情報セキュリティ規程体系の効率的な整備事例

片貝 理絵子

A Case of Efficiently Establishing a Set of Information Security Rules

Rieko Katakai

近年, 情報漏えい事件の増加や個人情報保護法の完全施行による法的基盤整備が進むなどの環境の影響から, 従来以上に各企業では情報セキュリティの確立が急務となっている. そうした取り組みの第一歩として, 各企業の情報セキュリティ規程体系の整備が重要である. そこで本論文では, 情報セキュリティ規程体系の効率的な整備を可能にするため, 規程の階層的体系および国際標準規格を効果的に利用した整備事例を紹介する.

It has recently become far more urgent than ever to establish an information security system in each enterprise due to changes in the surrounding environment, such as the advancement of legal infrastructure to cope with the increasing number of incidents of information being leaked and full enforcement of the personal information protection law. As the first step in this effort, it is important to establish a set of information security rules. This paper presents an example of the establishment a set of information security rules by effectively utilizing a hierarchy of information security rules and international standards.

Key Words & Phrases : 情報セキュリティ, ベストプラクティス, ISO/IEC17799, 規程体系, 規程整備
Information security, ISO/IEC 17799, best practice, system of rules, establishment of rules

1. はじめに

近年, 情報漏えい事件の増加や個人情報保護法[1]の完全施行による法的基盤整備が進むなどの環境の影響から, 企業に対して情報セキュリティの確保が社会的に要求されており, 従来以上に各企業では情報セキュリティの確立が急務となっている. また, 企業における情報セキュリティの確立を証明し, 社会的な信頼を獲得するためにISMS認証[2]やプライバシーマーク[3]の取得を目指す企業が増加している.

そうした情報セキュリティを確立し、ISMS認証基準などの国際標準で求められている情報セキュリティレベルを実現するための取り組みの第一歩として, 各企業の情報セキュリティ規程体系の整備が重要である. しかし, 規程体系の整備を行うにあたっては, 2つの課題がある. 1つ目は, ほとんどの企業では既に何らかの関連規程を制定しているため, それらとの整合性をいかにとるかという点である. 2つ目は, 情報セキュリティのベストプラクティスが提唱するセキュリティ・ポリシーを最上位, スタンダードを第2層, ガイドラインを第3層という階層的体系をいかに実現するかという点である. これまでにも, こうした情報セキュリティの規程体系を整備する方法は紹介されているが, 具体的にはどのような方法で効率よく網羅的に整備するかについてはあまり紹介されていない.

本論文では, これらの課題を解決し, 情報セキュリティ規程体系の効率的な整備を可能にするため, 規程の階層的体系および国際標準規格を効果的に利用した整備事例を紹介する.

まず第2章では, 情報セキュリティ対策の実施における規程整備の重要性について明確にする.

次に, 第3章では必要な規程類が策定されているかどうかを確認するためのツールを使って, 新たに策定すべき規程や同じ内容が複数存在する規程を特定し, 各規程の位置づけやレベル, 関連性を記録するための事例を紹介する.

第4章では, 必要な内容が各規程に記載されているかどうか確認するためのツールを使って, 各規程の内容に記載されていなければならない項目, 重複や抜け漏れ, 修正すべき点などがないかどうかを確認するための事例を紹介する.

最後に第5章で, 結論および今後の課題について

提出日 : 2005年08月31日　再提出日 : 2006年3月28日

述べる.

2. 情報セキュリティ対策の実施における規程整備の重要性

より効果的で, 強固な情報セキュリティを確立するためには, PDCAサイクルを継続的に繰り返すことが必要である(**図1**).

PDCAサイクルとは,

- Plan:情報セキュリティ対策の具体的計画・目標を策定する.
- Do:計画に基づいて対策の実施・運用を行う.
- Check:実施した結果の点検・監視を行う.
- Act:経営陣による見直しを行い, 改善・処置する.

であり, PDCAサイクルをまわすことにより, 情報セキュリティレベルの向上を図ることが可能となる.

