情報セキュリティ対策における
連携の推進について

総合セキュリティ対策会議　報告書

平成１４年３月

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、ハイテク犯罪の検挙数の急増、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おり、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は、国民の利益に直接的な影響を及ぼす問題となっている。

このたび、１９人の委員が、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議論を行った。委員は、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、地方公共団体、消費者団体の方々であり、委員会においては広い分野の有識者により幅の広い議論が活発に行われた。

本報告書は、当委員会での成果をまとめたものである。可能な限り広い範囲を扱い、情報セキュリティに関する産業界等と警察との連携の在り方について、今後の指針となるようその全体像を浮かび上がらせることを目指したものである。時には、連携の在り方に関連し、より高い視点や、より長期的な視野に立った議論、指摘が行われたこともあった。このようなものについても、「一歩踏み込んだ」報告書とするため、「今後の課題（第６章）」として記載することとした。

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なく、各委員が属する企業・組織の立場を反映したものでもないことをお断りしておく。また、本報告書は、限られた回数の会議の中でまとめられたものであり、必ずしも十分な議論がなされたとは言えない部分もあるところである。このようなことも踏まえ、希望のあった委員については、それぞれの意見を報告書の最後に掲載することとした。

今後、本報告書で述べられた各事項について、より深い議論がなされ、より多くの施策が現実のものとなることが期待される。

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１４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

前田雅英 （委員長）	東京都立大学 教授
伊藤穰一	（株）ネオテニー 代表取締役社長
稲垣隆一	弁護士
岡野直樹	サン・マイクロシステムズ（株） 技術推進統括本部ｴﾝﾀｰﾌﾟﾗｲｽﾞ技術本部第二技術部部長
角田健男	日本電気（株） NEC ソリューションズ政策調査部調査担当部長
桑子博行	（社）テレコムサービス協会 事業者倫理・インターネット委員会委員長 （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
笹木直美	楽天（株） 法務審査部部長
佐々木良一	東京電機大学 教授
下浦敏治	ニフティ（株） システム統括部長
田尾陽一	セコムトラストネット（株） 社長

永田　実　　ソニー（株）
モーバイルネットワークカンパニー　VAIO カスタマーリンク統括部長

東　貴彦　　マイクロソフト（株）
取締役経営戦略担当

平野　晋　　（株）エヌ・ティ・ティ・ドコモ
総務部法務室室長

別所直哉　　ヤフー（株）
法務部部長

増谷信一　　（社）日本ＰＴＡ全国協議会
副会長

松崎秀樹　　浦安市
市長

山口　英　　奈良先端科学技術大学院大学
教授

吉岡初子　　主婦連合会
事務局長

（特別参加）
渡邊幸治　　国家公安委員会委員

（五〇音順、敬称略）

（オブザーバー）
内閣官房情報セキュリティ対策推進室
外務省
経済産業省

事務局　警察庁生活安全局生活安全企画課セキュリティシステム対策室

目次

本編

資料編Ⅰ（諸外国における産業界等との連携の現状等に関する調査）

資料編Ⅱ（参考資料）

（補遺）

第１章　会議の目的

高度情報通信ネットワークを利用することによってあらゆる分野における創造的かつ活力ある発展が可能となる社会、すなわち高度情報通信ネットワーク社会を実現することは、我が国にとって極めて重要であり、このための取組みが、官民を挙げて行われている。

他方、高度情報通信ネットワーク社会の光の部分の伸長に比例して、その陰の部分も露呈してきており、例えばハイテク犯罪の検挙件数は急激に増加してきている。情報通信ネットワークの安全性及び信頼性を確保することにより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、ネットワーク・セキュリティの確保は喫緊の課題となっている。

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いること、ハイテク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情報通信インフラは、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対処するためには極めて速いスピードで発展している高度な技術を活用することが必要であることからすると、ネットワーク・セキュリティは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り、ネットワーク・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との連携が不可欠である。

これまで、ネットワーク・セキュリティに関する産業界等と警察との連携は、自治体（都道府県）において、プロバイダ等連絡協議会を通じた各種の取組み等が行われてきたところである。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ており、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）では、各国内でも産業界等と法執行機関との連携を議論することの重要性が再認識された。

本「総合セキュリティ対策会議」は、こうした状況を受けて、情報セキュリティを始めと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、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ついて検討を行い、連携の在り方に関する基本方針を提示することを目的としている。

なお、上記のような連携の在り方については、我が国において議論が始まったばかりであり、未だ暗中模索の状態といっても過言ではなく、本報告書で提示された基本方針も、固定的なものではなく、今後とも内外の世論等を踏まえた上で、適宜見直しが行われるべきものであることを付言する。

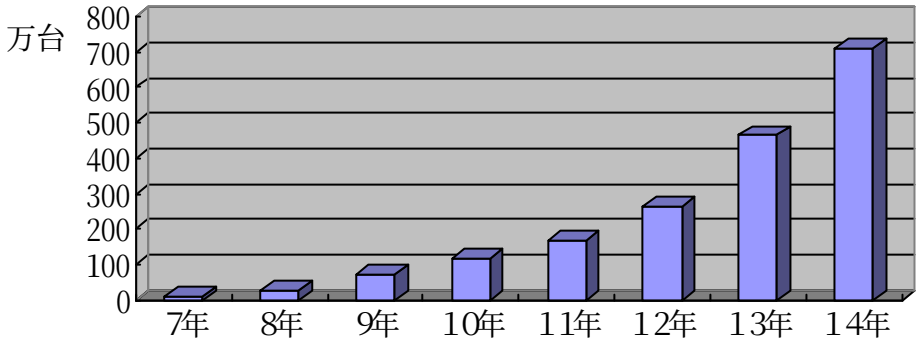
第２章　産業界等と政府との連携の重要性

ネットワーク化の進展に伴って、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１４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712 万台であり、その数は、近年急激に増加している（図２－１）。

図 2－１　インターネットに接続されている国内コンピュータ数

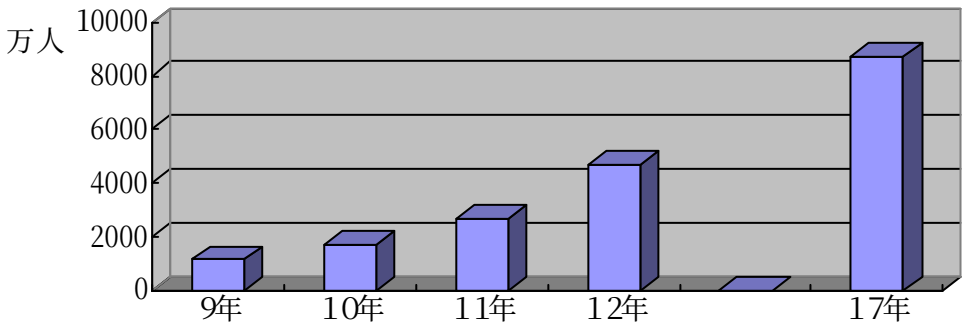


ドメイン名を割り当てられているＩＰアドレスから算出

Network Wizards(http://www.nw.com)

また、国内のインターネット利用者は、平成１２年末において約 4,708 万人であり、平成１７年には 8,720 万人に増加するものと見込まれている（図２－２）。

図2－2　国内インターネット利用者



平成１３年情報通信に関する現状報告（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、そ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、後に見るように、ハイテク犯罪の検挙件数、ハイテク犯罪等に関する相談件数も急激に増加している（第５章３．）。

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。情報セキュリティが語られる際に、官民の連携、すなわち産業界等と政府との連携の重要性が強調されることが多いが、それは次のような観点において、産業界等と政府との連携が重要であると考えられるためである。

(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、信頼性の確保は、国家及び産業界等の双方に共通の課題となっていることから、双方が協力して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

インターネット等の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る。ハイテク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、これら脅威に対しては、警察等の法執行機関のみで対処することは困難であり、産業界等との連携が不可欠である。

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るし、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との連携が不可欠である。

(3)　高度な技術を利用した事象

ハイテク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い。しかも、その技術は極めて速いスピードで進展している。

したがって、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　国際的な潮流（Ｇ８における取組み）

情報セキュリティに関する脅威に対処するための産業界等と政府との連携は、国際的にも重要視されている。ここでは、Ｇ８における取組みを概観する。

また、諸外国における取組みについての調査結果を資料編Ⅰにまとめた。

1．Ｇ８におけるハイテク犯罪対策

平成７年（1995 年）のハリファックス・サミットにおいて設置された、Ｇ８国際組織犯罪上級専門家会合は、同会合が策定した国際組織犯罪に関する４０の勧告が平成８年（1996 年）のリヨン・サミットにおいて各国の首脳に承認されたことから、リヨングループと通称されている。４０の勧告中、勧告１６において、ハイテク犯罪を含んだ現代技術の乱用の処罰が謳われている。

> *１６．（現代技術の乱用の処罰）*
>
> *各国は、刑事処罰に値する現代技術の乱用を犯罪とし、及びその乱用に関する裁判権、法執行体制、捜査、訓練、犯罪防止、国際協力に関する問題に効果的に対応できるよう国内法を見直すべきである。異なった国の間における法執行機関と訴追機関の連携は、それらの問題を提起する際の経験の共有を含めて改善されるべきである。*
>
> *各国は、この分野における研究を促進し、最新技術の犯罪と捜査の問題を提起するための取決めと合意を行うべきである。*

平成９年（1997 年）には、リヨングループ内にコンピュータ技術及び電気通信技術を悪用した犯罪を取り扱うハイテク犯罪サブグループが設置された。

また、Ｇ８には、リヨングループでの検討結果を土台に、国際組織犯罪対策への一層の政治的取組みを強化する趣旨で、平成９年（1997 年）以降、司法・内務閣僚級会合が開催されており、ハイテク犯罪対策が主要議題の一つになっている。

なお、ここの引用したもの及び資料編Ⅱに掲載したもののほか、Ｇ８において作成された各種文書については、警察庁のホームページ（http://www.npa.go.jp/kokusai2/toc_main.htm）及び外務省のホームページ（サミット関連について http://www.mofa.go.jp/mofaj/gaiko/summit/index.html、ハイテク犯罪関連について http://www.mofa.go.jp/mofaj/gaiko/hitech/index.html）に詳しい。

2．Ｇ８における産業界等と政府との連携

官民連携の課題は、Ｇ８においても問題意識を持って取り組まれてきている。

平成９年（1997 年）ワシントンで開催された司法・内務閣僚級会合のコミュニケに添付

された「ハイテク犯罪と闘うための原則と行動計画」では、行動計画７において、産業界との連携が謳われている。

７．

重要な証拠の保全・収集によりハイテク犯罪と闘おうとする我々の努力を新技術が促進するよう、産業界と共同で作業を行う。

この原則と行動計画は、翌平成１０年（1998 年）のバーミンガム・サミットのコミュニケにおいて次のように言及され、その実施について首脳レベルでの合意が形成された。

我々は、我々の閣僚により合意されたハイテク犯罪に関する１０の原則及び１０の行動計画を迅速に実施することに意見の一致をみた。我々は、適切なプライバシーの保護を維持しつつ、証拠として電子データを取得し、提示し、保存するための法的な枠組みについて、及びこれらの犯罪の証拠を国際的なパートナーと共有することについて合意するため、産業界との緊密な協力を呼びかける。これは、インターネット及び他の新たな技術の悪用を含む広範な種類の犯罪と闘うことに資する。

3．官民合同会合

官民連携の在り方を具体的に検討する場として、官民合同会合が開催されている。

平成１１年（1999 年）にモスクワで開催された司法・内務閣僚級会合のコミュニケにおいては、

２２．産業界とのパートナーシップ

ワシントン閣僚級会合において、ハイテク犯罪に対する効果的な解決策を見出すためには、これまで以上の政府と産業界との協力が求められる旨言及した。それ以来、我々は産業界と定期的に協議を行い、効果的にハイテクその他のコンピュータ関連犯罪と対処することにより、インターネットの成長及びこれに対する信頼を促進するべく努めてきた。この重要な対話をさらに進め、協力的な解決策を発展することについての現行の努力を支持するためにも、我々は今や我々の代表者に指示をして、インターネット犯罪について、殊にインターネット犯罪者の探知及び特定の問題につき重点的に、Ｇ８と産業界がアイデアを共有することができるような会議を開催する。

とされ、これを受け、平成１２年（2000 年）５月に、パリにおいて、第１回官民合同ハイレベル会合が開催された（資料編Ⅱ参照）。

同年７月に我が国で開催された九州・沖縄サミットにおいても、産業界等と政府の対話を促進することが合意され、コミュニケ（「沖縄 2000」）及び「グローバルな情報社会に関する沖縄憲章（ＩＴ憲章）」において、それぞれ次のように言及された。

