NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

IT セキュリティ対策施策の導入・実施状況とその満足度調査

集計結果報告書

２００５年１月

特定非営利活動法人　日本ネットワークセキュリティ協会

目　次

JNSA　政策部会　マーケットリサーチ・ワーキンググループ

ワーキンググループリーダー
　玉井　節朗　　株式会社ＩＤＧジャパン

ワーキンググループメンバー
　渡部　真江　　株式会社アークン
　浜武　千恵　　株式会社アークン
　前田　浩　　株式会社アークン
　塚本　卓郎　　ＩＤＣ Japan 株式会社
　荒川　弘　　株式会社ＩＴサービス
　番野　邦彦　　キヤノンシステムソリューションズ株式会社
　郷間　佳市郎　京セラ コミュニケーションシステム株式会社
　飯島　邦夫　　クオリティ株式会社
　山田　勝志　　クオリティ株式会社
　勝見　勉　　グローバルセキュリティエキスパート株式会社
　依田　真一　　コンピュータ・アソシエイツ株式会社
　金子　以澄　　コンピュータ・アソシエイツ株式会社
　小川　博久　　株式会社シーフォーテクノロジー
　中津　有美　　株式会社ジェイエムシー
　米澤　一樹　　セキュアコンピューティングジャパン株式会社
　斉藤　麻衣子　トレンドマイクロ株式会社

［エグゼキュティブ･サマリー］　（概容要約版）

日本ネットワークセキュリティ協会（ＪＮＳＡ）政策部会 マーケットリサーチ･ワーキンググループでは、「IT セキュリティ対策施策の導入･実施状況とその満足度調査」と題する調査を実施した。調査は 2004 年８月から９月にかけて、郵送によるアンケート調査方式で実施、上場･非上場の全国主要企業の情報システム担当役員･部長クラスに対し 3166 通を発送して、全体の 13.1%に当る 416 社から回答を得た。その結果の概要は中間報告として 2004 年 10 月 29 日に JNSA 主催の NSF2004 の中で発表し、同時に報道に対しても情報提供を行った。

［調査項目］

調査は 1)情報セキュリティに対する社内体制の整備状況、2)情報セキュリティガバナンスに対する取り組み状況、3)IT セキュリティ対策ツールの導入状況の３カテゴリーについて実施･導入の有無を尋ねた。また同時にこれら施策に関する外部サービスの利用状況と、導入したツールやサービスに関する満足度も確認した。特にサービスの利用状況や製品･サービスの満足度については調査事例が少なく、ユーザー実態の一端を把握するためのデータとして貴重なものと言える。

［調査結果の概要］

１．情報セキュリティに対する社内体制の整備状況

- 担当部署や要員の配置については、特に定めていないとしたのが 16%で、８割以上が対応体制を敷いている。
- 専任部署 26%、非専任の担当部署 28%と、過半数が担当部署を置いており、残り 30%は部署までは指定していないが専任または兼任で要員を手当てしている。
- 担当役員の設定については 26%の企業で CSO（セキュリティ対策担当役員）または CISO（情報セキュリティ対策担当役員）を指定しており、CIO（情報システム担当役員）または CEO（最高経営責任者または社長）が所管する企業も 31%ある一方、まだ 44%の企業が役員レベルでの所管を定義していない。
- 経営資源としての情報の位置づけ、あるいは経営リスク対策対象としての情報の認識がまだ十分に浸透していないことを示している。

２．情報セキュリティガバナンスに対する取り組み状況

1) 情報セキュリティポリシーについて

- 情報セキュリティポリシーを策定済みの企業が 56%、策定中または検討中が 37%と、合わせて 93%が情報セキュリティポリシーを制定（または予定）している。
- これは対応体制の整備以上に高率で取り組まれていることを示しており、予想以上に「セキュリティポリシー」が定着していることが確認された。
- また、その運用（日常の管理に対する反映）や見直しについても、ポリシーを策定済みの企業ではほぼ全数が「運用できている」状態であり、定期･不定期を問わず見直し･更新を行っている企業も 87%に上る等、セキュリティポリシーを経営管理の中で生かしている姿勢が鮮明に読み取れた。

- セキュリティポリシーの策定や運用に関するサービスの利用については、策定で 15%程度、運用・見直しでは数%と、利用は活発ではない。
- サービスの利用者における不満はそれ程顕在化していないが、コンサルテーションがステレオタイプで自社の実態に合わないと感じているところも相当数ある模様。
- セキュリティ管理に関する ISMS 等の公的認証は 48%が取得済みまたは取得意向を持っており、かなり定着してきたと言える。

2) プライバシーポリシーについて

- 「策定の予定はない」としたのが 17%あり、また策定予定が 47%を占めるなど、情報セキュリティポリシーに比較してその定着度は低い。
- プライバシーマークも過半数が取得予定はないとしており、個人情報保護法の全面施行が迫る中、対策への関心が急速に高まっている反面、具体的対応策にまだ戸惑いを持っている企業が相当数あることを示唆していると見られる。

3．IT セキュリティ対策ツールの導入状況

1) セキュリティ対策ツールの普及状況

ファイアウォール：	96%（うち予定･検討中 1%）
侵入検知･防御システム：	64%（うち予定･検討中 14%）
ウイルス対策システム：	97%（うち予定･検討中 0%）
ウイルス以外のコンテンツセキュリティ	67%（うち予定･検討中 13%）
（アンチスパム、ウェブフィルタリング、アンチフィッシング等）	
個人認証及びユーザーＩＤ管理	95%（うち予定･検討中 3%）
リモートアクセスの安全対策	84%（うち予定･検討中 5%）
脆弱性検査・ポリシー監査システム	57%（うち予定･検討中 19%）

- 以上から、ネットワークセキュリティ対策の最低限の必要技術である個人認証、アンチウイルス、ファイアウォールはほとんどすべての企業で導入されていることが確認された。
- 一方、防御の質や安全度をいっそう高めるために役立つとされる侵入検知やコンテンツ対策については半分程度、導入予定や検討中を含めれば３分の２程度の普及率となっている。これはその導入や運用の難易度からすれば比較的高い数字と言え、防御対策技術・手法が相当浸透していることを示している。これに対し、脆弱性検査については 4 割を切り、予定を含めても 57%と、普及は今一歩の感がある。

2) アプライアンス製品の利用状況

- セキュリティ対策ツールでは、近年ハードウェアと対策ソフトが一体となったアプライアンス製品の提供が活発である。そこで今回調査では各対策カテゴリーの中でアプライアンスの利用程度についても調べた。
- 複数回答で「アプライアンスを導入」とした比率は、ファイアウォール 59%、侵入検知･防御 22%、ウイルス対策 16%、という結果となった。特にファイアウォールについては比較的早くからアプライアンス化が進んでおり、その普及率も 60%に迫るところまで来ていることが確認できた。

- 今回１回の調査では結論を出すわけに行かないが、趨勢的にはアプライアンス化の方向は強まるものと推測される。

3) 外部サービスの利用状況

- ファイアウォールや侵入検知はその導入･設定･運用に高度な技術を必要とすることから、それらをまとめてアウトソースサービスとして提供するベンダーが多数存在している。今回は併せてその利用の普及度も探った。
- 第三者による監視･運用サービスを導入しているとした企業は、ファイアウォールが 20%、侵入検知･防御が 15%、ウイルス対策が 18%、コンテンツセキュリティ対策が 11%、脆弱性検査が 24%という結果であった。その技術的専門性の価値の割には低い数字と思われる。
- 監視･運用とは別の意味となるが、他に外部サービスの利用としては電子認証サービス（いわゆる PKI 等）が 4%とまだ極めて低く、VPN サービスが 18%という結果であった。
- 結局ネットワークの構成や運用政策といった内部情報を第三者に提供する必要のあるサービスについては、まだ導入に躊躇があるものと見られ、プロフェッショナルによる高度のサービスに価値を見出すアメリカ型のカルチャーに移行するには、更に時間と意識の転換が必要なように思われる。

４．セキュリティ製品･サービスに対する満足度

- 満足度は製品・サービスを区別せず、「不満はない」「機能に不満」「性能（パフォーマンス･スループット）に不満」「品質･信頼性に不満」「費用対効果に不満」の５項目に類型化して訊いた。
- 製品によって無回答のものも多く、回答があったものだけの中で比率をとると、何らかの不満を回答した比率は、ファイアウォール：19%、侵入検知･防御：24%、ウイルス対策：30%、コンテンツセキュリティ：29%、個人認証：46%、リモートアクセス：30%、脆弱性検査･ポリシー監査：24%と、おおむね有効回答数のうち 25～30%のユーザーに何らかの不満があることがわかった。
- なお、個人認証についてだけは「個人の使い方、管理の面で不満、不安」という選択肢を追加したところ、これだけで 30%の回答者が不満･不安を訴えており、結果として不満の比率を押し上げている。個人認証においてはその運用上の最大の課題が個人の対応の問題であり、一人ひとりの意識や自覚、教育についての課題が大きいことを示している。
- 不満について求めた自由記入では、コストへの不満、設定の難しさ、データ更新頻度･スピードの問題、マシン負荷が大きい、誤報･誤検知問題、ログの解析の困難さ、ベンダーのサポート対応に対する不満、パフォーマンスの低下やハングアップ、サービス業者の応答の悪さ等を指摘する声が目立った。

エグセキュティブサマリ：以上

第一部　調 査 概 要 編

１． はじめに

ＮＰＯ日本ネットワークセキュリティ協会（JNSA）では、IT セキュリティの研究･普及･啓発のためにさまざまな活動に取り組んでいる。多岐にわたる活動テーマの中のひとつの課題として､IT セキュリティにおけるユーザー実態に関する情報の入手というテーマがあった。実際、IT セキュリティ業界においては、各ベンダーが自社のユーザーの状況についての情報を個別的に持っていることはあり得ても、業界としてその全体像を捉える方法も機会も、今まで持ち合わせていなかったというのが実態である。

今回、JNSA の政策部会内部で、そのような調査に対する取り組みの声が上がり、有志を募って実態調査に取り組むこととなった。そこで、2004 年度の政策部会活動の一環として、マーケットリサーチ･ワーキンググループを結成し、市場調査活動を行った。この種の調査においては、一部市場調査企業がベンダーサイドの情報を集合する形で調査報告を出しており、また研究機関やユーザー団体が部分的にセキュリティ対策の普及度を調査することがあった。今回はそれらとは視点を変えて、対策施策の普及度を確認しつつ、その満足度と問題点についても調査することを試みた。

なお、アンケートの作成と調査方法については、社団法人日本システムユーザー協会（JUAS）のご指導とご協力を得た。またアンケートの発送に関しては株式会社 IDG ジャパンの全面的なご協力をいただいた。ここに報告書を上梓するに当たって、特に記してお礼を申し上げたい。

２． アンケート調査実施の目的

今回のアンケート調査の実施に当っては、ユーザー企業におけるセキュリティへの取り組み状況と、ユーザーが抱えている取り組み上の問題点を拾い上げることを狙いとした。

特に満足度調査は、主としてセキュリティ対策ベンダーの集まりである JNSA として、マスとしての顧客実態を知る上で興味深いテーマであった。

これらの点を考慮して、アンケートの調査項目としては、1)セキュリティの取り組み体制 2)情報セキュリティガバナンスの定着状況　3)セキュリティツールまたはサービスの導入状況　4)その問題点　の４カテゴリーとした。

具体的には、1)第一部の回答企業プロファイルの中で回答企業の規模や業種とともに、情報セキュリティ対策部署･要員や担当役員の状態を確認､2)第二部でセキュリティポリシーの策定状況とセキュリティ管理に関する公的認証、プライバシーポリシーの策定状況とＰマークの取得状況について質問、3)第三部において、代表的な IT セキュリティ防護策について、ツールやサービスの導入状況とその満足度について質問、という構成とした。

情報セキュリティに関する調査においては、通常、ネットワークセキュリティの防護対策については、具体的な情報を聞き出すことが極めて困難であり、また導入製品のメーカーや機種についての情報は出す方も受け取る方も取り扱いに慎重にならざるを得ない。これらの点について具体的な解答を求めるような質問は、回答数の減少につながる可能性をはらんで

いる。

今回は、多数のサンプルに基づいてユーザー実態をマクロで捉えたいという狙いを持っていたので、できるだけ多くの回答が得られるように意識した。そのために、回答は極力類型的な選択肢から選ぶ形式とし、個別具体的な回答をあえて求めないものとした。結果としては下記に記すように多くの回答を得ることができ、企業におけるセキュリティ対策の現状をマクロ的に示すデータが得られたものと考えている。

3． アンケート調査の概要

今回のアンケート調査の概要は次の通りである。

3.1 実施時期：　2004 年８月２７日発送
2004 年９月１５日締切

・実際には、締め切り期日を過ぎてから到着する回答票が相当数あり、できるだけ多くのサンプルを統計に反映することと、せっかくのご回答を生かす意味で、９月中に事務局に到着した回答は全て集計対象とした。

3.2 方法：　調査票の発送も回収も全て郵送によった。

3.3 調査票の発送対象：　全国の上場・非上場の企業を対象に、原則として情報部門の担当部長以上の、固有名詞が確認できる方を対象とした。

また、JNSA 会員企業に対しては全社を対象としてご協力を願った。

これらを合せた質問票発送総数は 3,166 件である。

今回は企業ユーザーに対象を限定し、政府、地方公共団体、医療、教育等の分野は対象から除外した。社会全体の状況を知るためには、これらの分野についても調査対象として行きたいが、相手先の特定やデータベースの整備状況ならびに入手可能性の問題から今回は見送った。今後の課題としたい。

3.4 回答回収数と回収率：　回答票の回収総数は 416 件で、回収率は 13.1%

一般的なアンケート調査の場合の回収率が数パーセントと言われる中で、13.1%という回収率は極めて高いものと理解しており、セキュリティに対する関心の高さを確認できるひとつの指標となったものと考えている。

なお、この種の調査における回答促進のインセンティブとして金品や情報の提供を約束するケースが多いが、今回は JNSA が送料実費負担で配布しているセキュリティ対策講座「ネットワーク社会のここが危ない!!」の CD-ROM つき冊子の提供と、調査結果公表時（分析結果は一般公開を予定）に通知を差し上げることを提示した。どちらの情報も、アンケートの回答の有無によらずに入手可能なものではあるが、多少回答を促す作用をした可能性はあると想像される。

第二部　分　析　編

第一章　回答企業のプロフィール分析

1　回答企業の業種と企業規模の分布

回答企業 416 社の業種と企業規模の分布は以下の通りとなった。

1.1 業種別の分布

業種については図 1 に示すように簡素化のために５分類に絞り込んで訊いた。

製造業関連が 35%、情報･ソフトウェア関連が27%とこの2業種で過半を占める。金融はさすがに 5%と少ないがサンプル数は 22 あり、統計的に有意の回答数が得られた。ほぼ全業種をバランスよくカバーできていると思われる。

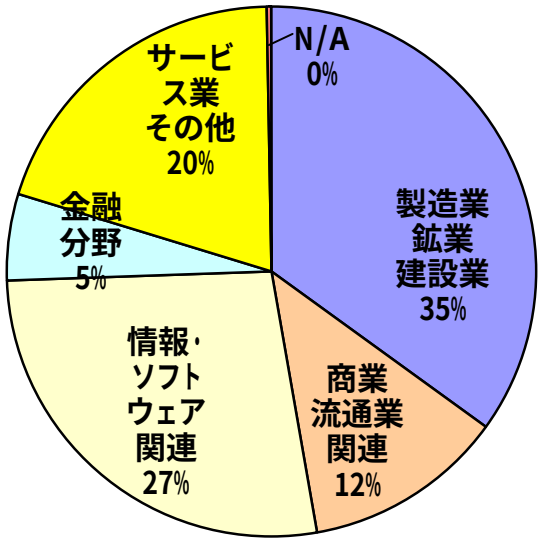


図 1　回答企業の業種分布

1.2 企業規模の分布

企業規模については、売上高と従業員数について回答を求めた。売上高 100 億円未満の中小企業が 27%、100 億円以上 1000 億円未満の中堅企業が 38%、1000 億円以上の大企業が 31%と、売上規模別には中小、中堅、大企業をバランスよく網羅できた。(図 2)

従業員数については 100 名未満が 9%、100 名以上 500 名未満が 30%、500 名以上 1000 名未満が 15%、1000 名以上 5000 名未満が 31%、5000 名以上が 15%と、売上高ほどにはきれいな分布とならなかったが、概ね中小から大企業までを洩れなくカバーできたと見ている。(図 3)

特に、製造業と情報･ソフトウェアの業種、更にはサービス業も比較的多いことが、売上規模に比して従業員数が多めに出て、100 名以上 500 名未満と 1000 名以上 5000 名未満のところにピークを作った要因であると推測できる。

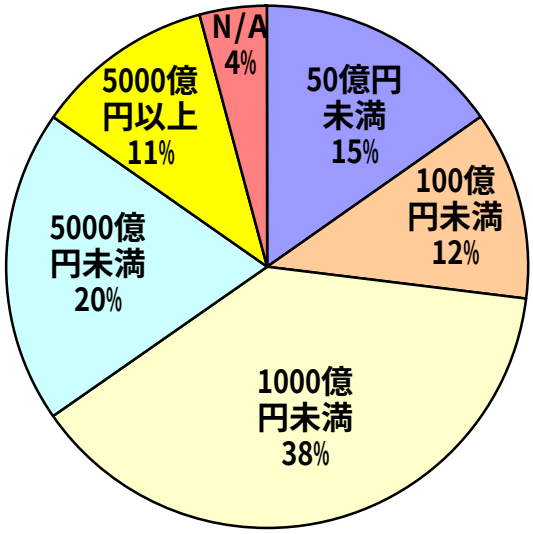


図 2.　回答企業の売上高規模分布

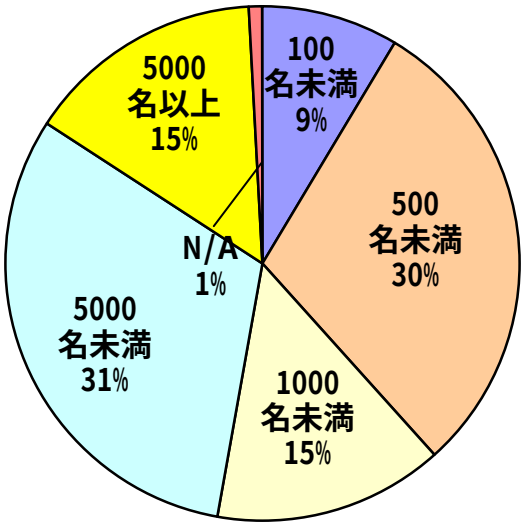


図 3.　回答企業の従業員規模分布

2　IT 予算とセキュリティ予算

今回のように企業規模の分布の広がりの大きい調査では、予算の絶対額を尋ねることはそれほど有意の意味を持たないと判断して、IT 予算については売上高対比で、またセキュリティ対策予算については IT 予算に占める割合で訊いた。

2.1 売上高比 IT 予算規模

全体では、IT 予算額が売上高対比 1%未満とした企業が 39%、1%以上 3%未満が 31%、3%以上 5%未満が 8%、5%以上 10%未満が同じく 8%、10%以上が 4%という結果になった。

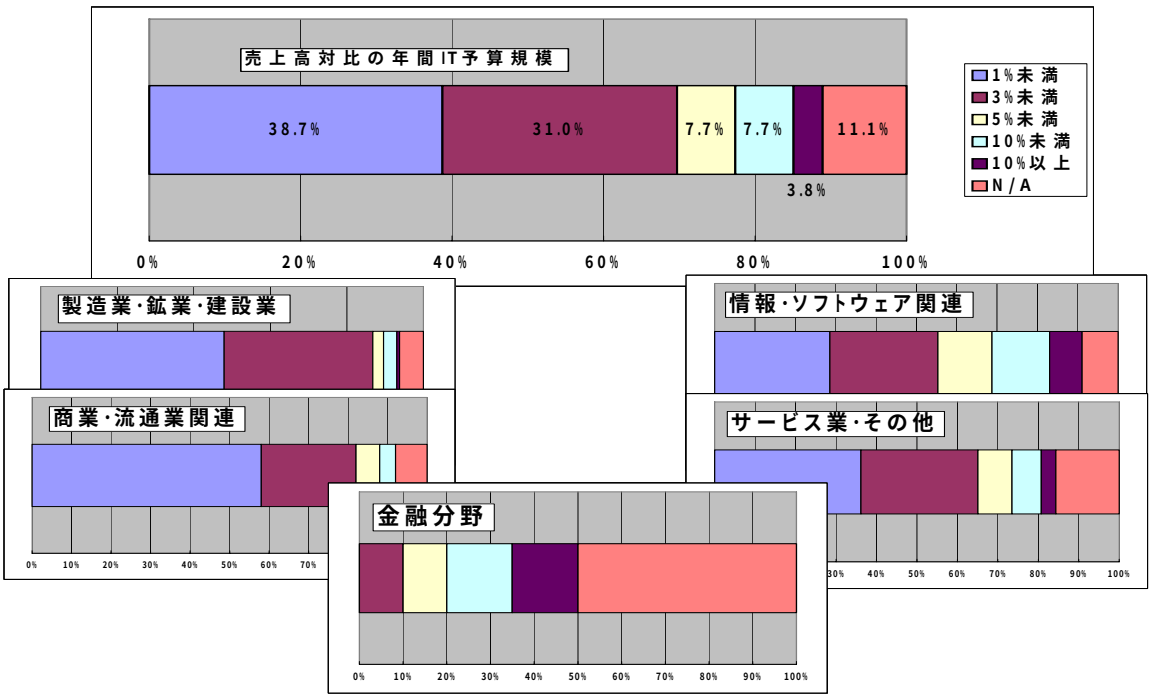


図 4.　IT 予算の対売上高比率の分布

製造、商業関連は売上規模が大きく出やすいので IT 投資額を売上高比で見る場合、数字は低くなる。それが全体にも反映している。金融はもっとも IT 依存係数の高い業種で、5%以上 10%未満、10%以上の比率が高い。（売上高比という設問に対して経常収益比との読み替えをせず N/A とした回答が半数を占めたが、傾向としてやはり IT 投資が活発であることを示している。）

情報･ソフトウェア関連でも過半数が 3%未満と比較的低い数字だったのは意外だった。それでも 3%以上 5%未満、5%以上 10%未満も各 13-14%を占め、ほかの業種に比べれば比較的 IT 依存度が高いことを示した。その中間がサービス･その他で、全体として業態と IT 投資度または依存度の関係もきれいに趨勢値を反映していると見られる。

なお、あくまでも仮説的試算であるが、加重平均ベースで IT 予算額は約 42 億円、売上高比で約 2.4%、有効な全データの中位値では、IT 予算額は約 8 億円、売上高比で約 1.4%という数字が得られた。各選択肢の数値区分帯を平均と想定される数字に代表させての試算であり、正確性は期せないが、多少のイメージは持てるかもしれない。

2.2 IT 予算のうちセキュリティ費用・投資が占める比率

1%未満とした企業が有効回答の 31%、1%以上 5%未満が 29%、5%以上 10%未満が 16%、10%以上 20%未満が 6%、20%以上としたところも 7%あった。全体の 60%が IT 予算のうちセキュリティに 5%未満という最低限の予算しか回していない実態が浮かび上がった。

一方、全体の約 8 分の 1 が IT 予算の 10%以上をセキュリティ対策に費やしていることも明らかになった。従来、IT のうちセキュリティに回されるお金は 3～5%と言われていたのが、5～10%とした企業が 16%に上ることからも、ここへ来て IT 予算に占めるセキュリティ対策費は確実に増加していると見ることができる。

一定の仮定を設定して中位値および加重平均値を試算してみた。中位値 4%程度、加重平均値は 5.5%程度という結果となった。この数値からも、従来大雑把に、経験則及びアメリカのデータから 3～5%程度と言われていたセキュリティへの IT 予算の配分が、若干上方シフトを起こしていることが伺える。

3　OS プラットフォームの選択とネットワークシステムの運用状況

今日、OS の選択が外部からのセキュリティ脅威の度合を大きく左右する状態が出現して

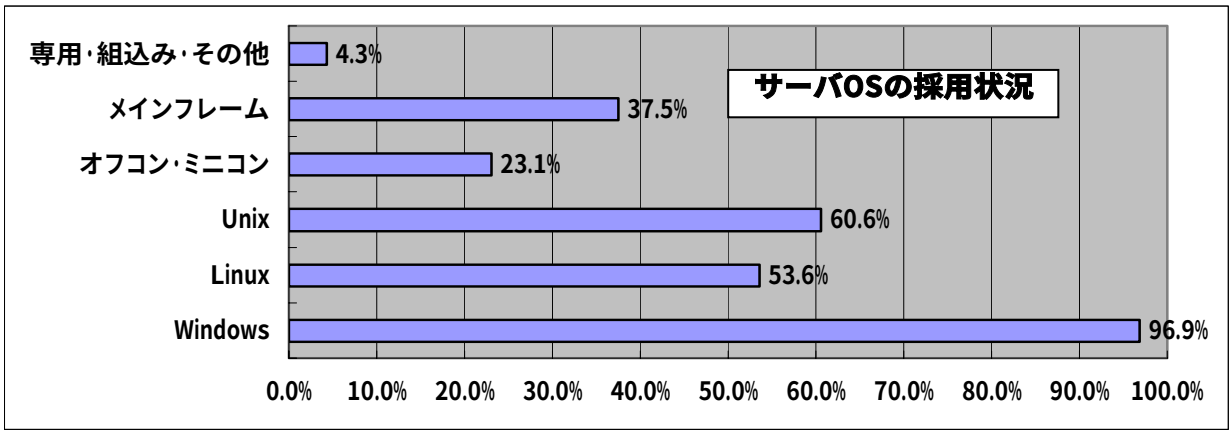


図５　サーバーOS の採用状況（複数回答：N=416）

いることから、サーバーならびにクライアントについて、使用 OS を複数回答で確認した。(図５，６)　結果、サーバーについてもクライアントについても、ほぼ 100%が Windows を採用していることが確認でき、その普及率の高さと潜在的脅威の可能性を裏付けられた。Linux, UNIX の浸透が確実に高まっていることも確認された。クライアントでは各々20%の企業で使われ、サーバー環境にいたっては UNIX で 60%、Linux でもすでに 54%の企業が採用している。サーバーやアプライアンスにおける UNIX、Linux の普及を物語るものとして注目される。

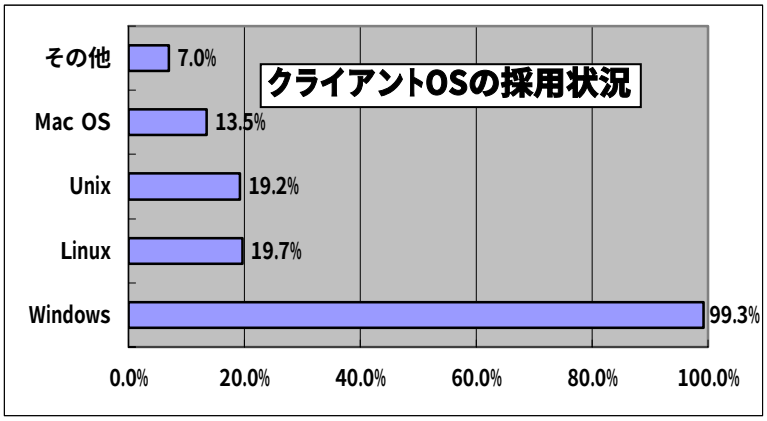


図６　クライアント OS の採用状況（複数回答：N=416）

ネットワークシステムについては、未採用企業がないという前提で、運用主体が自社か外部委託かについて回答を求めた。その結果 71%が自社運用であり、次いで多かったのが情報子会社･関連会社の 16%。純粋の外部委託は 15%にとどまった。（重複回答があり、合計が 100%を超えている。）売上高規模別に見ると 5000 億円以上の超大企業では 63%がアウトソースしており、そのうち 49%ポイントと全体の約半数が情報子会社または関連会社への外部委託となっている。売上高 1000 億円以上 5000 億円未満では 43%、100 億円以上 1000 億円未満でも 29%が何らかのアウトソースを行っており、超大企業において情報子会社化がかなり浸透しているのに加え、大企業と中堅企業の一部で、ポリシーとしてのアウトソーシングが浸透し出したことを示していると推測される。

第二章　情報セキュリティに対する対応体制

今回の調査では、企業の組織体制として、情報セキュリティに対する対応がどこまで浸透しているかを見るために、部署や要員の有無と担当役員の配置についてたずねた。

４　情報セキュリティ対策体制

情報セキュリティに対する組織体制を確認するため、対応部署と所管役員について調べた。

４.1 情報セキュリティへの対応体制

「対策要員は特に定めていない」としたのが全体の 16%であり、84%は何らかの形でセキュリティに対する対応体制をとっていると見られる。全体の 54%（重複回答除く）が、兼任もしくは専任で情報セキュリティ対応部署を定義している。（図７）残る 30%は部署までは定義していないが対応要員を置いているものの、そのほとんどが兼務要員であり、実質的には情報システム部員等が必要に応じセキュリティに対応しているというのが実態と見られる。これは「対策要員は特に定めていない」とする回答と実質的に近い要素があり、概算で 40%が余り明示的な体制を実現できていない想定される。できれば専任の要員を配置してセキュリティ対策を推進すべきであるが、少なくとも明示的にセキュリティ対応の任務を定義し、きちんとアサインされた兼任の対応要員を配置することが望まれる。

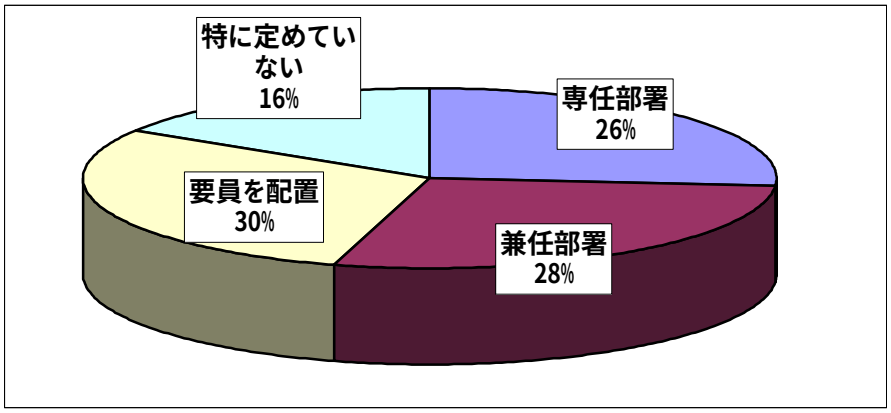


図７　情報セキュリティ対応体制について（重複回答整理後）

４.2 情報セキュリティ担当役員

全体の約４分の１が CISO（情報セキュリティ対策担当役員）または CSO（セキュリティ対策担当役員）を設置していると回答した。ただし、これは複数回答を重複カウントした場合の数字であり、複数回答のかなりが CISO がいるとしつつ、「情報セキュリティは CIO（情報システム担当役員）の所管である」にも○をしている状態で、これらの意味するところは「CISO はいますけど、CIO の兼務ですよ」ということになる。従い、これを「CIO の所管」と読めば、純粋に CISO または CSO のいる企業は全体の 18%程度になる。これはほぼ専任の役員が配置されていると考えられ、役員レベルでセキュリティ対策を位置づける姿勢が、大企業を中心に浸透してきていることを示していると言えるのではないか。一方、３割が CIO の所管としており、CEO（最高経営責任者）の直接所管とした 8%と合わせて４割近くが、情報システム部門とセキュリティ管理の分離、相互チェック体制の構築ができていないことを示した。上記の、CIO が CSO または CISO を兼ねている可能性の高い部分を加えると５割近い数字となり、

セキュリティに対する意識は根付きつつも、依然情報システム部門任せの傾向が強いことを示していると思われる。

これ以上に問題なのが、「セキュリティ担当役員は特に定めていない」とする回答が 44%に上ったことであろう。特に、売上高 1000 億円未満の企業では 53%が担当役員を置いておらず、このクラスが「セキュリティ担当役員は特に定めていない」とする回答の 78%を占めている。やはり企業規模が小さいほど、役員レベルでのセキュリティ対応体制が十分に取れていないことが確認された。IT が今後ますます経営戦略上の重要性を増す中で、企業規模を問わず、IT セキュリティへの経営レベルでの取り組み、位置づけがなされることが望まれる。

第三章　情報セキュリティガバナンスへの取り組み状況

第二章に見たように、依然情報システム部門に帰属する問題という認識にとどまり、独立した経営課題という認識レベルまでは到達していないものの、情報セキュリティはようやく、IT 技術・ネットワーク技術領域におけるテクニカルな課題から、経営そのものにとっての課題であるという認識に昇華しつつある。それがどの程度定着しているのか、質問をできるだけ簡略化しつつ実態を探る試みを行った。

技術課題から経営課題への認識の転換を大きく後押ししたものが、個人情報保護法である。その意味で、企業が個人情報、あるいはプライバシー情報に対してどれだけの対応体制を取れているのかも興味のあるテーマであった。そこで、情報セキュリティガバナンスへの取り組みの典型的モデルとして、プライバシー情報に関する取扱体制についても確認することとした。

5　情報セキュリティポリシーへの取り組み状況

情報セキュリティポリシーについては、その策定状況、運用状況、見直し・更新の状況、外部サービスの活用について、更に外部サービスの提供事業者の業態について調査した。

5.1 情報セキュリティポリシーの策定状況

回答企業の 56%が策定済み、37%が検討中または策定予定と回答した。合わせて 93%の高率でセキュリティポリシー構築への取り組みがなされている。これは予想を大きく上回る高い数字で、セキュリティポリシーの必要性への認識が浸透し定着していることを物語っている。37%の「予定」が早く既定になることを期待したい。(図 8)

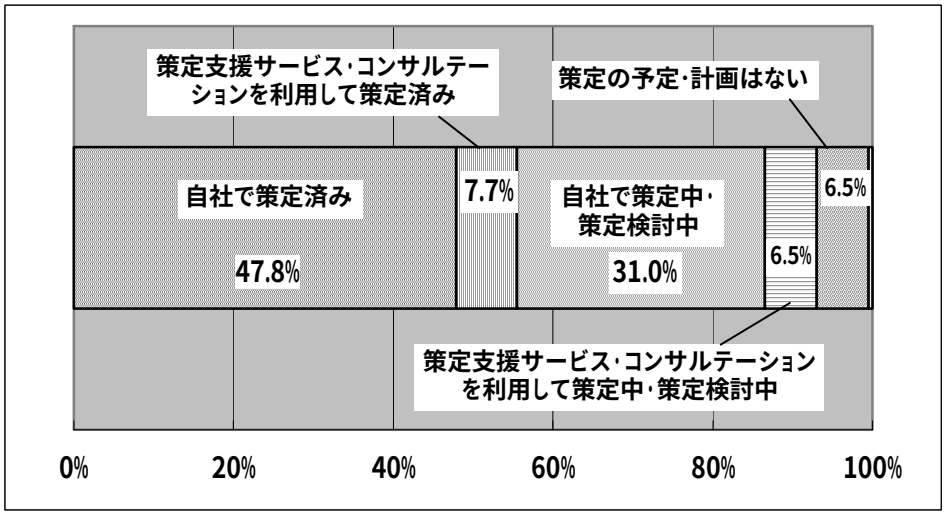


図 8　　情報セキュリティポリシーの策定状況

業種別では、策定済みの比率が高い順に、金融分野 73%、情報・ソフトウェア関連 69%、製造・鉱業・建設業 51%、サービス業・その他 49%。ほとんどの業種が約半分以上でセキュリティポリシーを策定済みである一方、商業・流通業関連のみが 40%と低迷している。

売上規模別では、5000 億円以上が最も高く 91%が自社または外部サービスを活用して策定済み。以下 1000 億円以上 5000 億円未満 63%、50 億円未満 53%と続く。なお、大半が金融機関と思われる売上規模無回答層は 59%が策定済みであった。

一方、セキュリティポリシーの策定を自社で行ったか、外部の支援サービスやコンサルテーションを活用したかについては、策定済み・予定を合わせても 14%が活用したとしているに過ぎず、大部分が自社での取り組みとなっている。他人任せにしない主体的な姿勢が読み取れる一方、コスト負担を嫌って専門的知識の導入をためらっている可能性も危惧され、専門的アドバイスを反映しないセキュリティポリシーの有効性について、若干の不安を禁じえない。

また、このような専門サービスは、需要が適正に形成されて始めて、供給側の量と質も伴ってくるという関係にあり、このような外部サービスの活用姿勢の低さは、マクロで見たときの産業の形勢・発展や、それに伴うサービス品質の充実を阻害することにもなり、健全な実用・実践の定着という意味では課題を残していることをくっきりと示す結果になったと認識している。

5.2 情報セキュリティポリシーの運用状況

セキュリティポリシーの運用状況については、セキュリティポリシーを自社で、または外部サービスを使って策定ずみとした企業 232 社のうち、運用していないとしたのが 1 社、無回答が 1 社あるだけで、94%が自社で、5%が外部のサービス業者を使って、運用ができていることが確認できた。

単純集計では約 30%が運用ができていないという結果になっているが、このほとんどが、現在策定中かセキュリティポリシーを未策定の企業の回答であり、策定済みの企業ではほとんどきちんと運用がされている訳で、ポリシーを策定する趣旨が徹底しているという、決して「仏作って魂入れず」というようなことは起こっていないことが確認された。

5.3 情報セキュリティポリシーの見直し状況

運用と共に情報セキュリティポリシーの見直しも重要な課題である。「運用」の問題は、出来上がったポリシーをいかに現場のオペレーションへ反映させるかの管理プロセスであるが、見直し・更新はセキュリティポリシーそのものの管理プロセスである。セキュリティポリシーは、他の経営課題と同様に、状況に応じて見直し進化させていくべきもので、プラン・ドゥ・チェック・アクションの管理サイクルを回す中で、状況に応じて的確かつ迅速に変化させ進化させる必要がある。せっかく策定したポリシーも、状況の変化に応じて柔軟に変化していなければ、場合によっては害にもなりかねず、見直しは非常に重要な管理プロセスである。

ここでは、自社、外部サービスを合わせて定期的見直しが 28%、不定期の見直しが 29%を占めた。更に見直し予定が 18%あり、全体の 4 分の 3 が見直し・更新に取り組んでいる実態が確認された。セキュリティポリシーそのものに対する管理サイクルは相当程度定着していると見られ、喜ばしい結果となった。

今後は、まだ 20%を占める「見直しの予定がない」または「ポリシー未策定」をいかに減らすか、また不定期な見直しをいかに定期化するか、が課題となりそうである。

5.4 情報セキュリティポリシーに関する外部サービス活用とその満足度

情報セキュリティポリシーの策定に関する外部サービスの活用は 14%、60 社とまだ極めて限られる実情である。その中で、サービスに対する不満について質問したが、当然ながら無回答が圧倒的比率を占めることとなった。何らかの回答を寄せていただいた回答者も、多くは「特に不満はない」と答えている。不満があるとしたのは、内容・質に対してが 11 件、コストに対してが同じく 11 件であり、

有効回答の各 12%を占めた。絶対数としては非常に小さいながら、その多くが、コンサルテーションが教科書的･ステレオタイプで自社の実情を反映していないという点についてのものとなっている。コストに対する不満も、そのような質に比較してというニュアンスが強い。これは供給側がまだ応用問題に十分習熟してなく、また事例の蓄積も少ないためにフレキシブルな対応･指導ができていない面があると同時に、利用側でも何でもコンサル業者に任せればベストのものを作ってくれるという甘えなり過度の期待があるのでないかと推測される。

コンサルテーションは本来、発注側が主体的に関わって共同作業をする中でコンサル側のノウハウを身につけるところに意義がある要素もあり、発注側の意識変化も必要ではなかろうか。同時に供給側のレベルアップも図られなければならないと考える。

5.5 外部コンサルテーション・サービス業者のカテゴリー区分

セキュリティポリシーに関するコンサルテーションや支援サービスの提供は近年相当活発になってきているとの感触があった。そこでそのようなサービスは、どのような業態の事業者が主に提供しているのか、言い換えればサービスを利用する側はどのような業者に発注しているのかを探るためにこの設問を設けた。

結果的には、外部サービスの活用そのものが 14%程度と極めて低率であることが判明し、その少ない事例の中で比較的多い選択肢から選んでもらう形になり、データ量としては満足を得られるものとはならなかった。回答の選択肢は、a)主としてコンサルティングサービスを提供する業者　b)主として専門的セキュリティサービスを提供する業者（たとえばセキュリティ監視サービスのプロバイダー等を想定している）c)主としてセキュリティ製品を販売する業者　d)主としてネットワークサービスを提供する業者（たとえばネットワークの運用サービスや監視サービスを行うサービスプロバイダー等）e)主としてシステムインテグレーションを提供する業者　f)主として保守サービスを提供する業者　g)いわゆる情報子会社　の８項目である。(図 9)

