# 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慶び申し上げます。

情報セキュリティは今や企業・組織だけではなく、一般社会においても重要な課題であり、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おります。

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関する研究を行っており、本調査では、情報セキュリティマネジメントの取組み状況やリスク認識、支出動向等の調査を行い、社会における情報セキュリティマネジメントの現状について分析すると共に、課題を抽出したいと考えております。

お忙しい中、大変恐縮ではございますが、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。

敬具

［調査について］

本調査は、プライバシーマーク(Pマーク)取得企業、ISMS取得企業、BCMS取得企業、官公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。

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サイト上で公開する予定です。これまでの調査結果につきましては（ http://lab.iisec.ac.jp/~harada_lab/survey.html ）にて公開しております。

［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。
本用紙は**2015年8月31日（月曜日）までにご投函**くださいますようお願い申し上げます。

［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） | 企業全体の情報セキュリティに関する基本方針のこと。情報セキュリティ基本方針や対策基準(管理策とその基準数値)が該当し、実施手順等の具体的な手順は含まない。<br>基準数値の例としてパスワードは 6 ケタ以上、3 か月ごとに更新等。 |
| 例外措置 | 情報セキュリティ関連規定に基づいて業務を遂行するにあたり、当該規定へ適用させることが適正な業務遂行を著しく妨げる等の理由により、当該規定とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合にとる手続きをさす。<br>さらに例外措置が当該関連規定に記載されている箇所を「例外規定」とする。 |
| 電子データ | PC やシステムで作成、編集、保存、アーカイブできる形式のデータのこと。<br>(例)メール、Microsoft Office 文書、Web サイト、CAD/CAM ファイル等 |

［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/ ）
電子メール：harada.survey@iisec.ac.jp　FAX：045-410-0238

## ［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 | 3 | 事業部長 | 5 | 課長 | 7 | 専門職 |
| 2 | 執行役・執行役員 | 4 | 部長 | 6 | 係長・主任 | 8 | 一般社員 |

9　その他 [　　]

**[Q3].** 貴社・貴組織(以下「貴社」という。)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・文字情報制作業を含む) | 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) | 4 | 3 億円～5 億円未満 | 7 | 50 億円～100 億円未満 | 10 | 500 億円～1,000 億円未満 |
| 2 | 1 億円未満 | 5 | 5 億円～10 億円未満 | 8 | 100 億円～300 億円未満 | 11 | 1,000 億円以上 |
| 3 | 1 億円～3 億円未満 | 6 | 10 億円～50 億円未満 | 9 | 300 億円～500 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 | 3 | 101～300 人 | 5 | 501～1,000 人 | 7 | 1,501～5,000 人 | 9 | 10,001～50,000 人 |
| 2 | 51～100 人 | 4 | 301～500 人 | 6 | 1,001～1,500 人 | 8 | 5,001～10,000 人 | 10 | 50,001人以上 |

**[Q6].** 貴社ではＰマーク、ISMS、BCMS を取得していますか。(複数選択可)

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

**[Q7].** 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

**[Q8].** 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【→Q10へ】 |

**[Q9].** 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等の理由)[ ] |
| 4 | 法律・条令の改正 | 8 | 情報資産の棚卸 | | |

**[Q10].** 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 必要となる社内情報の収集が難しい | 1 | 2 | 3 | 4 |
| 5 上司(経営者等)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 |
| 7 実施方法が変わって、対応できない | 1 | 2 | 3 | 4 |
| 8 部分的な対応に留まってしまう | 1 | 2 | 3 | 4 |

**[Q11].** 情報セキュリティポリシー(全体)の策定・見直しの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) | 4 | 委員会組織で見直し、代表者が手続きを行っている |
| 2 | 情報システム部門・情報セキュリティ部門 | 5 | 情報セキュリティポリシーはない【→Q14<第3章>へ】 |
| 3 | 情報システム部門・情報セキュリティ部門「以外」の部門 | 6 | その他[ ] |

