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、スマートフォンとクラウド、標的型攻撃への対応、アクセス制御と証跡（ログ）管理、個人情報漏えい事故のお詫び金及び情報セキュリティに関するリスク分析の実施状況の調査を行い、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、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2011年4月1日から2012年3月31日とし、従業員数・売上高（または予算額）などは2012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、調査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、調査回答票は**2012年8月20日（月）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。

[本調査における用語]

用 語	用語の説明
スマートデバイス	スマートフォンおよびタブレット端末のこと。
クラウド・コンピューティング	インターネットを使ったコンピューティング・サービスの総称のこと。歴史的なコンピュータの利用形態から、1）自社のサーバを利用した（集中・分散自前処理）、2）ネットワークを利用して第三者サーバをアクセス（ネットワークサービス） 3）分散したユーザがサーバを意識せずサービスを受ける（クラウド・コンピューティング） に分けられる。
サイバー攻撃	コンピュータやネットワークに不正に侵入し、データの詐取や改ざん、システム破壊や機能不全に陥らせるなどを行うこと。
標的型攻撃	サイバー攻撃において、特定の企業や組織に対して、行われる攻撃のこと。
アクセス制御	一般的に正当な主体（人、装置、プロセス、通信データなど）にはネットワークや情報および情報システムにアクセスすることを許し、不当な主体のアクセスは拒否するような制御の事をいう。対象によって、1） 情報や情報システム 2）ネットワークセグメント間 3）建物、フロア、部屋などに対するアクセス制御がある。
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。
第三者が提供するサービス	対象とする組織に属さないが、業務上関係のある人・組織が、提供するセキュリティ管理策を含む、提供するサービスのこと。
ログ（log）	コンピュータシステムの動作、状態、操作状況、データ通信などを記録したもの。 OSの稼働状況を記録するシステムログ、システムへのログオン/ログオフを記録する認証操作ログ、データベースやファイルへのアクセスを記録するアクセス（監査）ログ、Applicationの起動・停止・コマンド実行などの情報を記録するアプリケーションログ、Webやファイヤーウォール等で利用状況・作業を記録するセッション（イベント）ログ等がある。

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	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]. 貴社の会社規模　（○印はひとつだけ）

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。
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。
3　旅館業であり、資本金 5 千万円以下または従業員 200 人以下。
4　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。
5　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。
6　全てに当てはまらない。

[Q5]. 貴社[単独]の年間売上高　（○印はひとつだけ。対象期間:2011 年 4 月 1 日から 2012 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		

[Q6]. 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

[Q7]. 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

[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。（○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

[第2章]　貴社のスマートデバイスの利用についてお伺いします。

[Q9]. スマートデバイスの業務利用※を認めていますか。（○印はひとつだけ）
※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。→[Q10へ、Q14まで回答ください]	2　認めていない（禁止している）→[Q15へ]

[Q10]. 認めているデバイスは以下のうち、どれにあてはまりますか。（○印はひとつだけ）

1	会社貸与のもののみ	2	会社貸与・個人所有両方	3	個人所有のもののみ

[Q11]. スマートデバイスの業務利用を認めるにあたって利用ルールを定めていますか。（〇印はひとつだけ）

1 規定/基準/ガイドライン等を策定した(もしくは改訂した)。
2 通達あるいは連絡文書等で周知した。
3 何もしていないが、必要と感じている。
4 携帯電話と同じ扱いにしており、何もしていない。
5 ノートPCと同じ扱いにしており何もしていない。
6 その他[ ]

[Q12]. セキュリティ上、どのようなことが懸念されますか。（複数選択可）

1 紛失／盗難されたデバイスからの情報漏洩
2 ユーザの意図しない情報開示(GPS情報など)
3 廃棄するデバイスのデータ復元による情報漏洩
4 フィッシング
5 マルウェア
6 通信の盗聴(無線LANなどから)
7 なりすまし(リモートアクセスや業務システム)
8 監視アプリなどによる、情報の漏えい
9 ダイヤラー(SMSや電話を勝手に利用するアプリ)
10 ネットワークの利用不可(輻輳による)
11 その他[ ]

