

Privacy by Design:
(プライバシー・バイ・デザイン)
ポリシーからプラクティスへ



2011 年 9 月



Information and Privacy Commissioner,
Ontario, Canada



謝辞

カナダ オンタリオ州 情報&プライバシー・コミッショナー(IPC)は、大規模かつグローバルに拠点を展開する企業であっても、どのようにすれば組織が*Privacy by Design*を導入できるのかについての貴重な事例情報をご提供いただきましたIBMコーポレーションに、心より感謝の意を表します。また、VP Security Counsel & Chief Privacy OfficerのHarriet Pearson氏、Global Privacy & Data Protection Executive & IBM Canada Chief Privacy OfficerのYim Chan氏、Privacy Program ManagerのHoward Young氏にもご協力いただきましたことに厚く御礼申し上げます。



Information and Privacy Commissioner,
Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

目次

序文	1
はじめに	3
ポリシーからプラクティスへの転換	3
プライバシー自己評価プログラムおよびツール	4
プライバシー教育および意識向上のトレーニング	7
データ・インシデント管理	8
学んだ教訓	10
プライバシー自己評価	10
データ・インシデント対応	10
プライバシー教育および意識向上のトレーニング	10
総括	11
主なメリット	11
まとめ	12

序文

ヴィクトル・ユーゴー(Victor Hugo)が「軍隊の侵略に抵抗することはできるが、思想が広まるのに抵抗することはできない。」という言葉を残した時代、ユーゴーは、*Privacy by Design (PbD)*について考えていたわけではありません。にもかかわらず、この言葉は、この概念の導入の着実な広がり表現するにふさわしい言葉となっています。この概念の誕生以降、引き合いに出されることが多くなった*Privacy by Design*は、この数年の間に、世界のプライバシー・コミュニティ内ではおなじみのテーマの一つとなっています。

欧州データ保護スーパーバイザー¹のピーター・ハスティンクス(Peter Hustinx)氏、欧州委員会司法・基本権利・市民権担当の副委員長²のビビアン・レディング(Viviane Reding)氏、米国連邦取引委員会委員長³のジョン・レイボビッツ(John Leibowitz)氏など、世界のプライバシー・リーダーが、*PbD*の重要性を支持しています。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で、私は*Privacy by Design*決議案⁴を提出し、全会一致で可決、採択されました。これは「画期的な決議」とみなされ、*Privacy by Design*が「基本的なプライバシー保護の重要な要素」の一つとして認識されるようになりました。

*Privacy by Design*という概念は1990年代半ばに誕生したのですが、その時、私は技術の相互接続がさらに進むことで、個人情報もボーダーレスに収集できるような状況になるだろうと考えていました。プライバシーを確実に保護するには、法令順守のみに頼るだけでは不十分であることは明白です。したがって、組織は、設計段階で技術の中に直接プライバシーを保護するような仕組みの構築を推進していくことが必要となり、最初の段階から確実にプライバシーを保護することが求められています。

*PbD*の根幹は技術にあります。その概念の適用は次第に責任あるビジネス・プロセスおよび物理的スペースやネットワーク・インフラストラクチャーの設計にも及ぶものとなっています。

*Privacy by Design*では、7つの基本原則⁵に基づき、公正な情報処理(FIPS: Fair Information Practices)を検証して展開し、可能な限りの最高の世界基準を追求していきます。7つの原則については以下のとおりです:

1. リアクティブ(事後)でなく**プロアクティブ(事前)**; 事後の措置でなく**事前に予防**
2. **デフォルト設定**でプライバシー保護
3. 設計時に**組み込む**プライバシー対策
4. 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**
5. 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**
6. **可視化と透明性**; **オープンにする**
7. 個人のプライバシー**尊重**; 個人を主体に考える

1. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf
2. <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16>
3. http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=0bfb9dfc-bbd7-40d6-8467-3b3344c72235&Statement_id=dcce94bb-6956-4313-ae81-e0fc87976c4c&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2010
4. <http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf>
5. <http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf>

