Privacy by Design

7つの基本原則

アン・カブキアン博士

カナダ・オンタリオ州

情報プライバシー・コミッショナー

プライバシー・バイ・デザイン は、情報通信技術および大規模にネットワーク化された情報システムの絶え間なく増大する全般的な影響に対処するため、私が90年代に開発した概念である。

*プライバシー・バイ・デザイン*により、プライバシーの未来は、単に規制の枠組みを遵守するだけでは保障できないという考え方が推進されている。むしろ、理想的には、プライバシーの保障が組織の活動における標準形態となる必要がある。

当初、プライバシー強化技術（PETs）の利用が、解決策であるとみられた。今日、われわれは、より実質的なアプローチをとる必要があると認識している。－PETs の利用を PETS Plusまで拡張する－ ゼロサムではなく、ポジティブサム(全機能的)アプローチをとることである。それは、PETS *Plus*の*"Plus"*の部分である。ゼロサム(間違った二分法)の二者択一ではなく、ポジティブサムである。

プライバシー・バイ・デザイン は、幅広く適用されるべき三つの側面に拡大する。それらは、1）ITシステム、2）責任あるビジネス・プラクティス、そして、3）物理的設計とネットワーク基盤である。

出典 "Information & Privacy

Commissioner of Ontario"ウェブサイト

プライバシー・バイ・デザイン の原則は、あらゆる種類の個人情報に適用され得るが、医療情報や財務データといった機微なデータには、特に強力に適用されなければならない。プライバシー対策の強度は、データの機微性の高さに相応する傾向がある。

プライバシー・バイ・デザイン の目標 ― プライバシーを確保することと自己の情報に対する個人のコントロールを獲得すること、そして、組織のために、持続可能な競争的利点を獲得すること ― は、次に掲げる 7 つの基本原則を実践することで達成することができる*(以下のページを参照)*。

7 つの基本原則

1. 事後的ではなく、*事前的*; 救済的策でなく *予防的*

プライバシー・バイ・デザイン(PbD) のアプローチは、受け身で対応するというより、むしろ先見的に対応することが特徴である。プライバシー侵害が発生する前に、それを予想し予防することである。PbDは、プライバシーの脅威が具体的に起きるのを待つものではなく、また、一旦それらが起こった場合に、プライバシー侵害を解決するための救済策を提供するものでもない。 ― それらの発生を防ぐことを目的としている。要するに、*プライバシー・バイ・デザイン*は、事後ではなく、事前に作用する。

2. *初期設定*としてのプライバシー

われわれは、一つのことについて確信し得ている ― 標準ルールである！ *プライバシー・バイ・デザイン*は、所定のITシステムまたはビジネス・プラクティスにおいて、個人データが自動的に保護されることを確保することによって、最大級のプライバシー保護を提供することを目指している。個人が何もしなくても、彼らのプライバシーはそのまま保護される。彼らのプライバシーを保護するために、個別の措置は不要である。 ― それは、システムに*最初から*で組み込まれているものである。

3. デザインに*組み込まれる*プライバシー

*プライバシー・バイ・デザイン*は、ITシステムおよびビジネス・プラクティスのデザインおよび構造に組み込まれるものである。事後的に、付加機能として追加するものではない。これによって、プライバシーが、提供される中心的な機能の重要な構成要素になる。プライバシーは、機能を損なうことなく、システムに不可欠なものである。

4. 全機能的 ― ゼロサムではなく、*ポジティブサム*

*プライバシー・バイ・デザイン*は、不要なトレードオフの関係を作ってしまう時代遅れのゼロサムアプローチではなく、ポジティブサムの「ウインーウイン」の方法で、すべての正当な利益および目標を収めることを目指している。*プライバシー・バイ・デザイン* は、プライバシーとセキュリティの両方とも持つことが可能で**あること**を実証し、プライバシー**対**セキュリティのような誤った二分法を回避する。

5. 最初から最後までのセキュリティ — *すべてのライフサイクルを保護*

*プライバシー・バイ・デザイン*は、情報の最初の構成部分が収集されるより前にシステムに組み込まれことから、関係するデータのライフサイクル全体を通じて安全に拡張する。 — 強力なセキュリティ対策は、最初から最後まで、プライバシーに不可欠である。このことは、時期を逃さず、すべてのデータが安全に保持され、プロセスの終了時には確実に破棄されることを確保している。このように、 *プライバシー・バイ・デザイン* は、情報の安全なライフサイクル管理を、揺りかごから墓場まで、終始、全ライフサイクルにわたって確保している。

6. *可視性と透明性 — 公開* の維持

*プライバシー・バイ・デザイン*は、どのようなビジネス・プラクティスまたは技術が関係しようとも、立の検証を受けることを条件に、決まった手続および目的に従って、実際には機能することをすべての関係者に保証することを目指している。その構成部分および機能は、利用者および提供者に一様に、可視的で透明でありつづける。記憶し、信頼するが、検証すべきである。

7. 利用者のプライバシーの*尊重 — 利用者中心主義を維持する*

特に、*プライバシー・バイ・デザイン*は、設計者および管理者に対し、強力なプライバシー標準、適切な通知、および権限付与の簡単なオプションのような手段を提供することによって、個人の利益を最大限に維持することを求めている。利用者中心主義を維持すべきである。

Published: September 2011
Translation provided by: Masao Horibe
Professor Emeritus at Hitotsubashi University
Tokyo, Japan

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario • CANADA • M4W 1A8

Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Email: info@ipc.on.ca