

情報セキュリティ関連被害等の状況調査票

独立行政法人 情報処理推進機構
セキュリティセンター

ご記入にあたってのお願い

貴企業または貴自治体の「情報セキュリティの管理者(責任者・担当者)の方」がご回答ください。
貴方がそれ以外の方の場合は、お手数ですが、該当者にお渡しくださいますようお願い申し上げます。

情報処理推進機構セキュリティセンターでは、国内の企業における「情報セキュリティに関する被害状況を捉える」ことを目的としたアンケートを実施しております。今回の調査結果は、2008年4月頃、情報処理推進機構セキュリティセンターのホームページにて公開する予定です。ご回答の内容については、すべて統計数値として集計いたしますので、会社名や個人名などが公表されることは一切ございません。

この調査の実施、取り纏めにつきましては、株式会社三菱総合研究所に委託しております。

お答えは、特に説明のないかぎり、あてはまる項目をお選びになって、該当する番号に をおつけください。
また、お答えが「その他()」にあてはまる場合は、お手数ですが()にその内容を具体的にご記入ください。

お答えいただいた内容により、次の設問への進み先が異なる場合がありますので、ご注意ください。

自治体の方の場合は、設問の企業を自治体と読み替えてご回答ください。

ご記入いただいた用紙は、同封の返信用封筒(切手不要)に入れ、平成20年1月25日(金)までにご投函くださいますようお願い申し上げます。

このアンケートについてご不明な点がございましたら、下記までお問合せください。

情報処理推進機構(IPA)について

独立行政法人 情報処理推進機構(IPA)は、経済産業省の告示に基づき、コンピュータウイルス、不正アクセスおよび脆弱性情報に関する発見・被害の届出を受け付け、それを元に被害の拡大・再発の防止、情報セキュリティ対策などの普及啓発を行っています。

URL: <http://www.ipa.go.jp/security/>



【調査主旨に関するお問合せ先】
独立行政法人 情報処理推進機構
セキュリティセンター
担当: 花村、木邑
電話: 03-5978-7527
E-mail: isec-survey@ipa.go.jp

【調査実施に関するお問合せ先】
株式会社三菱総合研究所
情報セキュリティ研究グループ
担当: 井上、川口
電話: 03-3277-0749
E-mail: incident-07@mri.co.jp

* 三菱総合研究所はプライバシーマーク取得企業です

この調査は、企業・団体の単位でお答えください

貴企業(当該企業・当該自治体)についてお伺いします。

問1 貴企業の主な業種をお答えください。(は1つ)

- | | | |
|------------|-----------------|------------|
| 1 農林漁業・鉱業 | 2 建設業 | 3 機械器具製造業 |
| 4 他の製造業 | 5 電気・ガス・熱供給・水道業 | 6 情報通信業 |
| 7 運輸業 | 8 卸売業 | 9 小売業 |
| 10 金融・保険業 | 11 不動産業 | 12 飲食店、宿泊業 |
| 13 他のサービス業 | 14 自治体・公共団体 | 15 その他 () |

問2 貴企業の総従業員数(有給役員、正社員・正職員、準社員・準職員、アルバイト等を含む)をお答えください。

十万	万	千	百	十	一

人

常時従業員の総数。有給役員及び常時雇用者(正社員・正職員、準社員・準職員、アルバイト等、1ヶ月を超える雇用契約者)とし、人材派遣業者からの派遣従業員は含めません。

問3 貴企業の直近年度の総売上高(単体)をお答えください。(自治体の方は問5へ)

兆	千億	百億	十億	億	千万	百万

百万円

学校、組合団体など営業活動を行わない組織の場合は、当該年度における収入高とします。

問4 貴企業の直近年度の経常利益(単体)をお答えください。

兆	千億	百億	十億	億	千万	百万

百万円

マイナスの場合は先頭に をお付けください。

問5 貴企業の規定年間営業日数および1日の営業時間をお答えください。

年間営業日数 _____日/年 1日あたり営業時間 _____時間/日

問6 貴企業のIT関連の支出総額について、昨年1年間(2007年1月～12月)にかけた費用を、概算でお答えください。

兆	千億	百億	十億	億	千万	百万

百万円

問7 貴企業で利用されているクライアント(パソコン)の台数をご記入ください。

Windows系 約 _____台 Macintosh系 約 _____台 Unix・Linux系 約 _____台

問8 貴企業におけるLANやWAN等のネットワークの構築状況は、下記のどれに該当しますか。(は1つ)