**[Q12].** 情報セキュリティポリシー(管理策)についてお伺いします。以下の**管理策項目**の内、2013 年 10 月以降で新規導入・見直ししたのはどの項目ですか。(複数選択可)

| | | | |
|---|---|---|---|
| 1 | セキュリティ方針(経営陣の方向性表明)とレビュー | 11 | 運用セキュリティ(操作手順・変更・能力の管理、マルウエア対策、バックアップ等) |
| 2 | 情報セキュリティのための内部組織(職務の分離等) | 12 | 暗号による管理策(利用方針策定、鍵管理) |
| 3 | モバイル機器及びテレワーキング(方針と対策) | 13 | 運用ソフトウェア導入管理と技術的脆弱性管理 |
| 4 | 資産管理(情報分類等(含む取外し可能媒体)) | 14 | 情報システム監査(実施影響の合意等) |
| 5 | 利用者に秘密認証情報保護の責任を持たせる | 15 | 通信(ネットワークにおける情報保護と情報の転送)の管理 |
| 6 | アクセス制御方針と利用者(含む特権)アクセスの管理 | 16 | システムの取得、開発及び変更保守(含む外部委託、テスト) |
| 7 | 人的資源のセキュリティ(雇用開始から教育、雇用の終了迄) | 17 | 供給者(第三者サービスの監視・レビューを含む)の情報アクセス |
| 8 | システム及び業務ソフト(情報、ソースコード等)のアクセス制御 | 18 | セキュリティ・インシデント管理(弱点報告、対応、証拠収集を含む) |
| 9 | ログ取得及び監視(イベントの記録とその保護、定期レビュー) | 19 | 事業継続管理の情報セキュリティの側面(評価及び冗長性を含む) |
| 10 | 物理的・環境的セキュリティ(境界・入退管理、装置、クリアディスク・スクリーン方針) | 20 | 順守(法的及び契約上の要求事項、知的財産、PII等の記録保護)とセキュリティの独立したレビュー |

**[Q13].** 情報セキュリティポリシー(管理策)を新規導入、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)利用拡大 | 7 | ISMSの取得・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)[ ] |
| 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 | Pマークの取得・更新 |
| 5 | 監査等の指摘事項の対応 | 10 | 3年間は管理策の見直しがない |
| 6 | 事業継続計画(BCP/BCM)と緊急時対応 | 11 | その他[ ] |

## [第3章] 情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄの「例外措置」への取組みについてお伺いします

**[Q14].** 貴社の情報セキュリティに関わる内部規定全般において「例外規定」の項目がありますか。(○印はひとつだけ)

| | | | | | |
|---|---|---|---|---|---|
| 1 | すべての内部規定にある | 3 | 内部規定にはない | 5 | 答えたくない |
| 2 | 一部の内部規定にある | 4 | わからない・知らない | 6 | その他 [ ] |

**[Q15].** 例外規定が明記されていない事象(障害、事故・事件、災害等)に対して、一時的に例外措置した経験がありますか。2011 年の東日本大震災直後からこれまでの期間でお教えください。(○印はひとつだけ)

| | | | | | |
|---|---|---|---|---|---|
| 1 | 自分自身ある | 3 | 措置したことがあると聞いている | 5 | わからない |
| 2 | 自分はないが措置したことがある | 4 | 措置したことはない | 6 | 答えたくない |

**[Q16].** 以下の具体的な業務上の事象において、例外規定はありますか。それぞれにつきひとつだけお教えください。

| 事象 | 通常規定に設定 | | 例外規定に設定 | | 例外規定がない | |
|---|---|---|---|---|---|---|
| | 元来通常措置としている | 例外措置から変更した | 規定に従い例外措置をしている | 例外措置をしたことがない | 一時的措置をとったことがある | 例外措置をしたこともない |
| 1 ウイルス対策ソフトウェアを導入していない PC を利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 サポート切れのOSやソフトウェアをPCで利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 3 貴社管理外ソフトを利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 4 貴社管理外のPCを利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 5 私物可搬型デバイス(スマホ・タブレット等)を利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 6 可搬型メディア(USBメモリ、SDカード等)を利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 外部インターネットを利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 プログラム保守のための外部からの一時的アクセスを許可する | 1 | 2 | 3 | 4 | 5 | 6 |
| 9 外部業者への特権IDを付与する | 1 | 2 | 3 | 4 | 5 | 6 |
| 10 第三者認証のない外部クラウドを利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 11 米国パトリオット法等非日本国内法準拠のクラウドを利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 12 個人で利用しているクラウドサービス(Dropbox等)を利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 13 個人で利用しているメールに社内メールを転送する | 1 | 2 | 3 | 4 | 5 | 6 |
| 14 公衆無線LAN(暗号無し)を利用する | 1 | 2 | 3 | 4 | 5 | 6 |
| 15 その他[ ] | 1 | 2 | 3 | 4 | 5 | 6 |