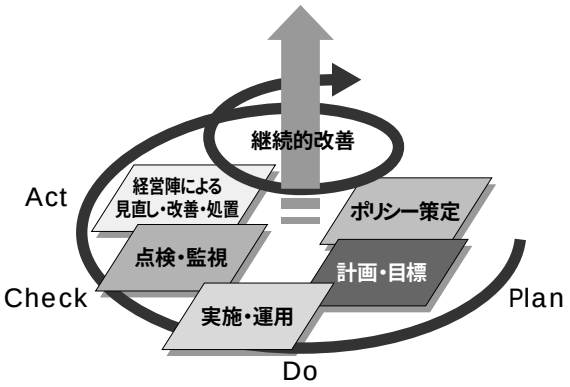

図1. PDCAサイクル[4]

実際に, 全社統一的に適切にPDCAサイクルをまわすためには, 情報セキュリティに対する企業の基本的な方針や取り組みを明確にした情報セキュリティ・ポリシーおよび情報セキュリティ・スタンダードを始め, 手順やガイドラインなどの規程類を策定し, それらに基づいて運営されることが不可欠である.

しかし, これらの規程類が整備されていない場合, 情報セキュリティ対策を実施するための判断基準が不明確となり, 各個人の判断に任せられた対策や局所的な対策などが場当たり的に行われる恐れがある. その結果, 情報セキュリティレベルの高い部分と低い部分の差ができてしまい, 全体的なセキュリティレベルの維持・向上を図ることが困難となり, セキュリティレベルの低い部分がセキュリティホールになりかねない(**図2**).

さらに, ほとんどの企業では既に何らかの関連規程を制定しているため, それらとの整合性をいかにとるかという点が問題となる.

では, 情報セキュリティ対策を実施するための判断

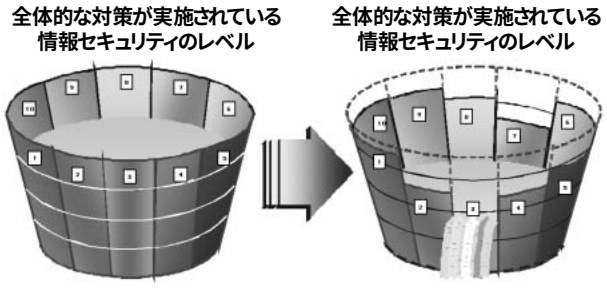

図2. 情報セキュリティのレベルの差[5]

基準となり, 全体的なセキュリティレベルの維持・向上を図るために規程類をどのように整備するべきか.

情報セキュリティの規程類は,

- 目的, 基本的な考え方(原則)などを示した方針書
- 方針に基づく標準的な管理, 運用を示した標準書
- 個別の組織やシステムに合わせた具体的なガイドライン(手順書やマニュアルなど)

の3階層構成で体系的に整備することが重要である(**図3**).

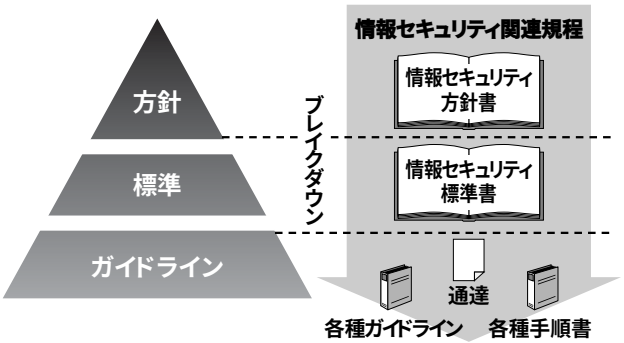

図3. 情報セキュリティ規程体系[6]

また, 規程類の策定にあたっては, 情報セキュリティを確立するためのベストプラクティスであり, ISMSを構築するための要求事項をまとめた国際標準規格であるISO/IEC17799(Information technology - Code of practice for information security management:情報技術ー情報セキュリティマネジメントの実践のための規範)[7]をベースとし, 全体的な情報セキュリティ対策を実施するために, ISO/IEC17799で要求されている10個の管理区分すべてを検討する必要がある(**図4**).

