セキュリティ担当者意識調査

2008年11月実施

※本調査は、大川情報通信基金（平成19年度）によるものです。

予備調査

※実際の調査では、青色の注意書きは表示されません。

Q1 あなたの職業をお知らせください。【必須】

- ○ 会社役員・経営者
- ○ 会社員（管理職）
- ○ 会社員（一般社員）
- ○ 公務員・教職員・団体職員（管理職）
- ○ 公務員・教職員・団体職員（一般職員）
- ○ 契約社員・派遣社員　→終了
- ○ 自営業・自由業　→終了
- ○ パート・アルバイト　→終了
- ○ 専業主婦　→終了
- ○ 学生　→終了
- ○ 無職（定年退職含む）　→終了
- ○ その他　→終了

【----------改ページ----------】

Q2 あなたはご自身の組織の情報セキュリティ対策（特にネットワークセキュリティ対策）に関する業務をされていますか。【必須】

- ○ はい
- ○ いいえ　→終了

【----------改ページ----------】

Q3 あなたはその業務にどれくらいの期間、携わってますか。【必須】

- ○ 1年未満　→終了
- ○ 1年以上3年未満
- ○ 3年以上

【----------改ページ----------】

Q4 あなたの現在の役職をお答え下さい。【必須】

- ○ 社長・CEO・COO
- ○ 役員・CIO
- ○ 部長・事業部長

- ○ 次長・課長
- ○ 係長・主任
- ○ その他
- ○ 役職なし　→終了

【----------改ページ----------】

Q5 あなたは全社的な情報セキュリティ対策（特にネットワークセキュリティ対策）についてどの程度ご存知ですか。【必須】

- ○ ほとんど全て把握している　<GO>
- ○ ある程度は把握している　<GO>
- ○ あまり把握していない
- ○ 全く把握していない

本調査

※実際の調査では、青色の注意書きは表示されません。

Q1 あなたがお勤めの会社が該当する業種について最も近いものを1つお選びください。【必須】

- ○ 食品
- ○ 繊維・アパレル
- ○ 紙・パルプ
- ○ 化学
- ○ 医薬
- ○ 医療
- ○ 石油・ガス
- ○ 鉄鋼・金属
- ○ 機械・精密機器
- ○ 電機機器
- ○ 自動車製造業
- ○ その他の製造業
- ○ 銀行
- ○ 証券
- ○ 商社・流通・卸
- ○ 小売
- ○ 鉄道・航空
- ○ 運輸
- ○ コンサルティング・シンクタンク
- ○ マスコミ・出版・印刷・広告
- ○ 情報処理・ソフトウェア・SE
- ○ ISP・CATV・xDSL事業
- ○ その他通信・放送
- ○ その他のサービス業
- ○ 建設・土木・不動産
- ○ 福祉
- ○ 教育・研究機関
- ○ 電力

- ○ 保険
- ○ その他金融
- ○ 農林水産漁業・鉱業
- ○ その他　具体的に記入してください。【FA必須】

【----------改ページ----------】

Q2 あなたがお勤めの会社の従業員数（派遣、アルバイトを含む）をお選びください。【必須】

- ○ 9人以下
- ○ 10～49人
- ○ 50～99人
- ○ 100～299人
- ○ 300～999人
- ○ 1,000～2,999人
- ○ 3,000～4,999人
- ○ 5,000～9,999人
- ○ 10,000～99,999人
- ○ 100,000～149,999人
- ○ 150,000人以上

Q3 あなたがお勤めの会社の派遣、アルバイトの割合をお選びください。【必須】

- ○ 5%未満
- ○ 5%～9%
- ○ 10%～14%
- ○ 15%～19%
- ○ 20%～24%
- ○ 25%～29%
- ○ 30%～34%
- ○ 35%～39%
- ○ 40%～44%
- ○ 45%～49%
- ○ 50%以上
- ○ わからない

【----------改ページ----------】

Q4 あなたがお勤めの会社の年間売上をお選びください。【必須】

- ○ 1千万円未満
- ○ 1千万円以上～5千万円未満
- ○ 5千万円以上～1億円未満
- ○ 1億円以上～5億円未満
- ○ 5億円以上～30億円未満
- ○ 30億円以上～50億円未満
- ○ 50億円以上～100億円未満
- ○ 100億円以上～500億円未満
- ○ 500億円以上～1千億円未満
- ○ 1千億円以上

