個人情報保護専門監査人部会
活動報告

2008年6月6日
個人情報保護専門監査人部会

個人情報保護専門監査人部会の状況

◆ 個人情報保護専門監査人　2008年5月現在　49名

◆ 部会の構成と主要WG

- 部会長　　稲垣　隆一（弁護士）
- 部会長補佐　　黒澤　兵夫（TAKE国際技術士研究所）

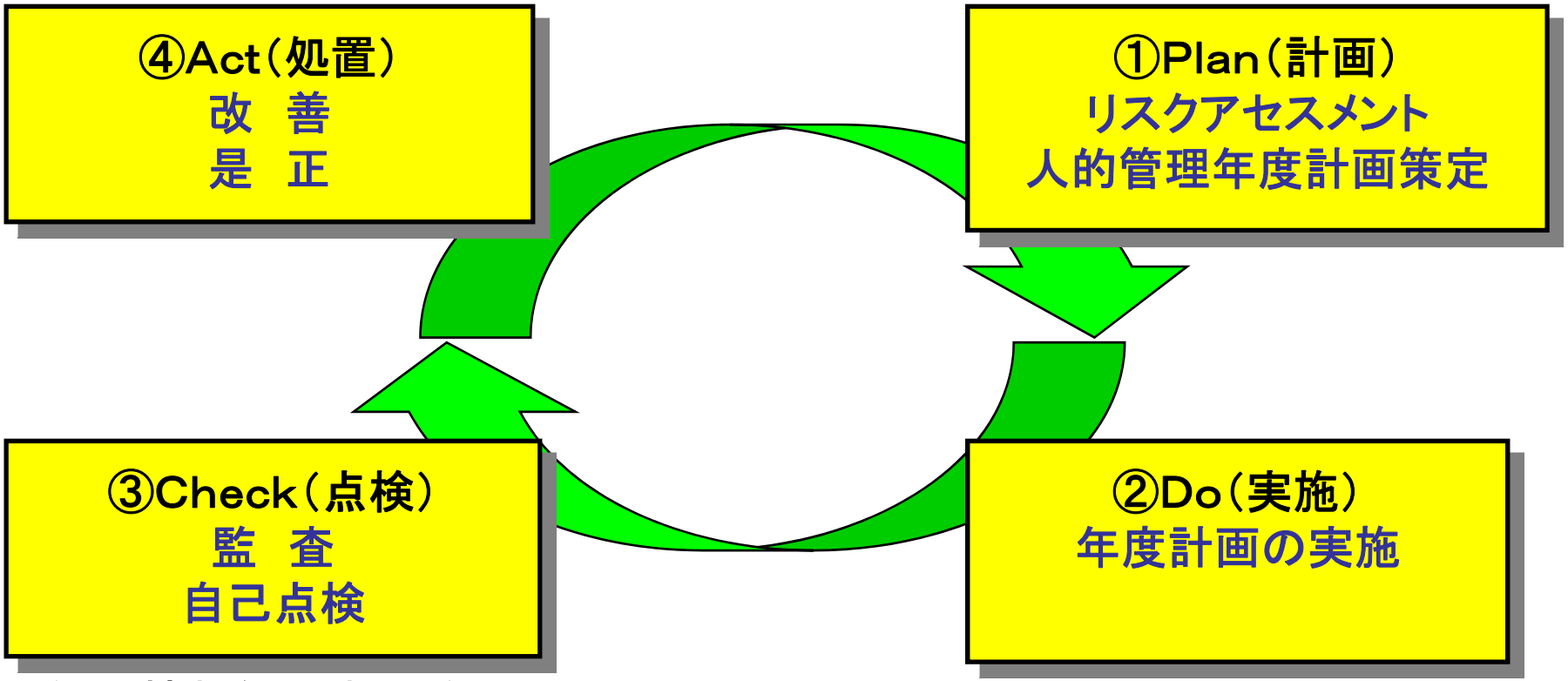
- WG1　個人情報保護の管理基準の検討
  主査　清水　政幸
  ⇒ テーマをWG1-1 と WG1-2 に分けて検討している。
- WG1－1　人的管理基準強化の検討
  主査　斉川　夏樹
- WG1－2　OECD8原則を実装した情報システムの
  システム監査基準の検討
  主査　舩津　宏
- WG2　最近の個人情報関連の事件事故事例
  主査　広口　正之
- WG3　個人情報保護のための内部統制の考察
  主査　古川　研吾

