「スマートシティセキュリティガイドライン（第2.0版）」（案）への御意見に対する考え方

別紙1

※提出されたご意見のうち、公表を希望しない提出意見が1件あり

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
1	法人A（ヴイエムウェア株式会社）	2. スマートシティセキュリティの考え方	（スマートシティセキュリティガイドライン（第2.0版）（案）P21中「プラットフォーム単体のセキュリティとして一般的なクラウドセキュリティの実装が求められる。都市OS の構築・運用を担うのは都市OSベンダであり、セキュリティ対策の実施も都市OS ベンダが中心となって実施する必要がある。」との記載部分） ・意見内容 当該部分について「プラットフォーム単体のセキュリティ として一般的なクラウドセキュリティの実装が求められる。また、複数のスマートシティのおける都市OSの連携及びクラウド間連携を考慮したネットワークセキュリティの実装が求められる。都市 OS の構築・運用を担うの は都市 OS ベンダであり、セキュリティ対策の実施も都市 OS ベンダが中心となって実施する必要がある。」との変更を提案します。 （理由） スマートシティの進展により、都市OSにおいて複数のクラウド基盤の連携が必要とされることは明らかであり、また、複数のクラウド基盤の連携において当該“連携を考慮したネットワークセキュリティ”は同ページ後段にある単一のサービスを前提としたセキュリティ機能とは別のものであることから、連携を考慮したセキュリティ機能に言及することが必要です。 そのため「複数のスマートシティのおける都市OSの連携及びクラウド間連携を考慮したネットワークセキュリティの実装」との文言でその必要性を明示することを提案します。	都市OS間の連携に関する記述はP52「3.2.3.データ連携時のセキュリティ」に記載があること、クラウド間連携を考慮したネットワークセキュリティはクラウドセキュリティの一つの要素であり、それだけに言及することは不適切であることから、P21の記載について以下のとおり修正します。 「一般的なクラウドセキュリティの実装が求められる。」 ⇒「クラウド同士の連携やクラウドの特性を考慮したクラウドセキュリティの実装が求められる」	有
2	法人B（株式会社ラック）	2. スマートシティセキュリティの考え方	「図2-4スマートシティ組織のイメージ」の上段の関係図におきまして、「Dアドバイザー」の”助言”と「E監視・チェック者」の”指導”が相反することはないのか懸念いたします。双方の定義をより明確にしていただくようご提案いたします。	図2-4中において、「アドバイザー」及び「監視・チェック者」の定義を追記いたします。	有
3	法人B（株式会社ラック）	2. スマートシティセキュリティの考え方	「図2-12都市OS におけるセキュリティ上のリスクのイメージ」、「図2-13アセットにおけるセキュリティ上のリスクのイメージ」と関連する章において、それぞれの運用に関わる事業者内の仕組みに関しても、セキュリティ対策について言及する必要があると考えます。また、それらの不足機能を補う目的での「共通プラットフォーム」となる機能の定義について今後検討を進める必要があると考えます。	各事業者におけるセキュリティ管理体制の必要性に関しては、「サプライチェーン②：委託先のセキュリティ管理体制を評価する」に言及されています。 また、「共通プラットフォーム」の必要性やあるべき姿については、今後の検討課題として承りました。	無
4	法人A（ヴイエムウェア株式会社）	3. スマートシティにおけるセキュリティ対策	（「スマートシティセキュリティガイドライン（第2.0版）（案）P39 後段「都市OSを構成するサーバ等が配置されているセグメントに外部から通信をする場合は、ファイアウォール等を実装する等し、適切なアクセス制御を実装する必要がある。」との記載部分） ・意見内容 当該部分について「都市OSを構成するサーバ等が配置されているセグメントに外部から通信をする場合及び同一セグメント内に配置されているシステム間で通信する場合は、ファイアウォール等を実装する等し、適切なアクセス制御を実装する必要がある。」との変更を提案します。 （理由） 攻撃手法が巧妙化する現在の情勢において、外部攻撃への対策として、外部との境界における対策はもちろんのこと、同一セグメント内であってもシステム間での通信をチェック、制御、検知する等の内部対策を行い、内部に侵入した攻撃を早期検知して対処する必要があります。 『地方公共団体における情報セキュリティポリシーに関するガイドライン(令和2年12月版）』における[不正アクセス対策]-[標的型攻撃]（ii-41）においても下記が明示されています。 https://www.soumu.go.jp/main_content/000727474.pdf 「統括情報セキュリティ責任者及び情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。」 「都市OSへのアクセス制御を実装、運用する」という本項目をより確実に行うため、変更を提案します。	いただいたご意見の趣旨を踏まえ、当該箇所（P39）に以下の文言を追記いたします。 「なお、外部からの通信に限らず、システム内の他セグメントからの通信や同一セグメント内の通信においても適切なアクセス制御の実装は必要である点に注意する。」	有

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
5	法人A（ヴイエムウェア株式会社）	3. スマートシティにおけるセキュリティ対策	（「スマートシティセキュリティガイドライン（第2.0版）（案）P36中「ネットワークにおけるセキュリティ監視としては、インターネットとシステムの境界にIDS（不正侵入検知システム）やIPS（不正侵入防止システム）を設置し、それを監視することによって、不正なコマンドが含まれた通信等を検知、遮断することが可能となる。」との記載部分） ・意見内容 当該部分について「ネットワークにおけるセキュリティ監視としては、インターネットとシステムの境界にIDS（不正侵入検知システム）やIPS（不正侵入防止システム）を設置し、それを監視すること、及び提供するサービスや取り扱うデータにあわせて、内部通信においてもIDS及びIPSを行うための必要な設定を行うことによって、不正なコマンドが含まれた通信等を検知、遮断することが可能となる。」との変更を提案します。 （理由） NIST SP800-207等に示される通り、サービスによってはマイクロセグメンテーションによるより細かい監視が必要なケースがあります。よってインターネットとシステムの境界のみならず、内部通信においてもIDS/IPSによる監視を実施する事により、内部に侵入した攻撃を検知する内部対策が必要です。 「セキュリティ監視を実施する」という本項目をより確実に行うため、変更を提案します。	いただいたご意見の趣旨を踏まえ、該当箇所（P36）に以下の文言を追記します。 「同一システム内に複数のセグメントが存在する場合は、セグメント間の通信においてもIDS/IPSによる監視が有効な場合がある。」	有
6	法人A（ヴイエムウェア株式会社）	3. スマートシティにおけるセキュリティ対策	（「スマートシティセキュリティガイドライン（第2.0版）（案）P40後段「ネットワークにおけるセキュリティ監視としては、インターネットとシステムの境界にIDS（不正侵入検知システム）やIPS（不正侵入防止システム）を設置し、それを監視することによって、不正なコマンドが含まれた通信等を検知、遮断することが可能となる。」との記載部分） ・意見内容 当該部分について「ネットワークにおけるセキュリティ監視としては、インターネットとシステムの境界にIDS（不正侵入検知システム）やIPS（不正侵入防止システム）を設置し、それを監視すること、及び提供するサービスや取り扱うデータにあわせて、内部通信においてもIDS及びIPSを行うための必要な設定を行うことによって、不正なコマンドが含まれた通信等を検知、遮断することが可能となる。」との変更を提案します。 （理由） NIST SP800-207等に示される通り、都市OSによってはマイクロセグメンテーションによるより細かい監視が必要なケースがあります。よってインターネットとシステムの境界のみならず、内部通信においてもIDS/IPSによる監視を実施する事により、内部に侵入した攻撃を検知する内部対策が必要です。 「セキュリティ監視を実施する」という本項目をより確実に行うため、変更を提案します。	いただいたご意見の趣旨を踏まえ、該当箇所（P40）に以下の文言を追記します。 「同一システム内に複数のセグメントが存在する場合は、セグメント間の通信においてもIDS/IPSによる監視が有効な場合がある。」	有
7	法人A（ヴイエムウェア株式会社）	3. スマートシティにおけるセキュリティ対策	（「スマートシティセキュリティガイドライン（第2.0版）（案）P32 後段「そのため、リスクアセスメントの時期を予算要求前に設定し、アセスメント結果を元に適切なセキュリティ対策を決定することで、効率的にセキュリティへの投資をしつつセキュリティの維持・向上を図ることができる。」との記載部分） ・意見内容 当該部分について「そのため、リスクアセスメントの時期を予算要求前に設定し、アセスメント結果を元に適切なセキュリティ対策を決定することで、効率的にセキュリティへの投資をしつつセキュリティの維持・向上を図ることができる。また、アセスメントにおいては、利用するクラウドサービスの構成、設定などが事前に定義するポリシーに準拠しているかを確認する。」との変更を提案します。 （理由） クラウドサービスの利用者自身による設定ミスや構成ミスを突いたインシデント及び外部からの攻撃が既に発生しており、従来のセキュリティ対策への投資に加えて利用者自身のミスをセキュリティ対策の一部とする投資が必要です。継続的なセキュリティ対策の適切な投資の一つとしてポリシー準拠の確認を明示し、その周知を図るため、変更を提案します。	いただいたご意見（ポリシーの準拠の確認）については、P30「②　マルチステークホルダへのポリシーの浸透」において、同趣旨の内容が記載されているため、原案のとおりとします。	無

