プライバシー・バイ・デザインの実務的な基本概念と重要性

EYアドバイザリー・アンド・コンサルティング(株)
公認情報システム監査人（CISA） 公認内部監査人（CIA） 杉山幸人

▸ Yukito Sugiyama
個人情報保護をはじめとするシステム監査、情報セキュリティ監査および各種システム構築支援などに従事。2015年3月～17年4月、特定個人情報保護委員会（現個人情報保護委員会）上席政策調査員、個人情報保護委員会 課長補佐として、特定個人情報保護評価に従事。情報処理安全確保支援士。（Tel：03 3503 1490　E-mail：Yukito.Sugiyama@jp.ey.com）

Ⅰ　はじめに

ここ数年、国内において、マイナンバー法の施行をはじめ、改正個人情報保護法の施行、サイバーセキュリティ基本法の施行など、個人情報およびセキュリティに関する新法、改正法の施行が続いています。また、国外においても、欧州連合（EU）における新しい個人情報保護の枠組みとして、EU一般データ保護規則（General Data Protection Regulation：GDPR）が2018年5月25日から適用が決まりました。

このような大きなトレンドの中で、プライバシー・バイ・デザインやセキュリティ・バイ・デザインという、プライバシー保護やセキュリティ保護の仕組みを構築する概念が重要になっています。

本稿では、両者の共通概念を整理し、特にプライバシー・バイ・デザインについて、関連した規格の紹介とともにその重要性を解説します。

Ⅱ　プライバシー・バイ・デザインとセキュリティ・バイ・デザインの実務的な基本概念

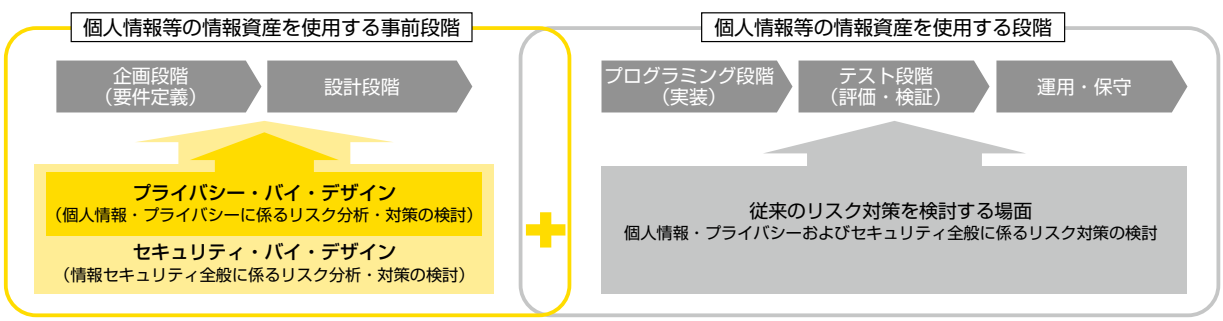
1. プライバシー・バイ・デザイン

カナダ・オンタリオ州情報プライバシーコミッショナーのアン・カブキアン博士が1990年代の半ばに提唱したもので、個人情報をシステムや業務にて「使用する段階」にプライバシー保護の施策を検討するのではなく、その事前段階の「企画・設計段階」から組み込むという考え方です。

2. セキュリティ・バイ・デザイン

プライバシー・バイ・デザインは、対象を個人情報・プライバシーに絞った概念ですが、セキュリティ・バイ・デザインは、その対象を情報セキュリティ全般に拡張した概念です。内閣サイバーセキュリティセンター（NISC）が公表している「情報システムに係る政府調達におけるセキュリティ要件策定マ

▶図1　実務面におけるプライバシー・バイ・デザインとセキュリティ・バイ・デザインの基本概念図



▶表1　主な国際規格（ISO/IEC）およびJIS規格（2017年9月現在）

No	関連規格	規格化の状況	名称
1	ISO/IEC 29100	2011年　規格化済	Privacy Framework
2	JIS X 9250	2017年　規格化済	プライバシーフレームワーク（プライバシー保護の枠組み及び原則） ※上記のISO/IEC 29100がJIS化されたもの
3	ISO/IEC 29101	2013年　規格化済	Privacy Architecture Framework
4	ISO/IEC 29134	2017年　規格化済	Guidelines for privacy impact assessment
5	ISO/IEC 29151	2017年　規格化済	Code of practice for personally identifiable information protection
6	ISO/IEC 29184	策定準備中	Guidelines for online privacy notices and consent
7	JIS Q 15001	改定中（意見受付公告中）	個人情報保護マネジメントシステム－要求事項

ニュアル」においても、「情報セキュリティを企画・設計段階から確保するための方策」として、セキュリティ・バイ・デザインの考え方を取り入れています。

両者の共通概念は、従来のリスク対策を検討する場面に加え、企画・設計段階にリスク対策を検討し、事前的・予防的にリスク対策を組み込むというものです。また、単に情報システムだけを対象とするのではなく、業務プロセス全般での対応が必要だと考えるものです。両者ともにシステム開発の初期段階にリスク対策を検討することで、網羅的で過剰なリスク対策やプログラミングなどの手戻り工数の増大を抑えるメリットがあります。　（＜図1＞参照）

Ⅲ　プライバシー影響評価（Privacy Impact Assessment：PIA）

プライバシー・バイ・デザインの概念にのっとり「企画、設計段階」で個人情報・プライバシーに係るリスク分析・評価、対策検討を行う手法に、プライバシー影響評価（Privacy Impact Assessment：PIA）があります。

情報システムの新規開発や改修に当たり、個人情報を取り扱うプロセス（取得、利用、保存、提供、削除・廃棄など）のどの部分で個人情報漏えいなどのプライバシーへの影響（リスク）が生じ得るかを事前に評価し、それに応じたリスク対策をプログラミング段階でインプットするものです。

日本では、マイナンバー法（第27条、第28条）において、マイナンバーを含む個人情報ファイル（特定個人情報ファイル）を保有する行政機関・自治体などに対して、「特定個人情報保護評価」と呼ばれるPIAの実施が義務付けられています。また、EUのGDPRにおいては、保有する個人情報について、プライバシーに係るリスクを測定、分析、評価するプライバシー保護対策として、Data Protection Impact Assessment（DPIA）の実施（第35条）が求められています。このDPIAはPIAと同じ概念であることがGDPRに注記されています。

Ⅳ　個人情報保護・プライバシー分野の主な国際規格およびJIS規格

日本では、改正個人情報保護法の施行に合わせ、個人情報保護委員会、官庁から関連する各種ガイドラインが公表されましたが、プライバシー分野では、国際規格（ISO/IEC※）およびJIS規格も着々とリリースされています。特に策定準備中のISO/IEC29134はGuidelines for privacy impact assessment（PIAのためのガイドライン）であることにも注目です。

（＜表1＞参照）

Ⅴ　おわりに

現在、国内において、プライバシー・バイ・デザインおよびその実施手法としてのPIAは、一般的に普及しているとは言えないかもしれません。しかし、国外においては、これを義務付けるGDPRが来年の施行を控え、さらに関係するISO/IECおよびJIS規格も着々と整備が進んでいる状況です。情報システムの新規開発、改修や業務プロセスの変更時にこのような概念を取り入れて情報保護の強化・改善の手段とすることが、今後、重要になっていくと思われます。

※　国際標準化機構（ISO）および国際電気標準会議（IEC）によって定められた国際規格