スマートフォン時代における
安心・安全な利用環境の在り方に関するWG（第2回）配布資料

於：総務省

資料6

スマートフォン・アプリケーション格付け準備状況

情報セキュリティ格付け制度研究会

（株式会社アイ･エス･レーティング）

2013年1月22日

当資料に記載の内容は予告なく変更することが御座いますので、予めご了承願います。

目次

■スマートフォン・アプリケーション格付け準備委員会

- 設置目的
- 取組状況

■第三者証明書発行サービスの開始・・・・・・マネジメント・プロセスの確認

- 総務省「スマートフォン プライバシー イニシアティブ」を用いた対策状況確認
- 業界団体の特殊性を加味するための取組み

■スマホ・アプリ格付サービスの準備・・・・・・・アプリの振る舞い確認

- ホワイトリスト用（真正性チェック等）の格付データベース提供（想定）
- スマートフォン用の安全性チェック・アプリ提供（想定）

（参考）格付け準備委員会の取組み記事

スマホ・アプリ格付け準備委員会

準備委員会の設置目的

- 今般、株式会社アイ・エス・レーティングがスマートフォンのアプリケーション格付けサービスを開始するに先立ち、その格付け方針、手法、ビジネスモデル等を策定するにあたり、関係企業・団体の方々からなるスマートフォン・アプリケーション格付け準備委員会を設置することと致しました。
- この準備委員会では、格付基準の妥当性を審議し、意見を集約することで『スマホ・アプリの信頼確保に向けた取組の見える化を通じた、アプリ及びデバイスの健全な普及と発展』に資する格付基準とビジネスモデルの策定を目的にしています。
- この格付けは、アプリ提供組織等（企業・団体）からの依頼に基づき行うものとなる見通しです。また、格付結果の公表についてはアプリ提供組織の同意が前提となる仕組みを想定しています。

■準備委員会参加組織

➢ 委員

●NKSJリスクマネジメント株式会社
●株式会社シマンテック
●ダイヤモンドレンタルシステム株式会社
●株式会社フォティーンフォティ技術研究所
●富士ゼロックス株式会社
●株式会社ブロードバンドセキュリティ
●大日本印刷株式会社
●ネットエージェント株式会社
●パナソニック株式会社
●株式会社ラック
●株式会社アイ・エス・レーティング

