附属書3

ドローン航路セキュリティ対策の手引き

（案）

Annex-3
security measures guide for UAS Lines services

2026 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

本附属書は、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「デジタルライフライン整備事業／ドローン航路」において作成されたものです。

改定履歴

Edition No.	変更頁	変更内容	発行日
1.0（案）	-	初版発行	2026 年 3 月 31 日

目 次

1. ドローン航路セキュリティ対策の概要

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、ドローン航路政策を推進している。ドローン航路を利用することにより、運航事業者は従来個別に実施していた関係者との調整に係るコスト負担が軽減されることが期待される。この時、個別の事業者が実施しているドローン運航に係る諸手続きや業務がドローン航路システムを通じて、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、国土交通省をはじめとする重要インフラ所管省庁やドローン航路システム間との連携やデータの共有が求められるため、安全保障面や事業継続面等での適切なセキュリティ対策を講じる必要がある。このような高度にネットワーク化された環境に対する脅威は、より複雑化するとともに増大するため、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セキュリティ基準に準拠した対策が重要となる。

昨今のセキュリティ事案を見ると、1 社が受けた被害がサプライチェーンにも波及する事例が多々発生しており、サプライチェーンマネジメントでアプローチする必要性が広く認識されるようになっている。米国では、NIST[1] が 2014 年 2 月に策定した、重要インフラに対するサイバーセキュリティ対策フレームワーク（Cybersecurity Framework）について、2018 年 4 月の改訂により、サプライチェーンのリスク管理（Supply Chain Risk Management）を行うことが追加され、サプライチェーン全体で対策を実施することや、必要に応じて監査を行うことが要求されている。このような世界的な動きを受け、我が国でも、サイバーセキュリティ基本法に基づき、経済産業省が、2019 年に「サイバー・フィジカル・セキュリティ対策フレームワーク（Version 1.0）」[2]（以下「CPSF」という。）を策定し公開した。

本書では、経済産業省で策定された CPSF を指針とし、この基準を踏まえたドローン航路のセキュリティ対策検討のプロセスや実施例を提供し、ドローン航路運営者が構築/運用するシステム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。

なお、実施例で使用している分析用のテンプレートや判断基準については、独立行政法人情報処理推進機構が公開している「制御システムのセキュリティリスク分析ガイド 第 2 版」[3] を引用し、使用した。

1-2 本書の位置づけ

本書は、「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」の附属書として、ドローン航路運営者がドローン航路の構築/運用/廃止まで、ライフサイクルを通して必要となるセキュリティ対策検討の手引書としての適用を想定して纏めたものである。「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」において示されるセキュリティ対策の基本方針を踏まえ、ドローン航路運営者が自らの事業環境に即したセキュリティ対策を検討・整理するための手引書である。

---

[1] National Institute of Standards and Technology（米国国立標準技術研究所）

[2] https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html 参照。

[3] https://www.ipa.go.jp/security/controlsystem/riskanalysis.html 参照。

本書に記載する分析手法、判断基準、実施例は一律の実装を求めるものではなく、具体的な必須要件は、ドローン航路登録制度における適合性評価要件および関係法令等に従うものとする。

内容は、あくまで、一般的なシステム環境を含む事業環境を想定してセキュリティリスク分析を行った手引書の位置づけのドキュメントであり、本書を参照するドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿った検討が必要であるとともに、検討結果は、自己の責任範囲であり、当然実施すべきセキュリティ対策は、自己判断の範囲で対応する必要がある。このため、セキュリティリスク分析は、情報処理安全確保士[4] による実施、または情報処理安全確保士による分析結果の確認が望ましい。

また、ドローン航路運営者は、一通りのセキュリティリスク分析を一度実施して終わりではなく、分析結果を活用してどこにセキュリティリスクがあるかを把握し、システム環境・事業環境・取り巻く環境等の変化も考慮し、誰が、どのリスクを、いつまでに対策するかを管理するための、セキュリティリスクマネジメントを確立することが必要である。

1-3 適用範囲

本ガイドラインはドローン航路サービスの提供を検討している自治体や民間事業者を対象とし、ドローン航路の構築/運用/廃止まで、事業遂行に必要なセキュリティ対策検討の手引書として適用する。

[4] https://www.ipa.go.jp/jinzai/riss/index.html 参照。

2. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要

ここでは、CPSF の概要について説明する。詳細は、脚注 2 の「サイバー・フィジカル・セキュリティ対策フレームワーク」の最新版を参照すること。

2-1 CPSF の基本的な考え方

あらゆるものがつながる IoT、データがインテリジェンスを生み出す AI などによって実現される「Society5.0」（人間中心の社会）、「Connected Industries」では、製品・サービスを生み出す工程（サプライチェーン）も上流から下流へとつながる従来の定型的・直線的なものとは異なり、多様なつながりによる非定型の形態を取ることになる。

CPSF では、このような「Society5.0」型のサプライチェーンをこれまでのサプライチェーンとは区別して認識するため、価値創造過程（バリュークリエイションプロセス）と定義し、「Society5.0」、「Connected Industries」によって拡張したサプライチェーンの概念に求められるセキュリティへの対応指針を示すことを目指している。

従来のサプライチェーンでは、セキュリティ対応をしっかりと行った主体間で行われる取引であれば、そのプロセス全体のセキュリティが確保されるという考え方に基づいていた。一方、「Society5.0」では、従来のサプライチェーンのように、組織のマネジメントの信頼性にのみ基点を置くことでバリュークリエイションプロセスの信頼性を確保することは困難となる。こうした、従来のサプライチェーンの活動範囲から拡張された付加価値を創造する活動のセキュリティ上のリスク源を的確に洗い出し、対処方針を示すためのモデルが必要となり、CPSF では、「三層構造モデル」と「６つの構成要素」で整理する手法を提供している。

３つの層でバリュークリエイションプロセスのリスク源を洗い出し、６つの構成要素について各リスク源に対する対策要件及び具体的な対策例を示すのが、CPSF の基本構成となっている。

1) 三層構造モデル

三層構造モデルは、バリュークリエイションプロセスのセキュリティ確保のための、信頼性の基点を設定するために使用される。従来のサプライチェーンの活動範囲から拡張された付加価値を創造する活動のセキュリティ上のリスク源を的確に洗い出し、対応方針を示すため、バリュークリエイションプロセスが発生する産業社会を、以下のように３つの「層」で整理し、セキュリティ確保のための信頼性の基点を明確化する。

- 第 1 層：企業間のつながりにおける、企業（組織）のマネジメントの信頼性の確保
- 第 2 層：フィジカルとサイバー空間のつながりにおける、正確に“転写”する機能の信頼性の確保
- 第 3 層：サイバー空間のつながりにおける、データの信頼性の確保

2) ６つの構成要素

６つの構成要素は、動的で柔軟なバリュークリエイションプロセスを捉えるための構成要素として使用される。前述の三層構造のモデルからリスク源を抽出し、オペレーションレベルでこうしたリスク源へ対応していくためには、リスク源となる脆弱性を持つ要素を明確にする必要がある。一方で、バリュークリエイションプロ

セスは動的に柔軟に構成されるものであるため、ビジネス資産を固定的に把握してリスク源に対応していく方法では、その構成が動的に変化するバリュークリエイションプロセスで本質的に防御しなければならない対象を見逃す恐れがある。そのため、バリュークリエイションプロセスに関与する構成要素を分解してある程度抽象化し、動的な構成の変化にも対応してリスク源に対応できるようにし構成要素ごとにセキュリティ対策の指針を示すことが必要である。CPSF では、対策を講じるための単位として、サプライチェーンを構成する要素を以下の６つに整理して捉える。

- ソシキ：バリュークリエイションプロセスに参加する企業・団体・ソシキ
- ヒト　：ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
- モノ　：ハードウェア、ソフトウェア及びそれらの部品を操作する機器を含む
- データ：フィジカル空間で収集された情報、共有・分析・シミュレーションを通じて加工された情報
- プロシージャ　：定義された目的を達成するために一連の活動を定めたもの
- システム　　：目的を実現するためにモノで構成される仕組み・インフラ

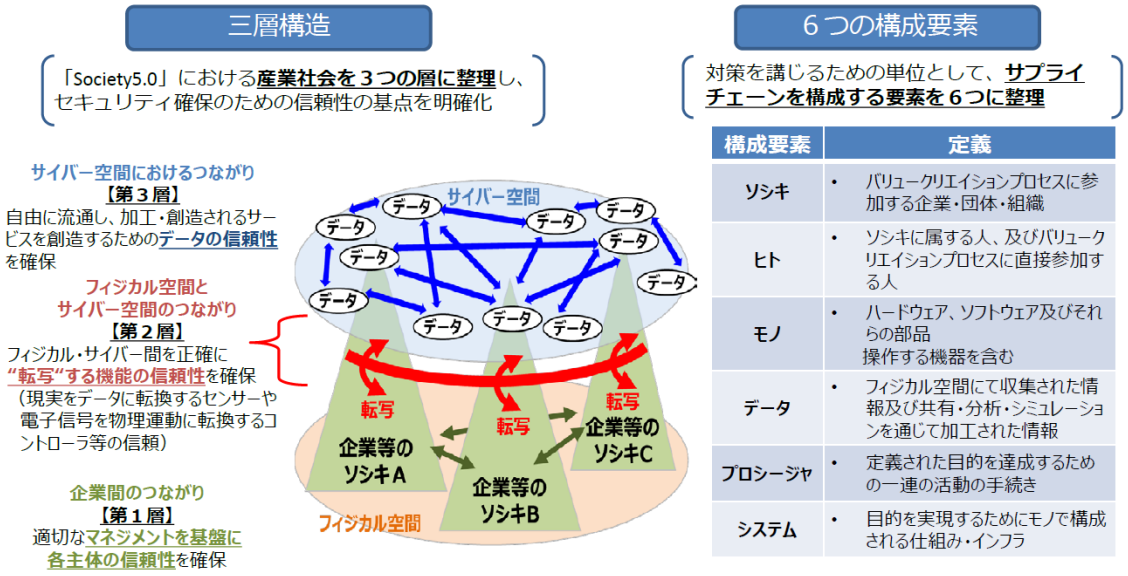


図　１　三層構造と６つの構成要素

3) リスク源と対応する方針の整理

三層構造モデルと６つの構成要素に基づいて、バリュークリエイションプロセスのリスク源と対応方針（ポリシー）を整理していく。リスク源はそれぞれの層で捉え方が異なり、対応方針もまた各層で異なることになる。こうした理解を踏まえて、本フレームワーク全体で、各層毎に守るべきものとリスク源を整理し、どのような方針に基づいてどのような対策を講じるかを整理する。

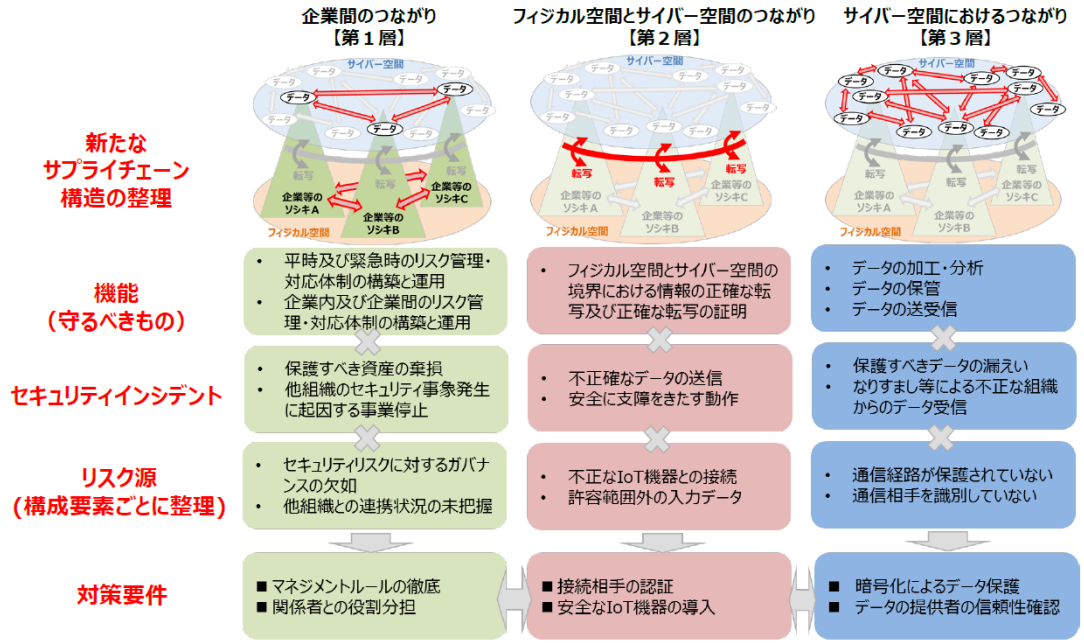


図 2 CPSF の全体概要

4) 信頼性の確保の考え方

三層構造モデルに基づいて、各層の信頼性の基点となる構成要素のセキュリティを各主体がそれぞれ確保することによって、バリュークリエイションプロセス全体のセキュリティ確保が実現される。

各構成要素について必要なセキュリティ要件が満たされていることを確認し(**信頼の創出**)、確認した主体以外の者による照会ができるようにし(**信頼の証明**)、それを繰り返し行い、広く共有して(**信頼のチェーンの構築、維持**)、バリュークリエイションプロセス全体のセキュリティを実現することになる。

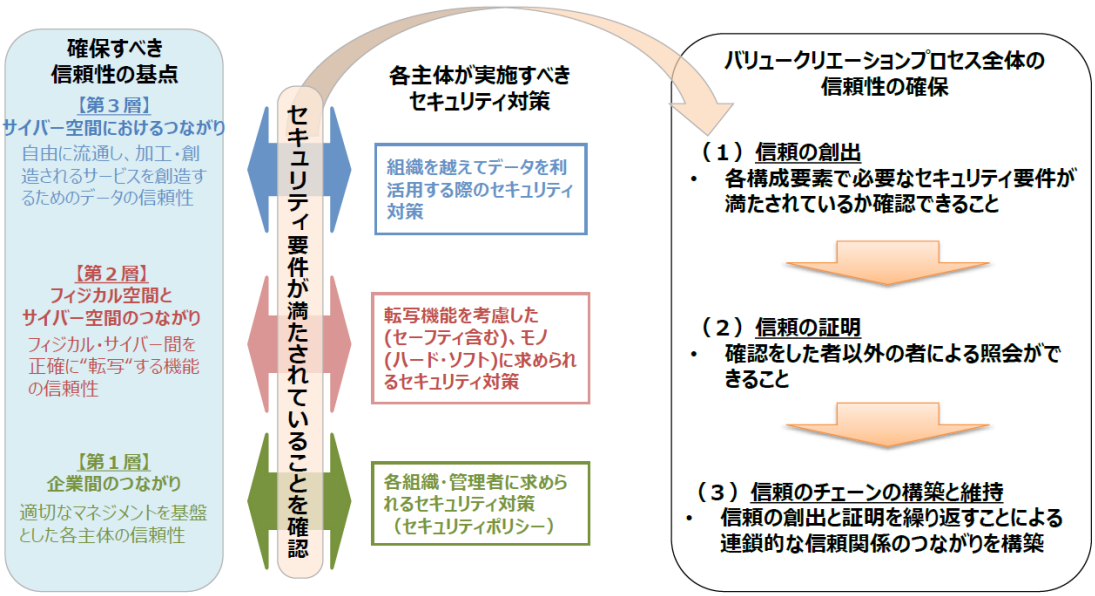


図 3 信頼性の確保の考え方

2-2 CPSF の検討プロセス

ドローン航路運営者は、JIS Q 31000:2010 や JIS Q 27001:2014 等のリスクマネジメントにおける標準的なプロセスを活用して、CPSF を利用することができる。「JIS Q 31000:2019 リスクマネジメント－原則及び指針」を基にしたリスクマネジメントの一般的なプロセスを図 4 に示す。

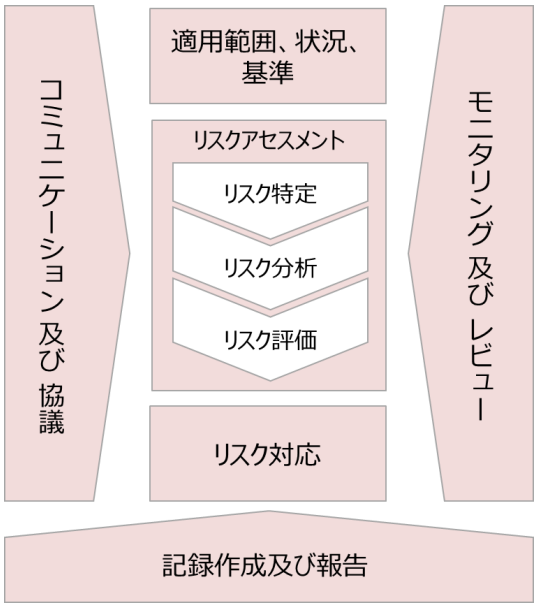


図 4 リスクマネジメントの一般的なプロセス

CPSF のセキュリティリスクマネジメントにおける具体的な適用範囲、状況、基準、リスクアセスメント及びリスク対応は、以下のプロセスで実施していく。

1) 適用範囲、状況、基準

① 分析対象の明確化

三層構造モデルに基づき、分析対象となるバリュークリエイションプロセスを明確化し、各層における構成要素を把握する。

② 想定されるセキュリティインシデント及び事業被害レベルの設定

自組織の事業に対して、各層の機能が脅かされることになると想定されるセキュリティインシデント及びそのセキュリティインシデントの結果、事業に影響がどの程度及ぶかについて、事業被害レベルとして設定する。

2) リスクアセスメント

③ リスク分析の実施

①で定義した分析対象の資産や、②で定義したセキュリティインシデントについて、リスクを脅威と脆弱性の観点から分析する。

3) リスク対応

④ リスク対応の実施

リスク分析の結果を受けて、リスク対応を実施する。

本書では、CPSF と「制御システムのセキュリティリスク分析ガイド」をベースにしたリスクマネジメントの流れと各プロセスにおける実施内容を図 5 のように定義する。

CPSF プロセス	検討内容
1．分析対象の明確化 （本書 3-1 節参照）	(1) 分析範囲の決定
	(2) 資産の明確化
	(3) システム構成の明確化
	(4) データフローの明確化
2．想定されるセキュリティインシデント及び事業被害レベルの設定 （本書 3-2 節参照）	(1) 資産重要度の検討
	(2) 事業被害と事業被害レベルの検討
	(3) 脅威レベル判断基準の検討
3．リスク分析の実施 （本書 3-3 節参照）	(1) 資産ベースのリスク分析
	(2) 事業被害ベースのリスク分析
	(3) CPSF ベースのリスク分析
4．リスク対応の実施 （本書 3-4 節参照）	(1) 改善箇所の抽出、選定
	(2) リスクの低減
	(3) リスク低減効果の把握

図 5 リスクマネジメントのプロセスと実施項目

3. セキュリティリスクマネジメント実施例

CPSF は、サイバー空間とフィジカル空間が高度に融合した新たな産業社会となる「Society5.0」におけるバリュークリエイションプロセスの全産業に共通的なセキュリティ対策を示している。ドローン航路においても、航路の相互接続やデータスペースを介してのデータ流通等、同様の観点でのセキュリティ対策が必要である。以下に示す内容は、あくまで、一般的なシステム環境を含む事業環境を前提としてセキュリティ分析を行った実施例であり、本書を参照するドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿った検討が必要であるとともに、検討結果は、自己の責任範囲であり、当然実施すべきセキュリティ対策は、もれなく対応する必要がある。

本書では、近年問題となっているサプライチェーンに対するセキュリティリスクを把握するため、分析対象としては外部事業者、外部システム、運航事業者等を含めて分析しているが、当該主体に対する直接的な対策実装義務を定めるものではない。具体的な責任分界および実装範囲は、契約、標準約款、SLA 等に基づき整理される。

3-1 分析対象の明確化

本プロセスでは、リスクアセスメントを実施するに当たり、事前準備として、分析対象を明確化し、三層構造モデルへの落とし込みを実施する。ドローン航路運営者は、分析範囲を決定し資産を明確化した後で、当該範囲内におけるシステム構成やデータフローを明確化することで、リスクアセスメントを実施する対象に対する理解を詳細化する。本プロセスで実施する内容は、以下の通り

(1) 分析範囲の決定（3-1-1 節）
(2) 資産の明確化（3-1-2 節）
(3) システム構成の明確化（3-1-3 節）
(4) データフローの明確化（3-1-4 節）

3-1-1 分析範囲の決定

分析対象の明確化を行うにあたっては、まず、表２に示すような各層の特性及びその果たすべき機能・役割を整理する必要がある。これらの機能・役割に照らして、分析対象のシステムが果たす機能に着目し、三層構造に基づいて分析範囲及び資産の分類を行う。

企業等が管理するモノはすべて第１層に含まれる。その中で、第２層、第３層の機能を備えるモノについては、その層に含まれるモノとして分析する必要がある。また、第 2 層の機能と第 3 層の機能を併せ持つモノについては、両方の層での分析が必要であることに留意する。その際、機能を踏まえてモノやシステムが設置される「場所」や、ヒトに対して特定のプロシージャを要求する「場所」も、リスクアセスメントにおいて留意する必要がある。

実施例検討に当たり、システム環境や事業環境を想定し整理した前提を以下に示す。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

1) 実施例検討で想定したバリュークリエイションプロセス

- ドローン航路運営者は、運航事業者と契約し、ドローン航路サービスを提供する。
- ドローン航路運営者は、外部システム(SDSP、UTMS、離着陸場管理システム、認証システム、航空局システム等)と連携し、ドローン航路サービスの安全を確保する。

2) フレームワークの留意点を踏まえた実施例検討の特徴

- 外部システムの情報を利用して、航路の環境情報提供／離着陸場管理／適合性評価／リスク分析を実施する。
- 目視外自律飛行するドローンをリアルタイムで監視する。(動態管理)
- 他ドローン航路システムと相互乗り入れのため接続する。

3) 資産等の各層への分類

ドローン航路に係る、分析対象の分類の実施例を表 1 に示す。

表 1 資産等の各層への分類の実施例

三層モデル	分析対象の分類
第 1 層	・ドローン航路運営者：運航事業者の要求によりドローン航路サービスを提供 ・SDSP：航路に係る環境情報をドローン航路運営者、USP、運航事業者に提供 ・運航事業者：ドローン航路サービスの提供を受け、ドローンを運航 ・関連システム運営者：ドローン航路運営者に運航事業者等の認証サービスを提供、また、事業者間の決済サービスを提供 ・離着陸場管理者：ドローン航路運営者にドローン離着陸場の情報を提供 ・航空局：ドローン航路運営者の申請に応じ航路情報を公開、運航事業者の申請に応じ飛行許可
第 2 層	・環境情報(気象/地図情報等)／ドローンの動態情報：安全確保のためドローン航路システムに収集するとともに運航事業者に提供 ・認証情報：ドローン航路システムにアクセスする人／システムは関連システム(ODS等)で認証され、認証結果に基づきドローン航路システムで認可 ・精算決済情報：ドローン航路システムの相互乗り入れ等で発生する精算情報は関連システムの精算決済サービスで決済
第 3 層	・環境情報：気象情報、地形情報等は安全確保のためドローン航路システムが収集 ・動態情報：ドローンの動態情報は安全確保のため運航管理システム等を介してドローン航路システムが収集 ・認証情報：ドローン航路システムにアクセスする人／システムは関連システムで認証し、認証結果に基づきドローン航路システムが認可 ・精算決済情報：ドローン航路システムの相互乗り入れ等で発生する精算情報は関連システムの精算決済サービスで決済

三層構造モデルにおける各層の特性、機能・役割、分析対象の検討と、前提条件の整理を抽象化したモデルとして、分析範囲と資産の配置の概念図検討の実施例を、付録１に示す。

3-1-2 資産の明確化

資産の配置を念頭に、具体的に資産の分類、機能、設置場所、接続先 NW、管理ポートの有無、ベンダー、OS、プロトコル等、資産一覧を整理する。また、現状の物理的対策・運用的対策といった資産の外部環境の対策と、資産自身の技術的対策を整理する。システム環境や事業環境を想定して検討した実施例を付録２に示す。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

