IPA

活用の手引き

重要情報を扱うシステムの 要求策定ガイド（別冊）

～重要なシステムを扱う事業者のみなさまへ～

戦後最も厳しく複雑な安全保障環境に直面し、サイバー攻撃による重要インフラの機能停止や破壊、機微情報の窃取などが、国家を背景とした形でも平素から行われている現在、重要インフラを運営する事業者のみなさまは、十分な備えができているでしょうか。

本書は、２０２３年７月に公開した「重要情報を扱うシステムの要求策定ガイド」（以下、重要システムガイドと示します）の概要と適用効果を、**ビジネスを担う事業者（注釈１）のみなさまに向け**て説明するものです。

厳しい環境の下、緊急時の対応、悪意のある攻撃者への対応について理解を深めることができます。さらに、システム運用を長期的な視点でとらえた場合の投資対効果の高いサービスの選択について、その方法をあわせて紹介します。

（注釈１）「重要情報を扱うシステムの要求策定ガイド」では、「事業者」のことを「管理者」と示しています。

０．　はじめに

生成 AI の台頭、国際的な対立など、ビジネスを取り巻く環境が変動していく中、金融や通信などの重要インフラにおいては、変わらぬサービスを提供するとともに、市場の変化に柔軟に対応することが求められます。こうした大きな環境変化に迅速に対応できるクラウドサービス（以下、クラウドと示します）の活用は一般的な選択肢となっています。

一方で、クラウドは、いわゆる「ブラックボックス化」の課題があり、クラウドのシステム構成や処理が外部から見えにくくなっています。また、このブラックボックス化はクラウドに限らず、事業者が、システムの設計・構築・運用などに関与せず、すべてをベンダーに任せた場合も同様です。緊急時の対応においては、ブラックボックス化によりエンドユーザーへの説明に影響を与える可能性があります。

また、システムで使用しているサービスの価格上昇圧力がこの先発生する可能性もあります。重要システムガイドでは、これらの課題に対して対応策を示しています。

事業者においては、本書を用いて長期的視点からの効果などをご理解いただいたうえで、重要システムガイドを実践いただくことをおすすめします。

1． 重要システムガイドとは

重要システムガイドは、経済産業省からの要請を受けて独立行政法人情報処理推進機構（IPA）デジタル基盤センターが作成し、２０２３年７月に公開されました。金融や通信などをはじめとした重要情報を扱うシステムでは、サービスの安定供給が求められます。変動するビジネス環境の中で、長期的にサービスを維持し成長していくためには、進化している技術を適切なタイミングで取り入れる「利便性」が求められます。さらに、運用者による不正な操作が原因でデータが漏洩したり、サプライチェーンが断絶したり、価格が高騰したりするなどのリスクが顕在化した場合でも、事業者には統制力を確保する「自律性」が求められます。

重要システムガイドは、これら「利便性」と「自律性」の両立を支援します。

1．1 背景 ～利便性・自律性の両立の重要性～

生成 AI のような新技術の登場は、市場のニーズに大きな変化を引き起こしました。長期的なサービス提供を目指す場合、このような技術環境の変化に柔軟に適応することが重要です。また、国際的な対立や感染症の流行下では、ビジネスを継続するために、安全な場所への急速なデータの移行やワークスペース変更の必要性が増しました。こうした大きな環境変化に迅速に対応できるクラウドの活用は、我が国においても一般的な選択肢となっています。

一方で、クラウドはいわゆる「ブラックボックス化」の課題があり、特に重要なサービスを提供するシステムでは敬遠される傾向にありました。ブラックボックス化とは、クラウド内部のシステム構成や処理およびその運用などが外部から見えにくい状態にあることを示しています。この不透明さは、サービスの提供に支障が生じるような問題が発生した場合に、原因を素早く特定し解決することや、利用者にタイムリーに説明することが難しくなるリスクとなります。このため、重要なサービスを提供する企業では、新たな技術は使わず、過去に開発した信頼性の高いシステム（レガシー技術）を使い続けることで、透明性を確保し、統制を図る「自律性」を維持してきました。

しかしながら、「自律性」のみを重視し、レガシー技術を使い続けることは、社会の変化に対応した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の課題を抱えることとなります。このため、これからのシステムでは、新たな技術を活用し環境変化に追随するための「利便性」の確保も大切です。

したがって、環境変化の大きい近年では、環境変化に対応するための「利便性」と、システムの透明性を確保し、非平常時においても、原因調査、対策および利用者への説明など、運用を統制する「自律性」の両立が必要となります(図１)。

図１　利便性・自律性の両立

１．２　重要情報を扱うシステムへの適用

重要システムガイドでは、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や情報の改ざん・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、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、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じるものを、「重要情報」と定義しています。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」と定義しています。

現在、情報技術を活用した EC（注釈２）や SNS（注釈２）など様々なサービスが提供され国民生活を豊かにし、経済の発展を支えています。その中には当たり前に受け入れられている金融や通信といったような基盤となるサービスがあり、自然災害や外的な妨害行為などによりサービス提供に支障が生じた場合、国民生活や経済活動に大きな影響を及ぼす可能性があります。「重要情報を扱うシステム」の例としては、このような欠くことのできない基盤サービスを実現するシステムがあげられます。

