資料３－３

外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書

2015 年 5 月 21 日
内閣サイバーセキュリティセンター

改訂日	改訂理由	備考
2015/5/21	初版	

内容

1. 総則

1.1 本書の目的

情報システムの高度化に伴い、その調達に関係する部品数やソフトウェアの要素数、構築や保守に必要な工数は幾何級数的に増加しており、結果として政府機関で利用される情報システムに関与する事業者や従業者の数は膨大なものとなっている。また、情報システムの開発や機器等の製造に係るサプライチェーンの国際的な分業が進んだことにより、サプライチェーンに介在する全ての事業者を適切に管理することが困難になっている。その結果、情報セキュリティ管理が不適切な事業者がサプライチェーン上に存在することによる情報漏えい等が懸念されている。さらに、サプライチェーンの中には、自国との利益相反が存在する可能性がある他国の政府によって所有、指示又は補助を受けている事業者が存在していることが否定できないことから、そのような事業者による不正行為に起因した情報窃取等が懸念されている。

これら情報システム開発の委託先をはじめとした関係組織によって、不正プログラム等が委託元である政府機関の意図に反して情報システムに埋め込まれ、情報窃取が行われるなどのいわゆる情報セキュリティ上のサプライチェーン・リスクへの対応が、近年新たな課題となっている。海外では、特定のメーカーの製品利用を禁止する勧告が出されるなどの措置も取られており【参考１】、日本政府においても対策の強化が必要となっている。

このような現状を踏まえ、「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）」（以下、「政府機関統一基準」という）では、府省庁外の者に情報システムの構築やアプリケーションの開発等を外部委託する場合や機器等を調達する場合等において、調達元となる府省庁の組織が実施すべき情報セキュリティ上のサプライチェーン・リスクへの対応に係る遵守事項（1.4節参照）を定めている。

本書は、当該遵守事項を適切に実施するための「目的、判断ポイント、具体的な対策の例」等を解説しており、政府機関統一基準の遵守事項に対する理解を深めるとともに、府省庁における情報セキュリティ上のサプライチェーン・リスクに対応するための調達仕様書の円滑な作成に資することを目的としている。

【参考１】サプライチェーン・リスクに関連する海外の動向

（※平成26年版防衛白書（P109）より一部抜粋。）

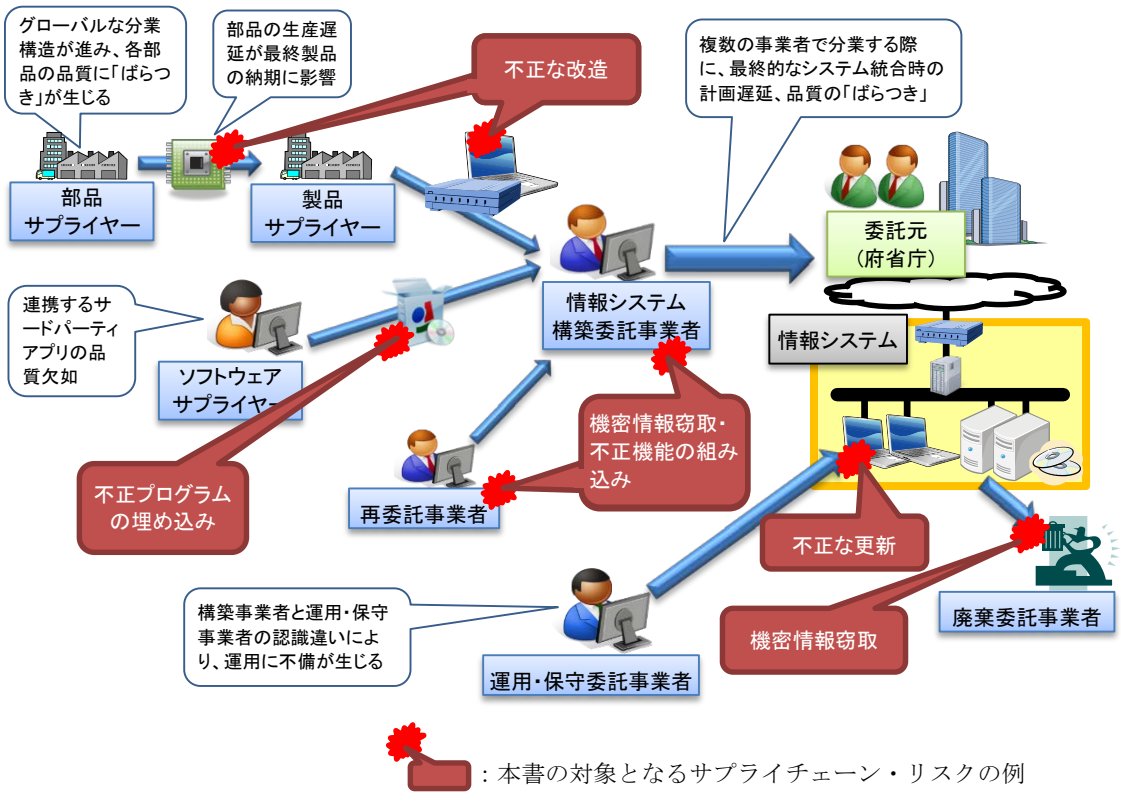
12（平成24）年10月、米下院情報特別委員会による「中国通信機器企業華為技術および中興通訊が米国国家安全保障に及ぼす問題」と題する調査報告書では、米国重要インフラに対するサイバー攻撃能力や企図に対する懸念や、中国主要IT企業と中央政府、共産党、人民解放軍との不透明な関係がサプライチェーン・リスクを増大させることへの強い懸念といった、国家安全保障上の脅威を理由に、中国大手通信機器メーカー「華為技術」および「中興通訊」の製品を利用しないように勧告された。フランス、オーストラリア、カナダ、インドおよび台湾などでも同様の動きがみられ、英国および韓国などでは注意を促す動きがみられる。

