Cookie規制と企業に求められる姿勢
～プラットフォーム研究会検討を中心に～

一般財団法人 日本情報経済社会推進協会
主席研究員 寺田眞治

2023,3

Profile

所属　一般財団法人日本情報経済社会推進協会　主席研究員
一般社団法人モバイルコンテンツフォーラム　常務理事
一般社団法人融合研究所　上席研究員

委員等　総務省　プラットフォームサービスに関する研究会
プラットフォームサービスの利用者情報の取扱いに関するWG
経済産業省　スマートシティ関連データ連携標準TF
経済産業省/総務省　データ流通促進WG
消費者庁　インターネット消費者取引連絡会
ステルスマーケティングに関する検討会

その他　ISO/IEC TC307 Blockchain and distributed ledger technologies
国内審議団体事務局長
ISO/IEC TC317 Privacy by Design　国内審議団体事務局
一般社団法人安心ネットづくり促進協議会　監事
一般社団法人データ社会推進協会　認定審査委員会　諮問委員
デジタル政策フォーラム
株式会社東芝　顧問コンサル

2021年11月号
【特集】デジタル広告の法的問題

◇アドフラウドから見るデジタル広告の課題
寺田眞治

神戸新聞、オムロンのハウスエージェンシーにおける企画職を経て、インターネットのコンテンツ、メディア、マーケティング分野での起業、経営戦略、海外事業、M&A 等に従事するとともに、業界団体の役員を歴任。総務省、経済産業省などの通信政策、国際競争、青少年保護、個人情報保護等に関する委員やオブザーバーを務め、関連する書籍の執筆や専門誌への寄稿多数。

日本とグローバルのプライバシー保護

日本の個人情報保護、プライバシー保護の規制は、グローバルと比較して厳しいのか？

1．日本の保護すべき「個人情報（個人情報保護法）」の定義の範囲は狭い

2．日本の保護すべき「利用者情報（改正電気通信事業法）」の対象者は狭い

3．日本の「個人情報」「利用者情報」の取扱い規定は緩い

個人情報保護法、改正電気通信事業法を遵守しても、まだグローバルの規制に追いつかない
※海外展開するときには十分注意※
↓
グローバルの基準に合わせれば、概ね日本の規制を遵守できる
いずれ、日本もグローバルと同等になる

保護の対象：「個人情報」と「Personal Data」

国際標準規格（ISO/IEC 27000シリーズ等）
PII（Personally Identifiable Information）
個人を識別できる**可能性**のある情報。
※単独では特定の個人を識別できなくても、**他の情報と組み合わせたり照合する**ことで個人を特定できる**可能性**のある情報はすべてPII（性別/年齢/住所、cookie、端末ID、位置情報等）

EU
Personal Data → PIIとほぼ同等

米国
一般にPersonal Dataと使われる場合は、EUと同等（PIIとほぼ同等）

グローバルではほぼ一致しており、日本だけ対象が狭い

日本
個人情報 → **特定の**個人を識別できる情報。単独ではなく、**保有している情報を組み合わせたり、他の情報と容易に照合できる**ことによって**特定の**個人を識別できる情報

保護の対象：「利用者情報」

グローバル（米国含む）

Personal Data、PIIは、個人を識別できる可能性のある情報であれば、端末の内外は問わない。

EU

ePrivacy規則案：電子通信データ（電子通信における通信中のデータ、端末内のデータの全てが対象。

※GDPRを補完するもので、電子通信におけるデータ保護について細則を定めている。

グローバルでは端末内の情報は元々対象となっている
日本は改正電気通信事業法で対象情報がグローバルに近付くことになった

日本

改正電気通信事業法：利用者に関する情報　→　利用者の端末に記録された、個人情報を含む当該利用者に関する情報

※利用目的によって対象外となる情報があるが、**基本的に端末内の情報は全て該当する。**

端末内から外部送信させた情報が個人情報保護法にて取扱いが定められている場合（匿名加工情報、仮名加工情報、個人関連情報等も含む）は、個人情報保護法も遵守しなければならない

※個人情報保護法と電気通信事業法は併存する異なる法律：**ただし重複する部分は工夫次第でまとめることは可能**

（参考）個人情報の分類

<table>
<tr><th colspan="2">名称</th><th colspan="4">定　　義</th><th>例示</th></tr>
<tr><td rowspan="6">個人情報</td><td>特定個人情報</td><td colspan="4">個人番号をその内容に含む個人情報（マイナンバー）</td><td></td></tr>
<tr><td>要配慮個人情報</td><td colspan="4">本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するもの</td><td>本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実</td></tr>
<tr><td rowspan="4">個人情報</td><td rowspan="3">（それだけで）特定の個人を識別できるもの</td><td rowspan="3">単独で個人情報となるもの</td><td colspan="2"></td><td>氏名</td></tr>
<tr><td rowspan="2">個人識別符号</td><td>特定の個人の身体の一部の特徴</td><td>DNA、指紋、歩容データ、顔データ</td></tr>
<tr><td>個人に付与される符号</td><td>パスポート、運転免許証</td></tr>
<tr><td colspan="3">組み合わせて個人情報となるもの</td><td></td></tr>
<tr><td colspan="4">他の情報と容易に照合することができ、それにより特定個人を識別することができることとなるもの</td><td>住所と住宅地図</td></tr>
<tr><td>仮名加工情報</td><td colspan="4">他の情報と照合しない限り特定の個人を識別することができないように加工した個人に関する情報（加工基準は個人上保護委員会規則で定める）
※共同利用、業務委託などで他の事業者が扱う場合には「個人情報ではない仮名加工情報」になる</td><td></td></tr>
<tr><td colspan="2">匿名加工情報</td><td colspan="4">特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、（匿名加工情報を作成したものも含めて）当該個人情報を復元することができないようにしたもの（加工基準は個人情報保護委員会規則で定める）</td><td></td></tr>
<tr><td colspan="2">個人関連情報</td><td colspan="4">生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの</td><td>cookie、おおまかな位置情報、端末ID、広告ID</td></tr>
</table>

