官民における情報セキュリティ関連情報の共有の在り方について

平成１５年度総合セキュリティ対策会議　報告書

総合セキュリティ対策会議

はじめに

近年目覚ましい発展を遂げている情報通信ネットワークは、私たちの生活の利便性を向上させるにとどまらず、社会・経済活動の根幹を支える重大なシステムとして機能するに至っている。その一方で、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。

「総合セキュリティ対策会議」は、情報セキュリティに関する産業界等と政府機関との連携の在り方、特に警察との連携の在り方について検討を行うことを目的として平成１３年度に設置されたものである。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、消費者団体の方々という広い分野の有識者により、幅の広い議論が活発に行われており、平成１３年度に報告書「情報セキュリティ対策における連携の推進について」、昨年、平成１４年度は報告書「情報セキュリティに関する脅威の実態把握・分析について」をそれぞれ取りまとめた。

本年度は、「官民における情報セキュリティ関連情報の共有の在り方」というテーマを選び、情報共有に関する現状の課題を明らかにするとともに、具体的な事例を通じた官民の情報共有の在り方について話し合い、官民の情報共有のスキームを提示することを試みた。本報告書は、本会議での成果をまとめたものである。

なお、各委員には、それぞれが有する個人的な知見に基づいて、個人の立場において自由に議論に参加していただいたのであり、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。

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１６年３月

総合セキュリティ対策会議委員長

前田　雅英

総合セキュリティ対策会議委員名簿

前田雅英 （委員長）	東京都立大学 教授
伊藤穰一	（株）ネオテニー 代表取締役社長
稲垣隆一	弁護士
小田啓二	特定非営利活動法人　日本ガーディアン・エンジェルス 理事長
小野田誓	（社）日本PTA全国協議会 常務理事
加藤雄一	ニフティ（株） 常務取締役システム事業部長
桑子博行	（社）テレコムサービス協会　サービス倫理委員会　委員長 （AT＆Tグローバル・サービス（株）通信渉外部長）
国分明男	（財）インターネット協会 副理事長
佐々木良一	東京電機大学 教授
下道高志	サン・マイクロシステムズ（株）　システム技術統括本部 オープン・システム・センター　ITアーキテクト
杉浦昌	日本電気（株）NEC システムソフトウエア事業本部 IT基盤システム開発事業部　セキュリティ技術センター コンサルティングマネジャー

田尾陽一	セコムトラストネット（株） 会長
高山健	楽天（株） 常務取締役
冨谷真一	ソニー（株） ITC VCL 企画管理課 統括課長
東貴彦	マイクロソフト（株） 取締役経営戦略担当
別所直哉	ヤフー（株） 法務部部長
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 会長
吉川誠司	WEB110 代表

（特別参加）

渡邊幸治	国家公安委員会委員

（敬称略・50音順）

（オブザーバー）

内閣官房（情報セキュリティ対策推進室）
総務省
法務省
外務省
経済産業省

事務局：警察庁生活安全局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（参考資料）

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引き続き増加傾向にある。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、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、平成13年度には報告書「情報セキュリティ対策における連携の推進について」を作成し、情報セキュリティに関する産業界等と政府機関の連携の在り方、特に警察との連携の在り方に関する全体像を提示した。また、平成14年度には報告書「情報セキュリティに関する脅威の実態把握・分析について」をとりまとめ、アンケート調査等を通じ、官民が連携して情報セキュリティ対策を講じる上で参考となるであろう脅威の実態について分析を行った。

本年度（平成15年度）の会議においては、情報セキュリティ上の脅威を克服するためには、官民でどのような連携をとるべきか、という視点から引き続き情報セキュリティ上の脅威を把握するための調査結果について検討するとともに、「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」というテーマを選び、具体的な事例を通じた官民の情報共有のスキームについて検討を行った。

なお、ネットワーク・セキュリティをめぐる状況の変化は急速であり、アンケート調査で明らかとなった実態はあくまでも平成 15 年秋時点のものであることを付言する。

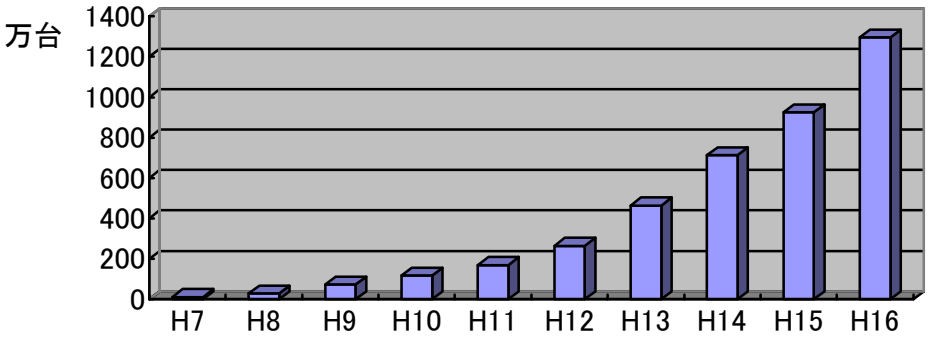
第２章　産業界等と政府との連携の重要性

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 16 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 1,296 万台であり、その数は、近年急激に増加している。

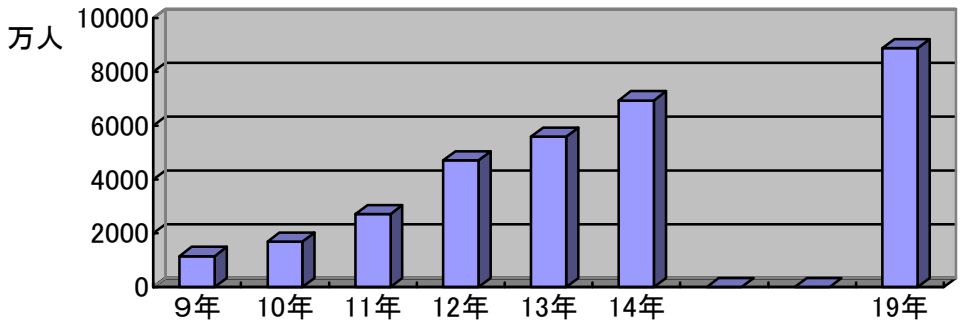
インターネットに接続されている国内コンピュータ数



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

また、国内のインターネット利用者は、平成 14 年末において約 6,942 万人（人口普及率 54.5%）であり、平成 19 年には 8,892 万人に増加するものと見込まれている。

国内インターネット利用者



平成 15 年情報通信白書（総務省）

2. 情報セキュリティに関する脅威の増大

このようなネットワーク利用の急増に対応し、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、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引き続き増加傾向にある。

3. 産業界等と政府との連携

このような状況にあって、ネットワークの安全性及び信頼性を確保し、ネットワークを安心して利用することができるようにするためには、ネットワークにおける情報セキュリティを向上させることが喫緊の課題となっている。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　産業界等における情報セキュリティに関する被害と対策の実態

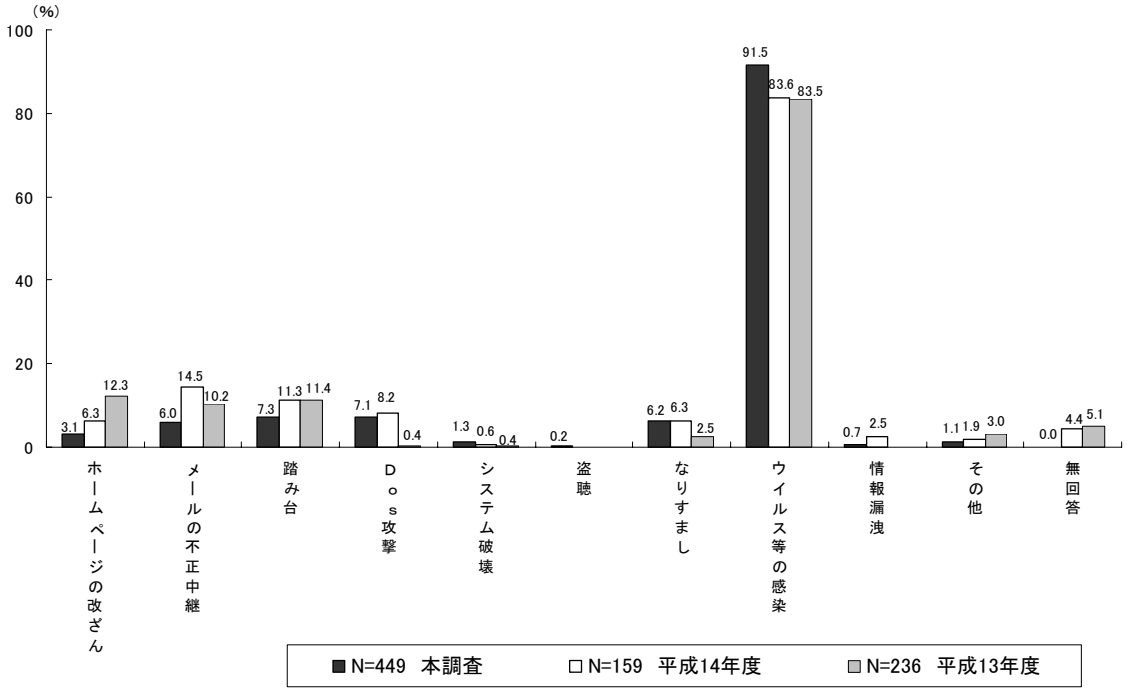
昨年度は、「情報セキュリティに関する脅威の実態把握・分析」をテーマに検討を行ったが、情報セキュリティにかかる状況の変遷は急激であり、経年変化を比較する必要があることから、本年度も警察庁が実施した「不正アクセス行為対策等の実態調査」（以下、「アンケート調査」という。）を参考に、不正アクセス行為等の情報セキュリティに関する被害の状況や情報セキュリティ対策の実態について検討を行った。

なお、アンケート調査は、平成 15 年９月から 10 月にかけて、全国の企業、情報通信関連、医療関連、教育関連、行政サービス機関から偏りのないよう抽出した 2,000 団体に送付し、そのうち回答のあった 732 団体についてまとめたものである。

1．被害状況

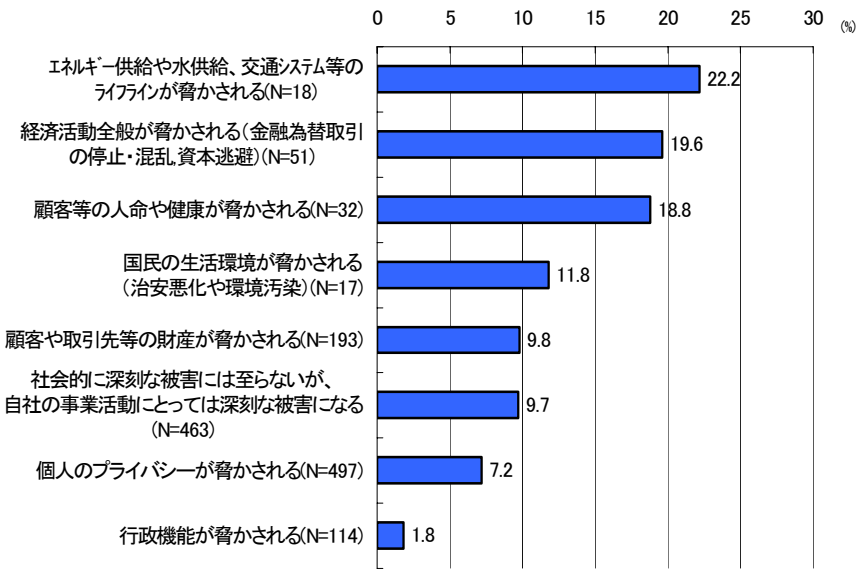
この１年間に何らかの被害にあった団体は、61.4%に上っており、特に被害がなかった団体は 37.4%であった。被害にあった団体のうち、コンピュータウイルス感染が 91.5%と最も多く、年々増加しており、依然としてウイルスの猛威は衰えていない。