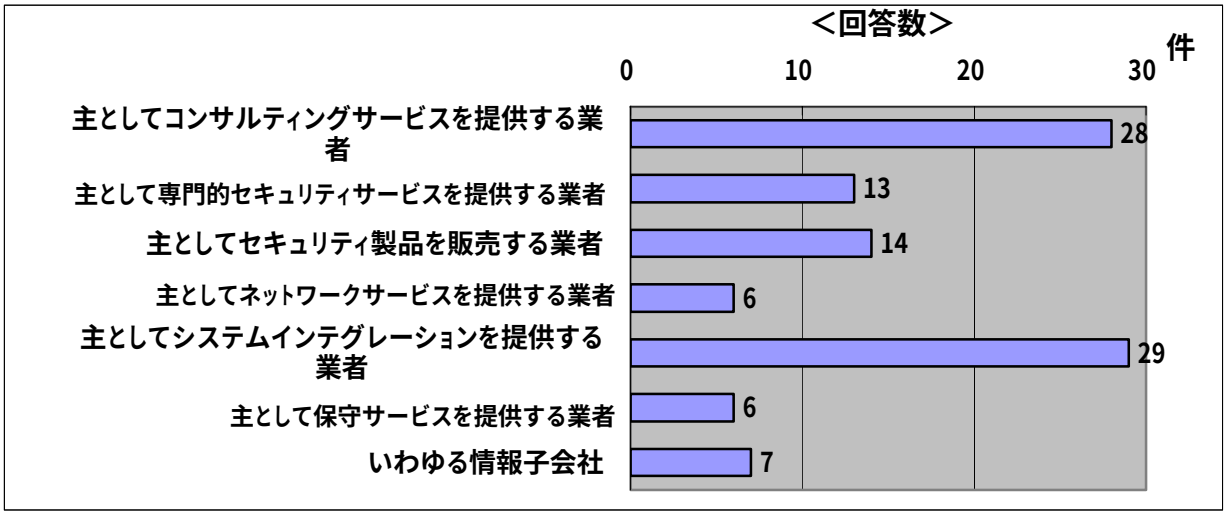


図 9　　外部サービスの提供主体の種類

回答数は、システムインテグレータ(e)とする答えとコンサルティングサービス業者(a)とする答えが各々29 件、28 件と群を抜いて多かった。これに続くのがセキュリティ製品ベンダー(c)の 14 件と専門的セキュリティサービス業者(b)の 13 件で、ほとんどのケースでセキュリティ分野の業者に依存

している傾向が読み取れた。情報セキュリティは、情報システムと密接に関わりその一部を構成するものであるから、システムインテグレータへの依存度が高くて然るべきであるが、やはりセキュリティということで『その道のプロ』に依存する傾向が強いようである。これは裏返せばセキュリティをまだ特殊なカテゴリーの課題と認識していることを意味し、システムの一環として、また経営管理の一環として位置づける理解に達するところまではまだ距離があるということであろうか。

6　セキュリティ管理に対する公的認証への取り組み状況

セキュリティ管理に関する公的認証では、BS7799、ISO17799、ISMS が一般に認知され出している。また、これらの確定した状態を認定し支える枠組みとは別に、セキュリティ管理、あるいはその意識の推進・定着を狙った制度として、2003 年から情報セキュリティ監査制度がスタートしている。ここでは、これらの種類を問わず何らかの公的認証に取り組んでいるかを問うことで、セキュリティポリシーの策定のみならず、それに基づく実際の管理プロセスに対してまで、客観基準の中で運用することを目指しているかどうかを調べる狙いで質問を行った。

6.1 セキュリティに関する公的認証の取得状況

全体の 18%が取得済みで、31%が取り組み中または検討中という回答であった。合わせて 49%というのは相当の高率であり、単にセキュリティポリシーの策定や運用にとどまらずセキュリティ管理プロセスそのものに客観基準を導入しようという意欲が読み取れる。

ただ一方で、ほぼ同数の 48%が取得を予定していない状態であり、ISO9000 や ISO14000 のように二極化が進む可能性を示唆している。(N/A=3.6%)（図 10）

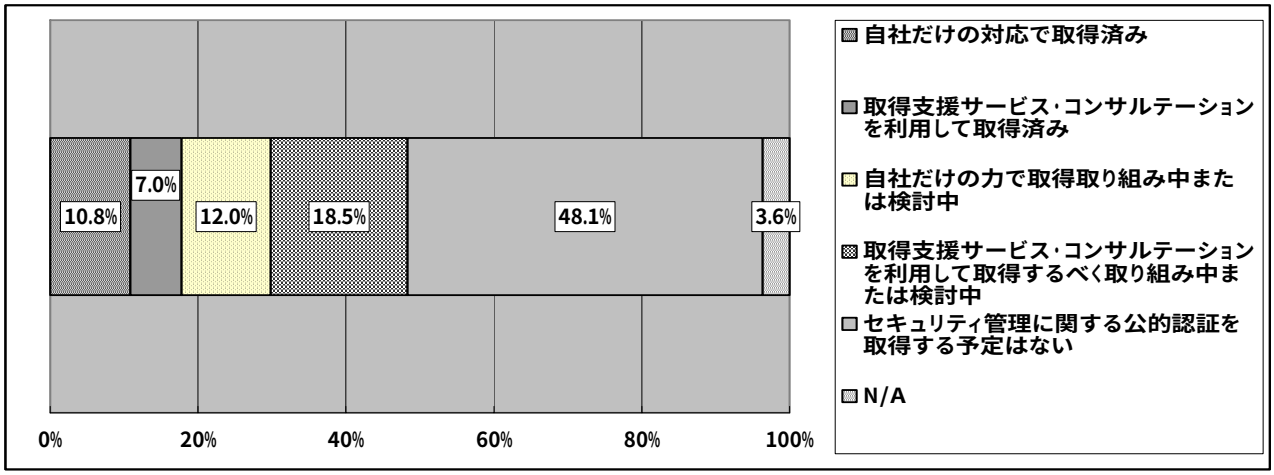


図 10　　セキュリティに関する公的認証の取得状況

企業規模別に見てみると、売上高 5000 億円以上の超大企業では取得済みと取得取り組み中または検討中が各々30%、1000 億円超 5000 億円未満の大企業で取得済み 22%、予定 24%、100 億円以上 1000 億円未満の中堅企業で各々16%と 32%、50 億円以上 100 億円未満のクラスでは各々14%、38%、50 億円未満クラスでは 14%、31%となっており、企業規模が大きいほど取得済みの比率は高まるものの、取得済みに取り組み中と検討中を加えると企業規模に関係なく、おおむね半数弱が取得意向を示している。一方、取得予定なしとした回答も、売上高 5000 億円以上の超大企業で 34%と低いほかは規模に関係なく 5 割弱を占めている。二極化傾向は企業規模によらず見られる現象と推定される。

認証取得に対する外部の支援サービス・コンサルテーションの利用状況については、セキュリティポリシーの場合と逆に「自社だけで」23%に対して回答者の 26%が活用（予定含む）しており、外部基準で計られるものにはプロの手助けを手当てしようという意識がうかがえる。

6.2 セキュリティに関する公的認証の維持管理状況

公的認証は定期的に維持管理状況をチェックすることで認証の実効を維持する仕組みとなっており、取得と同等以上に維持管理が重要である。そこで、維持管理の状況について、その取り組みの有無と自社か外部サービスかの組み合わせで聞いた。しかし、公的認証の取得への取り組み状況への回答と照らし合わせて見てみると、公的認証の取得予定がないとしているにもかかわらず自社で維持管理しているとした回答が 6 件あるなど、回答側に若干の混乱があった模様である。

個別的には、自社で公的認証を取得した企業 45 社のうち 44 社が自社で、1 社が情報子会社に委託して維持管理している。また、外部のサービスを活用して公的認証を取得した企業 30 社においては、1 社のみが維持管理していないという回答であったほかは、自社で維持管理が 24 社(80%)、外部サービスを活用しての維持管理が 5 社(17%)であった。合せて、公的認証取得済み企業のほぼ 100%近くが、維持管理にもきちんと取り組んでいる実態が確認できた。これはセキュリティ管理に対する認証の意図するところが十分に認識･理解され活かされている状態ということができ、喜ばしい結果となった。

経営管理に関する国際標準に基づく第三者認証の制度は、IS09000 シリーズ、IS014000 シリーズといった品質や環境に関する認証がよく知られ定着している。多くの企業が認証を取得しているこれらの基準も、定着と一般化が進むにつれ、それが外形基準ベースのチェックであることから、日日の運用よりは、定期点検時点での瞬間風速で維持管理をクリアしようとする傾向が指摘されるようになってきている。情報セキュリティ管理についても、同様の意識のギャップが発生するようだと、認証制度の本来の趣旨から離れてしまう。維持管理のプロセスの中で、システムとその運用に、基準の要求がどのように実現し遵守されているか、実態に即してチェックし改善につなげていくことが重要である。セキュリティの認証制度の本来の趣旨を活かす意味で、認証自体以上に、日ごろの運用プロセス、その管理サイクルを生かしての維持管理の実現に、取得企業の意識が向かうことが望まれる。

6.3. セキュリティに関する公的認証の取得支援サービス・コンサルテーションの利用満足度

公的認証の取得に関する外部サービスに対する満足度についても調査した。外部サービスの活用が予定を含めても 100 社弱と限られ、不満があるとした回答数が合計 13 とサンプル数は極めて限られたものとなった。しかし、自由記述で書いていただいた内容には、取得段階だけでそれを経営管理過程に活かす部分についての支援がないことに対する不満や、同様の趣旨と思われるが、具体的事例の提供が少ない（参考事例を多数示して自社に合った管理手法をアドバイスすることを期待しているものと推測できる）といった不満が寄せられた。どちらも、取得そのものを自己目的化せず、認証の趣旨を管理に活かして生きた管理にすることの重要性を理解した上で、その具体策の提案や助言を期待しているものと理解される。

セキュリティ管理の公的認証の蓄積が浅いことと新規参入が相次いでいる初期における、供給側の限界を示唆するデータとも解釈できるが、取得を目指す側がいかにそれを経営に活かすかの正しい意識を持っている点が確認できたことが収穫だと考える。

7　プライバシーポリシー、個人情報保護管理基準等の策定状況

個人情報保護法の告示と来年４月からの全面施行をにらんで、個人情報保護に対する取り組みが本格化している。これに先立ち、すでに 1998 年にはプライバシーマーク制度が実施に移されており、企業等が取得する個人情報やプライバシー情報の取り扱い･保護について、強い社会的要請がかけられている。企業においては、情報セキュリティ管理の中でも、特に意識し注意を払うべき領域であり、どこまでの取り組み･対策ができているかを調査対象とした。

7.1 プライバシーポリシーの策定状況

ウェブ等に表示されているいわゆるプライバシーポリシーや、個人情報保護法で個人情報取扱事業者に課せられることになる個人情報保護管理基準等の個人情報の取り扱いに関するポリシーの策定状況を訊いた。（図 11）

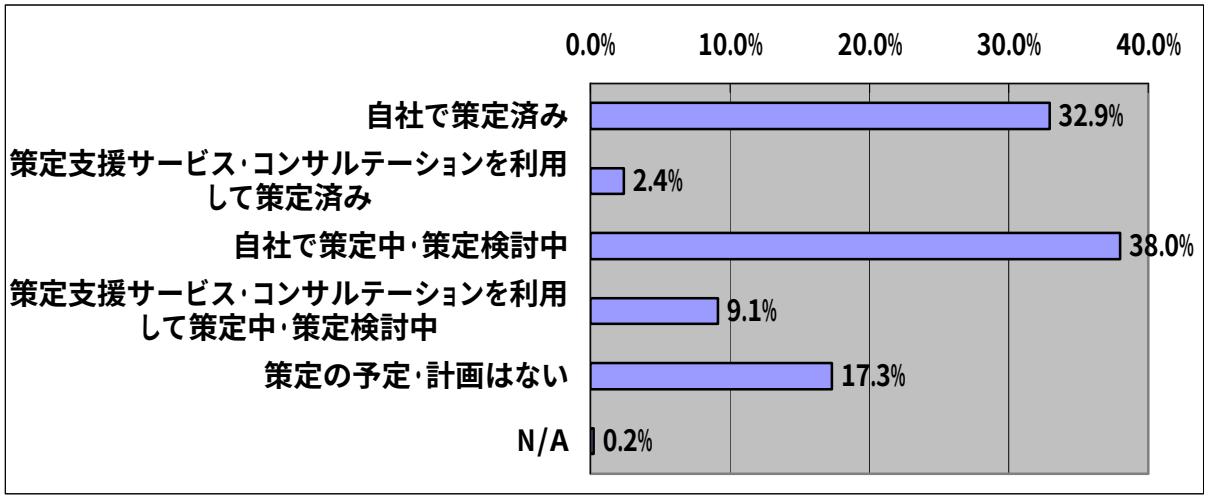


図 11　　プライバシーポリシーの策定状況

社会的関心の高さを反映して、82%が策定済みまたは予定としている。業態的にいわゆる個人情報取扱事業者の定義に該当しない企業も一定程度はいることを考えると、何らかの対応を必要とする企業は対応済みか、既に視野に入れていると見ることができよう。とは言いつつも気になるのは、策定済みが 35%で予定が 47%である点。その合計がセキュリティポリシーの 93%を大きく下回っていると共に、「策定済み」と「予定」の比率がセキュリティポリシーとは逆転しており、取り組みの出遅れが感じられる。個人情報保護法の完全施行を控えて早急に改善が必要なのではなかろうか。

また、ここでも、自社での対応としているのが 71%に上っており、外部サービスの活用はあまり視野に入っていない。個人情報保護に関連する事故が起こった場合の経営リスクは巨大化する傾向にあり、その未然防止のためにも、プロの視点を一度は反映することを検討してみてはいかがだろうか。

7.2 プライバシーポリシーの運用状況

プライバシーポリシーの運用状況について尋ねたところ、ポリシーを策定済みの企業では、100%が運用もきちんと行っているという回答結果が得られた。ポリシーを定めた以上運用もきちんとするのは当然と言えば当然であるが、１社の漏れもなく運用に取り組んでいることは、意識の定着度合いとしてきわめて高いものであり、驚嘆に値する。更に、ポリシー策定を予定しているレベルでも、既

に４分の１が自前での運用を考えており、意識の高い層では策定と同時に運用についても視野に入れていることがわかる。

ポリシーというものは、策定と同等以上にそれを日日の経営管理過程に反映する運用面が重要であり、今回の回答を見る限りはその点の理解は十分に行き届いていると言える。

７.3. プライバシーポリシーの見直しに対する意識

プライバシーポリシーの見直しについては、何らかの形で見直しを実施している企業が 40%、予定企業が 18%ある一方、見直しの予定なしも 20%ある。策定しない企業が 17%あるので、策定企業の大半は見直しを考えていると理解してよいであろう。ポリシーは定期的に見直してこそ生きたポリシーになるし、それが定着浸透して意識の変化を生み、更に見直しを通じてより良いものに改善されていく好循環を生むことを期待したい。

８　プライバシーマークの取得状況

プライバシーポリシー、あるいは個人のプライバシーに関わる情報をいかに保護するかの経営政策に対応する公的認証という意味で、プライバシーマークの取得状況について訊いた。

ウェブをビジネスの直接の手段･場として使う、いわゆる e-ビジネス企業以外はプライバシーマークの取得までのインセンティブは働きにくく、それを反映して取得済みは合計 14%と低位にとどまる。一方、取得予定は 30%以上の企業が考えており、個人情報保護法が引金になって関心が高まっていることが裏付けられた。

ただし、52%は取得予定はないと回答しており、やはりセキュリティ管理に関する公的認証に比べると、その趣旨が限定される分と、取得メリットが特定業態に限られる分、取得意欲には限界があることを示していると思われる。

第四章　個別セキュリティツール・サービスの導入状況とその満足度

アンケート調査の第三部として、典型的なネットワークセキュリティの対策ツールもしくはサービスについて、導入状況とその満足度を調査した。

この関連の調査は比較的良く行われていて、たとえばウイルス対策の普及率は 90%を超えているとか、ファイアウォールについても、統計データでばらつきはあるものの最低 60%、最高 90%程度の普及率になっているといった程度の共通認識は形成されている。

そこでこの調査では、最近普及が著しいアプライアンス型が従来のソフトウェアタイプに対してどのような浸透を見せているかの視野を加えた。また同様に、自社でツールを購入して運用する代わりに、第三者のサービスに依存する、つまり物でなくサービスを買う方向が現れてきており、この点についても併せて調査を試みた。

これらを詳しく聞こうとすると、調査項目が広がり複雑になる恐れがある。そのことが調査の手間とコストに響くほかに回収率に影響することも危惧されたため、質問はこれら要素をひとつの設問内の回答の選択肢に押し込むように単純化した。その分掘り下げにくいデータとはなったが、概容と傾向を知るにはシンプルで使いやすいデータが得られたのでないかと考えている。

また、特にセキュリティ対策製品のベンダー企業が会員にかなりの比率を占める JNSA としては、各製品に対して、ユーザーがどの程度満足しているのか、どんな不満を感じているのかはぜひ知りたいポイントであった。そこで、主なセキュリティ対策製品についての満足度も併せて調査した。ここでも質問をシンプルにする意味で、不満を 1)機能に関するもの　2)性能・パフォーマンスに関するもの　3)品質･信頼性に関するもの　4)コスト（費用対効果）に関するもの　の４類型の選択肢を設けて聞くと同時に、自由記入欄を設けて不満の内容を具体的に書いてもらうようにした。

全体としては、不満を持っている比率はかなり低い結果となった。このひとつの要因は、回答者として IT セキュリティまたは情報システムを所管する部長･役員クラスを対象としたことから、現場の苦労が直接には認識されていなくてアンケートに反映されなかったことが考えられる。またインシデントの経験頻度がそれほど高くなく、具体的不満点を浮かび上がらせるにいたっていないことも、可能性として想定されるが、いずれも推測の域を出ず、実際のところどうなのかの判断は、更なる掘り下げ調査に委ねる必要がある。

なお、個別には以下に見て行くが、今回調査対象とした対策ツールの導入状況の一覧は図 12 の通りである。

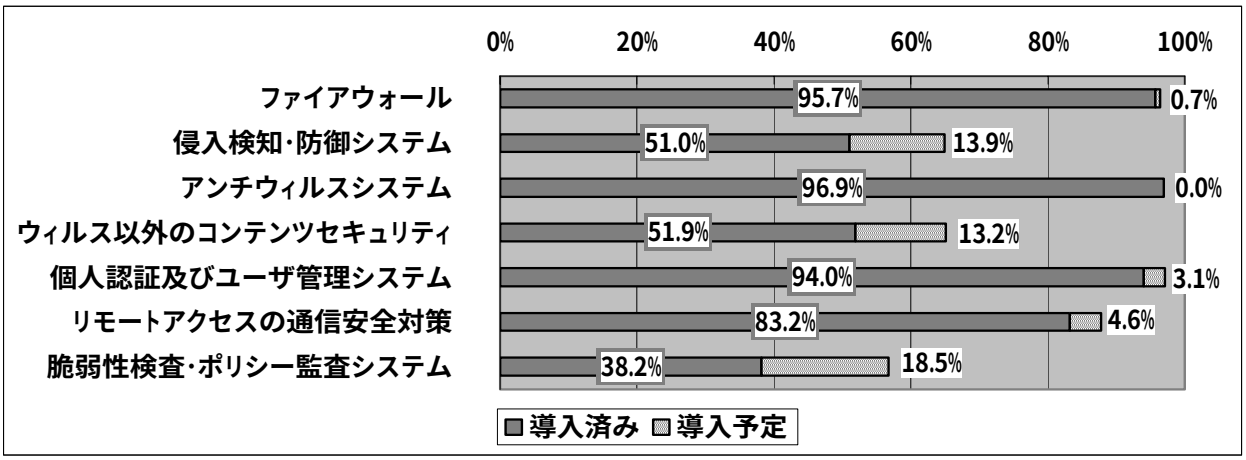


図 12　セキュリティ対策ツールの導入状況

９　ファイアウォールの導入状況

インターネットに接続するなら、そのゲートウェイにはファイアウォールを設置するという考えは、もはや常識の粋に達しているのではないかというのが、我々調査に当った者の感覚である。従って、ファイアウォールに関する調査の関心は、アプライアンスの普及度、外部サービスの導入程度、またどのような不満を抱えているか、といった面であった。これらを単一の設問で知るために、ソフトウェア、アプライアンス、サービスが混在する選択肢から、複数回答でどのようなファイアウォール及びサービスを導入しているか訊いた。分析に際しては、回答数を全回答企業数で割ることで、調査対象企業における各製品・サービスの普及度を確認できるようにした。

９.1. ファイアウォールのタイプ別導入状況

分析の結果、アプライアンス型ファイアウォールが約 6 割と非常に高い普及率を見せ、ソフトウェア型も引き続き 4 割弱の企業で使われていることが判った。このうち、ソフトウェア型もアプライアンス型も併用している企業が 13%ある。一方、アプライアンスの自社運用と外部サービスの併用、ソフトウェア型ファイアウォールと外部サービスの併用も各々19 社(4.6%)、10 社(2.4%)あり、更に３種類を併用するところも 10 社(2.4%)あった。外部サービスだけで対応している企業を合わせると全回答企業の約２割は単独または併用で第三者によるファイアウォール監視サービスを利用している。（図 13）

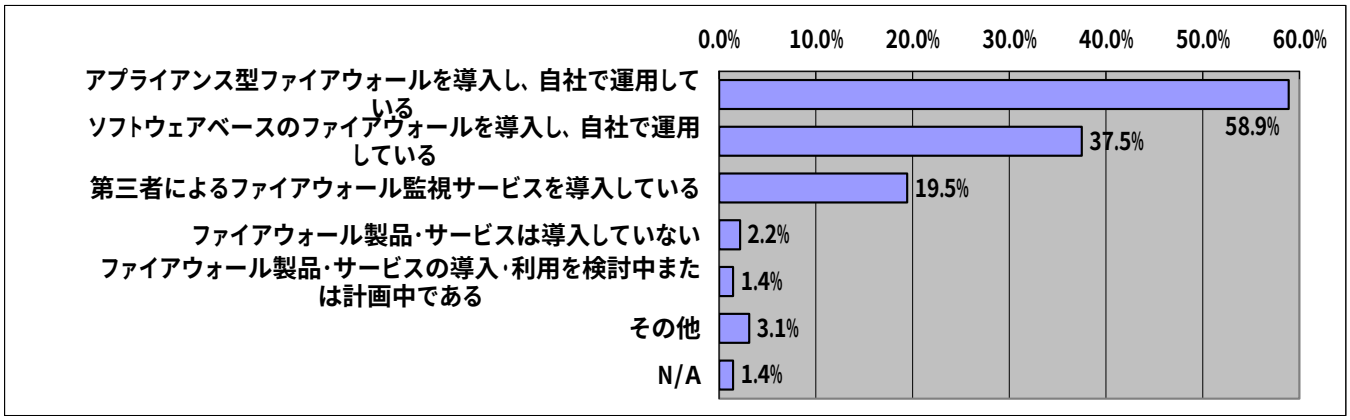


図 13　　ファイアウォールの導入状況（複数回答：N=416）

「その他」と答えた中で多かったのが、ルータのフィルタリング機能でまかなっているものと、親会社のネットワークの下位レイヤーに入っているので直接インターネットと接していないためというものであった。まったく導入していない割合がわずか 2%であることも確認され、ファイアウォールが必須のセキュリティデバイスであることは完全に定着したと見られる。

９.2. ファイアウォール監視サービスの普及状況

上述のように、回答企業の約２割、８１社が単独または自社運用と平行して第三者によるファイアウォールの監視サービスを導入していることが確認できた。近年複雑な設定やログ解析、インシデント対応をまとめて外部の専門家によるサービスに依存しようという考え方が浸透しつつあり、その傾向を反映するデータとして注目される。ただ、ファイアウォールの監視サービスが、第三者によるサービスの中で比較的早くから提供され、参入しているサービスプロバイダーも数多い中で、この約 2 割 81 件という回答数が、果たして多いと捉えていいものか、慎重な検討が必要であろう。提供され

るサービスの技術的水準と価格水準からは、また自社ではなかなか専門スキルの確保が難しいことも考えると、プロフェッショナルサービスへの依存度がもっと上っても然るべきではないかとも思われる。

９.3.ファイアウォール製品またはサービスに対する満足度

ファイアウォールの導入･運用上の不満・問題点について訊いた。何らかの不満を寄せた企業数は78社で、全体の19%に相当する。不満の比率は他の対策製品よりかなり低く、技術的にも成熟度が高まっていると想定される。複数回答で、機能･性能･品質･コストに対する不満を上げたのは全416社のうち各々6.0%、7.0%、4.6%、5.8%であった。各項目ともある程度の不満を持たれている中で、やはりスループットもしくはパフォーマンスかが気になる回答者が一番多い結果となった。ゲートウェイにおける直列型配置の機器としては、ある種宿命とも言える課題であろう。

自由記述に寄せていただいた回答の中には、厳密には不満とは言えないが、導入製品がかなり古く、OS対応、スループット、メンテナンス等の面で悩みを抱えているという記述が散見された。ネットワーク技術の革新とインターネットトラフィックの増大、回線容量の飛躍的拡大という技術･環境変化に対応して、適宜対策技術･製品を更新しないと十分な防御は期待できない。このことを十分に認識せずに「ファイアウォールを入れているから安心」と思い込んでしまう認識ギャップが存在していることをうかがわせる。一編の調査結果に依存して、単に「対策導入済み」との回答だけで安心するわけに行かないのではないか、との懸念を喚起するものとして注目したい。

その他の不満としては、正しく動いているか不安、アタックがないので有効性が確認できない、といった動作に対する不安や、ログの解析に関する不満（解析機能に関するもの、解析が大変だというもの）が目に付いた。また、ブラックボックス化しているとか、想定外のアクセスがある、あるいはすり抜けがある、といった、設定や運用に起因する問題を、そのようには認識せずに、ファイアウォールの問題と理解しているケースもいくつか見られた。

理解不足、認識不足の結果、せっかく導入してファイアウォールが活かされていないとか、古いまま放置されているとすれば、セキュリティ上のリスクが放置されていることになる。正しい認識に基づいた正しい運用が徹底されるよう期待したいところである。

１０ 侵入検知・防御システムの導入状況

企業内ネットワークは、通常インターネットとの接続点にファイアウォールを置いて不要な通信を制限するとともに、外部から不正な意図を持って内部ネットワークにアクセスする動きをブロックするように構築するのが一般的である。しかし、ファイアウォールが通信を許可しているプロトコルやファイアウォールの設定の欠陥なり弱点を突いて侵入して来る攻撃がありうる。侵入検知はIDS(Intrusion Detection System)と呼ばれて、このような攻撃を即座に検知して対策の発動を促すセンサー兼警報装置として数年前から普及期に入った技術である。また、侵入防御はIPS(Intrusion Prevention もしくは Protection System)と呼ばれて、不正侵入の動きを検知するとそれに対して自動的に遮断したりして内部ネットワークを防御する装置で、最近製品の提供が増えだした技術である。どちらもファイアウォール等で防御している点を越えて侵入してくるアタックを検知し更には対応するという意味で、同一カテゴリーにくくって質問した。なお、回答は複数回答としている。

１０.1. 侵入検知･防御システムの普及状況

複数回答を整理した結果、何らかの形で導入済みの企業は 51%、導入を検討中または計画中の企業を加えると 65%となった。ファイアウォールと違って、従来補完的対策と考えられている面もあり、また運用面では特有の高度な知識や技術を必要するところから、普及率は予定を含めても 65%と、ファイアウォールの 96%とはかなり差のある状態である。また実際に導入済みが約半分という結果は、業界の実感とぴたりと符合するものとなった。

IDS/IPS はアンチウイルスやファイアウォールと一体化されて統合型アプライアンスとして提供される製品の種類も増えている。ひとつには、高いパフォーマンスを求められることから専用ハードを用いて最適チューニングを目指すためであり、また別の視点から、個別のデバイスを運用することが困難な中小企業や大企業の出先オフィス等で、ＳＩや本社の情報システム部門があらかじめ設定した状態でブラックボックス化して使う形態が志向されだしているためである。この傾向を反映して、ソフトウェア型より既にアプライアンス型の導入率が上回っている。（図 14）

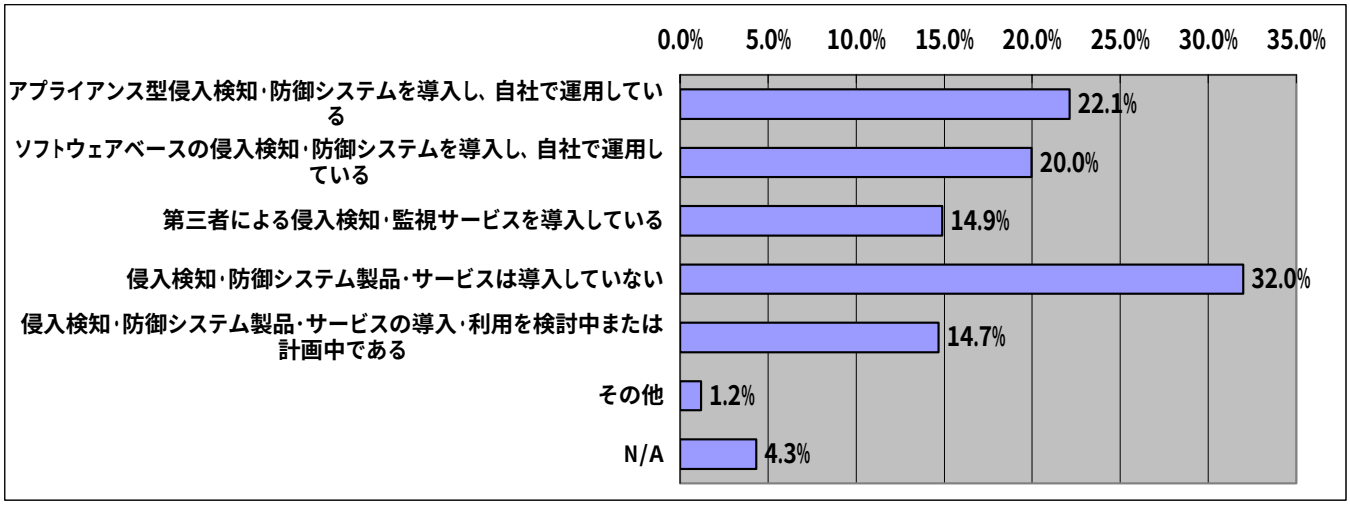


図 14　侵入検知･防御システムの導入状況（複数回答：N=416）

特に今後導入が広がるとすれば上記の後者のケースでの導入が中心になると見られ、簡易型の IPS で使い勝手のよいものが増えてくれば、IDS/IPS の普及が進む可能性を秘めている。それは同時に、一層のアプライアンス化の動きを促すことにもなろう。

１０.2. 侵入検知･監視サービスの導入状況

侵入検知において技術的に難しい要素のひとつに、ある通信が実際に不正アクセスなのか、通常の通信なのかの判断の問題がある。この判断アルゴリズムはさまざまに工夫されているが決定的な解決は難しいのが実情で、感度を高めれば誤報の確率は増え、下げれば取り逃がしの可能性が発生することになる。そのために、プロの知識とノウハウを常時活用する手法として、専門業者による侵入検知･監視サービスが提供されている。クリティカルなネットワークを持つ企業やセキュリティにセンシティブな企業ではこのようなサービスを活用するケースが増えており、今回のケースでも、他の対策との併用も含めると 62 社 15%の企業が活用している。

ファイアウォールにおけるプロフェッショナルサービスの利用が 20%であるのと比較すると、全体の導入率が半分程度しかない中での 15%であり、相対的に外部サービスへの依存度の高い分野であ

ると言える。またその導入の歴史が比較的浅いことを考え合わせると、侵入検知におけるプロフェッショナルサービスの活用が定着しつつあると見ることができ、今後アプライアンス化とともにサービス化が進むのではないかと予想される。

１０.3. 侵入検知･防御システム製品･サービスに対する満足度

実際に IDS/IPS の製品やサービスを導入済みの企業が半数程度なので、不満についても無回答の企業が 45%に上った。何らかの回答を寄せていただいたうち、特に不満はないとしたのが全体の 42%であり、何らかの不満を寄せた企業は 55 社 13%であった。しかし有効回答の範囲で見ると約 4 分の１は不満を持っており、とりわけ機能に対する不満が多かった。

内容的には誤報問題の他、パターンファイル（攻撃かどうかの判断に用いる攻撃パターン一覧）更新スピード・頻度の問題やスループットの不満、設定の複雑さ･難しさ、更に総じて運用が難しいことへの不満が寄せられている。IDS/IPS について一般的に感じられている問題点を、ユーザーの目からも裏付けるデータと言える。

１１　アンチウイルスシステムの導入状況

コンピュータウイルスは、外部からのセキュリティ脅威の中ではもっとも普遍的に存在し、発生頻度や、実際にウイルスに感染したメールや媒体に接する機会も多い、そういう意味ではもっとも身近なセキュリティ脅威である。企業・個人を問わず、誰でも最低一度はウイルスとの接近遭遇を経験しており、また感染した経験をお持ちの方も多いと思われる。その結果、アンチウイルスシステムは、IT セキュリティ対策の中では最も一般化し、普及も進んでいるカテゴリーとなっている。そのことを反映して対策手段も多様化しており、防御のレイヤーとしても外部ネットワークとの接点であるゲートウェイから、ネットワークコンピューティングの中核を担う各種サーバーレベル、更に各個人の端末であるクライアントレベルまで階層面での多様化が進んでいる。

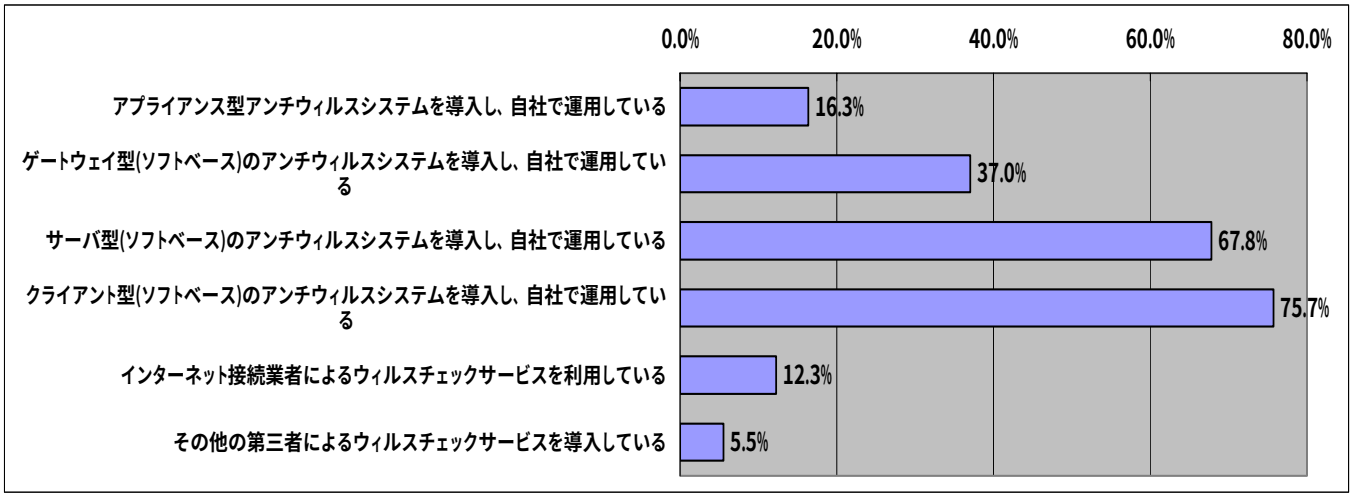


図 15　　アンチウイルスシステムの導入状況（複数回答：N=416）

また製品の態様としても、ここでも最も一般的なソフトウェア製品のみならず、アプライアンス型、専門サービス型、プロバイダーによる一体サービス型等さまざまな形態が登場している。今回のアンケートではどの製品･サービスを導入しているか、複数回答で訊いた。（図 15）

１１.1. アンチウイルスシステムの導入状況

グラフの簡略化のために、分析に影響を及ぼさない選択肢は省略した。「アンチウイルス製品･サービスはいずれも導入していない」は回答ゼロであり、ウイルス対策については何もしていない企業はないことが改めて確認できた。(但し、無回答が 3%あり。) 複数回答の選択肢に対して、対策を 1 種類だけ答えた回答数が 80 件 19%、2 種類が 175 件 42%、3 種類が 125 件 30%、4 種類活用する企業も 18 件 4%あり、実に 5 種類を使いこなす企業も 4 件 1%あった。既に何らかの対策を導入しながらも「製品･サービスの導入を予定している」にも印をつけた企業も 3 件あり、ウイルスに関しては複数の対策を施すことが常識化している実態が確認できた。

実際問題として、ウイルス被害を有効に防ぐには、ゲートウェイ、サーバー、クライアントの各レイヤー毎に対策を施す他、デスクトップファイアウォール機能や侵入検知機能を併せ持つ製品を導入してファイル共有やウェブ閲覧ルートでの感染を防ぐ等の工夫が必要である。今回の結果は、ほとんどの企業で複数の対策を講じていることが確認でき、ここでも、少なくともウイルスに関しては対策が浸透し意識が高まっていることを裏付ける結果となっている。

１１.2 レイヤー別の導入状況

対策の基本はエンドポイントを確実に守るという意味で、クライアント型のアンチウイルスシステムを導入している企業は 76%と 4 分の 3 に上った。この多くがサーバー型やゲートウェイ型との併用である。組合せとしてはゲートウェイ型、サーバー型、クライアント型の 3 レイヤー並存タイプが最も多く 101 件 24%、次いでサーバー型とクライアント型の併用が 96 件 23%、ゲートウェイ型とクライアント型の併用が 41 件 10%であり、ゲートウェイ型とサーバー型での対応も 16 件 4%程度あった。なお、この分析では位置的にゲートウェイ型と同じ役割を担うアプライアンス型もゲートウェイ型の数に含めて集計している。

一方、ネットワーク環境が比較的固定的であればゲートウェイやサーバーレベルで統合管理することでコストと効率を稼げるケースがあり、アプライアンスを含むゲートウェイ型単独導入と、サーバー型単独導入は共に 23 件 6%であった。逆にクライアント型だけで済ませているケースの方がわずかながら少なく、22 件 5%に過ぎない。

つまり、ウイルス対策は複数手段を組み合わせて、というのが常識化していると見てよいと思われる。その結果、グラフに見るように、クライアントレベルで 76%、サーバーレベルで 68%、ゲートウェイレベルで 49%（アプライアンス型も含め重複を除いた計数）と各レイヤー共その対策の浸透度は高くなっており、全く何も対策していない企業は今回回答の中ではゼロという結果につながっていると考えられる。

１１.3. アプライアンス型アンチウイルスシステムの導入状況

ウイルス対策製品は従来ソフトウェアタイプのものが主流であったが、近年アプライアンス型の製品も登場している。アプライアンス型はネットワークトポロジー上はゲートウェイに位置する。ここではスループットの高さがひとつの課題であり、その意味で専門特化が可能なアプライアンス型は魅力がある。また、アプライアンス型では単にアンチウイルスだけでなくファイアウォールや侵入検知の機能を併せ持つ機種も多い。この場合は１台で複数の機能をカバーできることが魅力であり、導入時にベンダーやシステムインテグレーション業者に設定を依存することで、専門的知識に欠ける中小

規模事業所でも複合型の対策が構築しやすくなるというメリットがある。

今回調査では、アプライアンス型アンチウイルス製品を導入している企業が、68 件 16%に上った。このうち単独設置は 20 件 5%であり、ゲートウェイ型ソフトウェアとの併用（更に他の対策との併用を含む）が 19 件 5%、それ以外との併用が 29 件 7%であった。

ウイルス対策システムはソフトウェア製品を中心に比較的早くから普及が進んできたセキュリティ対策であるが、その分野で既にアプライアンス型が 16%の普及率を見せていることは、上述のようにスループット重視、あるいは逆にオールインワン型の簡便さの両面から、今後普及が進む可能性を示しているのではなかろうか。

１１.4. ウイルスチェックサービスの導入状況

サービスについてみると、インターネット接続事業者、いわゆる iSP によるサービスが 50 件 12%、専門業者によるサービスが 23 件 6%程度の利用率となっている。合せて約 18%（両サービスの併用企業はない）と、ファイアウォールや侵入検知におけるサービスと似たような普及率となっている。どちらも、定義ファイルの常時更新やクライアントでの負荷、感染時の対策等の運用上の手間を省く意味で活用が進むと見られる領域である。

ただ、iSP によるサービスはネットワーク構成やそこで行う業務が比較的固定的な場合に依存できる性質のものであり、SOHO 等中小事業所中心になろう。一方、専門業者によるサービスはいろいろな態様が考えられ、事業規模や業態と利用度の相関は薄いと思われるが、サービスだけに頼って防御の万全を期すことは現状では難しく、ほかの対策との組み合わせで考える必要があろう。現実に、iSP によるサービスだけに依存しているケースは 4 件、その他の第三者（主として専門業者）によるサービスだけしか導入していないケースは 7 件であり、他は全て自社での対策ツールの導入・運用との組合せであった。

iSP も含む専門家によるサービスのもう一つのメリットは、ウイルスの定義ファイルの更新が自社運用よりは迅速でタイムリーに実施される可能性が高いことであろう。価格的にも比較的リーズナブルに利用可能であり、自社運用を補完するものとして活用が進むことが期待される。

１１.5. アンチウイルス製品･サービスに対する満足度

次にアンチウイルス製品･サービスに関する満足度を見てみたい。

無回答 19 件を除く 397 件のうち、273 件は「特に不満はない」ということで、率にして 66%は満足しているという結論になった。一方、「機能に不満」が 43 件 10%、「性能に不満」が 38 件 9%、「品質･信頼性に不満」が 39 件 9%（重複回答を含む）と、各々全回答企業の 10%前後に上り、他の製品よりはかなり高い率で不満が示された。これは日常もっとも関わる機会、もしくはお世話になる機会が多いのがアンチウイルスなので、それだけ問題点を意識する機会も多い結果であろうと思われる。一方、コストパフォーマンスに対する不満は 6%と一段低く、現状の価格水準がおおむね妥当なものと受け止められていると考えてよいであろう。

具体的記述としては、パターンファイル･ウイルス定義ファイルの更新スピード、タイミングが遅いというものが圧倒的に多く、29 件に上っている。ウイルス検知技術の基本がパターンマッチングである限り、このラグは宿命的に起こるが、近年、感染力の強いウイルスが頻発しており、一部には定義ファイルの更新が間に合わずに感染にいたるケースが発生しているため、不満も多くなっていると

