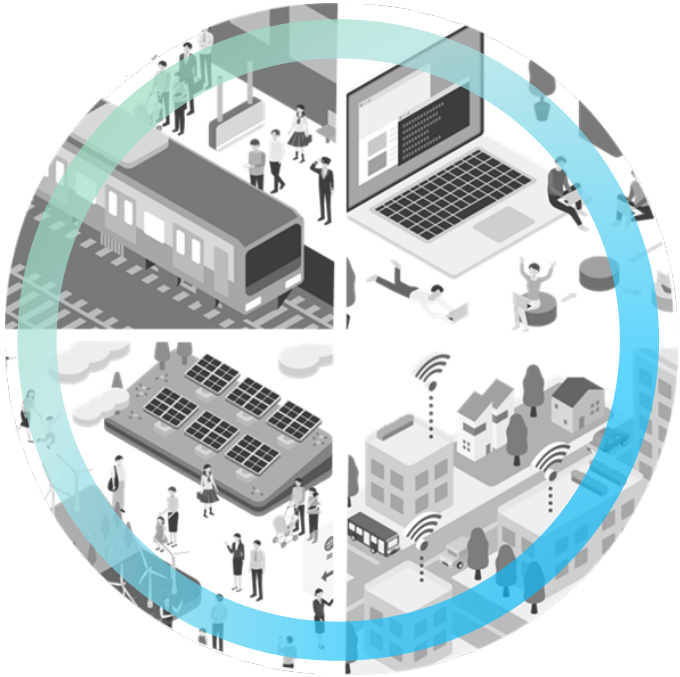


IPA Better Life with IT

重要情報を扱うシステムの
要求策定ガイド

Ver. 1.0

2023年7月

独立行政法人情報処理推進機構

目次

１．重要情報を扱うシステムの要求策定ガイドについて

1.1 重要情報を扱うシステムに求められること

- 重要情報を扱うシステムとは

「重要情報」とは、国民生活や経済活動の基盤となるサービスで使われる情報のうち、その情報に不正なアクセスがなされた場合、その情報の改ざん・破損があった場合、または、その情報の滅失・紛失または利用が不可能であった場合に、そのサービス提供に支障が生じ、国家および国民の安全や秩序などを損なう恐れや、経済活動に与える影響が特に大きいものおよびそれに準ずるものと定義する。

また、「重要情報」を取り扱うシステムを「重要情報を扱うシステム」と定義する。具体的な例は、「4.1 対象システムの例」を参照のこと。

- 重要情報を扱うシステムにおける課題

重要情報を扱うシステムは、システムの停止や情報漏洩などによる社会的影響は計り知れなく、急激な環境変化の中でもサービスの安定供給が常に求められる。そのため、システムの管理者は、不測の事態においても運用を統制しきることが必要となる。

一方、ビジネス環境の変化に対して、柔軟な運用ができ、最新技術の導入が容易にできるなどの「利便性」を享受できるクラウドサービスは、システムの構成や運用の詳細などのブラックボックス化が進み、運用の統制も効きにくいことから、重要情報を扱うシステムでは敬遠される傾向にあった。しかし、環境が急激に変化する今日において、クラウドサービスなどの最新技術やサービスを利用せずに、レガシー技術を使い続けることは、社会に対して継続的な価値提供が難しくなるだけでなく、システムの保守サポートやレガシー技術を扱える人材の確保が困難になるなど、保守管理上の課題を抱えることとなる。

また、昨今の国際環境の変化により、たとえベンダーとの間で保守委託の契約を締結していたとしても、法や規制などの影響により、技術サポートの途絶、保守部材の調達の停滞など、予測し得ないようなリスクが増大してきている。

- 重要情報を扱うシステムの管理者に要求されること

重要情報を扱うシステムの管理者は、当該システムの業務のあるべき姿を見定めた上で、最新技術を活用し、環境変化に追随するための「利便性」を追求するとともに、データの漏洩や、改ざんの可能性の排除、システム構成要素（ソフトウェア、ハードウェア等）のサプライチェーンを含めたシステムの安全性の確保、さらに、予測し得ないような非平常時においても、システムの運用を統制し続け、事態の収拾を図る結果責任を全うするための「自律性」が要求される。

これからの**重要情報を扱うシステムは、「利便性」と「自律性」の両立**が求められる。

1.2 本ガイドの目的と位置づけ

- 重要情報を扱うシステムの要求策定ガイドの目的

  重要情報を扱うシステムの要求策定ガイド（以下、本ガイド）は、重要情報を扱うシステムの管理者が、「利便性」と「自律性」の観点からシステムの特性を踏まえて、問題・リスクを分析し、その対策を自ら策定できることを目的としている。
  これにより管理者が、非平常時においても自ら統制力を持ってシステムの安定運用を実現することで、国家および国民の安全や秩序の維持や、経済活動の安定化を目指した。
  そのため、本ガイドでは単に要求項目を示すだけではなく、管理者が自ら要求項目を策定できるように、樹形図によって問題・リスクと対策の関連性も示すなどの、工夫をしている。
  また、要求項目は、システムの特性により異なり一律とならないため、管理者自らが必要な項目を取捨選択し、要求項目を策定できるものとした。管理者が策定した要求項目によって、当該システムはパブリッククラウド、プライベートクラウド、オンプレミスなどの形態になる。

- 継続的な見直し

  国際環境、ビジネス環境、技術環境など変化し続ける環境下においては、想定される問題・リスクも変化し、それに対する対策も、改める必要がある。そのため、管理者は定期的に要求項目の見直しをすることが求められる。
  なお、本ガイドも、各種環境の変化に伴い更新するため、管理者には常に最新版のガイドの確認をお願いしたい。

- 既存のガイドライン等との関係

  クレジットカード・セキュリティガイドライン、金融機関向けFISC安全対策基準、政府向けISMAP管理基準等のシステムを構築する際の安全対策を含むガイドラインや、基準などが多く活用されている。しかし、これらのガイドライン等は、対策指針や管理基準などが整理・記載されているが、予測し得ないようなリスクに対しても対策を考え、最終的に結果責任を果たすための要求項目と、その策定プロセスを示すものではない。
  したがって、本ガイドは、上記視点で補完するものであり、既存のガイドライン等と併用することを前提とする。

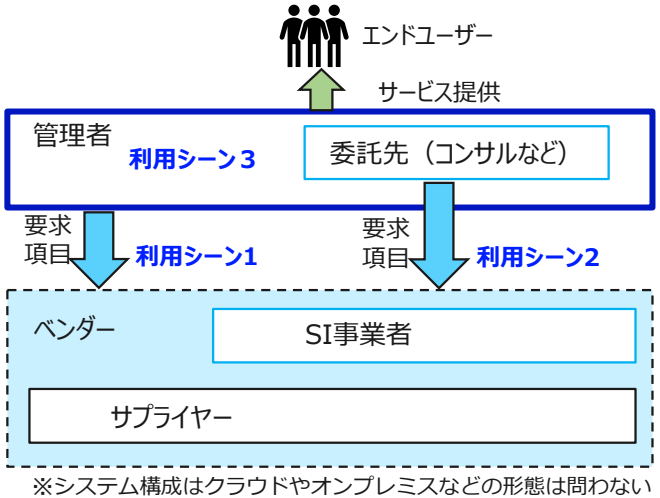
1.3 本ガイドの利用シーンとステークホルダー

- 本ガイドのステークホルダーとして、エンドユーザ、管理者、SI事業者、サプライヤーを以下のように想定している。
  なお、SI事業者とサプライヤーを総称した概念としてベンダーと定義する。

- 本ガイドの利用シーンは以下の通り。
  - ・管理者自らが調達仕様書を策定する場合　（利用シーン１）
  - ・委託先(コンサルなど)が調達仕様書を策定する場合　（利用シーン２）
  - ・管理者自らが構築、運用を行う場合　（利用シーン３）

  ※本ガイドは調達先に対する要求項目としてまとめているため、ベンダーに指示する要求を自らが行う要件として読み替えが必要となる。

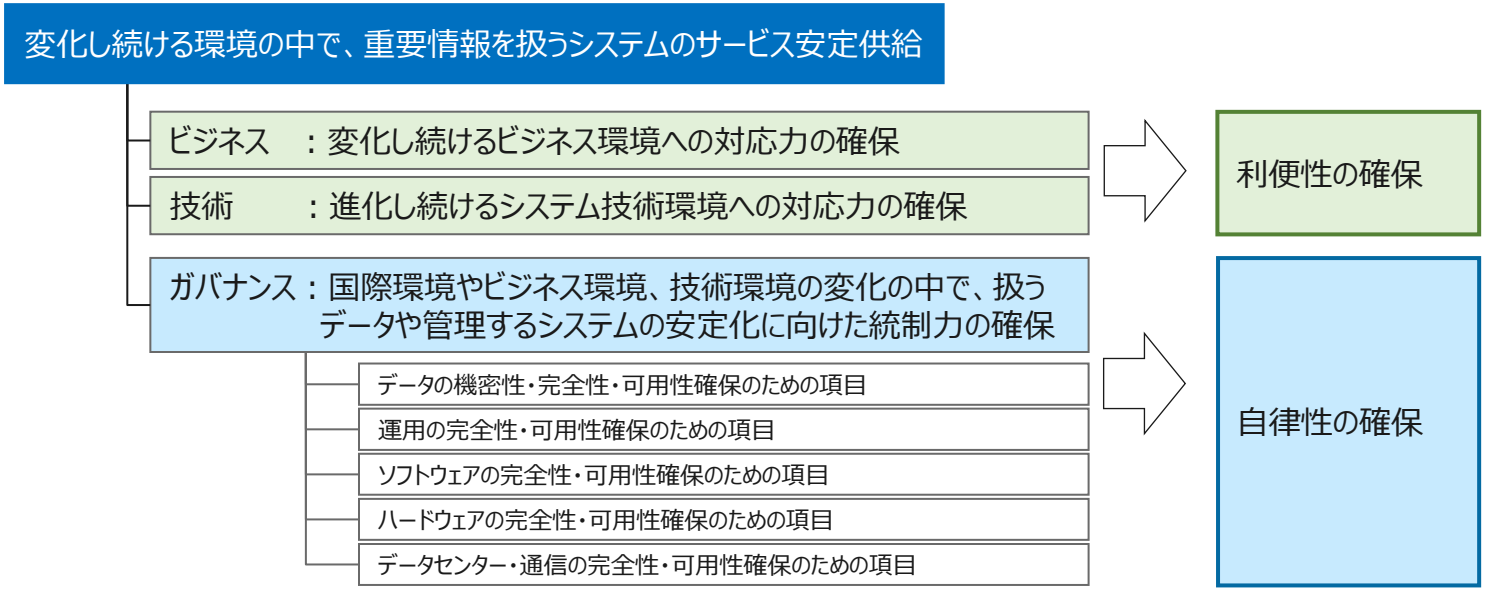
ステークホルダー		役割
エンドユーザー		重要情報を扱うシステムを利用して業務を遂行する
管理者		重要情報を扱うシステムで提供するサービスのあるべき姿を定め、システムの調達および運用の責任をもつ
ベンダー	SI事業者	管理者が示す要求項目に基づいてシステムを設計、構築、運用するサービスを提供する
	サプライヤー	クラウドサービスおよびシステムの構成要素（ハードウェア、ソフトウェア、データセンター・通信など）を提供する