WG1－1

人的管理基準強化の検討
（監査チェックリストの検討）

人的管理のPDCAサイクル

1. 人的管理のPDCAサイクルを強化する。
2. 人的管理のリスクアセスメントを実施する。
3. 特に、PDCAサイクルのP(計画)とC(点検)を強化する。



(個人情報保護専門監査人)

P(計画)の強化内容(その1)

1. 人的リスクアセスメントを適切に実施する。

- ◆ 脅威の検討
  - ▶ 外部の脅威、内部の脅威、ヒューマンエラー
- ◆ 脆弱性の検討
  - ▶ 対策の基準やルールがあるか
  - ▶ 社員等が基準やルールを認知しているか
  - ▶ 社員等が基準やルールを遵守しているか
  - ▶ 基準やルールが定期的に見直されているか
- ◆ リスクの把握(重要な個人情報ﾃﾞｰﾀﾍﾞｰｽ単位で)
  - ▶ リスク値＝個人情報DBの重要性×脅威×脆弱性
- ◆ 対策の決定
  - ▶ リスクの低減(対策)、受容、回避、移転

P(計画)の強化内容(その2)

2. 人的管理の年度計画を作成する。

(1) 定期的見直しの年度計画

- 人的管理リスクアセスメントの見直し
- 人的情報セキュリティ対策、特にリスク低減対策の見直し
- 情報セキュリティ対策基準とマニュアルの見直し
- 職務権限とアクセス権の見直し
- 人的管理体制と人的監視体制
- 社員遵守事項あるいはルールの見直し

(2) 職制による人的管理の年度計画

- (個人情報取扱い)担当者の面接計画
- 担当者の情報セキュリティ／個人情報保護に関する評価計画
- 日常的管理の計画(朝礼、会議、パトロール等)

続き

(3) 教育と啓蒙活動の年度計画

(4) 自己点検年度計画

(5) 監査年度計画(内部監査／外部監査)

(6) アクセス制御点検の年度計画

- IDとパスワード管理の点検
- アクセス権管理の点検
- 特権IDとパスワード管理の点検

(7) 外部人材管理の年度計画

- 派遣社員と臨時社員等の管理
- 外部委託管理

(8) 電子メールの運用ルール

C(点検)の強化内容と監査ポイント

1. C(点検)の強化内容

- ◆ 人的管理の年度計画があり、トップマネジメントに承認されているか。
- ◆ 人的管理年度計画どおりに実施されているか。
- ◆ 実施結果は有効であると評価されているか。
- ◆ PDCAサイクルが回っているか。

2. 個人情報保護専門監査人による監査のポイント

- ◆ 人的管理PDCAサイクルが有効に回っているか。
- ◆ 人的管理のリスクアセスメントが実施されているか。
- ◆ 有効な人的管理年度計画が策定されているか。
- ◆ 年度計画の実施が有効に評価されているか。
- ◆ マネジメント層が実質的！にコミットしているか。
- ◆ 管理者と社員等の意識が高いか。

WG1－2

OECD8原則を実装した情報システムのシステム監査基準の検討

OECD8原則を実装した情報システムのシステム監査基準

・OECDの8原則は、個人情報を利用するものにとってのコンプライアンスモデルと言える。
・そこで、OECD8原則を実装した情報システムを検討し、この情報システムの要求事項を整理する。
・この要求事項をもとに、「OECD8原則を実装した情報システムのシステム監査基準（管理基準）」を検討する。