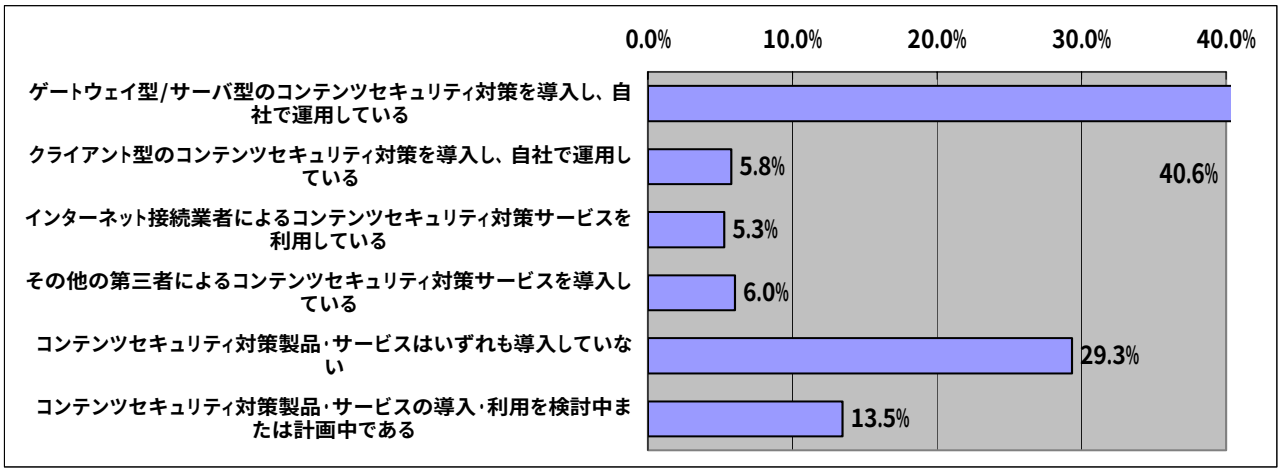
推測される。次に多いのが、製品の不具合も含めた機能不足に対する不満で 13 件、それに並んでパフォーマンスに対する不満が、マシンに負荷をかけるというものを合せると 12 件に達する。更に、バージョンアップが頻繁という不満も含めて管理に手間がかかるとした意見が 8 件あった。

ウイルスを全て防ぐことができない、等、対策手法としての限界や特性を理解しないための不満や、感染メールの受信がなくならないことへの不満など、製品の問題とは別の不満も寄せられた。メーカーの対応の悪さに対する指摘もあるが、他の不満に比べると意外と少ないというのが本音ベースの実感であり、いろいろな意味で身近になっている分、不満もあるがこなれてもいる、といったところではないだろうか。

１２　アンチウイルス以外のコンテンツセキュリティ対策の導入状況

電子メールとウェブ閲覧というインターネットの二大用途の中で、ウイルスについで近年問題となり出しているのが、スパムメール、不適正ホームページの閲覧、フィッシングといわれるだまし行為等である。これらの新たな脅威は、対策の方程式が立てにくいという要素もあって新たな脅威となって迫って来ており、アメリカの経営層の意識では、いまやウイルス以上にスパムが脅威だとする見方も出てきている。また最近では急速にフィッシング被害がクローズアップされており、これらの『迷惑系』、『だまし系』が新たな脅威として浮上してきている。

そこで今回調査では、アンチスパム、アンチフィッシング、ウェブフィルタリング等の対策ツールが、どの程度導入されているか訊くことにした。有効回答が 90%以上あることから、コンテンツセキュリティの概念も十分定着していると見てよいと思われる。ただ、コンテンツセキュリティといった場合に、コピープロテクション等、著作権や情報漏えいの関連での内容の防御という面でも使われることがあるので、



今後概念整理と共に定義の明確化が必要かも知れない。

図 16　アンチウイルス以外のコンテンツセキュリティ対策の導入状況（複数回答：N=416）

何らかのコンテンツセキュリティ対策を実施している企業は 216 社 52%であった。計画中または検討中が 55 社 13%である。（図 16）対策を実施している企業のほとんどが「ゲートウェイ･サーバー型のコンテンツセキュリティ対策を導入している」(169 社 41%、他の選択肢との重複回答を含む)である。典型的には、URL フィルタリングやスパムメールのフィルタリングによる対策となるため、アーキテクチャ的にゲ

ートウェイまたはサーバーでの対策が中心となる。また、インターネットサービスプロバイダーやセキュリティサービス業者のサービスを利用するところも 46 社 11%あった。この分野は最近になって注目されているカテゴリーであり、今後対策の導入が進むものと思われる。

次にコンテンツフィルタリング製品･サービスに関する満足度を聞いた。ここでも不満を回答した絶対数は限られるが、その内容としては、ブロック対象とする URL やドメインのリストに対して、その正確性への疑問、判断アルゴリズムのブラックボックス性、更新サイクルの遅さ等に関するものが中心となっている。

１３．個人認証システム及びユーザーID 管理の導入状況

各個人が自分の作業環境として使うクライアントパソコンそのものへのアクセスを始めとして、ネットワークログオン、各種サーバーへのログオン、データやシステムへのアクセスにおいて、いかに正当な権限を持った者を正しく認識して必要な資源を使えるようにし、それ以外の者の不正な、あるいは権限外の、あるいは想定しないアクセスをいかに防ぐかは、セキュリティ管理以前に、資源管理やシステム、データの保護という視点からも必須の、最低限備えるべき機能である。

この機能は、外部からの不正侵入・不正アクセスの防止のために必須であるのみならず、内部で発生する不正または過誤の防止策にもなる。権限外の、あるいは不要なコンピューティング資源またはデータへのアクセスは、情報漏えい、データの改ざん、システムの停止やスローダウンといった、深刻な被害に結びつく可能性が高い。またネットワークの内側にいる人間に対してはゲートウェイでのガードが無意味なため、個人認証とそれに基づくアクセス権のコントロールは最も重要で基礎的な対策であると言える。

これらは OS やアプリケーションのレベルでもそれぞれに当然の認証機能として提供されているが、その信頼性、統合管理が可能か、成りすましをいかに防ぐか、といったさまざまな観点から、多種多様なレベルで多種多様な対策が提供されている。この調査は掘り下げればそれだけで一つのアンケートを形成する程であるが、今回は一つの質問に押し込んで（複数回答）どのような手法がどの程度使われているか概容を探った。

１３.1. 個人認証システム及びユーザーID 管理の普及度・活用度

当然のことながら、ID と固定パスワードという最低限のログオンチェックは 353 社 85%で採用されている。このうち単純な ID と固定パスワードの組合せのみでユーザー認証している企業は 141 社 34%であった。212 社 51%は、固定パスワード以外の認証手段を併用していることになる。（図 17）

次に突出して多かったのが「NT ドメイン、またはアクティブディレクトリを全社的に導入し自社で運用している」で 151 社 36%に上った。比較的導入と運用が容易なマイクロソフトのソリューションへの依存度が高いことが確認できた。なお、ここでもこの選択肢単独の回答は 19 社 5%程度であり、ほとんどのケースで複数の認証手段を組み合わせて使っている。

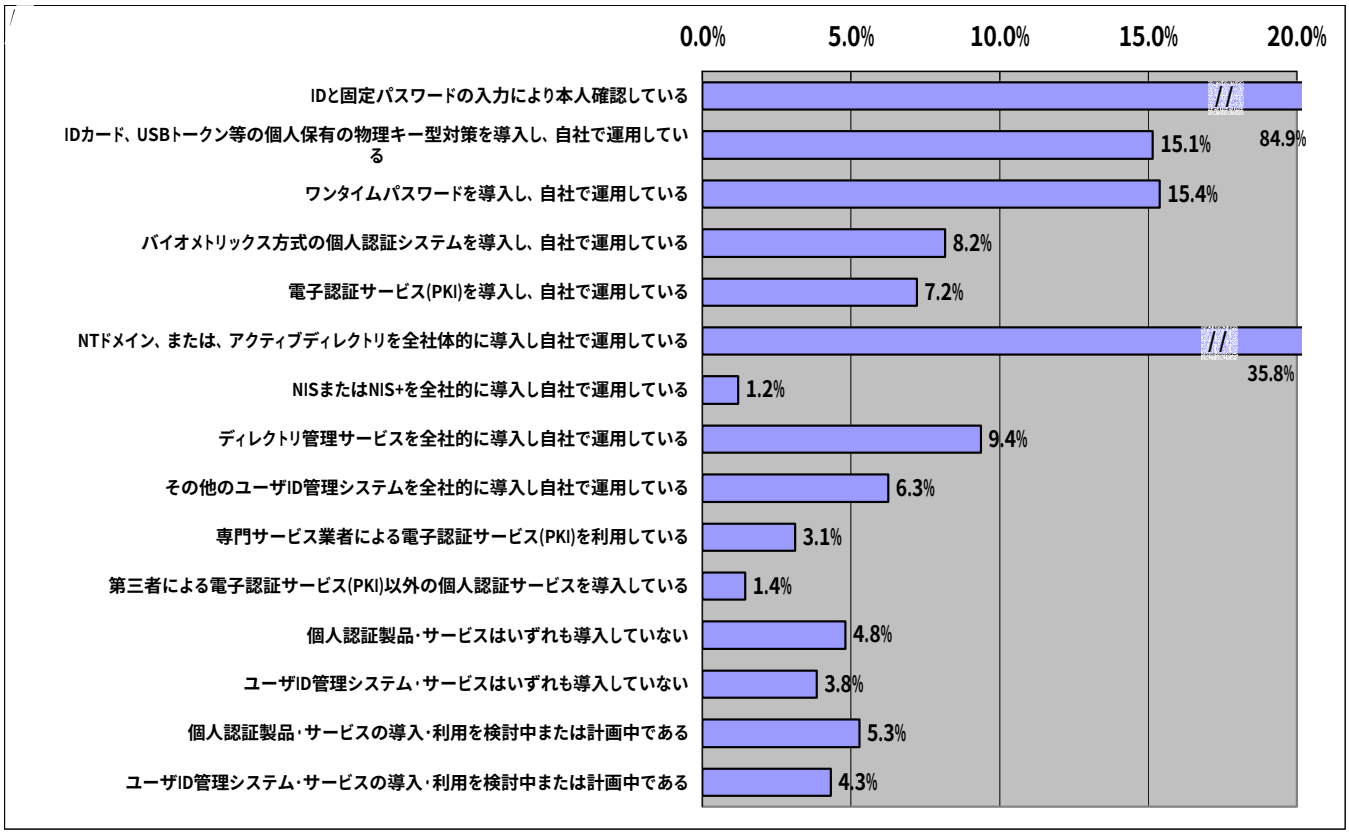


図 17　システムへのログオンに際しての個人（本人）認証及びユーザーID 管理の導入状況
（複数回答：N=416）

次に多かったのが「ID カード、USB キー等の個人保有の物理キー型対策」62 社と、「ワンタイムパスワード」61 社で、共に約 15%である。これらは、システム管理者の管理の面ならびに管理される個人の側のどちらにとっても物理的なものを介しての管理ということでシンプル性があり、導入と事後管理の両面で使いやすいことから普及が進んでいると考えられる。特に ID カードや USB キーでは、単なる個人認証だけでなく、ログオン対象の制御や暗号の応用等、そのほかの管理や防御を組み合わせることが容易であり、応用性に優れる。従い、これらシンプルなツールは導入と管理の容易さから今後も導入率の維持または拡大が期待される。なお、ここでも単独使用は各々3 件と少なく、他の手段との組合せが一般化している。

これらと似た特性を持つ認証ツールにバイオメトリックスがある。24 社約 6%が導入している。やはり導入と管理のシンプルさが誘因と考えられるが、利用する身体的特徴のバリエーションが多様化し製品種類も豊富になって話題性が高い割には導入実績はまだ限られている。バイオメトリックスの特徴は、認証の元となるデータが本人固有の物理的特長に依存し、改ざんや成りすましが困難な点が優れていることである。デバイスの多様化や低価格化、応用のバリエーションの広がりと共に今後普及して行くものと見込まれる。

このほか、ディレクトリ管理や電子認証を自社で運用しているケースが各 9%、6%と比較的回答が多かった。反面、第三者によるサービスはほとんど導入されていないことが浮き彫りになっており、やはりここでも外部サービスはまだ定着していないことが裏付けられた。

１３.2. 個人認証システム･ユーザーID 管理ソリューションの満足度

個人認証システムの満足度に関しては、このカテゴリーだけ「各個人の使い方、管理の面で不満、不安がある」という選択肢を付け加えた。結果として、やはり、この選択肢を選んだ回答企業は 104 社 25%に上っている。ID･認証という個人に密着した問題では、常に社員一人ひとりの理解と自覚と自己管理に依存する要素がつきまとうわけで、管理者としてはその点が悩みの種であることを如実に物語っていると言える。対策ツール面からのアプローチではなかなか浮かび上がらない「個人」の問題、セキュリティリテラシー、教育、ネットワーク倫理といった問題が垣間見える貴重なデータであると考える。

なお、機能、性能、品質、コストについては、各々数%の企業が不満を回答しているが、他のツールと比べても大差ないレベルの結果となっている。パスワード管理や変更以外の自由記入で目立ったのが、認証をシステム間でばらばらに実施せざるを得ないことによる煩雑さや管理の手間の問題で、シングルサインオンのソリューションへの期待がにじみ出ていた。

１４．リモートアクセスの通信安全対策

ブロードバンド接続環境が広く普及し、また世界一安いコストで利用できる環境が急速に整う中で、自宅やサテライトオフィスから仕事をする、あるいは出張先・立回り先から全くのモバイル環境で仕事をする形がかなり速いピッチで広がりつつある。その時に会社のネットワークとの間での通信をいかに安全に確保するかが極めて重要なテーマとして改めて浮上している。そこで今回の調査の中で、リモートアクセスのセキュリティについても調査することとした。

１４.1. リモートアクセスの通信安全対策の導入状況

社外から社内ネットワークに接続する場合、もっとも一般的でもっとも古くから使われてきたのが電話回線である。公衆電話や携帯電話から自社の接続点であるリモートアクセスサーバー（RAS サーバー）にダイアルアップし、そこから社内ネットワークに入る。この際に本人確認をした上で接続を許可するのが普通で、この、RAS サーバーにおける認証がやはり 143 社 34%と最も多い方式という結果が出た。（図 18）

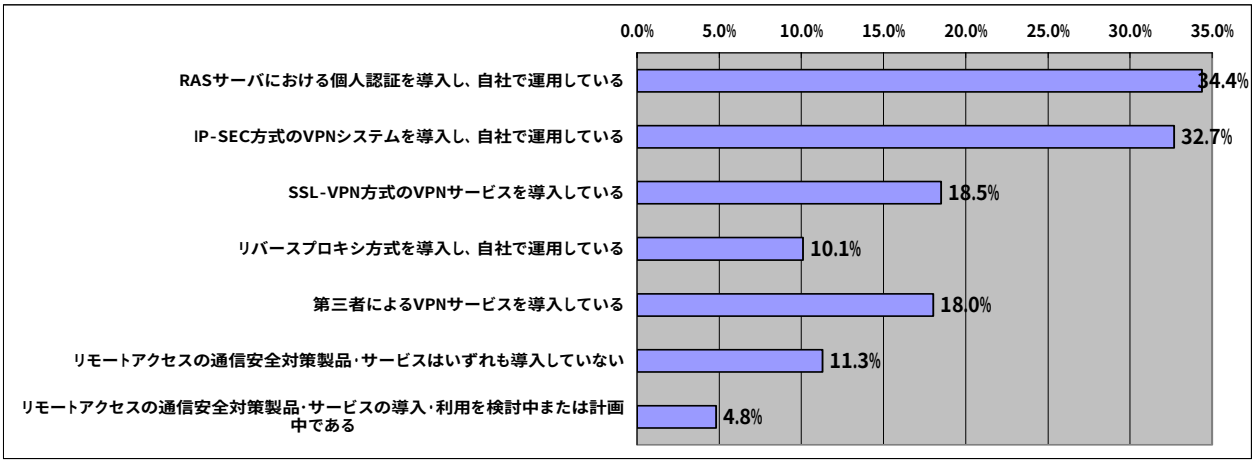


図 18　リモートアクセスの通信安全対策の導入状況（複数回答：N=416）

他の方式としては、プロバイダーのアクセスポイントまでダイアルアップで接続し、そこからインターネットまたはプロバイダーのリモートアクセスサービスネットワークに入るもの、更には無線 LAN の接続ポイントであるホットスポットを利用して直接インターネット接続を得るものと、リモートアクセスのサービスは多様化してきている。これらの通信経路の多くはオープンな状態で、第三者による盗み見や改ざんの可能性を秘めている。その防止策として、暗号通信を組み合わせることが一般化しており、VPN（仮想私設網）と呼ばれて普及している。

メーカー間の差異を吸収して相互接続性を確保する目的で規格化がされており、そのもっとも代表的なものが IP-SEC 方式と言われている。この IP-SEC 方式の VPN も RAS とほとんど同じ普及率で、136 社 33%の企業が採用していることが明らかになった。また、クライアント側に特別のアプリケーションを必要としない等、最近その使い勝手から注目を集めている SSL-VPN も 76 社 19%とかなり使われるようになっている。SSL-VPN 対応では、社内ネットワーク側の接続点を専用装置で簡単に実現するアプライアンス型製品等も出だしていることもあり、導入と運用の容易さから、今後更に普及することが見込まれる。

なお、余談であるが、JNSA では長年にわたり IP-SEC 準拠の VPN 装置の相互接続性評価に取り組んで来ている。規格準拠とは言え、メーカー間で場合によっては通信がうまく行かないことが多かった IP-SEC 方式を、実際に各ベンダーから機器の提供を受け、JNSA 内の有志参加者で接続性を検証する作業は、ベンダーにもユーザーにも安心と保証を与えることができ、IP-SEC VPN の普及に大きく貢献したものと自負している。IP-SEC VPN の普及率の高さの裏には、このような取り組みの成果が生きているものと思われる。

他の対策手段と様子を異にするのが、第三者による VPN サービスの利用が 18%とかなり高いことである。これは、他のセキュリティ対策における第三者サービスが、多かれ少なかれ自社のシステムやネットワークの情報もしくは資源に対するアクセスを第三者に提供する必要があるところが抵抗感を呼ぶのに対し、VPN サービスは純粋に通信経路部分をサービスとして受けられるところが、比較的容易に導入できる要因になっているのではなかろうか。

その他、少数だが「リモートアクセスは実施しない、または認めない」とするコメントをいただいた。「導入していない」「その他」の中には、ポリシーとして、安全策重視の観点から、また労務管理の必要上、あるいは単純に業務上のニーズが限られていることから、社員によるリモートアクセスを一切認めないとする企業が少なからずあることも認識しておきたい。

１４.2. リモートアクセスの通信安全対策に対する不満･不安

有効回答数の約 70%は不満はないとしており、総体に満足度は高い。有効回答数に対する不満件数の率で見ると、機能について 10%、性能について 11%、品質について 7%、コストについて 7%と、それでも一定程度の不満はある模様である。これはやはり、日常比較的身近に接する機会の多いサービスであることによるものであろう。

不満要素に関する自由記述回答では、通信速度が遅いことに対する不満が多かった。これはダイアルアップ回線自体のスループットを問題にするもの、VPN のスループットを問題にするものの両方があった。前者はセキュリティ対策の問題としては質を異にするが、IT 管理者にとっては悩みの種ということであろう。次に多いのは、通信コストの問題で、これもセキュリティ問題とは別問題ではあるが、共通の悩みのようである。セキュリティの課題としては「不安」を上げるものが多いが、具体

的な安全への脅威や事故の例は見られず、漠然とオープンな環境を通ってくる通信ということに対する不安と解釈される。この他、端末の操作やスループット上の負荷･負担を指摘する声もいくつかあった。

厳しい企業ではリモートアクセスを認めないところもあるが、やはり利便性と業務効率からリモートアクセスを活用しているものの、どこまで何をやれば安心できるのか、漠然とした不安があることが確認できた。プロのプロバイダーによるサービスの活用が進み、PKI が普及するようになれば、この辺も緩和されてくるのではないかと期待される。

１５．脆弱性検査、ポリシー監査システムの導入状況

OS や通信モジュールや各種アプリケーションにおける脆弱性の発見が相次ぎ、その弱点を狙うことで被害を発生させるワーム等の攻撃が、その頻度と危険度を増している中で、自社のシステムに潜む脆弱性をいかに未然に発見して事故が起こる前に手を打つか、という取り組みが、以前より格段に重要性を増してきている。また潜在的脆弱性の大きな要素として、決められたポリシーから外れた設定のままでシステムを運用していたり、アプリケーションその他の設定の中で知らないうちにセキュリティ管理基準に外れた設定に変わっていたりする問題がある。これらの点をカバーして、弱点を未然に発見することで脆弱性を補い、また適正な設定に導くことで未然にセキュリティホールを塞ぎ、不足の被害を予防するのが脆弱性検査･ポリシー監査ツールである。

これらツールはセキュリティの脅威に対する事前的、あるいはリアルタイム的対策ツールである。脆弱性評価にはそのアプローチの違いからネットワークスキャン型とホスト型がある。ネットワークスキャン型は、インターネットから、あるいは社内ネットワークの内側から、ネットワーク上のサーバー等コンピューティング資源に対して、ハッカーと同様のアクセス手法を使って不正侵入の可能性をテストするものである。これにより、あらかじめ、ハッカーから見たときの自社のネットワークの弱点を把握し、対策を施すことで、起こりうる不正侵入を未然に防ぐことを目的とする。

一方、ホスト型の脆弱性検査・ポリシー監査システムとは、検査対象となるサーバー等のホストに、検査のためのアプリケーションソフトを走らせて、そのホスト自身の脆弱性を診断するもので、あらかじめ設定したインプットパラメータに対して、実際にそのマシンの設定が要求を満たしているか、あるいは不足しているかをチェックして報告するツールである。ハッカーの脅威に対する予防という視点もさることながら、システム運用上のセキュリティポリシーに対して、ネットワーク上の資源の実際の設定や運用のデコボコをならして全体としてのセキュリティレベルを、設定したレベルにそろえることを狙いとする。

つまり両者は対外的防御と内部管理の各々の視点からセキュリティの弱点を指摘するツールである。このように基礎体力改善対策はベースラインの確保という意味で重要であり、それらがどの程度普及しているかを調べた。結論としては、残念ながら、この対策カテゴリーはまだほとんど普及していないのが実態であるということである。

１５.1. 脆弱性検査･ポリシー監査システムの導入状況

脆弱性検査･ポリシー監査システムの導入はネットワークスキャン型で 61 社 15%、ホスト型で 22 社 5%であり、両方実施している企業もあるため、ネットワーク型にしろホスト型にしろ何らかの対策を自社で実施しているとする回答は 64 社にとどまり、率では 15%超に過ぎない。（図 19）

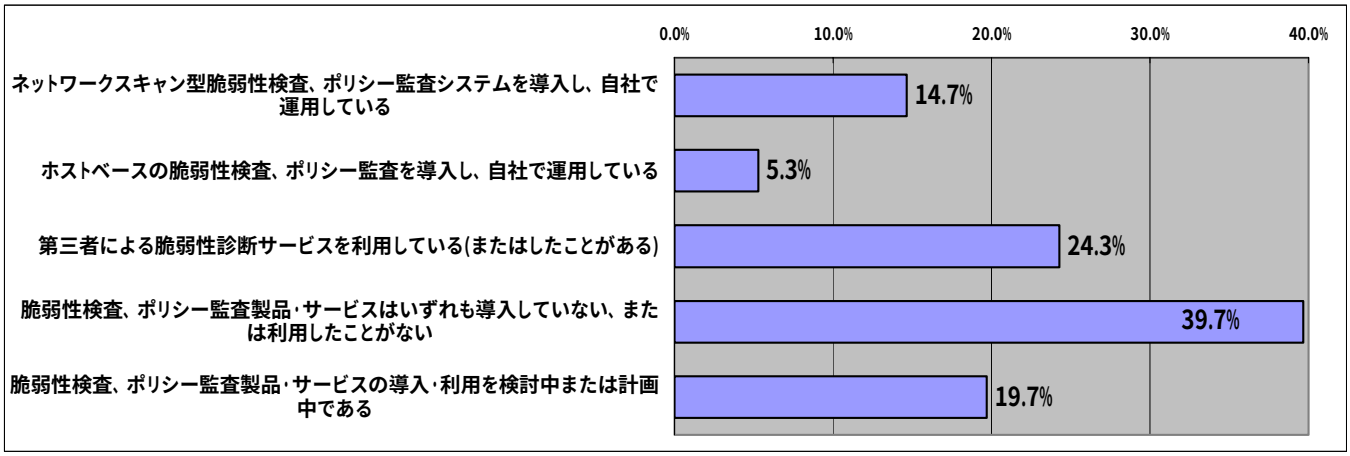


図 19　　脆弱性検査･ポリシー監査システムの導入状況（複数回答：N=416）

一方、他の対策と著しく状況が異なるものに、第三者による脆弱性診断サービスの利用があり、自社対応との併用も含めると、ちょうど 100 社 24%が利用している。つまりその利用率が他の対策手段に比べて高いと同時に、このカテゴリーにおいてだけ自社での実施を第三者サービスの利用が上回っていることである。この種の検査はある程度専門知識を必要とすること、また当事者が見落としているものを別の視点であぶりだす意味で、第三者の目で実施することに意味がある面がある。その意味では自社での対策よりは第三者のサービスを活用することが望ましいカテゴリーであり、それを反映した結果になっていると言える。

一方で「全く導入･利用したことがな」く、導入･利用の検討も計画もしていない企業が 161 社 39%ある。脆弱性検査の意味や必要性がまだ十分浸透していないことが原因と思われる。この状況は日々潜在的セキュリティ脅威が高まっている現状からははなはだ残念な結果ではあるが、今後ユーザー側の理解が深まり状況が改善することを期待すると共に、ベンダーの立場からは一層の普及啓発への取り組みの必要を痛感する。

救いは「導入・利用予定」が 20%あることである。ネットワークとそこに接続しているコンピューティング資源について、インシデントが発生する前から健康状態を常時チェックするというのは、必要性が理解できてもなかなか実施できない部分ではあるが、ひとたび事故が起こってからではその被害は計り知れないものにもなりかねず、日常から定期的にヘルスチェックを実施しておくことが望まれる。

この種の診断は健康診断を医師に頼るのと同様、プロに依存することにも意味があり、かつその価格も普及に連れてリーズナブルなものになりつつあるので、年度毎、期毎に予算化することで定期的にチェックしておくことが望まれる。またそのような需要喚起と対応して、サービスの提供側も質の高い、適正な価格水準のサービスを提供するべく努力していくことが求められる。

１５.2. 脆弱性検査、ポリシー監査の導入･運用上の不満・問題点

このカテゴリーについては、導入企業の絶対数が少ないため、不満や問題点を回答した件数もかなり少なかった。その中で相対的に多かったのが「費用対効果」に対する不満である。これは、脆弱性診断とその対策があたかもセキュリティの健康診断のようなもので、実施しないことの効果というか結果が必ずしも現れるとは限らないのに対し、コストのほうは否応なくかかることに起因すると思

われる。また検査のコストも対象のマシン数が増えると総額的に膨らむケースがあり、費用対効果に対する目を一層厳しくするものになっているものと思われる。この問題も含め、健康診断とそれに基づく予防措置が、結果的にセキュリティ対策として有効な手段であるとの認識を浸透させていく必要を感じる。

第五章　おわりに

以上、今回得られたデータを元に、情報セキュリティ対応体制、情報セキュリティガバナンスならびに IT セキュリティ対策の導入状況とその満足度を見てきた。対応体制が思いのほか高率で整えられており、情報セキュリティガバナンスの「始めの一歩」とも言うべき情報セキュリティポリシーへの取り組みがほとんどの企業で対応できていることを確認できたのは大きな成果であった。と同時に、それが経営管理プロセスの一環として組み入れられ定着するところまでは到達していない実態もうかがわれ、情報セキュリティ対策はようやく動き出したものの、それが本当に活かされるにはもう一段の取り組みが必要と感じる。

今回調査では、とりあえずユーザーの実態を知ること、またさまざまな切り口の情報を幅広く知りたいという調査側の希望から、総花的・網羅的な調査となった。結果として全体像を知り問題点の所在を伺うには期待以上の成果を得ることができた。期末の忙しい時間を割いて短納期のアンケート調査にご協力いただいた各社のご担当役員・責任者の方々には厚くお礼申し上げたい。

JNSA としては、このような形の実態調査を今回の成果を踏まえて継続すると共に、将来的に情報セキュリティの市場実態を定量化する試みにも取り組む必要があると考えている。ベンダー団体としての立場から来る困難さと責任の両面を見据えつつ、情報セキュリティの更なる浸透と定着、そして業界の健全な発展とそれによる社会貢献に資する市場調査を実現するべく、今後も積極的な取り組みを進めたいと考えている。

ユーザー企業、関連諸団体、会員企業諸氏の引き続いてのご協力と、ご指導ご支援をお願いし、今回のアンケートに対するご協力に感謝して、本報告の結びとしたい。ご協力ありがとうございました。

以上

第三部　デ ー タ 編

＜その１＞

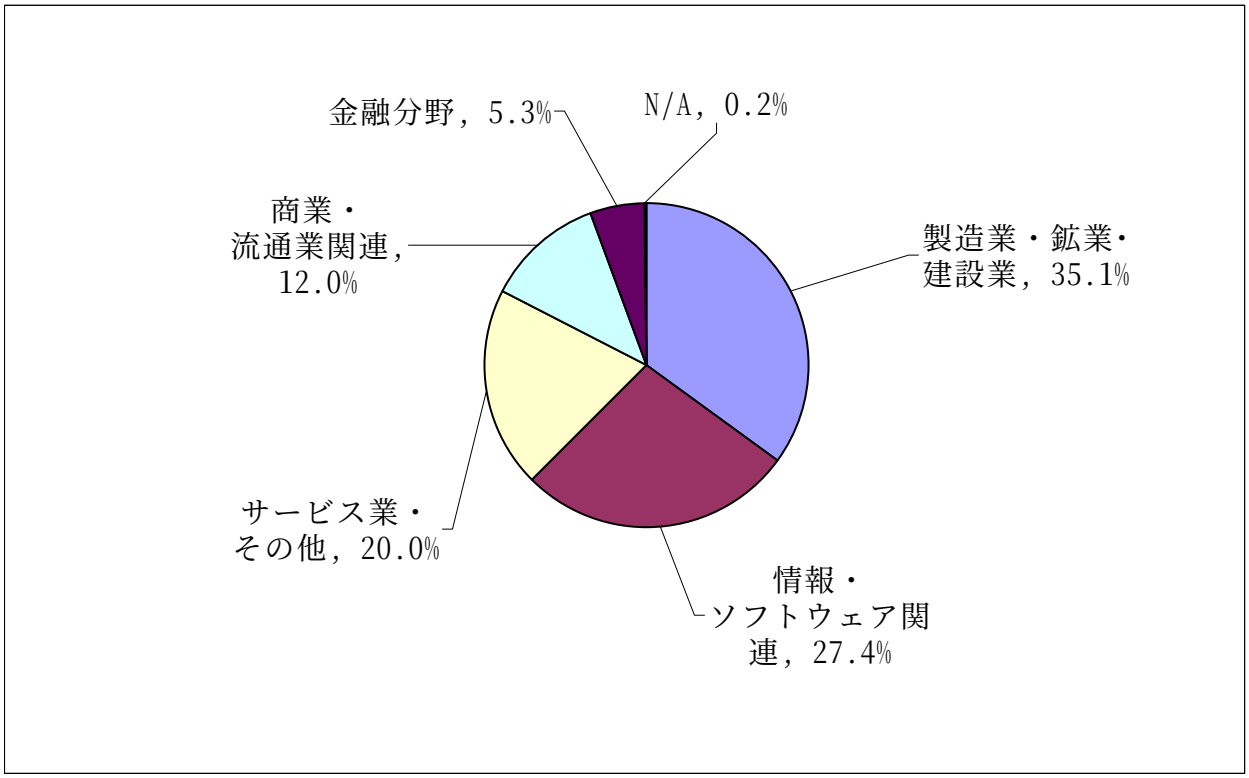
質問項目別回答数と分布

ならびに自由記述コメント

第一部 回答企業プロフィール

1.業種

	製造業・鉱業・建設業	情報・ソフトウェア関連	サービス業・その他	商業・流通業関連	金融分野	N/A	合計
回答数	146	114	83	50	22	1	416
占有率	35.1%	27.4%	20.0%	12.0%	5.3%	0.2%	100%

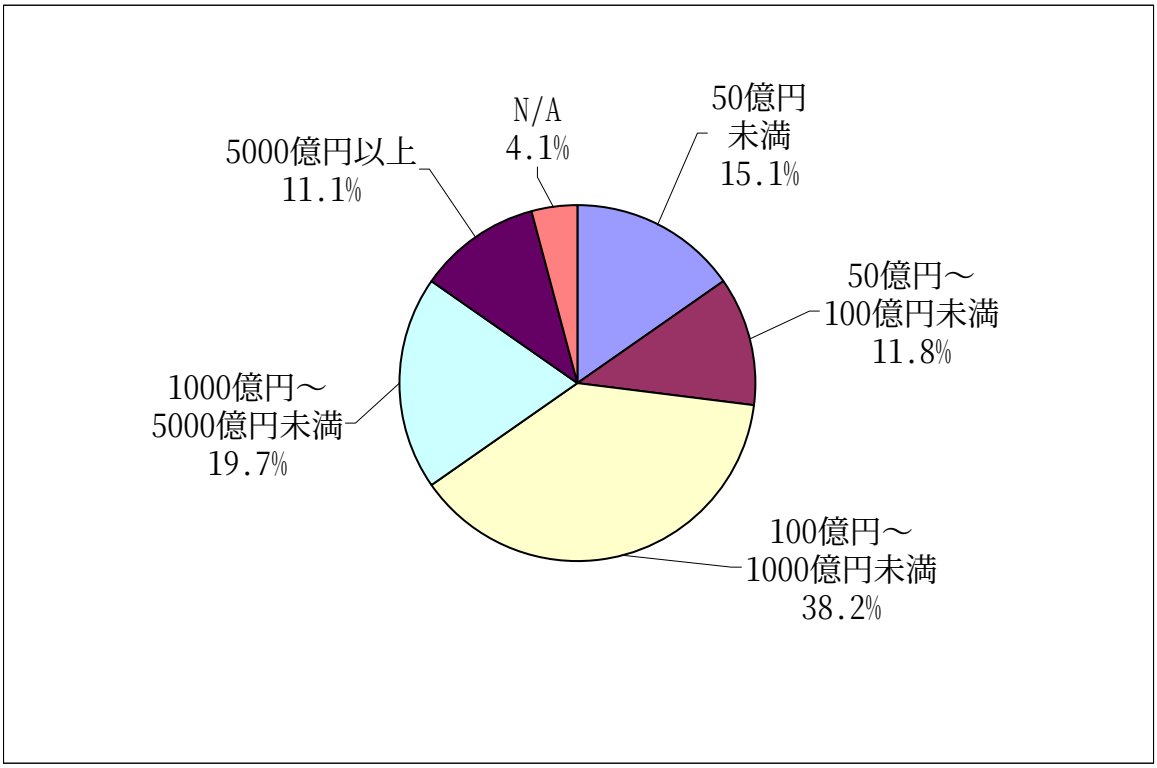


Note

・今回のアンケート回答を業種別に見てみると、「製造業・鉱業・建設業」が 35.1%と最も多く、続いて「情報・ソフトウェア関連が 27.4%、「サービス業・その他」が 20.0%、「商業・流通業関連」が 12.0%、「金融分野」が 5.3%となった。

2.年間売上規模

	50億円未満	50億円～100億円未満	100億円～1000億円未満	1000億円～5000億円未満	5000億円以上	N/A	合計
回答数	63	49	159	82	46	17	416
占有率	15.1%	11.8%	38.2%	19.7%	11.1%	4.1%	100.0%

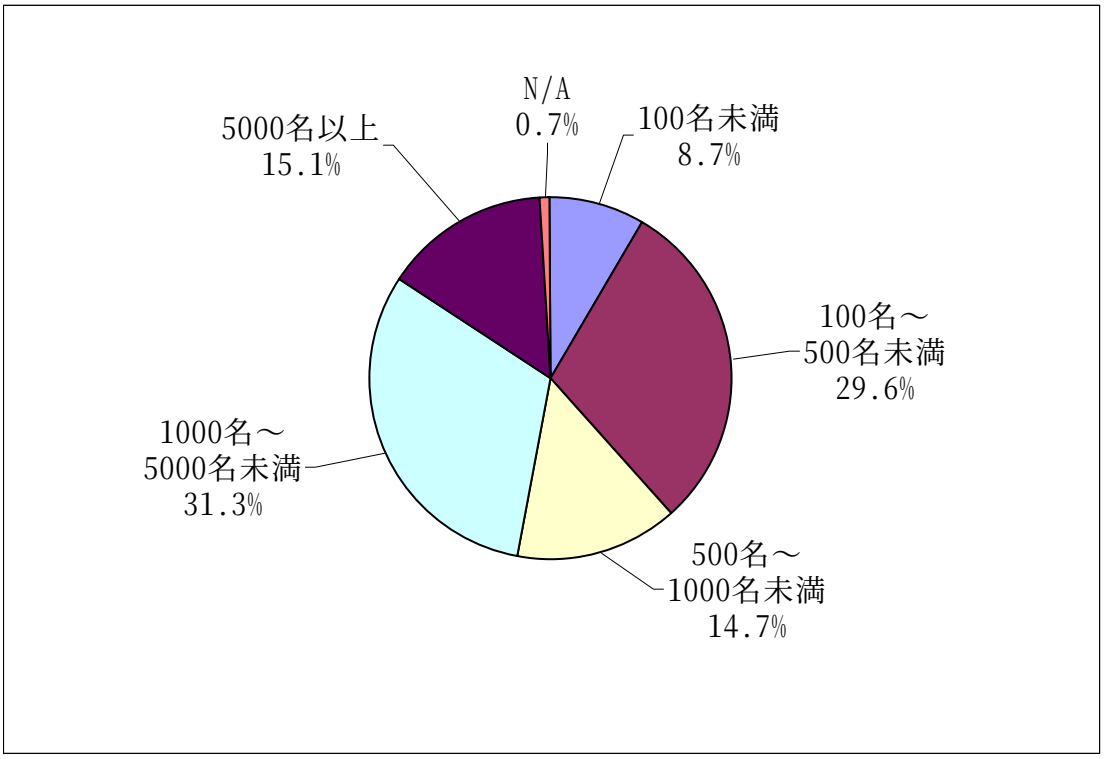


Note

・年間売上規模別に見てみると、「50 億円未満」が 15.1%、「50 億円～100 億円未満」が 11.8%、「100 億円～1000 億円未満」が 38.2%、「1000 億円～5000 億円未満」が 19.7%、「5000 億円以上」が 11.1%となった。

3.従業員数

	100名未満	100名～500名未満	500名～1000名未満	1000名～5000名未満	5000名以上	N/A	合計
回答数	36	123	61	130	63	3	416
占有率	8.7%	29.6%	14.7%	31.3%	15.1%	0.7%	100.0%

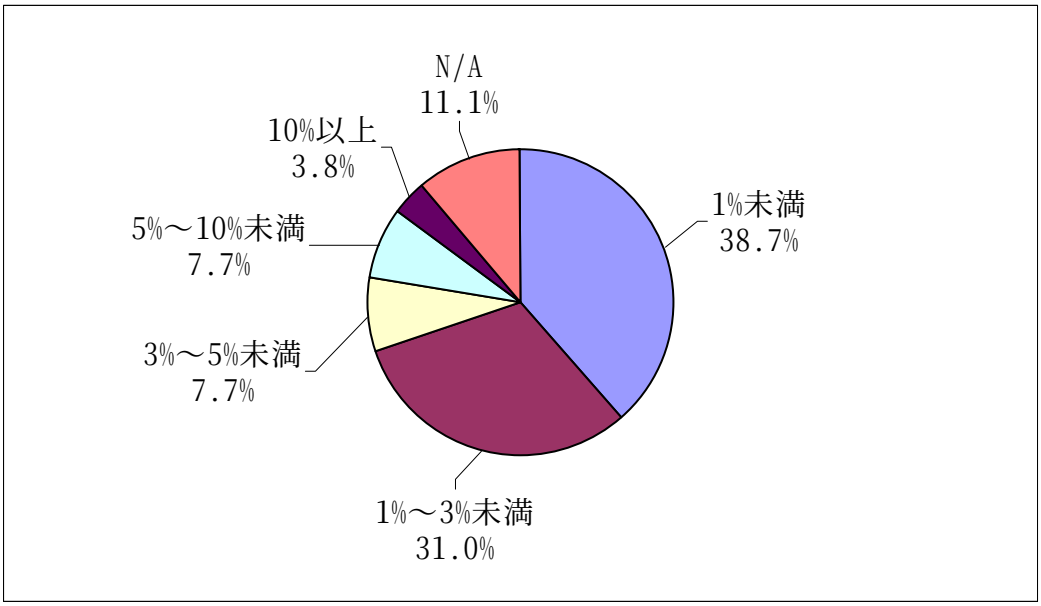


Note

・従業員数別に見てみると、「100 名未満」が 8.7%、「100 名～500 名未満」が 29.6%、「500 名～1000 名未満」が 14.7%、「1000 名～5000 名未満」が 31.3%、「5000 名以上」が 15.1%となった。

4.売上高に占める年間 IT 予算規模

	1%未満	1%～3%未満	3%～5%未満	5%～10%未満	10%以上	N/A	合計
回答数	161	129	32	32	16	46	416
占有率	38.7%	31.0%	7.7%	7.7%	3.8%	11.1%	100.0%



