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ると言えます。 それに伴い、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について研究を行っております。本アンケートでは、研究の一環として、プライバシーマーク取得やセキュリティマネジメントの運用状況、これから本格化する番号制度への意識やデジタル・フォレンジックの実態を調査し、課題を抽出したいと考えております。本趣旨をご理解頂き、ご記入できる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。

質問の対象期間は2010年4月1日から2011年3月31日とし、従業員数・売上高（または予算額）などは平成23年7月1日現在、あるいは直近の決算日のものをご回答ください。

なお、アンケートはすべて統計的な処理を行い、すべての内容について貴社名・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、ご記入いただいた内容は本アンケートに関連するもの以外に利用することはありません。アンケートの分析結果につきましては、上記に配慮した上で11月上旬に本学のホームページ（http://www.iisec.ac.jp/）に公開する予定です。

大変お忙しいことと存じますが、アンケートは**平成23年8月10日（水）までにご投函**いただきますよう、重ねて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
電子メール：harada.survey@iisec.ac.jp　FAX：045-410-0238
※研究室に在室していることが少ないため、お手数ですがご連絡は電子メールまたはFAXにていただければ幸いです。

［本アンケート調査における用語］

用 語	用語の説明
プライバシーマーク事務局	各事業者において、プライバシーマークの取得・維持活動を、全社の中心として推進するグループメンバー（プロジェクトメンバー、プロジェクトチーム）のこと。
情報セキュリティ・ポリシー	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情報セキュリティ対策基準等が該当し、情報セキュリティ実施手順等の具体的な手順は含みません。 例）業務で使用するPCはパスワードで保護すること。
情報セキュリティ・ルール	情報セキュリティ・ポリシーを遵守するための具体的な手順のこと。情報セキュリティ実施手順等が該当します。　例）業務で使用するPCには、7文字以上のパスワードを設定すること。
グループポリシー	所属する企業グループにおける共通のポリシーのこと。
デジタル・フォレンジック	不正アクセスや機密情報漏えいなどコンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称
共通番号	政府が検討を進めている「国民ID」や「社会保障・税に関わる番号」など、国民一人ひとりに付番する固有の番号。この番号を用いることで、行政分野だけでなく、民間企業においても事務の効率化、サービスの向上が図られるとしている。
情報提供元	番号制度において共通番号により紐づけられた情報を提供する組織。共通番号は、当面、社会保障と税分野での利用となるが、将来的には民間サービスでの利用も視野に入っており、共通番号により連携している組織では、それぞれが情報の提供元となりうる。
データ正確性	情報システムが保有するデータの内容が事実と合致していること。ただし、その精度については、データの利用目的により異なる。

情報セキュリティ調査　質問回答票　　情報セキュリティ大学院大学

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。
記述式設問のご回答は、回答記入欄に数値または文章を記入してください。

[第1章]　まず初めに、貴社の概要・IT環境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	社長室	11	情報システム開発部門
2	人事	7	企画部門	12	事業部門
3	経理	8	情報システム管理部門	13	監査部門
4	情報セキュリティ担当部門	9	事業推進部門	14	その他[　　]
5	リスク管理担当部門	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	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	13	教育学習支援業
2	建設業	8	金融業、保険業	14	医療、福祉
3	製造業	9	不動産業、物品賃貸業	15	大学
4	電気・ガス・熱供給・水道業	10	宿泊業、飲食店	16	公務（政府・自治体）
5	情報通信業	11	学術研究、専門・技術サービス業	17	その他[　　]
6	運輸業、郵便業	12	生活関連サービス業、娯楽業		

[Q4]. 貴社の組織構造 （複数選択可）

1	事業部制組織	5	SBU（戦略事業単位）制	9	企業グループ（子）
2	職能別組織	6	マトリックス組織	10	該当なし
3	カンパニー制	7	社内ベンチャー制度	11	その他[　　]
4	部門制（セクター制）	8	企業グループ（親）		