コミュニケ　４４．

我々は、世界的な情報社会における安全と信頼性を著しく脅かし得るサイバー犯罪などのハイテク犯罪に対し、協調したアプローチをとらなければならない。我々のアプローチは、グローバルな情報社会に関する沖縄憲章に述べられている。これを進めるため、我々は、１０月の合同ベルリン会合を含め、産業界との対話を推進する。我々は、パリでのサイバー空間における安全性と信頼性に関する政府と産業界との対話によって生み出された結果及びモメンタムを歓迎し、産業界の参加の下で日本で開催されるハイテク犯罪に関する第２回ハイレベル会合に期待する。

ＩＴ憲章　８．

グローバルな情報社会を構築するための国際的な努力には、犯罪のない安全なサイバー空間を強化するための協調行動が伴わなければならない。我々は、サイバー犯罪と闘うために、情報システムの安全のための OECD ガイドラインに示されている効果的な措置が実施されることを確保しなければならない。国際組織犯罪に関するリヨングループの枠組みにおけるＧ８の協力は強化される。我々は、最近の「Ｇ８パリ会合：サイバー空間における安全性と信頼性に関する政府と産業界との対話」の成功を基礎として、産業界との対話を更に推進する。ハッキングやウィルスといった安全性に関する緊急な問題についても効果的な政策的対応を必要とする。我々は、枢要な情報基盤を保護するために産業界及びその他の利害関係者との関与を継続する。

引き続き、平成１２年（2000 年）１０月に、ベルリンにおいて、政府・産業界合同ワークショップが開催された（資料編Ⅱ参照）。

翌平成１３年（2001 年）２月に、ミラノで開催された司法・内務閣僚級会合のコミュニケでは、次のようにパリ会合及びベルリン会合への賞賛と、来る東京会合への期待が表明された。

１１．

我々はハイテク犯罪に取り組むためには政府・産業界及びその他関係者の間の協力が不可欠であると考える。そこで、我々は、2000 年５月のＧ８パリ官民合同会合及び同年１０月のＧ８ベルリン・ワークショップ会合を賞賛し、今春東京に

て開催されるＧ８ハイテク犯罪対策・政府産業界合同ハイレベル会合における実際的な成果に期待する。

平成１３年（2001 年）５月に東京において開催された、第２回官民合同ハイレベル会合においては、５つのワークショップに分かれて、①データの保存、②データの保全、③脅威の分析及び予防、④電子商取引の保護及びユーザー認証及び⑤トレーニングの各テーマについて議論が行われた（資料編Ⅱ参照）。

第４章　政府の取組み

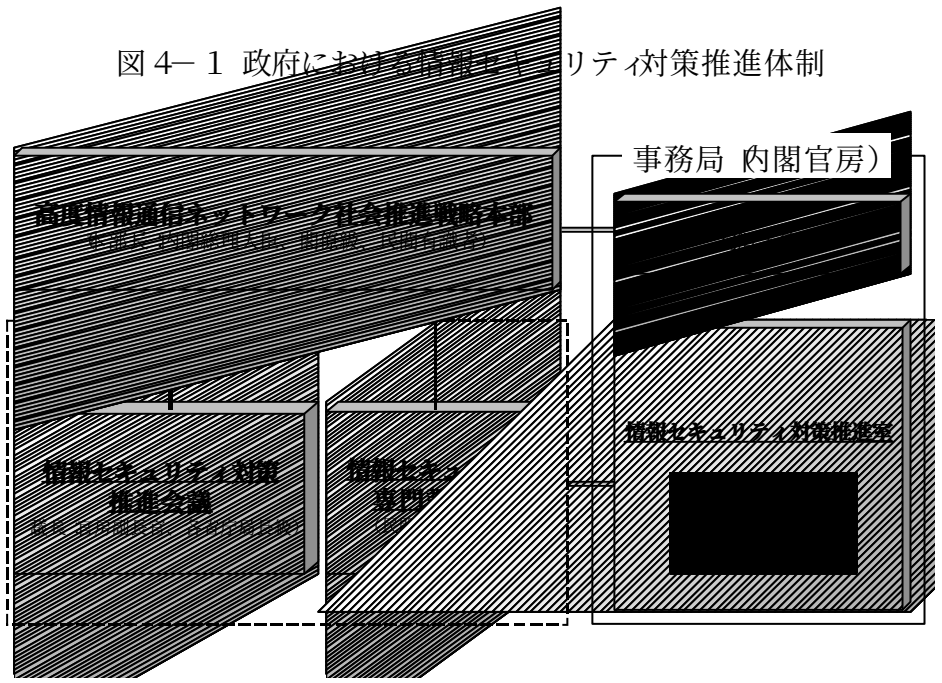
政府においては、「情報通信技術の活用により世界的規模で生じている急激かつ大幅な社会経済構造の変化に適確に対応することの緊要性にかんがみ、高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進すること」（高度情報通信ネットワーク社会形成基本法（ＩＴ基本法）第１条）としているが、その際には、「高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置」（同法第２２条）を講じることとされており、情報セキュリティ対策が行われている。

政府における情報セキュリティ対策においても、官民連携は、重要なテーマとなっている。

1．体制

高度情報通信ネットワーク社会推進戦略本部（ＩＴ戦略本部）の下に全省庁の局長級の会議である「情報セキュリティ対策推進会議」を設置すると共に、ＩＴ戦略本部の下で情報セキュリティに関する民間有識者から成る「情報セキュリティ専門調査会」が開催されている。また、内閣官房（内閣安全保障・危機管理室）に、「情報セキュリティ対策推進室」を設置し、対策の総合的な推進を図っている（図４－１）。

図４－１　政府における情報セキュリティ対策推進体制



2．取組み

平成12年1月　ＩＴ社会の進展に見合った適切なセキュリティ水準を達成するため、「ハッカー対策等の基盤整備に係る行動計画」を策定

7月　全省庁のセキュリティ水準を向上させるため、「情報セキュリティポリシーに関するガイドライン」を整備。

12月　官民の連携・連絡体制の構築、政府の緊急対処能力の強化等を内容とする「重要インフラのサイバーテロ対策に係る特別行動計画」を策定。

13年1月　ＩＴ基本法を施行。

同　我が国を世界最先端のＩＴ国家にするための国家戦略として「e-Japan戦略」を決定。

3月　「e-Japan重点計画」において、高度情報通信ネットワークの安全性及び信頼性の確保のための政府の取組みをとりまとめ。

6月　「e-Japan重点計画」を各府省の平成１４年度の施策に反映する年次プログラムである「e-Japan2002プログラム」において、「高度情報通信ネットワークの安全性及び信頼性の確保」のための政府の取組みをとりまとめ。

10月　「重要インフラのサイバーテロ対策に係る特別行動計画」を踏まえ、「サイバーテロ対策に係る官民の連携・連絡体制」を策定。

同　平成１４年度からの電子政府の実現に向けて、「電子政府の情報セキュリティ確保のためのアクションプラン」を策定。

なお、政府における情報セキュリティ政策は、首相官邸のホームページ（http://www.kantei.go.jp/jp/it/security/index.html）に詳しい。

（「e-Japan 重点計画」、「e-Japan2002 プログラム」、「重要インフラのサイバーテロ対策に係る特別行動計画」及び「サイバーテロ対策に係る官民の連携・連絡体制」については、資料編Ⅱ参照。）

第５章　産業界等と警察との連携の在り方

1.　連携の主体

「官民の連携」における民側の主体は、主に電気通信事業者が念頭に置かれることが多かったが、ネットワーク・セキュリティ確保のためには、警察は、電気通信事業者以外の事業者や、他の組織・団体、国民一般とも、広く連携を行っていくことが重要である。

(1)　電気通信事業者

ハイテク犯罪の舞台となる情報通信インフラを利用し電気通信事業を営む企業は、ネットワーク・セキュリティ確保のための産業界等と警察との連携においても、重要な役割を果たす。

(2)　ハードウェア、ソフトウェア等を提供する事業者

ハードウェア、ソフトウェア等の製品はネットワークの利用に密接に関連したものであり、これらを提供する事業者（メーカー等）はネットワーク・セキュリティ確保にも密接に関連していることから、これら事業者は電気通信事業者同様、産業界等と警察との連携において、重要な役割を果たす。

(3)　ネットワーク・セキュリティ事業者

フィジカル・セキュリティの分野においては、民間によるセキュリティサービスが幅広い分野で定着しているが、近年、技術進歩や社会環境の変化に対応して、情報通信ネットワークに係るセキュリティサービスも発展してきており、経済社会システムにおける犯罪抑止力の形成を図る上での産業界等と警察との連携において、ネットワーク・セキュリティ事業者は重要な役割を果たしている。

(4)　ネットワーク上でサービスを提供する事業者

インターネット上で提供されるサービスを舞台としたインターネットユーザーへの脅威（ユーザーとしての脅威）やインターネット上を流通する違法・有害情報による脅威への対応に関しては、ネットワーク上でサービスを提供する事業者（コンテンツ事業者等）と警察との連携が重要となる。

(5)　自治体

各自治体においては、2003 年までの電子自治体の実現に向けて、その準備を進めているところである。電子自治体の安全性・信頼性確保のためには、住民に関する個人情報を保有する自治体の情報セキュリティが確保されることが不可欠であるが、必ずしも情報セキュリティ確保のために万全な体制が整っているとはいえない状況であり、電子自治体の実現に向けて、自治体と警察とが連携して自治体の情報セキュリティを確保することが重要である。

(6)　教育機関

情報セキュリティの確保のためには、ネットワークを利用する者の情報セキュリティ意識を向上させることが重要であるが、そのためには、各段階での教育が大きな役割を

果たす。コンピュータやネットワークの利用を開始する年齢が低下していることから、小学校や中学校という早い段階から児童に情報セキュリティに関する意識を持たせるための教育を行うことが必要であり、また、高度な知識・技術を有する者が、その知識・技術を悪用することのないよう、大学・大学院・研究機関といった場において情報セキュリティに関する教育を行うことも必要である。

現在、中学校の「技術・家庭」の授業で「情報とコンピュータ」について学ぶこととされており、また、高等学校においては「技術」が必修科目とされており、これら授業において、情報セキュリティに関する教育が行われることが期待される。

また、少年がネットワーク犯罪等の被害に巻き込まれる事例も多くなってきており、少年保護の観点から情報セキュリティ教育を行うことも必要である。

このような情報セキュリティ意識に関する教育に関しては、連絡協議会等を通じて教育機関と警察との連携を強化すると共に実践的な連携を保っていくことが重要である。

他方、大学・大学院・研究機関においては、ネットワーク・セキュリティに関する研究が行われており、知識・技術面からもネットワーク・セキュリティに関与している。これら機関と警察とが連携してネットワーク・セキュリティに関する技術開発を行っていることも期待される。

(7)　法曹界

国民の権利保護という共通の目的の下、これまでも暴力団犯罪の被害者対策等の被害者対策において法曹界と警察は連携してきており、今後は、ハイテク犯罪の被害者保護に関しても警察と法曹界との連携強化が期待される。

(8)　国民

第２章で触れたように、国内のインターネット利用者数は、平成１２年末において約4,708 万人であり、平成１７年には 8,720 万人に増加するものと見込まれている。国民の大多数がネットワークを利用する時代において、ネットワークの安全を確保するための産業界等と警察との連携を考えるに当たっては、一部の事業者や組織・団体だけを念頭に置くのではなく、広く国民全体を視野に入れなければならない。

2．　脅威の実態把握・分析

情報通信ネットワークが社会・経済活動の根幹を担い、その利用が国民生活の隅々まで行き渡っている状況にかんがみれば、情報セキュリティ確保の重要性は明らかである。しかし、「情報セキュリティ」といっても、情報セキュリティに関する脅威の実態が明確にならなければ、何を、どのように、いかなるコストをかけて守ればよいのかが明らかにならない。

産業界等と連携した情報セキュリティ対策を的確に実施するためは、社会の諸分野における情報セキュリティに関する脅威の影響を明確にし、かつ、対策の効果についての調査・分析を継続的に実施することにより、対策の定量的な効果測定を行うことが必要

である。

3. 警察としてのハイテク犯罪への対応

ここでは、ハイテク犯罪の現状を俯瞰し、これに対する警察の取組みを紹介しつつ、産業界等との連携の在り方を検討する。

(1) 現状

ハイテク犯罪の検挙件数は、増加傾向が続いており、平成１３年の検挙件数は、平成１２年に比べて約４５％増加している（図５－１）。検挙件数の内訳を見ると、ネットワーク利用犯罪が全体の約８８％を占め、なかでも、児童買春・児童ポルノ法違反事件やネットワークを利用した詐欺事件の増加が顕著である（図５－２）。