過去１年間の情報セキュリティに関する被害状況（被害にあった団体の被害内容）



有している情報システムの特徴別に被害の発生率を見ると、攻撃を受けた時に、顧客等の人命・健康や経済活動全般、ライフラインに大きな影響が及ぶような重要な情報システムを保有している団体では、情報セキュリティに関する被害の発生率が 20%前後と、他の団体と比べて相対的に高く、攻撃の対象になりやすくなっているのが現状である。

情報セキュリティに関する被害の発生率（情報システムの特徴別）



2．被害金額

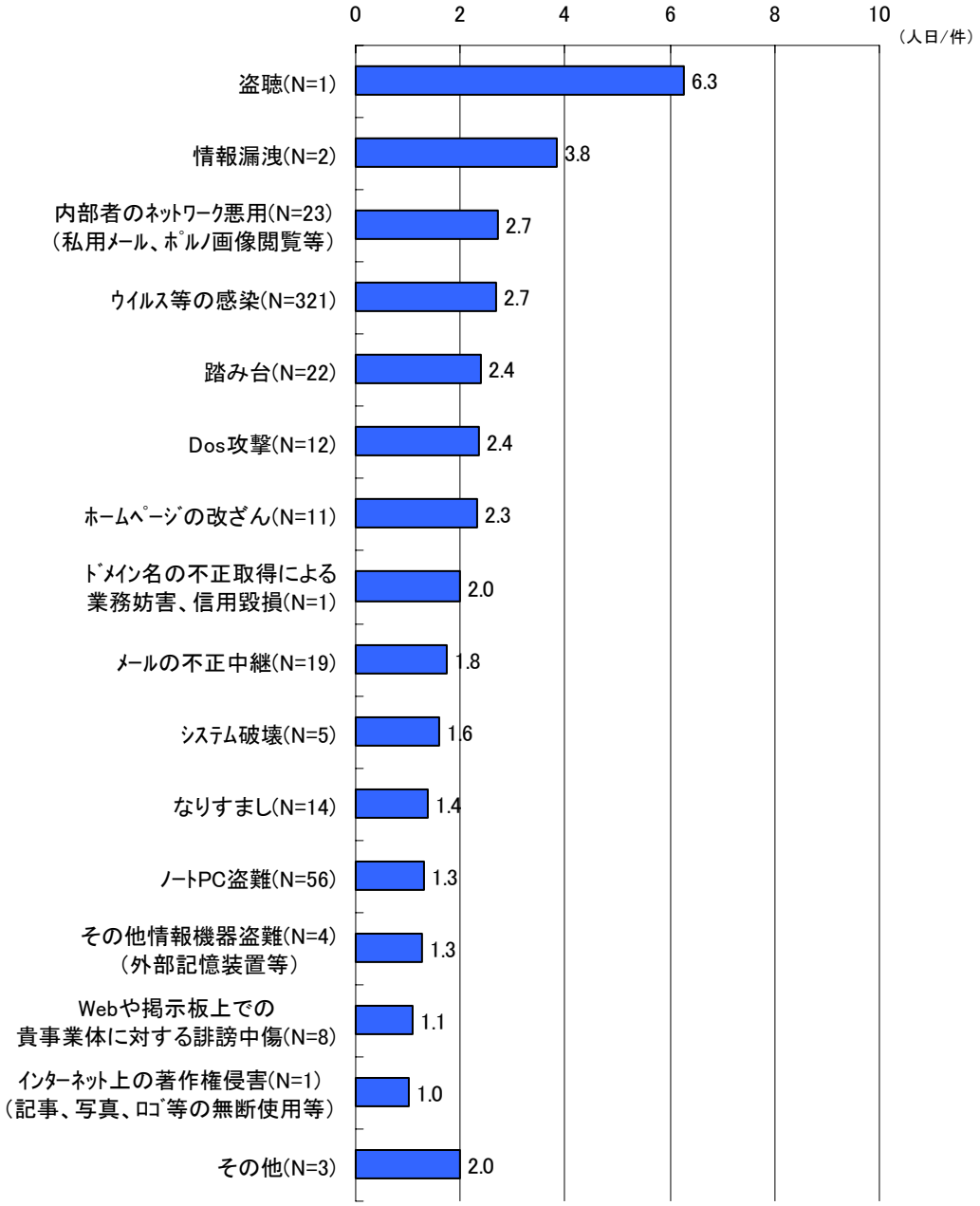
アンケート調査では、被害を受けた場合の「復旧処理に要した組織内の職員の稼働人日（注１）」「復旧コスト（注２）」について調査した。

復旧処理に要した平均稼働人日については、「内部者のネットワーク悪用」や「ウイルス等の感染」の値が大きい。また、回答数が少ないものの、「盗聴」や「情報漏洩」の値も大きくなっている。

注１：　組織内以外からの応援人員や外注先からの派遣人員等の稼働人日は除く。

注２：　システム・データ復旧にかかる外注費、ハードウェア・ソフトウェアの買い替え等の復旧にかかった費用。復旧処理にかかった内部の人件費は除く。

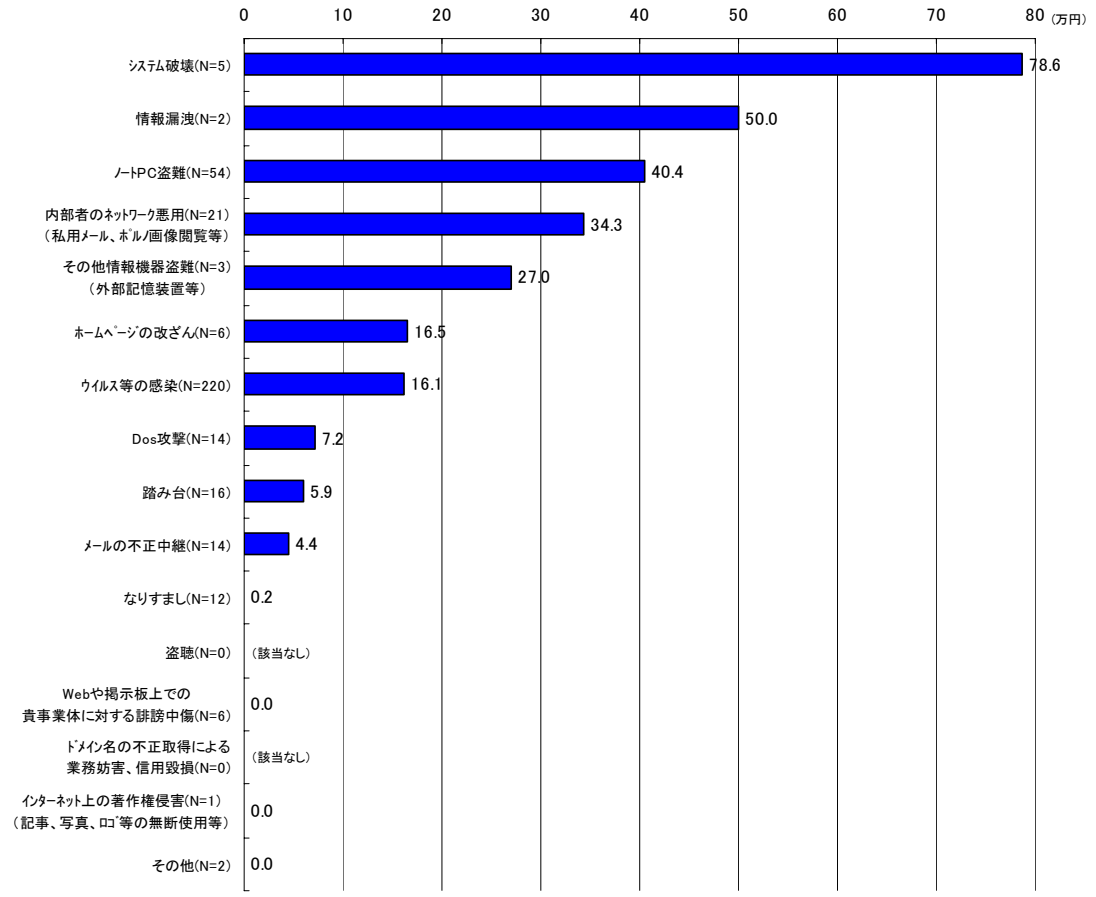
復旧処理に要した組織内の職員の平均稼働人日（被害件数１件あたり）



平均復旧コストは、「ノート PC 盗難」や「内部者のネットワーク悪用」の値が大きく、また回答数が少ないものの、「システム破壊」や「情報漏洩」の値も大きくなっている。

復旧コストの最大額については、「ウイルス等の感染」による被害が発生した団体で 694 万円に上った。

平均復旧コスト（人件費を除く）



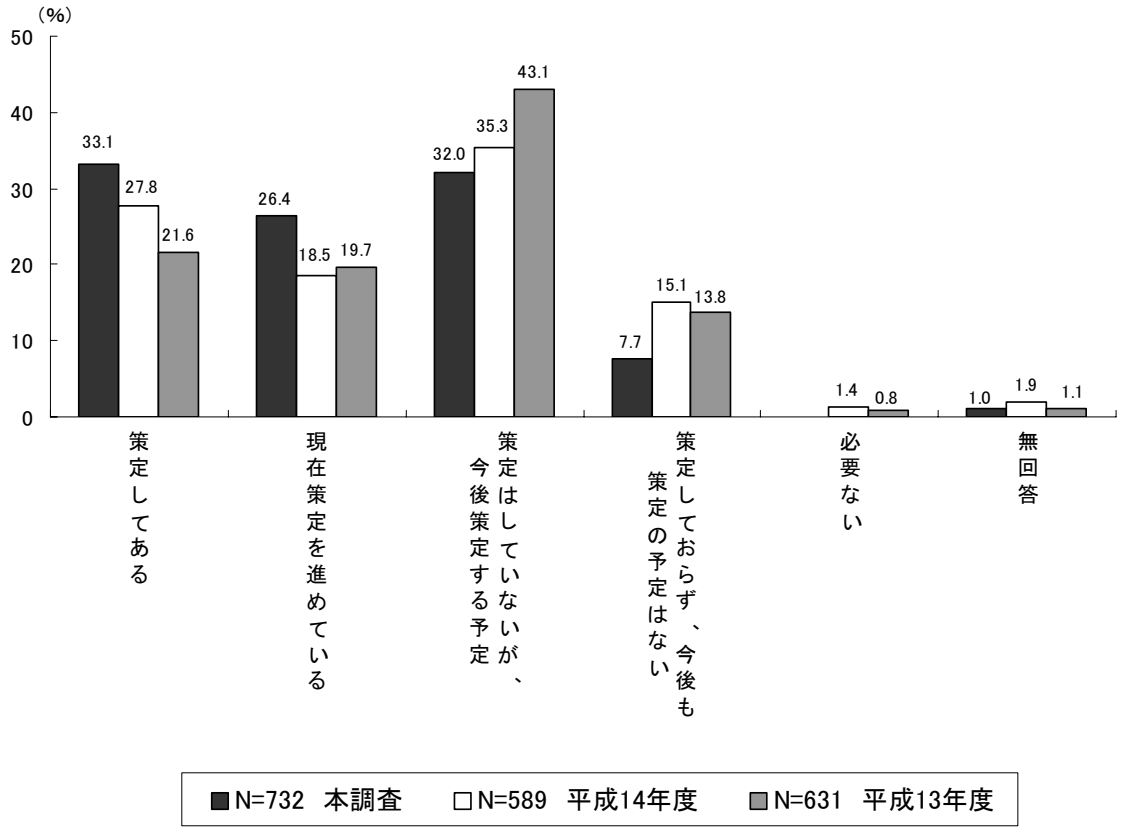
3. 情報セキュリティ対策の現状

アンケート調査の結果によると、情報セキュリティ対策の現状は以下のようなものである。

(1) 情報セキュリティポリシーの策定状況

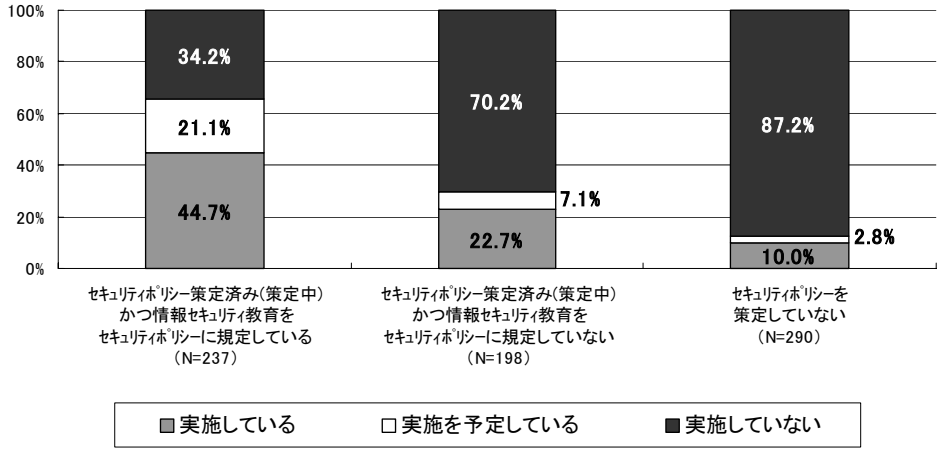
セキュリティポリシー策定の動きは加速化しており、策定済と策定中を合わせた割合は、昨年度調査の 46.3%から 59.5%となり、13.2%増加した。策定済の割合も、昨年度の 27.8%から 33.1%に増加したが、依然として普及率が高いとは言えない。

