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4,500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。

[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**2017年8月31日（木曜日）までにご投函**くださいますようお願い申し上げます。

[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.survey2017@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	9	5～7 を除く政府・自治体等
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	10	大学
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	11	その他(1～10 に当てはまらない)
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	8	1～4 を除く中堅・大企業		

[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）
※リスク分析評・価とは、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分析・評価すること。

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【→Q12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	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		

[Q11]. リスク分析・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・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	数年に一回、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、過去 3 年間に新規導入・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、マルウェア対策、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	モバイル端末(スマートフォン、携帯)利用拡大	8	個人情報保護法改正への対応
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	9	その他法律・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	10	情報セキュリティ事件・事故(サイバー攻撃、情報漏洩、マルウェア感染等)の増大
5	監査等の指摘事項の対応		
6	事業継続計画(BCP/BCM)と緊急時対応	11	過去3年間は対策(管理策)の見直しがない
7	ISMSやPマークの認証取得・更新	12	その他 [ ]

[Q16]. 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1～5で○印はひとつだけ)

情報セキュリティ対策を推進する上での難しさ	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	わからない
16-1 実施する人材を確保すること	1	2	3	4	5
16-2 実施する技術・ノウハウを獲得すること	1	2	3	4	5
16-3 費用対効果を説明すること	1	2	3	4	5
16-4 予算を確保すること	1	2	3	4	5
16-5 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
16-6 重要性を組織に浸透させること	1	2	3	4	5
16-7 業務効率の低下を防ぐこと	1	2	3	4	5
16-8 利便性の低下を防ぐこと	1	2	3	4	5
16-9 従業員の作業負担増を防ぐこと	1	2	3	4	5
16-10 効果を測定すること	1	2	3	4	5
16-11 経営層に必要性を説得すること	1	2	3	4	5
16-12 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
16-13 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
16-14 推進する組織体制を整備・運営すること	1	2	3	4	5
16-15 推進する組織が、内部から評価を得ること	1	2	3	4	5

[Q17]. 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(政府・自治体・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

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(17-2と3)をお答えください。 また、**組織全体の売上(予算)について前期から今期にかけての動向(17-4)**を教えてください。(各項目の 1～6 で○印はひとつだけ)

	著しく増加(20%以上増)	増加	ほぼ横ばい	減少	著しく減少(20%以上減)	その他
17-2 前期と今期の**支出比較**	1	2	3	4	5	6
17-3 今後の**支出変化**	1	2	3	4	5	6
17-4 **組織全体の売上(予算)の動向**	1	2	3	4	5	6

[Q18]. 以下に挙げた情報セキュリティに関するガイドラインについて、どの程度認知しているか、**最も近いものの番号に○印を付けてください。**（各項目の 1～4 で○印はひとつだけ）

内容		内容を理解している	読んだことはあるが内容を覚えていない	知っているが読んだことは無い	知らなかった
18-1	情報セキュリティ管理基準(経済産業省)	1	2	3	4
18-2	情報セキュリティ監査基準(経済産業省)	1	2	3	4
18-3	サイバーセキュリティ経営ガイドライン(経済産業省)	1	2	3	4
18-4	情報セキュリティガバナンス導入ガイダンス(経済産業省)	1	2	3	4
18-5	情報セキュリティ監査企業台帳(経済産業省)	1	2	3	4
18-6	情報セキュリティ対策ビデオ(警察庁)	1	2	3	4
18-7	@police セキュリティポータルサイト (警察庁)	1	2	3	4
18-8	サイバーセキュリティ戦略(閣議決定)	1	2	3	4
18-9	情報セキュリティハンドブック(内閣サイバーセキュリティセンター)	1	2	3	4
18-10	地方公共団体における情報セキュリティポリシーに関するガイドライン(総務省)	1	2	3	4
18-11	IoT セキュリティガイドライン(総務省)	1	2	3	4

［第3章］個人情報保護法の改正についてお伺いします

[Q19]. 保有個人データ※の保有件数についてお答えください。（○印はひとつだけ）
※保有個人データ:開示等および第三者への提供の停止を行うことのできる権限を有する個人データ

