# 情報セキュリティ調査へのご協力のお願い

拝啓　時下ますますご清祥のこととお喜び申し上げます。

情報システムは今や企業・組織だけではなく、一般社会においても重要な基盤であり、情報システムの安全性・信頼性を確保するための情報セキュリティ対策が非常に重要となっています。

私ども情報セキュリティ大学院大学 原田研究室（教授：原田要之助）では、情報セキュリティマネジメント等について研究を行っており、今年度の調査では、情報セキュリティマネジメントの取組状況、人的要因に関する情報セキュリティへの取組、情報セキュリティの人材育成と教育、個人の行動履歴データの取扱いの調査を行い、課題を抽出したいと考えております。

本調査は、プライバシーマーク取得企業、ISMS取得企業、公官庁及び教育機関から4,500組織を選定し依頼しております。

本趣旨をご理解頂き、可能な範囲で結構ですので、是非ともご回答頂きますようお願い申し上げます。

調査結果は統計的な処理を行い、貴社名・ご記入者名等の個別属性を公開することはありません。

また、ご回答いただいた内容は本調査に関連するもの以外に利用することはありません。

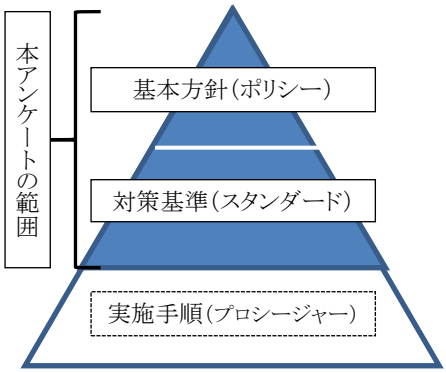
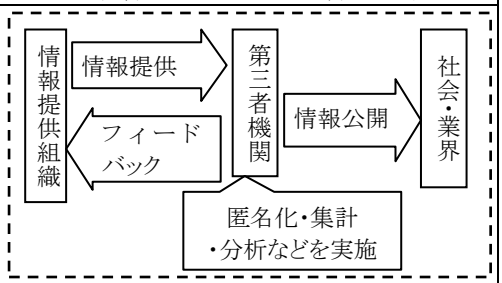
調査の分析結果は、12月上旬に本学のWebサイト（http://www.iisec.ac.jp/）上で公開する予定です。

お忙しい中、大変恐縮ではございますが、調査回答票は**2014年8月22日（金曜日）までにご投函**くださいますようお願い申し上げます。

敬具

［ご質問・お問合せ先］　情報セキュリティ大学院大学 原田研究室
原田研究室Webサイト(http://lab.iisec.ac.jp/~harada_lab/professor.html)
電子メール：harada.survey@iisec.ac.jp　FAX：045-410-0238

［本調査における用語］

| 用 語 | 用語の説明 |
|---|---|
| リスク分析 | リスク分析とは、保護すべき情報資産を明らかにし、それらに対するリスクを評価すること。 |
| 情報セキュリティポリシー（方針・基準） | 企業（組織）全体の情報セキュリティに関する基本方針・対策基準のこと（右図において範囲を示す）。本アンケートにおいては情報セキュリティ実施手順等の具体的な手順は含まない。<br>**・基本方針**:「なぜセキュリティが必要か」について規定し、何をどこまで守るのか（対象範囲）、誰が責任者かを明確にする。<br>**・対策基準**:基本方針で作成した目的を受けて、「何を実施しなければならないか」について記述する。組織的に情報セキュリティ対策を行うためのルール集、規程類に相当。<br>**・実施手順**：対策基準で定めた規程を実施する際に、「どのように実施するか」というマニュアル的な位置づけの文書であり、詳細な手順を記述。バックアップ手順書やサーバー運用手順書など特定の業務で使用。<br>  |
| ヒヤリ・ハット | 以下に掲げる事例をいう<br>① 誤った行為等が、実施される前に発見された事例<br>② 誤った行為等が実施されたが、結果として社会に影響を及ぼすに至らなかった事例<br>（誤った行為等が実施され、結果として社会に何らかの影響を及ぼした事例は含まない） |
| 第三者機関 | 情報共有の体制の中でいかなる組織に対しても公平・中立で独立して存在する組織。<br>例えば、医療の分野では、医療事故情報収集等事業における、「日本医療機能評価機構」、情報セキュリティの分野では、サイバー情報共有イニシアティブ（J-CSIP）における、「情報処理推進機構（IPA）」のような機関を指す。<br>  |

［質問回答方法］

本用紙に回答をご記入のうえ、同封の封筒によりご返送ください。

選択式設問のご回答は、該当する選択肢の番号を○で囲んでください。

## ［第1章］ 貴社の概要についてお伺いします

**[Q1].** ご記入者の所属 （○印はひとつだけ）

| | | |
|---|---|---|
| 1 総務部門 | 6 情報セキュリティ担当部門 | 11 リスク管理担当部門 |
| 2 人事部門 | 7 情報システム開発部門 | 12 監査部門 |
| 3 経理部門 | 8 情報システム管理部門 | 13 事業/営業部門 |
| 4 社長室又は役員室 | 9 法務部門 | 14 その他[ ] |
| 5 企画部門 | 10 コンプライアンス担当部門 | |

**[Q2].** ご記入者の役職 （○印はひとつだけ）

| | | |
|---|---|---|
| 1 会長・社長・取締役 | 4 部長 | 7 専門職 |
| 2 執行役・執行役員 | 5 課長 | 8 一般社員 |
| 3 事業部長 | 6 係長・主任 | 9 その他[ ] |

