を支える重要なインフラとして必要不可欠なものとなる中で、こうした状況に乗じたサイバー犯罪が発生している。平成 23 年中に発生した地方銀行のインターネットバンキングに対する不正アクセス事案では、インターネットバンキングの利用者のＩＤ・パスワード等を盗み、不正アクセスを行い、不正送金するといった手口により、平成 23 年 12 月末現在、35 都道府県における 56 の金融機関の 165 口座が被害に遭い、不正送金総額は約３億円に上っていることを把握しており、多くの国民が日常的に利用しているインターネットバンキングがサイバー犯罪の標的となっている。

今後、国民生活においてインターネットを利用した様々なサービスが開始・普及し、ますますその重要性が増していくものと考えられるが、このような中で、サイバー犯罪から国民の生命、身体及び財産を守るためにサイバー空間における安全・安心を確保することは急務であるといえる。そのためには、急激な増加傾向にあるサイバー犯罪に対して、犯人を検挙するための取締りとサイバー犯罪の発生自体を抑えるための防止対策の両面からサイバー犯罪の発生抑止を図っていくことが重要である。

---

[1] 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をいう。

[2] その実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪をいう。

図１－１　刑法犯の検挙件数の推移

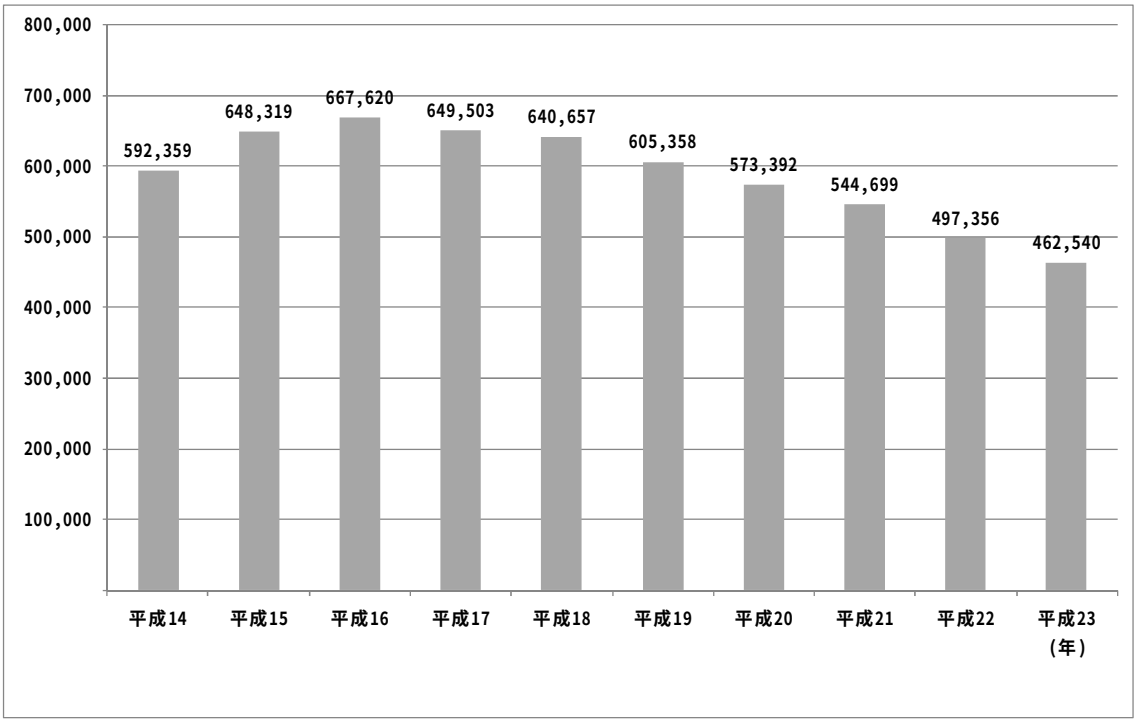
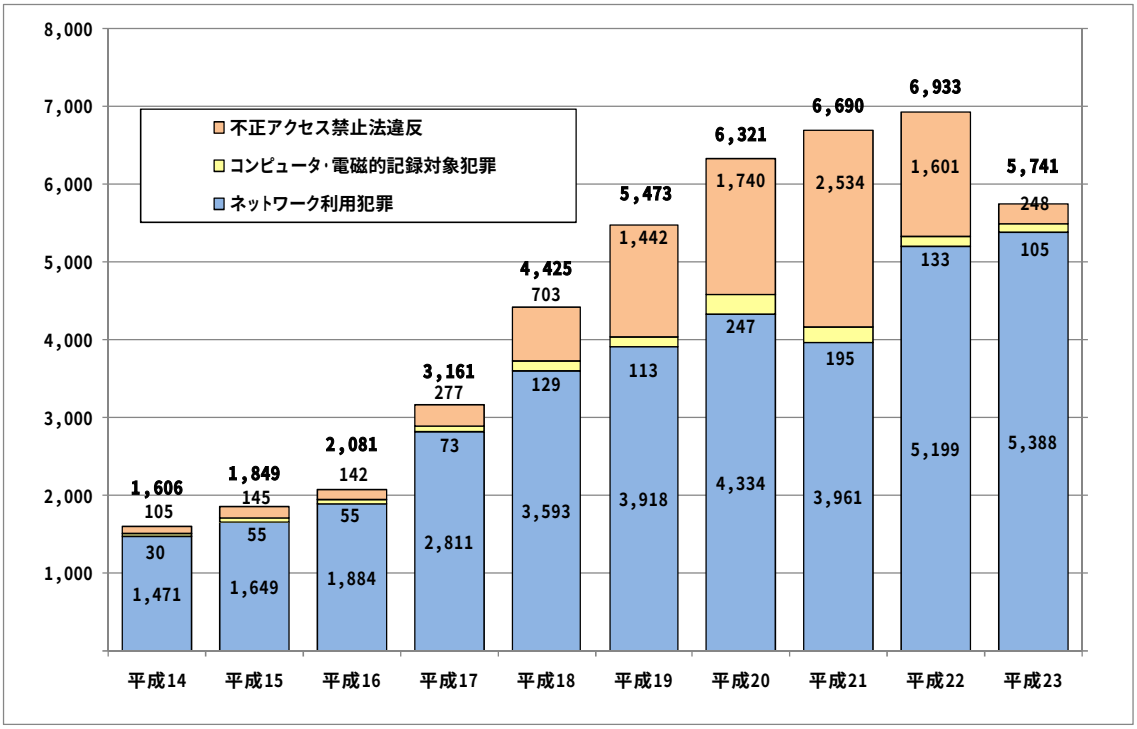


図１－２　サイバー犯罪の検挙件数の推移



2　サイバー犯罪の発生抑止

現実空間において、犯罪の取締りと発生抑止とは表裏一体の関係にあるが、これはサイバー空間においても同様である。つまり、警察によるサイバー犯罪の取締りが十分に行われ、「サイバー犯罪を行えば必ず捕まる」という意識を犯罪企図者に抱かせることができれば、サイバー犯罪の企図者数は減少し、結果として、サイバー犯罪の発生抑止につながるのである。逆に、発生した犯罪を確実に取り締まることができなければ、犯罪企図者に「自分が犯人だとは分からないだろう」という意識を生じさせ、犯罪を起こすことに対する心理的な抵抗感が減少し、発生件数は増加すると考えられる。このように、サイバー犯罪の発生抑止には、十分な取締りが行われることが不可欠な要素であり、現実空間と異なり、匿名性が高く痕跡が残りにくいという特徴を有するサイバー空間においても、現実空間と同様の取締活動の水準を確保することが重要であるといえる。

発生したサイバー犯罪を的確に取り締まるため、これまでに警察では、インターネット・ホットラインセンター[3]に通報される違法・有害情報における全国協働捜査方式[4]の導入、サイバー犯罪捜査に従事する捜査員の増員等、捜査体制の強化を推進してきたところである。しかしながら、今後ますます手口の多様化・巧妙化が懸念されるサイバー犯罪に対しては、捜査体制の強化により的確な取締りを推進し、発生抑止を図っていくことに加えて、インターネットにおける事後追跡可能性を確保するなど捜査環境を改善していく必要がある。

3　サイバー犯罪の抑止と犯人側の匿名化の問題

(1)　サイバー犯罪の取締りと事後追跡上の障害

サイバー犯罪の取締りが十分に行われるためには、現実空間における犯罪の場合と同様、発生後に捜査機関が捜査を進め、犯人の特定及び検挙が可能な捜査環境が整備されていなければならない。つまり、現実空間において、犯行現場から足跡、指紋等を分析し、犯人に到達できるように、サイバー空間で行われた犯罪についても、犯人が利用したインターネット端末や経由したサーバの記録などから得られる各種情報を分析するなどして追跡し、犯人まで到達できること、すなわち事後追跡が可能であることが必要である。事後追跡に障害がある場合、事件捜査を行い、犯人に到達するまでに、膨大な捜査体制、費用等を要するほか、捜査期間が長期にわたるなど、円滑に捜査活動を行うことができないばかりでなく、最終的に犯人を特定することができず、未検挙に終わるという事態を生じさせることとなる。

前述したように、サイバー犯罪の発生抑止のためには、取締りが十分に機能し

---

[3]　平成18年６月より、財団法人インターネット協会が警察庁の委託を受け運用を開始しており、一般のインターネット利用者からの違法情報・有害情報に関する通報を受理し、違法情報の警察への通報や国内のウェブサーバに蔵置された違法・有害情報に係るサイト管理者等への削除依頼を行っている。

[4]　インターネット・ホットラインセンターに通報された違法情報について、発信元を割り出すための初期捜査を警視庁が一元的に行い、これによって発信元が判明した違法情報について、警察庁の調整により、発信元を管轄する都道府県警察がその後の捜査を行う捜査方式で、平成23年７月より本格的に運用を開始している。さらに、平成23年９月には、同センターから通報される有害情報についても、本捜査方式に準じた捜査上の対応の試行を実施している。