（順不同/敬称略）

スマホ・アプリ格付け準備委員会

準備委員会の取組状況

■ 開催概要

今年度内に数回の準備委員会を開催し、格付基準やビジネスモデルに関する審議する。

■ 開催状況

□第一回委員会　8月　7日（火）　14:00～16:00　（終了後、記念撮影）

テーマ「準備委員会設置の趣旨説明、今後の進め方と参加規約等について」

□第二回委員会　9月11日（火）　14:00～16:00

テーマ「アンケート結果の共有、ブレーンストーミング」

□第三回委員会　9月19日（水）　13:00～20:00　（懇親会込み）

テーマ「格付基準及びビジネスモデルに関する各社の期待や意向の共有」

□第四回委員会 10月12日（金）　13:00～15:00

テーマ「第三回委員会を踏まえた事務局案に関する意見交換」

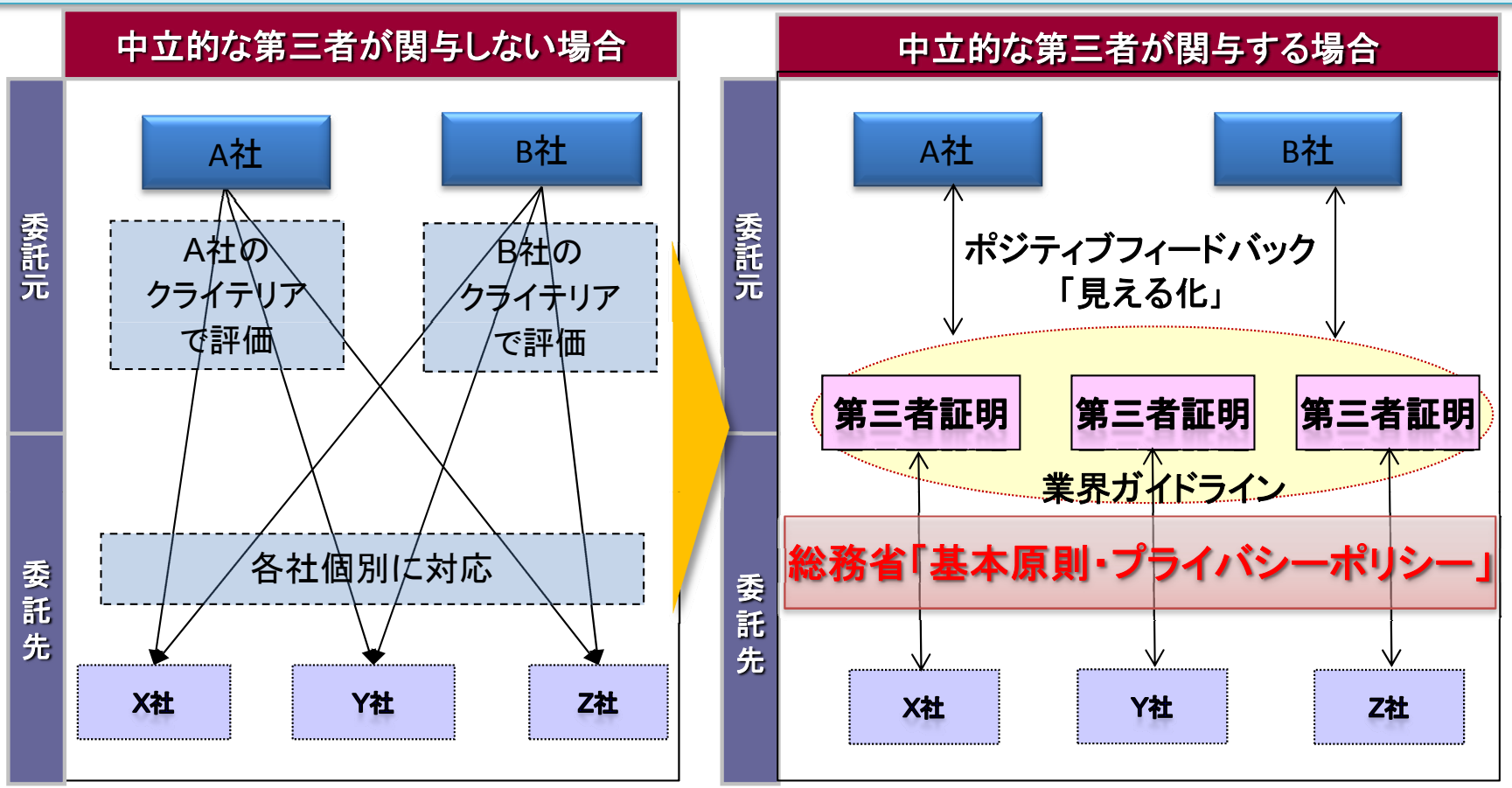
第三者証明書発行サービス
“開始”

⇒

スマホ・アプリ格付サービス
“準備中”