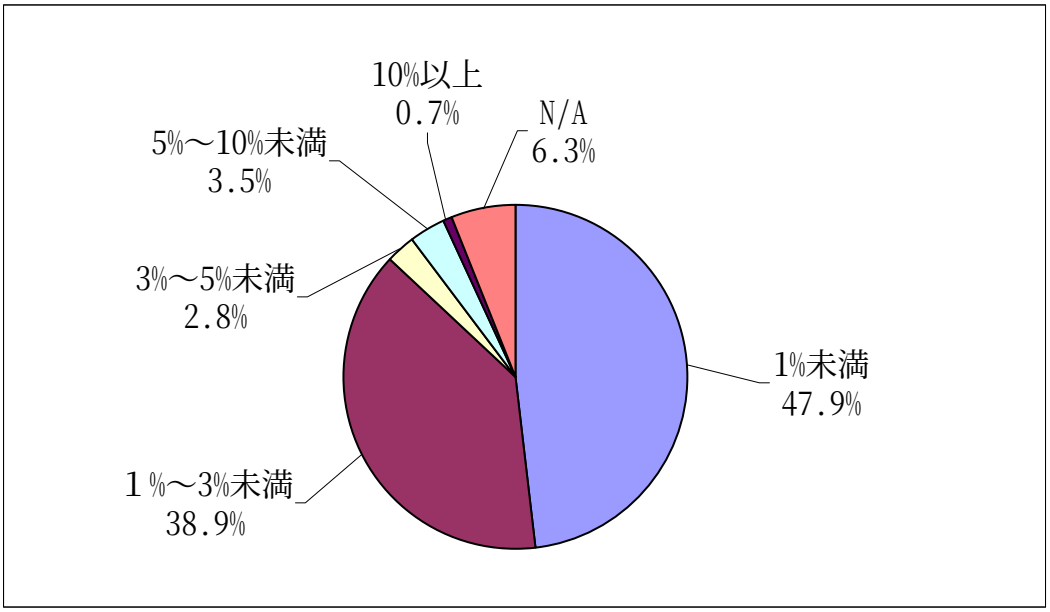
Note

・売上高に占める年間 IT 予算規模別に見てみると、「1%未満」が 38.7%、「1%～3%未満」が 31.0%、「3%～5%未満」が 7.7%、「5%～10%未満」が 7.7%、「10%以上」が 3.8%であった。

4.売上高に占める年間 IT 予算規模(a)

業種別：製造業・鉱業・建設業

	1%未満	1％～3%未満	3%～5%未満	5%～10%未満	10%以上	N/A	合計
回答数	69	56	4	5	1	9	144
占有率	47.9%	38.9%	2.8%	3.5%	0.7%	6.3%	100.0%



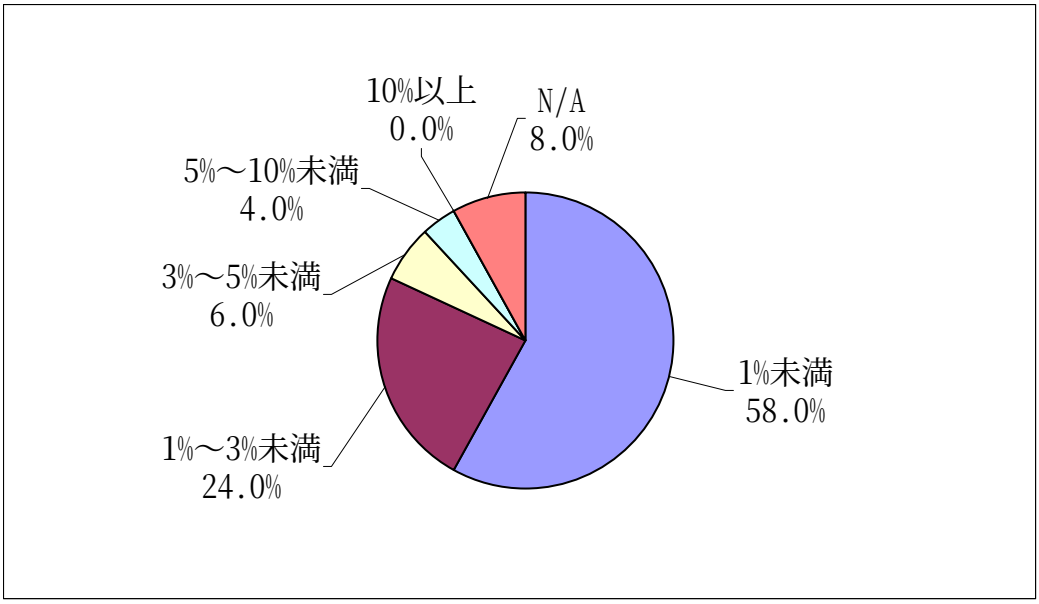
Note

・売上高に占める年間 IT 予算規模を業種別に見てみると、「製造業・鉱業・建設業」では、「1%未満」が 47.9%、「1%～3%未満」が 38.9%、「3%～5%未満」が 2.8%、「5%～10%未満」が 3.5%、「10%以上」が 0.7%であった。

4.売上高に占める年間 IT 予算規模(b)

業種別：商業・流通業関連

	1%未満	1%～3%未満	3%～5%未満	5%～10%未満	10%以上	N/A	合計
回答数	29	12	3	2	0	4	50
占有率	58.0%	24.0%	6.0%	4.0%	0.0%	8.0%	100.0%



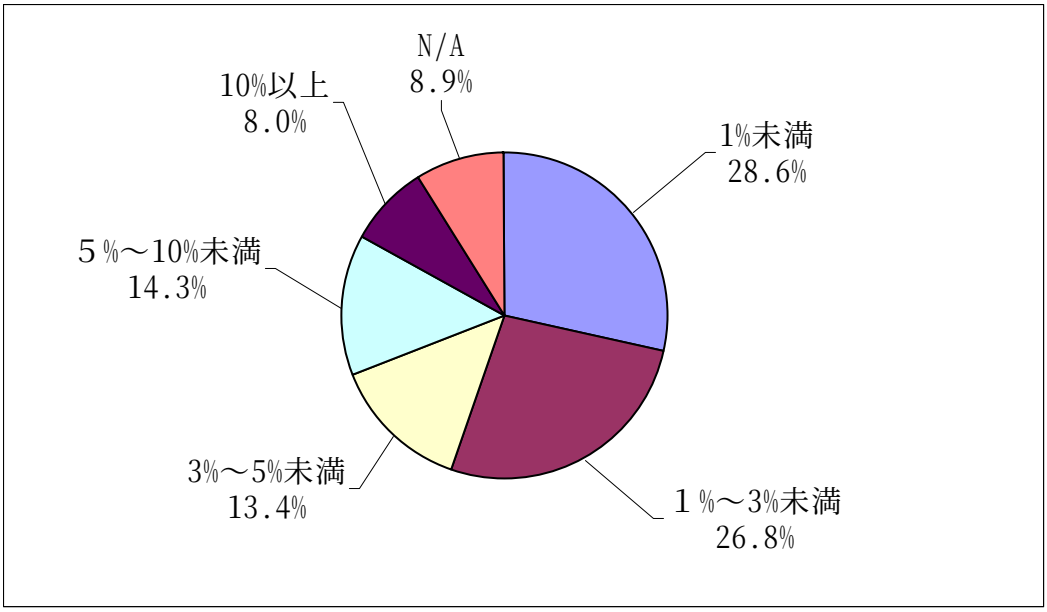
Note

・売上高に占める年間 IT 予算規模を業種別に見てみると、「商業・流通業関連」では、「1%未満」が 58.0%、「1%～3%未満」が 24.0%、「3%～5%未満」が 6.0%、「5%～10%未満」が 4%、「10%以上」が 0%であった。

4.売上高に占める年間 IT 予算規模(c)

業種別：情報・ソフトウェア関連

	1%未満	1％～3%未満	3%～5%未満	5％～10%未満	10%以上	N/A	合計
回答数	32	30	15	16	9	10	112
占有率	28.6%	26.8%	13.4%	14.3%	8.0%	8.9%	100.0%



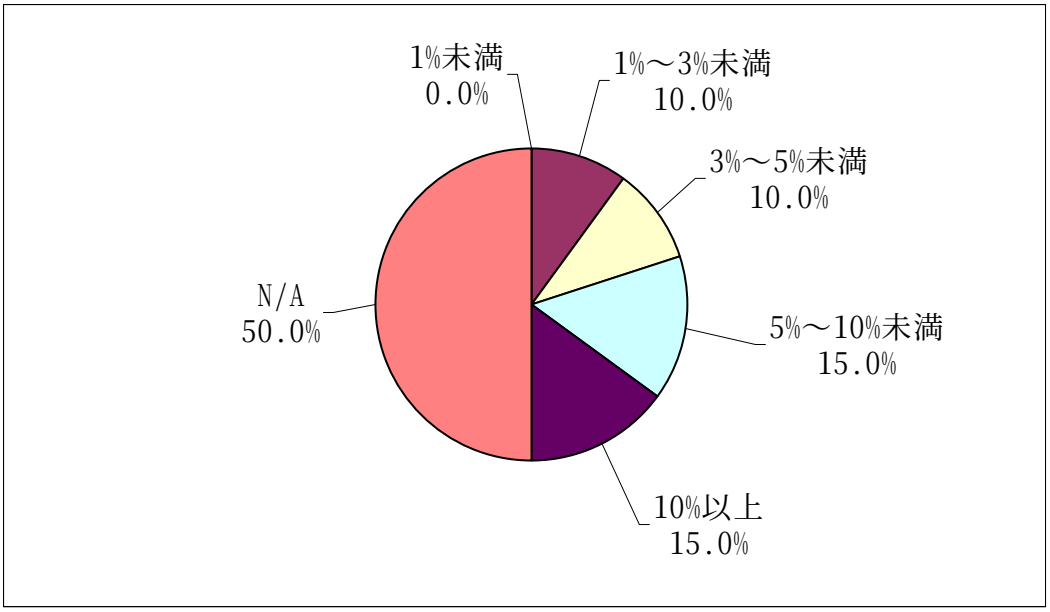
Note

・売上高に占める年間 IT 予算規模を業種別に見てみると、「情報・ソフトウェア関連」では、「1%未満」が 28.6%、「1%～3%未満」が 26.8%、「3%～5%未満」が 13.4%、「5%～10%未満」が 14.3%、「10%以上」が 8.0%であった。

4.売上高に占める年間 IT 予算規模(d)

業種別：金融分野

	1%未満	1%～3%未満	3%～5%未満	5%～10%未満	10%以上	N/A	合計
回答数	0	2	2	3	3	10	20
占有率	0.0%	10.0%	10.0%	15.0%	15.0%	50.0%	100.0%



Note

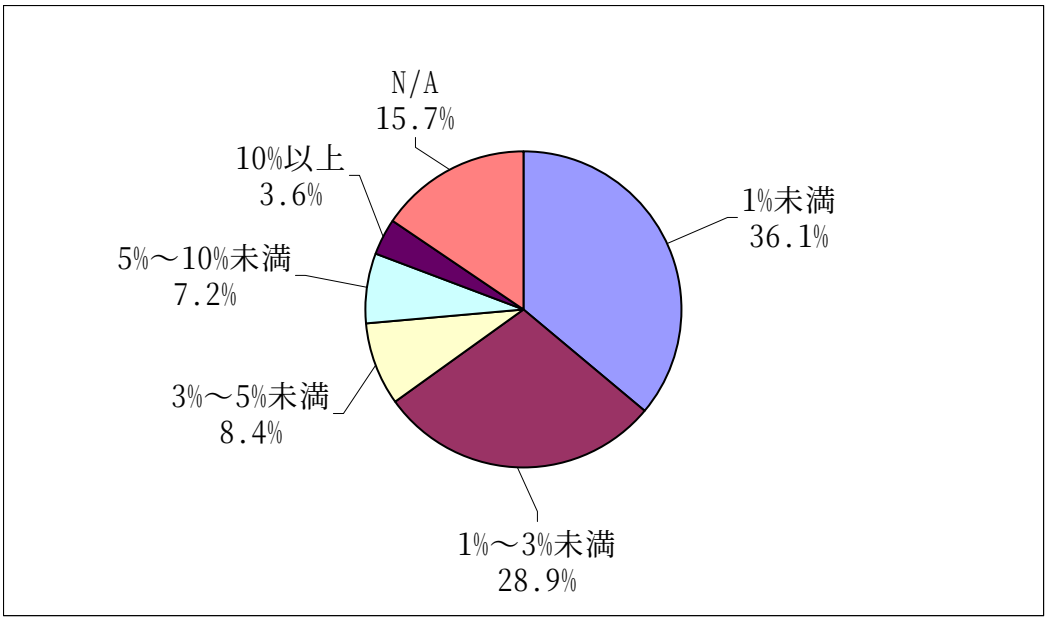
・売上高に占める年間 IT 予算規模を業種別に見てみると、「金融分野」では、「1%未満」が 0%、「1%～3%未満」が 10.0%、「3%～5%未満」が 10.0%、「5%～10%未満」が 15.0%、「10%以上」が 15.0%であった。

・金融機関の場合、「売上高」に直接該当する経営指標がないため、N/A が半数になったと思われる。有効回答の 10 件は、経営収益対比で回答いただいたものと推測される。

4.売上高に占める年間 IT 予算規模(e)

業種別：サービス業・その他

	1%未満	1%～3%未満	3%～5%未満	5%～10%未満	10%以上	N/A	合計
回答数	30	24	7	6	3	13	83
占有率	36.1%	28.9%	8.4%	7.2%	3.6%	15.7%	100.0%

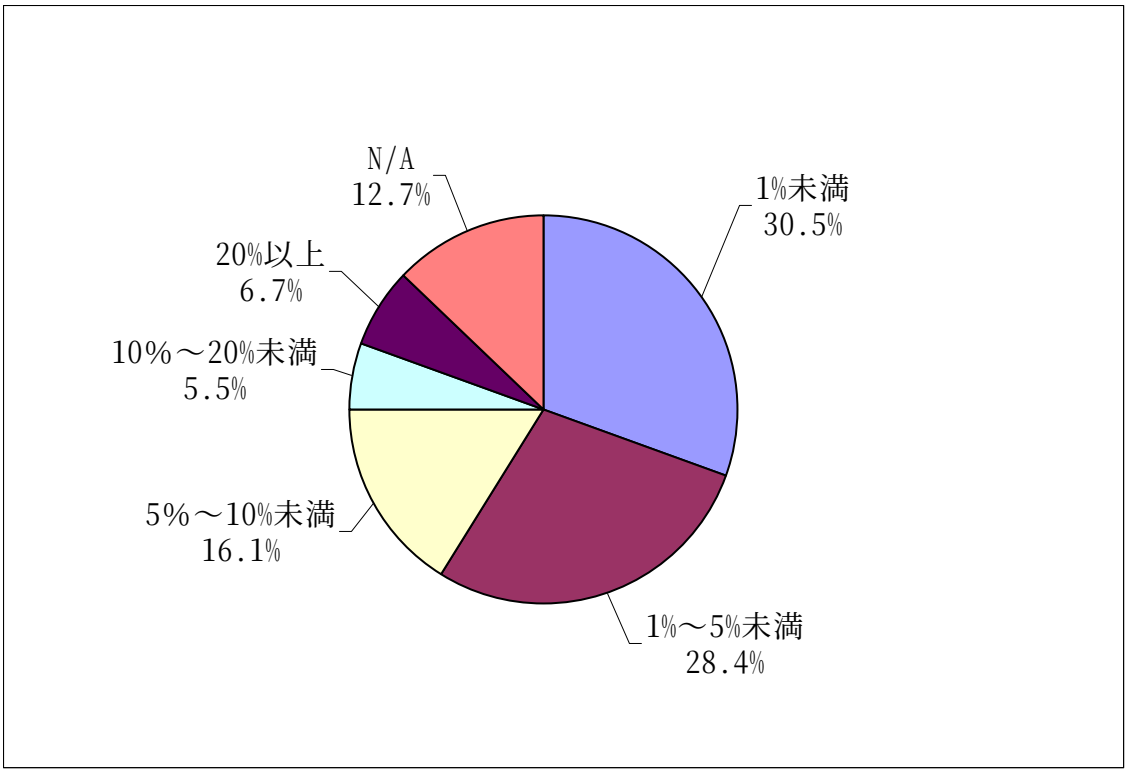


Note

・売上高に占める年間 IT 予算規模を業種別に見てみると、「サービス業・その他」では、「1%未満」が 36.1%、「1%～3%未満」が 28.9%、「3%～5%未満」が 8.4%、「5%～10%未満」が 7.2%、「10%以上」が 3.6%であった。

5.IT 予算の中のセキュリティ費用・投資の占める割合

	1%未満	1%～5%未満	5%～10%未満	10%～20%未満	20%以上	N/A	合計
回答数	127	118	67	23	28	53	416
占有率	30.5%	28.4%	16.1%	5.5%	6.7%	12.7%	100.0%

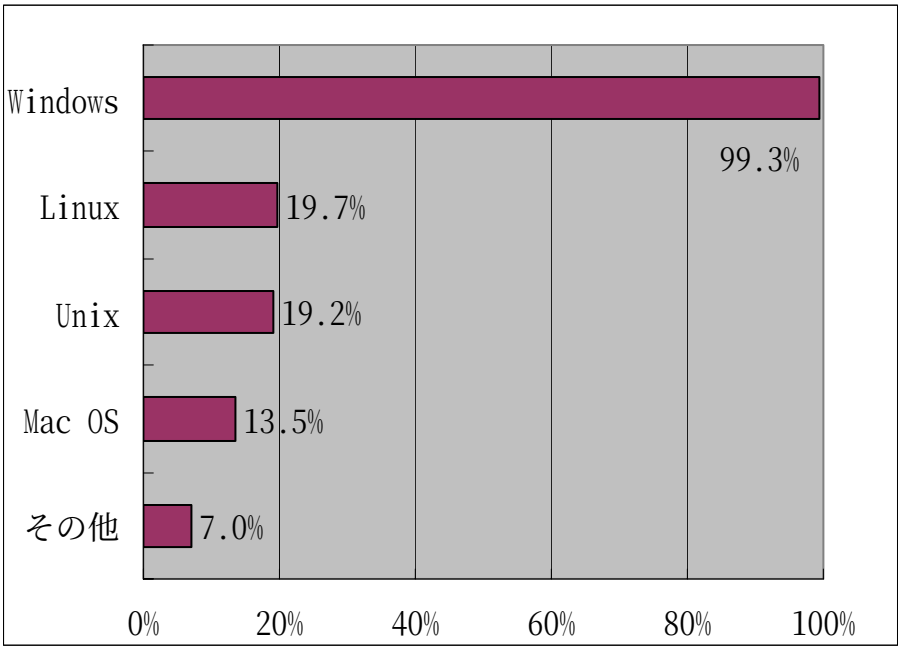


Note

・IT 予算の中のセキュリティ費用・投資の占める割合を見てみると、「1%未満」は 30.5%、「1%～5%未満」は 28.4%、「5%～10%未満」は 16.1%、「10%～20%未満」は 5.5%、「20%以上」は 6.7%であった。

6.ご利用されているクライアントの OS（複数回答可）n=416

	Windows	Linux	Unix	Mac OS	その他	合計
回答数	413	82	80	56	29	660
占有率	99.3%	19.7%	19.2%	13.5%	7.0%	158.7%



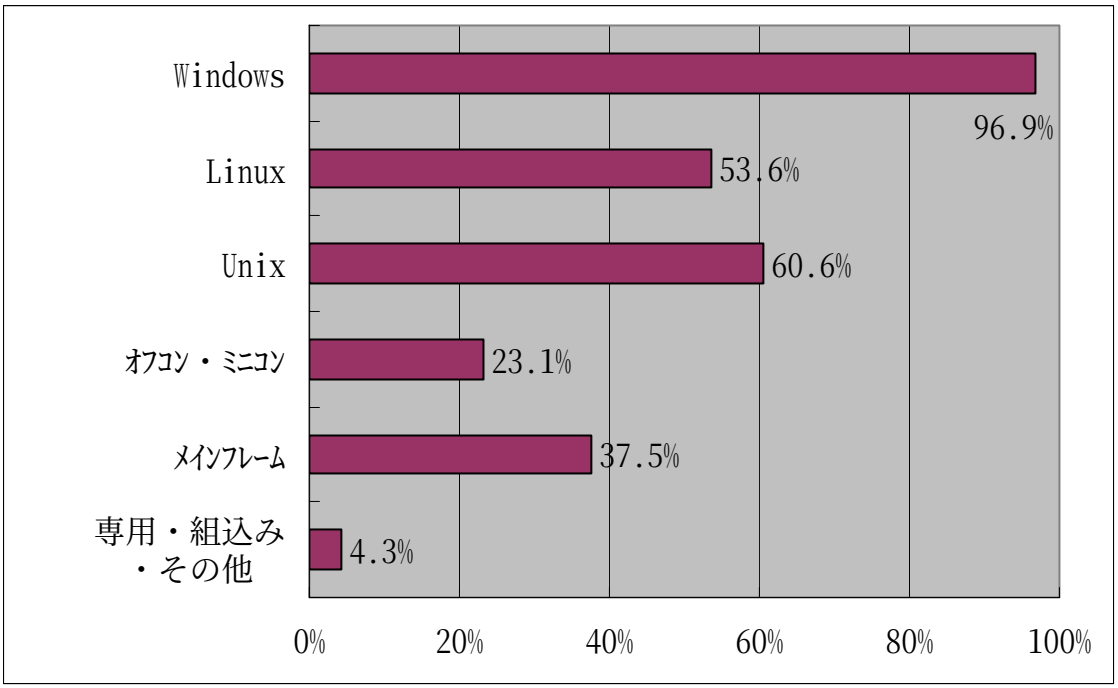
Note

・利用しているクライアント OS は、「Windows」が 99.3%、「Linux」が 19.7%、「Unix」が 19.2%、「Mac OS」が 13.5%、その他が 7.0%となった。

・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。

7.ご利用されているサーバーの OS・システム（複数回答可）n=416

	Windows	Linux	Unix	ｵﾌｺﾝ・ﾐﾆｺﾝ	ﾒｲﾝﾌﾚｰﾑ	専用・組込み・その他	合計
回答数	403	223	252	96	156	18	1148
占有率	96.9%	53.6%	60.6%	23.1%	37.5%	4.3%	276.0%



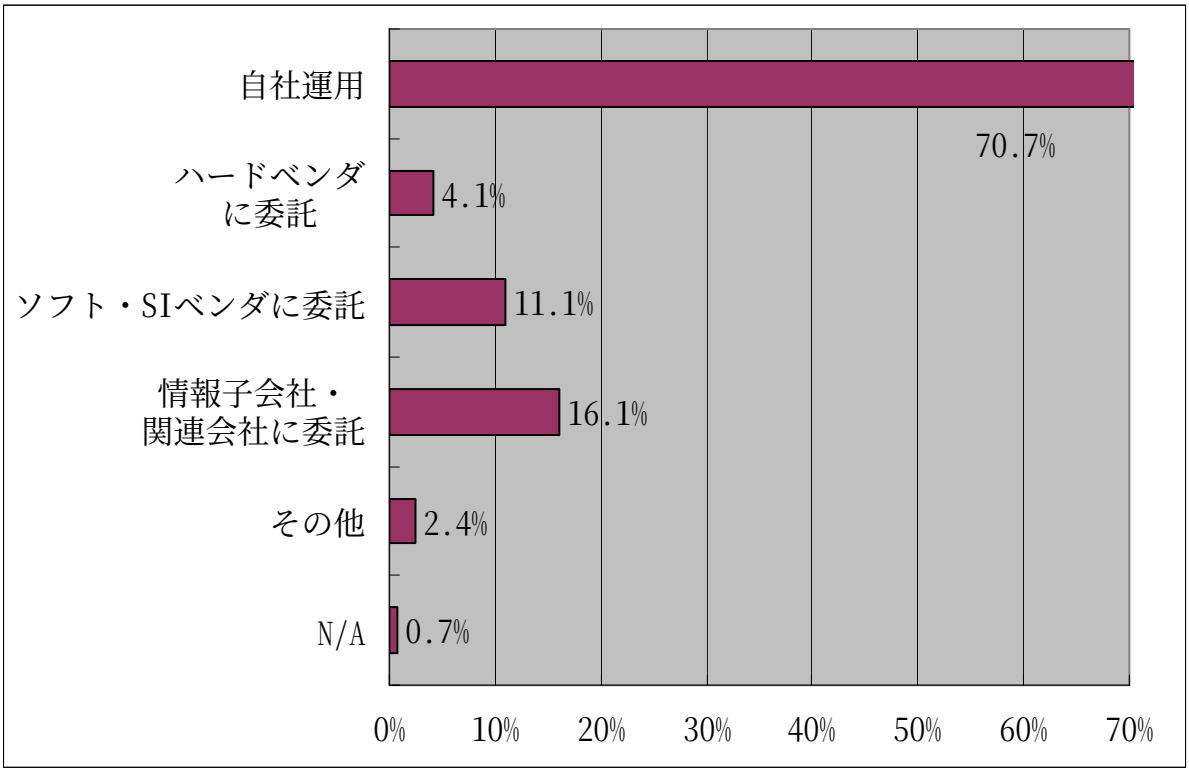
Note

・利用しているサーバーの OS・システムは、「Windows」が 96.9%、「Linux」が 53.6%、「Unix」が 60.6%、「オフコン・ミニコン」が 23.1%、「メインフレーム」が 37.5%、「専用・組込み・その他」が 4.3%となった。

・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。

8.ネットワークシステムの運用について n=416

	自社運用	ハードベンダに委託	ソフト・SIベンダに委託	情報子会社・関連会社に委託	その他	N/A	合計
回答数	294	17	46	67	10	3	437
占有率	70.7%	4.1%	11.1%	16.1%	2.4%	0.7%	105.0%



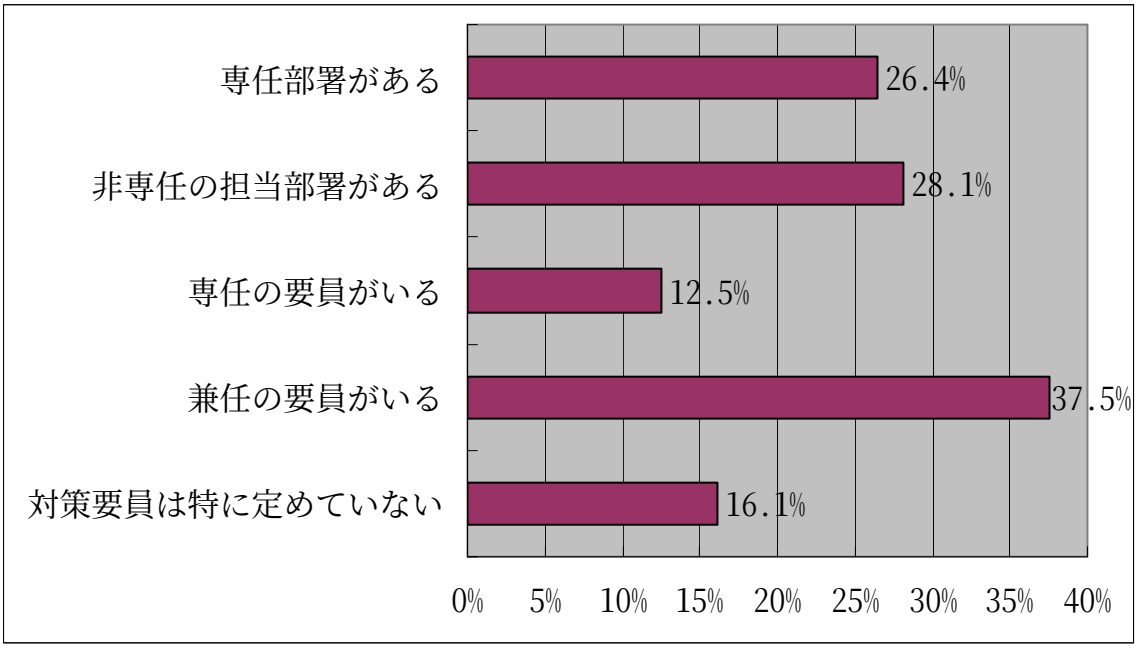
Note

・ネットワークシステムの運用状況については、「自社運用」が 70.7%、「ハードベンダに委託」が 4.1%、「ソフト・SI ベンダに委託」が 11.1%、「情報子会社・関連会社に委託」が 16.1%、「その他」が 2.4%となった。

・この設問は単一解答を求めたが、一部で複数回答をいただいた。複数回答は全て 1 回答として集計したため、回答総数は n=416 を上回った。占有率は複数回答の設問と同じく、回投票総数の n=416 を 100 とするパーセンテージで表示している。

9.情報セキュリティ対策体制について（複数回答可）n=416

	専任部署がある	非専任の担当部署がある	専任の要員がいる	兼任の要員がいる	対策要員は特に定めていない	合計
回答数	110	117	52	156	67	502
占有率	26.4%	28.1%	12.5%	37.5%	16.1%	120.7%



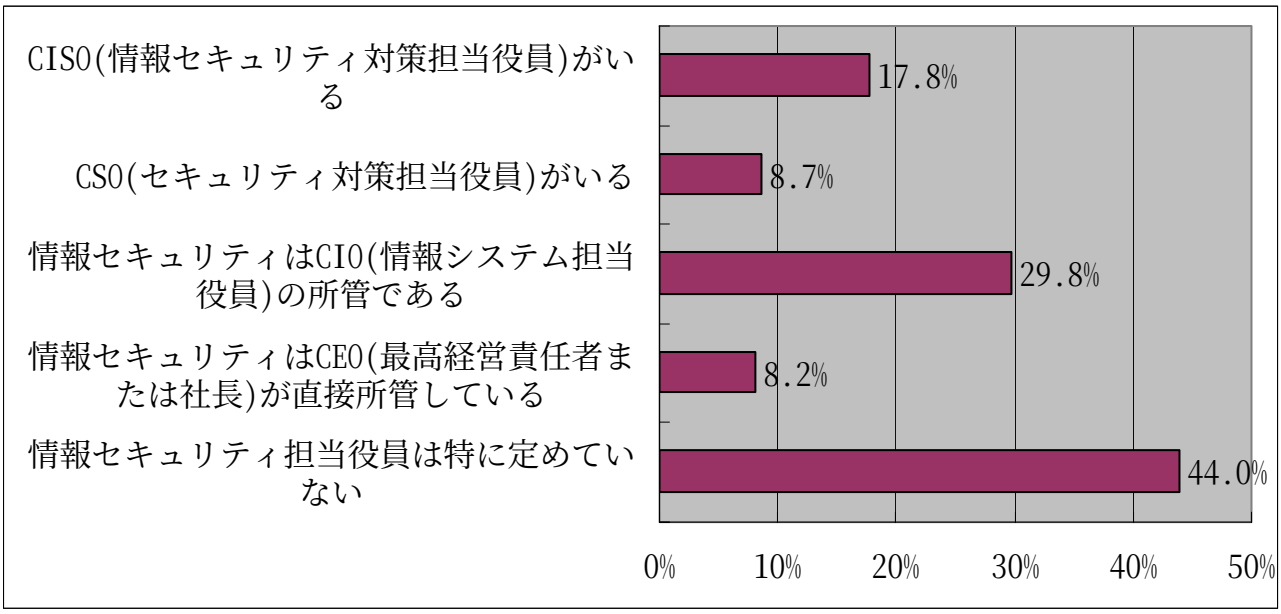
Note

・情報セキュリティ対策体制については「専任部署がある」が 26.4%、「非専任の担当部署がある」が 28.1%、「専任の要員がいる」が 12.5%、「兼任の要員がいる」が 37.5%、「対策要員は特に定めていない」が 16.1%となった。

・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。なお、「専任の要員がいる」のうち「専任部署がある」にも○をしたものが 28 件 6.7%、「兼任の要員がいる」のうち「非専任の担当部署がある」にも○をしたものが 42 件 10.1%あった。その他いろいろな組合せの複数回答をいただいており、専任と非専任の部署や要員を組合せで体制を構築しているところも多いことが確認できている。

10. 情報セキュリティ担当役員について（複数回答可） n=416

	CISO(情報セキュリティ対策担当役員)がいる	CSO(セキュリティ対策担当役員)がいる	情報セキュリティはCIO(情報システム担当役員)の所管である	情報セキュリティはCEO(最高経営責任者または社長)が直接所管している	情報セキュリティ担当役員は特に定めていない	合計
回答数	74	36	124	34	183	451
占有率	17.8%	8.7%	29.8%	8.2%	44.0%	108.4%



Note

・情報セキュリティ担当役員については、「CISO(情報セキュリティ対策担当役員)がいる」が 17.8%、「CSO(セキュリティ対策担当役員)がいる」が 8.7%、「情報セキュリティは CIO(情報システム担当役員)の所管である」が 29.8%、「情報セキュリティは CEO(最高経営責任者または社長)が直接所管している」は 8.2%、「情報セキュリティ担当役員は特に定めていない」は 44.0%であった。

・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。

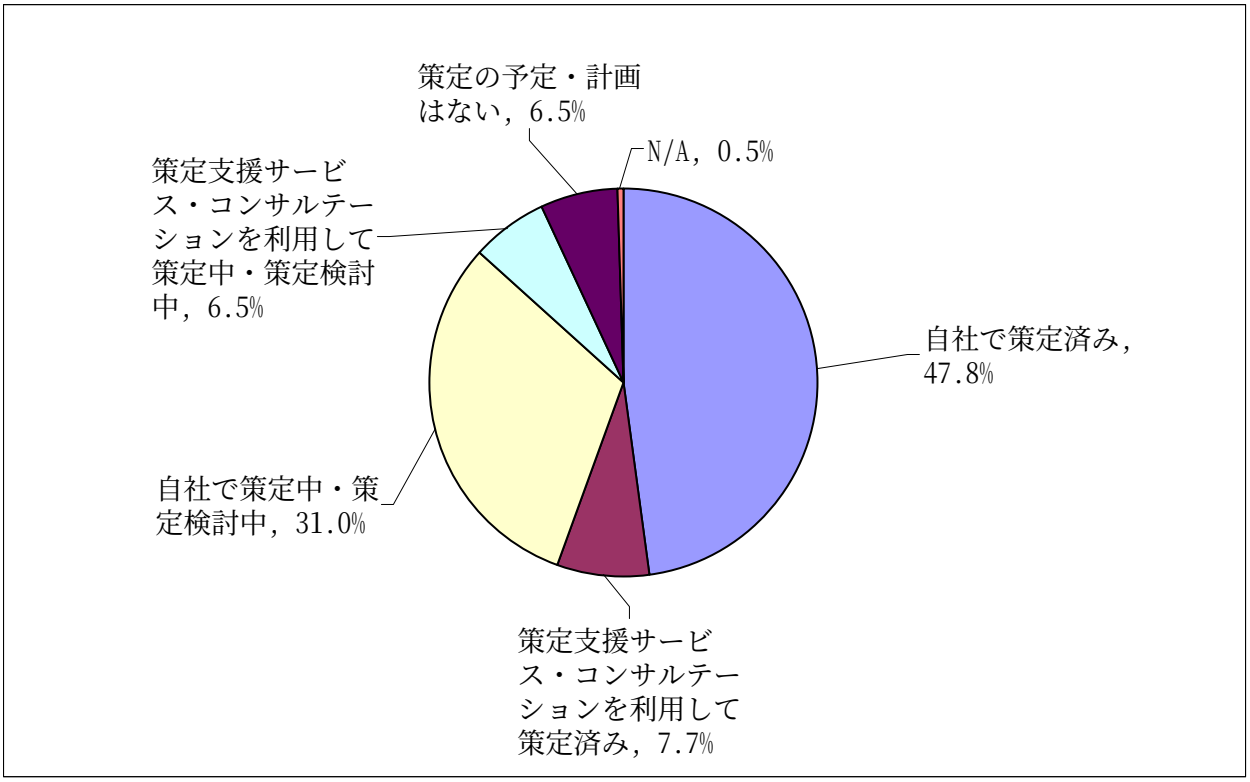
・なお、CISO がいる、としたうち、「情報セキュリティは CIO の所管である」あるいは「情報セキュリティは CEO が直接所管している」のどちらかまたは両方にも回答をいただいた調査票の件数は 20 件 4.8%であった。また、同様に CSO がいる、との回答のうち、「情報セキュリティは CIO の所管である」あるいは「情報セキュリティは CEO が直接所管している」のどちらかまたは両方にも回答をいただいた調査票の件数は 12 件 2.9%であった。

第二部　セキュリティ管理対策の実施状況と満足度

A.　情報セキュリティポリシーの策定

A-1. 情報セキュリティポリシーの策定状況について、当てはまるものはどれですか

	自社で策定済み	策定支援サービス・コンサルテーションを利用して策定済み	自社で策定中・策定検討中	策定支援サービス・コンサルテーションを利用して策定中・策定検討中	策定の予定・計画はない	N/A	合計
回答数	199	32	129	27	27	2	416
占有率	47.8%	7.7%	31.0%	6.5%	6.5%	0.5%	100.0%

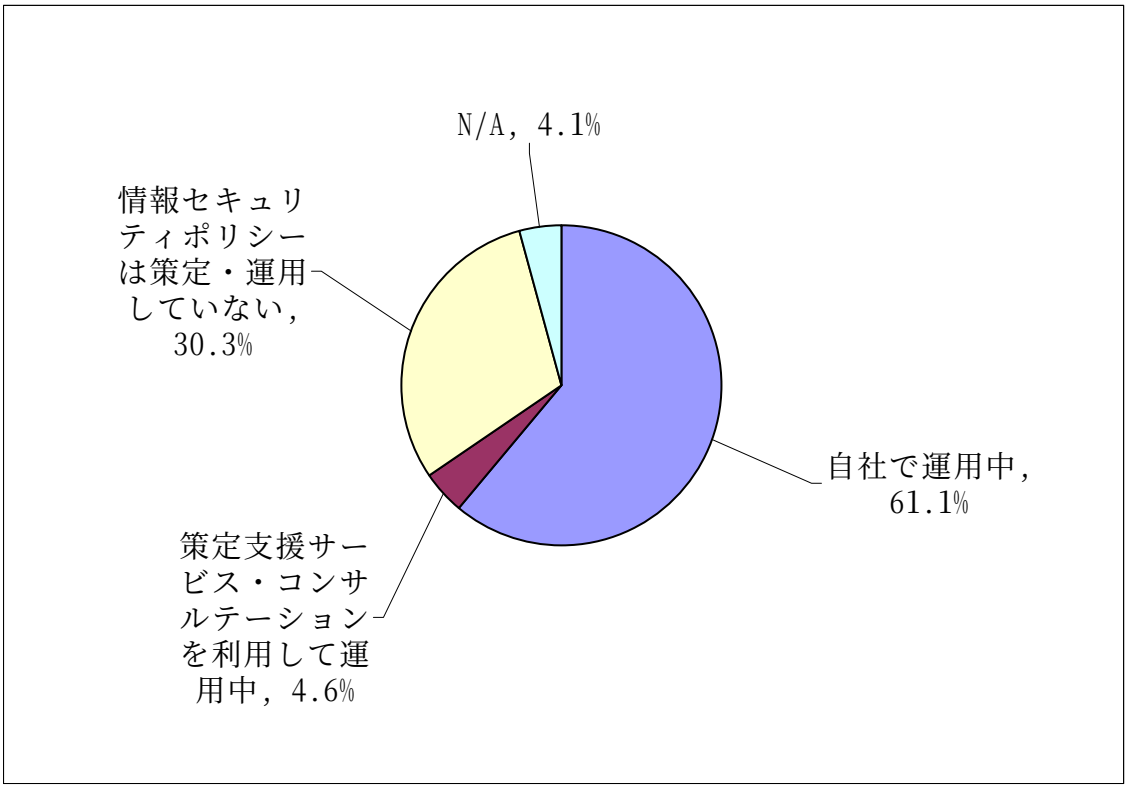


Note

・情報セキュリティポリシーの策定状況について見てみると、「自社で策定済み」が 47.8%、「策定支援サービス・コンサルテーションを利用して策定済み」が 7.7%、「自社で策定中・策定検討中」が 31.0%、「策定支援サービス・コンサルテーションを利用して策定中・策定検討中」が 6.5%、「策定の予定・計画はない」が 6.5%であった。

A-2. 情報セキュリティポリシーの運用状況について、当てはまるものはどれですか

	自社で運用中	策定支援サービス・コンサルテーションを利用して運用中	情報セキュリティポリシーは策定・運用していない	N/A	合計
回答数	254	19	126	17	416
占有率	61.1%	4.6%	30.3%	4.1%	100.0%

