# Ａｎｄｒｏｉｄアプリ ＤＲＭガイドライン

## ～　コンテンツプロバイダーにおける
## アプリ開発・アプリ市場導入の観点から　～

２０１２年５月１５日

一般社団法人モバイル・コンテンツ・フォーラム

はじめに

携帯電話でのコンテンツビジネスが開始され、早１２年となりました。携帯電話は通信・通話といったシンプルな機能から、ネット接続可能な高機能へと進化していきました。普及台数は急速に増加し、国民一人当たり約一台の時代になりました。携帯電話の高機能化は、様々なコンテンツサービスが提供できる環境を整えることとなり、コンテンツプロバイダと呼ばれる事業者を生みだしました。そして、我が国において発展した産業の一つとなるコンテンツ市場を形成するに至りました。

コンテンツサービスは、携帯電話の機能や通信回線容量とともに変化・拡大してきました。白黒の待ち受け画像､単音の着信メロディ､ＷＥＢブラウザを駆使したシンプルなゲーム等は、その後の液晶カラー化、和音化、ファイル・アプリケーションのダウンロード化等の高機能化と通信回線容量大幅増等の複合的要因により、良質な画像や動画、高音質の着うた、Ｊａｖａ等を使用したゲームアプリに変化し、取り扱えるアプリケーションは機能等に応じて急激に拡大していきました。

このような急激な発展が可能となった背景には、通信キャリアの存在と支援があったことを忘れてはなりません。例えば事業者は、通信キャリアからコンテンツプラットフォームと呼ばれるコンテンツ配信の為の様々な技術的仕組み及びツール等の提供を受けてきました。音楽系コンテンツ（着信メロディ・着うた）であれば、コンバーターと呼ばれるツールが一事例でしょう。データフォーマットにより容易にデータ作成が可能となり、ＤＲＭ（Degital Rights Management）の仕組み等も同時に提供されるため、著作権侵害行為からコンテンツビジネスを保護できるものとなっていました。また、コンテンツプラットフォーム上のサービスルールにより、大よその著作権団体等と調整した利用条件が適用され、個別交渉することなく、コンテンツビジネスを容易に開始することができました。このような通信キャリアの存在と支援といった背景のもと、我が国のコンテンツ産業とその市場は、形成・発展してきたのです。

近年、Ａｎｄｒｏｉｄ等スマートフォンと総称される新しいオープンプラットフォームでの仕組みでコンテンツを提供するといった、大きな環境変化が起こりました。この環境変化に対して、当初、多くの事業者が戸惑いました。なぜならば、今までのように通信キャリアによって用意・提供されてきたコンテンツ配信の仕組みがないためです。

特にＤＲＭについては、ほとんど意識をしなくてもコンテンツ配信が行える環境に事業者が慣れてしまっていた状況がありました。Ａｎｄｒｏｉｄ等スマートフォンで、従前同様のコンテンツサービスを提供するには、コンテンツの種類によって、知識・技術の習得、時間、莫大な費用等、大きな負担を強いられることになりました。

環境に依存していた事業者はじめ関係者においては、大いに反省し、今後の発展に向けて、どのように解決をするべきかを真剣に考える良い機会であると捉えたいと思います。

当団体では、一部ではありますがＡｎｄｒｏｉｄ用のコンテンツ配信において重要となるＤＲＭ関連についてのガイドラインを、以下に取りまとめました。今後のＡｎｄｒｏｉｄ用コンテンツの仕組みとして貢献できれば幸いであります。

本稿をまとめるにあたり、ご協力いただきました企業の皆様、知財・著作権委員会ならびにモバイル著作権部会の皆様、監修を引き受けてくださった森・濱田松本法律事務所パートナー弁護士 飯田耕一郎先生、関係者の皆様に厚く御礼申し上げます。

２０１２年５月１５日

一般社団法人モバイル・コンテンツ・フォーラム　常務理事　佐藤　慎吾

目次

## １．ＡｎｄｒｏｉｄアプリＤＲＭガイドラインの利用にあたって

### （１）目的

本ガイドラインは、オープンプラットフォームであるＡｎｄｒｏｉｄＯＳにおいて、安全にビジネスを展開する上で必要となるＤＲＭ（Degital Rights Management：デジタルコンテンツの著作権を保護する技術等の総称）技術について検討し、ビジネスにおいてＤＲＭ技術を取り扱う上での一助となることを目的としています。

### （２）対象

音楽・動画・映像・画像・ゲームなど（総称してコンテンツ）の配信をするコンテンツプロバイダー（以下、ＣＰという）のほか、著作権者等の権利者など、モバイルコンテンツビジネスをされる方を対象にしております。

## ２．Ａｎｄｒｏｉｄアプリをとりまく環境

従来、ＣＰは、携帯電話を通じたコンテンツサービスの実施において、携帯電話通信サービス会社（以下、キャリアという）が指定したＤＲＭを施せば、基本的なセキュリティ対応ができていました。そのため、ＣＰによる携帯電話を通じたコンテンツサービス市場への参入は容易にそして安心して行うことができました。

しかし、近年、従来の携帯電話からスマートフォンへと携帯端末市場は大きくシェアが変化しました。この市場の変化により、コンテンツサービスは、オープンマーケットで一気にグローバル化しました。市場で大きいシェアを有することとなったＡｎｄｒｏｉｄＯＳ端末においては、ＣＰがＡｎｄｒｏｉｄアプリを開発・市場導入するにあたって、独自にＤＲＭ等のセキュリティを施すか判断し、そのセキュリティレベルを設定し、そして、セキュリティにかかる初期費用から維持費用の全てを負担する状況となりました。

従来のコンテンツサービスにおけるＤＲＭは、データファイルにのみ施すケースが多く見られました。ＡｎｄｒｏｉｄＯＳ端末においては、セキュリティの問題点を突いたマルウェアなどの問題などが急増しました。そのため、ＡｎｄｒｏｉｄＯＳ端末におけるＤＲＭ等のセキュリティを施す必要性があるとの認識が高まりました。