[Q5]. 貴社の主な電子商取引形態 （○印はひとつだけ）

1	対企業（B to B）	3	対政府・自治体（B to G）	5	対従業員（B to E）
2	対消費者（B to C）	4	消費者間取引の斡旋（C to C）	6	該当なし

[Q6]. 貴社[単独]の年間売上高 （○印はひとつだけ。対象期間:2010 年 4 月 1 日から 2011 年 3 月 31 日）
（大学・公務等は予算額、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		

[Q7]. 貴社[単独]の全従業員数 （○印はひとつだけ）

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

[Q8]. 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	100台以下	4	501～1,000台	7	5,001～10,000台
2	101～300台	5	1,001～1,500台	8	10,001～50,000台
3	301～500台	6	1,501～5,000台	9	50,001台以上

[Q9]. 貴社[単独]の個人情報の保護に関する法律で定義されている「保有個人データ」の件数 （○印はひとつだけ）

1	100件以下	4	501～1,000件	7	5,001～10,000件
2	101～300件	5	1,001～1,500件	8	10,001～50,000件
3	301～500件	6	1,501～5,000件	9	50,001件以上

[Q10]. 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。（○印はいくつでも）

1	実施していない	3	外部監査を実施している	5	Pマークの監査を実施している
2	内部監査を実施している	4	ISMSの監査を実施している	6	PCI DSSの監査を実施している

[Q11]. 貴社において、機密情報の誤送信(メール/FAX)や紛失、盗難、ファイル交換ソフト(P2Pソフト)による情報流出などの情報セキュリティ事故/事件が発生したことがありますか。(○印はひとつだけ)

1 発生したことはない	3 2～4回/年に発生	5 10回以上/年に発生
2 1回/年に発生	4 5～9回/年に発生	6 その他[ ]

[第2章] 次に、貴社のプライバシーマークの取得状況についてお伺いします。

※第 2 章の質問は<u>プライバシーマーク事務局リーダーまたは、メンバーの方</u>にご回答いただけます様、お願いいたします。

[Q12]. 貴社はプライバシーマークを取得していますか。(○印はひとつだけ)

1 取得している → [Q13へ] 2 取得していない → [第3章へ]

[Q13]. 認証取得の主な目的をお答えください。(複数選択可)

1 会社業務の運営をプライバシーマーク 認証に基づいた方法にするため
2 プライバシーマーク 認証の考え方を部分的に入れて業務の改善を狙ったため
3 プライバシーマーク 認証を得ることで営業活動において有利になる、あるいは不利にならないことを狙ったため
4 入札その他でプライバシーマーク 認証取得が条件になっているため
5 グループ会社等の方針で決まっているため
6 全社の情報セキュリティ対策、個人情報保護の向上のため
7 従業員の個人情報保護意識の向上のため
8 その他[ ]

[Q14]. 認証を取得して得られた効果をお答えください。(複数選択可)

1 情報流出や漏えいの防止・軽減	10 個人情報保護体制の整備と人員確保
2 盗難や忘失などの防止・軽減	11 経営陣の個人情報保護への理解と実践
3 セキュリティ事件・事故の減少	12 社員への個人情報保護意識の浸透と実践
4 事故発生時の体制・計画の整備	13 業務記録等の整理と検索性の向上
5 事故発生時の対応時間の軽減・短縮	14 情報資産/個人情報の利用・保存状況の改善
6 災害発生時の体制・計画の整備	15 事務局メンバーの知識向上
7 情報資産/個人情報の明確化と整理	16 特に無い
8 情報管理計画の明確化と必要な対策の実施	17 その他[ ]
9 セキュリティ関係予算の確保	

[Q15]. 貴社の個人情報保護管理者の役職 (○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	5 課長	8 一般社員
3 事業部長	6 係長・主任	9 その他[ ]

[Q16]. 個人情報保護管理者の所属組織 (○印はひとつだけ)

