情報セキュリティに関する
脅威の実態把握・分析について

平成１４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昨年度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きており、昨年度は報告書「情報セキュリティ対策における連携の推進について」を取りまとめた。

本年度は、「情報セキュリティに関する脅威の実態把握・分析」というテーマを選び、アンケート調査などを通じて、官民が連携して情報セキュリティ対策を講ずる上で参考となるであろう脅威の実態を明らかにすることを試みた。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１５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
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
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 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
佐々木良一	東京電機大学 教授
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　ｺﾝｻﾂﾃｨﾝｸﾞﾏﾈｰｼﾞｬｰ
田尾陽一	セコムトラストネット（株） 社長

高山健	楽天（株） 常務取締役
永田実	ソニー（株） ﾓｰﾊﾞｲﾙﾈｯﾄﾜｰｸｶﾝﾊﾟﾆｰ　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
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 監事
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

（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ところである。

本年度（平成１４年度）の会議においては、情報セキュリティ対策を講ずる上で脅威の実態が明らかになっていることが不可欠であるとの認識の下、上記報告書に記載されたテーマから「情報セキュリティに関する脅威の実態把握・分析」を選び、より詳細な検討を行った。

なお、ネットワーク・セキュリティをめぐる状況は急速に変化しており、本報告書の内容も現時点の状況を前提としたものとして理解されるべきであり、数年後の状況においても当然に妥当するものではないことを付言する。

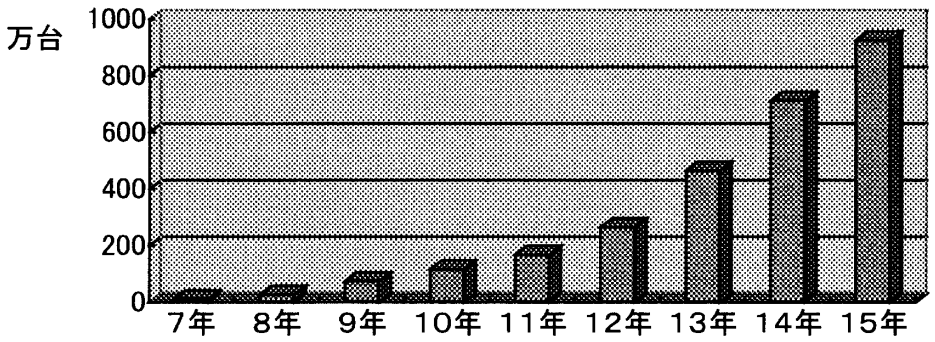
第２章　産業界等と政府との連携の重要性

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１５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926万台であり、その数は、近年急激に増加している。

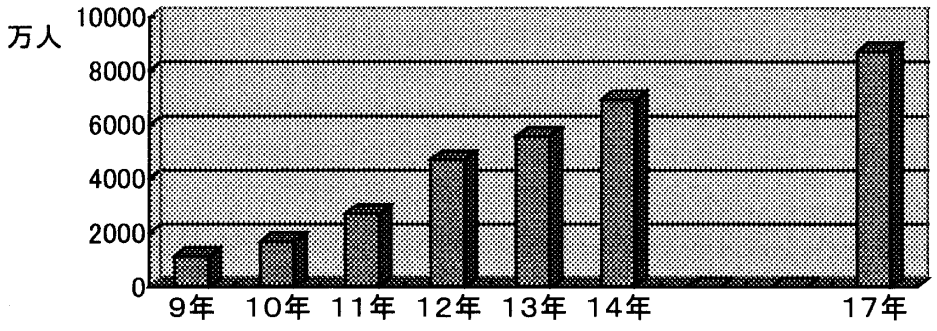
インターネットに接続されている国内コンピュータ数



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１７年には8,720万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１４年通信利用動向調査、平成１４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　脅威の実態把握・分析の必要性

本年度の会議においては、情報セキュリティ対策を講ずる上で脅威の実態が明らかになっていることが不可欠であるとの認識の下、昨年度の報告書に記載されたテーマから「情報セキュリティに関する脅威の実態把握・分析」を選び、より詳細な検討を行った。

1．情報セキュリティ対策

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、情報セキュリティに関する脅威は、政府機関や企業などに限らずすべての国民にとって重大な脅威として現れてくることが懸念される。万全の情報セキュリティ対策を講じ、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、必須の課題である。

2．情報セキュリティ対策における問題点

情報セキュリティの基本は、守るべき資産を明確にし、その脆弱性とそれに対する脅威を基にリスクを評価し、講ずべき対策を決定するというものである。

しかし、この際に、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。アンケート調査（後述（第５章））の結果からも、約65%の企業が情報セキュリティ対策を行う上での問題点として、「費用対効果が見えない」という点を指摘している。

3．脅威の実態把握・分析の必要性

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。

第４章　脅威として把握すべき対象

アンケート調査（後述（第５章））においては、情報セキュリティに関する脅威を次のように分類、整理している。

1	コンピュータウイルス、ワームへの感染
2	ファイルやデータベースの改ざん、不正な書込み、破壊
3	ホームページの改ざん
4	システム、ネットワークの破壊
5	Dos 攻撃
6	メールの不正中継、踏み台
7	機密情報、個人情報等の盗難、漏洩
8	盗聴
9	社内からの不正アクセス
10	内部者のネットワーク悪用（私用メール、ポルノ画像閲覧等）
11	ノート PC 盗難
12	その他情報機器（外部記憶装置等）盗難
13	ネット詐欺
14	Ｗｅｂや掲示板上での誹謗・中傷
15	ドメイン名の不正取得による業務妨害、信用毀損
16	インターネット上の著作権侵害
17	インターネット上の商標権侵害
18	その他

１～１０は、情報セキュリティを直接の対象とした脅威であり、１１及び１２は物理的な盗難である。

１３～１７については、必ずしも情報セキュリティを直接の対象とした脅威でないが、情報セキュリティ対策が十分に行われていないことによって生じる脅威を含み得るものであり、所要の対策を講ずることが求められるものとして把握すべき対象に含めている。

