ホワイトペーパー

GDPR、CCPA、さらなる規制：

企業のコンプライアンスと顧客からの信頼向上に役立つアイデンティティガバナンス

エグゼクティブサマリー

ビジネスに影響を与えるプライバシー規制が、世界的な傾向として広まっています。話題になった EU の一般データ保護規則（GDPR）は、2018 年に施行されました。2020 年 1 月 1 日にはカリフォルニア州消費者プライバシー法（CCPA）が施行され、世界第 5 位の経済規模を持つカリフォルニア州でビジネスを展開する企業に影響を与えます。

しかし、これは始まりに過ぎません。広く報じられたデータ漏えい、ID の窃盗、関連スキャンダルがきっかけとなり、プライバシーとコンプライアンスの規制の成立が世界中で急速に進んでいます。米国だけでも 9 つの州で、個人を特定できる情報（PII）について企業や組織に幅広い責任を課し、高い透明性とより優れたコントロールを消費者に提供することを求める法案が提出または通過しています。

企業は、このような新しいプライバシー法や規制を無視するわけにはいきません。金銭的な数値から見ただけでも、GDPR 施行後、最初の 12 か月間はそれほど高額でなかった罰金が、現在では 2 億ドル超とかなりの額に膨れ上がっています。しかも、それでもまだ世界全体の年間売上高の 4% という上限には達していないのです。しかし、グローバル企業の損失は財務面だけではありません。危険にさらされているのは、消費者からの信頼です。

重要なプライバシーの保護について、顧客が企業や組織を信頼していない場合、その負の影響は営業やマーケティングに及びます。今日の企業は、明示的な同意を得ないと個人データを処理できません。同意を得るには、信頼が必要です。信頼がなければ、同意は得られません。同意が得られなければ、データは提供されません。データが提供されなければ、営業やマーケティングキャンペーンの効果は望めないのです。

プライバシーの尊重は、コンプライアンスの問題であるだけでなく、ビジネスの重要な強みにもなります。企業や組織にとって、プライバシーとアイデンティティのガバナンスは、ユーザーや顧客との信頼関係の構築に役立ち、ゆくゆくは顧客ロイヤルティの向上、さらにビジネス収益の大幅な増加へとつながっていくのです。

このホワイトペーパーでは、GDPR、CCPA、および関連する世界中のプライバシー規制の概要をご紹介します。法規制コンプライアンス、アイデンティティガバナンス、データ保護を通じて顧客の信頼を築くための事例を提供し、適切なアイデンティティ管理ソリューションの必要性について論じます。また、大手ブランド 2 社がプライバシーコンプライアンスの目標をどのように達成したのかについてもご説明します。

EU 一般データ保護規則

2018 年 5 月 25 日に GDPR が施行されました。この包括的なデータ保護法の目的は、ヨーロッパ全体で地域ごとに存在するデータ保護法を統合することにあります。この法の適用対象には、ヨーロッパ拠点の企業だけでなく、EU 域内でビジネスを展開するすべての企業および組織が含まれます。

GDPR では、PII の収集・保存・使用の方法および不正アクセスに対抗するためのデータの保護方法について、非常に細かい要件が定められています[1]。これには、個人データの識別やセキュリティ確保の方法だけでなく、新しい透明性要件への対応方法、個人データの漏えいの検知と報告の方法、プライバシー担当者のトレーニング方法も含まれます。

GDPR では、GDPR の原則に違反した組織に罰金を科すことができるため、財務状況に重大な影響が及ぶ可能性があります。初期のプライバシー違反に科された罰金は比較的軽微でしたが、最近の罰金に関しては世界中のニュースで大きく報じられているため、業界での注目も高まっています。多額の罰金を科せられた例は 2 件あります。1 件は 50 万人に影響を及ぼすデータ漏えいが発生した大手航空会社[2]（2 億 3,000 万ドル）で、もう 1 件は 3 億 8,300 万人のホテル滞在客の個人情報がハッキングされた世界大手のホスピタリティ企業[3]（1 億 2,300 万ドル）です。これらは特にグローバル企業からの注目を集めています。