④利用制限の原則より、検討開始

④利用制限の原則
データ主体の同意がある場合や法律の規定による場合を除いて、収集したデータを目的以外に利用してはならない。

＜言い換えると＞
＝＞収集目的への合致が確認できない場合、データ利用ができないようになっていること

情報システムのモデル（企業運営システム（インハウスシステム））

企業運営システム（インハウスシステム）をモデルに要求事項を検討する。

企業運営システムのモデル

企業運営システムとは、企業活動で必要とされる従業者及び取引先の管理システムの意味で使っている。

一般的な利用目的

従業者の個人情報の利用目的
- 労務管理（勤務管理、業績管理、給与管理、福利厚生・健康管理、内部統制・安全管理）
- 事業運営上の窓口・連絡
- 個別の福利厚生や業務活用のための個人情報の提供

取引先の個人情報の利用目的
- 契約上の当事者
- 事業運営上の窓口・連絡
- 安全管理のための記録

企業運営システムの「利用制限の原則」に対する要求事項（案）

①利用目的対応の処理を実装し、それ以外での処理ができないようになっていること。

②例外的対応については、取り扱いが権限者に限定されること。

③役割、機能毎に利用目的（利用範囲）を限定すること。

④個人毎に同意を得た利用目的を管理すること。

⑤利用目的の同意済みの判断は、個人毎に行い、同意を得ていない場合、利用できないように制限されること。