多くの組織が、*Privacy by Design*の原則を導入し始めています。本書では、この概念をいち早く導入したIBMコーポレーションの事例について検討していきます。この事例は、*PbD*を企業のオペレーションのアーキテクチャー基盤の指針とした場合に、何が実現できるのかを示す変革の一例となります。IBMのような複雑な構造の多国籍企業がこのような原則から恩恵を得ることは当然のことではありますが、提示されている教訓があらゆる規模の組織にも当てはまるものであるということを念頭に置いてください。

IBMでは、このプライバシーへの戦略的フォーカスによって、確実に運用コストの削減およびコンプライアンスの文書化につながるプロセス改善が実現されました。

ただし、効率性の実現が、IBMの*PbD*に基づくプライバシー・プラクティスの唯一もしくは最も重要なメリットと言うわけではありません。Big Blue (IBM) チームは、*Privacy by Design*により、各組織のプライバシー・プログラムの中心となる基本目標を超えて、企業のビジネス戦略を直接後押しできるような、さらなる野心的課題に取り組むことができるようになることを発見しました。結論として、顧客の「スマーター・プラネット」の導入支援を目指す組織であれば、信用され、信頼される立場において、その取り組みを進めていくことが不可欠であり、特に、政府から消費財企業、公益事業、医療機関に至るまで、世界の多くの最重要組織の業務の遂行、データの処理にIBMが果たす重要な役割を考えれば、絶対的に必要であることは言うまでもありません。

IBMのポリシーからプラクティスへの道のりが重要な教訓を物語っています。*PbD*を導入するその他の組織の経験とともに、本書の情報は、*Privacy by Design*の時代が本格的に到来した事実を強く裏づけるものとなります。

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

はじめに

プライバシー・リーダーたちは、最も先進的な最高水準のプライバシーおよびデータ保護ポリシーであっても、効果を発揮するには、設計の段階から組織全体で徹底して運用しなければならないことを認識しています。国際的な組織は、各国、各地域の複数かつ異なるプライバシー保護法の要件に対応しなければならず、さらなる課題を抱えることとなります。

この課題は、IBMのようにビジネス・プロセスやオペレーションが世界各地に広がり、従業員も世界各地に分散し、文化的にも多様な企業ではさらに大きなものとなります。このような企業全体の課題に対応するには、プライバシーおよびデータ保護ポリシーを組織構造に組み込むしかありません。各レベルにおいて、事業部門およびサポート部門(プライバシーおよびITスタッフなど)では、責任をもつ領域のパフォーマンスがどのような状況にあるかを把握するための有効な尺度が必要になります。これらの情報を基に組織の各部分がどのように個人情報を扱っているかをよりよく管理することができます。

IBMは、PbDベースのアプローチが、このような要件に対応するのに理想的なものであると考えました。PbDの基本原則の一つは、責任あるビジネス・プロセスおよびテクノロジーの設計にプライバシーを直接組み込むことを提案しています。この概念の取り組みの中で、IBMは、事前予防、ビジネス目標へのポジティブサム(Win-Win)対応、プライバシー尊重を特徴とするユーザー中心の環境構築など、その他のPbD原則の実現においても飛躍的な進歩を遂げています。本書で取り上げられている事例研究では、IBMのPbDプログラムの重要要素について述べられています。

ポリシーからプラクティスへの転換

IBMのプライバシーおよびデータ保護への取り組みは、企業全体のプライバシー・ポリシーの枠組みから始められています。この枠組みが最初に導入されたのは40年以上も前のことで、全従業員に極めて重要な「トップからの視点」が示されています。もちろん、強力なポリシーは必要ですが、プライバシー・リスクや法令順守義務に対応するにはそれだけでは不十分です。特にIBM⁶のような大規模かつ多様性のある組織では、義務の遂行および厳格な監視も必要となります。

ポリシーからプラクティスへ転換するため、IBMの戦略は、企業全体のPbDプログラムの柱となる3つの主要イニシアチブで構成されています：

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

PIAは、適切に実行・導入されることで、個人情報保護を強化すべきビジネス・プロセスやITアプリケーションを特定し、対応できるプロアクティブ(事前予防)な方法の一つとなります。