[Q13]. どのようなセキュリティ対策をしていますか。（複数選択可）

紛失・盗難
1 社外への持ち出し禁止
2 デバイスのパスワードの設定
3 リモートワイプ／ロック
4 外部記憶媒体(SDカード等)の使用制限
5 内部/外部記憶媒体の暗号化

ネットワーク
6 社内ネットワークへのアクセス制限
7 通信の暗号化(VPNなど)
8 無線LANの使用制限(公衆無線LANのみ制限)
9 無線LANの使用制限(全ての無線LANの制限)
10 リモートアクセス時のパスワード
11 業務システム利用時のパスワード

マルウェア等
12 アプリの使用制限
13 公式マーケット以外の利用禁止
14 ウィルス対策ソフトの導入
15 OSのアップデート
16 アプリのアップデート
17 改造の禁止

その他
18 機能(GPS、カメラなど)の使用制限
19 MDM(モバイルデバイス管理)
20 その他[ ]

[Q14]. 運用上、どのようなことが課題になっていますか。（複数選択可）: 回答終了後、第 3 章へお進みください。

1 デバイスのセキュリティレベルを合わせられない。(ウィルス対策やアプリの制限・パスワード設定など)
2 従業員が使用しているデバイスの把握ができない
3 利用者に利用ルールを守らせることができない。
4 私物を勝手に(許可なく)業務に利用している。
5 その他[ ]

[Q15]. [Q9]で「2」を選択した場合にご回答ください。スマートデバイスの業務利用を認めない理由は何ですか。（複数選択可）

1 組織として意思決定ができていない。
2 特に要望がない
3 コストの問題
4 セキュリティ上の懸念
5 個人所有のものの扱いが決められない。
6 その他[ ]

[Q16]. セキュリティ上、どのようなことが懸念されますか。（複数選択可）

1 紛失／盗難されたデバイスからの情報漏洩
2 ユーザの意図しない情報開示(GPS情報など)
3 廃棄するデバイスのデータ復元による情報漏洩
4 フィッシング
5 マルウェア
6 通信の盗聴(無線LANなどから)
7 なりすまし(リモートアクセスや業務システム)
8 監視アプリなどによる、情報の漏えい
9 ダイヤラー(SMSや電話を勝手に利用するアプリ)
10 ネットワークの利用不可(輻輳による)
11 その他[ ]

[Q17]. 運用上、どのようなことが課題になると予想されますか。（複数選択可）

1 デバイスのセキュリティレベルを合わせられない。(ウィルス対策やアプリの制限・パスワード設定など)
2 従業員が使用しているデバイスの把握ができない
3 利用者に利用ルールを守らせることができない。
4 私物を勝手に(許可なく)業務に利用される。
5 その他[ ]

［第3章］ 貴社のクラウド・コンピューティング（クラウド）についてお伺いします。

[Q18]. クラウド・コンピューティングを利用していますか。（〇印はひとつだけ）

1 利用している →[Q19へ]
2 利用を予定している →[Q21へ]
3 未利用だが、利用を検討したい →[Q21へ]
4 未利用であり、利用するつもりもない→[Q21へ]

[Q19]. クラウド・コンピューティング（複数ある場合は最大のサービス）の利用料金形態は以下のいずれでしょうか。

1 利用ユーザ数毎の課金
2 サービスメニュー単位の定額課金(ユーザ数関係なし)
3 利用ユーザ数の上限(例:50ユーザまで)毎の定額課金
4 ユーザ利用者毎・サービス毎の従量制
5 その他[ ]

[Q20]. クラウド・コンピューティング（複数ある場合は最大サービス）の利用者登録の形態は以下のいずれでしょうか。

1 アクセス管理(ユーザの設定、維持、退職などによる削除)は、自社担当者が行う
2 アクセス管理は、クラウド・サービス側に依頼して行う。
3 アクセス管理は、利用ユーザに任されている。
4 その他[ ]

[Q21]. 自組織管理下にあるシステムに対するセキュリティ上の脅威と、クラウド・コンピューティングに対するセキュリティ上の脅威とで、どちらの脅威が大きいと感じますか。（○印は一つだけ）