保護の対象：対象事業者

グローバル（米国含む）

Personal Data、 PIIを取扱う者は、全て対象者に該当する。

EU

ePrivacy規則案：電子通信データを取扱う者は全て対象者となる。

※GDPRを補完するもので、電子通信におけるデータ保護について細則を定めている。

グローバルでは対象者は限定されていない
日本は改正電気通信事業法でも対象事業者は限定されている

日本

改正電気通信事業法：電気通信事業法で定められた者のみが対象となる。

※電気通信事業者及び電気通信事業を営む者で「利用者の利益に及ぼす影響が大きい」「利用者の利益に及ぼす影響が少なくない」情報を取扱う者

規制の内容

EU

GDPR：Personal Dataの取扱いは原則禁止（**明確な同意取得**などの条件によって例外として取扱いが可能となる）

ePrivacy規則案：電子通信データは秘密とする（リスニング、保管、監視等エンドユーザー以外の干渉を禁止　→　同意取得などの条件によって例外として取扱いが可能となる）

米国

州法、セクトラル法により異なるが、「透明性、アカウンタビリティ」が求められており、**オプトアウトが義務化**されるのが一般的

グローバルでは同意取得もしくはオプトアウトできることが前提
日本は改正電気通信事業法でも「通知・公表」のみで足りる

日本

個人情報保護法：個人情報を取得する場合は「通知・公表」のみが必須
※要配慮個人情報は同意取得が必要

改正電気通信事業法：（個人情報を含む）利用者情報を端末から外部送信させる場合は、「通知・公表」「同意」「オプトアウト」のいずれかが必須となる

（参考）電気通信における欧米のプライバシー保護制度との違い

	EU	USA	日本
対象データ	電子通信データすべて ・端末内のデータ ・通信中のデータ ・M2M含む	※通信に限定せず※ 消費者の情報全般	利用者の端末内のデータすべて
対象事業者	電子通信データを取り扱う事業者すべて	※通信に限定せず※ 消費者の情報を取得、利用する者全般	電気通信事業者及び電気通信事業を営む者
規制の原則	電子通信データは秘密とする ・リスニング、保管、監視、等エンドユーザー以外の干渉を禁止 許容されるものを列記 ・同意を取得した場合等	利用者の権利への対応 ・オプトアウト必須	外部送信を行う場合には通知・公表、同意、オプトアウトのいずれか必須 ※通信の秘密（個人間の通信）に該当する場合は原則取扱い禁止

電気通信事業法改正の経緯

電気通信事業法改正の前段

2009年4月
利用者視点を踏まえたICTサービスに係る諸問題に関する研究会

2010年5月
第二次提言：ライフログ活用サービスに関する検討について「配慮原則」公表

① 広報、普及・啓発活動の推進
② 透明性の確保
③ 利用者関与の機会の確保
④ 適正な手段による取得の確保
⑤ 適切な安全管理の確保
⑥ 苦情・質問への対応体制の確保

配慮原則の対象となる情報は、特定の端末、機器及びブラウザ等（以下「端末等」という。）を識別することができるものとする。対象情報は、個人情報保護法上の個人情報であるか否かを問わない。
例えば、クッキー技術等を用いて生成された識別情報、携帯電話端末に係るいわゆる契約者固有 ID、ログイン中の利用者を識別する ID、端末等のシリアル番号、MAC アドレスや IC タグの ID も、特定の端末等を識別することが可能であるから対象情報となる。また、これらと結びつけることが可能な閲覧履歴、検索履歴、購買履歴等の行動履歴も対象情報に含まれる。

電気通信事業法改正の前段

2012年8月
スマートフォン プライバシー イニシアティブ（SPI）
―利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション―　公表

アプリケーション提供者や情報収集モジュール提供者等を中心に、アプリケーション提供サイト運営事業者・ＯＳ提供事業者、移動体通信事業者等のスマートフォンの関係事業者に広く適用可能な「スマートフォン利用者情報取扱指針」を示す

(1)プライバシー・ポリシーの作成

☞ 以下の項目を記載したプライバシーポリシーを、アプリケーションや情報収集モジュールごとに分かりやすく作成する。（簡略版も作成する。）

（記載項目）

① 情報を取得するアプリ提供者等の氏名又は名称
② 取得される情報の項目
③ 取得方法
④ 利用目的の特定・明示
⑤ 通知・公表又は同意取得の方法、利用者関与の方法*1,2
⑥ 外部送信・第三者提供・情報収集モジュールの有無
⑦ 問合せ窓口
⑧ プライバシーポリシーの変更を行う場合の手続

*1 同意取得：　一部のプライバシー性の高い情報については、原則同意を取得する（電話帳、位置情報、通信履歴等）。
*2 利用者関与：利用者がアプリによる利用者情報の利用や取得の中止を希望する場合に、その方法を記載する。