ハイテク犯罪等に関する相談受理件数（都道府県警察に寄せられた相談として警察庁に報告があったもの）についても、平成１３年の受理件数は前年に比べて約５５％増加している。内訳を見ると、わいせつ画像、違法薬物販売等の違法・有害情報に関する相談が全体の約１９％を占めるほか、迷惑メールに関する相談や不正アクセス、コンピュータウイルスに関する相談が急増している（図５－３）。

ハイテク犯罪の現状に関する資料は、警察庁ハイテク犯罪対策のホームページに詳しい（http://www.npa.go.jp/hightech/）。

図５－１　ハイテク犯罪の検挙件数の推移

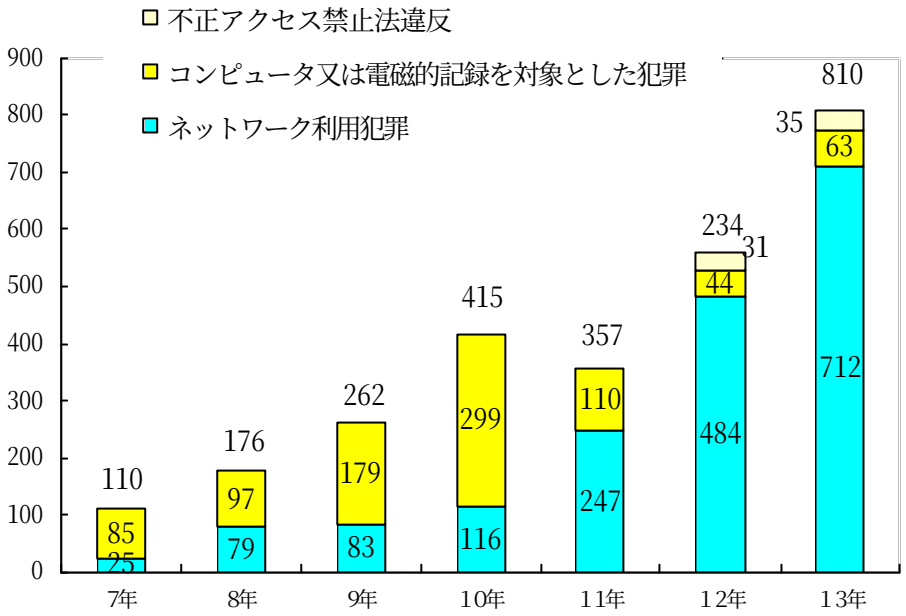


図５－２　ハイテク犯罪の検挙状況

		平成１１年	平成１２年	平成１３年
コンピュータ、電磁的記録対象犯罪		１１０件	４４件	６３件
	電子計算機使用詐欺	９８件	３３件	４８件
	電子計算機損壊等業務妨害	７件	２件	４件
	電磁的記録不正作出・毀棄	５件	９件	１１件
ネットワーク利用犯罪		２４７件	４８４件	７１２件
	わいせつ物頒布等	１４７件	１５４件	１０３件
	児童買春・児童ポルノ法違反	９件	１２１件	２４５件
	詐欺	２３件	５３件	１０３件
	名誉毀損	１２件	３０件	４２件
	著作権法違反	２１件	２９件	２８件
	その他	３５件	９７件	１５１件
不正アクセス禁止法違反		－	３１件	３５件
合　計		３５７件	５５９件	８１０件

＊　その他には、銃砲刀剣類所持等取締法違反、薬事法違反、商標法違反、恐喝等がある。

図５－３　ハイテク犯罪等に関する相談受理件数

	平成13年	平成12年	増　　減
違法・有害情報に関する相談	3,282件	2,896件	386件
迷惑メールに関する相談	2,647件	1,352件	1,295件
名誉毀損・誹謗中傷等に関する相談	2,267件	1,884件	383件
インターネット・オークションに関する相談	2,099件	1,301件	798件
詐欺・悪質商法に関する相談（ｲﾝﾀｰﾈｯﾄ･ｵｰｸｼｮﾝ関係を除く）	1,963件	1,396件	567件
不正アクセス・コンピュータウイルスに関する相談	1,335件	505件	830件
その他	3,684件	1,801件	1,883件
合　　計	17,277件	11,135件	6,142件

＊　その他には、プロバイダ、有料サービス会社とのトラブルに関する相談、ネットワーク・セキュリティ全般に関する相談等がある。

(2)　ハイテク犯罪に対処するための警察における体制整備

ハイテク犯罪は、比較的新しいタイプの犯罪であり、警察においては、このような犯罪に対処するための体制整備を行っている。

①　ハイテク犯罪対策プロジェクトの設置

都道府県警察においては、ハイテク犯罪に関する事務を効果的に行うため、警察内部の各部門が連携の上、ハイテク犯罪に精通した者により構成されるハイテク犯罪対策プロジェクトが設置されている。

②　ハイテク犯罪捜査官の確保

情報通信技術に関する専門的な知識経験を有する人材を、警察部外からも採用している。

③　ハイテク犯罪捜査に資する装備資機材の整備

ネットワークに接続した捜査用パソコン、押収品等の解析用資機材といった各種装備資機材等の整備を図っている。

④　警察庁技術対策課、同技術センターの設置

ハイテク犯罪対策に関し都道府県警察を技術的にリードするナショナルセンターとして、警察庁に技術対策課を設置し、その技術的中核として、同課に警察庁技術センターを開設した。

(3)　ハイテク犯罪情報の集約・分析・提供機能の向上

警察がハイテク犯罪対策を効果的に行うためには、ハイテク犯罪に関する情報を的確に把握することが必要である。そのためには、ハイテク犯罪情報（国民からのハイテク犯罪等に関する相談の情報、アンチウイルス・ベンダー等産業界からの情報、認知・検挙した事件の犯罪手口の検証結果等）を収集・分析し、被疑者の迅速な検挙や被害防止対策といった警察活動に活用することが必要である。

(4)　捜査官間、都道府県警察間の連携の強化

犯罪への対応において捜査官同士の連携が重要なのはもとより、都道府県境を越えて敢行されることの多いハイテク犯罪に効果的に対処するためには、都道府県警察間の連係を強化することが重要である。そこで、産業界等からの情報提供、ハイテク犯罪捜査官の情報・ノウハウの共有、警察庁による連絡・調整等により、捜査官間、都道府県警察間の連携を強化し、捜査効率を向上させることが必要である。

(5)　ハイテク犯罪捜査能力の向上

ハイテク犯罪捜査のためには、ネットワーク等に関する高度な知識・技術が要求される。そこで、最新のコンピュータ・システムやハッカーの手口等に関する教育について、部内での実施に加え、産業界等外部にも委託することによって、ハイテク犯罪捜査官等の能力を向上させることが必要である。

また、都道府県警察間の捜査能力の格差を解消するよう努めることも必要である。

(6)　法執行等に係る情報セキュリティ技術水準の向上

ハイテク犯罪に対処するために必要な情報セキュリティ技術を向上させるため、産業界等と連携した調査・研究開発を通じて、法執行等に係る情報セキュリティ技術水準の向上を図ることとしている。

4．インターネット機能に対する脅威への対応

インターネットの機能そのものを対象とした事案は、ネットワークに関する脅威の中でも、最も重要なものであり、このような脅威への対応はネットワークの機能を保護するものとして重要である。

(1)　現状

警察が認知した不正アクセス行為は、平成１２年（不正アクセス禁止法の施行日である平成１２年２月１３日から１２月３１日まで。）が 106 件であったのに対し、平成１３年は 1,253 件と、約１２倍になっている（図５－４）。

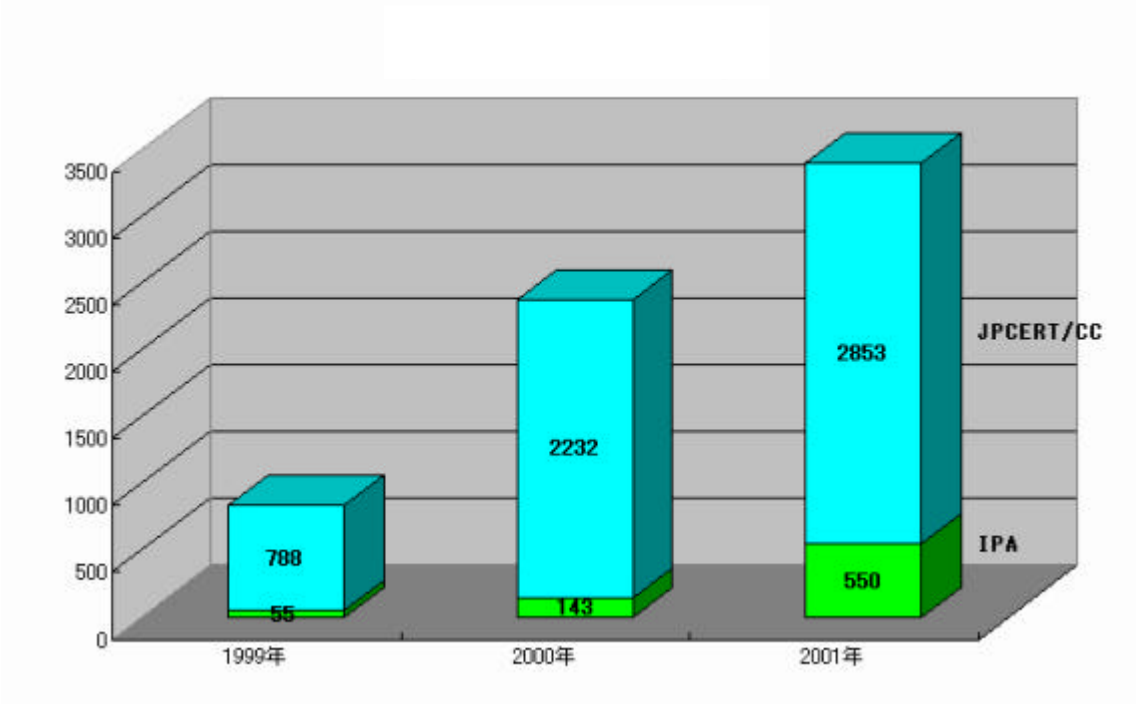
情報処理振興事業協会セキュリティセンター(IPA/ISEC)及びコンピュータセキュリティインシデント（コンピュータセキュリティに関係する人為的事象。例えば、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示や、さらにそれらに至るための行為（事象）などがある。）報告の受付窓口となっているコンピュータ緊急対応センター(Japan Computer Emergency Response Team / Coordination Center(JPCERT/CC))が受け付けた不正アクセス関連行為の届出件数も急増している（図

５－５)。

図５－４　不正アクセス行為の発生状況（警察）

		平成13年	平成12年	増　減
認　知　件　数		1,253	106	1,147
	海外からのアクセス	448	25	423
	国内からのアクセス	258	73	185
	不明	547	8	539

