「IoTセキュリティガイドライン」（案）に対する意見募集の結果について

別紙３

1　概要

「IoT推進コンソーシアム　セキュリティワーキンググループ」における議論をまとめたIoTセキュリティガイドライン（案）について、総務省ホームページ及び電子政府の総合窓口を通じ、平成28年6月1日（水）～同6月14日（火）までの間、幅広く国民より意見募集を実施。

2　意見提出者

計29者から意見提出あり。意見提出者は下表のとおり。

＜企業・団体:　22者＞　　（50音順）

1	アラクサラネットワークス株式会社
2	一般社団法人重要生活機器連携セキュリティ協議会
3	一般社団法人情報処理学会
4	一般社団法人情報通信ネットワーク産業協会（CIAJ）
5	一般社団法人テレコムサービス協会
6	一般社団法人電子情報技術産業協会（JEITA）
7	一般社団法人日本クラウドセキュリティアライアンス
8	インテル株式会社
9	NPO日本ネットワークセキュリティ協会
10	株式会社パソナサイバーラボ
11	株式会社ベリサーブ
12	株式会社ラック
13	KDDI株式会社
14	次世代ICカードシステム研究会
15	日本シノプシス合同会社
16	ネットエージェント株式会社
17	三菱電機インフォメーションシステムズ株式会社
18	モバイルコンピューティング推進コンソーシアム
19	力武健次技術士事務所
20	企業・団体（匿名）A
21	企業・団体（匿名）B
22	企業・団体（匿名）C

＜個人:　5者＞

＜記名なし:　2者＞

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
1	個人A	全体	全体	全体	再検討を提言致します。 セキュリティーの対象は情報というコンテンツである。 IoTは戦略である。 戦略にセキュリティーは存在できない。 存在できないものにガイドラインはない。 そして「基本方針を定める」とか「経営者がコミット」などはガイドラインではない。（技術伝承ドットコム）	今後の取組の検討にあたっての参考にさせていただきます。
2	インテル株式会社	全体	全体	全体	インテル株式会社は、日本政府がIoTに関するセキュリティ対策に関して産業界および利用者を対象に指針を示すことは、他国に例が無く、国際的な枠組みの中で日本がリーダーシップを積極的にとり健全な国際的デジタルインフラの構築に寄与するという観点から、この文書の公開に賛成します。	本ガイドラインに対する賛同意見として承ります。
3	モバイルコンピューティング推進コンソーシアム	全般	全般	全般	【全般】 ガイドラインとして設計者に対し具体的な対策例・ユースケースが記載され利用できる。 しかしながら本ガイドラインを守ったサービス・機能を提供する際、サービス提供者、機器ベンダーの開発費用がアップする。 特にコンシューマ（一般利用者）製品では、現状セキュリティ対策は非機能要件であり価格に転嫁させることが難しいのが実態である。 本ガイドラインを浸透させるには、一般利用者がセキュリティ対策レベルを認識できる見える化、それによるセキュリティリスクに対する投資意識の向上、など普及促進に対する施策が課題であり検討事項として今後取り組んでもらいたい。	本ガイドラインに対する賛同意見として承ります。
4	個人B	全般	全般	全般	私は将来、情報セキュリティに関わる職業を目指している高校生です。 このたびは、IoTセキュリティに関わるパブリックコメントの募集がありましたので、投稿いたします。 本ガイドラインをすべて読ませていただきました。 私はこのガイドラインの必要性に疑問を感じました。 このガイドラインが、企業または利用者にとって「何を促進させ、何を円滑にする」になるためのものなのかというテーマが見えてこないように感じました。 ガイドラインなのですから、わかりやすく。そして、何をガイドするためのものなのかを具体的に示す必要があると考えます。 また、本ガイドラインにおいてIoTの危険性に重点がおかれていますが、IoTの利便性やメリットに関しても触れるべきだと考えます。	本ガイドラインの目的は1．2で記載しております。 なお、御指摘については、今後の検討における参考として承ります。
5	一般社団法人テレコムサービス協会	全体	全体	全体	本ガイドラインが「1.2 ガイドラインの目的」で書かれているように、「関係者間の相互の情報共有を促すための材料を提供する」として策定されることは極めて有用であると考えます。 IoTを取り巻く技術や環境の進歩が早いため、ガイドライン制定後も、常に更新することを期待します。	本ガイドラインに対する賛同意見として承ります。 また、御指摘の点に関しては、第4章に「今後、必要に応じて改訂を行っていく必要がある。」と記載しております。
6	株式会社ラックサイバー・グリッド・ジャパン	全体	全体	全体	総務省、経済産業省はじめ関係機関が、今般本ガイドラインをとりまとめされようとしていることに敬意を表する。ガイドライン策定後は、製造者や利用者への普及活動に関係者全員が取り組み、本ガイドラインの目的が達成されることを望む。	本ガイドラインに対する賛同意見として承ります。
7	株式会社ラックサイバー・グリッド・ジャパン	全体	全体	全体	特に、「一般利用者」については、対象読者として記述された部分は、P.11表2で示すように本ガイドラインのごく一部に過ぎないが、該当部分への理解を促すには一般利用者向け解説が必要と考える。	本ガイドラインに対する賛同意見として承ります。
8	一般社団法人電子情報技術産業協会（JEITA）	全体			今後のサイバーセキュリティ対応を考える上で基本となる非常によい資料であると認識している。関係各者のご尽力に感謝。 その一方で一般人（利用者）に対して1.1.1項 表1ベースメーカの事例等過度に危機感を与える例示があり、またIoTとして低廉な機材においてもとれる対策（例えば、以下の「要点8 ② 図9」に対する意見）があるように思う。 以下、具体的にコメントする。	次回改訂の際、参考とさせていただきます。
9	一般社団法人電子情報技術産業協会（JEITA）	全体			本ガイドラインに記載されている対策、あるいは脅威やリスクが表として一覧化されていると、ガイドラインの内容がより活用しやすいものになると考える。	
10	一般社団法人電子情報技術産業協会（JEITA）	全体			付録に参考文献一覧があると分かりやすい。	
11	一般社団法人重要生活機器連携セキュリティ協議会	全般	全般	全般	1）ガイドライン（案）全般について 日常生活をより便利にする様々なIoTサービスが、今後市場に展開されるにあたり、より安全・安心して利活用できるものとして提供される様、「セキュリティ・バイ・デザイン」の基本的な考え方を、IoTサービスにも展開するべくガイドラインとして全般的によくまとめられており、歓迎します。 特にIoTは、機器間、機器・サーバ間の連携構成が不可欠のため、IoTサービスを構成する機器メーカー・システム提供者、サービス提供者の関係者がそれぞれの視点で、連携機能を狙うセキュリティ脅威から守ることが強調されている点がCCDSの考え方とも一致しています。	本ガイドラインに対する賛同意見として承ります。
12	個人C	全般	全般	全般	現状についてよく認識された、なかなか良いガイドラインであると思われた。 特に問題点があるようには思えなかった。	本ガイドラインに対する賛同意見として承ります。
13	三菱電機インフォメーションシステムズ株式会社	－	その他		Raspberry Pi等で個人が製作した様な機器、フリーソフト等に潜むリスクに対する考え方も必要ではないでしょうか。	今後の検討における参考として承ります。
14	三菱電機インフォメーションシステムズ株式会社	－	その他		国際的な法規制との連携等の考え方、方針等の情報を提供いただきたい。	御指摘の点に関しては、第4章の今後の検討事項の法的責任として整理していく必要があると考えており、今後の取組の検討の参考とさせていただきます。
15	三菱電機インフォメーションシステムズ株式会社	－	その他		IoTコアモジュール（デバイス、ゲートウェイ、クラウド、ほか）の個々についてセキュリティの第三者認証が必要ではないでしょうか。	第三者認証については、要点12にその有用性を記述してありますが、IoTコアモジュール（デバイス、ゲートウェイ、クラウド、ほか）の個々についてセキュリティの第三者認証の必要性については今後の取組の検討にあたっての参考にさせていただきます。
16	三菱電機インフォメーションシステムズ株式会社	－	その他		IoTセキュリティマネジメントの法人認定資格等の整備の検討も必要ではないでしょうか。	今後の取組の検討にあたっての参考にさせていただきます。
17	次世代ICカードシステム研究会	－	その他（留意事項や情報提供など）		（留意事項） IoT機器やサービスはグローバルに展開されているため、提供者、利用者ともに情報の取扱いに関する各国の法規制や罰則などに注意する必要があることを明記すべきです（個人情報保護法の他、IoT分野特有の国際的な連携を想定しています）。	今後の検討における参考とさせていただきます。
18	一般社団法人情報通信ネットワーク産業協会(CIAJ)	－	その他		本ガイドラインは、一般ユーザーにも周知が必要なものであり、どのように国民に理解を深めてもらうかの工夫も必要だと思います。	今後の検討における参考とさせていただきます。
19	一般社団法人情報処理学会	－			IoTデバイスの普及が，今後も飛躍的に増加すると予測される中，IoTに特化したセキュリティのガイドラインが策定されることに賛同いたします． ご提示の案はIoT機器・システム・サービスの関係者に対するセキュリティのガイドラインとして，何をすべきか／した方が良いのかという点において複数の異なる視点で整理され指標が提示されており，特にサービス提供者にとって有益なガイドラインになっていると考えます．	本ガイドラインに対する賛同意見として承ります。
20	一般社団法人情報処理学会	6			一方で，ぜひ検討していただきたい点について以下に記します． 1点目として，IoTに特化していない内容も含まれているのではないでしょうか． 1.2節にガイドラインの目的として，「本ガイドラインは，上記のIoT特有の性質とセキュリティ対策の必要性を踏まえて・・」とありますが，2章冒頭の要点1と2は，IoT特有の話ではなく情報システム一般の話ではないでしょうか． よって，一般的な情報システムとの差分・位置づけを明確化し，IoT特有の性質に由来するセキュリティ対策・ガイドラインとなることを期待します． 情報システム一般と峻別するために，対象とするIoT機器を，少なくともPCやスマートフォンといった従来型情報機器では無いモノとして分かり易く定義を行う必要があるのではないでしょうか．	御指摘の情報システムとIoT機器等との差分・位置付けについては、IoTがクラウド等、情報システムと連携して活用されることが多いことから、IoT機器等と一体となった運用が想定されるシステムも含めて記載しております。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
21	一般社団法人情報処理学会	-			2点目として，本ガイドラインは全てのデバイスが直接インターネットに接続されることを想定しているような印象を受けます． そのため，各機器に要求しているソフトウェアの機能がかなり高機能になっている印象があります． 今後の検討事項にも「リスク分析に基づく分野別の対策について」の検討は記されていますが，p.29～30「要点8.個々でも全体でも守れる設計をする」において，「対策が不十分なIoT機器・システムを上位のIoT機器・システムで守る対策」として，低機能な機器の構成への検討が述べられているように，上位と下位に分けそれぞれの観点でセキュリティ対策のガイドラインを提示した方が，より明確になるのではないかと思います． さらに下位の形態を特に検討し，「下位のIoT機器で最低限守られるべき項目はどれか」という対応分けが必要に思います． その理由は以下のとおりです． ・IoT機器は数が多くなる分，個々のデバイスに対するコスト抑制圧力が強いため十分な機能を有するほどのスペック面での余裕がない． ・セキュリティ面の脆弱性は常に内在していると考えるべきで，それに対する対応（ソフトウェアの更新）は，「デバイス自体の機能の有無」「更新ソフトウェア提供の継続性」「デバイス数の規模による作業の困難さ」を考慮すると，容易ではないと推察される． ・暗号等のセキュリティ技術でよく見られるように，ある段階の保護技術は数年経過すると十分な強度を持たなくなる．	IoT機器は低機能から高機能のものまで種々あり、また接続形態は千差万別であるので、本ガイドラインでは、要点8で「個々でも全体でも守れる設計をする」ことを挙げています。詳細化した要件は、分野ごとに異なるので、今後の検討事項として考えております。
22	一般社団法人情報処理学会	-			3点目として，これまで「事故前提（セキュリティに絶対はなく事故は起こりうるものという前提）」の考え方に基づく取り組みが必要不可欠と言われていました． IoTにおいても同様に，複数の機器が攻撃の踏み台になったり，改ざんされたデータが送付されたりする脅威が存在していると考えられます． 事故前提の考え方はとても重要であり，IoTセキュリティにおいても踏襲されることが必要不可欠であると考えます． 本ガイドラインにおいても，明示的に謳うことを期待いたします．	御指摘を踏まえ、第2章を修正いたしました。
23	一般社団法人情報処理学会	-			4点目として，人とモノ，モノ同士がつながることによって発生しうるセキュリティの脅威に対しては，提供者と利用者の双方で対策を実施することが重要と考えます． 本ガイドラインにおいては，双方とも対象読者として書かれていますが，第3者からのセキュリティ脅威を，IoTセキュリティ機器・システム・サービス提供者がどのように対策をするかという視点にもっとも重点が置かれている（第2章）ように思われ，もっとも重要な利用者の安全とセキュリティを守るという本来の目的からすると，以下の視点が弱いと感じます． ・IoTセキュリティ機器・システム・サービス提供者による，利用者の安全，セキュリティ侵害への対策 ・利用者自身による安全，セキュリティ対策 ・利用者自身によるサービス提供者への攻撃の防止（注意喚起）…（当たり前ですが…）	御指摘の利用者自身におけるセキュリティ対策については、第３章に一般利用者のためのルールとして記載しており、趣旨は含まれているものと考えます。
24	一般社団法人情報処理学会	-			最後に，本ガイドラインで示すセキュリティ対策をどのように実現するのかについては，分野，製品，企業によって適切な対策が異なるため，現案では対策例としていくつかの方法が示されているにとどまっていますが，実社会における実効性のあるガイドラインとするためには，今後も継続して議論されるべきであり，また必要に応じて適切にメインテナンスされることが望ましいと考えます．	御指摘の今後の課題や本ガイドラインの更新については４章記載のとおり、今後必要に応じて行っていくこととしており、趣旨は含まれていると考えます。
25	一般社団法人情報処理学会	-	その他		その他，IoT特有のセキュリティ問題として，本ガイドラインに追加した方が望ましいと思われる項目を，下記に示します． ■長期間利用される機材について 10年間，あるいはそれ以上利用される耐久消費財・設備機器などにおいては，ベンダが存在しなくなった／サポートをとりやめた後どうするかというポリシーを事前に定めておくべきではないでしょうか．	要点１８において「サポート期間未通知、サポート期間を過ぎた継続利用」について記載しておりますが、御指摘の点にあたっては、今後の取組の検討にあたっての参考とさせていただきます。
26	一般社団法人情報処理学会	-	その他		■IoT機器の所有者によるアクセス認可 本ガイドラインにおいて認証に関する記述はありますが，IoT機器への（アクセス権限）所有者によるアクセス認可に関する記述が見当たりません． セキュリティやプライバシーの観点から，ユーザが明示的に許諾したアクセスしか許可されないように対策することは極めて重要だと考えます． 特にコンシューマ向けのIoT機器は，所有者が明確に定まるケースが多いと考えられます．IoT機器は，システム・サービスへの接続時に，所有者との紐付けが確実に行われ（所有者の許諾のもとに，ネットワーク接続が開始され），サービス，他機器，アプリから当該IoT機器へのアクセスは，紐付けられた所有者による明示的な認可を前提として行われるようにデザインされるべきです． これは，UI等を持たない非力なIoT機器においても同様に対策されるべきだと考えます． （IETF OAuthWG, ACE WG等で検討が進んでおり，対策は現実的なものとなってきています） 追加箇所としてのご提案： - 2.2【分析】IoT機器に対する，所有者が認可していないアクセス（未認可アクセス）もセキュリティリスクとして加える． - 2.3【設計】他機器，システム・サービス，User Agent（アプリやWebブラウザ）からの直接アクセス，システム上での当該機器のデータ利用について，所有者の明示的な認可を経るように設計する． - 2.4【構築・接続】IoT機器のネットワークへの接続時に，所有者との紐付けが行われ，所有者の認可の元に接続が行われるように設計する等．	御指摘のアクセス権限に関しては、要点8の対策例の①の「外部インターフェース経由のリスクへの対策」で「利用者認証などの対策」として、例示的に記載しています。
27	一般社団法人情報処理学会	-	その他		■IoT機器のライフサイクル，特にサービス終了時の考慮 IoT機器には，ネットワーク接続（システム・サービスとの連携）が前提となっているものがあり，主要機能がネットワーク接続を前提にする点は，IoT機器特有のものといえます．本ガイドラインには，「サポート終了」については言及がありますが，PCやソフトウェアと同様のニュアンスで記述されているような印象を受けます．例えば，サービス停止によるIoT機器の主要機能の停止，それに伴うセキュリティリスクにフォーカスした記述を追加すると良いのではないでしょうか．以下，参考情報として最近の事例を挙げます． ・スマホで開ける南京錠「246Padlock」，サービス終了で開錠不能に． http://japanese.engadget.com/2016/04/27/246padlock-6-30/ 追加箇所としてのご提案： - 2.1【方針】：経営者は，サービス終了＝主要機能停止なIoT機器について，特に，サービス終了時の対応・セキュリティリスク洗い出し・対策について企画段階から考慮する等 - 2.2【分析】サービス終了＆機能停止時のリスク分析 - 2.3【設計】サービス終了時のセキュリティ対策設計	御指摘のサービスが終了した場合の機能に対する影響は、業種や用途に応じて異なることから、各分野において今後検討が必要な事項と考えています。
28	一般社団法人情報処理学会	-	その他		■既存法との整合性と今後の発展 既存の機器やシステムは，ネットワークに接続するしないにかかわらず，安全安心が担保できるような法整備や規制が行われてきました． p.19にあるエアコンを例にとれば電気用品安全法がそれにあたります． すでに整備されている法や規制と整合性をとりながら，産業界による積極的な開発等の取組を促すとともに，利用者が安心してIoT 機器やシステム，サービスを利用できる環境を生み出すことにつなげる必要があると考えます．	御指摘の既存法との関係については、第２章の冒頭や要点10に記載のとおり、既存の法令等を踏まえた上でセキュリティ対策を検討することが重要であり、趣旨は含まれているものと考えます。