3. ベストプラクティスに基づく規程の特定と各規程のレベルおよび関連性の明確化

最初に, 必要な規程類が策定されているかどうかを確認するためのツールを使って, 規程のあるべき姿を第1層(上位層)から第3層(下位層)まで分類し,

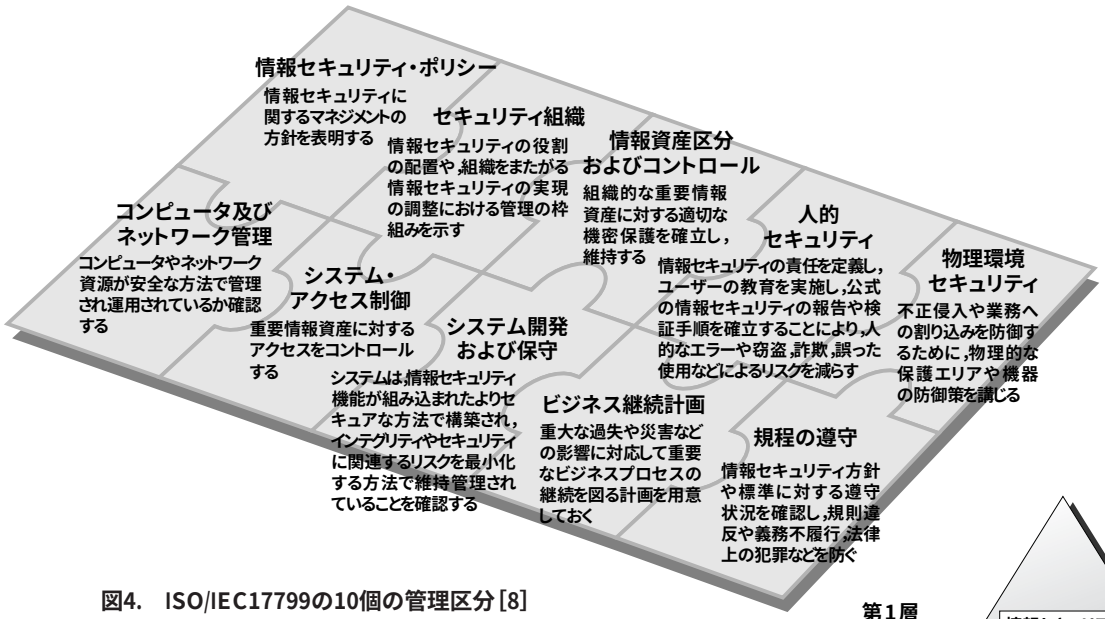

図4.　ISO/IEC17799の10個の管理区分[8]

既存規程を分類する.

図3でも示したように, 規程体系の各階層は以下のように定義されている.

- **第1層：方針**

経営理念に準拠した, 全社としての情報セキュリティの方針を定めたもの.

（例）情報セキュリティ・ポリシー

- **第2層：標準**

方針を具現化し, 全社共通の標準を定めたもの.

（例）情報セキュリティ・スタンダード

- **第3層：ガイドライン**

方針や標準から, 実際に情報資産を管理／利用する際の詳細な実施手順を作成するための全社共通の基本的なプロセスを定めたもの.

（例）マニュアル, 手順書, 運用細則

上記の定義をもとに, それぞれの既存の規程がどの階層に該当するか, 内容を確認し, 分類する（**図5**）. その結果, どの階層にどのような規程が存在しているか, また策定が必要な階層の規程は何なのかを階層ごとに把握することができる.

次に, 各階層に分類されたそれぞれの規程を, 図4で示したISO/IEC17799で要求されている10個の管理区分のうち, どの管理区分に当てはまるか検討する.

10個の各管理区分について, 関連する規程の例を以下に示す.

