資料３

政府機関等のサイバーセキュリティ対策のための統一基準群の改定に伴う対応

総 務 省

令和６年11月27日

総務省自治行政局

デジタル基盤推進室

「政府機関等の対策基準策定のためのガイドライン」の一部改定（令和６年７月）

✓ 政府機関等のサイバーセキュリティ対策のための統一基準群（政府統一基準群）の１つである、政府機関等の対策基準策定のためのガイドライン（以下「政府機関等策定ガイドライン」という。）の改定をガイドラインに反映する。

１．情報セキュリティに関するサプライチェーン・リスク対策の強化

２．IoT機器等に対するセキュリティ対策の強化

３．ソフトウェアコンポーネントの管理、脆弱性管理の強化

４．要管理対策区域外での端末利用時の対策の強化

５．BYOD対策の強化

６．電子メール不正中継対策の強化

１．情報セキュリティに関するサプライチェーン・リスク対策の強化

１．情報セキュリティに関するサプライチェーン・リスク対策の強化

➢ **適正なかつ透明性のある手続(例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で、外国の法執行機関の命令により、データセンター内のデータやクラウドサービス内の情報が強制的に開示されるといったリスクについて明記する形にしてはいかがか。**

政府機関等策定ガイドライン（解説）　（赤字が改定部分）

基本対策事項4.1.2(4)-2
「国内法以外の法令及び規制が適用されるリスク」について

国内法以外の法令及び規制が適用されるリスクとして、**適正なかつ透明性のある手続(例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で**データセンター内のデータが外国の法執行機関の命令により強制的に開示される**といったリスクがあると判断される場合には留意が必要である。**

遵守事項4.2.1(2)(b)(イ)
「情報が保存される国・地域」について

クラウドサービスの利用においては、利用するクラウドサービスの形態及び仕様によって情報が保存される国や地域を指定することができるものもある。また、定型約款等において情報の保存される国や地域が指定されているサービスも存在する。そのため、クラウドサービスで取り扱う情報を保存できる国や地域を事前に定めておく必要がある。**適切なかつ透明性のある手続き(例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で**クラウドサービス内の情報が外国の法執行機関の命令により強制的に開示される**といったリスクがあると判断される場合には留意が必要である。**なお、準拠法・裁判管轄を指定しても情報の開示が懸念される場合は、機関等の管理する暗号鍵で情報を暗号化するなどの措置を検討するとよい。ただし、この場合において、暗号鍵管理にクラウドサービス等を利用する場合には暗号鍵に係る情報が保存される国や地域にも注意が必要である。

改定案：対策基準（解説）

8.1.業務委託
(1)業務委託に係る運用規程の整備

①「委託判断基準」について
委託事業者に許可されていない情報の提供が行われないように、委託事業者に提供する情報に関する地方公共団体の基準を規定することを求めている。規定すべき内容としては、例えば以下の事項が考えられる。
・業務委託を許可（又は禁止）する業務の範囲（委託事業者に開示できない情報を取り扱う業務は業務委託不可等）
・業務委託への提供を許可（又は禁止）する情報の範囲（委託業務に関係しない情報は提供不可等）
・情報資産の分類及び取扱制限その他提供する情報の特性に応じた、情報の取扱いを許可（又は禁止）する場所（自治体機密性３情報は要管理対策区域外での取扱いを禁止するなど）
特に、委託業務で取り扱われる情報に対して国外の法令等が適用される場合があり、国内であれば不適切と判断されるアクセス等が行われる可能性があることに注意が必要である。**具体的には、適切なかつ透明性のある手続(例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で、外国の法執行機関の命令により、データセンター内のデータが強制的に開示されるといったリスクがあると判断される場合には留意が必要である。**

１．情報セキュリティに関するサプライチェーン・リスク対策の強化

- **適正なかつ透明性のある手続(例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で、外国の法執行機関の命令により、クラウドサービス内の情報が強制的に開示されるといったリスクについて明記する形にしてはいかがか。**
- **構成員の意見を踏まえ、基本的に政府統一基準群に記載を合せることとし、重複する内容に係る記載については削除する。**

政府機関等策定ガイドライン（解説）　（赤字が改定部分）

遵守事項4.2.1(2)(b)(イ)
「情報が保存される国・地域」について

クラウドサービスの利用においては、利用するクラウドサービスの形態及び仕様によって情報が保存される国や地域を指定することができるものもある。また、定型約款等において情報の保存される国や地域が指定されているサービスも存在する。そのため、クラウドサービスで取り扱う情報を保存できる国や地域を事前に定めておく必要がある。**適切なかつ透明性のある手続き(例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形でクラウドサービス内の情報が外国の法執行機関の命令により強制的に開示されるといったリスクがあると判断される場合には留意が必要である。**なお、準拠法・裁判管轄を指定しても情報の開示が懸念される場合は、機関等の管理する暗号鍵で情報を暗号化するなどの措置を検討するとよい。ただし、この場合において、暗号鍵管理にクラウドサービス等を利用する場合には暗号鍵に係る情報が保存される国や地域にも注意が必要である。

改定案：対策基準（解説）

8.3.外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱う場合）
(3)クラウドサービスの選定

②インターネットを介して提供されるクラウドサービスの利用に当たっては、クラウドサービス提供者の事業所の場所にかかわらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、（「クラウドサービス～必要がある。」までを削除）**適正なかつ透明性のある手続(例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形でクラウドサービス内の情報が外国の法執行機関の命令により強制的に開示されるといったリスクがあると判断される場合には留意が必要である。クラウドサービスの利用においては、利用するクラウドサービスの形態及び仕様によって情報が保存される国や地域を指定することができるものもある。また、定型約款等において情報の保存される国や地域が指定されているサービスも存在する。そのため、クラウドサービスで取り扱う情報を保存できる国や地域を事前に定めておく必要がある。なお、準拠法・裁判管轄を指定しても情報の開示が懸念される場合は、地方公共団体の管理する暗号鍵で情報を暗号化するなどの措置を検討するとよい。ただし、この場合において、暗号鍵管理にクラウドサービス等を利用する場合には暗号鍵に係る情報が保存される国や地域にも注意が必要である。**
（「また、外国に～十分に留意が必要となる。」までを削除）

