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。本調査では、研究の一環として、情報セキュリティマネジメントの取組み状況、情報セキュリティへの管理体制と人材育成、情報セキュリティのガバナンス、営業秘密の管理、クラウド・コンピューティング、事業継続計画の調査を行い、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、記入頂ける範囲で結構ですので、是非ともご回答くださいますようお願い申し上げます。

従業員数・売上高（または予算額）等は、2013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、すべての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、ご記入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。調査の分析結果につきましては、上記に配慮した上で11月中旬に本学のホームページ（http://www.iisec.ac.jp/）上で公開する予定です。

お忙しい中、大変恐縮ではございますが、調査回答票は**2013年8月23日（金曜日）までにご投函**くださいますようお願い申し上げます。

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
※不在のことが多い為、お手数ではございますが、
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まない。
営業秘密	営業秘密とは、不正競争防止法に記載されている「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」のこと。また、同法上で営業秘密として保護されるためには、3 つの要件<①秘密として管理されていること（秘密管理性）、②有用な情報であること（有用性）、③公然と知られていないこと（非公知性）>を満たす必要がある。 所属の組織が官公庁などの場合、営業秘密を「機密情報」に置き換えた上、ご回答ください。
情報資産の分類	企業・組織の保有する情報から洗い出された情報資産に対し、機密性、完全性、可用性の3つの側面から重要性を検討し、分類する。
事業継続計画(BCP)	潜在的損失によるインパクトの認識を行い実行可能な継続戦略の策定と実施、事故発生時の事業継続を確実にする継続計画。事故発生時に備えて開発、編成、維持されている手順及び情報を文書化した事業継続の成果物。

[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。
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］ 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 社長室又は役員室	11 情報システム開発部門
2 人事部門	7 企画部門	12 事業部門
3 経理部門	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、飲食店	17 複合サービス事業（郵便局、共同組合）
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、インターネット付随サービス業、映像・音声・文字情報制作を含む）	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]の年間売上高 （○印はひとつだけ。対象期間:2012 年 4 月 1 日から 2013 年 3 月 31 日）
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）	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	

[Q5]. 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

[Q6]. 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 50台以下 （保有していないを含む）	4 501～1,000台	7 5,001～10,000台
2 51～300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

[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 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

［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]. 貴社ではプライバシーマーク(P マーク)またはISMSを取得していますか。（○印はひとつだけ）

1 いずれも取得	3 ISMSのみ取得
2 Pマークのみ取得(設問[Q10]へお進みください)	4 いずれも取得していない(設問[Q10]へお進みください)

[Q9]. ISMSを管理している部門をお答えください。(複数選択可)

1 総務部門	6 社長室又は役員室	11 情報システム開発部門
2 人事部門	7 企画部門	12 事業部門
3 経理部門	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 法務部門
5 リスク管理担当部門	10 コンプライアンス担当部門	15 その他[ ]

[Q10]. 情報セキュリティ上の脅威のうち、現時点で重視するものはどれですか。(○印は**3つ**まで)

1	クライアントソフトの脆弱性をついた攻撃	4	ウィルスを使った遠隔操作	7	パスワード流出の脅威
2	機密情報を狙う諜報的な標的型攻撃の脅威	5	予期せぬ業務停止(人為ミス、ハードウェア障害、自然災害等)	8	内部犯行 (機密情報や個人情報の持出し)
3	スマートデバイスを狙った悪意あるアプリの横行	6	ウェブサイトを狙った攻撃(サイト内の情報取得、改ざん等)		

[Q11]. 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

[Q12]. 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	4	法律・条令の改正	7	新たな脅威への対応
2	社内組織の改編	5	他社の情報セキュリティ事故発生	8	情報資産の棚卸
3	業務内容の変更	6	自社の情報セキュリティ事故発生	9	その他 [ ]

[Q13]. リスク分析を行う際の問題点について、最も近い番号にひとつずつ○印を付けてください。

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 必要となる情報の収集が難しい	1	2	3	4
5 上司の理解がない	1	2	3	4
6 関係部署の協力が得られない	1	2	3	4