1 5,000 件以下	2 5,001 件～50,000 件	3 50,001 件以上	4 わからない

[Q20]. 改正個人情報保護法への理解度についてお答えください。（○印はひとつだけ）

改正項目		十分理解している	およそ理解している	知っているがあまり理解はしていない	知らない
20-1	中小規模事業者特例(5,000 人要件)の廃止	1	2	3	4
20-2	個人識別符号	1	2	3	4
20-3	匿名加工情報	1	2	3	4
20-4	要配慮個人情報	1	2	3	4
20-5	第三者提供に係る記録等の義務	1	2	3	4
20-6	第三者提供のオプトアウトに対する規制	1	2	3	4
20-7	外国にある第三者への提供	1	2	3	4
20-8	個人データの消去努力義務	1	2	3	4
20-9	個人情報データベース等盗用罪	1	2	3	4

[Q21]. 個人情報保護法改正に対する対応のため，実施した施策についてお答えください。(複数回答可)

1 個人情報保護方針，規程類の新規作成	8 新たな物理的安全管理措置の導入
2 個人情報保護方針，規程類の見直し	9 新たな技術的安全管理措置の導入
3 社内管理体制の構築・見直し	10 委託先管理についての見直し
4 従業者教育の実施	11 外国にある第三者への提供の見直し
5 保有する個人情報の棚卸し	12 その他
6 個人情報の取扱いフローの見直し	13 特に施策は実施していない
7 リスク分析・評価の実施	

［第4章］情報セキュリティガバナンス体制に関してお伺いします

本章において、「情報システム部門」とは、会社の情報システムの企画、開発、運用、委託を行っている部門をいい、兼務を含みます。
「IT セキュリティ」とは、サイバーリスクに対するネットワークなどの技術的対策やウイルス対策ソフトなどのセキュリティ製品の導入・運用などをいいます。

[Q22]. 社長を補佐して、会社としての情報セキュリティの責任を負っている責任者（以下、情報セキュリティ責任者といいます）の職位をお答えください。（○印はひとつだけ）

1 役員クラス(CISO)	3 課長クラス	5 社長の他にはいない
2 部長クラス	4 その他［ ］	

[Q23]. 情報セキュリティ責任者に最も期待する役割をお答えください。(○印はひとつだけ)

1	情報セキュリティに関する投資やリスクの受容(リスクを受け入れるかどうか)等に関する経営判断
2	経営者との意思疎通(経営者がわかる視点、言葉での説明により、判断や理解を促す)
3	IT セキュリティの技術対策の導入判断や推進(セキュリティ製品、サイバーセキュリティ対策など)
4	情報セキュリティや内部統制の推進(全社規程整備や全組織への徹底、社員教育など)
5	個人情報保護法などの法令順守徹底
6	インシデント発生時の対応の指揮や指示(大規模な情報漏洩やサイバー攻撃への対応の陣頭指揮)
7	組織内での情報セキュリティに関する調整役(部門間の調整や説明、コミュニケーション)
8	その他 ( )

[Q24]. 情報セキュリティ責任者が主としている職務をお答えください。(○印はひとつだけ)

1	情報セキュリティ	4	リスクマネジメント	7	総務
2	情報システム	5	法務	8	その他 [ ]
3	内部統制	6	人事		

[Q25]. 情報セキュリティ上の要請と、情報システム上の要請が対立するとき(例えば、運用上の困難、IT コストの上昇、効率性の低下など)の対応についてお答えください。

25-1 優先順位の判断(リスク判断)をする主な部門をお答えください。(1～5 で○印はひとつだけ)

	経営者	情報セキュリティ部門	情報システム部門	いない・決まっていない	その他(他部門、委員会等)
判断する主な部門等	1	2	3	4	5 [ ]

25-2 リスクを判断する部門が IT セキュリティを実行する部門を説得するために必要と考えることをお答え下さい。(複数選択可)

