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、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認証取得企業、ISMS認証取得企業、官公庁及び教育機関から4,800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。

［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。
調査回答票は**2016年8月31日（水曜日）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
リスクの分析・評価	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分析・評価すること。
情報セキュリティポリシー（方針・対策基準）	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）が該当し、実施手順等の具体的な手順は含まない。

［ご質問・お問合せ先］

本アンケートに関するお問い合わせは、下記連絡先まで電子メール又はFAXでお願いします。

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/survey.html）
電子メール：harada.survey2016@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].　ご記入者の役職又は相当職　（○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	9　その他［　　］
2　執行役・執行役員	4　部長	6　係長・主任	8　一般社員	

[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)を選択してください。

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)
政府・自治体・大学等は予算額、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]. 貴社の会社種別及び規模 (○印はひとつだけ)

会社の種別					
中小企業		自治体		その他	
1	卸売業であり、資本金 1 億円以下または従業員 100 人以下	5	市区町村であり、人口 30 万人以上	8	1～4 を除く中堅・大企業
2	小売業であり、資本金 5 千万円以下または従業員 50 人以下	6	市区町村であり、人口 10 万人以上 30 万人未満	9	5～7 を除く政府・自治体等
3	情報処理業以外のサービス業であり、資本金 5 千万円以下または従業員 100 人以下	7	市区町村であり、人口 10 万人未満	10	大学
4	上記以外(ソフトウェア業・情報処理サービス業を含む)で、資本金 3 億円以下または従業員 300 人以下			11	その他(1～10 に当てはまらない)

[Q7]. 貴社ではプライバシーマーク(P マーク)、ISMS、BCMS を認証取得していますか。(複数選択可)

1 P マーク認証取得	2 ISMS 認証取得	3 BCMS 認証取得	4 いずれも認証取得していない

[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 認証の維持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の分析・評価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]. リスクの分析・評価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	組織内の改編	6	自社の情報セキュリティ事故発生	10	熊本地震等への対応
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		

[Q11]. リスクの分析・評価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。**リスクの分析・評価を行っていない場合は実施しない理由を、行っている場合は実施時の問題点をお答えください。(各項目の 1～4 で○印はひとつだけ)

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
11-1 実施方法が分かる人材が不足している	1	2	3	4
11-2 収益に直結しない	1	2	3	4
11-3 通常の業務に比べ、優先度が低い	1	2	3	4
11-4 必要となる組織内情報の収集が難しい	1	2	3	4
11-5 上司(経営層等)の理解がない	1	2	3	4
11-6 関係部門の協力が得られない	1	2	3	4
11-7 実施方法が変わって、対応できない	1	2	3	4
11-8 部分的な対応に留まってしまう	1	2	3	4

[Q12]. 情報セキュリティポリシー(方針・対策基準)の策定と見直し状況についてお答えください。(○印はひとつだけ)

1	策定していない【→Q16 へ】	3	年に 1 回、定期的に実施している
2	策定後、一度も見直しを行っていない	4	数年に 1 回、実施している

[Q13]. 情報セキュリティポリシー(方針・対策基準)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)が策定・見直しをしている	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が策定・見直しをしている	5	情報セキュリティポリシーはない
3	情報システム部門・情報セキュリティ部門「以外」の部門が策定・見直しをしている	6	その他 [ ]

[Q14]. 情報セキュリティポリシー(対策基準)についてお伺いします。以下の**対策(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(経営層の方向性表明)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	暗号による対策(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(取外し可能媒体を含む))	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(特権を含む)アクセスの管理	16	システムの取得、開発及び変更保守(外部委託、テストを含む)
7	人的資源のセキュリティ(雇用開始から教育、雇用の終了まで)	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、クリアデスク・クリアスクリーン方針)	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

[Q15]. 情報セキュリティポリシー(対策基準)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の認証取得・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マークの認証取得・更新
5	監査等の指摘事項の対応	10	2013年10月以降の対策(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[ ]

[Q16]. 情報セキュリティマネジメントの仕組みを導入してからの運用期間についてお答えください。(○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

[Q17]. 情報セキュリティに関する支出[注)]についてお伺いします。**売上(政府・自治体・大学等の場合は予算)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。)

注) 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

17-1.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

支出の傾向をお答えください。(各項目の 1～6 で○印はひとつだけ)