1 自組織管理下にあるシステム	2 同じ	3 クラウド

[Q22]. 従来のアウトソーシング（ホスティング）に対するセキュリティ上の脅威と、クラウド・コンピューティングに対するセキュリティ上の脅威とで、どちらの脅威が大きいと感じますか。（○印は一つだけ）

1 従来のアウトソーシング	2 同じ	3 クラウド

［第4章］ 貴社の標的型攻撃への対応についてお伺いします。

[Q23]. 「標的型攻撃」という言葉を知っていますか。（○印はひとつだけ）（注）言葉の意味は「本調査における用語」を参照ください。

1 知っている	2 少し知っている	3 知らない

以降の質問[Q24]～[Q32]は、[Q23]で「1」若しくは「2」を選択した方への質問になります。「3」を選択した方は、第 5 章へ進んでください。

[Q24]. 標的型攻撃に関連するキーワードで知っているものを教えてください。（複数選択可）

1 APT（Advanced Persistent Threat）	8 RAT（Remote Access Tool）
2 なりすましメールを利用した攻撃	9 C&Cサーバ（Command and Control サーバ）
3 外部媒体（USBメモリなど）を利用した攻撃	10 入口対策（メールフィルタ、ウィルス対策など）
4 社外Webサイトなどへの不正アクセス	11 出口対策（プロキシ認証、Webフィルタリングなど）
5 ソーシャルエンジニアリング	12 SPF （Sender Policy Framework）認証
6 企業ネットワークへの潜伏活動	13 サイバー情報共有イニシアティブ（J-CSIP）
7 データの不正アップロード	14 サイバーインテリジェンス情報共有ネットワーク

[Q25]. 標的型攻撃又は標的型攻撃と思われる攻撃を受けた経験はありますか。（○印はひとつだけ）

1 受けたことがある→[Q26]へ	2 受けたことはない→[Q28]へ	3 受けているかどうかわからない→[Q28]へ

[Q26]. それはどのような攻撃手法でしたか。（複数選択可）

1 メールによるもの	4 不正アクセスによる社内ネットワークへの侵入によるもの
2 外部媒体（USBメモリなど）によるもの	5 その他[ ]
3 社外Webサイトへの不正アクセスによるもの	

[Q27]. その攻撃をどうやって発見しましたか。（複数選択可）

1 社内ネットワーク上の機器で不審な動作を発見した	5 外部からの情報提供内容を元に社内調査をして発見した
2 不審メールを受信した申告があり調査により発見した	6 マルウェア感染を検知し発見した
3 外部との不正な通信を自ら発見した	7 その他[ ]
4 外部団体から申告があり調査により発見した	

[Q28]. 標的型攻撃対策を行っていますか。（○印はひとつだけ）

1 行っている→[Q29]へ	2 特に行っていない→[Q32]へ	3 わからない→[Q32]へ

[Q29]. どのような対策を行っていますか。（複数選択可）

1 メール対策強化	6 Adobe,JRE セキュリティパッチ適用強化	11 内部ネットワーク監視強化
2 Webアクセス対策強化	7 標的型攻撃セキュリティ教育	12 インシデントレスポンス強化
3 外部媒体対策強化	8 標的型攻撃対策訓練	13 CSIRTの立ち上げ
4 マルウェア検知強化	9 情報資産の分類と管理強化	14 攻撃事例、ノウハウの収集
5 マイクロソフトセキュリティパッチ適用強化	10 各種システム監視及びログ監視強化	15 その他[ ]

[Q30]. 標的型攻撃の検知や対策を行う上で困っていることがあれば教えてください。（複数選択可）

1 攻撃手法や攻撃事例に関する情報が少ない	4 導入すべきセキュリティ関連製品がわからない
2 どうやって対策をしていいかわからない	5 特に困っていない
3 攻撃を検知することが難しい	6 その他[ ]

[Q31]. 標的型攻撃の検知や対策で困っていることへ、今後必要だと思う事を教えてください。（複数選択可）

1 攻撃手法や攻撃事例に関する情報を公開して欲しい	3 攻撃を検知するノウハウを公開して欲しい
2 具体的な対策方法を共有して欲しい	4 その他[ ]

