特定非営利活動法人
SAAJ 日本システム監査人協会報

(特集) 個人情報保護マネジメントシステム(PMS)の監査について

－JIS Q 15001：2006対応

No.7081 一村 義夫

1.はじめに

財団法人日本情報処理開発協会のプライバシーマーク制度がスタートしたのは、1998年でした。そのときの審査基準は、通産省告示「民間における電子計算機処理に係る個人情報保護に関するガイドライン」でした。これが、翌年の1999年、JIS Q 15001に切り替わり、そして7年ぶり、2006年5月20日、改正されました。

2006年7月11日現在、プライバシーマークの使用を許諾されている事業者は、4,580社に上ります。これだけの事業者が今後、旧JIS準拠の「個人情報保護に関するコンプライアンス・プログラム」から新JIS準拠の「個人情報保護マネジメントシステム」に切り替えることになります。切り替えに許される期間として、財団法人日本情報処理開発協会は、経過措置期間(2006年5月20日～2006年11月19日)及び移行措置期間(経過措置期間後から2年間)を設けました。

さて、この4,580に上る事業者の個人情報保護監査責任者(以下、監査責任者という)は、自社の新JIS準拠の「個人情報保護マネジメントシステム」移行にどう対応すればよいでしょうか。本稿が、この4,580に上る事業者の監査責任者及び新規に新JIS準拠のプライバシーマーク付与申請を予定する事業者の監査責任者の一助となれば幸いです。

2.監査責任者の責任及び権限に変更はない

旧JISでは、監査が個人情報保護に関するコンプライアンス・プログラムのPDCAのCプロセスそのものとして位置づけられていました。新JISでは、監査が点検の一部に位置づけされました。監査と並ぶもうひとつの点検が、各部門及び各階層の管理者による日常業務における定期的なマネジメントシステムの運用の確認です。しかし、これは、監査の重要性が薄まったことを意味しません。新JISになっても監査責任者の責任及び権限にいささかの変更はありません。

3.既プライバシーマーク認定事業者の監査責任者に求められる新JIS対応作業

監査責任者の実務は、【図1】のとおりですが、既プライバシーマーク認定事業者の監査責任者は、【図1】の「2．監査を計画する」のプロセスにおいて新JIS対応作業が発生します。具体的には、以下の①～③の作業であり、次項以降で説明します。勿論、これから新JISでプライバシーマー

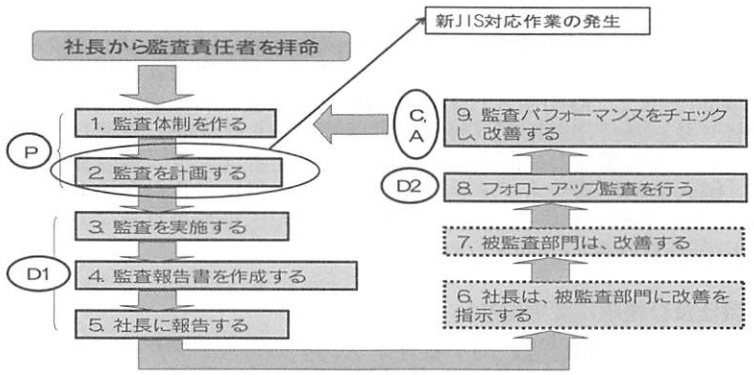
目 次

ク付与申請を予定する事業者の監査責任者は、【図１】に示す全プロセスを監査責任者の責任及び権限に基づき遂行することになります。しかし、本稿では、紙幅の都合により、全プロセスの説明を割愛します。

① 監査実施時期の見直し
② 確立した個人情報保護マネジメントシステムの新JISへの適合状況を監査するためのチェックリスト（以下、適合性監査チェックリストという）の作成
③ 確立した個人情報保護マネジメントシステムの運用状況を監査するためのチェックリスト（以下、運用監査チェックリストという）の作成

４．監査実施時期を見直す

監査責任者は、新JIS移行の責任者に自社の移行計画を確認します。新JIS準拠の個人情報保護マネジメントシステムの確立と実施が本年度中に行われる場合は、本年度の監査実施時期を見直すことになります。監査実施時期の設定に当たっては、個人情報保護マネジメントシステムの確立時期、実施・運用期間が少なくとも1ヶ月経過する時期、及び更新申請時期を見定めることがポイントになります。移行措置期間内であれば、更新申請可能期間（従来、更新申請可能期間は、有効期限の４ヶ月前から３ヶ月前までの間）に関係なく前倒しして更新申請をすることができますので、会社として前倒しで更新申請をする場合は、監査も前倒しで実施することになります。



【図1】監査責任者の実務と新JISへの対応作業

５．監査の内容は変わらないが、監査基準が変わる

監査の内容について、旧JISでは「事業者は、コンプライアンス・プログラムがこの規格の要求事項と合致していること、及びその運用状況を定期的に監査しなければならない。」（１）とあります。新JISでは「事業者は、個人情報保護マネジメントシステムのこの規格への適合状況及び個人情報保護マネジメントシステムの運用状況を定期的に監査しなければならない。」（２）とあります。「コンプライアンス・プログラム」から「個人情報保護マネジメントシステム」への名称変更のほか文言の多少の変更はあるものの、監査の内容は変わりません。しかし、適合状況の監査基準は、旧JISから新JISに変わり、運用状況の監査基準は、自社のコンプライアンス・プログラム（旧JIS準拠）から自社の個人情報保護マネジメントシステム（新JIS準拠）に変わります。新JISに対応する監査を整理すると、【表1】のようになります。従って、監査責任者は、監査チェックリストを新JISに対応するよう、改定することが必要になります。

【表1】監査テーマ、監査の内容、監査基準及び監査対象

項番	監査テーマ	監査の内容	監査基準	監査対象
1	適合性監査	自社の個人情報保護マネジメントシステムのJIS Q15001:2006などへの適合状況	JIS Q 15001:2006などの個人情報保護マネジメントシステム要求事項	自社の個人情報保護マネジメントシステム文書（記録除く）
2	運用監査	自社の個人情報保護マネジメントシステムの運用状況 ・体制整備状況 ・運用状況 ・個人情報保護マネジメントシステムの見直し状況	自社の個人情報保護マネジメントシステム 監査基準が変わる	1. コーポレートレベルの体制整備状況 2. 各部門及び各階層の体制整備状況、運用状況 3. 個人情報保護マネジメントシステムの見直し状況

6. 新JISに対応する適合性監査チェックリストの作成

適合性監査のチェックリスト例を【表2】に示します。このチェックリストは、監査業務の一貫性や記録性を高めるため、監査項目ごとにチェック内容、確認方法、確認対象、使用する様式、評価、指摘事項、改善事項、及びフォローアップ監査結果までの一連の監査結果を、通しで記載できる様式にしています。また、財団法人日本情報処理開発協会などにプライバシーマークの付与申請をするとき、個人情報保護マネジメントシステムの要求事項（新JISや新JISに準拠した業界ガイドライン）に対応する自社の個人情報保護マネジメントシステム文書（記録を除く）の規程の名称と項番を整理した書類を提出し、審査を受けますが、適合性監査は、これに近いものと考えることができます。従って、このチェックリストは、申請書類作成時に活用することができますので、好都合です。

【表2】の適合性監査チェックリストの表頭の①～⑫の各項目に関する説明を【表3】に示します。

監査責任者は、【表2】と【表3】を参考にして、新JISに対応する適合性監査チェックリストを作成することができます。

7. 新JISに対応する運用監査チェックリストの作成

改めて言うまでもなく、立派な個人情報保護マネジメントシステム文書（記録を除く）が存在していても実施･運用されていなければ個人情報保護マネジメントシステムのPDCAサイクルが回っているとは言えません。運用監査は、そうならないように、実施・運用記録を取り寄せたり、現場に出向いて現物を確認したりし、問題があれば、指摘し、個人情報保護マネジメントシステムの改善につなげる役割を担います。

運用監査のチェックリスト例を【表4】に示します。このチェックリストは、適合性監査チェックリストと同様に、監査業務の一貫性や記録性を高めるため、監査項目ごとにチェック内容、確認方法、確認対象、評価、指摘事項、改善事項、及びフォローアップ監査までの一連の監査結果を、通しで記載できる様式にしています。適合性監査チェックリストと比べると一見同じように見えますが、事実上、同じではありません。これは、監査基準の違いから来るものです。即ち、運用状況の監査項目は、JIS Q 15001：2006の要求事項ではなく、あくまで自社の個人情報保護マネジメントシステムに基づき設定されるためです。特定した個人情報について、その取扱いの各局面におけるリスクを認識し、分析し、その結果、講ずることとしたリスク対策が監査項目になります。

従って、この監査項目によるチェックを効率的に行うためには、【表5】の運用監査チェックリストの表頭の①～⑫の各項目に関する説明を理解する必要があります。

監査責任者は、【表4】と【表5】を参考にして、運用監査チェックリストを作成することができます。

【表5】の項番⑨の評価で、リスク分析の結果、講ずることとしたリスク対策（安全管理措置）の内容が適切か否かをチェックし、評価する際、以下のことに留意する必要があります。

・プライバシーマーク審査における安全管理措置の事実上の審査基準

JIS Q 15001：2006などの個人情報保護マネジメントシステムの要求事項では、安全管理措置について何をどのレベルまでやりなさいということまで具体的に要求していません。安全管理措置は、自社が保有する個人情報のそれぞれについて、リスクを認識し、分析し、その結果に基づき決定されます。しかし、財団法人日本情報処理開発協会やプライバシーマーク付与認定指定機関が行う審査では、マスコミ等で大きく報道された個人情報漏洩事故・事件で他の企業でも十分に起こりうるリスクについて、事故・事件の再発防止の観点から具体的な安全管理措置、例えば、ウイルス対策ソフトの実装やWebによる個人情報取得時の暗号化などを要求しています。すなわち、これらの安全管理措置は、事実上の審査基準となっています。セキュリティを巡る社会状況の悪化傾向が益々強まる中、こういった事実上の審査基準は、恐らく、増えこそすれ、減ることはないと思われます。一方、経済産業省の『個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン』ほか各主務官庁のガイドラインは、主務大臣が法を執行する際の基準である旨、明言していますので、ガイドラインに具体的に明示されている安全管理措置についても、最低限の安全管理措置として認識せざるを得ないように思います。

・プライバシーマーク審査を前提にした自社の安全管理措置の監査

上記のような状況を考慮すると、リスク分析の結果、講ずることとした安全管理措置が十分かどうかを評価する際、財団法人日本情報処理開発協会やプライバシーマーク付与認定指定機関が要求する安全管理措置や所管官庁のガイドラインが示す安全管理措置を自社の監査基準とみ

なし、自社が講じている安全管理措置の妥当性を評価することは、監査責任者としてのひとつの見識だと思います。すなわち、仮に自社でそのような安全管理措置を講じていない場合があるとき、「該当するリスクは、本当にないのか、見落としていないか、リスクの認識が甘くないか、或いはリスク対策としての安全管理措置が不足していないか」といった観点から、自社が講じている安全管理措置を評価することができます。

【表2】新JISに対応する適合性監査チェックリスト（1／2）

チェックリスト例1　適合性監査チェクリスト

監査責任者 ⇄ 監査人

適合性監査チェックリスト

■被監査部門：プライバシーマーク取得プロジェクトまたは規程所管部署
■予備調査実施日：
■本調査実施日：
■フォローアップ監査実施日：

表頭	項番	タイトル	監査項目	チェック内容	確認方法		(→続く)
					規程等	現地	
	①	②	③	④	⑤	⑥	
	‥						
	3.3.3	リスクなどの認識、分析及び対策[3]	‥‥‥‥	1）対応する規程はあるか	○		
				2）目的外利用防止の対策手順はあるか	○		
				3）リスク認識、リスク分析、リスク対策、残存リスク管理の手順はあるか	○		

【表2】新JISに対応する適合性監査チェックリスト（2／2）

(→続き)	確認対象	使用する様式	評価	指摘事項	改善事項	フォローアップ結果
	⑦	⑧	⑨	⑩	⑪	⑫
	1）個人情報保護規程xx条リスク分析	―	○	なし	なし	―
	2）目的外利用防止に関する細則	様式x目的外利用申請書	○	なし	なし	―
	3）リスク分析に関する細則	様式yリスク分析兼リスク対策表	○	なし	なし	―

【表３】新JISに対応する適合性監査チェックリストの各項目に関する説明

表頭の項番	表頭の項目名	項　目　の　説　明
①	項番	個人情報保護マネジメントシステム要求事項（JIS Q 15001:2006）の章、節、項、小項の項番を順に記入します。
②	タイトル	章、節、項、小項のタイトルを記入します
③	監査項目	章、節、項、小項の本文をそのまま記入します
④	チェック内容	要求事項を基に、対応する個人情報保護マネジメントシステム文書（記録を除く文書）があるかどうかを確認するために「・・・はあるか」という具合に作成しますが、複数に分解する場合があります。 ＊適合性監査の監査基準は、個人情報保護マネジメントシステム要求事項（JIS　Q15001:2006など）です。監査の対象は、自社の個人情報保護マネジメントシステム文書（記録を除く）です。従って、監査人は、ひとつひとつの要求事項について、要求事項の内容のすべてが自社の個人情報保護マネジメントシステム文書に反映されているかどうかをチェックします。
⑤⑥	確認方法	監査人は、予備調査で規程等をチェックしますが、不明点は、現地で確認します。 ⑤規程等：項番④のチェック内容と自社の個人情報保護マネジメントシステム文書(記録を除く)を突き合わせることにより要求事項に対応する規程があるか確認します。 ⑥現地：不明点について、に説明を求めます。
⑦	確認対象	項番④のチェック内容に対応する自社の個人情報保護マネジメントシステムの規程の名称と項番を上位規程から下位の手順まで階層的に記入し、監査人は、該当する規程本文を確認していきます。 ＊確認対象の記入は、予備調査に間に合うよう、被監査部門に依頼する方法を勧めます。監査人が、予備調査時に、個人情報保護マネジメント文書（記録を除く）の名称と項番を調査して記入する方法もありますが、効率的ではありません。
⑧	使用する様式	項番⑦の規程、手順で様式類、文書の雛形（例えば、通知文など）を規定していれば、それを記入します。記入は、項番⑦に同じく、被監査部門に依頼します。
⑨	評価	項番①～⑧によりチェックした結果を○、△、×の３段階で評価します。△と×の場合は、⑩指摘事項及び⑪改善事項を記入します。 ○（適合）：要求事項に対応する自社の規程が明確にある。 △（適合でも不適合でもない）：要求事項に対応する自社の規程があるが問題がある。 ×（不適合）：要求事項に対応する自社の規程が欠落している。
⑩	指摘事項	問題として把握したことを指摘事項にします。 ＊　必要に応じ、詳細を別紙に添付し、参照する資料番号を記入します。
⑪	改善事項	監査人としての改善勧告内容を、上記指摘事項に対する改善事項として記入します。 ＊　必要に応じ、詳細を別紙に添付し、参照する資料番号を記入します。
⑫	フォローアップ結果	フォローアップ監査を行ったときの結果を○、△、×の３段階で評価します。 ＊　評価は、項番⑨に同じ。監査人は、是正及び予防処置の結果を確認し評価します。 是正及び予防処置を別紙に添付し、参照する資料番号を記入します。