Q5 あなたがお勤めの会社の上場の有無をお選びください。【必須】

- ○ 上場
- ○ 非上場

【----------改ページ----------】

Q6 あなたがお勤めの会社の事業は、国家や社会基盤、経済基盤に与える影響の観点から、どの程度の公益性がありますか。
該当するものを選んでチェックをつけてください。【必須】

- ○ ほとんどない
- ○ 少ない
- ○ 他の業種に比べると高い
- ○ 事業の性質上極めて高い

Q7 あなたがお勤めの会社の主要な業務に関わる業務プロセスのうち、情報システム（社外のシステムを含む）およびインターネットに依存している割合はどの程度ですか。
該当するものを選んでチェックをつけてください。【必須】

	一部にとどまる	若干依存している	多くの部分が	ほとんどの部分が

	(25%以下)	(25%以上、50%以下)	依存している(50%以上、75%以下)	依存している(75%以上)
情報システム(社外のシステムを含む)	○	○	○	○
インターネット	○	○	○	○

【----------改ページ----------】

Q8 あなたがお勤めの会社において、電子商取引(EC)業務の売上が、全体の売上に占める割合を1つ選んで、チェックをつけてください。傘下事業所(支社・支店・出張所等)も含めてご回答ください。

ここではEC業務として、物流(物流手配、出荷、輸送管理)、顧客から対価を受取るサービスの提供、販売(見積・商談、販売計画、販売促進、受注管理、顧客情報管理、請求、決済)、金融分野における決済代行、振込・送金、預金獲得、融資、保険契約等の、売上げに直結する業務を想定します。【必須】

- ○ 0%
- ○ 10%
- ○ 20%
- ○ 30%
- ○ 40%
- ○ 50%
- ○ 60%
- ○ 70%
- ○ 80%
- ○ 90%
- ○ 100%

Q9 あなたがお勤めの会社における情報セキュリティの担当者数(外注は含みません)に関して当てはまるものを選んでチェックをつけてください。【必須】

- ○ 0人
- ○ 9人以下
- ○ 10～49人
- ○ 50～99人
- ○ 100～299人
- ○ 300～999人
- ○ 1,000～2,999人
- ○ 3,000～4,999人
- ○ 5,000～9,999人
- ○ 10,000人以上

Q10 あなたがお勤めの会社において存在する役職を全て選んで、チェックをつけてください。【必須(チェックはいくつでも)】

- [ ] 最高情報責任者（CIO）
- [ ] 最高セキュリティ責任者（CSO）
- [ ] 最高リスク管理責任者（CRO）
- [ ] 最高プライバシー責任者（CPO）
- [ ] 最高情報セキュリティ責任者（CISO）
- [ ] 最高コンプライアンス責任者（CCO）
- [ ] あてはまるものはない　<EX>

【----------改ページ----------】

Q11 あなたがお勤めの会社におけるパソコンの台数（リースやレンタルも含む）で該当するものを選んでチェックをつけてください。【必須】

- ○ 10台未満
- ○ 10～ 99台
- ○ 100～999台
- ○ 1,000台以上

Q12 あなたがお勤めの会社におけるサーバの台数（リースやレンタルも含む）で、該当するものを選んでチェックをつけてください。【必須】

- ○ 5台未満
- ○ 5～9台
- ○ 10～29台
- ○ 30～49台
- ○ 50～99台
- ○ 100～499台
- ○ 500～999台
- ○ 1,000台以上
- ○ 全てアウトソースしているので0台
- ○ サーバは必要ないので0台

【----------改ページ----------】

Q13 あなたがお勤めの会社では情報セキュリティ対策の運用についてどのような方針をお持ちでしょうか。
以下の中から最も近いものを1つ選んで、チェックをつけてください。【必須】

- ○ 全て自社で運用する方針である　→ Q15へ
- ○ 現在は運用をアウトソースしているが、将来的にはできるだけ自社で運用したい　→ Q15へ
- ○ 現在は自社で運用しているが，将来的にはできるだけアウトソースしたい
- ○ 原則としてアウトソースする方針である
- ○ 上記のような方針は特にない　→ Q15へ