1	経営者の指示	4	予算を持っていること	7	その他
2	情報システムの運用や投資の事情に通じていること	5	IT セキュリティを実行する部門が判断するので説得不要		( )
3	IT セキュリティの知識、リスク状況、対策の相場等の知見があること	6	説得はできない		

[Q26]. 情報セキュリティ部門と情報システム部門の関係についてお答えください。

26-1 情報セキュリティ部門と情報システム部門とは独立してあるべきだと考えるかどうかをお答えください。(○印はひとつだけ)

1 はい	2 いいえ	3 どちらともいえない・わからない	4 その他 [ ]

26-2 その理由をお答えください。(複数選択可)

1	使命が違い、情報システムへの牽制となる	4	専門性が違う	7	部門間の連携で十分
2	情報システムも幅広く事業視点がある	5	社内への行政力	8	わからない
3	情報セキュリティとサイバーセキュリティは別である	6	分けているのは非効率	9	その他 [ ]

[第5章] Webアプリケーションセキュリティ管理の状況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。

[Q27]. Web アプリケーションセキュリティの管理に当たって、貴社の主な役割として最も当てはまるものはどれですか。(○印はひとつだけ)

1	Webアプリケーション開発	4	外部委託して実施
2	Webアプリケーション運営	5	実施していない
3	Webアプリケーション開発運営両方	6	不明・わからない

[Q28]. Web アプリケーションセキュリティ対策を適用しているものを選択してください。(複数選択可)

1	公開用Webアプリケーション	5	クラウドサービスプロバイダが管理する商用アプリケーション
2	外部委託先によって開発されたカスタムアプリケーション	6	既存のWebアプリケーション
3	社内で管理する商用アプリケーション	7	不明・わからない
4	サードパーティのオープンソースアプリケーション	8	その他 [ ]

[Q29]. これまでに受けた攻撃と被害状況についてご回答ください。(○印はひとつだけ)

被害発生の原因	攻撃を受け被害が出た	攻撃を受けたが被害なし	攻撃を受けたことがない	攻撃を受けたか分からない
29-1 Web アプリケーションの脆弱性	1	2	3	4
29-2 OS/ミドルウェアの脆弱性	1	2	3	4
29-3 マルウェアによる情報漏洩・毀損	1	2	3	4
29-4 その他/攻撃手法不明	1	2	3	4

[Q30]. 貴社で使用している Web アプリケーションで危険性の高い情報漏えい又はクロスサイトスクリプティングなどの脆弱性が発見された場合、実施するセキュリティ対策と、対策又は修正に要する平均時間をお答えください。
（各項目の 1～9 で○印はひとつだけ）

セキュリティ対策の実施内容	対策又は修正に要する平均時間								
	1 日以内	数日	1週間	1ヶ月～3ヶ月	3ヶ月～6ヶ月	1年以内	対応しない	不明・わからない	その他
30-1 Secure SDLC（開発手順）の実践を通して根本的な原因を修正する	1	2	3	4	5	6	7	8	9
30-2 サードパーティのオープンソースソフトウェアをアップグレードする	1	2	3	4	5	6	7	8	9
30-3 任意のソースコードパッチで修正する	1	2	3	4	5	6	7	8	9
30-4 アプリケーションの機能を無効にする	1	2	3	4	5	6	7	8	9
30-5 運営環境でネットワークアーキテクチャ、その他の保護メカニズムで対応する	1	2	3	4	5	6	7	8	9
30-6 WAFのルール設定 /バーチャルパッチを適用する	1	2	3	4	5	6	7	8	9
30-7 脆弱性診断を実施する	1	2	3	4	5	6	7	8	9
30-8 次期システム導入を検討・導入する	1	2	3	4	5	6	7	8	9
30-9 その他[ ]	1	2	3	4	5	6	7	8	9

[Q31]. 危険性の高い情報漏えい又はクロスサイトスクリプティングなどの脆弱性のある Web アプリケーションのリスクを減らすために、どのような活動をしていますか？ （複数選択可）