**[Q3].** 貴社の業種 （○印はひとつだけ）
複数業種に該当する場合、売上高が最も高い業種（日本標準産業分類をベースとして使用）をお選びください。

| | | |
|---|---|---|
| 1 農業、林業、漁業、鉱業 | 7 卸売業、小売業 | 14 医療、福祉 |
| 2 建設業 | 8 金融業、保険業 | 15 大学 |
| 3 製造業（印刷業を含む） | 9 不動産業、物品賃貸業 | 16 公務（政府・自治体） |
| 4 電気・ガス・熱供給・水道業 | 10 宿泊業、飲食サービス業 | 17 複合サービス事業（郵便局、協同組合） |
| 5 情報通信業（通信業、放送業、情報サービス業、ソフトウェア業、インターネット附随サービス業、映像・音声・文字情報制作業） | 11 学術研究、専門・技術サービス業（法律事務所、行政書士事務所、広告業、デザイン業を含む） | 18 サービス業（廃棄物処理業、自動車整備業、機械等修理業、職業紹介・労働者派遣業、その他事業サービス業を含む） |
| | 12 生活関連サービス業、娯楽業 | |
| 6 運輸業、郵便業 | 13 教育、学習支援業 | 19 その他[ ] |

**[Q4].** 貴社[単独]の直近期の売上高 （○印はひとつだけ）
大学・官公庁等は予算額、銀行は経常収益高、保険は収入保険料または正味保険料、証券は営業収入高。

| | | |
|---|---|---|
| 1 売上高はない（非営利団体） | 5 5億円～10億円未満 | 9 300億円～500億円未満 |
| 2 1億円未満 | 6 10億円～50億円未満 | 10 500億円～1,000億円未満 |
| 3 1億円～3億円未満 | 7 50億円～100億円未満 | 11 1,000億円以上 |
| 4 3億円～5億円未満 | 8 100億円～300億円未満 | |

**[Q5].** 貴社[単独]の直近の全従業員数 （○印はひとつだけ）

| | | |
|---|---|---|
| 1 50人以下 | 5 501～1,000人 | 9 10,001～50,000人 |
| 2 51～100人 | 6 1,001～1,500人 | 10 50,001人以上 |
| 3 101～300人 | 7 1,501～5,000人 | |
| 4 301～500人 | 8 5,001～10,000人 | |

**[Q6].** 貴社[単独]の PC 数（全社のおおまかな台数） （○印はひとつだけ）

| | | |
|---|---|---|
| 1 50台以下 （保有していないを含む） | 5 501～1,000台 | 9 10,001～50,000台 |
| 2 51～100台 | 6 1,001～1,500台 | 10 50,001台以上 |
| 3 101～300台 | 7 1,501～5,000台 | |
| 4 301～500台 | 8 5,001～10,000台 | |

**[Q7].** 貴社ではプライバシーマーク(P マーク)、ISMSを取得していますか。（○印はひとつだけ）

| | |
|---|---|
| 1 いずれも取得 | 3 ISMSのみ取得 |
| 2 Pマークのみ取得 | 4 いずれも取得していない |

**[Q8].** 貴社において情報セキュリティ監査を実施していますか。（複数選択可）

| | | |
|---|---|---|
| 1 認証の維持目的に実施している | 2 認証目的以外に実施している | 3 実施していない |

## ［第2章］ 情報セキュリティマネジメントの取組み状況についてお伺いします

**[Q9].** 情報セキュリティに関するリスク分析を最後に実施したのはいつですか。（○印はひとつだけ）

| | | |
|---|---|---|
| 1 半年未満 | 3 1年以上2年未満 | 5 3年以上 |
| 2 半年以上1年未満 | 4 2年以上3年未満 | 6 実施していない **【→Q11へ】** |

**[Q10].** リスク分析を実施した理由として当てはまるものはどれですか。（複数選択可）

| | | |
|---|---|---|
| 1 内部規程の改訂 | 5 他社の情報セキュリティ事故発生 | 9 ISMSやPマークへの対応 |
| 2 社内組織の改編 | 6 自社の情報セキュリティ事故発生 | 10 ISMSの規格が変更になったため |
| 3 業務内容の変更 | 7 新たな脅威への対応 | 11 その他（会社の合併や事業の再編などの理由）[ ] |
| 4 法律・条令の改正 | 8 情報資産の棚卸 | |

**[Q11].** リスク分析を行う際の問題点について、最も近いものの番号に○印を付けてください。(各項目について○印はひとつだけ)

リスク分析を行っていない場合は実施しない理由を、リスク分析を行っている場合は実施時の問題点をお答えください。

| 内容 | そう思う | どちらかと言えばそう思う | どちらかと言えばそう思わない | そう思わない |
|---|---|---|---|---|
| 1 実施方法が分かる人材が不足している | 1 | 2 | 3 | 4 |
| 2 収益に直結しない | 1 | 2 | 3 | 4 |
| 3 通常の業務に比べ、優先度が低い | 1 | 2 | 3 | 4 |
| 4 必要となる情報の収集が難しい | 1 | 2 | 3 | 4 |
| 5 上司(経営者など)の理解がない | 1 | 2 | 3 | 4 |
| 6 関係部署の協力が得られない | 1 | 2 | 3 | 4 |

