情報セキュリティ調査アンケート回答用紙

拝啓　時下ますますご清祥のこととお慶び申し上げます。

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

[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、ソフトウエア業、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	製造業、建設業、運輸業、その他の業種(2～4 を除く)であり、資本金 3 億円以下または従業員 300 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	卸売業であり、資本金 1 億円以下または従業員 100 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	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	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	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/CSMS、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/CSMS 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/CSMS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/CSMSの規格変更のため
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	運用ソフトウエ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	9	GDPR（EU一般データ保護規則）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	10	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	11	情報セキュリティ事件・事故(サイバー攻撃、情報漏えい、マルウエア感染等)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	12	プライバシーマークの規格JISQ15001改正への対応
7	ISMS/CSMSやPマークの認証取得・更新	13	過去3年間は対策（管理策）の見直しがない
8	個人情報保護法改正への対応	14	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前期から今期にかけての動向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)

内容	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
17-1 前期と今期の支出比較	1	2	3	4	5	6
17-2 今後の支出変化	1	2	3	4	5	6
17-3 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 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
18-3 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
18-4 政府機関等の情報セキュリティ対策のための統一基準群(内閣サイバーセキュ リティセンター)	1	2	3	4
18-5 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
18-6 IoT セキュリティガイドライン(総務省)	1	2	3	4
18-7 SP800-82 産業制御システム(ICS)セキュリティガイド 日英対訳版(NIST)	1	2	3	4
18-8 制御システムのセキュリティリスク分析ガイド(IPA)	1	2	3	4
18-9 組織における内部不正防止ガイドライン(IPA)	1	2	3	4

[第3章]情報セキュリティ対応体制・人材育成についてお伺いします

本章において、「非 IT 部門」とは、会社の情報システムの企画・開発・運用・委託といった業務を主として実施していない部門(事業部門、営業部門、製造現場など)のことをいいます。また、「橋渡し人材」とは、情報セキュリティに関する知識を有し、経営層や非 IT 部門など会社の幅広いに部門を対象として、サイバーセキュリティ方策の企画、立案、教育などのサポートができる人材のことをいいます。

[Q19]. 自社のセキュリティ対策に関わる人材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)

内容	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	
19-1 標的型攻撃などのサイバー攻撃に対処(指揮命令)ができる人材	1	2	3	4	5	6
19-2 コンピュータやネットワークに関する高度な知識や技術を持つ人材(いわゆるホワイトハッカー)	1	2	3	4	5	6
19-3 コンピュータウイルスの分析やフォレンジック調査ができる人材	1	2	3	4	5	6
19-4 システム構築・製品開発においてセキュリティの機能をどのように織り込むかを考えることができる人材	1	2	3	4	5	6
19-5 セキュリティ教育や啓発など、リテラシー向上ができる人材	1	2	3	4	5	6

[Q20]. 自社の非 IT 部門でも必要と思うセキュリティ人材について教えてください（各項目の 1～3 で○印はひとつだけ）

内容		必要	不要	不明・わからない
20-1	標的型攻撃などのサイバー攻撃に対処（指揮命令）ができる人材	1	2	3
20-2	コンピュータやネットワークに関する高度な知識や技術を持つ人材（いわゆるホワイトハッカー）	1	2	3
20-3	コンピュータウイルスの分析やフォレンジック調査ができる人材	1	2	3
20-4	システム構築・製品開発においてセキュリティの機能をどのように織り込むかを考えることができる人材	1	2	3
20-5	セキュリティ教育や啓発など、リテラシー向上ができる人材	1	2	3

[Q21]. 自社のセキュリティ人材育成を行うための仕組み作りは、次のどちらが良いと思いますか？ （○印はひとつだけ）

1	非 IT 部門が自ら考えてセキュリティ対策ができるように、非 IT 部門の担当者にセキュリティを学ばせる
2	迅速なインシデント対応ができるように、セキュリティ専門者に非 IT 部門の業務（例：OT などの制御・運用技術）を学ばせる
3	不明・分からない
4	その他［ ］