【表４】新JISに対応する運用監査チェックリスト（１／４）

チェックリスト例2　運用監査チェックリスト

運用監査チェックリスト

監査責任者 ← → 監査人

■被監査部門：関東市場販売促進部
■監査対象：顧客データベース管理業務
■予備調査実施日：
■本調査実施日：
■フォローアップ監査実施日：

表頭	項番	タイトル	監査項目	チェック内容	確認方法 記録	確認方法 文書	確認方法 現地	確認対象
	①	②	③	④	⑤	⑥	⑦	⑧
	3.3.3	リスクなどの認識、分析及び対策〔3〕	……	1）目的外利用はないか			ヒアリング	
				2）目的外利用申請は、適切に運用されているか	○		○	様式x目的外利用申請書
				3）リスク分析は行っているか、内容は適切か	○		○	様式yリスク分析兼リスク対策表

（→2/4に続く）

【表４】新JISに対応する運用監査チェックリスト（２／４）

（→1/4の続き）

評価	指摘事項	改善事項	フォローアップ結果
⑨	⑩	⑪	⑫
○	なし	なし	－
該当なし	－	－	－
△	3)-1複写作業のリスク分析が抜けている	a. リスク分析表兼リスク対策表に追加、 b. 取扱規定に安全対策措置を追加、 c. 作業担当者にbを周知	○
	3)-2不正アクセス対策として、アクセスログの点検が抜けている	a. リスク分析表兼リスク対策表に追加、 b. 取扱規定に追加、 c. 作業担当者にbを周知	○

【表４】新JISに対応する運用監査チェックリスト（３／４）

（→4/4に続く）

項番	タイトル	監査項目	チェック内容	確認方法 記録	確認方法 文書	確認方法 現地	確認対象
①	②	③	④	⑤	⑥	⑦	⑧
3.4.3.2	安全管理措置〔4〕	……	取得に関する安全対策を遵守しているか				
			…．				
			利用に関する安全対策を遵守しているか	○		○	イ）アカウント発行、更新、削除記録、 ロ）作業担当者にヒアリング、 ハ）アクセスログ、 ニ）アクセスログ点検記録　他
			…．				
			廃棄・消去に関する安全対策を遵守しているか				

【表４】新JISに対応する運用監査チェックリスト（４／４）

（→3/4の続き）

評価	指摘事項	改善事項	フォローアップ結果
⑨	⑩	⑪	⑫
×	イ）削除記録を保存していない、 ロ）指摘なし、 ハ）指摘なし、 ニ）管理者、作業担当者ともアクセスログを点検していない	イ）保存期限を設定。取扱規定に追加し、作業担当者に周知、 ニ）点検確認表を作成し、再周知	○

【表５】新JISに対応する運用監査チェックリストの各項目に関する説明

表頭の項番	表頭の項目名	項　目　の　説　明
①	項番	個人情報保護マネジメントシステム要求事項（JIS Q 15001:2006）の章、節、項、小項の項番を順に記入する ＊適合性監査チェックリストをコピーし、運用監査に関係のない項番は、除外します。
②	タイトル	章、節、項、小項のタイトル
③	監査項目	章、節、項、小項の本文
④	チェック内容	適合性監査チェックリストの項番⑦の規程名称と項番を頼りに、自社の個人情報保護マネジメントシステムを基に運用面を確認するために「・・・しているか」という具合に作成しますが、複数に分解する場合があります。運用監査の主な対象は、特定した個人情報の取扱規程（リスク対策含む）及びそれらの運用状況と管理体制の整備状況です。 ＊運用監査の基準は、自社の個人情報保護マネジメントシステム文書（記録を除く）ですが、リスク対策のチェック内容の作成方法は、他と少し異なります。個人情報の取扱局面ごとにリスク対策を講ずることとしていますが、個人情報が異なれば、取扱局面及びリスク対策の内容は、原則として同じではありません。しかし、個人情報ごとにチェック内容を詳細に作成する作業は、現実的ではありません。運用監査チェックリスト記入例にあるように、「利用に関する安全対策を遵守しているか」という具合に、せいぜい、取扱局面ごとに作成し、実際のチェック時は、当該個人情報に関するリスク分析兼リスク対策表や個人情報取扱規程で規定した具体的なリスク対策のひとつひとつがチェック内容になります。
⑤⑥⑦	確認方法	項番④のチェック内容とそれに対応する運用記録などとを突合せ、確認します。具体的なリスク対策を規定した、リスク分析兼リスク対策表や個人情報取扱規程を傍らにおいて、ひとつひとつのリスク対策の遵守状況をチェックすることになります。予備調査でサンプル的にチェックし、本調査に備えることもありますが、運用監査は、現地での本調査が中心になります。
⑧	確認対象	監査人が確認する対象を具体的に記入します。 ・記録：記録の名称 ・文書（記録を除く）：文書の名称 ・現地：現物及び運用の実際　（入退室や鍵の管理状況、ウイルス対策ソフトの実装など）
⑨	評価	項番①～⑧によりチェックした結果を○、△、×の３段階で評価します。△と×の場合は、⑩指摘事項及び⑪改善事項を記入します。 ○（適合）：個人情報の取扱規程が整備されている。体制が整備されている。ルールを守って運用している。 △（適合でも不適合でもない）：個人情報の取扱規程は整備されているが問題がある。体制は整備されているが問題がある。ルールに則り運用しているが問題がある。 ×（不適合）：個人情報の取扱規程が整備されていない。体制が整備されていない。ルールに則った運用ができていない。
⑩	指摘事項	問題として把握したことを指摘事項にします。 ＊　必要に応じ、詳細を別紙に添付し、参照する資料番号を記入します。
⑪	改善事項	監査人としての改善勧告内容を、上記指摘事項に対する改善事項として記入します。 ＊　必要に応じ、詳細を別紙に添付し、参照する資料番号を記入します。
⑫	フォローアップ結果	フォローアップ監査を行ったときの結果を○、△、×の３段階で評価します。 ＊　評価は、項番⑨に同じ。監査人は、是正及び予防処置の結果を確認し評価します。是正及び予防処置を別紙に添付し、参照する資料番号を記入します。

8. おわりに

本年9月初旬に、㈱工業調査会から編著者当協会個人情報保護監査研究会による『個人情報保護マネジメントシステム実践マニュアル－JIS Q 15001:2006年版対応』（仮称）が発行される予定です。同書籍には、紙幅の都合で割愛した監査業務の全プロセスの説明並びに実践的にすぐ役立つ豊富な書式及びチェックリスト（CDファイルに収録）を盛り込んでいますので、是非購入下さい。

引用文献
〔1〕『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 15001：1999』、財団法人日本規格協会、平成11年4月2日、5ページ
〔2〕『個人情報保護マネジメントシステム－要求事項　JIS Q 15001：2006』、財団法人日本規格協会、平成18年5月20日、10ページ
〔3〕『個人情報保護マネジメントシステム－要求事項　JIS Q 15001：2006』、財団法人日本規格協会、平成18年5月20日、3ページ
〔4〕『個人情報保護マネジメントシステム－要求事項　JIS Q 15001：2006』、財団法人日本規格協会、平成18年5月20日、7ページ

参考文献
(1) 財団法人日本情報処理開発協会　プライバシーマーク事務局　プライバシーマーク（r）制度『JIS Q 15001 改正に伴う申請について』（平成18年5月18日）、http://privacymark.jp/appl/2006yoshiki.html、（2006年7月）
(2) 財団法人日本情報処理開発協会　プライバシーマーク事務局　プライバシーマーク（r）制度『プライバシーマーク制度における監査ガイドライン』第1版（平成12年3月）、http://privacymark.jp/ref/、（2006年7月）
(3)『個人情報保護マネジメントシステム－要求事項（JIS Q 15001:2006）』、財団法人日本規格協会、平成18年5月20日
(4)『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 15001:1999』、財団法人日本規格協会、平成11年4月2日
(5)『新版　システム監査基準　解説書』（平成16年基準改定版）、財団法人日本情報処理開発協会、2005年1月31日
(6) 経済産業省、『個人情報の保護に関する法律についての経済産業分野を対象としたガイドライン』（平成16年6月）、http://www.meti.go.jp/policy/it_policy/press/0005321/、（2006年7月）
(7) 社団法人情報サービス産業協会、『JISA「情報サービス産業 個人情報保護ガイドライン」の改定と新基準への移行計画について』（平成18年6月22日）、http://www.jisa.or.jp/privacy/pr/060622.html、（2006年7月）

(トピックス)
NPO事業継続推進機構（BCAO）の設立と活動について

事業継続推進機構　副理事長　東京海上日動リスクコンサルティング株式会社
情報グループ　グループリーダー　前システム監査人協会理事
指田　朝久

この度、災害、事故等の際の企業・団体の「事業継続」を推進していく意志を持つ有識者、コンサルタント、各企業の担当者等が「特定非営利活動法人 事業継続推進機構」(BCAO)を設立し、内閣府よりNPO認証を取得しました。また、7月10日にNPO認証記念セミナーを東京で開催しました。

平成16年度以降大規模災害が連続し、企業の防災・危機管理対策の重要性が改めて認識されています。また、情報セキュリティガバナンスの立場からも、情報システムの継続性の重要度はますます高まっています。そこで、政府は、本年、事業継続に関するガイドラインや指針を相次いで発表し、中小企業も含め、企業の取組みの重要性を強調しています。さらに、政府の大規模地震対策にも、企業防災の柱として事業継続が位置づけられました。

この「事業継続」とは、災害、事件、事故等による企業、団体等の活動の中断をなるべく少なく抑え、かつ、できるだけ早期に回復する経営マネジメント戦略です。BCP（事業継続計画：Business Continuity Plan)を策定し、運用、訓練、見直し等を行うBCM（総称して事業継続管理：Business Continuity Management)の取組みのことをいいます。これまでコンピュータ2000年問題、ニューヨークの9.11同時多発テロ等で有効性が注目され、米英等で普及が先行しました。このため、我が国企業が海外取引先からBCMの提示を求められる例が増えています。また、事業継続はサプライチェーン全体での取組みが必要になるため、国内有力企業も取引先に対応を求める動きを始めています。

このような状況を踏まえ、私たちは、事業継続の支援者・推進者として、国際連携も視野に入れつつ、非営利公益的な活動を行ってまいります。当機構の事業は、事業継続の普及・啓発、専門家育成、標準化、表彰、調査研究・情報提供、出版、講演会、企業・団体の取組支援などを予定しています。現在、約100名の個人会員、20数社の法人会員（個人活動枠10人または5人）のご参加を得て、分科会活動を開始し、資料の標準化、セミナーや講習会、資格制度の準備に意欲的に取り組んでいます。

今後の活動予定としては、
- ＮＰＯ認証記念セミナーを東京にひき続き大阪でも開催いたします。
- 東京及び大阪で、事業継続担当者の意見交換の場を夏頃からスタートさせます。
- 事業継続に関する教材資料を、現在作成中です。
- 専門家育成講座のカリキュラムを準備中で、年度内には開催予定です。

また、現在、活動している委員会・分科会は以下のとおりです。
① 標準化・教育委員会　-標準化分科会、カリキュラム分科会、セミナー分科会
② 普及啓発委員会　-ニュースレター分科会、地域振興分科会
③ 国際委員会　-国際連係分科会
④ ＢＣ基本事項委員会　-ビジネスインパクト分科会、情報システム分科会、バックアップオフィス分科会、ファイナンス分科会、自然災害分科会、テロ・事件分科会
⑤ 調査・分析委員会　-ＢＣ事例調査分科会、文献・統計分科会

これから参加される方々の活躍の場は大きく、分科会も増えるものと考えています。BCM、BCPを実施していく個人・法人、それを指導していく個人・法人、そして、今後BCMを学ぼうとする方の入会を歓迎します。ぜひ、私たち事業継続推進機構の活動にご参加・ご支援をお願いいたします。
(http://www.bcao.org/)

システム監査実践セミナー in 名古屋 実施報告 事例研究会・中部支部

今年5月、名古屋にて2日間のシステム監査実践セミナーが開催されました。

システム監査実践セミナーは、講師が被監査企業側、受講者が監査人となって、ロールプレイング形式で実施されます。事例研究会が実施したシステム監査普及サービスの事例をアレンジしたものをケーススタディとして取り上げ、3～4名のグループにわかれて、予備調査、本調査、監査報告の実際を体験することができます。

今回は中部支部も共催で実施することができました。中部支部では3年ぶり2度目の開催となります。

以下に今回の実施内容をご報告いたします。

1. 開催概要

(1) 日時：2006年5月27日（土）13時
～ 5月28日（日）15時
(2) 場所：愛知県名古屋市港区
邦和セミナープラザ
(3) 受講者数：10名
(4) 講師（敬称略）：
沼野 伸夫、畠中 道雄、石井 成美
(5) 参加費：会員 84,000円、非会員 105,000円