- 1 事業所内ネットワーク(LAN)のみ構築
- 2 事業所内だけではなく、組織内の事業所間ネットワーク(WAN:本社と支社・工場間等)まで構築
- 3 組織内だけではなく、外部とのネットワーク(例:サプライチェーン)まで構築
- 4 社内情報ネットワークは構築していない

貴企業における情報セキュリティ対策についてお伺いします。

問9 貴企業では、情報セキュリティ対策の管理を組織的に行っていますか。(は1つ)

- 1 専門部署(担当者)がある
- 2 兼務だが担当責任者が任命されている
- 3 外部委託している
- 4 組織的には行っていない(各自の対応)
- 5 わからない

問10 貴企業における情報セキュリティ対策の導入状況について伺います。

各対策の導入状況について該当する番号に をご記入ください。(は1行につき1つ)

	9割以上に 導入済	半数に 導入済	半数未満に 導入済	導入して いない
各自のクライアント(パソコン)への導入				
a. ウイルス対策ソフト	1	2	3	4
b. スパイウェア (*1) 対策ソフト	1	2	3	4
c. パーソナルファイアウォール	1	2	3	4
d. スпамメール対策 (メーラー付属機能あるいは専用ソフト)	1	2	3	4
e. P2Pソフトウェア等のインストール状況チェック	1	2	3	4
ネットワークサーバ(メールサーバ、Webサーバなど)への導入				
f. ウイルス対策ソフト	1	2	3	4
g. スパイウェア対策ソフト	1	2	3	4
h. スпамメール対策ソフト	1	2	3	4
ローカルサーバ(ファイルサーバ、プリントサーバなど)への導入				
i. ウイルス対策ソフト	1	2	3	4
j. スパイウェア対策ソフト	1	2	3	4
その他				
k. ファイアウォール	1	2	3	4
l. IDS/IPS (*2) による侵入検知	1	2	3	4
m. プロバイダによるウイルスチェックサービス	1	2	3	4

(*1) スパイウェアとは、利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等のことを指します。

(*2) IDSとは、ネットワーク上などへの不正なアクセスの兆候を検知し、ネットワーク管理者に通報する機能のことです。
IPSとは、異常を通知するだけでなく、通信遮断などのネットワーク防御を自動で行う機能のことです。

問11 問10に挙げたセキュリティ対策ソフトの導入・更新および装置の導入について、昨年1年間(2007年1月~12月)にかけた費用(*3)を、概算でお答えください。

_____ 万円 / 年 (購入・更新なしなら「0」と記入)

(*3) セキュリティ対策用のソフトウェアのバージョンアップやパターンファイル更新、ファイアウォール等のハードウェアの購入費用を指します。導入や更新にかかる人件費は含めないでください。

11-1 来年1年間(2008年)のセキュリティ対策への投資額はどのように想定されていますか。(は1つ)

- 1 2007年よりも増額する
- 2 2007年と同程度
- 3 2007年よりも減額する

問12 問 10に挙げた以外には、どのような情報セキュリティ関連製品やソリューションを導入していますか。導入済みのものの番号に をご記入ください。(はいくつでも)

- | | | |
|-----------------|------------------|----------------------------|
| 1 ウェブ閲覧のフィルタリング | 2 顧客情報等の暗号化 | 3 ISO/IEC15408 (*4) 認証取得製品 |
| 4 VPN | 5 検疫ネットワーク (*5) | 6 シンククライアント (*6) |
| 7 電子署名 | 8 生体認証(バイオメトリクス) | |
| 9 その他 () | | 10 特にない |