※システム構成はクラウドやオンプレミスなどの形態は問わない

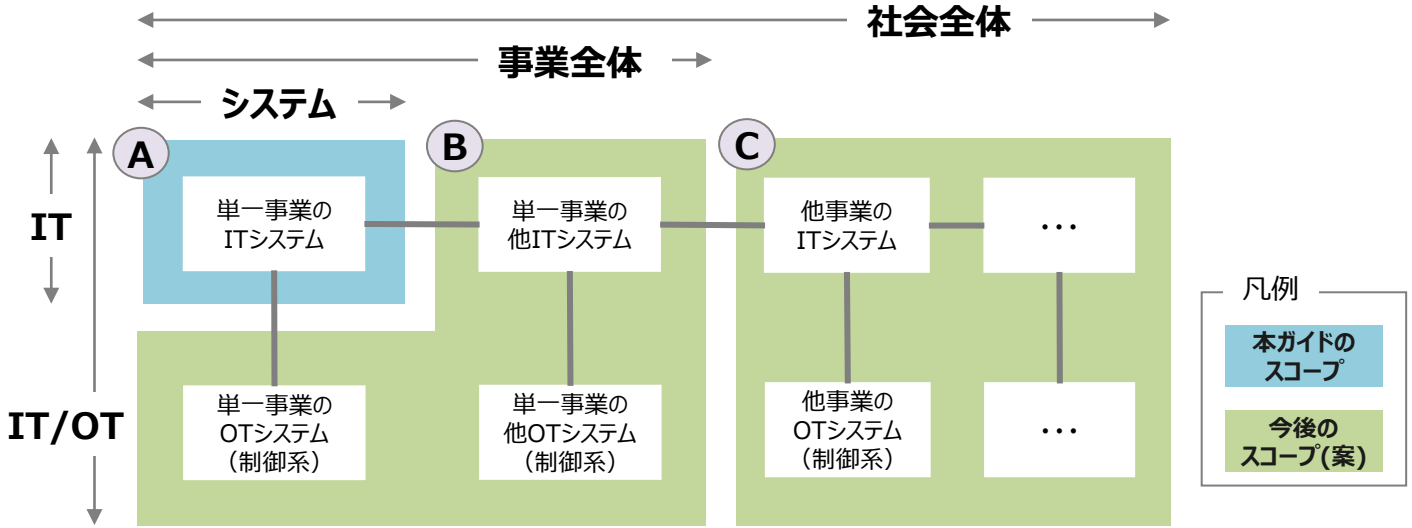
1.4 要求項目の整理の考え方

- 変化し続ける環境の中で、様々なリスクを想定（4.2 サービスの安定供給を阻害するリスク参照）し、重要情報を扱うシステムのサービス安定供給を継続するために、「利便性」をビジネスと技術の観点で、「自律性」をガバナンスの観点で要求項目を整理した。
  - 利便性確保の観点は、ビジネス環境や技術環境における変化への対応力として、その対策を整理した。
  - 自律性確保の観点は、国際環境やビジネス環境、技術環境の変化の中でのシステム安定化に向けた統制力をサービスの構成要素ごとに、機密性・完全性・可用性の観点から、問題・リスクを洗い出したうえで対策を整理した。



1.5 本ガイドのスコープと将来に向けたロードマップ

- 本ガイドは、重要情報を扱うシステムにおいて、管理者自らが調達・運用する「単一事業のITシステム」を対象とし、利便性と自律性の確保について言及している。
- 今後、OT（Operational Technology）システムを含む複数のシステムで構成される事業全体、さらに、単一事業に留まらず、社会全体を対象とするか否かを含め検討する。



例）
A：X電力の料金システム、B：X電力の電力事業（発電・送電などの電力制御システムなどを含む）、C：通信事業など
A：Y自動車の販売管理システム、B：Y自動車の製造事業（サプライチェーンに関わるサプライヤーなどのシステムなども含む）、C：通信事業、物流事業など

2．本ガイドの利用方法

2.1 要求項目策定の考え方

本ガイドは、重要情報を扱うシステムのサービスの安定供給を実現するために、管理者がベンダーに要求すべき項目を策定するなかで、システムを取り巻く環境の変化を捉え、それに伴う問題・リスクを整理し、対策を考えるという、一連のプロセスに重点を置いている。

今まで予測し得ないような非平常時においても、管理者が、客観的な状況の把握と説明を行うとともに、事態の収拾を図る必要がある。そのためには、事前にシステムに対する問題・リスクと対策の因果関係が体系的に整理されている必要がある。本ガイドでは、それらの関係を示すために樹形図の形式にて表現している。

なお、策定後については、不測の事態における柔軟な対応のため、管理者はベンダーに対しても対策内容だけでなく、その背景となる問題・リスクや対策の目的も共有することが大切である。

2.1.1 要求項目の策定ステップ

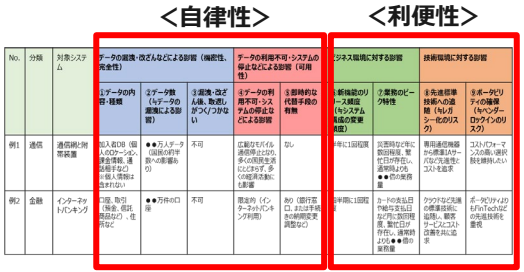
- 管理者は、以下のステップを通して要求項目を策定する。

① システムの特性評価

システム特性を９つの観点で評価し、「享受したい内容」を整理する。

→（自律性）「データの漏洩・改ざんなどの防止」を優先すべきか、「データの利用不可・システム停止などの防止」を優先すべきか、または両方なのかを見極める。

→（利便性）「変化し続けるビジネス環境への対応」を優先すべきか、「進化し続けるシステム技術環境への対応」を優先すべきか、または両方なのかを見極める。

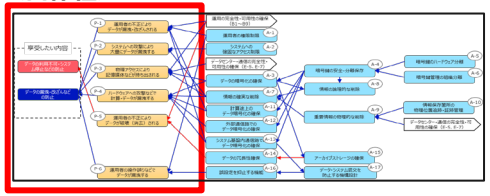


② 問題・リスク／利便性要素の選定

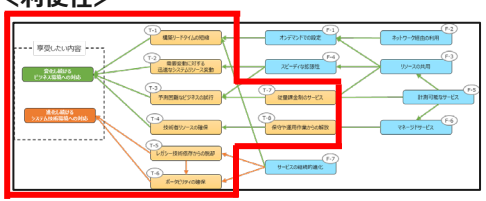
優先すべき享受したい内容をもとに、自律性では「問題・リスク」を、利便性では「利便性の要素」を、樹形図から整理する。

→ どの問題・リスクに対策を講じるか・講じないか（問題・リスクを許容するか）、または、どの利便性の要素を享受するか、しないかを見極める。

<自律性>



<利便性>

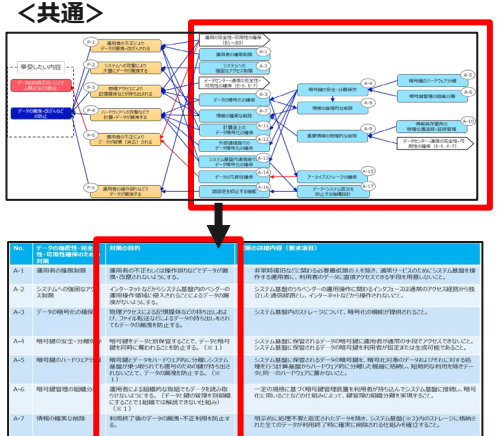


③ 必要な対策の選定

自律性では問題・リスク、利便性では利便性の要素に紐づく「対策」を目的と照らし合わせて検討する。

→ 必要とされる対策（要求項目）を選定する。

<共通>



2.1.2 システムの特性評価方法

- システムの特性を評価する項目を、以下の表①～⑨に記載する（表の記載内容は参考例）。

（自律性）「データの漏洩・改ざんなどの防止」を優先すべきか、「データの利用不可・システム停止などの防止」を優先すべきか、または両方なのかの享受したい内容を見極める。

（利便性）「変化し続けるビジネス環境への対応」を優先すべきか、「進化し続けるシステム技術環境への対応」を優先すべきか、または両方なのかの享受したい内容を見極める。

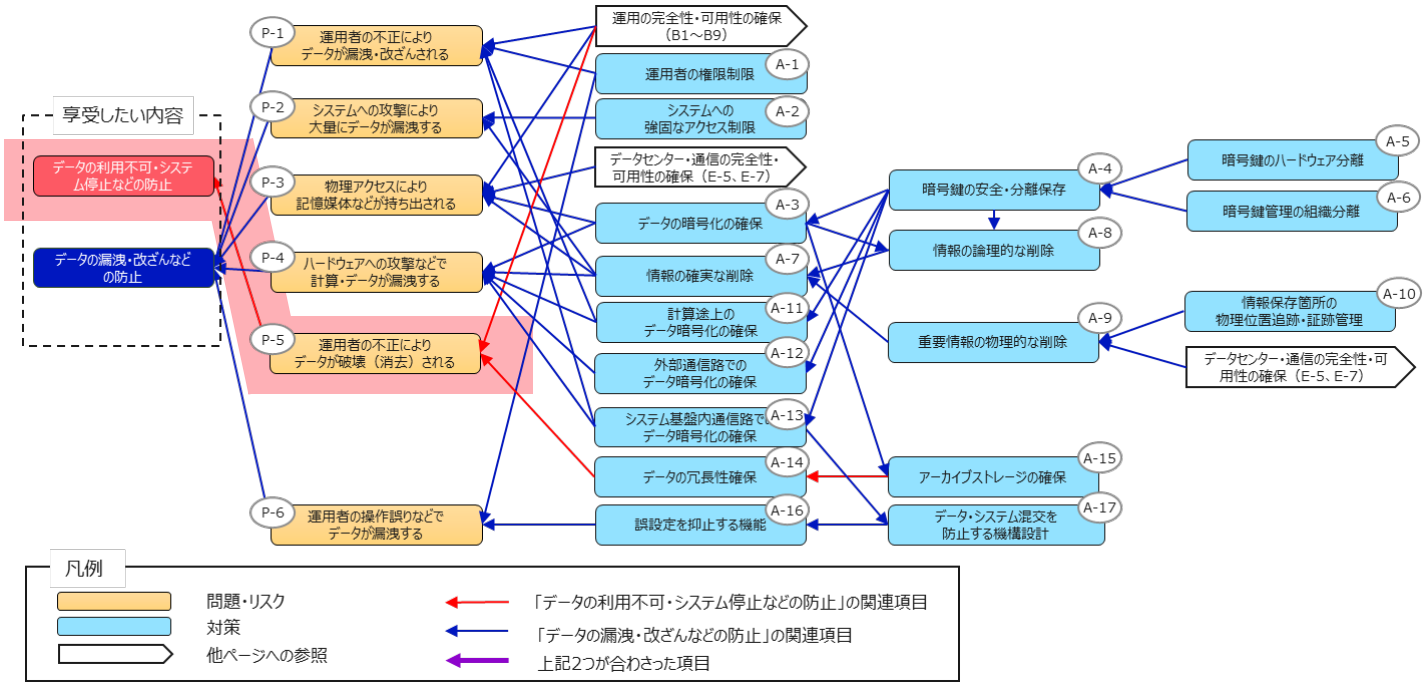
自律性に関する評価項目

利便性に関する評価項目

No.	分類	対象システム	データの漏洩・改ざんなどによる影響（機密性、完全性）			データの利用不可・システムの停止などによる影響（可用性）		ビジネス環境に対する影響		技術環境に対する影響	
			①データの内容・種類	②データ数（≒データの漏洩による影響）	③漏洩・改ざん後、取返しがつく/つかない	④データの利用不可・システムの停止などによる影響	⑤即時的な代替手段の有無	⑥新機能のリリース頻度（≒システム構成の変更頻度）	⑦業務のピーク特性	⑧先進標準技術への追随（≒レガシー化のリスク）	⑨ポータビリティの確保（≒ベンダーロックインのリスク）
例1	通信	通信網と附帯装置	加入者DB（個人のロケーション、課金情報、通話相手など） ※個人情報は含まれない	●●万人データ（国民の約半数への影響あり）	不可	広範なモバイル通信停止となり、多くの国民生活にとどまらず、多くの経済活動にも影響	なし	半年に1回程度	災害時など年に数回程度、繁忙日が存在し、通常時よりも●●倍の業務量	専用通信機器から標準IAサーバなど先進性とコストを追求	コストパフォーマンスの高い選択肢を維持したい
例2	金融	インターネットバンキング	口座、取引（預金、信託商品など）、住所など	●●万件の口座	不可	限定的（インターネットバンキング利用）	あり（銀行窓口、または手続きの納期変更調整など）	四半期に1回程度	カードの支払日や給与支払日など月に数回程度、繁忙日が存在し、通常時よりも●●倍の業務量	クラウドなど先進の標準技術に追随し、顧客サービスとコスト改善を共に追求	ポータビリティよりもFinTechなどの先進技術を重視

