

CPRA解説オンラインセミナー ～ BtoB企業が求められる実務対応を分かりや すく解説 ～

(2021年1月13日)

主催: ジェトロ・サンフランシスコ/ロサンゼルス様

協力: 北加日本商工会議所様、南カリフォルニア日系企業協会様

S&K Brussels 法律事務所

事務所代表・マネージングパートナー(東京・NYオフィス)

弁護士 杉本 武重

T+81 3 6429 8040; +1 347 259 2661; +32 494 67 33 51

takeshige.sugimoto@sandkbrussels.com

目次

I.	CPRAの執行開始に向けた動きとBtoB企業	3
II.	CPRAの影響範囲の画定－BtoB企業の「事業者」への該当性	10
III.	BtoB企業が収集している個人情報とCPRAの適用関係	16
IV.	BtoB企業のためのCPRAコンプライアンスへのロードマップ	28
V.	まとめ	44
	付録1(CPRAデータマッピング質問票－人材採用の例での回答)	48
	付録2(CPRA下で紛争化しやすい類型を考える上で参考となるGDPR制裁金決定事例)	70

I. CPRAの執行開始に向けた動きとBtoB企業

はじめに

- カリフォルニア州の新しい個人情報保護法であるCCPAをさらに強化する形で改正するカリフォルニア州プライバシー権利法(CPRA: California Privacy Rights Act)が2020年11月3日にカリフォルニア州の住民投票において可決された。
- CPRAは、既存のCCPAを、EUの厳しい個人情報保護法であるGDPR(General Data Protection Regulation: 一般データ保護規則)の内容に近づけるとともに、かつ独自に強化することを内容とするものである。
- CPRAは幅広いBtoB企業に対して適用される。程度の差こそあれ、適用対象となるCPRA上の「事業者」に該当する場合には、CPRA対応を行う必要がある。
- 本プレゼンテーションでは、BtoB企業が求められるCPRAの実務対応について解説する。

CCPAとBtoB企業

- カリフォルニア州内に止まらず、全米におけるプライバシー保護水準である。これは今後立法される米国連邦データプライバシー法においても当然の前提として位置づけられることに注意が必要である。すなわち、BtoB企業であっても、CCPAが求めるプライバシー保護水準を早期に満たしておくことが極めて重要となる事態が近い将来に生じることが考えられる。
 - カリフォルニア州の消費者(住民)の個人情報について当該消費者に以下の権利を与えた。
 - プライバシー通知において詳細な内容の開示を行うことを事業者に義務付けた。
 - 個人情報を処理するサービスプロバイダの活動を契約上制限することを事業者に義務付けた。
 - 消費者の権利行使に関係する従業員に一定のCCPAに関するトレーニングを受けさせることを事業者に義務付けた。
- CCPAの遵守期限は2020年1月1日、CCPAの執行開始は2020年7月1日。CCPA規則は2020年8月14日に適用開始となった。

CCPA執行動向

- カリフォルニア州司法長官によって執行可能なCCPA条項
 - 差し止め及び①違反ごとに最大2500ドルの民事制裁金、又は②意図的な違反ごとに最大7500ドルの民事制裁金
 - 事業者はカリフォルニア州司法長官からのCCPA不遵守の通知後30日間違反状態を治癒することができる。
 - カリフォルニア州司法長官は、2020年7月1日に30日間の通知(30-day notices)の送付を開始
 - ほとんどの通知は「Do Not Sell My Personal Information」のリンクが事業者のウェブサイトに含まれていないことに基づいている。
- 私的訴訟権(但し、消費者の(狭義の)「個人情報」の侵害に関してのみ)
 - インシデント毎に消費者一人あたり最大750ドル(法定損害)、又は実損害のいずれか高い方の金額での損害賠償請求が可能
 - 法定損害賠償の訴訟
 - 事業者は30日間の書面通知及び違反を治癒する機会を提供しなければならない。
 - 実損害賠償の訴訟
 - 事業者への通知は不要

CCPA関連のデータ侵害に関する最初の和解(2020年12月)

In Re: Hanna Andersson and Salesforce.com Data Breach Litigation

- 子供服小売販売のHanna Anderssonと当社が利用していたEコマースプラットフォームの提供元であるSalesforce.comに対しての集団訴訟が2020年2月に提起された。不正アクセスからのマルウェア感染により、顧客名、住所、クレジットカード番号、当該カードのCVVコード、カード有効期限等の個人情報(200,273名分の米国の消費者の個人情報。うちカリフォルニア州の消費者の個人情報は10,000件以下)が漏洩。Hanna AnderssonはSalesforce.comのEコマースプラットフォームを利用しており、当該プラットフォームがマルウェアに感染していたと主張。
- 上記の個人情報の漏洩自体は、CCPAの適用開始日の前である2019年中に発生したものであったため、この点に関する裁判所の判断が注目されたが、本訴訟は訴え提起の段階を超えて進行することはなかったため、判断は示されなかった模様
- 400,000米ドルの和解基金: 参加者1人あたり最大500ドル(追加の償還のオプションあり) 及び参加者1人あたり最大38ドル(推定) - CCPAの私的訴訟権によって規定された消費者1人あたり100ドルから750ドルよりはるかに少ない
- Hanna Anderssonが必要とされるセキュリティの改善
 - NISTリスクマネジメント管理フレームワークと一致するリスク評価
 - リスクマネジメントフレームワーク(RMF: Risk Management Framework)とは、組織や情報システムにおける情報セキュリティリスク(プライバシーリスクを含む)の管理方法を示したもの
 - ▶ NIST Risk Management Framework: <https://www.nist.gov/cyberframework/risk-management-framework>
 - クラウドサービスアカウントの多要素認証及びアラートプロセス
 - サイバーセキュリティのディレクターを含む追加の技術者
 - PCI(Payment Card Industry) 認定資格のあるセキュリティ評価者と連携したPCIコンプライアンス証明書
 - フィッシングと侵入テスト、追加の侵入検知と防止、マルウェアとウイルス対策及び監視アプリケーション
 - eコマースログの定期的なレビュー

CPRAの重要な概要：新当局及び私的訴訟権

- カリフォルニアプライバシー保護当局（**CPPA**: California Privacy Protection Agency）の創設
 - CPRAの実施及び執行と制裁金の賦課を担当する新当局
 - 委員長を含む5名の委員によって構成される委員会。委員長及び委員1名は州知事が任命、司法長官、上院規則委員会及び下院議長がそれぞれ1名の委員を任命する。これらの任命は、プライバシー、技術、消費者権利の分野に専門知識を持つカリフォルニア州の住民から行われる。
- 私的訴訟権への修正
 - CCPAの私的訴訟権を拡大し、パスワード又はセキュリティ上の質問との組み合わせの電子メール・アドレス及びそのアカウントへのアクセスが許可される回答が、無権限アクセス、流出、窃取又は開示の対象となるデータ侵害をカバーする
 - データ侵害後の合理的セキュリティ手続・慣行の実施及び維持が当該データ侵害に関して「治癒」を構成しないことを明確化
- 治癒期間が保証されないこととなった。
- 16歳未満の消費者の個人情報に関するCCPA違反への制裁金の増額

BtoB企業に関連するCPRAのタイムライン

日程	関連イベント
2020年11月3日	■ CPRA住民投票
2020年12月	■ 役職員等の雇用関連個人情報及び取引先の従業員の個人情報に関するCPRA一部規定の適用猶予に関する規定等の発効 ■ カリフォルニアプライバシー保護当局(CPPA : California Privacy Protection Agency)の創設に向けた動きの開始
2021年7月1日	■ カリフォルニアプライバシー保護当局によるCPRA規則のドラフトの開始(2021年冬にはCPRA規則のファーストドラフトが公表されることが予想される)
2022年1月1日	■ 12か月のlook back期間の開始(CPRA上の事業者の義務は2022年1月1日以降に収集した個人情報に関して適用される)
2022年7月1日	■ カリフォルニアプライバシー保護当局によるCPRA規則の採択期限
2023年1月1日	■ CPRA適用開始日 ■ 役職員等の雇用関連個人情報及び取引先の従業員の個人情報に関するCPRA一部規定の適用猶予に関する規定の失効
2023年7月1日	■ CPRA執行開始日

II. CPRAの影響範囲の画定－BtoB 企業の「事業者」への該当性

CPRAの適用を受けるBtoB企業

- 「CPRAの適用を受けるBtoB企業」は、カリフォルニア州内の米国子会社だけではない。
 - ✓ カリフォルニア州外の他の米国子会社
 - ✓ カリフォルニア州内に事業所を持つ日本国内の日本企業
 - ✓ カリフォルニア州内に事業所を持たない日本国内の日本企業（米国子会社の親会社）

CPRAの影響範囲の画定－BtoB企業と「事業者」

- CPRA対応の要否を判断するには、まず、自社またはそのグループ会社がCPRAの適用を受ける「事業者(business)」に該当するかを検討する必要がある。
- 次の<テスト1>、<テスト2>、<テスト3>又は<テスト4>に該当する場合には、「事業者」に該当し、CPRAの適用を受けるため、CPRA対応を取ることが必要となる。

<テスト1>

要件① 消費者(カリフォルニア州の住民)の個人情報を取得(第三者が自身のために個人情報を取得する場合も含む)し、単独又は共同でその処理の目的と手段を決定し、カリフォルニア州で事業を行っている、利益又は金銭的便益を目的とする主体であること

要件② 以下の3つの事由のいずれかを充足すること

(A) 暦年の1月1日時点で、前暦年の年間総収入(annual gross revenues)が2500万米ドルを超えていること

(B) 10万件以上の消費者又は世帯の個人情報を、年間ベースで、単独若しくは組み合わせで購入若しくは販売又は共有する。

(C) 消費者の個人情報の販売又は共有から年間収入の50%以上を得ている。

CPRAの影響範囲の画定－BtoB企業と「事業者」

<テスト1>

要件①

■ 「カリフォルニア州で事業を行っている」の要件

- ✓ 日本企業又はその米国拠点についてカリフォルニア州内に拠点は無いが
 - ✓ ウェブサイトを通じてカリフォルニア州の住民の個人情報を取得する場合
 - ✓ カリフォルニア州の住民の商品又はサービスを提供している場合、又は
 - ✓ カリフォルニア州内に取引先や代理店がある場合

要件②

■ (A) 暦年の1月1日時点で、前暦年の年間総収入 (annual gross revenues) が2500万米ドルを超えていること

- ✓ 法人ごとに、単体ベース、世界ベースで総収入の金額を算定して対応する(この実務に沿ったCA州AGオフィスのパブコメへの回答も存在する)
- ✓ 年間総収入は、費用を引く前の収入を意味する。

■ (B) 10万件以上の消費者又は世帯の個人情報を、年間ベースで、単独若しくは組み合わせて購入若しくは販売、又は共有する。

- ✓ 要件(A)を満たさない場合、ウェブサイトを通じてカリフォルニア州からのアクセスが多くある場合には、カリフォルニア州の個人からIPアドレスやCookie識別子等の個人情報を収集していることがある。
- ✓ この件数が年間10万件以上(1日平均で約274件)の場合には、要件(B)を満たすことになる。

