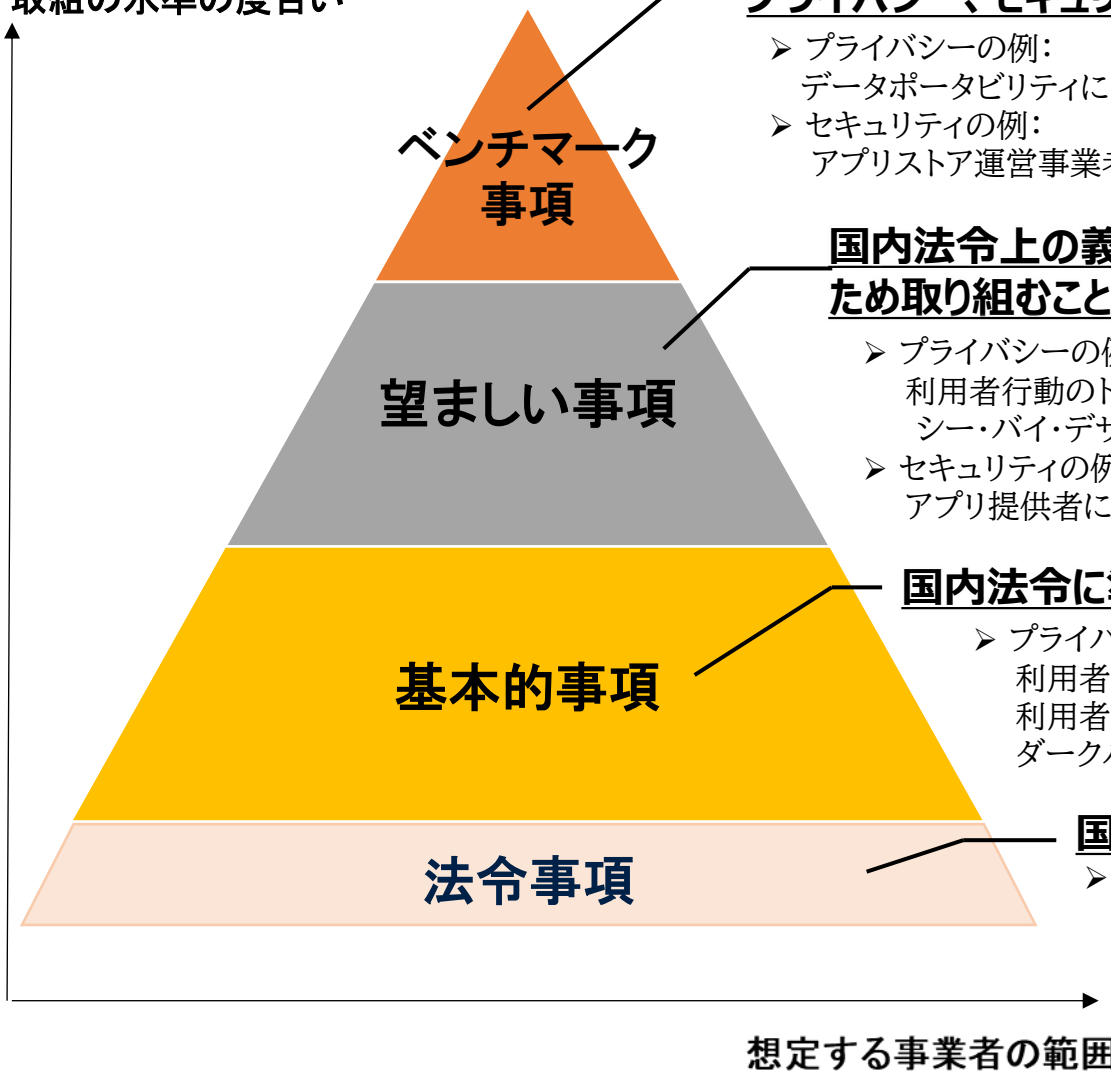
SPSIにおける望ましい事項の再整理のイメージ（概要）



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、プライバシー・バイ・デザインなど
- 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、セキュリティ・バイ・デザインなど

