参考①

企業における情報セキュリティガバナンスのあり方に関する研究会　報告書

参考資料

情報セキュリティ対策ベンチマーク

１．評価システム

（１）全体の枠組み

情報セキュリティ対策ベンチマークは、普及啓発のため、多くの企業にとって利用しやすいWeb 上でのセルフチェックツールとして提供することを想定する。

ツールの機能としては､情報セキュリティ対策の取組状況に関するセルフチェックの結果から、回答企業の水準と望まれる水準のギャップを示すレーダーチャートや、全体のスコア、推奨される取組み等を表示する機能が想定される。

処理手順のイメージは次のとおり。

①評価項目に沿って、セルフチェックを実施

②企業プロフィールに基づき回答企業を分類した上で、該当する企業群に応じて適切な「望まれる水準」を設定

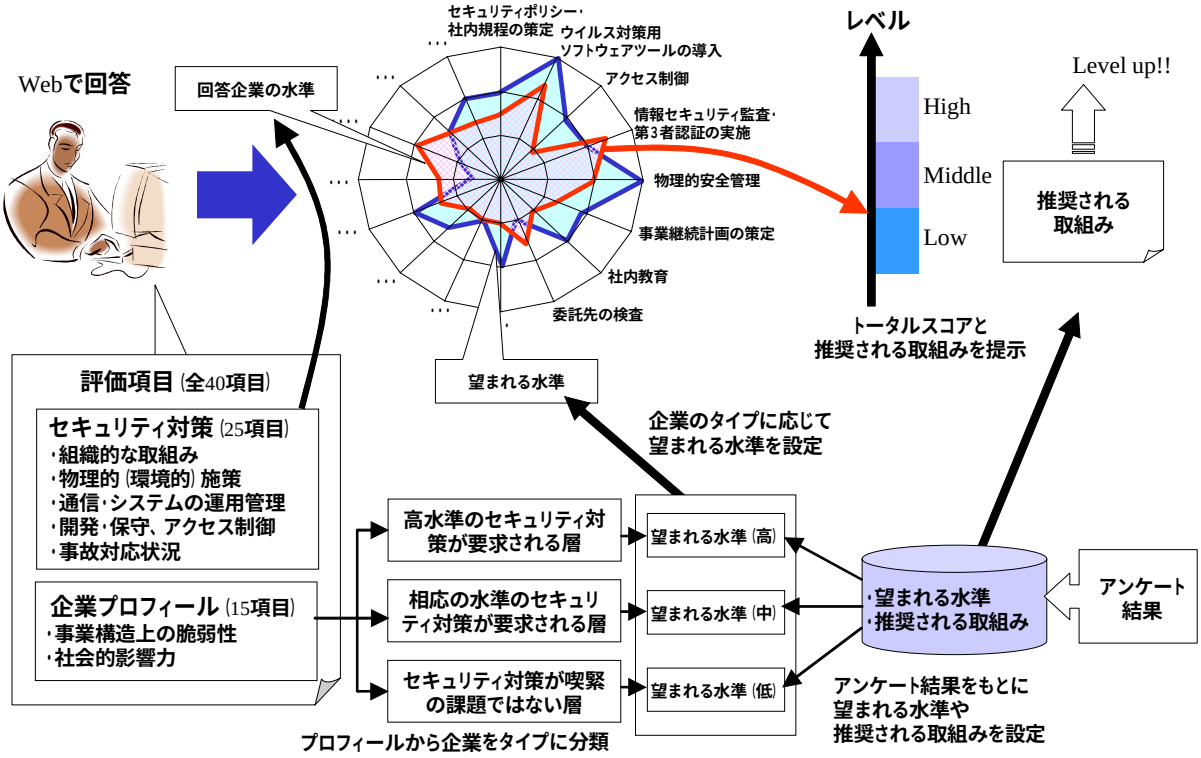
③対策の取組状況に関する項目の回答値と「望まれる水準」からレーダーチャートやトータルスコア等を作成

④評価結果と共に、推奨される取組みを提示

評価項目は、セキュリティ対策の取組状況を把握するための項目（25 項目）と、企業プロフィールに関する項目（15 項目）で構成される（(2)参照)。

「望まれる水準」とは、企業が、株主、消費者、取引先のみならず、社会全体から望まれる適正な水準であり、一様ではなく、企業の業態や保有する情報資産等の属性によって異なると考えられる。そこで、セルフチェックから得られるこれらの属性をもとに企業を分類し、それぞれの企業群に対して「望まれる水準」を設定することとする。具体的には、企業に対するアンケートの結果をもとに、企業群ごとに導出した（2.参照)。

図　１　情報セキュリティ対策ベンチマークのイメージ



（2）評価項目

①セキュリティ対策の取組状況

セキュリティ対策の取組状況に関する評価項目は、ISMS 評価基準 Ver.2.0 の詳細管理策をベースに、専門家による WG の検討に経て策定された。その際、社内の情報セキュリティ対策の統括を担当する役員クラスが利用する想定のもと、平易な言葉でわかりやすくすること、また評価項目の量を抑えることを心懸けた。

評価作業では、各評価項目に関する自社の取組みの「成熟度」を確認する。

図 2　成熟度の構成

できていない

できている

1．経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2．経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3．経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4．経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5．4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

評価項目は次の 5 グループで構成され、グループごとに 3～7 項の評価項目を設定した。

(a) 情報セキュリティに対する組織的な取組状況（7 項）
(b) 物理的（環境的）セキュリティ上の施策（5 項）
(c) 通信ネットワーク及び情報システムの運用管理（5 項）
(d) 情報システムの開発、保守におけるセキュリティ対策及び情報や情報システムへのアクセス制御の状況（5 項）
(e) 情報セキュリティ上の事故対応状況（3 項）

以下に、具体的な評価項目の内容を示す。

(a) 情報セキュリティに対する組織的な取組状況

ア）貴社では、情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。自社の状況に見合った規程とするためには、サンプルのコピーではなく、自社の事業やリスクを鑑みたものであることが重要です。

イ）貴社では、経営層を含めた情報セキュリティの推進体制やコンプライアンス(法令遵守)の推進体制を整備していますか。

推進体制の整備のためには、監査を含めた各担当者の責任が明文化されることが重要です。

ウ）貴社では、重要な情報資産（情報及び情報システム）については、重要性のレベルごとに分け、そのレベルに応じて管理していますか。

エ）貴社では、個人データなど重要な情報については、取得、利用、保管、開示、消去などの一連の業務工程ごとにきめ細かく適切な措置を講じていますか。

適切な措置とは、作業責任者や手順の明確化、取扱者の限定や処理の記録、確認などを指します。

オ）貴社では、社外の組織に業務を委託する際の契約書に、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。

セキュリティ上の理由とは、データの漏えいや消失、情報あるいは情報システムの誤用などを指します。

カ） 貴社では、従業者（派遣を含む）に対し、入社、退職の際に機密保持に関する書面を取り交わすなどして就業上のセキュリティに関する義務を明確にしていますか。

キ） 貴社では、従業者（派遣を含む）に対し、情報セキュリティに関する貴社の取組みや関連ルールについての計画的な教育や指導を実施していますか。

(b) 物理的（環境的）セキュリティ上の施策

ア） 貴社では、ベンダーや清掃業者など貴社に出入りする様々な人々に対するセキュリティ上のルールを定め、それを実践していますか。

イ） 貴社では、特にセキュリティを強化したい建物や区画について、必要に応じたセキュリティ対策を実施していますか。

対策には、外部とのセキュリティ上の境界を明確に意識した入退館･入退室管理や警報装置の設置などがあります。

ウ） 貴社では、重要な情報機器や配線等は、安全性に配慮して配置・設置していますか。

安全性に配慮した配置･設置とは例えば、人目につかない場所への設置、配線類の地下や床下への配置、浸水等を考慮した配置などを言います。

エ） 貴社では、重要な書類や記憶媒体の適切な管理を行っていますか。

適切な管理とは例えば、キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉砕廃棄などを言います。

オ） 貴社では、実稼働環境の情報システム（本番環境）やデータ（本番データ）を適切に保護していますか。

適切な保護には、実稼働環境と開発環境の分離、変更管理手順の策定、開発での本番データの使用制限などが含まれます。

(c) 通信ネットワーク及び情報システムの運用管理

ア）貴社では、情報システムの運用に必要なセキュリティ対策を実施していますか。

必要とされるセキュリティ対策には、セキュリティ要件の明確化、各種手順書の策定、セキュリティログの記録とチェックなどがあります。

イ）貴社では、不正ソフトウェア（ウイルス、ワーム等）に対する対策を実施していますか。

不正ソフトウェア対策にはコンピュータウイルス対策ソフトを導入し、パターンファイルのアップデートを適時行うことなどが含まれます。

ウ） 貴社では、貴社で導入しているソフトウェアに対して適切な脆弱性対策を実施していますか。

適切な脆弱性対策とは、セキュリティを考慮した設定や、パッチ（脆弱性修正プログラム）の適用、定期的な脆弱性検査などを言います。

エ）貴社では、通信ネットワークに流れるデータに関して、暗号化などの適切な保護策を実施していますか。

適切な保護策にはＶＰＮの使用や、重要な情報のＳＳＬ等での暗号化が含まれます。

オ）貴社では、携帯 PC やフロッピーディスク等の記憶媒体に対して、盗難、紛失等を想定し

た適切なセキュリティ対策を実施していますか。

携帯 PC やフロッピーディスク等の記憶媒体の使用場所に は、社外のパブリックスペースやリモートオフィス、自宅などを含みます。

(d) 情報システムの開発、保守におけるセキュリティ対策及び情報や情報システムへのアクセス制御の状況

ア）貴社では、業務システムの開発に際し、開発したシステムに脆弱性が残らないようにする施策を実施していますか。

施策としては、仕様書にセキュリティ上の要求事項を盛り込むことなどがあります。

イ）貴社では、ソフトウェアの選定・購入、システムの開発・保守に際して、工程ごとにセキュリティの観点からチェックを行うなど、セキュリティ管理が実施されていますか。

ウ）貴社では、情報（データ）へのアクセスを制限するための利用者管理や認証を適切に実施していますか。

適切な利用者管理には、不要な利用者IDの定期的な見直しや共用IDの制限、単純なパスワードの設定禁止などがあります。

エ）貴社では、業務アプリケーションに対するアクセス制御を適切に実施していますか。

適切な業務アプリケーションに対するアクセス制御には、例えば利用者ごとに利用できる機能の制限などがあります。

オ）貴社では、ネットワークのアクセス制御を適切に実施していますか。

適切なネットワークのアクセス制御には、例えばネットワークの分離や社外からの接続時の認証などがあります。

(e) 情報セキュリティ上の事故対応状況

ア）貴社では、情報システムの障害発生を想定した適切な対策を実施していますか。

適切な対策には、例えばシステムの冗長構成やバックアップ、障害対応手順書の策定、運用記録の取得、社外委託先とのサービスレベルの合意などがあります。

イ）貴社では、情報セキュリティに関連する事件や事故が発生した際の行動や報告、判断の基準を定めた対応手続きを準備していますか。

ウ）貴社では、何らかの理由で情報システムが停止した場合でも事業を継続するための取組みが、組織全体を通じて検討されていますか。

②企業プロフィール

企業プロフィールについては、一般的な企業属性に加え、事業構造上の脆弱性や社会的影響力に着目する形で構成した。

(a) 従業者数（派遣、アルバイトを含む）及びそのうちの正社員の割合

(b) 売上高、国内外の拠点数（支社・支店・営業所）

(c) 業種

(d) 国家や社会基盤、経済基盤に与える影響の観点から見た公益性

(e) 事業が、顧客の生命・身体・財産・名誉等に与える影響の大きさ

(f) 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）に依存している割合

(g) 主要な業務に関わる業務プロセスのうち、インターネットに依存している割合

(h) 主要な情報システムについて、（月間）売上高に影響を及ぼさないで済む許容停止時間

(i) 主要な情報システムが営業日に「24 時間」停止した場合の、当該日の売上高への影響

(j) 情報セキュリティ関連の事故が発生した場合のブランド（企業イメージ）への影響

(k) 元請や代理店、フランチャイジー等のビジネスパートナーへの依存度

(l) 重要情報（国家機密、営業機密、プライバシー情報等）の保有、管理または使用状況

(m) 個人情報の取扱量

(n) 離職率（直近の１年間に退職・転職された従業者の割合）

(o) 事業活動に影響を与えるような情報セキュリティ関連の事故の発生経験

（3）企業分類

企業分類に際しては、企業プロフィールから、事業構造上の脆弱性と社会的影響力を分類軸として算出し、それらに基づいて分類する。分類軸の内容を以下に示す。

［分類軸１］社会的影響力

自社の価値、社会的責任、保有する情報資産の性質などをもって IT 事故が発生した場合に社会に与える影響度の高さを評価するもの。自社の価値とは、売上規模やブランドイメージに対して IT 事故が及ぼす影響の大きさを指す。社会的責任とは、事業の公益性（国家、社会、経済等）や、IT 事故が発生した場合の消費者への影響度（生命・身体・財産・名誉等）の高さを指す。情報資産とは、重要情報の保有量（国家機密、営業機密、プライバシー等）を指す。IT 事故が発生した場合の社会的影響の大きい企業ほど、社会的責任の観点からも高いレベルの対策が必要であると考えられる。

［分類軸２］事業構造上の脆弱性

事業の情報システム依存、業務の外部依存性、関与者の範囲などをもって、自社が抱える事業構造上の脆弱性の高さを評価するもの。事業の情報システム依存とは、業種特性や基幹業務の情報システム依存度を指す。業務の外部依存性とは、代理店等への依存度、インターネットへの依存度、正社員・非正社員の比率を指す。関与者の範囲とは、拠点数、海外拠点の有無、従業者の離職率を指す。これらの数値が高いほど IT 事故に対して脆弱である（統制が困難で IT 事故が発生しやすい、もしくは IT 事故が深刻化する可能性がある）と考えられ、リスクマネジメントの観点からも高いレベルの対策が必要であると考えられる。

上記の２軸に基づき、以下の３グループに分類する。

①高水準のセキュリティレベルが要求される層

事業構造上の脆弱性が高く、かつ IT 事故が発生した場合の社会的影響が大きい企業にとっては、高水準のセキュリティレベルが要求される。例えば、IT 依存度が高く、かつ大量の個人情報を取り扱う金融・保険業や情報サービス、また広範な SCM を構築している大手製造業等が該当する。

