パブリックコメントで寄せられたご意見に対する考え方

ID	No	提出者	御意見の概要	御意見に対する考え方
1	1	企業	pp.16,19,22 共同住宅の共用部分に設置された・・・の文章の一部がBoldになっている。フォントの設定ミスと思われる。 pp.28 「タンパ機能」は「耐タンパー機能」が正しい。「耐タンパー機能」は一般的な用語ではないため、用語集に入れたほうがよい。 pp.29 「機器やネットワークの管理・運用は適切に行う」について、主語が「管理受託会社」なので「機器やネットワークの管理・運用を適切に行う」としたほうがよい。 pp.29 4.5.2「機器やサービスは用途・用法を守る」は「機器やサービスの用途・用法を守る」が正しい。 pp.30 「IoT機器やサービスは用途・用法を守って使う」について、主語が「スマートホームの住まい手」なので、「IoT機器やサービスを用途・用法を守って使う」としたほうがよい。同じ理由で「個人情報は自分で守る」は「個人情報を自分で守る」としたほうがよい。	いただいた御意見を踏まえ、以下のとおり修正します。 ・文字のフォントを統一。 ・「タンパ機能」を「耐タンパー機能」と修正。「耐タンパー機能」を用語集へ追記。 ・「機器やネットワークの管理・運用は適切に行う」を「機器やネットワークの管理・運用を適切に行う」と修正。 ・「機器やサービスは用途・用法を守る」を「機器やサービスの用途・用法を守る」と修正。 ・「IoT機器やサービスは用途・用法を守って使う」を「機器やサービスの用途・用法を守る」と修正。 ・「個人情報は自分で守る」を「個人情報を自分で守る」と修正。
2	1	個人	特定の国に関連する企業や、アメリカから制裁企業認定されているものは参加させない。	今後の政策を検討する上での御意見として承ります。
3	1	個人	スマートホーム化が進む中で家庭に対するサイバー攻撃を防ぐためにガイドラインを設けるのは正しいのですが、どうも議論が１軒の中に留まっており、複数の家で連携した場合が想定されていないという認識を持ちました。スマートシティの文脈で言えば、複数の家が連携することも想定されるのではないでしょうか。例えば、地縁に基づかないバーチャル自治会、のようなこともあり得るかも知れません。そういったことを想定した時にこのガイドラインが適切なのか厳し過ぎるのか、或いはそういったことを想定する必要はないのか、その辺りを触れていただきたいと考えます。	本ガイドラインは、スマートホームを対象としております。いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
4	1	個人	「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（New Radio）」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。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
5	1	個人	以下文面のご確認お願い致します。 p.7 米国のある調査・・利用せざるを得ない状況にあるまで生活に根付いているものもある。 ↓修正案（日本語に違和感があります） 米国のある調査・・利用せざるを得ない状況として生活に根付いているものもある。 影響を受ける機器の種類と数量は極めて多いと想定されるものである。 ↓修正案（日本語に違和感があります） 影響を受ける機器の種類と数量は極めて多いと想定される。 p.25 提供者側の事業者が想定しない設定や運用がなされる可能性も想定される。 ↓修正案（日本語に違和感があります） 提供者側の事業者が想定しない設定や運用がなされる可能性がある。 p.26、p.27 4.2.1と4.3.1項は、「重要である」、「必要である」それ以外は「望ましい」です。 4.2.1と4.3.1項も「望ましい」かと思います。 添付D-1　2）　と　3） ・・・・生命・財産を侵害に繋がる事例 ↓修正案（日本語に違和感があります） ・・・・生命・財産の侵害などに繋がる事例	いただいた御意見を踏まえ、以下のとおり修正します。 ・「利用せざるを得ない状況にあるまで生活に根付いているものもある」を「利用せざるを得ない状況として生活に根付いているものもある」と修正。 ・「影響を受ける機器の種類と数量は極めて多いと想定されるものである」を「影響を受ける機器の種類と数量は極めて多いと想定される」と修正。 ・「提供者側の事業者が想定しない設定や運用がなされる可能性も想定される」を「提供者側の事業者が想定しない設定や運用がされる可能性もある」と修正。 ・「生命・財産を侵害に繋がる事例」を「生命・財産の侵害などにつながる事例」と修正。 なお、p.26からの「4. スマートホームに求められる最低限のセキュリティ対策」は、各項冒頭で記載するとおり「望ましい」対策事項となります。各項目の末尾については、前後の文との関係からも「重要である」、「必要である」を採用させていただきます。
6	1	個人	おそらく、誤記と思われるものを見つけていますのでご連絡します。 p.3　2行目 ・・作成時点(2019年)時点・・ ※時点が２つ明記あります p.5　表2内　4箇所 スートホーム　⇒　スマートホーム p.15 想定されるインシデント内の　(3) ⇒ 3) p.18、19 想定されるインシデント内の　(2) ⇒ 2)　、(1) ⇒ 1) p.28 タンパ機能　⇒　耐タンパ機能 ご確認お願い致します。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「作成時点(2019年)時点」を「作成時点(2021年3月)」と修正。 ・「スートホーム」を「スマートホーム」と修正。 ・添付Dの番号の表記を整理。 ・「タンパ機能」を「耐タンパー機能」と修正。

7	1	個人	スマートホームをセーフティに使っていくにはサイバーフィジカルセキュリティが大事なのは勿論の事でパブリックコメントのアイデアをガイドラインにインプットするのに賛成です。 しかしながらスマートホームのようなインターネットを使用するハードウェアのカテゴリではアメリカやEUが先進的でありそのアイデアをクローンして日本で使うべきだと思います。 グローバルスタンダードをクローンすればインプットはクリアできます。 イージーなのでインプットやアウトプットという次元ではありません。 ジャパンオリジナルをクリエイトするのはハイコストです。 ですからその事でディスカッションする必要はありません。 ディスカッションも含めてハイコストなのでありヒューマンリソースを別の事に使うべきです。 ガラパゴスというONE JAPANよりもグローバルというONE WORLDに方針転換すべきです。	今後の政策を検討する上での御意見として承ります。
8	1	個人	「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。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
9	1	企業	弊社は、経済産業省が進めているIoT技術を家庭で安全・安心に利用するための仕組みづくりに関する取組を支援いたします。また、 物理空間とサイバー空間をつなぐ機器・システムに内在する多様なリスクに関する経済産業省の認識をサポートいたします。加えて、スマートホームサービスのインフラとして、クラウドの活用に言及されたことに強く賛同いたします。 弊社は、経済産業省が、今後の政策の検討に当たって、世界中のIoTユーザーにサービスを提供している弊社の知見を踏まえていただくことを希望いたします。 また、経済産業省が、信頼性とリスク評価のための参照点として、ISO27001やSOCレポートのような既存の業界をリードするメカニズムを継続的に活用するとともに、民間企業においてもこうしたメカニズムを柔軟に利用できるよう配慮いただくことを希望いたします。 弊社は、経済産業省が、ガイドラインの策定に当たって、各ステークホルダーがとるべき具体的なセキュリティ対策を規定するのではなく、各ステークホルダーのセキュリティやプライバシー保護に関する責任のあり方を定めることに焦点を当てていただくよう要望いたします。また、ガイドラインの作成や改訂の際には、デジタルサービスのダイナミックな変化に対応するために、企業や業界団体と協議しながら行っていただくようお願いいたします。仮に事業者の自主性を阻害する措置を伴う場合には、費用・便益の観点から慎重な検討を行っていただくようお願いいたします。 弊社は、経済産業省が、IoTサービスやシステムのセキュリティの技術的側面を評価するため、国際的に認められた業界のセキュリティ基準や第三者監査の重要性を認識していただくことを希望いたします。弊社は、スマートホームのセキュリティを向上させるためには、サイバーセキュリティを強化し、世界的なコンセンサスに基づいた業界標準やベストプラクティスに基づいたリスクベースのアプローチを活用していくことが重要と考えます。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