CPRAの影響範囲の画定－BtoB企業と「事業者」

<テスト2>

テスト1に該当する事業者を支配し、又は、当該事業者により支配され、かつ、当該事業者と共通のブランドを有し、**当該事業者が消費者の個人情報を共有する主体**

■ 「支配」:

- ① 事業者の発行済議決権株式の50%超について、保有しているか、議決権を有していること
- ② 役員の過半数もしくは同様の権能を行使する個人を何らかの方法で支配していること、又は
- ③ 会社の経営について支配的な影響を及ぼす権限を有していること

■ 「共通のブランド」: 共有された名称、サービスマーク又は商標であって、**平均的な消費者が二つ以上の団体が共通に所有していることを理解できるような、共通の名称、サービス・マーク又は商標**

- ✓ 日本企業は、グループ会社の中にテスト1に該当する事業者があり、かつ商号の一部が共通している等で当該事業者と共通のブランドを有している場合であって、当該事業者から消費者の個人情報の共有を受けている場合には、テスト2に該当することになる。
 - ✓ 多くの日本企業が米国子会社から従業員の個人情報や取引先の従業員の個人情報の共有を受けていることを踏まえると、これらの個人情報にカリフォルニア州の個人のもが含まれている場合には、多くの日本企業がCPRAが適用される事業者該当することになる。

CPRAの影響範囲の画定－BtoB企業と「事業者」

＜テスト3＞

各事業者が少なくとも40%の持分を有する事業者で構成されるジョイントベンチャー又はパートナーシップ

- ジョイントベンチャー又はパートナーシップと、ジョイントベンチャー又はパートナーシップを構成する各事業者は、それぞれ別の事業者とみなされる。
- 各事業者が保有している個人情報、及びジョイントベンチャー又はパートナーシップに開示されている個人情報を他の事業者と共有することはできない。

＜テスト4＞

カリフォルニア州で事業を行う者で、テスト1、テスト2又はテスト3の対象とならず、CPRAに準拠、拘束されることに同意することを自主的にカリフォルニア州プライバシー保護当局に証明する者

III. BtoB企業が収集している個人情報とCPRAの適用関係

BtoB企業が収集している個人情報とCPRA

- BtoB企業が収集している個人情報は、CPRAとの関係では、以下の類型に整理することができる。

A) CPRA一部規定の適用猶予の対象となる以下の個人情報

1. 役職員等の雇用関連個人情報
2. 取引先の従業員の個人情報

- ✓ 従業員/契約受託先のプライバシーの利益も保護されるべきであるが、従業員/契約受託先と事業者の関係は、消費者と事業者の関係とは異なるため、当該保護においても相違点が考慮されるべきである。また、CPRAはNational Labor Relations Actの下での組合加入権や団体交渉に干渉することを意図したものではない。それがCCPA上の従業員及びBtoBコミュニケーションのための適用除外を2023年1月1日まで延長することとした目的及び意図である(SEC. 3. Purpose and Intent, A. Consumer Rights, para 8)。

B) CPRA一部規定の適用猶予の対象とならない以下の個人情報

3. ウェブサイトへの訪問者の個人情報(クッキーを通じた取得)
4. それ以外の個人情報、例えば
 - ✓ 自社ウェブサイトの問い合わせフォームからの連絡
 - ✓ マーケティングを通じて収集する個人情報のうち上記2の適用猶予対象となる文脈以外で取得したもの

A) CPRA一部規定の適用猶予の対象

1. 役職員等の雇用関連個人情報

- 以下の役職員等の雇用関連個人情報について、以下の範囲に限りCPRAの一部の規定の適用が2023年1月1日まで猶予される。

適用猶予となる個人情報	適用猶予となる利用目的の範囲
事業者の求職者、従業員、所有者、役員、オフィサー、医療スタッフメンバー又は契約受託先(「役職員等」)として行動する過程において、当該事業者が当該自然人について収集する個人情報	当該自然人の個人情報が、役職員等としての当該自然人の役割又は以前の役割の文脈内でのみ収集及び使用されるもの
事業者が収集する、役職員等として行動する自然人の緊急連絡先である個人情報	当該個人情報が専ら緊急連絡先をファイルに入れる文脈内で収集及び使用されるもの
役職員等として行動する自然人に関連する他の自然人の特典を管理するために保有が必要な個人情報	当該特典を管理する文脈内でのみ収集及び使用されるもの

- ✓ 役職員等の雇用関連個人情報の収集の一部には適用猶予とならないものがある。
 - ✓ 適用猶予となる範囲から外れる可能性があるもの→外れると全てのCPRAの規定の適用を受ける
 - ✓ 日本本社が、①米国子会社での幹部候補者の採用を承認するためにCVを受け取る(「事業者」の「求職者」ではない)、②米国子会社所属の駐在員の個人情報を収集する(「事業者」の「従業員」ではない場合)、③日本本社のグローバル内部通報制度によって米国子会社の従業員からの通報を受け取る(「事業者」の「従業員」ではない)等
 - ✓ 役職員の家族の個人情報を収集・使用する
 - ✓ 事業所の防犯カメラに撮影された従業員の映像に含まれる個人情報を防犯目的以外で使用する
 - ✓ 従業員の人事評価に関する情報を担当者以外の他の従業員と共有する
 - ✓ 役職員等の個人情報についてもCPRA対応のためのデータマッピングを行うことが必要
- ✓ 2023年1月1日より前に適用猶予の期限を延期又は恒久化する法改正がなされなければ、役職員等の個人情報について適用猶予されているCPRAの他の規定も全て適用されることになる。

A) CPRA一部規定の適用猶予の対象

1. 役職員等の雇用関連個人情報

- 役職員等の雇用関連個人情報についてCPRAの適用が猶予される場合であっても、以下については適用が猶予されず、(CPRAによる改正前の)CCPAが適用されている。
 - ① 収集する個人情報の種類とその利用目的についての、収集時又は収集前の、消費者への通知義務
 - ✓ CPRAによって当該通知義務は以下の通り拡張されるため、2023年1月1日以降は、以下の内容を通知に含められるように事前に準備が必要である。
 1. 当該個人情報共有されるか。
 2. 収集されるセンシティブ個人情報の類型及び当該センシティブ個人情報の類型が収集又は使用される目的及び当該情報が販売又は共有されるか。
 3. センシティブ個人情報を含む個人情報の各類型の保持を意図する期間、又は、それが可能でない場合、当該期間を定めるために使用される基準
 - ② 通知未提供での新たな個人情報の種類の収集禁止及び目的外利用の禁止
 - CPRAによって当該禁止の対象に、通知未提供での新たなセンシティブ個人情報の種類の収集禁止及び目的外利用の禁止が追加された
 - ③ 個人情報漏洩した場合に消費者に付与される損害賠償請求権
 - CPRAによって、「パスワード又はセキュリティ上の質問との組み合わせの電子メール・アドレス及びそのアカウントへのアクセスが許可される回答が、無権限アクセス、流出、窃取又は開示の対象となった場合」についても、これが個人情報を保護するため情報の性質に適切な合理的なセキュリティ手続きとプラクティスを実施し維持する義務に事業者が違反した結果として起こった場合には、消費者に付与される損害賠償請求権に含まれることとなった。
- CPRAによって以下の事業者の義務が適用猶予されないものとして追加された。
 - ④ 開示された利用目的に合理的に必要なとされる期間を超える消費者の個人情報・センシティブ個人情報の保持の禁止(保持期間の制限)

A) CPRA一部規定の適用猶予の対象

2. 取引先の担当者の個人情報

- BtoBの文脈での取引先の担当者の個人情報についても、CPRAの一部の規定の適用が2023年1月1日まで猶予される。

適用猶予となる個人情報	適用猶予となる範囲
消費者が、会社、パートナーシップ、個人事業主、非営利又は政府機関(「会社等」)に対して従業員、所有者、役員、オフィサー又は契約受託先として活動する自然人である場合(消費者が会社等の役職員等である場合)に、事業者と消費者との間の書面又は口頭による連絡又は取引を反映した個人情報	事業者との連絡又は取引が、以下の文脈に限って生じる場合 ①消費者が所属している会社等に関して事業者がデューディリジェンスを実施する、 ②当該会社等に対する商品やサービスの提供、又は ③当該会社等からの商品やサービスの受領

- 上記適用猶予規定は、あらゆるBtoBの文脈での取引先の担当者の個人情報の収集、利用、移転に適用されるものではない。
 - ✓ BtoBの文脈で収集した取引先の担当者の個人情報を商品やサービスの提供や受領の文脈とは異なる文脈でマーケティングに用いた場合
 - ✓ 取引先の担当者の名刺を、当該担当者の所属先の会社等への商品やサービスの提供とは無関係に、当該担当者個人に対する連絡に用いた場合
 - ✓ 例えば、一般的な市況に関するものをはじめとする商品やサービスの提供と無関係な情報交換への誘い、ヘッドハンティングの声掛け、個人的な会食への誘い等
 - ✓ BtoBの取引先の担当者の個人情報についてもCPRA対応のデータマッピングが必要
 - ✓ 2023年1月1日より前に適用猶予の期限を延期又は恒久化する法改正がなされなければ、BtoBの取引先の担当者の個人情報について適用猶予されているCPRAの他の規定も全て適用されることになる。

A) CPRA一部規定の適用猶予の対象

2. 取引先の担当者の個人情報

- BtoBの文脈での取引先の担当者の個人情報についてCPRAの適用が猶予される場合であっても、以下については適用が猶予されず、(CPRAによる改正前の)CCPAが適用されている。
 - ① オプトアウトの権利に伴う義務
 - ✓ オプトアウトの権利を認める必要のある「売却」又は「共有」に該当する個人情報の移転がないかを確認する必要がある。
 - ✓ 例えば、米国子会社が、取引先の担当者の名刺に記載された個人情報を、日本企業(日本本社)へ移転している場合がこれに該当する可能性がある。
 - ② 消費者を差別的に取り扱わない権利に伴う義務
 - ③ 個人情報が漏洩した場合に消費者に付与される損害賠償請求権
 - CPRAによって、「パスワード又はセキュリティ上の質問との組み合わせの電子メール・アドレス及びそのアカウントへのアクセスが許可される回答が、無権限アクセス、流出、窃取又は開示の対象となった場合」についても、これが個人情報^{を保護するため情報の性質に適切な合理的なセキュリティ手続きとプラクティスを実施し維持する義務}に事業者が違反した結果として起こった場合には、消費者に付与される損害賠償請求権に含まれることとなった。
 - ✓ 個人情報が漏洩した場合には、取引先の担当者等から損害賠償請求がなされる可能性がある。
 - ✓ 個人情報の性質に照らして合理的なセキュリティの手續と慣行が実装されているかを確認する必要がある。