	17-2.二期前と前期比較	17-3.前期と今期の比較	17-4.今後の変化
著しく増加(支出の割合 20%以上増)	1	1	1
増加	2	2	2
ほぼ横ばい	3	3	3
減少	4	4	4
著しく減少(支出の割合 20%以上減)	5	5	5
その他	6 [ ]	6 [ ]	6 [ ]

[第3章] IT資産の利用・管理体制に関してお伺いします

[Q18]. 従業員の私有 IT 資産(ハードウェア・ソフトウェア)の業務利用[注)]を認めていますか。(○印はひとつだけ)

注) 業務利用:業務上の情報を取り扱うケース(メールやスケジュール等も含む)

1	認めている(規定等の文書で明文化している)	4	認めていない(規定等の文書で明文化していない)
2	認めている(規定等の文書で明文化していない)	5	決めていない
3	認めていない(規定等の文書で明文化している)	6	不明・わからない

[Q19]. 業務で利用しているIT資産について、どの程度管理できていると考えていますか。（各項目の1～5で○印はひとつだけ）

管理対象		全て管理できている	概ね管理できている	あまり管理できていない	全く管理できていない	不明・わからない
19-1	社有ハードウェア	1	2	3	4	5
19-2	社有ソフトウェア	1	2	3	4	5
19-3	私有ハードウェア	1	2	3	4	5
19-4	私有ソフトウェア	1	2	3	4	5

[Q20]. 業務で利用しているIT資産について、どのようなセキュリティ対策を実施していますか。（複数選択可）

紛失・盗難	1 外部への持ち出し禁止	マルウエア等	12 アプリケーションの使用制限
	2 デバイスのパスワードの設定		13 公式マーケット以外の利用禁止
	3 リモートワイプ／ロック		14 ウイルス対策ソフトの導入
	4 外部記憶媒体（SDカード等）の使用制限		15 OSのアップデート
	5 内部/外部記憶媒体の暗号化		16 アプリケーションのアップデート
ネットワーク	6 内部ネットワークへのアクセス制限		17 ハードウェアの改造禁止
	7 通信の暗号化（VPNなど）	その他	18 規定やガイドライン等を策定・改定
	8 無線LANの使用制限（公衆無線LANのみ制限）		19 台帳管理
	9 無線LANの使用制限（全ての無線LANの制限）		20 機能（GPS、カメラなど）の使用制限
	10 リモートアクセス時のパスワード		21 MDM（モバイルデバイス管理）
	11 業務システム利用時のパスワード		22 その他[ ]

[Q21]. IT資産管理・運用に関して、どのようなセキュリティ課題や懸念事項がありますか。（複数選択可）

1	紛失／盗難されたハードウェア等からの情報漏えい	7	なりすまし（リモートアクセスや業務システム）
2	ユーザの意図しない情報開示（GPS情報など）	8	ダイヤラー（SMSや電話を勝手に利用するアプリ）
3	廃棄するハードウェア等のデータ復元による情報漏えい	9	ネットワークの利用不可（輻輳による）
4	フィッシング	10	IT資産利用に関するルール違反（手続き省略等）
5	マルウエア	11	セキュリティ対策・管理コストの問題
6	通信の盗聴（無線LANなどから）	12	その他[ ]

[Q22]. 今後、貴社の役員・各部門へ私有IT資産の業務利用を認める予定はありますか。（各項目の1～2で○印はひとつだけ）

対象	22-1 役員（経営層）	22-2 営業部門	22-3 事務部門	22-4 技術開発部門	22-5 システム運用部門	22-6 生産管理部門	22-7 販売部門	22-8 その他
認める予定はない	1	1	1	1	1	1	1	1
認める予定はある（限定的な利用も含む）	2	2	2	2	2	2	2	2
不明・わからない	3	3	3	3	3	3	3	3

