資料29－１

スマートシティセキュリティガイドライン
改定の方向性について

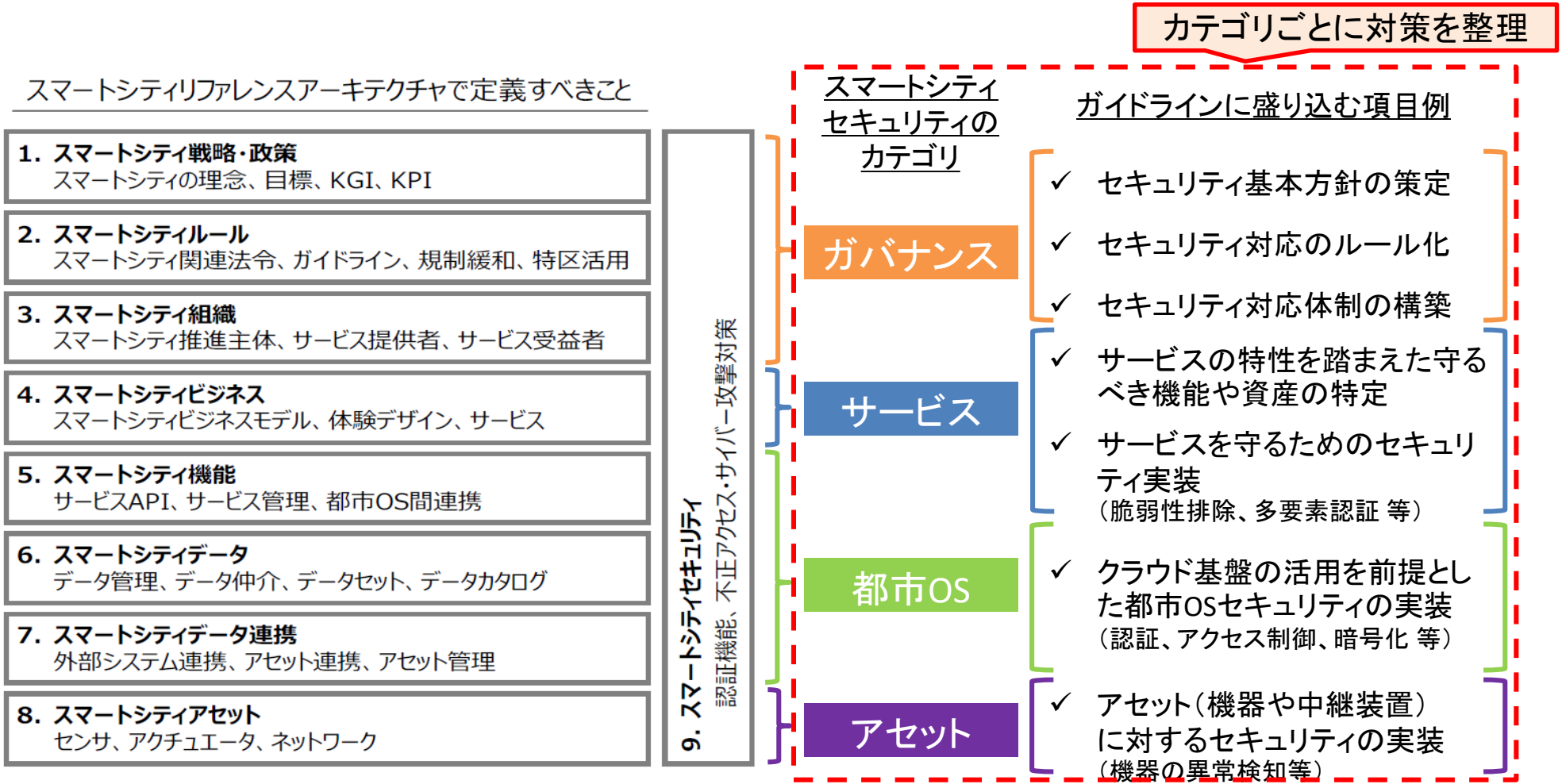
令和３年３月９日

サイバーセキュリティタスクフォース事務局

スマートシティセキュリティガイドライン（第1.0版）の概要について

■ 令和２年１０月、スマートシティ推進におけるセキュリティの考え方や、セキュリティ対策を整理した「スマートシティセキュリティガイドライン（第1.0版）」を作成し、公表。