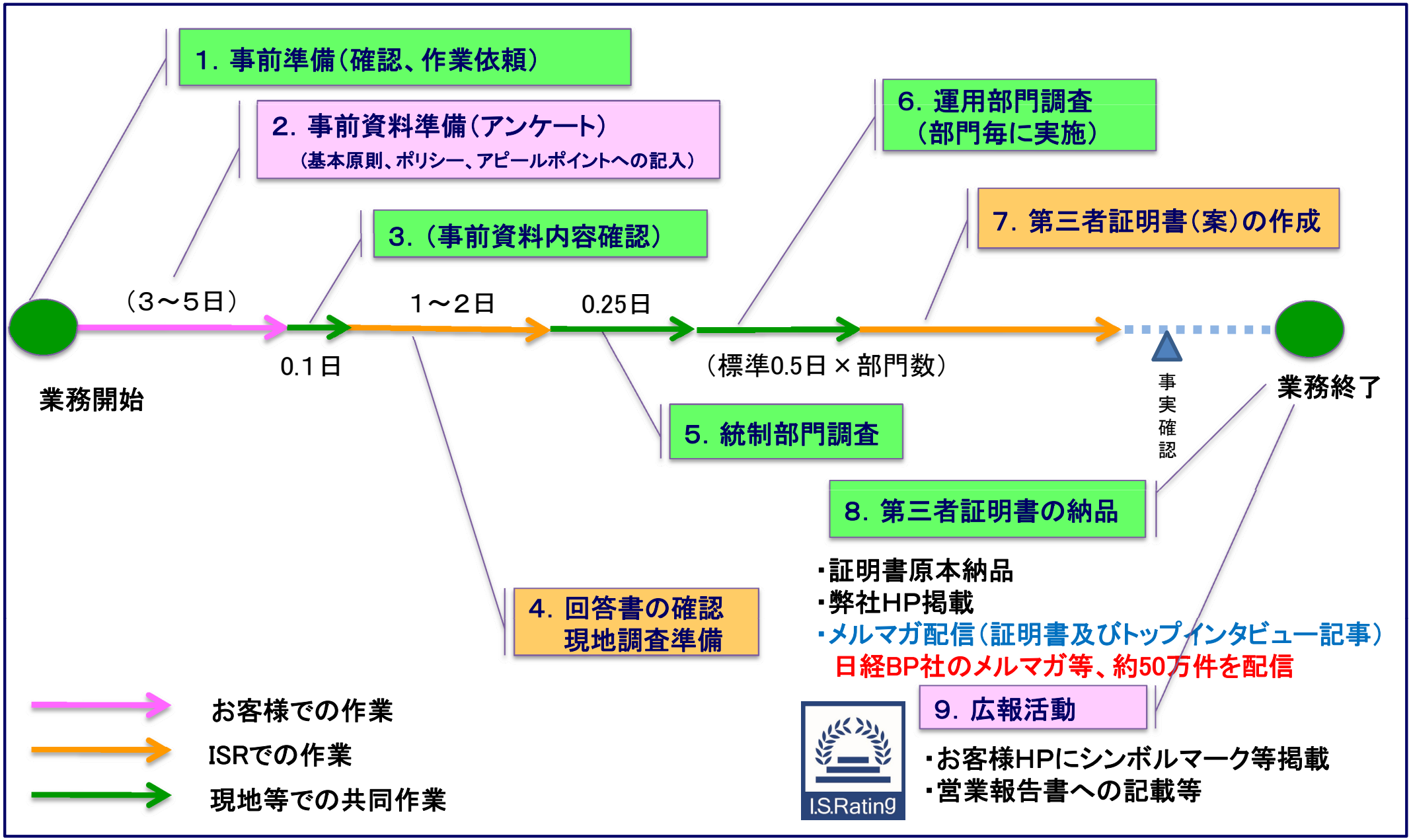
第三者証明書発行サービスの目的

- 総務省スマートフォン プライバシー イニシアティブの基本原則とプライバシーポリシーを活用して、アプリケーション提供事業者のマネジメント・プロセスを客観的に確認。ひいては、事業者間で輻輳しかねない相互の取引確認を第三者証明書を用いて解消し、調査コスト・工数の効率化を図るなど社会的なコスト削減。
- 第三者証明書により信頼確保に向けた取組の“見える化”により説明責任を果たすとともに、ステークホルダーにアピールすることで販路拡大等につなげる機会を創出。
- 第三者が客観的な立場で対策状況を診断することで自社の強み・弱みが浮き彫りになり、経営資源配分等の基礎資料として活用可能。



スマホ・アプリ格付け準備委員会

第三者証明書発行の標準工程



第三者証明書の構成（1）

調査概要

〇〇業務における、プライバシーポリシーの実施状況について、マネジメントプロセスに関する調査を行いました。
本書において、以下に掲載した事案が事実であることを第三者として証明します。

1．調査概要

企業・団体名	〇〇〇株式会社
調査スコープ	プログラム開発センター
調査対象	アプリケーション品質管理業務
調査事項	プライバシーポリシーの実施状況
リファレンス	総務省「スマートフォンプライバシーイニシアティブ」
調査日	2012年10月15日～11月14日
本書交付日	2012年11月15日
利用期限	本書交付日から1年
証明IDコード	10000000000B1202

■調査スコープと調査対象を設定して、アプリ開発等の対象部門や対象業務等を特定可能です。
■調査の方法は、責任者等へのヒアリング、規程および台帳類の閲覧、関連設備の視察等によります。
■第三者証明書は、調査実施日における事象について事実であることを証明するものです。
■利用期限は、証明書交付日から1年を目安としています。
■第三者証明書は、被調査組織等から入手した情報に依拠して形成した当社の意見であり、被開示者、閲覧者等に対し、参考情報として提供いたします。

第三者証明書の構成（2）

確認事項1「基本原則」

基本原則	実施策
①透明性の確保	･･･
②利用者関与の機会の確保	･･･
	･･･
	･･･

確認事項2「プライバシーポリシー」

プライバシポリシー	実施策
① 情報を取得するアプリケーション提供者等の氏名又は名称	･･･
② 取得される情報の項目	･･･

確認事項3「アピールポイント」

項目	優れている点
①蓄積データ、伝送データの漏えい防止策	･･･
②アプリの不正改ざんに対する防御対策	･･･
③今年の特別確認テーマ「ＳＮＳ利用」に関する取組み	･･･