29	一般社団法人情報処理学会	-	その他		■既存のIPA，官公庁（経産省・総務省等）によるセキュリティガイドラインとの差分や関係性の明確化 本案のp.9には，IoTの分野として，自動車，家電（HEMS），医療，工場が挙げられていますが，各分野では既にセキュリティガイドラインが策定されている，あるいは，策定に向けた取り組みが行われています． よって，既存のガイドラインも参照可能とすることで，より有益なガイドラインになるのではないでしょうか． また，本ガイドラインのp.58において，「分野それぞれにおいて求められるセキュリティのレベルは自ずと異なってくる」と記載があるため，本ガイドラインの読者がセキュリティ対策を検討するためにも分野別のガイドラインの情報を掲載した方が良いと考えます． 以下に既存のガイドラインの例を示します． (1) 医療関係 経産・総務・厚労3省から複数のガイドラインが発行されている．例えば，「医療情報システムの安全管理に関するガイドライン」，「医療情報を受託管理する情報処理事業者向けガイドライン」などがある． (2) 自動車関係 IPAが「自動車の情報セキュリティへの取組みガイド」を発行している． (3) HEMS関係 スマートメーターの運用ガイドラインがある．また，セキュリティ・ガイドラインも検討中である（スマートメーター制度検討会 セキュリティ検討ワーキンググループ 報告書）． (4) その他 工場関係では，IPAが「制御システム利用者のための脆弱性対応ガイド」を発行している．	各分野別のガイドラインについては、個々に、また逐次に検討が進められていることから、本ガイドラインは分野を特定せず包括的内容を扱ったものです。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
30	個人D	－	その他		業種と問わずIoTの関係者がセキュリティ確保のための基本的な項目を示し、相互の認識の共有を促すためにIoTセキュリティガイドラインを作成することは意義あることである。 一方、行政の責任はガイドラインを出すに留まることではない。 例えば、米国は携帯端末のソフトウェアアップデートの義務化を打ち出しているが、そのような強制的な施策を実施するのは、そうしなければ一定のセキュリティを担保できないからである。 本IoTセキュリティガイドラインだけでは、担保されない部分に対する施策についても検討を進めるべきである。 IoT機器の周りに迷惑をかけないような対策についても記述すべきである。 例えば、動いているか、止まっているのか、外部から見て分かるようにする。 変な電波や音を出さない。故障／停止を音や光で知らせる等。	御指摘のIoT機器の周りに迷惑をかけないような対策については、要点9において趣旨が含まれていると考えます。
31	個人D	－	その他		ON/OFFの手順を共通化する等の利用シーンを想定した対策についても記述すべきである。 例えば、海外の製品は、0/1の表記が分かりにくい場合の利用者への説明。ON時やOFF時に、特別な手順が必要なのはよくないこと。 電源ブチでも壊れないようにすること。 緊急停止ボタンを付けておくこと等である。	御指摘のON/OFF手順の共通化は、利用する機器・システムにおいて必要性や検討すべき項目が異なることから、分野や機器に応じて個別に検討されるものと考えます。
32	個人D	－	その他		プロトコルの上位互換を考慮して設計開発すべきであることを記載すべきである。 例えば、後で拡張しようとして困らないようにする。 プロトコルのバージョンが分かるようにする等である。	御指摘のプロトコルの上位互換については利用するプロトコル、機器の目的等で異なることから、各分野において今後検討が必要な事項と考えています。
33	NPO日本ネットワークセキュリティ協会	－	その他		2その他全般 意見：IoTでの「トラスト（信頼関係）」および「リスク（被害想定）」という検討が必要である。 理由：複数のサービス、マルチベンダー機器が繋がる際に、繋いで良いか悪いかは 「セキュリティ視点」だけでは決まらず、「トラストの視点」が必要と思われる。 技術的には「認可（OAuth、OpenID Connectなど）」によって接続されるが、認可の判断となるのは提供されるサービス連携が「可能かどうか」という以外に、「法的側面（特に海外など）」、「セキュリティ性」、「個人情報の利用目的」、「管理体制」、「許可した場合のインセンティブ」、「情報提供によるリスク（被害想定）」などが考えられる。 少なくともユースケース別のB2Cユーザーにとって「リスク（被害想定）」に対するガイドが必要であり、さらに言えば「トラスト（信頼関係）」に繋がる指標のようなものが検討されるべきではないかと考える。	御指摘の「トラスト」及び「リスク」の検討については、要点11対策例に記載しているとおり、接続相手の素性に応じて提供機能や情報の範囲を考えることが重要だと考えています。技術的な実現方法については、各分野において個別に検討されるものと考えています。
34	KDDI株式会社	－			IoTは、今後、重要な社会基盤となり、広範囲に適用されていくと考えられます。 ここで、日々、高度化、多様化されるサイバー攻撃は、IoTにおいても喫緊の課題と考えており、IoTサービスを普及促進していくうえで、利用者、メーカ、サービス事業者、経営者に至るまで幅広い関係者を対象とするセキュリティガイドラインとして、課題解決の指針を整理された点について、賛同いたします。 今後、ユースケース毎の要件整理、各プレーヤの責任分界点の明確化、パーソナル情報の扱い、IoTシステム全体のフェールセーフ対応、総合的なセキュリティ対策等について、引き続き検討され、広く活用されるガイドラインとなることを期待します。 また、IoTにおけるセキュリティは、グローバルな課題であり、oneM2Mでセキュリティやプライバシー保護機能が、GSMAなどの国際的な業界団体でセキュリティガイドラインの検討が進んでおります。 国際的な活動との整合性、連携も視野に入れて検討が進められることを期待します。 一方、ガイドラインが規制となり、オープンイノベーションやグローバル展開に対する阻害要因とならないよう、事業者の過度の負担にならないバランスの取れた施策として取り組まれることを期待します。 例えば、IoT機器に対して、設計時の安全性検証（指針3）や、リリース後の安全性の確保について（指針5）が示されていますが、安価なIoT機器に対する評価・検証や、ライフサイクルが10年以上も想定されるIoT機器のソフトウェアアップデートは、技術的・コスト的な課題があり、その対応については、個々のユースケースに基づいて最適な指針を検討することが望ましいと考えます。	本ガイドラインに対する賛同意見として承ります。 また御指摘については、リスク分析に基づく分野別の対策として、各分野において検討がなされる事項として考えています。
35	個人C	－			ただ、施策面で言うのであれば、機器初期設定については経産省と協議の上で、メーカー側にも協力を求めていくのが望ましいと考える（例えば、標準設定では通信について閉鎖的・防御的なポリシーとしておく等。 現状の様に、ネットワーク関連機器について、デフォルトで全ポート開放、というのは問題であると考える。デフォルトではコントロール用端末との通信に用いるポート以外は「DENY」の設定で簡単にポート開放可能としておくのが望ましいと考える。）。 また、回線業者やISPに対しても、更なるセキュリティの確保を行わせるようにしていくのが望ましいと考える（認証の強化、DNSSECの積極導入、利用者−ISP間の通信経路暗号化機能の標準的提供要請（IPv6促進はこれを支援する。）等。 また、ISPに接続した利用者の通信について、その全てのものにSPI（ステートフルパケットフィルタ）のオプションを標準では自動で適用するように求めていく事も望ましいと考える。 これは非常に協力にセキュリティ問題の対策を打つ事が可能なはずである（外部からの攻撃をほぼ完全に防げるようになるので。）。 この機能を接続時に自動適用する設定をISPの利用者に標準で提供するとともに、その有効無効切り替えボタン等を設けると、日本におけるセキュリティ問題の相当多くが一気に片付くのではないだろうか。 仕組み的にはLinuxで言うiptables相当の機能によってユーザー単位で自動的にSPIを適用させるだけで簡単に構築出来るものなので、実のところ一昼夜程度で実装の行えるものなので、各ISPに導入を促していただきたい。）。	御指摘の各ISPへの技術的対策の適用については、ネットワークの提供形態や契約条件等、有効性や実現性が異なるため、用途に応じて個別に検討されるものと考えています。
36	一般社団法人情報処理学会	1			＜その他＞ その他，細かい内容ではございますが，文言の統一など気になった点を下記に示します． ・ p.1 「本ガイドラインは，IoT 機器やシステム，サービスの供給者及び利用者を対象として，サイバー攻撃などによる新たなリスクが，モノの安全や，」 →モノの安全性について，説明が必要だと考えます．物理的な価値の損失のみを指しているのでしょうか．おそらく，ガイドラインの主旨としては，“モノの利用者”の安全も含まれるのではないかと想像します．	御意見を踏まえ、該当箇所を修正いたしました。
37	一般社団法人情報処理学会	3			・ p.3 IoT の関係者=1.4対象読者という解釈で正しいでしょうか．	御指摘のとおり、P3 IoTの関係者は1.4 対象読者を想定しております。
38	ネットエージェント株式会社	4	1.1.1 IoT の動向と近年の脅威事例		□ 4ページ　1.1.1 IoT の動向と近年の脅威事例 ・ 非コネクテッドカーの事例が、コネクテッドカーの事例に入っている。 例示されているのは、有線のCANバスでの制御の事例です。コネクテッドの部分からの侵入ではありません。コネクテッドカーの事例ならクライスラーのジープ チェロキー（Blackhat 2015）の事例と差し替えてください。	御意見を踏まえ、該当箇所を修正いたしました。
39	一般社団法人情報処理学会	4	第1章	1.1.1 IoTの動向と近年の脅威事例	以下，各章の内容について個別にコメントいたします． ＜第1章＞ ■1.1.1「セキュリティの脅威の範囲の拡充」 IoT機器に対するセキュリティの脅威（セキュリティを侵害する／脅かす要因）として，「第3者による攻撃」のみが触れられていますが，利用者が意図せずモノを繋げてしまっていることや，サービス提供者が利用者の情報を適切に管理してないことによる脅威も存在すると思われます． これらの脅威は，第3者による攻撃の脅威よりも，場合によっては，利用者の生命・財産に，比較的容易に，深刻な結果をもたらすことが想定されます． 例：サービス提供者が利用者に事前通知なく，遠隔制御機能を提供している． サービス提供者が，利用者の個人情報を企業のサーバに保存しており，適切に管理されていない．	御指摘の利用者やサービス提供者による意図しない接続による脅威については1.1.2にIoT特有の性質として、また要点9 つながる相手に迷惑をかけない設計をするという観点で記載しており、御指摘の趣旨は含まれているものと考えます。
40	一般社団法人情報処理学会	4	第1章	1.1.2 IoT特有の性質とセキュリティ対策の必要性	■1.1.2「IoT 特有の性質」における利用者視点の追加 性質1と性質6において，利用者の視点が抜けていると思われます． 開発者だけでなく，利用者にとっても，所有する機器の接続範囲，影響度（繋ぐことのリスク）を想定・把握することが困難になるという性質があろうかと思います． サービス提供者／開発者よりも，ITスキルの乏しい利用者（未成年者や高齢者など）にとって，この性質は大きな影響を及ぼすものと思われます． 例えば，第2章の要点18，要点19に繋がるので，p.4でも触れた方が良いと思われます． また，要点19で，利用者にリスクを認識してもらう上でも，十分な情報提供と説明が必要であることを明記した方が良いと思います．	一般利用者については第3章で記載しており、御指摘については今後の検討における参考として承ります。

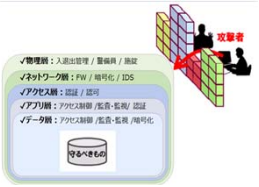
No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
41	一般社団法人電子情報技術産業協会（JEITA）	4	1.1.1	表1	ここに記載する事例は、単に引用するのではなく、事実関係の確認、更に社会への影響を踏まえて選定、利用頂く必要があると思う。 IoTの脅威事例として「ペースメーカと不正な通信を行うことによって、830ボルトの電圧を発生させることが可能」と紹介されているが、ペースメーカはIoTであるか。 また、ペースメーカ等は通常植込部位（体表）に強力なマグネットをあてることで通信モードになるため、仮にその通信内容を傍受・解析して悪用したとしても（遠隔からの）攻撃対象となる可能性は低いのではないか。 文面からペースメーカではなく植込式心除細動器と想像される。 重大性で危機を煽る意味で引用されたと思うが、事実関係などに加え、患者等への心理的影響を踏まえて引用や表現を行うべきではないか。（植込式心除細動器適応患者とペースメーカ適応患者の比率は後者が格段に多く、不要な心配を与えることになる。） また、要点7で過去のインシデントと対策を紹介しているが、ここで例示するなら、要点7に対策例を書くべきではないか。 同様にコネクテッドカー、サブシステムの事例もCANへアクセスするためには自動車を分解し、奥底にあるHUBに通信アダプタを接続しなくてはならないと聞いている。これも今回適切な事例であるか。	本ガイドラインに記載した事例は、IoTに関する脅威イメージを例示したものです。御指摘を踏まえ一部修正させていただくとともに、今後の検討における参考とさせていただきます。
42	法人・団体（匿名）A	4-5	第1章1.1.2	【IoT特有の性質】	IoTデバイスがネットワーク経由ではなく直接物理的な接触を受けて攻撃される可能性や偽物にすり替えられる可能性があるという性質を持つ旨、追記が必要と考えます。	御指摘の物理的な接触による攻撃の可能性は、IoTの性質3の監視が行き届きにくいという点に起因し、要点6の物理的リスクの想定として記載しており、御指摘の趣旨は含まれているものと考えます。
43	法人・団体（匿名）A	4-11	第1章	全体	本ガイドラインの対象読者として経営者やサービス提供者を想定するのであれば、本ガイドラインを参照する（採用する）メリットに関する記載があると、より経営者やサービス提供者にとって有用であると考えます。	今後の検討における参考として承ります。
44	法人・団体（匿名）A	4-11	第1章	全体	上記と同様、2章以降をまとめたエグゼクティブサマリーがあると有用であると考えます。	ガイドラインとともにガイドラインの概要を公開しておりますのでご覧下さい。
45	インテル株式会社	5	1.1.2 IoT特有の性質とセキュリティ対策の必要性	性質2	特に1.1.2「IoT特有の性質」に示されている性質2，3および5は、下記の理由から、政府および産業界が共有すべき課題として明確にしていることが非常に有効で重要と考えます。 （性質2）について：設計から廃棄までのすべてのフェーズでのセキュリティ対策を施す事が大変重要で、製造側と利用側が歩み寄りながら最適な解を見つけていく事が現在の課題であると認識します。	本ガイドラインに対する賛同意見として承ります。
46	インテル株式会社	5	1.1.2 IoT特有の性質とセキュリティ対策の必要性	性質3および性質5	（性質3）および（性質5）について：今後の技術開発により改善が期待される分野であり、現在利用されている制御システムや機構の要求条件をそのまま当てはめるのではなく、（性質2）同様に新たな視点での検討、開発によって解決が可能な課題であると考えます。 これらIoT特有の性質を踏まえ、新たな視点に立って、技術の応用につき広く対話の場を設けていくことが非常に重要であると考えます。	本ガイドラインに対する賛同意見として承ります。
47	個人E	5	1.1.2	性質2	「セキュリティ対策が不十分なまま」ではなく、「セキュリティ対策が不十分になった機器が」の方が良い。	御意見を踏まえ、該当箇所を修正いたしました。
48	個人E	5	1.1.2	性質3	「管理されていないモノが勝手にネットワークにつながり」の他に、「IoT機器が盗まれたり、盗まれた機器が別のネットワークにつながり」という場合がある。	御指摘の盗まれるといった点については、性質3に起因し監視が行き届きにくいという特徴を踏まえ要点6に記載しており、御指摘の趣旨は含まれていると考えます。
49	ネットエージェント株式会社	5	1.1.2 IoT 特有の性質とセキュリティ対策の必要性		□ 5ページ 1.1.2 IoT 特有の性質とセキュリティ対策の必要性 ・ 可用性に関する特性を入れてください IoTデバイスでクラウド連携が必須となっているものはサービスの終了とともに使用できなくなる可用性に問題があることがあります。これは通常の製品寿命より短くなるため、一般購入者も含め認識しておく必要があります。	御指摘のサービスが終了した場合の機能に対する影響は、業種や用途に応じて異なることから、各分野において今後検討が必要な事項と考えています。
50	ネットエージェント株式会社	5	1.1.2 IoT 特有の性質とセキュリティ対策の必要性		□ 5ページ 1.1.2 IoT 特有の性質とセキュリティ対策の必要性 ・プライバシーが侵害される特性を入れてください スマートメーターやHEMSコントローラ、体重計、婦人用体温計、活動量計など、クラウド利用が前提のものが多くあります。これらの機器で取得したプライバシーをサービス提供者や第三者に提供することを同意しないと使えない、重要な項目を個人情報として扱わないなど利用者のプライバシーを十分保護しない製品が多くあります。	御指摘のIoT機器が取得するデータについては、第4章に記載のIoT時代のデータ管理の在り方として、各分野において今後検討が必要な事項と考えています。
51	一般社団法人情報処理学会	5、8			・p.5,8「安全」が"誰の／何の"安全なのか，対象が曖昧に記述されているので，関係者のうち，誰の／何の安全性を指しているのか明記すべきと考えます．対象が曖昧ですと，対策を検討する上でも曖昧な議論になりがちです．	御指摘の安全が何を指すかは、製品単体として捉えるか、システムとして捉えるかなどによって重要性や対策が異なるため、各分野において個別に検討されるものと考えています。
52	一般社団法人電子情報技術産業協会（JEITA）	5	1.1.2	（性質5）	「リソースが限られた」はIoT機器の特性としては重要である。その中でセキュリティ対策として「暗号等」とならんで「コンピュータウイルス対策」もあると思われるので、追加をご検討願いたい。	御指摘のコンピュータウィルス対策は、一般的にセキュリティ対策に含まれていると考えられることや、要点7対策例に記載していることから、御指摘の趣旨は含まれていると考えます。
53	個人E	6	1.2	ガイドラインの目的	「なお、本ガイドラインの目的は」ではなく、「なお、本ガイドラインが対象とする範囲は」の方が良い。	1．2では本ガイドラインの目的を記載していることから、このように記載しております。
54	個人B	6	1.2 ガイドラインの目的		～以下、文書内における具体的な指摘～ <本ガイドラインの目的と対象> ・一般利用者も注意すべき点についての記載が少ないと考えます。一般利用者対象の部分は、専門的な用語を使うことなく、具体例などを使った上でわかりやすく記載する必要があると考えます。 <該当部分> p6:「加えて、本ガイドラインでは、数多くの IoT 機器やシステム、サービスが、既に国民の日常生活に浸透していることから、一般利用者が注意すべき点についても記載する。」	今後の検討における参考として承ります。
55	個人D	6	1.2		「本ガイドラインは、その対象者に対し、一律に具体的なセキュリティ対策の実施を求めるもの ではなく、その対象者において、守るべきものやリスクの大きさ等を踏まえ、役割・立場に応じて適切なセキュリティ対策の検討が行われることを期待するものである。」に関して 一律に具体的なセキュリティ対策の実施を求めるものではないため、守るべきものやリスクの大きさ等を踏まえ、適切なセキュリティ対策を検討できるように具体的な事例を示す必要があると思われる。 しかし、「第4章 今後の検討事項」では、「・リスク分析に基づく分野別の対策について」において「具体的なIoTの利用シーンを想定し、詳細なリスク分析を行った上で、その分野の性質、特徴に応じた対策を検討する必要がある。」とあり、セキュリティ対策を検討するための具体的なIoTの利用シーンや詳細なリスク分析を示していない。 そのため「IoTセキュリティガイドライン」というよりは、「IoT機器へ接続する開発にあたっての心構え」という内容であるため、適切なセキュリティ対策を検討できるように具体的な事例を追加した後に、本ガイドラインを発行すべきではないか。	御指摘の具体的な利用シーンやリスク分析はその分野の性質、特徴などに応じて行われるべきものであるため、各分野において今後検討が必要な事項と考えています。
