

第2回 利用者情報に関するWG

モバイル・コンテンツ業界における プライバシー保護の取り組み

一般社団法人 モバイル・コンテンツ・フォーラム
常務理事 寺田真治

+
•
0

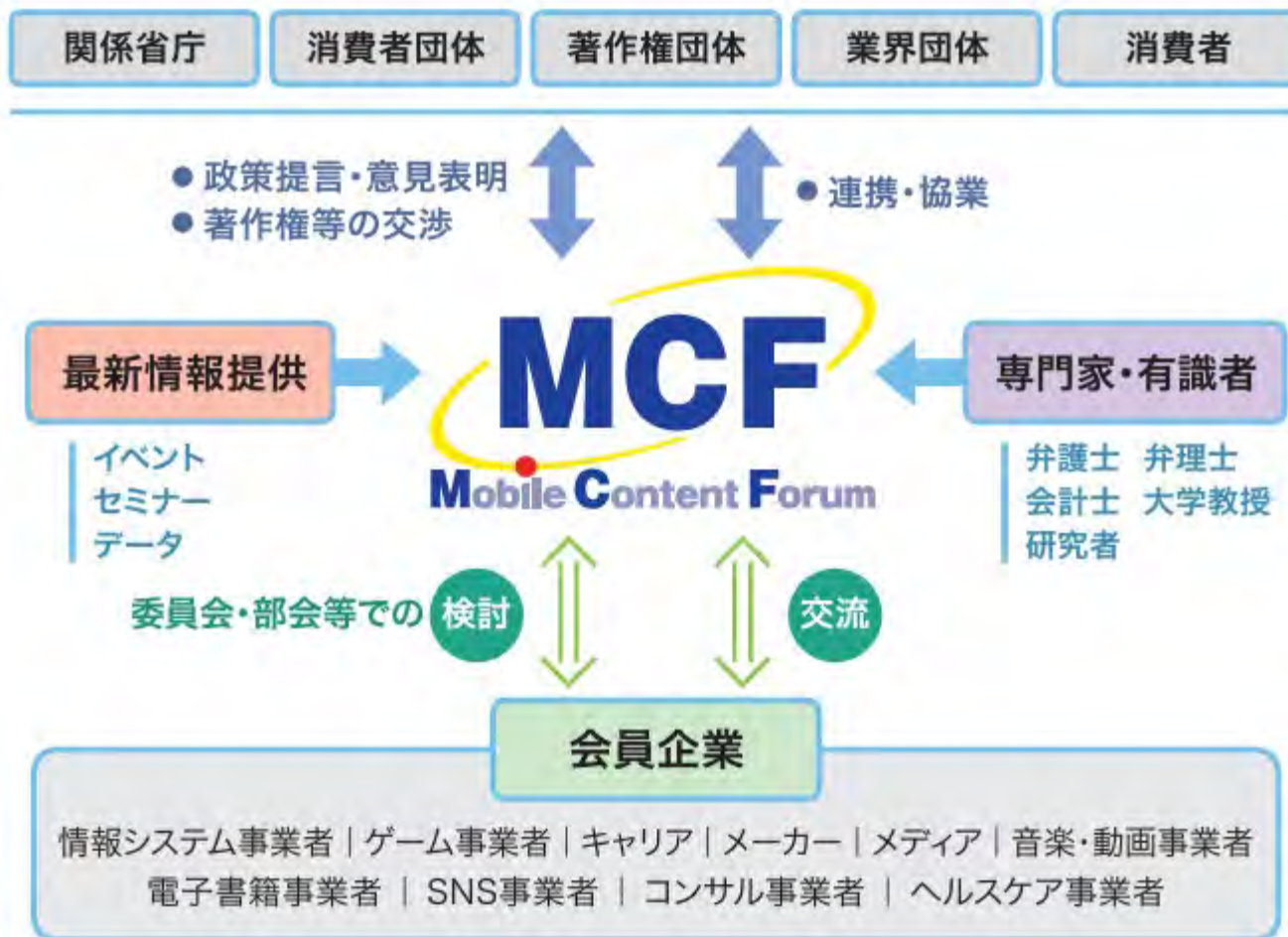
モバイル・コンテンツ・フォーラム (MCF)

MCFのビジョン

- デジタル化、インターネット化、グローバル化による事業展開を推進し、日本社会の幸福な未来を実現する。

MCFのミッション

- デジタルコンテンツサービス関連産業の健全な発展のため、関連する事業者、プラットフォーム、消費者、団体等と円滑な関係を構築し、また、海外マーケットを含めた新たな市場開拓を支援する。



MCFにおけるプライバシー保護に関する取り組みの概要



MCFはプライバシーマーク審査機関です。

MCF会員を対象として、プライバシーマークの新規付与申請、更新申請を受け付けております。

認定個人情報保護団体

ビックデータ、IoT、人工知能、ヘルスケア分野等の次世代ビジネスも見据えた革新的な業界個人情報保護指針の策定を目指します。

ガイドライン等の策定

1. モバイルコンテンツ関連事業者のための個人情報保護ガイドライン

当団体がプライバシーマークの審査を行う際に、本ガイドラインの遵守を条件とするもの。それ以外のモバイルコンテンツ関連事業者においても、本ガイドラインの遵守を推奨する。