■ 同ガイドラインは、「スマートシティリファレンスアーキテクチャ」で定義された階層をセキュリティの観点から４つのカテゴリに整理し、それぞれのカテゴリにおけるセキュリティの考え方やセキュリティ対策をガイドラインに記述するとともに、「スマートシティ特有のセキュリティ留意点」を記述。



スマートシティセキュリティガイドラインの改定の方向性

■ その後、第1.0版の更なるブラッシュアップのため、スマートシティに取り組む自治体等からのヒアリングや、有識者・民間事業者・自治体を交えた検討会での意見等を踏まえ、主として下記に記載した改定ポイントを中心に、ガイドラインの改定作業中。

主な改定のポイント（案）

＜総論＞

1. **全体構成の見直し**：スマートシティ特有のセキュリティに関する考慮事項を強調するため、構成を一部変更
2. **関係主体及びガイドラインのスコープの明確化**：本ガイドラインが主に想定する主体について明確化するとともに、関係主体が講じるべき対策として、本ガイドラインで定めるスコープを明確化

（その他、セキュリティリスクに関する記述の充実など）

＜各論＞

3. **データ連携時のセキュリティに関する記述**：スマートシティ内での連携及び他のスマートシティとの連携の両方
4. **サプライチェーンリスク管理に関する記述**：特定高度情報通信技術活用システムの認定要件の趣旨の反映
5. **ゼロトラスト関連の記述**：「一元的にアクセス権限を管理、制御する機能」の活用を対策の一例として記載

（その他、ベストプラクティスの追加など）

＜今後のスケジュール＞

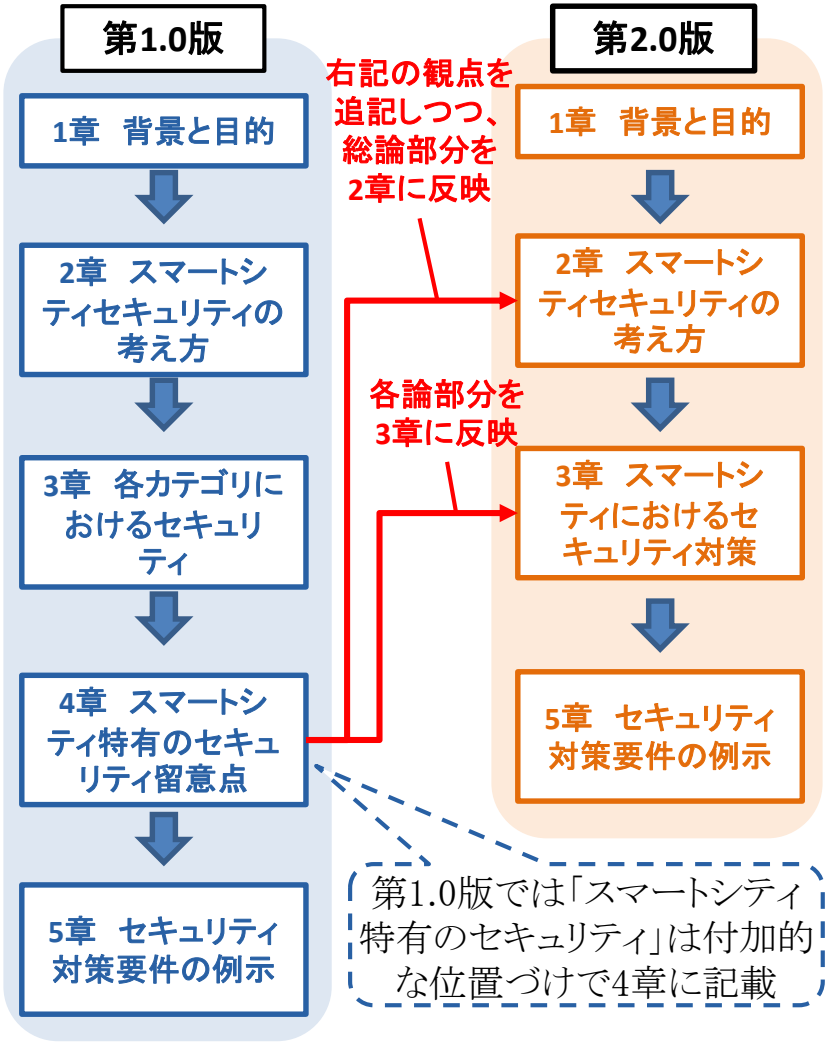
■ 今月中に第2.0版の素案を完成させ、4月以降パブリックコメントを実施、公表予定。