A) CPRA一部規定の適用猶予の対象

個人情報情報が漏洩した場合に消費者に付与される損害賠償請求権の行使を防ぐため、BtoB事業者も守らなければならないこと

1. 個人情報を保護するため、情報の性質に応じた合理的なセキュリティ手続きとプラクティスを実施し、
 - ✓ 業務ごとに処理する個人情報の性質からプライバシーリスクを評価し、これに相応する管理策を定め、社内ルールとして実施すること
 - ✓ 処理する個人情報の性質に見合ったセキュリティ対策が必要
 - ✓ カリフォルニア州司法長官(カマラ・ハリス次期米副大統領)が2016年に2月に出したCalifornia Data Breach Report での推奨策としてはCenter for Internet Security(CIS)のCritical Security Controls(CSC)の20の管理策を最低限の実装として推奨している。
 - ✓ CIS Control® V7.1(英語版)
 - ✓ <https://learn.cisecurity.org/cis-controls-download>
2. 1798.81.5 条(d)(1)(A)に定める個人情報又は「パスワード又はセキュリティ上の質問との組み合わせの電子メール・アドレス及びそのアカウントへのアクセスが許可される回答」が、
 - ✓ 前者(1798.81.5 条(d)(1)(A)に定める個人情報)はカリフォルニア州民法典の「顧客記録」に定められる以下の定義となり、CCPAが定義する個人情報よりも狭くなっている。
 - 個人のファーストネーム、もしくはファーストイニシャル+ラストネームと、以下の情報の組み合わせ
 - ソーシャルセキュリティ番号、運転免許証番号、カリフォルニア州IDカード番号、納税者番号、パスポート番号、軍用ID番号、特定の個人を確認する政府文書に、付与された固有の識別番号、銀行口座番号、クレジットカード・デビットカード番号とそれらのセキュリティコード、アクセスコード、パスワードの組み合わせ、医療情報、健康保険情報、特定の個人を認証するために使われる指紋等の生体情報
3. 暗号化や編集がされていない状態で、
4. 無権限アクセス、流出、窃取又は開示の影響下に置かれることを防ぐこと

B)CPRA一部規定の適用猶予の対象とならない個人情報

3. ウェブサイトへの訪問者の個人情報(クッキーを通じた取得)

- CPRAは、プロファイリングを、個人データの自動処理によって職場での成績、経済状況、健康状況、趣味嗜好、興味、扶養関係、行動、位置・移動などを予想することと定義。CPRAは、このようなプロファイリングを行う場合、情報提供及びオプトアウト権の付与を義務づける規則を今後制定する旨規定。
 - ✓ ターゲティング広告のように、閲覧履歴の分析により、閲覧者の趣味嗜好・購買傾向に関するプロファイリングを行う場合、情報提供及びオプトアウトが求められる。
- CCPAは、個人データを販売(おおむね、経済的なメリットのために委託先以外の者に開示する行為)に対するオプトアウト権を認めているが、CPRAはこれを一歩進め、個人データの共有(share)についても消費者のオプトアウト権を認める。「共有」は、事業者の利益のために、ウェブやアプリをまたがる消費者のネット上の行動履歴を共有、開示、移転することを含むこととされている。
 - ✓ CCPAでは、ターゲティング広告の効果を上げるという経済的利益のために第三者クッキーによる閲覧履歴を広告エージェンシーに共有することについて、これが「販売(sell)」に該当するかどうかについて議論があったが、CPRAでは共有がある時点でオプトアウトが求められる。

B)CPRA一部規定の適用猶予の対象とならない個人情報

3. ウェブサイトへの訪問者の個人情報(クッキーを通じた取得)

✓ 実装のポイント

- ✓ クッキーバナーを利用してウェブサイト閲覧者のプロファイリング、ターゲティング広告を行う場合における情報提供
- ✓ オプトアウト機会提供については、従来にも増して的確な対応が必要
- ✓ 情報提供及びオプトアウト機会提供のために適切なクッキーバナーツールを実装すること
- ✓ タグマネジャーの適切な設定により、ウェブサイト閲覧者の選択がクッキー設定に正確に反映されるように実装すること。
- ✓ 実装が不適切な場合、法違反のリスク

B)CPRA一部規定の適用猶予の対象とならない個人情報

3. ウェブサイトへの訪問者の個人情報(クッキーを通じた取得)

実装例

バナー第1層(概括的な情報提供)



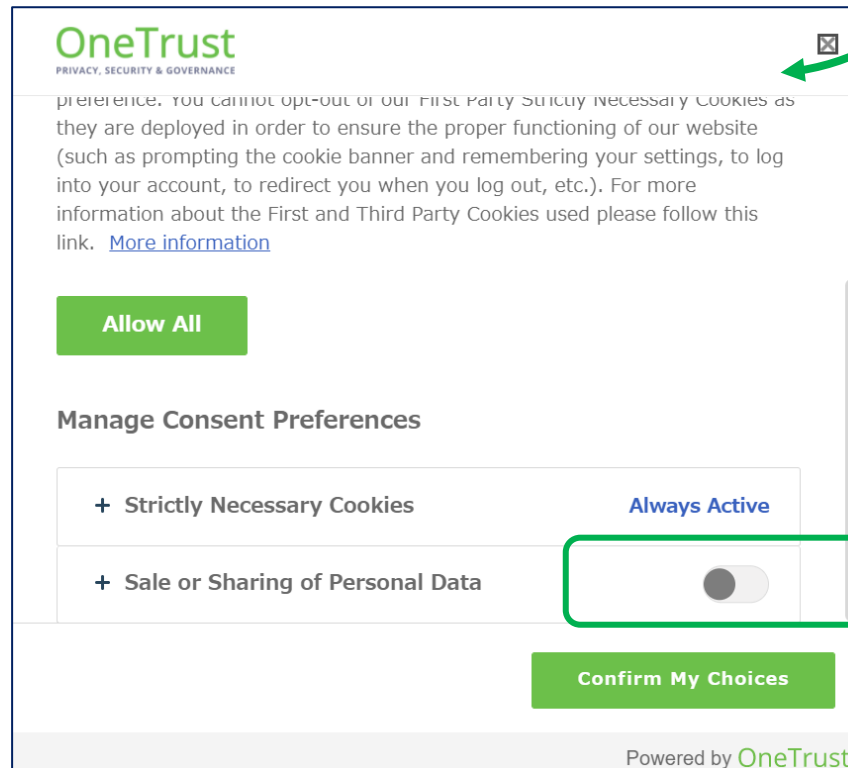
Do Not Sell or Share My Personal Information

This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners.

[Do Not Sell or Share My Personal Information](#)

Accept Cookies

“Do Not Sell or Share My Personal Information”のリンク

A screenshot of the OneTrust privacy management interface. At the top, it says 'OneTrust' and 'PRIVACY, SECURITY & GOVERNANCE'. Below this, there is a paragraph of text explaining cookie usage and a link to 'More information'. There are two green buttons: 'Allow All' and 'Manage Consent Preferences'. Under 'Manage Consent Preferences', there are two rows of controls. The first row is for 'Strictly Necessary Cookies' and is marked 'Always Active'. The second row is for 'Sale or Sharing of Personal Data' and has a toggle switch that is currently turned off. A green box highlights this toggle switch with the label 'オプトアウト' (Opt-out). At the bottom right of the interface is a green button labeled 'Confirm My Choices'. The footer says 'Powered by OneTrust'.

バナー第2層
(より詳細な情報提供と
オプトアウト機会提供)

オプトアウト

S&K
Brussels

B)CPRA一部規定の適用猶予の対象とならない個人情報

3. ウェブサイトへの訪問者の個人情報(クッキーを通じた取得)

現実的な対応策

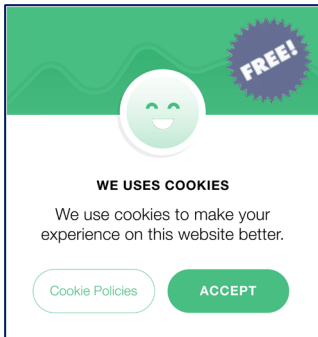
自社開発



デメリット

- ✓ システム開発以外に専門的な法律知識が必要
- ✓ ユーザーがクッキー取扱にオプトアウトした際の記録管理が難しい
- ✓ 法改正にあわせシステム更新が必要
- ✓ 開発コストが膨大
- ✓ 開発のためのリソースの確保が困難

フリーツール



デメリット

- ✓ 法律の要件にあったクッキーバナーを表示できない
- ✓ ユーザーのアクセス元の判定による法域ごとのバナー出し分けができない
- ✓ 細かいカスタマイズができない
- ✓ オプトアウトの実装が難しい、もしくは対応できない

- 多くの利用実績のあるクッキーバナーツールの利用が現実的
- クッキーツール導入サービスの利用も費用対効果が比較的高い
- 日本語対応サポートサービスもある方が楽(CPRAのみならず、日本、ブラジル、タイ、中国、インド等の法規制のクッキー対応が必要)

B)CPRA一部規定の適用猶予の対象とならない個人情報

4. それ以外の個人情報

- ✓ BtoB企業であっても、役職員の雇用関連個人情報や取引先の従業員の個人情報を、適用猶予規定が定めるのと異なる文脈で収集・使用したり、それら以外の個人情報を収集する場合には、以下に代表される一連のCPRA対応を全て実行しなければならなくなる。そのような場合に該当するか否かは、CPRAに準拠したデータマッピングの質問票によって、詳細にデータマッピングを行わなければ、正確に判断することは難しい。IV章ではBtoB企業のためのCPRAコンプライアンスへのロードマップを示す。
 - ✓ CPRAにおいて要求される開示事項をプライバシー通知に入れ込むために改訂する
 - ✓ CPRA上の新しいプライバシー権の行使を受け取り、回答し及び有効化するために、ポリシー並びに消費者に面したメカニズムをアップデートする
 - ✓ 事業目的で個人情報を販売し、共有し又は開示するサービスプロバイダ、契約受託先及び第三者を特定し、テンプレートの契約文言を作成する
 - ✓ 必要性及び比例性の原則を遵守するため、個人情報の収集、使用、保持及び共有を管理するポリシー及び手続を準備する
 - ✓ センシティブ個人情報の処理、自動化された意思決定技術(プロファイリングを含む)の使用及びクロスコンテキスト行動広告の使用に関するCPRA上の義務を分析し運用する
 - ✓ サイバーセキュリティ監査及びリスク評価枠組を発展させる
 - ✓ センシティブ個人情報用のものを含む、データ保持ポリシーを準備する
 - ✓ トレーニング文書のアップデート及びトレーニングセッションの実行
 - ✓ 今後公表されるCPRA規則の解釈

IV. BtoB企業のためのCPRAコンプライアンスへのロードマップ

BtoB企業のためのCPRAコンプライアンスへのロードマップ

1. CPRAを踏まえたデータマッピングの実行
 - (1) 「個人情報」の定義の新しい例外が適用されるかを特定する
 - (2) 個人情報の転送が「共有」と見なされるかどうかを評価する
 - (3) 収集している「センシティブ個人情報」を特定する
 - (4) 事業者のプライバシー通知における追加の開示の要求に対応した情報を収集
 - (5) 事業者が行う個人情報の転送を洗い出し評価して、各受領者との間で締結すべき契約の内容を確定する
2. データマッピングの結果を踏まえたコンプライアンス文書の作成
 - (1) プライバシー通知及びオプトアウトリンクの更新
 - (2) 第三者、サービスプロバイダ、及び契約受託先との契約を確認及び更新する
 - (3) 個人の権利手続きと対応資料を更新する
 - (4) 個人情報の収集と保持に関連する社内慣行を確認する
 - (5) 個人情報処理活動における同意の役割と方法を評価する
3. 今後公表されるCPRA規則の内容の把握と解釈