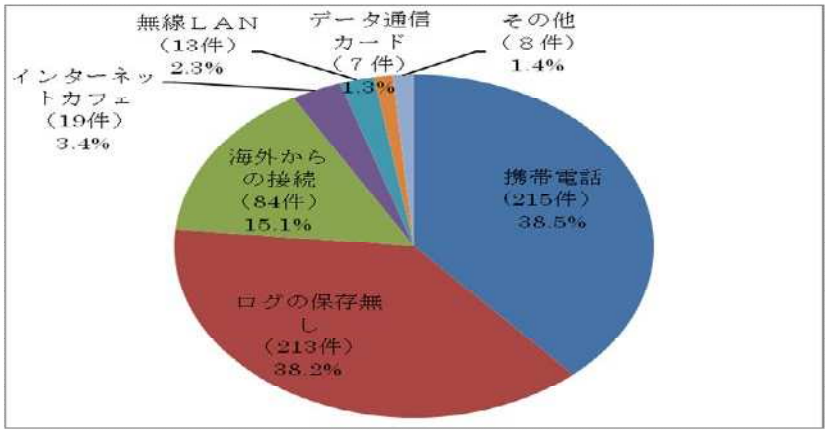
ていることが必要であるが、犯罪の取締りが十分に機能するとは、個々のサイバー犯罪事件の捜査活動が円滑に進展することで、捜査機関による取締りを犯罪企図者に強く意識させ、その犯行を思いとどまらせるという取締りの実効性が社会的に波及するということであり、そのためには、事後追跡上の障害について改善していくことが重要である。

(2) 事後追跡上の障害に関する実態調査結果

現在、インターネットカフェ、データ通信カード・無線ＬＡＮ等、誰もが簡単にインターネットを利用することができる施設・サービスが普及している一方で、それらの中には、利用や機器購入の際の本人確認が十分でないものが見られるところであり、こうした利用者の匿名性の高い施設・サービスを、犯人が捜査機関の追跡を免れるための手段、すなわち匿名化手段として悪用する事例が散見されている。

平成23年６月、警察庁において、サイバー犯罪捜査における事後追跡上の障害に関する実態調査（以下「実態調査」という。）を実施したところ、平成22年中に認知し平成23年５月末までに未検挙であるサイバー犯罪捜査に係る事後追跡上の障害については、ネットワーク上の障害により捜査が困難となっていることが判明した559件のうち、携帯電話215件（38.5%）、ログの保存無し[5]213件（38.1%）、海外からの接続[6]84件（15.0%）、インターネットカフェ[7]19件（3.4%）、無線ＬＡＮ[8]13件（2.3%）、データ通信カード[9]７件（1.3%）となっており、様々な匿名化手段が捜査上の障害となっているために、捜査活動が円滑に進展していない状況が明らかとなった（図１－３）。

図１－３　サイバー犯罪捜査に係る事後追跡上の障害



[5] ログの保存無しとは、被害サーバ、プロバイダ、プロキシサーバ等においてログの保存がなされていなかった場合を示す。

[6] 海外からの接続とは、犯人が被害者に攻撃を行う過程の中で、海外からのインターネット接続が行われていた場合を示す。

[7] インターネットカフェとは、個室等においてインターネットに接続されたコンピュータを利用させることを営業の全部又は一部としている施設（個室ビデオ店は除く。）に設置された端末が利用された場合を示す。

[8] 無線ＬＡＮとは、インターネットに接続される電気通信回線の一部が無線設備（携帯電話及びＰＨＳ端末を除く。）によって構成される電気通信サービスが利用された場合を示す。

[9] データ通信カードとは、コンピュータ等に差し込み、携帯電話やＰＨＳの通信網を利用することにより、インターネットのサービスを利用する通信用カードが利用された場合を示す。

(3) サイバー犯罪の発生抑止と犯人側の匿名化手段

サイバー犯罪の発生を抑止するために十分な取締活動の水準を確保するためには、図１－３に掲げられた、捜査機関側の事後追跡を免れるために犯人側に用いられる様々な匿名化手段について、それぞれに対策を講じることで、サイバー犯罪における匿名性をできる限り排除し、匿名化工作の手段としては悪用できないものにすること、すなわち犯人側の匿名化手段を無効化することにより、捜査活動の円滑性を回復していくことが必要である。

4 サイバー犯罪の事後追跡可能性について

(1) 匿名化手段の性質

犯人側の匿名化手段とは、利用契約時に本人確認が的確に実施されていないことなどにより、誰が、いつ、どこで、どのようにその通信手段・環境を利用したかといった利用者に関する情報が残されず、利用者の匿名性を高めている携帯電話やデータ通信カード等の通信手段やインターネットカフェ等の通信環境のことである。通常、捜査機関は、通信手段・環境に残された利用者に関する情報を収集・分析し、犯人を特定することになるが、サイバー犯罪においては、通信手段・環境に残された利用者に関する情報は、ログ等の電磁的記録や利用契約時の書面等の記録等に限られるものであり、これらの記録が現実空間に存在する犯人を結び付けるための唯一の手掛かりであるといえる。

それぞれの匿名化手段に対して、利用者に関する情報が残るよう措置がなされ、犯行の痕跡を捕捉することが可能になれば、犯人は捜査機関に追跡・検挙されることを恐れて、それらの通信手段・環境を匿名化手段として悪用することを萎縮するようになり、その結果、匿名化手段は無効化されるものと考えられる。つまり、犯人側の匿名化手段は、その事後追跡可能性が開かれることによって無効化が可能となる性質のものと考えられる。

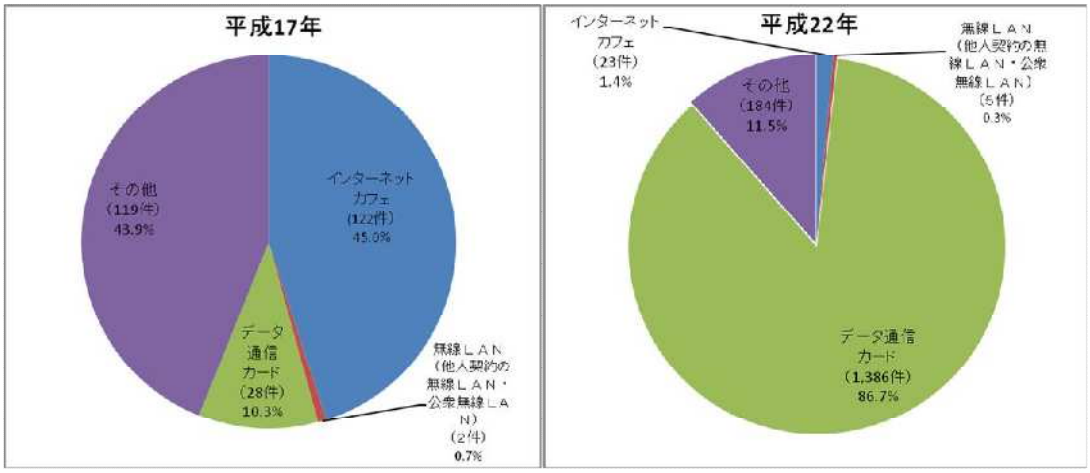
(2) 匿名化手段の変遷

犯人側の匿名化手段は、各種対策の進展や新たな通信機器の普及等により変遷し、過去５年間で大幅に変化している。不正アクセス禁止法違反検挙件数における匿名化手段を比較すると、平成17年ではインターネットカフェの件数が122件（45.0%）で最も多かったが、平成 22 年ではインターネットカフェの件数が23件（1.4%）と大幅に低下している。この要因としては、平成18年度総合セキュリティ対策会議報告書に基づくインターネットカフェ等における匿名性等の問題への各種対策や、平成22年７月１日より東京都において施行されているインターネット端末利用営業の規制に関する条例（以下「インターネットカフェ条例」という。）が有効に機能し、インターネットカフェを匿名化手段として用いることが、以前に比べて困難になりつつあることが考えられる。

一方、データ通信カードについては、平成17年の28件（10.3%）から、平成22年は1,386件（86.7%）に、また無線ＬＡＮについては、２件（0.7%）から

５件（0.3%）に増加している。この要因としては、データ通信カードや無線ＬＡＮのような新たな通信機器・サービスが、国民にとって一般に利用可能なものとして広く普及している中、それらの利用契約時等において、事業者ごとに店頭における契約者の本人確認が十分に実施されていない場合があること、また、利用者の理解が不十分であったり、危機意識の希薄さからセキュリティ設定がされずに利用されていることなどから、犯人にとって、こうした通信機器・サービスが匿名化手段として用いやすい状況にあるということが考えられる（図１－４）。

図１－４　不正アクセス禁止法違反検挙件数における匿名化手段の比較（平成17年、22年）



(3)　まとめ

ア　検討を実施した匿名化手段について

サイバー犯罪捜査において事後追跡可能性の障害となっている匿名化手段については、図１－３に示されるとおり多岐にわたる。このうち、携帯電話については、平成17年に成立した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）において、携帯音声通信事業者に、契約者に対する契約締結時の本人確認義務等を課しており、名義を偽った携帯電話という匿名化手段を入手することに対する一定の法律上の措置がなされているところである。また、ログの保存無しについては、平成23年６月に成立した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によって、刑事訴訟法に、捜査機関がプロバイダ等において業務上記録している通信履歴に対して、消去しないよう要請できる旨の規定が新設されたことから、こちらについても、一定の法律上の措置がなされたところである。法律上の措置がなされた匿名化手段については、時間の経過とともに、犯人が匿名化手段として用いることを萎縮するようになるなど、状況が改善される可能性がある。

さらに、海外からの接続については、攻撃の発信元が海外にある以上、対策を検討するに当たっては海外の捜査機関等との緊密な連携が必要不可欠である。警察では、海外から我が国に向けたサイバー犯罪が発生した際には、国際刑事警察

機構（ICPO-Interpol）[10]、刑事共助条約（協定）[11]、サイバー犯罪に関する24時間コンタクトポイント[12]等の海外の捜査機関等との国際捜査協力体制の枠組みを活用しているほか、各種国際会議、海外の捜査機関との協議を通じ、情報交換や協力関係の確立に取り組んでおり、海外からの接続という匿名化手段については、今後も引き続きこれまでの警察の既存の取組を推進していくことで、改善される可能性がある。

以上のことから、サイバー犯罪捜査において、事後追跡上の障害となっている匿名化手段のうち、携帯電話、ログの保存無し及び海外からの接続については、既になされた措置による今後の状況の変化等の経過を注視していくこととし、本年度の総合セキュリティ対策会議においては、これら以外のデータ通信カード・無線ＬＡＮ、インターネットカフェ及びインターネット上の高度匿名化技術を取り上げて、事後追跡上の障害の改善に向けた今後の在り方を検討し、取りまとめた。