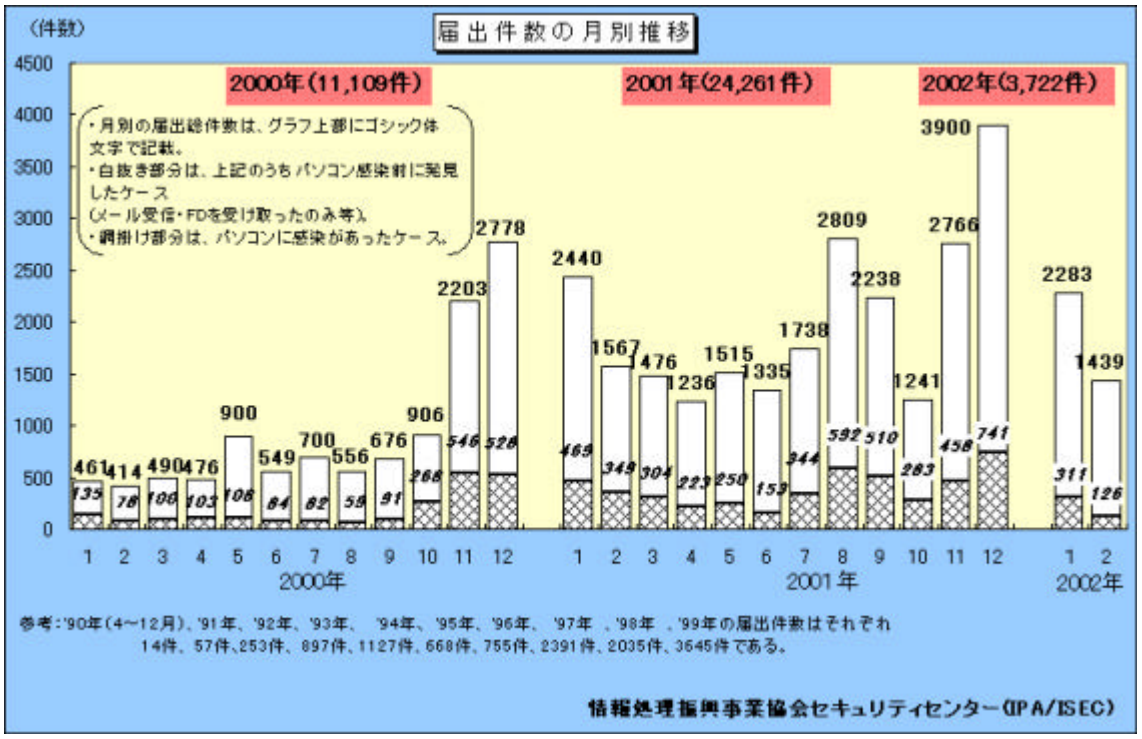
図５－５　不正アクセス関連行為届出件数（ＩＰＡ、JPCERT/CC）



http://www.ipa.go.jp/security/crack_report/20020201/01all.html

また、情報処理振興事業協会セキュリティセンター(IPA/ISEC)に届出のあったコンピュータウイルスの件数も増加している（図５－６)。

図５－６　コンピュータウイルス届出件数（ＩＰＡ）



http://www.ipa.go.jp/security/txt/2002_03.html

この他、サービス不能攻撃（DoS 攻撃）による事案も多く発生しており、例えば、平成１３年３月３１日には、インターネット上でホームページを開設している政党、中央省庁、新聞社等に対し攻撃が行われ、これらホームページの閲覧が一時的に困難となる現象が生じた。

(2)　犯人の追跡性の向上等

このようなインターネットに関する脅威に対処するためには、攻撃元の所在を探知し、特定することが必要である。ネットワーク上の犯人の追跡に関しては、Ｇ８ハイテク犯罪サブグループにおける主要な議題にもなっている。ここでは、Ｇ８における議論を参考にしつつ、犯人追跡性向上のための産業界等と法執行機関との連携の在り方を検討する。

検討に当たっては、技術的側面を常に視野に入れることが重要である。また、ここに挙げたテーマについては、特に、産業界等から様々な意見が出されており、これらの意見を十分に踏まえつつ、法制度、体制、これらの運用、技術といった多面的な観点から検討を行うことが必要である。

①　データの利用可能性

法執行機関がネットワーク上で犯人を追跡するためには、通信記録、加入者情報等のデータが利用可能であることが不可欠であり、これらのデータが常時保存されてい

ることが望ましい。また、このことは、セキュリティ水準の確保や国民の裁判を受ける権利の確保にも資することになる。他方、データの利用可能性については、プライバシーや通信の秘密の観点から問題点が指摘されていることに加え、コストへの懸念も示されている。

データの利用可能性の問題は、官民連携に関する問題の中でも、両者の調整が困難な問題であるが、今後は、次のようなより具体的な論点について検討を行うことによって議論を深めていくことが必要である。

プライバシー、通信の秘密に関する論点：これら権利の保護が及ぶ範囲、程度等
法執行機関に関する論点：捜査に必要なデータの種類、その必要性の程度等
産業界等に関する論点：データ保存の実態、データ保存に要するコスト等

これらの論点を検討するに当たっては、産業界等の負担を軽減するための措置（財政・税制その他の施策を含む。）等についても留意しなければならない。

② データ保全の迅速化（海外との協力も含む）

ハイテク犯罪等の事案が起きた際、法執行機関は必要なデータの保全を要請することとなるが、データの消失や改変を防止するためには、保全の迅速化が必要である。

データ保全の迅速化についても、①と同様に、法執行機関にとっての必要性、産業界等の負担、通信の秘密やプライバシーとの関係等について具体的な議論を行うことが必要である。

また、海外からの要請、海外への要請の迅速化についての検討や、通信が複数のシステムを経由している場合の保全したデータの一部開示についての議論も必要である。

③ リアルタイム・トレーシング

Ｇ８では、ネットワーク上の犯人のリアルタイム・トレーシングに関する議論が行われている。議論に際しては、リアルタイム・トレーシングを可能とする技術に関する議論が不可欠であり、またプライバシーや通信の秘密への配慮も必要である。

④ 追跡を可能とするネットワーク構成の奨励

Ｇ８においては、産業界等に対する、高いセキュリティを有し、また、犯人の追跡を可能とするネットワーク構成の奨励に関しても議論が行われている。議論を行うに際しては、①で述べたような産業界等のコスト負担への配慮も必要である。

⑤ 適切なユーザー認証の奨励

また、Ｇ８では、産業界等に対する適切なユーザー認証の奨励についても議論されている。この議論においては、産業界等のコスト負担への配慮に加え、技術的中立性（特定の技術に依存したものではないこと）にも配慮し、ユーザーによる選択を尊重しなければならないとされている。

(3) 産業界等との情報交換

インターネットに関する脅威については、ネットワーク・セキュリティ・ベンダーや、アンチウイルス・ベンダー等が、不正アクセス、コンピュータウイルス等に関する豊富

な情報を保有している。これら産業界等と警察が、攻撃手法、防御方策等に関する情報を交換することによって対策を講じていくことが必要である。

5. 企業・組織にとっての脅威への対応

企業・組織の活動がネットワークに依存している現在においては、その活動に係る情報セキュリティに対する脅威が即企業・組織に関する脅威となる。企業・組織の活動を守るためには、情報セキュリティの確保が必須である。

(1) 現状

① 不正アクセス、ウイルス、サービス不能攻撃（DoS 攻撃）・サイバープロテスト等

企業・組織の活動がネットワークに依存していることから、不正アクセス、ウイルス、サービス不能攻撃等は、企業・組織に対する大きな脅威である。

② 名誉毀損・誹謗中傷、偽Ｗｅｂページ、ドメイン名の不正取得等

ネットワークを利用した企業・組織の名誉・信用に対する攻撃や業務妨害も、大きな脅威である。掲示板等における名誉毀損・誹謗中傷は、一個人が多数の者に向かって容易に情報を発信できるというネットワークの特性から、大きな影響を及ぼすものである。また、偽Ｗｅｂページの開設、ドメイン名の不正取得といった、ネットワークに固有な手法による業務妨害も、企業活動のネットワーク依存度の高まりに応じて大きな脅威となる。

③ 情報漏洩

企業・組織が保有する顧客情報等個人情報の漏洩は、企業・組織の信用にとって、大きなダメージとなる。情報漏洩は、ネットワークと必然的に結びつくものではないが、個人情報がコンピュータに蓄積されて管理され、企業・組織の活動がネットワークに依存するようになると、ネットワークを通じた情報の漏洩が大きな問題となる。実際に、ウィルスによる情報漏洩事案、ホームページを通じた情報漏洩事案などが発生し問題となっている。

(2) 情報管理

情報漏洩等を防止するためには、企業・組織における情報管理の強化が必要であるが、これに際しては、警察からも検挙事例を基にした防犯措置に関する情報提供等をより積極的に行うことが求められる。

(3) 内部からの脅威への対応

企業・組織に関する脅威については、ともすると外部からの脅威に目が向かいがちであるが、内部からの脅威（内部犯行）も大きな脅威である。

企業・組織は、信用・名誉維持の観点から、内部犯行が公になることを嫌い、警察への届出がなされないなど、適切な対応が取られないことが多い。しかし、内部犯行についても厳正な対処を行うことが、ひいては信用・名誉の維持にもつながるのであり、責任ある企業・組織による対応として、警察への届出等適切な対処を行うことが求められ

る。このことは、情報セキュリティに関する脅威の的確な把握とこれに基づいた効果的な対策の構築にも資するものである。

警察としても、届出を促すため、事件捜査等の対応に当たって、企業・組織の信用・名誉に配慮することが必要である。また、検挙事例を基にした情報提供等を行うことも求められる。

企業・組織が警察への届出を行わないことの理由として、捜査活動により業務の遂行に支障を生じることへの懸念があると思われる。警察としては、できる限り企業・組織への業務に支障が生じないように捜査等を行うように配意しなければならないのはもちろんであるが、そのような配慮を行っていることについて周知を図るよう努めることも必要である。

(4)　ドメイン名の不正取得等

ドメイン名の不正取得等については、裁判外紛争処理機関による手続きが整備されているものもあり、これら機関と警察との連携についての検討が求められる。また、警察から、検挙事例を基にした情報提供等を行うことも求められる。

6．インターネットユーザーへの脅威（ユーザーとしての被害）への対応

インターネットが国民生活に浸透し、多くの国民がオンラインショッピングなどにおいてインターネットを利用するようになった結果、これらインターネットユーザーが悪質商法等の被害に遭う機会も増大してきている。

(1)　現状

ホームページ、電子メール等を利用したネット上での悪質商法（詐欺、無限連鎖講（ねずみ講）、マルチ商法等）による被害が後を絶たない。

平成１３年中のネットワークを利用した詐欺事件の検挙件数は 103 件で、前年（５３件）より約９４％増加した。また、平成１２年にはなかったネットワークを利用したねずみ講事犯の検挙人員は３８人であった。

(2)　犯罪手口に関する情報収集

悪質商法は、同一犯によるものや同一手口によるものが多いため、国民からの相談の情報、産業界等からの情報、認知・検挙した事件に係る情報を収集・分析し、これを警察内部で共有したり産業界等へ提供したりすることにより被疑者の迅速な検挙や被害防止対策に活用することが望まれる。

7．インターネットを利用した犯罪・事象への対応

インターネットを利用した犯罪には、児童ポルノ頒布、わいせつ物頒布、名誉毀損、脅迫、著作権法違反等の違法・有害情報に関するものが多く、違法・有害情報対策は、ハイテク犯罪対策において重要な位置を占める。

また、インターネットを利用した児童買春事犯も急増しており、少年保護の観点から対

策が望まれる。

(1)　現状

違法情報に関する犯罪の検挙状況は、前述のとおりであるが（図５－２）、情報自体が違法であるものの他、犯罪が行われている疑いのある情報（わいせつ図画、銃器、薬物、毒劇物等禁制品及び規制品の売買に関する情報等）や犯罪や事件を誘発する等公共の安全と秩序の維持の観点から放置することのできない情報（犯罪方法を教示する情報、少年の健全育成を阻害するおそれのある情報等）についても、対策を講ずることが求められている（違法・有害情報に関する相談受理状況について図５－３）。

平成１３年のインターネットを利用した児童買春事犯の検挙件数は 117 件であり、急激に増加している。

(2)　サイバーパトロールモニターの委嘱

警察においては、ネットワーク上を流通する違法・有害情報を把握するとともに、関係者に対する指導、検挙、連絡、要請等適宜の措置を講ずることにより、これら情報の流通による害悪の発生の防止を図っている（サイバーパトロール）。

ネットワーク上を流通する違法・有害情報把握については、これまでもボランティア等国民と協力して取組みを行ってきたが、違法・有害情報が氾濫している現状にかんがみれば、インターネット上の違法・有害情報の巡回チェック体制の強化が必要であり、国民にサイバーパトロール業務を委嘱し、これに必要な経費の一部を警察が手当てする、サイバーパトロールの技能を高めるための研修を行うといった施策が望まれる。

このように、国民と警察が協力して違法・有害情報の把握に努めることにより、単にこれら情報の流通による害悪の防止が図られるだけでなく、このような活動に参加した国民の情報セキュリティに対する意識が向上することも期待される。

8．　インターネットに関連する犯罪・事象への対応

インターネットの急激な普及に伴い、インターネットが犯罪に何らかの形で関与する事案やインターネットに関連して何らかの問題が生じる事案も急激に増加している。これらは、必ずしもハイテク犯罪と呼べるものではないが、インターネットに関連する犯罪・事象として、何らかの対策を講ずることが求められている。

(1)　現状

①　出会い系サイト利用をきっかけにした犯罪・事象

平成１３年中のいわゆる出会い系サイトに関係した事件の検挙数は、前年の約 8.5 倍と急増している。出会い系サイトがきっかけとなった重要犯罪（殺人、強盗、強姦等）も数多く発生している。また、児童買春・児童ポルノ法違反事件の検挙数が前年の約 9.4 倍と急増している。被害者についてみると、未成年者が７９％と大きな割合を占めている（図５－７）。