1. CPRAを踏まえたデータマッピングの実行

(1)「個人情報」の定義の新しい例外が適用されるかを特定する

- ✓ データマッピングを行った結果備えることになる個人情報のインベントリー（データマップ）を見直し、「個人情報」としてCPRA上規制される範囲を再評価する（下の緑字部分がCPRAによって追加となる例外）。
 - 公に利用可能な情報又は適法に入手した公の関心事である正確な情報は「個人情報」に含まれない
 - 「公に利用可能」とは、
 - 連邦、州若しくは地域の政府の記録から適法に利用可能な情報、又は
 - 事業者が、消費者若しくは広く分布されているメディアによって適法に一般公衆に利用可能にされていると信じるための合理的な根拠がある情報、又は
 - 消費者が特定の聴衆に情報を制限していない場合には、消費者が情報を開示した者によって利用可能にされた情報
- ✓ 但し、何をもって上記例外に該当するかについては、精査が必要であり、データマッピングの質問票の回答においては、当該例外に該当すると考えられるものもカバーし、社内の担当者又は外部の専門家によって例外規定の適用の有無について判断してもらうことが望ましい。

1. CPRAを踏まえたデータマッピングの実行

(2) 個人情報の転送が「共有」に該当するかを評価する

- ✓ データマッピングを行った結果備えることになる個人情報のインベントリー（データマップ）を見直し、事業者は個人情報の開示が「共有」に該当するかどうかを評価し、該当する場合、適切なオプトアウト措置を実施する必要がある。
 - CPRAは情報の「共有 (share)」という新しい概念を導入。これは対価が交換されるかどうかに関係なく、クロスコンテキスト行動広告のために第三者に個人情報を開示することとして定義される。事業者が共有を行う場合、「Do Not Share My Personal Information」というタイトルのリンクを投稿し、消費者に共有をオプトアウトする機会を提供する必要がある。
- ✓ すでにCCPAに準拠している事業者の場合、これは既存の「販売 (sale)」のオプトアウト要件に類似するもの。現在のCCPAに基づく「販売」は、個人情報が「またはその他の貴重な対価」と引き換えに第三者に転送または利用可能になった場合に発生する。「その他の価値ある対価」のためにクロスコンテキスト行動広告が行われ、したがって「販売」オプトアウトの対象となるかどうかについて議論があった。CPRAの下での「共有」の新しい定義は、このタイプの開示は消費者のオプトアウトの対象となることを明確にしている。
- ✓ 共有は「サービスプロバイダ」や「契約受託先」への転送を含まない。多くのオンライン広告主、Cookieプロバイダー及びその他のアドテックの利害関係者がサービスプロバイダとして機能するため注目に値する。当該サービスプロバイダが個人情報の使用に関する特定の制限に同意する場合、当該サービスプロバイダへの転送は拡張されたオプトアウト権の対象にはならない。

1. CPRAを踏まえたデータマッピングの実行

(3) 収集している「センシティブ個人情報」を特定する

- ✓ 事業者が収集するすべてのセンシティブ個人情報を特定する(ステップ1)。当該センシティブ個人情報がどのように使用され、それらの使用が新しいオプトアウト権の対象となるかどうかを評価する(ステップ2)。対象となる場合、事業者は「Limit the Use of My Sensitive Personal Information」のリンクを貼り、制限要求を実行するための内部手続の導入を計画する必要がある。別の選択肢は、複雑な制限プロセスの導入を回避するためにセンシティブ個人情報の使用を取りやめる。
- CPRAは以下を明らかにする情報を**センシティブ個人情報**として定義。
 - 消費者の社会保障、運転免許証、州の身分証明書、パスポート番号
 - 必要なセキュリティコード、アクセスコード、パスワード、又はアカウントへのアクセスを許可する資格情報との組み合わせによる消費者のアカウントログイン、金融口座、デビットカード、又はクレジットカード番号
 - 消費者の正確な位置
 - 消費者の人種的又は民族的出自、宗教的又は哲学的信条、又は組合への加入
 - 消費者の郵便物、電子メール、テキストメッセージの内容(但し、事業者が通信の対象となる受信者でない場合)
 - 消費者の遺伝子データ
 - 消費者を一意的に特定するために処理される生体情報
 - 消費者の健康に関し収集・分析された個人情報、又は
 - 消費者の性生活や性的指向に関し収集・分析された個人情報
- CPRAは、事業者のプライバシーポリシーでのセンシティブ個人情報の使用について及びアクセス権の要求に応じて一定の開示を義務付ける。CPRAは、事業者がセンシティブ個人情報を使用して消費者の特性を推測する範囲で、事業者がオンラインサービスに「Limit the Use of My Sensitive Personal Information」のリンクを公開することを義務付ける。消費者がこの権利を行使する場合、事業者はセンシティブ個人情報の使用を平均的な消費者が合理的に期待するサービスの実行または商品の提供に必要なもの及び法令及び今後の規制で指定される追加の事業目的に制限する必要がある(例、製品の改善とセキュリティの目的)。

1. CPRAを踏まえたデータマッピングの実行

(4) 事業者のプライバシー通知における追加の開示の要求に対応した情報を収集

- ✓ データマッピングを行った結果備えることになる個人情報のインベントリー(データマップ)を見直し、以下の事業者のプライバシー通知における追加の開示の要求に対応した情報を収集し、プライバシー通知を準備できるようにする。
 - 事業者のプライバシー通知における追加の開示の要求
 - クロスコンテキスト行動広告のため事業者が共有した個人情報のカテゴリ
 - ▶ クロスコンテキスト行動広告: 明確にブランド化された事業者のウェブサイト、アプリケーション又はそれ以外の消費者が意図的にやりとりしている事業者のサービスから得られた消費者の個人情報に基づいて、消費者を対象として広告活動すること
 - センシティブ個人情報の事業者による処理に関する情報
 - ▶ 収集されたセンシティブ個人情報のカテゴリ
 - ▶ センシティブ個人情報の使用される目的、及び
 - ▶ センシティブ個人情報が販売されるか又はクロスコンテキスト行動広告のために共有されるかどうか
 - 事業者が個人情報の各カテゴリを保持することを意図する時間の長さ
 - ▶ 当該開示が不可能である場合、当該期間を決定するために使用される基準

1. CPRAを踏まえたデータマッピングの実行

(5) 事業者が行う個人情報の転送を洗い出し評価して、各受領者との間で締結すべき契約の内容を確定する

- ✓ 事業者が行う個人情報の転送を洗い出し評価して、各受領者がサービスプロバイダ、契約受託先又は第三者のいずれに該当するかを判断し、それによって各受領者との間で締結すべき契約の内容を確定させる。各転送の事業目的も下の表を利用する等して洗い出しを行う。
 - CPRAは**事業目的(CPRAによって改訂)**での個人情報のすべての販売、共有、及び開示を契約に従って行うことを義務付ける。サービスプロバイダ及び契約受託先と呼ばれる新しい種類の受領者への開示も含まれる。契約受託先はサービスプロバイダに似ているが、特定の状況では個人情報を独自の事業目的で使用する場合があります、その後の使用及び開示には厳しい制限がある。

事業目的のカテゴリ	事業目的の説明
監査及び広告インプレッション	消費者との現在の交流及び同時の取引に関する監査、ユニーク・ビジターに対するインプレッションの算定、広告インプレッションのポジション及び質の確認、ならびに仕様及びその他の基準の遵守の監査。
セキュリティ事象の検出/保護	セキュリティ事故の検出、悪意のある、偽装の、不正な、または違法な活動からの保護、及び当該活動に関する請求。
デバッグ	意図された既存の機能を害するエラーを特定し修正するためのデバッグ。
短期/一時的な使用	その他の第三者に開示されておらず、または消費者プロファイルを構築するために使用されていない個人情報の、短期の一時的な使用(事業者と消費者の現在の交流の一環として表示されるパーソナライズされていない広告を含むが、これに限られない。)。但し、消費者の個人情報は、事業者との現在の交流の外での消費者の体験を変えるために使用されないことを要する。
事業者/サービス提供者のためのサービス	事業者またはサービス提供者のためのサービスの履行(事業者またはサービス提供者のための、アカウントのメンテナンスまたはサービス、カスタマー・サービスの提供、注文及び取引の処理または実行、消費者情報の確認、支払の処理、資金提供、分析サービスの提供、ストレージの提供または類似のサービスの提供を含むが、これらに限られない)。
広告/マーケティング内部調査	広告及びマーケティング・サービスの提供(顧客に対するクロスコンテキスト行動広告を除く)。 技術開発及び実証のための内部調査の実施。
サービス/商品のメンテナンス及び改良	事業者が所有し、製造し、事業者のために製造され、または事業者が管理するサービスまたはデバイスの質もしくは安全性を確認もしくは維持し、またはこれを改善、アップグレード、もしくは改良するための活動の実施。

2. データマッピングの結果を踏まえたコンプライアンス文書の作成

(1) プライバシー通知とオプトアウトのリンクを更新する

- ✓ 既存のCCPA準拠のプライバシー通知に、CPRAによって導入された新しい消費者の権利や保持慣行に関する義務的な開示など、CPRA上の新しい通知義務に準拠するための更新を行う。
 - 事業者のプライバシー通知における追加の開示の要求
 - クロスコンテキスト行動広告のため事業者が共有した個人情報のカテゴリ
 - センシティブ個人情報の事業者による処理に関する情報
 - ▶ 収集されたセンシティブ個人情報のカテゴリ
 - ▶ センシティブ個人情報の使用される目的、及び
 - ▶ センシティブ個人情報が販売されるか又はクロスコンテキスト行動広告のために共有されるかどうか
 - 事業者が個人情報の各カテゴリを保持することを意図する時間の長さ
 - ▶ 当該開示が不可能である場合、当該期間を決定するために使用される基準
 - 新しい消費者の権利の説明
 - ▶ 訂正権 (Right of correction)
 - ▶ 「共有」のオプトアウト権 (Right to opt-out of “sharing”)
 - ▶ クロスコンテキスト行動広告目的での個人情報の「共有」の定義の追加
 - ▶ 事業者が消費者の年齢を実際に知っている場合、16歳未満の消費者の個人情報の「共有」に対する積極的な同意の要求
 - ▶ センシティブ個人情報の使用及び開示を限定する権利

2. データマッピングの結果を踏まえたコンプライアンス文書の作成

(1) プライバシー通知とオプトアウトのリンクを更新する

- ✓ 個人情報を「共有」したり、センシティブ個人情報を収集して特定の方法で使用する事業者は、それらの慣行についての説明を含める。当該事業者は、ウェブサイトやモバイルアプリケーションに「共有」のオプトアウトリンク及びセンシティブ個人情報の使用の「制限」リンクを追加し、「Do Not Sell My Personal Information」のリンクをクリックした場合の効果を更新する。