**[Q17].** 内部規定に例外規定がない事象で緊急を要する事態において一時的措置をとる場合、「最初」にどのような手段をとりますか（とると想定していますか）。（○印はひとつだけ）

| | | | |
|---|---|---|---|
| 1 | CISO等経営責任者に直接経営判断をあおぐ | 4 | 従業者の判断で、事務的・システム的に運用をとる |
| 2 | 情報セキュリティ委員会での決議を受ける | 5 | その他 [ ] |
| 3 | 情報セキュリティ責任者による現場判断を受ける | | |

**[Q18].** 内部規定に新規の例外規定を策定する場合、何を参考にしますか（すると想定していますか）。（複数選択可）

| | | | | | |
|---|---|---|---|---|---|
| 1 | 他社の内部規定や具体的な事例 | 3 | 政府・官公庁の管理基準 | 5 | ISO、ISMS等国際規格 |
| 2 | 貴社の過去におけるインシデント等への一時的措置例 | 4 | 貴社が想定する今後のインシデント等に対する一時的措置 | 6 | その他[ ] |

**[Q19].** 例外規定を策定するにあたり、規程の策定と管理の事務処理をする主体部門はどこですか。（複数選択可）

| | | | | | |
|---|---|---|---|---|---|
| 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 | | |

**[Q20].** 例外規定は、貴社全体で統一された内部規定のみですか、又は現場組織ごとにも規定されていますか。（○印はひとつだけ）

| | | | | | |
|---|---|---|---|---|---|
| 1 | 統一管理基準のみ | 3 | 統一管理基準と現場組織の両方 | 5 | その他 [ ] |
| 2 | 現場組織ごと | 4 | どちらもない | | |

**[Q21].** 例外規定における例外措置の業務にはどのような手続きが盛り込まれていますか。（複数選択可）

| | | | | | |
|---|---|---|---|---|---|
| 1 | 指定書式の申請書 | 4 | CISO等経営責任者への審査報告 | 7 | 措置手順の見直し |
| 2 | 申請窓口 | 5 | 運用・管理指導（実施・終了） | 8 | その他 [ ] |
| 3 | 審査（稟議・通知） | 6 | 罰則の適用 | | |

**[Q22].** 例外規定の見直し頻度をお教えください。（○印はひとつだけ）

| | | | | | |
|---|---|---|---|---|---|
| 1 随時 | 2 ～1 年ごと | 3 ～2 年ごと | 4 ～3 年ごと | 5 3 年～ごと | 6 その他[ ] |

**[Q23].** 具体的な目的や効果に対してどのような効果があると、主観的に感じていますか。それぞれにつきひとつだけお教えください。

| 例外規定による効果 | | とても満足・安全 | 満足・安全 | どちらといえば満足・安全 | どちらといえば不満・不安 | 不満・不安 | とても不満・不安 | 具体的な措置例（任意回答） |
|---|---|---|---|---|---|---|---|---|
| 1 | 迅速に業務手続きで業務停止を防ぐ | 1 | 2 | 3 | 4 | 5 | 6 | [ ] |
| 2 | 通常手続きに係る時間・コストが節約でき、機会損失・被害を未然に防ぐ | 1 | 2 | 3 | 4 | 5 | 6 | [ ] |
| 3 | 現時点では想定外で、通常手続きに書いていない事象にも、予め審議体制を確立できている | 1 | 2 | 3 | 4 | 5 | 6 | [ ] |
| 4 | 規定違反として罰則適用を未然に防ぐ | 1 | 2 | 3 | 4 | 5 | 6 | [ ] |
| 5 | 次期規定策定への参考、事例となる | 1 | 2 | 3 | 4 | 5 | 6 | [ ] |
| 6 | 内部・外部監査への適用しやすくなる | 1 | 2 | 3 | 4 | 5 | 6 | [ ] |
| 7 | 経営ガバナンスに貢献できる | 1 | 2 | 3 | 4 | 5 | 6 | [ ] |
| 8 | ISMS 等第三者認証の更新が容易になる | 1 | 2 | 3 | 4 | 5 | 6 | [ ] |
| 9 | 情報セキュリティ関連規定全体に効果がある | 1 | 2 | 3 | 4 | 5 | 6 | [ ] |
| 10 | その他[ ] | 1 | 2 | 3 | 4 | 5 | 6 | [ ] |