[Q22]. 自社の情報キュリティ対策において、橋渡し人材が必要と感じていますか？（○印はひとつだけ）

1 はい	2 いいえ	3 不明・わからない	4 その他［ ］

[Q23]. 質問[Q22]で「はい」と答えた方への質問です。橋渡し人材に一番期待する役割は何ですか？（○印はひとつだけ）

1	セキュリティに関する情報（知識、ノウハウ）の提供、受け渡し	4	不明・わからない
2	セキュリティ対策の企画、立案、対策の実行	5	その他［ ］
3	セキュリティに関する専門的な事項を現場業務に当てはめて説明できるスキル		

[Q24]. 自社のセキュリティ人材に対するインセンティブはありますか？（複数選択可）

1	セキュリティ資格取得の奨励金または手当がある	4	不明・わからない
2	セキュリティ資格取得を人事評価（昇進）に利用している	5	特になし
3	CISO やセキュリティ部門のマネージャーなど、セキュリティ実務経験者のポスト、キャリアパスがある	6	その他［ ］

［第4章］ 制御システムにおける情報セキュリティに関する課題についてお伺いします。

※【前提】本章の「制御システム」とは他の機器やシステムの動作を管理、指示、制御するシステムであり、センサやアクチュエータ等のフィールド機器、制御用のネットワーク、コントローラ、監視・制御システム等で構成されている機器群(システム)をさす。顧客系向け IoT 機器の制御システムや監視カメラは対象としない。

[Q25]. 貴社の制御システムにおいて最も関係のある分野を1つ選択してください。（○はひとつだけ）

1	情報通信（電気通信・放送等）	8	医療	15	鉄鋼製造
2	金融（銀行・証券・保険）	9	水道	16	食品製造
3	航空	10	物流	17	印刷
4	鉄道	11	化学（材料・薬品）	18	防災設備・ビル管理
5	電力	12	クレジット	19	教育
6	ガス	13	石油	20	制御システムと関係は無い[→Q30へ]
7	政府・行政サービス	14	加工組立製造（機械、自動車、半導体、電気機器、電線、デバイス）	21	その他[ ]

[Q26]. 貴社の制御システムにおいて RASIS（信頼性、可用性、保守性、保全性、機密性）の観点から、貴社の運用状況から最も近いものを1つ選択してください。（各項目で○印はひとつだけ）

内容		とても重視する	ある程度重視する	どちらともいえない	あまり重視しない	重視しない
26-1	信頼性（安定して稼働するための故障への耐性度合い）	1	2	3	4	5
26-2	可用性（稼働率を高める度合い（冗長構成など））	1	2	3	4	5
26-3	保守性（障害復旧、メンテナンスの容易さの度合い）	1	2	3	4	5
26-4	保全性(情報の完全性を保つ度合い（情報改竄対策など）)	1	2	3	4	5
26-5	機密性（情報漏えいの起りにくさの度合い）	1	2	3	4	5

[Q27]. 貴社の制御システムのセキュリティ管理状況について最も近いものを1つ選択してください。（各項目で○印はひとつだけ）

内容		実施している	一部のみ実施している	未実施だが実施の計画がある	実施していない	不明・わからない
27-1	図面や仕様書について施錠等で適切な管理、廃棄を実施している	1	2	3	4	5
27-2	図面や仕様書（データ含む）の社内閲覧、配布等の公開範囲について業務上必要な範囲に定めている	1	2	3	4	5
27-3	管理システムへアクセスにおいて誰がどのような操作をおこなったか管理できる仕組みがあり、管理権限をもつ従業員を限定している	1	2	3	4	5
27-4	定期的にログ監視（アクセスログ・イベントログ等）を実施している	1	2	3	4	5
27-5	制御システムのセキュリティポリシーを定め、定期的に見直しを行っている	1	2	3	4	5

[Q28]. 貴社の制御システムにおける IT の開発・運用の委託先企業、再委託先企業のセキュリティマネジメント状況について最も近いものを1つ選択してください。(各項目で○印はひとつだけ)