- 管理区分1：情報セキュリティ基本方針
  （例）情報セキュリティ・ポリシー
- 管理区分2：組織のセキュリティ
  （例）組織規則, 外部委託管理規程
- 管理区分3：資産の分類および管理
  （例）文書管理規程, 営業秘密管理規程

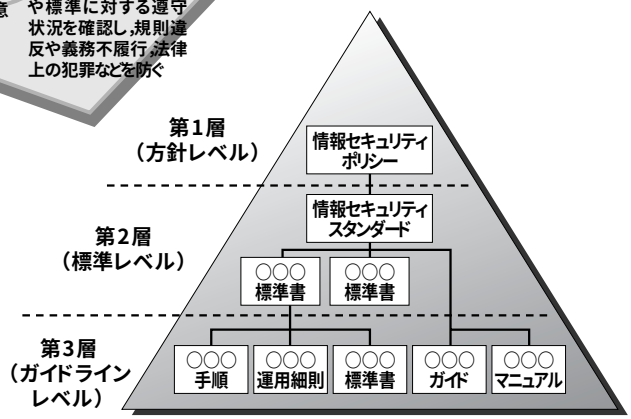

図5.　階層ごとの分類

- 管理区分4：人的セキュリティ
  （例）就業規則, 職務規程
- 管理区分5：物理的および環境的セキュリティ
  （例）入退館管理規程
- 管理区分6：通信および運用管理
  （例）コンピュータ利用規程, システム運用管理規程
- 管理区分7：アクセス制御
  （例）システム運用管理規程, ユーザ・マニュアル
- 管理区分8：システムの開発および保守
  （例）開発業務管理規程
- 管理区分9：事業継続管理
  （例）危機管理マニュアル, 緊急対策規程
- 管理区分10：適合性
  （例）個人情報保護規程, コンプライアンスマニュアル, 監査規程

上記の例をもとに, それぞれの既存の規程がどの管理区分に該当するか, 内容を確認し, 分類する. また, 規程によっては記載内容が重複していたり, 複数の管理区分に該当していたりする場合がある. そのため, 各規程の該当箇所と関連をツリー図で表すことによって明確にし, どの管理区分の規程が存在しているか, 関連する規程はどれか, また新たに策定が必要な管理区分の規程は何なのかを特定する（**図6**）.

