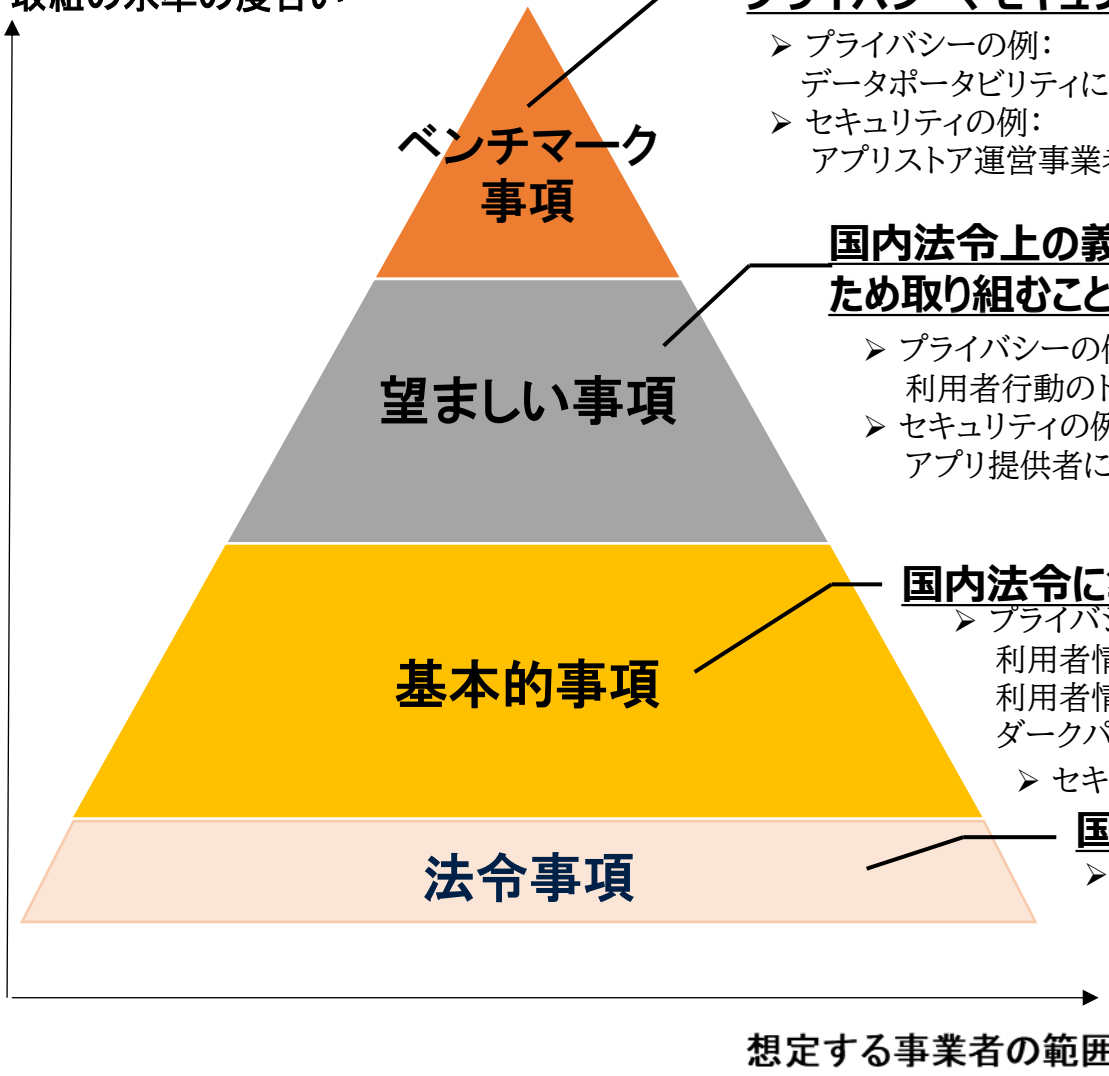
SPSIにおける望ましい事項の再整理のイメージ（概要）



プライバシー、セキュリティ確保のための民間事業者の先導的取組

- プライバシーの例：
  データポータビリティに関する事項など
- セキュリティの例：
  アプリストア運営事業者によるアプリ審査や脆弱性があるアプリへの対応など

