見　本

■セキュリティ管理やシステム運用に関する取り組み

Q49. 情報セキュリティについて、どのような対策を施していますか。 (各1つに○印)

	対策実施済み	現在、検討中	必要ない
1. セキュリティポリシーの策定	1	2	3
2. 全社的なセキュリティ管理者の配置	1	2	3
3. 部門ごとのセキュリティ管理者の配置	1	2	3
4. 従業員に対する情報セキュリティ教育	1	2	3
5. 重要なコンピュータ室への入退出管理	1	2	3
6. 重要なシステムへの内部でのアクセス管理	1	2	3
7. データの暗号化	1	2	3
8. ファイアウォールの配置	1	2	3
9. セキュリティ監視ソフトの導入	1	2	3
10. 外部専門家による常時セキュリティ監視	1	2	3
11. 外部専門家による定期的なシステム監査	1	2	3
12. 内部による定期的なシステム監査	1	2	3
13. 外部専門家による定期的な情報セキュリティ監査	1	2	3
14. 内部による定期的な情報セキュリティ監査	1	2	3

Q50. 貴社では過去1年間に情報漏洩のトラブルが発覚しましたか。 (1つに○印)

1. 内部者による情報漏洩のトラブルが発覚した
2. 委託先による情報漏洩のトラブルが発覚した
3. 内部者、委託先の両方で情報漏洩のトラブルが発覚した
4. なかった

Q51. 社内で使っているハードウエアやOS、ミドルウエアなどをすべて把握していますか。 (1つに○印)

1. 全社の最新情報を一元管理している
2. 一部の利用部門が勝手に導入している可能性を否定できない
3. 把握していない

Q52. システムを修整した際に、修整していない機能が従来通り正しく動作するかを確認する「回帰テスト」を実施していますか。 (1つに○印)

1. ルールに基づき情報システム部門が実施している
2. ルールはないが実施している
3. 外注先に任せている
4. 実施しない

Q53. IT全般統制に関わる従業員に、内部統制の確立に向けた教育を実施していますか。 (1つに○印)

1. 教育制度を設け、それに基づき実施している
2. 制度はないが実施している
3. 2007年度中に実施する予定
4. 2010年度までに実施する予定
5. 実施する予定なはい

SQ. Q53で「1. 実施している」、「2. 制度はないが実施している」と回答した方にのみうかがいます。
教育・研修に情報システム部門が関与していますか。 (1つに○印)

1. 責任部門として関与している
2. 責任部門ではないが、他部門を支援する形で関与している
3. ほとんど関与していない

Q54. セキュリティ・ホールなどシステムのぜい弱性を突いた外部からの攻撃、あるいはシステム障害、セキュリティ違反が発生した場合、どのように情報収集および社内外への伝達をしていますか。 (1つに○印)

1. あらかじめ定めたルールに従い実施している
2. ルールはないが、必要に応じて実施している
3. 特に何もしていない

見　本

Q55. システム企画・開発、運用保守など、情報システム関連業務にかかわるプロセス・統制・活動について、文書化および作業のモニタリングをしていますか。 **(1つに○印)**

1. すべて文書化しており、モニタリングもしている
2. 一部は文書化しており、モニタリングもしている
3. すべて文書化しているが、モニタリングはしていない
4. 一部は文書化しているが、モニタリングはしていない
5. 2007 年度中に文書化する予定
6. 2010 年度までに文書化する予定
7. 文書化の予定はない

Q56. 情報システムの運用作業について、以下の手順書を文書化していますか。A. B. についてそれぞれご回答下さい。

A. 標準的なオペレーション **(1つに○印)**

1. すべて文書化しており、文書に従い作業しているかどうか定期的に確認している
2. 一部は文書化しており、文書に従い作業しているかどうか定期的に確認している
3. すべて文書化しているが、作業の定期的な確認はしていない
4. 一部は文書化しているが、作業の定期的な確認はしていない
5. 2007 年度中に文書化する予定
6. 2010 年度までに文書化する予定
7. 文書化の予定はない