イ　検討するに当たっての基本的考え方

犯人側の匿名化手段については、前述のとおり、各種対策の進展や新たな通信機器・サービスの出現等の影響を受けて、時間の経過とともに大きく変遷するものである。したがって、事後追跡上の障害の改善に向けた今後の在り方については、こうした変遷にも対応できるよう、匿名化手段を、現在、事後追跡上の大きな障害となっているもの、過去において事後追跡上の大きな障害となっていたものの対策を講じたことにより改善されつつあるもの、将来的に事後追跡上の大きな障害となる可能性を有するものの３つの視点で分類し、それぞれ異なる観点から検討した。

以上のことから、現在悪用事例が多発し、大きな障害となっているデータ通信カード・無線ＬＡＮについては、障害となっている状況を速やかに改善するための対策の実施という観点から検討した。また、既に対策が実施され、改善されつつあるインターネットカフェについては、軌道に乗った対策の制度化という観点から検討した。さらに、プライバシー保護のために開発されたインターネット上の高度匿名化技術については、将来的な悪用に備えた対応方策の調査研究という観点から検討した。

10　International Criminal Police Organization-Interpol

11　捜査共助の実施を条約上の義務とすることで捜査共助の一層確実な実施を期するとともに、捜査共助の実施のための連絡を外交当局間ではなく、条約が指定する中央当局間で直接行うことにより、手続の効率化・迅速化を図るものである。

12　平成９年12月のＧ８司法内務閣僚会合で策定された「ハイテク犯罪と闘うための原則と行動計画」に基づき設置されたもので、現在58の国・地域に設置されている。

第２章　匿名化手段における事後追跡上の障害の改善に向けた今後の在り方について

第１　データ通信カード・無線ＬＡＮ

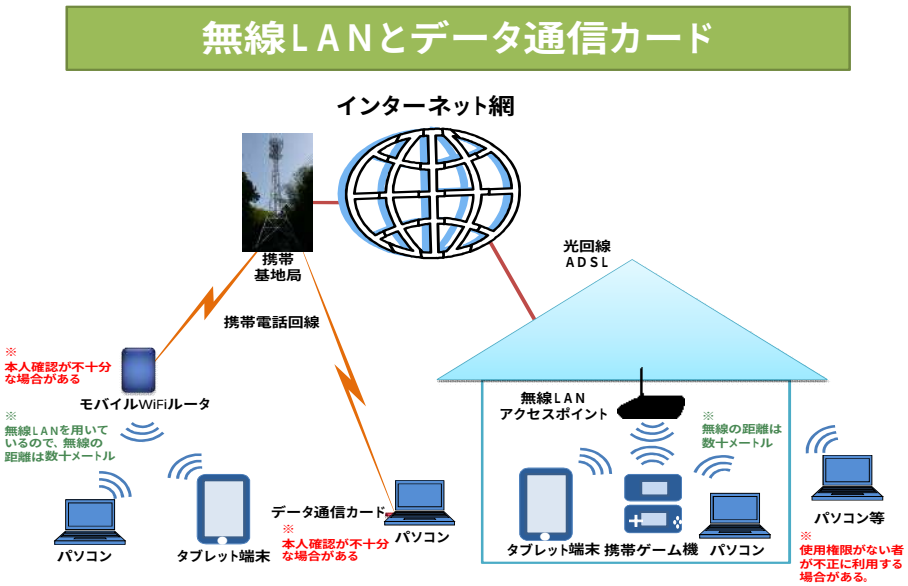
１　事後追跡上の障害の現状

(1)　データ通信カード・無線ＬＡＮについて

データ通信カードとは、ＰＨＳや携帯電話等の無線回線を利用して、外出先でパソコン等をインターネットに接続する機器である。最近では、高速通信可能な第３世代携帯電話方式を採用したものが主流となっており、無線ながら高速でインターネットを利用することができる。運用当初は、ＵＳＢ等の端子に差し込んで使用するものであったが、パソコンやタブレット端末等とデータ通信カードの間を無線ＬＡＮで接続し、同時に複数の機器からインターネットを利用できる「モバイルWi-Fiルータ」と呼ばれるものも出現している。

また、無線ＬＡＮとは、有線ケーブルの代わりに無線通信を利用して無線ＬＡＮアクセスポイント（親機）と無線ＬＡＮ機能を持つパソコン（子機）との間で、データの送受信を行うネットワーク環境のことである。親機と子機の双方に設定することで通信が可能となり、電波の届く範囲なら障害物を越えてどこでも通信が可能という便利さを備えている。配線工事等の手間がないため、最近では、企業や学校のみならず、一般家庭においても広く利用されている。公衆エリアにおける無線ＬＡＮの利用形態としては、電気通信事業者が契約者に対して駅や空港等に利用者向けにアクセスポイントを設置してインターネット接続環境を提供する公衆無線ＬＡＮサービスや、ファーストフード店等が商業利用のために店舗内にアクセスポイントを設置して無料で使用できるようにした店舗開放型無線ＬＡＮサービスなどがある(図２－１－１)。

図２－１－１　無線ＬＡＮとデータ通信カード



(2) 事後追跡上の障害の現状

データ通信カード・無線ＬＡＮの出現により、インターネット利用者にとって利便性は大きく向上した一方で、サイバー犯罪を敢行する際の匿名化手段としても悪用され、捜査における事後追跡上の障害として問題となっている。実態調査の結果によれば、データ通信カードを利用したサイバー犯罪の検挙件数は、1,383 件となっている（表２－１－１）。この 1,383 件を分析すると、グループを摘発したことによる大量検挙を含むものであるが、その全てが利用契約時における本人確認が緩やかな事業者が販売するデータ通信カードが、他人名義で購入され、これらが悪用されたものであることが判明した。

また、無線ＬＡＮを悪用したサイバー犯罪の検挙件数については、平成 21 年には 97 件であったものが、平成 22 年には 26 件と一時的に減少したものの、平成 23 年は 42 件と前年の総件数を上回っている（表２－１－２）ほか、平成 22 年中に認知し 23 年５月末までに未検挙であるサイバー犯罪捜査に係る事後追跡上の障害については、無線ＬＡＮが 13 件(うち、ただ乗り２件、公衆無線ＬＡＮ11 件[13])となっており（前掲図１－３）、無線ＬＡＮが、サイバー犯罪敢行の際の匿名化手段として悪用され、事後追跡上の障害となっている状況がうかがえる。

表２－１－１　データ通信カードを利用したサイバー犯罪について（件数）

検挙	1,383
未検挙	7
計	1,390

検挙　・・・平成 22 年中及び 23 年上半期に検挙したサイバー犯罪のうちデータ通信カードが使用されたもの

未検挙・・・平成 22 年中に認知し平成 23 年５月末までに未検挙のサイバー犯罪のうちデータ通信カードが使用されたもの

表２－１－２　無線ＬＡＮを悪用したサイバー犯罪の検挙件数

	H19	H20	H21	H22	H23
不正アクセス禁止法違反	6（0）	87（0）	57（７）	5（4）	3 (1)
ネットワーク利用犯罪			40（13）	21（0）	39（6）
合計	6	87	97（20）	26（4）	42（7）

（）は公衆無線ＬＡＮを使用した件数

[13] 誰もが簡単にアクセスできるよう暗号化等のセキュリティ設定のなされていない公衆無線ＬＡＮについても、サイバー犯罪に悪用されている実態があることから、今後、匿名化手段としての悪用状況について注視し、状況に応じて対策等を検討することが必要になるものと思われる。

(3) 悪用事例

データ通信カードを悪用した事例としては、他人名義で契約したデータ通信カードを使用してフィッシングメールの送信を行い、入手した他人のクレジットカード情報を使用してインターネットショッピングにおいて商品を詐取したものがある。

本事例において、他人名義でデータ通信カードを契約した方法については、利用料金の支払をクレジットカード払いにした場合に公的書類による本人確認の必要がないデータ通信カード事業者をわざわざ選び、オンラインサイトにフィッシングにより入手した他人のクレジットカード情報を入力して他人名義で利用契約を結ぶというものであった。さらに、購入したデータ通信カードの受取先については、クレジットカード名義人の住所ではなく、アパートの空き部屋や私設私書箱等を指定することで、契約の際に使用したクレジットカードの名義人やデータ通信カード事業者に気付かれることなく、入手に成功していた。

このように匿名で入手した他人名義のデータ通信カードを使用し、犯行場所を察知されないよう、配線工事等が不要な無線回線の利点を悪用し、アジトを転々と変えて犯行に及んでいたものである。

事例　フィッシングにより他人のＩＤ・パスワードやクレジットカード番号等を不正に入手し、インターネットショッピングにおいて商品をだまし取った不正アクセス禁止法違反及び詐欺事件

無職の男（32）らは、無線ＬＡＮの不正使用やデータ通信端末などを駆使し、フィッシングにより他人のＩＤ・パスワードやクレジットカード番号等を入手し、会員専用サイトに不正アクセスを行い、個人情報を入手した上、それを用いて他人になりすましてインターネットショッピングにおいて商品をだまし取った。

データ通信端末の発信場所の位置情報を多数入手して分析したところ、付近にビジネスホテルが点在していることから、ホテルの協力を得て捜査した結果、ホテル内での犯行と判明した。

無線ＬＡＮを悪用した事例としては、悪意ある者が、ウォードライビング（War Driving）と呼ばれる行為によって、セキュリティ設定が簡易で無防備なアクセスポイントを探し回り犯行に及ぶものがある。これは、自動車で市街地を移動して、暗号化等によるセキュリティの設定がなされていない一般家庭等の無線ＬＡＮルータから発せられる電波を傍受できるアクセスポイントを探し、当該ポイントを発見した場合には、付近に駐車した車内からモバイル端末等によって、インターネットにアクセスする行為である。犯人は、周囲から不審に思われ犯行を察知されないよう短時間に次から次へと場所を移動し、別のアクセスポイントに接続して犯行を繰り返している。

通常、捜査機関は、サイバー犯罪の発生を認知した後に、ログからアクセスポイントを割り出し、そのアクセスポイントの利用者に係る内偵捜査によって犯人を特定するが、利用者が複数存在するアクセスポイントについては、利用実態を解明するために数ヶ月に及ぶ張り込み等により、ようやく犯人に到達しているのが現状である。