## [第4章] 情報セキュリティリスクの認識と支出の動向についてお伺いします

**[Q24].** 情報セキュリティリスクについて**最も重要だと考える脅威**についてお伺いします。（1～4 でひとつ選んでください。）

| | | 内部の不正(例：情報漏えい、機器盗難) | 業務委託先での事故(例：情報漏えい、不正行為) | 外部からの攻撃（例：不正アクセス、標的型攻撃） | その他 |
|---|---|---|---|---|---|
| 1 | 現時点でどのようにお考えですか | 1 | 2 | 3 | 4[ ] |
| 2 | 2 年前にはどのようにお考えでしたか | 1 | 2 | 3 | 4[ ] |
| 3 | 今後はどのように変化するとお考えですか | 1 | 2 | 3 | 4[ ] |

**[Q25].** 情報セキュリティにおいて**最も重視する項目**についてお伺いします。（1～4 でひとつ選んでください。）

| | | 機密性（例：情報漏えい） | 完全性（例：データの改ざん） | 可用性（例：システムの停止） | その他 |
|---|---|---|---|---|---|
| 1 | 現時点でどのようにお考えですか | 1 | 2 | 3 | 4[ ] |
| 2 | 2 年前にはどのようにお考えでしたか | 1 | 2 | 3 | 4[ ] |
| 3 | 今後はどのように変化するとお考えですか | 1 | 2 | 3 | 4[ ] |

**[Q26].** 情報セキュリティにおける**最も重点を置く対策**についてお伺いします。(1～5 でひとつ選んでください。)

| | 教育等セキュリティ啓発活動や権限分離等のルール | アクセスログ記録等の内部管理ツール | ファイアウォール等の外部からの攻撃を遮断するツール | セキュリティソフト等ウイルス検知ツール利用 | その他 |
|---|---|---|---|---|---|
| 1 現時点でどのようにお考えですか | 1 | 2 | 3 | 4 | 5[ ] |
| 2 2 年前にはどのようにお考えでしたか | 1 | 2 | 3 | 4 | 5[ ] |
| 3 今後はどのように変化するとお考えですか | 1 | 2 | 3 | 4 | 5[ ] |

**[Q27].** 情報セキュリティに関する支出*についてお伺いします。**売上(官公庁・大学の場合は予算)に対して情報セキュリティに関する「支出の割合」**はどの程度ですか。(例 売上 50 億円、情報セキュリティに関する支出 5 百万円の場合は 0.1%となります。)

*支出:セキュリティ関連システム開発、運用、ライセンス等外部への支出総計

27-1.前期の実績はいかがでしたか。(○印はひとつだけ)

| | | |
|---|---|---|
| 1 0.01%未満 | 3 0.05%以上～0.1%未満 | 5 0.5%以上 |
| 2 0.01%以上～0.05%未満 | 4 0.1%以上～0.5%未満 | 6 認識していない |

27-2.支出の傾向をお伺いします。(1～6 でひとつ選んでください。)

| | 著しく増加(支出の割合 20%以上増) | 増加 | ほぼ横ばい | 減少 | 著しく減少(支出の割合 20%以上減) | その他 |
|---|---|---|---|---|---|---|
| 1 二期前と前期比較 | 1 | 2 | 3 | 4 | 5 | 6[ ] |
| 2 前期と今期の比較 | 1 | 2 | 3 | 4 | 5 | 6[ ] |
| 3 今後の変化 | 1 | 2 | 3 | 4 | 5 | 6[ ] |

## [第5章] 情報セキュリティマネジメントの運用についてお伺いします

**[Q28].** 情報セキュリティマネジメントを導入してからの運用期間についてお伺いします。(○印はひとつだけ)

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 1 年以下 | 2 2年 | 3 3 年 | 4 4 年 | 5 5 年 | 6 6 年以上 | 7 導入していない【→Q35<第 6 章>へ】 |

**[Q29].** 情報セキュリティマネジメントの運用における PDCA(計画、実行、評価・監査、改善)の各段階について、社内における取組み状況の満足度をお教えください。(1～4 でひとつ選んでください。)

| | 満足 | 普通 | 不満 | 実施していない |
|---|---|---|---|---|
| 1 P(計画) | 1 | 2 | 3 | 4 |
| 2 D(実行) | 1 | 2 | 3 | 4 |
| 3 C(評価・監査) | 1 | 2 | 3 | 4 |
| 4 A(改善) | 1 | 2 | 3 | 4 |

