ドローン航路システムの
セキュリティ調査報告書

2025 年 3 月

国立研究開発法人新エネルギー・産業技術総合開発機構
委託先　グリッドスカイウェイ有限責任事業組合

本調査報告書は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務「産業DXのためのデジタルインフラ整備事業／デジタルライフラインの先行実装に資する基盤に関する研究開発／ドローン航路」の結果得られたものです。

目　次

1. 調査報告書の概要

1-1 背景と目的

現在、政府はドローン産業の市場活性化および社会実装の促進を目指し、民間事業者が個別に実施している汎用的な業務の一元化を進めている。この一元化により、民間事業者のコスト負担が軽減され、サービス価格の適正化が促進されることが期待される。その一環として、ドローン航路システムの提供が進められ、これにより、個別の事業者が実施している航路関連の手続きや業務がシステム化され、サービスとして提供されることとなる。

ドローン航路システムにおけるサービス提供は、重要インフラの一環として位置づけられ、国土交通省をはじめとする重要インフラ所管省庁との連携やデータの共有が求められる。これに伴い、サイバーセキュリティの強化は重要な課題であり、政府が定めたサイバーセキュリティ基本法や重要インフラのセキュリティ基準に準拠した対策が必須となる。特に、ドローン航路システムはサイバーセキュリティ基本法に基づく重要インフラに関連するため、安全保障面での適切なセキュリティ対策を講じることが求められることになる。

本「ドローン航路システムのセキュリティ調査報告書」書（以下「本調査報告書」という）は、ドローン航路システムに関するサイバーセキュリティ対策の骨格を示す方針案を策定し、ドローン航路に係るセキュリティ対策検討の参考文書となることを目的としている。そのために、サイバーセキュリティ基本法に基づく「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」 (以下「統一基準」という)を指針とし、この基準を踏まえたセキュリティ対策の方針案を作成する。

1-2 調査報告書の位置づけ

本調査報告書は「ドローン航路運営者向けドローン航路導入ガイドライン Ver1.0」及びその附属書並びに「運航事業者向けドローン航路運航ガイドライン Ver1.0」の将来的な改版に向けて関連する論点等について、事前に調査を実施した参考資料である。

本資料はガイドラインとの整合性を担保する、またはガイドラインを補完する位置付けの文書ではなく、本事業において将来的に必要と考えられる論点に対して仮説的に調査を行ったものであるということに留意する必要がある。また、本調査報告書は最新版を利用するとともに関連する法令が最新の内容であることを確認して利用すること。

1-3 調査報告書利用時の留意点

本調査報告書を以下の事項に注意して利用すること。

- ドローン航路等に関する正式な定義及び仕様・規格等については、「ドローン航路運営者向けドローン航路導入ガイドライン」及びその附属書並びに「運航事業者向けドローン航路運航ガイドライン」の最新版を参照すること。本資料はあくまで、ガイドラインとは紐づいていない調査報告書であり、本調査報告書の利用にあっては、必ず利用者が責任をもってガイドラインとの整合性について調査・分析を事前に実施し、定義・解釈等に齟齬が存在する場合は、ガイドラインに準じること。
- 本調査報告書の記載内容と、法令・規格等で定められる内容が異なる場合は、法令・規格等を

遵守すること。

・ 本調査報告書を利用した結果生じた損害に対して、NEDO、グリッドスカイウェイ有限責任事業組合は一切の責任を負わない。

2. システム構成概要

ドローン航路システムは複数のサービス利用者・関係者向けに、外部システムやその他の取り組みと連携しながら、ドローン航路の画定・予約・手配・運航管理等のサービス提供を行う。

飛行するドローンの操作・飛行情報等は UTMS（ドローン運航管理システム）を介して情報を収集・保存し、飛行するドローンとの直接的なアクセスはしない。

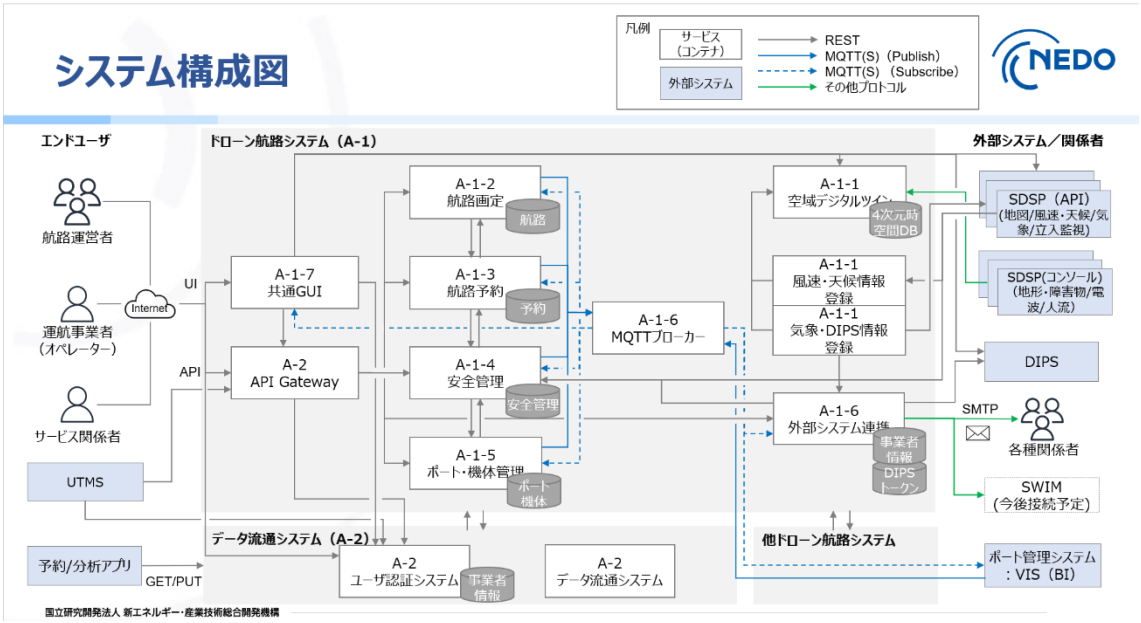


図 1　ドローン航路システムの概要

3. 情報の格付の区分

統一基準 1.2 において定義されている情報の格付の区分・取扱制限を以下に再度掲載する。

情報について、機密性、完全性及び可用性の 3 つの観点を区別し、本統一基準の遵守事項で用いる格付の区分の定義を示す。

なお、機関等において格付の定義を変更又は追加する場合には、その定義に従って区分された情報が、本統一基準の遵守事項で定めるセキュリティ水準と同等以上の水準で取り扱われるようにしなければならない。

3-1 機密性についての格付の定義

格付の区分	分類の基準
機密性３情報	国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取扱いを要する情報 独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報
機密性２情報	国の行政機関における業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報 独立行政法人における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報。また、指定法人のうち、独法等情報公開法の別表第一に掲げる法人（以下「別表指定法人」という。）についても同様とする。 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報
機密性１情報	国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 独立行政法人又は別表指定法人における業務で取り扱う情報のうち、独法等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報

なお、機密性２情報及び機密性３情報を「要機密情報」という。

3-2 完全性についての格付の定義

格付の区分	分類の基準
完全性２情報	業務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は業務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報（書面を除く。）

なお、完全性２情報を「要保全情報」という。

3-3 可用性についての格付の定義

格付の区分	分類の基準
可用性２情報	業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報（書面を除く。）

なお、可用性２情報を「要安定情報」という。

また、その情報が要機密情報、要保全情報及び要安定情報に一つでも該当する場合は「要保護情報」という。

4. システム業務概要

ドローン航路システムでは「表 1 Actor 整理表」に記載の利用者によって「表 2 システム業務一覧」の業務が実施される。ここで、システムを直接操作するユーザのことを Actor（アクター）と呼び、「図 1 ドローン航路システムの概要」に記載の Actor を、一般的な「サービス利用者」「システム管理者」の分類で整理する。

なお、各業務の詳細内容は「別紙①業務・データフロー（業務名）」を参照すること。

表 1 Actor 整理表

分類	Actor		システム利用方法	
			ネットワークアクセス	利用端末
サービス利用者				
ドローン航路システムのサービスを利用する利用者を記入する。	ドローン航路運営者	ドローン航路を整備、管理し、ドローン航路システムを使用して提供する者。	インターネットアクセス	自社端末・個人端末
	運航事業者	ドローン航路システムを使用して、提供されているドローン航路の予約およびドローンの飛行を行う。	インターネットアクセス	自社端末・個人端末
	サービス関係者（地上関係者、上空関係者、地方自治体等）	ドローン航路に関連する土地や上空の関係者。ドローン航路の情報や、運航の情報をドローン航路システムを通して把握し、リスクの評価を行う者。	インターネットアクセス	自社端末・個人端末
システム管理者				
ドローン航路システムの開発・運用等の維持管理でシステムにアクセスする利用者を記入する。	ドローン航路システム事業者	ドローン航路システムを構築、保守及び運用し、ドローン航路運営者に機能を提供する者。ドローン航路運営者が兼務する可能性あり（事業者次第）。	インターネットアクセス	自社端末・個人端末

表 2 システム業務一覧

#	業務	業務タスク	取り扱い情報	ドローン航路運営者	運航事業者	サービス関係者
1	航路画定	最大落下許容範囲登録・削除	最大落下許容範囲	○		
2		最大落下許容範囲参照	最大落下許容範囲	○	○	○
3		航路画定・削除・閉塞	航路	○		
4		航路参照	航路	○	○	○
5		航路と離着陸場の紐づけ	航路 離着陸場	○		
6		関係者登録	航路 事業者情報	○		
7	航路予約	航路予約・キャンセル	航路予約		○	
8		航路予約参照	航路予約	○	○	○
9		航路予約撤回	航路予約	○		
10	安全管理	運航状況参照	運航情報	○	○	
11		航路適合性評価	風速・天候 第三者立入監視 規制／イベント 鉄道運行	○	○	
12	離着陸場・機体管理	離着陸場登録・更新・削除	離着陸場	○		
13		離着陸場参照	離着陸場	○	○	○
14		機体登録・更新・削除	機体	○		
15		機体参照	機体	○	○	○
18		離着陸場予約登録・更新・削除	離着陸場予約		○	
17		離着陸場予約参照	離着陸場予約	○	○	○
18		機体予約登録・更新・削除	機体予約		○	
19		機体予約参照	機体予約	○	○	○

#	業務	業務タスク	取り扱い情報	ドローン航路運営者	運航事業者	サービス関係者
20	ユーザ認証	ログイン	事業者情報	○	○	○
21		ユーザ情報登録	事業者情報	○		
22	共通	画面共通	（動的） 地図 風速・天候 気象 第三者立入監視 DIPS 情報 （静的） 地形・障害物 電波 人流	○	○	○

5. 取り扱う情報資産

ドローン航路システムにて取り扱う情報および機密性・完全性・可用性の格付けは「別紙②情報資産整理表」に整理される。

「表 3 情報資産整理表（例）」に一部抜粋したように、機密性・完全性・可用性の格付け“２”以上である要保護情報が存在していることから、適切な情報セキュリティ対策が求められる。

表 3 情報資産整理表（例）

格付け		業務・機能	取り扱い情報
機密性	3	なし	なし
	2	ユーザ認証	事業者情報（ユーザ認証システム管理、航路システム管理） 例：事業者メールアドレス、ログイン ID/パスワード、事業者 ID
	1	航路画定	当該業務・機能における全ての取り扱い情報
		外部データ参照	当該業務・機能における全ての取り扱い情報
		ユーザ認証	アクセストークン 例：アクセストークン、リフレッシュトークン
完全性	2	航路画定	最大落下許容範囲情報、飛行経路/ドローン航路情報、航路対応機種情報 例：最大落下許容範囲 ID、航路画定 ID、対応機種 ID
		航路予約	航路予約情報

格付け		業務・機能	取り扱い情報
			例：運航事業者 ID、航路予約 ID、航路区画 ID
		安全管理	航路予約情報、運航情報、リモート ID 情報 例：航路予約毎の識別 ID、予約開始日時、シリアルナンバー、フライト識別 ID
		離着陸場・機体管理	ドローンポート情報、ドローンポート予約情報、機体情報 例：ドローンポート ID、ドローンポート予約 ID、機体 ID、製造番号
		外部データ参照	外部データ（蓄積）※航路システムに蓄積する情報 例：風速・天候情報、第三者立入監視情報、飛行禁止エリア情報、地形・障害物情報、電波情報、人流情報
		ユーザ認証	事業者情報（ユーザ認証システム管理、航路システム管理） 例：事業者メールアドレス、ログイン ID/パスワード、事業者 ID
	1	航路画定	紐づけ情報（航路-離着陸場、航路-事業者情報） 例：ドローンポート-航路区画マッピング ID、航路区画 ID、航路 ID、事業者 ID
		航路予約	メール周知履歴 例：事業者 ID、周知種別、周知先、送信内容
		安全管理	運航情報蓄積 例：テレメトリ情報取得日時、運航状況、飛行時間
		離着陸場・機体管理	ドローンポート状態、VIS テレメトリ情報、機体リソース管理 例：動作状況(使用可、使用不可)、VIS ステータス、予約日時範囲
		外部データ参照	外部データ（リアルタイム）※外部システムから API で取得する情報、DIPS トークン 例：地図情報、風速・天候情報、気象情報、第三者立入監視情報、アクセストークン、リフレッシュトークン
		ユーザ認証	アクセストークン 例：アクセストークン、リフレッシュトークン
可用性	2	航路画定	最大落下許容範囲情報、飛行経路/ドローン航路情報 例：最大落下許容範囲 ID、最大標高・地形、航路区画情報
		安全管理	航路予約情報、運航情報、リモート ID 情報 例：航路予約毎の識別 ID、予約開始日時、シリアルナンバー、フライト識別 ID
		外部データ参照	外部データ（リアルタイム）※外部システムから API で取得する情報 例：地図情報、風速・天候情報、気象情報、第三者立入監視情報
		ユーザ認証	アクセストークン 例：アクセストークン、リフレッシュトークン
	1	航路画定	航路対応機種情報、紐づけ情報（航路-離着陸場、航路-事業者情報） 例：対応機種 ID、ドローンポート-航路区画マッピング ID、航路区画 ID
		航路予約	航路予約情報、メール周知履歴

格付け		業務・機能	取り扱い情報
			例：航路予約毎の識別 ID、予約開始日時、周知種別、周知先、送信内容
		安全管理	運航情報蓄積 例：テレメトリ情報取得日時、運航状況、飛行時間
		離着陸場・機体管理	ドローンポート情報、ドローンポート状態、ドローンポート予約情報、VIS テレメトリ情報、機体情報、機体リソース管理 例：ドローンポート ID、動作状況(使用可、使用不可)、ドローンポート予約 ID、VIS ステータス、機体 ID、機体予約 ID
		外部データ参照	DIPS トークン 例：アクセストークン、リフレッシュトークン、ID トークン
		ユーザ認証	アクセストークン 例：アクセストークン、リフレッシュトークン

6. リスク評価

ドローン航路システムはドローン航路の画定・予約・手配・運航管理等の各種手続きをインターネット経由でサービス提供を行っており、リアルタイムでのデータ通信や外部システムとの連携機能を有している。また業務の特性として、ドローンの運航が人命や公共の安全に関わる可能性があるため、悪意のある攻撃や不正アクセスによる影響が広範囲に及ぶリスクがある。こういった背景からシステムのセキュリティ確保は非常に重要であり、外部からの脅威に対する十分な対策が求められる。

「表 4 ドローン航路システムにおける外部脅威（例）」では、格付けした取り扱い情報について想定される外部脅威リスクについて例示している。

ドローン航路システムにおける外部脅威に関するリスクについての詳細は「別紙③リスク・技術対策一覧」を参照すること。

表４ ドローン航路システムにおける外部脅威（例）

格付け		業務・機能毎の取り扱い情報	想定脅威に対するリスク
機密性	3	なし	なし
	2	➢ **ユーザ認証** 事業者情報（ユーザ認証システム管理、航路システム管理）	・アカウント情報が漏洩するとアカウント乗っ取りに利用される。 例）フィッシングやブルートフォース攻撃によるアカウント情報奪取 ・メールアドレスが奪われるとアカウントの悪用や機密情報の漏洩につながる。 例）フィッシングによる情報漏洩
	1	機密性 2 以外の全ての取り扱い情報	影響は限定的だが、サイバー攻撃により特権 ID の悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例）SQL インジェクションによる情報搾取

格付け		業務・機能毎の取り扱い情報	想定脅威に対するリスク
完全性	2	➢ **航路画定** ・最大落下許容範囲情報 ・飛行経路/ドローン航路情報 ・航路対応機種情報 ➢ **航路予約** ・航路予約情報 ➢ **安全管理** ・航路予約情報、運航情報 ・リモート ID 情報 ➢ **離着陸場・機体管理** ・ドローンポート情報 ・ドローンポート予約情報 ・機体情報 ➢ **外部データ参照** ・外部データ（蓄積） ※航路システムに蓄積する情報 ➢ **ユーザ認証** ・事業者情報（ユーザ認証システム管理、航路システム管理）	・情報が改ざんされると誤った航路情報となり、不正な航路飛行や事故につながる。 例）クロスサイトスクリプティング、標的型攻撃による情報の改ざん ・分析情報が改ざん・破壊されるとビジネスとして不利益を被る。 例）ランサムウェアによる蓄積情報の改ざん・破壊 ・アカウント情報が改ざん・破壊されるとユーザがサービスを利用できなくなる。 例）ランサムウェアによる情報の改ざん・破壊 ・ユーザ情報が改ざんされるとサービスの利用不可や異なる権限へアクセスが可能となりサービス利用に障害が生じる。 例）ランサムウェアによるユーザ情報の改ざん・破壊
	1	完全性２以外の全ての取り扱い情報	・影響は限定的であるものの、サイバー攻撃により特権 ID が奪われ情報が改ざん、破壊される。 例）標的型攻撃による特権 ID の取得
可用性	2	➢ **航路画定** ・最大落下許容範囲情報 ・飛行経路/ドローン航路情報 ➢ **安全管理** ・航路予約情報 ・運航情報 ・リモート ID 情報	・サイバー攻撃によりシステムサービス提供を妨害される。 例）DDoS 攻撃によるシステムサービス停止 ・サイバー攻撃により情報が破壊されると航路が参照できずサービス停止、事故につながる。 例）ランサムウェアによる情報の破壊 ・サイバー攻撃により情報が改ざん・破壊されるとフライト中の参照が不可能となり飛行に支障がでる。 例）ランサムウェアによる情報の破壊

格付け		業務・機能毎の取り扱い情報	想定脅威に対するリスク
		➢ **外部データ参照** ・外部データ（リアルタイム） ※外部システムから API で取得する情報 ➢ **ユーザ認証** ・アクセストークン	・サイバー攻撃によりシステムが利用不可となるとサービス提供や業務が妨害される。また、サービス提供ができなくなる。 例）DDoS 攻撃によるシステムサービス停止
	1	可用性２以外の全ての取り扱い情報	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害されることでシステム運用、サービス提供に支障が生じる。 例）DDoS 攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可

7. セキュリティ対策指針

7-1 取り扱い情報毎の対策指針

前章で導出したリスクに対して、「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」を参考にシステム構成要素（端末・サーバ・通信回線・ソフトウエア・アプリケーションコンテツ）単位で対策すべき指針を文書化し、今後のドローン航路に係るセキュリティ対策検討の基礎となる骨格を策定する。

具体的な対策案、および対策の具体例については「別紙③リスク・技術対策一覧」に記載されている「技術対策（案）_対策の具体例」のシートを参照すること。

表５　技術対策案（例）

格付け		業務・機能毎の取り扱い情報	対策例
機密性	3	該当なし	該当なしのため対象外
	2	➢ **ユーザ認証** 事業者情報（ユーザ認証システム管理、航路システム管理）	・主体認証を行うシステムにおける主体認証情報の不正行為防止対策 ・取り扱う情報や取扱制限等に応じたアクセス権限の設定機能の導入 ・取り扱い情報の暗号化機能の必要性検討、および導入 ・各構成要素の脆弱性管理、対策計画および措置の実施 例） ・主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定める ・セキュリティリスクが高い機器等について、セキュリティパッチの適用又はソフトウェアのバージョンアップ等の措置を講ずる ・ファイル暗号化等のセキュリティ機能を持つアプリケーションの導入 ・ウィルス対策ソフトによるスキャンで不正プログラムの検知

格付け		業務・機能毎の取り扱い情報	対策例
	1	機密性 2 以外の全ての取り扱い情報	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
完全性	2	➢ **航路画定** ・最大落下許容範囲情報 ・飛行経路/ドローン航路情報 ・航路対応機種情報 ➢ **航路予約** ・航路予約情報 ➢ **安全管理** ・航路予約情報、運航情報 ・リモート ID 情報 ➢ **離着陸場・機体管理** ・ドローンポート情報 ・ドローンポート予約情報 ・機体情報 ➢ **外部データ参照** ・外部データ（蓄積） ※航路システムに蓄積する情報 ➢ **ユーザ認証** ・事業者情報（ユーザ認証システム管理、航路システム管理）	・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。 例） ・電磁的記録媒体に対する電子署名、タイムスタンプの付与 ・TLS 機能の導入 ・バックアップデータの暗号化、不正プログラムの検出措置、危機的事象（天災、情報セキュリティインシデント）を想定した適切な保管場所の選定 ・正式な証明書発行機関により発行された電子証明書（サーバ証明書）の導入 ・暗号技術検討会及び関連委員会（CRYPTREC）の「TLS 暗号設定ガイドライン」に準拠した設定の実施 ・「電子政府推奨暗号リスト」に準拠した暗号化アルゴリズムの導入
	1	完全性 2 以外の全ての取り扱い情報	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば盗聴及び改ざんの防止策として TLS 機能の導入や、定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること等が該当する。
可用性	2	➢ **航路画定** ・最大落下許容範囲情報 ・飛行経路/ドローン航路情報	・適切な方法で情報のバックアップを実施すること。 ・インターネットからアクセスを受ける情報システムはサービス不能攻撃（DDoS 攻撃）への対策を行うこと。また、サービス不能攻撃の被害を最小化する手段を備えたシステム構築を検討すること。

格付け		業務・機能毎の取り扱い情報	対策例
		➢ **安全管理** ・航路予約情報 ・運航情報 ・リモート ID 情報 ➢ **外部データ参照** ・外部データ（リアルタイム） ※外部システムから API で取得する情報 ➢ **ユーザ認証** ・アクセストークン	・サービス不能攻撃を受けるシステム構成要素に対する監視対策を実施すること。 例） ・サーバ装置、通信回線等の冗長化 ・許容停止時間等を踏まえた、バックアップの取得 ・論理的に切り離されたネットワークへのバックアップ保存 ・サイバー攻撃を考慮した物理的な媒体へのバックアップ保存 ・通信回線の性能低下や異常の有無を確認することを目的とした、通信回線利用率、接続率等の運用状態を定常的に確認、分析する機能の導入 ・端末等がシステムと通信可能な代替手段の整備
	1	可用性 2 以外の全ての取り扱い情報	影響が限定的でリスクが低いものの一般的な DDoS 対策（例：トラフィック監視、過剰なトラフィックの自動遮断）を実施し、必要に応じて外部サービスを活用すること。また、システムの可用性を保つための監視体制を整えること。

7-2 外部システムとの接続に関する対策指針

外部システムとの接続部分のセキュリティ対策については、「7-1 取り扱い情報毎の対策指針」に従って検討することに加え、「表６　外部システムとの接続部分のセキュリティ対策例」に示すとおり、システム認証や API 実行時のトークン検証等の仕組みを外部システム側の要件とも調整して実装すること。

表６　外部システムとの接続部分のセキュリティ対策例

ドローン航路システム周辺の外部システム	入出力	セキュリティ対策例
UTMS	入力 (運航情報)	ユーザ認証システムを利用したシステム認証（API キーの事前発行）
予約/分析アプリ	出力 (予約情報等)	ユーザ認証システムを利用したシステム認証（API キーの事前発行）
DIPS	入力 (飛行禁止エリア情報)	DIPS API 仕様に従った個別認証
SDSP	入力 (地図、気象情報等)	システムごとの個別認証
VIS	入出力 (ポートに関する情報)	MQTTS によるシステム認証

8. セキュリティ推進体制

セキュリティ対策を推進するために組織に応じた体制づくりが必要となる。「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」を参考として、以下に情報セキュリティ体制を例示する。

各役割については「表　7　役割体制」に内容をまとめる。具体的な体制整備にあたっては、組織が担う業務範囲や目的、規模等に応じた適切な体制が求められる。

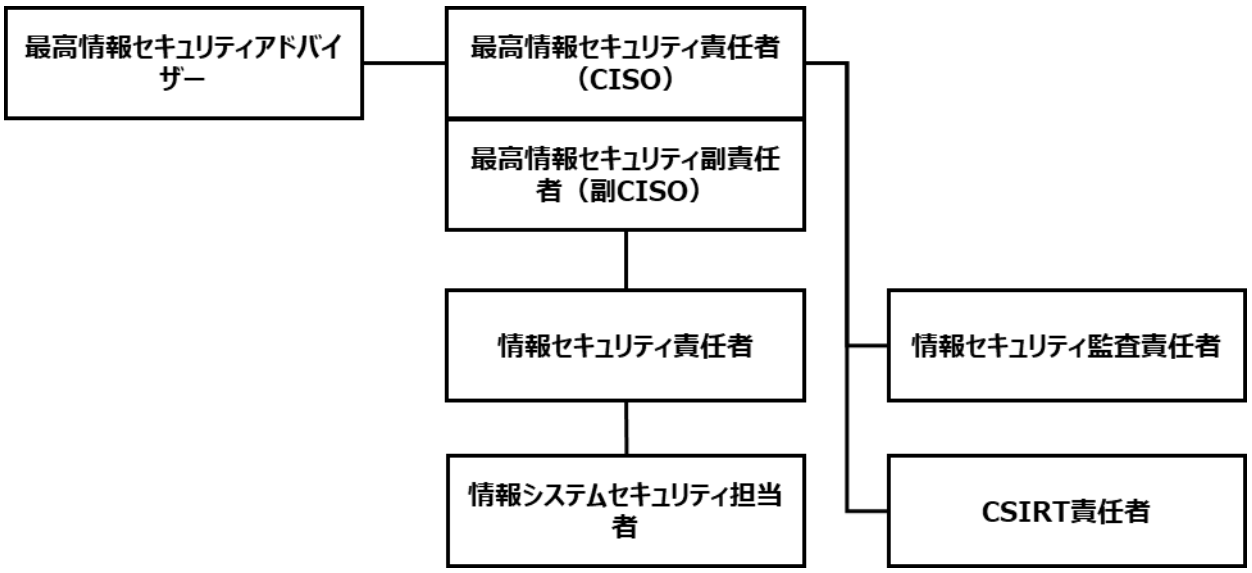


図２　体制イメージ

表７　役割体制

役割	内容
最高情報セキュリティ責任者 （CISO）	組織等における情報セキュリティに関する事務を統括する 例）情報セキュリティ対策推進のための組織・体制の整備、対策基準の決定・見直し
最高情報セキュリティ副責任者 （副 CISO）	最高情報セキュリティ責任者の命を受けて組織等の情報セキュリティに関する事務を統括する 例）対策推進計画の決定・見直し（情報セキュリティに関する重要事項のうち、最高情報セキュリティ責任者に委任されたもの）
情報セキュリティ監査責任者	最高情報セキュリティ責任者の指示に基づき実施する監査に関する事務を統括する 例）監査実施計画の策定、監査実施体制の整備
最高情報セキュリティアドバイザー	情報セキュリティについて専門的な知識及び経験を有する者であり、最高情報セキュリティ責任者が業務内容を定める