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

[Q17]. 貴社には、現場で個人情報保護活動を推進する「個人情報保護担当者」が存在しますか。(○印はひとつだけ)

1 存在する 2 存在しない

[Q18]. 貴社の個人情報保護担当者の役職(多数存在する場合は、最も多い役職) (○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	5 課長	8 一般社員
3 事業部長	6 係長・主任	9 その他[ ]

[Q19]. 貴社ではプライバシーマーク事務局(以下「事務局」という。)メンバーをどの様に編成しましたか。(○印はひとつだけ)

1 既存の組織(総務部門、企画部門、システム部門等)の枠組みの中で、組織全員をそのまま事務局メンバーとした
2 既存の組織の中で、一部の人間を招集し、事務局メンバーとした
3 組織横断的に人員を招集し、事務局メンバーとした
4 その他[ ]

[Q20]. 前回審査時の事務局のメンバーは何人ですか。(複数選択可)

1 専任(人) 2 兼務(人) 3 その他(人)

[Q21]. 「事務局リーダー」が存在し、機能していましたか。(○印はひとつだけ)

1 存在し機能していた	4 存在しておらず、機能もしていなかった → [Q29へ]
2 存在していたが、機能していなかった	5 その他[ ]
3 明確には存在しなかったが、実質的なリーダーが存在し、機能していた	

[Q22]. 前回審査時、事務局リーダーはどの様に配置されていましたか。（○印はひとつだけ）

1 専任	2 兼務	3 その他

[Q23]. 個人情報保護管理者と事務局リーダーは同一人物ですか。（○印はひとつだけ）

1 同一人物	2 同一人物ではない

[Q24]. 前回審査時の事務局リーダーの役職 （○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	5 課長	8 一般社員
3 事業部長	6 係長・主任	9 その他[ ]

[Q25]. 前回審査時の事務局リーダーのプライバシーマーク認証業務に関するご経験年数 （○印はひとつだけ）

1 1年未満	3 3年以上 5年未満	5 7年以上 9年未満
2 1年以上 3年未満	4 5年以上 7年未満	6 9年以上

[Q26]. 前回審査時に、初回認証取得の際の事務局リーダーが事務局に残っていましたか。（○印はひとつだけ）

1 残っていた	2 残っていなかった	3 その他[ ]

[Q27]. 前回審査時において、事務局リーダーが主体的に取り組んだ業務は何でしたか。（複数選択可）

1 コストの見積もり	5 事業推進部、現場との調整	9 事務局のメンバーの編成
2 審査員との折衝	6 審査書類、説明資料の作成	10 事務局内のコミュニケーション
3 幹部への説明	7 指摘事項の是正	11 その他[ ]
4 事務局内の教育	8 人員・予算の確保	

[Q28]. 前回審査時において、事務局リーダーの JISQ15001 の理解度は如何でしたか。（○印はひとつだけ）

1 良く理解していない	4 他の事務局メンバーを教育・指導することができる
2 要点について説明できる	5 改善案を提案することができる
3 他の規格との差異を説明できる	6 その他[ ]

[Q29]. 事務局の新しいメンバーに対して、どのような形でプライバシーマークに関連したスキル習得を行いましたか。（複数選択可）

1 外部講習によるスキル習得	3 OJT による習得	5 特になし
2 社内講習によるスキル習得	4 独学(個人に任せている)	6 その他[ ]