1.2 本書の対象となるサプライチェーン・リスクの範囲

サプライチェーンとは、一般的に、ある製品の原材料が生産されてから、最終消費者に届くまでのプロセスを意味するものであるが、本書においては、特に、情報通信技術に係るサプライチェーンを対象としており、情報システムの構築や機器等の調達において、発注者へ情報システムや機器等が納入されるまでの開発や製造に係る一連の工程に加えて、当該情報システムや機器等の運用・保守・廃棄を含むライフサイクル全般を対象としている。

サプライチェーン・リスクには、部品供給元の工場の火災によりハードウェアの納入が延期されたり、ソフトウェア開発者の退職により仕様どおりの開発が不可能になったりすること等により、発注者の事業が計画どおりに実施できなくなるなどの様々な脅威や脆弱性により生じるものも含まれると考えられるが、本書においては、図―１に示すとおり、特に、ハードウェア製品を意図的に不正改造したり、情報システムやソフトウェアに不正なプログラムを埋め込んだりするなど、発注者の意図しない変更を攻撃者が情報システムや機器等に加えることにより、機密情報を窃取するなどの情報セキュリティ上のサプライチェーン・リスクに限定している。

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。



図－１　本書において対象としているサプライチェーン・リスクの範囲

1.3 本書の使い方

本書は、情報システムの構築、運用等の外部委託や機器等の調達を行う機会がある行政事務従事者（以下「調達担当者」という。）を対象としており、調達担当者が実施する情報システムの構築等の外部委託や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情報セキュリティ対策要件の定め方や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、まず、2.1 節において示すサプライチェーン・リスクに係る脅威や、2.2 節において示すサプライチェーン・リスクを増大させる要因となる脆弱性の例を参照し、情報システムの構築等の外部委託や機器等の調達におけるサプライチェーン・リスクを特定、分析し、対応すべきサプライチェーン・リスクの範囲を決定する。

次に、2.3 節に示す対策の考え方を参照した上で対策要件を決定し、３章及び４章に示す仕様書への記載の例を参考に、仕様書への記載事項を決定する。

なお、本書は、情報システムの構築、運用等の外部委託や機器等の調達のうち、WTO 政府調達協定第三条【参考２】における安全保障のための例外及び一般的例外を除いたものを主な対象として想定している。また、本書は、一定の網羅性を有する内容となるよう作成したものであり、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。

【参考２】政府調達に関する協定（２０１４年に改正されたもの）　第三条

第三条　安全保障のための例外及び一般的例外

１　この協定のいかなる規定も、締約国が自国の安全保障上の重大な利益の保護のために必要と認める措置又は情報であって、武器、弾薬若しくは軍需品の調達又は国家の安全保障のため若しくは国家の防衛上の目的のために不可欠の調達に関連するものにつき、その措置をとること又はその情報を公表しないことを妨げるものと解してはならない。