内容		実施している	一部のみ実施している	未実施だが実施の計画がある	実施していない	不明・わからない
28-1	委託先企業間で制御システムのセキュリティポリシーを共有し遵守を徹底させている	1	2	3	4	5
28-2	再委託先(孫受け、購買先)で制御システムのセキュリティポリシーを共有し遵守を徹底させている	1	2	3	4	5
28-3	委託先企業間で秘密保持契約を結び、従業員による情報取り扱い関して徹底させている	1	2	3	4	5
28-4	再委託先(孫受け、購買先)で秘密保持契約を結び、従業員による情報取り扱い関して徹底させている	1	2	3	4	5
28-5	委託先企業間でオフィス、機器室への入室管理を徹底している	1	2	3	4	5
28-6	委託先企業間で製作、運用しているインストール媒体やテストプログラムについても強固なルールを徹底している	1	2	3	4	5

[Q29]. 貴社の制御システムにおけるセキュリティ対策を困難とさせている重要な課題を選択してください。(最大3つまで複数選択可能)

1	OSのセキュリティパッチ適用やネットワーク機器のファームウェア更新が難しい	5	セキュリティ機器は耐用年数が短く、他の機器とライフサイクルが合わない	9	セキュリティ機器導入後の運用・保守オペレーションがない
2	接続されている他システムとのインターフェースの変更が必要となるため難しい	6	委託先企業(サプライヤー)との業務遂行上ルールを強制できない	10	セキュリティ導入の開発・運用予算を確保することが難しい
3	セキュリティ機器を導入することで制御システムの可用性低下が懸念される	7	制御システム専用のセキュリティ規定・ポリシーを作ることが難しい	11	既存システムの改修量が多すぎるため現実的でない
4	セキュリティ技術を持つ人材が不足している(企画・開発・保守・運用を含む)	8	管理コントロールする事業所が遠隔地にあるため対策が困難	12	その他[ ]

[第5章] 匿名加工情報の取扱いに関してお伺いします。

※匿名加工情報とは、個人情報保護法第 2 条 9 項で定義されている、個人情報を個人情報の区分に応じて定められた措置を講じて特定の個人を識別することができないように加工して得られる個人に関する情報であって、当該個人情報を復元して特定の個人を再識別することができないようにしたものです。

[Q30]. 匿名加工情報の作成・利用をおこなっていますか。(○印はひとつだけ)

1	匿名加工情報を作成していない、かつ提供を受けていない[→Q32 へ]
2	匿名加工情報を作成していないが、提供を受けて利用している[→Q31 へ]
3	匿名加工情報を作成していないが、将来、利用を検討している[→Q32 へ]
4	匿名加工情報を作成して、第三者提供をしている(但し、自社内で利用はしていない)[→Q31 へ]
5	匿名加工情報を作成して、自社内で利用をしている(但し、第三者提供はしていない)[→Q31 へ]
6	匿名加工情報を作成して、第三者提供及び自社内で利用している[→Q31 へ]
7	不明・わからない[→Q32 へ]

[Q31]. 作成・利用している匿名加工情報で該当するものをお答えください。(複数選択可)

1	購買履歴	8	医療情報(既往歴等)
2	公共交通機関乗降履歴	9	介護情報
3	移動履歴	10	保険関連の情報
4	インターネット閲覧履歴	11	金融関連の情報
5	テレビ視聴履歴	12	クレジットカード関連の情報
6	電力・ガス・水道の使用履歴	13	人材斡旋情報(職歴・スキル等)
7	健康情報	14	資格検定情報
15	その他[ ]		

[Q32]. 匿名加工情報を作成しようとした時に感じる阻害要因、あるいは普及が進まない阻害要因としてあてはまるものをすべてお答えください。(複数選択可)

1	匿名加工情報の再識別リスク	7	顧客からのクレーム／レピュテーションリスク
2	匿名加工情報及び加工方法等情報の漏えいリスク	8	自社にて取扱いのルール・規程が整備されていない
3	匿名加工情報の利活用の事例が少ない	9	個人情報保護法に準拠する具体的な加工方法がわからない
4	匿名加工情報に対応した良質で廉価な市販のパッケージソフトが少ない	10	自社の保有する個人データに係るニーズ／ユースケースが不明
5	認定個人情報保護団体や業界団体等において取扱いのルールが整備されていない	11	個人データを管理しているシステムの制限(利用ネットワーク、データフォーマット、アクセス制御、運用方法等)から対応が難しい
6	自社にてデータ加工に関する専門知識を有する人材がいない・不足している	12	その他[ ]