2. データマッピングの結果を踏まえたコンプライアンス文書の作成

(2) サービスプロバイダ、契約受託先及び第三者との契約を更新

①共通に必要なとなる条項

- ✓ 契約の更新に備えて必要な契約資料(サービスプロバイダ、契約受託先又は第三者との契約又は Addendum、チェックリスト等)を作成し、必要な契約の更新と交渉のプロセスを開始する。
 - CPRAは、サービスプロバイダ、契約受託先及び第三者(合わせて「受領者」と)との契約が以下の通りとすることを要求する。
 1. 個人情報、限定されかつ特定された目的のためにのみ、事業者によって販売され又は開示されることを特定する。
 2. CPRAにおいて適用される義務を遵守し、CPRAによって要求されるのと同レベルのプライバシー保護を提供することを、受領者に義務付けること
 3. 受領者が移転された個人情報をCPRAの下での事業者の義務と一致した形で使用することを確保するのを助けるため、合理的かつ適切なステップを経る権利を事業者に与える
 4. 受領者がCPRAの下での義務を遵守できないと判断した場合に事業者に通知することを当該受領者に要求する
 5. 通知があり次第、個人情報の未承諾の使用を停止し修正するため、事業者に合理的かつ適切なステップを経る権利
 - 「第三者(third party)」:(1)消費者が意図的にやりとりし、かつ、消費者と事業者の進行中のやりとりの一部として消費者から個人情報を収集する事業者、(2)事業者へのサービスプロバイダ、(3)契約受託先のいずれでもない者
 - 「者」:個人、事業体、事業者、パートナーシップ、ジョイント・ベンチャー、シンジケート、事業信託、会社、法人、有限責任会社、団体、委員会、またその他の共同行為をする者の組織又はグループ

2. データマッピングの結果を踏まえたコンプライアンス文書の作成

(2) サービスプロバイダ、契約受託先及び第三者との契約を更新

② 契約受託先との関係で必要な契約条項

- ✓ データマッピングを通じて洗い出した契約受託先との関係で、契約の更新に備えて必要な契約資料(契約受託先との契約又はAddendum)を作成し、必要な契約の更新と交渉のプロセスを開始する。
- ✓ 「**契約受託先(contractor)**」: 事業者との書面による契約に基づき、事業者が事業目的のために消費者の個人情報を利用できるようにする者。当該契約は以下の通りに定める。
 - (A) 契約受託先が以下を行うことを禁止する。
 - 個人情報を販売又は共有すること。
 - 契約で定められた事業目的以外の目的のために個人情報を保持、使用、又は開示すること。それには、契約で定められた、又は本巻で許可されている事業目的以外の商業目的のために個人情報を保持、使用、又は開示することを含む。
 - 契約受託先と事業者との直接的な取引関係以外で、情報を保持、使用、又は開示すること。
 - 契約受託先が事業者との書面による契約に基づき受領した個人情報と、契約受託先が他の者若しくは複数人から、又は事業者に代わって受け取る個人情報を組み合わせたり、自らの消費者とのやりとりから収集したりすること。ただし、契約受託先は...及びカリフォルニア州プライバシー保護当局によって採択された規則に規定されている場合を除き、...に従って採択された規則に定義されている事業目的を実行するために個人情報を組み合わせることができる。
 - (B) 契約受託先が(A)の制限事項を理解し、それを遵守するという契約受託先が作成した証明書を含む。
 - (C) 契約受託先との合意に基づき、事業者が、少なくとも12か月に1回、手動による継続的見直しや自動スキャン、定期的な評価、監査、その他の技術的及び運用的テストを含むがこれらに限らない対策を通じて、契約受託先の契約への準拠を監視することを許可する。

2. データマッピングの結果を踏まえたコンプライアンス文書の作成

(2) サービスプロバイダ、契約受託先及び第三者との契約を更新

③ サービスプロバイダとの関係で必要な契約条項

- ✓ データマッピングを通じて洗い出したサービスプロバイダとの関係で、契約の更新に備えて必要な契約資料(サービスプロバイダとの契約又はAddendum)を作成し必要な契約の更新と交渉のプロセスを開始する。
- ✓ 「サービスプロバイダ(service provider)」とは、事業者にとって個人情報を処理し、かつ、事業目的のために書面の契約により、事業者から又は事業者にとって受領する消費者の個人情報を処理する者を意味し、事業者との契約で以下の通り定める。
 - (1) 事業者との契約により、人が、当該契約で事業目的以外の目的のために、個人情報を保持し、使用し又は開示すること(事業者との契約又はその他本巻で認められたものによって事業目的以外の商業目的のために(A)個人情報を販売し又は共有し、(B)個人情報を保持し、使用し又は開示し、(C)サービスプロバイダ及び事業者との直接の業務関係外の情報を保持し、使用し、又は開示し、また(D)事業者から又は事業者にとってサービスプロバイダが受領する個人情報、別の者から又は別の者に代わって受領する個人情報を組み合わせ、又は消費者とのやりとりから収集することを禁止する。
 - この契約は、サービスプロバイダとの合意に基づき、事業者が、少なくとも12か月に1回、手動による継続的見直しや自動スキャン、定期的な評価、監査、その他の技術的及び運用的テストを含むがこれらに限らない対策を通じて、サービスプロバイダの契約への準拠を監視することを許可することができる。
 - (2) サービスプロバイダが事業者にとって事業目的のため個人情報を処理することにつき、サービスプロバイダの支援に他の者を従事させる場合、又はサービスプロバイダによって従事させられる他の者が当該目的のため個人情報処理の支援に別の者を従事させる場合、サービス提供はその旨を事業者に通知するものとし、他の者に従事させることについては、その者に(1)に定めるすべての要件を遵守させる書面の契約に従うものとする。
- ある事業者が、サービスプロバイダであるマーケティング業者を使用して、当該サービスプロバイダが保有する個人情報の名簿に基づき、当該名簿に連絡先が掲載されている消費者に対して、ダイレクトメールを送信する場合、事業者はCPRA上の責任を負う。例えば、消費者から当該事業者に対して削除権の行使があった場合、当該事業者は連絡先の個人情報を保有していないが、当該サービスプロバイダに削除権の行使があったことを通知する義務があり、当該サービスプロバイダは削除の義務がある。

2. データマッピングの結果を踏まえたコンプライアンス文書の作成

(3) 個人の権利手続きと対応資料を更新する

- ✓ 事業者は新しいCPRAの権利行使へ対応するために必要な技術的又は運用上の変更を実装し、個々の権利対応ポリシーと手順を更新し、それに応じて対応資料を更新する。
 - CPRAは、訂正の権利、センシティブ個人情報の使用を制限する権利、共有をオプトアウトする権利など、運用上の変更を必要とする可能性のあるいくつかの新しい消費者の権利を導入する。
 - 既存のアクセス権に変更がある。消費者に関して収集される個人情報のカテゴリに「知る要求」には、センシティブ個人情報の開示と共有を含める必要がある。
 - 特定の個人情報の「知る要求」は、情報が別の個人に関連する場合や、セキュリティまたはデータの整合性の目的で情報が生成される場合など、新しい例外の対象となる。
 - CPRAはサービスプロバイダ、契約受託先及び第三者に削除要求を通知するなど、特定の権利要求を連絡する義務を追加する。

2. データマッピングの結果を踏まえたコンプライアンス文書の作成

(4) 個人情報の収集と保持に関連する社内慣行を確認する

- ✓ CPRAはGDPRスタイルのデータ最小化とデータ保持要件を導入する。事業者は件をデータ最小化及びデータ保持の手順を既存のプライバシーポリシーを改訂して組み込むか、必要に応じて、これらの要件に対応するための新しいポリシーと手順を作成する。
- ✓ これまでGDPRへの遵守を行っていない事業者の場合、情報の収集、保存、匿名化または仮名化及び削除の慣行に関して、運用上の大幅な変更が必要になる場合がある。
 - CPRAの下では、個人情報の収集、使用、保持、及び共有は、収集の目的を達成するために合理的に必要であり、比例している必要がある。したがって、事業者は必要以上の個人情報を収集してはならず、開示された目的のために合理的に必要な期間を超えて個人情報を保持してはならない。

2. データマッピングの結果を踏まえたコンプライアンス文書の作成

(5) 個人情報処理活動における同意の役割と方法を評価する

- ✓ CPRAに関係するさまざまな消費者との接触について同意に依存することを意図している場合、事業者は同意へのアプローチとユーザーインターフェイスをこれらの要件に準拠させる必要がある。例えば、オンラインの消費者オプトアウト設定の上書きなどである。クッキーとの関係での同意の要件への遵守は、実績のあるクッキーバナーツールを導入することで確保することが一般的である。
 - CPRAは、GDPRの定義に沿った「同意」の定義を追加する。
 - ▶ 「同意」は「自由に与えられ、特定の、情報に基づいた、不明瞭でない消費者の希望の明示」として定義される。
 - ▶ CPRAは「個人情報の処理の説明と他の無関係な情報を含む一般的又は広範な利用規約若しくは同様の文書の受諾は同意を構成しない」ことを明確にしている。
 - ▶ 事業者はいわゆる「ダークパターン」、すなわち、選択を損なうように設計されたユーザーインターフェイス(CPRA規則によってさらに定義される)を使用したり、特定のオブジェクトにカーソルを合わせたり、ミュートしたり、一時停止したり、内容の一部を閉じたりすることによって同意を得ることができない。

3. 今後公表されるCPRA規則の内容の把握と解釈

- ✓ 今後当局によってドラフトが公表されるCPRA規則の内容を注視する。
 - CCPA規則(CCPA Regulation)と同様にCPRA規則を策定するための新しいルール作成プロセスが開始する。これは2022年7月1日までに最終決定する必要がある。CCPA規則は法律の特定の側面を明確にする可能性があるが、ほぼ確実に追加のコンプライアンス要件を設定することになる。CPRAは特に以下の各論点に関する規制の策定を要求している。
 - 訂正の権利、共有をオプトアウトする権利、センシティブ個人情報の使用を制限する権利を含む、新しい個人の権利。
 - 販売または共有をオプトアウトする消費者の意図を示すために使用できるグローバルオプトアウト/プリファレンスシグナルの要件と技術仕様。
 - 未定義の用語である「重大なリスク」を伴う処理の監査及びリスク評価の要件
 - 「プロファイリング」を含む、自動化された意思決定テクノロジーの使用に関連する新しいオプトアウト権。

V. まとめ

まとめ1

- CPRAは、BtoB企業にとっても、米国において事業を行う上で達すべきプライバシー水準であり、早期に遵守に向けた取り組みを進めるべきである。米国子会社であるBtoB企業は、CCPA/CPRAへの遵守のための予算確保における社内説明において苦勞するケースも散見されるため、実際のCPRA遵守プロジェクトの開始に先立って早めに動き出すことが望ましいと考えられる。
- 民主党が大統領及び連邦議会上下院のコントロールを次の2022年の中間選挙まで基本的に確保したことから米国連邦プライバシー法が年内又は遅くとも来年2022年秋前に採択される可能性は非常に高い。
 - ...Democrats are committed to policies that will protect individuals' privacy and data rights while continuing to support and enable innovation and improve accessibility in the technology sector. We will update the Consumer Privacy Bill of Rights proposed by the Obama-Biden Administration, including adding strong national standards to protect consumers, employees, patients, and students from data breaches, and work with Congress to pass it into law... (page 25 of "2020 Democratic Party Platform": <https://www.demconvention.com/wp-content/uploads/2020/08/2020-07-31-Democratic-Party-Platform-For-Distribution.pdf>)
 - カマラ・ハリス次期米副大統領はカリフォルニア州司法長官時代に、企業にウェブユーザーから個人データを収集しているかどうか及びどのように収集しているかを公に特定することを義務付ける米国における最初の法律の一つであるカリフォルニア州オンラインプライバシー保護法を可決させ、またプライバシー執行及び保護ユニットを司法長官オフィス内に創設した。
- 民主党における主力の連邦データプライバシー法案は、COPRA (the Consumer Online Privacy Rights Act)である。COPRAは違反の場合の個人によるクラスアクションの提起及び懲罰的損害賠償を認め、また連邦法と州法との関係、すなわち先占の論点においても、個人に対してより高いレベルの保護を提供する場合にのみ連邦法が州法に優先するものとしている。CPRAよりも広範かつ厳しいクラスアクションの制度が連邦法によって創設される可能性が高く、CPRA中の厳しい規定は連邦法の効力発生後も有効とされる可能性がある。