セキュリティポリシーの策定状況



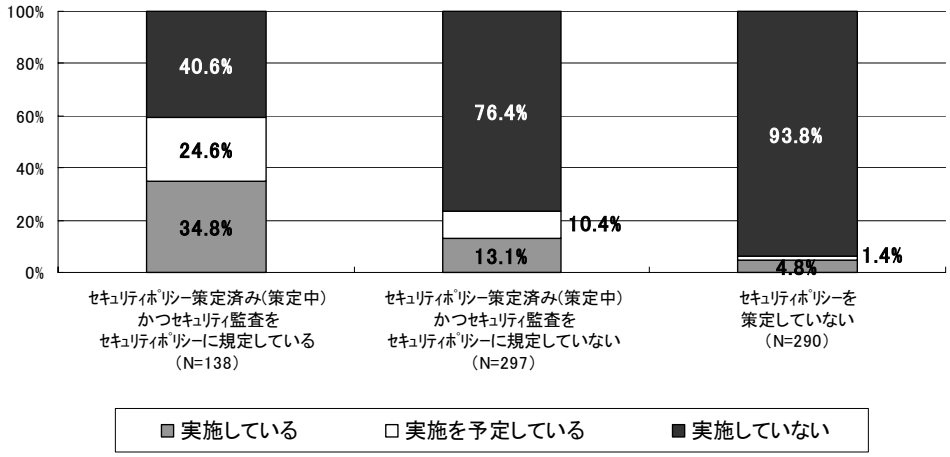
一方、セキュリティポリシー規定事項の実践状況を見ると、セキュリティポリシーに情報セキュリティ教育を規定している団体のうち、34.2%は実際にはセキュリティ教育を実施していないことが分かった。

情報セキュリティ教育の実践状況



また、セキュリティポリシーにセキュリティ監査を規定している団体のうち、40.6%は実際にはセキュリティ監査を実施していないことも分かった。

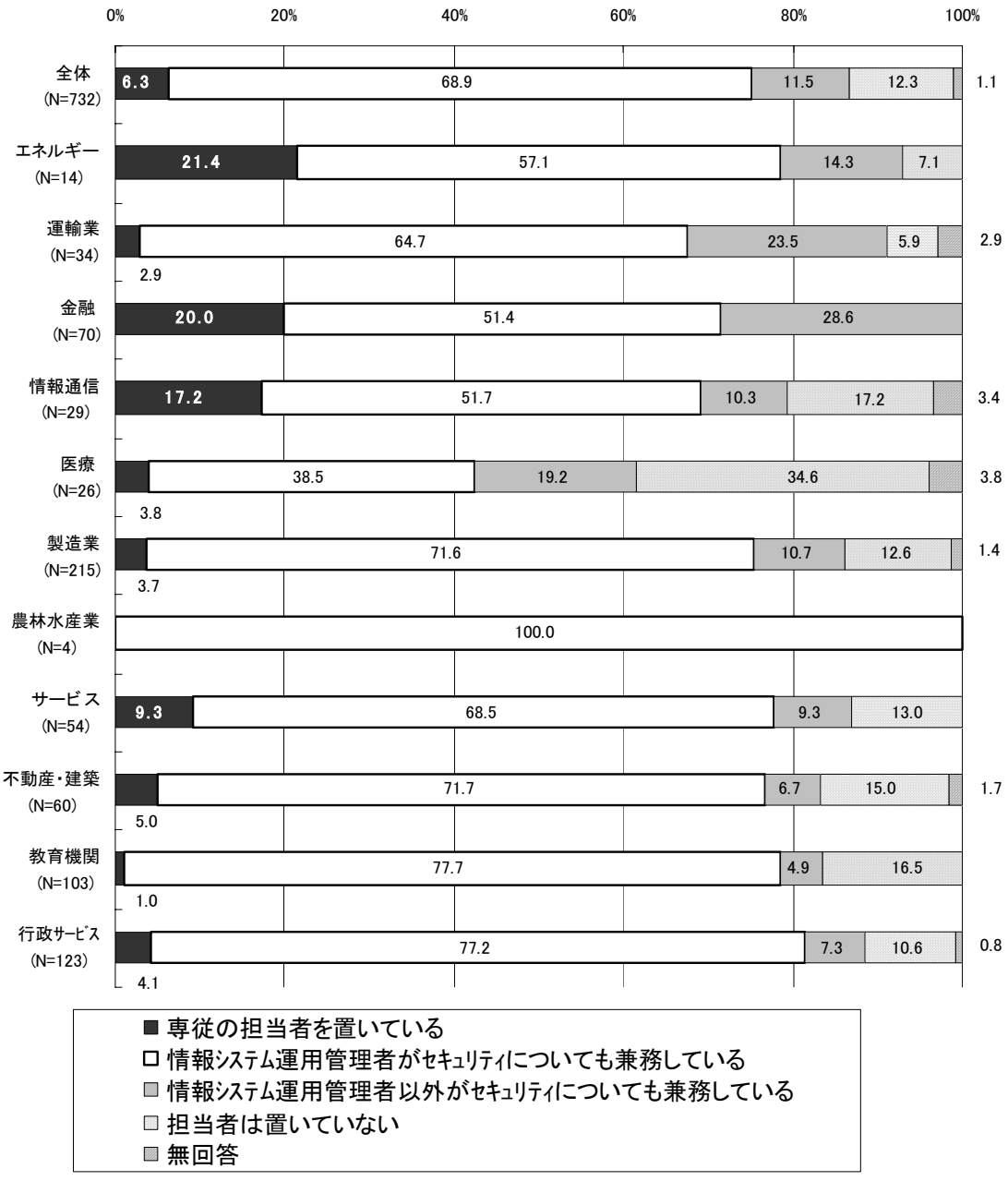
セキュリティ監査の実践状況



(2)　情報セキュリティ担当者の設置状況

専従の情報セキュリティ担当者を設置している団体は 6.3%と少数であり、情報システム運用管理者がセキュリティについても兼務している団体が 68.9%である。業種別では、専従の情報セキュリティ担当者を設置している割合が高いのが、エネルギー、金融、情報通信の業種であり、割合が低いのは教育機関、製造業、医療等である。

情報セキュリティ担当者の設置状況



(3)　情報セキュリティ対策投資

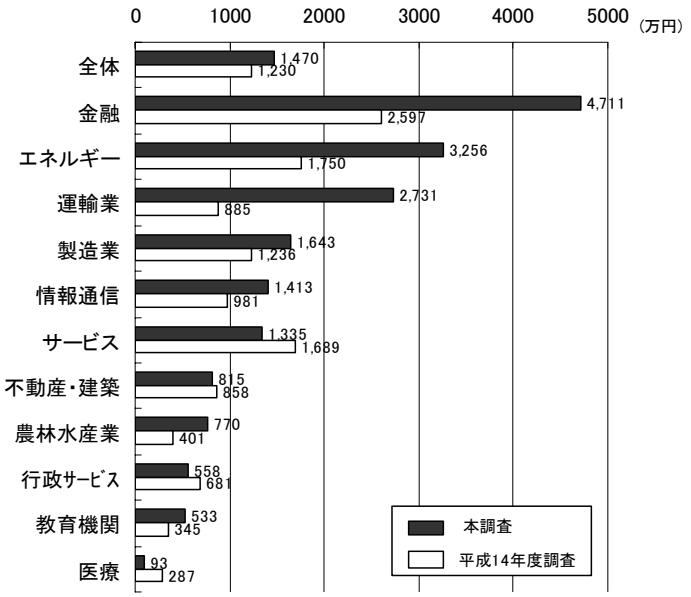
情報セキュリティ対策にかかる投資は、増加しており、ハード・ソフトにかかる情報セキュリティ対策の平均投資額は、昨年度調査に比べて約 240 万円増加し、１社あたり 1,470 万円に達した。

また、保守・メンテナンスにかかる情報セキュリティ対策の投資平均額は、昨年度調査に比べて約 239 万円増加し、862 万円となった。

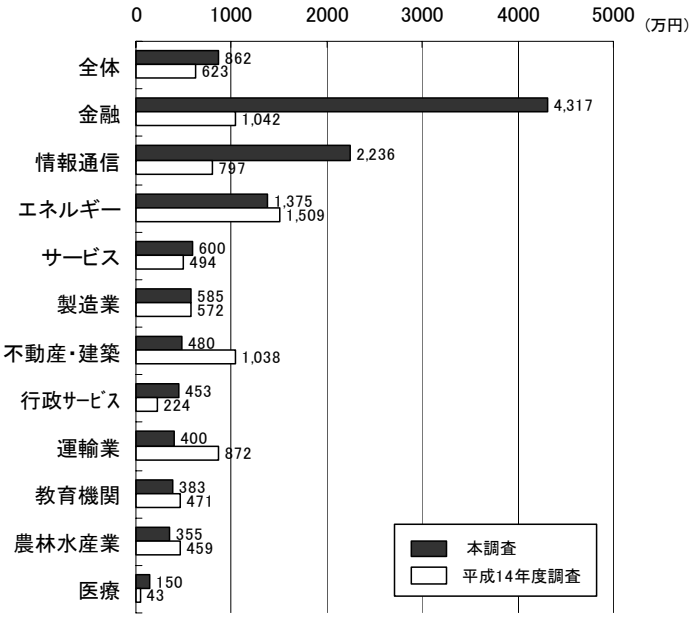
なお、アンケート調査の対象団体の予算規模は、グラフのとおりである。

業種別では、ハード・ソフトへの投資額が高いのは、金融、エネルギー、運輸業であり、保守・メンテナンスへの投資額が高いのは、金融、情報通信である。投資額が低いのは、いずれも医療である。