31-1 開発段階	1	開発者向けのセキュアコーディング教育の実施	4 Secure SDLC（開発手順）の導入	7	開発段階のツールによる脆弱性診断
	2	脅威の評価	5 Secure ライブラリ導入	8	その他 [ ]
	3	セキュアコーディングガイドを提供	6 開発段階のツールによる脆弱性診断		
31-2 運用段階	1	運用段階のソースコードレベルの脆弱性検査	4 WAF /バーチャルパッチの導入	7	SOC運営又は委託
	2	専門家による脆弱性診断	5 監査又はコンプライアンス遵守活動	8	その他 [ ]
	3	ツールによる脆弱性診断	6 ISMSなどの認証取得		

[Q32]. Web アプリケーションのセキュリティリスクが十分に管理されてない理由に当てはまるものはどれですか? （複数選択可）

1 不十分な予算	4 独自の専門知識の不足	7 開発チームと運営チームとの連携が難しい
2 短い開発スケジュール	5 効果的なテストツールの欠如	8 不明・わからない
3 組織が高い優先順位で考慮していない	6 セキュリティ教育の欠如	9 その他 [ ]

[Q33]. 脆弱性発見時のレポートの手順と修正手順がありますか。（○印はひとつだけ）

1 ある	2 ない	3 不明・わからない

[第6章]人工知能技術に関してお伺いします

本章において意味する人工知能(以下 AI)技術とはコールセンター業務や記事の作成など企業で活用しているものとし、スマートフォンやパソコンに標準搭載されているものや翻訳サイト等に導入されているものを除きます。

[Q34]. 貴社の AI 技術の導入状況について最も近いものを選択してください。（○印はひとつだけ）

1 導入し積極的に活用している	2 導入してないが導入予定	3 導入予定なし、または不明

[Q35]. AI 技術を業務で導入した際の利点として考えられるものを選択してください。（複数選択可）

1 人件費の削減	4 新たなサービスの提案・開発	7 利点はない
2 業務の自動化・効率化	5 他企業との提携・差別化	8 よくわからない
3 新事業への展開	6 セキュリティの強化	9 その他 [ ]

[Q36]. AI 技術を業務や他企業との提携で導入した際のリスクとして考えられるものを選択してください。（複数選択可）

1 人材育成	4 著作権などの権利問題	7 リスクはない
2 顧客の減少やクレーム	5 AIによる企業秘密の流出	8 よくわからない
3 AIによる法律違反	6 AIの学習への情報提供	9 その他 [ ]

[Q37]. AI 技術を業務に導入することへの考えで最も近いものを選択してください。（○印はひとつだけ）

1 業務全般で積極的に活用すべき	3 法律や制度である程度制限すべき	5 よくわからない
2 活用すべきだが一部に限る	4 まだAI技術を活用すべきではない	6 その他 [ ]

［第7章］ 緊急時対応の実効性に関してお伺いします

以下に挙げる状況が発生した場合を想定して、各質問にご回答ください。

状況 1　自社 Web サイトの改ざん：自社 Web サイトが不正に改ざんされていることを発見した。

状況 2　ランサムウェアへの感染：自分の PC がコンピュータウィルスに感染した。全てのファイルが暗号化され操作不能となり、画面には「身代金」を要求するメッセージが表示されている。

状況 3　ソーシャルエンジニアリング：警察を名乗る男から「貴社のメールサーバーがハッカーに乗っ取られているので、セキュリティ担当者の氏名と連絡先を教えてほしい」と要請された。（電話の相手が本物か確認できない）

[Q38]. 各状況を想定した／適用可能な文書（手順書等）は策定していますか？（各項目の 1～3 で○印はひとつだけ）

状況	策定している	策定していない	不明・わからない
38-1　自社 Web サイトの改ざん	1	2	3
38-2　ランサムウェアへの感染	1	2	3
38-3　ソーシャルエンジニアリング	1	2	3