役割	内容
	例）機関等全体の情報セキュリティ対策の推進に係る最高情報セキュリティ責任者及び最高情報セキュリティ副責任者への助言
情報セキュリティ責任者	最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐し、情報セキュリティ対策に関する事務を統括する。複数のベンダー・組織で対応する場合、情報セキュリティ責任者を統括する統括情報セキュリティ責任者を配置することもある 例）情報セキュリティ対策に関する運用規程・実施手順の整備及び見直し
情報システムセキュリティ担当者	所管する情報システムに対する情報セキュリティ対策に関する事務の担当者。区域（施設及び執務環境に係る対策を行う単位）ごと、課室ごとに設置する場合もある 例）所管情報システムへの情報セキュリティ対策の実施
CSIRT	組織における情報セキュリティインシデントに対処するための体制（専門的な知識または適正を有する責任者、職員等）

9. まとめ

本調査報告書では、航路運営者がドローン航路システムの運用及びサービス提供を行う際に必要なサイバーセキュリティ対策の調査を行った。本調査報告書がドローン航路に係るセキュリティ検討の一助となれば幸いである。

10. 参考文献

・ 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

(https://www.nisc.go.jp/policy/group/general/kijun.html)

11. 別紙

・ 【調査報告書】ドローン航路システムのセキュリティ調査報告書_別紙①業務・データフロー

・ 【調査報告書】ドローン航路システムのセキュリティ調査報告書_別紙②情報資産整理表

・ 【調査報告書】ドローン航路システムのセキュリティ調査報告書_別紙③リスク・技術対策一覧

別紙①：業務・データフロー

業務・データフロー

・対象業務	航路画定
・業務概要	最大落下許容範囲にドローン航路を設定すること。 具体的な空間位置の設定と、落下分散範囲を考慮し飛行可能なドローンの条件をドローン航路運営事業者が定めること。 ドローン航路システムに条件が格納される。

NO	業務タスク	運航事業者	ドローン航路運営者	関係者	ドローン航路システム	関連システム	取扱い情報
1	最大落下許容範囲登録・削除		最大落下許容範囲作成/申請キャンセル		A-1-2_航路画定機能 最大落下許容範囲		①最大落下許容範囲情報
2	最大落下許容範囲参照		最大落下許容範囲一覧/詳細		A-1-2_航路画定機能		①最大落下許容範囲情報
3	航路画定・削除・閉塞		航路作成/申請取り下げ 航路閉塞/申請取り下げ		A-1-2_航路画定機能 飛行経路/ドローン航路 航路対応機種		②飛行経路/ドローン航路情報 ③航路対応機種情報
4	航路参照		航路画定一覧/詳細 航路閉塞一覧/詳細		A-1-2_航路画定機能		②飛行経路/ドローン航路情報 ③航路対応機種情報
5	航路と離着陸場の紐づけ		航路-離着陸場の紐づけ API手動実行		A-1-2_航路画定機能 紐づけ情報（航路-離着陸場）		④紐づけ情報（航路-離着陸場） *※今年度は画面がないため、APIを手動実行して紐づけ* *情報の作成ではなく、情報間の紐づけ*
6	関係者登録		関係者登録 メール受信		A-1-6_外部システム連携機能 紐づけ情報（航路-事業者情報）		⑤紐づけ情報（航路-事業者情報） ＜業務で必要となる情報＞ 周知先メールアドレス *※航路画定時に、関係者にメールが通知（関係者周知）される* *情報の作成ではなく、情報間の紐づけ*

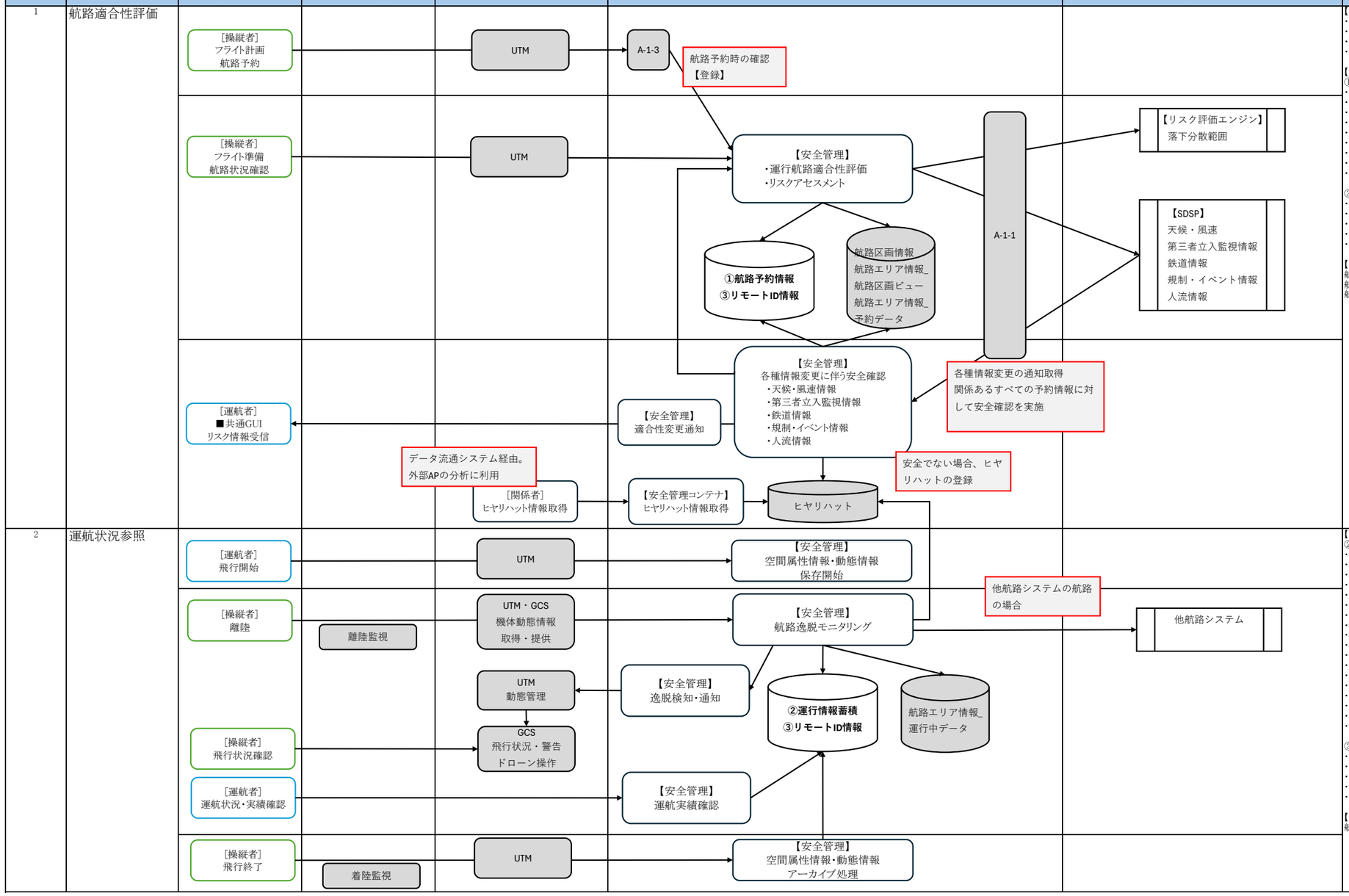
業務・データフロー

・対象業務	航路予約
・業務概要	運航事業者の利用用途に合わせて、予約するドローン航路の航路区画の設定と、予約の開始日時・終了日時を設定し、航路予約情報を作成・取り下げすること。 ドローン航路システムに航路予約情報が格納される。 航路予約情報を一覧や詳細にて確認すること。 航路運営事業者が航路のメンテナンスを行うために、すでに予約されている航路予約情報を撤回すること。 航路予約情報が作成・取り消し・撤回された場合、予約者や予約された航路の関係者にメール通知されること。

NO	業務タスク	運航事業者	ドローン航路運営者	関係者	ドローン航路システム	関連システム	取扱い情報
1	航路予約・キャンセル	航路予約情報作成 航路予約情報取り下げ		メール受信 (予約した航路に関連する 関係機関のみ)	**A-1-3_航路予約機能** 航路予約情報更新 航路予約情報通知 **①航路予約情報** **A-1-6_外部システム連携機能** 航路予約通知情報更新 関係者通知 **②航路予約情報** **③予約航路関連情報** **④メール周知履歴**		①航路予約情報 運航事業者ID 航路予約ID 航路区画ID 航路区画毎の予約開始日時 航路区画毎の予約終了日時 航路予約ステータス 予約完了日時 予約状態更新日時(登録時も更新) ②航路予約情報 航路予約ID 運航事業者(予約者)ID PublishイベントID 処理区分 予約完了日時 予約状態更新日時 ③予約航路関連情報 航路予約ID 航路区画ID 予約開始日時 予約終了日時 ④メール周知履歴 メール送信内容や送信結果等 ＜メール周知にて参照するデータ＞ ■周知先情報 メールアドレス 事業者名
2	航路予約参照	航路予約情報一覧/詳細			**A-1-3_航路予約機能** 航路予約情報取得 **①航路予約情報**		①航路予約情報 運航事業者ID 航路予約ID 航路区画ID 航路区画毎の予約開始日時 航路区画毎の予約終了日時 航路予約ステータス 予約完了日時 予約状態更新日時(登録時も更新)
3	航路予約撤回	航路予約情報撤回 メール受信 (予約者のみ)		メール受信 (予約した航路に関連する 関係機関のみ)	**A-1-3_航路予約機能** 航路予約情報更新 航路予約情報通知 **①航路予約情報** **A-1-6_外部システム連携機能** 航路予約通知情報更新 関係者通知 **②航路予約情報** **③予約航路関連情報** **④メール周知履歴**		①航路予約情報 運航事業者ID 航路予約ID 航路区画ID 航路区画毎の予約開始日時 航路区画毎の予約終了日時 航路予約ステータス 予約完了日時 予約状態更新日時(登録時も更新) ②航路予約情報 航路予約ID 運航事業者(予約者)ID PublishイベントID 処理区分 予約完了日時 予約状態更新日時 ③予約航路関連情報 航路予約ID 航路区画ID 予約開始日時 予約終了日時 ④メール周知履歴 メール送信内容や送信結果等 ＜メール周知にて参照するデータ＞ ■周知先情報 メールアドレス 事業者名

業務・データフロー

・対象業務	安全管理
・業務概要	適合性評価に必要な情報を受信し、航路の適合性評価を実施する。 航路の予約IDとフライトを実施する機体のリモートIDの紐付けを実施する。 ヒヤリハット情報（適合性評価にて安全不正）を生成し、MQTT経由で配信及びAPIにて返却する。



【外部情報】
・風速・天候情報
・第三者立入監視情報
・規制／イベント情報
・鉄道運行情報

【テーブル】
①航路予約情報
・航路予約毎の識別ID
・予約開始日時
・予約終了日時
・予約登録日時
・航路区画ID配列
・運航事業者ID
・適合性評価結果
・第三者立入監視情報 適合性評価結果
・鉄道運航情報 適合性評価結果

③リモートID情報（t_remote_data）
・航路予約毎の識別ID
・シリアルナンバー
・登録ID
・セッションID
・フライト識別ID

【ビュー】
航路区画情報ビュー
航路エリア情報_航路区間ビュー
航路エリア情報_予約データビュー

【テーブル】
②運行情報蓄積（t_drone_location）
・エリア情報のサブスクリプション ID
・機体の登録 ID
・機体の種別
・テレメトリ情報取得日時
・緯度
・経度
・対地高度
・機体の進行方向
・機体の速度
・機体の垂直速度
・航路逸脱割合
・航路逸脱割合更新時刻
・航路予約 ID
・航路 ID
・航路区画 ID
・運航状況
・運航者 ID
・飛行時間

③リモートID情報（t_remote_data）
・航路予約毎の識別ID
・シリアルナンバー
・登録ID
・セッションID
・フライト識別ID

【ビュー】
航路エリア情報_運航中データビュー

業務・データフロー

・対象業務	離着陸場・機体管理
・業務概要	・離着陸場・機体の情報を格納すること。また、格納した情報を一覧から確認できること。 ・航路予約時に離着陸場予約・機体予約を実施すること。また、予約情報を一覧から確認できること。

NO	業務タスク	運航者	ドローン航路運営事業者	関係者	ドローン航路システム	関連システム	取扱い情報
1	離着陸場登録・更新・削除		離着陸場登録・更新・削除		A-1-5 離着陸場・機体管理機能 離着陸場登録・更新・削除 離着陸場情報		①離着陸場情報(マスタデータ管理) ■ドローンポート情報 ドローンポートID, ドローンポート名, 設置場所住所, 製造メーカー, 製造番号, 離着陸場種類, VISドローンポート事業者ID, 緯度, 経度, 着陸面対地高度, 対応機体, 画像, 画像フォーマット, オペレータID, 更新者ID, 登録日時, 更新日時, 削除フラグ ■ドローンポート状態 ドローンポートID, 動作状況(使用可), 動作状況(使用不可), 使用不可日時範囲, 格納中機体ID, オペレータID, 更新者ID, 登録日時, 更新日時, 削除フラグ ■VISテレメトリ情報 ドローンポートID, IPアドレス, ドローンポート名, ドローンポートステータス, VISステータス, 緯度, 経度, 着陸面対地高度, 風向, 風速, 最大風速時風向, 最大風速, 雨量, 気温, 湿度, 気圧, 照度, 紫外線, 観測時間, 侵入検知有無, 検知物カテゴリ, 閾値(風速), 拠点ID, 拠点住所, 拠点名称, 拠点ステータス, ドローンポート使用可否状態, エラーコード, エラー内容
2	離着陸場参照	離着陸場参照			A-1-5 離着陸場・機体管理機能 離着陸場情報取得 離着陸場情報		①離着陸場情報 ■ドローンポート情報 ドローンポートID, ドローンポート名, 設置場所住所, 製造メーカー, 製造番号, 離着陸場種類, VISドローンポート事業者ID, 緯度, 経度, 着陸面対地高度, 対応機体, 画像, 画像フォーマット, オペレータID, 更新者ID, 登録日時, 更新日時, 削除フラグ ■ドローンポート状態 ドローンポートID, 動作状況(使用可), 動作状況(使用不可), 使用不可日時範囲, 格納中機体ID, オペレータID, 更新者ID, 登録日時, 更新日時, 削除フラグ ■VISテレメトリ情報 ドローンポートID, IPアドレス, ドローンポート名, ドローンポートステータス, VISステータス, 緯度, 経度, 着陸面対地高度, 風向, 風速, 最大風速時風向, 最大風速, 雨量, 気温, 湿度, 気圧, 照度, 紫外線, 観測時間, 侵入検知有無, 検知物カテゴリ, 閾値(風速), 拠点ID, 拠点住所, 拠点名称, 拠点ステータス, ドローンポート使用可否状態, エラーコード, エラー内容
3	機体登録・更新・削除		機体登録・更新・削除		A-1-5 離着陸場・機体管理機能 機体登録・更新・削除 機体情報		②機体情報(マスタデータ管理) ■機体情報 機体ID, 機体名, 製造メーカー, 製造番号, 機体の種類, 最大離陸重量, 重量, 最大速度, 最大飛行時間, 位置情報(緯度), 位置情報(経度), 機体認証の有無, DIPS登録記号, 機体所有種別, 所有者ID, 画像データ, 画像フォーマット, オペレータID, 更新者ID, 登録日時, 更新日時, 削除フラグ
4	機体参照	機体参照			A-1-5 離着陸場・機体管理機能 機体情報取得 機体情報		②機体情報 ■機体情報 機体ID, 機体名, 製造メーカー, 製造番号, 機体の種類, 最大離陸重量, 重量, 最大速度, 最大飛行時間, 位置情報(緯度), 位置情報(経度), 機体認証の有無, DIPS登録記号, 機体所有種別, 所有者ID, 画像データ, 画像フォーマット, オペレータID, 更新者ID, 登録日時, 更新日時, 削除フラグ

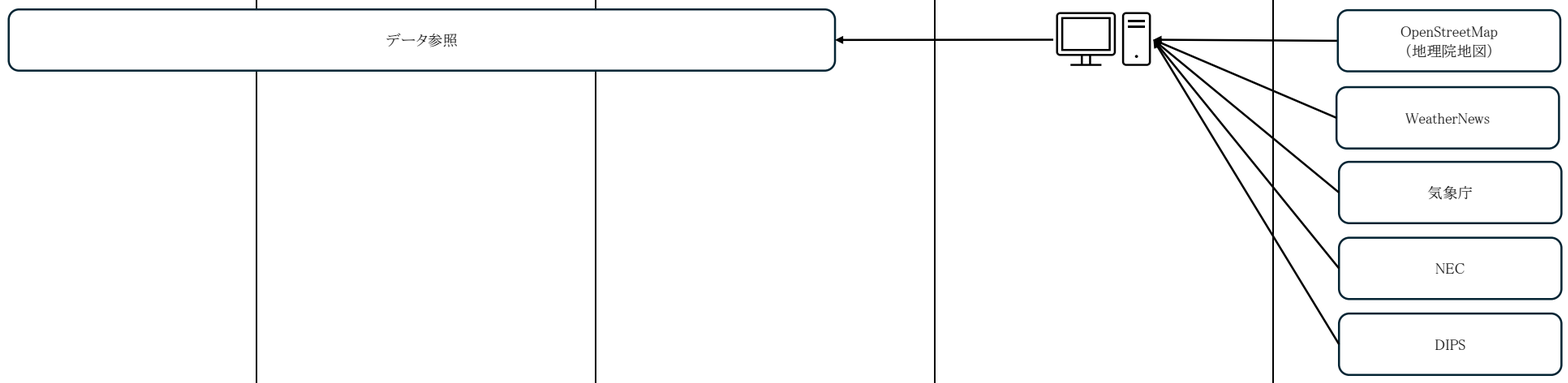
業務・データフロー

・対象業務	離着陸場・機体管理
・業務概要	・離着陸場・機体の情報を格納すること。また、格納した情報を一覧から確認できること。 ・航路予約時に離着陸場予約・機体予約を実施すること。また、予約情報を一覧から確認できること。

NO	業務タスク	運航者	ドローン航路運営事業者	関係者	ドローン航路システム	関連システム	取扱い情報
5	離着陸場予約登録・更新・削除	離着陸場予約登録・更新・削除			**A-1-5 離着陸場・機体管理機能** 離着陸場予約登録・更新・削除 **離着陸場予約情報**		③離着陸場予約情報（航路予約と合わせて実施） ■ドローンポート予約情報 ドローンポート予約ID，ドローンポートID，使用機体ID，航路予約ID，利用形態，予約日時範囲，予約有効フラグ，オペレータID，更新者ID，登録日時，更新日時，削除フラグ
6	離着陸場予約参照	離着陸場予約参照			**A-1-5 離着陸場・機体管理機能** 離着陸場予約情報取得 **離着陸場予約情報**		③離着陸場予約情報 ■ドローンポート予約情報 ドローンポート予約ID，ドローンポートID，使用機体ID，航路予約ID，利用形態，予約日時範囲，予約有効フラグ，オペレータID，更新者ID，登録日時，更新日時，削除フラグ
7	機体予約登録・更新・削除	機体予約登録・更新・削除			**A-1-5 離着陸場・機体管理機能** 機体予約登録・更新・削除 **機体予約情報**		④機体予約情報（航路予約と合わせて実施） ■機体リソース管理 機体予約ID，機体ID，予約日時範囲，オペレータID，更新者ID，登録日時，更新日時，削除フラグ
8	機体予約参照	機体予約参照			**A-1-5 離着陸場・機体管理機能** 機体予約情報取得 **機体予約情報**		④機体予約情報 ■機体リソース管理 機体予約ID，機体ID，予約日時範囲，オペレータID，更新者ID，登録日時，更新日時，削除フラグ

業務・データフロー

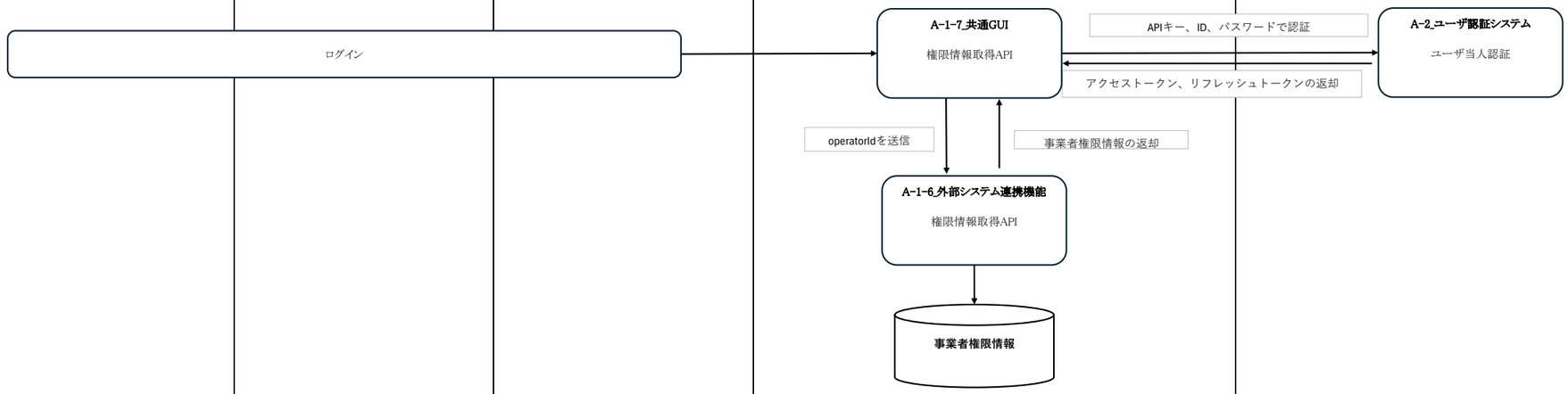
・対象業務	外部データ参照
・業務概要	データ提供事業者（SDSP）からのデータをシステムに取り込み、航路利用時の適合性評価、画面表示を行う

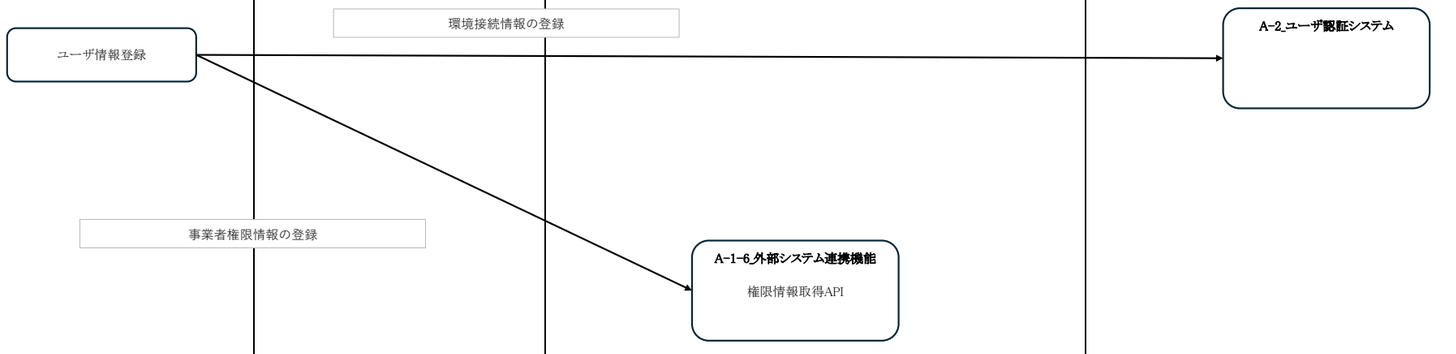
NO	業務タスク	運航事業者	ドローン航路運営者	関係者	ドローン航路システム	関連システム	取扱い情報
1	外部データ参照（リアルタイム）						＜動的データ＞ ①地図情報 ②風速・天候情報 ③気象情報 ④第三者立入監視情報 ⑤飛行禁止エリア情報 ＜静的データ＞ ⑥地形・障害物情報 ⑦電波情報 ⑧人流情報
2	外部データ参照（蓄積）						＜動的データ＞ ②風速・天候情報 ③気象情報 ④第三者立入監視情報 ⑤飛行禁止エリア情報 ＜静的データ＞ ⑥地形・障害物情報 ⑦電波情報 ⑧人流情報

業務・データフロー

・対象業務	ユーザ認証
・業務概要	ログイン:ドローン航路システムを利用するユーザの認証を行う。ユーザ認証システムの機能を利用する。ユーザはドローン航路システムの共通GUIよりユーザ認証システムへ認証を行い、取得したアクセストークンに含まれるoperatorIdを用いて、関連するユーザ属性を外部システム連携から取得する。 ユーザ情報登録:ドローン航路システムの利用可能なユーザの情報を登録する。システムを介さず、オフラインによる登録を行う。

NO	業務タスク	運航事業者	ドローン航路運営者	関係者	ドローン航路システム	関連システム	取扱い情報
1	ログイン						■環境接続情報 ・APIキー ユーザ認証システムから認証用に払いだされたAPIキー。共通GUI内部で保有している。 ・ID ユーザ認証システムへログインに利用するID。ユーザが画面上で入力する。 ・パスワード ユーザ認証システムへログインに利用するパスワード。ユーザが画面上で入力する ■ユーザ認証システムからの発行 ・アクセストークン ユーザ認証システムのAPI実行に利用する。 ・リフレッシュトークン アクセストークンのリフレッシュに利用する。 ・operatorId アクセストークンに埋め込まれており、デコードして取得する。 ■事業者権限情報 ・operatorId ・operatorName ・roleList 権限情報リスト(権限(1:航路運営事業者 2:運航事業者 3:関係者)
2	ユーザ情報登録						■ユーザ認証システム申請情報 ○利用システム(クライアント側) ・テーマ ・事業者名 ・システム/アプリ名 ・必要アカウント数 ・接続元IPアドレス ・認証フロー ・環境接続予定 ○連携システム(サーバ側) ・テーマ ・接続先システム ・接続先URL ・接続元IPアドレス ・環境接続予定 ■環境接続情報 ○接続先URL ・データ流通システム ・ユーザ認証システム ○ログイン情報(ユーザ主体認証利用時) ・APIキー ユーザ認証システムから認証用に払いだされたAPIキー ・ID ・パスワード ○ログイン情報(クライアントシステム認証利用時) ・クライアントID ・クライアントシークレット ・公開システム識別子 ■事業者権限情報 ・operatorId ・operatorName ・roleList 権限情報リスト(権限(1:航路運営事業者 2:運航事業者 3:関係者)