2. モバイルコンテンツ関連事業における個人情報保護指針

法の定めに従い当団体の対象事業者が遵守・励行する事項を定めるとともに、当団体が認定個人情報保護団体として実施すべき責務と役割を推進するための事項を定めたもの。

3. スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン

スマートフォンのアプリケーションを開発もしくは提供する事業者、個人等が、利用者の端末内情報の取り扱いに関して、利用者にわかりやすく適切に「アプリケーション・プライバシーポリシー」を作成し、掲示できるようにとりまとめたもの。

1. モバイルコンテンツ関連事業者のための個人情報保護ガイドライン

当団体がプライバシーマークの審査を行う際に、本ガイドラインの遵守を条件とするもの。それ以外のモバイルコンテンツ関連事業者においても、本ガイドラインの遵守を推奨している。

https://www.mcf.or.jp/mcfxswp/wp-content/uploads/2023/11/guideline_for_mobilecontent_v4.pdf

当該ガイドラインのうち、すべてのアプリケーション配信事業者において対応を必要とする事項（利用者情報及びアプリケーション・プライバシーポリシー）は**MCF以外でもプライバシーマークの審査を行う際に確認**を行っている。

（スマートフォン等のアプリケーション配信事業者対象）利用者情報の取扱い、アプリケーション・プライバシーポリシーについて

https://privacymark.jp/system/operation/spapp/pdf/spapp_kaisetsu_220428.pdf

- 特定の個人を識別できるとは言えない**利用者情報**であっても、蓄積などを通じて特定の個人を識別できる場合がありえることから、**個人情報と同等と捉える**。
 - **個人情報を管理するための台帳に、利用者情報を特定すること**
利用者情報の個人情報保護リスクを特定すること
対策については、個人情報と同様の対応
- 事業者毎の「個人情報保護指針」とアプリケーション毎の「アプリケーション・プライバシーポリシー」とは異なり、**分けて公表することが望ましい**。
 - **利用者情報を取得する場合、あらかじめアプリケーション・プライバシーポリシーを文書化した情報を、利用者に通知または公表すること**

2. モバイルコンテンツ関連事業における個人情報保護指針

法の定めに従い当団体の対象事業者が遵守・励行する事項を定めるとともに、当団体が認定個人情報保護団体として実施すべき責務と役割を推進するための事項を定めたもの。

https://www.mcf.or.jp/mcfxswp/wp-content/uploads/2023/07/GuidelinesforPI_MCF20230711.pdf

個人情報保護法を遵守する上での個人情報保護指針に加えて、モバイルコンテンツ関連事業において遵守すべき改正電気通信事業法に基づく指針を追加

第1章：個人情報保護法におけるガイドラインを含む電気通信事業における個人情報等のガイドラインに基づく指針

第2章：電気通信事業法において定められた、ブラウザその他のソフトウェアにより、利用者の電気通信設備を送信先とする**情報送信指令通信を行おうとする者への追加事項**

3. スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン

第1部 充足すべき必要要件

概要

個人情報保護に関する法律についてのガイドライン

https://www.mcf.or.jp/mcfxswp/wp-content/uploads/2023/09/mcf_spappp_guidline.pdf

通則編

外国にある第三者への提供編

仮名加工情報・匿名加工情報編

電気通信事業における個人情報保護に関するガイドラインの解説

プライバシーポリシー

位置情報

外部送信に係る利用者に関する情報の取扱い

(参考) スマートフォン プライバシー イニシアティブⅢ

スマートフォン利用者情報取扱指針

総則

アプリケーション提供者等における取組

法やガイドライン等において通知や公表すべきとされている事項が、どこに記載されているかを示す

第2部 実装にあたっての推奨要件

1. 同意を必要とするものについて
2. アプリケーション・プライバシーポリシーの変更について
3. 同意が得られなかった場合、オプトアウトした場合に制限される事項について
4. 取得した利用者情報の取扱いについて
5. 必要要件以外の同意取得について
6. 本人の知り得る状態について
7. 日本語以外での説明に対する対応について
8. 既存のアプリケーションの本ガイドラインへの対応について

法やガイドライン等以外で、プライバシーポリシーを実装するさいに留意すべき事項や推奨される事項を上乗せ

3部 アプリケーション・プライバシーポリシーのモデル案

(参考) アプリケーション・プライバシーポリシー 概要案

(参考) チェックシート

(参考) 実装にあたっての推奨要件 (1)

1. 同意を必要とするものについて

同意を必要とするものについては、同意の取得の際だけではなく、透明性の確保、説明責任の観点からも、アプリケーション・プライバシーポリシーにも記載することを推奨

2. アプリケーション・プライバシーポリシーの変更について

- ・利用者情報においても、利用者が想定することが困難であると認められる利用目的の変更を行う場合には、改めて本人の同意を得ることを推奨
- ・履歴を掲示すると同時に過去のアプリケーション・プライバシーポリシーを閲覧できるようにすることも有用