6. IBMは、40万人以上の従業員を抱え、150カ国以上で事業を展開している企業であり、2009年には958億米ドルの収益を上げています。



図 1- プライバシー・プラクティスの3つの柱

継続的なプライバシー教育および意識向上のトレーニングは、日常的な個人情報に対する意識の向上および適切な処理に必要な情報を全従業員に提供します。

組織は情報漏洩の可能性に備えなければならないため、データ・インシデント管理も必要となります。データ・インシデントが発生した場合に備え、その状況を迅速に管理し、そのインシデントを解決、防止するための適切な措置を講じる手順を整備しておかなければなりません。

IBMのプライバシー・プログラムは、社内外の要求や期待の変化に応じて成熟してきたため、これら3つのイニシアチブは、この10年間で劇的な進化を遂げています。基本的なスプレッドシートやプレゼンテーション・モジュールとして始まり、現在利用されている実行ツールでは、ユーザー中心の設計、自動化された自己診断、カスタマイズされた尺度の広範囲の取得と表示を組み合わせています。同じく重要な点として、これらのツールが、世界的な規模で企業の基幹プロセスに組み込まれている点です。

プライバシー自己評価プログラムおよびツール

多くの組織にとって、PIAは、手作業での時間のかかる労働集約型のプロジェクトになります。プライバシー・リスク・レベルの特定に必要な質問内容の作成、インタビューの実施、集めた回答の検証に多くの時間を費やすこととなります。通常、専門家(サブジェクト・マター・エキスパート)が回答内容を分析し、プライバシー・リスクを判断して、分析結果および推奨事項をまとめなければなりません。組織の中には、スプレッドシートを使ってPIAを実施しているため、企業レベルの実用的な管理レポートの作成が非常に困難な作業となっているところもあります。実際、プライバシー・リスクを判断するのに、単一のビジネス・プロセスを評価するだけで、数週間、時には数ヶ月かかる場合もあります。

しかしながら、PIAが適切に導入されれば、プライバシー・コンプライアンスを確実なものとする重要な監視機能となるため、PIAはPbDの実現には欠かすことのできないツールであるといえます。IBMでは、このグローバル企業全体でPIAを積極的に利用するため、5年以上前に企業内のあらゆるビジネス・プロセスやITアプリケーションに適用できるWeb対応のプライバシー自己評価ツールを開発しました。

この評価メソッドロジーの設計時に、IBMは、プライバシー・オフィスよりもむしろ、各事業部門の個人がプロセスおよびITアプリケーションのプライバシー・コンプライアンスに責任を負うべきだと判断しました。また、以下の役割の間にも重要な区別が存在しています：

- ビジネス・オーナー：プロセス・コンプライアンスの責任者。自己評価結果を受け、適用可能なアクションの実行に同意します。
- プロセス・オーナー：ビジネス・ユニットに代わってプライバシー評価を実施する責任者。エンドツーエンド・プロセスについて知識のある人もしくはビジネス・オーナーがこの役割を担う場合もあります。

評価を実施する人が誰であろうと、最終的にはビジネス・オーナーがコンプライアンスの責任を負うことになるため、IBMにおけるこの自己評価は、プロセスや関連するITアプリケーションといった側面のみを考慮するだけでなく、エンドツーエンド・プロセスの関係性(PbDアプローチの重要な要素)についても考慮されています。

ビジネスまたはプロセス・オーナーが自己評価を完了すると、このツールがその回答をリアルタイムに分析します。該当プロセスに関連するプライバシー関連のリスク・レベルが、実行した個人および企業のプライバシー・オフィスに対して即座に可視化されます。特定されたプライバシー・リスクは、プロセスおよびコントロールの問題点となる可能性があります。全体的なアプローチを通して、そのビジネス・オーナーに対し、プライバシー関連の問題をひとまとめにして提示することができます。

ビジネスおよびプロセス・オーナーは、(およそ)45の質問を30分で完了することができるため、従来のPIAでは数週間がかかっていたであろう状況を考えると、大幅な時間の節約となります。では、どのようにしてこれを実現するのでしょうか？IBMでは、プライバシー、法務、技術チームが密に協力し、以下を可能にするツールおよびプロセスを設計しました：