[Q32]. 今後どのような対策が必要だとおもいますか。（複数選択可）

1 メール対策強化	6 Adobe,JRE セキュリティパッチ適用強化	11 内部ネットワーク監視強化
2 Webアクセス対策強化	7 標的型攻撃セキュリティ教育	12 インシデントレスポンス強化
3 外部媒体対策強化	8 標的型攻撃対策訓練	13 CSIRTの立ち上げ
4 マルウェア検知強化	9 情報資産の分類と管理強化	14 攻撃事例、ノウハウの収集
5 マイクロソフトセキュリティパッチ適用強化	10 各種システム監視及びログ監視強化	15 その他[ ]

[第5章] 貴社のアクセス制御と証跡（ログ）管理についてお伺いします。

[Q33]. 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（2009 年以降）で見直した'管理策の項目'はなんですか。（複数選択可） 回答が、「12」～「14」の方は [Q35]へお進みください。

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無い
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無い
5	物理的・環境的セキュリティ	10	事業継続管理	15	その他[ ]

[Q34]. 過去 3 年で情報セキュリティポリシーの見直しがされた理由はなんですか。（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	6	BCP/BCM（事業継続計画）と緊急時対応
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	7	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。	8	その他
5	監査などの指摘事項の対応		[ ]

[Q35]. 次にアクセス制御に関してお伺いします。セキュリティポリシーでは、アクセス制御に係る以下の管理策を採用していますか。（1.採用していない、2.採用しているが不十分 3.採用して活用出来ている）

	管理策の内容	選択項目		
1	アクセス制御方針（利用者毎のアクセス制御規則・権利）を文書化し、業務ルールとして公表している。	1	2	3
2	利用者の登録・削除の手順が確立しており、与えられる利用権限が組織の規定と合致を確認している。	1	2	3
3	特権（管理者権限）の割当て及び利用は、制限され、管理（記録され、確認がなされる）されている。	1	2	3
4	パスワード管理プログラム（申請・身元確認・承認、仮パスワード発行・再発行等）として運用されている。	1	2	3
5	管理者は正式に利用者のアクセス権を定められた間隔でレビューしている。	1	2	3
6	利用者にパスワード設定ルール（桁数・文字列制限、辞書掲載語句の使用禁止など）を要求している。	1	2	3
7	利用者が一定時間席を外す場合や無人装置には、保護対策（スクリーン制御等）を備える規定がある。	1	2	3

[Q36]. セキュリティポリシーでは、アクセス制御に係る[Q35]の管理策を採用し難い、もしくは活用し難いものがありましたら、それを強化するにはどの様な方策を取るべきであると考えますか。（複数選択可）

1	経営陣から組織方針（権限分離等）や実践指針が提示され、利用者等が規定に従うように指示するべきである。
2	登録・管理を効率化するためにシステム・インフラを整備するべきである。
3	利用者等への教育活動を行うべきである。
4	定期的な社内レビュー、若しくは第三者（社内・社外）からの監査を受けるべきである。
5	現状で全く問題ない。
6	その他[ ]

[Q37]. セキュリティポリシーでは、アクセス制御に係る以下の管理策（ネットワーク・OS）を採用して活用出来ていますか。（1. 採用していない 2. 採用しているが不十分 3. 採用して活用出来ている）

	管理策の内容	選択項目		
1	ネットワークサービスの利用に関して、方針（アクセス権の許可される人の定義や、登録・承認手続）を文書化し、業務ルールとして公表している。	1	2	3
2	遠隔利用(リモート・アクセス等)を管理する為の認証方法（ﾊｰﾄﾞｳｪｱﾄｰｸﾝなど）が定義され、管理されている。	1	2	3
3	無線ネットワーク・アクセスの認証管理策（装置識別やネットワーク接続の制限等）を実施している。	1	2	3
4	オペレーションシステム（OS）への特権アクセスは、方針（アクセス許可される人の定義、登録・承認手続）を文書化し、業務ルールとして公表している。	1	2	3
5	OS への特権によるログオンは、ログオンの記録（利用者個人の ID, 端末等）がログに残る。	1	2	3
6	OS への特権によるログオンは、許容失敗回数（例えば 3 回）や試行時間を制限している。	1	2	3
7	リスクの高い業務用ソフトウェアやユーティリティ（データ修正,データ転送等）は使用制限している。	1	2	3