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
8	法人A（ヴイエムウェア株式会社）	3. スマートシティにおけるセキュリティ対策	（「スマートシティセキュリティガイドライン（第2.0版）（案）P34 後段「サービスに関わるシステムが配置されているセグメントに外部から通信をする場合は、ファイアウォール等を実装する等し、適切なアクセス制御を実装する必要がある。」との記載部分） ・意見内容 当該部分について「サービスに関わるシステムが配置されているセグメントに外部から通信をする場合及び同一セグメント内に配置されているシステム間で通信する場合は、ファイアウォール等を実装する等し、適切なアクセス制御を実装する必要がある。」との変更を提案します。 （理由） 攻撃手法が巧妙化する現在の情勢において、外部攻撃への対策として、外部との境界における対策はもちろんのこと、同一セグメント内であってもシステム間での通信をチェック、制御、検知する等の内部対策を行い、内部に侵入した攻撃を早期検知して対処する必要があります。 『地方公共団体における情報セキュリティポリシーに関するガイドライン(令和 2 年 12 月版）』における[不正アクセス対策]-[標的型攻撃]（ii-41）においても下記が明示されています。 https://www.soumu.go.jp/main_content/000727474.pdf 「統括情報セキュリティ責任者及び情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。」 「サービスへのアクセス制御を実装、運用する」という本項目をより確実に行うため、変更を提案します。	いただいたご意見の趣旨を踏まえ、当該箇所（P34）に以下の文言を追記いたします。 「なお、外部からの通信に限らず、システム内の他セグメントからの通信や同一セグメント内の通信においても適切なアクセス制御の実装は必要である点に注意する。」	有
9	法人A（ヴイエムウェア株式会社）	3. スマートシティにおけるセキュリティ対策	（「スマートシティセキュリティガイドライン（第2.0版）（案）P37中段「そのため、運用管理端末へのアクセス制御の実施や認証の導入はもちろん、ウィルス対策ソフトの導入やOS等の脆弱性への対応といった、基本的なセキュリティ対策の実施が必要となる。」との記載部分） ・意見内容 当該部分について「そのため、運用管理端末へのアクセス制御の実施や認証の導入はもちろん、ウィルス対策ソフトの導入、道の不正プログラムへの対策、OS等の脆弱性への対応、OSやドライバ等のシステム動作のログ及びファイルやレジストリへの読み書きに関連する全てのログの取得、疑義端末を発見した場合に当該疑義端末の隔離やシステム停止を自動的に行うことといった、基本的なセキュリティ対策の実施が必要となる。」との変更を提案します。 （理由） 運用管理端末へのセキュリティ対策として、未知の不正プログラムへの対策や驚異検出に必要となる端末上のOSやドライバ等のシステム動作のログ及びファイルやレジストリへの読み書きに関連する全てのログの取得は、従来のパターンマッチング型で検出できない数多くの攻撃に対するエンドポイントセキュリティ対策として基本的な事項です。またそれら驚異検出時への迅速な対応のために被疑端末の隔離を自動化することが必要です。 「運用管理端末へのセキュリティ対策を実施する」という本項目をより確実に行うため、変更を提案します。	いただいたご意見の趣旨及び当該箇所の記載粒度を考慮し、当該箇所は以下の通り修文します。 「ウィルス対策ソフトの導入やOS等の脆弱性への対応といった、基本的なセキュリティ対策の実施が必要となる。」 ⇒「ウィルス対策ソフトの導入や未知の不正プログラムへの対策、OS等の脆弱性への対応、運用管理端末でのシステム動作ログ等の取得といった、基本的なセキュリティ対策の実施が必要となる。」	有
10	法人A（ヴイエムウェア株式会社）	3. スマートシティにおけるセキュリティ対策	（「スマートシティセキュリティガイドライン（第2.0版）（案）P42上段「そのため、運用管理端末へのアクセス制御の実施や認証の導入はもちろん、ウィルス対策ソフトの導入やOS等の脆弱性への対応といった、基本的なセキュリティ対策の実施が必要となる。」との記載部分） ・意見内容 当該部分について「そのため、運用管理端末へのアクセス制御の実施や認証の導入はもちろん、ウィルス対策ソフトの導入、道の不正プログラムへの対策、OS等の脆弱性への対応、OSやドライバ等のシステム動作のログ及びファイルやレジストリへの読み書きに関連する全てのログの取得、疑義端末を発見した場合に当該疑義端末の隔離やシステム停止を自動的に行うことといった、基本的なセキュリティ対策の実施が必要となる。」との変更を提案します。 （理由） 運用管理端末へのセキュリティ対策として、未知の不正プログラムへの対策や驚異検出に必要となる端末上のOSやドライバ等のシステム動作のログ及びファイルやレジストリへの読み書きに関連する全てのログの取得は、従来のパターンマッチング型で検出できない数多くの攻撃に対するエンドポイントセキュリティ対策として基本的な事項です。またそれら驚異検出時への迅速な対応のために被疑端末の隔離を自動化することが必要です。 「運用管理端末へのセキュリティ対策を実施する」という本項目をより確実に行うため、変更を提案します。	いただいたご意見の趣旨及び当該箇所の記載粒度を考慮し、当該箇所は以下の通り修文します。 「ウィルス対策ソフトの導入やOS等の脆弱性への対応といった、基本的なセキュリティ対策の実施が必要となる。」 ⇒「ウィルス対策ソフトの導入や未知の不正プログラムへの対策、OS等の脆弱性への対応、運用管理端末でのシステム動作ログ等の取得といった、基本的なセキュリティ対策の実施が必要となる。」	有

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
11	法人A（ヴイエムウェア株式会社）	3. スマートシティにおけるセキュリティ対策	（「スマートシティセキュリティガイドライン（第2.0版）（案）P43中段「また、クラウドサービスによってはサーバが海外のデータセンタに位置することもあるため、推進主体からの要求を反映できるようなクラウドサービス選定やリージョンの選択などが求められる。」との記載部分） ・意見内容 当該部分について「また、クラウドサービスによってはサーバが海外のデータセンタに位置することもあるため、推進主体からの要求を反映できるようなクラウドサービス選定やリージョンの選択などが求められる。特にクラウドサービス選定やリージョンの選択をする上ではサービスで提供されるSLA（Service Level Agreement）に留意する必要がある。」との変更を提案します。 （理由） 『都市OS(4)-3』においてリージョン間での可用性に関して言及されており、クラウドサービスのSLAに関しては、利用するサービス、構成により大きく異なるため、クラウドサービス選定やリージョンの選択にあたっては、SLAを意識すべきことを明記する必要があります。 「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」という本項目をより確実に行うため、変更を提案します。	原文にある「推進主体からの要求」の中にサービスの可用性（SLA）に関する要求が含まれている事から、いただいたコメントの趣旨を考慮し、当該箇所は以下の通り修文します。 「また、クラウドサービスによってはサーバが海外のデータセンタに位置することもあるため、推進主体からの要求を反映できるようなクラウドサービス選定やリージョンの選択などが求められる。」 ⇒「また、クラウドサービスによってはサーバが海外のデータセンタに位置することもあるため、推進主体からのデータロケーションやサービスの可用性（SLA）に関する要求を実現できるようなクラウドサービス選定やリージョンの選択などが求められる。」	有
12	法人B（株式会社ラック）	3. スマートシティにおけるセキュリティ対策	「インシデント対応時の連携」と関連する章において、地域の警察や消防等の公的団体との連携も含め、今後具体性を持たせる必要があると考えます。	いただいたご意見を踏まえ、P52のインシデント対応時の連携先に関する記述を以下のとおり修正いたします。 「主管官庁や警察、JPCERT/CCなど」 ⇒「主管官庁や警察などの公的機関、JPCERT/CCなど」	有
13	法人B（株式会社ラック）	3. スマートシティにおけるセキュリティ対策	「③データ連携時のセキュリティ」と関連する章において、自都市のスマートシティ外の連携によるリスクには、案に記載いただいた「データの改ざんや消失」の他に、データの定義の錯誤による意味付けの誤り、またその結果によるスマートシティ内に誤ったデータが流通することによる適切なサービス提供の阻害・信頼の失墜などもあるのではないかと存じます。この点につきまして、記載の充実を要望いたします。	いただいたご意見の趣旨を踏まえ、P55「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」の記載を下記のとおり修正いたします。 「利用先においてデータが加工されてしまうことで」 ⇒「利用先においてデータが加工されてしまったり、データの定義が誤って設定されてしまうことで」	有
14	法人C（一般社団法人重要生活機器連携セキュリティ協議会）	3. スマートシティにおけるセキュリティ対策	・P.29、「ガバナンス①-7 ：リスクアセスメントを実施する」 ■意見区分： ③ガイドライン案の記載に対する追加要望 ■意見内容： 利用者の安全や人命に影響する脅威については、リスク評価の方法を、検討する必要するのではないか。 ■理由： 本書で記載されている通り、災害対策サービス、高齢者の見守りや医療システムとの連携を想定した場合、間接的に人命に影響するリスクが想定される。 本書のリスクアセスメントでは「資産や機能に対して発生する可能性のある脅威とその発生確率、発生した場合の影響度を評価する」とあるが、上記のようなケースでは、従来の情報セキュリティにおける影響度の考え方では、適切なリスク評価が難しいのではないか。下記の文書における安全や健康、人命に影響するリスク評価基準について、追記及び出典文書の掲載をご検討いただきたい。 ■出典・参考文書： ・下記の文書では安全や健康、人命に影響する脅威に対するリスク評価基準を提唱している。 [1]一般社団法人重要生活機器連携セキュリティ協議会（CCDS）、「CCDS製品分野別セキュリティガイドライン_スマートホーム編_Ver.1.0」 https://www.ccds.or.jp/public_document/index.html#20201124_report2 [2][Caralli 2007] Caralli, Richard; Stevens, James; Young, Lisa; Wilson, William. “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.” CMU/SEI-2007-TR-012. Carnegie Mellon University, Software Engineering Institute, May 2007. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf	いただいたご意見の趣旨を踏まえ、P29の該当箇所の記述を以下の通り修正します。 「資産や機能に対して発生する可能性のある脅威」 ⇒「資産や機能、人命や健康に対して発生する可能性のある脅威」 また、「CCDS製品分野別セキュリティガイドライン_スマートホーム編」については、スマートシティに一部類するスマートホームにおける脅威・リスク分析について、特に人命や健康という観点を踏まえた脅威・リスク分析に関する記述が参考となることから、上述の脚注として、「CCDS製品分野別セキュリティガイドライン_スマートホーム編」を掲載いたします。	有