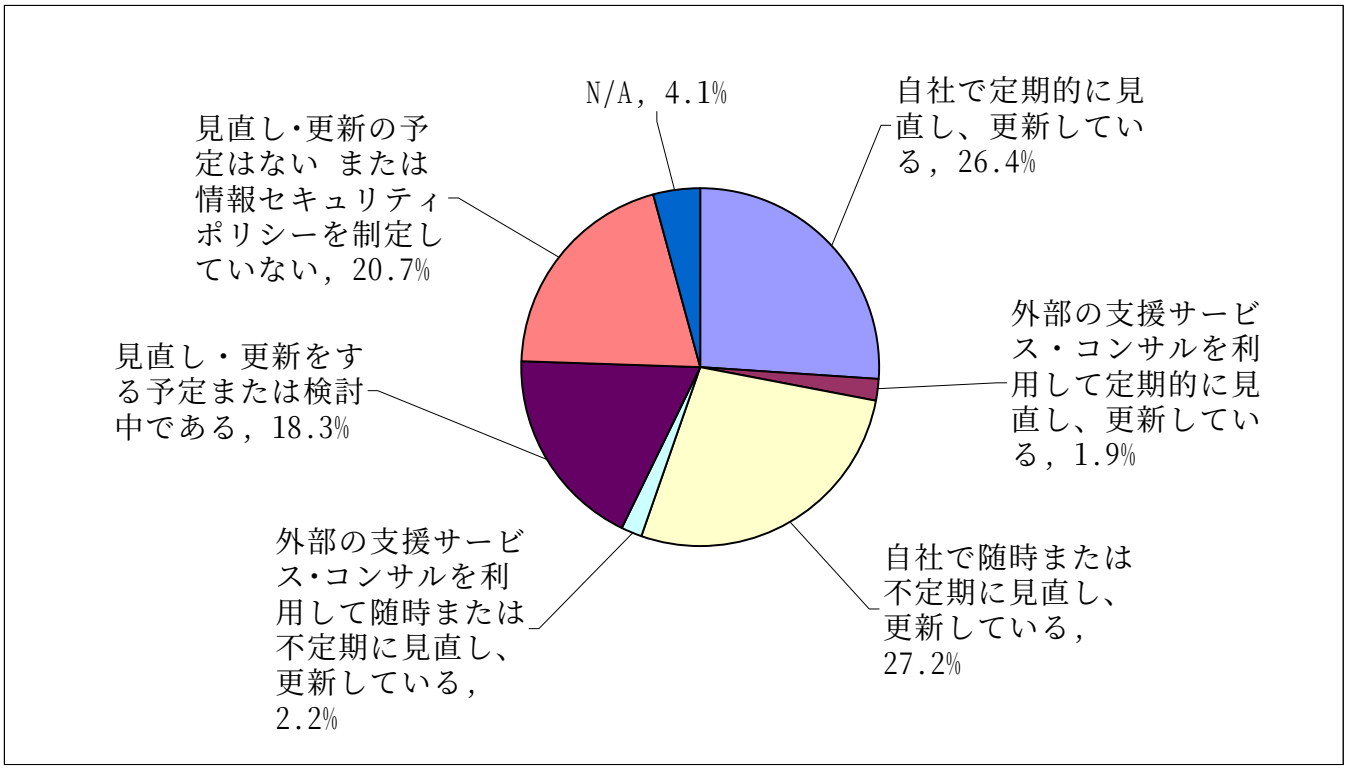


Note

・情報セキュリティポリシーの運用状況については、「自社で運用中」が 61.1%、「策定支援サービス・コンサルテーションを利用して運用中」が 4.6%、「情報セキュリティポリシーは策定・運用していない」が 30.3%となった。

A-3. 情報セキュリティポリシーの見直しについて、当てはまるものはどれですか

	自社で定期的に見直し、更新している	外部の支援サービス・コンサルを利用して定期的に見直し、更新している	自社で随時または不定期に見直し、更新している	外部の支援サービス･コンサルを利用して随時または不定期に見直し、更新している	見直し・更新をする予定または検討中である	見直し･更新の予定はない または 情報セキュリティポリシーを制定していない	N/A	合計
回答数	110	8	113	9	76	86	17	419
占有率	26.4%	1.9%	27.2%	2.2%	18.3%	20.7%	4.1%	100.8%

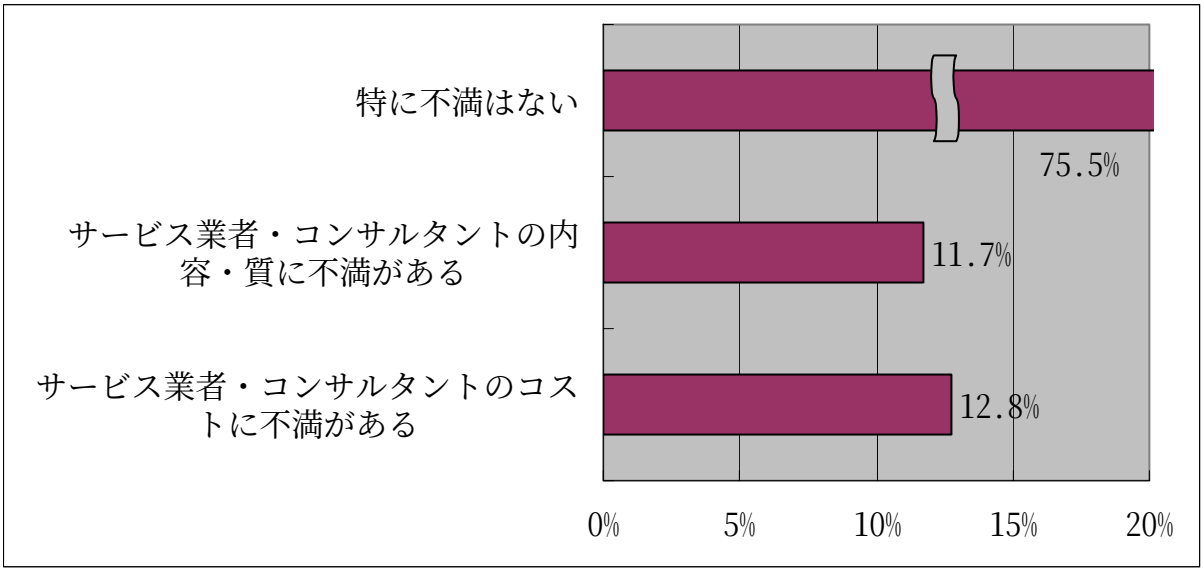


Note

・情報セキュリティポリシーの見直しについては、「自社で定期的に見直し、更新している」が 26.4%、「外部の支援サービス・コンサルを利用して定期的に見直し、更新している」が 1.9%、「自社で随時または不定期に見直し、更新している」が 27.2%、「外部の支援サービス･コンサルを利用して随時または不定期に見直し、更新している」が 2.2%、「見直し・更新をする予定または検討中である」が 18.3%、「見直し･更新の予定はない または 情報セキュリティポリシーを制定していない」が 20.7%であった。

A-4. 情報セキュリティポリシー策定支援サービス・コンサルテーションを利用している場合、利用上の不満・問題点について、次のうち当てはまるのはどれですか（複数回答可）

	特に不満はない	サービス業者・コンサルタントの内容・質に不満がある	サービス業者・コンサルタントのコストに不満がある	合計
回答数	71	11	12	94
占有率	75.5%	11.7%	12.8%	100.0%



Note

・情報セキュリティポリシー策定支援サービス・コンサルテーションを利用している場合の不満・問題点については、「特に不満はない」が 75.5%を占め、以下、「サービス業者・コンサルタントの内容・質に不満がある」が 11.7%、「サービス業者・コンサルタントのコストに不満がある」が 12.8%となった。

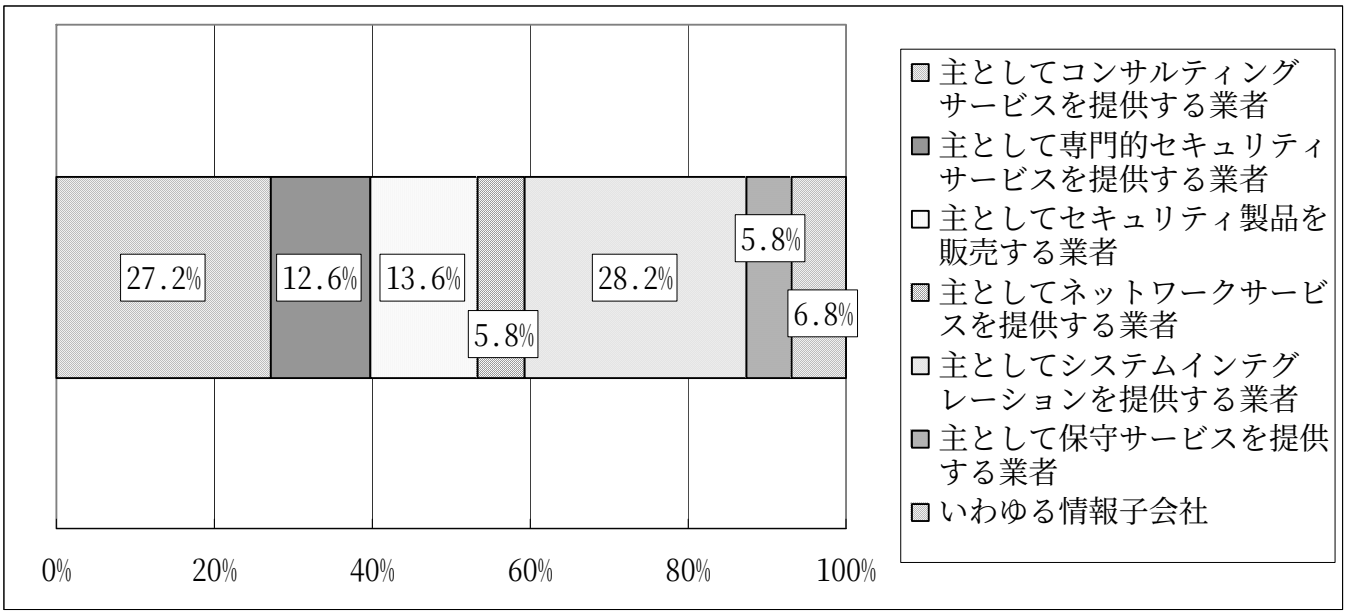
・この質問は該当企業だけに回答いただくものなので、無回答のものを除き、有効回答総数を 100%として占有率を算出した。

○不満がある場合の自由記述内容（記入されたとおりに収録。順不同）

・内容が一般的で当社に合ったものと思えない。
・社内の多様な要求／意見をまとめあげる能力（コンサル）不足。
・コンサルが教科書的で、当社業務に適したポリシーを描けない。描こうとしない。
・内容がきちっと整理できていない。文章表現が適格でない。
・内容が一般的なものになりがちで、各社の個別事情に沿ったコンサルティングがなかなかできない。
・不満というか弊社の仕様や予算にうまく合致する製品を探すことに労力がかかる。
・内容がステレオタイプ
・コンサルテーション内容は一般的であるにも関わらず、費用が高過ぎる。
・コストをかけていない事もあり、アドバイス程度となっている。

A-5. 外部のサービス業者、コンサルタントを利用している場合、それは次のどれに該当しますか
（複数回答可）

	主としてコンサルティングサービスを提供する業者	主として専門的セキュリティサービスを提供する業者	主としてセキュリティ製品を販売する業者	主としてネットワークサービスを提供する業者	主としてシステムインテグレーションを提供する業者	主として保守サービスを提供する業者	いわゆる情報子会社	合計
回答数	28	13	14	6	29	6	7	103
占有率	27.2%	12.6%	13.6%	5.8%	28.2%	5.8%	6.8%	100.0%



Note

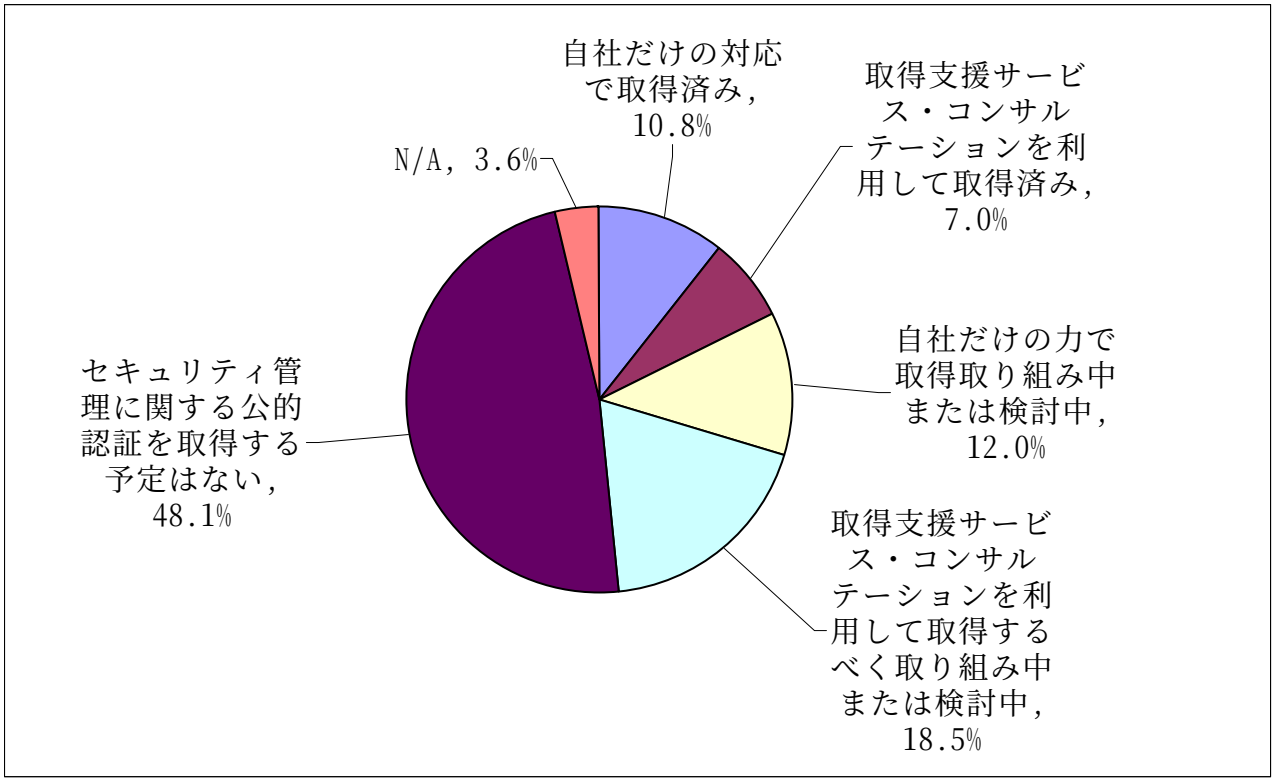
・外部のサービス業者、コンサルタントを利用している場合、該当するのは、「主としてコンサルティングサービスを提供する業者」が 27.2%を占め、以下、「主として専門的セキュリティサービスを提供する業者」が 12.6%、「主としてセキュリティ製品を販売する業者」が 13.6%、「主としてネットワークサービスを提供する業者」が 5.8%、「主としてシステムインテグレーションを提供する業者」が 28.2%、「主として保守サービスを提供する業者」が 5.8%、「いわゆる情報子会社」が 6.8%となった。

・この質問は該当企業だけに回答いただくものなので、無回答のものを除き、有効回答数を 100%として占有率を算出した。

B.セキュリティ管理に関する公的認証（BS7799,ISO17799,ISMS,セキュリティ監査制度）の取得

B-1. セキュリティ管理に関する公的認証の取得状況について、当てはまるものはどれですか

	自社だけの対応で取得済み	取得支援サービス・コンサルテーションを利用して取得済み	自社だけの力で取得取り組み中または検討中	取得支援サービス・コンサルテーションを利用して取得するべく取り組み中または検討中	セキュリティ管理に関する公的認証を取得する予定はない	N/A	合計
回答数	45	29	50	77	200	15	416
占有率	10.8%	7.0%	12.0%	18.5%	48.1%	3.6%	100.0%

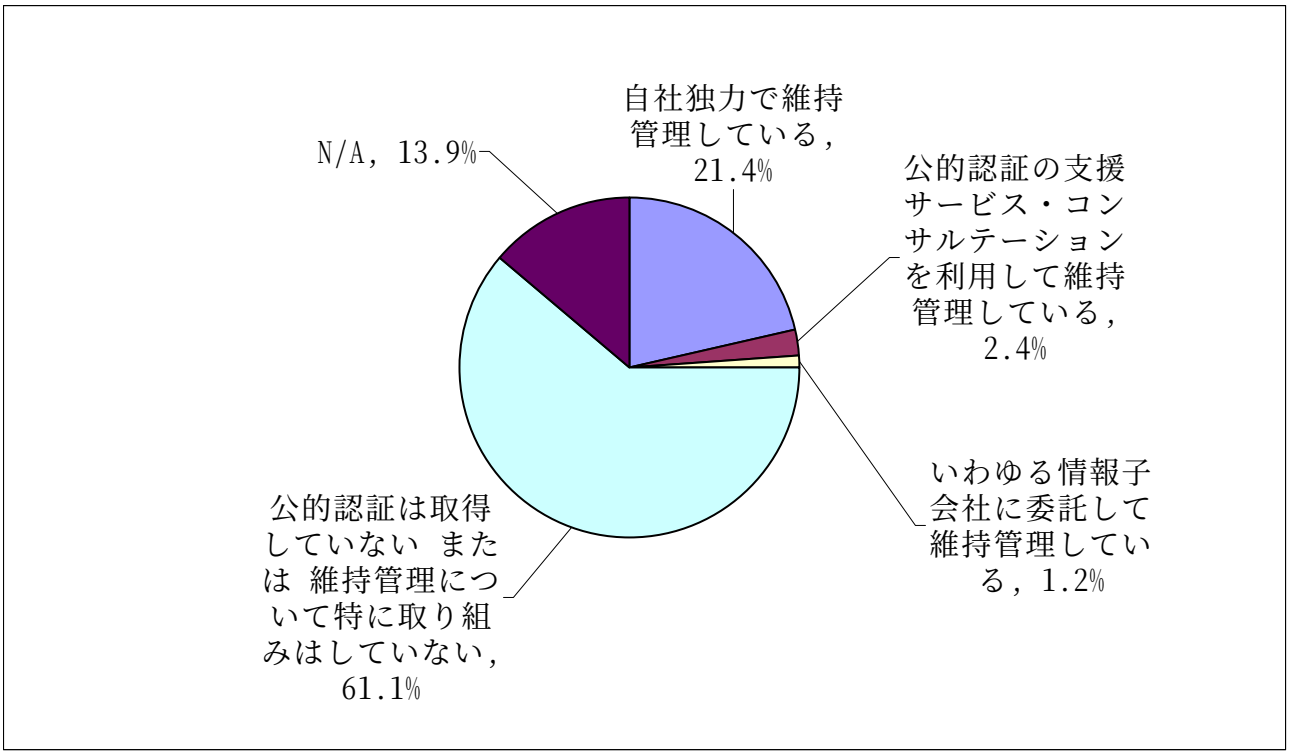


Note

・セキュリティ管理に関する公的認証の取得状況については、「自社だけの対応で取得済み」が 10.8%、「取得支援サービス・コンサルテーションを利用して取得済み」が 7.0%、「自社だけの力で取得取り組み中または検討中」が 12.0%、「取得支援サービス・コンサルテーションを利用して取得するべく取り組み中または検討中」が 18.5%、「セキュリティ管理に関する公的認証を取得する予定はない」が 48.1%となった。

B-2. セキュリティ管理に関する公的認証の維持管理状況について、当てはまるものはどれですか

	自社独力で維持管理している	公的認証の支援サービス・コンサルテーションを利用して維持管理している	いわゆる情報子会社に委託して維持管理している	公的認証は取得していない または 維持管理について特に取り組みはしていない	N/A	合計
回答数	89	10	5	254	58	416
占有率	21.4%	2.4%	1.2%	61.1%	13.9%	100.0%

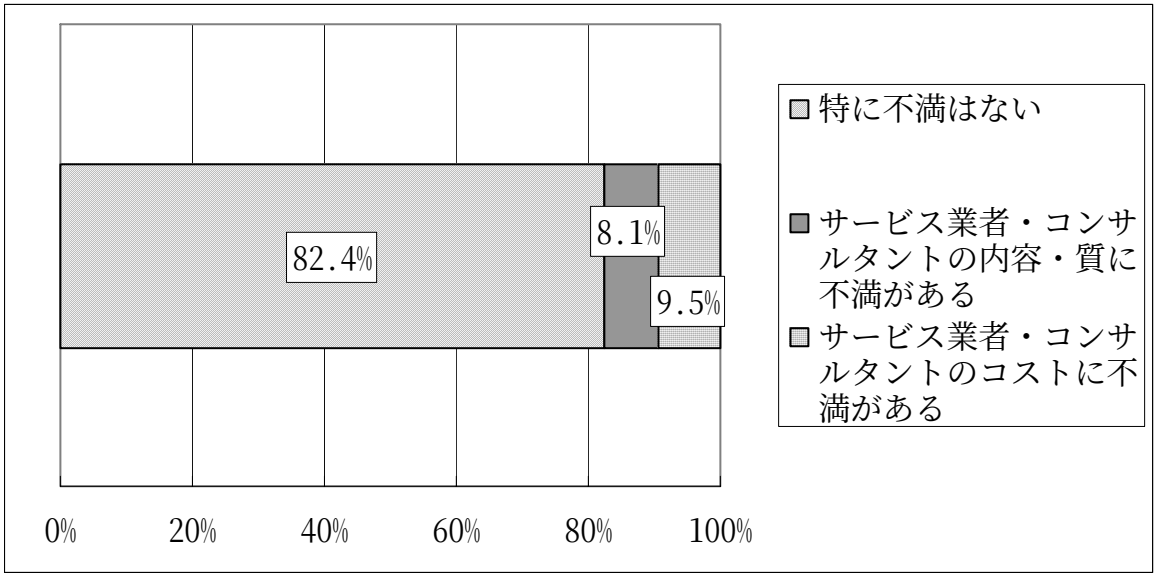


Note

・セキュリティ管理に関する公的認証の維持管理状況については、「自社独力で維持管理している」が 21.4%、「公的認証の支援サービス・コンサルテーションを利用して維持管理している」が 2.4%、「いわゆる情報子会社に委託して維持管理している」が 1.2%、「公的認証は取得していない　または維持管理については特に取り組みはしていない」が 61.1%となった。

B-3．セキュリティ管理に関する公的認証の取得支援サービス・コンサルテーションを利用している場合、利用上の不満・問題点について、次のうち当てはまるものはどれですか（複数回答可）

	特に不満はない	サービス業者・コンサルタントの内容・質に不満がある	サービス業者・コンサルタントのコストに不満がある	合計
回答数	61	6	7	74
占有率	82.4%	8.1%	9.5%	100.0%



Note

・セキュリティ管理に関する公的認証の取得支援サービス・コンサルテーションを利用している場合の不満・問題点については、「特に不満はない」が 82.4%を占め、以下「サービス業者・コンサルタントの内容・質に不満がある」が 8.1%、「サービス業者・コンサルタントのコストに不満がある」が 9.5%となった。

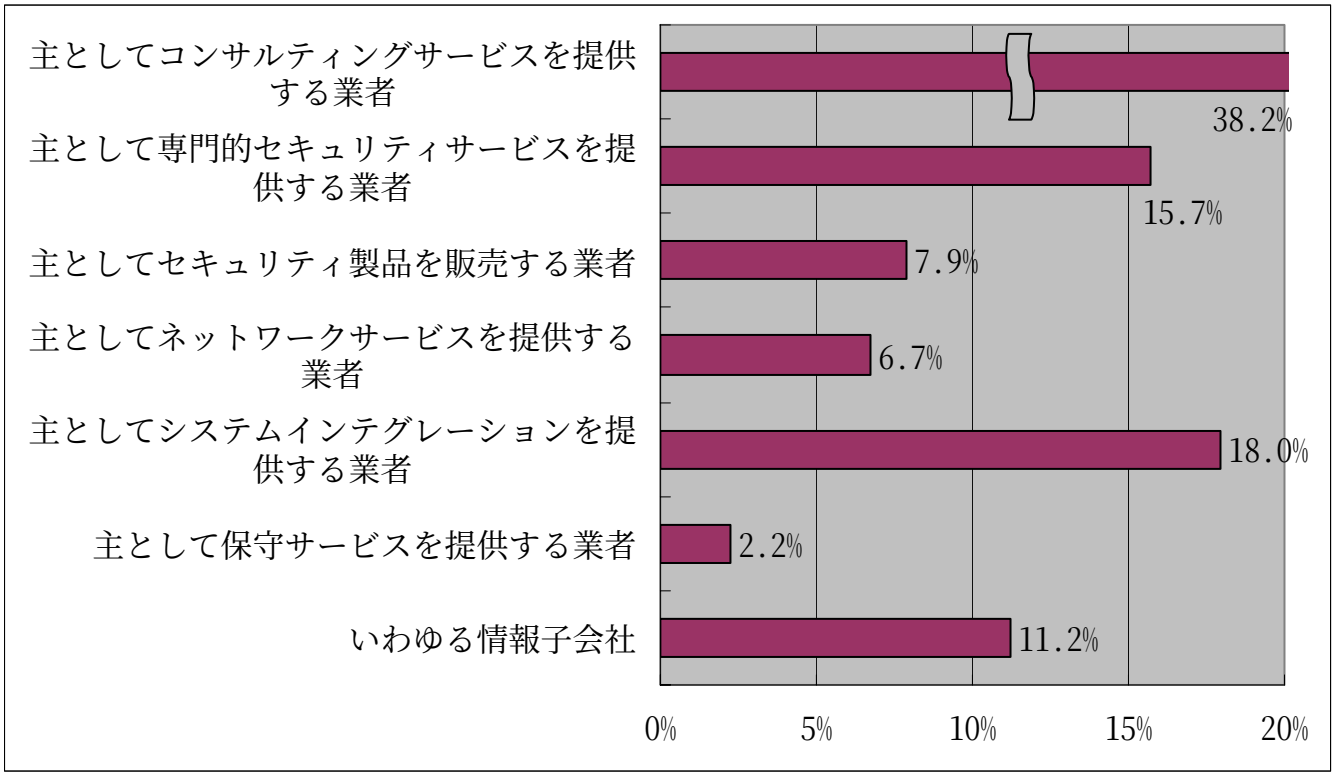
・この質問は該当企業だけに回答いただくものなので、無回答のものを除き、有効回答数を 100%として占有率を算出した。

○不満がある場合の自由記述内容（記入されたとおりに収録。順不同）

・各各提案を見てもコンサル価値が不透明
・利用していない
・取得タスクフォースチームではないので回答不能
・認証の証書をとるためだけのコンサルで、実態としてセキュリティリスク対策としてどうＩＳＭＳを活用すべき等･･･。本質的な部分での問題提起、改善提案にならない。
・対応が遅い
・サービス内容に対するコストの割高感。
・具体的な事例が少ない。

B-4. 外部のサービス業者、コンサルタントを利用している場合、それは次のどれに該当しますか
（複数回答可）

	主としてコンサルティングサービスを提供する業者	主として専門的セキュリティサービスを提供する業者	主としてセキュリティ製品を販売する業者	主としてネットワークサービスを提供する業者	主としてシステムインテグレーションを提供する業者	主として保守サービスを提供する業者	いわゆる情報子会社	合計
回答数	34	14	7	6	16	2	10	89
占有率	38.2%	15.7%	7.9%	6.7%	18.0%	2.2%	11.2%	100.0%



Note

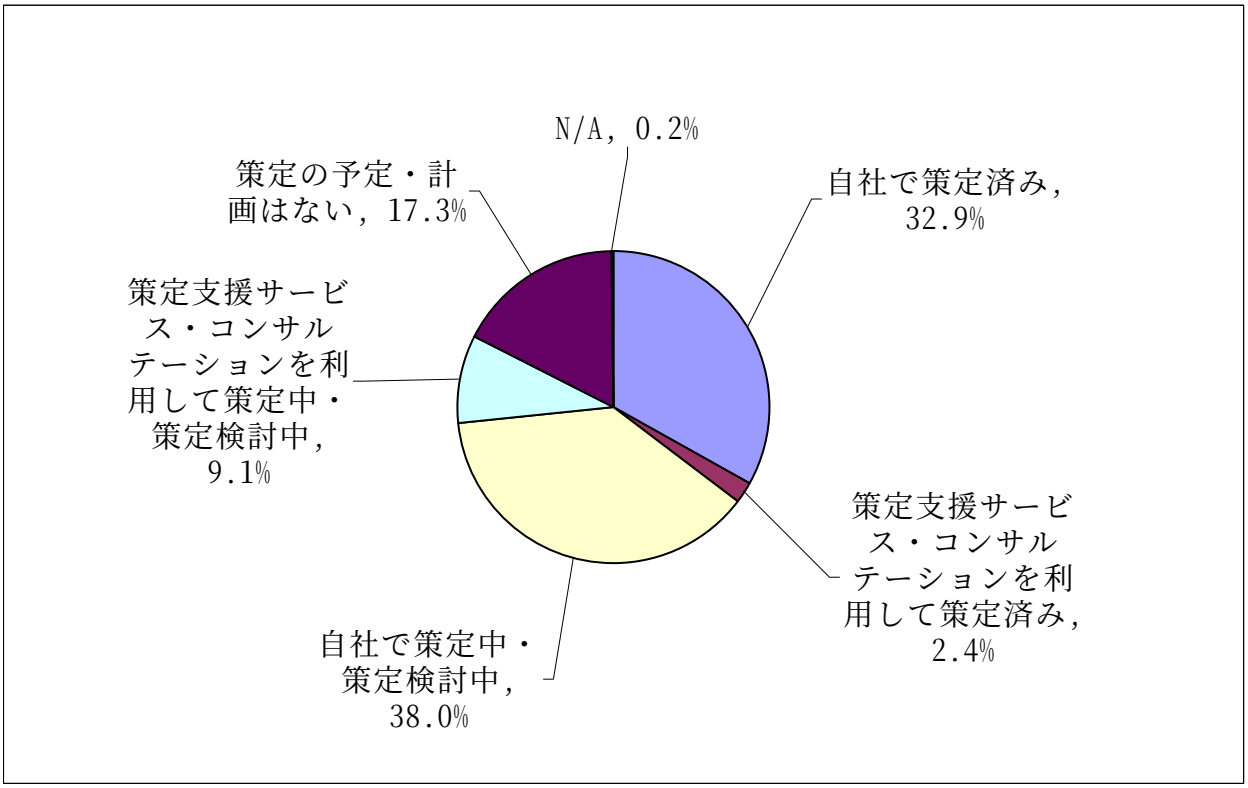
・外部のサービス業者、コンサルタントを利用している場合、その提供主体は、「主としてコンサルティングサービスを提供する業者」が 38.2%を占め、「主として専門的セキュリティサービスを提供する業者」が 15.7%、「主としてセキュリティ製品を販売する業者」が 7.9%、「主としてネットワークサービスを提供する業者」が 6.7%、「主としてシステムインテグレーションを提供する業者」が 18.0%、「主として保守サービスを提供する業者」が 2.2%、「いわゆる情報子会社」が 11.2%となった。

・この質問は該当企業だけに回答いただくものなので、無回答のものを除き、有効回答数を 100%として占有率を算出した。

C. プライバシーポリシー、個人情報保護管理基準等の策定

C-1. プライバシーポリシー、個人情報保護管理基準等（以下、プライバシーポリシーと総称）の策定状況について、当てはまるものはどれですか

	自社で策定済み	策定支援サービス・コンサルテーションを利用して策定済み	自社で策定中・策定検討中	策定支援サービス・コンサルテーションを利用して策定中・策定検討中	策定の予定・計画はない	N/A	合計
回答数	137	10	158	38	72	1	416
占有率	32.9%	2.4%	38.0%	9.1%	17.3%	0.2%	100.0%

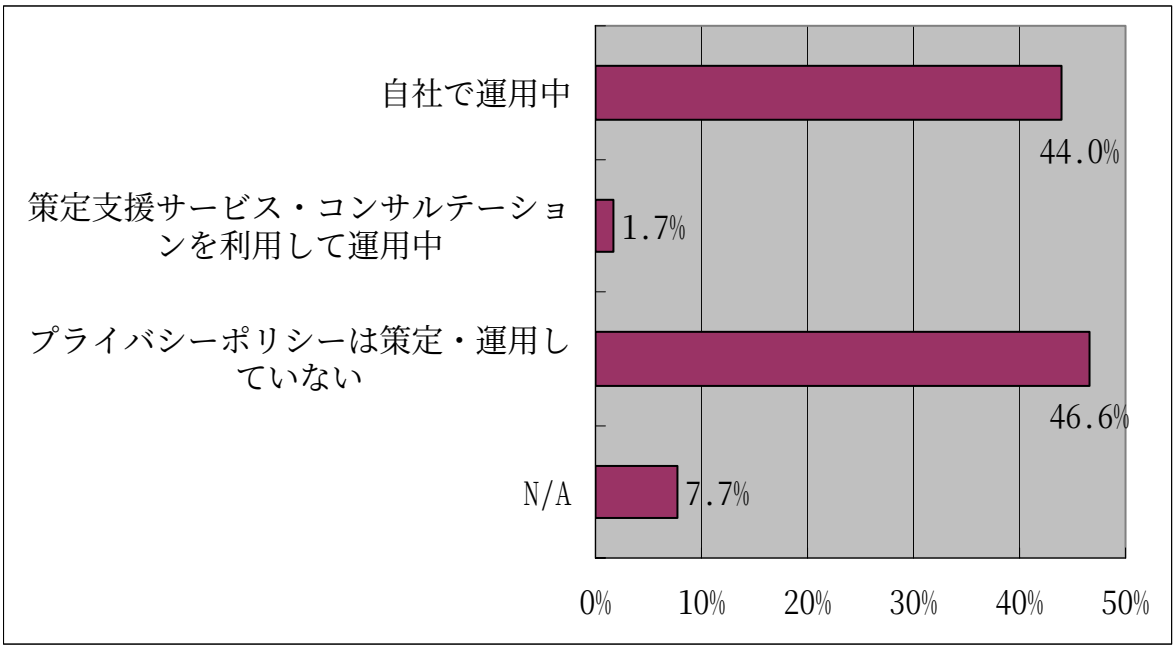


Note

・プライバシーポリシー、個人情報保護管理基準等の策定状況については、「自社で策定済み」が 32.9%、「策定支援サービス・コンサルテーションを利用して策定済み」が 2.4%、「自社で策定中・策定検討中」が 38.0%、「策定支援サービス・コンサルテーションを利用して策定中・策定検討中」が 9.1%、「策定の予定・計画はない」が 17.3%となった。

C-2. プライバシーポリシーの運用状況について、当てはまるものはどれですか

	自社で運用中	策定支援サービス・コンサルテーションを利用して運用中	プライバシーポリシーは策定・運用していない	N/A	合計
回答数	183	7	194	32	416
占有率	44.0%	1.7%	46.6%	7.7%	100.0%

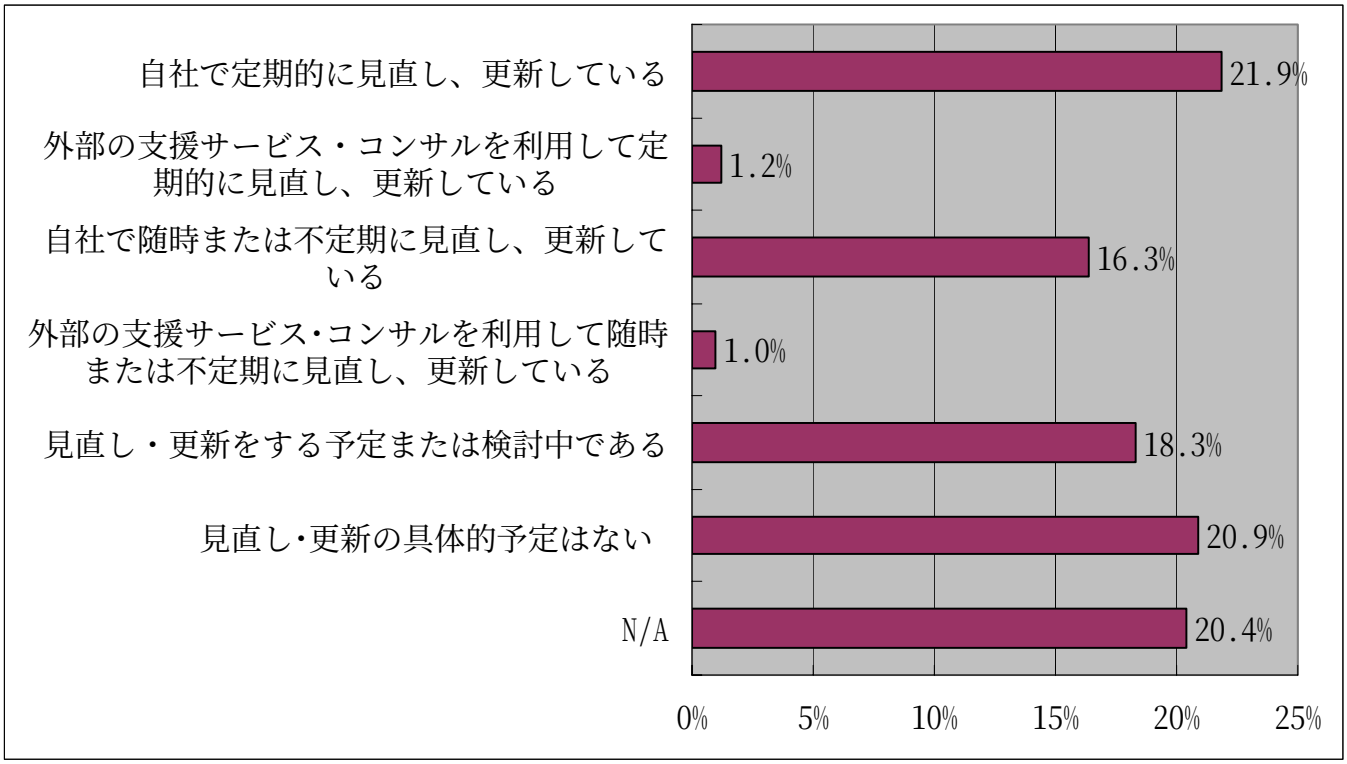


Note

・プライバシーポリシーの運用状況については、「自社で運用中」が 44.0%、「策定支援サービス・コンサルテーションを利用して運用中」が 1.7%、「プライバシーポリシーは策定・運用していない」は 46.6%となった。

C-3. プライバシーポリシーの見直しについて、当てはまるものはどれですか

	自社で定期的に見直し、更新している	外部の支援サービス・コンサルを利用して定期的に見直し、更新している	自社で随時または不定期に見直し、更新している	外部の支援サービス･コンサルを利用して随時または不定期に見直し、更新している	見直し・更新をする予定または検討中である	見直し･更新の具体的予定はない	N/A	合計
回答数	91	5	68	4	76	87	85	416
占有率	21.9%	1.2%	16.3%	1.0%	18.3%	20.9%	20.4%	100.0%

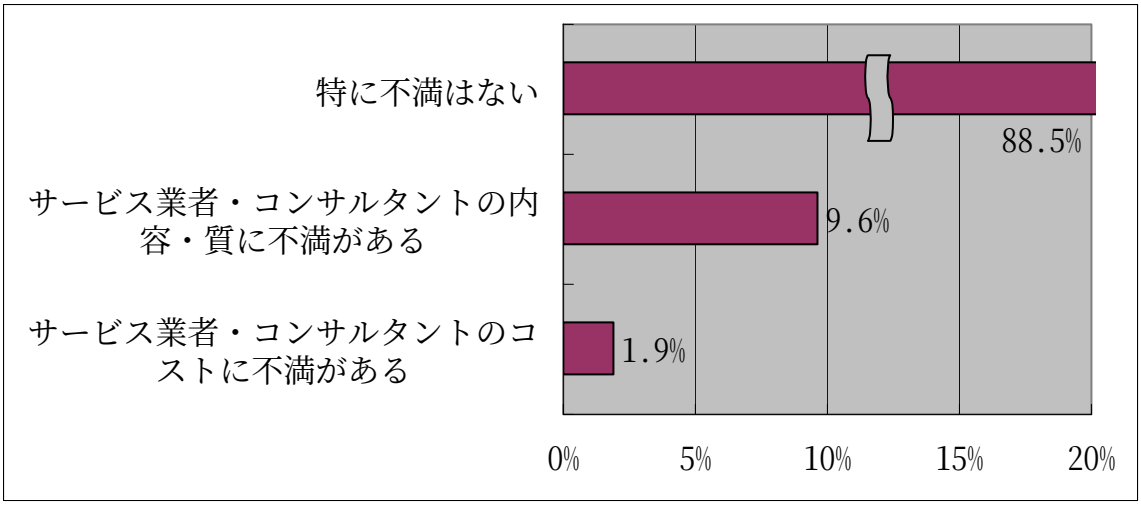


Note

・プライバシーポリシーの見直しについては、「自社で定期的に見直し、更新している」が 21.9%、「外部の支援サービス・コンサルを利用して定期的に見直し、更新している」が 1.2%、「自社で随時または不定期に見直し、更新している」が 16.3%、「外部の支援サービス･コンサルを利用して随時または不定期に見直し、更新している」が 1.0%、「見直し・更新を資する予定または検討中である」が 18.3%、「見直し･更新の具体的予定はない」が 20.9%となった。

C-4. プライバシーポリシー策定支援サービス・コンサルテーションを利用している場合、利用上の不満・問題点について、次のうち当てはまるものはどれですか（複数回答可）

	特に不満はない	サービス業者・コンサルタントの内容・質に不満がある	サービス業者・コンサルタントのコストに不満がある	合計
回答数	46	5	1	52
占有率	88.5%	9.6%	1.9%	100.0%



Note

・プライバシーポリシー策定支援サービス・コンサルテーションを利用している場合の不満・問題点については、「特に不満はない」が 88.5%を占め、以下「サービス業者・コンサルタントの内容・質に不満がある」が 9.6%、「サービス業者・コンサルタントのコストに不満がある」が 1.9%となった。

