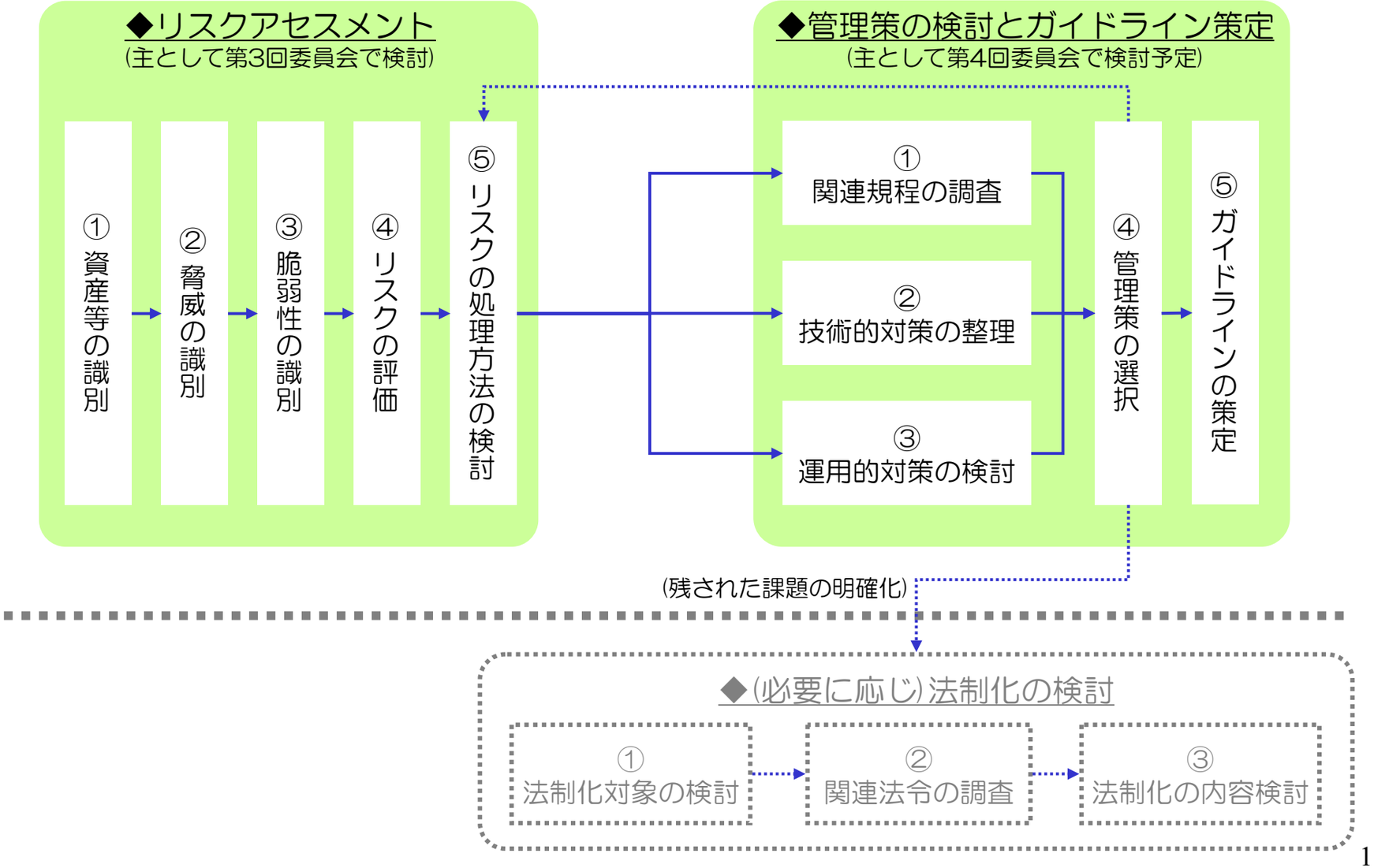
第3回　自律移動支援プロジェクト　セキュリティポリシー検討専門委員会　　資料－3

リスク分析の考え方

平成18年8月

自律移動支援プロジェクト　**セキュリティポリシーガイドラインの検討フロー**



リスク分析の考え方

第2回委員会での議論を踏まえ、以下のリスク抽出作業を実施

（参考資料－1、2）

- ◆ 早期実用化を図る10のサービスについて、利用者に影響を及ぼす脅威・リスクの抽出を実施
- ◆ 各サービスについて、主体別・フェーズ別（設置時・平常運用時・非常時・撤去時・廃棄時）に抽出作業を実施
- ◆ 抽出されたリスクについて、それぞれ、影響・損失の大きさと発生頻度・発生確率を想定し、リスクの大きさを評価（注1）
- ◆ リスクの内容・種類・評価に応じて、主として利用者が蒙る悪影響を低減させるためにサービス提供主体が講じるべき処理策案を想定（注2）