- 理解しやすい質問を提示(ビジネスおよびプロセス・オーナーは、プライバシーについての専門家ではないため)
- トレーニングの必要性を最小化する直感的なインターフェースおよびロジック・フローを使用
- ツールの完了時に即座に結果を提供(数週間も後に提供したのでは、ビジネスまたはプロセス・オーナーが、他の作業に移ってしまっていたり、質問にどのように回答したかさえも覚えていない場合がある)



図 2 – IBMのプライバシー自己評価ツールのダイアログ・フロー

さらに、IBMのプライバシー自己評価ツール内には、制度および規制に関する知識やベスト・プラクティスが組み込まれており、ビジネスおよびプロセス・オーナーが、特定された問題に対応するためのワーク・プランを作成することが容易になっています。カスタマイズされたナレッジ・データベースから、自己評価の結果に対して適用できる100以上の個別アクションを提案することもできます。アクション・プランが完成すると、その完了まで追跡されることとなります。

プライバシー自己評価ツールのフローは図2に示されています。ビジネスまたはプロセス・オーナーが、この安全なイントラネット・サイトにサインオンすると、評価ツールについての簡単な紹介と、分かりやすい操作方法が表示されます。次に、このツール内で質問に答えます。質問には2つのタイプがあります：

- *Prologue Questions (プロローグの質問)*: 収集した個人情報のタイプおよびその情報がどこで使用、管理されているかを特定します。これらの質問の回答から以下の評価のための質問が生成されます。
- *Assessment Questions (アセスメントの質問)*: 評価対象のプロセス固有の質問内容で、関連する国、個人情報の取り扱い方、誰が個人情報を処理するのも考慮に入れられています。

すべての質問に答えると、2つのグラフィカルなレポートが即座に作成され、潜在的なプライバシー・リスクが提示されます。これらのインタラクティブなレポートでは、ビジネスおよびプロセス・オーナーが棒グラフや円グラフ上をクリックすれば、詳細な情報までドリルダウンすることもできます。プライバシー・リスクへの体制を強化する必要がある場合、最終的かつ重要なステップは、それらのリスクをなくすためのアクション・プランを設定することとなります。

すべての自己評価データおよび結果は、集中管理データベースに保管されます。報告ツールでは、ビジネス・ユニットのエグゼクティブ、プライバシー責任者向けに、企業、国、地域レベルの結果をまとめた尺度およびスコアカードの測定値が提供されます。また、レポートを通して、評価ステータスがサポート責任の領域内にあるかをIBMのプライバシー・チームが追跡できるようにサポートします。

プロセス全体が効率化され、多くのケースで自動化されているため、プライバシー担当者は、個々の評価に関する事務作業の管理よりも、実質的価値を高めることに集中することができます。たとえば、電子メール通知は、特定の条件(例: 開始されていない評価、アクションが保留状態または期限切れとなっている評価)に基づいて自動的に発信されます。

現在、個人情報保護および電子文書に関する法律に対し、効率的にコンプライアンスを確保できる方法としてカナダで生まれたプロセスおよびIBMのPIAツールVersion 1.0が、社内でのオペレーション全体でグローバルに利用できるようになっています。IBMのグローバル・プライバシー・チームは、このツールのナレッジ・ベースの規制情報を段階的に拡大し、欧州連合(EU)のすべての国々を含め、すべての地域が利用できるように拡張することにより、統制された方法でこの基盤の増強を図ってきました。こうして、プライバシー・チームでは、企業全体を通して、分析およびサマリー・レポートにより十分な情報を得ることで、一貫性のある情報に基づくプライバシー決定プロセスを確立することができるようになりました。

プライバシー教育および意識向上のトレーニング

このデジタルな世界において、従業員は、データ・プライバシーを理解し、機密情報の管理方法を把握しておかなければなりません。このような認識は、PbDの重要原則の一つであるエンドツーエンドのセキュリティを実現するのに必要であると同時に、プライバシーへのより幅広いアプローチを可能にする鍵にもなります。この分野で何を期待されているのかを従業員に認識させることで、個人情報の保護を大事にする文化を築くこととなります。技術やセキュリティだけでは十分ではありません。組織の個人情報という資産を効果的に管理するには、「プライバシー・スマート(プライバシー意識の高い)」な従業員の存在が欠かせないのです。