**[Q12].** セキュリティ対策を進める上で、経営者(責任者)に対する説得材料として有用と思うものを上位3つを目途にお答えください。(3 つを目途に選択可)

| | | | |
|---|---|---|---|
| 1 | 実被害事例(自社・グループ会社) | 6 | セキュリティ事件・事故による想定被害額や賠償額の試算値 |
| 2 | 実被害事例(**同**業他社) | 7 | テレビ・新聞などのマスコミ報道 |
| 3 | 実被害事例(**他**業種) | 8 | 政府・公的機関のガイドライン |
| 4 | セキュリティ対策事例(**同**業他社) | 9 | リスク分析を実施した結果 |
| 5 | セキュリティ対策事例(**他**業種) | 10 | その他[ ] |

**[Q13].** 社内(組織内)にサービス(システム)を新たに導入する場合のセキュリティ管理者(セキュリティ担当部門)の関与の仕方についてお答えください。(複数選択可)

| | | | |
|---|---|---|---|
| 1 | セキュリティ管理者(セキュリティ担当部門)の承認が必要 | 5 | セキュリティ面で不安があるときのみセキュリティ管理者(セキュリティ担当部門)に確認 |
| 2 | セキュリティ管理者(セキュリティ担当部門)がサービス(システム)選定の場に参加(アドバイザー的役割) | 6 | セキュリティ管理者(セキュリティ担当部門)は関与しない |
| 3 | セキュリティ管理者(セキュリティ担当部門)がセキュリティ機能の設計を実施 | 7 | その他[ ] |
| 4 | セキュリティ管理者(セキュリティ担当部門)が設計書のレビューを実施 | | |

**[Q14].** 情報セキュリティポリシーの有無と定着度の変化についてお伺いします。

※「情報セキュリティポリシー」の定義については表紙の[本調査における用語]をご参照願います。

Q14-1.情報セキュリティポリシーを制定していますか。している場合、制定してから何年ですか。(○印はひとつだけ)

| | | | |
|---|---|---|---|
| 1 | 1年未満 | 4 | 5年以上 |
| 2 | 1年以上3年未満 | 5 | 情報セキュリティポリシーはない**【→Q21(5ﾍﾟｰｼﾞ)へ】** |
| 3 | 3年以上5年未満 | 6 | その他[ ] |

■Q14-2～6 は情報セキュリティポリシーを制定している場合に回答してください。

Q14-2.情報セキュリティポリシー制定のきっかけは何ですか。(○印はひとつだけ)

| | | | |
|---|---|---|---|
| 1 | PマークやISMSを取得するため | 5 | 体系的なセキュリティ対策を実施するため |
| 2 | 取引先から求められたため | 6 | 企業(組織)のイメージ戦略のため |
| 3 | 政府・公的機関のガイドラインに則るため | 7 | わからない |
| 4 | セキュリティ事故が起きたため | 8 | その他[ ] |

Q14-3.情報セキュリティポリシー制定時もしくは改訂時に従業員に定着しやすいように工夫している(工夫した)ことはありますか。(複数選択可)

| | | | |
|---|---|---|---|
| 1 | 全体説明会にてポリシー制定(改訂)の目的やセキュリティ対策内容の詳しい説明を実施 | 5 | 情報セキュリティポリシーに関する意見交換会の開催 |
| 2 | 部門や箇所ごとの説明会にてポリシー制定(改訂)の目的やセキュリティ対策内容の詳しい説明を実施 | 6 | 社内Webに掲載、ハンドブックの配布など情報セキュリティポリシーの内容を確認しやすいようにした |
| 3 | 情報セキュリティポリシー制定(改訂)の目的やセキュリティ対策内容についての資料を配布 | 7 | 何も行わない(トップダウンによる命令など) |
| 4 | 部門や箇所ごとの研修・勉強会を開催 | 8 | その他[ ] |

Q14-4.情報セキュリティポリシーは従業員に定着していると思いますか。(複数選択可)

| | | | |
|---|---|---|---|
| 1 | 全体的に定着している | 5 | 一般社員(情報セキュリティポリシー制定部門以外)には定着している |
| 2 | 管理職(情報セキュリティポリシー制定部門)には定着している | 6 | 改善すべき点はあるが、対応方法を検討中**【→Q14-6.へ】** |
| 3 | 管理職(情報セキュリティポリシー制定部門以外)には定着している | 7 | わからない**【→Q14-6.へ】** |
| 4 | 一般社員(情報セキュリティポリシー制定部門)には定着している | 8 | その他[ ] |

Q14-5.【Q14-4.で「1～5（定着している）」を選択した方のみ】
定着していると思う場合、定着した理由は何だと思いますか。（複数選択可）

| | | | |
|---|---|---|---|
| 1 | 教育・研修等による周知徹底の効果 | 7 | 社内Webに掲載、ﾊﾝﾄﾞﾌﾞｯｸの配布など情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの内容を確認しやすいようにした |
| 2 | 定期的に意見交換会を実施する等従業員の反応を確認できるようにしている | 8 | 情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの詳細な解説書を作成した |
| 3 | 定期的に内容の見直し・改訂を行い形骸化しないようにしている | 9 | 各部署でｾｷｭﾘﾃｨ推進者を定めるなど情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰへの関心を高める工夫をしている |
| 4 | 定期的に定着度ﾁｪｯｸ（ﾃｽﾄ、ｷｬﾝﾍﾟｰﾝなど）を実施している | 10 | ポリシーを守れていない従業員に対し従業員間で注意しあえる雰囲気をつくった |
| 5 | 情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰを守らない場合の罰則規定がある | 11 | わからない |
| 6 | 情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰを具体的に実施するための手順が確立されている | 12 | その他[ ] |