9	2	企業	ガイドライン1.2「ガイドラインの対象者」において、スマートホームの安全・安心の確保に当たっては、ステークホルダーの責任が複雑かつ動的であることを基本認識として明記していただくようお願いいたします。この考え方は、スマートホーム向けのサービス事業者である、クラウドサービス事業者とクラウドサービス利用者の間で共有される責任に当てはまるものです。弊社のクラウドサービスでは、お客様の責任は選択した 弊社クラウドのサービスに応じて異なり、お客様は、選択したサービスの性質に応じてセキュリティ環境を設定します。弊社は、弊社 クラウドで提供されるすべてのサービスを実行するインフラストラクチャの保護について責任を負います。経済産業省におかれましては、こうしたスマートホームにおける情報セキュリティのステークホルダーの相互関係を認識するようお願いいたします。	クラウドサービス事業者が提供するサービスの範囲や形態はさまざまであり、御意見にもあるとおりステークホルダーの責任は複雑です。そのため、サービスの形態等が定まらないことには、責任の線引きや具体的な対応方法等を示すことは困難であると考えています。他方、サービス形態に従って何らかのポリシーを決定して提示することは重要ですので、4.3.2で「管理のポリシーを提示し遵守する」ことを記載しておりますが、いただいた御意見を踏まえ、以下のとおり修正します。 ・「さらに、スマートホームには様々なステークホルダーが関与し、多様な脅威に対しステークホルダーがそれぞれで対応する必要がある」と追記。 ・「スマートホーム向けのサービス事業者と直接関係するステークホルダーは、例えば、サービサーやプラットフォーマーなどとなる。セキュリティパッチ適用などのセキュリティ対策を実施する主体を契約等で明示することで、これらのステークホルダーとの責任の所在を明確にすることができる。」と追記。 ・「IoT機器やサービスを導入する際には、各事業者による個人情報を含む様々なデータ管理などのポリシーや、セキュリティ対策に留意して、」と追記。
9	3	企業	1.4「ガイドライン作成の背景」では、スマートホームに関するセキュリティ上のリスクについて多くの記載がされています。弊社は、経済産業省が、高信頼性、セキュリティ、コスト削減、革新的なサービスへのスピードと容易さなどの多くの利点から、情報セキュリティが最も要求される世界中のユーザーがクラウドサービスを採用していることを認識していただくよう希望いたします。クラウドサービスを利用することで、AIやIoTなどの先端技術を活用したビッグデータの革新的な利用が可能になっていることについても、是非ご理解いただくようお願いいたします。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
9	4	企業	4.3. (3)「スマートホーム向けのサービス事業者」（添付Cにも記載）では、クラウドサービス事業者を含むスマートホーム向けサービス事業者に対して、セキュリティ脆弱性への対応、不正アクセスや不正操作の防止、システムやデバイスの交換・廃棄時の個人情報の削除、サービス提供に係るセキュリティポリシーや利用方法の共有など、スマートホームにおける安全性確保のための対策を講じることを推奨しています。しかしながら、スマートホームに関するサービスを提供する様々なステークホルダーが、具体的にどのようにセキュリティの責任を分担するのか、現行の文言では明確になっておりません。弊社は、クラウドサービス事業者はスマートホームでのIoT利用の安全性を確保するためのセキュリティツールや情報を提供する責任を負い、クラウドサービス利用者は安全なアプリケーションの構築や、セキュリティインシデントやデータ漏洩を防ぐためのアクセス制御などの責任を負うことを、ガイドラインで明確にしていただくことを希望いたします。弊社の責任共有モデルでは、クラウドサービス利用者であるお客様には、ゲストオペレーティングシステム (更新とセキュリティパッチを含む)、その他の関連アプリケーションソフトウェア、および弊社 が提供するセキュリティグループファイアウォールの設定に対する責任と管理を担っていただいています。また、弊社のお客様は、情報管理を行っていただいています。他方で弊社は、クラウドで提供されるすべてのサービスを実行するインフラストラクチャの保護について責任を負います。このインフラストラクチャはハードウェア、ソフトウェア、ネットワーキング、クラウドのサービスを実行する施設で構成されます。また弊社がさまざまなセキュリティ基準や規制に準拠していることを検証した第三者監査法人からの定期的なレポートを提供しています。	本ガイドラインは、スマートホームにおけるセキュリティ対策の考え方、ならびに各ステークホルダーが考慮すべき最低限のセキュリティ対策を示すことを目的としております。ステークホルダー間での責任分担等については更なる検討が必要ですので、いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。

9	5	企業	4.3. (3)「スマートホーム向けのサービス事業者」で規定されている重要情報の保護について、 データ保護の方法としては、システム機器の交換や廃棄時のデータ削除（サニタイズ）といった手法のみならず、様々な有効な方法があることを記載していただくようお願いいたします。クラウドサービス利用中は、データを暗号化し、暗号化に使用された鍵と暗号化されたデータへのアクセスを分離することで、不正な第三者によるデータへのアクセスを防ぐことができます。お客様が弊社のクラウドサービスの利用を終了した後も、暗号消去によりデータへの不正アクセスを防ぐことができます。暗号鍵へのアクセスを失うことで、破棄されたデータへのアクセスを防ぐことができます。また、暗号消去により、お客様は破棄証明書の代わりに暗号化で保護されたレコードを自動的に取得して管理することが可能になります。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「適切に廃棄処理」を「再利用等できないよう適切に処理」と修正。
9	6	企業	4.3. (3)「スマートホーム向けのサービス事業者」において、住まい手への発生しうるインシデントや危害についても情報提供するよう求めていますが、この記述は削除いただくようお願いいたします。スマートホーム向けサービス事業者には、クラウドサービス事業者も含まれますが、クラウドサービス事業者がスマートホームの住まい手と直接契約を結ぶことはほとんどありません。このため、クラウドサービス事業者は、スマートホームの住民にセキュリティ情報を提供する立場にありません。該当記述を削除することが困難である場合、代わりにガイドラインにおいて、クラウドサービス事業者が居住者とスマートホーム向けサービスについて直接契約関係を持たない限り、スマートホームの利用者にセキュリティ情報を提供する責任を負わないことを明確にするようお願いいたします。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「住まい手に対して、発生しうる」を「直接関係するステークホルダーに対して、発生しうる」と修正。
10	1	個人	情報の抜き取りやサイバー攻撃をする可能性のあるメーカーや通信会社をいかに排除するか、どのようにお考えでしょうか。	いただいた御意見は今回のパブリックコメントで求めているガイドライン本文への修正意見ではないため、パブリックコメントの回答としては差し控えさせていただきます。
11	1	団体	ガイドライン（案）における対象者としての管理組合やマンション管理業者の対応について 　１．２．（６）において、区分所有型の共同住宅や団地において、共用部分に設置されたＩｏＴ機器や共用部分のネットワーク回線を管理する者として、管理組合や管理受託会社（マンション管理業者）が位置付けられています。 　管理組合より管理受託するマンション管理業者は、管理委託契約に基づき共用部分の管理をしています。その管理委託契約において一般的には、共用部分のＩｏＴ機器やネットワーク回線の管理を管理委託契約に含むことはありません。 　共用部分のＩｏＴ機器やネットワーク回線については、新築時からのものと既存管理組合の意思決定で新たに設置するケースがありますが、いずれも管理組合とＩｏＴ機器業者やネットワーク回線業者との直接契約が一般的です。また、管理組合から契約に含むよう交渉があった場合は、マンション管理業者各々の判断となりますが、マンション管理業者にとってＩｏＴ機器やネットワーク回線の管理は専門外であることから、管理委託契約に含むケースは多くはないと考えられ、管理委託契約に含んでも、その業務内容や責任範囲の明確化することは困難であると考えます。ついては、マンション管理業者が管理委託契約に含めマンション管理業務としてＩｏＴ機器やネットワーク回線の管理を行う場合における管理委託契約に記載する具体的指針を示していただきたい。	いただいた御意見を踏まえ、以下のとおり修正します。 ・脚注に「分譲共同住宅の管理組合や賃貸共同住宅の所有者（オーナー）と管理受託会社が締結する契約等に、共用スペースのIoT機器やネットワーク回線等を管理する条項が含まれている場合には、原則として条項の内容に従う。」と追記。 ・「分譲共同住宅・団地の管理組合および賃貸住宅の所有者が、IoT機器やネットワーク回線等の管理を管理受託会社（場合によってはその下請け再委託先も含む）に委託する場合、セキュリティパッチ適用などのセキュリティ対策を実施する主体を契約等で明示することで、責任の所在を明確にすることができる。契約等に盛り込むセキュリティ対策の実施等については、業種・業態に応じて具体化する必要がある。」と追記。 なお、本ガイドラインは、スマートホームにおけるセキュリティ対策の考え方、ならびに各ステークホルダーが考慮すべき指針として最低限のセキュリティ対策を示しております。具体的な業種・業態に特化したセキュリティ対策等については更なる検討が必要ですので、いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