重要システムガイドでは、「重要情報を扱うシステム」のオーナーである**事業者が**、変化し続ける環境の中で利便性・自律性の観点から問題・リスクを分析し、その対策を**自らが策定できることを目的**にしています。利便性では、ビジネス環境と技術環境の変化に対する対応力を確保するための対策を設定しています。自律性では、国際環境やビジネス環境および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の確保を実現するため、システムを構成するデータ、運用、ソフトウェア、ハードウェア、データセンター・通信のカテゴリごとに対策を設定しています。

１．３　他のセキュリティ基準などとの関係

民間の情報システムにおいては、例えば金融機関では FISC 安全対策基準やクレジットカード・セキュリティガイドラインなど、情報システムを構築する際の安全対策を含むガイドライン・基準など

が分野ごとに提供されています。これらのガイドラインなどは、対策指針や管理基準などが整理・記載されています。

一方、重要システムガイドは、国際的な対立など今まで予測し得ないような非平常時でも、サービスを提供し続けること、および、サービス提供に支障が出た場合の迅速な復旧といった、事業者として責任を果たすための要求項目と、その策定プロセスを整理しています。このため、重要システムガイドは、重要情報を扱うシステムにおいて、既存のガイドラインなどを補完するものになります。

政府情報システムにおいては、「安全保障等の機微な情報等に係る政府情報システムの取扱い（２０２３年（令和５年）７月１９日デジタル社会推進会議幹事会決定）」（注釈３）において「「重要情報を扱うシステムの要求策定ガイド」（令和５年７月１８日 独立行政法人情報処理推進機構）や諸外国における情報システム調達に係る動向等を、必要に応じて参照すること等が考えられる」旨が、記載されています。

（注釈２）　EC: Electronic Commerce、　SNS: Social Networking Service
（注釈３）　デジタル社会推進標準ガイドライン
「DS-910 安全保障等の機微な情報等に係る政府情報システムの取扱い」項目の資料参照
https://www.digital.go.jp/resources/standard_guidelines/

２．重要システムガイドの適用効果

システム構築・運用などにおいて、IT の有識者であるベンダーの参画は欠かせません。しかしながら、事業者がシステムに関与せず、すべてをベンダーにゆだねてしまい、システムがブラックボックス化していることはないでしょうか。

このような状態でシステムに問題が発生すると、事業者はエンドユーザーに対して説明が求められますが、説明するために十分な情報がベンダーから提供されておらず、エンドユーザーへのタイムリーな情報共有が困難となる場合があります。また、ブラックボックス化が長期に続くと、内部不正の温床にもなりかねません。

近年では、サービスやものの価格が上昇しています。事業者がベンダーにすべてをゆだねた場合、ベンダーが提案する価格上昇を受け入れざるを得なくなります。

重要システムガイドでは、このようなケースにおいて有効な対策を示しています。各対策で共通して求められることは、**事業者自らが主体的に対策を策定**し、ベンダーと協力してシステムの構築・運用を行うことです。

次に**これを実践した場合の効果**についてケースごとに示します。

なお、本章の【】内は、重要システムガイドの要求項目番号(後述付録１参照)を示します。

（1）緊急時の対応

システムの重要な要素に問題が発生した場合、緊急対応が求められます。例えば、システム障害がエンドユーザーに提供するサービスに影響を及ぼした場合を考えてみます（図2の左側「事業者が把握できていない」参照)。このような状況では、事業者はベンダーと協力して障害の原因を調査し、同時にエンドユーザーへの説明を行う必要があります。システムがブラックボックス化している場合、ベンダーからの報告を理解するのに時間がかかり、かつ、ベンダーからの報告が不十分な場合も考えられます。エンドユーザーへのタイムリーな情報が提供できないと、クレームが増えてしまい、信頼性に影響する可能性が出てきます。これに対処するためは、システム上最も守りたいことを定め、それに対するリスクに備えておくことが肝要です。

例えば、このシステムは、どのようなことがあっても情報漏洩を防ぎたい場合、情報セキュリティ要素（機密性、完全性、可用性）の中で機密性を重視した対策を講じます。事業者は、機密性に関する対策を重要システムガイドにより策定し、これをベンダーと共有し、協力して構築していきます【要求項目A（データ)，B（運用)，C（ソフトウェア)，D（ハードウェア)，E（データセンター・通信)】。

実際にリスクが顕在化した場合、事前に備えた管理策が有効に働きます。事業者は、サービスを利用するエンドユーザーへの説明が必要になるため、事業者が主導でベンダーに回避策および、原因調査を求めるとともに、エンドユーザーへの説明に必要な情報の提供を依頼することで、エンドユーザーへのタイムリーな説明をしつつ、システムを復旧することができるようになります（図2の右側「事業者が把握できている」参照）【要求項目 B-8（障害などに対する対応と事後報告)，B-9(国内体制での障害および再発防止の対応), B-10(管理者主導での障害などに対する対応)】。