図５－７　いわゆる出会い系サイトに関係した事件の検挙数

		平成１３年	平成１２年	増　減
重要犯罪	殺　人	６件	１件	５件
	強　盗	１０件	２件	８件
	強　姦	４４件	８件	３６件
	略取誘拐	３件	１件	２件
	強制わいせつ	１０件	３件	７件
恐　喝		３４件	４件	３０件
脅　迫		１６件	２件	１４件
暴　行		３件	１件	２件
窃　盗		２３件	－	２３件
詐　欺		２６件	１件	２５件
児童買春・児童ポルノ法違反		３８７件	４１件	３４６件
青少年保護等条例違反		２２１件	２０件	２０１件
その他		１０５件	２０件	８５件
合　計		８８８件	１０４件	７８４件

＊　対象は、インターネット上で異性間の出会いの場を提供する電子掲示板、チャット等（いわゆる出会い系サイト）が関係した事件。

	被害者数	うち未成年者	うち女性
平成１２年	１０２	７１(69.6%)	９６(94.1%)
平成１３年	７５７	５９８(79.0%)	６９９(92.3%)

＊　（　）は被害者に対する構成比

② 迷惑メール

警察に寄せられたハイテク犯罪等に関する相談受理状況を見ると、迷惑メールに関する相談件数は、平成１３年は前年の約２倍に増加している（図５－３）。

また、平成１３年１０月には、出会い系サイトの宣伝メールを不特定多数のユーザーに送信していた業者が、未着信のエラーメール等が返信されないように、自分とは無関係な会社のメールアドレスを返信先として使用して発信し、同社に多量のエラーメールを返信させ、同社の業務を妨害したとして、業務妨害罪で検挙されている。

③ インターネットが連絡手段等として用いられた犯罪・事象

このほか、インターネットが連絡手段等何らかの形で犯罪に関連している事案は枚挙にいとまがない。これらの事案においては、フリーメールやインターネットカフェ等の匿名性が高い手段も多く利用されており、匿名性を悪用して他人になりすまして

犯罪が行われる場合も多い。

(2)　身分確認・なりすまし防止策

インターネットが関係する犯罪の捜査においては、匿名性が捜査の支障となる場合が多い。例えば、フリーメールやインターネットカフェが利用された事案においては、利用者を特定することが困難な場合が多い。

警察はプロバイダ等との契約時の身分確認、インターネットカフェ利用者の身分確認等ネットワーク社会と現実社会との接点での身分確認の必要性を感じているが、他方で、通信の秘密・プライバシーとの関係や、身分確認等にともなうコスト負担の問題もあることから、産業界等と警察が連携してより良い解決策を模索していく必要がある。

また、なりすましを防止するため、第三者が容易に推察し得るパスワードを登録できないシステムの導入、パスワードを忘れた利用者に対する再発行機能（いわゆる「リマインダ機能」）について悪用されにくいシステムの導入等の防止策を講ずることが求められる。

(3)　国民の情報セキュリティ意識の向上

これら犯罪・事象による被害を防止するためには、インターネットを利用する者がインターネットに内在する危険性を認識する、利用者がインターネットを悪用しないといった意識を持つことが必要であり、産業界等と警察が連携してインターネットを利用する国民の意識の向上に努めなければならない。

9．サイバーテロへの対応

重要インフラ（情報通信・情報サービス、金融、航空、鉄道、電力、ガス、政府・行政サービス等）に対する情報通信ネットワークや情報システムを利用した攻撃は、攻撃に要するコストが低く、少人数でも実行が可能であり、地理的・時間的な制約がないこと等から敢行が容易である一方で、国民生活や社会経済活動に重大な影響を及ぼす可能性があり、いなかなる攻撃からも重要インフラを守ることが必要である。

(1)　現状

平成１２年１月から２月にかけて多数の中央省庁のホームページが改ざんされる事案が発生し、平成１３年３月に政党等に対するアクセス集中によるホームページ攻撃事案が発生するなど、サイバーテロの脅威が高まりつつある。

また、平成１３年９月１１日に発生した米国同時多発テロ以降、このようなテロが電気通信技術を悪用して行われる危険性に対する認識が高まってきている。

(2)　サイバーテロ対策の充実強化

サイバーテロ対策の目的は、発生の未然防止、被害拡大の防止及びサイバーテロ事件の検挙である。このため、産業界等と連携を行いつつ、サイバーテロに関する情報の収集（サイバーテロを敢行するおそれのある組織・団体等の動向等）やサイバーテロ防止のためのセキュリティ情報の提供を行うほか、捜査体制や緊急対処体制の整備・強化を

図ることが必要である。

また、産業界等と連携してサイバーテロ対策要員の能力向上を図ることが必要である。

(3)　機動的技術部隊「サイバーフォース」

警察においては、サイバーテロ対策の技術的中核として、「サイバーフォース」と呼ばれる機動的技術部隊を設置し、全国に約６０名の高度な技術を持つ要員を配置している。

サイバーフォースは、①攻撃手法等の情報収集、②防御手法等の研究開発、③脆弱性の評価、④事案の認知・緊急対処、⑤事案の把握等の活動を行うこととしているが、③～⑤の活動については、重要インフラと連携を取りつつ行われなければならない。

また、要員の技術力等を向上させるため、産業界等と連携したトレーニングの実施も必要である。

10．新たな脅威への対応

新たな技術が開発されるとその技術を悪用した脅威が出現し、新たなサービスが登場するとそのサービスを悪用した脅威が出現する。例えば、電子署名技術の開発によって、電子署名を悪用した犯罪が出現し、インターネットバンキングの登場によってインターネットを利用したマネーロンダリングが出現する。

産業界等と警察が連携を強化することによって、このような新たな脅威にも迅速かつ的確に対応していかなければならない。

11．産業界等との連携体制の強化

ここでは、産業界等と警察の連携の場・枠組みの在り方を検討する。

(1)　プロバイダ連絡協議会等

ハイテク犯罪のターゲットとなるおそれのある企業及びプロバイダと警察との間で、ハイテク犯罪情勢に係る情報交換を行うとともに、犯罪手口等の犯罪実態や防犯のための具体的な情報提供等を警察から行うための連絡協議会を、各都道府県警察において設置している。これらプロバイダ連絡協議会においては、情報交換、情報提供の他、シンポジウムや勉強会の開催等の活動が行われており、今後も活発な活動の継続が期待される。

また、教育機関、行政機関等との連絡協議会、被害者保護を図るための弁護士会及び消費生活センターとの協議会等の各種協議会が設置され活動を行っているところであり、このような連携の場の広がりも期待される。

(2)　総合セキュリティ対策会議

情報セキュリティに関する有識者等により産業界等と警察の連携の在り方について検討を行う場である本会議を継続して開催し、具体的テーマに関する検討を深めていくことが期待される。

(3)　サイバーテロ対策協議会

サイバーテロの発生を防止するとともに、サイバーテロが発生した場合には被害の拡大を防止し、事案への対応が迅速・的確に行えるようにするため、重要インフラ企業等と警察との間で情報や意見の交換等を行うための協議会が設置されており、このような場を通じた連携の強化が期待される。

(4)　コンタクトポイントの設定

産業界等と警察との連携を迅速かつ円滑に行うためには、双方がコンタクトポイントを有することが好ましい。産業界等のコスト負担等の事情を考慮しつつ、コンタクトポイントの在り方についても検討すべきである。

(5)　Ｇ８における官民対話への参加とこれを踏まえた国内的な対応

産業界等及び警察の代表は、今後もＧ８における官民対話の場に積極的に参加すると共に、その成果を踏まえて国内における連携を強化していくことが期待される。

(6)　情報セキュリティ技術水準の向上

警察の技術対応力を強化するため、産業界等の有する知識・技術の導入が必要である。そのための連携の場を作るため、学会の設立などにより、コンピュータ法科学(Digital Forensics)ともいうべき学問分野を確立することが望まれる。

また、情報セキュリティに関する知識・技術をデータベース化する等して、これを広く共有できるようにすることも必要である。

12．国民との連携の強化（情報セキュリティ意識の向上）

ネットワーク・セキュリティ対策の根本は、ネットワークを利用する者が、ネットワークに潜在・顕在する脅威を正しく認識し、その脅威を避けるために適切な行動を選択すること（情報セキュリティ意識の向上）である。国民の多くがネットワークを利用している今日において、ネットワーク利用者の情報セキュリティ意識を向上させるためには、広く国民と警察が連携し、国民各層の情報セキュリティ意識の向上を図っていくことが必要である。

ここでは、各種取組みに横断的な課題としての国民の情報セキュリティ意識の向上のための産業界等と警察の連携の在り方を検討する。

(1)　情報セキュリティアドバイザー

ハイテク犯罪等に関する相談への対応や不正アクセス禁止法に規定された援助を行うため、都道府県警察に情報セキュリティアドバイザーが設置されており、産業界等の協力を得て、最新のシステム、ハッカーの攻撃手法及びそれからの防御手法、相談への的確なアドバイス手法等についての教育を行っている。今後も活発な活動が継続されることが期待される。

(2)　情報セキュリティコミュニティセンター

地方公共団体職員、学校教育関係者等を対象とした研修、意見交換等を実施する場と

して、都道府県警察に情報セキュリティコミュニティセンターが設置されており、このような場を通じた連携の強化が期待される。

(3)　広報啓発活動

警察においては、国民の情報セキュリティ意識の向上を目的として、ビデオ、パンフレット等の各種広報啓発資料の作成、配布等の広報啓発活動を推進している。

平成１３年は４月を情報セキュリティ対策の広報重点月間と定め、市町村や学校における講演、パンフレット、チラシ等による広報啓発活動を推進した。財団法人宝くじ協会の助成により財団法人警察協会が制作した情報セキュリティ対策ビデオ「虚構からの誘惑」を警察庁が監修しており、本ビデオは、警察協会から各都道府県警察に寄付され、自治体や学校等に配布されている。

今後も各種広報啓発活動の推進が期待される。

(4)　モデル事業

警察においては、ハイテク犯罪に対処するための方策に関するモデル事業を、国民の協力を得て実施することとしている。平成１４年度には、少年が安心してインターネットを利用できる環境を整備するための家庭へのフィルタリングの普及を目的として、保護者を対象としてインターネット上の違法・有害情報の現状とフィルタリングの必要性を認識してもらうための広報啓発を推進するためのモデル事業が実施される予定であり、今後も国民と協力した各種モデル事業の実施が期待される。

(5)　トレーニング

産業界等と警察が連携して、ハイテク犯罪への対処に関するトレーニングを実施することが期待される。情報技術に関する知識、セキュリティ意識、脅威及びセキュリティに関する知識、法的素養、鑑識・解析技術等のテーマについて、産業界等と警察のそれぞれにおいて情報セキュリティ対策に携わる者に対してトレーニングを行うことが期待される。

(6)　相談への対応

都道府県警察においては、ハイテク犯罪等に関する相談を受理する体制を整備しているところであり、ハイテク犯罪による被害に遭い、遭いそうな場合や違法情報を発見した場合等に、早期に警察に通報し、又は相談することについて広報啓発を行うことが必要である。

また、警察としては、同様の相談を受け付けている団体との連携を強化し、全体として国民の相談に対応する体制を強化していく必要がある。

(7)　ネットワーク相談対応システム

警察が行っている国民からの相談受付業務を充実させるためには、全国ベースで一元化されたシステムを導入し、インターネット上で自動回答を行うなどにより、相談に迅速かつ的確に対応することが期待される。また、相談の傾向等を分析し、ネットワーク上における脅威予測、予防措置等に役立てることが必要である。

(8)　セキュリティポータルサイト

インターネット利用者にとって有用な情報を積極的に提供し、また、情報セキュリティに係る啓蒙等の官民の連携強化を図るため、警察の情報セキュリティに関するポータルサイトを設置することが期待される。

(9)　不正アクセス行為の再発防止のための援助

都道府県公安委員会は、不正アクセス行為による被害にあった者からの申し出により、システムを不正アクセス行為から防御するため必要な措置が講じられるよう、援助を行っている。援助に当たっては、必要な事例分析を産業界等に委託することができることとされている（不正アクセス禁止法第６条）。

援助の実施件数は、平成１２年が６件、平成１３年が２１件であり、今後も積極的な運用が期待される。

(10)　不正アクセス行為からの防御に関する啓発及び知識の普及

国家公安委員会は、総務大臣及び経済産業大臣と共に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を公表することとされており（不正アクセス禁止法第７条）、このほかにも不正アクセス行為からの防御に関する啓発及び知識の普及に努めることが期待される。