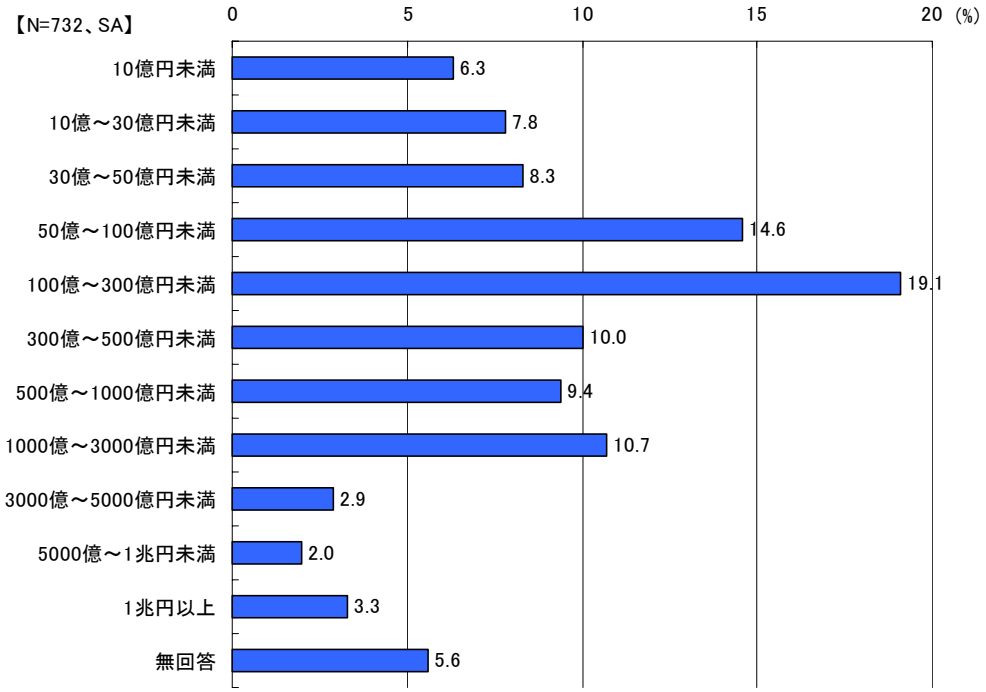
ハード・ソフトにかかる情報セキュリティ対策費用



保守・メンテナンスにかかる情報セキュリティ対策費用



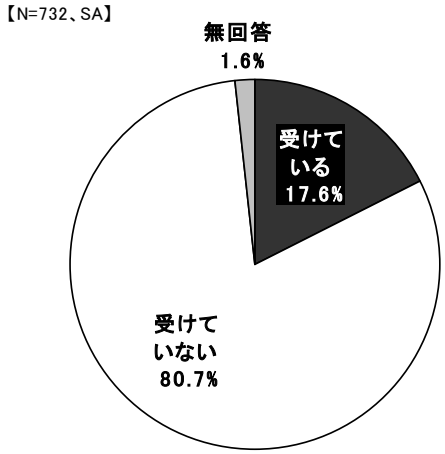
回答団体の年間売上高又は予算規模



(4)　脆弱性検査の実施状況

脆弱性検査（ペネトレーションテスト）を受けている団体は、全体の 17.6%である。

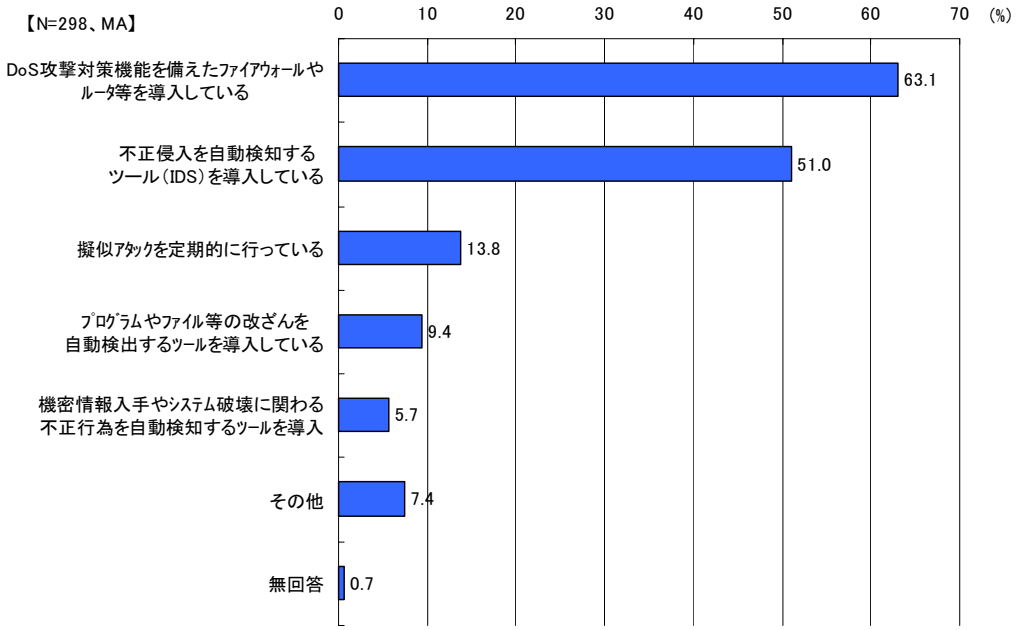
脆弱性検査の実施の有無



(5)　不正アクセス対策

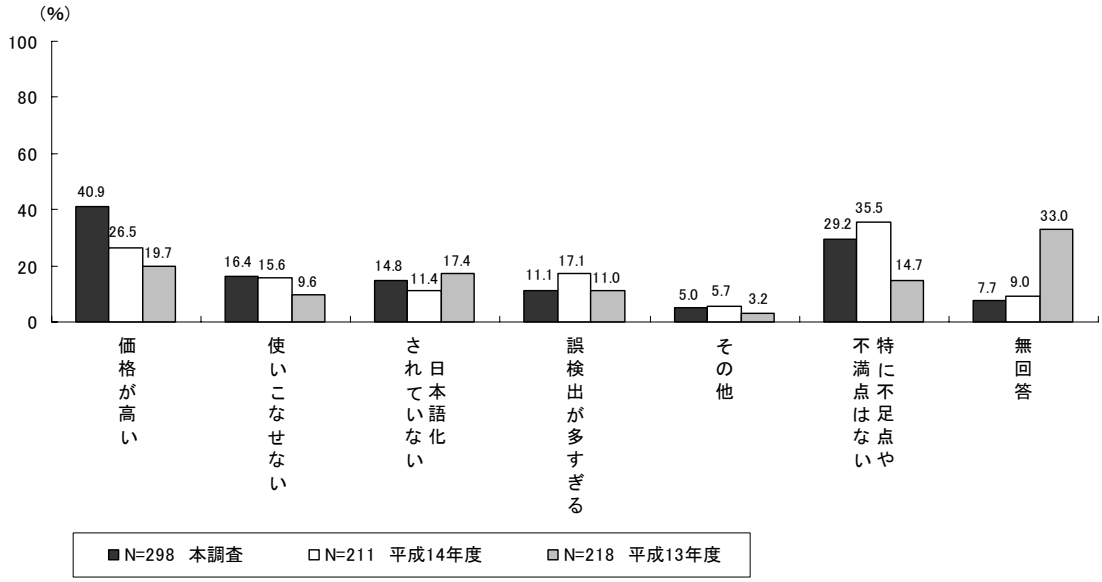
不正アクセス対策として、ファイアウォールやルータ等の導入は 63.1%、侵入検知システム（IDS）の導入は 51.0%で実施されている。

不正アクセス等の検知対策状況



提供されている機能に対しては、価格が高いという不満が、最も多く、昨年度調査と比較しても増加している。

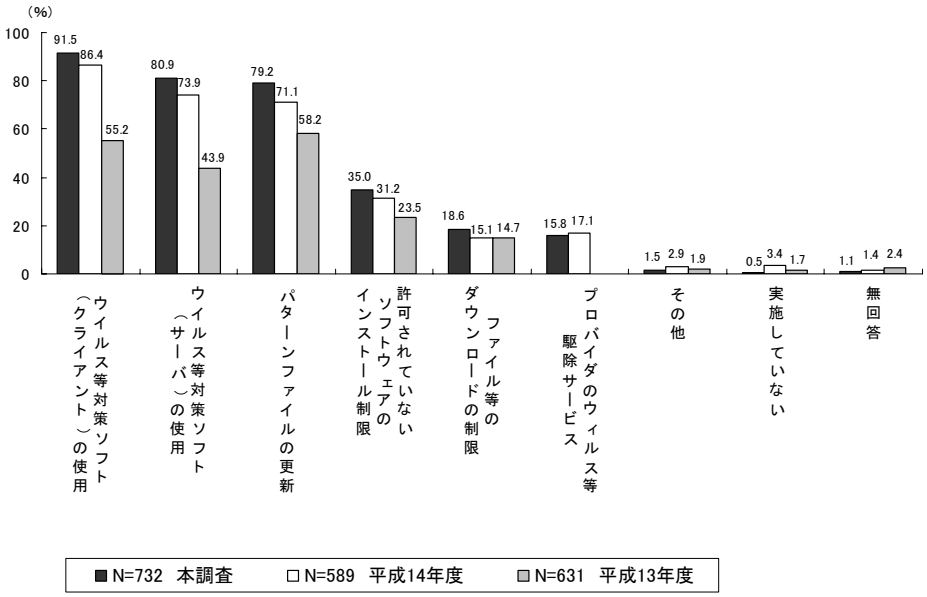
提供されている機能に対する不足・不満点



(6)　ウイルス感染防止対策

全体の 91.5%で、クライアント端末にウイルス対策ソフトを使用している。全体的に、ウイルス感染防止対策の取組みは昨年度より進んだといえる。

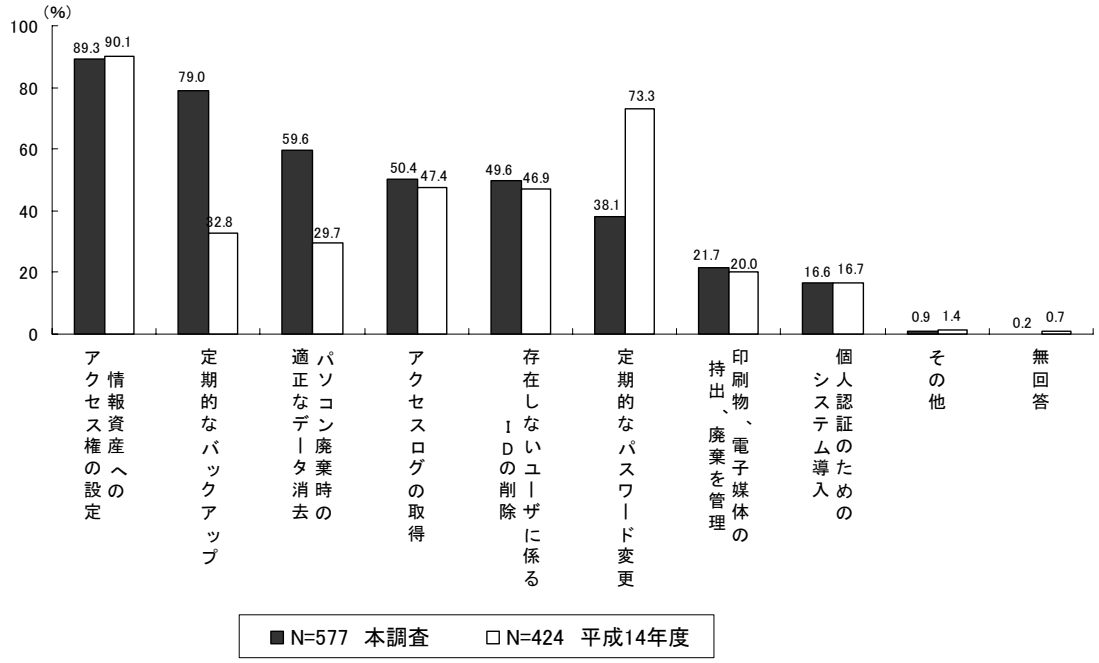
ウイルス・ワーム等の不正プログラムに対する対策の取組み状況



(7)　内部からの情報漏洩防止対策

実施されている割合が高い対策は、情報資産へのアクセス権の設定が 89.3%等であった。昨年度調査と比べると、定期的なバックアップやパソコン廃棄時の適正なデータ消去が倍増し、定期的なパスワード変更が半減した。