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
15	法人C（一般社団法人重要生活機器連携セキュリティ協議会）	3. スマートシティにおけるセキュリティ対策	・P.49、「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」 ■意見区分： ③ガイドライン案の記載に対する追加要望 ■意見内容： IoT製品に含まれるソフトウェア及びハードウェアコンポーネントの構成管理について、セキュリティ対策の追加及び、出典文書の掲載をご検討いただきたい。 ■理由： IoT製品に含まれるソフトウェア及びハードウェアコンポーネントには、サードベンダーの製品やオープンソースのソフトウェアが組み込まれている可能性もあり、脆弱性やバージョン管理については製造企業にとっても課題となっている。 ・本書のAppendixAに記載の「政府機関等の情報セキュリティ対策のための統一基準群」には付随文書「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」[3]があり、システムの構成管理について対策として記述されている。 ・経済産業省の「別冊 2 機器メーカに向けた脅威分析及びセキュリティ検証の解説書」[4]において、ソフトウェアの構成管理が対策として記述されている。 ■出典・参考文書： [3]内閣サイバーセキュリティセンター（NISC）、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」、「付録A. 対策要件集」 https://www.nisc.go.jp/active/general/pdf/SBD_manual.pdf https://www.nisc.go.jp/active/general/pdf/SBD_manual_annex_a.pdf ※P.21 「障害対策（事業継続対応） 構成管理（DA-1）」 [4]経済産業省 商務情報政策局 サイバーセキュリティ課、「機器のサイバーセキュリティ確保のための セキュリティ検証の手引き 別冊 2 機器メーカに向けた脅威分析及びセキュリティ検証の解説書」 https://www.meti.go.jp/press/2021/04/20210419003/20210419003-3.pdf ※P.65 「次期製品開発へのフィードバック」 「・ソフトウェア構成表（ソフトウェア BOM）を管理、更新する」	いただいたご意見を踏まえ、P49の該当箇所において、以下の通り脚注を追加します。 ＃＃＃ 「ソフトウェアやハードウェア等の構成管理にあたっては、以下のドキュメントが参考となる。 ・内閣サイバーセキュリティセンター（NISC）「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」 ・経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」 ＃＃＃	有
16	法人D（京セラ株式会社）	3. スマートシティにおけるセキュリティ対策	■SOC（Security Operation Center）に関して 【現状】 各カテゴリ別のセキュリティ対策としてSOCが記載されているが、各レイヤー毎に分断されている。 スマートシティ全体としての情報収集や、集められた情報の分析や判断を一貫して行うことが望ましい。 【提案】 都市OSベンダがまとめてSOC機能を構築、提案を行う。 その提案に対しての判断は推進主体（自治体等）のガバナンスレイヤーで判断する形	スマートシティにおけるSOC機能の在り方については、それぞれのスマートシティのビジネスモデルによって様々なケースが想定されるため、P61の補足において、以下の記載を追加いたします。 「SOC/CSIRTの在り方については、それぞれのスマートシティのビジネスモデルのよって様々なケースが想定されるが、例えば推進主体が主導で対応するケース、都市OSベンダが主導で対応するケースなどが想定される。」	有
17	法人D（京セラ株式会社）	3. スマートシティにおけるセキュリティ対策	■事業重要性 【現状】 事業継続性については記載があるものの、各サービス及び情報について重要度区分するための方針がなく、優先する機能や保護対象選別基準がない。 ※スマートシティだからこそ、セキュリティ観点で優先すべき機能や保護対象の優先順位の方針が必要 【提案】 サービスレイヤーの各サービスにおいて重要度を分けるため方針設定が必要。 そのために扱う情報（データ）の分類の方針設定が必要。 ※事業継続に関する対策事例も追加。	いただいたご意見を踏まえ、P34「サービス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」の記載を下記のとおり修正いたします。 「それぞれのサービスにおいて守るべき情報資産や機能を特定し」 「それぞれのサービスにおいて守るべき情報資産や機能を、予め策定したスマートシティのセキュリティに関するポリシー（リスク評価基準やデータ取扱い基準等）を踏まえて特定し」	有
18	法人D（京セラ株式会社）	3. スマートシティにおけるセキュリティ対策	■認証管理 【現状】 アカウントの認証機能の実施のみが記載されており、認証の手段やレベルの記載がない 【提案】 都市機能としては、サイバー空間のみならず、物理空間両方が存在しており、様々な場面で本人確認の必要性が発生するため本人である確認手段の具体的な方針などが必要（アカウントの確認レベル） 例）対面、非対面、公的証明書、など	いただいたご意見を踏まえ、P35「サービス②－３：認証機能を実装する」及びP40「都市OS①－３：認証機能を実装する」において、下記の文言を追記いたします。 「なお、どのような認証を採用するかについては、認証を実装するシステムやサービス等の特性や重要度に応じて適切に決定する必要があることに留意する。」	有
19	法人D（京セラ株式会社）	4.セキュリティ検討のための補助コンテンツ	・機器認証機能実装: p76 【相談】 認証機能を実施していない機器への対応について たとえば、電池持ちなどを考慮し、認証機能を持っていない機器への管理など・・・	ご指摘の点については、今後の取組の参考とさせていただきます。	無