[Q14]. 外部委託している運用中のシステムのセキュリティ管理は、どのような手法を用いていますか。(複数選択可)

1	外部委託業務はない	4	立入監査	7	その他[ ]
2	ヒアリング、観察	5	第三者による監査結果の入手		
3	定期報告書の受領	6	委託先にまかせている		

[Q15]. システム部門以外の従業員に対して、情報セキュリティ教育を行っていますか。(○印はひとつだけ)

1	全従業員を対象に行っている	3	実施計画または予定がある(現在は未実施)
2	一部の従業員を対象に行っている	4	行う予定はない

[第3章] 情報セキュリティ管理体制と人材育成に関してお伺いします

[Q16]. 情報セキュリティ管理体制についてお伺いします。

16-1. 情報セキュリティを主に管理されているのは、どなたですか。(○印はひとつだけ)

1 情報システム部門(業務・メール・ネットワーク等の管理部門)の従業員が担当している
2 情報セキュリティ部門の従業員が担当している
3 総務等管理部門の従業員が兼務して担当している
4 パソコンに詳しい従業員が対応している(1～3以外の部門)
5 特に定めていない
6 その他[ ]

16-2. 情報セキュリティの管理を担当されている方は何名いますか。(○印はひとつだけ)

1	0 人	4	5～9人
2	1人	5	10人以上
3	2～4人		

[Q17]. 情報セキュリティの推進者の人材育成に関してどのような制度等がありますか。(複数選択可)

1 専門性を高める為に、専門学校・大学・大学院へ会社負担で派遣する制度がある
2 大学・大学院へ入学を希望する場合は、費用や時間のサポート制度がある
3 制度は無いが、希望する従業員へは費用や時間の支援を行っている
4 外部研修会・セミナーに積極的に参加させている(費用は会社負担)
5 自己啓発を奨励し資格取得者への報奨制度(一時金・資格手当等)がある
6 特に定めていない

[Q18]. 貴社で今後必要と思われる情報セキュリティ関連の資格は何ですか。(複数選択可)

1	情報セキュリティ技術関連(暗号・ネットワーク等)	3	情報セキュリティ運用関連(インシデント管理等)
2	情報セキュリティマネジメント関連(ISMS 等)	4	情報セキュリティ審査員・監査関連

[Q19]. 情報セキュリティ関連の資格保有を組織の活動に利用していますか。(複数選択可)

1 採用や異動の参考にしている	4 取得奨励金(一時金)制度がある
2 人事評価(昇進)に利用している	5 現在は何も利用していない
3 対外的なアピールに利用している	6 その他[ ]

[Q20]. 情報セキュリティに関する従業員への教育(集合研修・E ラーニング等)に関してお伺いします。

20-1. 従業員への教育は年間何回位実施していますか。(○印はひとつだけ)

1 1 回	4 4 回以上
2 2 回	5 実施していない
3 3 回	

20-2. 従業員への教育は年間延べ何時間位実施 していますか。(○印はひとつだけ)

1 1 時間未満	4 5 時間以上 10 時間未満
2 1 時間以上 3 時間未満	5 10 時間以上
3 3 時間以上 5 時間未満	6 実施していない

20-3. 上記従業員への教育の効果を確認していますか。(複数選択可)

1 テストを実施している	3 特に実施していない
2 感想文・レポート・アンケートを提出させている	4 その他[ ]

[第4章] 情報セキュリティのガバナンスについてお伺いします

[Q21]. IT ガバナンスの定義について次のうちから自分の考えに近いものを選んでください。(○印はひとつだけ)

1	ITガバナンスは、システムの開発、運用、変更管理やアクセス制御等の手続きをいう	5	ITガバナンスは、システムの開発や運用の仕様に関わる取引先への要求事項をいう
2	ITガバナンスは、業務上遂行されるプロセスに関して行われる電子承認や電子証跡などのITの機能をいう	6	ITガバナンスは、システムの開発や運用の仕様に関わる取引先からの要望事項をいう
3	ITガバナンスは、内部統制の一部でIT全般統制のことをいう	7	ITガバナンスは、企業が競争優位性の構築を目的としてIT戦略の策定及び実行をコントロールし、あるべき方向へと導く組織能力をいう
4	ITガバナンスは、システムの運用管理に関するベストプラクティスを示すフレームワークをいう	8	ITガバナンスは、ITのリスクマネジメントとパフォーマンスマネジメントを実施するにあたっての健全性確保のためのコンプライアンスマネジメントの確立をいう