■ 普及啓発のための補助資料として、あわせてガイドブックも策定予定。

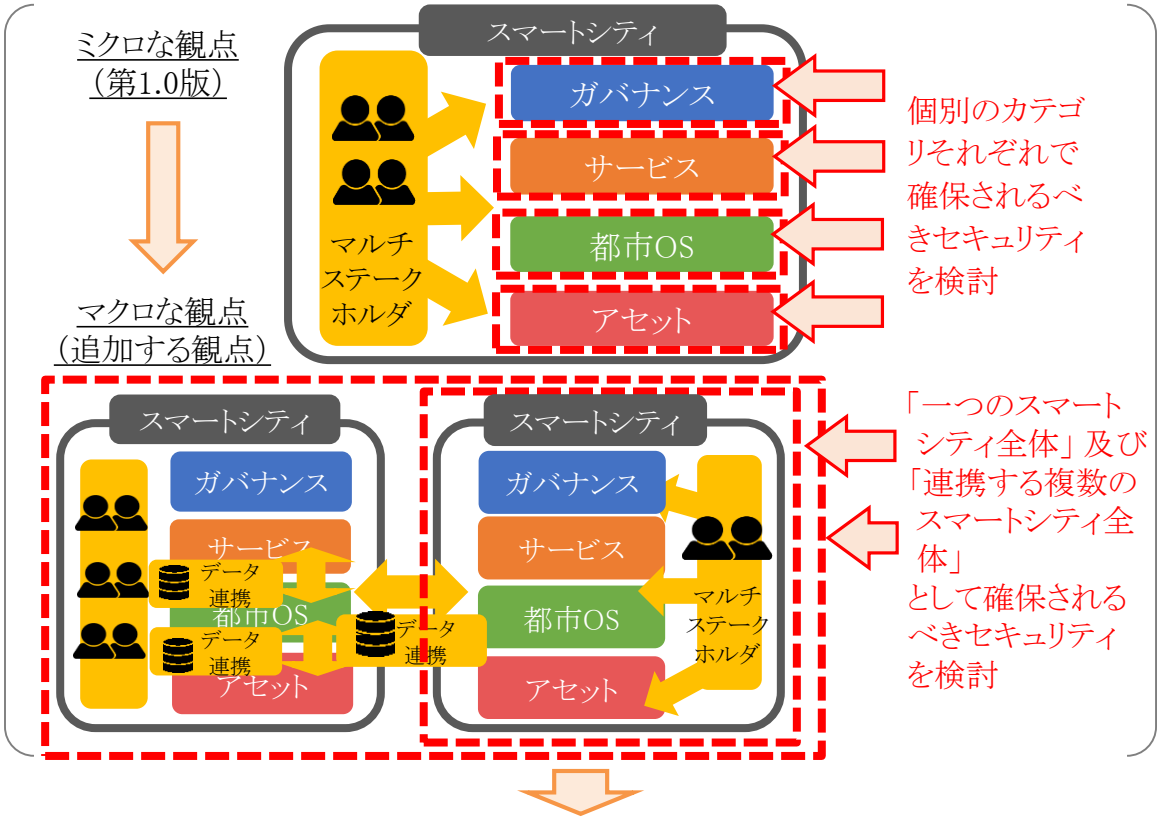
1．全体構成の見直し等について

■ スマートシティ特有の、セキュリティに関する考慮事項について、各構成要素それぞれで確保されるべきセキュリティの観点（ミクロ）に加えて、スマートシティ全体として確保されるべきセキュリティの観点（マクロ）から、わかりやすく整理・分類するとともに、全体構成を見直し。

全体構成の見直し（案）



スマートシティ特有の考慮事項の整理



