プライバシーWG
日本版 CoC-JP

クラウドプライバシワーキンググループ

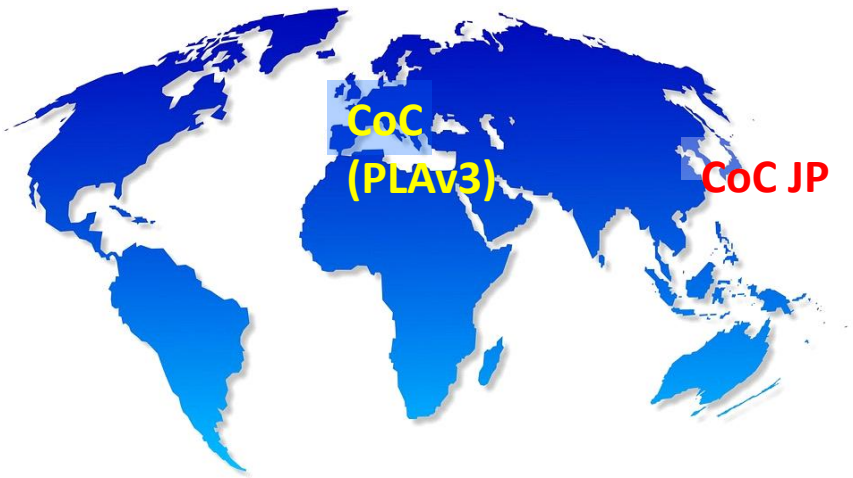
山崎　万丈

CSA JC cloud security alliance SM Japan Chapter

CSA JC cloud security alliance SM Japan Chapter　CSA cloud security alliance SM

Code of Conduct for APPI Compliance

- CSA CoC for GDPR Complianceの日本版
- 個人情報保護法の Code of Conduct



CoC JP

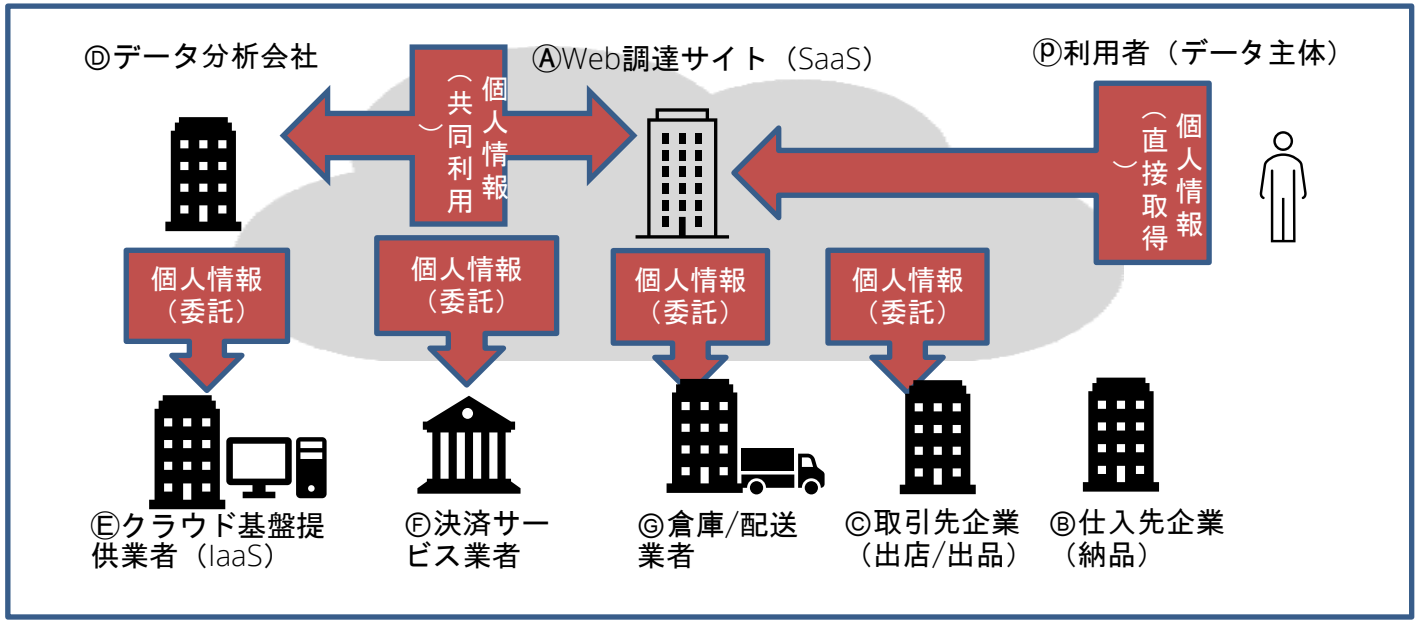
- 個人情報の保護に関する法律およびそのSub setであるガイドライン群を対象
- 付属書はCCMとの対比を日本版として作成
- 現行版(2016年版)として作成。
- 法令の2022年施行版については一部コメントとして記述があるが、フル対応は2022年以降に発行される次期verのCoC JPにて対応する予定