[Q30]. 貴社はプライバシーマークを何回更新していますか。（○印はひとつだけ）

1 0回(未更新) → [Q33へ]	3 2回	5 4回
2 1回	4 3回	6 5回以上

[Q31]. 事務局リーダーは前々回更新時と前回更新時で変わりましたか。（○印はひとつだけ）

1 変わった	2 変わっていない

[Q32]. 前回審査時、初回認証取得の際のメンバーが、どのくらいの割合で残っていましたか。（○印はひとつだけ）

1 全員残っていた	3 5割未満	5 一人もいなかった
2 7割未満	4 3割未満	

[Q33]. 前回審査時、審査必要書類を送付するための準備期間 （○印はひとつだけ）

1 1ヶ月未満	2 1ヶ月以上 3ヶ月未満	3 3ヶ月以上

[Q34]. 前回審査時、現地審査での指摘事項数はいくつでしたか。（○印はひとつだけ）

1 0(指摘なし) → [Q37へ]	3 5以上 10未満	5 15以上 20未満
2 1以上 5未満	4 10以上 15未満	6 20以上

[Q35]. 前回審査時、指摘事項を全て是正するまでにかかった期間 （○印はひとつだけ）

1 1ヶ月未満	2 1ヶ月以上 3ヶ月未満	3 3ヶ月以上

[Q36]. 前回審査時、是正に最も時間を要した要求事項は、次の内どれですか。（○印はひとつだけ）

1 3.3.1 個人情報の特定	4 3.4.2.5 個人情報を3.4.2.4 以外の方法によって取得した場合の措置	7 3.7.2 監査
2 3.3.3 リスク認識・分析・対策	5 3.4.3.2 安全管理措置	8 3.8 是正処置・予防処置
3 3.4.2.4 直接書面による取得	6 3.4.3.4 委託先の監督	9 その他[ ]

[Q37]. 前回審査時、現地審査にかかった時間は何時間ですか。（○印はひとつだけ）

1 2時間未満	3 4時間以上 6時間未満	5 8時間以上
2 2時間以上 4時間未満	4 6時間以上 8時間未満	

[Q38]. 前回審査時に、審査必要書類を送付するための準備作業の中で、最も時間を要した作業 （○印はひとつだけ）

1 コストの見積もり	4 事務局内の教育	7 人員・予算の確保
2 PMS実施記録の収集・整理	5 審査書類の作成	8 事業推進部、現場との調整
3 前々回審査記録の確認	6 幹部・内部説明	9 その他[ ]

[Q39]. 貴社において、個人情報保護関連の記録類や手順書を、現場で十分活用できていますか。（〇印はひとつだけ）

1 十分活用できている	3 どちらとも言えない	5 活用できていない
2 ある程度活用できている	4 あまり活用できていない	

[Q40]. 個人情報保護関連の記録類や手順書を、現場で十分活用できていない原因として何が考えられますか。（複数選択可）

1 プライバシーポリシー（個人情報保護規程）が実業務を十分反映できていない
2 手順書や記録様式の質が低く、使いづらい
3 個人情報保護担当者が機能していない
4 現場の意識が低い
5 事務局が、手順書や記録を、効果的に周知・展開できていない
6 その他[ ]

[Q41]. 貴社において、プライバシーマークの効果を高めるために重点的に取り組んでいるもの、あるいは取り組む予定のあるものをお答えください。（複数選択可）

1 経営陣の認識・理解の向上	5 内部監査担当のスキル強化	9 全社の教育研修の改善
2 管理者層の認識・理解の強化	6 有効性評価手法の改善	10 文書・記録管理の改善
3 一般社員の認識・理解の強化	7 費用対効果の説明手法の明確化	11 インシデント対応の向上
4 マニュアルの整備	8 リスク分析手法の改善	12 その他[ ]

[Q42]. 「3.3.3 個人情報のリスク認識、分析、対策」について、「個人情報の取り扱いの各局面におけるリスクを認識し、分析し、必要な対策を講じる手順の確立、維持」をするための取り組み状況は如何ですか。（〇印はひとつだけ）

1 個人的な範囲で取り組んでいる
2 事務局内のみで取り組んでいる
3 各部署で個別に取り組んでいる
4 現場も含め、全組織で取り組んでいる。
5 取り組み状況をモニタリングし、基準から逸脱しない様、全組織で取り組んでいる
6 取り組み状況をモニタリングし、基準から逸脱しない様、全組織で取り組むと共に、継続的な改善を実施している