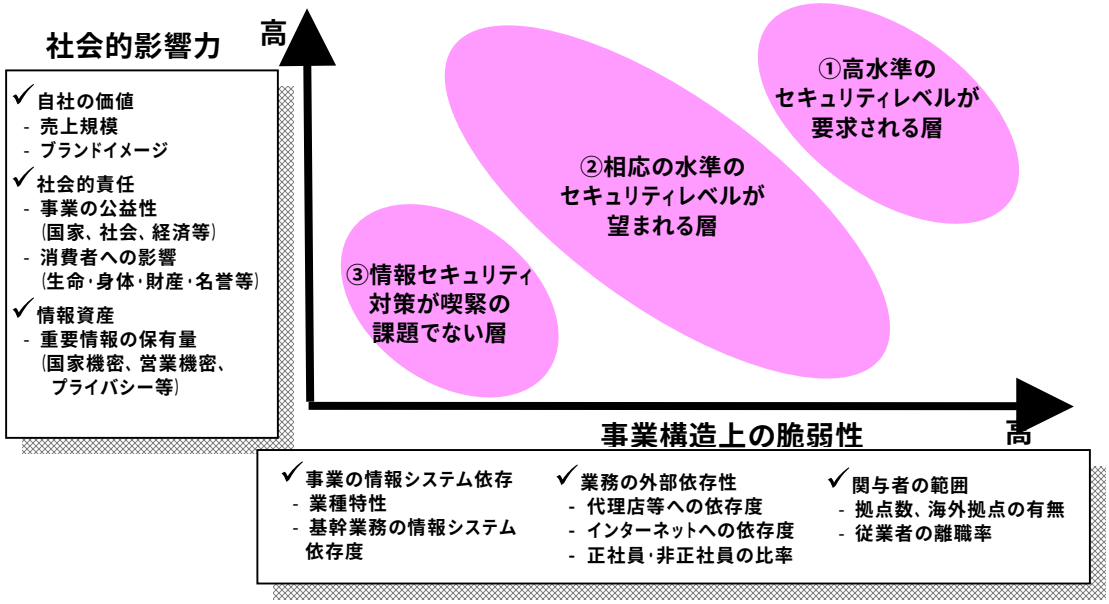
②相応の水準のセキュリティレベルが望まれる層

事業構造上の脆弱性もしくは社会的影響力のいずれか一方だけが高い企業には、IT 事故の社会的影響は小さいが発生もしくは深刻化する可能性があるタイプと、IT 事故が発生しやすいわけではないが、発生すると社会的影響が大きいタイプがあり、いずれも①ほどではないが、相応な水準でのセキュリティ対策が望まれる。例えば、多数の顧客情報を抱える卸売・小売業や、拠点数の多い大手建設業等が該当する。いずれの場合も、対策ベンチマークを活用するなどして自社の状況を分析し、望まれる水準に応じた対策に取り組む必要がある。

③情報セキュリティ対策が喫緊の課題でない層

事業構造上の脆弱性と社会的影響力のいずれも高くない企業にとっては、情報セキュリティ対策が喫緊の課題ではない。例えば、中小の建設業や製造業、卸売・小売業等が該当する。ただし、これらの企業も、ネットワーク社会の一員として最低限の対策を講じる必要があり、対策ベンチマークを活用するなどして望まれる水準に応じた対策の実施が望まれる。

図　3　要求される情報セキュリティの水準に基づく分類

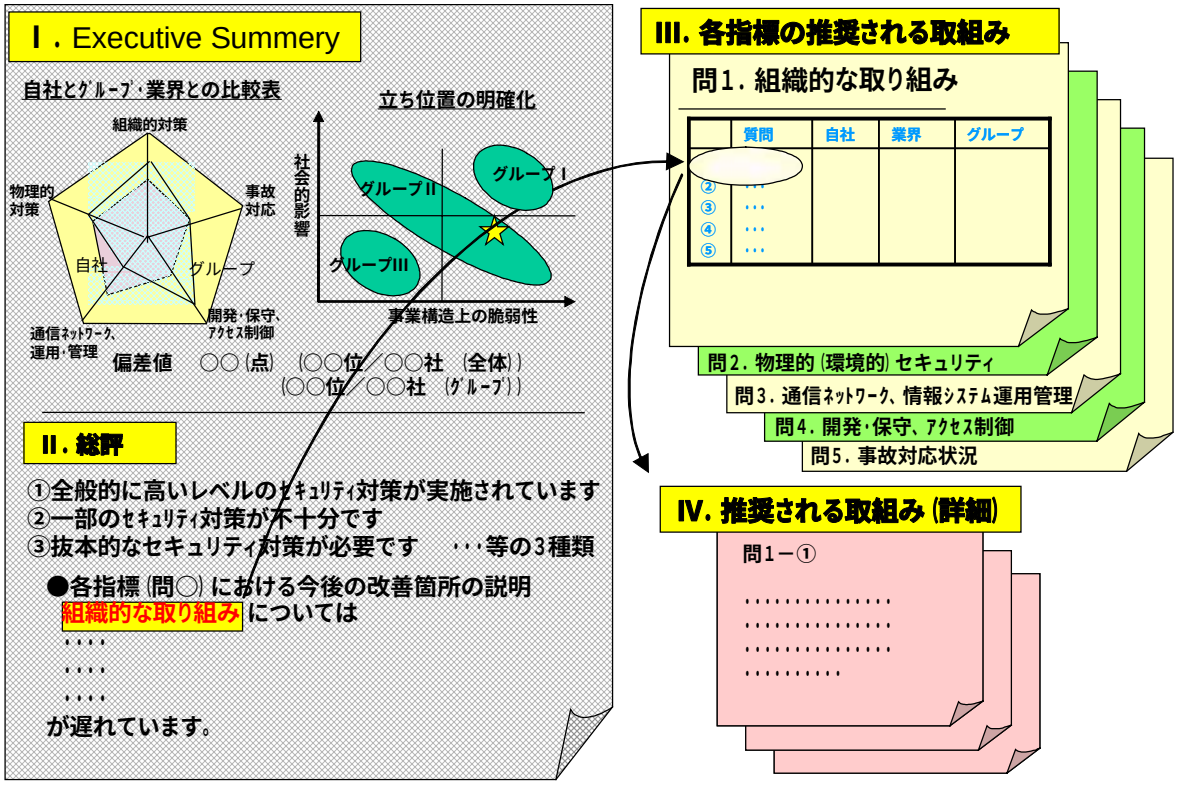


（4）推奨される取組みの案

Web ツールによるセルフチェックの結果は、その目的により、「経営者向けのエグゼクティブサマリ」と「実務者向けのアドバイス」の２通りに分けて提示する形を想定する。

前者については、経営層の理解とトップダウンの対策実施を目指し、可視化された比較表や偏差値などを用いて説明する。また、後者については、具体的な「推奨される取組み」を提示する。

図　4　セルフチェック結果のイメージ



推奨される取組みとして回答者に提示されるセルフチェックの結果の事例を紹介する。

大項目1. 貴社における情報セキュリティに対する組織的な取組状況についてうかがいます。

① 貴社では、情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。

説明 ポリシーや規程が有効なものであるためには、それらが自社の状況に見合ったものである必要があります。ポリシーや規程は、サンプルのコピーではなく、自社の事業やリスクを鑑みたものであることが重要です。

対策のポイント

●情報セキュリティポリシーや管理規程が策定されているか
●ひな形、サンプル、他社事例等のコピーではなく、社内で十分な討議を経て、自社の状況に見合った内容となっているか
●ポリシーは全社をカバーしているか
●社長ないし上級役員が承認しているか
●全従業者（派遣を含む）に対して通知・公表済みか
●定期的に見直すための手続きを定めているか
●既に見直し時期が到来していた場合、見直しを実施したか
●改訂結果について、社長ないし上級役員の承認を得て、再度通知・公表したか
●従業員がポリシーや関連規程類を遵守し、率先垂範していることを確認するための手続きを定めているか
●情報システムに対し、いわゆるネットワーク検査やペネトレーションテストを定期的に実施し、ポリシーの実装状況を確認しているか

解説

効果的な情報セキュリティ対策を実現するためには、情報セキュリティに関するポリシーや関連する諸規程を定めて組織内部における統制の方針や手順等を明らかにし、それを確実に実践することが重要です。

そうしたポリシーや関連する諸規程を定めるに当たっては、ひな型やサンプルあるいは他社の事例等をコピーし、会社名や組織名あるいは役職名などを単純に置き換えるだけでは、自社に合った効果的な統制を実現することが難しい場合があります。なぜなら、組織にあった統制のあり方は、組織によってそれぞれに異なるからです。組織の実状に沿ったポリシーや規程類を策定するためには、社内での十分な討議を経て、自社の組織や業務との整合を図っていくことが重要です。

また、社内カンパニー制を採用して、各部署が独立性を持って事業を営んでいる場合など、特殊なケースを除いて、一般的には全社で共通のポリシーとした方が良いでしょう。一緒に仕事をする複数の部署で、それぞれに考え方の異なるポリシーを定めているようだと、情報セキュリティの実現は難しくなります。

そのこととも関連しますが、情報セキュリティポリシーを正しく実践するためには、会社で言えば社長や上級の役員が、ポリシーの策定に関与し、その実現に自ら責任を持つことが重要です。さもなければ、本当に必要なリソースを投入することや、会社全体として必要な約束事を実践することが難しくなります。

ポリシーや規程類を策定したならば、それを関連する全従業員に対して周知、徹底する必要があります。関連する従業員が認知していないポリシーや規程類は、「絵に描いた餅」に過ぎません。加えて、情報セキュリティに関連する事故は、一人の不注意や怠慢から発生し、大きく広がることがあるのです。

また、ポリシーや諸規程は、一度定めたら終わりで未来永劫使い続けられるとは限りません。一般の社規などでもそうですが、関連する法令が変わったり、情報システムに関連する技術が変化したりといった周りの環境の変化に追従していかなければ、せっかく作ったポリシーや諸規程も形骸化してしまいます。特に情報技術の進展はめざましく、1年も経てば情報システムを取り巻く脅威に大きな変化が起こっているかも知れません。こうした変化に対応するためには、ポリシーや諸規程類を定期的に見直すことが必要ですので、見直し自体を規定として定めておき、組織の義務として確実に実施することが望まれます。

既に策定済みのポリシーや規程類については、見直しが必要となっていないか、定期的な見直しが確実に実施されるような規定が含まれているかを確認してください。

そうした規定に沿って改訂を実施した結果についても、最初のポリシーや規程類の策定時点と同様に、やはり社長や上級役員の承認を得ること、従業員に再度周知、徹底することが重要です。

さらに、従業員がポリシーや関連規程類を遵守し、率先垂範していることを確認するための手続きを定めることにより、ポリシーや規程を実効的なものとすることも重要です。例えば、情報システムに対して、いわゆるネットワーク検査やペネトレーションテストを定期的に実施することで、ポリシーの実装状況を確認しておくとよいでしょう。

（了）

② 貴社では、経営層を含めた情報セキュリティの推進体制やコンプライアンス(法令遵守)の推進体制を整備していますか。

説明 推進体制の整備のためには、監査を含めた各担当者の責任が明文化されることが重要です。

対策のポイント
●社内の情報セキュリティのあり方を決定する組織が整備されているか
●その組織の責任者は経営層の人間が担当しているか
●その組織において、情報セキュリティに関する適切な責任や資源分配を検討しているか
●その組織は、社内の情報セキュリティ対策に関する監査の実施を推進しているか
●事業を遂行する上で遵守すべき法令、規制、契約等を網羅的に、かつ正確に把握しているか
●他者の知的財産権を保護するための手続きを定めて実践しているか（例えば、ソフトウェアの不正コピーを予防するための手当てなど）
●自社が実施した様々な活動について、それらを記録する仕組みはあるか
●特に法定の保存文書について、厳格に保管を実施しているか
●個人情報保護法を前提として、個人情報を保護するために必要な対策を定め、それらを実施しているか
●不正競争防止法で保護される情報の要件を把握しているか
●電子署名法について、把握しているか
●情報システムが、業務以外の目的で利用されることを防止するための措置を講じているか

解説

実効的な情報セキュリティ対策の推進には、全社的な取組みが必要です。そのためには、経営層のリーダシップと各組織のセキュリティ上の責任が明確化されている必要があります。

また、企業の情報セキュリティのあり方を決定する組織を設置し、監査やコンプライアンスの実践といった役割を持たせることが必要です。

情報セキュリティのあり方を決定する組織の責任者は、経営層の中から任命することが望まれます。なぜなら、情報セキュリティは、その企業の経営方針やビジネスプロセスなどと密接に関わるものだからです。情報セキュリティは、保有する情報資産や業務に不可欠な情報システム、情報セキュリティ上の事故が発生した場合の業務への影響などのファクターを考慮しながら推進すべきであり、そのためには、情報セキュリティ担当の責任者は、情報セキュリティと経営の両方に目配りができる立場にいることが重要です。

情報セキュリティ対策の推進に当たって、情報セキュリティ担当責任者は、まず、必要なリソースを、その企業の情報セキュリティ上のニーズやプライオリティに応じて分配するという役割を担う必要があります。リソースの分配とは具体的には、予算の配分であったり、人的リソースの配分であったりということになります。情報セキュリティ上プライオリティの高い項目にはより多くのスタッフと予算を割り当てて、優先的に実施することになります。さらに、必要に応じて個々の対策を推進する責任者を任命してもよいでしょう。

情報セキュリティ対策が、組織が抱えているリスクに応じて実施されていることを確認するために、情報セキュリティ監査は有効な手段です。会計監査が法律で義務付けられているのに対し、情報セキュリティ監査は任意であり、いつまでに実施しなければならないという規定がないので、情報セキュリティ担当責任者がイニチアチブを取って計画的に実施する必要があります。

事業を遂行する上で遵守すべき法令、規制、契約等を網羅的に把握しておくことは企業として当然のことですが、情報技術の変化は年々早くなっており、それに伴って、法律や規制が新たに制定されたり、修正が加えられる頻度も増していくことが予想されます。したがって、事業に関わる法律や規制についての定期的な情報収集とその業務への影響の分析、遵守するための取組みの徹底が求められています。

情報セキュリティの分野において特にコンプライアンスが求められる法律には、著作権法（ソフトウェアの不正コピーの防止等、知的財産権の侵害防止）、不正競争防止法、個人情報保護法、電子署名法、e-文書法などがあります。これらの法律については、その趣旨を正確に理解して、遵守に向けた取組みを行うことが必要です。

従業員が会社の PC を業務以外の用途に使用することがないようにすることは、業務効率の低下を防止するだけでなく、インターネット上の掲示板への不適切な書込みの防止や、業務とは無関係の Web サイトにアクセスし、気付かないうちにスパイウエアなどの不正なプログラムをダウンロードしてしまう(情報漏えいにつながる危険がある)といったことがないようにするためにも重要です。

（了）

③ 貴社では、重要な情報資産（情報及び情報システム）については、重要性のレベルごとに分け、そのレベルに応じて管理していますか。

説明 情報セキュリティ対策を効率的にかつ高いコスト効果をもって実施するためには、情報資産を明確化し、情報資産の重要度に応じて管理することが必要です。

対策のポイント
●情報システムに関連づけて重要な情報資産の目録を作成しているか
●情報資産の重要度とそれに応じた保護のレベルを分類しているか
●情報資産の管理責任を明確化しているか
●情報の分類を定める責任、定期的な見直しの責任が明確になっているか
●出力した情報について、保護のレベルを明確化しているか