[Q38]. セキュリティポリシーでは、アクセス制御に係る[Q37]の管理策を採用し難い、もしくは活用し難いものがありましたら、それを強化するにはどの様な方策を取るべきであると考えますか。（複数選択可）

1	経営陣から組織の規定（外部アクセス等）及び実践指針が提示されるべきである。
2	ネットワーク及びネットワークサービスは技術進歩が速いので、外部専門家に任せるべきである。
3	登録・管理を効率化するためにシステム・インフラを整備するべきである。
4	経営陣から組織の規定（特権アクセス等）及び実践指針が提示されるべきである。
5	オペレーション及び運用保守サービスは、セキュリティに強い外部専門家（第三者）に任せるべきである。
6	登録及び証跡（ログ）管理を効率化するためにシステム・インフラを整備するべきである。
7	オペレーション・運用保守担当者への技術教育活動を行うべきである。
8	定期的な社内レビュー、若しくは第三者（社内・社外）からの監査を受けるべきである。
9	現状で全く問題ない。
10	その他[ ]

[Q39]. セキュリティポリシーでは、アクセス制御に係る以下の管理策（情報・業務プログラム）を採用して活用出来ていますか。（1. 採用していない　2. 採用しているが不十分　3. 採用して活用出来ている）

	管理策の内容	選択項目		
1	情報は、組織に対しての価値、法的要求事項、取扱の重要性等から分類し、ラベル付している。	1	2	3
2	情報は重要性の分類に従い、処理、保存、伝達、破棄を含む取扱い手順を定めている。	1	2	3
3	利用者・サポート要員による情報及び業務プログラムへのアクセスは、方針（アクセスが許可される人の定義、登録・承認手続）を文書化し、業務ルールとして公表している。	1	2	3
4	取扱いに慎重を要する情報を扱うシステムは、専用（隔離された）環境で動かしている。	1	2	3
5	モバイル・コンピューティング（ノート型 PC，携帯電話などを用いた移動・外出先からのアクセス）のリスク（盗聴、盗難等）が定義され、正式な対応方針が作成されている。	1	2	3
6	テレワーキング（所属組織外から要員が遠隔作業する）のための方針、運用手順書が策定されている。	1	2	3

[Q40]. セキュリティポリシーでは、アクセス制御に係る[Q39]の管理策を採用し難い、もしくは活用し難いものがありましたら、それを強化するにはどの様な方策を取るべきであると考えますか。（複数選択可）

1 経営陣から組織規定（情報取扱い方針等）及び実践指針が提示されるべきである。
2 経営陣から組織規定（モバイルコンピューティング等）及び実践指針が提示されるべきである。
3 経営陣から組織規定（テレワーキング等）及び実践指針が提示されるべきである。
4 運用保守サービスは、セキュリティに強い外部専門家（第三者）に任せるべきである。
5 ファイル/プログラムアクセスの証跡（ログ）管理を効率化するためにシステム・インフラを整備するべきである。
6 利用者等への教育活動を行うべきである。
7 定期的な社内レビュー、若しくは第三者（社内・社外）からの監査を受けるべきである。
8 現状で全く問題ない。
9 その他[　　]

[Q41]. セキュリティポリシーでは、ログ管理（監視）に係る以下の管理策を採用して活用出来ていますか。（1. 採用していない　2. 採用しているが不十分　3. 採用して活用出来ている）

	管理策の内容	選択項目		
1	ネットワークセキュリティに関連した活動を記録できるように、適切なログ管理規定がある。	1	2	3
2	利用者の活動、例外処理等を記録した監査ログを取得し、将来の調査等ため一定期間保持している。	1	2	3
3	運用保守サービスの特権による作業は、時刻、関連ファイル、利用 ID 等が記録されレビューしている。	1	2	3
4	大規模な情報処理施設(データセンタ等)では、使用状況（特権操作、不認可アクセスの試み、警告又は不具合メッセージ、セキュリティ設定変更等）を監視する手順が決められ、リスクに応じてレビューしている。	1	2	3
5	ログ機能及びログ情報は，改ざん及び認可されないアクセスから保護されている。	1	2	3
6	情報処理システム内のクロックは、正確な時刻源（例えば Network Time Protocol）と同期させている。	1	2	3

