JIPDECセミナー
「個人情報のクラウド保管 実務における対応ポイント」講演資料

講演資料03
「CBPR認証とクラウド利用でデータ越境移転に省力対応」

本資料は、2023年9月5日（火）開催、JIPDECセミナーで配布した資料です。セミナーお申込み者様限定での配布となりますので、WEB、SNS等への掲載、転載はご遠慮ください。

また、本セミナー（資料）は、プライバシーマークの構築運用指針を解説するものではありません。

2023.09.05

JIPDECセミナー
個人情報のクラウド保管 実務における対応ポイント

CBPR認証とクラウド利用で データ越境移転に省力対応

APECCBPRs
JIPDEC, Japan

2023年9月5日
インタセクト・コミュニケーションズ株式会社

会社概要

インタセクト・コミュニケーションズ株式会社

所在地　：東京都千代田区神田小川町３丁目１番地B･Mビル
設立　　：2000年11月
代表者　：代表取締役社長　譚 玉峰
拠点　　：北海道・京都・大阪・兵庫(姫路)・福岡
人員　　：152名

グループ：中国各社（北京、上海、成都、長春、太原）

事業内容：マルチ決済サービス、中国向け越境EC、アジア向け海外プロモーション・インバウンド支援、アフィリエイト運用代行、システム開発など

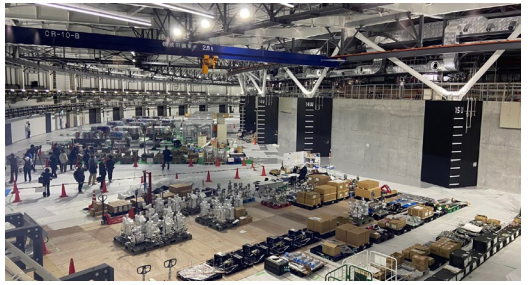
自己紹介

甘利 友朗

経営管理本部 リスク管理室 室長
amari.tomoaki@intasect.co.jp

略歴
・通信事業者にてエンジニアリングに従事
・ソフトバンク株式会社（現：ソフトバンクグループ株式会社）にてグループ情報セキュリティマネジメントに従事
・株式会社ドワンゴにてリスクマネジメント、グループ内部統制に従事
・現在、インタセクトにてリスクマネジメント、経営企画、DX推進プロジェクト、大阪大学 健康情報工学共同研究講座 研究員、等に従事

東北大学内 次世代放射光施設「ナノテラス」の名付け親



CBPR認証とは

CBPR（Cross Border Privacy Rules/APEC越境プライバシーシステム）は、企業等の越境個人データの保護に関して、APECプライバシー原則への適合性を認証するシステムです。