カリフォルニア州消費者プライバシー法

プライバシー保護に関して企業にさらなるプレッシャーをかけるかのように、カリフォルニア州消費者プライバシー法（CCPA）の施行日が近づいてきました[4]。2020 年 1 月 1 日より、カリフォルニア州でビジネスを行う大規模な企業または組織には、このカリフォルニア州の新しい厳格なプライバシー法を遵守することが要求されます。このプライバシー法は、同州内のすべての居住者に関する法的拘束力のあるプライバシー権を策定したものです。GDPR と同じく、この新規制の適用対象はカリフォルニア州に拠点を置く企業だけではありません。同州でビジネスを展開するすべての企業が対象です。

CCPA では、カリフォルニア州の消費者の個人データに対し、次の対策が定められています。[5]

- **所有権：**消費者が企業に対して、個人情報を共有または販売しないように伝えることができる権利
- **コントロール：**消費者が自分自身について収集された個人情報をコントロールできる権利
- **セキュリティ：**個人情報を保護する責任は企業が負う
- 次の条件に 1 つでも該当する企業または組織は、CCPA を遵守する必要があります。
  - 2,500 万ドルを超える年間総売上を達成している
  - 商業目的で 5 万件以上の消費者、世帯、デバイスに関する個人情報を購入、取得、販売、共有する
  - 消費者の個人情報の販売によって年間売上の 50% を得ている

昨年は、多くの企業が GDPR を遵守するために大きな困難に直面しましたが、今回は CCPA も遵守しなければなりません。施行日がすぐそこに迫ってきているため、時間の余裕はありません。カリフォルニア州で顧客のアイデンティティデータを収集し、パーソナライズされたマーケティングキャンペーンのために顧客プロファイルを構築している企業は、すぐに行動する必要があります。そうしなければ、大規模な罰金が科せられるリスクを負うことになります。

GDPR と CCPA の比較

CCPA の範囲は GDPR とは少し異なってはいますが、消費者に自分のデータの使用を制御および拒否できるという権利が認められています。いずれの規制でも、企業は、セキュリティを確保した環境でデータを保存し、収集する個人データの種類を明らかにし、消費者からの個人データの削除要請に応じる（一般に「忘れられる権利」と呼ばれます）必要があります。つまり、組織にあるすべてのシステムから個人データを削除できる必要があるのです。

データ処理の法的根拠となる同意については、CCPA と GDPR で異なります。前者が消費者によるオプトアウトを可能にする必要があるのに対し、後者は PII の収集前に明示的な同意を得る必要があります。

世界のその他の規制

さらに重要なのは、GDPR と CCPA がこの世界的傾向の始まりに過ぎないという点です。世界中で、検討中または成立済みのプライバシーとコンプライアンスの法規制が数多くあります。米国だけでも、他の 9 の州において、PII の透明性とコントロールを消費者に提供することを目的に、企業に幅広い責任を負わせる法案が提出されています。[6]

国際レベルでは、プライバシー規則の厳格化（およびビジネスへの影響の拡大）が、企業や組織が無視できない世界的な現象になっています。下の表は、カナダの個人情報保護および電子文書法（PIPEDA）など、新規または審議中の法規制の一部をまとめたものです。

表：施行済み、近日施行予定、または提案中のデータ保護およびプライバシー規制の一例

南北アメリカ	EMEA	アジア太平洋地域
アルゼンチン：PDPL ／法案 No. MEN-2018-147-APN-PTE[7] 米国： カリフォルニア州：CCPA（AB 375） カナダ：PIPEDA[8] ハワイ州：SB 418[9] メリーランド州：SB 0613[10] マサチューセッツ州：SD 341[11] ミシシッピ州：HB 2153[12] ニューメキシコ州：SB 176[13] ニューヨーク州：S00224[14] ノースダコタ州：HB 1485[15] ロードアイランド州：S0234[16] テキサス州：HB 4518[17]	EU：GDPR ロシア：連邦法 No. 152-FZ[18]	オーストラリア：1988 年連邦プライバシー法／情報プライバシー原則（IPPs）[19] 中国：Personal Information Security Specification（個人情報セキュリティ仕様）[20] インド：個人情報保護法案[21] 日本：個人情報保護法（2020 年改正予定）[22]