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）など

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。

望ましい事項の再整理に関する主なご指摘（概要）（令和7年4月7日）

【蔦オブザーバ】
① 4分類は個人的には多いと感じるが、見せ方の工夫はできるので特段異存ない。②**安全管理措置は完全にセキュリティの法令事項**。プライバシーと平仄がとれているのか気になる。

【森構成員】
4分類自体には特に異論ない。①**利用者行動のトラッキングはベンチマークではなく望ましい事項ではないか**。②個情法の**安全管理措置のうちセキュリティに一般的に分類されるものは法令事項に入るはず。**アプリ提供者は個人情報取扱事業者であることが時々あることから、一番下の法令事項が空欄であることにはならないのではないか。

【仲上オブザーバ】
4分類の方針に異存ない。①金融庁のGLは脆弱性診断におけるTLPT等高レベルの事項を「望ましい」に入れている。一方、**JSSECの実施規範に含めているのは「必ず行ってほしい」取り組みであり、「できればやって」という受け取られ方をすることを危惧。ぜひ「基本的事項」に盛り込むべき**。②各層のレベル感については、参考になるレベルの施策を提示することは可能。

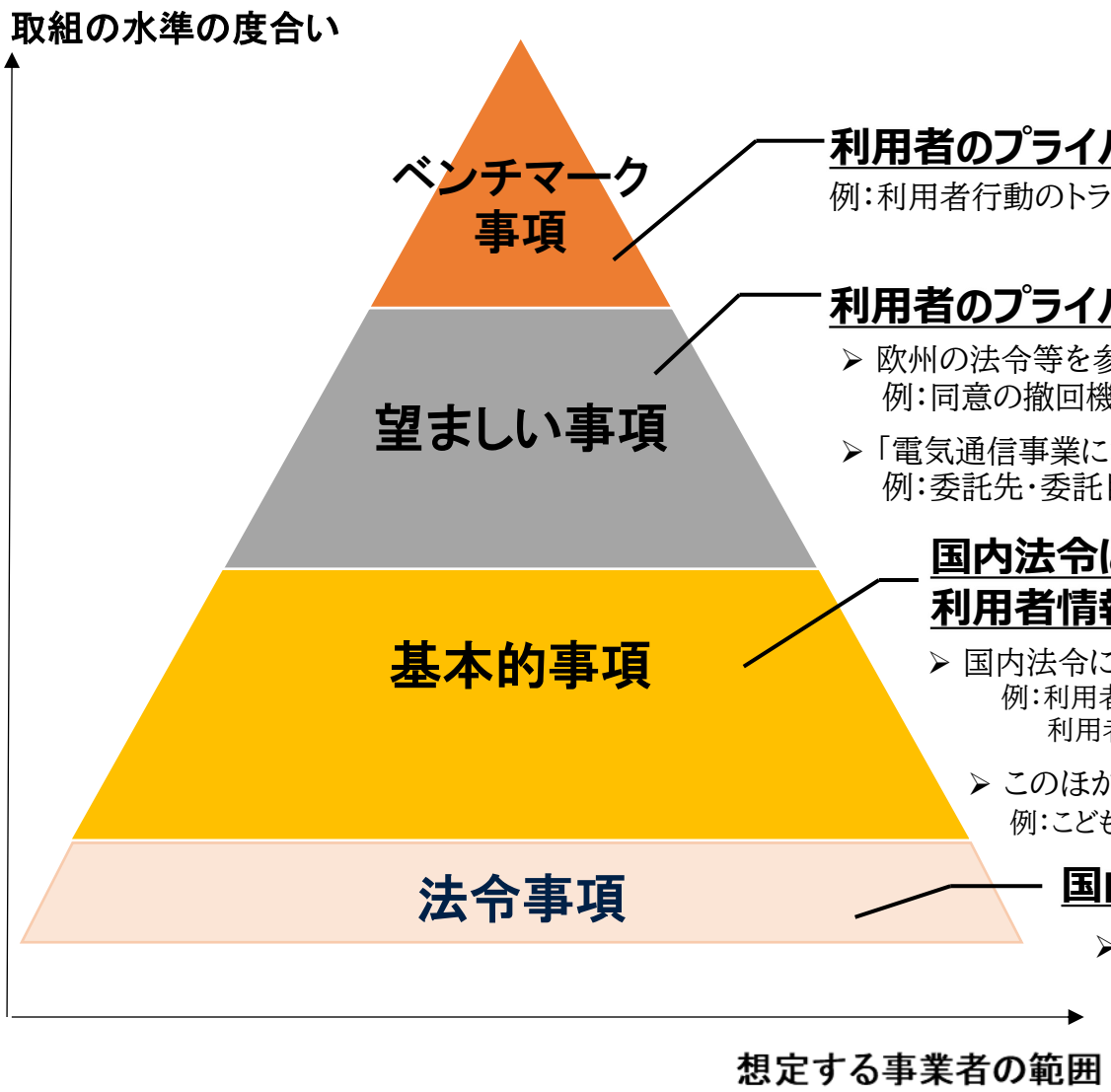
【寺田構成員】
4分類は少し多いが問題ない。①GoogleやAppleがアプリ提供者に課していることが事実上の標準になっているので、一度調べた上でどの事項をどの層に入れるべきか明確にした方がよい。②Cookieや端末IDなどの特定の個人に働きかけ可能な個人関連情報に関する規律は今後の個人情報保護法の見直しにより法令事項となるかもしれず要検討。