B. 本番システムにおけるプログラム変更、パッチ当て、ハードウエアの定期メンテナンス、機器更改などの作業 **(1 つに○印)**

1. すべて文書化しており、文書に従い作業しているかどうか定期的に確認している
2. 一部は文書化しており、文書に従い作業しているかどうか定期的に確認している
3. すべて文書化しているが、作業の定期的な確認はしていない
4. 一部は文書化しているが、作業の定期的な確認はしていない
5. 2007 年度中に文書化する予定
6. 2010 年度までに文書化する予定
7. 文書化の予定はない

Q57. 運用手順を守らせるために、どのような施策を実施していますか。 **(あてはまるものすべてに○印)**

1. パスワードで運用操作の権限を分けている
2. ワークフローシステムなどにより、責任者による承認がなければ作業が進まないような仕組みを盛り込んでいる
3. 運用現場の責任者に任せている
4. 運用オペレータ、一人ひとりの判断に任せている

Q58. BCP (ビジネス継続計画) についてうかがいます。以下に挙げる計画・体制がありますか。 **(各1つに○印)**

	ある	2007 年度中に作成予定	2010 年度までに作成予定	作成する予定はない
1. メインのデータセンターが災害などの被害にあった際に、事業を継続するためのバックアップ・センター	1	2	3	4
2. 災害などによるシステムの被害の大きさに応じた、システムの復旧計画	1	2	3	4
3. 災害や大規模なシステム障害など緊急時の連絡網	1	2	3	4

見　本

Q59. メインのデータセンター（委託している場合も含む）が完全に停止した際、貴社の事業活動はどうなりますか。　（1つに○印）

1. バックアップ用のデータセンターを使って、主要業務だけを継続できる
2. バックアップ用のデータセンターを使って、通常業務を継続できる
3. システムは動かないが、手作業で主要業務を継続できる
4. 事業活動は停止する

Q60. システム開発の契約締結前に、情報システム部門以外が契約内容を確認することがありますか。
以下の中から当てはまるものを選んで下さい。2を選んだ場合はカッコ内に金額もご記入下さい。　（1つに○印）

1. すべての案件について確認している
2. 一定金額（　　億円）以上など条件により確認している
3. 特に確認はしていない

SQ. Q60で「1. すべての案件について確認している」「2. 一定金額以上など条件により確認している」と回答した方にのみうかがいます。確認するのは誰ですか。　（あてはまるものすべてに○印）

1. 法務部門が確認している
2. 弁護士が確認している（社内外を含む）
3. 弁護士以外の外部の専門家が確認している

Q61. データセンターを集約していますか。　（1つに○印）

1. 2007年度中に集約する予定
2. 2010年度までに集約する予定
3. すでに集約した
4. 集約する予定はない

Q62.　Q49からQ61までの「セキュリティ管理やシステムの運用」について、海外拠点の状況をお聞かせ下さい。　（1つに○印）

1. 現地の状況が国内とは異なるので、各拠点の判断に任せている
2. 情報システム部門の人材を配置していないが、現地の利用部門に国内と同じ取り組みを要請している
3. 主要拠点に情報システム部門の人材を配置し、国内と同じレベルの取り組みができるような体制にしている
4. 海外に拠点がない

■ 企業イメージ

ITの活用が進んでいると思う企業を3社まで挙げて下さい（自社を除く）。対象は外資系を含む日本企業です。

	企業名	（↓何も記入しないで下さい）				
1 位						
2 位						
3 位						

＜最後に、ITベンダーとして事業を展開している企業の方にのみうかがいます。＞

Q63. 以下の項目について、PMBOK（プロジェクト・マネジメントの国際的な知識体系）などに基づき定めた規定集のようなものがありますか。
（各1つに○印）

	ある	2007年度中に定める予定	ない
1. システム開発プロジェクトの実施手順	1	2	3
2. プロジェクトで利用する「システム開発標準」	1	2	3
3. プロジェクトで作成する成果物	1	2	3
4. 仕様変更の管理方法	1	2	3
5. 成果物の管理方法	1	2	3
6. 開発作業の進捗の管理方法	1	2	3

質問は以上で終了です。お忙しいところ長時間ありがとうございました。