**[Q30].** 情報セキュリティマネジメントの運用における PDCA の各段階について、社内で重視している順番をお教えください。

| | 1 位 | 2 位 | 3 位 | 4 位 |
|---|---|---|---|---|
| 1 P(計画) | 1 | 2 | 3 | 4 |
| 2 D(実行) | 1 | 2 | 3 | 4 |
| 3 C(評価・監査) | 1 | 2 | 3 | 4 |
| 4 A(改善) | 1 | 2 | 3 | 4 |

**[Q31].** 過去 3 年以内に情報セキュリティマネジメントに関する規程を改定した回数をお教えください。(○印はひとつだけ)

| | | |
|---|---|---|
| 1 0回 | 3 2回 | 5 4回 |
| 2 1回 | 4 3回 | 6 5回以上 |

**[Q32].** C(評価・監査)について、1 年間の実施頻度をお教えください。(ISMS 認証機関による審査を除く)(○印はひとつだけ)

| | | |
|---|---|---|
| 1 0回 | 3 2回 | 5 4回 |
| 2 1回 | 4 3回 | 6 不定期に実施 |

**[Q33].** A(改善)に関して、規程の改定時に参考とする事柄についてお伺いします。(複数選択可)

| | |
|---|---|
| 1 認証機関による指摘事項 | 5 他社の障害・事故事例 |
| 2 内部監査の結果 | 6 リスク分析の結果 |
| 3 IT ベンダーやコンサルタント等の外部専門家の意見 | 7 その他 [ ] |
| 4 社員からの改善要望 | |

**[Q34].** 情報セキュリティマネジメントシステムの運用にあたり重要と考えられる事柄についてお伺いします。(3 つまで)

| | |
|---|---|
| 1 リスク分析・抽出 | 6 監査による課題点の抽出 |
| 2 実行性のある計画の策定 | 7 社員の取組み状況の評価 |
| 3 規程・マニュアルの整備 | 8 規程・マニュアルの迅速な改訂 |
| 4 管理施策の実施や導入 | 9 情報セキュリティに対する組織風土の醸成 |
| 5 社員教育による規程・マニュアルの徹底 | 10 その他[ ] |

## [第6章] 事業継続に関わる取組みの実施状況についてお伺いします

**[Q35].** 事業継続に関わる以下の項目について、実施状況をお教えください。
また、「実施済」「実施予定」の場合はその実施を検討したきっかけをお教えください。

| 項目 | 実施状況 | | | 実施を検討したきっかけ(各項目毎に○印はひとつだけ) | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 未実施 | 実施済 | 実施予定 | 危機管理の強化 | 業務の受注に有利 | 災害や事故へ対応 | 社会的な信用の向上 | 取引先からの要求 | その他 |
| 1 情報システムのバックアップや2重化 | 1 | 2 | 3 | 1 | 2 | 3 | 4 | 5 | 6 [ ] |
| 2 バックアップデータの遠隔地保存 | 1 | 2 | 3 | 1 | 2 | 3 | 4 | 5 | 6 [ ] |
| 3 情報システムのクラウド移行 | 1 | 2 | 3 | 1 | 2 | 3 | 4 | 5 | 6 [ ] |
| 4 在宅勤務(テレワーク)環境の整備 | 1 | 2 | 3 | 1 | 2 | 3 | 4 | 5 | 6 [ ] |
| 5 緊急時等を想定した訓練 | 1 | 2 | 3 | 1 | 2 | 3 | 4 | 5 | 6 [ ] |
| 6 BCP/BCM の作成 | 1 | 2 | 3 | 1 | 2 | 3 | 4 | 5 | 6 [ ] |
| 7 BCMS 認証取得 | 1 | 2 | 3 | 1 | 2 | 3 | 4 | 5 | 6 [ ] |
| 8 取引先への事業継続対策の確認 | 1 | 2 | 3 | 1 | 2 | 3 | 4 | 5 | 6 [ ] |