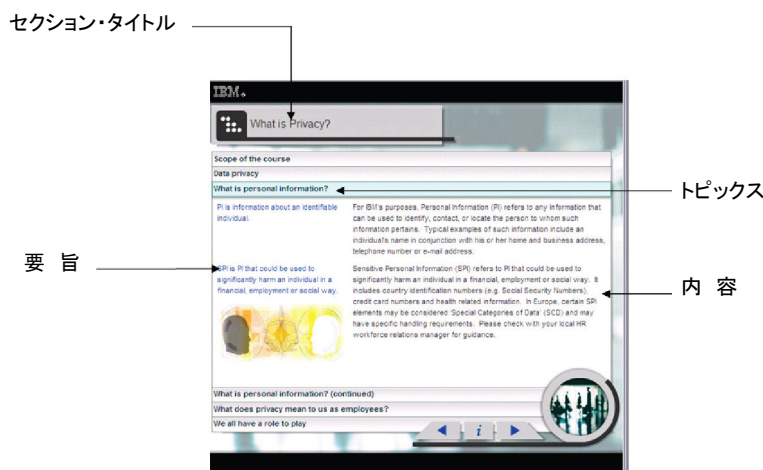


図 3 - プライバシー教育および意識向上のトレーニング・ツール

有意義かつ効果的な教育の重要性は誰もが認めるところです。IBMの取り組む課題は、コンテンツを整理し、効果的に提供するベストな方法を見つけることにありました。ホワイト・ペーパー、社内のWebサイト、事前にパッケージ化されたプレゼンテーションなど、これらはどれも、組織の人員に重要な情報を提供することが可能な手段であり、これらを適切に組み合わせることで効果的に展開できます。しかしながら、IBMのプライバシー・チームが早くから認識していたこととして、コンテンツやメッセージングが重要であると同時に、学習内容の記憶維持に影響を与える重要なものの一つが、教育コンテンツを提供する際のフォーマットにあるということでした。

したがって、IBMは、プライバシー教育および意識向上ツールをカスタマイズする際、受講者が情報を理解しやすいように、簡単に把握できるひとまとまりの要旨である「ナレッジ・ナゲット(Knowledge Nugget)」に基づいてコンテンツを整理するテクニックに重点を置きました。各ナゲットには、習得すべき内容を示す短いメッセージが示されています。このナゲットは各セクションに分類されており、従業員が直面するであろう現実的なシチュエーションの事例もそれぞれに示されています。最後に、短い多肢選択式クイズが出題され、間違った解答であれば、正しい解答を説明するポップアップ画面が表示されるようになっています。これらすべては、情報の記憶維持の向上のために設計されたものです。

プライバシー教育および意識向上ツールへのサインインはすべてログに記録され、教育コースの進捗が電子的に追跡されます。従業員が適切にコースを終了すれば、証明書が発行され、管理者用にコースの統計情報が集計されます。

他にも重要なものとして、以下の2つのグローバルな、企業全体の意識向上の取り組みが、これらのプライバシー重視の取り組みを補完し、強化しています。IBMでは毎年、すべての従業員が、企業の「ビジネス・コンダクト・ガイドライン(企業行動基準)」についてプライバシー教育と同様のわかりやすいコースを受講し、理解したことを証明しなければなりません。その他の重要なトピックに加え、これらのガイドラインには、プライバシーや情報のセキュリティも含まれています。さらに、従業員全体が、情報セキュリティを焦点とするトレーニングを受けています。この全従業員を対象とするトレーニングは、プライバシーおよびデータ・セキュリティ教育でさらに強化され、企業の事業部門およびスタッフ部門以外にも広められています。

これらの継続的な取り組みが総合して、企業全体のプライバシーおよびデータ保護への意識を高め、慎重に扱う姿勢づくりに大きな役割を果たすこととなります。

データ・インシデント管理

いかなる規模の組織も、データ・セキュリティのインシデントに対応できるような体制づくりがますます重要になっています。これらのインシデントの原因は、悪意のある行為から、個人データを処理する過程での不注意による過失までさまざまです。問題がいつ、どこで発生しても、またどのような理由であっても、個人を保護し、規制当局の期待に応え、最終的には関係組織の評判を守るような形で状況に対処するため、統制のとれた迅速な対応が必要となります。