2. スケジュール

＜5月27日（土）＞

13:00～13:15 開始セレモニー
13:15～14:30 講義 システム監査技法等解説
14:30～16:30 チーム演習
監査計画と予備調査項目検討
16:30～17:00 講義
予備調査インタビュー
テクニック
17:00～18:00 ロールプレイ 予備調査
18:00～19:00 （夕食）
19:00～20:45 チーム演習
予備調査結果と本調査項目検討
20:45～21:00 講義
本調査インタビュー
テクニック
21:00～ （懇親会）

＜5月28日（日）＞

7:30～ （朝食）
9:00～10:00 チーム演習
本調査項目検討（続き）
10:00～11:00 ロールプレイ 本調査
11:00～12:30 チーム演習 監査報告書作成
12:30～13:30 （昼食）
13:30～14:30 ロールプレイ 監査報告会
14:30～15:00 講師講評、事後課題説明

講義 セミナーが始まります

3. 受講者の声

(1) 受講者アンケート（抜粋）
時間：よい3名、まあまあ5名、不足2名
日程：よい8名、もう1日2名
講師対応：よい10名
金額：安い1名、まあまあ5名、高い2名
事例への要望：自治体、ソフトウェア開発、
プロジェクト監査、
企画プロセス、運用

(2) セミナー受講の心得

No.1563 松井 真一

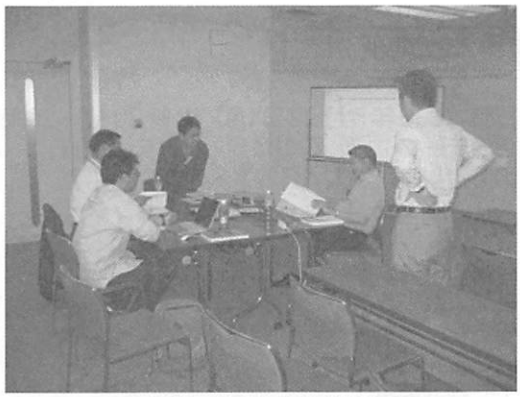
私は17年度秋期の監査人、監査人補の募集時に監査人補に認定いただきました。しかし、元来は通信屋である私は、情報セキュリティ監査の経験は有るものの、システム監査の経験はありませんでした。今回のセミナーでは、システム監査を模擬体験することにより、システム監査人認定の条件を満足することを目的に参加いたしました。

セミナーでは、実際にシステム監査普及サービスにて監査を行なった旅行業の事例を教材として、システム企画業務について予備調査から監査報告会までをロールプレイングを通じて体験しました。

監査報告会のロールプレイでは、会社側役員役となった講師陣からだけではなく、他チームの受講者からも活発な質問がされました。実監査の経験が浅い私にとっては、経営側の立場で監査をすることの重要性を実感できた貴重な体験となりました。

今後、本セミナーを受講される方に私が申しあげられる教訓としては、事前学習を充分に行なうべきである、という点です。2日間という短い時間内で、予備調査から監査報告会までを体験するスケジュールであるために、作業時間が短く、企

業概要などの監査資料を読み返す時間は充分にはありません。受講の案内に記述されますが、“配布テキストの熟読”と“事前課題の実施”を指示どおりに実施して受講に望まれることをお勧めします。



チーム演習　真剣な議論が続きます

(3)“盛り上がった懇親会”
－システム監査実践セミナーin名古屋
に参加して

No.1264　伊藤　裕

監査実践力をつけるべくセミナーに参加しました。セミナー自体も、非常に緊張感のあるものでしたが、初日夜の懇親会では、翌日にまだセミナー続編があるというのに、北陸地区や、東京、大阪からもセミナー参加者がいらっしゃって、夜更けまでシステム監査などをとりまく国内の政治動向から、温泉の話まで、大変アカデミックかつにぎやかな会となり、大変有意義な時間を過ごす事ができました（東海北陸自動車道による経済効果のお話とともに、某講師が大変温泉好きということも知りましたし、また、氷見の魚が大変おいしいという貴重な情報も得ることができました）。

セミナー講師の沼野様、畠中様、会場準備や、当日の食事、宿泊、懇親会の準備で活躍していただいた、中部支部若原会長。今回はチーム担当講師をしていただきながら、懇親会の買出しまでしていただいた中部支部石井様には大変お世話になりました。また受講者の方々は、それぞれの分野で活躍されている方ばかりで、大変よい交流の場ともさせていただきましたこと、紙面をお借りしてお礼申し上げます。

懇親会　遅くまで盛り上がりました

4. 講師雑感

(4)セミナー講評

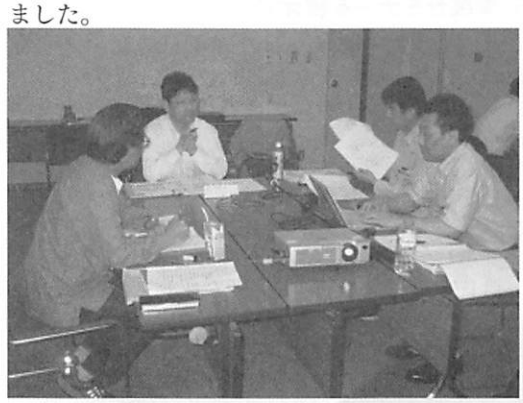
事例研究会　No.750　畠中　道雄

今回使用した教材は、比較的読みやすい資料が多いため、受講者の皆さんは事前配布資料を良く読んでおられ、講師が予想しなかったような質問で切り込んできました。特に、ITにかかわる最新のキーワード（戦略情報化企画、セキュリティ、事業継続計画）については身近な問題でもあり、高い関心を示して臨まれました。世の中の動向も視野に入れたこのような対応は、実際の監査でも重要です。

アンケート結果から、受講者の皆さんには、概ね受講目的を達成していただけたと考えております。加えて、快適な施設を利用できたこともあり、懇親会でのお話も大きなおみやげになったのではないでしょうか。

実践セミナーの進め方は、これまでの経験を踏まえて改善を重ねた結果、現在に至っておりますが、講義とチーム作業の順序やタイミングなどで、さらに見直したいと思います。

なお、今回のセミナーでは、準備段階から中部支部の若原さん、石井さんに全面的にご協力いただき、大変感謝しております。ありがとうございました。



ロールプレイング　鋭い質問が飛び出しました

(5)中部支部講師第一号として

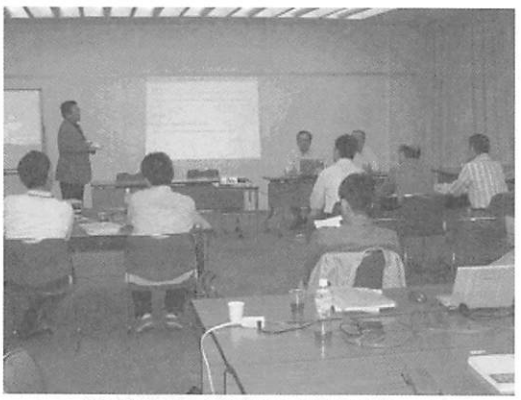
中部支部　No.1224　石井　成美

今回のセミナーが、中部支部との共催ということから、中部支部より一人講師を選出することになりました。受講する意思を示していた私に対し、諸先輩方から“習うより教えるほうが勉強になる”とのアドバイスを頂いたことから、僭越とは存じましたが講師を引き受けさせて頂きました。

私事ですが、今年の4月より23年間勤務したNECソフトウェア中部を辞め、中京短期大学情報コースの専任教授となりました。

現在は、学生を相手に実務経験を活かした講義をしておりますが、久しぶりに社会人を相手に講師をやってみて感じたことは、講義を受ける人のモチベーションの高さと、実務経験をベースとした習得レベルの高さの違いです。特に、今回のセミナー受講者の皆さんは、私より先輩の方々も多くお見えになり、いつまでも自己を向上させようとする熱意が伝わってきて、私自身とても刺激を受けると共に、大変勉強になりました。

ご指導頂いた畠中講師、沼野講師と受講者の皆様にこの場を借りて感謝申し上げます。



監査報告会　2日間の成果の発表です

5. 実践セミナーを終えて

今回の実践セミナーは、昨年11月に事例研究会から打診をいただきました。私は、2003年の大垣での実践セミナーに引き続き、会場確保や受講者の募集などで、事務局のお手伝いをさせていただきました。今回は中部支部からも石井様に講師として参加いただきました。無事開催できたことを、大変うれしく思います。講師の沼野様、畠中様、そして石井様、ありがとうございました。

「1円61万株」誤発注、ライブドアショックによる東証取引停止など、情報システム障害の社会的影響が日々、深刻化してきています。このような情報システムの混乱を防ぐためにも、システム監査人養成の必要性が大きくなってきているのではないでしょうか。地方での開催には苦労も伴いますが、それだけに今回受講してくださった方々の、今後のご活躍を期待したいと思います。

(中部支部　No.808　若原　達朗)

第120回月例会

日時:2006年5月22日(月) 18時30分～20時
講演テーマ:「新JISの概要とシステム監査」
講演者:財団法人　日本情報処理開発協会
　　プライバシーマーク推進センター
　　副センター長　　関本　貢氏
会場:中央大学駿河台記念館
参加人数:
報告者:一村　義夫 (No.6005)

1．講演要旨

(1) プライバシーマーク制度

着実に実績を伸ばしている。2006年3月31現在、3,508社が取得。2005年4月の個人情報保護法全面施行の影響が大きい。指定機関も10団体になった。業界団体が主体だったが、九州、中部、関西の3地域に地域主体の新しい機関ができた。これにより、地方の事業者にとって、審査員の旅費等実費負担が軽減される。また、申請時に要求される欠格事項への非該当判断について、透明性を高めるため、JIPDECのホームページに関連情報が公開された。法人単位の申請が条件である。申請時に教育研修実績記録、監査記録は必須であるが、CP見直しの実施までは、要求していない。

(2) 新JIS対応

プライバシーマーク審査機関の書類調査項目が1999年版の60項目から約2倍(120項目前後か？)になり、現地調査項目が1999年版の49項目から約4倍(200項目前後か？)になった由。新JISは、個人情報保護法への適合性を確保しているだけでなく、個人情報保護法より厳しい内容(個人情報は、生存者に限定しない。取扱件数に制約なし。PDCAなど)を規定している。

(3) 改正までの動き

個人情報保護法及び各省庁のガイドライン発行が大きな影響を与えた。

(4) 改正のポイント

改正のポイントは、6つある。①個人情報保護法の概念の導入・明確化(本人の同意なしに第三者提供を行う措置。従業者の監督。委託先の監督。開示対象個人情報)　②保護法の用語に統一

(本人。情報の提供を受ける者。取得。取扱の委託)、③1999年版の継続（変えないもの。直接書面取得時の同意原則。特定の機微な個人情報取得の制限)、④PDCAサイクルの明確化(ISO Guide 72準拠。他のマネジメントシステム規格との構造上の整合性確保）、⑤プライバシーマークの運用実績を踏まえ審査事項を明確化（リスクの認識・分析及び対策。緊急事態への準備。個人情報保護マネジメントシステム文書。是正処置及び予防処置)、⑥CPから個人情報マネジメントシステムへ名称変更、である。

(5) 新設された要求事項

9項目が新設された。①緊急事態への準備、②運用手順、③本人にアクセスする場合の措置、④提供に関する措置、⑤従業者の監督、⑥委託先の監督、⑦記録の管理、⑧運用の確認、⑨是正処置及び予防処置、である。

(6) 改正ポイントと対応

全部で12項目についての説明があった。旧JISでプライバシーマークを取得している事業者は、いろいろ注意が必要である。次項2の講演内容で報告する。

①保護方針関係、②リスク認識・分析関係、③資源・役割・責任・権限関係、④内部規程関係、⑤取得関係、⑥目的外利用関係、⑦本人へのアクセス関係、⑧提供関係、⑨緊急事態への対応関係、⑩従業者監督への対応関係、⑪委託先監督への対応関係、⑫運用確認への対応関係、である。

(7) 新JISへの移行計画

2006年5月の新JIS制定を基点に30ヵ月を経過すると旧JISの適用は廃止される。2008年11月までに新JISへの移行を完了しなければならない。

2. 講演の内容

旧JISでプライバシーマークを取得している事業者が新JIS準拠の個人情報保護マネジメンシステムへ移行する際の必要な対応について説明があった。以下、その内容である。他は、割愛する。

① 保護方針関係：理念の明確な記述。目的外利用に関する記述。苦情及び相談に関する記述。
② リスク認識・分析関係：目的外利用防止対策を講じる手順の確立・維持に関する記述。リスクに関する記述の追加。個人情報の取扱いの各局面におけるリスク云々の表現の追加。
残存リスクの把握・管理
③ 資源・役割・責任・権限関係：個人情報保護管理者の社長への運用状況報告に関する記述追加。
④ 内部規程関係：新JISへの対応。手順の文書化。内部規程は、リスク分析、分析及び対策をベースに規定化。
⑤ 取得関係：間接収集の概念がなくなった。通知項目の追加。「書面による明示」の記述。
ただし書きの内容に関する記述追加。本人から直接書面によって取得する場合以外の方法による取得に関する規定の追加。
⑥ 目的外利用関係：ただし書きの新JISへの対応。
⑦ 本人へのアクセス関係：通知事項の追加他。
⑧ 提供関係：通知事項の追加他。
⑨ 緊急事態への対応関係：規定の追加。
⑩ 従業者監督への対応関係：規定の追加。
⑪ 委託先監督への対応関係：契約条項の新JISへの対応。
⑫ 運用確認への対応関係：規定追加。

3. 質疑

(若干質疑応答があったが、記録を取っていない。)

4.所感

講師は、肩書きのとおり、わが国のプライバシーマーク制度の権威である。今回の月例会は、2006年5月20日の新JIS（JIS Q 15001：2006）の発行直後であり、参加者が大きな期待を寄せたタイムリーな演題、適切な講師の選択であった。講演内容は、参加者の期待を裏切らない充実した内容であり、参加者の新JISへの理解が一気に深まったように思う。月例会担当理事他関係者の御尽力に感謝する。