スマートフォン プライバシー イニシアティブⅡ、Ⅲ　/　スマートフォン プライバシー アウトルックⅠ～Ⅸ

電気通信事業法改正：実質的にアプリケーションガイドラインがWEBを含む電気通信役務に適用拡大され義務化

外部送信される情報の分類と対応（SPIIIより）

区分	情報の種類	情報の種類	利用者による変更可能性	個人識別性等
第三者に関する情報	電話帳 で管理されるデータ	氏名、電話番号、メールアドレス等	×～△	電話帳には一般に氏名、電話番号等が登録されることが多く、個人識別性を有している場合が多い。
利用者の識別に係る情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、電話番号等の情報や、クレジットカード番号等の個人信用情報等	×～△	契約者情報には一般に氏名、住所等が含まれており、個人識別性を有している場合が多い。
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報	△～○ 利用者が必要に応じて変更・修正を行うことが可能	・ログインのための識別情報は変更可能な場合も有り。 ・ログインのための識別情報は、氏名等個人識別性を有する場合もあり、単なる数字や記号等で単体では個人識別性を有さない場合もある。
	クッキー技術を用いて生成された識別情報	ウェブサイト訪問時、ウェブブラウザを通じ一時的に PC に書込み記録されたデータ等	○ 利用者が必要に応じて削除することが可能	・利用者がウェブブラウザ上で削除やオプトアウトを行うことが可能。 ・単体では個人識別性を有しないが、発行元等において他情報と照合し個人識別性を有する場合がある。
業界及びプラットフォーム事業者の自主規制により、（適用等除外でない限り）取得、利用しない	**契約者・端末固有 ID**	**OSが生成するID（Android ID）、独自端末識別番号（UDID）、加入者識別 ID（IMSI）、ICカード識別番号（ICCID）、端末識別ID（IMEI）、MACアドレス等**	**× 端末交換や契約変更をしない限り変更が困難**	**・スマートフォンの OS やシステムプログラム、SIMカード、端末そのもの等に割り振られ管理される。利用者は端末交換や契約変更をしない限り変更困難。 ・単体では個人識別性を有しない。他の情報と容易に照合できる場合、個人識別性を獲得する。 ・同一 ID に紐付けて行動履歴や位置情報を集積する場合、プライバシー上の懸念が指摘される。**
	広告 ID	IDFA（Identification For Advertisers）、AdID（Advertising ID）	○ 利用者が必要に応じて変更・修正を行うことが可能	・単体では個人識別性を有しない。他の情報と容易に照合できる場合、個人識別性を獲得する可能性がある。 ・利用者が OS の設定でオプトアウトを行うことが可能。
通信サービス上の行動履歴や利用者の状態に関する情報	通信履歴	通話内容・履歴、メール内容・送受信履歴	×～△ 端末や電気通信事業者のサーバーにおいて管理	・通信相手、記録の性質等により個人識別性を有する場合がある。 ・電気通信事業者の取扱い中のものは通信の秘密の保護の対象。 ・通信履歴はプライバシー上の懸念が指摘される。
	ウェブページ上の行動履歴	利用者のウェブページ上における閲覧履歴、購買履歴、検索履歴等の行動履歴	**×～△ 端末やウェブページ管理者、アプリケーション提供者等のサーバーにおいて管理**	**・利用者の行動履歴や状態に関する情報については、内容・利用目的等によりプライバシー上の懸念が指摘される。 ・相当程度長期間にわたり時系列に蓄積された場合等、態様によって個人が推定可能になる可能性がある。**
	アプリケーションの利用履歴等	アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等		
	位置情報	**GPS 機器によって計測される位置情報、基地局に送信される位置登録情報**		
	写真・動画等	スマートフォン等で撮影された写真、動画		・内容、利用目的等によりプライバシー上の懸念がある。 ・個人が判別できる写真・動画等は、個人情報に該当する。

電気通信事業法改正の経緯

プラットフォーム事業者が大量の利用者情報を活用してサービスを提供していることを踏まえ、利用者情報の適切な取扱いの確保の在り方等について検討

プラットフォームサービスに関する研究会
（平成30年10月）

※現在はフェイクニュース、
誹謗中傷についても検討

トラストサービス検討WG

（デジタル庁）
データ戦略推進WG
トラストを確保したDX推進SWG

（内閣官房デジタル市場競争本部）
デジタル広告市場の競争評価報告書

プラットフォームサービスに係る利用者情報の取扱いに関するWG

1．個人情報保護法改正に合わせたガイドラインの改定
（2022年4月施行）

2．利用者情報の取扱いに関わる電気通信事業法の改正に向けた検討
→外部送信規制

LINEによる中国でのデータ処理問題
（経済安全保障）

電気通信事業におけるガバナンス検討会

電気通信事業法の改正
2023年6月施行

電気通信事業法改正の要点

適用除外の範囲見直し

↓

電気通信事業法で規制することが出来る範囲を拡大

利用者の利益に及ぼす影響が大きいもの
（特定利用者情報）

↓

大手プラットフォームに対する規制

義務化：透明性確保とｱｶｳﾝﾀﾋﾞﾘﾃｨの強化

情報取扱規程の届出
情報取扱方針の公表
毎年自己評価し規定と方針を更新
特定利用者情報統括管理者の選任と届出

利用者の利益に及ぼす影響が少なくないもの

↓

利用者情報の外部送信に対する規制

義務化：通知または公表、同意、オプトアウトのいずれか

①利用者の影響に及ぼす影響が少なくない電気通信役務
②利用者に通知し又は容易に知りうる状態に置く際に満たすべき要件
③利用者に通知し又は容易に知りうる状態に置くべき事項
④オプトアウト措置の際に利用者が容易に知りうる状態に置く事項
⑤利用者が電気通信役務を利用する際に送信をすることが必要な情報