構成・目次

目次

モデルを使って解説

- 法人向けECサイトを使って、解説事例を章によっては採用



第１章　個人情報の取得や個人データの留保に関する事業者の対応

- 個人情報の取得
  - 法１５条から１８条
    - 特定・制限・適正取得・通知
- 個人データの留保
  - 法19条
    - 正確性確保等

第２章 安全管理措置

表７　安全管理措置に関連する各文書の該当箇所

個人情報の保護に関する法律	個人情報保護委員会（平成 28 年 11 月）（令和２年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」	*個人情報保護マネジメントシステム－要求事項（JIS Q 15001：2017）*	*CCM*
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、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。	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、滅失又は毀損（以下「漏えい 等」という。）の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならないが、当該措置は、個人データが漏えい等をした場合に本人が被る権利利益の 侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない。具体的に講じなければならない措置や当該項目を実践するための手法の例等については、「8（別添）講ずべき安全管理措置の内容」を参照のこと。	*A.3.4.3.2；B.3.4.3.2*	*GRM-04*

その講ずべき必要かつ適切な措置の具体的な内容については、個人情報保護委員会が「通則編」を始めいくつかの個人情報保護法ガイドラインを公開している。「個人情報の保護に関する法律についてのガイドライン（通則編）」では講ずべき安全管理措置およびその措置が応じなければならないリスクについて次のように述べている。

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN （英語）（2020 年 01 月 31 日時点アクセス）

第３章　事業者による従業員および委託先の監督

図２　個人情報保護法とGDPRの執行体体制の比較

義務を負う主体：　個人情報取扱事業者

個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。（法第2条第5項）

(1) 国の機関

(2) 地方公共団体

(3) 独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平 成 15

※ Data Controller とData Processor は、複数の加盟国にまたがって事業を行う場合、原理的には、複数の加盟国の監督当局を相手にする必要がある。

義務を負う主体：

(1) Data Controller(管理者)