まとめ2

- また、米国内の日本企業は、欧州においては既に非個人データの収集、処理、移転に関する規制の立法作業(EUのデータガバナンス法案)も開始されていることに注意されたい。
 - ジェトロ・ブリュッセル発2020年12月1日ビジネス短信「欧州委、官民のデータ共有促進を目指すデータガバナンス法案発表」
<https://www.jetro.go.jp/biznews/2020/12/e1aa363f69648a73.html>
 - 欧州委員会は11月25日、「欧州データ戦略」(2020年2月25日記事参照)の一環として、データガバナンス規則案外部サイトへ、新しいウィンドウで開きますを発表した。この法案は、個人や産業が生み出す膨大なデータを技術革新や経済成長につなげるために、データの取り扱いの安全性を確保するなど、データ共有への信頼性を高めながら、EU域内で官民を超えたデータ共有の促進を目指すものだ。さらに、EU型のデータ分野の「主権ある」単一市場を確立する狙いもある。
- CCPAやCPRAへの遵守に今から真剣に取り組まないことは、非個人データを含むデータの保護のみならずデータ利活用においても後れを取ることでありかねないことが懸念される。
- 次スライドに御参考としてお示しするように、包括的な個人データ保護法の立法が全世界で同時並行的に進んでおり、特に中国ではGDPRを輸入する形で提案された個人情報保護法の採択に向けた立法作業が急ピッチで進められており、2021年3月に採択予定である。中国との鋭い対立が不可避のバイデン次期政権としても、データ規制の分野で中国に後れを取ることは許容できず、国際的なデータ規制の枠組みにおける規制競争の文脈からも、連邦データプライバシー法を早期に採択し世界をリードすることを狙うであろう。CPRAが連邦データプライバシー法に及ぼす影響は大きく、特にCPRA規則は細部の実務的取扱の部分で、連邦データプライバシー法における細則にも影響を持つことになると考えられる。

包括的なデータ保護法制の世界的な拡がり

国	包括的データ保護法制/法案の名称	立法の状況	施行
日本	個人情報保護法	採択 (2003.05.30)	2005.04.01
EU	一般データ保護規則(“GDPR”)	採択 (2016.04.27)	2018.05.25
米国(連邦レベル)	セーフデータ法(データアクセス、透明性、説明責任を確保するための米国の枠組みの設定法)法案	共和党上院によって提案	該当なし
米国 (連邦レベル)	COPRA(消費者オンラインプライバシー法)法案	民主党上院によって提案	該当なし
米国 (加州)	カリフォルニア州消費者プライバシー法 (“CCPA”)	採択 (2018.06.28)	2020.01.01
米国 (加州)	カリフォルニアプライバシー権利法 (“CPRA”)	採択 (2020.11.03)	2023.01.01
ロシア	個人データに関する2006年7月27日付連邦法第152-FZ号	採択 (2006.07.27)	2006.07.27
シンガポール	2012年個人データ保護法	採択 (2012.11.20)	2013.01.02
フィリピン	2012年データプライバシー法	採択 (2012.08.15)	2012.09.08
ベトナム	個人データ保護に関する政令案	公共安全省によって提案	該当なし
マレーシア	2010年個人データ保護法	採択 (2010.06.02)	2013.11.15
インドネシア	私的個人データ保護に関する法案	下院において審議中	該当なし
タイ	個人データ保護法	採択 (2019.05.28)	2021.05.31
インド	個人データ保護法案	議会において審議中	該当なし
台湾	2015年個人情報保護法	採択 (2010.05)	2012.10
中華人民共和国	中華人民共和国個人情報保護法(草案)	草案がパブコメに付された (2020.10.21)	該当なし
香港	個人データ・プライバシー条例	採択 (1996)	2016
韓国	個人情報保護法	採択 (2011.03.29)	2011.09.30
ブラジル	ブラジル一般情報保護法 (“LGPD”)	採択 (2018.08.14)	2020.09.18
メキシコ	私的当事者によって保有される個人データ保護に関する連邦法	採択 (2010)	2010.07.06

付録1(CPRAデータマッピング質問票一人 材採用の例での回答)

CPRAデータマッピング質問票

人材採用の例

A. 部署及び記録

Q1. 部門、事業部または下位グループ

各行で特定される事業記録または処理活動を主に担当するグループを特定して下さい。

(回答)

- [グループ]
- 例: 人事部門

Q2. 事業記録または処理活動

CPRAの対象となる個人情報を含む事業記録または処理活動を特定して下さい。

(回答)

- [事業記録または処理活動]例: 電子メールマーケティング、人事採用、顧客記録、人事記録、マーケティングリスト
- 例: 人事採用

CPRAデータマッピング質問票

人材採用の例

A. 部署及び記録

Q3. 記録または処理活動の状況

記述された事業記録または処理活動がまだ元の形式で使用されているか(「アクティブ」)、まったく使用されなくなったか([日付]時点で使用されていない)、または元の形式から特定の変更を加えて使用されている(すなわち、[日付]から[変更内容]に変更された)を特定して下さい。

(回答)

- [活動ステータス]

- 例: **アクティブ**

Q4. 個人の数の記録

個人情報取得された消費者の数の推定を記載して下さい(過去12か月の合計数の推定を括弧内に記載して下さい)。個人情報取得したカリフォルニア州の住民数について、第二の推定を記載して下さい(過去12ヶ月間の合計数を括弧内に記載してください)。

(回答)

- [合計 # (過去12か月)]

- [カリフォルニア州 # (過去12か月)]

- 例: 全米合計: 180(90)

- [注: 全米でデータ保護コンプライアンス対応を行うことを想定]

- カリフォルニア州: 35(18)

CPRAデータマッピング質問票

人材採用の例

B. 消費者のカテゴリ: 誰

Q5. 消費者のカテゴリ

誰に関する個人情報であるかを特定して下さい。

(回答)

- [消費者のカテゴリ]カテゴリの例: 顧客、顧客候補、現在の従業員、ウェブサイト訪問者
 - 例: 採用候補者

Q6. 子供の個人情報

子供の情報が取得されるかどうかを特定して下さい(“はい”または“いいえ”)。
→ もし取得される場合、子供の年齢範囲を特定して下さい。

(回答)

- “[はい/いいえ][年齢範囲]”
 - 例: いいえ

CPRAデータマッピング質問票

人材採用の例

C. 個人情報の収集: 何を、なぜ、どこで

Q7. 取得された個人情報のカテゴリ

事業記録または処理活動に関して過去12ヶ月間に取得された個人情報のカテゴリ以外の数字を消去して下さい。

*一部の個人情報は複数のカテゴリに該当する場合があります。該当するカテゴリは全て残して下さい。

(回答)

- 1. 識別子
- 2. その他の識別子
- 3. 保護された分類上の特性
- 4. 商業情報
- 5. 生体情報
- 6. インターネット・ネットワーク情報
- 7. 位置データ
- 8. 知覚情報
- 9. 職業/雇用に関する情報
- 10. 教育情報
- 11. プロフィールに関するデータおよび推測
- 12 従業員情報
- 13. センシティブな個人情報 (CPRA)
- 14. カリフォルニア消費者記録カテゴリ
- 15. 子供の情報

CPRAデータマッピング質問票

人材採用の例

C. 個人情報の収集: 何を、なぜ、どこで

Q7. 取得された個人情報のカテゴリ

事業記録または処理活動に関して過去12ヶ月間に取得された個人情報のカテゴリ以外の数字を消去して下さい。

*一部の個人情報は複数のカテゴリに該当する場合があります。該当するカテゴリは全て残して下さい。

(回答)

例:

- 1. 識別子
- 2. その他の識別子
- 9. 職業/雇用に関する情報
- 10. 教育情報
- 11. プロフィールに関するデータおよび推測

CPRAデータマッピング質問票

人材採用の例

C. 個人情報の収集: 何を、なぜ、どこで

Q8. 取得された個人情報の具体的内容

チェックした個人情報のカテゴリごとに、→ 過去12ヶ月間に取得された個人情報の具体的内容を特定して下さい。

(回答)

例:

- 1→氏名、電話番号、メールアドレス、住所、IPアドレス、申請者ポータルクッキー
- 2→氏名、住所、電話、職歴
- 9→プロフェッショナル/雇用:以前の仕事と期間、雇用主のリファレンス
- 10→教育:学校、成績、学業区分
- 11→推論:知性

CPRAデータマッピング質問票

人材採用の例

C. 個人情報の収集: 何を、なぜ、どこで

Q9. 個人情報の取得・使用の目的

チェックした個人情報の各カテゴリについて、そのカテゴリ内の個人情報を収集/処理する目的を特定・説明し、目的ごとに→「事業目的」または「商業目的」かの特定を括弧内をお願いします。

注:「プロファイリング」(自動的処理の形態)を実施する場合は、個人情報の「プロファイル(profiled)」のカテゴリを特定してください。*個人情報の一部のカテゴリは、取得/処理に関する複数の異なる目的を伴う場合があります。関係するすべての目的と、その事業および/または商業の性質を特定してください。

(回答)例:

1、2→

- 特定の個人を内部で追跡し、重複するアプリケーションの提出を防止するため→(事業)
- 役職に関して特定の個人とコミュニケーションを取る→(事業)
- 名前ではなく識別子を使用して個人情報を保護する→(事業)

9、10、11 →

- 内部で特定の個人を追跡する (個人の記録)→(事業)
- 社内の役職に適した候補者を特定し、配置する→(事業)

CPRAデータマッピング質問票

人材採用の例

C. 個人情報の収集: 何を、なぜ、どこで

Q10. 個人情報の情報源

消費者(該当する場合)を含む、個人情報が取得された情報源のカテゴリ(消費者から直接、自動的に、又は第三者)を特定して下さい

→各カテゴリの情報源に関して、括弧内に特定の情報源及び各情報源から収集した個人情報のカテゴリ(数字で)を特定して下さい。

(回答)

例:

- 消費者から直接取得→(オンライン求人アプリケーション)→1、2、9、10、11
- 自動的なデータ取得→(会社ウェブサイト上のオンラインアプリケーションポータルは、応募者のIPアドレスを取得し、デバイス上にクッキーを配置する)→1、2
- 第三者から取得→(LinkedInが提供する候補者)→1、2、9、10、11