電気通信事業ガバナンス検討会
特定利用者情報の適正な取扱いに関するWG
（総務省総合通信基盤局電気通信事業部事業政策課）

ﾌﾟﾗｯﾄﾌｫｰﾑｻｰﾋﾞｽに関する研究会
ﾌﾟﾗｯﾄﾌｫｰﾑｻｰﾋﾞｽに係る利用者情報の取扱いに関するWG
（総務省総合通信基盤局電気通信事業部消費者行政第二課）

電気通信事業法の改正とプラットフォーム規制

オンラインにおけるプライバシー保護の法制度が日本の「個人情報保護法」の範疇を超える

プラットフォーム事業者の規制がプラットフォーム利用者へ影響を与える

デジタルプラットフォーム規制

1. デジタルプラットフォーム透明化法
EC/アプリのマーケットプレイス、広告

2. モバイルエコシステム
Apple、Googleのアプリマーケット開放
（モバイル・エコシステムに関する競争評価中間報告」デジタル市場競争本部）

3. 海外の法規制への対応
（欧州）GDPR、DSA、DMA等
（米国）CCPA、CPRA、FTCの規制等

電気通信事業法の改正

個人情報保護法以外の大規模なプライバシー保護の法制度

オンライン事業の大半が対象

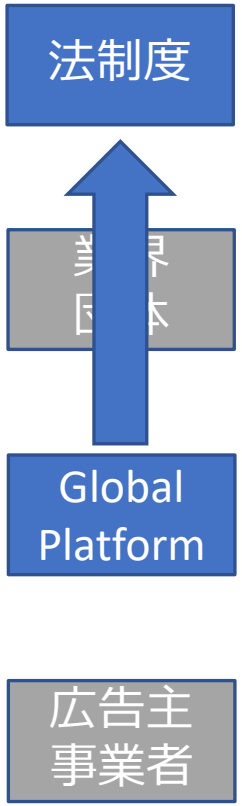
これまでの法規制対応
- 個人情報取得は通知・または公表
- 個人情報以外の利用者情報は自主規制

2023年6月～（改正電通法対象事業者）
- 個人情報以外の利用者情報についても通知/公表 or 同意 or オプトアウト

アプリ及び海外対応
- アプリ：プラットフォーム対応
- 海外：各国・地域の法規制に対応

（参考）Global Platformの動向

欧米の最も厳しい法制度（GDPR、CCPA/CPRA等）に対応するため
自主規制とこれを実現するためのソリューションを開発



Apple

iOS 14.5(Mobile)：プライバシー保護機能の強化（ATT：App Tracking Transparency）により、**広告ID（IDFA：Identifier For Advertising）を利用する場合にはユーザー同意が必須**となる

Safari(PC/Mobile)：ITP(Intelligent Tracking Prevention)により**3rd party cookieをはじめクロスサイトトラッキングをブロック。**1st party cookieについても制限有（有効期限等）

App Store(Mobile)：アプリケーションによって収集するデータの詳細な取得・用途の開示を義務付け

Private Relay：デバイスからのトラフィックを暗号化し2つのインターネットリレーを通じて送信

Google

Chrome(PC/Mobile)：3rd party cookieの段階的に廃止し、自社の広告商品では**ユーザーレベルIDを採用しない**

Google Play(Mobile)：規約の改定により徐々に透明性と同意に関する規制が強化。広告・分析利用は広告ID以外では禁止、また個人を特定できるまたは永続的なIDとの関連付けには同意が必須

Web Browserのすべてで3rd party cookieは利用できなくなる
Mobile Applicationでは、Platformが用意する識別子以外は禁止

（参考）EUの新たな規制

デジタル政策	データ政策	プライバシー保護
	デジタル政策のもと、プライバシーを保護しつつ自由で公正なデータ流通を活性化させる政策	
Digital Agenda for Europe（2010）		
欧州デジタル単一市場戦略（2015）		一般データ保護規則（2016）
欧州を単一市場として統一し、制度の共通化を図る産業政策 ↓ データ政策のベース	非個人データ規則（2018）	
	オープンデータ指令（2019）	
	欧州データ戦略（2020）	
Europe's Digital Decade（2021）		
デジタルサービス法 デジタル市場法（2022）	データガバナンス法（2022）	
	データ法（案）	**ePrivacy規則（案）**

※枠囲みは法令の公布年度
※法令は発表された複数の政策や戦略に基づくもので、相互に関連性があるため、個々の法令のみを注視するのではなく、全体を俯瞰して対応を検討することが求められる

●デジタルサービス法

2022年11月発効、主要適用2024年2月

オンライン上の仲介サービスを提供する全事業者を対象として透明性や事業者の説明責任を強化し、利用者の基本的権利を保護するもので、仲介事業者をサービスと規模に応じて分類し、影響の大きさに応じて規制のルールを強化

※EU においてオンライン事業を展開している場合は、この規則を順守しなければならない

●ePrivacy規則（案）

電子通信サービス分野におけるGDPRを補完する2次法。個人データであるか否かを問わず、電子通信および端末機器上の情報の完全性が対象。原則取得禁止。（一定の例外を除き同意取得が必要）