[Q39]. 各状況に遭遇した場合、誰にどうやって連絡したら良いか知っていますか？（各項目の1～4 で○印はひとつだけ）

状況	知っており、すぐに連絡できる	知っているが、連絡先は覚えていない	文書に記載していない	不明・記載しているかわからない
39-1　自社 Web サイトの改ざん	1	2	3	4
39-2　ランサムウェアへの感染	1	2	3	4
39-3　ソーシャルエンジニアリング	1	2	3	4

[Q40]. 各状況を想定した教育・研修を実施したことはありますか？（各項目の 1～4 で○印はひとつだけ）

状況	実施したことがある	類似事例なら実施したことがある	実施したことは無い	不明・わからない
40-1　自社 Web サイトの改ざん	1	2	3	4
40-2　ランサムウェアへの感染	1	2	3	4
40-3　ソーシャルエンジニアリング	1	2	3	4

[Q41]. 各状況を想定した訓練を実施したことはありますか？（各項目の 1～4 で○印はひとつだけ）

状況	実施したことがある	類似事例なら実施したことがある	実施したことは無い	不明・わからない
41-1　自社 Web サイトの改ざん	1	2	3	4
41-2　ランサムウェアへの感染	1	2	3	4
41-3　ソーシャルエンジニアリング	1	2	3	4

［第8章］情報セキュリティ人材に関する状況についてお伺いします

[Q42]. 自社の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の担当者の有無について教えてください。（各項目の 1～6 で○印はひとつだけ）

		いる			いない		不明・わからない
		専任者がいる	兼務者がいる	外部に委託している	必要だが予算/人がいない	不要と考えている	
42-1	インシデント対応の全体を管理し、指揮命令ができる技術者	1	2	3	4	5	6
42-2	ウイルスの解析やフォレンジック調査などができる技術者	1	2	3	4	5	6
42-3	セキュリティポリシーやセキュリティ設計などが正しく実装されているかを評価、確認できる技術者	1	2	3	4	5	6
42-4	セキュリティ教育や啓発など、リテラシー向上を行うことができる技術者	1	2	3	4	5	6

[Q43]. 情報セキュリティ担当者を育成するためのキャリアパスはありますか？（○印はひとつだけ）

1	ある（将来的なセキュリティパスとして CISO などのセキュリティ責任者の役職にするなど）
2	決めていない
3	不明・わからない
4	その他［　　］

[Q44]. 情報セキュリティ業務の担当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9章］ その他

[Q45]. 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	偽造銀聯（ぎんれん）カードATM 不正引き出し事件	6	大手百貨店店員や銀行協会職員を装い、キャッ シュカードをだまし取る手口が増加	11	IoT 機器を乗っ取り、DDoS 攻撃を引き起こすマルウェア「Mirai」流行
2	ポケモンGO偽アプリ出回る	7	FBI が米 Apple に対して、捜査のため iPhone のロック解除を要請	12	防衛省と自衛隊の情報基盤へのサイバー攻撃
3	JTB、メールによる標的型攻撃で、マルウェア感染、個人情報 793 万件流出。	8	金融通信メッセージングサービス SWIFT がサイバー犯罪者の標的に	13	国際的ハッカー集団「アノニマス」による日本への攻撃
4	県立高校情報システムへの不正アクセスで 17 歳の少年が逮捕	9	米民主党全国委員会（Democratic National Committee、DNC）からメール情報が流出。	14	英 Tesco Bank がオンライン犯罪攻撃の対象となり、2万口座から預金が盗まれる。
5	繰り返す Yahoo からの情報漏えい（10 億人以上の個人情報漏えい）	10	ランサムウェア「WannaCry」世界的規模で感染拡大	15	IPA新設国家資格「情報処理安全確保支援士」の初回申請受付を開始

[Q46]. 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	セキュリティレジリエンス	9	匿名加工情報	17	CISA
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	エクスプロイト	11	OWASP	19	CSIRT
4	ダークネット	12	Apache Struts2 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	SMB v1 の脆弱性
8	WAF	16	Bug Bounty（バグ発見報奨）	24	ディープラーニング（深層学習）

[Q47]. 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。