内部からの情報防止対策の実施状況

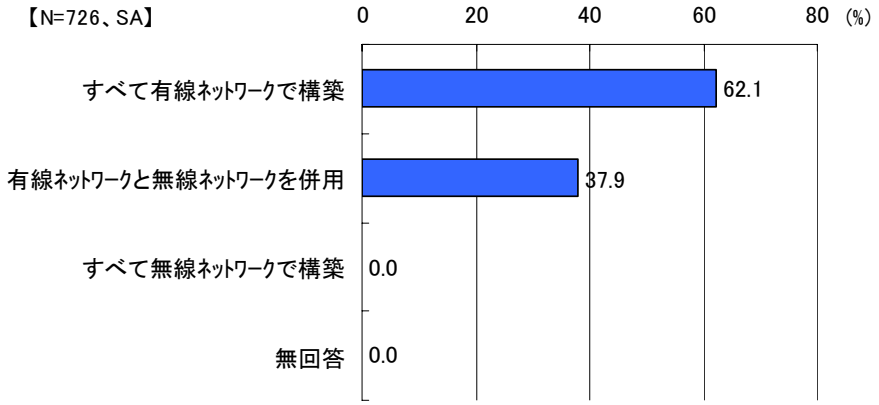


(8)　無線 LAN

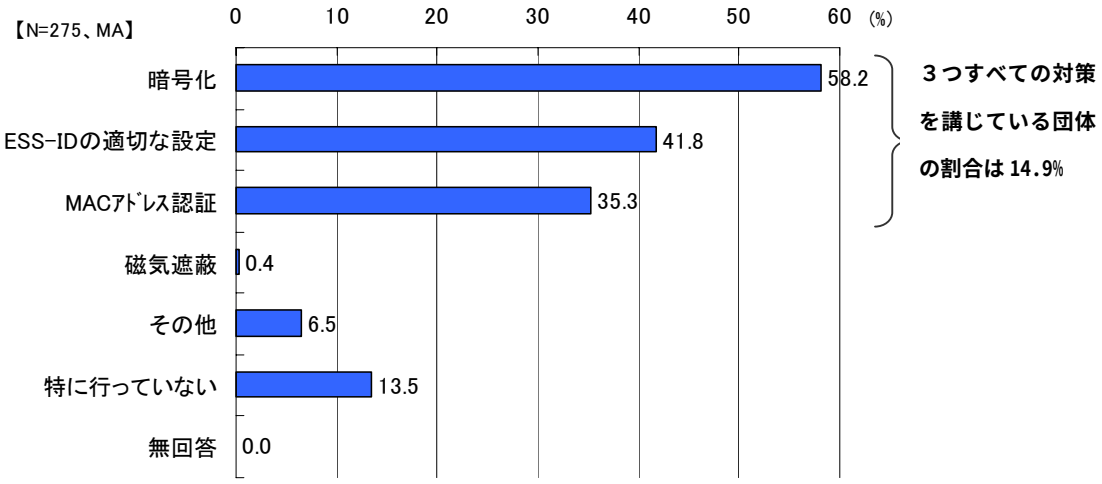
無線 LAN は、37.9%の団体で利用されており、昨年度調査より 11.8%増加し、普及が進んでいる。しかし、ESS-ID、暗号化、MAC アドレス全てを利用したセキュリティ対策を実施している団体は、14.9%と、昨年度調査の 15.0%とほとんど変わっていない。

通信媒体の性格上、無線 LAN のセキュリティには特に注意を払い、ユーザ認証等、あらゆる対策を講じ、高いセキュリティレベルを確保する必要がある。

組織内の LAN の種類



無線 LAN のセキュリティ対策

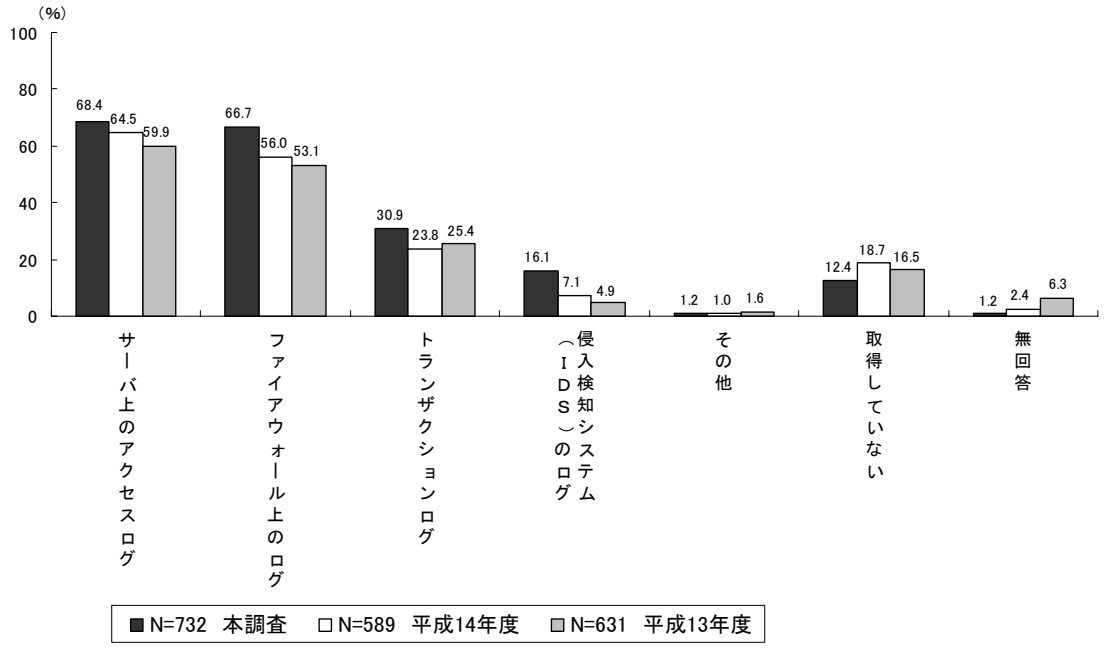


(9)　アクセスログ

サーバ上のアクセスログは 68.4%、ファイアウォール上のログは 66.7%の団体が取得している。取得していないと回答したのは、12.4%にとどまり、全体的にアクセスログを取得している団体の割合は増加している。サーバ上のアクセスログはもとより、ファイアウォール上のログやトランザクションログ、侵入検知システム（IDS）のログなど多様なログについて、取得する傾向が強くなっている。

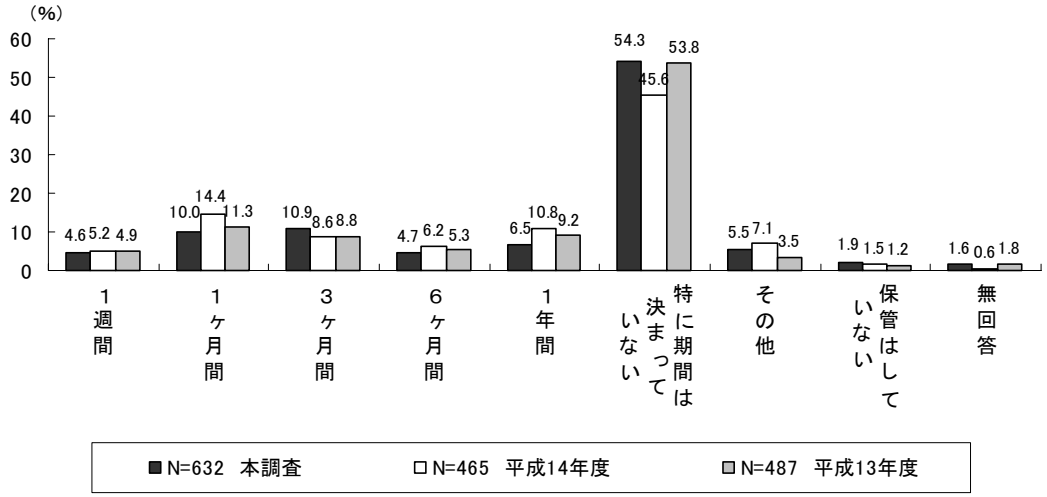
その要因としては、不正アクセスなど何らかのセキュリティ侵害が発生した際の原因の特定や解析に加え、セキュリティ侵害を受けた証拠としての活用などログが果たすべき役割が広がりつつあることが考えられる。

アクセスログの取得状況



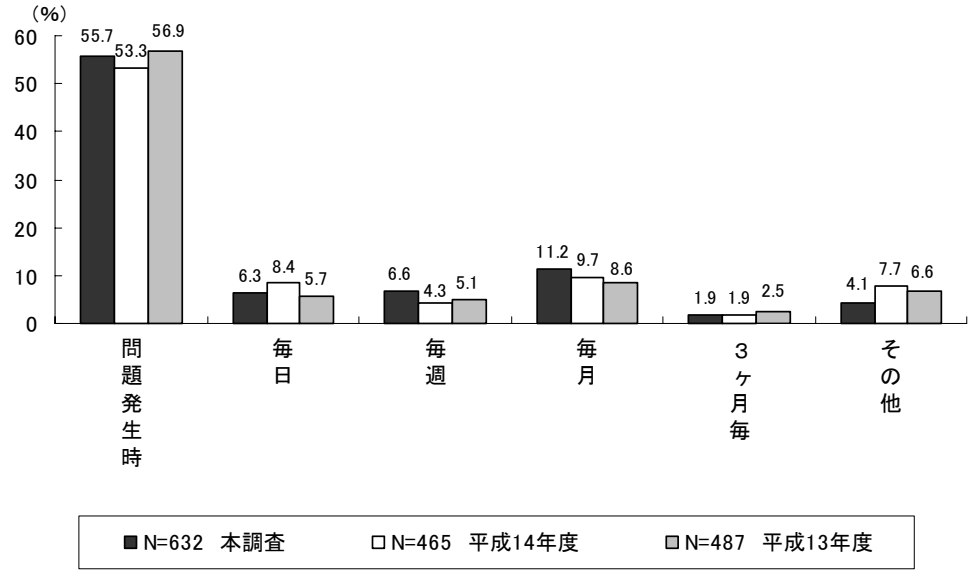
セキュリティ侵害を受けた証拠として活用するためには、ログ保存期間が重要であるが、アクセスログを取得している団体のうち、保管はしていないとの回答はほとんどなく、保管期間については、特に期間は決まっていないという団体が 54.3%であった。

