別紙３－２　１２．スマートシティセキュリティガイドライン導入チェックシート

	項目	チェック欄	補足説明欄（任意）
カテゴリ1　ガバナンス	①セキュリティに関するポリシーの策定		
	ガバナンス①-1：情報セキュリティ基本方針を策定する 目的や対象範囲など基本的な事項のほか、セキュリティを担保するための取組方針が記載された情報セキュリティ基本方針を策定する	①既に対応済み ②これから対応予定（〇月） ③対応の予定なし ※当てはまる番号を記載ください。	
	ガバナンス①-2：セキュリティ対策基準を策定する 組織体制や情報資産の分類・管理に関する項目のほか、管理的及び技術的なセキュリティ対策等について具体的な遵守事項や判断基準等を定めたセキュリティ対策基準を策定する		
	ガバナンス①-3：データ取扱い基準を策定する スマートシティで取り扱われるデータを分類するとともに、適切なデータの取扱いに関する事項や、法令等への対応等を定めたデータ取扱い基準を策定する		
	ガバナンス①-4：インシデント対応手順を策定する インシデント対応に関与する関係主体やそれぞれの責任範囲の明確化、連絡体制や連絡先などの整備、対応における判断基準やインシデント対応フロー等のインシデント対応手順を策定する		
	ガバナンス①-5：事業継続計画を策定する 障害やセキュリティ事故等が発生した際にどの機能を優先して保護するかといった判断基準や、スマートシティ事業継続のための役割分担、対応手順等を定めた事業継続計画を策定する		
	ガバナンス①-6：委託先や提携先の評価基準を策定する セキュリティ管理体制やセキュリティに関する第三者認証の取得有無等、外部委託等を実施する際に求めるべき内容や選定条件などを定めた評価基準を策定する		
	ガバナンス①-7：リスクアセスメントを実施する スマートシティの全体構成や守るべき機能や情報資産を踏まえ、リスク評価を実施する		
	ガバナンス①-8：法令やガイドライン等との整合性を確認する スマートシティのセキュリティに関するポリシー策定時に、自身のスマートシティにおいて遵守することが求められる法令を把握する。また、それらの法令が遵守できる形でガイドラインを参考としながらポリシーを策定する。		
	ガバナンス①-9：各種文書の作成や各活動の記録を取り共有・管理する機能を整備する 様々な方針・基準・手順をステークホルダに浸透させ、必要な文書改訂とそれらを共有・管理するための体制および機能を整備する		
	②マルチステークホルダへのポリシーの浸透		
	ガバナンス②-1：ポリシーを遵守するためのセキュリティ要件を調達仕様書に反映する セキュリティに関するポリシーに則り、情報セキュリティの管理体制の構築やセキュリティインシデントへの対処などのセキュリティ要件を調達仕様書に反映させる		
	ガバナンス②-2：データ取扱い基準を契約・規約に反映する データの流通や利活用における取扱いについて、データ取扱い基準で定めた内容を委託先や提携先との契約・規約に反映する		
	ガバナンス②-3：契約・規約で責任範囲を明確化する システムの責任分界点とデータの責任分界点を委託先や提携先との契約・規約の中で明確化する		
	ガバナンス②-4：接続を希望する事業者のセキュリティ対応レベル審査・監査 スマートシティに接続を希望する事業者のセキュリティ対応レベルを評価する ために、事前にプロセスや役割を整理する		
	ガバナンス②-5：運営関係者に対する定期的なトレーニングを実施する スマートシティの運営関係者に対する教育や情報提供を目的としたトレーニングを 定期的に実施する		
	③ガバナンス維持のための取組		
	ガバナンス③-1：継続的なリスクアセスメントの実施とセキュリティに関するポリシーの見直しを実施する 提供するサービスの変化や脅威の拡大等に応じ、継続的にリスクアセスメントを実施し、セキュリティに関するポリシーの見直しを実施する		
	ガバナンス③-2：セキュリティ対策への適切な投資を継続的に実施する セキュリティの維持・向上を図るため、セキュリティ対策への適切な投資を継続的に実施する		