現状のＡｎｄｒｏｉｄ用のコンテンツサービスの主流は、アプリダウンロード型となっているため、ＤＲＭ等のセキュリティを施す場合はそのアプリに対してＤＲＭを施す必要性があります。セキュリティは、コピーコントロール、ビジネス上重要となっている個人情報を含むデータ保護、さらにはＩＤ・パスワードを主としたアクセスコントロール（ユーザーの利用時に認証を行うことでシステム利用を制御すること）の観点を考慮しなければなりません。

そこで、ＤＲＭ等セキュリティ技術についての現状を把握したところ、ＤＲＭ技術に関して、データファイルへのＤＲＭに加え、実行プログラムにＤＲＭを施さなければ、セキュリティとしては問題が生じる可能性があるということ、セキュリティレベルを上げるためには実行プログラムにＤＲＭを施す必要性が高いという状況であると考えられました。

３．ＡｎｄｒｏｉｄＯＳに対応したＤＲＭの参考項目について
（コンテンツプロバイダーがＡｎｄｒｏｉｄアプリを開発・市場導入するにあたって）

Ａｎｄｒｏｉｄアプリをとりまく環境で説明したように、ＣＰはＤＲＭなどのセキュリティを独自に検討し、実装する必要がでました。
そこで、ＣＰがＤＲＭなどのセキュリティを検討するにあたって、まずはどのような項目や要素を検討したらよいのかが、非常に重要で基礎的な事項となります。
本ガイドラインでは、ＡｎｄｒｏｉｄＯＳを対象にしたＤＲＭなどのセキュリティの検討にあたっての参考となるよう、その項目や要素を検討しました。
その結果、大項目として、サービス提供者プロフィール、技術要件、クライアントミドルウェア、ビジネス要件、契約要件といった５項目に分類をしました。さらに、項目のなかで複数の小項目等に分類をしました。
また、参考までに、項目や分類等を一覧表とした一事例を添付しています。
このような一覧表を活用することで、安全にビジネスを展開できるよう期待します。

項目Ａ．サービス提供者プロフィール
ＤＲＭ サービス提供事業者を記載します。
本ガイドラインでは、事業者を次の３タイプに分類しました。
・ＤＲＭ ベンダー：主に ＤＲＭ 技術を提供している事業者
・セキュリティベンダー： ＤＲＭ 技術を保護もしくはミドルウェアに組み込み、ＤＲＭ 技術についての安全性（セキュリティ）を提供している事業者
・ＡＳＰベンダー：特定の ＤＲＭ 技術をＡＳＰとして一元的に提供している事業者

項目Ｂ．技術要件
ＤＲＭ ベンダーが提供するＤＲＭ 技術をＣＰ等が利用する上で、必要となるシステム構成や暗号化強度をはじめ、ＤＲＭ 技術の適応範囲や対応するコンテンツ等のスペックを中心とした情報を記載します。

項目Ｃ．クライアントミドルウェア
ＤＲＭ 技術を採用して製作されたクライアントミドルウェアに対しての静的解析や動的解析などのセキュリティ対策における、当該クライアントミドルウェアが対応している状況の有無などを記載します。
本ガイドラインでは、この項目が非常に重要となるため、項目内の小項目である静的解析対策機能と動的解析対策機能の内容について説明します。

Ｃ－１　静的解析対策機能
・Ｃ－１－１　逆アセンブル対策の暗号化
逆アセンブルとは、実行ファイルを可読な形式（＝ソースコード）に戻す行為。
ｓｏファイルの暗号化は逆アセンブル阻止に最も有効な手段となります。
・Ｃ－１－２　ｓｏファイル改竄対策
クラッカーはセキュリティ除去などの目的でｓｏファイルを改竄します。
ｓｏファイル改竄を阻止するとクラッカーによる前記攻撃を防御できます。
・Ｃ－１－３　ｄｅｘファイル改竄対策
クラッカーはセキュリティ除去などの目的でｄｅｘファイルを改竄します。

ｄｅｘファイルはｓｏファイルよりも容易に改竄することができます。
ｄｅｘファイル改竄を阻止することでクラッカーによる前記攻撃が防御できます。

Ｃ－２　動的解析対策機能

・Ｃ－２－１　ルート化対策
ルート化とは、端末を管理者権限で実行できるようにする行為。
ルート化すると端末上で禁止されている行為も可能となります。
ルート化を阻止すると前記行為を防御できます。

・Ｃ－２－２　ＵＳＢデバッグ対策
ＰＣと端末をＵＳＢ接続すると、ＰＣ上でプログラムを自由にデバッグできるようになります。
ＵＳＢデバッグ接続を阻止すると前記行為を防御できます。

・Ｃ－２－３　デバッガ対策
デバッガは端末のプログラムを解析するために最も有効な手段の一つとなります。
デバッガを阻止するとプログラムの解析を防御できます。

・Ｃ－２－４　再パッケージ化対策
再パッケージ化とは、マーケットで配布されているパッケージ（ａｐｋ）を改竄して別のパッケージを作成する行為。
クラッカーは海賊版作成などの目的で再パッケージ化します。

・Ｃ－２－５　Ａｎｄｒｏｉｄ　ＳＤＫ付属エミュレータ対策
Ａｎｄｒｏｉｄ　ＳＤＫ付属エミュレータを使用することでプログラムのメモリスナップショットが可能となります。
Ａｎｄｒｏｉｄ　ＳＤＫ付属エミュレータを阻止すると前記行為を防御できます。

・Ｃ－２－６　偽ｄｅｘ対策
クラッカーは海賊版作成などの目的で正規ｄｅｘファイルを偽ｄｅｘファイルに差し替えます。
偽ｄｅｘファイルの使用を阻止すると前記行為を防御できます。