11	2	団体	ガイドライン（案）における管理組合による管理方法について 　１．２．（６）における管理組合において、ＩｏＴ機器やネットワーク回線の管理方法等について、その意思決定する必要がある旨の記載や業務内容、責任範囲に関する記載がありません。また、４．２．３．における「管理のポリシー」の提示、遵守についても、個人情報取扱事業者である管理組合は、個人情報保護法で求められる安全管理の方法との連携も求められることから、その具体的指針を示していただきたい。 　なお多くの管理組合は、その区分所有者等からの問合せに対し、管理委託契約に基づき管理受託するマンション管理業者に確認することとなります。その場合においてもマンション管理業者は、国土交通省　マンション標準管理委託契約書　別表第１　事務管理業務　２．基幹事務以外の事務管理業務（１）理事会支援業務　として、共用部分の管理業務の一部として、契約関係を説明の後、マンション管理業者がＩｏＴ機器やネットワーク回線業者へ対応手配をするか、連絡先の案内をするかが一般的です。	いただいた御意見を踏まえ、以下のとおり修正します。 ・脚注に「分譲共同住宅・団地の廊下や階段等の共用部分は、区分所有法でいうところの区分所有者が共同で所有するものである。このため、共用部分に設置されたIoT機器やネットワーク回線等は、原則として、区分所有者によって組織された管理組合が管理・運営する必要がある。共用部分の管理においては、その対象に応じた管理方法や責任範囲を検討する必要がある。」を追加。 ・「ポリシー」について、誤解のない表現へ修正。 なお、本ガイドラインは、スマートホームにおけるセキュリティ対策の考え方、ならびに各ステークホルダーが考慮すべき指針として最低限のセキュリティ対策を示しております。具体的な業種・業態に特化したセキュリティ対策等については更なる検討が必要ですので、いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
11	3	団体	ガイドライン（案）の表記方法について 　１．２．（６）（８）におけるガイドラインの対象者に管理組合や管理受託会社（マンション管理業者）、スマートホームの住まい手（区分所有者、占有者等）を対象としているが、表記の方法が、専門用語を中心とした技術専門職を対象とした表記となり、多くの管理組合、マンション管理業者、スマートホームの住まい手には馴染まない表記となっています。ガイドラインとして示すのであれば、対象者に馴染む表記、構成にしないと、管理組合、マンション管理業者、スマートホームの住まい手が、ＩｏＴ機器やネットワーク回線に対し、利便性の高さに対する活用の反面、ネットワークに侵入を防ぐための対策へのリスクヘッジを構築し、運用することの理解を浸透することが困難と考えます。	いただいた御意見を踏まえ、住宅に関わる専門用語なども含め添付Ｅの用語集を充足いたしました。
11	4	団体	令和2年8月3日付日本経済新聞記事「「つながる住宅」官民で安全指針、サイバー防衛力を高める」」との関係について 　同記事では、「指針の素案ではマンションなどの機器の維持や管理をめぐり、明確な管理者が決まっていないことが多いと指摘した。問題が発生した際に混乱しないよう、対応策や作業の分担について居住者や管理受託会社の間であらかじめ擦り合わせておく重要性を強調している。」と掲載されています。本ガイドライン（案）のどこにその旨の記載があるかが不明です。	当該記事は経済産業省が記載したものではなく、お答えすることは困難です。
12	1	企業	米国のポンペオ国務長官が２０２０年８月５日に発表した「クリーンネットワーク政策」に準拠したガイドラインにしなければならないと思います。 クリーンネットワークについては日経新聞で概要が報道されています。次のリンク先のとおりです。 https://www.nikkei.com/article/DGXMZO62348950W0A800C2MM0000/ また、特定の国との関係があるアプリケーションについてもクリーンネットワーク政策によって対策をうつことが必要です。	いただいた御意見は今回のパブリックコメントで求めているガイドライン本文への修正意見ではありませんが、今後のサイバーセキュリティ政策を進める上で参考にさせていただきます。
13	1	個人	日本が切り拓いて行こうとしているSociety 5.0の世界を、世界標準レベルに持ち上げていくには、 ガイドラインの中にEchonet liteの活用を提示しておく事が必要だと思いました。 積極的に日本発の基準を活用すべきです。 （Echonet liteは、アジア諸国からは注目されていると聞きました） まず、IoT製品、家電製品は、中国製を始めとした安価でそれなりの機能を有した製品が次々と出てくる実態を考慮しておくべきです。 なぜ、考慮しておかなければならないかというと、当ガイドラインにそった製品とはならないだろうからです。 この類の製品の日本におけるシェアが高まると、Society5.0が目指す世界からは、離れていくばかりです。 この課題は簡単に阻止できません。 スマートホームの住まい手、およびスマートホームを供給する事業者は、市場原理に従うからです。 とすると、住まい手および事業者がこぞって、このガイドラインに沿ったセキュアな製品を導入したくなる 利便性をこのガイドラインで明示しておくのが一方法かと思います。 その為には、競争領域と協業領域の2つを上手に作る必要があります。 アイディアは、 　屋内は、各メーカーが独自色を出すリモコン／アプリの競争領域とし、 　屋外からの遠隔操作は、Echonet lite仕様のスマホアプリで 　操作する協業領域とする案です。 この遠隔アプリは、Echonet協議会から出荷するのが望ましいと考えますが、絶対条件でもないと思います。 このアイディアの基本は、屋外からスマートホームの住まい手が屋内のIoT製品、家電製品を制御したい要素は、 最大公約数的な機能さえ使えれば満足すると考えるからです。 この仕組みが提供できれば、住まい手はいろんなメーカーの製品を一つのスマホアプリで制御できます。 現在は、エアコン一つとっても、住まい手は購入したメーカー数だけのスマホアプリを搭載しておく必要があり、 決して利便性の高いものではありませんし、メーカーもガイドラインに従ったものを個々に作成し、運用し、サポートしていかなければなりません。 デベロッパーなどの供給者もサポートコストを抑える事が可能です。 住まい手が、遠隔操作したいのは購入した製品のフル機能でなくても満足してくれるという仮説に基づいています。 遠隔操作指示後、いつまでたっても帰宅しないケースは、照明の消灯やドア鍵のロック状態の確認ぐらいでしょう。 しかもこれも、Echonet liteの世界で解決できます。 この結果、ガイドラインに沿った世界を提供しやすくなるだけでなく、住まい手の利用のしやすさとセキュリティ向上も望めます。 結果、諸外国の製品もEchonet lite仕様に対応した製品をリリースするでしょう。 協業領域としたこのスマホアプリは、Echonet lite仕様を満たした製品なら何でも利用できるので、市場に参入しやすくなります。 また、日本以外の市場拡大も望めると考えます。 まとめるとIoT製品、家電製品を遠隔操作するスマホアプリは、共通アプリとすべきです。 こうすると、ガイドラインを守りやすくなるだけでなく、ガイドラインに沿った製品の流通が広まります。 結果、日本発のSociety 5.0が世界標準となる可能性を高めれます。 最後に、GAFAを始めとしたスマートスピーカーは、このガイドラインに合わせてくることはないでしょうし、 遠隔操作は苦手分野である事を記しておきます。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。