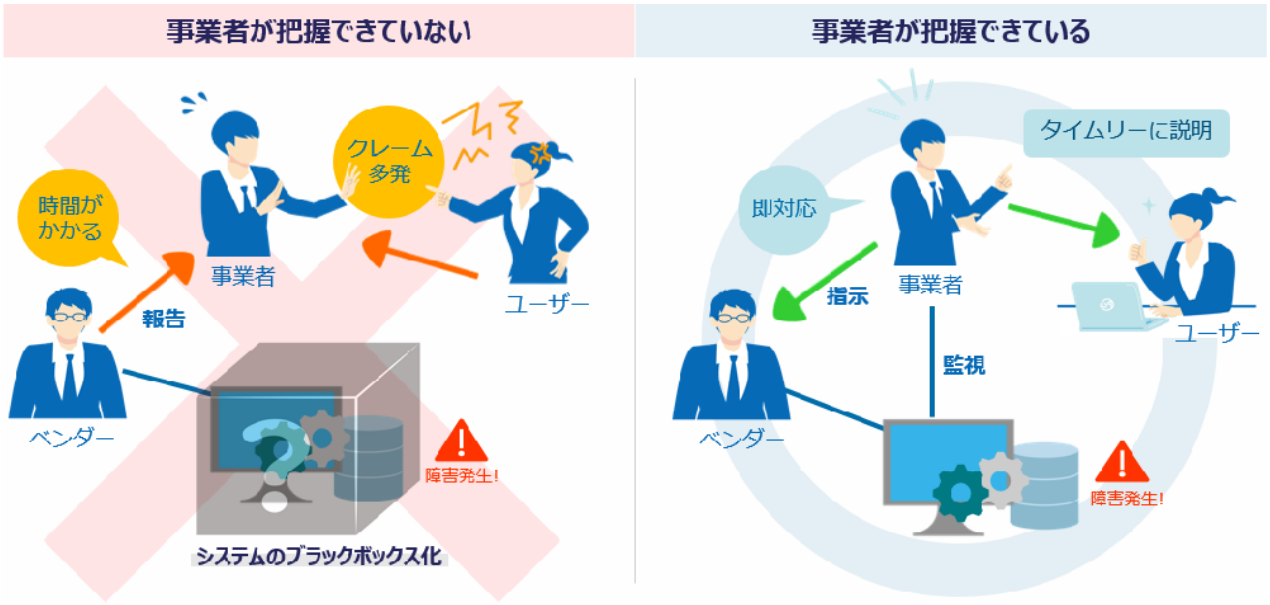


図2　緊急時の対応

（２）悪意のある攻撃者への対応

近年の国際的な対立などにより、事業者は今まで想定していなかったリスクへの対応が必要になってきました。たとえば、委託先のシステムの運用者が敵対する組織の資本的配下に入るなどのケースです。この場合、その運用者が属する組織からの指示により不正な操作を強要されメモリダンプを取得して機密情報を持ちだすようなことが考えられます（図３の左側「事業者が把握できていない」参照)。

このようなケースにおける対応として、運用者が属する組織の資本的支配者の継続的なアセスメントが有効です【要求項目 B-3(資本・支配関係の比較法的チェック)】。また、すでにシステムオーナーの意図しない操作が行われデータが持ち出された場合においても、メモリ上のデータを含めて暗号化されているためデータを解読できず、情報漏洩を防止できます（図３の右側「事業者が把握できている」参照）【要求項目 A-11(計算途上のデータ暗号化の確保)】。

