別紙

地方公共団体の機器等の調達における
サプライチェーン・リスク対策のための
選定基準及び仕様書策定手引書

令和８年７月

総務省

1. 総則

1.1. 本書の目的

地方公共団体が調達する機器等（ネットワーク、情報システム、ネットワーク又は情報システムに関する施設及び設備、電磁的記録媒体等の情報資産をいう。以下同じ。）に必要なセキュリティ機能が装備されていない場合、当該機器等の製造過程で不正な変更が加えられている場合、及び調達後にセキュリティ対策が継続的に行うことができない場合は、セキュリティが維持できなくなるおそれがある。このため、機器等の調達に当たっては、セキュリティ維持の観点から適切な機器等を選定することが求められる。機器等を適切に選定するためには、地方公共団体において、選定基準及び選定基準に沿った仕様書を適切に策定することが必要である。

本書は、地方公共団体の機器等の調達におけるサプライチェーン・リスク対策のための選定基準及び仕様書の円滑な策定に資することを目的としている。

1.2. 本書の対象となるサプライチェーン・リスクの範囲

本書においては、サプライチェーン・リスクの中でも、特に、「地方自治法施行規則の一部を改正する省令の公布等について（通知）」（令和８年６月２６日付け総行サ第４２号、総務省自治行政局長通知。以下「局長通知」という。）の別紙１「３．新規則に規定するサプライチェーン・リスク対策」において例示した、「機器等を開発・供給する事業者及びそのサプライヤー・委託事業者（再委託事業者等を含む。以下同じ。）並びに当該機器等の設置、保守等の役務を提供する事業者及びその委託先事業者について、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」に関して取り扱うものとする。

以降、本書の記述において「サプライチェーン・リスク」としているものは、特に断りのない限り、本項に示す範囲のサプライチェーン・リスクを指すものとする。

1.3. 本書の使い方

本書は、機器等の調達を行う機会がある地方公共団体の事務従事者（以下「調達担当者」という。）を対象としており、調達担当者が関与する機器等の調達において、サプライチェーン・リスクを軽減させるために必要な選定基準及び仕様書への記載事項の例を示すものである。調達担当者は、「2. 機器等の調達に係る選定基準の例」及び「3. 機器等の調

達に係る仕様書の記載例」を参考に、選定基準及び仕様書への記載事項を決定する。

なお、本書は、一定の網羅的な内容となるよう策定したものであり、サプライチェーン・リスクが増大又は顕在化した場合であっても、影響が軽微と考えられる調達案件については、本書に記載する内容の全てを考慮する必要はない。

1.4. 地方自治法施行規則の一部を改正する省令（令和８年総務省令第８０号）との関係

地方自治法施行規則の一部を改正する省令（令和８年総務省令第８０号）による改正後の地方自治法施行規則（昭和２２年内務省令第２９号。以下「新規則」という。）において、「情報システム等の開発、導入及び保守の適切な実施」（新規則第１６条の３第１項第５号）並びに「適切な業務委託（情報システム等に関するものを含む。）の実施」及び「インターネットその他の高度情報通信ネットワークを通じて電子計算機を他人の情報処理の用に供する役務の適切な利用」（新規則第１６条の３第１項第７号）が規定され、併せて局長通知において、情報システム等のサプライチェーン・リスク対策に係る事項を示したところである。

本書は、新規則及び局長通知に示されているサプライチェーン・リスク対策を実効的なものとするため、選定基準及び仕様書への記載事項について、技術的な助言を行うものである。

1.5. 本書の対象となる機器等の調達の範囲

本書は、以下の機器等の調達に適用する。

(1) 地方公共団体における機器等の調達。

(2) 売買契約の方法のほか、リース契約、役務の提供等の方法による機器等の調達。

(3) 業務委託（情報システムに関するものを含む。）の実施に併せた機器等の調達又は利用。

1.6. 本書の改定

サプライチェーン・リスクに適切に対応していくためには、状況の変化を的確にとらえ、それに応じて対策内容の強化や見直しを行うことが重要である。したがって、サプライチェーン・リスクに関する事案の発生状況や外国政府の動向等に変化が認められる場合には、政府機関の情報セキュリティ対策のための統一基準の遵守事項及び当該遵守事項に対応する総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」の規定内容を踏まえつつ、本書の改定について検討するものとする。

2. 機器等の調達に係る選定基準の例

機器等の調達において、サプライチェーン・リスクを軽減させるために必要な選定基準の例を、以下のとおり示す。

機器等の選定に関する基準

１．目的

【市】が調達する機器等（ネットワーク、情報システム、ネットワーク又は情報システムに関する施設及び設備、電磁的記録媒体等の情報資産をいう。以下同じ。）に必要なセキュリティ機能が装備されていない場合、当該機器等の製造過程で不正な変更が加えられている場合、及び調達後にセキュリティ対策が継続的に行うことができない場合は、セキュリティが維持できなくなるおそれがある。このため、機器等の調達に当たっては、セキュリティ維持の観点から適切な機器等を選定することが求められる。