別紙②：情報資産整理表

情報資産整理表

業務・機能	取扱い情報 (データのメタデータ(登録日、更新日など)は、省略)		情報システム格付け		
			分類	格付レベル 統一基準に定める格付けを指針	格付け理由
航路画定					
	最大落下許容範囲情報	最大落下許容範囲ID 事業者番号 航路運営者ID 名称 エリア名 最大標高・地形 ジオメトリ 削除	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	2	情報が改ざんされた場合、誤った航路作成に繋がり、しいては不正な航路飛行を招く可能性があるため完全性は高い
			可用性	2	航路画定時、予約時以外にも適合性評価時に参照する情報のため、可用性は高い
	飛行経路/ドローン航路情報	航路画定ID 事業者番号 最大落下許容範囲ID 断面分割数 削除 航路ID 名称 親ノード航路ID 航路運営者ID 飛行目的 航路区画情報(ID/名称のみ) 落下範囲節情報(緯度経度:LineString) ジャンクション情報(緯度経度高度) 落下空間情報(緯度経度高度) ジャンクション/航路区画マッピング情報(ID/名称のみ)	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	2	情報が改ざんされた場合、誤った航路飛行により事故が発生する可能性があるため完全性は高い
			可用性	2	フライト中、逸脱判定などで航路情報を参照するため、可用性は高い
	航路対応機種情報	対応機種ID 機体情報ID 航路画定ID 製造メーカー名 型式(モデル) 機種名 機体種別 IP番号 機体長 重量 最大離陸重量 最大飛行時間	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	2	情報が改ざんされた場合、不正な適合性評価の結果となり、事故を招く可能性があるため完全性は高い
			可用性	1	航路画定時や予約時のみ参照する情報で、常に参照はしないため可用性は低い
	紐づけ情報(航路-離着陸場)	ドローンポート-航路区画マッピングID 航路区画ID ドローンポートID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	1	情報が改ざんされた場合、使用できるはずのドローンポートが使用できなくなってしまう可能性がある。
			可用性	1	航路画定時や航路予約時のみ参照する情報で、常に参照はしないため可用性は低い
	紐づけ情報(航路-事業者情報)	航路ID 事業者ID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	1	情報が改ざんされた場合、航路画定・予約時などに誤った宛先に周知されることになるが、重大な影響はない。かつ、修正可能
			可用性	1	航路画定時や航路予約時のみ参照する情報で、常に参照はしないため可用性は低い

情報資産整理表

業務・機能	取扱い情報 (データのメタデータ(登録日、更新日など)は、省略)		情報システム格付け		
			分類	格付レベル 統一基準に定める格付けを指針	格付け理由
航路予約					
	航路予約情報	運航事業者ID 航路予約ID 航路区画ID 航路区画毎の予約開始日時 航路区画毎の予約終了日時 航路予約ステータス 予約完了日時 予約状態更新日時	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	2	情報が改ざんされた場合、誤った航路飛行により事故が発生する可能性があるため完全性は高い
			可用性	1	予約時のみ参照する情報で、常に参照はしないため可用性は低い
	メール周知履歴	事業者ID 周知種別 周知先 周知方法 送信内容 送信結果 失敗理由 送信日時	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	1	情報が改ざんされた場合でも、メールの多重送信などは起こり得るが、システムへの被害は発生しない
			可用性	1	メール送信時のみ参照するデータで、常に参照はしないため可用性は低い
安全管理					
	航路予約情報	航路予約毎の識別ID 予約開始日時 予約終了日時 予約登録日時 航路区画ID配列 運航事業者ID 適合性評価結果 第三者立入監視情報 適合性評価結果 鉄道運航情報 適合性評価結果	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	2	情報が改ざんされた場合、誤った航路飛行により事故が発生する可能性があるため完全性は高い
			可用性	2	フライト中に、適合性評価を行う際にアクセスするため、可用性は高い
	運航情報	エリア情報のサブスクリプション ID 機体の登録 ID 機体の種別 テレメトリ情報取得日時 緯度 経度 対地高度 機体の進行方向 機体の速度 機体の垂直速度 航路逸脱割合 航路逸脱割合更新時刻 航路予約 ID 航路 ID 航路区画 ID 運航状況 運航者 ID 飛行時間	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	1	情報が改ざんされた場合、飛行後の記録情報の扱いのため事故が発生する可能性までは至らないため完全性は低い
			可用性	1	飛行後の記録情報の扱いのため、可用性は低い
	リモートID情報	航路予約毎の識別ID シリアルナンバー 登録ID セッションID フライト識別ID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	2	情報が改ざんされた場合、誤った機体と判定して運航管理できなくなる可能性があるため完全性は高い
			可用性	2	フライト中に常時参照を行うため、可用性は高い

情報資産整理表

業務・機能	取扱い情報 (データのメタデータ(登録日、更新日など)は、省略)		情報システム格付け		
			分類	格付レベル 統一基準に定める格付けを指針	格付け理由
離着陸場・機体管理					
	ドローンポート情報	ドローンポートID ドローンポート名 設置場所住所 製造メーカー 製造番号 離着陸場種類 VISドローンポート事業者ID 緯度 経度 着陸面対地高度 対応機体 画像 オペレータID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	2	情報が改ざんされた場合、誤った離着陸場に基づく飛行を招くことで事故が発生する可能性があるため完全性は高い
			可用性	1	予約時のみ参照する情報で、常に参照はしないため可用性は低い
	ドローンポート状態	ドローンポートID 動作状況(使用可) 動作状況(使用不可) 使用不可日時範囲 格納中機体ID オペレータID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	1	情報が改ざんされた場合、ドローンポートの利用可否を誤判定する可能性はあるが、予約時のみ利用する情報でオペレーション回避も可能
			可用性	1	予約時のみ参照する情報で、常に参照はしないため可用性は低い
	ドローンポート予約情報	ドローンポート予約ID ドローンポートID 使用機体ID 航路予約ID 利用形態 予約日時範囲 予約有効フラグ オペレータID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	2	情報が改ざんされた場合、誤った航路飛行により事故が発生する可能性があるため完全性は高い
			可用性	1	機械式のドローンポートを利用したフライトにおいては、フライト中常に参照するが、それ以外は予約時のみ参照するため、可用性は低い
	VISテレメトリ情報	ドローンポートID IPアドレス ドローンポート名 ドローンポートステータス VISステータス テレメトリ情報(緯度, 経度, 着陸面対地高度, 風向, 風速, 最大風速時風向, 最大風速, 雨量, 気温, 湿度, 気圧, 照度, 紫外線, 観測時間, 侵入検知有無, 検知物カテゴリ, 閾値(風速)) 拠点ID 拠点住所 拠点名称 拠点ステータス ドローンポート使用可否状態 エラーコード エラー内容	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	1	情報が改ざんされても、参照情報の位置づけのため、システムへの被害は発生しない
			可用性	1	VISを利用する場合のみ参照し、常に参照する必要が低いため、可用性は低い 情報にアクセスできなくても、カメラ等で状況確認は可能なため、可用性は低い
	機体情報	機体ID 機体名 製造メーカー 製造番号 機体の種類 最大離陸重量 重量 最大速度 最大飛行時間 位置情報(緯度) 位置情報(経度) 機体認証の有無 DIPS登録記号 機体所有種別 所有者ID 画像データ 画像フォーマット オペレータID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	2	情報が改ざんされた場合、誤った飛行情報により事故が発生する可能性があるため完全性は高い
			可用性	1	予約時のみ参照する情報で、常に参照はしないため可用性は低い
	機体リソース管理	機体予約ID 機体ID 予約日時範囲 オペレータID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	1	情報が改ざんされた場合、機体の利用可否を誤判定する可能性はあるが、予約時のみ利用する情報でオペレーション回避も可能
			可用性	1	予約時のみ参照する情報で、常に参照はしないため可用性は低い

情報資産整理表

業務・機能	取扱い情報 (データのメタデータ(登録日、更新日など)は、省略)		情報システム格付け		
			分類	格付レベル 統一基準に定める格付けを指針	格付け理由
外部データ参照	外部データ(リアルタイム)	地図情報 風速・天候情報 気象情報 第三者立入監視情報 飛行禁止エリア情報 ※外部システムからAPIで取得する情報	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	1	外部システムから随時参照するデータのため、ドローンシステムでは完全性は担保対象外
			可用性	2	利用できない場合、該当外部データを参照する業務すべてに影響が発生するため高い可用性が必要
	外部データ(蓄積)	＜動的データ＞ 風速・天候情報 気象情報 第三者立入監視情報 飛行禁止エリア情報 ＜静的データ＞ 地形・障害物情報 電波情報 人流情報 ※航路システムに蓄積する情報	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	2	情報が改ざんされた場合、ヒヤリハットなどの分析結果が不正となり、ビジネス的に不利益を被る可能性があるため、完全性は高い
			可用性	1	蓄積データは常に参照する必要が低いため可用性は低い
	DIPSトークン	事業者ID アクセストークン リフレッシュトークン IDトークン	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	1	情報が改ざんされてもDIPSにアクセスできないだけで、システムへの被害は発生しない
			可用性	1	常に参照する必要が低いため可用性は低い
ユーザ認証	事業者情報 ※ユーザ認証システム管理	事業者ID(UUID)　※事業者識別子(内部) 事業者番号　※事業者識別子(ローカル) 事業者アカウントID(メールアドレス) パスワード	機密性	2	・ログインID/パスワードは外部漏洩時にアカウント乗っ取りなどサイバー攻撃被害の可能性があるため機密性2とする。 ・事業者メールアドレスは限定的ではあるもののプライバシーを侵害する可能性があるため、機密性2とする。(今年度時点では、ユーザは法人に限定)
			完全性	2	情報が改ざんされた場合、ユーザがサービスを利用できなくなるため完全性は高い
			可用性	1	ログイン時のみ利用する情報で、常に参照する必要が低いため可用性は低い
	事業者情報(航路システム管理)	事業者ID 事業者名称 ユーザ区分 周知方法 周知先(メールアドレス、電話番号)	機密性	2	事業者メールアドレスは限定的ではあるもののプライバシーを侵害する可能性があるため、機密性2とする。(今年度時点では、ユーザは法人に限定)
			完全性	2	情報が改ざんされた場合、サービスを利用できない、または本来与えられた権限とは異なる情報にアクセスできる可能性があるため、完全性は高い
			可用性	1	ログイン時のみ利用する情報で、常に参照する必要が低いため可用性は低い
	アクセストークン	アクセストークン リフレッシュトークン	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い
			完全性	1	情報が改ざんされてもユーザがサービスを利用できないが、システムへの被害は発生しない
			可用性	2	利用できない場合、システムのサービスを呼び出しできないため、高い可用性が必要　※ただし、保存先はWebブラウザ

情報の格付け定義

種別	区分	分類基準（原文）	分類基準（要約）	ドローン航路システムにおける該当項目（例）	評価内容補足	財務会計システムにおける評価例（主に業務影響を評価）
機密性	3	国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドラインに定める**秘密文書**としての取扱いを要する情報 独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報	**取り扱う内容が秘密文書レベル（※1）となる情報** **※1：漏洩により国の安全や国益が侵害される内容**	なし	漏洩した際に、国の安全や国益が侵害される機密性の高い情報は取り扱わないため	なし
	2	国の行政機関における業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律 （平成11年法律第42号。以下「情報公開法」という。）第５条各号における**不開示情報**に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報 独立行政法人における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成13年法律第140号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報。また、指定法人のうち、独法等情報公開法の別表第一に掲げられる法人（以下「別表指定法人」という。）についても同様とする。 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報	**取り扱う内容が不開示情報レベル（※2）となる情報** **※2：以下参照** **・個人情報、特定個人情報** **・法人情報の内、漏洩すると利益侵害となりうる情報** **・公共の安全と秩序の維持に支障がでる情報** **・漏洩すると事業の遂行に支障がでる情報**	・事業者メールアドレス※限定的な影響（PIA資料参照） ・ログインID/パスワード（乗っ取り被害の可能性）	・事業者メールアドレスは限定的ではあるもののプライバシーを侵害する可能性があることが外部機関の調査によって確認されているため機密性2とする。 ・ログインID/パスワードは外部漏洩時にアカウント乗っ取りなどサイバー攻撃被害の可能性があるため機密性2とする。	・ユーザの個人情報（氏名、住所、口座番号、マイナンバー）：財務会計システムに保有されている個人情報は個人情報保護法により厳密な管理が定められている。漏洩した場合、個人に対する重大な犯罪被害をもたらす可能性が高い。また企業に対する致命的な社会的な信用毀損は避けられないため、高い機密性・完全性が求められる（評価によっては機密性3にもなりうる）。 ・仕訳データ（伝票番号、勘定科目、金額、税区分）：非公開情報となり漏洩時に事業被害、社会的な信用棄損の可能性がある。 ・売掛・買掛（取引先、請求書番号、支払期限）：非公開情報となり漏洩時に事業被害、社会的な信用棄損の可能性がある。 ・ログインID/パスワード：漏洩した場合、アカウントの乗っ取りや情報搾取など被害にある可能性がある
	1	国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 独立行政法人又は別表指定法人における業務で取り扱う情報のうち、独法等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報	**機密性2、3以外の情報**	・離着陸場・機体管理：②機体情報（機体ID, 機体名, 製造メーカー, 製造番号, 機体の種類etc…）	機体情報は個人情報等を含まない一般的な情報となるため機密性は低い	・サービスプレスリリース情報、サービスに関するお知らせ：公開情報のため機密性要件は低い ・投資家向け決算資料：すでに公開している情報の場合、機密性要件は低い（公開前の場合は評価値が上がる） ・市場取引データ（株価、為替）：ほとんどの市場データは公開情報であるため機密性は低い
完全性	2	業務で取り扱う情報（書面を除く。）のうち、改ざん、誤ひゅう又は破損により、国民の権利が侵害され又は業務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	**改ざんされると業務遂行に支障がでる情報**	・航路予約情報（飛行エリア, 航路、日時、離着陸場etc…）	情報が改ざんされた場合、誤った航路飛行により事故が発生する可能性があるため完全性は高い	・ユーザの個人情報（氏名、住所、口座番号、マイナンバー）：情報が改ざんされた場合、データの不整合や認識齟齬による多数の被害が想定される。 ・仕訳データ（伝票番号、勘定科目、金額、税区分）：改ざんされた場合、データ不整合により業務が停止する ・売掛・買掛（取引先、請求書番号、支払期限）：改ざんされた場合、データ不整合により業務が停止する ・決算書・財務報告データ：改ざんされた事実に気づかない場合、実際の売り上げと異なる不正会計として処罰対象になる可能性がある
	1	完全性２情報以外の情報（書面を除く。）	**完全性2以外の情報**	・安全管理：ヒヤリハット情報	ヒヤリハット情報は参考情報となり改ざん時にシステムへの被害は発生しない	・統計情報、経営状況分析などの分析データ：分析結果として出力されるデータのため、データの完全性が損なわれても業務継続への影響は少ない。
				・外部データ（地図情報,風速・天候情報,気象情報,第三者立入監視情報,飛行禁止エリア情報etc…）	外部システムから随時参照データとなる（想定）ためドローンシステムで完全性は担保対象外	
可用性	2	業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	**利用不可になると業務遂行に支障がでる情報**	・外部データ（地図情報,風速・天候情報,気象情報,第三者立入監視情報,飛行禁止エリア情報etc…）	利用できない場合、該当外部データを参照する業務すべてに影響が発生するため高い可用性が必要	・ユーザの個人情報（氏名、住所、口座番号、マイナンバー）：一時的に利用できなくなっても即業務停止にはつながらないものの、業務継続のためには一定以上の可用性が必要となる ・金融取引データ（入出金履歴、決済情報）：金融機関との取引はリアルタイムにデータ処理が行われるため高い可用性が必要。停止時の業務影響が大きい。
	1	可用性２情報以外の情報（書面を除く。）	**可用性1以外の情報**	・航路予約情報（飛行エリア, 航路、日時、離着陸場etc…）	フライト中は情報にアクセスしないため可用性要件は低い	・監査ログ：システムのセキュリティを担保する役割となるが、業務継続に必須となるデータではないため ・アプリケーション、サーバログ：システムの稼働状況を確認する役割となるが、業務継続に必須となるデータではないため
				・航路画定：航路対応機種情報	ドローンの航路対応機種情報は航路画定時に参照するが常に参照する必要が低いため可用性要件は低い	
				・履歴データ	履歴データは常に参照する必要が低いため可用性は低い	

別紙③：リスク・技術対策一覧

リスク・技術対策一覧

業務・機能	取扱い情報 (データのメタデータ(登録日、更新日など)は、省略)		情報システム格付け			リスク	技術対策(案)					
							情報システム構成要素 該当:● 非該当:空欄					対策案
			分類	格付けレベル 統一基準に定める格付けを指針	格付け理由		端末	サーバ	通信回線	ソフトウェア	アプリケーション・コンテンツ	
航路画定												
	最大落下許容範囲情報	最大落下許容範囲ID 事業者番号 航路運営者ID 名称 エリア名 最大標高・地形 ジオメトリ 削除	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	2	情報が改ざんされた場合、誤った航路作成に繋がり、いいては不正な航路飛行を招く可能性があるため完全性は高い	サイバー攻撃により情報が改ざんされると誤った航路作成となり不正な航路飛行や事故につながる。 例)クロスサイトスクリプティングによる情報の改ざん		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	2	航路画定時、予約時以外にも適合性評価時に参照する情報のため、可用性は高い	サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止		●	●			以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・適切な方法で情報のバックアップを実施すること。 ・インターネットからアクセスを受ける情報システムはサービス不能攻撃への対策を行うこと。 ・サービス不能攻撃の被害を最小化する手段を備えたシステムの構築 ・サービス不能攻撃を受けるシステム構成要素に対する監視。
	飛行経路/ドローン航路情報	航路画定ID 事業者番号 最大落下許容範囲ID 断面分割数 削除 航路ID 名称 親ノード航路ID 航路運営者ID 飛行目的 航路区画情報(ID/名称のみ) 落下範囲箇所情報(緯度経度:LineString) ジャンクション情報(緯度経度高度) 落下空間情報(緯度経度高度) ジャンクション/航路区画マッピング情報(ID/名称のみ)	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	2	情報が改ざんされた場合、誤った航路飛行により事故が発生する可能性があるため完全性は高い	サイバー攻撃により情報が改ざんされると誤った航路飛行により事故につながる。 例)標的型攻撃による情報の改ざん		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	2	フライト中、逸脱判定などで航路情報を参照するため、可用性は高い	サイバー攻撃により情報が改ざん・破壊されると航路を誤り事故につながる。 例)ランサムウェアによる情報の改ざん・破壊		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・適切な方法で情報のバックアップを実施すること。 ・インターネットからアクセスを受ける情報システムはサービス不能攻撃への対策を行うこと。 ・サービス不能攻撃の被害を最小化する手段を備えたシステムの構築 ・サービス不能攻撃を受けるシステム構成要素に対する監視。
	航路対応機種情報	対応機種ID 機体情報ID 航路画定ID 製造メーカー名 型式(モデル) 機種名 機体種別 IP番号 機体長 重量 最大搬送重量 最大飛行時間	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	2	情報が改ざんされた場合、不正な適合性評価の結果となり、事故を招く可能性があるため完全性は高い	サイバー攻撃により情報が改ざんされると不正な適合性評価結果となり事故につながる。 例)SQLインジェクションによる情報の改ざん		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	1	航路画定時や予約時のみ参照する情報で、常に参照はしないため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保ったための監視体制を整える。
	紐づけ情報(航路-離着陸場)	ドローンポート-航路区画マッピングID 航路区画ID ドローンポートID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	1	情報が改ざんされた場合、使用できるはずのドローンポートが使用できなくなってしまう可能性がある。	影響は限定的であるものの、サイバー攻撃により特権IDが奪われ情報が改ざん・破壊される。 例)標的型攻撃による特権IDの取得		●				影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること。
			可用性	1	航路画定時や航路予約時のみ参照する情報で、常に参照はしないため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保ったための監視体制を整える。
	紐づけ情報(航路-事業者情報)	航路ID 事業者ID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	1	情報が改ざんされた場合、航路画定・予約時などに誤った宛先に周知されることになるが、重大な影響はない。かつ、修正可能	影響は限定的であるものの、サイバー攻撃により特権IDが奪われ情報が改ざん・破壊される。 例)標的型攻撃による特権IDの取得		●				影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること。
			可用性	1	航路画定時や航路予約時のみ参照する情報で、常に参照はしないため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保ったための監視体制を整える。

リスク・技術対策一覧

業務・機能	取扱い情報 (データのメタデータ(登録日、更新日など)は、省略)		情報システム格付け			リスク	技術対策(案)					
							情報システム構成要素 該当:● 非該当:空欄					対策案
			分類	格付けレベル 統一基準に定める格付けを指針	格付け理由		端末	サーバ	通信回線	ソフトウェア	アプリケーション・コンテンツ	
航路予約												
	航路予約情報	運航事業者ID 航路予約ID 航路区画ID 航路区画毎の予約開始日時 航路区画毎の予約終了日時 航路予約ステータス 予約完了日時 予約状態更新日時	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	2	情報が改ざんされた場合、誤った航路飛行により事故が発生する可能性があるため完全性は高い	サイバー攻撃により情報が改ざんされると誤った航路飛行により事故につながる。 例)クロスサイトスクリプティングによる情報の改ざん		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	1	予約時のみ参照する情報で、常に参照はしないため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
	メール周知履歴	事業者ID 周知種別 周知先 周知方法 送信内容 送信結果 失敗理由 送信日時	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	1	情報が改ざんされた場合でも、メールの多重送信などは起こり得るが、システムへの被害は発生しない	影響は限定的であるものの、サイバー攻撃により特権IDが奪われ情報が改ざん・破壊される。 例)標的型攻撃による特権IDの取得		●				影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること。
			可用性	1	メール送信時のみ参照するデータで、常に参照はしないため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
安全管理												
	航路予約情報	航路予約毎の識別ID 予約開始日時 予約終了日時 予約登録日時 航路区画ID配列 運航事業者ID 適合性評価結果 第三者立入監視情報 適合性評価結果 鉄道運航情報 適合性評価結果	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	2	情報が改ざんされた場合、誤った航路飛行により事故が発生する可能性があるため完全性は高い	サイバー攻撃により情報が改ざんさられとれ誤った航路情報により事故につながる。 例)標的型攻撃による情報の改ざん		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	2	フライト中に、適合性評価を行う際にアクセスするため、可用性は高い	サイバー攻撃により情報が改ざん・破壊されるとシステムが利用できなくなり適合性評価に支障がでる。 例)ランサムウェアによる情報の改ざん・破壊		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・適切な方法で情報のバックアップを実施すること。 ・インターネットからアクセスを受ける情報システムはサービス不能攻撃への対策を行うこと。 ・サービス不能攻撃の被害を最小化する手段を備えたシステムの構築 ・サービス不能攻撃を受けるシステム構成要素に対する監視。
	運航情報	エリア情報のサブスクリプション ID 機体の登録 ID 機体の種別 テレメトリ情報取得日時 緯度 経度 対地高度 機体の進行方向 機体の速度 機体の垂直速度 航路逸脱割合 航路逸脱割合更新時刻 航路予約 ID 航路 ID 航路区画 ID 運航状況 運航者 ID 飛行時間	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	1	情報が改ざんされた場合、飛行後の記録情報の扱いのため事故が発生する可能性までは至らないため完全性は低い	影響は限定的であるものの、サイバー攻撃により特権IDが奪われ情報が改ざん・破壊される。 例)標的型攻撃による特権IDの取得		●				影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること。
			可用性	1	飛行後の記録情報の扱いのため、可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
	リモートID情報	航路予約毎の識別ID シリアルナンバー 登録ID セッションID フライト識別ID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	2	情報が改ざんされた場合、誤った機体と判定して運航管理できなくなる可能性があるため完全性は高い	サイバー攻撃により情報が改ざんされると機体判定を誤り運航管理ができなくなる。 例)SQLインジェクションによる情報の改ざん		●	●	●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	2	フライト中に常時参照を行うため、可用性は高い	サイバー攻撃により情報が改ざん・破壊されるとフライト中の参照が不可能となり飛行に支障がでる。 例)ランサムウェアによる情報の改ざん・破壊		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・適切な方法で情報のバックアップを実施すること。 ・インターネットからアクセスを受ける情報システムはサービス不能攻撃への対策を行うこと。 ・サービス不能攻撃の被害を最小化する手段を備えたシステムの構築 ・サービス不能攻撃を受けるシステム構成要素に対する監視。