2.1.3 問題・リスクの選定方法

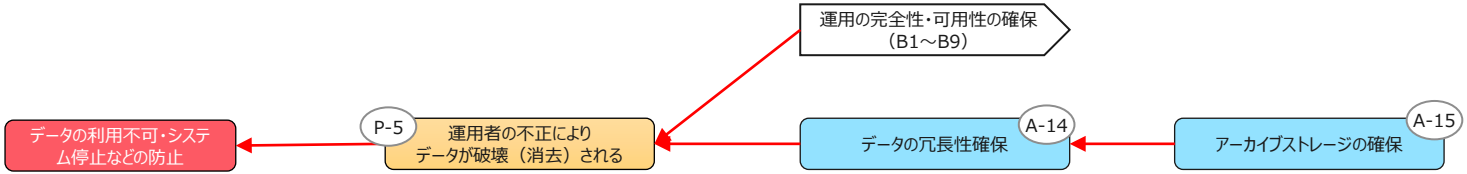
- 2.1.2で整理した享受したい内容をもとに、自律性ではサービスの構成要素（データ、運用、ソフトウェア、ハードウェア、データセンター・通信）ごとに対策を講じるべき問題・リスクを選定し、利便性では享受すべき利便性の要素を選定する。
- 享受したい内容が「データの利用不可・システム停止などの防止」の場合は、赤矢印で関連付けた問題・リスクへの対応を考える。



※関係者間で問題・リスクや対策に対して会話しやすくするように、「問題・リスク」項目ごとに番号(P1～U8)を、「対策(要求項目)」項目ごとに番号（A1～F-7)付与している。

2.1.4 必要な対策の選定方法（1／2）

- １つの問題・リスクに対して対策が複数存在する場合があるが、対策ごとの目的を踏まえ、重要情報を扱うシステムの管理者は必要性を検討し対策を定める。



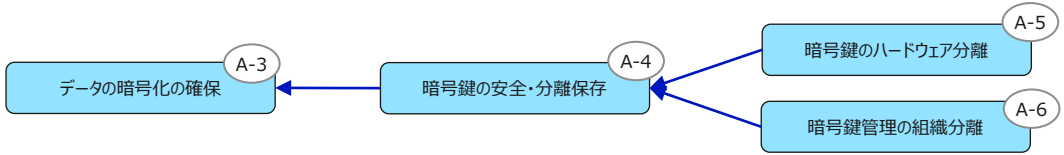
No.	データの機密性・完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
A-14	データの冗長性確保	故障・災害などによるデータの消失や、運用者の不正によりデータが破壊（消去）されることを防止する。	• 記憶装置は媒体の故障に対する冗長性を有すること。 • 重要情報を扱うシステムの管理者の指定により、記憶されたデータを自動的に別拠点の記憶媒体にバックアップすることができ、また、自動的なバックアップを行わないことを指定できること。
A-15	アーカイブストレージの確保	故障・災害などによるデータの破壊およびデータの誤った消去・上書きによるデータの消失を防止する。 また、アーカイブストレージへの不正アクセスによるデータの漏洩を防止する。	• 重要情報を扱うシステムの管理者の指定したデータベースなどのデータを定期的にバックアップするアーカイブストレージの機能を提供すること。 • アーカイブストレージは、公開鍵暗号（ハイブリッド暗号）または本表の他項の基準により安全に鍵の管理された共通鍵暗号により暗号化されること。 • アーカイブストレージにバックアップされたデータから復元を重要情報を扱うシステムの管理者により確認できること。
…	…	…	• …

2.1.4 必要な対策の選定方法（2／2）

- 対策の項目間で関連性があるものに対しては、関連性を踏まえたうえで対策を選定する。

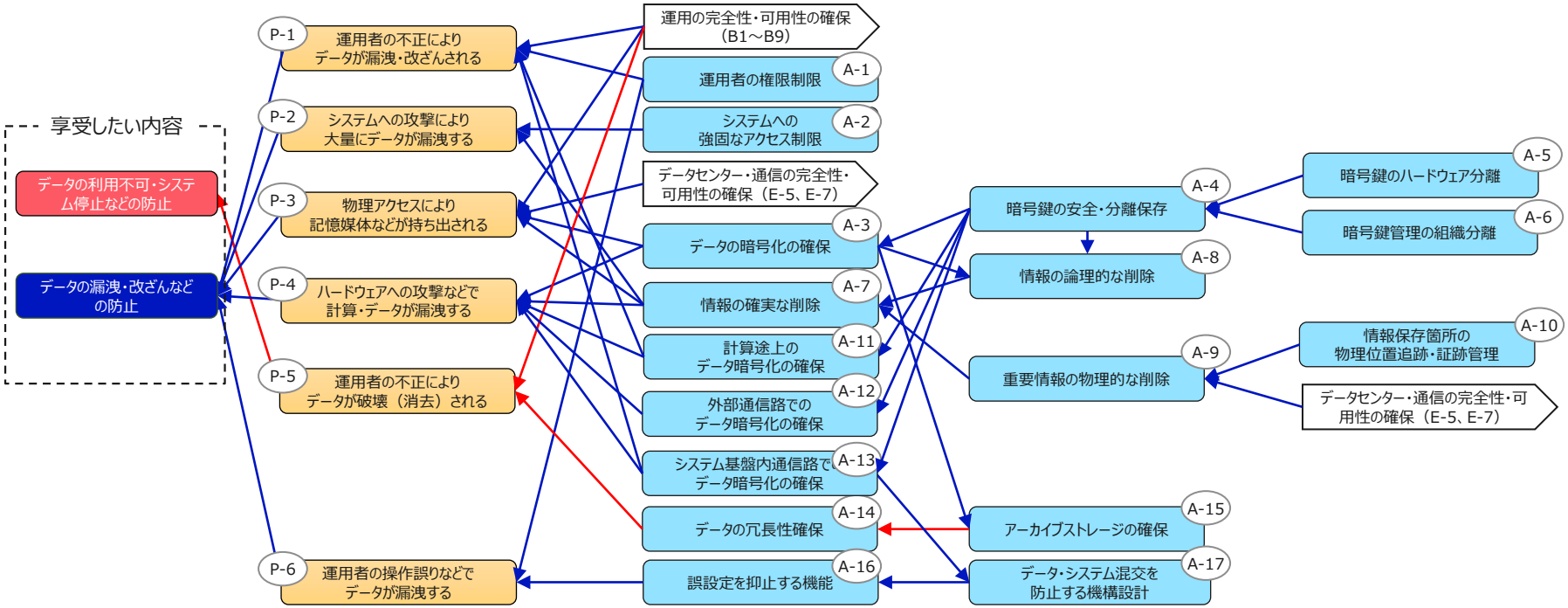
対策の項目間で関連性がある場合の記載例

以下の例においては、A-3を前提としてA-4も実施すべきか、さらに、A-3、A-4を前提としてA-5やA-6まで実施すべきかは、対策の目的を踏まえたうえで判断する。



No.	データの機密性・完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
A-3	データの暗号化の確保	物理アクセスによる記憶媒体などの持ち出しおよびファイル転送などによるデータの持ち出しをされてもデータの漏洩を防止する。	• システム基盤内のストレージについて、暗号化の機能が提供されること。
A-4	暗号鍵の安全・分離保存	暗号鍵をデータと別保管することで、データと暗号鍵を同時に奪われることを防止する。	• システム基盤に保管されるデータの暗号鍵に運用者が通常の手段でアクセスできないこと。 • システム基盤に保管されるデータの暗号鍵を重要情報を扱うシステムの管理者が指定または生成可能であること。
A-5	暗号鍵のハードウェア分離	暗号鍵とデータをハードウェア的に分離しシステム基盤が乗っ取られても復号のための鍵が持ち出されないことで、データの漏洩を防止する。	• システム基盤に保管されるデータの暗号鍵を、暗号化対象のデータおよびそれに対する処理を行う計算基盤からハードウェア的に分離した機器に格納し、短期的な利用を除きデータと同一のハードウェアに置かないこと。
A-6	暗号鍵管理の組織分離	運用者による組織的な取組でもデータを読み取らせないようにする。（データと鍵の管理を別組織にすることで1組織では解読できない仕組み）	• 一定の規格に基づく暗号鍵管理装置を重要情報を扱うシステムの管理者が持ち込んでシステム基盤に接続し、暗号化に用いることなどの仕組みによって、鍵管理の組織分離を実現すること。

2.2 自律性確保のための要求項目一覧（データ） （1／17）



2.2 自律性確保のための要求項目一覧（データ） （2／17）

No.	データの機密性・完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
A-1	運用者の権限制限	運用者の不正もしくは操作誤りなどでデータが漏洩・改ざんされないようにする。	• 非常時復旧などに関わる必要最低限の人を除き、通常サービスのためにシステム基盤を操作する運用者に、重要情報を扱うシステムの業務データに直接アクセスできる手段を用意しないこと。
A-2	システムへの強固なアクセス制限	インターネットなどからシステム基盤内のベンダーの運用操作領域に侵入されることによるデータの漏洩がないようにする。	• システム基盤のうちベンダーの運用操作に関わるインタフェースは通常のアクセス経路から独立した通信経路とし、インターネットなどから操作されないこと。
A-3	データの暗号化の確保	物理アクセスによる記憶媒体などの持ち出しおよびファイル転送などによるデータの持ち出しをされてもデータの漏洩を防止する。	• システム基盤内のストレージについて、暗号化の機能が提供されること。
A-4	暗号鍵の安全・分離保存	暗号鍵をデータと別保管することで、データと暗号鍵を同時に奪われることを防止する。	• システム基盤に保管されるデータの暗号鍵に運用者が通常の手段でアクセスできないこと。 • システム基盤に保管されるデータの暗号鍵を重要情報を扱うシステムの管理者が指定または生成可能であること。
A-5	暗号鍵のハードウェア分離	暗号鍵とデータをハードウェア的に分離しシステム基盤に侵入されても復号のための鍵が持ち出されないことで、データの漏洩を防止する。	• システム基盤に保管されるデータの暗号鍵を、暗号化対象のデータおよびそれに対する処理を行う計算基盤からハードウェア的に分離した機器に格納し、短期的な利用を除きデータと同一のハードウェアに置かないこと。
A-6	暗号鍵管理の組織分離	運用者による組織的な取組でもデータを読み取らせないようにする。（データと鍵の管理を別組織にすることで1組織では解読できない仕組み）	• 一定の規格に基づく暗号鍵管理装置を重要情報を扱うシステムの管理者が持ち込んでシステム基盤に接続し、暗号化に用いることなどの仕組みによって、鍵管理の組織分離を実現すること。
A-7	情報の確実な削除	利用終了後のデータの漏洩・不正利用を防止する。	• 明示的に処理不要と指定されたデータを除き、システム基盤内のストレージに格納された全てのデータが利用終了時に確実に削除される仕組みを確立すること。