２　この協定のいかなる規定も、締約国が、次のいずれかの措置を講ずること又は実施することを妨げるものと解してはならない。ただし、それらの措置が、同じ条件の下にある締約国間において恣意的若しくは不当な差別の手段となるような態様で、又は国際貿易に対する偽装した制限となるような態様で適用されないことを条件とする。

(a)公衆の道徳、公の秩序又は公共の安全の保護のために必要な措置

(b)人、動物又は植物の生命又は健康の保護のために必要な措置

(c)知的財産の保護のために必要な措置

(d)障害者、慈善団体又は刑務所労働により生産される物品又は提供されるサービスに関する措置

1.4 対象となる政府機関統一基準の遵守事項

本書の対象となる政府機関統一基準の遵守事項を以下に示す（下線部がサプライチェーン・リスクに関連する記載）。

4.1.1 外部委託

(2) 外部委託に係る契約

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。

（中略）

（ウ）委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制

（エ）委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

（中略）

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること。

（ア）情報セキュリティ監査の受入れ

（中略）

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(a)(b)の措置の実施を委託先に担保させること。

5.1.2 機器等の調達に係る規定の整備

遵守事項

(1) 機器等の調達に係る規定の整備

(a) 統括情報セキュリティ責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を府省庁が確認できることを加えること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

1.5 国際規格との関係

近年、IT 調達における調達側と供給側の管理の手法に関する国際規格として、ISO/IEC 27036 が策定されている。これは 4 つのパートから構成されており、特に、パート 3 の情報通信技術に係るサプライチェーンに関するセキュリティのガイドラインでは、昨今国境をまたいで増大するサプライチェーン・リスクに対応するために、WTO による政府調達協定を尊重しつつ、供給側との関係を構築し、モニタリングして、調達案件における情報セキュリティを確保することが必要であると謳われている。

このような国際標準化の動向を踏まえて、本書においても、対策の考え方や具体的な対策事項を記述するに当たって、ISO/IEC 27036 の策定内容を参考としている。

1.6 本書の改訂

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、政府機関統一基準の遵守事項及び当該遵守事項に対応する府省庁対策基準策定のためのガイドラインの規定内容を踏まえつつ、本書の改訂について検討するものとする。

1.7 用語

本書においては、特別に定義する用語以外は、基本的に政府機関統一基準及び府省庁対策基準策定のためのガイドラインにおける用語を使用している。

2. サプライチェーン・リスク対応の考え方

サプライチェーン・リスクを生じさせる脅威や脆弱性を全てのサプライチェーンから完全に排除することは困難であるが、調達担当者は、調達案件ごとに、2.1 節に掲げた脅威や 2.2 節に掲げた脆弱性の有無を踏まえ、2.3 節に例示する手順で、調達案件ごとにサプライチェーン・リスクを特定、分析し、これを許容可能な水準まで軽減させることを検討する必要がある。

2.1 政府機関において想定される脅威の例

以下にサプライチェーン・リスクに係る脅威の例を示す。

- 府省庁の情報システムの構築を受託した事業者又は再委託事業者（再委託先、再々委託先等の再委託契約の末端となる事業者まで全てを含む。以下「再委託先等」という。）の従業員が、システムが稼働した後に容易に機密情報を窃取することを可能とする仕組みを開発時に悪意を持って組み込むことにより、当該情報システムの稼働開始後に、当該情報システムで取り扱われる要機密情報を窃取するなどの攻撃が行われる
- 悪意のある製品ベンダ又は当該ベンダの従業員によって、機器が構成するシステムに不正に侵入することができる経路や、不正に情報を窃取するための経路等を生じさせる不正プログラムを製造過程においてあらかじめ組み込み、当該製品を府省庁で調達することで、当該情報システムの稼働開始後に、情報システムを停止させるなどして情報システムを機能不全に陥れ、府省庁の業務を混乱させる
- 情報システムの運用保守を受託した事業者又は再委託先等の従業員が、ソフトウェア更新作業の際に不正プログラムを情報システムに組み込むことにより、当該情報システムが踏み台となって、他の情報システムへ攻撃が行われる
- 情報システムの運用事業者又は再委託先等の従業員の中に日本政府との利益相反が生じる外国の政府機関に関連する者が存在し、当該従業員が正規の運用作業を装って、情報システムから外国との交渉に関わる要機密情報を窃取する