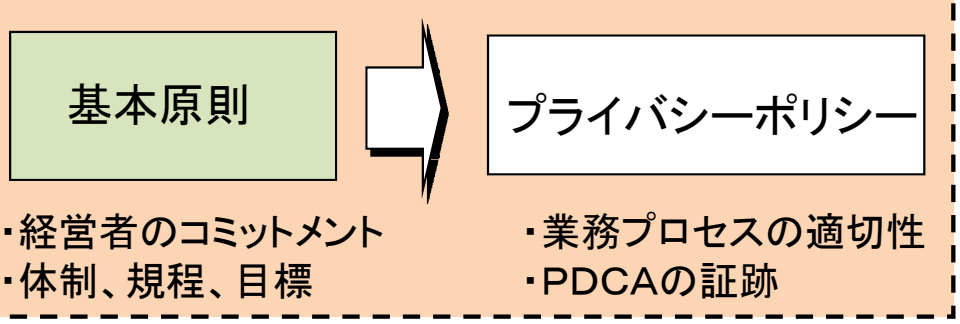
■確認事項1「基本原則」と確認事項2「プライバシーポリシー」は、総務省スマートフォン プライバシー イニシアティブの基本原則（6項目）とプライバシーポリシー（8項目）の計14項目を対象に、マネジメント･プロセスにおいて確認した事実を記載しています。

■事実確認は、対策を講じていない事実も対象となります。例えば、対策を講じていない項目があれば、「〇〇についての対策は確認できなかった。」「△△については来年度実施する計画がある。」等の表現となります。

■ステークホルダーへのアピールポイントについての取組み内容を確認します。取引先からよく聞かれる項目を説明することで、販路拡大等につなげる機会を創出。
■業界における特別な取組みや特定業務における高度な取組みなど、特筆すべき事項についての事実確認が可能です。

第三者証明書の確認事項（1）基本原則の確認

■総務省スマートフォン プライバシー イニシアティブの基本原則とプライバシーポリシーを用い、第三者として組織の統制状況と業務プロセスの適切性を確認（業務設計と運用実施の状況を確認）のうえ、第三者証明書を発行する。



総務省「基本原則」

① 透明性の確保

関係事業者等は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知りうる状態に置く。利用者に通知又は公表あるいは利用者の同意を取得する場合、その方法は利用者が容易に認識かつ理解できるものとする。

② 利用者関与の機会の確保

関係事業者等は、その事業の特性に応じ、その取得する情報や利用目的、第三者提供の範囲等必要な事項につき、利用者に対し通知又は公表あるいは同意取得を行う。また、対象情報の取得停止や利用停止等の利用者関与の手段を提供するものとする。

③ 適正な手段による取得の確保

関係事業者等は、対象情報を適正な手段により取得するものとする。

④ 適切な安全管理の確保

関係事業者等は、取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要・適切な措置を講じるものとする。

⑤ 苦情・相談への対応体制の確保

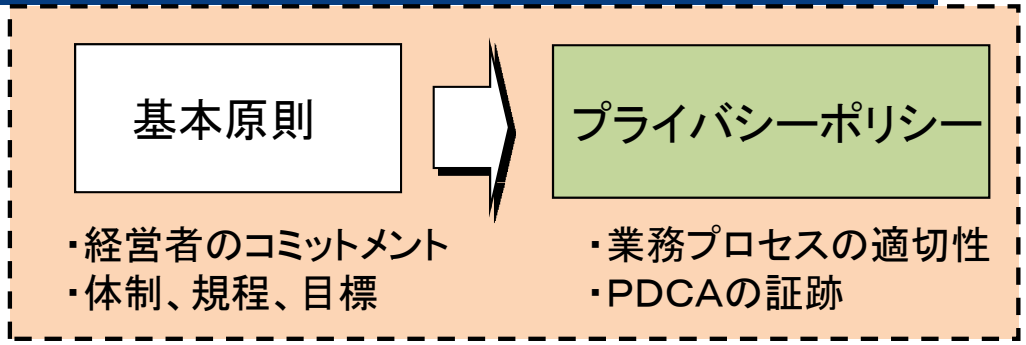
関係事業者等は、対象情報の取扱いに関する苦情・相談に対し適切かつ迅速に対応するものとする。

⑥ プライバシー・バイ・デザイン

関係事業者等は、新たなアプリケーションやサービスの開発時、あるいはアプリケーション提供サイト等やソフトウェア、端末の開発時から、利用者の個人情報やプライバシーが尊重され保護されるようにあらかじめ設計するものとする。利用者の個人情報やプライバシーに関する権利や期待を十分認識し、利用者の視点から、利用者が理解しやすいアプリケーションやサービス等の設計・開発を行うものとする。

第三者証明書の確認事項(2)ポリシーの確認

■総務省スマートフォン プライバシー イニシアティブの基本原則とプライバシーポリシーを用い、第三者として組織の統制状況と業務プロセスの適切性を確認(業務設計と運用実施の状況を確認)のうえ、第三者証明書を発行する。