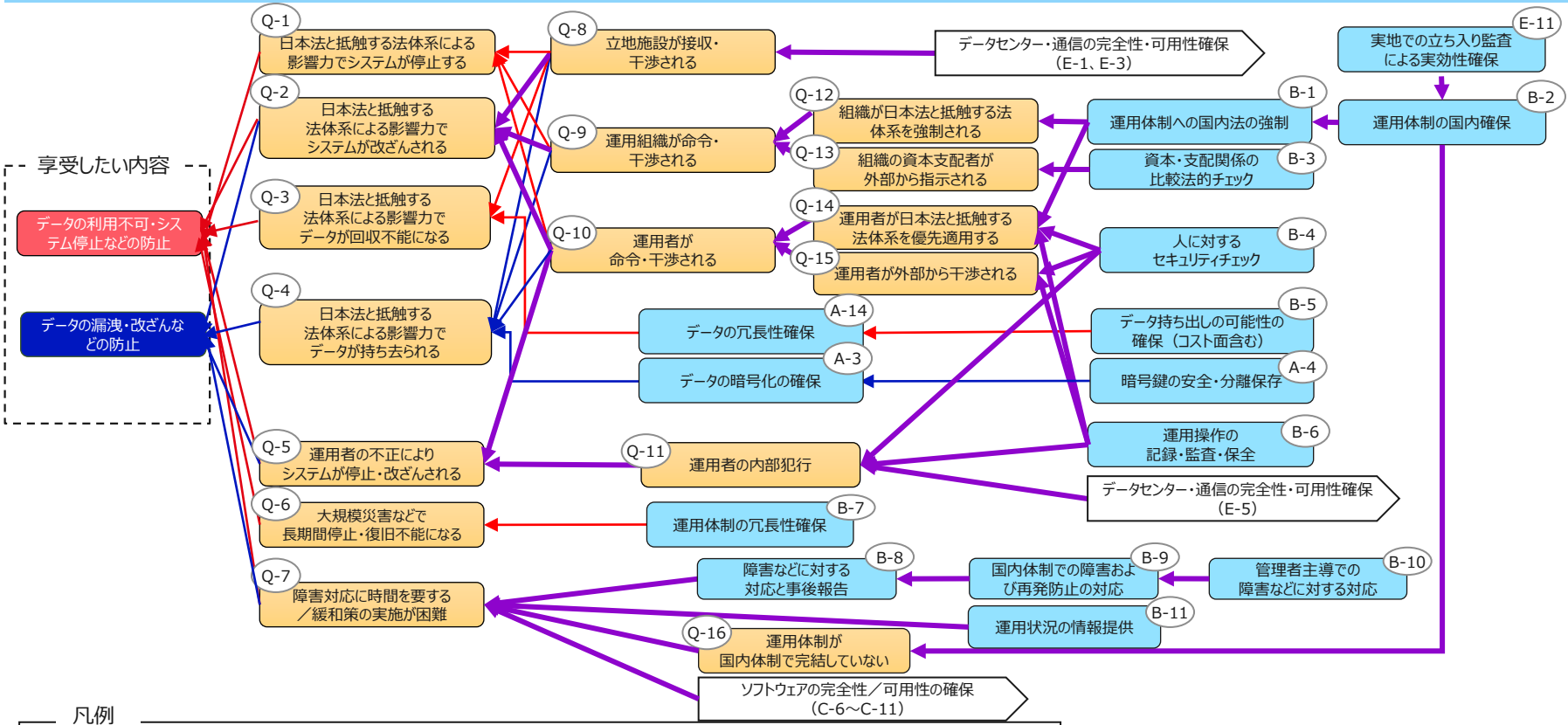
2.2 自律性確保のための要求項目一覧（データ） （3／17）

No.	データの機密性・完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
A-8	情報の論理的な削除	利用終了後のデータの復元操作などによる漏洩・不正利用を防止する。	• 対応する暗号鍵を削除することにより、システム基盤上でストレージに格納された全てのデータが利用終了時に確実に削除される仕組みを確立すること。 • 論理的な情報削除が実装されない場合には、重要情報を扱うシステム毎にストレージを分離するなどの仕組みにより、利用終了時にデータの格納された記憶媒体を物理的に破壊すること。
A-9	重要情報の物理的な削除	運用者による重要なデータの削除漏れなどがあっても、記憶媒体からの重要なデータの漏洩を防止する。	• 特に指定した重要なデータについて、暗号消去による論理的な情報削除に加え、データの格納された記憶媒体を物理的に破壊することにより確実にデータを抹消する仕組みを提供すること。 • 特に指定した重要なデータについて、情報消去の証跡を提示できること。
A-10	情報保存箇所の物理位置追跡・証跡管理	インシデント発生後に、データの物理的位置を追跡することで被害の範囲を特定できるようにする。	• システム基盤中に保存したデータが格納された物理的な装置の記録を作成し、インシデント発生時に追跡可能であること。 • 物理的な記憶媒体の交換・廃棄作業などについての記録を作成し、インシデント発生時に追跡可能であること。
A-11	計算途上のデータ暗号化の確保	ハードウェアへの攻撃や管理者権限を有する運用者の不正などによって、メモリからデータの中身を読み取ろうとしても、読み取らせないようにする。	• 特に重要なデータを扱うアプリケーションについて、例えば、ハードウェア技術を用いて、計算機のメモリ上などに格納される全ての一時的な計算結果が暗号化・隔離されるような仕組みにより、運用者などからも秘匿される機能を提供すること。 • 当該隔離機能は鍵管理機能と連動し、計算結果の隔離機構外部との全てのやり取りが暗号化され、当該アプリケーションを利用している者以外に解読されないこと。 • 当該隔離機能の利用に際し、信用しなければならないトラストアンカー（CPUチップベンダー・鍵管理装置ベンダーなど）を確認すること。 ※計算途上のデータ暗号化のためには、特殊なハードウェアやソフトウェアに限定されるなどの現時点では課題があり、その対応状況はIPAサイトにて共有する。
A-12	外部通信路でのデータ暗号化の確保	ネットワークタッピングにより運用者としてシステムを操作されることによるデータの漏洩を防止する。	• 重要情報を扱うシステムの管理者が操作する管理インタフェースとの通信およびベンダーの運用者が操作する管理インタフェースとの外部通信は暗号化・保護されていること。

2.2 自律性確保のための要求項目一覧（データ） （4／17）

No.	データの機密性・完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
A-13	システム基盤内通信路でのデータ暗号化の確保	外部からシステム基盤内へ侵入された場合や内部の運用者が不正を行った場合においても、ネットワークタッピングなどによるデータの漏洩を防止する。	• 重要なデータを扱うアプリケーションについて、システム基盤内の複数の機器間における全ての通信路上の通信が暗号化されること。
A-14	データの冗長性確保	故障・災害などによるデータの消失や、運用者の不正によりデータが破壊（消去）されることを防止する。	• 記憶装置は媒体の故障に対する冗長性を有すること。 • 重要情報を扱うシステムの管理者の指定により、記憶されたデータを自動的に別拠点の記憶媒体にバックアップすることができ、また、自動的なバックアップを行わないことを指定できること。
A-15	アーカイブストレージの確保	故障・災害などによるデータの破壊およびデータの誤った消去・上書きによるデータの消失を防止する。また、アーカイブストレージへの不正アクセスによるデータの漏洩を防止する。	• 重要情報を扱うシステムの管理者の指定したデータベースなどのデータを定期的にバックアップするアーカイブストレージの機能を提供すること。 • アーカイブストレージは、公開鍵暗号（ハイブリッド暗号）または本表の他項の基準により安全に鍵の管理された共通鍵暗号により暗号化されること。 • アーカイブストレージにバックアップされたデータからの復元を重要情報を扱うシステムの管理者により確認できること。
A-16	誤設定を抑止する機能	ベンダーの運用者および重要情報を扱うシステムの管理者の操作誤りなどによるデータの漏洩を防止する。	• ベンダーの運用者および重要情報を扱うシステムの管理者の操作誤りによりデータの漏洩などを防止するため、複数の基本セキュリティポリシーを提供し、設定の内容とポリシーを照合して誤設定を指摘する機能を提供すること。
A-17	データ・システム混交を防止する機構設計	記憶媒体・通信経路などの設定に対する障害やベンダーの運用者および重要情報を扱うシステムの管理者の操作誤りなどが起きた場合にも、他の仕組みによってデータの漏洩を防止する。（操作誤りなどによる漏洩防止のための高度な仕組みの一例）	• 例えば、アプリケーションごとのトークン付与、透過な暗号化・難読化その他の技術の組み合わせにより、記憶媒体・通信経路などの設定に障害が生じた場合においても、あるアプリケーションのデータや通信が、他の無関係のアプリケーションから有意なデータ・通信として、混交・読み取りができないような技術的設計を講じること。

2.2 自律性確保のための要求項目一覧（運用） （5／17）



2.2 自律性確保のための要求項目一覧（運用） （6／17）

No.	運用の完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
B-1	運用体制への国内法の強制	日本法と抵触する法体系の優先適用によって命令・強制等されることとなる運用組織または運用者によるシステムの停止・改ざんおよびデータの持ち出しを防止する。	• 運用者は日本法によって設立された法人であること。(※) • 契約において、「運用に関する全ての事項については、抵触法の原則の適用にかかわらず、日本法を準拠法とし、契約に起因し又はそれに関連して発生する紛争の一切は、日本の裁判所の管轄に服するものとすること」などと明記すること。 • 可能な限り、上記の内容を事前に内外の所轄当局と合意しておくこと。 • 日本法に基づかない執行に対しては、事前の措置を含め可能なあらゆる法的手段を講じて、法的に争うこと。 • 講じた手段および法的なリスク評価を明らかにすること。 • 捜査共助などにより日本法の管轄で執行される命令などについては、その限りでない。
B-2	運用体制の国内確保	日本法と抵触する法体系の優先適用によって命令・強制等されることとなる運用組織または運用者によるシステムの停止・改ざんおよびデータの持ち出しを防止する。	• 運用に必要な運用拠点などを日本国内の立地に確保すること。(※) • 平常運用時の操作については国内拠点で完結し、その他の地域に存在するオペレーションセンターなどから操作されないこと。(※)
B-3	資本・支配関係の比較法的チェック	組織の資本支配者が日本法の適用地域外からの指示等を受けることにより運用組織が命令・強制等されることによるシステムの停止・改ざんおよびデータの持ち出しを防止する。	• 親会社・関連会社・外国会社の本社・大株主など資本的支配者であって日本法と抵触する法体系の管轄に服する主体から、運用に関して、日本法と抵触する内容の指揮・命令を受けないこと。(※) • 資本的支配者で、運用を継続する為に必要な情報を有する者について、有事においても、必要な情報を継続的に入手できる手段を講じること。 • 運用に影響が有り得る資本的支配者および外注先などの関係者について、日本法と抵触する法体系の管轄に服する主体から指示を受ける可能性とその影響をあらかじめ評価するとともに、継続的にアセスメントを行うこと。

※ただし、政府調達に関しては、WTO（World Trade Organization）政府調達協定およびEPA（Economic Partnership Agreement）政府調達章との整合性に留意。

2.2 自律性確保のための要求項目一覧（運用） （7／17）

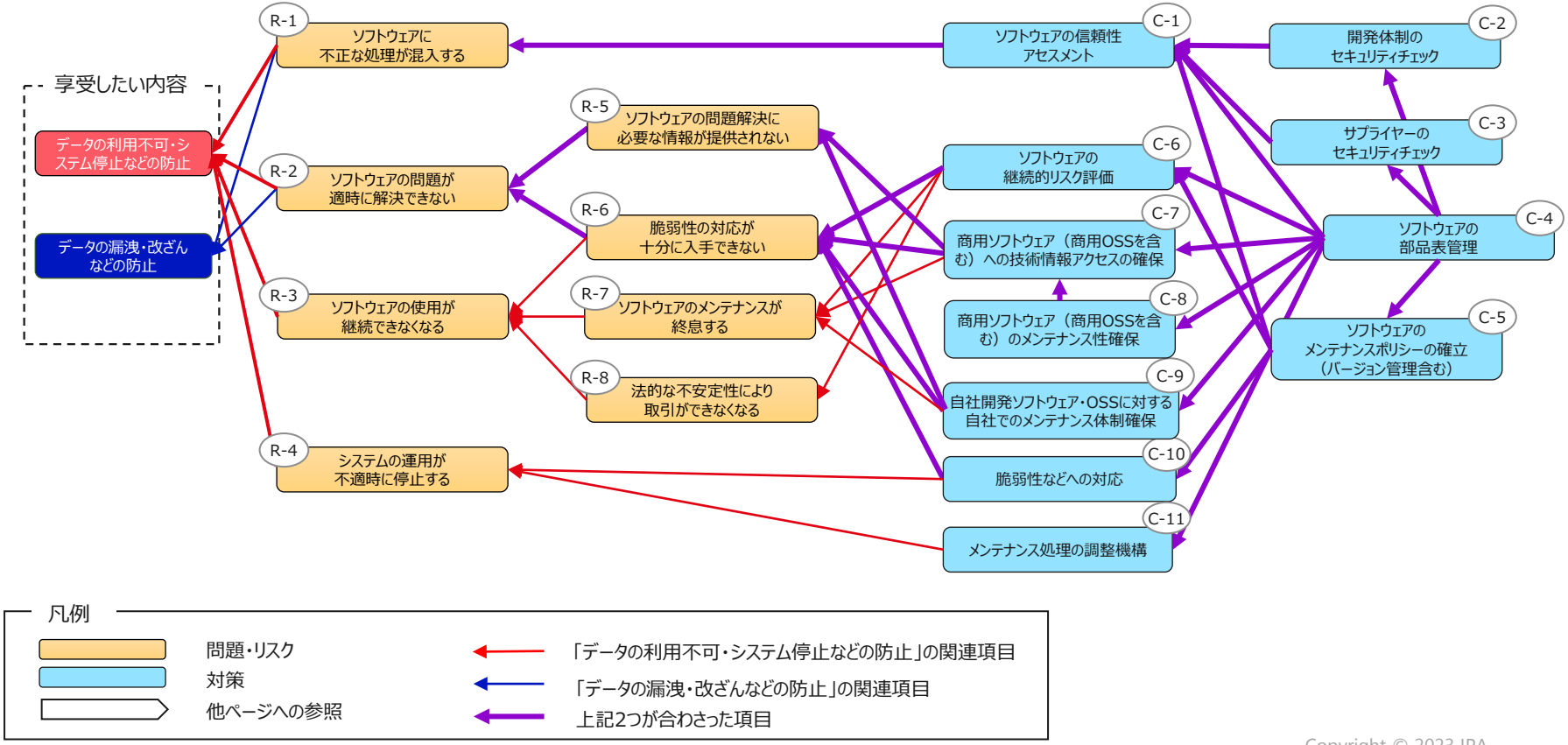
No.	運用の完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
B-4	人に対するセキュリティチェック	運用者に対する外部からの指示・強要等によるシステムの停止、データの持ち出しおよび改ざんを防止する。	• 法律に反しない範囲で、運用者の信頼性アセスメントをベンダーで行い、不正行為に関するリスクを低減するために、権限割り当てなどの措置を行う。 • 運用者について、その業務遂行が外部からの指示・強要等によって影響を受ける可能性が無いことをベンダーで確認し、継続的にアセスメントすること。 • 運用者については、生活の本拠地（自然人の場合）または事業活動の拠点（法人の場合）を日本国内に保持していること。(※)
B-5	データ持ち出しの可能性の確保 （コスト面含む）	日本法と抵触する法体系の優先適用によってデータが回収不能になるリスクやシステムの継続運用が困難になるリスクに備える。 また、他環境への現実的なデータの持ち出しを可能にする。	• システム基盤に格納されるデータは、日本国内のストレージに格納すること。(※) • システム基盤に格納されているデータを他の環境上のサーバなどに移転できること。また、その際の処理にかかる価格が無料であるか、調達条件に明示されており妥当な価格であること。
B-6	運用操作の記録・監査・保全	運用者などによる操作により不正なオペレーションやデータへのアクセスを監視し、追跡できるようにする。	• 保守などを含む全ての運用操作について、その監査記録を作成・保存し定期的に監査すること。 • 運用に関する監査記録は運用者などが書き換え・削除・破壊できない方策を講じること。 • また、地域分散など情報喪失に対する冗長性と、システム停止に対する可用性を確保すること。
B-7	運用体制の冗長性確保	大規模災害などによる長時間の運用停止を防止する。	• 地理的に隔離された複数の運用拠点（バックアップを含む）を確保し、災害時などにおける運用の継続性を高めること。

