デジタル社会推進実践ガイドブック DS-203

政府情報システムにおけるサイバーセキュリティに係る

サプライチェーン・リスクの課題整理

及び その対策のグッドプラクティス集

2025（令和 7）年 6 月 19 日

デジタル庁

〔ドキュメントの位置付け〕

Informative

参考とするドキュメント

〔キーワード〕

サプライチェーン・リスク、ビジネスサプライチェーン、サービスサプライチェーン、ソフトウェアサプライチェーン

〔概要〕

本書は、政府情報システムの関係者が政府情報システムにおけるサプライチェーンに起因するセキュリティインシデント等の発生リスクを低減し、政府情報システムのセキュリティ水準を向上させることを目的として、政府情報システムに関連する主要なサプライチェーン・リスクとそのセキュリティ対策を説明する。

改定履歴

改定年月日	改定箇所	改定内容
2025年6月19日	-	初版決定

目次

１　はじめに

本書は、政府情報システムの機器調達等におけるサイバーセキュリティに係るサプライチェーン・リスクについて理解を深め、適切に対応するため、その課題整理とセキュリティ対策におけるグッドプラクティスを示す。

１．１　目的

本書は「デジタル社会推進標準ガイドライン」におけるセキュリティに関する技術レポートと位置づけており、政府情報システムの開発や運用業務に従事する関係者に対して、政府情報システムの機器調達等におけるサイバーセキュリティ上の主要なサプライチェーン・リスクに関してその背景や影響等を説明し、各リスクへのセキュリティ対策のグッドプラクティスを示すことで、サプライチェーン・リスクに関する理解を深め、適切な対応に資することを目的とする。

なお、サプライチェーン・リスクを含めた政府情報システムに関する網羅的なセキュリティ対策については、政府機関等が講ずるべき情報セキュリティ対策のベースラインとして内閣サイバーセキュリティセンター（NISC）から公開されている「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」[i]及び「統一基準適用個別マニュアル群」などの関連文書に記載されている。

政府情報システムの開発や運用業務に従事する関係者は、本書に記載されている内容を参照し、政府情報システムの機器調達等におけるサプライチェーン・リスクへのセキュリティ対策を行うことで、サプライチェーンに起因するセキュリティインシデント等のリスクを低減でき、政府情報システムにおけるセキュリティ水準の向上に努めることが期待される。

１．２　適用対象

本書は、政府情報システムを適用対象として想定している。

１．３　位置づけ

本書は、標準ガイドライン群の Informative（情報提供）のレベルの参考文書である。

１．４　本書の構成

第２章では、サプライチェーン・リスクに関連する社会的な情勢や、サプライチェーン・リスクへのセキュリティ対策の必要性について言及するとともに、サプライチェーン・リスクの分類とその定義について解説する。なお、第２章は、第３章以降を読み進める際の前提となるため、留意すること。

第３章では、サプライチェーン・リスクへの対応にあたって、どのような政府情報システムにおいても対応が求められる実施事項を記載する。サプライチェーン・リスクへの対応にあたっては、まず、本章の内容を認識することに留意すること。

第４章では、第２章の政府情報システムにおけるサイバーセキュリティ上のサプライチェーン・リスクの分類に従って、分類ごとに想定される、主要なサプライチェーン・リスクの概要とそのセキュリティ対策を記述する。主要なサプライチェーン・リスクの選定については、政府情報システムへの監査やセキュリティに関する支援を通じて特に重大な影響を及ぼす可能性や発生頻度が高いと考えられるリスクや、世の中で発生した具体的なサプライチェーン関連の事例を踏まえた。また、セキュリティ対策については、技術的対策だけではなく管理的対策等も重要となるため、複数の観点から必要な対策を記載する。読者は、本章を基に自らの担当業務等のセキュリティ対策を見直すことで、サプライチェーン・リスクの低減が期待される。

１.５　用語

本書において使用する用語は、表１及び本書に別段の定めがある場合を除くほか、標準ガイドライン群用語集による。その他専門的な用語については、民間の用語定義を参照すること。

表１　用語の定義

用語	意味
サプライチェーン	サプライチェーンとは、一般的に、製品やサービスが原材料の調達から生産、加工、流通、販売を経て、最終消費者に届くまでの一連の流れを指す。本書では、政府情報システムに関連するサプライチェーンを対象とし、機器、ソフトウェア、クラウドサービス等の開発から納入までの一連の工程やその関連企業等に加え、政府情報システムのライフサイクル全般に関わる関連企業等についても、サプライチェーンとする。
政府情報システムの機器調達等におけるサイバーセキュリティ上のサプライチェーン・リ	本書では、政府情報システムの機器調達、外部委託、クラウドサービス選定等におけるサプライチェーンに関するサイバーセキュリティリスクを取り扱う。例えば、サードパーティ製の機器を調達する際の製造元に関するサイバーセキュリティリスク、外部委託先の管理に関する

用語	意味
スク	サイバーセキュリティリスク、クラウドサービスの運用に関するセキュリティリスクなどがある。

2　政府情報システムにおけるサプライチェーン・リスクの概要

2.1　サプライチェーン・リスクの情勢

政府情報システムに限らず、情報システムの構築・運用・保守においては、サードパーティ製の機器やソフトウェアの利用だけでなく、業務委託や各種サービスの活用など、自組織のみで対応することが難しい場合に、専門の外部事業者に依頼することがある。これらの外部事業者やその従業員はすべてサプライチェーンの一部と見なされる。特に近年ではクラウドサービスの利用が前提となり、サプライチェーンが一層拡大している。

その結果、表２に示すように、サプライチェーンに起因するセキュリティインシデントが多発しており、その被害も日々拡大している。

表２　サプライチェーンに起因するセキュリティインシデント

関係するサプライチェーン	事例内容
委託先	2022 年 10 月、大規模な医療機関においてサイバー攻撃によりランサムウェアに感染し、電子カルテを含む情報システムが停止する事態となった。この攻撃は、委託先のシステムを経由して侵入され、院内の他のシステムへと被害が拡大した。その結果、救急診療や外来診療、予定手術の停止を余儀なくされ、診療機能の復旧には約 2 ヶ月を要した。(機密性、可用性、完全性の損失)
クラウドサービス	2019 年 12 月、あるクラウドサービスが障害を起こし、全国の複数の自治体で住民票の発行や戸籍証明書の交付などの行政サービスが停止した。原因はストレージ装置のファームウェア不具合によるハードウェア故障で、復旧までに約 1 週間を要した。(可用性の損失)
ソフトウェア	2020 年 12 月、ある IT 管理ソフトウェア企業のネットワーク監視製品がサイバー攻撃を受け、アップデートにバックドア型マルウェアが仕込まれた。このマルウェアにより、約 18,000 の組織が影響を受け、海外政府の重要機関のシステムも侵害された。(機密性の損失)
委託先	2018 年２月、ある公的機関が、個人情報のデータ入力業務を国内の業者に委託したが、その業者が許可なく海外の業者に再委託し、個人情報が海外に渡っていたことが発覚した。(機密性の損失)

２.２　サプライチェーン・リスクへのセキュリティ対策の必要性

表２の事例が示すように、自らの組織や情報システムのセキュリティ対策のみならず、サプライチェーン全体のリスクも考慮した上で、適切なセキュリティ対策を実施しなければ、結果的に自らにまで悪影響が及ぶことになる。そのため、政府情報システムにおいても、表３に代表されるサプライチェーン・リスクに起因する大規模な攻撃や事故等に備えて、様々な観点で十分なセキュリティ対策を実施することが求められる。

さらに、様々な情報システムやモノが繋がる時代において、サプライチェーン・リスクの影響は特定の機関に限定されず、複数機関、ひいては政府全体にまで波及する可能性を懸念し、多層でのセキュリティ対策を実施することが求められている。

また、サプライチェーン・リスクは、経済安全保障分野においても想定されている。「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（令和４年法律第 43 号）に基づく「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針」[ii]では、特定妨害行為[1]の例示として、我が国の外部から特定社会基盤役務の安定的な提供を妨害しようとする主体の影響を受けた特定重要設備又は構成設備の供給者が、当該特定重要設備に不正なプログラムを埋め込み、そのプログラムにより当該特定重要設備の機能を停止させ、又は低下させる行為といったものなどが挙げられている。

以上を踏まえると、サプライチェーン・リスクへの対応を喫緊の課題として認識し、実施することは極めて重要である。

表３　サプライチェーン・リスクに起因する影響例

影響例	内容
データ漏えい	悪意ある攻撃者が脆弱性を悪用し、機密情報や個人情報、顧客データにアクセスすることで、データが外部に漏えいする可能性がある。また悪意ある作業従事者がアクセスすることで、同時に外部に漏洩する可能性がある。これらにより、組織の信用失墜や法的な問題が発生するおそれがある。
サービス停止（ダウンタイム）	脆弱性を利用した攻撃により、サービスが一時的または長期にわたって停止する可能性がある。これにより、ユーザのアクセスが遮断され、組織の信頼性が損なわれるとともに、経済的損失も乗じるおそれがある。

