プライバシー影響評価ガイドラインの開発と民間および行政システムへの実施適用

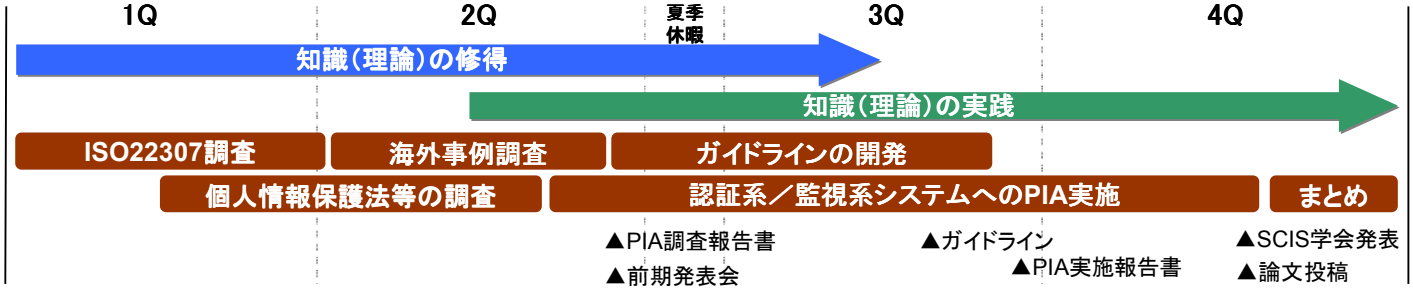
PBLの目的

■プライバシー影響評価PIA（Privacy Impact Assessment）は，個人情報，特にプライバシー情報を扱うシステムを構築する際に実施するリスクコミュニケーション手法である．PIAに関する調査研究を行う．

■日本でPIAを実施するフレームワークに関し，技術的，法的および社会的側面から実現手段を検討し，ガイドラインを開発する．ガイドラインに従い民間および行政システムに対しPIAを実施する．

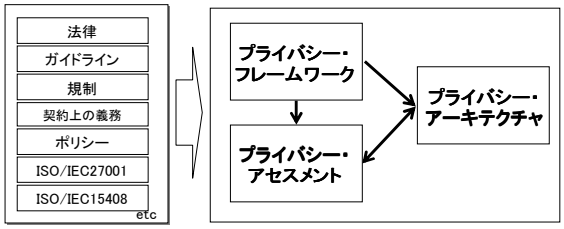
■PBL活動を通じて実践的な理論の修得および社会人基礎能力の向上を図る．

実施スケジュール



プライバシー影響評価（PIA）とは

個人情報の収集を伴うシステムの導入または改修の際に，プライバシーリスクの回避および低減のために，プライバシーへの影響を「事前評価」するリスクコミュニケーション手法である．
プライバシーフレームワーク，プライバシーアセスメント，およびプライバシーアーキテクチャの3つの機能で構成される．



■プライバシー・フレームワーク
法律，ガイドライン，規則，契約上の義務，既存のポリシー等を基に，対象システムに必要なプライバシー要件の抽出や評価シートを作成する．

■プライバシー・アセスメント
プライバシーフレームワークを基に，システムのデータフロー分析および評価シートなどによるプライバシーに関する影響分析を行い，個人情報の収集，利用，管理について，設計仕様を評価する．

■プライバシー・アーキテクチャ
プライバシーアセスメントで確認された問題に対し，システム設計仕様を検討し，技術的にプライバシーに関する問題解決を図る．問題解決のための技術をPET（Privacy Enhancing Technology）と呼ぶ．

海外事例

・海外ではプライバシー保護に関する法律や社会制度の整備が進んでいる．
・カナダ，米国，オーストラリアでの実施状況を調査した結果，PIA実施には，実施のための法律，独立し中立な監査体制，および実施手順を具体的に示すガイドラインが必要だと認識した．