(*4) 情報セキュリティの観点から IT 製品およびシステムの設計と実装に関して評価を行うための基準(国際標準)。

(*5) 検疫ネットワークとは、持ち込むパソコンを社内 LAN に接続する際に、いったん別のネットワークに繋いでウイルスの検査等を行い、接続が許可されたパソコンであることを確認するシステムのことを指します。

(*6) シンククライアントとは、処理をサーバ側に集中させ、クライアントで必要最小限の処理のみを行うシステムを指します。ここではファイルの保存をサーバのみで行う場合も含めてください。

問13 情報セキュリティ関連被害を防止するために、どのような組織面・運用面の対策を実施していますか。実施している対策の番号に をご記入ください。(はいくつでも)

- | | |
|-------------------------|------------------------|
| 1 モバイル機器に関するセキュリティ強化 | 2 無線 LAN に関するセキュリティ強化 |
| 3 機器や記録媒体の持ち込み・持出しの制限 | 4 ID/パスワード、アクセス権限管理の強化 |
| 5 ログの取得・保存 | 6 入退出管理の強化 |
| 7 専門家によるセキュリティ監視サービスの導入 | 8 ハードディスク等の廃棄時の破壊 |
| 9 事業継続計画の策定 | 10 重要なシステム・データのバックアップ |
| 11 その他 () | 12 特にない |

問14 貴企業では、Microsoft Update などの手段でセキュリティパッチ(脆弱性の修正)を適用していますか。最も近いものに をご記入ください。(は各1つ)

a. クライアント(パソコン)

- | | | |
|---------------------|----------------------------|---------|
| 1 常に適用し、適用状況も把握している | 2 常に適用する方針・設定だが、実際の適用状況は不明 | |
| 3 各ユーザに適用を任せている | 4 ほとんど適用していない | 5 分からない |

b. 外部に公開しているネットワークサーバ(メールサーバ、Webサーバなど)

- | | | |
|---------------------|-----------------------------|---------|
| 1 ほぼ全サーバに計画的に適用している | 2 一部のサーバには計画的に適用、他は気がついたら適用 | |
| 3 気がついたときに適用 | 4 ほとんど適用していない | 5 分からない |

c. 内部で利用しているローカルサーバ(ファイルサーバ、プリントサーバなど)

- | | | |
|---------------------|-----------------------------|---------|
| 1 ほぼ全サーバに計画的に適用している | 2 一部のサーバには計画的に適用、他は気がついたら適用 | |
| 3 気がついたときに適用 | 4 ほとんど適用していない | 5 分からない |

問15 セキュリティパッチを適用しなかった理由について、もっともよく当てはまるものに をご記入ください。(はひとつ)

- 1 既存のシステム/サービスの動作を重視し、パッチの適用により生じる悪影響や改修作業を避けた
- 2 パッチ以外の手段によってセキュリティ上の脅威は回避できた
- 3 対象の脆弱性は大きな脅威ではなく、パッチの適用は不要と判断した
- 4 パッチの評価や適用に多大なコストがかかるので見合わせた
- 5 その他 ()
- 6 特に理由はない

問16 貴企業で現在使用しているパソコンのうち、Windows 98 / Me がインストールされているものはどれくらいの割合ですか。最も近いものにご記入ください。(は1つ)

- | | | | | | | | |
|---|-----|----|-----|----|------|---|-----|
| 1 | 0% | 2 | 10% | 3 | 20% | 4 | 30% |
| 5 | 40% | 6 | 50% | 7 | 60% | 8 | 70% |
| 9 | 80% | 10 | 90% | 11 | 100% | | |

問17 貴企業では、役職員等に対し、情報セキュリティ対策に関する教育をどのようにされていますか。役職ごとに該当する教育手法の番号にご記入ください。(はいくつでも)

	eラーニング(*7)	講習会やセミナーの実施・参加	関連情報の周知	特に実施していない
a. 役員(経営トップを含む)	1	2	3	4
b. 正社員・正職員	1	2	3	4
c. 準社員・準職員・アルバイト	1	2	3	4

(*7) eラーニングとは、パソコン、携帯端末等を使い、ネットワークやCD-ROMで教材を配信し、受講状況や成績の管理を伴う学習を想定しています。

その他の手法で教育を実施されている場合は、具体的にご記入ください

問18 現在、情報セキュリティ対策に関連して知りたいと思っている情報として、該当するものを下記よりすべてお選びください。(はいくつでも)