[1] 特定重要設備の導入又は重要維持管理等の委託に関して我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為をいう。

不正な操作や改ざん	攻撃者が脆弱性を悪用してシステム内に侵入し、データの改ざんや操作を行うことで、システムの品質や正確性が損なわれる危険性がある。特に行政機関では、改ざんによって国民に誤った情報が流布される等の被害が大きな影響となるおそれがある。
攻撃の踏み台化	脆弱性を利用した攻撃により、自組織のシステムが他のシステムやネットワークへの攻撃の踏み台として利用される可能性がある。これにより、サプライチェーン全体に悪影響が及び、取引先や顧客に対する信用を損なうおそれがある。
法的責任と罰則	個人情報や機密情報が漏洩した場合、関連する法律や規制（例：GDPR、個人情報保護法など）に違反し、罰金や制裁措置が科される可能性がある。さらに、被害者からの訴訟に発展するおそれがある。
行政機関の信用の毀損	サイバー攻撃を受けたことが公表されると、行政機関の信用が大きく損なわれ、利用者離れが起きる可能性がある。特に大規模な個人情報漏えいが発生した場合、行政機関が推進・運営する事業や行政サービスの継続にも影響を及ぼすおそれがある。
社会的な混乱	インフラ系のシステムや行政サービスで脆弱性が悪用された場合、社会的混乱を招く可能性があり、組織の対応が遅れれば遅れるほど国民が必要なサービスを利用できない等の被害が拡大する可能性がある。

２.３　政府情報システムにおけるサプライチェーン・リスクの分類と定義

本書では、政府情報システムにおけるサプライチェーン・リスクの分類と定義について、「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」でサプライチェーン・リスクに言及している「第４部　外部委託」において、業務委託、クラウドサービス、機器等の調達に分けて遵守事項等が定められていることを基に、政府情報システムの開発や運用業務に従事する関係者、システムの構成要素、サプライチェーンに関するインシデント事例などを考慮した。

以上を踏まえ、政府情報システムにおけるサプライチェーン・リスクを、表４のとおり、３つに分類して定義する。

表４　政府情報システムにおけるサプライチェーン・リスクの分類と定義

リスクの分類	定義

ビジネスサプライチェーン・リスク	政府情報システムの開発・運用・保守等の業務を請け負う委託先や再委託先（それ以降も同様）に関連する、内部不正による情報漏えいやマルウェア感染等のサイバー攻撃による事業停止等が発生するセキュリティリスク
サービスサプライチェーン・リスク	政府情報システム等で利用する事業者によって提供されるクラウドサービスに関連する情報漏えい、業務停止等が発生するセキュリティリスク
機器・ソフトウェアサプライチェーン・リスク	政府情報システムで利用するソフトウェアやハードウェアに含まれるバックドアや致命的な脆弱性が悪用され、システムへの不正アクセスやマルウェア感染等のサイバー攻撃を受け、情報漏えい、業務停止等が発生するセキュリティリスク

３　サプライチェーン・リスク対応における必須事項

第２章では、政府情報システムにおけるサプライチェーン・リスクの概要を記述し、サプライチェーン・リスク対応の必要性を示した。

本章では、サプライチェーン・リスク対応にあたり、効果的なセキュリティ対策を実施するためにまず取り組むべきと考えられる事項を記述する。

３．１　総合的なリスクアセスメントの実施

サプライチェーン・リスクは、本書でもビジネスサプライチェーン・リスク、サービスサプライチェーン・リスク、機器・ソフトウェアサプライチェーン・リスクの３つに分類したとおり、異なる領域にまたがる。また、サプライチェーン・リスク以外でも、様々なセキュリティリスクがある。そのため、サプライチェーン・リスク以外のリスクも含めて、政府情報システムに係るリスク全体に関する総合的なリスクアセスメントを確実に実施することが重要である。特に、業務委託先やクラウドプロバイダなどの外部の機関が関与する場合、その相手先でのセキュリティ対策などを適切に把握することが求められる。なお、リスクアセスメントについては、「政府機関等の対策基準策定のためのガイドライン」[iii]、「DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン～ベースラインと事業被害の組み合わせアプローチ～」[iv]などの政府機関等向けのリスクアセスメントに関する基準やガイドラインを参考にされたい。

３．２　委託先等との協力体制の強化

サプライチェーン・リスクを軽減するためには、委託先、サプライヤー、サービス提供者などとの緊密な協力が不可欠である。契約書の中に情報セキュリティ条項を明確に盛り込むだけでなく、定期的なリスクレビューの実施や緊急時を含めた連絡体制の確立も重要である。また、委託先等のセキュリティ体制やインシデント対応能力を評価し、必要であれば改善を促す取組が必要である。

これらの取組を効果的に実施するためには、日々のコミュニケーションを通じて信頼関係を構築・強化し、効率的な協力体制を構築することが重要である。

３．３　継続的な監視と評価の重要性

サプライチェーン・リスクは動的なものであり、技術の進化や新たな脅威の発生により、リスクの性質や影響範囲が変化することがある。そのため、初回のリスク評価や対策実施にとどまらず、継続的な監視と再評価を行うことが重要である。特に、新しい機能の導入や既存のサービスのアップデートが行われた際などには、速やかに既存のリスクを含めて、リスク評価を更新するプロセ

スを設けることが有効である。また、併せて、リスクに関する情報を集約し、関係者全体で共有することができる体制構築も重要となる。

３．４　インシデント対応計画の整備

サプライチェーン・リスクが顕在化した場合の対応を適切に行うために、あらかじめインシデント対応計画を整備しておくことに留意する必要がある。インシデント対応計画には、インシデントの検知、報告、対応、復旧の手順を明確に定め、委託先等の関係者との協力体制を事前に整えておく必要がある。また、インシデント対応計画は定期的に見直し、演習を通じて関係者が迅速に対応できるようにしておくことが重要である。

３．５　まとめ

サプライチェーン・リスクへの対応は、組織内外を問わず、多くの関係者との協力と継続的なリスクマネジメントが必要である。総合的なリスクアセスメントの実施、業務委託先等との協力体制の強化、継続的な監視と評価、そして、インシデント対応計画の整備といった取組に留意しながら進めることで、より堅牢なサプライチェーン・リスク管理体制を構築することが可能である。

これらの取組が、次章に記述する各セキュリティ対策がより効果的なものとなり、政府情報システムにおけるセキュリティ水準の向上に努めることが期待される。

４　想定される主要なサプライチェーン・リスクと対策

本章では、第２章で分類、定義したサプライチェーン・リスクに基づいた主要なリスクとそれに対するセキュリティ対策を記述する。なお、セキュリティ対策については、技術的対策のみならず管理的対策など複数の観点から分類している。

４.１　ビジネスサプライチェーン・リスク

昨今、委託先に関連するセキュリティインシデントの事例が数多く報告されている。2023 年には、大手通信事業者グループの子会社において、委託先の元派遣社員が約 10 年間にわたり、システム管理者権限を悪用して数百万人分の個人情報を不正に持ち出し、第三者に販売していたことが判明した。このセキュリティインシデントは、長期間にわたり事案が検知できなかったことや、初回の調査では情報漏えいを確認できていなかったことなど、サプライチェーンである委託先におけるリスクに関して多くの要素を含んでいる。

この事例からもわかるように、業務委託においては、委託先がシステムにおける上位の権限を付与され、重要な情報を扱うこともある。付与された権限で実行可能な行為は、全て不正に繋がるリスクがあると考えられる。その場合、委託先でのセキュリティ管理が不十分であれば、情報漏えいや不正アクセスなどのセキュリティインシデントが発生し、委託元にも大きな影響を及ぼす。そのため、委託先におけるリスクを把握し、リスクを軽減等するためのセキュリティ対策を実施することが必要である。

なお、ビジネスサプライチェーン・リスクについて検討する際には、ビジネスリスクへの対策を検討する際のフレームワークとしても引用されることが多いアメリカ国立標準技術研究所（NIST：National Institute of Standards and Technology）が発行する「The NIST Cybersecurity Framework（CSF）2.0[v]（以下「CSF」という。）のカテゴリーを当てはめて、検討することができる。具体的には、委託業務に関連するリスクは、全般的な「統制（Govern)」の観点から、組織のリスクとして捉え、どのように対策を実施するか、組織のリスク管理の戦略を当てはめて考える必要がある。委託先に対しては、リスク対策の内容だけではなく、リスクの発生頻度、業務影響などリスク管理に関する情報を共有する必要がある。また、委託業務に関連して保護すべき資産に対する脅威と影響を「識別（Identify)」し、そのリスク評価結果に応じた事前の「防御（Protect)」策、攻撃や不正に繋がる異常を「検知（Detect)」するために監視や記録の分析、実際にセキュリティインシデントが発生した際の「対応（Respond)」に必要な体制やコミュニケーション、破壊または紛失した資産の「復旧（Recover)」等、セキュリティ対策について委託先に求める役割権限を