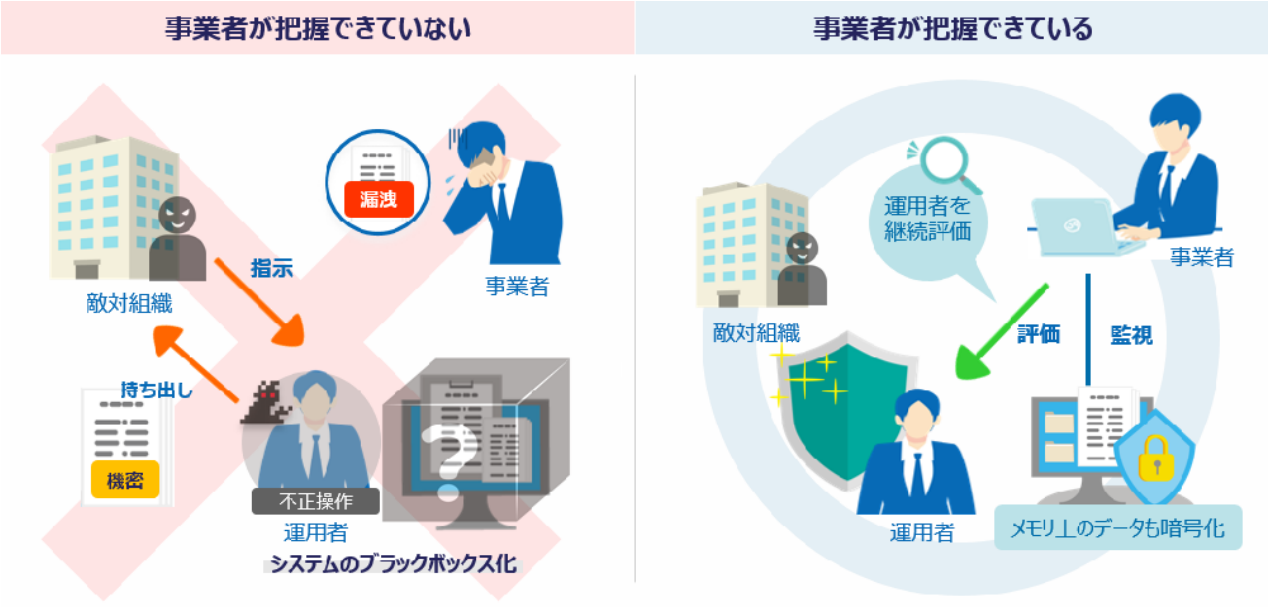


図３　悪意のある攻撃者への対応

（３）投資対効果の高いサービスの選択

近年のインフレ傾向で、使用するサービスの価格が上昇してきています。ベンダーの提供する独自のサービスを使用している場合、ベンダーロックインが発生し、ベンダーの都合による価格上昇を受け入れざるを得ません（図４の左側「事業者が把握できていない」参照）。このようなケースに対応するために、設計の段階から標準仕様を取り入れるなどシステムに移行性を持たせて備えておきます【要求項目 F-7(サービスの継続的進化)】。

例えば、事業者がシステムで使用しているサービスの価格上昇に直面した場合、一度そのサービスで使用している機能を棚卸します。そのうえで、必要な機能を提供している別のサービスとの比較を行い、投資対効果の高いサービスへ移行することで対応します。このようにすることで、事業者がサービス提供者を選択できるようになり、このサービス分野において自然と競争環境が生まれ、価格上昇に対して抑止力を働かせることができます（図４の右側「事業者が把握できている」参照）。

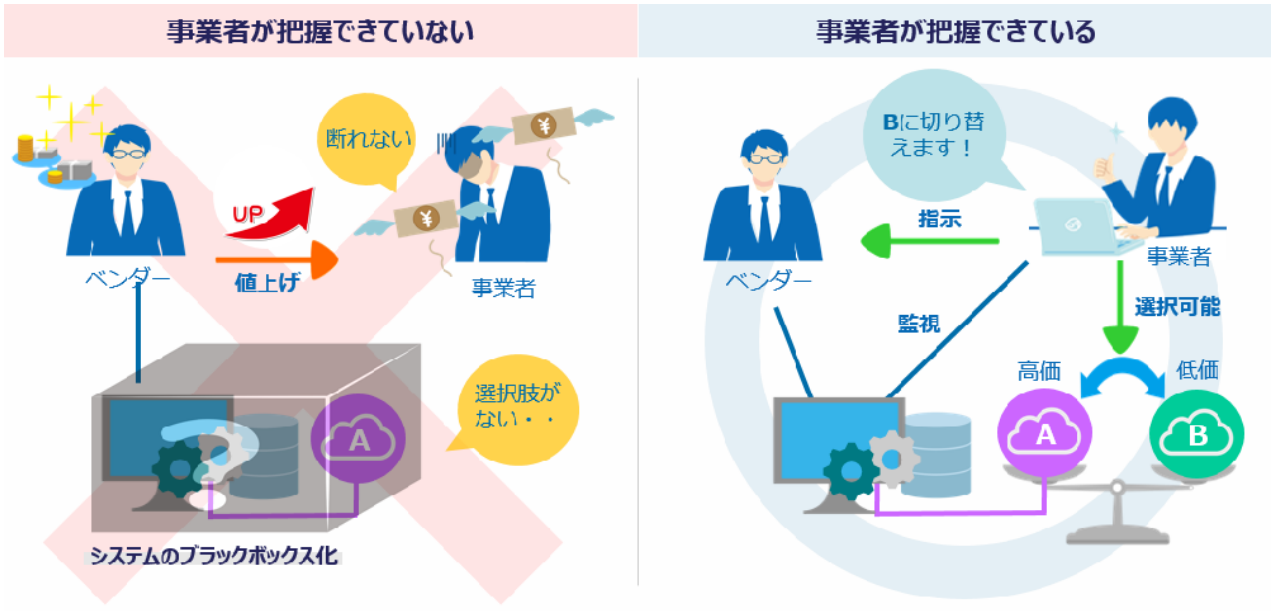


図４　投資対効果の高いサービスの選択

３．重要システムガイドの利用方法

重要システムガイドは、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、事業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**を置いています。今まで予測し得ないような非平常時においても、事業者は客観的な状況の把握と利用者への的確な説明を行うとともに、事態の収拾を図る必要があります。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ります。重要システムガイドでは、それらの関係を示すために樹形図の形式で表現しています。

なお、**不測の事態における柔軟な対応のため、事業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を含めて共有することが大切になります。

自律性・利便性確保のための対策を策定するにあたり重要システムガイドは、３つのステップを用意しています(図５)。

［ステップ１］　システムの特性評価

自律性、利便性に関してシステムの特性を９つの観点で評価していきます。これにより、現在のシステムとそれを取り巻く環境の変化による影響を整理し、自律性、利便性の観点から優先すべき享受したい内容を明確にしていきます。

【作業内容】　テンプレートを用いてシステムの特性を書き出し評価（図５①参照)。

［ステップ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、利便性の観点から問題・リスクを樹形図にて確認していきます。システムの特性から、問題・リスクの中には、対策が必要なものや許容できるものが出てくると考えられますので、これらを判断していきます。