[Q43]. 事務局が、個人情報保護関連施策を現場に展開する際、誰の名前で依頼を実施していますか。（〇印はひとつだけ）

1 個人情報保護責任者	3 所属組織長	5 事務局メンバー（担当者）
2 個人情報保護管理者	4 事務局リーダー	6 その他[ ]

[Q44]. 貴社では、誰が、個人情報保護施策の決定権を持っていますか。（〇印はひとつだけ）

1 個人情報保護責任者	3 所属組織長	5 事務局メンバー（担当者）
2 個人情報保護管理者	4 事務局リーダー	6 その他[ ]

[Q45]. 事務局は、個人情報に関わる法定、法令環境の変化に対応する事ができていますか。（〇印はひとつだけ）

1 十分対応できている	3 どちらとも言えない	5 対応できていない
2 ある程度対応できている	4 あまり対応できていない	

[Q46]. 前回の更新（または新規取得）の際、コンサルタントを利用しましたか。（〇印はひとつだけ）

1 審査時に利用した	3 審査後も利用している	5 利用していない → [Q48へ]
2 審査時に一部利用した	4 審査後も一部利用している	

[Q47]. 前回審査時、コンサルタントとコミュニケーションをうまく取ることができましたか。（〇印はひとつだけ）

できなかった← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | →できた

[Q48]. 前回審査時、プライバシーマーク審査員とコミュニケーションをうまく取ることができましたか。（〇印はひとつだけ）

できなかった← | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | →できた

［第3章］ 次に、貴社のセキュリティ・ポリシー、ルールの改訂についてお伺いします。

[Q49]. 情報セキュリティ・ポリシーを制定していますか。（〇印はひとつだけ）

1 制定している → [Q50へ]	2 制定していない → [Q58へ]

[Q50]. 情報セキュリティ・ポリシーは全社で共通したものを制定していますか。（〇印はひとつだけ）
（部署毎【部、課、事業所など】で異なるポリシーを制定している場合は、"2 制定していない（部署毎）"とご回答ください。）

1 制定している（全社共通）	3 制定している（全社共通のポリシーを制定の上、部署毎でも制定）
2 制定していない（部署毎）	4 その他[ ]

[Q51]. 情報セキュリティ・ポリシーは、どちらの部署で作成しましたか。（複数選択可）

1 特定の部署（社内）	3 各々の部署（社内）	5 その他[ ]
2 作成専門のプロジェクト（社内）	4 外部委託（社外）	

[Q52]. 情報セキュリティ・ポリシーの見直し（改訂）を、最後に実施したのは何年前ですか。（〇印はひとつだけ）

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 見直しは行っていない → [Q55へ]

[Q53]. （Q52 で “6 見直しは行っていない”以外 を選択した場合、ご回答ください）
情報セキュリティ・ポリシーの見直し（改訂）を実施した理由は何ですか。（複数選択可）

1 法律/条例の改正	4 内部規定の改訂	7 定期的な見直しの一環 →[Q54へ]
2 認証審査のため	5 グループポリシーの改訂	8 インシデント/事故の発生
3 社内組織の改編	6 業務内容の変更	9 その他[ ]

[Q54]. （Q53 で “7 定期的な見直しの一環” を選択した場合、ご回答ください）
定期的な見直しを実施する頻度はどの程度ですか。（〇印はひとつだけ）

1 半年に一度	3 1年半に一度	5 その他[ ]
2 1年に一度	4 2年に一度	

[Q55]. 情報セキュリティ・ポリシーに基づき作成するドキュメントの数について、どのように感じていますか。（〇印はひとつだけ）
また、作成しているドキュメントの数はどの程度ですか。（把握できる範囲の数で支障ございません）

1 多すぎる	2 ちょうどよい	3 少なすぎる
ドキュメント数[ ] （例. 50、100程度、不明 etc・・・）		

[Q56]. 情報セキュリティ・ポリシー関連の管理項目数について、どのように感じていますか。（〇印はひとつだけ）
また、設定している管理項目の数はどの程度ですか。（把握できる範囲の数で支障ございません）