含めて検討する。

こうしたフレームワークを活用して組織内で検討したセキュリティ対策は、委託業務を調達する際に仕様書のセキュリティ要件に含めるとともに、一般競争入札（総合評価落札方式）やプロポーザル型企画競争における評価基準として委託業務を遂行するための能力とセキュリティ水準に関する項目を加え、セキュリティ対策を確実に実施可能か評価する必要がある。さらに調達時のみならず、委託業務期間中での継続的なセキュリティ水準の維持のため、委託元が継続的に委託先におけるセキュリティ対策の実施状況を確認することも重要である。

本項では、委託先に関連したビジネスサプライチェーン・リスクにおける主要なリスクについて、その特性や影響を説明し、リスクを軽減するための対策を提案する。

1)委託先における管理不備のリスク

ア　リスク概要

a)背景

① 情報システムを構築・運用・保守する際に、組織内の専門的な知識や工数を補うため、外部の専門性の高い事業者に委託することがある。また、情報システムの構築・運用・保守とは関係なく、業務自体を委託することがある。どちらも、委託業務を遂行するために、委託元が保有する情報を委託先に対して、提供しまたは情報の権限管理を付与することにより、委託先は機密性が求められる情報を知ることが可能となる。

② 委託元との通信か否かに関わらず委託先に付設されたネットワークにおいて、セキュリティ設定やネットワーク機器の管理に不備がある場合、それらの不備を狙った攻撃や委託先を起点としたセキュリティインシデントが起き、委託元にも二次的な被害が及ぶ可能性がある。例えば、一時的な通信許可の設定を元に戻すことを失念したことで、不正アクセスを受けることや、マルウェアを受信することが考えられる。

b)想定される影響と結果

委託業務のために委託先に提供した情報や、委託先において委託業務に従事する職員（以下「委託業務従事者」という。）が知り得る情報は、個人情報、機微な情報または重要な情報である場合が多く、委託先においても安全に保護されなければならない。しかし、委託先におけるセキュリティ対策が不十分な場合、これらの情報が、委託業務従事者以外の委託先の職

員を含めた第三者に漏えいすることがある。

イ　リスクへの対策

a)管理的対策

- 委託元の情報セキュリティポリシーに加え、委託業務のリスクを考慮したセキュリティ対策の要件を、調達仕様書に加える。
- 契約時に、委託先から、情報の適正な取扱いのための情報セキュリティ対策が含まれた計画書の提供を受ける。
- 委託期間中、調達仕様書で求めたセキュリティ対策と委託業務の実施状況に合わせて、定期的に上記計画書に記載された事項の実施状況の報告を受ける。
- 情報が取り扱われる前に、セキュリティ対策が十分であるか立ち入り調査を実施し、その際に確認された課題について、改善を要求する。（「別紙１　立入調査時点検項目例」参照）

2)委託先における内部不正のリスク

ア　リスク概要

a)背景

内部不正自体は、委託先に限らず委託元の組織内でも発生しうるリスクであるが、委託先における内部不正については、委託元が直接その職員を管理していないことから、発見が困難である。特に、属人的に業務が実施されている場合、他の業務従事者による実施内容の確認や評価などのけん制ができず、不正行為が起こりやすく、発見することも難しい。

さらに、委託業務においては、技術的に専門性が高い業務を委託することが多く、そのような場合、委託元が委託先の組織内で行われた委託業務従事者による不正を発見することは、専門性の高さも相まって、一層困難である。

b)想定される影響と結果

付与された権限で実行可能な行為は、全て不正に繋がるリスクがあると考えられる。

委託先の関係者による情報漏えいや情報の持ち出しといった一次的な被害に加え、個人情報の第三者への転売や、漏洩した組織情報が攻撃者に悪用されることで起こるセキュリティインシデントなどによる二次的な被害も考えられる。機密性に関わるセキュリティインシデントであるため、一次的な被害よりもむしろ二次的な被害の方が業務に与える影響が大きくな

る危険性がある。

また、委託先の関係者による資産の破壊は、可用性に関わるセキュリティインシデントであるため、業務継続や個人情報等情報の主体者の生活等に影響を与えることがある。

イ　リスクへの対策

委託先における内部不正への対策については、委託先で十分な予防的な対策と不正を検知する対策が実施されているかを確認する必要がある。また、委託先でのセキュリティ対策の内容の共有は、内部不正のけん制に繋がる。

a)管理的対策

- 委託業務に関する情報を取り扱う委託業務従事者（以下「情報取扱者」という。）を識別し、その一覧を入手する。
- 情報取扱者には、委託業務従事者に加え、品質管理者等の間接部門において委託業務に関する保護すべき情報に触れる者も含む。
- 情報取扱者は、定期的に異動や退職等による変更がないかを確認する。
- 管理者権限等の特権を保有する情報取扱者を必要最小限とした上で、相互けん制の仕組みを導入し、複数の担当者が互いに監視できる体制を整える。

b)技術的対策

- 情報取扱者の一覧に基づき、委託先において、委託業務に関する保護すべき情報の保存先やシステムのアクセス権限を限定する。
- 情報のコピーやダウンロードなど情報の持ち出しに繋がる機能は、一度に多量の情報を扱えないように制限し、記録を取得する。
- 委託先に対して、委託業務に関する保護すべき情報へのアクセスや操作の記録を複合的に分析し、不審な操作を定期的に確認した結果の報告を求める。

3)委託先のセキュリティインシデントによる二次被害の可能性

ア　リスク概要

a)背景

委託先においてセキュリティインシデントが発生した場合、メディアやSNS 等に取り上げられることにより、委託先への信頼性に対するイメージが低下する。

委託先については、調達に関する公開情報により明らかになっているため、委託先のセキュリティインシデントが直接、委託業務に関連していな

い場合でも、委託元の信用に悪影響を及ぼす可能性がある。特に、委託先のセキュリティインシデントがセキュリティ対策の不足や管理の甘さに起因している場合、委託元の選定基準も疑問視されることになる。

b)想定される影響と結果

委託元は、外部からの問い合わせ対応を求められることや、委託先の選定基準と評価の根拠を求められる可能性がある。これに加え、委託先と調査方法、調査結果、報告、公表等の協議にも時間が取られる。

また、委託先ではセキュリティインシデントの対応工数が負担となり、委託業務の遂行において、リソースが制限されることや遅延が生じることなど、影響が生じる可能性がある。例えば、委託先でのセキュリティインシデントが委託業務にも使用していたツールに関係していた場合、そのツールが利用できなくなるケースがあり、委託元としても委託先との情報管理方法やコミュニケーション方法を変更することとなる。

イ　リスクへの対策

a)管理的対策

- 委託先の選定にあたり、一般的な選定基準だけではなく、委託業務のリスクに応じた委託先の選定基準を作成し、公正に評価する。
- 委託先においてセキュリティインシデントが発生した場合、外部からの問い合わせ対応のために、セキュリティインシデントが委託業務に直接関係していることが判明していない状況でも早期に委託先から一報を入手する。
- 被害の拡散防止や公表に向けた協議を行うため、両者間でセキュリティインシデント対応時の体制を事前に確立する。
- セキュリティインシデントにより委託業務上で使用できなくなる可能性があるツール、情報システム等は、業務継続計画（BCP）を事前に合意する。
- 業務手順について、代替業務手順（コンティンジェンシープラン）を事前に定める。

委託業務に関連して委託先が使用するツール等がクラウドサービスやソフトウェアである場合のリスク対策については、「４．２　サービスサプライチェーン・リスク」及び「４．３　機器・ソフトウェアサプライチェーン・リスク」の項で示す。

4)未承認の再委託やオフショアのリスク

ア　リスク概要

a)背景

委託先が保有している人的リソースや知識、経験が不足している場合、委託元によって承認されていない再委託や、オフショア[2]によって補われることがある。なお、委託業務の作業場所が海外となった場合は、国内法が及ばず、逆に現地国の法に対応しなければならないといったカントリーリスクが存在する。

b)想定される影響と結果

オフショアがある場合、作業場所となる国において、何らかの理由により海外に持ち出された情報が現地国の機関から提出するよう求められることが考えられ、これによる情報漏えいの可能性がある。

また、未承認の委託先やオフショアがある場合は、どちらの場合でも、作業場所への委託先に対する監査の実施が難しく、作業場所や使用する機器などのセキュリティ対策状況が確認できない。結果的に、調達仕様書のセキュリティ要件が満たされていない場合、外部からの攻撃により情報漏えいする危険性がある。例えば、使用されるネットワーク機器の脆弱性管理が不十分であったため、サイバー攻撃によりネットワーク機器の脆弱性を突かれ、委託先のシステムに侵入され、情報が漏えいするなどが考えられる。

また、未承認の再委託先で取り扱っていた情報は、契約終了時のデータ消去の対象範囲から漏れる可能性がある。このような状況で契約に違反した再委託先に保存されていた情報が漏えいすることが考えられる。

イ　リスク対策

a)管理的対策

- 委託業務を実施する上で必要な保有資格を調達仕様書に盛り込む。
- 調達時において、応札者の処理能力や保有する人的リソース等の体制を評価することにより、不適切な委託となる可能性を下げる。
- 委託先への監査等により、委託業務従事者リストに記載された委託業務従事者の保有資格、作業場所、在籍状況等を確認し、委託業務を遂行する能力が十分であることを確認する。
- 機微な情報を取り扱うシステムの開発・運用においては、海外法人