※ただし、政府調達に関しては、WTO（World Trade Organization）政府調達協定およびEPA（Economic Partnership Agreement）政府調達章との整合性に留意。

2.2 自律性確保のための要求項目一覧（運用） （8／17）

No.	運用の完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
B-8	障害などに対する対応と事後報告	重要情報を扱うシステムの管理者からの求めに応じて、ベンダーによる障害への対応と事後報告を可能とする。	• 重要情報を扱うシステムの管理者からの求めに応じて、障害の復旧過程を随時報告すると共に障害回避策を可及的速やかに提供すること。障害回避策の実施結果を確認できること。 • 発生した障害の原因を迅速に究明するために、必要な情報（ハードウェアやソフトウェアなどの各種ログや運用者の操作履歴など）の取得・保持ができるようにしておくこと。
B-9	国内体制での障害および再発防止の対応	発生した障害への対策および再発防止策の策定・報告実施を国内で完結する体制で可能とする。	• B-8に対する対策と、以下の再発防止策を国内で対応できる体制としておくこと。 発生した障害の根本原因を含む再発防止策とその対応時期を可及的速やかに提供すること。再発防止策の実施結果を確認できること。
B-10	管理者主導での障害などに対する対応	重要情報を扱うシステムの管理者にシステムの詳細情報を共有するとともに、必要に応じて管理者主導で障害対策から復旧までをベンダーとともに実行できるようにする。	• ベンダーが持つシステム基盤の内部ロジック、障害DB、診断・解析ツールなど障害対応に必要な情報やツールを管理者と共有すること。 • 必要に応じて管理者からの指示にしたがい、障害対策を立案、実行し、復旧過程を随時共有し、障害対策を可及的速やかに実施、報告できるようにしておくこと。
B-11	運用状況の情報提供	システム基盤側の障害であっても、重要情報を扱うシステムの管理者がシステム基盤の状況などを自ら把握でき、的確な対処ができるようにする。	• ベンダー側の提供条件内の障害により、重要情報を扱うシステムの管理者側からエンドユーザーに提供するサービスに障害が発生した場合において、発生原因や修正・回避策の可能性について、管理者側の対処に必要な情報提供を行うこと。 • システム基盤の構成要素（ハードウェア・ソフトウェア）などのうち重要情報を扱うシステムの管理者が現に利用しているものについての運用状況・脆弱性対応状況などを抽出し、ダッシュボードまたはAPIなどを通じて提供すること。

2.2 自律性確保のための要求項目一覧（ソフトウェア） （9／17）



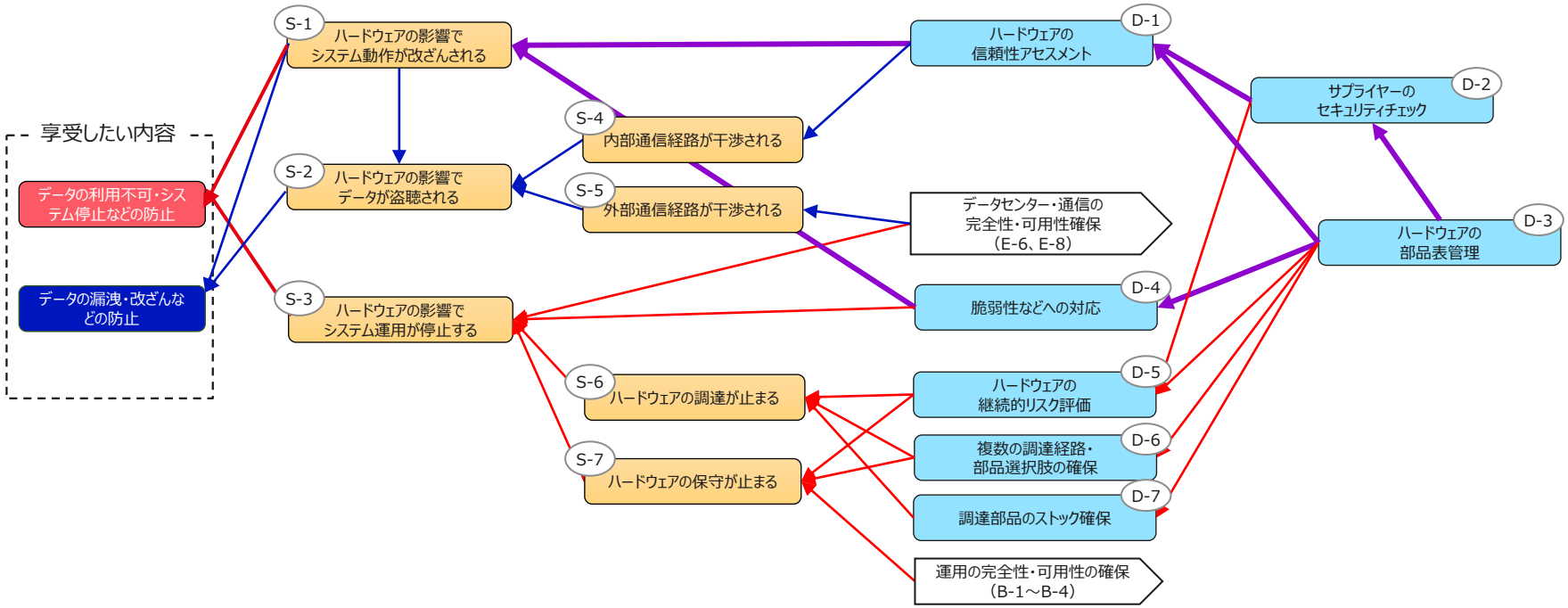
2.2 自律性確保のための要求項目一覧（ソフトウェア） （10／17）

No.	ソフトウェアの完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
C-1	ソフトウェアの信頼性アセスメント	ソフトウェアに不正な処理が混入しないようにする。	• ソフトウェア部品表（C-4に相当）に掲載された全ての要素について、不正なコードを混入させないために、受入検査その他の検証体制を構築すること。(※) ※受入検査その他の検証体制について：自社開発ソフトウェアの場合は、C-2(開発体制のセキュリティチェック）の内容を確認し、自社開発ソフトウェア以外（商用ソフトウェア、OSS(Open Source Software)など）の場合は、C-３（サプライヤーのセキュリティチェック）の内容を確認する。
C-2	開発体制のセキュリティチェック	ソフトウェア（ベンダーの自社開発範囲）に不正な処理が混入しないようにする。	• ソフトウェア部品表（C-4に相当）に掲載された要素のうち、自社開発したものについて、不正なコードを混入させないために、開発者・開発環境・検証体制などを継続的にアセスメントすること。
C-3	サプライヤーのセキュリティチェック	ソフトウェア（ベンダーの自社開発以外の範囲）に不正な処理が混入しないようにする。	• ソフトウェア部品表（C-4に相当）に掲載された要素のうち、自社開発以外のものについて、その開発者の信頼性を客観的な指標で評価し、継続的にアセスメントすること。
C-4	ソフトウェアの部品表管理	ソフトウェアのサプライチェーンを可視化し、脆弱性、品質に関するリスク管理ができるようにする。	• 運用に利用するソフトウェアおよびそれらが内部で利用するライブラリなどについて、バージョン管理に必要な単位でソフトウェア部品表を常時管理すること。 ※なお、全てのソフトウェアを網羅した部品表の実現には、業界内のすべてのサプライヤーが部品表による管理を行い、それぞれの部品表を統合することが求められるが、部品表フォーマットの標準化・互換性などについて課題があり、業界全体での取り組みが必要となる。業界における取り組みの状況はIPAサイトにて共有する。
C-5	ソフトウェアのメンテナンスポリシーの確立（バージョン管理含む）	ソフトウェアに関する脆弱性などの問題が発生した際に適時解決が図れないことがないようにする。	• ソフトウェア部品表に掲載された全ての要素について、脆弱性などの問題が発生した際のメンテナンスポリシーを事前に整理すること。
C-6	ソフトウェアの継続的リスク評価	ソフトウェアのメンテナンス終息や利用停止などが突然判明することがないようにする。	• ソフトウェア部品表に掲載された要素の全てについて、定常運用に必要なバージョンアップの頻度や、バージョンアップの提供が断絶するリスクを継続的に評価すること。