規制コンプライアンスの枠を超えて：信頼関係の構築

これらの規制により、消費者との信頼関係の構築が、世界中の企業や組織にとってますます重要になっています。GDPR や CCPA、その他の関連規制では、該当する場合、企業は、顧客データの収集および使用について、事前に顧客の同意を取得し、その同意を記録する必要があります。

また、プライバシーは、規制へのコンプライアンスを確保するだけでなく、信頼性に優れた強固なデジタル関係を顧客との間に構築するためにも重要です。個人データのプライバシー保護とセキュリティに対する顧客の期待は高まる一方です。データの悪用、漏えい、認証情報の窃盗などのケースが多数公表されているため、企業が個人データの信頼できる保管者とみなされるためには、高いハードルを超えなければなりません。顧客は、組織にデータを預ける際、その組織を信頼して契約を結びます。その信頼が裏切られた場合、それを取り戻すのはかなり難しくなります。

企業による個人データの処理に消費者が同意するのは、価値のある見返りが提供されるからだけではありません。消費者が企業を信頼しているからでもあります。信頼がなければ、同意は得られません。同意が得られなければ、データは提供されません。つまり、まったく効果のない（または、非常に非効率的な）営業やマーケティングキャンペーンになってしまうのです。信頼は、顧客データの獲得を目指す企業の「新たな通貨」と呼ばれています。

同意の重要性：ユーザー体験の見直し

GDPR および CCPA では、顧客が自身の同意の確認、変更、さらには撤回を随時行える必要があります。つまり、同意の取得時には使いやすい Web 形式を用意し、同意の撤回時には複雑な事務的プロセスを用意することで撤回を意図的に難しくしている企業は、規制に反しているとみなされます。さらに、企業は個人データの収集理由と使用目的も明らかにする必要があります。

これは、マーケティング組織に多大な影響をもたらします。たとえば GDPR では、新規見込み客の開拓を目的とした登録閲覧制コンテンツのランディングページで、事前にチェックを入れたボックスを表示して同意を得ることができなくなりました。同意は、オプトアウトではなくオプトインでなければなりません。つまり、消費者がボックスにチェックを入れて同意する必要があるのです。これに対し CCPA では、黙示の同意が認められているため、事前にチェックを入れたボックスを表示させても規制違反ではありません。この相違は、グローバル企業にとって悩みの種です。2 つの主要市場に対応するため、Web サイトやアプリで異なる登録フォームを表示できるようにする必要があるのです。または、地域に応じてまったく異なる Web サイトやアプリを展開しなければならないため、コードの開発やメンテナンスの負担が倍増します。

新しい規制では、過剰なデータ収集も禁止されています。企業は、提供するサービスや製品に必要な個人データしか収集できません。ニュースレターの送信やホワイトペーパーのダウンロードのために電話番号や性別を求めることは、規制違反になります。つまり企業は、ユーザー体験の見直しや再設計を行い、登録ページなどのあらゆるフォームから過剰なデータ収集とみなされる可能性のあるすべてのデータフィールドを削除する必要があるのです。

グローバルな小売企業が集約型ソリューションを導入し、現在および将来のプライバシー法へのコンプライアンスをシンプル化

ある世界的な小売企業が、最近、Akamai Identity Cloud を導入してプライバシーコンプライアンス要件に対応しました。このソリューションにより、顧客に自身の個人データの透明性とコントロールを提供できるようになったのです。これは、登録時に取得される PII を最小限にするとともにデータ処理の前に同意を求めることにより実現しました。