13	2	個人	4.1.「（1）スマートホーム向けIoT機器の事業者」に書かれている望ましい対策に関してですが、 あらゆるスマートホーム向けIoT機器は、このガイドラインに沿う事を望ましいとしていますが 日本の競争力を削ぐ事につながらないでしょうか？ というのは、日本のメーカーの開発部門はガイドラインを参照してから仕様を決めて開発に取り掛かるケースが多いと思うからです。 （もちろん、Echonetのケースを見ると海外企業も参加し対応製品を出荷しているのでステレオタイプ的な見方で 問題がある言い方かもしれません。「日本のメーカー」という言い方は） ガイドラインの存在を知らないとか無視するという企業が出荷する製品とガイドラインに従った製品を出荷する企業の製品とでは、 Society5.0を実現していく中では、後者が望ましいのは火を見るより明らかです。 また、困ったことに前者の製品は、後者の製品より安く流通させることができるので、 導入コストと期待されるセキュリティ効果を天秤にかけると前者が選ばれる可能性が高いと言わざるを得ません。 一方、IoT製品を眺めてみると、以下の観点で結構大きな違いがあるようです。 ・ネットに流すあるいはネットからもらうデータ量が多いか、少ないか ・そのデータは、連続的に続くか、断片的か ・インターネットに直接接続か、他の装置を通して接続か ・ＴＣＰ／ＩＰか、それ以外か ・グローバルＩＰアドレス運用か、プライベートＩＰアドレスか ・遠隔操作を前提にしているか、否か など。 ガイドラインに沿っていないIoT機器の流通を少なくすることが4章の他の項にも、好影響を与えるはずです。 上記に提示した以外の区分もあるかと思いますが、コメントしたかったのは、スマートホーム用のIoT機器において、 グレード分けを明示する事により、4.1に書かれた望ましい姿に複数のバリエーションを設ける事ができます。 この結果、満たすべきセキュリティ機能も明確になるだけでなく、グレードの低いIoT機器は、それなりの定価に抑える事が可能となります。 つまり、様々なIoT機器がある中、一律同じセキュリティを要求するのは、投資対効果が悪く、ビジネスにおいても得策ではないので、 グレードごとに、望ましいIoT機器が満たすべきガイドラインに変更したほうが、良いのではないかという事です。 例えば、トイレセンサーなどの各種既存IoT製品がガイドライン適合製品として認知させることが可能になるでしょう。 現在のガイドラインのままでしたなら、住まい手及び関係業者も正しい選択をすることは、難しいと思います。 ひいては、目指すSociety5.0を実現させるスピードを阻害します。 （対応製品を区別するためのグレード別マークなどが、今後必要になるかと思います） （マークに関しては、電気製品のPSEのような考えかたが必要だと思います） また、ガイドラインに沿っていない低価格のIoT製品ばかりが流通するのを防ぐ一助にもなると思います。 グレードを設け、ガイドラインに記す目的は、IoT製品を、住まい手のみならず他の関係者も 自信をもって正しく選択できるようにする為です。 日本を訪れた観光客の多くは、日本の治安の良さに感心するらしいですが、 サイバー防御に関する治安を考えると、やられ放題の状況とも言えそうです。 スーパーシティ構想の一端を担うスマートホームからサイバー治安を考えるのは、日本の産業界においても有益であり、 競争力を高める事につながると思います。 また、都合の良い事に、スマートホーム向けのEchonet lite仕様もあります。 日本の家電業界が他国の家電業界と競争して抜き出る一つの切っ掛けがスマートホームであり、Echonet liteであると思います。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。

13	3	個人	セキュリティ要件は、ＩｏＴ機器ごとにグレード分けする必要があるのではないかと発言したものですが、 スマートホームとＩｏＴ機器のサービスをスマホにまで広めてサービスしている場合は、ＩｏＴ機器メーカーが 運用しているクラウドへの接続が基本設計になっているようです。 （ＩｏＴ機器　→　メーカークラウド　←　スマホ）---------　Ａ この方針の良くない所をいくつか列挙すると ・住まい手視点からすると、スマートホーム内のＩｏＴ機器がメーカー毎のクラウドへの接続になるので、利用費用アップと 運用手間の増大に直結する。 （Ｒ社からＮ社に給湯システムを変えた場合とかホーム内に、Ａ社、Ｂ社、Ｃ社のエアコンと監視カメラがあるとか） ・メーカー視点からすると、販売ＩｏＴ機器の原価の中にクラウド運用コストを入れなければならないが、５年分を見込むのか ２０年分を見込むのかと考えると、住まい手に負担をお願いしなければならないが、負担を要望しない競合会社があると、 競争力視点で考えると足並みを合わせなければならないという考えになりがち。 ・デベロッパーの視点からすると、ビルトインで提供したＩｏＴ機器のメーカーはいつまでも、競争力のあるバージョンアップ製品を 供給して欲しいが、いっぽうベンダーロックによる競争力低下は避けたい。 ・メーカー視点からすると、クラウド運用のセキュリティ対策費用は、今後ますます高騰する事が予想されるので、 できればクラウドは利用したくない（万一、クラウドをハッキングされた場合のリカバリーコストが膨大になる） 海外にＩｏＴ機器を展開するにも、クラウドが日本にある事が問題になりそう。　また、欧米の個人情報に関する要求レベルに応えるのは厳しい。 結果、ガラパゴス仕様になる可能性がある。 いっぽう、スマートホームから始まるSociety5.0の視点から見ると住まい手が利用したいというサービスは、それがクラウドを利用するもので あっても、どんどん増えて欲しいはずです。 ただしセキュリティを落とさずにです。 例えば監視カメラを引き合いに出すと、日本のメーカーのコンプライアンスがしっかりした企業が提供するサービスは、クラウドを利用しています。 ネットを流れるデータ量が多い事もあるからだと思いますが１台あたり月額１０００円前後です。 一方、安さを訴求する輸入業者が販売するカメラは、クラウドを利用しない仕組みを提供しており、月額費用は、不要ですが、 セキュリティに対しては万全ではない事を説明書に書いています。 何か問題が発生したら説明書に書いている事で担保しようとしているように見受けられます。 当然、Society5.0が目指すセキュリティではないです。 住まい手が、トイレセンサーを設置した場合も、あるメーカーの提示金額は、これも月額１０００円前後です。 このように、住まい手が使用したいサービスがあれば、１つのシステムに対してこの程度の金額が、発生するようです。 となると、利用したいサービスがｎ個あると、月額費用は　ｎ×１０００円となり、未来のスマートホームは、お金がかかるねってことで ＩｏＴ機器を利用したいというマインドの醸成は難しいのではないでしょうか？ メーカーもクラウドを利用したいわけではないですが、現状はクラウドが必須の状態です。 この結果、クラウドを利用する限り、以下の選択肢しかないように思えます。 ・メーカーで仲間づくりして、クラウドサービスを提供する （例：ＰチームとＳチームなど） ・デベロッパーが、独自にＨＵＢ的クラウドを作り上げ運用する各メーカーのクラウドは、デベロッパーのＨＵＢの下につくイメージ ・Echonet協議会のような団体が、必要経費を集める仕組みを作りメーカーにクラウドを提供する ガイドラインには、住まい手がスマートホームならではのサービスを受ける為に必要な費用を抑える仕組みが書かれていません。 しかし、課題として認識している事を記しておく事は、様々な分野から英知を集めるきっかけになるのではないでしょうか？ まとめると、スマートホームの家の中のＩｏＴ機器の制御は、家の中だけにとどまらない方向で世の中は動いていくと感じています。 スマホとの連携を念頭に置いたSociety5.0を進めるなら、サービスを増やす事だけがエンジンになるのではなく 住まい手が利用する際のコストを抑える事も必要であり、この二つがそろってはじめて、Society5.0が利用され、 他の国のスーパーシティと有意な比較が可能となると思います。 その為には、上記のＡで示したデータの流れを変えるのが、課題解決に至る一案になりそうです。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