総務省「プライバシー ポリシー」

① **情報を取得するアプリケーション提供者等の氏名又は名称**:アプリケーション提供者等の名称、連絡先等を記載する。

② **取得される情報の項目**:取得される利用者情報の項目・内容を列挙する。

③ **取得方法**: 利用者の入力によるものか、ｱﾌﾟﾘｹｰｼｮﾝがスマートフォン内部の情報を自動取得するものなのか等を示す。

④ **利用目的の特定・明示**: 利用者情報を、アプリケーション自体の利用者に対するサービス提供のために用いるのか、それ以外の目的のために用いるのか記載する。広告配信・表示やマーケティング目的のために取得する場合には、その旨明示する。

⑤ **通知・公表又は同意取得の方法、利用者関与の方法**: 通知・公表の方法、同意取得の方法は、プライバシーポリシー等の掲示場所や掲示方法、同意取得の対象、タイミング等について記載する。利用者関与の方法は、利用者情報の利用を中止する方法等を記載する。

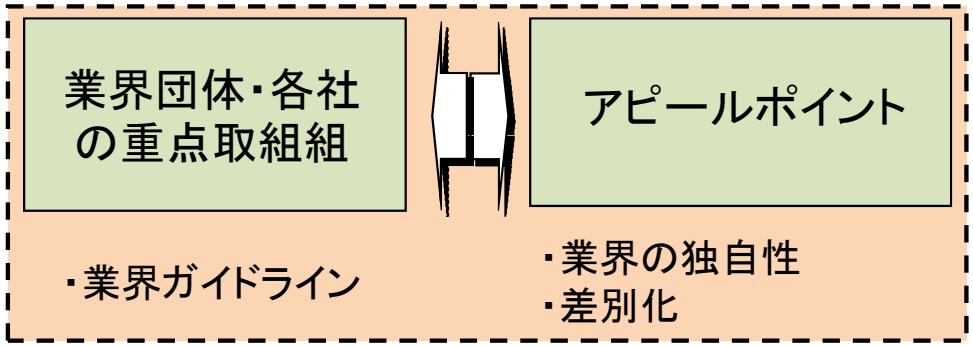
⑥ **外部送信・第三者提供・情報収集モジュールの有無**: 外部送信・第三者提供・情報収集モジュールの組込みの有無を記載する。

⑦ **問合せ窓口**: 問合せ窓口の連絡先等(電話番号、メールアドレス等)を記載する。

⑧ **プライバシーポリシーの変更を行う場合の手続**:プライバシーポリシーの変更を行った場合の通知方法等を記載する。(当初取得した同意の範囲が変更される場合、改めて同意取得を行う。)

第三者証明書の確認事項（3）アピールポイント等

■業界団体が発行しているガイドラインや当該事業において求められる要件を加味したうえで、アプリ提供会社が第三者証明書を用いてステークホルダーに対し、業務品質をアピールできる枠組みを提供する。



業界団体「ガイドライン等」

金融業界、行動ターゲティング広告業界の例

①蓄積データの漏えい防止策

・端末への利用者情報の保存状況及び保存状態（暗号化の有無等）の確認。

・サービス解約時に、サーバへの蓄積データを含むすべてのデータを消去していることの確認。

②伝送データの漏えい防止策

・サーバ等の通信先への利用者情報の通信内容（暗号化の有無）の確認。

③コンピュータウイルス等不正プログラムへの防御対策

・コンピュータウイルス等不正プログラムの検知対策、プログラムの改ざんを防止する対策確認。

・システムに不正プログラムが組み込まれないよう、プログラム(自機関開発プログラム、外部開発委託プログラム、パッケージプログラムおよびダウンロードプログラム等を含む)をシステムに組み込む場合には、事前に十分な検証を行う。