CPRAデータマッピング質問票

人材採用の例

D. 受領団体

Q11. 受領団体

過去12ヶ月間に個人情報を開示した、全ての受領団体/会社を列挙してください。→当該受領者が(1)関連している*、(2)外部/非関連、または(3)不明確、のいずれかを括弧内で特定してください。

*(1)各関連団体について→関連性または関係性、および共通のブランドを共有しているか否かを、括弧内に記載してください。

注:この目的で、関連団体は、子会社、親団体および兄弟団体、ならびに共通の所有またはブランドを共有する団体(商標または名称の共有等)を含みます。

(回答)例:

- Google Drive→(外部)
- Microsoft Exchange→(外部)
- HostGator→(外部)
- NY HQ → (関連) → 親会社(100%支配)であるが、異なる名称/ブランド
- テキサスに拠点を置く関連会社 → (関連) → 異なる名称/ブランドを有する兄弟会社

CPRAデータマッピング質問票

人材採用の例

D. 受領団体

Q12. 外部受領者に移転された個人情報のカテゴリ

Q11において列挙された各受領者について(共通のブランドを共有する親団体または子団体を除く。)—受領者を列挙してください。→過去12ヶ月間に当該受領者に開示された個人情報のカテゴリを、括弧内で番号により特定してください。→開示された各カテゴリについて、当該開示の目的を記載してください。

(回答)例:

- Google Drive→(1、2、9、1、11) → クラウド・インフラストラクチャーおよびストレージ・データベースの目的
- Microsoft Exchange→(2、9、10、11) → 従業員のインボックスならびに内部および外部のEメール通信
- HostGator→(1、2、9、10、11) → HRのNetworked H Driveのための外部サービス
- NY HQ→(2、9、10、11) → HQレベルでの採用および面接のための候補者情報の提供
- 日本HQ→(2、9、10、11)→日本HQレベルでの候補者採用の承認
- テキサスに拠点を置く関連会社 → (2、9、10、11) → 採用および面接のための候補者情報の提供

CPRAデータマッピング質問票

人材採用の例

E. 過去12ヶ月間の個人情報の販売、共有および事業目的開示

Q13. 販売

Q12において列挙された、金銭またはその他の価値ある対価のための「販売」と記載された全ての個人情報の開示について—受領団体を特定してください。

→括弧内で、「販売」された個人情報のカテゴリを番号で列挙してください。→当該各カテゴリについて、販売の商業目的を説明してください。

(回答)

例:

- テキサスに拠点を置く関連会社 → (2、9、10、11) → 候補者情報の提供、および採用が成功した場合、報酬の受領

CPRAデータマッピング質問票

人材採用の例

E. 過去12ヶ月間の個人情報の販売、共有および事業目的開示

Q14. 共有

Q12において列挙された、クロスコンテキスト行動広告のための「共有」と記載された全ての個人情報の開示について—受領団体を特定してください。

→括弧内で、「共有」された個人情報のカテゴリを番号で列挙してください。→当該各カテゴリについて、共有の商業目的を説明してください。

(回答)

例:

■ 適用なし

CPRAデータマッピング質問票

人材採用の例

E. 過去12ヶ月間の個人情報の販売、共有および事業目的開示

Q15. 事業目的の開示

Q12において列挙された、「事業目的」の開示と記載された全ての個人情報の開示について—受領団体を特定してください。

→括弧内で、事業目的をアルファベットで列挙してください。

→当該各事業目的について、開示された個人情報のカテゴリを番号で列挙してください。

(回答)

例:

- Google Drive→(E)→1、2、9、10、11
- Microsoft Exchange→(E、I-通信)→2、9、10、11
- HostGator→(E)→1、2、9、10、11
- NY HQ → (E) → 2、9、10、11

CPRAデータマッピング質問票

人材採用の例

E. 過去12ヶ月間の個人情報の販売、共有および事業目的開示

Q16. 第三者受領者による商業使用

Q15において特定された全ての開示について→ 開示された個人情報を第三者に対して再販売し、共有し、もしくはさらなる開示を行う、または契約上再販売(もしくは共有もしくはさらなる開示)を行う能力を有する受領者を列挙してください。

注: 開示された個人情報のさらなる販売/共有/使用について契約に定めがない場合、ここに記載してください。

(回答)

例:

- HostGator(契約において禁止されていない)

CPRAデータマッピング質問票

人材採用の例

F. 経済的インセンティブ・プログラム

Q17. 経済的インセンティブ

事業記録のためまたは事業者の処理活動に関連して、個人情報の取得、販売/共有または削除の対価として提供される金銭的インセンティブ（または罰則）を特定し、記載して下さい。

（回答）

例:

■ なし

CPRAデータマッピング質問票

人材採用の例

G. 保存、保持およびセキュリティ実務

Q18. 保存場所

貴社が個人情報を保存する場所（関連する場合、第三者の名前を含む）を特定して下さい→（保存場所が物理的または電子的であるかを含む）

（回答）

例：

- 外部クラウド →（Googleドライブ）
- 従業員の受信トレイ →（マイクロソフトエクスチェンジ）
- HR のネットワーク化されたHドライブ →（X 社が提供する外部サーバー）
- 物理的な紙ファイル →（オンサイト）

CPRAデータマッピング質問票

人材採用の例

G. 保存、保持およびセキュリティ実務

Q19. 保存された情報に関する組織化および再識別の能力

特定の個人、場所、および消費者のカテゴリに属するすべての保存された内容および/または個人情報のカテゴリの識別を可能にする、組織および検索機能について記載して下さい。

(回答)

例:

- 取得された任意のタイプの個人情報で検索/分類できる (IPアドレスとクッキーを除く)
- (カリフォルニア州を含む) 郵送先住所で検索することができる。

CPRAデータマッピング質問票

人材採用の例

G. 保存、保持およびセキュリティ実務

Q20. 保存期間

消費者の個人情報that保存される時間の長さ(個人情報のカテゴリによって時間の長さが異なる場合は、そのようなバリエーションとそれらが適用される個人情報カテゴリを括弧内に記載して下さい)を記載して下さい。

(回答)

例:

- 10年

CPRAデータマッピング質問票

人材採用の例

G. 保存、保持およびセキュリティ実務

Q21. セキュリティ・コントロール

不正な開示/データ漏洩を防止するために、内部および外部のセキュリティに関する手続/実務のカテゴリ(技術的、管理的、および/または物理的)を特定し、その後→各カテゴリの特定の種類のセキュリティ管理を括弧内に記載して下さい。

(回答)

例:

- 技術面 → (暗号、ファイアウォール、ウイルス対策プログラム)

CPRAデータマッピング質問票

人材採用の例

H. 消費者通知/連絡

Q22. 消費者への通知・連絡

個人情報の取得、処理、販売/共有、および当該情報に関する権利、ならびに消費者が当該個人情報に関する問い合わせおよび要求を行う方法について、消費者に通知するための仕組みを特定し、記載して下さい。

(回答)

例:

- クッキーの取得に関する通知
- 人事の連絡先メールアドレスおよび電話番号はオンラインで公開されている

CPRAデータマッピング質問票

人材採用の例

I. 法的分析 - 受領者のカテゴリ

Q23. サービスプロバイダ

サービスプロバイダの定義に該当する、貴社が個人情報を共有するQ12の受領者を特定し→共有される個人情報のカテゴリを括弧内に列挙し(数字で)→該当する契約が必要な条件が含まれていることを確認したか否かについて特定して下さい。

(回答)

例:

- Google ドライブ → (1、2、9、10、11)→契約が必要な条件を満たしていることを確認した。
- マイクロソフトエクステンジ → (2、9、10、11)→契約が必要な条件を満たしていることを確認した。

付録2(CPRA下で紛争化しやすい類型を考える上で参考となるGDPR制裁金決定事例)

データ処理に関する原則を遵守しなかった場合(GDPR5条) 適法、公平かつ透明性のある方法で処理すること(GDPR5条1項(a))



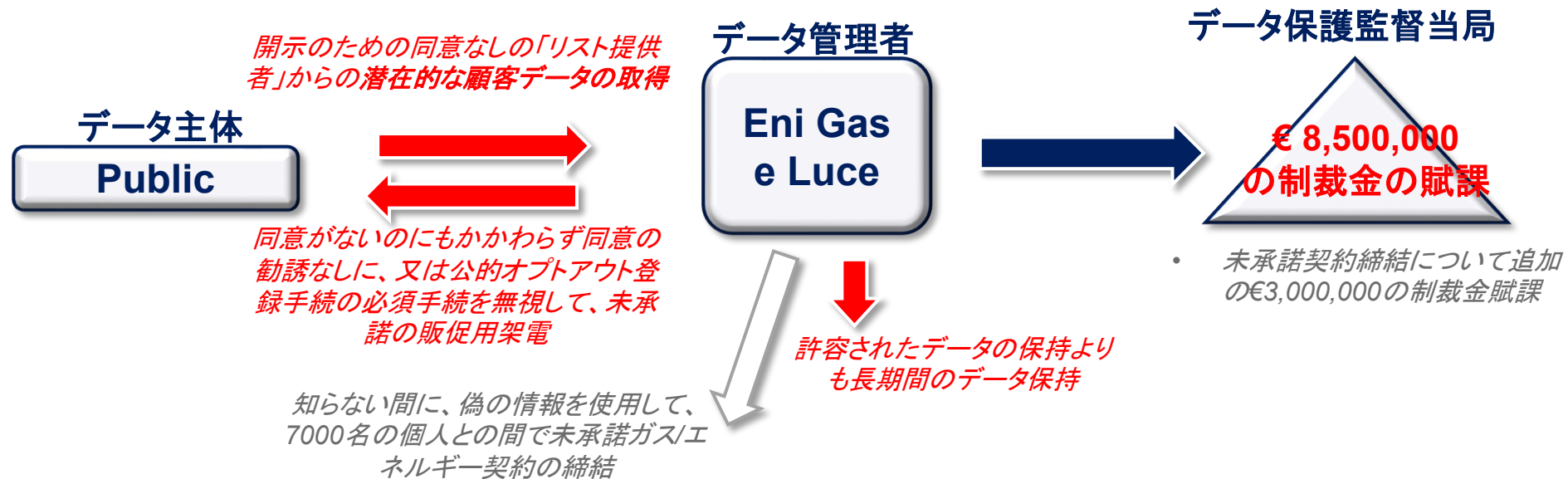
監督当局	ドイツ(ハンブルグ)	決定の日付	2020年10月1日
制裁金の金額	35,258,708ユーロ(約44億円)	被決定人	H&M Online Shop (ニュルンベルクサービスセンター)
事案の概要	少なくとも2014年以降、被決定人の従業員の一部の私生活の状況が包括的に記録され、記録されたデータがネットワークドライブに保存された。例えば、被決定人は、従業員が休暇や病気で職場に戻った後、「ウェルカムバックトーク」を実施した。これによって被決定人が知るところとなった情報(従業員の病気の症状や診断に関する情報など)が記録され、保存された。さらに、一部の管理職は「Flurfunk」(ブドウの木を通して何かを聞くことを意味する)を使用して、家族の問題や宗教的信念など、個々の従業員の幅広い知識を習得した。ネットワークドライブに保存された情報は、最大50人の会社の管理職がアクセスでき、従業員の作業パフォーマンスの評価や雇用決定に使用された。当該データ収集は、技術的エラーによって発覚。2019年10月、ネットワークドライブに保存されたデータは全社的に数時間アクセス可能となった。違反が判明した後、経営陣は従業員に謝罪し、金銭的補償を提供した。さらに、データ保護監督当局とともにさらなる保護的措置を導入した。		