１．情報セキュリティに関するサプライチェーン・リスク対策の強化

➢ **暗号鍵の保管場所についても、適正なかつ透明性のある手続(例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で、外国の法執行機関の命令により、強制的に開示されるといったリスクについて明記する形にしてはいかがか。**

政府機関等策定ガイドライン（解説）　（赤字が改定部分）

基本対策事項4.2.2(2)-6 c)
「暗号化に用いる鍵の保管場所等の管理」について

基本対策事項4.2.2(1)-9 a)において定めている運用規程に基づき、クラウドサービス管理者は、情報の暗号化に用いる鍵の保管場所に関するセキュリティ要件を定める必要がある。例えば、暗号鍵の保管場所については、暗号化した情報とは別の場所で管理することや、**適正なかつ透明性のある手続き（例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で暗号鍵が外国の法執行機関の命令により強制的に開示されるといったリスクがあると判断される場所**には保管しないなどが考えられる。暗号鍵の管理については、基本対策事項7.1.5(1)-3 b)「管理手順を定めること」を参照するとよい。

改定案：対策基準（解説）

8.3.外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱う場合）
(7)クラウドサービスを利用した情報システムの運用・保守時の対策

①（オ）統括情報セキュリティ責任者は、運用・保守時における暗号化に係る規定を策定する場合、以下を含む内容を規定すること。
・暗号化に用いる鍵の管理者と鍵の保管場所（暗号化した情報とは別の場所で暗号鍵を管理すること）
（イ）鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価
・鍵管理機能をクラウドサービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価
・適正なかつ透明性のある手続（例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で暗号鍵が外国の法執行機関の命令により強制的に開示されるといったリスク

１．情報セキュリティに関するサプライチェーン・リスク対策の強化

➢ **機器等の調達において考慮すべきリスクを、詳細に記載してはいかがか。**

政府機関等策定ガイドライン（解説）　（赤字が改定部分）

遵守事項4.3.1(1)(α)
「不正な変更が加えられない」について

機関等は、機器等の開発や製造過程において、情報の窃取・破壊や情報システムの停止等の悪意ある機能が組み込まれるサプライチェーン・リスクの懸念が払拭できない機器等を調達しないようにする必要があり、機器等の調達において、考慮すべきリスクとして以下のようなものがある。統括情報セキュリティ責任者は、以下を例とするリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、調達の可否を決定する必要がある。

・機器等を開発・供給する事業者やそのサプライヤー・委託先事業者（再委託先事業者等を含む）、及び当該機器等の設置や保守等の役務を提供する事業者やその委託先事業者（再委託先事業者等を含む）について、当該事業者等の本社等（当該事業者等の総株主等の議決権の過半数を直接又は間接に保有する者の本社等を含む）の立地する場所の法的環境や外部主体の指示等により、当該機器等に係る開発・供給又は役務の提供等の適切性が影響を受け、これにより悪意ある機能や不正な変更が機器等に組み込まれる又は当該機器等が取り扱う情報が窃取・破壊される等のリスク

このサプライチェーン・リスクに対応する方法として、機関等が、国内外の情報セキュリティに関する情報を収集し、こうした知見をもとにサプライチェーン・リスクを当該調達に関する要件の一つとして取り上げることにより、開発・製造過程において悪意ある機能が組み込まれる懸念が払拭できない機器等、及びサプライチェーン・リスクに係る懸念が払拭できない企業の機器等を調達しないことが求められる。

改定案：対策基準（解説）

6.3.システム開発、導入、保守等
（１）　機器等の調達に係る運用規程の整備

①「機器等の選定基準」について
（前略）
また、地方公共団体は、機器等の開発や製造過程において、情報の窃取・破壊や情報システムの停止等の悪意ある機能が組み込まれるサプライチェーン・リスクの懸念が払拭できない機器等を調達しないようにする必要があり、機器等の調達において、考慮すべきリスクとして以下のようなものがある。統括情報セキュリティ責任者は、以下を例とするリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、調達の可否を決定する必要がある。

・機器等を開発・供給する事業者やそのサプライヤー・委託先事業者（再委託先事業者等を含む）、及び当該機器等の設置や保守等の役務を提供する事業者やその委託先事業者（再委託先事業者等を含む）について、当該事業者等の本社等（当該事業者等の総株主等の議決権の過半数を直接又は間接に保有する者の本社等を含む）の立地する場所の法的環境や外部主体の指示等により、当該機器等に係る開発・供給又は役務の提供等の適切性が影響を受け、これにより悪意ある機能や不正な変更が機器等に組み込まれる又は当該機器等が取り扱う情報が窃取・破壊される等のリスク

このサプライチェーン・リスクに対応する方法として、地方公共団体が、国内外の情報セキュリティに関する情報を収集し、こうした知見をもとにサプライチェーン・リスクを当該調達に関する要件の一つとして取り上げることにより、開発・製造過程において悪意ある機能が組み込まれる懸念が払拭できない機器等、及びサプライチェーン・リスクに係る懸念が払拭できない企業の機器等を調達しないことが求められる。