Q14-6. さらに定着させるために改善すべき点があるとしたら何だと思いますか。（複数選択可）

| | | | |
|---|---|---|---|
| 1 | これ以上改善すべき点はない | 8 | 部門や箇所ごとに自主的な勉強会を開催させる |
| 2 | 教育・研修等を部門や箇所ごとに行う等、より細分化した内容で実施する | 9 | 定期的に意見交換会を実施する等従業員の反応を確認できるようにする |
| 3 | 社内Webに掲載、ﾊﾝﾄﾞﾌﾞｯｸの配布など情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの内容を確認しやすいようにする | 10 | 情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰを具体的に実施するための手順を確立する |
| 4 | 情報セキュリティポリシーの詳細な解説書を作成する | 11 | 各部署でｾｷｭﾘﾃｨ推進者を定めるなど情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰへの関心を高める工夫をする |
| 5 | 定期的に内容の見直し・改訂を行い形骸化しないようにする | 12 | ポリシーを守れていない従業員に対し従業員間で注意しあえる雰囲気をつくる |
| 6 | 定期的に定着度ﾁｪｯｸ（ﾃｽﾄ、ｷｬﾝﾍﾟｰﾝなど）を実施 | 13 | わからない |
| 7 | 情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰを守らない場合の罰則規定を導入 | 14 | その他[ ] |

**[Q15].** 情報セキュリティポリシーを守らなかった場合の罰則規定はありますか。（○印はひとつだけ）

| | | | |
|---|---|---|---|
| 1 | 罰則規定がある | 4 | 罰則は科さず報告書（始末書）を書かせるよう検討中 |
| 2 | 罰則は科さず報告書（始末書）を書かせている | 5 | 罰則規定導入の予定はない |
| 3 | 罰則規定の導入を検討中 | 6 | その他[ ] |

**[Q16].** 情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの改善要望についてお伺いします。
Q16-1. 社内（組織内）（情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ制定部門以外）から改善要望が出たことはありますか。（○印はひとつだけ）

| | | | |
|---|---|---|---|
| 1 | 改善要望が出たことがある | 3 | 改善要望を確認する機会や受付窓口はなく、改善要望が出たこともない |
| 2 | 改善要望を確認する機会や受付窓口はあるが改善要望が出たことはない | 4 | その他<br>[ ] |

Q16-2.改善要望を情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰに取り入れたことはありますか。（複数選択可）

| | | | |
|---|---|---|---|
| 1 | 既存の情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰに対する不満点（厳しすぎる等）への改善要望を取り入れた | 4 | 既存の情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰに不足している項目（緩すぎる、新しい分野への対応等）への改善要望を次回改訂時に取り入れる予定 |
| 2 | 既存の情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰに不足している項目（緩すぎる、新しい分野への対応等）への改善要望を取り入れた | 5 | 取り入れたことはない |
| | | 6 | 改善要望が出たことはい |
| 3 | 既存の情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰに対する不満点（厳しすぎる等）への改善要望を次回改訂時に取り入れる予定 | 7 | その他<br>[ ] |

**[Q17].** 情報セキュリティポリシー(全体)の制定・見直しの手続きについてお伺いします。手続きを行っているのはどの部門ですか。（○印はひとつだけ）

| | | | |
|---|---|---|---|
| 1 | 経営層（取締役以上）が制定・見直しをしている | 3 | 情報システム部門・情報セキュリティ部門**「以外」**の部門が制定・見直しをしている |
| 2 | 情報ｼｽﾃﾑ部門・情報ｾｷｭﾘﾃｨ部門が制定・見直しをしている | 4 | その他[ ] |

**[Q18].** 情報セキュリティポリシー（全体）についてお伺いします。**過去 3 年(2012 年 1 月以降)**でどの’管理策の項目’を見直しましたか。（複数選択可）

| | | | | | |
|---|---|---|---|---|---|
| 1 | セキュリティ基本方針全般 | 6 | 通信及び環境セキュリティ（含む監視） | 11 | 法令遵守（コンプライアンス） |
| 2 | 情報セキュリティのための組織 | 7 | アクセス制御 | 12 | 3年以内に新規作成した |
| 3 | 資産管理 | 8 | 情報システムの取得、開発及び保守 | 13 | 3年間は管理策の見直しがない |
| 4 | 人的資源のセキュリティ | 9 | 情報セキュリティ・インシデント管理 | 14 | その他<br>[ ] |
| 5 | 物理的・環境的セキュリティ | 10 | 事業継続管理 | | |

【Q18 に関する注意】 ISO/IEC 27001:2013 附属書 A（規定）管理目的及び管理策では、6 の通信及び環境セキュリティ（含む監視）が運用管理と通信のネットワークに分離、8 の情報システムの取得・開発及び保守から暗号、供給者管理が分離、10 事業継続管理が情報セキュリティ側面のみに限定されるなど変化が有りました。今回は移行途中ですので ISO/IEC 27001:2005 の管理策項目のままでお答えください。

**[Q19].** 過去 3 年で情報セキュリティポリシー（全体）を見直した理由として当てはまるものはどれですか。（複数選択可）

| | | | |
|---|---|---|---|
| 1 | モバイルコード（スマートフォン、携帯電話等）の利用拡大 | 7 | ISMSの更新 |
| 2 | クラウド・コンピューティング（業務システム等）の利用拡大 | 8 | 法律・規制への対応（差し支え無ければ、具体的に）<br>[ ] |
| 3 | 第三者が提供するサービス（開発・運用業務）拡大 | | |
| 4 | 効率化（ツール導入等）したので変えた | 9 | 3年間は管理策の見直しがない |
| 5 | 監査などの指摘事項への対応 | 10 | その他<br>[ ] |
| 6 | 事業継続計画（BCP/BCM）と緊急時対応 | | |