・この質問は該当企業だけに回答いただくものなので、無回答のものを除き、有効回答数を 100%として占有率を算出した。

○不満がある場合の自由記述内容（記入されたとおりに収録。順不同）

・利用していない

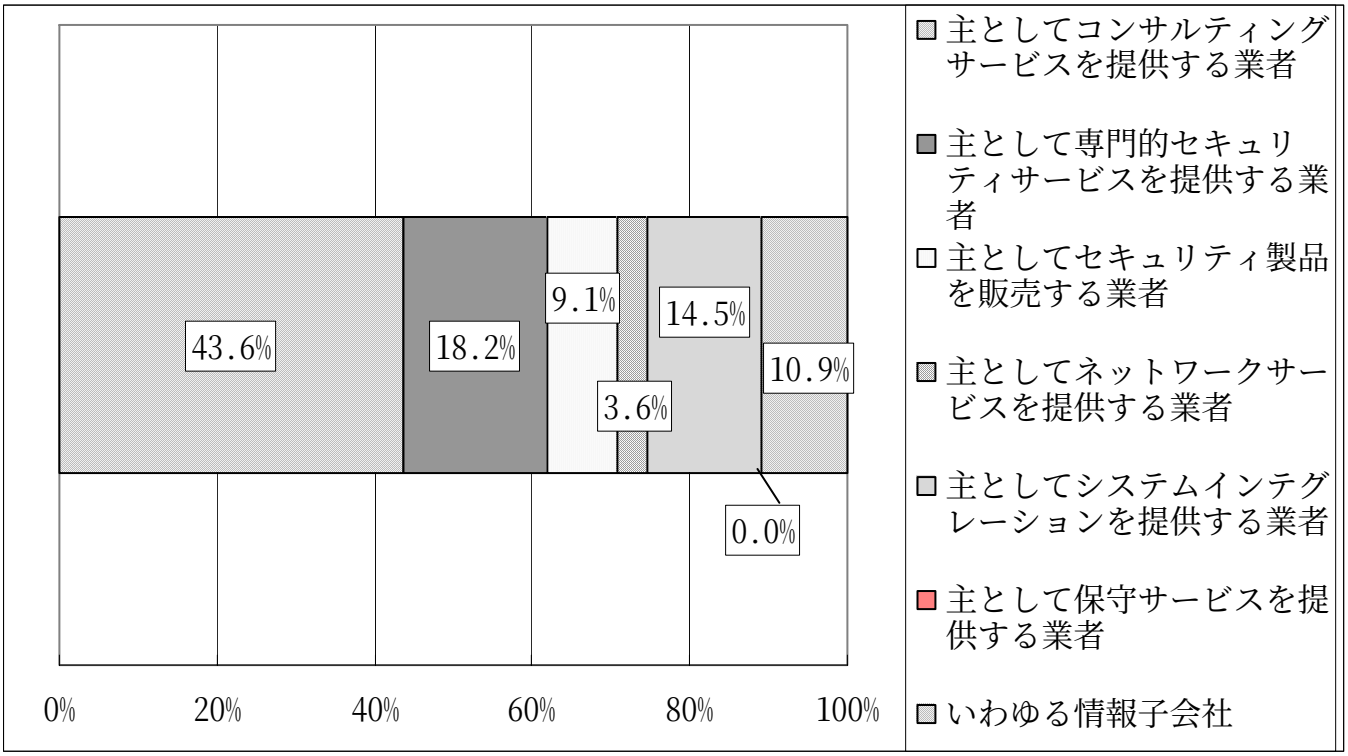
・当社業務に合っていない。あくまで教科書的。

・対応が遅い

・コストをかけていない事もあり、アドバイス程度となっている。

C-5. 外部のサービス業者、コンサルタントを利用している場合、それは次のどれに該当しますか
（複数回答可）

	主としてコンサルティングサービスを提供する業者	主として専門的セキュリティサービスを提供する業者	主としてセキュリティ製品を販売する業者	主としてネットワークサービスを提供する業者	主としてシステムインテグレーションを提供する業者	主として保守サービスを提供する業者	いわゆる情報子会社	合計
回答数	24	10	5	2	8	0	6	55
占有率	43.6%	18.2%	9.1%	3.6%	14.5%	0.0%	10.9%	100.0%



Note

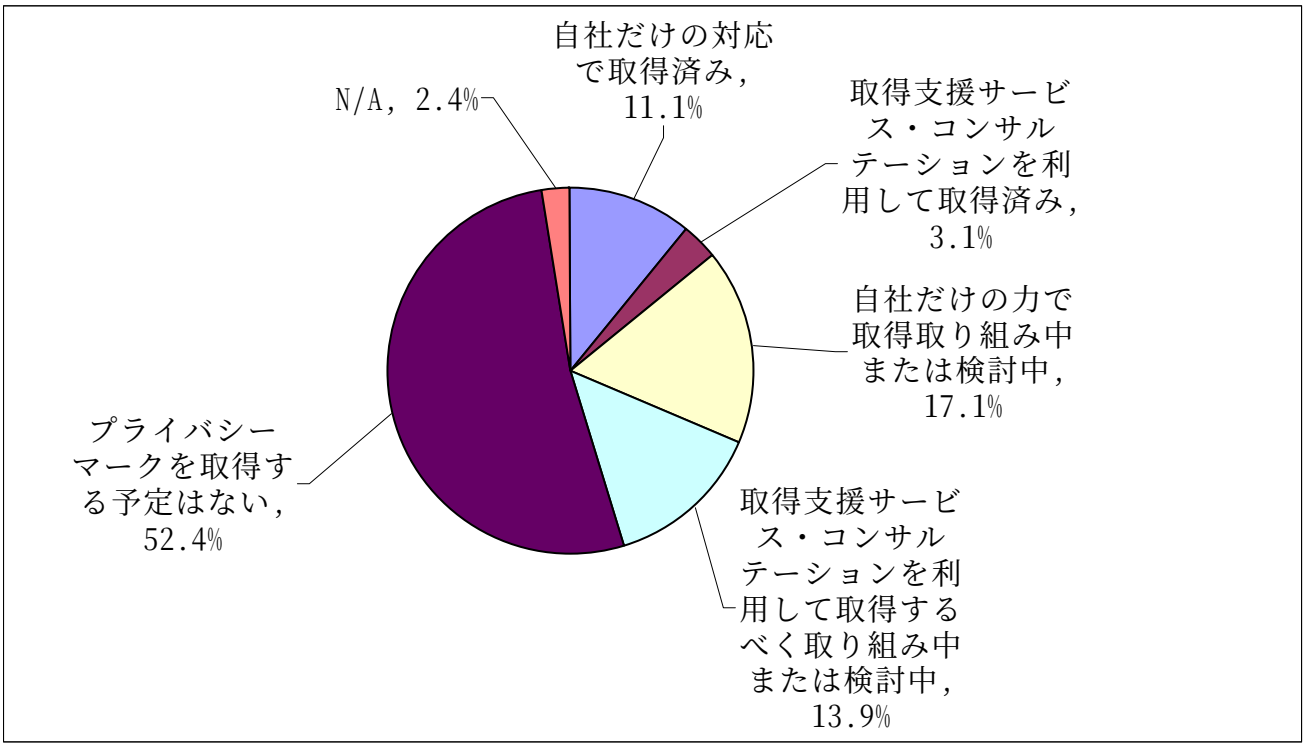
・外部のサービス業者、コンサルタントを利用している場合、その提供主体は、「主としてコンサルティングサービスを提供する業者」が 43.6%を占め、「主として専門的セキュリティサービスを提供する業者」が 18.2%、「主としてセキュリティ製品を販売する業者」が 9.1%、「主としてネットワークサービスを提供する業者」が 3.6%、「主としてシステムインテグレーションを提供する業者」が 14.5%、「主として保守サービスを提供する業者」が 0%、「いわゆる情報子会社」が 10.9%となった。

・この質問は該当企業だけに回答いただくものなので、無回答のものを除き、有効回答数を 100%として占有率を算出した。

D.プライバシーマークの取得

D-1. プライバシーマークの取得状況について、当てはまるものはどれですか

	自社だけの対応で取得済み	取得支援サービス・コンサルテーションを利用して取得済み	自社だけの力で取得取り組み中または検討中	取得支援サービス・コンサルテーションを利用して取得するべく取り組み中または検討中	プライバシーマークを取得する予定はない	N/A	合計
回答数	46	13	71	58	218	10	416
占有率	11.1%	3.1%	17.1%	13.9%	52.4%	2.4%	100.0%

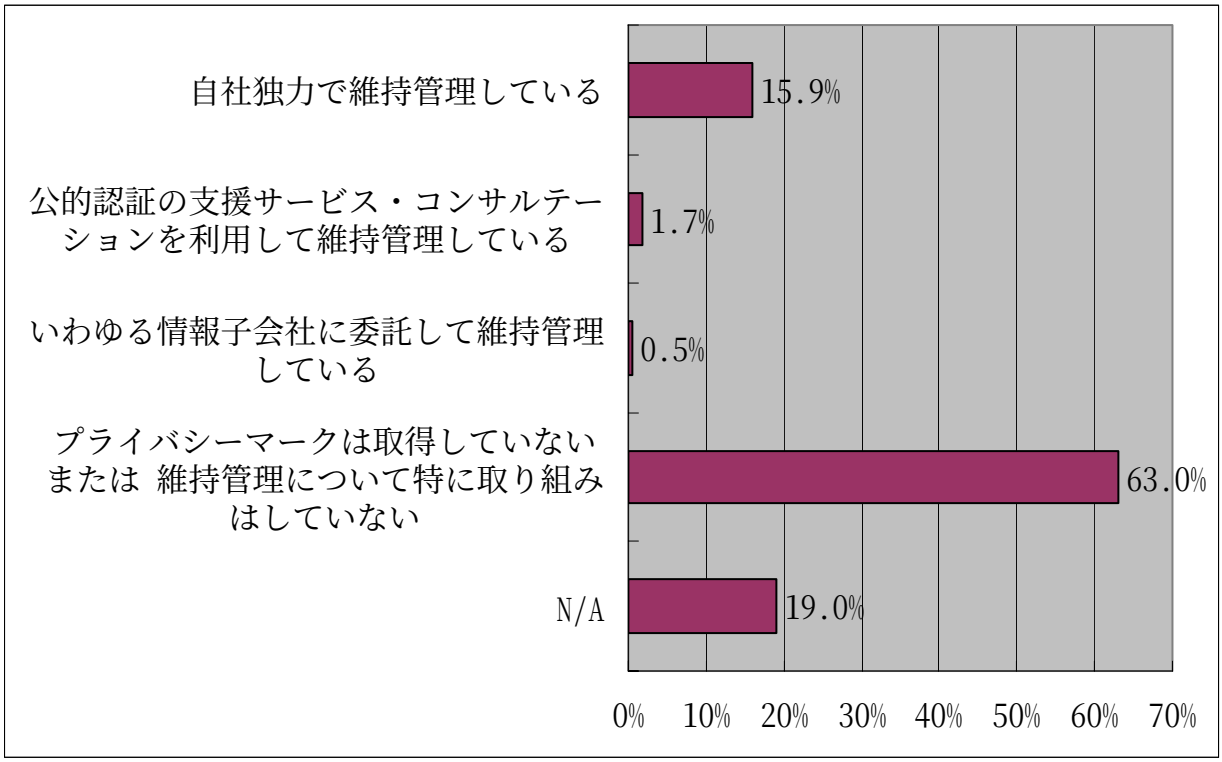


Note

・プライバシーマークの取得状況については、「自社だけの対応で取得済み」が 11.1%、「取得支援サービス・コンサルテーションを利用して取得済み」が 3.1%、「自社だけの力で取得取り組み中または検討中」が 17.1%、「取得支援サービス・コンサルテーションを利用して取得するべく取り組み中または検討中」が 13.9%、「プライバシーマークを取得する予定はない」が 52.4%となった。

D-2．プライバシーマークの維持管理状況について、当てはまるものはどれですか

	自社独力で維持管理している	公的認証の支援サービス・コンサルテーションを利用して維持管理している	いわゆる情報子会社に委託して維持管理している	プライバシーマークは取得していない または維持管理について特に取り組みはしていない	N/A	合計
回答数	66	7	2	262	79	416
占有率	15.9%	1.7%	0.5%	63.0%	19.0%	100.0%

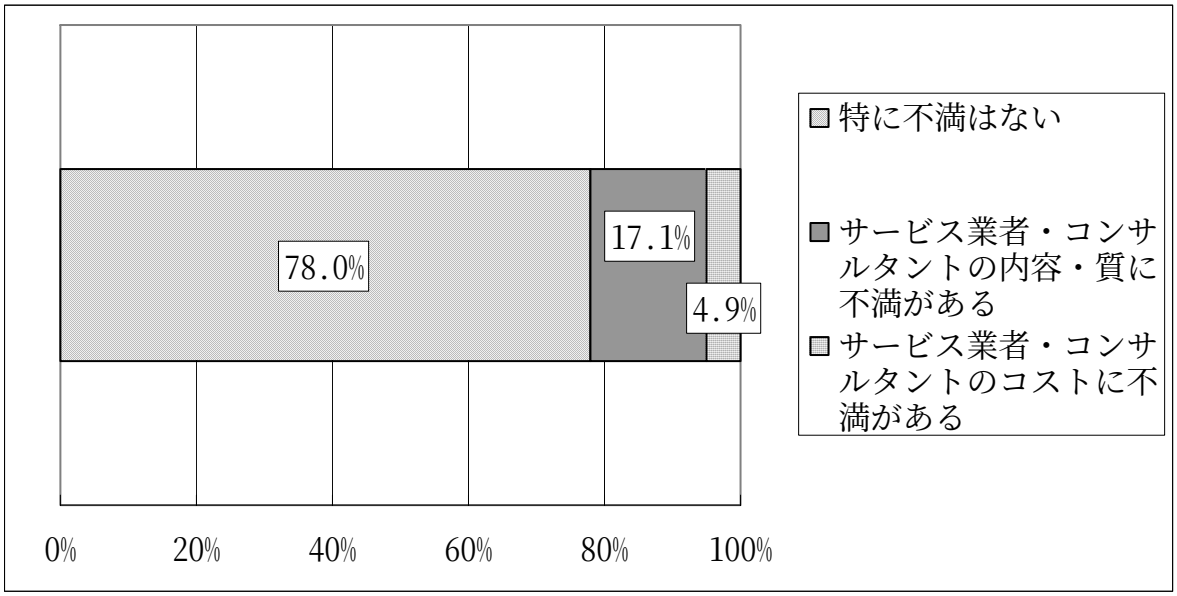


Note

・プライバシーマークの維持管理状況については、「自社独力で維持管理している」が 15.9%、「公的認証の支援サービス・コンサルテーションを利用して維持管理している」が 1.7%、「いわゆる情報子会社に委託して維持管理している」が 0.5%、「プライバシーマークは取得していない　または維持管理について特に取り組みはしていない」が 63.0%となった。

D-3．プライバシーマークの取得支援サービス・コンサルテーションを利用している場合、利用上の不満・問題点について、次のうち当てはまるものはどれですか（複数回答可）

	特に不満はない	サービス業者・コンサルタントの内容・質に不満がある	サービス業者・コンサルタントのコストに不満がある	合計
回答数	32	7	2	41
占有率	78.0%	17.1%	4.9%	100.0%



Note

・プライバシーマークの取得支援サービス・コンサルテーションを利用している場合の不満・問題点については、「特に不満はない」が 78.0%を占め、以下、「サービス業者・コンサルタントの内容・質に不満がある」が 17.1%、「サービス業者・コンサルタントのコストに不満がある」が 4.9%となった。

・この質問は該当企業だけに回答いただくものなので、無回答のものを除き、有効回答総数を 100%として占有率を算出した。

○不満がある場合の自由記述内容（記入されたとおりに収録。順不同）

・知識が浅い。

・教科書的。当社業務における解決提示に欠ける。

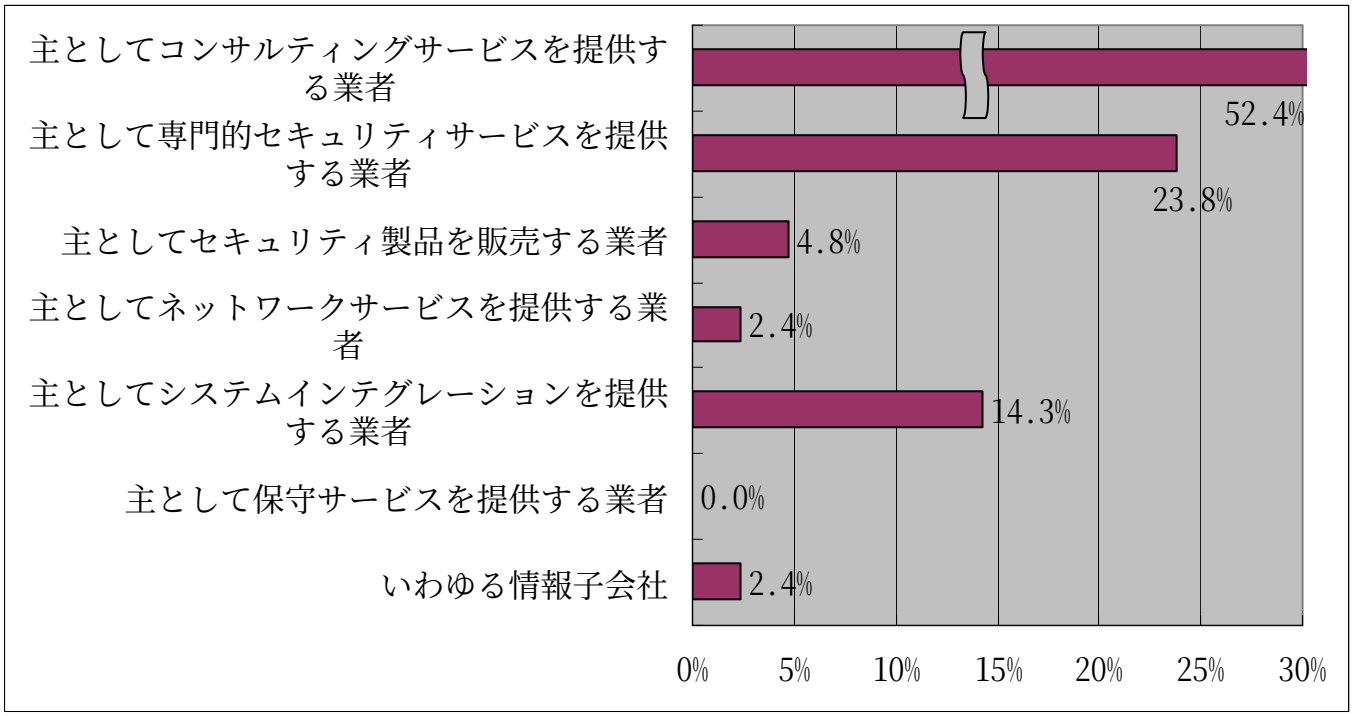
・対応が遅い

・運用策定に於いて、白・黒、明確な回答が得られない。

・ISMS 取得の検討で代用

D-4. 外部のサービス業者、コンサルタントを利用している場合、それは次のどれに該当しますか
（複数回答可）

	主としてコンサルティングサービスを提供する業者	主として専門的セキュリティサービスを提供する業者	主としてセキュリティ製品を販売する業者	主としてネットワークサービスを提供する業者	主としてシステムインテグレーションを提供する業者	主として保守サービスを提供する業者	いわゆる情報子会社	合計
回答数	22	10	2	1	6	0	1	42
占有率	52.4%	23.8%	4.8%	2.4%	14.3%	0.0%	2.4%	100.0%



Note

・外部のサービス業者、コンサルタントを利用している場合、その提供主体は、「主としてコンサルティングサービスを提供する業者」が 52.4%を占め、以下、「主として専門的セキュリティサービスを提供する業者」が 23.8%、「主としてセキュリティ製品を販売する業者」が 4.8%、「主としてネットワークサービスを提供する業者」が 2.4%、「主としてシステムインテグレーションを提供する業者」が 14.3%、「主として保守サービスを提供する業者」が 0%、「いわゆる情報子会社」が 2.4%となった。

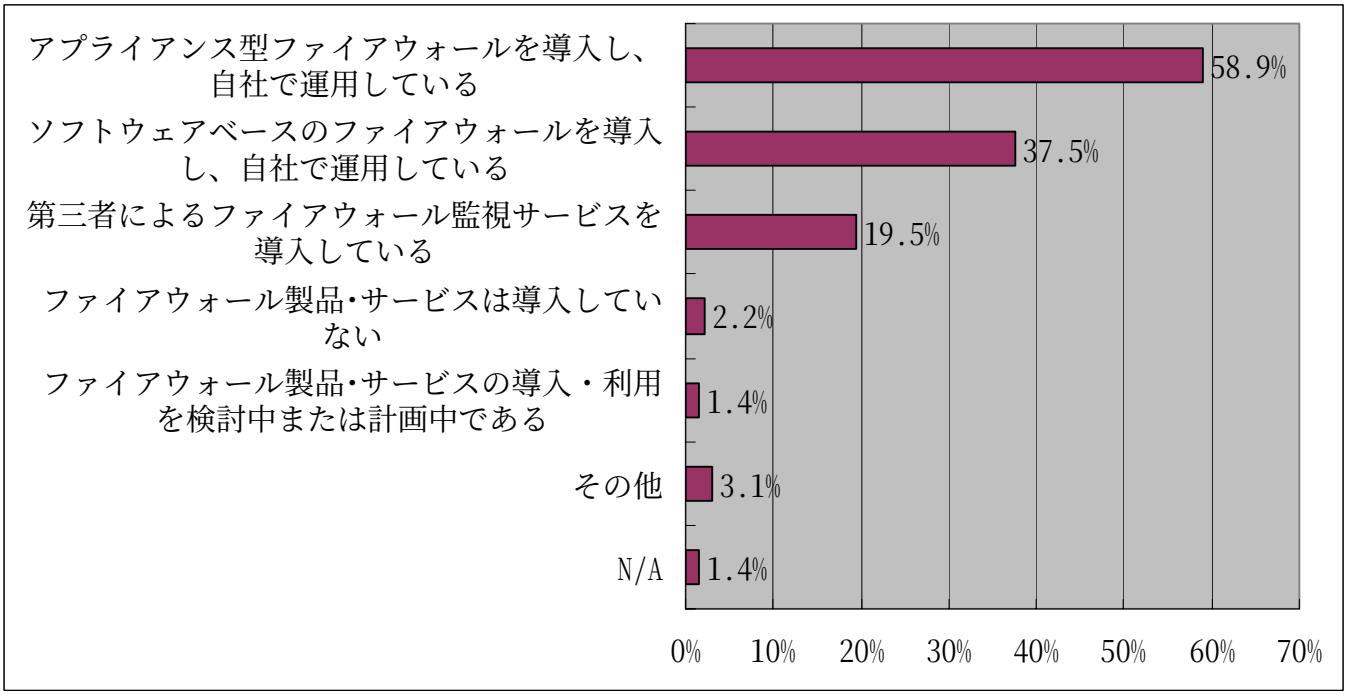
・この質問は該当企業だけに回答いただくものなので、無回答のものを除き、有効回答総数を 100%として占有率を算出した。

第三部　セキュリティ対策製品の導入状況と満足度

E.ファイアウォール

E-1. ファイアウォールの導入状況について、当てはまるものはどれですか（複数回答可 n=416）

	アプライアンス型ファイアウォールを導入し、自社で運用している	ソフトウェアベースのファイアウォールを導入し、自社で運用している	第三者によるファイアウォール監視サービスを導入している	ファイアウォール製品･サービスは導入していない	ファイアウォール製品･サービスの導入・利用を検討中または計画中である	その他	N/A	合計
回答数	245	156	81	9	6	13	6	516
占有率	58.9%	37.5%	19.5%	2.2%	1.4%	3.1%	1.4%	124.0%



Note

・ファイアウォールの導入状況については、「アプライアンス型ファイアウォールを導入し、自社で運用している」が 58.9%、「ソフトウェアベースのファイアウォールを導入し、自社で運用している」が 37.5%、「第三者によるファイアウォール監視サービスを導入している」が 19.5%、「ファイアウォール製品･サービスは導入していない」が 2.2%、「ファイアウォール製品･サービスの導入・利用を検討中または計画中である」が 1.4%、「その他」が 3.1%となった。

・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。

○「その他」の自由記述内容（記入されたとおりに収録。順不同）

・関係会社の WAN の一部を利用している為、何型のファイアウォールか不明

・情報子会社

・ルータのファイアウォール機能

・a（アプライアンス型ファイアウォールを導入し、自社で運用している）か、b（ソフトウェアベースのファイアウォールを導入し、自社で運用している）どちらか不明

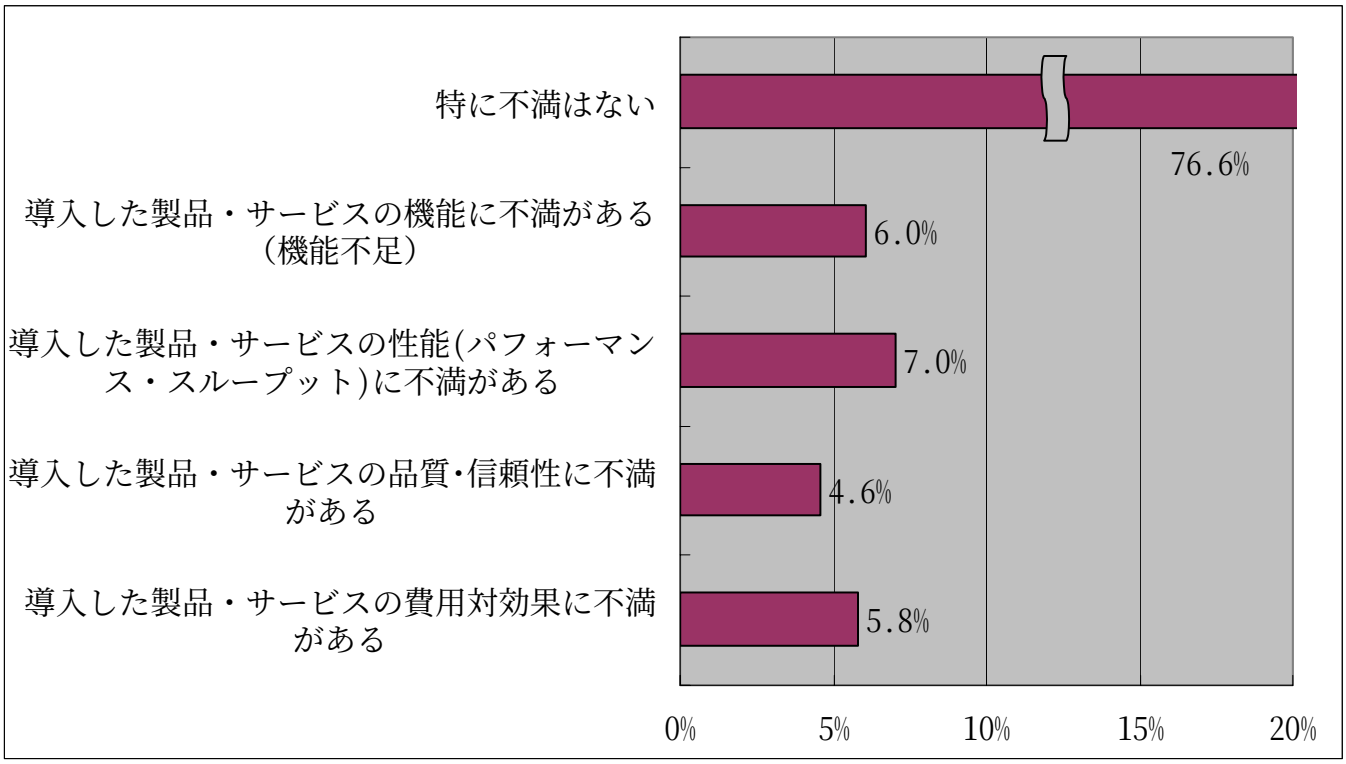
・ルータを使用している

・ルータのパケットフィルター等

・親会社システムの下で運用
・上位組織のゲートウェイにてファイアウォールを運用している（アプライアンス型ファイアウォールのタイプ）
・簡易ファイアウォールを導入中
・ネットワーク２系の内一方はソフトウェアベースのファイアウォール。残りの一方は、親会社のサービスを利用。
・インターネット以外で利用している。
・富士通より Web 一式導入(ファイアウォール AMZ)
・グループ会社(親会社)で導入

E-2．ファイアウォールの導入・運用上の不満・問題点について、次のうち当てはまるものはどれですか
（複数回答可）

	特に不満はない	導入した製品・サービスの機能に不満がある（機能不足）	導入した製品・サービスの性能(パフォーマンス・スループット)に不満がある	導入した製品・サービスの品質・信頼性に不満がある	導入した製品・サービスの費用対効果に不満がある	合計
回答数	317	25	29	19	24	414
占有率	76.6%	6.0%	7.0%	4.6%	5.8%	100.0%



Note

・ファイアウォールの導入・運用上の不満・問題点については、「特に不満はない」が 76.6%、「導入した製品・サービスの機能に不満がある（機能不足）」が 6.0%、「導入した製品・サービスの性能（パフォーマンス・スループット）に不満がある」が 7.0%、「導入した製品・サービスの品質・信頼性に不満がある」が 4.6%、「導入した製品・サービスの費用対効果に不満がある」が 5.8%となった。
・無回答のものを除き、有効回答総数を 100%として占有率を算出した。

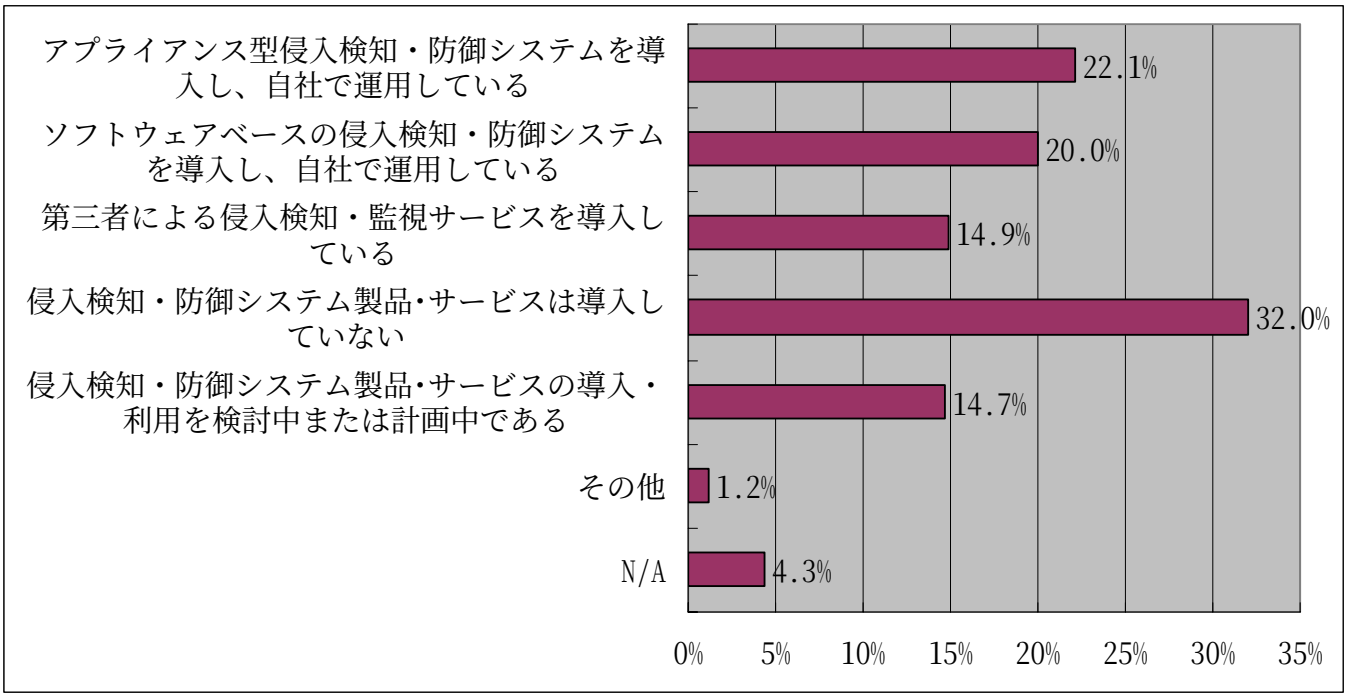
○不満がある場合の自由記述内容（記入されたとおりに収録。順不同）
・年間の保守料、定期的なライセンス費用が高い。
・費用対効果に不満
・速度パフォーマンス
・弊社では不明
・脅威にリアルに対応できているかの不安
・IP アドレスによる単純な制御しかできない点
・品質や運用において、可能なこと不可能なことが不明確で、ケースバイケースの対応となっている。運用者により解り易いマニュアル等の整備が必要。
・ログの解析機能に不満あり
・設定の問題ではあるが、想定外のアクセスが外部よりある。

・日毎に変わるアタック等の実態が不明のまま。これでいいのか？
・明確ではないが、正しく動作しているか不安がある。
・サービスが向上しないのに、費用は一定で変わらない点。
・保守料が高価である点
・ログを容易に参照できない
・急にネットワークパフォーマンスが落ち、原因不明（原因追求不能）に陥る場合がある。
・セキュリティ要員の育成
・ファイアウォールソフトのサポート 0S が、年々変わること。
・ダウンすることが多くある。
・問い合せに対する回答が遅い
・メンテナンスに手間がかかる。また知識が必要。
・保守費用が高い。
・Ｆ／Wを設置しても各種の監視、結果分析が必要であり、防御体制の構築にコストが掛かる。
・老巧化により、保守費に見合うだけの機能・性能が無くなってきている。
・運用費用が高い。
・障害時に膨大なログから情報を取得することが作業負荷となっている。また、ログの保存、消去にも苦慮している。簡易かつ強力な検知・通知機能が欲しい。
・現在使用している製品のライセンスカウントに柔軟性が無く、結果高く感じる。効果そのものに不満はない。
・メンテナンス性が悪く、機種も古い為にスループットにも問題有り。
・具体的な効果が見えない。外部からのセキュリティインデントが無い＝効果が有ると見なしているのが実情。
・価格が高い
・すり抜けある
・マニュアルがわかりづらく、設定をするのが難しい。
・ポリシー変更の度に費用発生する事。アクセスログ解析が難しい事。
・大量のウイルスメールやアタックを受けた際のパフォーマンス低下。
・機能不足
・時々フリーズする。

F. 侵入検知・防御システム（IDS, IDP, IPS）

F-1 侵入検知・防御システムの導入状況について、当てはまるものはどれですか（複数回答可）n=416

	アプライアンス型侵入検知・防御システムを導入し、自社で運用している	ソフトウェアベースの侵入検知・防御システムを導入し、自社で運用している	第三者による侵入検知・監視サービスを導入している	侵入検知・防御システム製品･サービスは導入していない	侵入検知・防御システム製品･サービスの導入・利用を検討中または計画中である	その他	N/A	合計
回答数	92	83	62	133	61	5	18	454
占有率	22.1%	20.0%	14.9%	32.0%	14.7%	1.2%	4.3%	109.1%



Note

・侵入検知・防御システムの導入状況については「アプライアンス型侵入検知・防御システムを導入し、自社で運用している」が 22.1%、「ソフトウェアベースの侵入検知・防御システムを導入し、自社で運用している」が 20.0%、「第三者による侵入検知・監視サービスを導入している」が 14.9%、「侵入検知・防御システム製品･サービスは導入していない」が 32.0%、「侵入検知・防御システム製品･サービスの導入・利用を検討中または計画中である」が 14.7%、「その他」が 1.2%となった。

・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。

○「その他」の自由記述内容（記入されたとおりに収録。順不同）

・情報子会社によるサービス

・a（アプライアンス型侵入検知・防御システムを導入し、自社で運用している）か、b（ソフトウェアベースの侵入検知・防御システムを導入し、自社で運用している）か不明。

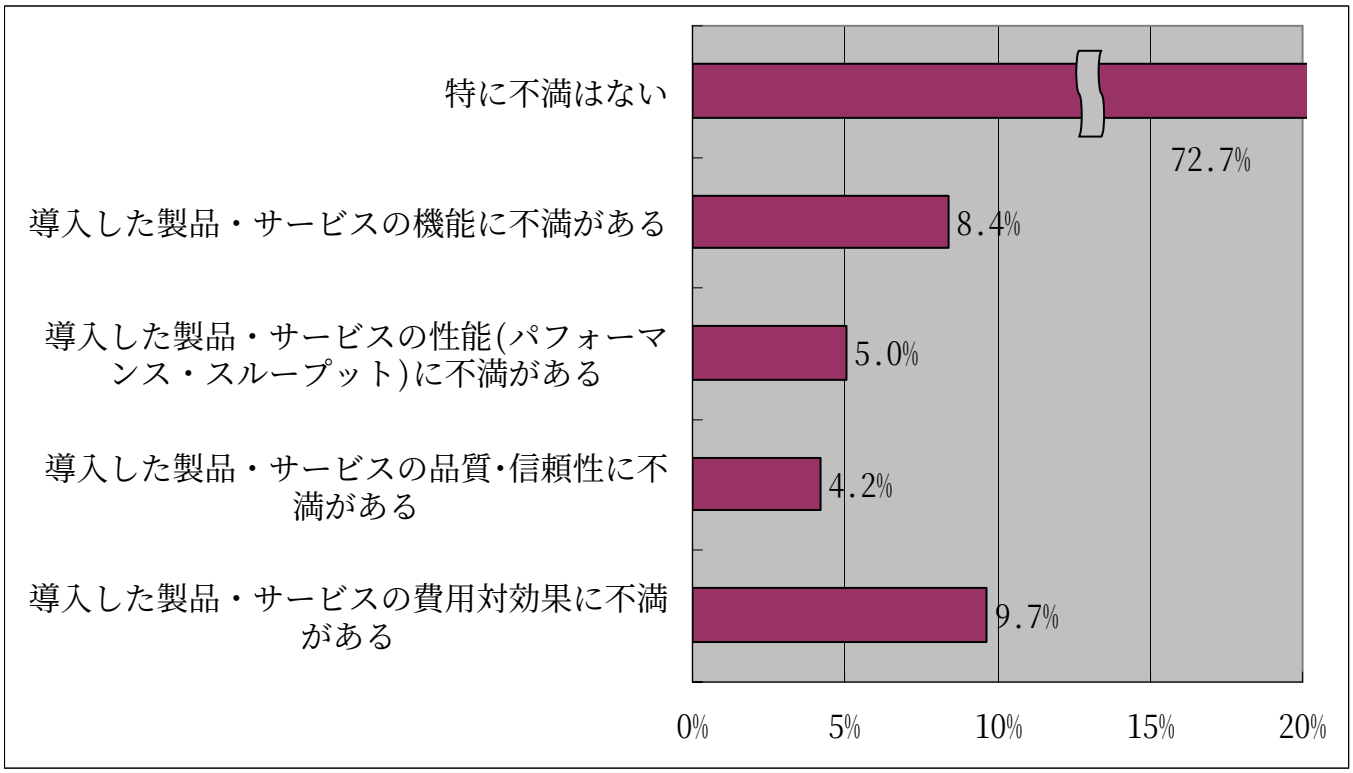
・親会社システムの下で運用

・ネットワーク２系の内一方はアプライアンス型侵入検知・防御システム。残りの一方は、親会社のサービスを利用。

・シスコ　ネットワーク型を導入

F-2. 侵入検知・防御システムの導入・運用上の不満・問題点について、次のうち当てはまるものはどれですか（複数回答可）

	特に不満はない	導入した製品・サービスの機能に不満がある	導入した製品・サービスの性能(パフォーマンス・スループット)に不満がある	導入した製品・サービスの品質・信頼性に不満がある	導入した製品・サービスの費用対効果に不満がある	合計
回答数	173	20	12	10	23	238
占有率	72.7%	8.4%	5.0%	4.2%	9.7%	100.0%



Note

・侵入検知・防御システムの導入・運用上の不満・問題点については、「特に不満はない」が 72.7%、「導入した製品・サービスの機能に不満がある」が 8.4%、「導入した製品・サービスの性能（パフォーマンス・スループット）に不満がある」が 5.0%、「導入した製品・サービスの品質・信頼性に不満がある」が 4.2%、「導入した製品・サービスの費用対効果に不満がある」が 9.7%となった。
・無回答のものを除き、有効回答総数を 100%として占有率を算出した。

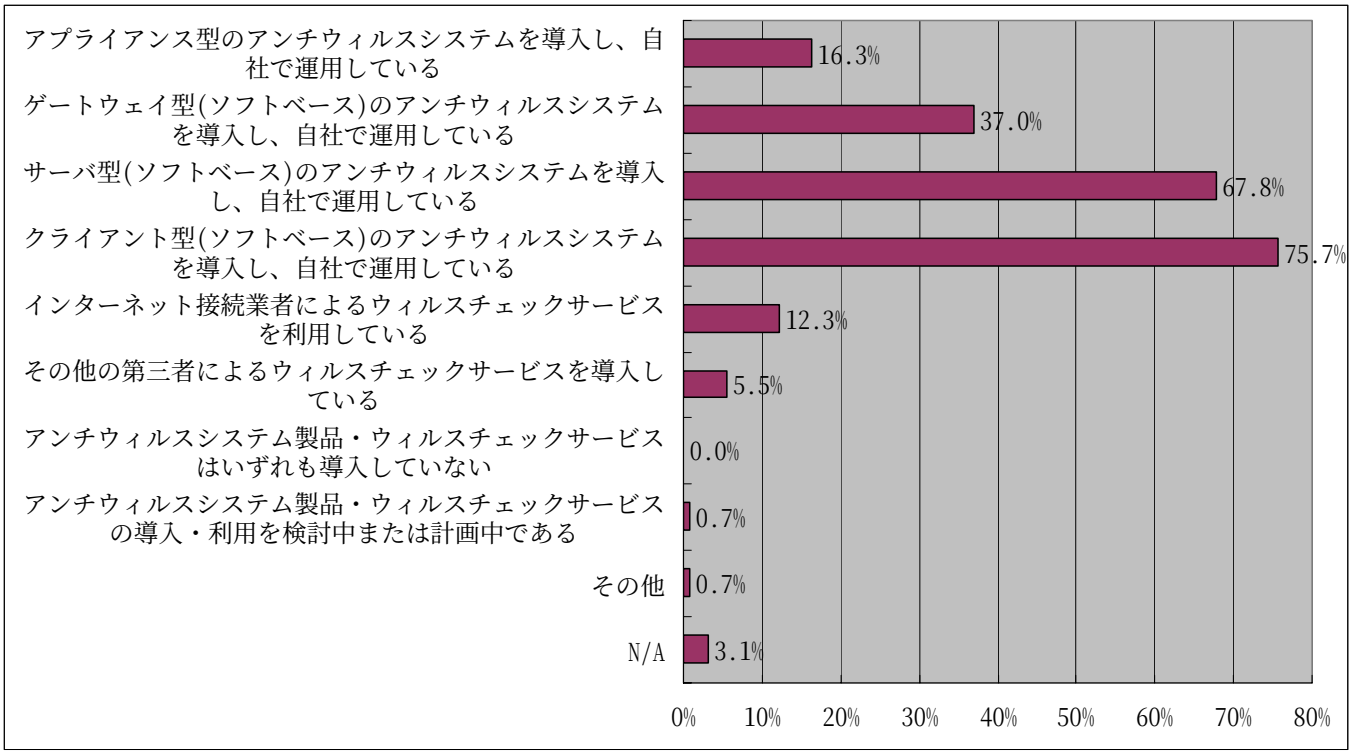
○不満がある場合の自由記述内容（記入されたとおりに収録。順不同）
・効果が見えにくい。運用状況が変化してあたりまえだが理解されていないので、何が正しいのかわからなくなる。
・本当に何が出来て、何が出来ないのか？難しい？まる投げのユーザーが多いのか？
・誤検知、あるいは過敏なアラーム
・レポート出力能力
・リスクに対するコストの算定基準が確立されていない
・DOS 等の兆候をキャッチして、少しでも事前防止につながる分析状況の提供がない。
・保守費用・対応の遅さに不満。
・検討中なので回答できない