※今回の改正電気通信事業法に近似だがより厳しい「同意」が前提

DFFT(Data Free Flow with Trust)の実現を目指すと、これらの潮流と整合性をとる必要があり、すでに各省庁で検討が進められている

（参考）米国の新たな規制

実態として機能している州法

●**CCPA**（カリフォルニア州消費者プライバシー法：California Consumer Privacy Act）:2020年1月施行
カリフォルニア州の消費者の個人データを取り扱うカリフォルニアで事業を行う法人に対する規制。
消費者にプライバシーの権利を与え、企業に適切な管理を求める。

●**CPRA**（カリフォルニア州プライバシー権法：California Privacy Rights Act）：2023年1月施行
CCPAを修正し、消費者の権利をさらに拡大、企業の義務を強化。

※GDPRと異なり、個人データの取得はオプトイン（同意取得）ではなく、オプトアウトが義務化され、消費者の開示・訂正・削除等の請求権、企業の透明化（通知義務等）、安全管理措置の義務化等が中心。

※2023年施行（予定）のその他州法：バージニア州、コロラド州、コネチカット州、ユタ州

州法を塗り替える可能性のある連邦法

●**ADPPA**（米国データプライバシー保護法：The American Data Privacy and Protection Act）
2022年7月に超党派法案として米下院のエネルギー・商業委員会にて可決され、下院本会議に送られたが、今会期中には成立せず。今後の見通しは不明。

規制当局(FTC)による新たな規制

●**商業的監視(Commercial Surveillance)及びデータセキュリティ(Data Security)に関する規則**
2022年8月、規則制定に向けた、Advance Notice of Proposed Rulemakingを公表。

商業的監視：消費者のデータ及びそこから直接派生する情報の収集、集約、分析、保持、移転又はそれによる収益化
データセキュリティ：データ侵害リスクの軽減、データ管理・保持、データ最小化、及び侵害の通知・開示のプラクティス

商業的監視社会において消費者を適切に保護するために、個別の事案ごとの対処では足りず、プライバシーとデータセキュリティについて企業が遵守すべき要件を明確化する

いずれも、透明性とアカウンタビリティの確保が中心で、オプトアウトの必須化が含まれる

プライバシーガバナンス

フレームの関係性：個人情報、プライバシー、ガバナンス。。。

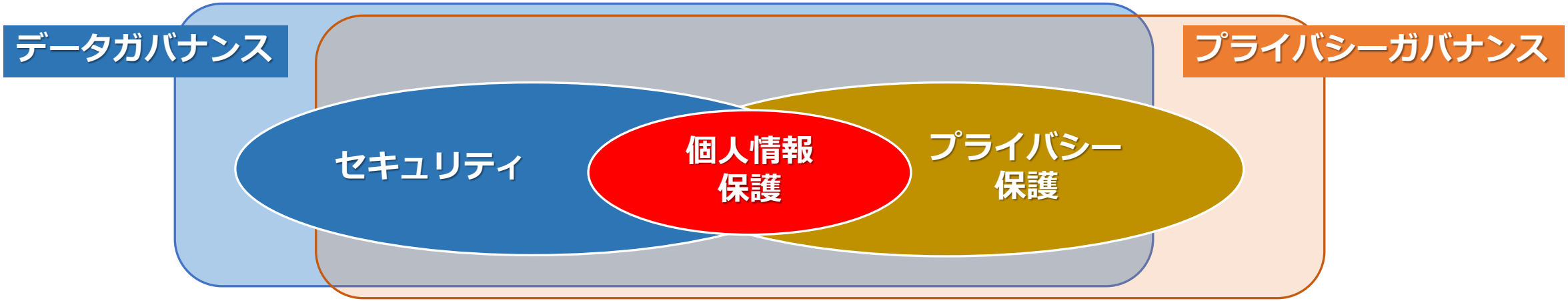
データガバナンス

データ資産の管理を統制(計画・監視・執行)すること。
具体的には、データの生成・蓄積・公開・利用・廃棄に係わる管理の在り方を規定し、統制すること。

プライバシーガバナンス

プライバシー問題の適切なリスク管理と信頼の確保による企業価値の向上に向けて、経営者が積極的にプライバシー問題への取組にコミットし、組織全体でプライバシー問題に取り組むための体制を構築し、それを機能させること。

ガバナンス ＝ 統治、統制



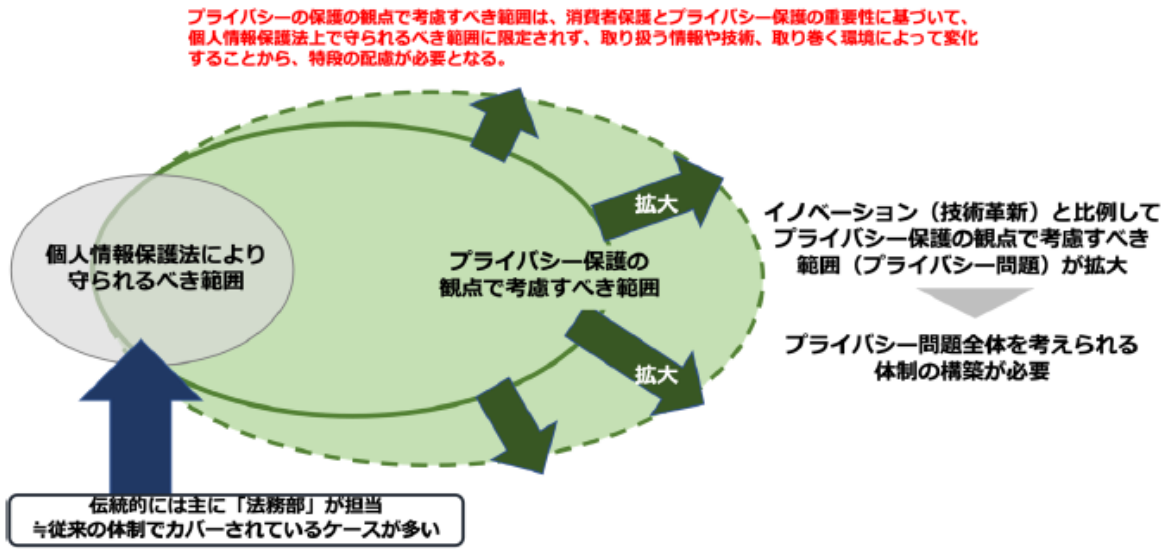
重なる部分も多いがはみ出しているところも少なくない　→　ガバナンスを効かせることで保護する