【太田構成員】
①プライバシーの4分類とセキュリティの4分類は別々に存在するのか、それともSPSIの全体として4分類があって、その中にセキュリティとプライバシーが混ぜて書かれるのか。②何を「基本的」とし、何を「望ましい」とするかについて、**プライバシーとセキュリティのレベル感を合わせる必要がある**。読む方からしても、例えばトラッキングについて、プライバシーでは「望ましい」だが、トラッキングと関係するウェブスキミングがセキュリティでは「基本的事項」となっていると分かりづらい。

【木村構成員】
プライバシーとセキュリティを2つ並べてみて、レベル感が違うと感じている。今の段階で整理が必要。

【山本主査】
今後、青少年保護もこの4分類を維持して議論していくと思うところ、**プライバシー・セキュリティ・青少年保護で（レベル感の）齟齬がでないように整理してほしい**。

SPSIにおける望ましい事項の再整理のイメージ



利用者のプライバシー確保のための民間事業者の先導的取組

例：利用者行動のトラッキングの同意取得、データポータビリティに関する事項

利用者のプライバシー確保のため取り組むことが望ましい事項

- 欧州の法令等を参考にしている事項
  例：同意の撤回機会の提供とその方法のプライバシーポリシーへの記載
- 「電気通信事業における個人情報等の保護に関するガイドライン」の記載事項
  例：委託先・委託目的等のプライバシーポリシーへの記載

国内法令に準じた形で取扱いが求められるなど、利用者情報の保護に関する基本的な事項

- 国内法令に準じた形で利用者情報の取扱いで実施が求められる事項
  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）
- このほか、利用者情報の保護に関して実施が求められる事項
  例：こどもの利用者情報、ダークパターンの回避