【作業内容】　樹形図に従い対策が必要な問題・リスクを選定（図５②参照)。

［ステップ３］　必要な対策の選定

対策が必要と判断した問題・リスクに対する対策を選定していきます。樹形図を用いて選定した問題・リスクに紐づく対策項目を確認していきます。その後、要求項目一覧を参照し、対策項目の目的と対策内容を定めていきます。

【作業内容】　樹形図と要求項目一覧から対策内容を選定（図５③参照)。

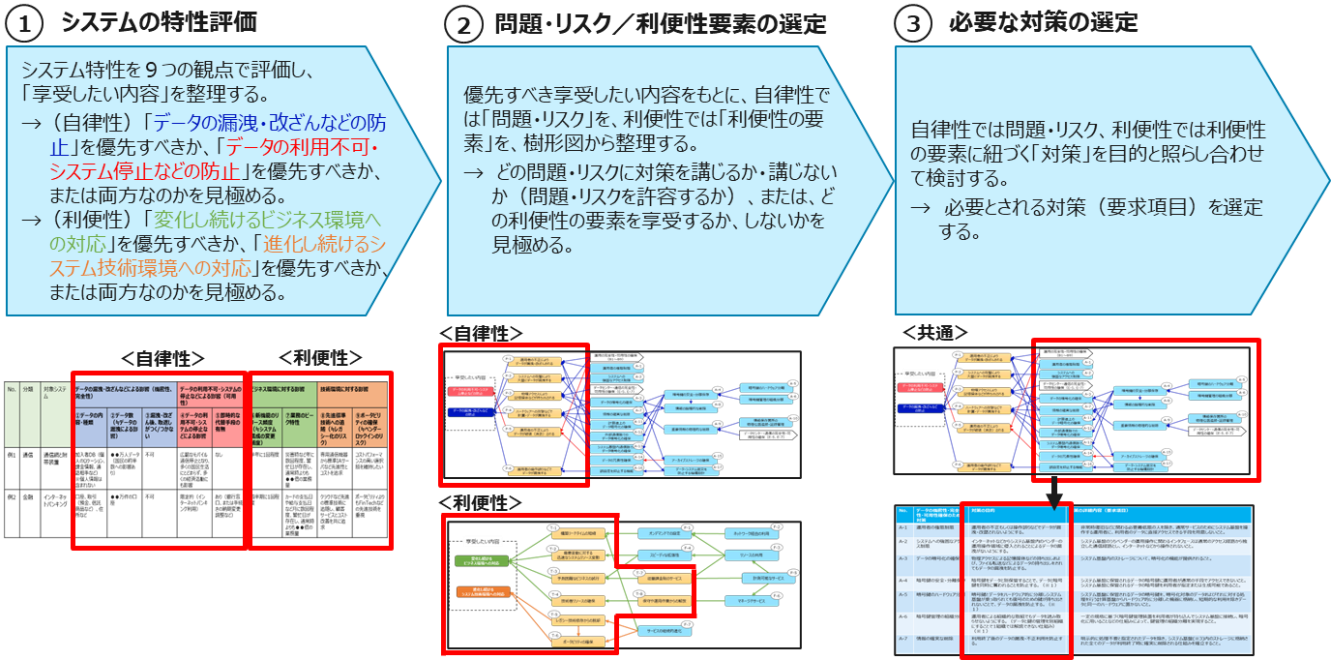


図５　策定ステップ

次に各ステップについて詳しく説明します。

３．１　システムの特性評価

自律性、利便性に関してシステムの特性を９つの観点（３．１．１①～⑨）で評価していきます。この評価を行うことで、自律性に関しては「データの漏洩・改ざんなどの防止」、「データの利用不可・システム停止などの防止」のどちらを優先すべきか、または両方なのかを見極めます。利便性に関しては「変化し続けるビジネス環境への対応」、「進化し続けるシステム技術環境への対応」のどちらを優先すべきか、または両方なのかを見極めていきます。以下、評価項目の概要と、具体的な例を用いた評価について説明していきます。

３．１．１　評価項目

（１）自律性に関する評価項目

自律性では機密性・完全性・可用性の観点からそれらが毀損された場合の影響を以下の項目を確認することで明確にしていきます。

（ア）データの漏洩・改ざんなどによる影響（機密性、完全性）

① データの内容・種類

事業者がサービスを提供するために必要なデータの内、当該システムに格納するものについて、その内容および種類を記載します。

② データ数（≒データの漏洩による影響）

当該データの数量を確認し、これらが漏洩した場合の影響を明確にします。

③ 漏洩・改ざん後、取返しがつく／つかない

当該データが漏洩・改ざんされた場合、取返しがつくか否かを判断します。

（イ）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）

④ データの利用不可・システムの停止などによる影響

上記（ア）で示すデータにアクセスできなくなった場合、もしくは、システムが停止した場合の影響について明確にします。

⑤ 即時的な代替手段の有無

上記④の事象が発生した場合、代替となる手段がすぐに用意できるかを記載します。

（２）利便性に関する評価項目

利便性では、変化しているビジネス環境と技術環境を捉えシステムに対する影響を明確にしていきます。

（ア）ビジネス環境に対する影響

⑥ 新機能のリリース頻度

システムに対して新たな機能が追加されるなどの変更頻度を記載します。

⑦ 業務のピーク特性

システムに対する負荷の傾向について明確にします。定期・不定期な繁忙期や将来の傾向に関しても明確にしていきます。

（イ）技術環境に対する影響

⑧ 先進標準技術への追随（≒レガシー化のリスク）

業界標準ではない技術や現在は標準にはなっていないレガシー技術を使用している場合、その内容と課題を記載します。また、この課題を許容できるか否かの考えもあわせて記載します。