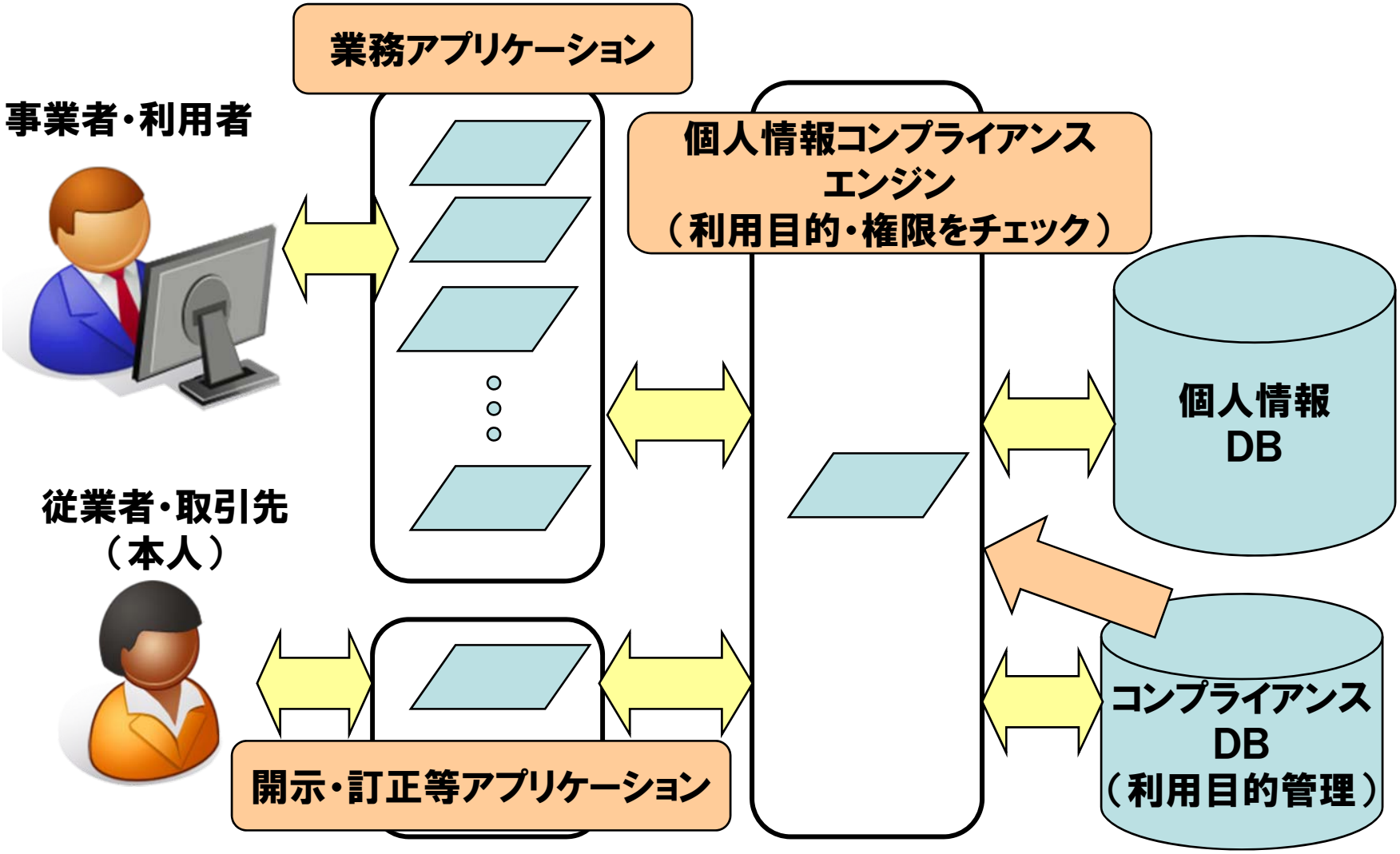
企業運営システムの実装仕様（検討中）

詳細仕様（検討中）

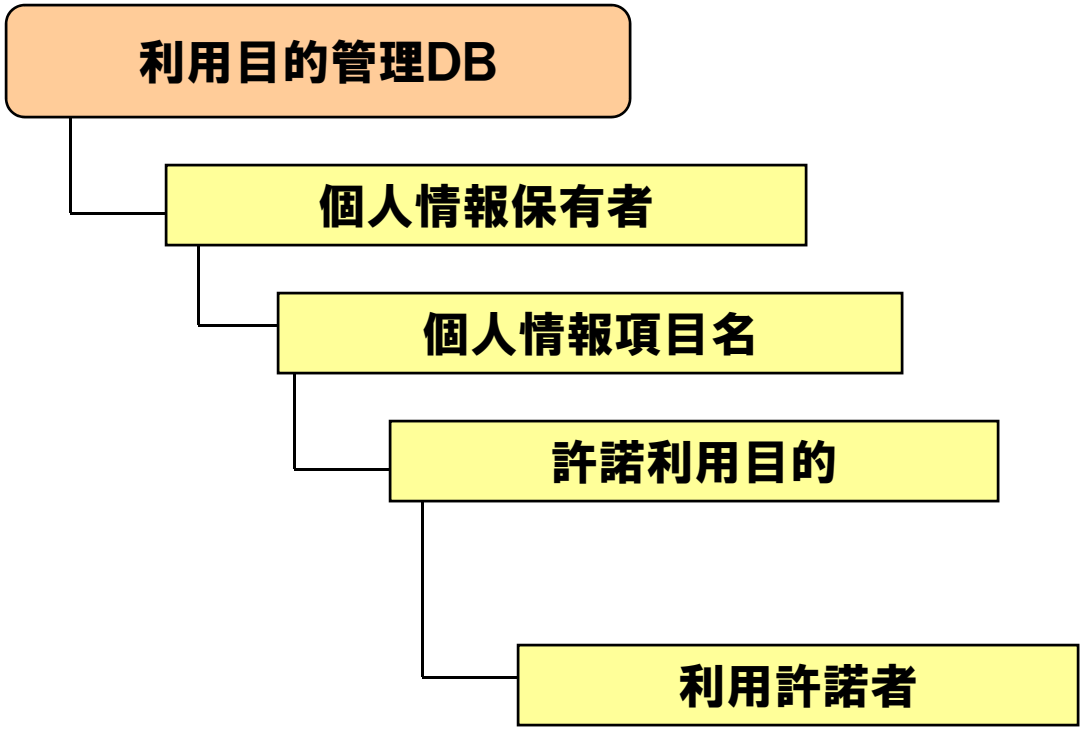
①利用目的対応の処理を実装し、それ以外での処理ができないようになっていること。

●個人情報DBを公開しない。
- **業務アプリケーションを介して利用する。**
- **DB自体は暗号化する。**

企業運営システムモデル（検討中）



コンプライアンスDB（検討中）



例

山田　太郎

携帯電話番号

通常連絡
（携帯連絡先表示のある
参照アプリケーション）

総務部員、部長、課長、
係長、同僚A、同僚B

WG1－2の今後の予定

◆システム監査基準(管理基準)の検討

現在、要求仕様をもとに実装仕様(DB構造)等を検討している段階です。
今後は、実装仕様の整理の中で要求仕様を見直し、システム管理の基準としてまとめる予定です。

WG2

個人情報保護の事件事故の解析

最近の事件事故の概観

- ◆公表事例で1000件弱（2006年）
- ◆プライバシーマーク取得事業者で708件（2006年度）
- ◆大規模漏洩、大規模紛失案件が発生
- ◆紙媒体、電子媒体：紛失、盗難が多い
- ◆電子データ：内部からの持ち出しが多い
- ◆Winny経由も依然として多い