Identity Cloud では、登録時およびログイン時のユーザー体験を完全にカスタマイズでき、同意フォームを目的に応じて随時呼び出せます。これにより、消費者は、提供に同意したデータの使用目的や自身で行ったオプトアウトについて把握しやすくなります。消費者が自身の同意設定の確認、変更、撤回をいつでも行うことができるのです。

同社は、Identity Cloud のスコープアクセス機能を活用して、アイデンティティデータにアクセスする担当者の役割に応じて、データレコードやレコード内の特定フィールドへのアクセスを制限しています。つまり、カスタマーサービス担当者、マーケティング担当者、開発者のアクセス権がそれぞれ異なるということです。この Identity Cloud 独自の機能により、顧客データが露出するリスクが軽減し、データセキュリティのレベルが飛躍的に向上します。

Identity Cloud は、顧客データを 1 つの中央リポジトリにまとめ、きめ細かいアクセス制御を可能にすることで、「有害な」アイデンティティデータ（顧客が同意を撤回または削除を要求した後もデータベースに保存されているデータなど）が無秩序に分散するのを緩和できます。中央リポジトリは、「忘れられる権利」に対応するためのデータ削除のシンプル化にも役立ちます。

すべての同意設定は、顧客プロファイルとともに、監査に対応した一つのフォームに保存されます。さらに、変更ログと監査証跡も一緒に保存されるため、誰がどのリソースにいつアクセスしたかがわかります。

データを確実に保護

コンプライアンスは、プライバシーに配慮するだけではありません。顧客データのセキュリティを確保し、攻撃者から保護することも、プライバシー確保と密接につながっています。個人のアイデンティティデータは不正利用や悪用が生じやすく、ハッキング攻撃の主要な標的となっています。IBM Security がスポンサーとなり、Ponemon Institute が実施した 2018 年の Cost of a Data Breach Report[23] では、調査対象組織の 48% が、データ漏えいの根本原因として悪意のある攻撃または犯罪者の攻撃を挙げ、漏えいしたアイデンティティレコードあたりの平均コストは約 157 ドルであることがわかりました。

データ漏えいには数十万（時には数百万）ものレコードが関連することが多く、それによるコストは企業に深刻な影響を及ぼす可能性があります。さらに、評判の低下、顧客からの信用の失墜、GDPR や CCPA に伴う罰金などによる収益損失も加わります。

アイデンティティガバナンスの必要性

個人のアイデンティティは貴重な資産です。それは、PII を収集してまとめる企業にとってだけではありません。情報の提供元であり、保護を強く求め、誤用を許容できない個人の消費者にとっては、その重要度はさらに高まります。

消費者個人の生活に占めるデジタル領域が拡大するにつれ、企業のプロファイルデータには、さまざまな個人データ（名前、住所、電話番号、性別、支払情報から、個人的な嗜好、買い物や閲覧の履歴などの行動データまで）が含まれることになります。企業が重要なデータのセキュリティを確保し保護する必要性は大幅に高まり、世界の規制機関も規制をさらに厳格化することでこのニーズに対応しつつあります。

規制コンプライアンスとセキュリティは、アイデンティティ管理を著しく複雑で重大なものにする主な要因です。しかし、エンタープライズグレードのアイデンティティ管理ソリューションなら、登録時に取得されるデータ量を最小限に抑え、データ処理の前に同意を求めることにより、顧客に自身の個人データの透明性とコントロールを提供できます。

適切なアイデンティティ管理によって、企業は消費者の信頼を取り戻すことができるのです。

世界的な飲料ブランドが GDPR へのコンプライアンスを短期間で達成

ある世界的な飲料会社が、わずか 2 か月間で自社ブランドの欧州内全顧客向けに GDPR のプライバシーコンプライアンスを確保するという難問に直面しました。同社は、すでに Identity Cloud を導入していましたが、今回は、変化する消費者プライバシー保護規制へのコンプライアンスを迅速に確保する必要がありました。