**[Q36].** 事業継続に関わる取組みで、「過去に実施していたがやめた事」があればお教えください。(複数選択可)

| | | | | | |
|---|---|---|---|---|---|
| 1 | 情報システムのバックアップや2重化 | 5 | 緊急時等を想定した訓練 | 9 | やめた取組みはない |
| 2 | バックアップデータの遠隔地保存 | 6 | BCP/BCMの作成 | 10 | その他 [ ] |
| 3 | 情報システムのクラウド移行 | 7 | BCMS認証取得 | | |
| 4 | 在宅勤務(テレワーク)環境の整備 | 8 | 取引先への事業継続対策の確認 | | |

**[Q37].** 事業継続に関わる取組みの中で「事業継続以外の目的」でも活用している事があればお教えください。(複数選択可)

| | | | | | |
|---|---|---|---|---|---|
| 1 | 情報システムのバックアップ | 3 | 情報システムのクラウド移行 | 5 | 活用事例はない |
| 2 | バックアップデータの遠隔地保存 | 4 | 在宅勤務(テレワーク)環境の整備 | 6 | その他[ ] |

## [第7章] 電子データの管理についてお伺いします

**[Q38].** 電子データの作成・編集及び保管・保存・廃棄を規定した文書管理規則はありますか。(○印はひとつだけ)

| | | | |
|---|---|---|---|
| 1 | 紙文書・電子データが一体で規定された文書管理規則がある | 4 | 紙文書・電子データともに文書管理規則はない<br>【→Q46 へ<第 8 章>】 |
| 2 | 電子データの文書管理規則がある | 5 | その他<br>[ ] |
| 3 | 紙文書の文書管理規則のみある | | |

**[Q39].** 文書管理規則を策定・運用している目的としてあてはまるものはどれですか。(2 つまで)

| | | | | | |
|---|---|---|---|---|---|
| 1 | 法令順守のため | 3 | 内部統制強化のため | 5 | 経営効率化のため |
| 2 | リスク(特許関係、PL 法関係、訴訟関係、バイタルレコード)緩和のため | 4 | 事業継続のため | 6 | その他[ ] |

**[Q40].** どの電子データを文書管理規則の対象としていますか。(複数選択可)

| | | | | | |
|---|---|---|---|---|---|
| 1 | 法定保存文書 | 4 | 内部統制にて求められる文書 | 7 | メール |
| 2 | JIS Q 27001、JIS Q 14001、JIS Q 9001 の認証基準で求められる文書 | 5 | リスク対応文書(特許関係、PL法関係、訴訟関係、バイタルレコード) | 8 | 非正式文書(仕掛中文書、ドラフト等) |
| 3 | 任意の自主規制文書 | 6 | CSRに基づく文書 | 9 | その他[ ] |

**[Q41].** 電子データの完全性の確保に必要な電子署名・タイムスタンプの付与を行っていますか。(○印はひとつだけ)

| | | | | | |
|---|---|---|---|---|---|
| 1 | すべての電子データに付与している | 3 | 今後付与する予定 | 5 | その他<br>[ ] |
| 2 | 重要な電子データのみ付与している | 4 | 付与していない | | |

**[Q42].** 法令・コンプライアンス・訴訟対応で求められるメール保管対策をどのような方法で実施していますか。(○印はひとつだけ)

| | | | | | |
|---|---|---|---|---|---|
| 1 | 社内でアーカイブを実施している | 3 | アーカイブではなくバックアップを実施している | 4 | 実施していない |
| 2 | 社外でアーカイブを実施している | | | 5 | その他[ ] |

**[Q43].** 電子データ利用者から、例えば裁判の証拠として、訴訟ホールド(訴訟に関連する可能性のあるデータのみをまとめて、改ざんや消去から保護する作業)をしてほしいと依頼があった場合、対応手順はありますか。(○印はひとつだけ)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 対応手順を作成済 | 2 | 対応手順を今後作成予定 | 3 | 対応手順はない | 4 | その他[ ] |

**[Q44].** 保存期間満了し、廃棄フェーズとなった電子データはどのように取扱っていますか。(○印はひとつだけ)

| | | | |
|---|---|---|---|
| 1 | 電子データを削除する。廃棄の作業過程(いつ、誰が、どのように)が分かる証跡を<u>作成する</u> | 3 | 電子データを削除する。別媒体にバックアップ<u>取得する</u> |
| 2 | 電子データを削除する。廃棄の作業過程(いつ、誰が、どのように)が分かる証跡を<u>作成していない</u> | 4 | 電子データを<u>削除していない</u> |
| | | 5 | その他[ ] |