- | | |
|------------------------------|---------------------------------|
| 1 ウイルス感染時の復旧方法、感染を防ぐ方法 | 2 新種ウイルス、要注意ウイルスの警戒情報 |
| 3 不正アクセスを受けた際の対処方法 | 4 情報漏えいが発生した場合の対処方法 |
| 5 他社における各種情報セキュリティ対策の導入状況 | 6 情報セキュリティ対策の導入・運用に関する基準やガイドライン |
| 7 委託先のセキュリティ対策実施状況に関するチェック事項 | 8 情報セキュリティ対策を外部委託する際のチェック事項 |
| 9 情報セキュリティに関わる試験、検定情報 | 10 国内・海外の情報セキュリティ被害の状況 |
| 11 その他() | 12 特にない |

問19 経済産業省告示の「コンピュータウイルス対策基準」をご存知ですか。(は1つ)

- | | | | |
|-------------|------------|------------|--------|
| 1 内容を理解している | 2 読んだことがある | 3 存在は知っている | 4 知らない |
|-------------|------------|------------|--------|

問20 コンピュータウイルス被害の拡大と再発防止のために、情報処理推進機構(IPA)がウイルスに関する届出を受け付ける指定機関になっていることをご存知ですか。(は1つ)

- | | |
|---------|--------|
| 1 知っている | 2 知らない |
|---------|--------|

問21 今後感染が発見されたとき、情報処理推進機構(IPA)に届出を行いますか。(は1つ)

- | | |
|----------------------------|------------------|
| 1 届出を行う | |
| 2 届出を行わない -> その理由(はいくつでも) | |
| a 届出に手間がかかる | b 届出方法が不明なため |
| c 届出る時間がないため | d 自分で修復できるため |
| e 被害が大きければ届出する | f 社内規定による届出で済ませる |
| g その他() | |

・ **コンピュータウイルス(*8) の発見と感染被害に関してお伺いします。**

(*8) コンピュータウイルスとは、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能の3つの機能のうち、ひとつ以上を有するものです。

問22 貴企業では、昨年1年間(2007年1月～12月)に、コンピュータウイルスに感染したこと、または感染には至らないが発見したことがありますか。一度でもあればお答えください。(は1つ)

*** 傘下事業所(支社・支店・出張所等)も含めてご回答ください。**

- 1 ウイルスには感染も発見もしなかった . **問 40 にお進みください**
- 2 ウイルスを発見したが、感染には至らなかった
- 3 ウイルスに感染した

問23 感染または発見したウイルスの具体的な名称として、該当するものを下記よりすべてお選びください。(感染したものには、発見のみは をつけてください)

- | | |
|----------------|---------------|
| 1 W32/Netsky | 2 W32/Bagle |
| 3 W32/Mytob | 4 W32/Mydoom |
| 5 W32/Stration | 6 W32/Mywife |
| 7 W32/Sality | 8 W32/Klez |
| 9 W32/Lovgate | 10 W32/Mimail |
| 11 W32/Looked | 12 その他(名称:) |
| 13 不明 | |

問 22 で2と答えた方は、 . 問 40 へお進みください。

問 22 で3と答えた方は、引き続き 問 24 へお進みください。

【 問 22 で「3 ウイルスに感染した」と回答した方に伺います。 】

問24 昨年 1 年間(2007 年 1 月～12 月)のコンピュータウイルスへの感染件数をお答えください。
同時期に報告された同種・同感染元と想定される場合をまとめて 1 件と数えます。

_____ 件 / 年 (感染なしなら「0」と記入)

問25 ウイルスに感染したクライアント(パソコン)、サーバの台数は年間延べ何台ですか、それぞれに該当する台数をひとつずつ選び番号に をご記入ください。(は各 1 つ)

	0 台	1～4 台	5～9 台	10～19 台	20～49 台	50～99 台	100 台以上
a. クライアント(パソコン)	1	2	3	4	5	6	7
b. サーバ	1	2	3	4	5	6	7