２．IoT機器等に対するセキュリティ対策の強化

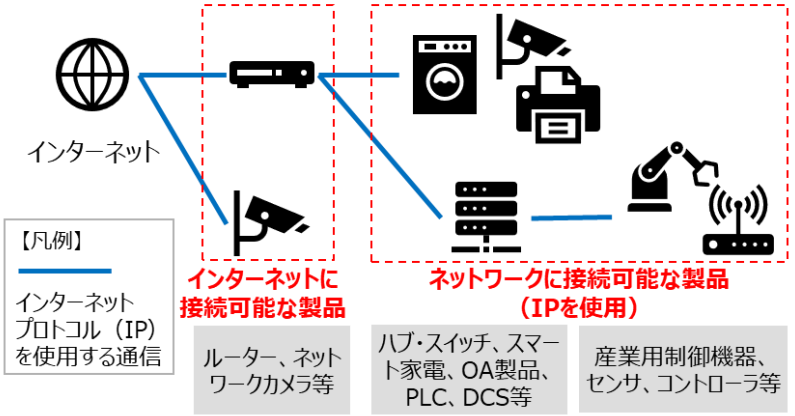
（参考）IoTセキュリティ適合性評価制度　※前回検討会提示

✓ **ルータ、ハブ・スイッチ、監視カメラ等**、インターネットに直接的又は間接的に接続される製品が対象となる。

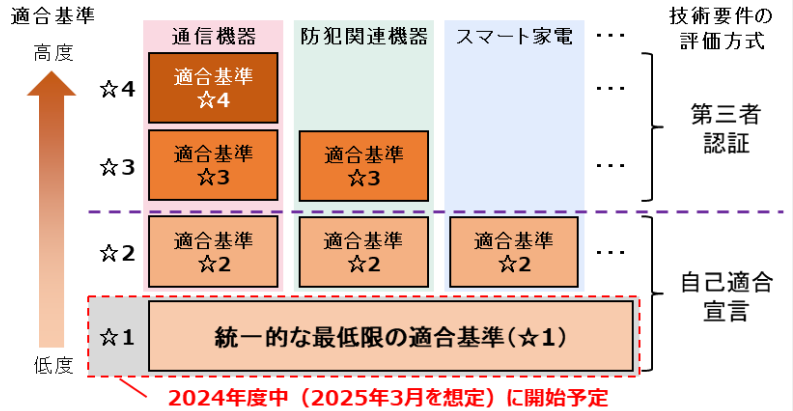
IoTセキュリティ適合性評価制度の概要

- IoT製品の脆弱性を狙ったサイバー脅威が高まっていることを踏まえ、経済産業省にて、IoTセキュリティ適合性評価制度を構築中。2024年3月～４月に制度構築方針（案）のパブリックコメントを実施。パブリックコメントを踏まえた**最終制度構築方針(※1)を8月23日に公表**。
- インターネットに直接的又は間接的に接続されるIoT製品を対象とし、複数のレベル（☆1～4）を用いた任意制度を構築予定。まずは、**全ての対象製品の統一的な最低限の基準（☆１）について、2024年度末（2025年3月頃）に受付を開始**予定。IoT製品類型ごとの特徴に応じた基準（☆2～☆4）については、順次策定予定。
- G7各国を中心に、諸外国においても同様のIoT製品の適合性評価制度の検討が進んでいる。IoT製品ベンダーの負担を抑えるため、**米国やEUの当局と相互承認に向けた議論を実施中**。

対象製品の概要(※2)



適合性評価レベル（☆1～☆4）のイメージ



レベル	位置付け	適合基準	技術要件の評価方式
☆3以上	**政府機関等や重要インフラ事業者、大企業の重要なシステムでの利用を想定**したIoT製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを**独立した第三者が評価して示す**もの	製品類型別	第三者認証
☆2	**IoT製品類型ごとの特徴を考慮**し、☆1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型別	自己適合宣言
☆1	IoT製品として共通して求められる**最低限のセキュリティ要件**を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型共通	自己適合宣言

(※1)経済産業省, IoT製品に対するセキュリティ適合性評価制度構築方針 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html
(※2)国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外

(経済産業省資料)

2. IoT機器等に対するセキュリティ対策の強化

➢ **政府機関等策定ガイドラインを参考に、機器等の調達についての解説部分にIoT機器等に必要な機能等について追記してはいかがか。**

政府機関等策定ガイドライン

（新設）

基本対策事項
＜4.3.1(1)(a)関連＞
4.3.1(1)-2統括情報セキュリティ責任者は、機器等の選定基準に、機器等に必要なセキュリティ機能が適切に実装されていることを含めること。

（解説）
基本対策事項4.3.1(1)-2
「必要なセキュリティ機能が適切に実装されていること」について

必要なセキュリティ対策を実施するためには、機器等に必要なセキュリティ機能が適切に実装されていることが求められる。例えば、IoT機器等に必要なセキュリティ機能の具体例としては、少なくとも以下の内容が考えられる。
・容易に推測可能な初期パスワードの設定禁止
・主体認証のネットワークを介した総当たり攻撃対策
・容易に行えるソフトウェアの脆弱性対策（アップデート等）
・機器内のセキュリティパラメータの保護
・安全な通信の確保
・利用者が作成したデータの容易な消去
・利用しない機能や通信ポートの無効化

機器等に必要な情報セキュリティ対策が適切に実装されていることを確認するには、機器等の仕様書の確認、製造者へのヒアリングの実施のほか、次の「IoT製品のセキュリティ適合性評価制度」の活用が考えられる。
（続く）