⑨ ポータビリティの確保（≒ベンダーロックインのリスク）

ベンダーに特化した製品や、サービスを使用している場合（ベンダーロックイン）、その内容と課題に関して記載します。また、ベンダーロックインに対する課題を明確にし、その課題を許容できるか否かの考えもあわせて記載します。

3．1．2　評価の具体例

ここで、具体的なシステムの例をもとにシステムの特性を評価します。なお、**次の例は、IPA にて作成した架空のシステム**です。

（1）システムの概要と特性確認

通信網と付帯装置システムの特性を評価項目に従い図 6 に示すように評価した。

■自律性に関する評価項目

□データの漏洩・改ざんなどによる影響（機密性、完全性）

① データの内容・種類

本システムは、ユーザーの情報として、ユーザーのロケーション、課金情報、通話相手の情報を通信管理 DB にて管理している。ただし、個人情報は含まれない。

② データ数（≒データの漏洩による影響）

国民の約半数分である○○万人のデータあり。

③ 漏洩・改ざん後、取返しがつく／つかない

漏洩した場合、取返しはつかない。

□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）

④ データの利用不可・システムの停止などによる影響

サービスを利用しているユーザーは非常に多く、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、経済活動へも影響する。また、問題が発生した際には、問題を正確かつ素早く把握し、事業者自らが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。

⑤ 即時的な代替手段の有無

なし。

（続き）

■利便性に関する評価項目

□ビジネス環境に対する影響

⑥ 新機能のリリース頻度

半年に 1 度程度新機能のリリースがある。

⑦ 業務のピーク特性

災害時など年に数回程度、繁忙日が存在し、通常時よりも〇〇倍の業務量が想定される。

また、サービスの利用ユーザーは増加傾向にあり、年に数回スケールアウトすることが考えられる。

□技術環境に対する影響

⑧ 先進標準技術への追随（≒レガシー化のリスク）

専用通信機器から標準 IA サーバなどに切り替えるといった先進性と投資対効果を追求する。

⑨ ポータビリティの確保（≒ベンダーロックインのリスク）

システムの長期利用を想定していることから、現在もレガシーなアーキテクチャや製品を使い続けている。将来の保守に関してサポート切れや技術者確保が困難となること、保守費の増加も想定される。このため、投資対効果の高い選択肢を設けたい。

			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	通信管理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	〇〇万人データ（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、通常時よりも〇〇倍の業務量が想定される。また、年に数回程度スケールアウトすることが考えられる	専用通信機器から標準IAサーバなど先進性と投資対効果を追求	レガシーなアーキテクチャや製品を使用。将来の保守費増加リスクあり。投資対効果の高い選択肢を設けたい。

図6 システム特性評価

（2）システムの特性評価および対策の優先付け

（a）自律性の観点

通信管理 DB で管理しているデータは重要であり、データの漏洩・改ざんが発生した場合、ユーザーに影響を与えるとともに、システムの動作にも影響する。一方、システムの停止に関しては、通信サービスが利用できなくなるため、国民生活・経済活動への影響は計り知れない。

これらを比較した場合、データ漏洩・改ざんに関しては、影響は大きいものの個人情報が含まれていないため、システム停止の影響の方がより大きいと考えられる。このため、自律性に関しては、「**データの利用不可・システム停止などの防止**」**を優先**させる。

（b）利便性の観点

システムの利用ユーザーは今後も増加が予想され、この増加に応じたタイムリーなスケールアウトが求められる。また、レガシー技術を使い続けてきたため、その技術をサポートするための技術者確保が困難になるだけでなく、コスト効率のよい標準ＩＡサーバへの切り替えも課題となる。このため、**利便性では「ビジネス環境に対する影響」と「技術環境に対する影響」の両方を優先**させる。

３．２　問題・リスクの選定方法

次は、情報システムを取りまく問題・リスクの抽出をおこないます。

自律性・利便性の観点からシステムの特性を評価した後、それをもとに、自律性ではシステムの構成要素（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していきます。この選定には、樹形図を使用します。樹形図（図７）は、一番左の枠が「享受したい内容」、黄色の四角が「問題・リスク」(番号 P-1～P-6)、青い四角が「対策」(番号 A-1～A-17)を示しています。

この例では、享受したい内容として「データの利用不可・システム停止などの防止」を選択しています。ここから赤い矢印で関連付けられた問題・リスクとして P-5 を確認します。