問26 ウイルスに感染した影響で生じた直接的な被害の有無についてお答えください。(はいいくつでも)

- | | | |
|-------------|---------------|---------------|
| 1 情報破壊 | 2 情報流出 | 3 ウイルスメール等の発信 |
| 4 ネットワークの遅延 | 5 システム停止・性能低下 | 6 パソコン単体の停止 |
| 7 関連部門の業務停滞 | 8 個人の業務停滞 | 9 取引先への感染拡大 |
| 10 その他() | 11 特になし | |

問27 電子商取引(EC)業務(*9)を行っている方にお聞きします。

貴企業において、電子商取引(EC)業務の売上が、全体の売上に占める割合をお答えください。(は 1 つ)

*傘下事業所(支社・支店・出張所等)も含めてご回答ください。

- | | | | |
|-------|--------|---------|-------|
| 1 0% | 2 10% | 3 20% | 4 30% |
| 5 40% | 6 50% | 7 60% | 8 70% |
| 9 80% | 10 90% | 11 100% | |

(*9) ここでは EC 業務として、物流(物流手配、出荷、輸送管理)、顧客から対価を受取るサービスの提供、販売(見積・商談、販売計画、販売促進、受注管理、顧客情報管理、請求、決済)、金融分野における決済代行、振込・送金、預金獲得、融資、保険契約 等の、売上げに直結する業務を想定します。

問28 電子商取引(EC)業務を行っている方にお聞きします。

ウイルスに感染した影響によって、電子商取引(EC)業務が停止した期間は年間延べ何日ですか。(は 1 つ)

- | | | |
|---------|----------|--------------|
| 1 0 日 | 2 1 日以内 | 3 2～3 日 |
| 4 4～5 日 | 5 6～10 日 | 6 11日以上 (日) |

問29 ウイルスに感染した影響によって、EC 関連以外の業務遂行上重要なサーバ(メールサーバ、ウェブサーバ、DNS サーバ等)が停止した期間は年間延べ何日ですか。(は 1 つ)

* 傘下事業所(支社・支店・出張所等)も含めてご回答ください。

1 0 日	2 1 日以内	3 2～3 日
4 4～5 日	5 6～10 日	6 11日以上 (日)

↓
問 29-1 その期間中の売上高への影響はどの程度だったと思われますか。(は 1 つ)

(自治体の方は回答せずに 問 30 へお進みください)

- | | | |
|--------|---------|--------|
| 1 0%減 | 2 5%減 | 3 10%減 |
| 4 20%減 | 5 40%減 | 6 60%減 |
| 7 80%減 | 8 100%減 | |

問30 昨年1年間(2007年1月～12月)に、情報管理部門が行ったウイルス感染からの復旧作業(*10)は年間延べ何人・日ですか。(は1つ)

- | | | |
|--------------------------|------------|------------|
| 1 0人・日 | 2 1人・日以内 | 3 2～3人・日 |
| 4 4～5人・日 | 5 6～10人・日 | 6 11～15人・日 |
| 7 16～20人・日 | 8 21～25人・日 | 9 26～30人・日 |
| 10 31人・日以上 (人・日) | | |

(*10) ここでは、ウイルス感染を確認後に、駆除や再インストール等を行い、システムを停止状態から稼働状態に戻して、システム機能を回復させるまでの作業を指します。

問31 昨年1年間(2007年1月～12月)に、システム復旧に関して新たに購入した代替機器の費用(*11)をお答えください。(は1つ)

- | | |
|------------------|---------------|
| 1 0円 | 2 10万円未満 |
| 3 10～30万円未満 | 4 30～50万円未満 |
| 5 50～70万円未満 | 6 70～100万円未満 |
| 7 100～200万円未満 | 8 200～300万円未満 |
| 9 <u>300万円以上</u> | |

→ 具体的にご記入ください

_____万円 / 年

(*11) 一時的に利用するために事後に購入したハードウェアやソフトウェアの費用のみを指します。
恒久的な対策強化を目的に購入した機器の費用は含めないでください。