グローバルな企業では、例えば、対応チームの構成や、情報漏洩の抑制に役立つ専門知識やリソースの可用性などについて、対応プロセスからサポートおよびガイダンスを提供しなければなりません。インシデントの責任追跡についてのポリシーは、複数の管轄および事業部門を巻き込む可能性のある状況にも対処できるように、あらかじめ決定しておく必要があります。

多くの企業は、現在、データ・インシデントに関する情報を記録するのに、スプレッドシートや類似のツールを使用しています。これは、インシデントについてのデータを収集するのに便利な方法であるかもしれませんが、少なくとも2つの欠点があります：

- スプレッドシートおよびその他のドキュメントは、個人のパソコン上に保存される可能性が高く、タイムリーかつ安全な方法で情報を共有することをますます難しくする可能性があります。
- 世界の異なる地域や異なるビジネスまたはスタッフ・ユニットで収集されたデータの記録に一貫性がない可能性があり、相互参照やトレンドの分析、レポートの生成が困難となります。

これらの問題を克服するため、IBMのプライバシー・チームは、収集される情報の種類別にプロセスを標準化するWebベースのデータ・インシデント・ツールを開発しました。このツールおよびツール内のデータへのアクセスは、役割および責任に基づく一連のユーザー権限レベルによって管理されています。

このツールで実行されるプロセスは、4つのステップで構成されており、インシデントの提示から始まります。最初から最後までで少なくとも20の質問に答える必要があります。このツールでは、自動のインテリジェントな質問ロジック・フローを使用して、特に重要な領域に「ドリルダウン」するためにさらなる質問が促される場合もあります。



図 4 - データ・インシデント・ツール

インシデントに関する情報の収集に加え、このツールでは、ユーザーが適切な手順を取れるように誘導していきます。たとえば、ノート・パソコンの紛失の場合、ユーザーは、資産保護を担当する組織にこのインシデントを報告するように促されます。この機能により、このツールでは、インシデント情報の簡易リポジトリ以上のことを行うことができます。

インシデントが提示され、場所、インシデントのタイプ、潜在的なリスクに関する質問の回答に基づき、データ・インシデント・ツールが、そのインシデントの対応をサポートできる専門のエキスパートを特定し、その個人に関連情報を送ります。特定されたプライバシー担当者に電子メールが自動的に送信され、データ・インシデントが割り当てられた旨を連絡します。そのインシデントの「オーナー」は、データ・インシデント・ツールにアクセスすることができ、調査を実施してインシデントを解決するための必要なステップへのガイダンスとしてこのツールを利用します。

データ・インシデント・ツールおよび関連プロセスが多数のメリットを提供します：

- 対応プロセスおよび企業内で収集が必要な情報が標準化されます。
- 各インシデントに関連する調査、フォローアップ、リカバリー作業のリポジトリとしての役割を果たし、権限のある社内のステークホルダーが、インシデントの進捗をモニターし、追跡できるようになります。
- 報告ツールを使うことで、監視およびガイダンスが改善され、スコアカード・尺度に加え、傾向および根本原因の分析も可能となります。
- 一貫性のあるインシデント報告プロセスにより、(チーム内およびステークホルダーとの)インシデント対応についてのコミュニケーションが改善されます。

学んだ教訓

IBMの「プライバシー・ポリシーをプラクティスへ変換する」という目標は、セルフヘルプのソフトウェア・ツールおよびプロセスの開発によって促進されました。これらの開発を通して学んだ重要な教訓の一部を以下に挙げています。

プライバシー自己評価

事務管理タスクにではなく、プライバシーを改善するためのアクションに集中 – 原則はプロアクティブであること。プライバシー自己評価ツールおよびプロセスが、IBMのプライバシー専門家の知識をまとめ、活用し、ベスト・プラクティスとして組み込みます。プライバシーおよびデータ保護を改善する必要がある場合、このツールから必要となるアクションが提案されるため、グローバル・プライバシー・チームは、評価自体の事務管理作業に多くの時間を取られることなく、ビジネスの助言や支援に集中することができます。