[Q42]. セキュリティポリシーでは、ログ管理に係る[Q41]の管理策を採用し難い、もしくは活用し難いものがありましたら、それを強化するにはどの様な方策を取るべきであると考えますか。（複数選択可）

1 経営陣から組織規定（ログ管理方針等）及び実践指針が提示されるべきである。
2 ネットワーク及びネットワークサービスは、セキュリティに強い外部専門家（第三者）に任せるべきである。
3 証跡（ログ）管理を効率化するためにシステム・インフラを整備するべきである。
4 監査ログの取得・分析等のガイドラインを用意し、要員の教育を行うべきである。
5 定期的な社内レビュー、若しくは第三者（社内・社外）からの監査を受けるべきである。
6 現状で全く問題ない。
7 その他[　　]

[Q43]. ログ管理手順書が作成され、運用されていますか。（複数選択可）

1 重要度及び法的要請に基づく情報分類がされ、対象ログの取得、分析、報告の手順書が作成され、運用されている。
2 ネットワークセキュリティに関連したログ管理手順書が作成され、運用されている。
3 利用者の活動、例外及びセキュリティ事象を記録した監査ログの取得、保管の手順書が作成され、運用されている。
4 監査ログに対する定期的なレビュー、報告手順が作成され、運用されている。
5 重要な情報処理施設の使用状況を監視し、レビューする手順書が作成され、運用されている。
6 運用保守サービスの作業を記録し、レビューする手順書が作成され、運用されている。
7 障害のログを取得し、分析し、報告する手順書が作成され、運用されている。
8 公式なログ管理手順書はない。

[Q44]. 取得及び分析を行っているログの種類は何でしょうか。（複数選択可）

1 システムログ（OS 起動、コマンド指示）
2 アプリケーションログ（起動、停止、コマンド実行）
3 ネットワークイベント（セッション）ログ
4 認証・操作ログ（サーバ、クライアントのログイン・ログオフ）
5 アクセス（監査）ログ（業務ファイル、Data Base 等）
6 その他[　　]

[Q45]. ログ管理を効率化するのに、自動化ツールを使っていますか。（複数選択可）

1 自社ではログを保管しているが、システム化(情報を選別し・フォーマットを変換)していない。
2 自社でログ管理のシステム（情報を選別し、フォーマットを替え、保管する等）を開発・導入している。
3 自社に ベンダー(国内)提供の統合ログ管理パッケージを導入している。
4 自社に ベンダー(海外)提供の統合ログ管理パッケージを導入している。
5 自社内で、分析し、通報する機能までシステム化できている。
6 ログの取得、分析、報告は第三者ベンダーに任せている。
7 自社ではログ管理(OS, DB, Network等)していない。
8 その他[ ]

[Q46]. ログ保管期間はどのように規定（対象ログ限定）していますか。（〇印はひとつだけ）

1 保存していない
2 1か月未満
3 1～3 か月未満
4 3か月以上～1 年未満
5 1 年以上～3 年未満
6 3 年以上～7 年未満
7 7 年以上～
8 保存期間を決めていない（規定がない）

[Q47]. ログ管理を効率化するために一番必要なことは何だと考えますか。（〇印はひとつだけ）

1 実践的なガイドライン
2 統合ログ管理ツールとその活用ノウハウ
3 外部サービスの活用
4 管理・分析要員の養成
5 その他[ ]

[第6章] 貴社の個人情報漏えい事故のお詫び金についてお伺いします。

[Q48]. プライバシーマークまたは ISMS を取得していますか。（〇印はひとつだけ）

1 いずれも取得
2 プライバシーマークのみ取得
3 ISMSのみ取得
4 いずれも取得していない

[Q49]. 個人情報漏えい事故発生時のお詫び金支払額についての基準を事前に定めていますか。（〇印はひとつだけ）

1 定めている
2 定めていない→(Q51へ)