【----------改ページ----------】

Q14 Q13で<ANS Q13>を選んだ方におうかがいします。
その理由として、あてはまるものを全て選んで、チェックをつけてください。【必須(チェックはいくつでも)】

- □ コスト削減のため
- □ 社内に適当な人材がいないため
- □ 専門家に依頼したほうが安全・確実なため
- □ 統合セキュリティサービスが必要なため
- □ その他　具体的に記入してください。　【FA必須】

【回答引継ぎ】
【----------改ページ----------】

Q15 あなたがお勤めの会社における情報セキュリティに対する取り組みの方針や目的について、それぞれ該当するものを各項目1つずつ選んで、チェックをつけてください。【必須】

	よくあてはまる	どちらかといえばあてはまる	どちらかといえばあてはまらない	全くあてはまらない
情報セキュリティ対策は重要な経営課題である	○	○	○	○
リスクマネジメントの一環として	○	○	○	○
事業を推進する上で必須の項目である	○	○	○	○
セキュリティ事故によるブランドイメージの失墜や業績の悪化を未然に防止するため	○	○	○	○
顧客に提供する製品やサービスに一定レベルのクオリティを確保するため	○	○	○	○
社会的責任を果たすため	○	○	○	○

企業としての競争力を高める（他社の製品やサービスとの差別化を図るため	○	○	○	○
ビジネスプロセスの合理化の一環として	○	○	○	○
事業活動に情報セキュリティ活動を整合させることが重要であるため	○	○	○	○
法律や業界ガイドラインに従う必要があるため	○	○	○	○
他社の取り組み状況に遅れないようにするため	○	○	○	○
顧客・取引先との間に信頼関係を確立するため	○	○	○	○

Q16 情報セキュリティへの取り組みを実施したことによる効果について、それぞれ該当するものを各項目1つずつ選んで、チェックをつけてください。【必須】

	よくあてはまる	どちらかといえばあてはまる	どちらかといえばあてはまらない	全くあてはまらない
情報資産の見直しが実施できた	○	○	○	○
業務プロセスの見直し・修正が実施できた	○	○	○	○
業務が効率化された	○	○	○	○
ビジネスパートナーや顧客からの評価が高まった	○	○	○	○
案件の受注につながるなど，競争力が高まった	○	○	○	○
従業員の情報セキュリティに対する意識が向上した	○	○	○	○
業務効率や生産性が低下した	○	○	○	○
リスク管理の重要性に対する理解・認識が向上した	○	○	○	○
経営層による情報セキュリティへのコミットメントが得られた	○	○	○	○
情報セキュリティを企業の社会的責任として考えるようになった	○	○	○	○
社内における情報の共有・活用が進んだ	○	○	○	○
取引先の選定や，契約締結の判断をする際に，相手企業の情報セキュリティに対する取り組み状況を考慮するようになった	○	○	○	○
セキュリティ管理のトータルコストを削減することができた	○	○	○	○
提供する製品やサービスの質が向上した	○	○	○	○
組織における情報セキュリティマネジメント能力が向上した	○	○	○	○

Q17 あなたがお勤めの会社で実施している情報セキュリティマネジメントに関する対策について、それぞれ該当するものを各項目1つずつ選んで、チェックをつけてください。【必須】

	2年以上前から取り組んでいる	ここ2年以内に取り組んでいる	今後取り組むことを予定もしくは検討中	今後取り組む予定はない
全社的な情報セキュリティマネジメント	○	○	○	○
部門ごとの情報セキュリティマネジメント	○	○	○	○
業務上重要な事項に対するセキュリティ対策の実施	○	○	○	○
リスクマネジメントの観点からの情報セキュリティ対策の実施	○	○	○	○
PDCAサイクル等の情報セキュリティマネジメントサイクルの導入	○	○	○	○
ISMS等，情報セキュリティに関する何らかの認証の取得	○	○	○	○
パスワードルール等の情報セキュリティの基本事項の徹底	○	○	○	○
個人情報保護法対応	○	○	○	○
情報セキュリティ保険への加入	○	○	○	○
投資対効果に基づいた情報セキュリティ対策の実施	○	○	○	○
事業継続計画の策定	○	○	○	○
事業継続計画に沿った具体的な対策の実施	○	○	○	○
取引先企業に対する一定レベルの情報セキュリティ対策の実施要求	○	○	○	○
情報セキュリティ監査（内部）の実施	○	○	○	○
情報セキュリティ監査(外部)の実施	○	○	○	○
情報セキュリティ報告書の発行やCSR報告書への情報セキュリティ関連項目の記載	○	○	○	○
セキュリティポリシーの策定	○	○	○	○