2.2 政府機関において想定される脆弱性の例

以下にサプライチェーン・リスクを増大させる要因となる脆弱性の例を示す。

- 委託事業者又は再委託先等において、納入する機器やソフトウェアの設計書の管理が不十分である
- 委託事業者又は再委託先等の従業員に対する情報セキュリティに係る管理が不十分である
- 委託事業者又は再委託先等において、開発環境や納入物品、従業員等の情報セキュリティ管理に係る手順が整備されていない

・ 委託事業者が、再委託先等の情報管理に対して責任を負うことを意識していない又はその能力を有していない
・ 運用中の情報システムのハードウェア交換、ソフトウェア更新等の作業において、交換するハードウェア又は更新ソフトウェアの安全性の確認、交換又は更新作業の情報セキュリティに係る管理が不十分である
・ 委託事業者又は再委託先等が、製造過程や製造場所等が不明確な機器等を使用しているなど、機器等の製造事業者から安全性に関わる十分な情報を得ていない
・ 委託事業者又は再委託先等の資本関係又は委託事業者の役員又は従業員の中に、日本政府との利益相反が生じる可能性がある外国の政府機関に関連する者が存在する

2.3 サプライチェーン・リスクを軽減するための対策の考え方

サプライチェーン・リスクを軽減するためには、委託元である府省庁において、委託事業者によって提供された製品やサービス等の成果物が自府省庁の業務や情報を守る上で信頼できるものか否かを見極めなければならない。しかしながら、全てのハードウェア及びソフトウェアに、府省庁が要求していない機能が存在しないことを検証することは困難であり、膨大なコストが必要となる。そのため、委託先に対して、委託事業の実施状況に係る情報を求める、サプライチェーン・リスクへの対応のための厳格な管理体制を求めるなどの現実的な対策を中心に検討する必要がある。また、委託事業者が使用する機器等、サービス及びそれらに係る再委託先等に対する管理の強化も重要である。

対策を検討するに当たっては、2.1 節や 2.2 節を例とする脅威や脆弱性の有無によりサプライチェーン・リスクは増加、あるいは顕在化することから、調達担当者は、調達案件に関連する業務や取り扱う情報の特性に応じた脅威や脆弱性を踏まえ、サプライチェーン・リスクを特定、分析し、図２－１に示すとおり、情報システム等の企画・要件定義、調達・構築、運用・保守・廃棄のライフサイクルの各工程で必要となる対策を実施する必要がある。

（１）情報システム等の企画・要件定義	・サプライチェーン・リスクを特定、分析し、対応のための対策要件を決定する ・３章及び４章を参考に、調達仕様書等に要件を記載する
（２）情報システム等の調達・構築	・委託先候補事業者から提供された委託先における事業の管理体制や実施方法等から、委託先候補事業者がサプライチェーン・リスクに対する対策要件を遵守可能であることを確認する ・サプライチェーン・リスクの対策要件を遵守可能な事業者を選定する
（３）情報システム等の運用・保守・廃棄	・サプライチェーン・リスク対策計画について委託先と合意する ・委託事業の実施において、サプライチェーン・リスクの対策要件を遵守していることを確認する ・必要に応じて委託先の監査を行う

図２－１　情報システム等のライフサイクルの各工程における対策の概要

3. 外部委託の際に考慮すべき事項及び仕様書記載例

2.3 節に示す対策の考え方に基づき、外部委託を行う際にサプライチェーン・リスクを軽減させるために考慮すべき事項及び調達仕様書等に具体的に記載すべき事項を示す。

なお、本章で示す仕様書記載例は、あくまで例示であるので、各調達案件に関連する業務や取り扱う情報の特性等に従い、サプライチェーン・リスクを評価し、調達案件ごとに必要な事項を選択する必要がある。