[2] 委託先が、自社内の国外拠点で委託業務を実施すること、または、国外のグループ企業等の関連会社に業務を再委託すること

（委託先の関連法人を含む）へのオフショアについて、当該海外法人に対する情報へのアクセスや保存等の制限、セキュリティ対策とその実施状況の確認において、条件を設定する。

5)曖昧な責任分界によるリスク

ア　リスク概要

a)背景

委託元及び委託先は、委託業務を実施し、その目的を達成する上で、それぞれが果たすべき責任について合意し、お互いに理解しなければならない。

また、責任がそれぞれに分担されるため、委託元と委託先との間でセキュリティ対策の連携が重要となる。

b)想定される影響と結果

委託元と委託先によって合意された本来の役割が実施されなかった場合、委託業務に遅延などの影響が起きるだけではなく、責任範囲の不明瞭さから生じる不満が引き金となり、内部不正による情報漏えいや改ざんに繋がる危険性がある。

イ　リスク対策

a)管理的対策

- 委託先に対して、委託業務に伴うリスクとその影響の評価、責任分界点を共有する。
- 委託先への監査により、委託業務を実施する上で充分なリソースが確保された業務実施体制であることを確認する。
- 委託先においても、委託元の情報セキュリティポリシーと同等以上のセキュリティ対策が実施され、情報セキュリティ体制が構築されていることを確認する。

４.２　サービスサプライチェーン・リスク

現代のビジネスにおいて、クラウドサービスやマネージドサービスを利用することは、企業の業務効率化と競争力強化に必要不可欠な要素となっている。これらのサービスを通じ、企業は、例えば、オンプレミスのサーバを維持するコストを削減し、IT 管理にかかる負担を減らすことで、社員が自社の主要業務により専念できるようになる。

他方、政府機関においては、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2021 年（令和３年）３月 30 日各府省情報化統括責任者（CIO）連絡会議決定）のもと、クラウドバイデフォルト原則を掲げ、情報システムの環境をオンプレミスからクラウドへ移行してきた。その上で、さらなるクラウドサービスなどによる利用メリットを享受するため、同方針を抜本的に見直した「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」（2023 年（令和５年）９月 29 日デジタル社会推進会議幹事会決定。以下「新方針」という。）[vi]のもと、単にクラウドサービスを利用するだけでなく、「適切な利用」を推進しているところである。

しかし、これらのサービスは多大なるメリットもある一方で、統制が難しい領域があるなど新たなリスクも生じさせる。

本項では、クラウドサービスやマネージドサービスに関連した「サービスサプライチェーン・リスク」における主要なリスクについて、その特性や影響を説明し、リスクを軽減するための対策を提案する。

なお、本書で説明しているセキュリティ対策に資する制度として、「政府情報システムのためのセキュリティ評価制度」（Information system Security Management and Assessment Program:通称、ISMAP（イスマップ））[3]がある。政府機関は、原則として、ISMAP により安全性が評価された「ISMAP クラウドサービスリスト」または「ISMAP-LIU クラウドサービスリスト」（以下「ISMAP 等サービスリスト」という。）に掲載されたサービスから調達することとされている。ただし、ISMAP 等サービスリストに掲載されていることだけで判断せず、その詳細情報を調達時等のリスク評価に活用することが重要である。

[3] 政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とする。

1)役割・責任範囲の理解・認識不足のリスク

ア　リスク概要

a)背景

クラウドサービスでは、サービス提供者と利用者の間で責任が共有される責任共有モデルが採用されている。オンプレミス環境では、情報システム全体の管理は利用者が直接行うが、クラウドサービスでは提供者と利用者がそれぞれの責任を分担する形になる。

したがって、クラウドサービスは、利用者にとって柔軟なスケーラビリティと運用負荷の軽減という利便性がある一方で、利用者側でセキュリティ設定やデータ管理を適切に行うことの重要性が高まる。この責任共有モデルでは、どの部分がサービス提供者の責任であり、どの部分が利用者の責任であるかが明確に定義されている。具体的な責任範囲は各クラウドサービスの利用規約や契約内容などによって異なる場合もあるが、例えば、SaaS においては、物理的なインフラストラクチャの管理はクラウドサービスプロバイダ（以下「CSP」という。）の責任だが、データの管理や適切なアクセス制御の設定は利用者の責任となる。

このように、クラウドサービスではCSP と利用者の両方がそれぞれの役割を担うことで、全体的なセキュリティ水準が保証される。

b)想定される影響と結果

クラウドサービスの利用において、サービス提供者と利用者の責任範囲を十分に理解・認識していない場合、重大なセキュリティ対策の漏れが生じる可能性がある。例えば、CSP が対応すると誤解して、利用者が実施すべき必要なセキュリティ設定が未実施となるケースが考えられる。このような状況は、セキュリティホールを生じさせ、攻撃者に悪用されるリスクを高める。その結果、政府の機密情報や国民の個人情報が漏洩し、国家安全保障や個人のプライバシーが脅かされるおそれがある。

また、インシデント発生時において、どちらがどう対応を実施すべきかを確認する時間が必要となり、対応に遅れが生じ、結果として被害の拡大を招く可能性がある。

さらに、必要なセキュリティ対策の不足やコンプライアンス要件の未達成を引き起こし、規則違反を問われるリスクがある。このような不備は、組織のガバナンス体制の問題と見なされ、政府機関の信頼性を損ね、結果的にサービスの利用率低下に繋がるおそれがある。

イ　リスクへの対策

a)管理的対策

・　サービス内容の変更時など、CSP がウェブサイトなどで提示する責任範囲を確認する。

b)人的対策

・　利用者側の担当職員への役割や責任範囲に関する教育を実施する。

c)その他の対策

・　サービス検討時にサービス内容、規約などを確認し、要求事項を満たすかあらかじめ検証する。
・　独立した第三者機関による定期的な監査を実施し、責任範囲の理解と遵守状況を客観的に評価する。

2)クラウドサービスにおける障害など可用性のリスク

ア　リスク概要

a)背景

政府情報システムには国民生活に直結する重要な行政サービスを提供するシステムが含まれており、高い可用性が求められる場合がある。一方、クラウドサービスでは、利用者のみならず、CSP が責任を持ち管理運用する領域が存在し、CSP の管理運用に起因する障害、クラウドサービス自身がサイバー攻撃の標的になるなどの CSP にとっての外部要因に起因する障害にも考慮する必要がある。

また、クラウドサービスでの可用性確保は、一般的にはインターネットを介して利用することからネットワークの安定性の影響や、クラウドサービスにおけるサービスや機能の提供内容や状況が影響することが特徴である。なお、提供されるサービスが標準化されている場合は、利用者からの個別の要求を柔軟に反映することが難しいこともある。

b)想定される影響と結果

上記のとおり、クラウドサービスには、外部要因によるクラウドサービス自身の障害や停止、または通信回線の不調といったリスクが存在する。例えば、クラウドサービスのデータセンターにおいてハードウェア障害が発生した場合、サービスの一部が利用不能となり、影響を受ける可能性がある。また、DDoS 攻撃などの悪意ある攻撃によりクラウドサービスへのアクセスが妨害されることや、通信回線の不調によりクラウド環境へのアク

セスが困難となることも考えられる。

これらの障害や停止により、政府情報システムや行政サービスに深刻な影響が生じる可能性がある。例えば、クラウドサービスが停止した場合、重要なシステムが利用不能となり、行政手続が遅延し、国民へのサービス提供が著しく妨げられることが懸念される。特に、社会保障や税務手続に関連するシステムが停止した場合、国民の生活に直接的な支障をきたし、混乱が発生するリスクが高まる。

さらに、内部事務などで利用しているクラウドサービスにアクセスできない状況となると、通常業務の遅延や効率の低下を招くことになる。この結果、復旧作業や原因究明に多大な人的・金銭的リソースを要し、最終的には政府機関の信頼性が低下する事態に発展するおそれがある。

