CSA の考える GDPR 対応と個人情報保護法対応

運営委員
山崎　万丈

CSAJC cloud security alliance SM Japan Chapter

CSAJC cloud security alliance SM Japan Chapter　CSA cloud security alliance SM

CSA CoCとは

- Code of Conduct　行動規範のこと
- 欧州の一般データ保護規制（GDPR）準拠のためのCSA行動規範（CoC）を作成
  - あらゆる規模のクラウド利用者向けの、異なる複数のCSPによって提供される個人データ保護レベルを評価するツール
  - 世界中のCSPに、各国の個人データ保護の法令に遵守し、利用者に提供している個人データ保護レベルを、体系化された方法で明示するためのガイダンス

Phase-1 CoC-GDPR翻訳

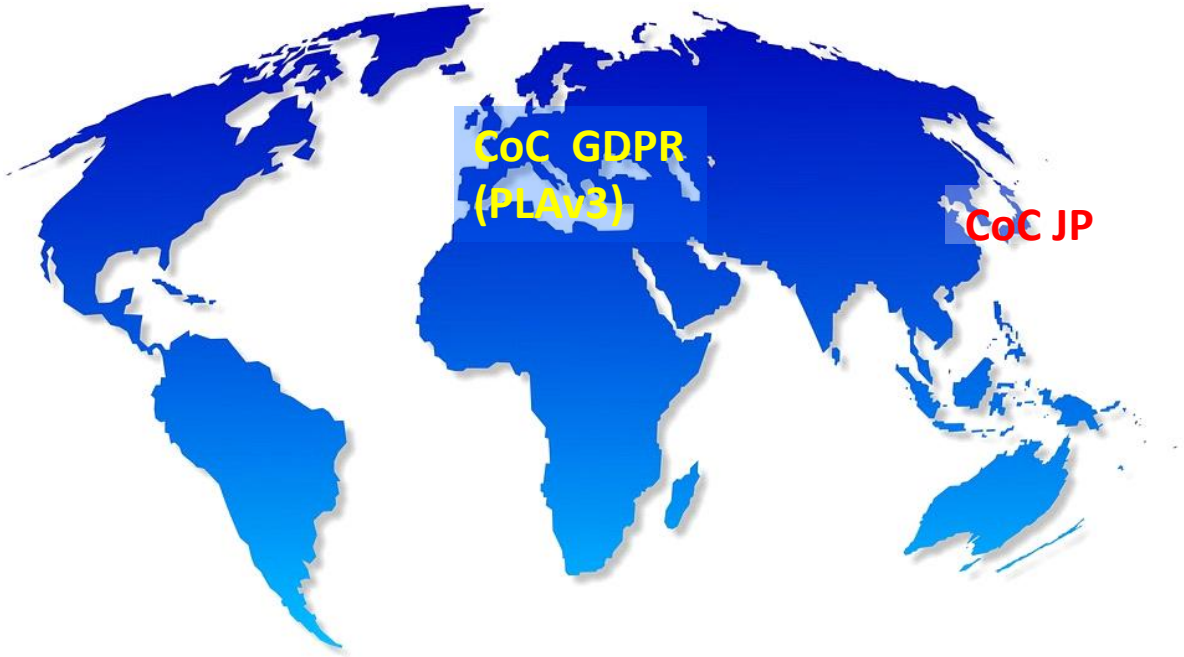
- CoC-GDPRの翻訳版を2018年8月にリリース
- 今後Pahse-2で作成する日本版との区別の為に以後GDPR対応の物はCoC-GDPR、日本の法令対応版はCoC-JPとする