[Q33]. 匿名加工情報の普及にあたり重要と思うものについてお答えください。(各項目 1～5 で○印はひとつだけ)

	内容	重要と思う	どちらかといえば重要と思う	どちらかといえば重要と思わない	重要と思わない	わからない
33-1	匿名加工情報の作成している事業者や提供を希望している事業者の情報	1	2	3	4	5
33-2	匿名加工情報の認証制度	1	2	3	4	5
33-3	匿名加工情報の取扱いの監査の実施	1	2	3	4	5
33-4	個人情報保護法における加工基準の明確化	1	2	3	4	5
33-5	認定個人情報保護団体や業界団体等における取扱いルールの整備	1	2	3	4	5
33-6	匿名加工情報の流通のためのマーケットプレイスやプラットフォーム	1	2	3	4	5
33-7	個人情報を提供する本人へのポイント付与等のインセンティブ	1	2	3	4	5
33-8	匿名加工情報を利活用する企業に対する補助金や優遇税制等のインセンティブ	1	2	3	4	5

[第6章] 情報セキュリティマネジメントへの例外措置についてお伺いします

[Q34]. 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「例外措置」の項目がありますか。(○印はひとつだけ)

1	内部規定に全て明記している	3	内部規定には明記していない	5	答えたくない
2	内部規定に一部明記している	4	わからない・知らない	6	その他 [ ]

[Q35]. 例外措置は、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	わからない・知らない
2	現場組織ごと	4	どちらもない	6	その他 [ ]

[Q36]. 例外措置を策定するにあたり、規定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		

[Q37]. 例外措置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[ ]

[Q38]. 以下の具体的な業務上の事象において、例外措置を明記していますか。それぞれにつきひとつだけお教えください。

	事象	通常規定に明記		例外措置を明記		規定に記載なし	
		通常措置としている	例外措置から変更	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
38-1	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
38-2	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
38-3	外部業者への特権IDを付与する	1	2	3	4	5	6
38-4	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
38-5	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

[Q39]. 以下の具体的な業務上の事象において、どちらの策定案を選択しますか。それぞれに近いものにつき、1か2のいずれかお教えください。(○印はひとつだけ)

	事象		策定案1		策定案2
39-1	外部インターネットの使用	1	許可なく外部インターネットの利用は禁止する	2	業務上理由がある場合は，申請の上，外部インターネットの利用を許可する
39-2	プログラム保守のための外部からの一時的アクセス	1	プログラム保守による外部からのアクセスは事前承認を要する	2	緊急措置が必要であると経営者が判断した場合は事後申請で構わない
39-3	サポート切れの OS やソフトウエアの継続使用	1	サポート切れの OSやソフトウエアの使用は全面禁止である	2	全く外部ネットに接続しないレガシーシステムについては許可することもある
39-4	非日本国内法準拠のクラウドの利用	1	社内審査の許可があれば，企業が契約するクラウドを利用する	2	取引先からの指示などやむを得ない場合は，申請の上，一時的に利用を許可することもある
39-5	自社が管理していないソフトウエアの使用	1	自社保有ライセンス以外のソフトウエアの利用は原則禁止	2	業務上理由がある場合は，申請の上，利用を許可する
39-6	個人で利用しているクラウドサービス(Dropbox 等)の利用	1	原則禁止とし，企業が契約するクラウドを利用する	2	取引先からの指示などやむを得ない場合は，申請の上，一時的に利用を許可することもある

[第7章]職場での人工知能(AI)や自律型ロボットの導入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)とはコールセンター業務や記事の作成など職場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。また自律型ロボットとは人間の指示通りに単純作業を繰り返すものではなく、自らの判断で人を手助けするものを指します。

[Q40]. 職場での AI や自律型ロボットの利用状況について最も近いものを1つ選択してください。（○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

[Q41]. AI や自律型ロボットを職場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	3 新たなサービスの提案・開発	5 利点はない
2 仕事の自動化・効率化	4 他企業との差別化又は業務連携	6 わからない