13	4	団体	貴省が 平成３０年３月１３日に「産業サイバーセキュリティ研究会WG スマートホームSWG」を設置、検討を続けられ、「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン（案）」にまとめられ、私たち利用者に向けた対策まで検討されたことは高く評価致します。さらに、わかりやすい内容で、「スマートホーム」について学ぶことに役立ち、大変勉強になりました。ただ、残念なことも目につきましたので意見を述べさせていただきます。 住まい手の対策が、あまりにも当たり前な内容で有益な情報に思えません。貴省のホームページで「産業サイバーセキュリティ研究会WG スマートホームSWG」の委員名簿を拝見、「スマートホームの住まい手」の立場の委員はご不在のようで、今回の専門家目線の内容を理解した次第です。 利用者の立場の委員の参加も必要ではないでしょうか。さらに、利用者の総合的な相談窓口設置などもご検討願います。 P25　4.1.　「（１）スマートホーム向けIoT機器の事業者」 ４．１　　機器のセキュリティについて　住まい手が使用するIoT機器について　住まい手が不正アクセスされた機器であることが分かる機器の認証制度を作る取り組みを希望します。 P26　4.1.4「スマートホーム向けIoT機器の事業者」 利用者にIoT機器の使い方や使用環境をガイドすることは機器を利用する者にとって必要であり大変重要なものです。住まい手が読みやすくわかり易い内容であって欲しいものです。ガイドは一回のみではなく、一定の期間ごとあるいは変更があるごとに行われることが望ましいと思います。利用者と繋がることで、購入後の新たなリスクを共有できると考えます。 P27　4.3.2「スマートホーム向けのサービス事業者」 サービス事業者は、スマートホーム全体のセキュリティシステムを扱う立場から、被害が発生した場合の対応窓口を明確にし、契約書に明記する等の方法により、住まい手に対応窓口を周知してください。 P28　4.4　「(4)スマートホームを供給する事業者」 分譲共同住宅、賃貸共同住宅において、IoT機器やネットワークを配置する場合、子育て世代、単身者や高齢者など様々な住まい手のニーズに合った機器で、住まい手が使用方法、安全性やリスクを理解して正しく使用できるものが望ましいと思います。そのような機器の選択と、使用者への機器の操作や安全性、リスクについての丁寧な説明を供給する事業者に求めます。 P29　4.5「(6)スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社」 「(7)スマートホーム化された賃貸住宅の所有者や管理受託会社」 共同住宅では予めIoT機器が設置されていることもあり、機器の維持、管理について、管理組合や管理組合から委託された管理受託会社に、担当する管理者が必要と考えます。 一部の住戸または共有部分のIoT機器から、個人情報漏洩や物理的被害などが生じた場合、他の住戸に被害が及ぶリスクもあり、事故や、問題が生じた時に対応できるようにしておくことが重要と思います。 P30～31　4.6.1～4.6.3「スマートホームの住まい手」 4.6１～３.住まい手に向けたガイドラインは、住まい手が安全に安心して機器を利用する上でとても大切なことで、住まい手がきちんとこれらのことを行うことが望まれます。しかしながら、どれだけの住まい手がこれらのことに関心があり、また機器の仕組を理解し、リスクを認識して機器を選択・使用できるかはわかりません。消費者庁とも連携し、住まい手の啓発をより一層進めていくことで、超スマート社会（Society5.0）が安全に発展していくことにつながると考えます。 その他 今回のガイドラインは最低限の対策ということですが、スマートホームの住人は複数である場合が多く、機器操作に対しての理解度に差があることが予想されます。誤操作を防ぐシステムは最高の物であってほしいと思います。 また、火災や機器の暴走など何らかの事故が発生した場合、住まい手自身でその原因を調査することは困難です。何らかの保険や事故の原因を総合的に調査する機関があると利用者の安心につながるのではないかと思います。 以上。	いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。

14	1	団体	P1「1.1ガイドラインを策定する目的」の第４段落１行目「実際の対象は一般住宅であり」を、「実際の対象は大別すると戸建住宅と共同住宅であり」と修正する。 （理由）この「一般住宅」の言葉で表現したい内容は、P3「1.3対象とするスマートホーム」の第４段落第１行目～２行目「一般的に、住宅は「戸建」と「共同住宅」の二つに分類される」を包含したものであると考えられる。一方、政府で住宅政策を所管する国土交通省は、住宅税制において「一般住宅」の言葉を「質の高い住宅以外の住宅」として用いており、今回のガイドラインで表現したい内容と異なっている。他省庁とはいえ同一政府の文書の中で、このような違いがあると、読者の誤解を招くおそれが大きい。そのため、表現を修正すべきと考える。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「実際の対象は一般住宅であり」を、「対象は戸建住宅や共同住宅等の住宅である」と修正。
14	2	団体	P1「1.1ガイドラインを策定する目的」の第４段落第６～７行目「スマートホームでは、一般住宅の様々なIoT機器がサイバー攻撃の対象となるため、その数は膨大となる。」を、「スマートホームでは、戸建と共同住宅の様々なIoT機器がサイバー攻撃の対象となるため、セキュリティ対策が必要な機器の数は膨大となる。中でも、共同住宅の共用部分に設置されたIoT機器等がサイバー攻撃の対象となった場合、対応する主体が共用部の所有者（分譲共同住宅の場合は全ての区分所有者）となることに留意が必要である。」と修正する。 （理由）「一般住宅」の表記を修正するのは（１）の指摘と同じ趣旨。 「その数は膨大となる」の表記で、誤解を生まないよう、「その」の内容を明確に示すことが望ましいと考える。 また、共同住宅には専有部と共用部があり、戸建には存在しない共用部の対策が必要となる点に留意が必要である（専有部のサイバーセキュリティ対策は戸建とほぼ同一である）。共用部の対策が必要となることを、分譲共同住宅の区分所有者、賃貸共同住宅の所有者に認識してもらい、適切に対処してもらうことが、P1「１．はじめに」の「本ガイドラインは、スマートホームにおけるセキュリティ対策の考え方、ならびに各関係者が考慮すべき最低限のセキュリティ対策を示している」に資することであるので、本「1.1ガイドラインを策定する目的」においても明記しておくことが望ましいと考える。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「スマートホームでは、一般住宅の様々なIoT機器がサイバー攻撃の対象となるため、その数は膨大となる。」を、「スマートホームでは、住宅の様々なIoT機器がサイバー攻撃の対象となるため、セキュリティ対策が必要な機器の数は膨大となる。」とし、更に続けて「さらに、スマートホームには様々なステークホルダーが関与し、多様な脅威に対しステークホルダーがそれぞれで対応する必要がある・・。」と修正。 ・脚注に「例えば、共同住宅の共用部分に設置されたIoT機器等がサイバー攻撃の対象となった場合、対応する主体が共用部分の所有者（分譲共同住宅の場合は全ての区分所有者）となることに留意が必要である。」と追記。
14	3	団体	P2「1.2ガイドラインの対象者　(6)スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社」の文末に「なお、管理受託会社がステークホルダーとなるためには、管理組合と管理受託会社が締結する管理委託契約（あるいは管理委託契約とは別個に管理組合と管理受託会社が締結する契約、以下「管理委託契約等」と表記する）に、機器やネットワーク回線の管理に関する条項が含まれていることが必要であることに留意すべきである。」と追加する。 （理由）管理組合が管理受託会社に委託する業務内容は管理委託契約等の中に明記される。管理組合は、通常は機器やネットワーク回線の管理を管理受託会社（又はその下請け再委託先）に委託すると考えられるため、その内容を管理委託契約等に明記する必要がある。 なお管理委託契約等に明記しない場合は、管理受託会社等が機器やネットワーク回線の管理を受託しないため、ステークホルダーにならず、管理組合が自ら対応することになる。	いただいた御意見を踏まえ、以下のとおり修正します。 ・脚注に「分譲共同住宅の管理組合や賃貸共同住宅の所有者（オーナー）と管理受託会社が締結する契約等に、共用スペースのIoT機器やネットワーク回線等を管理する条項が含まれている場合には、原則として条項の内容に従う。」と追記。
14	4	団体	P4「表1.戸建住宅に関するステークホルダー」、宅内のネットワークの１つめの（）内およびIoT機器の２つ目の（）内、「スートホーム」は、「スマートホーム」の誤り（P5-6表2にも同様の箇所が４か所存在）。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「スートホーム」を「スマートホーム」に修正。