3.1 外部委託の際に考慮すべき事項

（1）企画・要件定義の際に考慮すべき事項

① 委託事業を実施するに当たって、サプライチェーン・リスクの要因となる脆弱性を発生させない（又は増大させない）ための管理体制を委託事業者に提示させる。

② 委託事業者のサプライチェーン・リスクに係る管理体制が適切であることを確認するために必要な情報を、委託事業者に提示させる。

③ サプライチェーン・リスクに係る情報セキュリティインシデントを認知した場合や、その疑いが生じた際に、必要に応じて委託事業者の業務、作業プロセス及び成果物を立ち入り検査等で確認することを要件とする。

④ 委託事業の実施後（実施中）に、情報セキュリティ要件を履行した（している）ことを委託事業者に証明させることを要件とする。

⑤ 再委託を禁止する必要がある調達案件は、その旨を要件に明示する。再委託を禁止しない場合であっても、再委託の実施について、契約前に委託元の許可を得ることを要件とする。

⑥ サプライチェーン・リスク対応を含む情報セキュリティ対策要件は、委託事業者を含むすべての関係者（再委託先等も含まれる）に適用するものと位置付け、委託事業者が再委託先等における情報セキュリティ管理の責任を負うことをもって再委託等を許可する条件とすることを要件とする。

（2）情報システムの調達・構築時に考慮すべき事項

① サプライチェーン全般における機能的な管理体制、管理プロセスが委託元に対して透明化・可視化されている委託事業者を選定する。

② 委託元において、サプライチェーン・リスクを増大させる要因となる脆弱性の存在有無等を確認するために必要な、委託事業者や委託事業に従事する者（再委託先等も同様）の身元や専門性等の情報を提供することができる委託事業者を選定する。

③ 委託事業者を選定するに当たり、組織における人の権利、義務、業務内容等、業務を進める上での手順、情報セキュリティに対する組織文化に関する過去の実績を考慮する。

④ 再委託先等を管理するための手順が明らかであり、当該手順により再委託先等を管理する能力を有すると認められる事業者を選定する。

⑤ 委託事業の実施において、情報セキュリティインシデントが発生した場合に情報セキュリティ監査を受け入れることが可能な事業者又は委託元からインシデント対応結果や再発防止策の実施等を求められた際に、必要な情報を委託元に提供可能な事業者を選定する。

（3）情報システムの運用開始前及び運用・保守・廃棄において考慮すべき事項

① 委託事業における情報セキュリティ対策の実施プロセス及び実施結果を、受入れ検査時に確認する。

② 委託事業者における運用（又は保守）業務の実施において、サプライチェーン管理に係る要件を満たしていることが疑わしい場合は、委託事業者の情報セキュリティ監査を実施する。

③ 運用中の情報システムのハードウェア交換、ソフトウェア更新、廃棄作業において、交換するハードウェア又は更新ソフトウェアの安全性の確認、作業の情報セキュリティ管理に係る実施手順を運用管理規程等に定め、遵守させる。

3.2 外部委託の際の仕様書記載例

（１）「意図せざる変更が加えられないための管理体制」を確認するための仕様書記載例
（政府機関統一基準 遵守事項）

> 4.1.1 外部委託
> (2) 外部委託に係る契約
> (a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。
> （中略）
> （ウ）委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制

政府機関統一基準 4.1.1(2)(a)(ウ)では、委託事業者（再委託先等を含む。）の従業員その他の委託事業に関連する者が、委託事業に関連する全ての場合において、委託元が意図しない不正な変更を情報システムのハードウェア又はソフトウェア等に加えることがないようにするための管理体制を委託先候補となる事業者に提示させ、委託事業者の選定時において、当該体制の妥当性を委託元において確認することを求めている。

仕様書への記載に当たっては、3.1 節の考慮すべき事項を参照しつつ、管理体制の妥当性【参考３】が可能な限り確認できる要件とすべきであるが、委託元において具体的に指定することが困難な場合は、サプライチェーン上に発生し得るリスクをあらかじめ想定して、委託先候補となる事業者に広範な情報の提供を求めることが重要である。

<u>仕様書記載例</u>

- 情報システムの【設計・構築／運用・保守／廃棄 等の各工程のうち、調達内容に応じて必要な場面を選択】工程において、【府省庁名】の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。**[3.1 節（１）①、②、④／3.1 節（２）①／3.1 節（３）③に対応する仕様書記載例]**
- 【府省庁名】の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。第三者機関による品質保証体制を証明する書類等が提出可能な場合は、提出すること。**[3.1 節（１）①、②、④／3.1 節（３）①、③に対応する仕様書記載例]**