プライバシーマーク審査機関の書類調査項目が1999年版の60項目から約2倍になり、現地調査項目が1999年版の49項目から約4倍になったという話があったが、審査項目の大幅増加は、審査員及び審査を受ける事業者へ大きな影響が出る。すでに旧JISでプライバシーマークを取得している企業が新JIS準拠に移行したときの最初の監査では、適合性監査が必須であり、また、運用監査についても、監査する側、被監査部門ともに、負荷の増大が予想される。今後、当協会の活動で、新JIS対応の実務書が出版される他、セミナーや研究発表が活発に行われ、新JIS対応の渦中にある当協会会員に有益な情報が発信されることを期待する。演題にある、「・・・・システム監査」については、プライバシーマークの運用実績を踏まえた、監査業務に関するコメントが聞けることを期待したものの、残念ながらそれはなかった。

第121回月例研究会報告

日時：2006年7月3日（月）18:30～20:30
場所：中央大学駿河台記念館
演題：「システム監査とJSOX」
講師：日本大学商学部・大学院商学研究科
堀江　正之　教授

報告者　No.893(北海道支部) 渡部　洋子

1．講演要旨（ポイント）

(1) JSOX404条対応への要請を、単なる負荷だと考えるところから脱却し、変革のトリガーととらえて、企業文化を変革させる方向へ成長していかなければならない。意識を前向きに変える良い機会といえる。

(2) JSOX404条対応は、内部統制の一部に過ぎない。ここで求められているのは、あくまでも「財務報告に係る内部統制」であるが、業務の有効性と効率性に係る内部統制など、企業の内部経営管理の仕組みとして内部統制はもっと広く解釈される。財務報告に係る内部統制だけを整備しても意味がない。

(3) 財務報告に係る内部統制を足がかりに、全社的な戦略達成をサポートする内部統制構築へと進んでいくことが望ましい。

(4) IT統制も定型的なものだけでなく、もっと広く、ITガバナンス（IT戦略、ITアライアンス、IT組織構造、ITセキュリティポリシー、ITリスク情報開示）をベースとして考えなければならない。

2．講演内容

(1) 財務報告に係る内部統制評価と監査の概要

経営者が自社の内部統制を評価して「内部統制報告書」を作成し、監査法人がそれを監査して「内部統制監査報告書」を作成する。会計士監査と同様に、いきなり問題を指摘するのではなく、指導的機能によるフィードバックが働く。

米国の実例では、「内部統制監査報告書」で以下の2種類の評価がなされている。

・経営者による評価が適正に行われているという評価
・財務報告に係る内部統制が適正に行われているという評価

前者がアサーションであり、後者がダイレクトレポーティングであるが、JSOXで要求されているのは前者である。

このアサーション方式では、企業の内部統制を監査するのではなく、経営者の評価を監査することになり、経営者が自社の内部統制は有効でないと評価し、実際に有効でないと評価するなら「適正」であるという監査結果になってしまう。内部統制には欠陥があるが財務諸表は適正であるということは現実的にありえるが、自社の内部統制が有効でないと告白することは、虚偽表示が起こりえると経営者が宣誓するようなものである。

(2) JSOX404条の制度化

・法制化の状況：2006年6月7日成立の証券取引法等の改正（金融商品取引法）により、2009年3月期決算から、内部統制の経営者評価と外部監査が導入される。経営者による内部統制報告書と外部監査人による内部統制監査報告書の記載事項は、内閣府令により決定される予定。
・金融庁の動向：現在公表中の「財務報告に係る内部統制の評価及び監査の基準のあり方について」の解釈指針として「実施基準」の公表が決定しており、早ければ今年の夏にも草案が公開される見通し。
・日本公認会計士協会の動向：内閣府令の制定を待って内部統制の外部監査のための委員会報告が公表されるはず。ただしこれはあくまで外部監査のためであり、経営者向けではない。

先行事例を見ると、マイナス評価される事例では、内部統制コストだけに目が行ったり防御に専念したりしているが、プラス評価される事例では、内部統制の設計が予防にシフトして、欠陥の有無が業績につながるという調査結果もある。国内の事例を見ても、内部統制の不備が時系列的に財務報告につながることがわかる。

(3) 経営者による内部統制評価のポイント

現在、監査だけがクローズアップされているが、リスクから統制、監査へのつながりを明確に意識することが必要である。リスクの連鎖や大きさを評価して、それを踏まえた統制を行わなければ意味がない。

経営者が内部統制を評価する際には、組織内外のリスクを踏まえた全社的な統制の評価と、統制上の要点ごとに業務プロセスに係る統制の評価の両面で実施する。後者では、手続きの整備状況と運用状況の2段階で評価する。評価の際には記録を取るが、現行の業務フローにリスク評価を重ね合わせ、さらに統制フローまで重ねていくと、全体を見渡すことができ、不備を見つけやすくなる。

内部統制報告書の末尾には、評価結果と区別して、付記事項を記述する。期末日後に実施し

た重要な欠陥に対する是正処置などを記述するので、1年目には付記事項が多くなることも予想される。

(4) 金融庁「内部統制基準」にみるIT統制のポイント

ITへの対応は、そこだけ独立したものではなく、他の内部統制の基本的要素と一体となって機能するものであることを忘れてはいけない。現在ではインターネット環境が前提であり、ITの開発／運用の外部委託に係る統制も対象である。IT統制という大きな領域の中に、「統制へのITの活用」と「ITシステムの統制」が一部重複して含まれる形となる。

全社レベルの統制から業務プロセスレベルの統制に落とし込んでいくように、全般統制から適用業務統制に落とし込んでいく。COBITforSOXの体系の通りであるが、今日のクライアントサーバー環境などでは、全般統制・適用業務統制という区別がほとんど意味のないものになってきているという実態もある。

(5) 本来の内部統制をめざして

理想的には、企業の事業環境の中で、戦略や文化、業務プロセス、個人の技能と役割といったものの中心にIT統制が位置付けられる。ITリスクは、あくまでもビジネスリスクの一つであり、機会リスクという側面もあるし、コンテンジェンシー計画も含まれる。SOX法対応だからといって、ブレーキを踏む統制ばかりでなく、アクセルを踏む統制を忘れてはならない。

最後にシステム監査としての課題を2つあげる。最初は、ITへの対応の部分では内部監査の利用が効果的であるが、そこでシステム監査が行われれば、経営者評価及び監査法人監査でそれを利用することが考慮される。一歩進めて「専門家業務の利用」を提言できるが、現段階ではどこにも入っていない。2つ目は、JSOX対応に限定すれば、あくまでも財務報告に係る内部統制の評価と監査のスキームとなるので、そこでシステム監査が入ってきたとしても、財務諸表監査に関して会計上の細かな知識が必要とされることになる。

3．質疑

・監査法人との癒着などが問題となっており、米SOX法には監査法人への規制ルールなどが盛り込まれたがJSOXではどうか。

日本では公認会計士法の改正などで対応しており、全体として規制する方向になっているのは同様である

・監査委員会や監査役の役割はどう位置付けられるのか。

経営者評価とそれに対する監査の仕組みとは別に、経営層へのチェック機能として働く。この仕組みの中で独立して動くというより、統制環境の一部と考えられる。

・ドイツの従業員を参加させるやり方と比較してどうか。

枠組みが異なるので一概に比較できない。

・システム監査としての「専門家業務の利用」を推進するには、どうしたらよいか。

これから公開される草案ではパブリックコメントを求めるはずなので、そこで提言するのが一番である。（協会として対応して欲しいとの意見あり）

4．感想

このテーマでは下手をすると眠くなるのではないかと恐れていたのですが、ユーモアを交え聞き手を引き付ける語り口で楽しませていただきました。様々な情報があふれている割にはすっきり理解できないJSOXについて明快にご説明いただき、頭の整理ができたようです。

特に、アサーション方式としての限界や注意点が明確になり、全体像が見えてきた（ような気がする）ところ、また、ここで萎縮して守りに入るのではなくもう1ステップ前進するトリガーにすべきだという方向性が示されたことに感謝したいと思います。「アクセルを踏む統制」という表現が、私にとってのキーワードとなりました。

今回の月例会報告は、北海道支部の渡部がお送りしました。出張の隙間で出席したのですが、行って良かったというのが実感です。地方の皆さまも、出張の折などタイミングが合いましたら、ぜひ月例研究会へのご出席をお勧めします。

「個人情報保護管理者/監査責任者の実務」セミナー企画書

主催　ＮＰＯ日本システム監査人協会

後援　(財)日本情報処理開発協会
(社)情報サービス産業協会
(社)日本情報システム・ユーザ協会
(財)日本データ通信協会

趣旨

このセミナーは、
① 個人情報保護に企業としてどのように対応すべきか
② 新JIS Q 15001個人情報保護マネジメントシステムとは
プライバシーマーク制度の概要と、取得するには
③ 個人情報保護管理者の行う実務
④ 個人情報保護監査責任者の行う実務
を学ぶものです。企業内においてすぐに役立つよう、できるだけ具体的な形で進めます。

1．日程　大阪(9月2,3日)、東京(10月7,8日)、富山(11月11,12日)
2．場所　大阪：ドーンセンター(大阪府立女性総合センター)
東京：中央大学駿河台記念館　7日330号室、8日560号室
富山：(富山駅前)ＣＩＣビル3階市民学習室
3．内容
第一日目　1．企業の内部統制と個人情報保護法対応　10:00～12:00
㈱筑波総合研究所　代表取締役　公認システム監査人　打矢　隆司
2．新JIS Q 15001解説とプライバーマーク制度　13:00～14:50
(財)日本情報処理開発協会　講師未定
3．個人情報保護のための安全管理の実務　15:00～17:00
㈱ビジネスソリューション　代表取締役　公認システム監査人　松枝　憲司
第二日目　1．個人情報保護管理者の実務　10:00～12:40
んじゃろ監査事務所　代表　公認システム監査人　竹下和孝
2．個人情報保護監査責任者の実務　13:40～16:20
㈱日立情報システムズ　ＣＳＲ本部　副本部長　公認システム監査人　一村　義夫
3．確認テスト　16:25～17:00
4．個別相談会(実施は講師の都合による)　17:00～17:30
開催時間については、開催地により、前後します。
4．参考資料として、JIS Q 15001:2006(日本規格協会発行)を受講者に配布します。
5．参考資料として、出版物「個人情報保護マネジメントシステム実践マニュアル」
(ＮＰＯ日本システム監査人協会監修　㈱工業調査会出版)を格安にて提供します
6．確認テストで一定レベルの内容が確認されたものには、後日、協会会長名の修了証を送る。
7．継続教育等の認定
・公認システム監査人・システム監査人補における継続教育時間として認定(12時間相当)
・(依頼中)ＩＴコーディネータ継続教育（12時間3ポイント分)
8．受講料　ＮＰＯ日本システム監査人協会会員及び後援団体の会員　21,000円（消費税込み)
非会員　25,200円（消費税込み)
9．募集対象人数　開催地により異なる。各30人程度
10．担当者連絡先
本部　〒103-0025　東京都中央区日本橋茅場町2-8-8共同ビル(市場通り)
ＮＰＯ日本システム監査人協会
電話　03-3666-6341　FAX　03-3666-6342
担当者　蓮見節夫　E-MAILアドレス　hasumi-setuo@nifty.com
大阪地区　喜多　陽太郎　kita06@is-solution.co.jp
富山地区

案内書については、ＮＰＯ日本システム監査人協会ホームページに掲載予定
ＮＰＯ日本システム監査人協会ホームページ　http://www.saaj.or.jp/

「個人情報保護マネジメントシステム実践マニュアル」出版予告

今年、5月20日にJIS Q 15001：1999に代わり、JIS Q 15001:2006個人情報保護マネジメントシステム要求事項が発表になりました。

私たち、個人情報保護監査研究会では、システム監査の応用編として、個人情報保護マネジメントシステムの一部を構成する個人情報保護監査を研究しています。当協会の多くの会員も、企業内のそれぞれの場で、個人情報保護マネジメントシステムの構築推進を実践しています。こうしたことを背景に、培ったノウハウを「個人情報保護マネジメントシステム実践マニュアル」(新JIS Q 15001対応)(仮称)としてまとめました。㈱工業調査会のご協力の下に近日中に出版されます。(価格：未定)

【本の構成】

序　章　この本の役割
第1章　JIS Q 15001:2006の観点で業種の特徴をひも解く
第2章　JIS Q 15001:2006個人情報保護マネジメントシステム要求事項を理解する
第3章　プライバシーマーク制度と取得の手順を知る
第4章　個人情報保護マネジメントシステムの構築推進のプロジェクト体制を作る
第5章　個人情報の特定とリスクを洗い出す
第6章　物理的・技術的安全対策のポイント
第7章　個人情報保護マネジメントシステムの文書化を行う
第8章　個人情報保護の運用体制を作る
第9章　個人情報保護教育を進める
第10章　個人情報保護マネジメントシステムを運用する
第11章　運用管理と監査で点検する
第12章　是正処置及び予防処置を実施する
第13章　個人情報保護マネジメントシステムの見直しを行う
第14章　プライバシーマーク認定を申請し認定を受ける
第15章　プライバシーマーク認定後の運用ポイントを押える
第16章　プライバシーマーク既取得者が新JISに対応する

組織内において個人情報保護マネジメントシステムを確立したいと考えている、経営者の方、推進プロジェクト、個人情報保護管理者、監査責任者、これらを支援する人たちにとって、十分にお役に立つものと確信しています。

当協会では、先に「情報システム監査実践マニュアル」を工業調査会より出版しました。その姉妹編として、ご活用ください。

個人情報保護監査研究会代表　蓮見節夫

2006.7

韓国システム監査事情に関する講演会の予告

協会公認システム監査人等認定委員会では、継続教育セミナーとして、下記の講演会の実施を予定している。

社団法人韓国情報システム監理協会との提携記念講演会
(継続教育セミナー)