改定案：対策基準（解説）　（赤字が追記部分）

6.3. システム開発、導入、保守等
(２) 機器等及び情報システムの調達
　機器等及び情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、機器等及び情報システムのライフサイクルで必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。（略）
（注１）情報機器及びソフトウェア等の情報セキュリティ機能の評価に当たっては（略）独立行政法人情報処理推進機構のサイトを参照のこと。
　さらに、必要なセキュリティ対策を実施するためには、機器等に必要なセキュリティ機能が適切に実装されていることが求められる。例えば、IoT機器等（通信回線装置、特定用途機器、複合機等）に必要なセキュリティ機能の具体例としては、少なくとも以下の内容が考えられる。

IoT機器等の範囲について、「IoT製品に対するセキュリティ適合性評価制度構築方針」を参考に補足

・容易に推測可能な初期パスワードの設定禁止
・主体認証のネットワークを介した総当たり攻撃対策
・容易に行えるソフトウェアの脆弱性対策（アップデート等）
・機器内のセキュリティパラメータの保護
・安全な通信の確保
・利用者が作成したデータの容易な消去
・利用しない機能や通信ポートの無効化

　機器等に必要な情報セキュリティ対策が適切に実装されていることを確認するには、機器等の仕様書の確認、製造者へのヒアリングの実施のほか、「IoT製品に対するセキュリティ適合性評価制度構築方針」（令和６年８月経済産業省 商務情報政策局サイバーセキュリティ課）に基づき構築された制度の活用が考えられる。
（続く）

2．IoT機器等に対するセキュリティ対策の強化

- **政府機関等策定ガイドラインや「IoT製品に対するセキュリティ適合性評価制度構築方針」、最新の情報が掲載されている独立行政法人情報処理推進機構（IPA）のウェブサイト等を参考に追記してはいかがか。**
- **今年度は「IoT製品に対するセキュリティ適合性評価制度」の★１のラベル付与が開始予定であることを踏まえ、まずは★１について規定することとし、★２以上は制度整備の状況を踏まえ次年度以降に追記を検討してはいかがか。**

政府機関等策定ガイドライン

（続き）

IoT 機器等に対する要求すべきセキュリティ要件に関連して、2024 年度中（2025 年３月頃）に「IoT 製品に対するセキュリティ適合性評価制度」の☆１のラベル付与が開始される予定であり、今後の調達における活用が考えられる。☆１は機器等共通の最低限満たすべきセキュリティ項目を満たしていることを製造業者が自己で評価し、その適合性を宣言することで取得可能となるものである。☆１の取得を確認することで、上記に記載しているセキュリティ機能の実装状況の確認の代用とすることができる。

また同制度では、製品種別毎により高度なセキュリティ適合基準に対する評価を行う☆２（自己適合宣言）、☆３以上（第三者認証）が順次整備される予定である。制度整備の状況を踏まえつつ、2025 年度中に同制度の☆１以上を取得していることを機器等の選定基準に含めるとともに、以降も、☆２、☆３以上の対象機器の拡充に応じて選定基準への反映を順次行っていく予定である。

情報システムの重要度に応じて「重要度：低」は☆１以上、「重要度：高～中」は少なくとも☆３以上の IoT 機器等を各機関等の選定基準に含めることの追加を検討している。なお、ラベル付与製品が普及する時期をめどに、政府機関等では求めるセキュリティ水準に応じたラベル付与製品の調達を必須化する方針である。

制度の整備状況を踏まえ次年度以降追記を検討

改定案：対策基準（解説）　（赤字が追記部分）

（略）「IoT製品に対するセキュリティ適合性評価制度構築方針」（令和６年８月経済産業省 商務情報政策局サイバーセキュリティ課）に基づき構築された制度の活用が考えられる。セキュリティ要件適合評価及びラベリング制度（JC-STAR）は、「IoT製品に対するセキュリティ適合性評価制度構築方針」に基づき構築された制度で、独立行政法人情報処理推進機構が運営している。

独立行政法人情報処理推進機構ウェブサイトに記載（次ページ参照）

例えば、IoT機器等の調達時に★１（IoT製品共通の最低限満たすべきセキュリティ項目）の取得を確認することで、上記に記載しているセキュリティ機能の実装状況を確認することが考えられる。ただし、あくまでも最低限満たすべきセキュリティ項目であることを鑑み、機器の用途や重要度によっては、個別のセキュリティ要件への対応を確認することも必要である。

- 読みやすさの観点から、「確認の代用」ではなく、単に「確認」と記載
- ★１が、あくまでも「最低限満たすべきセキュリティ項目」であることを踏まえ、場合によって個別のセキュリティ要件への適用を確認する必要性が生じることも追記（重要度の高い機器を調達する場合など）

参考：経済産業省「IoT製品のセキュリティ適合性評価制度構築方針」（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html）

参考：独立行政法人情報処理推進機構ウェブサイト「セキュリティラベリング制度（JC-STAR）についての詳細情報」（https://www.ipa.go.jp/security/jc-star/detail.html）

（続く）

2. IoT機器等に対するセキュリティ対策の強化

➢ **「IoT製品のセキュリティ適合性評価制度」については、最新の情報が掲載されている独立行政法人情報処理推進機構（IPA）のウェブサイトの記載を紹介する形で規定してはいかがか。**

独立行政法人情報処理推進機構ウェブサイト
（https://www.ipa.go.jp/security/jc-star/detail.html）

セキュリティラベリング制度（JC-STAR）についての詳細情報

（略）**本制度は2024年8月に経済産業省が公表した「IoT製品に対するセキュリティ適合性評価制度構築方針」に基づき構築された制度で、IPAが運営しています。**（略）

セキュリティ要件適合評価及びラベリング制度（JC-STAR）
★1 レベル適合基準・評価手法（令和６年９月独立行政法人情報処理推進機構）

1.1 適合ラベルとは

適合ラベルとは、定められた適合基準や評価ガイドに従い、その適合基準が想定する脅威に対抗するために IoT 製品のセキュリティ機能として最低限満たしてほしい水準を達しています。（略）