・ 情報システムに【府省庁名】の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、【府省庁名】と連携して原因を調査し、排除するための手順及び体制（例えば、運用・保守業務におけるシステムの操作ログや作業履歴等を記録し、発注先から要求された場合には提出させるようにするなど）を整備していること。また、当該手順及び体制が妥当であることを証明するための書類を提出すること。**［3.1 節（１）③／3.1 節（３）②、③に対応する仕様書記載例］**

（再委託の可能性がある場合）

・ 【府省庁名】の許可無く、作業の一部又は全部を第三者（再委託先）に請け負わせてはならない。ただし、【府省庁名】が許可した場合には、受託者は、【府省庁名】との契約上受託者に求められる水準と同等の情報セキュリティ水準を、再委託先においても確保すること。また、受託者は、再委託先が実施する情報セキュリティ対策及びその実施状況について、【府省庁名】に報告すること。**［3.1 節（１）⑤、⑥に対応する仕様書記載例］**

・ 委託事業において取り扱う情報について、再委託先が閲覧することがないように、受託者は情報を厳重に管理すること。止むを得ず、再委託先において委託事業に係る情報を閲覧する必要がある場合には、受託者は、事前に【府省庁名】の担当者と調整し、【府省庁名】の担当者の指示に従うこと。（再委託先における情報の取り扱いを含む包括的な秘密保持契約を締結する、作業の都度情報の取り扱いについて調整するなどの手続き方法について合意すること。）**［3.1 節（１）⑥に対応する仕様書記載例］**

【参考３】委託先におけるサプライチェーンの管理体制

委託先において、サプライチェーン・リスク対応が適切に行われていることを明確に判断することは困難なため、以下に例示する情報セキュリティ管理体制や管理手順の明確化により判断することが考えられる。

・ 特定の従業員一人のみが委託元から提供された要機密情報にアクセスしないよう、複数担当者による相互監視を手順に加えている。
・ 開発システムや運用システムの操作ログや作業履歴等の保管に関する手順が明確であり、ログの確認による不正行為の有無を定期的に確認している。
・ 定められた要員以外が、設計書や開発中のシステムに物理的にアクセスできないようにする管理手順が明確である。
・ 運用要員を限定し、作業日報等の提出、操作ログと日報の突合せ等で不正な操作を行っていないか確認する手順が明確であり、全委託作業従事者がその手順を徹底している。
・ システム操作卓やマシン室の内外に監視カメラが設置されており、不正な者が立ち入らないように日常から監視されている拠点や居室において開発等を行っている。
・ 委託事業従事者や管理責任者に対して、情報セキュリティに関する教育や研修が定期的に実施されており、情報セキュリティリテラシーの維持向上に努めている。

（２）「委託先の資本関係・役員の情報等に関する情報提供」に係る仕様書記載例
（政府機関統一基準 遵守事項）

4.1.1(2) (a) （中略） (エ) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

情報システムの開発や運用等を委託する際には、どのような委託事業者（以下、この項においては再委託先等を含む）がその委託業務を行うのかをあらかじめ認識しておくことが重要である。特に、海外の事業者に委託する場合には、当該国の法制度の仕組み、情報セキュリティ管理の仕組みの違い等によるリスクの増大を考慮した上で、適切に委託先を管理する必要がある。

このような観点から、政府機関統一基準 4.1.1(2)(a)(エ)では、委託事業者、委託事業の実施場所、委託事業従事者に係る様々な情報を開示させる仕様とし、その情報を基に前述の「意図せざる変更が加えられないための管理体制」における管理体制等の妥当性を確認することで、サプライチェーン・リスクの増大又は顕在化の防止を求めている。

特に、機密性の高い情報を取り扱うシステムの構築等の外部委託において、委託事業者及び委託事業の従事者について日本政府との利益相反が生じ得る可能性が否定できない場合は、利益相反を解消するための措置を委託事業者に求めるとともに、提案書等で当該措置が確認できるようにすることが重要である。

なお、委託事業の従業者に係る情報については、個人名等の詳細な情報は必ずしも必要ではなく、例えば、「委託事業従事者のうち■■国籍の者が○○名（又は○○%）」等の形で必要な範囲の情報の提供を受けることも考えられる。