・Ｃ－２－７　一時ファイル解析対策
一時ファイルを使用するとプログラムを容易に作成できます。
一時ファイルは解析の対象になるため、その対策をすることが有効となります。

・Ｃ－２－８　実行端末のホワイトリスト化
悪意的に改造した端末（原理的には可能であるが実在は未確認）を使用するとプログラムの解析が容易になります。
ホワイトリストにより前記端末でのプログラム実行を阻止できるので安全となります。

項目Ｄ．ビジネス要件

本項目は、ＤＲＭ 技術を利用しコンテンツビジネスを行う上で、コンテンツホルダーが希望する、もしくは、コンテンツの流通上必要となる各種制限事項に対して、ＤＲＭ 技術が対応しているかを記載します。

項目Ｅ．契約要件

この項目は、ＤＲＭベンダー、セキュリティベンダー、ＡＳＰベンダーを利用する上で、ＣＰへの提供形態、システム内容、ソフトウェア、費用等の情報を記載します。

＊参考　（ＡｎｄｒｏｉｄＯＳに対応したＤＲＭについての項目一覧表の一例）
例えば、このような一覧表へアプリに実装するＤＲＭなどのセキュリティを記入し、セキュリティの内容をチェックすることなどが期待されます。

| | | | | |
|---|---|---|---|---|
| A | | | **サービス提供者プロフィール** | 記入欄 |
| A | 1 | | ベンダータイプ | |
| A | 1 | 1 | | |
| A | 2 | | サービス名称 | |
| A | 2 | 1 | サービス名称 | |
| A | 3 | | 提供社名 | |
| A | 3 | 1 | 社名 | |
| A | 3 | 2 | 所在地 | |
| A | 4 | | 特徴点:特記等 | |
| A | 4 | 1 | | |

| | | | | |
|---|---|---|---|---|
| B | | | **技術要件** | 記入欄 |
| B | 1 | | 配信システムの構成 | |
| B | 1 | 1 | WEBサーバ | |
| B | 1 | 2 | ライセンスサーバ | |
| B | 2 | | DRMの適用範囲 | |
| B | 2 | 1 | プレーヤー | |
| B | 2 | 2 | コンテンツ | |
| B | 3 | | 暗号化レベル | |
| B | 3 | 1 | コンテンツ暗号化 | |
| B | 3 | 2 | 電子署名 | |
| B | 3 | 3 | ハッシュ関数 | |
| B | 4 | | 対応OS | |
| B | 4 | 1 | android version | |
| B | 5 | | 認証方法 | |
| B | 5 | 1 | 組み合わせ | |
| B | 5 | 2 | 生成範囲 | |
| B | 6 | | 開発環境 | |
| B | 6 | 1 | 開発言語 | |
| B | 6 | 2 | SDK （利用するためのシステム要件） | |
| B | 6 | 3 | 暗号化ツール （利用するためのシステム要件） | |
| B | 7 | | 対応コンテンツ | |
| B | 7 | 1 | 対応フォーマット | |
| B | 8 | | その他搭載の前提条件 | |
| B | 8 | 1 | | |

| C | | | クライアントミドルウェア | 記入欄 |
|---|---|---|---|---|
| C | 1 | | 静的解析対策機能 | |
| C | 1 | 1 | 逆アセンブル対策の暗号化 | |
| C | 1 | 2 | so ファイル改竄対策 | |
| C | 1 | 3 | dex ファイル改竄対策 | |
| C | 2 | | 動的解析対策機能 | |
| C | 2 | 1 | ルート化対策 | |
| C | 2 | 2 | USB デバッグ対策 | |
| C | 2 | 3 | デバッガ対策 | |
| C | 2 | 4 | 再パッケージ化対策 | |
| C | 2 | 5 | Android SDK 付属エミュレータ対策 | |
| C | 2 | 6 | 偽 dex 対策 | |
| C | 2 | 7 | 一時ファイル解析対策 | |
| C | 2 | 8 | 実行端末のホワイトリスト化 | |
| C | 3 | | その他 | |
| C | 3 | 1 | 実行時の負荷 | |
| C | 3 | 2 | ファイル圧縮 | |

| D | | | | ビジネス要件 | 記入欄 |
|---|---|---|---|---|---|
| D | 1 | | | 配信形式 | |
| D | 1 | 1 | | ダウンロード型 | |
| D | 1 | 1 | 1 | ID制限 | |
| D | 1 | 1 | 2 | 機器制限 | |
| D | 1 | 1 | 3 | サブスクリプション可否 | |
| D | 1 | 1 | 4 | クラウド利用可否 | |
| D | 1 | 1 | 5 | 超流通(クロスプラットフォーム)への対応 | |
| D | 1 | 2 | | ストリーム型 | |
| D | 1 | 2 | 1 | ID制限 | |
| D | 1 | 2 | 2 | 機器制限 | |
| D | 1 | 2 | 3 | クラウド利用可否 | |
| D | 1 | 2 | 4 | 超流通(クロスプラットフォーム)への対応 | |
| D | 2 | | | 暗号化ファイルの取扱 | |
| D | 2 | 1 | | 暗号化ファイルの共有（DL とストリームでのファイル共用） | |
| D | 2 | 2 | | その他 | |
| D | 3 | | | 複製制限 | |
| D | 3 | 1 | | SDカードへの保存・移動の制限 | |
| D | 3 | 2 | | 同一コンテンツの別アプリの利用許可の制限 | |
| D | 3 | 3 | | アプリ内付加情報（歌詞等）の複製制限 | |
| D | 3 | 4 | | 複製回数の制限 | |
| D | 4 | | | 利用制限 | |
| D | 4 | 1 | | IDによる制限 | |
| D | 4 | 2 | | 機器による制限（許可端末以外での認証可否コントロール） | |