・リスク分析が未完了
・セキュリティ製品の性質上やむをえないが、バージョンアップの頻度が高く、その都度、信頼性の検証等の対応工数が多大。
・緊急時の通知が遅い。高い。
・障害時に膨大なログから情報を取得することが作業負荷となっている。また、ログの保存、消去にも苦慮している。簡易かつ強力な検知・通知機能が欲しい。
・スループットが半分となっている。
・カタログ値との格差が大きい。
・運用が大変。　一般運用に併せるところまで技術が成熟していない。
・パターンファイルの更新が遅い
・アラートのプライオリティや対応手順の結びつきが不明。
・誤検知が多く、運用が大変なだけであまり有効とはいえない。
・適切なアラームレベルに設定しないと、アラームばかりが表示されて結局監視ができなくなると聞いている。
・案件を追加する場合に一時費用がかかる。
・検知すべき攻撃のポリシー策定に多くの労力を要する。
・運用が難しい。（アラームのチューニング）

G．アンチウイルス（ウイルス・ワーム対策）システム

G-1．アンチウイルスシステムの導入状況について、当てはまるものはどれですか（複数回答可）n=416

	アプライアンス型のアンチウィルスシステムを導入し、自社で運用している	ゲートウェイ型(ソフトベース)のアンチウィルスシステムを導入し、自社で運用している	サーバ型(ソフトベース)のアンチウィルスシステムを導入し、自社で運用している	クライアント型(ソフトベース)のアンチウィルスシステムを導入し、自社で運用している	インターネット接続業者によるウィルスチェックサービスを利用している	その他の第三者によるウィルスチェックサービスを導入している	アンチウィルスシステム製品・ウィルスチェックサービスはいずれも導入していない	アンチウィルスシステム製品・ウィルスチェックサービスの導入・利用を検討中または計画中である	その他	N/A	合計
回答数	68	154	282	315	51	23	0	3	3	13	912
占有率	16.3%	37.0%	67.8%	75.7%	12.3%	5.5%	0.0%	0.7%	0.7%	3.1%	219.2%



Note

・アンチウイルスシステムの導入状況については、「アプライアンス型のアンチウイルスシステムを導入し、自社で運用している」が 16.3%、「ゲートウェイ型(ソフトベース)のアンチウイルスシステムを導入し、自社で運用している」37.0%、「サーバー型(ソフトベース)のアンチウイルスシステムを導入し、自社で運用している」が 67.8%、「クライアント型(ソフトベース)のアンチウイルスシステムを導入し、自社で運用している」が 75.7%、「インターネット接続業者によるウイルスチェックサービスを利用している」が 12.3%、「その他の第三者によるウイルスチェックサービスを導入している」が 5.5%、「アンチウイルスシステム製品・ウイルスチェックサービスはいずれも導入していない」が 0%、「アンチウイルスシステム製品・ウイルスチェックサービスの導入・利用を検討中または計画中である」が 0.7%、「その他」が 0.7%となった。

・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。

○「その他」の自由記述内容（記入されたとおりに収録。順不同）

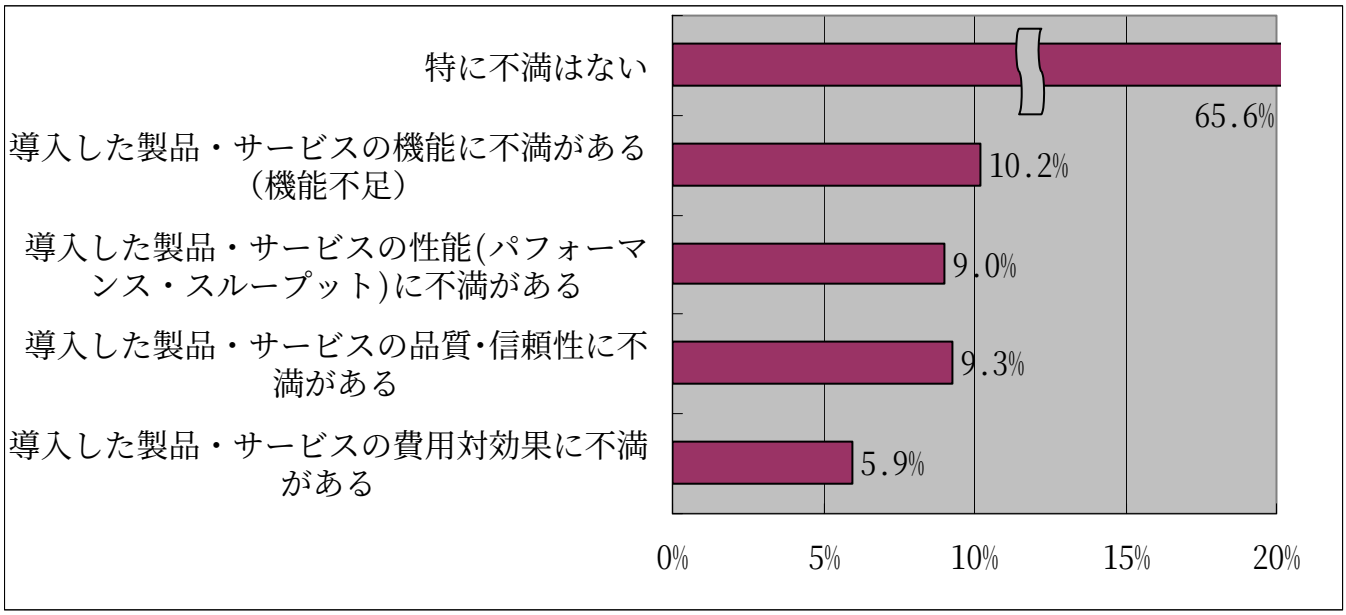
・非公開

・親会社のメールシステム下で運用中

・トレンドマイクロ　インターSCAN 導入

G-2．ウイルスチェックシステムの導入・運用上の不満・問題点について、次のうち当てはまるものはどれですか（複数回答可）

	特に不満はない	導入した製品・サービスの機能に不満がある（機能不足）	導入した製品・サービスの性能(パフォーマンス・スループット)に不満がある	導入した製品・サービスの品質･信頼性に不満がある	導入した製品・サービスの費用対効果に不満がある	合計
回答数	276	43	38	39	25	421
占有率	65.6%	10.2%	9.0%	9.3%	5.9%	100.0%



Note

・「特に不満はない」が 65.6%、「導入した製品・サービスの機能に不満がある（機能不足）」が 10.2%、「導入した製品・サービスの性能（パフォーマンス・スループット）に不満がある」が 9.0%、「導入した製品・サービスの品質･信頼性に不満がある」が 9.3%、「導入した製品･サービスの費用対効果に不満がある」が 5.9%となった。

・無回答のものを除き、有効回答総数を 100%として占有率を算出した。但し、複数回答を可としているので、回答総数は回収調査票総数を上回る 421 ある。これを 100 とするパーセンテージで表示している。

○不満がある場合の自由記述内容（記入されたとおりに収録。順不同）

・メールが多いとスループットが落ちるし、ソフトベンダーの対応もあいまいであったり、24h でない事が多い。
・パターンファイル更新タイミング
・年間費用が年々高くなっている
・対応へのスピード性
・ウイルス定義ファイル（パターン）の更新がウイルスの侵入に間に合わない場合がある。
・定義ファイルの更新が a 回／日にしか実行できない点（現状は、手動操作にて対応）
・ウイルスソフトの為、動作不能や不安定となったソフト有り。
・年数回、パターンファイルが間に合わなくウイルス、ワームがすりぬけてきたものがある。
・最新 OS での動作不安定（サポート対応も今一つ）
・ウイルス情報提供、定義ファイル提供が遅い（他社と比べて）
・サーバー、クライアント両方でチェックをしている。非常に大きな資源ロスの感じがする。

・パターンファイルの更新が遅い
・ワクチンの更新タイミング
・サーバー自身（OS に対する）対策が不明確
・手間がかかる。
・最近ウイルス発生が多いこともありパターンファイル更新が遅れることがある。
・メモリに常駐するサイズが大きい。
・ウイルススキャンが遅い。
・マシンが非常に遅くなる。
・機能的に不十分と思う（ウイルス削除やレポート機能）
・シグニチャの提供が間に合わなく、イントラネットに侵入を許し、広がる場合がある。
・バグが多く見られる
・新種対応が他社に比べ遅い
・それでもウイルスメールが大量に送信されてくる。また、相手先にメールを送信しても、はじかれてしまうので、連絡・やり取りが面倒だ。
・資源の食い過ぎ
・ウイルス発生からパターンファイル配信までにかかるタイムラグ
・導入製品の UPDATE が多い
・クライアントで稼動しているアンチウイルスソフトのウイルス定義ファイルが最新になっていることをリモートで確認できない。この点はバージョンアップにより集中管理が可能になり、現在計画中。
・クライアント型アンチウイルスシステムについて。それを導入しても、１００％感染を防ぐ事ができるとは言えない。電子メール、資料配布により、お客様に迷惑がかからない様細心の注意が常に必要とされる。
・製品の不具合が多少ある。
・ウイルス発生が初発（最初）の場合、対応するパターンが作成されるまで、時間を要する場合が有る。
・ネットワーク OS のバージョンが古く、アンチウイルスソフトも古いバージョンを使わざるを得ない。
・日本語版がない（様だ）
・全部は防げない
・新種ウイルスにパターンファイルが追いつかないケースが発生する。
・クライアント型なので、管理が難しい
・費用がかかり過ぎる
・導入した PC の利用ソフト及びパフォーマンスに影響がある。
・エンドユーザーの作業がふえてしまっている。
・パターンファイルの早期提供
・製品のバージョンが上がる毎にパフォーマンスが悪くなる。
・ときどき、パターンファイル・エンジンの更新が PC やサーバーの障害を引き起こす。
・緊急なウイルス対策が発表された後の各ソフトウェア業者の迅速な対応方法を求む。
・拡散力が強く、特に緊急性の高いメール添付型ウイルスに対し、パターンファイルの適用が間に合わないケースもあった。
・必要以上にメンテに手間がかかるものがある。
・完璧にウイルス駆除できない。
・新ウイルス発生時のパターンファイル提供までのタイムラグが長い。
・パフォーマンスとして性能向上を望む。
・新種ウイルスのパターンファイル提供のスピード。
・ライセンス更新時のサービス内容の変更。（ex.ライセンス無制限→ボリュームライセンス）

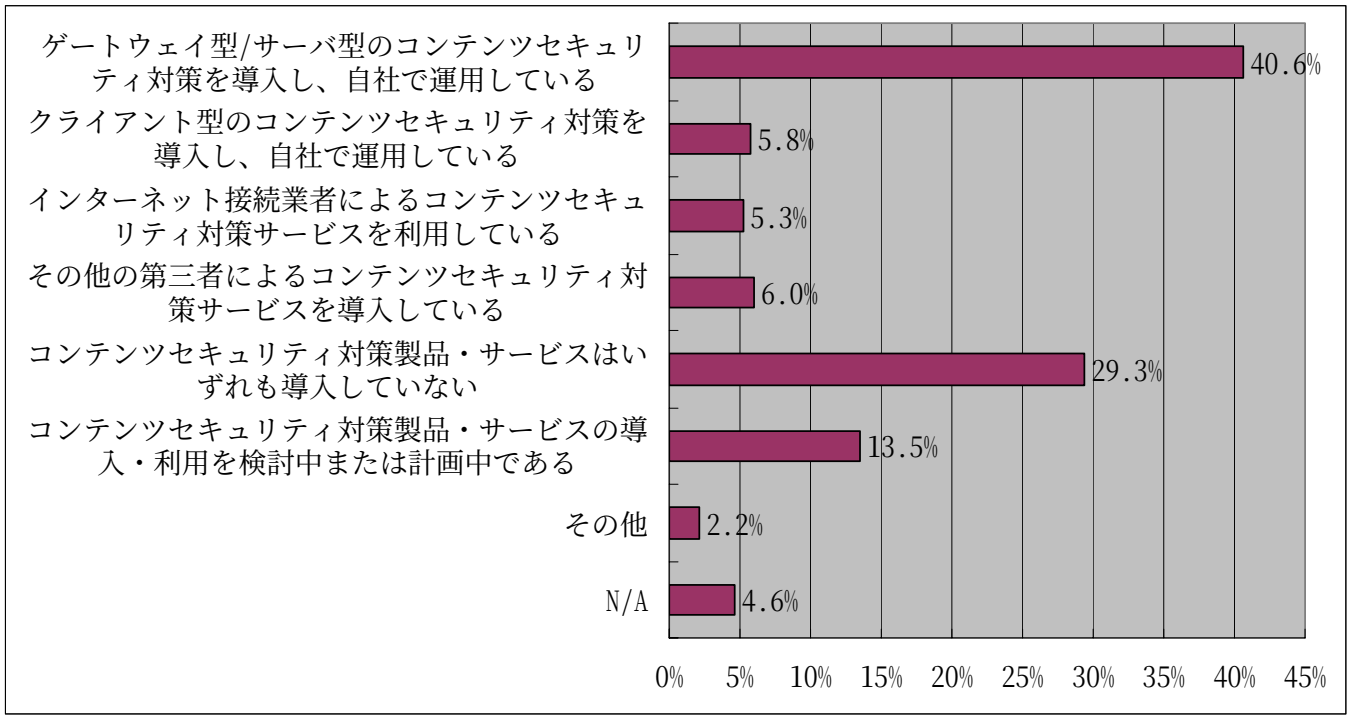
・セキュリティ製品の性質上やむをえないが、バージョンアップの頻度が高く、その都度、信頼性の検証等の対応工数が多大。
・新種ウイルスに対するパターン公開が遅い
・ウイルス感染のトラブルが、発生することがある。
・パターンファイルの更新が遅い。
・ウイルス発生時の対応の遅れ
・未知の新種ウイルスに対する検知・防御機能が弱い。
・強いて言えば新型ウイルスへの対策を早めて欲しい。
・パターンファイルの更新速度　クライアントに反映されるまでが遅い。
・日本語の製品でない為、画面操作がしにくい。管理者ガイドだけでは難しい。
・ファーストアタックは防ぎようが無い。
・メールサーバーのチェックソフトを導入中であるがパフォーマンスに不満がある。
・旧式のパソコンの場合、負担が大きいことがある
・導入がクライアントより、上手く行かない場合がある。
・導入当初には、インタースキャンの関係で機能不足が見られたが、現状では、改善されている。スパムメールのチェック（カットの判断）があいまいである。
・サーバー負荷が高くなり、他のアプリの性能に影響を与える。
・ウイルスのパターンファイルの更新が遅い時があった。
・問い合せ対応に不満（質、ＴＡＴとも）
・差分を自動的にダウンロードしているうちにウイルスソフトが停止起動しなくなった。
・製品のバージョンアップが多くあり、更新維持コストがかかる。
・NAT が入るとパターン配信できない。
・ウイルス付メールの排除などの機能不足
・残念ながらウイルスを検知するためのシグネチャ（パターン）の更新、適用に時間的な差が存在するため、ウイルスの検知・感染を完全に防ぐことが出来ない。
・マニュアルがわかりづらく、設定をするのが難しい。
・ソフトのバージョンアップが多い。全国の営業所へ展開している場合のバージョンアップ方法への配慮を考えて欲しい。
・クライアント製品の統合管理機能に、機能不足を感じる。
・クライアントモジュールがクライアントシステムに対して、負荷をかける事が多い。
・検索エンジン更新時バージョンアップ時の動作不具合が多い。
・大量のウイルスメールやアタックを受けた際のパフォーマンス低下。
・ウイルスの伝播が早く、ワクチンの対応が遅れることが多い。
・ワクチン対応が遅い場合がある。
・パターンファイル更新が遅い。サーバーが分かれているとログが別々になる。
・クライアント更新管理機能の管理者負担が大きい。
・定義ファイルのリリースタイミングが遅い場合がある。

H．アンチウイルス以外のコンテンツセキュリティ対策

（アンチスパム、URL フィルタリング、メールフィルタリング）

H-1．アンチウイルス以外のコンテンツセキュリティ対策の導入状況について、当てはまるものはどれですか(複数回答可）n=416

	ゲートウェイ型/サーバ型のコンテンツセキュリティ対策を導入し、自社で運用している	クライアント型のコンテンツセキュリティ対策を導入し、自社で運用している	インターネット接続業者によるコンテンツセキュリティ対策サービスを利用している	その他の第三者によるコンテンツセキュリティ対策サービスを導入している	コンテンツセキュリティ対策製品・サービスはいずれも導入していない	コンテンツセキュリティ対策製品・サービスの導入・利用を検討中または計画中である	その他	N/A	合計
回答数	169	24	22	25	122	56	9	19	446
占有率	40.6%	5.8%	5.3%	6.0%	29.3%	13.5%	2.2%	4.6%	107.2%



Note

・「ゲートウェイ型/サーバー型のコンテンツセキュリティ対策を導入し、自社で運用している 」が 40.6%、「クライアント型のコンテンツセキュリティ対策を導入し、自社で運用している」が 5.8%、「インターネット接続業者によるコンテンツセキュリティ対策サービスを利用している」が 5.3%、「その他の第三者によるコンテンツセキュリティ対策サービスを導入している」が 6.0%、「コンテンツセキュリティ対策製品・サービスはいずれも導入していない」が 29.3%、「コンテンツセキュリティ対策製品・サービスの導入・利用を検討中または計画中である」が 13.5%、「その他」が 2.2%となった。

・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。

○「その他」の自由記述内容（記入されたとおりに収録。順不同）

・非公開

・URL については（フリーソフトで手動でチェック）接続制限

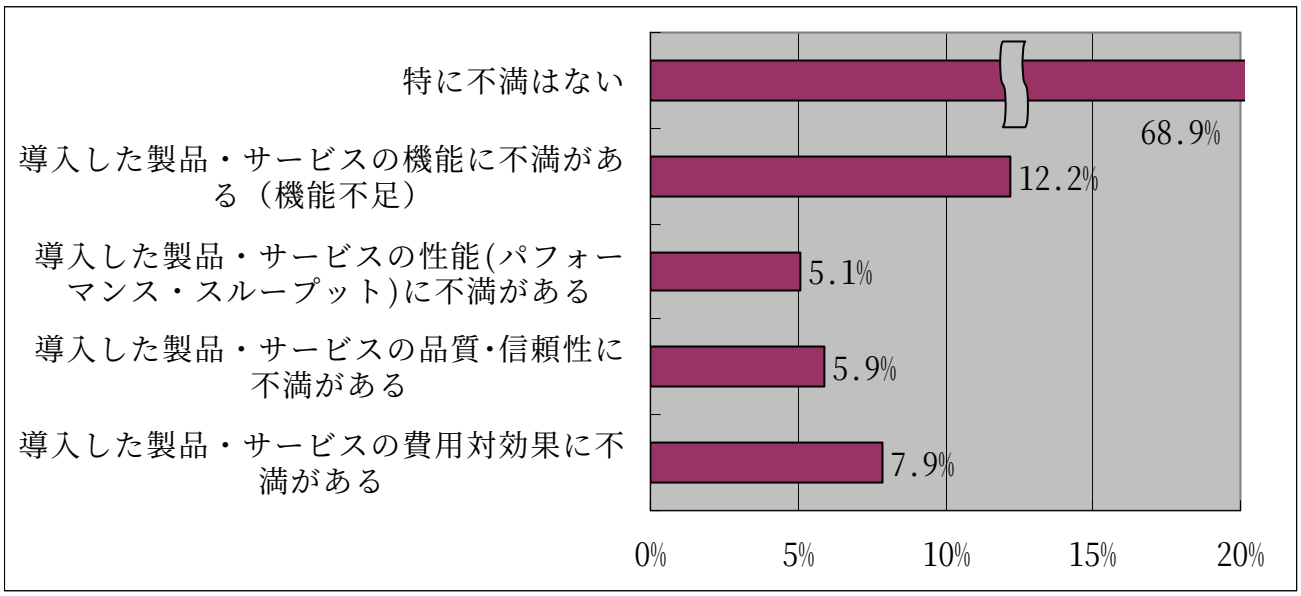
・導入しているが機能させていない。

・親会社システムの下で運用中

・上位組織のゲートウェイにコンテンツセキュリティ対策を導入し運用中（ゲートウェイ型/サーバー型のタイプ）
・不明

H-2．コンテンツセキュリティ対策の導入・運用上の不満・問題点について、次のうち当てはまるものはどれですか（複数回答可）

特に不満はない	導入した製品・サービスの機能に不満がある（機能不足）	導入した製品・サービスの性能(パフォーマンス・スループット)に不満がある	導入した製品・サービスの品質・信頼性に不満がある	導入した製品・サービスの費用対効果に不満がある	合計
175	31	13	15	20	254
68.9%	12.2%	5.1%	5.9%	7.9%	100.0%



Note

・コンテンツセキュリティ対策の導入・運用上の不満・問題点については、「特に不満はない」が 68.9%、「導入した製品・サービスの機能に不満がある（機能不足）」が 12.2%、「導入した製品・サービスの性能（パフォーマンス・スループット）に不満がある」が 5.1%、「導入した製品・サービスの品質・信頼性に不満がある」が 5.9%、「導入した製品・サービスの費用対効果に不満がある」が 7.9%となった。
・無回答のものを除き、有効回答総数を 100%として占有率を算出した。

○不満がある場合の自由記述内容（記入されたとおりに収録。順不同）
・アプリケーションを新規で立上げた時に不具合があってもベンダーに調査能力が無い事が多い。
・全面的に信頼の出来るレベルの商品がない。複数の組合せが必要かつ万全とは言えない。
・運用管理の機能不足
・フィルタのデータベースの内容が甘くスルーするＵＲＬが多い。
・レポート機能などもう少し欲しい。
・確証機能
・業務にふさわしくないコンテンツ（アダルト等）の自動フィルタリング機能がない。
・入れたばかりで特になし
・ＵＲＬフィルタリングを導入しているが、適格な設定が難しい
・日本語
・維持費が高く、コスト効果の点で見劣りがする。
・費用が高い
・精度の不足

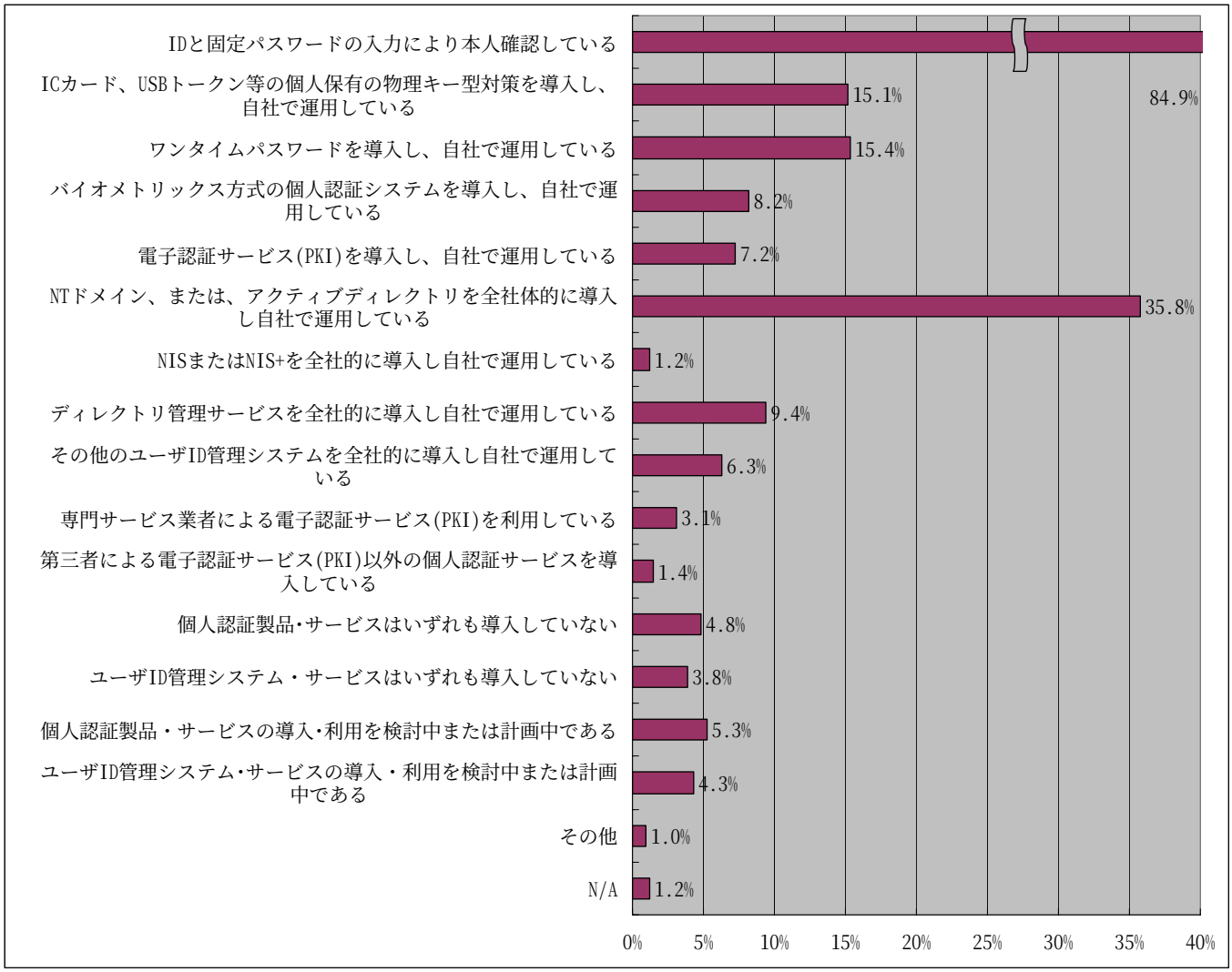
・特定ＵＲＬへのアクセスのパフォーマンスが悪い。
・フィルタリングリストの妥当性を判断することが難しい。たまに明らかに誤った設定が施されていることがある。（１～２件／年）
・ＵＲＬ、スパム共に、いたちごっこが続いており、直ぐに陳腐化する。
・パフォーマンス、スループットの向上を望む。
・ログ解析機能（集計等）が不満。
・実現機能に対し、製品価格が高い。
・登録ミスがある。
・コンテンツの制御などを実施する場合、組織の違いのため、一律の設定では対応できない状況がある。
・費用が高い。
・日本語の製品でない為、画面操作がしにくい。管理者ガイドだけでは難しい。
・コンテンツの決定、メンテナンスに手間がかかりすぎる。
・今回のバージョンアップで機能不足は改善された。
・フィルタそのもののメンテナンス性が必ずしも良くない。
・フィルタリングの内容が不明確な為、ユーザー説明にこまる。
・当社の業務形態が大きく影響しているが、対策（URL フィルタリング等）の適用範囲が限定的になっている。適用範囲が全社となるようなプロダクトの登場を望む。
・余計なＵＲＬまでフィルタリングされている。
・フィルタリング等の追加設定時に、一時費用がかかり、且つ納期がかかる。（1 週間程度）
・カテゴリーの定義があいまい。
・フィルタリングポリシーがユーザーへ公開されていない。

I．システムへのログオンに際しての個人（本人）認証及びユーザーID 管理

I-1．個人認証システム及びユーザーID 管理の導入状況について、当てはまるものはどれですか（複数回答可）

n=416

	IDと固定パスワードの入力により本人確認している	ICカード、USBトークン等の個人保有の物理キー型対策を導入し、自社で運用している	ワンタイムパスワードを導入し、自社で運用している	バイオメトリックス方式の個人認証システムを導入し、自社で運用している	電子認証サービス(PKI)を導入し、自社で運用している	NTドメイン、または、アクティブディレクトリを全社体的に導入し自社で運用している	NISまたはNIS+を全社的に導入し自社で運用している	ディレクトリ管理サービスを全社的に導入し自社で運用している	その他のユーザID管理システムを全社的に導入し自社で運用している	専門サービス業者による電子認証サービス(PKI)を利用している
回答数	353	63	64	34	30	149	5	39	26	13
占有率	84.9%	15.1%	15.4%	8.2%	7.2%	35.8%	1.2%	9.4%	6.3%	3.1%
	第三者による電子認証サービス(PKI)以外の個人認証サービスを導入している	個人認証製品・サービスはいずれも導入していない	ユーザID管理システム・サービスはいずれも導入していない	個人認証製品・サービスの導入・利用を検討中または計画中である	ユーザID管理システム・サービスの導入・利用を検討中または計画中である	その他	N/A	合計		
回答数	6	20	16	22	18	4	5	867		
占有率	1.4%	4.8%	3.8%	5.3%	4.3%	1.0%	1.2%	208.4%		



Note

・個人認証システム及びユーザーID 管理の導入状況については、「ID と固定パスワードの入力により本人確認している」が 84.9%、「IC カード、USB トークン等の個人保有の物理キー型対策を導入し、自社で運用している」が 15.1%、「ワンタイムパスワードを導入し、自社で運用している」が 15.4%、「バイオメトリックス方式の個人認証システムを導入し、自社で運用している」が 8.2%、「電子認証サービス(PKI)を導入し、自社で運用している」が 7.2%、「NT ドメイン、または、アクティブディレクトリを全社体的に導入し自社で運用している」が 35.8%、「NIS または NIS+を全社的に導入し自社で運用している」が 1.2%、「ディレクトリ管理サービスを全社的に導入し自社で運用している」が 9.4%、「その他のユーザーID 管理システムを全社的に導入し

自社で運用している」が 6.3%、「専門サービス業者による電子認証サービス(PKI)を利用している」が 3.1%、「第三者による電子認証サービス(PKI)以外の個人認証サービスを導入している」が 1.4%、「個人認証製品・サービスはいずれも導入していない」が 4.8%、「ユーザーID 管理システム・サービスはいずれも導入していない」が 3.8%、「個人認証製品・サービスの導入・利用を検討中または計画中である」が 5.3%、「ユーザーID 管理システム・サービスの導入・利用を検討中または計画中である」が 4.3%、「その他」が 1.0%となった。

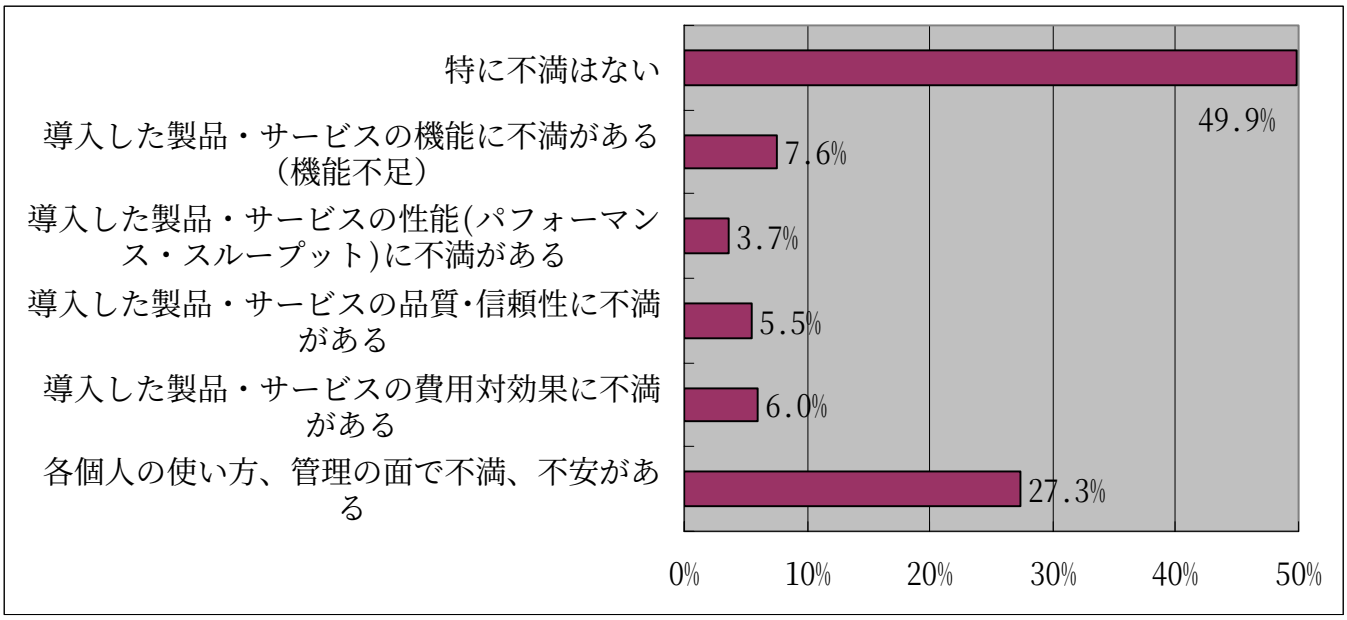
・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。

○「その他」の自由記述内容（記入されたとおりに収録。順不同）

・非公開
・システムへのログオン時に個人認証は行っていない。
・LDAP
・IC カードの併用を検討中

I-2. 個人認証システム、及びユーザーID 管理システムの導入・運用上の不満・問題点について、
次のうち当てはまるものはどれですか（複数回答可）

	特に不満はない	導入した製品・サービスの機能に不満がある（機能不足）	導入した製品・サービスの性能(パフォーマンス・スループット)に不満がある	導入した製品・サービスの品質･信頼性に不満がある	導入した製品・サービスの費用対効果に不満がある	各個人の使い方、管理の面で不満、不安がある	合計
回答数	190	29	14	21	23	104	381
占有率	49.9%	7.6%	3.7%	5.5%	6.0%	27.3%	100.0%



Note

・個人認証システム、及びユーザーID 管理システムの導入・運用上の不満・問題点については、「特に不満はない」が 49.9%、「導入した製品・サービスの機能に不満がある（機能不足）」が 7.6%、「導入した製品・サービスの性能（パフォーマンス・スループット）に不満がある」が 3.7%、「導入した製品・サービスの品質・信頼性に不満がある」が 5.5%、「導入した製品・サービスの費用対効果に不満がある」が 6.0%、「各個人の使い方、管理の面で不満、不安がある」が 27.3%となった。
・無回答のものを除き、有効回答総数を 100%として占有率を算出した。

○不満や不安がある場合の自由記述内容（記入されたとおりに収録。順不同）
・使い勝手と、費用対効果を考え、どれが自社に一番良いのかの見極めが難しい。
・NT ドメインと AD が混在している為、業務上パスワードを設定出来ないユーザーが存在する。
・他人がすぐ発覚する様なパスワードを使用し、長期にわたってそれを使用し続けている。
・アプリケーションにより、ID と PW を使い分けなければならない場合があり、不便な時がある。
・パスワードの運用に工数大。
・基幹のオフコンが脆弱
・パスワードの変更を運用上強制しきれない。
・個人のセキュリティ意識が最善の解決策
・セキュリティカードの運用が繁雑である。ディレクトリーサービスとの連携等を検討している。
・パスワードの変更が困難な為、パスワードが固定化されている。
・パスワードが組織内の人間であれば、大部分分かってしまう。

・管理業務が繁雑。ユーザー情報の統一がむずかしい
・ユーザーのパスワード管理が杜撰。教育・啓蒙しても、根付かない。
・運営・システム構成の統一と実施管理の強化が必要
・定期見直し、特に異動・退職など、関連会社やアルバイトを含め完全性が保てない。
・ID がシステムごとにあり Password を定期的に変更は現実的にできない。
・パスワードの管理がルーズになる。
・認証に特化していて、権限付与などの機能が不十分。
・現在の固定パスワードによる認証は脆弱であることは否めない。シングルサインオンなどにより、ユーザーの利便性を確保しつつ、安全性を向上できる環境を構築していくべきと考える。
・使い勝手が悪い
・パスワードの変更があまり行われない。
・パスワード管理の仕方に見直しが必要。（固定ＩＤ、パスワードの運用の見直し→定期的なパスワード変更の運用など）
・バイオメトリクスに移行したい
・共有 ID、固定パスワードのシステムがある。（一部）
・「なりすまし」対策が弱い
・将来的には Javacard のようなシステムを導入したい。
・標準の管理機能（登録／改廃）では、運用上機能不足で、別途仕組みを作って運用している。
・各ユーザーのパスワード管理に多少の不安がある。各パソコンの管理者権限の管理が難しい（運用負荷とセキュリティレベルのトレードオフ）
・システム毎に認証しており、複数の認証サーバーが稼動している。
・ID／パスの変更管理が不十分なため、リスクを感じることがある。
・各人の意識の向上が課題
・パスワード漏洩。アルバイト社員を含めた従業員の意識の低さ。
・ワンタイムパスワードについて導入希望が多い。
・パスワードの定期的変更等、個人管理に任される部分の徹底が図りにくい。
・各ＰＣへの導入が面倒で手間が掛かる。
・①ネットワーク上に個人情報が平文で流れている。②ユーザー管理がシステム毎。③認証の方式が甘い。
・個人認証システム構築の費用対効果が、明確に現れない。製品の統合化。
・パスワードのルールや定期的な変更が弱い。
・他人（他の社員）にパスワード等を教えたりしていないか。
・利用システムにより、認証方式を使い分けるが面倒。ユーザーの追加、削除も各認証システムに行うのが面倒であり、認定漏れの可能性もある。
・シングルサインオンを目指したが、なかなかうまくいかない。
・指数認証を導入したが登録してある個人の判定が不安定です。マーチエラー多発、１台に MAX６人登録しかできないため、運用で不便。
・パスワードの更新は個人が管理しているので信頼性に不安がある。
・高負荷時の信頼性。
・システム毎に個別の運用となっている。近々統一する事を検討している。
・認証の仕組みが複雑化しているため、障害時の対応に苦慮する。
・ID を複数人で使用しても分からない。
・パスワード管理体制強化に取組み中
・脆弱性などのメンテナンス作業に工数がかかる。

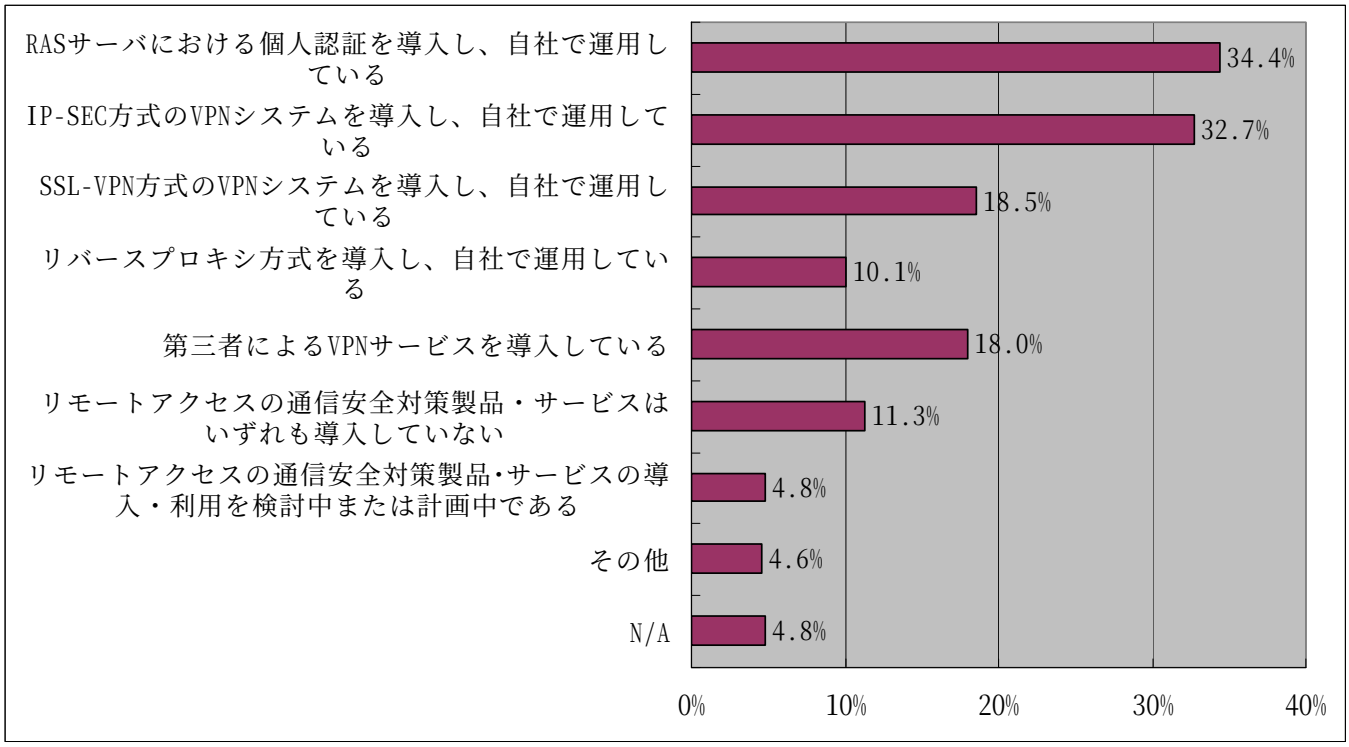
・認証に一環性がなく、幾度となく認証を求められる事。
・統合を容易に使いたい。
・パスワード管理について不安がある。
・エンドユーザーがパスワードの重要性を認識していない
・各個人の認識が不十分。
・多数のシステムを扱っている為、認証の仕組みを個別で持っており管理が大変。
・導入当初の不満であり、改善要求が受入れられた。
・　パスワードの定期的な更新が徹底しない。
・ＩＣカードによる個人認証を導入（部分的）しているか、入退管理以外の用途（ＰＣセキュリティ等）との体系的な使用法が未整備で、整合がとれていない。
・ユーザーに負担をかけない事が望ましいが、そこまで到達していない。
・正規の運用ルールが徹底されているか不安である。
・費用がかかりすぎる
・ディレクトリーの導入による運用の簡素化
・簡単かつ強固な管理・認証の仕組みがない。
・定期的なパスワード変更などの運用対策が不安
・個人毎にパソコンの能力に差があり、セキュリティレベルの高い運用を実施するのが困難。
・各個人のパスワード管理に関する教育が徹底されていない。
・不適切なパスワードを設定している。
・パスワード変更を定期的に指示しているが、変更されたかどうか判断できない。
・ID パスワードの漏洩、ログインした状態での放置など。
・定期的なパスワード変更の実施が徹底されていない。
・ワンタイムパスワードは、カード型を利用しているため電池切れ等の対応のための管理負荷が高い。
・運用管理の負荷
・管理者の運用負荷が高い。