仕様書記載例

- 受託者は、資本関係・役員の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提示すること。**[3.1 節（１）②／3.1 節（２）②、③に対応する仕様書記載例]**
- 委託事業の運用に係る要員を限定すること。また、全ての要員の所属、専門性（資格等）、実績及び国籍について掲示すること。委託事業の実施期間中に要員を変更する場合は、事前に【府省庁名】の担当者へ連絡し、許可（又は確認）を得ること。**[3.1 節（１）①、②／3.1 節（２）②、③に対応する仕様書記載例]**
- 運用に係る者の所属（契約社員、派遣社員等の雇用形態は問わず、委託事業に従事する全ての要員）、実績（経験年数、資格等）及び国籍について、【府省庁名】の担当者

にあらかじめ提出し、許可（又は確認）を得ること。**[3.1 節（１）②／3.1 節（２）②、③に対応する仕様書記載例]**

（再委託の可能性がある場合）

・　再委託を行う場合には、受託者は、再委託先の事業者名、住所、再委託対象とする業務の範囲、再委託する必要性について、委託元である府省庁の担当者へ提示し、許可（又は確認）を得ること。**[3.1 節（１）⑤に対応する仕様書記載例]**

・　前号に掲げる情報の提供に加えて、再委託先において本委託事業に関わる要員の所属、専門性（資格等）、実績及び国籍についての情報を委託元である府省庁の担当者へ提示すること。**[3.1 節（１）⑥に対応する仕様書記載例]**

（３）「情報セキュリティ監査の受入れ」に係る仕様書記載例

（政府機関統一基準 遵守事項）

4.1.1 外部委託 (2) 外部委託に係る契約 (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること。 (ア) 情報セキュリティ監査の受入れ

委託事業者やその再委託先等において、委託事業に関わる要員は日々入れ替わっており、委託事業者又はその従業員、再委託先等による意図せざる変更を防止するための管理体制が維持できていないことが懸念される。また、サプライチェーン・リスクに係る外部動向の変化等に対応した管理手順の見直し、強化が適切に実施されていない場合も想定される。

万が一、委託事業においてサプライチェーン・リスクに関連する情報セキュリティインシデントが発生してしまった場合は、委託元が委託事業者の事業所等への立入検査を実施する必要がある場合も考えられるが、その際には、委託事業者が協力を惜しまずに委託元と協力してインシデント対処を実施できるよう、立入検査や委託事業の実施状況の監査等の受入れを仕様書に規定しておくことが重要である。このような主旨の下、政府機関統一基準 4.1.1(2)(b)(ア)は規定されている。

他方で、委託事業者を監査することは、委託元、委託事業者双方において大きな負担を強いることも考えられることから、4.1.1(2)(b)(ア)では「必要に応じて」との条件を付している。インシデント発生時の影響範囲の想定及び委託事業の実施形態等を勘案した上で、実際の情報セキュリティ監査の必要性を判断し、監査の実施に係る具体的な要件について、委託事業の開始までに委託事業者と合意しておくことを求めている。

<u>仕様書記載例</u>

・ 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、【府省庁名】が情報セキュリティ監査の実施を必要と判断した場合は、【府省庁名】が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報セキュリティ監査を受託者は受け入れること。（【府省庁名】が別途選定した事業者による監査を含む）。**［3.1 節（１）③、④／3.1 節（２）④、⑤に対応する仕様書記載例］**

4. 機器等の調達の際に考慮すべき事項及び仕様書記載例

政府機関統一基準では、統括情報セキュリティ責任者が機器等の選定基準を定めるよう求めており、２章で示すサプライチェーン・リスクに係る脅威やサプライチェーン・リスクを増大させる要因となる脆弱性を考慮した上で選定基準を定める必要があるが、本章で示す仕様書への記載事項を府省庁の実施手順として定め、選定基準に代替することも考えられる。

なお、本章で示す仕様書記載例は、あくまで例示であるので、各調達案件に関連する業務や取り扱う情報の特性等に従い、サプライチェーン・リスクを評価し、調達案件ごとに必要な事項を選択する必要がある。

4.1 機器等の調達の際に考慮すべき事項

① サプライチェーンを通じて組み合わされたソフトウェア、ハードウェア製品及び部品要素等に意図せざる変更を加えられていないことを担保することができる製造事業者による機器等を選定する。（委託事業者によって担保可能であることを証明可能な書類等を提示させるなども考えられる。）