| | | | | | | |
|---|---|---|---|---|---|---|
| D | 4 | 3 | | | 同一ユーザーの複数機器でのコンテンツ利用の可否 | |
| D | 5 | | | | 配信期間 | |
| D | 5 | 1 | | | 日付管理されているコンテンツの保護制限 | |
| D | 6 | | | | 再生回数の制限 | |
| D | 6 | 1 | | | 再生回数の制限 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| E | | | | | **契約要件（CP が DRM を利用する場合）** | 記入欄 |
| E | 1 | | | | DRMソリューション利用コスト（単独契約の場合） | |
| E | 1 | 1 | | | ライセンス料 | |
| E | 1 | 1 | 1 | | イニシャルコスト | |
| E | 1 | 1 | 2 | | ランニングコスト | |
| E | 1 | 2 | | | 開発費用 | |
| E | 1 | 2 | 1 | | イニシャルコスト | |
| E | 1 | 2 | 2 | | ランニングコスト | |
| E | 1 | 3 | | | その他費用 | |
| E | 1 | 3 | 1 | | イニシャルコスト | |
| E | 1 | 3 | 2 | | ランニングコスト | |
| E | 2 | | | | DRMソリューションの ASP 形態での提供 | |
| E | 2 | 1 | | | ASP 形式での提供有無 | |
| E | 2 | 2 | | | その他記載事項 | |
| E | 3 | | | | ASP 形態での提供時の内容 | |
| E | 3 | 1 | | | 使用 DRM サービス | |
| F | 3 | 1 | 1 | | DRM サービス名称 | |
| E | 3 | 2 | | | 対応OS | |
| E | 3 | 2 | 1 | | android version | |
| E | 3 | 3 | | | ASP　システムの構成 | |
| E | 3 | 3 | 1 | | ライセンスサーバ | |
| E | 3 | 2 | 2 | | コンテンツ配信サーバ | |
| E | 3 | 3 | 3 | | プレーヤー | |
| E | 3 | 3 | 4 | | パッケージングツール | |
| E | 3 | 4 | | | プレーヤー （提供ありの場合） | |
| E | 3 | 4 | 1 | | ミドルウェア提供 | |
| E | 3 | 5 | | | パッケージングツール （提供ありの場合） | |
| E | 3 | 5 | 1 | | 提供形式 | |
| E | 3 | 5 | 2 | | 作業代行 | |
| E | 3 | 6 | | | ASPソリューション利用コスト | |
| E | 3 | 6 | 1 | | 利用料 | |
| E | 4 | | | | 契約主体 | |
| E | 4 | 1 | | | ライセンサー | |
| E | 4 | 2 | | | 実装主体（機器への実装責任はどこにあるのか） | |
| E | 4 | 3 | | | バージョンアップの責任の所在 | |
| E | 4 | 4 | | | その他契約条件 | |

## ４．規格制定団体による文書等

本ガイドラインのほかに、規格制定団体による文書にも留意が必要となります。
著作物が違法に利用されないよう、著作物の保護を目的として、規格制定団体から文書が発行されているケースがあるためです。

例えば、国際標準化機構（ International Organization for Standardization ： ＩＳＯ ）と国際電気標準会議（ International Electrotechnical Commission ： ＩＥＣ ）が共同で作成した「 Ｃｏｐｙｒｉｇｈｔ，ｓｔａｎｄａｒｄｓ ａｎｄ ｔｈｅ ｉｎｔｅｒｎｅｔ 」がその留意すべき文書の一つとなります。
この文書においては、電子透かし（ウォーターマーク）などによって、著作物が違法に利用されないようにすることなどが記載されています。
電子透かし（ウォーターマーク）とは、ＤＲＭの一つで、ダウンロードされるＰＤＦに埋め込まれたライセンス情報等を表示します。
ここでいうライセンス情報とは、購入者の氏名、注文番号、ダウンロードした日付、その他の表示などとされています。
詳しくは、ＩＳＯおよびＩＥＣのホームページから、「 Ｃｏｐｙｒｉｇｈｔ，ｓｔａｎｄａｒｄｓ ａｎｄ ｔｈｅ ｉｎｔｅｒｎｅｔ 」のダウンロードが可能となっていますので、そちらの文書をご参照ください。
このように、ＣＰにおいては、実施するビジネスに応じて、本ガイドラインのほかに規格制定団体による文書があることなどにも留意することが必要となります。

## ５．我が国の関係法律

ＤＲＭに関係する可能性のある我が国の関係法律を取り上げます。
ＣＰが活動していくにあたり、実際にＤＲＭなどのセキュリティが破られたとき、我が国にどのような法律があり、どのような保護を受け得るのかということは知っておきたい情報だと思われるためです。
ＣＰとしては、セキュリティ対策を十分に実施していなければ、法的な保護が受けられない場合もあることに留意が必要となります。ＤＲＭなどのセキュリティが破られたときに法律上の保護を受け得るには、我々自身がセキュリティを破られないようにしておくといった義務や努力義務が法律上明記されているケースもあるためです。
なお、実際にセキュリティが破られた場合に適用される法律は、個別の事情によるところが大きくなりますので、この情報はあくまでも参考の情報となります。そして、セキュリティを破られた場合の適用法律は、グローバル化に伴い、我が国の法律だけではなく外国の法律が状況によっては適用されることになることにも留意が必要となります。
さらに、近年のインターネット等の技術の進歩と犯罪行為の増加により、法律の改正も頻繁になってきていますので、法律の改正にも留意が必要となります。
このようなことから、情報セキュリティ分野に長けた、我が国のみならず外国事案にも対応できる専門の弁護士にご相談されることが重要となります。

