日本DPO協会第8回個人情報保護セミナー
「サイバーセキュリティの有事・平時の対応と役員の責任　その２」
一般財団法人国際経済連携推進センター
主任研究員　金子 啓子 先生

2023年2月9日（木）15:00～16:00

あいさつ「プライバシーとセキュリティ」

一般社団法人日本DPO協会代表理事

堀部　政男

（一橋大学名誉教授・元個人情報保護委員会委員長）

【前回資料】
日本DPO協会第7回個人情報保護セミナー
「サイバーセキュリティの有事・平時の対応と役員の責任」
渥美坂井法律事務所・外国法共同事業
パートナー弁護士　松岡史朗氏

2023年1月19日（木）15:00～16:00

あいさつ「プライバシーとセキュリティ」

一般社団法人日本DPO協会代表理事

堀部　政男

（一橋大学名誉教授・元個人情報保護委員会委員長）

【前回資料】
第7回個人情報保護セミナー

- 「サイバーセキュリティの有事・平時の対応と役員の責任」
- 講師：渥美坂井法律事務所・外国法共同事業
- パートナー弁護士　松岡史朗　先生

【前回資料】
プライバシーとセキュリティ―不可分の関係
OECD1980年プライバシー・ガイドラインの8原則

- 1 収集制限の原則（Collection Limitation Principle）
- 2 データの質の原則（Data Quality Principle）
- 3 目的明確化の原則（Purpose Specification Principle）
- 4 使用制限の原則（Use Limitation Principle）
- 5 安全保護措置の原則（Security Safeguards Principle）
- 6 公開の原則（Openness Principle）
- 7 個人参加の原則（Individual Participation Principle）
- 8 責任の原則（Accountability Principle）

【前回資料】

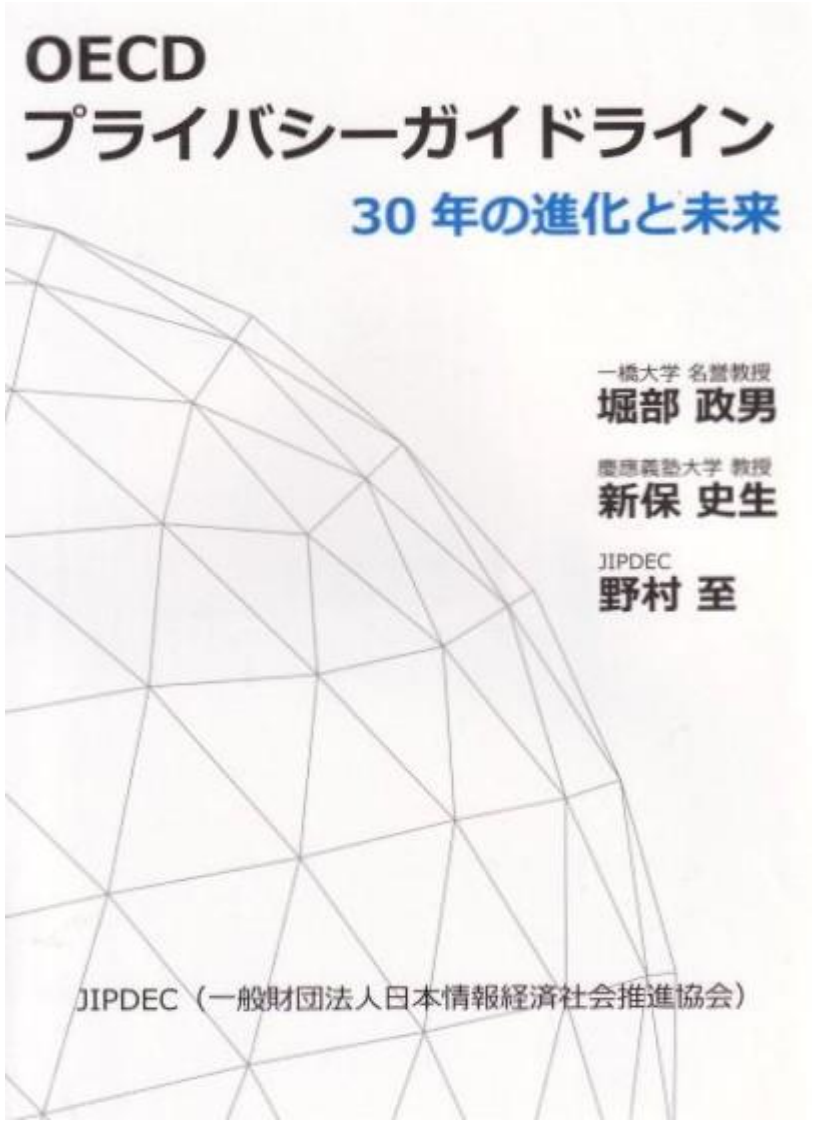
OECD1980年プライバシーガイドラインの「安全保護の原則」

- 安全保護の原則
- Security Safeguards Principle
- 個人データは、その紛失もしくは不当なアクセス、破壊、使用、修正、開示等の危険に対し、合理的な安全保護措置により保護されなければならない。
- Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