なお会議において、情報セキュリティ対策を講ずるに当たっては、上記の脅威も含め、広く次のような脅威を考慮に入れるべきであるとの指摘もなされた。

- 災害等
- テロ等
- 故障・障害
- 無権限（不正）
- 過失

- 準拠違反（法、ポリシー）
- 要員

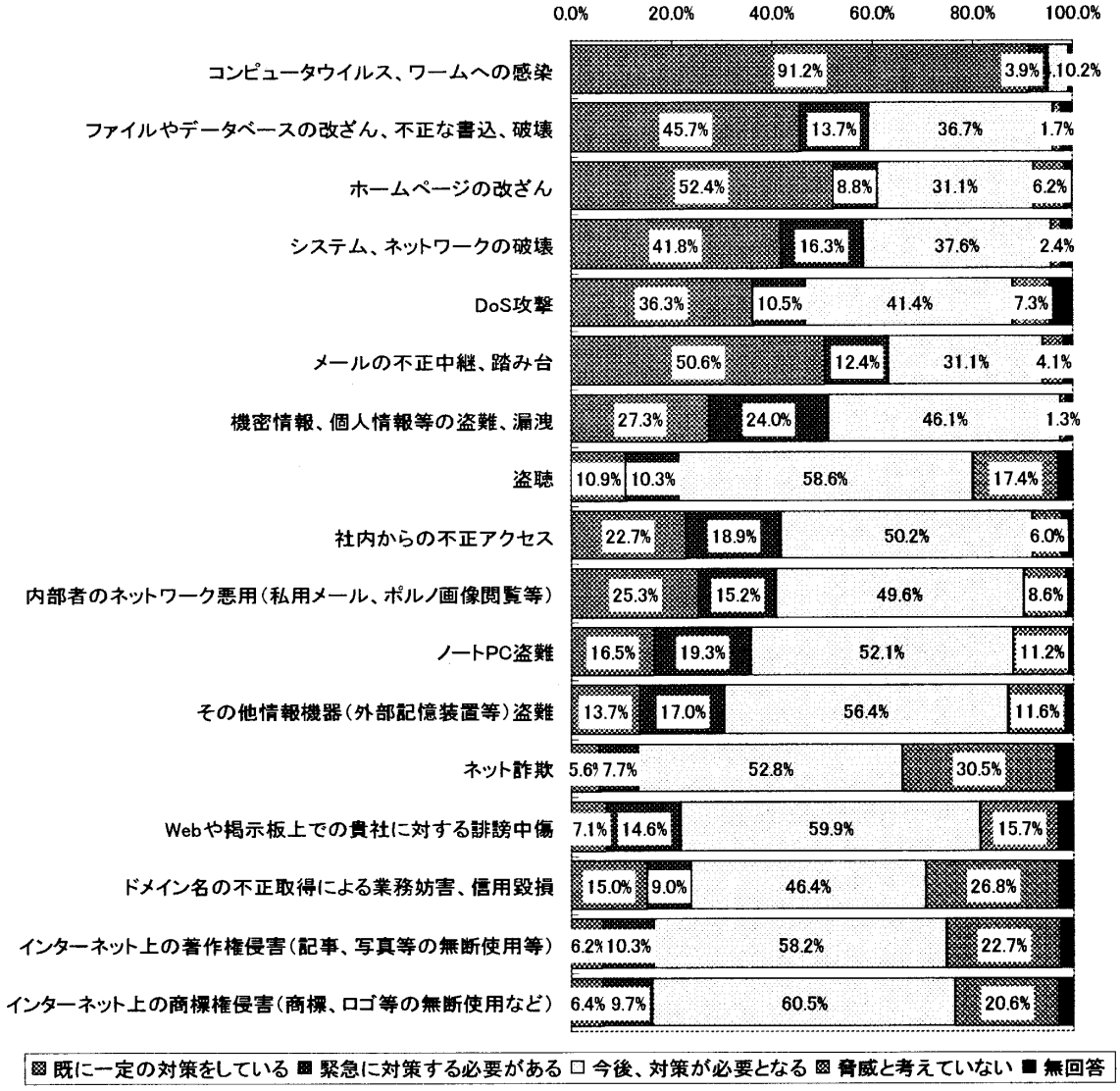
第５章　脅威の実態把握・分析

本年度の会議においては、警察庁が企業・行政機関・教育機関を対象に行った「ハイテク犯罪等に係る被害状況の調査」（以下「アンケート調査」）の結果を議論の参考にした。

1．情報セキュリティに関連した脅威

アンケート調査の結果、いずれの項目も脅威として認識されていることがうかがえる。

情報セキュリティに関連した脅威への対応状況（ｎ＝466（企業））

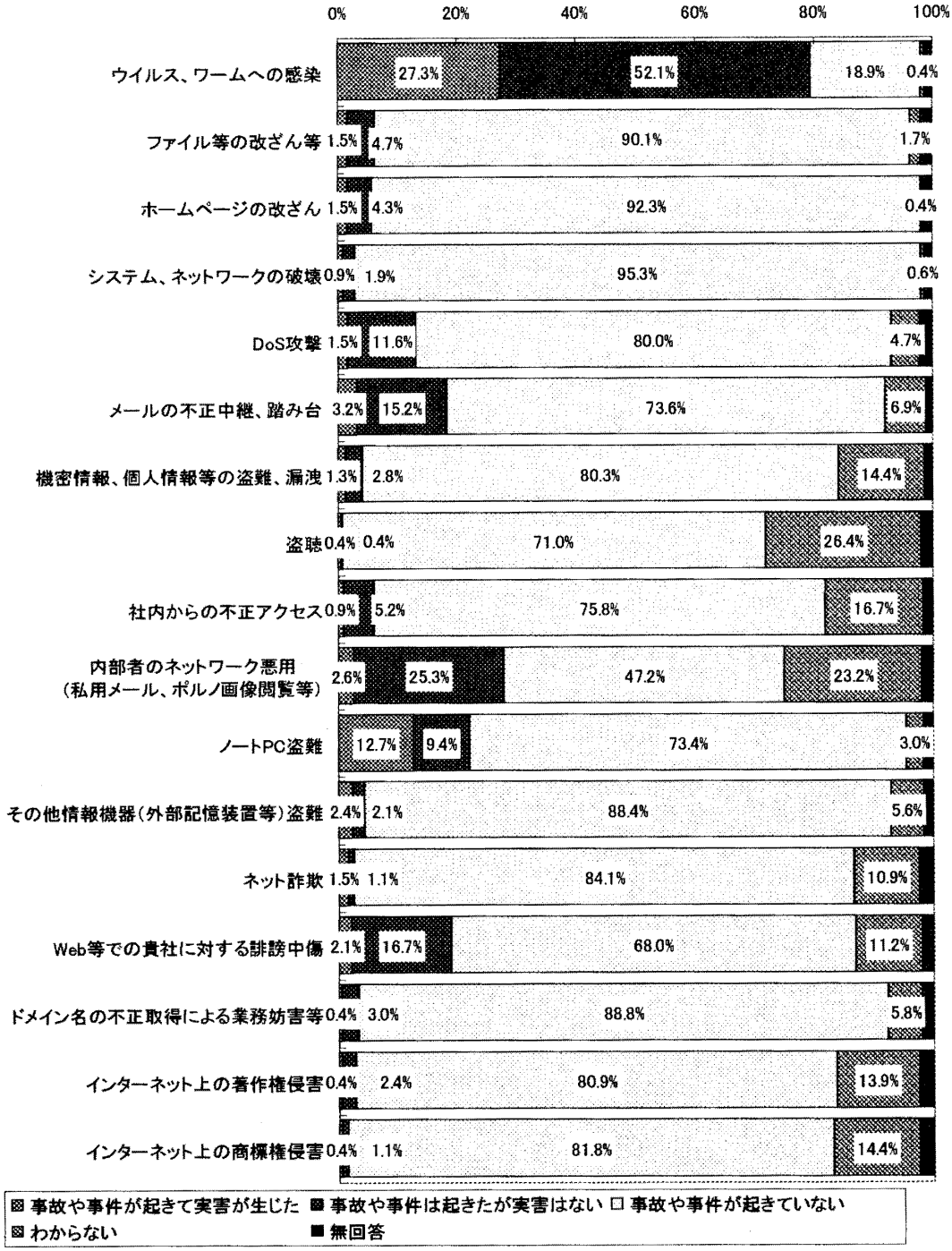


（注）「ネット詐欺」、「Webや掲示板上での貴社に対する誹謗中傷」、「ドメイン名の不正取得による業務妨害、信用毀損」、「インターネット上の著作権侵害」、「インターネット上の商標権侵害」は、必ずしも情報セキュリティを直接の対象とした脅威ではないが、情報セキュリティ対策が十分に行われていないことによって生じる脅威を含み得るものであることから、ここでは項目として加えている。

2．被害状況

事故・事件の発生については、コンピュータウイルス感染が約 79%と最も多く、メールの不正中継約 18%、DoS 攻撃約 13%も他の項目と比較して多い。また、内部者のネットワーク悪用約 28%、ノートＰＣ盗難約 22%やＷｅｂ等による誹謗中傷約 19%も多く、ノートＰＣ盗難の実害発生の高さ約 13%は特徴的である。実害発生についてはコンピュータウイルス感染が約 27%で最も多い。

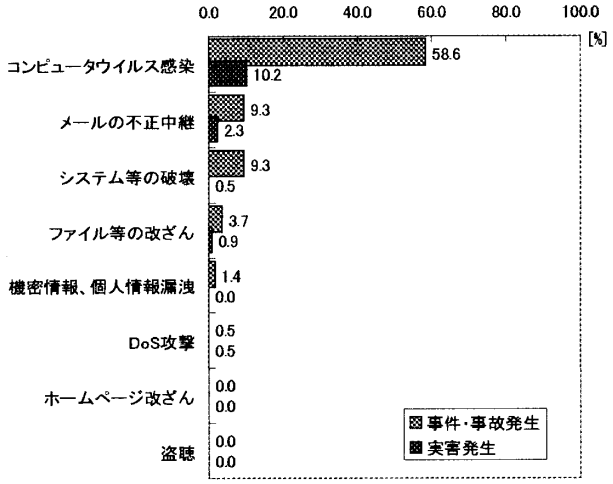
過去１年間のハイテク犯罪等による被害発生状況（企業：n=466）



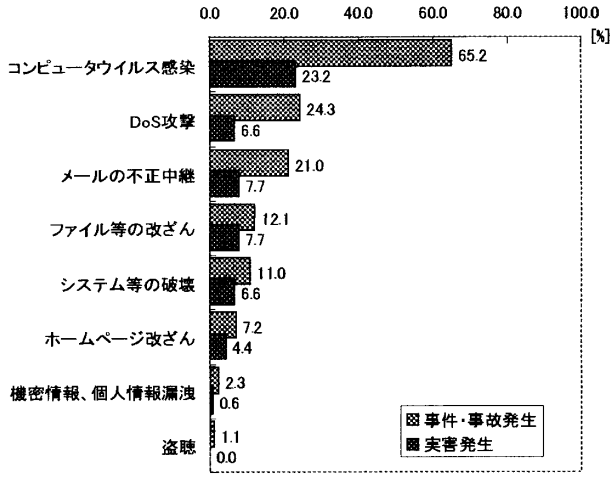
対象別に見ると、行政機関の事故・事件の発生率は全体的に低めであるのに対し、教育機関は高いことが分かる。

過去1年間の外部からの脅威によるハイテク犯罪等の発生状況

（行政機関：n=215）

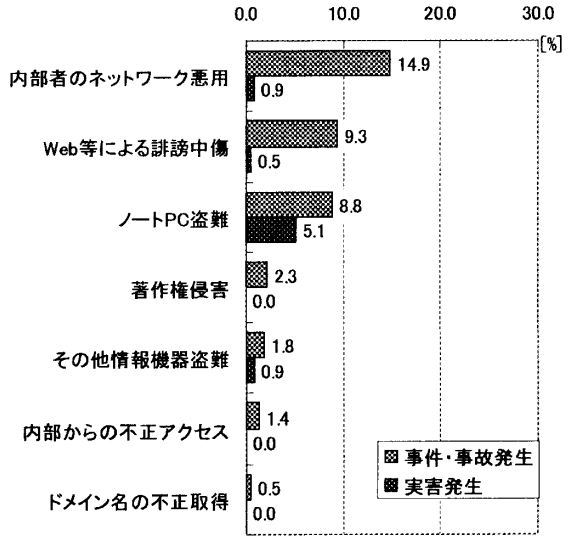


（教育機関：n=181）

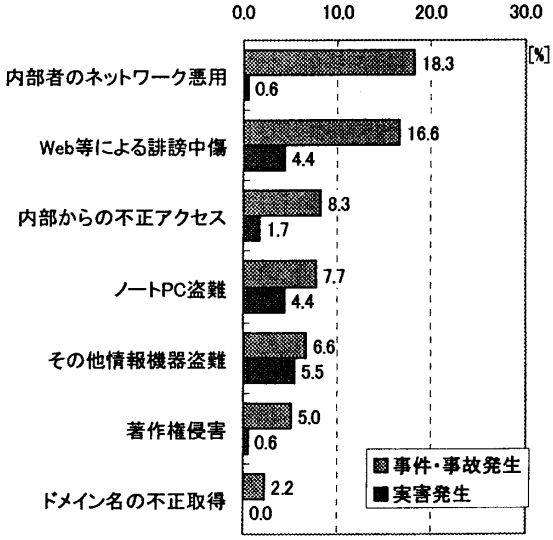


過去1年間のその他の脅威によるハイテク犯罪等の発生状況

（行政機関：n=215）



（教育機関：n=181）



3．被害金額

アンケート調査では、被害を受けた場合の「復旧に要した人日」、「復旧コスト（注１）」、「推定逸失利益額（注２）」について調査した。

注１：　復旧にかかった費用（外注費、ハードウェア、ソフトウェアの買い替えコスト等）。復旧処理にかかった社内の人件費は除く。

注２：　ＥＣサイトの停止等により逸した利益等。

「機密情報、個人情報等の盗難、漏洩」が発生した際の復旧に多くの人員・コストを要している状況が見られる。また、ウイルス感染やメールの不正中継、ネット詐欺、ノートＰＣについても、他と比較して被害金額が大きい。

実害発生企業における過去1年間に生じた被害金額の平均

	実害発生企業数	平均復旧人日（人日）	平均復旧コスト（円）	平均逸失利益額（円）
コンピュータウイルス、ワームへの感染	127	18.0	777,357	562,350
ファイルやデータベースの改ざん	7	6.0	1,000	224,000
ホームページの改ざん	7	1.3	30,000	-
システム、ネットワークの破壊	4	10.5	-	-
DoS攻撃	7	1.9	20,000	-
メールの不正中継、踏み台	15	6.7	135,000	500,000
機密情報、個人情報等の盗難、漏洩	6	30.0	5,000,000	-
盗聴	2	-	-	-
社内からの不正アクセス	4	1.0	-	-
内部者のネットワーク悪用	12	16.3	62,500	100,000
ノートPC盗難	59	5.4	436,406	478,200
その他情報機器盗難	11	0.8	282,500	22,500
ネット詐欺	7	5.3	1,510,000	120,000
Webや掲示板上での誹謗中傷	10	5.0	-	-
ドメイン名の不正取得による業務妨害、信用毀損	2	3.0	150,000	100,000
著作権侵害	2	2.0	-	200,000
商標権侵害	2	2.0	-	200,000