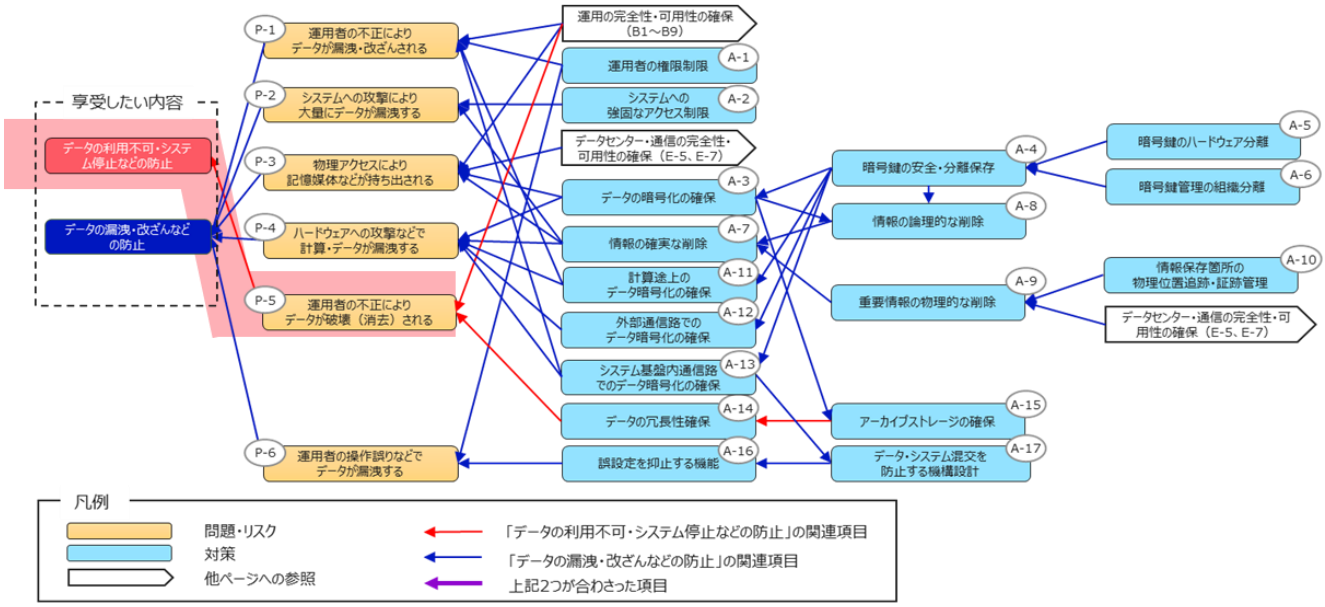


図７　樹形図

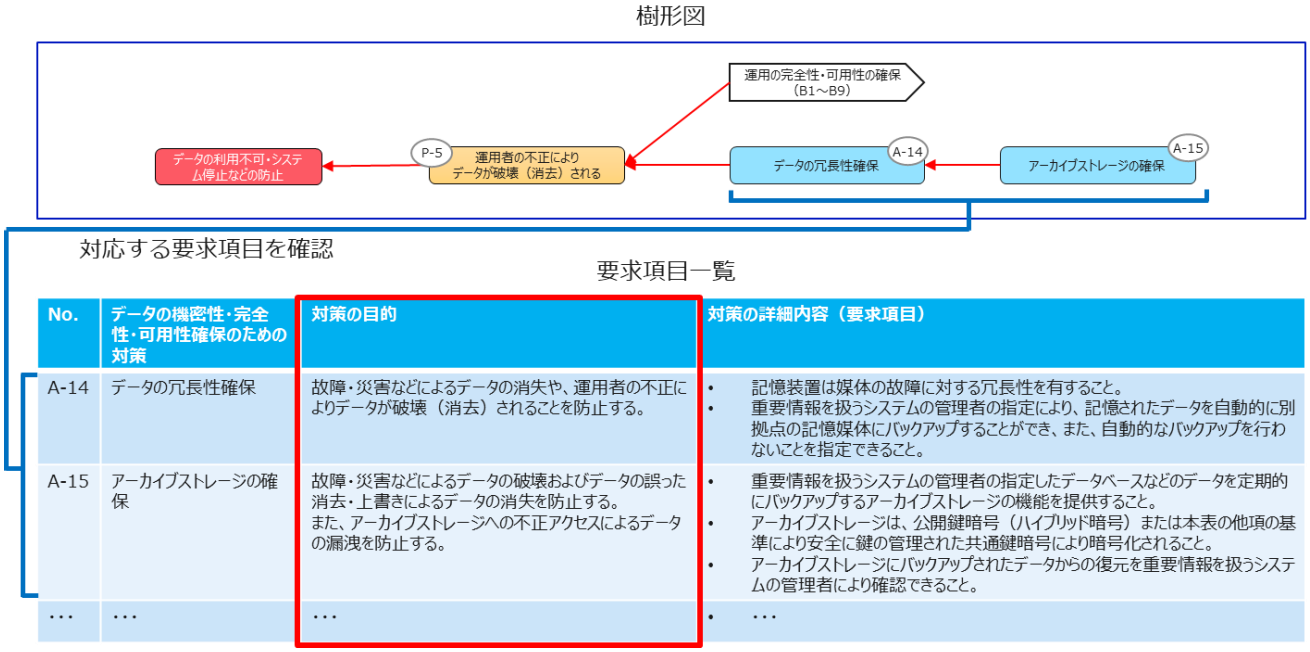
３．３　必要な対策（要求項目）の選定方法

３．２で対策が必要な問題・リスクを選定後、次にそれに紐づく対策を樹形図で確認します。

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りますが、対策ごとの目的を踏まえ、重要情報を扱うシステムの事業者は必要性を検討し対策を定めていきます。