ログの保管期間



ログの解析については、定期的に実施している団体が 26.0%、問題が発生した時だけ実施してしている団体が 55.7%であった。

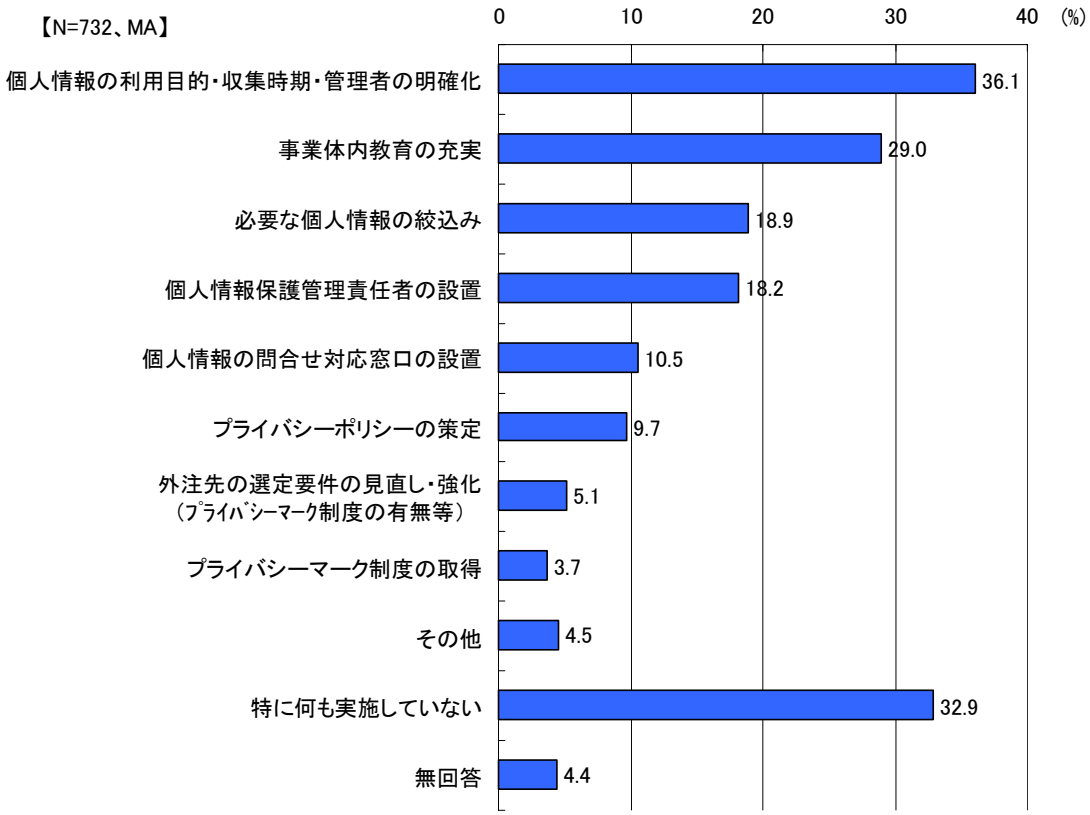
ログ解析の頻度



(10) 個人情報保護対策

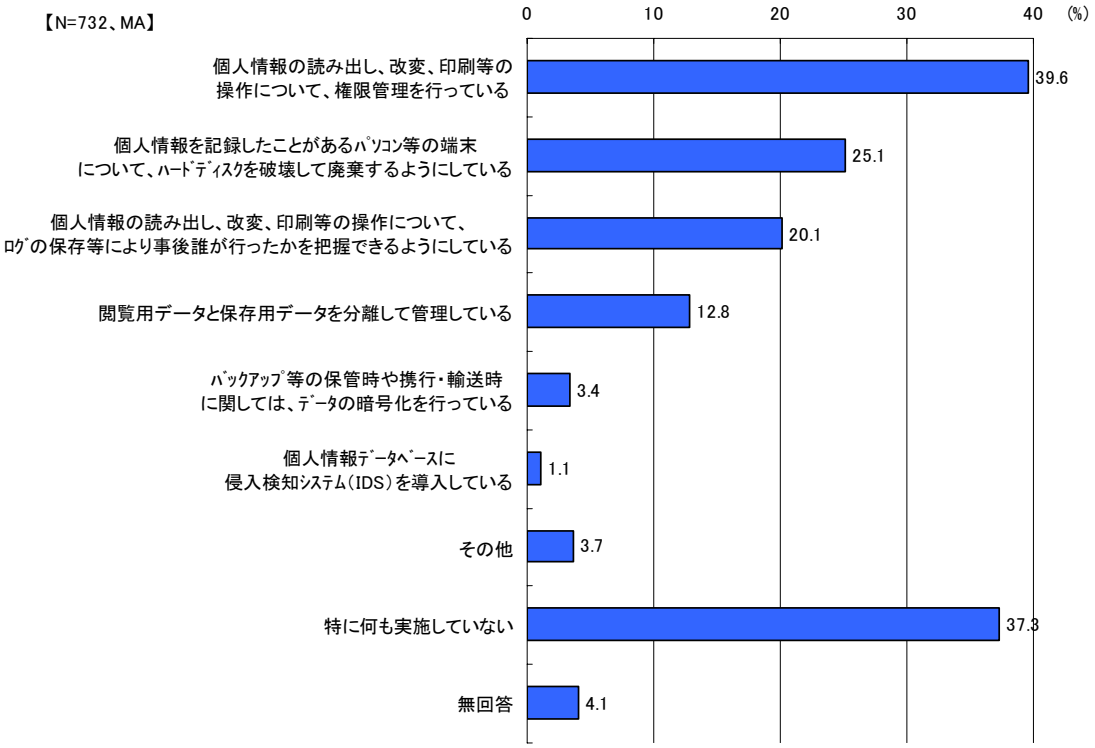
個人情報保護に対する組織・制度面の対策としては、個人情報の利用目的・収集時期・管理者の明確化を実施している割合が高い。

個人情報保護に対する組織・制度面の対策



また、個人情報保護に対するシステム・技術面の対策としては、個人情報の読み出し・改変・印刷等の操作について権限管理を行っている割合が高い。

個人情報保護に対するシステム・技術面の対策

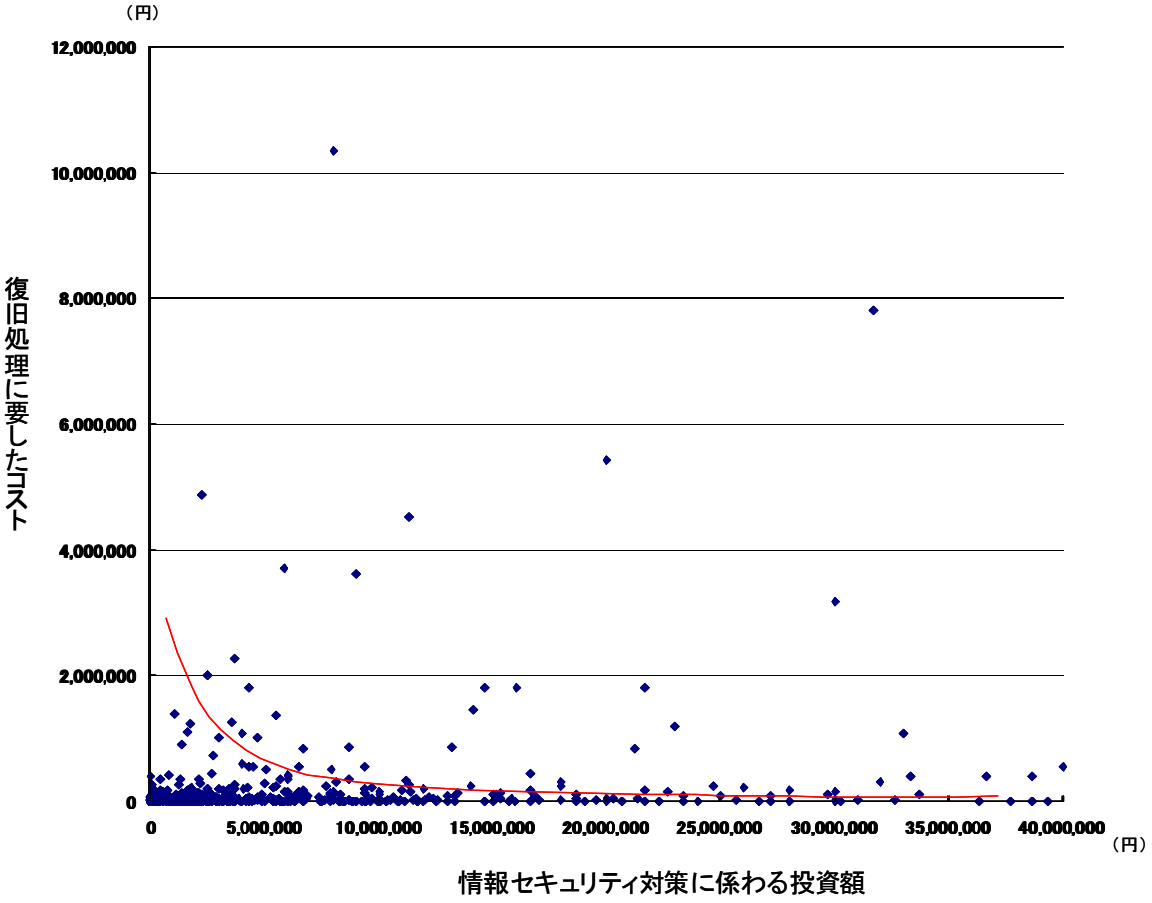


一方で、特に何も実施していないと回答した団体も、組織・制度面では 32.9%、システム・技術面では 37.3%存在する。

4．情報セキュリティ対策にかかる費用対効果

情報セキュリティ対策にかかる投資額と被害発生時の復旧処理に要したコストとの相関についてみると、復旧処理コストの比較的大きいものは、投資額の比較的小さい領域に集中している。これは、情報セキュリティ対策にかかる投資額の大きさが、被害の発生や拡大の抑制に寄与することを表しており、情報セキュリティ対策は、投資額に見合う一定のセキュリティ効果を上げている。

情報セキュリティ対策にかかる投資額と復旧処理に要したコストとの相関



※情報セキュリティ対策に係わる投資額について

「情報セキュリティ対策に係わる投資額」は、本調査で実施したアンケート調査により得られた、ア）セキュリティ対策に係わるハードウェア、ソフトウェアを合わせた費用（アンケート調査では、過去３年間の支出額について質問しているが、１年分に均等按分して用いている）、イ）保守、メンテナンス等にかかる費用（年額）、ウ）セキュリティサービス業者への外注費（年額）の３つを合計した金額を用いている。

※復旧処理に要したコストについて

被害発生時の復旧処理に要したコストは、過去１年間に生じたホームページの改ざん、メールの不正中継、踏み台、DoS 攻撃、システム破壊、盗聴、なりすまし、ウイルス等の感染及び情報漏洩に係わるものを対象としている。

復旧処理に要したコストには、組織内の職員の復旧処理に伴う人件費、復旧処理に要した外注費、代替ハードウェア・ソフトウェアの購入費、訴訟(準備)費用などが含まれる。

組織内の職員の復旧処理に伴う人件費については、本調査で実施したアンケート調査により得られた、復旧処理に要した組織内の職員の稼働人日に業種ごとの人件費単価を掛け合わせることにより算定している。

業種ごとの人件費単価については、国税庁の民間給与実態統計調査（平成 14 年度分）における年間平均給与を 245 日(稼働日)で除した値を用いている。

＜業種別人件費単価（計算値）＞

農林水産・鉱業：10,600 円／日

不動産・建築：17,212 円／日

製造業：18,069 円／日

エネルギー、運輸業、情報通信、医療、教育、行政サービス：19,890 円／日

金融：20,457 円／日

サービス：14,522 円／日

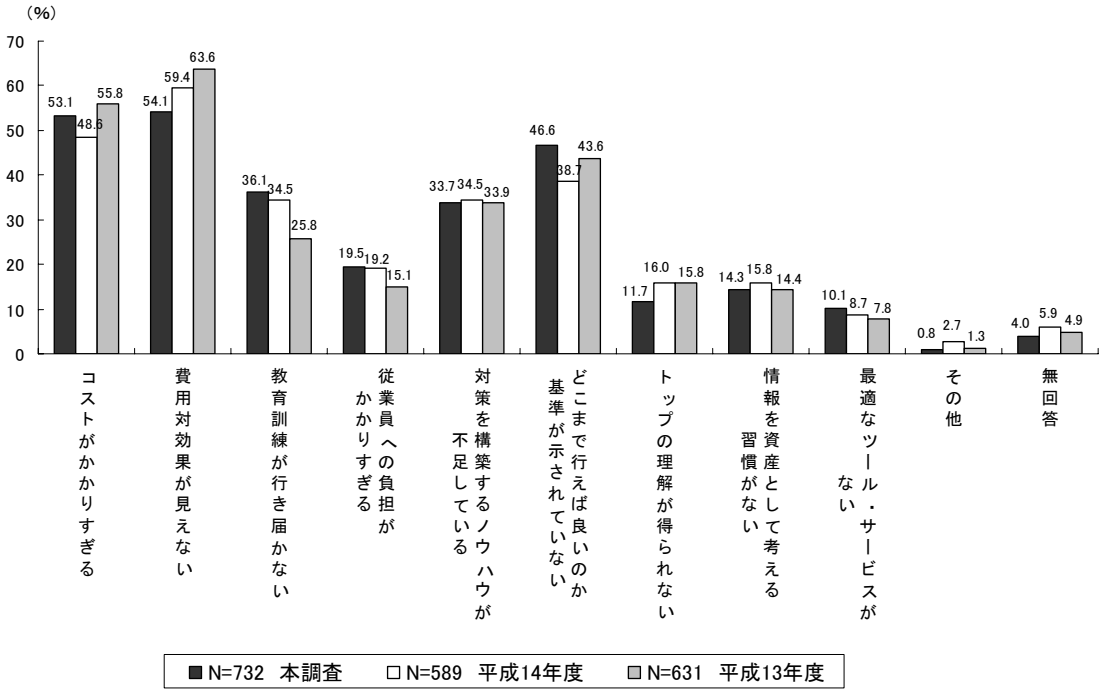
第４章　情報セキュリティに関する問題点

1. 産業界等における情報セキュリティ対策の問題点

前章でのアンケート調査の結果によれば、昨年度調査と比較し、セキュリティポリシーの策定は進みつつあるものの、セキュリティポリシーに規定している事項が実際は実践されていないことや、無線 LAN のセキュリティ対策の実施率が依然として低いこと等、情報セキュリティ対策が進んでいるとは必ずしも言えない状況にある。また、この１年間に61.4%の団体が、何らかの情報セキュリティにかかる被害にあっており、被害発生時の復旧処理に要したコストが 1,000 万円を超える団体もあり、情報セキュリティ対策の一層の普及が望まれる。