解説

主な情報資産には、情報と情報システムがあります。情報には、個人情報のように社外に漏えいした場合に顧客に迷惑をかけるものや、ホームページのコンテンツのように改ざんされると問題になるものがあります。情報システムには、個人情報が保管されているものや障害が発生すると業務が停止してしまうものなどがあります。情報セキュリティ対策の最初のステップとして、これら情報と情報システムとの関連を含む、情報資産を記録した目録を作成する必要があります。

情報資産は、その機密性（情報が漏えいしないように保持すること）、完全性(情報が正しいこと)、可用性(必要な時に利用できること)の 3 つの観点から重要度を分類し、重要度に応じた保護レベルを規定します。守るべき情報資産の明確化が完了したら、さらに、それらの情報資産の管理責任者を明確化し、保護レベルに応じた管理策を定めて実施します。

情報資産やその重要度は、自社の事業の変化や、社会状況の変化、情報技術の進歩等の外部環境の変化によって変わるものなので、定期的に見直しをする必要があります。したがって、情報資産の分類や分類基準の見直しを担当する人、作成した目録の見直しと改訂を担当する人などを決める必要があります。

また、守るべき情報は、電子的な情報に限りません。紙に印刷された情報も、電子的な情報と同様に守るべき情報資産です。冒頭に挙げたような各種の重要情報をプリントアウトした書類は、例えば鍵のかかる書庫に保管する必要があります。印刷した重要情報をプリンタのトレイに置きっ放しにするなどということはあってはなりません。

（了）

④ 貴社では、個人データなど重要な情報については、取得、利用、保管、開示、消去などの一連の業務工程ごとにきめ細かく適切な措置を講じていますか。

説明 個人情報保護法の規定やガイドラインにみられるように、重要情報の取得、利用、保管、開示、消去などに当たっては、作業責任者や手順の明確化、取扱者の限定や処理の記録、確認などが必要です。

対策のポイント

●各工程の作業責任者が明確化されているか
●各工程における作業手順が明確化され、その手順に基づいて作業が実施されているか
●各工程における作業担当者が限定されていて、適切な担当者のみが操作の権限を有しているか
●作業担当者の識別や権限付与の状況を確認しているか
●重要情報に対するアクセスの記録･保管、権限外作業の有無を確認しているか

解説

特に重要な情報については、セキュリティを考慮した処理の手順を定めておく必要があります。個人情報保護法では、情報の取得、利用時の手続きや本人からの開示要求への対応など、企業の遵守すべき事項が多岐に渡るため、それぞれの工程ごとに行うべき作業を定義し、作業実施責任者とそれらの作業が適切に実施されているかどうかをチェックする責任者を設置することが望まれます。

各工程で実施すべき作業については、誰が実施しても間違いがないように、明確に手順を定めておくことが必要です。さらに、作業が手順通りに実施されていることを、上述した作業実施のチェック責任者が確認することが求められます。

各工程における作業は決められた担当者だけが実施するようにしておく必要があります。具体的には、情報が保管されているシステムや書庫にアクセスできる人を制限したり、アクセスできる情報を作業担当者ごとに制限することが求められます。また、作業担当者の交代が多い組織では、作業担当者の ID 管理や作業権限の定期的なチェックが必要になります。

作業担当者には、それぞれ別の ID を付与し、誰が作業を実施したのかが識別できるようにします。複数の作業担当者が一つの ID を共有することは、情報にアクセスしたのが誰なのかを後から特定することができないといった問題があるので避けるべきです。また、各作業担当者が実施可能な作業についても、作業担当者ごとに個別に必要十分なだけの権限を付与し明確化しておくことが必要です。

重要情報に対するアクセスの記録を取得し、一定の期間保管しておく必要もあります。アクセスの記録は定期的にチェックし、不正なアクセスが行われていないかどうか、権限外の作業が行われていないかどうかなどの点についてチェックすることも有効な管理策です。

（了）

⑤ 貴社では、社外の組織に業務を委託する際の契約書に、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。

説明 社外の組織に業務を委託する際の契約書には、データの漏えいや消失の防止、情報あるいは情報システムの誤用の防止を徹底するために、これらに関する条件を記載しておく必要があります。

対策のポイント

●どのような業務が外部に委託されているかについて、全件を掌握しているか
●業務委託先と交わす契約書において、記載されるべきセキュリティ上の要求事項をあらかじめ明確に定めているか
●外部委託によるソフトウェア開発を行う場合、使用許諾、知的所有権などについて取り決めているか

●外部委託によるソフトウェア開発を行う場合、品質や作業範囲、標準となる契約書や合意書を用意しているか

解説

社外の組織に業務を委託するということは、自社で定めたセキュリティポリシーが適用されない、あるいは、実施しているセキュリティ対策の効果が及ばないところで業務が行われるということであり、社内向けの対策とは異なる対策が必要になります。新規の契約を結ぶ場合には、契約書にセキュリティ上の要求事項を記載するようにします。既に結んでいる契約についてはまず、どのような業務を委託しているのかを正確に把握することが必要です。

委託している業務が明らかになったら、それぞれの業務について、委託先との間で交わされている契約の内容が委託する業務の内容や情報資産の重要性を鑑みて適切かどうかを確認し、セキュリティ上の要求事項が記載されていなかったり、適切なセキュリティ管理が望めないような記述となっていたりする場合には、契約書にそれらを追加、修正できないかどうかを委託先と協議してみる必要があります。

契約書に記載すべきセキュリティ上の要求事項が明確になっていない場合には、情報セキュリティ担当責任者がイニシアティブをとって記載すべき項目を明確化します。それをもとに業務委託時のセキュリティ上の要求事項の雛型を用意しておくとよいでしょう。

情報セキュリティと関連する項目で契約書に記載すべき項目には、ソフトウェア開発を委託する場合の使用許諾、知的所有権などについての取り決めや、品質や作業範囲に関するものなどがあります。可能であれば、品質の要求事項に、既知の脆弱性を含まないようにするなどの条件を入れておくべきでしょう。

（了）

⑥ 貴社では、従業者（派遣を含む）に対し、入社、退職の際に機密保持に関する書面を取り交わすなどして就業上のセキュリティに関する義務を明確にしていますか。

説明 情報セキュリティ対策の基本の一つは、人のマネジメントです。すべての従業者に対して、入社や退職の際に、情報セキュリティ上の義務や、業務上知りえた機密情報を(退職後も)外部に漏らさないこと等、セキュリティ上の遵守事項を誓約させることで、情報セキュリティ上の注意義務を自覚させるとともに、情報セキュリティ対策に実効性をもたせます。

対策のポイント

●従業者（派遣を含む）を採用する際に、機密保持契約を締結しているか
●従業者（派遣を含む）の退職に際して、退職後における機密保持を約する書面を交わしているか
●雇用契約時に、セキュリティ上の義務を明示しているか
●就業規則ないし服務規律に、従業者（派遣を含む）が遵守すべき事項を明示しているか

解説

情報セキュリティ対策の基本の一つは、人のマネジメントです。すべての従業者に対して、入社や退職の際に、情報セキュリティ上の義務や、業務上知りえた機密情報を(退職後も)外部に漏らさないこと等、セキュリティ上の遵守事項を誓約させることで、一人一人に情報セキュリティ上の注意義務を自覚させるとともに、情報セキュリティ対策を実効性のあるものにすることができます。具体的には、従業者（派遣を含む）の採用・退職に際して、業務遂行時の情報セキュリティ上の義務や、在職中及び退職後における機密保持を約する書面を交わすことなどです。現在業務に携わっている従業者で、まだ機密保持契約を交わしていない人についても、改めて書面を交わすとよいでしょう。

雇用契約時には、すべての採用者に対して、従うべき情報セキュリティ上の義務を明示してください。また、実際に業務に就く前に入社時の研修等でパスワードを扱う際の遵守事項、ウイルス対策や OS・ソフトウェアのパッチ当てを適切に実施すること、電子メールを使用する際の注意など個別具体的な実施事項について教育する必要があります。

就業規則ないし服務規律に、従業者（派遣を含む）が遵守すべき情報セキュリティ上の要求事項を明示しておくことも必要です。定期的に就業規則ないし服務規律の遵守状況をチェックし、遵守されていない場合には、従業者に対して、遵守の徹底を促すことも重要です。

（了）

⑦ 貴社では、従業者（派遣を含む）に対し、情報セキュリティに関する貴社の取組みや関連ルールについての計画的な教育や指導を実施していますか。

説明 従業者に対する教育は、情報セキュリティ対策の有効性を向上させるために必要不可欠なものです。教育を適切に実施し、効果が得られていることを確認することによって、技術的なセキュリティ対策との相乗効果が期待できます。

対策のポイント

●ポリシー及び関連規程を従業者（派遣を含む）が理解し、実践するために必要な教育を実施しているか
●パスワードの管理や、暗号鍵の管理について教育を行なっているか
●出来合いの教材だけでなく、自社の状況に即した適切な教材を用意しているか
●定期的に教育を実施しているか
●教育が有効であることを確認するための仕組みを用意しているか

解説

従業者に対する教育は、情報セキュリティ対策の有効性を向上させるために必要不可欠なものです。従業者に対する教育には、ポリシーや関連規程の周知といった全体を俯瞰するための事項から、パスワードの管理や暗号鍵の管理、電

子メールを使用する際の注意点といった個別の項目まで幅広く実施する必要があります。

基本的・一般的な事項については市販されている教材を使用することで、費用と効果のバランスをとることができますが、事業活動に直接関わる項目や、特に重点を置いている項目、対策を徹底したい項目については、自社の状況に即した教材を作成するなどの工夫をすることも必要です。

また、職位や職種によって、情報セキュリティ上の責任が異なるので、教育や研修は、すべての従業者に共通のものと、従業者の職位や職種(情報セキュリティ管理者向け、一般従業員向け、管理職向けなど)に応じたものとに分けて実施すると効果的です。

教育は1度実施しただけで、100%の効果が得られるというものではないので、3ヶ月ごとや半年ごとというように定期的に実施することが必要です。また、社会状況の変化や技術の進歩に伴い、新規に教育すべき項目が出てくるので、それらにキャッチアップするためにも定期的な教育が必要となります。

教育の効果は従業者一人一人によっても異なります。すべての従業者の教育効果を一定のレベル以上とするためには、効果を確認するためのテストを実施したり、何らかのインセンティブを設けたりするなどの施策が必要な場合もあります。情報セキュリティ上の事故が発生したと仮定した事故対応訓練を実施することは、実際に事故が発生した場合の被害を低減することや従業者の意識喚起に効果があります。

(了)

大項目2. 貴社における物理的(環境的)セキュリティ上の施策についてうかがいます。

①貴社では、ベンダや清掃業者など貴社に出入りする様々な人々に対するセキュリティ上のルールを定め、それを実践していますか。

説明　建物や事務所の中には、数多くの情報や関連する設備が所在しています。これらの情報や設備に触れる機会のある外部業者に対しては、それぞれのリスクの状況を踏まえたルールの制定と、それに従った運用を行うことが必要です。

対策のポイント

●人々の出入りによって、どのようなリスクが生じるかを評価する手続きを定めているか
●その手続きに従って評価を実施したか
●評価を実施した結果、明らかになったリスクについて適切な対策を実施したか
●出入りする様々な人々について、自社対相手方の組織(ないしは人)との間で、セキュリティに関する取り決めを契約として定めているか

解説

会社の建物には、情報システムベンダのメンテナンスやビルのメンテナンス業者、清掃業者、配送業者、什器業者、コンサルタント、常駐の業務委託先社員などいろいろな種類の社外の人が出入りします。

外部業者に関連するリスクの評価は、担当者の勘だけで行うと重要なポイントが抜ける可能性があります。そうした抜けを防止するためには、リスク評価の手順を組織として正式に定めておくことが望まれます。会社の建物に出入りする委託業者のリスク評価においては、以下の点がポイントとなります。

・外部業者の業務内容と業務上必要な行動範囲の洗い出し
・外部業者が起こす故意や過失による盗難や盗み見、損壊や紛失などのリスクの分析
・リスクが現実となった場合の影響の分析

リスク評価の作業は、職人的に実施されることも多く、属人化しやすいものの一つです。これらの評価作業が有効に機能していることを確認するためには、リスク評価の結果を正式に承認する手続きが重要です。また、環境の変化や新しい脅威に対応するため、定期的に再評価を実施することも重要です。

多くの場合、リスク評価の結果、様々なリスクが確認されます。この中で、影響の大きなリスクについては、対策の実施が必要です。また、対策の中には、すぐに実施することが可能ではなく、多額の費用や長い期間を要するものがあります。こうした対策が必要と判断されたリスクについては、対策の実施計画や実施状況などを適切に管理することが必要です。

情報セキュリティを維持するために必要な事項について、自社に出入りする様々な人々との間で契約を交わすことが求められます。具体的には、契約書に機密保持条項や損害発生時の責任を明記したり、また、組織内の人から機密保持誓約書を取り付けたり、就業規則に罰則規定を付加することなどが考えられます。

(了)

②貴社では、特にセキュリティを強化したい建物や区画について、必要に応じたセキュリティ対策を実施していますか。

説明　重要な情報や関連する設備が数多く所在する場所については、セキュリティ対策として特段の配慮が必要となります。このような場所（建物や区画）については、入室可能な人をできるだけ制限したり、外部からの侵入者に対する防護策を強化することが必要です。対策としては、外部とのセキュリティ上の境界を明確に意識した入退館・入退室管理や警報装置の設置などがあります。

対策のポイント

●セキュリティ境界を明確に定義し、その安全管理措置に関する規程を整備しているか
●侵入を防止するために必要な建物や警報設備などの基準を設定しているか
●敷地及び建物に入ることができる人を制限しているか
●その制限の対象になる人を識別できるようにしているか
●入退館（室）の履歴を記録し、その記録を適切に管理しているか
●基幹業務システムや機密情報を保有するシステムを許可された者だけが立ち入ることのできる場所に設置しているか

解説

セキュリティ境界内の安全性を保つためには、管理者の意識だけに頼らず、安全管理措置として守るべき事項を規程として整備し、徹底することが必要です。まず、①でも述べたリスク分析に基づいてセキュリティ境界を適切に設定しなければなりません。また、そのセキュリティ境界に係る防災及び防犯上の安全管理措置について、規程類を整備し、ルールを徹底する必要があります。

通常、セキュリティ境界の区分は多段階となり、また場所も一箇所とは限りません。それぞれの場所のセキュリティレベルを保つためには、各種保安設備の設置基準を作成することが必要です。具体的には、ICカードや個人認証などを利用した入退室の監視設備の設置基準、また、赤外線や振動センサなど防犯用の各種警報設備の設置基準などを設定することが求められます。