（注）平均は、無回答を除いて算出した。

被害額の算定については、何を被害ととらえるのか、その被害をいかに算定するか等、必ずしも容易ではないが、アンケート調査をもとに上場企業全体の年間被害金額を推計したところ、上場企業全体の情報セキュリティに関する被害は、復旧コスト 11.5 億円、逸失利益 7.9 億円、復旧に要する人日 23,011 人日となった。ただし、情報漏洩による逸失利益等の算定や著作権・商標権侵害等の被害状況の把握が困難であり、また、この推計は上場

企業に限ったものであることから、日本全体の被害額よりは過少に評価されたものであると考えられる。

なお、上場企業の売上高が、全企業の売上高の合計に占める割合は約３割である。

情報セキュリティに関連する事件や事故による上場企業全体の被害金額の推計

	復旧人日（人日）	復旧コスト（億円）	逸失利益額（億円）
コンピュータウイルス、ワームへの感染	16,197	7.12	5.14
ファイルやデータベースの改ざん	361	－	0.10
ホームページの改ざん	62	0.01	－
システム、ネットワークの破壊	297	－	－
DoS攻撃	93	0.01	－
メールの不正中継、踏み台	707	0.14	0.53
機密情報、個人情報等の盗難、漏洩	1,273	2,12	－
盗聴	－	－	－
社内からの不正アクセス	28	－	－
内部者のネットワーク悪用	1,369	0.05	0.08
ノートPC盗難	2,242	1.80	2.03
その他情報機器盗難	57	0.25	0.00
ネット詐欺	－	－	－
Webや掲示板上での誹謗中傷	283	－	－
ドメイン名の不正取得による業務妨害、信用毀損	42	0.02	0.01
著作権侵害	－	－	－
商標権侵害	－	－	－
合計	23,011	11.53	7.89

4．ハイテク犯罪等に関する訴訟の状況

アンケート調査の結果では、情報セキュリティに関連する事故・事件に関連した訴訟は少数であった。しかし、今後、情報漏洩やウイルス等の被害に関してセキュリティ対策の不備等の責任を追及する訴訟の増加が予想される。また、Ｗｅｂ等での誹謗中傷やネット詐欺がセキュリティ対策の不備に乗じた、いわゆる「なりすまし」等により行われた場合に、被害を受けた者が同様にセキュリティ対策の不備等の責任の追及を求めて提起する訴訟の増加も予想される。

第６章　情報セキュリティ対策への活用

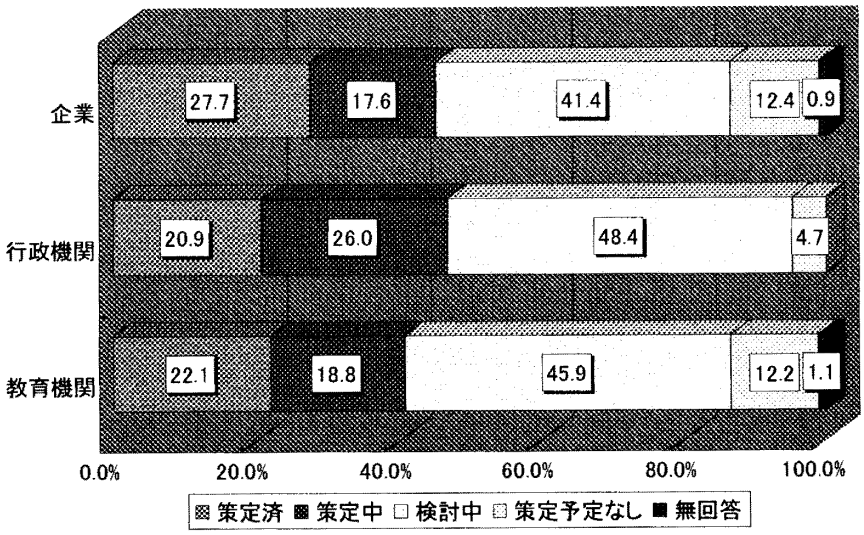
1．対策の現状

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。

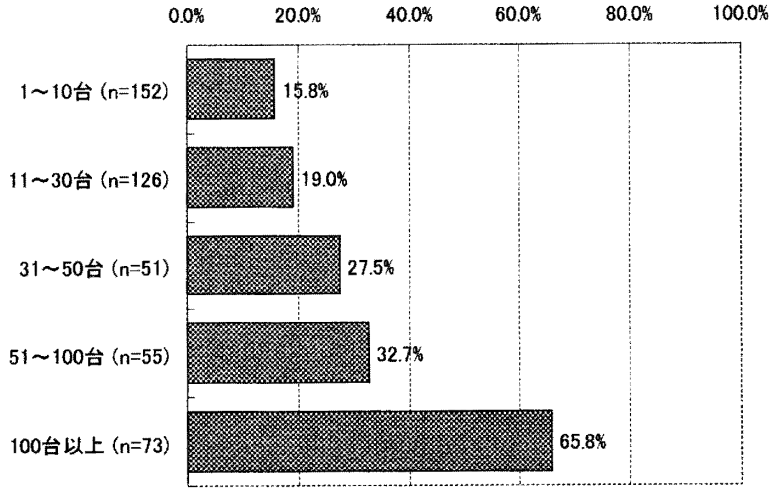
(1)　情報セキュリティポリシーの策定状況

策定済、策定中、検討中を加えると約 87%に達することから、セキュリティポリシーへの関心の高さはうかがえる。しかし、策定済の比率は、サーバを 100 台以上保有している企業では、65.8%が策定済みであるが、企業全体では約 28%、行政機関は約 21%、教育機関では約 22%にとどまっており、普及率は依然として低調である。

セキュリティポリシーの策定状況



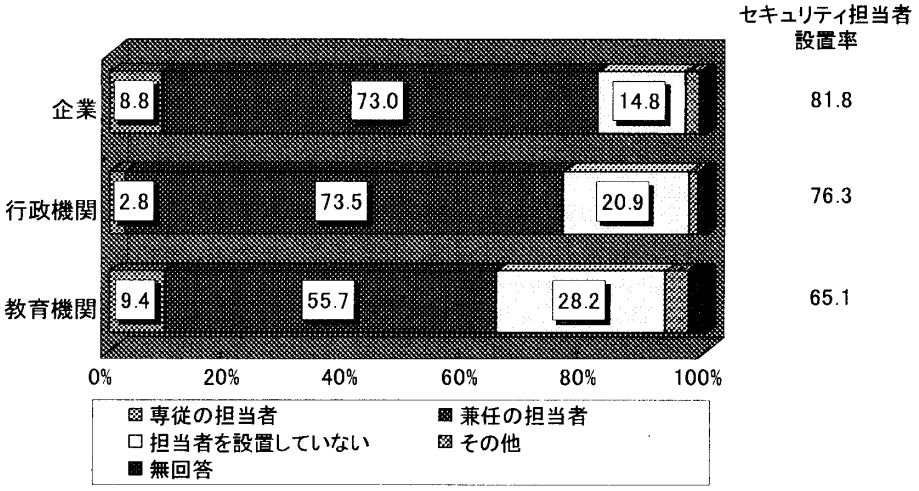
保有サーバ台数別にみたセキュリティポリシー策定済み企業の割合　n=466



(2)　情報セキュリティ担当者の設置状況

専従の担当者を置いているところは少数であるが、約 82%の企業が情報セキュリティ担当者を設置している。教育機関の約 28%はセキュリティ担当者を設置していない。

情報セキュリティ担当者の設置状況



(3)　セキュリティ対策投資

情報システム投資額の約６％が情報セキュリティ対策に投資されている。

情報セキュリティ対策投資額が情報システム投資額に占める割合（平成14年度）

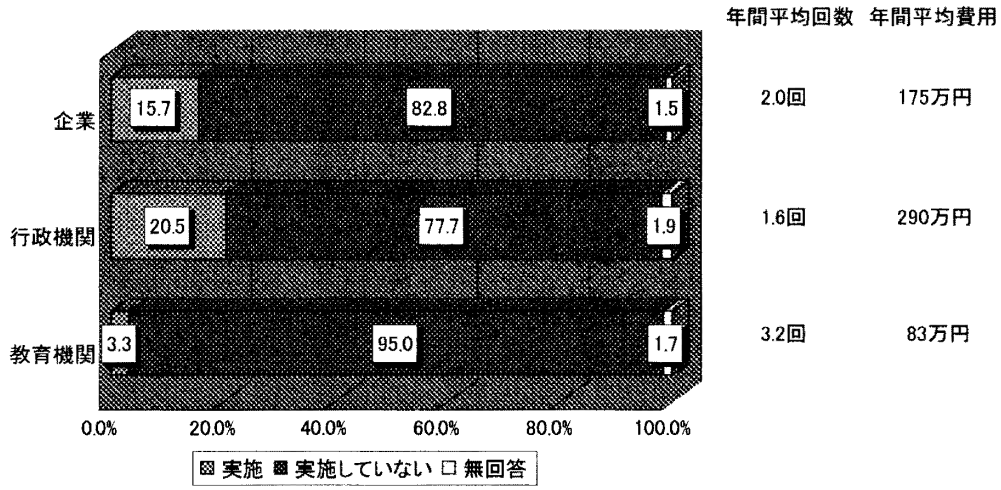
	企業	行政機関	教育機関
情報セキュリティ投資額／情報システム投資額	5.8%	6.8%	6.2%