［第4章］情報セキュリティ対策に関してお伺いします

[Q23]. 情報セキュリティ対策として実施している項目は何ですか。（複数選択可）

1	主要な情報資産について、情報セキュリティ対策実施手順を策定している
2	情報システム運用等の外部委託先に対し、指導や監査を実施している
3	緊急時対応計画（情報セキュリティに関する事故及び障害等が発生した場合の体制と対応手順）を整備している
4	CIO（Chief Information Officer：情報統括責任者）を任命している
5	CISO（Chief Information Security Officer：最高情報セキュリティ責任者）を任命している
6	情報システム（電子メール、電子掲示板、スケジュール管理、文書管理等）に関する運用管理規程を策定している
7	情報システムに関する障害時マニュアルを策定している
8	情報システムに関する利用者研修を、採用時等に実施している
9	ネットワーク、情報システム（基幹業務系を含む）及び端末等に関する情報システム台帳を整備している
10	情報システムの最適化や調達などのため、SLA（契約を行う際に、あらかじめ、事業者などから提供されるサービスの内容と範囲、品質に対する要求（達成）水準を明確化して、合意しておくこと）を導入している
11	情報システムの最適化や調達などのため、SLM（サービスレベルの最適化を継続的に行うための運営手法）を導入している
12	情報セキュリティポリシー等の順守状況について、自己点検（自ら導入した個々の対策の効果や達成度を、チェックリストなどを使い評価すること）を実施している

[Q24]. 情報セキュリティ対策を推進する上での難しさについて、最も当てはまるものはどれですか。
（各項目の 1～6 で○印はひとつだけ）

情報セキュリティ対策	難しくない	どちらかといえば難しくない	どちらかといえば難しい	難しい	とても難しい	わからない
24-1 予算を確保すること	1	2	3	4	5	6
24-2 推進する組織が、内部から評価を得ること	1	2	3	4	5	6
24-3 組織の情報セキュリティレベルを把握すること	1	2	3	4	5	6
24-4 重要性を組織に浸透させること	1	2	3	4	5	6
24-5 業務効率の低下を防ぐこと	1	2	3	4	5	6
24-6 費用対効果を説明すること	1	2	3	4	5	6
24-7 経営層に必要性を説得すること	1	2	3	4	5	6
24-8 実施する技術・ノウハウを獲得すること	1	2	3	4	5	6
24-9 情報セキュリティのルールを従業員に順守させること	1	2	3	4	5	6
24-10 従業員の作業負担増を防ぐこと	1	2	3	4	5	6
24-11 効果を測定すること	1	2	3	4	5	6
24-12 推進する組織体制を整備・運営すること	1	2	3	4	5	6
24-13 実施する人材を確保すること	1	2	3	4	5	6
24-14 従業員に情報セキュリティ教育を実施すること	1	2	3	4	5	6
24-15 利便性の低下を防ぐこと	1	2	3	4	5	6

[Q25]. 情報セキュリティ監査（審査を含む）の実施（過去 1 年間）についてお答えください。（○印はひとつだけ）

1	情報セキュリティについて内部監査のみを実施	3	情報セキュリティについて内部監査及び外部監査共に実施
2	情報セキュリティについて外部監査のみを実施	4	実施していない

[Q26]. 情報システムに関する事業継続計画（BCP）の策定状況等についてお伺いします。

26-1.事業継続計画の策定の有無をお答えください。（○印はひとつだけ）

1	策定済	2	本年度中に策定済み、もしくは策定予定	3	平成 29 年度以降に策定予定	4	策定予定はない

26-2. 事業継続に関する訓練の実施状況についてお答えください。（複数回答可）

1	IT 部門だけで机上訓練[注 1)]を行っている	5	サプライヤー等の関係事業者を含めた大規模な実地訓練を行っている
2	組織の業務関連部門を含め机上演習を行っている		
3	IT 部門だけで実地訓練[注 2)]を行っている	6	訓練を行っていない（策定していないを含む）
4	組織の業務関連部門を含め実地訓練を行っている		

注 1）机上訓練：要員が一室に集まり、役割と事業継続手順を確認する等　注 2）実地訓練：要員が実際に行動し検証する等

[Q27]. 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」があればお答えください。（複数選択可）

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

［第5章］ 情報セキュリティインシデント対応の体制と人材育成に関してお伺いします

[Q28]. 情報セキュリティインシデント（ウイルス感染、不正アクセス等）に関わる以下の業務を主に担当しているのはどこですか。
（各項目の 1～5 で○印はひとつだけ）

		情報セキュリティ専門の部門または専任者	情報セキュリティ専門外の部門または兼務者	外部に委託	決めていない	不明・わからない
28-1	情報セキュリティインシデント対応ルールの策定・改定	1	2	3	4	5
28-2	情報セキュリティインシデント発生時の初動対応（原因調査、対応策の検討・実施を含まない）	1	2	3	4	5
28-3	情報セキュリティインシデント発生時の外部の専門家との窓口	1	2	3	4	5
28-4	情報セキュリティインシデントの原因調査、対応策の検討・実施	1	2	3	4	5

