

# 「スマートシティセキュリティガイドライン(第3.0版)」(案) に対するご意見及びその考え方

---

総務省

- 実施期間：令和6年4月26日（金）から令和5月27日（月）まで
- 意見提出数：460件（法人：3件、個人：457件）
- 意見提出者：

	意見提出者
1	エムオーテックス株式会社
2	一般社団法人セキュアIoTプラットフォーム協議会
3	株式会社ラック
－	個人（457件）

※意見の内訳

A. ガイドライン案の内容に直接関係するご意見…5件

B. A以外で多く寄せられたご意見…455件

A. ガイドライン案の内容に  
直接関係するご意見とその考え方

# A. ガイドライン案の内容に直接関係するご意見とその考え方 3

該当箇所	提出されたご意見	ご意見に対する考え方
2. スマートシティセキュリティの考え方		
2. 3. スマートシティのセキュリティの概要		
2. 3. 1. 各カテゴリにおけるセキュリティの概要		
2.3.1.	<p>○該当箇所 P.25 2.3.1. 各カテゴリにおけるセキュリティの概要 4 アセット</p> <p>○意見内容 セキュリティ対策について設計・運用の記載がありますが、「サービス」や「都市OS」の項目と同様にデバイスなどのアセットに対して、推進主体やサービス提供者、IoT機器ベンダによってセキュリティ検証や脆弱性診断を実施する旨の記載をするべきではないでしょうか。</p> <p>○理由 特に広く、多くのデバイスを設置する必要がある場合には、サービスイン前や設置前にセキュリティに問題がないか確認しておく必要性が高いと考えられるため。</p> <p style="text-align: right;">【エムオーテックス株式会社】</p>	<p>ご意見として承ります。IoT機器デバイスなどのアセットに対しては全体的な監視・管理やアセット自体へのセキュリティ対策が必要な旨記載しているところですが、今後の更新・改定の検討にあたり、参考とさせていただきます。</p>
2.3.2.	<p>【該当箇所】</p> <ul style="list-style-type: none"> <li>・2.3.2.横断的なセキュリティの概要</li> <li>・1 適切なサプライチェーン管理</li> </ul> <p>【意見内容】 具体的な対策としてSBOM導入の有効性を記載した方がよいと考えます。</p> <p style="text-align: right;">【一般社団法人セキュアIoTプラットフォーム協議会】</p>	<p>ご意見として承ります。SBOMに関しては認識はしており、今後導入動向等を踏まえまして、更新・改定の検討にあたり、参考とさせていただきます。</p>
2.3.2.	<p>○該当箇所 P.27 2.3.2. 横断的なセキュリティの概要 2 インシデント対応時の連携</p> <p>○意見内容 「マルチステークホルダそれぞれがセキュリティインシデントに対応できる体制を構築する必要があり」とありますが、推進主体を中心とする横断的なSIRT機能も構築しておくべきではないでしょうか。</p> <p>○理由 スマートシティサービスでインシデントが発生した際には、ステークホルダそれぞれの対応だけでなく、スマートシティ全体として横断的な対応が必要になると考えられるため。</p> <p style="text-align: right;">【エムオーテックス株式会社】</p>	<p>ご意見として承ります。ガイドラインでは、「インシデント発生時にはマルチステークホルダ間で連携して対処することが求められる。」と記載しております。</p>