	ガバナンス③-3：ユーザに対する情報発信やリテラシ向上の取り組みを実施する 利用者に対して適切な情報発信の場や、IT リテラシのトレーニング機会を設けるなどの取り組みを、検討・実施する		

カテゴリ2 サービス	①サービス個別でのリスクアセスメントの実施		
	サービス①-1：それぞれのサービスにおいてリスクアセスメントを実施する 個々のサービスにおいて守るべき情報資産や機能を特定した上で、リスクアセスメントを実施する		
	② 外部からの攻撃等を防ぐセキュリティ対策		
	サービス②-1：サービスの不正な利用を規約・契約で抑止する サービスの利用開始やアカウント登録時に、運営に支障を与える行為等の禁止事項を明確にし、それらが疑われる場合にはアカウント停止、損害賠償等の必要な措置を取ることに対し同意取得をする		
	サービス②-２：サービスへのアクセス制御を実装、運用する 外部からサービスに関わるシステムに通信をする場合は、ファイアウォール等を実装し、適切なアクセス制御を実装する		
	サービス②-３：適切な権限設定を実施し、管理する 必要な人や役割などに限定した権限設定を行い、アカウントの一覧表を作成し、定期的に棚卸しするなどして適切に管理する		
	サービス②-4：身元確認機能を実装する サービス利用登録時や必要なタイミングで身元確認を適切に行い、サービスを提供可能か判断する		
	サービス②-５：認証機能を実装する アクセスした人が本人であるかを確認するための認証機能を実装する		
	サービス②-６：セキュリティ監視を実施する IDSやIPS、WAFなどを設置し、外部からの不正なコマンドが含まれた通信等のシステムへのサイバー攻撃を監視する		
	③ セキュリティインシデント発生の未然防止のためのセキュリティ対策		
	サービス③-1：サービスの企画・設計・開発工程における脆弱性を適切に管理する セキュア設計やセキュアコーディング、サービスイン前のセキュリティテストや脆弱性診断などによってサービスの企画・設計・開発工程における脆弱性を適切に管理する		
	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 定期的な脆弱性診断の実施や、継続的な脆弱性情報の収集によって自システムの脆弱性を把握しつつ、構成情報を適切に管理し、それらの情報を元に適切にバージョンアップやセキュリティパッチの適用等の対策を実施する		
	サービス③-3：運用管理端末へのセキュリティ対策を実施する システムへ直接アクセスが可能な運用管理端末は、当該端末へのアクセス制御と認証の導入をした上で、ウィルス対策ソフトの導入、OS等の脆弱性への対応、物理的なアクセス制限等の対策を実施する		
	④インシデント発生時に備えたセキュリティ対策		
	サービス④-1：外部との通信やデータの暗号化を実施する 外部との通信やシステムに保存されるデータは十分な強度の暗号アルゴリズムで暗号化を実施する		
	サービス④-2：定期的にバックアップを取得する システムの構成情報や重要なデータは定期的にバックアップし、災害や復旧を踏まえた保管を行う		
	サービス④-3：証跡確保のためのログを取得する 証跡を確保するための様々なログを取得し、適切に保管する		
	サービス④-4：インシデント発生時のリスク軽減策を検討する セキュリティインシデントが発生に備え、セキュリティインシデント対応体制が構築されていることを確認する		

カテゴリ3　都市OS	①外部からの攻撃、侵入等を防ぐセキュリティ対策		
	都市OS①-1：都市OSへのアクセス制御を実装、運用する 外部から都市OSに関わるシステムに通信をする場合は、ファイアウォール等を実装し、適切なアクセス制御を実装する		
	都市OS①-2：適切な権限設定を実施し、管理する 必要な人や役割などに限定した権限設定を行い、アカウントの一覧表を作成し、定期的に棚卸しするなどして適切に管理する		
	都市OS①-3：認証機能を実装する アクセスした人が本人であるかを確認するための認証機能を実装する		