2.2 自律性確保のための要求項目一覧（ソフトウェア） （11／17）

No.	ソフトウェアの完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
C-7	商用ソフトウェア（商用OSSを含む）への技術情報アクセスの確保	商用ソフトウェア（商用OSSを含む）の技術支援が一定期間（システム移行などにかかる時間）途絶えても対象ソフトウェアの通常メンテナンスができるようにする。	• ソフトウェア部品表に掲載された要素のうち、外部から商用調達したもので、ベンダーがシステム基盤の機能維持に極めて重要なものについて、日本国内で継続的にメンテナンスするための技術情報にアクセスでき、非常時に一定期間独立して運用できる体制を保持していること。
C-8	商用ソフトウェア（商用OSSを含む）のメンテナンス性確保	商用ソフトウェア（商用OSSを含む）の技術支援が完全に途絶えても、対象ソフトウェアのメンテナンスができるようにする。	• ソフトウェア部品表に掲載された要素のうち、外部から商用調達したもので、ベンダーがシステム基盤の機能維持に必要な技術要素（重要なコンポーネントの設計情報・ソースコードなど）を保持し、運用できる体制を保持していること。または、代替ソフトウェアへの切り替えを行えること。
C-9	自社開発ソフトウェア・OSSに対する自社でのメンテナンス体制確保	自社開発ソフトウェア・OSSの技術支援が途絶えても対象ソフトウェアの通常メンテナンスができるようにする。	• ソフトウェア部品表に掲載された要素のうち、自社開発ソフトウェア・OSSでベンダーがシステム基盤の機能維持に極めて重要なものについて、自社内または日本国内での外部委託などによるメンテナンス体制を確保し、非常時に一定期間独立で運用できる体制を保持していること。
C-10	脆弱性などへの対応	ソフトウェアの脆弱性などによって、システムが不適時に停止することを防止する。また、重要情報を扱うシステムの管理者が脆弱性などの情報を適時かつ十分に取得できないことで適切な対応が遅れる事態を防止する。	• ソフトウェア部品表に掲載された要素に発見された脆弱性に対して速やかに適切な対応をするとともに、その対応状況を逐次共有すること。 • ソフトウェア部品表に掲載された要素について、公知のセキュリティ脆弱性情報などへの対応状況をリアルタイムに取得できるAPIまたは一覧できるダッシュボードなどを提供すること。 • 公知のセキュリティ脆弱性情報に対応するだけではなく、新たな脅威や脆弱性を発見して予防的対応を行える体制を保持していること。
C-11	メンテナンス処理の調整機構	重要情報を扱うシステムがベンダー側のメンテナンスによって不適時に停止することを予防する。	• ソフトウェア部品表に掲載された要素について、複数のポリシーを提供すること。 • 提供されるポリシーの1つは、メンテナンス・更新などのタイミングを重要情報を扱うシステムの管理者側から指定できるものであること。複数の重要情報を扱うシステムの管理者などで共用されるソフトウェア基盤で一義的な更新タイミングを指定できないものについては、そのタイミングに関して事前協議を行えること。

2.2 自律性確保のための要求項目一覧（ハードウェア） （12／17）



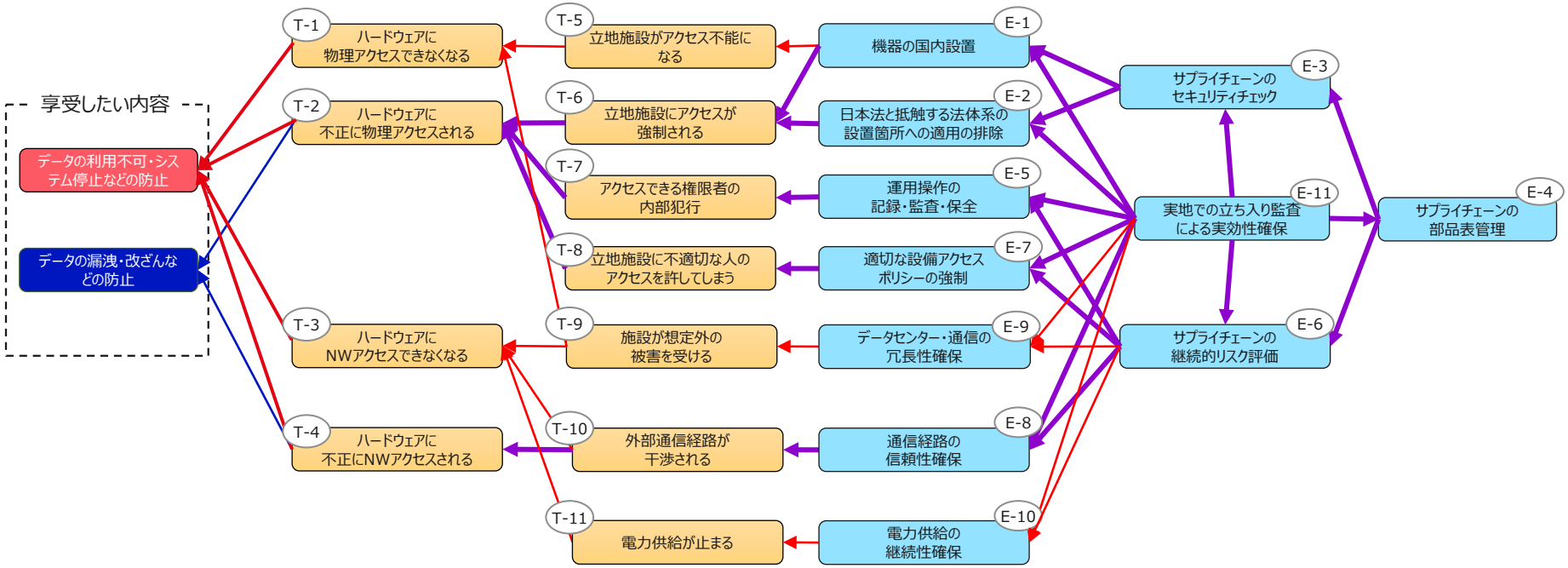
2.2 自律性確保のための要求項目一覧（ハードウェア） （13／17）

No.	ハードウェアの完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
D-1	ハードウェアの信頼性アセスメント	不正なハードウェアの影響によるシステムへの侵入、データの漏洩およびシステム動作の改ざんなどを防止する。	• ハードウェア部品表（D-3に相当）に掲載された全ての要素について、その内部の部品に不正な部品などが混入しないことを可能な限り確認し、継続的にアセスメントすること。 • 内部部品に関する情報が直接確認できない要素については、その要素の提供元の内部部品に関するセキュリティ管理体制を確認し、継続的にアセスメントすること。
D-2	サプライヤーのセキュリティチェック	不正なハードウェアの影響によるシステムへの侵入、データの漏洩およびシステム動作の改ざんなどを防止する。	• ハードウェア部品表（D-3に相当）に掲載された全ての要素の調達元について、調達元の信頼性を事前に評価し、運用中も継続的にアセスメントすること。
D-3	ハードウェアの部品表管理	ハードウェアのサプライチェーンを可視化し、システム全体のリスク管理をできるようにする。	• 運用に利用するハードウェア機器および部品などについて、調達・交換に必要な単位でハードウェア部品表を常時管理すること。 ※なお、全ての部品表の実現には、業界内のすべてのサプライヤーが部品表による管理を行い、それぞれの部品表を統合することが求められるが、部品表フォーマットの標準化・互換性などについて課題があり、業界全体での取り組みが必要となる。業界における取り組みの状況はIPAサイトにて共有する。
D-4	脆弱性などへの対応	脆弱性のあるハードウェアの影響でシステム動作の改ざんによるシステム停止やデータの漏洩を防止する。	• ハードウェア部品表に掲載された要素に発見された脆弱性に対して速やかに適切な対応をするとともに、その対応状況を逐次共有すること。 • ハードウェア部品表に掲載された要素について、公知のセキュリティ脆弱性情報などへの対応状況をリアルタイムに取得できるAPIまたは一覧できるダッシュボードなどを提供すること。 • 公知のセキュリティ脆弱性情報に対応するだけではなく、新たな脅威や脆弱性を発見して予防的対応を行える体制を保持していること。

2.2 自律性確保のための要求項目一覧（ハードウェア） （14／17）

No.	ハードウェアの完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
D-5	ハードウェアの継続的リスク評価	ハードウェアの調達および保守が止まることでシステムが停止することを防止する。	• ハードウェア部品表に掲載された全ての要素について、その調達の継続性および信頼性を継続的に評価すること。 • 調達の継続性および信頼性が懸念される事態においては、速やかに代替の部品調達を検討すること。
D-6	複数の調達経路・部品選択肢の確保	ハードウェアの調達および保守が止まることでシステム運用が停止することを防止する。	• 可能な限り、全ての要素について複数の調達経路・選択肢を確保するとともに、代替の確保が困難なものについて、システムの運用継続性に懸念がある場合には速やかに重要情報を扱うシステムの管理者に情報を共有すること。
D-7	調達部品のストック確保	部品調達経路が閉ざされても一定期間継続して保守運用できるようにする。	• 可能な限り、全ての要素について調達部品のストックを確保すること。

2.2 自律性確保のための要求項目一覧（データセンター・通信）（15／17）



2.2 自律性確保のための要求項目一覧（データセンター・通信）（16／17）

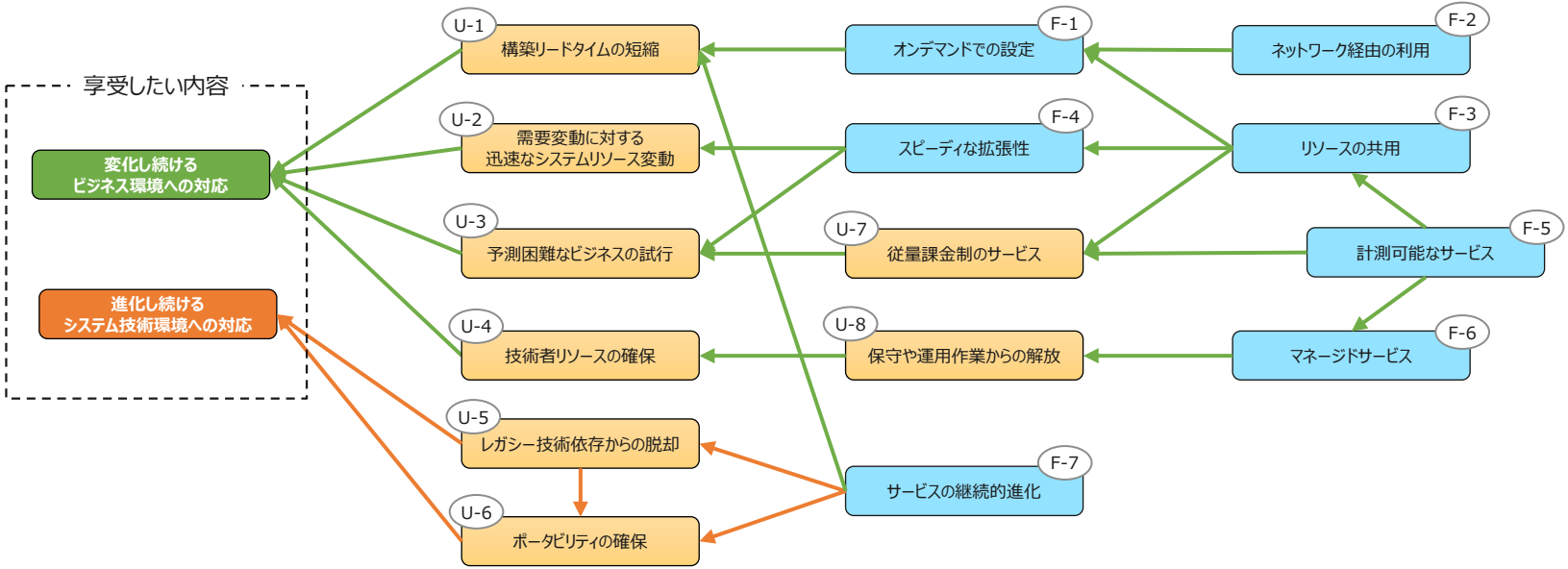
No.	データセンター・通信の完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
E-1	機器の国内設置	立地施設にアクセスできなくなることおよびアクセスが強制されることを防止する。	• 立地施設にアクセスできなくなるもしくは、アクセスが強制されることを防止できない場合には、運用に直接必要な全ての構成要素（管理体制を含む）は日本国内に設置すること。（※）
E-2	日本法と抵触する法体系の設置箇所への適用の排除	日本法と抵触する法体系の優先適用によってアクセスが強制されることを防止する。	• データセンターを管理する者などは、日本法以外の管轄・命令を受けるものでないこと。（※）
E-3	サプライチェーンのセキュリティチェック	データセンター施設や通信機器の敵対的操作につながるバックドアなどが無いようにする。	• サプライチェーン部品表（E-4の部品表に相当）の全ての要素について、不正な・敵対的な操作が行われた際のリスクを評価すること。そのリスクが大きい要素については、不正な・敵対的な操作が行われる可能性、または、日本法と抵触する法体系の優先適用によって強制される可能性が十分低いことを事前に評価し、継続的にアセスメントすること。（※）
E-4	サプライチェーンの部品表管理	物理環境（入退室セキュリティ設備、通信設備、電源、空調など）のサプライチェーンを可視化し、システム全体のリスク管理をできるようにする。	• 運用に必要な全ての物理環境（入退室セキュリティ設備、通信設備、電源、空調など）について、サプライチェーン部品表が管理されていること。データセンターなどでその管理が設備設置者に任されている場合は、設備設置者をサプライヤーとみなしD-2を実施する。
E-5	運用操作の記録・監査・保全	施設内のハードウェアに触れる権限のある者が不正な操作などを行った際に、その対象者を特定できるようにする。	• 保守などを含む全てのハードウェアなどへの操作について、入退室・ラックアクセスなどを記録するとともに、その記録を保存し定期的に監査すること。 • また、保守・廃棄などに伴い、持ち込み・持ち出しされる部品については、セキュリティ上の影響がないことを事前に評価し担保すること。
E-6	サプライチェーンの継続的リスク評価	施設を構成する設備や通信の調達および保守が止まることでデータセンターの運用が停止することを防止する。	• サプライチェーン部品表に掲載された全ての要素について、その資源提供の継続性および信頼性を継続的に評価すること。 • 資源提供の継続性および信頼性が懸念される事態においては、速やかに代替手段を検討すること。