本選定基準は、機器等の選定・調達においてセキュリティの観点から考慮すべき基準について定め、もって【市】におけるセキュリティの確保に資することを目的とする。なお、本基準は、入札参加資格に関するものではない。

２．対象者

調達する機器等を構成要素とすることとなる情報システムの情報セキュリティ責任者以下、当該調達に関与する職員。

３．本基準を適用する機器等の調達の範囲

本基準は、以下の機器等の調達に適用する。

(1) 【市】における機器等の調達。

(2) 機器等の調達には、売買契約の方法のほか、リース契約、役務の提供等の方法による機器等の調達を含む。

(3) 機器等の調達には、業務委託（情報システムに関するものを含む。）の実施に併せて機器等を調達又は利用する場合を含む。

４．機器等の選定基準

情報システム管理者は、事業者と適宜調整を行いつつ、以下に例示する内容を機器等の調達仕様書等に含めること等を通じて、必要なセキュリティ機能が調達する機器等へ実装されることを担保すること。

（１）基本的なセキュリティ対策

(a) 必要なセキュリティ機能を含んでいること。

(b) 設置時や保守時のサポート体制が確立されていること。

(c) 利用マニュアル・ガイダンスが適切に整備されていること。
(d) 脆弱性検査等のテストの実施が確認できること。

（2）サプライチェーン・リスク対策
(a) 情報資産の分類に応じて、原則として、「セキュリティ要件適合評価及びラベリング制度（ＪＣ－ＳＴＡＲ、経済産業省）」、「政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ、ＩＳＭＡＰ－ＬＩＵ、国家サイバー統括室・デジタル庁・総務省・経済産業省）」又は「デジタルマーケットプレイス（ＤＭＰ、デジタル庁）」（以下「政府の評価・登録制度」という。）に登録等がなされていることが確認できること。
(b) 政府の評価・登録制度に登録等がなされていない機器等（政府の評価・登録制度の対象とならない製品分野に属する機器等を含む。）に関しては、次のとおり適切なサプライチェーン・リスク対策が講じられていることが確認できること。
① 機器等の開発等のライフサイクルにおいて、不正な変更が加えられない管理がなされていることが確認できること。具体的には以下のとおり。
ⅰ 製造工程（開発工程を含む。以下同じ。）において、機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者（再委託先事業者等を含む。以下同じ。）による信頼できる品質保証体制が確立されていること。
ⅱ 製造工程における不正な変更の有無について、機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者において、定期的又は随時に確認を行うこと。
ⅲ 製造環境（開発環境を含む。）において、定められた要員以外がアクセスできないよう、機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者が、アクセス可能な要員を物理的（監視カメラ等の入退室管理等）かつ論理的（データシステム等へのアクセス制御）に適切に制限していること。
ⅳ 調達した機器等に不正な変更やそのおそれがあることを発見した場合には、機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者並びに当該機器等の設置、保守等の役務を提供する事業者及びその委託先事業者に対して、必要に応じて追跡調査や立入検査を行う等、【市】と【市】の契約相手方が連携して原因を調査・排除できる体制を整備していること。
② 機器等を開発・供給する事業者及びそのサプライヤー・委託先事業者並びに当該機器等の設置、保守等の役務を提供する事業者及びその委託先事業者について、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に係る懸念が払拭できな

い機器等を調達しないこと又は役務の提供を受けないこと。

③ ISO/IEC 15408 等、国際標準に基づく第三者認証の取得又は第三者による監査結果により、セキュリティ機能の適切な実装、開発環境の管理体制の検査、脆弱性テスト等について客観的に評価できること。

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、提供等を行っていること。

3. 機器等の調達に係る仕様書の記載例

「2.機器等の調達に係る選定基準の例」の内容のうち、特に「４．機器等の選定基準」の「（２）サプライチェーン・リスク対策」について、仕様書への記載例を以下に示す。

なお、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）において示す自治体機密性２以上の情報を取り扱う機器等の調達を実施する際は、仕様書に定めるサプライチェーン・リスク対策を含めたセキュリティ対策の内容に適合することについて、入札参加希望事業者に確認書の提出を求め、異議がない場合は承諾書を交付する旨、仕様書に記載すること。