1．日時：平成18年（2006）９月30日（土）午後２時30分から午後６時

2．場所：東京新宿区西新宿　京王プラザホテル

3．テーマ：
「韓国におけるシステム監査の現状と今後の展開
～システム監査の法制化はどこまで進んでいるか～」

4．演題及び講師：

1）韓国におけるシステム監査の現状と今後の展望（日本語）
韓国システム監理協会名誉会長Lee, Kingduck（李 敬徳） 氏

2）韓国システム監理協会の現況と今後の展開（韓国語、逐次通訳）
韓国システム監理協会会長Choi, Jiyun 氏

5．参加費　　協会会員￥2,000　　非会員￥3,000

6．継続教育申告時間６時間（協会主催のため履修時間を1.5倍として扱う）

会報投稿論文

個人情報保護の実態と有効的な情報セキュリティ対策

No.1015 黒川 信弘

1. はじめに

1.1 個人情報の漏洩事故が止まらない

2003年5月に個人情報保護法が成立し、2年間の準備の後、2005年4月1日に民間事業者も含めた形で全面施行された。多くの企業や組織団体では相当な準備をしてきたのではなかろうか。中にはプライバシーマーク1のような第三者認証を取得して、他社との差別化を図ろうとしている企業も多々ある。個人情報保護法の周りで、多くの企業の思惑が交錯し、悲喜こもごもの現状を現出している。

4月1日の全面施行までは、毎日のように漏洩事故が報道されていた。それはおよそ年に200件以上に及ぶと思われる。2005年4月の全面施行というハードルを越えてしまえば、事故は大幅に減るのではないかと、一部では楽観視されてもいた。しかし、ルビコン川を越えた今、漏洩事故は減ったであろうか。2005年4月1日に報道された小児患者60名分の電子カルテがネットに漏洩した事故を皮切りに、2ケ月間で100件以上が報道され、3月までを上回るペースで事故が発生し続けた。そして2005年1年間でおよそ1000件の事故が報道された。予想に反して、漏洩事故は一向に減る気配がない。

これは一体どうしたことであろうか。我々が2年間準備してきたことに、何か大きな間違いがあったのであろうか。それともこのまま様子を見ていれば、落ち着いてくるのであろうか。本稿では、そこのあたりの原因・課題を浮き彫りにし、その対策を考えていきたい。

1.2 監督官庁からの是正勧告

2005年5月20日、個人情報保護法に基づく初の勧告が出された。これからの道のりの遠さを暗示するかのように、金融機関が最初の勧告対象となった。みちのく銀行は、預金残高1兆8千億円、従業員数1200名弱の青森県のローカルバンクである。地方銀行ならではの特異な市場を狙って、かなりユニークな事業展開をしてきた銀行である。同銀行は、2002年には青森県住宅供給公社の職員による14億円横領事件の舞台裏となり、2003年には銀行員による着服事件などの不祥事を起こし、監督官庁への報告時においても事実を隠蔽するなどの不備があったという。そして個人情報保護法が施行された2005年4月に128万件の顧客情報が入ったCD-ROM 3枚を紛失する事故を発生させてしまった。事ここに及んで、東北財務局は「経営責任の明確化」などを求める業務改善命令を出した。また金融庁は個人情報保護法に基づく改善措置を取るように是正勧告を行ったのである。128万件の個人情報漏洩件数は金融機関では最大であり、当局の調査の結果、行内の管理に重大な問題があると判断した結果であるという。

それから約1年後の2006年4月25日、個人情報保護法に基づく勧告第2号が出た。みずほ銀行新宿西口支店における課長職が顧客データ約1200件を詐欺グループに渡していたという事件などにより銀行法第26条に基づく業務改善命令と同時に個人情報保護法勧告が出された。

個人情報保護の面については、情報漏洩が社会に与える影響度の大きさに鑑みて、金融機関、医療機関、情報通信分野を重点3分野と呼ぶ。奇しくもその金融分野から是正勧告が続いて出たわけだが、果たしてこれは偶然なのだろうか。金融機関を筆頭に現在の企業・団体の個人情報保護の取り組みに何か抜本的に欠けることがあるのではないか。数例の企業の現場を目の当たりに観察した結果も含めて、そのあたりの実態を浮き彫りにしていきたい。

2. 個人情報保護の実態

2.1 JR福知山線脱線事故に見る混乱

個人情報保護法が施行されてまもなくの2005年4月25日、JR史上最も悲惨な事故が発生した。JR福知山線での脱線事故である。107名の方々が亡くなり、460名が重軽傷を負った。1週間以上にわたって救出作業が行われ、その現場は刻々とTV報道された。まさに地獄を絵に描いたような混乱と恐怖の状況であった。多くの方は救急車で、トラックで、あるいは近隣住民の車で近くの病院へ搬送された。このとき新聞報道によると、これら死傷された方々の個人情報の扱いについて、現場では少しばかりの混乱が発生したようである。

たとえば、死傷された方々の労災手続き迅速化のために労働局がJR西日本へ死傷者リストを要求した。その際、当初JR西日本では個人情報保護法に基づいて個人情報の提供を拒否した模様である。恐らく個人情報の提供を拒否された負傷者もおられたのではないかと推測する。法律施行後初めての大惨事のため対応をどうすればいいか、若干の混乱が生じたことは否めない。その後、JR西日本の対応が国会で問題視された。このような悲惨かつ迅速化が要求される場面で、個人情報の提供を拒否するとはどう

いうことか。そんなニュアンスであったと思う。個人情報を保有する側と提供される側の思惑が交錯して新たな議論を創出している。

さらには多くの死傷者が搬入された病院での扱いもそれぞれに異なったようだ。5月21日の日経新聞によると、兵庫医大病院の場合、負傷者に関する電話での個別の問い合わせに応じ、院内でもリストの貼り出しを行った。一方、宝塚市立病院では、電話での個別の問い合わせには応じたが、院内でのリストの貼り出しは行わなかったし、報道機関への情報提供は負傷者本人の同意を確認したうえで行った。その他に、尼崎市の情報提供要請に5、6病院が個人情報保護法に抵触するため提供を断ったとある。このように医療現場での個人情報の扱いについては多くの病院でも混乱を来たしている。プライバシーの問題、病状告知の問題、本人確認の問題など医療現場での解決すべき課題は多い。

内閣府によると今回のような事故の場合、本人の同意を得ることが困難な重症患者などのガイドライン例外規定にあたるという。ただし、どんな情報でも出していいわけではなく、それぞれの機関の判断が必要という玉虫色のコメントである。

個人情報保護の本質的な論議からすると、今回のような事故の場合、個人情報を迅速に公開すべき事例ではなかろうか。組織によってその対応が異なれば、現場では多くの混乱と無用な労力を発生させてしまう。災害や重大事故などの緊急時対応のコンセンサスを作っておく必要がある。内閣府や厚生労働省では2006年3月および4月に災害時対応など今回のような混乱の中での個人情報の扱い方の指針を改定した。

2.2 その他の社会的な混乱事例

JR西日本の事故に続いて、多くの局面で個人情報保護の行き過ぎた面が浮かび上がってきた。官公庁の役職者の個人情報や医師国家試験合格者の氏名を非公開としたり、高額納税者や住民基本台帳など市民情報の公開を取りやめた。また、2005年度の国勢調査での調査員を中心とした混乱は記憶に新しい。

一般企業でも多くの様々な混乱がある。職場では名簿を作らない、顧客から注文を受けても名前・住所・電話番号を保存しない、一方的に責任を押し付けるような誓約書を派遣社員から取るなどである。医療機関・病院でも患者の名前を呼ばない、怪我をした生徒の個人情報を教師や警官に伝えないなどの事態が発生している。

学校でも合格発表では名前を発表しないとか、緊急連絡網や同窓会名簿を作らない、あるいは運動会の写真撮影はだめなどという混乱もある。また、2006年正月の年賀状の減少という事態も話題となった。

2.3 筆者の個人的体験

筆者の場合、ITベンダーのセミナー申し込み時にWebサイトから詳細な個人情報を入力する場合が多い。会社名、氏名、eメールアドレスなどの基本情報は理解できるが、FAX番号、役職名、職位、職種、決裁権などを求めるリスクと価値のバランスはどうであろうか。その場合、ほとんどの項目を入力し利用目的の同意ボタンを押さないとサービスを提供してくれないという半強制的な個人情報取得手法になっているのも気になる。

個人情報を登録したあとには受講票を送ってくる。その受講票を持ってセミナーに出席すると受付で受講票を引き取ってくれるのであるが、それ以外に名刺も求める。名刺がない場合はA4用紙に会社名、氏名、住所など詳細な個人情報を書かせる。既に情報登録をしているのだから、改めて個人情報を取得する意味が分からない。このような過度な個人情報の取得を行う企業に対して、顧客は不信感を持つであろう。

あるビジネスホテルでは当日の宿泊顧客リストをフロントテーブルに置いてチェックしている。宿泊客の会社名、氏名など誰でも覗き込んで見ることができるのは、フロント現場への指導がいきわたっていない証拠である。

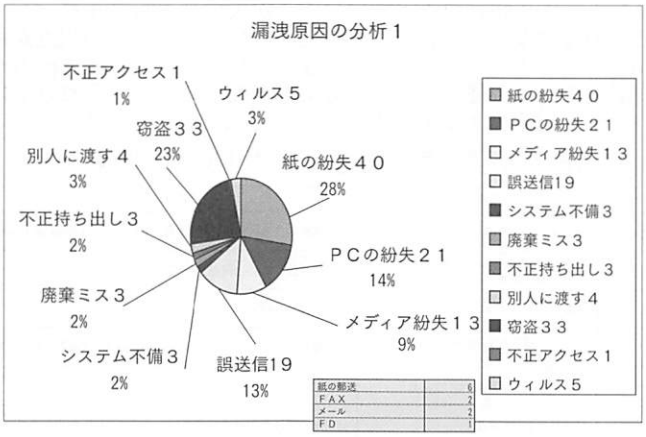
また、あるクレジット会社から会員勧誘のためのDMを送ってきた例であるが、連絡窓口に電話してDMを止めてくれるように依頼すると、そのDMは別の名簿会社から送付しているものなので、そちらへ連絡して欲しいという。DMに会社名と社長名を明記したそのクレジット会社は、DMのどこにも書いてない名簿会社の責任だと言う。個人情報保護の本質を理解していないクレジット会社に対し、本来のクレジット業務の信頼性を疑う。

最近はWebサイトで買い物ができるものが多くなった。あらかじめサイトから会員登録をして商品を注文する。一旦、会員になると商品勧誘のメールが頻繁に来始める。そのしつこさに会員を取りやめようとするが、肝心の脱退方法がわからない。多くのWebサイトでは、会員になるための個人情報の入力方法は目立ったところにあってすぐに分かるのだが、脱退の方法はかなり複雑な方法になっている。有名な大手企業でさえこのような対応を取っていることは、消費者の一人として個人情報を与えることに、より慎重にならざるを得ない。

以上はすべて筆者の個人的体験例であるが、このような無神経な個人情報の取り扱いもその企業の体質をあからさまに社会に公表しているようなものである。良くも悪くも社会的に個人情報保護について多くの混乱があるのは確かである。

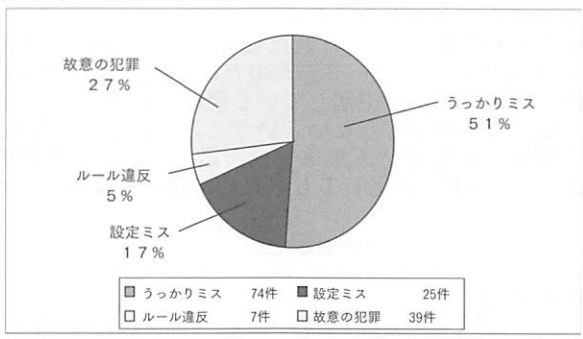
2.4 漏洩事故の実態

個人情報の漏洩が起きた事故・事件の実態はどうなのであろうか。グラフ1は個人情報保護法が全面施行された2005年4月から5月にかけて報道された漏洩事故115件を分析したものである。紙媒体28%、パソコン14%、メディア9%の紛失が群を抜いている。また、郵送やFAX、メールなどによる誤送信13%が多いのも目につく。



グラフ１，個人情報漏洩の詳細原因
（2005年4月～5月）

これらをうっかりミス、設定ミス、ルール違反、故意の犯罪という原因別にまとめてみると、グラフ2のようになる。うっかりミスとは、忘れる、落とす、失う、間違えるという人間の不完全性に起因するミスである。設定ミスとは、正しい理解をしなかったり、何かの誤解でシステムの設定を間違えるといったものである。次にルール違反とは、分かってはいるが、つい面倒だとか、時間がかかるとの理由で決められたルールを守らない行動であり、重度な悪意のないものをいう。故意の犯罪とは、明らかに犯罪と知りながら犯す行為であり、悪意を含むものである。過失及び重度の悪意のないものということで、うっかりミス、設定ミス、ルール違反を大きく同種の領域と見ると、事故の約4分の3はうっかりミスの範疇に近いものと考えてよいのではないだろうか。個人情報漏洩の対策を考えるとき、うっかりミスの対策と故意の犯罪の対策は大きく異なるのである。



グラフ２個人情報漏洩の原因（2005年4月～5月）

2.5 不正使用の実態

次に漏洩した個人情報がどのようになっているかということを考える。まず、“ 漏洩” という言葉自体の使い方に問題があるように思う。個人情報を格納したノートPCを紛失したからといって個人情報が“ 漏洩” したかどうかは断定できないはずだ。この場合は正しくは個人情報の“ 紛失” と言うべきであろう。次に、“ 漏洩” を問題視するのは“ 漏洩” した個人情報が悪用されることがあるからだが、本当に悪用されているのであろうか。この点になると実態を把握することは非常に難しいことになってくるが、“ 漏洩” 後の不正使用について報道されることはほとんどない。最近でこそ、マスコミ報道の中には“ 漏洩” 事故を伝える中で、「今のところ不正使用は確認されていない」という文言を入れる場合が出てきた。表1は2005年6月から2006年5月までの1年間に報道された個人情報“ 漏洩” 事故の中で“ 漏洩” した個人情報を悪用された事例である。この1年間に報道された“ 漏洩” 事故が1000件前後と思われるので、およそ１％しか不正使用が発覚していないことになる。しかも、悪用された個人情報は