事例　他人の無線ＬＡＮを使用してインターネットにアクセスし、電子掲示板に銀行口座や偽造身分証を販売するとの情報を掲載し、購入を希望した者から現金をだまし取った詐欺事件

被疑者（無職・男・５２歳）は、ホームセンター事業者が運営する無線ＬＡＮを使用してインターネットにアクセスし、電子掲示板に銀行口座や偽造身分証を販売するとの情報を掲載し、購入を希望した者から現金をだまし取った。

犯人を特定するため不正利用された無線ＬＡＮを調査・分析し、使用回数が比較的多い場所を捜査したところ、ホームセンターに隣接する駐車場で無線ＬＡＮを使用しパソコンを操作している者を確認し、犯行を特定した。

(4)　まとめ

データ通信カード・無線ＬＡＮが犯人側の匿名化手段として悪用されていることからも分かるように、犯人は、安価で市場に多く出回り、使用方法も比較的容易であるなど利便性が高く、本人確認が簡略で入手が容易であることや犯行場所の特定を困難にさせる機器等の検挙されにくいものを有効な匿名化手段として選定し、サイバー犯罪に集中的に悪用していることがうかがえる。

2　現状の問題点

(1)　データ通信カード

ア　事業者における本人確認の実施状況等の現状

データ通信カードの取得に当たって本人確認が不十分であることにより匿名化手段として悪用されている問題を踏まえ、警察庁では、平成 23 年５月下旬から７月上旬にかけてデータ通信カードの事業者７社に対してヒアリングを実施した。主なヒアリング内容及び結果は以下の４点である（表２－１－３）。

１点目は料金の支払方法として口座引き落としを選択した利用者に対する本人確認方法についてである。７社のうち６社は運転免許証、健康保険証等の公的書類により本人確認を実施している。残り１社については、利用者が一定期間インターネット通信を利用する権利を前払で購入するプリペイド式データ通信カードを販売しており、利用料金の支払が購入契約の時点で行われ、利用料金の滞納者に対する料金請求という事態が想定されないため、公的書類による本人確認の必要がなく、実施されていない。ただし、この事業者では、データ通信カードの初回使用時に携帯電話番号を登録する必要があり、これをもって利用者確認を行っている。

２点目は料金の支払方法としてクレジットカード払いを選択した利用者に対する本人確認方法についてである。７社のうち３社は公的書類により本人確認を実施している。残りの３社はクレジットカード払いの場合には、クレジットカードという支払に関する一定の証明を既に提示していることを理由に、公的書類による本人確認を実施していない。

３点目は、契約名義人の住居以外での受取についてであるが、７社のうち６社

が住居以外での受取が可能となっている。他人名義で契約したデータ通信カードを契約名義人の住居以外で受取を可能にすると、アパートの空き部屋や私設私書箱等の契約名義人が実際には居住していない場所において入手されるという問題がある。

４点目は事業者間で本人確認要領が異なることに関する意見であるが、本人確認方法について共通の基準を設けるべきであるという意見が多数であった。また、共通の基準の作成に当たっては、所管省庁の下で、事業者間での検討を進めていくべきではないかという意見があった。

表２－１－３　データ通信カード事業者における本人確認の実施状況等（平成23年７月末現在）

聴取項目＼事業者	A	B	C	D	E	F	G
料金口座引き落としの際の本人確認方法	公的書類	公的書類	公的書類	プリペイド販売のため本人確認なし（使用に際しては携帯電話番号を登録する必要がある）	公的書類	公的書類	公的書類
料金クレジットカード払いの際の本人確認方法	公的書類	公的書類	公的書類		なし	なし	なし
住居以外での受取	不可	可	可	可	可	可	可
事業者間で本人確認要領が違うことに関する意見	電気通信事業者協会で話し合うことと思う。協会に加入していない事業者とも話をする場が有れば話し合いたい。	本人確認の基準を検討するならば、事業者間で基準を合わせたい。どの様な検討の場がふさわしいかは、総務省や警察庁の意見や情報を踏まえたい。	共通の確認方法が望ましい。 店頭での間違いがないよう携帯と共通の確認方法としている。	共通の基準を設けることには賛成。通信事業に関することであるので、総務省にリーダーシップを取っていただきたい。	電気通信事業者協会団体で共通の方法で本人確認をする必要があると思う。 事業者間での検討に参加したい。	全事業者が共通の基準で本人確認をすることは理解できるが、オンラインで即時加入できるサービスへの対応が課題となる。	電気通信事業者協会の中にも検討する場があることから、その中で話し合うことも可能であると思う。

イ　問題点

データ通信カードにおいては、前述のとおり、クレジットカード情報をもって利用契約を可能とする事業者が一部見られるところであるが、フィッシング等により入手した他人のクレジットカード情報を使用して利用契約を行うことにより、他人名義で購入することが可能になり、これが犯人側の匿名化手段として用いられると、データ通信カードの契約名義人を特定しようとしても、利用契約時に無断使用されたクレジットカードの名義人しか判明せず、犯人を割り出すことはできないこととなる。

また、データ通信カードの送付先をアパートの空き部屋や私設私書箱等の契約名義人の住居以外に指定できる場合には、受取者の特定が非常に困難であるため、こちらも犯人を追跡する上で大きな障害となる。

このように利用契約時等に本人確認が十分でなく、契約名義人の住居地の確認が取れない場合があるデータ通信カードでは、他人へのなりすましによる悪用の余地があり、これを利用した犯罪を捜査する場合において、契約者名義人と異なる真の利用者の特定が困難になるという問題がある。

(2) 無線ＬＡＮ

ア セキュリティ等の現状

無線ＬＡＮの利便性は、家庭内のどこにいてもインターネットに無線接続ができることにある一方で、電波が届く場合には、家庭内に限らず屋外からでも接続が可能であるため、外部から悪意ある者が不正に接続することにより、データを収集されてしまうことが問題となっている。不正利用による無線ＬＡＮの悪用を防止するためには、より高度な暗号方式が設定された状態であることが重要である。

無線ＬＡＮの暗号方式については、無線ＬＡＮが一般家庭に普及し始めた平成 12 年頃の初期段階では、ＷＥＰ[14]と呼ばれる暗号方式が導入されたが、この暗号方式は暗号化に使用する鍵データの生成方法が単純であるため解析が容易であることや、パスワードを変更しない限り暗号化に使用する鍵は同じものが使用され続けることなどの脆弱性が指摘された。その後、事業者等の取組により、現在に至るまでにＷＰＡ[15]、ＷＰＡ２[16]等のより高度な暗号方式が開発・採用されており、セキュリティに関する技術は高度なものとなっている。

無線ＬＡＮのセキュリティレベルについては、全く設定されていない形態、ＷＥＰ方式による比較的簡易な暗号方式を設定した形態及びＷＰＡ方式による高度な暗号方式を設定した形態の大きく３段階に分類することができるが、不正利用による無線ＬＡＮの悪用を防止するためには、ＷＰＡ方式による高度な暗号方式を設定した形態が一般的なものとして普及することが重要である。

高度な暗号方式を設定した形態を普及させなければならない一方で、これを設定するためには、これまでは利用者にとって手動による複雑な作業を必要とすることなどを理由に設定を行うこと自体が敬遠される傾向にあった。このような状況を踏まえ、事業者側では、平成 15 年ころから無線ＬＡＮの接続及び暗号化をボタン一つで初心者でも簡単かつ確実に暗号方式の設定ができる仕組みを開発し、事業者のそれぞれの無線ＬＡＮに搭載されるようになり、平成 18 年には、暗号化方式の簡易な設定方法に係る統一した標準規格であるＷＰＳ[17]が定められた。以降、無線ＬＡＮにはＷＰＳ等による設定方法が標準的に搭載されるようになり、最近では、高度な暗号方式が既に設定された製品を出荷するなどの取組も実施されて無線ＬＡＮのアクセスポイントの不正利用を排除する対策が伸展している。

イ 問題点

前述のとおり、近年、無線ＬＡＮのアクセスポイントや新たに開発されるアクセスポイントに接続可能な携帯型ゲーム機等は、ＷＰＡ等の高度な暗号方式

---

[14] WEP(Wired Equivalent Privacy) 無線 LAN 初期の暗号化するための規格。脆弱性が指摘されている。
[15] WPA(Wi-Fi Protected Access) 欠点が多い WEP の代わりに考えられたより高度な暗号化するための規格
[16] WPA2(Wi-Fi Protected Access2) WPA の改良版でさらに高度な暗号化するための規格
[17] WPS(Wi-Fi Protected Setup) WPA を初心者にも簡単に設定できるようにする標準規格

の設定が可能なものとなりつつあるほか、高度な暗号方式を簡単に設定するための機能が搭載されたものも普及している。また、事業者によっては、工場出荷時においてあらかじめ高度な暗号方式を設定するなどの対策をとっており、無線ＬＡＮのアクセスポイントの不正利用を排除するため、各種関連製品のセキュリティレベルを向上させる対策が伸展している状況にあるといえる。

しかし、高度な暗号方式の設定等の対策のなされていない無線ＬＡＮ製品についても依然として一般家庭等において使用されている状況が見受けられるところである。

また、高度な暗号方式の設定や簡単接続等の機能が備わっているにもかかわらず、利用者において、無線ＬＡＮのアクセスポイントに対する不正利用についての危機意識が欠如していることなどを理由に、こうした設定が実施されない状況が見られる。特に、ＷＰＳ導入以前の無線ＬＡＮのアクセスポイントについては、そもそも設定方法を十分に理解していない、面倒であるなどの理由により、暗号方式の設定をせずに無防備な状態のまま、現在に至るまで使用していたり、例えば、旧型の携帯ゲーム機を始め、ＷＥＰしか設定できない無線ＬＡＮ組込製品を接続するために、意図的に無線ＬＡＮのアクセスポイントのセキュリティレベルを下げるなどの状況も見受けられるところである。