**[Q20].** 2013 年秋に ISMS の基本基準である ISO/IEC 27001 および 27002 が改訂されましたが、貴社（組織）情報セキュリティポリシーに対する影響をどのようにお考えですか。（○印はひとつだけ）

| | | | |
|---|---|---|---|
| 1 | 改訂されたことを知らなかった | 5 | 改訂内容を、1年以内に反映する予定 |
| 2 | 改訂は知っているが、ISMSを取得しておらず影響なし | 6 | 改訂内容について検討中 |
| 3 | 改訂は知っているが、影響がないことを確認した | 7 | 既に改訂内容を反映させた |
| 4 | 改訂内容を、2年以内に反映する予定で準備中 | 8 | その他［ ］ |

## ［第3章］ 人的要因に関する情報セキュリティへの取組みについてお伺いします

**[Q21].** 直近の一年間で社員・派遣社員などの人的要因により情報セキュリティに関連する、どのような事故・トラブルが発生しましたか。（複数選択可）

| | | | |
|---|---|---|---|
| 1 | 発生していない | 9 | スマートフォン・携帯電話の紛失 |
| 2 | 情報の持出しによる情報の流出 | 10 | USB メモリ等情報記録媒体の紛失 |
| 3 | サーバ・制御機器への悪意のある操作によるｼｽﾃﾑﾀﾞｳﾝ | 11 | 紙媒体の紛失 |
| 4 | SNS への書き込みによる損害の発生 | 12 | 紙媒体の誤送付・誤交付 |
| 5 | サーバ・制御機器への誤操作によるｼｽﾃﾑﾀﾞｳﾝ | 13 | FAX の誤送信 |
| 6 | 業務システムなどへの入力間違いによる損害の発生 | 14 | 電子メールの誤送信 |
| 7 | Web サーバ等の設定ミスによる情報の流出 | 15 | その他[ ] |
| 8 | PC・タブレットの紛失 | | |

**[Q22].** 社員・派遣社員などによる情報セキュリティに関連する不正行為を防ぐためにどのような対策を講じていますか。（複数選択可）

| | | | |
|---|---|---|---|
| 1 | 特に対策は行っていない | 7 | 重要情報等へのアクセスログを保存している |
| 2 | 経営者の責任を明確にしている | 8 | 重要情報等へのアクセスログを確認している |
| 3 | 情報へのアクセス制限を行っている | 9 | 雇用終了時に秘密保持を課す誓約を締結している |
| 4 | 共有アカウントの利用を禁止している | 10 | 就業規則で内部不正者への懲戒手続きを定めている |
| 5 | 入退室管理を行っている | 11 | 内部不正に関する通報制度を整備している |
| 6 | 情報記録媒体の持出管理を行っている | 12 | その他[ ] |

**[Q23].** 貴社組織内において、どのような場合に、人的ミスによる事故・トラブルの情報を集めていますか。（複数選択可）

※「ヒヤリ・ハット」の定義については表紙の[本調査における用語]をご参照願います。

| | | | |
|---|---|---|---|
| 1 | 人的ミスだけが原因の場合情報は集めていない | 5 | 紛失・置き忘れによりヒヤリ・ハットが発生した場合 |
| 2 | 誤操作により社会に影響を及ぼした場合 | 6 | 設定ミスにより社会に影響を及ぼした場合 |
| 3 | 誤操作によりヒヤリ・ハットが発生した場合 | 7 | 設定ミスによりヒヤリ・ハットが発生した場合 |
| 4 | 紛失・置き忘れにより社会に影響を及ぼした場合 | 8 | その他[ ] |

**以下の設問では、社会に影響を与えていない、ヒヤリ・ハットの情報に限ってお伺いします。**

**[Q24].** 自組織内の情報ｾｷｭﾘﾃｨのヒヤリ・ハット事例情報を外部に公表している組織に対してどのように評価しますか。（複数選択可）

| | | | |
|---|---|---|---|
| 1 | 自浄作用が働いている組織で信用できる | 4 | 事故・トラブルを起こす可能性があり信用できない |
| 2 | 組織内人員の情報セキュリティに対する意識が高い | 5 | 何も評価しない |
| 3 | 社会・業界の人的ミスの減少に貢献している | 6 | その他[ ] |

**[Q25].** 貴社が自組織内の情報ｾｷｭﾘﾃｨのヒヤリ・ハット事例情報を外部に公表・提供する場合どのような効果を期待しますか。（複数選択可）

| | | | |
|---|---|---|---|
| 1 | 自浄作用が働いている組織として信用の向上 | 4 | 実際の事故・トラブル時に（全部又は一部）免責される |
| 2 | 自組織内の事故・トラブル件数の減少 | 5 | その他[ ] |
| 3 | 社会・業界の人的ミスの減少への貢献 | | |

**[Q26].** 国などによりガイドラインが示され、ヒヤリ・ハット**事例情報の収集・分析・公表を担当する公平・中立的で独立した第三者機関が設立された場合、**どのような条件があれば貴社組織内の情報セキュリティのヒヤリ・ハット事例情報を第三者機関に提供することができますか。提供する要素として大きなものを3つ以内でお答えください。（3つまで選択可）

| | | | |
|---|---|---|---|
| 1 | 情報の収集目的が明確に示されている | 6 | 報告には手間がかからない |
| 2 | 提供した情報については免責される（処罰されない） | 7 | 提供しない組織に比べより多くの情報を入手できる |
| 3 | 第三者機関が情報の出所を特定できないようにしている | 8 | 多くの組織が情報提供の取組みに参加している |
| 4 | 第三者機関の情報セキュリティが保たれている | 9 | その他[ ] |
| 5 | 第三者機関の取組みが社会に認められている | 10 | どのような条件であっても提供することはない |