【前回資料】
OECDのセキュリティ・プライバシー関係文書

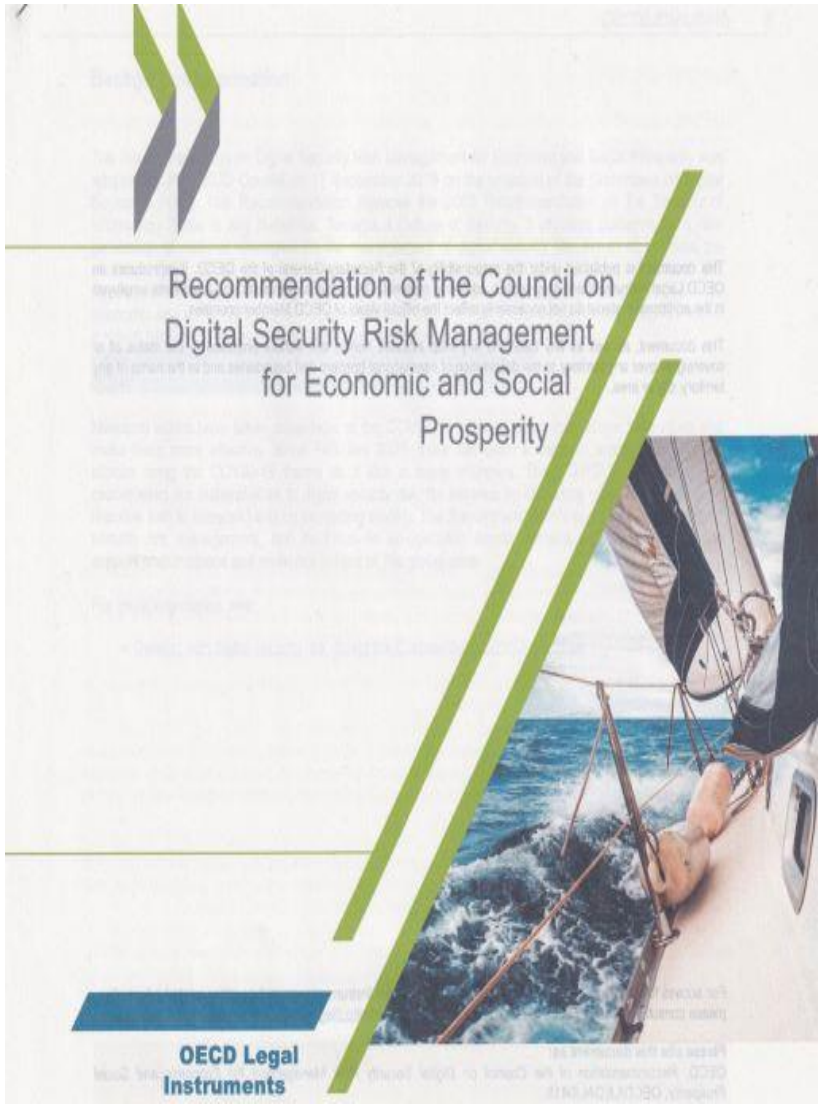
- ア　プライバシー・ガイドライン（1980年）―「プライバシー保護と個人データの国際流通についてのガイドライン」（Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）が1980年9月23日に理事会で採択された。
- イ　セキュリティ・ガイドライン（1992年）―「情報システムのセキュリティのためのガイドライン」（Guidelines for the Security of Information Systems）が1992年11月26日に理事会で採択された。
- ウ　暗号政策ガイドライン（1997年）―「暗号政策ガイドライン」（Guidelines for Cryptography Policy）が1997年3月27日に理事会で採択された。
- エ　セキュリティ・ガイドライン改正（2002年）―「情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて」（Guidelines for the Security of Information Systems and Networks：Towards a Culture of Security）が2002年7月25日に理事会で採択された。
- オ　プライバシー・ガイドライン改正（2013年）―改正プライバシー・ガイドライン（Revised Privacy Guidelines）が 2013年7月11日に理事会で採択された。