56	個人D	6	1.2		「本ガイドラインの目的は、サイバー攻撃などによる被害発生時におけるIoT機器やシステム、サービスの関係者間の法的責任の所在を一律に明らかにすることではなく、むしろ関係者が取り組むべきIoTのセキュリティ対策の認識を促すとともに、その認識のもと、関係者間の相互の情報共有を促すための材料を提供することである。」に関して 複数の関係者が相互に連携し、利用者にサービス提供する場合には、法的責任を明確にする必要もあり、関係者間の法的責任の所在を一律に明らかにしなくとも、法的責任の参考となる既存の法令や判例及び事例は示す必要がある。 そのため、法的責任の参考となる既存の法令や判例及び事例を追加した後に、本ガイドラインを発行すべきではないか。	御指摘の法的責任については、第4章に記載の法的責任関係として、各分野において今後検討が必要な事項と考えています。
57	法人・団体（匿名）B	－	－	全体	IoT機器・システムの利用発展を支えるセキュリティ対策の必要性から本ガイドラインの策定は重要であると考えます。 つきましては、本ガイドライン発行にあたり、今後も多様化するIoT機器・システムへの適用を踏まえ、趣旨をより明確に記載していただいたほうがよいかと考えます。 次の内容をご考慮いただけますようお願いいたします。	今後の検討における参考として承ります。また、御指摘の機能・性能レベルの異なるIoT機器やシステム全体でのセキュリティ確保という点は重要ですが、IoTの特徴は機能・性能レベルのみではないため、限定せず記載しており、御指摘の趣旨は含まれるものと考えます。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
58	法人・団体（匿名）B	6	1.2節	第3段落	「このため、本ガイドラインは、その対象者に対し、一律に具体的なセキュリティ対策の実施を求めるものではなく、その対象者において、守るべきものやリスクの大きさ等を踏まえ、役割・立場に応じて適切なセキュリティ対策の検討が行われることを期待するものである。」に関して、 以下のように変更することを提案します： 「本ガイドラインは、機能・性能レベルの異なるIoT機器が混在する環境を前提とすることから、IoT システム・サービス全体でのセキュリティ確保に向けて、一律に具体的なセキュリティ対策の実施を求めるものではなく、その対象者において、守るべきものやリスクの大きさ等を踏まえ、役割・立場に応じて適切なセキュリティ対策の検討が行われることを期待するものである。」 （修正理由）主に本ガイドラインの要点14 に記載されている、機能・性能レベルの異なるIoT機器が混在する環境を前提としてIoTシステム・サービス全体でセキュリティを確保する、という考え方は非常に重要だと考えます。本ガイドラインの趣旨をより明確にするために、上記のように変更することを提案いたします。	
59	個人E	7	1.3.1	図1	1.～5.の説明が何を示しているのか解りにくい。IoTの特色なのか、SoSの特色なのか、それとも両者の特色なのかがわかりにくい。	御指摘を踏まえ、修正いたしました。
60	個人D	7	1.3.1	ITU（国際電気通信連合）の勧告（ITU-T Y.2060）では	ITU-T Y.2060は、ITU-T Y.4000である（2016年2月5日に再番号されている）。	御意見を踏まえ、該当箇所を修正いたしました。
61	個人E	8	1.4	対象読者	対象読者を文章で書いているため、文の区切りが曖昧で、誰が対象なのか解りにくい。対象読者は下記のように箇条書きにした方がわかりやすい。 ・XXの供給者である経営者 ・XXの利用者である企業利用者 ・XX	御意見を踏まえ、該当箇所を修正いたしました。
62	次世代ICカードシステム研究会	8	1.4 対象読者	P8図 2 対象読者のイメージ P9表 1 対象読者の例	P8では、システム提供者とサービス提供者がわけて定義されておりますが、P9の表では一体化されており、区分が不明確です。 ガイドラインであるため、対象者を明確にすべきと考えます。	御指摘のシステム提供者とサービス提供者については、図2は関係者がイメージし易いよう、IoTサービスの構成例として記載しております。IoTでは、あるサービスやシステムを利用して、別のサービスやシステムとして提供されることがあり、システム提供者でありながら自身がサービス提供者や企業利用者でもある場合も想定されるため、一括して記載しております。
63	個人D	8	1.4	図2の説明文章	図2は、サービス、プラットフォーム、ネットワーク、機器という4つのレイヤがあり、サービス提供者、システム提供者、機器メーカ等の関係者と各々の経営者を示している重要な図であるが、説明文章が短く正確に理解できない。 そのため、この図2を例示している表1、対象読者を示した表2も理解できない。 図2、表1、表2の説明文を追加すべきである。	今後の検討における参考とさせていただきます。
64	株式会社パソナサイバーラボ	9	表 1 対象読者の例		P.9 「表1 対象読者の例」に「防犯サービス」の記載も入れたほうがよい。過去に監視カメラなどがサイバー攻撃の踏み台になった事例がマスコミに取り上げられたことがあり、世間の関心が高まったことがあったので、この事例の箇所で例示したほうがよいと思われる。	表1では、参考事例として一部の事例のみ記載しております。
65	個人E	9	1.4	表1	分野にNISCが定義する重要インフラを付け加えた方が良い。具体的には金融・クレジット(ATM)、電気・ガス・水道等のインフラ(スマートメーター)、物流(POS)など。	御指摘の表1は、対象読者の分類イメージがつきやすいよう例示を記載したものであり、本ガイドラインの対象を限定するものではありません。
66	個人D	9	1.4	表1	例示されている分野やサービスが、比較的高いセキュリティを求められる分野やサービスであり、農業センサーなどの低リソースの事例がなく偏っている。 そのため、本ガイドライン全体がIoTの中でも高いセキュリティを扱ったかのような印象を与えるため、低リソースなIoT機器についても解説すべきである。	御指摘の低リソースの機器については、要点14の対策例に記載しているとおり、機器の機能・性能を考慮し、システム・サービス全体でセキュリティを確保すること記載しており、御指摘の趣旨は含まれていると考えます。
67	一般社団法人電子情報技術産業協会（JEITA）	9	1.4	表1	分野：医療において、利用者として「患者」を「患者及びその家族」とした方が現実的と思う。	御意見を踏まえ、該当箇所を修正いたしました。
68	法人・団体（匿名）A	9	第1章1.4	表1	金融業界におけるIoTにはセキュリティが必須との認識が既に広まっていること、また本書の後半に金融の事例が登場することなどから、「金融」の例も追加するのが良いと考えます。	御指摘の表1は、対象読者の分類イメージがつきやすいよう例示を記載したものであり、本ガイドラインの対象を限定するものではありません。
69	個人E	10	1.5	全体構成	本書が全部で4章構成であることを最初に記載する。	本書の構成については目次および表2に記載しているため、御指摘の内容は含まれていると考えます。
70	一般社団法人テレコムサービス協会	11	1.5節	表2 機器メーカ 要点16	要点16.「認証機能を導入する」は、システム・サービス提供者/企業利用者のみが対象読者になっており、機器メーカは対象者になっていません。 しかし、認証機能は、機器に実装されていなければ利用できないため、機器メーカも主な読者とするのが良いと考えます。	御意見を踏まえ、該当箇所を修正いたしました。
71	一般社団法人情報通信ネットワーク産業協会（CIAJ）	11	1.5節 ガイドラインの全体構成	表 2	対象読者の表現について p9の表1「対象読者の例」には、“企業利用者”の意味が脚注にて説明されていますが、表2では、“供給者（一部企業利用者）”という表現で、この“一部企業利用者”の意味が不明瞭になっています。 従いまして、“一部企業利用者”の条件は、やはり、表2にも注記として付記しておくことが妥当と考えます。	御意見を踏まえ、該当箇所を修正いたしました。
72	個人D	11	1.5	表2	経営者が一括りになっているが、CISO（Chief Information Security Officer）やCTO（Chief Technology Officer）によっては読む箇所が異なるのではないか。	御指摘の経営者の役職による読む箇所については、本書はセキュリティ確保の観点から求められる基本的な取組を記載しており、役職によらず読んでいただくことを期待します。
73	一般社団法人電子情報技術産業協会（JEITA）	11	1.5	表2	要点14～16は「機器メーカ」にとっても重要な視点と考えられる。主な読者として追加が妥当と思われる。	表2は主な読者として記載しており、要点14～16においても機器メーカを排除するものではありませんが、御意見を踏まえ、特に関係のある要点16をを追加致しました。
74	株式会社 ベリサーブ	12	表3	分析	「要点8. リスクの特性・重大性を認識する」を追加する。これに伴い、要点8以降の番号を修正する。	御指摘の点については、要点3～6において考慮しています。
75	株式会社 ベリサーブ	12	表3	構築・接続	「要点17. 感染を検知したら拡大を遮断する機能を設ける」を追加する。これに伴い要点17以降の番号を修正する。	御指摘の点については、要点9において考慮しています。
76	ネットエージェント株式会社	12～55	第2章 IoT セキュリティ対策の 5 つの指針		□ 12～55ページ IoT セキュリティ対策の 5 つの指針 設計 構築・接続について IoT特有の対策にメーカー視点がない CPUやメモリなどのリソース制限や、接続用容易性を確保しながらの認証法など、IoTにおけるセキュリティの胆の部分が一切説明されていない。 IoTのセキュリティが重要になるのは、今までセキュリティが必要でなかった分野の製品がインターネットに接続されることで発生する。 セキュリティ設計としては一般的な方法ができないことも多く、他の方法で実施する必要がある。	御指摘のセキュリティの確保に対する対策や考え方は、要点8、14、16等で記載しており、御指摘の趣旨は含まれていると考えます。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
77	日本シノプシス合同会社	12～55	第2章 IoT セキュリティ対策の 5 つの指針		a.　P-12 to P-55 第2章 IoTに関するセキュリティの具体的な取組みの指針が欠如している状況において、本ガイドラインはセキュリティに対する取組みの指針を与えるものとして非常に有益と評価しております。 しかし、機器メーカーやシステム提供者としての指針が多く、「要点10 (3) 対策例(P.34)」に発注元、外注先などのセキュリティ設計品質の説明・合意に関して触れられていますが、発注元としての具体的な対策案には欠けます。 実際は、機器メーカーやシステム提供者、サービス利用者の全てが発注元となることも一般的であると考えられ、「要点18 ③ (P-48 to P-50)」に記載されているように提供者の視点からの対策のみならず、発注元としての視点からの対策も記されるべきです。 添付資料は外部からソフトウェア、デバイス等を調達する際に必要なセキュリティ要件をまとめたものですが、こうした調達サイドからの視点で明文化された対策の記載が必要と考えます。	御指摘の発注元としての対策は、発注する機器やシステムによって異なり、要点18、20に記載のとおり、関係者間で役割の認識を合わせ、検討することが重要であり、今後個別に検討されるものと考えます。
78	日本シノプシス合同会社	－			6.　添付資料 「サプライチェーンにおけるサイバー アシュアランスのための調達基準」 FY16 SIG TC WP Procurement Language 1.0_0608-2.pdf	
79	次世代ICカードシステム研究会	12	第2章	IoTセキュリティ対策の5つの指針	指針毎に独立して記載されていますが、実際には、分析→設計→構築・接続→運用保守の順番で関係しています。 そのため、PDCAサイクルを参考に全体の指針の関係を示し、スパイラルアップを図ることを明記すべきと考えます。	今後の取組の検討にあたっての参考にさせていただきます。
80	一般社団法人情報処理学会	12	第2章	全般	＜第2章＞ ■全般 関係者に加え，機器や機能も多く存在するため，システムとしてリスク分析やセキュリティ・バイ・デザインの取り組みが必要と考えます． 【運用・保守】における指針として，『IoTシステム・サービスにおいては，多くの関係者が存在し，かつ，複雑な関係となっている』という記述に同意いたします． この観点を【運用・保守】に限定されることなくさらに踏み込んでいただき，当該文章の「関係者」の部分を「機器」「機能」と置き換えて捉えることが重要と考えます． すなわち，他フェーズ（【方針】【分析】【設計】【構築・接続】）において，（多くの機器や機能が存在し複雑な関係となっている）IoTシステム・サービス全体に対する「リスクの分析」「セキュリティ・バイ・デザイン」などの取り組みが求められるよう明記することを期待します．	御指摘のとおり、リスク分析は、セキュリティバイデザインによる取組は重要であると考えます。ガイドラインにおいても、1．2のガイドラインの目的で「セキュリティバイデザインを基本原則としつつ明確化するものである」と記載しております。
81	個人E	13	2章	表3	「一般利用者向け」は2章の範囲では無いため、削除する。	御指摘を踏まえ、修正いたしました。
82	一般社団法人情報処理学会	14			・ p.14「利用者」→「ユーザ」という表現に変わっています．統一するべきと考えます．	御指摘を踏まえ、修正いたしました。
83	株式会社 ベリサーブ	15	(3)対策例	①	以下の2つを追加する ・経営層にセキュリティ対策担当責任者を置き、定期的にPDCAの実施状況を把握し、フォローする。	御指摘については、要点1の対策例で記載の「サイバーセキュリティ経営ガイドライン」に記載しております。
84	株式会社 ベリサーブ	15	(3)対策例	①	・セキュリティリスクと対策について各組織で話し合い、必要な対策をとりまとめて責任者に報告する。ディペンダビリティ確保を示すセキュリティ・ケース図で、組織に展開するリスクと対策の考え方をわかりやすく示せるようにする。	御指摘については、要点1に体制の整備が必要としています。個々の対策例については代表的な事例を扱っています。
85	インテル株式会社	15	要点1. 経営者がIoTセキュリティにコミットする		以下、本ガイドラインの質を向上させるために、その内容に関していくつかのコメントさせて頂きます。 (1)「要点1. 経営者がIoTセキュリティにコミットする（15ページ）」の表現について 日本語としてより明確にガイドラインの意図を示すために「経営者がIoTセキュリティに関して責任を明確化し、それを行動に移す」などの表現が適切と思います。 「コミット」は日常的に日本語として使われ始めてはいますが、その本来の意味について一般的に共通の理解はなされていない恐れがあります。	今後の取組の検討にあたっての参考にさせていただきます。
86	個人E	15	2.1	(1)ポイント	「必要な体制・人材を整備する」ではなく、「必要な体制・人材を整備し、維持し、適宜見直す」の方が良い。	要点1においてPDCAサイクルを回して体制を見直すことを記載しております。
87	個人E	15	2.1	(1)ポイント	「人材」について、情報セキュリティの専門家(有資格者)が望ましいことを明記する。 例として公認情報セキュリティマネージャー(CISM)やCISSPなど。 国家資格ではなく国際資格とした理由は2点ある。 1.サイバーセキュリティが国内だけの対策では不十分であり、グローバルな視点が求められること 2.古いセキュリティ知識では役に立たず、定期的な知識の更新が必要であること(CISMやCISSPはISO/IEC 17024の認証を受けており、これをクリアしている)	必要な人材については、「サイバーセキュリティ経営ガイドライン」においても、セキュリティ人材の育成や確保について記載されていますが、今後更に検討が必要な事項として考えています。
88	株式会社ラックサイバー・グリッド・ジャパン	15	第2章 2.1 要点1.	「(3)対策例 ①組織としてセキュリティ対策に取り組む」下の囲み	提案1:以下の文言を囲み内の例示前に追記する。 以下のようなCSIRT構築方法を参考に、パートナーやユーザと共にセキュリティ上の問題に取り組むことが出来るCSIRTを構築する。	CSIRTの構築については、要点1の対策例で記載してある「サイバーセキュリティ経営ガイドライン」で記載しております。
89	株式会社ラックサイバー・グリッド・ジャパン	15	第2章 2.1 要点1.	「(3)対策例 ①組織としてセキュリティ対策に取り組む」下の囲み	提案2:CSIRTは自組織内のインシデントに対応する組織であるが、IoTの場合、製品の販売先またはサービスの販売先で生じた当該製品起因のインシデントに対応する組織PSIRT (Product security Incident Response Team)も重要であり、その事例を例示に追記する。 理由:先に掲げられたCSIRT構築の2例はどちらも社内で発生する問題に対応するための組織づくりであり、これだけでは不十分である。 社内だけなら自組織の情報セキュリティガバナンスにより問題のコントロールは可能でも、IoTで連携した先のコントロールまではできない。 お客様までガバナンスでコントロール出来ない分、お客様にも協力していただける仕組みづくりが必要で、その一つとしてProduct Security Incident Response Team(PSIRT)の取り組みがある。 《参考》PSIRTの事例 ・パナソニック株式会社のPanasonic Product Security Incident Response Team(Panasonic PSIRT) https://www.panasonic.com/global/corporate/product-security/sec/psirt/jp.html ・シスコシステムズのPSIRT https://tools.cisco.com/security/center/publicationListing.x ・日本電気株式会社NEC-CSIRT https://www.jpcert.or.jp/magazine/security/fieldww-neccsirt.html	御指摘の取組は重要と考えており、今後の参考とさせていただきます。
90	一般社団法人情報処理学会	15	2.1	要点1. 経営者がIoTセキュリティにコミットする	■2.1【方針】要点1「経営者がIoTセキュリティにコミットする」 運用・保守時に新たに発見，把握したセキュリティの脆弱性に関する情報を，JP-CERT，IPA等に通知すること，また利用者からの問い合わせに対応する窓口の設置を強く推奨するべきだと考えます． 情報の把握に関しては，要点18(3)①で少し言及されていますが，明示すべきであると考えます． また，p.57の利用者のルール1で，サービス提供者から提示される情報を定期的に確認することを追記すると良いと思います． これらのことは，直ちに使用を停止すべき深刻な脆弱性が見つかった場合には，サービス提供者側だけでなく，利用者の行動を促すことが重要と考えるため，追記の検討をお願いします．	今後の検討における参考として承ります。
91	法人・団体（匿名）C	15	第2章 2.1要点1	(3)対策例	部分部分でのセキュリティの考慮はもちろん、IoTシステム全体としてのセキュリティ品質の確保を認識する」というような文言が入ってもよいかなと思います。 どうしてもデバイス部分、サーバ部分と個別で考えがちですが、IoTはデバイスとサーバ側のセットでのサービスとなりますので、経営者としては、IoTシステム全体での考慮が必要かと思います。	要点1の対策例に組織としてIoTシステム・サービスのリスクを認識することを記載しております。経営者がシステム全体を考慮することを含めています。
92	法人・団体（匿名）C	16	第2章 2.1要点2	(2)解説	内部不正等への対処は現在、人的管理策だけではなく不正がやりにくいセキュリテイバイデザイン手法が推奨されている。 日本国においても各種ガイドライン等で推薦されている。 そこで解説の末尾に次の文章を挿入してはいかがでしょうか。 「「サイバーセキュリティ経営ガイドライン」や「『高度標的型攻撃』対策に向けたシステム設計ガイド」では水際対策だけではなく内部対策も必要であることから、すべての階層で防御する多層防御の考え方を推奨している。」	御指摘の点については、セキュリティバイデザインの推奨されている多層防御の考え方については、(6P)セキュリティバイデザインを基本原則としつつ明確化するものと記載しており、内部対策の必要性については、要点2において対策例を記載しております。