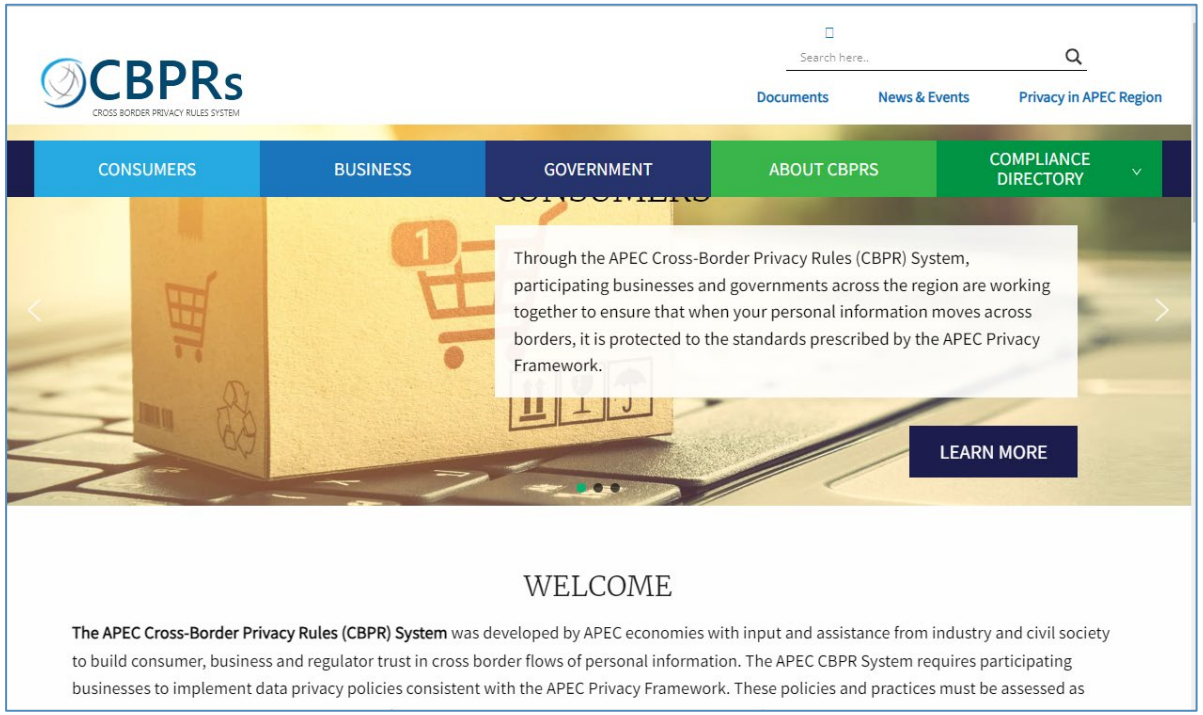
参加している国・地域（9）

日本、アメリカ、韓国、シンガポール、
カナダ、メキシコ、台湾、フィリピン、
オーストラリア

イギリスも意欲的

認証取得事業者（71社）

日本　　：5社 ヤフージャパン、IIJ、PayPay
アメリカ：47社 セールスフォース、アップル、IBM
韓国　　：8社 ネイバー
シンガポール：11社 アリババクラウド



CBPR認証取得の理由

アジアエリアへの事業拡大のため
QRマルチ決済、越境EC、インバウンドなど展開中

1つのアプリで
全て対応

QRマルチ決済サービス「**IntaPay**」対象サービス（2022年12月）

2022年12月
CBPR認証取得

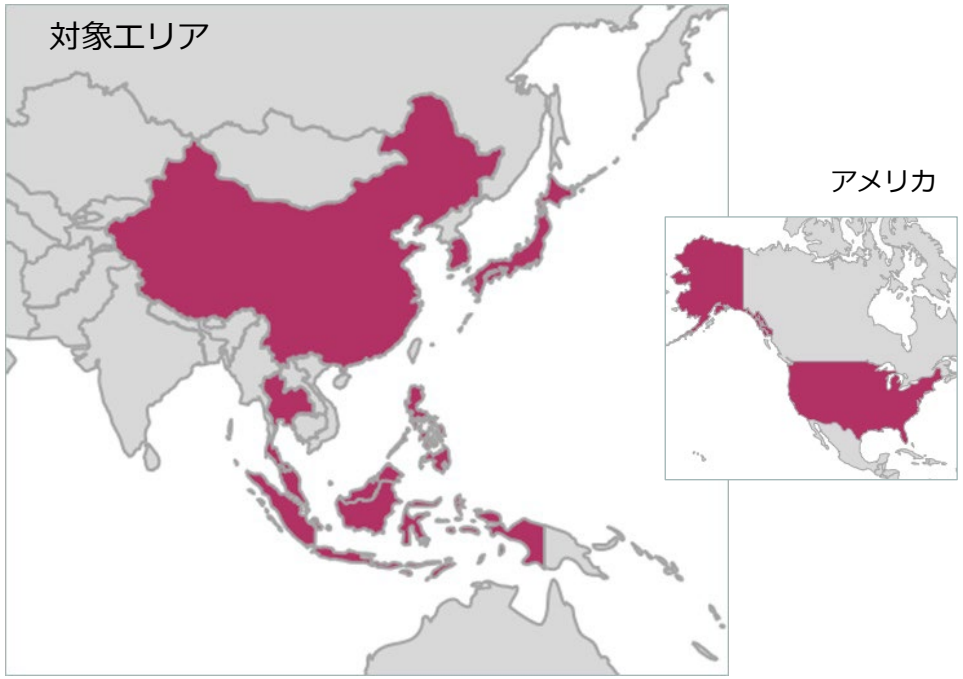
国内対応QR決済サービス

PayPay / 楽天ペイ / LINE Pay / d払い / au PAY / merpay / J-Coin Pay / 銀行Pay / QUOカードPay / Bank Pay / Smart Code ™ / AEON Pay