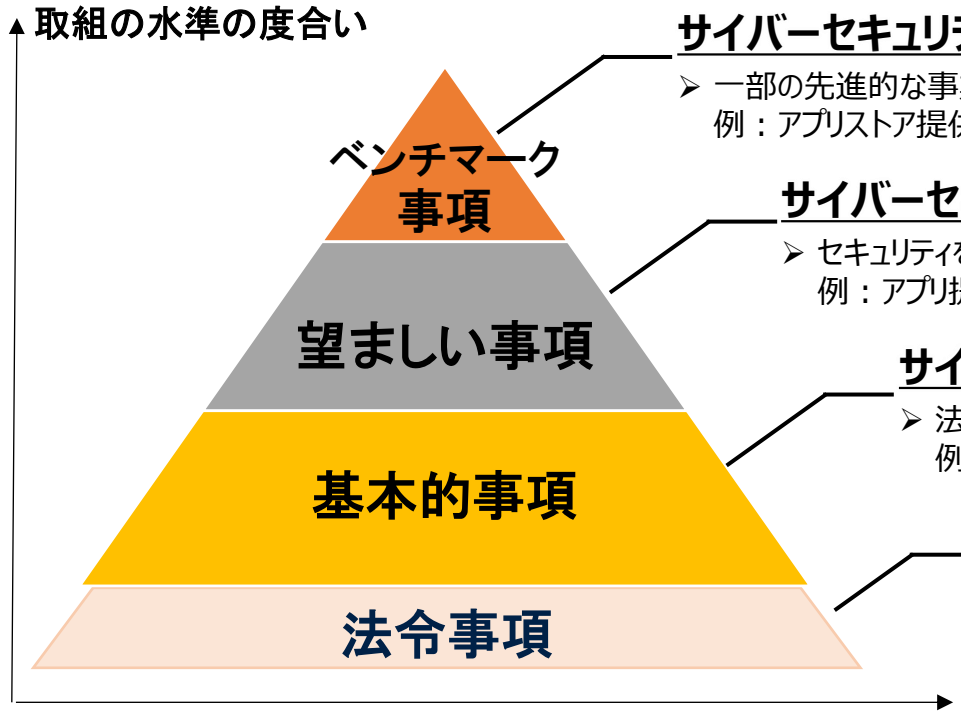
国内法令上義務とされている事項

- 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）

サイバーセキュリティに係る事項の再整理案<イメージ>

- アプリ提供事業者やアプリストア提供事業者等に求められるセキュリティ確保事項として、以下のとおり再整理してはどうか。
  - 「**基本的事項**」には、インシデント発生時のリスク及びその対応の重要性に鑑み、**法令では義務付けられていないものの利用者保護のために特に重要な事項**を分類。
  - 「**望ましい事項**」には、国内の事業者団体の取組※1や英国のCode of Practice※2などを参照しつつ、**国内外の様々な主体においてセキュリティを維持または向上させる取組として広く一般に認知されている事項**を分類。
  - 「**ベンチマーク事項**」には、**一部の先進的な事業者による取組のうち他社が参考とすべきもの**を分類。
- なお、いずれの事項についても、アプリ提供事業者やアプリストア提供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。

※1 一般社団法人日本スマートフォンセキュリティ協会(JSSEC)「スマートフォンアプリケーション開発者の実施規範」、 ※2 英国DSIT「Code of Practice for app store operators and app developers」



サイバーセキュリティを高いレベルで確保する先進的な取組

- 一部の先進的な事業者による取組のうち他社が参考とすべきもの
  例：アプリストア提供事業者による、アプリ審査、脆弱性があるアプリへの対応など

サイバ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

- セキュリティを維持または向上させる取組として広く一般に認知されている事項
  例：アプリ提供事業者による、セキュア・バイ・デザイン、脆弱性があるアプリへの対応など

サイバーセキュリティ確保のための基本的な事項

- 法令では義務付けられていないものの利用者保護のために特に重要な事項
  例：アプリストア提供事業者による、不正なアプリケーションへの対応など

国内法令上義務とされている事項

- SPSIサイバーセキュリティに係る事項は
  個別の国内法令に基づく義務ではないため、該当なし