93	一般社団法人電子情報技術産業協会（JEITA）	16	2.1	要点2	要点2（内部不正やミスに備える）の「(2)解説」において、自動車の管理サービスの不正操作や、ATMへの不正な接続の例が記載されている。 「(3)対策例」には技術的な対策について書かれていないが、実際には要点8（個々でも全体でも守れる設計をする）などの技術的な対策も必要であるため、他の要点に記載されている対策についても参照させたほうが良い。	要点2では体制面での内部不正やミスの対策のみを記載しております。
94	法人・団体（匿名）A	16	第2章2.1 要点2.	(3)対策例	対策例の記載が現状のままでは不十分と思われ、経営者は少なくとも要点3を参照し、守るべきものを明確にした上で要点2の対策を考える必要があると思います。	リスクを認識した結果、体制の修正につながることも考えられます。対策例の記載の充実については今後の取組の検討にあたっての参考にさせていただきます。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
95	株式会社 ベリサーブ	17	(3)対策例	②	以下の文を追加する ・組織で話し合ったセキュリティリスクについて、具体的なユースケースに展開し、各ユースケースごとに、何が最も重要かつ必要な対策か議論してまとめ、それを組織に展開運用し、定期的にチェックして改善していくPDCAサイクルを実施する。	PDCAサイクルについて要点1に記載しております。対策例の記載の充実については今後の取組の検討にあたって参考にさせていただきます。
96	法人・団体（匿名）C	17	第2章 2.1 要点2	（3）対策例	上記を受け、一案として次のような修正はいかがでしょうか。 「・・・被害を最小限にとどめるための多層防御等の措置を記述した『『高度標的型攻撃』対策に向けたシステム設計ガイド』を公開している。」	対策例として一部の事例のみ記載しております。
97	法人・団体（匿名）A	18	第2章2.2 【分析】指針 2	（要点の追加）	要点レベルで、可用性が損なわれるリスクがあることを想定する必要があると考えます。事例としては、バッテリーで動作する機器に対する、バッテリーを消耗させるような攻撃等があります。	可用性が損なわれるリスクの想定については、要点3の守るべきものの特定に含まれると考えております。
98	株式会社 ベリサーブ	19	(1)ポイント		以下の文を追加する ③ 洗い出した「守るべきもの」を重要度の高い順に階層的に配置して整理する	御指摘の点については、(P12)に「それぞれの分野におけるリスクを考慮し、実施の要否を含め、IoTセキュリティ対策を検討することが重要である」との記載において、「重要度の高い順に階層的に配置して整理する」ことを考慮しております。
99	一般社団法人日本クラウドセキュリティアイランス	19	要点3	要点3全体	機器自体や取り扱う情報に加え、ネットワークを経由した集中管理・保守機能についても言及が必要と考える。IoT 機器の大半は、集中管理されており、ソフトウエア（ファームウェア）の更新などが、こうした管理サービスを経由して行われるので、サービスサイトの侵害により、機器を含むシ ステム全体が乗っ取られる危険がある。この点には是非言及していただきたい。	サービスサイトも含めてIoTシステムとしてとらえており侵害されればIoTシステムとして影響を受けるということもあるとの認識で（P24)に要点5を記載しています。なお、集中管理については、要点9にて監視サーバについて記載しています。
100	インテル株式会社	19	要点3. 守るべきものを特定する		(2)「要点3. 守るべきものを特定する（19ページ）」の表現について 「守るべきものを特定し、その価値、守れなかった場合のインパクトを明確化する」と明記すべきだと考えます。何故ならばセキュリティ環境の構築には投資が必要ですが、守るべきものの価値とリスクを知ることで、初めて環境構築への投資額が決められるからです。	御指摘の点については、(P12)に「それぞれの分野におけるリスクを考慮し、実施の要否を含め、IoTセキュリティ対策を検討することが重要である」との記載において、「重要度の高い順に階層的に配置して整理する」ことを考慮しております。
101	個人E	19	2.2	表5	「ユーザ情報」の説明に「プライバシー情報」を含める。	ユーザ情報の説明には個人情報や操作履歴、GPS等を記載しており、御指摘の趣旨は含まれていると考えます。
102	個人E	19	2.2	表5	「ソフトウェアの設定情報」の説明に「設定変更の記録」を含める。	御指摘を踏まえ、修正いたしました。
103	一般社団法人情報処理学会	19	2.2	要点3. 守るべきものを特定する	■2.2【分析】 要点3「守るべきものを特定する」 対象をIoTと考えると，「デバイスの数」の観点が欠かせないのではないでしょうか． その点では「リスクの認識」の段階から，『数』を考慮に入れてリスクを把握し，負荷の高い対策が必要な機器を最小化する，といった観点も記載されていて良いのではないでしょうか．	御指摘を踏まえ、要点3解説に「また、IoT機器はその数が多い場合も想定したリスク認識が必要である。」を追記いたしました。
104	一般社団法人情報処理学会	19	2.2	要点3. 守るべきものを特定する	■2.2【分析】 要点3「守るべきものを特定する」 また，IoT セキュリティにおいて守るべきものの一つとして，IoT機器・システムが収集する個人情報（プライバシー含む）が挙げられています． ただ，Suicaの事例が示すように，単一の機器で収集された情報それぞれにはプライバシー上の懸念がなくとも，複数の機器からの情報を集約することにより，個人のプライバシーを犯しうるデータが生成されるリスクがあります． この点に関して，データを集約・蓄積することによるプライバシーリスクについて適切に啓発するとともに，サービスの提供に必須とは言えないデータについては，事業者自身を個人情報保護法違反のリスクから守る観点からも，収集しない，もしくは蓄積しない，などの対策を積極的に検討するよう促すことも重要かと思われます．	御指摘の利用者のプライバシーについては、4章のIoT時代のデータ管理の在り方に記載のとおり、用途に応じて、各分野において今後の課題として検討されるべきものであると考えます。
105	一般社団法人情報処理学会	19	2.2	要点3. 守るべきものを特定する	■2.2【分析】 要点3「守るべきものを特定する」 さらに，要点3で特定した情報資産，及び要点13で収集した情報を，サービス提供者が保存，廃棄するルールについて，すなわち価値，個人情報（プライバシ情報を含む）を企業が保持することのリスクについて言及し，適切に保存，廃棄することの重要性を追記することの検討をお願いします． 例えば，要点21を実施するためには，IoT機器とその利用者の対応情報をサービス提供者側が把握・管理する必要があると思われますが，逆にそれによって得られる情報の流出，機能の悪用等のインシデントが想定されます． さらに，「「安全安心」は，「セーフティ」「セキュリティ」及び「リライアビリティ」を含んだ概念であり，対象とする機器やシステムのセーフティ，セキュリティ，リライアビリティが確保されていること．」と定義されていますが，機器やシステムのみを対象としており，そのまま解釈すれば利用者の生命は含まれないことになります． 利用者の安全性やセキュリティも明記した方が良いと思われます． また，"安心"は，安全からくる利用者の主観により決められる心理であり，何を達成すべきか曖昧なものでありますが，要点10,11,12,17においても"安心"について，具体的な事柄が述べられていません． 安心性は提供者側が一定程度高めることは可能と思われますが，最終的な判断は利用者に委ねるのが自然であると思われます． その意味で，サービス提供者は，利用者が安心できるための必要な情報を正しく迅速に提供するべきであると考えます． "安心"という言葉を削除するか，具体的にガイドライン中で言及されると良いと考えます． また，本来機能を，"つながる"ことが不要な機能，"つながる"ことでより良いサービスを提供する機能，"つながる"ことが必須の機能などに分けて分類してはどうかと考えます． サービス提供者は，安全・セキュリティ分析において，これらの分類を実施すべきである．一方，利用者は，これらの機能を把握し，必要／不要を選択する権利があると思われます（例えば，リスクを許容したくないので，"つながる"ことが必須の機能は停止するなど）．	(1)御指摘の個人情報については、要点3で守るべきものの対象として抽出しています。それに対する対策は指針3として包括的に「守るべきものを守る設計を考える」として記述しています。但し、適切な保存とは何かについて個別に検討が必要であると考えています。 廃棄の件は、(49P)要点18に記載しております。 (2)機器やシステムのセーフティやセキュリティにより事故や攻撃を防ぎ、その結果、利用者の生命を守ることを想定しています。 (3)また、本ガイドラインでは「安全安心」の一語でセーフティ、セキュリティ及びリライアビリティを概念としております。一般的な主観により決められる心理の「安心」とは別とお考え下さい。 (4)本来機能の細分化については、個々のIoT機器毎に検討がなされる事項として考えています。
106	法人・団体（匿名）C	19	第2章 2.2 要点3	（2）解説	米国における、業界の先行例である『Industrial Internet Reference Architecture ver.1.7（2015）』及び『Reference Architecture Model Industry 4.0 (RAMI4.0)2015』とある程度のコンセプトの共有を図ることが今後を考えると望ましい。 そこで次のようにIoTシステムの記述を整理することも一案と思い提案させていただきます。 「・・・ユーザの身体や生命、財産を守るための機能を有していた。機器やシステムがつながりを持つIoTに変化すると、さらに複雑な状況が生まれる。機器制御の機能をもつIoTは、原則としてセンス＆アクチュエーションという働きを有しており、IoTシステム側の運用プロセスの不具合、IoT機器の誤作動及び誤作動の他機器・システムへの波及、つながるための機能を逆用した外部の攻撃から、IoT（システム）を守るとともに、IoTシステムの生成・保有する情報が漏洩しないよう守る必要がある。 その際、IoTの安全安心の観点から、守るべき対象はIoT機器の本来機能、IoTシステム（サービス）相互及びネットワークとの連携（つながり）、IoTシステム及び保持するデータの可用性及び完全性、データの機密性である。」	御指摘の「保持するデータの可用性」及び「完全性」、「データの機密性」については、今後の検討における参考とさせていただきます。
107	一般社団法人電子情報技術産業協会（JEITA）	19-20	2.2	要点3 (2)解説、(3)対策例	本書内において、「本来機能」の意味する範囲の中に、セーフティ機能が含まれるか否かの整合がとれていないように見える。 要点3の(2)では「エアコンであれば冷暖房のような固有の機能に加え、事故や誤動作が発生してもユーザの身体や生命、財産を防ぐための機能も備えている」と書かれており、セーフティ機能を含むように見える。 一方、要点3の(3)では「IoT機器・システムが有する本来機能（～中略～）、セーフティを実現する機能、～省略～」と書かれており、セーフティ機能を含まないように見える。P.35（要点10 (3)②）でも同様に「守るべき機能（本来機能やセーフティ関連機能）」と書かれている。	御指摘を踏まえ、要点3及び要点10を修正いたしました。 (19P)要点3の(3)の「セーフティを実現する機能、」の削除 (35P)（本来機能やセーフティ関連機能）の削除
108	一般社団法人電子情報技術産業協会（JEITA）	19		安全安心	安全安心の用語のさらなる整理、検討が必要ではないか。 19ページ注7ではセーフティ、セキュリティ、リライアビリティを含んだ概念としているが、要点11及び12ではセーフティ、セキュリティのみを示している。	御指摘を踏まえ、要点によりそれぞれの比重が異なる場合がありますが、今後の取組の検討にあたっての参考にさせていただきます。
109	一般社団法人電子情報技術産業協会（JEITA）	19	2.2	要点3 (3)対策例	守るべきものを最小限に絞った仕様・設計とすることも重要である。	指針3の冒頭に、「限られた予算や人材でIoTのセキュリティ対策を実現するためには、守るべきものを絞り込んだり、」と記載しております。
110	法人・団体（匿名）A	19	第2章2.2 要点3.	(3)対策例 ①守るべき本来機能や情報の洗い出しの表5	守るべき情報の例として、機器の内部にある認証の為の情報は極めて重要なものであると考えます。従って、表5の情報資産として、「暗号鍵やPINなどの機密情報」を追加するのが良いと考えます。	表の「機器情報」の「機器認証情報等」に含まれると考えております。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
111	株式会社 ベリサーブ	20	(1)ポイント		以下の文を追加する ③ 洗い出した「守るべきもの」の重要度順につながりを考慮して表に整理する たとえば、企業の重要システムのうち、DNSサーバーは、アクセスしてくる端末認証において最重要機器なので、重要度レベルAとする。ファイアーウォールやLANスイッチは重要度レベルBのように、階層に分けて整理するとリスクを考えやすくなる。	御指摘を踏まえ、修正いたしました。
112	法人・団体(匿名)A	20	第2章2.2 要点3.	(3)対策例 ①守るべき本来機能や情報の洗い出し設計情報、内部ロジック	電磁波等から読み取られるのは内部データや機密情報でありロジックではないため、誤解のない表現への修正を要望致します。	読み取られるデータの傾向によるロジックの類推を含んで記載しています。
113	一般社団法人日本クラウドセキュリティアイインス	21	要点4	要点4全体	System of Systemsとして複数のIoTシステム/サービスが連携した場合に生じるリスクも想定に加えていただきたい。 単一のIoTシステムではプライバシー侵害に至らなくとも、情報集積度が上がることでプライバシー侵害度が上がる(個人特定できる可能性が生じる)ケースがあり得る。この場合、関係者が意図しないままリスクが上昇してしまっている場合もあり、十分な想定検討が必要と思われる。	御指摘の点は、第4章の今後の検討事項の「IoT時代のデータ管理の在り方について」において記載しております。
114	一般社団法人テレコムサービス協会	21～24	要点4,5		要点4「つながることによるリスク」で記載されているように、クローズドなネットワークや保守時のリスクを想定することは重要と考えます。 「つながることによるリスク」を広く周知し、「セキュリティ・バイ・デザイン」の考え方が広がり、安全・安心なIoTシステムが増えることを期待します。	本ガイドラインの賛同の意見として承ります。
115	次世代ICカードシステム研究会	21	(3)対策例	①IoT機器・システムとしてのリスク想定	具体的な対策事例について列挙されております。しかし、パスワードを中心とした対策となっており、今後の認証技術を活用することが想定されていません。 例えば、ICカードやSIM(UICC)等のセキュアなデバイスを活用することで、知識認証のみに依存しないセキュリティレベルの向上ができます。こうした趣旨の内容を記載すべきと考えます。	対策例として一部の事例として記載しています。
116	次世代ICカードシステム研究会	21	(3)対策例	①IoT機器・システムとしてのリスク想定	パスワード認証における注意点の中でブルートフォースアタックに対応するため、 ・一定回数以上の失敗に合わせて機能制限をする。 ・繰り返し行われる攻撃に対応して遅延時間を挿入する。 という趣旨の内容を記載すべきと考えます。	御意見を踏まえ、「・一定回数以上の失敗に併せて機能制限をする」を追記いたしました。
117	一般社団法人情報処理学会	21	2.2	要点4. つながることによるリスクを想定する	■2.2【分析】要点4「つながることによりリスクを想定する」 対策例としてパスワードの堅牢化が挙げられていますが，ガイドラインとして出すと，ある程度基準化してしまう可能性があると思われます． パスワード認証については，長時間をかけた総当たり攻撃が想定されますが，管理者がそれに気づかないといずれは破られる可能性が高いため，総当たり攻撃への対策(たとえば一定期間に一定回数以上認証に失敗すると，しばらくの間は認証を行えないようにするなど)を対策例に含めてはどうでしょうか． また，機器との間の直接パスワード認証以外の方法を検討すべきではないでしょうか． 例えば，クラウド(側のtrust anchor)をまじえた認証システム，証明書ベースのセッション認証など，他の事例も含めた方が良いのではないでしょうか． また，①IoT機器・システムとしてのリスク想定にて「一定期間，パスワードが変更されない場合」が問題のある状況とされていますが，現在では，パスワードの定期変更はコスト(労力)の割には効果が薄く，パスワードは漏洩の可能性があった場合以外は変更は不要だという意見もあります． 特に，IoT機器ではパスワード変更のコストは大きくなることが予測されるため，「パスワードの定期変更」を促す方向は再考する必要があるのではないでしょうか． あえて書くならば，「漏洩の可能性があった場合に変更を促す」ではいかがでしょうか．	(1)御意見を踏まえ、「・一定回数以上の失敗に併せて機能制限をする」を追記いたしました。 (2)認証方法は、多岐に渡るため対策例として一部の事例のみ記載しております。 (3)御指摘を踏まえ、「・一定期間、パスワードが変更されない場合」を削除し、「攻撃の可能性があった場合に変更を促す」に修正いたしました。
118	法人・団体(匿名)C	21	第2章 2.2 要点4	(2)解説	(1)において「クローズな環境」を明示しているので(2)を次のように修正し、事例を紹介するのも一考かと思います。 「・・・ことが原因と考えられる。また、インターネット等の外部ネットワークから隔離され運用されていた制御系又は情報系システムが、保守用に持ち込む等のUSBにより感染し、機器の誤作動、内部情報の持ち出しという攻撃を受けたとされている事例が起きている(Stuxnet等)。そのとき利用された特殊なマルウエアは亜種を生成しながら拡散している。」	工場へのUSB持込と類似の事例のため、追記は見送らせていただきます。
119	一般社団法人電子情報技術産業協会(JEITA)	21	2.2	要点4	不要なものは接続しない、接続するものは全てウィルスチェックする説明を強くするべきである。 電子タバコを充電目的で接続してマルウェアに感染した事例がある。注意文言として、要点4(3)対策例①1)に「充電または電源供給のためのUSB機器接続を行わない。」を追加してはどうか。 また、要点4(3)対策例①1)の具体例5つ目：の 「持ち込むパソコンやUSBのウィルスチェックを行う」を 「持ち込むパソコンやUSB、CD/DVD等のメディアのウィルスチェックを行う」に修正してはどうか。	今後の取組の検討にあたっての参考にさせていただきます。
120	一般社団法人電子情報技術産業協会(JEITA)	21	2.2	要点4 (3)対策例	仕様上不要なネットワークやポータブルメディア(及び接続ポート)は設けない、保守上必要であれば通常は塞いでおくことも対策となるのではないか。	要点8表6の中で「不要な非正規I/Fや露出した配線の除去」といった対策例を示しております。
121	個人E	22	2.2	(3)対策例	「2)問題がある状況への対応」の機能として、「設定情報が変更(書き換え)された場合」を追加する。	今後の取組の検討にあたっての参考にさせていただきます。
122	個人E	22	2.2	要点6	「物理的なリスクを認識する」ではなく、「物理的なリスクを想定する」の方が良い。	まずリスクがあることを認識し、その上で必要に応じたリスクの想定が行われるという趣旨で「認識」としています。