海外対応QR決済サービス

WeChatPay(微信支付) / Alipay(アリペイ) / UnionPay(銀聯)

支付宝 / Alipay HK / GCash / pay / Touch 'n Go eWallet / truemoney wallet / Alipay+ PARTNER



国内：PayPay、楽天ペイ、LINE Pay、d払い、au PAY、merpay、J-Coin Pay、銀行Pay、
QUOカードPay、Bank Pay、Smart Code、AEON Pay
海外：WeChatPay（中国）、Alipay（中国）、UnionPay（中国）、KakaoPay（韓国）、
TrueMoney（タイ）、GCash（フィリピン）、EZ-link（シンガポール）、
Touch'n Go（マレーシア）、DANA（インドネシア）、Amazon Pay（アメリカ）

CBPR取り組み例

越境ECの場合

WeChat ECモールの例

日本

中国

カスタマーサポートセンター

（グループ会社/中国四川省成都市）

問い合わせ・商品に対する対応等

購入者

注文　＜商品代金+関税+送料＞

商品掲載

出品企業

旅マエも、
旅アトも。

税関事前登録
在庫商品の納品

JAL HONGYUAN

提携倉庫（東京都）

航空便

●納税
●通関

引き渡し

中国国内配達

CBPR申請概要

ざっくり言うと、

認証基準を満たし、
50の質問に答え、
根拠文書を提出する。

※認証基準は個人情報保護全般だが、
Pマークを取得していれば問題にならない内容

※詳しくはJIPDECサイトをご確認ください。
https://www.jipdec.or.jp/project/cbpr.html

■APEC プライバシーフレームワーク原則と APEC CBPR 質問表

原則	APEC CBPR 質問表	確認する内容
通知	1～4	APEC 通知原則に照らし、①取得される個人情報、移転先、及び利用目的に関する貴社のポリシーを本人に必ず理解してもらっているか、②必要最低限の取得になっていることを条件として、本人の個人情報が取得されるタイミング、移転先、及び利用目的を本人に必ず通知しているか。
取得の制限	5～7	APEC 取得原則に照らし、個人情報の取得がその取得のために表明した目的に確実に限定されているか。
個人情報の利用	8～13	APEC 利用原則に照らし、個人情報の利用が取得目的及びこれに適合又は関連するその他の目的を達成することに限定されているか。
選択	14～20	選択手順に関する規定の条件に照らし、個人情報の取得、利用及び開示に関して本人が必ず選択できるようになっているか。
個人情報の完全性	21～25	記録について正確性及び完全性を維持させ、並びに最新な状態に維持しているか。
セキュリティ対策	26～35	個人がその個人情報を組織に預ける際に、個人情報の紛失、不正なアクセス、不正な破壊・利用・変更若しくは開示、又はその他の不正使用を防ぐために、その個人情報が合理的なセキュリティ対策によって確実に保護されているか。
アクセス及び訂正	36～38	本人がその個人情報にアクセスして、訂正することができることを保証しているか。
責任	39～50	APEC 原則の実施方法を遵守することについて確実に責任を果たしているか、また、移転後にこの原則に従って個人情報を確実に保護するための合理的な措置を用意しているか。