マクロな観点における**マルチステークホルダが関与するという特徴**を軸に置きつつ、スマートシティ特有のセキュリティの整理として以下の3つに分類。

- **適切なサプライチェーン管理**
- **インシデント対応時の連携**
- **データ連携時のセキュリティ**

2．関係主体及びガイドラインのスコープの明確化

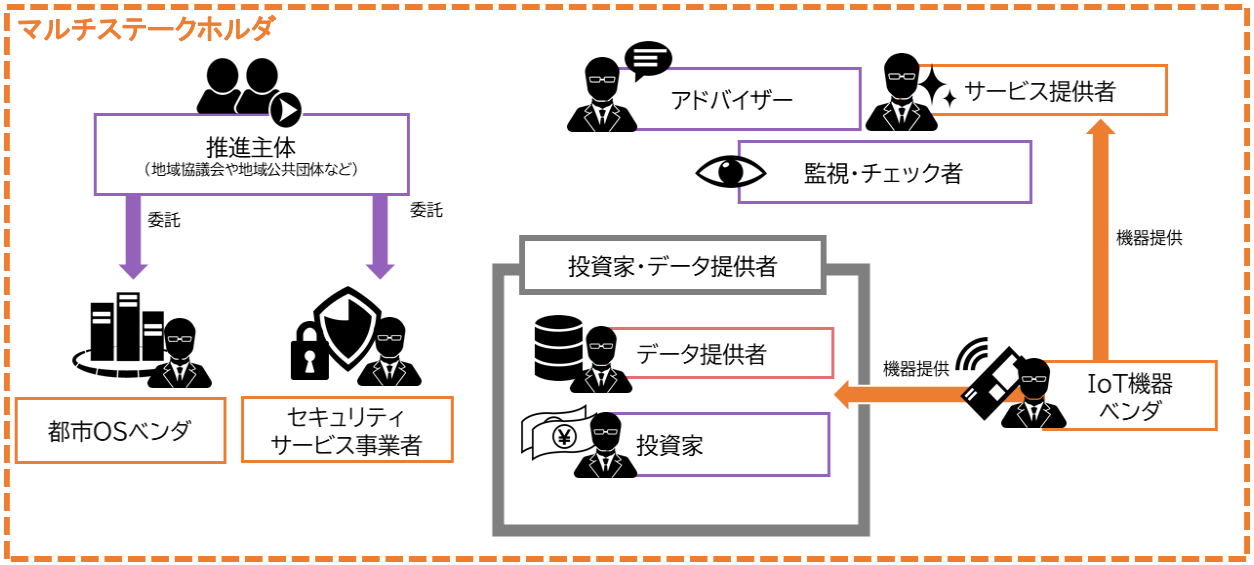
■ スマートシティでは様々な主体が複雑に関与しあうことから、ガイドライン内において登場する主体を第1章で整理・明確化。