イ　リスクへの対策

a)管理的対策

- CSP が提示するサービスレベルを確認し、必要とする可用性を確保できるかを確認する。また、可能であれば個別にサービスレベルアグリーメント（SLA）を締結することで、可用性の目標値を明確に定義する。
- CSP が公表するサービス稼働時間などの可用性レポートを定期的に確認し、想定されるリスクを評価し、必要に応じて対策を見直す。
- 障害が発生した場合に備え、サービス中断時の代替手段などを検討のうえ、業務継続計画（BCP）を整備する。

b)技術的対策

- 複数のリージョンやアベイラビリティゾーンに渡ってシステムを分散配置するなど、冗長化構成とする。
- 自動的にバックアップシステムに切り替わる仕組みを導入する。
- 特に高い可用性を要求する場合、複数のクラウドサービスを利用するマルチクラウド戦略や、オンプレミス環境などと併用するハイブリッドクラウド構成を採用する。

c)人的対策

- 可用性に影響を与えるインシデントを想定した訓練を定期的に実施し、業務継続計画（BCP）やインシデント対応手順への対応力を向上させる。
- 障害発生時に迅速に対応できる体制を構築する。

d)その他の対策

・　障害発生時に備え、組織内でのインシデント対応に必要な情報を、CSP がウェブサイトなどで提示する情報等を基に確認する。

3)適切な設定が実施されないリスク

ア　リスク概要

a)背景

クラウドサービスは多くのサービスがある一方で、その分、多くの設定項目が存在し、管理は複雑になる。特に、クラウドサービスでは、アクセス制御、ネットワーク設定、暗号化設定などのセキュリティに関する設定なども含めて、従来のオンプレミス環境とは異なるクラウドサービス固有の名称や機能であることも多い。さらに、クラウドサービスは頻繁にアップデートされることが多く、その際に設定がデフォルト値に戻ることや新機能が追加されることがあるため、これらの変更に対応する必要がある。

また、政府情報システムに限らず、組織のセキュリティポリシー等にのっとった設定が必要となるが、利用者が設定する責任範囲については、クラウドサービスの利用形態（IaaS、PaaS、SaaS）によっても責任範囲が変化することに加え、サービスの内容や利用条件等によっても異なる。

b)想定される影響と結果

クラウドサービスを利用する際には、設定不備が発生する原因がいくつか存在する。まず、クラウドの設定に不慣れであるため、アクセス権限やネットワーク設定において誤りや抜けが生じやすくなる。また、IaaS、PaaS、SaaS といったサービスの種類によって管理する責任範囲が異なるため、利用者がどの範囲を管理すべきか判断しづらく、結果として設定が不十分になることがある。さらに、クラウドサービスは頻繁にアップデートされるため、その対応が遅れることや設定変更に気付かないことなどミスが発生しやすくなる。加えて、設定作業が手作業で行われることが多いため、ヒューマンエラーが起こりやすく、設定作業の煩雑さや多忙な状況によって誤設定のリスクが高まる。

こうした設定不備が発生すると、重大なセキュリティホールが生じ、組織に大きな影響を及ぼす可能性がある。例えば、誤ったアクセス権限の設定により、本来アクセスできないはずの機密情報に外部から不正にアクセスされるおそれがある。また、内部システムが誤ってインターネットに公開されることでサイバー攻撃の標的となりやすくなり、重要なデータの改ざんや破壊のリスクも高まる。さらに、データの暗号化設定が不適切であ

る場合、情報漏えい時の被害が甚大になる可能性がある。これらの問題は、政府情報システム全体のセキュリティを脅かし、連鎖的に重要なデータの改ざんや破壊を引き起こすおそれがある。

また、設定不備は、インシデント対応における対応の遅延や問題の特定を困難にすることにも繋がる。設定不備が原因となり、適切なログ管理や監視体制が整っていない場合、問題解決に多大な時間と労力がかかり、その結果として被害が拡大する可能性が高まる。

イ　リスクへの対策

設定不備のリスクへの対策について、以下のとおり、主要な対策と考えられるものを挙げているが、具体的に推奨されるセキュリティ対策については総務省が公表している「クラウドサービス利用・提供における適切な設定のためのガイドライン」[vii]も参照されたい。

また、対策を検討する際には、潜在的なリスクを事前に予測し、不適切な設定や操作を未然に防ぐための予防的統制と、組織で定めたポリシーの準拠状況（暗号化やログ取得の実施状況、外部公開設定など）やリスクの発生に繋がる操作等を監視して検知し、必要に応じて修正するための発見的統制の考え方[viii]を踏まえることが望ましい。

a)管理的対策

- クラウドサービスのアップデート等の情報を確実に入手するための体制を整備し、必要な設定変更を行えるようにする。
- 設定変更時のレビューと承認プロセスを確立し、管理方法を定める。
- 定期的に、設定に関する自己点検や監査などのセキュリティ評価を実施する。
- ログの監視が可能なマネージドサービスを活用する。[viii]

b)技術的対策

- CSPM（Cloud Security Posture Management）などのクラウドサービスの設定を自動チェックするツールを導入する。
- セキュリティに関する設定のテンプレート化し、強制適用する。
- CSP によって提供されているベストプラクティスに準拠した最新の対策を行う[ix]。
- インシデント発生時の調査に必要な環境を自動的に構築する機能が提供されている場合、当該機能を活用する[x]ことを検討する。

c)人的対策

- 担当職員に対して、クラウドサービスの設定に関する専門的なトレー

ニングを実施する。
・ クラウドサービスに関する最新情報を担当内で共有し、内容を確認する。

d)その他の対策
・ アップデート対応を義務的な改修負担としてイベント的に捉えるのではなく、通常のアップデートと捉えて日常的に対応を行い、適宜、設計の見直しも実施する[xi]。
・ CSP によるクラウドサービスの変更に関する手順や通知事項を事前に確認する。
・ 独立した第三者機関による定期的な監査を実施し、責任範囲の理解と遵守状況を客観的に評価する。

4)国内法以外の法令及び規制が適用されるリスク

ア　リスク概要

a)背景

前述のとおり、クラウドサービスにおける責任共有モデルを踏まえると、クラウドサービスにおける利用者データ（以下「利用者データ」という。）のセキュリティ対策については利用者の責任となる。また、当然のことであるが、利用者データについてはそもそも組織が管理すべき情報となるため、その取扱いを利用者が把握・確認した上でクラウドサービスを利用することが必要不可欠である。利用者データは、クラウドサービスが提供されているデータセンターにあるハードウェア上で物理的に保存される。データセンターは、特に大手事業者になると、世界中のさまざまな場所に分散している場合があり、それらのデータセンターに対しては、設置されているそれぞれの国の法令などが適用されることが一般的である。

b)想定される影響と結果

利用者はクラウドサービスの利用時にリージョンを選択することで自身のデータ保存先を把握・選択できるが、サービスによっては日本国内を選択できない場合がある。そのような場合、利用者データが海外のデータセンターに保存されるため、国内法以外の法令及び規制が適用され、海外の法執行機関の命令によりデータが強制的に開示される可能性がある。

これにより、政府の機密情報や国民の個人情報が意図せず外部に渡り、重大な情報漏えいが発生するおそれがある。ひいては、国家安全保障や個人のプライバシーが侵害されるリスクが高まる。

また、利用するクラウドサービスのデータセンターが設置されている国の政治的・経済的状況により、データアクセス制限や予期せぬ法令変更が発生し、重要な行政サービスの提供に支障をきたす可能性がある。

さらに、海外のデータセンターを利用することで通信の遅延が発生し、リアルタイム性が求められる政府情報システムの性能低下や信頼性の低下を招くおそれがある。

イ　リスクへの対策

a)管理的対策

- データセンターの設置場所に関しては、国内であることを基本とする[xii]。
- 他国である場合は、各国の法令や規制を調査し、コンプライアンスを確保するためのポリシーを策定する。
- データの保存場所や転送に関する規則を明確にし、契約に盛り込む。

b)技術的対策

- 最新の「CRYPTREC 暗号リスト（電子政府推奨暗号)」[4]に掲載されている暗号又は同等の暗号を用いて利用者データの暗号化を行うこと。また、利用者データの機密性によっては、利用者自身の暗号鍵によるデータの保護と鍵管理（クラウドの鍵管理サービス提供の利用者が主体的に管理する鍵の利用や BYOK 等）を行い、CSP や監督権限を持った政府等が利用者データを判読不能とする措置を行う[xii]。
- バックアップデータの保存は、別の地域を選択する。

c)人的対策

- 他国での保存となる場合は、法務部門やコンプライアンス部門にも相談し、国際的な法令遵守を徹底する。

d)その他の対策

- 契約において、データの取扱いや移転に関する条項を明確に定め、リスクを最小限に抑える。

[4] https://www.cryptrec.go.jp/list.html

5)データ消去の不確実性のリスク

ア　リスク概要

a)背景

政府情報システムでは、機密情報や個人情報など、適切に管理・消去すべき重要なデータを扱う。クラウドサービスでは、データはデータセンターやリージョンなどの違いにより複数の物理サーバに分散して保存されることが多く、また、複数のバックアップデータが存在する可能性もある。加えて、CSP がクラウドサービス上の物理的資産を有することが一般的であるため、CSP が定めるデータ消去プロセスを受け入れざるを得ないこともある。これらのことから、クラウドサービスでは、利用者自身でデータを所有することが多いオンプレミス環境と比較して、利用者が自らのデータを完全に消去することや、消去されたことを自身で確認することが困難である。

b)想定される影響と結果

クラウドサービスにおけるデータ消去には不確実性が伴い、データが完全に消去されないリスクが存在する。例えば、物理的に分散保存されたデータの一部が残存する可能性や、複数のバックアップが意図せず残ることで後に復元されるリスクが挙げられる。さらに、データ消去作業やプロセスが CSP 依存している場合、利用者が直接確認することが困難であり、消去が適切に行われているかの確証が難しい。また、データ消去の確実性を証明できなければ、監査や法的要件への対応が難しくなる可能性がある。