	都市OS①-4：セキュリティ監視を実施する IDSやIPSを設置し、不正なコマンドが含まれた通信等のシステムへのサイバー攻撃を監視する		
	② セキュリティインシデント発生の未然防止のためのセキュリティ対策		
	都市OS②-1：都市OSの企画・設計・開発工程における脆弱性を適切に管理する 都市OSを構成するシステムの企画・設計・開発等の各段階においてセキュリティを検討・実施する		
	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 定期的な脆弱性診断の実施や、継続的な脆弱性情報の収集によって自システムの脆弱性を把握しつつ、構成情報を適切に管理し、それらの情報を元に適切にバージョンアップやセキュリティパッチの適用等の対策を実施する		
	都市OS②-3：運用管理端末へのセキュリティ対策を実施する システムへ直接アクセスが可能な運用管理端末は、当該端末へのアクセス制御と認証の導入をした上で、ウィルス対策ソフトの導入、OS等の脆弱性への対応、物理的なアクセス制限等の対策を実施する		
	③ インシデント発生時に備えたセキュリティ対策		
	都市OS③-1：外部との通信やデータの暗号化を実施する 外部との通信やシステムに保存されるデータは十分な強度の暗号アルゴリズムで暗号化を実施する		
	都市OS③-2：定期的にバックアップを取得する システムの構成情報や重要なデータは定期的にバックアップし、災害や復旧を踏まえた保管を行う		
	都市OS③-3：証跡確保のためのログを取得する 証跡を確保するための様々なログを取得し、適切に保管する		
	④ 推進主体からの要求に応じた適切なクラウドサービスの利用		
	都市OS④-1：クラウドサービスの利用者と提供事業者間の責任分界点を把握する クラウド基盤としてIaaS/PaaSを利用する場合、責任分界点について正確に把握し、それに応じたセキュリティ対策を実施する		
	都市OS④-2：データロケーションに関する推進主体からの要求事項に対応する クラウド基盤を利用する場合、都市OS上で取り扱うデータの種類や適用される法令を理解した上で、クラウドの設置場所（リージョン）に関する推進主体からの要求事項に対応できているかを確認し利用する		
	都市OS④-3：複数リージョン選択等により、可用性を担保する クラウド基盤を利用する場合、障害や復旧の観点から複数リージョンの選択を検討する		

カテゴリ4　アセット	① アセットの監視・管理		
	<u>アセット①-1：アセットの監視・管理を実施する</u> アセットの死活監視をしたうえで、バージョン情報などの基本的な情報を管理する		
	<u>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</u> アセットの脆弱性情報を継続的に収集・把握し、適切なタイミングでバージョンアップの対応を行う		
	② アセットそのものへのセキュリティ対策		
	<u>アセット②-1：外部との通信や、保有するデータを暗号化する</u> アセットと外部との通信やアセットで保有するデータは十分な強度の暗号アルゴリズムで暗号化を実施する		
	<u>アセット②-2：認証機能を実装する</u> アセットにアクセスする際の認証機能を実装する。パスワードは工場出荷状態でのデフォルトパスワードや容易なパスワードを避け、サービス利用者側でデバイス管理をする場合は、適切なパスワードの設定や管理などの注意喚起をする		
	<u>アセット②-3：物理的なセキュリティ対策を実施する</u> デバイスに対する物理的な破壊や盗難からの保護対策を行う。誤動作が起きたとしても人命への影響が発生しないよう、フェイルセーフを考慮した設計をする。また、デバイスを廃棄する場合は物理的に破壊するなど情報漏洩対策を実施する		

項目		チェック欄	補足説明欄（任意）
スマートシティ特有のセキュリティ対策	1　適切なサプライチェーン管理		