以上のような状況を踏まえると、今後時間の経過とともに利用者が製品の買換え等を行うため、対策が講じられる前の脆弱なセキュリティ設定のみの無線ＬＡＮ製品や無線ＬＡＮ組込製品については、そのシェアが自然減少するものと予想されるため、無線ＬＡＮのアクセスポイントのセキュリティについては、中期的には状況改善の見込みがあるといえる。しかしながら、前述のとおり、高度な暗号方式の設定が可能な製品が普及しても、利用者の理解が不十分であったり、危機意識が希薄であることにより、高度な暗号方式が設定されない無線ＬＡＮ製品や無線ＬＡＮ組込製品が今後も使用され、結果として、セキュリティの脆弱な無線ＬＡＮのアクセスポイントが存在し続け、サイバー犯罪敢行の際の匿名化手段として悪用されるという問題が残されている。

3　今後の在り方

(1)　データ通信カードの利用契約時等における契約者の本人確認の確実な実施等

データ通信カードにおいて事後追跡可能性を確保するためには、現実空間との接点である利用契約を始めとする通信手段の開設に当たって、契約名義人が利用者本人であるということを確実に特定するなどして、他人へのなりすまし防止対策の充実を図ることが必要である。

そのためには、事業者は、利用契約時やオンラインによる即時加入時等に、契約名義人の本人確認を確実に実施することが望ましい。その際、契約名義人の人定を特定するために、例えば、契約名義人の氏名、住所、生年月日、連絡先番号等を免許証や健康保険証等の公的書類で確認する方法が考えられる。また、データ通信カードを送付した住居地における受領者を特定するために、データ通信カードを後日送付する場合には契約名義人の住所以外には認めないこととするか、

又は契約名義人以外の住所に送付する場合には、契約名義人の場合と同様、利用者の本人確認を実施する方法等が考えられる。

総合セキュリティ対策会議における議論を契機として、業界団体である（社）電気通信事業者協会において、会員事業者を構成員とする検討部会の中で、他人へのなりすまし防止対策の充実が検討されているところである。今後は、各事業者がデータ通信カードに係る利用契約時の手続の見直しに向けて、利用者の利便性を考慮しつつ、平成 24 年４月から、順次本人確認の強化を図ることによって、本人確認手続の悪用を抑制し、他人へのなりすましによる犯罪を抑止するための対策を講じることが期待される。

(2) 無線ＬＡＮ製品の使用者に対する働き掛け

無線ＬＡＮのアクセスポイントがサイバー犯罪の手段に悪用されないようにするためには、外部から使用権限のない者に不正利用されないように、セキュリティ対策として高度な暗号化の設定を行うことが必要である。特に、ＷＰＳ等による設定方法が標準的に搭載されるようになった平成 18 年よりも前の対策前の無線ＬＡＮ製品については、高度な暗号化の設定がされておらず、不正利用されるおそれが高いといえる。

以上を踏まえ、無線ＬＡＮを取り扱う事業者は、対策前の無線ＬＡＮ製品を使用している者に対し、製品の販売や広告、新製品の説明や無線ＬＡＮに関するキャンペーン等の機会を通じて、不正利用の危険性について注意喚起し、高度な暗号化方式の設定が可能な無線ＬＡＮ製品への買換えを促すことが望ましい。

また、高度な暗号化方式の設定が可能な無線ＬＡＮ製品であっても、解除するなどして高度な暗号化の設定をしないまま使用されている現状があることから、無線ＬＡＮを取り扱う事業者は、このような無線ＬＡＮ製品を使用している者に対し、製品の販売や広告等の機会を通じて、高度な暗号化の機能について理解を深め、設定を確実に行うよう今まで以上に注意喚起して、利用者の意識改革を図ることが望ましい。

第２　インターネットカフェ

１　事後追跡上の障害の現状

(1)　問題の解決に向けた取組の経緯

インターネットカフェにおいては、利用者の確実な本人確認が実施されていない、又は利用者の入退店時刻やコンピュータの使用状況が記録されていない営業形態の場合、事業者が利用者を特定するための情報を保有していないことになる。また、外部から客席を見通すことが困難な構造の場合、事業者が客席内の利用状況を把握することが困難である。このような営業形態や構造は、サイバー犯罪捜査における事後追跡上の障害となり、犯人や犯行状況の特定を困難にしている。

これらの問題は、平成 18 年度総合セキュリティ対策会議において、サイバー犯罪捜査の大きな障壁になっていることが指摘され、その対策の在り方が議論された。そして、インターネットカフェを利用したサイバー犯罪の防止を図るとともに、当該犯罪を確実に検挙するためには、インターネットカフェにおける利用者の匿名性を排除するための対策が必要であり、具体的には、事業者が自主的な取組として、利用者の本人確認を確実に行うとともに利用者の特定に資する情報を一定期間保存すること、利用者の入退店時刻や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こと等が取りまとめられた。これを踏まえ、警察庁では、インターネットカフェ等の事業者団体である日本複合カフェ協会に対し、利用者の匿名化排除対策等の強化について要請を行ってきた。また、都道府県警察においても、管轄区域内のインターネットカフェの実態を把握するとともに、事業者との連携を強化し、サイバー犯罪の防止等の観点から、利用者の匿名化排除対策として、例えば、事業者に対して書面等による本人確認の実施や利用者の入退店時刻の記録化等についての働き掛けを推進してきたところである。また、東京都においては、インターネットカフェにおけるサイバー犯罪の防止を図ることなどを目的として、インターネットカフェ条例が制定され、東京都内で営業する事業者に対し、本人確認実施の義務化等もなされたところである。

(2)　事後追跡上の障害となる状況の一時的な改善

インターネットカフェが事後追跡上の障害となる状況については、平成 19 年当時と現在を比較すると、以下のとおり、大きく変化している。

平成18年における都道府県警察に対する実態調査では、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、未検挙のものは 277 件（認知件数の 46.8%）であり、そのうち212件（未検挙件数の76.5%）は事後追跡上の障害により捜査に進展が見られないものであった。この中で、インターネットカフェが捜査の障害となっていたものは139件（事後追跡上の障害による未検挙件数の65.6%）となっていた。

平成23年に実施した実態調査では、平成22年中に警察が認知した不正アクセス行為 1,885 件のうち、平成 23 年５月末の時点で未検挙のものは 300 件（認知件数の 15.9%）という結果となっており、そのうち 159 件（未検挙件数の 53%）は事後追跡上の障害により捜査が困難となっていることが判明した。この中で、インタ

ーネットカフェが捜査の障害となっていたものが 13 件（事後追跡上の障害による未検挙件数の 8.2%）となっていた。

平成 18 年と平成 23 年の調査結果を比較すると、サイバー犯罪捜査における事後追跡上の障害のうちインターネットカフェの占める割合は平成 18 年の 65.6%から平成 23 年には 8.2%と大幅に減少している（図２－２－１）。

このように事後追跡上の障害としてインターネットカフェの占める割合が大幅に減少している背景には、第１章の４の(4)で述べたように、不正アクセス禁止法違反検挙件数における匿名化手段について、平成 17 年にはインターネットカフェが最も多かったが、平成 22 年にはデータ通信カードが最も多くなり、この５年間で犯人側の匿名化手段がインターネットカフェからデータ通信カードに移行していることが要因としてあると考えられる。つまり、犯人にとって匿名化手段は、その時々の状況に応じて、複数ある中から最も利便性が高く検挙されにくい通信手段・環境を選定するものであるが、この５年間で犯人側の匿名化手段としての有用性がデータ通信カードよりもインターネットカフェが相対的に低くなり、犯人側の匿名化手段として選定され、インターネットカフェにおいてサイバー犯罪を敢行することが少なくなったことから、事後追跡上の障害となる状況が一時的に改善している可能性があると考えられる。

図２－２－１　事後追跡上の障害に関する実態調査結果の比較

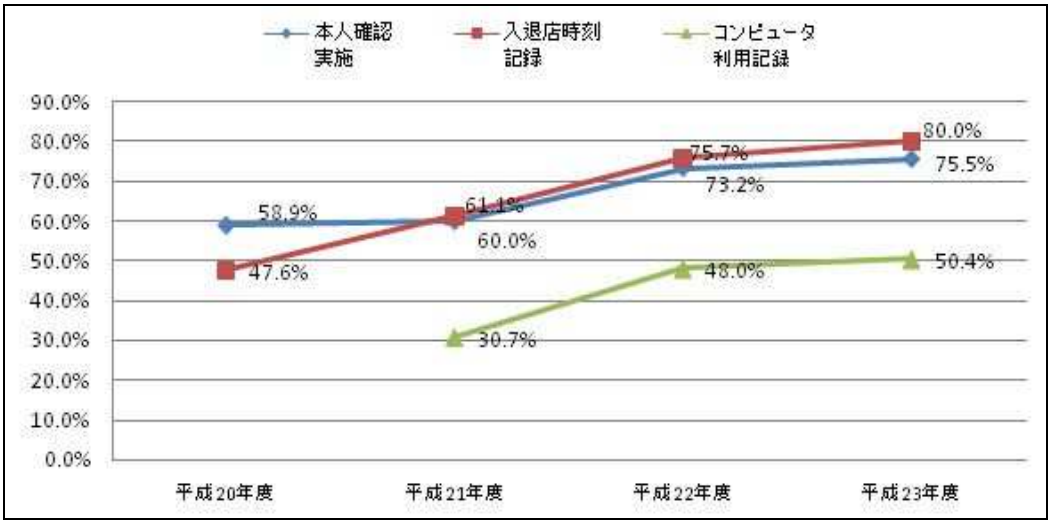
	①　不正アクセス行為の未検挙件数(何らかの障害)	②　不正アクセス行為の未検挙件数(インターネットカフェが障害)	割合（②／①）
平成18年	２１２	１３９	65.6%
平成23年	１５９	１３	8.2%

(3)　匿名化排除対策の実施状況の改善

平成 19 年以降、事業者による利用者の匿名化排除対策が推進されており、警察庁において平成 20 年から実施している対策の推進状況の調査では、全国のインターネットカフェにおける本人確認の実施率、利用者の入退店時刻記録率及び利用者が利用したコンピュータの利用記録率は平成 20 年から平成 23 年にかけて増加しており、平成 23 年の本人確認実施率は約 75.5%（平成 20 年：約 58.9%）、利用者の入退店時刻記録率は約 80.0%（平成 20 年：約 47.6%）、コンピュータの利用記録率は約 50.4%（平成 21 年：約 30.7%）となっている。このように、インターネットカフェにおいて、利用者の匿名化排除対策が継続してなされており、これまで都道府県警察が事業者に対して行ってきた行政指導について一定の成果が見られるところである(図２－２－２)。