3-1-3 システム構成の明確化

分析対象システムのシステム構成図を整理する。作成に当たっては、ネットワーク接続状況と資産の物理的な設置場所が把握できるようにする。システム環境や事業環境を想定して検討した実施例を付録３に示す。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

3-1-4 データフローの明確化

分析対象システムの業務の流れを整理する。また、資産間で送受信されるネットワークデータをデータフローマトリクス表とデータフロー図に整理する。さらに、サービス毎に、取扱情報を含めた業務・データフロー図を整理し、資産同士の通信と通信の目的を明確化する。システム環境や事業環境を想定して検討した実施例を付録４に示す。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

3-2 想定されるセキュリティインシデント及び事業被害レベルの設定

本プロセスでは、明確化された分析対象の事業活動に対し、重大な影響を及ぼし得るセキュリティインシデントを整理し、それによる事業への影響を整理する。本プロセスで実施する内容は、以下の通り。

(1) 資産重要度の検討（3-2-1 節）
(2) 事業被害と事業被害レベルの検討（3-2-2 節）
(3) 脅威レベル判断基準の検討（3-2-3 節）

3-2-1 資産重要度の検討

1) 資産重要度の判断基準

まず、資産重要度の判断基準を検討する。資産の重要度を 3 段階で評価する場合の判断基準（被害大：3 ＞ 被害中：2 ＞被害小：1）を検討する。システム環境や事業環境を想定して検討した実施例を表 2 に示す。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

表 2 資産重要度の判断基準例

評価値	判断基準
3	・資産が失われた、もしくは不正に操作された場合、事業上の被害は大。 －システムが長期間停止（2 週間以上停止）する。 －長期間ドローン航路サービス提供が出来なくなり、業務が停滞する。
2	・資産が失われた、もしくは不正に操作された場合、事業上の被害は中。 －システムが一定期間停止（3 日～2 週間未満停止）する。 －一定期間ドローン航路サービス提供が出来なくなり、業務が停滞する。
1	・資産が失われた、もしくは不正に操作された場合、事業上の被害は小。 －システムが一定期間停止（3 日未満）する。 －一定期間ドローン航路サービス提供が出来なくなり、業務が停滞するが、挽回可能なレベル。

2) 資産重要度

前項で整理した資産重要度の判断基準に従い、資産一覧で整理した各資産の重要度を検討する。システム環境や事業環境を想定して検討した実施例を付録 5 に示す。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

3-2-2 事業被害と事業被害レベルの検討

1) 事業被害レベルの判断基準

まず、事業被害レベルの判断基準を検討する。事業被害レベルを 3 段階で評価する場合の判断基準（被害大：3 ＞ 被害中：2 ＞被害小：1）を検討する。システム環境や事業環境を想定して検討した実施例を表 3 に示す。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

表 3 事業被害レベルの判断基準例

評価値		判断基準
3	事業上の被害が大きい	・資産が失われた、もしくは不正に操作された場合、事業上の被害は大。 －システムが長期間停止（2 週間以上停止）する。 －長期間ドローン航路サービス提供が出来なくなり、業務が停滞する。
2	事業上の被害が中程度	・資産が失われた、もしくは不正に操作された場合、事業上の被害は中。 －システムが一定期間停止（3 日～2 週間未満停止）する。 －一定期間ドローン航路サービス提供が出来なくなり、業務が停滞する。
1	事業上の被害が小さい	・資産が失われた、もしくは不正に操作された場合、事業上の被害は小。 －システムが一定期間停止（3 日未満）する。 －一定期間ドローン航路サービス提供が出来なくなり、業務が停滞するが、挽回可能なレベル。

2) 事業被害と事業被害レベル

前項で整理した事業被害レベルの判断基準に従い、分析対象の事業被害を整理するとともに、その事業被害レベルを判断根拠と合わせて検討する。

情報の改竄や漏洩のリスクに関しては、直接的な被害リスクが無くても、間接的な被害リスク（例えば、地図情報の改竄や個人情報の漏洩等による影響）が存在し得るため、事業被害レベルを検討する際は、考慮する必要がある。システム環境や事業環境を想定して検討した実施例を付録 6 に示す。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

3-2-3 脅威レベル判断基準の検討

脅威レベルの判断基準（発生可能性 3：高＞2：中＞1：低）を表 4 に示す。

表 4 脅威レベルの判断基準

脅威レベル	悪意のある第三者の攻撃による判断基準	資産の論理的な配置による判断基準	資産の物理的な配置による判断基準
3	個人の攻撃者（スキルは問わない）によって攻撃された場合、攻撃が成功する可能性が高い。	インターネットと接続可能なネットワーク（情報ネットワーク）上にある資産。	敷地と部屋への入室制限がなく、誰でもアクセスできる場所にある資産。
2	一定のスキルを持った攻撃者によって攻撃された場合、攻撃が成功する可能性がある。	情報ネットワークと間接的に接続しているネットワーク（社内ネットワーク）上にある資産。	敷地と部屋への入室制限がある場所にある資産。
1	国家レベルのサイバー攻撃者（軍隊及びそれに準ずる団体）によって攻撃された場合、攻撃が成功する可能性がある。	隔離されたネットワーク上にある資産。	厳重な有人監視体制と、敷地と部屋への入室制限に厳重な認証を有する部屋にある資産。

注：「制御システムのセキュリティリスク分析ガイド 第 2 版」より引用

3-3 リスク分析の実施

本プロセスでは、「制御システムのセキュリティリスク分析ガイド」のプロセスに準じて、3-1 節及び 3-2 節で検討した内容を踏まえた資産ベースのリスク分析、及び事業被害ベースのリスク分析を実施し、リスク源（脅威/脆弱性）の評価等を行う。最終的に、CPSF リスク分析シートに対策を含め整理する。本プロセスで実施する内容は、以下の通り。

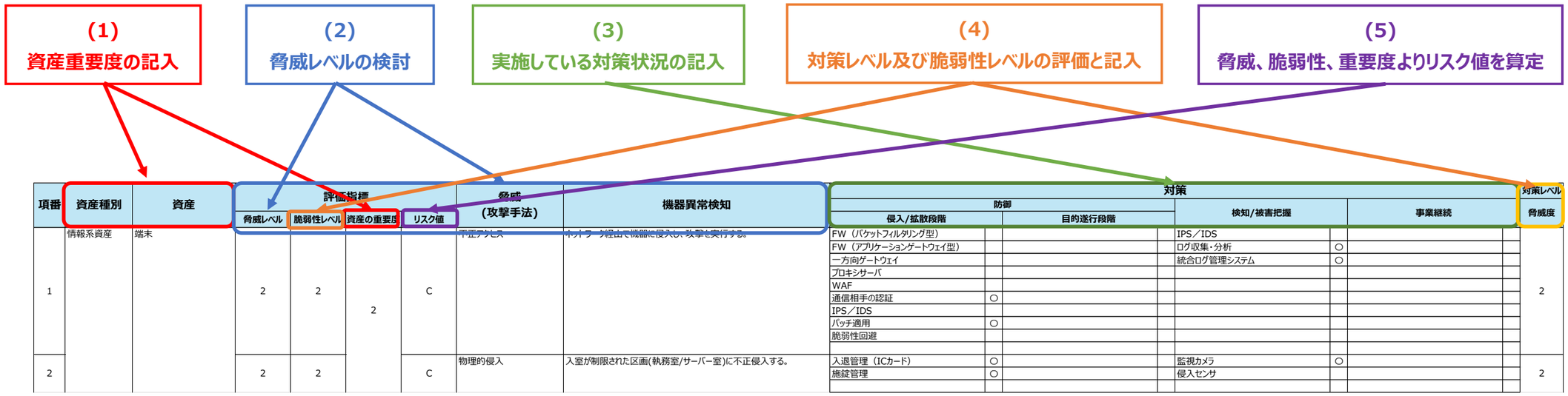
(1) 資産ベースのリスク分析（3-3-1 節）
(2) 事業被害ベースのリスク分析（3-3-2 節）
(3) CPSF ベースのリスク分析（3-3-3 節）

3-3-1 資産ベースのリスク分析

資産ベースのリスク分析は、保護すべきシステムを構成する各資産を対象に、その重要度（価値）、想定される脅威の発生可能性、脅威に対する脆弱性の 3 つを評価指標として、リスクを評価する分析手法である。

「3-1-2 資産の明確化」で整理した分析対象の各資産に対して、リスク分析を実施する。資産ベースのリスク分析シートの作成は、以下の手順で行う。概要を図 6 に示す。

(1) 資産重要度の記入
(2) 脅威レベルの検討
(3) 実施している対策状況の記入
(4) 対策レベル及び脆弱性レベルの評価と記入
(5) 脅威、脆弱性、重要度よりリスク値を算定



項番	資産種別	資産	評価指標				脅威	機器異常検知	対策						対策レベル
			脅威レベル	脆弱性レベル	資産の重要度	リスク値	(攻撃手法)		防御		検知/被害把握		事業継続		脅威度
									侵入/拡散段階		目的遂行段階				
1	情報系資産	端末	2	2	2	C	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW（パケットフィルタリング型）			IPS／IDS			2
									FW（アプリケーションゲートウェイ型）			ログ収集・分析	○		
									一方向ゲートウェイ			統合ログ管理システム	○		
									プロキシサーバ						
									WAF						
									通信相手の認証	○					
									IPS／IDS						
									パッチ適用	○					
									脆弱性回避						
2			2	2		C	物理的侵入	入室が制限された区画(執務室/サーバー室)に不正侵入する。	入退管理（ICカード）	○		監視カメラ	○		2
									施錠管理	○		侵入センサ			

図 6 資産ベースのリスク分析シート作成の手順

1) 資産重要度の記入

各資産に対し「3-2-1 資産重要度の検討」で整理した資産重要度を「資産ベースのリスク分析シート」（付録 7（5）の実施例を参照）に記入する。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

2) 脅威レベルの検討

分析対象の各資産に対して想定される脅威（攻撃手法）を整理する。（付録 7（1）の実施例を参照）

次に、各資産に対する脅威の脅威レベルとその設定根拠を整理する。（付録 7（2）及び付録 7（3）の実施例を参照）

整理した脅威レベルを「資産ベースのリスク分析シート」に記入する。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

3) 実施している対策状況の記入

想定する脅威（攻撃手法）に対するセキュリティ対策の実施状況を「資産ベースのリスク分析シート」（付録 7（5）の実施例を参照）に記入する。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

4) 対策レベル及び脆弱性レベルの評価と記入

「対策レベル」は、想定する脅威に対するセキュリティ対策状況の有効性を 3 段階で評価した値である。想定する脅威（攻撃手法）が発生した場合、現在実施している対策で防止できる可能性を表す。対策レベル＝3 は脅威に対するセキュリティ対策が有効＝攻撃が成功する可能性が低いことを意味し、対策レベル＝1 は脅威に対するセキュリティ対策が無効＝攻撃が成功する可能性が高いことを意味する。対策レベルの判断基準を表 5 に示す。

表 5 対策レベルの判断基準

対策レベル	具体的な判断基準の例
3	脅威の対策が十分実施されており、攻撃が成功する可能性は低い。
2	脅威の対策が実施されているが、十分とは言えないため、攻撃が成功する可能性は中程度である。
1	脅威の対策が実施されておらず、攻撃が成功する可能性は高い。

注：「制御システムのセキュリティリスク分析ガイド 第 2 版」より引用

評価指標「脆弱性」とは、リスク分析で用いる評価指標の一つであり、システムに対して発生する脅威の受容可能性を表す。「脆弱性レベル」は、評価指標「脆弱性」（発生した脅威を受け入れる可能性）を 3 段階（1～3）で評価した値である。脆弱性レベル＝3 は脅威を受け入れる可能性が高いことを意味し、脆弱性レベル＝1 は脅威を受け入れる可能性が低いことを意味する。脆弱性レベルの判断基準を表 6 に示す。

表 6 脆弱性レベルの判断基準

脆弱性レベル	具体的な判断基準の例
3	脅威が発生した場合、受け入れる可能性が高い。
2	脅威が発生した場合、受け入れる可能性が中程度である。
1	脅威が発生した場合、受け入れる可能性が低い。

注：「制御システムのセキュリティリスク分析ガイド 第 2 版」より引用

「脆弱性レベル」の算定に当たっては、各脅威に対するセキュリティ対策状況の評価値「対策レベル」で評価し、その値から脆弱性レベルの値を求める。脆弱性レベルと対策レベルの関係を表 7 に示す。

この結果を、脆弱性レベル一覧表に整理する。（付録 7（4）の実施例を参照）なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

表 7 脆弱性レベルと対策レベルの関係

評価値		判断基準
脆弱性レベル	対策レベル	
3	1	脅威が発生した場合、受け入れる可能性が高い。 脅威の対策が実施されておらず、攻撃が成功する可能性は高い。 【例】 ・過去の事例において、脆弱性を利用した攻撃が発生・成功し、被害が生じたことが確認されている。
2	2	脅威が発生した場合、受け入れる可能性が中程度である。 脅威の対策が実施されているが、十分とは言えないため、攻撃が成功する可能性は中程度である。 【例】 ・一般的な対策を実施しており、攻撃が成功するか否かは攻撃者のレベルに依る。 ・過去の事例において、脆弱性を利用した攻撃が発生したが、大きな被害に至らなかったことが確認されている。
1	3	脅威が発生した場合、受け入れる可能性が低い。 脅威の対策が十分実施されており、攻撃が成功する可能性は低い。 【例】 ・効果的な対策や多層的な対策を実施しており、攻撃が成功する可能性は低い。 ・過去の事例において、脆弱性を利用した攻撃は発生していない。

注：「制御システムのセキュリティリスク分析ガイド 第 2 版」より引用

5) 脅威、脆弱性、重要度よりリスク値を算定

資産ベースのリスク分析における「リスク値」は、資産に対する脅威の総合的なリスクレベルを表す。即ち、各々の資産に対する脅威（攻撃手法）が発生して被害を生じるリスクを、脅威の発生可能性／受容性と被害の大きさから、相対評価可能な値として算定したものである。

リスク値は、3 つの評価指標「脅威レベル」「脆弱性レベル」及び「資産の重要度」によって算定する。リスク値は、A（リスクが非常に高い）～ E（リスクが非常に低い）の 5 段階で評価する。

3 つの評価指標に基づくリスク値の算定基準を表 8 に示す

表 8　資産ベースのリスク分析におけるリスク値の算定基準

評価指標と評価値			リスク値	判定条件
脅威 レベル	脆弱性 レベル	資産の 重要度		
3	3	3	A	重要度＝3 6≦脅威×脆弱性≦9
3	2	3		
2	3	3		
2	2	3	B	重要度＝3 3≦脅威×脆弱性＜6
3	1	3		
1	3	3		
3	3	2		重要度＝2 6≦脅威×脆弱性≦9
3	2	2		
2	3	2		
2	1	3	C	重要度＝3 1≦脅威×脆弱性＜3
1	2	3		
1	1	3		
2	2	2		重要度＝2 3≦脅威×脆弱性＜6
3	1	2		
1	3	2		
3	3	1		重要度＝1 6＜脅威×脆弱性≦9
2	1	2	D	重要度＝2 1≦脅威×脆弱性＜3
1	2	2		
1	1	2		
3	2	1		重要度＝1 3＜脅威×脆弱性≦6
2	3	1		
2	2	1		
3	1	1	E	重要度＝1 1≦脅威×脆弱性≦3
1	3	1		
2	1	1		
1	2	1		
1	1	1		

注：「制御システムのセキュリティリスク分析ガイド 第 2 版」より引用

6) 資産ベースのリスク分析まとめ

以上の手順を各資産に対し整理する。一例として端末を対象にした資産ベースのリスク分析シートの実施例を付録 7（5）に示す。本シートは、各資産で整理する。

各資産ベースのリスク分析シートを整理した後、リスク値を一覧表として整理する。これにより、

① リスク分析シートは資産ごとに分かれているが、この表により、全ての資産のリスク値の評価値を俯瞰することができる。

② 同種の脅威（攻撃手法）に対する各資産のリスク値を比較し、同一であること、あるいは資産によって異なることの妥当性を再確認する手助けとなる。

リスク値まとめ表の実施例を、付録 7（6）に示す。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

3-3-2 事業被害ベースのリスク分析

事業被害ベースのリスク分析は、システムで実現している事業やサービスに対して、事業被害とそのレベル、事業被害を引き起こす攻撃ツリーの発生可能性、攻撃に対する脆弱性の３つを評価指標として、リスクを評価する分析手法である。

「3-2-2 事業被害と事業被害レベルの検討」で整理した事業被害に対して、回避したい事業被害を明確化し、事業被害を引き起こすと想定される攻撃について、事業被害の大きさと、攻撃の発生可能性と受容可能性（脆弱性）の相乗値によって、事業のリスクを評価するリスク分析方法である。事業被害ベースのリスク分析シートの作成は、以下の手順で行う。概要を図 7 に示す。

(1) 攻撃シナリオの検討
(2) 攻撃ルートの検討
(3) 事業被害レベルの記入
(4) 脅威レベルの記入
(5) セキュリティ対策状況の記入
(6) 対策レベル／脆弱性レベルの記入
(7) リスク値の評価

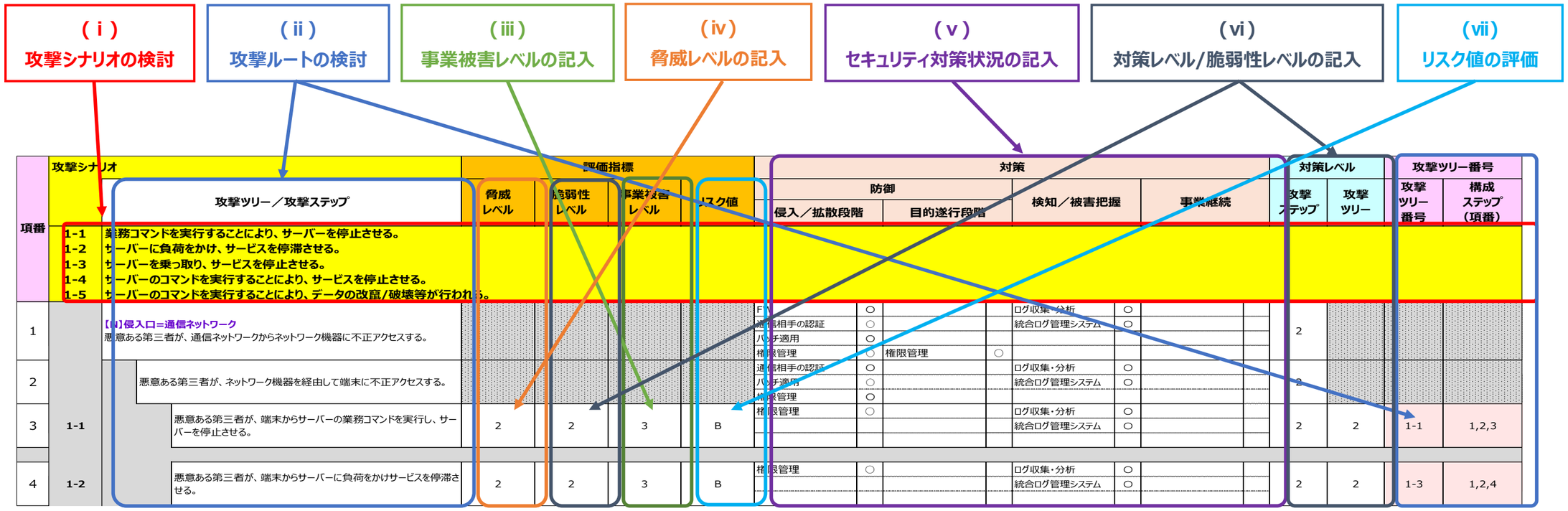


図 7　事業被害ベースのリスク分析シート作成の手順

1) 攻撃シナリオの検討

「3-2-2 事業被害と事業被害レベルの検討」をベースに、事業被害を引き起こす可能性のある攻撃拠点・攻撃対象・最終攻撃を具体化したシナリオを整理する。

シナリオ検討に当たっては、回避したい事業被害について、事業被害を選定して攻撃シナリオを検討する。例えば、事業被害レベル＝3 と判断した事業被害は、攻撃が成功裏に行われた場合、事業者にとって甚大な打撃を被ると判断されたものである。そのような事業被害レベルの高い事業被害を優先的に選定し、攻撃シナリオを検討することが考えられる。

システム環境や事業環境を想定して検討した攻撃シナリオの実施例を付録８（1）に示す。

ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

2) 攻撃ルートの検討

攻撃ルートの検討では、以下の手順で行う。

(1) 侵入口の検討と選定

「侵入口」は、攻撃者が攻撃を行う際に攻撃の入口となる資産である。本節では、侵入口となり得るネットワークや機器をシステム構成図から全て洗い出し、事業被害ベースのリスク分析で分析対象とする侵入口を選定する。

ネットワーク経由の攻撃の侵入口は、悪意のある第三者が制御システムへの攻撃を試みる際に、まず狙う侵入経路と考えられるため、基本的に全て分析を行う。

物理アクセスによる攻撃の侵入口は、攻撃者が物理アクセスによる攻撃を行う場合、内部関係者はもちろん悪意のある第三者も、攻撃のしやすさが同等であれば最終攻撃に有利な機器を優先的に狙うと推察されるため、最終攻撃に有利な機器を優先して分析することを推奨する。

(2) 攻撃者の検討と選定

「攻撃者」は、システムに対する攻撃を行う個人・組織・団体である。想定される攻撃者を洗い出し、事業被害ベースのリスク分析で分析対象とする攻撃者を選定する。

攻撃者には、「悪意のある第三者」、「内部関係者（過失）」、「内部関係者（故意）」が想定される。

(3) 攻撃ルートの検討と選定

「攻撃ルート」は、攻撃者が侵入口から経由を通って攻撃拠点に到達するまでのルートである。想定される攻撃ルートを洗い出し、最終的に分析対象とする攻撃ルートを選定する。

攻撃ルートは、攻撃シナリオで洗い出した攻撃拠点と、侵入口を結ぶルートを、「誰が」（攻撃者）、「どこから」（侵入口）、「どうやって」（侵入口～攻撃拠点までのルート（経由する必要がある機器））、「どこで」（攻撃拠点・攻撃対象）、「何をする」（最終攻撃）の観点で検討する。

分析対象の攻撃シナリオについて攻撃ルートが洗い出せたら、次に、実際に攻撃ツリーを作成する攻撃ルートを選定する。攻撃者が攻撃を行う場合、特に悪意のある第三者は、最終攻撃が行え

る機器（攻撃拠点）に到達するのになるべく攻撃コストが掛からないルートを優先的に狙うと推察されるため、まずは、攻撃コストが低い攻撃ルートを適当数（20～100 程度）選定して分析することを推奨する。

(4) 攻撃ツリーの組立てと記入

「攻撃ツリー」は、攻撃拠点で実行される最終攻撃に向けて、侵入口から攻撃拠点まで進んで行く一連の攻撃手順である。そして、各攻撃段階（侵入口への侵入、侵入口から経由への侵入、経由から攻撃拠点への侵入、攻撃拠点から攻撃対象への最終攻撃の実行）が、攻撃ステップとなる。システム環境や事業環境を想定して検討した実施例を付録８（2）に示す。

各攻撃ツリーは、一連の攻撃手順（攻撃ステップ）から構成される。それぞれの攻撃ステップは、前節で選定した攻撃ルートの「攻撃者」「侵入口」「経由」「攻撃拠点」「攻撃対象」「最終攻撃」を用いて組み立てる。実施例を付録８（3）に示す。

整理した攻撃ツリーは、事業被害ベースのリスク分析シートの「攻撃ツリー／攻撃ステップ」欄に記入する。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

3) 事業被害レベルの記入

評価指標「事業被害」の評価値「事業被害レベル」は、システムによって実現している事業が損なわれた場合の被害の大きさを 3 段階で評価した値である。事業被害ベースのリスク分析においては、攻撃ツリー単位で評価し、想定した攻撃ツリーが発生した場合の被害の大きさを表す。

事業被害レベルは、各々の攻撃ツリーが想定している事業被害に従い、「3-2-2 事業被害と事業被害レベルの検討」で整理した事業被害レベルを、リスク分析シートの「評価指標」の「事業被害レベル」欄に記入する。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