(11)　被害の未然防止・被害拡大防止のための情報提供

警察は、コンピュータウイルスやサイバー攻撃による被害を未然に防止し、またその被害拡大を防止するために有益な情報を、産業界等と連携して提供することとしており、警察庁は、平成１３年中、ホームページ書き換え事案（２月）、ホームページ書き換えプログラム事案（５月）、Code Red2（８月）、Nimda（９月）、Badtrans（１１月）及びGoner（１２月）について情報提供を行った。

今後も積極的な情報提供が望まれる。

(12)　情報システム安全対策指針

警察は、情報システムに係る犯罪・被害を未然に防止するための対策や犯罪発生時における警察との連携を確保するための措置を内容とする指針（情報システム安全対策指針）を示すことにより、安全対策の実施を広く呼びかけているところであり（資料編Ⅱ参照）、今後も情報セキュリティ確保のために必要な基準を提示してくことが望まれる。

第６章　今後の課題

前章では、個別の施策を中心に産業界等と警察との連携の在り方を検討したが、本会議においては、連携の在り方に関して、より広いテーマやより長期的な課題についても活発な議論が行われた。

本章においては、そのような議論を紹介し、今後の課題として提示することとした。

1.　プライバシーとの関係

警察活動のあらゆる場面において、プライバシーとの関係をいかに考えるかは常に問題となる。しかし、自己の真の姿を明らかにすることなくネットワーク上で活動することのできる匿名性がインターネットの大きな特徴であること、ネットワーク上の通信には憲法で保障された通信の秘密の保障が及ぶこと、といった事情により、ハイテク犯罪に係る警察の活動においてプライバシーとの関係を如何に考えるかは、特に大きな問題となっている。

産業界等と警察の間での捜査に係る協力や犯罪の防止のための情報交換・提供を議論するに当たっては、単にその必要性を議論するだけではなく、プライバシーや通信の秘密の保護との関係で、産業界等がいかなる情報を持ち得るのか、いかなる情報をどのように交換・提供し得るのかを、関係法制の在り方や解釈の在り方まで立ち入って検討を行っていく必要がある。このような検討は、警察のみで行えるものではないことから、関係機関を交えた議論が行われることが期待される。

なお、プライバシーを巡る議論は、犯罪情勢の変化や技術の発達といった情勢の変化によって議論の方向性が動き得るものであることから、これら情勢の変化を常に視野に入れておくことが重要である。また、ＥＵ等国際的な動向を視野に入れることも重要である。

2.　警察の捜査における課題

警察の捜査に関しては、前章においても、産業界等と連携した、捜査官間、都道府県警察間の連携の強化や捜査官の能力向上の必要性を指摘したところであるが、本会議においては、より根本的な問題として、警察制度の在り方についても議論が行われた。

現行の警察制度は都道府県警察が基本的な単位となっているが、ネットワークを舞台とするハイテク犯罪は、都道府県境を越えて行われることが多く、被疑者の所在地、被害者の所在地（複数にわたる場合も多い）、証拠の所在地がすべて異なる都道府県となる場合も数多くある。同一事件について複数の都道府県警察が独自に捜査を行うこととなると、捜査効率の面からも問題があるだけでなく、捜査に協力する産業界等にとっても、複数の都道府県警察との間で同様の協力を行わなければならず、負担となるとの指摘があった。このような状況に対しては、警察庁が都道府県警察間の調整を行い、捜査の効率化を図っているところであるが、根本的な問題として、ハイテク犯罪のような地域性の低い犯罪に対

して現行の都道府県警察を基本とする警察制度が最適なのか、警察制度の在り方についても議論を行うべきであるとの指摘がなされた。

また、これに関連して、ハイテク犯罪は、都道府県境はもとより国境を越えて行われることも多いことから、国外における捜査の在り方や法の適用についても検討が必要であるとの指摘もなされた。

3. 犯罪の予防における課題

(1) ハイテク犯罪における犯罪予防の重要性

ハイテク犯罪の特徴として、匿名性が高いこと、犯罪の痕跡が残りにくいこと、地域性が低いこと等が挙げられるが、これらの特徴は、ハイテク犯罪の捜査を困難とする要因でもある。また、都道府県境を越え、国境を越えた犯罪の捜査には、多額の捜査費用が投入されることになる。

もとより犯罪が発生した際に的確に捜査を行い犯人を検挙することは、犯罪防止の観点からも重要であることは当然であるが、そもそも犯罪に遭わない、被害を生じさせないための犯罪予防活動も重要であり、ハイテク犯罪の事後捜査は他の犯罪捜査に比べて困難であり、また、多額の費用が費やされるという上記のような事情にかんがみ、ハイテク犯罪においては、犯罪予防活動の重要性が特に高いと言える。

(2) ネットワーク・セキュリティの担い手

現実社会においては、警察のみならず、様々な組織・団体が社会生活の安全の維持に貢献している。ボランティア団体やＮＰＯ、警備会社、法曹界、警察以外の行政機関等である。

ネットワーク・セキュリティの世界においても、ボランティアによるサイバーパトロール、各種団体による相談等が活発に行われているほか、商業ベースでサイバー・セキュリティを提供する企業も発達してきている。

現実社会においては、長い歴史の中でこれらの組織・団体と警察との役割分担や協力関係が比較的明確になっているが、歴史の浅いサイバー・セキュリティにおいては、いまだ発展途上である。例えば、警備会社は顧客がどのような被害に遭ったかを第三者に伝えることは原則としてできないが、一定の場合には警察・消防に通報することができることとされているのに対し、サイバー・セキュリティ・ビジネスにおいては、いかなる場合にサービス提供会社が警察に通報できるかについて明確な基準が形成されていないといった点が指摘された。また、国民からの相談についても、各種団体と警察との協力関係の構築の必要性が指摘された。

また、法曹界は、犯罪等による被害にあった国民の権利を保護するとの観点から各種活動を行っており、このような活動に関する警察との連携強化の必要性も指摘された。

今後、サイバー・セキュリティの確保に関して、いかなる組織・団体が、いかなる役割を担い、それら組織・団体と警察とがどのように連携をしていくか、役割分担や協力

関係の在り方を確立していく必要がある。

また、行政機関内部での連携の重要性も指摘された。ネットワーク・セキュリティに関しては、各行政機関がそれぞれの所掌に基づいて各種施策を講じているが、それらの間での連携が必ずしも円滑に行われていないのではないかといった指摘がなされた。官民の連携も重要であるが、官内部での連携が円滑であってこそ官民の連携も大きな成果を生み出すのである。

ネットワーク・セキュリティの担い手について考える際には、各担い手の間の連携をより効率的に行うため、誰（どの部署）が何をするのかを具体的に考えることが重要である。

(3)　ハードウェア、ソフトウェアベンダーの役割

ハイテク犯罪は、産業界等が発展させてきた情報通信インフラを舞台とする犯罪であることから、ハイテク犯罪対策において、電気通信回線を保有する企業や、電気通信回線を利用したサービスを提供する企業が大きな役割を果たすことは言をまたない。しかし、これら情報通信インフラを利用するためには、コンピュータの利用が不可欠であり、ハードウェア、ソフトウェアを提供する企業の役割も非常に大きい。

まず、利用者がハイテク犯罪の被害に遭わないようなセキュアな製品を提供することが期待される。

また、製品に不具合や脆弱性（セキュリティホール等）があることが明らかになった場合、いかなる対応を行うことが適切なのかについての議論も必要である。かかる対応については、不具合や脆弱性に関する情報を詳細に公表することによってその悪用を招くことはないのかといった点についての考慮も必要である。

さらに、製品の不具合によって生じた損害を誰が負担すべきか、あるいは、製品の不具合をなくすためのコストを誰が負担すべきかといった点についても、今後の議論の必要性が指摘された。

(4)　国民の保護

第２章において、インターネットに接続されているコンピュータ数やインターネット利用者数が急増していることを紹介したが、このことは、ネットワークやコンピュータに関する専門的な知識を持たない国民や、そもそも犯罪に対する認識が一般的に未熟である少年がハイテク犯罪等の被害に遭う可能性が急増していることを意味する。

国民の情報セキュリティ意識の向上の必要性は前章でも指摘したが、被害に遭う可能性に晒されている一般国民や、少年を犯罪被害から保護するための施策の重要性は、特に強調されるべきである。

(5)　情報漏洩対策

前章において、情報漏洩は企業・組織にとって大きな脅威であり、情報の適切な管理や内部犯行への対応が重要であるとの指摘を行った。企業・組織がその保有する個人情報を漏洩させないことは、社会のネットワーク・セキュリティ確保のために一般の企

業・組織が行える重要な方策の一つである。

本会議における議論においては、前章での指摘に加え、多数の住民に関する個人情報を保有する地方自治体や、取材を通じて蓄積された情報を保有する報道機関といった、大量の個人情報を蓄積している組織におけるセキュリティ確保の重要性が特に強調された。

他方で、情報漏洩対策の困難性も提起された。組織に出入りする外部の者や業務の委託先といった組織周辺の者についてまで情報漏洩対策の徹底を図ることは困難なことであるが、これら組織周辺の者からの情報漏洩も大きな割合を占めることからすれば、これらの者に対しても情報漏洩対策の徹底を図ることは極めて重要である。

また、ネットワークの時代においては情報管理の困難性が増大しているので、不要な情報は作成・保有しないという考え方が必要であるとの指摘もあった。

第７章　委員からの意見

本報告書は、限られた回数の会議の中でまとめられたものであり、必ずしも十分な議論がなされたとは言えない部分もあるところである。このようなことも踏まえ、希望のあった委員については、それぞれの意見を掲載することとした。

次の委員から意見が提出された。

- 稲垣隆一
- 岡野直樹
- 角田健男
- 桑子博行
  国分明男
  笹木直美
  下浦敏治
  平野　晋
  別所直哉
- 東　貴彦
- 吉岡初子

（五〇音順、敬称略）

稲垣　隆一

1.　サミット合意を受けてサイバー犯罪対策に関する産業界との連携を正面から課題に据えた会議が行われたことは高く評価される。会議では，国際的な連携と協調すべき課題のみならず,サイバー犯罪対策に関する産業界,自治体,教育,消費者に関連する論点が多数抽出され,今後の方向が議論された。今回の会議では,これらの論点に関する実践的な結論を得るに至らなかったが,会議では,関係者の協力の重要性,国民の文化・リテラシーをふまえて世界の先例となる日本のベストプラクティスを考える必要がある旨指摘されたところでもあり,今後もこのような会議が継続され,より一層の論点の発掘と実務的対応が検討され,実現されることが期待される。

2.　産業界との連携の課題　他省庁との協力・ＮＰＯ

サイバー犯罪に関して産業界との連携が重要である理由は,サイバー犯罪が,日々進化する高度電子通信技術と機器の特性を利用する特性を持つのに対し,それらに関する情報,管理がシステムやサービスの開発者,供給者側に集中し,その予防,捜査,被害者救済にあたっては,その協力が必要とされることにある。

特に,サイバー犯罪条約の求める実体法カタログの増加,データの応急保全や部分開示、捜索・押収、トラフィック・データのリアルタイム収集などを人権保障と調和させつつ国内法化し,執行するためには,機器,プログラムやシステムの開発・運用や通信ログやデータの保存,セキュリティ対策や一定の技術情報の提供・共有など,産業界との連携が不可欠である。これらが適切に行われることは,民事上の被害救済にも重要である。その意味で産業界に対する期待は大きなものとならざるを得ない。

この点に関して会議で提起された主たる論点は,協力に際しての産業界の主体性の確保とコスト負担の公平をどう図るか,他の制度や契約による守秘義務などとの整合性をどう図るかなどである。

連携にあたっての産業界の主体性確保のあり方は,今後,手続法制を検討するにあたって検討されるべき重要な課題である。

サイバー犯罪対策におけるコストは,高度電子通信技術による有用性を享受する国民全てが負担すべきであることは当然であり,セキュリティ対策,個人情報保護マネジメント,優良事業者への消費者の誘導,協力にあたっての免責，セキュリティ対策・個人情報保護マネジメントや通報,記録の保存・保全・提出など協力に伴うメリットの付与，守秘義務の解除や一定の民事免責の導入もまた重要な課題であり,税制の問題とも関係する。

更に,上記の問題に限らず,たとえば電気通信事業分野における通信の秘密法制との整合,労働関係,学校教育,消費者保護・消費者教育,住基ネットを含む行政ネットワークに関するサイバー犯罪対策との連携など,関係省庁との協同が必要な課題も存在す