問32 昨年1年間(2007年1月～12月)に、システム復旧に関し外部に発注した業務の費用をお答えください。(は1つ)

- | | |
|------------------|---------------|
| 1 0円 | 2 10万円未満 |
| 3 10～30万円未満 | 4 30～50万円未満 |
| 5 50～70万円未満 | 6 70～100万円未満 |
| 7 100～200万円未満 | 8 200～300万円未満 |
| 9 <u>300万円以上</u> | |

→ 具体的にご記入ください

_____万円 / 年

問33 昨年1年間(2007年1月～12月)に、ウイルス感染が原因で、業務部門が行った追加のデータ処理作業(*12)は年間延べ何人・日ですか。(は1つ)

- | | | |
|-------------------------|-----------|------------|
| 1 0人・日 | 2 1人・日以内 | 3 2～3人・日 |
| 4 4～5人・日 | 5 6～10人・日 | 6 11～15人・日 |
| 7 16人・日以上 (人・日) | | |

(*12) ここでは、消失したデータの再登録や、一時的に手作業等で作成したデータのシステムへの登録などの作業を指します。

問34 昨年1年間(2007年1月～12月)に、ウイルス感染時の対応として実施した内容について該当する番号に をご記入ください。また、社内で発生したおおよその作業規模をお答えください。(はいくつでも)

a. 原因追求・影響範囲特定のための外部調査	対応の有無	社内で発生した作業の規模	
b. 問合せ窓口の設置	1	約	人・日
c. 電話郵送等での取引先・顧客等への謝罪	2	約	人・日
d. 謝罪広告の出稿	3	約	人・日
e. 社内に配布する対策用CD-ROMの作成	4	約	人・日
f. その他 ()	5	約	人・日
g. 特に実施していない	6	約	人・日
	7		

問35 昨年1年間(2007年1月～12月)に、ウイルス感染時の対応として実施した問34の実施内容のうち、外部に発注した業務(原因・被害範囲の調査、システムや情報の復旧、対策の見直し作業等)の費用をお答えください。(実施していないなら「0円」を選択、 は1つ)

- | | | |
|---------------|---------------|----------------|
| 1 0円 | 2 10万円未満 | 3 10～100万円未満 |
| 4 100～300万円未満 | 5 300～500万円未満 | 6 500～1000万円未満 |
| 7 1000万円以上 | | |

具体的にご記入ください

_____万円 / 年

【 以後の設問は、影響が最も大きかったウイルスについてお答えください。 】

問36 貴企業において、昨年1年間(2007年1月～12月)に感染または発見したコンピュータウイルスのうち影響が最も大きかったウイルスの名称と発見時期をご記入ください。

ウイルス名 _____ 発見日 2007年 _____ 月 _____

問37 コンピュータウイルスを発見した経緯について、該当するものを下記よりすべてお選びください。

(はいくつでも)

- | | |
|------------------------|---------------|
| 1 クライアント対策ソフト | 2 ゲートウェイ対策ソフト |
| 3 プロバイダのチェッカーサービス | 4 ファイアウォール |
| 5 IDS、IPS (*13)による侵入検知 | 6 目視による |
| 7 外部からの連絡 | 8 その他() |

(*13) IDS とは、ネットワーク上などへの不正なアクセスの兆候を検知し、ネットワーク管理者に通報する機能のことです。
IPS とは、異常を通知するだけでなく、通信遮断などのネットワーク防御を自動で行う機能のことです。

問38 想定されるコンピュータウイルスの感染経路は、下記のどれに該当しますか。(は1つ)

- | | |
|-------------------------|---------------------------------|
| 1 電子メール | 2 インターネット接続 (ホームページ閲覧など) |
| 3 自らダウンロードしたファイル | 4 P2P(Peer to Peer)などのファイル共有ソフト |
| 5 外部媒体、持ち込みクライアント(パソコン) | 6 その他 () |
| 7 不明 | |

問39 コンピュータウイルスに感染したクライアント(パソコン)の台数をご記入ください。(感染なしなら「0」と記入)