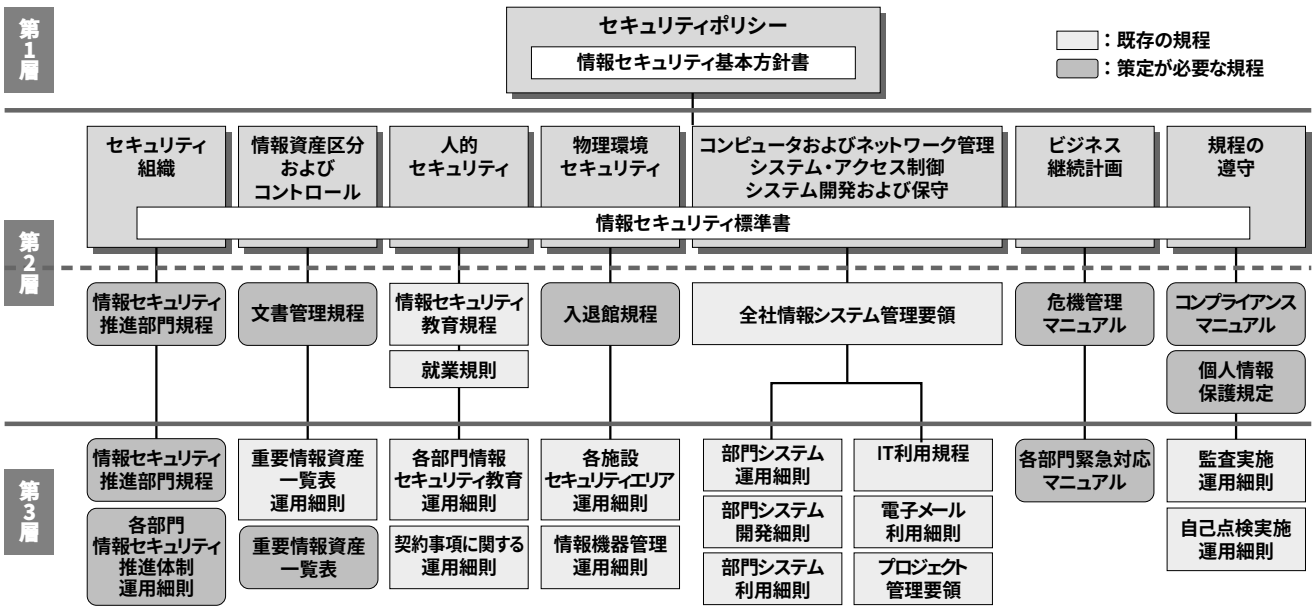

図6.　管理区分ごとの分類（ある事例での適用例）

以上の手法で, 第1層から第3層までの規程階層を縦軸とし, 10個の管理区分を横軸とすることにより, ベストプラクティスに基づく階層的体系から見た規程の特定と各規程の位置づけやレベル, 関連性を明確に把握することが可能となる.

4. ベストプラクティスに基づく規定すべき項目の特定および文書化

各規程の把握が終わったら, 次は必要な内容が各規程に記載されているかどうかを確認するためのツールを使って, 規定すべき項目ごとに既存規程の内容を分解してマッピングすることにより, 各規程の内容に記載されていなければならない項目を確認し, 見直しを行う.

ISO/IEC17799の10個それぞれの管理区分における管理すべき項目は, さらに詳しく36の中項目および127の小項目に分けられ, 詳細管理策として要求されている. 例えば, 管理区分1の「情報セキュリティ基本方針」では, 中項目として,

- 情報セキュリティ基本方針文書
- 見直しおよび評価

がある. さらに,「情報セキュリティ基本方針文書」には,

- 経営陣の責任を明記し, 情報セキュリティの管理に対する取り組み方法を明示した基本方針文書が, 経営陣によって承認され発行されていること
- 標準およびガイドラインは, 方針を展開して, 作成され, 業務に使用されていること
- 基本方針文書は, 利用可能で, かつ理解しやすい形で, 組織全体にわたって利用者に知らせること

の3つの小項目があり,「見直しおよび評価」には,

- 定められた手続きに従って基本方針の維持および見直しに責任を持つものを任命し, 記録されたセキュリティの事件・事故の性質, 回数および影響によって示される基本方針の有効性, 事業効率, 技術変更などについて, 日程を定め, 定期的に見直しを実施すること

の1つの小項目がある.

これらの詳細管理策は, それぞれの管理区分においてどのような対策をとるべきか判断する基準として具体的に記載されており, これらはセキュリティ対策を実施するための項目として, 規程に織り込まれていなければならない.

そこで, これらの詳細管理策を縦軸とし, それぞれの既存規程を横軸とした対応表を作成して, それぞれの内容がどの詳細管理策の項目に該当するかを確認し, マッピングする（**表1**）.

これにより, それぞれの既存規程の記載内容と詳細管理策で要求されている対策のあるべき姿とを比較して, ギャップを容易に見つけることができると同時に, 内容に記載されていなければならない項目が織り込まれているかどうか, また, 記載内容に重複や抜け漏れ, 修正すべき点がないかどうかを効率的に確認することが可能となる.

さらに, 新たに作成すべき規程についても, この手法を使うことにより, 規程の内容に記載すべき詳細管理策の項目をチェックし, 最終的な規程体系の各構成要素である各規程に織り込むべき内容の特定を容易に行うことができる.