4) 脅威レベルの記入

評価指標「脅威」の評価値「脅威レベル」は、システムに対する脅威の発生可能性を 3 段階で評価した値である。事業被害ベースのリスク分析においては、攻撃ツリー全体で評価し、想定した攻撃ツリーが発生する可能性を表す。

脅威レベルは、攻撃ツリーごとに、攻撃者が侵入口から侵入し、攻撃拠点まで到達し、最終攻撃を実行するに至る可能性を評価する。「3-2-3 脅威レベル判断基準の検討」で定義した判断基準に基づいて評価し、リスク分析シートの「評価指標」の「脅威レベル」欄に記入する。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

5) セキュリティ対策状況の記入

事業被害ベースのリスク分析における「セキュリティ対策状況」は、想定する攻撃に対するセキュリティ対

策の実施状況を示し、攻撃ステップ単位で記入する。

セキュリティ対策は、各攻撃ステップで想定する攻撃に対して、現状実施（実装）している対策を、リスク分析シートの「対策」欄に記入する。各対策は、用途と目的によって 4 つの分類（「防御（侵入／拡散段階）」、「防御（目的遂行段階）」、「検知／被害把握」、「事業継続」）に区分し、該当欄に記入する。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

6) 対策レベル／脆弱性レベルの記入

評価指標「セキュリティ対策状況」の評価値「対策レベル」は、システムに対して発生した脅威に対するセキュリティ対策状況の有効性を 3 段階で評価した値である。事業被害ベースのリスク分析においては、攻撃ステップ及び攻撃ツリーについて対策レベルの評価を行い、想定した攻撃（攻撃ステップ、攻撃ツリー）が発生した場合、現在実施している対策で防止できる可能性を表す。

攻撃ステップの対策レベルは、「3-3-1 資産ベースのリスク分析」で整理した判断基準に基づいて評価し、事業被害ベースのリスク分析シートの「対策レベル（攻撃ステップ）」欄に記入する。

評価指標「脆弱性」の評価値「脆弱性レベル」は、システムに対して発生した脅威の受容可能性を 3 段階で評価した値である。事業被害ベースのリスク分析においては、攻撃ツリーについて脆弱性レベルの評価を行い、想定する攻撃ツリーが発生した場合、それを受け入れてしまう可能性、即ち、攻撃が成功する可能性を表す。

攻撃ツリーの脆弱性レベルの値は、双対の関係にある攻撃ツリーの対策レベルの値から算出し、事業被害ベースのリスク分析シートの「評価指標」の「脆弱性レベル」欄に記入する。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

7) リスク値の評価

事業被害ベースのリスク分析における「リスク値」は、攻撃ツリーが成立する総合的なリスクレベルを表す。即ち、各々の攻撃ツリーの攻撃が実行・完遂され、事業被害が発生するリスクを、攻撃ツリーの発生可能性／受容可能性と被害の大きさから、相対評価可能な値として算定したものである。

リスク値は、3 つの評価指標「脅威レベル」「脆弱性レベル」及び「事業被害レベル」から算定する。リスク値は、A（リスクが非常に高い）～E（リスクが非常に低い）の 5 段階で評価する。

3 つの評価指標に基づくリスク値の算定基準を表 9 に示す。

表 9　事業被害ベースのリスク分析におけるリスク値の算定基準

評価指標と評価値			リスク値	判定条件
脅威レベル	脆弱性レベル	事業被害レベル		
3	3	3	A	事業被害＝3 6≦脅威×脆弱性≦9
3	2	3		
2	3	3		
2	2	3	B	事業被害＝3 3≦脅威×脆弱性＜6
3	1	3		
1	3	3		
3	3	2		事業被害＝2 6≦脅威×脆弱性≦9
3	2	2		
2	3	2		
2	1	3	C	事業被害＝3 1≦脅威×脆弱性＜3
1	2	3		
1	1	3		
2	2	2		事業被害＝2 3≦脅威×脆弱性＜6
3	1	2		
1	3	2		
3	3	1		事業被害＝1 6＜脅威×脆弱性≦9
2	1	2	D	事業被害＝2 1≦脅威×脆弱性＜3
1	2	2		
1	1	2		
3	2	1		事業被害＝1 3＜脅威×脆弱性≦6
2	3	1		
2	2	1		
3	1	1	E	事業被害＝1 1≦脅威×脆弱性≦3
1	3	1		
2	1	1		
1	2	1		
1	1	1		

注：「制御システムのセキュリティリスク分析ガイド 第 2 版」より引用

8) 事業被害ベースのリスク分析まとめ

以上の手順を各シナリオに対し整理する。システム環境や事業環境を想定して検討した事業被害ベースのリスク分析の実施例を付録 8（4）に示す。

事業被害ベースのリスク分析シートを整理した後、リスク値を一覧表として整理する。これにより、

① リスク分析結果の全体像（全体におけるリスク値の分布）を把握できる

② 各事業被害／攻撃シナリオにおけるリスク値の分布を把握できる

③ どの事業被害／攻撃シナリオにリスク値の高い攻撃ツリーが存在するかを把握できる

リスク値まとめ表の実施例を付録 8（5）に示す。なお、ドローン航路運営者は、自己のシステム環境を含む、実際の事業環境に沿って検討すること。

3-3-3 CPSF ベースのリスク分析

前節まで、「3-3-1 資産ベースのリスク分析」で、資産ベースのリスク分析結果である資産ごとのリスク値、「3-3-2 事業被害ベースのリスク分析」で、事業被害レベル値と攻撃ツリーのリスク値が得られた。

これらの結果を、CPSF の特徴である、「三層構造モデル」と「６つの構成要素」に基づいて、バリュークリエイションプロセスのリスク源と対応方針（ポリシー）を整理する。

1) 第 1 層：企業（組織）間のつながり

第 1 層における機能／想定されるセキュリティインシデント／リスク源／対策要件を整理する。

システム環境や事業環境を想定して検討した実施例を付録 9（1）に示す。

2) 第 2 層：フィジカル空間とサイバー空間のつながり

第 2 層における機能／想定されるセキュリティインシデント／リスク源／対策要件を整理する。

システム環境や事業環境を想定して検討した実施例を付録 9（2）に示す。

3) 第 3 層：サイバー空間におけるつながり

第 3 層における機能／想定されるセキュリティインシデント／リスク源／対策要件を整理する。

システム環境や事業環境を想定して検討した実施例を付録 9（3）に示す。

3-4 リスク対応の実施

3-4-1 セキュリティリスクマネジメントの確立

リスク分析結果の解釈及び活用のねらいは、システムのセキュリティ上の弱点を見つけ、サイバー攻撃に対するリスクを低減することにある。そのためには、得られたリスク値を可能な限り低減することが理想的ではあるが、コスト上の制約や有効な対策が見当たらない、システムの稼働状態等の理由から現実的には難しい。このため、リスク分析結果を活用しセキュリティリスクマネジメントを確立することが重要である。

ドローン航路運営者は、一通りのセキュリティリスク分析を一度実施して終わりではなく、どこにセキュリティリスクがあるかを把握し、システム環境・事業環境・取り巻く環境等の変化も考慮し、誰が、どのリスクを、いつまでに対策するかを管理するための、セキュリティリスクマネジメントを確立する必要がある。

3-3 節で提供した実施例は、「サイバー・フィジカル・セキュリティ対策フレームワーク（Version 1.0）」及び「制御システムのセキュリティリスク分析ガイド 第 2 版」のテンプレートをそのまま利用した一例であるが、セキュリティリスクマネジメントへの活用のために、必要なテンプレートに担当部署/社内規定/責任者などの管理欄を設けるなどの修正を加えて利用しても良いし、独自のテンプレートを利用しても良い。

1) 付録 6「事業被害一覧と事業被害レベル」の活用

付録 6 の「事業被害の概要」欄で、「担当部署」「社内規定」「責任者」を決め、管理する活用例を図 8 示す。

項番	事業被害	事業被害の概要	担当部署	社内規定	責任者
1	ドローン航路サービスの長期間サービス提供停止	サーバーへのサイバー攻撃により、業務コマンドを悪用されてサービス停止、重要情報の改竄/破壊等が実行され、ドローン航路サービス提供が長期間停止する。			
2	ドローン航路サービスの一定期間サービス提供停止	端末へのサイバー攻撃により、操作不能になった場合、一定期間、ドローン航路サービス提供が停止する恐れがある。 また、端末が乗っ取られた場合、サーバー等への不正アクセスが可能になり、一定期間、ドローン航路サービス提供が停止する。			
3		ネットワーク機器へのサイバー攻撃により、フィルタ設定情報が改竄されると、情報ネットワークからサーバー等への不正アクセスが可能になり、一定期間、ドローン航路サービス提供が停止する。			
4		関連システムへのサイバー攻撃により、認証情報や決済情報が改竄されたり、認証や決済機能が停止し、間接的に一定期間、ドローン航路サービス提供が停止する。			

図 8 テンプレートの活用例：「事業被害一覧と事業被害レベル」

2) 付録 9「CPSF ベースのリスク分析」の活用

付録 9 の CPSF の「対策要件」欄は、あくまで、対策例を示したものであり、管理するには煩雑すぎて適さない。そのため、ドローン航路運営者層が比較的理解しやすい「脆弱性」欄レベルで、「担当部署」「社内規定」「責任者」を決めて管理すると管理しやすい。実施例を図 9 示す。

項番	機能	想定される セキュリティインシデント	リスク源			担当部署	社内規定	責任者
			脅威		脆弱性			
1-1	組織として平時のリスク管理体制を構築し適切に運用する	組織で管理している領域から保護すべきデータが漏洩する	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・入力確認の不備を突いたインジェクション攻撃	L1_1_a_ORG	**[ソシキ]** ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない			
				L1_1_a_PEO	**[ヒト]** ・自身が関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない			
					[ヒト] ・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない			
				L1_1_a_COM	**[モノ]** ・モノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない			
				L1_1_a_SYS	**[システム]** ・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない			

図 9 テンプレートの活用例：「CPSF ベースのリスク分析」

前述の通り、ドローン航路運営者層が比較的理解しやすい「脆弱性」欄レベルで管理すると、管理者層とセキュリティ担当者層との意思疎通が図りやすくなる利点がある。脆弱性の項目の概要を表 10 示す。詳細については、「脆弱性」の項目のみを各層でまとめた脆弱性一覧表を付録 10 に示す。

表 10 脆弱性の概要

リスク領域	代表的な事象（例）	リスク対応（例）
ガバナンス／手順	・リスクマネジメント未実行 ・法令準拠ルール未整備 ・IR 手順なし	・方針・手順の制定 ・BCP への位置づけ
資産・構成管理	・棚卸・構成・パッチ状況を把握できない	・台帳整備と自動収集 ・可視化
脆弱性／設定	・修正遅延 ・弱い PW・不要ポート	・是正 SLA ・セキュア設定の標準化
アクセス／認証	・管理権限の制御不備 ・相手認証なし	・最小権限 ・多要素認証 ・相互認証
監視／検知／IR	・不正機器・不正通信を検知遮断不可	・ログ基盤 ・監視 ・演習
データ保護	・機密区分不明 ・改ざん検知なし	・区分定義 ・暗号化 ・完全性検証
調達／物理／通信	・供給者信頼性未確認 ・物理対策不足 ・通信保護不足	・要求定義・評価 ・物理統制 ・セグメンテーション

3-4-2 セキュリティリスク分析結果の活用

リスク分析結果は、以下のように活用することができる。

1) リスクの把握

対象システムにおけるリスク値の分布と、総合的なリスクのレベルを把握することができる。資産ベースのリスク分析においては、資産ごとのリスク値を、事業被害ベースのリスク分析においては、大きな事業被害をもたらす攻撃ごとのリスク値を把握することができる。

2) 改善箇所の抽出、選定

全体のリスク値を低減するためには、まずリスク値が高い部分を抽出、選定してその改善を検討することが最も効果的である。資産ベースのリスク分析においては、リスク値の高い資産を、事業被害ベースのリスク分析においては、大きな事業被害をもたらす攻撃シナリオと攻撃ツリーを抽出、選定することができる。

3) リスクの低減

資産ベースのリスク分析シートを用いて、改善箇所として選定した資産に対して、リスク値を高くなっている脅威に対する、追加すべき対策項目を検討することができる。事業被害ベースのリスク分析シートを用いて、改善箇所として選定した攻撃シナリオと攻撃ツリーに対して、そのリスク値を低減するために効果的な、対策箇所（攻撃ステップ）と追加すべき対策項目を検討することができる。この検討にあたっては、追加すべき対策項目の優先順位を判断することができる

「サイバー・フィジカル・セキュリティ対策フレームワーク（Version 1.0）」の添付 C には、セキュリティ対策例の一覧が紹介されており、これらを参考にして、自組織におけるセキュリティポリシーの策定及びセキュリティ対策の実装に取り組むことができる。なお、対策例集は、あくまで対策の一例を示すものであり、他の実装を何ら否定するものではない。企業等のセキュリティ対策の実施担当者は、適用対象となる組織やシステムの重要度やリスク分析の結果、取り巻く環境の変化等に応じて、対策例集も参考に適切なセキュリティ対策を検討する必要がある。

4) リスクの低減の効果の把握

3)項で検討した追加すべき対策項目を実施した場合、各対象箇所のリスクの低減とシステム全体におけるリスクの低減として期待される効果を、定量的に把握することができる。また、実際に追加対策を実施した後、期待通りの効果が得られたか否かを、定量的に確認することができる。

5) セキュリティテストの対象箇所の抽出、特定

リスク分析結果と追加対策によるリスクの低減効果を基に、実システムにおけるセキュリティテストの必要性の有無の検討を行う。セキュリティテストは、本番環境、模擬環境等の実機環境を用いた各種のテストのことを指す。これらのテストは、現状のシステム上の不備や机上評価の限界を補うために有効ではあるが、非常に時間とコストがかかるだけでなく、稼動システムへの影響も十分に考慮しなければならない。

従って、リスク分析の結果を活用して、攻撃の懸念が高く、かつ実機での検証が必要と判断される箇所や攻撃を抽出、特定して実施を検討することが、現実的な対応となる。

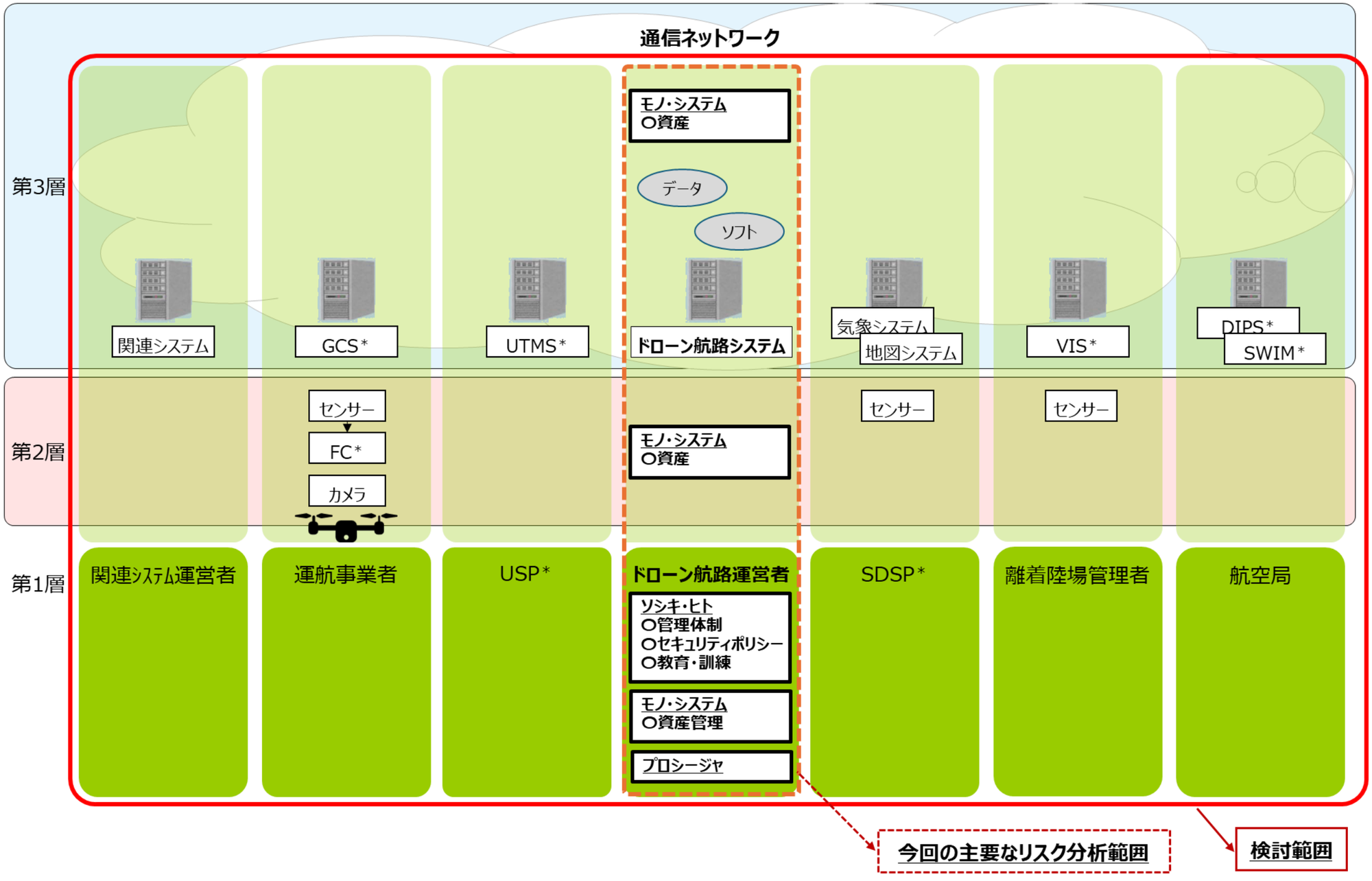
付　録

付録１：分析範囲の決定

（1）三層構造モデルにおける各層の特性、機能・役割、分析対象検討の実施例

特性	機能・役割	分析対象	分析対象の具体的イメージ
第１層 － ドローン航路運営者間のつながり			
個々のドローン航路運営者の適切なガバナンス・マネジメントによって信頼を維持 個々のドローン航路運営者が適切な業務連携によって信頼を維持する	・ドローン航路運営者として平時のリスク管理体制を構築し、適切に運用すること ・ドローン航路運営者としてセキュリティインシデント発生時においても適切に自ドローン航路運営者の事業を継続すること ・フィジカル空間での製品・サービスが、望まれる品質を備えて提供されること **【セキュリティ分析ポイント】** **・ドローン航路運営者単位のセキュリティポリシーを定めて維持すること** **・インシデント発生時のレジリエンスを考慮すること** **【信頼性の基点】** **ドローン航路運営者・マネジメント**	・ドローン航路運営者等で管理されるヒト・モノ・データ・プロシージャ・システム ・上記の要素が管理される場所 ・ドローン航路運営者間のデータ流通 ・ドローン航路運営者と外部システム運営者(管理者)間のデータ流通	・従業員 ・ＩＴ資産 ・セキュリティポリシー ・企業間契約　等
第２層 － フィジカル空間とサイバー空間のつながり			
IoT 機器を介して、フィジカル空間とサイバー空間のつながりが拡大 サイバー空間からのインプットに基づいて、フィジカル空間において作業を実行する機器が増加する	・フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能 ・一定のルールに基づき、サイバー空間から受け取ったデータから、モノを制御したり、データを可視化したりする機能 **【セキュリティ分析ポイント】** **サイバー空間とフィジカル空間との間の転写におけるセキュリティを確保すること** **【信頼性の基点】** **ルールに沿って正しくサイバー空間とフィジカル空間とを転写する機能**	・転写機能に関わるソシキ・ヒト ・正しくサイバー空間とフィジカル空間を転写する機能を備えるモノ・システム ・転写に関するデータ ・転写するプロシージャ	・ジャイロセンサー ・加速度センサー ・気圧センサー ・ビジョンセンサー ・超音波センサー ・磁気方位センサー ・GPS ・カメラの映像情報 ・気象センサー ・ドローンの動態情報 ・認証情報 ・これらの機器等を構成する転写機能に関わる部品　等
第３層 － サイバー空間におけるつながり			
・サイバー空間にて他のドローン航路運営者と相互接続し航路予約。航路の安全確保のため、 ・気象情報やドローンの動態情報等、多様かつ大量なデータを外部システムから収集・蓄積・加工・分析。 ドローン航路運営者や関係機関をまたいで様々なエンドポイントからデータが収集される ストリーミングデータや機密データ等を含む、様々なデータが収集される 複数のデータソースから取得したデータが安全確保のために加工される 自社の蓄積データが、ドローン航路運営者をまたいで様々なエンドポイントからアクセスされる可能性がある サイバー空間におけるデータのサプライチェーンの構成は、動的に変化する	・データを送受信する機能 ・データを加工・分析する機能 ・データを保管する機能 **【セキュリティ分析ポイント】** **サイバー空間におけるデータの送受信等におけるセキュリティを確保すること** **【信頼性の基点】** **データ**	・ドローン航路運営者間や外部システムとの間でデータをやりとりするソシキ・ヒト ・データを送受信、加工、分析、保管するモノ・システム ・ドローン航路運営者間や外部システムとの間で流通するデータ ・ドローン航路運営者間や外部システムとの間でデータを扱う際の共通の規則・プロシージャ	・サーバー、ネットワーク機器 ・ドローン航路システムを構成するハードウェア、ソフトウェア（OS、ミドルウェア、アプリケーション　等） ・流通データ ・データ管理規則、ポリシー　等

（2）分析範囲と資産の配置の概念図検討の実施例



付録２：資産の明確化

資産一覧の実施例

No.		1	2	3	4	5	6	7
		ドローン航路システム						
資産名		端末	ファイアウォール(FW)	ルーター	スイッチ(SW)		サーバー	
							航路画定	航路予約
資産種別	情報系機器	○					○	
	制御系機器							
	ネットワーク資産		○	○	○			
	ソフト資産						○	○
資産の持つ機能	入出力	○				○	○	○
	データ保存					○	○	○
	コマンド発行					○	○	○
	ゲート		○	○	○			
回線種別					LAN			
設置場所		執務室	サーバー室	サーバー室	サーバー室	サーバー室		
接続先NW	情報NW	○	○	○	○		○	
	その他							
管理ポートの接続先			○					
操作I/Fの有無		○						
USBポート／通信I/Fの利用		○	○	○	○		○	
媒体・機器接続の定常運用の有無								
無線機能の有無		○						
定常稼働、非定常稼働		定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働
データの種類と経路		データフローマトリックスに記載						
構築ベンダー／機器メーカー		–	–	–	–	–	–	–
OSの種類／バージョン		Windows	独自OS	独自OS	独自OS	windows server	windows server	windows server
使用するプロトコル		TCP, UDP	TCP, UDP	TCP, UDP	TCP, UDP	TCP, UDP	–	–
役割・機能		・ドローン航路サービスのパラメータ等を入出力するための端末。 ・ドローン航路の安全性を監視するための端末。	・外部のネットワークからの攻撃や侵入を防ぐための機能を有する機器。	・外部ネットワークと接続する機器。	・ネットワークを集線、中継する機器。	・ドローン航路サービスを提供するサーバー。 ・外部システムとの連携。	・航路画定サービス	・航路予約サービス
影響範囲・事業継続への影響		・端末が操作不能になった場合、一定期間、ドローン航路サービス提供が停止する恐れがある。また、端末が乗っ取られた場合、サーバー等への不正アクセスが可能になり、一定期間、ドローン航路サービス提供が停止する恐れがある。 ・機能停止しても複数台設置により事業継続可能。	・フィルタ設定情報が改ざんされると、情報ネットワークからサーバー等への不正アクセスが可能になり、一定期間、ドローン航路サービス提供が停止する恐れがある。 ・機能停止すると、運航事業者を含む外部接続サービスが停止し事業継続不可。	・フィルタ設定情報が改ざんされると、情報ネットワークからサーバー等への不正アクセスが可能になり、一定期間、ドローン航路サービス提供が停止する恐れがある。 ・機能停止すると、運航事業者を含む外部接続サービスが停止し事業継続不可。	・攻撃を受け機能が停止すると、情報ネットワークのアクセスが出来なくなり、一定期間、ドローン航路サービス提供が停止する恐れがある。	・不正アクセスされた場合、サービス停止、重要情報の情報漏洩、改竄等が実行され、長期間、ドローン航路サービス提供が停止する恐れがある。		
セキュリティ対策状況（物理的・運用的）		・機器が設置されている事業者敷地、建屋、執務室には、物理セキュリティ対策（警備員の配置、施錠管理、入退管理等）が実施されている。 ・執務室の機器に物理的にアクセスできる人は、事業者の従業員となっている。	・機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・機器の操作者は、物理的・論理的に、必要最低限の従業員に制限されている。	・機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・機器の操作者は、物理的・論理的に、必要最低限の従業員に制限されている。	・機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・機器の操作者は、物理的・論理的に、必要最低限の従業員に制限されている。	・機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・機器の操作者は、物理的・論理的に、必要最低限の従業員に制限されている。		
セキュリティ対策状況（技術的）		・OSはWindowsで、アップデートを随時適用している。 ・情報系システムの一般的なセキュリティ対策がされており、アンチウィルス、メールフィルタ、Webフィルタ等の対策製品を使用している。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。	・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは管理者のみで、操作者用アカウントはない。リモート管理機能は、管理者アカウントのみ利用可能。 ・ファイアウォールはパケットフィルタ型で、ファイアウォールルールの許可通信を適用。 ・ファイアウォールのファームウェアアップデートを随時実施。アップデートタイミングは保守ベンダー主導で実施する。	・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは管理者のみで、操作者用アカウントはない。リモート管理機能は、管理者アカウントのみ利用可能。 ・ルーターのファームウェアアップデートを随時実施。アップデートタイミングは保守ベンダー主導で実施する。	・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは管理者のみで、操作者用アカウントはない。リモート管理機能は、管理者アカウントのみ利用可能。 ・スイッチのファームウェアアップデートを随時実施。アップデートタイミングは保守ベンダー主導で実施する。	・OSはWindowsで、アップデートを随時適用している。 ・情報系システムの一般的なセキュリティ対策がされている。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは管理者のみで、リモート管理機能は管理者アカウントのみ利用可能。 ・バックアップ間隔は日次で、3世代分を保管。		

