CSA の考える
プライバシー保護の在り方について
クラウド環境下で考慮すべきプライバシー法制の対応

クラウドプライバシワーキンググループ

山崎　万丈

CSAJC cloud security alliance SM Japan Chapter

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

今回の内容

- GDPRについて
- CoC-EUについて
- CoC-JPについて

EUの法制度

- **(1)規則：Regulation**
  - 欧州連合内各国の法令を統一するために制定され、直接の効力を持ち各国内法は不要。すべての国内法に優先。
- **(2)指令：Directive**
  - 国内法に置き換えられた時にのみ各国に効力がある。
    欧州閣僚理事会と欧州議会においてその国の閣僚により可決します。
    ※国内法への置き換えに際し、加盟国にはある一定の裁量権が与えられている。
- **(3)決定：Decision**
  - 加盟国、企業及び個人を対象にして具体的な行為の実施あるいは廃止等を直接的に適用します。
- **(4)勧告：Recommendation**
  - 加盟国、企業及び個人等に一定の行為の実施を期待することを欧州委員会が表明するもの。拘束力が無い。

指令⇒規則

- EUデータ保護指令　Data Protection Directive
  - 1995年～2017年
  - 各国の国内法が必要
- EU一般データ保護規則　General Data Protection Regulation
  - 2018年5月25日～
  - EU各国の国内法は不要

用語

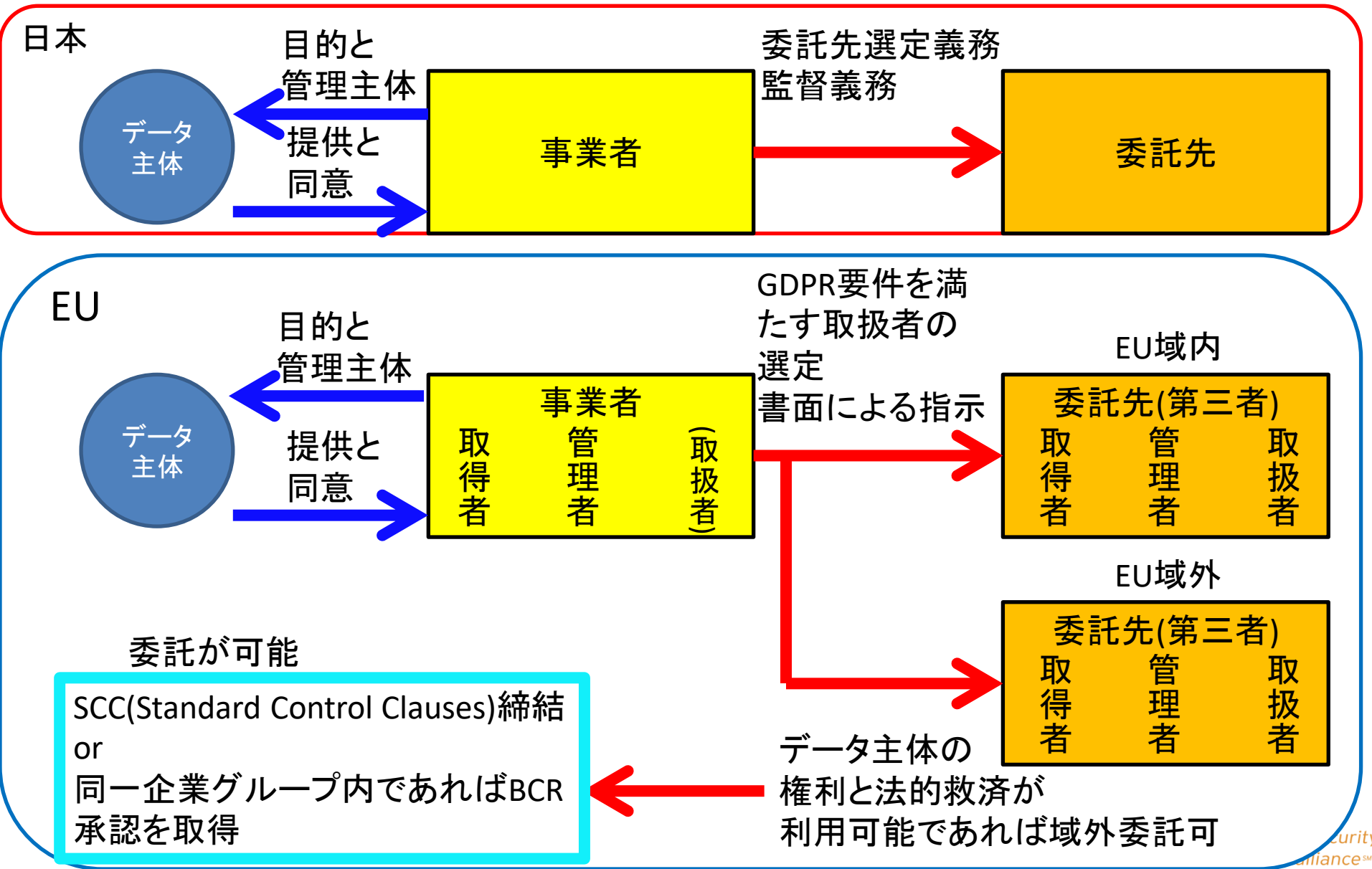
- 個人情報　個人(データ主体)に関するあらゆるデータ
- 取扱い　取得・記録・編集・構造化・保存・修正・復旧・参照・利用・転移による開示・制限・消去
- 仮名化　個人データをデータ主体が識別化されえないように保証する為に技術的・組織的措置を施された物