123	株式会社ラックサイバー・グリッド・ジャパン	22	第2章 2.2 要点4.	「一定期間、パスワードが変更されない場合」	提案:左記項目を削除する。 理由:定期的変更は推奨されないため。 このような時代遅れのセキュリティ対策の押し付けは慎むべきである。 定期的変更によりユーザの負担を増大させ、弱いパスワードを設定させてしまうリスクが生じる。 また、定期的変更を促す通知を模したフィッシングメールにだまされたユーザがパスワードを漏えいさせるリスクを増大させる。 マイクロソフトではパスワードの取り扱いについて以下のガイダンスを出している。 https://blogs.technet.microsoft.com/jpntsblog/2016/05/27 /マイクロソフトのパスワードに関するガイダンス/	御意見を踏まえ、修正いたしました。
124	法人・団体(匿名)C	22	第2章 2.2 要点4	(3)対策例	高セキュリティ型の要求設定として電子証明書を利用するという方式も例としてあってもよいかと思います	今後の取組の検討にあたっての参考にさせていただきます。
125	一般社団法人電子情報技術産業協会(JEITA)	22	2.2	要点4 (3)対策例	「ペネトレーション・テストの実施」の記述があるが、ホワイトボックス・テスト、ブラックボックス・テストに細分化して記述してはどうか。 また、推奨するテスト・ツール、検証ツール等の参考情報を掲載されるのが望ましいと考える。	対策例として一部の事例のみ記載しています。
126	一般社団法人電子情報技術産業協会(JEITA)	22	2.2	要点4	TELNETサービス・ポートの閉鎖等、実際に被害の大きいものは、より具体的な文言を盛り込むべきである。 第一回審議資料3-2「まとめ」にも「安易なTELNETコンソール解放」が挙げられている。 例えば、要点15(3)対策例の「①4)不要なサービス・ポートの停止」の冒頭に「TELNETやFTP等のサービス・ポートが狙われて不正アクセスを受ける可能性がある。」を追加してはどうか。	御意見を踏まえ、該当箇所を修正いたしました。
127	法人・団体(匿名)A	22	第2章2.2 要点4.	(3)対策例 ①IoT機器・システムとしてのリスク想定	3)ペネトレーションテストの実施については、内部不正防止のため、外部の専門業者(信頼できる第三者機関)に委託するのが有効であると考えます。	今後の取組の検討にあたっての参考にさせていただきます。
128	法人・団体(匿名)A	22	第2章2.2 要点4.	(3)対策例 ②保守時のリスク、保守用ツールの悪用によるリスク	1)保守時のリスクを想定することは大前提であるとの観点から、「そこで特に重要な機器については、内部不正の抑制に加え、保守時のリスクも想定する。」の文章において、「特に重要な機器やシステムについては」は削除した方が良いと思います。 記載されていないリスクとして、認証情報がコピーされたり、改ざんされたりすることによって機器のなりすまし等が発生するリスクを追加することが望ましいと考えます。	(1)御意見を踏まえ、修正いたしました。 (2)想定されるリスクが多岐に渡るため網羅的に記載しておりません。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
129	一般社団法人日本クラウドセキュリティアイアンス	23	要点5	要点5全体	つながる機器の台数もリスク要素として言及すべきと思われる。個々の機器やサービスのリスクは小さくても、管理サービスへの侵害などで、全体が乗っ取られるなどした場合、多数の機器から構成されるIoTシステムでは、悪用による影響が大きくなる可能性が高い。	御意見を踏まえ、要点3(2)解説にて「また、IoT機器はその数が多い場合も想定したリスク認識が必要である。」を追記いたしました。また、要点5（2）解説にて「つながりを通じて影響が広範囲に伝播することが懸念される。」において御指摘の点を含んでいます。
130	インテル株式会社	23	要点5. つながりで波及するリスクを想定する		(3)「要点5. つながりで波及するリスクを想定する（23ページ）」の内容について 要点5では物理的に接続されたシステムに関するリスク想定の指針を述べています。しかしながら、スタックスネット（Stuxnet）のように物理的にインターネットに接続されていないスタンドアローンの機器がウイルスに感染する例（原子力発電所の制御コンピュータが感染など）もあるため、つながりを想定しない利用方法や接続によるリスクの評価に関する記載が必要であろうと考えます。	御指摘の件は、リスク分析に基づく分野別の対策として、各分野において今後の取組の検討にあたっての参考にさせていただきます。
131	個人B	23、50、52、53、58		パスワード設定関連	<パスワード設定関連> ・「他社が推移しにくいパスワード設定」とあるが、具体性があまりないので、推測されにくいパスワードの具体例などを入れるとよいのではないか。 <該当部分> p23:「出荷時の初期パスワードを同一にしない。また、推定されにくいものとする。」 p50:「他社が推定可能なパスワード設定」 p52:「他社が推定しにくいパスワード設定や～～」 p53:「他社が推定しにくいパスワード設定」 p58:「生年月日等他の人が推測しやすいもの」	IPAなど、適切なパスワードに関する情報提供を行っている団体も多いため、本ガイドラインでは現状のままとさせていただきます。
132	法人・団体（匿名）C	23	第2章 2.2 要点5	（1）ポイント	・「守るべきもの」に対するリスクを想定する際に、攻撃の出入り口のリスクに加えて、万が一、入り口が破られた際や、内部犯行に対するリスクを想定するべきです。 サイバーセキュリティ経営ガイドラインでは、出入り口対策に加え、「多層防御」について言及しています。つきましては「守るべきもの」そのものに対するリスクとして以下を追加してはいかがでしょうか。 「③影響が波及するリスクが守るべきもの（データ）におよぶリスクを想定する。」	御指摘の点については、(24P)「IoT同士が接続して大きなIoTを構成する中で、個々のIoT機器・システムのリスクがIoT全体に波及する可能性を想定することも必要である。」との記載において考慮しています。
133	法人・団体（匿名）C	24	第2章 2.2 要点5	（3）対策例	上記を受け対策例として「サイバーセキュリティ経営者ガイドライン」に記載されている記述である以下を引用することを提案します。 「高い対策レベルであっても破られた場合に守るべきものを守るための処置、被害回避・低減のために複数の対策を多層に重ねる「多層防御措置」を講じ、一枚岩のリスク対策の軽減を図る。 多層防御とは、物理層、ネットワーク層からデータ層までの多層防御を導入することで、1つの機器やソフトウェアに依存する拠点防御対策や、単一の境界防御層（主としてネットワーク境界）に依存する対策の場合より、未知のマルウェアや新たな攻撃手法の登場により容易に突破されるリスクの軽減が期待される。」  	
134	法人・団体（匿名）A	25	第2章2.2 要点6.	(3)対策例	対策例にはリスクの想定しか記載されていません。対策例を追記すべきであると考えます。	御指摘の件については、想定したリスクの対策例は要点8以降に記載しております。
135	一般社団法人重要生活機器連携セキュリティ協議会	25	第2章 2.2【分析】 指針2 IoTのリスクを認識する	要点6.物理的なリスクを認識する	2）要点6「物理的なリスクを認識する」の項目について 要点6では、IoT機器器への物理的攻撃（盗難、不正機器への置き換えなど）に言及されているが、1.1.2 IoT特有の性質1でも触れているように、物理的リスクは、最終的に人命や金銭的被害、不正制御による施設破壊など物理的被害につながることを認識すべきことを補足しておくとよいと思います。	御指摘の件は、(5P)（性質1）「IoT機器の制御（アクチュエーション）にまで攻撃の影響が及んだ場合、生命が危険にさらされる場面さえも想定される」という記載において考慮されています。
136	個人E	26	2.2	要点7	「過去の事例に学ぶ」ではなく、「先行事例や過去の事例に学ぶ」の方が良い。	先行事例含めて過去の事例と考えておりますため、御指摘の趣旨は含まれていると考えます。
137	個人E	26	2.2	(1)ポイント	ポイントの3番目として「各種団体のIoTセキュリティガイドラインを学ぶ」を追加する。	今後の検討における参考として承ります。
138	個人E	26	2.2	(3)対策例	IoTセキュリティについて提言しているガイドラインやガイダンスを追加する。一例としてCSA(クラウドセキュリティアライアンス)の「Security Guidance for Early Adoptors of the Internet of Things」がある。これは日本語版がCSAJC(日本クラウドセキュリティアライアンス)によって公開されている。 https://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf	今後の検討における参考として承ります。
139	法人・団体（匿名）C	26	第2章 2.2 要点7	（1）ポイント	ICTの代表例を「パソコン等」という表現にまとめるのは、最近の高度サイバー攻撃等の脅威を矮小化するおそれがあり、以下の通りに修正すべきと考えます。 「① ICTの過去事例から攻撃事例や対象事例を学ぶ。 ② IoTの先行事例から攻撃事例や対策事例を学ぶ。」	ICTとIoTの差分をわかりやすく例示したものです。
140	法人・団体（匿名）C	26	第2章 2.2 要点7	（2）解説	最近のサイバー攻撃の顕著な特徴は情報系（IT）のみならず、制御系に対する攻撃も複合して行われるようになっています。 その際、ネットワーク経由だけでなく、システムのファームウエアのアップデート等の機会を利用して実施されるオフライン攻撃も実際に行われています。従って、記載をより厳しい現実に合わせるべきと考えました。 「・・・インシデント発生の際の対策の参考とすることができる。 近年、ICTに対するサイバー攻撃は、インターネット等の外部ネットワーク経由の攻撃のみならず、制御系システムのアップデート更新を悪用した攻撃も発生しており、情報系システム、制御系システム及びネットワークという全ての領域における脆弱性を監視する必要が生まれている。 その状況はIoTにおいても、同様であり、ICTで発生した攻撃事例や対策等を参考にし、IoTにおけるセキュリティ対策を検討することが有効である。・・・」	ファームウェアのアップデートについては要点17等で記載しており、御指摘の趣旨は含まれていると考えます。
141	法人・団体（匿名）C	26	第2章 2.2 要点7	（3）対策例	第2章2.1要点他でも記載しましたが、サイバー攻撃へのシステム設計上の対策として多層防御の概念を取り込むべきと考えます。 以下が一案です。 「① ICTの過去事例と対策事例 21世紀に入ってから情報系システムに対する攻撃は年々規模を増大させ、その攻撃技法も高度化している。また、制御系システムがオープンシステム化するに伴い従来は聖域と見なされてきた制御系システムも攻撃対象となっている。また最近ではATMの脆弱性を悪用した現場での不正引出も頻発した。 ICTにおけるセキュリティ対策は、境界防御対策だけでは不可能であり、内部対策を含めた多層防御が必要とされる。その代表例を以下に示す。 1）物理セキュリティ 中古IoT機器の解析防止（耐タンパー性）、IoTシステムのサーバ等への直接侵入防止（データセンターの警備、施錠等） 2）境界セキュリティ ファイヤウォール機能の強化、ウイルス対策ソフトの強制利用 3）アプリケーションセキュリティ 更新プログラムの自動化、マルウェアの活性化防止（ホワイトリステイングの活用） 4）データセキュリティ データベース暗号化、データベースファイヤウォールの設置 5）アイデンティティ管理 アイデンティティライフサイクルの確立、ロールベースアクセス管理」	御指摘の多層防御の観点は要点8の外部インターフェース経由等のリスクに対しての対策の検討および個々のIoT機器・システムで対応しきれない場合は、それらの上位のIoT機器・システムを含めて対策を行うこととしており、趣旨は含まれていると考えます。
142	一般社団法人電子情報技術産業協会（JEITA）	26	2.2	要点7	4ページ表1へのコメントの繰り返しとなるが、冒頭で紹介する事例はここで対策案を示したらどうか。また読者が詳細を把握できるように引用元などのリンク等を紹介してはどうか。過去の事例は対策がとられていると思う。	御指摘の対策例は、IoT一般に係る主な事例を記載したものです。また、事例に関する情報は各社の公開情報等を基にしており、多岐にわたるため、掲載はいたしておりません。
143	法人・団体（匿名）A	26	第2章2.2 要点7.	(3)対策例	サイドチャネルアタックと対策としてのICカードやセキュリティ対策済み決済端末等、金融系の事例追加することを要望致します。	御指摘の対策例は、IoT一般に係る主な事例を記載したものであり、各分野やシステムに応じた事例や対策は、個別に検討されるものと考えます。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
144	株式会社 ベリサーブ	27	要点7の後	新規追加	「要点8. リスクの特性・重大性を認識する」の追加に伴い、以下の文を追加する 要点3.から要点7.で洗い出した「守るべきもの」に対するリスクについて、その特性、重大性によって分類するため、特性と重大性を縦と横に置いた表を作成し、その中に具体的なリスクを記入する。 このようにして全体のリスクを認識し、整理する。リスクの特性は、外部と内部の2種類に分けて、不正アクセス、盗聴、攻撃・感染や、持出し、紛失、改ざん・消失などがある。	御意見を踏まえ、要点3（3）②に「なお、洗い出した守るべきものは、必要に応じて重要度を整理する。」を追記いたします。
145	法人・団体（匿名）A	28	2.3【設計】指針3	（要点の追加）	要点レベルで、IoT機器内において、ライフサイクルを意識した情報管理の方法を設計することを追記するよう要望致します。（例えば、廃棄時に電源が入らない機器から確実に機密情報や設定情報を消去する方法など）	本ガイドラインでは御指摘のとおりライフサイクルを意識した構成になっており、例えば廃棄に関しましても要点6、8、18でも記載しております。
146	一般社団法人日本クラウドセキュリティアイインス	29	要点8(2)	解説	保守用インターフェイスが、保守要員による直接管理でなく、管理サービス（サーバ）からの集中管理の場合、管理サービスそのものが侵害された場合や、サービス管理者の内部犯行などは、機器システム全体に影響が及ぶため、非常にリスクが高い。従って、管理システムの設計はこのような事項を考慮したものである必要がある。こうした問題への言及も必要と考える。	御指摘の点は、（29P）要点8(3)対策例①1）「保守用I/Fは保守・運用者用のI/F～～～での接続の例も増えている。」と厳しめの対策を記述しており、リスクの高さは認識しております。
147	個人E	29	2.3	(3)対策例	対策の例として「認証のロギングを通知」を追加する。	対策例の一部の事例のみ記載しております。
148	個人E	29	2.3	(3)対策例	対策の例として「非正規I/Fは不要であればそもそも使用しない」を追加する。	表6に「不要な非正規I/Fや露出した配線の除去」を記載しております。
149	個人D	29	要点8	全般	境界防御的視点からゼロトラストへのシフトを要請することについても検討すべきである。	今後の取組の検討にあたっての参考にさせていただきます。
150	法人・団体（匿名）A	29	第2章2.3 要点8.	(2)解説	図8にてI/Fとして想定している部分への攻撃のみならず、パッケージを破壊することによるブロービング等の物理的攻撃、消費電力測定や電磁波照射等のサイドチャネルアタック等といった脅威についても記載することを要望致します。	御意見を踏まえ、図に物理的攻撃を追加させていただきます。ただし、概要を示す図のため、詳細は記載いたしません。
151	法人・団体（匿名）B	29	要点8	「個々でも全体でも守れる設計をする」	以下のように変更することを提案いたします： 「個々でも／全体でも守れる設計をする」 （修正理由）P29. 要点8(1)ポイントの意図として、①または②のいずれかを満たせばよいと理解いたしましたので、その意図を明確化するために、上記のように加筆することを提案いたします。	いずれか一方ではなく個々と全体の両視点から捉えていただき、その上で可能な対策を検討していただきたいため、現状のままとさせていただきます。
152	一般社団法人重要生活機器連携セキュリティ協議会	29	第2章2.3【設計】指針3 守るべきものを守る設計を考える	要点8. 個々でも全体でも守れる設計をする	3）要点8「個々でも全体でも守れる設計をする」の項目について 設計ということから、IoT機器寄りの設計対策に視点が寄っている印象があります。 冒頭1.4にあるIoTサービスを構成する関係者（機器メーカ、システム提供者、サービス提供者）それぞれができる対策をサービス全体の設計に反映させる考え方、また要点14の対策例で指摘されているIoTシステム・サービス全体でセキュリティ確保する設計、機器・ネットワーク・プラットフォーム・サービスの各階層でセキュリティ対策の役割を分担してサービス全体のセキュリティを確保する考え方を、ここでも補足してはどうか、と考えます。	要点8はIoTサービスを提供する要素となるIoT機器・システムの設計を中心に記載しています。それらの活用するIoTサービスの設計については要点14で扱うように分離して記載しております。
153	一般社団法人日本クラウドセキュリティアイインス	30	要点8(3)対策例①2)	内包リスクへの対策	開発のためにオープンソースのプラットホームを利用する場合の注意点が必要と考える。特にLinux等のOSをプラットホームとして用いる場合、不要機能やサービスを削除することやデフォルトのセキュリティ設定を見直すなどセキュリティ上の最適化を行うことが極めて重要となる。	対策例の一部の事例のみ記載しております。
154	個人E	30	2.3	(3)対策例	「有償コンテンツ」とあるが、有償に限らない(無償コンテンツでも同様)のため、「有償」を削除する。	御意見を踏まえ、該当箇所を修正いたしました。
155	日本シノプシス合同会社	30、48	●第2章 2.3 要点8 (3) 2) 内包リスクへの対策 ●第2章2.5 要点 18 ① 脆弱性情報の収集・分析、情報発信		b.　P-30 第2章 2.3 要点8 (3) 2) 内包リスクへの対策 P-48 第2章2.5 要点 18 ① 脆弱性情報の収集・分析、情報発信 P-30では「外部調達における設計データや品質データによる対策」について記述されています。また、P-48では脆弱性情報の継続的管理（収集・分析・発信・対策）が記載されています。 脆弱性がシステム中、機器構成部品あるいはソフトウェアのどの部分に含まれるものかという管理、即ち、部品表による機器・システム・サービスの構成管理は脆弱性情報管理の基礎となります。 対象がソフトウェアの場合は、ソフトウェアコンポーネント分析により対象ソフトウェアを構成するパーツを管理することとなります。 ハード、ソフト共に部品表管理が基礎となる旨の記載をご検討願います。	脆弱性情報の管理は御指摘のとおりと考えますが、IoTに限らず一般的な議論であると考えております。
156	日本シノプシス合同会社	30	第2章 2.3 要点8 (3) 2)内包リスクへの対策		c.　P-30 第2章 2.3 要点8 (3) 2) スマートフォンなどのオープンな…ソースコードのセキュリティ検査ツール… ソースコードのセキュリティ検査ツールは、ソフトウェア開発時に実施可能なセキュリティ対策として有効且つメリットの高い手法です。 オープンなプラットホームに限定せず利用可能な対策である旨の記載をご検討願います。	対策例の一部の事例のみ記載しております。