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
20	法人D（京セラ株式会社）	3. スマートシティにおけるセキュリティ対策	■データの原本性について 【現状】 データの原本性保証について記載されているが、どの状態でのデータ（機器から取得された生データ or 一度解析され、整理されたデータ or サービスレイヤーで最終的に利用されるデータ）であるかが不明 【提案】 原本となるデータの明示的記載、もしくはどのようなデータを原本データにするかの方針などの記載が必要	どのようなデータを原本とするかは、それぞれのスマートシティにおけるデータの取り扱い方に依存するものであり、本ガイドラインにおいて定義をすることは困難であることから、原案のとおりとします。	無
21	法人D（京セラ株式会社）	3. スマートシティにおけるセキュリティ対策	【その他】 データ連携④:データの原本性を確保したデータ信頼性を確保する。(p55) データ連駅⑥:APIにおけるセキュリティ（機密性・・・真正性）を確保する。(p55) 上記の“原本証”、“真正性”の明確な区分、もしくは定義をした方が望ましい。	いただいたご意見を踏まえ、P53の原本性保証及びP56の真正性において、脚注で以下のとおり記載いたします。 「原本性保証とは、原本（オリジナル）から改ざんされていないことを保証することである。」 「真正性とは、アクセス者などのエンティティがなりすましでない（本物である）ことを明確にすることである。」	有
22	法人D（京セラ株式会社）	3. スマートシティにおけるセキュリティ対策	P23 ：2.3.1 各カテゴリにおけるセキュリティの考え方 - ④アセット P46 ：3.1.4 アセット アセット②-3 物理的なセキュリティ対策 【現状】 物理的な破壊や盗難からの保護について記載されている。 【提案】 機器内へデータ保存する場合は、機器の耐タンパ性確保で不正データ取得ができないよう対策。 （データを機器内に保存しない場合（クラウドへのデータ転送でデータを保持しない場合）は対象外） P118：セキュリティ対策一覧（カテゴリ毎）アセット AM:資産管理 物理的な破壊、盗難、耐タンパ性等の記述がない。	いただいたご意見を踏まえ、P23及びP46の該当箇所を以下の通り修正いたします。 P23 「また、デバイスで保有するデータに個人情報や秘密情報など機密性の高い情報が含まれる場合はデータの暗号化も必要である。」 ⇒「また、デバイスで保有するデータに個人情報や秘密情報など機密性の高い情報が含まれる場合はデータの暗号化や、機器の耐タンパ性確保といった対策も必要である」 P46 以下の記述を追加。 「さらに、アセット内でデータを保有する際には、機器の耐タンパ性を確保する等によって、不正にデータが取得できないように対策する必要がある。」 なお、セキュリティ対策一覧に関しては、物理的な破壊、盗難に関するセキュリティ対策について、CPS.IP-5において「自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施」とあるため、こちらでカバーされています。また、耐タンパ性に関しては、CPS.DS-8において記載があります。よって、アセットカテゴリにおけるセキュリティ対策については、ご指摘いただいた内容は既に記載がされていることから、原案のとおりとします。	有
23	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●経済産業省（IPA）により、中小企業のポリシー策定に対して国家資格者である「情報処理安全確保支援士」による支援事業が実施されている。 それに対して、本書では各種ガイドラインを参照しながら、自らリスクアセスメントを行うことを想定しているが、スマートシティの取り組みは多くの個人情報を扱い、生活に密着する事業となることを踏まえると、中小企業以上に専門家の参画は重要であると考えられるし、所管省庁が違うことにより一方には情報処理安全確保支援士が活用され、一方では無資格者（情報セキュリティの知見を有すると自称する素人）が既存のガイドラインを参照しながら作成するということは、情報セキュリティ上のリスクを増すばかりであり、施策としての一貫性に欠けるものである。 よって、 P18 ①ガバナンス なお、スマートシティにおいてポリシーを策定する場合は、スマートシティ全体の構成や関係主体等を把握したうえで、「必要に応じて情報処理安全確保支援士といった国家資格者の支援を仰ぎながら」、リスクアセスメントを行い とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。 P19 ①ガバナンス その観点からも、推進主体において自身のスマートシティのリスクを正確に把握するとともに、「必要に応じて情報処理安全確保支援士といった国家資格者の支援を得ながら」、適切にセキュリティ対策への投資を行う必要がある。 とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
24	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●情報セキュリティ上のリスクイメージの例について、あくまでも「例」であり、実施主体に所属する情報処理安全確保支援士が個別に検討すべきことであるとは思うが、IoTデバイスそのものの計算リソースに対する不正利用や、IoTデバイスを不正制御することによる電気・水道・ガスといった生活リソースの不正利用が懸念される。 この点に考慮して、以下の2つの図について、リソースの不正利用についても記載すべきであると、一般社団法人情報処理安全確保支援士会としては考えている。 P20 図2－11 サービスにおけるセキュリティ上のリスクのイメージ P22 図2－12 都市OSにおけるセキュリティ上のリスクのイメージ	IoTデバイスに対するセキュリティ上のリスクについてはP23に記載があるため、ご指摘の箇所においては原案のとおりとします。	無