る。これらは,いずれも,ひとり警察のみが対処しうるものではない。

サイバー犯罪対策に関する産業界との連携を検討するこの会議は,関係各省庁,自治体とも連携・協力が図られるものへと発展することが望まれる。

更に,情報セキュリティマネジメントやシステム監査,インターネット技術の構築,サイバーワールドの秩序維持に,ＮＰＯが重要な役割を担っていることに鑑み,これらとの連携も考慮されるべきである。

3. 連携のありかた　サイバー犯罪条約の国内法制化を前にして

産業界との連携にあたっては,文化の違いをふまえた日本のあるべき姿を考えるべきだとの指摘がなされたことは重要である。この指摘は,上記サイバー犯罪条約の国内法化作業,特に,データの応急保全や部分開示、捜索・押収、トラフィック・データのリアルタイム収集などの手続法の検討にあたり十分に考慮される必要がある。我が国の刑事訴訟法制,警察制度には,固有の歴史的特性があり,産業界・消費者・教育の「かたち」がある。今回の国内法制化は,条約を契機とする点で,通信傍受法制定時と同様,行政警察と司法警察の区分を動かし,有体物を前提とする刑事法制にパラダイムの転換をも迫るものとなる可能性があり,その影響は甚大である。犯罪捜査の中核を担い,国家や国民生活の安全を担う警察には,国内法制化と定着にむけ,産業界,法曹界,学会との透明性ある連携を築き,広く国民の支持を得て,方向付けに関する検討,実施成果の確認と改良のためのモニタリングを行い,サイバー犯罪捜査や国民生活の安全の確保に生かすことが望まれる。

4. サイバー犯罪の予防・捜査能力の確保と人権保障との調和のために

会議ではサイバー犯罪捜査への産業界との協力にあたっては,プライバシーの保護,通信の秘密,報道の自由とのバランスや制度的な整合性を図るべきことが指摘された。また,検討のためには,脅威の実証的な把握,サイバー犯罪とサイバーテロの峻別,手続に応じた対象犯罪や犯罪者の類型化,犯罪技術の絞り込み,警察と連携の担い手のそれぞれが,できることできないこと及び直ちにできることと実施に時間を要するものの切り分け,対策の優先順位を決すべきことが指摘された。

高度情報通信技術の成果を享受する社会の安全を確保するには,情報通信や画像処理技術を応用したサイバー犯罪の予防・捜査能力の強化は不断に図られるべきである。しかし,それらとプライバシーなどの人権保障,通信の秘密,報道の自由とのバランスが実質的にも手続的にも確保されるべきこともまた必要である。

しかしながら,これらの人権状況は，個人情報のデジタル化とその利用の高まり,インターネットによる情報流通,電子国家・電子自治体ネットワーク,民間取引の電子ネットワーク化などを迎え,それ以前と相当に様相を異にするに至っている。特にプライバシーについては,多くの人が,その個人情報,行動情報を様々に電子化して蓄積す

ることを許す一方でデジタル化されない権利,自己情報コントロール権が主張されるなど,その規範に関する議論は流動的である。しかも,新技術がプライバシー保護のあり方や考え方を劇的に変化させることも考えられる。プライバシー保護とセキュリティ対策との関係も,ＯＥＣＤ新ガイドラインの策定にみられるように流動的である。

警察によるサイバー犯罪の予防・捜査活動と人権保障の均衡は,最終的には司法判断にゆだねられる。しかし,司法判断を待つまでもなく,基本的人権の保障を全うしつつ法執行を積極的かつトラブルなく行い,産業界との連携をきめ細かく,機動的に図ってゆく必要がある。そのためには,警察と連携の担い手が,相互の情報提供によって,日々進化する技術,サイバー犯罪の状況認識を共有し,サイバー犯罪の予防や捜査のための連携のガイドラインを不断にかつ実務的に検討できる制度が設けられることが望ましい。制度の一例としては,公安委員会下に,担い手,技術者,官学実務法曹などによる論点に応じた臨機の補助機関を設置するとともに,公安委員会が告示としてガイドライン化することなども考えられる。なお,そこでは,会議での指摘のとおり,情報の共有による脅威の実証的把握,対象犯罪や犯罪者の類型化や犯罪技術の絞り込みによる対策の類型化,各担い手の能力による対策の優先順位の決定が行われることが有用である。また,連携の目的は,検討や情報提供を超え,成果が具体的な制度,ガイドラインとして現実に実施されることにあることに鑑み,検討プロセスや結果が公表され,広く国民からの意見を経て制度化するなど,民主的な基礎と透明性に配慮した制度づくりが望ましい。今回の会議の概要がインターネットで常時公開されたことは評価されるべきである。

岡野　直樹

本報告書につきましては、「第１章　会議の目的」に挙げられている事項に関し、基本的な部分は、警察庁殿により示された提言であると考えております。
また、産業界と警察庁および他の政府機関との連携の在り方に関する各論について、具体的な検討および施策などについては、今後期待されるものであり、本報告書に含まれないものと考えております。

ハードウェアおよびソフトウェアを提供する事業者は、ネットワーク・セキュリティおよびハイテク犯罪に関する取り組みについて、産業界、警察庁および他の政府機関と協調するにしても、基本的には独自の判断において実施するべきものであると考えております。

ネットワーク・セキュリティおよびハイテク犯罪に関する警察庁殿に対するサン・マイクロシステムズ株式会社（以下サン）のこれまでの取り組みとして、サンは、警察庁殿のご要望に応じ、各種の技術に関する教育やセミナの提供、および、サンが提供するハードウェアおよびソフトウェアが犯罪などの対象として関わった事象において、警察庁殿のご要請に応じ、技術的な事項に関する情報の提供などを行ってまいりました。

産業界と警察庁および他の政府機関との連携の在り方に関する各論について、今後、社会的な観点および技術的な観点から十分な検討がなされる場が設けられることを期待しており、その際には、サンは、その検討に積極的に参加させて頂きたいと考えております。
また、ネットワーク・セキュリティおよびハイテク犯罪に関する警察庁殿に対するサンの今後の取り組みについて、産業界、警察庁およびその他の政府機関と協調しつつ、サンの判断において実施させて頂きたいと考えております。

角田　健男

１．会議で議論された課題に対する実務的な議論の必要性について

平成１３年度に開催された３回の会議の議論では、ハイテク犯罪やサイバーテロ防止のために、現在の日本の重要インフラの事態発生時の官民連携の在り方特に警察と産業界等との連携の在り方について多数の課題の抽出がなされたが、明確な方針や結論が出るまでには至らなかった。通信事業者やサービス事業者の通信の秘密に係わる情報の保存や保全の問題とプライバシー保護に対する問題、重要なネットワークインフラの保護や維持体制の強化整備の課題、事態発生時の重要インフラ事業者と省庁間の連携の重要性、ネットワークシステム運用管理者・管理方法の強化の必要性、セキュリティ関連製品ベンダーの役割、犯罪防止のための技術開発の必要性、人的啓蒙教育の必要性等の課題に対して、関連省庁間や関連業界等の組織間を巻き込んだ議論、しかも法制度の専門家に技術者も交えグローバルな視点から解決策に向けた実務的な議論が一層必要と考えます。

２．国家レベルのセキュリティ対策の優先度について

セキュリティ対策は、総合的な見地から進める必要があり、議論の俎上にのった多数の課題に対する現状の達成度分析・評価をまず実施し、早急に対策を取るべきものと、長期にわたる実効性のある強化対策を取るべきものに優先度をつける必要がある。緊急事態での官民の連携体制や国全体のセキュリティ向上維持のための官民連携した国家レベルの実務的な管理組織の確立、重要インフラ自身のセキュリティ対策の強化の在り方、セキュリティ製品ベンダとしての製品の改善ならびに製品改版時のユーザー支援実施、国民のセキュリティ意識の向上教育・啓蒙の実施などは既に開始されているものもあるが早急に実施すべきと思われます。

３．セキュリティ対策に関する技術研究開発の推進とセキュリティ管理の重要性

会議では制度面に関連した問題に議論が集中したが、犯罪防止や犯罪追跡のための技術的な実現性の裏付けに基づく議論が必要と思われる。そのためにはハイテク犯罪やサイバーテロ防止のための技術的な研究開発や重要インフラの運用維持の課題にもっと焦点を当てる必要があるし、省庁間の枠にとらわれない産官学の協力体制により即時に研究開発計画立案作業ならびに実行が必要と思われる。海外の機関との連携による研究開発も一層必要と思われます。また、PC や携帯端末や情報家電のネットワークへの常時接続や無線ネットワークの普及傾向に伴い、ベンダー製品のセキュリティ強化とユーザー自身の機器のセキュリティ強化対策並びに日常のセキュリティ管理が一層重要になってきていると思われる。

桑子　博行
国分　明男
笹木　直美
下浦　敏治
平野　　晋
別所　直哉

●　私たちとしましては、今回の報告書が３回の会議しか経ないで作成されるものであり、プライバシーや個人情報、通信の秘密、さらには事業者の負担といった重要な問題について十分な議論がなされたわけではなく、民間側の意思が正しく反映されたものであるとはいえないものと考えております。また、インターネットの発展と適正な規制をどのように調和させていくべきかという社会的コンセンサスをどのように取っていくべきかということについても議論されないまま本委員会の意見が代表的意見であると位置付けられることにも問題があると考えます。

従って、事業者として、この報告書の内容に同意していると受け取られることには非常に問題があると考えており、本報告書の内容はまだ充分に議論がなされていないものであって報告書の内容から一定の方針や方向性を導くことができるほど成熟したものとは言い難いものであることが明記されることが不可欠であると考えます。

●　私たちとしましては、具体的には以下のような意見を有しております。

１．セキュリティ対策については、事業者にとっても重要な問題と認識しております。しかしながら、基本的には事業者が自らの判断において取り組むべき問題であり、事業者の判断を第一に尊重すべきと考えます。

→　事業者の自主的対応ではまかなえない部分について取締りの必要性を議論すべきであります。その際、事業者に過度の負担を強いることは、事業全体の競争力を削ぐことになるものであり、適切でないと思われます。

２．我が国全体としてのセキュリティ対策、特に民間との連携を検討するに当たっては、この問題が、事業者の負担のみならずプライバシーや通信の秘密といった基本的人権に深く関わる問題である以上、慎重に検討が進められるべき問題であり、まず関係各省庁や産業界が参加した場において議論が行われるべきと考えます。

３．インターネットは全世界的な広がりを持つものであり、セキュリティ対策の点も国際的な整合性をとる必要があります。

→　サイバー犯罪条約における議論やＧ８官民合同会合における議論においても、データ保存の義務づけや民間側のコンタクトポイントの設定は採用されていません。日本

においてこのような制度を設けることを前提とした議論をすることが有益であるとは思われません。

東　貴彦

本件はすべての委員の方々および政府関係機関の方々のご認識どおり、公益（犯罪の捜査・予防をはじめとする）と個人や企業の権利・義務（プライバシー、通信の秘密、企業秘密の保護等）の境界領域に立ち入るデリケートな面があると考えます。従って第三者的にみて双方のバランスがとれた対策であること、ならびに事案ごとの柔軟な対応と明確な説明が出来る対応が求められると考えます。情報ネットワークの利用者に「警察はセキュリティについてのすべての情報をもっており、どんなセキュリティプロテクションも破ることができるらしい」と感じさせてしまうと情報通信ネットワークの健全な発展や警察に対する国民の信頼維持に影響を与える恐れがあるとも考えます。もちろん民間企業はその社会的責務として公益の尊重すなわち犯罪の捜査・予防に最大限の協力と貢献を惜しんではならないと考えますが、同時に顧客・取引先の権利・義務に対する責任も持っています。したがって民間企業としては、個別の事案に対処する場合のガイドライン、例えば裁判所の令状があればどこまで、任意の協力であればどこまでといった線引きを明確にした上で政府機関との協力と公益への貢献を図りたいと考える次第です。

吉岡　初子

昨今のインターネット等の目覚ましい進展と、普及状況から、利便性とともに多くの問題が発生していることは、利用者として危惧しているところです。

従って、安心してインターネット等の電気通信の利用ができる環境を整備することは重要であることは申すまでもありません。

しかし、プライバシーや通信の秘密等、国民にとって重要な問題について、十分な配慮が必要であり、間違っても国民の基本的人権に抵触するようなことになってはならないと考えています。

このような重要な問題について、十分な審議がされたとはいえない現段階の報告書であり、犯罪防止の立場は理解できるものの、消費者の立場を十分配慮した内容とする必要があります。