1 多すぎる	2 ちょうどよい	3 少なすぎる
管理項目数[ ] （例. 50、100程度、不明 etc・・・）		

[Q57]. 情報セキュリティ・ポリシーと情報セキュリティ・ルールとの間に、乖離があると感じますか。（〇印はひとつだけ）

1 乖離を感じる	2 乖離を感じない

[Q58]. 情報セキュリティ・ルールを制定していますか。（〇印はひとつだけ）

1 制定している →[Q59へ]	2 制定していない →[Q65へ]

[Q59]. 情報セキュリティ・ルールは全社で共通したものを使用していますか。（〇印はひとつだけ）
（部署毎【部、課、事業所など】で異なるルールを使用している場合は、”2 使用していない（部署毎）”とご回答ください。）

1 使用している（全社共通）	3 使用している（全社共通のルールを制定の上、部署毎でも制定）
2 使用していない（部署毎）	4 その他[ ]

[Q60]. 情報セキュリティ・ルールは、どちらの部署で作成しましたか。（複数選択可）

1 特定の部署（社内）	3 各々の部署（社内）	5 その他[ ]
2 作成専門のプロジェクト（社内）	4 外部委託（社外）	

[Q61]. 情報セキュリティ・ルールの見直し（改訂）を、最後に実施したのは何年前ですか。（〇印はひとつだけ）

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 見直しは行っていない →[Q64へ]

[Q62]. （Q61 で “6 見直しは行っていない”以外 を選択した場合、ご回答ください）
情報セキュリティ・ルールの見直し（改訂）を実施した理由は何ですか。（複数選択可）

1 法律/条例の改正	4 内部規定の改訂	7 定期的な見直しの一環 →[Q63へ]
2 認証審査のため	5 グループポリシーの改訂	8 インシデント/事故の発生
3 社内組織の改編	6 業務内容の変更	9 その他[ ]

[Q63]. （Q62 で “7 定期的な見直しの一環” を選択した場合、ご回答ください）
定期的な見直しを実施する頻度はどの程度ですか。（〇印はひとつだけ）

1 半年に一度	3 1年半に一度	5 その他[ ]
2 1年に一度	4 2年に一度	

[Q64]. 情報セキュリティ・ルールと実業務との間に、乖離があると感じますか。（〇印はひとつだけ）

1 乖離を感じる	2 乖離を感じない

[Q65]. 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何年前ですか。（〇印はひとつだけ）

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 →[第4章へ]

[Q66]. （Q65 で “6 実施していない”以外 を選択した場合、ご回答ください）
情報セキュリティに関するリスク分析を実施した理由は何ですか。（複数選択可）

1 法律/条例の改正	4 内部規定の改訂	7 定期的な見直しの一環 →[Q67へ]
2 認証審査のため	5 グループポリシーの改訂	8 インシデント/事故の発生
3 社内組織の改編	6 業務内容の変更	9 その他[ ]

[Q67]. （Q66 で “7 定期的な見直しの一環” を選択した場合、ご回答ください）
定期的な情報セキュリティに関するリスク分析を実施する頻度はどの程度ですか。（〇印はひとつだけ）

1 半年に一度	3 1年半に一度	5 その他[ ]
2 1年に一度	4 2年に一度	

［第4章］ 次に、デジタル・フォレンジックについてお伺いします。

[Q68]. 貴社はデジタル・フォレンジックを実施していますか。（○印はひとつだけ）

1 既に実施済み → [Q69へ]	3 必要性を感じるが保留 → [Q69へ]	5 不明 → [Q74へ]
2 実施を検討中 → [Q69へ]	4 必要性を感じない → [Q74へ]	6 デジタル・フォレンジックを知らない → [Q74へ]