Windows系 約 _____ 台 Macintosh系 約 _____ 台 Unix・Linux系 約 _____ 台

【 全員の方に伺います。 】

・ Winny などのファイル共有ソフトを介した情報漏えいについて伺います。

問40 貴企業では、昨年1年間(2007年1月～12月)に、Winny などファイル共有ソフトのウイルス感染による個人情報、業務情報の流出により被害を受けた経験がありますか。(は1つ)

1 被害経験がある

2 被害経験はない

被害経験がある場合は、被害内容、対策状況をご記入ください。

→ 流出した情報の内容は何ですか。(はいくつでも)

1 顧客(個人)情報

2 顧客(企業)情報

3 社内の業務情報

4 その他 ()

→ 対応に要した作業は年間延べ何人・日ですか。(は1つ)

1 0人・日

2 1人・日以内

3 2～3人・日

4 4～5人・日

5 6～10人・日

6 11～15人・日

7 16人・日以上 (人・日)

→ 対応として実施した内容について該当する番号に をご記入ください。また、社内で発生したおおよその作業規模をお答えください。(はいくつでも)

a. 原因追求・影響範囲特定のための外部調査
b. 問合せ窓口の設置
c. 電話郵送等での取引先・顧客等への謝罪
d. 謝罪広告の出稿
e. 社内に配布する対策用 CD-ROM の作成
f. その他 ()
g. 特に実施していない

対応の有無
1
2
3
4
5
6
7

社内で発生した作業の規模	
約	人・日
約	人・日
約	人・日
約	人・日
約	人・日
約	人・日

→ さしつかえのない範囲で、流出した情報の内容(件数)や対応策について、ご記入ください。

・ 標的型攻撃(*14)による被害について伺います。

(*14) 標的型攻撃とは、主に電子メールを用いて特定の組織や個人を狙う手法です。典型的な例として、メール受信者の仕事に関係しそうな偽の話題等を含む本文や件名で騙し、添付ファイル(ウイルス)のクリックを促す場合が知られています。

問41 貴企業では、昨年1年間(2007年1月～12月)に、貴企業を狙い撃つような標的型攻撃の電子メールを受信しましたか。(は1つ)

1 なし

2 標的型攻撃の発見のみ

3 標的型攻撃が原因と考えられるウイルス感染、不正アクセス、情報流出等が確認された

→ さしつかえのない範囲で、受信した電子メールの内容や対応策について、ご記入ください。

・ **スパイウェア (*15) による被害についてお伺いします。**

(*15) スパイウェアとは、利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等のことを指します。

問42 貴企業では、昨年1年間(2007年1月～12月)にスパイウェアの被害に遭いましたか。(は1つ)

- 1 なし
- 2 スパイウェアの発見のみ
- 3 発見したスパイウェアが原因と考えられる情報流出等が確認された

問43 発見されたスパイウェアの侵入経路は、どのように想定されますか。(は1つ)

- 1 電子メール
- 2 インターネット接続 (ホームページ閲覧など)
- 3 自らダウンロードしたファイル
- 4 P2P(Peer to Peer)などのファイル共有ソフト
- 5 外部媒体、持ち込みクライアント(パソコン)
- 6 その他 ()
- 7 不明

・ **情報セキュリティ事象に関連する間接的被害(信用の低下等)についてお伺いします。**

問44 貴企業では、昨年1年間(2007年1月～12月)に、ウイルスやスパイウェア、情報漏えい等によって間接的な被害がありましたか。あてはまるものをご記入ください。(はいくつでも)

* パソコンの紛失のような人的ミスによる情報セキュリティ被害は含みません。

	ウイルスやスパイウェアが原因	情報漏洩が原因
a. 顧客の喪失・減少	1	1
b. 取引先等への補償・補填、損害賠償、訴訟への対応	2	2
c. 中傷、流言	3	3
d. その他 ()	4	4
e. 特に間接的な被害は受けなかった	5	5

次頁「個人情報のお取り扱いについて」にご同意の上、ご記名下さい。

貴企業・貴事業所名			
お名前		所属部署・役職	
ご住所	〒		
	TEL:		
E-mail アドレス			

ご回答くださった方には、調査結果概要版をメールにて送付させていただきます。

ご協力ありがとうございました