セキュリティ境界内の安全確保のためには、この境界内に立ち入る人をできるだけ少なくすることが大切です。そのためには、重要な場所の施錠管理を徹底すること、さらに、ICカードなどによる、セキュリティレベルに応じた入室制限を行うことが必要になります。

防犯設備などによる侵入対策に加え、許可された人物であるかどうかを一目で確認できることも重要です。よく利用される対策としては、ゲストと従業者を名札の色で識別する方法などが挙げられます。

万が一の際に事故原因を究明するためには、セキュリティ境界内に入った人物が誰であるかを確認する必要があります。また、記録を取ることは犯罪や不正行為の抑止にもつながります。そのためには、ICカードによる個人識別などを利用して、入退室の記録を管理したり、入退室時の記帳管理を徹底するといった取組みが必要です。

基幹業務システムや機密情報を保有しているシステムは、一般の従業員や来訪者から隔離し、容易に触れられない場所に設置することが重要です。入場制限の無いパブリックエリア（廊下、通路、打ち合わせ場所など）からは確実に隔離する必要があります。また、施錠や入退室管理、さらに多段階のセキュリティ区分を設定することも重要です。

（了）

③貴社では、重要な情報機器や配線等は、安全性に配慮して配置・設置していますか。

説明　重要な情報機器や配線については、偶然の事故による損壊や悪意による損壊を防ぐなど、安全上の配慮が必要です。偶然の事故に対しては、機器の転倒防止、漏水被害対策、周辺での飲食禁止、踏みつけや引っ張りによる断線の防止など、設備本体や周辺で起こりうる事故を洗い出し、有効な対策を行うことが重要です。また、悪意のある損壊に対しては、機器や配線などに、容易に接触できないようにすることが重要です。

対策のポイント

●執務室の入口から見えないように情報処理設備を配置しているか
●使用中に画面を盗み見されないように配置を工夫しているか
●電源コードや通信ケーブルが損傷しないように配置しているか

解説

情報処理設備や配線などを悪意による損壊などから保護するためには、それらに容易に接触できないようにすることが大切です。そのためには、まず機器や配線などの設備が入口や通路などから容易に発見できないようにすることが重要です。

カウンターや通路、打ち合わせ場所から情報機器の画面などが容易にのぞき見できてしまうと、画面に表示されている情報が漏えいするだけでなく、当該端末で実施できる作業を来訪者に伝えているようなものです。このような状況を避けるためには、事務所レイアウトや画面の向きなどを変更し、外部者や担当外の従業者が画面を覗けないようにするなどの工夫が必要です。

安全管理を行う際、情報処理の機器本体だけに注意が行きがちですが、設備の安全面を考えると、電源や通信ケーブルなどの配線の保護も重要です。複数の企業が入居するテナントビルなどでは、企業として管理の手が及ばないケーブルシャフト扉の施錠などの管理状況の確認が望まれます。

また、機器の転倒や漏水など偶然の事故への対策も必要です。重要な情報機器は日常の業務を行う場所とは別のセキュリティ境界内に設置し、情報機器や配線についても地震や火災、踏みつけや引っ張りによる断線や緩みなど、災害や過失による損壊への対策を行う必要があります。また、こうした区画内では飲食を禁止するなど、禁止行為を定めることも必要です。

（了）

④貴社では、重要な書類や記憶媒体の適切な管理を行っていますか。

説明　書類や電子的な記憶媒体などによって情報が漏えいする事故が数多く発生しています。キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉砕廃棄など、重要な情報が記録されている書類や記憶媒体を適切に管理することが必要です。

対策のポイント

●事務所内の机上、書庫、会議室などの整理整頓が実施されているか
●事務所、机の施錠管理が実施されているか
●郵便物、FAX、印刷物などの放置禁止や保護が実施されているか
●書類や記憶媒体などの廃棄処理が徹底されているか

解説

適切な管理が行われていない書類や記憶媒体などから情報が漏えいする事故が数多く発生しています。重要な情報が記録されている書類や記憶媒体については、適切な管理が必要ですが、非常に身近なものであるため、管理が行き届きにくいという面もあります。情報漏えいを防止するためには、次のような管理を徹底する必要があります。

まず、重要な情報が記録されている書類や記憶媒体についての管理方法を定めることが必要です。この管理方法には、作成、利用、修正、保管、廃棄の工程ごとにその業務を行うことのできる人の明確化と、その実施を確かにするための技術的対策や手順の策定が含まれます。例えば、機密情報はキャビネットに施錠保管し、担当者以外がその情報を参照する場合には、その機密情報の管理責任者の事前の承認を得るというルールを定めることなどです。

また、事務所内の机上、書庫、会議室など、身近な場所の整理整頓を行い、重要な情報が記録されている書類や記憶媒体が他に紛れ込まないようにすることが必要です。

放置された郵便物、FAX、印刷物の盗難により、情報が漏えいする場合があります。このような事故を防止するためには、次のような管理が必要です。

- 郵便物受けの施錠管理
- 郵便物の授受管理
- FAX着信物の早期回収
- FAX送信時の番号確認、事前･事後の電話連絡
- プリントアウトした印刷物の早期回収

また、書類や記憶媒体の廃棄処理が不適切であったことに起因する情報漏えい事故も数多く起こっています。書類や記憶媒体などは粉砕処理すること、また大量廃棄で専門廃棄業者を利用する際は廃棄証明を入手することなども重要です。

（了）

⑤貴社では、実稼働環境の情報システム（本番環境）やデータ（本番データ）を適切に保護していますか。

説明　システム開発には、多数の作業者が関与するため、通常の運用業務に比べ、大きなリスクが潜在しています。そのため、システム開発においては、実稼働システムと開発システムの分離、変更管理手順の策定、本番データの使用制限などの対策が重要となります。

対策のポイント

●実稼働システムを開発システムやテスト用のシステムから隔離しているか
●個人情報等の重要なデータをテストに用いないためのルールを規定しているか
●実稼動システムの変更手順を規定に定めているか
●実稼働システムの変更が規定に沿って行われ、記録されているか
●必要な場合、システムの性能･容量管理が行われているか

解説

実稼働中の情報システムやデータは、適切に管理することが必要です。システム開発においては、開発費用の削減のために新たなテスト用のシステムを構築せず、実稼働システムを利用したテストを行う場合があります。しかし、重要なシステムの開発においては、実稼働システムへの影響を防止するため、別途テスト用のシステムを用意し、テスト用システムにおいて開発及びテストを実施することが望まれます。

個人情報や機密情報などを取り扱うシステムで、開発したシステムの最終的な検証を本番データ（実在する個人のデータなど）を用いて行う場合があります。そのような場合には、次の点を明確にすることが必要です。

・本番データを使用しなければならない理由と検証すべき範囲
・テストに使用する本番データの重要度
・作業者、作業場所及び作業に用いる装置の制限
・データの持ち出し、コピー等の禁止
・本番データを利用する際の承認手続き
・使用後の消去手続きと確認方法

開発したシステムを実稼働システムへ移行する際には、予想外のトラブルが発生する場合があります。そのため、実稼働システムの変更に際しては、変更作業の承認や手順、変更内容の記録などの規程を定め、トラブルが発生するリスクを軽減するとともに、万が一トラブルが発生した場合の対応方法などを明確にしておくことが必要です。

実稼働システムの変更については、規程を踏まえた手続きが行われているかを確認することが必要です。変更によるトラブルが発生していない場合でも、規程が形骸化している場合があるので、変更後には必ず作業内容を確認することが必要です。また、緊急にシステムの変更が必要な場合も想定されます。こうした場合に備え、事前に連絡体制や判断基準などを定めておくことも重要です。

実稼働しているシステムでは、利用状況の変化やデータの蓄積などにより、システム資源の状況が大きく変化します。システムの性能・容量管理においては、利用状況を定期的に把握するとともに、計画に沿った変更や季節変動などの要因を考慮し、必要なシステムの能力を予測することが必要です。予測結果がシステムの能力を超えるような場合には、拡張計画を立案し、不要なシステムトラブルを未然に防ぐことが望まれます。

（了）

大項目３．貴社における通信ネットワーク及び情報システムの運用管理に関するセキュリティ対策についてうかがいます。

①貴社では、情報システムの運用に必要なセキュリティ対策を実施していますか。

説明　通信ネットワークや情報システムの運用管理に必要な情報セキュリティ対策には、セキュリティ要件の明確化、各種手順書の策定、セキュリティに影響するイベントの記録とチェックなどがあります。

対策のポイント

●情報システムを運用する際のセキュリティ要求事項は明確にされているか
●情報システムの運用手順書は整備されているか
●日々のシステム運用に不手際が生じないようにするための工夫はされているか
●システム運用はチェックされているか

解説

情報システムを構築するに当たって、まず、情報システムを構成する各情報資産を明確にする必要があります。それぞれの情報資産の特性を正しく理解し、脅威や脆弱性を把握してください。そのためには、情報資産の価値、情報資産に対する脅威や脆弱性から事故の発生頻度や被害の大きさを割り出す作業、つまり、リスクアセスメント（リスク評価）が必要になります。

情報システムに求められるセキュリティ要件は、情報システムの機能ごとに異なります。どのような業務でどのような情報システムが利用されているのか、またその情報システムへのアクセス権の設定などが、アクセスする人間の職務に対応しているのかということについても詳しく調査し、それぞれの情報システムに必要な機能について、それぞれ適切なセキュリティ機能を実装してください。

情報システムを適切に運用するためには、安定運用やセキュリティの観点からの監視やバックアップ、またニーズの変更に伴い各種機器の設定の変更などが必要になります。管理者または利用者がこうした作業を安全に実施するためには、マニュアル（手順書類）を整備しておく必要があります。マニュアルには、正しく運用が実施されているかどうかを判断するための指針やサービスレベルを記載し、これらを管理するための仕組みを盛り込むことを忘れないようにしてください。マニュアルは誰でもが理解できるようにシンプルでわかりやすいものでなければいけません。また、「～してはならない」という記述は網羅性に欠ける場合があります。どうすれば正しい作業ができるのかという点に着目し、「～すること」というルールの書き方ができるように業務の見直しを行うことも必要です。

特に重要なシステムの運用では、実施した操作や検出された障害、セキュリティに関連する事象（イベント）について記録しておくことが必要です。

マニュアル通りの正しい作業ができているかどうかをチェックするのは管理者の役目です。情報システム管理者はそれぞれの情報システムから得ることのできる記録をもとに、すべての利用者が正しい作業を実施できているかどうかを確認してください。また、問題の早期発見に努めるという意味で、定期的な確認作業が必要になります。できれば、社内に情報システムに関するサービスデスクを設置し、情報システムの利用における相談などを一元的に受けられるようにすると良いでしょう。

（了）

②貴社では、不正ソフトウェア（ウイルス、ワーム等）に対する対策を実施していますか。

説明　不正ソフトウェア対策にはコンピュータウイルス対策ソフトを導入し、パターンファイルのアップデートを適時行うことなどが含まれます。

対策のポイント

●ウイルス対策ソフトは適切に配置されているか
●ウイルス対策ソフトのパターンファイルの更新は適切に行われているか
●各サーバ、クライアント PC についての定期的なウイルス検査は行われているか
●システムの利用者は、ウイルス対策や問題が生じた場合における必要な処置について十分に認識しているか
●ウイルスに限らず、不正ソフトウェア対策のためのパッチマネジメントを行っているか

解説

ウイルスやワーム等の悪意のある不正なソフトウェアに対する技術的な対策としては、インターネット等社外とのネットワーク接続点におけるゲートウェイ型のウイルス対策ソフトの導入や、クライアント PC、サーバへのファイル監視型のウイルス対策ソフトなどの導入があります。

現在、一般に市販されているウイルス対策ソフトは、新種のウイルスへの対応など完全にウイルスを検出、遮断できるものではありません。このため、ウイルスやワームに感染した場合に、被害を最小範囲に留め、全社に広まらないようにするためには、発見から対応までの迅速な行動が求められます。このためには、発見時にはネットワークケーブルを抜くといった、利用者が実施できる行動に加えて、情報セキュリティあるいは情報システムの管理担当部署に対する迅速な報告と、管理部署から必要な対策を関係者に指示する手順が必要です。

迅速な状況報告を行うためには、ウイルスやワームを発見したすべての従業員が担当部署に情報を伝達できるようにエスカレーション手順を構築することから始めてください。また、情報を集約する場所として情報セキュリティ委員会や SOC（セキュリティオペレーションセンター）を指定し、報告された情報に基づいて適切な行動を指示する責任者を配置する必要があります。正しいエスカレーションを実現するには、すべての情報が責任者の元に届く仕組みが必須条件となるだけではなく、これらの情報を評価・判断するための技術者の配置も必要になります。組織内にこれらの要員をおくことができない場合は、アウトソーシングによる監視サービスなどを導入することも検討してください。

ウイルス対策においては、ウイルス対策ソフトウェアの導入だけではなく、パターンファイルの更新や情報収集を行うための体制を構築することが重要です。インベントリ管理ソフトウェアなどを利用して、ウイルス対策ソフトウェアのパターンファイルが最新のものとなっているか、定期的なウイルススキャンは行われているか、OS のパッチが正しく当てられているか、不正なアプリケーションが導入されていないか検査することによって、感染抑止効果を得ることができます。

ウイルス対策はどうしてもウイルスに感染したときの対応策ばかりを考えがちですが、未然に防ぐという観点で IT 資産の管理を行うこと、また従業員に対してウイルス感染による被害に関する教育を行うなどして、感染抑止機能を充実させることも重要な対策となります。

（了）

③貴社では、貴社で導入しているソフトウェアに対して適切な脆弱性対策を実施していますか。

説明　適切な脆弱性対策とは、セキュリティを考慮した設定や、パッチ（脆弱性修正プログラム）の適用、定期的な脆弱性検査などを言います。

対策のポイント

●ソフトウェアのパッチ(脆弱性修正プログラム）についてテスト・適用が適切になされているか
●導入したソフトウェアについてセキュリティ上必要な設定変更を実施しているか
●定期的に脆弱性検査を行い、問題点の検出・解決を行っているか

解説

情報資産としてのソフトウェアについては、ライセンス管理やバージョン管理だけではなく、ソフトウェア自身の脆弱性の管理も実施しなくてはいけません。ソフトウェアの脆弱性はパッチ(脆弱性修正プログラム)を適用することで低減することができます。しかしながら、パッチの提供は信頼のおけるソフトウェア開発元が提供しているソフトウェアに限られると考えなければいけません。すでにサポートが終了しているソフトウェアや、インターネットや雑誌添付の CD-ROM などで配布されているマクロプログラムや CGI プログラムなどは、十分な脆弱性テストが実施されていない場合もありますので、特に注意が必要です。

