

セキュリティガイドラインの 構成の考え方

平成18年8月

ガイドラインの目的

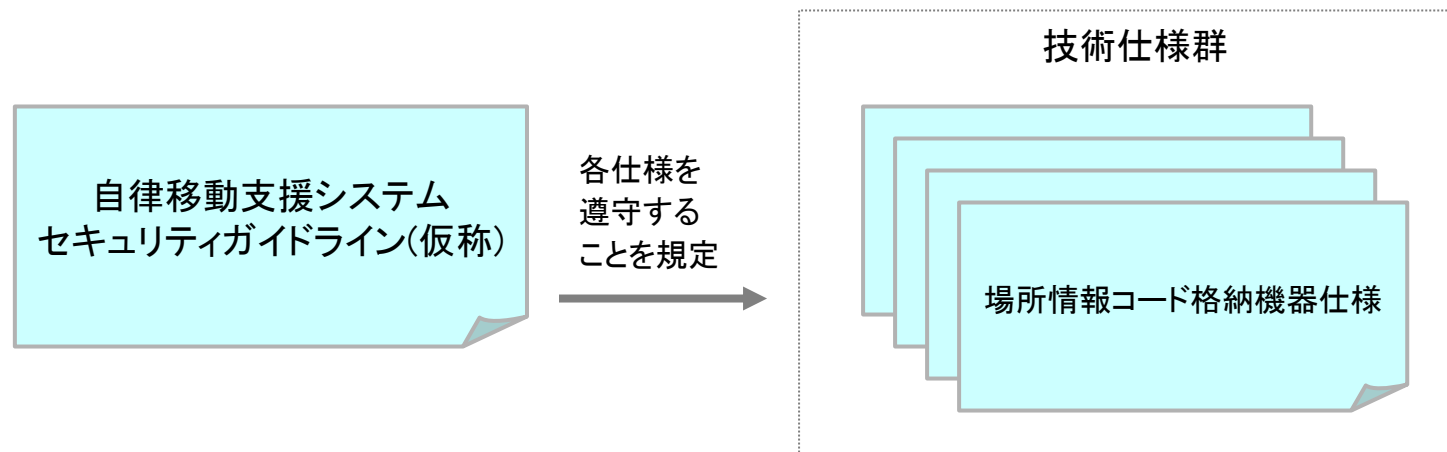
自律移動支援システムについて、関係者がとるべき行動基準を明確化することにより、利用者の保護等、関係者の利益の尊重を前提に、発生するリスクを可能な限り軽減し、本システムの普及と円滑かつ健全な利用を促進すること

ガイドラインの性格

- ◆ 本委員会が本システムの関係者に向けて示すもの
- ◆ 関係者は、これを遵守するという前提でサービスを事業化する(その遵守を相互の調達や契約条件にすることで担保することもある)
- ◆ 直接的な法的拘束力は持たない
- ◆ ガイドラインを策定する中で、法的な対策が必要と考えられる個別事項が見出された場合には、別途提言を行う

ガイドラインの位置付け(技術仕様との関係)