なお、適合ラベルの取得・維持に際して以下の点に留意すること。

- **定められた適合基準に適合していることを示すものであって、完全・完璧なセキュリティが確保されていることを保証するものではない。**
- **★1、★2 は、IoT 製品ベンダーが本制度で定められた適合基準・評価手順により自己評価を行った結果を記載したチェックリストに基づき、IPA が適合ラベルを付与する自己適合宣言方式である。適合ラベル交付時に定められた適合基準に適合しているかを IPA は確認しない。つまり、評価の信頼性はベンダーの信頼性に依存することになる。**
- **★3、★4 は、政府機関等や重要インフラ事業者等向け製品を想定し、独立した第三者評価機関による評価報告書に基づき、IPA が認証・適合ラベルを付与することでより高い信頼性を確保する。**
- **証跡の保管義務を、IoT 製造ベンダーに課す。**

改定案：対策基準（解説）　**（赤字が追記部分）**

（続き）

＜参考：セキュリティ要件適合評価及びラベリング制度（JC-STAR）における適合ラベル＞

独立行政法人情報処理推進機構は、JC-STARにおける適合ラベルについて、以下の点に留意するよう示している。

- **定められた適合基準に適合していることを示すものであって、完全・完璧なセキュリティが確保されていることを保証するものではない。**
- **★1、★2 は、IoT 製品ベンダーが本制度で定められた適合基準・評価手順により自己評価を行った結果を記載したチェックリストに基づき、IPA が適合ラベルを付与する自己適合宣言方式である。適合ラベル交付時に定められた適合基準に適合しているかを IPA は確認しない。つまり、評価の信頼性はベンダの信頼性に依存することになる。**
- **★3、★4 は、政府機関等や重要インフラ事業者等向け製品を想定し、独立した第三者評価機関による評価報告書に基づき、IPA が認証・適合ラベルを付与することでより高い信頼性を確保する。**
- **証跡の保管義務を、IoT 製品ベンダーに課す。**

※参考文書
『セキュリティ要件適合評価及びラベリング制度（JC-STAR）★1レベル適合基準・評価手法（令和６年９月）』
https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/begoj90000004zgc-att/star1_requirements.pdf

2. IoT機器等に対するセキュリティ対策の強化

- **IoT機器について触れられている特定用途機器に係る規定からも「IoT製品に対するセキュリティ適合性評価制度」を参照できるように、注書きに追記してはいかがか。**

改定案：対策基準（解説）　（赤字が追記部分）

6.1.コンピュータ及びネットワークの管理
(12) IoT機器を含む特定用途機器のセキュリティ管理
　テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続する機能を備えている又は内蔵電磁的記録媒体を備えているものを「特定用途機器」という。（略）
（注９）IoT機器に関するセキュリティ対策については、「IoTセキュリティガイドライン ver 1.0」（平成28年7月　IoT推進コンソーシアム 総務省 経済産業省）を参照されたい。
（注10）特定用途機器の選定、調達時における「IoT製品に対するセキュリティ適合性評価制度構築方針」（令和６年８月経済産業省商務情報政策局サイバーセキュリティ課）に基づき構築された制度の活用については、6.3. システム開発、導入、保守等　（２）機器等及び情報システムの調達　（注１）を参照されたい。

3. ソフトウェアコンポーネントの管理、脆弱性管理の強化

3．ソフトウェアコンポーネントの管理、脆弱性管理の強化

➢ **政府機関等策定ガイドラインにおけるSBOM（Software Bill of Materials：ソフトウェア部品表）の追記を踏まえ、ガイドラインにも同様の内容を規定する方向にしてはいかがか。**

政府機関等策定ガイドライン

（新設）

基本対策事項

＜4.3.1(1)(a)関連＞

4.3.1(1)-4 統括情報セキュリティ責任者は、ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認を必要とする場合には、SBOM（Software Bill of Materials：ソフトウェア部品表）の作成、提供等を、調達時の評価項目とすることを機器等の選定基準として定めること。

（解説）

基本対策事項4.3.1(1)-4

「ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認」について

ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認については、当該ソフトウェア及び機器等に関するSBOMの作成、提供等を調達先に求めることや、調達先が安全なソフトウェア開発の慣行に基づく開発を実施していることを確認することが挙げられる。（略）なお、安全なソフトウェア開発の慣行に基づく開発については、NISTが公表している以下のフレームワークを参考にするとよい。

参考：NIST「SP800-218: Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities」（https://csrc.nist.gov/pubs/sp/800/218/final）

改定案：対策基準（解説）　（赤字が追記部分）

6.3. システム開発、導入、保守等

（２） 機器等及び情報システムの調達

機器等及び情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、機器等及び情報システムのライフサイクルで必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。（略）また、調達における透明性の確認を必要とする場合には、SBOM（Software Bill of Materials：ソフトウェア部品表）の作成、提供等を、調達時の評価項目とすることを機器等の選定基準として定めることも考えられる。（略）

（章末に以下を追記）

＜参考：調達における透明性を確認するためのSBOM（Software Bill of Materials：ソフトウェア部品表）の活用＞

ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認については、当該ソフトウェア及び機器等に関するSBOMの作成、提供等を調達先に求めることや、調達先が安全なソフトウェア開発の慣行に基づく開発を実施していることを確認することが挙げられる。なお、安全なソフトウェア開発の慣行に基づく開発については、NISTが公表している以下のフレームワークを参考にするとよい。

参考：NIST「SP800-218: Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities」（https://csrc.nist.gov/pubs/sp/800/218/final）