ソフトウェアの管理については、例えば社内標準システム（標準構成）という概念を取り入れ、一元管理を行うことをお勧めします。社内標準システムとは、業務に利用するアプリケーションを特定し、利用環境を想定したセキュリティ対策をあらかじめ施したコンピュータのことを言います。ソフトウェアの脆弱性情報などについても一元管理できるように、情報共有のための仕組みを取り入れることが望まれます。

ソフトウェアを適切に管理するためには、システムの利用者それぞれがソフトウェアのインストールを行うのではなく、例えば情報システム担当者の責任のもとに一元的にインストールを行うことで、設定ミスや脆弱性の残留を抑えることが可能になります。ソフトウェアやデータの廃棄についても手順を定め、情報システム担当者が一元的に行うなどの取り決めをする

ことも、ソフトウェアに関わるトラブルの低減に役立ちます。

また、ファイアウォールや社内サーバなどは、利用環境によって設定が異なる場合が少なくありません。さらに、新たな脅威に対する防御という意味でも設定の見直しを定期的に実施することが必要になります。これらの作業を計画的に行うには、単なる情報収集だけではなく、設定の有効期限という概念を取り入れ、定期的に設定の入れ替えを実施することが必要です。管理する機器が多い場合には、作業の効率化とメンテナンスのし忘れの防止のために、自動的なログ分析に基づくリアルタイムな設定変更などについても十分に検討しなければなりません。

問題が発生する予兆があるにもかかわらず、簡単に予防できない場合には専門家に相談することも必要です。事故が起こってから業者を選定するのではなく、いつでも相談できるようにあらかじめ保守サービスや運用サービスを行っている業者にコンタクトをとっておくなどの準備も重要です。

（了）

④貴社では、通信ネットワークに流れるデータに関して、暗号化などの適切な保護策を実施していますか。

説明　適切な保護策にはVPNの使用や、重要な情報の SSL 等による暗号化が含まれます。

対策のポイント

●社外のネットワークから社内のネットワークや情報システムへアクセスする場合に、VPN 等を用いて暗号化された通信路を使用しているか
●Web にアクセスする際、必要に応じて SSL 等を用いて通信経路を暗号化しているか
●電子メールをやり取りする場合に、重要な内容については暗号化しているか

解説

ネットワークについても、その他の情報資産と同様にどのようなデータが流れるのか、セキュリティ対策はどうなっているのかといったことを調査し、重要度を決定する必要があります。重要なネットワークには優先的に適切な保護対策を実施しなければいけません。ネットワークは一見、あらゆるシステムと接続しているように見えますが、実はセグメントという考え方で部分的に分離することが可能です。重要な情報資産が接続されているネットワークについては、一般のネットワークとは別のセグメントに隔離し、認証によるアクセス制御を実施してください。アクセス制御のポリシーは、ファイルサーバのフォルダ管理と同様に、誰がアクセスして良いのか、どのような操作をして良いのか（ネットワークサービスの制限）ということを前提として検討する必要があります。

インターネットだけではなく、社内のネットワークにおいても重要な通信は暗号化して行わなければなりません。例えば、各部門の経理担当者が経理サーバにアクセスする場合、担当者から経理サーバまでのネットワーク経路が他の部門をまたぐことになります。このような場合、多くの従業員に対して経路の途中で情報を傍受する機会を与えることになります。こうした環境では、たとえ社内 LAN であっても VPN を導入して経路を暗号化するか、スイッチングハブなどを利用して部門ごとにネットワークを分離するようにしてください。特に、無線 LAN を使用している場合には、建物の外からでも傍受できることがあるため、必ず暗号化通信の設定をしてください。

また、社内の情報システムでウェブアプリケーションを利用している場合には、アプリケーション層でのセキュリティも考慮しなければなりません。ウェブでは SSL などの暗号化プロトコルを導入することで、サーバとクライアントの間を暗号化することができます。これで通信経路上のデータは保護することができますが、情報システムに保存されたデータ、画面に表示されたデータ、プリントアウトされたデータなどは暗号化されているわけではないので、トータルセキュリティという観点ではこれらのデータの保護対策についても検討するのを忘れないでください。

なお、インターネットを利用した本支店間の通信や、出張先・外出先からのインターネット利用においては、VPN を導入して経路を暗号化してください。出張先のホテルなどから社内ネットワークにアクセスする場合、VPN によって経路全体を暗号化しないと、情報がホテル内のネットワークに漏えいするおそれもあります。社外からアクセスしてメールや社内ポータルを閲覧する場合には、セキュリティ環境が整った状態でのみ利用するというルールを作り、これを従業員に周知徹底させなければなりません。

また、重要なメールのやりとりについては、添付書類を暗号化したり、メッセージそのものを暗号化したりすることも必要になります。多くの圧縮ソフトウェアでは、ファイルの暗号化機能もサポートしていますので、それらを活用するなど、利用環境にあわせて暗号化ツールを選択してください。

（了）

⑤貴社では、携帯 PC やフロッピーディスク等の記憶媒体に対して、盗難、紛失等を想定した適切なセキュリティ対策を実施していますか。

説明　携帯 PC やフロッピーディスク等の記憶媒体の使用場所には、社外のパブリックスペースやリモートオフィス、自宅などを含みます。

対策のポイント

●携帯 PC や USB Key 型のメモリ、FD、CD などの記憶媒体について、社外持ち出し規程を定めているか
●パブリックスペースやリモートオフィスでの使用あるいは在宅作業等、社外で携帯 PC を使用する場合の物理的な盗難防止策を講じているか
●携帯 PC にログオンする際に、利用者 ID とパスワードによる利用者認証を実施しているか

●社外で使用した携帯 PC を社内ネットワークに接続する前に、ウイルス駆除等の検疫処理を行っているか
●USB Key 型のメモリや FD、CD などの記憶媒体について、紛失・盗難防止などのセキュリティ対策を実施しているか
●携帯 PC に保存されているデータを、その重要度に応じて暗号化しているか

解説

携帯 PC の置き忘れや盗難による個人情報の漏えい事件が多く発生しています。携帯 PC や持ち出し可能なメディアのセキュリティについては多くの組織が危機感を持っており、なんらかの対策をとっていますが、まだ十分であるとは言えません。携帯 PC やメディアの持ち出しルールを決める際には、それらに記録されている情報の明細を作ることをお勧めします。また、基本的な考え方として、データとアプリケーションの分離という概念も導入する必要があります。これは、データを閲覧するためにはアプリケーションが必要であることから、そのアプリケーションの入手や利用に制限を設けることで、データの閲覧を困難にするという考え方です。

携帯 PC やメディアの持ち出しを禁止している組織も多くありますが、これによって紙媒体の持ち出しが増えてしまったというケースが少なくありません。紙媒体は最も閲覧が容易なデータ形式であると言えます。また、コピーもコンビニエンスストアなどで容易に行うことができるという点で、情報が漏えいした場合の被害が拡大しやすいと考えられます。

PC やメディアに利用者認証機構を導入し論理的なロックをすることも有効な対策の一つです。利用者の認証には、「知っていること（ID、パスワード）」、「持っているもの（USB キー、IC カード）」、「本人の属性（バイオメトリクス）」という3つの要素を組み合わせて利用するようにしてください。すべての携帯 PC やメディアにこれらの対策すべてを導入するのではなく、情報資産の重要度や問題の予想発生頻度に応じて選択することが望まれます。

PC のハードディスクには様々なデータが保存されています。重要な情報が蓄積される場合には、それが蓄積される区画やあるいはハードディスク全体を暗号化し、PC 本体へのアクセス制限に加えて、もう一段深いセキュリティをかけておくことが重要です。
ただし、気をつけなければいけないのは、その暗号化のキーも PC の利用者認証に使用するのと同じキー（ID、パスワード、USB キーなど）で開けられてしまっては意味がないということです。例えば、部屋に入るまでに鍵のかかるドアが 5 枚あっても、すべてのドアが同じキーで開いてしまうのであれば、ドアが 1 枚しかないのと同じ理由です。

最後に、携帯 PC をネットワークに接続する際のセキュリティについても検討しなければいけません。ルータやファイアウォールなどで分離されたネットワークに接続するのであれば直接攻撃を受けることは少ないでしょうが、PHS や携帯電話を介して直接インターネットに接続しているときは攻撃される危険が非常に高いと言えます。パーソナルファイアウォールを導入するなど、端末単位のセキュリティについても十分に検討する必要があります。

（了）

大項目4. 貴社における情報システムの開発、保守におけるセキュリティ対策及び情報や情報システムへのアクセス制御の状況についてうかがいます。

①貴社では、業務システムの開発に際し、開発したシステムに脆弱性が残らないようにするための施策を実施していますか。

説明

業務システムは完成してしまった後に改変を加えることは困難で、コストも嵩みます。企画、設計の初期の段階から情報セキュリティについて配慮することが必要です。

対策のポイント

●利用者の認証機能は、必要に応じて適切に実装されているか
●業務処理プロセスは適切に実装されているか
●入力データの正当性チェックは適切に行われているか
●情報の保護機能は適切に実装されているか
●ソフトウェアの構造上潜在しうる脆弱性が残されていないことが確認されているか

解説

施策としては、情報セキュリティ上の要求事項をシステムの仕様書に盛り込むことなどがあります。また、開発した業務システムに適切な情報セキュリティ対策が施されているかどうかを把握する必要もあります。アクセス制御は一般的ですが、単に利用者の範囲を限定するだけでは十分ではありません。

認証による利用者の制限は、最低限の情報セキュリティ対策です。業務システムを使用できる人とできない人を明確に分ける必要があります。

利用者のアクセス制御は業務ごとに行うことが必要です。例えば、機密文書を参照する権限を持つ利用者や照査の権限を持つ利用者を限定する機能は、現実の業務に即して設定できることが必要です。業務フローから逸脱した参照行為や照査行為などが行われないように業務システムが構築されているかどうかを確認してください。

現実の世界では、一人の人が複数の役割を持つことがよくあります。このような複数の役割を持つ人が、越

権行為ができないようにすることも必要になります。業務フローと現実の役割をよく吟味して、権限などを設定できるようにしなければなりません。

データの入力に際しては、要求されていない数値や文字列の入力ができないように制限を設けることも必要です。数値の範囲が決まっている場合や文字の種類が決まっている場合、文字列の長さが決まっている場合などには､条件に合わないデータの入力ができないようなチェックの仕組みを組み込んでおくのが良いでしょう。

読み書きの制限や削除の制限など、システムに記録されている情報(ファイル)の保護機能が実装されている必要があります。利用者ごとに読み書きや削除の制限を変えることは最低でも必要です。その他、利用する形態に応じて、部署単位や職務形態単位など、グループごとに保護機能があることが望ましく、必要に応じてアクセス制限による保護などを実装します。

システムには、開発時には意図していなかったデータの入力などによって動作が不安定になる脆弱性が潜んでいる場合があるため、脆弱性をチェックするサービスやソフトウェアなどを利用して、潜在的な脆弱性を取り除いておく必要があります。このとき、どのようなソフトウェアを使い、どのような方法を用いて脆弱性をチェックしたのかをあとでわかるように記録しておきます。

このような対策は、システムの開発時に配慮するのはもちろんのこと、仕様書に要求として盛り込んでおくことが大切です。そのためには、どのような人たちが使用するのか、どのような権限の区分があるのか、複数の業務フローの交差(複数の役割を持つ人の存在)など、扱うデータや文書の種類などを整理し、把握しておく必要があります。また、どの利用者がどのような操作をおこなったのかをログに記録するなどして、あとから参照できるようにしておくことも大切です。これによって、事故が発生した場合に原因を追究することができるだけでなく、操作のログが残されていることを周知することで、使用者の悪意ある行為を未然に防ぐことにもつながります。

攻撃の手法は年々進化しており、セキュリティ意識が低い開発者によって、コーディング時に脆弱性を内包してしまうことも多くあります。開発者向けにセキュアなコーディング手法を教育したり、開発ガイドラインを定めておくのもよい方法でしょう。

（了）

②貴社では、ソフトウェアの選定・購入、システムの開発・保守に際して、工程ごとにセキュリティの観点からチェックを行うなど、セキュリティ管理が実施されていますか。

説明　ソフトウェアにセキュリティ上の問題が混入しないための管理が重要です。購入に際しては、ソフトウェアの開発元の確認、開発の際のセキュリティチェックやレビュー記録などを確認できることが望まれます。

対策のポイント

●ソフトウェアの購入に際して、開発元の定評の確認や製品の評価を行った記録のレビューができるか
●ソフトウェアのバージョン変更の記録、導入前の試験記録をレビューできるか
●システムの開発プロセスが整備されているか
●各プロセスで生成される成果物が適切な管理のもとで保管されているか
●そのための方針があり、実施状況の把握ができるか

解説

ソフトウェアの導入前に、その評価を行い、評価方法や評価内容の記録を残すことが重要です。こうしておくことで脆弱性が見つかった場合、評価に漏れがなかったかどうかを後で確認することができます。開発元の定評は、ソフトウェアの品質の評価の目安になりますが、新しいベンチャー企業などでもしっかりした開発を行っている企業もありますので、定評は目安としてください。

ソフトウェアを含む情報資産全般の変更記録は基本的な項目です。変更記録により、どのような構成のソフトウェアを使用しているのか、新たな脆弱性が見つかったときに、使用しているソフトウェアがその脆弱性を有するバージョンであるかどうかなどを容易に確認できるようになります。変更記録を適切に実施することにより、ソフトウェアの構成管理を行ってください。

システムの開発においては、レビューの実施と記録が特に重要です。開発プロセスを整備することにより、プログラマによる余分なコードの追加、不要な脆弱性の残留といったことを予防することができます。レビューの項目としては、ソフトウェアの選定・購入に際しては必要なセキュリティ機能が具備されていること、既知の脆弱性が含まれていないこと、脆弱性等に関する情報が提供されることが挙げられます。また、設計段階では、リスク分析の結果必要とされるセキュリティ機能が盛り込まれていること、セキュリティに関する運用面の考慮もされていること、システム運用とセキュリティ運用に必要な管理者及び利用者向けの手順書類が明記されていることが挙げられます。開発段階では、開発のための十分な人員やセキュリティを考慮した環境が割り当てられていること、開発及びテスト用の機器やソフトウェア等の環境が整備されていること、最新の攻撃手法を考慮した十分なテストが実施されていることなどが挙げられます。

各プロセスで生成される記録やドキュメント類、ソフトウェアやデータなどの紛失、盗難、改竄などを防止する必要があります。関係者以外には秘密にされている情報に権限のない者がアクセスできないようにすると

ともに、権限があっても不必要に外部に持ち出さないようにするための管理が重要です。
　ソフトウェアの選定、購入、システムの開発・保守等の方針は、関係者に周知徹底することも必要です。定めた方針が周知できていることを確認する仕組みを作り、実施状況を把握します。さらに、もし方針と実施状況の間にギャップがあれば、是正処置を行います。

