資料2

Privacy by Design

2013年1月11日
IBM Security Services

Masaharu Itoi

目次

プライバシー・バイ・デザインの背景

・利用者（市民、消費者、顧客）のプライバシー情報の保護

・プライバシー強化技術の進化
（PETs：Privacy　Enhancing Technologies）

・プライバシー情報の主体である利用者の保護と同時に
サービス提供側の自己的保護

・サービス提供側としてのより能動的なビジネスプロセスでの
プライバシー保護（ステークホルダーに対してどのような責任を
持つのかの明確化）

・第32回データ保護・プライバシー・コミッショナー国際会議（2010/10、
イスラエル・エルサレム）での「基本的なプライバシー保護の不可欠な
要素として認識」とする議決

プライバシー・バイ・デザインとは（7つの原則）

- リアクティブでなくプロアクティブ； 事後の措置ではなく事前に予防
- デフォルト設定でプライバシー保護
- 設計時に組み込むプライバシー対策
- すべての機能に対して－ゼロサムではなくポジティブサム
- エンドツーエンドのセキュリティ； ライフサイクル全体の保護
- 可視化と透明性； オープンにする
- 個人のプライバシー尊重； 個人を主体に考える

IBMにおけるプライバシー・バイ・デザインの実践

IBMプライバシー・プラクティスの3イニシアティブ

1. プライバシー影響評価（PIA）
2. プライバシー教育および意識向上のトレーニング
3. データ・インシデント管理

1. プライバシー影響評価（PIA）

プライバシー自己評価ツール
- ・該当プロセスに関連するプライバシー関連のリスクレベルの可視化
- ・約45問の質問項目、完了時に即座の結果提供
  Prologue Questions, Assessment Questions
- ・ナレッジデータベースとして適用アクションの提示も可能
- ・ビジネスオーナー、プロセスオーナーが最終的に判断
- ・自己評価データ、結果は集中管理データベースに保管
  （IBMプライバシーチームとのデータ共有）

基本設問とオプション設問

＜基本設問＞　　全部で33問

1. Accountability(説明責任)	5 問
2. Collection(収集)	5 問
3. Notice(通知)	6 問
4. Consent(同意)	4 問
5. Access Control(アクセス制御)	3 問
6. Security(セキュリティー)	6 問
7. Retention and Disposal(保存および破棄)	4 問