国内法令上の義務は必ずしもないが、プライバシー、セキュリティ確保のため取り組むことが望ましい事項（欧州の法令等を参照、国内法令のガイドラインに記載）

- プライバシーの例：
  利用者行動のトラッキング、同意の撤回機会の提供、こどもの利用者情報など
- セキュリティの例：
  アプリ提供者による脆弱性があるアプリへの対応など

国内法令に準じた形で取扱いが求められる基本的な事項

- プライバシーの例：
  利用者情報の利用目的の特定（個情法17条に準じる）
  利用者情報の安全管理措置（個情法23条に準じる）
  ダークパターンの回避（個情法20条に準じる）、プライバシー・バイ・デザインなど
- セキュリティの例：セキュリティ・バイ・デザイン

国内法令上義務とされている事項

- 国内法令（個人情報保護法、電気通信事業法）に基づく義務
  例：個人情報の利用目的の特定（個情法17条）
  個人データの安全管理措置（個情法23条）（※）
  特定利用者情報規律（※）・外部送信規律（電気通信事業法）など
  （※）については、プライバシーのみならずセキュリティにも関係

（注1） 「望ましい事項」は、事業者が「やらなくて良い」という事項ではなく、事業者の取組が当然期待されている事項であることに留意が必要。
（注2） セキュリティについては、いずれの事項についても、アプリ提供者やアプリストア運営事業者等に対し一律の対応を求めるものではなく、事業者自らが、自らを取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定、評価し、リスクに見合った低減措置を講ずること（いわゆる「リスクベース・アプローチ」を採ること）が求められることに留意が必要。

第２３回WG(4/23)におけるご指摘(総論:本文修正時に反映)

○　望ましい事項の中に例外的に基本的事項となっているようなものがばらばらになって出てきてしまうので、最終的な書きぶりをどうするのかという問題はありますが、少し分かりやすく書いていただければよいのではないか。【寺田構成員】

○　リスクベース・アプローチのことが書いてあって、これは望ましいことだと思っている。このことについて、今セキュリティだけに関わる書きぶりになっているが、これはプライバシー全般に係るとまでは言えないと思うが、先ほどの青少年保護の部分も場合によってはそういったリスクの評価やリスクを含めたリスクベース・アプローチの在り方が求められる局面も多いのかなと思い、大変重要な考え方だと思うので、果たしてどのレイヤーに位置づけるかというのは最終的な修文のときに検討されてもよいのかなと思った。【生貝構成員】

○　注ではなくてきちっと書いていないと、注だと飛ばしてしまうのではないかと思われ、図では、「法律の義務は必ずしもないが、プライバシー」云々と、ベンチマーク事項はこういうこと、望ましい事項はこういうこと、基本的な事項はこういうこと、と書いてあるので、そこで望ましいと書いてしまうとどうしても曖昧に受けとる人もいるのではないか。【木村構成員】

○　脚注１にこれを書くのであれば、望ましい事項のところで下線を引いているところで「国内法令上の義務は必ずしもないが、プライバシー、セキュリティ確保のため当然期待されている事項」だと言い切ってしまったほうがよいのではないか。ベンチマーク事項の方を見ると、「先導的取組」というふうに、それをより具体化する形で言っているので、あえてその具体化しているものからさらに脚注に落とすよりは、脚注に落としているものを、ちゃんと望ましい事項をこういうふうに我々は捉えているのだと正面から位置づけるのが望ましいと思った。【江藤構成員】