3.6.2 **根拠文書の例**

■規程類

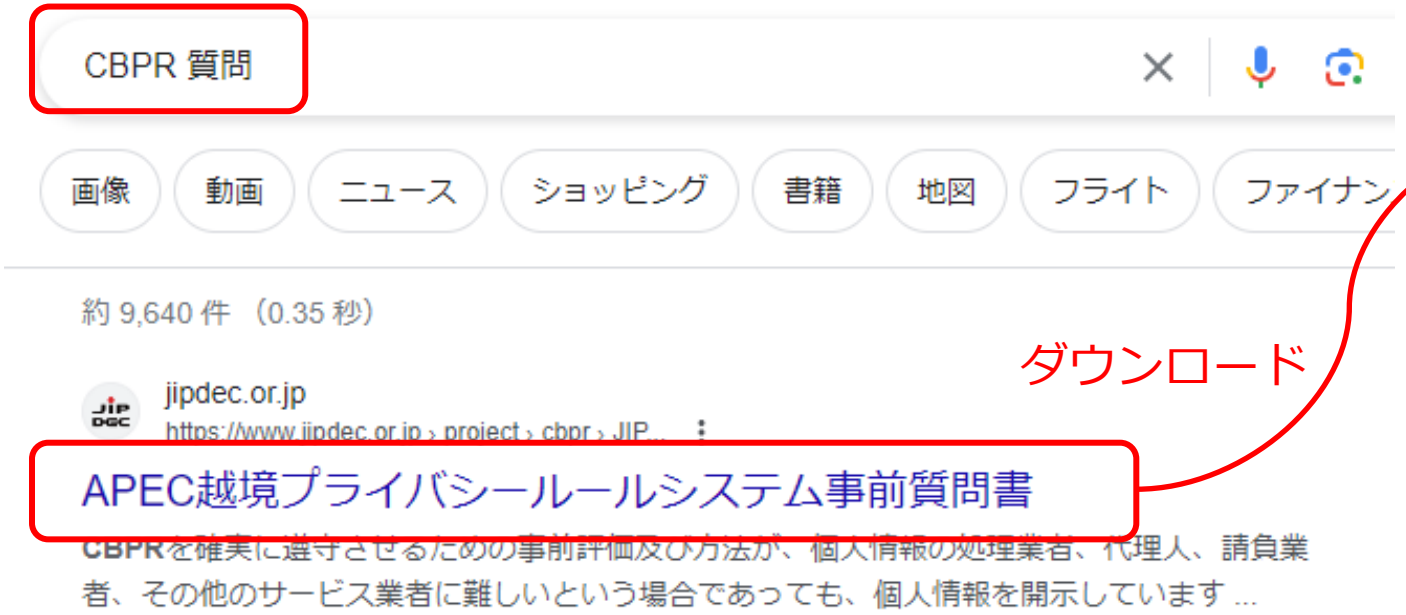
No	提出が求められる文書例
1	プライバシーポリシー（プライバシーステイトメント、個人情報保護方針など）
2	個人情報を特定する手順に関する規程
3	法令、国が定める指針その他の規範の特定、参照及び維持に関する規程
4	個人情報に関するリスクの認識、分析及び対策の手順に関する規程
5	事業者の各部門における個人情報を保護するための権限及び責任の規程
6	緊急事態（個人情報を漏えい、滅失またはき損など）への対応に関する規程
7	個人情報の取得、利用及び提供に関する規程
8	個人情報の適正管理に関する規規程（委託先に関する規程、従業者管理に関する規程、安全管理に関する規程など）
9	本人からの開示等の求めへの対応に関する規程
10	教育に関する規程
11	内部規程の文書管理に関する規程
12	苦情及び相談への対応に関する規程
13	点検や内部監査に関する規程
14	是正処置及び予防処置に関する規程
15	代表者等による見直しに関する規程
16	内部規程の違反に関する罰則規程

