

複雑な条件下におけるクラウドシステム間のAPIデータ連携に関する検討

垣岡 順子

APIデータ連携における問題点

外資系企業の本社の人事システム(国外)と日本法人の人事システム(国内)との間で、従業員のデータ(=個人情報を含むデータ)の連携を実現しようとする場合、様々な懸念点がある

調査による解決

想定される懸念点について、法的側面と技術的側面の両面で調査し、それぞれの考慮ポイントと重要度を整理

背景・懸念点・調査方針

背景

- ・ 外資系企業の本社と日本法人で、各々運用しているシステムがある
- ・ セキュリティおよび業務効率化の観点から、API技術によるシステム間の自動データ連携を実現したい

懸念点

- ・ システム間が国境を跨ぐ
- ・ 国外の法令も考慮する必要がある
- ・ 連携するデータに個人情報が含まれる
- ・ 本社が欧米企業の場合、セキュリティに非常に厳しい傾向

調査方針

以下の想定ケースを設定し、前提条件とした調査

- ・ グループ企業内のシステム間における「プライベートAPI」によるデータ連携
- ・ 個人情報を含むデータを連携
- ・ EU圏にある本社のシステムとのデータ連携

法的側面のポイント

日本側

個人情報の保護に関する法律
(個人情報保護法)

EU側

一般データ保護規制
General Data Protection Regulation
(GDPR)

- ・ いずれの法令も、原則ではデータの越境を制限しているが、特例で相互(日本⇔EU)に許容
- ・ GDPRでは「地理的適用範囲」を明文化(国外事業者でも対応が必要になるケースがあり、日本側での意識が必要)

技術的側面のポイント

入力データ検証/バージョン管理

重要度
★★★

正確なデータ連携のための前提条件
(特定のシステムを扱う場合、その独自仕様を意識した適切な対応が必要)

重要度
★★

監視と保守/監査とログ記録/
セキュリティテスト

法令遵守の観点

(各種法令において関連する記述がある)

重要度
★

認証と認可/通信・暗号化プロトコル

より強固な対策が望ましい事項
(可能な限りでの対応を実施)