（了）

③貴社では、情報（データ）へのアクセスを制限するための利用者管理や認証を適切に実施していますか。

説明　適切な利用者管理には、利用者 ID の定期的な見直しによる不要 ID の削除や共用 ID の制限、単純なパスワードの設定禁止などがあります。

対策のポイント

●利用者の登録及び削除に関する規程は定められているか
●不要な利用者 ID や利用者に対する必要以上の権限の付与の有無などを定期的にチェックしているか
●利用者に、空白のパスワードや単純な文字列のパスワードを設定しないよう要求しているか
●情報にアクセスできる利用者を限定し、利用者ごとに割り当てられた ID とパスワードによる認証を実施しているか
●重要情報を格納した情報システムについては、利用時間の制限を徹底しているか

解説

　適切な利用者管理のためには、利用者の登録・削除に関する手続きを定める必要があります。登録しようとする利用者の権限や正当性の確認と、それを承認するプロセスを定めます。利用者の異動や退社によって利用者 ID が不要になった場合に、その ID が登録されたままになることは避けなければなりません。なぜなら、使用されない利用者 ID は、権限をもたない者によって不正に使用された場合に、それが不正な使用であることをすぐに発見できないことがあるためです。不要な利用者 ID は削除することが望まれます。

　職務の変更や異動によって利用者の権限の変更が発生した場合には、照査権限を持たない利用者が他部署の情報を照査することを防止するために利用者の情報へのアクセス権限を変更しなければなりません。そのためには、すべての利用者の ID の必要性や権限を異動などのタイミングで定期的に見直す必要があります。

　一方、ID の権限などをいくら厳密に管理しても、パスワードが設定されていなかったり、簡単に推測できるようなパスワードが設定されていると、ID を不正に使用される可能性があります。しかし、記憶することが困難なパスワードを設定してしまったためにパスワードを紙に書いて机に張り出しておくなどの行為は本末転倒であり、絶対にあってはなりません。思い出しやすいフレーズなどをうまく利用し、数字や文字だけでなく、記号などを織り交ぜたパスワードを設定するなどの工夫が必要です。また、単純なパスワードを使用しないようにルールを定めるとともに、可能であればシステムの設定で単純なパスワードを排除するようにします。

　情報にアクセスできる利用者を限定し、利用者ごとに割り当てられた ID とパスワードによる認証を実施します。その際、一つの ID を複数の利用者が共有しないようにします。ID が共有されているとパスワードが利用者以外にも広く知れ渡ってしまう傾向にあり、結果的に誰でも情報にアクセスできてしまい、秘密が守れなくなります。また、その ID で情報にアクセスしたのが誰なのかを特定することが困難になります。そのため、情報が漏れたりシステムが破壊された場合に、ID は特定できても、その ID を使用したのが誰なのかを後から追跡することができず、コンプライアンス違反が発生しても、当事者を見つけることが難しくなります。また、パスワードの変更も困難になります。

　監督者や承認者が不在の時間帯、あるいは周囲の監視の目がなくなる時間帯などに不正行為が発生する可能性があります。また、必要以上に長時間の利用は、不正行為を増長させる可能性もあります。したがって、重要情報を格納した情報システムについては利用時間を制限して、不正行為の発生を防止することも有効です。

（了）

④貴社では、業務アプリケーションに対するアクセス制御を適切に実施していますか。

説明　業務アプリケーションに対する適切なアクセス制御には、例えば利用者ごとに利用できる機能を制限することがあります。

対策のポイント

●利用者ごとにアクセス可能なサービスを制限しているか
●業務アプリケーションの利用者に対して、アクセス制御を実施しているか

解説

　例えば人事データを閲覧できる利用者を制限したり、派遣社員と正社員の利用できるサービスを区分するなど、利用者ごとに利用可能なサービスに制限を設けることが必要です。職務と権限に見合ったサービスを利用できるようにするとともに、権限のない者に対する制限を行う必要があります。

　業務アプリケーションそのものの利用の可否だけでなく、同じ業務アプリケーションの中でも照査権限や変更権限などの権限区分を含めて、アクセス制御を行うことが必要です。また照査権限の中でも、一度に参照できるデータの件数を区別するなどの権限区分を設定することも考えるべきです。役職上の権限に合わせてコンピュータの提供する業務アプリケーションのサービスの利用権限を管理するために、アクセス制御を行います。

（了）

⑤貴社では、ネットワークのアクセス制御を適切に実施していますか。

説明　適切なネットワークのアクセス制御には、例えばネットワークの分離や社外からの接続時の認証などがあります。

対策のポイント

●社外のネットワークから社内システムへアクセスする際(携帯 PC を使用する場合を含む)に、利用者認証を実施しているか
●サービスやシステムにアクセス可能な利用者を制限するために、ネットワークを物理的あるいは論理的に切り離しているか
●許可されていないワイヤレスアクセスポイントの設置を禁止しているか
●社外のホットスポットを利用してネットワークにアクセスする場合のセキュリティ対策を実施しているか
●社内のネットワークに接続する端末機器について、接続時に認証を実施しているか
●外部のネットワークサービスを利用する場合に、そのサービスにどのようなセキュリティ上の対策が実施されているかについて確認しているか

解説

社外から社内システムへのアクセスを許す場合、利用者認証を実施して正当な利用者であることを確認する必要があります。認証の記録を残し、許可されていない行為(持ち出し禁止のファイルのコピーなど)が行われていないかどうかを利用者ごとに確認します。

また、ハードウェアベンダのリモートメンテナンスや業務提携先との情報交換など、社外の組織と何らかの形でネットワークの接続を行う際には、必要とされる機器や情報にのみアクセスができるよう、アクセス制御が必要です。ネットワークのアクセス制御には、パケットレベル、セッションレベル、アプリケーションレベルなどいくつかのレイヤーがありますが、どの方式にするかはリスク分析を行い、また費用等を勘案して決定します。

保護すべき重要なデータが入っているシステムは、それ以外のシステムが接続しているネットワークから物理的に切り離し、特定の端末あるいはネットワークセグメントからのみ操作できるようにするのが最善の策です。しかし、作業効率の面などを考慮して、便宜上、その他のシステムもつながっているネットワークに接続しなければならない場合もあります。このような場合には、物理的に切り離したのと同等のセキュリティが確保されるように、重要システムとネットワークとの間にファイアウォールを設置し、特定の端末あるいはネットワークセグメントからのみアクセスできるようにする(論理的に隔離する)ことが必要です。

ワイヤレスアクセスポイントを許可なく設置すると、会社の建物の外など、予期しない場所からのアクセスが可能になることがあります。ワイヤレスアクセスポイントは、個別の部署が設置するのではなく、情報セキュリティ担当部署や社内システムの管理部署の担当者など、セキュリティ上の設定に詳しい者が、正当な許可を得て設置する必要があります。

社外の公衆無線 LAN サービスでは、アクセスしている PC が相互に通信可能となり、互いに共有ファイルなどが参照できる状態になることがあります。これによって、機密データなどの重要データが、第三者によって参照されてしまう場合があります。また、パーソナルファイアウォール等のセキュリティ対策が実施されていない場合には、ウイルスなどが容易に侵入する可能性があります。社外でネットワークに接続する場合には、PC 自体にセキュリティ対策を施しておく必要があります。

ウイルスの侵入や許可されていないデータの参照などが行われないようにするために､許可されていない PC が社内ネットワークに接続されることを防ぐ必要があります。接続する PC を限定するためには、ネットワーク接続時に PC の認証を行うことが必要になります。

その他、同じネットワークサービスを利用する PC 同士が不用意に接続してしまうことを防止するための対策など、ネットワークに関する情報セキュリティ上の対策の実施状況を確認しておかなければなりません。その上で、自分の PC に対して必要なセキュリティ対策を施し、注意してネットワークサービスを利用する必要があります。

（了）

大項目5. 貴社における情報セキュリティ上の事故対応状況についてうかがいます。

①貴社では、情報システムの障害発生を想定した適切な対策を実施していますか。

説明　情報セキュリティの重要な要素の一つである可用性に影響を与える事象のうち、影響の度合いが最も大きいのは、情報システム関連機器の故障であると言っても過言ではありません。情報システムに求められる可用性の条件を満たすためには、可用性に関する要求に対応した適切な障害対策機能のシステムへの組込みが欠かせません。

対策のポイント

●情報システムの可用性に関する要求は明確で妥当なものか
●システム全体としての障害対策のスキームは確立しているか
●事故への即応処理としてのシステムの切り離しや縮退機能、情報の回復や情報システムの復旧に必要となる機能は、情報システムに組み込まれているか
●復旧に必要なバックアップや運用の記録等の確保は適切に行われているか
●障害発生時の対応手順や障害対策の実施要領は確立しているか
●現場における障害対応能力は確保できているか
●社外にシステムの運用を委託している場合、障害発生時も考慮したサービスレベルが保証されているか

解説

必要となる障害対策の内容は、可用性に関する要求の程度によって大きく左右されます。そのため、障害対策の是非を論じるに当たっては、まず、対象となるシステムの可用性に関する要求を明確化し、その妥当性をチェックしなければなりません。可用性に関する要求として明確にすべきことには、次の事項があります。

- 原則的な運用時間帯
- 情報システムが停止してから復旧・再開までの許容停止時間

障害対策を検討する上で最も重要な要素には、次のようなものがあります。

- 対策の対象とする障害
- 障害発生時における、機能の縮退、バックアップ機への切替、システムの一時停止等の対応
- システム停止時の情報の回復やシステムの復旧の方式

これらを中心とした障害対策の仕組みがよく検討されていないと、技術的な対応と運用面での対応に齟齬が生じる場合があります。障害対策は技術面と運用面の連携が不可欠であり、連携がうまく行かないと、全体としての障害対策が効果的に機能しないことがあります。

また、事故への即応処理としてのシステムの切り離し、縮退機能や、情報の回復やシステムの復旧に必要となる機能は、障害発生時に円滑に機能することが確認されていなければなりません。そのためには、障害対策機能に関するテストの実施や、システム環境の変化に対応するための定期的なチェックが必要となります。

システムに組み込まれた障害対策機能が正常に実行されるためには、バックアップデータや運用の記録等が必要となります。このため、日常のシステム運用の中で、バックアップデータや運用の記録の確保も欠かせません。

また、障害対策の実行は、日常の運用から見れば、大きな例外作業であるため、次のようなことが確立していなければ、障害発生時に必要な対応を迅速に行うことは、あまり期待できません。

- 障害検知時の報告要領
- 障害対策の実施責任者の設置と作業体制の確保
- 障害発生時のシステムの切替え手順や、情報の回復からシステムの復旧に至るまでの処理手順や操作要領

また、障害対策の実施要員が、非日常的作業である障害対応作業を適切に実施することができるようにするためには、関係者に対する障害対応要領の周知や、障害発生時に必要な作業を実行するためのスキルを教育や訓練等によって要員に身につけさせることも重要な課題の一つになります。

社外にシステムの運用を委託している場合、障害発生時においても、必要なサービスレベルが保証されるようにしておくことが必要です。そのためには、委託に当たって、次のようなことを明確にしておくことが必要となります。

- 最大停止時間等の要求条件
- 委託先が障害発生時に実施すべき作業や対応

（了）

②貴社では、情報セキュリティに関連する事件や事故が発生した際の行動や報告、判断の基準を定めた対応手続きを準備していますか。

説明 情報セキュリティに関連する事件や事故が発生した場合、被害の拡大を防ぎ、被害を限定的なものにするためには、組織全体として事件や事故に必要な対応が適切かつ迅速にできなければなりません。そのためには、事件や事故の

形態ごとに、実施すべき作業やその実施要領を確立するとともに、現場の要員がいざというときに対応作業を円滑に実行できるようにしておくことが必要となります。

対策のポイント

●事件や事故の種類ごとに、必要な対応作業の実施要領を定めているか
●事件や事故の発生に備えて、対応要領の現場の要員への徹底を行っているか
●事件や事故の形態ごとに対応体制を定めているか
●事故対策に必要なツールやリソースの確保と、その稼働確認を定期的に実施しているか

解説

事件や事故の種類ごとに以下のようなことが確立していなければ、非日常的な処置の積み重ねとなる事件や事故への対応を迅速かつ適切に行うことはできません。

- 社内の関係者への報告（誰にどのような報告を行うか）
- ネットワークの遮断、システムや業務の一時停止等の必要に応じて実施すべき緊急処置とその適用基準や実行手順
- 被害状況の調査（被害範囲や被害の内容等）
- 原因の調査と対策の実施
- 被害者への連絡や社外への周知等のリスクコミュニケーションの体制の確保
- 通常のオペレーションへの復旧手順
- 業務の再開手順

これらの具体的な内容は、個人情報の漏えい、営業機密情報の漏えい、システムや情報の混乱、システムの長時間停止、コンプライアンス違反など、発生した事件や事故の種類によって異なります。このため、事件や事故発生時の対応要領は、それぞれの組織に与える影響が大きいと考えられる事件や事故の形態ごとに定めておかなければなりません。

また、事件や事故発生時の対応要領が定められていても、その内容が作業実施要員に十分に伝わっていなければ、いざというときに必要な対応作業を迅速に行うことができません。このためには、以下が必要となります。

- 対策現場における対応要領の周知
- 事件や事故対応訓練を通じた関係者の対応能力の育成

また、事件や事故の処理には、組織的な対応が不可欠です。このため、日頃から、以下のようなことについての確認も必要となります。

- 緊急連絡網を確立し常時機能するようになっているか
- 責任者と対応実施体制が決まっており、当事者が自分の責任を認識しているか

事件や事故によっては、被害状況の調査や情報の回復、一時停止したシステムの再開始に必要なツールやハードディスク等が必要となるため、事前に準備しておく必要があります。ただし、これらの機器はシステム環境の変化等によって使用できなくなっていたり、普段は使う機会がないために使用に手間取ったりすることがよくあります。そのような事態を防ぐために、これらの機器が正常に稼働することを定期的にチェックすることも必要です。

（了）

③貴社では、何らかの理由で情報システムが停止した場合でも事業を継続するための取組みが、組織全体を通じて検討されていますか。

説明　災害、施設・システム機器・業務ソフト・業務データの損壊や、情報システムに生じた重大事故等によって、情報システムが停止し、短期間での復旧の目処がたたなくなるような事態の発生が考えられます。このような状況においても事業の継続ができるようにするためには、情報システム全体のバックアップセンターの準備や、ソフトウェア資産・業務データのバックアップとその安全な保管、さらには手作業により業務の遂行ができるようにしておくなどの準備が必要となります。事業活動の多くを情報システムに依存している組織においては、事業継続への取組みは十分に検討しておくべきです。