[Q42]. AI や自律型ロボットを業務や他社との提携で導入した際のリスク等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 AI・ロボットが人間を指導・育成することによる人材の質の低下	4 導入したAI・ロボットの著作権等の権利問題	7 リスクはない
2 顧客減少による収入減やクレーム対応等への業務負荷	5 AI・ロボットによる企業秘密の流出	8 よくわからない
3 AI・ロボットによる法律違反	6 AI・ロボットに学習させるために様々な情報を提供する作業負荷	9 その他［ ］

[Q43]. AI や自律型ロボットを職場で使うことへの考えで最も近いものを1つ選択してください。（○印はひとつだけ）

1 業務全般で積極的に活用すべき	3 法律や制度等に準拠できなければ、活用すべきではない	5 わからない
2 活用すべきだが一部の業務に限られる	4 業務全般でまだ活用すべきではない	6 その他［ ］

[第8章] グループ企業における情報セキュリティポリシーについてお伺いします

本章において、「親会社」、「子会社」、「グループ企業」とは、以下のことをいいます。
親会社 ： 子会社の株式の 50%超を所有する会社　　グループ企業 ： 親会社、子会社の総称
子会社 ： 親会社に株式の 50%超を所有されている会社(孫会社の場合も含みます)

以下[Q44～Q47]の設問は、親会社、または子会社の関係がある企業様のみ、ご回答ください。

[Q44]. 本設問では、グループ企業同士が VPN など何らかの専用ネットワークで接続されていることを WAN と呼びます。貴社の従業員が使用する PC は、WAN を経由して、他のグループ企業と接続されていますか？(○印はひとつだけ)

1 全グループ企業の PC が WAN で接続されている。	4 わからない。
2 一部のグループ企業の PC が WAN で接続されている。	5 その他[ ]
3 各社別々のネットワークを使っており、接続されていない。	

[Q45]. グループ企業の情報セキュリティポリシーについて、貴社に最も近いものを選択してください。(○印はひとつだけ)

1	全グループ企業に、親会社と共通のポリシーを適用している。
2	全グループ企業に、親会社のポリシーを一部変更して適用している。
3	一部のグループ企業に、親会社と共通のポリシーを適用している。
4	一部のグループ企業に、親会社のポリシーを一部変更して適用している。
5	共通のポリシーはなく、各社個別のポリシーを作成している。
6	情報セキュリティポリシーは特に定めていない。
7 わからない	8 その他[ ]

[Q46]. グループ企業の情報セキュリティポリシー遵守状況や、改善活動の進捗状況の確認について、貴社に最も近いものを選択してください。(○印はひとつだけ)

1	全グループ企業に、共通の評価基準で、親会社の監査担当部門などによる確認を定期的に実施している。
2	全グループ企業に、親会社の評価基準を一部変更して、親会社の監査担当部門などによる確認を定期的に実施している。
3	一部のグループ企業に、共通の評価基準で、親会社の監査担当部門などによる確認を定期的に実施している。
4	一部のグループ企業に、親会社の評価基準を一部変更して、親会社の監査担当部門などによる確認を定期的に実施している。
5	各社で、共通の評価基準による自己点検を定期的に実施している。
6	各社で、各自で作成した評価基準による自己点検を定期的に実施している。
7	親会社のセキュリティ担当部門などによる確認や、自己点検は実施していない。
8 わからない	9 その他［ ］

[Q47]. グループ企業における貴社の立場と、グループ企業全体で情報セキュリティポリシー遵守を徹底する上での難しさについて、貴社に最も近いものを選択してください。

Q47-1.貴社の立場(○印はひとつだけ)

1 グループ企業にポリシーを守るよう働きかける親会社の立場	2 ポリシーを守る子会社の立場	3 親会社と孫会社の中間に位置する両方の立場

Q47-2～47-9 は、Q47-1 で 1.親会社 または 3.両方 と答えた方のみご回答ください。（各項目 1～5 で○印はひとつだけ）

グループ企業全体で 情報セキュリティポリシー遵守を徹底する上での難しさ	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
47-2 子会社の経営層に必要性を理解してもらうこと	1	2	3	4	5
47-3 子会社の管理職・従業員に必要性を理解してもらうこと	1	2	3	4	5
47-4 グループ企業全体に適用できる共通ポリシーを策定すること	1	2	3	4	5
47-5 グループ企業のまとめ役になれる人材を確保すること	1	2	3	4	5
47-6 グループ企業にセキュリティ教育を行える人材を確保すること	1	2	3	4	5
47-7 グループ企業の遵守状況の監査を行える人材を確保すること	1	2	3	4	5
47-8 グループ全体に推進する組織が、内部から評価を得ること	1	2	3	4	5
47-9 その他[ ]	1	2	3	4	5