[Q69]. 貴社でのデジタル・フォレンジックの実施理由を挙げてください。（複数選択可）

1 訴訟対応	4 事故(障害)対応	7 犯罪抑止
2 不正侵入の立証	5 データ復旧・回復	8 その他[ ]
3 内部犯行の立証	6 労務管理	

[Q70]. 貴社でのデジタル・フォレンジック実施の主管部門をお選びください。（複数選択可）

1 情報システム部門	4 知財管理部門	7 その他[ ]
2 法務部門	5 事業部門	
3 監査部門	6 危機管理部門	

[Q71]. 貴社でのデジタル・フォレンジックの実施方法についてお選びください。（○印はひとつだけ）

1 全て外部委託	3 全て自社対応	5 実施していない
2 一部外部委託(一部自社対応)	4 不明	

[Q72]. 貴社のデジタル・フォレンジックの効果についてお選びください。（○印はそれぞれひとつだけ）

1. 訴訟対応	非常に大きい	大きい	小さい	ない	わからない
2. 不正侵入の立証	非常に大きい	大きい	小さい	ない	わからない
3. 内部犯行の立証	非常に大きい	大きい	小さい	ない	わからない
4. 事故(障害)対応	非常に大きい	大きい	小さい	ない	わからない
5. データ復旧・回復	非常に大きい	大きい	小さい	ない	わからない
6. 労務管理	非常に大きい	大きい	小さい	ない	わからない
7. 犯罪抑止	非常に大きい	大きい	小さい	ない	わからない
	非常に大きい	大きい	小さい	ない	わからない

[Q73]. 貴社でのデジタル・フォレンジックの実施における阻害要因をお選びください。（複数選択可）

1 コストパフォーマンス	4 人的リソース・スキルの不足
2 業務効率への影響	5 社内制度による情報取扱いの制限
3 機密情報の外部への流出リスク	6 その他[ ]

[Q74]. 貴社においてデジタル証拠取得時に重要であると思うものをお選びください。（複数選択可）

1 記録が保存されている	7 取得した情報が正しい
2 誰の行為であるか記録されている	8 他の関連した記録がすべて保存されている
3 いつの行為か記録されている	9 記録内容のバージョン管理ができている
4 記録内容が変更されていない	10 他の記録と整合性がある
5 どのように発生したか記録されている	11 異常を検知し、その対処記録が残されている
6 記録の意味を証明できる	12 その他[ ]

[Q75]. 貴社においてデジタル証拠として有効なデータをお選びください。（複数選択可）

1 アクセスログ(サーバ側)	5 電子メール(サーバ側)	9 各種ファイルのプロパティ情報
2 イベントログ(サーバ・クライアント側)	6 電子メール(クライアント側)	10 ネットワーク上のパケット
3 ネットワークログ	7 レジストリ情報(サーバ・クライアント側)	11 その他[ ]
4 操作ログ(サーバ・クライアント側)	8 Cookie(クライアント側)	

[Q76]. 貴社のログ管理に導入している機能・手法をお選びください。（複数選択可）
統合ログ管理ツールを使用している場合は、その機能をお選びください。

1 第三者機関発行のタイムスタンプ機能	5 ホスト型IDS(改ざん検知)
2 ライトワンス型メディア(CD-R、 DVD-Rなど)	6 不明
3 ハッシュ値を用いた電子署名	7 その他[ ]
4 外部保管(改ざん防止)	

[Q77]. 貴社のログの保存期間をお選びください。（○印はひとつだけ）

1 保存していない	4 3ヶ月以上 1年未満	7 5年以上 7年未満
2 1ヶ月未満	5 1年以上 3年未満	8 7年以上
3 1ヶ月以上 3ヶ月未満	6 3年以上 5年未満	9 保存期間を決めていない