[Q22]. 情報セキュリティポリシー(全体)の策定・見直しの手続きについてお伺いします。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	情報セキュリティポリシーはない
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	その他 [ ]
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		

[Q23]. 情報セキュリティポリシー(全体)についてお伺いします。過去 3 年(2010 年以降)でどの'管理策の項目'を見直しましたか。(複数選択可)

1 セキュリティ基本方針全般	6 通信及び環境セキュリティ(含む監視)	11 遵守(コンプライアンス)
2 情報セキュリティのための組織	7 アクセス制御	12 3年以内に新規作成した
3 資産管理	8 情報システムの取得、開発及び保守	13 3年間は管理策の見直しがない
4 人的資源のセキュリティ	9 情報セキュリティ・インシデント管理	14 情報セキュリティポリシーはない
5 物理的・環境的セキュリティ	10 事業継続管理	15 その他[ ]

[Q24]. 過去 3 年で情報セキュリティポリシーを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	3年間は管理策の見直しがない
5	監査などの指摘事項の対応	10	情報セキュリティポリシーはない
6	事業継続計画(BCP/BCM)と緊急時対応	11	その他 [ ]

[Q25]. 情報セキュリティポリシーの中で委託先に関する項目はありますか。(○印はひとつだけ)

1 項目があり、委託先が守るべき項目を明記している	3 項目はなく、契約時に決めている
2 項目はあるが、委託先が守るべき事項は明記していない	4 項目はなく、契約時にも決めていない

[Q26]. 顧客の立場として、購買方針や調達方針(IT 委託、業務委託を含む)が策定されていますか。策定されている場合、個人情報保護および情報セキュリティに関する項目が含まれていますか。(各項目について○印はひとつだけ)

	調達・購買方針がある		調達・購買方針がない	その他
	左記項目を含む	左記項目を含まない		
26-1. 情報セキュリティに関する項目	1	2	3	[ ]
26-2. 個人情報保護に関する項目	1	2	3	[ ]

[Q27]. 顧客の立場として委託先・調達先を選定する際、情報セキュリティの観点から最も重要な項目はどれですか。

(各項目について○印はひとつだけ)

	機密情報(設計図面や顧客情報等)の漏えい	設備やシステム障害等による業務停止	不正確なデータや欠落による業務停止	該当する委託・調達はない	その他
27-1. IT サービスを委託する場合	1	2	3	4	[ ]
27-2. 生産や物流などの業務委託を行う場合	1	2	3	4	[ ]
27-3. 経理や給与計算等の業務委託を行う場合	1	2	3	4	[ ]
27-4. 原材料・部品・商品等を調達する場合	1	2	3	4	[ ]

[Q28]. 顧客の立場として委託先を選定する際に、情報セキュリティのリスク対応として要求している事項はどれですか。

(各項目について複数選択可)

	認証を要求する			契約(SLA等)に自組織基準を要求する	チェックシートの確認を要求する	委託・調達はあるが、要求しない	該当する委託・調達はない	その他
	ISMS認証	Pマーク認証	その他第三者認証					
28-1. IT サービスを委託する場合	1	2	3 [ ]	4	5	6	7	8 [ ]
28-2. 生産や物流などの業務委託を行う場合	1	2	3 [ ]	4	5	6	7	8 [ ]
28-3. 経理や給与計算等の業務委託を行う場合	1	2	3 [ ]	4	5	6	7	8 [ ]
28-4. 原材料・部品・商品等を調達する場合	1	2	3 [ ]	4	5	6	7	8 [ ]

[Q29]. 顧客の立場として委託先・調達先を選定する際に、下請けになる二次、三次といった委託先・調達先に情報セキュリティ管理(**個人情報保護を除く**)を要求していますか。該当するものを一つ選んでください。(各項目について○印はひとつだけ)