適用範囲

- 3条1項　EU域内の事業者が個人データを取り扱う場合。
  - 取扱う実際の場所は問わない
- 3条2項　EU域内に拠点のない事業者がEU内在住のデータ主体の個人データを扱う場合

第三国への転移については第5章(第44条～第50条)で詳しく規定

GDPRと改正個人情報保護法の注意点



制裁金について

- ２種類
- 企業の場合、全世界の前年売上高を基準に算定

2%もしくは1千万ユーロいずれか高い方

安全管理策を取らなかった場合
義務付けられた記録を保持して居なかった場合
個人データに対する侵害発生時に報告しなかった場合
DPOを任命して居なかった場合

4%もしくは2千万ユーロいずれか高い方

データ処理に関する原則や同意の取得・センシティブ情報の取り扱いを順守しなかった場合
個人データの域外転移に関するルールを守らなかった場合
監督機関からの命令を守らなかった場合

CLOUD SECURITY ALLIANCE

CODE OF CONDUCT FOR GDPR COMPLIANCE

CSAJC cloud security alliance SM Japan Chapter

CSA cloud security alliance SM

PLAとは

2017/11/21リリース

- Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union
- Code of Conduct (CoC) for GDPR Compliance

自主規制の調整用ツールとして2013年に発表
CSPが顧客および潜在顧客に対して個人データの保護レベルを説明するための物

個人データ保護に必要なベースラインが模索され続けたまま

GDPRで規定されている要件を追加
GDPR第40条Code of Conductも満たす

I序論
II背景
III行動規範の構成

構成

1章　CSA CoCの目的、範囲、方法論、前提条件＆注釈

1.CoCの目的
2.範囲と方法論
3.前提条件
　3.1クラウド利用者の内部環境分析
　3.2クラウド利用者の外部環境分析
4.解説

2章　PLAの行動規範

1.コンプライアンスと説明責任についてのCSPの言明
2. CSP関連窓口とその役割
3.データの処理方法
　3.1概要
　3.2個人情報の位置
　3.3委託先
　3.4クラウド利用者のシステムにインストールされるソフト
　3.5データ処理契約
4.記録の保管2. CSP関連窓口とその役割
　4.1CSP管理者の記録の保管
　4.2CSP処理者の記録の保管
5.データの転移
6.データ保護対策
7.モニタリング
8.個人データ違反
9.データの移植性・移行および転送
10.処理の制限
11.データの保持・返却および削除
　11.1ポリシー
　11.2データ保持
　11.3法的要件を満たしたデータ保持
　11.4データの返却と削除
12協力
13情報提供
14救済
15補償