資産一覧の実施例（続き）

No.		8	9	10	11	12	13	14
		ドローン航路システム				外部システム		
資産名		サーバー				関連システム	ドローン	
		安全管理	離着陸場/機体管理	外部データ参照	ユーザー認証		GCS	機体
資産種別	情報系機器	○				○	○	
	制御系機器							○
	ネットワーク資産							
	ソフト資産	○	○	○	○			
資産の持つ機能	入出力	○	○	○	○	○	○	○
	データ保存	○	○	○	○		○	
	コマンド発行	○	○	○	○		○	
	ゲート							
回線種別								
設置場所		サーバー室						
接続先NW	情報NW	○						
	その他					インターネット	インターネット	インターネット
管理ポートの接続先								
操作I/Fの有無								
USBポート／通信I/Fの利用		○				○	○	○
媒体・機器接続の定常運用の有無								○
無線機能の有無								○
定常稼働、非定常稼働		定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働
データの種類と経路		データフローマトリックスに記載						
構築ベンダー／機器メーカー		–	–	–	–	–	–	–
OSの種類／バージョン		windows server	windows server	windows server	windows server	windows server	Windows	独自OS
使用するプロトコル		–	–	–	–	TCP, UDP	TCP, UDP	TCP, UDP
役割・機能		・安全管理サービス	・離着陸場管理サービス ・機体管理サービス	・外部データ参照サービス	・ユーザー認証サービス	・認証や決済機能	・ドローンの制御	・ドローン本体
影響範囲・事業継続への影響		・不正アクセスされた場合、サービス停止、重要情報の情報漏洩、改竄等が実行され、長期間、ドローン航路サービス提供が停止する恐れがある。				・データの改竄や機能停止されると、認証や決済機能が停止し、一定期間、ドローン航路サービスの提供が停止する恐れがある。	・通信妨害や機能停止されると、飛行中のドローンの制御や動態状況把握が出来なくなり、一定期間、ドローン航路サービス提供が停止する恐れがある。	・通信妨害や機能停止されると、飛行中の航路逸脱や墜落が生じる恐れがあり、一定期間、ドローン航路サービス提供が停止する恐れがある。
セキュリティ対策状況（物理的・運用的）		・機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・機器の操作者は、物理的・論理的に、必要最低限の従業員に制限されている。				・機器が設置されている事業者敷地、建屋、執務室には、物理セキュリティ対策（警備員の配置、施錠管理、入退管理等）が実施されている。 ・執務室の機器に物理的にアクセスできる人は、事業者の従業員となっている。	・機器の操作者は、物理的・論理的に、必要最低限の従業員に制限されている。	・機器の操作者は、物理的・論理的に、必要最低限の従業員に制限されている。
セキュリティ対策状況（技術的）		・OSはWindowsで、アップデートを随時適用している。 ・情報系システムの一般的なセキュリティ対策がされている。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは管理者のみで、リモート管理機能は管理者アカウントのみ利用可能。 ・バックアップ間隔は日次で、3世代分を保管。				・OSはWindowsで、アップデートを随時適用している。 ・情報系システムの一般的なセキュリティ対策がされており、アンチウィルス、メールフィルタ、Webフィルタ等の対策製品を使用している。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。	・OSはWindowsで、アップデートを随時適用している。 ・情報系システムの一般的なセキュリティ対策がされており、アンチウィルス、メールフィルタ、Webフィルタ等の対策製品を使用している。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。	・ログイン時はユーザ認証あり。 ・アカウントは管理者のみで、操作者用アカウントはない。 ・ファームウェアアップデートを随時実施。アップデートタイミングは保守ベンダー主導で実施する。

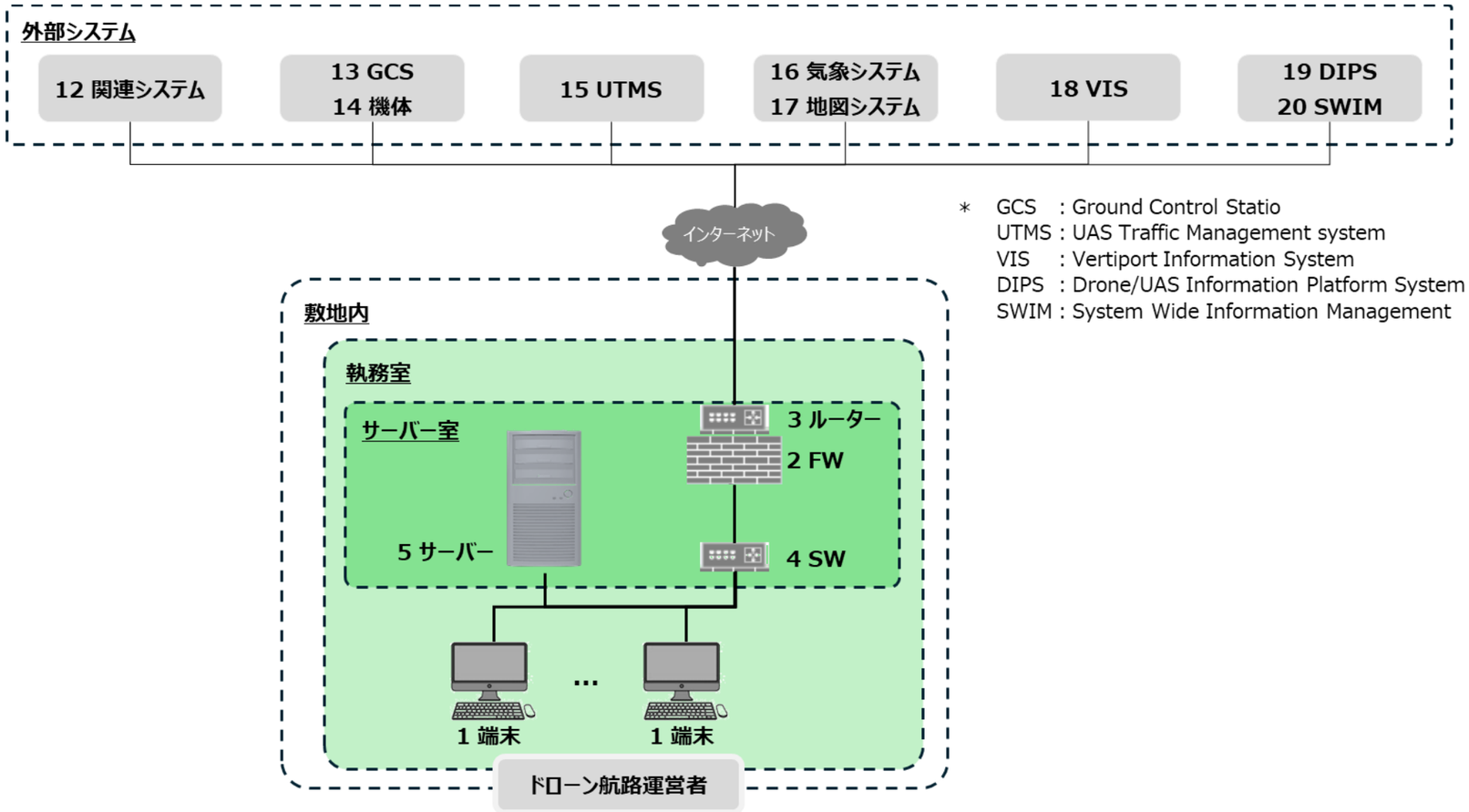
資産一覧の実施例（続き）

資産		15	16	17	18	19	20
		外部システム					
資産名		UTMS	SDSP		VIS	航空局	
			気象システム	地図システム		DIPS	SWIM
資産種別	情報系機器	○	○	○	○	○	○
	制御系機器						
	ネットワーク資産						
	ソフト資産						
資産の持つ機能	入出力	○	○	○	○	○	○
	データ保存					○	○
	コマンド発行						
	ゲート						
回線種別							
設置場所							
接続先NW	情報NW						
	その他	インターネット	インターネット	インターネット	インターネット	インターネット	インターネット
管理ポートの接続先							
操作I/Fの有無							
USBポート／通信I/Fの利用		○	○	○	○	○	○
媒体・機器接続の定常運用の有無							
無線機能の有無							
定常稼働、非定常稼働		定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働
データの種類と経路		データフローマトリックスに記載					
構築ベンダー／機器メーカー		※	※	※	※	※	※
OSの種類／バージョン		※	※	※	※	※	※
使用するプロトコル		※	※	※	※	※	※
役割・機能		・空域を飛行するドローンの運航管理	・気象情報を提供	・地形情報を提供	・ポートの利用状況を提供	・飛行計画の受付・登録	・ドローン航路を登録
影響範囲・事業継続への影響		・データの改竄や機能停止されると、飛行中の適合性評価やドローンの動態状況把握が出来なくなり、間接的に一定期間、ドローン航路サービス提供が停止する恐れがある。	・データの改竄や機能停止されると、気象情報ベースの安全性評価が出来なくなり、間接的に一定期間、ドローン航路サービス提供が停止する恐れがある。	・データの改竄や機能停止されると、計画段階での地形情報ベースの安全性評価が出来なくなり、間接的に一定期間、一部のドローン航路サービス提供が停止する恐れがある。	・データの改竄や機能停止されると、離着陸場予約、飛行中のポート位置情報や開閉状況等の安全性評価が出来なくなり、間接的に一定期間、ドローン航路サービス提供が停止する恐れがある。	・データの改竄や機能停止されると、飛行計画の登録が出来なくなり、間接的に一定期間、一部のドローン航路サービス提供が停止する恐れがある。	・データの改竄や機能停止されると、ドローン航路情報の登録/修正/削除が出来なくなり、間接的に一定期間、一部のドローン航路サービス提供が停止する恐れがある。
セキュリティ対策状況（物理的・運用的）		※	※	※	※	※	※
セキュリティ対策状況（技術的）		※	※	※	※	※	※

(※)実施例の表ではあるが、外部システムに関する仕様は機微情報に当たるため非表示とする。

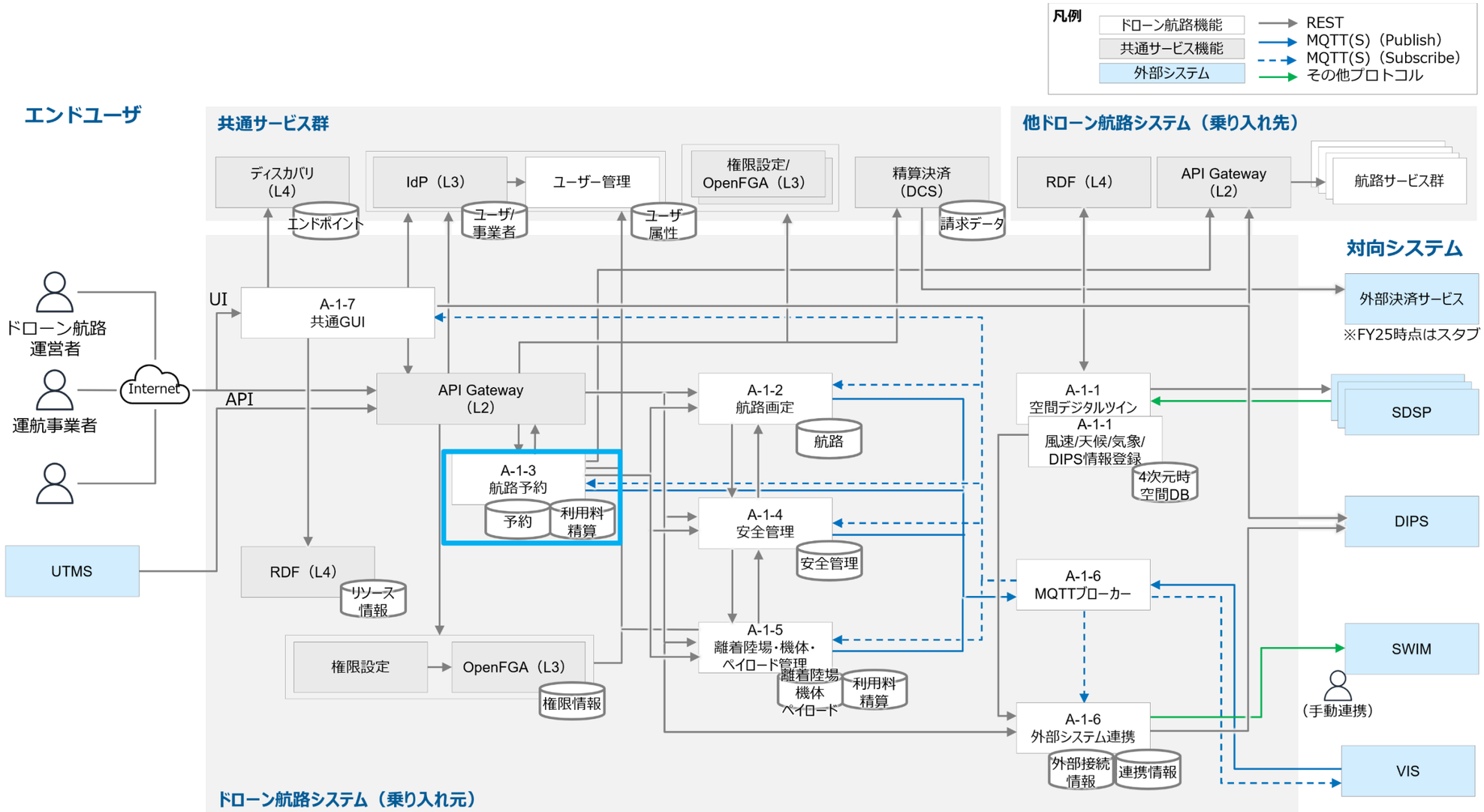
付録３：システム構成の明確化

（１）システム構成図（ハードウェア）の実施例



ハードウェア構成図の実施例

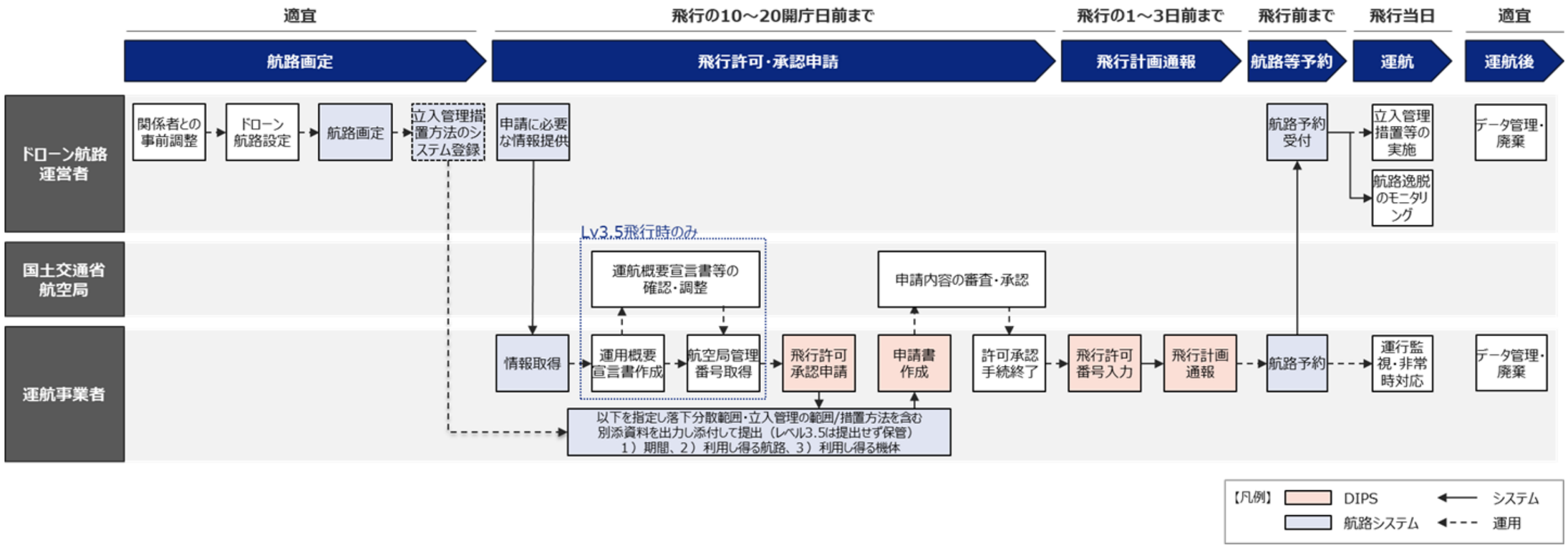
（１）システム構成図（ソフトウェア）の実施例



ソフトウェア構成図の実施例

付録 4：データフローの明確化

（1）業務フロー図の実施例



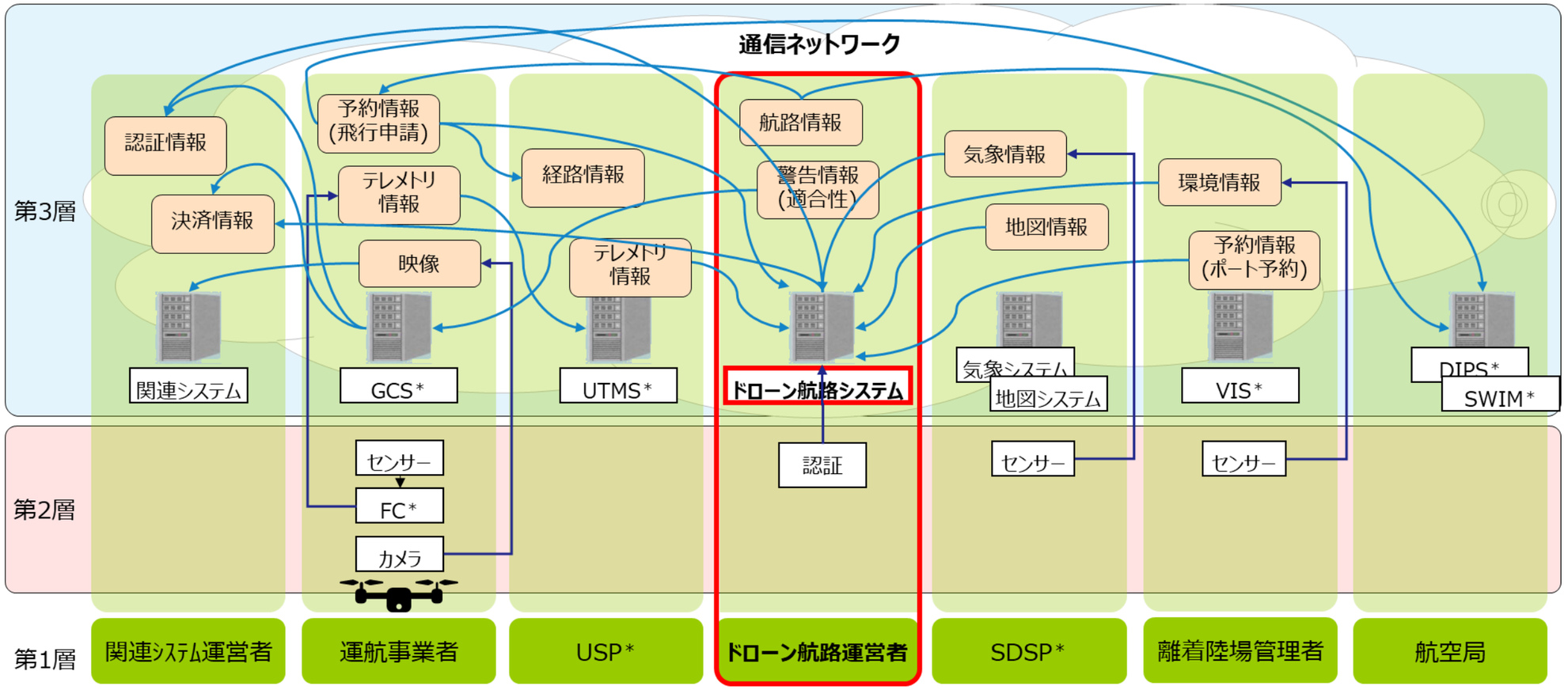
業務フロー図の実施例

（2）データフローマトリックスの実施例

送信側＼受信側		経路	端末	サーバー						外部システム							
				航路画定	航路予約	安全管理	離着陸場/機体管理	外部データ参照	ユーザー認証	関連システム	運航事業者(GCS)	USP(UTMS)	SDSP(地図システム)	SDSP(気象システム)	離着陸場管理者(VIS)	航空局(DIPS)	航空局(SWIM)
端末		情報NW		業務コマンド	業務コマンド		業務コマンド		認証情報/ユーザー情報	認証情報/ユーザー情報							
サーバー	航路画定	情報NW	航路情報								航路情報						航路情報
	航路予約	情報NW	予約情報								予約情報					予約情報	
	安全管理	情報NW	逸脱情報								逸脱情報						
	離着陸場/機体管理	情報NW	離着陸場/機体情報								離着陸場/機体情報						
	外部データ参照	情報NW	環境情報/地図情報								環境情報/地図情報						
	ユーザー認証	情報NW	認可情報								認可情報						
外部システム	関連システム	インターネット															
	運航事業者(GCS)	インターネット				動態情報			認証情報/ユーザー情報								
	USP(UTMS)	インターネット				動態情報			認証情報/ユーザー情報								
	SDSP(地図システム)	インターネット				地図情報			認証情報/ユーザー情報								
	SDSP(気象システム)	インターネット				気象情報			認証情報/ユーザー情報								
	ポート管理者(VIS)	インターネット				ポート情報			認証情報/ユーザー情報								
	航空局(DIPS)	インターネット															
	航空局(SWIM)	インターネット															

データフローマトリックスの実施例

（3）データフロー図の実施例



＊ GCS : Ground Control Statio
UTMS : UAS Traffic Management system
VIS : Vertiport Information System

DIPS : Drone/UAS Information Platform System
SWIM : System Wide Information Management
FC : Flight Controller