故意の犯罪などによって不正に取得したものであり、紛失などの過失が原因のものの不正使用の報道は皆無である。従って、個人情報を紛失しても故意の犯罪による“漏洩”でない限り、個人情報の不正使用はほとんど考えられないと言ってよいのではないか。

もちろん、報道されていないからといって、悪用されていないということの証明にはならない。紛失したことで何らかの不正使用につながる可能性は考えておかなければならない。筆者が主張したいのは、紛失したことのみをことさら強調するのではなく、紛失後の追跡フォローがマスコミはじめ社会的な共通認識として必要なのではないかと言うことである。現在は、そこの視点が弱く、紛失したことそのものをあまりに強調しすぎるきらいがある。困難なことではあるが、紛失後の不正使用の経緯や実態を克明に調べる努力が必要である。従って、紛失対策も重要であるが、それ以上に個人情報を紛失しても漏洩問題が起きないような対策により重きを置くべきではないかと考える。

表1. 二次被害・悪用が発覚した事例（2005/6～2006/5）

報道年月日	事件名	不正使用の被害
2005. 6. 20	米国クレジットカード流出事件	4000万件のうち国内流出は7万件。1億5千万円の不正使用を確認
2005. 10. 20	神奈川・群馬県のゴルフ場スキミング事件	預金引き出し212人分8億1千万円被害
2005. 11. 2	千葉銀行CD-ROMスパイウェア事件	300万円口座移動
2005. 11. 20	ワコール オンラインショッピングサイト不正アクセス	顧客情報4700人流出カード番号不正使用10件・現金引き落としはなし
2005. 11. 11	ジャパネット銀行スパイウェア	顧客にスパイウェアフィッシング10件1140万円の被害
2005. 12. 25	埼玉信用金庫ATM盗難	41口座　3000万円不正引き出し
2006. 3. 7	岐阜・愛知県のUFJ銀行、十六銀行などのATMでスキミング	6人の口座から1100万円引き出し
2006. 3. 29	NTTデータ元社員ATM取引記録を不正持ち出し	クレジットカード偽造後、現金引き出し17人分3100万円
2006. 5. 30	ヤフーオークションフィッシング詐欺	個人情報を不正取得し成りすましで架空出品、落札者から現金取得8人逮捕　被害総額1億円

3. 個人情報保護に対する有効的な情報セキュリティ対策

3.1 人間の行動特性を考えよう

それではまず、紛失対策を考えよう。その大前提には、「人間はミスをする」ということがある（表2）。筆者の息子は通学定期を3年間に3度も紛失した。息子だけではなく鉄道の駅の窓口に行くと、定期券などの紛失物の掲示が沢山載っている。また、自動車のキーの閉じ込め2、エレベータから降りたら違うフロアーだったなどということは多くの人が経験していることであろう。このように人間はうっかりミスをする生き物なのである。

また人間は忘れるということがある。覚えなければならないパスワードが最近非常に増えてきたのだが、郵便局では年間37万件ものパスワード忘れのための問い合わせがあるという。ITが社会的に浸透してきて日常生活にパスワードが氾濫している現状を考えると、このこともしかたないと言えよう。その次には、人間はルールを守らないということを忘れてはならない。

危険とは分かっていても電車への駆け込み乗車や横断道路での信号無視は多くの人も心当たりがあるであろう。これらはいくら罰則を強化しても本質的にはなくならないものだと考えなくてはならない。

表2. 人間の行動特性

■落とす／失くす
- 息子は通学定期券を３年間に３度も落とした
- ＪＲの駅の事務所には、届いた定期券の持ち主名が20名も貼り出してあった（大井町）

⇒落としても返って来るしくみが必要

■ミスをする
- 自動車のキーを車内に閉じ込める
- エレベータから降りたら違うフロアーだった
- 電車から降りたら違う駅だった
- 組織やルールを知らなかった

⇒何重もの安全のためのしくみが必要

■忘れる
- 増えすぎたパスワードを忘れる・・・郵便局には年間37万件以上の暗証番号の問い合わせがある

⇒パスワードだけで信頼性の担保はできない

■ルールを守らない
- 車が来なければ信号無視して歩く
- 書類を期限までに提出しない
- 電車への割り込み乗車、駆け込み乗車

⇒強制、罰則だけでは事故はなくならない

■プライバシー確保
- 自分の行動を人に知られたくない
- とやかく干渉しないで放っておいて欲しい

⇒他人に知られたくないという人間の本能

そういった人間ならではの行動特性を個人情報保護の取り組みの中で考えているであろうか。いくら教育しても人間のうっかりミスは0にはならないし、いくらルールで担保しても人間はルール違反をするものなのである。今後の情報セキュリティ対策はそういった人間の行動特性というものをもう少し重要視していかなければならない。

表3. ミスの種類と対策

具体的な事例	ミスの種類		対策方法	
・かばんを電車に忘れた ・ＣＤ－ＲＯＭなどのメディアを失くした ・メールアドレスを間違えて送った ・送信先ＦＡＸ番号を間違えて送った ・ウィルスファイルを開いた ・アクセス権限の設定を間違えた	うっかりミス（73%）	うっかりミス（51%）	・環境／ツール／手順の整備 ・教育・訓練の実施 ・適性評価の実施 ・フールプルーフ ・フェイルセイフ	情報セキュリティ監査
・パスワードファイルを暗号化しなかった ・ＤＭＺに機密ファイルを置いていた ・ハードディスク消去など廃棄処理が充分でなかった ・パスワードを簡単に推測できるものにしていた ・退職者のアカウント削除をしていなかった ・セキュリティホールのバージョンアップを忘れた		設定ミス（17%）	上記に加え ・レビュー励行 ・報告チェックしくみの構築	
・ＰＣを無断で持ちだした ・ハードディスクを暗号化していなかった ・ＰＣに個人情報を入れていた ・ＰＣや機密情報を施錠保管していなかった ・個人情報をシュレッダー廃棄せずにゴミ箱に捨てた ・持ち出し許可を取らなかった（ＰＣ、機密情報） ・ＰＣを持ち出し用に申請登録をしなかった ・機密情報を家に持ち帰った ・無許可にアプリケーションをインストールした ・許可なしにコピーした（印刷、通信、配布した） ・機密エリアに無断で出入りした		ルール違反（5%）	上記に加え ・教育、監視（抑止） ・罰則の周知徹底	
・機密情報をコピーして盗んだ ・他人のＩＤを使って不正アクセスをした ・会社の顧客情報を他社に売った ・不法入手した個人情報で架空請求した ・迷惑メールを送った ・その他の犯罪、不法行為	故意の犯罪（27%）		上記に加え ・法知識の習得 （個人情報保護法、不正競争防止法、刑法など） ・デジタルフォレンジック整備	

うっかりミス対策としては表3のように環境・ツール・手順の整備が有効である。その上でミスを起こしても大丈夫なように、フールプルーフ3やフェイルセイフ4のようなしくみを構築しておくことが最も重要である。この部分に機械による自動化システムを活用する。人間のミスを機械でフォローするという考え方である。設定ミスに対しては、これらに加えて、レビュー励行、報告チェックの仕組みをしっかり作って日常の確認活動が重要となる。

ルール違反に対しての効果的な手法は、ルール遵守のためのハードルを下げることである。なぜルールを守らないかといえば、面倒くさいからという理由が多い。ルールを実行する場合に手間がかかる、時間がかかるなどエネルギーが必要なことが問題である。そういった部分には機械による自動化で人間が意識してエネルギーを使わないでもできるしくみを作っておくことである。機械による自動化と抑止を目的とした監視と罰則の周知徹底がこれらに加わり、相乗効果を持つ。ただし、罰則の適用は信賞必罰および公平性と透明性を兼ね備えた運用が生命線となる。

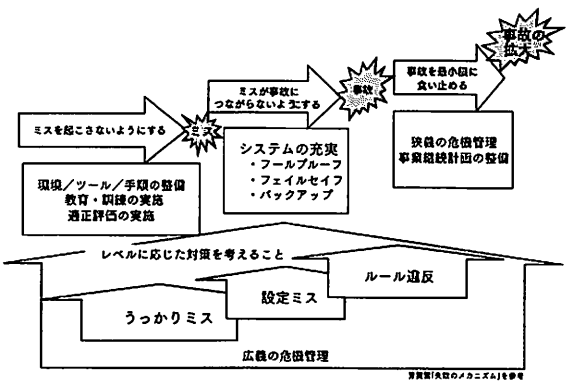


図1. 紛失事故を起こさない手法

これら一連の対策を整理すると、図1のように「ミスを起こさないようにする」「ミスが事故につながらないようにする」「事故を最小限に食い止める」というステップで対処する危機管理の考え方が参考になる5。また、この一連のうっかりミスに故意の犯罪を加えたすべての事象に対して情報セキュリティ監査が有効な対策となる。

3.2 紛失事故に対する備え

うっかりミス対策に続いて、情報を紛失しても“漏洩”しないようにしておくことが肝要である。持ち運びやすいことが特徴のノートパソコンは、その宿命として盗難・紛失が多い。電車の網棚の上に置き忘れた、車上荒しにあった、空き巣に入られたということで盗難にあうリスクが高い。2005年4月5月の報道事故の中の14%がパソコン盗難による紛失事故である。企業の情報セキュリティ事故の中で最も多いのもノートパソコン紛失事故である。こういった事故に対して、ノートパソコンには個人情報を入れない、ファイルやハードディスクを暗号化する、複数段階でのパスワードを設定するなどの対策を導入するのが通例である。最近では、個人情報を格納できないノンディスク型のシンクライアントが脚光を浴びている。個人情報保護という面では情報の分散よりも蓄積と処理の集中化がひとつの選択肢であるともいえる。あるいは紛失したPCやメディアの記憶エリアには一定時間アクセスがなければ自動的にデータ消去するという機能も考えられる。

ノートPCの個人情報紛失届けを監督官庁へ報告した企業の例である。紛失したノートPCはBIOSパスワード、HDパスワード、OSパスワードなどの設定を行っていた。それに加えてハードディスクの暗号化も実施していた。そのようなセキュリティ管理策を実施していたにもかかわらず、監督官庁に紛失届けをしたときに指摘されたのは、個人情報が漏洩したという事実だけであり、多くの管理策を実施していたことはまったく評価されなかったということだ。では企業に指導・推奨している情報セキュリティの一連の取り組みは一体何なのであろうか。国家を挙げて推進しているISMS適合性評価制度やプライバシーマーク制度などで実施しているリスクアセスメントからリスク管理策を実施するという一連の取り組みは何なのであろうか。紛失したことに対する過失責任はあるにしても暗号化などの一連の情報セキュリティ対策の実施をもう少し評価してもいいのではなかろうか。そうでなければ情報セキュリティ対策へのモチベーションは極端に下がってしまう。暗号化も100%安全ではないが、どんな管理策を取ろうともリスクを持った対策に他ならないのであるから。

3.3 不要な情報の削除

個人情報保護法の成立を契機として企業は保有する個人情報の見直しを始めた。どこに、どれほどの、どのような個人情報があるのかを調べあげ、本当にそれらが必要なのかどうかを検討してきたはずである。企業にとって必要な情報だけに絞り込むことが個人情報保護のポイントであるが、その情報の取捨選択に間違いはなかったであろうか。2005年5月20日に日本航空の情報漏洩が報道されたが、それによると航空機の搭乗券の半券369枚を紛失したという。その半券のうち48人分のクレジットカードNo.が流出した可能性が高いという。どうして飛行機の搭乗券にクレジットカード番号を印刷しておく必要があるのであろうか。最近では、クレジットカードの利用明細にもカード番号はマスキングされているし、銀行の口座利用明細にも口座番号は記載されない方向にある。不必要な情報は余計なリスクを増やすだけである。

あるいは、冒頭に記したように企業が集める顧客情報にはリスクと価値のアンバランスなデータ項目がある。セミナー申し込みやアンケートに詳細な情報を記入するが、その情報をもとにアクセスを受けた経験は筆者の場合1割にも満たない。企業は情報を集めても、それだけで満足してしまい、せいぜい統計資料を作る程度であり、実効的な活用ができているのだろうか。企業もいま一度見直しをして、本当に必要な情報に絞り込むことを実践して欲しい。不必要な情報を持っているがために漏洩時に余計な被害を出さないように再度、情報の活用について総点検をすることが必要である。

3.4 厳罰化は業務効率を引き下げる

個人情報の紛失事故が減らない現実に、企業の中には罰則強化に走っているものもある。故意の犯罪あるいは不注意でノートPCを紛失したなどで個人情報紛失を起こした社員は、過失の程度により減給、降格、解雇などの厳しい処分を課すことを表明している企業もある。

ここで注意して頂きたいのは、故意の犯罪と過失を同類として扱わないで欲しいということである。過失は、今まで記してきたように、人間ならどうしても起こしてしまう可能性のあるものである。どんなに注意しても人間の不完全性に起因した事故はなくならない。これを犯罪と同様なルールで厳罰処分してしまうと、忠実で有能な社員たちを犯罪者にしたてあげることになる。業務に熱心で効率の高い社員ほど携帯PCを持ち歩いて会社の事業の効率化に貢献しているし、逆に熱意のない非効率極まりない社員は就業時間以外にPCを持ち歩いて仕事をする意欲もない。すると個人情報を紛失してしまう可能性を持つのは有能な社員ばかりということになる。そういった社員の過失をあげつらって全社員の見せしめにすることが企業にとってどんな結果になるか、言わなくても明々白々である。厳罰化された状況