プライバシー対応に関する企業内ガバナンスの必要性

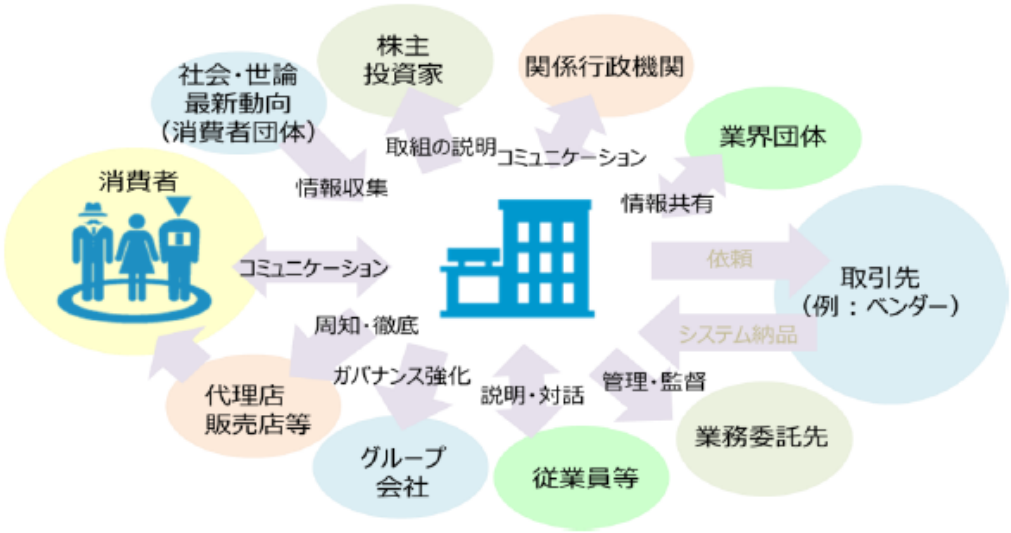
DX時代における企業のプライバシーガバナンスブックより

- 昨今ビジネスモデルの変革や技術革新が著しく、イノベーションの中心的役割を担うDX企業は、**イノベーションから生じる様々なリスクの低減を、自ら図っていかなければならない。**
- プライバシーに関する問題について、個人情報保護法を遵守しているか否か（コンプライアンス）の点を中心に検討されることが多かった。しかし法令を遵守していても、本人への差別、不利益、不安を与えるとの点から、**批判を避けきれず炎上し、企業の存続に関わるような問題として顕在化**するケースも見られる。
- 企業は、**プライバシーに関する問題について能動的に対応し**、消費者やステークホルダーに対して、積極的に説明責任を果たし、**社会からの信頼を獲得する**ことが必要である。経営者は、プライバシー問題の向き合い方について、経営戦略として捉えることで、企業価値向上につながるといえる。

プライバシー保護の観点で考慮すべき範囲と体制構築の必要性



ステークホルダーとのコミュニケーション



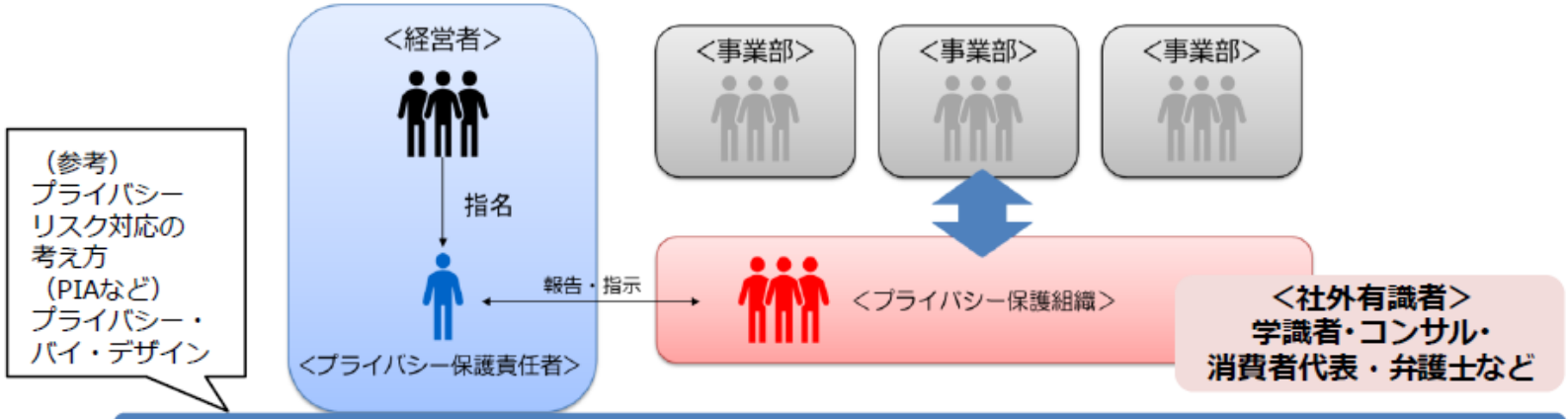
DX時代における企業のプライバシーガバナンスガイドブックの概要

経営者が取り組むべき3要件

要件１：プライバシーガバナンスに係る姿勢の明文化
経営戦略上の重要課題として、プライバシーに係る基本的考え方や姿勢を明文化し、組織内外へ知らしめる。経営者には、明文化した内容に基づいた実施についてアカウンタビリティを確保することが求められる。