(4)　脆弱性検査の実施状況

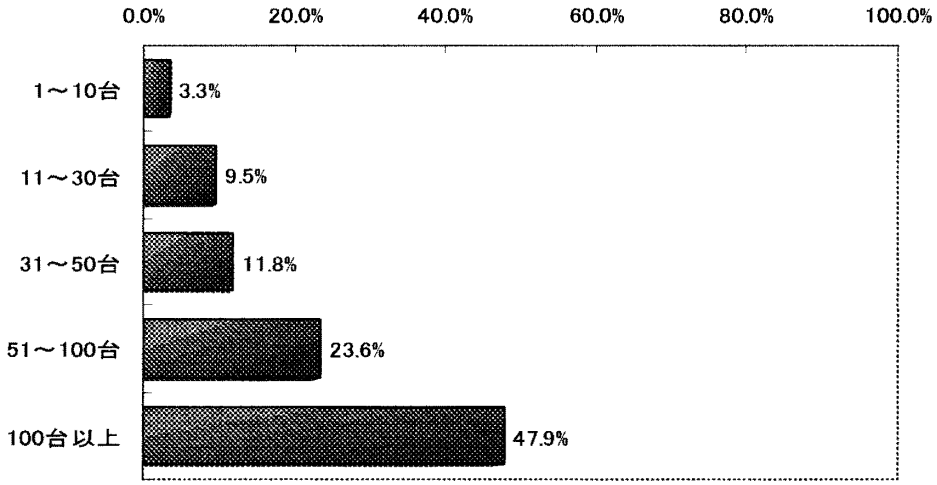
企業の約 15%、行政機関の約 20%が実施している。企業については、システム規模が大きいほど実施率が高い。年間のコストは、企業が約 175 万円、行政が約 290 万円であり、実施回数は、企業が 2.0 回、企業が 1.6 回となっている。

教育機関における実施率は約３％と低い。

過去1年間の脆弱性検査の実施状況

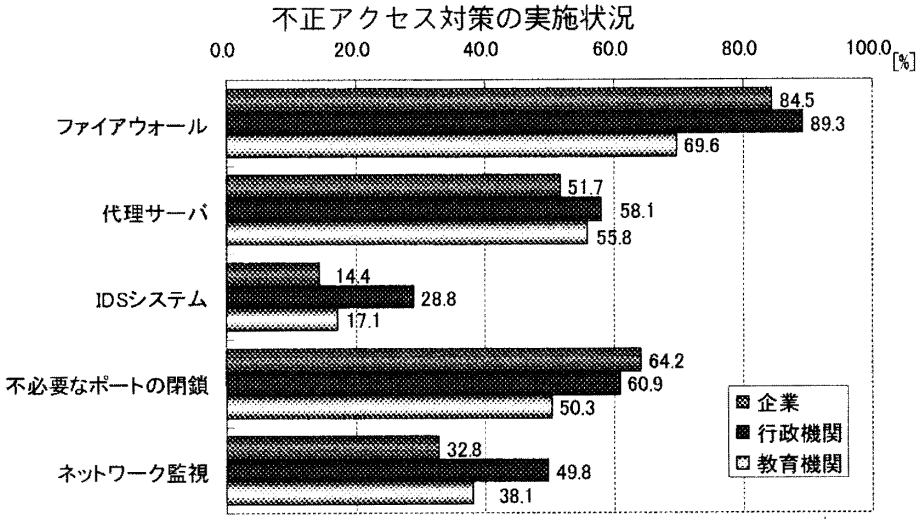


サーバ保有台数別にみた脆弱性検査実施企業の比率



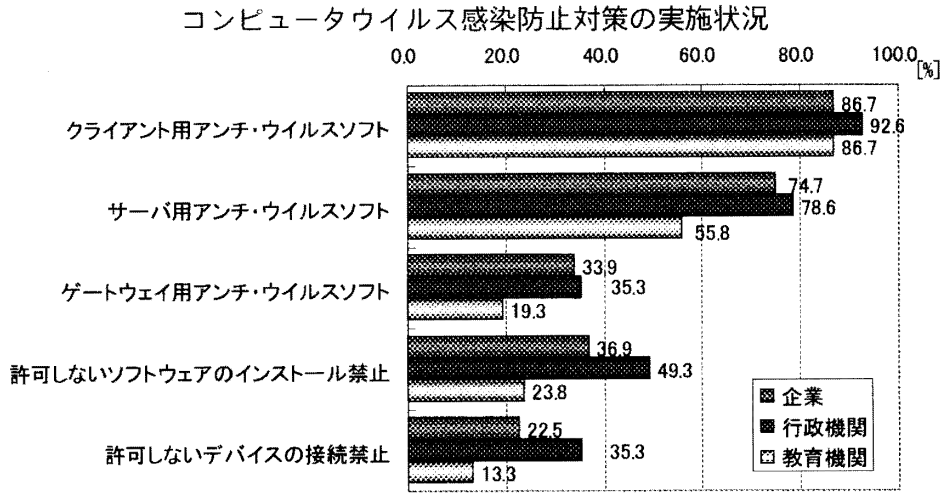
(5)　不正アクセス対策

ファイアーウォールの導入は企業の約85%、行政機関の約89%、教育機関の約70%で行われている。また、半数以上が不必要なポートを閉鎖している。ＩＤＳの導入は約10～30%にとどまっている。



(6)　ウイルス感染防止対策

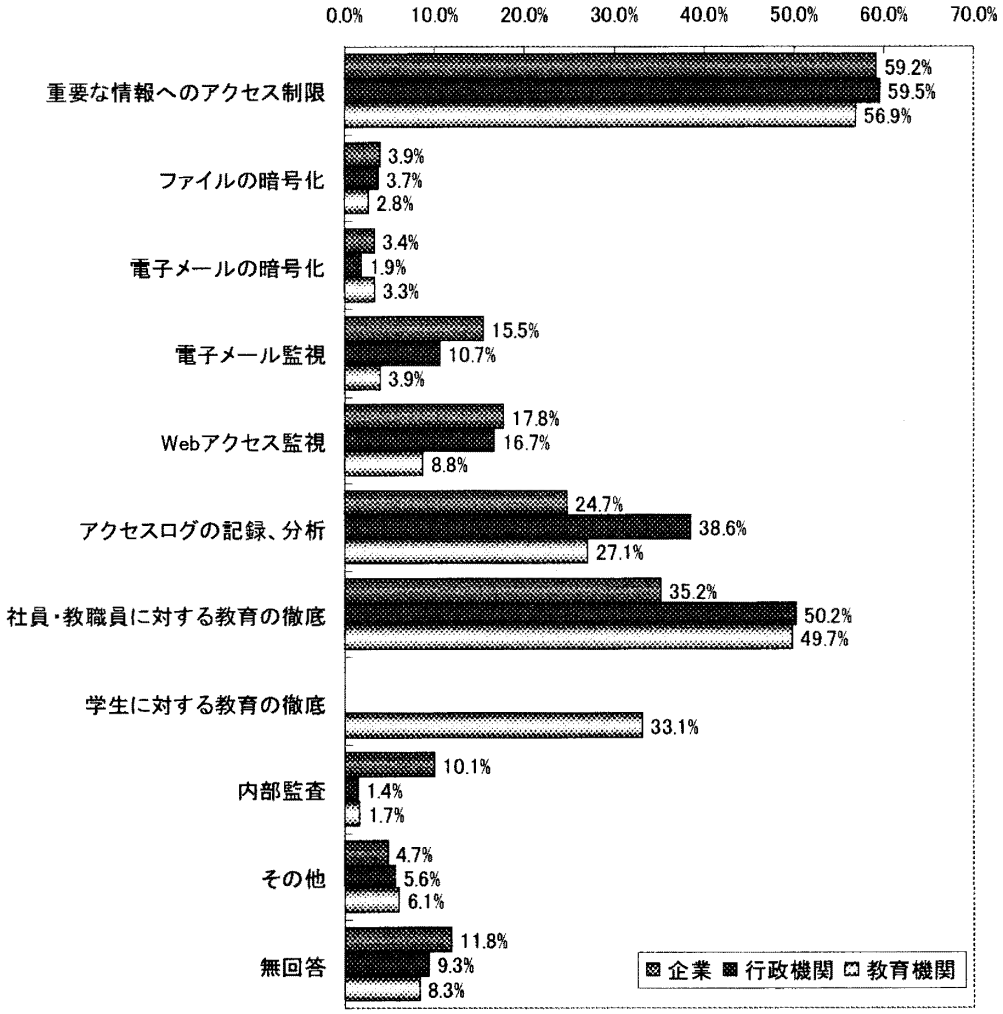
約90%前後がクライアント用アンチ・ウイルスソフトを、企業・行政機関の約75%がサーバ用アンチ・ウイルスソフトを導入している。ソフトウェアのインストール制限やデバイス接続禁止は行政機関で取組みが進んでいる。他方で、教育機関では取組みが遅れている。



(7)　内部からの情報漏洩防止対策

主な対策は、重要な情報へのアクセス制限（約 60%弱）と教育の徹底（約 40～50%）となっている。また、アクセスログの記録・分析も約 20～40%が実施している。暗号の利用や電子メールの監視は少数にとどまっている。