Q18 あなたがお勤めの会社で実施している情報セキュリティに関する組織・体制面での対策について、それぞれ該当するものを各項目1つずつ選んで、チェックをつけてください。【必須】

	2年以上前から取り	ここ2年以内に取り	今後取り組むことを	今後取り組む予定は

	組んでいる	組んでいる	予定もしくは検討中	ない
情報セキュリティ担当責任者（CISO）の設置	○	○	○	○
情報セキュリティ担当部署の設置／明確化	○	○	○	○
情報セキュリティ担当スタッフの確保と役割の明確化	○	○	○	○
経営者による情報セキュリティへの取り組み方針（ポリシー）の明確化	○	○	○	○
セキュリティホール（脆弱性）情報の収集体制の構築・運用	○	○	○	○
情報セキュリティを担当する人材の育成	○	○	○	○
情報セキュリティに関する知識・ノウハウの継続的な蓄積と社内での共有	○	○	○	○
情報セキュリティインシデント対応手順の整備や対応体制（CSIRTなど）の確立・保有	○	○	○	○
社内における情報の共有・活用の推進	○	○	○	○
従業員への情報セキュリティ教育・研修	○	○	○	○
従業員の管理・監視や内部統制の強化	○	○	○	○
従業員の情報セキュリティに対する取り組みの業績評価への組み入れ	○	○	○	○
物理的セキュリティ対策	○	○	○	○
機密情報や重要情報の漏洩防止対策	○	○	○	○

【----------改ページ----------】

Q19 あなたがお勤めの会社のパソコンの利用状況について該当するものを1つ選び、チェックをつけてください。【必須】

- ○ 1人1台以上で利用している
- ○ 数人で1台利用している
- ○ 部課単位で数台利用している
- ○ 利用していない

Q20 あなたがお勤めの会社におけるメールボックス数について、該当するものを1つ選んで、チェックをつけてください。【必須】

- ○ 10未満
- ○ 10～99
- ○ 100～499
- ○ 500～999
- ○ 1000～4999

- ○ 5000以上

Q21 あなたがお勤めの会社における受信メール全体に占めるスパムメールの割合について、該当するものを1つ選んで、チェックをつけてください。【必須】

- ○ 81%以上
- ○ 80%
- ○ 60%
- ○ 40%
- ○ 30%
- ○ 10%
- ○ スパムメールはほとんど受信していない

【----------改ページ----------】

Q22 サーバについて、あなたがお勤めの会社で利用されているサーバの管理方法について、それぞれ該当するものを各項目1つずつ選んで、チェックをつけてください。【必須】

	利用していない	自社にサーバを設置して利用している	アウトソーシングでサーバを利用している	わからない
Webサーバ	○	○	○	○
メールサーバ	○	○	○	○
ファイルサーバ	○	○	○	○
DBサーバ	○	○	○	○
PROXYサーバ	○	○	○	○

Q23 あなたがお勤めの会社の情報セキュリティの投資効果の算出方法で該当するものを全て選び、チェックをつけてください。【必須(チェックはいくつでも)】

- ☐ ROI
- ☐ NPV
- ☐ IRR
- ☐ ROSI
- ☐ その他
- ☐ 不明 <EX>
- ☐ 計算していない <EX>

Q24 あなたがお勤めの会社の情報セキュリティ業務の外部委託割合を1つ選び、チェックをつけてください。【必須】

- ○ 0%
- ○ 1～20%
- ○ 21～40%
- ○ 41～60%
- ○ 61～80%
- ○ 81%～

Q25 あなたがお勤めの会社の情報セキュリティ教育で重要だと思われるもので該当するものを全て選び、チェックをつけてください。【必須(チェックはいくつでも)】

- □ セキュリティポリシー
- □ ネットワークセキュリティ
- □ アクセス制御システム
- □ セキュリティマネジメント
- □ セキュリティの経済側面
- □ セキュリティシステム構成
- □ 情報法科学(Information Forensics)
- □ 暗号関連
- □ セキュリティ投資／法律
- □ その他 _____ 【FA必須】