リスク・技術対策一覧

業務・機能	取扱い情報 (データのメタデータ(登録日、更新日など)は、省略)		情報システム格付け			リスク	技術対策(案)					
							情報システム構成要素 該当:● 非該当:空欄					対策案
			分類	格付レベル 統一基準に定める格付けを指針	格付け理由		端末	サーバ	通信回線	ソフトウェア	アプリケーション・コンテンツ	
離着陸場・機体管理												
	ドローンポート情報	ドローンポートID ドローンポート名 設置場所住所 製造メーカー 製造番号 離着陸場種類 VISドローンポート事業者ID 緯度 経度 着陸面対地高度 対応機体 画像 オペレータID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	2	情報が改ざんされた場合、誤った離着陸場に基づく飛行を招くことで事故が発生する可能性があるため完全性は高い	サイバー攻撃により情報が改ざんされると誤った離着陸場に基づく飛行により事故につながる。 例)SQLインジェクションによる情報の改ざん		●	●	●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	1	予約時のみ参照する情報で、常に参照はしないため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
	ドローンポート状態	ドローンポートID 動作状況(使用可) 動作状況(使用不可) 使用不可日時範囲 格納中機体ID オペレータID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	1	情報が改ざんされた場合、ドローンポートの利用可否を誤判定する可能性はあるが、予約時のみ利用する情報でオペレーション回避も可能	影響は限定的であるものの、サイバー攻撃により特権IDが奪われ情報が改ざん・破壊される。 例)標的型攻撃による特権IDの取得		●				影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること。
			可用性	1	予約時のみ参照する情報で、常に参照はしないため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
	ドローンポート予約情報	ドローンポート予約ID ドローンポートID 使用機体ID 航路予約ID 利用形態 予約日時範囲 予約有効フラグ オペレータID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	2	情報が改ざんされた場合、誤った航路飛行により事故が発生する可能性があるため完全性は高い	サイバー攻撃により情報が改ざんされると誤った航路飛行により事故につながる。 例)SQLインジェクションによる情報の改ざん		●	●	●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	1	機械式のドローンポートを利用したフライトにおいては、フライト中常に参照するが、それ以外は予約時のみ参照するため、可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
	VISテレメトリ情報	ドローンポートID IPアドレス ドローンポート名 ドローンポートステータス VISステータス テレメトリ情報(緯度,経度,着陸面対地高度,風向,風速,最大風速時風向,最大風速,雨量,気温,湿度,気圧,照度,紫外線,観測時間,侵入検知有無,検知物カテゴリ,閾値(風速)) 拠点ID 拠点住所 拠点名称 拠点ステータス ドローンポート使用可否状態 エラーコード エラー内容	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	1	情報が改ざんされても、参照情報の位置づけのため、システムへの被害は発生しない	影響は限定的であるものの、サイバー攻撃により特権IDが奪われ情報が改ざん・破壊される。 例)標的型攻撃による特権IDの取得		●				影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること。
			可用性	1	VISを利用する場合のみ参照し、常に参照する必要が低いため、可用性は低い 情報にアクセスできなくても、カメラ等で状況確認は可能なため、可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
	機体情報	機体ID 機体名 製造メーカー 製造番号 機体の種類 最大離陸重量 重量 最大速度 最大飛行時間 位置情報(緯度) 位置情報(経度) 機体認証の有無 DIPS登録記号 機体所有種別 所有者ID 画像データ 画像フォーマット オペレータID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	2	情報が改ざんされた場合、誤った飛行情報により事故が発生する可能性があるため完全性は高い	サイバー攻撃により情報が改ざんされると誤った飛行情報により事故につながる。 例)SQLインジェクションによる情報の改ざん		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	1	予約時のみ参照する情報で、常に参照はしないため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
	機体リソース管理	機体予約ID 機体ID 予約日時範囲 オペレータID	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	1	情報が改ざんされた場合、機体の利用可否を誤判定する可能性はあるが、予約時のみ利用する情報でオペレーション回避も可能	影響は限定的であるものの、サイバー攻撃により特権IDが奪われ情報が改ざん・破壊される。 例)標的型攻撃による特権IDの取得		●				影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること。
			可用性	1	予約時のみ参照する情報で、常に参照はしないため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。

リスク・技術対策一覧

業務・機能	取扱い情報 (データのメタデータ(登録日、更新日など)は、省略)		情報システム格付け			リスク	技術対策(案)					
							情報システム構成要素 該当:● 非該当:空欄					対策案
			分類	格付けレベル 統一基準に定める格付けを指針	格付け理由		端末	サーバ	通信回線	ソフトウェア	アプリケーション・コンテンツ	
外部データ参照												
	外部データ(リアルタイム)	地図情報 風速・天候情報 気象情報 第三者立入監視情報 飛行禁止エリア情報 ※外部システムからAPIで取得する情報	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	1	外部システムから随時参照するデータのため、ドローンシステムでは完全性は担保対象外	影響は限定的であるものの、サイバー攻撃により特権IDが奪われ情報が改ざん・破壊される。 例)標的型攻撃による特権IDの取得		●				影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること。
			可用性	2	利用できない場合、該当外部データを参照する業務すべてに影響が発生するため高い可用性が必要	サイバー攻撃により当システムが利用不可となるとサービス提供や業務が妨害される。 例)Ddos攻撃によるシステムサービス停止		●	●	●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・適切な方法で情報のバックアップを実施すること。 ・インターネットからアクセスを受ける情報システムはサービス不能攻撃への対策を行うこと。 ・サービス不能攻撃の被害を最小化する手段を備えたシステムの構築 ・サービス不能攻撃を受けるシステム構成要素に対する監視。
	外部データ(蓄積)	＜動的データ＞ 風速・天候情報 気象情報 第三者立入監視情報 飛行禁止エリア情報 ＜静的データ＞ 地形・障害物情報 電波情報 人流情報 ※航路システムに蓄積する情報	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	2	情報が改ざんされた場合、ヒヤリハットなどの分析結果が不正となり、ビジネスの不利益を被る可能性があるため、完全性は高い	サイバー攻撃により分析情報が改ざん・破壊されるとビジネスとして不利益を被る。 例)ランサムウェアによる蓄積情報の改ざん・破壊		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	1	蓄積データは常に参照する必要が低いため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
	DIPSトークン	事業者ID アクセストークン リフレッシュトークン IDトークン	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	1	情報が改ざんされてもDIPSにアクセスできないだけで、システムへの被害は発生しない	影響は限定的であるものの、サイバー攻撃により特権IDが奪われ情報が改ざん・破壊される。 例)標的型攻撃による特権IDの取得		●				影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること。
			可用性	1	常に参照する必要が低いため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。

リスク・技術対策一覧

業務・機能	取扱い情報 (データのメタデータ(登録日、更新日など)は、省略)		情報システム格付け			リスク	技術対策(案)					
							情報システム構成要素 該当:● 非該当:空欄					対策案
			分類	格付けレベル 統一基準に定める格付けを指針	格付け理由		端末	サーバ	通信回線	ソフトウェア	アプリケーション・コンテンツ	
ユーザ認証												
	事業者情報 ※ユーザ認証システム管理	事業者ID(UUID) ※事業者識別子(内部) 事業者番号 ※事業者識別子(ローカル) 事業者アカウントID(メールアドレス) パスワード	機密性	2	・ログインID/パスワードは外部漏洩時にアカウント乗っ取りなどサイバー攻撃被害の可能性があるため機密性2とする。 ・事業者メールアドレスは限定的ではあるもののプライバシーを侵害する可能性があるため、機密性2とする。(今年度時点では、ユーザは法人に限定)	・サイバー攻撃によりアカウント情報が漏洩するとアカウント乗っ取りに利用される。 例)フィッシングやブルートフォース攻撃によるアカウント情報が奪取される ・サイバー攻撃によりメールアドレスが奪われるとアカウントの悪用や機密情報の漏洩につながる。 例)フィッシングによる情報の漏洩	●	●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・主体認証を行うシステムにおける主体認証情報の不正行為防止対策 ・取り扱う情報や取扱制限等に応じたアクセス権限の設定機能の導入 ・取り扱い情報の暗号化機能の必要性検討、および導入 ・各構成要素の脆弱性管理、対策計画および措置の実施
			完全性	2	情報が改ざんされた場合、ユーザがサービスを利用できなくなるため完全性は高い	サイバー攻撃によりアカウント情報が改ざん・破壊されるとユーザがサービスを利用できなくなる。 例)ランサムウェアによる情報の改ざん・破壊		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	1	ログイン時のみ利用する情報で、常に参照する必要が低いため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
	事業者情報(航路システム管理)	事業者ID 事業者名称 ユーザ区分 周知方法 周知先(メールアドレス、電話番号)	機密性	2	事業者メールアドレスは限定的ではあるもののプライバシーを侵害する可能性があるため、機密性2とする。(今年度時点では、ユーザは法人に限定)	サイバー攻撃によりメールアドレスが奪われるとアカウントの悪用や機密情報の漏洩につながる。 例)フィッシングによる情報の漏洩	●	●		●		以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・主体認証を行うシステムにおける主体認証情報の不正行為防止対策 ・取り扱う情報や取扱制限等に応じたアクセス権限の設定機能の導入 ・取り扱い情報の暗号化機能の必要性検討、および導入 ・各構成要素の脆弱性管理、対策計画および措置の実施
			完全性	2	情報が改ざんされた場合、サービスを利用できない、または本来与えられた権限とは異なる情報にアクセスできる可能性があるため、完全性は高い	サイバー攻撃により ユーザ情報が改ざんされるとサービスの利用不可や異なる権限の情報へのアクセスが可能となる。 例)ランサムウェアによるユーザ情報の改ざん・破壊		●		●		以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。
			可用性	1	ログイン時のみ利用する情報で、常に参照する必要が低いため可用性は低い	影響は限定的であるものの、サイバー攻撃によりシステムサービス提供を妨害される。 例)Ddos攻撃によるシステムサービス停止、通信遅延やシステムアクセスの一時的な不可		●	●			基本的なDDoS対策(例:トラフィック監視、過剰なトラフィックの自動遮断)を実施し、必要に応じて外部サービスを活用する。システムの可用性を保つための監視体制を整える。
	アクセストークン	アクセストークン リフレッシュトークン	機密性	1	個人情報等を含まない一般的な情報となるため機密性は低い	影響は限定的であるものの、サイバー攻撃により特権IDの悪用や、アプリケーションの脆弱性を突かれ情報が不正に参照、搾取される。 例)SQLインジェクションによる情報搾取	●	●	●	●	●	影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば端末の不正プログラム感染防止、サーバの冗長構成の確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策を実施すること。
			完全性	1	情報が改ざんされてもユーザがサービスを利用できないが、システムへの被害は発生しない	影響は限定的であるものの、サイバー攻撃により特権IDが奪われ情報が改ざん・破壊される。 例)標的型攻撃による特権IDの取得		●				影響が限定的でリスクが低いものの一般的なセキュリティ対策を実施すること。例えば定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること。
			可用性	2	利用できない場合、システムのサービスを呼び出しできないため、高い可用性が必要 ※ただし、保存先はWebブラウザ	サイバー攻撃により情報が改ざんされるとサービスが利用できなくなる。 例)クロスサイトスクリプティングよる情報の改ざん・破壊		●		●	●	以下対策案を実施すること。より詳細な対策案は「技術対策(案)_対策の具体例」シートを参照。 ・適切な方法で情報のバックアップを実施すること。 ・インターネットからアクセスを受ける情報システムはサービス不能攻撃への対策を行うこと。 ・サービス不能攻撃の被害を最小化する手段を備えたシステムの構築 ・サービス不能攻撃を受けるシステム構成要素に対する監視。

技術対策（案）_対策の具体例

種別	区分	情報の取り扱い定義	情報システム構成要素 該当：● 非該当：空欄 端末	サーバ	通信回線	ソフトウェア	アプリケーション・コンテンツ	対策案	対策の具体例（共通）	対策の具体例（端末）	対策の具体例（サーバ）	対策の具体例（通信回線）	対策の具体例（ソフトウェア）	対策の具体例（アプリケーション・コンテンツ）
機密性	3	要機密情報						機密性3に該当する取り扱い情報は無い	対象外	対象外	対象外	対象外	対象外	対象外
機密性	2	要機密情報	●	●		●	●	・主体認証を行うシステムにおける主体認証情報の不正行為防止対策 ・取り扱う情報や取扱制限等に応じたアクセス権限の設定機能の導入 ・取り扱い情報の暗号化機能の必要性検討、および導入 ・各構成要素の脆弱性管理、対策計画および措置の実施	・主体認証情報の漏えい等による不正なアクセスを防止するため、以下を全て含む措置を講ずること。 a)原則として、機器等において初期値として設定されている識別コードを使用しない。 b)不要な識別コードを無効にする。 ・主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること ・アクセス制御の要件を定めて対策すること。要件例は以下の通り。 a)利用時間や利用時間帯によるアクセス制御 b)同一主体による複数アクセスの制限 c)IPアドレスによる端末の制限 d)ネットワークセグメントの分割によるアクセス制御 e)ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御 f)認証・認可の統合管理基盤を用いたアクセス制御 g)アクセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御 ・アクセス制限の対象に対して暗号化等の措置を考慮すること ・以下のようなセキュリティリスクが高い機器等については原則、セキュリティパッチの適用又はソフトウェアのバージョンアップ等の措置を講ずる a)ネットワーク境界にある通信回線装置 b)認証サーバ c)要機密情報を保有するサーバ等	・物理的端末に情報を保存させないリモートアクセス環境の構築（シンクライアント、仮想デスクトップ、セキュアブラウザ等） ・ファイル暗号化等のセキュリティ機能を持つアプリケーションの導入 ・端末ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能の導入、または端末ファイルを暗号化する機能の導入 ・ハードディスク等の電磁的記録媒体に保存されている情報を遠隔命令等により暗号化消去する機能の導入 ・高度なセキュリティ機能を備えたOSを搭載するスマートフォンやタブレット端末等の導入 ・端末のUSBポート無効化、または物理的ロック（塞ぐ） ・機関等支給以外の端末利用の原則禁止 ・機関等支給以外の端末に対する要機密情報の保存の禁止	◆サーバ ・物理的なサーバ装置については、クラス2以上の要管理対策区域に設置し、盗難及び不正な持ち出しを防止する対策を講ずること。 ・データベースに格納されているデータに対する暗号化の実施（バックアップデータやトランザクションデータ等を含む） （ウェブサーバのみ）以下設定および管理対策を実施する。 ・ウェブ公開用ディレクトリ（ドキュメントルート）への不要ファイルの配置 ・初期状態で用意されるサンプルページやプログラム等の不要ファイル削除 ・サービスの提供に必要のない情報の保存を禁止する設定、または管理策 ・（メールサーバのみ）以下を全て含む送信ドメイン認証技術（SPF、DKIM、DRMARC等）による電子メールのなりすまし防止策 ・DMARCによる送信側の対策を行う。DMARCによる送信側の対策を行うためには、SPF、DKIMのいずれか又は両方による対策 ・DMARCによる受信側の対策を行う。DMARCによる受信側の対策を行うためには、SPF、DKIMの両方による対策 ・S/MIME等の電子メールにおける電子署名によなりすましの防止策の導入 （DNSサーバのみ）システム内部用DNSサーバは外部向けのコンテンツサーバと別々に設置し、ファイアウォール等でアクセス制御を行うこと。	対象外	情報格付区分2の要機密情報「対策の具体例（共通）」を参照	◆アプリケーション・コンテンツ 以下対策を実施する ・ウィルス対策ソフトによるスキャンで不正プログラムの検知 ・脆弱性診断によるプログラム内の脆弱性検出、確認 ・実行プログラム（.exe）形式でのコンテンツ提供の禁止 ・（アプリケーションプログラムの場合）コードサイニング証明書の導入、またはハッシュ値による整合性の確認 ・脆弱性が存在するバージョンのOS,ソフトウェアの禁止 ・システムを利用する利用者端末にセキュリティ低下を招くようなシステム仕様の禁止 ・トラッキング処理や利用者のキー入力を意図しない形で送信するなど、必要なくサービス利用者情報を同意なく第三者に提供する機能の禁止 ・システム外部へのアクセスを自動的に発生させるコンテンツ、または機能の禁止
機密性	1		●	●	●	●	●	機密性の格付け区分1に分類される取り扱い情報は、情報公開法第5条各号における「不開示情報に該当すると判断される蓋然性の高い情報」を含まない情報となり、影響が限定的でリスクが低いことから、明示的な対策の指針は示されていない。 但し、国の重要インフラ利用や所管省庁とのデータ連携などの観点から、一般的なセキュリティ対策については実施することが推奨される。 例えば端末の不正プログラム感染防止、サーバの冗長構成の検討および確保、利用するソフトウェアやアプリケーションに関連する公開された脆弱性についての対策の実施などが該当する。						
完全性	2	要保全情報		●	●	●	●	・改ざん防止のための措置を講ずること。 ・適切な方法で情報のバックアップを実施すること。 ・必要に応じて電子署名の付与及び検証を行う機能を設けること。	・電磁的記録媒体に対する電子署名、タイムスタンプの付与 ・要保全情報又は要安定情報に対する以下を例にした対策の実施 a)適切な方法でのバックアップ実施 例） ✓想定する危機的事象（地震、津波、火災、高出力電磁波、感染症、情報セキュリティインシデント等） ✓バックアップの対象（対象とするシステム、データ、ソフトウェアその他） ✓バックアップの範囲（フルバックアップ、差分バックアップ等） ✓バックアップを保存する電磁的記録媒体等の種類 ✓バックアップの周期、頻度、世代管理の方法 ✓使用するバックアップツール ✓バックアップデータの秘匿性確保、改ざん防止の方法 b)バックアップの周期は可能な限り短くすること c)バックアップデータに対する不正プログラム対策ソフトウェア等によるスキャン実施	対象外	・TLS機能の導入 ・正式な証明書発行機関により発行された電子証明書（サーバ証明書）の導入 ・暗号技術検討会及び関連委員会（CRYPTREC）の「TLS暗号設定ガイドライン」に準拠した設定の実施 以下を例とする電子メールの盗聴及び改ざんの防止策の導入（メールサーバのみ） ・SMTPによるサーバ間通信をTLSにより保護 ・S/MIME等の電子メールにおける暗号化及び電子署名の利用 ・DNSコンテンツサーバにおいて管理ドメインに関する情報が正確であることを定期的に確認すること。 レコードの例：Aレコード、AAAAレコード、MXレコード、TXTレコード、SPFレコード ・不必要なデータの操作を検知することを目的としたSIEM（Security Information and Event Management）やUEBA（User and Entity Behavior Analytics）等の導入。または上記製品と同等の対策実施。	・TLS、IPsec等による暗号化の実施※使用する暗号アルゴリズム及び鍵長は、「電子政府推奨暗号リスト」に準拠することが推奨	情報格付区分2の要保全情報「対策の具体例（共通）」を参照	以下対策を実施する ・ウィルス対策ソフトによるスキャンで不正プログラムの検知 ・脆弱性診断によるプログラム内の脆弱性検出、確認 ・実行プログラム（.exe）形式でのコンテンツ提供の禁止 ・（アプリケーションプログラムの場合）コードサイニング証明書の導入、またはハッシュ値による整合性の確認 ・脆弱性が存在するバージョンのOS,ソフトウェアの禁止 ・システムを利用する利用者端末にセキュリティ低下を招くようなシステム仕様の禁止 ・トラッキング処理や利用者のキー入力を意図しない形で送信するなど、必要なくサービス利用者情報を同意なく第三者に提供する機能の禁止 ・システム外部へのアクセスを自動的に発生させるコンテンツ、または機能の禁止
完全性	1			●				完全性の格付け区分1に分類される取り扱い情報は、要保全情報に該当する取り扱い情報と比較して改ざん、誤びゅう又は破損により、国民の権利が侵害され又は業務の適切な遂行に支障が出るものではなく、影響が限定的でリスクが低いものであることから、明示的な指針は示されていない。 但し、国の重要インフラ利用や所管省庁とのデータ連携などの観点から、一般的なセキュリティ対策を実施することが推奨される。 例えば盗聴及び改ざんの防止策としてTLS機能の導入や、定期的なバックアップを実施し、バックアップデータからの復旧体制を整備すること等が該当する。						
可用性	2	要安定情報		●	●	●	●	・適切な方法で情報のバックアップを実施すること。 ・インターネットからアクセスを受ける情報システムはサービス不能攻撃への対策を行うこと。 ・サービス不能攻撃の被害を最小化する手段を備えたシステムの構築 ・サービス不能攻撃を受けるシステム構成要素に対する監視。	・要保全情報又は要安定情報に対する以下を例にした対策の実施 a)適切な方法でのバックアップ実施（情報格付区分2の要保全情報「対策の具体例（共通）」参照） b)バックアップの周期は可能な限り短くすること c)バックアップデータに対する不正プログラム対策ソフトウェア等によるスキャン実施 ・サーバ装置、端末及び通信回線装置について、サービス不能攻撃に対抗するための以下の機能の有効化 a)パケットフィルタリング機能 b)3-way handshake時のタイムアウトの短縮 c)各種Flood攻撃への防御 d)アプリケーションゲートウェイ機能 ・以下を例とするサービス不能攻撃への対策の実施 a)サービス不能攻撃の影響を排除又は低減するための専用の対策装置やサービスの導入 b)サーバ装置、端末及び通信回線装置及び通信回線の冗長化 c)インターネットに接続している通信回線の提供元となる事業者やクラウドサービス提供者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策 d)コンテンツデリバリーネットワーク（CDN）サービスの利用 ・サービス不能攻撃を受けた場合の影響を最小とする手段を備えること 例：外部ネットワークからの遮断、通信回線の通信量制限、冗長構成等 ・サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること	対象外	・必要なサーバ装置を冗長構成にするなどにより可用性を確保する。 ・許容停止時間等を踏まえた、適切な方法でのバックアップを取得する ・バックアップの保存場所に関しては論理的に切り離されたネットワークに保存することや、バックアップを取得する媒体を物理的な媒体に保存することを検討する ・運用時に定めているバックアップ要件の適時見直し ・サーバ構成やソフトウェア等の設定変更が行われた際、及びにサーバ復旧手順の定期的な見直し	・通信回線の性能低下や異常の有無を確認することを目的とした、通信回線利用率、接続率等の運用状態を定常的に確認、分析する機能の導入 ・通信回線及び通信回線装置を冗長構成にする。 ・端末等が情報システムと通信可能な代替手段の整備。 ・運用状態を復元するために必要な設定情報等のバックアップの取得および保管。	情報格付区分2の要安定情報「対策の具体例（共通）」を参照	情報格付区分2の要安定情報「対策の具体例（共通）」を参照
可用性	1			●	●			可用性の格付け区分1に分類される取り扱い情報は、要安定情報に該当する取り扱い情報と比較して、滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障が出るものではなく、影響が限定的でリスクが低いものであることから、明示的な指針は示されていない。 但し、国の重要インフラ利用や所管省庁とのデータ連携などの観点から、一般的なセキュリティ対策を実施することが推奨される。 例えば基本的なDDoS対策（例：トラフィック監視、過剰なトラフィックの自動遮断）を実施し、必要に応じて外部サービスを活用することや、システムの可用性を保つための監視体制を整えることなどが該当する。						