プライバシー関連

第２３回WG(4/23)における指摘等に伴う整理替え①

	SPSIの記載	ご意見	修正案
47	（アプリケーション提供者は、アプリケーションに情報収集モジュールを組み込んでいる場合、）アプリケーションのプライバシーポリシーにおいても、各情報収集モジュール提供者のプライバシーポリシーにリンクを張るなどして容易に参照できるようにすることが望ましい。（情報収集モジュール提供者のプライバシーポリシーが日本語でない場合、アプリケーションのプライバシーポリシーにおいてその概要を明示する）。 【望ましい事項】	望ましい事項となっているが、一部外部送信規律の内容が含まれているところがあり、例えば電気通信事業ガイドラインの解説において、リンクで示す場合は日本語である必要があって、リンク先は英語であることが認められず、日本語で書きましょうとされているので、法令上の義務が一部あることを考えると基本的事項でよいのでないかと思う。 【太田構成員】	ご指摘の部分は、外部送信規律の解釈として電気通信ガイドラインの解説に記載している事項であるため、「基本的事項」に修正します。

第２３回WG(4/23)における指摘等に伴う整理替え②

	SPSIの記載	ご意見	修正案
81	アプリケーションに関するOSによるパーミッションは一般にアプリケーションがどのような情報にアクセスするかを示しているが、利用目的やスマートフォン外部への送信・第三者提供・共同利用の有無等の項目の記載がない場合には、OSによるパーミッションのみでは本項に示す通知又は公表あるいは同意取得として十分ではない。OSによるパーミッションが表示される際に別途アプリケーション提供者が作成したプライバシーポリシーのリンク先を示すなどの方法により通知又は公表を行うか、必要に応じて個別の情報に関する同意取得等を行うことが望ましい。【ベンチマーク事項】	ベンチマーク事項となっているが、利用目的の話なので、OSのパーミッションでパーミッションされるのはそのアプリケーションから、例えば位置情報にアクセスしてもよいかということだけなので、それを何に使いますよという利用目的の通知・公表は法令事項だと思う。そのため、81番はパーミッションを得るときに本項に示す通知または公表あるいは同意取得として十分ではないといったことが記載されており、それはおそらく法令事項なので、これも基本的事項になるのではないか。 【太田構成員】	ご指摘の通り、第1文は、OSによるパーミッションのみでは利用目的の通知又は公表あるいは同意取得として十分ではないという部分は、法令に関するものであることから、「基本的事項」に修正し、第2文は原案どおり「ベンチマーク事項」とします。

第２３回WG(4/23)における指摘等に伴う整理替え③

	SPSIの記載	ご意見	修正案
119	なお、アプリケーションの更新等により、当初の同意取得の対象であった利用者情報の範囲・取扱方法が変更される場合には、元の利用者情報の範囲・取扱方法について、利用者との間での合意が成立しているため、利用者から同意を取得することが必要となる。 【望ましい事項】	同意の取り直しをしないと既に成立している契約違反となることがあるため、法令上の義務がないとはいえず、基本的事項にしていただくべきものと考える。 【森構成員】	「基本的事項」に修正します。

第23回WG(4/23)における指摘等に伴う整理替え④

	SPSIの記載	ご意見	修正案
131	（略）加えて、アプリケーション提供者は、あらかじめプライバシーポリシーを作成するとともに、委託先からのアプリケーションの納品を受ける際に、プライバシーポリシーの記載事項とアプリケーションの挙動が一致するかを検証することが望ましい。【望ましい事項】	・法令上義務なしと書いてあるが、アプリケーションの挙動がプライバシーポリシーの記載事項と一致しているか検証することは基本であり、挙動が違う場合はそもそも利用目的をしっかりと公表できていないということになるので、これも一部法令上の義務ありになるのではないでしょうか。記載事項と挙動が一致していない状態で出して、プライバシーポリシーに書いていない利用目的で利用していたことになってしまうのは法令上の違反になると思うので、これは法令上の義務ありで基本的事項になると思う。 【太田構成員】 ・プライバシーポリシーの記載事項とアプリケーションの挙動が一致しない場合には、適正取得義務違反、プライバシー侵害等の問題を生じうるため、基本的事項にしていただいたほうがいいと思う。 【森構成員】	アプリの実際の挙動がプライバシーポリシーに合致しないことにより法令違反につながることもあり得ることから、「基本的事項」に修正します。