（続く）

3. ソフトウェアコンポーネントの管理、脆弱性管理の強化

政府機関等策定ガイドライン（解説）

（新設）
基本対策事項4.3.1(1)-4
「SBOM（Software Bill of Materials：ソフトウェア部品表）」について
SBOMとは、ソフトウェアコンポーネントに関する情報を含んだ機械処理可能な一覧リストのことで、オープンソースソフトウェアに関する情報だけではなく、プロプライエタリソフトウェア（ソフトウェア配布者がその知的財産を保持しており、改変や複製が制限されているソフトウェア）に関する情報も含めることができる。ソフトウェアに関する選定基準の一つとして、SBOMの情報を機関等が確認できることに関する基準を加えることで、ソフトウェアの透明性の確認を行うことができる。さらに、脆弱性に関する対策の効率化の観点からSBOMを活用することも考えられる。SBOMの項目は多様であり、SBOMの対応範囲に応じてコストと効果が大きく異なるため、分野やシステム利用環境のリスクの違いに応じて妥当な対応範囲を目指すことが効果的である。従って、選定基準においては、SBOMの提供有無の二者択一ではなく、SBOMの対象とするソフトウェアの範囲や脆弱性管理の範囲等について、対象ソフトウェアのリスクを踏まえ、調達先への過度な要求とならない範囲で明示するとよい。例えば、利用時のリスクが低いソフトウェアについては、最小限のSBOM対応範囲に留めることなどにより、コストを抑えることも考えられる。
SBOMやSBOM対応範囲の考え方については、経済産業省が公表している以下の手引を参考にするとよい。

参考：経済産業省「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」（令和５年７月28日）（https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html）

改定案：対策基準（解説）　（赤字が追記部分）

（続き）
SBOMとは、ソフトウェアコンポーネントに関する情報を含んだ機械処理可能な一覧リストのことで、オープンソースソフトウェアに関する情報だけではなく、プロプライエタリソフトウェア（ソフトウェア配布者がその知的財産を保持しており、改変や複製が制限されているソフトウェア）に関する情報も含めることができる。ソフトウェアに関する選定基準の一つとして、SBOMの情報を地方公共団体が確認できることに関する基準を加えることで、ソフトウェアの透明性の確認を行うことができる。さらに、脆弱性に関する対策の効率化の観点からSBOMを活用することも考えられる。SBOMの項目は多様であり、SBOMの対応範囲に応じてコストと効果が大きく異なるため、分野やシステム利用環境のリスクの違いに応じて妥当な対応範囲を目指すことが効果的である。従って、選定基準においては、SBOMの提供有無の二者択一ではなく、SBOMの対象とするソフトウェアの範囲や脆弱性管理の範囲等について、対象ソフトウェアのリスクを踏まえ、調達先への過度な要求とならない範囲で明示するとよい。例えば、利用時のリスクが低いソフトウェアについては、最小限のSBOM対応範囲に留めることなどにより、コストを抑えることも考えられる。
SBOMやSBOM対応範囲の考え方については、経済産業省が公表している以下の手引を参考にするとよい。

参考：経済産業省「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver.2.0」（令和６年８月29日）
（https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html）

最新の情報に更新

4. 要管理対策区域外での端末利用時の対策の強化

4. 要管理対策区域外での端末利用時の対策の強化

➢ **第三者による物理的なアクセスのリスクについて、モバイル端末の持ち出しについての章に規定してはいかがか。**

政府機関等策定ガイドライン

（新設）
＜6.1.2(2)(a)(b)関連＞
6.1.2(2)-1 情報セキュリティリスクが相対的に高いと考えられる地域等においては、第三者による物理的なアクセスのリスクへの対策を実施する。

（解説）
基本対策事項6.1.2(2)-1「第三者による物理的なアクセスのリスクへの対策」について

情報セキュリティリスクが相対的に高いと考えられる地域等においては、第三者による物理的なアクセスのリスクを十分に考慮する必要がある。このような地域等においては、例えば、使用する端末のUSBポート等を物理的にロック（塞ぐ）して封印、システム設定で端末のUSBポート等を無効にするといった対策を施した専用のモバイル端末で業務を行うとともに、端末は常時携行し、このような地域等から戻った際には、端末を工場出荷時の状態に戻すことが望ましい。

改定案：対策基準（解説）　（赤字が追記部分）

5.1.職員等の遵守事項
（１） 職員等の遵守事項
①モバイル端末の持ち出し及び外部における情報処理作業
（前略）

（注３）持ち出し専用パソコンによる情報の持ち出しにおいては、万一当該パソコンを紛失した場合に、記録されている情報を容易に特定するため、日常においては当該パソコンに情報を記録しないようにし、持ち出し時においては持ち出し情報が必要最小限であるかどうか確認を行った上で情報を記録し、返却時においては情報の完全削除をするといった運用を行う必要がある。また情報セキュリティリスクが相対的に高いと考えられる庁舎外への持ち出しにおいては、第三者による物理的なアクセスのリスクを十分に考慮する必要がある。第三者が端末に物理的にアクセスしやすく、情報が持ち出される可能性が高い環境下においては、例えば、使用する端末のUSBポート等を物理的にロック（塞ぐ）して封印、システム設定で端末のUSBポート等を無効にするといった対策を施した持ち出し専用パソコンで業務を行うことが根本的な対策として考えられる。