157	法人・団体（匿名）C	30	第2章 2.3 要点8	(3)対策例	「外部インタフェース経由のリスクへの対策」について ・遠隔からの操作によって、IoT機器内の各種入出力インタフェースを直接操作できないような実装を設けるのは現状のWebシステムにおいて典型的な実装形態です（例: Java、Flash など）ので、これを代表例として記載しておくのがよいかと思います。 ・IoT機器への外部ネットワークからの侵入をそもそも許可しない構成を推奨例の一つとするのはいかがでしょうか? 例えば、IoT機器から事前に設定されたサーバー側だけに定期的にアクセスしてサーバーからの操作要求を取得し、その後、IoT機器内での処理を行うという処理構成で疑似的に双方向通信を実現する方式があります。これは IoT機器への外部侵入を困難な形にできるため、よりセキュアになります。	対策例の一部の事例のみ記載しております。
158	個人D	31	要点8 (3) 4)		以下に関して ・性能が不十分でセキュリティ機能を載せられない IoT 機器・システムは、下図のようにそれらを 含む「上位の IoT 機器・システム」で守る対策を検討する。 ・IoT 機器・システムがインターネットにつながる接点を絞り込むとともにゲートウェイを設け、攻撃を遮断する設計を行う。 ⇒IoT機器は携帯網等の無線通信部分を介して上位機器に接続することが多いが、その全体像を見た場合に最も脆弱な部分は、末端のリソースが少ない機器／システムと上位機器の間の通信であることが考察されていない。	御意見を踏まえ、修正いたしました。
159	一般社団法人電子情報技術産業協会（JEITA）	31	2.3	要点8②図9	OTSなどを利用する場合の既知の脆弱性対策を確認・実施すること、低廉・処理能力の低いデバイスの対策例等も記述戴きたい。 例えば、ホワイトリスト型ウイルスソフトに倣って、ソフトウェアやデータの不用意な変更禁止（改ざん検知及びセキュアな更新方法）、起動制御などは廉価の機器等でも比較的導入しやすい対策と思う。	対策例の一部の事例のみ記載していますので、現状のままとさせていただきます。
160	個人D	32	要点9 (1)及び(2)		無線通信、インターネットなどベストエフォートで信頼性の低い通信路を「制御」に使うことの是非から論じるべきである。 例えば、BGPハイジャックで上位システムまるごと乗っ取られる場合や、偽基地局を設置され、悪意のある指令が下位に出されるといったことは検討範囲内であるか、さらに下位機器は簡単に人の手が届く範囲にあるとは限らないことなど、想定されていることと想定されていないことの区別ができない。 むしろ「こう使ってはいけない」という例示をすべきではないか。 例えば、センサーからの情報が細工された場合にも破綻しない上位システムの設計といった検討課題も扱うべきである。	御指摘の用途に応じた通信品質等については、第4章に記載のリスク分析に基づき個別に検討が必要な事項と考えます。
161	個人D	32	要点9	全般	センサー（トランスデューサー）としたとしても検討すべきである。	
162	法人・団体（匿名）A	32	第2章2.3 要点9.	(3)対策例①異常状態の検知と波及防止	異常状態の検知として、認証情報の有効期限チェック等を追加すべきと考えます。	対策例として一部の事例のみ記載しています。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
163	法人・団体(匿名)A	32	第2章2.3 要点9.	(3)対策例	ハードウェア構成並びにソフトウェア及び設定の改ざんを検知するセキュアブートなど、IoT機器の真正性確認に関する記述を追加すべきと考えます。	対策例として一部の事例のみ記載しています。
164	個人E	32	2.3	(3)対策例	「1)異常状態の検知」の監視の例に「相関分析機能や人工知能(AI)を搭載したSIEM(Security Information and Event Manager)による監視も有効である」を追加する。	対策例として一部の事例のみ記載しています。
165	個人E	34	2.3	(3)対策例	「経緯や根拠も含めて可視化」ではなく、「経緯や根拠も含めて文書化」の方が良い。	図表示やプログラムのコメント行の記述は文書ではないという解釈もあるので、それを避けるために可視化という表現をしています。
166	一般社団法人電子情報技術産業協会(JEITA)	34	2.3	要点10図10	元々の出典は記載のとおりと思われるが、2016年3月にIPAから出ている「つながる世界の開発指針」の60ページ図4-24と同じと思われる。その指針との関係も記載すべきではないか。	本ガイドラインは、「つながる世界の開発指針」を参考にしており、(10P)にその旨を記載しています。
167	一般社団法人電子情報技術産業協会(JEITA)	34-35	2.3	要点10 (3)①	「設計の『見える化』とは、設計における分析、設計、評価などのプロセスを経緯や根拠も含めて可視化すること」と書かれているが、具体例が記載されていると理解しやすい。	今後の検討における参考として承ります。
168	一般社団法人情報処理学会	35			・p.35「守るべき機能(要件)に対する脅威・リスク分析，セキュリティ対策検討，効果及び守るべき機能への影響の分析・評価を行い，評価結果が不十分であると判断される場合には再分析・再検討を行う．」―「守るべき機能(要件)に対する脅威・リスク分析，セキュリティ対策検討，効果及び守るべき機能への影響の分析・評価を行い，評価結果を受容可能でない場合には，対策を検討し，再度分析を繰り返す．」でしょうか．	御意見を踏まえ、該当箇所を修正いたしました。
169	法人・団体(匿名)A	36	第2章2.3 要点11.	(3)対策例	「・」の2つ目「・つながる相手が相応の権限を有する機器と確認できた場合のみ」の事例にあるように、機器のなりすまし対策として認証が重要であることを明記することを要望致します。	対策に認証を用いるのはすべての要点に当てはまるものですが、要点16にまとめて記載しています。
170	次世代ICカードシステム研究会	37	(3)対策例	①検証・評価への反映項目例	具体的な対策事例について列挙されております。 この中でコモンクライテリア(ISO/IEC15408)について記載されておりますが、この評価の基礎となるプロテクション・プロファイル等の評価仕様が未整備です。 このため、評価の結果の実効性が必ずしも判断できません。 そこで、評価で利用する仕様について業界団体等で整備することについても明記すべきです。	本ガイドラインでは、(第2章)「それぞれおの分野におけるリスクを考慮し、実施の要否も含め、IoTセキュリティ対策を検討することが重要である。」との認識を示している。
171	一般社団法人電子情報技術産業協会(JEITA)	37	2.3	要点12(3)対策例	一部の業界ではISO 26262、ISO/IEC 15408の規格・認証制度の取得が定着しているが、より幅広いIoT製品(特に、コンシューマデバイス等)に対応するため、簡易的な認証制度を検討されてはどうか。 認証制度の定着が製造側のセキュリティ投資に対するモチベーションの向上につながると考える。 ただし、各分野の性質に応じ、過度な負担にならないよう制度設計への配慮が必要である。	今後の取組の検討にあたっての参考にさせていただきます。
172	法人・団体(匿名)A	37	第2章2.3 要点12.	(3)対策例	機器やシステムを開発するベンダー、中古機器を扱うベンダーが適切なセキュリティマネジメントシステム(ISMSやPCI DSSなど)の認証を得ていることを推奨すべきとの記載を追加するよう要望致します。	認証を受けた信頼性の高いシステム・サービスの利用について要点14において記載していますが、御指摘の点については、今後の取組の検討にあたっての参考にさせていただきます。
173	一般社団法人重要生活機器連携セキュリティ協議会	37	2.3【設計】指針3 守るべきものを守る設計を考える	要点12. 安全安心を実現する設計の検証・評価を行う	6)軽微な書式設定について 要点12の解説にある図11の図と出典の記述がセンタリングされていないので、他の図と書式を合わせるとよいと思います。	御意見を踏まえ、該当箇所を修正いたしました。
174	株式会社パソナサイバーラボ	38	要点12. 安全安心を実現する設計の検証・評価を行う	(3)対策例①2)	P.38 上から2行目に誤字と思われる記載あり。前後の文脈から推測すると「制度」ではなく、「制御」とするのが正しいと思われる。	御意見を踏まえ、該当箇所を修正いたしました。
175	株式会社パソナサイバーラボ	38	要点12. 安全安心を実現する設計の検証・評価を行う		P.38 IoTのセーフティ及びセキュリティ設計の検証・評価について。 IoTに該当する機器・サービス(P.9ページ参照)とこれに対応する安心安全のベストプラクティス、第三者評価制度、国際規格・国内規格といった網羅的な対照表(マッピング表)のようなものを参考資料として添付してはどうか？本ガイドラインをトップ文書とし、その先の参照文書としてこの対照表を添付することができれば、利便性が高まるのではないかと思われる。本ガイドラインの位置付けとして、本文書をトップ文書として、このガイドラインに紐付くを手順書やマニュアルのような下位文書が必要と思われる。今後このような文書作成を検討されている場合は、お声がけいただければと思います。	今後の取組の検討にあたっての参考にさせていただきます。
176	個人E	38	2.3	(3)対策例	「その他」に「クラウドコンピューティングを使用する場合、STAR認証やISO/IEC 27017認証等も有効である」を追加する。	対策例として一部の事例のみ記載しています。
177	日本シノプシス合同会社	38	第2章 2.3 要点12 ① 2) その他		d. P-38 第2章 2.3 要点12 ① 2) その他 ICSA Labs、NSS Labs、CCDSなどが紹介されていますが、UL Cybersecurity Assurance Program (UL CAP)はWhite House Cybersecurity Action Planに呼応した認証プログラムとして重要なポジションにあると考えます。また、その対象カバレッジが広いことも有用です。UL CAPを併記頂く様ご検討お願いします。	対策例として一部の事例のみ記載しています。
178	個人D	38	要点12 (3)①		「国内では一般社団法人重 要生活機器連携セキュリティ協議会(CCDS)が ATM、車載器(カーナビ等)などのセキュリティ評価ガイドラインを作成している。」に関して セキュリティ評価ガイドラインは、同業種以外にも参考になるため、公開されている場合は参照先を示すことが望ましい。 また、公開されていないガイドラインは非公開であることを示すべきである。	各分野別のガイドラインについては、個々に、また逐次に検討が進められていることから、本ガイドラインは分野を特定せず包括的内容を扱ったものです。
179	一般社団法人情報通信ネットワーク産業協会(CIAJ)	39	第2章 2.4節 【構築・接続】		ネットワーク上での対策について 現状においても、重要度の高いネットワークは、障害や災害発生への対策として構成機器の冗長構成化や回線の複数ルート化等の施策が織り込まれています。 これらの施策はセキュリティ対応上(マルウェア感染機器の切り離し、攻撃による特定ルートの遮断、システム障害時の冗長機器によるサービスの継続等)も有益と考えられ、外部からの攻撃等のセキュリティ上の脅威の特性をあらかじめ理解したうえで、ネットワークの設計時に冗長化等の対応を行えば、より有効となり脅威への耐力も増強されるものと考えます。 本節の要点にネットワークとしての冗長化を考慮して設計を行うことによるセキュリティ対応力の強化について、記載追加を希望いたします。	御指摘のネットワークの冗長化は、IoT機器やシステムの構造や用途によって必要性・有効性等が異なることから、第4章に記載のリスク分析に基づく分野別の対策として、各分野において今後検討が必要な事項と考えています。
180	個人E	40	2.4	(3)対策例	「記録の不正な消去、改ざんの防止」に「改ざん防止機能を備えた統合ログ管理システムを導入する方法がある」を追加する。	対策例として一部の事例のみ記載しています。
181	次世代ICカードシステム研究会	40	要点13	(2)解説	IoTにカテゴライズされる分野は多種多様であり、他の機器との通信状況を把握、記録することまた記録が消去・改ざんされないようにすることはすべてに必要であるとは思われません。 状態把握・記録の異常に対するリスク分析をした上で必要性に合わせて対策すべきです。	(12P)に「それぞれの分野におけるリスクを考慮し、実施の要否も含め、IoTセキュリティ対策を検討することが重要である。」と記載しています。
182	株式会社ラックサイバー・グリッド・ジャパン	40	第2章 2.4 要点13.	(2)解説	提案:5行目の「その内容を不正に消去・改ざんされてしまうと」の前に、「攻撃者等により」を追加する。 理由:ログの消去・改ざんといったリスクを引き起こす主体を明示するため。	御意見を踏まえ、該当箇所を修正いたしました。
183	株式会社ラックサイバー・グリッド・ジャパン	40	第2章 2.4 要点13.	(3)対策例 ②記録の不正な消去、改ざんの防止	提案:「ログを保管する機能を有するIoT機器・システムや専用の装置等」を「ログを保管・分析する機能を有するIoT機器・システム(クラウド)や専用の装置等」に修正する。 理由:ログの外部に記録することにより、ログを分析し、攻撃を予兆する等の可能性が生まれる。 また、「(クラウド)」と付記した方が理解しやすい。	「分析する」や「クラウド」という表現を付け加えると範囲を限定してしまうので、現行の表現としています。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
184	法人・団体（匿名）C	40	第2章 2.4 要点13	（2）解説	IoT（システム）の生成・処理するデータは、今後、二次利用、三次利用されていきます。 しかも、従来は単なるイベントログであったデータが、購買タイミングや付随情報として利用される場合も十分に想定されます。 従って、Big Data化する各種ログデータの必要な部分はオーナーシップと紐づけられた再利用可能データとして、各種システムのアプリケーションサーバではなく厳正な管理の可能なBig Data対応のデータベース等に格納されるべきとかんがえます。 次のような修正が考えられます。 「・・・正しく記録できるよう対策を講じる必要がある。 　また、従来はログデータとして監視・監査用に保管されたデータが再利用可能なデータとして（プライバシー関連項目を削除の上）他のサービスで活用される局面もあることから、必要なデータについてはデータオーナーシップを含む再検証可能な履歴としてデータベースに保管されるべきである。なお、IoT機器・システムの中には・・・」	蓄積されたデータが目的外に利用されることや再利用については、第4章今後の検討事項（IoT時代のデータの在り方について）で記載しており、今後の検討がなされる事項として考えております。
185	法人・団体（匿名）A	40	第2章2.4 要点13.	（3）対策例 ②記録の不正な消去、改ざんの防止	「ログに対してアクセス権限の設定、暗号化・・・を行う方法がある」を、「ログに対するアクセス権限の設定、暗号化に加えて電子署名を用いた真正性確認」に修正するよう要望致します。	対策例として一部の事例のみ記載しています。
186	一般社団法人日本クラウドセキュリティアイアンス	41	要点14（3） 対策例①3）	HSM等の専用の暗号装置で保護することも検討する	IoTシステムにおいてはHSMの採用は困難なケースも多いため、「Trusted Execution Environment（TEE）」、「Trusted Platform Module（TPM）」等への言及も必要と思われる。	御意見を踏まえ、該当箇所を修正いたしました。
187	モバイルコンピューティング推進コンソーシアム	41	要点14 機能及び用途に応じて適切にネットワーク接続する。		【各論】 要点１４　機能及び用途に応じて適切にネットワーク接続する。 　無線ネットワークの種別として、品質・セキュリティが担保されているセルラーネットワーク、安価・簡便に設置できる無線LAN、サービスの応用が拡大しているBluetooth等の近距離無線、など多様な無線ネットワークの利用浸透が進んでいる。 一方、機器設置、対向機器間のパラメータ調整など無線技術の未習熟による問題が散見されおり導入運用に関する考慮、教育等が必要。	御指摘の無線技術の未習熟については、本ガイドラインの対象外と考えます。
188	アラクサラネットワークス株式会社	41	要点14. 機能及び用途に応じて適切にネットワーク接続する	（3）対策例 （2）IoT 機器の機能・性能レベルの考慮	このようなセキュリティガイドラインは重要ですので、ぜひすすめてください。 細かいところですが、以下のような補足を追加することで、より明確になるとおもいます。 ------ P.41　要点１4．機能及び用途に応じて適切にネットワーク接続する 　　（3）対策例　（2）IoT 機器の機能・性能レベルの考慮 >セキュリティ対策の困難なIoT機器をネットワークに接続する場合、 >インターネットへつながる手前でセキュアなゲートウェイを経由させる等、 >セキュリティを確保する手段を講じる。 ★補足案 本手段はIoTセキュリティの確保において有効な対策である。 ここで言う「ゲートウェイ」は広義の意味で、入口・出口としての対策だけでなく、 内部での通信のふるまい監視やホワイトリスト化等による対策も含む。 これらの手段の組合せが重要であり、セキュリティを確保する手段として重要である。	御指摘のゲートウェイが具体的にどのような機能を持つべきかについては、IoT機器等の用途等によってことなることから、各分野において今後検討が必要な事項と考えます。
189	個人D	41	要点14 （3）①		「有線接続ではTLS、無線接続ではWPA2等のネットワーク暗号化を適用する等、ネットワークの通信路のデータの盗聴や改ざんへの対策を行う。」に関して IoTを支える通信部分において、あらゆるところで TLSが利用されている。 一方、当該部分では、安全なTLSを使うためには、どうすべきか？という観点が記述されていない。 安全なTLSを利用するための情報や参照文献等を追加すべきである。	今後の検討における参考として承ります。
190	法人・団体（匿名）C	41	第2章 2.4 要点14	（3）対策例	3）の2項目目の鍵管理の部分は、近年の技術を勘案し、次の通り、より高度化も一考に値すると考えます。 「・・・不正アクセスへの対策を行う。特に暗号鍵、証明書等の枢要なデータについては、鍵管理機能等を有するソフトウェアによる保護又は必要に応じて専用の暗号装置（HSM等）の利用等を検討する。」	御意見を踏まえ、該当箇所を修正いたしました。
191	一般社団法人電子情報技術産業協会（JEITA）	41-42	2.4	要点14 ②IoT 機器の機能・性能レベルの考慮	センサー等の機能・性能が限られたIoT 機器では、「電子政府推奨暗号リスト」に基づく暗号を実装することは困難である。 しかし、そのような場合でも、all or nothingではなく、IoT機器の制約に合せて、軽量かつ安全な暗号方式を適用しておくことは、システム全体のセキュリティ確保にとっても望ましいと考える。 これを踏まえると、例えば、以下のような表現（下線部）が、より適切ではないか。 （例）「②IoT 機器の機能・性能レベルの考慮」の冒頭部分 「センサー等の機能・性能が限られたIoT 機器では、暗号等のセキュリティ対策を十分に適用できない場合がある。こうした制約のあるIoT 機器のセキュリティを確保するには、その制約に合せた軽量かつ安全な暗号方式を適用することを検討する一方で、IoT 機器単体でのセキュリティ対策のみに依存せず、機器、ネットワーク、プラットフォーム、サービス等の階層ごとにセキュリティ対策の役割を分担し、IoT システム・サービス全体でセキュリティを確保することが必要である。」	御意見を踏まえ、該当箇所を修正いたしました。
192	匿名A	42ページ	2.4【構築・接続】 指針4 ネットワーク上での対策を考える	図12 セキュアなゲートウェイを経由する接続イメージ	ガイドラインの42ページの「図12 セキュアなゲートウェイを経由する接続イメージ」に「IoT機器の仮想化」とはいう記述があるが、これをどのように解釈すればよいか。 本文に記載された「セキュリティ対策を確保する手段」のことを「IoT機器の仮想化」と言っているのか。セキュリティ対策のための特殊な技術のように思える。 それとも単にネットワーク接続機能を持たないエアコンのリモコン機能を仮想的に持つホームゲートウェイのようなものを意味しているのか。	御指摘のゲートウェイが具体的にどのような機能を持つべきかについては、IoT機器等の用途等によってことなることから、各分野において今後検討が必要な事項と考えます。