[Q29]. 情報セキュリティインシデント対応を担当する専門の部門または専任者の設置について、貴社の考えに一番近いものをお答えください。（○印はひとつだけ）

1	専門の部門の設置・強化、または専任者の増員を予定している（新設または強化を予定）
2	専門の部門は設置済みであり、専任者の増員予定はない（設置済み・現状維持）
3	専門の部門または専任者はなく、設置の予定もない（未設置または兼任・現状維持）
4	専門の部門の廃止、または専任者の削減を予定している（削減を予定）
5	決めていない
6	不明・わからない

[Q30]. 情報セキュリティインシデント対応における最終的な指示・決定を行う方の役職に該当するものをお答えください。（○印はひとつだけ）

1	経営層（取締役以上）	5	係長・主任クラス
2	CIO または CISO	6	その他[ ]
3	部長クラス（事業部長・部長等）	7	決めていない
4	課長クラス	8	不明・わからない

[Q31]. 情報セキュリティインシデント対応の専任者の育成方針について、該当するものをすべてお答えください。（複数選択可）

1	中堅者のなかから育成する（勤続年数が長い従業員・組織内の業務に精通している従業員を育成）
2	若手のなかから育成する（勤続年数が少ない従業員・組織内の業務経験が浅い従業員を育成）
3	情報セキュリティの専門知識がある者を採用する（中途採用・新卒採用・出向受け）
4	情報セキュリティの専任者を育成する必要はない（外部の専門家に任せるなど）
5	その他[ ]
6	育成方針を決めていない
7	育成方針は不明・わからない

[Q32]. 情報セキュリティインシデント対応の専任者に必要と考えるスキル（知識・ノウハウ）は何ですか。（複数選択可）

1	判断力	8	インターネット、ネットワークに関する知識
2	コミュニケーション能力・調整力	9	情報セキュリティマネジメントに関する知識（ISMS 等）
3	行動力・リーダーシップ能力	10	コンピュータ・ネットワークの脅威に関する知識（ウイルス、不正アクセス等）
4	問題解決能力	11	情報システムに関する知識・ノウハウ（バックアップ、セキュリティパッチ等）
5	マネジメント力・時間管理能力	12	情報セキュリティインシデント対応の実践経験
6	法律・社会制度関連の知識・ノウハウ	13	その他[ ]
7	組織の制度・業務関連の知識・ノウハウ		

［第6章］ クラウド利用状況および利用における課題についてお伺いします

[Q33]. クラウドサービスの利用状況についてお答えください。（各項目の 1～6 で○印はひとつだけ）

サービス種別		利用中				利用予定あり	利用予定なし
		情報システム部門主導		その他部門主導			
		全社導入	部門導入	全社導入	部門導入		
33-1	[コミュニケーション・コラボレーション] メール/グループウェア/文書管理/ワークフロー	1	2	3	4	5	6
33-2	[業務システム] e-learning/人事給与/財務会計/営業支援/CRM/ERP/データ分析	1	2	3	4	5	6
33-3	[業務インフラ] 仮想デスクトップ/オンラインストレージ	1	2	3	4	5	6
33-4	[システムインフラ] サーバー利用/システム開発・テスト/Web サイト構築/認証・セキュリティ	1	2	3	4	5	6
33-5	その他 [ ]	1	2	3	4	5	－

[Q34]. クラウドサービスに対する組織の方針についてお答えください。（○印はひとつだけ）

1	優先的にクラウドサービスを利用している	3	クラウドサービスは利用しない
2	対象業務・扱うデータに応じてクラウドサービスを利用する	4	クラウドサービスについてよく分からない、判断できない

[Q35]. クラウドサービス利用における規定やガイドラインを整備していますか。（○印はひとつだけ）

1	整備している	2	整備する予定	3	整備されていない	4	わからない

[Q36]. クラウドサービス利用の阻害要因、および懸念することについてお答えください。（複数選択可）

1	情報漏えいなどのセキュリティに不安感がある	7	経営層・承認者の理解が得られない
2	サービスの安定性・継続性に不安感がある	8	クラウドサービス導入を推進する人材がいない
3	自社のセキュリティ要件を満たさない、コンプライアンスを確保できない	9	IT ベンダーよりクラウドサービス導入の提案がない
4	契約内容（利用規約・約款・法律準拠・SLA）に合意できない	10	自社業務に合わない [具体的な業務内容:]
5	費用対効果が出ない、メリットがない	11	クラウドサービスを利用する必要がない [理由:]
6	クラウド事業者の公開情報が不十分である	12	その他 [ ]