3.1. 仕様書の記載例

(1) 「2.機器等の調達に係る選定基準の例」「（２）サプライチェーン・リスク対策」(a)を確認するための仕様書の記載例

受注事業者は、本調達において、原則として以下の政府の評価・登録制度に登録等がなされていることが確認できる機器等を提供すること。

・調達する製品が、セキュリティ要件適合評価及びラベリング制度（ＪＣ－ＳＴＡＲ）※1のラベル（★１以上）を取得していること。また、取得の内容を証明する資料を提出すること。

・提供するクラウドサービスが、ＩＳＭＡＰクラウドサービスリスト又はＩＳＭＡＰ－ＬＩＵ※2クラウドサービスリストに掲載されていること。また、掲載の内容を証明する資料を提出すること。

・提供するソフトウェアが、デジタルマーケットプレイスカタログサイト※3に登録されていること。また、登録の内容を証明する資料を提出すること。

※1 「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」は、インターネットに直接接続されない製品も含め、インターネットプロトコルを使用する通信機能を持つ幅広い IoT 製品を対象（パソコン、スマートフォン等は対象外）としている。令和７年５月 21 日から、独立行政法人情報処理推進機構（IPA）の Web サイトにおいて「適合ラベル取得製品リスト」が公開されている。

・「適合ラベル取得製品リスト」
https://www.ipa.go.jp/security/jc-star/list/jc-star-product-list/index.html

※2 ISMAP-LIU は、「ISMAP が対象とするクラウドサービス」のうち、セキュリティ上のリスクの小さな業務・情報の処理に用いる SaaS サービスに対する仕組みであり、また情報システムの調達においては、業務・情報の影響度に

応じたセキュリティを確保すべきとの考え方から、影響度が低いと評価される業務、情報に用いられる SaaS を対象とする制度として策定されている。

・「ISMAP クラウドサービスリスト」
https://www.ismap.go.jp/csm?id=cloud_service_list

・「ISMAP-LIU クラウドサービスリスト」
https://www.ismap.go.jp/csm?id=cloud_service_list_liu

※3 ・「デジタルマーケットプレイスカタログサイト」
https://www.dmp-official.digital.go.jp/

(2) 「2.機器等の調達に係る選定基準の例」「(２)サプライチェーン・リスク対策」(b)を確認するための仕様書の記載例

(機器等の提供に当たってのガイドラインの準拠)

本調達において、受注事業者は、機器等の提供に当たり、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）に準拠して、サプライチェーン・リスク対策を含むサイバーセキュリティ対策を講じること。

(役務の提供に当たってのガイドラインの準拠)

本調達において、受注事業者は、役務の提供に当たり、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）に準拠して、サプライチェーン・リスク対策を含むサイバーセキュリティ対策を講じること。

(3) 機器等リストの提出にかかる仕様書の記載例

候補となる機器等については予め【市】に機器等リストを提出し、【市】がサプライチェーン・リスクに係る懸念が払拭できないと判断した場合には、代替品選定やリスク軽減策等、【市】と迅速かつ密接に連携し提案の見直しを図ること。

(4) 確認書の提出及び承諾書の交付にかかる仕様書の記載例※4

(確認書の提出)

入札参加希望事業者は、【市】に対し、【公示の日以後、指定する日】において、仕様書に定めるサプライチェーン・リスク対策を含めたセキュリティ対策の実施について、必要な確認を可能な限り行い、別紙１のとおり確認書を提出すること。

（承諾書の交付）

【市】は入札参加希望事業者から提出された確認書について、異議がない場合、当該事業者に対して別紙２のとおり承諾書を交付すること。この場合において、【市】が【期間】内に承諾書を交付しないときは、確認書の内容を承諾したものとみなす。

※4　機器等の機能要件や技術要件等の確認結果の通知等、地方公共団体における既存の調達プロセスに組み込んで実施することも考えられる。

（別紙１）

確認書

●年●月●日付けで【市】が公告した【案件名】について、【市】に提供する機器等（ネットワーク、情報システム、ネットワーク又は情報システムに関する施設又は設備、電磁的記録媒体等の情報資産をいう。）又は役務に関し、予め【市】に機器等リストを提出した上で調整した結果も踏まえ、仕様書に定めるサプライチェーン・リスク対策を含めたセキュリティ対策の内容に適合したものであることを確認します。

●年●月●日
社　　名
代表者名

（別紙２）

承諾書

●年●月●日付けで【市】に提出された、【案件名】にかかる確認書の内容について、承諾します。

●年●月●日
【市】長　　氏　名

4. その他特記事項

受注事業者がサプライチェーン・リスク対策を講じる際、予期しない外部的事情により、代替品の選定、履行期日の調整等が必要となる可能性もあるため、地方公共団体は、適切に事業者と協議を行うこと。

改定履歴

改定年月日	改定内容
2026 年 7 月 31 日	初版