# A. ガイドライン案の内容に直接関係するご意見とその考え方 4

該当箇所	提出されたご意見	ご意見に対する考え方
<b>3. スマートシティにおけるセキュリティ対策</b>		
<b>3. 1. 各カテゴリのセキュリティ対策</b>		
<b>3. 1. 2. サービス</b>		
3.1.2.	<p>○該当箇所 P.42 3.1.2. サービス サービス2-6：セキュリティ監視を実施する</p> <p>○意見内容 セキュリティ監視について、IDSやIPSのような境界防御、その他改ざん検知の仕組みについて記載されています。EDRやNDR、XDRといった近年になって普及している管理ソリューションについても記載してはいかがでしょうか。</p> <p>○理由 近年では、境界防御だけでは防ぐことの難しいサイバー攻撃が増えているため。</p> <p style="text-align: right;">【エムオーテックス株式会社】</p>	<p>ご意見として承ります。EDRやNDR、XDRの導入動向等を踏まえて、今後の更新・改定の検討にあたり、参考とさせていただきます。</p>
3.1.2.	<p>○該当箇所 ・P.44 3.1.2. サービス サービス3-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する</p> <p>・P.50 都市OS2-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する</p> <p>○意見内容 「自身のシステムで利用している OS やミドルウェア、ソフトウェア等の構成管理情報を常に最新化して管理しつつ、新規の脆弱性情報を収集し、」 上記の記載について、SBOM（ソフトウェア部品表）を活用してソフトウェア等の構成管理情報を管理する文章にしてはいかがでしょうか。 案：「SBOMを活用することで、自身のシステムで利用している OS やミドルウェア、ソフトウェア等の構成管理情報を常に最新化して管理しつつ、新規の脆弱性情報を収集し、」</p> <p>○理由 近年では日本国内外でSBOMの活用の重要性が議論され、法整備も進んでいるため。</p> <p style="text-align: right;">【エムオーテックス株式会社】</p>	<p>ご意見として承ります。SBOMに関しては認識はしており、今後導入動向等を踏まえまして、更新・改定の検討にあたり、参考とさせていただきます。</p>

# A. ガイドライン案の内容に直接関係するご意見とその考え方 5

該当箇所	提出されたご意見	ご意見に対する考え方
3.1.2.	<p>○該当箇所</p> <ul style="list-style-type: none"> <li>・P.45</li> <li>3.1.2. サービス</li> <li>4 インシデント発生時に備えたセキュリティ対策</li> <li>・P.50</li> <li>3.1.3. 都市 OS</li> <li>3 インシデント発生時に備えたセキュリティ対策</li> </ul> <p>○意見内容</p> <p>定期的なバックアップの取得についての記載がありますが、新しい項目として、「インシデントからの復旧訓練」を追加してはいかがでしょうか。</p> <p>○理由</p> <p>「バックアップを定期的にとっても、インシデント発生時にバックアップからシステムやデータをうまく復旧できないケース」の発生が考えられるため。</p> <p style="text-align: right;">【エムオーテックス株式会社】</p>	<p>ご意見として承ります。取得したバックアップが復旧できない事例があり、インシデントからの復旧できないケースがあることは認識しておりますが、まずはバックアップ取得の普及浸透を推進したいと考えております。今後の更新・改定の検討にあたり、動向を踏まえまして参考とさせていただきます。</p>
<b>3. 1. 3. 都市OS</b>		
3.1.3.	<p>【該当箇所】</p> <ul style="list-style-type: none"> <li>・3.1.3.都市 OS</li> </ul> <p>【意見内容】</p> <p>コスト効率とコミュニティの透明性の観点から、スマートシティにおけるOSSの活用も記載すべきと考えます。</p> <p style="text-align: right;">【一般社団法人セキュアIoTプラットフォーム協議会】</p>	<p>ご意見として承ります。スマートシティにおける活用状況等を踏まえ、今後の更新・改定の検討にあたり、参考とさせていただきます。</p>
3.1.3.	<p>【該当箇所】</p> <ul style="list-style-type: none"> <li>・3.1.3.都市 OS</li> <li>・都市 OS 2-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する</li> </ul> <p>【意見内容】</p> <p>定期的な脆弱性診断に加えて、脆弱性管理ツールの導入が必要だと考えます。</p> <p style="text-align: right;">【一般社団法人セキュアIoTプラットフォーム協議会】</p>	<p>ご意見として承ります。脆弱性情報の管理・収集に関しては、「自身のシステムで利用しているOSやミドルウェア、ソフトウェア等の構成管理情報を常に最新化して管理しつつ、新規の脆弱性情報を収集」と記載しております。</p>