小さな部分から始め、段階的に拡大 – *Privacy by Design*プログラムを始めることは、組織の規模に関わらず、計り知れない取り組みに思えるかもしれません。IBMのプライバシー・チームは、まず、カナダ一国からPIAの取り組みを始めました。その際の導入から学び、そのプログラムを基に改善を図り、他の場所にも展開していきました。グッド・プラクティスとなるのは、企業の管理しやすい部分を選択し、プログラムの最適化に集中して取り組み、その後、企業全体を対象として拡張していく方法です。

データ・インシデント対応

一貫性のあるプロセスを確立 – データ・インシデント・ツールは、データ収集だけでなく、ワークフローやコラボレーションのサポートにも利用されています。このツールを通してインシデント・オーナーが特定されるため、責任およびアカウントビリティ（説明責任）の所在が明確になります。さらに、インテリジェントな質問ロジック・フローの使用により、情報の質が高まるため、インシデント対応をサポートする必要がある最初のチームを迅速に特定できるようになります。また、不要なデータ収集やその他のタスクを繰り返すことが最小限に抑えられます。

体系的アプローチをインシデント情報の収集に導入 – タイムリーに情報を共有することが、コラボレーションを成功させるためには不可欠であり、まさに、このエンタープライズ・ツールの使用により達成できることと言えます。一貫したコミュニケーションが可能となれば、異なる国、異なるビジネス・ユニットや機能から調査チーム・メンバーを集めることができます。また、体系的アプローチにより、類似したインシデントをグループ化し、企業全体の根本原因のパターンを探ることができます。

プライバシー教育および意識向上のトレーニング

受講者の学習の記憶維持が焦点 – グローバルな組織では、通信教育や自己学習への依存度が高くなります。コンテンツが重要であることはもちろん、そのフォーマットやプレゼンテーションも学習と記憶維持にとって重要な要素となります。

適切な場所にプライバシー・コンテンツを組み込む – 単一の総合的プライバシー・モジュールの構築に満足するだけでなく、IBMのプライバシー・チームは、組織の中でプライバシー関連情報を従業員のコミュニケーションと教育に組み込み可能なパートナーを特定する組織的キャンペーンに取り組みました。これらのパートナーには、コンプライアンス、IT部門/CIOおよびさまざまなビジネス・ユニットが含まれています。そうすることで、最も有意義かつ有益な場所およびタイミングで、多数の従業員がプライバシー関連情報を目にする機会が増えることとなります。

総括

パートナーシップおよびコラボレーションが鍵となる – いずれのプログラム(自己評価、インシデント対応、教育)においても、PbDイニシアチブには、IT部門や法務部門など、組織内の多数の部門との密接な協力が必要となります。

統制のとれたデータ収集および表示により、アクションが可能となり、信頼性も増す – IBMのPbDプログラムの最も重要な機能の一つが、事実に基づき、一貫して提示される尺度の作成と共有です。入念に設計され、慎重に共有することで、これらの尺度を通して、企業のプライバシー・チームは、幅広いビジネスおよび機能リーダーと、的を絞った、有効な話し合いを行うことができます。

主なメリット

IBMが最初にPbDベースの企業プライバシー対策の取り組みを開始したとき(そして現在も)、その目標はコンプライアンスを確保し、プライバシー関連のリスクを削減することにあります。これらの目標は常に重要なものですが、他のメリットや機会の実現も可能であり、また、実現されています。

プライバシー自己評価ツールがその良い例です。IBMが5年前にこのツールを最初に導入したとき、個人情報の処理に伴うリスクを削減することを目的としていました。現在、これまで行われた何千もの評価が蓄積された結果、IBMは、個人情報を収集および管理するプロセスのインベントリー(目録)を作成しました。その結果として創出される情報が重要な役割を果たしています。個人データを管理するプロセスおよびITアプリケーションに関するこの充実したインベントリーが、この種のデータを処理する手順やプロセスを標準化するための取り組みの情報源となります。さらに、このインベントリーにより、プライバシー・チームおよびその他のチームは、プロセスを検証し、そもそも個人情報の収集や使用が実際に必要なかどうかを徹底的に追究することができます。つまり、事業におけるデータ最小化の機会も探ることができます。