利用可能な事件事故情報

- ◆ 国民生活センター
  - 消費者からの相談事例：全体で11,574件、うち漏えい紛失2,760件
  - 「2006年度 個人情報に関する相談の概要」2007年5月
- ◆ 警察庁
  - 「不正アクセス行為対策等の実態調査」2008年2月
  - 613の会社、機関から回収したアンケートに基づく分析
- ◆ 日本情報処理開発協会（JIPDEC）
  - 「個人情報の取扱いにおける事故報告にみる傾向と注意点」2007年6月
  - プライバシーマーク取得事業者中、439社で 708件の事故
- ◆ 日本ネットワークセキュリティ協会（JNSA）
  - 「情報セキュリティインシデントに関する調査報告書」2007年7月
  - 公表事例を集計分析、2006年の事件事故は 993件、2200万人分

事件事故事例：印刷業D社

◆ 事件事故の経緯

- 2007年3月発表、863万件漏洩
- 委託先社員が故意に光ディスクを持ち出す
- 持ち出した個人情報を詐欺グループに売却、実被害発生
- 保険会社、信販会社、プロバイダなど、43社分流出
- 東京地裁は、元社員に窃盗罪で懲役2年、執行猶予5年の判決

◆ 監査のポイント

- 委託先からの事件事故が多い ⇒ できるだけ自社でやる
- 権限を持つ者の故意の行為は防げない ⇒ 極力、人を限定する
- 牽制を効かせているか ⇒ アクセスログの取得・点検

事件事故事例：日本郵政公社

◆ 事件事故の経緯

- 2007年9月10日公表、1,443万件紛失
- 保存期限終了前の書類を誤廃棄
- 全国すべての貯金事務センター11箇所と沖縄支社
- 自動移替利用申込書 368万件、郵便振替払込書 277万件など
- 保存書類は、保存期間の異なるケースも含め、約1800種類ある
- 内規で書類ごとに1カ月－50年の保存期間が決まっている
- 法改正やサービス内容改善に伴い、保存期間をたびたび変更

◆ 監査のポイント

- 複雑すぎるルールは守れない ⇒ ルールを簡素化する
- 改訂内容が現場に浸透していない ⇒ 分かりやすく表示する

WG3

個人情報保護のための
内部統制の考察
～最終報告～

活動計画

◆ 実施項目（3年間）

① 公表された基準類の枠組の利用・反映方法等を検討

- ✓ 実施基準
- ✓ COBIT for Sarbanes-Oxley　etc.