## ［第4章］ 情報セキュリティの人材育成と教育に関してお伺いします

**[Q27].** 情報セキュリティの推進者の人材育成に関してどのような制度等がありますか。(複数選択可)

1 専門性を高める為に、専門学校・大学・大学院へ会社負担で派遣する制度がある
2 大学・大学院へ入学を希望する場合は、費用や時間のサポート制度がある
3 制度はないが、希望する従業員へは費用や時間の支援を行っている
4 外部研修会・セミナーに積極的に参加させている(費用は会社負担)
5 自己啓発を奨励し資格取得者への報奨制度(一時金・資格手当等)がある
6 社内研修・OJT 等による人材育成制度を設けている
7 特に定めていない
8 その他[ ]

**[Q28].** 情報セキュリティに関する従業員への教育(集合研修・E ラーニング等)に関してお伺いします。

Q28-1. 全社員向けの教育を年間何回位実施していますか。(○印はひとつだけ)

1 1 回
2 2 回
3 3 回
4 4 回以上
5 不定期(数年に 1 回も含む)に実施している
6 情報セキュリティポリシー改訂時のみ実施する
7 全社員向けには実施していない**【→Q28-3.へ】**
8 教育を実施していない**【→Q29 へ】**
9 その他[ ]

Q28-2.【Q28-1.で 1～6 を回答された方のみ】上記従業員への教育の効果を確認していますか。(複数選択可)

1 テストを実施している
2 感想文・レポート・アンケートを提出させている
3 特に実施していない
4 その他[ ]

Q28-3. 全社員向けの定期的な教育以外に特定の社員を対象とした教育を年間何回位実施していますか。(○印はひとつだけ)

1 1 回
2 2 回
3 3 回
4 4 回以上
5 不定期(数年に 1 回も含む)に実施している
6 情報セキュリティポリシー改訂時のみ実施する
7 実施していない **【→Q29 へ】**
8 その他[ ]

Q28-4.【Q28-3.で 1～6 を回答された方のみ】定期的ではない教育の対象となる従業員はどれですか。(複数選択可)

1 新入社員
2 転入社員(新たに企業(組織)に所属した社員)
3 入社 3 年次等、特定年次の社員(新入社員を除く)
4 システム部門の社員
5 セキュリティ管理部門の社員
6 昇進・昇職する社員
7 異動・担当業務変更する社員
8 管理職社員
9 受講を希望した社員
10 派遣社員(常駐社員を含む)
11 委託先社員
12 その他[ ]

Q28-5.【Q28-3.で 1～6 を回答された方のみ】上記従業員への教育の効果を確認していますか。(複数選択可)

1 定期的な教育より詳細なテストを実施している
2 定期的な教育と同程度のテストを実施している
3 定期的な教育より詳細な感想文・レポート・アンケートを提出させている
4 定期的な教育と同程度の感想文・レポート・アンケートを提出させている
5 特に実施していない
6 その他 [ ]

## ［第5章］ 貴社における「個人の行動履歴データ」の取扱いについてお伺いします

**■「個人の行動履歴データ」の定義**
**“個人の行動履歴をデータ化したもの”**
(例)WEB のアクセス履歴、ｲﾝﾀｰﾈｯﾄｼｮｯﾋﾟﾝｸﾞ履歴、POS データ、SNS、通信履歴、携帯電話の GPS などの位置情報、交通機関利用データ、防犯カメラ映像など、人が入力したデータや、人の活動を記録したデータ

**[Q29].**「個人の行動履歴データ」を業務で取り扱っていますか。※「個人の行動履歴データ」の定義は上記参照

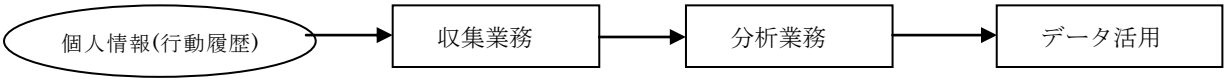
1 取り扱っている
2 取り扱っていない **【→Q45 (8 ページ)へ】**

**以下[Q30～Q44]の設問は、Q29 で 「1. 取り扱っている」 と回答した場合のみ、ご回答願います。**

**[Q30].** 取り扱っている「個人の行動履歴データ」の種類は以下のどれですか。(取り扱っているものすべて選択)

1 購買履歴(ｲﾝﾀｰﾈｯﾄｼｮｯﾋﾟﾝｸﾞ、ﾋﾞﾃﾞｵﾚﾝﾀﾙなど)
2 POS ﾃﾞｰﾀ(実店舗での売上ﾃﾞｰﾀなど)
3 WEB アクセス履歴
4 位置情報、移動履歴(GPS など)
5 ブログ、掲示板、SNS、Twitter 投稿などの書き込み情報
6 個人の健康情報ﾃﾞｰﾀ
7 通信履歴、通話履歴
8 監視カメラ等で取得した画像、映像
9 交通機関利用ﾃﾞｰﾀ(自動改札での IC カード利用等)
10 自動車等の装置ﾃﾞｰﾀ(走行ﾃﾞｰﾀ、操作ログ、状態ログ)
11 わからない
12 その他[ ]