※ただし、政府調達に関しては、WTO（World Trade Organization）政府調達協定およびEPA（Economic Partnership Agreement）政府調達章との整合性に留意。

2.2 自律性確保のための要求項目一覧（データセンター・通信）（17／17）

No.	データセンター・通信の完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
E-7	適切な設備アクセスポリシーの強制	施設内のハードウェアに触れる権限のない者の物理アクセスを防止する。	• 運用に必要な全ての構成要素はその設置位置が特定され、運用に必要な者以外が物理的に接触できないことが担保されていること。 • 保守などで臨時に設備に接触する者について、その必要性の判断および許可が明示的になされること。 • 保守などを含む全ての設備へのアクセスについて、監視カメラなどで記録するとともに、操作者などの記録を作成・保存し定期的に監査すること。
E-8	通信経路の信頼性確保	外部からの干渉などにより通信の安全性・信頼性が損なわれないようにする。	• 提供される通信サービスについて、日本国内に閉じた通信路が少なくとも1経路確保されていること。 • 提供される通信サービスに対して、重要情報を扱うシステムの管理者が要求したサービスレベル（帯域幅、物理的・論理的に独立した経路など）を確保しているかを確認する手段が提供されていること。
E-9	データセンター・通信の冗長性の確保	大規模災害などによる場合でも継続的に安定運用ができるようにする。	• 自然災害に耐えうる立地を考慮の上、地理的に隔離された複数のデータセンター（データバックアップ用拠点を含む）を確保し、災害時などにおけるシステムの可用性を高めること。 • 主要な通信路は物理的・論理的に複数経路を確保し、災害時などにおける同時障害の可能性を低減すること。
E-10	電力供給の継続性確保	大規模災害や、他国からのエネルギー調達ができない場合でも、継続的に電力供給をできるようにする。	• 電力は特定の電力会社からの供給が途絶えても供給が継続できるように、複数の電力系統を確保すること。 • 他国からの燃料に依存した電力設備だけではなく、国内に閉じて安定的な電力供給が可能な電力設備の利用も検討すること。
E-11	実地での立ち入り監査による実効性確保	ベンダーによるセキュリティ担保の取り組みについて、その実効性を確認できるようにする。 またインシデント発生時、重要情報を扱うシステムの管理者が十分な対処を取れるようにする。	• E-1～E-10の管理状況について、定期・インシデント発生時などに重要情報を扱うシステムの管理者または第三者による立入監査に応じること。

2.3 利便性確保のための要求項目一覧（1／3）



凡例

- 利便性の要素
- 対策
- 「変化し続けるビジネス環境への対応」の関連項目
- 「進化し続けるシステム技術環境への対応」の関連項目

2.3 利便性確保のための要求項目一覧（2／3）

No.	利便性確保のための対策	対策の目的	対策の詳細内容（要求項目）
F-1	オンデマンドでの設定	構築リードタイムを短縮するために、重要情報を扱うシステムの管理者自らがいつでもリソースの追加・削除をできるようにする。	• 重要情報を扱うシステムの管理者が必要な時にサーバーやストレージ、ネットワーク帯域などのリソースの制御（追加・削減など）ができること。
F-2	ネットワーク経由の利用	重要情報を扱うシステムの管理者がどこでもシステムのリソース監視や制御を行うことができるようにする。	• 重要情報を扱うシステムの管理者がインターネットなどのネットワークから、標準的な仕組み（ポータルのGUIおよびWeb API）でシステムに接続し、リソースの監視や制御ができること。 • システム基盤上で稼働する重要情報を扱うシステムやアプリケーションに、エンドユーザーがインターネットなどのネットワークから標準的な仕組みで接続できる手段を提供すること。
F-3	リソース共用	重要情報を扱うシステムの管理者が資産を保有せずに、保有するより安価にシステムを構築できるようにする。 また、性能改善や法的規制などに対応するため、重要情報を扱うシステムの管理者がシステムのロケーションを選択できるようにする。	• リソースを集積（プール化）し、マルチテナント的に複数の重要情報を扱うシステムの管理者の需要に応じて動的に割り当て・再割り当て可能であること。 なお、(A-9)重要情報の物理的な削除の要件を求めた場合、ストレージの共有はできず専用型のストレージを選択することになる。構築するシステムの特性を見極め、対策項目を決定する必要がある。 • 複数のデータセンターからサービスを提供する場合には、重要情報を扱うシステムの管理者が抽象的なレベル（例:地方、都市、データセンター)で指定可能であること。
F-4	スピーディな拡張性	予想を超える需要増加などに対するタイムリーなリソースの確保および市場の需要変動に応じたリソースの調整をできるようにする。	• 需要に応じて、リソースを即座にスケールアウト/スケールインできること。

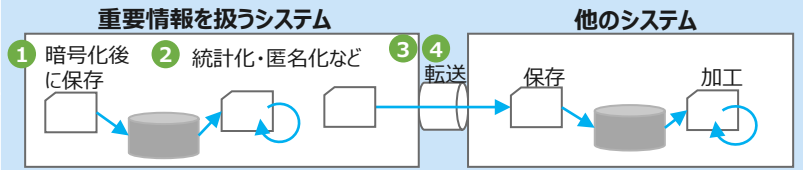
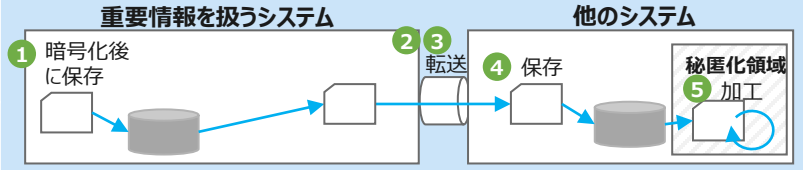
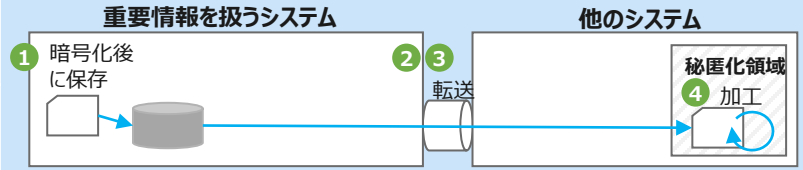
2.3 利便性確保のための要求項目一覧（3／3）

No.	利便性確保のための対策	対策の目的	対策の詳細内容（要求項目）
F-5	計測可能なサービス	重要情報を扱うシステムの管理者がシステムの運転状況を把握するため、リソースの利用状況を確認できるようにする。また、管理者が自ら利用推移を観測し利用料金を予測、調整できるようにする。	• 重要情報を扱うシステムの管理者が自身で利用したリソースをサービスの種類（ストレージ、処理能力、帯域、実利用中のアカウント数など）に適した管理レベルで利用状況をモニタできること。 • 利用料金は、リソースの実利用量に応じたものであること。
F-6	マネージドサービス	重要情報を扱うシステムの管理者がサービス利用に伴う機器や各種ソフトウェアの管理から解放できるようにする。	• 重要情報を扱うシステムの管理者が機器やソフトウェアなどを購入・構築・運用しなくても必要な機能をサービスとして利用できること。
F-7	サービスの継続的進化	重要情報を扱うシステムの管理者が進化するシステム技術環境に追随できるようにする。	• 重要情報を扱うシステムの管理者が技術の進化に伴う機能やサービスを追随して利用できること（例えば、データベース、データ分析、簡易にアプリケーションを開発できるサービスなどの機能）。 • アプリケーションの実行、運用に関係するインフラ構築がコード化され、コードの実行だけで構築を可能とする。 • ベンダーから進化したハードウェア・ソフトウェアによる新しいシステム基盤が提供された場合、基本的に環境や技術の制約を受けることなく、重要情報を扱うシステムのアプリケーションを容易に新しいシステム基盤に移行できること。

３．データ連携における留意点

3.1 データ連携における留意点（1／2）

- クラウド化の特長を活かしつつ、自律性を確保していくためには、クラウドを含む複数のシステムを組み合わせて利用する形態も想定した配慮が必要である。
- その際には、各々がデータを保存するのか否か、データを処理するのか否か、の観点から以下のデータ連携パターンが想定される。

データ連携パターン		重要情報を扱うシステム	他のシステム	データ連携時の処理プロセス ※図中の番号は次頁に示す留意点の番号
パターン１	データ保存	あり	あり （統計化・匿名化されたデータを保存）	
	データ処理	あり （連携対象データの統計化・匿名化）	あり	
パターン２	データ保存	あり	あり （重要情報を扱うシステムと同じく暗号化されたデータを保存）	
	データ処理	なし	あり	
パターン３	データ保存	あり	なし （処理結果のみを保存）	
	データ処理	なし	あり	

※秘匿化領域：特殊なハードウェア機能により、重要情報を扱うシステムの管理者のデータやコードをベンダーからも安全に隔離し、不可視化する技術（機密コンピューティング技術）などを用いて実現された実行領域

3.1 データ連携における留意点（2／2）

- 前頁のデータ連携パターン1～3における留意点を以下に示す。

データ連携パターン	留意点　※留意点の番号は前頁に示す図中の番号
パターン１	①　暗号化されたデータをストレージに保存すること ②　他のシステムへのデータ転送前に、データを加工（統計化・匿名化など）すること ③　データ連携先の真正性を確認すること ④　通信路のセキュリティレベルを確認すること
パターン２	①　暗号化されたデータをストレージに保存すること ②　データ連携先の真正性を確認すること ③　通信路のセキュリティレベルを確認すること ④　暗号化されたデータをストレージに保存すること ※重要情報を扱うシステムからの連携データはすでに暗号化済の想定 ⑤　運用者などからも安全に隔離された秘匿化領域を構築し、その中でデータを加工すること
パターン３	①　暗号化されたデータをストレージに保存すること ②　データ連携先の真正性を確認すること ③　通信路のセキュリティレベルに加えて、帯域などを確認すること ④　運用者などからも安全に隔離された秘匿化領域を構築し、その中でデータを加工すること

４．補足資料

4.1 対象システムの例（1／2）

- 本ガイドの対象となるシステム例をいくつか示しているので、対象か否かに迷った場合には判断の参考にしていただきたい。

分類	対象システム	システムの特性と主な要求項目
通信	通信網と付帯設備	機微な情報を扱ってはいないが、サービスを利用している者は非常に多く、代替手段もないため、サービスが利用できなくなった際には多くの国民生活にとどまらず、経済活動へも影響し、その影響は計り知れない。また、問題が発生した際には、問題を正確かつ迅速に把握することで自らの説明責任を果たすとともに、迅速なサービス復旧を行う必要がある。 そのため、機器の障害だけではなく、自然災害や、ハードウェアやソフトウェアなどの供給途絶、外部からの技術支援の途絶、日本法と抵触する法体系の優先適用によるシステムへの干渉などの不測の事態においても、サービスを供給できるような非常に高い可用性が求められる。さらに、不測の事態に際しては自らがサービスを統制しきるために、システムの構成要素（ハードウェア・ソフトウェアなど）や運用の詳細を把握できることなどの高い透明性も求められる。 業務のピーク特性に関しては、災害発生時に瞬間的に業務量が平常時と比較して非常に多くなるため、迅速な拡張性が求められる。 また、システム利用年数は長期を想定しているため、レガシーなアーキテクチャや製品を採用すると、将来、サポートレベルの低下やサポート切れ、技術者確保が困難といった課題に直面するリスクが高いため、新しい技術の採用とともに、技術の継続的なアップデートが求められる。
電力	電力供給に係わるシステム	電力安定供給の根幹に関わる機微な情報も扱っているため、漏洩したデータを不正に利用された場合や不正アクセスを受けた場合には多くの国民の安全・秩序に影響を与えかねない。 そのため、脆弱性を狙ったゼロデイ攻撃や、運用者による内部犯行（管理者権限を有する運用者による組織的な不正など）、日本法に抵触する法体系の優先適用によるシステムへの強制などの不測の事態においてもデータの漏洩や不正アクセスを防げるような非常に高い機密性が求められる。 また、機器の障害や自然災害等によるシステム停止も多くの国民の安全・秩序に影響を与えかねないことから、高い可用性が求められる。