[Q50]. 個人情報の種類（レベル）によって、お詫び金支払額が区分されていますか。（〇印はひとつだけ）

1 区分されている
2 区分されていない

[Q51]. 個人情報が漏えいした場合、1 名あたりに支払うべきお詫び金支払額はいくらが妥当であると考えますか。各項目につき〇印をひとつずつお付けください。50,001 円以上を選択した場合、具体的な数値をご記入下さい。

個人情報の種類	0 円	1～500 円	501～1,000 円	1,001～5,000 円	5,001～10,000 円	10,001～20,000 円	20,001～50,000 円	50,001 円以上 [具体的な数値]
1 電話番号	1	2	3	4	5	6	7	8 [ ]
2 身体情報	1	2	3	4	5	6	7	8 [ ]
3 カルテ	1	2	3	4	5	6	7	8 [ ]
4 購入に関する情報	1	2	3	4	5	6	7	8 [ ]
5 保有資産情報（土地建物等）	1	2	3	4	5	6	7	8 [ ]
6 債務情報	1	2	3	4	5	6	7	8 [ ]
7 口座番号	1	2	3	4	5	6	7	8 [ ]
8 遺言書	1	2	3	4	5	6	7	8 [ ]
9 与信ブラックリスト	1	2	3	4	5	6	7	8 [ ]

[第7章] 貴社のリスク分析の実施状況についてお伺いします。

[Q52]. 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。（〇印はひとつだけ）

1 半年未満→[Q53へ]
2 半年以上1年未満→[Q53へ]
3 1年以上2年未満→[Q53へ]
4 2年以上3年未満→[Q53へ]
5 3年以上前→[Q53へ]
6 実施していない→[Q58へ]

[Q53]. 情報セキュリティに関するリスク分析を定期的に行っていますか。（〇印はひとつだけ）

1 行っている→[Q54へ]
2 行っていない→[Q56へ]

[Q54]. 定期的な情報セキュリティに関するリスク分析を行うタイミングとしてあてはまるのはどれですか。（複数選択可）

1 ISMSやPマーク等の認証更新時
2 認証制度以外の監査時
3 規程類で定められている間隔
4 その他[ ]

[Q55]. 定期的な情報セキュリティに関するリスク分析の結果は、実際のセキュリティ対策に反映されていますか。（〇印はひとつだけ）

1 反映されている
2 どちらかといえば反映されている
3 どちらかといえば反映されていない
4 反映されていない

[Q56]. 2年以内(2010年4月～2012年3月)に定期的でない(非定期的な)情報セキュリティに関するリスク分析を実施しましたか。（○印はひとつだけ）

1	実施した→[Q57へ]	2	実施していない→[Q58へ]

[Q57]. 非定期的に情報セキュリティに関するリスク分析を実施した理由としてあてはまるのはどれですか。（複数選択可能）

1	内部規定の改訂	4	法律・条令の改正	7	自社の情報セキュリティ事故発生
2	社内組織の改編	5	東日本大震災の発生	8	新たに発生した脅威への対応
3	業務内容の変更	6	他社の情報セキュリティ事故発生	9	その他[ ]

[Q58]. リスク分析を行わない理由、またはリスク分析を行う際の問題点として、貴社の現状に最も近い番号にひとつずつ○印を付けて下さい。（1. そう思う 2. どちらかといえばそう思う 3. どちらかといえばそう思わない 4. そう思わない）

内容		評価結果			
1	リスク分析の実施方法が難しく、わかりづらい	1	2	3	4
2	リスク分析を行うことの意義が理解できない	1	2	3	4
3	リスク分析にかかる費用・時間がかかりすぎる	1	2	3	4
4	リスク分析を行う対象となる事柄の情報収集が難しい	1	2	3	4
5	定期的なリスク分析をどの程度の頻度で行うべきなのかわからない	1	2	3	4
6	非定期的なリスク分析をどのようなタイミングで行うべきかわからない	1	2	3	4