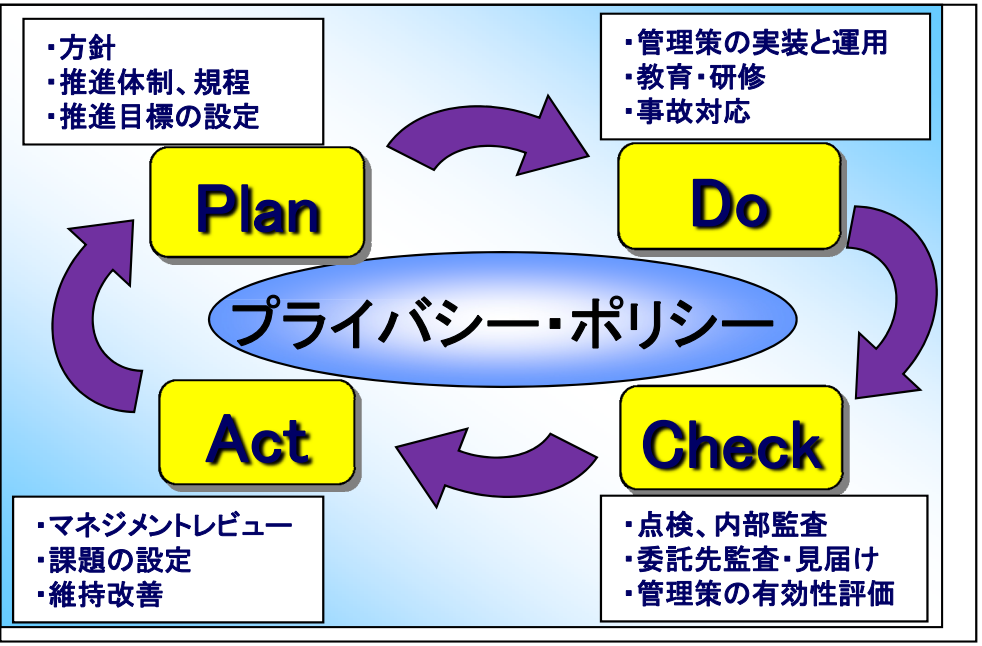
④利用者関与の機会の確保（オプトアウト）と蓄積データの漏えい対策

・収集した行動履歴情報を行動ターゲティング広告に利用することの可否を、ユーザーが容易に選択できる手段の提供。加えて蓄積データの漏洩対策等の情報管理状況の見える化。

スマホ･アプリ格付け準備委員会

今後の取組み　＝全体図＝

第三者証明書発行サービス【組織単位】



セキュア支援サービス

パートナー企業群
- ･アプリ診断サービス
- ･アプリ開発支援サービス
- ･教育研修サービス

アナリスト･セールスパートナー等として参画

格付データ･ベース【企業単位】

証明書取得企業は、格付けDBに自社の公開鍵を登録可能

格付データ･ベース
（検討中）

- ･アプリ開発事業者の実在
- ･経営者の姿勢（コミットメント）
- ･業務プロセス（PDCA）
- ･アピールポイント

取得企業の公開鍵を登録し、アプリの改ざん検知に利用

BBSec等で検討中

ユーザのリスクが高まりかねないアプリの振る舞いについて、ソースコードを自動チェック
- ･root権限の使用
- ･SDカードの読取り
- ･録音、カメラ利用
- ･サーバ機能
- ･起動時の実行等