構成2

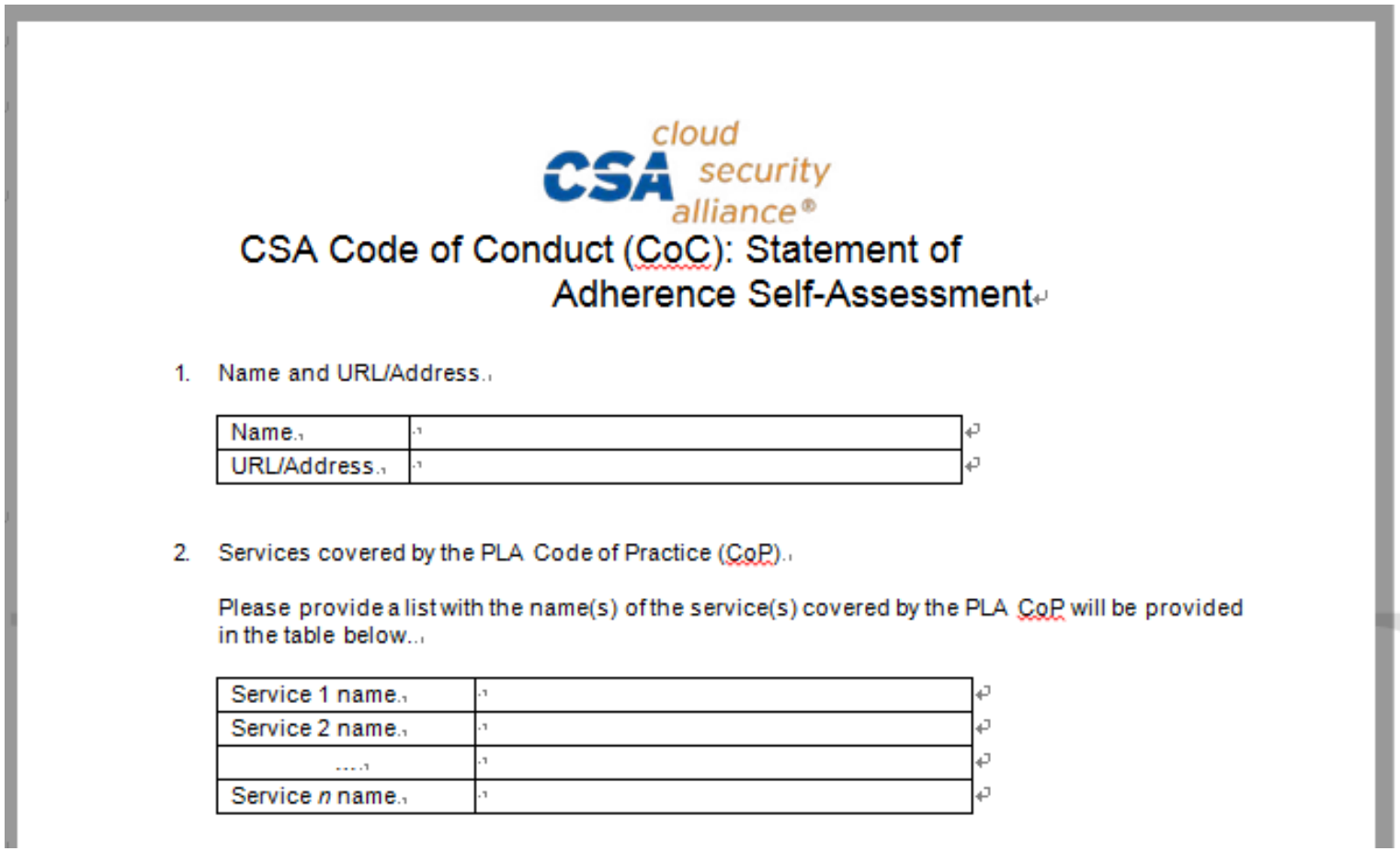
3章　CoCの統制と順守メカニズム

1.技術的要素
  1.1PLA実践規範
  1.2認証スキーム/規範への追従メカニズム
    1.2.1CoC自己評価
    1.2.2CoC第三者認証(評価証明)
  1.3倫理規程
  1.4PLA　WGとOPEN CERTIFICATION FRAMEWORK　WG
2.ガバナンス体制、役割、責任
  2.1PLA実践規範
  2.1PLA WG
  2.2OCF WG
  2.3CSA
  2.4連携組織
3.ガバナンスのプロセスと活動
  3.1PLA　レビュー態勢
  3.2CoC認証レビュー態勢
  3.3
  3.4倫理規定レビュー態勢
  3.5ドキュメントレビュープロセス

別表

1.**PLA3テンプレート**
2.宣誓テンプレート/外部認証に関する宣誓
3.CSA STARプログラムとOCF
4.倫理綱領
5.PLA WG　憲章
6.OCFWG　憲章