【参考】構成要素と要保護情報の対策

No	構成要素	分類	大項番	中項番	遵守事項（統一基準 第6部より）	基本的対策事項（ガイドラインより）	対策事項の解説（ガイドラインより）	具体的な対策案
1	端末	要保護情報	6.1.1 端末	(1) 端末の導入時の対策	(1) 端末の導入時の対策 (a)情報システムセキュリティ責任者は、**要保護情報**を取り扱う物理的な端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。 6.1.1(1)-2 情報システムセキュリティ責任者は、物理的な端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。 モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定する。 モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意する。 6.1.1(1)-3 情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を全て含む対策を講ずること。 一定時間操作が無いと自動的にスクリーンロックするよう設定する。 不特定多数の人が出入りする場所で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける。	<6.1.1(1)(a)関連> 6.1.1(1)-1 情報システムセキュリティ責任者は、モバイル端末を除く物理的な端末について、原則として**クラス２**（職員等以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域）以上の要管理対策区域に設置すること。 6.1.1(1)-2 情報システムセキュリティ責任者は、物理的な端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。 モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定する。 モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意する。 6.1.1(1)-3 情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を全て含む対策を講ずること。 一定時間操作が無いと自動的にスクリーンロックするよう設定する。 不特定多数の人が出入りする場所で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける。	● 基本対策事項 **6.1.1(1)-1**「原則としてクラス２以上の要管理対策区域に設置する」について 要保護情報を取り扱う端末はクラス２以上の区域に設置することが望ましい。クラス２より低位の区域に設置する必要がある場合は、利用者が常時監視できる場所への設置を義務付けるなど、クラス２の区域に設置する場合と同程度の安全性を確保するための代替策を講ずること。 ● 基本対策事項 **6.1.1(1)-2**「物理的な端末の盗難及び不正な持ち出しを防止」について モバイル端末を除く物理的な端末については、設置する場所によっては、ハードディスク等の電磁的記録媒体の盗難についても注意する必要がある。そのような端末においては筐体を施錠する等の対策も検討するとよい。また、モバイル端末については紛失した際のリスクを軽減するため、ハードディスク等の電磁的記録媒体を暗号化するなどの措置を講ずる等の対策も検討するとよい。 ● 基本対策事項 **6.1.1(1)-3**「第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を全て含む対策を講ずる」について 第三者による不正操作等の防止のための対策事項であるが、その他、端末の操作のロックの解除に **IC** カード等の主体認証情報格納装置を使用し、主体認証情報格納装置が無い状態で又は操作の無い状態が一定時間続くことで端末の操作がロックされるようにし、かつ、当該主体認証情報格納装置を執務室からの退出の確認にも利用するという方法が考えられる（これにより、利用者が執務室外にいる際には端末の操作が確実にロックできる）。 また、正規の利用者による不正操作や誤操作の防止として、端末が備える機能のうち、利用しない機能を停止することが考えられる。停止する機能の例としては、無線**LAN** 等の通信用のインタフェース、**USB** ポート等の外部電磁的記録媒体を接続するためのインタフェース、機能として不要な場合は、マイク、ウェブカメラ等が考えられる。	・物理的な端末を設置する場合、クラス2以上の管理区域に設置すること ・クラス2より低位の区域に設置する必要がある場合、クラス2の区域に設置する場合と同程度の安全性を確保するための代替策を講ずる ・物理的に設置した端末はセキュリティワイヤ等を用いて搬出が困難となるように固定する ・モバイル端末を補完するための設備（施錠可能な袖机やキャビネット等）を設置する ・一定時間端末操作が無い場合は自動的にスクリーンロックが実行される設定を講ずる ・不特定多数の人が出入りする場合覗き見防止フィルターを取り付ける ・無線LAN、USBポート、マイク、ウェブカメラ等の利用しない機能は無効化する
2		要保護情報	6.1.2 要管理対策区域外での端末利用時の対策	(1) 機関等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用に係る運用規程の整備	(a) 統括情報セキュリティ責任者は、職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）を用いて**要保護情報**を取り扱う場合について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を実施手順として定めること。	<6.1.2(1)(a)関連> 6.1.2(1)-1 統括情報セキュリティ責任者は、職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合の利用手順を実施手順として、以下を例として定めること。 a)端末での利用する電磁的記録媒体に保存されている要機密情報の暗号化 b)盗み見に対する対策（のぞき見防止フィルタの利用等） c)置離・紛失に対する対策（不要な情報を端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど） d)利用する場所や時間の限定 e)端末の盗難・紛失が発生した際の緊急対応手順 6.1.2(1)-2 統括情報セキュリティ責任者は、職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合について、以下を全て含む許可手続を実施手順として定めること。 a)利用時の許可申請手続 b)接続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線への接続形態等） c)利用期間満了時の手続 d)可権限者（課室情報セキュリティ責任者）による手続内容の記録	●b基本対策事項**6.1.2(1)-1 c)**「盗難・紛失に対する対策」について 一般的に、以下に例を挙げる状況では、盗難・紛失が発生しやすいため、要機密情報を含むモバイル端末を携行する場合には十分注意させること。特に以下の例では、飲酒を伴う際に発生するケースが多いことから、飲酒が想定される場合は、モバイル端末は携行しないことが重要である。 a)電車での移動中に、モバイル端末の入ったかばん等を網棚に置き、そのまま下車する。 b)酒が想定されるいわゆる宴会等でモバイル端末の入ったかばん等を置いたまま帰宅する。 ●b基本対策事項**6.1.2(1)-2 c)**「利用期間満了時の手続」について 利用期間満了時は、職員等に報告を求めるよう手続に定める必要がある。特に機密性３情報等の取扱いに注意すべき情報を要管理対策区域外に持ち出す場合においては、以下を例とする管理手順を設けるとよい。 a)利用期間満了時の連絡が無い場合は、当該利用者に確認する。 a)利用期間の延長が必要であれば、再手続を要請する。 a)利用期間満了前に利用が終了した際には、利用終了時に報告を求める。	・要保護情報を取り扱う端末に対する以下の対策 a)端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化 b)盗み見に対する対策（のぞき見防止フィルタの利用等） c)置離・紛失に対する対策（不要な情報を端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど） d)利用する場所や時間の限定 e)端末の盗難・紛失が発生した際の緊急対応手順の整備 ・要保護情報を取り扱う物理的な端末を要管理対策区域外で使用する場合に限り、以下実施手順を整備する a)利用時の許可申請手続 b)接続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線への接続形態等） c)利用期間満了時の手続 d)可権限者（課室情報セキュリティ責任者）による手続内容の記録
3		要保護情報	6.1.3端末等支給以外の端末の導入及び利用時の対策	(2)端末等支給以外の端末の利用に関する運用規程等の整備	(b)統括情報セキュリティ責任者は、職員等が機関等支給以外の端末を用いて**要保護情報**を取り扱う場合について、盗難、紛失、不正プログラムの感染等により情報窃取されるなどのリスクを踏まえた利用手順及び許可手続を実施手順として定めること。	なし	なし	・盗難、紛失、不正プログラムの感染等により情報窃取されるなどのリスクを踏まえた利用手順及び許可手続の整備
4		要保護情報	6.1.3端末等支給以外の端末の導入及び利用時の対策	(4)端末等支給以外の端末の利用時の対策	(b)端末等は、機関等支給以外の端末を用いて**要保護情報**を取り扱う場合は、(2)(b)で定める利用手順に従うこと。	なし	●b遵守事項**6.1.3(4)(b)**「利用手順に従う」について 職員等は、機関等支給以外の端末の利用に係る機関等全体のポリシーをよく理解し、安全管理措置を徹底し、また、利用手順に従い、情報セキュリティインシデントの回避に努めなければならない。特にスマートフォン等の利用については、その特性に応じたリスクを利用者である職員等自身もよく理解した上で利用することが求められる。	・機関等支給以外の端末を用いて要保護情報を取り扱う際の手順整備および遵守
5		要保護情報	6.1.3端末等支給以外の端末の導入及び利用時の対策	(4)端末等支給以外の端末の利用時の対策	(d)端末等は、情報処理の目的を完了した場合は、**要保護情報**を機関等支給以外の端末から消去すること。	なし	●b遵守事項**6.1.3(4)(d)**「要保護情報を機関等支給以外の端末から消去する」について 要保護情報を消去することは必須であるが、不必要な情報及び業務用のアプリケーション等についても併せて消去しておくことが望ましい。	機関等支給以外の端末について情報処理の目的を完了した場合は、**要保護情報**を消去すること。
6		要機密情報	6.1.2 要管理対策区域外での端末利用時の対策	(1) 機関等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用に係る運用規程の整備	(b) 統括情報セキュリティ責任者は、**要機密情報**を取り扱う機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置に関する運用規程を整備すること。	<6.1.2(1)(b)関連> 6.1.2(1)-3 統括情報セキュリティ責任者は、要機密情報を取り扱う機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）について、以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能を検討し、要管理対策区域外で使用する物理的な端末に求める技術的な措置に関する運用規程を設けること。 a)仮想クライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。 b)安全なブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。 c)ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入する。 d)端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける。 e)記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設ける。 f)ードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設ける。 g)度なセキュリティ機能を備えたOSを搭載するスマートフォンやタブレット端末等を使用する。	<6.1.2(1)(b)関連> 6.1.2(1)-3 統括情報セキュリティ責任者は、要機密情報を取り扱う機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）について、以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能を検討し、要管理対策区域外で使用する物理的な端末に求める技術的な措置に関する運用規程を設けること。 a)仮想クライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。 b)安全なブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。 c)ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入する。 d)端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける。 e)記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設ける。 f)ードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設ける。 g)度なセキュリティ機能を備えたOSを搭載するスマートフォンやタブレット端末等を使用する。	●b遵守事項**6.1.2(1)(b)**「要機密情報を取り扱う機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）」について 要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）とは、モバイル端末が該当する。 以下は原文参照 ●b基本対策事項**6.1.2(1)-3**「暗号化」について ●b基本対策事項**6.1.2(1)-3 a)**「シンクライアント等」について ●b基本対策事項**6.1.2(1)-3 b)**「セキュアブラウザ等」について ●b基本対策事項**6.1.2(1)-3 e)**「ファイルを暗号化する機能を設ける」について ●b基本対策事項**6.1.2(1)-3 f)**「遠隔からの命令等により暗号化消去する機能」について ●b基本対策事項**6.1.2(1)-3 g)**「高度なセキュリティ機能を備えたOSを搭載するスマートフォンやタブレット端末等」について	・物理的な端末に対して以下の対策を講じる a)仮想クライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境の構築 b)安全なブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境の構築 c)ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入 d)端末にハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能の導入 e)記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能の導入 f)ードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能の導入 g)度なセキュリティ機能を備えたOSを搭載するスマートフォンやタブレット端末等の使用
7		要機密情報	6.1.2 要管理対策区域外での端末利用時の対策	(2)端末等が支給する端末（要管理対策区域外で使用する場合に限る）の導入及び利用時の対策	(a)情報システムセキュリティ責任者は、職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）を用いて**要機密情報**を取り扱う場合は、当該端末について前条(b)の技術的な措置を講ずること。	<6.1.2(2)(a)(b)関連> 6.1.2(2)-1 情報セキュリティリスクが相対的に高いと考えられる地域においては、第三者による物理的なアクセスのリスクへの対策を実施する。	●b遵守事項**6.1.2(2)(a)**「前条(b)の技術的な措置を講ずる」について 職員等が機関等が支給する物理的な端末（要管理対策区域外で使用する場合に限る）を用いて要機密情報を取り扱う場合は、遵守事項**6.1.2(1)(b)**において定めた運用規程に基づき、当該端末に対して技術的な措置を講ずることが求められる。 ●b基本対策事項**6.1.2(2)-1**「第三者による物理的なアクセスのリスクへの対策」について 情報セキュリティリスクが相対的に高いと考えられる地域等においては、第三者による物理的なアクセスのリスクを十分に考慮する必要がある。このような地域等においては、例えば、使用する端末のUSBポート等を物理的にロック（塞ぐ）して封印、システム設定で端末のUSBポート等を無効にするといった対策を施した専用のモバイル端末で業務を行うとともに、端末は常時携行し、このような地域等から戻った際には、端末を工場出荷時の状態に戻すことが望ましい。	・端末のUSBポートを物理的にロック（塞ぐ）して封印する ・システム設定でUSBポートを無効にする ・他、同上
8		要機密情報	6.1.3端末等支給以外の端末の導入及び利用時の対策	(1)端末等支給以外の端末の利用可否の判断	(a)要求情報セキュリティ責任者は、機関等支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、機関等が講じる安全管理措置、当該端末の管理は機関等ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、機関等における機関等支給以外の端末の利用の可否を判断すること。	なし	●b遵守事項**6.1.3(1)(a)**「求められる情報セキュリティの水準の達成の見込み」について 機関等支給以外の端末の導入に当たっては、以下のようなリスクが想定される。 a)不正プログラムに感染し、**要機密情報**が外部に漏えいする。 a)接続先の情報システムが、機関等支給以外の端末を通じて不正プログラムに感染し、業務の継続が困難になる等の影響が生じる。 a)端末の盗難・紛失等により、**要機密情報**が外部に漏えいする。 a)利用者の知識不足により、利用者の意図に反して要機密情報が国外のサーバ装置等に保存され、第三者に閲覧される。 a)家族や知人の端末操作により端末内の**要機密情報が外部に漏えい**する。	・機関等支給以外の端末の利用を原則許可しない ・機関等支給以外の端末に対して要機密情報の保存を許可しない

【参考】構成要素と要保護情報の対策

No	構成要素	分類	大項番	中項番	遵守事項（統一基準 第6部より）	基本的対策事項（ガイドラインより）	対策事項の解説（ガイドラインより）	具体的な対策案
9		要機密情報	6.1.3(2)関等支給以外の端末の導入及び利用時の対策	(2)(2)関等支給以外の端末の利用に関する運用規程等の整備	(c)(2)括情報セキュリティ責任者は、**要機密情報**を取り扱う機関等支給以外の端末について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置を含めた安全管理措置に関する運用規程を整備すること。	<6.1.3(2)(c)関連> 6.1.3(2)-6(2)括情報セキュリティ責任者は、**要機密情報**を取り扱う機関等支給以外の端末について、以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための対策の検討のほか、端末で機密性３情報を取り扱うことができない対策についても検討し、要機密情報を取り扱う機関等支給以外の端末に求める安全管理措置に関する運用規程のうちの技術的な措置として加えること。 なお、可能な限り端末に情報を保存させない機能を設けることも運用規程に含めること。 a)(2)シクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。 b)(2)キュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。 c)(2)ァイル暗号化等のセキュリティ機能を持つアプリケーションを導入する。 d)(2)端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける。 e)(2)記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設ける。 f)(2)ードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設ける。 g)(2)度なセキュリティ機能を備えたOSを搭載するスマートフォンやタブレット端末等を使用する。	●遵守事項**6.1.3(2)(c)**「要機密情報を取り扱う機関等支給以外の端末」について 要機密情報を取り扱う機関等支給以外の端末とは、機関等支給以外のモバイル端末と職員等の自宅で業務を行う際に用いる機関等支給以外の据え置き型端末が該当する。 以下は原文参照 ●**基**本対策事項**6.1.3(2)-6**「暗号化」について ●**基**本対策事項**6.1.3(2)-6 a)**「シンクライアント等」について ●**基**本対策事項**6.1.3(2)-6 b)**「セキュアブラウザ等」について ●**基**本対策事項**6.1.3(2)-6 c)**「ファイル暗号化等のセキュリティ機能を持つアプリケーション」について ●**基**本対策事項**6.1.3(2)-6 d)**「ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能」について ●**基**本対策事項**6.1.3(2)-6 e)**「ファイルを暗号化する機能を設ける」について ●**基**本対策事項**6.1.3(2)-6 f)**「遠隔からの命令等により暗号化消去する機能」について ●**基**本対策事項**6.1.3(2)-6 g)**「高度なセキュリティ機能を備えたOSを搭載するスマートフォンやタブレット端末等」について	・機関等支給以外の端末を利用する場合は以下の対策を講じること a)(2)ンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境の構築 b)(2)キュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境の構築 c)(2)ァイル暗号化等のセキュリティ機能を持つアプリケーションの導入 d)(2)端末にハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能 e)(2)記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能 f)(2)ードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能 g)(2)度なセキュリティ機能を備えたOSを搭載するスマートフォンやタブレット端末等の使用
10		要機密情報	6.1.3(4)関等支給以外の端末の導入及び利用時の対策	(4)(4)関等支給以外の端末の利用時の対策	(c)(4)末管理責任者等は、**要機密情報**を取り扱う機関等支給以外の端末について、(2)(c)に定める安全管理措置を講じる又は職員等に講じさせること。	なし	●遵守事項**6.1.3(4)(c)**「端末管理責任者等」について 遵守事項**6.1.3(2)(c)**に定める安全管理措置のうち、機関等支給以外の端末から機関等**LAN**等の情報システムにアクセスさせる場合、当該情報システムの情報システムセキュリティ責任者が、機関等支給以外の端末に対する安全管理措置と併せて、当該情報システム側で対応すべき措置を実施することも考えられる。 例えば、基本対策事項**6.1.3(2)-6 a)**の規定を参考とし、シンクライントを用いた機関等**LAN**システムへのリモートアクセス環境を構築する場合は、端末に専用のシンクライアントアプリケーションをインストールすることに加え、サーバ装置に仮想マシンを構築することが考えられる。この場合は、機関等支給以外の端末から利用される機関等**LAN**に知見を有している、機関等**LAN**を管理する情報システムセキュリティ責任者が機関等支給以外の端末に対して本項を行うことが適切とも考えられる。 ●遵守事項**6.1.3(4)(c)**「職員等に講じさせる」について 基本対策事項**6.1.3(2)-6**の安全管理措置のうち、職員等が講ずることが適当な項目としては、例えばOSの機能を利用する**6.1.3(2)-6 d)**の「ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能」や**6.1.3(2)-6 e)**の「ファイルを暗号化する機能」が考えられる。	同上
11		要保全情報	なし	なし	なし	なし	なし	なし
12		要安定情報	なし	なし	なし	なし	なし	なし
13	サーバ装置	要保護情報	6.2.1(5)ーバ装置	(1)(5)ーバ装置の導入時の対策	(a)(5)報システムセキュリティ責任者は、**要保護情報**を取り扱う物理的なサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。	<6.2.1(1)(a)関連> 6.2.1(1)-1(5)報システムセキュリティ責任者は、要保護情報を取り扱う物理的なサーバ装置については、クラス２以上の要管理対策区域に設置すること。 6.2.1(1)-2(5)報システムセキュリティ責任者は、物理的なサーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。 a)(5)錠可能なサーバラックに設置して施錠する。 b)(5)易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。 6.2.1(1)-3(5)報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。 a)(5)定時間操作が無いと自動的にスクリーンロックするよう設定する。	●**基**本対策事項**6.2.1(1)-1**「クラス２以上の要管理対策区域に設置する」について サーバ装置に関しては、取り扱う情報の重要性に応じて原則としてクラス３の区域に設置すること。また、クラス２の区域（執務室等）に設置する場合においては、原則として常時施錠されたサーバラックに置くことが重要である。	・要保護情報を取り扱う物理的なサーバ装置については、クラス２以上の要管理対策区域に設置すること。 ・情報システムセキュリティ責任者は、物理的なサーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。 a)(5)錠可能なサーバラックに設置して施錠する。 b)(5)易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。 ・情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、一定時間操作が無いと自動的にスクリーンロックするよう設定する等の対策を実施すること。
14		要機密情報	なし	なし	なし	なし	なし	なし
15		要保全情報	なし	なし	なし	なし	なし	なし
16		要安定情報	6.2.1(5)ーバ装置	(1)(5)ーバ装置の導入時の対策	(b)(5)報システムセキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、**要安定情報**を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。	<6.2.1(1)(b)関連> 6.2.1(1)-4(5)報システムセキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため要安定情報を取り扱う情報システムについては、将来の見通しも考慮し、以下を例とする対策を講ずること。 a)(5)荷分散装置、DNSラウンドロビン方式等による負荷分散 b)(5)ーシステムを２系統で構成することによる冗長化	●**基**本対策事項**6.2.1(1)-4 b)**「冗長化」について 「冗長化」とは、障害や過度のアクセスが発生した場合を想定し、サービスを提供するサーバ装置を代替サーバ装置に切り替えることで、サービスが中断しないように、情報システムを構成することである。可用性を高めるためには、サーバ装置本体だけでなく、ハードディスク等のコンポーネント単位で冗長化することも考えられる。 なお、災害等を想定して冗長化する場合には、代替のサーバ装置を遠隔地に設置することが望ましい。	・要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。 例） a)(5)荷分散装置、DNSラウンドロビン方式等による負荷分散 b)(5)ーシステムを２系統で構成することによる冗長化
17		要安定情報	6.2.1(5)ーバ装置	(1)(5)ーバ装置の導入時の対策	(g)(5)報システムセキュリティ責任者は、**要安定情報**を取り扱うサーバ装置について、適切な方法でサーバ装置のバックアップを取得すること。	なし	●遵守事項**6.2.1(1)(g)**「適切な方法でサーバ装置のバックアップを取得する」について 要安定情報を取り扱うサーバ装置については、情報システムにおいて許容される停止時間等を踏まえて、適切な方法でバックアップを取得する必要がある。そのバックアップの方法については、OSやアプリケーションなどを含むサーバ装置全体をバックアップする方法やサーバ装置の複製をバックアップとして用意しておく方法などが存在する。 また、バックアップを取得する際は、バックアップの世代管理、保存場所や媒体についても考慮する必要がある。 バックアップの取得については、「（解説）基本対策事項**5.2.3(1)-7 a)**「適切なバックアップの取得及びバックアップ要件の確認による見直し」について」を参照のこと。	・システムにおいて許容される停止時間等を踏まえて、適切な方法でバックアップを取得すること ・不正アクセス等による攻撃に備えて、バックアップの保存場所に関しては論理的に切り離されたネットワークに保存することや、バックアップを取得する媒体を物理的な媒体に保存することを検討すること
18		要安定情報	6.2.1(5)ーバ装置	(2)(5)ーバ装置の運用時の対策	(d)(5)報システムセキュリティ責任者は、**要安定情報**を取り扱うサーバ装置について、危機的事象発生時に適切な対処が行えるよう運用をすること。	<6.2.1(2)(d)関連> 6.2.1(2)-3(5)報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置について、以下を全て含む運用をすること。 a)(5)ーバ装置全体の適切なバックアップの取得及びバックアップ要件の確認による見直し b)(5)ーバ装置の構成やソフトウェア等の設定の変更が行われた際及び定期的に、サーバ装置が停止した際の復旧手順の確認による見直し	●**基**本対策事項**6.2.1(2)-3 a)**「適切なバックアップの取得及びバックアップ要件の確認による見直し」について 「（解説）基本対策事項**5.2.3(1)-7 a)**「適切なバックアップの取得及びバックアップ要件の確認による見直し」について」を参照のこと。 ●**基**本対策事項**6.2.1(2)-3 b)**「サーバ装置が停止した際の復旧手順の確認による見直し」について 「（解説）基本対策事項**5.2.3(1)-7 b)**「情報システムが停止した際の復旧手順の確認による見直し」について」を参照のこと。	・サーバ装置について、以下を全て含む運用をすること。 a)(5)ーバ装置全体の適切なバックアップの取得、および運用時に定めているバックアップ要件の適時見直し b)(5)ーバ装置の構成やソフトウェア等の設定の変更が行われた際及び定期的に、サーバ装置が停止した際の復旧手順の見直し
21	電子メール	要保護情報	6.2.2(3)子メール	(1)(3)子メールの導入時の対策	(c)(3)報システムセキュリティ責任者は、電子メールの**なりすましの防止策**を講ずること。	<6.2.2(1)(c)関連> 6.2.2(1)-3(3)報システムセキュリティ責任者は、以下を全て含む送信ドメイン認証技術による電子メールのなりすましの防止策を講ずること。 a)(3)MARCによる送信側の対策を行う。DMARCによる送信側の対策を行うためには、SPF、DKIMのいずれか又は両方による対策を行う必要がある。 b)(3)MARCによる受信側の対策を行う。DMARCによる受信側の対策を行うためには、SPF、DKIMの両方による対策を行う必要がある。 6.2.2(1)-4(3)報システムセキュリティ責任者は、必要に応じて、S/MIME等の電子メールにおける電子署名の技術による電子メールのなりすましの防止策を講ずること。 6.2.2(1)-5(3)報システムセキュリティ責任者は、職員等が機関等外の者と電子メールを送受信する場合には、政府ドメイン名を取得できない場合を除き、政府ドメイン名を使用した電子メールアドレスが利用される機能を備えること。	以下は原文参照 ●**基**本対策事項**6.2.2(1)-3**「送信ドメイン認証技術」について ●**基**本対策事項**6.2.2(1)-3 a)**「DMARC」について ●**基**本対策事項**6.2.2(1)-3 a)**「送信側の対策」について ●**基**本対策事項**6.2.2(1)-3 a)**「SPF」について ●**基**本対策事項**6.2.2(1)-3 a)**「DKIM」について ●**基**本対策事項**6.2.2(1)-3 a)**「いずれか又は両方による対策を行う必要」について ●**基**本対策事項**6.2.2(1)-3 b)**「受信側の対策」について ●**基**本対策事項**6.2.2(1)-3 b)**「SPF、DKIMの両方による対策を行う必要がある」について ●**基**本対策事項**6.2.2(1)-4**「必要に応じて、S/MIME等の電子メールにおける電子署名」について ●**基**本対策事項**6.2.2(1)-5**「政府ドメイン名を取得できない場合を除き、政府ドメイン名を使用した電子メールアドレスが利用される機能」について	・以下を全て含む送信ドメイン認証技術（SPF、DKIM、DRMARC等）による電子メールのなりすましの防止策を講ずること。 a)(3)MARCによる送信側の対策を行う。DMARCによる送信側の対策を行うためには、SPF、DKIMのいずれか又は両方による対策 b)(3)MARCによる受信側の対策を行う。DMARCによる受信側の対策を行うためには、SPF、DKIMの両方による対策 ・必要に応じて、S/MIME等の電子メールにおける電子署名の技術による電子メールのなりすましの防止策を講ずること。 ・職員等が機関等外の者と電子メールを送受信する場合には、政府ドメイン名を取得できない場合を除き、政府ドメイン名を使用した電子メールアドレスが利用される機能を備えること。
20		要機密情報	なし	なし	なし	なし	なし	なし