# A. ガイドライン案の内容に直接関係するご意見とその考え方 6

該当箇所	提出されたご意見	ご意見に対する考え方
<b>3. 1. 4. アセット</b>		
3.1.4.	<p>【該当箇所】</p> <ul style="list-style-type: none"> <li>・3.1.4.アセット</li> <li>・アセット 1-2：新規の脆弱性情報を把握し、ファームウェア、ソフトウェア等のバージョンアップを適切に実施する</li> </ul> <p>【意見内容】</p> <p>正しい機器に正しいソフトウェアをアップデートできるように、IoT機器の識別とソフトウェアに対するコード署名の仕組みが望まれます。</p> <p>またOTA(Over The Air)のような確実なファームウェアアップデートの仕組みが必要だと考えます。</p> <p style="text-align: right;">【一般社団法人セキュアIoTプラットフォーム協議会】</p>	<p>ご意見として承ります。OTA(Over The Air)技術が自動車等の高機能デバイスで利用が進んでいることは認識しておりますが、スマートシティで利用するIoTデバイスでの導入状況等も踏まえながら、今後の更新・改定の検討にあたり、参考とさせていただきます。</p>
3.1.4.	<p>【該当箇所】</p> <ul style="list-style-type: none"> <li>・3.1.4.アセット</li> <li>・アセット 2-2：認証機能を実装する</li> </ul> <p>【意見内容】</p> <p>ID/パスワードに加えて、クライアント証明書など電子認証の仕組みを実装することが望まれます。</p> <p style="text-align: right;">【一般社団法人セキュアIoTプラットフォーム協議会】</p>	<p>ご意見として承ります。クライアント証明書など電子認証の仕組みについて、スマートシティで利用するIoTデバイスでの導入状況等も踏まえながら、今後の更新・改定の検討にあたり、参考とさせていただきます。</p>

# A. ガイドライン案の内容に直接関係するご意見とその考え方 7

該当箇所	提出されたご意見	ご意見に対する考え方
<b>3. 2. 横断的なセキュリティ対策</b>		
<b>3. 2. 1. サプライチェーン管理</b>		
3.2.1.	<p>【該当箇所】</p> <ul style="list-style-type: none"> <li>・3.2.1. サプライチェーン管理</li> <li>・サプライチェーン 1：サプライチェーン全体のリスクを管理・把握する</li> <li>・サプライチェーン 3：サプライチェーン全体の脆弱性情報を適切に把握し、対応する</li> </ul> <p>【意見内容】</p> <p>サプライチェーン管理の重要性が記載されているが、もう少し踏み込んでサプライチェーン全体の脆弱性情報の把握と管理をどう実現するのかを記載した方がよいかと思えます。例えばSBOMを利活用したソフトウェア情報の把握と脆弱性の管理の重要性に言及すべきだと考えます。</p> <p style="text-align: right;">【一般社団法人セキュアIoTプラットフォーム協議会】</p>	<p>ご意見として承ります。SBOMに関しては認識はしており、今後導入動向等を踏まえまして、更新・改定の検討にあたり、参考とさせていただきます。</p>
3.2.2.	<p>【該当箇所】</p> <ul style="list-style-type: none"> <li>・3.2.2. インシデント対応時の連携</li> </ul> <p>【意見内容】</p> <p>実際のインシデント対応事例を追加し、具体的な対応手順を示すことで、現場での実用性を高めることができると思えます。</p> <p style="text-align: right;">【一般社団法人セキュアIoTプラットフォーム協議会】</p>	<p>ご意見として承ります。実際のインシデント対応事例は個別の事例ごとに対応が違う認識のため、対応手順は記載はいたしません。</p>
<b>3. 3. スマートシティで起こりうる問題事象と対策例</b>		
<b>3. 3. 5. データ連携先の拡大に関する問題</b>		
3.3.5.	<p>○該当箇所</p> <p>P.78</p> <p>3.3.5. データの連携先の拡大に関する問題</p> <p>コラム：海外のスマートシティ事例から得られる示唆</p> <p>○意見内容</p> <p>シンガポールの事例紹介にとどまり、「得られる示唆」にまで記述が至っていないように見受けられます。コラムタイトルを変更するか、例えば「国民に安心してスマートシティを利用してもらうためには、強固なセキュリティ対策が必要であることを示している」といったような示唆を書いてははいかがでしょうか。</p> <p>○理由</p> <p>タイトルの「示唆」が明記されていないと思われるため。</p> <p style="text-align: right;">【エムオーテックス株式会社】</p>	<p>ご意見を踏まえ、題名を「<u>コラム：海外のスマートシティ事例</u>」に修正いたします。</p>