Q26 あなたがお勤めの会社で2年以上前から実施している技術的対策で該当するものを全て選び、チェックをつけてください。【必須(チェックはいくつでも)】

- □ ファイアウォール
- □ ウィルス対策ソフト
- □ スパイウェア対策ソフト
- □ アクセス制御（サーバ用）
- □ 侵入検知システム(IDS)
- □ 送信中のデータ暗号化
- □ ログ管理ソフトウェア
- □ アプリケーションファイアウォール
- □ ICカード
- □ ワンタイムパスワード
- □ フォレンジックスソフト
- □ PKI
- □ 検疫ネットワークシステム
- □ VPN
- □ パッチマネジメント
- □ 通信の暗号化
- □ URLフィルタリング
- □ 無線LANセキュリティソフト

- [ ] 保存ファイルの暗号化
- [ ] 生体認証システム
- [ ] その他
- [ ] 一般的なパスワード認証
- [ ] シンクライアント
- [ ] 実施していない <EX>
- [ ] 侵入防止システム（IPS）
- [ ] メールフィルタリング

【----------改ページ----------】

Q27 あなたがお勤めの会社で実施して2年未満である技術的対策で該当するものを全て選び、チェックをつけてください。【必須(チェックはいくつでも)】

- [ ] ファイアウォール
- [ ] ログ管理ソフトウェア
- [ ] 検疫ネットワークシステム
- [ ] ウィルス対策ソフト
- [ ] アプリケーションファイアウォール
- [ ] VPN
- [ ] スパイウェア対策ソフト
- [ ] ICカード
- [ ] パッチマネジメント
- [ ] アクセス制御（サーバ用）
- [ ] ワンタイムパスワード
- [ ] 通信の暗号化
- [ ] 侵入検知システム（IDS）
- [ ] フォレンジックスソフト
- [ ] URLフィルタリング
- [ ] 送信中のデータ暗号化
- [ ] PKI
- [ ] 無線LANセキュリティソフト
- [ ] 保存ファイルの暗号化
- [ ] 生体認証システム
- [ ] その他
- [ ] 一般的なパスワード認証
- [ ] シンクライアント
- [ ] 実施していない <EX>
- [ ] 侵入防止システム（IPS）
- [ ] メールフィルタリング

【絞り込み（非選択）設定← Q26 】
【----------改ページ----------】

Q28 あなたがお勤めの会社で情報セキュリティ確保のため、最も効果的だと思う対策を全て選び、チェックをつけてください。【必須(チェックはいくつでも)】

- [ ] 内部セキュリティ監査
- [ ] 技術者を対象にした情報セキュリティ教育
- [ ] ペネトレーションテスト
- [ ] マニュアル整備
- [ ] 脆弱性検査ソフト
- [ ] 社員のセキュリティ意識の向上
- [ ] メール監視ソフト
- [ ] 情報セキュリティポリシーの強化
- [ ] ウェブ監視ソフト
- [ ] その他
- [ ] 一般社員を対象にした情報セキュリティ教育
- [ ] 効果的な対策なし <EX>

Q29 あなたがお勤めの会社における情報セキュリティに関する業務を担当する人材に関しての問題点は何ですか。
該当するものを全て選び、チェックをつけてください。【必須(チェックはいくつでも)】

- [ ] 社内に必要な知識を持つ人材が少ない

- ☐ 技術の変化が早く、担当者の知識を保つのが難しい
- ☐ 人材の育成が難しい
- ☐ 採用募集しても条件にあう技術を持った人材が少ない
- ☐ 採用募集した人材の技術を測るのが難しい
- ☐ どのような人材を採用募集すればよいかわからない
- ☐ その他　具体的に記入してください。＿＿＿＿＿＿＿＿ 【FA必須】
- ☐ 特に問題はない　<EX>
- ☐ わからない　<EX>