193	次世代ICカードシステム研究会	42	図12	図左部分	図12の主旨が必ずしも明確でないため、分かり易くしていただきたい。 特に、守るべき対象を明確にしていただきたい。 例えば、図12「セキュアなゲートウェイを経由する接続イメージ」では、「セキュリティを十分確保できない機器」に向けて「セキュアデバイス」を関与させる矢印があります。 セキュアなデバイスでもセキュアゲートウェイを経由しなくてはならないのでしょうか？	メーカ、ベンダがセキュリティを確保した機器を提供した場合も、脆弱性の発見等の環境変化による新たな脅威を想定してゲートウェイで機器の管理を行う等のセキュリティ対策を講ずることも考えられることから、現在の図としています。
194	個人E	43	2.4	（3）対策例	「3）ソフトウェアのアップデート」に「一定期間内にアップデートしないIoT機器はネットワークから切り離す（ネットワークに接続させない）ことも検討する」を追加する。	御指摘のアップデートしないIoT機器をネットワークから切り離すことについては、IoT機器等の用途によって条件や必要性が異なることから、第4章に記載のリスク分析に基づく分野別の対策として、各分野において今後検討が必要な事項と考えています。
195	次世代ICカードシステム研究会	43	（3）対策例	②利用者への初期設定に関する注意喚起	最下段「初期パスワードの変更が行われなければ、機能を制限するなどの対策も有効である。」と記載されておりますが、どのような場面で、どのような場合に初期設定から変更されていないと判断するのでしょうか。	御指摘の初期設定からの変更が行われたかどうかの判断方法については、IoT機器等によって実現方法が異なることから、個別に検討されるものと考えています。
196	法人・団体（匿名）C	43	第2章 2.4 要点15	（3）対策例	IoTの中でも中古車販売によって所有者（利用者）が移転する可能性があり、運転情報と運転手を連携させ、保険料算定に利用するテレマティクス保険等の存在を考慮すると、今後は物理キーによる確認・制御だけではなく、運転者を特定するアイデンティティ管理との連携も不可欠でと考えられます。 そこで、①の2）項を以下のように追加したらいかがなものか、と考えました。 「2」アイデンティテイ・アクセス管理の適用 　　直接的な物理デバイス自体だけでなく、利用者に対する適切なアイデンティティ管理と連携することにより、IoTシステム全体に厳正なアクセス管理を実施し、外部からの不正アクセス、メンテナンスを悪用した内部不正の発生を防止する。」	御指摘のアイデンティティ・アクセス管理の適用については、IoT機器等の用途によって条件や必要性が異なることから、個別に検討が必要な事項と考えています。
197	一般社団法人電子情報技術産業協会（JEITA）	43	2.4	要点15①1）	初期パスワードが変更されていない場合、重要な設定は変更できない、初期パスワードの変更は近接操作が必要な仕様とする等も効果的と思う。	要点15（3）対策例②に賛同の御意見として承ります。
198	個人D	44	要点15 （3）①	2）アップデート等の機能の搭載	コード署名を追加すべきである。	御意見を踏まえ、該当箇所を修正いたしました。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
199	株式会社 ベリサーブ	45	要点16の後	新規追加	「要点17. 感染を検知したら拡大を遮断する機能を設ける」の追加に伴い、以下の文を追加する (1)ポイント ① IoTシステムのどこかで感染を検知したら、どこで全体への感染を遮断すべきか検討する。 ② 検知→感染の種類、場所の特定→遮断箇所の特定→遮断実行のフローを検討する。 (2)解説 IoTシステムは、自社の基幹システムと接続されているだけでなく、インターネットや無線LANを通じて多くの外部システムとも接続されている。ゼロデイ攻撃など防御対策が間に合わない場合も考慮すると、感染を検知したら迅速にそのエリアを隔離することが重要になる。そのためには、感染場所を特定し、守るべきシステムにつながる経路を感染から遮断することが必要である。 (3)対策例 ① IoT端末のネットワークと基幹システムのネットワークを分離 1) ネットワークのセキュリティ方針 基幹システムに自由に常時接続できるようなネットワーク構成にすると、感染に対して脆弱になるため、ゲートウェイやファイアウォールなどのセキュリティ機器をどのように配置したり、どんな設定をするかという方針を立てる。 2) セキュリティ対策の適用 具体的なセキュリティ機器の配置と設定を行い、感染検知の種類や重要度ごとに、感染時にはどのように遮断するか検討して適用する。 3) セキュリティ対策の有効性評価 感染時の対応シナリオを用意し、対策の有効性を評価検証し、最適な設定にする。 専門的な知識を必要とする場合もあるため、セキュリティ対策の専門業者のサービスを利用することも検討する。	御指摘の感染を検知した場合の遮断については、要点9(3)対策例①2)異常状態の影響の波及防止に記載のとおり、IoTのセキュリティ対策として重要な事項である一方、IoT機器等の用途によって判断基準や実装方法が異なることから、詳細については、第4章に記載のリスク分析に基づく分野別の対策として、各分野において今後検討が必要な事項と考えています。
200	一般社団法人日本クラウドセキュリティアイアンス	45	要点16(3)対策例①	接続するIoTシステム・サービス相互で鍵・証明書等を使用した認証を行う。	IoTシステムの長いライフサイクルや保守の困難性に応じ、IoT機器が用いる鍵や証明書の有効期間をどのように設定し、IoT機器のリスク判定にどのように活かすかの検討が必要となるため、そうした観点への言及も必要と思われる。	御指摘のライフサイクルに応じた鍵や証明書の有効期間の設定については、IoT機器等の用途によって条件が異なることから、第4章に記載のリスク分析に基づく分野別の対策として、各分野において今後検討が必要な事項と考えています。
201	次世代ICカードシステム研究会	45	(3)対策例	①セキュリティの確保を実現する認証機能	1番目の「●」に記載される「IoT機器の識別子による認証を行い」の識別子とはどのようなものが想定されているのでしょうか。 また、それは耐タンパ装置に保存することを想定しているのでしょうか。	御指摘の識別子の種別や実装方法については用途・機器によって識別子として利用する情報が異なり、さらにその情報の保管場所についても用途によって重要性が異なることから個別に検討が必要な事項と考えます。
202	個人D	45	要点16	全般	認証機能だけでなく認証後の認可についても追加すべきである。	今後の検討における参考として承ります。
203	個人D	45	要点16		「接続する相手のシステム・サービスのなりすましへの対策を行う。接続するIoTシステム・サービス相 互で鍵・証明書等を使用した認証を行う。」に関して 任意団体であるOnline Trust Allianceが発行しているIoT Trust Frameworkに示されている通り、鍵・証明書を用いた認証においても信頼性が必要な用途も想定されるため、信頼できるルートの説明も追加すべきである。 また、失効の説明も追加すべきである。	御指摘の信頼できるルート証明書やその失効については分野や用途によって条件が異なることから、各分野において今後検討が必要な事項と考えています。
204	個人D	45	要点16 (3)①		「接続する相手のシステム・サービスのなりすましへの対策を行う。接続するIoTシステム・サービス相 互で鍵・証明書等を使用した認証を行う。」に関して 証明書は、電子証明書に修正すべきである。	御意見を踏まえ、該当箇所を修正いたしました。
205	個人D	45	要点16 (3)②		以下に関して 暗号を用いた認証の適用 IoT機器のファームウェア更新時には、過失または故意によって、ファームウェアの改ざん等の脅威が想定される。 そうした脅威に対してIoT機器のファームウェアを正しく更新するためには、更新データの正当性を担保する必要がある。 ⇒暗号を用いた認証ではなく、暗号技術を用いた認証が適切である。 また、該当部分に示した文章は、認証の必要性を説明していなく、改ざん検知等の必要性を説明している。 ここで示すべきは、正しい相手先から正しい更新データを確認するための認証と改ざん検知である。	ファームウェア更新にかかる対策に関する御指摘の趣旨は現在の記載に含まれていると考えます。
206	法人・団体(匿名)C	45	第2章 2.4 要点16	(1)ポイント	本要点16では、「利用者」を含むIoTシステム全体を言及しているので、「認証機能」だけではありません。 「アイデンティティ・アクセス管理」にするべきと考えました。 「① IoTシステム・サービス全体で適切なアイデンティティ・アクセス管理等を実施する。 ② IoT機器の機能・性能の制約を踏まえた適切な管理方式を採用する。」	御指摘のアイデンティティ管理については想定するシステムに応じて個別に検討されるものと考えます。
207	法人・団体(匿名)C	45	第2章 2.4 要点16	(2)解説	「・・・そうしたなりすましや盗聴等の脅威への対策として、アイデンティティ・アクセス管理及び通信経路における相互認証、通信暗号化等の仕組みの導入が必要である。」	御指摘のアイデンティティ管理については想定するシステムに応じて個別に検討されるものと考えます。
208	法人・団体(匿名)C	45	第2章 2.4 要点16	(3)対策例	上記をふまえて以下が提案する一例となります。 「① IoTシステム・サービス全体で適切なアイデンティティ・アクセス管理等 IoTシステム・サービス全体で適切なアイデンティティ・アクセス管理等を実施する。 具体例を以下に示す。 ・ 接続するIoT機器のなりすましへの対策を行う。IoT機器の識別子、IoTシステムに保管された属性情報等に基づくアクセス管理を実施し、不正な、又は属性情報等が極度に疑わしいIoT機器をアクセス拒否する。 ・ 認証後も機器のなりすましを困難にするために、単純な接続ではなく、定期的にセッションをリフレッシュしたり、認証とメッセージ送信の方式を変えるなどの処理を施して、接続状態を同じ状態のままにしておかない。 ・ 利用者のなりすましへの対策を行う。利用者を識別するID、パスワード及び生体認証等のクレデンシャル、ICカード及びスマートキー等のトークンを適切に利用し、必要に応じて利用時間帯、位置情報等の属性情報による警報を含めたアイデンティティ・アクセス管理を実施する。必要に応じて利用者のプロビジョニング、デプロビジョニングの体制をIoTサービスとして提供する。 ・ 接続する相手のシステム・サービスのなりすましへの対策を行う。接続するIoTシステムのフェデレーションを強化し、サービスの相互認証を行うとともに、必要に応じて接続先のトラストモデルを適用したサービス利用に対する警報を準備する。 ② IoT機器の機能・性能の制約を踏まえた適切な管理方式 取り扱う情報の種類に応じ、IoT機器の機能・性能に制約があても、データの改竄や漏えいを防ぐことのできる識別認証技術を採用するとともに、人間の生命の安全に係わる制御系のIoTにおいては、必要に応じて否認防止を検討する。 具体例を以下に示す。 ・ 暗号技術を用いた識別認証の確保 IoT機器のファームウエア更新時には、過失又は故意によるファームウェアの改さん等の脅威が想定される。IoT機器のファームウェアを正しく更新するためには、更新データの正当性を担保すべく、ハッシュ関数等の暗号技術を用いた機器認証、利用者認証及び通信内容の識別認証が有効である。ただし、IoT機器が長期間利用される場合は、その暗号アルゴリズムにはIoT機器の使用期間終了まで危殆化しないと予想される電子政府推奨暗号等を採用することが適当である。」	御指摘のアイデンティティ管理については想定するシステムに応じて個別に検討されるものと考えます。
209	一般社団法人電子情報技術産業協会 (JEITA)	45	2.4	要点16	要点16でパスワード以外の認証も記載されているが、認証に関連した他の要点でもパスワード以外の認証方法について追加が必要ではないか。 IoT機器はキーボードがなく、パスワードによる認証を実施しにくい機器が比較的多いと思われる。 要点4、7及び15の対策例では、パスワードの例が示されている。 低廉なIoT機器が実現しやすいパスワード以外の例示も必要ではないか。	御指摘のパスワード以外の認証については、理解が容易になる様、各要点では論点を絞って記載しており、認証については要点16に集約して記載しております。
210	法人・団体(匿名)A	45	第2章2.4 要点16.	(3)対策例	IoT機器の識別子による認証だけでなく、クライアント証明書による認証、メッセージ認証などの手法を追記するよう要望致します。	御意見を踏まえ、該当箇所を修正いたしました。
211	法人・団体(匿名)A	45	第2章2.4 要点16.	(3)対策例	暗号鍵や証明書のコピー・改ざんに対する対策を記載するよう要望致します。	御指摘の暗号鍵や証明書のコピー・改ざんに対する対策については各分野において今後検討が必要な事項と考えています。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
212	法人・団体(匿名)A	45	第2章2.4 要点16.	(3)対策例	更新データの正当性確認として電子署名の付与と検証機能を追記するよう要望致します。	御意見を踏まえ、該当箇所を修正いたしました。
213	法人・団体(匿名)A	45	第2章2.4 要点16.	(3)対策例	利用者とシステム・サービスについては、クレデンシャルを利用した認証が述べられていますが、IoT機器のなりすましへの対策については、「IoT機器の識別子による認証を行い」と記述されています。IoT機器の認証においても、機器の識別子だけでなく、何らかのクレデンシャルが必要であるという趣旨の記述に修正を要望致します。	御意見を踏まえ、該当箇所を修正いたしました。
214	次世代ICカードシステム研究会	46	第2章	【運用・保守】	一般利用者・企業利用者は機器性能・サービスのメリットのみに注目し、その背景にある仕組みについてはあまり意識しないと想定されます。 このため、IoTで利用される機器及びサービスについて安全性を簡単に確認することができる表示方法について検討すべきです。 例えば、製造物責任法・消費生活用製品安全法に定める製品安全文化の定着のため、安全確保のための表示に関するガイドラインを各工業会で策定しています。 IoTの想定するインターネット接続及び継続的な情報収集・連携については新しい分野であり、セキュリティに関する安全性が重要な要素と考えます。 そこで、各工業会での自主規定を促すためにも表示方法を検討すべきです。	今後の検討における参考として承ります。
215	次世代ICカードシステム研究会	46	第2章	【運用・保守】	表示機能のないIoT機器やサービスは外部から状況を確認することが困難です。 そこで、例えば接続状態と非接続状態を明示するためのLED表示を実装すること等を推奨すべきです。	対策例として一部の事例のみ記載しています。
216	一般社団法人情報通信ネットワーク産業協会(CIAJ)	46	第2章 2.5節 【運用・保守】		インシデント発生時の対応について 各種のセキュリティ対策はもちろん重要ですが、その実施にもかかわらず、万が一インシデントが発生した場合の対応についても重要と考えます。 インシデント発生時の対応の観点から、「2.5【運用・保守】」において、システムのサービス停止等の直接的被害をいかに最小限として食い止めるか、外部への感染や影響の拡大をいかに防止するか等の観点からインシデント発生時の対応(特に初動対応)について、ガイドラインへの記載を期待します。	御指摘のインシデント発生時の対応については、IoTの用途に応じてインパクトや対処方法が異なることから、第4章に記載のリスク分析に基づく分野別の対策として、各分野において今後検討が必要な事項と考えています。
217	力武健次技術士事務所	47から51ページ	2.5【運用・保守】 指針5 安全安心な状態を維持し、情報発信・共有を行う	●要点17 出荷・リリース後も安全安心な状態を維持する ●要点18 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える	IoT技術を応用した製品は、数年以上の長期間にわたって使われる可能性が高く、同種のIoT技術を応用していない製品と形状や利用形態等が特に変わらないものが多いことを考えれば、これらの製品がIoT技術を利用したことに伴う脆弱性について、製造者はより積極的に明示して利用者に注意喚起を実行しなければならないと考えます。 上記の観点から考えた場合、本ガイドライン案には、IoT技術に対応するソフトウェアを使ったことにより発生し得る脆弱性を考慮したプロダクトライフサイクル(標準使用期間の年数、あるいは年限)の明示についての記述がありません。 これは現在の製造物責任に関する製品への表示を考えた場合不十分であり、「製品の安全性は無期限に維持できない」という観点に立って、プロダクトライフサイクルの明示をガイドラインで義務づける必要があると考えます。具体的には、「使用期限: ～年まで、これ以降の使用はサポートしない」旨を各製品にシールなどで明示すべきです。	御指摘の製品の安全性の維持については重要な課題と認識しており、第4章の法的責任関係において、各分野において今後検討が必要な事項と考えています。
218	一般社団法人日本クラウドセキュリティアインス	47	要点17(3)対策例①	IoT機器のアップデート	アップデートパッケージが正式にメーカーから提供された物で、改ざんされていないことを確認するための方策(電子署名の検証等)を導入することが望ましい。ファームウェア改ざんはすべてのセキュリティを根底から覆す可能性があり、アップデートを考える際には、必ず意識すべきと考える。	御意見を踏まえ、該当箇所を修正いたしました。
219	次世代ICカードシステム研究会	47	要点17	(1)ポイント	IoT機器のセキュリティ上重要なアップデート等は、IoTシステム・サービスの提供者が検討し、適用するとしております。 しかし、機器メーカの関与が必要と想定されることから、関係者とすべきではないでしょうか。	御意見を踏まえ、該当箇所を修正いたしました。
220	法人・団体(匿名)C	47	第2章 2.5 要点17	(3)対策例	1の前に、今のIoT機器の状態(内部ソフトウェアバージョン)をきちんと管理し、IoT機器上のソフトウェアの改編が行われるなどの変化を遠隔でも検知できるような仕組みが必要かと思われます。遠隔から常時状態を認識できる仕組みを用意する、などが対策例になります。	御意見を踏まえ、該当箇所を修正いたしました。
221	法人・団体(匿名)A	47	第2章2.5 要点17.	(3)対策例	IoT機器はPCとは異なり、利用者が自らアップデートを適用するとは限らない(危険な放置状態が続く)と考えます。 そのため、IoT機器においては、アップデートの適用状況を機器メーカーが判別し、危機の度合いによっては強制的に更新する仕組みが必要と考えます。 第3段落末尾に以下の文案を追記するのはいかがでしょうか。 「また、IoT機器の製造者は、各機器のアップデート適用状況の成功、失敗、無適用という状態を適切に把握する仕組みの導入を推奨する。」	御指摘の機器のアップデート適用を管理する仕組みについては、第4章に記載のリスク分析に基づく分野別の対策として、各分野において今後検討が必要な事項と考えています。
222	一般社団法人重要生活機器連携セキュリティ協議会	47	第2章 2.5【運用・保守】 指針5安全安心な状態を維持し、情報発信・共有を行う	要点17. 出荷・リリース後も安全安心な状態を維持する	4)要点17「出荷・リリース後も安全安心な状態を維持する」の項目について IoT機器のアップデートについて記述がありますが、リモートアップデート機能は、攻撃者が機器を乗っ取るために狙う機能であるため、アップデート機能のセキュリティ対策も不可欠であることを補足しておくとよいと考えます。	御指摘のアップデート機能に係る対策は、IoT機器等の用途によって条件や必要性が異なることから、個別に検討が必要な事項と考えています。