[Q37]. クラウド事業者の選定において重視する点を 3 つまで選択してください。（○印は 3 つまで）

1	ブランド	8	BCP 対応（バックアップサイトなど）
2	経営の健全性	9	利用コスト
3	データセンターの場所（国内/国外）	10	第三者認証、認定
4	国内法準拠かどうか	11	SLA（Service Level Agreement）
5	提供されるサービス内容・機能	12	サプライチェーン構造とガバナンス
6	サービスが自社業務に合わせてカスタマイズ可能か	13	サポート体制
7	利用事例・実績	14	その他 [ ]
8	セキュリティ対策		

[Q38]. クラウド事業者が取得している第三者認証、認定について、知っているもの、および重視するものをお答えください。（複数選択可）

		知っている	重視する
38-1	ISMS	1	2
38-2	P マーク	1	2
38-3	SOC 報告書	1	2
38-4	PCI DSS	1	2
38-5	STAR 認証（クラウドセキュリティ認証）	1	2
38-6	ASP・SaaS の安全・信頼性に係る情報開示認定制度	1	2
38-7	IaaS・PaaS の安全・信頼性に係る情報開示認定制度	1	2
38-8	ISO/IEC 27018（クラウドサービスにおける個人情報保護）	1	2
38-9	ISO/IEC 27017（クラウドセキュリティ認証）	1	2
38-10	CS マーク（クラウド情報セキュリティ監査）	1	2

［第7章］ アプリケーションセキュリティのリスク管理に関してお伺いします。

※ 本章において、アプリケーションとはウェブアプリケーションやモバイルアプリ等を指します。
※ アプリケーションセキュリティとは、ウェブページの改ざん、重要情報の搾取、サービス拒否等の攻撃からこれらのアプリケーションを守ることを指します。
※ セキュアコーディングとは、アプリケーション開発の際に、脆弱性をもたないようにプログラミングすることです。

[Q39]. アプリケーションセキュリティのリスク管理は、誰が担当していますか。（複数選択可）

1	CIOまたはCISO	3	品質保証責任者	5	不明・わからない
2	ソフトウェア開発責任者	4	システム運用部門の責任者	6	その他[ ]

[Q40]. 運営中のすべてのウェブやモバイルのアプリケーションをどの程度管理していますか。（○印はひとつだけ）

1	全て管理できている	3	あまり管理できていない	5	不明・わからない
2	概ね管理できている	4	全く管理できていない		

[Q41]. 貴社のアプリケーションの開発運営形態に当てはまるものはどれですか。（複数選択可）

1	独自開発	3	パッケージソフトウェアの導入
2	第三者（外注）の開発	4	その他[ ]

[Q42]. この一年でアプリケーションセキュリティのリスクに変化があったと考えていますか。（○印はひとつだけ）

1	非常に増加している	3	変化はない	5	非常に減少している
2	増加している	4	減少している	6	不明・わからない

[Q43]. アプリケーションセキュリティのリスク管理の目的で一番重視しているものを選択してください。（○はひとつだけ）

1	ブランドの保護	2	情報漏えいの防止	3	業務の中断時間の抑制	4	その他[ ]

[Q44]. 脆弱性のあるアプリケーションのリスクへの対策として何を実施していますか。（複数選択可）

1	開発者向けのセキュアコーディング教育の実施	4	ソースコードレベルの脆弱性検査	7	実施していない
2	セキュアコーディングガイドの提供	5	運用段階での脆弱性診断	8	その他 [ ]
3	開発段階の脆弱性診断	6	外部専門会社の脆弱性診断		

[Q45]. アプリケーションセキュリティのリスク管理ができない理由を選択してください。（複数選択可）

1	十分な予算が確保できない	4	リーダーシップの不足	7	アプリケーションリリースへの抵抗感
2	アプリケーションの脆弱性の増加	5	テストツールの不足	8	その他[ ]
3	専門知識の不足	6	組織内での優先順位が低い	9	特にない