・関係法律一覧（２０１２年３月現在）
本ガイドラインでは、次の５つの法律を事例としてとりあげます。

（１）不正アクセス行為の禁止等に関する法律
（２）刑法
（３）著作権法
（４）不正競争防止法
（５）個人情報の保護に関する法律

・各法律の概要
簡単に各法律における該当個所や内容を説明いたします。
なお、各法の刑事罰や民事罰については割愛しています。

＊「」内は参考条文

### （１）不正アクセス行為の禁止等に関する法律

我が国における不正アクセス行為の増加にともない、犯罪の防止およびアクセス制御機能により実現される秩序の維持により、ハイテク犯罪から市民を守り、あわせてＩＴ業界の健全な発展に寄与するといった観点から、同法が定められました。
この法律は、不正アクセス行為を禁止するとともに、この行為の罰則（刑事罰）を定め、そして再発防止のため不正アクセス行為を受けたアクセス管理者に対しての援助措置も定めています。

① アクセス管理者の定義（2条1項）

アクセス管理者として、ネットワーク経由でユーザーなどに利用させる範囲を決定する権限を有している者とされています。

「この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。）につき当該特定電子計算機の動作を管理する者をいう。 」

② 識別符号の定義（2条2項）

ネットワークで利用する識別符号について定めています。例えば、パスワードなどが識別符号にあてはまります。

「この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下この項において「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。

一　当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号

二　当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号

三　当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号 」

③ アクセス制御機能の定義（2条3項）

アクセスコントロールについて定められています。

「この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。次条第二項第一号及び第二号において同じ。）であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。」

④ 不正アクセス行為の禁止（3条）

不正アクセス行為とはアクセス制御機能による利用制限を免れて利用をできる状態にする行為となり、大きく分けて二つの類型があります。

・他人の識別符号を無断で入力する（3条2項1号）
　他人のＩＤ・ＰＡＳＳを無断で入力すること自体が不正アクセス行為とされています。

・識別符号以外の情報または指令を入力する（3条2項2号、3号）
　セキュリティホールを攻撃してコンピュータや端末に侵入することなどが不正アクセス行為とされています。

「何人も、不正アクセス行為をしてはならない。

２　前項に規定する不正アクセス行為とは、次の各号の一に該当する行為をいう。

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為 」

⑤ 不正アクセス行為を助長する行為の禁止（4条）

他人のＩＤ・ＰＡＳＳを本人に無断で第三者に提供することは、不正アクセス行為を助長する行為とされています。提供方法は、口頭、電子メール、掲示板など、何でもこれに該当します。

「何人も、アクセス制御機能に係る他人の識別符号を、その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして、又はこれを知っている者の求めに応じて、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。ただし、当該アクセス管理者がする場合又は当該アクセス管理者若しくは当該利用権者の承諾を得てする場合は、この限りでない。」

⑥ アクセス管理者による防御措置（5条）

サービスを提供するＣＰの努力義務となりますので、留意が必要です。

不正アクセス行為の防止は、法律による処罰に頼るのみでは実現できません。不正アクセス行為がされにくい環境を整備することが必要であり、アクセス管理者自らによる防御措置を講ずべき義務があることがこの法律で定められています。

「アクセス制御機能を特定電子計算機に付加したアクセス管理者は、当該アクセス制御機能に係る識別符号又はこれを当該アクセス制御機能により確認するために用いる符号の適正な管理に努めるとともに、常に当該アクセス制御機能の有効性を検証し、必要があると認めるときは速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする。」

⑦ 都道府県公安委員会による援助（6条）

サービスを提供するＣＰにおいて、不正アクセス行為があったと認められ、アクセス管理者（例えばサービスを提供する我々自身）から、都道府県公安委員会および方面公安委員会に援助を申し出て、その申し出が相当であると認められたときには、再発防止のための援助が受けられます。公安委員会による援助は、手口・防御措置の解明から、資料提供や助言・指導などを受けることができるとされています。

「都道府県公安委員会（道警察本部の所在地を包括する方面（警察法（昭和二十九年法律第百六十二号）第五十一条第一項本文に規定する方面をいう。以下この項において同じ。）を除く方面にあっては、方面公安委員会。以下この条において同じ。）は、不正アクセス行為が行われたと認められる場合において、当該不正アクセス行為に係る特定電子計算機に係るアクセス管理者から、その再発を防止するため、当該不正アクセス行為が行われた際の当該特定電子計算機の作動状況及び管理状況その他の参考となるべき事項に関する書類その他の物件を添えて、援助を受けたい旨の申出があり、その申出を相当と認めるときは、当該アクセス管理者に対し、当該不正アクセス行為の手口又はこれが行われた原因に応じ当該特定電子計算機を不正アクセス行為から防御するため必要な応急の措置が的確に講じられるよう、必要な資料の提供、助言、指導その他の援助を行うものとする。

２　都道府県公安委員会は、前項の規定による援助を行うため必要な事例分析（当該援助に係る不正アクセス行為の手口、それが行われた原因等に関する技術的な調査及び分析を行うことをいう。次項において同じ。）の実施の事務の全部又は一部を国家公安委員会規則で定める者に委託することができる。

３　前項の規定により都道府県公安委員会が委託した事例分析の実施の事務に従事した者は、その実施に関して知り得た秘密を漏らしてはならない。

４　前三項に定めるもののほか、第一項の規定による援助に関し必要な事項は、国家公安委員会規則で定める。」

（２）刑法

刑法では、さまざまなコンピュータ犯罪に関して刑罰が定められています。
近年のインターネットやコンピュータの技術の進歩にともなって頻発している犯罪に対応するために、明確に刑事罰を定めています。

①電磁的記録の定義（7条の2）

刑法における電磁的記録の定義となります。

「この法律において「電磁的記録」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。」

②電磁的記録不正作出および供用(161条の2第1項)

文書偽造における罪の一類型として定められています。

「人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作った者は、５年以下の懲役又は 50 万円以下の罰金に処する。」

③電子計算機使用詐欺(246条の2)

詐欺罪の一類型として定められています。

「前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、10 年以下の懲役に処する。」

④電子計算機損壊等業務妨害(234条の2)

信用および業務に対する罪の一類型として定められています。

「人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、５年以下の懲役又は100万円以下の罰金に処する。」

