CPRA と GDPR・(日本の)個人情報保護法との比較

項目	GDPR	CPRA	日本法
保護対象情報／Cookie	「個人データ」: 特定された(され得る)個人に関係する情報。Cookie データも多くの場合該当。	「個人情報」: 特定の消費者・世帯に関連付けできる情報。 Cookie データも多くの場合該当。	「個人情報」: 特定の個人を識別できる情報。Cookie データは氏名等と紐付け管理している場合に該当。
機微情報	「特別カテゴリーの個人データ」	「機微個人情報」	「要配慮個人情報」
義務主体	「管理者」／「処理者」。	「事業者」／「サービス提供者」／「契約業者」／「サードパーティ」	「個人情報取扱事業者」／取扱い委託先。
域外適用	(a) EU 域内データ主体への物品・サービス提供, または, (b) EU 域内データ主体の行動監視に関連する処理等。	ほぼ GDPR の(a)に相当する域外適用あり。	ほぼ GDPR の(a)に相当する域外適用あり。
処理の原則	目的の制限／データ最小化／保存期間の制限。	ほぼ GDPR と同じ。	目的の制限。
処理の適法性／同意	個人データの全処理に同意その他限定列挙された適法性の根拠を要求。 特別カテゴリーの個人データの処理は原則明確な同意要。	16 歳未満消費者の個人情報の販売・共有等は同意要。 収集・利用自体には同意その他具体的根拠要求されず。	不正収集・不適正利用の禁止。 要配慮個人情報収集は原則同意要。 その他収集・利用自体には同意その他具体的根拠要求されず。
同意の要件	自由意思による／目的ごとの／情報を与えられた上での／言葉または積極的行為による／明確な意思表示。	ほぼ GDPR と同じ。	なし。[1]
本人への情報提供／プライバシーポリシー等による公表	**【提供時期・方法】** 直接収集の場合は収集時点で／間接収集の場合は収集後遅くとも 1 か月内に通知。	**【提供時期・方法】**直接収集の場合は収集時かその前に通知／間接収集の場合は事前公表で代替可。	**【提供時期・方法】** 書面(電磁的記録を含む)収集の場合は事前通知。その他の場合は直接間接問わず事前公表または事後に通知か公表。
	【主な項目】 処理目的／処理の適法性の根拠／(間接収集の場合)収集個人データのカテゴリー／受領者(提供先)のカテゴリー／域外移転の有無と根拠／保存予定期間または決定基準／データ主体の権利内容／(間接収集の場合)情報源／自動意思決定の有無と処理ロジック。	**【主な項目】** **(収集時通知)**収集個人情報のカテゴリー／収集・利用目的／販売・共有の有無／保存予定期間・決定基準。 **(プライバシーポリシー等による公表)** 過去 12 ヶ月間の収集情報のカテゴリー,その情報源のカテゴリーと収集目的／過去 12 ヶ月間の販売・共有情報のカテゴリー, 販売・共有先のカテゴリーと販売・共有目的／16 歳未満の情報販売・共有の認識／過去 12 ヶ月間の業務目的開示情報のカテゴリー, その開示先カテゴリーと開示目的／機微個人情報の所定の目的外利用・開示の有無／各権利の説明・権利行使手続(請求フォーム・リンク含む)とその結果／個人情報大量処理者の前年消費者請求対応情報(指標)	**【主な項目】** **(収集時通知)**利用目的。 **(プライバシーポリシー等による公表)**利用目的／権利行使手続／安全管理措置／苦情申出先／オプトアウトによる第三者提供に関する情報／共同利用に関する情報／安全管理措置(安全管理に支障を及ぼすおそれがあるものを除く)。

本人の権利	開示請求権(アクセス権)／訂正請求権／消去請求権／処理制限権／データ・ポータビリティの権利／処理禁止権(異議申立権)／完全自動意思決定に服さない権利。	開示請求権／訂正請求権／削除請求権／販売・共有オプトアウト権またはオプトイン権／機微個人情報の利用・開示制限権／データ・ポータビリティの権利／自動意思決定(プロファイリングを含む)に関する開示請求・オプトアウト権(但し規則未制定)／権利行使を理由に差別・報復されない権利。	開示請求権／訂正請求権／利用停止・消去請求権／個人データの電子ファイル形態での開示請求権。
説明責任／記録等	GDPR 遵守とその説明・証明責任／処理全般の記録義務。	消費者請求対応記録・保存／大量処理者の研修・請求対応件数等の情報(指標)公表義務。	第三者提供に係る記録義務。
処理委託	GDPR 遵守を十分保証できる者にのみ委託／所定の契約条件／再委託制限。	委託目的は「業務目的」に制限／所定の契約条件／再委託制限。	委託先の監督義務。
セキュリティ	適切なセキュリティ措置実施義務(32)。	合理的セキュリティ措置実施義務。	必要適切な安全管理措置実施義務。
漏えい等(侵害)の報告／本人への通知義務	監督機関への報告／高リスク侵害の場合本人に通知。	(加州データ侵害通知法)所定個人情報の漏えい等の場合本人に通知／被害者 500 名超の場合州司法長官に通知書サンプル提出。	所定の場合，個人情報保護委員会に報告・本人に通知。
処理のリスク評価義務／高リスク処理の制限・禁止	高リスク処理について「データ保護影響評価」(DPIA)・監督機関との事前協議／場合により処理の制限・禁止。	重大リスク処理についてサイバーセキュリティ監査・保護庁への定期的リスク評価書提出／場合により処理の制限・禁止(但し規則未制定)。	なし。
域外移転	十分性認定，SCC その他の移転根拠(同意は例外的)必要。	特別な規定なし(販売・共有・業務目的開示その他開示に関する規定適用)。	十分性認定国以外への移転は同意または所定の移転契約等がなければ不可。同意を得る前に所定情報提供。
執行機関	EU 各加盟国の監督機関。	カリフォルニア州プライバシー保護庁／州司法長官	個人情報保護委員会。
違反に対する救済と制裁	**【データ主体の権利】** 監督機関への苦情申立とその不服申立訴訟／損害賠償請求を含む司法救済 **【監督機関による制裁】** 全世界売上の 2%または 4%内の制裁金その他処分。	**【消費者の権利】** 保護庁への苦情申立／所定個人情報の漏えい等に関する法定損害賠償を含む損害賠償・差止請求訴訟提訴権 **【保護庁／州司法長官による制裁】** 違反 1 件 2,500 ドル(故意／16 歳未満個人情報に関する違反はその 7,500 ドル)以下の制裁金・排除措置・差止。	**【本人の権利】** 特に規定はないが，事業者の行為が民法の不法行為に該当する場合は損害賠償請求可。 **【制裁】** 制裁金はない。個人情報保護委員会の命令に違反等した個人の刑罰規定と両罰規定がある。
その他各法に特有の制度	ePrivacy 指令により，Cookie(その他パソコン，スマートフォン等への情報保存・アクセス技術)の利用に，Cookie 等が個人データか否かを問わず，事前に GDPR 上の要件を満たす同意が必要。	販売・共有と機微個人情報の所定の目的外利用に関し，"Your Privacy Choices"等のリンク設置必要。 オプトアウト設定シグナルに応じることが必要。	オプトアウトによる第三者提供制度がある。 個人データ利活用手段として「匿名加工情報」および「仮名加工情報」の各制度あり。

[1] **【日本法おける同意の要件】** 但し，ガイドライン(通則編)では，『…「本人の同意を得(る)」とは，…本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない』とされている。