Statement of Adherence Self-Assessment



CSA Code of Conduct (CoC): Statement of Adherence Self-Assessment

1. Name and URL/Address

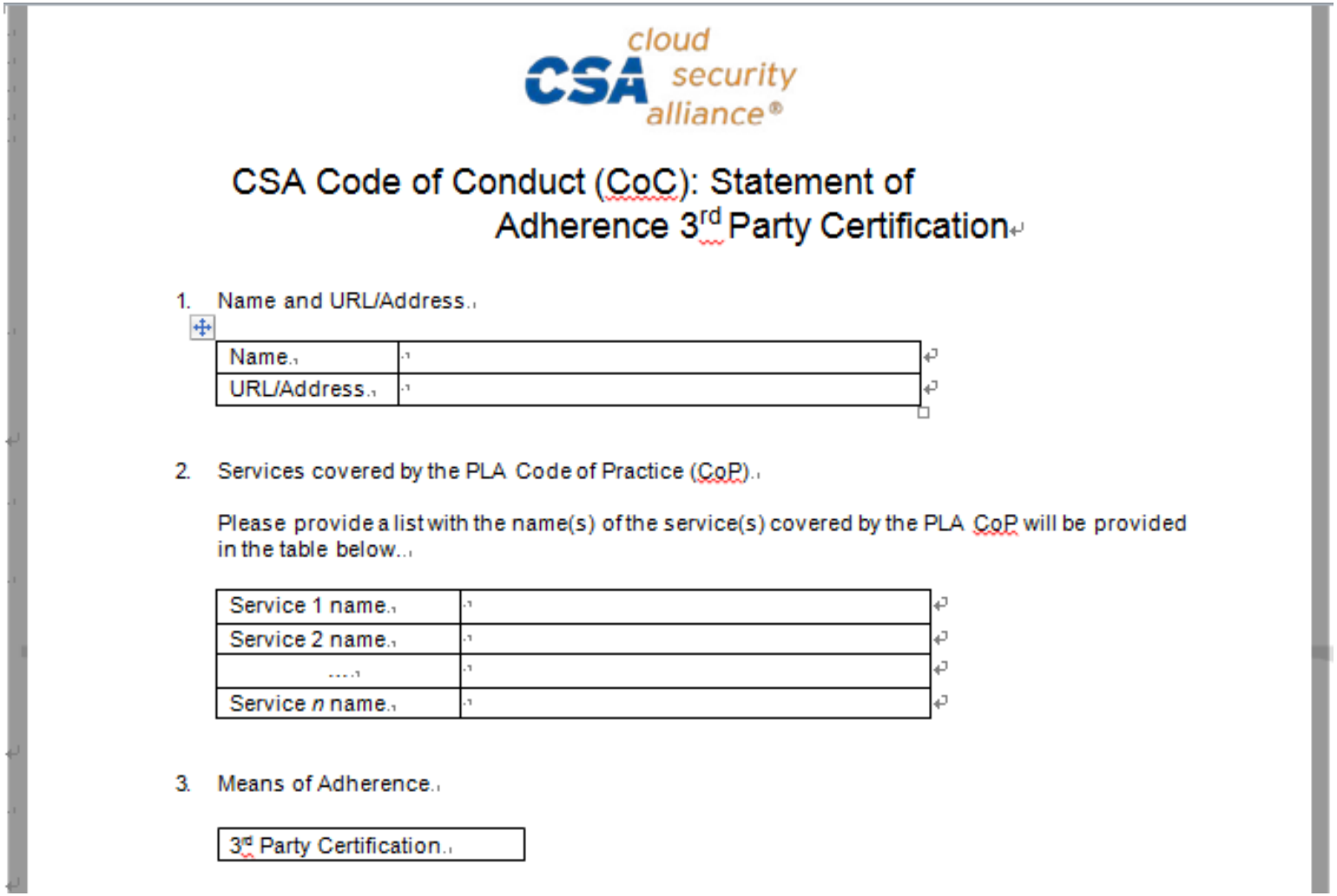
Name	
URL/Address	

2. Services covered by the PLA Code of Practice (CoP)

Please provide a list with the name(s) of the service(s) covered by the PLA CoP will be provided in the table below.