**[Q45].** 電子データの作成・編集及び保管・保存・廃棄を監査する仕組みは備わっていますか。(○印はひとつだけ)

| | | | |
|---|---|---|---|
| 1　内部監査によって実施 | 2　外部監査によって実施 | 3　監査を実施していない | 4　その他[　　] |

## [第8章]　貴社の個人情報漏えい事故のお詫び金についてお伺いします

**[Q46].** 過去にお詫び金を支払ったことがありますか。(○印はひとつだけ)

| | | |
|---|---|---|
| 1　支払ったことがある | 2　支払ったことはない【→Q48へ】 | |

**[Q47].** 過去に支払ったお詫び金はどのように金額を決定しましたか。(○印はひとつだけ)

| | | |
|---|---|---|
| 1　過去の事例を参考 | 2　事前に定められた基準 | 3　その他[　　] |

**[Q48].** 個人情報漏えい事故発生時のお詫び金支払額についての基準を事前に定めていますか。(○印はひとつだけ)

| | | | |
|---|---|---|---|
| 1　定めている | 2　定めていない【→Q50 へ】 | 3　現在検討中である【→Q50 へ】 | 4　その他[　　] |

**[Q49].** 個人情報の種類(レベル)によって、お詫び金支払額が区分されていますか。(○印はひとつだけ)

| | |
|---|---|
| 1　区分されている | 2　区分されていない |

**[Q50].** 2014 年 7 月頃に起きた某通信教育会社における個人情報漏えい事件を受けてお詫び金に関する規定の改定や作成等に関して影響をうけましたか。(○印はひとつだけ)

| | | |
|---|---|---|
| 1　影響があった | 2　特に影響はなし【→Q52へ】 | 3　その他[　　] |

**[Q51].** お詫び金に関する規定の改定や作成等に関して影響をうけた内容はどのようなものですか。(○印はひとつだけ)

| | | | |
|---|---|---|---|
| 1　規定を改定した | 3　規定を制定した | 5 | その他 |
| 2　規定の改定を検討中 | 4　規定の制定を検討中 | | [　　] |

**[Q52].** 個人情報が漏えいした場合、どのような対応を考えていますか。(複数選択可)

| | | | |
|---|---|---|---|
| 1　謝罪・告知 | 3　訴訟に対する準備(和解を含む) | 5　検討中 | |
| 2　お詫び金(粗品等)での対応 | 4　保険による対応(賠償責任保険等) | 6　その他[　　] | |

**[Q53].** 個人情報が漏えいした場合、1 名あたりに支払うべきお詫び金支払額はいくらが妥当であると考えますか。各項目につき○印をひとつずつお付けください。50,001 円以上を選択した場合、具体的な数値をご記入ください。

| 個人情報の種類 | 0 円 | 1～500 円 | 501～1,000 円 | 1,001～5,000 円 | 5,001～10,000 円 | 10,001～20,000 円 | 20,001～50,000 円 | 50,001 円以上 [具体的な数値] |
|---|---|---|---|---|---|---|---|---|
| 1 電話番号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 2 身体情報 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 3 カルテ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 4 購入に関する情報 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 5 保有資産情報(土地建物等) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 6 債務情報 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 7 口座番号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 8 遺言書 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 9 与信ブラックリスト | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 10 生年月日 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 11 生年月日(子供) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 12 学歴 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |
| 13 学歴(子供) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 [　　] |

## [第9章]　情報システムの管理者権限（特権ID）についてお伺いします

**[Q54].** 管理者権限(特権 ID)の運用ルールについてお伺いします。(○印はひとつ)

| | | |
|---|---|---|
| 1　管理規則を定めている | 2　管理規則を定めていない | 3　その他 [　　] |

**[Q55].** 管理者権限(特権 ID)に関して重視している施策を 3 つまで選択してください。

| | |
|---|---|
| 1 | 使用者を必要な人のみに限定している |
| 2 | 使用する権限を要求事項に基づいて最小限に限定している |
| 3 | 承認プロセスを記録し、承認されるまで使用を許可しない |
| 4 | 特権業務のアサインが外れた時の手続きを定めている(異動・退職等) |
| 5 | 管理者権限(特権 ID)と、通常業務で使用する ID を分けている |
| 6 | 管理者権限(特権 ID)使用者に関して、力量をレビューしている |
| 7 | システムの構成管理機能に応じて、管理者権限(特権 ID)の使用手順を定めて運用している |
| 8 | 管理者権限(特権 ID)を共有している場合は、秘密認証情報(パスワード等)の管理方法を定めている |
| 9 | その他[　　] |