対策のポイント

●業務の重要度や、業務システムのトラブルが業務に及ぼす影響について把握しているか
●情報システムの長期停止を想定した事業継続計画は確立されているか
●バックアップセンターを利用する場合、バックアップセンターへの切替えが円滑に行われるようになっているか

●バックアップセンターへの切替え時や、システム復旧後の業務の再開に用いる業務データやソフトウェアのバックアップがとられ、安全な場所に保管されているか
●非常時において、手作業で業務を遂行するための備えはできているか

解説

情報システムの停止が長期に及ぶような場合を想定した事業継続計画は、業務の重要度や、情報システムのトラブルが業務や事業に及ぼす影響に関する判断（ビジネス・インパクト分析）に則して策定しなければなりません。また、事業継続計画が非常時及び復旧後の事業活動に大きな影響を及ぼすことを考えれば、計画には経営陣の承認も必要です。

バックアップセンターへの切替えが円滑に行われるようにするためには、日頃から、以下のような備えが必要となります。

- バックアップセンターの確保
- バックアップセンターへの切替え要領の確立
- バックアップセンターへ切替るために必要となる機能やツールの準備
- バックアップセンターへの切替えに関わる要員に対する教育や訓練による対応能力の確保

障害発生時には、現用の業務データが失われていることも多いため、バックアップセンターへの切替え時や復旧後の業務再開の際に用いる業務データやソフトウェアを他の安全な場所で保管するようにしておくことも必要となります。

バックアップセンターを準備していない場合や、バックアップセンターへの切替えがうまく行えない場合には、情報システムに頼っていた業務を手作業での実施に切替えなければなりません。手作業に切替えて業務処理を行えるようにするためには、日頃から、以下のような備えが必要となります。

- 手作業での業務処理要領の整備
- 手作業での業務の遂行時の体制やオフィスの使用方法等の検討
- 手作業の業務に用いる台帳等の必要な情報の日頃からの準備

（了）

２.「望まれる水準」の導出

企業アンケート結果をもとに、企業にとって「望まれる水準」を設定した。なお、この分析には、全回収票 1,633 件中、すべての設問に回答があった 885 件（大手企業 474 件、中小企業 411 件）分を活用した[1]。

（１）回答企業の分類

まず、企業を分類する２軸について、それぞれ該当する変数についての主成分分析を行い、以下の式を導出した。

✓ 事業構造上の脆弱性指標

正社員割合、総拠点数、IT 依存度、インターネット依存度、ビジネスパートナーへの依存度、年間離職率の６変数について主成分分析を行い、事業構造上の脆弱性指標値を設定する[2]。

事業構造上の脆弱性指標

= -0.0018×正社員割合+ .0710×総拠点数+ 0.5389× IT 依存度

+ 0.5326×インターネット依存度+ 0.3588×ビジネスパートナーへの依存度- 0.0302×年間離職率

✓ 社会的影響力指標

売上高、公益性、顧客への影響、ブランドへの影響、機密情報の保有度、保有個人情報数の６変数について主成分分析を行い、社会的影響力指標値を設定する[2]。

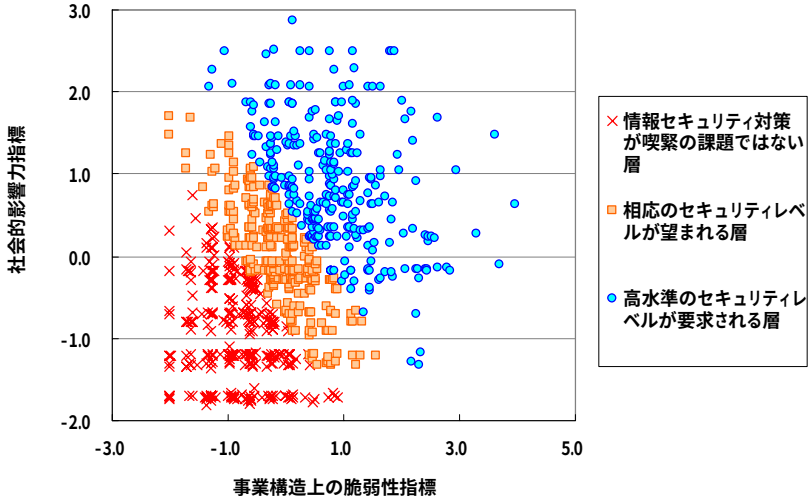
社会的影響力指標

= 0.1331×売上高 + 0.2764×公益性 + 0.3082×顧客への影響

+ 0.3044×ブランドへの影響 + 0.3214×機密情報の保有度 + 0.2212×保有個人情報数

この式に則り、上記の２軸に沿った各社の分布を図 ５に示す。これら回答企業は、事業構造上の脆弱性や社会的影響力の大きい順に、回答社数が均等になるよう３つのグループ（各 295 社）に分類した。

図 ５ 回答企業の分布



[1] 「回答企業の分類」で企業を分類する２軸の算出式を導出する段階では、それぞれ基礎となる変数の回答があるもの（社会的影響力指標:n=1180、事業構造上の脆弱性指標:n=1268）を用いた。

[2] 各式の基礎となる変数は、素点ではなく正規化（平均=0、分散=1）したものを用いる。詳細は A1-30 頁参照。

（２）トータルスコア

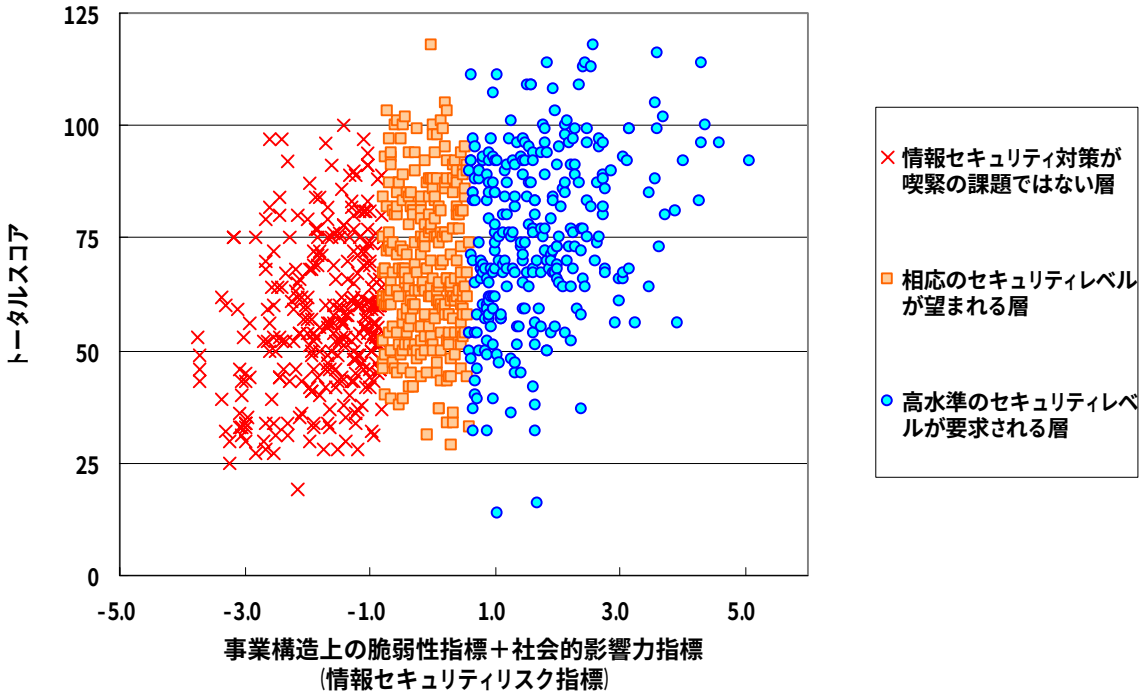
簡略化のため、

情報セキュリティリスク指標　＝　事業構造上の脆弱性指標＋社会的影響力指標

として、これと対策の取組状況のトータルスコアの関係を図 ６に示す。

なお、トータルスコアは、評価項目全 25 項目について、５段階評価を点数に換算し、各項５点満点、合計 125 点満点として算出した。

図 ６　トータルスコアの分布



これらの平均値をまとめると次のようになる。

表 １　各層の平均値

	事業構造上の脆弱性指標	社会的影響力指標	情報セキュリティリスク指標	トータルスコア
情報セキュリティ対策が喫緊の課題ではない層	-0.837	-0.908	-1.745	57.186
相応の水準のセキュリティレベルが望まれる層	-0.120	0.023	-0.096	68.044
高水準のセキュリティレベルが要求される層	0.838	0.871	1.709	75.349

各層のトータルスコアの平均を比較すると、要求されるセキュリティレベルが高い（内在するリスクが高い）ほど、トータルスコアの平均も高く、より積極的に対策に取り組んでいることがわかる。ただし、各層ともトータルスコアのばらつきが大きい。例えば、高水準のセキュリティレベルが要求される層の中にも、低いトータルスコアに留まる企業がある。

（３）望まれる水準

ISMS の認証取得に至るレベルであれば、本来の成熟度は「4」（経営層の指示と承認のもとに方針やルールを定め、全社的に周知･実施しており、かつ責任者による状況の定期的確認も行っている）に達していると考えられる。ただし、特定の部門のみ ISMS 認証を取得している場合には、企業全体で考えると成熟度「3」（経営者の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない）～「4」の間に位置するのではないかと考えられる。したがって、高水準のセキュリティレベルが要求される層の場合、それと同等のレベル、すなわち「3」～「4」の間にあることが求められる（①）。

また、「情報セキュリティ対策が喫緊の課題ではない層」でも、「経営層の承認のもとに方針やルールを定め、全社的に周知･実施する(＝3)」のレベルを求めていくことが妥当と考えられる（②）。

しかし、各層とも全体平均値は 3.0 以下であることを考えれば、直ちに①②のレベルを求めることは実質的には困難である。

以上のことから、望まれる水準としては、「各層の上位１／３における平均値を目標としつつ、各層における全体平均値に達していない企業については、各層における全体平均値を、早期に達成すべき暫定的目標として設定する」ことが適当である（図　７参照）。具体的な値を表　２に示す。

図　７　望まれる水準の設定

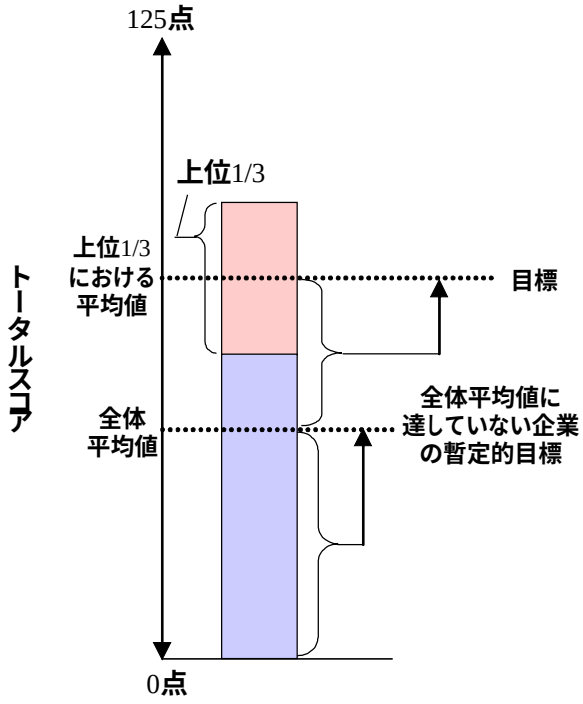


表　２　望まれる水準の具体的な値

	全体	高水準のｾｷｭﾘﾃｨﾚﾍﾞﾙが要求される層	相応のｾｷｭﾘﾃｨﾚﾍﾞﾙが望まれる層	情報ｾｷｭﾘﾃｨ対策が喫緊の課題ではない層
上位 1/3 の平均値	88(3.5)	96(3.8)	87(3.5)	76(3.1)
全体平均値	67(2.7)	75(3.0)	68(2.7)	57(2.3)

注：（　）内の数値は、企業における取組みの成熟度に換算したもの。

ただし、この「望まれる水準」は、企業の業務内容・IT 依存度の変化といった内的要因だけではなく、社会全体のネットワーク化の更なる進展といった外的要因によっても変動していくものであることに十分な留意が必要である。

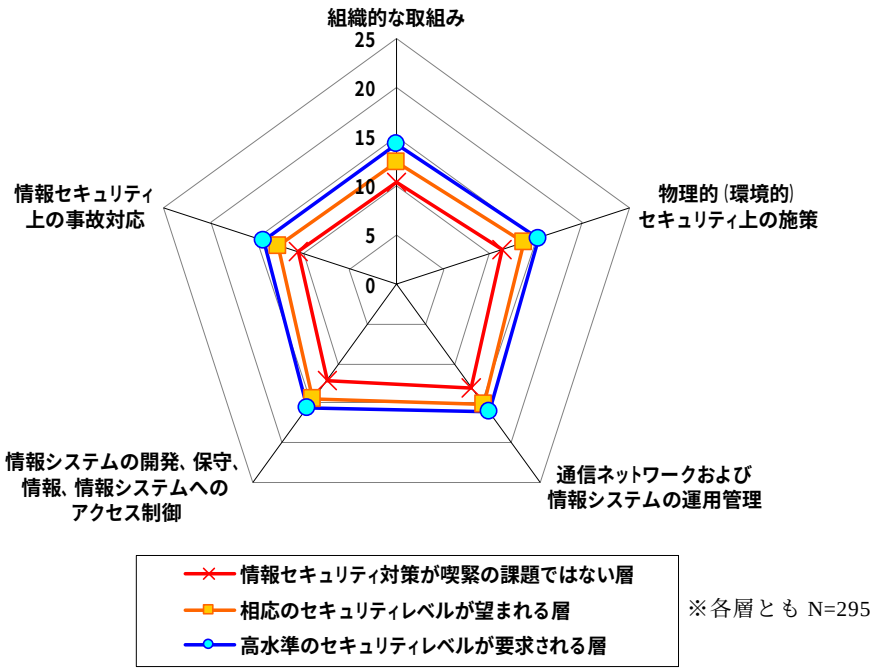
なお、「望まれる水準」の設定に当たっては、検討の過程で、「相対基準ではなく絶対基準が望ましい」との意見もあったが、情報セキュリティ対策が十分に進んでいない国内企業のレベル向上を目指すに当たり、絶対基準の設定が適当かは慎重な検討が必要であること、また、既に ISMS 認証基準のような絶対基準もあること等から、現段階で対策ベンチマークにかかる絶対基準は設定しないこととした。

（4）設問別の平均

設問グループごとのグラフでは、要求されるセキュリティレベルが高い層は、情報セキュリティ対策が喫緊の課題ではない層に比べ全体的に上回っているが、大きな差は見られなかった。