（３）著作権法

著作権法は、著作物の公正な利用に留意しつつ、著作者の権利の保護を図り、もって文化の発展に寄与することを目的としています。

著作権法においては、技術的保護手段を定義して保護を図っています。留意しなければならないのは、採用する方法が技術的保護手段の定義にあてはまるかどうかの検証が必要であることです。

① 技術的保護手段の定義（2条1項20号）

著作権法における技術的保護手段を定義しています。

「技術的保護手段　電子的方法、磁気的方法その他の人の知覚によつて認識することができない方法（次号において「電磁的方法」という。）により、第十七条第一項に規定する著作者人格権若しくは著作権又は第八十九条第一項に規定する実演家人格権若しくは同条第六項に規定する著作隣接権（以下この号において「著作権等」という。）を侵害する行為の防止又は抑止（著作権等を侵害する行為の結果に著しい障害を生じさせることによる当該行為の抑止をいう。第三十条第一項第二号において同じ。）をする手段（著作権等を有する者の意思に基づくことなく用いられているものを除く。）であつて、著作物、実演、レコード、放送又は有線放送（次号において「著作物等」という。）の利用（著作者又は実演家の同意を得ないで行つたとしたならば著作者人格権又は実演家人格権の侵害となるべき行為を含む。）に際しこれに用いられる機器が特定の反応をする信号を著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは影像とともに記録媒体に記録し、又は送信する方式によるものをいう。」

② 権利制限の除外（30条1項柱書きおよび同項2号）

ユーザーが、私的に使用するためにある一定の範囲で著作物を複製利用することは適法とされていますが、技術的保護手段を回避しての複製は法律違反となることが定められています。

よって、著作権等の保護のために、技術的保護手段の実装が重要となっていることに留意が必要となります。

「著作権の目的となつている著作物（以下この款において単に「著作物」という。）は、個人的に又は家庭内その他これに準ずる限られた範囲内において使用すること（以下「私的使用」という。）を目的とするときは、次に掲げる場合を除き、その使用する者が複製することができる。」

「技術的保護手段の回避（技術的保護手段に用いられている信号の除去又は改変（記録又は送信の方式の変換に伴う技術的な制約による除去又は改変を除く。）を行うことによ

り、当該技術的保護手段によつて防止される行為を可能とし、又は当該技術的保護手段によつて抑止される行為の結果に障害を生じないようにすることをいう。第百二十条の二第一号及び第二号において同じ。）により可能となり、又はその結果に障害が生じないようになつた複製を、その事実を知りながら行う場合 」

『③参考　ＷＩＰＯ著作権条約　１１条（技術的手段に関する義務）
ＷＩＰＯ著作権条約は、コピーコントロール解除装置を用いてなどの著作権法違反となるような行為について、適切な法的措置を採用するように各国へ義務付けています。この点については、具体的にどのような装置が該当するのか議論されているところでもあり、まだ留意が必要になっています。
「Article 11 Obligations concerning Technological Measures
Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

11条　技術的手段に関する義務
締約国は、著作者によって許諾されておらず、かつ、法令で許容されていない行為がその著作物について実行されることを抑制するための効果的な技術的手段であって、この条約又はベルヌ条約に基づく権利の行使に関連して当該著作者が用いるものに関し、そのような技術的手段の回避を防ぐための適当な法的保護及び効果的な法的救済について定める。」　　』

（４） 不正競争防止法
不正競争防止法では、営業上用いられている『技術的制限手段』を定め、その効果を妨げることにより可能とする機能をもつ装置やプログラム等の譲渡や公衆送信等を禁止しています。これらの禁止行為は、コピーコントロールだけではなく、アクセスコントロールにも適用が可能である点に留意が必要となります。

① ＤＲＭ等の技術的制限手段を回避するプログラムなどを公衆送信などすることを禁止（2条1項10号）
「営業上用いられている技術的制限手段（他人が特定の者以外の者に影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録をさせないために用いているものを除く。）により制限されている影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録（以下この号において「影像の視聴等」という。）を当該技術的制限手段の効果を妨げることにより可能とする機能を有する装置（当該装置を組み込んだ機器及び当該装置の部品一式であって容易に組み立てることができるものを含む。）若しくは当該機能を有するプログラム（当該プログラムが他のプログラムと組み合わされたものを含む。）を記録した記録媒体若しくは記憶した機器を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、又は当該機能を有するプログラムを電気通信回線を通じて提供する行為（当該装置又は当該プログラムが当該機能以外の機能を併せて有する場合にあっては、影像の視聴等を当該技術的制限手段の効果を妨げることにより可能とする用途に供するために行うものに限る。） 」

② 他人が特定の者以外の者に、ＤＲＭ等の技術的制限手段を回避するプログラムなどを公衆送信などすることを禁止(2条1項11号)

「他人が特定の者以外の者に影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録をさせないために営業上用いている技術的制限手段により制限されている影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録（以下この号において「影像の視聴等」という。）を当該技術的制限手段の効果を妨げることにより可能とする機能を有する装置（当該装置を組み込んだ機器及び当該装置の部品一式であって容易に組み立てることができるものを含む。）若しくは当該機能を有するプログラム（当該プログラムが他のプログラムと組み合わされたものを含む。）を記録した記録媒体若しくは記憶した機器を当該特定の者以外の者に譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、又は当該機能を有するプログラムを電気通信回線を通じて提供する行為（当該装置又は当該プログラムが当該機能以外の機能を併せて有する場合にあっては、影像の視聴等を当該技術的制限手段の効果を妨げることにより可能とする用途に供するために行うものに限る。）」

（５） 個人情報の保護に関する法律

不正アクセスの事件において、クラッカーは顧客の個人情報を狙ってくることが多くあります。個人情報が高額で取引されたり、犯罪等に利用されたりするケースが多くなっているためです。