第23回WG(4/23)における指摘等に伴う整理替え⑤

	SPSIの記載	ご意見	修正案
158	ただし、アプリケーションの利用者に対する通知又は公表あるいは同意取得に関しては情報収集モジュール提供者自身が実施することは困難だと考えられ、アプリケーション提供者を介して行われることが想定されるため、情報収集モジュール提供者は、関連する内容を含むプライバシーポリシーを公表し、アプリケーション提供者へ通知することが望ましい。 【望ましい事項】	158番、159番について情報収集モジュール提供者もプライバシーポリシーを公表するということは基本的事項なのではないのかなと思います。アプリケーション提供者へ通知することは望ましい事項かもしれないが、利用目的の公表または通知は法的義務のところだと思うし、159番の削除についても情報収集モジュールが取得した利用者情報が個人情報だった場合は削除の義務も一部あると思うので、それも基本的事項ではないのかなと思う。 【太田構成員】	情報収集モジュール提供者が個人情報取扱事業者である場合はご指摘のとおりですので、「基本的事項」に修正します。
159	アプリケーションの利用者から、情報収集モジュール提供者に対し、取得した利用者情報に関する問合せ又は取得した利用者情報の消去等の申出があった場合、必要に応じてアプリケーション提供者と協力し、これに応じることが望ましい。 【望ましい事項】		

第２３回WG(4/23)における指摘等に伴う整理替え⑥

	SPSIの記載	ご意見	修正案
162	苦情相談への対応体制の確保及び安全管理措置については、1.2.1.3、1.2.1.4及び1.2.1.6を踏まえて取り組むことが望ましい。【望ましい事項】	162番の苦情相談への対応体制の確保及び安全管理措置について、安全管理措置、苦情相談だが、それは個人情報保護法で安全管理措置の公表については義務であるため、こちらも基本的事項ではないかと思った。 【太田構成員】	情報収集モジュール提供者が個人情報取扱事業者であればご指摘のとおりですので、「基本的事項」に修正します。

第23回WG(4/23)における指摘等に伴う修正(注釈での対応)

	SPSIの記載	ご意見	修正案
79	プライバシーポリシーによる通知又は公表あるいは同意取得は、原則として利用者がアプリケーションをダウンロード又はインストールあるいは利用開始しようとする前に行うことが望ましく、それらの時点で行うことが難しい場合には、初回起動時に処理が実行される前に行うことが望ましい。【望ましい事項】	「望ましい事項」となっていますが初回起動前に外部送信が発生することはないか。【森構成員】	注釈にて外部送信規律に基づく通知・公表のタイミングを記載します。
88	④ 利用者行動のトラッキング　利用者は、端末やアプリケーション等によって提供される広告ID等の識別子に関連付けられることがあり、これらの識別子を他の情報と組み合わせることで、特定の個人の識別性を獲得する可能性があると考えられること、また、特定の個人の識別性は獲得しないものの利用者に対するプロファイリングが可能となることから、プライバシー侵害を回避する観点又は利用者利益の保護の観点から、事業者横断的なトラッキングを実施するために利用者情報を取得する際には、個別の情報に関する同意取得を行うことが望ましい。 【望ましい事項】	事業者横断的なトラッキングを実施する際には外部送信が行われるので、その部分は同意ではないが、通知、公表は一定の事業者にとっては法的義務になっているということは書いていただかないといけない、望ましい事項ではないと思う。脚注等でお書きいただくということだったのでそれでもいいと思うし、また、この原案はやはり外部送信規律がなかった時代のものなので、文章を書き分けていただいて、横断的トラッキングというのはこういう構成になっているけれども、この部分は通知、公表をやらなければいけない。同意を取ることが望ましい、オプトアウトさせることが望ましいといった書き方をしていただいてもいいかなと思う。【森構成員】	既存の注40「電気通信事業法における外部送信規律は、同意の取得を義務とするものではなく、通知又は容易に知り得る状態に置くことを求めるものであるところ、ここでは取り組むことが望ましい事項として記載している。」を修正し、通知・公表は義務、同意は望ましい旨記載します。
160	プライバシーポリシーの内容について変更があった場合は、プライバシーポリシーを更新するものとし、プライバシーポリシーの内容について重要な変更があった場合には、プライバシーポリシーを更新し、公表するとともに、アプリケーション提供者へ通知することが望ましい。【望ましい事項】	物によってはユーザーとの間で合意されていることがあるので、変更する場合には同意の取り直しということになる。特に、重要な変更が個人情報の利用目的の追加みたいなことである場合には同意が必須となる。【森構成員】	注釈にて、特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱う場合は、同意が求められる旨追記します。