特に、犯罪に関係のない広範な人々の個人情報が取得されてしまうことについて、強い懸念を持っています。

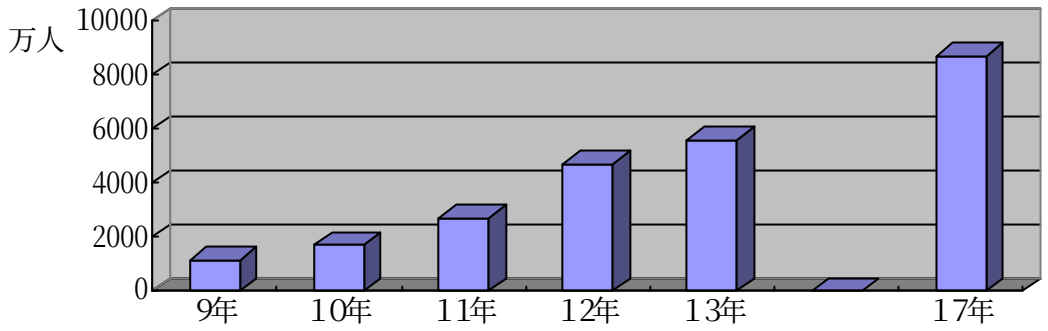
このような重要な内容の検討に３回の会議で、議論を尽くしたとはいえないと思います。また、関係省庁との連携が不可欠だと思いますので、この点についても配慮されるようにご検討下さい。

消費者団体の代表として報告書案に同意していると思われることは､立場上も問題がありますので、今回を最後にとりまとめを公表するのであれば、各委員の意見を添付されることを提案致します。

（補遺）

P.9

図２－２　国内インターネット利用者



平成１４年情報通信に関する現状報告（総務省）
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm

P.11

Ｇ８におけるハイテク犯罪対策

平成１４年(2002 年)５月にモン・トレンブラント（カナダ）で開催された司法内務閣僚会合においては、国際組織犯罪に関する４０の勧告が改定され、新たな勧告が作成された。新しい勧告では、PartIV SectionDにおいてハイテク・コンピュータ関連犯罪に言及されている。また、同会合では、ハイテク犯罪に関し、「テロ・犯罪捜査における国境を越えたネットワーク通信追跡のための勧告」、「公共の安全を保護するために不可欠なデータの利用可能性に関する原則」、「データ保全に関するチェックリスト」及び「Ｇ８データ保護制度に関する声明」の４つの文書が採択された（資料II（補遺）参照)。

P.16

取組み

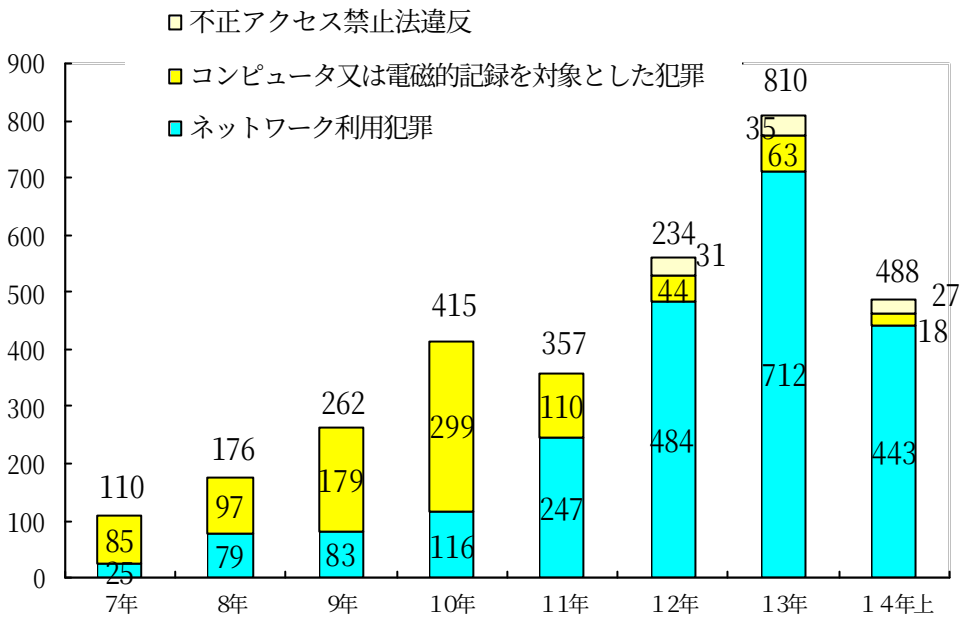
平成 14 年 4 月　「電子政府の情報セキュリティ確保のためのアクションプラン」等を踏まえ、「緊急対応支援チーム」(通称 NIRT; National Incident Response Team)を設置。

なお、平成１４年４月に、内閣官房情報セキュリティ対策推進室のホームページが開設された（http://www.bits.go.jp/index.html)。

（「緊急対応支援チーム」については、資料編II（補遺）参照。）

P.20

図５－１　ハイテク犯罪の検挙件数の推移



http://www.npa.go.jp/hightech/toukei/index.htm

P.20

図５－２　ハイテク犯罪の検挙状況

			平成14年上半期	平成13年上半期	平成13年	昨年同期との比較
コンピュータ、電磁的記録対象犯罪			１８	３３	６３	▲１５
	電子計算機使用詐欺		１２	２８	４８	▲１６
	電磁的記録不正作出・毀棄		５	２	１１	３
	電子計算機損壊等業務妨害		１	３	４	▲　２
ネットワーク利用犯罪			４４３	３１９	７１２	１２４
	児童買春・児童ポルノ法違反	児童買春	１１４	４６	１１７	６８
		児童ﾎﾟﾙﾉ	６４	５５	１２８	９
	詐欺		５９	５３	１０３	６
	わいせつ物頒布等		５５	４９	１０３	６
	青少年保護育成条例違反		２５	２	１０	２３
	脅迫		１８	２８	４０	▲１０
	著作権法違反		１６	１０	２８	６
	名誉毀損		１３	１８	４２	▲　５
	その他		７９	５８	１４１	２１
不正アクセス禁止法違反			２７	１３	３５	１４
合　　計			４８８	３６５	８１０	１２３

＊　その他には、銃砲刀剣類所持等取締法違反、覚せい剤取締法違反等の薬物事犯、売春防止法違反、児童福祉法違反等がある。

http://www.npa.go.jp/hightech/toukei/index.htm

P.21

図５－３　ハイテク犯罪等に関する相談受理件数

	平成 14 年上半期	平成 13 年		昨年同期との比較
		上半期		
インターネット・オークションに関する相談	1,495	1,360	2,099	135
詐欺・悪質商法に関する相談（ｲﾝﾀｰﾈｯﾄ・ｵｰｸｼｮﾝ関係を除く）	1,331	898	1,963	433
名誉毀損・誹謗中傷等に関する相談	1,229	1,081	2,267	148
迷惑メールに関する相談	1,180	1,193	2,647	▲ 13
違法・有害情報に関する相談	1,176	2,012	3,282	▲ 836
不正アクセス、コンピュータウイルスに関する相談	693	568	1,335	125
その他	1,988	1,850	3,684	138
合　　計	9,092	8,962	17,277	130

http://www.npa.go.jp/hightech/toukei/index.htm

P.23

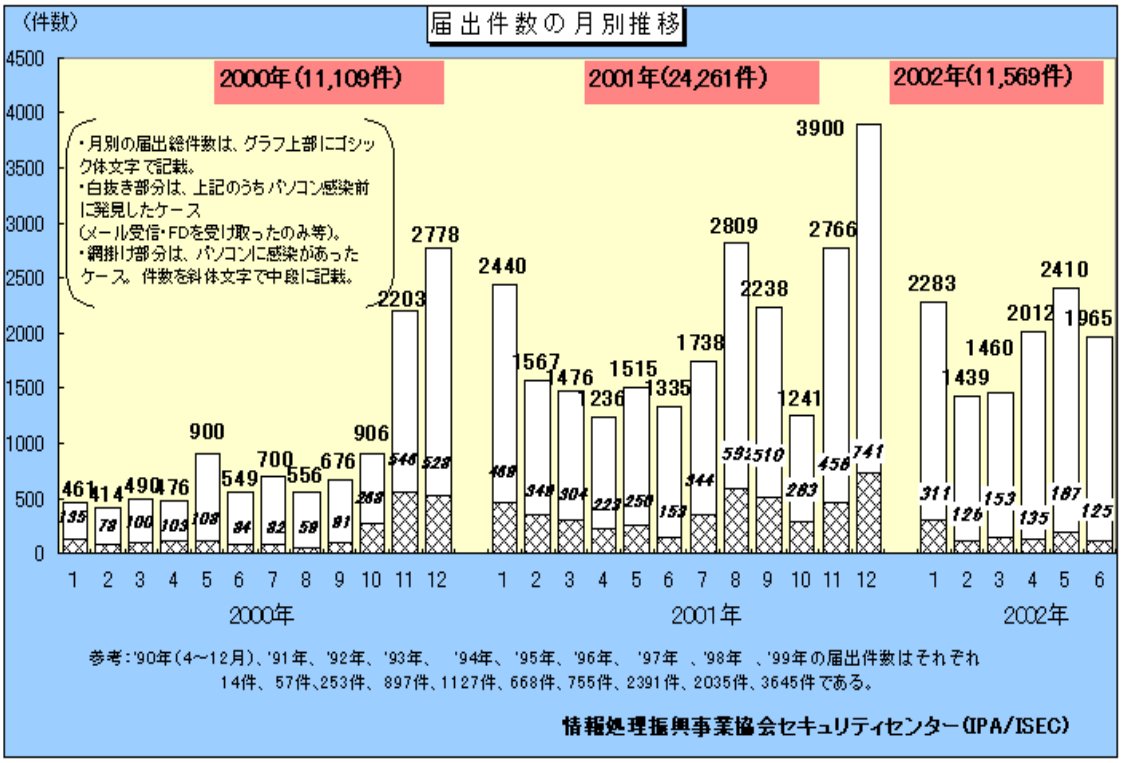
図５－４　不正アクセス行為の発生状況（警察）

	平成 14 年上半期	平成 13 年		平成 12 年	
		通年	上半期	通年	法施行後半年（注）
認　知　件　数	94	1,253	959	106	35
海外からのアクセス	4	448	418	25	14
国内からのアクセス	71	258	165	73	20
アクセス元不明	19	547	376	8	1

http://www.npa.go.jp/hightech/toukei/index.htm

P.24

図５－６　コンピュータウイルス届出件数（ＩＰＡ）



http://www.ipa.go.jp/security/outline/todokede-j.html

P．29

図５－７　いわゆる出会い系サイトに関係した事件の検挙数

		平成14年上半期	平成13年 上半期	平成13年	昨年同期との比較
重要犯罪	殺　人	1	5	6	▲ 4
	強　盗	6	2	１０	4
	強　姦	２３	２０	４４	3
	略取誘拐	1	1	3	0
	強制わいせつ	3	7	１０	▲ 4
暴　行		1	2	3	▲ 1
傷　害		１１	5	１３	6
脅　迫		１３	8	１６	5
恐　喝		３３	8	３４	２５
窃　盗		１３	１４	２３	▲ 1
詐　欺		１３	8	２６	5
児童買春・児童ポルノ法違反	児童買春	４００	１３３	３７９	２６７
	児童ﾎﾟﾙﾉ	１０	0	8	１０
青少年保護育成条例違反		２１３	５９	２２１	１５４
その他		５２	３０	９２	２２
合　計		７９３	３０２	８８８	４９１

＊　対象は、インターネット上で異性間の出会いの場を提供する電子掲示板、チャット等のいわゆる出会い系サイトが関係した事件として警察庁に報告のあったもの。

	被害者数	うち未成年者	うち女性
平成12年	１０２	７１(69.6%)	９６(94.1%)
平成13年	７５７	５９８(79.0%)	６９９(92.3%)
上半期	２８３	２１８(77.0%)	２６５(93.6%)
平成14年上半期	６９２	６１０(88.2%)	６４７(93.5%)

＊　（　）は被害者数に対する構成比

http://www.npa.go.jp/hightech/toukei/index.htm

P.34

不正アクセス行為の再発防止のための援助

平成１４年上半期の援助の実施件数は、４件。

http://www.npa.go.jp/hightech/toukei/index.htm

被害の未然防止・被害拡大防止他のための情報提供

平成１４年中の情報提供は次のとおり。

- **個人情報の流出事案に関する対策について（６月）**
- **Web サーバ用プログラム「Apache」のセキュリティホールに関する対策について（６月）**

http://www.npa.go.jp/hightech/sisin/index.htm