USP : UTM Service Providers
SDSP : supplemental data supply Providers

データフロー図の実施例

（4）業務・データフロー図の実施例

「外部データ参照」業務を一例に、業務・データフロー図の実施例を示す。本シートは、各業務資産で整理する。

・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）	データ参照				OpenStreetMap（地理院地図） WeatherNews 気象庁 VIS DIPS	＜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）	データ参照					＜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・データフロー図の実施例

付録 5：資産重要度の検討

重要度一覧の実施例

項番	資産		重要度	判断基準
1	端末		2	・端末が操作不能になった場合、予約業務や安全管理業務等、一定期間、ドローン航路サービス提供が停止する恐れがある。また、端末が乗っ取られた場合、サーバー等への不正アクセスが可能になり、一定期間、ドローン航路サービス提供が停止する恐れがある。 ・機能停止しても複数台設置により事業継続可能。
2	ファイアウォール		2	・フィルタ設定情報が改竄されると、情報ネットワークからサーバー等への不正アクセスが可能になり、一定期間、ドローン航路サービス提供が停止する恐れがある。 ・機能停止すると、運航事業者を含む外部接続サービスが停止し事業継続不可。
3	ルーター		2	・フィルタ設定情報が改竄されると、情報ネットワークからサーバー等への不正アクセスが可能になり、一定期間、ドローン航路サービス提供が停止する恐れがある。 ・機能停止すると、運航事業者を含む外部接続サービスが停止し事業継続不可。
4	スイッチ		2	・攻撃を受け機能が停止すると、情報ネットワークのアクセスが出来なくなり、一定期間、ドローン航路サービス提供が停止する恐れがある。
5	サーバー		3	・不正アクセスされた場合、サービス停止、重要情報の情報漏洩、改竄等が実行され、長期間、ドローン航路サービス提供が停止する恐れがある。
6	サーバー	航路画定	3	
7		航路予約	3	
8		安全管理	3	
9		離着陸場/機体管理	3	
10		外部データ参照	3	
11		ユーザ認証	3	
12	関連システム		2	・データの改竄や機能停止されると、認証や決済機能が停止し、間接的に一定期間、ドローン航路サービスの提供が停止する恐れがある。
13	ドローン	GCS	2	・通信妨害や機能停止されると、飛行中のドローンの制御や動態状況把握が出来なくなり、間接的に一定期間、ドローン航路サービス提供が停止する恐れがある。
14		機体	2	・通信妨害や機能停止されると、飛行中の飛行経路計画可能空間逸脱や墜落が生じる恐れがあり、一定期間、ドローン航路サービス提供が停止する恐れがある。
15	UTMS		2	・データの改竄や機能停止されると、飛行中の適合性評価やドローンの動態状況把握が出来なくなり、間接的に一定期間、ドローン航路サービス提供が停止する恐れがある。
16	SDSP	気象システム	2	・データの改竄や機能停止されると、気象情報ベースの安全性評価が出来なくなり、間接的に一定期間、ドローン航路サービス提供が停止する恐れがある。
17		地図システム	1	・データの改竄や機能停止されると、計画段階で、最新の地形情報の入手が出来なくなり、間接的に一定期間、一部のドローン航路サービス提供が停止する恐れがある。
18	VIS		2	・データの改竄や機能停止されると、離着陸場予約、飛行中の離着陸場位置情報や開閉状況等の安全性評価が出来なくなり、間接的に一定期間、ドローン航路サービス提供が停止する恐れがある。
19	航空局	DIPS	1	・データの改竄や機能停止されると、飛行計画の登録が出来なくなり、間接的に一定期間、一部のドローン航路サービス提供が停止する恐れがある。
20		SWIM	1	・データの改竄や機能停止されると、ドローン航路の登録が出来なくなり、間接的に一定期間、一部のドローン航路サービス提供が停止する恐れがある。

（凡例）資産重要度：被害大：3 ＞ 被害中：2 ＞被害小：1

付録 6：事業被害一覧と事業被害レベルの検討

事業被害一覧と事業被害レベルの実施例

項番	事業被害	事業被害の概要	事業被害レベル	根拠
1	ドローン航路サービスの長期間サービス提供停止	サーバーへのサイバー攻撃により、業務コマンドを悪用されてサービス停止、重要情報の改竄/破壊等が実行され、ドローン航路サービス提供が長期間停止する。	3	長期間サービス提供できず、運航事業者との契約が解除される恐れがあるため、レベル「3」の評価とする。
2	ドローン航路サービスの一定期間サービス提供停止	端末へのサイバー攻撃により、操作不能になった場合、一定期間、ドローン航路サービス提供が停止する恐れがある。 また、端末が乗っ取られた場合、サーバー等への不正アクセスが可能になり、一定期間、ドローン航路サービス提供が停止する。	2	端末機能が停止しても、複数台設置により事業継続可能。一定期間サービス提供できないが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
3		ネットワーク機器へのサイバー攻撃により、フィルタ設定情報が改ざんされると、情報ネットワークからサーバー等への不正アクセスが可能になり、一定期間、ドローン航路サービス提供が停止する。	2	一定期間サービス提供できないが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
4		関連システムへのサイバー攻撃により、認証情報や決済情報が改竄されたり、認証や決済機能が停止し、間接的に一定期間、ドローン航路サービス提供が停止する。	2	一定期間サービス提供ができないが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
5		GCS/機体/UTMSへのサイバー攻撃により、動態情報が改竄されたり、受信が停止して安全性評価が出来なくなり、間接的に一定期間、ドローン航路サービス提供が停止する。	2	一定期間サービス提供できないが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
6		気象システムへのサイバー攻撃により、気象情報が改竄されたり、受信が停止して、気象情報ベースの安全性評価が出来なくなり、間接的に一定期間、ドローン航路サービス提供が停止する。	2	一定期間サービス提供できないが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
7		地図システムへのサイバー攻撃により、地図情報が改竄されたり、受信が停止して、計画段階で、最新の地形情報の入手が出来なくなり、間接的に一定期間、一部のドローン航路サービス提供が停止する。	1	一定期間、計画段階で使用する一部のサービス提供ができない恐れがあるが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「1」の評価とする。
8		VISへのサイバー攻撃により、ポート予約情報、ポート位置情報、開閉情報等が改竄されたり、受信が停止して、安全性評価が出来なくなり、間接的に一定期間、ドローン航路サービス提供が停止する。	2	一定期間サービス提供できないが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
9		DIPSへのサイバー攻撃により、飛行計画の登録が出来なくなり、間接的に一定期間、一部のドローン航路サービス提供が停止する。	1	一定期間、計画段階で使用する一部のサービス提供ができない恐れがあるが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「1」の評価とする。
10		SWIMへのサイバー攻撃により、ドローン航路情報の登録/修正/削除が出来なくなり、間接的に一定期間、一部のドローン航路サービス提供が停止する。	1	一定期間、計画段階で使用する一部のサービス提供ができない恐れがあるが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「1」の評価とする。
11	ドローン航路内外でのドローン墜落	GCSや機体へのサイバー攻撃により、ドローンの乗っ取りや通信妨害等が実行されて墜落し、ドローン航路を一時封鎖する必要があるため、ドローン航路サービス提供が一定期間停止する。	2	一定期間サービス提供できないが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
12	ドローン航路からの逸脱	GCSや機体へのサイバー攻撃により、ドローンの乗っ取りや通信妨害等が実行されて航路を逸脱し、ドローン航路を一時封鎖する必要があるため、ドローン航路サービス提供が一定期間停止する。	2	一定期間サービス提供できないが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
13		GCSや機体へのサイバー攻撃により、ドローンの乗っ取りや通信妨害等が実行されてドローンを紛失し、ドローン航路を一時封鎖する必要があるため、ドローン航路サービス提供が一定期間停止する。	2	一定期間サービス提供できないが、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
14	機密情報の漏洩	サーバーへのサイバー攻撃により、重要情報(航路情報/ポート情報/機体情報/運航計画/飛行ログ等)が外部に漏洩し、信頼が大きく低下する。	3	信用失墜により、運航事業者との契約が解除される恐れがあるため、レベル「3」の評価とする。
15		関連システムへのサイバー攻撃により、重要情報(認証情報/決済情報等)が外部に漏洩し、信頼が低下するとともに、一定期間、一部のドローン航路サービスの提供が停止する。	1	信頼は低下するが、一定期間、計画段階で使用する一部のサービス提供ができないレベルの被害に留まると想定され、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「1」の評価とする。
16		GCSへのサイバー攻撃により、重要情報(航路情報/ポート情報/機体情報/運航計画/飛行ログ等)が外部に漏洩し、信頼が低下するとともに、一定期間、ドローン航路サービスの提供が停止する。	2	信頼は低下するが、一定期間、サービス提供ができないレベルの被害に留まると想定され、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
17		機体へのサイバー攻撃により、重要情報(航路情報/ポート情報/機体情報/運航計画/飛行ログ等)が外部に漏洩し、信頼が低下するとともに、一定期間、ドローン航路サービスの提供が停止する。	2	信頼は低下するが、一定期間、サービス提供ができないレベルの被害に留まると想定され、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
18		UTMSへのサイバー攻撃により、重要情報(運航計画/飛行ログ等)が外部に漏洩し、信頼が低下するとともに、一定期間、ドローン航路サービスの提供が停止する。	2	信頼は低下するが、一定期間、サービス提供ができないレベルの被害に留まると想定され、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
19		VISへのサイバー攻撃により、重要情報(ポート情報等)が外部に漏洩し、信頼が低下するとともに、一定期間、ドローン航路サービスの提供が停止する。	2	信頼は低下するが、一定期間、サービス提供ができないレベルの被害に留まると想定され、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「2」の評価とする。
20		DIPSへのサイバー攻撃により、重要情報(航路情報/ポート情報/機体情報/運航計画/飛行ログ等)が外部に漏洩し、信頼が低下するとともに、一定期間、一部のドローン航路サービスの提供が停止する。	1	信頼は低下するが、一定期間、一部のサービス提供ができないレベルの被害に留まると想定され、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「1」の評価とする。
21		SWIMへのサイバー攻撃により、重要情報(航路情報/ポート情報等)が外部に漏洩し、信頼が低下するとともに、一定期間、一部のドローン航路サービスの提供が停止する。	1	信頼は低下するが、一定期間、一部のサービス提供ができないレベルの被害に留まると想定され、運航事業者との契約が解除されるまでは至らないと想定されるため、レベル「1」の評価とする。

（凡例）事業被害レベル：被害大：3 ＞ 被害中：2 ＞被害小：1

付録 7：資産ベースのリスク分析

（１）資産に想定される脅威一覧の実施例

資産 / 脅威	1 端末	2 ファイアウォール (FW)	3 ルーター	4 スイッチ (SW)	5 サーバー	6 航路画定	7 航路予約	8 安全管理	9 離着陸場/機体管理	10 外部データ参照	11 ユーザー認証
情報系資産	○				○						
ネットワーク資産		○	○	○							
ソフト資産						○	○	○	○	○	○
外部資産											
不正アクセス	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
物理的侵入	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
不正操作	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
過失操作	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
不正媒体・機器接続	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
プロセス不正実行	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
マルウェア感染	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
情報窃取	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
情報改ざん	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
情報破壊	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
不正送信	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
機能停止	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
制御不能・異常動作	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
高負荷攻撃	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
窃盗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
盗難・廃棄時の情報窃取	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
経路遮断		✓	✓	✓							
通信輻輳		✓	✓	✓							
無線妨害											
盗聴		✓	✓	✓							
通信データ改ざん		✓	✓	✓							
不正機器接続		✓	✓	✓							

（凡例）✓印：各資産に想定される脅威

資産に想定される脅威一覧の実施例（続き）

資産 / 脅威	外部システム								
	12 関連システム	13 GCS	14 機体	15 UTMS	16 気象システム	17 地図システム	18 VIS	19 DIPS	20 SWIM
情報系資産									
ネットワーク資産									
ソフト資産									
外部資産	○	○	○	○	○	○	○	○	○
不正アクセス	✓	✓	✓	✓	✓	✓	✓	✓	✓
物理的侵入	✓	✓	✓	✓	✓	✓	✓	✓	✓
不正操作	✓	✓	✓	✓	✓	✓	✓	✓	✓
過失操作	✓	✓	✓	✓	✓	✓	✓	✓	✓
不正媒体･機器接続	✓	✓	✓	✓	✓	✓	✓	✓	✓
プロセス不正実行	✓	✓	✓	✓	✓	✓	✓	✓	✓
マルウェア感染	✓	✓	✓	✓	✓	✓	✓	✓	✓
情報窃取	✓	✓	✓	✓	✓	✓	✓	✓	✓
情報改ざん	✓	✓	✓	✓	✓	✓	✓	✓	✓
情報破壊	✓	✓	✓	✓	✓	✓	✓	✓	✓
不正送信	✓	✓	✓	✓	✓	✓	✓	✓	✓
機能停止	✓	✓	✓	✓	✓	✓	✓	✓	✓
制御不能･異常動作	✓	✓	✓	✓	✓	✓	✓	✓	✓
高負荷攻撃	✓	✓	✓	✓	✓	✓	✓	✓	✓
窃盗									
盗難･廃棄時の情報窃取									
経路遮断	✓	✓	✓	✓	✓	✓	✓	✓	✓
通信輻輳	✓	✓	✓	✓	✓	✓	✓	✓	✓
無線妨害		✓	✓						
盗聴	✓	✓	✓	✓			✓	✓	✓
通信データ改ざん	✓	✓	✓	✓	✓	✓	✓	✓	✓
不正機器接続									

（凡例）✓印：各資産に想定される脅威

（２）脅威レベルまとめ表の実施例

資産 / 脅威	1 端末	2 ファイアウォール (FW)	3 ルーター	4 スイッチ (SW)	5 サーバー	6 画定	7 航路予約	8 安全管理	9 離着陸場/機体管理	10 外部データ参照	11 ユーザー認証
情報系資産	○				○						
ネットワーク資産		○	○	○							
ソフト資産						○	○	○	○	○	○
外部資産											
不正アクセス	2	2	2	2	3	3	3	3	3	3	3
物理的侵入	2	2	2	2	3	3	3	3	3	3	3
不正操作	2	2	2	2	3	3	3	3	3	3	3
過失操作	2	2	2	2	3	3	3	3	3	3	3
不正媒体・機器接続	2	2	2	2	3	3	3	3	3	3	3
プロセス不正実行	2	2	1	1	3	3	3	3	3	3	3
マルウェア感染	2	2	1	1	3	3	3	3	3	3	3
情報窃取	2	2	1	1	3	3	3	3	3	3	3
情報改ざん	2	2	1	1	3	3	3	3	3	3	3
情報破壊	2	2	1	1	3	3	3	3	3	3	3
不正送信	2	2	1	1	3	3	3	3	3	3	3
機能停止	2	2	1	1	3	3	3	3	3	3	3
制御不能・異常動作	2	2	1	1	3	3	3	3	3	3	3
高負荷攻撃	2	2	2	2	2	2	2	2	2	2	2
窃盗	2	2	2	2	1	1	1	1	1	1	1
盗難・廃棄時の情報窃取	2	2	2	2	1	1	1	1	1	1	1
経路遮断		2	2	2							
通信輻輳		2	2	2							
無線妨害											
盗聴		2	2	2							
通信データ改ざん		2	2	2							
不正機器接続		2	2	2							

（凡例）脅威レベル：発生可能性大：３ ＞ 発生可能性中：２ ＞発生可能性小：1

脅威レベルまとめ表の実施例（続き）

資産 / 脅威	外部システム								
	12 関連システム	13 GCS	14 機体	15 UTMS	16 気象システム	17 地図システム	18 VIS	19 DIPS	20 SWIM
情報系資産									
ネットワーク資産									
ソフト資産									
外部資産	○	○	○	○	○	○	○	○	○
不正アクセス	2	2	2	2	2	1	2	1	1
物理的侵入	2	2	2	2	2	1	2	1	1
不正操作	2	2	2	2	2	1	2	1	1
過失操作	2	2	2	2	2	1	2	1	1
不正媒体・機器接続	2	2	2	2	2	1	2	1	1
プロセス不正実行	2	2	2	2	2	1	2	1	1
マルウェア感染	2	2	2	2	2	1	2	1	1
情報窃取	2	2	2	2	2	1	2	1	1
情報改ざん	2	2	2	2	2	1	2	1	1
情報破壊	2	2	2	2	2	1	2	1	1
不正送信	2	2	2	2	2	1	2	1	1
機能停止	2	2	2	2	2	1	2	1	1
制御不能・異常動作	2	2	2	2	2	1	2	1	1
高負荷攻撃	2	2	2	2	2	1	2	1	1
窃盗									
盗難・廃棄時の情報窃取									
経路遮断	2	2	2	2	2	1	2	1	1
通信輻輳	2	2	2	2	2	1	2	1	1
無線妨害		2	2						
盗聴	2	2	2	2			2	1	1
通信データ改ざん	2	2	2	2	2	1	2	1	1
不正機器接続									

（凡例）脅威レベル：発生可能性大：3 ＞ 発生可能性中：2 ＞発生可能性小：1

（３）脅威レベル設定根拠の実施例

資産 / 脅威	根拠										
	1 端末	2 ファイアウォール	3 ルーター	4 スイッチ	5 サーバー	6 航路画定	7 航路予約	8 安全管理	9 離着陸場/機体管理	10 外部データ参照	11 ユーザー認証
情報系資産	○				○						
ネットワーク資産		○	○	○							
ソフト資産						○	○	○	○	○	○
外部資産											
不正アクセス	ハッキングツールが存在するため、一定スキルを持った攻撃者により可能。				サーバーへの攻撃により、情報漏洩や改竄等が実行され、信頼が低下したり、長期間、ドローン航路サービスが停止したりする。						
物理的侵入	一定のソーシャルエンジニアリング能力（構内侵入等）を持った攻撃者により可能。										
不正操作	スキルを問わず,物理的に侵入すれば、攻撃者により操作可能。										
過失操作	システムに精通した攻撃者による、内部関係者の過失操作の誘発と攻撃が可能。										
不正媒体・機器接続	スキルを問わず、物理的に侵入すれば、不正持ち込み媒体・機器のシステム構成機器への接続と攻撃実行が可能。										
プロセス不正実行	一定スキルを持った攻撃者により可能。										
マルウェア感染	メールの添付ファイル開封／リンク押下等によりマルウェア攻撃が可能。										
情報窃取	マルウェアに感染した場合、容易に攻撃が可能。										
情報改ざん											
情報破壊											
不正送信											
機能停止											
制御不能・異常動作											
高負荷攻撃	DDoS 攻撃等によって、正常動作を妨害する攻撃が可能。										
窃盗	一定のソーシャルエンジニアリング能力（構内侵入等）を持った攻撃者により可能。				サーバーの窃盗は、可能性が低い。						
盗難・廃棄時の情報窃取	盗難にあった機器や廃棄した機器のリバースエンジニアリングにより情報窃取が可能。										
経路遮断	対象外		ハッキングツールが存在するため、一定スキルを持った攻撃者により可能。		対象外						
通信輻輳			対象外								
無線妨害											
盗聴			ハッキングツールが存在するため、一定スキルを持った攻撃者により可能。								
通信データ改ざん											
不正機器接続											

脅威レベル設定根拠の実施例（続き）

<table>
<tr><th rowspan="2">資 産
脅 威</th><th colspan="9">根拠</th></tr>
<tr><th>12 関連システム</th><th>13 GCS</th><th>14 機体</th><th>15 UTMS</th><th>16 気象システム</th><th>17 地図システム</th><th>18 VIS</th><th>19 DIPS</th><th>20 SWIM</th></tr>
<tr><td>情報系資産</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>ネットワーク資産</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>ソフト資産</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>外部資産</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td><td>○</td></tr>
<tr><td>不正アクセス</td><td rowspan="10">＊１</td><td colspan="3" rowspan="10">・GCS/機体/UTMSへの攻撃により、動態情報が改竄されたり、受信が停止して安全性評価が出来なくなり、一定期間
サービスが停止する。
・GCS/機体への攻撃により、ドローンの乗っ取りや通信妨害等が実行され、墜落したり、航路を逸脱したり、機体を紛失したりして、ドローン航路を一時封鎖する必要があるため、一定期間サービスが停止する。</td><td rowspan="10">＊５</td><td rowspan="10">＊６</td><td rowspan="10">＊７</td><td rowspan="10">＊９</td><td rowspan="10">＊１１</td></tr>
<tr><td>物理的侵入</td></tr>
<tr><td>不正操作</td></tr>
<tr><td>過失操作</td></tr>
<tr><td>不正媒体・機器接続</td></tr>
<tr><td>プロセス不正実行</td></tr>
<tr><td>マルウェア感染</td></tr>
<tr><td>　情報窃取</td></tr>
<tr><td>　情報改ざん</td></tr>
<tr><td>　情報破壊</td></tr>
<tr><td>　不正送信</td></tr>
<tr><td>　機能停止</td></tr>
<tr><td>　制御不能・異常動作</td></tr>
<tr><td>高負荷攻撃</td></tr>
<tr><td>窃盗</td><td colspan="9" rowspan="2">対象外</td></tr>
<tr><td>　盗難・廃棄時の情報窃取</td></tr>
<tr><td>経路遮断</td><td rowspan="2">＊１</td><td colspan="3" rowspan="2">＊３</td><td rowspan="2">＊５</td><td rowspan="2">＊６</td><td rowspan="2">＊７</td><td rowspan="2">＊９</td><td rowspan="2">＊１１</td></tr>
<tr><td>通信輻輳</td></tr>
<tr><td>無線妨害</td><td>対象外</td><td colspan="2">＊３</td><td colspan="7">対象外</td></tr>
<tr><td>盗聴</td><td rowspan="2">＊２</td><td colspan="3">＊４</td><td colspan="2">対象外</td><td>＊８</td><td>＊１０</td><td>＊１２</td></tr>
<tr><td>通信データ改ざん</td><td colspan="3">＊３</td><td>＊５</td><td>＊６</td><td>＊７</td><td>＊９</td><td>＊１１</td></tr>
<tr><td>不正機器接続</td><td colspan="9">対象外</td></tr>
</table>

＊１： 関連システムへの攻撃により、認証情報や決済情報が改竄されたり、認証や決済機能が停止し、一定期間サービスが停止する。

＊２： 関連システムへの攻撃により、認証情報や決済情報が漏洩し、信頼が低下するとともに、一定期間サービスが停止する。

＊３： 通信路や無線への攻撃により、動態情報の受信が停止して安全性評価が出来なくなったり、墜落したり、航路を逸脱したり、機体を紛失したりして、ドローン航路を一時封鎖する必要があるため、一定期間、サービスが停止する。

＊４： GCS/機体/UTMSへの攻撃により、動態情報が漏洩し、信頼が低下するとともに、一定期間、サービスが停止する。

＊５： 気象システムへの攻撃により、気象情報が改竄されたり、受信が停止して安全性評価が出来なくなり、一定期間サービスが停止する。

＊６： 地図システムへの攻撃により、地図情報が改竄されたり、受信が停止して安全性評価が出来なくなり、一定期間、計画段階で使用する一部のサービスが停止する。

＊７： VISへの攻撃により、ポート情報が改竄されたり、受信が停止して安全性評価が出来なくなったり、墜落したり、航路を逸脱したり、機体を紛失したりして、ドローン航路を一時封鎖する必要があるため、一定期間サービスが停止する。

＊８： VISへの攻撃により、ポート情報が漏洩し、信頼が低下するとともに、一定期間、サービスが停止する。

＊９： DIPSへの攻撃により、飛行計画の登録が出来なくなり、一定期間、一部のドローン航路サービスが停止する。

＊１０： DIPSへの攻撃により、重要情報(航路情報/ポート情報/機体情報/運航計画/飛行ログ等)が漏洩し、信頼が低下するとともに、一定期間、一部のサービスが停止する。