② 上記が困難な場合は、機器等の製造プロセスや情報セキュリティ管理体制が透明化、可視化されており、機器に不正が見つかったときの追跡力（トレーサビリティ）【参考４】を確保するなどのサプライチェーン・リスクを増大させる要因となる脆弱性を可能な限り軽減させるための対策が製造工程において実施されている機器等を選定する。

③ サプライチェーン・リスクに係る情報セキュリティインシデントが発生した場合に、立ち入り検査等を受け入れるなど、委託元と協力してインシデント対処を実施することが可能な製造事業者による機器等を選定する。

4.2 機器等の調達の際の仕様書記載例

（政府機関統一基準 遵守事項）

5.1.2 機器等の調達に係る規定の整備

(1) 機器等の調達に係る規定の整備

(a) 統括情報セキュリティ責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を府省庁が確認できることを加えること。

機密性の高い情報を取り扱う機器等の調達においては、製造工程における不正行為の有無について定期的な監査を行っていること、機器等の製造環境にアクセス可能な従業員が適切に制限されていること、運用手順の定期的な点検が行われていること等を示さ

せ、その妥当性を委託元が確認できるよう、政府機関統一基準 5.1.2(1)(a)は規定されている。

ただし、機器等の利用環境によって、調達時に求める要件が異なるため、機器等を調達又は利用する組織や、当該機器等で取り扱う情報の特性に応じて、必要となる要件を決定することが重要である。

【参考４】機器に不正が見つかったときの追跡力（トレーサビリティ）について

サーバ装置や端末等の情報システムを構成する機器（完成品）は、膨大な数の部品類により構成されており、当該機器の設計、開発、製造、流通等の一連の工程に関係する事業者から成るサプライチェーンは、今では必ずと言ってよいほど多数かつ多国籍の事業者が関わっていることが常識になっている。このため、機器等の調達におけるトレーサビリティの確保が重要となっている。

機器等の調達におけるトレーサビリティとは、サプライチェーンにおける機器の製造工程を履歴として記録し、事業者の所在や事業に関わる者に係る情報等と併せて、調達先が確認できる仕組みを指す。海外製の部品が組み込まれた IT 製品の調達において、海外の事業者によって部品や機器への不正な変更が加えられた際も、トレーサビリティを確保しておけば、原因調査や再発防止策の検討に役立つ情報を入手することができる。

なお、トレーサビリティの確保といっても、機器（完成品）によって必要とされる水準が異なる。厳密なトレーサビリティを求めるのであれば、個々の部品単位で設計や製造過程をトレースできる状態を確保する必要があるが、管理工数や管理情報が肥大化して、結果的に効果が薄まってしまうことが懸念されることから、必要な水準と管理工数を勘案して、対象となる部品を絞り込む等、効率化を図ることも必要である。

仕様書記載例

- 当該機器等の製造工程において意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。**[4.1 節 ①、②に対応する仕様書記載例]**
- 当該機器等の製造工程の履歴に関する記録を含む製造工程の管理体制が適切に整備されていること。また、当該管理体制を証明する資料を提出すること。**[4.1 節 ①、②に対応する仕様書記載例]**
- 機器等に対して不正な変更が加えられないように製造者等が定めたセキュリティ確保のための基準等が整備されており、その基準等が当該機器等に適用されていること。また、それらを証明する資料を提出すること。**[4.1 節 ①、②に対応する仕様書記載例]**

- 機器等の設計から部品検査、製造、完成品検査に至る工程について、不正な変更が行われないことを保証する管理が一貫した品質保証体制の下でなされていること。機器に不正が見つかったときに、追跡調査や立入検査等、【府省庁名】と迅速かつ密接に連携して原因を調査し、排除できる体制を整備している生産工程による製品であること。
- 情報システムを構成する要素（ソフトウェア、ハードウェア）に対して不正な変更があった場合に識別できる構成管理体制が確立していること。また、当該構成管理体制が書類等で確認できること。**[4.1 節 ③に対応する仕様書記載例]**
- 受託者が情報システムを構成する要素（ソフトウェア、ハードウェア）として採用した機器等について、不正な変更が加えられていないことを検査する体制が受託者において確立していること。また、当該検査体制が書類等で確認できること。**[4.1 節 ②に対応する仕様書記載例]**