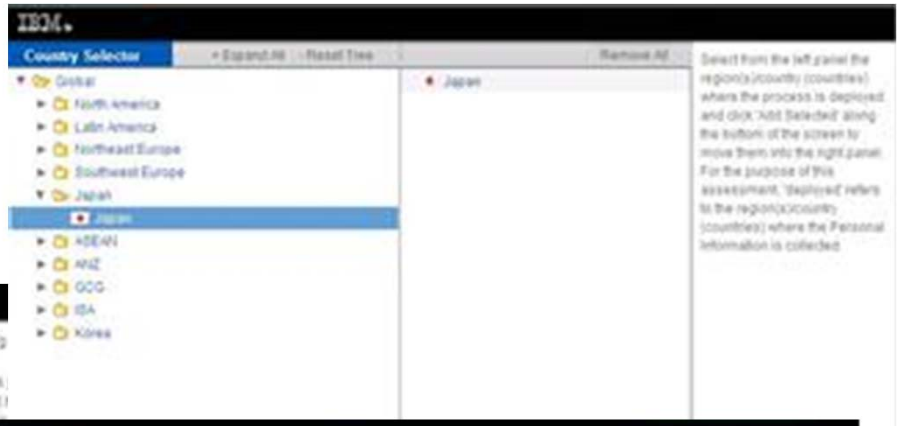
＜オプション設問＞　全部で8問　第三者からの提供や開示など状況により、異なる

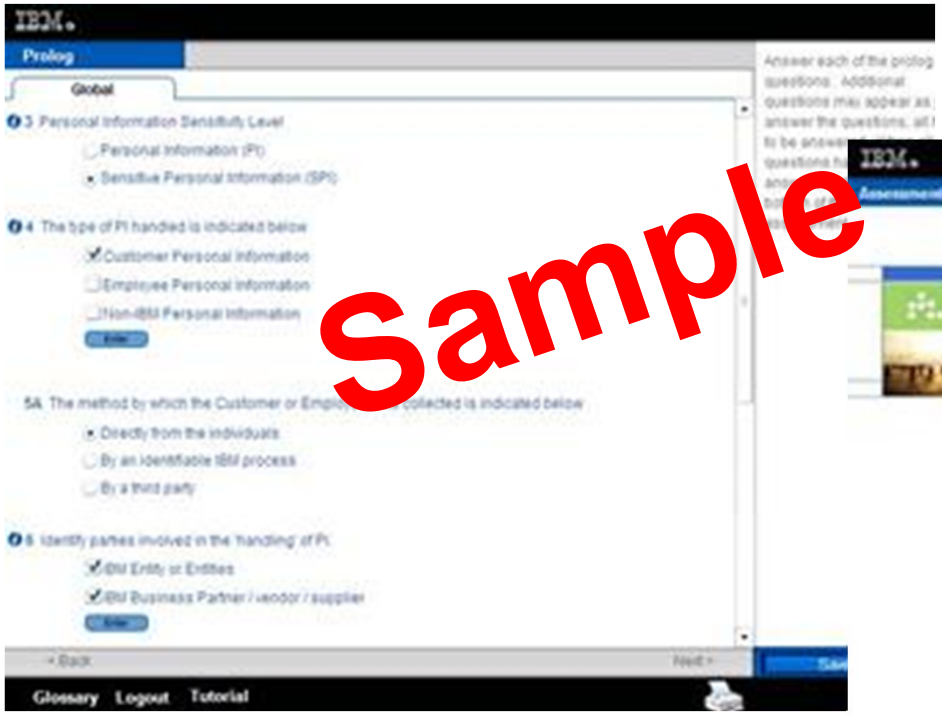
8. IBM 以外の個人情報を提供する第三者	2 問
9. IBM の個人情報を取り扱う第三者	5 問
13.EU以外の国の要件	1 問

オプション設問は、第三者から提供を受ける、第三者に開示する、SPIを取り扱うなどアセスメントするプロセスの状況により、異なります。すべての設問に答える必要があります。

Prologue＆Assessment Questions

アセスメントするプロセスを選択
アセスメント対象の国を選択





最初にPrologにプロセスの状況を入力

設問（Assessment）には基本とオプションがあります。Prologでの結果にしたがい、オプションの設問が自動的に出てくるようになります。

回答結果と適用アクション

すべての設問に回答すると、
その結果がグラフで表示されます。

「不足項目」「問題点」「対応すべきアクション」
の視点で状況を確認することができます。

日本独自の設問と完了アクション

SPIを取り扱うプロセスの場合には、日本独自の設問「You have indicated your process is handling SPI from Japan. An notification email will be sent to the Japan Privacy Office.」に回答することになります。

すべての設問で正しい対応がされると、
コンプライアンス100%になって、その状況は保管されます。

２．プライバシー教育および意識向上のトレーニング

グローバルな教育（トレーニング）ツール
- 「プライバシー・スマート（プライバシー意識の高い）」な従業員の育成
- 受講者の理解度、記憶維持を重視
  （現実的なシチュエーションの事例、クイズ）
- 受講（ツールへのサインイン）のログ記録、統計情報の集計
- 教育コースの電子的な進捗管理、完了時の証明書の発行
- ビジネス・コンダクト・ガイドライン（企業行動基準）との連携

３．データ・インシデント管理

データ・インシデント・ツール
- インシデント対応の体制運用のベースとしてのデータ共有ツール
- スプレッドシートからツールへ
  （データ共用のタイムリー化、データ記録のグローバル一貫性）
- データアクセスは役割、責任によるユーザー権限レベルで管理
- 対象は以下のデータを含むインシデント
  - **Client Information**
  - **Government Information**
  - **IBM Confidential - Technical & Scientific Information**
  - **IBM Personal Information**
- ツールのメリット
  - 収集情報の標準化
  - インシデントの進捗モニター、追跡
  - 傾向分析、原因分析
  - 一貫性のあるインシデント報告プロセス

課題点

・プライバシー・バイ・デザインの実践は企業としての強力なガバナンスが必要

・システム開発におけるプライバシー・バイ・デザインもツール化の推進が必要

・ビックデータ環境においては匿名化と解析精度のトレードオフが存在（暗号化などの技術によるブレークスルーを期待）

今後の展望

・プライバシー・バイ・デザインはあらゆる組織にとって実現可能なもの

・IBMでのプライバシー・バイ・デザインの実践は1つの例、アイデアであり、
今後、各組織でプライバシー・バイ・デザインの7つの基本原則に基づき
プロアクティブな管理アプローチがとられていくべき

・個人情報の管理に優れた組織が多くなればなるほど、より効果的に
プライバシーを保護できる社会へと発展する