**[Q31].** 貴社における「個人の行動履歴データ」に関する業務で、該当するものを○で囲ってください。※表内へ回答願います。




(各項目について○印はひとつだけ)

| | 自社で行っている | | 行っていない |
|---|---|---|---|
| | 自社のビジネスとして | 受託ビジネスとして | |
| Q31-1. 収集業務 | 1 | 2 | 3 |
| Q31-2. 分析業務 | 1 | 2 | 3 |
| Q31-3. データ活用 | 1 | 2 | 3 |

**[Q32].** 取り扱っている「個人の行動履歴データ」の対象人数の総数を教えてください。(○印はひとつだけ)

| | |
|---|---|
| 1 100 人未満 | 4 5,000 人～10 万人未満 |
| 2 100 人～999 人 | 5 10 万人以上 |
| 3 1,000 人～4,999 人 | 6 わからない |

**[Q33].** 「個人の行動履歴データ」を取り扱っている業務の目的は何ですか。(複数選択可)

| | |
|---|---|
| 1 ターゲッティング広告(レコメンド機能含む) | 8 データ自体の販売 |
| 2 マーケティング(市場分析、顧客分析) | 9 分析結果の販売 |
| 3 サービス提供用途 | 10 犯罪、不正の防止 |
| 4 サービス品質の向上 | 11 経営判断(投資、事業撤退など) |
| 5 サービスの解約防止 | 12 わからない |
| 6 公共的な活用目的(災害対策や道路計画など) | 13 その他[ ] |
| 7 製品、商品の開発 | |

**[Q34].** 「個人の行動履歴データ」取り扱い業務を行うことで、どのようなメリットがありますか。(複数選択可)

| | |
|---|---|
| 1 顧客数の増加 | 6 経費の削減 |
| 2 受注率の向上 | 7 クレーム数の低減 |
| 3 顧客単価の向上 | 8 経営判断のスピードアップ |
| 4 サービス満足度の向上 | 9 メリットはない |
| 5 サービス、商品の様々な兆候を把握できる | 10 その他[ ] |

**[Q35].** 「個人の行動履歴データ」取り扱い業務は、売上／利益に影響していますか。(○印はひとつだけ)

| | |
|---|---|
| 1 売上／利益に貢献している | 4 わからない |
| 2 減収／減益に影響した | 5 その他[ ] |
| 3 特に影響はない | |

**[Q36].** 貴社における「個人の行動履歴データ」を取り扱う業務の位置付けを教えてください。(○印はひとつだけ)

| | |
|---|---|
| 1 自社の主たるビジネスと考えている | 3 わからない |
| 2 補助的なビジネスと考えている | 4 その他[ ] |

**[Q37].** 「個人の行動履歴データ」取り扱い業務の拡大予定について教えてください。(○印はひとつだけ)

| | |
|---|---|
| 1 拡大予定である | 3 縮小、または撤退の予定である |
| 2 現状維持の予定である | 4 わからない |

**[Q38].** 「個人の行動履歴データ」取り扱いの、拡大、縮小/撤退、現状維持の理由を教えてください。(複数選択可)

| | |
|---|---|
| 1 投資効果が表れている為 | 7 有効な分析結果が得られない為 |
| 2 これから本格的に投資していきたい為 | 8 コストがかかりすぎる為 |
| 3 将来の為に継続する | 9 人材を確保するのが困難な為 |
| 4 親会社や取引先からの委託業務である為 | 10 顧客からのクレーム |
| 5 既に投資してしまった為 | 11 わからない |
| 6 法的な理由 | 12 その他[ ] |

**[Q39].** 「個人の行動履歴データ」の取り扱いにあたって、主な課題は何ですか。(複数選択可)

| | |
|---|---|
| 1 プライバシー面の課題 | 8 分析業務の委託コスト |
| 2 情報セキュリティ面の課題 | 9 情報セキュリティ対策コスト |
| 3 有効な分析結果が得られない | 10 人材の育成、採用コスト |
| 4 必要なデータが入手できない | 11 データ収集のコスト |
| 5 データ加工の手間がかかりすぎる | 12 その他[ ] |
| 6 分析・活用ができる人材がいない | 13 特に課題はない |
| 7 分析システムの導入コスト | 14 わからない |

**[Q40].** 貴社にデータ分析の専門家はいますか。(○印はひとつだけ)

| | | |
|---|---|---|
| 1 分析の専門家がいる | 3 いない、採用や育成の予定もない | 5 その他 |
| 2 採用、育成を予定している | 4 わからない | [ ] |

**[Q41].**「個人の行動履歴データ」の収集・分析・活用業務を取り扱うにあたり、どのようなリスクを認識していますか。（複数選択可）

| | | | |
|---|---|---|---|
| 1 | プライバシー侵害などの訴訟リスク | 5 | 企業イメージが失墜するリスク |
| 2 | 情報漏洩リスク | 6 | 投資対効果が得られないリスク |
| 3 | 法令違反のリスク | 7 | その他[ ] |
| 4 | データが消滅、改ざんされるリスク | 8 | 特にリスクは認識していない |

**[Q42].**「個人の行動履歴データ」を収集するにあたり、どのような点を考慮していますか。（複数選択可）

| | | | |
|---|---|---|---|
| 1 | データの取得目的を理解してもらうこと | 7 | 自社の企業イメージを保つこと |
| 2 | データの取得内容、範囲を理解してもらうこと | 8 | コンプライアンスを順守していること |
| 3 | データの取得方法に不信感を持たれないこと | 9 | データ取得の対価として、相応の付加価値（ポイント等）を提供すること |
| 4 | データ取得に対する同意の取り方 | | |
| 5 | データ取得が極端に強制的になっていないこと | 10 | 収集業務は行っていない |
| 6 | データ管理をしっかりやっていることを理解してもらうこと | 11 | その他[ ] |