■関連文書

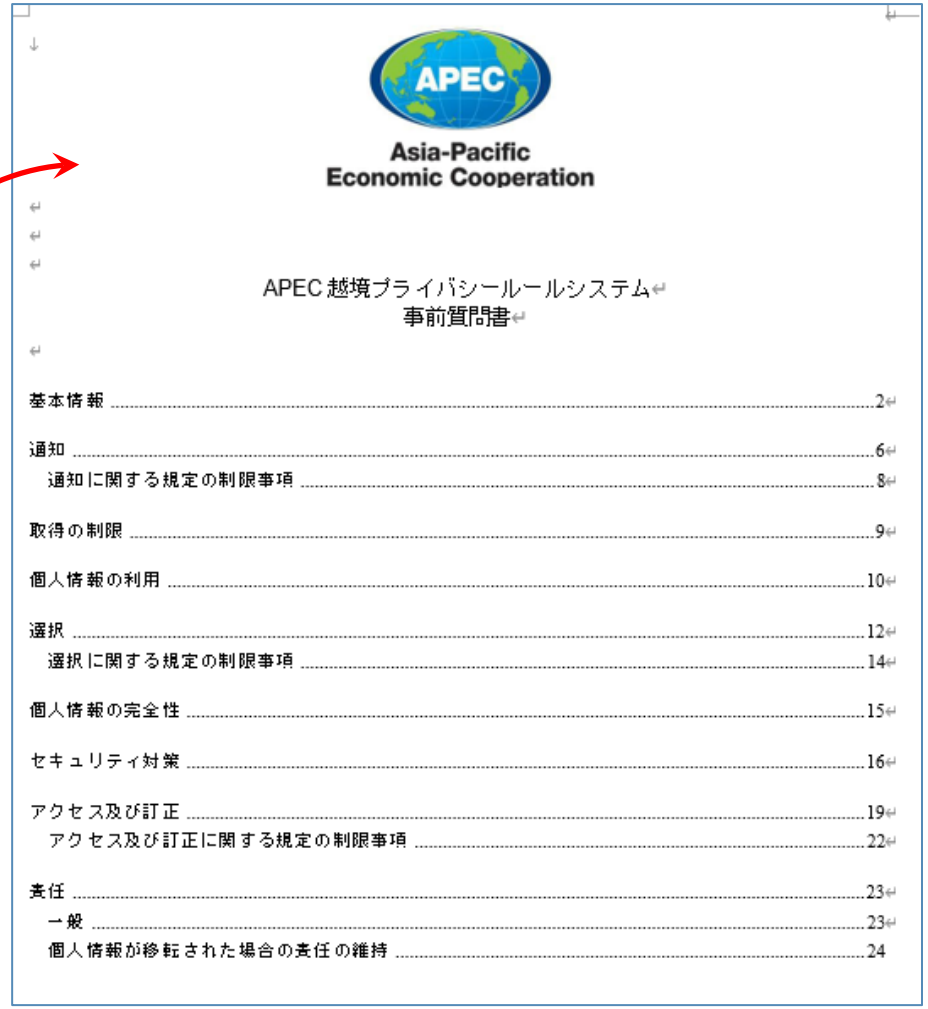
No	提出が求められる文書例
17	参照すべき法令、国が定める指針その他の規範の一覧
18	組織図、CBPR 体制
19	システム構成（システム構成図やネットワーク図などシステム仕様の文書）
20	セキュリティポリシー（情報セキュリティ基本方針等）
21	リスク分析及びリスクに対して講ずべき対策の一覧
22	個人情報取得時に本人に通知している文書
23	個人情報を特定し管理する台帳
24	委託先及び提供先の一覧
25	委託先及び提供先を評価選定した記録
26	委託先及び提供先との契約書
27	教育を実施した記録及び教育テキスト
28	監査を実施した記録及び監査チェックリスト

越境データ移転対応の可視化

検索



ダウンロード



Asia-Pacific Economic Cooperation

APEC 越境プライバシールールシステム
事前質問書

越境データ移転対応の可視化

セキュリティ対策（質問 26~35）

このセクションの質問は、個人がその個人情報を貴社に預けるときに、個人情報の紛失、不正なアクセス、不正な破壊、利用、変更若しくは開示、又はその他の不正使用を防ぐために、その個人情報が合理的なセキュリティ対策によって確実に保護されるために設けられている。

26. 情報セキュリティ方針を実装していますか？

はい		いいえ	

27. 個人情報を、情報の紛失または不正なアクセス、破壊、利用、修正または開示またはその他の悪用のリスクから保護するために実施している、物理的、技術的、運営上の安全保護策について説明してください。