223	個人E	48	2.5	(2)解説	「この間、以下のような安全安心上の問題が想定されるため、関係者に守ってもらいたいことを伝える必要がある」とあるが、具体的に何を守ってもらいたいか不明。「この間、以下のような安全安心上の問題が想定される」で良い。	御意見を踏まえ、該当箇所を修正いたしました。
224	一般社団法人電子情報技術産業協会(JEITA)	49	2.5	要点18(3)対策例	PSIRT(Product Security Incident Response Team)の設置等を明記してはどうか。	今後の取組の検討にあたっての参考とさせていただきます。
225	株式会社パソナサイバーラボ	50	要点18. 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える	(3)対策例①②)	P.50 IoTの脆弱性情報の発信について、脆弱性情報の情報集約および発信先機関として、CSIRT、JPCERT、ISACが例示されている。これに加えて、例えば各IoTの業界団体ごとに脆弱性情報を一元的に情報発信する仕組みがあるとよいと思われる。	御指摘の脆弱性情報の集約、発信は重要な課題と捉えおり、第4章のIoTに対する総合セキュリティ対策において、今後検討が必要な事項と考えています。
226	株式会社ラックサイバー・グリッド・ジャパン	51	第2章 2.5 要点18	3)リユース・廃棄時の対策	提案:対策として以下の項目を追加する。 ・記憶メディアを物理的に破壊する。 理由: ・耐タンパ性を考慮するため。 ・ユーザにデータ抹消の分かりやすさを提供するため。 ・廃棄時のユーザの利便性を向上させるため。データの完全消去は時間がかかり、失敗する恐れもある。 参考:データの完全消去はコストがかさむなどマイナスの要素も大きい。製品の分解によるフラッシュメモリの除去破壊のためのコストがかさむ、逆に再利用することによりコストを節減 したい場合は、フラッシュメモリの内容を常時暗号化した状態で運用し、鍵をTPM(Trusted Platform Module)内で管理して、鍵の廃棄により個人情報の消去(注)とみなす方策もある。そのためには、消去とみなされる一定の基準を満たした暗号方式の採用及び鍵管理方法を定める必要がある。 注:個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン(平成26年厚生労働省・経済産業省告示第4号。以下「個人情報法ガイドライン」と略。)2-2-5-4※5において、保有個人データに関し、「「消去」とは、保有個人データを保有個人データとして使えなくすることであり、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等を含む」との解釈指針が示されている。本ガイドライン(案)においては、同法の「保有個人データ」以外についても「個人情報」として言及していることから、個人情報保護法ガイドラインの表現に準じ「個人情報の消去」と記載した。	対策例として一部の事例のみ記載しています。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
227	株式会社ラックサイバー・グリッド・ジャパン	52	第2章 2.5 要点19.	「安全に消去するためのプログラムの利用」	提案:以下のように修正する。 「要点18.(3)③」で例示した完全に消去するためのプログラムの利用 理由:利用者が自身の持つデータ消去ツールを用いてIoTデバイス上の個人情報等を消去するのは極めて困難であることから、要点18で例示されたあらかじめ搭載したプログラムの利用を意図したものと理解するが、「安全に消去」の表現が要点18の例示(完全に消去)と相違し分かり辛いことから、対応関係を明示する。	御意見を踏まえ、該当箇所を修正いたしました。
228	一般社団法人情報処理学会	52	2.5	要点19. つながることによるリスクを一般利用者に知ってもらう	■2.5【運用保守】要点19「つながることによるリスクを一般利用者に知ってもらう」 リスクの一般利用者への周知のところ等で, どのような個人情報が取得され流出する恐れがあるのか理解した上で使ってもらうといった視点の記述が必要ではないでしょうか.	御指摘のどのような個人情報があるかについては分野や用途によって異なることから、その扱いについては今後検討が必要な事項と考えます。
229	一般社団法人電子情報技術産業協会（JEITA）	52	2.5	要点19(3)対策例	IoTが自動的に収集してしまう情報に対する「利用者のプライバシーの考慮」を追記してはどうか。	御指摘のどのような個人情報があるかについては分野や用途によって異なることから、その扱いについては今後検討が必要な事項と考えます。
230	個人E	54	2.5	(3)対策例	具体例に「一定期間内に脆弱性対策を実施しないIoT機器はネットワークから切り離す(ネットワークに接続させない)」を追加する。	御指摘の一定期間内に脆弱性対策を実施しないIoT機器はネットワークから切り離すについては用途によって条件や必要性が異なることから、第4章に記載のリスク分析に基づく分野別の対策として、各分野において今後検討が必要な事項と考えています
231	次世代ICカードシステム研究会	54	要点21	(1)ポイント	機器メーカや機種名が明らかな場合のみ、脆弱性を管理可能です。 海外等で製造され非常に安価な機器の場合にはシリアル番号等による製品管理がされない場合も想定されることから、IoTで利用する機器としては避けるべきことを例示すべきです。	御指摘の製品管理がされない機器については一般利用者のためのルール　1）の記載で御指摘の趣旨が含まれているものと考えます。
232	株式会社ラックサイバー・グリッド・ジャパン	54	第2章 2.5 要点21.	要点21.全体、特に(3)	提案:要点21.全体、少なくとも(3)対策例を削除し、当該事項は今後の検討事項として第4章に移す。 理由: 現状「(3)対策例」として示されている例は、次のとおりいずれも問題があり、今後継続して検討を行う必要がある。 《問題点》 ・①について、一般利用者の特定といっても、IPアドレスや位置情報(ただし、あらかじめ利用者の明示の同意を要する。)しか把握できず、対策を求めるのに必要な住所、電話番号、メールアドレス等の把握については、なお整理すべき課題がある。 ・②について、テレコムアイザック推進会議が https://www.telecom-isac.jp/news/news20130830.htmlなどで公表した対策を下敷きにしていると考えられるが、このような対策をとる前に供給者が取り組むべき事項、対策の着手時機及び費用負担について議論しないと、実効的に機能しにくいものと考えられる。 また、JPCERT/CCによる注意喚起は既に行われているが、一般利用者に対する効果としては供給者自身による注意喚起を超えるものではない。	御意見を踏まえ、該当箇所を修正いたしました。
233	一般社団法人情報通信ネットワーク産業協会(CIAJ)	56	第3章 一般利用者のルール		インシデント発生時の対応について また、「第3章　一般利用者のルール」の章にも、インシデント発生時にあわてないために、発生例等を基にして、望ましい対応事例を記載していただけると、一般利用者も本ガイドラインをより広く活用できるものと考えます。	一般利用者の理解がより深まるものとなる様、今後の検討における参考といたします。
234	一般社団法人情報処理学会	56	第3章		＜第3章＞ IoT機器・システム・サービスの利用における, 安全性とセキュリティを確保するためには, 利用者自身による対策が必要不可欠だと考えます. IoT機器が収集する情報は, 各種センサデータなど多岐にわたり, また, 利用者が自発的に入力するとは限らないものが多いと想定されます. どのようなデータが収集され, また蓄積もしくは利用されるかについて, 個人情報保護(適切な個人情報の取得)の原則からも, 利用者(機器の所有者と限らない可能性があります)に適切に認識してもらえるようにする必要があります. また, IoT機器・システムの利用者に対しても, リスクから身を守るための原則として, その機器・システムにおいて適切な情報の収集・管理がなされているかを積極的に確認するように第3章(一般利用者のためのルール)などで啓発することが重要と考えます. そこで以下のルールを追加することを検討願います. ・「使用機器, サービスの最新情報を把握し, 必要に応じて使用機器やサービスの保守を実施する」	今後の検討における参考として承ります。
235	一般社団法人情報処理学会	56	第3章		・「使用機器, サービスに関して, サービス提供者による接続の目的・意図を把握し, 理解できない機能やサービスの利用を控える」 →要点18～21との対応. 特に要点18(3)②における重要事項説明等に追記するのはいかがでしょうか.	機能を理解した上で利用することが重要と考えており、利用上の注意等を説明するよう記載しています。
236	一般社団法人情報処理学会	56	第3章		・「利用者自身による物理的なセキュリティへの対策（注意喚起）」 →第3章に, 利用者自身が, IoT機器の管理, 保有の重要性を理解し, 個人情報(プライバシ情報を含む)場合には, その管理に十分気をつける(盗難や転売の防止)ことを追加するのはいかがでしょうか.	盗難や転売等を含めた御指摘の趣旨はルール4に含まれていると考えます。
237	一般社団法人情報処理学会	56	第3章		・「利用者自身による機能・設定の見直し」 →第3章 要点19の内容を受けて, 利用者自身が, 「必要な機能とそのリスクを把握し, 機能・設定を定期的にチェックする」という事項を追加するのが望ましいと考えます.	今後の検討における参考として承ります。
238	一般社団法人情報処理学会	56	第3章		・「利用者自身によるサービス提供者への攻撃の防止（注意喚起）」の追加 →第3章に, 利用者自身によるIoT機器の悪用, サービス提供者への攻撃を防止するための注意喚起を追加してはどうか. 他の利用者にも悪影響を及ぼす可能性が考えられます.	今後の検討における参考として承ります。
239	個人D	56	3章	（※1）：IoTとは	IoTの定義は、1.3.1に記載しているため、注釈は不要である。注釈を削除するか、1.3.1を参照すべきである。	一般利用者が第3章のみを閲覧する可能性を考慮して、記載しています。
240	株式会社パソナサイバーラボ	57	第3章 一般利用者のためのルール		P.57 一般利用者のためのルールの項目で、「使用中の機器やサービス」のルールも必要と思われる。一般ユーザの場合、使用している機器がIoTに該当することすら意識していない場合もあると思われる。一般利用者から見て、どのような機器・サービスが本ガイドラインのIoTセキュリティの範囲に該当するかを網羅的に識別できるリストがあるとよいと思われる。	今後の検討における参考として承ります。
241	株式会社パソナサイバーラボ	57	第3章 一般利用者のためのルール	ルール4)機器を手放すときはデータを消す	P.57 ルール4)で、一般利用者は「機器を手放すときはデータを消す」の裏返しで、供給者側及び機器メーカ側においては、一般利用者側でのデータ削除により「データの復元が不可能な仕組み」の導入を検討するとよいと思われる。(P.25 不正な読み出しの想定例に関連)データ消去により、不可逆的にデータの復元が不能となる、という安心感を担保できたほうがよいと思われる。	要点18に完全に消去する機能を搭載することを記載しております。
242	三菱電機インフォメーションシステムズ株式会社	57	第3章 一般利用者のためのルール		ルール5：収集されるデータを確認する：IoTサービス提供会社が運用中に利用者から収集する情報が何であるかを確認し、了解した上でIoT機器を接続する。 知られたくないプライバシー情報が、IoT機器を通して、勝手に収集されないように気をつける必要があるのではないでしょうか。	御指摘の利用者のプライバシーについては、4章のIoT時代のデータ管理の在り方に記載のとおり、用途に応じて、各分野において今後の課題として検討されるべきものであると考えます。
243	三菱電機インフォメーションシステムズ株式会社	57	第3章 一般利用者のためのルール		ルール6：接続不可になったIoT機器は電源を切る 今まで接続していたIoT機器が突然接続できなくなっていたら、故障と決めつけずに、外部からのアクセスで遠隔操作されている可能性も疑って電源は切るべきと考えられる。 電源を入れたままにしておくと、内部不正の犯罪にそのIoT機器が利用されてしまうのではないでしょうか。	御意見を踏まえ、該当箇所を修正いたしました。

No.	提出者	ページ	項目	該当部分	案に対する意見	考え方
244	個人B	57	第3章 一般利用者のためのルール		<一般利用者のためのルール> ・「情報を確実に削除する」とあるが、フォーマットなど一般的にデータ削除と呼ばれる動作をしただけではデータは復元可能であることの明記をした上で、復元不可能なデータの削除方法を記載するべきだと考えます <該当部分> p57:「ルール4）機器を手放す時はデータを消す」	要点18、19に完全に消去する機能の搭載、利用について記載しており、御指摘の趣旨は含まれていると考えます。
245	次世代ICカードシステム研究会	57	第3章	ルール4）	「機器を手放すときはデータを消す。」と単純に書いてありますが難しいことです。 具体的に、例えば工場出荷時に戻す機能、ICカードを抜けば完全にデータ消去ができる方式などを提供すべきことを例示すべきです。	要点18、19に完全に消去する機能の搭載、利用について記載しており、御指摘の趣旨は含まれていると考えます。
246	株式会社ラックサイバー・グリッド・ジャパン	58	第4章		提案:具体的な検討事項として4点挙げられているが、さらに次の3点の追加を提案する。 ・国際的な調和とセキュリティ意識の向上 IoTは、国境を越えて流通・利用されていることから、日本政府や国内関係者だけでセキュリティを向上させることにはおのずから限界がある。 本ガイドラインの発展に合わせ、国際標準化を含む調和と世界的なセキュリティ意識の向上を図っていくことが望まれる。 ・プライバシーの保護基準の検討 プライバシーの保護について、現状、国・地域により様々な検討が進められているところである。 厳格な基準を策定し、それを遵守する方が、利用者が安心して利用でき普及が進むことも踏まえ、各国との整合を図りながら世界をリードする基準を検討していく必要がある。 ・リバースエンジニアリングへの対応の検討 ファームウェアを改ざんされたり不正ファームウェアを構成されたりする可能性もある。 そのため、ファームウェアを難読化するなどの対策もある反面、オープンソフトウェアライセンスで開発されるものも多く、それぞれ適切な対応が必要である。 このような問題にどう対応するのか、今後検討しなければならない。	御指摘の国際的な調和やプライバシー、リバースエンジニアリングへの対応は各点とも重要な課題と認識しておりますが、前2点は第4章に記載の法的責任関係やIoT時代のデータ管理の在り方において、3点目はリスク分析に基づく分野別の対策として、御指摘の点も踏まえ、各分野において今後検討が必要と考えております。
247	一般社団法人電子情報技術産業協会（JEITA）	58	今後の検討課題		1）本ガイドラインの対策網羅性についての検証、不足部分の補強も課題ではないか。 例えば、NIST（The National Institute of Standards and Technology)のサイバーセキュリティフレームワークとの比較等も有効と思う。 2）法的責任関係において、業法との整合性を図るためのスキームの方針明確化も検討願いたい。 例えば、医療機器では医薬品医療機器法があり、サイバーセキュリティ関連の規制が重畳しない、矛盾しないことが必要である。 3）IoTは国内だけではなく、海外も関係する。 日本以外の関連規制や、その内容と本ガイドラインの関係などを示したり、日本からそれらに働きかける方針等も示したりしてはどうか。	(1)対策例として一部の事例のみ記載しています。 (2)御指摘の点は、4章の法的責任となっており、今後の検討が必要な事項として考えています。また、「矛盾しないことが必要である」との御指摘は、第2章で「既存の安全確保や性能に関する法令・規制要求事項が存在している分野については、それらを順守することが大前提である」と記載していることか考慮しております。 (3)今後の取組の検討にあたっての参考にさせていただきます。
248	法人・団体（匿名）A	58	第4章	IoT時代のデータ管理の在り方について	個人情報に関しては、適切な取得と利用・廃棄が重要と考えます。「データを取得・保持・管理・利用・廃棄する者」 および 「適切に取得・保持・管理・利用・廃棄すること」 と記載すべきと考えます。	御意見を踏まえ、該当箇所を修正いたしました。
249	法人・団体（匿名）A	58	第4章	IoT時代のデータ管理の在り方について	取得した個人情報などは取得から廃棄まで、データのライフサイクルの観点で検討する必要があると考えます。「その具体的な方法について、データの取得から廃棄に至るライフサイクルの観点で、検討していく必要がある。」 と記載すべきと考えます。	
250	NPO日本ネットワークセキュリティ協会	58	第4章		1.第4章今後の検討課題について (1)IoT時代のデータ管理の在り方について（P58） 意見：「個人情報や技術情報など重要データを適切に保持・管理～その具体的な方法について検討必要」とあるが、「重要データ」「重要な機能」をどう決めるのか、という検討が必要である。 理由：ガイドライン案の中で「重要」といった用語が散見されるが、「例示」だけが存在し定義がわからない。 ・重要な情報（例えば個人の生活データ、工場のデバイスから得た生産情報等）（P5） ・ 守るべきものの重要度に応じたセキュリティ対策 （P30） ・重要な機能を多重のゲートウェイにより守ることが可能（P30） ・サーバ送信することで機器本体に重要情報を残さない方法（P30） ・つながる相手が相応の権限を有する機器と確認できた場合のみ重要な機能を利用(P36) ・重要なアップデート（P47） ・セキュリティに関する重要な事項（P48） IoTに関わるどのステークホルダーの視点で重要性を考えるかによって、「重要」の意味が異なってくる可能性がある。 (2)法的責任関係について 意見：個人情報については「改正個人情報保護法」との関連性を含めた検討が必要である。 理由：法的責任といった場合に、技術的な視点だけのガイドだけでは判断がしにくい。	御指摘の「重要」の考え方については、IoTに関わる関係者の立場によって捉え方が異なるため、本ガイドラインでは例示を記載しているものであり、具体的に重要なデータ等の内容については、用途等に応じて各分野において個別に検討されるものと考えております。 また、法的責任関係は、個人情報保護法を含め既存の法律等を十分に考慮した上で各分野において今後検討が必要な事項と考えております。
251	一般社団法人重要生活機器連携セキュリティ協議会	58	第4章 今後の検討事項		5）今後の検討事項について 指針2や今後の検討事項にも記載されている通り、リスク評価は必要であり、また業種、分野毎にそのリスク評価の内容は異なっているので、さらなる検討が必要と思われます。 メーカ、サービス側で対応が必要なのは、脅威分析からリスク評価をした後、その対策にかかる費用と得られる効果を吟味することかと思います。 そこで、今後の課題において「費用対効果を検討できるような指標の検討も必要である」という点を加えて頂ければと思います。 例： 「脅威分析からリスク評価をした後、その対策にかかる費用と得られる効果を吟味するための手法や指標についての検討も必要がある」	御指摘の対策にかかる費用と効果については第4章の法的責任関係について記載のとおり、費用負担の観点も含めて今後検討が必要な事項と考えます。
252	匿名B	60	用語集	IoT	60ページ目の付録の用語集を拝見させていただいたところ。 IoTの意味が「モノのインターネット」と出来の悪い翻訳ツールを通したとしか思えない、お粗末な説明になっています。 書き手としては付録でしょうが、題名にもなっていますし、あれだけ「IoT」と連呼されていると、意味が分からないと思った賢い読み手はまず確認するのではないでしょうか？	御意見を踏まえ、該当箇所を修正いたしました。