の中で、既に多くの有能な社員はそのようなリスクをかけてまで携帯PCを持ち歩くことを諦めているようにも見える。業務の非効率化は益々促進されているのである。

厳罰化は情報セキュリティをあらぬ方向へ導く。事故の隠蔽などが起これば、真の原因究明や対策が進まなくなることは危機管理の中で経験済みである。情報セキュリティに対する社員のポテンシャルは下がるばかりとなる。社員の心を萎縮させ、活力を削ぎ、組織の雰囲気を停滞させることほど企業にとって怖いことはない。

3.5 一般市民への説明責任

読者は個人情報保護法に基づく利用目的の通知を目にしたことがあるだろうか。おそらく一般市民ではまったく気がつかないであろう。JR駅のみどりの窓口などに行くと、A4の紙が張ってある。A4の大きさだから1メートルも離れていては何が書いてあるのかまったく分からない。近眼、老眼の筆者の場合は、紙面から40センチ程度に近づかないと、その書面の内容はよく見えない。もちろん、内容は結構難しい表現で書いてあるので、一般人であれば、文字が読めたにしても、全文を読み上げてそれを理解するのに10分以上の時間がかかると思われる。新幹線の切符を買うために並んでいる場で、そのような書面を読む人がいるだろうか。よほど暇な人間か、変わり者だろう。また、周りからもそのように思われるだろうことも想像に難くない。

病院や薬局の待合所にもB4の紙が張ってある。もちろん、細かな文字で書いてあるし、大勢の患者が見ている中で壁の前に立って読む気にはならない。求めても、その紙を配布してくれるところはまずない。

一般家庭にはガス会社から個人情報の利用目的の通知が来ている。検針員が郵便受けに投げ込んでいる場合や新聞広告に入っている場合などがある。通常であれば、単なる広告と同様にすぐにゴミ箱行きである。その内容を読んでも難しい文面が並んでいて、おじいちゃん、おばあちゃんには到底理解できないであろうと思われる。

さらには会社員の方々は、勤務している会社から社員情報の利用目的の通知を受けているはずである。通常は、給与支払いや福祉制度の提供、公的機関への義務を果たすためという利用目的になっているはずであるが、それに加えてこの際とばかりに多くの付帯的な利用目的をあげている場合がある。会社によってはその通知に対して社員の同意まで取得するところもある。このような包括的な利用目的の通知を行い、そのすべての利用目的の同意を一括要求するのも行き過ぎのような気もする。通知された多くの利用目的の中であいまいなもの、第三者提供リストの中の特定名称のないものなど疑義のある場合、どうすればいいのだろうか。これに同意しないと給与もくれないとなると社員は同意ボタンを否応なく押すことになる。

以上のような状況は多くの企業、組織でも同様であろうと思われる。これで利用目的の通知が本当にできているのであろうか。多くの顧客、消費者はその内容を理解しているのであろうか。

IT時代になって企業の提供するサービスは複雑怪奇になった。ISPや通信事業者の多様なサービス内容や料金体系を理解するのに専門家である筆者でも苦労する。サービスを注文したくてもWebサイトの説明だけでは理解できず、窓口に聞いてみるがその疑問が解決できたことがない。あきらかに企業はステークホルダーに対する説明責任を全うしていない。このことは個人情報にまつわるあらゆる説明責任にも当てはめられる。一般市民が理解しやすい、分かりやすい、通知、公表、明示と安心できる親切丁寧な説明が欲しい。

3.6 苦情窓口と現場力の養成

個人情報保護法には、個人情報の主体者からの情報開示・訂正・利用停止などの要求に対応する義務がある。また、苦情処理の努力義務が設けられている。これらの要求にスムーズに対応するノウハウ構築は企業にとってはかなりの労力を要するところである。従来から存在する企業サービスとしてのコールセンターの対応状況を見ると、個人情報の現場対応についてもいくばかりかの不安を感じる。

企業に設置されたコールセンターの現状を解説すると、まず、電話が通じない。最近では電話対応の機械化が進んでいるが、機械アナウンスに従って何度も電話のプッシュボタンを押さねばならない。それを通り抜けても、次には順番待ち状態を告げられ、長い間受話器を持って順番待ちをすることになる。運良く電話がオペレータに繋がって、やっと苦情なり要件を伝えると、それはこの窓口ではないと別の電話番号を告げられる。同様の手順を踏んで、新たに紹介された別の窓口に繋がると、また同じ要件を最初から伝える。それでその要件が解決できればいいが、そのオペレータでは分からない場合は、あらためて連絡するなどということになる。顧客サービスのための機能が、反対にクレーム対象になっているのである。

このように苦情窓口の対応の問題も含めて顧客と接する企業現場の人材教育が課題である。りっぱなプライバシーポリシーを公開しても、最適な利用目的を通知しても、企業の営業所や店舗で実際に顧客と接する担当者が顧客の具体要求に十分な対応ができなければ、顧客や市場の理解は得られない。量・質の両面で窓口の対応力を強化することが望まれる。そのためには、教育・訓練が重要であり、例えば、毎朝の朝礼や連絡会でポリシーを唱和する、昨日の問い合わせの内容を全員でレビューする、日報・月

報などに個人情報保護という項目を設けて定期的に報告させるなどの工夫がいる。或いは情報セキュリティなどの資格制度を活用し、資格保有者に対するインセンティブ制度を設けるなど社内的な奨励のしくみを検討して欲しい。窓口対応能力の高い企業に対する消費者からの信頼は厚い。ユーザからの信頼は企業の宝である。次のような法則があることを肝に銘じたい。

・クレームを訴え解決された顧客は、5～8人にその事実を話す。
・問題を解決できなかった顧客は、8～16人にその悪い経験を話す6。

4. おわりに

個人情報保護法が全面施行された2005年4月以降、以前にも増して情報紛失の事故が多発している。それは個人情報保護では利益は増えないという企業経営者の本音に根ざした形式主義が一因であるとも思える。高邁なプライバシーポリシーは作っても徹底されずに神棚の上に祭ってある。個人情報の洗い出しに注力はしたが、それで疲れてしまい、リスクアセスメントも管理策選定も適当にお茶を濁して実効ある運用に繋がっていない、そういう企業の実態が垣間見えてくる。

実は、日常の企業活動の中の紛失事故をよく調査してみると、ローテクで人間そのものに起因した部分が事故の原因となっている場合が多いのに気がつく。だからネットワーク機器やセキュリティ設備などの機械システムは、人間ならではのミスを補完する意味合いで装備する視点が重要なのである。紛失事故の実体は、企業経営が人間を対象にした現場をおろそかにしているしっぺ返しであるともいえる。

個人情報保護法は、企業の活動を制限するものではない。貴重な個人情報という企業資産を無駄に使うのではなく、さらに有効に活用するための指針でもある。情報漏洩は機械による監視だけで防げるものではなく、人間的な実に泥臭い企業経営そのものに根ざしたところに注力しなければ根絶することはできない。情報漏洩を起こさない企業、即ち社員や顧客を大切にし、個人情報を事業活動に有効に活用する企業だけが今後の21世紀の荒波を生残っていくことは間違いないと思える。

＜参考文献＞

[1] プライバシーマーク制度 （財）日本情報処理開発協会(JIPDEC) http://privacymark.jp/
[2]「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)」
[3] 日本経済新聞
[4] 朝日新聞
[5] ISMS適合性評価制度 （財）日本情報処理開発協会(JIPDEC) http://www.isms.jipdec.or.jp/
[6]（財）日本情報処理開発協会 「ISMS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 －ISMS認証基準（V2.0）－」(平成15年4月21日)
[7] 芳賀繁「失敗のメカニズム -忘れ物から巨大事故まで-」(角川書店) 平成15年11月20日
[8] 芳賀繁「失敗の心理学 - ミスをしない人間はいない-」(日本経済新聞社) 2004年10月1日
[9]黒田勲「信じられないミスは何故起こる - ヒューマンファクタ - の分析」(中央労働災害防止協会) 平成14年6月28日
[10]田中辰巳「企業危機管理 実践論」(文藝春秋) 平成11年6月10日
[11]畑村洋太郎「失敗を生かす仕事術」(講談社) 2003年12月2日
[12]畑村洋太郎「失敗学の法則」(文藝春秋) 2003年10月1日
[13]村上陽一郎「安全と安心の科学」(集英社) 2005年1月19日
[14]広瀬弘忠「人はなぜ逃げおくれるか - 災害の心理学 -」(集英社) 2004年3月23日

＜著者略歴＞

所属：松下電器産業株式会社 にて情報セキュリティコンサルタントを担当
セキュリティ専門資格：
・システム監査技術者／公認システム監査人 ・技術士（情報工学、総合技術監理）
・情報セキュリティアドミニストレータ ・ISMS審査員 など
所属学協会：
①日本システム監査人協会
②日本セキュリティマネジメント学会
③システム監査学会
④日本技術士会
⑤日本プロジェクトマネジメント協会 など

論文・著作：
・IT関連専門誌や業界団体／学協会の技術誌に連載記事や技術論文等を多数執筆

(脚注)
1. 個人情報保護の取組みが組織として十分な状態にあることを認定する第三者認証制度。経済産業省のもと日本情報処理開発協会(JIPDEC)が認証している。
2. 年間52万件(2005年度JAFロードサービスによる)
3. 事前に定義されていないデータを入力したり、誤操作を行った場合でも、誤動作を起こさずに正常に動作するように設計する方法。面倒な手順がいるようにする。
4. 故障や操作ミス、設計上の不具合などの障害が発生することをあらかじめ想定し、起きた際の被害を最小限にとどめるような工夫をしておくという設計思想。機械が故障したり人間がミスをしたりしたら、安全側の状態に倒してしまうというのがフェイルセイフの考え方。
5. 芳賀繁(立教大学 現代心理学部心理学科教授)「失敗のメカニズム」より
6. 「サービス・マネジメント」(カール・アルブレヒト、ロン・ゼンケ共著、ダイヤモンド社) e サティスファイドットコムの調査

平成18年度第6回理事会議事録 日本システム監査人協会

平成18年6月8日(木) 18:30～20:30
於:三井物産(株) 20階3号会議室
出席者 鈴木(信)、小野、橘和、鈴木(実)、吉田(裕)、馬場、蒲ヶ原、斉藤、桜井(由)、須田、力、仲、中山、松枝、若原(中部支部長)、金子(記録)

1. 資料

① システム監査人の「継続教育要項」改定の件
② 公認システム監査人等人数

2. 審議事項

(1) 継続教育要項の改定(鈴木会長)
資料①について会長説明と討議内容は次の通りです。
(前書き)適用は、7月1日からとする。
(項2.3)継続教育実績申告期限
・年末、年始に作業が出来るよう配慮し、1月を申請期間、2月を審査期間とした。
(項2.4)継続教育実績申告方法
・電子メールによる継続教育実績の申告を可能とした。
3年毎の更新申請手続きについては、別途定める。
Q:更新申請手続きに反映させるのはいつごろか?
A:秋の申請に間に合うよう、出来るだけ早く実施する。
(項3.1)継続教育義務時間
・前回の理事会で最低義務時間改定の提案をしたが、その提案は撤回し、今回改めて提案した。今回提案では最低義務時間は現行通りとする。
・主に、継続教育の範囲について「システム監査に関する」に含まれる範囲の変更を行った。
「種別a」…
当協会主催の教育について優遇する。(実時間X1.5倍)
Q:7月1日から適用するとあるが、それ以前の教育は?
A:改訂前のセミナーは、実時間(優遇処置なし)となる。
審査時には改訂前・後をチェックする。
7月1日以降の対象教育については、教育実施の都度その旨を案内する。
「種別b1」…
ISMS審査員研修, プライバシーマーク審査要員補研修を明記した。
Q:記載のないQMS等の審査員研修の取扱いは?
A:準じて取扱う。
「種別b2」…
通信教育及び自主学習を加えた。
Q:記載のない「本」で自主学習した場合の取扱いは?
A:準じて取扱う。
「種別b3」…
情報システムベンダーが主催する製品発表会等を加えた。理由は、ベンダー製品を推奨するという事でなく、これら新製品発表には、最新技術、ノウハウ、考え方について役立つものが必ずあるという判断である。
「種別c」…
実務時間の上限を20時間から30時間に拡大した。
「種別f」…
発生都度の個別審査についての問合せが多いため、継続教育績申請時に審査できるよう書類に添付することをを明記した。
個別審査は、申請を受けてから審査するようにした。(申請者が適切に判断したものは、審査側でも承認できる内容であるだろうという判断があり、研修の都度確認するのではなく、自信を持って申請して欲しい)
(項3.4)最低義務時間に達しない場合の取扱い
・更新時に、それまでの各年30時間(計90時間)を確保しながら、120時間に達しなかった者を救済する処置を追加した。
・海外出張、長期療養等の特別の事情を有する者に資格の一時留保処置を追加した。
→採決の結果本提案は承認された。

3. 報告事項

(1) 公認システム監査人等の人数について（鈴木会長）
資料②について報告

- 公認システム監査人　2006/6/6　現在有効者　343名
- システム監査人補　2006/6/6　現在有効者　239名

(2) 法人部会報告（小野副会長）
- 自治体向け情報セキュリティセミナーは、これまでの希望する自治体主催のセミナーに講師を派遣する形態に加えて、今年度は、法人部会主催でセミナーを実施することも計画している。
- 両方の案内をDMにして、関東地区の自治体約200箇所にDMを出状する。
- 各支部には、昨年度に引き続いて、担当地域でのDM発送のご協力をお願いする。別途、支部長に依頼するので、ご協力をよろしく。

(3) 公認システム監査人利用推進（力理事）
- 会合を6月からスタートさせたい。
- 今後の進め方について、アンケートを実施して参考としたい。
- 東北支部から「公認システム監査人認定証」の発行を求められて検討中である。「公認システム監査人認定証」のサンプルを理事会席上で回覧。
(写真入、ラミネートシールでコーティング、原価30円程度)

Q：「公認システム監査人認定証」の作成については、以前、理事会に提案されたが、提案趣旨の再検討として取り下げられた経緯がある。
受付、発行の事務は事務局作業であるため、事務局と十分相談し、運用を明確にした上で再提案をして欲しい。