最後に, それぞれの規程に具体的に織り込むべき内容の既存規程への項目追加やその内容に沿った

表1.　詳細管理策と各規程の対応表の例（一部抜粋）
既存規程の内容と詳細管理策の項目をマッピングして，必要事項の抜けがないかを確認する．

			情報セキュリティ・ポリシー	組織規則	外部委託管理規程	文書管理規程	職務規程	コンプライアンスマニュアル	個人情報保護規程	
1. 情報セキュリティ基本方針										
1(1) 情報セキュリティ方針										
1(1)①	情報セキュリティ基本方針文書	基本方針文書は，経営者によって承認され，適当な手段で，全従業員に公表し，通知すること	○（第1章）							
1(1)②	見直しおよび評価	基本方針は，依然として適切であることを確実にするために，定期的に，また影響を及ぼす変化があった場合に，見直すこと	○（第10章）		○（第8章）			○（第10章）	○（第10章）	
2. 組織のセキュリティ										
2(1) 情報セキュリティ基盤										
2(1)①	情報セキュリティ運営委員会	セキュリティを主導するための明りょうな方向付けおよび経営者による目に見える形での支持を確実にするために，運営委員会を設置すること．運営委員会は，適切な責任分担および十分な資源配分によって，セキュリティを促進すること	○（第2章）	○（第3章）			○（第2章）	○（第2章）	○（第2章）	
2(1)②	情報セキュリティの調整	大きな組織では，情報セキュリティの管理対策の実施を調整するために，組織の関連部門から管理者の代表を集めた委員会を設置すること		○（第4章）						
2(1)③	情報セキュリティ責任の割当て	個々の資産の保護に対する責任および特定のセキュリティ手続きの実施に対する責任を，明確に定めること		○（第4章）	○（第2章）		○（第3章）	○（第4章）	○（第4章）	
2(1)④	情報処理設備の認可手続	新しい情報処理設備に対する経営陣による認可手続を確立すること								
2(1)⑤	専門家による情報セキュリティの助言	専門家による情報セキュリティの助言を内部又は外部の助言者から求め，組織全体を調整すること		○（第7章）						
2(1)⑥	組織間の協力	行政機関，規制機関，情報サービス提供者および通信事業者との適切な関係を維持すること	○（第3章）	○（第8章）	○（第5章）			○（第5章）	○（第5章）	
2(1)⑦	情報セキュリティの他者によるレビュー	情報セキュリティ基本方針の実施を，他者がレビューすること								

表2.　規程の修正と文書化の例（一部抜粋）
既存規程の内容と該当する詳細管理策の内容とを対比して，追加・修正を行う．

IT利用者規程（現行）		IT利用者規程（改訂後）		ISO17799該当箇所	
PC等情報機器の管理について					
3. 記憶媒体の使用方法	フロッピーディスクやその他の記憶媒体（MO，CD-ROMなど）の使用は禁止とする．業務上やむをえず，外部からの持込み，外部への持出しを行わなければならない場合は，「記憶媒体の管理手続き」に基づいて所定の手続きを行うこと．	3. 記憶媒体の使用方法	（修正） フロッピーディスクやその他の記憶媒体（MO，CD-ROMなど）の使用は原則禁止とする． 業務上やむをえず，外部からの持込み，外部への持出しを行わなければならない場合は，「記憶媒体の管理手続き」に基づいて所定の手続きを行うこと． （追加） ただし，保管を目的とした外部への持出しについては，情報システム部へ申請し，承認を受けること． 〈業務上やむをえない外部からの持込み，外部への持出しの例〉 ・ 顧客や契約先などとの契約において，記録媒体の持込み，持出しを行うことが定められている場合．	8.6.3 情報の取扱手順	認可されていない露呈又は誤用から情報を保護するために，情報の取扱いおよび保管についての手順を確立すること． (1) 情報の取扱い手順は，文書，計算処理システム，ネットワーク，移動型計算処理（mobile computing），移動通信，メール，音声メール，一般の音声通信，マルチメディア，郵便サービス・施設，ファクシミリの使用，他の取扱いに慎重を要するものすべて（例えば，未使用の小切手，送り状）について，その情報の分類に対応させて策定すること． (2) 情報の取扱い手順の策定においては，すべての媒体の取扱いおよびラベル付けについて考慮すること． (3) 情報の取扱い手順の策定においては，認可されていない者を識別するためのアクセス制限について考慮すること． (4) ・・・・・・
8. その他	① 端末（PC） 各社員は業務開始時に電源を投入し，業務終了後に電源を切断する． ノート型PCは，業務終了後に机やキャビネットなどの施錠可能な場所に保管する．ただし，セキュリティ用ワイヤーで机に固定するなど，容易に持ち出せないような対策が講じられているものは除く． ② プリンタ 最初の使用者が電源を投入し，最後に退出する者が電源を切断する． 印刷した紙は放置せず，速やかに取り出すこと． トナーの交換作業は各部署単位で行う．	8. その他	（追加） ① 端末（PC） ・・・講じられているものは除く． 情報を表示する端末の画面は，容易に見られない位置に設置する．	7.3.1 クリアデスクおよびクリアスクリーンの個別方針	組織は，情報への認可されていないアクセス，情報の消失および損傷のリスクを軽減するための，クリアデスク方針およびクリアスクリーン方針を持つこと． (4) ・・・・・・ (5) パーソナルコンピュータ，コンピュータ端末および印字装置は，ログオン状態で離席しないこと (6) パーソナルコンピュータ，コンピュータ端末および印字装置は，使用しないときは，施錠，パスワード又は他の管理策によって保護すること (7) ・・・・・・