Q30 あなたがお勤めの会社では、役職員等に対し、情報セキュリティ対策に関する教育をどのようにされていますか。
役職ごとに該当する教育手法の該当箇所全てにチェックをつけてください。【必須(それぞれチェックはいくつでも)】

	eラーニング	講習会やセミナーの実施・参加	関連情報の周知	特に実施していない <EX>
役員（経営トップを含む）	☐	☐	☐	☐
正社員・正職員	☐	☐	☐	☐
準社員・準職員・アルバイト	☐	☐	☐	☐

【----------改ページ----------】

Q31 あなたがお勤めの会社において、**正社員・正職員**対象に実施されている情報セキュリティ教育・研修のテーマはどのようなものですか。
以下の項目の中からあてはまるものを全て選んで、チェックをつけてください。【必須(チェックはいくつでも)】

- ☐ インターネットの仕組みなど技術的な項目
- ☐ 情報セキュリティに関する自社の制度（セキュリティポリシーの内容など）
- ☐ セキュリティ事故やそれによる損害の実例
- ☐ 自社業務における情報セキュリティの重要性および情報セキュリティへの取り組み
- ☐ ウィルス感染や情報漏洩等の情報セキュリティ侵害が発生したときの対処
- ☐ ウィルス対策やパッチ当ての方法や社内ルール
- ☐ パスワードルールやデータのバックアップ方法
- ☐ ソーシャルエンジニアリング（偽装電話等）への対処方法
- ☐ 情報資産へのアクセスコントロールに関する規定
- ☐ 機密情報や重要情報の取り扱い規定や社外への情報の持ち出しに関する規定
- ☐ 携帯PCのセキュリティ対策や社外利用時のルール
- ☐ 個人情報保護に関する社内ルール
- ☐ 内部統制に関する項目

情報セキュリティに関する法律やガイドライン

- [ ]
- [ ] 事業継続計画
- [ ] 物理的なセキュリティ
- [ ] その他 _____ 【FA必須】

【設問表示設定:[Q30-2-1] または[Q30-2-2] または[Q30-2-3]】
【----------改ページ----------】

Q32 あなたがお勤めの会社において、**準社員・準職員・アルバイト**を対象に実施されている情報セキュリティ教育・研修のテーマはどのようなものですか。
以下の項目の中からあてはまるものを全て選んで、チェックをつけてください。【必須(チェックはいくつでも)】

- [ ] インターネットの仕組みなど技術的な項目
- [ ] 情報セキュリティに関する自社の制度(セキュリティポリシーの内容など)
- [ ] セキュリティ事故やそれによる損害の実例
- [ ] 自社業務における情報セキュリティの重要性および情報セキュリティへの取り組み
- [ ] ウィルス感染や情報漏洩等の情報セキュリティ侵害が発生したときの対処
- [ ] ウィルス対策やパッチ当ての方法や社内ルール
- [ ] パスワードルールやデータのバックアップ方法
- [ ] ソーシャルエンジニアリング(偽装電話等)への対処方法
- [ ] 情報資産へのアクセスコントロールに関する規定
- [ ] 機密情報や重要情報の取り扱い規定や社外への情報の持ち出しに関する規定
- [ ] 携帯PCのセキュリティ対策や社外利用時のルール
- [ ] 個人情報保護に関する社内ルール
- [ ] 内部統制に関する項目
- [ ] 情報セキュリティに関する法律やガイドライン
- [ ] 事業継続計画
- [ ] 物理的なセキュリティ
- [ ] その他 _____ 【FA必須】

【設問表示設定:[Q30-3-1] または[Q30-3-2] または[Q30-3-3]】

Q33 あなたがお勤めの会社の情報セキュリティ対策について、現在の課題や問題点として該当するものを全て選んで、チェックをつけてください。【必須(チェックはいくつでも)】