情報セキュリティリスクが相対的に高いと考えられる場所として、庁舎外が考えられる

5. BYOD対策の強化

5. BYOD対策の強化

- **既に自治体機密性２以上の情報の利用の有無等を申請内容に記載する旨について規定しているため、改定の必要はないと考えられる。**

政府機関等策定ガイドライン（解説）　（赤字が改定部分）

遵守事項6.1.3(1)(a)
「可否を判断すること」について

（前略）
機関等支給以外の端末の利用に当たっては、厳格な管理を行うことが不可欠であるため、機関等支給以外の端末の利用を許可するに当たり、機関等としての利用方針を定めて、その利用方針の下、厳格な管理を行うことが求められる。
機関等支給以外の端末の利用方針として、例えば以下の事項の明確化が考えられる。
･利用を許可する部局・課室等の組織の単位
･利用を許可する職員等の条件
･利用を許可する端末の種類（スマートフォン、携帯電話、PC等）
･利用を許可する端末のOS及びそのバージョン
･利用を許可する業務（出張時の連絡、危機的事象発生時の緊急対処業務 等）
･利用する機能（電子メール及びウェブ閲覧に限定 等）
･利用を許可する情報の格付（機密性１情報又は機密性２情報　等）

また、機関等支給以外の端末の利用に際して、利用する通信回線やサーバ装置等、情報システム全体として情報セキュリティを確保することが重要であることから、リモートアクセス環境や端末の安全管理措置について、システム機能として提供することも考慮すべきである。
併せて、最高情報セキュリティ責任者による機関等支給以外の端末の利用可否及びその利用方針について、当該事項を対策基準に記載するとともに、職員等へ周知することで機関等支給以外の端末の適切な利用が行われるようにすることも重要である。

改定案：対策基準（解説）

5.1.職員等の遵守事項
(１)職員等の遵守事項

②支給以外のパソコンやモバイル端末等の業務利用
（注５）支給された端末以外の利用申請内容については、以下を含めること。
・申請者の氏名、所属、連絡先
・利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合）
・利用する端末の製造企業名、機種名、OSの種類及びバージョン
・利用目的、取り扱う情報の概要、自治体機密性２以上の情報の利用の有無等
・主要な利用場所
・利用する主要な通信回線サービス
・利用する期間

5. BYOD対策の強化

➢ **モバイル端末OSについて、カスタマイズされていたり様々なバージョンがある場合に、業務への利用を許可できるOS、バージョンであるか等について確認する旨を規定してはいかがか。**

政府機関等策定ガイドライン（解説）　（赤字が改定部分）

基本対策事項6.1.3(2)-1 a)
「利用する端末の製造企業名、機種名、OSの種類及びバージョン」について

職員等が利用する機関等支給以外の端末についても、機関等が支給する端末を調達する際と同等の情報セキュリティ水準でサプライチェーン・リスクに対応することが適当である。
機関等支給以外の端末について、製造企業名、機種名を把握し、「IT調達に係る国等の物品又は役務の調達方針及び調達手続に関する申合せ」（平成30年12月10日関係省庁申合せ）の趣旨を踏まえた対応として、内閣官房内閣サイバーセキュリティセンターに助言を求める。**また、スマートフォンのAndroid OSのように製造企業によってカスタマイズされたOSがある場合や様々なバージョンが利用されている場合、機関等が許可できるOS、バージョンであるか、利用する情報システムの情報セキュリティ対策が対応できる端末であるかを判断する。**
利用の可否については、内閣官房内閣サイバーセキュリティセンターの助言や判断結果を踏まえて、適切に判断する必要がある。

薄ピンク色の字の部分は基本的に、政府機関等において特に防護すべき情報システム・機器・役務等に関する調達の基本的な方針及び手続を定めた「IT調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成30年12月10日関係省庁申合せ）に規定されている内容が追記されている。
（https://www.nisc.go.jp/pdf/policy/kihon2/IT_moushiawase.pdf）

改定案：対策基準（解説）　（赤字が改定部分）

5.1.職員等の遵守事項
(１)職員等の遵守事項

②支給以外のパソコンやモバイル端末等の業務利用
自宅や庁外等での情報処理作業においては支給された端末を使用することとし、支給以外の端末の使用は原則禁止とする。
止むを得ず支給以外の端末を使用する場合は、以下のような対策を実施することが必要である。

・統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者の許可を得る
・支給以外の端末のコンピュータウイルスチェックが実施されていることやファイル共有ソフトウェアの導入がされていないことを情報セキュリティ管理者が確認する
・パスワードによる端末ロック機能や遠隔消去機能などの要件を満たしていることを情報セキュリティ管理者が確認する
・自治体機密性３の情報資産については支給された端末以外での作業を禁止とする
・支給以外の端末のセキュリティに関する教育を受けた者のみ使用を許可する
・無許可で行政情報等を記録、持ち出す行為を禁止する
・業務利用する必要がなくなった場合は、支給以外のパソコンやモバイル端末等から業務に関係する情報を削除する
・モバイル端末のOSが、Android OSのように製造企業によってカスタマイズされたOSがある場合や様々なバージョンが利用されている場合、業務への利用を許可できるOS、バージョンであるか、利用する情報システムの情報セキュリティ対策が対応できる端末であるか確認する

6.電子メール不正中継対策の強化

6. 電子メール不正中継対策の強化

- **電子メールの不正中継についてガイドラインでは禁止しているため、中継を許可する電子メールに係る追記は不要なのではないか。**
- **送信元のメールのなりすまし対策については、SPF･DKIM･DMARCについてすでに規定している。**

政府機関等策定ガイドライン　（赤字が改定部分）

（新設）
＜6.2.2(1)(a)関連＞
6.2.2(1)-1 情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように以下を例とする設定をすること。
a)送信元の電子メールサーバのIPアドレスによって中継を制限する設定
b)送信元のメールアドレスのドメイン名によって中継を制限する設定
c)宛先のメールアドレスのドメイン名によって中継を制限する設定