これらのようにデータが完全に消去されず第三者に復元された場合、政府の機密情報や個人情報が漏洩し、国家の安全保障が脅かされるほか、個人のプライバシーが侵害されるおそれがある。さらに、データ消去の証明が困難である場合、監査時に証跡を提出できず、規則違反やコンプライアンス違反となる可能性がある。加えて、CSP が定めるデータ削除プロセスにより、個人情報の削除要求に迅速に対応できない場合も考えられる。

イ　リスクへの対策

a)管理的対策

- サービス利用開始前に、約款のデータ削除に関する項目を確認する。
- クラウドサービス上で取り扱うデータ一覧を文書化するなどして把握し、管理する。
- CSP からの情報提供を通じて、データ消去状況を確認する。

b)技術的対策

・ データを暗号化し、削除時には暗号鍵を無効化することで、論理的なデータ消去（暗号消去）も実施する。

c)人的対策

・ データに関する管理体制を整備し、責任と役割を明確化する。

d)その他の対策

・ データ消去プロセスの透明性を重視したクラウドサービスを選定する。
・ CSP に対する外部の監査機関によるデータ消去のプロセスの確認と証明を取得し、内容を確認する。

6)クラウドサービスが利用しているクラウドサービス等に関するリスク

ア　リスク概要

a)背景

クラウドサービス自体が、他のクラウドサービス、基盤、サードパーティ製ソフトウェアなどを利用していることも多く、これらの相互依存関係が複雑なサプライチェーンを形成している。例えば、SaaS プロバイダが IaaS プロバイダのインフラを利用することや、複数のクラウドサービスが連携して機能を提供することが一般的になっている。このように、クラウドサービス間の相互依存関係は複雑化しており、一見して単一のサービスに見えるものでも、実際には多層的なサプライチェーンを形成している。

b)想定される影響と結果

クラウドサービスのサプライチェーンが政府情報システムに波及するリスクが存在する。まず、基盤サービスの障害が最も懸念される。例えば、基盤として利用している IaaS に障害が発生した場合、そのインフラを利用する多数の SaaS サービスが同時に停止し、国民に対する行政サービスの提供が不能となるほか、内部事務業務の実施も困難となる。

また、セキュリティ侵害の連鎖リスクも考えられる。CSP が利用するサードパーティ製ソフトウェアの重大な脆弱性が攻撃者に悪用されることや、下請け業者などのサプライチェーンを通じた不正アクセスやマルウェアの混入により、政府情報システムに影響が及ぶ可能性がある。これにより、情報漏えいが発生した場合、直接的な契約関係がないことから、迅速な対応が困難となり、被害が拡大するおそれがある。

さらに、データ管理の複雑化により、データの所在や保護状況の把握が困難となり、データ消去の確実性が担保できない場合、監査や法的要件へ

の対応が困難となる可能性がある。これらのリスクは、クラウドサービスの停止やセキュリティ侵害を通じて行政サービスの提供に支障をきたし、国家の安全保障や個人のプライバシーを脅かすほか、規則違反やコンプライアンス違反に繋がる可能性がある。

イ　リスクへの対策

a)管理的対策

- クラウドサービスに関連するサプライチェーン全体を把握し、そのリスクを評価する。
- CSP が実施するサプライチェーン・リスク管理状況を把握し、定期的に評価する。

b)技術的対策

- CSP に対して、クラウドサービス間のインターフェースにおけるアクセス制御と監視の状況を確認し、必要であれば、強化を求める。
- 障害が発生した場合に備えた冗長性を確保する。

c)人的対策

- CSP に対して、サプライチェーン・リスクに関する教育を CSP 側の従業員に対して実施するよう求める。

d)その他の対策

- CSP に対する外部の監査機関によるサプライチェーン・リスク評価を取得し、内容を確認する。
- 潜在的リスクがないことを事前に確認する[xiii]。

４.３　機器・ソフトウェアサプライチェーン・リスク

情報システムの開発では、構成要素すべてを自作するのではなく、一部を組織の外部から調達し、それらを組み合わせることがある。外部の既製品やライブラリを活用することで、開発のコストを大幅に削減し、システム開発期間の短縮にもなる。また、幅広く使用され実績がある外部製品は、品質が高いことが期待できる。

このように外部調達を活用した開発アプローチではメリットが多くある一方で、調達した外部製品にセキュリティ上の問題があった場合は、その問題が開発するシステムに組み込まれてしまうというリスクもある。外部製品を使用する際には、システム管理者はセキュリティリスクとその対策を十分に検討する必要がある。

本項では、ハードウェアやソフトウェアなどに関連した「機器・ソフトウェアサプライチェーン・リスク」における主要なリスクについて、その特性や影響を説明し、リスクを軽減するための対策を提案する。

1)外部調達のソフトウェアに内在する脆弱性によるリスク

ア　リスク概要

a)背景

ソフトウェアに脆弱性が存在すると、攻撃者がそれを悪用し、システムやサービスに多大な被害を与える可能性がある。既製品である外部調達のソフトウェアは、多くの組織で共通して利用されることが多いため、一度脆弱性が発見されると、同じ攻撃手法を用いて複数のシステムが攻撃対象となるリスクがある。このため、攻撃者にとって効率的なターゲットとなりやすい状況である。

こうした背景から、システムに組み込まれた外部調達のソフトウェアに脆弱性がない状態を維持することが重要となる。

b)想定される影響と結果

外部調達のソフトウェアの脆弱性を管理するには、自らが担当するシステムにどのようなソフトウェアが組み込まれているかを正確に把握する必要がある。しかし、システムの構成情報が十分に整備されていない、あるいは不備があるケースや、外部調達のソフトウェアに含まれるコンポーネントの詳細が開発者に共有されていないなどの要因によって、外部調達のソフトウェアの脆弱性を正確に把握することが困難になる場合がある。

さらに、脆弱性はソフトウェア導入時に既知のものだけでなく、導入後に新たに発見されたり、新たに発生したりすることがある。これらの脆弱

性に対して、適時に適切な対策を講じられないリスクが存在する。 その対策としては、ソフトウェア提供元が提供する修正プログラムやアップデートを迅速に適用することが求められる。しかし、修正プログラムの適用を怠った場合や、OSS（Open Source Software）において、ソフトウェア提供元の活動停止や製品サポート終了により修正プログラムが提供されなくなった場合など、対策が滞る可能性がある。

また、クラウドサービスの利用では、クラウド提供側がすべての脆弱性対策を実施すると誤解して脆弱性が残されるケースもあるため、注意が必要である。

これらの状況下で脆弱性対策が十分に実施されない場合、攻撃者が脆弱性を悪用する可能性がある。その結果、多岐にわたる被害が生じるおそれがある。

イ　リスクへの対策

外部調達のソフトウェアに内在する脆弱性を悪用されるリスクを低減するためには、脆弱性管理やセキュリティ対策を徹底することが重要である。以下に具体的な対策を示す。

a)管理的対策

- 使用しているすべての外部調達のソフトウェアをリスト化するなどして把握し、バージョン情報や依存関係を管理する。
- 脆弱性データベース（NVD：National Vulnerability Database）やサードパーティの脆弱性報告プラットフォームを活用し、新たな脆弱性が発見されていないか最新情報を定期的に確認する。
- ソフトウェアの更新やパッチ適用のプロセスを明確化し、脆弱性が見つかった際に迅速に対応できるよう準備する。また、更新時の影響を考慮したテストと検証のプロセスも事前に整備しておく。
- 外部調達のソフトウェアの採用時には、以下の要素を確認する。
  - 提供元のサポート体制
  - パッチ提供状況とアップデート頻度
  - 脆弱性発見時の迅速な対応の可否

  これにより、信頼性の高いソフトウェアを採用し、脆弱性発生時の迅速な対策を確保する。
- CSP との責任共有モデルを把握し、利用するサービス形態（IaaS、PaaS、SaaS）ごとの脆弱性対策の責任範囲を明確に理解する。

b)技術的対策

- ソフトウェアの構成管理及び脆弱性の自動スキャンを行うツールを導

入する。
・ 脆弱性の検知および修正を管理するプラットフォームを活用し、効率的な対応を可能にする。

c)人的対策
・ 脆弱性管理プロセスを整備し、システム管理者に周知・教育する。
・ システム管理者に対して、脆弱性情報の収集方法や対応策についてのトレーニングを実施する。

d)その他の対策
・ 新しい脆弱性が報告された際に、即座に対応できる計画を整備する。
・ 脆弱性対応の報告を受け、他システムへの対応を水平展開するとともに、脆弱性管理プロセスの改善に活用する。

2)マルウェア（悪意のあるコード）の混入によるリスク

ア　リスク概要

a)背景

攻撃者は、サプライチェーンのいずれかでソフトウェアのコンポーネントにマルウェアを仕込み、セキュリティ対策を回避しながら、ターゲットとするシステムにマルウェアを送り込む手法を用いる。