修正, また新規規程の作成など, 実際に文書化する(**表2**).

以上の方法により, 規程体系の整備が効率的に実現でき,「既存の規程との整合性をいかにとるか」と「規程の階層的体系をいかに実現するか」という2つの課題を解決することができる.

これまでいくつかのクライアントに適用した結果, 企業の規模や環境, 条件などによりその期間は異なるものの, ベストプラクティスで要求している項目を網羅的に織り込んだ情報セキュリティ規程体系を, これまでの2分の1から3分の1の期間(平均2〜3か月)で整備することが可能となり, 本手法の有効性を示すことができた. 今後もお客様の抱える課題を解決するため, お客様にとって価値のある効率的な事例を, 今後の提案やプロジェクトワークに生かしていく予定である.

5. おわりに

本論文では, 情報セキュリティの3階層体系、ISO/IEC17799の10個の管理区分および詳細管理策の分類を利用し、既存規程を効率的かつ短期間で整備する事例を紹介した.

企業の中に存在する膨大な数の規程を整備するには, 想像以上の手間と時間を必要とする. さらに, 規程整備だけでなく, インフラ整備やシステム環境の強化, 社員への教育, 事業継続計画など, 情報セキュリティにおける企業が取り組むべき問題は多岐にわたっている. まずは, それらの取り組みの基準となり手順となる規程を整備して, 情報セキュリティにおける方針や取り組みの基盤を作り, 取り組むべき問題を計画的に解決することが情報セキュリティ確立の早期実現につながる.

今後の課題は, PDCAサイクルの観点から整備した規程が形骸化しないようにどのように維持し, 見直していくか, また, 策定した規程をどのように社員に周知・徹底させるか, 規程に沿った効果的な教育をどのように行っていくかなどが課題となる.

謝辞

本論文を執筆するにあたって, 課題を検討するきっかけとなったいくつかのプロジェクトに参画したほか, 現在のプロジェクトマネージャである長谷容子さんを始め, これまでのプロジェクトでご一緒させていただいた多くの方々より多数の助言をいただきました. あらためて深謝いたします.

参考文献

[1] 個人情報の保護に関する法律, http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html
[2] ISMS : Information Security Management System (情報セキュリティマネジメントシステム)適合性評価制度, http://www.isms.jipdec.jp/
[3] プライバシーマーク : 個人情報保護に関するコンプライアンス・プログラムの要求事項(JIS Q 15001), http://privacymark.jp/
[4] PDCAサイクル, http://www.isms.jipdec.jp/isms/index.html
[5]「経営戦略としての情報セキュリティ」p100, 大木栄二郎著, 工業調査会(出版), 2001年7月
[6] 荒木吉雄,「プライバシー保護とCPOの役割」ProVISION No.42, p18, 2002年6月
[7] ISO/IEC17799 : Information technology - Security techniques - Code of practice for Information security management
[8]「経営戦略としての情報セキュリティ」p167, 大木栄二郎著, 工業調査会(出版), 2001年7月

アイ・ビー・エム ビジネスコンサルティング サービス株式会社
アプリケーション・イノベーション
セキュリティ・ソリューション・コンサルティング
コンサルタント

片貝 理絵子 Rieko Katakai

[プロフィール]
1999年、IBCSに入社。2003年よりセキュリティーコンサルタントとして、金融業・製造業・流通業における情報セキュリティー構築やISMS構築支援、個人情報保護プロジェクトなどに参画し、セキュリティー／プライバシー・アセスメントおよび各種規定策定等を担当。
LC079650@jp.ibm.com