着手からわずか 2 か月後にコンプライアンスを達成できました。同社の取り組みの中心は、GDPR の要件を遵守するために、個人データをマーケティングとパーソナル化に利用することについて消費者から明示的な同意を取得することでした。Identity Cloud には、高度にカスタマイズできるきめ細かい同意フォームがあり、Web サイト、モバイルアプリケーション、IoT デバイスなど、あらゆるデジタル資産で随時呼び出すことができます。この強力な機能により、GDPR へのコンプライアンスを達成できただけではありません。顧客が自身の同意に関する設定の確認や管理を行いやすくなったため、顧客との信頼関係の構築にもつながりました。

導入全体で特に難しかったのは、GDPR の「忘れられる権利」と、消費者向けプロモーションの期間中はデータを保持するという法的義務、この 2 つを両立することです。Identity Cloud の機能により、法的に定められた期間はデータを保持し、その期間の最後にデータを確実に消去して、それを顧客に伝えることができました。

Akamai Identity Cloud

Identity Cloud は、Akamai のカスタマー・アイデンティティ・アクセス管理ソリューションです。このプラットフォームは、顧客による個人アカウントの作成や、Web サイト、モバイルアプリ、IoT ベースアプリケーションへの安全なログインを可能にするために必要な機能をすべて備えています。また、プライバシーコンプライアンスの負担を大幅に軽減するツールも備えているほか、安全性の高い顧客プロファイルレポジトリを提供し、顧客の全体像の把握を可能にします。

Identity Cloud は、規制要件への取り組みに役立つ具体的な機能やユーザー体験を提供します。Identity Cloud のプライバシーおよびデータ保護機能には、顧客登録、ログイン、認証、シングルサインオン、スコープアクセス制御、設定／同意管理など、個人データの収集、管理、セキュリティ確保に必要な機能が多数含まれています。

Identity Cloud は次のような機能を通じて、エンタープライズによるプライバシーコンプライアンス規制への対応を支援します。

- 「同意する」チェックボックスの仕組みによる明示的な同意
- 集約型ガバナンスによるアクセス制御
- プログレッシブ（段階を踏んで入力を促す）な許可、登録、プロファイリング
- 簡単なデータアクセスのしくみ
- データ修正および整合性のメカニズム
- データポータビリティ
- データの消去／削除
- 利用者に即したスコープ付きアクセスと統合化
- データの仮名化
- 年齢制限

Identity Cloud を導入することで、企業や組織は、迅速かつ柔軟な方法でエンタープライズグレードのアイデンティティ管理を実装できます。クラウドネイティブなアーキテクチャで設計されたこのソリューションは、トラフィックの急増に対応し、数億人のユーザーに高度なユーザー体験を提供するため、容量のニーズに合わせてインテリジェントに拡張できます。Akamai Identity Cloud は、すべての地域やアプリケーションにまたがってデータを安全に利用できるようにすることで、世界のプライバシー規制の遵守、ブランドへの信頼の構築、顧客データの管理、リスクの緩和をサポートするように設計されています。

Akamai Identity Cloud について詳しくは、akamai.com/identitycloud をご覧ください。

まとめ

顧客と信頼関係を築いて維持したいと考えるすべての企業や組織にとって、GDPR や CCPA、その他の関連プライバシー規制へのコンプライアンスは、セキュリティの保証とともに重要な要素です。消費者は、透明性を求め、重要な個人データのプライバシー保護とセキュリティ確保を要求しています。最近のデータ漏えいや個人情報の盗難、それに関連するグローバル規模の事件は、企業が早急に PII の信頼できる管理人として認められる必要があることを如実に示しています。

顧客が自身の個人情報の収集や保存を組織に許可するときは、その組織を信頼して契約を結ぶものです。その信頼を裏切ると、取り戻すのは非常に困難です。顧客データの取得と保存、および顧客の認証情報や個人情報の処理は、今日の企業にとって違反や妥協が許されない注意義務事項です。信頼を裏切ったら、企業のブランド評価、顧客ロイヤルティ、そして最終的には収益やビジネスの成功も、容易にリスクにさらされてしまうのです。