＊１１： SWIMへの攻撃により、ドローン航路情報の登録/修正/削除が出来なくなり、一定期間、一部のドローン航路サービスが停止する。

＊１２： SWIMへの攻撃により、重要情報(航路情報/ポート情報等)が漏洩し、信頼が低下するとともに、一定期間、一部のサービスが停止する。

（４）脆弱性レベルまとめ表の実施例

資産 / 脅威	1 端末	2 ファイアウォール (FW)	3 ルーター	4 スイッチ (SW)	5 サーバー	6 画定	7 航路予約	8 安全管理	9 離着陸場/機体管理	10 外部データ参照	11 ユーザー認証
不正アクセス	2	2	2	2	2	2	2	2	2	2	2
物理的侵入	2	2	2	2	2	2	2	2	2	2	2
不正操作	2	2	2	2	2	2	2	2	2	2	2
過失操作	2	2	2	2	2	2	2	2	2	2	2
不正媒体・機器接続	2	2	2	2	2	2	2	2	2	2	2
プロセス不正実行	2	2	2	2	2	2	2	2	2	2	2
マルウェア感染	2	2	2	2	2	2	2	2	2	2	2
情報窃取	2	2	2	2	2	2	2	2	2	2	2
情報改ざん	2	2	2	2	2	2	2	2	2	2	2
情報破壊	2	2	2	2	2	2	2	2	2	2	2
不正送信	2	2	2	2	2	2	2	2	2	2	2
機能停止	2	2	2	2	2	2	2	2	2	2	2
制御不能・異常動作	2	2	2	2	2	2	2	2	2	2	2
高負荷攻撃	2	2	2	2	2	2	2	2	2	2	2
窃盗	2	2	2	2	2	2	2	2	2	2	2
盗難・廃棄時の情報窃取	2	2	2	2	2	2	2	2	2	2	2
経路遮断		2	2	2							
通信輻輳		2	2	2							
無線妨害											
盗聴		2	2	2							
通信データ改ざん		2	2	2							
不正機器接続		2	2	2							

（凡例）脆弱性レベル：脆弱性レベル＝３ は脅威を受け入れる可能性が高いことを意味し、脆弱性レベル＝１ は脅威を受け入れる可能性が低いことを意味する。

脆弱性レベルまとめ表の実施例（続き）

資産 / 脅威	外部システム								
	12 関連システム	13 GCS	14 機体	15 UTMS	16 気象システム	17 地図システム	18 VIS	19 DIPS	20 SWIM
不正アクセス	2	2	2	2	2	2	2	2	2
物理的侵入	2	2	2	2	2	2	2	2	2
不正操作	2	2	2	2	2	2	2	2	2
過失操作	2	2	2	2	2	2	2	2	2
不正媒体・機器接続	2	2	2	2	2	2	2	2	2
プロセス不正実行	2	2	2	2	2	2	2	2	2
マルウェア感染	2	2	2	2	2	2	2	2	2
情報窃取	2	2	2	2	2	2	2	2	2
情報改ざん	2	2	2	2	2	2	2	2	2
情報破壊	2	2	2	2	2	2	2	2	2
不正送信	2	2	2	2	2	2	2	2	2
機能停止	2	2	2	2	2	2	2	2	2
制御不能・異常動作	2	2	2	2	2	2	2	2	2
高負荷攻撃	2	2	2	2	2	2	2	2	2
窃盗									
盗難・廃棄時の情報窃取									
経路遮断	2	2	2	2	2	2	2	2	2
通信輻輳	2	2	2	2	2	2	2	2	2
無線妨害		2	2						
盗聴	2	2	2	2			2	2	2
通信データ改ざん	2	2	2	2	2	2	2	2	2
不正機器接続									

（凡例）脆弱性レベル：脆弱性レベル＝３ は脅威を受け入れる可能性が高いことを意味し、脆弱性レベル＝１ は脅威を受け入れる可能性が低いことを意味する。

（５）資産ベースのリスク分析シートの実施例

資産ベースのリスク分析シート（端末）の実施例

	資産種別	資産	評価指標				脅威 (攻撃手法)	機器異常検知	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威度
1	情報系資産	端末	2	2	2	C	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避	 ○ ○ 			IPS／IDS ログ収集・分析 統合ログ管理システム	 ○ ○			2
2			2	2		C	物理的侵入	入室が制限された区画(執務室/サーバー室)に不正侵入する。	入退管理（ICカード） 施錠管理	○ ○			監視カメラ 侵入センサ	○			2
3			2	2		C	不正操作	区画に不正侵入後、機器のコンソール等を直接操作し攻撃を実行する。	操作者認証	○							2
4			2	2		C	過失操作	内部関係者(社員や協力者で、当該機器へのアクセス権を有する者)の過失操作を誘発し攻撃を実行する。機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレビュテーション メールフィルタリング	○ ○							2
5			2	2		C	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し攻撃を実行する。	デバイス接続・利用制限	○	デバイス接続・利用制限	○	デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム	○ ○ ○			2
6			2	2	2	C	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	○ ○ 	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制 重要操作の承認	○ ○ 	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	○ ○ ○ ○			2
7			2	2		C	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・実行させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	○ ○ 			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	○ ○ ○ ○			2
8			2	2		C	情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○ ○ 	権限管理 アクセス制御 データ暗号化 DLP	○ ○ 	ログ収集・分析 統合ログ管理システム	○ ○			2
9			2	2		C	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名	○ ○ 	権限管理 アクセス制御 データ署名	 	機器異常検知 ログ収集・分析 統合ログ管理システム	○ ○ ○	データバックアップ		2
10			2	2		C	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。		○ ○	権限管理 アクセス制御	○ ○	機器異常検知 ログ収集・分析 統合ログ管理システム	○ ○ ○	データバックアップ		2
11			2	2		C	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認	○ 	セグメント分割／ゾーニング データ署名 重要操作の承認	 	ログ収集・分析 統合ログ管理システム	○ ○			2
12			2	2		C	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	○ ○ ○ ○	冗長化 フェールセーフ設計		2

資産ベースのリスク分析シート（端末）の実施例（続き）

	資産種別	資産	評価指標				脅威 (攻撃手法)	機器異常検知	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威度
13	情報系資産	端末	2	2	2	C	制御不能・異常動作	機器を制御不能にしたり、異常動作させる。					機器異常検知	○	冗長化		2
													機器死活監視	○	フェールセーフ設計		
													ログ収集・分析	○			
													統合ログ管理システム	○			
14			2	2		C	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知	○	冗長化		2
													機器死活監視	○	フェールセーフ設計		
													ログ収集・分析	○			
													統合ログ管理システム	○			
15			2	2		C	窃盗	機器を窃盗する。	施錠管理	○	施錠管理	○	施錠管理	○			2
16			2	2		C	盗難・廃棄時の情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー		耐タンパー						2
									難読化		難読化						
									セキュア消去	○	セキュア消去	○					
17					2		経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理（ICカード）				機器異常検知		冗長化		
									施錠管理				機器死活監視				
													ログ収集・分析				
													統合ログ管理システム				
													監視カメラ				
													侵入センサ				
18							通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW（パケットフィルタリング型）				機器異常検知		冗長化		
									FW（アプリケーションゲートウェイ型）				機器死活監視				
									WAF				ログ収集・分析				
									IPS／IDS				統合ログ管理システム				
									DDoS対策								
19							無線妨害	無線通信を妨害する。					機器異常検知		冗長化		
													機器死活監視				
													ログ収集・分析				
													統合ログ管理システム				
20							盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化								
									データ暗号化								
									専用線								
21							通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化				ログ収集・分析				
									データ署名				統合ログ管理システム				
									専用線								
22							不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限				
													ログ収集・分析				
													統合ログ管理システム				

（６）資産ベースのリスク分析：リスク値まとめ表の実施例

脅威＼資産	1 端末	2 ファイアウォール (FW)	3 ルーター	4 スイッチ (SW)	5 サーバー	6 画定	7 航路予約	8 安全管理	9 離着陸場/機体管理	10 外部データ参照	11 ユーザー認証
不正アクセス	C	C	C	C	A	A	A	A	A	A	A
物理的侵入	C	C	C	C	A	A	A	A	A	A	A
不正操作	C	C	C	C	A	A	A	A	A	A	A
過失操作	C	C	C	C	A	A	A	A	A	A	A
不正媒体・機器接続	C	C	C	C	A	A	A	A	A	A	A
プロセス不正実行	C	C	C	C	A	A	A	A	A	A	A
マルウェア感染	C	C	D	D	A	A	A	A	A	A	A
情報窃取	C	C	D	D	A	A	A	A	A	A	A
情報改ざん	C	C	D	D	A	A	A	A	A	A	A
情報破壊	C	C	D	D	A	A	A	A	A	A	A
不正送信	C	C	D	D	A	A	A	A	A	A	A
機能停止	C	C	D	D	A	A	A	A	A	A	A
制御不能・異常動作	C	C	D	D	A	A	A	A	A	A	A
高負荷攻撃	C	C	C	C	A	A	A	A	A	A	A
窃盗	C	C	C	C	C	C	C	C	C	C	C
盗難・廃棄時の情報窃取	C	C	C	C	C	C	C	C	C	C	C
経路遮断		C	C	C							
通信輻輳		C	C	C							
無線妨害											
盗聴		C	C	C							
通信データ改ざん		C	C	C							
不正機器接続		C	C	C							

（凡例）リスク値：３つの評価指標「脅威レベル」「脆弱性レベル」「資産の重要度」によって算定し、 A（リスクが非常に高い）～ E（リスクが非常に低い）の５ 段階。

資産ベースのリスク分析：リスク値まとめ表の実施例（続き）

資産 / 脅威	外部システム								
	12 関連システム	13 GCS	14 機体	15 UTMS	16 気象システム	17 地図システム	18 VIS	19 DIPS	20 SWIM
不正アクセス	C	C	C	C	C	D	C	E	E
物理的侵入	C	C	C	C	C	D	C	E	E
不正操作	C	C	C	C	C	D	C	E	E
過失操作	C	C	C	C	C	D	C	E	E
不正媒体・機器接続	C	C	C	C	C	D	C	E	E
プロセス不正実行	C	C	C	C	C	D	C	E	E
マルウェア感染	C	C	C	C	C	D	C	E	E
情報窃取	C	C	C	C	C	D	C	E	E
情報改ざん	C	C	C	C	C	D	C	E	E
情報破壊	C	C	C	C	C	D	C	E	E
不正送信	C	C	C	C	C	D	C	E	E
機能停止	C	C	C	C	C	D	C	E	E
制御不能・異常動作	C	C	C	C	C	D	C	E	E
高負荷攻撃	C	C	C	C	C	D	C	E	E
窃盗									
盗難・廃棄時の情報窃取									
経路遮断	C	C	C	C	C	D	C	E	E
通信輻輳	C	C	C	C	C	D	C	E	E
無線妨害		C	C						
盗聴	C	C	C	C			C	E	E
通信データ改ざん	C	C	C	C	C	D	C	E	E
不正機器接続									

（凡例）リスク値：３つの評価指標「脅威レベル」「脆弱性レベル」「資産の重要度」によって算定し、 A（リスクが非常に高い）～ E（リスクが非常に低い）の５ 段階。

付録 8：事業被害ベースのリスク分析

（１）攻撃シナリオ一覧の実施例

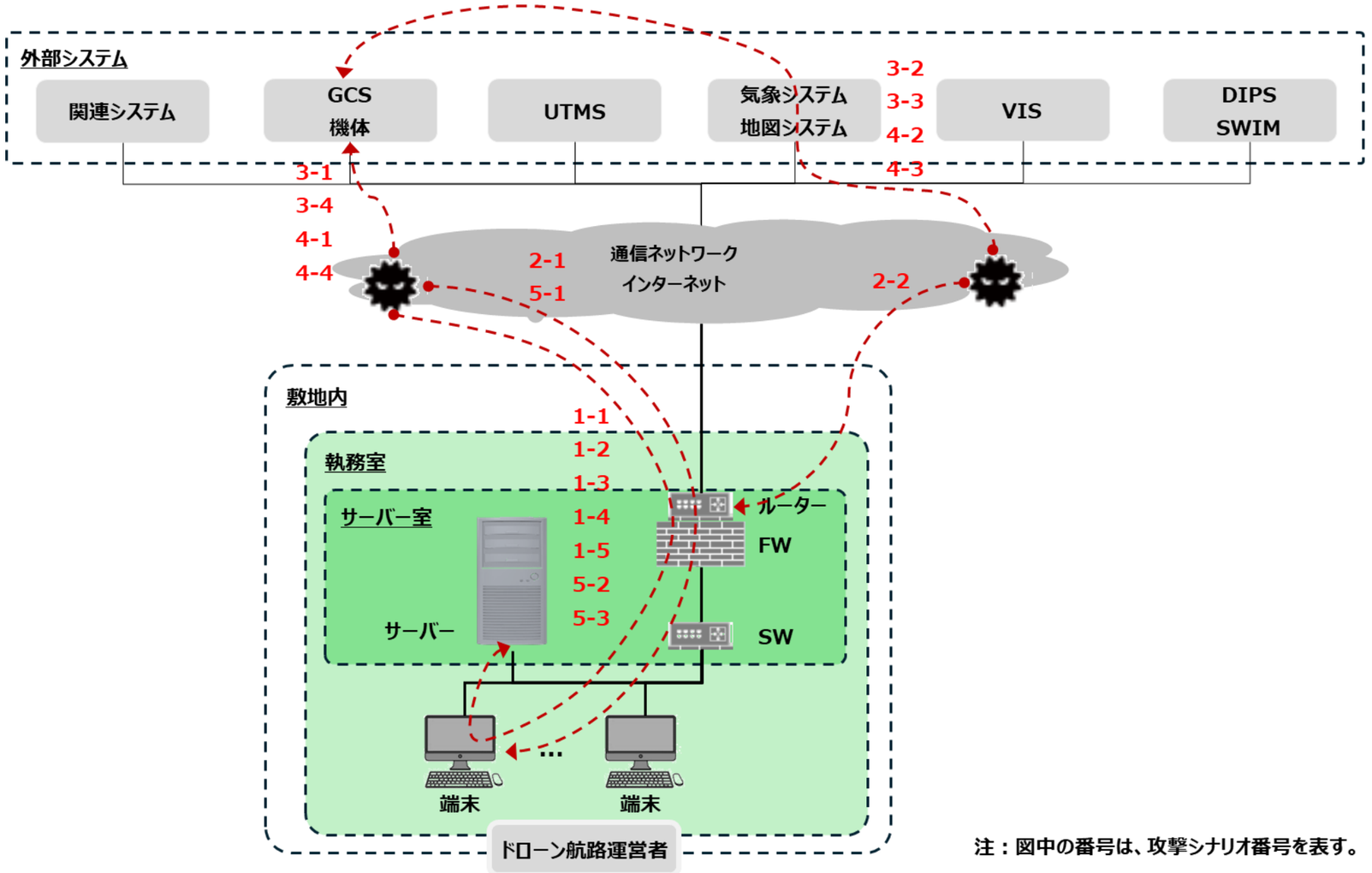
項番	事業被害	事業被害の概要と攻撃シナリオ				事業被害レベル
1	ドローン航路サービスの 長期間サービス停止	サーバーへのサイバー攻撃により、業務コマンドを悪用されてサービス停止、データの改竄/破壊等が実行されドローン航路サービスが長期間停止し、運航事業者との契約が解除される恐れがある。				3
		シナリオ#	**攻撃シナリオ**	**攻撃拠点**	**攻撃対象**	**最終攻撃**
		1-1	業務コマンドを実行することにより、サーバーを停止させる。	端末	サーバー	サーバーの破壊/停止操作が実行される。
		1-2	サーバーに負荷をかけ、サービスを停滞させる。	端末	各サービス	各サービスが停滞する。
		1-3	サーバーを乗っ取り、サービスを停止させる。	端末	各サービス	各サービスが停止する。
		1-4	サーバーのコマンドを実行することにより、サービスを停止させる。	端末	各サービス	各サービスの破壊/停止操作が実行される。
		1-5	サーバーのコマンドを実行することにより、サーバー情報の改竄/破壊等が行われる。	端末	各サービス	各サービスが利用する重要のデータ改竄/破壊操作が実行される。
2	ドローン航路サービスの 一定期間サービス停止	端末やネットワーク機器へのサイバー攻撃により、高負荷、情報漏洩、改竄等が実行されてドローン航路サービスが一定期間停止する。				2
		シナリオ#	**攻撃シナリオ**	**攻撃拠点**	**攻撃対象**	**最終攻撃**
		2-1	端末を乗っ取り、端末情報の改竄等が実行される。	通信ネットワーク	端末	情報改竄により、結果として、一定期間サービスを停止せざるを得ない。
		2-2	ネットワーク機器に負荷をかけ、サービスを停滞させる。	通信ネットワーク	ネットワーク機器	一定期間サービスが停滞する。
3	ドローン航路内外での ドローン墜落	ドローン本体や環境情報へのサイバー攻撃により、ドローンの乗っ取りや通信妨害等が実行されて墜落し、ドローン航路を一時封鎖する必要があるため、ドローン航路サービスが一定期間停止する。				2
		シナリオ#	**攻撃シナリオ**	**攻撃拠点**	**攻撃対象**	**最終攻撃**
		3-1	GPSセンサーへの通信妨害等を実行し、ドローンを墜落させる。	通信ネットワーク	ドローン	ドローンの墜落により、結果として、一定期間サービスを停止せざるを得ない。
		3-2	気象システムへの通信妨害等を実行し、ドローンを墜落させる。	気象システム	ドローン	ドローンの墜落により、結果として、一定期間サービスを停止せざるを得ない。
		3-3	地図システムへの通信妨害等を実行し、ドローンを墜落させる。	地図システム	ドローン	ドローンの墜落により、結果として、一定期間サービスを停止せざるを得ない。
		3-4	ドローンを乗っ取り、ドローンを墜落させる。	通信ネットワーク	ドローン	ドローンの墜落により、結果として、一定期間サービスを停止せざるを得ない。
4	ドローン航路からの逸脱/紛失	ドローン本体や環境情報へのサイバー攻撃により、ドローンの乗っ取りや通信妨害等が実行されて航路を逸脱したり紛失したりして、ドローン航路を一時封鎖する必要があるため、ドローン航路サービスが一定期間停止する。				2
		シナリオ#	**攻撃シナリオ**	**攻撃拠点**	**攻撃対象**	**最終攻撃**
		4-1	GPSセンサーへの通信妨害等を実行し、航路を逸脱させたり紛失させたりする。	通信ネットワーク	ドローン	ドローンの航路逸脱や紛失により、結果として、一定期間サービスを停止せざるを得ない。
		4-2	気象システムへの通信妨害等を実行し、航路を逸脱させたり紛失させたりする。	気象システム	ドローン	ドローンの航路逸脱や紛失により、結果として、一定期間サービスを停止せざるを得ない。
		4-3	地図システムへの通信妨害等を実行し、航路を逸脱させたり紛失させたりする。	地図システム	ドローン	ドローンの航路逸脱や紛失により、結果として、一定期間サービスを停止せざるを得ない。
		4-4	ドローンの乗っ取りを、航路を逸脱させたり紛失させたりする。	通信ネットワーク	ドローン	ドローンの航路逸脱や紛失により、結果として、一定期間サービスを停止せざるを得ない。
5	個人情報や機密情報の漏洩	端末やサーバーへのサイバー攻撃により、個人情報や機密情報(航路情報/ポート情報/機体情報/運航計画/歩行ログ等)等の重要データが外部に漏洩し、信頼が大きく低下する。				3
		シナリオ#	**攻撃シナリオ**	**攻撃拠点**	**攻撃対象**	**最終攻撃**
		5-1	端末に保存されている重要データを窃取し、外部に漏洩させる。	通信ネットワーク	端末	端末に保存されている重要データが窃取される。
		5-2	サーバーに保存されている重要データを窃取し、外部に漏洩させる。	通信ネットワーク	サーバー	サーバーに保存されている重要データが窃取される。
		5-3	各サービスが利用する重要データを窃取し、外部に漏洩させる。	通信ネットワーク	各サービス	各サービスが利用する重要データが窃取される。

（凡例）事業被害レベル：被害大：3 ＞ 被害中：2 ＞被害小：1

（２）攻撃ルート一覧の実施例

攻撃ツリー	攻撃シナリオ	誰が	どこから	どうやって					
番号	番号	攻撃者	侵入口	経由１	経由２	経由３	攻撃拠点	攻撃対象	最終攻撃
1-1	1-1	悪意のある第三者	通信ネットワーク	ネットワーク機器			端末	サーバー	サーバーの破壊/停止操作が実行される。
1-2	1-1	内部関係者(故意)	端末				端末	サーバー	サーバーの破壊/停止操作が実行される。
1-3	1-2	悪意のある第三者	通信ネットワーク	ネットワーク機器	端末		端末	各サービス	各サービスが停滞する。
1-4	1-2	内部関係者(故意)	端末				端末	各サービス	各サービスが停滞する。
1-5	1-3	悪意のある第三者	通信ネットワーク	ネットワーク機器	端末		端末	サーバー	各サービスが停止する。
1-6	1-3	内部関係者(故意)	端末				端末	サーバー	各サービスが停止する。
1-7	1-4	悪意のある第三者	通信ネットワーク	ネットワーク機器	端末		端末	各サービス	各サービスの破壊/停止操作が実行される。
1-8	1-4	内部関係者(故意)	端末				端末	各サービス	各サービスの破壊/停止操作が実行される。
1-9	1-5	悪意のある第三者	通信ネットワーク	ネットワーク機器	端末		端末	各サービス	各サービスが利用する重要のデータ改竄/破壊操作が実行される。
1-10	1-5	内部関係者(故意)	端末				端末	各サービス	各サービスが利用する重要のデータ改竄/破壊操作が実行される。
2-1	2-1	悪意のある第三者	通信ネットワーク	ネットワーク機器			通信ネットワーク	端末	情報改竄により、結果として、一定期間サービスを停止せざるを得ない。
2-2	2-1	内部関係者(過失)	端末				通信ネットワーク	端末	情報改竄により、結果として、一定期間サービスを停止せざるを得ない。
2-3	2-2	悪意のある第三者	通信ネットワーク	ネットワーク機器			通信ネットワーク	ネットワーク機器	一定期間サービスが停滞する。
3-1	3-1	悪意のある第三者	通信ネットワーク	GPSセンサー			通信ネットワーク	ドローン	ドローンの墜落により、結果として、一定期間サービスを停止せざるを得ない。
3-2	3-2	悪意のある第三者	通信ネットワーク	気象システム			気象システム	ドローン	ドローンの墜落により、結果として、一定期間サービスを停止せざるを得ない。
3-3	3-3	悪意のある第三者	通信ネットワーク	地図システム			地図システム	ドローン	ドローンの墜落により、結果として、一定期間サービスを停止せざるを得ない。
3-4	3-4	悪意のある第三者	通信ネットワーク				通信ネットワーク	ドローン	ドローンの墜落により、結果として、一定期間サービスを停止せざるを得ない。
4-1	4-1	悪意のある第三者	通信ネットワーク	GPSセンサー			通信ネットワーク	ドローン	ドローンの航路逸脱/紛失により、結果として、一定期間サービスを停止せざるを得ない。
4-2	4-2	悪意のある第三者	通信ネットワーク	気象センサー	気象システム		通信ネットワーク	ドローン	ドローンの航路逸脱/紛失により、結果として、一定期間サービスを停止せざるを得ない。
4-3	4-3	悪意のある第三者	通信ネットワーク	地図システム			通信ネットワーク	ドローン	ドローンの航路逸脱/紛失により、結果として、一定期間サービスを停止せざるを得ない。
4-3	4-3	悪意のある第三者	通信ネットワーク				通信ネットワーク	ドローン	ドローンの航路逸脱/紛失により、結果として、一定期間サービスを停止せざるを得ない。
5-1	5-1	悪意のある第三者	通信ネットワーク	ネットワーク機器			通信ネットワーク	端末	端末に保存されている重要データが窃取される。
5-2	5-1	内部関係者(過失)	端末				通信ネットワーク	端末	端末に保存されている重要データが窃取される。
5-3	5-2	悪意のある第三者	通信ネットワーク	ネットワーク機器	端末		端末	サーバー	サーバーに保存されている重要データが窃取される。
5-4	5-2	内部関係者(過失)	端末				端末	サーバー	サーバーに保存されている重要データが窃取される。
5-5	5-3	悪意のある第三者	通信ネットワーク	ネットワーク機器	端末		端末	各サービス	各サービスが利用する重要データが窃取される。
5-6	5-3	内部関係者(過失)	端末				端末	各サービス	各サービスが利用する重要データが窃取される。