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
25	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●脆弱性診断について、本書の記載ではサービスに対して適切な診断が何かを判断でき、その実施した診断に基づきアドバイスができる主体が想定されておらず、こういった部分についても、経済産業省の施策と同様に「情報処理安全確保支援士」の専門的支援を受けることが必須であると考える。 よって、 P20 ②サービス サービスイン前に「情報処理安全確保支援士」によるセキュリティ検証や脆弱性診断を行い、とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。 P20 ②サービス それぞれのサービスにおいて守るべき機能やデータ等の資産を特定し、サービス単体においてもリスクを把握した上で、「情報処理安全確保支援士」の専門的支援を受け、適切にセキュリティ対策を決定、実施する必要がある。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
26	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●都市OSについて 単に都市OSベンダとした場合、充分なセキュリティ対策を実施する要員を割かず、それによって住民に被害が出る恐れがある。よって、住民に大きな影響を及ぼす都市OSを提供するベンダについては、通信事業者に無線従事者免許所持者や、電気通信主任技術者といった国家資格者を必置としているのと同様、住民の安全に対する配慮が必要であると考える。各ベンダの自主性に任せるのではなく、国家資格者である情報処理安全確保支援士の必置措置を講じることにより、情報セキュリティといった新たな脅威から住民を保護する責任を果たすことができるよう、制度設計することが重要であると考える。 よって、 P21 ③都市OS ・セキュリティ対策の実施も「情報セキュリティに関する国家資格者である情報処理安全確保支援士が所属している」都市OSベンダが中心となって ・サービスイン前に「情報処理安全確保支援士による」セキュリティ検証や脆弱性診断を行い、あらかじめ排除することが望ましい。 ・都市OSで求められるサービスレベルを理解し、「情報処理安全確保支援士により」、そのサービスレベルを満たす堅牢性や可用性、信頼性が担保できるクラウドサービスを「選定し」利用することが推奨される。 とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
27	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●アセットについて 都市OSにとって、データを収集する重要な要素であるアセットとして、各種機器のセキュリティは極めて重要である。しかし、現時点においてもネットワーク機器におけるファームウェアのバージョンアップ漏れによる情報セキュリティ事故等、専門職が必置化されていないが故に安全性が確保されていない事例は、それを業として行っている事業者においてもみられる事態である。 更に、都市OSという住民の安全に直結するものを取り扱う以上、もし総務省が人命に配慮したスマートシティのガイドラインを作成するつもりがあるのであれば、専門職として国家資格者である情報処理安全確保支援士の必置は他の分野と同様必須要件とすべきだと考えている。 P23 …それらのアセットの死活監視を行うとともに、「情報処理安全確保支援士の助言を得て」その脆弱性情報を把握しつつ… …モビリティなどの物理的な制御をサービスとして提供する場合は、「情報処理安全確保支援士の助言を得て」安全性に配慮した設計・運用も… とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
28	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●サプライチェーン管理について 2019年度から、サプライチェーンの情報セキュリティを維持することを目的をして、中小企業の情報セキュリティマネジメント指導業務が実施されており、サプライチェーンの情報セキュリティ管理において、情報処理安全確保支援士がその業を遂行することは、経済産業省によって推進されている重要な事業である。 よって、国策としての平仄を考慮し、サプライチェーン管理については情報処理安全確保支援士による助言を得ることは当然記載されるべき事項である。 P24 ①適切なサプライチェーン管理 …委託先や再委託先等におけるセキュリティ管理が十分であるかを確認するために、「情報処理安全確保支援士の助言を得て」作成したセキュリティに関するチェックシート… とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
29	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●インシデント対応について 一企業におけるインシデント対応と比較しても難易度が高くなることは本書において言及されているが、適切な体制の構築について考慮されていない。これについて、情報セキュリティに関する統括役として位置づけられている情報処理安全確保支援士をインシデントハンドリングの担当者として必置しないことは、インシデント発生時に住民の生命を危険に晒す恐れもある。その点を踏まえて、専門家の必置は必至であると考える。 よって、 P25 …一企業におけるインシデント対応と比較しても難易度が高くなるため、「情報処理安全確保支援士を常勤の情報セキュリティの統括役として任命し」、充分なインシデント対応体制を構築し… とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
30	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●データ連携時のセキュリティ データ連携において、連携元・先の体制を確認することが重要であるという認識そのものは適切であると考える。しかし、その確認は一事業者の見識等に委ねられるものではなく、実際に資金決済事業者等のテストケース設計における考慮漏れによる事故も相次いでいたことからも、関係者に対して適切な実施を促すといった程度では十分ではない。よって、責任あるスマートシティを推進するため、情報処理安全確保支援士の必置化が必要であると考える。 よって、 P25 …そこで、データ連携時のセキュリティとして求められる対策として、まずはデータ連携先のセキュリティ体制「の確認を情報処理安全確保支援士に依頼し」、信頼できる連携先かどうかを… とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
31	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●セキュリティポリシーの策定について 既存のポリシーを参考にして定めるということをガイドラインと示すことは、各組織の戦略を踏まえていないポリシーを「形だけ作る」ことを促進し、すなわち実効性に乏しい、単なるコピペ文書が大量生産されるだけの事態を招いてしまう。また、単なる中小企業におけるポリシー作成であればともかく、スマートシティという多数の住民の生命にもかかわるポリシーをそのような安易な手法で策定することを推奨するような文章をガイドラインに記載する総務省の見識を問わざるを得ない。 スマートシティ実施組織となるにあたっては、情報処理安全確保支援士をセキュリティ統括者として常勤とし、組織や地域の戦略を踏まえ、適切なセキュリティポリシーの策定とその実効性の確保を促進すべきである。 よって、 P27 …推進主体として既に保有しているポリシーとの整合性も鑑みて策定する必要があること「を踏まえつつ、住民の生命に関わる需要なポリシーであることをしっかりと認識し、スマートシティの実施においては、情報処理安全確保支援士を常勤の情報セキュリティ統括者として配置し、その者により実効性を担保したポリシーを策定することが望ましい。」 とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
32	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●データ取扱い基準について データの分類等については、情報処理安全確保支援士の試験でも問われる重要かつ難易度の高い知識項目であり、各種テンプレートを参考として住民の安全に関するデータを、無資格者が分類することは、社会に対する責任放棄であり、重大なセキュリティインシデントの原因になることが懸念される。 よって、 P28 …データ取扱い基準では、取り扱うデータをセキュリティやプライバシーの観点を踏まえてこれらの分類に「適切に当てはめる能力が担保されている国家資格者である、情報処理安全確保支援士により当てはめを行う」とともに、 とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
33	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●リスクアセスメントについて 本書で記載されているとおり「リスクアセスメントの結果を基にした実施すべきセキュリティ対策の策定は専門的な知見を要する」ことは正しい認識であるが、「大学教授などの有識者が参画する推進協議会のような場において検討するという方法」は誤った対策である。 大学教授といっても専門性に課題があり、実際に情報セキュリティについては、従来の研究型の大学ではなく、専門職大学院で推進されているのが実態であり、大学教授を有識者の代表のように記載するのは実態にそぐわない。 また、セキュリティに知見のあるベンダという表現もくくりが大きすぎてわかりづらい。脆弱性診断等の技術的領域が得意なベンダは多数存在するが、セキュリティアセスメントについては、セキュリティアドバイザリー業務を提供している監査法人の方が適切であり、この点についても実態にそぐわない。 なにより、現時点において、セキュリティ対策の策定について専門的な知見を有していることを国家資格者として担保されているのは唯一情報処理安全確保支援士であり、それを踏まえたものにすべきである。 よって、 P29 …セキュリティ対策の策定は専門的な知見を要することから、「それらの知見を持っていることが国により担保されている情報処理安全確保支援士に検討を委託することが必要である。」 とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	該当箇所においては、セキュリティに関する専門的知見を有する人物の一例を挙げています。 また、専門職大学院における教授のみならず、大学においても情報セキュリティを専攻している教授は多数いることから、その趣旨を明確化するために、以下のように修正いたします。 「セキュリティに知見のあるベンダや、大学教授などの有識者」 ⇒「例えば、セキュリティに知見のあるベンダや、大学・大学院の教授などの有識者」	有
34	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●調達仕様書におけるセキュリティ要件の記載について セキュリティ要件について調達仕様書に記載しても、読み解ける者がいなければ意味がない。実際に、官公庁や金融機関において十分に吟味された調達仕様書であっても、受託者側がその意図を十分にくみ取っていないことにより、情報セキュリティのCIAについて支障が生じた事例は毎週のように発生している。 これが、スマートシティという生活に直結した分野において生じた場合、住民の生命が毎週何かしらのインシデントで脅かされる事態となってしまい、単に「要件を記載した」ということだけでは免罪符にならず、セキュリティ要件については受託者側も十分に理解し実施することを担保するため、委託側、受託側双方に情報処理安全確保支援士を必置として推進する必要があると考える。 よって、 P30 情報セキュリティ基本方針や、セキュリティ対策基準等のセキュリティに関するポリシーに則り、「情報セキュリティ統括者たる情報処理安全確保支援士が任命されていること」をセキュリティ要件とし、調達仕様書へ反映することで… …セキュリティ要件を策定する際は、ポリシー策定時と同様、当該委託事業におけるシステムやサービスの種類や取り扱う情報などに応じて「情報処理安全確保支援士」によるリスクアセスメントを行い、 とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	専門的な知見を有する人材を配置することは手段に過ぎず、P31に記載の「情報セキュリティ管理体制の構築」に包含される内容であることから、原案のとおりとします。	無
35	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●セキュリティチェックシートについて P49　チェックシートを作成しても、チェックする者がセキュリティに関する知見を有していないと、有効に機能しない可能性があることから、情報処理安全確保支援士の関与について記載すべきである。 よって …その回答を「委託元の情報処理安全確保支援士が確認する」ことをもって委託先のセキュリティを評価するとすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
36	法人E（一般社団法人情報処理安全確保支援士会）	3. スマートシティにおけるセキュリティ対策	●SOC/CSIRTについて P61　SOC/CSIRTについては、情報ネットワークが事実上生活インフラ化している現状を踏まえ、政府機関が発行する全てのガイドラインの類において、情報セキュリティに関する国家資格者である情報処理安全確保支援士の設置を推奨すべき段階に到達していると考えている。 よって …それを実現するためにも、「情報処理安全確保支援士を最高情報セキュリティ責任者とした」組織横断的なセキュリティ対応機能を具備するSOC/CSIRTの設置が推奨される。 とすることが適切であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
37	個人A	3. スマートシティにおけるセキュリティ対策	34ページの「ユーザ情報」欄には「個人情報」と「利用履歴・操作履歴」が別に記載されているが、これは個人情報保護法の解釈に関し誤解を招くおそれがあるため、履歴等は個人情報に含めるべきである。	いただいたご意見を踏まえ、該当する箇所を以下の通り修正いたします。 「ユーザの個人情報（氏名/住所/電話番号/生年月日/クレジットカード番号等）、ユーザ認証情報、利用履歴 ・操作履歴 等」 ⇒「ユーザの個人情報（氏名/住所/電話番号/生年月日/クレジットカード番号/利用履歴・操作履歴 等）、ユーザ認証情報 等」	有
38	個人A	3. スマートシティにおけるセキュリティ対策	35ページには認証方法の例としてSMS認証が挙げられているが、これには既知の危険性がある。したがって、SMS認証は「実装すべきでない/安全でない認証方法」と明記するか、記述ごと削除すべきである。	いただいたご意見を踏まえ、脚注において以下のように補足いたします。 「SMS認証はSMSの盗聴（予めインストールされた不正アプリやロックされていても通知時にメッセージの中身が見えてしまう、等）やSIMに対する攻撃などでパスコードを窃取される危険性があるため、SMS認証を活用する際はこれらのリスクについて評価し、適切に対策が取れている前提で利用することが望ましい。」	有