A：今回は状況報告であり、具体案を作成し再提案する。

(4) 会報（須田理事）
- 6月号は既に発送した。
- 次号は8月発行予定で計画中である。

(5) 教育研修委員会（鈴木（実）副会長）
- 特認研修機関への希望企業が1社有。申請書を提出するよう連絡する。

(6) 中山理事報告
- 名古屋で認定委員を務めた。
- 所属企業が変更になる(理事会メールで連絡済)

(7) 月例研究会（仲理事）
- 第120回月例研究会：
開催日：5月22日（月）
テーマ：
「新JIS(個人情報保護に関するマネジメントシステム－要求事項)の概要とシステム監査」
講演者：
財団法人日本情報処理開発協会
プライバシーマーク推進センター
副センター長　関本　貢　氏
参加者数：約170名
- 第121回月例研究会：
開催日：7月3日（月）
テーマ：「システム監査とJSOX」
講演者：日本大学商学部　教授
堀江　正之　先生
参加予定者数：6/12現在約250名の申し込みを受付けている。
- 第122回月例研究会：
テーマ、講師等調整中
- 11月の月例研で講師をお願いしている前理事の指田氏が副理事長を勤める団体（NPO 事業継続推進機構）において7月10日に設立記念セミナーが開催されるのでお知らせする。

(8) システム監査基準研究会（松枝理事）
- 第3回定例会議を6月16日に開催した。
- JSOX法について勉強会を実施中。
参照資料：「サーベイランス・オクスリー法（企業改革法）遵守のためのIT統制目標」（日本語版：ISACA東京支部）

(9) 中部支部報告（若原支部長）
- 5月20日　例会を実施した。
- 5月27,28日　システム監査実践セミナーを実施した。
- 名古屋で公認システム監査人の面接を行う。

(10)ホームページ（馬場理事）
- ホームページに「メールアドレス変更申請」及び「得意分野情報の変更申請」ページを追加した。近々リリースする予定。

(11)事例研究会（吉田副会長）
- 定例研究会では、日本版SOX法の勉強を行っている。今後は、日本版SOX法検討ワーキングを発足させ、セミナー又は研修会が出来るように考えている。
- 7月8,9日の東北支部実践セミナー申込みは現在1名のみである。再度募集案内を行う。
- 実践セミナー、実務セミナーを共同又は主催で実施したいと希望している企業が2社あり。セミナー受講生の募集には苦労しており、会報やホームページの案内だけでは多くを望めないため、協賛する企業、団体に案内してもらうことも必要であると考えている。
採算面や事務労力を考えると、多くの受講生確保を望める企業と一緒にやることも必要と考えている。

(会長) 企業と協賛することに対する不安は何なのか。

(吉田副会長) 特に無いと考えます。

(会長) 不安が無いのであれば、他企業との提携については、進めて欲しい。
実務セミナー年2回の計画にこだわる

ことなく、実現性の高いものからどんどん実施して欲しい。

(12)JIPDEC訪問について（鈴木会長）

- 5月30日にJIPDEC高取氏を訪問し、ISMS審査員資格取得及び更新の条件に、システム監査技術者は含まれているが公認システム監査人が含まれていないことに対し、理由の説明を求めるとともに、含めることの要請をおこなった。
- 高取氏は「システム監査技術者を入れているから良い」と考えていることから、「公認システム監査人は、特認制度もあり全員がシステム監査技術者ではない」旨回答した。その後論議になり結論の出ないまま、特認の内ISMSの審査経験者が何人いるかを調査することを約束し打合せは終了した。

(13)登記簿変更について（鈴木会長）

- 蓮見理事の代行で登記簿変更を行った。（本日提出済み）
- 定款について次の問題点を指摘されたが、見直しする条件で申請は受理された。
- 「本協会の定款では、役員の任期は2年であるため、就任の総会から2年を経過した日より後に総会を開催した場合、2年を経過した日から総会までの間は役員がゼロという状態が発生する。」
- NPO 法ではこの場合の救済処置があるため、本協会の定款を救済処置に合わせるよう変更する必要あり。

以上

議　　長　鈴木信夫
議事録署名人　金子長男
　　馬場孝悦

支部活動報告
近畿支部　第96回定例研究会活動報告

日　時　平成18年5月19日(金) 19:00～21:00
場　所　国際カンファレンスプラザ会議室
テーマ　内部統制に役立つ情報技術
講　師　森末　清成　氏（当協会会員）

講演概要

内部統制を、単に証券取引法等の法規制に関するものと限定せず、システム監査技術者として、実際に企業実務に携わる実務家の立場から、内部統制の機能を整理し、その機能を実現するための情報技術を具体的に対応させて簡潔にわかりやすく解説していただいた。

No.1472 近畿支部会員 筆島　務

内部統制の目的を事業責任の確保、社会規範の尊重、事業資産の保全と位置づけた場合、具体的な内部統制のプロセスは組織により千差万別であるが、費用対効果を配慮して効果的に構築しなければならない。また、内部統制のポイントはモニタリング、組織風土の醸成、リスク認識と対策、第三者評価などであるが、人手だけに頼ってそれらを行うことは非能率である。そこで、情報と通信の技術を利用する。

内部統制のサイクルは、事業と組織の理解、目標の設定、対応策の策定、準備と定着化、監視と分析という5つのプロセスを回すことであるが、監視と分析は、機械向きのプロセスである。内部統制の階層を経営層、管理層、実務層、個人層に分けて考えると、経営層は、企業内部、株主、地域社会、顧客、銀行、調達先などとのプロセス連鎖の上に内部統制を構築する。さらに、管理層は、情報システムの支援を受けながら、市場競争力、利益率といった要求に対して、コストの削減、品質確保、在庫削減、納期保証などのプロセスを通じて、売上高、製品競争力の増大を達成し、顧客満足を拡大する。また、実務層の内部統制は、上流プロセスから受け入れた物、価値、情報を生産性指標、品質指標、リスク管理などの指標にしたがってプロセス管理し、モニタリングと継続的改善によって、付加価値をつけた上で下流プロセスに渡すことである。

内部統制は、各層における個別プロセス連鎖が、戦略的事業目標、構成員の意識と企業文化によって、相互に連鎖しながら、全体としての資源の効率的使用を達成するものである。

内部統制に必要な機能を達成するための情報技術として、認証と権限管理、エラーチェック、ワークフロー、ログの取得、リアルタイム処理、ベースライン分析、多次元解析、データマイニングなどがある。

内部統制は、いろいろな観点から検討されるべきであり、財務報告だけが目的ではなく、また、各層によって統制の内容が変わる。ICTの活用で有効かつ効率的な内部統制が期待できる。

以上

日本システム監査人協会西日本支部合同研究会開催のご案内

謹啓　盛夏の候　益々ご清栄のこととお慶び申し上げます。
平素から格別のご高配を賜り厚く御礼申し上げます。
中部支部・北信越支部・近畿支部・中国支部・九州支部で西日本支部合同研究会を開催することになりました。ご多用の事と存じますが、是非ご出席くださいますようご案内申し上げます。

－記－

日本システム監査人協会西日本支部合同研究会

【開催日時】2006年10月7日（土）13:00～17:00
【場　　所】RCC文化センター 〒730-0015 広島市中区橋本町5-11
TEL：082-222-2277 FAX：082-222-2270
ＨＰ：http://www.rccbc.co.jp/index.html
地図：http://www.rccbc.co.jp/img/map01.gif

【メインテーマ】情報化社会におけるシステム監査人の役割と未来
【プログラム】開会のご挨拶　13:00～13:20（20分）　中四国支部　高田 裕史（2006年度幹事）
セッション１：「セキュリティとICタグ」（仮称）　13:20～14:10（50分）
中部支部　　堤　薫　様
セッション２：テーマ未定　14:10～15:00（50分）
北信越支部　森様またはその他の代表者（未定）
― 休憩 15:00～15:10（10分）―
セッション３：「JISQ15001：2006に基づくプライバシーマークについて」（仮称）
15:10～16:00（50分）　近畿支部 喜多　陽太郎　様
セッション４：「ITILとシステム監査」　16:00～16:50（50分）
九州支部 中溝　統明　様
閉会のご挨拶　16:50～17:00（10分）
2007年度幹事予定支部代表者予定
※発表者、発表内容等変更になる場合があります。
【会　費】会員：1,000円　非会員：2,000円
【定　員】50名（定員になり次第締め切らせていただきます。）

懇親会及び大和ミュージアム見学のご案内

【懇親会】合同研究会で、支部会員の親睦を深めることを目的として、セミナー終了後、懇親会を開催したいと思います。
2006年10月7日（日）18:30～20:30　広島市内　場所未定
（参加当日にご連絡申し上げます。）予算3,000円～4,000円程度
【大和ミュージアム見学】遠方からお越しの方でご宿泊の方と合同研究会翌日観光を行いたいと思います。
2006年10月8日（日）09:00～
【西日本合同研修会・懇親会・大和ミュージアム観光に関するお問い合わせ】
日本システム監査人協会　中四国支部　高田　hiroshi.takada@jp.pwc.com

【参加申込】下記の申込み内容を記入の上E-Mailでお申込下さい。
（E-Mail：hiroshi.takada@jp.pwc.com）
【申込期限】2006年9月22日（金）
日本システム監査人協会西日本支部会　参加申込書
1．氏名
2．会員番号（非会員の場合は記入しないでください）
3．連絡先
4．E-Mail
5．参加するものにチェックしてください
□ 西日本支部会
□ 懇親会
□ 呉市海事歴史科学館見学

会員執筆の書籍紹介

No.841　沼野　伸生

「リスク図による　情報セキュリティ監査の実践」

島田裕次　著
＜同文舘出版／2006年4月15日初版発行／
A5版218頁／定価（2,500円＋税）＞

情報セキュリティに関する書籍は巷に溢れています。しかし、情報セキュリティ監査実践の書はまだそう多くはありません。そういう中で、本書は、当協会の会員である島田裕次氏が、ご自身の長年に亘る監査実務経験を踏まえ、情報セキュリティ監査をどのように実施すればよいのかを、実践的にまとめた書です。

著者の島田氏は、東京ガス㈱の監査部情報システム監査グループマネジャーとして監査実務に長年携われ、また、現在情報処理技術者試験委員、日本大学商学部の非常勤講師もされています。

本書の特徴の第一は、情報セキュリティ監査実践の手法として、「リスク図」の活用を提案している点です。「リスク図」は監査対象となる部門やプロセスを図に描くことによって、リスクを把握し、それを低減するためのコントロールを、点検・評価しやすくしようとするものとされています。本書の中では、この「リスク図」作成のポイントや、実際の「リスク図」の例を多く示し、その活用方法を平易に解説しています。

そして特徴の第二は、監査工程毎、また監査テーマ別に、著者島田氏の長年の監査実務経験を踏まえた、情報セキュリティ監査実施に当たっての実務家の着眼ポイントが随所に織り込まれ、難解な理論書や、単なる知識整理型の本とは一線を隔す、文字通り情報セキュリティ監査実践の書になっている点です。

本書は、別掲の目次にあるとおり、情報セキュリティ監査を取り巻く環境、「リスク図」によるアプローチ、そしてシステムライフサイクル毎・監査テーマ毎の監査の進め方・留意点のポイントが網羅的に述べられ、また多くの「リスク図」が盛り込まれていることから、紙面の関係上、個々の内容についての詳細な論述というより、そのポイントを網羅的に整理した内容になっています。従って、ベテランの監査人には、実務遂行上の要点確認に、また、これから情報セキュリティ監査に取組もうとする人にとっては、監査実践に当たっての着眼点を知るという上で絶好の書といえます。

本書のような、実務に携わる方の、その経験に基づいた実践の書の積み重ねが、情報セキュリティ監査のレベルを一層向上させ、ひいては情報社会のセキュリティレベル向上に寄与するものと思います。

是非、ご一読下さい。

＜目　次＞

《編集後記》

今号の会報記事は、期せずして個人情報保護についての特集になりました。

5月20日に、日本規格協会からJIS Q 15001:2006版が発行になり、規格の名称も「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」から「個人情報保護マネジメントシステム－要求事項」に変わりました。ISMSも5月20日に日本規格協会からJIS Q 27001:2006版として発行されました。個人情報保護マネジメントシステムはPMSという名称で情報セキュリティマネジメントシステムISMSと並ぶ存在になります。

当協会においては、今号の特集記事にも説明があるように個人情報保護監査研究会のメンバーによる「個人情報保護マネジメントシステム実践マニュアル」(新JIS Q 15001対応)(仮称)を、近々、出版する予定です。会員諸氏には、ぜひ、ご購入をお願いし、個人情報保護の実務に役立てて頂きたいと思います。

さて、いわゆる日本版SOX法への注目が集まっています。月例研究会では7月3日に「システム監査とJSOX」をテーマに掲げて研究会を開催しましたが満席の状況でした。上場企業において対応する時期が2008年4月からであれば、対応まであと2年をきっています。当協会では基準研究会で、鋭意、研究が進められています。

今号では、個人情報保護に関する会員論文を掲載しています。コンプライアンスからマネジメントシステムまでシステム監査に関わることであれば何でもテーマにして頂いて論文募集に応募をお願いしたいと思います。一人で論文執筆はおっくうになるところをひとつのテーマを論壇風に二人の会員が論文を書くというのもおもしろいかと思います。 (AN)

発行所 特定非営利活動法人 日本システム監査人協会
発行人 鈴木 信夫
事務局 〒103-0025
東京都中央区日本橋茅場町2-8-8
共同ビル(市場通り)6階65号室
TEL. 03(3666)6341 FAX. 03(3666)6342
事務局メール：saajjk1@titan.ocn.ne.jp
ホームページ http://www.saaj.or.jp/

会報担当委員
竹下 和孝 富山 伸夫
須田 勉 吉田 裕孝
木村 陽一 仲 厚吉
藤野 明夫 森本 哲也
山田 正寛

※会員のみなさまからの投稿(連載、随筆等何でもOK)を募集します。記名記事は薄謝進呈します。書籍紹介欄もありますので、執筆されたかたはお知らせ下さい。
会報担当メール：saaj-kaihoh@yahoogroups.jp