（３）攻撃ルート図の実施例



注：図中の番号は、攻撃シナリオ番号を表す。

（４）事業被害レベルのリスク分析の実施例

実施例①：ドローン航路サービスの長期間サービス停止：サーバーへのサイバー攻撃により、業務コマンドを悪用されてサービス停止、データの改竄/破壊等が実行されドローン航路サービスが長期間停止し、運航事業者との契約が解除される恐れがある。

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御 侵入／拡散段階	防御 目的遂行段階	検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
	1-1 1-2 1-3 1-4 1-5	業務コマンドを実行することにより、サーバーを停止させる。 サーバーに負荷をかけ、サービスを停滞させる。 サーバーを乗っ取り、サービスを停止させる。 サーバーのコマンドを実行することにより、サービスを停止させる。 サーバーのコマンドを実行することにより、データの改竄/破壊等が行われる。													
1		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークからネットワーク機器に不正アクセスする。					FW ○ 通信相手の認証 ○ パッチ適用 ○ 権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2			
2		悪意ある第三者が、ネットワーク機器を経由して端末に不正アクセスする。					通信相手の認証 ○ パッチ適用 ○ 権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2			
3	1-1	悪意ある第三者が、端末からサーバーの業務コマンドを実行し、サーバーを停止させる。	2	2	3	B	権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2	2	1-1	1,2,3
4	1-2	悪意ある第三者が、端末からサーバーに負荷をかけサービスを停滞させる。	2	2	3	B	権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2	2	1-3	1,2,4
5	1-3	悪意ある第三者が、端末からサーバーを乗っ取りサービスを停止させる。	2	2	3	B	権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2	2	1-5	1,2,5
6	1-4	悪意ある第三者が、端末からサーバーのコマンドを実行することによりサービスを停止させる。	2	2	3	B	権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2	2	1-7	1,2,6
7	1-5	悪意ある第三者が、端末からサーバーのコマンドを実行することによりデータの改竄/破壊等が行われる。	2	2	3	B	権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2	2	1-9	1,2,7
8		【N】侵入口=端末 内部関係者が、故意に端末を不正利用する。					通信相手の認証 ○ パッチ適用 ○ 権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2			
9	1-1	端末から不正にサーバーの業務コマンドを実行し、サーバーを停止させる。	2	2	3	B	通信相手の認証 ○ パッチ適用 ○ 権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2	2	1-2	8,9
10	1-2	端末から不正にサーバーに負荷をかけサービスを停滞させる。	2	2	3	B	通信相手の認証 ○ パッチ適用 ○ 権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2	2	1-4	8,10
11	1-3	端末から不正にサーバーを乗っ取りサービスを停止させる。	2	2	3	B	通信相手の認証 ○ パッチ適用 ○ 権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2	2	1-6	8,11
12	1-4	端末から不正にサーバーのコマンドを実行することによりサービスを停止させる。	2	2	3	B	通信相手の認証 通信 パッチ適用 パッチ ○ 権限管理 権限 ○		ログ収 統合ログ管理システム ○		2	2	1-8	8,12
13	1-5	端末から不正にサーバーの業務コマンドを実行することによりサーバー情報の改竄/破壊等が行われる。	2	2	3	B	通信相手の認証 ○ パッチ適用 ○ 権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2	2	1-10	8,13

（凡例）脅威レベル：発生可能性大：３ ＞ 発生可能性中：２ ＞発生可能性小：1

脆弱性レベル：脆弱性レベル＝3 は脅威を受け入れる可能性が高いことを意味し、脆弱性レベル＝1 は脅威を受け入れる可能性が低いことを意味する

事業被害レベル：被害大：３ ＞ 被害中：２ ＞被害小：1

リスク値：３つの評価指標「脅威レベル」「脆弱性レベル」「資産の重要度」によって算定し、 A（リスクが非常に高い）～ E（リスクが非常に低い）の５ 段階。

実施例②：ドローン航路サービスの一定期間サービス停止：端末やネットワーク機器へのサイバー攻撃により、高負荷、情報改竄等が実行されてドローン航路サービスが一定期間停止する。

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策						対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御				検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階		目的遂行段階							
	2-1	端末を乗っ取り、端末の情報改竄等が実行される。														
14		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークからネットワーク機器に不正アクセスする。					FW ○ 通信相手の認証 ○ パッチ適用 ○ 権限管理 ○		権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2			
15		悪意ある第三者が、ネットワーク機器を経由して端末に不正アクセスする。					通信相手の認証 ○ パッチ適用 ○ 権限管理 ○				ログ収集・分析 ○ 統合ログ管理システム ○		2			
16		悪意ある第三者が、端末の情報を改竄する。	2	2	2	C	権限管理 ○				ログ収集・分析 ○ 統合ログ管理システム ○		2	2	2-1	14,15,16
17		【N】侵入口=端末 内部者の過失により、マルウェアに感染したUSB媒体を端末に接続して、端末がマルウェアに感染する。					通信相手の認証 ○ パッチ適用 ○ 権限管理 ○				ログ収集・分析 ○ 統合ログ管理システム ○		2			
18		マルウェアが、端末の情報を改竄する。	2	2	2	C	通信相手の認証 ○ パッチ適用 ○ 権限管理 ○				ログ収集・分析 ○ 統合ログ管理システム ○		2	2	2-1	17,18
	2-2	ネットワーク機器に負荷をかけ、サービスを停滞させる。														
19		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークからネットワーク機器に不正アクセスする。					FW ○ 通信相手の認証 ○ パッチ適用 ○ 権限管理 ○		権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2			
20		悪意ある第三者が、ネットワーク機器に負荷をかけサービスを停滞させる。	2	2	2	C	FW ○ 通信相手の認証 ○ パッチ適用 ○ 権限管理 ○		権限管理 ○		ログ収集・分析 ○ 統合ログ管理システム ○		2	2	2-2	19,20

（凡例）脅威レベル：発生可能性大：3 ＞ 発生可能性中：2 ＞発生可能性小：1

脆弱性レベル：脆弱性レベル＝3 は脅威を受け入れる可能性が高いことを意味し、脆弱性レベル＝1 は脅威を受け入れる可能性が低いことを意味する

事業被害レベル：被害大：3 ＞ 被害中：2 ＞被害小：1

リスク値：3 つの評価指標「脅威レベル」「脆弱性レベル」「資産の重要度」によって算定し、 A（リスクが非常に高い）～ E（リスクが非常に低い）の 5 段階。

実施例③：ドローン航路内外でのドローン墜落：ドローン本体や環境情報へのサイバー攻撃により、ドローンの乗っ取りや通信妨害等が実行されて墜落し、ドローン航路を一時封鎖する必要があるため、ドローン航路サービスが一定期間停止する。

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	3-1	GPSセンサーへの通信妨害等を実行し、ドローンを墜落させる。												
21		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークからGPSセンサーにスプーフィング攻撃する。									1			
22		GPSセンサーからドローンに偽情報(高度、位置等)を入力し、墜落させたり、障害物に衝突させたりする。	2	3	2	B					1	1	3-1	21,22
	3-2	気象システムへの通信妨害等を実行し、ドローンを墜落させる。												
23		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークから気象システムになりすまし、偽情報(気象情報)を関係者に配信する。									1			
24		悪意ある第三者の偽情報により、荒天でドローンを運航させ墜落させる。	2	3	2	B					1	1	3-2	23,24
	3-3	地図システムへの通信妨害等を実行し、ドローンを墜落させる。												
25		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークから地図システムになりすまし、偽情報(地図情報)を関係者に配信する。									1			
26		悪意ある第三者の偽情報により、間違った座標や高度でドローンを運航させ墜落させる。	2	3	2	B					1	1	3-3	25,26
	3-4	ドローンを乗っ取り、ドローンを墜落させる。												
27		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークからGCSになりすまし、ドローンを乗っ取る。									1			
28		悪意ある第三者が、制御コマンドを実行することによりドローンを墜落させる。	2	3	2	B					1	1	3-4	27,28

（凡例）脅威レベル：発生可能性大：3 ＞ 発生可能性中：2 ＞発生可能性小：1

脆弱性レベル：脆弱性レベル＝3 は脅威を受け入れる可能性が高いことを意味し、脆弱性レベル＝1 は脅威を受け入れる可能性が低いことを意味する

事業被害レベル：被害大：3 ＞ 被害中：2 ＞被害小：1

リスク値：3 つの評価指標「脅威レベル」「脆弱性レベル」「資産の重要度」によって算定し、 A（リスクが非常に高い）～ E（リスクが非常に低い）の 5 段階。

実施例④：ドローン本体や環境情報へのサイバー攻撃により、ドローンの乗っ取りや通信妨害等が実行されて飛行経路計画可能空間を逸脱したり紛失したりして、ドローン航路を一時封鎖する必要があるため、ドローン航路サービスが一定期間停止する。

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	4-1	GPSセンサーへの通信妨害等を実行し、航路を逸脱させたり紛失させたりする。												
29		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークからGPSセンサーにスプーフィング攻撃する。									1			
30		GPSセンサーからドローンに偽情報(高度、位置等)が入力され、航路を逸脱させたり紛失させたりする。	2	3	2	B					1	1	4-1	29,30
	4-2	気象システムへの通信妨害等を実行し、航路を逸脱させたり紛失させたりする。												
31		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークから気象システムになりすまし、偽情報(気象情報)を関係者に配信する。									1			
32		悪意ある第三者の偽情報により、荒天でドローンを運航させ航路を逸脱させたり紛失させたりする。	2	3	2	B					1	1	4-2	31,32
	4-3	地図システムへの通信妨害等を実行し、航路を逸脱させたり紛失させたりする。												
33		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークから地図システムになりすまし、偽情報(地図情報)を関係者に配信する。									1			
34		悪意ある第三者の偽情報により、間違った座標や高度でドローンを運航させ航路を逸脱させたり紛失させたりする。	2	3	2	B					1	1	4-3	33,34
	4-4	ドローンの乗っ取り、航路を逸脱させたり紛失させたりする。												
35		【N】侵入口=通信ネットワーク 悪意ある第三者が、通信ネットワークからGCSになりすまし、ドローンを乗っ取る。									1			
36		悪意ある第三者が、制御コマンドを実行し、航路を逸脱させたり紛失させたりする。	2	3	2	B					1	1	4-4	35,36

（凡例）脅威レベル：発生可能性大：３ ＞ 発生可能性中：２ ＞発生可能性小：１

脆弱性レベル：脆弱性レベル＝３ は脅威を受け入れる可能性が高いことを意味し、脆弱性レベル＝１ は脅威を受け入れる可能性が低いことを意味する

事業被害レベル：被害大：３ ＞ 被害中：２ ＞被害小：１

リスク値：３つの評価指標「脅威レベル」「脆弱性レベル」「資産の重要度」によって算定し、 A（リスクが非常に高い）～ E（リスクが非常に低い）の５ 段階。

実施例⑤：端末やサーバーへのサイバー攻撃により、個人情報や機密情報(航路情報/離着陸場情報/機体情報/運航計画/歩行ログ等)等の重要データが外部に漏洩し、信頼が大きく低下する。

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策								対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御				検知／被害把握		事業継続		攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階		目的遂行段階									
	5-1 5-2 5-3	**端末に保存されている重要データを窃取し、外部に漏洩させる。** **サーバーに保存されている重要データを窃取し、外部に漏洩させる。** **各サービスが利用する重要データを窃取し、外部に漏洩させる。**																
37		**【N】侵入口=通信ネットワーク** 悪意ある第三者が、通信ネットワークからネットワーク機器に不正アクセスする。					FW 通信相手の認証 パッチ適用 権限管理	○ ○ ○ ○			ログ収集・分析 統合ログ管理システム	○ ○			2			
38		悪意ある第三者が、ネットワーク機器を経由して端末に不正アクセスする。					通信相手の認証 パッチ適用 権限管理	○ ○ ○			ログ収集・分析 統合ログ管理システム	○ ○			2			
39	5-1	悪意ある第三者が、端末の情報を搾取する。	2	2	3	B	権限管理	○			ログ収集・分析 統合ログ管理システム	○ ○			2	2	5-1	37,38,39
40	5-2	悪意ある第三者が、端末からサーバーの業務コマンドを実行し、サーバーの情報を搾取する。	2	2	3	B	権限管理	○			ログ収集・分析 統合ログ管理システム	○ ○			2	2	5-2	37,38,40
41	5-3	悪意ある第三者が、端末からサービスの業務コマンドを実行し、サービスが利用する情報を搾取する。	2	2	3	B	権限管理	○			ログ収集・分析 統合ログ管理システム	○ ○			2	2	5-3	37,38,41
42		**【N】侵入口=端末** 内部者の過失により、マルウェアに感染したUSB媒体を端末に接続して、端末がマルウェアに感染する。					通信相手の認証 パッチ適用 権限管理	○ ○ ○			ログ収集・分析 統合ログ管理システム	○ ○			2			
43	5-1	マルウェアが、端末の情報を搾取する。	2	2	3	B	通信相手の認証 パッチ適用 権限管理	○ ○ ○			ログ収集・分析 統合ログ管理システム	○ ○			2	2	5-1	42,43
44	5-2	マルウェアが、端末からサーバーの業務コマンドを実行し、サーバーの情報を搾取する。	2	2	3	B	通信相手の認証 パッチ適用 権限管理	○ ○ ○			ログ収集・分析 統合ログ管理システム	○ ○			2	2	5-2	42,44
45	5-3	マルウェアが、端末からサービスの業務コマンドを実行し、サービスが利用する情報を搾取する。	2	2	3	B	通信相手の認証 パッチ適用 権限管理	○ ○ ○			ログ収集・分析 統合ログ管理システム	○ ○			2	2	5-3	42,45

（凡例）脅威レベル：発生可能性大：３ ＞ 発生可能性中：２ ＞発生可能性小：１

脆弱性レベル：脆弱性レベル＝３ は脅威を受け入れる可能性が高いことを意味し、脆弱性レベル＝１ は脅威を受け入れる可能性が低いことを意味する

事業被害レベル：被害大：３ ＞ 被害中：２ ＞被害小：１

リスク値：３つの評価指標「脅威レベル」「脆弱性レベル」「資産の重要度」によって算定し、 A（リスクが非常に高い）～ E（リスクが非常に低い）の５ 段階。

（５）事業被害ベースのリスク分析：リスク値まとめ表の実施例

項番	事業被害	事業被害レベル	攻撃シナリオ			攻撃ツリーのリスク値					
							A	B	C	D	E	小計
1	ドローン航路サービスの長期間サービス停止	3	サーバーへのサイバー攻撃により、業務コマンドを悪用されてサービス停止、データの改竄/破壊等が実行されドローン航路サービス提供が長期間停止し、運航事業者との契約が解除される恐れがある。									
				1-1	業務コマンドを実行することにより、サーバーを停止させる。		0	2	0	0	0	2
				1-2	サーバーに負荷をかけ、サービスを停止させる。		0	2	0	0	0	2
				1-3	サーバーを乗っ取り、サービスを停止させる。		0	2	0	0	0	2
				1-4	サーバーのコマンドを実行することにより、サービスを停止させる。		0	2	0	0	0	2
				1-5	サーバーのコマンドを実行することにより、データの改竄/破壊等が行われる。		0	2	0	0	0	2
						小計	0	10	0	0	0	10
2	ドローン航路サービスの一定期間サービス停止	2	端末やネットワーク機器へのサイバー攻撃により、高負荷、情報改竄等が実行されてドローン航路サービス提供が一定期間停止する。									
				2-1	端末を乗っ取り、端末情報の改竄等が実行される。		0	0	2	0	0	2
				2-2	ネットワーク機器に負荷をかけ、サービスを停滞させる。		0	0	1	0	0	1
						小計	0	0	3	0	0	3
3	ドローン航路内外でのドローン墜落	2	ドローン本体や環境情報へのサイバー攻撃により、ドローンの乗っ取りや通信妨害等が実行されて墜落し、ドローン航路を一時封鎖する必要があるため、ドローン航路サービスが一定期間停止する。									
				3-1	GPSセンサーへの通信妨害等を実行し、ドローンを墜落させる。		0	1	0	0	0	1
				3-2	気象システムへの通信妨害等を実行し、ドローンを墜落させる。		0	1	0	0	0	1
				3-3	地図システムへの通信妨害等を実行し、ドローンを墜落させる。		0	1	0	0	0	1
				3-4	ドローンを乗っ取り、ドローンを墜落させる。		0	1	0	0	0	1
						小計	0	4	0	0	0	4
4	ドローン航路からの逸脱/紛失	2	ドローン本体や環境情報へのサイバー攻撃により、ドローンの乗っ取りや通信妨害等が実行されて航路を逸脱したり紛失したりして、ドローン航路を一時封鎖する必要があるため、ドローン航路サービスが一定期間停止する。									
				4-1	GPSセンサーへの通信妨害等を実行し、航路を逸脱させたり紛失させたりする。		0	1	0	0	0	1
				4-2	気象システムへの通信妨害等を実行し、航路を逸脱させたり紛失させたりする。		0	1	0	0	0	1
				4-3	地図システムへの通信妨害等を実行し、航路を逸脱させたり紛失させたりする。		0	1	0	0	0	1
				4-4	ドローンの乗っ取りを、航路を逸脱させたり紛失させたりする。		0	1	0	0	0	1
						小計	0	4	0	0	0	4
5	個人情報や機密情報の漏洩	3	端末やサーバーへのサイバー攻撃により、個人情報や機密情報(航路情報/ポート情報/機体情報/運航計画/歩行ログ等)等の重要データが外部に漏洩し、信頼が大きく低下する。									
				5-1	端末に保存されている重要データを窃取し、外部に漏洩させる。		0	2	0	0	0	2
				5-2	サーバーに保存されている重要データを窃取し、外部に漏洩させる。		0	2	0	0	0	2
				5-3	各サービスが利用する重要データを窃取し、外部に漏洩させる。		0	2	0	0	0	2
						小計	0	6	0	0	0	6

（凡例）リスク値：３つの評価指標「脅威レベル」「脆弱性レベル」「資産の重要度」によって算定し、 A（リスクが非常に高い）～ E（リスクが非常に低い）の５ 段階。

付録 9：CPSF ベースのリスク分析

（1）第 1 層：企業（組織）間のつながり

項番	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件 ID
			脅威		脆弱性		
1-1	組織として平時のリスク管理体制を構築し適切に運用する	組織で管理している領域から保護すべきデータが漏洩する	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・入力確認の不備を突いたインジェクション攻撃 （例：SQL インジェクション、XSS） ・ネットワーク上の通信の盗聴 ・保護が必要なエリアに対する不正なヒトの物理的な侵入 ・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし ・正規ユーザによる内部不正	L1_1_a_ORG	**[ソシキ]** ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
						・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー、対策基準を明確化し、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。	CPS.BE-2
						・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。	CPS.SC-1
						・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・システムを管理するためのシステム開発ライフサイクルを導入する。	CPS.IP-3
				L1_1_a_PEO	**[ヒト]** ・自身が関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
					[ヒト] ・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し運用する。	CPS.SC-5
						・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	CPS.IP-9

				L1_1_a_COM	**[モノ]** ・モノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・自組織の資産が接続している外部情報システムの一覧を作成し適切に管理する。	CPS.AM-5
						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発行、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L1_1_a_SYS	**[システム]** ・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	CPS.RA-1
						・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	CPS.RA-3
						・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。 ・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。	CPS.RA-5
						・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。	CPS.RA-6

						・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。	CPS.RM-2
					[システム] ・自組織のシステムにおいて、対処すべき脆弱性が放置されている	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・IoT 機器、サーバー等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10
						・IoT 機器、サーバー等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1
						・自組織の IoT 機器、サーバー等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・自組織の管理している IoT 機器、サーバー等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7
					[システム] ・保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている	・IoT 機器、サーバー等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・IoT 機器、サーバー等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバー等の機能を必要最小限とする。	CPS.IP-2
					[システム] 保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3

						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発行、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・職務及び責任範囲（例：ユーザ／システム管理者）を適切に分離する。	CPS.AC-5
						・特権を持つユーザのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	CPS.AC-6
						・IoT 機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
					[システム] ・IoT 機器、サーバー等の設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・IoT 機器、サーバー等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバー等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5
						・IoT 機器、サーバー等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバー等の機能を必要最小限とする。	CPS.PT-2
						・IoT 機器、サーバー等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.CM-2
					[システム] ・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	CPS.PT-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	CPS.CM-1

						・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行う IoT 機器を導入する。 ・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
				L1_1_a_DAT	**[データ]** ・自組織で管理しているデータの保護に係る区分が明確になっていない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
					[データ] ・定められた機密区分に沿った情報の保護が実装されていない	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・情報を適切な強度の方式で暗号化して保管する。	CPS.DS-2
						・IoT 機器、サーバー等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	CPS.DS-3
						・情報を送受信する際に、情報そのものを暗号化して送受信する。	CPS.DS-4
						・送受信する情報データ、保管する情報データの暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	CPS.DS-5
						・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	CPS.DS-9
				L1_1_a_PRO	**[プロシージャ]** ・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	・セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。	CPS.GV-1

						・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。	CPS.GV-4
						・自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・取引先等の関係する他組織との契約が終了する際（例：契約期間の満了、サポートの終了）に実施すべきプロシージャを策定し、運用する。	CPS.SC-10
						・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	CPS.SC-11
						・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	CPS.IP-7

		自組織で管理している領域において保護すべきデータが改ざんされる	・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし ・通信系路上でデータを改ざんする中間者攻撃等 ・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・正規ユーザによる内部不正 ・保護が必要なエリアに対する不正なヒトの物理的な侵入 ・保護が必要なデータを扱う媒体の物理的な破壊	L1_1_b_ORG	[ソシキ] ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
						・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。	CPS.BE-2
						・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。	CPS.SC-1
						・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・システムを管理するためのシステム開発ライフサイクルを導入する。	CPS.IP-3
				L1_1_b_PEO	**[ヒト]** ・自身が関わりうるセキュリティやセーフティに関係するリスクに対して十分な認識を有していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
					[ヒト] ・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5
						・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	CPS.IP-9
				L1_1_b_COM	**[モノ]** ・情報システムや産業用制御システムを構成しているモノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5

						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発行、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L1_1_b_SYS	**[システム]** ・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	CPS.RA-1
						・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	CPS.RA-3
						・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。 ・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。	CPS.RA-5
						・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。	CPS.RA-6
						・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。	CPS.RM-2
					[システム] ・保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている	・IoT 機器、サーバー等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1

						・IoT 機器、サーバー等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバー等の機能を必要最小限とする。	CPS.PT-2
					[システム] ・保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発行、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・職務及び責任範囲（例：ユーザ／システム管理者）を適切に分離する。	CPS.AC-5
						・特権を持つユーザのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	CPS.AC-6
						・IoT 機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
					[システム] ・早期にネットワーク上での異常(例：なりすまし、メッセージの改ざん)を素早く検知し、対処するような仕組みがシステムに実装されていない	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。	CPS.AE-3
						・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3
						・セキュリティ事象の検知プロセスを継続的に改善する。	CPS.DP-4
				L1_1_b_PRO	**[プロシージャ]** ・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	・セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。	CPS.GV-1
						・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。	CPS.GV-4

						・自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・取引先等の関係する他組織との契約が終了する際（例：契約期間の満了、サポートの終了）に実施すべきプロシージャを策定し、運用する。	CPS.SC-10
						・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	CPS.SC-11
						・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	CPS.IP-7
				L1_1_b_DAT	**[データ]** ・通信路及び通信路上のデータが十分に保護されていない	・IoT 機器、サーバー等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	CPS.DS-3
						・情報を送受信する際に、情報そのものを暗号化して送受信する。	CPS.DS-4

					[データ] ・取り扱うデータに改ざんを検知するメカニズムがない	・送受信・保管する情報に完全性チェックメカニズムを使用する。	CPS.DS-11
		サービス拒否攻撃、ランサムウェアへの感染等に より、自組織のデータを取り扱うシステムが停止する	・システムを構成するサーバー等の電算機器、通信機器等に対するサービス拒否攻撃 ・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・妨害電波の発信	L1_1_c_ORG	**[ソシキ]** ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
						・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。	CPS.BE-2
						・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。	CPS.SC-1
						・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・システムを管理するためのシステム開発ライフサイクルを導入する。	CPS.IP-3
				L1_1_c_PEO	**[ヒト]** ・自身が関わりうるセーフティやセキュリティに関わるリスクに対して十分な認識を有していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
					[ヒト] ・ヒトに関わるセーフティやセキュリティに関係するリスクに対するガバナンスが十分でない	・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
						・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	CPS.IP-9