	孫請けは禁止している、もしくは一次委託先・調達先で完結している	一次委託先・調達先に任せており、情報セキュリティ管理について		全ての委託先・調達先に、情報セキュリティ管理を		該当する委託・調達はない
		要求していない	管理状況を報告させている	要求している	要求していない	
29-1. IT サービスを委託する場合	1	2	3	4	5	6
29-2. 生産や物流などの業務委託を行う場合	1	2	3	4	5	6
29-3. 経理や給与計算等の業務委託を行う場合	1	2	3	4	5	6
29-4. 原材料・部品・商品等を調達する場合	1	2	3	4	5	6

[Q30]. **受託者・供給者の立場**として、**顧客から**情報セキュリティのリスク対応を要求されていますか。(各項目について複数選択可)

	認証を要求される			契約(SLA等)に自組織基準を要求される	チェックシートの確認を要求される	受託・供給はあるが、要求されない	該当する受託・供給はない	その他
	ISMS認証	Pマーク認証	その他第三者認証					
30-1. IT サービスを受託する場合	1	2	3 [ ]	4	5	6	7	8 [ ]
30-2. 生産や物流などの業務を受託する場合	1	2	3 [ ]	4	5	6	7	8 [ ]
30-3. 経理や給与計算等の業務を受託する場合	1	2	3 [ ]	4	5	6	7	8 [ ]
30-4. 原材料・部品・商品等を供給する場合	1	2	3 [ ]	4	5	6	7	8 [ ]

[Q31]. 受託者・供給者の立場として、顧客に対して調達方針や情報セキュリティ方針において情報セキュリティ上の遵守事項の公開を望みますか。(各項目について○印はひとつだけ)

	WEB 等で常時、一般に公開して欲しい	常時公開不要、問合せ時に回答して欲しい	常時公開不要、見積時に提示して欲しい	該当する受託・供給はない	その他
31-1. IT サービスを受託する場合	1	2	3	4	5[ ]
31-2. 生産や物流などの業務を受託する場合	1	2	3	4	5[ ]
31-3. 経理や給与計算等の業務を受託する場合	1	2	3	4	5[ ]
31-4. 原材料・部品・商品等を供給する場合	1	2	3	4	5[ ]

[Q32]. 外部との委託先・調達先に対する情報セキュリティガバナンスに関する下記のガイドライン、ツールについてご存知ですか。(各項目について○印はひとつだけ)

	利用している	読んだが利用していない	名前だけ知っている	知らない
32-1. 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
32-2. アウトソーシングに関する情報セキュリティ対策ガイダンス (経済産業省)	1	2	3	4
32-3. クラウドサービス利用のための情報セキュリティマネジメントガイドライン(経済産業省)	1	2	3	4
32-4. サプライチェーン情報セキュリティ管理 (JASA 日本セキュリティ監査協会)	1	2	3	4

[第5章] 営業秘密の管理についてお伺いします

[Q33]. 営業秘密の管理している部門をお答えください。(複数選択可)

1 総務部門	6 社長室又は役員室	11 情報システム開発部門
2 人事部門	7 企画部門	12 事業部門
3 経理部門	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 法務部門
5 リスク管理担当部門	10 コンプライアンス担当部門	15 その他[ ]

[Q34]. 以下にあげる情報を営業秘密として扱っていますか。(複数選択可)

1 仕入先・取引先の情報(商品の原価など金額情報)	5 製造方法
2 仕入先・取引先の情報(顧客の情報)	6 製造図面
3 ソフトウェア仕様	7 従業員情報(派遣社員情報等を含む)
4 経営情報(取締役会議事録等)	8 その他 [ ]

[Q35]. 営業秘密を秘密度に応じて区分(極秘、秘、社外秘等)していますか。(○印はひとつだけ)

1 区分している	3 区分していない(設問[Q38]へお進みください)
2 区分しているが、徹底されていない	4 その他[ ]

[Q36]. 営業秘密を秘密度に応じて区分するための基準について明文化されていますか。(○印はひとつだけ)

