プライバシー・リスク の マネジメントと監査

GTAG5
(IT監査の国際的ガイダンス５)

目　次

- プライバシーとは何か
- プライバシーの原則とフレームワーク
- プライバシーの影響度とリスク モデル
- プライバシー統制
- プライバシー統制の実行適格度
- 内部監査の役割
- プライバシーの監査
- CAEからのプライバシーに関する質問　トップ 10

プライバシーとは何か

- プライバシーの様々な背景と意味
  - 場所 - 伝達 - 情報
  - 個人のプライバシー:
    肉体的なプライバシー 、精神的なプライバシー
  - 顧客としての、従業員としての、
    国民としての プライバシー
- 個人情報
  - 紙ベースの情報、電子的な情報
  - 機微情報、匿名扱いの情報

プライバシーに関わる役割

- データ本人
- データ管理者
- プライバシー オフィサー
- プライバシー責任者
- サービス・プロバイダー

プライバシーの原則とフレームワーク

- ベンチマークとなる基準の提供
  - 法律、規則、規約、専門職的かつ業務運営上のフレームワーク、取決め、…
  - 世界的基準 - 国家的基準 - 産業的基準 - 個人的基準
  - 監査、経営管理者、業務運営のための基準
- 国際的に認められた、核心となる原則
  - OECD 1980, EU 1995, CoE, UN, …

プライバシーの原則

- 収集と利用範囲の限定
- データのクオリティ
- セキュリティ保護
- 不可視性
- 個人限定のアクセス
- 説明責任

OECD 1980

プライバシーの
影響度とリスク モデル

- リスク
  - 個人的、組織的、財務上、風評上
- 個人に対する脅威
  - 顕在化するコスト、監視、IDの盗難、
    スパム、人権の制限
- 組織に対する脅威
  - 訴訟、ネガティブ広告、財務的な損失／余分な支出、
    業務運営への妨害、市場の失敗

COSO ERMモデルを使用したプライバシー統制

GTAGからの一例

統制活動

リスクの評価

モニタリング

情報と伝達

内部環境

リスクへの対応

事象の識別

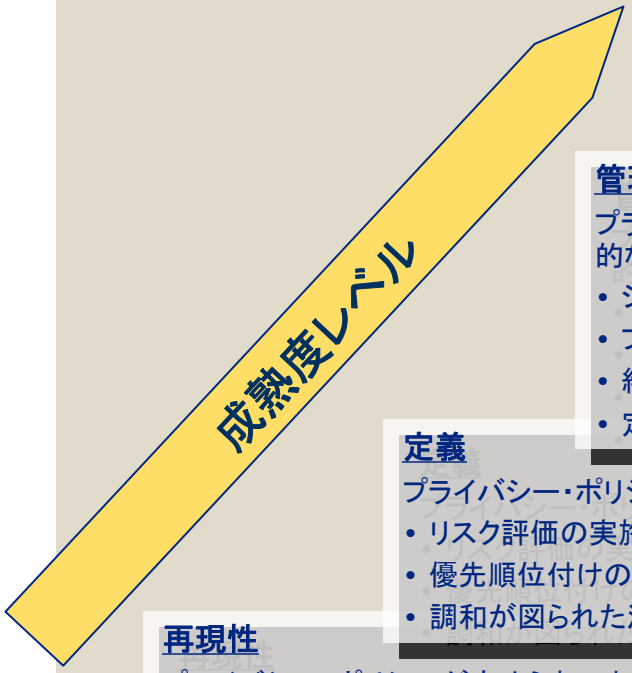
目的の設定

統制活動
リスクへの対応を確実にするような、組織のポリシー、手続、体系が、データセキュリティ、アクセスコントロール、インテグリティ及びコンティンジェンシーコントロール、プライバシーのレビュー、プライバシー苦情処理、等のさまざまな要件を達成している。