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
39	個人A	3. スマートシティにおけるセキュリティ対策	35ページのPKIの説明には、「接続するシステム・サービス相互で暗号鍵・電子証明書等を所持」とあるが、これではWeb of TrustなのかChain of Trustなのかが不明である。また、「暗号鍵を所持」が「他のシステムの秘密鍵を所持」と解釈されないよう「公開鍵を所持」とするべきである。	ここで記載するPKIについては、Web of Trust、Chain of Trustいずれかに限定するような意図はありません。 「暗号鍵を所持」については、意図を明確化するために、以下のとおり修正いたします。 「接続するシステム・サービス相互で暗号鍵・電子証明書等を所持し、照会する事でアクセスを許可する」 ⇒「接続するシステム・サービス相互で公開鍵暗号技術や電子証明書等を活用し、照会する事でアクセスを許可する」	有
40	個人A	3. スマートシティにおけるセキュリティ対策	36ページのWAFの説明中、WAFは完全な遮断能力を持たないことを明記すべきである。	「アプリケーションレベルで」と記載があることから、左記の趣旨は明確である一方で、暗号化された通信についてはWAFにおいても検出・遮断をすることができないことから、該当箇所を以下のとおり修正いたします。 「ウェブアプリケーションとの通信など、暗号化された通信については、IDS/IPS での監視が困難となることから、ウェブアプリケーションを提供する場合は、アプリケーション層におけるセキュリティ監視としてWAF（Web Application Firewall）を実装することで、アプリケーションレベルで不正なコマンドを検知、遮断することが可能となる。」 ⇒「IDS/IPSではアプリケーションレイヤの監視はできないため、ウェブアプリケーションのセキュリティ監視を実施する場合はWAF（Web Application Firewall）を実装することで、アプリケーションレベルで不正なコマンドを検知、遮断することが可能となる。なお、IDS/IPS及びWAFは暗号化通信（SSL/TLS通信）を監視できないため、暗号化通信の終端位置を考慮する等し、通信の監視をできる環境を検討・構築する必要がある。」	有
41	個人B	3. スマートシティにおけるセキュリティ対策	P36 ウェブアプリケーションとの通信など、暗号化された通信については、IDS/IPS での監視 が困難となることから、ウェブアプリケーションを提供する場合は、アプリケーション層 におけるセキュリティ監視として WAF(Web Application Firewall)を実装することで… の記載についてです。WAFも暗号化通信は通常監視できないため、以下のような記載はいかかでしょうか。 サンプル IDS/IPSではアプリケーションレイヤーの監視ができないため、WAFも合わせて導入が望ましい。 IDS/IPSおよびWAFは暗号化通信(SSL/TLS通信)を監視できないため、暗号化通信の終端位置を考慮し該当機器の配置位置を決定する必要がある。	※項番4と同様 いただいたご意見の趣旨を踏まえ、該当箇所を以下のように修文いたします。 「ウェブアプリケーションとの通信など、暗号化された通信については、IDS/IPS での監視が困難となることから、ウェブアプリケーションを提供する場合は、アプリケーション層におけるセキュリティ監視としてWAF（Web Application Firewall）を実装することで、アプリケーションレベルで不正なコマンドを検知、遮断することが可能となる。」 ⇒「IDS/IPSではアプリケーションレイヤの監視はできないため、ウェブアプリケーションのセキュリティ監視を実施する場合はWAF（Web Application Firewall）を実装することで、アプリケーションレベルで不正なコマンドを検知、遮断することが可能となる。なお、IDS/IPS及びWAFは暗号化通信（SSL/TLS通信）を監視できないため、暗号化通信の終端位置を考慮する等し、通信の監視をできる環境を検討・構築する必要がある。」	有
42	個人B	3. スマートシティにおけるセキュリティ対策	P37 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。についてです。 インシデント発生時に備えたセキュリティ対策ではなく、2外部からの攻撃等を防ぐセキュリティ対策に記載した方がよいと思われます。（特に通信の暗号化は外部の盗聴を防ぐ目的であるため、2外部からの攻撃等を防ぐセキュリティ対策に記載した方がよい） （都市OSに関する箇所も同様かと存じます）	いただいたご意見の趣旨を踏まえ、該当箇所（P38、P42）に以下の記述を追加します。 「なお、通信の暗号化に関しては盗聴を防ぐという観点で、外部からの攻撃等を防ぐセキュリティ対策としても有効である。」	有
43	個人B	3. スマートシティにおけるセキュリティ対策	P38 サービス4-3:証跡確保のためのログを取得する 以下にように必要に応じてログ分析基盤の導入を推奨してはいかかでしょうか。 必要に応じてログ分析基盤を導入しログを一元管理することで、相関的な分析が可能となる。 （都市OSに関する箇所も同様かと存じます）	いただいたご意見を踏まえ、該当箇所（P38、P43）に以下の記述を追加します。 「また、システム構成が複雑化することにより複数のログを管理・監視する必要がある場合は、ログ分析基盤を導入し、ログを一元管理することで相関的な分析が可能となる。」	有
44	法人C（一般社団法人重要生活機器連携セキュリティ協議会）	その他	■意見区分： ①ガイドライン案の記載に賛同する部分 ■意見内容： 文書全体に分かりやすくかつ、適度な粒度でまとめていただいているが、特にデータ連携におけるAPIのセキュリティについて、OAuth 2.0、OpenIDによる認証など可用性にも配慮した具体的な対策が記述されており、非常に参考となった。 ■理由： 上記の通り ■出典・参考文書： 特になし	賛同のご意見として承りました。	無

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
45	法人C（一般社団法人重要生活機器連携セキュリティ協議会）	その他	■意見区分： ③ガイドライン案の記載に対する追加要望 ■意見内容： 一般社団法人　重要生活機器連携セキュリティ協議会（CCDS）のスマートホームのサイバーセキュリティガイドラインをAppendix Aに追記頂きたい。 ■理由： 一般社団法人　重要生活機器連携セキュリティ協議会（CCDS）のスマートホームのサイバーセキュリティガイドラインは、スマートシティの一部にもなりうる、スマートホームに関するサイバーセキュリティのガイドラインを取りまとめている。スマートホームのセキュリティガイドラインもスマートシティのガイドラインに近しい考え方でガイドしており、AppendixAに追記されたい。 ■出典・参考文書： [5]一般社団法人重要生活機器連携セキュリティ協議会（CCDS）「CCDS製品分野別セキュリティガイドライン_スマートホーム編_Ver.1.0」 https://www.ccds.or.jp/public_document/index.html#20201124_report2	いただいたご意見を踏まえ、Appendix Aに「CCDS製品分野別セキュリティガイドライン_スマートホーム編」を追加いたします。	有
46	法人E（一般社団法人情報処理安全確保支援士会）	その他	【ガイドライン全般について】 　内閣府国家戦略特区が令和3年4月に出した、「スーパーシティ構想について」という資料において、スーパーシティにおいて構築されることが予定されるデータ連携基盤におけるデータの安全管理基準として、「要員（情報処理安全確保支援士等）の確保」という要件が明記されている（19ページ）。 　スーパーシティとスマートシティは単に表現の差異であり、実質として実現される成果は同一であり、なにより国民生活の安全性に直結するこれら施策において、要員（情報処理安全確保支援士等）を確保せずに行うことは、積極的に国民を危険に晒す行為であり、本ガイドラインにおいて情報処理安全確保支援士について一切言及されていないことは、内閣府の構想とも齟齬が生じている。更に、総務省が内閣府の決定を考慮していないことのみではなく、国民の安全性についても考慮せずに本件ガイドラインを作成しようとしているのではないかという違和感を持たざるを得ない。 　従来総務省が作成する各種ガイドラインで言われていた「情報セキュリティに関する知見を有する人材」といった抽象的な存在では、情報セキュリティのCIAに関して責任ある施策を講じることができてないことは、コロナ対策の各種システムをはじめとして、毎週のように報道される情報システムトラブルで知られつつあるところであり、今後地域社会を維持するための重要施策であるスマートシティ（又はスーパーシティ）の推進において、現状唯一の国家資格者である情報処理安全確保支援士の必置を求めることは、何よりも国民生活の安心・安全の確保のために必要なことであると考えている。 　あわせて、迅速な施策の推進のために、自治体内情報処理安全確保支援士の抜擢や、既存のCIO補等採用への交付金措置の要件として「情報処理安全確保支援士であること」を総務省において各自治体に指示することで、本件に対する対応は容易に実現できると考える。 これらの観点を中心として、一般社団法人情報処理安全確保支援士会として以下の提言を行う。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
47	法人E（一般社団法人情報処理安全確保支援士会）	その他	●推進主体については、地域全体のスマートシティサービスの推進において主導権を持ち、自組織及びベンダ等提供者の情報セキュリティリスクアセスメントを主体的に実施できる必要がある。よって、情報セキュリティに関する専門的知見を有している人材については委託等に頼ることなく、自組織で常勤により配置するとともに、十分な権限を与える必要がある。 現状、地方公共団体等において、多くの場合CISOは単なる充て職となっており、情報セキュリティに関する知見を有している職員が就いているとは言い難い。また、これを補佐するためのCIO補等を非常勤で委託する手法を採用している自治体もあるが、これについても資格要件が定められていないことにより、情報セキュリティについて必要な知見を有していない人物が採用されている事例も散見される。 よって、スマートシティサービスを推進する地方公共団体等においては、情報セキュリティに関する唯一の国家資格者である情報処理安全確保支援士を常勤の局長級又は副首長級のCISOとすることで、単にスマートシティ事業のみならず、庁内及び地域社会に対する情報セキュリティの責任者として、充分な知識と権限を担保する必要があると考える、よって P5 表１－１　本ガイドラインにおける関係主体の定義 推進主体：…本ガイドラインにおいては「情報処理安全確保支援士を常勤のCISO（局長又は副首長級）として任命した」地域協議会や地方公共団体などが推進主体に該当し、 とすることが国民の生命・身体・財産を守るためにも必須であると、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有
48	法人E（一般社団法人情報処理安全確保支援士会）	その他	●スマートシティの推進主体について、内閣府が作成した「スーパーシティ構想について」に記載されているとおり、CISOとしての情報処理安全確保支援士を必置すべきことはもちろんだが、推進主体の監視・チェック者についても、情報処理安全確保支援士でなければ監査の有効性が担保できないと考える、よって P13　図のEについて ・提供されるサービスや推進の全体を「常勤の情報処理安全確保支援士により」常時確認し、 とすることが望ましいと、一般社団法人情報処理安全確保支援士会としては考えている。	セキュリティ人材の育成・適切な配置が必要という観点から、P32「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」において、以下の記述を追加します。 「また、金銭的な投資のみならず、セキュリティの知見を保有する人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。」	有