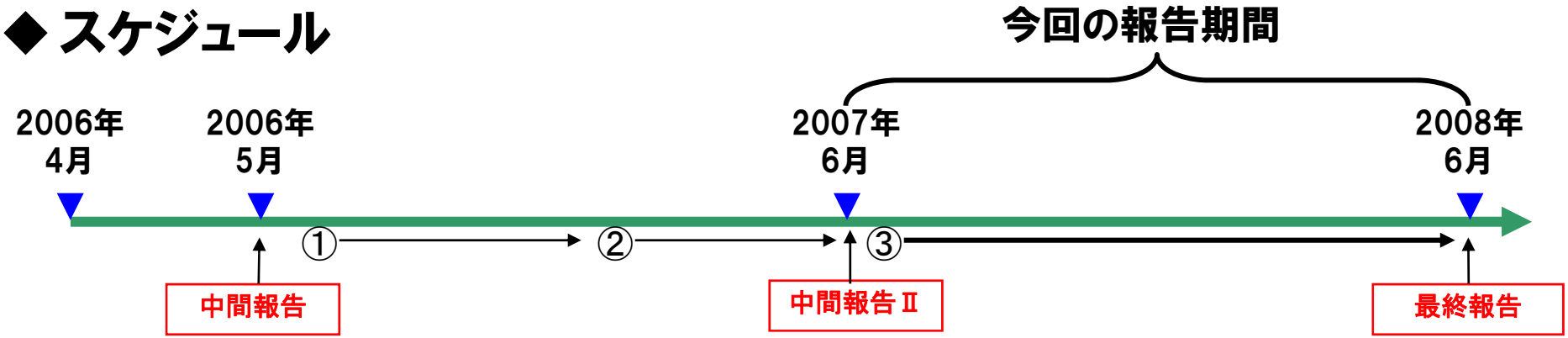
② 具体的な内部統制手続の提示

- ✓ 個人情報保護のための具体的な内部統制としての管理手続の体系化と提案

③ 監査ツールの開発

- ✓ 個人情報保護の内部統制についての監査技法の検討
- ✓ システム管理（監査）基準のサブセットとしてのチェックリスト作成
- ✓ 実際の評価作業でのフィードバック収集

◆ スケジュール



活動の経過と成果(2007/6～2008/5) その1

1. 昨年度からの継続課題 ー 内部統制手続の具体化

- 実践的な内部統制評価に役立つ構成

  ⇒「評価チェックリスト」として作成

- チェックリストに関連した監査技術の体系化
  - ✓ 評価チェックリストをまとめる過程で検討実施
  - ✓ ほぼシステム監査または情報セキュリティ監査における監査技術(手続き)と同一で、異なるものではない。
  - ✓ 技術的な分野(アクセス、プライバシーセキュリティ等)については、有用であるためさらに検討した。

WG3

個人情報保護 – 内部統制の評価チェックリスト(例)