付録：プライバシー規制要件の概要

この付録では、GDPR と CCPA のほか、世界の多くのデータ保護やプライバシーの規制に含まれる一般的な要件（同意、異議を唱える権利、アクセスする権利、忘れられる権利、データポータビリティ、セキュリティ、漏えいの通知など）の概要を説明します。これらの権利の実装については、制定されているプライバシーおよびデータ保護法によって異なるため、各法規制の影響については弁護士にご相談の上、判断してください。

これらの規制のコンプライアンス要件への取り組みに Akamai Identity Cloud がどのように役立つのかについては、Akamai のブログ投稿をご確認ください。

同意	組織は通常、特定の目的で個人データを収集し処理する前に、エンドユーザーに同意を得なければなりません。有効な同意の取得や同意が必要な場面に関する要件は、適用される法規制によって異なります。
異議を唱える権利	個人データがダイレクトマーケティングや統計分析などの特定の種類のデータ処理に使用されることに対し、データ主体（Data Subject）に異議を唱える権利を与えます。
アクセスする権利	多くの法規制では、処理されている個人データへのアクセス・確認・修正の権利、また、場合によっては、当該データの使用や公開に関する追加情報を求める権利をデータ主体に与えています。

個人データを消去または削除する権利	多くの法規制では、個人データを削除し、第三者への拡散や第三者による処理を一切禁止する、「忘れられる権利」が消費者に認められています。
データポータビリティ	企業および組織は、データ主体に自身のデータのコピーを一般的に利用され機械可読性のある形式で提供し、データ主体がそのデータを妨害なく他の組織に提供できるようにする必要があります。
セキュリティ	企業および組織は、リスクに基づいて適切なデータセキュリティ保護対策を導入し、データが不注意で、または不法にアクセス、変更、紛失、破壊、または公開されるのを防がなければいけません。
漏えいの通知	企業および組織は、データ漏えいを認識したら、一定期間内にその状況をエンドユーザーに通知する必要があります。

出典

1) https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
2) https://www.cnet.com/news/british-airways-faces-record-breaking-230m-gdpr-fine-for-2018-data-breach/
3) https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
4) https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
5) https://www.caprivacy.org/
6) https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf
8) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
9) https://www.capitol.hawaii.gov/measure_indiv.aspx?billtype=SB&billnumber=418&year=2019
10) http://mgaleg.maryland.gov/webmga/frmMain.aspx?pid=billpage&stab=01&id=sb0613&tab=subject3&ys=2019rs
11) https://malegislature.gov/Bills/191/SD341
12) http://billstatus.ls.state.ms.us/documents/2019/html/HB/1200-1299/HB1253IN.htm
13) https://www.nmlegis.gov/Legislation/Legislation?chamber=S&legType=B&legNo=176&year=19
14) https://assembly.state.ny.us/leg/?default_fld=&bn=S00224&term=2019&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y
15) https://www.legis.nd.gov/assembly/66-2019/bill-index/bi1485.html
16) http://webserver.rilin.state.ri.us/billtext19/senatetext19/S0234.htm
17) https://capitol.texas.gov/tlodocs/86R/billtext/html/HB04518I.htm
18) https://pd.rkn.gov.ru/authority/p146/p164/
19) https://pd.rkn.gov.ru/authority/p146/p164/
20) https://www.tc260.org.cn/front/postDetail.html?id=20190201173320
21) https://meity.gov.in/content/personal-data-protection-bill-2018
22) https://www.ppc.go.jp/en/
23) https://www.ibm.com/security/data-breach

Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、ウェブ／モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日 /24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com、blogs.akamai.com、および Twitter の @Akamai でご紹介しています。全事業所の連絡先情報は、www.akamai.com/locations をご覧ください。公開日：2019 年 11 月。