データ処理に関する原則を遵守しなかった場合(GDPR5条) 適法、公平かつ透明性のある方法で処理すること(GDPR5条1項(a))



監督当局	イタリア	決定の日付	2019年12月11日
制裁金の金額	850万ユーロ (約11億円)	被決定人	Eni Gas e Luce (電気ガス)
事案の概要	管理者は、テレマーケティングおよびテレセールス活動において、データ主体の同意を取得しておらず、データ主体が販促に関する電話の受信を拒否した場合でも販促の電話を行い、また公的なオプトアウト登録をチェックするための手続も経ていなかった。管理者では販売促進に関してデータ主体の意思について考慮するための技術的・組織的対策が欠けていた。また、個人データは許可されたデータ保持期間よりも長く処理されていた。潜在的な顧客に関するデータは、データの開示に同意を得ずに第三者(リストプロバイダー)から収集されていた。監督当局は、これらの違反行為について、制裁金を課した。		



- 事業者が行うマーケティングにおける個人情報の収集・使用に関してもCPRA遵守について特に注意が必要である。特に、利用目的との関係で必要な保持期間を限定し、限定された保持期間を遵守する形で使用することも重要である。

データ処理に関する原則を遵守しなかった場合(GDPR5条)
不正又は違法な処理からの保護、不慮の損失、破壊、
損失からの保護を含み、個人データの適切なセキュリティが
確保される形で処理すること(GDPR5条1項(f))



監督当局	スペイン	決定の日付	2020年3月9日
制裁金の金額	1万5,000ユーロ(約186万円)	被決定人	ホテル
事案の概要	ホテルのマネジメントおよび従業員代表者は、データ主体が被ったハラスメントの被害に関する情報(健康状況を含む)が記載されたレターを受領した後、閲覧する権限のない他の従業員との会議においてレターの内容を明らかにした。監督当局は、当該行為は 完全性及び機密性の原則 に違反するとの判断を示した。		



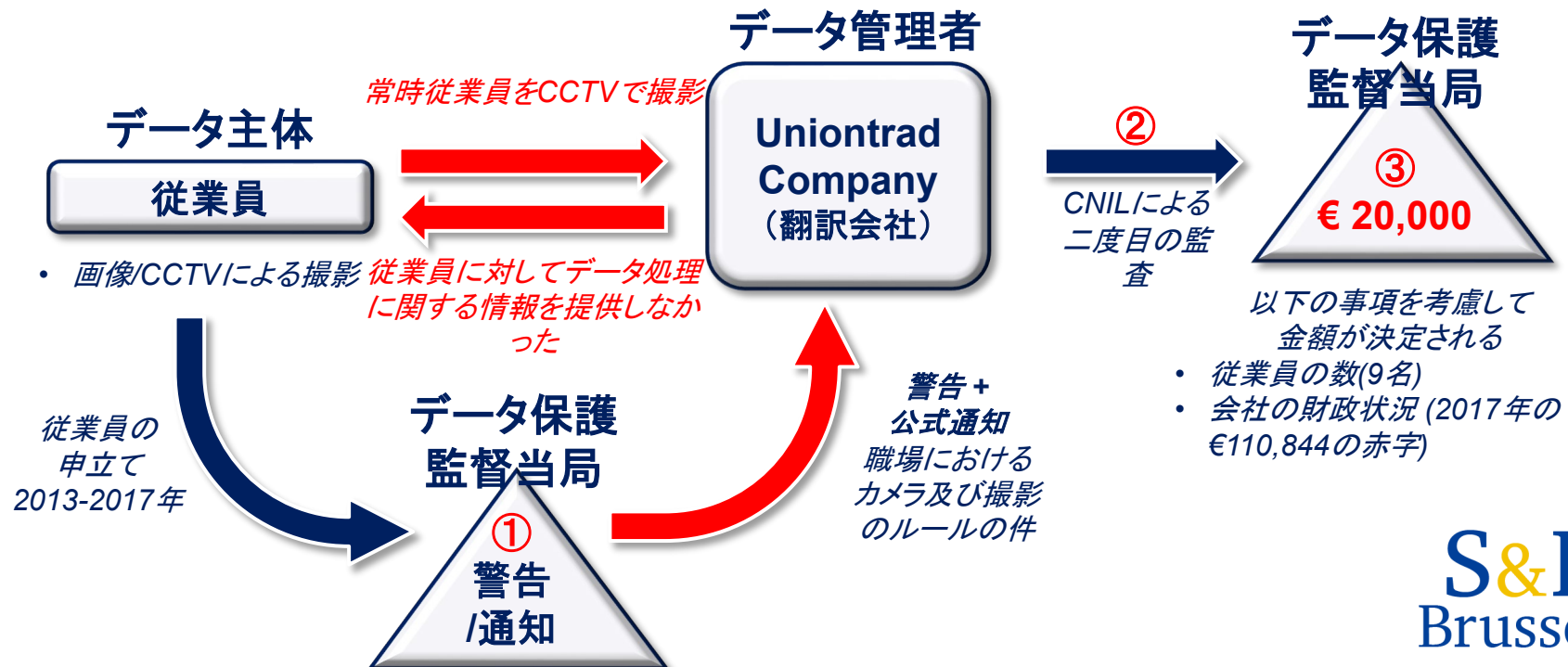
- 事業者が職場内でのトラブルに関連して収集・使用する従業員の個人情報については従業員に通知した使用目的外での使用を行わないようにCPRA上も注意する必要がある。

適法に個人データを処理しなかった場合(GDPR6条)



- 下記事案では監視カメラが問題となったが、職場において防犯目的等の監視カメラの設置を行うことは珍しい。米国子会社においても職場に防犯目的で設置した監視カメラによって撮影された従業員の映像に含まれる従業員の個人情報の収集の事実を意識し、防犯目的以外に使用しないことを確保する必要がある。

監督当局	フランス(CNIL)	決定の日付	2019年6月13日
制裁金の金額	2万ユーロ(約248万円)	被決定人	Uniontrad Company(翻訳会社)
事案の概要	監督当局は、管理者による職場での処理行為について、以下の違反行為を認定した。 ● 6名の従業員が職場においてカメラで常時撮影されていた(適法性の原則違反) ● 従業員に対して情報提供がなされていなかった(透明性の原則違反) ● コンピュータの作業ステーションはパスワード管理されておらず、各従業員が共有の職場の電子メールにアクセスできた(完全性及び機密性の原則違反)		





杉本 武重

Takeshige Sugimoto

takeshige.sugimoto@sandkbrussels.com
www.sandkbrussels.com

直通 03-6429-8040; 携帯+1 347 259 2661;
080-8051-4848; +32 494 67 33 51

S&K Brussels法律事務所

Tokyo Office (HQ): 〒143-0023 東京都大田区山王2-5-6山王ブリッジB1F

New York Office: 1330 6th Avenue, Suite 23, New York, NY 10019 US

Brussels Office: Bastion Tower 20F, Place du Champ de Mars 5, 1050 Brussels, Belgium

Washington D.C. Office, S&K Brussels Consulting (S&K Brussels Consulting USA Corporation)

1717 Pennsylvania Avenue NW Suite 1025, Washington, DC 20006 USA

2006年 弁護士登録(59期)
同年 第一東京弁護士会所属
2013年 ニューヨーク州弁護士登録
同年 ニューヨーク州弁護士会所属
同年 ブリュッセル弁護士会登録(B-List)
同年 同会所属

S&K Brussels法律事務所 事務所代表
マネージングパートナー(東京・NY)・パートナー(ブリュッセル) 弁護士 杉本 武重

経歴

2000年 駒場東邦高等学校卒業
2004年 慶應義塾大学法学部法律学科卒業
2006年-2013年 長島・大野・常松法律事務所アソシエイト
2012年 シカゴ大学ロースクール法学修士課程卒業(LL.M)
2013年 オックスフォード大学法学部法学修士課程卒業(Magister Juris)
2013年-2014年 WilmerHale法律事務所ブリュッセルオフィス・アソシエイト、2015年-2017年シニアアソシエイト
2015年-現在 デュッセルドルフ日本商工会議所法務委員会専門委員
2016年-2017年 公正取引委員会競争政策研究センター客員研究員
2017年-2018年 Gibson Dunn & Crutcher法律事務所ブリュッセルオフィス・オブカウンセル
2018年-2019年 Bird & Bird法律事務所ブリュッセルオフィス・パートナー
2018年-現在 一般財団法人情報法制研究所上席研究員
2019年-現在 当事務所開設・事務所代表、ニューヨークオフィス・マネージングパートナー、ブリュッセルオフィス・パートナー
2019年-現在 一般社団法人日本DPO協会理事
2020年-現在 当事務所東京オフィス・マネージングパートナー
2020年-現在 (一社)次世代基盤政策研究所上席研究員

主要な取扱分野

- カリフォルニア州消費者プライバシー法(CCPA)、カリフォルニアプライバシー権利法(CPPRA)、米国連邦データプライバシー法案、EUの一般データ保護規則(GDPR)、タイ、中国及びブラジルのデータ保護法をはじめとするグローバルデータ保護コンプライアンス
- EU競争法、特に国際カルテル調査対応、ガンジャンピング規制対応を含む企業結合規制対応に関する助言

最近の主要著作

- 「ホット・イシュー 欧州委員会が2020年11月25日に公表 EUデータガバナンス法案の概要と日本企業への影響」(2021年2月、経理情報2021.2.1 (No. 1601)24-27頁(中央経済社))
- 「カリフォルニア州消費者プライバシー法(CCPA)実務ハンドブック」(2019年12月、日本貿易振興機構(ジェトロ)サンフランシスコ事務所・イノベーション・知的財産部 スタートアップ支援課)

最近の主要講演

- 第2弾CCPA解説ウェビナー(法務編)(2020年9月29日、主催:ジェトロ・サンフランシスコ/ロサンゼルス様、協力:北加日本商工会議所様、南カリフォルニア日系企業協会様)
- CCPA最新動向解説ウェビナー(2020年7月31日、Keidanren USA)
- CCPA最新動向解説ウェビナー(2020年7月14日、主催:ジェトロ・サンフランシスコ/ロサンゼルス、協力:北加日本商工会議所、南カリフォルニア日系企業協会)

最近の受賞実績

- 2019年12月16日付日本経済新聞朝刊11面(法務)の「企業が選ぶ弁護士ランキング」の「データ関連」の部門で第4位に、同月15日付日本経済新聞電子版「2019年第15回企業法務・弁護士調査」で「ライジングスター」部門に、それぞれ選出
- EUデータ保護法: Legal 500 EMEA 2019 & 2020: Belgium: EU Regulatory: Privacy and Data Protection
- EU競争法: Legal 500 EMEA 2018 & 2019: Belgium: Competition: EU and global

オンライン名刺交換は下のQRコードを御利用下さい



S&K
Brussels