情報漏洩対策の実施状況

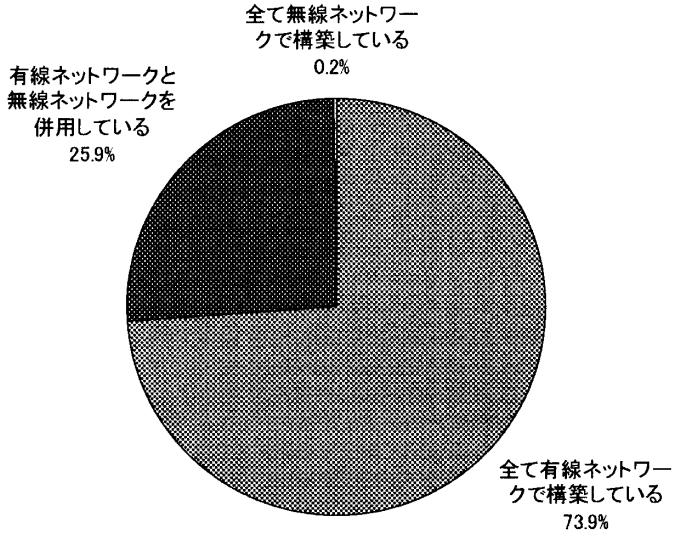


(8)　無線ＬＡＮ

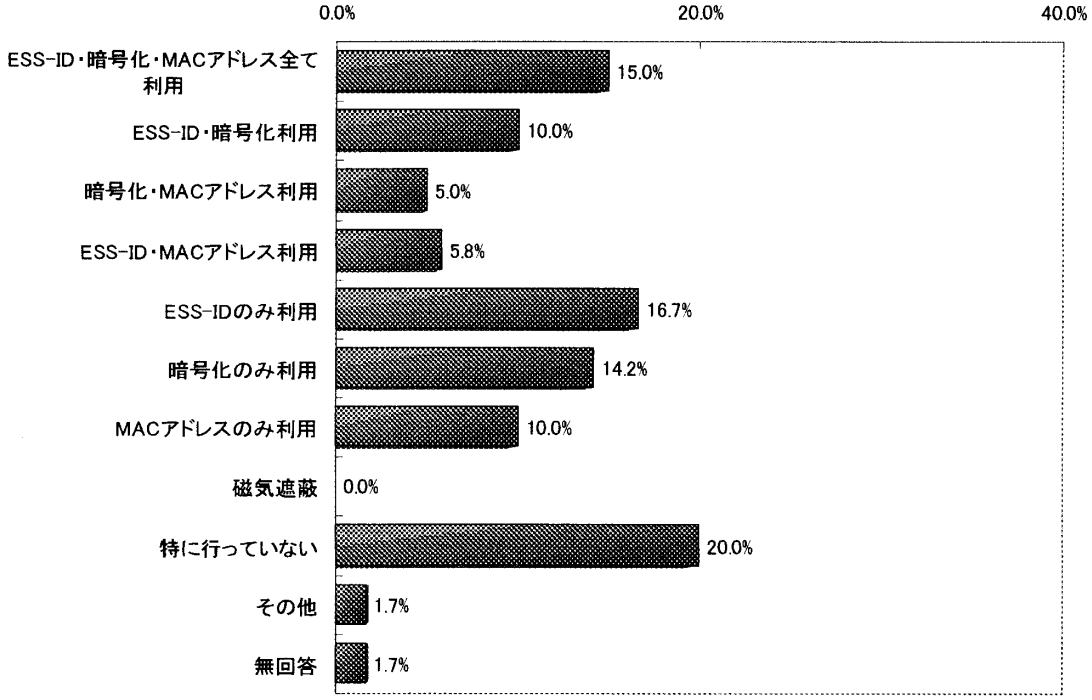
無線ＬＡＮを利用して社内ＬＡＮを構築している企業が約 74%に達している。そのうち約 15%で ESS-ID、暗号化、MAC アドレス認証の全てを実施している一方で、約 20%はセキュリティ対策を特に行っておらず、無線ＬＡＮのセキュリティに対する意識にばらつきが見られる。

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、セッションセキュリティやユーザ認証など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。

社内LANの構築形態　n=459



無線LANに対して行っているセキュリティ対策の組み合わせの状況　n=120



(9)　アクセスログ

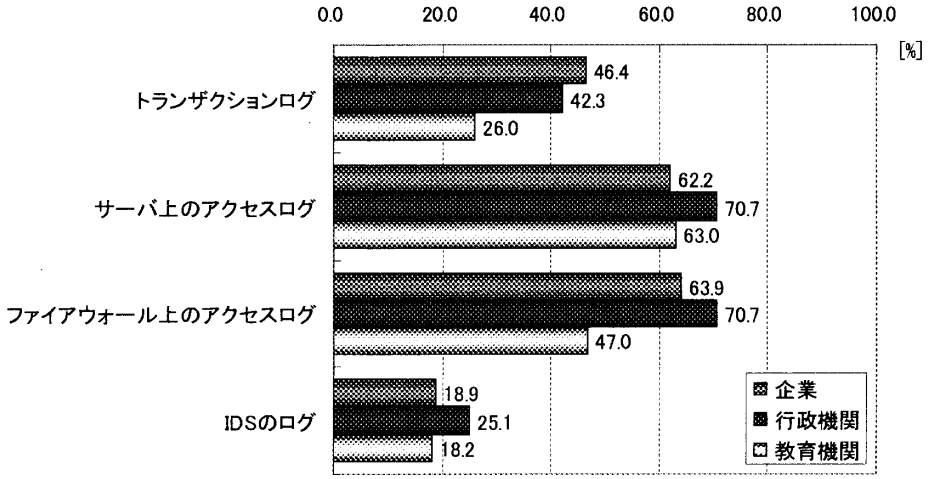
サーバ上のアクセスログの取得は約 60～70%で行われている。また、企業・教育機関の約 60～70%がファイアーウォール上のアクセスログを取得している。

ログの取得を行っている 90%以上がログを保存しており、保存期間は、平均半年から 9 ヶ月程度である。

ログの保存にかかる 1 年間のコストは企業・教育機関において 50 万円前後、行政機関においては約 80 万円となっている。

ログ保存の負担感は、事業や業務の形態、規模等に左右されることも考えられるが、全体の約 40%前後はログの保存を負担とは考えていない。また、約 50～60%はログの保存を負担ではあるが必要なことと考えており、これらを合計すると、約 90%以上がログの保存の必要性を認識している。

アクセスログの取得状況



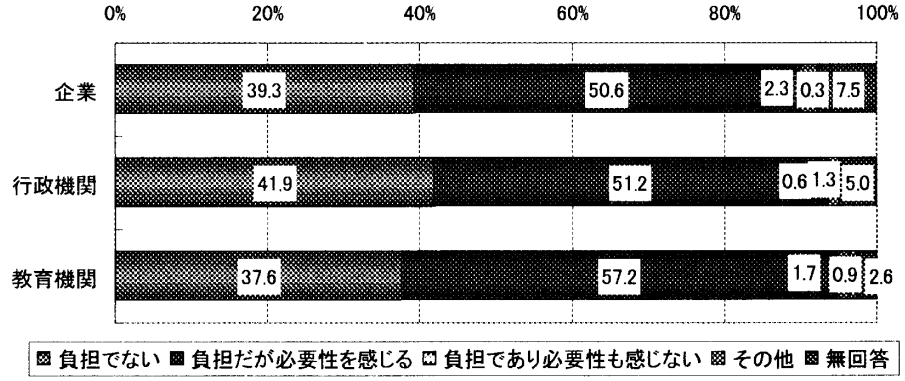
アクセスログの保存期間

	企業	行政機関	教育機関
トランザクションログ	180 日	230 日	200 日
サーバ上のアクセスログ	190 日	270 日	200 日
ファイアウォール上のアクセスログ	180 日	260 日	210 日
IDS のログ	220 日	290 日	200 日

アクセスログの保存コスト

	企業	行政機関	教育機関
ログ保存の平均コスト	55 万円	79 万円	48 万円

アクセスログ保存の負担感



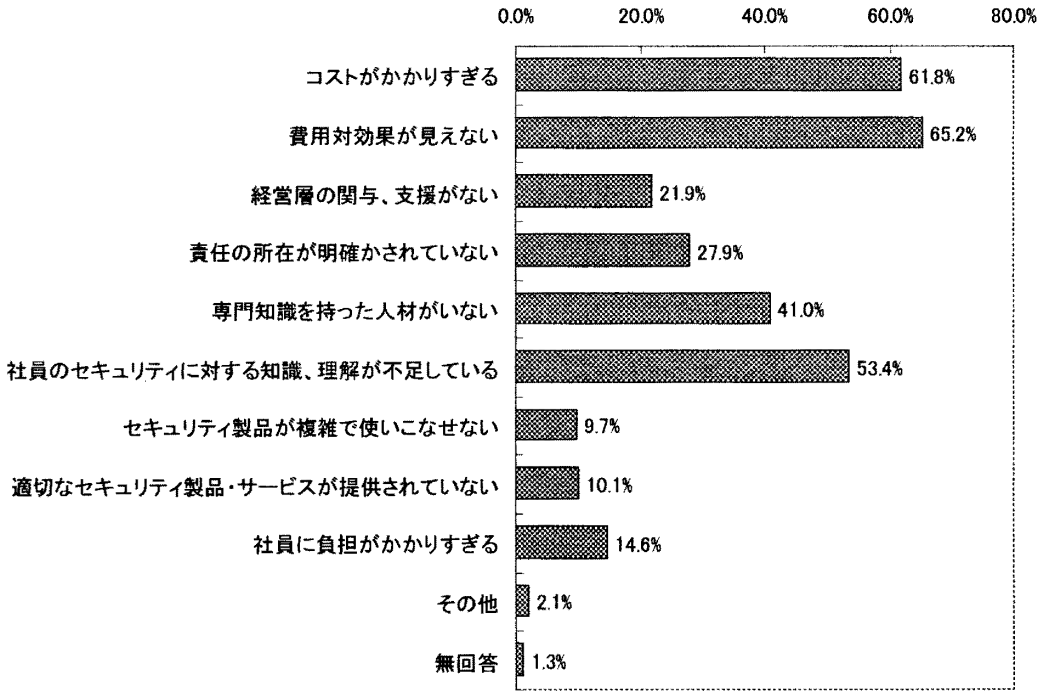
2．対策の在り方

アンケート調査の結果、セキュリティポリシーの策定率の低さ、脆弱性検査の実施率の低さ、無線ＬＡＮのセキュリティ対策の実施率の低さ等、必ずしも十分なセキュリティ対策が講じられていない実情が明らかになった。他方で、情報セキュリティに関連した被害は、上場企業に限っても、年間で復旧コスト 11.5 億円、逸失利益 7.9 億円、復旧に要する人日 23,011 人日と推計され、今後も一層の情報セキュリティ対策を講じていく必要がある。

(1)　人材の育成、意識の向上

アンケート調査によると、約 82%の企業でセキュリティ担当者が設置されているが、同時に、情報セキュリティ対策を行う上での問題点として、「社員のセキュリティ知識が不足」、「専門知識をもった人材がいない」といった点が指摘されており、今後、セキュリティに関連する人材の育成や、情報セキュリティ意識の向上を計っていくことが必要である。

情報セキュリティ対策を行う上での問題点　n=466



(2)　経営層の関与

「経営層の関与、支援がない」という点も、情報セキュリティ対策を行う上での問題点として指摘されている。セキュリティ担当者が問題意識を持っていても、上層部の認識が低ければ満足な対策を講ずることはできない。企業がＩＴへの依存度を高める状況にあって、情報セキュリティ問題は経営に直結する問題であり、経営陣が情報セキュリティの重要性を認識し、どのような資産をどのようなリスクからどのように

守り、また、どのようなリスクを残余リスクとして認識しそれに対してどのように対処するのか、といった判断を、企業における経営判断として行っていくことが求められる。

この場合、経営層には、情報セキュリティ対策に要するコストとこれにより得られるリスクの低減の相関関係に十分留意する一方、100%安全な情報セキュリティ対策は存在し得ないことを認識した上で、個別の情報セキュリティ対策について決定を下すことが望まれる。

(3) 行政機関・教育機関のセキュリティの向上

アンケート調査の結果からは、企業に比べて行政機関や教育機関のセキュリティ対策が遅れていることがうかがわれる。しかし、電子政府の実現に向けた取組みや学校教育のＩＴ化・ＩＴ教育の推進といった取組みが行われていることからも、行政機関・教育機関におけるセキュリティの向上は喫緊の課題である。