14	5	団体	P5脚注1.「管理主体とは、スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社、またはスマートホーム化された賃貸住宅の所有者や管理受託会社である。」を「管理主体とは、スマートホーム化された分譲共同住宅・団地の管理組合、またはスマートホーム化された賃貸住宅の所有者であり、それぞれが管理受託会社（又はその下請け再委託先。以下両方を包含して「管理受託会社等」と表記する）に共用部分のネットワーク・IoT機器等の管理を委託する場合には管理受託会社等も含む。」と修正する。 （理由）ネットワーク・IoT機器等の管理について管理委託契約等に明記していない場合は、管理受託会社等が当該管理を受託しないため、ステークホルダーとならないため。	いただいた御意見を踏まえ、以下のとおり修正します。 ・脚注に「分譲共同住宅の管理組合や賃貸共同住宅の所有者（オーナー）と管理受託会社が締結する契約等に、共用スペースのIoT機器やネットワーク回線等を管理する条項が含まれている場合には、原則として条項の内容に従う。」と追記。 ・脚注「管理主体とは、スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社、またはスマートホーム化された賃貸住宅の所有者や管理受託会社である。」を「管理主体とは、スマートホーム化された分譲共同住宅・団地の管理組合、またはスマートホーム化された賃貸住宅の所有者であるが、IoT機器やネットワーク回線等の管理を契約等により管理受託会社等（場合によってはその下請け再委託先も含む）に委託する場合、管理受託会社等も管理主体となる。」と修正。
14	6	団体	P16脆弱性の表内(U1_V.5)「共同住宅の共用部分に設置されたIoT 機器では、住棟内ネットワーク、住棟内ネットワークに接続されている他の機器、宅内のネットワーク、宅内のネットワークに接続された他の機器が、想定された用途・用法に基づき設置・設定・運用されていない。」を「共同住宅の共用部分に設置されたIoT 機器では、共用部分内のネットワーク、および共用部分内のネットワークに接続されている他の機器が、また専有部分内のネットワーク、および専有部分内のネットワークに接続されている他の機器が、それぞれ想定された用途・用法に基づき設置・設定・運用されていない。」と修正する。 （理由）(U1_V.4)の表記に合わせつつ、共用部分と専有部分の記述が並列であることを明確にするため。また、「宅内」「住棟内」の表記を、建物の区分所有等に関する法律の文言の「共用部分」「専有部分」に平仄を合わせるため（なお、この表記はガイドライン全体に散見されるため、全て同様に修正する）。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「共同住宅の共用部分に設置されたIoT 機器では、住棟内ネットワーク、住棟内ネットワークに接続されている他の機器、宅内のネットワーク、宅内のネットワークに接続された他の機器が、想定された用途・用法に基づき設置・設定・運用されていない。」を「共同住宅では、住棟内ネットワーク、住棟内ネットワークに接続されているIoT機器以外の機器、および住戸内ネットワーク、住戸内ネットワークに接続されているIoT機器以外の機器が、想定された用途・用法に基づき設置・設定・運用されていない。」と修正。 ・脚注に「本書では、建物内に存在する共用スペースのネットワークのことを指す。共用スペースのネットワークは、住まい手が管理すべき住戸のネットワークとは異なる者が一般的に管理する。例えば、分譲住宅では、階段等の共用部分は、各住戸の住まい手が共同して所有・管理する位置付けであり、各住戸の住まい手から構成される管理組合が、共用部分の機器やネットワークを主体的に管理・運用する必要がある。」と追記。 ・関連する他の箇所にも同様の修正。 ・「共用スペース」を用語集へ追記。
14	7	団体	P20【共同住宅の共用部分におけるIoT 機器】表内「前提条件」の「共同住宅の共用部分においては、マンションデベロッパー等をはじめとするスマートホームを供給する事業者により、施工時からネットワークやIoT 機器が据え付けられている場合が基本となるが、分譲共同住宅・団地の管理組合や管理受託会社、または賃貸住宅の所有者や管理受託会社管理組合または管理受託会社によって据え付けられることもある。」を「共同住宅の共用部分においては、分譲共同住宅・団地の区分所有者または賃貸住宅の所有者が引渡しを受ける前から設置される場合はマンションデベロッパー等をはじめとするスマートホームを供給する事業者によってネットワークやIoT 機器が据え付けられるが、引渡し後では分譲共同住宅・団地の管理組合、または賃貸住宅の所有者等により据え付けられる」と修正する。 （理由）住宅の事業の各タイミングにおける設置主体の関係を明確にするため。 なお所有者が１名の１棟賃貸共同住宅の場合には管理組合は存在しないため、誤解を招かないように原表記を変更する。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「共同住宅の共用部分においては、マンションデベロッパー等をはじめとするスマートホームを供給する事業者により、施工時からネットワークやIoT 機器が据え付けられている場合が基本となるが、分譲共同住宅・団地の管理組合や管理受託会社、または賃貸住宅の所有者や管理受託会社管理組合または管理受託会社によって据え付けられることもある。」を「 IoT機器やネットワーク設備は、一般的に、分譲共同住宅・団地の区分所有者または賃貸住宅の所有者への引き渡し前にマンションデベロッパー等をはじめとするスマートホームを供給する事業者によって据え付けられる。引き渡し後については、分譲共同住宅・団地の管理組合、または賃貸住宅の所有者等によりIoT機器が据え付けられる」と修正。
14	8	団体	P29　『4.5.「（６）スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社」「（７）スマートホーム化された賃貸住宅の所有者や管理受託会社」』の枠内に記載された２つの対策に加えて、最後に「・分譲共同住宅・団地の管理組合、賃貸住宅の所有者は、IoT機器やネットワークの管理、ファームウェアアップデート等の事項を、管理受託会社等と締結する管理委託契約等に入れる」を追加する。 （理由）管理組合が管理受託会社に委託する業務内容は管理委託契約等の中に明記される。管理組合は、通常は機器やネットワーク回線の管理を管理受託会社等に委託すると考えられるため、その内容を管理委託契約等に明記する必要がある。 なお管理委託契約等に明記しない場合は、管理受託会社等が機器やネットワーク回線の管理を受託しないため、ステークホルダーにならず、管理組合が自ら対応することになる。	いただいた御意見を踏まえ、以下のとおり修正します。 ・脚注に「分譲共同住宅の管理組合や賃貸共同住宅の所有者（オーナー）と管理受託会社が締結する契約等に、共用スペースのIoT機器やネットワーク回線等を管理する条項が含まれている場合には、原則として条項の内容に従う。」と追記。 ・「分譲共同住宅・団地の管理組合および賃貸住宅の所有者が、IoT機器やネットワーク回線等の管理を管理受託会社（場合によってはその下請け再委託先も含む）に委託する場合、セキュリティパッチ適用などのセキュリティ対策を実施する主体を契約等で明示することで、責任の所在を明確にすることができる。契約等に盛り込むセキュリティ対策の実施等については、業種・業態に応じて具体化する必要がある。」と追記。 ・4.5.1に「特に、導入している機器等 に脆弱性が発見されていないかを定期的に調べることや、最新のセキュリティパッチの適用やファームウェアアップデートなどを行うことが望まれる。」と追記。
14	9	団体	P29　『4.5.「（６）スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社」「（７）スマートホーム化された賃貸住宅の所有者や管理受託会社」』の「4.5.1共用部分や賃貸している住戸に設置する機器の選定と、機器やネットワークの管理・運用は適切に行う」の最後の段落「なお共同住宅においては、運用の一環として、セキュリティ事故発生時の対応フローや作業分担を、住まい手同士（管理組合）や管理受託会社と整合しておくことが有効である。」を削除する。 （理由）管理組合が管理受託会社に委託する業務内容は管理委託契約等の中に明記される。管理組合は、通常は機器やネットワーク回線の管理を管理受託会社等に委託すると考えられるため、その内容を管理委託契約等に明記する必要がある。 なお管理委託契約等に明記しない場合は、管理受託会社等が機器やネットワーク回線の管理を受託しないため、ステークホルダーにならず、管理組合が自ら対応することになる。	いただいた御意見を踏まえ、以下のとおり修正します。 ・脚注に「分譲共同住宅の管理組合や賃貸共同住宅の所有者（オーナー）と管理受託会社が締結する契約等に、共用スペースのIoT機器やネットワーク回線等を管理する条項が含まれている場合には、原則として条項の内容に従う。」と追記。 ・「分譲共同住宅・団地の管理組合および賃貸住宅の所有者が、IoT機器やネットワーク回線等の管理を管理受託会社（場合によってはその下請け再委託先も含む）に委託する場合、セキュリティパッチ適用などのセキュリティ対策を実施する主体を契約等で明示することで、責任の所在を明確にすることができる。契約等に盛り込むセキュリティ対策の実施等については、業種・業態に応じて具体化する必要がある。」と追記。