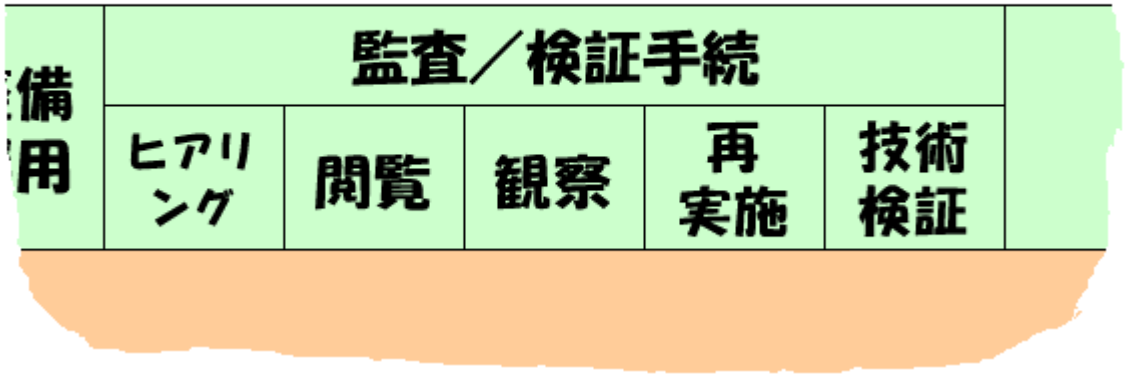
No.	原則の規準	統制の例示と説明	対象区分	評価の対象例示	整備運用	監査／検証手続 ヒアリング	閲覧	観察	再実施	技術検証	統制評価手続	評価並びに検出事項
(プライバシーのためのセキュリティ)												
8.2.5	個人情報が、インターネット、公衆回線、メールによって伝達される場合、個人情報の転送、受信のための業界標準の暗号化技術を利用して、保護される。	下記のシステムと手続が採用されている。										
		・情報の機密保持、伝達、インターネットあるいは他の公衆回線で伝送された個人情報の適切な保護に対処する。	規則	個人情報保護規程、プライバシーポリシー	整備		☆				制定されている規定上、機密保持ポリシーに関する規定をレビューしその関連と妥当性を確かめる。	
			作業	作業マニュアル	整備			☆			プライバシーポリシー等をうけて、具体的な作業マニュアルに記載又は参照指示等がなされていることを確かめる。	
		・暗号化と内部統制の最低レベルを定義する。	規則	個人情報保護規程、プライバシーポリシー	整備		☆				制定されている規定上、情報の暗号化に関する規定をレビューし、実際の統制手続きとの関連性と妥当性を確かめる。	
			作業	作業マニュアル	整備			☆			プライバシーポリシー等をうけて、具体的な作業マニュアルに記載又は参照指示等がなされていることを確かめる。	
			IT	アプリケーションテスト	運用					☆	暗号化の実装方法について、アプリケーションレベルのコントロールを確認する。運用に当たってのテスト記録を入手し、妥当性を検討する。	
		・個人情報の転送、受信に対して業界標準の暗号化技術(例えば、128ビットのSSL)を利用する。	規則	個人情報保護規程、プライバシーポリシー	整備		☆				制定されている規定上、機密保持ポリシーの規定をレビューし、暗号化の項目の内容を検討しその妥当性を確かめる。	
			IT	アプリケーションテスト	運用					☆	暗号化の実装方法について、アプリケーションレベルのコントロールを確認する。運用に当たってのテスト記録を入手し、妥当性を検討する。	
		・外部のネットワーク接続を承認する。	規則	個人情報保護規程、プライバシーポリシー	整備		☆				制定されている規定上、機密保持ポリシーに関する規定のうち、外部のネットワークとの接続に関する事項をレビューしその関連と妥当性を確かめる。	
			作業	作業マニュアル	整備			☆			プライバシーポリシー等をうけて、具体的な作業マニュアルに記載又は参照指示等がなされていることを確かめる。	
			作業	ネットワーク図	運用		☆			☆	最新の(更新された)ネットワーク設計図を入手し、論理構成、物理構成について妥当性を検討する。	
			IT	セキュリティ環境設定	整備・運用					☆	特に外部ネットワークとの接続部分(ルーター、ファイアウォール等)については環境設定の内容について妥当性を検討する。	
		・メール、運送業者、その他の物理的手段によって送られた情報を保護する。	規則	個人情報保護規程、プライバシーポリシー、文書管理規程	整備		☆				制定されている規定上、個人情報を含む書類等が適切なルールに基づき配布される際に、物理的手段の適切な選定がなされていることを確認する。	
			作業	作業マニュアル	整備			☆			プライバシーポリシー等をうけて、具体的な作業マニュアルに記載又は参照指示等がなされていることを確かめる。	
			作業	配送記録、受領記録	運用			☆			配送記録や受領記録を入手し、送られた情報が漏れなく確実に到着していることを確かめる。別途、配送途中での事故報告があれば内容を吟味し、対応の妥当性を検討する。	
8.2.6	個人情報を保護している重要な管理的、技術的、物理的保護措置の有効性のテストが少なくとも毎年行われる。	下記のシステムと手続が採用されている。										
		・個人情報を保護している重要な管理策、技術的、物理的保護措置の有効性を定期的にテストする。	規則	個人情報保護規程、プライバシーポリシー	整備		☆				制定されている規定上、管理策や保護措置の有効性をテストする規定を確認し、その内容の妥当性を確かめる。	
			作業	作業マニュアル	整備		☆				プライバシーポリシー等をうけて、具体的な作業マニュアルに記載又は参照指示等がなされていることを確かめる。	
		・内部、あるいは外部監査人を利用してセキュリティ内部統制の独立した監査を定期的に受ける。	規則	個人情報保護規程、プライバシーポリシー	整備		☆				制定されている規定上、内部、あるいは外部監査人を利用してセキュリティ内部統制の独立した監査を定期的に受ける旨の規定を確認し、その内容の妥当性を確かめる。	
			作業	作業(監査)マニュアル	整備		☆				プライバシーポリシー等をうけて、具体的な監査実施項目を作業マニュアルに記載又は参照指示等がなされていることを確かめる。	
			作業	監査報告書、監査調書	運用	☆	☆				セキュリティ内部統制を対象とした監査の監査報告書、監査調書等を入手し、指摘事項・改善提案等を確認する。必要であれば監査人から内容についてヒアリングを実施する。	