1 明文化されている	3 明文化されておらず、周知もされていない
2 明文化されているが、周知されていない	4 わからない

[Q37]. 秘密度に応じて区分した営業秘密の適応範囲を教えてください。(○印はひとつだけ)

1 全社的に統一している	3 会社・組織としては定めておらず、事業部門に任せている
2 会社・組織のルールで事業部門ごとに取り決めている	4 その他[ ]

設問[Q38]～[Q41]では、情報セキュリティ上の「情報資産の機密度(機密度 3、機密度 2、機密度 1 等)に応じた分類」と「営業秘密の秘密度に応じた区分」との関係についてお尋ねします。

[Q38]. 情報資産を機密度に応じて分類していますか。(○印はひとつだけ)

1 機密度に応じて分類している	2 機密度に応じて分類していない

[Q39]. 情報資産の機密度と営業秘密の秘密度は関連付けられていますか、それとも区別されていますか。(○印はひとつだけ)

1 機密度と営業秘密の秘密度は関連付けられている	2 機密度と営業秘密の秘密度は別体系で区別されている

[Q40]. 営業秘密の管理について、以下の中からお困りの点を選択してください。また、その他にお困りの点がありましたらコメント欄にご記入ください。(複数選択可)

1	営業秘密によっては、時間の経過と共に秘密度が変化する為、管理が煩雑になる	4	営業秘密が膨大である為、情報資産の機密度に応じた分類を行う上で手間がかかる
2	営業秘密を区分する基準が不明確であり、判断の基準がぶれてしまう	5	情報資産の機密度に応じた分類と営業秘密の秘密度に応じた区分が別体系であり、管理に手間がかかる
3	秘密度に応じて区分を行う者が限られている為、時間を取られる	6	情報資産の機密度と営業秘密の秘密度の管理方法が異なる為、現場運用が煩雑になる
コメント: [ ]			

[Q41]. 情報資産の機密度と営業秘密の秘密度との対応関係について、どのような考えをお持ちですか。
(○印はひとつだけ)

1	秘密度に機密度を対応させる必要がある	3	別体系で区別していればよい
2	秘密度に機密度を対応させる必要はない	4	その他[ ]

[第6章] クラウド・コンピューティング(クラウド)についてお伺いします

[Q42]. 貴社では、クラウドを利用していますか。(○印はひとつだけ)

1	利用している	3	利用を検討している
2	利用を予定している	4	利用する予定はない

[Q43]. 以下の情報セキュリティの第三者認証制度または情報公開制度を知っていますか。知っている場合、クラウドサービスの選定材料として利用または利用を予定していますか。

認証制度・情報公開制度等	選択項目		
	知っており、選定材料として利用している、または利用予定である	知っているが、選定材料として利用していない	知らない
1 ISMS 認証	1	2	3
2 P マーク認証	1	2	3
3 ITSMS 認証	1	2	3
4 SOC1(旧 SAS70 type2)	1	2	3
5 SOC2	1	2	3
6 SOC3(SysTrust・WebTrust)	1	2	3
7 BCMS 認証	1	2	3
8 PCI DSS	1	2	3
9 情報セキュリティ報告書	1	2	3
10 情報セキュリティ対策ベンチマーク	1	2	3
11 クラウドサービス情報開示認定制度(ASP・SaaS 情報開示認定)	1	2	3
12 クラウドサービス情報開示認定制度(IaaS・PaaS 情報開示認定)	1	2	3
13 クラウドサービス情報開示認定制度(データセンター情報開示認定)	1	2	3
14 Security, Trust & Assurance Resources(STAR)	1	2	3

[第7章] 貴社の事業継続計画ついてお伺いします

[Q44]. 貴社では事業継続計画(BCP)を策定していますか。(○印はひとつだけ)

1	策定している	3	策定を検討している
2	策定を予定している	4	策定する予定はない

[Q45]. 設問[Q44]で 1, 2 とお答えいただいた方にお伺いします。想定する脅威は何ですか(複数選択可)