14	10	団体	P30『4.5.「（６）スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社」「（７）スマートホーム化された賃貸住宅の所有者や管理受託会社」』に、以下の通り4.5.3の項目を追加する。 「4.5.3.　分譲共同住宅・団地の管理組合、賃貸住宅の所有者は、IoT機器やネットワークの管理、ファームウェアアップデート等の事項を、管理受託会社等と締結する管理委託契約等に盛り込む 　4.5.1.の内容を適切に行うためには、共同住宅の共用部分を管理する管理受託会社等に行ってもらうことが望ましい。そのためには、分譲共同住宅の場合は管理組合が、賃貸住宅の場合は所有者が、それぞれ管理受託会社等と締結する管理委託契約等において、4.5.1.の内容の実施に関する事項、および運用の一環として、セキュリティ事故発生時の対応フローや作業分担を、明確に位置付けることが必要である。」を追加する。 （理由）管理組合が管理受託会社に委託する業務内容は管理委託契約等の中に明記される。管理組合は、通常は機器やネットワーク回線の管理を管理受託会社等に委託すると考えられるため、その内容を管理委託契約等に明記する必要がある。 なお管理委託契約等に明記しない場合は、管理受託会社等が機器やネットワーク回線の管理を受託しないため、ステークホルダーにならず、管理組合が自ら対応することになる。	いただいた御意見を踏まえ、以下のとおり修正します。 ・脚注に「分譲共同住宅の管理組合や賃貸共同住宅の所有者（オーナー）と管理受託会社が締結する契約等に、共用スペースのIoT機器やネットワーク回線等を管理する条項が含まれている場合には、原則として条項の内容に従う。」と追記。 ・「分譲共同住宅・団地の管理組合および賃貸住宅の所有者が、IoT機器やネットワーク回線等の管理を管理受託会社（場合によってはその下請け再委託先も含む）に委託する場合、セキュリティパッチ適用などのセキュリティ対策を実施する主体を契約等で明示することで、責任の所在を明確にすることができる。契約等に盛り込むセキュリティ対策の実施等については、業種・業態に応じて具体化する必要がある。」と追記。 ・脚注に「共同住宅の共用部分のIoT機器やネットワーク回線等の管理を管理受託会社等に委託する場合は、4.5.1の内容の実施に関する事項だけでなく、セキュリティ事故発生時の対応フローや作業分担を、契約等に明記するべきである。例えば、分譲共同住宅の場合には、管理組合と管理受託会社等との間で締結する契約等に明記すべきである。賃貸住宅の場合には、住宅の所有者と管理受託会社等との間で締結する契約等に明記すべきである。」と追記。
15	1	個人	・目次のローマ数字３の「添付Ｃ　対策要件（添付Ａ）とガイドの対応」は「添付Ｃ　ガイドと対策要件（添付Ａ）との対応」のほうがよいと思います。 ・３ページの１６行目「スマートメーター」と貼付A-1の「想定されるインシデント」欄の「エネルギーメータ」とは同じものを指しているのか？（同じものであるならば、「メーター」と「メータ」とは、どちらかに字句を統一したほうがよい。） ・４ページの２行目「表1 戸建住宅」は「表1.戸建住宅」の誤記ではないか？ ・４ページの「表1」の「関連するステークホルダー」欄の「宅内のネットワーク」の５行目「スマート向け」は「スマートホーム向け」の誤記ではないか？ ・４ページの「表1」の「関連するステークホルダー」欄の「IoT機器」の７行目「スマートホーム向」は「スマートホーム向け」の誤記ではないか？ ・６ページの最下行から上に５行目「つながる」と、８ページの４行目等の「繋がる」とは、意味に違いがあるのか？ ・添付E-1ページの添付E-1ページの「さ行」の４行目「Cyber」は「Cyber Space」の誤記ではないか？「 ・添付E-2ページの「さ行」の「Society5.0」は「Society 5.0」のほうがよいと思います。 ・添付E-2ページの「た行」の「DDos」は「DDoS」の誤記ではないか？ ・添付E-2ページの「な行」の記載内容がないのであれば削除したほうがよいと思います。 ・添付E-3ページの３行目「範囲」は「距離の範囲」のことを意味しているのか？ ・添付E-3ページの「ら行」の２行目の行末の記載が漏れています。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「添付Ｃ　対策要件（添付Ａ）とガイドの対応」を「添付Ｃ　ガイドと対策要件（添付Ａ）との対応」と修正。 ・「メーター」に統一。 ・「表1 戸建住宅」を「表1.戸建住宅」と修正。 ・「スマート向け」を「スマートホーム向け」と修正。 ・「つながる」に統一。 ・「Cyber」を「Cyber Space」と修正。 ・「Society5.0」を「Society 5.0」と修正。 ・「DDos」を「DDoS」と修正。 ・「LAN」の行末を「建物内部などの限られた範囲のネットワークも含む。」と修正。 なお、記載事項のない行についても明記をさせていただいております。
16	1	個人	スマートホームとＩｏＴ機器のサービスをスマホにまで広めてサービスしている場合は、ＩｏＴ機器メーカーが運用しているクラウドへの 接続が基本設計になっていて、以下の接続です。 （ＩｏＴ機器　→　メーカークラウド　←　スマホ）---------　A と発信した者ですが Aの図式でメーカークラウドを利用する理由は、２つあると思います。 ・スマホのグローバルIPアドレスが固定でない事。 ・メーカーが情報を収集する為。 今、考えるべきは、汎用TCP／IP製品・システムを利用する事がセキュリティ防御の視点から見て Ａの図式が最適か否かという事ですが、そうではないと考えます。 では、どうするのかというと、スマートホームからインターネット経由で接続する相手は、 スマートホームに住む、住まい手に限定するべきだという考えかたです。 別言すると、汎用TCP／IP製品・システムを利用するのではなくて、スマートホーム内のIoT機器と、 このスマートホームに住む、住まい手が保有・所持するスマホとの間だけの接続しか許さない、接続制限を課すいう事です。 この標準化ができれば、セキュリティ投資コストを抑える事が出来るだけでなくセキュリティ強化にも役立ちます。 Aの場合、グローバルIPアドレスで運用しているクラウドサーバーは、ハッカーの標的になりがちで、対策が恒久的に必要です。 また、Aの手法でルーターの配下にあるIoT機器（プライベートIPアドレスで運用されている）であっても 通信先を限定していないので、DNS詐称攻撃に限らず、既知の攻撃手法でのハッキングが可能です。 新しいハッカー対策を図式すると以下になります。 （ＩｏＴ機器　←→　スマホ）---------　B このBのメリットは、住まい手がIoT機器とこれらのIoT機器と接続可能なスマホを自分で登録管理（ACLを構築する）しなければ、 実現できないシステムとして提供できるという点にあります。 また、今月、８月４日（火）の日経新聞に掲載されていた記事によるとスマートホームのIoT機器が今後備えるべき機能として政府が要求する 素案として挙げられていた「侵入による突然の接続を日常的な接続と区別し、遮断する仕組み」をＢなら実現しやすくなります。 さらには、情報銀行との親和性をも高める事が出来ます。情報銀行をBにいれると、以下になります。 （ＩｏＴ機器　←→　スマホ　→　情報銀行　→　メーカー）---------　C このように、スマートホームに、情報銀行に情報を提供するスキームも ガイドラインの記述を追加する事により、きれいにできると考えます。 以上、私のパブリックコメントをまとめると ・サイバー攻撃に強いスマートホームが、スーパーシティ構想の礎になる。 ・スマートホームのIoT機器を利用するシーンにおいて、セキュリティが要求されるのは、遠隔操作を許可したIoT機器とスマホ。 （GAFAが市場を取りたがっているスマートスピーカーへの攻撃は 直接的なサイバー攻撃ではないので、今回の議論から省く） ・スマートホームのIoT機器を遠隔操作したい場合は、最大公約数的な機能を搭載したアプリで対応すべき （住まい手がメーカーに限らず利用可能となるだけでなく、世界標準仕様になりうるEchonet Liteを支援するタイミングとして最適ではないか） （Echonet Lite仕様のアプリを推奨） （IoT機器の差別化機能を利用したい住まい手は、スマートホームに着いてから利用してもらえばよいという考え方） ・スマート家電、センサーの標準仕様を広く世界に広めれる可能性が増す。 （なるべく早いタイミングでガイドラインを意識して業界統一仕様の利用に推進していかないと、 世の中に非互換でセキュリティの弱いIoT機器が氾濫し、ガイドラインがあっても、目指す安全なスマートホームの実現が難しくなる） ・遠隔操作する制御データやIoT機器からのデータをメーカーのクラウド サーバーで中継する手法は、コスト、セキュリティの観点から望ましくない。 ・図式Bの考えかたが、一般的なサイバー攻撃に強いのは、スマートホームのルーターの配下のIoTゲートウェイ配下のIoT機器は、 プライベートIPアドレスになり、IoTゲートウェイを上記に記した汎用性のない特定のIoT機器と特定のスマホとの間でしか通信できない 仕組みにすることにより、ハッカーの大半の攻撃を遮断できる ・情報銀行との親和性が高い。理由はデータの販売管理が個人の判断によらざるを得ない。 クラウドサーバーに蓄えられた個人データーの販売を個人が許可するスキームより理解しやすく安心。 ・スマート工場にも適用可能。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