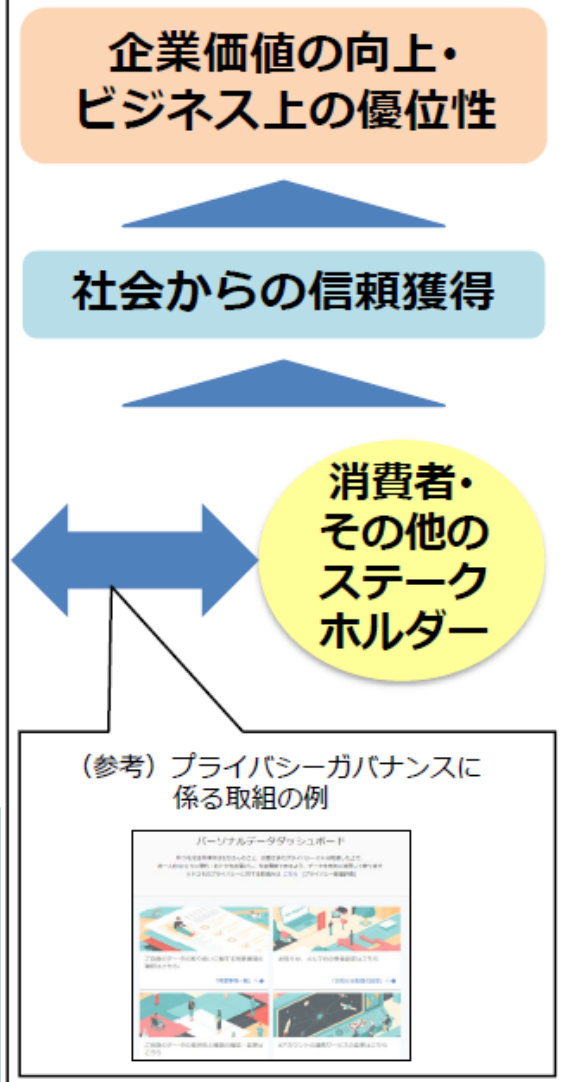
要件２：プライバシー保護責任者の指名
組織全体のプライバシー問題への対応の責任者を指名し、権限と責任の両方を与える。

要件３：プライバシーへの取組に対するリソースの投入
必要十分な経営資源（ヒト・モノ・カネ）を漸次投入し、体制の構築、人材の配置・育成・確保等を行う。



プライバシーガバナンスの重要項目

1. **体制の構築**（内部統制、プライバシー保護組織の設置、社外有識者との連携）
2. **運用ルールの策定と周知**（運用を徹底するためのルールを策定、組織内への周知）
3. **企業内のプライバシーに係る文化の醸成**（個々の従業員がプライバシー意識を持つよう企業文化を醸成）
4. **消費者とのコミュニケーション**（組織の取組について普及・広報、消費者と継続的にコミュニケーション）
5. **その他のステークホルダーとのコミュニケーション**
（ビジネスパートナー、グループ企業等、投資家・株主、行政機関、業界団体、従業員等とのコミュニケーション）