# A. ガイドライン案の内容に直接関係するご意見とその考え方 8

該当箇所	提出されたご意見	ご意見考え方
<b>4. セキュリティ検討のための補助コンテンツ</b>		
<b>4. 2. スマートシティセキュリティ導入チェックシート</b>		
スマートシティセキュリティ導入チェックシート	○該当箇所 P.85 スマートシティセキュリティ導入チェックシート 1 マルチステークホルダへのポリシーの浸透 ○意見内容 「丸1」と記載されていますが、cの誤りではないかと思われます。 ○理由 タイトルの下に続く記載が、「ガバナンス2-1」のようにになっているため。 <div style="text-align: right;">【エムオーテックス株式会社】</div>	ご意見を踏まえ、「②マルチステークホルダへのポリシーの浸透」に修正いたします。
<b>【Appendix】 B</b>		
【Appendix】 B	○該当箇所 P.114、P.116、P.117、P.122 【Appendix】 B セキュリティ上のリスク一覧 ○意見内容 「リスク源 > 脅威」の欄に「All threats」や「All threats（再掲）」の記述が散見されますが、日本語での表記にしていた方が読み取りやすいかと思われます。 ○理由 この表記だけ英語となっていることから、唐突感があり、意味がやや読み取りづらいと感じたため。 <div style="text-align: right;">【エムオーテックス株式会社】</div>	ご意見として承ります。今後の更新・改定の検討にあたり、参考とさせていただきます。

# A. ガイドライン案の内容に直接関係するご意見とその考え方 9

該当箇所	提出されたご意見	ご意見に対する考え方
全般	<p>御省におかれましては、スマートシティのセキュリティ確保のための指針として、令和2年10月に「スマートシティセキュリティガイドライン」を策定され、引き続き、第2版を令和3年6月に策定されるなど、スマートシティを取り巻く環境の変化等を踏まえて適切な見直しを取り組みました。</p> <p>今般、ガイドラインの前提であるスマートシティリファレンスアーキテクチャの第2版の公表や事例調査の結果なども踏まえたガイドラインの見直しに取り組みられたことは、誠に時宜を得たものであり、改定案につきましては、賛同致します。</p> <p>改定案の公表により、スマートシティの推進に関わるあらゆる主体において、安全・安心なスマートシティが実現されることを期待致します。</p> <p style="text-align: right;">【株式会社ラック】</p>	<p>賛同のご意見として承ります。</p>
全般	<p>スマートシティガイドラインを拝見させていただきメールさせていただきました。今回のスマートシティセキュリティガイドラインは、セキュリティ対策はよろしいかと思えます。今現在のITを駆使して人の生活にも使用されるようになりました。10代～40代位でしたら理解をすることができますが、高齢者の方では完璧に使い方など知っている人は少なくないかと思えます。高齢者の方にもしようにできるような取り組みはあるのでしょうか？</p> <p style="text-align: right;">【個人】</p>	<p>セキュリティ対策について、賛同のご意見として承ります。</p> <p>また、スマートシティは多様な利用者の参加が想定されることから、利用者自身が安心してスマートシティのメリットを最大限享受できるように、サービス内容や利用方法、運営・問合せ先について、利用者に対して分かりやすく適切な情報発信を行うなど、スマートシティに関する情報発信の充実が重要である旨記載しております。ご意見については、今後の更新・改定の検討にあたり、参考とさせていただきます。</p>
全般	<p>スマートシティを機能させるために重要なA IとM Lの導入が記載されていない。</p> <p>運営する上で重要なマルチステークホルダの透明性の選定基準が記載されていない。</p> <p>マルチステークホルダの透明性を確保するには、以下の項目が必要では。</p> <ol style="list-style-type: none"> <li>1. 基準の明確化: 適任者がどのような資格やスキルを持っている必要があるか、明確に示す</li> <li>2. 透明性の確保: 選考基準や選定手順を公開し、関係者に情報を提供する</li> <li>3. 公平性の確保: 差別的な行動や不正行為を防止し、候補者を公平に評価する</li> <li>4. 外部監査: 独立した第三者による監査やレビューを行い、選定プロセスの適正性を確認する</li> <li>5. 候補者へのフィードバック: 候補者が自己評価を行い、今後の成長や向上に役立てることができるようにする</li> <li>6. 複数の参加者による評価: 複数の視点や意見を取り入れることで、客観的な評価が行われるようにします。</li> <li>7. 文書化と記録: 選定プロセス全ての段階を文書化し、記録を残し、選定プロセスの透明性と責任の追跡を確保する</li> </ol> <p style="text-align: right;">【個人】</p>	<p>ご意見として承ります。AIに関しては活用の増加が想定されることから、AIに関するガイドライン等の外部資料を引用しながら、AIを活用する際には、セキュリティ上の留意点を踏まえて設計・開発することを推奨する旨記載しております。AIや機械学習等の動向を踏まえて、今後の更新・改定の検討にあたり、参考とさせていただきます。</p>