セキュリティ関連

第２３回WG(4/23)における指摘等に伴う整理替え①

	SPSIの記載	ご意見	修正案
190	アプリケーション提供者は、アプリケーションの開発時には、セキュリティが適切に確保されるよう、アプリケーションの企画及び設計の段階から、当該アプリケーションにおけるセキュリティの確保について検討し、適切な仕組みをアプリケーションに組み込むことが望ましい（例：業界標準の暗号化技術の使用、最小権限、セキュアコーディング　等）。 【望ましい事項】	・セキュリティに関して、法律以前の問題としてセキュリティの確保は基本というよりはもはや常識、やって当たり前のもので、特にセキュリティ・バイ・デザインは透明性確保などと並んで基本中の基本ですので、その点についても再検討し、もう少し厳しく見ていったほうがよいのではないか。 【寺田構成員】 ・190番、193番、194番というのは、安全管理措置の中に含まれるものとして基本的事項にしたほうがいいのではないかなと思います。 【太田構成員】	ご指摘を踏まえ「基本的事項」に修正します。
191	アプリケーション提供者は、提供するアプリケーションにおいて使用する情報収集モジュールについて、セキュリティの確保の観点から内容を確認することが望ましい。 【望ましい事項】	・セキュリティに関して、法律以前の問題としてセキュリティの確保は基本というよりはもはや常識、やって当たり前のもので、特にセキュリティ・バイ・デザインは透明性確保などと並んで基本中の基本ですので、その点についても再検討し、もう少し厳しく見ていったほうがよいのではないか。 【寺田構成員】	「基本的事項」に修正します。

第２３回WG(4/23)における指摘等に伴う整理替え②

	SPSIの記載	ご意見	修正案
193	アプリケーション提供者は、アプリケーションに係る脆弱性情報を継続して収集するとともに、アプリケーション内に発見された脆弱性について適切かつ迅速に報告を受けられるよう、脆弱性情報の窓口・連絡先を設置するなど必要な体制の整備に努める。 【望ましい事項】	特にこの190番、193番、194番というのは、安全管理措置の中に含まれるものとして基本的事項にしたほうがいいのではないか。 【太田構成員】	ご指摘を踏まえ「基本的事項」に修正します。
194	アプリケーション提供者は、アプリケーションを提供する際にはセキュリティの確保に影響を与え得る脆弱性が含まれないようにあらかじめ確認するとともに、セキュリティの確保に影響を与え得る脆弱性が発見された場合には、アプリケーションのアップデートを適切かつ迅速に提供するなど、必要な対応を取ることが望ましい。 【望ましい事項】		