(4) 運用の重要性

情報セキュリティに対して関心が持たれている場合であっても、制度や組織だけ作って事足りるとされる場合が多い。しかし、情報セキュリティにおいて重要なのはこれらをいかに運用するかであり、セキュリティポリシー等の運用についてより意識が向けられることが必要である。

(5) 内部からの脅威へ対応

情報セキュリティに関する脅威の多くの部分が内部からの脅威であると思われる。アンケート調査においても、内部者のネットワーク悪用や社内からの不正アクセスが緊急に対処が必要な脅威として認識されている。

「外部のネットワークに接続されていないのでセキュリティ対策は不要である」といった考えは、内部犯行の脅威の大きさに鑑みれば無意味であり、内部からの脅威にも適切に対応することが必要である。

(6) 追跡性の確保

会議においては、追跡性の確保にも言及された。インターネットの特徴である匿名性と追跡性は相反するものではない。被害を被った場合に加害者に責任を追及できることは、被害回復の観点からも、また、威嚇的効果による将来の被害の防止という観点からも必要である。また、情報漏洩やウイルス等の被害に関してセキュリティ対策の不備等の責任を追及する訴訟やＷｅｂ等での誹謗中傷、ネット詐欺によって被害を受けた者が被害の賠償を求めて提起する訴訟の増加も予想されるなか、不当な責任追及を回避するという自己防衛の観点からも、追跡性を確保することが好ましいと思われる。

3. 官民連携の在り方

官民連携の重要性は第２章においても触れているが、会議においても、以下のような議論が行われた。

(1) 情報セキュリティ意識の向上

情報セキュリティの根本は、情報通信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）である点については、昨年度の報告書においても指摘したところである。

警察においては、情報セキュリティ・アドバイザーによる相談対応、情報セキュリティコミュニティセンターを通じた広報啓発活動等の活動を行ってきているが、引き続き情報セキュリティ意識の向上に向けた取組みの推進が求められる。特に、今後の情報通信ネットワーク社会の担い手となる一方で違法有害情報等による影響を最も受けやすい少年や、ネットワーク社会の進展に伴って新たにネットワークを利用することとなる者を対象とした活動について、被害者になることを防止するとともに無意識のうちに加害者・犯罪者となってしまうことを防止するとの観点から、その重要性が指摘された。

(2) 脅威の実態分析・評価に関する共通の基盤

官民が連携して情報セキュリティを高めていくためには、情報セキュリティ対策を講じていく上での基礎となる脅威の実態について共通の認識を有することが必要であり、事業あるいは業務の形態、規模等により資産が異なる点や脅威の性質により重要度や被害回復の困難度が異なる点を踏まえた上で、脅威の実態分析・評価に関する官民共通の基盤を有することの必要性が指摘された。

(3) 情報発信

情報セキュリティについては、これまでも政府や警察において様々な取組みがなされてきたところであるが、それらの取組みに関する情報や政府・警察の有する問題意識が、必ずしも広く伝わっていないとの指摘がなされた。

政府や警察からの情報発信の強化が求められる。

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。

- 岡野　直樹
- 加藤　雄一
- 桑子　博行
- 別所　直也
- 東　　貴彦
- 吉岡　初子

（五十音順、敬称略）

岡野　直樹

本年度の会議の目的である脅威の実態の把握において、まず、調査が実施できたこと自体が有意義であったと言えよう。

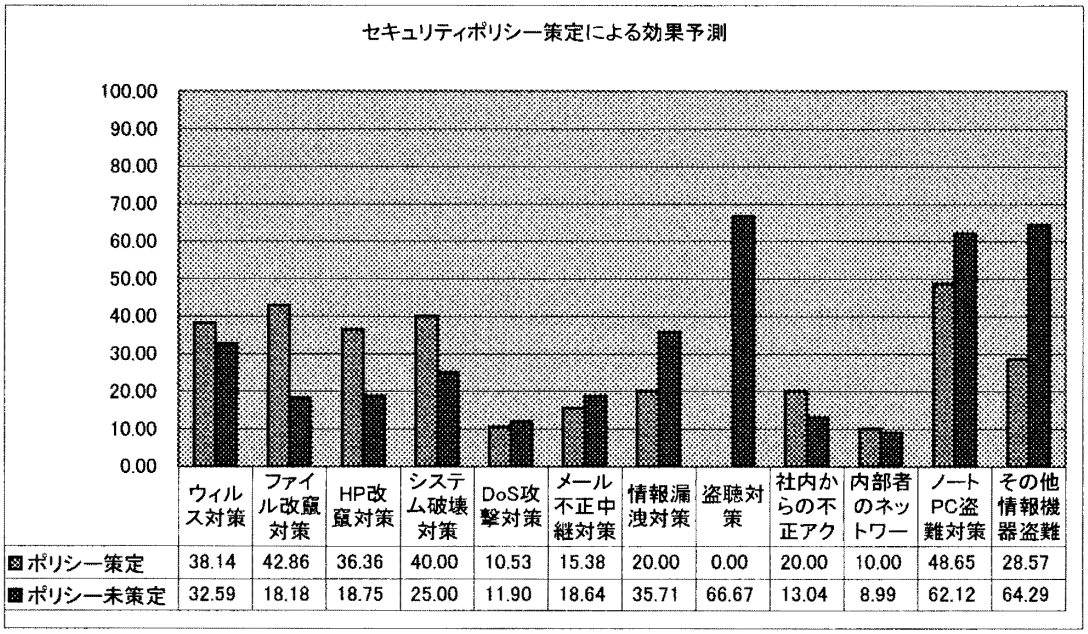
また、本調査の結果から、セキュリティ対策の実施状況、それに対する事件・事故の発生状況や実害の発生状況に関する、ある程度の実態が把握できるのではないだろうか。

ここで、特に企業におけるセキュリティ対策と効果について、別冊「ハイテク犯罪等に係る被害状況の調査」のデータを基に独自に集計し予測することを試みてみたい。

効果の予測については、実害発生率を以下の計算式により求め、対策の実施の如何による実害発生率の違いを見ることにする。

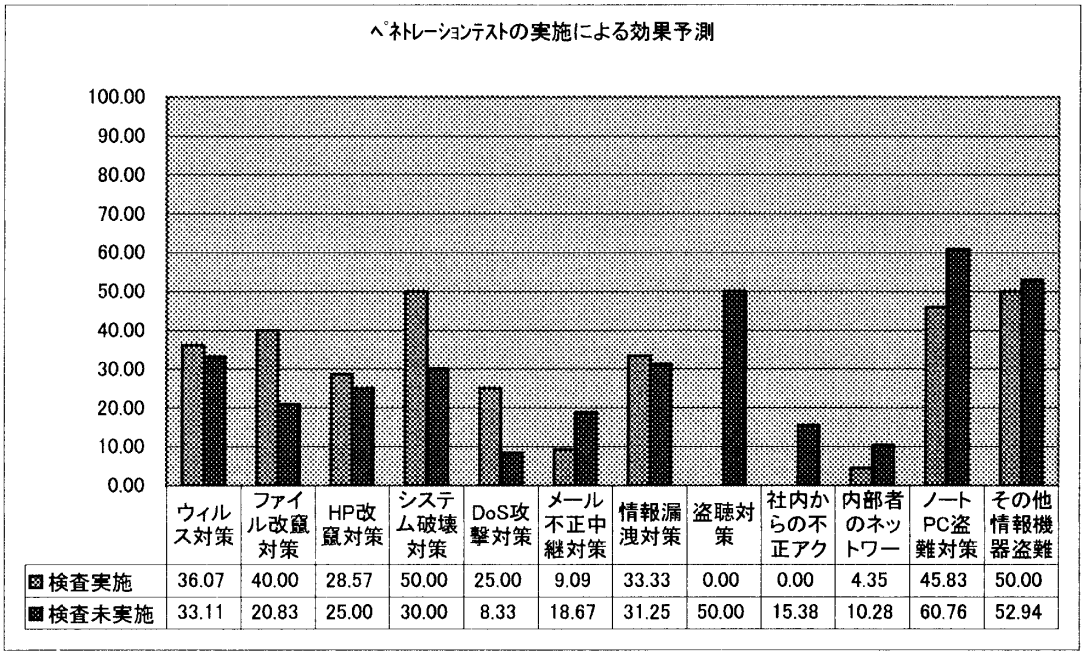
実害発生率　＝　実害発生企業数 / 事件・事故発生企業数 ×　１００

なお、注意しておかなければならないのは、アンケートでは事件・事故および実害の明確な定義が無く、回答企業の主観によるものであること、また、これらを検知するための機器の設置や調査などが行われていなければ、そもそも回答企業が実態を把握できていない可能性があるなど、データ自体の不安定要因が多く定量的な分析が難しいことである。



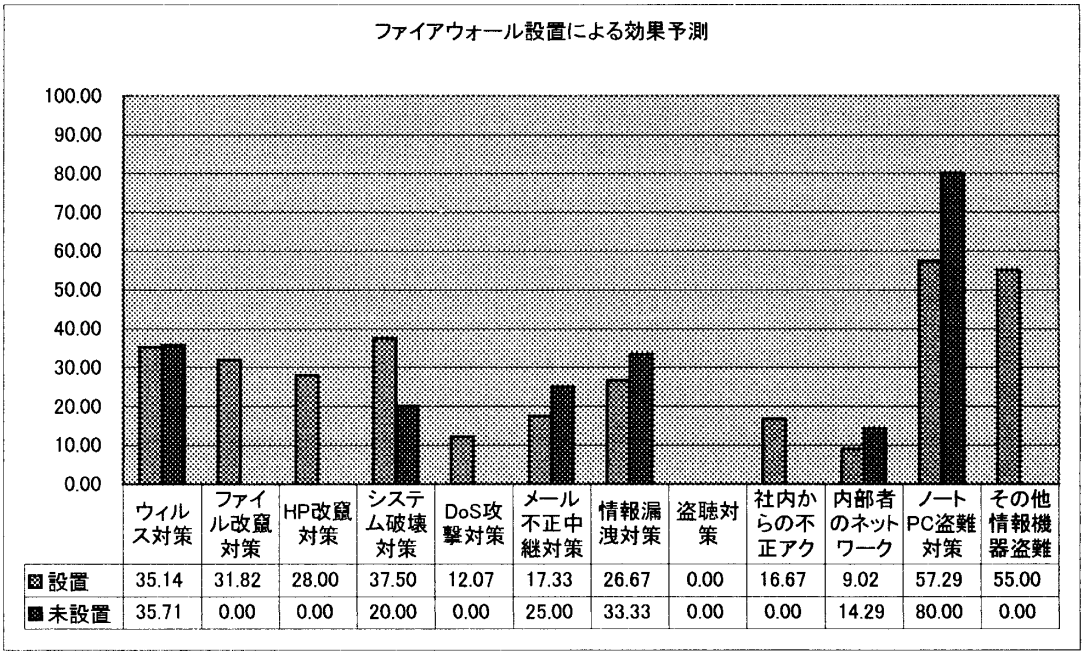
	ウィルス対策	ファイル改竄対策	HP改竄対策	システム破壊対策	DoS攻撃対策	メール不正中継対策	情報漏洩対策	盗聴対策	社内からの不正アク	内部者のネットワー	ノートPC盗難対策	その他情報機器盗難
ポリシー策定	38.14	42.86	36.36	40.00	10.53	15.38	20.00	0.00	20.00	10.00	48.65	28.57
ポリシー未策定	32.59	18.18	18.75	25.00	11.90	18.64	35.71	66.67	13.04	8.99	62.12	64.29