(2) Data Processor（処理者）

上記2区分に該当する場合、法人格の有無、営利性の有無は問わず、自然人、法人、公的機関、行政機関又はその他の団体の全てが適用対象となる。（第4条第7号・第3号）

第４章　個人情報の提供

- 国内での提供
- 海外への提供

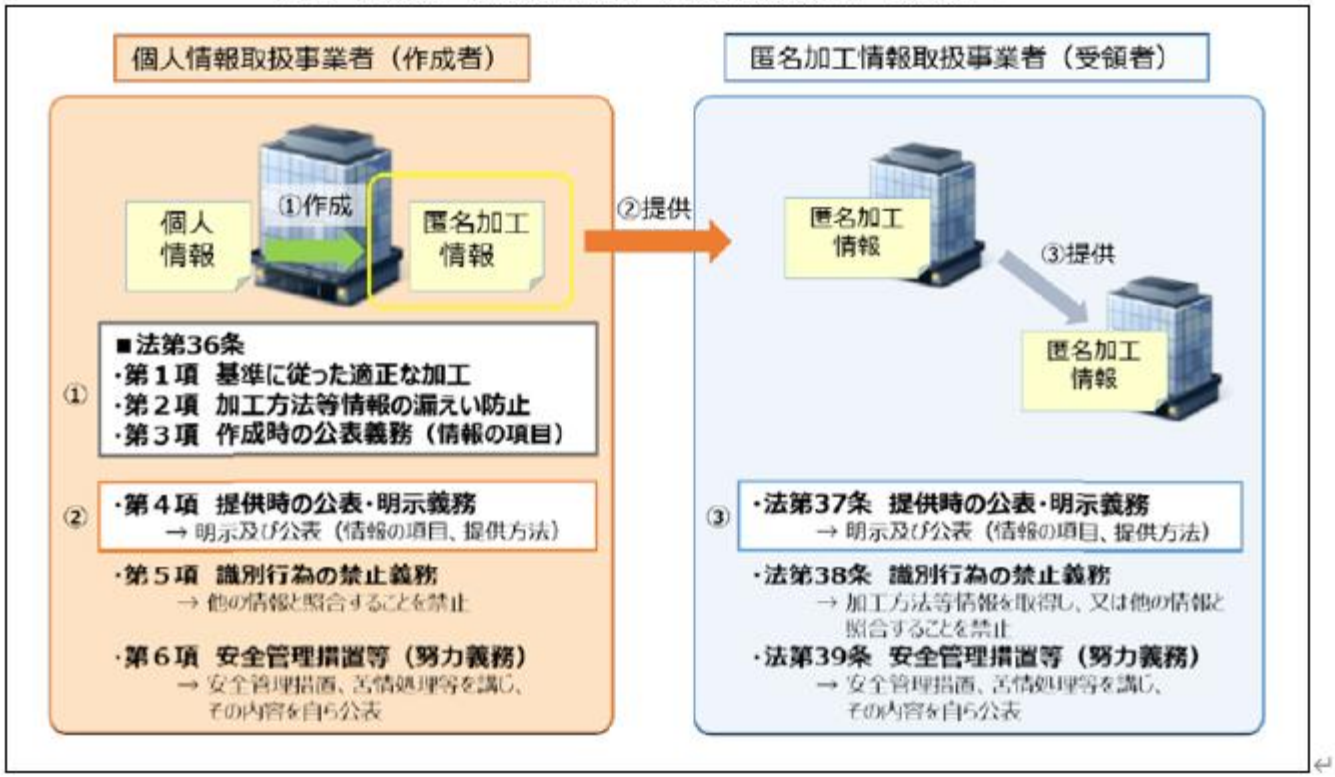
表 24　現行法との比較（個人情報保護法とGDPR）

比較対象 / 比較項目	（現行法）個人情報保護法（2015改正、2017年施行）	（現行法）GDPR一般データ保護規則（2016制定、2018年施行）
上位法令の違い	日本国憲法において、「個人情報保護」の条文なし	EU 憲法において、「I-51 条：個人情報保護」の条文あり
定義の違い	＜比較＞ ・法の対象者 生存者、取扱事業者、第三者、委託先、共同利用者、事業継承者 ＜関連条文＞ 2 条（定義） ・生存者とは、生存する本人 ・取扱事業者とは、個人情報データベース等を事業の用にしている者 ・第三者とは、上記以外の者 その他 ・委託先とは、処理を委託される者 ・共同利用者とは、共同利用する者 ・事業継承者とは、合併等で事業を継承する者	＜比較＞ ・法の対象者 自然人、管理者、共同管理者、処理者、取得者、第三者 ＜関連条文＞ 4 条（定義） ・自然人とは、データ主体 ・管理者とは、単独で取扱を決定する者 ・共同管理者とは、共同して決定する者 ・処理者とは、管理者に代わり取扱う者 ・取得者とは、開示請求を受ける者 ・第三者とは、上記以外の者
同意の違い	＜比較＞ ・個人情報の取扱は、公表同意 ・子供の同意は、明記なし ・要配慮情報は、提供が禁止	＜比較＞ ・個人情報の取扱は、主体同意 ・16 才未満の子供は、親権者の同意 ・機微情報は、原則、取得が禁止

第５章　　個人情報に関する本人の権利と事業者の対応

第６章　匿名加工情報個人情報に関する本人の権利と事業者の対応

図５　匿名加工情報の作成者・受領者が遵守すべき規定[48]



付録 CCMとの対比

- 保護法･ガイドラインのCCM該当箇所の対比

	個人情報の保護に関する法律	個人情報の保護に関する法律　条文	ガイドライン（通則編）	ガイドライン（外国にある第三者への提供編）	個人データの漏えい等の事案が発生した場合等の対応について	金融分野における個人情報保護に関するガイドライン	医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス	JIS　Q　15001　：　2017
１５条　利用目的の特定	BCR-01 BCR-04 GRM-01 GRM-02 GRM-03 GRM-04 GRM-05 GRM-07 GRM-08 GRM-09 GRM-10 HRS-10 SEF-03 SEF-04 STA-03 STA-04 STA-05 STA-07 STA-08		BCR-01 BCR-04 GRM-01 GRM-02 GRM-03 GRM-04 GRM-05 GRM-07 GRM-08 GRM-09 GRM-10 HRS-10 SEF-03 SEF-04 STA-03 STA-04 STA-05 STA-07 STA-08	BCR-01 BCR-04 GRM-01 GRM-02 GRM-03 GRM-04 GRM-05 GRM-07 GRM-08 GRM-09 GRM-10 HRS-10 SEF-03 SEF-04 STA-03 STA-04 STA-05 STA-07 STA-08	SEF-03 SEF-04	BCR-01 BCR-04 GRM-01 GRM-02 GRM-03 GRM-04 GRM-05 GRM-07 GRM-08 GRM-09 GRM-10 HRS-10 SEF-03 SEF-04 STA-03 STA-04 STA-05 STA-07 STA-08	BCR-01 BCR-04 GRM-01 GRM-02 GRM-03 GRM-04 GRM-05 GRM-07 GRM-08 GRM-09 GRM-10 HRS-10 SEF-03 SEF-04 STA-03 STA-04 STA-05 STA-07 STA-08	BCR-01 BCR-04 GRM-01 GRM-02 GRM-03 GRM-04 GRM-05 GRM-07 GRM-08 GRM-09 GRM-10 HRS-10 SEF-03 SEF-04 STA-03 STA-04 STA-05 STA-07 STA-08
	BCR-01 BCR-04 GRM-01 GRM-02		BCR-01 BCR-04 GRM-01 GRM-02	BCR-01 BCR-04 GRM-01 GRM-02		BCR-01 BCR-04 GRM-01 GRM-02	BCR-01 BCR-04 GRM-01 GRM-02	BCR-01 BCR-04 GRM-01 GRM-02

次期バージョンについて

- 法2022年4月施行版及びガイドラインを対象にした版の作成検討中

Q&A

ご清聴ありがとうございました。