（注）リスク評価および処理策案については、次ページ以降の考え方による

自律移動支援プロジェクト　リスク分析の考え方　（注1）

自律移動支援システムのリスクの大きさについては、下記のように考えることとする。

◆「影響」・・・・想定される損失の大きさについて3段階で評価

◆「発生確率」・・・・発生頻度について3段階で評価

1.重（非常に大きな損失）

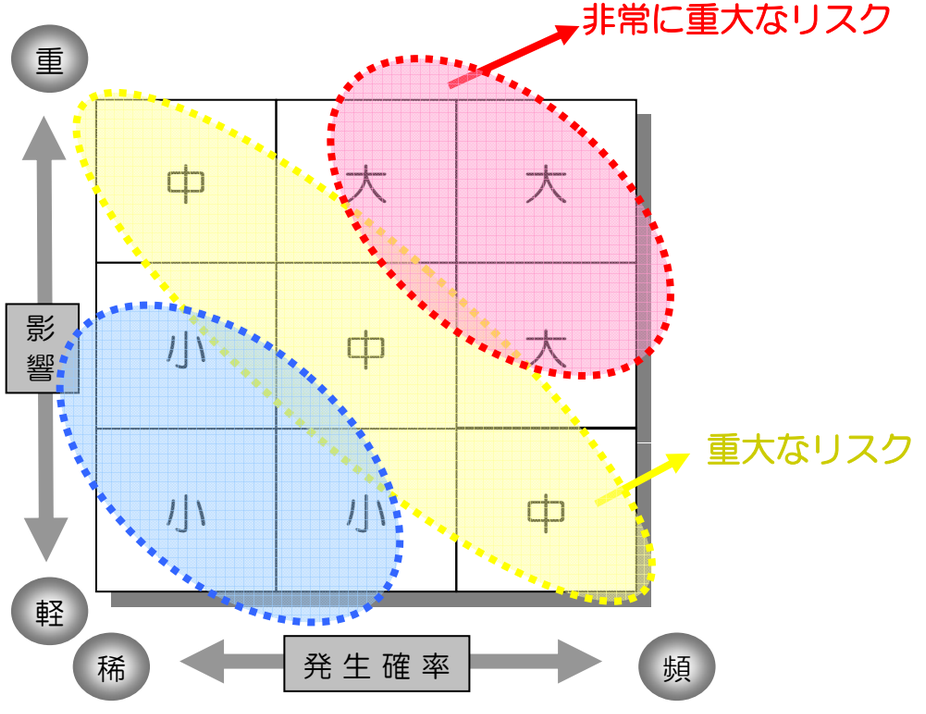
（例）死者が発生する、もしくは、民間事業者を想定した場合、個人情報保護法に違背するなど。（個人データレベルの情報漏洩をイメージ。）当然ながら、社会的指弾を浴び、システム・サービスの存続に関わるレベルの損失。

2.中（大きな損失）

（例）負傷者が発生する、もしくは、民間事業者を想定した場合、個人情報が漏洩するなど。（個人情報レベルの情報漏洩をイメージ。）結果的に、システム・サービスを停止せざるを得ないレベルの損失。

3.軽（損失）

（例）利用者の物権・債権上の権利が侵害される、もしくは、利用者が非常に困惑する。



3.稀（当該フェーズにおいて発生しうる）

（例）発生の可能性を排除できない

2.中（当該フェーズにおいて発生頻度が高い）

（例）時々、発生することが想定される

1.頻（当該フェーズにおいて非常に発生頻度が高い）

（例）常態的に頻発することが想定される

リスク分析の考え方　（注2-1）

自律移動支援システムのリスクの処理策案については、次の4つの方法によるものとする

■保有

- あるリスクからの損失の負担を受容すること
- 保有されるリスクは
  - •識別され受容されるリスク
  - •識別されずに組織に内在するリスク

があるが、ここでいう「保有」は、識別され受容されるリスクを対象としたもの

■最適化

- 適切な管理策を採用し、リスクを低減する方法のこと
- 現実には、対策の実施によるリスクの完全な除去は不可能なため、利便性の確保や、対策にかかる費用と効果の比較により顕在化したときのリスクを受容可能な水準にとどめるのに十分な費用を投入して対策を実施し、残留リスクを保有する

■移転

- 契約等によりリスクを他者(他社)に移転すること
- リスクを移転する方法には、
  - •情報資産や情報セキュリティ対策を外部に委託する方法(アウトソーシング)
  - •リスクファイナンスの一種として保険等を利用する方法

がある

■回避

- リスク対応を考えてもコストの割に利益が得られない場合や適切な対応が見出されない場合、リスクを回避するために、業務を廃止したり、情報資産を破棄するといった方法をとること

(“TR Q 0008”“ISMS認証基準Ver.2.0”等に基づく)

自律移動支援プロジェクト　リスク分析の考え方　（注2-2）

また、処理策案の検討については、下記の考え方によることとする。（フローチャート参照）

（1）好ましくない結果及びその発生確率を最小化するため、「**リスクの最適化**」を基本方針とし、『管理策』の検討を行ったうえで、『ガイドライン』に反映させる。

（2）ただし、運営主体としてリスクを抱え込まないよう、「通信ネットワーク提供者」など、システム・サービス全体の重要な構成主体ではあるが、サービス運営主体からのアウトソーシング先(委託業者)の立場となる可能性が高い主体を、「**リスクの移転**」(共有)先として位置づける。

※リスク移転のための『管理策』の検討→『ガイドライン』への反映は必要

（3）一定以上の重大さのリスクについては、それぞれのリスクに対する対応策を想定し、実現の蓋然性の高い対応策について、今後、具体的な検討を進め、そうでない場合には、「**リスクの回避**」も処理策案として位置づける。

※リスク回避のための『管理策』の検討→『ガイドライン』への反映は必要

（4）一定以下の重大さのリスクについても、それぞれのリスクに対する対応策を想定し、実現の蓋然性の高い対応策について、今後、具体的な検討を進め、そうでない場合には、「**リスクの保有**」も処理策案として位置づける。
また、リスクの種類・影響(損失)等を勘案のうえ、自己責任として受容すべきリスクについても、「リスクの保有」を処理策として位置づける。

（※事業フォーメーションなど、具体的なサービスモデルが決定していない段階での検討のため、
サービスモデルの具体化に伴い処理策も見直し続ける必要がある。）

自律移動支援プロジェクト　リスク分析の考え方　（フローチャート）