図１　セキュリティポリシー策定による効果予測



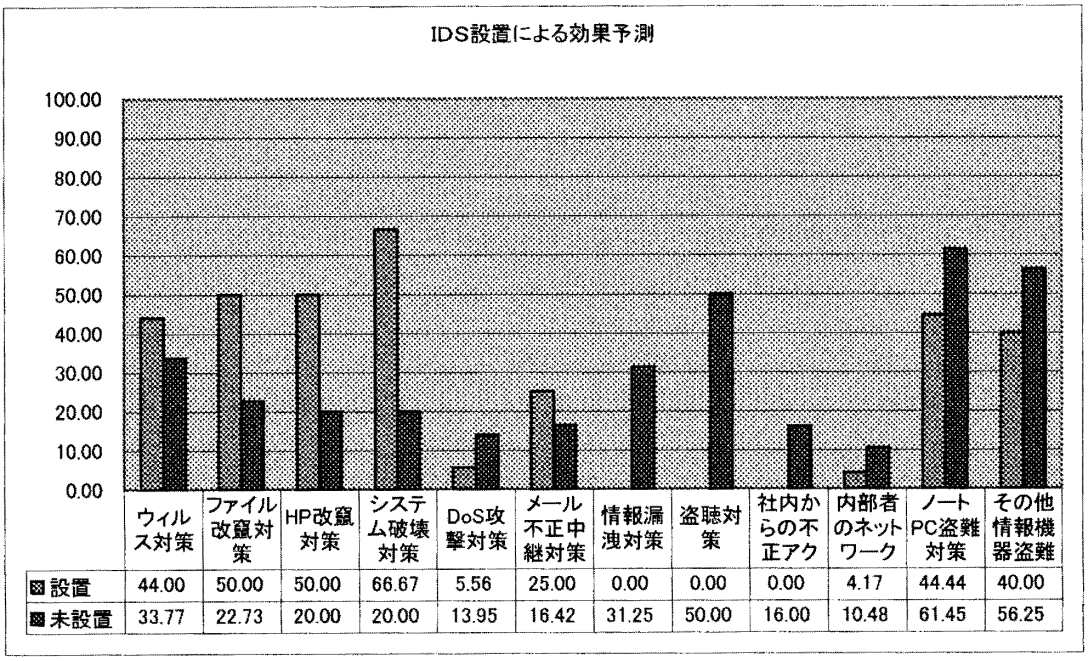
	ウィルス対策	ファイル改竄対策	HP改竄対策	システム破壊対策	DoS攻撃対策	メール不正中継対策	情報漏洩対策	盗聴対策	社内からの不正アク	内部者のネットワー	ノートPC盗難対策	その他情報機器盗難
▨検査実施	36.07	40.00	28.57	50.00	25.00	9.09	33.33	0.00	0.00	4.35	45.83	50.00
▩検査未実施	33.11	20.83	25.00	30.00	8.33	18.67	31.25	50.00	15.38	10.28	60.76	52.94

図２ ﾍﾟﾈﾄﾚｰｼｮﾝﾃｽﾄの実施による効果予測



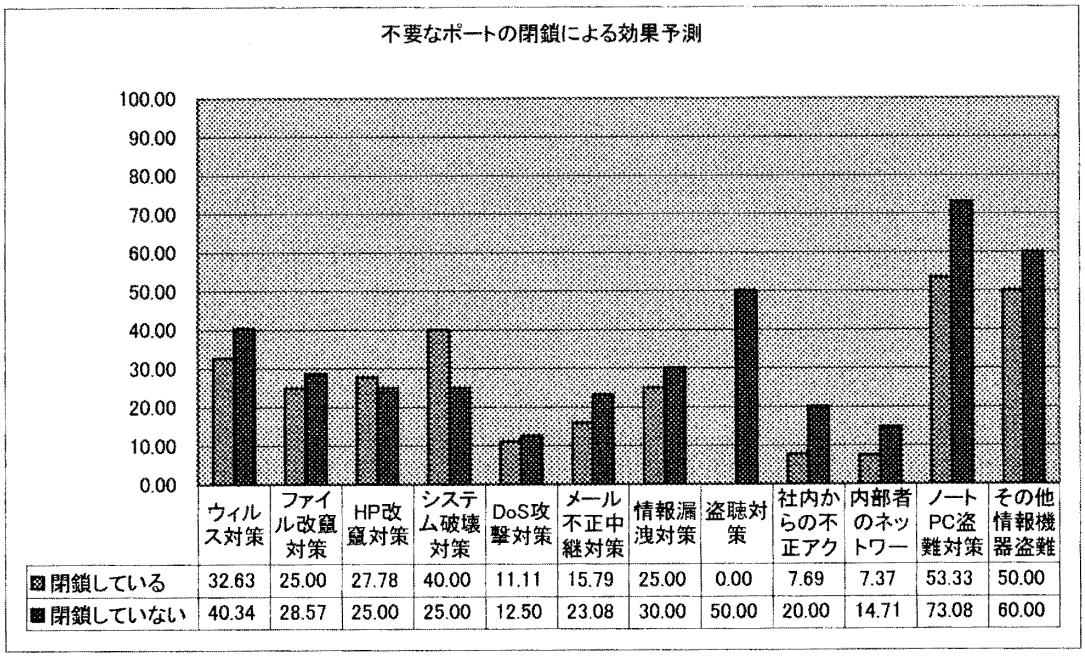
	ウィルス対策	ファイル改竄対策	HP改竄対策	システム破壊対策	DoS攻撃対策	メール不正中継対策	情報漏洩対策	盗聴対策	社内からの不正アク	内部者のネットワーク	ノートPC盗難対策	その他情報機器盗難
▨設置	35.14	31.82	28.00	37.50	12.07	17.33	26.67	0.00	16.67	9.02	57.29	55.00
▩未設置	35.71	0.00	0.00	20.00	0.00	25.00	33.33	0.00	0.00	14.29	80.00	0.00

図３ ファイアウォール設置による効果予測



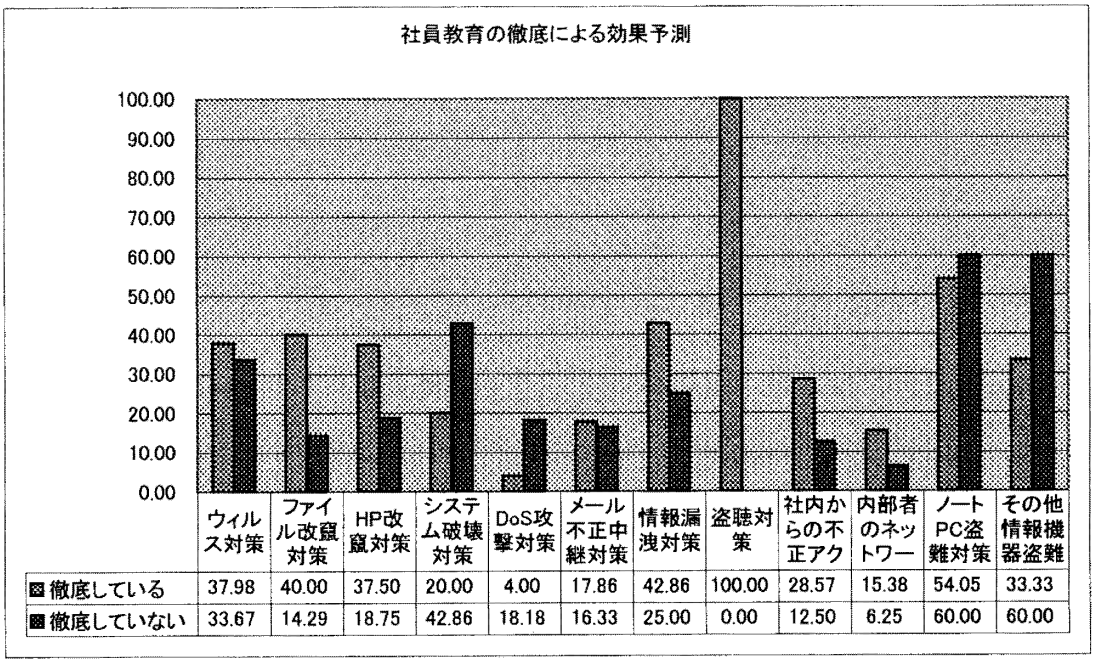
	ウィルス対策	ファイル改竄対策	HP改竄対策	システム破壊対策	DoS攻撃対策	メール不正中継対策	情報漏洩対策	盗聴対策	社内からの不正アク	内部者のネットワーク	ノートPC盗難対策	その他情報機器盗難
設置	44.00	50.00	50.00	66.67	5.56	25.00	0.00	0.00	0.00	4.17	44.44	40.00
未設置	33.77	22.73	20.00	20.00	13.95	16.42	31.25	50.00	16.00	10.48	61.45	56.25

図4　ＩＤＳ設置による効果予測



	ウィルス対策	ファイル改竄対策	HP改竄対策	システム破壊対策	DoS攻撃対策	メール不正中継対策	情報漏洩対策	盗聴対策	社内からの不正アク	内部者のネットワー	ノートPC盗難対策	その他情報機器盗難
閉鎖している	32.63	25.00	27.78	40.00	11.11	15.79	25.00	0.00	7.69	7.37	53.33	50.00
閉鎖していない	40.34	28.57	25.00	25.00	12.50	23.08	30.00	50.00	20.00	14.71	73.08	60.00