- [ ] 社員のセキュリティに対する意識が低い
- [ ] 顕在化していない情報セキュリティに関する事故・トラブルがあるのではという不安

- [ ] 現在の対策が十分かどうかわからない
- [ ] 事故が発生した時の対応策が十分でない
- [ ] 情報セキュリティ対策に投じる費用対効果が見えにくい
- [ ] 実際に事故やトラブルがあったときの会社の損失が見えにくい
- [ ] 情報セキュリティ対策に精通している部門や社員がいない
- [ ] 部署ごとに独自の対策をしており、全社的なシステムが導入しづらい
- [ ] 対策についてどこから手をつければいいかわからない
- [ ] 情報セキュリティ対策をどの企業に依頼すればいいかがわからない
- [ ] その他　具体的に記入してください。 【FA必須】

Q34 情報セキュリティ関連投資に対するあなたがお勤めの会社の方針や考え方として、該当するものを全て選んで、チェックをつけてください。【必須(チェックはいくつでも)】

- [ ] 自社業務を確実に継続するために必要であれば，積極的にセキュリティ対策に投資する
- [ ] できるだけコストを抑えたいので，必要最小限のセキュリティ対策への投資に留めている
- [ ] 全社的に情報セキュリティ関連投資をおこなっている
- [ ] 部門ごとに情報セキュリティ関連投資をおこなっている
- [ ] 他のIT関連投資よりも優先度を高くしている
- [ ] 一般的な投資とほぼ重要度は同じである
- [ ] 業界ガイドラインに準拠する程度、あるいは他社と同程度の投資を行うようにしている
- [ ] リスク分析や情報資産の定量化を実施し、優先度の高い対策に対して投資している
- [ ] 投資対効果を算出し、効果が高い対策に投資している
- [ ] 投資対効果を算出していないが、効果があると思われる対策には積極的に投資している
- [ ] 効果が高いものであっても、投資額が高い場合には採用しない
- [ ] その他　具体的に記入してください。 _____ 【FA必須】

【----------改ページ----------】

Q35 あなたがお勤めの会社では過去2年間で、以下の事柄がどの程度、起こったことがありますか。
該当するものを各項目1つずつ選んで、チェックをつけてください。【必須】

	まったくない	1回あった	2～3回あった	4～5回あった	それ以上あった	わからない
故意による企業情報漏洩	○	○	○	○	○	○
故意による個人情報漏洩	○	○	○	○	○	○
過失による企業情報漏洩	○	○	○	○	○	○
過失による個人情報漏洩						

情報資産の盗難	○	○	○	○	○	○
外部者による不正アクセス	○	○	○	○	○	○
内部者による不正アクセス	○	○	○	○	○	○
ウィルスやワームの感染	○	○	○	○	○	○
DoS攻撃によるシステムダウン	○	○	○	○	○	○
ボットネット・スパイウェア感染	○	○	○	○	○	○
フィッシング	○	○	○	○	○	○
パスワード盗聴	○	○	○	○	○	○
迷惑メールによるシステム遅延	○	○	○	○	○	○
システム侵入	○	○	○	○	○	○
踏み台	○	○	○	○	○	○
データの破壊	○	○	○	○	○	○
ホームページの改竄	○	○	○	○	○	○
ノートPCなどの盗難	○	○	○	○	○	○
ソーシャルエンジニアリング	○	○	○	○	○	○
	まったくない	1回あった	2～3回あった	4～5回あった	それ以上あった	わからない

Q36 情報セキュリティ被害を受けたとき、自社にどのような影響を及ぼすと考えますか、また実際に被害にあったとき、どのような被害がありましたか。
該当するものを全て選んで、チェックをつけてください。【必須(チェックはいくつでも)】

- ☐ 売上高の減少
- ☐ 企業の信頼度の失墜
- ☐ ブランドイメージの悪化
- ☐ 顧客・取引先からの取引の停止
- ☐ 業務自粛等によるビジネス上の損害
- ☐ (元請け企業からの)契約義務違反による処罰
- ☐ 第三者認証(プライバシーマーク等)の剥奪
- ☐ 株価への影響
- ☐ 顧客離れ
- ☐ その他　具体的に記入してください。　【FA必須】

【----------改ページ----------】

Q37 情報セキュリティに関して、政府や自治体に行ってほしい施策はありますか。
該当するものを全て選んで、チェックをつけてください。【必須(チェックはいくつでも)】