【前回資料】OECD1980年プライバシー・ガイドラインの2013年改正参考文献



- 発行・発売　JIPDEC
- 2014年5月23日発行

【前回資料】Digital Security Risk Management（2015）



- Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity
- 2015年9月17日に理事会によって採択された。

【前回資料】OECD2015年デジタル・セキュリティ・リスク・マネジメント勧告

- 「経済的・社会的繁栄のためのデジタル・セキュリティ・リスク・マネジメントに関する理事会勧告」（Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity）は、2015年9月17日に理事会によって採択された。

【前回資料】一般原則（General Principles）

- 1. 意識向上、技能及び強力化（Awareness, skills and empowerment）
- 2. 責任（Responsibility）
- 3. 人権及び基本的価値（Human rights and fundamental values）
- 4. 協力（Co-operation）
- 5. リスク評価及び対応サイクル（Risk assessment and treatment cycle）
- 6. セキュリティ手段（Security measures）
- 7. 革新性（Innovation）
- 8. 準備性及び継続性（Preparedness and continuity）

【今回資料】Data Breach Notification
データ侵害通知

- 日本DPO協会第8回個人情報保護セミナー
- 2023月2月9日
- GDPRの第4条　定義
- GDPR第33条　監督機関に対する個人データ侵害の通知

【今回資料】Data Breach Notification
データ侵害通知

- Guidelines on Personal data breach notification under Regulation
- Article 4 Definitions（第4条　定義）
- (12) ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (12)「個人データ侵害」とは、偶発的又は違法な、破壊、喪失、改変、無権限の開示又は無権限のアクセスを導くような、送信され、記録保存され、又は、その他の取扱いが行われる個人データの安全性に対する侵害を意味する。

- ＊日本語訳は、個人情報保護委員会ウェブサイト掲載のものによる。

【今回資料】Article 33 Notification of a personal data breach to the supervisory authority
第33 条 監督機関に対する個人データ侵害の通知

- 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

【今回資料】第33 条 監督機関に対する個人データ侵害の通知

- 1. 個人データ侵害が発生した場合、管理者は、その個人データ侵害が自然人の権利及び自由に対するリスクを発生させるおそれがない場合を除き、不当な遅滞なく、かつ、それが実施可能なときは、その侵害に気づいた時から遅くとも72 時間以内に、第55 条に従って所轄監督機関に対し、その個人データ侵害を通知しなければならない。監督機関に対する通知が72 時間以内に行われない場合、その通知は、その遅延の理由を付さなければならない。

【今回資料】Article 34 Communication of a personal data breach to the data subject
第34 条 データ主体に対する個人データ侵害の連絡

- 1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
- 1. 個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させる可能性がある場合、管理者は、そのデータ主体に対し、不当な遅滞なく、その個人データ侵害を連絡しなければならない。

【今回資料】Data Breach Notification
データ侵害通知

- 2003年個人情報保護法第7条（個人情報の保護に関する基本方針）第1項
- 政府は、個人情報の保護に関する施策の総合的かつ一体的な推進を図るため、個人情報の保護に関する基本方針（以下「基本方針」という。）を定めなければならない。
- 「個人情報の保護に関する基本方針」（平成16（2004）年4月2日閣議決定）
- ６　個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項

【今回資料】Data Breach Notification
データ侵害通知

- (1) 個人情報取扱事業者に関する事項
- ① 事業者が行う措置の対外的明確化
- ② 消費者等の権利利益の一層の保護
- 「また、事業者において、個人情報の漏えい等の事案が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表することが重要である。」
- ③ 責任体制の確保
- ④ 従業者の啓発
- ⑤ 安全管理措置の程度

【今回資料】個人情報保護法第26条

- 法第26条（第1項）
- 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者又は行政機関等から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者又は行政機関等に通知したときは、この限りでない。

【今回資料】個人情報保護委員会ウェブサイト
https://www.ppc.go.jp/personalinfo/legal/leakAction/

- 漏えい等の対応とお役立ち資料
- 漏えい等の報告について
- 報告対象となる事態
- 下記の要件に該当する場合、漏えい等報告が義務付けられています。
- 1.（1）要配慮個人情報が含まれる個人データの漏えい等（又はそのおそれ）
- 2.（2）不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等（又はそのおそれ）
- 3.（3）不正の目的をもって行われたおそれがある個人データの漏えい等（又はそのおそれ）
- 4.（4）個人データに係る本人の数が1,000人を超える漏えい等（又はそのおそれ）※民間事業者
- 保有個人情報に係る本人の数が100人を超える漏えい等（又はそのおそれ）※行政機関等