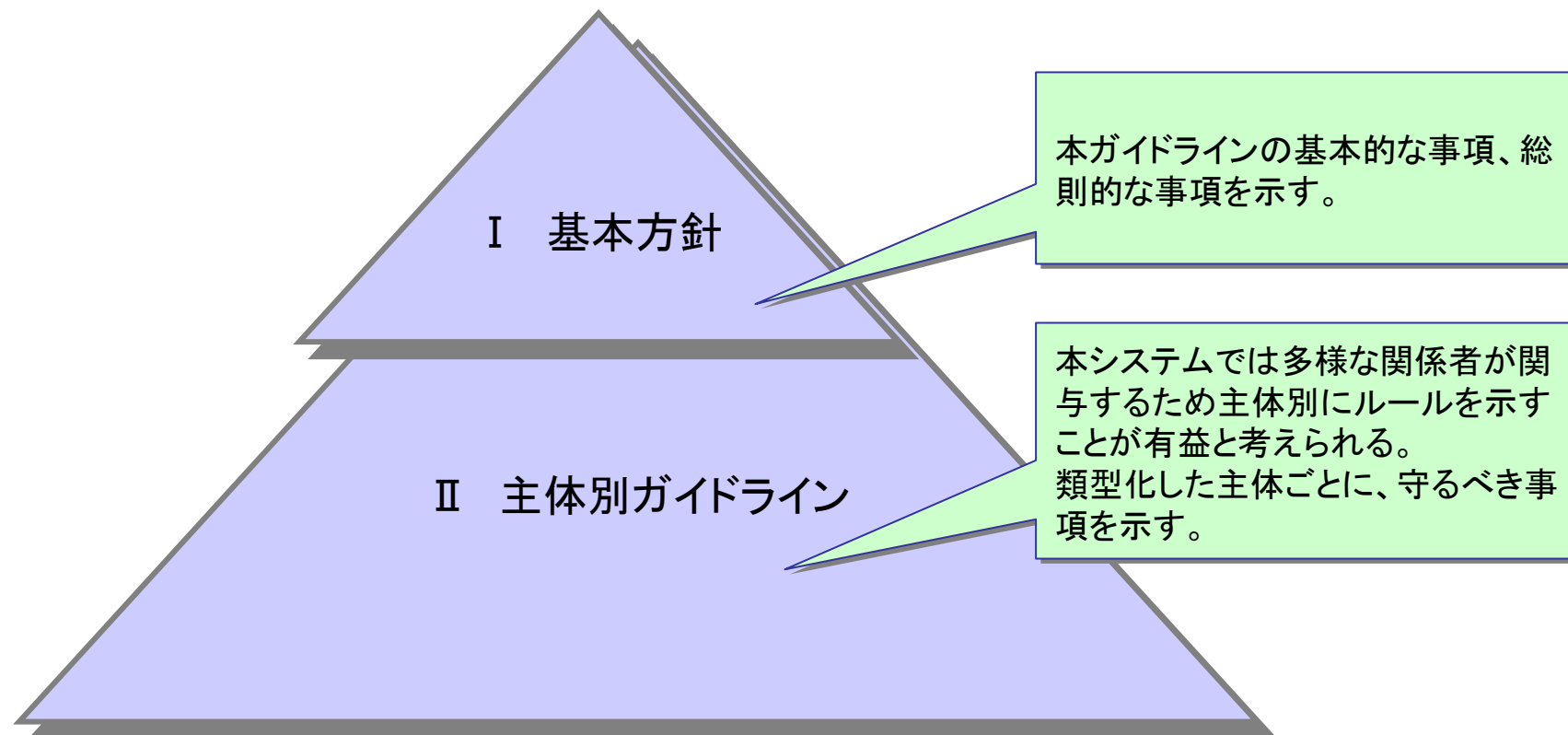
- ◆ 情報セキュリティや個人情報保護の観点で守るべきルールを、運用的、技術的、物理的等の側面から網羅的・体系的に示すもの。
- ◆ ただし、技術的、物理的側面についての具体的な規程は、原則的に各技術仕様に記載することとし、本ガイドラインではそれを遵守すべきことを規定する。



ガイドラインの記述の詳細度

- ◆ 本ガイドラインは、リスク分析の結果を踏まえ、遵守すべきルールをできるだけ具体的に定める。
- ◆ しかし、今回行うリスク分析は、想定される前提の範囲内で行うものであり、あまりに詳細に規定しすぎると、バランスを欠いた規定となったり、サービスの普及・発展を阻害するおそれもある。
- ◆ 実際の記述にあたっては、その規定がもたらす副次的影響にも留意しながら、ある程度の抽象性を持たすことも考慮する。

ガイドラインは、大きく以下の2段階の構成とする。



「I 基本方針」では、以下の内容を記述することを想定している。

項目	記述内容	備考
1. 目的と位置付け	本ガイドラインの目的や位置付けを示す。 対象システムやサービスの変更、環境変化等に対応して、本ガイドラインの見直しを行うことを示す。	スライド1の内容をベース。
2. 定義	本ガイドラインで用いる用語の定義を行う。	
3. 対象範囲	下記のような本ガイドラインの対象範囲を示す。 ・対象サービス ・対象となる関係主体(類型化した主体)	
4. 対策の実施	関係主体は、下記の対策を実施する必要があることをうたう。 ・情報セキュリティ対策 ・個人情報保護対策 ・その他システムに対するリスク対策	
5. 管理体制	関係主体は、上記の対策のために管理体制を整備する必要があることをうたう。	
6. 法令遵守	関係主体は、関係法令の遵守をしなければならないことをうたう。	