- [ ] 侵害行為を取り締まる法制度の整備
- [ ] セキュリティ業者の評価・格付けの制度化
- [ ] 情報セキュリティに関する専門的な人材の資格制度化
- [ ] セキュリティサービス利用への助成
- [ ] 機器・ソフトウェア購入への助成
- [ ] 社員教育への助成
- [ ] 情報セキュリティに関する講習会・セミナー・研修の開催
- [ ] 各種製品・サービス情報の提供
- [ ] ウィルス、セキュリティホール等に関する警戒情報の提供
- [ ] ウィルス、セキュリティホール等に対する技術の開発
- [ ] その他　具体的に記入してください。　【FA必須】
- [ ] 特にない　<EX>

Q38 ここ2年間で、あなたがお勤めの会社の情報セキュリティ管理はどのようになったとお感じですか。
該当するものを1つだけ選んで、チェックをつけてください。【必須】

- ○ 情報セキュリティ管理が厳しくなった
- ○ 情報セキュリティ管理は甘くなった
- ○ 特に何も変わらない
- ○ その他　具体的に記入してください。＿＿＿＿＿＿＿＿　【FA必須】

Q39 企業内における情報管理を徹底させるためには、どのような方策が望ましいと思いますか。
お考えに近いものを5つまで選んで、チェックをつけてください。【必須（1 ～ 5個）】

- [ ] 会社の経営層の情報セキュリティ管理への参画
- [ ] 社員の情報セキュリティ教育の実施
- [ ] 社内の情報管理ルールの明確化
- [ ] 社内情報のアクセス権限の厳格化
- [ ] 社内で管理すべき情報の共有
- [ ] 社内ネットワークのアクセス権限の管理
- [ ] ウィルス対策ソフトやパッチ対策等のネットワークセキュリティの強化
- [ ] 会社のパソコンや携帯電話の利用ルールの明確化
- [ ] 情報管理に違反した社員に対する罰則

- [ ] 情報セキュリティマネジメントシステム(ISMS)、プライバシーマーク等の認証取得
- [ ] 公的機関による企業の情報セキュリティ管理レベルの公表
- [ ] 情報セキュリティに対する法規制など制度の強化
- [ ] その他　具体的に記入してください。＿＿＿＿＿＿＿＿ 【FA必須】
- [ ] 特に必要ない　<EX>

Q40 社内における情報セキュリティ担当者以外の社員の情報セキュリティ意識について、教えて下さい。
該当するものを1つだけ選んで、チェックをつけてください。【必須】

- ○ トップ、役員クラスから社員に至るまで情報セキュリティ意識は高い
- ○ トップ、役員クラス管理職クラスまでは意識が高いが、それより下になると意識は低い
- ○ トップ、役員クラスから部長クラスまでは意識が高いが、それより下になると意識は低い
- ○ 意識が高いのは、トップ、役員クラスまでである
- ○ 情報セキュリティ担当者以外は、意識は低い

Q41 今後、実施や導入を検討しているセキュリティ対策について優先度の高いものを5つまで選んで、チェックをつけてください。【必須（1 ～ 5個）】

- [ ] データ・電子メールの暗号化
- [ ] VPNの導入
- [ ] ウィルス対策ソフトウェアの導入
- [ ] スパイウェア対策ソフトウェアの導入
- [ ] メール・Webのフィルタリング
- [ ] ファイアウォールの導入
- [ ] OS・アプリケーションの堅牢化
- [ ] 不正侵入検知ツール(IDS)の導入
- [ ] Web改ざん検出ツールの導入
- [ ] バイオメトリクス認証ツールの導入
- [ ] PKI/デジタル証明書の導入
- [ ] ワンタイムパスワードツールの導入
- [ ] ポートスキャン検査の実施
- [ ] 脆弱性アセスメントの実施(脆弱性解析、擬似アタック等)
- [ ] ログ解析の実施

- [ ] セキュリティ監査・コンサルティングの実施
- [ ] リスク分析の実施
- [ ] 情報セキュリティポリシーの策定
- [ ] 社員教育の実施
- [ ] その他　具体的に記入してください。 _____ 【FA必須】