［第8章］ マイナンバーの取り組みに対してお伺いします。

[Q46]. マイナンバー制度の内容について、ご存知のものを選択してください。（複数選択可）

1	マイナンバーの取り扱いと、従来の個人情報の取り扱いには違いがある
2	マイナンバーが漏えいすると個人が特定される可能性がある
3	マイナンバーは、平成 15 年に制定された個人情報保護法では規定されていなかった
4	マイナンバー制度の新設などにより、平成 27 年に改正個人情報保護法が成立・公布された
5	マイナンバー制度では、従業員が不正目的でマイナンバーを漏えいさせた場合、本人と法人が罰せられる

[Q47]. 従業員のマイナンバーの取り扱いについて、取り組んだ事について選択してください。(複数選択可)

1	マイナンバーをアクセス権限のあるデータベースで厳密に管理している
2	マイナンバーを物理的に施錠して保管している
3	マイナンバーの導入にあたって、新しく情報システムを構築・導入した
4	マイナンバーを、個人情報を管理している情報システムで管理している
5	マイナンバーの導入にあたっては、情報システムでは管理せずに、紙で管理している
6	マイナンバーを管理するパッケージを購入して管理している
7	マイナンバーに関する新たなポリシーやルールを導入した
8	マイナンバーについて従業員教育を実施した
9	回答できない

[Q48]. 以下の違法行為について、従業員への教育状況を選択してください。(各項目の 1～3 で○印はひとつだけ)

マイナンバーに関する違法行為		選択項目		
		全ての従業員に教育している	取り扱う従業員だけ教育している	特に教育していない
48-1	従業員が正当な理由なく、個人の秘密が記録された特定個人情報ファイルを他人に提供する行為	1	2	3
48-2	従業員が業務に関して知り得たマイナンバーを自己は第三者の不正な利益を図る目的で提供し、または盗用する行為	1	2	3
48-3	従業員が個人情報保護委員会の命令に違反する行為	1	2	3
48-4	従業員がマイナンバーについて虚偽の報告、虚偽の資料提出、答弁や検査の拒否、検査妨害などをする行為	1	2	3
48-5	職権を乱用して、職務以外の目的で個人の秘密に属する特定個人情報が記録された文書などを収集する行為	1	2	3
48-6	自治体において、情報連携や情報提供ネットワークシステムの業務に関して知り得た秘密を洩らし、または盗用する行為	1	2	3

[第9章] その他

[Q49]. 次の出来事について、ご存知のものを選択してください。(複数選択可)

1	Yahoo!メールで約 97 万 ID の約 258 万通の新着メールが消失	6	複数のマスメディアでゼロデイ攻撃により個人情報が流出	11	Baidu 社の Android 用 SDK にバックドア機能や不正プログラムを確認
2	不動産店従業員が芸能人の賃貸物件情報を Twitter へ投稿	7	ポップアップがサイト閲覧のみで表示されるゼロクリック詐欺の登場	12	レノボ社 ThinkPad シリーズに外部への個人情報送信疑惑
3	日本年金機構の個人情報流出事故をうけ CSIRT の体制強化を勧告	8	暗号化型ランサムウェアの vvv ウイルスが日本でも相当数流入	13	AndroidOS 9 億 5 千万台のスマホに影響をあたえる脆弱性が発覚
4	標的型サイバー攻撃相談件数が前年比 6 倍に増加	9	Google Chrome、Windows XP/Vista のサポートが 2016 年 4 月に終了	14	米国で普及しているガレージドア用リモコンに脆弱性が発覚
5	全国初の無線 LAN ただ乗りによる電波法違反容疑で逮捕者	10	Gmail で、暗号化されていないメールに警告アイコン表示機能が追加	15	2015 年 9 月米中サイバーセキュリティ合意でサイバー戦争回避

[Q50]. 次の用語ついて、ご存知のものを選択してください。(複数選択可)

1	スタックスネット	9	不正アクセス禁止法	17	CISSP
2	MITB攻撃	10	公認情報セキュリティ監査人資格制度	18	SOC
3	個人情報保護法改正	11	OWASP	19	CSIRT
4	標的型攻撃	12	Wordpressの脆弱性	20	ブロックチェーン
5	CTF	13	RSA Conference	21	フィンテック
6	eディスカバリ	14	Security Intelligence	22	FIDO
7	SIEM	15	EDR(Endpoint Detection and Response)	23	ウェアラブル機器
8	WAF	16	Bug Bounty(バグ発見報奨)	24	機械学習

[Q51]. 本アンケートに対す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。