そこで、個人情報の保護に関する法律では、個人情報取扱事業者にその情報の漏えいなどに対しての安全管理のために必要かつ適切な措置を講じることを定めています。

個人情報を保護するために必要なセキュリティを施さずに、クラッカーなどによる情報漏えい事件を発生させた場合、安全管理措置の義務違反となる可能性があり、主務大臣からの是正勧告や命令を受ける可能性もあることに留意しなければなりません。

① 安全管理措置の義務(20条)

「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」

## ６．コンテンツプロバイダーのためのＤＲＭ選択参考基準

本ガイドラインでは、ＣＰにおいてはＤＲＭなどのセキュリティを実装する際の参考にするために、著作権者などにおいては貸し出す著作物に対してどのようなレベルのＤＲＭなどのセキュリティが施されているのかの判断の一助とするために、ＤＲＭ選択参考基準を検討・考察しました。
ＤＲＭを検討するうえで非常に重要な項目となるのは、「Ｃ．クライアントミドルウェア」の項目となります。この項目の「静的解析対策」を施している場合と「動的解析対策」を施している場合で大きくセキュリティレベルは異なると認識されます。
その結果、下記表のようにＬｅｖｅｌ．０から５までの６段階での参考基準を作成するに至りました。
下記表では、Ｌｅｖｅｌの数値が上がるほど、ＤＲＭなどのセキュリティ強度も高くなるように表現をしました。

各Ｌｅｖｅｌの説明

・Ｌｅｖｅｌ．０　：　ＤＲＭ等のセキュリティを何も施さない状態（いわゆるＤＲＭフリー）
・Ｌｅｖｅｌ．１　：　ＩＤ・ＰＡＳＳ管理を行うアクセスコントロールだけを実装
・Ｌｅｖｅｌ．２　：　Ｌｅｖｅｌ．１に、コピーコントロールとして一部暗号化などの静的解析対策を実装
・Ｌｅｖｅｌ．３　：　Ｌｅｖｅｌ．１に、必要な静的解析対策を全て実装
・Ｌｅｖｅｌ．４　：　Ｌｅｖｅｌ．３に、動的解析対策の一部を実装
・Ｌｅｖｅｌ．５　：　Ｌｅｖｅｌ．３に、必要な動的解析対策の全てを実装


| セキュリティ / Level | アクセスコントロール | コピーコントロール | |
|---|---|---|---|
| | | 静的解析対策 | 動的解析対策 |
| 5 | ○ | ○ | ○ |
| 4 | ○ | ○ | △ |
| 3 | ○ | ○ | × |
| 2 | ○ | △ | × |
| 1 | ○ | × | × |
| 0 | × | × | × |

表．ＤＲＭ選択参考基準

## ７．本ガイドラインの考察とまとめ

本ガイドラインを作成するにあたり、様々な技術をＤＲＭ関連サービス提供企業からご教示いただき、関係者での検討をすすめました。その結果として、ＡｎｄｒｏｉｄＯＳにおけるＤＲＭなどのセキュリティは、ビジネスモデルによってそのセキュリティレベルを考慮する必要があると考えられました。
具体的には、著作物やプログラムの保護においては、静的解析対策だけではなく、実行時にも保護する、すなわち動的解析対策の必要性があると考察されました。例えば、著作権ビジネスを前提とすると、そのほとんどは著作物やプログラムを容易に複製等されないようする必要性のあるビジネスであり、ＤＲＭ選択参考基準の Ｌｅｖｅｌ．５ のＤＲＭ項目を参考にすることが好ましいと考えられました。なぜならば、静的な状態で保護されていたとしても、実際に利用者が利用しているときに著作物やプログラムなどを容易に複製等されてしまっては、実効ある保護ができていないためです。これは法律上の保護を受け得るという観点ではなく、実際に複製等をされてしまうといったことに実効ある対策をするとの観点から、このように考えられました。
一方で、著作権ビジネスのなかには、著作物を保護する必要性が余り求められないビジネスもあります。例えば、権利者も理解した上でのＤＲＭフリーでのプロモーションなどがその一つとなります。このようなビジネスにおいては、ＤＲＭ選択参考基準の Ｌｅｖｅｌ．０ から ３ を参考にされればよいかと考えられます。敢えて強固なＤＲＭを施さないことによって、ユーザーによる複製を容易にし、情報を広く利用させ、広告効果を高めることを可能にするためです。
このように、ＣＰにおけるビジネス戦略を考慮して、ＤＲＭなどのセキュリティの強度を設定することが有効であると考察されました。
また、コンテンツビジネスを行っていく上で、法律上の保護として、不正アクセス行為を禁止する法律、不正に技術的保護手段を回避する行為を取り締まるための法制度等が整備されています。

監修のことば

今回、一般社団法人モバイル・コンテンツ・フォーラムが本ガイドラインをまとめるにあたって、法的事項に関する監修を行った。具体的には、本報告書の「５．我が国の関係法律」の部分である。

ＤＲＭについては、技術面において著しく進化しているだけでなく、近年、法制度的な動きも急である。不正競争防止法については平成２３年に改正が行われて技術的制限手段の回避行為の範囲が拡大され、あわせて刑事罰が定められた。また、著作権法についても、これに合わせて技術的保護手段の回避行為の規制範囲を拡大する改正案が国会に提出されている。ＤＲＭの提供・利用を行う企業は、今後とも制度改正の動きを十分注視していく必要があろう。

最後になるが、スマートフォンの本格的な普及が始まってから、さほどの時を置かずにこのようなガイドラインをまとめられた関係者の努力に敬意を表したい。

２０１２年５月１５日

森・濱田松本法律事務所　パートナー　弁護士　飯田　耕一郎

参考資料

本ガイドライン作成にあたりご協力いただいたＤＲＭ関連サービス提供企業一覧
（２０１２年５月１５日現在）

企業名　　株式会社ハイパーテック
プレゼンター　代表取締役 小川 秀明 氏
住所　　京都市下京区中堂寺南町１３４番地
　　京都リサーチパーク（財）京都高度技術研究所ビル
ホームページ　http://www.hypertech.co.jp/
提供情報　　「ＣｒａｃｋＰｒｏｏｆ ｆｏｒ Ａｎｄｒｏｉｄ ｓｏ版」
　　「ＣｒａｃｋＰｒｏｏｆ ｆｏｒ Ａｎｄｒｏｉｄ ｄｅｘ版」