アプリ格付けは、次の取組みを検討
- ･格付基準とビジネスモデル
- ･実機テスト項目
- ･アプリのリスク自動診断（会員が先行実施中）

実効性の強化【スマホ単位】

利用者は以下を想定
- ･企業･組織向け
- ･一般消費者向け

アプリの真正性確認（DNP等で検討中）

キッティングサービス
保護者向けサービス

真正性チェック･アプリ

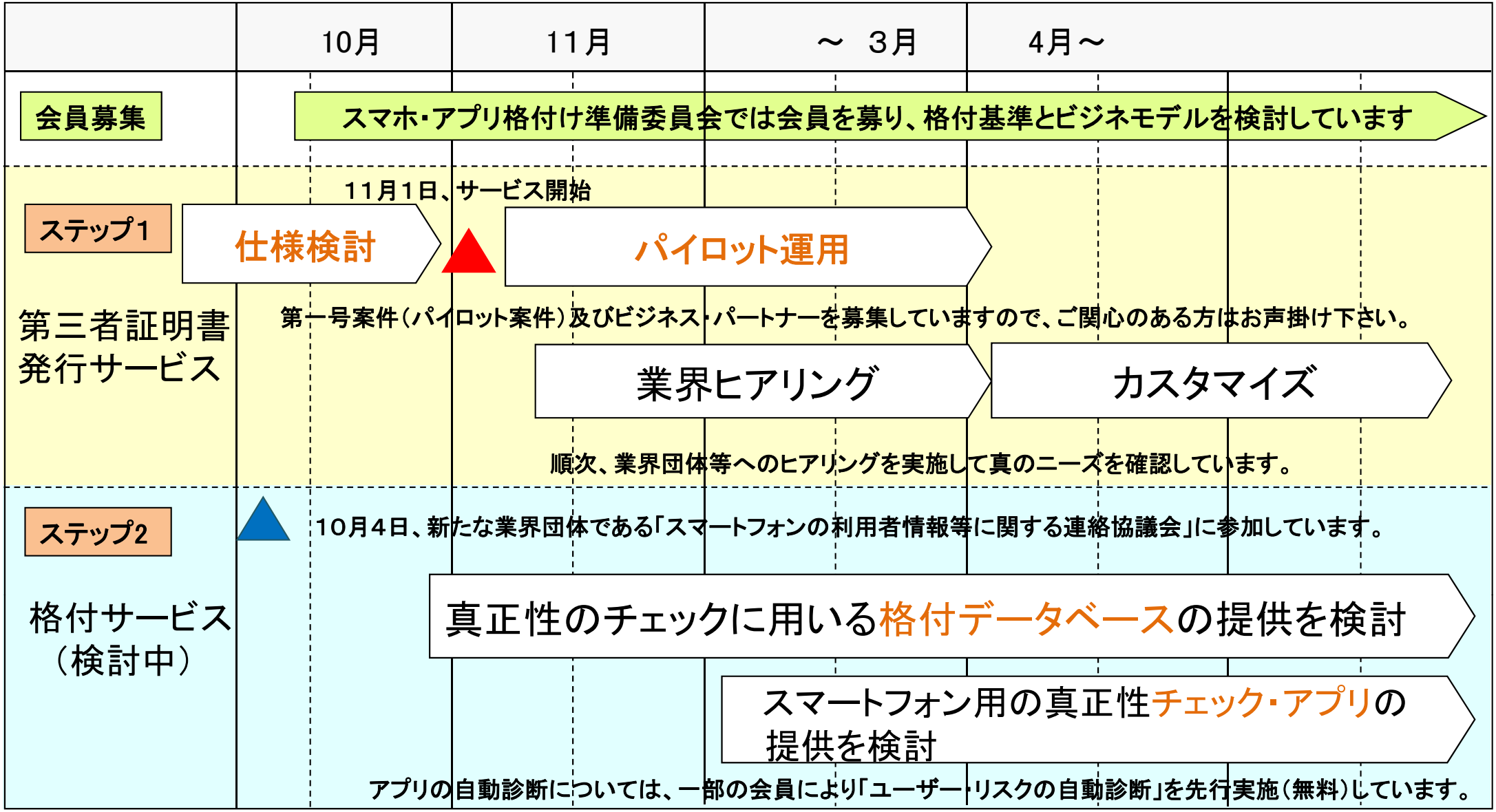
利用者のスマホにインストール

＜第3者証明書取得企業が作成した安全なアプリか否かを確認＞

利用者のスマホにインストール済みの真正性チェック･アプリが、第3者証明書を取得した企業が提供しているアプリかどうかを格付DBを用いて確認

スマホ・アプリ格付け準備委員会

今後の取組み　＝推進スケジュール＝



当準備委員会の最新動向

■メディア露出度の強化（市場メカニズムによる企業価値向上）

□総務省「スマートフォン プライバシー イニシアティブ」への対策状況を示す第三者証明書及びトップインタビュー記事を対象に、日経BP社のメールマガジン等を利用して、１件辺り約50万先に配信する体制が整った。現在、第三者証明書の取得を考えている企業等から高い関心が寄せられている。

■実効性の強化（安心安全を利用者／企業に提供）

□格付けDBに登録されていない公開鍵で署名されたアプリの起動を停止するサービスの提供を検討中。

□アンドロイドアプリのホワイトリストDBの作成を先行して始め、当委員会の構成メンバからMDM関連企業などへの提供を検討中。

＜参考＞ニュース

日経ニューメディア「格付け準備委員会の取組み記事を掲載」

スマートフォンアプリの格付け準備委員会が11月にも第三者証明の発行開始

2012/10/23

ニュース　日経ニューメディア

スマートフォンアプリの格付け準備委員会が11月にも第三者証明の発行開始

2012/10/23
滝沢 泰盛＝日経ニューメディア
出典：日経ニューメディア2012年10月22日号 p.4より（一部情報追加）
（記事は執筆時の情報に基づいており、現在では異なる場合があります）

記事一覧へ >>　いいね！ 35　ツイート 55

スマートフォンアプリが取得するユーザー情報の取り扱いなどについて、一定の信頼性が確保されているかどうかの証明や格付けを実施することを検討している「スマートフォン・アプリケーション格付け準備委員会」は、2012年11月にもアプリ提供事業者に対する第三者証明の発行を開始する。

総務省が2012年8月に公表した提言「スマートフォン　プライバシーイニシアティブ」を受けて実施するもの。アプリ提供会社の運営体制が、提言に示された基本原則やプライバシーポリシーなどに沿っていることを証明する。

具体的な確認項目は、アプリケーションを通じて取得する情報の種類や取得方法、取得した情報の利用目的などを提示しているかどうか、問い合わせ窓口を設置しているかなどである。