一方で、情報セキュリティ対策を実施する上での問題として、費用対効果が見えないことやコストがかかりすぎること等を挙げる団体が多い。

情報セキュリティ対策を実施する上での問題点



2. 高度情報通信ネットワークにかかる現状の問題点

会議における議論の中では、現状の問題点として、主に次の３つの事案が取り上げられた。

(1)　インターネットを利用した広域詐欺

インターネットを利用した詐欺にも様々な手口があるが、いわゆる架空請求メールは、平成１５年中、ハイテク犯罪等に関する相談受理件数の約 43%を占めるほど大々的に横行した。架空請求詐欺の被害者は、被害者１人の被害はそれほど大きくないが、全国的に見れば被害総額は多額になる一方で、被害者は全国に点在しているため、全体を把握しにくいという問題点がある。広域詐欺は、組織犯罪等の資金源等にもなりうることから、全体を把握し、厳重に対処することが重要である。

他にもインターネット・オークション詐欺では、被害者は、全国に点在する他の被害者の存在が確認できず、また、たとえ被疑者が検挙されても、被疑者の本名等が分からないため、詐欺にあったかどうか判断しにくいことが挙げられた。

さらにクレジットカード詐欺では、保険で補償され、利用者自身は被害がないことから、被害総額が高額であっても、被害として発覚されにくく、捜査もされていないことがあるという指摘があった。

(2) ウイルスのまん延

平成１５年８月にいわゆる Blaster ワームがまん延する等、依然としてウイルスの猛威は衰えておらず、大規模なウイルスがまん延すると、ごく短期間に数十万件の相談があるなど関係する企業及び政府機関等に問い合わせが殺到し、その対応は大きな負担となる。

こうした現状に対し、ソフトベンダー等においては、啓蒙活動の強化、コールセンタ等の危機管理体制の強化など、各種対策を進めている。また、政府においても、警察庁、総務省及び経済産業省が３省庁連名で注意喚起を実施するなど、コンピュータ・ウイルス対策を強化している。

しかし、ウイルスが発生してからまん延するまでの期間は徐々に短くなっており、対策を練る期間、周知のための期間も短くなっているが、ウイルス発生前は、特定ポートのトラフィック増加や Exploit Code 等の端緒情報をつかんだとしても注意喚起すべきタイミングが難しいことや、メールや Web での注意喚起では、一般ユーザまで情報が浸透しないという問題がある。また、対処のための情報が、提供する企業や機関によって用語が異なり、一般ユーザが混乱するという点も問題点として挙げられる。

(3) 違法・有害な書き込み

インターネット上の掲示板等の中には、違法・有害な書き込みがなされる場合があり、名誉毀損などの違法な書き込みのほか、様々な問題が発生している。

インターネット上で自殺希望者を募り、知らない人同士が集まって自殺するといういわゆるネット自殺もその一つであるが、「自殺する」旨の書き込み自体は犯罪ではないため、捜査手続によって書き込みした人物を特定することができない。

このように、明らかに犯罪とは言えないが、社会的に問題のあるインターネット上の行為に対し、それを防止する方法が明らかとなっていないことが問題となっている。

第５章　官民における情報セキュリティ関連情報の共有

1. 官民において共有すべき情報

どのような情報を共有すべきかについては、「どのような目的で」「どのような場合に」「誰と誰が」共有するのかによって異なると考えられるため、それぞれの具体的事例の類型ごとに共有すべき情報が何かを検討すべきである。

まず目的については、主に警察と産業界等との情報共有の目的は、①犯罪の検挙と②犯罪の予防・被害の最小化の２つに分けられる。

(1)　犯罪の検挙のための情報共有

現在、刑法・刑事訴訟法の改正等により、サイバー犯罪の捜査のための法整備が進められているところであるが、より安全なネットワーク社会の実現のためには、犯罪が行われた場合に、これを特定・検挙することが出来るようにすることが、インターネット等を利用する者等の権利・利益の保護の上から重要である。

よって、犯罪の検挙のためには、犯人の特定・検挙に資する情報を共有すべきであり、具体的には、民側が官側（警察）に、被害者が所有している被害情報、ISP 等が所有している顧客情報や通信記録等の情報を提供することが考えられる。

問題点としては、個人情報の保護の観点から、目的外の用途で使用しないこと等の情報の取り扱いに関する条件を設定する必要があること、また、通信記録保存等については経済的な負担がかかることなどが挙げられる。

その他、通信の秘密の保護についても考慮すべきとの意見があった。

(2)　犯罪の予防のための情報共有

この場合には、平時と緊急時・事案発生時に分けて情報共有について考えることとする。

平時については、情報セキュリティ対策に関する情報や最新の技術情報を共有すべきであり、一般ユーザに対する注意喚起等の情報提供が主であると考えられる。具体的には、官側から民側にハイテク犯罪の被害状況や情報セキュリティ対策の取組み状況についてまとめたものを提供することなどが考えられる。民側から官側への情報提供としては、メーカー等が所有している脆弱性とその対策に関する情報を官側に提供し、官側が一般ユーザへの広報啓発に利用することなどが考えられる。

緊急時・事案発生時については、被害情報や被害の最小化に資する情報を共有すべきであり、具体的には、民側（被害者等）が官側に被害に関する情報を提供し、官側は民側（個人）に対し、犯罪手法や攻撃手法等に関する情報等を提供し、被害の最小化を図る必要がある。

犯罪の予防のための情報共有についての問題点としては、平時・緊急時とも、個人情報保護や公務員の守秘義務を確保しつつどのような情報共有が可能かということや、被害情報の公表により模倣犯を誘発する可能性があるということ、他人の被害防止の

ための情報提供にかかるコストを負担すること等が挙げられる。

その他、通信の秘密の保護についても考慮すべきとの意見があった。

2．官民における情報共有の在り方

共有すべき情報は、各事例によって異なることから、さらに目的や対象を明確化する必要があるため、具体的事例に沿って検討することとした。具体的事例については、情報共有のスキームとして、現状の問題点を解決するスキームを検討するため、第４章の２で「高度情報通信ネットワークにかかる現状の問題点」として取り上げられた３つの事例に焦点を当て、議論を進めた。

3．官民における情報共有のための課題

会議における議論では、官から民への情報提供について、メールや Web で注意喚起をしても、一般ユーザには必ずしも伝わらないため、情報セキュリティ意識の底上げを図るにはＴＶや新聞等の従来のマスメディアの利用や、直接の働きかけを行う運動が必要ではないかとの意見が挙がった。

民から官への情報提供については、インターネットの匿名性は重要であるが、インターネット上の犯罪を防止するためには、追跡性も必要であり、免責等を検討して犯人の特定のための情報開示を進めるとともに、違法情報の通報者の保護対策も考慮する必要があるとの意見があった。

また、民（ISP やサイト運営者等）から民（非営利団体や弁護士等）への情報提供についても言及があり、当事者（発信者）に係る情報が開示されれば民事的に解決できるトラブルも多いため、現在の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（以下、「プロバイダ責任制限法」という。）の枠組みを拡張して情報開示を促進していくべき、との意見もあった。

さらに、一般ユーザへ犯罪の手口等の情報提供を促進しても、次々と新しい手口が出ていたちごっこになるので、やはり検挙が重要であり、ネットワーク上の犯罪の検挙を促進するため、一般ユーザからも詐欺等の違法・有害情報を全国的に収集し、警察がそれを活用する枠組みがあれば効果的ではないかとの提案があった。

他に、官民における情報共有全体に対する意見として、情報の正確性を担保する必要があるため、情報を適切に管理する枠組みを検討すべきであるとの意見や、「民」といっても①専門家・有識者、②ISP 等、③その他の民間企業、④個人に分けて考える必要があるとの意見が挙がった。

第６章　具体的事例に沿った情報共有のスキーム

1．インターネットを利用した広域詐欺事案

(1)　事例内容

全国に被害が及ぶインターネットを利用した広域詐欺事案において、被害拡大防止や犯人の特定のため、どのような情報共有ができるかを検討した。

具体的には、架空請求メールによる詐欺、インターネット・オークション利用による詐欺等の事案を想定している。

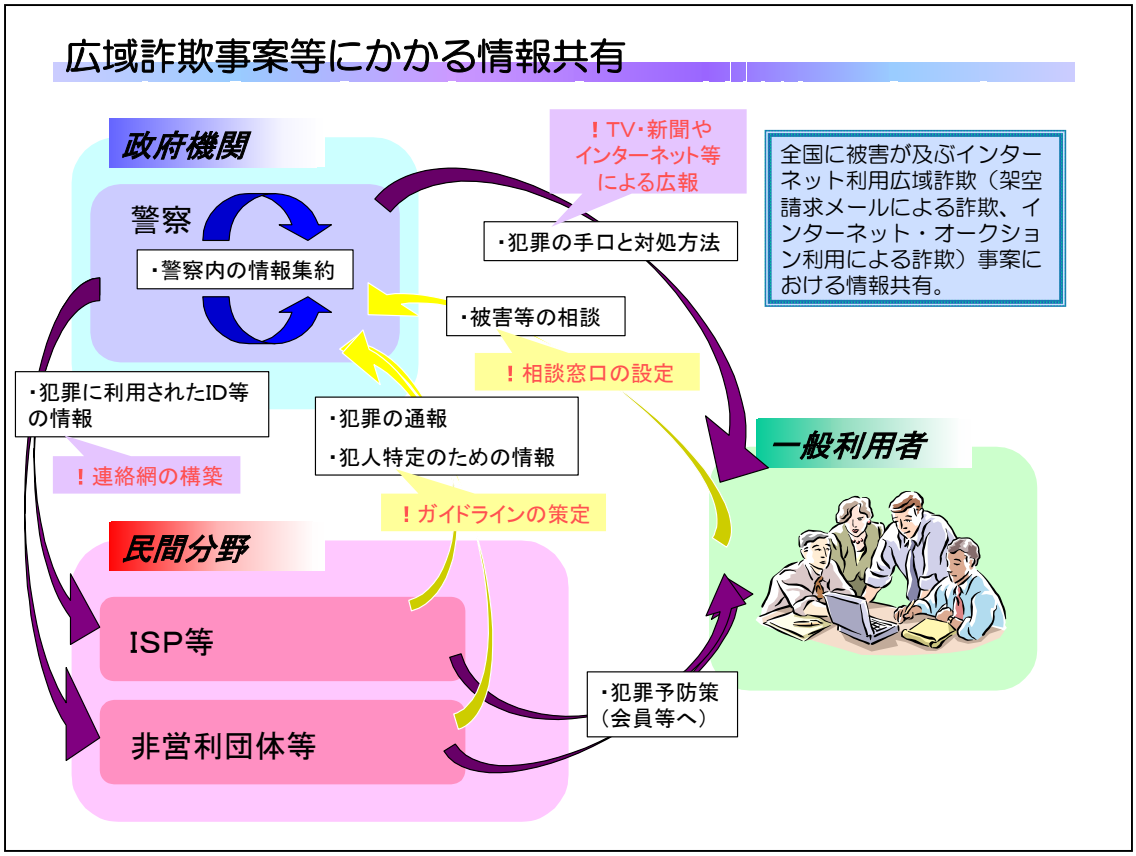
(2)　問題解決のための指針

警察の体制としては、取締りを強化するとともに、広報啓発を実施して消費者教育に取り組むため、これらインターネットを利用した犯罪に関する情報の一元化のための体制整備や被害者からの相談窓口の設置について検討しているところである。