## [第10章]　日本年金機構の個人情報流出事案に関連してお伺いします

**[Q56].** 日本年金機構の大量個人情報流出の報道を受け、貴社で保有する重要データに対して実施した(予定)のセキュリティ施策はありますか。(複数選択可)

| | | | | | |
|---|---|---|---|---|---|
| 1 | リスクの再分析 | 4 | セキュリティ機器(含ソフトウェア)の導入 | 7 | 保険による対応 |
| 2 | ルール・体制(管理方法)の見直し | 5 | セキュリティ教育(訓練)の実施 | 8 | 現状のまま変更なし |
| 3 | 注意喚起のメッセージ発信 | 6 | セキュリティ施策の監査 | 9 | その他[　　] |

**[Q57].** 不審なメールの受信時におけるルール・通報体制について、お伺いします。(○はひとつだけ)

| | |
|---|---|
| 1 | ルール・通報体制は整備されている |
| 2 | ルール・通報体制は整備され、従業員に周知している |
| 3 | ルール・通報体制は整備され、従業員に周知するとともに不審メール訓練を実施している |
| 4 | ルール・通報体制を検討中・準備中 |
| 5 | 対策をしていない |
| 6 | その他[　　] |

## [第11章]　その他

**[Q58].** 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 | ベネッセ顧客情報流出 | 9 | Yahoo!メールで大規模障害が発生、約380万ユーザーが利用不能 | 17 | 東芝データ流出事件、韓国企業と約330億円で和解 |
| 2 | 「サイバーセキュリティ基本法」が全面施行、NISCは省庁横断の司令塔 | 10 | LINE、乗っ取り対策として「PIN コード」設定を必須化 | 18 | 日本企業のセキュリティ投資額は世界平均の 2 分の 1 |
| 3 | ソニー・ピクチャー・エンターテイメント(SPE)へのサイバー攻撃 | 11 | 米英政府が IE の一時使用停止を呼びかけたゼロデイ脆弱性 | 19 | bashにコードインジェクションの脆弱性「Shellshock」 |
| 4 | 日本年金機構から大量の個人情報が流出 | 12 | 「WordPress 4.2」の更新版公開、全バージョンに深刻な脆弱性存在 | 20 | JALマルウエア感染でマイレージ情報流出 |
| 5 | グーグル地図、皇居内施設や原爆ドームの表示改ざん | 13 | サンリオの委託先の情報漏洩の可能性が 4 社 1 万 4333 人まで拡大 | 21 | 「iCloud」にハッキング攻撃か、セレブのプライベート画像が多数流出 |
| 6 | 企業秘密、海外漏洩を厳罰化　不正競争防止法改正案を閣議決定 | 14 | 「.tokyo」ドメインの詐欺サイトが出現、1万件以上のアクセスを確認 | 22 | 韓国で 2700 万人の個人情報が流出、容疑者 16 人を逮捕 |
| 7 | サイバー攻撃を受けたと認識している企業はおよそ 5 社に 1 社 | 15 | 米中央軍のツイッター等にハッキング　ISISの声明を掲載 | 23 | マイナンバー制度への対応が遅れぎみ、実施・実施予定層は 38% |
| 8 | 経産省、ベネッセ事件等を受けて個人情報ガイドライン改正 | 16 | 韓国の原発情報が流出、北朝鮮関与の可能性も | 24 | 「三菱東京 UFJ 銀行」を騙る偽サイトが再び出現 |

**[Q59].** 次の用語について、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 | SDx | 7 | e ディスカバリ | 13 | やり取り型攻撃 |
| 2 | サイバーセキュリティ基本法 | 8 | サイバー保険 | 14 | SIEM |
| 3 | NISC | 9 | 忘れられる権利 | 15 | ゼロデイ攻撃 |
| 4 | 個人情報保護法改正 | 10 | パーソナルデータの匿名化 | 16 | IoT |
| 5 | IDaaS | 11 | 特定個人情報保護委員会 | 17 | CSMS |
| 6 | 不正競争防止法改正 | 12 | WAF | 18 | M2M |

**[Q60].** 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。