28. 質問 27 に対応して特定した安全保護策が、脅かされる危害の可能性と程度、情報の機密性、また保管状況に鑑みてなぜ適当なのか説明してください。

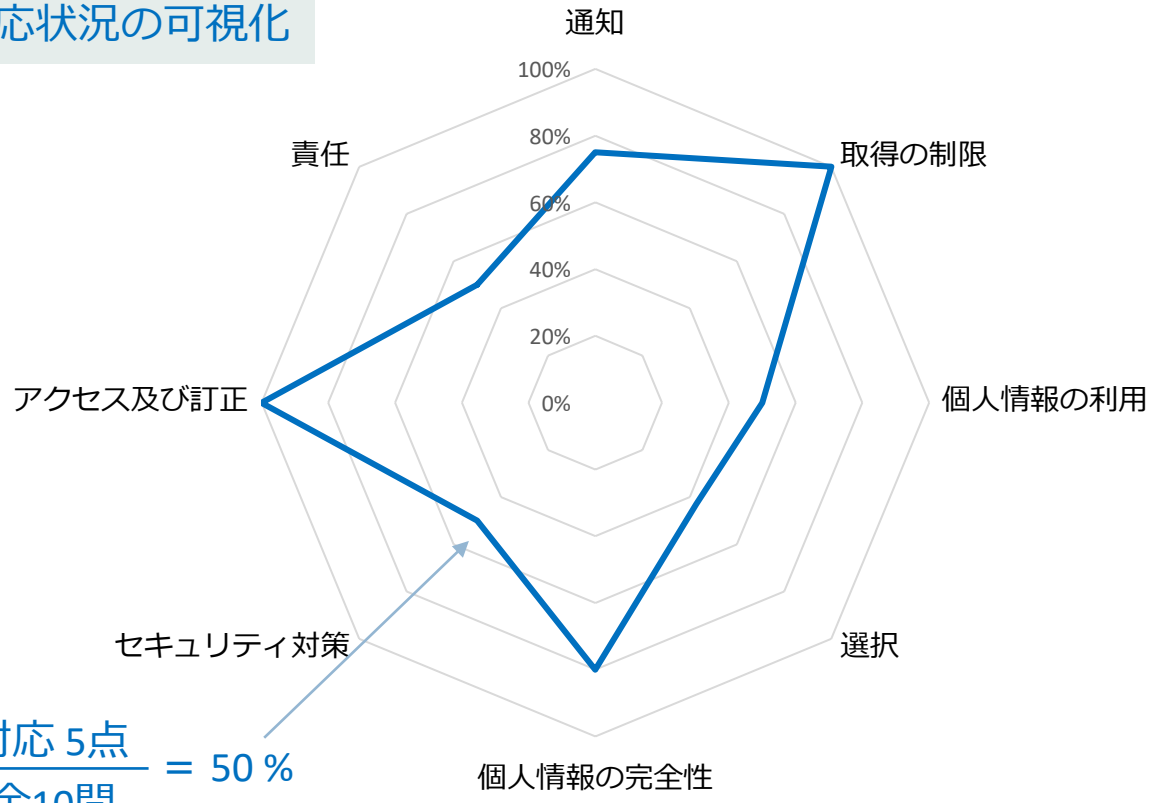
29. 従業員に個人情報のセキュリティの維持の重要性についてどのように認識させているか説明してください（定期的な研修や監督など）

<各項目に点数をつける>　1点　：対応できている
0.5点 ：一部対応している
0点　：対応できていない

「事前質問書」を使えば、APEC内でのレベル感が分かる
・調査が省力、説明が省力、計画策定が省力

CBPR基準 越境データ移転対応度

対応状況の可視化



対応 5点 / 全10問 ＝ 50 %

CBPR取得のポイント 2016年認証取得

- 前提として、当社はPマーク認証取得済み
- Pマーク認証を取得している場合、根拠資料を揃えやすい
- システムとネットワークは「ゼロトラスト・セキュリティ」

  内部からの不正アクセス対応　ファイルサーバー → クラウド・ストレージサービス
- 事務局人数 = 1.5人
- 準備期間 = 2ケ月
- 対象業務 = 2
- 根拠として準備した文書数 = 34（翻訳した文書 = 9）