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
49	法人E（一般社団法人情報処理安全確保支援士会）	その他	【追加の提言】 情報通信技術が生活インフラとなり、急速に生活全般に浸透しつつある。 総務省は従前から通信領域（OSI参照モデルにおけるレイヤー１～３）を主として所管し、通信事業者の監督業務を行っており、経済産業省が情報処理領域（同レイヤー４～７）を主として所管してきた。 しかし、実装技術と情報セキュリティ、そして通信技術は同モデルが生まれた当時（1977年）と比べてその関連性が密となり、領域が明確にできなくなりつつあることもSociety5.0の特徴ともいえる。 こういった現状を踏まえて、地域の情報化推進において経済産業省が実施している情報処理領域の国家資格者を積極的に活用することを総務省は検討する必要があると考えている。情報処理技術者試験や情報処理安全確保支援士は経済産業省が所管する試験・資格であるが、総務省が所管している工事担任者や無線従事者と同様の「国家資格」であることには変わりはなく、国民から見ればどこの省庁が所管しているかということよりも、安心・安全が確保されることが重要であることは言うまでもない。 こういった観点からも、今後は情報通信分野に関するガイドラインの作成に当たっては、単に経済産業省の資料を参考資料として例示するといった扱いにとどめるのみならず、総務省と経済産業省の両者が共創して作業にあたるようにすることが国民全体にとっても望ましいと考えている。 また、冒頭指摘したように、内閣府国家戦略特区が令和3年4月に出した、「スーパーシティ構想について」という大方針と齟齬が生じないガイドラインとなるように、本稿の決定にあたっては内閣府との調整も実施すべきであると考える。 従来「情報資産」のみを対象としていた情報セキュリティに関する知見は、スマートシティにより「生命」を対象とする領域へと拡張していることは本書においても言及しているところでもあり、特に総務省においては、情報処理産業において「無免許・無資格」で従事が可能であったこれまでの在り方を見直し、総務省が所管してきた通信行政と同様、行政分野において国家資格者の必置による推進を前提とした体制に早急に改める意識をもって各種施策を推進していただきたいと考えている。 更に、それがなければ、国民の「生命・身体・財産」を脅威にさらすことになるというしっかりとした認識を持ち、例えば、現在取り組んでいる地方自治体に対する「無資格・無免許でも経験があれば可」として人材選定をしている極めて無責任な地方情報化支援人材の派遣制度の見直しや、J-LIS等で実施している人材育成分野における無資格講師の排除、地方自治体における情報処理安全確保支援士を含む高度情報処理技術者資格所持者の抜擢といった「資格により能力の定量的評価が可能な」人材活用制度の導入を早急に進めていただきたいと考えている（これについては内閣府が実施している「自治体共創PF」において具体的な人事制度も提案・議論されているので、「官庁の縦割りを超え」早急に検討して頂きたい。）。	ご指摘の点については、今後の取組の参考とさせていただきます。	無
50	個人A	その他	99ページと110ページに「一定回数以上のログイン認証失敗によるロックアウト」とあるが、この機能を悪用し、正当なログインを不能にするサービス拒否攻撃が確認されていることから、再ログインの間隔をあける機能の使用を推奨すべきである。	本リストでは、不正ログインを防ぐための手段の1つとして当該機能を紹介しており、推奨／非推奨といった表現は盛り込んでいないため、原案のとおりとします。	無
51	個人C	その他	自分も、何回かインターネットで詐欺ページに誘導されて、サイバーセキュリティには詳しくはないのですが、ほとんどのホームページは画像や動画で表示されます。よくマルウェアとか聞くのですが、全然詳しくないのですが、そういったウィルスは画像や動画を含まないのですかね。もし、画像や動画を含まない、通信が来た場合、ウィルスの可能性があるのではないかと思いますが、詐欺には効果はありませんが、マルウェアの警告には効果あるのかなと思いますが、ITに詳しくない田舎者の考えで、華やか都会で仲間とかいたらインターネットに詳しくなると思いますが、全然参考にならないと思いますが、少しでもお役に立てたらなと思い書かせいただきました。	利用者側へのセキュリティ対策の推進という観点でのご意見と承っております。いただいたご意見は今後の取組の参考とさせていただきます。	無
52	個人D	その他	私は、スマホの使い方の教室を増やすべきだと考えます。 パスワードは、どの機種も設定するべきだと考えます。 6桁以上の、パスワードは、ルールにした方がいいと思いました。 スマホを落としたら、いけないルールも考えるといいと思います。 どこに言うのかわからない方も、多いと思います。 私は、セキュリティは、番号とニックネームを入力の頭文字とか、考えないといけないものも大切です。 スマホは、ライン・メール・電話・アプリ検索だけでも、充分な気もします。 セキュリティーは、もしものために、紙に書くことも大事です。 私は、もっと、スマホの教室に行きたくても、なかなか行けないです。 すぐに、募集がいっぱいになります。 私は、子供は、スマホを持たない方がいいと考えます。 使い方とか、パスワードとか、１７？２０歳からに使えれる方が、安心です。 パスワードは、１？２年の間に、１回は更新するべきだと考えます。 私は、アプリも、あまり、素人が作らない方がいいと考えます。 情報は、できるだけ言わない書かないと、マナーとルールは、スマホ会社さんも、言うべきです。 私は、もっと、詳しく、具体的に、マナーとかルールがあれば、ありがたいです。 スマホは、使っても、１？３台までとかも、決めるべきです。 家族の方も、使い方は、スマホ教室に行ってほしいです。 私は、授業でもスマホが、勉強した方がいいと考えました。 マナーとか、情報を守る大切なルールもです。 私は、一人ひとりのマナーとかルールを大切にすることも、大事だと考えます。 ありがとうございます。	利用者側へのセキュリティ対策の推進という観点でのご意見と承っております。いただいたご意見は今後の取組の参考とさせていただきます。	無

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
53	個人E	その他	すべてのステークホルダーには、外国資本や外国企業は参入できないことを100%明確に規定し、リスクを排除することを明記すべきと考えます。 利用/開発するハード、ソフト、サービスなどはすべて国内企業のもの限定とし、データの保管場所も国内限定、昨今問題になっている2次請負・3次請負で外国企業に委託されることないよう、国内企業限定として透明性を持った運用となることを明記してほしい。	本ガイドラインにおいては全てのステークホルダーに外国資本や外国企業が参入できないことは意図していません。一方で、委託先等におけるセキュリティ上のリスクについては、P49の「サプライチェーン② 委託先のセキュリティ管理体制を評価する」において、サプライチェーン・リスクへの対策という位置付けで言及しているため、原案のとおりとします。	無
54	個人F	その他	詳細に渡って記載されており、これを公表し、意見を収集するのはいいのですが、悪意を持った人間は、ここで記載されていないこと（気づいていないので弱いとみなされる）を重点的に攻撃するということも考えられます。 このような「記載漏れ（気づいていない）部分」を攻撃されることをどのように防いでいくのか、お知らせください。	P7の対象範囲において、「当ガイドラインに記載されているリスクやセキュリティ対策は、スマートシティを構築・運用するにあたり、特に検討・実施することが推奨される事項について記載しており、網羅的な記載となっていない」、「スマートシティ内で取り扱われる情報資産に対するリスク評価や、実施するセキュリティ対策、その対策の実施主体などは、それぞれのスマートシティのサービスやビジネスの形態に大きく依存することから、スマートシティごとに検討する必要があることに留意する」と記載しており、ご指摘いただいた内容をカバーできていると考えます。	無
55	個人G	その他	情報処理技術者試験の在り方を抜本的に再検討し、2年後を目途に、新方式への移行が検討されている。 情報処理技術者試験の目的 3．情報技術を利用する企業、官庁などが情報処理技術者の採用を行う際に役立つよう客観的な評価の尺度を提供し、これを通じて情報処理技術者の社会的地位の確立を図ること。 と記されているが，経済産業省においては「国家資格ではなく、能力を認定する国家試験」と回答している。 その一方で、ITPECアジア共通統一試験の合格者及び資格の取得者に対しては、日本での就労に必要な「技術・人文知識・国際業務」の在留資格に係る基準の特例が適用されます。と記されており、就労に必要な国家資格の扱いであり、職業的地位が保障されている。 抜本的に再検討するのであれば、名称独占型の国家資格として技術者個人の職業的地位を保障すべきではないか。 ・第二種情報処理技術者⇒システムの設計・開発を行い、信頼性・生産性の高いシステムを構築する。また、その安定的な運用サービスの実現に貢献する。 ・第一種情報処理技術者⇒高度情報処理技術者を目指す人材で、システムの設計・開発を行い、又は汎用製品の最適組合せ（インテグレーション）によって、信頼性・生産性の高いシステムを構築する。また、その安定的な運用サービスを実現する。 ・特種情報処理技術者⇒データベース、エンベデッドシステム、ネットワーク各試験区分のスペシャリストの名称。 ・高度情報処理技術者⇒論述式がある各試験区分の名称。 ・基本情報技術者⇒ITパスポートの上位試験に位置付けられ、基本戦略系・ITリテラシースタンダード1級における各領域に関する知識を横断的に活用し、実務の場でリーダーシップを発揮できる。 需要者（企業経営、社会システム）が直面する課題に対して、汎用製品の最適組合せ（インテグレーション）によって、信頼性・生産性の高いシステムを提案し、情報技術を活用した戦略立案に参加する。 ・ITパスポート試験⇒国家戦略として全ての社会人へ受験を奨励して行くことから、合否制を見直しスコア制の試験とする。 評価点600点以上でITの動向の領域に関する知識を前提とし、必要に応じて他領域の一部の知識を適宜選択・活用しながら実務に対応できるITLSの2級を認定する。 ・情報セキュリティマネジメント⇒情報処理安全確保支援士の下位に位置付けられる。	ご指摘の点については、今後の取組の参考とさせていただきます。	無