図８に樹形図と要求項目一覧を用いて対策を選定するまでの例を示します。樹形図で、P-5 の問題・リスクに紐づく対策を確認します。ここでは、A-14, A-15 が紐づいています。その番号に対応する対策を要求項目一覧で確認していきます。要求項目一覧では、対策の目的と対策の詳細内容（要求項目）が確認できます。

なお、重要システムガイドで示す対策一覧は、後述の「付録１　参考資料（対策一覧）」にまとめています。



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。
…	…	…	• …

図８　対策の選定方法

４．重要システムガイド利用時の留意点

よくいただく問い合わせをもとに、利用の際の留意点を以下に示します。

・重要システムガイド記載の対策項目に関して、必ずしもすべてを実施することが目的ではありません。変化する環境の中、非平常時でもシステム運用を統制するため、事業者自らがシステムの特性を踏まえて必要な対策項目を選定することが大切になります。

・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では、一定の対策を一度実施すれば十分ということはありません。このため、システムのオーナーである事業者は、定期的にリスクを見直し、変化した環境に即した対策を策定していきます。

５．結び

重要システムガイドは重要情報を扱うシステムを対象にしておりますが、昨今、生成 AI やノーコード、ローコードなど新たな機能がクラウドサービスとして提供されてきており、ブラックボックス化が進んでいるため、自律性・利便性の両立の考え方は、ますます重要となります。

重要システムガイドが、安定的なサービスの提供の一助となることを願っております。

重要情報を扱うシステムの要求策定ガイド
https://www.ipa.go.jp/digital/kaihatsu/system-youkyu.html

付録１　参考資料（対策一覧）

自律性、利便性の観点からリスクとして、災害、サプライチェーンの途絶、不正処理混入、日本法と抵触する法体系の影響およびレガシー技術へのロックインなどを想定し策定した対策項目を以下に示します。

表１　自律性確保（データ）要求項目

#	対策	#	対策	#	対策
A-1	運用者の権限制限	A-7	情報の確実な削除	A-13	システム基盤内通信路でのデータ暗号化の確保
A-2	システムへの強固なアクセス制限	A-8	情報の論理的な削除	A-14	データの冗長性確保
A-3	データの暗号化の確保	A-9	重要情報の物理的な削除	A-15	アーカイブストレージの確保
A-4	暗号鍵の安全・分離保存	A-10	情報保存箇所の物理位置追跡・証跡管理	A-16	誤設定を抑止する機能
A-5	暗号鍵のハードウェア分離	A-11	計算途上のデータ暗号化の確保	A-17	データ・システム混交を防止する機構設計
A-6	暗号鍵管理の組織分離	A-12	外部通信路でのデータ暗号化の確保		

表２　自律性確保（運用）要求項目

#	対策	#	対策	#	対策
B-1	運用体制への国内法の強制	B-5	データ持ち出しの可能性の確保	B-9	国内体制での障害および再発防止の対応
B-2	運用体制の国内確保	B-6	運用操作の記録・監査・保全	B-10	管理者主導での障害などに対する対応
B-3	資本・支配関係の比較法的チェック	B-7	運用体制の冗長性確保	B-11	運用状況の情報提供
B-4	人に対するセキュリティチェック	B-8	障害などに対する対応と事後報告		

表３　自律性確保（ソフトウェア）要求項目

#	対策	#	対策	#	対策
C-1	ソフトウェアの信頼性アセスメント	C-5	ソフトウェアのメンテナンスポリシーの確立	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
C-2	開発体制のセキュリティチェック	C-6	ソフトウェアの継続的リスク評価	C-10	脆弱性などへの対応
C-3	サプライヤーのセキュリティチェック	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	C-11	メンテナンス処理の調整機構
C-4	ソフトウェアの部品表管理	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		

表４　自律性確保（ハードウェア）要求項目

#	対策	#	対策	#	対策
D-1	ハードウェアの信頼性アセスメント	D-4	脆弱性などへの対応	D-7	調達部品のストック確保
D-2	サプライヤーのセキュリティチェック	D-5	ハードウェアの継続的リスク評価		
D-3	ハードウェアの部品表管理	D-6	複数の調達経路・部品選択肢の確保		

表５　自律性確保（データセンター・通信）要求項目

#	対策	#	対策	#	対策
E-1	機器の国内設置	E-5	運用操作の記録・監査・保全	E-9	データセンター・通信の冗長性の確保
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	E-6	サプライチェーンの継続的リスク評価	E-10	電力供給の継続性確保
E-3	サプライチェーンのセキュリティチェック	E-7	適切な設備アクセスポリシーの強制	E-11	実地での立ち入り監査による実効性確保
E-4	サプライチェーンの部品表管理	E-8	通信経路の信頼性確保		

表６　利便性確保要求項目

#	対策	#	対策	#	対策
F-1	オンデマンドでの設定	F-4	スピーディな拡張性	F-7	サービスの継続的進化
F-2	ネットワーク経由の利用	F-5	計測可能なサービス		
F-3	リソース共用	F-6	マネージドサービス		

この文書について

■文書名

重要情報を扱うシステムの要求策定ガイド（別冊）活用の手引き

■公開履歴

初版　　2024 年 7 月 29 日

■編集・発行

独立行政法人情報処理推進機構（IPA）