また、条例の制定による匿名化排除によって、サイバー犯罪捜査における事後追跡可能性を大きく向上させることとなった警視庁では、条例施行後１年間で、当該条例によって義務化された本人確認記録等を活用して電子計算機使用詐欺事件や詐欺未遂事件等４件を検挙している。

図２－２－２　インターネットカフェにおける匿名化排除対策の実施状況（全国）



(4)　まとめ

事後追跡上の障害としてインターネットカフェの占める割合が大幅に減少しているのは、インターネットカフェにおけるサイバー犯罪への悪用が減少した一方で、データ通信カードによるサイバー犯罪への悪用が増加したということである。

これは、インターネットカフェにおいて、店舗における本人確認の実施や利用者の入退店時刻・使用したコンピュータの記録化等利用者の匿名化排除対策が推進された結果、犯人側の匿名化手段として相対的にインターネットカフェが悪用しにくくなった可能性があること、匿名化手段としてインターネットカフェより犯人側にとっても利便性の高いデータ通信カードを選定するようになってきていること等が、インターネットカフェを利用したサイバー犯罪の減少につながっているものと考えられる。

2　現状の問題点

インターネットカフェがサイバー犯罪捜査の事後追跡上の障害となる状況は一時的に改善しているものの、現状では、次に掲げる問題点のとおり、犯人は本人確認未実施の店舗をわざわざ狙っており、これが事後追跡上の問題になることに加えて、事業者の本人確認の未実施等を行政指導によって改善するには限界があり、対策が及ばない店舗が存在し続ける可能性がある。また、次のとおり、業界全体のモラルハザードが進み、日本複合カフェ協会を脱退する事業者は本人確認を実施せず、今後は本人確認の未実施の店舗が増加する可能性があるなど、状況を悪化させる不安定要素が潜在化している。

このような中で、将来、他の通信手段・環境における匿名化排除対策が進展することなどにより、インターネットカフェが匿名化手段としての有用性が相対的に高くなり、事後追跡上の障害として大きな問題になることが懸念される。

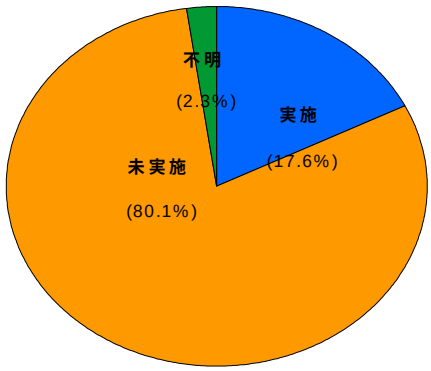
(1)　本人確認未実施の店舗を狙ったサイバー犯罪の敢行

実態調査の結果では、インターネットカフェを利用したサイバー犯罪 136 件のうち、本人確認未実施の店舗で敢行されたものが 109 件（80.1%）、実施店舗で敢行されたものが 24 件（17.6%）となっており、本人確認未実施の店舗がサイバー犯罪の敢行場所として狙われやすい状況になっている（図２－２－３）。すなわち、インターネットカフェにおける本人確認実施率が増加しているにもかかわらず、犯罪企図者はサイバー犯罪の痕跡を残さないために、あえて一部の本人確認の未実施の店舗をわざわざ狙っていることがうかがえる。

図２－２－３　犯行利用店舗における本人確認実施状況

本人確認状況	実施	未実施	不明	計
件数	２４	１０９	３	１３６

インターネットカフェを利用したサイバー犯罪 136 件は、平成 22 年から平成 23 年５月末までに検挙・未検挙の件数



これまで、行政指導の結果、インターネットカフェにおける本人確認実施率が改善してきているものの、あくまで事業者の自主的な取組によるところが大きいため、その改善には限界があるところである。

インターネットカフェ条例が制定された東京都においては、平成 21 年度から平成 23 年度にかけて本人確認実施率、利用者の入退店時刻記録率、コンピュータの使用記録率が年々大幅に改善しているが、他方で自主的な取組によっている東京都以外の道府県においては、各措置の実施が頭打ちの状況にあり、コンピュータの使用記録率に関しては約 36.6%と低水準にとどまっている状況にあることが、その限界を表しているといえる（図２－２－４、図２－２－５）。

以上を踏まえると、匿名化排除対策が進展していない店舗がサイバー犯罪の実行

場所として狙われやすいことがうかがえるものの、それら店舗に対する当該対策の改善要求は行政指導によることとなり、事業者の自主的な取組に頼らざるを得ず一定の限界があることから、インターネットカフェを利用してサイバー犯罪が敢行されている状況が継続する可能性がある。

図２－２－４　インターネットカフェにおける匿名化排除対策の実施状況（東京都）

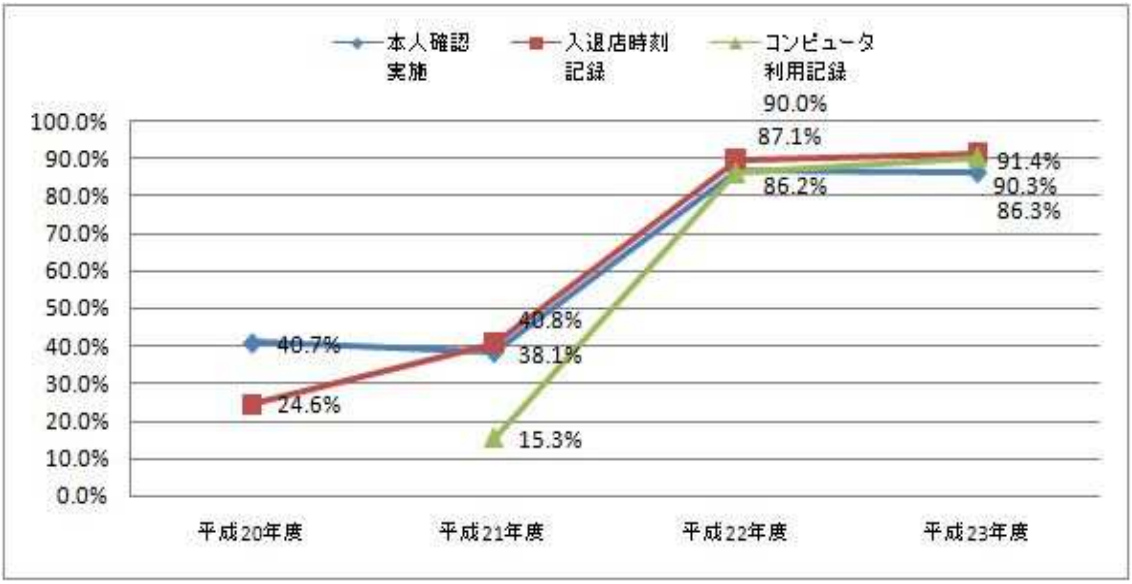
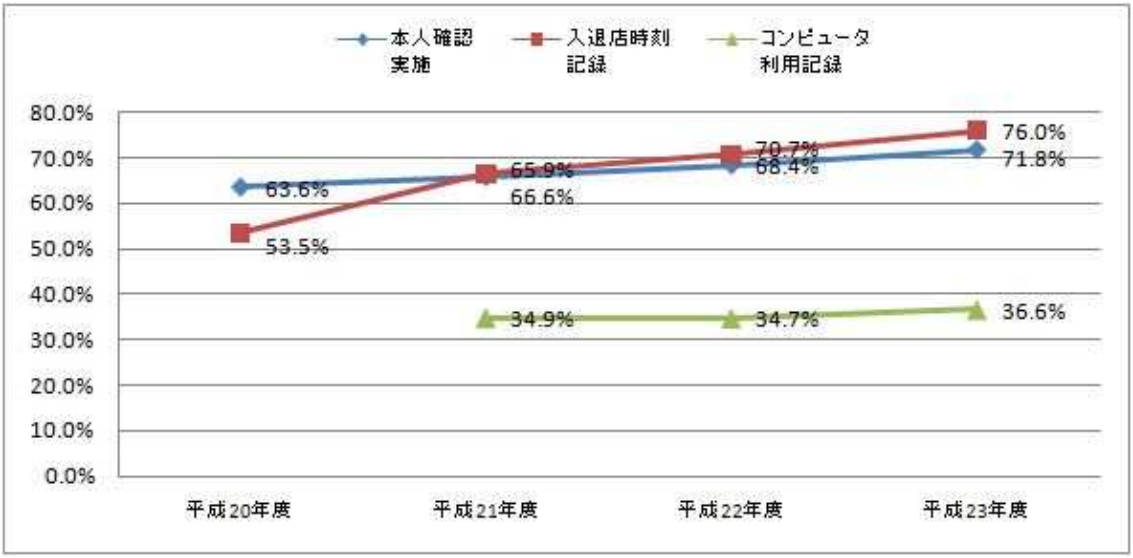


図２－２－５　インターネットカフェにおける匿名化排除対策の実施状況（道府県）



(2)　日本複合カフェ協会からの脱退傾向

日本複合カフェ協会では、犯罪防止、少年の非行防止等を図るため、警察庁の指導の下、運営ガイドラインを策定し、同協会に加盟している事業者（以下「加盟事業者」という。）に対して当該ガイドラインに従った店舗運営を推奨している。当該協会においては、平成 18 年度総合セキュリティ対策会議の取りまとめを契機に、

当該ガイドラインに会員制の義務化を盛り込んだところ、入店時の本人確認を煩わしく感じて敬遠することによる利用者の減少を懸念した加盟事業者が当該協会から脱退し、年々、加盟率が減少している状況にあり、現在の加盟率は約44%にとどまっている（図２－２－６）。

このように、遵法精神の高い加盟事業者がガイドラインに従った運営を行った結果、かえって利益の減少につながり、事業者間で不公平感が広がっていることから、今後は、業界全体のモラルハザードが進み、事業者が社会的責任を果たさなくなるおそれがあり、行政指導による事業者の自主的な取組だけでは、施策の継続性に懸念がある。

図２－２－６　日本複合カフェ協会への加盟率

※第２回総合セキュリティ対策会議における発表資料「インターネットカフェの現状」より抜粋

３　今後の在り方

インターネットカフェにおける事後追跡上の障害が一時的に改善されている現状においても、捜査における事後追跡を逃れるために、犯罪企図者は本人確認未実施の店舗をわざわざ見つけ出した上で、サイバー犯罪を敢行しており、インターネットカフェが未だに匿名化手段として悪用されている状況にあることから、今後も、本人確認未実施の店舗がサイバー犯罪に悪用される可能性は否定できず、事後追跡上の障害としての問題が残されている。