第23回WG(4/23)における指摘等に伴う修正(注釈での対応)①

	SPSIの記載	ご意見	修正案
190	アプリケーション提供者は、アプリケーションの開発時には、セキュリティが適切に確保されるよう、アプリケーションの企画及び設計の段階から、当該アプリケーションにおけるセキュリティの確保について検討し、適切な仕組みをアプリケーションに組み込むことが望ましい（例：業界標準の暗号化技術の使用、最小権限、セキュアコーディング　等）。 【望ましい事項】	190番の括弧の中の例で業界標準の暗号化技術と書いてありますが、業界標準とは何かがよく分からなかったというところがありました。例えば、業界でとても脆弱な暗号化技術を使っているという場合に、それでいいとういものではないと思いますので、ある程度安全性が確保されている暗号化技術を使わないといけないのではないかとは思っています。例えば、政府推奨暗号リストに載っているものやCRYPTRECが出しているものが参考になると思います。【蔦オブザーバー】	「業界標準」の内容を補足するため、業界標準として、例えば、CRYPTRECの政府推奨暗号リストに掲載されている暗号技術を参照すること等が考えられる旨を注釈に記載いたします。
194	アプリケーション提供者は、アプリケーションを提供する際にはセキュリティの確保に影響を与え得る脆弱性が含まれないようにあらかじめ確認するとともに、セキュリティの確保に影響を与え得る脆弱性が発見された場合には、アプリケーションのアップデートを適切かつ迅速に提供するなど、必要な対応を取ることが望ましい。 【望ましい事項】	（以下、仲上オブザーバーから事務局宛に参考として紹介いただいた、関連するセキュリティ対策施策の例示） （先進的な取組） ・第三者による脆弱性評価の実施（脆弱性診断サービスなどの客観的かつ専門的視点をもつ診断事業者による脆弱性評価の取組） ・ウェブサービスに対するペネトレーションテストの実施（スマホアプリと連携して動作するウェブサービス・APIサービスに対するセキュリティ態勢の脅威ベースでの評価の実施の取組） ・事業基盤（サービス環境）に対するペネトレーションテストの実施（サービスを提供する事業者や組織の事業基盤に対する、セキュリティ態勢の脅威ベースでの評価の実施の取組） （望ましい取組） ・ツールによる脆弱性診断の実施（オープンソースツールなどを利用した脆弱性診断ツールによる脆弱性の評価の取組）	事業者はリスクベースアプローチに基づきセキュリティに関する取組を実施すべきであるところ、アプリ提供者による脆弱性確認の手段として左記の取組の例示が参考になることから、注釈に参考情報として記載します。

第２３回WG(4/23)における指摘等に伴う修正(注釈での対応)②

	SPSIの記載	ご意見	修正案
204	③　　アプリストア内で提供されるアプリケーションが、脆弱性報告のための窓口を有し、かつ、アプリケーション提供者が適切なタイミングで脆弱性を開示するための手続を有していることを確認する 【ベンチマーク事項】	アプリケーション提供者の方の取組において、脆弱性の開示に関するものがないように思いましたので、193や194など、平仄を合わせた方がよいのではないか。脆弱性開示に関しては、汎用品については、いきなりメーカーから開示するというわけではなく、経産省が出している脆弱性の届出の告示、それを通じてIPAに報告しJPCERT/CCで調整してJVNというサイトで公表するのが1つのプラクティスだと思いますので、アプリ提供者側の脆弱性開示に関して、これらの取組に関するリンクもあったほうがよいのではないかと思いました。 【蔦オブザーバー】	補足情報として、アプリ提供事業者が適切な手段により脆弱性開示の取組を実施することが望ましい旨を注釈に記載いたします。
206	⑤ アプリケーションが長期間アップデートされない場合には、アプリケーション提供者にアプリのサポート状況を確認する。 【望ましい事項】	いわゆるエンドオブライフ、EOLの対応を念頭に置いたものだとは思っていますが、サポート状況が終わっているというのは、脆弱性が見つかっても何もしませんということになると思っておりますので、発動するトリガーはアプリが長期間アップデートされないという場合だけでよいのかは少し気になったところです。アプリ提供者もサポートが終了したのであればストアに届け出るなど、そういった取組を望ましい事項と位置づけるべきではないかと思いました。 【蔦オブザーバー】	補足情報として、アプリ提供事業者はサポート終了時にアプリストア提供事業者に連絡することが望ましい旨を注釈に記載いたします。