【参考】構成要素と要保護情報の対策

No	構成要素	分類	大項番	中項番	遵守事項（統一基準 第6部より）	基本的対策事項（ガイドラインより）	対策事項の解説（ガイドラインより）	具体的な対策案
22		要保全情報	6.2.2 電子メール	(1)電子メールの導入時の対策	(d)情報システムセキュリティ責任者は、インターネットを介して通信する電子メールの**盗聴及び改ざんの防止**のため、電子メールのサーバ間通信の暗号化の対策を講ずること。	<6.2.2(1)(d)関連> 6.2.2(1)-6情報システムセキュリティ責任者は、以下を例とする電子メールの盗聴及び改ざんの防止策を講ずること。 a) SMTPによるサーバ間通信をTLSにより保護する。 b) S/MIME等の電子メールにおける暗号化及び電子署名の技術を利用する。	●遵守事項**6.2.2(1)(d)**「サーバ間通信の暗号化」について 相手先サーバが暗号化に対応していない状況も考慮しなければならない。自らが送信側となる際には、相手先が暗号化に対応可能であることを確認し、確認が取れた場合には以降の通信を暗号化することが求められる。また、自らが受信側となる際には、相手先からの接続要求時に暗号化の機能に対応していることを示すことが求められる。 暗号化された通信の監視については、「（解説）遵守事項**5.2.1(3)(a)(イ)**『監視するデータが暗号化されている場合は、必要に応じて復号」について」を参照のこと。 また、電子メールクライアントと電子メールサーバ間の通信の暗号化についても併せて対応することが望ましい。 ●遵守事項**6.2.2(1)(d)**「対策を講ずること」について 技術的な事情等により対策に時間を要する場合は、「インターネット通信のセキュリティ強化と利用者に対する配慮について」（平成**29**年７月**10**日　内閣官房内閣サイバーセキュリティセンター事務連絡）に基づいて、計画的に対策を推進することが求められる。 以下は原文参照 ●**3**基本対策事項**6.2.2(1)-6 a)**「**SMTP**によるサーバ間通信を**TLS**により保護」について ●**3**基本対策事項**6.2.2(1)-6 b)**「**S/MIME**等の電子メールにおける暗号化及び電子署名」について	ウェブサーバからの情報漏えい防止策として、以下を全て含む管理や設定を行うこと。 a) 公開を想定していないファイルをウェブ公開用ディレクトリに置かない。 b) 開発時状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。 c) ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認する。
23		要安定情報	なし	なし	なし	なし	なし	なし
24	ウェブ	要保護情報	なし	なし	なし	なし	なし	なし
25		要機密情報	6.2.3 ウェブ	(1)ウェブサーバの導入・運用時の対策	(b)情報システムセキュリティ責任者は、ウェブサーバからの不用意な**情報漏えいを防止**するための措置を講ずること。	<6.2.3(1)(b)関連> 6.2.3(1)-2情報システムセキュリティ責任者は、ウェブサーバからの不用意な情報漏えいを防止するために、以下を全て含むウェブサーバの管理や設定を行うこと。 a) 公開を想定していないファイルをウェブ公開用ディレクトリに置かない。 b) 開発時状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。 c) ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認する。	なし	
26		要保全情報	6.2.3 ウェブ	(1)ウェブサーバの導入・運用時の対策	(d)情報システムセキュリティ責任者は、インターネットを介して転送される情報の**盗聴及び改ざんの防止**のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じること。	<6.2.3(1)(d)関連> 6.2.3(1)-5情報システムセキュリティ責任者は、通信時の盗聴による第三者への情報の漏えい及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を全て含むウェブサーバの実装を行うこと。 a) SSL/TLS機能を適切に用いる。 b) SSL/TLS機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いる。 c) 暗号技術検討会及び関連委員会（CRYPTREC）により作成された「TLS暗号設定ガイドライン」に従って、TLSサーバを適切に設定する。	●遵守事項**6.2.3(1)(d)**「対策を講じること」について 技術的な事情等により対策に時間を要する場合は、「インターネット通信のセキュリティ強化と利用者に対する配慮について」（平成**29**年７月**10**日内閣官房内閣サイバーセキュリティセンター事務連絡）に基づいて、計画的に対策を推進することが求められる。 以下は原文参照 ●**3**基本対策事項**6.2.3(1)-5 a)**「**TLS**機能を適切に用いる」について ●**3**基本対策事項**6.2.3(1)-5 b)**「利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局」について ●**3**基本対策事項**6.2.3(1)-5 c)**「「**TLS**暗号設定ガイドライン」に従って、**TLS**サーバを適切に設定」について	・以下を全て含むウェブサーバの実装を行うこと。 a) SSL/TLS機能を適切に用いる。 b) SSL/TLS機能のために必要となるサーバ証明書は、証明書発行機関により発行された電子証明書を用いる。 c) 暗号技術検討会及び関連委員会（CRYPTREC）の「TLS暗号設定ガイドライン」に準拠した設定を実施する。
27		要安定情報	なし	なし	なし	なし	なし	なし
28	ドメインネームシステム（DNS）	要保護情報	なし	なし	なし	なし	なし	なし
29		要機密情報	6.2.4 ドメインネームシステム（DNS）	(1)DNSの導入時の対策	(c)情報システムセキュリティ責任者は、コンテンツサーバにおいて、機関等のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に**漏えいしないための措置**を講ずること。	<6.2.4(1)(c)関連> 6.2.4(1)-4情報システムセキュリティ責任者は、機関等内のみで使用する名前の解決を提供するコンテンツサーバにおいて、以下を例とする当該コンテンツサーバで管理する情報の漏えいを防止するための措置を講ずること。 a) 外部向けのコンテンツサーバと別々に設置する。 b) ファイアウォール等でアクセス制御を行う。	●**3**基本対策事項**6.2.4(1)-4**「当該コンテンツサーバで管理する情報の漏えいを防止するための措置」について コンテンツサーバにおいて、機関等内のみで使用する名前の解決を提供する場合、内部のみで使用している名前情報を機関等外の者が取得できないようにすることを求めている。	システム内部でのみ利用するDNSコンテンツサーバにおいて、以下の措置を講ずること。 a) 外部向けのコンテンツサーバと別々に設置する。 b) ファイアウォール等でアクセス制御を行う。
30		要保全情報	6.2.4 ドメインネームシステム（DNS）	(2)DNSの運用時の対策	(b)情報システムセキュリティ責任者は、コンテンツサーバにおいて管理する**ドメインに関する情報が正確であること**を定期的に確認すること。	なし	●遵守事項**6.2.4(2)(b)**「ドメインに関する情報が正確であることを定期的に確認」について 国内で使用されているドメイン名の登録情報が不正に書き換えられ、攻撃者が用意したネームサーバの情報が追加される“ドメイン名ハイジャック”と呼ばれる攻撃がある。このような攻撃への対策として、コンテンツサーバで管理するドメインに関する情報について、設定誤りや不正な改ざん等が発生していないかを定期的に確認することで、情報の正確性を維持することを求めている。管理するドメインに関する情報の具体例として、以下に挙げる登録内容等を確認することが考えられる。 ・ホストのIPアドレス情報を登録するA（AAAA）レコード ・ドメインの電子メールサーバ名を登録するMXレコード ・機関等が送信した電子メールが詐称されていないかどうかを受信者側で認証するために必要なSPFレコード等を登録するTXTレコード なりすまし防止の観点からは、管理するドメインについてのSPFレコード等が正確であるか否かを確認したり、ドメインを廃止する場合には、ドメインの廃止申請を行い、当該ドメインが確実に廃止されていることを確認したりすることが重要である。 なお、廃止するドメインが政府ドメイン名でない場合は、廃止後のドメインの第三者による不正利用を防止するため、当該ドメインを利用しなくなった後でも一定期間登録を継続することや可能な限りウェブサイトからのリンクを解除したり、配布物等に記載しないようにすること等が必要である。また、政府ドメイン名を含むJPドメイン名では、第三者によってドメイン名の登録者名義やDNSサーバ情報等の登録情報を不正に書き換えられることを防ぐため、情報の変更申請を制限するサービス（レジストリロック）や第三者による意図しないドメイン名移転を防ぐため、指定事業者変更申請を制限するサービス（指定事業者変更ロック）が利用可能な場合があるので、当該サービスの利用を検討してもよい。	・DNSコンテンツサーバにおいて管理ドメインに関する情報が正確であることを定期的に確認すること。確認するレコード種別例は以下の通り 例） ・A（AAAA）レコード ・MXレコード ・TXTレコード ・SPFレコード ・ドメイン廃止時にはドメインの廃棄申請後、当該ドメインが確実に廃止されているかの確認を実施すること。 ・政府ドメイン名を含むJPドメイン名の利用においては、レジストリロック（情報の変更申請を制限するサービス）や、指定事業者変更ロック（指定事業者変更申請を制限するサービス）等のサービス利用を検討すること。
31		要安定情報	6.2.4 ドメインネームシステム（DNS）	(1)DNSの導入時の対策	(a)情報システムセキュリティ責任者は、**要安定情報**を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。	<6.2.4(1)(a)関連> 6.2.4(1)-1機関等システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、以下を例とする名前解決を停止させないための措置を講ずること。 a) コンテンツサーバを冗長化する。 b) 通信回線装置等や、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う。 c) IPS等が提供するマネージドDNSサービスやDDoS（Distributed Denial of Service）対策サービスを利用する。 d) IP及びTCPの両方でサービスを提供する。	●**3**基本対策事項**6.2.4(1)-1 a)**「冗長化」について コンテンツサーバは、冗長化しておくことが一般的である。その際には、ネットワーク障害等を考慮して各々のコンテンツサーバをそれぞれ異なるネットワークに配置しておく、災害等を考慮して物理的に離れた建物や遠隔地に設置しておくなど、情報と情報システムに要求される可用性の確保に応じて、最適な構成を検討する必要がある。ISP等が提供するセカンダリDNSの利用等も、遠隔地への設置による冗長化の措置の例である。また、要求される可用性の度合いに応じて、保守作業による復旧等、冗長化以外の措置を探ることも考えられる。	・DNSコンテンツサーバにおいて、以下を例とする名前解決機能を停止させないための措置を講ずること。 a) コンテンツサーバの冗長化 b) DNSコンテンツサーバへのサービス不能攻撃（DDoS等）に備えた通信回線装置等でのアクセス制御 c) IPS等が提供するマネージドDNSサービスやDDoS（Distributed Denial of Service）対策サービスの利用検討 d) IP及びTCP両方でのサービス提供
32	データベース	要保護情報	なし	なし	なし	なし	なし	なし
33		要機密情報	6.2.5 データベース	(1)データベースの導入・運用時の対策	(a)情報システムセキュリティ責任者は、データの窃取、電磁的記録媒体の盗難等による**情報の漏えいを防止**する必要がある場合は、適切に暗号化をすること。	<6.2.5(1)(e)関連> 6.2.5(1)-7情報システムセキュリティ責任者は、データベースに格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。	●遵守事項**6.2.5(1)(e)**「適切に暗号化」について データベースに格納されるデータを暗号化する方法には、電磁的記録媒体の暗号化、データベースのテーブルの暗号化、カラムの暗号化等がある。想定される脅威や利用環境等によってメリット・デメリットがあるため、適切な方式を選択することが望ましい。	・データベースに格納されているデータに対しては暗号化を実施すること。またバックアップデータやトランザクションデータ等についても暗号化を実施すること。
34		要保全情報	6.2.5 データベース	(1)データベースの導入・運用時の対策	(c)情報システムセキュリティ責任者は、データベースに格納されているデータに対するアクセス権を有する利用者による**データの不正な操作**を検知できるよう、対策を講ずること。	<6.2.5(1)(c)関連> 6.2.5(1)-4情報システムセキュリティ責任者は、業務を遂行するに当たって不必要なデータの操作を検知できるよう、以下を例とする措置を講ずること。 a) 定数以上のデータの取得に関するログを記録し、警告を発する。 b) データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する。	●遵守事項**6.2.5(1)(c)**「データの不正な操作を検知」について 通常業務では取り扱わないような大量のデータを取得することや業務時間外にデータの操作を行う等の不正な操作を、SIEM（Security Information and Event Management）やUEBA（User and Entity Behavior Analytics）等を導入することによってシステム的に検知する方法を用いるとよい。なお、データベースのログを目視によって確認する方法も考えられるが、人手に依存する方法は確認漏れ等が発生する可能性があり望ましくない。 データの不正な操作が発生したときの影響や操作ログの量等を踏まえて、システム的に検知する方法か人手に依存する方法かを選択するとよい	・不必要なデータの操作を検知できるよう、SIEM（Security Information and Event Management）やUEBA（User and Entity Behavior Analytics）等の導入、および同製品と同等の対策を実施すること。なお人手に依存する確認方法（ログの目視確認等）は推奨されない。
35		要安定情報	なし	なし	なし	なし	なし	なし
36	通信回線	要保護情報	なし	なし	なし	なし	なし	なし
37		要機密情報	6.4.1 通信回線	(1)通信回線の導入時の対策	(c)情報システムセキュリティ責任者は、**要機密情報**を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。	<6.4.1(1)(c)関連> 6.4.1(1)-2情報システムセキュリティ責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。通信回線の秘匿性確保の方法として、TLS、IPsec等による暗号化を行うこと。また、その際に使用する暗号アルゴリズム及び鍵長については、「電子政府推奨暗号リスト」を参照し決定すること。	なし	・TLS、IPsec等による暗号化を行うこと。なお、使用する暗号アルゴリズム及び鍵長については、「電子政府推奨暗号リスト」に従うことが推奨される。

【参考】構成要素と要保護情報の対策

No	構成要素	分類	大項番	中項番	遵守事項（統一基準 第6部より）	基本的対策事項（ガイドラインより）	対策事項の解説（ガイドラインより）	具体的な対策案
38		要機密情報	6.4.2 通信回線装置	(3)通信回線装置の運用終了時の対策	(a)情報システムセキュリティ責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた**情報が漏えいすることを防止**するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずること。	なし	●遵守事項**6.4.2(3)(a)**「情報を抹消するなど適切な措置」について 運用を終了した通信回線装置が再利用されたとき又は廃棄された後に、保存されていた情報が漏えいすることを防ぐための抹消の方法としては、通信回線装置の初期化、内蔵電磁的記録媒体の物理的な破壊等の方法がある。通信回線装置内にも、設定情報や通信ログ等の情報が保存されていることから、サーバ装置及び端末と同様に運用終了時に留意しておくことが必要である。 通信回線装置は通信事業者からリース提供されることがあり、その場合は通信回線の運用終了に伴い通信事業者に装置を返却することになるため、通信回線装置の初期化の手順等本項を遵守するための方法について、通信事業者に確認する必要がある。	・通信機器の運用終了や廃棄維持には、通信回線装置の初期化や内蔵電磁的記録媒体の物理的な破壊等、全ての情報を抹消する措置を講ずること。
39		要機密情報	6.4.3 無線LAN	(1)無線LAN環境導入時の対策	(a)情報システムセキュリティ責任者は、無線LAN技術を利用して機関等内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、**通信内容の秘匿性を確保**するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。	<6.4.3(1)(a)関連> 6.4.3(1)-1情報システムセキュリティ責任者は、無線LAN技術を利用して機関等内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、情報システムの分類に基づき、以下の対策を講ずること。 【基本セキュリティ対策】以下を全て含む対策を講ずること。 a)無線LAN通信の暗号化 b)無線LAN回線利用申請手続の整備 c)無線LAN機器の管理手順の整備 d)要許可者等に提供する無線LANによるインターネット接続回線と業務で使用する機関等LANの分離 【追加セキュリティ対策】基本セキュリティ対策の実施に加えて、以下を例とする対策を講ずること。 e)IEEE 802.1Xによる無線LANへのアクセス主体の認証	以下は原文参照 ●b基本対策事項6.4.3(1)-1 a)「無線LAN通信の暗号化」について ●b基本対策事項6.4.3(1)-1 c)「無線LAN機器の管理」について ●a基本対策事項6.4.3(1)-1 d)「未許可等に提供する無線LANによるインターネット接続回線」について ●b基本対策事項**6.4.3(1)-1 e)**「**IEEE 802.1X**による無線**LAN**へのアクセス主体の認証」について **IEEE 802.1X**認証については、機関等**LAN**システム等の無線**LAN**において**要機密情報**を扱う場合は、高度な情報セキュリティ対策を要求する情報システムに該当する場合に限定せず、導入することが望ましい。 **IEEE 802.1X**認証で用いられる**EAP**の規格について、脆弱性が指摘されている**EPA-MD5**や**LEAP**等の認証方式もあるため、利用する規格についてセキュリティ上問題が無いか確認すること。 また、偽のアクセスポイントを利用した攻撃等へ対抗するためにも相互認証に対応した規格を利用すること。また、認証に用いる識別符号（識別コード及びパスワード、電子証明書等）の安全な配布方法と運用手順についても整備すること。	・無線LAN技術を利用する場合は、通信内容の秘匿性を確保するために通信路の暗号化設定を実施する。例えばWPA3 Enterprise（Wi-Fi Protected Access 3 Enterprise）やWPA2 Enterprise（Wi-Fi Protected Access 2 Enterprise）方式を選択することが考えられる。なお、WEP（Wired Equivalent Privacy）、TKIP（Temporal Key Integrity Protocol）等は、比較的容易に解読できたり、通信を妨害できたりするという脆弱性が報告されているため、利用してはならない。 ・来訪者等に提供する無線LANと機関等LANをルータ等の通信回線装置によって論理的に分離すること ・機関等LANにはIEEE 802.1Xによる無線LANへのアクセス主体の認証を導入することが推奨される。
40		要保全情報	なし	なし	なし	なし	なし	なし
41		要安定情報	6.4.1 通信回線	(1)通信回線の導入時の対策	(a)情報システムセキュリティ責任者は、**要安定情報**を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。	<6.4.1(1)(e)関連> 6.4.1(1)-4情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムが接続される通信回線を構築する場合は、以下を例とする対策を講ずること。 a)通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける。 b)通信回線及び通信回線装置を冗長構成にする。 c)端末等が情報システムと通信可能な代替手段を整備する。	●b遵守事項6.4.1(1)(e)「要安定情報を取り扱う情報システム」について 要安定情報を取り扱う情報システムについては、「（解説）基本対策事項5.2.1(3)-7「要安定情報を取り扱う情報システム」について」を参照のこと。 ●b基本対策事項**6.4.1(1)-4 b)**「通信回線及び通信回線装置を冗長構成にする」について 高い可用性が求められる情報システムを構築する場合は、大規模災害の発生を想定し、通信回線を冗長構成にしておくことが望ましい。また、機関等の施設から外部に敷設する通信回線の管路についても、例えば、異なる通信事業者が敷設した通信回線による複数の経路で構築しておくことで、災害を受けた際に復旧にかかる時間が短縮されるなどの効果が期待される。	・以下を例とする対策を講ずること。 a)通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける。 b)通信回線及び通信回線装置を冗長構成にする。 c)端末等が情報システムと通信可能な代替手段を整備する。
42		要安定情報	6.4.2 通信回線装置	(2)通信回線装置の運用時の対策	(b)情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。	なし	なし	・運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。
43	ソフトウェア	要保護情報	なし	なし	なし	なし	なし	なし
44		要機密情報	6.5.1 情報システムの基盤を管理又は制御するソフトウェア	(1)情報システムの基盤を管理又は制御するソフトウェア導入時の対策	(a)情報システムセキュリティ責任者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及び**ソフトウェア自体を保護するための措置**を講ずること。	なし	●遵守事項**6.5.1(1)(a)**「情報システムの基盤を管理又は制御するソフトウェア」について 情報システムの基盤を管理又は制御するソフトウェアは、端末やサーバ装置、ネットワークなどを管理又は制御するための権限を用いてアクセスが可能な機能を有しているソフトウェアを想定しており、当該ソフトウェアが悪用された場合、被害が広範囲に及ぶリスクが高くなる。また、当該ソフトウェアにおいて**要機密情報**が取り扱われる場合は、当該ソフトウェアを保護することで情報を守る必要がある。したがって、情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及び当該ソフトウェア自体については、必要な措置を行う必要がある。なお、情報システムの基盤を管理又は制御するソフトウェアについては、以下のソフトウェアが考えられる。 -端末やサーバ装置、通信回線装置等を制御するソフトウェア -統合的な主体認証を管理するソフトウェア -ネットワークを制御・管理するソフトウェア -資産を管理するソフトウェア -監視に関連するソフトウェア -情報システムのセキュリティ機能として使用するソフトウェア 以下は原文参照 ●b遵守事項**6.5.1(1)(a)**「端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置」について	・情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及び当該ソフトウェア自体について情報システムのセキュリティ機能に示される以下の対策を実施する。 ・**B**.1「主体認証機能」 ・**B**.2「アクセス制御機能」 ・**B**.3「権限の管理」 ・**B**.4「ログの取得・管理」 ・**B**.1「ソフトウェアに関する脆弱性対策」
45		要保全情報	なし	なし	なし	なし	なし	なし
46		要安定情報	なし	なし	なし	なし	なし	なし
48	アプリケーション・コンテンツ	要保護情報	6.6.1 アプリケーション・コンテンツの作成・運用時の対策	(2)アプリケーション・コンテンツのセキュリティ要件の策定	(a)情報システムセキュリティ責任者は、機関等外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについてのセキュリティ要件を定め、仕様に含めること。	<6.6.1(2)(a)関連> 6.6.1(2)-1情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下を全て含む対策をセキュリティ要件として仕様に含めること。 a)アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。 b)機密委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。 6.6.1(2)-2情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツが脆弱性を含まないように開発することをセキュリティ要件として仕様に含めること。 6.6.1(2)-3情報システムセキュリティ責任者は、実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラムの形式でコンテンツを提供しないことをセキュリティ要件として仕様に含めること。 6.6.1(2)-4情報システムセキュリティ責任者は、電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与えることをセキュリティ要件として仕様に含めること。 6.6.1(2)-5情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのOSやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OSやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発することをセキュリティ要件として仕様に含めること。 6.6.1(2)-6情報システムセキュリティ責任者は、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなど、サービス利用に当たって必須ではない機能がアプリケーション・コンテンツに組み込まれることがないよう、以下を全て含む開発をすることをセキュリティ要件として仕様に含めること。 a)機関等外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTMLソースを表示させるなどして確認すること。必要があって当該機能を含める場合は、当該機関等外へのアクセスが情報セキュリティ上安全なものであることを確認すること。	以下は原文参照 ●a基本対策事項6.6.1(2)-1「不正プログラムを含まない」について ●a基本対策事項6.6.1(2)-2「脆弱性を含まない」について ●a基本対策事項6.6.1(2)-3「実行プログラムの形式でコンテンツを提供しない」について ●a基本対策事項6.6.1(2)-4「改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与える」について ●a基本対策事項6.6.1(2)-5「脆弱性が存在するバージョンのOSやソフトウェア等の利用を強制する」について ●a基本対策事項6.6.1(2)-5「情報セキュリティ水準を低下させる設定変更を、OSやソフトウェア等の利用者に要求する」について ●a基本対策事項6.6.1(2)-6「サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなど、サービス利用に当たって必須ではない機能」について ●a基本対策事項6.6.1(2)-6 a)「必要があって当該機能を含める場合」について ●a基本対策事項6.6.1(2)-6 b)「機関等外へのアクセスを自動的に発生させる機能」について	要保護情報を含むアプリケーション・コンテンツについて以下の対策を実施する ・ウィルス対策ソフトによるスキャンで不正プログラムの検知 ・脆弱性診断によるプログラム内の脆弱性検出、確認 ・実行プログラム（.exe）形式でのコンテンツ提供の禁止 ・（アプリケーションプログラムの場合）コードサイニング証明書の導入、またはハッシュ値による整合性の確認 ・脆弱性が存在するバージョンのOS,ソフトウェアの禁止 ・システムを利用する利用者端末にセキュリティ低下を招くようなシステム仕様の禁止 ・トラッキング処理や利用者のキー入力を意図しない形で送信するなど、必要なくサービス利用者情報を同意なく第三者に提供する機能の禁止 ・システム外部へのアクセスを自動的に発生させるコンテンツ、または機能の禁止
49		要機密情報	なし	なし	なし	なし	なし	なし
50		要保全情報	なし	なし	なし	なし	なし	なし
51		要安定情報	なし	なし	なし	なし	なし	なし

【参考】情報の取り扱い_情報システムセキュリティ要件

No	章	分類	大項番	中項番	遵守事項（統一基準 第3部,第7部より）	基本的対策事項（ガイドラインより）	対策事項の解説（ガイドラインより）	具体的な対策案	スコープ可否
1	3	要保護情報	3.1.1 ■報の取扱い	(1)■報の取扱いに係る規定の整備	(a)■括情報セキュリティ責任者は、以下を全て含む情報の取扱いに関する運用規程を整備し、職員等へ周知すること。 (イ)■報の格付及び取扱制限の明示等についての手続	<3.1.1(1)(a)(イ)関連> 3.1.1(1)-3■括情報セキュリティ責任者は、情報の格付及び取扱制限の明示を省略する必要がある場合には、これらに係る認識が共通となるその他の措置の実施条件や実施方法について、情報の取扱いに関する運用規程に含めて整備すること。	●■本対策事項3.1.1(1)-3「明示を省略」について 情報の格付及び取扱制限を確実に視認することができるよう、当該情報に明示しておくことが原則ではあるが、必要な場合には、以下を例に明示が省略可能な条件について定めておくとよい。 a)情報システムに記録される情報の格付及び取扱制限を当該情報システムの手順書等により明記し、当該情報システムの利用者にあらかじめ周知している場合。 b)情報の格付及び取扱制限の省略時における当該情報の格付及び取扱制限の取扱について、取扱手順に規定し、職員等にあらかじめ周知している場合。 ただし、格付及び取扱制限の明示を省略した場合には、以下の事項に注意する必要がある。 c)格付及び取扱制限の省略を認識できない者への情報の提供 格付の区分及び取扱制限が明示されていない**要保護情報**を、格付及び取扱制限の決定内容を認識できない職員等に提供する必要が生じた場合（例えば、他機関等に情報を提供等する場合）は、当該情報に格付の区分及び取扱制限を明示した上で提供するなどしなければならない。 d)取扱制限の明示を省略した場合における取扱制限の追加・変更 例えば、ある文書の取扱制限の明示を省略している場合であって、当該文書の一部に取扱制限を追加するときは、追加する取扱制限を明示すること。	※運用規定・ルールに関する要求のため対象外	対象外
2	3	要保護情報	3.1.1 ■報の取扱い	(3)■報の格付及び取扱制限の決定・明示等	(b)■員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。	なし	●■遵守事項3.1.1(3)(b)「継承」について 業務資料等を参考に新たに別の資料を作成する場合等において、元となった資料等に記載されていた情報の機密性に関する格付及び取扱制限について、新たに作成した資料等に適切に引き継ぐことを求めている。例えば**機密性３情報**を他の資料等に転用する場合においては、当該資料に記載されている転用部分については**機密性３情報**として取り扱われるべきである。また、**要保全情報又は要安定情報**を複製する場合については、複製された情報に対して過度な保護対策を求めないように、完全性１情報又は可用性１情報として格付を見直し再決定することが望ましい。ただし、バックアップを原本として情報を保管する目的で複写する場合は、**要保全情報**とすべきであるなど、状況に応じた適切な判断が求められる。	※運用規定・ルールに関する要求のため対象外	対象外
3	3	要保護情報	3.1.1 ■報の取扱い	(4)■報の利用・保存	(a)■員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。	<3.1.1(4)(a)(d)関連> 3.1.1(4)-1■員等は、情報の格付及び取扱制限に応じて、情報を取り扱う際は、以下を全て含む対策を講ずること。 a)**■保護情報**を放置しない。	なし	※運用規定・ルールに関する要求のため対象外	対象外
4	3	要保護情報	3.1.1 ■報の取扱い	(4)■報の利用・保存	(c)■員等は、**要保護情報**について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。	なし	●■遵守事項3.1.1(4)(c)「要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること」について 機関等外で開催される会議への出席等の際に、**要機密情報**を用いて情報処理を行う場合は、のぞき見の防止や不要となった情報の削除等の措置を講ずるなど、情報の格付や取扱制限に応じて適切な安全管理措置を講ずる必要がある。この際、技術的な対策については、遵守事項6.1.2(1)(b)及び遵守事項6.1.3(2)(c)に基づき定められた安全管理措置を参考にするとよい。	※技術的な対策については、遵守事項6.1.2(1)(b)及び遵守事項6.1.3(2)©になるので対象外	対象外
5	3	要保護情報	3.1.1 ■報の取扱い	(5)■報の提供・公表	(b)■員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。	なし	●■遵守事項3.1.1(5)(b)「提供先において」・「適切に取り扱われるよう」について **要保護情報**を機関等外の者に提供する場合には、提供先において当該情報が適切に取り扱われるように、情報の取扱い上の留意事項を提供先へ確実に伝達する必要がある。 伝達方法としては、他機関等や委託先等の情報の提供先に、対策基準や情報の取扱いに関する手順書、統一基準との格付定義の差分に関する説明等を提示し、格付や取扱制限に応じた取扱方法を示す方法が考えられる。 この場合、格付の区分だけを示しても、提供先においては当該格付区分がどのように取り扱われるべきものであるか認識できない可能性があるため、当該格付の区分の定義について提供先にあらかじめ周知しておく必要がある。また、提供する情報を適切に管理するために必要な措置が具体的に分かるようにする（例えば、「委員以外への再配布を禁止する」と明示する。）など、格付以外の方法で取扱方法を示すことも考慮する必要がある。	※運用規定・ルールに関する要求のため対象外	対象外
6	3	要保護情報	3.1.1 ■報の取扱い	(6)■報の運搬・送信	(a)■員等は、**要保護情報**が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。	<3.1.1(6)(a)関連> 3.1.1(6)-1■員等は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、セキュアな運送サービスを提供する運送事業者により運搬すること。	●■本対策事項3.1.1(6)-1「セキュアな運送サービス」について セキュアな運送サービスとしては、受取の際に本人確認を行うサービス（例えば、本人限定受取郵便）や、専用車両による配達サービス、配達状況の追跡が可能なサービス等が存在する。	※物理的な媒体の運送ルールに関する要求のため対象外	対象外
7	3	要保護情報	3.1.1 ■報の取扱い	(6)■報の運搬・送信	(b)■員等は、**要保護情報**である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること	<3.1.1(6)(b)関連> 3.1.1(6)-4■員等は、**要保護情報**である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定すること。 a)■関等管理の通信回線を用いて送信する。 b)■線できる通信回線を使用して送信する。 c)■PNを用いて送信する。 d)■MIME等の暗号化された電子メールを使用して送信する。 e)■関等独自で運用している又は機関等が利用を承認しているなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用する。	以下は原文参照 ●■本対策事項3.1.1(6)-4 b)「信頼できる通信回線」について ●■本対策事項3.1.1(6)-4 c)「VPN」について ●■本対策事項3.1.1(6)-4 e)「機関等独自で運用している又は機関等が利用を承認しているなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境」について	**ガイドライン　クラウドサービスを利用して要機密情報を取り扱う場合は、4.2.1「クラウドサービスの選定（要機密情報を取り扱う場合）」及び4.2.2「クラウドサービスの利用（要機密情報を取り扱う場合）」、クラウドサービスを利用して要機密情報を取り扱わない場合は、4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」を参照のこと。** 要保護情報に該当するデータを送信する場合は以下の例に同様の対策を行うこと。 a)■関等管理の通信回線を用いて送信する。 b)■線できる通信回線を使用して送信する。 c)■PNを用いて送信する。 d)■MIME等の暗号化された電子メールを使用して送信する。 e)■関等独自で運用している又は機関等が利用を承認しているなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用する。	対象
8	3	要機密情報	3.1.1 ■報の取扱い	(1)■報の取扱いに係る規定の整備	(a)■括情報セキュリティ責任者は、以下を全て含む情報の取扱いに関する運用規程を整備し、職員等へ周知すること。 (ウ)■報の格付及び取扱制限の継承、見直しに関する手続	<3.1.1(1)(a)(ウ)関連> 3.1.1(1)-4■括情報セキュリティ責任者は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、以下を例とする内容を、情報の取扱いに関する運用規程に含めて整備すること。 a)■報を作成する際に、参照した情報又は入手した情報の**機密性**に係る格付及び取扱制限を継承する。 b)■器存の情報に、より**機密性の高い情報**を追加するときは、格付及び取扱制限を見直す。 c)**機密性の高い情報**から機密に該当する部分を削除したときは、残りの情報の機密性に応じて格付及び取扱制限を見直す。 d)■報を複製する場合には、元となる情報の**機密性**に係る格付及び取扱制限を継承する。 f)■者が決定した情報の格付及び取扱制限を見直す必要がある場合には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下本欄において「決定者等」という。）に確認を求める。	●■本対策事項3.1.1(1)-4 f)「見直す必要がある場合」について 利用する元の情報への修正、追加又は削除のいずれでもないが、元の格付又は取扱制限そのものがその時点で不適当と考える場合には、格付又は取扱制限の見直しについてその決定者に確認を求める必要がある。また、異動等の事由により、当該決定者と相談することが困難である場合等においては、決定について引き継いだ者又は当該決定者の上司に相談し、その是非を検討することになる。決定者等による見直しが無い限り、当該情報の利用者がこれらの者に無断で、格付又は取扱制限を変更することは許されない。 なお、見直しを行わなければならない場合については、以下を参考に規定すること。 a)形成時には**要機密情報**だった情報の機密性が失われた場合（時間の経過により変化した場合） b)**機密性３情報**として格付されている資料等から**機密性３情報**に係る部分を全て削除した場合 c)取扱制限で参照先を限定していた情報について、その後参照先を変更する必要が生じた場合 d)取扱制限で保存期間を指定していた情報について、その後期間の延長をする場合 e)格付及び取扱制限を決定した際の判断が不適切であったと考えられる場合 f)行政文書管理規則等が、情報の作成又は入手時以降に改定されており、当該行政文書管理規則等における情報の取扱いに変更がある場合	※運用規定・ルールに関する要求のため対象外	対象外
9	3	要機密情報	3.1.1 ■報の取扱い	(3)■報の格付及び取扱制限の決定・明示等	(a)■員等は、情報の作成時及び機関等外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること。	なし	●■遵守事項3.1.1(3)(a)「格付及び取扱制限を決定」について 格付及び取扱制限が不十分な場合、情報漏えい等のリスクが高まるが、一方で、情報の利用を円滑に行うためには、格付及び取扱制限を必要以上に高くしないことが必要である。そのため、格付及び取扱制限を決定する際には、機関等の基準に照らして、要件に過不足が生じないようにすること。例えば、機密性１情報に相当する公開しても差し支えない情報をむやみに**要機密情報**に決定すると、過度な保護対策を求めることになり、業務の効率的な運営に支障をきたすおそれがある。 また、他機関等との情報の受け渡しを行う際には、統一基準との格付定義の差分に関する情報を当該機関等から得るなどして、自機関等の基準との差分について考慮の上、格付及び取扱制限を決定する必要がある。	※運用規定・ルールに関する要求のため対象外	対象外