Phase-2 CoC-JPの作業計画

- GDPRと日本法令の差異分を導き出す(中間目標)
- CoC-GDPRと同じ章立てで行けるか検討中
- CoC-JPのリリース　～2019年5月

Phase-3 CoC-JPの英訳と提案

- CoC-JPの英訳　　2018年9月～
- CoC-JP英語版の国際本部への共有　2019年1月～



CoC-JPの方向性

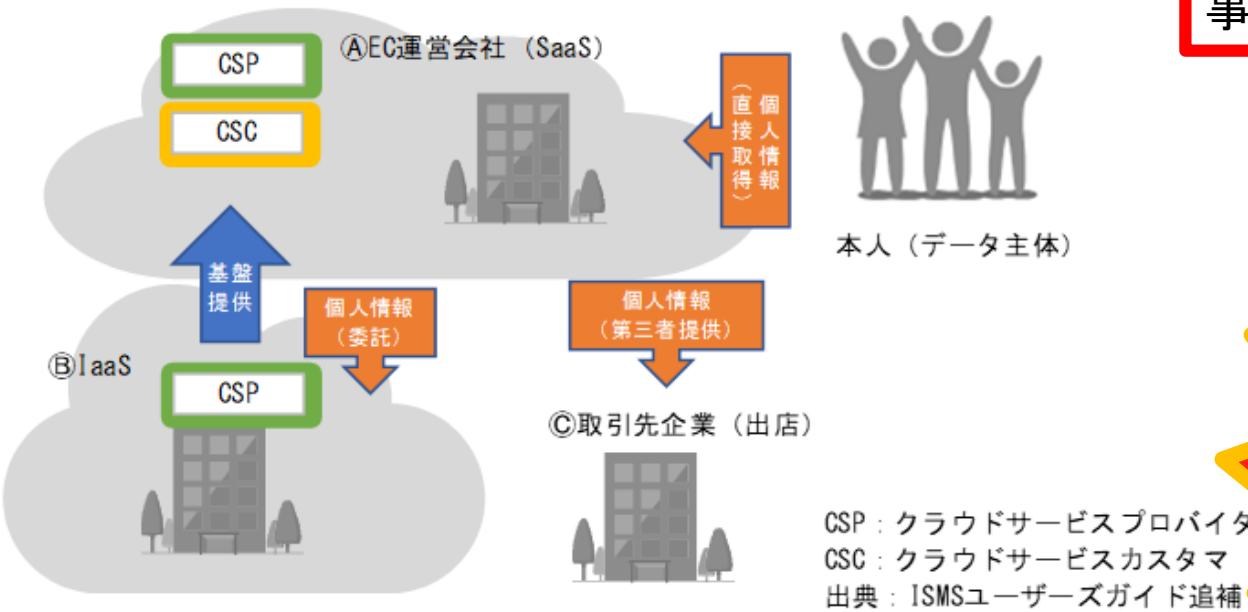
- CoC-GDPRの仕立てを踏襲できる部分は踏襲
- GDPRでは3rdPT(委託先)も取得者
- 保護法の関連するキーワード
  - 委託先管理義務(クラウド事業者は委託先)
  - 海外適用
  - プライバシーマーク(not MUST)

- GDPR充分性認定の着地点(相場)がまだ不明

■ECサイトのモデル

ⒶECサイト運営会社は、個人情報取扱事業者（直接取得）であり、クラウド利用者であり、CSP
ⒷIaaSは、個人情報取扱事業者であり、Ⓐの委託者としてのCSP
Ⓒ取引先企業は、個人情報取扱事業者（第三者提供）

AのECサイト事業者から見るとデータ主体はクラウド利用者
BのIaaS事業者から見ると、AのECサイト事業者はクラウド利用者



CSP：クラウドサービスプロバイダ
CSC：クラウドサービスカスタマ
出典：ISMSユーザーズガイド追補

読み手によって意味が変わってしまう

概略:GDPRと日本法令の違い

- CoC-GDPRはGDPRの元でのクラウド上に個人情報を移す時に気を付けるべき項目である。
- 同様の物を日本版として作る場合
  - 個人情報/個人データ/要配慮個人情報/匿名化個人情報によって法の要求事項が違う(主に同意取得段階)
  - CSPは単なる委託先になり、第三者提供には該当しないと明確に示され、管理監督義務はクラウド利用者(事業主)の責任と明示。
- 海外委託先への法令適用が明示されているが域外転移の禁止は明確には書かれていない。転移先国の法制度が未熟でも委託先の管理能力が十分と自己判定できれば委託可能。
  - 管理監督義務⇒能力確認が重要

とはいえ

- GDPRも保護法も
  - GDPRはEU域内居住者⇒EUからの来日旅行者
  - 保護法も国籍に関係なく個人の情報を対象

- 侵害発生時
  - 72時間以内に当局(各国)に報告できるのか?
    - GDPR　第33条(所轄監督機関への通知)
    - GDPR　第34条(データ主体への通知)
  - 保護法は監督機関への報告は努力義務
    - 金融分野は直ちに報告

GDPR対応について

- EUとの充分性認定の影響が不明瞭
  - 「個人情報の保護に関する法律についてのガイドライン（EU域内から十分性認定により移転を受けた 個人データの取扱い編）案　（施行日：欧州委員会が一般データ保護規則（GDPR）第45条に基づき行う、日本が個人データについて十分な保護水準を確保しているとの決定が効力を生ずる日）」が公表
  - EUは採択プロセスに9/5に入った。
- 充分性認定の範囲は転移についてのみ

対応済みですと報告はしない(除くBCRがEUに認証されている場合)

⇩

未確定要素が多く、法令等が改訂・確定次第対応

対応の一例　ex.GDPR第33条

- 情報漏えい等が起こった場合、72時間以内に当局報告←これを達成する為には
  - サイトを製作した業者では迅速/正確な分析は難しい・・・
    調べる能力があるなら侵入される前に対応できているハズ
  - セキュリティ専門の会社との新規取引
    - 業者選定>NDA締結>見積もり>契約>調査開始
- 予め、セキュリティ専門の会社との契約を結んでおく事により、時間を節約することが出来る。
  - 時間的/精神的にゆとりのある時に準備

CoC-JP版のみのパート

- GDPRを国内事業者で意識しておくべき事
  - 事例集にするか･･･これから検討

ご清聴ありがとうございました