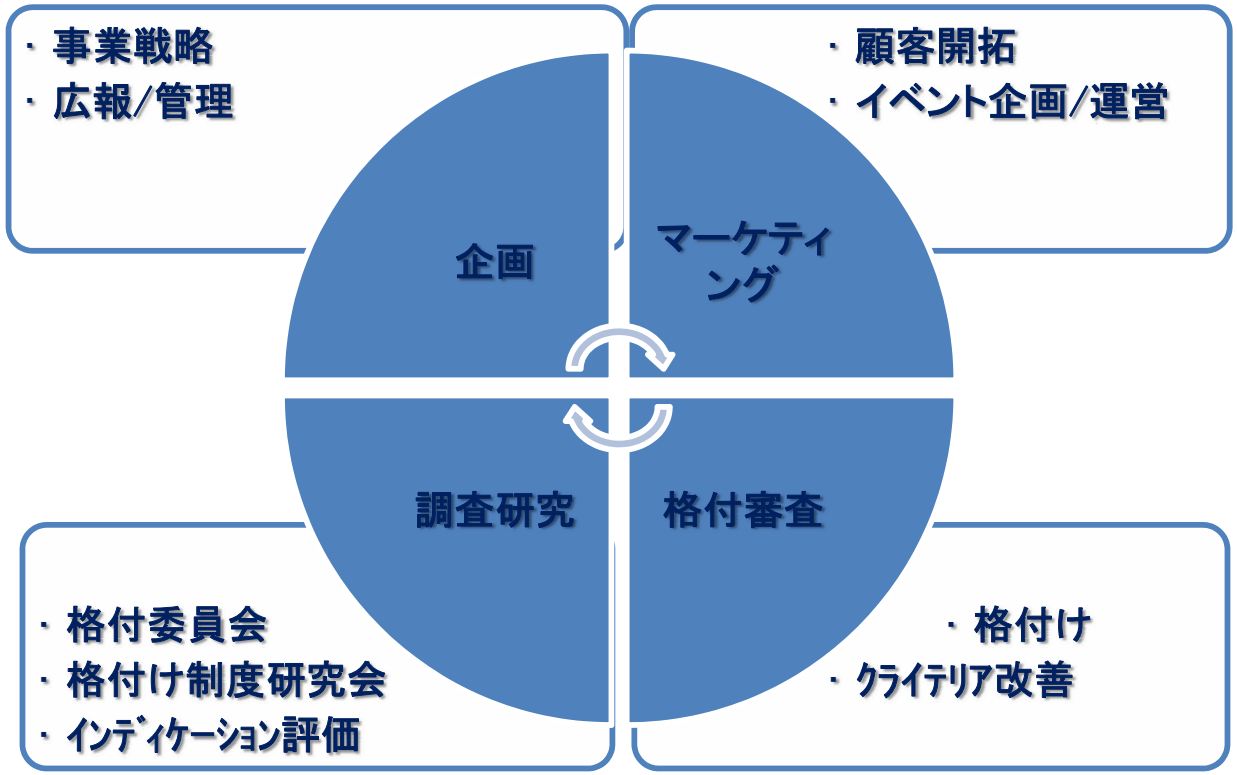
アプリ提供事業者は、証明を受けたことを自社サイトに提示したり、営業報告書などに掲載することで、一定のプライバシーポリシーを確保できているかどうかを第三者によって検証されたものとして外部に公表できるという。

委員会は、シマンテックやフォティーンフォティ技術研究所、ブロードバンドセキュリティ、ラックなどのセキュリティ関連企業、富士ゼロックス、大日本印刷、パナソニックなど11社で構成し、8月からスマートフォンアプリの格付けについて検討を進めてきた。今回開始する第三者証明は、委員会の事務局を運営するアイ・エス・レーティングが実施する。10月26日に開催予定の情報セキュリティ格付けセミナーでサービス開始に向けた準備状況を報告する。

今後委員会では、個別のスマートフォンアプリに対して格付けを行い、ホワイトリスト方式の格付けデータベースを運用したり、ユーザー自身が格付け情報を参照する仕組みについて検討を進める。2013年度にも個別アプリに対する格付けサービスを開始する方針である。

出典　http://itpro.nikkeibp.co.jp/article/NEWS/20121023/431962/

「第三者証明」で確かめ合う、情報の安全安心！



お問合せ先

株式会社アイ・エス・レーティング

TEL： 03-3273-8830

E-mail： ISR@israting.com http://www.israting.com/

なお、当資料に記載の内容は予告なく変更することが御座いますので、予めご了承願います。