【参考】情報の取り扱い_情報システムセキュリティ要件

No	章	分類	大項番	中項番	遵守事項（統一基準 第3部,第7部より）	基本的対策事項（ガイドラインより）	対策事項の解説（ガイドラインより）	具体的な対策案	スコープ可否
10	3	要機密情報	3.1.1 ■報の取扱い	(4) ■報の利用・保存	(b) ■員等は、**機密性３情報**について要管理対策区域外で情報処理を行う場合は、課室情報セキュリティ責任者の許可を得ること。	なし	なし	※運用規定・ルールに関する要求のため対象外	対象外
11	3	要機密情報	3.1.1 ■報の取扱い	(4) ■報の利用・保存	(d) ■員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。なお、独立行政法人及び指定法人における職員等は、**機密性３情報**を機器等に保存する際、以下の措置を講ずること。ただし、独立行政法人及び指定法人において、**機密性３情報**について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。 (ア) ■器等に保存する場合は、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用すること。 (イ) ■該情報に対し、暗号化による保護を行うこと。 (ウ) ■該情報を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずること。	＜3.1.1(4)(a)(d)関連＞ 3.1.1(4)-1 ■員等は、情報の格付及び取扱制限に応じて、情報を取り扱う際は、以下を全て含む対策を講ずること。 b) ■機密情報を必要以上に複製しない。 c) ■磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずる。	●b遵守事項**3.1.1(4)(d)**「保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること」について 情報システムに、ファイルに対する書込権限者の制限や、ファイルのセキュリティ設定でパスワード設定等のアクセス制御機能が装備されている場合、当該情報の格付及び取扱制限に従って、必要なアクセス制御の設定を行うことが求められる。例えば、取扱制限として閲覧範囲の制限が指定されている場合は、第三者等から参照されないよう、読取制限の属性を付与することや、要保全情報であれば、第三者等から変更されないよう、上書き禁止の属性を付与することがこれに当たる。 アクセス制御は、サーバ装置、端末、OS、アプリケーション、ファイル等を単位に行うことができるため、これらを選択し組み合わせて、適切なアクセス制御を実現するとよい。 なお、文書管理ガイドラインの秘密文書の管理に関するモデル要領において、「秘密文書については、インターネットに接続していない電子計算機又は媒体等に保存し、暗号化等による保護を行うとともに、当該秘密文書を記録する電子計算機、媒体等について、保存を金庫等で行うなどにより物理的な盗難防止措置を施すこと。秘文書については、インターネットからの侵入に対する多重防御による情報セキュリティ対策が施された電子計算機でも保存することができる。」とされている。 以下は原文参照 ●b遵守事項**3.1.1(4)(d)**「独立行政法人及び指定法人における職員等」について ●b遵守事項**3.1.1(4)(d)(ウ)**「盗難及び不正な持ち出し等の物理的な脅威から保護するための対策」について	機密性３情報に対するデータには以下を例にした対策を行う ・サーバ装置、端末、OS、アプリケーション、ファイルなどの単位でアクセス制御（書込権限者の制限、パスワード設定、読取制限の属性付与） ・秘密文書は、インターネットに接続していない電子計算機または媒体に保存する。 ・保存する秘密文書は暗号化等で保護する。 ・秘密文書を記録する電子計算機、媒体等について、物理的な盗難防止措置（例：金庫で保存）を施す。 ・秘密文書をインターネットからの侵入に対して多重防御が施された電子計算機でも保存することができる。 要保全情報に対するデータには以下を例にした対策を行う ・第三者から変更されないように上書き禁止の属性を付与	対象
12	3	要機密情報	3.1.1 ■報の取扱い	(5) ■報の提供・公表	(a) ■員等は、情報を公表する場合には、当該情報が**機密性１情報**に格付されるものであることを確認すること。	なし	●b遵守事項**3.1.1(5)(a)**「機密性１情報に格付されるもの」について 保有する情報をウェブサイト等により広く国民に提供する場合、公表しようとする情報の格付の適正さを再度検討し、格付及び取扱制限の明示を削除するなどを考慮する必要がある。 なお、情報の公表ではないものの、電子調達システム等において調達情報を委託先候補事業者に閲覧を許可する場合が考えられる。情報システムの構成図等サイバー攻撃を企図する者が有利になるような情報については、開示対象者と機密保持契約を締結するなどして厳重な管理のもと閲覧を許可するなどして、細心の注意を払う必要がある。	※運用規定・ルールに関する要求のため対象外	対象外
13	3	要機密情報	3.1.1 ■報の取扱い	(5) ■報の提供・公表	(c) ■立行政法人及び指定法人における職員等は、**機密性３情報**を閲覧制限の範囲外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。	なし	なし	※運用規定・ルールに関する要求のため対象外	対象外
14	3	要機密情報	3.1.1 ■報の取扱い	(5) ■報の提供・公表	(d) ■員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な**情報漏えいを防止**するための措置を講ずること。	＜3.1.1(5)(d)関連＞ 3.1.1(5)-1 ■員等は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な**要機密情報**を抹消すること。	●b遵守事項**3.1.1(5)(d)**「不用意な情報漏えい」について 情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDFファイルの「しおり」等に残留した不要な情報を除去する必要がある。 また、ソフトウェアを用いて文書の特定の部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある	※運用規定・ルールに関する要求のため対象外	対象外
15	3	要機密情報	3.1.1 ■報の取扱い	(6) ■報の運搬・送信	(a) ■立行政法人及び指定法人における職員等が、**機密性３情報**を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により運搬すること。ただし、他機関等の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。	＜3.1.1(6)(a)関連＞ 3.1.1(6)-2 ■員等は、要機密情報である電磁的記録を要管理対策区域外に運搬する場合には、以下を例とする情報漏えいを防止するための対策を講ずること。 a) ■搬する情報を暗号化する。 b) ■剰後の個別の情報から分割前の情報が容易に復元あるいは推測できないように要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬する。 c) ■体認証機能や暗号化機能等を備えるセキュアな外部電磁的記録媒体を利用する。	以下は原文参照 ●b基本対策事項**3.1.1(6)-2 a)**「運搬する情報を暗号化する」について ●b基本対策事項**3.1.1(6)-2 b)**・基本対策事項**3.1.1(6)-3 c)**「複数の情報に分割し」について ●b基本対策事項**3.1.1(6)-2 c)**「セキュアな外部電磁的記録媒体」について	機密性３情報に対するデータには以下を例にした対策を行う a) ■搬する情報を暗号化する。 b) ■剰後の個別の情報から分割前の情報が容易に復元あるいは推測できないように要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬する。 c) ■体認証機能や暗号化機能等を備えるセキュアな外部電磁的記録媒体を利用する。	対象
16	3	要機密情報	3.1.1 ■報の取扱い	(6) ■報の運搬・送信	(b) ■立行政法人及び指定法人における職員等が、**機密性３情報**を機関等外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、課室情報セキュリティ責任者が指定する方法により送信すること。ただし、独立行政法人及び指定法人において、機密性３情報について国の行政機関と同等の取扱いを行っている場合は、国の行政機関と同等の措置を講ずることをもって代えることができる。	＜3.1.1(6)(b)関連＞ 3.1.1(6)-3 ■員等は、**要機密情報**である電磁的記録を機関等外通信回線を使用して送信する場合には、以下を例とする情報漏えいを防止するための対策を講ずること。 a) ■信する情報を暗号化する。 b) ■信経路全般が暗号化されている通信経路を用いて送信する。 c) ■剰後の個別の情報から分割前の情報が容易に復元あるいは推測できないように要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて送信する。	●b基本対策事項3.1.1(6)-3 b)「通信経路全般が暗号化」について 通信経路における盗聴による情報漏えいを防止するために、通信経路全般における暗号化通信を求めている。例えば、オンラインストレージ等のファイル共有サービスを利用する場合、機関等外通信回線に接続された機器とファイル共有サービスの間の通信においてTLS通信等の暗号化通信が確実に実施されている場合は、通信経路全般が暗号化されていると考えることができる。なお、通信経路上の機器において監視を目的とした復号が行われている場合があるる。この場合は、復号を行う目的が情報窃取等の不正な目的ではないことが確認できた場合等、通信経路の途中で復号されたとしても情報漏えいの可能性がないと判断できる場合は、通信経路全般が暗号化されていると考えることができる。 また、情報を送受信する機器同士においてエンドツーエンド（E2E）の暗号化を行っている場合も、通信経路全般が暗号化されていると考えることができる。 なお、機関等外の者に電子メールを送信する場合、基本対策事項6.2.2(1)-6 a)で規定するSMTPによる電子メールサーバ間通信をTLSによる保護を行う対策では、最終的な受信先の電子メールサーバまでの通信及び電子メールサーバと電子メールクライアント間の通信が全て保護されることは保証されていないため、必ずしも通信経路全般が暗号化されていると考えることが出来ないことに留意する必要がある。	機密性３情報に対するデータを機関等外通信回線（インターネットを除く。）を使用して送信する場合は以下を例にした対策を行う a) ■信する情報を暗号化する。 b) ■信経路全般が暗号化されている通信経路を用いて送信する。 c) ■剰後の個別の情報から分割前の情報が容易に復元あるいは推測できないように要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて送信する。	対象
17	3	要機密情報	3.1.1 ■報の取扱い	(7) ■報の消去	(b) ■員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。	＜3.1.1(7)(b)関連＞ 3.1.1(7)-1 ■員等は、端末やサーバ装置等をリース契約で調達する場合は、契約終了に伴う返却時の情報の抹消方法及び履行状況の確認手段について、以下を例とする対策を行うこと。 a) ■ース契約の調達仕様書に記載し、契約内容にも含める b) ■ース契約終了に伴う情報の抹消について、役務提供契約を別途締結する	●b遵守事項**3.1.1(7)(b)**「抹消する」について 「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。電磁的記録媒体に記録されている情報を抹消するための方法を、機密性の高さに応じて分けた以下二つの表において例示する。 磁気媒体及びフラッシュメモリ媒体に対して、「表**3.1.1-1**　情報の抹消方法の例」に記載の方法を用いた場合、特殊な手段を用いることによって情報（断片を含む）が読み出されるリスクが存在する。当該リスクを許容できないような**機密性の高い情報**を抹消する場合は、「表**3.1.1-2**　機密性の高い情報の抹消方法の例」に記載の方法を用いるとよい。 ただし、暗号化消去は、「表**3.1.1-2**　機密性の高い情報の抹消方法の例」に記載の方法ではあるが、情報の抹消が高速に行えることや部分的な抹消が行えること等のメリットがあるため、機密性の高さによらず、抹消するための方法として優先的に検討するとよい。 また、クラウドサービスの利用を終了する際のクラウドサービスで取り扱った**要機密情報**を廃棄する方法は暗号化消去等が考えられる。遵守事項**4.2.2(5)**「クラウドサービスを利用した情報システムの更改・廃棄時の対策」を参照のこと。 なお、職員等自らが情報を抹消することが不可能な場合は、あらかじめ抹消の手段と抹消の措置を行う者を情報システム又は課室等の組織の単位で定めて実施し実施結果の記録を残すことや情報の抹消を外部の民間事業者等へ業務委託することも考えられるが、業務委託を実施する場合は、情報が適正に抹消されたことの証拠となる記録及び証明書の提出を求める、職員等による立ち合いを行う等、委託先での履行状況を確認することが重要である。	ガイドライン「表3.1.1-1　情報の抹消方法の例」を参照 **ガイドライン 遵守事項4.2.2(5)「クラウドサービスを利用した情報システムの更改・廃棄時の対策」を参照** ※運用規定・ルールに関する要求のため対象外	対象外

【参考】情報の取り扱い_情報システムセキュリティ要件

No	章	分類	大項番	中項番	遵守事項（統一基準 第3部,第7部より）	基本的対策事項（ガイドラインより）	対策事項の解説（ガイドラインより）	具体的な対策案	スコープ可否
18	3	要機密情報	3.1.1 情報の取扱い	(7)情報の消去	(c)職員等は、**要機密情報**である書面を廃棄する場合には、復元が困難な状態にすること。	なし	●b遵守事項**3.1.1(7)(c)**「復元が困難な状態にする」について 電磁的記録の抹消と同様に、書面が不要となった場合には、シュレッダーによる細断処理、焼却、溶解等により、復元が困難な状態にする必要がある。 なお、廃棄すべき書類が大量にあるなどの理由により、外部の廃棄処理業者へ業務委託する場合には、廃棄現場への立会いや廃棄処理証明書の取得等により、書面が確実に廃棄されていることを確認するとよい。また、無人の執務室に設置されている又は設置場所及び利用場所が確定していないなどの環境で利用される情報システム、外部電磁的記録媒体等については、不要な情報を可能な限り抹消しておくことが望ましい。	※運用規定・ルールに関する要求のため対象外	対象外
19	3	要機密情報	3.2.1 情報を取り扱う区域の管理	(2)区域ごとの対策の決定	(b)区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。	＜3.2.1(2)(b)関連＞ 3.2.1(2)-1区域情報セキュリティ責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定すること。	以下は原文参照 ●b基本対策事項3.2.1(2)-1「個別の対策」について	※運用規定・ルールに関する要求のため対象外	対象外
20	3	要保全情報	3.1.1 情報の取扱い	(4)情報の利用・保存	(a)職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。	＜3.1.1(4)(a)(d)関連＞ 3.1.1(4)-1職員等は、情報の格付及び取扱制限に応じて、情報を取り扱う際は、以下を全て含む対策を講ずること。 d)電磁的記録媒体に**要保全情報**を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講ずる。	●b基本対策事項**3.1.1(4)-1 d)**「電子署名の付与を行うなど」について 改ざん防止のための措置としては、電子署名を付与することや、情報を更新する必要がある主体に対してのみ更新権限を付与すること等が考えられる。保護を行う情報の格付、取扱制限等に応じて適切な措置を講ずるとよい。 電子署名を付与した場合、電子署名を付与した者が真正であること、電子署名が付与された情報が改ざんされていないことを検証することができる。しかし、電子署名を付与するだけでは、電子署名が付与された情報がどの時点において存在していたかを検証することができない。 この検証を可能とするためにはタイムスタンプを付与する必要がある。タイムスタンプを付与することによって、タイムスタンプを付与した時点において情報が存在していたこと、また、タイムスタンプを付与した後に情報が改ざんされていないことを検証することができる。 検証できることが電子署名とタイムスタンプによって異なることを踏まえ、情報の格付及び取扱制限に応じて適切な方法を用いるとよい。 なお、電子署名やタイムスタンプにはどちらも有効期限が存在する。電子署名やタイムスタンプの有効期限が切れた後においても電磁的記録媒体に保存する要保全情報に対して改ざん防止のための措置を講ずる必要がある場合は、さらに新たなタイムスタンプを付与することによって、電子署名やタイムスタンプの有効期限後であっても検証が可能となる、長期署名の仕組みを利用するとよい。 当該仕組みを利用できない場合は、原則として「電子政府推奨暗号リスト」に記載された暗号化方式を用いた電子署名を当該情報に再度付与する方法も考えられる。しかし、この方法を用いる場合はタイムスタンプを付与しないため、電子署名が再度付与された情報がどの時点において存在していたかを検証することができないことに留意が必要である。	要保全情報として取り扱うデータには以下を例にした対策を行う ・改ざん防止のための措置（電子署名・タイムスタンプの付与など）	対象
21	3	要保全情報	3.1.1 情報の取扱い	(1)情報の取扱いに係る規定の整備	(a)職括情報セキュリティ責任者は、以下を全て含む情報の取扱いに関する運用規程を整備し、職員等へ周知すること。 (ウ)情報の格付及び取扱制限の継承、見直しに関する手続	＜3.1.1(1)(a)(ウ)関連＞ e)**機全性及び可用性**については、作成時又は複製時に適切な格付を決定する。	●b基本対策事項**3.1.1(1)-4 e)**「複製時に適切な格付を決定」について 複製された情報は、一般的には完全性１情報及び可用性１情報と考えられるが、原本を複製し、それをバックアップファイルとして保存する場合も考えられるため、**完全性及び可用性**については、適宜、複製の目的に応じて格付を決定する必要がある。	※運用規定・ルールに関する要求のため対象外	対象外
22	3	要保全情報	3.1.1 情報の取扱い	(8)情報のバックアップ	(a)職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。	＜3.1.1(8)(a)関連＞ 3.1.1(8)-1職員等は、**要保全情報又は要安定情報**である電磁的記録又は重要な設計書について、バックアップを取得すること。	●b遵守事項**3.1.1(8)(a)**「適切な方法で情報のバックアップを実施する」について 災害や情報セキュリティインシデント等の危機的事象が発生し、サーバ装置等の電磁的記録が使用不可能になった際の復旧に備えて、要保全情報や要安定情報に格付される情報等の重要な情報を外部の記録媒体へバックアップすることを求めている。以下の例を参考に、情報のバックアップ方法について考慮するとよい。 a)想定する危機的事象（地震、津波、火災、高出力電磁波、感染症、情報セキュリティインシデント等） a)バックアップの対象（対象とするシステム、データ、ソフトウェアその他） a)バックアップの範囲（フルバックアップ、差分バックアップ等） a)バックアップを保存する電磁的記録媒体等の種類 a)バックアップの周期、頻度、世代管理の方法 a)使用するバックアップツール a)バックアップデータの秘匿性確保、改ざん防止の方法 バックアップの周期を短くすることで、危機的事象発生時点に近い状態に復旧できる可能性が高くなるため、バックアップの周期は可能な限り短くすることが望ましい。 しかし、サイバー攻撃を検知するまでに長期間を要する不正プログラムの存在が確認されており、バックアップの周期が短く、かつ、保存しているバックアップの世代が少ない場合は、バックアップしている全ての世代に不正プログラムが混入してしまう可能性がある。そのため、過去の事例等から不正プログラムの潜伏期間を想定し、情報の格付、取扱制限等を踏まえた上で、バックアップの周期や世代管理の方法等を定めるとよい。 また、復旧に用いるべきバックアップデータを事前に特定しておくことが重要である。そのため、バックアップデータに対して最新の定義ファイルが適用された状態の不正プログラム対策ソフトウェア等によるスキャンを行うとよい。 さらに、継続的に運用管理していく中においてバックアップ用の媒体が適切に挿入されていない等の運用ミス[illegible]	要保全情報又は要安定情報に対するデータには以下を例にした対策を行う ・適切な方法で情報のバックアップを実施 ・バックアップの周期は可能な限り短くすることが望ましい ・バックアップデータに対して最新の定義ファイルが適用された状態の不正プログラム対策ソフトウェア等によるスキャンを行うことが望ましい	対象
23	3	要保全情報	3.1.1 情報の取扱い	(8)情報のバックアップ	(b)職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。	＜3.1.1(8)(b)関連＞ 3.1.1(8)-2職員等は、**要保全情報若しくは要安定情報**である電磁的記録のバックアップ又は重要な設計書のバックアップについて、災害や情報セキュリティインシデント等の危機的事象により生ずる業務上の支障を考慮し、適切な保管場所を選定すること。**要保全情報又は要安定情報**である電磁的記録のバックアップについて、危機的事象として情報システムや情報が破壊される情報セキュリティインシデントを想定する場合は、必要に応じて、以下を例とする情報システムや情報とバックアップが同時に破壊されない保管場所を選定すること。 a)職バックアップ取得元の情報システムが接続するネットワークから物理的に隔離された保管場所 b)職バックアップ取得元の情報システムが接続するネットワークから論理的に隔離された保管場所	以下は原文参照 ●職守事項3.1.1(8)(b)「格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め」について ●職本対策事項3.1.1(8)-2「重要な設計書」について ●職本対策事項3.1.1(8)-2「適切な保管場所を選定する」について ●職本対策事項3.1.1(8)-2「情報システムや情報が破壊される情報セキュリティインシデント」について ●職本対策事項3.1.1(8)-2「必要に応じて」について ●職本対策事項3.1.1(8)-2「情報システムや情報とバックアップが同時に破壊されない保管場所を選定する」について ●職本対策事項3.1.1(8)-2 a)「物理的に隔離された保管場所」について ●職本対策事項3.1.1(8)-2 b)「論理的に隔離された保管場所」について	※運用規定・ルールに関する要求のため対象外	対象外
24	3	要安定情報	3.1.1 情報の取扱い	(1)情報の取扱いに係る規定の整備	(a)職括情報セキュリティ責任者は、以下を全て含む情報の取扱いに関する運用規程を整備し、職員等へ周知すること。 (ウ)情報の格付及び取扱制限の継承、見直しに関する手続	＜3.1.1(1)(a)(ウ)関連＞ e)**機全性及び可用性**については、作成時又は複製時に適切な格付を決定する。	●b基本対策事項**3.1.1(1)-4 e)**「複製時に適切な格付を決定」について 複製された情報は、一般的には完全性１情報及び可用性１情報と考えられるが、原本を複製し、それをバックアップファイルとして保存する場合も考えられるため、**完全性及び可用性**については、適宜、複製の目的に応じて格付を決定する必要がある。	※運用規定・ルールに関する要求のため対象外	対象外