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
56	個人G	その他	社会福祉法人東京コロニー・職能開発室から独立行政法人情報処理推進機構（IPA）に対し，障害を理由とする差別の解消の推進に関する対応要領，情報処理技術者試験に関する合理的配慮の具体例として意見書が下記の内容で提出されている。 https://www.tocolo.or.j...ipa_pubcomme_201508.pdf 未だ実現されていないものが多く，重度障がい者にとって就労につながるITスキルの証明であるCBT方式のITパスポート試験，基本情報技術者試験，情報セキュリティマネジメント試験の受験において「障害者差別解消法に基づいた合理的配慮」を国家の責務として講じてもらいたい。 （ルール・慣行の柔軟な変更の具体例） ・情報処理技術者試験のCBT受験において、障害により操作に時間がかかる際、時間延長を認める。（現状、ペーパー試験の特別措置受験のみ可能） ※CBT方式によるIT系資格試験の最大手プロメトリック社では、特別受験という形で時間延長や機材持ち込みの対応がなされております。 http://it.prometric-jp....cial_accommodation.html CBT方式の試験におきましても、プロメトリック社の試験会場を設けてますので、同様の配慮を受けることは可能ではないでしょうか。 上肢に障害があると、基本的なページめくりや筆記による記入が難しく、代理記入等の人的支援をいただいてはいるものの、試験問題のページ間参照や、回答の書き換えなどが自身の思うようにはできなかった。これらは合否において明らかに不利であったため、理解度の高い受講生でも合格できないという現実があった。 CBT方式ではマウス一つでこれらが行えるため、自力でページ間を移動して確認が行えたり、何度も回答を自分で書き直せるなど大きな利点がある。中問の問題がタブ形式で表示されることにより、複数ページに渡っていた長文の問題も解きやすい。 年2回の試験実施を待たず、希望する会場、希望する時間帯で随時受験ができるようになることは、体調が不安定な受験者等の利便性を飛躍的に向上させるものである。 CBT方式での受験が難しい方については従来通り年2回のペーパー試験が実施されるということで、そのような受け皿が残されていることは大変ありがたく思う。	ご指摘の点については、今後の取組の参考とさせていただきます。	無
57	個人G	その他	2001年、通商産業省による国家プロジェクトの一環としてITコーディネータ資格制度は設けられました。 経済産業省の推進資格として、約6500名の資格保有者が全国各地で活動しています。 ITの利活用に向け、経営者の立場に立った助言・支援を行い、デジタル経営を実現する人材です。 【ITコーディネータの再定義】 経済産業省の推進資格としての位置付けではなく、その認定試験等の実施を独立行政法人情報処理推進機構IPAが行う、情報処理技術者試験に加えることを提案いたします。 その理由として、 ・認定試験がCBT方式で実施されていること。 ・ITを利活用する側の人材にとって認定試験の難易度がITパスポート試験からのキャリアパスを鑑みたとき、無理のない適切な難易度であると思慮できるからです。 【ITコーディネータ制度の理想】 ・企業における戦略的デジタル投資が活性化していくためにも、ITコーディネータに対する社会的ニーズは大いに高まることが予測されるとともに、優秀な若い人材が参加することが期待されていたのであった。 【ITコーディネータ制度の現実と課題，協会を解散すべき理由の根拠】 ・ITコーディネータ資格認定に必要となる研修プログラムです。試験の合格、ケース研修修了の両方を、4年ごとに満たす必要があります。 受験料金の19,800円に加えて、資格認定に必要となるケース研修の受講に必要な費用が22万円と大変に高額なため若い人材が参加することへの障壁となっている。 ・週刊誌FRIDAYの記事によれば、「昨年、協会のトップである会長の秘書兼経理担当だった女性Aによる横領が発覚。昨年５月の内部監査で発覚するまでに4500万円近い金額を協会の口座から抜いていた。協会はITコーディネータの認定試験や資格取得に必要な研修受講費などの収入もあり、収支は億単位で動きます。」 事後の対応について事実の隠蔽では、という声については、 「弁護士とも相談しましたが、協会の内部で起きた問題で、広く公表する類いのものではない、と。報告に行った経産省にも、公表しなくてよいと言われました」 ※経産省は『弊省として、そのような対応をした事実はありません』と回答。	ご指摘の点については、今後の取組の参考とさせていただきます。	無

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方	修正の有無
58	個人G	その他	サイバーセキュリティー対策」が重要な構造と、私し個人は思います。例えばですが、「センサー技術、ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。具体的には、「電波規格（エレクトロリカルウェーブスペック）」及び「通信規格（トランスミッションスペック）」での「回線（サーキット）」の事例が有ります。（ア）「通信衛星回線（サテライトシステム）」における「トランスポンダー（中継器）」から成る「ファンクションコード（チャンネルコード及びソースコード）」のポート通信での「DFS（ダイナミックフレカンシーセレクション）」の構造。（イ）「電話回線（テレコミュニケーション）」における基地局制御サーバーから成る「SIP サーバー（セッションイニテーションプロトコル）」の構造。（ウ）「インターネット回線（ブロードバンド）」におけるISPサーバーから成る「DNSサーバー（ドメインネイムシステム）」の構造。（エ）「テレビ回線（ブロードキャスト）」における「通信衛星回線、電話回線、インターネット回線」の構造。具体的には、「方式（システムスペック）」での「回線（サーキット）」の事例が有ります。（ア）「3G（第3世代）」における「GPS（グローバルポジショニングシステム）」から成る「3GPP方式（GSM方式及びW-CDMA方式）」の構造。（イ）「4G（第4世代）」における「LTE方式（ロングタームエボリューション）」から成る「Wi-Fi（ワイアーレスローカルエリアネットワーキング）」の構造。（ウ）「5G（第5世代）」での「NR（NewRadio）」における「MCA方式（マルチチャンネルアクセス）」から成る「DFS（ダイナミックフレカンシーセレクション）」の構造。具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例が有ります。（ア）クラウドコンピューティングでは、「ビッグデータ（BD）」から成る「データーベース（DB）」の導入により、ITネットワークの構造。例えばですが、ファイアーウォールにおける強化では、ルーターとスイッチを挟み込む様に導入する事で、「クラウド側（プロバイダー側）←ルーター⇔ファイアーウォール⇔スイッチ→エッジ側（ユーザー側）」を融合する事で、ハードウェアーの強化の構造。（イ）エッジコンピューティングでは、Web上における「URL（ユニフォームリソースロケーター）」での「HTML（ハイパーテキストマークアップラングエッジ）」から成る「API（アプリケーションプログラミングインタフェース）」に導入により、「HTTP 通信（ハイパーテキストトランスファープロトコル）」における暗号化によるソフトウェアーでの「HTTPS（HTTP over SSL/TLS）」の融合により、AIネットワークの構造。具体的には、「サイバー空間（情報空間）」及び「フィジカル空間（物理空間）」での「回線（サーキット）」の事例が有ります。（ア）「サイバー空間（情報空間）」では、「SDN/NFV」における「仮想化サーバー（メールサーバー、Web サーバー、FTP サーバー、ファイルサーバー）」から成る「リレーポイント（中継点）」での「VPN（バーチャルプライベートネットワーク）」が主流な構造。（イ）「フィジカル空間（物理空間）」では、「AP（アクセスポイント）」が主流な構造。要約すると、「ボット（機械における自動的に実行する状態）」による「DoS攻撃」及び「DDoS攻撃」でのマルウェアーにおける「C＆Cサーバー（コマンド及びコントロール）」では、「LG-WAN（ローカルガーブメントワイドエリアネットワーク）」を導入した「EC（電子商取引）」の場合では、クラウドコンピューティング及びエッジコンピーティングにおける「NTP（ネットワークタイムプロトコル）」の場合では、「検知（ディテクション）⇒分析（アナライズ）⇒対処（リアクションメソッド）」での「サイバーセキュリティー対策」が重要と、私は考えます。	ご指摘の点については、今後の取組の参考とさせていただきます。	無