Service 1 name	
Service 2 name	
....	
Service *n* name	

Statement of Adherence 3rd Party Certification



CSA Code of Conduct (CoC): Statement of Adherence 3rd Party Certification

1. Name and URL/Address

Name	
URL/Address	

2. Services covered by the PLA Code of Practice (CoP)

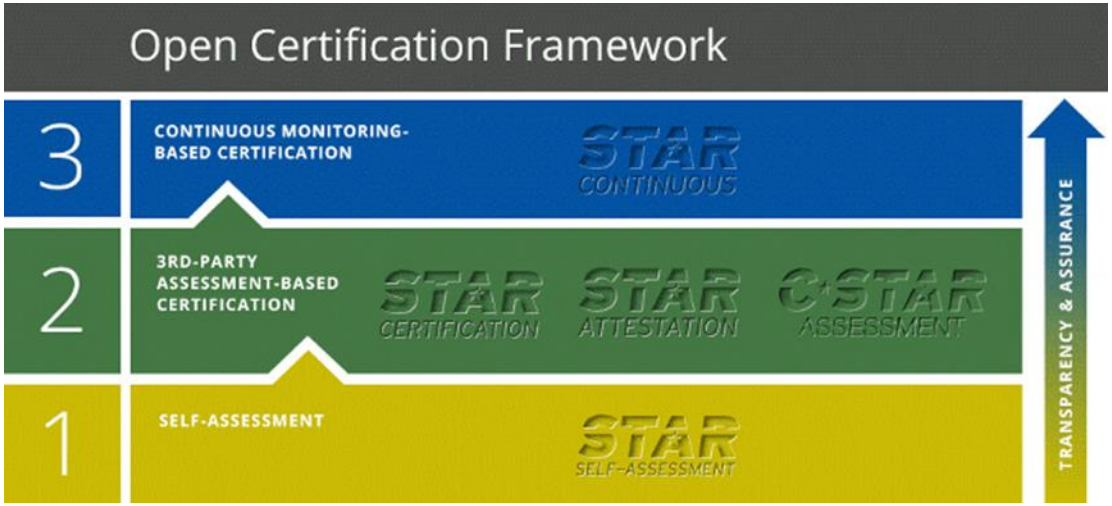
Please provide a list with the name(s) of the service(s) covered by the PLA CoP will be provided in the table below.

Service 1 name	
Service 2 name	
....	
Service *n* name	

3. Means of Adherence

3rd Party Certification

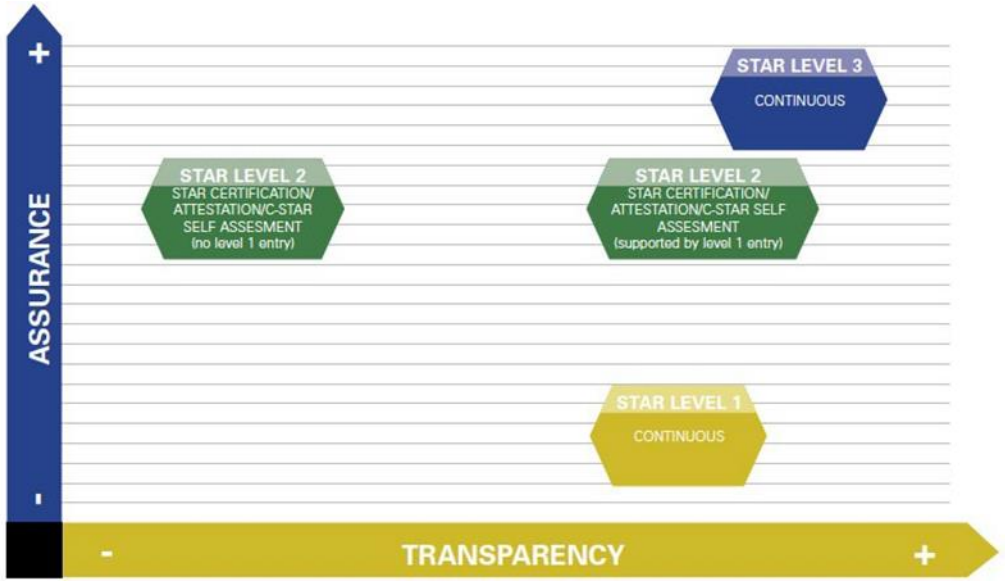
STARとOPEN CERTIFICATION FRAMEWORK



Level 3, 継続的なモニタリング

Level 2, 第三者による認証(認証機関)もしくは評価証明(監査法人)

Level 1, 自己評価のCSA STARレジストリへの登録(9か月以内)