内部環境
プライバシーに関する、組織の文化や意向が、顧客と社会的責任に密接にリンクしており、内部的な、プライバシーに関するリスク・統制環境にとって重要なものとなっている。

内部環境は、上級経営管理者によって確立・伝達され、プライバシー規約、プライバシー・ポリシー（暗黙的にせよ明示的にせよ）、またプライバシーに関する組織の文化を包含しており、その全てが、適切な法令と規制に準拠するよう整備されている。

実行適格度:
プライバシー成熟度モデル



最適化

プライバシー・ポリシー、手続の実施、統制は継続的に改善されており、以下が確保されている

- プライバシー・リスクの影響度に対して、システマチックに精査された変更
- プライバシー目標を達成するための、専属の資源の割り当て
- ハイレベルの職能横断的な統合と、プライバシー目標達成のためのチームワーク

管理

プライバシーへのマネジメント、必要条件、配慮が、組織内で熟考された結果一貫して効果的な水準に保たれており、以下が確保されている

- システムおよびプロセス開発における、プライバシーへの早期配慮
- プライバシーの、職能および事業実施目標への統合
- 組織レベルおよび事業機能レベルでのモニタリング
- 定期的なリスクベースのレビュー

定義

プライバシー・ポリシーと組織が整っており、以下が確保されている

- リスク評価の実施
- 優先順位付けの確立と、それに応じた資源の割り当て
- 調和が図られた活動と、効果的なプライバシー統制の配備

再現性

プライバシー・ポリシーが定められており、以下が確保されている

- しかるべき上級経営管理者のコミットメント
- 全社的な認識とコミットメント
- 高リスク領域に対する特定の計画

初期

場当たりの活動

内部監査の役割

- IIA 実践要綱 2100-8
  - プライバシー・フレームワークにおける内部監査人の役割
- プライバシー統制 ： 法的な／事業上の 必要条件
  - 組織のガバナンス機構は、適切なプライバシー・フレームワークを確立するための責任を有している
  - 内部監査にできること
  - フレームワークの評価
  - 重要なリスクの識別
  - 適切な勧告
- 監査人の独立性が損なわれる可能性

プライバシーの監査

- 監査の活動計画 - プライバシーを含む
  - データの優先順位付けと分類
  - リスク評価
    - 法的／組織的リスク、利用リスク、ビジネス・プロセス・リスク
- 監査業務の準備
  - 個人データの処理プロセスへの理解
  - 脅威の識別
  - コントロールと対策の識別
  - 優先順位付け

Figure 5.2 – Privacy Audit Assessment Matrix

Asset	Threat	Impact	Controls	Audit Work	Conclusion
Application	Loss	Financial	Preventive	Testing	Well controlled
Database	Damage	Reputation	Compensating	Interviews	Improvement required
File type	Unavailability	Compliance	Detective	Observation	Inadequate control
Relationship	Disclosure	Operational	...	...	
...	...	...	...	...	Maturity models can provide an alternative

プライバシーの監査

- 評価の実施
  - プライバシー・マネジメントの評価
  - テスト実行のメソドロジー
    - 脆弱性評価、侵入テスト
    - 物理的コントロールのテスト
    - ソーシャル・エンジニアリングのテスト
- 伝達とモニタリングの結果
- プライバシー・マネジメント と 監査マネジメント
  - 計画、機密性、スタッフ、それぞれのマネジメント

CAEからの プライバシーに関する質問 トップ 10

- 関連する法令と規制は？
- どのような個人情報が収集されているのか？
- 各種のポリシーと手続は整っているか？
- 管理責任と説明責任は割り当てられているか？
- 個人データの保管場所は知らしめられているか？
- どのようなデータ保護の仕組みが整っているのか？
- 第三者に対してどのような情報が公開されているか？
- 従業員に対する訓練は適切か？
- プライバシー・プログラムに割り当てられている資源は十分か？
- プライバシープログラムの実施状況は定期的に評価されているか？