[Q78]. 貴社のログの保存期間を決める基準をお選びください。（○印はひとつだけ）

1 保存していない	3 ストレージ容量	5 その他[ ]
2 法令・規制	4 基準を決めていない	

［第5章］ 次に、共通番号制度についてお伺いします。

[Q79]. 「国民 ID」や「社会保障・税に関わる番号」などの共通番号が導入された場合（民間企業でも使えるようになった場合）、貴社の業務で利用しますか。（○印はひとつだけ）

1 利用する（予定含む）	2 利用しない（予定含む）	3 不明・わからない

[Q80]. 貴社の業務で共通番号を利用する場合どのようなメリットがありますか。（複数選択可）

1 必要な情報が随時取得できる	5 行政保有情報の利用によりデータ正確性が向上する
2 手続が簡略化できる	6 情報が管理しやすくなる
3 内部の事務処理が効率的に行える	7 入力ミスなどによるデータの誤りが減少する
4 他組織への情報提供事務が効率化される	8 その他[ ]

[Q81]. 貴社の業務で共通番号を利用する場合どのような懸念がありますか。（複数選択可）

1 必要な情報が取得できなくなる	6 他組織への情報提供元として責任が発生する
2 手続が煩雑化する	7 取得情報の正確性が自組織で求めるレベルと異なる
3 内部の事務処理が効率的に行えなくなる	8 取得情報に誤りがあってもわからない
4 情報管理が困難になる	9 その他[ ]
5 情報漏えいした場合の責任がとれない	

[Q82]. 貴社の業務で共通番号を利用する場合どのような対策が必要となりますか。（複数選択可）

1 情報セキュリティ・ポリシー/プライバシ・ポリシーの見直し	5 外部の監査／認証を受ける
2 リスク分析のやり直し	6 今のままで十分
3 情報セキュリティ機器のリプレース	7 その他[ ]
4 情報セキュリティ体制の見直し	

[Q83]. 年金記録問題はデータ保有組織（社会保険庁）が保有するデータの正確性が大きな問題となりました。番号制度においてデータの正確性を確保するために有効と思われる取組みはどのようなものと考えますか。（○印は2つまで）

1 データ保有組織による正確性確保の法的義務（罰則あり）	5 第三者機関によるデータ保有組織の監督・調査
2 データ保有組織による正確性確保の努力	6 第三者機関によるデータ内容の監視・調査
3 本人による正確性確保の法的義務（罰則あり）	7 正確性確保の取組みは不要
4 本人による正確性確保の努力	8 その他[ ]

［第6章］ その他

[Q84]. 次の出来事について、ご存知のものをご選択ください。（複数選択可）

1 Sony個人情報流出（2011年）	5 米ロッキード社へのサイバー攻撃	9 アディダス社員Twitter中傷事件
2 みずほ銀行システム障害（2011年）	6 韓国農協へのサイバー攻撃	10 ヤマト運輸携帯Webサイトの脆弱性
3 Amazon EC2 障害（2011年）	7 サンプル百貨店個人情報流出	11 尖閣諸島中国漁船衝突映像流出
4 CLOUD9 障害（2011年）	8 三井情報個人情報流出（2010年）	12 大阪地検特捜部証拠改竄事件

[Q85]. 次の用語について、ご存知のものをご選択ください。（複数選択可）

1 SQLインジェクション	8 マッシュアップコンテンツ悪用型	15 Jailbreak（脱獄）
2 BCP/BCM	9 Stuxnet	16 APT攻撃
3 インシデントハンドリング	10 Night Dragon	17 ゼロデイ攻撃
4 ボットネット/ゾンビPC	11 Operation Aurora	18 標的型攻撃
5 Gumblar（ガンブラー）	12 マン・イン・ザ・ミドル（中間者）攻撃	19 短縮URL
6 SAS70/SSAE16	13 Sys Trust	20 ISAE3402
7 Android向けウィルス	14 XSS（クロスサイトスクリプティング）	21 Spearphishing（スピアフィッシング）

[Q86]. プライバシーマークや ISMS、共通番号制度、デジタル・フォレンジックについて、忌憚の無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。