	法律の整備状況	ガイドライン発行主体	PIA実施体制
米国	・米国電子法208条でPIAの実施を義務付 ・CPOの設置を法で規定 ・セーフハーバー法	行政管理予算局（OMB）	①システム構築組織の副責任者 ②組織内にCPO設置 ③OMBに報告書義務およびHPで公開義務、予算認可の条件
オーストラリア	・PIA実施法なし ・Privacy Act 1988	Privacy Commissioner	①プロジェクト実施組織 ②Privacy Commissioner ③行政用は報告書の公開義務
カナダ	・PIA実施法なし ・官：Privacy Act 民：Personal Information and Electronic Documents Acts （PIPEDA）	国家財政委員会	①プロジェクト実施組織 Deputy Minister ②Privacy Commissioner ③予算認可の条件、公開は推奨

注）①PIA実施指示、②中立的な検証組織、③PIA実施・公開義務
CPO：Chief Privacy Officer

ISO22307の要求事項

・米国から国際標準化委員会ISOTC68に提案され，2008年に国際標準規格ISO22307 Financial services - Privacy Impact Assessmentとして発行された．
・ISO22307には，6つの要求事項が記載されている．

6つの要求事項

1.PIA計画
準拠すべき国際標準，法律・法令，ガイドラインなどを調査し，プライバシーフレームワークを定義し，PIA評価の準備作業を行う．

2.PIA評価
計画段階で定義したPIAの実施対象範囲について，プライバシーリスクを洗い出し，指摘事項と指摘に対する推奨案を作成する．

3.PIA報告
PIA報告書として対象システムについて関係者間でレビューを行うため，評価・分析した事項を文書化する．

4.十分な専門知識
PIA実施には，必要な専門知識をプロジェクトメンバーが持つ必要がある．

5.独立性と公共性
PIAの実施には，利害関係者からの独立性を確保することが必要である．例えば，PIA実施結果の公表が挙げられる．

6.対象システムの意思決定の際の使用
対象システムにおけるプライバシー保護について意思決定を行う際に，判断材料としてPIAの結果を利用する．

ガイドライン及びアセスメント手法の開発

ガイドラインの開発

日本でPIAを実施する際には3つの課題がある．ガイドラインは，ISO22307の要求事項を充たすよう作成を行った．

	現状課題	対　策
根拠となる法律	・PIA実施法、プライバシー保護の法律未整備	・コモンクライテリア認証などによるコンフォーマンスの確保 ・条例（政令）などの整備
実施体制	・プライバシー問題に関し検討、助言を行う中立組織（制度）未整備 ・PIA報告書の承認・是正等の勧告に関わる組織が未整備	・現状の社会制度で可能な中立で公平なPIA実施体制の明確化 ・将来的には、Privacy Commissioner等の監督機関が必要
標準的な手順	・ガイドラインがなく、実施手順が定義されていない	・ISO22307の要求事項にあったPIA実施ガイドラインの開発

PIAの実施手順

PIAの実施手順は5つの手順で実施する．

(1)プロジェクト立ち上げ
　実施担当者の選定および実施チームの編成

(2)予備PIA実施
　システムの企画段階で，PIA実施の必要性および範囲を明確化

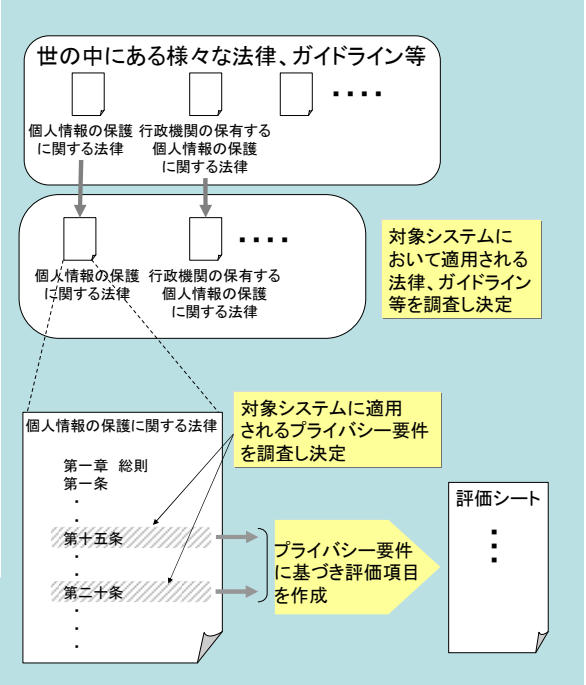
(3)PIA実施の準備
　プライバシーフレームワークの定義およびプライバシーアセスメントの準備作業実施