また、警察との連携としては、特に非営利団体・ISP 等と連携することが重要であり、情報共有を進めるためには、どのような情報をどのような手続で共有するかについて定める必要がある。

(3)　情報共有のスキーム

これらの情報共有のスキームをまとめて、図示化した。



(4) 今後の課題

議論の過程で、非営利団体や ISP 等においても、詐欺についての注意喚起や詐欺行為を行っていると思われる者の振込先口座リストの公表など、利用者に対する広報啓発を実施しており、口座の凍結等金融機関との連携も必要との意見や、架空請求詐欺のように模倣犯が出やすいものは、やはり検挙が重要であり、新規口座の作成や ISP への加入の際に、より確実な本人認証を行うなど、追跡性を確保すべきだとの意見があった。

また、全てを包含するようなポータルサイトを構築すべきとの意見もあった一方、あまりコンテンツを充実させすぎると、初心者にとっては目的のコンテンツを検索するのが困難になるため、ユーザが主体的に情報を集めたり調べたりしなくとも、情報が収集されるような仕組みが求められているのでは、との意見もあった。

2. ウイルスのまん延事案

(1) 事例内容

ウイルスによる広範な被害が発生した場合、又はそのような発生が予想される場合において、被害拡大防止やウイルス頒布者又は作成者の特定のために、どのような情報共有ができるかを検討した。

具体的には、いわゆる Slammer ワームや Blaster ワームのまん延等を想定している。

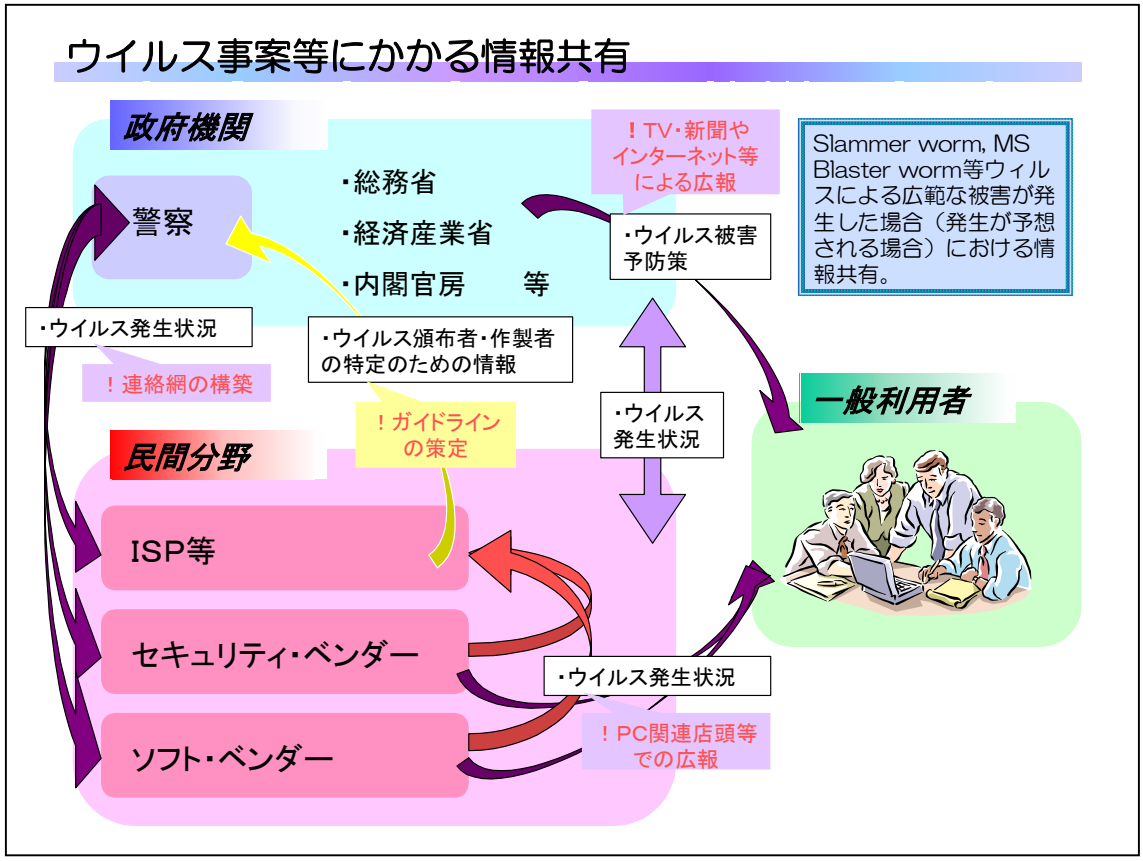
(2) 問題解決のための指針

政府内では、総務省、経済産業省、警察庁の３省庁が連名でウイルスに関する注意喚起をするなど、関係省庁間で連携した活動を推進している。

また、警察との連携としては、特に ISP・セキュリティ関連ベンダー等と連携することが重要であり、情報共有を進めるためには、情報提供の窓口を相互に設定する必要がある。

(3) 情報共有のスキーム

これらの情報共有のスキームをまとめて、図示化した。



(4)　今後の課題

会議では、トラフィック等に大きな影響を与えても感染したPCには症状が出ないタイプのウイルスについて、利用者に対して駆除や感染防止を実行する動機を与えるのが難しいという指摘があったほか、今後、様々なOSを対象とするウイルスやOSによらないウイルス、またPC以外の電子機器にも感染するウイルス等の新種のウイルスが発生する可能性も視野に入れる必要があることが示唆され、初心者に対してはWebによらない注意喚起や広報啓発を実施できるようにするための草の根活動の必要性が挙げられた。

また、ウイルスに関する情報共有を今まで以上に進展させるためは、企業にとってメリットを提示すべきではないかという意見に対し、ウイルスがまん延した際のトラフィックの増加や利用者の相談対応等による大きな負担を回避するというメリットはあるのではないかとのやりとりもあった。

他に、企業等も、裁判等の事態に備える必要が高まっていることから、コンピュータ・フォーレンジック（注）の研究を進める必要があるとの意見もあった。

（注）コンピュータ・フォレンジックについて

「コンピュータ・フォレンジック」とは、「計算機科学などを利用して、デジタルの世界の証拠性（evidence）を確保し、法的問題の解決を図る手段」と言われており、「ログの改ざん、破壊等これまでの種法会は証拠を検出することが困難な被害を受けたコンピュータに対しても、高度なツールによってコンピュータ内のデータを調査・分析することによい、不正アクセスの追跡を行う手段を含むものとされている。

3. 違法・有害書き込み事案

(1) 事例内容

インターネット上に、犯罪や事件を誘発するような違法・有害な情報が掲載された場合において、犯罪や事件の未然防止のために、どのような情報共有ができるかを検討した。

具体的には、インターネット上の掲示板に自殺の決行をほのめかす内容が書き込まれた場合、人命保護の観点から、書き込みした人物を特定して保護する必要がある。また、少年被疑者の実名等が書き込まれた場合、人権保護の観点から、こうした書き込みの拡大を防止する必要があること等を想定している。

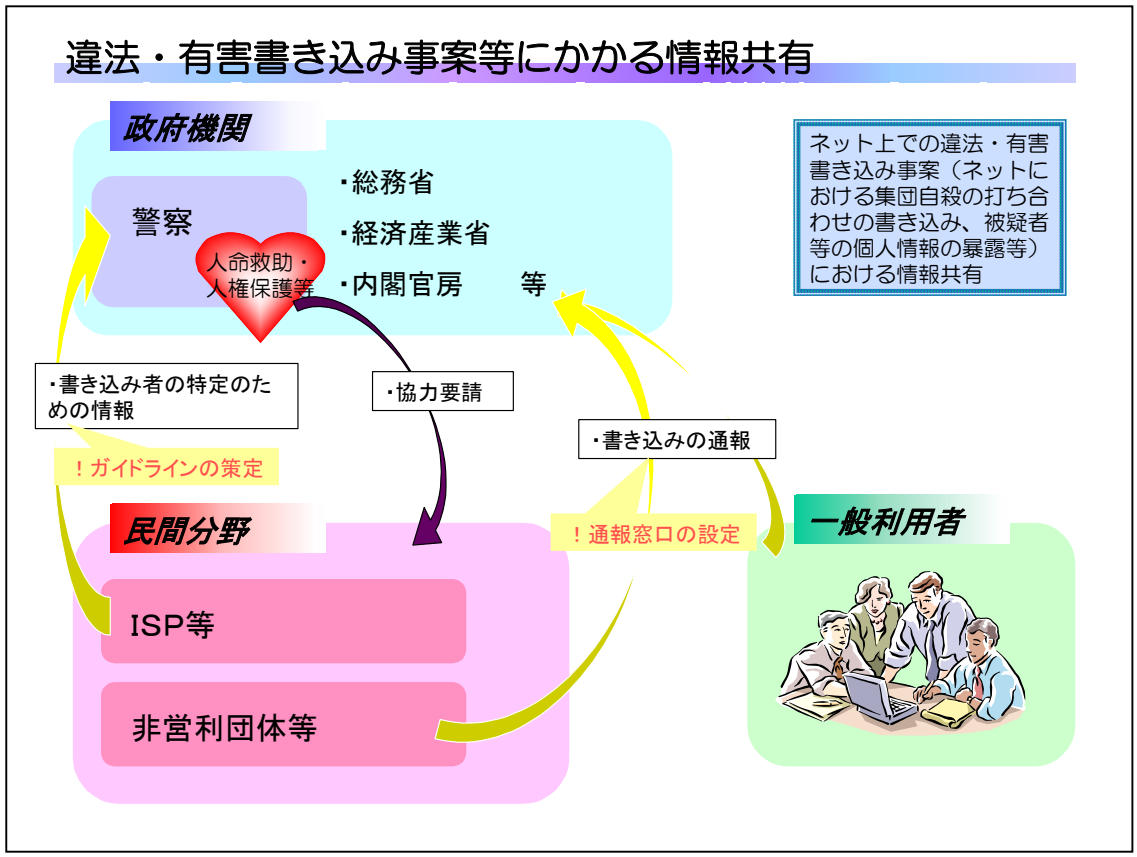
(2) 問題解決のための指針

政府内において、違法・有害コンテンツ対策に関する連携を強化しているほか、警察における体制として、違法・有害書き込み情報を通報する窓口の設定について検討しているところである。

また、警察との連携としては、特に ISP 等と連携することが重要であり、情報共有を進めるためには、人命等に関わる緊急な対応が必要な書き込みがあった場合等にどのような対応をとるべきかをあらかじめ定めておく必要がある。

(3) 情報共有のスキーム

これらの情報共有のスキームをまとめて、図示化した。



(4) 今後の課題

会議では、プロバイダ責任制限法の枠組みは、様々なタイプの ISP が参入してきている現状と若干乖離してきている可能性があることや、自殺や人権侵害の書き込みがあった場合、公益性の観点から削除要請する枠組みが必要ではないかという点について言及されたほか、グロテスクな画像の掲載等、他にも違法・有害なコンテンツは多種存在することから、コンテンツを総合的に評価する機関を設置すればよいのではないかとの提案もあった。

また、違法・有害な書き込み等に対する対応を示すガイドラインについては、ISP 自身が社会的責任を踏まえ、提示された問題点を精査して、主体的に約款やガイドラインを策定すべきだとの意見に対し、個別の判断を各個人や企業に委ねることには限界があり、利用者と ISP と双方が参加したガイドラインを策定すべきだとの意見があった。

どちらにしても、現在は、実際にどのような事例が緊急に対応すべきか判断が困難な場合もあるため、これをあきらかにする必要があるほか、今後、ISP のみならず、一般企業や自治体にも緊急の対応を迫られる可能性があることから、何らかの基準を示すガイドラインの策定が必要だ、との意見が多数挙がった。