自律移動支援プロジェクト ガイドライン骨子 II 主体別ガイドライン (1)構成

「II 主体別ガイドライン」では、以下の内容を記述することを想定している。

項目	記述内容	備考
●. ○○○○者		
●. 1 管理対象と責務	当該関係主体が果たすべき基本的な責務を示す。	リスク分析、管理策の検討結果を体系的に整理して盛り込む 安全管理策については情報セキュリティの項で記述。
●. 2 情報セキュリティ対策	情報セキュリティの観点で実施すべき対策を示す。	
●. 3 個人情報保護対策	個人情報保護の観点で実施すべき対策を示す。	
●. 4 その他必要な対策	その他必要と思われる対策を示す。	

主体の区分は、今のところ以下を想定

- | | |
|------------------------|---------------------|
| 1. 一般利用者 | 3. コンテンツ・サービス提供者 |
| 2. インフラ提供者 | 4. 機器製造者 |
| 2. 1 インテリジェント基準点設置・管理者 | 4. 1 端末製造者 |
| 2. 2 場所情報コード格納機器設置・管理者 | 4. 2 街角情報ステーション製造者 |
| 2. 3 街角情報ステーション設置・管理者 | 4. 3 場所情報コード格納機器製造者 |
| 2. 4 場所情報コード管理センター | |
| 2. 5 認証かぎ発行機関 | |
| 2. 6 通信ネットワーク提供者 | |

* 一般利用者についてはガイドラインに含めず、別途「利用マニュアル」のような形のものを作成することも考えられる

「II 主体別ガイドライン」の具体的な記述イメージは以下のとおり。

2.2 場所情報コード格納機器設置・管理者

本主体が関係する主な脅威

- ①通信不能(不具合・破壊・気象条件等)
- ②機器間の干渉
- ③誤った機器の設置
- ④誤った移設
- ⑤改ざん、悪意による移設
- ⑥誤った撤去、撤去漏れ
- ⑦利用者が認知しない撤去

2.2.1 管理対象と基本的責務

場所情報コード格納機器設置・管理者は、自ら設置・管理する「場所情報コード格納機器」が正しく機能することに務めることを基本的な責務とし、そのために必要な対策を実施するものとする。

2.2.2 情報セキュリティ対策

2.2.2.1 設置

- (1) 設置する場所情報コード格納機器は、「ucode格納機器仕様」に準拠したものとする。これを担保するために、納入に当たって認定書の提出を製造者に求めること。【①】
- (2) 場所情報コード格納機器の設置や移設に当たっては、「設置・保守基準」*を遵守すること。【①、②、③、④】...

2.2.2.2 保守

- (1) 場所情報コード格納機器の保守に当たっては、「設置・保守基準」を遵守すること。【①、②、③】
- (2) 場所情報コード格納機器の正常な動作を保証するため、保守の計画を定め、定期的な保守を実施すること【①、⑤】。...

2.2.2.3 撤去

- (1) 場所情報コード格納機器の撤去に当たっては、不適切な機器が設置されたままとなったり撤去の必要のない機器が撤去されることのないよう、管理体制を明確にした上で、確実に行うこと。【⑥】
- (2) 場所情報コード格納機器を撤去する場合には、事前に周知を行う等、利用者が撤去の事実を認知できるよう務めること。【⑦】...

2.2.3 個人情報保護対策

＜現時点で、特に個人情報に特化したリスクは見出されていないが、分担すべきものがあれば管理策を記述＞

2.2.4 その他必要な対策

...

「設置」、「保守」、「撤去」のような作業段階に沿って示すなど、関係主体にとって、実施すべき事項を理解しやすい記述を行う。

* 設置・保守基準には、設置計画、設置方法、耐久性、保守等についての一連の基準が記述されており、脅威①、②、③、④に対応すると考えられる管理策が含まれている。