3. 同意が得られなかった場合、オプトアウトした場合に制限される事項について

アプリケーションやサービスの利用が制限される場合は、その旨を説明することを推奨

4. 取得した利用者情報の取扱いについて

- ・アプリケーションをアンインストールせずに端末の買い替えをした場合、退会手続きを経ずにアプリケーションを削除した場合、長期間利用せずに放置した等で利用者の明確な意思表示がなかった場合の対応
- ・取得した利用者情報の保存期間や削除の方針をあらかじめ通知または公表することを推奨

(参考) 実装にあたっての推奨要件 (2)

5. 必要要件以外の同意取得について

「アプリケーション・プライバシーポリシー」および「契約者・端末固有ID等の取得」については同意を取得することを推奨

6. 本人の知り得る状態について

概要や一部をプライバシーポリシーに掲載し、残りを本人の求めに応じて遅滞なく回答を行うといった対応も可能だが、可能な限り具体的な内容をプライバシーポリシーに記載することを推奨

7. 日本語以外での説明に対する対応について

海外の情報収集モジュール提供者に日本語での情報提供を求めることを推奨

8. 既存のアプリケーションの本ガイドラインへの対応について

本ガイドラインへ可能な限り早く準拠すること

※アプリケーションの改修が必要な場合は、改修計画が着実に実行される体制を整備することを推奨

※改修中にプラポリと実際の運用との間に矛盾が起こらないように注意

(参考) プラポリモデル案におけるMCF推奨事項の例

- 法令上の義務やSPIの推奨事項だけでなく、グローバルの規制や消費者の意向に鑑みて、利用者情報をより丁寧に取り扱うことを求めている例

【MCF推奨】本条は、保有個人データの取扱いに関する公表事項として求められている事項ですが、**保有個人データ以外の情報の取扱いも同様であるべき**と考えられます。事業がアプリケーション中心の場合は企業のプライバシーポリシー閲覧までの導線が遠くなるため、アプリケーションのプライバシーポリシーに記載しておくことも有用と考えられます。

- 国際標準、JIS規格を積極的に取り入れることを意識した例。

【MCF推奨】取得する情報については、**利用者にとって重要と考えられるものから順に記載**することを推奨します。

- その他、個人情報（個人データ）と利用者情報の相違点を各所で指摘

※MCF会員企業がプラポリに取り入れることで、コピペする他企業へも広がることを期待している側面もある。

4. SPI改定に向けた要望

1. 通知又は公表すべき事項が、法令やガイドラインにおいて各所に散在していて分かりにくく、個人情報保護法と電気通信事業法で求められている内容も微妙に異なるため整理していただきたい。
2. MCFのアプリケーション・プライバシーポリシーにおいて推奨事項として追加している内容は、主に利用者の理解を助けるためのものであり、SPIにおいても、利用者視点を重視して追加することを検討していただきたい。
3. スマートフォン以外のスマートデバイス（タブレット、スマートウォッチ、スマートスピーカー、スマート家電、コネクテッドカー、その他IoTデバイス等）について、適用の可能性について検討していただきたい。

※スマートデバイスが非対象だと、規律の公平性の観点からも問題があるのではないかと。ただし、相違点もあるため、まずは調査・確認が必要。

4. 海外の規制、国際標準の動向に沿うことを検討していただきたい。

※例示等が多いのは事業者にとってはありがたい面もあるが、チェックシート型になってしまうことは好ましくない。リスク・マネジメントの考え方をベースとする「要求事項」としてのまとめ方が望ましい。

※グローバルで通用する用語（法令上難しい場合には併記）、ISO等の参照等。

(参考) プライバシー保護に関する国際標準規格

ISO/IEC 27001 (JIS Q 27001) : 情報セキュリティマネジメントシステム (ISMS)

ISO/IEC 27701 (JIS Q 27701) : プライバシー情報マネジメントのための拡張

※27701は、ISMSの要求事項にプライバシーを保護するための要求事項とガイドラインを追加したもの

※GDPRとのマッピングを示した付属書がある

ISO/IEC 29134 (JIS X 9251) : プライバシー影響評価のためのガイドライン (PIA)

ISO/IEC 29184 (JIS X 9252) : オンラインにおけるプライバシーに関する通知及び同意

※日本が提案し、EUのGDPR等各国の要件を追加し策定

※付属書A (参考) PC及びスマートフォンからPII主体の同意を得る場合のユーザーインターフェースの例

付属書B (参考) 同意領収書又は同意記録書の例

※同意：公正で、証明可能で透明性があり、曖昧でなく、かつPII主体が取消し（撤回）可能な方法でPII主体から確実に同意を得る。

PII主体がその処理に関して、自由に、具体的に、かつ、理解に基づいた同意を与えられるように、十分な詳細を提供しなければならない。同意は、簡単にアクセス、修正及び／又は撤回可能なようにしなければならない。

+
•
○

ご清聴ありがとうございました