1	地震 (噴火)	5	サイバー攻撃	9	不祥事(品質問題等)
2	津波、洪水、竜巻、台風	6	個人情報漏えい事故(サイバー攻撃以外)	10	大規模システム障害
3	火事	7	大規模停電	11	その他 [ ]
4	パンデミック(インフルエンザ等)	8	紛争、事変、戦争、武力衝突、テロなど		

[Q46]. 貴社では IT サービス継続に係る事業継続計画(IT-BCP)を策定していますか。(○印はひとつだけ)

1	策定している	3	策定を検討している
2	策定を予定している	4	策定する予定はない

[Q47]. 貴社において事業インパクトが大きいのはどちらですか。

1	ITサービスの停止	2	個人情報の漏えい

［第8章］ その他

[Q48]. 次の出来事について、ご存知なものをご選択ください。(複数選択可)

1	gooID への不正ﾛｸﾞｲﾝ要求(2013 年)	11	JINS ｵﾝﾗｲﾝｼｮｯﾌﾟ ｸﾚｶ情報流出	21	ｺﾈｸﾄﾌﾘｰによるｱｶｳﾝﾄ無断取得
2	攻撃者による不正国際 IP 電話発信	12	Yahoo! JAPAN ID の流出(2013 年)	22	農林水産省へのｻｲﾊﾞｰ攻撃
3	Anonymous による opJapan(2012 年)	13	NTT ﾃﾞｰﾀ委託職員偽造ｶｰﾄﾞ事件	23	Flame(Flamer)の脅威(2012 年)
4	秋田市個人情報流出事故(2012 年)	14	NewYorkTimes への攻撃(2013 年)	24	AP 通信の Twitter ハッキング
5	偽画面によるﾌｨｯｼﾝｸﾞ詐欺(2012 年)	15	遠隔操作ｳｨﾙｽ事件	25	My JR-EAST への不正ﾛｸﾞｲﾝ要求
6	Evernoteﾕｰｻﾞ情報流出(2013年)	16	「不正ｱｸｾｽ禁止法」改正(2012 年)	26	韓国へのｻｲﾊﾞｰ攻撃(2013 年 3 月)
7	ﾌｧｰｽﾄｻｰﾊﾞﾃﾞｰﾀ消失事故(2012 年)	17	ｽﾏﾎｱﾌﾟﾘによる個人情報流出	27	ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略最終案の策定
8	Apache の不正ﾓｼﾞｭｰﾙを用いた改竄	18	尖閣諸島中国漁船衝突映像流出	28	米国報告書「弾力的軍事ｼｽﾃﾑ及び先進的ｻｲﾊﾞｰ脅威」の発表(2013年3月)
9	AdobeReader の脆弱性(2013 年 2 月)	19	Java の脆弱性(2013 年 1 月)		
10	住基ﾈｯﾄの大規模障害(2013 年 3 月)	20	Operation Ababil		

[Q49]. 次の用語ついて、ご存知なものをご選択ください。 (複数選択可)

1	SpyEye	12	OAuth	23	ﾗﾝｻﾑｳｪｱ
2	BCP	13	ﾊｸﾃｨﾋﾞｽﾄ	24	SLA
3	CGI 版 PHP の脆弱性	14	ｴｸｽﾌﾟﾛｲﾄｷｯﾄ	25	Apache
4	2 要素認証(2段階認証)	15	WEP	26	WSUS 更新ﾌﾟﾛｸﾞﾗﾑ(KB2734608)
5	ﾜﾝﾀｲﾑﾊﾟｽﾜｰﾄﾞ	16	SIP	27	幽霊ﾄﾞﾒｲﾝ名
6	Shamoon(W32.Disttrack)	17	Office365	28	APT
7	弱い暗号鍵の無効化(KB2661254)	18	資産管理ｻｰﾊﾞ	29	Stuxnet
8	Open Resolver	19	Gauss	30	ﾀｯﾌﾟｼﾞｬｯｸ攻撃
9	pharming詐欺	20	Anonymous	31	Flashback
10	RAT	21	J-CSIP	32	Android向けｳｨﾙｽ
11	61398部隊	22	ﾏｲﾅﾝﾊﾞｰ法案可決(2013 年)	33	Need to Knowの原則

[Q50]. 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。