B. A以外で多く寄せられた  
ご意見とその考え方

# B. A以外で多く寄せられたご意見とその考え方

提出されたご意見	ご意見に対する考え方
ガイドライン全般に反対。	
<p>※意見提出者多数のため意見本文は割愛</p> <p style="text-align: right;">【個人】</p>	<p>ガイドラインのどの部分に対する反対が明確でないため、参考意見として承ります。</p>
個人情報保護やプライバシー侵害に懸念があるため、ガイドライン全般に反対。	
<p>※意見提出者多数のため意見本文は割愛</p> <p style="text-align: right;">【個人】</p>	<p>参考意見として承ります。                      なお、プライバシー情報のセキュリティ確保については、本ガイドラインでも記載しております。</p>
5Gや6Gによる健康被害への懸念があるため、ガイドライン全般に反対。	
<p>※意見提出者多数のため意見本文は割愛</p> <p style="text-align: right;">【個人】</p>	<p>参考意見として承ります。</p>
マイナンバーカードの記載に反対。	
<p>マイナンバーカードによるトラブル、詐欺が問題になっていて、国民の不信感から普及率も上がっていません。                      そのようなものの利用を前提としている箇所には反対です。</p> <p style="text-align: right;">【個人】</p>	<p>参考意見として承ります。</p>

# B. A以外で多く寄せられたご意見とその考え方

提出されたご意見	ご意見に対する考え方
<p>スマートシティに反対。</p> <p>※意見提出者多数のため意見本文は割愛</p>	<p>【個人】</p> <p>本意見募集の対象は、スマートシティに関する方針を定めるものではなく、スマートシティに関わるステークホルダーに参考としていただけるよう必要なセキュリティ対策をガイドラインとしてまとめたものであるため、参考意見として承ります。</p>
<p>スマートシティ法及びスマートシティ法案に反対。</p> <p>※意見提出者多数のため意見本文は割愛</p>	<p>【個人】</p> <p>本意見募集の対象は、スマートシティ法やスマートシティ法案ではなく、スマートシティに関わるステークホルダーに参考としていただけるよう必要なセキュリティ対策をガイドラインとしてまとめたものであるため、参考意見として承ります。 なお、「スマートシティ法」なるものはございません。</p>
<p>反対。</p> <p>※意見提出者多数のため意見本文は割愛</p>	<p>【個人】</p> <p>ガイドラインのどの部分に対する反対意見が明確でないため、参考意見として承ります。</p>
<p>マイナンバーカードに反対。</p> <p>マイナンバーカード（または、それ以降の個人カード）の表示内容とセキュリティの確証／確認について。</p> <ol style="list-style-type: none"> <li>表示内容で、現在氏名を「漢字」で表記していますが、よみがなとローマ字を追加してください。読み方がわからない名前が最近多い。 また、外国人も取得している場合もあるが、彼らの名前の読み方がわからない場合がある。（例：林／はやし／リン）</li> <li>偽造カード対策を早急に対応してほしい。 偽造カードにより民間が損失を被った場合は、政府が金額など保障してください。（パスポートや紙幣などレベルの偽造防止はできないのでしょうか？）</li> <li>マイナンバーカードの写真を偽造される場合がある。 パスポートのように、カード上の写真と、内部のICチップ（または、その他の技術）で、来た人と間違いがないか確認ができるレベルのシステムを作ってください。（顔認証技術とかAIとか、）</li> <li>紛失などがあった場合の検索システムはあるのでしょうか？ 再発行した場合、古いカードが他の人が使用できないシステムを作ってください。（マイナンバーカードの番号／または、暗号化された番号を総務省にネットで問い合わせると、有効／無効などを判断してもらう。また、無効カードを判断するシステム）</li> </ol>	<p>【個人】</p> <p>本意見募集の対象は、マイナンバーカードに関するものではなく、スマートシティに関わるステークホルダーに参考としていただけるよう必要なセキュリティ対策をガイドラインとしてまとめたものであるため、参考意見として承ります。</p>