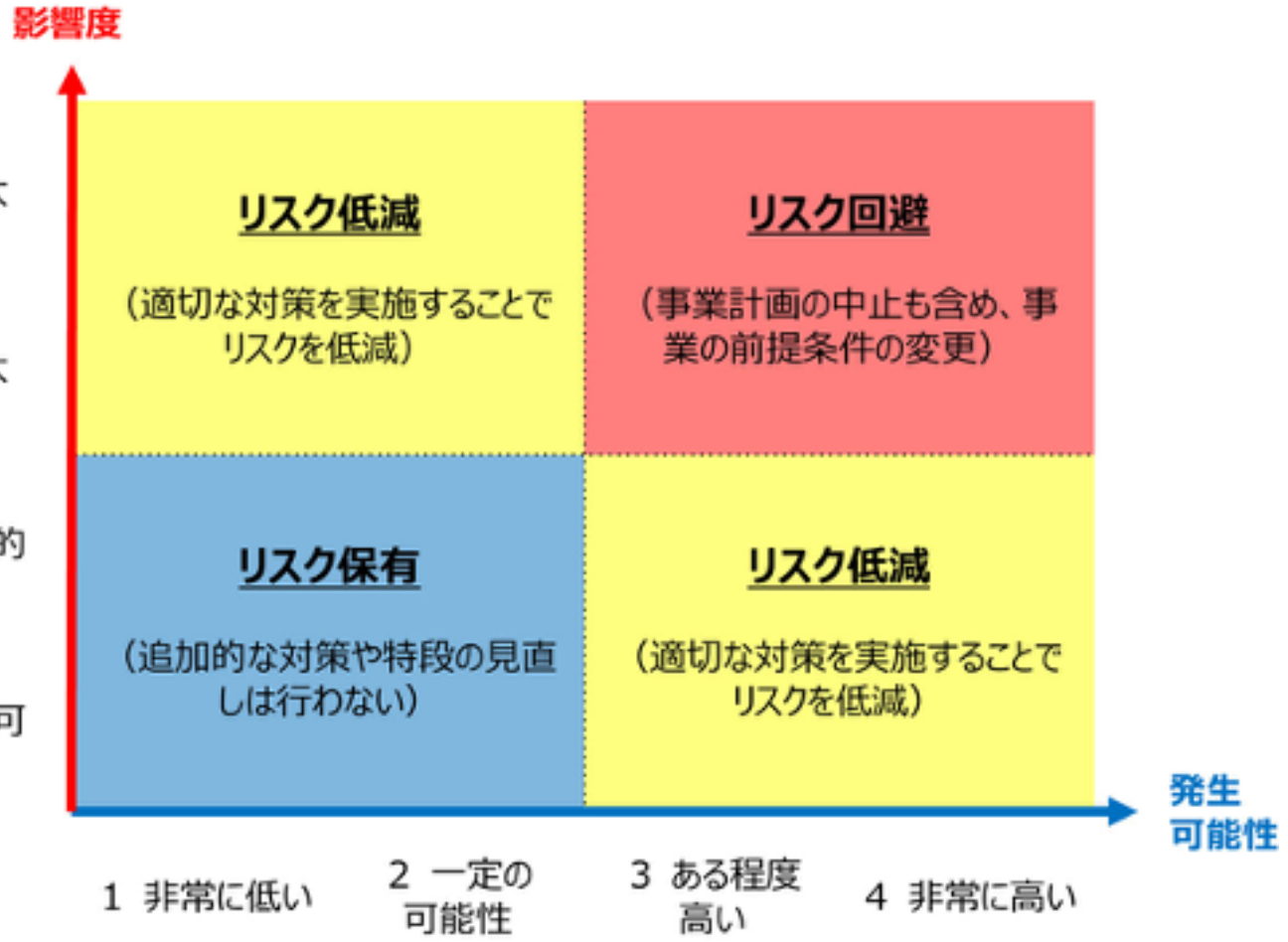


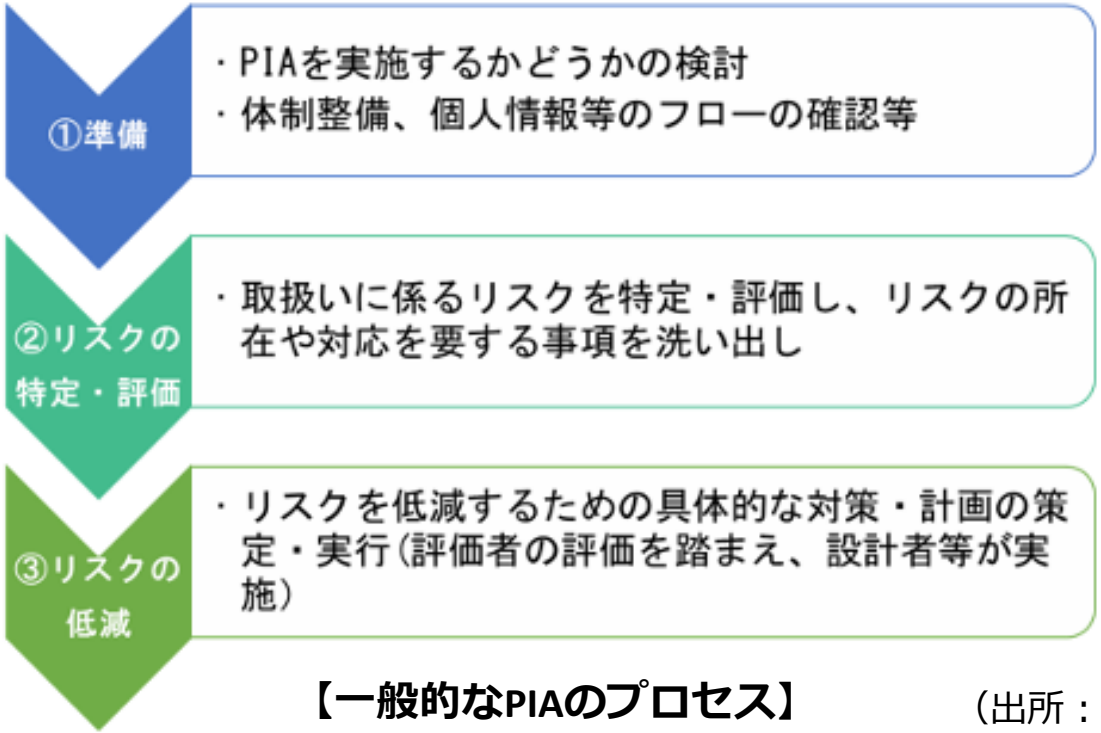
出典「DX時代における企業のプライバシーガバナンスブック」

PIA（Privacy Impact Assessment）

プライバシー影響評価（PIA）とは、**個人情報及びプライバシーに係るリスク分析、評価、対応検討を行う手法**である。
ISO/IEC 29134:2017は、PIAの実施プロセス及びPIA報告書の構成と内容についてのガイドラインを提供。2021年1月JIS X 9251:2021としてJIS規格になっている。

【プライバシーリスク対応方針の例】





【一般的なPIAのプロセス】

（出所：個人情報保護委員会「PIAの取組の促進について」）

ご清聴ありがとうございました