【参考】情報の取り扱い_情報システムセキュリティ要件

No	章	分類	大項番	中項番	遵守事項（統一基準 第3部,第7部より）	基本的対策事項（ガイドラインより）	対策事項の解説（ガイドラインより）	具体的な対策案	スコープ可否
25	3	要安定情報	3.1.1 ■報の取扱い	(8)■報のバックアップ	(a)■員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。	＜3.1.1(8)(a)関連＞ 3.1.1(8)-1■員等は、**要保全情報又は要安定情報**である電磁的記録又は重要な設計書について、バックアップを取得すること。	●b遵守事項3.1.1(8)(a)「適切な方法で情報のバックアップを実施する」について 災害や情報セキュリティインシデント等の危機的事象が発生し、サーバ装置等の電磁的記録が使用不可能になった際の復旧に備えて、要保全情報や要安定情報に格付される情報等の重要な情報を外部の記録媒体へバックアップすることを求めている。以下の例を参考に、情報のバックアップ方法について考慮するとよい。 a)想定する危機的事象（地震、津波、火災、高出力電磁波、感染症、情報セキュリティインシデント等） a)バックアップの対象（対象とするシステム、データ、ソフトウェアその他） a)バックアップの範囲（フルバックアップ、差分バックアップ等） a)バックアップを保存する電磁的記録媒体等の種類 a)バックアップの周期、頻度、世代管理の方法 a)使用するバックアップツール a)バックアップデータの秘匿性確保、改ざん防止の方法 バックアップの周期を短くすることで、危機的事象発生時点に近い状態に復旧できる可能性が高くなるため、バックアップの周期は可能な限り短くすることが望ましい。 しかし、サイバー攻撃を検知するまでに長期間を要する不正プログラムの存在が確認されており、バックアップの周期が短く、かつ、保存しているバックアップの世代が少ない場合は、バックアップしている全ての世代に不正プログラムが混入してしまう可能性がある。そのため、過去の事例等から不正プログラムの潜伏期間を想定し、情報の格付、取扱制限等を踏まえた上で、バックアップの周期や世代管理の方法等を定めるとよい。 また、復旧に用いるべきバックアップデータを事前に特定しておくことが重要である。そのため、バックアップデータに対して最新の定義ファイルが適用された状態の不正プログラム対策ソフトウェア等によるスキャンを行うとよい。 さらに、継続的に運用管理していく中においてバックアップ用の媒体が適切に挿入されていない等の運用ミスが発生するケースや、先般が延伸することでデータ量が増大し規定時間内にバックアップが取得できないケース	要保全情報又は要安定情報に対するデータには以下を例にした対策を行う ・適切な方法で情報のバックアップを実施 ・バックアップの周期は可能な限り短くすることが望ましい ・バックアップデータに対して最新の定義ファイルが適用された状態の不正プログラム対策ソフトウェア等によるスキャンを行うことが望ましい	対象
26	3	要安定情報	3.1.1 ■報の取扱い	(8)■報のバックアップ	(b)■員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。	＜3.1.1(8)(b)関連＞ 3.1.1(8)-2■員等は、**要保全情報若しくは要安定情報**である電磁的記録のバックアップ又は重要な設計書のバックアップについて、災害や情報セキュリティインシデント等の危機的事象により生ずる業務上の支障を考慮し、適切な保管場所を選定すること。**要保全情報又は要安定情報**である電磁的記録のバックアップについて、危機的事象として情報システムや情報が破壊される情報セキュリティインシデントを想定する場合は、必要に応じて、以下を例とする情報システムや情報とバックアップが同時に破壊されない保管場所を選定すること。 a)■ックアップ取得元の情報システムが接続するネットワークから物理的に隔離された保管場所 b)■ックアップ取得元の情報システムが接続するネットワークから論理的に隔離された保管場所	以下は原文参照 ●■守事項3.1.1(8)(b)「格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め」について ●■本対策事項3.1.1(8)-2「重要な設計書」について ●■本対策事項3.1.1(8)-2「適切な保管場所を選定する」について ●■本対策事項3.1.1(8)-2「情報システムや情報が破壊される情報セキュリティインシデント」について ●■本対策事項3.1.1(8)-2「必要に応じて」について ●■本対策事項3.1.1(8)-2「情報システムや情報とバックアップが同時に破壊されない保管場所を選定する」について ●■本対策事項3.1.1(8)-2 a)「物理的に隔離された保管場所」について ●■本対策事項3.1.1(8)-2 b)「論理的に隔離された保管場所」について	※運用規定・ルールに関する要求のため対象外	対象外
27	3	要安定情報	3.2.1 ■報を取り扱う区域の管理	(3)■管理対策区域における対策の実施	(b)■域情報セキュリティ責任者は、災害から**要安定情報**を取り扱う情報システムを保護するために物理的な対策を講ずること。	なし	●b遵守事項3.2.1(3)(b)「物理的な対策」について 地震、火災、停電等の災害から情報システムを保護するための対策を指す。 具体的な対策として、例えば、サーバラックの利用のほか、以下の設備等の設置が挙げられる。 a)ハロゲン化物消火設備 a)■停電電源装置 a)■家発電装置 a)■調設備 a)■震又は免震設備 これらの対策については、必ずしも区域情報セキュリティ責任者単独で実施できるものではないが、例えば、情報システムに関係する対策であれば情報システムセキュリティ責任者、施設管理に関係する対策であれば施設管理を行う部門の関係者と調整することが求められる。 また、情報システムへの対策として、作業する者が災害によりサーバ装置等に近づくことができない場合に、作業する者の安全性を確保した上で遠隔地からサーバ装置等の電源を遮断できるようにする機能を設けておくことも考えられる。	※運用規定・ルールに関する要求のため対象外	対象外
28	7	要保護情報	7.1.4 ■グの取得・管理	(1)■グの取得・管理	(b)■報システムセキュリティ責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、**要保護情報**の観点でのログ情報の取扱方法等について定め、適切にログを管理すること。	＜7.1.4(1)(b)関連＞ 7.1.4(1)-2■報システムセキュリティ責任者は、所管する情報システムの特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め、管理すること。 a)■象の主体（人物又は機器等）を示す識別コード b)■別コードの発行等の管理記録 c)■報システムの操作記録 d)■象の種類 e)■象の対象 f)■確な日付及び時刻 g)■みられたアクセスに関わる情報 h)■子メールのヘッダ情報及び送信内容 i)■信パケットの内容 j)■作する者、監視する者、保守する者等への通知の内容	●b遵守事項7.1.4(1)(b)「ログを取得する目的」について 情報システムにおけるログは、情報セキュリティインシデント発生時や情報セキュリティインシデントの予兆となる現象を特定する際に重要な役割を果たすことから、可能な限り保存し適切に保護、管理することが望ましい。 取得するログについては、情報システムの特性（取り扱われる情報、接続されるネットワーク、設置環境、利用者等）に応じ、当該情報システムでどのような事象を検知すべきかを目的として設定した上で、取得すべきログ情報やその保存期間等を検討することが望ましい。 例えば、JPCERT/CC「高度サイバー攻撃への対処におけるログの活用と分析方法」の「3. ログの採取と取扱」や、総務省「サイバー攻撃（標的型攻撃）対策防御モデルの解説」の「6.2. 検知」などを参考に、機器等における必要なログを見定めて取得し、分析するようにする。なお、機器等によっては、ログを保存できる物理的な容量が少なく長期間の保存ができない場合があるため、そのような機器等においてはログを一元的に管理するサーバ装置等に集約するなどし、ログを必要な期間取得しておくことが望ましい。 ●b遵守事項7.1.4(1)(b)「保存期間」について 保存期間については、情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは１年間以上保存することが望ましい。 なお、ログの長期保存にはコストがかかるため、費用を抑える観点から、直近のログはすぐに調査可能なハードディスク等のオンラインの電磁的記録媒体に保存し、それ以降はテープや光ディスク等の長期保存に適した外部電磁的記録媒体に保存する方法も考えられる。オンラインの電磁的記録媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する。	要保護情報に対するデータには以下を例にした対策を行う ・適切な目的、管理方法を定めてログを管理する。ログ取得項目は以下を例とする。 a)■象の主体（人物又は機器等）を示す識別コード b)■別コードの発行等の管理記録 c)■報システムの操作記録 d)■象の種類 e)■象の対象 f)■確な日付及び時刻 g)■みられたアクセスに関わる情報 h)■子メールのヘッダ情報及び送信内容 i)■信パケットの内容 j)■作する者、監視する者、保守する者等への通知の内容	対象
29	7	要機密情報	7.1.1 ■体認証機能	(1)■体認証機能の導入	(c)■報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証**情報の漏えい等**による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。	＜7.1.1(1)(c)関連＞ 7.1.1(1)-4■報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正なアクセスを防止するため、以下を全て含む措置を講ずること。 a)■則として、機器等において初期値として設定されている識別コードを使用しない。 b)■要な識別コードを無効にする。	●b遵守事項7.1.1(1)(c)「主体認証情報の漏えい等による不正行為を防止するための措置」について 主体認証情報の漏えい等が発生すると、悪意ある第三者によってなりすましによる不正アクセスをされ、情報の窃取や踏み台にされるなどのリスクが発生する。主体認証情報の漏えいしたアカウントを悪用されると、情報セキュリティ対策を無効にされることや、情報を窃取するために使用する不正プログラム等を導入される可能性がある。したがって、誰もが知っている機器等において初期値として設定されている識別コードは原則として利用しない措置を講ずることが重要である。また、開発時に使用した識別コードや一時的に利用したテスト用の識別コード等を運用時においても有効にしていた場合、そのような識別コードが何らかの手段によって攻撃者に渡り、悪用される可能性も高くなる。したがって、不要となった識別コードは無効にすることが有効である。 以下は原文参照 ●b遵守事項7.1.1(1)(c)「不正な主体認証の試行に対抗するための措置」について	・主体認証情報の漏えい等による不正なアクセスを防止するため、以下を全て含む措置を講ずること。 a)■則として、機器等において初期値として設定されている識別コードを使用しない。 b)■要な識別コードを無効にする。	対象

【参考】情報の取り扱い_情報システムセキュリティ要件

No	章	分類	大項番	中項番	遵守事項（統一基準 第3部,第7部より）	基本的対策事項（ガイドラインより）	対策事項の解説（ガイドラインより）	具体的な対策案	スコープ可否
30	7	要機密情報	7.1.2□クセス制御機能	(1)□クセス制御機能の導入	(a)■報システムセキュリティ責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。	<7.1.2(1)(a)関連> 7.1.2(1)-1■報システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定めること。また、情報システムの分類に基づき、以下の対策を実施すること。 【基本セキュリティ対策】以下を例とするアクセス制御機能の要件を定めること。 a)■用時間や利用時間帯によるアクセス制御 b)■■一主体による複数アクセスの制限 c)■アドレスによる端末の制限 d)■ットワークセグメントの分割によるアクセス制御 e)■ァイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御 【追加セキュリティ対策】基本セキュリティ対策の実施に加えて、以下を例とするアクセス制御機能を用いることを検討すること。 f)■証・認可の統合管理基盤を用いたアクセス制御 g)□クセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御	●B基本対策事項7.1.2(1)-1「主体の属性、アクセス対象の属性に基づくアクセス制御」について 具体的な手法としては、端末や共有フォルダ上のファイルやフォルダ（ディレクトリ）に対する許可属性のリストであるアクセス制御リスト（ACL： Access Control List）が挙げられる。ACLでは例えば、アクセス対象の所有者／所有者の属するグループ／全利用者といったアクセス主体に対して、読み取り／書き込み／実行の権限を設定する。 ただし、一般的な情報システムでは、利用者が適切なアクセス制御の設定を行っても、システムの管理者は全てのファイルやフォルダへアクセス可能である。実際に、運用保守の担当者が、管理者権限相当のアクセス権限を行使して、機密性の高い情報を不正に閲覧するといった事案も確認されている。そのため、アクセス対象が**要機密情報等**の場合は、アクセス制御機能のみに頼らず、アクセス権限の無い者に閲覧等されないよう、アクセス制限の対象に対して暗号化等の措置を考慮することが求められる。 以下は原文参照 ●B基本対策事項7.1.2(1)-1 d）「ネットワークセグメントの分割によるアクセス制御」について ●B基本対策事項7.1.2(1)-1 e）「ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御」について ●B基本対策事項7.1.2(1)-1 f）「認証・認可の統合管理基盤」について ●B基本対策事項7.1.2(1)-1 g）「動的なアクセス制御」について ●B基本対策事項7.1.2(1)-2「アクセス制御の要件の定期的な確認による見直し」について	・アクセス制御の要件を定めて対策すること。要件例は以下の通り。 a)■用時間や利用時間帯によるアクセス制御 b)■■一主体による複数アクセスの制限 c)■アドレスによる端末の制限 d)■ットワークセグメントの分割によるアクセス制御 e)■ァイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御 【追加セキュリティ対策】基本セキュリティ対策の実施に加えて、以下を例とするアクセス制御機能を用いることを検討すること。 f)■証・認可の統合管理基盤を用いたアクセス制御 g)□クセスの要求ごとに、主体等の状況を継続的に認証し認可する仕組みを実現する機能の一部である動的なアクセス制御 ・アクセス制御の対象に対して暗号化等の措置を考慮すること	対象
31	7	要機密情報	7.1.5■号・電子署名	(1)■号化機能・電子署名機能の導入	(a)■報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の全ての措置を講ずること。 (ア)**要機密情報**を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。	<7.1.5(1)(a)関連> 7.1.5(1)-1■報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。 a)■報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。 b)■数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択することが可能な構成とする。 c)■択したアルゴリズム及び鍵長がソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。 d)■号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。 e)■微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。	以下は原文参照 ●■本対策事項7.1.5(1)-1 a)「暗号モジュールを交換」について ●■本対策事項7.1.5(1)-1 b)「複数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択」について ●■本対策事項7.1.5(1)-1 c)「「暗号モジュール試験及び認証制度」に基づく認証」について ●■本対策事項7.1.5(1)-1 d)「耐タンパ性」について ●■本対策事項7.1.5(1)-1 e)「安全性に実績のあるプロトコル」について ●■本対策事項7.1.5(1)-1 e)「長期的な秘匿性」について	・暗号化の要件を定めて対策すること。要件例は以下の通り。 a)■報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。 b)■数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択することが可能な構成とする。 c)■択したアルゴリズム及び鍵長がソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。 d)■号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。 e)■微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。	対象
32	7	要機密情報	7.2.1□フトウェアに関する脆弱性対策	(1)□フトウェアに関する脆弱性対策の実施	(d)■報システムセキュリティ責任者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。	<7.2.1(1)(d)関連> 7.2.1(1)-8■報システムセキュリティ責任者は、ネットワーク境界にある通信回線装置や認証サーバ、**要機密情報**を保有するサーバ等のサイバーセキュリティリスクが高い機器等に対しては、原則、セキュリティパッチの適用又はソフトウェアのバージョンアップ等の措置を講ずること。リスク評価結果を踏まえ措置を講じないと判断した場合には、リスク評価結果の記録を残すこと。	●B基本対策事項7.2.1(1)-8「サイバーセキュリティリスクが高い機器等」について 例えば、NAS（Network Attached Storage）において、認証情報を不正に入手される可能性がある脆弱性が公表された際には情報漏えい等のリスクが高まることが考えられる。	・以下のようなセキュリティリスクが高い機器等については原則、セキュリティパッチの適用又はソフトウェアのバージョンアップ等の措置を講ずる ・ネットワーク境界にある通信回線装置 ・認証サーバ ・要機密情報を保有するサーバ等	対象
33	7	要保全情報	7.1.5■号・電子署名	(1)■号化機能・電子署名機能の導入	(a)■報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の全ての措置を講ずること。 (イ)**要保全情報**を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。	<7.1.5(1)(a)関連> 7.1.5(1)-1■報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。 a)■報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。 b)■数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択することが可能な構成とする。 c)■択したアルゴリズム及び鍵長がソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。 d)■号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。 e)■微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。	以下は原文参照 ●■本対策事項7.1.5(1)-1 a)「暗号モジュールを交換」について ●■本対策事項7.1.5(1)-1 b)「複数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択」について ●■本対策事項7.1.5(1)-1 c)「「暗号モジュール試験及び認証制度」に基づく認証」について ●■本対策事項7.1.5(1)-1 d)「耐タンパ性」について ●■本対策事項7.1.5(1)-1 e)「安全性に実績のあるプロトコル」について ●■本対策事項7.1.5(1)-1 e)「長期的な秘匿性」について	・暗号化の要件を定めて対策すること。要件例は以下の通り。 a)■報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。 b)■数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択することが可能な構成とする。 c)■択したアルゴリズム及び鍵長がソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。 d)■号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。 e)■微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。	対象
34	7	要安定情報	7.2.3■ービス不能攻撃対策	(1)■ービス不能攻撃対策の実施	(a)■報システムセキュリティ責任者は、**要安定情報**を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下本条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。	<7.2.3(1)(a)関連> 7.2.3(1)-1■報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置について、サービス不能攻撃に対抗するための以下の機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。 a)□ケットフィルタリング機能 b)□way handshake時のタイムアウトの短縮 c)■種Flood攻撃への防御 d)□プリケーションゲートウェイ機能 7.2.3(1)-2■報システムセキュリティ責任者は、以下を例とするサービス不能攻撃への対策を実施すること。 【基本セキュリティ対策】以下を例とする対策を実施すること。 a)■ービス不能攻撃の影響を排除又は低減するための専用の対策装置やサービスの導入 b)■ーバ装置、端末及び通信回線装置及び通信回線の冗長化 【追加セキュリティ対策】基本セキュリティ対策に加え、以下を例とする対策を検討すること。 c)□ンターネットに接続している通信回線の提供元となる事業者やクラウドサービス提供者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策 d)□ンテンツデリバリーネットワーク（CDN）サービスの利用	以下は原文参照 ●■守事項7.2.3(1)(a)「サービス不能攻撃」について ●■本対策事項7.2.3(1)-2 a)□対策装置」について ●■本対策事項7.2.3(1)-2 b)「冗長化」について ●■本対策事項7.2.3(1)-2 c)「インターネットに接続している通信回線」について ●■本対策事項7.2.3(1)-2 c)「サービス不能攻撃に係る通信の遮断等」について ●■本対策事項7.2.3(1)-2 d)「コンテンツデリバリーネットワーク（CDN）サービス」について	・サーバ装置、端末及び通信回線装置について、サービス不能攻撃に対抗するための以下の機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。 a)□ケットフィルタリング機能 b)□way handshake時のタイムアウトの短縮 c)■種Flood攻撃への防御 d)□プリケーションゲートウェイ機能 また、以下を例とするサービス不能攻撃への対策を実施すること。 a)■ービス不能攻撃の影響を排除又は低減するための専用の対策装置やサービスの導入 b)■ーバ装置、端末及び通信回線装置及び通信回線の冗長化 c)□ンターネットに接続している通信回線の提供元となる事業者やクラウドサービス提供者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策 d)□ンテンツデリバリーネットワーク（CDN）サービスの利用	対象
35	7	要安定情報	7.2.3■ービス不能攻撃対策	(1)■ービス不能攻撃対策の実施	(b)■報システムセキュリティ責任者は、**要安定情報**を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。	<7.2.3(1)(b)関連> 7.2.3(1)-3■報システムセキュリティ責任者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報システムを構築すること。 7.2.3(1)-4■報システムセキュリティ責任者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段の確保について検討すること。	●B基本対策事項7.2.3(1)-4「攻撃への対処を効率的に実施できる手段」について 対処例としては、サービス提供に利用している通信回線がサービス不能攻撃により過負荷状態に陥った場合においても、サービス不能攻撃を受けているサーバ装置、通信回線装置及びそれらを保護するための装置を操作できる手段を確保することが挙げられる。具体的には、管理者が当該装置を操作するためのサーバ装置、端末及び通信回線を、サービス提供に利用しているものとは別に用意することが挙げられる。 また、サービス不能攻撃に伴い、機関等の自己管理ウェブサイトの閲覧障害が発生した場合においても、緊急性・重要度が高い情報が長時間閲覧できなくなることは極力回避すべきである。これに鑑み、災害情報等の緊急性が高く、国民の生命や財産に著しく影響を及ぼし得るような重要情報については、広報担当とも協力するなどして、サービス不能攻撃を受けた際にも発信を可能とするよう、閲覧障害時の告知ページに最低限のテキストデータを掲載するなどの必要な措置を考慮するとよい。	・サービス不能攻撃を受けた場合の影響を最小とする手段を備えること 例：外部ネットワークからの遮断、通信回線の通信量制限、冗長構成等	対象

【参考】情報の取り扱い_情報システムセキュリティ要件

No	章	分類	大項番	中項番	遵守事項（統一基準 第3部,第7部より）	基本的対策事項（ガイドラインより）	対策事項の解説（ガイドラインより）	具体的な対策案	スコープ可否
36	7	**要安定情報**	7.2.3 関サービス不能攻撃対策	(1)関サービス不能攻撃対策の実施	(c)関報システムセキュリティ責任者は、**要安定情報**を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。	<7.2.3(1)(c)関連> 7.2.3(1)-5関報システムセキュリティ責任者は、特定した監視対象について、監視方針及び監視方法を定めること。 7.2.3(1)-6関報システムセキュリティ責任者は、監視対象の監視記録の保存期間を定め、監視記録を保存すること。 7.2.3(1)-7関報システムセキュリティ責任者は、監視対象の平常時の負荷の状況を把握し、監視においてこれを著しく逸脱したと判断する目安を定めること。 7.2.3(1)-8関報システムセキュリティ責任者は、監視において、前項で定めた目安を超える負荷の状況が確認された場合は、サービス不能攻撃の可能性が排除される場合を除き、速やかに遵守事項2.2.4(1)(a)で定める報告手順に基づきCSIRTに報告すること。 7.2.3(1)-9【追加セキュリティ対策】情報システムセキュリティ責任者は、脅威動向等の脅威情報を収集し、サービス不能攻撃を受ける可能性が予見される場合は、必要に応じて、CSIRT等の関係者に通知すること。	●B基本対策事項**7.2.3(1)-5**「監視方針及び監視方法」について インターネットからアクセスされるサーバ装置や、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるものを優先的に監視する必要がある。 「監視方針」については、監視対象の特性を踏まえて、監視する時間を定め、監視により認知した異常の程度の段階に応じた対応の優先度や情報共有範囲、対応時間帯（例えば24時間365日対応、平日の日中のみ対応など）等を定めることが考えられる。 「監視方法」については、サービス不能攻撃を受けることに関する監視には、稼動中か否かの状態把握や、システムの構成要素に対する負荷の定量的な把握(CPU使用率、プロセス数、ディスクI/O量、ネットワークトラフィック量等)がある。監視方法は多種多様であるため、当該情報システムの構成等の特性に応じて適切な方法を選択する必要がある。 ●B基本対策事項**7.2.3(1)-6**「監視対象の監視記録の保存期間を定め、監視記録を保存」について サーバ装置、端末、通信回線装置及び通信回線を監視している場合、監視対象の状態は一定ではなく変動することが一般的である。そのため、時間変動、曜日変動、週変動、月変動、季節変動等を監視対象の変動を把握するという目的に照らした上で記録の保存期間を定め、一定期間保存する。 ●B基本対策事項**7.2.3(1)-8**「サービス不能攻撃の可能性が排除される場合を除き」について サービス不能攻撃の可能性が排除される場合として、情報システムのメンテナンスのために一時的に一部機能等を制限した場合や、一時的にアクセスが集中することが考えられるコンテンツをウェブサイトに掲載した場合などが考えられる。 ●B基本対策事項**7.2.3(1)-9**「脅威動向等の脅威情報を収集」について 脅威動向等の脅威情報の収集については、内閣官房内閣サイバーセキュリティセンター等からの注意喚起等のほか、セキュリティベンダが提供している脅威情報の提供サービスを活用することも考えられる。	・サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること	対象

【参考】情報の格付け定義

種別	区分	情報の取り扱い定義		分類基準（原文）	分類基準（要約）	ドローン航路システムにおける該当項目（例）	評価内容補足	財務会計システムにおける評価例（主に業務影響を評価）
機密性	3	要機密情報	・要機密情報 ・要保全情報 ・要安定情報 いずれか一つでも該当する場合、「要保護情報」として取り扱う	国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドラインに定める秘密文書としての取扱いを要する情報 独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報	**取り扱う内容が秘密文書レベル（※1）となる情報** **※1：漏洩により国の安全や国益が侵害される内容**	なし	漏洩した際に、国の安全や国益が侵害される機密性の高い情報は取り扱わないため	なし
	2			国の行政機関における業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成11年法律第42号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報 独立行政法人における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成13年法律第140号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報。また、指定法人のうち、独法等情報公開法の別表第一に掲げられる法人（以下「別表指定法人」という。）についても同様とする。 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報	**取り扱う内容が不開示情報レベル（※2）となる情報** **※2：以下参照** **・個人情報、特定個人情報** **・法人情報の内、漏洩すると利益侵害となりうる情報** **・公共の安全と秩序の維持に支障がでる情報** **・漏洩すると事業の遂行に支障がでる情報**	・事業者メールアドレス※限定的な影響（PIA資料参照） ・ログインID/パスワード（乗っ取り被害の可能性）	・事業者メールアドレスは限定的ではあるもののプライバシーを侵害する可能性があることが外部機関の調査によって確認されているため機密性2とする。 ・ログインID/パスワードは外部漏洩時にアカウント乗っ取りなどサイバー攻撃被害の可能性があるため機密性2とする。	・ユーザの個人情報（氏名、住所、口座番号、マイナンバー）：財務会計システムに保有されている個人情報は個人情報保護法により厳密な管理が定められている。漏洩した場合、個人に対する重大な犯罪被害をもたらす可能性が高い。また企業に対する致命的な社会的な信用毀損は避けられないため、高い機密性・完全性が求められる（評価によっては機密性3にもなりうる）。 ・仕訳データ（伝票番号、勘定科目、金額、税区分）：非公開情報となり漏洩時に事業被害、社会的な信用棄損の可能性がある。 ・売掛・買掛（取引先、請求書番号、支払期限）：非公開情報となり漏洩時に事業被害、社会的な信用棄損の可能性がある。 ・ログインID/パスワード：漏洩した場合、アカウントの乗っ取りや情報搾取など被害にある可能性がある
	1			国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 独立行政法人又は別表指定法人における業務で取り扱う情報のうち、独法等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報	**機密性2、3以外の情報**	・離着陸場・機体管理：②機体情報（機体ID, 機体名, 製造メーカー, 製造番号, 機体の種類etc…）	機体情報は個人情報等を含まない一般的な情報となるため機密性は低い	・サービスプレスリリース情報、サービスに関するお知らせ：公開情報のため機密性要件は低い ・投資家向け決算資料：すでに公開している情報の場合、機密性要件は低い（公開前の場合は評価値が上がる） ・市場取引データ（株価、為替）：ほとんどの市場データは公開情報であるため機密性は低い
完全性	2	要保全情報		業務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は業務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	**改ざんされると業務遂行に支障がでる情報**	・航路予約情報（飛行エリア、航路、日時、離着陸場etc…）	情報が改ざんされた場合、誤った航路飛行により事故が発生する可能性があるため完全性は高い	・ユーザの個人情報（氏名、住所、口座番号、マイナンバー）：情報が改ざんされた場合、データの不整合や認識齟齬による多数の被害が想定される。 ・仕訳データ（伝票番号、勘定科目、金額、税区分）：改ざんされた場合、データ不整合により業務が停止する ・売掛・買掛（取引先、請求書番号、支払期限）：改ざんされた場合、データ不整合により業務が停止する ・決算書・財務報告データ：改ざんされた事実に気づかない場合、実際の売り上げと異なる不正会計として処罰対象になる可能性がある
	1			完全性２情報以外の情報（書面を除く。）	**完全性2以外の情報**	・安全管理：ヒヤリハット情報 ・外部データ（地図情報,風速・天候情報,気象情報,第三者立入監視情報,飛行禁止エリア情報etc…）	ヒヤリハット情報は参考情報となり改ざん時にシステムへの被害は発生しない 外部システムから随時参照データとなる（想定）ためドローンシステムで完全性は担保対象外	・統計情報、経営状況分析などの分析データ：分析結果として出力されるデータのため、データの完全性が損なわれても業務継続への影響は少ない。
可用性	2	要安定情報		業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	**利用不可になると業務遂行に支障がでる情報**	・外部データ（地図情報,風速・天候情報,気象情報,第三者立入監視情報,飛行禁止エリア情報etc…）	利用できない場合、該当外部データを参照する業務すべてに影響が発生するため高い可用性が必要	・ユーザの個人情報（氏名、住所、口座番号、マイナンバー）：一時的に利用できなくても即業務停止にはつながらないものの、業務継続のためには一定以上の可用性が必要となる ・金融取引データ（入出金履歴、決済情報）：金融機関との取引はリアルタイムにデータ処理が行われるため高い可用性が必要。停止時の業務影響が大きい。
	1			可用性２情報以外の情報（書面を除く。）	**可用性1以外の情報**	・航路予約情報（飛行エリア、航路、日時、離着陸場etc…） ・航路画定：航路対応機種情報 ・履歴データ	フライト中は情報にアクセスしないため可用性要件は低い ドローンの航路対応機種情報は航路画定時に参照するが常に参照する必要が低いため可用性要件は低い 履歴データは常に参照する必要が低いため可用性は低い	・監査ログ：システムのセキュリティを担保する役割となるが、業務継続に必須となるデータではないため ・アプリケーション、サーバログ：システムの稼働状況を確認する役割となるが、業務継続に必須となるデータではないため