4.1 対象システムの例（2／2）

分類	対象システム	システムの特性と主な要求項目
防災	災害影響予測システム	有事の際には状況が刻一刻と変化する中、膨大なリアル情報をもとに災害の影響を正確かつ迅速に予測することが求められる。また、どのような災害時であってもシステムは正常に稼働しなければならない。 そのため、サーバーやストレージなどのシステムリソースを即座に自動拡張できるような高いアジリティとともに、どのような災害であってもシステムが稼働し続けられるように地理的に分散された複数のデータセンター・通信設備および運用体制の確保などの高い可用性が求められる。 また、有事の際には膨大なリソースが必要となる一方で、平時ではほとんどリソースを使用しないため、サービスの料金体系については、リソースの使用量に応じた従量課金制が求められる。
鉄道	鉄道運行管理システム	鉄道が安全・安心、そして精密なダイヤグラムを守った高い水準での運行をするために、数秒単位で鉄道の運行を管理しており、機微な情報を扱っていないものの、システムの停止は列車の遅れや運休を引き起こし、その結果として多くの国民や社会活動に影響を及ぼしてしまう。 さらに、例えば、他システムとの連携や、運行管理システムの海外展開などを踏まえると、国際標準に即した技術（システム間のデータ連携など）を採用したシステム構成が求められる。 また、システムの利用年数は長期となるため、例えば、技術の継続的なアップデートや機能の拡張などが容易となるようなシステム構成が求められる。

4.2 サービスの安定供給を阻害するリスク

- 本ガイドで検討した重要情報を扱うシステムのサービス安定供給を阻害する主なリスクは、以下の通り。

リスク	リスクの概要
日本法と抵触する法体系による影響力	日本法と抵触する法体系により、データセンター設備の立地や、運用組織・運用者および技術サポート等の契約への影響が引き起こされる。
災害	自然災害や人為的災害によりシステムやデータセンターが破壊されることで、サービス提供が中断される。
設備アクセス・通信の途絶	データセンター設備へのアクセスができなくなることや、通信回線インフラの障害により、システムサービスの継続やパフォーマンスに影響がでる。
ソフトウェア、ハードウェアへの不正処理の混入	悪意のある行為によって、ソフトウェアに不正処理が埋め込まれることや、ハードウェアの製造工程などで不正な処理が埋め込まれることにより、機能やセキュリティが損なわれる。
システムへの物理的、または電子的な不正アクセス	悪意のある攻撃者によって、システムへの物理的または電子的な不正アクセスが行われることにより、機密情報の漏洩、データの改ざん、システムの停止などのサービスへの影響がでる。
メンテナンス・調達の途絶	システムの適切な保守作業や材料の調達が行われないことにより、システムの安定性や信頼性の維持に影響がでる。
運用者の不正や、操作ミス	システムの運用者が意図的に不正な行為を行うこと、または誤った操作を行うことによりシステムの正常な運用に影響がでる。
進化しない技術にロックイン	レガシー技術を使い続けることで、それを扱える人材の確保や保守サポートの継続ができなくなる。また、移行や切り替えの困難さが新たな技術の選択肢に制約を生じさせ、競争力の低下を引き起こす。

4.3 用語一覧（1／3）

	用語	意味
あ	アーカイブストレージ	データを長期保存するための保管場所や記録形式、保管用にひとまとめに整理されたデータなどを格納する装置のこと。
	暗号化	元となるデジタルデータを異なるデータに変換して、他者が容易に解読できない状態にすること。暗号化されたデータを元のデータに戻す操作を復号という。
	暗号鍵	データの暗号化や復号を行う際、計算手順に与える符号のこと。暗号鍵には暗号化の方法などにより「共通鍵」、「公開鍵・秘密鍵」などがある。
	暗号鍵の分離管理	暗号鍵を分離保存・管理することを示す。分離保存・管理する方法には暗号鍵を暗号化データと異なる別のハードウェアに保存する「ハードウェア分離」の方法と、暗号鍵を管理する組織とデータを管理する組織を別々にする方法の「組織分離」がある。 暗号化されたデータを保護するためには暗号鍵（暗号化に使用されるパスワードや鍵）を適切に保護する必要がある。暗号鍵が漏洩した場合、暗号化されたデータは容易に解読され、情報漏洩や不正利用のリスクが生じる。暗号鍵を別の場所に保存することで暗号化されたデータと暗号鍵を同時に奪われることを防ぎ、セキュリティの強化が図られる。
	インシデント	情報システムにおいて、対応すべき障害や問題などが発生している事象のこと。
	運用者	重要情報を扱うシステムの管理者に提供するサービスの維持・管理のためシステム基盤を運用管理するベンダーの運用者を示す。
	エンドユーザー	重要情報を扱うシステムを利用して業務を遂行する者を示す。
	オンデマンド	「要求に応じて」という意味。重要情報を扱うシステムの管理者が必要な時に利用できるサービスをオンデマンドサービスという。
か	ガバナンス	国際環境やビジネス環境、技術環境の変化の中で、扱うデータや管理するシステムの安定化に向けた統制力を確保すること。
	可用性	システムなどが使用できる状態を維持し続ける能力のこと。重要情報を扱うシステムの管理者などから見て、必要なときに使用可能な状態が継続されている度合いを表したもの。
	完全性	データや情報が正確で完全であること。意図せずデータが変更されたり、改ざんされることなく、信頼性が保たれている状態のこと。
	管理者	本ガイドでは、重要情報を扱うシステムのオーナーのことであり、構築、調達、運用の責任を持つ組織および構成員のこと。 なお、本ガイド中では、本用語を「重要情報を扱うシステムの管理者」と示す場合もある。
	機密性	ある情報へのアクセスが許可されていない対象（ユーザーやプログラム）に対し、その情報をアクセス不可または非開示にする特性のこと。

4.3 用語一覧（2／3）

	用語	意味
	計算途上のデータ暗号化	計算途上のデータの暗号化は、計算機のメモリ上などに格納される全ての一時的な計算結果の暗号化のこと。機密情報がストレージ上で暗号化されていても、計算途上ではメモリ内で復号されてしまう。このためマルウェアや不正コードの実行、運用者の内部犯行などによって機密情報が漏洩する可能性がある。一方、計算途上のデータの暗号化では、暗号化された状態で処理されるため、上述のリスクに対しても保護される。
	権限制限	運用者などに対してデータなどのアクセス権限を制限すること。本ガイドでは、システム基盤を操作する運用者に、重要情報を扱うシステムのデータに直接アクセスできる権限を制限することを示す。
	クラウド	まとまった計算資源を通信ネットワークを介して遠隔から利用するシステム形態のこと。広く一般の利用に供されるものを「パブリッククラウド」といい、特定の組織内での利用に限定するものを「プライベートクラウド」という。
さ	サプライチェーン	完成品を構成するコンポーネントおよび部品までの一連の提供のつながりのこと。
	サプライヤー	本ガイドでは、クラウドサービスやシステムの構成要素であるハードウェア、ソフトウェア、データセンター・通信などを提供する人や組織をいう。
	システム基盤	本ガイドでは、重要情報を扱うシステムの管理者にサービスを提供するためベンダーが構築し運用、管理および保守をするIT構成のこと。
	自律性	本ガイドでは、不測の事態において、重要情報を扱うシステムの管理者自らがシステムを統制、管理できる度合いを示す性質のこと。
	障害ＤＢ	障害データベースの略であり、過去発生した障害の情報を集めたデータベースのこと。
	スケールアウト	コンピュータシステムのリソースを増やすことで、性能や容量を拡張する手法のひとつ。⇔スケールイン
	スケールイン	コンピュータシステムのリソースを減らすことで、性能や容量を縮小する手法のひとつ。⇔スケールアウト
た	ダッシュボード	データを収集し、分析・加工して簡潔にまとめ、集計値、表などで一覧できるようにした画面のこと
	帯域幅	本ガイドでは、ネットワークや通信路がデータ転送できる最大データ量のこと。ネットワークの性能や、データ転送の速度に関係しており、応答時間や、パフォーマンスに影響を与える重要な要素である。
	トークン付与	アプリケーションごとのトークン付与は、データの隔離やセキュリティ強化に役立つ手法のこと。アプリケーションごとに割り当てた一意のトークンでデータのアクセスを制御することで、他のアプリケーションからのアクセスから保護する。
な	ネットワークタッピング	ネットワーク上の通信を監視・キャプチャする手法のこと。ネットワークの監視や、トラブルシューティング、セキュリティ分析、パフォーマンス測定などの目的で使用される。

凡例 ⇔： 用語集内に記載されている対になる用語を示す。

4.3 用語一覧（3／3）

	用語	意味
は	バックアップ	誤操作などによるデータ消失に備え、データを別の媒体や場所に退避しておくこと。
	バックドア	コンピュータシステムなどへ不正に侵入するための入り口のこと。
	秘匿化領域	情報セキュリティの観点で、特定のデータや情報を保護するために指定されたエリアのこと。例えば、データベースの暗号化領域やネットワークのセキュア領域、ハードウェア内の保護領域など。
	部品表	製品に必要な部品を一覧表として管理し、業界内で相互利用できるように標準化するもの。BOM(Bill of Materials)と呼ばれる。ソフトウェアにおいても、コンポーネントの情報をソフトウェア部品表（SBOM：Software Bill of Materials）として呼ばれる。
	ベンダー	重要情報を扱うシステムの管理者に情報システムを提供する者（サプライヤー、SI事業者を含む）のこと。
	ポータビリティ	ソフトウェア（重要情報を扱うシステムのアプリケーションなど）やデータの別環境への移植しやすさのこと。
ま	メンテナンスポリシー	ソフトウェアの更新などのメンテナンスを実施する方針のこと。
ら	利便性	本ガイドでは、変化し続けるビジネス環境への対応や、進化し続けるシステム技術環境への対応の程度を示す性質のこと。
	レガシー技術	進化していない古い技術のこと。古い標準に基づいているため、サポートやアップデートの制限がある、保守やメンテナンスの継続が困難である、他システムとの統合や連携が困難であるといった様々な問題を有す。
他	API	Application Programming Interfaceの略。ソフトウェアの機能や管理するデータなどを、外部の他のプログラムから呼び出して利用するための手順やデータ形式などを定めた規約のこと。
	OT	Operational Technologyの略。センサーやアクチュエータなど物理的なデバイスに対して焦点を当て、ソフトウェアを用いて制御や監視を行う技術およびシステムのこと。ITとOTの統合は産業の生産性の向上や効率性の向上などの利点をもたらすため、産業界では広く進みつつある。
	SI事業者	管理者が示す要求項目に基づいてシステムを設計、構築、運用するサービスを提供する者。

参考資料一覧

1. ISMAP運営委員会 「ISMAP管理基準（令和4年度最終改定版）」
2. 金融情報システムセンター（FISC）「FISC安全対策基準」
3. クレジット取引セキュリティ対策協議会 「クレジットカード・セキュリティガイドライン【4.0版】」
4. PCI Security Standards Council 「Payment Card Industry データセキュリティ基準（PCI DSS）v4.0」
5. 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適切な利用に係る基本方針（令和4年度版）」
6. 内閣サイバーセキュリティセンター（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（令和5年度版）」
7. 内閣サイバーセキュリティセンター（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）」
8. 総務省 「クラウドサービス提供における情報セキュリティ対策ガイドライン （第３版） 」
9. NIST 「NIST SP800-53 Rev5 情報システムと組織のためのセキュリティ管理策およびプライバシー管理策」
10. NIST 「NIST SP800-63 Rev3 電子認証に関するガイドライン」
11. NIST 「NIST SP800-145 The NIST Definition of Cloud Computing」
12. 情報処理推進機構（IPA）「NISTによるクラウドコンピューティングの定義」


IPA
Better Life
with IT