(4)PIAの評価
　評価シートを用いてプライバシーリスクを洗い出し，指摘事項と推奨案を作成

(5)PIA報告書の作成
　対象システムを保有する組織でレビューを実施できるようにするため，評価・分析した事項を文書化

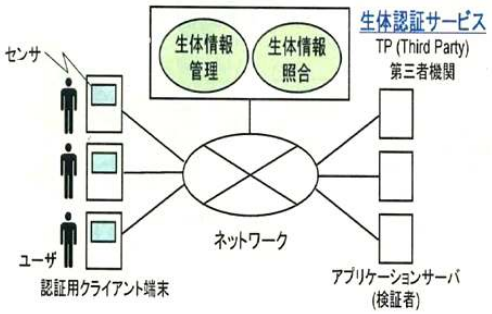
アセスメント手法

アセスメントで使用する評価シートは以下の手順で作成する．



認証系システムへのPIA実施

システム概要



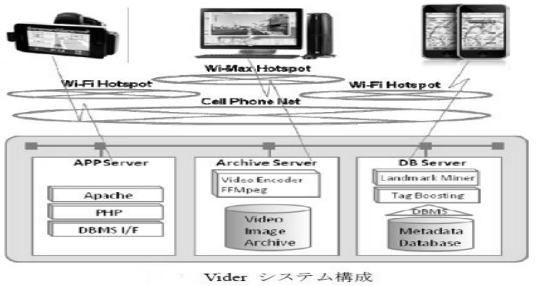
実施結果

■評価項目は，取得・公開，利用・保管，技術的な保護，説明責任の4つに分類し，全36項目であった．

■指摘事項
- サービス利用者が，生体認証情報の登録時に自分の意思で登録を行う仕組みが確認できない．
- 生体認証情報の取得時，なりすましによる登録に対する手続的，技術的な保護策を講じることが望ましい．　等

監視系システムへのPIA実施

システム概要



Vider システム構成

出典：嶋田茂ほか「スマートフォンによるドライブログの常時記録アーカイブと映像サービスシステムの構想，情報処理学会研究報告 Vol.2009-ITS-038, 2009

実施結果

■評価項目は，情報の取得・公開，システム及び情報の管理，苦情処理対応の3つに分類し，全29項目であった．

■指摘事項
- 情報の取得・公開に関して，サービス利用者に利用目的を明示する方法が確認できない．
- システムおよび情報の管理に関して，映像中の個人情報（顔，車番，システムのユーザ情報）を含んだデータの収集，管理，利用等の取り扱い方針の不備．　等

PIAの有効性と成果

システムを構築する前にプライバシーリスクを**事前に可視化**し，**プライバシーリスクの回避および低減**するための対策を設計等に反映できることから，PIAは，リスクコミュニケーションの手法として有効であることが確認できた．

本PBL活動を通じて，理論を修得し，修得した理論に基づき実践を行い，社会人基礎能力の向上が図れた．

1.理論の修得
PIA調査報告書（104ページ）

2.理論の実践
PIAガイドライン（38ページ）
認証系／監視系システム PIA実施報告書

3.理論の発信
論文発表
- 情報セキュリティ論文大賞の応募
- 暗号と情報セキュリティシンポジウム（SCIS2010）の発表
- 電子情報通信学会の発表