オペレーショナル・
エクセレンスの実践

2022年

事務局人数 = 1.5人

対象業務 = 9

根拠文書 = 93

CBPR取得のメリット

- 越境ビジネスを重視している取引先への信用向上
  越境での個人情報流通はクライアントにとって不安
- 他社との差別化
  高い個人情報保護意識、国際感覚、制度対応スピード
- 知名度向上
  日本第一号認証事業者
- リスクの最小化
  国際的な標準、JIPDECのフォロー

クラウドサービス

ゼロトラスト・セキュリティ

社内NWファイルサーバーをクラウドサービスに移行。

・セキュリティ対策が省力
・BCP対策が省力
・環境構築、運用が省力

03

強固なセキュリティ

様々な不正アクセスや情報漏えいの脅威から大切なデータを守ります

- AWS東京リージョンでサービス提供
- 未知のランサムウェアにも対応でき、軽快に動作するランサムウェア対策
- 機密情報のリモート削除に対応したIRM機能
- 情報の持ち出しを制御し、情報漏えいのリスクを防ぐDLP機能
- 通信経路の暗号化（SSL 256bit）およびパスワード暗号化（SHA-2）
- アップロード時のウイルスチェック後、無害ファイルのみAES-256暗号化方式で保存
- IPアドレス制限／ワンタイムパスワード／デバイス認証
- IDSによる侵入検知、Firewallによる通信の制御

クラウドサービス

リージョン、準拠法

リージョン（データセンターが設置されているエリア）を日本にすることで、データは日本にある。

越境移転する/しないは、リージョンをベースに考える。

合わせて準拠法も日本にする。

・調査が省力

AWS契約当事者	準拠法	管轄裁判所
Amazon Web Services Japan Good Kaisha	日本国法	東京地裁

クラウドサービス

AWS Security Hub

AWSのセキュリティ状態を包括的に把握することが可能で、セキュリティ業界標準およびベストプラクティスに照らした環境チェックを行うのに有効です。

＜基準＞
- AWS 基礎セキュリティのベストプラクティス v1.0.0
- NIST Special Publication 800-53 Revision 5
- PCI DSS v3.2.1
- CIS AWS Foundations Benchmark v1.2.0/v1.4.0

- 調査が省力
- 対応が省力
- 説明が省力

対策状況の可視化

クラウドサービス

脱炭素

Customer Carbon Footprint Tool
炭素排出量の算出、レポート、無料。
オンプレミスとの比較。
AWS側でも削減推進。

炭素排出量の可視化

- 調査が省力
- 排出量算出が省力
- 説明が省力
- 削減対応が省力

AWS

2040年までに二酸化炭素排出量を実質ゼロとする「気候変動対策に関する誓約」への参加企業が100社を突破

2021/05/12

本誓約に署名した105社は合計、全世界で年間1兆4000億ドル以上の売上高、16カ国25業種で500万人以上の雇用を創出

AmazonとGlobal Optimismが共同調印した「The Climate Pledge」は、パリ協定の目標を10年前倒しで達成する取り組みで、2040年までに炭素排出量の実質ゼロ化を目指す