システム管理者は、これらのマルウェアが運用中のシステムに混入しないよう防ぐことが求められる。もし、マルウェアの侵入を許すと、システムへの侵入、データ漏洩、サービス妨害などの被害を受ける可能性がある。

b)想定される影響と結果

ソフトウェアの導入前にマルウェアスキャンツールを使用してチェックすることが基本的な対策である。しかし、これを怠ることや、スキャンを無効化している場合、システムが攻撃者に侵害されるリスクが高まる。

マルウェアには、情報収集を目的とするものがあり、表向きは品質情報の収集を装いながら、不正にデータを収集するものも存在する。ソフトウェアの導入時にマルウェアが含まれていなくても、後にアップデート機能やリモートアクセス機能を利用してマルウェアを送り込む手法がある。この場合、ソフトウェアの導入時に実施するスキャンでは検出できないため、ソフトウェア提供元が信頼できるかどうかの確認が必要である。

また、ソフトウェア提供元に悪意がない場合でも、ソフトウェアの開発者や提供元の環境がハッキングされ、不正にコードが書換えられるリスクがある。これにより、完製品に不正なコードが混入し、攻撃者によるシス

テムへの侵害が発生する可能性がある。ソフトウェア提供元に対しては、組織としての信用の確認だけでなく、セキュリティ対策を十分にしているかの確認も必要となる。

さらに、攻撃者が人気のあるソフトウェアに似た悪意のあるソフトウェアを公開し、利用者を誤認させて使用させる、または、攻撃者がソフトウェアのアップデートサーバや配布経路を攻撃し、マルウェアを含む更新プログラムを配布することで、利用者に正規のソフトウェアと思わせてインストールさせるなどの攻撃方法がある。もし、正規のソフトウェアであることの確認を怠った場合には、被害を受ける可能性がある。

イ　リスクへの対策

マルウェアの混入リスクを軽減するためには、以下の対策が重要である。特にシステム管理者の注意と適切な対応が、マルウェア侵入の防止において重要となる。

a)管理的対策

- 提供元が不明なソフトウェアは導入しない。
- ソフトウェアの選定時に、ソフトウェアの提供元の信頼性を評価するため、提供する組織の運営状況、ポリシーなどコンプライアンス対策の状況、セキュリティ及び品質に対する姿勢、ライセンス契約及び利用規約の内容、実際のユーザ及び顧客からの評価などを確認する。
- 信頼できる経路でのみソフトウェアを入手する。
- ソフトウェア開発元のセキュリティ体制を評価し、契約時にセキュリティ要件を盛り込む。
- ソフトウェアの導入時には、検査プロセスを設定し、信頼性を確認する。

b)技術的対策

- ソフトウェア導入前にマルウェアスキャンツールを使用してチェックする。
- ソフトウェアのデジタル署名を検証し、正規のものであることを確認する。

c)人的対策

- システム管理者に対して、マルウェアやサプライチェーン攻撃に関する教育を実施する。
- サイバーセキュリティの最新トレンドや脅威情報を学び、知識を常にアップデートする。

・　問題が発生してから対処するのではなく、予防的な対応を重視するプロアクティブな姿勢を持つ。

d)その他の対策

・　マルウェア混入などのセキュリティインシデントが発生した際に備え、対応手順や連絡体制を整備する。

3)ハードウェアのセキュリティ侵害によるリスク

ア　リスク概要

a)背景

ハードウェアの製造や部品調達は、グローバルに分散した供給網を通じて行われており、複数の国や企業が関与している。そのため、サプライチェーンのどの段階で問題が発生しているかを特定するのは容易ではない。特に信用の低い製造元や提供元が関与している場合、不正な部品や改ざんが混入する可能性が高まる。このリスクを軽減するためには、信用できる製造元等の選定、サプライチェーンの透明性の確保、改ざん防止技術の導入が不可欠である。

システム管理者としては、ハードウェアセキュリティの重要性を理解し、適切な対策を講じることが求められる。

b)想定される影響と結果

ハードウェア自体に意図的に不正な機能（バックドア、キーロガーなど）が組み込まれる場合がある。これらの組み込みは、設計段階や製造工程で密かに行われるため、検出が非常に困難であり、重大なセキュリティ侵害に繋がる。

また、ハードウェアが出荷される途中で、物流業者や中間業者による改ざんが発生する場合がある。これにより、不正なコードや部品が追加され、システムのセキュリティが損なわれるリスクが生じる。

サプライチェーン・リスクは、導入時だけでなく、廃棄時にも存在する。例えば、使用済みハードウェアの廃棄やリサイクルの際、ハードウェア内部に保存されたデータが適切に削除されていない場合、データ漏洩や攻撃者による不正利用の可能性がある。

イ　リスクへの対策

ハードウェアのセキュリティ侵害によるリスクを低減するためには、以下の対策が重要である。特に、脆弱性管理やセキュリティ対策を徹底することが重要となる。

a)管理的対策

- ハードウェアの製造元等の信頼性を評価するため、製造元等の組織におけるセキュリティポリシー及び製造プロセスの透明性、過去の実績を確認する[5]。
- 認証[6]された信用の高い製造元等からのみ製品を調達する。
- ハードウェアの真正性を確認するために、基盤、チップなどの構成部品を確認し、生産時または輸送・保管時に非正規の部品が取り付けられていないか確認することで、偽造品や改ざん品の混入を防ぐ。
- ハードウェアの設置場所への物理的なアクセス制御を厳格に行い、改造や不正設置を防止する。
- 使用済みハードウェアを廃棄する際には、データを完全に削除するか、物理的に破壊する。また、信頼できるリサイクル業者を利用し、廃棄後の追跡可能性を確保する。

b)技術的対策

- ハードウェアの導入時には、不正改ざんがないか検査を実施する。
- ハードウェアの挙動を監視し、異常を早期に検出する。
- TPM（Trusted Platform Module）やセキュアエレメントを使用して、ハードウェアレベルでのセキュリティを強化する。

c)人的対策

- サプライチェーン・リスクやハードウェアのセキュリティに関するシステム管理者向けトレーニングを実施する。
- 最新のサイバー脅威や攻撃事例を共有し、システム管理者がリスクに対する意識を持てるようにする。

d)その他の対策

- ハードウェアに関連するセキュリティインシデント発生時に備え、対応手順や連絡体制を整備する。

[5] 政府の重要業務に係る情報システム・機器の調達などより一層サプライチェーン・リスクに対応することが必要であると判断されるものについて「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）に基づいて対応する

[6] 採用時の信頼性確認を確実にするために ISO/IEC 15408 に基づく認証取得製品を採用する

4) ファームウェアのセキュリティ侵害によるリスク

ア　リスク概要

a) 背景

ファームウェアは、PC や周辺機器を制御するために組み込まれたソフトウェアである。代表例として、PC が起動する際に制御を行う UEFI（BIOS）があげられる。これ以外にも、PC 内部には通信モジュールやハードディスクなど複数のファームウェアが存在する。

ファームウェアは、OS よりも低いレイヤーで動作するため、一般的なアンチウイルスソフトウェアやセキュリティツールでは検出が難しい。その動作は、普段の利用時には見えないため、ファームウェアの脆弱性が悪用された場合、気付かないままに重大なセキュリティリスクを引き起こす可能性がある。

b) 想定される影響と結果

ファームウェアにも脆弱性が発見される。脆弱性が発見された際のファームウェアの製造元等が提供するアップデートを適用しない場合、その脆弱性を攻撃者に悪用される可能性が高まる。これにより、システムへの侵入、データ漏洩、サービス妨害などの被害が発生する可能性がある。さらに、攻撃者は正規のアップデートに見せかけた偽のアップデートを配布する手法を取ることがある。このような偽のアップデートを適用してしまうと、マルウェアがシステムに侵入し、セキュリティが損なわれる。

また、セキュアブートは、起動時にファームウェアが正規のものであることをデジタル署名で検証する機能である。しかし、この機能が無効化された場合、不正なファームウェアが実行されるリスクがある。不正な書換えが気付かれず、システムがそのまま使用される可能性もある。

その他に、ファームウェアが供給される過程で、輸送中や保管中に攻撃者よる不正な書換えが行われるリスクがある。この結果、マルウェアや不正な機能がファームウェアに追加され、セキュリティ侵害に繋がる可能性がある。