	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 スマートシティ全体における、委託先・再委託先も含めたマルチステークホルダ全体のサプライチェーン・リスク（委託先等の立地する場所の法的環境等による影響や供給安定性に対するリスクを含む）を把握し、そのリスクへの対策を検討する	①既に対応済み ②これから対応予定（〇月） ③対応の予定なし ※当てはまる番号を記載ください。	
	サプライチェーン②：委託先／提携先のセキュリティ管理体制を評価する チェックシートや第三者認証の取得状況などを活用し、委託先のセキュリティ 管理体制を評価する。契約期間中においても継続的に確認・評価し、不十分な 点があれば改善を求める		
	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 継続的な脆弱性への対応が期待できるソフトウェアやハードウェアを選定するとともに、サプライチェーン間の契約や、調達時の仕様に脆弱性情報を適切に提供し、対応するといった記載を盛り込むことで、脆弱性情報を適切に把握し、対応できるようにする		
	サプライチェーン④：提携主体はステークホルダ毎の責任分界点を明確にする 推進主体とステークホルダ間の契約形態（業務委託・業務提携など）によって責任 を追う先が異なるため、提供するサービス等の責任範囲を明確にする		
	2　インシデント対応時の連携		
	インシデント対応①：責任範囲を明確にしたセキュリティインシデント対応体制を構築する セキュリティインシデントが発生した際の対応に関する責任分界点を明示したセキュリティインシデント対応体制を構築する		
	インシデント対応②：連絡窓口を整備し、マルチステークホルダ間で相互に共有する セキュリティインシデントの発生に備え、マルチステークホルダ間の連絡体制や緊急連絡先を予め把握・整備し、共有する		
	インシデント対応③：スマートシティ全体及び各マルチステークホルダにおけるインシデント対応手順を整備する セキュリティインシデントが発生に備え、それぞれのマルチステークホルダ内及びスマートシティ全体としてのインシデント対応手順を整備する		
	インシデント対応④：定期的にセキュリティインシデント対応訓練・演習を実施する インシデント対応手順や自組織内、組織外との連携対応の習熟などを目的とした、インシデント対応訓練・演習を実施する		
	インシデント対応⑤：新たな脅威やインシデント事例などの情報収集・分析する レジリエンス強化のため、インシデント対応関係者は新たな脅威やインシデント 事例などを情報収集し共有・学習を行い、既存の対応手順などの見直しを行う		
	3　データ連携時のセキュリティ		
	データ連携①：データ連携元・連携先のセキュリティ体制の確認・評価を実施する データの連携元・連携先組織のセキュリティマネジメントを、チェックシートや第三者認証の有無等を活用して確認し、評価する		
	データ連携②：データ提供事業者・サービス提供者等の認証と適切なアクセス制御を実施する 連携するデータの内容や個人情報の同意内容に沿った利用目的等を踏まえ、認証と適切なアクセス制御の付与することで適切なデータ連携を行う		
	データ連携③：データの追跡可能性を確保しデータ利用の透明性を担保する データ利用で生じるアクセスログやシステムログを取得し、分析・監視することで、データの追跡可能性を確保し、データ利用の透明性を担保する。		
	データ連携④：データの原本性保証を確保しデータの信頼性を担保する デジタル署名、電子透かしなど技術を活用し、原本性保証を確保することでデータの信頼性を担保する		
	データ連携⑤：必要性に応じたデータの匿名化・秘匿化を実施する データを提供する個人がそれを要望する場合等、必要性に応じてデータの提供元において匿名化・秘匿化の処理を行う		
	データ連携⑥：APIにおけるセキュリティ（機密性・完全性・可用性・真正性）を確保する APIの利用では認証や通信の暗号化、公開鍵暗号基盤の利用、サーバへの負荷対策、クロスドメインの通信を許可するなど、APIにおけるセキュリティを考慮する		