Privacy by Designのアプローチを導入することによるその他のメリット:

- **自動化による効率性** – IBMは、可能な場所があれば、効率化およびリソースのより効果的な展開のために、これらのプロセスを自動化してきました。したがって、人員や予算を比例して増やすことなく、これらのツールやプロセスのグローバルな利用および処理量を拡大してきました。
- **プロセスの制御および品質を改善するためにエンドツーエンドでフォーカス** – IBMは、オペレーションの自動化と監視およびガバナンス手順を結び付ける垂直プロセスに着目しました。その効果は、継続的な監視および改善サイクルになります。プライバシー・フォーカル・ポイントおよびビジネス・ポリシー・オーナーは、ガバナンス・プロセスを知らせるレポートを定期的に受け取り、必要に応じてポリシーの改善や新たなポリシーの導入が行えるようにしています。監視は、ビジネス制御とも結び付き、連携しています。このエコシステムの存在が、継続的な改善モデル内で、企業全体でのIBMのプライバシー・ポリシー導入をサポートしています。

自動化されたセルフヘルプ・ツールを介して導入された、文書化および統制されたグローバルなプロセスを通じて、IBMでは現在、以下の点が改善されています：

- 個人を特定できるような情報(PII: Personal Identifiable Information)を収集しているビジネス・プロセスおよびアプリケーションを特定し、どこで収集され、どのように処理されているのかを明確に把握
- データ・インシデントを記録、追跡し、より迅速に対応することで、可能性のある企業および個人のリスクを最小限に抑制
- プライバシーに関する考慮事項や義務事項への意識向上のための従業員の教育

まとめ

Privacy by Design はあらゆる組織にとって実現可能なものです。今回の事例研究の目的の一つは、IBMが独自のPbDプログラムで導入したアイデアの一つまたは複数を読者の皆様の今後の参考にさせていただくことにあります。

プライバシー評価およびリスク管理の目標の対応において、IBMは最終的に、7つのPbDの基本原則の実現が当初の目標を超える価値を生み出すことに気がきました。PbDが、従業員教育、技術、そして何よりも、プロアクティブな管理アプローチを取ることの重要性を指摘するものとなっています。

この経験からわかったことは：

- 新たな技術が新たなプライバシー・リスクを呼び起こしているように見えますが、技術は基本的にプライバシーにおいて中立です。したがって、問題となるのは、その導入方法になります。実際、PbDの大原則として、ビジネスの目的とプライバシーのニーズの両方を満たす環境を作り上げるために技術を使用するポジティブな方法が重要視されています。
- 情報漏洩には避けられないものもあります。そのような問題には、迅速かつ効果的な対応がベスト・プラクティスとなります。
- 高水準の従業員教育を常に追求していくことが極めて重要です。質の高い資料が適切に提供されているかに注意を払い、従業員の参加とパフォーマンスを追跡することに注意が必要です。このような方法を通して、プライバシーを保護する文化への上級管理職の真剣な取り組みが、顧客対応の最前線のスタッフからバックオフィスまでの従業員の中にも浸透することになります。
- 結局のところ、7つのPbDの基本原則に基づくツールの導入に成功することが、自己達成の予言となるのです。IBMでは現在、プライバシー保護への配慮が企業全体に行き渡っています。

IBMでは、これらの実績を共有することに積極的であり、他の組織が次のステップへのプライバシー・イニシアチブを実現できるように支援していきたいと考えています。最終的に、個人情報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します。7つのPbDの基本原則を実現する、プライバシー・ポリシーから統制のとれた効率的なプラクティスへと転換することが、さらに情報豊かな、相互接続された地球を実現するという目標達成に不可欠なのです。



Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
電話: (416) 326-3333
FAX: (416) 325-9195
Eメール: info@ipc.on.ca
Webサイト: www.ipc.on.ca

IBM Canada Ltd.

3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
電話: (905) 316-5000

本書に記載された情報は、予告なしに変更される場合があります。
IBM およびIPCは、本書に含まれる技術的または編集上の誤り、省略に対して一切の責任を負いません。

2011年9月

<http://www.privacybydesign> | <http://www.ibm.com/ca/>