また、法的根拠のない行政指導によって、事業者の自主的な取組として行われている匿名化排除対策を確固たるものにしておかなければ、他の通信手段・環境における対策が進展するなどの状況の変化によって、インターネットカフェが、犯罪企図者にとって匿名化手段としての有用性が相対的に高くなり、サイバー犯罪に再び悪用された場合に、事後追跡上の障害としての問題が大きくなる可能性は否定できないと考えられる。

このような予断を許さない状況に対応するためには、匿名化排除対策を軌道に乗

せて事後追跡可能性を確実に確保し、サイバー犯罪対策の防止を徹底する必要がある。

以上を踏まえ、全ての事業者に対し一律に実施させるため、次に掲げたとおり、現状の行政指導によって行われてきた取組についての法制化を検討することが望ましい。

(1) 利用者の本人確認の実施等の義務付け

インターネットカフェにおいてサイバー犯罪が敢行された場合に、犯人を特定するためには、事業者が利用者を特定するための情報を保有していることが必要であることから、事業者に対し、利用者の本人確認を実施するとともに、当該記録を作成し一定期間保存することを義務付けること。

(2) 利用者の入退店時刻・使用したコンピュータの記録化等の義務付け

インターネットカフェにおいてサイバー犯罪が敢行された場合に、犯罪の状況を特定するためには、事業者が利用者の利用状況を特定するための情報を保有していることが必要であることから、事業者に対し、利用者の入退店時刻・使用したコンピュータの記録を一定期間保存することを義務付けること。

(3) 店舗内におけるサイバー犯罪の利用を防止するための措置等の義務付け

店舗内におけるサイバー犯罪を防止するためには、事業者は、利用者が安全に利用できる環境を整備することが必要になることから、事業者に対し、例えば、顧客が入力した情報を他人が不正利用できないようにする機能を有するソフトウェアの導入や防犯カメラの設置等、店舗内でサイバー犯罪に利用されることを防止するための措置を義務付けること。

第３　インターネット上の高度匿名化技術

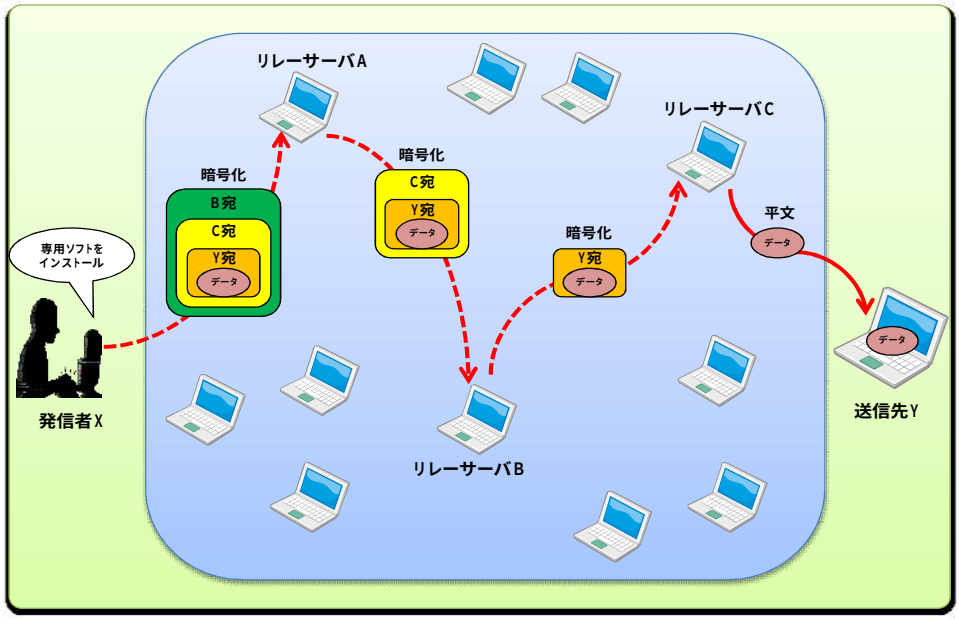
１　事後追跡上の障害の現状

インターネット上の高度匿名化技術とは、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やジャーナリストのレポートの保護等、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を目的として研究されてきた技術である。実際に、情報統制が行われている国々において民主化を主張する人々が、インターネット上で通信する際に、その活動と自己のプライバシーを保護するため利用されている。

(1)　匿名化に利用される技術の概要

高度匿名化技術は、使用者のコンピュータ、これにインストールする専用ソフトウェア及びインターネット網に存在するリレーサーバから構成され、リレーサーバはＰ２Ｐ技術[18]を応用して発信元のコンピュータから送信先のコンピュータまでの通信を中継するネットワークを構成している。一般的な通信の場合は、発信元のコンピュータと送信先のコンピュータとの間で直接通信を行うのに対し、高度匿名化技術を利用した通信の場合は、発信元コンピュータから世界中のインターネット上にあるリレーサーバのうち任意の３台を経由して、送信先のコンピュータと通信を行っている（図２－３－１）。このとき、リレーサーバは、当該通信に係る記録を残さないように設計されているため、送信先のコンピュータに残る通信に係る記録からは、発信者の特定が困難となる。

図２－３－１　インターネット上の高度匿名化技術の動作概要



[18] ネットワーク上のデータの送受信に関する技術の１つで、パソコン等の端末の間で直接データのやり取りをするもの。例えば、Winny、Share 等の一部のファイル共有ソフトは、Ｐ２Ｐ技術を応用することで、パソコン等の端末同士がアップロード用のサーバ等を介さずに、互いに直接通信しながら、バケツリレーのようにデータを転送し合うことで、ファイル交換を可能にしている。

(2) 研究・開発コミュニティ

現在、高度匿名化技術を構成する専用ソフトウェアは、オープンソースソフトウェアとしてインターネット上に無償で公開され、誰でもそのソフトウェアの利用、改良及び配布が可能となっている。そのため、世界中の技術者等が高度匿名化技術の学術研究・改良に参加することが可能であり、特に情報セキュリティ等の学術分野においては、高度匿名化技術をプライバシー保護のための基本的に善意で利用される技術と位置付けた上で、その技術の改良や普及・促進に取り組むコミュニティが海外を中心として形成されている。

(3) 犯罪への悪用状況

上記のとおり、高度匿名化技術を構成するソフトウェアは、誰でも自由にコンピュータにインストールできることから、高度匿名化技術は誰でも容易に利用することができる。また、本ソフトウェアをインストールしたコンピュータは、リレーサーバとして他人の通信の匿名化のために提供することも可能であることから、世界中には本ソフトウェアをインストールした数千台のリレーサーバがインターネット上で稼働している。したがって、犯罪企図者にとっても事後追跡を困難とする目的で高度匿名化技術を利用することが可能となっている。

海外においては、インターネット上に違法情報を流通させる場合に悪用された例も確認されており、高度匿名化技術はプライバシー保護等に利用される側面と犯罪インフラとして悪用される側面の両面を備えているといえる。

なお、国内においては、現在のところサイバー犯罪への悪用は、警察庁の実態調査結果によると、平成 22 年から平成 23 年５月末までの間に１件[19]のみが確認されている。

2 現状の問題点

上記のとおり、高度匿名化技術はプライバシーを保護する等正当な目的のために用いられる技術ではあるものの、インターネット上において無償で公開されているソフトウェアをインストールするだけで利用でき、さらに、世界中でリレーサーバが常時数千台稼働しているなど、犯罪企図者が容易に悪用可能な点に問題がある。また、リレーサーバが世界中に多数存在するほか、今後も、日本に限らず海外においても研究開発により匿名化に係る技術が進展することが考えられ、高度匿名化技術の悪用を防止するためには、国内のみを対象とした対策では限界があると考えられる。

3 今後の在り方

高度匿名化技術については、プライバシー等の保護を目的とする技術として研究が推進されてきた一方で、匿名化手段として容易に悪用可能であることから、サイバー犯罪への将来的な悪用への対策を調査研究する必要がある。

---

[19] このほか、国際テロ対策に係るデータのインターネット上への掲出事案では、インターネット上の高度匿名化技術が用いられたことが推測されている。

そのために、警察庁が国内及び海外におけるプライバシー保護技術としての利用状況や犯罪への悪用状況の実態を把握するとともに、事後追跡可能性を確保するための方策について、情報収集すべきである。

情報収集に当たっては、研究者を始めとする有識者やプライバシーの保護を目的とする技術として研究・促進している団体に対し、ヒアリングや意見交換を行うとともに、技術の最新状況を把握するために、ネットワークを形成するなどして連絡体制を構築しておくことが重要である。

また、高度匿名化技術がサイバー犯罪に悪用されて問題になった場合には国際的に協力して対応する必要があることから、警察庁は、各国の捜査機関等及び国際会議等を通じて意見交換をしながら国際的に連携して将来的な悪用への対策を検討すべきである。

第３章　事後追跡可能性の確保に向けた対策の今後の在り方について

これまで、データ通信カード・無線ＬＡＮ、インターネットカフェ、インターネット上の高度匿名化技術といった犯人側の匿名化手段となり問題となっている通信手段・環境について、現状では事後追跡上どのような障害があり、どのような問題点が生じているか、それぞれに対する障害の改善に向けた今後の在り方について述べてきたところである。そこで述べてきた対策を着実に実施していくことで当該通信手段・環境に関しては事後追跡上の問題が相当程度改善されると考えられるが、犯人側の匿名化手段はこれらに限られるものではなく、技術の進展、対策の影響等により時々刻々と変化していくものである。したがって、これら以外の別の通信手段・環境が犯人側の新たな匿名化手段として使用され始めるといった問題が顕在化した段階になって、初めてそのための対策を講じているようでは、通信手段・環境に関する事後追跡上の問題が真の意味で改善されたとはいえない。

そこで、本章では、犯人側の匿名化手段となり得る通信手段・環境全般について、それを匿名化手段として無効化するための方策として、サイバー犯罪の事後追跡可能性の確保という考え方を取りまとめた。