AWS使用による再生可能エネルギーへのシフト。

周辺環境

クライアント認証

・対応が省力

ID/Passwordだけでなく、クライアント証明書を使用して、
当社の社員かつ特定の端末だけがアクセス可能。

JCAN証明書

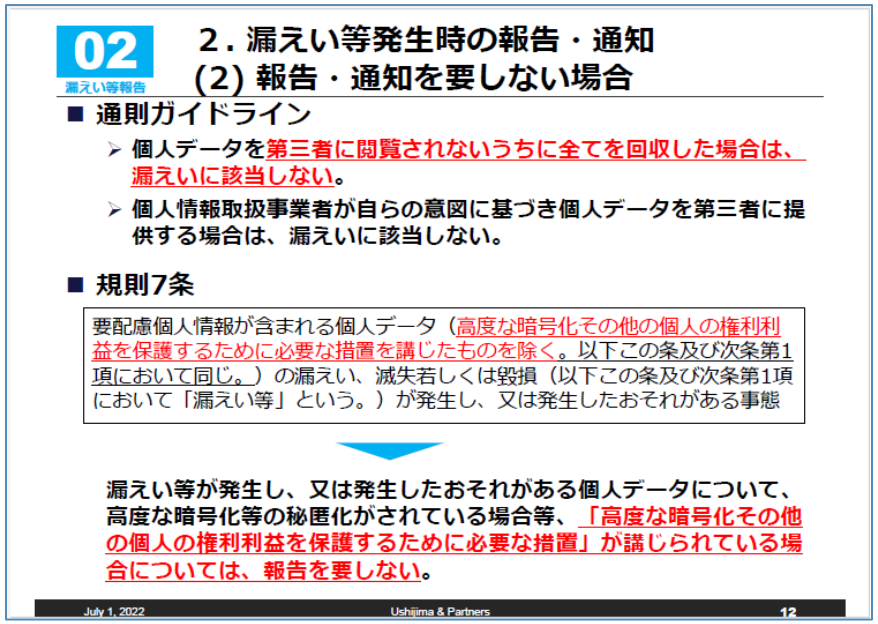
JCAN証明書は、インターネット上の企業内個人の証明書であり、所属する組織や役職などを証明することができます。

周辺環境

高度な暗号化

重要！

個人データが高度な技術によって暗号化されていれば、万一漏洩しても
個人情報保護委員会には報告不要。



02 漏えい等報告

2．漏えい等発生時の報告・通知
(2) 報告・通知を要しない場合

■ 通則ガイドライン

- 個人データを第三者に閲覧されないうちに全てを回収した場合は、漏えいに該当しない。
- 個人情報取扱事業者が自らの意図に基づき個人データを第三者に提供する場合は、漏えいに該当しない。

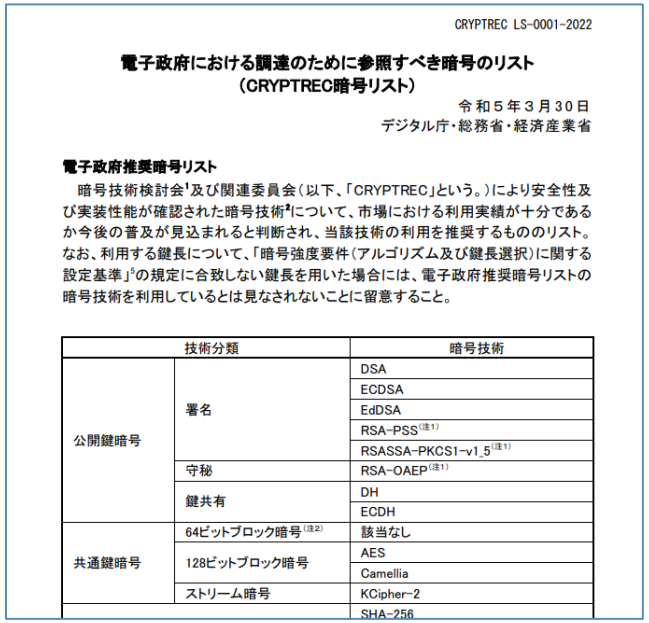
■ 規則7条

要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下この条及び次条第1項において同じ。）の漏えい、滅失若しくは毀損（以下この条及び次条第1項において「漏えい等」という。）が発生し、又は発生したおそれがある事態

漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合等、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合については、報告を要しない。

July 1, 2022 Ushijima & Partners 12

2022/7/1 JIPDECセミナーより



CRYPTREC LS-0001-2022

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

令和５年３月30日
デジタル庁・総務省・経済産業省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[5]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		EdDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
		SHA-256

電子政府推奨暗号リスト

JCAN証明書

JCAN証明書はクライアント認証の他に、電子契約、電子印鑑、メールなりすまし対策などの用途があります。

まとめ

CBPR認証とクラウド利用で省力化

- 調査　基準の活用
- 説明　状況の可視化
- セキュリティ　サービス利用、暗号化
- BCP　環境構築、被害軽減
- 脱炭素　算出作業、削減対策

結論

「 CBPR認証を取得したほうが楽。 」