企業名　　株式会社アクロディア
プレゼンター　代表取締役社長 堤 純也 氏
住所　　東京都目黒区上目黒２－１－１　中目黒ＧＴタワー１８Ｆ
ホームページ　http://www.acrodea.co.jp/
提供情報　　「Ａｎｄｒｏｉｄにおけるコンテンツ配信とＤＲＭ」

企業名　　サイファー･テック株式会社
プレゼンター　代表取締役社長 吉田 基晴 氏
住所　　東京都新宿区納戸町１２番地　第５長森ビル２Ｆ
ホームページ　http://www.cyphertec.co.jp/
提供情報　　「スマートフォンでもセキュアなコンテンツ配信を可能にするDRMサービスのご紹介」

企業名　　マイクロソフト コーポレーション
プレゼンター　インタラクティブ・エンターテインメント・ビジネス（ＩＥＢ）・メディア・プラットフォーム・ビジネス（ＭＰＢ）　アジア・パシフィック・シニアビジネスディベロップメントマネージャー　山本　博基 氏
住所　　東京都港区港南２－１６－３　品川グランドセントラルタワー
ホームページ　http://www.microsoft.com/japan
提供情報　　「ＰｌａｙＲｅａｄｙについて」

企業名　　ミルモ株式会社
プレゼンター　代表取締役社長 横地 俊哉 氏
住所　　東京都江東区２－７－４　ｔｈｅＳＯＨＯ　３１２
ホームページ　http://www.millmo.co.jp/
企業名　　株式会社電通
プレゼンター　プラットフォーム・ビジネス局事業室事業1部 部長 中西 康浩 氏
住所　　東京都港区東新橋１－８－１
ホームページ　http://www.dentsu.co.jp/
提供情報　　「ＲＯＴＡ２Ｕについて」

企業名　　株式会社Ｊストリーム
プレゼンター　制作・システム開発事業統括本部　プロデュース・インテグレーション部
次長 鈴木 紀夫 氏
住所　　東京都港区芝二丁目５－６　芝２５６スクェアビル６階
ホームページ　http://www.stream.co.jp/
提供情報　「スマートフォン向けDRMを核とする、音楽/映像配信ビジネス支援ソリューションについて 」

企業名　　株式会社デジタルハーツ
プレゼンター　ビジネスソリューション事業本部 高柳 勝彦 氏
住所　　東京都新宿区西新宿３－２０－２　東京オペラシティビル　３２Ｆ
ホームページ　http://www.digitalhearts.co.jp/
提供情報　「Ａｎｄｒｏｉｄセキュリティ検査Ｅｓｓｅｎｔｉａｌサービスのご案内」

企業名　　大日本印刷株式会社
プレゼンター　営業部第２課　エキスパート　平野　明宏 氏
住所　　東京都新宿区榎町７番地
ホームページ　http://www.dnp.co.jp/
提供情報　「ソースコード診断ツール「ＣｘＳｕｉｔｅ」のＡｎｄｒｏｉｄ開発環境対応について」

企業名　　株式会社アンラボ
プレゼンター　営業推進室　室長　山形　哲也 氏
住所　　東京都千代田区外神田４－１４－１　秋葉原ＵＤＸ　８階北
ホームページ　http://www.ahnlab.co.jp/
提供情報　「Ａｎｄｒｏｉｄ用アプリ組込セキュリティのパートナープログラムについて」

検討メンバー・執筆者一覧

一般社団法人 モバイル・コンテンツ・フォーラム

知財・著作権委員会

| | | |
|---|---|---|
| 常務理事 兼 委員長 | 佐藤　慎吾 | （株式会社サミーネットワークス） |
| 前委員長 | 世古　　干 | （ＪＶＣネットワークス株式会社） |
| 副委員長 | 長谷川　篤 | （株式会社第一興商） |
| 副委員長 | 板谷　恭史 | （株式会社サミーネットワークス） |
| 委員 | 鎌田　和幸 | （ＪＶＣネットワークス株式会社） |
| 委員 | 藤原　敏弘 | （株式会社ヤマハミュージックメディア） |
| 前委員 | 角谷　友行 | （株式会社エムティーアイ） |
| オブザーバー | 松浦　　賢 | （株式会社インデックス） |

モバイル著作権部会

| | | |
|---|---|---|
| 部会長 | 板谷　恭史 | （株式会社サミーネットワークス） |
| 副部会長 | 金子　美奈 | （株式会社ミクシィ） |
| 副部会長 | 高橋有理可 | （株式会社エムティーアイ） |
| 前副部会長 | 堀江　康明 | （株式会社エクシング） |
| ｽﾏｰﾄﾌｫﾝ音楽WGﾘｰﾀﾞｰ | 有馬　茂晃 | （株式会社第一興商） |
| 前ｽﾏｰﾄﾌｫﾝ関連WGﾘｰﾀﾞｰ | 井島　剛志 | （ＩＴプロデューサー） |

（部会員１４０名　２０１２年３月３１日現在）

総務委員会

| | | |
|---|---|---|
| 常務理事 兼 委員長 | 岸原　孝昌 | （一般社団法人モバイル･コンテンツ･フォーラム） |

監修　　森・濱田松本法律事務所　パートナー　弁護士　飯田　耕一郎


発行　　一般社団法人モバイル・コンテンツ・フォーラム
住所　　〒150-0011　東京都渋谷区東３－２２－８サワダビル４Ｆ
ＴＥＬ　０３－５４６８－５０９１
ＦＡＸ　０３－５４６８－１２３７
ｅ－ｍａｉｌ　info@mcf.to