■ よりガイドラインのスコープが明確となるよう、セーフティの観点やセキュリティ／プライバシーの線引き、取り扱う情報の前提等に関する記述を追加。

関係主体の定義

用語	定義（抜粋）
サービス提供者	スマートシティサービスを提供する主体
推進主体	スマートシティ全体の推進・運営に関して責任・決定権・主導権を持つ主体
都市OSベンダ	「推進主体」からの業務委託等を請け、都市OSの構築・運用を実施する事業者
データ提供者	「投資家・データ等提供者」の内、IoT機器等からデータを収集し、都市OSへデータを提供する事業者
IoT機器ベンダ	「データ提供者」に対してIoT機器を提供する事業者を指す
マルチステークホルダ	「サービス提供者」「推進主体」「データ提供者」「都市OSベンダ」「セキュリティサービス事業者」などのスマートシティ推進に直接的・間接的に関与する主体を総称を指す

※スマートシティリファレンスアーキテクチャの定義を踏襲しつつ、不足している点を本ガイドラインで新たに定義。



ガイドラインのスコープ（例）

管理運営面・技術面の
セキュリティ対策

事業者が実施する
セキュリティ対策

セーフティ対策を含む

データの取扱いを含む
（オープンデータのほか個人情報等のデータ）

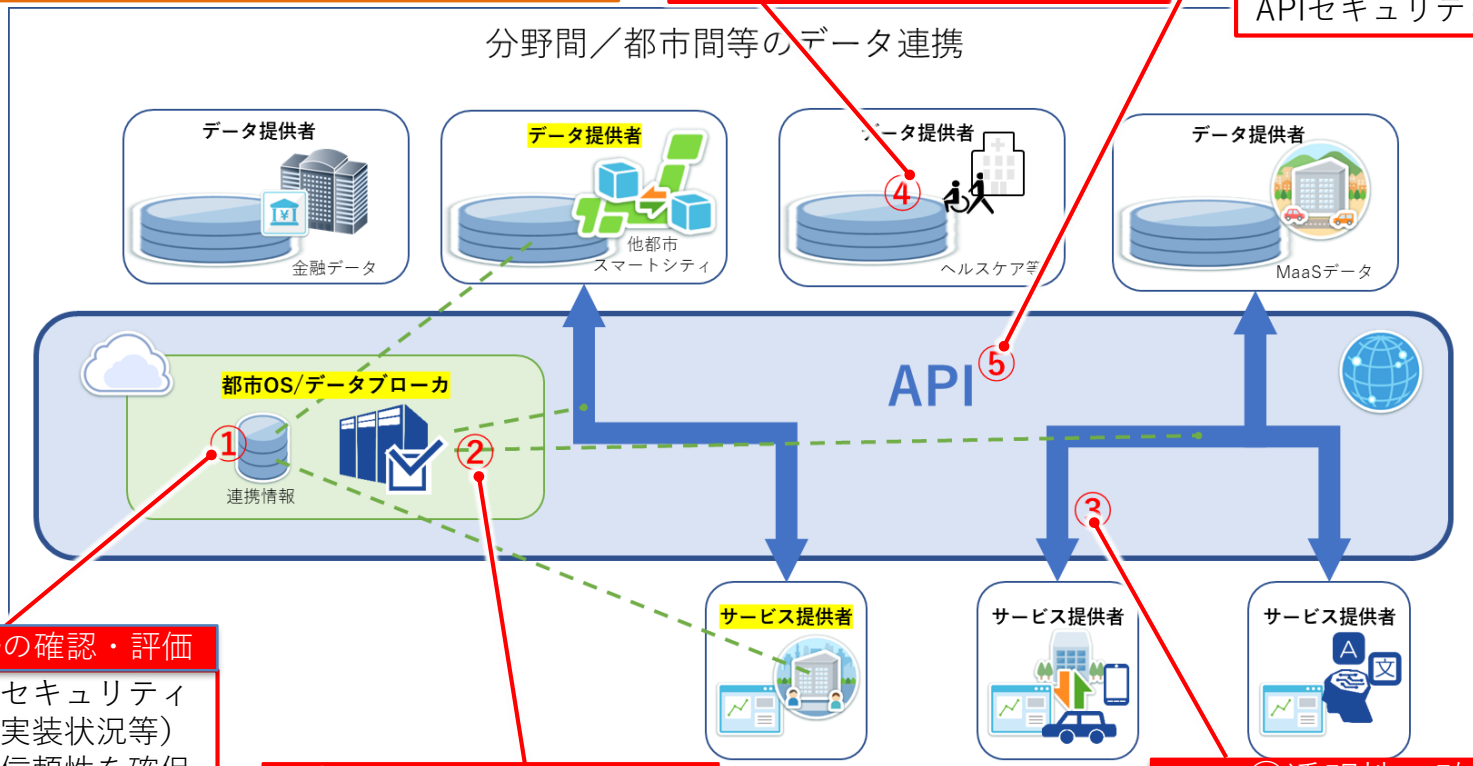
3．データ連携時のセキュリティについて

■ スマートシティ内の異なる都市ＯＳのデータ間の連携及び他のスマートシティのデータ間の連携に際して、留意すべき事項を整理。

① データ連携元・連携先のセキュリティ態勢の確認・評価
② データ提供者・サービス提供者等の認証と適切なアクセス制御
③ データの原本性保証や追跡可能性による透明性の確保
④ 必要性に応じたデータの匿名化・秘匿化
⑤ APIにおけるセキュリティ（機密性・完全性・真正性）の確保

④データの匿名化・秘匿化
データ連携元で匿名化・秘匿化した上でデータ連携を行う場合は、データ提供者側にて匿名化や秘匿化をおこなう

⑤APIセキュリティ