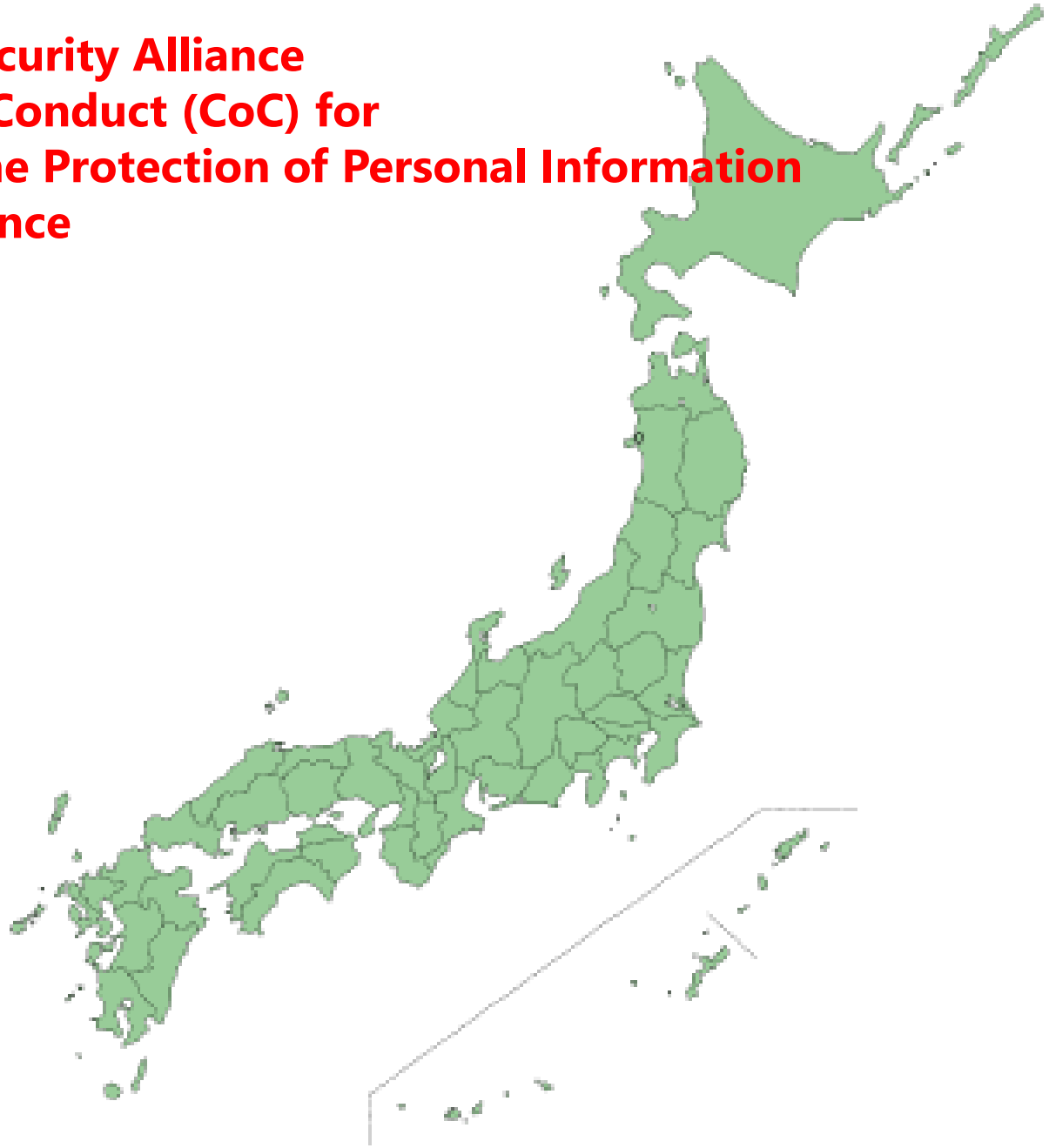


日本語訳版

- 現在　CSA-Japan　PLA WGにて翻訳作業中

NEXT STEP

Cloud Security Alliance
Code of Conduct (CoC) for
Act on the Protection of Personal Information
Compliance



CSAJC Japan Chapter cloud security alliance SM

CSA cloud security alliance SM

目的

日本の個人情報保護法が適用されるケースを想定し

日本のクラウド事業者と利用者や

日本で事業を展開しようと考えている海外の事業者が参考に出来る

行動規範

PLA V3ベース

- CSAとしてPLA(CoC)のフォーマットは踏襲する予定

ご清聴ありがとうございました