図5　不要なポートの閉鎖による効果予測



	ウィルス対策	ファイル改竄対策	HP改竄対策	システム破壊対策	DoS攻撃対策	メール不正中継対策	情報漏洩対策	盗聴対策	社内からの不正アク	内部者のネットワー	ノートPC盗難対策	その他情報機器盗難
徹底している	37.98	40.00	37.50	20.00	4.00	17.86	42.86	100.00	28.57	15.38	54.05	33.33
徹底していない	33.67	14.29	18.75	42.86	18.18	16.33	25.00	0.00	12.50	6.25	60.00	60.00

図６ 社員教育の徹底による効果予測

集計結果（図１～図６）から以下のようなことが予測できる。

外部からの脅威による事件・事故および実害について

- 最も高い、コンピュータウィルス感染については、不要なポートの閉鎖による効果が得られていること。
- 二番目に高い、メールの不正中継については、ペネトレーションテストによる効果が最も高いこと。
- 三番目に高い、ＤｏＳ攻撃については、ＩＤＳの設置による効果が得られていること。

内部やその他の脅威による事件・事故および実害について

- 最も高い、内部者のネットワーク悪用については、セキュリティポリシーの策定や社員教育の徹底では、逆に実害が多く発生していること。おそらく各対策による本来の目的と相反する結果であろう。
- 二番目に高い、ノートＰＣの盗難については、ここに上げられる全ての策定による効果が得られていること。おそらくセキュリティに対する対策意識が高い企業ほど盗難に対する対策意識も高いということであろう。
- 三番目に高い、システム破壊などについて、社員教育の徹底による効果が得られていること。

ただし、セキュリティ対策を実施したにも関わらず、逆に実害が発生していることになっているものが多くある。これは、セキュリティ対策を施す企業ほどアクセス数が多く、事件・事故および実害の発生が多く、また実害に対する定義が厳格であること、ま

たは、実害が発生したために、その後にセキュリティ対策を施していること、などが原因として考えることができる。

その他のセキュリティ対策について、特に、セキュリティパッチの適用による効果、ウィルス感染防止対策による効果なども、大変興味があるところである。

以上、企業におけるセキュリティ対策と効果について予測することを試みたが、上述の注意点などを鑑み、結果については参考と考えて頂きたく、アンケートのデータの活用方法について、効果的なセキュリティ対策が実施されるための啓発資料の参考となればと考えるところである。

なお、より定量的なキュリティ対策の効果予測をするためには、アンケートの内容として以下が加味されるべきであろう。

- 事件・事故および実害の定義の明確化
- 事件・事故および実害の発生回数（規模）
- サイトへのアクセス数（規模）

今後、このような調査が繰り返し実施されることが、脅威の実態を把握するだけでなく、企業、行政機関、教育機関などにおいて、セキュリティ対策の必要性が認識され、より洗練された知識が身に付けられ、より効果的なセキュリティ対策が実施されるための、啓発となることが考えられ、そのようになることを望んでいる。

加藤　雄一
桑子　博行
別所　直哉

● 私たちは、平成１３年度の会議においても、わずか３回程度の会議しか経ないで報告書が作成され、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ていないことの問題を申し上げたところでございます。今回、また十分な議論がなされているとはいえない段階で、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報告書が取りまとめられることについての懸念があることを改めて申し上げさせていただきたいと考えております。特にインターネットの発展及び産業界の利益と規制ないし産業界の負担の調和に関する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前提となる問題について十分な議論がされないまま本会議の報告書における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．セキュリティに関する実態把握及び問題点の分析については、事業者にとっても重要な問題であると認識しております。しかしながら、セキュリティ対策については基本的には事業者が想定されるリスクとコストのバランス、技術動向等を勘案の上、自らの判断において犯罪予防や犯罪捜査とは別個の観点で取り組むべき問題であります。なぜならば、日々新たに生起するセキュリティ上の脅威に対しては、事業者の自主的取組みによる方が、より柔軟に対応できるためであり、また、事業者にとっては、自らの信用を維持し、事業を継続するためには、犯罪予防や犯罪捜査とは関係なく、自主的にセキュリティ対策を講じるインセンティブを有しているためです。

また、今回の報告書案においても警察等との連携が強く述べられていますが、事業者としては、プライバシーや個人情報、通信の秘密の保護、あるいは負担の問題を度外視した連携を行うことは困難であります。従いまして、この問題に関しては事業者の判断を第一に尊重すべきと考えます。

→ 本会議においては事業者の自主的対応ではまかなえない部分についての対応の要否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、我が国のインターネット業界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．今回の報告書

第５章及び第６章におきましては、警察庁において行ったアンケート結果をもとに脅威の実態把握・分析及びそれに対する対策が述べられておりますが、何を脅威として捉え、どのような対策を講じるかについては、各事業者や設備の設置者ごとに全く異なった事情があり、それぞれの事情のもとで判断されていくものであり、個別の事情を捨象した分析を行い、対策を論じることに意味があるとは思われません。

→　例えば、「アクセスログ保存の負担感」についてのアンケート結果ですが、事業者は業務の必要上アクセスログを保存しているのであって、セキュリティ対策により業務の必要以上に保存を行うことが負担かどうかについて企業等がどのように感じているのかがアンケートからは明らかではありません。報告書にある、約９割がログの保存の必要性を認識している、という記述は必ずしも正確ではなく、誤解をまねきかねないと考えます。

→　何を情報セキュリティ上の脅威と捉えるかについても、慎重な検討が必要だと考えます。警察庁が今回実施したアンケートにおいては、ノートＰＣの盗難、ネット上の誹謗中傷、ネット詐欺、著作権・商標権侵害などがハイテク犯罪として位置付けられており、第６章では、これらの犯罪の被害実態を元に対策が論じられています。しかし、メールの不正中継、DoS 攻撃、内部者のネットワーク不正悪用、不正アクセスなどと比べると、重要度や被害回復の困難度が異なると言わざるを得ません。このように、情報セキュリティ上の脅威を、重要度や被害回復の困難度を捨象して総花的に論じることは、現実的な対応とはいえず、議論の対象を整理する必要があると考えます。

→　第６章で言及されている各対策も各事業者のビジネスモデルに応じて経営判断の中で講じていくべき問題であり、一律に必要性を述べることには違和感を覚えます。

→　第６章の２．（６）では、追跡性を確保することが好ましいと提言されており、その理由として、情報漏洩やウィルス等の被害に関してセキュリティ対策の不備等の責任を追及する訴訟や、Ｗｅｂ等での誹謗中傷、ネット詐欺の被害者による損害賠償請求訴訟から自己防衛をする必要があることが述べられています。これは、事業者の利益を考慮してのご提案と理解しますが、一方で加害者の追跡性を確保することは、プライバシー保護や通信の秘密といった基本的人権の保護の要請と相反しますし、事業者側のコスト負担増にもつながります。また、因果関係や予見可能性の欠如から、個別の事例では、事業者側に必ず責任が生じるとも言えません。現実には、事業者としては、加害者の特定が困難であることを前提として、実務や裁判を通じて培った、自主的取組みにより、上記のような訴訟リスクの軽減を図っております。したがって、本論点を報告書中に盛り込むことに関しては、慎重な検討が必要と考えます。

３．我が国全体としてのセキュリティ対策、特に政府と民間との連携を検討するにあたっては、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。今回の報告書案ではアクセスログの保存についての言及がなされていますが、上記のような問題を強く含むものであり、少なくとも私たちとしては慎重な検討を要するものと考えております。また、

議論を行うに際しては、いわゆるハイテク犯罪全般を総花的に射程に入れるのではなく、情報通信ネットワークの安全性及び信頼性に直接脅威を及ぼす要因に対象を限定すべきと考えます。

4．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ることに注意すべきと考えます。

東　貴彦

報告書の内容は、一般的なセキュリティ対策の不足点を端的に取りまとめており、政府機関や企業が認識しなければならないポイントを再確認するための良い材料になりうると考えます。情報セキュリティ上のリスクを回避するには利用者全員がそのリスクを認識した上で情報通信インフラを利用する意識と知識が求められますが、一般にいずれも低いレベルにとどまっていることは報告書の指摘するとおりです。従って今後行政、警察、産業界から様々な形で啓蒙、技術的対策の提案、法制度や運用による抑止が進められる必要がありますが、とりわけ法制度とその運用（例えば追跡性の確保）についてはプライバシー保護など個人の基本的な権利にかかわる微妙な問題をはらみます。ついては従来にもまして十分な説明と事前同意（informed consent）の尊重に配慮がなされることを希望します。

また、社会的インフラとなった情報通信システムについて官民連携して対処することの重要性は報告書が随所で指摘し呼びかけている通りと考えますが、ただし時として利害の相反する当事者間で連携を維持推進することは大きな困難が伴います。官民連携の実効を上げるためにも双務的で互恵的な連携プログラムの開発と表現上の工夫が必要と考えます。

吉岡　初子

昨今のインターネット等のめざましい進展と普及状況は、利便性を広げる一方、多くの問題が発生している事を危惧しています。

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の整備が重要であることは、昨年も述べたとおりです。

従って情報セキュリティの充実強化は不可欠であることは言うまでもありませんが、同時に、プライバシーや通信の秘密など、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事態は避けなければなりません。

こうした観点から、今年の審議にあたって、十分な審議ができる時間を取ってほしい旨、申し上げましたが、今年も拙速ではなかったかと納得できないものがあります。

今回のテーマは情報セキュリティに関する脅威の実態把握・分析に焦点を当てていますので、ウィールス問題、HP 改ざん、システム破壊、情報漏洩等ハイテク犯罪の実害状況等に言及していることは当然ですが、ネット詐欺やノートパソコンの盗難までが上げられていますと、整理が不十分であるかのような誤認を招きます。アンケート結果の分析、評価等については更に精査する必要があります。

今回の調査対象は、企業、行政、学校ですが、情報セキュリティに対する脅威の実態を把握するには一般の消費者、利用者を対象にアンケートを実施し、消費者の立場を充分配慮した内容を盛り込むことが大切だと思います。

また、情報セキュリティの確保は重要ですが、消費者、利用者としては情報セキュリティの確保という大義名分によって、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、取り締まりの範囲が際限なく広がり、無意識のうちに犯罪者とされてしまうことについても強い懸念を持っています。

情報通信分野の進展が急速であることを鑑みれば、関係省庁との連携が不可欠だと考えますので、この点についても配慮されることを望みます。