Q47-10～47-16 は、Q47-1 で 2.子会社 または 3.両方 と答えた方のみご回答ください。（各項目 1～5 で○印はひとつだけ）

47-10 自社の経営層に必要性を理解してもらうこと	1	2	3	4	5
47-11 自社の管理職・従業員に必要性を理解してもらうこと	1	2	3	4	5
47-12 親会社と同じポリシーに合わせること(業務特性上困難 など)	1	2	3	4	5
47-13 親会社と同じポリシーに準拠するための予算を確保すること	1	2	3	4	5
47-14 自社の特性に応じてセキュリティポリシーを適正に変更すること	1	2	3	4	5
47-15 自社でポリシー周知徹底、点検を行える人材を確保すること	1	2	3	4	5
47-16 その他[ ]	1	2	3	4	5

［第9章］ EU一般データ保護規則(GDPR)への対応に関してお伺いします。

[Q48]. 以下の EU 一般データ保護規則(GDPR)に関する事項でご存じのものをすべて選択してください。（複数選択可）

1	削除権(忘れられる権利)	6	十分性認定(日本は 2018 年中に取得見込み)
2	データポータビリティの権利	7	BCR(拘束的企業準則)
3	異議を述べる権利	8	SCC(標準契約条項)
4	プロファイリングを含む自動処理に基づく決定に服さない権利	9	制裁金(最高で 2000 万ユーロまたは全世界年間売上高 4%)
5	データ影響評価	10	データ侵害の場合の監督機関への 72 時間以内の通知

[Q49]. 貴社(貴団体)における GDPR への対応状況を以下の中から選んでください。（○印はひとつだけ）

1	対応不要(対象外のため)	4	対応中
2	対応を回避(EU関連のビジネスの中止や見直し等)	5	対応を検討中
3	対応済み(対応の施策を実施)	6	未着手

［第10章］ その他

[Q50]. 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	企業(Amazon、楽天、JCB)をかたる利用者を狙ったフィッシング攻撃が発生	10	Google の Chrome ウェブストアに偽の広告ブロッカー、約 2000 万人がダウンロード
2	2018 年 4 月 20 日「システム監査基準」及び「システム管理基準」が改訂	11	日本年金機構職員が窃盗容疑で逮捕 － 個人情報持ち出し
3	Wi-Fi 暗号化規格(WPA2)で KRACK と呼ばれる新しい脆弱性が発見される	12	2017 年 8 月 25 日 Google の経路情報設定ミスで日本の通信インフラが混乱
4	Windows10 にプレインストールされていたパスワード管理ソフト「Keeper」に情報漏えいの脆弱性が発見される	13	2017 年 12 月 20 日 日本航空 ビジネスメール詐欺にだまされ 3 億 8000 万円余被害
5	macOS で誰でも管理者権限取得可能な脆弱性が発見される	14	2017 年 12 月 5 日 長野県の高校生が SNS のフィッシングサイトを開設し不正アクセス容疑で逮捕される
6	総務省「パスワードの定期的な変更は不要」と方針転換	15	仮想通貨発掘マルウエアが急増
7	米 Yahoo!で、不正アクセスにより最終的に 30 億人分以上のユーザー個人情報が漏えいしていたことが判明	16	IoT 機器に感染するマルウエア Mirai の亜種「Satori」(別名 Okiru)の感染が拡大
8	Uber 社、約 60 万人の運転手の個人情報が 2016 年に窃取されていたことを公表	17	IoTデバイスを標的とするIoTroop(Reaper)が100万以上の組織で感染
9	Facebook の個人情報がアクセス可能状態にあった問題	18	NTT、海賊版サイト「漫画村」などのブロッキングを決定

[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。