J.リモートアクセスの通信安全対策システム

J-1.リモートアクセスの通信安全対策の導入状況について、当てはまるものはどれですか（複数回答可）

n=416

	RASサーバにおける個人認証を導入し、自社で運用している	IP-SEC方式のVPNシステムを導入し、自社で運用している	SSL-VPN方式のVPNシステムを導入し、自社で運用している	リバースプロキシ方式を導入し、自社で運用している	第三者によるVPNサービスを導入している	リモートアクセスの通信安全対策製品・サービスはいずれも導入していない	リモートアクセスの通信安全対策製品･サービスの導入・利用を検討中または計画中である	その他	N/A	合計
回答数	143	136	77	42	75	47	20	19	20	559
占有率	34.4%	32.7%	18.5%	10.1%	18.0%	11.3%	4.8%	4.6%	4.8%	134.4%



Note

・リモートアクセスの通信安全対策の導入状況については、「RAS サーバーにおける個人認証を導入し、自社で運用している」が 34.4%、「IP-SEC 方式の VPN システムを導入し、自社で運用している」が 32.7%、「SSL-VPN 方式の VPN システムを導入し、自社で運用している」が 18.5%、「リバースプロキシ方式を導入し、自社で運用している」が 10.1%、「第三者による VPN サービスを導入している」が 18.0%、「リモートアクセスの通信安全対策製品・サービスはいずれも導入していない」が 11.3%、「リモートアクセスの通信安全対策製品･サービスの導入・利用を検討中または計画中である」が 4.8%、「その他」が 4.6%となった。

・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。

○「その他」の自由記述内容（記入されたとおりに収録。順不同）

・特殊な例以外 RASVPN 系のリモートアクセスは用いない。PKI によるアクセスを利用。

・非公開

・PPTP ルータ接続での VPN システム

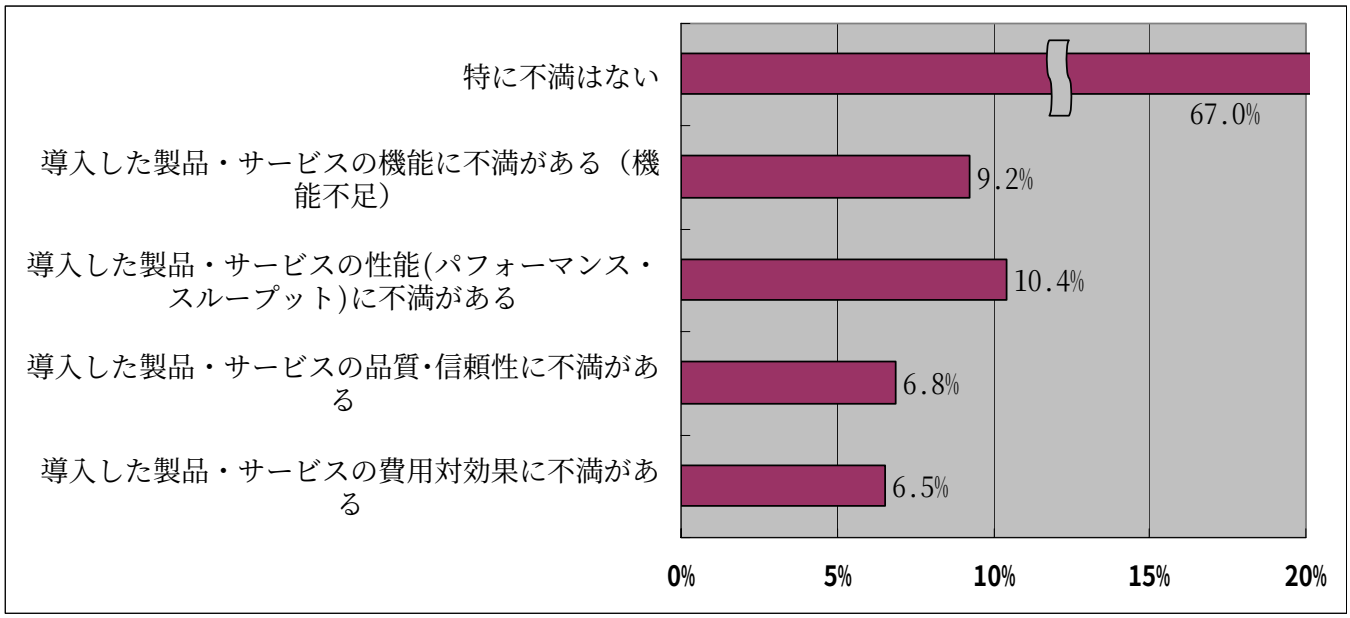
・インターネット VPN の導入を検討中である（RAS からの一部移行）

・導入したが、自社運用の為、セキュリティ上不安有運用停止した。

・グループ会社製のアプライアンス型 IP-VPN の導入
・閉域網サービスの利用
・リモートアクセスをしていない。
・リモートアクセス環境を構築していない。
・個人は認めていない、拠点間はインターネットを利用しない方式で接続。
・PIAFS 発信者認証
・AT&T セキュア IP サービス
・PPTP 方式の VPN システム
・リモートアクセス不可としている
・リモートアクセスルーター
・MPPE 方式
・ファイアーウォール・アプライアンス製品の VPN を利用
・未導入
・親会社による運用

J-2.リモートアクセスの通信安全対策の導入・運用上の不満・問題点について、次のうち当てはまるものはどれですか（複数回答可）

	特に不満はない	導入した製品・サービスの機能に不満がある（機能不足）	導入した製品・サービスの性能(パフォーマンス・スループット)に不満がある	導入した製品・サービスの品質･信頼性に不満がある	導入した製品・サービスの費用対効果に不満がある	合計
回答数	225	31	35	23	22	336
占有率	67.0%	9.2%	10.4%	6.8%	6.5%	100.0%



Note

・リモートアクセスの通信安全対策の導入・運用上の不満・問題点については、「特に不満はない」が 67.0%、「導入した製品・サービスの機能に不満がある（機能不足）」が 9.2%、「導入した製品・サービスの性能（パフォーマンス・スループット）に不満がある」が 10.4%、「導入した製品・サービスの品質・信頼性に不満がある」が 6.8%、「導入した製品・サービスの費用対効果に不満がある」が 6.5%となった。
・無回答のものを除き、有効回答総数を 100%として占有率を算出した。

○不満がある場合の自由記述内容（記入されたとおりに収録。順不同）
・アップグレードしようとしたが、高価な為アップグレード出来なかった。
・高速なアクセスポイントが欲しい。
・VPN サービスのメニューにウイルス対策が無い
・IP-SEC、L2TP に変更したい。又は IPV6 に変更したい。
・RAS サーバーは導入して、時間がたっているので現在のクライアント OS に対応していないので、使えない機能が出て、セキュリティ上問題が出ている。
・１ユーザー当りのコストがまだ高い。
・なりすましのリスクは避けられない。
・ログがとれない。
・P-in メモリ（phs）により、64Kbps しか出ないのは遅すぎる。FOMA にするとパケット課金であり、料金が不安。安くて早いリモートアクセスができないと、実務処理は不可能。または制限されてしまう。
・通信スピードの割に料金が高い
・INS64K でのアクセスのため、通信費と速度に不満がある。

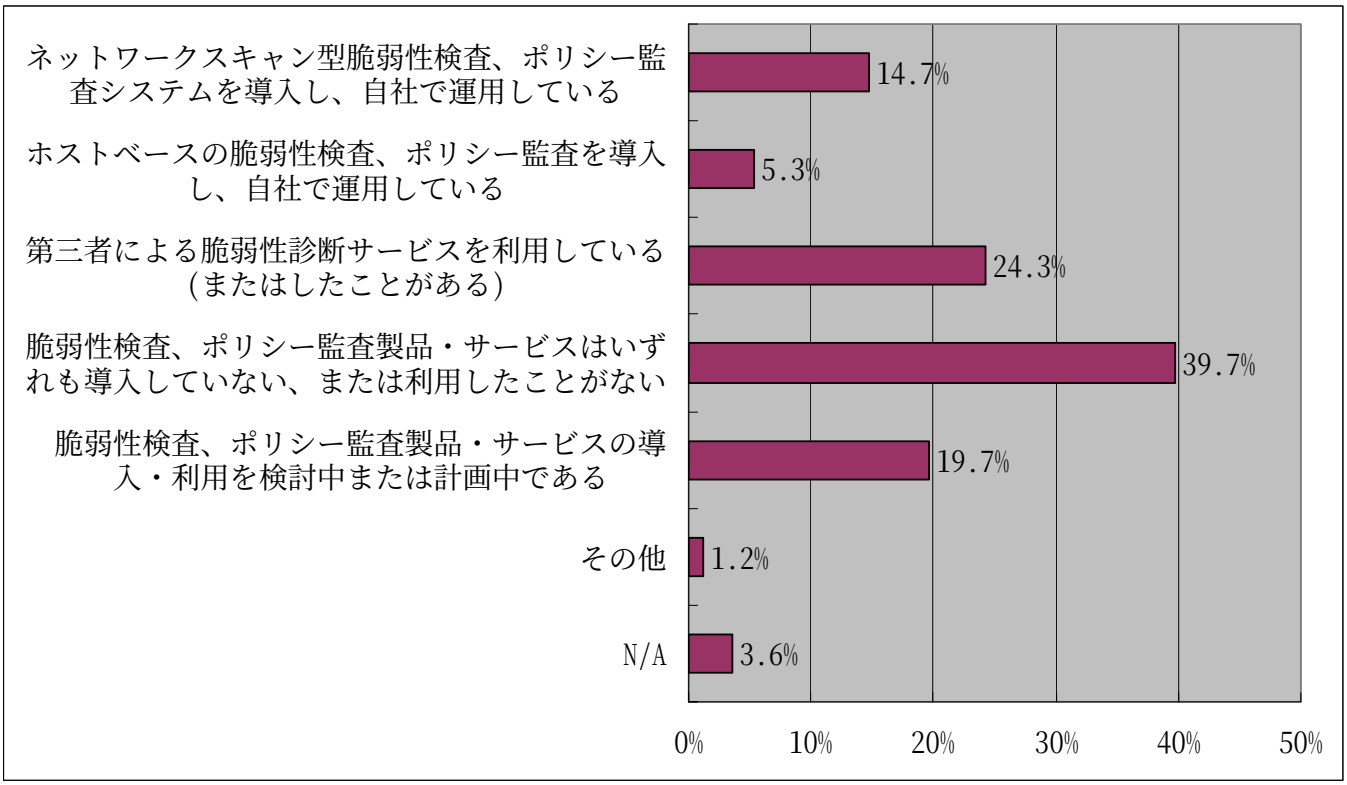
・７拠点中３拠点延べ４回のハードウェアトラブル発生。設置後一年以内の発生率としては高いと考える。
・RAS サーバーのメンテに工数がかかる上
・回線速度が遅い。
・リモート端末のセキュリティ状況が常に不安の種。
・運用・管理が面倒である。
・ID 単位の課金のため、利用 ID が増えればコスト増になる。
・RAS による認証方式の安全制が低い為、現在ＶＰＮへの切換えを検討中。
・ブラウザでの運用なので、ファイルサーバーへの対応が（ファイル共有）できていない
・IP-SEC・SSL-VPN 両方使っている。品質安定せず。（負荷がかかると安定しない）
・トラブル発生時の早期回復
・①IP-SEC　VNP はユーザーの負担が大きい。②RAS サーバーは電話回線経由なので速度が低い。
・製品の老巧化による相対的性能低下
・応答時間が遅い。回線費用が高価。
・バックボーンの容量・品質を向上して欲しい。
・不満というより不安感がある。
・PC と VPN ソフトの相性がある。
・運用上のセキュリティの不安がある。
・遅い
・ログ取得が弱い（アクセス記録など）
・リモートアクセス設定に専門技術が必要なので不満がある。
・価格が安価なサービスがどんどんでてきた。移行時期検討中。
・固有 port が使用不可。
・接続するクライアント環境の制約条件が多い。
・クライアントに暗号化ソフトをインストールする必要がある。FW 越えがデフォルトで不可。
・64Kbps までしか対応していない。
・サービス毎に対応した場合、費用増となる。
・回線速度が遅い
・高価格
・スループットが期待ほどでない。
・古いので最新のクライアント OS に対応していない
・障害対応が出来ていない。
・ベンダーの対応に不満。カード発行が遅れた。
・IC カードなどコストがかかる。
・ポリシーの変更と統一サービスの実現
・回復速度が遅い（ISDN）
・設定がややこしい。
・認証ステップが多く(ワンタイム認証)ユーザーに負荷をかけてしまう。
・通信速度が遅い。

K. 脆弱性検査、ポリシー監査（システム内部の設定に関するポリシー遵守チェックツール）システム

K-1. 脆弱性検査、ポリシー監査システムの導入状況について、当てはまるものはどれですか（複数回答可）

n=416

	ネットワークスキャン型脆弱性検査、ポリシー監査システムを導入し、自社で運用している	ホストベースの脆弱性検査、ポリシー監査を導入し、自社で運用している	第三者による脆弱性診断サービスを利用している(またはしたことがある)	脆弱性検査、ポリシー監査製品・サービスはいずれも導入していない、または利用したことがない	脆弱性検査、ポリシー監査製品・サービスの導入・利用を検討中または計画中である	その他	N/A	合計
回答数	61	22	101	165	82	5	15	451
占有率	14.7%	5.3%	24.3%	39.7%	19.7%	1.2%	3.6%	108.4%



Note

・脆弱性検査、ポリシー監査システムの導入状況については、「ネットワークスキャン型脆弱性検査、ポリシー監査システムを導入し、自社で運用している」が 14.7%、「ホストベースの脆弱性検査、ポリシー監査を導入し、自社で運用している」が 5.3%、「第三者による脆弱性診断サービスを利用している(またはしたことがある)」が 24.3%、「脆弱性検査、ポリシー監査製品・サービスはいずれも導入していない、または利用したことがない」が 39.7%、「脆弱性検査、ポリシー監査製品・サービスの導入・利用を検討中または計画中である」が 19.7%、「その他」が 1.2%となった。

・この設問では複数回答を可とした。占有率は回答票総数の n=416 を 100 とするパーセンテージで表示している。

○「その他」の自由記述内容（記入されたとおりに収録。順不同）

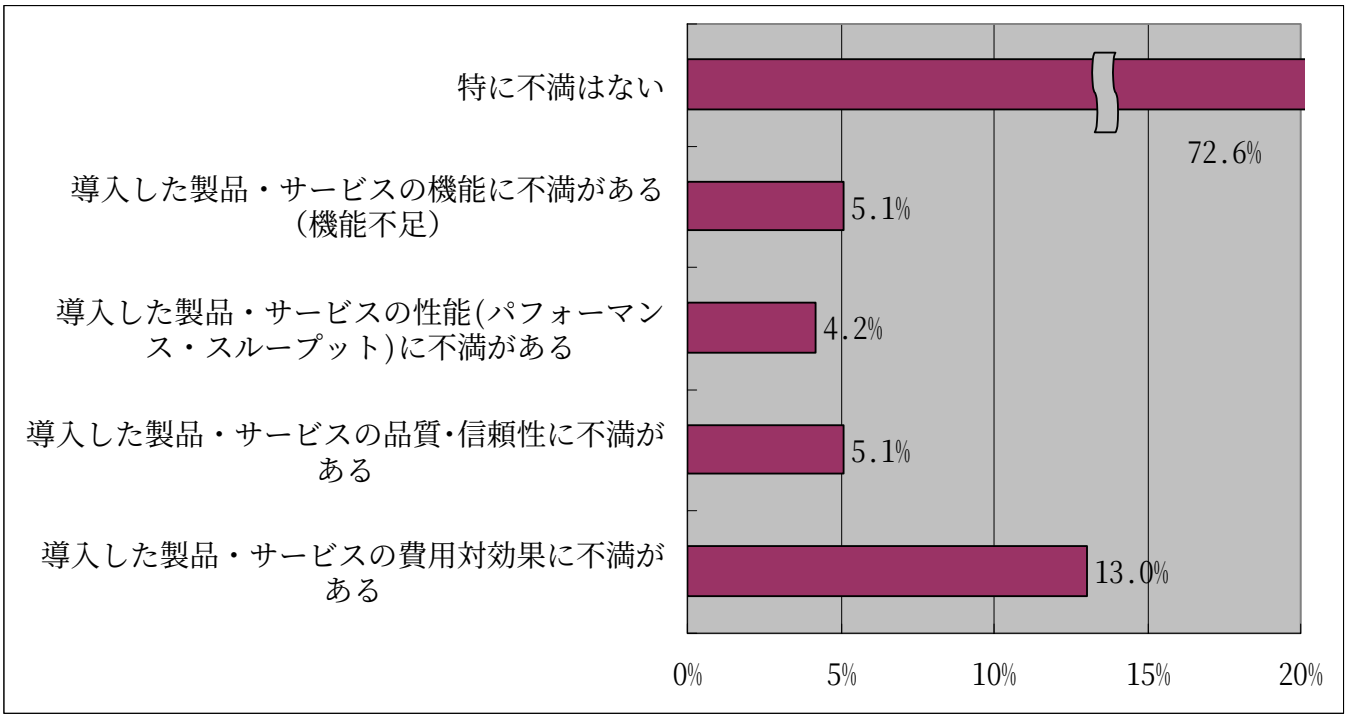
・インターネットサイトからの簡易診断は何回か実施。

・以前自社で実行

・未導入

K-2. 脆弱性検査、ポリシー監査の導入・運用上の不満・問題点について、次のうち当てはまるものはどれですか（複数回答可）

	特に不満はない	導入した製品・サービスの機能に不満がある（機能不足）	導入した製品・サービスの性能(パフォーマンス・スループット)に不満がある	導入した製品・サービスの品質・信頼性に不満がある	導入した製品・サービスの費用対効果に不満がある	合計
回答数	156	11	9	11	28	215
占有率	72.6%	5.1%	4.2%	5.1%	13.0%	100.0%



Note

・脆弱性検査、ポリシー監査の導入・運用上の不満・問題点については、「特に不満はない」が 72.6%、「導入した製品・サービスの機能に不満がある」が 5.1%、「導入した製品・サービスの性能（パフォーマンス・スループット）に不満がある」が 4.2%、「導入した製品・サービスの品質・信頼性に不満がある」が 5.1%、「導入した製品・サービスの費用対効果に不満がある」が 13.0%となった。
・無回答のものを除き、有効回答総数を 100%として占有率を算出した。

○不満がある場合の自由記述内容（記入されたとおりに収録。順不同）

・業者次第か？選定が難しいが必要。
・費用対効果の考え方
・AP をターゲットとした検査製品が少ない。AP をターゲットとした製品では、評価サーバーを立てなければならず、運用中のマシンを無停止で検査できない。
・的確な診断結果が少ない。
・広範囲に実施しようとすると高額になる。
・会社によってサービス内容に大差がある。どこのサービスを選ぶのが Best かがわからない。
・価格が高い
・運用工数がかかりすぎるし、専門知識がいる
・第３者の脆弱性検査を実施しているが、その検査実施が常に同じ条件下で行われず、検査結果に品質に問題がある。

・よく分かりません。
・サービス毎に対応した場合、費用増となる。
・テストから報告書が手元にくるまでやや時間がかかる。
・高価格
・脆弱性検査に関して、即効性が思ったよりも高くなく修正モジュールの適用等、検査後の対応に助言・アドバイスできる機能が欲しい。また、費用対効果の評価が難しいため、適切な投資が判断できていない。
・高い
・検査結果が解りづらい
・コストとマンパワーが必要。

第三部　デ ー タ 編
＜その２＞

アンケート質問票サンプル

ITセキュリティ対策施策の導入･実施状況とその満足度調査

２００４年　８　月

ＮＰＯ日本ネットワークセキュリティ協会

第一部　回答企業プロフィール

該当する項目にチェック（レ）をお願いします

１．業種

□a．製造・鉱業・建設業　□b．商業・流通業関連　□c．情報･ソフトウェア関連　□d．金融分野

□e．サービス業・その他

２．　年間売上規模

□a．50億円未満　□b．100億円未満　□c．1000億円未満　□d．5000億円未満　□e．5000億円以上

３．　従業員数

□a．100名未満　□b．500名未満　□c．1000名未満　□d．5000名未満　□e．5000名以上

４．　売上高に占める年間IT予算規模

□a．1%未満　□b．3%未満　□c．5%未満　□d．10%未満　□e．10%以上

５．IT予算の中のセキュリティ費用･投資の占める割合

□a．1%未満　□b．5%未満　□c．10%未満　□d．20%未満　□e．20%以上

６．　ご利用されているクライアントのOS　（複数回答可）

□a．Windows　□b．Linux　□c．Unix　□d．Mac OS　□e．その他

７．　ご利用されているサーバーのOS・システム　（複数回答可）

□a．Windows　□b．Linux　□c．Unix　□d．オフコン・ミニコン　□e．メインフレーム

□f．専用・組込み・その他

８．　ネットワークシステムの運用について

□a．自社運用　□b．ハードベンダに委託　□c．ソフト・ＳＩベンダに委託　□d．情報子会社・関連会社に委託

□e．その他

９．　情報セキュリティ対策体制について（複数回答可）

□a．専任部署がある　□b．非専任の担当部署がある　□c．専任の要員がいる　□d．兼任の要員がいる

□e．対策要員は特に定めていない

１０．　情報セキュリティ担当役員について（複数回答可）

□a．CISO（情報セキュリティ対策担当役員）がいる　□b．CSO（セキュリティ対策担当役員）がいる

□c．情報セキュリティはCIO（情報システム担当役員）の所管である

□d．情報セキュリティはCEO（最高経営責任者または社長）が直接所管している

□e．情報セキュリティ担当役員は特に定めていない

第二部　セキュリティ管理対策の実施状況と満足度

該当する項目にチェック（レ）をお願いします

Ａ．情報セキュリティポリシーの策定

Ａ－１．　情報セキュリティポリシーの策定状況について、当てはまるものはどれですか

□a．自社で策定済み □b．策定支援サービス・コンサルテーションを利用して策定済み

□c．自社で策定中・策定検討中　□d．策定支援サービス・コンサルテーションを利用して策定中・策定検討中

□e．策定の予定･計画はない

Ａ－２．　情報セキュリティポリシーの運用状況について、当てはまるものはどれですか

□a．自社で運用中　□b．策定支援サービス・コンサルテーションを利用して運用中

□c．情報セキュリティポリシーは策定・運用していない

Ａ－３．　情報セキュリティポリシーの見直しについて、当てはまるものはどれですか

□a．自社で定期的に見直し、更新している

□b．外部の支援サービス・コンサルを利用して定期的に見直し、更新している

□c．自社で随時または不定期に見直し、更新している

□d．外部の支援サービス・コンサルを利用して随時または不定期に見直し、更新している

□e．見直し･更新を資する予定または検討中である

□f．見直し･更新の予定はない　または　情報セキュリティポリシーを制定していない

Ａ－４．　情報セキュリティポリシー策定支援サービス・コンサルテーションを利用している場合、利用上の不満･問題点について、次のうち当てはまるものはどれですか（複数回答可）

□a．特に不満はない

□b．サービス業者・コンサルタントの内容・質に不満がある

□c．サービス業者・コンサルタントのコストに不満がある

※不満がある場合、その内容はどういうものですか。以下に記述下さい。

Ａ－５．外部のサービス業者、コンサルタントを利用している場合、それは次のどれに該当しますか（複数回答可）

□a．主としてコンサルティングサービスを提供する業者

□b．主として専門的セキュリティサービスを提供する業者

□c．主としてセキュリティ製品を販売する業者　□d．主としてネットワークサービスを提供する業者

□e．主としてシステムインテグレーションを提供する業者　□f．主として保守サービスを提供する業者

□g．いわゆる情報子会社

Ｂ．セキュリティ管理に関する公的認証（BS7799，ISO17799，ISMS,セキュリティ監査制度）の取得

Ｂ－１．　セキュリティ管理に関する公的認証の取得状況について、当てはまるものはどれですか

□a．自社だけの対応で取得済み

□b．取得支援サービス・コンサルテーションを利用して取得済み

□c．自社だけの力で取得取り組み中または検討中

□d．取得支援サービス・コンサルテーションを利用して取得するべく取り組み中または検討中

□e．セキュリティ管理に関する公的認証を取得する予定はない

Ｂ－２．　セキュリティ管理に関する公的認証の維持管理状況について、当てはまるものはどれですか

□a．自社独力で維持管理している

□b．公的認証の支援サービス・コンサルテーションを利用して維持管理している

□c．いわゆる情報子会社に委託して維持管理している

□d．公的認証は取得していない　または　維持管理について特に取り組みはしていない

Ｂ－３．　セキュリティ管理に関する公的認証の取得支援サービス・コンサルテーションを利用している場合、利用上の不満・問題点について、次のうち当てはまるものはどれですか（複数回答可）

□a．特に不満はない

□b．サービス業者・コンサルタントの内容・質に不満がある

□c．サービス業者・コンサルタントのコストに不満がある

※不満がある場合、その内容はどういうものですか。以下に記述下さい。

Ｂ－４．外部のサービス業者、コンサルタントを利用している場合、それは次のどれに該当しますか（複数回答可）

□a．主としてコンサルティングサービスを提供する業者

□b．主として専門的セキュリティサービスを提供する業者

□c．主としてセキュリティ製品を販売する業者

□d．主としてネットワークサービスを提供する業者

□e．主としてシステムインテグレーションを提供する業者

□f．主として保守サービスを提供する業者

□g．いわゆる情報子会社

C．プライバシーポリシー、個人情報保護管理基準等の策定

C－１．　プライバシーポリシー、個人情報保護管理基準等（以下、プライバシーポリシーと総称）の策定状況について、当てはまるものはどれですか

□a．自社で策定済み　□b．策定支援サービス・コンサルテーションを利用して策定済み

□c．自社で策定中・策定検討中　□d．策定支援サービス・コンサルテーションを利用して策定中・策定検討中

□e．策定の予定･計画はない

C－２．　プライバシーポリシーの運用状況について、当てはまるものはどれですか

□a．自社で運用中　□b．策定支援サービス・コンサルテーションを利用して運用中

□c．プライバシーポリシーは策定・運用していない

C－３．　プライバシーポリシーの見直しについて、当てはまるものはどれですか

□a．自社で定期的に見直し、更新している

□b．外部の支援サービス・コンサルを利用して定期的に見直し、更新している

□c．自社で随時または不定期に見直し、更新している

□d．外部の支援サービス・コンサルを利用して随時または不定期に見直し、更新している

□e．見直し･更新をする予定または検討中である

□f．見直し･更新の具体的予定はない

C－４．　プライバシーポリシー策定支援サービス･コンサルテーションを利用している場合､利用上の不満･問題点について、次のうち当てはまるものはどれですか（複数回答可）

□a．特に不満はない

□b．サービス業者・コンサルタントの内容・質に不満がある

□c．サービス業者・コンサルタントのコストに不満がある

※不満がある場合、その内容はどういうものですか。以下に記述下さい。

C－５．外部のサービス業者、コンサルタントを利用している場合、それは次のどれに該当しますか（複数回答可）

□a．主としてコンサルティングサービスを提供する業者

□b．主として専門的セキュリティサービスを提供する業者

□c．主としてセキュリティ製品を販売する業者　□d．主としてネットワークサービスを提供する業者

□e．主としてシステムインテグレーションを提供する業者　□f．主として保守サービスを提供する業者

□g．いわゆる情報子会社

D．プライバシーマークの取得

D－１．　プライバシーマークの取得状況について、当てはまるものはどれですか

□a．自社だけの対応で取得済み

□b．取得支援サービス・コンサルテーションを利用して取得済み

□c．自社だけの力で取得取り組み中または検討中

□d．取得支援サービス・コンサルテーションを利用して取得するべく取り組み中または検討中

□e．プライバシーマークを取得する予定はない

D－２．　プライバシーマークの維持管理状況について、当てはまるものはどれですか

□a．自社独力で維持管理している

□b．公的認証の支援サービス・コンサルテーションを利用して維持管理している

□c．いわゆる情報子会社に委託して維持管理している中

□d．プライバシーマークは取得していない　または　維持管理について特に取り組みはしていない

D－３．　プライバシーマークの取得支援サービス・コンサルテーションを利用している場合、利用上の不満・問題点について、次のうち当てはまるものはどれですか（複数回答可）

□a．特に不満はない

□b．サービス業者・コンサルタントの内容・質に不満がある

□c．サービス業者・コンサルタントのコストに不満がある

※不満がある場合、その内容はどういうものですか。以下に記述下さい。

D－４．外部のサービス業者、コンサルタントを利用している場合、それは次のどれに該当しますか（複数回答可）

□a．主としてコンサルティングサービスを提供する業者

□b．主として専門的セキュリティサービスを提供する業者

□c．主としてセキュリティ製品を販売する業者

□d．主としてネットワークサービスを提供する業者

□e．主としてシステムインテグレーションを提供する業者

□f．主として保守サービスを提供する業者

□g．いわゆる情報子会社

第三部　キュリティ対策製品の導入状況と満足度

ネットワークおよびそのセキュリティ対策の運用を、いわゆる情報子会社にアウトソースしている場合は、以下の設問はアウトソース先の情報子会社にご記入いただいても結構です。
その場合、当該アウトソース先の情報子会社と本体企業とを一体のものとして認識していただき、「自社」とある場合はアウトソース先の情報子会社または関連会社を含むものと読み替えてご回答下さい。

該当する項目にチェック（レ）をお願いします

［E］　ファイアウォール

Ｅ－１．　ファイアウォールの導入状況について、当てはまるものはどれですか　（複数回答可）

□a．アプライアンス型ファイアウォールを導入し、自社で運用している

□b．ソフトウェアベースのファイアウォールを導入し、自社で運用している

□c．第三者によるファイアウォール監視サービスを導入している

□d．ファイアウォール製品・サービスは導入していない

□e．ファイアウォール製品・サービスの導入･利用を検討中または計画中である

□f．その他〔　　〕

Ｅ－２．　ファイアウォールの導入・運用上の不満･問題点について、次のうち当てはまるものはどれですか（複数回答可）

□a．特に不満はない

□b．導入した製品・サービスの機能に不満がある。（機能不足）

□c．導入した製品･サービスの性能（パフォーマンス･スループット）に不満がある

□d．導入した製品・サービスの品質・信頼性に不満がある

□e．導入した製品・サービスの費用対効果に不満がある

不満がある場合、その内容はどういうものですか。以下に記述下さい。

［F］　侵入検知･防御システム（ＩＤＳ，ＩＤＰ，ＩＰＳ）

Ｆ－１．　侵入検知･防御システムの導入状況について、当てはまるものはどれですか　（複数回答可）

□a．アプライアンス型侵入検知･防御システムを導入し、自社で運用している

□b．ソフトウェアベースの侵入検知･防御システムを導入し、自社で運用している

□c．第三者による侵入検知･監視サービスを導入している

□d．侵入検知･防御システム製品・サービスは導入していない

□e．侵入検知･防御システム製品・サービスの導入･利用を検討中または計画中である

□f．その他〔　　〕

Ｆ－２．　侵入検知･防御システムの導入・運用上の不満･問題点について、次のうち当てはまるものはどれですか（複数回答可）

□a．特に不満はない

□b．導入した製品・サービスの機能に不満がある。（機能不足）

□c．導入した製品･サービスの性能（パフォーマンス･スループット）に不満がある

□d．導入した製品・サービスの品質・信頼性に不満がある

□e．導入した製品・サービスの費用対効果に不満がある

※不満がある場合、その内容はどういうものですか。以下に記述下さい。

［G］　アンチウイルス（ウイルス･ワーム対策）システム

Ｇ－１．　アンチウイルスシステムの導入状況について、当てはまるものはどれですか　（複数回答可）

□a．アプライアンス型のアンチウイルスシステムを導入し、自社で運用している

□b．ゲートウェイ型（ソフトベース）のアンチウイルスシステムを導入し、自社で運用している

□c．サーバー型（ソフトベース）のアンチウイルスシステムを導入し、自社で運用している

□d．クライアント型（ソフトベース）のアンチウイルスシステムを導入し、自社で運用している

□e．インターネット接続業者によるウイルスチェックサービスを利用している

□f．その他の第三者によるウイルスチェックサービスを導入している

□g．アンチウイルスシステム製品・ウイルスチェックサービスはいずれも導入していない

□h．アンチウイルスシステム製品・ウイルスチェックサービスの導入･利用を検討中または計画中である

□i．その他〔　　〕

Ｇ－２．　ウイルスチェックシステムの導入・運用上の不満･問題点について、次のうち当てはまるものはどれですか

（複数回答可）

□a．特に不満はない

□b．導入した製品・サービスの機能に不満がある。（機能不足）

□c．導入した製品･サービスの性能（パフォーマンス･スループット）に不満がある

□d．導入した製品・サービスの品質・信頼性に不満がある

□e．導入した製品・サービスの費用対効果に不満がある

※不満がある場合、その内容はどういうものですか。以下に記述下さい。

［H］　アンチウイルス以外のコンテンツセキュリティ対策（アンチスパム、ＵＲＬフィルタリング、メールフィルタリング）

Ｈ－１．　アンチウイルス以外のコンテンツセキュリティ対策の導入状況について、当てはまるものはどれですか

（複数回答可）

□a．ゲートウェイ型／サーバー型のコンテンツセキュリティ対策を導入し、自社で運用している

□b．クライアント型のコンテンツセキュリティ対策を導入し、自社で運用している

□c．インターネット接続業者によるコンテンツセキュリティ対策サービスを利用している

□d．その他の第三者によるコンテンツセキュリティ対策サービスを導入している

□e．コンテンツセキュリティ対策製品・サービスはいずれも導入していない

□f．コンテンツセキュリティ対策製品・サービスの導入･利用を検討中または計画中である

□g．その他〔　　〕

Ｈ－２．　コンテンツセキュリティ対策の導入・運用上の不満･問題点について、次のうち当てはまるものはどれですか

（複数回答可）

□a．特に不満はない

□b．導入した製品・サービスの機能に不満がある。（機能不足）

□c．導入した製品･サービスの性能（パフォーマンス･スループット）に不満がある

□d．導入した製品・サービスの品質・信頼性に不満がある

□e．導入した製品・サービスの費用対効果に不満がある

※不満がある場合、その内容はどういうものですか。以下に記述下さい。

［I］　システムへのログオンに際しての個人（本人）認証及びユーザーID管理

Ｉ－１．　個人認証システム及びユーザーID管理の導入状況について、当てはまるものはどれですか　（複数回答可）

□a．ＩＤと固定パスワードの入力により本人確認している

□b．ＩＣカード、ＵＳＢトークン等の個人保有の物理キー型対策を導入し、自社で運用している

□c．ワンタイムパスワードを導入し、自社で運用している

□d．バイオメトリックス方式の個人認証システムを導入し、自社で運用している

□e．電子認証サービス（ＰＫＩ）を導入し、自社で運用している

□f．NTドメイン、または、アクティブディレクトリを全社的に導入し自社で運用している

□g．NISまたはNIS＋を全社的に導入し自社で運用している

□h．ディレクトリ管理サービスを全社的に導入し自社で運用している

□i．その他のユーザーID管理システムを全社的に導入し自社で運用している

□j．専門サービス業者による電子認証サービス（ＰＫＩ）を利用している

□k．第三者による電子認証サービス（ＰＫＩ）以外の個人認証サービスを導入している

□l．個人認証製品・サービスはいずれも導入していない

□m．ユーザーID管理システム・サービスはいずれも導入していない

□n．個人認証製品・サービスの導入･利用を検討中または計画中である

□o．ユーザーID管理システム・サービスの導入･利用を検討中または計画中である

□p．その他〔　　〕

Ｉ－２．　個人認証システム、及びユーザーID管理システムの導入・運用上の不満･問題点について、次のうち当てはまるものはどれですか（複数回答可）

□a．特に不満はない

□b．導入した製品・サービスの機能に不満がある（機能不足）

□c．導入した製品･サービスの性能（パフォーマンス･スループット）に不満がある

□d．導入した製品・サービスの品質・信頼性に不満がある

□e．導入した製品・サービスの費用対効果に不満がある

□f．各個人の使い方、管理の面で不満、不安がある

※不満や不安がある場合、その内容はどういうものですか。以下に記述下さい。

［J］　リモートアクセスの通信安全対策システム

Ｊ－１．　リモートアクセスの通信安全対策の導入状況について、当てはまるものはどれですか　（複数回答可）

□a．ＲＡＳサーバーにおける個人認証を導入し、自社で運用している

□b．ＩＰ－ＳＥＣ方式のＶＰＮシステムを導入し、自社で運用している

□c．ＳＳＬ－ＶＰＮ方式のＶＰＮシステムを導入し、自社で運用している

□d．リバースプロキ方式を導入し、自社で運用している

□e．第三者によるＶＰＮサービスを導入している

□f．リモートアクセスの通信安全対策製品・サービスはいずれも導入していない

□g．リモートアクセスの通信安全対策製品・サービスの導入･利用を検討中または計画中である

□h．その他〔　　〕

Ｊ－２．　リモートアクセスの通信安全対策の導入・運用上の不満･問題点について、次のうち当てはまるものはどれですか（複数回答可）

□a．特に不満はない

□b．導入した製品・サービスの機能に不満がある。（機能不足）

□c．導入した製品･サービスの性能（パフォーマンス･スループット）に不満がある

□d．導入した製品・サービスの品質・信頼性に不満がある

□e．導入した製品・サービスの費用対効果に不満がある

※不満がある場合、その内容はどういうものですか。以下に記述下さい。

［K］　脆弱性検査、ポリシー監査（システム内部の設定に関するポリシー遵守チェックツール）システム

Ｋ－１．　脆弱性検査、ポリシー監査システムの導入状況について、当てはまるものはどれですか　（複数回答可）

□a．ネットワークスキャン型脆弱性検査、ポリシー監査システムを導入し、自社で運用している

□b．ホストベースの脆弱性検査、ポリシー監査を導入し、自社で運用している

□c．第三者による脆弱性診断サービスを利用している（またはしたことがある）

□d．脆弱性検査、ポリシー監査製品・サービスはいずれも導入していない、または利用したことがない

□e．脆弱性検査、ポリシー監査製品・サービスの導入･利用を検討中または計画中である

□f．その他〔　　〕

Ｋ－２．　脆弱性検査、ポリシー監査の導入・運用上の不満･問題点について、次のうち当てはまるものはどれですか（複数回答可）

□a．特に不満はない

□b．導入した製品・サービスの機能に不満がある。（機能不足）

□c．導入した製品･サービスの性能（パフォーマンス･スループット）に不満がある

□d．導入した製品・サービスの品質・信頼性に不満がある

□e．導入した製品・サービスの費用対効果に不満がある

※不満がある場合、その内容はどういうものですか。以下に記述下さい。

質問は以上です。ご協力ありがとうございました。

ご回答いただいた内容は、全て統計処理をした結果のみを公表し、個別企業・団体やご回答者様と特定の回答内容が対応付けられて認識される形では一切外部に伝達されることはありませんのでご安心下さい。

ご回答いただいた方には、JNSAで有償配布しておりますセキュリティ対策講座「ネットワーク社会のここが危ない！！」の冊子付ＣＤ－ＲＯＭを差し上げます。ご希望の方は、下記にお届け先・ご連絡先をご記入下さい。
また、メールアドレスをご記入いただければ、アンケート調査結果公開時には、その旨ご連絡差し上げます。（メールアドレスのみのご記入でも結構です。）

ご住所：　〒
会社名
部署・役職名
ご芳名
電話
fax
e-mailアドレス

平成 17 年 1 月発行
発行：特定非営利活動法人
日本ネットワークセキュリティ協会

東京都江東区新砂 1-6-35
T.T.ランディック東陽町ビル１Ｆ
Tel:03-5633-6061
E-mail: sec@jnsa.org
http://www.jnsa.org/