１　匿名化手段における事後追跡上の障害の改善に向けた今後の在り方のまとめ

第２章で取り上げた犯人側の匿名化手段については、その事後追跡可能性が開かれることによって無効化が可能となるものであることを踏まえ、事後追跡可能性を確保するために、それぞれの観点から検討し、障害の改善に向けた今後の在り方についてまとめたものである。

現在悪用事例が多発し、大きな障害となっているデータ通信カード・無線ＬＡＮについては、使用権限のない者が集中的に悪用していることから、障害となっている状況を速やかに改善するための対策を実施する観点からまとめた。データ通信カードについては、他人へのなりすまし防止対策の充実のため、事業者は利用契約時等に契約名義人の本人確認を確実に実施すること、無線ＬＡＮについては、不正利用の防止のため、高度な暗号方式の設定が可能な無線ＬＡＮ製品への買換えを促すこと、高度な暗号化方式の設定を確実に行うように利用者の意識改革を図ることが望ましい旨の意見をまとめた。

既に対策が実施され、改善されつつあるインターネットカフェについては、一部の店舗が事後追跡上の障害としての問題として残っている中で、今後もインターネットカフェがサイバー犯罪に悪用される可能性は否定できないことなどから、事後追跡可能性を確実に確保し、サイバー犯罪の防止を徹底して、軌道に乗った対策を制度化するという観点から、全ての事業者に対し、現状の行政指導によって行われてきた取組について法制化を検討することが望ましい旨の意見をまとめた。

プライバシー保護等のために開発されたインターネット上の高度匿名化技術については、将来的な悪用に備えた対策の調査研究という観点から、国内及び海外におけるプライバシー保護技術としての利用状況や当該技術の悪用状況とともに、事後追跡可能性を確保するための方策について情報収集することが望ましい旨の意見をまとめた。

それぞれの匿名化手段については、これらの対策を着実に実施していくことで当該通信手段・環境に関しては事後追跡上の問題が相当程度改善されることが期待される。しかしながら、法律上の措置を含め各種対策が講じられたとしても、犯人は巧妙な手口で別の方法により悪用することも考えられることから、対策後も再び匿名化手段として悪用されていないかどうかについて注視し、問題が発覚した場合には、二次的な対策を講じることも重要である。

2　通信手段・環境に関する事後追跡可能性の意義

これまでの議論を踏まえ、通信手段・環境に関する事後追跡可能性の意義は、次のとおりまとめることができる。

通信手段・環境に関する事後追跡可能性とは、携帯電話、インターネット等の通信手段やインターネットカフェ等の通信環境について事後追跡可能性が確保されている状態をいうが、その意義としては、第一には、通信手段・環境を利用して敢行されるサイバー犯罪について、どのような者がどのような方法により当該犯罪を敢行したかなどを事後的に把握することが可能となり、捜査活動が円滑に進展できるようになることが挙げられる。

また、通信手段・環境の事後追跡可能性が確保されれば、現実空間で防犯カメラが整備されていると、犯罪が発生した場合にこの記録を手掛かりに犯人の特定がしやすくなるなど捜査活動の円滑化だけでなく、その設置自体が犯罪企図者に心理的影響を与えて犯行を思いとどまらせ、当該地域での犯罪発生そのものが抑止されるようになるのと同様の効果を有すると考えられる。すなわち、通信手段・環境に関する事後追跡可能性は、サイバー犯罪の捜査活動の円滑化だけでなく、サイバー犯罪の抑止に資するというもう一つの重要な意義を有しているものである。

なお、上記の抑止効果を最大限に引き出すためには、犯罪企図者に対して、対策を講じた匿名手段について、事後追跡可能性が開かれ検挙されるということを強く意識させるよう広報、啓発等の取組を講じていくことが必要である。

3　サイバー犯罪の事後追跡可能性の確保について

近年、サイバー犯罪の急激な増加は特に深刻な状況であり、このような状況に的確に対処するためには、サイバー犯罪の捜査活動の円滑化によりその十分な抑止を図ることが必要不可欠であることはこれまでに述べたとおりであるが、そうした中にあって、サイバー犯罪の事後追跡可能性が果たす役割は極めて大きい。

ここでいうサイバー犯罪の事後追跡可能性とは、あくまでサイバー犯罪発生の認知後に、当該通信手段・環境を誰が使用したのかを遡る術を確保しておくということであり、刑事訴訟法が定める手続によって捜査を進める際に、通信手段・環境の利用者情報を始め捜査上必要となる証拠資料がその時点で存置されていることを指すものである。それを確保する方法としては、一つは予めログの保存を義務付けるものがあり、例えば、イギリスにおける爆破テロの発生等を受けて、重大犯罪に対して捜査・探知及び訴追のための情報を確保できる環境を整備する必要性が高まったことを背景に、欧州 22 か国において、ＥＵデータ保全指令に基づき、プロバイダ等に対し一

定期間のログの保存が義務付けられている[20]。一方、我が国では、予めログの保存を義務付けておらず、刑事訴訟法に、捜査機関がプロバイダ等の保有する通信履歴に対して消去しないよう要請できる旨の規定が新設され、事後追跡可能性の確保に向けた一定の法律上の措置がなされた[21]ところである。

サイバー犯罪の事後追跡可能性の確保は、通信手段・環境がサイバー犯罪の手段として無効化されることを意味し、サイバー犯罪の未然防止にもつながるものである。我が国では、これまでにもサイバー犯罪が発生した場合には、警察から関係事業者に捜査上必要な範囲で、大手プロバイダを対象に一定期間のログの保存を要請したりするなど民間事業者に対する協力要請を行ってきたところであるが、今後、安全で安心なサイバー空間を実現させていくためには、事後追跡可能性の確保という考え方に基づき、通信手段・環境に関わる民間事業者の協力を更に広く呼び掛けていき、そうした中で事後追跡可能性を確保することの重要性について理解を求め、この考え方をサイバー空間に関わる全ての当事者の間で広く浸透させていくことが重要である。

なお、サイバー犯罪の事後追跡可能性の確保という考え方を広く浸透させていく過程においては、民間事業者との十分な調整が必要である。

また、現時点においても、新しい通信手段・環境のサービスが続々と登場しているところであるが、これらが新たに匿名化手段としてサイバー犯罪に悪用された場合には、国民の生命、身体及び財産に重大な危害が及ぶおそれがあり、かつこれらが一般利用者にとって新しいサービスを利用する際の萎縮効果として働く可能性もあることから、これらについても、それぞれ民間事業者の自由な経済活動や個人のプライバシーの保護等に配慮しつつ、社会的合意の下、事後追跡可能性を確保するための仕組みについての検討がなされることが必要である。

したがって、これらが新たに導入されようとする段階で、サービスを提供する事業者において、上記の配慮事項を十分に踏まえつつ、犯人側の匿名化手段となる余地がないかということを含めて安全・安心な利用についての検討が行われるようになることが望ましいと考えられる。これにより、新しい通信手段・環境のサービスについても事後追跡可能性が確保され、国民が安全に、また、安心して利用することができるようになり、ひいては、これらのサービスの発展につながるものと考えられる。

---

[20] 欧州 22 か国（平成 21 年４月現在。ＥＵ加盟国 27 か国のうち残り５か国は国内法未整備）では、各国の法令に基づき６か月から２年の範囲で義務付けている。イギリス、オランダ、イタリア、スペイン等は１年間、ポーランドは２年間、フランスはインターネットカフェ等にも拡大して１年間それぞれ義務付けている。
ただし、個人情報保護、人権保護等の観点から、ルーマニア、ドイツ、チェコ等において違憲訴訟が提起されており、実際に、ＥＵ保全指令が違憲とされた国もある。

[21] 刑事訴訟法第 197 条第３項及び第４項に、捜査機関が電気通信事業者等に対して、通信履歴の電磁的記録のうち必要なものと特定し、30 日を超えない期間（特に必要があるときは、さらに 30 日延長が可能）を定めてこれを消去しないように求めることができる旨が規定された。当該規定による保全要請の対象となるのは、要請があった時点においてプロバイダ等が業務上記録しているものに限られ、そもそも記録していないものや、保存期間の超過等により既に削除されたものは対象にはならない。

平成２３年度総合セキュリティ対策会議委員名簿

前田　雅英　　首都大学東京 法科大学院教授

（委員長）

片山　　建　　日本マイクロソフト（株）　法務・政策企画統括本部

政策企画本部　次長

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

齋藤　雅弘　　弁護士

塩崎　哲夫　　富士通(株)　クラウドＣＥＲＴ室長

関　　聡司　　楽天(株)　執行役員　広報渉外室　室長

関口　和一　　日本経済新聞社　論説委員兼編集委員

徳田　敏文　　日本アイ・ビー・エム(株)　経営品質・情報セキュリティ

情報セキュリティ担当部長

中野目善則　　中央大学　法科大学院教授

西本　逸郎　　(株)ラック　取締役　最高技術責任者

平原　伸昭　　トレンドマイクロ(株)　セキュリティエキスパート本部

セキュリティエンハンスメントサポートグループ　部長代行

藤原　靜雄　　中央大学　法科大学院教授

別所　直哉　　ヤフー(株)　最高コンプライアンス責任者（ＣＣＯ）・法務本

部長兼政策企画室長

保木口知子　　(独)国民生活センター　相談情報部　相談支援課長

松浦　幹太　　東京大学　生産技術研究所　准教授

松浦　長洋　　(株)バッファロー　ブロードバンドソリューションズ事業部
担当次長

松浦眞紀子　　神奈川県少年補導員連絡協議会　会長

宮下　正彦　　弁護士

矢橋　康雄　　(社)電気通信事業者協会　業務部長

山田　浩史　　(社)日本ＰＴＡ全国協議会　副会長

與口　真三　　日本クレジット協会　業務企画部　部長

吉川　誠司　　ＷＥＢ１１０　主宰

若松　　修　　日本複合カフェ協会　顧問

計２３名（敬称略・５０音順）

（オブザーバ）

内閣官房

消費者庁

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

平成 23 年度総合セキュリティ対策会議の開催状況

第１回会議　　平成 23 年　６月27日（月）

第２回会議　　平成 23 年　７月22日（金）

第３回会議　　平成 23 年　９月８日（木）

第４回会議　　平成 23 年　11月２日（水）

第５回会議　　平成 23 年　12月20日（火）

第６回会議　　平成 24 年　２月９日（木）

第７回会議　　平成 24 年　３月９日（金）