17	1	団体	本ガイドラインの対象者にはガイドに記載されておりますように， (6)スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社 (7)スマートホーム化された賃貸住宅の所有者や管理受託会社 (8)スマートホームの住まい手 が想定されておりますが，これらの一般の方によりよく理解いただくために，下記の内容について対応いただけるとよいと考えます。 １．「1.1ガイドラインを策定する目的」における事例の組み入れ タイトルの安心・安全に対して，どのようなリスクに対してのガイドラインを策定・記載しているのかを添付Ｄのサイバー攻撃の事例の前段記載の3つの分類を記載して示した方が，より興味をもって理解いただけると考えます。 個々の事例は添付Ｄに記載している旨も追記すると良いと考えます。 ２．全般的に耳慣れない用語について，ガイド(案)文中の初出時点で添付Ｅに説明の旨があることの記載があると理解の助けになると考えます。 以上，コメントさせていただきます。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「また、IoT 機器の誤使用の可能性、サービスで必要となる個人情報の漏洩、サービスによってはサイバー攻撃が開錠や閉じ込めといったフィジカル空間の問題を引き起こす可能性もある。」を「また、添付Dに示す事例のように、IoT 機器の脆弱性、サービスで必要となる個人情報の漏洩、サービスによってはサイバー攻撃がドアの開錠や空調などの家電の不正操作といったフィジカル空間のセーフティまで影響を及ぼす可能性もある。さらに、社会全体で考えると、IoT 機器が乗っ取られ踏み台として悪用されることも脅威となる。」と修正。 なお、添付Eは用語集という位置づけのため目次記載のみにとどめさせていただきます。

18	1	企業	以下の箇所に誤字・脱字があると思われます。 p4 表1 「スマート向けに」⇒「スマートホーム向けに」(1か所) 「スートホーム」⇒「スマートホーム」(4か所) p5 表2 「スートホーム」⇒「スマートホーム」(6か所) p19 16行目 「暗号化されていないによる無線通信」⇒「暗号化されていない無線通信」 p27 3行目 「廃棄処理するこが必要」⇒「廃棄処理することが必要」 p27 31行目 「廃棄処理するこが必要」⇒「廃棄処理することが必要」 p26 6行目 「IoT 機内に」⇒「IoT 機器内に」 p27 7行目 「機内に保存」⇒「機器内に保存」	いただいた御意見を踏まえ、以下のとおり修正します。 ・「スマート向けに」を「スマートホーム向けに」に修正。 ・「スートホーム」を「スマートホーム」に修正。 ・「暗号化されていないによる無線通信」を「暗号化されていない無線通信」に修正。 ・「処理するこが必要」を「処理することが必要」に修正。 ・「IoT 機内に」を「IoT 機器内に」に修正。 ・「機内に保存」を「機器内に保存」に修正。
18	2	企業	体裁のみの内容となりますが、以下の箇所のみフォントがゴシック体になっているため、明朝体に合わせるべきと考えます。 p4 表1 「～向けにメンテナンスやサポートを行う事業者」 p16 4行目 「～に設置されたIoT機器では、住棟内ネットワーク、住棟内ネットワークに接続されている他の機器、宅内のネットワーク、宅内のネットワークに接続された他の機器が、想定された用途・用法に基づき設置・設定・運用されていない。」	いただいた御意見を踏まえ、以下のとおり修正します。 ・文字のフォントを統一。
18	3	企業	添付E-3のら行の文中において、「LAN」の説明が途中までの記載となっているため、最後までの内容記載が必要です	いただいた御意見を踏まえ、以下のとおり修正します。 ・「LAN」の行末を「建物内部などの限られた範囲のネットワークも含む。」と修正。
18	4	企業	以下の箇所で「容易に削除できる機能を提供する」との記載となっていますが、削除できる機能を提供することが対策であり、容易さを求める必要性はないと思われるので「削除できる機能を提供する」で良いと考えます。 添付B-2 MO.12 添付B-3 RMO.4, SO.4	いただいた御意見を踏まえ、以下のとおり修正します。 ・「容易に削除できる機能を提供する」を「消去（サニタイズ）するなど、データの再利用を防止する機能を提供する」と修正。
18	5	企業	以下の箇所の「・IoT機器のソフトウェア自動更新機能を有効化して運用すること」にあるソフトウェア自動更新機能が、もしMO.14及びHO.2によりソフトウェアの完全性の検証機能を有する前提なのであれば「・完全性を検証する機能を有する場合は、IoT機器のソフトウェア自動更新機能を有効化して運用すること。」のように明記する必要はないでしょうか。 添付B-2 RMO.1 添付B-4 SMO.1	いただいた御意見は、ガイドラインの更なる検討を進めていくに当たって参考にさせていただきます。
18	6	企業	添付E-1 インシデントの説明文において、「事業運営を危うくする確率および脅かす確率が高いもの。」との2つの確率を並べた記載に違和感があります。 もし「JIS Q 27000:2014 箇条 2.36」記載を踏襲されているのであれば「事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。」になるのではないでしょうか。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「望まない単独若しくは一連の事象、または予期しない単独若しくは一連の事象であって、事業運営を危うくする確率及び脅かす確率が高いもの。」を「望まない単独若しくは一連のサイバーセキュリティ事象、又は予期しない単独若しくは一連のサイバーセキュリティ事象であって，事業運営を危うくする確率及びサイバーセキュリティを脅かす確率が高いもの。」と修正。
18	7	企業	p1 15,16行目のSociety 5.0の説明において「仮想空間と現実空間を」と記載されていますが、CPSFでは「サイバー空間とフィジカル空間」として記載されており、他箇所でもサイバー空間、フィジカル空間を主に使用(仮想空間、現実空間は括弧による表記)されているので、一貫性の観点では「サイバー空間とフィジカル空間」と記載するほうが良いのではないでしょうか。	いただいた御意見を踏まえ、以下のとおり修正します。 ・「仮想空間と現実空間」を「サイバー空間とフィジカル空間」と修正。
19	1	個人	各所の各機器及び各通信機器について、適切にファイアウォール・SPIフィルタの設定が行えるようになっている事（必要性がある場合のMACアドレスフィルタもであるが。）、ログ機能が充実している事が行われていると適切なはずである、という意見を、依然として行う。 もう20年以上、そういう事が主張され続けてきているのではないかと思われるのであるが、各所において、ファイアウォールとSPIフィルタの使用がなされると、セキュリティは大幅に高まるのではないかと考える。(また、適切なログがあれば、侵入の検知も行えるし、各種の診断も行えるはずである。） しかし、経済産業省も、電気通信にいくばくか関わりがある省庁であれば、有線通信について、Wi-Fiと同じような、暗号化通信と端末の接続管理機能がある様なルータ・ハブ（もちろん、有線通信であるので衝突事態への対応などの方式は変えて良いが）の開発を行うようにしていただけないであろうか。（まずは研究開発の段階からであろうが、総務省と共同所管している配下の行政的な機関がいくつかあるはずであろう。貴省などが、その様な機器について推進するべき立場だという事には、なるはずである。） 市民としては、無線通信であれば安くから暗号化通信や接続端末管理機能が付いているルータ・アクセスポイントが標準的なのに、有線通信ではその様なルータ・ハブが無いのが疑問であり不満であるのであるが、市井のセキュリティ向上のため、その様な事も行っていただきたいと考える。 まず要素技術について確実なものとしていくのが良いのではないかと考えるが、各所の各機器が安全であるようにしていっていただきたい。 でないと、スマートホームなど、とても怖くて導入していく気になれない、というのが市民としての意見である。 意見は以上である。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。