個人情報保護 – 内部統制の評価チェックリスト(例)

対象区分:
- **規則(規定等)**
- **作業(人間系作業)**
- **IT(情報システム)**

- **対象区分、手続き区分等を追加し、使用環境に応じてカスタマイズ可能な形式とした。**

No.	原則の規準	統制の例示と説明	対象区分	評価の対象例示	整備/運用	監査/検証手続					統制評価手続	評価並びに検出事項	調書番号	統制評価結果
						ヒアリング	閲覧	観察	再実施	技術検証				
(プライバシーのためのセキュリティ)														
8.2.3	個人情報への物理的アクセスが(個人情報を含んでいるか、あるいは保護する企業のシステム構成要素も含めて)どんな形式についても制限される。	下記のシステムと手続が採用されている。 ・ハードコピー、アーカイブ、バックアップコピーを含めて、個人情報への論理的、物理的アクセスを管理する。	規則	個人情報保護規程、プライバシーポリシー、アクセス管理規程	整備		☆				制定されている規定上、個人情報への論理的・物理的アクセスが制限されていることを確認する。			
			作業	個人情報取扱記録、入退出記録	運用		☆	☆			ハードコピー、アーカイブ、バックアップコピーを含めた「個人情報取扱記録」を確認する。また、物理的な個人情報へのアクセスの管理簿としての「入退室記録」をレビューする。			
		・個人情報へのアクセスログを取得し、モニタリングする。	規則	個人情報保護規程、プライバシーポリシー、アクセス管理規程	整備		☆				制定された規定上、個人情報へのアクセスに際してはアクセスログを取得するルールが存在すること。及び、アクセスログを定期的にモニタリングする手順があることを確認する。			
			作業	アクセスログ解析結果、レビュー結果報告書	運用			☆			アクセスログの解析結果または、レビュー結果報告書等を入手し、定期的に、適切な項目が確認されていることを確かめる。			



活動の経過と成果(2007/6～2008/5) その2

2. 実際の評価作業でのフィードバック、情報収集

- 「評価チェックリスト」の現場での実践・・・失敗に終わる。
  - ✓WG内での呼びかけ、調査依頼
  - ✓個人情報保護を明示的に評価範囲に含めている企業は見つけられなかった。

- 内部統制の評価活動(J-SOX対応)の実務は「最低限」の対応
  - ✓「財務報告の信頼性」を優先(企業によっては特化・限定)しての対応
  - ✓取り組み姿勢にもよるが、限定された制度上の取り組みでは個人情報保護への対応は不十分

これまでの活動状況の感想

◆WGの活動

- 現状の内部統制評価制度との連携・オーバーラップは困難
- 将来的な個人情報保護の取り組みに期待する。
  - ✓会社法の内部統制－ 法令遵守の観点
  - ✓次世代J-SOXでの対応（財務報告以外の目的への広がり）

◆個人情報保護の内部統制への取り組み（提言）

- 個人情報保護の内部統制は「専門監査人」が専門家として社会に広げなければならない課題であると再認識した。
  - ✓専門家集団としてのサービス提供体制の確立
  - ✓構築時＝個人情報保護専門監査人の支援（コンサルテーション）機能
  - ✓運用時＝内部監査、第三者監査としての評価機能

今後の課題と活動について

◆WG1-1:個人情報保護の管理基準(監査チェックリスト)について

- 実際の監査への適用を図るが、別途計画される予定の模擬監査への提供もスコープに入れて検討を進める。

◆WG1-2:「利用制限の原則」に基づいた実装仕様について

- 今後は、実装仕様の整理の中で要求事項を見直し、システム管理の基準としてまとめたいと考えている。

◆WG2:個人情報関連の事故事例について

- 事故事例は時事の状況で変化するので、WGとして検討するより、ルーチンワークとして調査した方が効果的なため、WG2のテーマを再検討する。

◆WG3:個人情報保護のための内部統制の考察

- J-SOX対応が一段落する今年度以降は、企業活動のコンプライアンス整備の一環として個人情報保護体制を組み入れることが内部統制の実現につながると考えるため、WG3は一旦完了とする。