（解説）
遵守事項6.2.2(1)(a)「不正な中継」について

（前略）
これらを回避するため、電子メールの不正な中継を行わないように、中継を許可する電子メールを必要最小限とする設定を電子メールサーバに行うことが必要である。
特に、電子メールサーバ間で送受信する電子メールを中継するメール中継サーバが設置される場合、電子メールの不正な中継を行わない設定をメール中継サーバで必ず実施し、IPアドレスによる制限等の対策をファイアウォールによる通信制限のみに依存しないよう留意する必要がある。
なお、当該設定においては、多重防御の考えに基づき、メール中継サーバを含む全ての電子メールサーバにおいて実施するとともに、設定が可能な範囲で複数の設定を行うことが必要である。
さらに、送信元のメールがなりすまされていないか検証する必要がある場合には、電子メールの中継を行う電子メールサーバにおいて、電子メールのなりすまし防止対策を講じることも考えられる。

改定案：対策基準

6.1.コンピュータ及びネットワークの管理
(１４)電子メールのセキュリティ管理

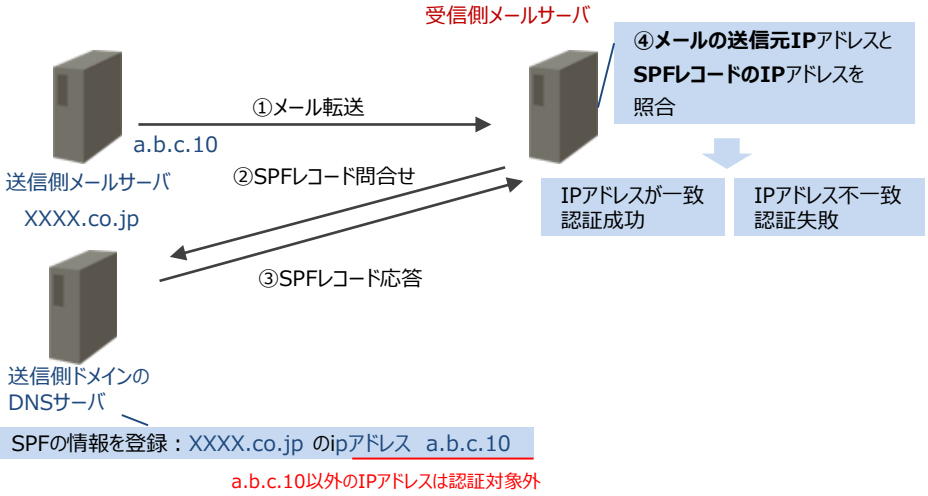
メールサーバに対するセキュリティ対策等、電子メールのセキュリティ管理について定める。外部からの電子メール受信及び外部への電子メール送信においてなりすましを防ぐため、メールサーバのセキュリティ対策として電子署名を用いたDKIM（DomainKeys Identified Mail）やSPF（Sender Policy Framework）等の対策を実施するとともに、DMARC（Domain-based Message Authentication, Reporting & Conformance）も実施しなければならない。また、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、SMTPによるサーバ間通信をTLSによる保護や、S/MIME等の電子メールにおける暗号化及び電子署名の技術の利用等、電子メールのサーバ間通信の暗号化の対策を講ずることも考えられる。
加えて、電子メールの不正な中継を行わないようにメールサーバを設定しなければならない。外部へ情報を持ち出すために電子メールが用いられることを考慮し、フィルタリングソフトウェア等による監視を実施することが望ましい。
中継処理の禁止は、メールサーバが踏み台となり他のサーバに攻撃を行うことを防止するために必要がある。
職員等が電子メールの送信等により情報の外部への不正な持ち出しをしていないか監視するためには、フィルタリングソフトウェア等を利用する。
（後略）

（参考）メールセキュリティ対策　SPF・DKIM・DMARC

➢ **SPF・DKIM・DMARCは、攻撃メールやスパムメール対策のため送信側のドメインに基づいて、メールを受信したメールサーバが送信側のメールサーバの正当性を検証する仕組みである。**

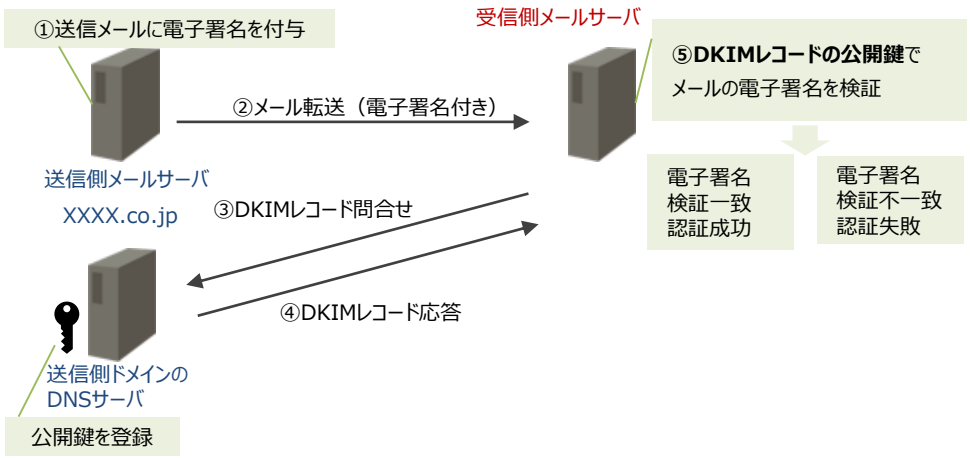
SPF

メールが正規のサーバから送信されていることを、送信元のドメインと送信元のIPアドレスで検証する



DKIM

メールが正規のサーバから送信されていることを、電子署名にてを検証する



DMARC

SPFやDKIMの認証が失敗した場合の対応を定める仕組み、送信側が受信側の認証失敗時のアクションをDNSに「DMARCポリシー」として宣言
受信側は認証失敗時にDMARCポリシーを参照して、受信メールの扱いを判断