[Q59]. 情報セキュリティリスクに対する管理策の内容についてあてはまるのはどれですか。（○印はひとつだけ）

1	過剰である	3	ちょうど良い	5	不足している
2	やや過剰気味である	4	やや不足している	6	わからない

[Q60]. 情報セキュリティリスクに対する管理策の実業務への影響についてあてはまるのはどれですか。（○印はひとつだけ）

1	影響があり、改善が必要である	2	影響はあるが、許容範囲内である	3	影響はない

［第8章］ その他

[Q61]. 貴社の情報セキュリティ関連の資格の活用について教えてください。（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	その他[ ]
3	対外的なアピールに利用している	6	何もしていない→[Q63へ]

[Q62]. 貴社の今後必要と思われる情報セキュリティ関連の資格はなんですか。（複数選択可）

1	情報セキュリティ技術関連（暗号、ネットワークなど）	3	情報セキュリティ運用関連（ｲﾝｼﾃﾞﾝﾄ管理など）
2	情報セキュリティマネジメント関連（ISMS など）	4	情報セキュリティ審査員・監査関連

[Q63]. 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	ﾄﾞｺﾓ・KDDIの通信障害(2012年)	8	DigiNoter電子証明書不正発行	15	東証ｼｽﾃﾑ障害(2012年)
2	岡崎市立中央図書館事件(2010年)	9	Comodogate電子証明書不正発行	16	DropBoxｾｷｭﾘﾃｨ障害(2011年)
3	Google利用規約/ﾌﾟﾗｲﾊﾞｼﾎﾟﾘｼ統一	10	ｾﾃﾞｨﾅ ｶｰﾄﾞ/会員情報不正売却	17	「探偵ﾄﾞﾘﾗﾝﾄﾞ」無限増殖ﾊﾞｸﾞ
4	RSA社へのｻｲﾊﾞｰ攻撃(2011年3月)	11	GREE利用者ﾃﾞｰﾀ改竄(2011年)	18	暗号の2010年問題
5	ﾍﾞｸﾀｰ サーバー不正ｱｸｾｽ(2012年)	12	AppLogによる端末情報不正取得	19	地銀ﾈｯﾄﾊﾞﾝｸ不正ｱｸｾｽ(2011年)
6	三菱重工へのｻｲﾊﾞｰ攻撃(2011年)	13	PASMO履歴照会ｻｰﾋﾞｽ停止	20	LulzSecの活動停止(2011年)
7	連続自動入力ﾌﾟﾛｸﾞﾗﾑ不正ﾛｸﾞｲﾝ攻撃	14	衆議院へのｻｲﾊﾞｰ攻撃(2011年)	21	″The Movie″ﾏﾙｳｪｱ(2012年)

[Q64]. 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	Anonymous(ｱﾉﾆﾏｽ)	10	かんたんﾛｸﾞｲﾝ(携帯固有ID認証)	19	SHA-3
2	Duqu	11	ｼﾝｸﾞﾙｻｲﾝｵﾝ	20	ﾗﾝｻﾑｳｪｱ
3	偽ｾｷｭﾘﾃｨｿﾌﾄ	12	Koobface	21	ｶﾚﾛｸﾞ
4	DNS Changer	13	Twitterﾌｨｯｼﾝｸﾞ	22	Flame(Flamer)
5	ｽﾏｰﾄﾌｫﾝ向けﾌｨｯｼﾝｸﾞｻｲﾄ	14	Stuxnet	23	CISPA
6	ｺﾝﾌﾟｶﾞﾁｬ(ｺﾝﾌﾟﾘｰﾄｶﾞﾁｬ)	15	EU個人情報保護指令改正案	24	SOPA
7	Identity Theft	16	BYOD	25	Black Hat
8	ForcefulBrowsing(強制ﾌﾞﾗｳｽﾞ)	17	RMT(ﾘｱﾙﾏﾈｰﾄﾚｰﾃﾞｨﾝｸﾞ)	26	Guidelines for Smart Grid Cyber Security (NISTIR 7628)
9	Adobe Reader Xの保護モード	18	DEFCON CTF		

[Q65]. スマートデバイス、クラウド、標的型攻撃、ログ取得と利活用、個人情報漏えい事故のお詫び金、情報セキュリティマネジメントの取組みについて、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。