暗号化による改ざん・盗聴防止、APIキー認証、呼び出し先／元処理の整合性などAPIセキュリティを確保する



①セキュリティ態勢の確認・評価
接続主体との契約やセキュリティ態勢（セキュリティ実装状況等）の確認・評価による信頼性を確保する

②認証・アクセス制御
データ連携毎に認証を行い、データと接続主体とのアクセス制御を適切（動的）におこなう

③透明性の確保
データの原本性（完全性・機密性）と、データの利用途を把握するための追跡可能性を担保する

4．その他各論の改定について

■ 自治体等へのヒアリング調査結果を踏まえ、各論部分について、実態に合わせた記載の修正、新規セキュリティ対策の追加、セキュリティ対策例の追記などにより、記載内容をブラッシュアップ

第2.0版の章構成案（各論箇所を抜粋）

章節番号	タイトル
3	スマートシティにおけるセキュリティ対策
3.1	各カテゴリのセキュリティ対策
3.1.1	ガバナンス
3.1.2	サービス
3.1.3	都市OS
3.1.4	アセット
3.2	スマートシティ特有のセキュリティ対策
3.2.1	適切なサプライチェーン管理
3.2.2	インシデント対応時の連携
3.2.3	データ連携時のセキュリティ 【新規】
3.3	スマートシティ特有のセキュリティ対策事例

✓ **実態に合わせた記載の修正**
（セキュリティポリシーの策定と関係主体への浸透のプロセスに関する記載修正）

✓ **新規セキュリティ対策の追加**
（例：バックアップ、脆弱性診断対応、DDoS対策、マルウェア対策、ログ取得等）

✓ **新規セキュリティ対策の追加**
（例：脆弱性管理、アセットの一元管理・監視等）

✓ **サプライチェーンの記載の強化**
（例：委託先等の評価、サプライチェーン全体の管理、製品の脆弱性情報の把握等）

✓ **新しい章節の追加**
（データ提供者・サービス提供者等の認証と適切なアクセス制御、データの原本性保証や追跡可能性による透明性の確保等）

※3.2.1～3.2.3については、新規章節の追加に伴い再整理を実施