イ　リスクへの対策

ファームウェアのセキュリティ侵害によるリスクを低減するには、脆弱性管理や包括的なセキュリティ対策を徹底することが重要である。以下に具体的な対策を示す。

a) 管理的対策

・　ファームウェアを含むハードウェアの製造元等の信用を評価するため、

製造元等の組織におけるセキュリティポリシーや製造プロセスの透明性、過去の実績を確認する。 内蔵モジュールのファームウェアについても提供元に確認を行う。

- 製造元等が提供するファームウェアのアップデートを定期的に適用し、脆弱性が放置されないよう管理する。
- ファームウェアのアップデートは、信頼できる経路でアップデートファイルを入手する。正規のものかデジタル署名を確認する。
- ファームウェアの改ざん等の履歴がチェックできるような仕組みを活用する。

b)技術的対策

- セキュアブートを有効化し、起動時に信頼できるデジタル署名付きファームウェアのみをロードする。
- IoT 機器についても、ファームウェアの不正書換え対策を実施している製造元等の製品を選定する。

c)人的対策

- ファームウェアセキュリティの重要性に関するトレーニングを実施する。特に、アップデートの適用や改ざんの検出の手順について明確に教える。

d)その他の対策

- ファームウェアに関連するセキュリティインシデント発生時に備え、対応手順や連絡体制を整備する。

別紙１　立入調査時点検項目例

No.	確認事項	セキュリティ対策の実施状況の確認	根拠等エビデンスの確認例
1	目的外利用の禁止	（予防）目的外利用（二次利用）の禁止が情報取扱者に対してどのように周知、徹底されるか。 （予防）電子ファイルや紙媒体の保存先が情報取扱者に限定されているか。 （予防）電子ファイルや紙媒体は安全に廃棄されているか。 （予防）情報取扱者に対して、目的外利用の禁止について周知した記録があるか。 （予防）電子ファイルの出力際、権限者のみ出力された紙を回収可能か。 （予防）電子媒体や紙は、許可無く指定された場所から持ち出すことができないか。 （発見）電子ファイルや紙媒体へのアクセスや使用の履歴が保存されて、コピーの取得等が確認できるか。	・　情報取扱者が特定されていること（業務従事者とは異なる場合、別途情報取扱者リストを提出していること）を確認する。 ・　ファイル保存先フォルダーの権限が情報取扱者のみに設定されていることを確認する。 ・　権限設定の依頼だけではなく、依頼通り設定されていることを確認する。 ・　当該契約に関連した情報の目的外利用の禁止を、メール、掲示、配布物等で周知していることを確認する。 ・　契約期間中、電子ファイルへの操作ログ等により、許可がないコピーの取得等、不正な操作を検知したり調査したりすることが可能か確認する。 ・　紙媒体を保存しているキャビネット等の施錠と、鍵の使用記録を取得しているか確認する。
2	委託先における情報セキュリティ対策の実施内容及び管理体制	（予防）情報セキュリティ責任者及び情報取扱者の情報が提出されているか。 （予防）業務実施者の情報が提出されているか。 （予防）業務実施者は情報セキュリティに関する教育を受講しているか。 （予防）インシデント対応責任者等が定められているか。 （予防）情報セキュリティの対策実施計画が定められて、定期的に実施状況が確認されているか。	・　情報取扱者が委託先のセキュリティ規定を理解し遵守するために受けた直近の教育履歴を確認し、一年以内に受講しているか確認する。（教育は、情報セキュリティと個人情報の取扱いに関するものを含む） ・　契約時に示された情報セキュリティ体制が委託先の情報セキュリティの規定と異なる場合、それぞれの体制がどのように連携するか確認する。 ・　情報セキュリティ、品質管理、インシデント対応（CSIRT)の責任者が示されているか確認する。 ・　委託先の情報セキュリティ規程等で、情報セキュリティ対策を示し、定期的に下記の対策を点検していることを確認する。 ➢　PC 等の端末装置、電子ファイルを保存しているファイルサ

			ーバ、ネットワーク機器等の脆弱性対策（セキュリティパッチ）を実施している。 ➢ パスワード強度の担保、多要素認証の採用等、第三者からの不正アクセスを防御するために十分な強度を持つ認証の仕組みを導入している。 ➢ アカウント付与時に必要最低限の権限のみに限定している。 ➢ アカウント付与時に、予めアカウントの使用期限を設定している。 ➢ アカウントと電子ファイルへのアクセス権限を定期的に棚卸している。 ➢ 作業実施場所は、権限を有さない者の入室できない等、物理的なセキュリティが確保されているか確認する。 ➢ 在宅勤務（テレワーク）に関する委託先の規定によって、自宅等管理区域外で業務を実施する際においても情報漏えい対策を実施している。 ・ 上記で確認するセキュリティ規程が個人情報保護のセキュリティ対策も包含するか確認する。 ・ 構築した情報システムの特権の保有者が情報セキュリティ管理体制上の責任者等に限定されているか確認する。
3	情報セキュリティインシデントへの対処方法	（予防）情報セキュリティインシデントの体制が明確に規定されているか。 （予防）情報セキュリティインシデントの対応手順が規定されているか。	・ 委託先の情報セキュリティ規程等で、情報セキュリティ体制を示していることを確認する。 ・ 契約に示された情報セキュリティ体制が委託先の規定と異なる場合、それぞれの体制がどのように連携するか確認する。 ・ 情報セキュリティインシデントが委託先で発生した場合、契約業務への影響の有無にかかわらず、速やかに一報を報告した後、影響の調査と再発防止のための改善策が協議されるか確認する。

4	情報セキュリティ対策その他の契約の履行状況の確認方法	（対応）情報の取扱に関する対策等契約の履行状況を定期的に確認し報告されるか。	・ 契約、SLA、情報の取扱に関する誓約書及び情報セキュリティ管理計画書等で定められた実施事項の状況を、月次報告会等において定期的に報告することが契約書上に謳われていることを確認する。 ➢ 委託事業実施前に、監査等にて情報セキュリティの対策状況の確認を受ける。 ➢ 委託事業を開始した後も、委託事業実施前に確認を受けた対策を継続していることを、月次報告会等で定期的に報告する。 ・ 情報の取扱に関する誓約書及び情報セキュリティ管理計画書から、月次報告会等で定期的に報告をする対策を抜き出し、報告されていることを確認する。
5	情報セキュリティ対策の履行が不十分な場合の対処方法	（予防）履行状況が不十分な場合、対処することが明確に謳われているか。 （対応）履行状況が不十分な場合、対処方法は、協議の上、実施されるか。	・ 情報セキュリティインシデント、点検、状況報告等において、情報セキュリティ対策の履行が不十分だと認識した、又は認識された場合、対処について協議の上、妥当な期間と金額の範囲内で、対処することを確認する。 ➢ 対処方法については、短期的及び中長期的な観点で検討する。 ➢ 対処の対象は、再発防止の観点から直接的な対象のみに限定しないで、横展開されている。

引用文書

[i] NISC「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」、NISC ホームページ、https://www.nisc.go.jp/policy/group/general/kijun.html（2025 年２月 20 日閲覧）
※サプライチェーン・リスクに関しては、第４部 外部委託において言及されている。

[ii] 内閣府「特定重要技術の研究開発の促進及びその成果の適切な活用に関する基本指針」、内閣府ホームページ、https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/doc/kihonshishin2.pdf（2025 年２月 20 日閲覧）

[iii] NISC「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」2.1.3 情報セキュリティ関係規程の整備(1)リスク評価の実施、NISC ホームページ、https://www.nisc.go.jp/pdf/policy/general/guider6.pdf（2025 年２月 20 日閲覧）

[iv] デジタル庁「DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン～ベースラインと事業被害の組み合わせアプローチ～」、デジタル庁ホームページ、https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1b65a1dc/20230411_resources_standard_guidelines_guideline_01.pdf（2025 年２月 20 日閲覧）

[vi] デジタル庁「政府情報システムにおけるクラウドサービスの利用に係る基本方針」、デジタル庁ホームページ、https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5167e265/20230929_resources_standard_guidelines_guideline_01.pdf（2025 年２月 20 日閲覧）

[vii] 総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン」、総務省ホームページ、https://www.soumu.go.jp/main_content/000843318.pdf（2025 年２月 20 日閲覧）

[viii] デジタル庁「政府情報システムにおけるクラウドサービスの利用に係る基本方針」３．６ 4）予防的統制と発見的統制の実施、https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a612d406/20250619_resources_standard_guidelines_guideline_08.pdf（2025 年６月 19 日閲覧））

[ix] デジタル庁「政府情報システムにおけるクラウドサービスの利用に係る基本方針」３．６ 10）インシデント対応と自動化、https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a612d406/20250619_resources_standard_guidelines_guideline_08.pdf（2025 年６月 19 日閲覧））

[x] デジタル庁「政府情報システムにおけるクラウドサービスの利用に係る基本方針」３．６ 10）インシデント対応と自動化、https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a612d406/20250619_resour

ces_standard_guidelines_guideline_08.pdf（2025 年６月 19 日閲覧）

[xi] デジタル庁「政府情報システムにおけるクラウドサービスの利用に係る基本方針」３．６ 9）継続的なアップデートへの対応、https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a612d406/20250619_resources_standard_guidelines_guideline_08.pdf（2025 年６月 19 日閲覧）

[xii] デジタル庁「政府情報システムにおけるクラウドサービスの利用に係る基本方針」３．２ クラウド利用者のデータが所在する地域と適用される法令等について、https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a612d406/20250619_resources_standard_guidelines_guideline_08.pdf（2025 年６月 19 日閲覧）

[xiii] デジタル庁「政府情報システムにおけるクラウドサービスの利用に係る基本方針」３．１ クラウドサービスの選択、https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a612d406/20250619_resources_standard_guidelines_guideline_08.pdf（2025 年６月 19 日閲覧）