**[Q43].**「個人の行動履歴データ」から、本人の希望でデータから除外できますか。（○印はひとつだけ）

| | | | |
|---|---|---|---|
| 1 | 本人の申告ベースで、データから除外できる | 4 | 収集業務は行っていない |
| 2 | 提供の許可を得た場合のみ、データを取得している | 5 | わからない |
| 3 | 除外できる仕組みはない | 6 | その他[ ] |

**[Q44].**「個人の行動履歴データ」を分析・活用する際に、個人が特定できないように加工していますか。（○印はひとつだけ）

| | | | |
|---|---|---|---|
| 1 | 個人を特定できないように加工している | 3 | 分析・活用を行っていない |
| 2 | 個人が特定できるデータのまま、活用している | 4 | その他[ ] |

## ［第6章］ その他

**[Q45].** 次の出来事について、ご存知なものをご選択ください。（数字に○を記入・複数選択可）

| | | | | | |
|---|---|---|---|---|---|
| 1 | 米国から中国に「ｻｲﾊﾞｰ攻撃による窃盗行為を止めるように」と強い要請を行った事案 | 8 | Googleｸﾞﾙｰﾌﾟで共有していた官公庁の情報が誰でも閲覧可能になっていた事案 | 15 | 百度の文字変換ｱﾌﾟﾘ「Baidu IME」「Simeji」が、ﾕｰｻﾞｰの入力内容を同社へ無断送信していた事案 |
| 2 | JAL・ANAﾏｲﾚｰｼﾞが、不正ｱｸｾｽによりﾎﾟｲﾝﾄを不正利用された事件 | 9 | 他者のパソコンを遠隔操作し、犯罪予告を行った事件 | 16 | ﾋﾞｯﾄｺｲﾝ取引所であるﾏｳﾝﾄｺﾞｯｸｽ社が倒産 |
| 3 | PC内のﾃﾞｰﾀをﾛｯｸし身代金を要求するランサムウェアの感染拡大（CryptoLockerなど） | 10 | 米国で100Gbpsのﾄﾗﾌｨｯｸが絶え間なく9時間継続観測、史上最大のDDoS攻撃発生 | 17 | ﾛﾘﾎﾟｯﾌﾟﾚﾝﾀﾙｻｰﾊﾞｰが管理する8,438ｳｪﾌﾞｻｲﾄが改ざん被害 |
| 4 | 不正ｱｸｾｽにより、米ﾀｰｹﾞｯﾄ社が4000万枚のｶｰﾄﾞ情報搾取被害 | 11 | ﾋﾟｻﾞｰﾗ、ﾏﾂｷﾖの公式ｱﾌﾟﾘを騙る偽ｱﾌﾟﾘがAppStoreで提供された事案 | 18 | JR東日本のSuica履歴販売に対しﾌﾟﾗｲﾊﾞｼｰ問題の指摘 |
| 5 | ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞの不正送金被害が発生。2013年の被害額は約14億円と報道発表（警察庁調べ） | 12 | 「ウイルス対策」を騙ったｱﾌﾟﾘで電話帳データが約3,700万人分抜き取られた事件 | 19 | ｱﾄﾞﾋﾞｼｽﾃﾑｽﾞへの不正ｱｸｾｽにより、ｸﾚｼﾞｯﾄｶｰﾄﾞ番号を含む3800万人の顧客情報が流出 |
| 6 | ﾊﾟｰｿﾅﾙﾃﾞｰﾀ利活用に向けた法制の見直し | 13 | 元米政府職員ｽﾉｰﾃﾞﾝ氏による政府の盗聴活動の暴露 | 20 | ISO/IEC27001規格が改定 |
| 7 | Twitterへの悪ふざけ写真投稿による炎上事件（ﾊﾞｶｯﾀｰとも呼ぶ） | 14 | InternetExplorerやOpenSSL脆弱性を利用した標的型攻撃を確認 | 21 | Windows XPサポート終了 |

**[Q46].** 次の用語について、ご存知なものをご選択ください。（複数選択可）

| | | | | | |
|---|---|---|---|---|---|
| 1 | マルウェア | 9 | MITB攻撃 | 17 | 特定秘密保護法案 |
| 2 | パーソナルデータ | 10 | アカウントリスト型ハッキング | 18 | リベンジポルノ |
| 3 | ランサムウェア | 11 | ショルダーハッキング | 19 | @police |
| 4 | ワンタイムパスワード | 12 | ペネトレーションテスト | 20 | SDN |
| 5 | DDoS攻撃 | 13 | Apache Struts2の脆弱性 | 21 | ZeuS |
| 6 | ブルートフォース攻撃 | 14 | CMSの脆弱性 | 22 | ダークネット |
| 7 | ゼロデイ攻撃 | 15 | マイナンバー法案 | 23 | エシュロン(Echelon) |
| 8 | 水飲み場型攻撃 | 16 | ライフログ | 24 | k匿名性 |

**[Q47].** 本アンケートにおける忌憚のないご意見をお聞かせください。
また、関心のある情報セキュリティ関連の出来事や用語について、ご記入ください。（下欄に自由にご記入ください）

以上で終了です。ご協力いただきまして、誠にありがとうございました。