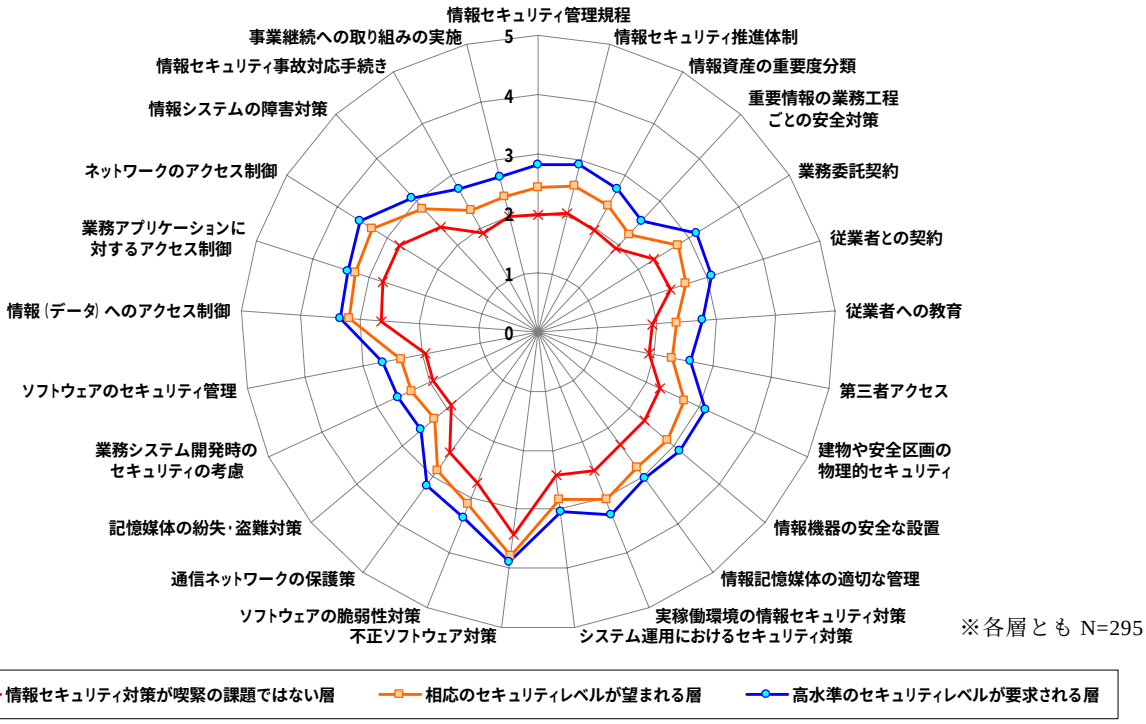
また、小問ごとのグラフでは、各層とも対策が進んでいる項目（例.Q3-2 不正ソフトウェア対策）と遅れている項目（例.Q1-4 重要情報の業務工程ごとの安全対策）についての傾向は同様であった。

図 8　設問グループごとの回答層別平均



※各層とも N=295

図 9　小問ごとの回答層別平均



※各層とも N=295

【参考１】企業分類に係る指標の算出方法

各回答企業の「事業構造上の脆弱性指標」「社会的影響力指標」はいずれも、該当する項目の回答を数値化して（a 欄）、その平均点・標準偏差を算出（b 欄・c 欄）、正規化した上で（d 欄）、主成分分析により導出した項目係数（e 欄）を乗じたもの（f 欄）を合計して算出した。

①事業構造上の脆弱性指標

		a欄	b欄	c欄	d欄	e欄	f欄
項目	内容	数量化 （各項目についてを以下の基準により数量化）	平均値 （※）	標準偏差 （※）	正規化値	項目係数	指標の各項目毎の因子
正社員割合	貴社の従業者数（派遣、アルバイトを含む）に対する正社員の割合	（単位：%）	77.673	23.249	（a欄－b欄）／（c欄）	-0.0018	（d欄×e欄）
総拠点数	貴社の国内外の拠点（支社・支店・営業所）の数	（単位：個所）	36.133	288.791	（a欄－b欄）／（c欄）	0.0710	（d欄×e欄）
IT依存度	貴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）に依存している割合はどの程度か	以下の4段階で点数化 一部にとどまる（25%以下）：1点 若干依存している（25%以上、50%以下）：2点 多くの部分が依存している（50%以上、75%以下）：3点 ほとんどの部分が依存している（75%以上）：4点	2.797	1.054	（a欄－b欄）／（c欄）	0.5389	（d欄×e欄）
インターネット依存度	貴社の主要な業務に関わる業務プロセスのうち、インターネットに依存している割合はどの程度か	以下の4段階で点数化 一部にとどまる（25%以下）：1点 若干依存している（25%以上、50%以下）：2点 多くの部分が依存している（50%以上、75%以下）：3点 ほとんどの部分が依存している（75%以上）：4点	1.611	0.858	（a欄－b欄）／（c欄）	0.5326	（d欄×e欄）
ビジネスパートナーへの依存度	貴社の業務の、元請や代理店、フランチャイジー等のビジネスパートナーへの依存度はどの程度か	以下の4段階で点数化 ほとんど依存していない：1点 部分的に依存している：2点 大きく依存している：3点 元請や代理店、フランチャイジーなしでは事業が成り立たない：4点	2.028	0.892	（a欄－b欄）／（c欄）	0.3588	（d欄×e欄）
年間離職率	貴社における離職率（直近の1年間に退職・転職された従業者の割合）はどの程度か	（単位：%）	6.037	8.305	（a欄－b欄）／（c欄）	-0.0302	（d欄×e欄）
事業構造上の脆弱性指標（f欄の合計）							（f欄の合計値）

※b欄およびc欄の平均値、標準偏差はアンケート結果を基に得られた値（標本数 n=1268）

②社会的影響力指標

		a欄	b欄	c欄	d欄	e欄	f欄
項目	内容	数量化 （各項目についてを以下の基準により数量化）	平均値 （※）	標準偏差 （※）	正規化値	項目係数	指標の各項目毎の因子
売上高		（単位：百万円）	61526.4	127537.8	（a欄－b欄）／（c欄）	0.1331	（d欄×e欄）
公益性	貴社の事業が、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るか	以下の4段階で点数化 ほとんどない：1点 少ない：2点 他の業種に比べると高い：3点 事業の性質上極めて高い：4点	2.354	0.913	（a欄－b欄）／（c欄）	0.2764	（d欄×e欄）
顧客への影響	貴社の事業が、顧客の生命・身体・財産・名誉等に与える影響の大きさはどの程度か	以下の4段階で点数化 ほとんどない：1点 少ない：2点 大きな影響がある：3点 極めて大きな影響がある：4点	2.203	0.865	（a欄－b欄）／（c欄）	0.3082	（d欄×e欄）
ブランドへの影響度	個人情報漏洩等、情報セキュリティ関連の事故が発生した場合、貴社のブランド（企業イメージ）に与える影響の大きさはどの程度か	以下の4段階で点数化 ほとんどない：1点 部分的に影響がある：2点 大きな影響がある：3点 企業の存続に関わる影響がある：4点	2.598	0.803	（a欄－b欄）／（c欄）	0.3044	（d欄×e欄）
機密情報の保有度	外部に漏洩すると事業に極めて深刻な影響が生じる重要情報（国家機密、営業機密、プライバシー情報等）をどの程度保有、管理または使用しているか	以下の4段階で点数化 ほとんどない：1点 少ない：2点 全体の半分程度：3点 ほとんどがその種の情報である：4点	2.256	0.899	（a欄－b欄）／（c欄）	0.3214	（d欄×e欄）
保有個人情報数	事業を実施する上で何名分程度の個人情報を取り扱っているか（データの述べ数ではなく、対象とする人の数の概数）	（単位：人分）	249308.1	822664.5	（a欄－b欄）／（c欄）	0.2212	（d欄×e欄）
社会的影響力指標（f欄の合計）							（f欄の合計値）

※b欄およびc欄の平均値、標準偏差はアンケート結果を基に得られた値（標本数 n=1180）

【参考２】業種別の傾向

今回の企業アンケートにおける業種別の結果について、参考として図 １０、図 １１に示す。

ただし、今回回収できたサンプル数には業種間で大きなばらつきがあるため、以下のデータをもってそれぞれの業種における取組みの進展度を比較することは困難である。

図 １０　設問グループごとの業種別平均

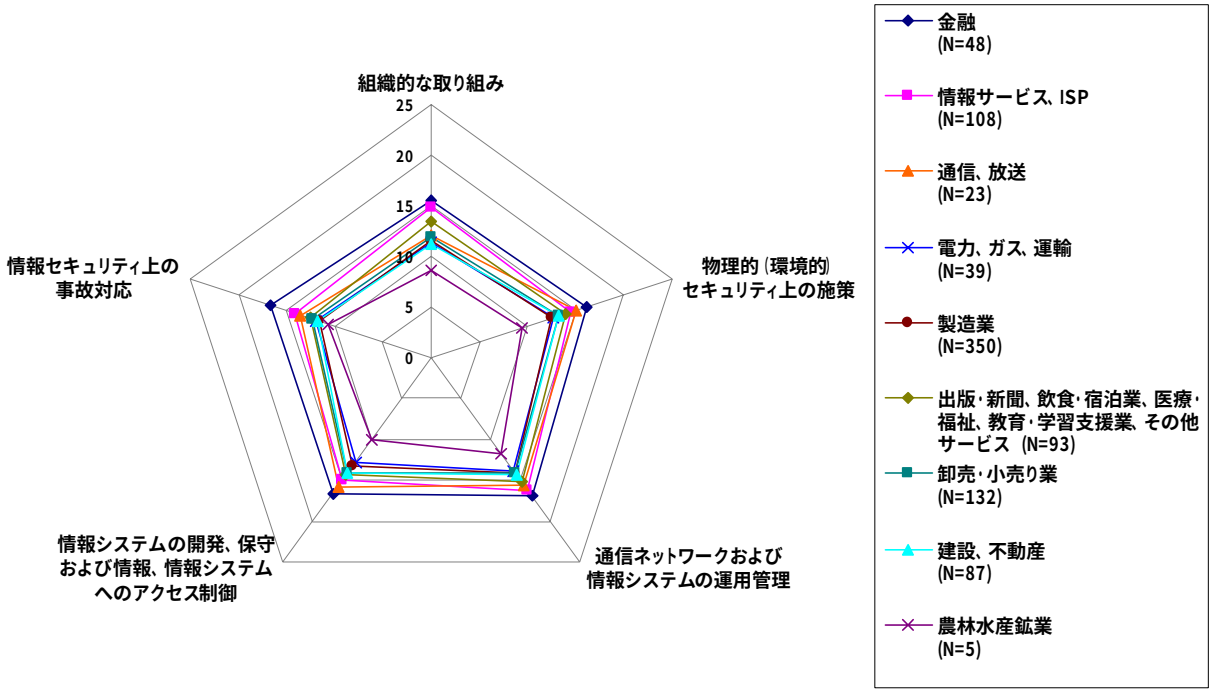
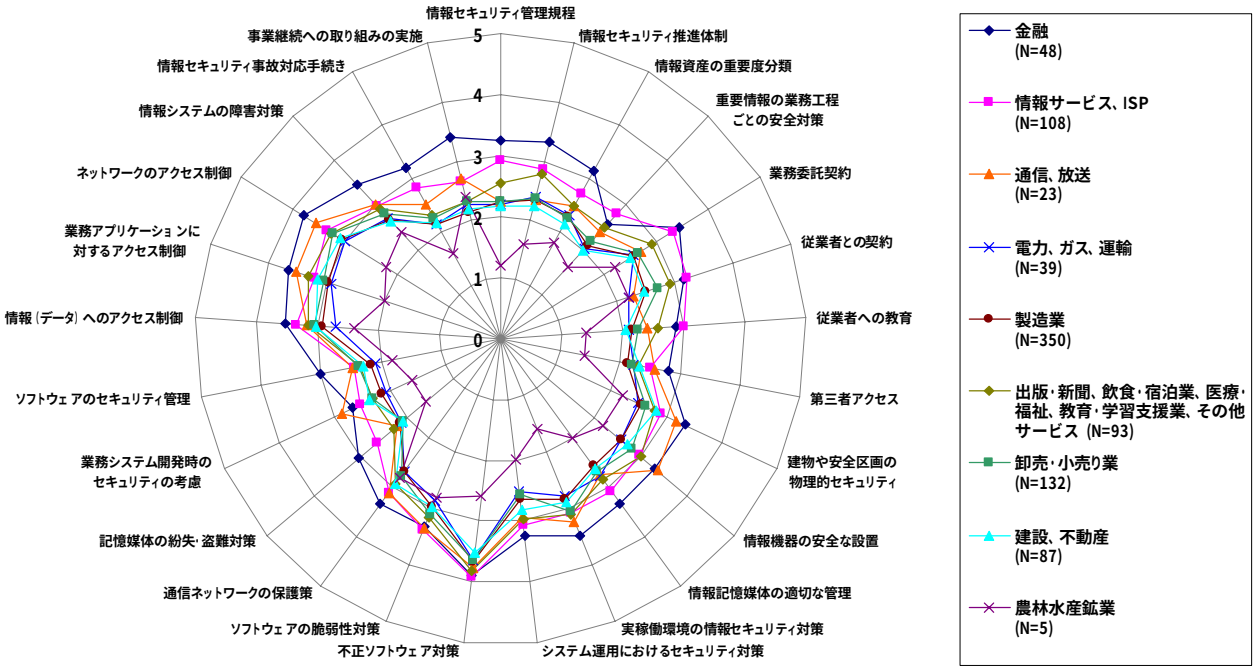


図 １１　小問ごとの業種別平均



【参考３】海外の事例

海外においても、民間機関や政府機関から、情報セキュリティ対策ベンチマークと同様の趣旨のセルフチェック・評価ツールが公表されている。

①アメリカ：ISG (Information Security Governance) Program[3]

民間団体 The National Cyber Security Partnership (NCSP)民間の情報セキュリティレベルを高めるための、経営者レベルの意識改革の観点から、「Information Security Governance　A Call to Action」を 2004 年 4 月発表。企業の情報セキュリティの責任主体を経営レベルとし、また別添資料には CEO が情報セキュリティ環境をどのように評価するのかについての簡易な評価法が附されている。

②イギリス：e-Security Health check[4]

政府機関 DTI（Department of Trade and Industry）が提供するセルフチェックツール。英国の情報セキュリティマネジメント規格である BS7799 をベースに作成した質問項目に回答することにより、企業のステータスを体重計の形式で結果を可視化する。

③フランス：EBIOS[5]（Expression of Needs and Identification of Security Objectives）

フランス政府機関で情報セキュリティを担当する DCSSI (Central Information Systems Security Division)が提供する無料のリスク評価ツール。

[3] ISG (Information Security Governance) :http://www.cyberpartnership.org/init-governance.html
[4] e-Security Health check: http://www.dti-bestpractice-tools.org/healthcheck
[5] EBIOS: http://www.ssi.gouv.fr/en/confidence/methods.html