				L1_1_c_COM	**[モノ]** ・情報システムや制御システムを構成しているモノのセキュリティ状況やネットワーク接続状況が適切に管理（例：資産の棚卸し、モニタリング）されていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5
						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発行、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L1_1_c_SYS	**[システム]** ・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	CPS.RA-1
						・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	CPS.RA-3
						・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。	CPS.RA-4
						・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する	CPS.RA-5
						・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。	CPS.RA-6
						・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。	CPS.RM-2

					[システム] ・IoT、サーバー等に対する通信を適切に制御していない	・IoT 機器、サーバー等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバー等の機能を必要最小限とする。	CPS.PT-2
						・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	CPS.CM-1
					[システム] ・IoT、サーバー等に対する物理的な妨害（例：妨害電波）に対処できていない	・IoT 機器、サーバー等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバー等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5
						・IoT 機器、サーバー等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.CM-2
					[システム] ・IoT 機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。	CPS.DS-6
						・IoT 機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	CPS.DS-7
				L1_1_c_PRO	**[プロシージャ]** ・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	・セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。	CPS.GV-1
						・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。	CPS.GV-4
						・自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1

						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・取引先等の関係する他組織との契約が終了する際（例：契約期間の満了、サポートの終了）に実施すべきプロシージャを策定し、運用する。	CPS.SC-10
						・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	CPS.SC-11
						・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	CPS.IP-7
		法制度等で規定されている水準のセキュリティ対策を実装できない	All threats	L1_2_a_ORG	**[ソシキ]** ・遵守すべき法制度等を認識していないか、法制度に準 拠した組織内のルールを策定・運用していない	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	CPS.GV-2
						・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する。	CPS.DP-2
				L1_2_a_PEO	**[ヒト]** ・遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを遵守していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1

				L1_2_a_COM	**[モノ]** ・法制度等で一定の保護を義務付けられている種のモノが、要求される水準の保護を適用されていない	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	CPS.GV-2
				L1_2_a_SYS	**[システム]** ・法制度等で一定の保護を義務付けられている種のシステムが、要求される水準の保護を適用されていない	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	CPS.GV-2
				L1_2_a_PRO	**[プロシージャ]** ・組織内で規定されているプロシージャが関連する法規制等を遵守するような内容となっていない	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	CPS.GV-2
				L1_2_a_DAT	**[データ]** ・法制度等で一定の保護を義務付けられている種のデータが、要求される水準の保護を適用されていない	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	CPS.GV-2
1_2	組織としてセキュリティインシデント発生時においても適切に自組織の事業を継続すること	自組織のセキュリティインシデントにより自組織が適切に事業継続できない	All threats	L1_3_a_ORG	**[ソシキ]** ・セキュリティ事象を的確に検知するための体制が構築されていない	・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	CPS.AE-2
						・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする。	CPS.DP-1
						・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する。	CPS.DP-2
						・監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	CPS.DP-3
						・セキュリティ事象の検知プロセスを継続的に改善する。	CPS.DP-4
					[ソシキ] ・セキュリティインシデントに的確に対応するための体制が構築されていない	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情	CPS.RA-2

						報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	
						・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	CPS.AE-2
						・セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する。	CPS.IM-1
						・セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急事対応計画を継続的に改善する。	CPS.IM-2
				L1_3_a_PEO	**[ヒト]** ・セキュリティインシデント発生時に適切なアクションを取ることができない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
				L1_3_a_COM	**[モノ]** ・セキュリティインシデントにより被害を受けた自組織の事業の範囲(製品等)を特定することができない	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。	CPS.AM-2
						・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。	CPS.AM-3
						・セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。	CPS.AN-1
				L1_3_a_SYS	**[システム]** ・セキュリティインシデントを適切に検知するための機器等が導入されていないか、あるいは正しく運用されていない	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。	CPS.AE-3
						・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	CPS.CM-1

						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L1_3_a_PRO	**[プロシージャ]** ・自組織におけるセキュリティインシデントへの対応手順が策定されていない	・セキュリティ事象の危険度の判定基準を定める。	CPS.AE-5
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
						・セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。	CPS.AN-1
						・セキュリティインシデント発生後に、デジタルフォレンジックを実施する。	CPS.AN-2
						・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	CPS.AN-3
						・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。	CPS.MI-1
					[プロシージャ] ・事業継続計画にセキュリティインシデントが位置づけられておらず、セキュリティインシデント発生時に自組織の事業継続に支障が生じる	・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。	CPS.RP-3
						・セキュリティインシデント発生後の情報公表時のルールを策定し、運用する。	CPS.CO-1
						・事業継続計画又は緊急事対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	CPS.CO-2
						・復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急事対応計画の中に位置づける。	CPS.CO-3
				L1_3_a_DAT	**[データ]** ・セキュリティインシデント発生時に事業を継続するために必要なデータが、適切に準	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1

					備されていない、又は準備されてるが適切に機能しない	・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.AT-2
						・構成要素（IoT 機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする。	CPS.IP-4
						・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。	CPS.RP-3
		自組織のセキュリティインシデントにより関係する他組織が適切に事業継続できない	All threats	L1_3_b_ORG	**[ソシキ]** ・自組織のモノ/システム/データのサイバー空間における他組織との連携状況を把握していない	・組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。	CPS.AM-4
						・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
					[ソシキ] ・自組織と他組織(サプライヤー等)とのフィジカル空間における連携状況および責任分界を把握していない	・自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。	CPS.AM-7
						・サプライチェーンにおいて、自組織が担う役割を特定し共有する。	CPS.BE-1
						・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	CPS.BE-3
						・自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジ	CPS.RM-1

						メントの実施状況を確認するプロセスを確立し、実施する。	
				L1_3_b_PEO	**[ヒト]** ・他組織のヒトが自組織のセキュリティ事象発生時に適切なアクションを取ることができない	・サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	CPS.SC-9
						・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.AT-2
						・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
						・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	CPS.RP-2
				L1_3_b_COM	**[モノ]** ・セキュリティ事象による被害を受けたモノ(製品)・サービスが生じる	・セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ（製品）に対して適切な対応を行う。	CPS.RP-4
					[モノ] ・自組織が提供する/されるモノ(製品)に関する記録(例：製造日/識別ナンバー/提供先)が保持されていない	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。	CPS.AM-2
						・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。	CPS.AM-3
				L1_3_b_PRO	**[プロシージャ]** ・関係する他組織と連携したセキュリティ事象対応手順が策定されていない	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。	CPS.AE-4
						・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	CPS.RP-2
		関係する他組織のセキュリティインシデントにより自組織が適切に事業継続できない	All threats	L1_3_c_ORG	**[ソシキ]** ・自組織のモノ/システム/データのサイバー空間における他組織との連携状況を把握していない	・組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。	CPS.AM-4
						・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1

						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
					[ソシキ] ・自組織と他組織(サプライヤー等)とのフィジカル空間における連携状況および責任分界を把握していない	・自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。	CPS.AM-7
						・サプライチェーンにおいて、自組織が担う役割を特定し共有する。	CPS.BE-1
						・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	CPS.BE-3
						・自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	CPS.RM-1
				L1_3_c_PEO	**[ヒト]** ・自組織のヒトが他組織のセキュリティ事象発生時に適切なアクションを取ることができない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
						・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	CPS.RP-2
				L1_3_c_PRO	**[プロシージャ]** ・関係する他組織と連携したセキュリティ事象対応手順が策定されていない	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	CPS.RP-2
1_3	フィジカル空間での製品・サービスが、望まれる品質を備えて入荷又は出荷されること	製品・サービスの提供チャネルでセキュリティ事象が発生	・悪意を持った自組織内外のヒトによる不正改ざん ・正規の機器を模した偽造品の挿入	L1_1_d_ORG	**[ソシキ]** ・製品・サービスを調達する際、それが信頼できるものかを確認していない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織	CPS.SC-3

		し、機器の破損等の意図しない品質劣化が生じる				のセキュリティマネジメントが適合していることを確認する。	
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L1_1_d_PEO	**[ヒト]** ・自組織の調達に関わる要員が、調達に係るセキュリティリスクを十分に認識していない。	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
				L1_1_d_COM	**[モノ]** ・調達する製品・サービスが十分な物理的保護を実施されていない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。	CPS.DS-8
				L1_1_d_PRO	**[プロシージャ]** ・製品・サービスの調達時に、調達品の適格性を確認するプロシージャが存在しない	・送受信・保管する情報に完全性チェックメカニズムを使用する。	CPS.DS-11
						・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。	CPS.DS-12
						・IoT 機器やソフトウェアが正規品であることを定期的（起動時等）に確認する。	CPS.DS-13

（2）第 2 層：フィジカル空間とサイバー空間のつながり

項番	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件 ID
			脅威	脆弱性 ID	脆弱性		
2_共通	下記機能の双方 ・フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能 ・サイバー空間から受け取ったデータにより、一定のルールに基づいて、モノを制御したり、データを可視化したりする機能	脆弱性を悪用して IoT 機器（ドローン等）内部に不正アクセスされ、事前に想定されていない動作をする	・攻撃ツール等を利用した IoT 機器におけるセキュリティ上の脆弱性を利用したマルウェア感染	L2_1_a_ORG	**[ソシキ]** ・情報システムや産業用制御システムに接続している自組織の IoT 機器のセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・IoT 機器、サーバー等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・IoT 機器、サーバー等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
					[ソシキ] ・利用している IoT 機器に関わる脆弱性情報、脅威情報を収集・分析し、適切に対応していない。	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	CPS.IP-7
						・保護技術の有効性について、適切なパートナーとの間で情報を共有する。	CPS.IP-8
						・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10
						・IoT 機器、サーバー等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 ・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えた IoT 機器を導入する。	CPS.MA-1

						・自組織の IoT 機器、サーバー等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
				L2_1_a_COM	**[モノ]** ・利用している IoT 機器が十分なセキュリティ機能を実装していない	・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.RA-6
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。	CPS.DS-15
				L2_1_a_PRO	**[プロシージャ]** ・調達時に、適切なレベルのセキュリティ機能が実装されているかを確認するプロシージャがない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。	CPS.DS-15
						・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.RA-6
					[プロシージャ] ・IoT 機器の誤動作を検知した後の対応手順が定義されていない	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システム	CPS.RP-1

						の対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	
		正規のユーザになりすましてIoT 機器内部に不正アクセスされ、事前に想定されていない動作をする	・窃取した ID 等を利用した正規ホストへのなりすまし ・セキュリティが実装されていない脆弱なプロトコルを悪用した不正アクセス	L2_1_b_ORG	**[ソシキ]** ・ネットワークの適正利用を確認していない	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	CPS.PT-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	CPS.CM-1
				L2_1_b_COM	**[モノ]** ・セキュリティの観点において強度が十分でない設定(パスワード、ポート等)がなされている	・IoT 機器、サーバー等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・IoT 機器、サーバー等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバー等の機能を必要最小限とする。	CPS.PT-2
				L2_1_b_SYS	**[システム]** ・通信相手に対するアクセス制御が十分でない	・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT 機器、サーバー等に対する不正ログインを防ぐ。	CPS.AC-4
						・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT 機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	CPS.AC-7
						・IoT 機器、サーバー等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	CPS.AC-8
						・IoT 機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
				L2_1_b_PRO	**[プロシージャ]** ・IoT 機器のセキュリティ設定手順が定められていない	・IoT 機器、サーバー等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1

					[プロシージャ] ・IoT 機器の誤動作を検知した後の対応手順が定義されていない	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
		遠隔から IoT 機器を管理するシステムに不正アクセスされ、IoT 機器に不正な入力をされ、事前に想定されていない動作をする。	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし ・IoT 機器を管理するシステムから IoT 機器への不正なコマンド送信	L2_1_c_ORG	**[ソシキ]** ・IoT 機器を管理するシステムのセキュリティ対策状況（ソフトウェア構成情報、パッチ適用状況等）を把握できていない	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L2_1_c_SYS	**[システム]** ・システム管理権限に対するアクセス制御が十分でない	・職務及び責任範囲（例：ユーザ／システム管理者)を適切に分離する 。	CPS.AC-5
						・特権を持つユーザのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	CPS.AC-6
					[システム] ・システムにおいて対処すべき脆弱性が適切に対処されていない	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・IoT 機器、サーバー等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・IoT 機器、サーバー等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1
						・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えた IoT 機器を導入する。	CPS.MA-1
						・自組織の IoT 機器、サーバー等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6

						・自組織の管理している IoT 機器、サーバー等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7
				L2_1_c_PRO	**[プロシージャ]** ・IoT 機器の誤動作を検知した後の対応手順が定義されていない	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
		サービス拒否攻撃等により、IoT 機器や通信機器等の機能が停止する	・IoT システムを構成する IoT 機器、通信機器等に対するサービス拒否攻撃	L2_1_d_SYS	**[システム]** ・IoT 機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する。	CPS.DS-6
						・IoT 機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	CPS.DS-7
						・構成要素（IoT 機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする。	CPS.IP-4
				L2_1_d_PRO	**[プロシージャ]** ・IoT 機器の停止を検知した後の対応手順が定義されていない	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
2_1	サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、モノを制御したり、データを可視化したりする機能	正常動作・異常動作に関わらず、安全に支障をきたすような動作をする	・不正なエンティティによるコマンドインジェクション攻撃 ・サイバー空間からの許容範囲外のインプットデータ ・マルウェアによる制御信号の改ざん	L2_2_a_ORG	**[ソシキ]** ・機器を調達する際、安全性を実装しているかを確認していない	・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7

						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
						・ネットワークにつながることを踏まえた安全性を実装する IoT 機器を導入する。	CPS.PT-3
				L2_2_a_COM	**[モノ]** ・インプットされたデータを検証する仕組みが無い	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行う IoT 機器を導入する。 ・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3
				L2_2_a_SYS	**[システム]** ・稼動するシステムとして、安全計装が考慮されていない。	・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	CPS.RA-4
						・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 ・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	CPS.RA-6
				L2_2_a_PRO	**[プロシージャ]** ・安全に支障をきたしうる機器等の兆候を発見した際のプロシージャが定められていない	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
2_2	フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能	データが IoT 機器・サイバー空間間の通信路上で改ざんされる	・通信系路上でデータを改ざんする中間者攻撃等	L2_3_a_ORG	**[ソシキ]** ・機器を調達する際、改ざん検知機能及び改ざん防止機能を実装しているかを確認していない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。	CPS.DS-15

		(監視が行き届かない場所に設置された機器の運用中、あるいは廃止後の盗難等の後)改ざんされた IoT 機器がネットワーク接続され、故障や正確でないデータの送信等が発生する	・盗難等により不正な改造を施された IoT 機器によるネットワーク接続 ・悪意を持った自組織内外のヒトによる不正改ざん ・センサーの測定値、閾値、設定の改ざん	L2_3_b_ORG	**[ソシキ]** ・自組織の情報システムや産業用制御システムに接続している機器の状態を把握できていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・IoT 機器、サーバー等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
				L2_3_b_PEO	**[ヒト]** ・自組織内外のヒトによる IoT 機器に対する物理的な不正行為を防げない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5
						・IoT 機器、サーバー等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・IoT 機器、サーバー等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.CM-2
				L2_3_b_COM	**[モノ]** ・利用している機器に耐タンパー性がなく、物理的な改ざんを防げない	・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。	CPS.DS-8
				L2_3_b_SYS	**[システム]** ・定期的に接続機器の完全性を検証していない	・IoT 機器、サーバー等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。	CPS.DS-10
						・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。	CPS.DS-12
					[システム] ・不正な機器がネットワークに接続されたことを適切に検知できない。	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6

					[システム] ・IoT 機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・IoT 機器、サーバー等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバー等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5
						・IoT 機器、サーバー等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバー等の機能を必要最小限とする。	CPS.PT-2
						・IoT 機器、サーバー等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.CM-2
				L2_3_b_DAT	**[データ]** ・IoT 機器の廃止時に、データを削除（又は読み取りできない状態に）する手順がない	・IoT 機器、サーバー等の廃止時には、内部に保存されているデータ及び、正規 IoT 機器、サーバー等を一意に識別する ID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする。	CPS.IP-6
		品質や信頼性の低い IoT 機器がネットワーク接続され、故障や正確でないデータの送信、想定していない通信先へのデータ送信等が発生する	・品質や信頼性の低い IoT 機器のネットワーク接続 ・正規の機器を模した偽造品の挿入	L2_3_c_ORG	**[ソシキ]** ・IoT 機器を調達する際、調達製品が信頼できるものかを確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見さ	CPS.SC-7

						れた場合に実施すべきプロシージャを策定し、運用する。	
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
					[ソシキ] ・運用時に IoT 機器やソフトウェアが正規品である（改ざんされていない）ことを確認していない	・IoT 機器やソフトウェアが正規品であることを定期的（起動時等）に確認する。	CPS.DS-13
				L2_3_c_SYS	**[システム]** ・不正な機器によるネットワーク接続（有線あるいは無線）を防止できない	・IoT 機器、サーバー等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無線接続先（ユーザや IoT 機器、サーバー等）を正しく認証する。	CPS.AC-3
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
					[システム] ・組織外部への不正な通信を適切に検知し、遮断する等の対応ができない	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	CPS.DS-9
						・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	CPS.CM-1
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
					[システム] ・サイバー空間および正規の機器に接続する機器が正規のものかを確認する仕組みが実装されていない	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発行、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・IoT 機器やソフトウェアが正規品であることを定期的（起動時等）に確認する。	CPS.DS-13

				L2_3_c_PRO	**[プロシージャ]** ・IoT 機器を調達する際に、調達製品が信頼できるものかを確認するプロシージャがない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
		計測機能に対する物理的な不正行為により、正確でないデータの送信等が発生する	・悪意を持った自組織内外のヒトによる計測機能に対する不正行為	L2_3_d_ORG	**[ソシキ]** ・IoT 機器を調達する際、調達製品が計測セキュリティを考慮しているものかを確認していない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。	CPS.DS-15
				L2_3_d_SYS	**[システム]** ・IoT 機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・IoT 機器、サーバー等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2
						・無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバー等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5
						・IoT 機器、サーバー等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.CM-2

（3）第 3 層：サイバー空間におけるつながり

項番	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件 ID
			脅威	脆弱性 ID	脆弱性		
3_共通	下記すべてに関わる ・データを加工・分析する機能 ・データを保管する機能 ・データを送受信する機能	サービス拒否攻撃により、関係する他組織における自組織のデータを取り扱うシステムが停止する	・システムを構成するサーバー等の電算機器、通信機器等に対するサービス拒否攻撃 ・妨害電波の発信	L3_3_b_ORG	**[ソシキ]** ・データの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
		攻撃の有無に関わらず、データを取り扱うシステムが停止する	・品質や信頼性の低いシステムによるサービス提供	L3_3_c_ORG	**[ソシキ]** ・サービスサプライヤーに対して、組織、システム等の信頼性を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3

						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L3_3_c_SYS	**[システム]** ・IoT 機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例：ヒト、モト、システム）を確保する。	CPS.DS-6
						・IoT 機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	CPS.DS-7
						・構成要素（IoT 機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする。	CPS.IP-4
		サイバー空間におけるデータ保護を規定する法規制等への違反が発生する	・データ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・データ保管エリアに対する不正なエンティティの物理的な侵入 ・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし	L3_4_a_ORG	**[ソシキ]** ・保護すべきデータの管理に関する組織内の責任が明確でない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
					[ソシキ] ・対応が必要なデータ保護に関する法規制等を十分に認識してない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3

				L3_4_a_PEO	**[ヒト]** ・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
				L3_4_a_PRO	**[プロシージャ]** ・データの取り扱いについて、必要なプロシージャを規定していない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
					[プロシージャ] ・データの取り扱いについて、必要なプロシージャを満たしているかを確認していない	・データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する。	CPS.DS-14
				L3_4_a_DAT	**[データ]** ・複数の組織、システム等に個人情報等が分散して所在している	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
					[データ] 自組織で扱うデータが保護が必要な特定の種類のデータであることが識別されていない	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取り決める。	CPS.DS-1
		一部の関係者だけで共有する秘匿性の高いデータのセキュリティ要求が設定・対応されていない	・データ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・データ保管エリアに対する不正なエンティティの物理的な侵入 ・正規ユーザによる内部不正 ・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし	L3_4_b_ORG	**[ソシキ]** ・対応が必要なデータ保護に関する法規制等を十分に認識してない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
				L3_4_b_PEO	**[ヒト]** ・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1

						・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
				L3_4_b_PRO	**[プロシージャ]** ・データの取り扱いについて、必要なプロシージャを規定していない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
					[プロシージャ] ・データの取り扱いについて、必要なプロシージャを満たしているかを確認していない	・データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理 する。	CPS.DS-14
				L3_4_b_SYS	**[システム]** ・データを扱うシステムにおいてデータの秘匿性に応じた設計がなされていない	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT 機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	CPS.AC-7
						・IoT 機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
						・情報を適切な強度の方式で暗号化して保管する。	CPS.DS-2
				L3_4_b_DAT	**[データ]** ・複数の組織、システム等に個人情報等が分散して所在している	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
					[データ] ・自組織で扱うデータが保護が必要な特定の種類のデータであることが識別されていない	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取り決める。	CPS.DS-1
3_1	データを加工・分析する機能 ・航路画定 ・航路予約	関係する他組織で管理している(データ加工・分析)領	・他組織の管理するデータ加工・分析システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染	L3_1_b_ORG	**[ソシキ]** ・データを加工・分析する組織、システム等	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2

	・安全管理 ・離着陸場/機体管理 ・外部データ参照 ・ユーザ認証	域から自組織の保護すべきデータが漏洩する	・他組織の管理するデータ加工・分析エリアに対する不正なエンティティの物理的な侵入 ・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし ・他組織のエンティティによる保護すべきデータの適切でない持出行為		の安全性・信頼性を契約前、契約後に確認していない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L3_1_b_PEO	[ヒト] ・データの加工・分析を委託する組織における要員の信頼性を契約前、契約後に確認していない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5
				L3_1_b_DAT	**[データ]** ・セキュリティ水準が統一されていない複数の組織、システム等に自組織の保護すべき情報が分散して所在している	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
		データ加工・分析システムが誤動作することで、適切でない分析結果が出力される	・データ加工・分析システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染	L3_3_d_ORG	**[ソシキ]** ・データを加工・分析する組織、システム等	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2

			・データ加工・分析システムに対する攻撃コードを含んだ許容範囲外のインプットデータ		の安全性・信頼性を契約前、契約後に確認していない	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L3_3_d_SYS	**[システム]** ・データを加工・分析するシステムにおいて、セキュアでない設定がなされている	・IoT 機器、サーバー等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・IoT 機器、サーバー等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバー等の機能を必要最小限とする。	CPS.PT-2
					[システム] ・データを加工・分析するシステムにおいて、対処すべき脆弱性が放置されている	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・IoT 機器、サーバー等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10

						・IoT 機器、サーバー等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1
						・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT 機器を導入する。	CPS.MA-1
						・自組織の IoT 機器、サーバー等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・自組織の管理している IoT 機器、サーバー等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7
					[システム] ・システム上でデータが十分に保護されていない	・情報を適切な強度の方式で暗号化して保管する。	CPS.DS-2
						・IoT 機器、サーバー等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	CPS.DS-3
						・情報を送受信する際に、情報そのものを暗号化して送受信する。	CPS.DS-4
					[システム] インプットとなるデータを十分に確認していない	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行う IoT 機器を導入する。 ・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3
						・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.CM-4
					[システム] ・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	CPS.PT-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1

						・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	CPS.CM-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
3_2	データを保管する機能 ・航路画定 ・航路予約 ・安全管理 ・離着陸場/機体管理 ・外部データ参照 ・ユーザ認証	自組織で管理している(データ保管)領域から関係する他組織の保護すべきデータが漏洩する	・他組織の管理するデータ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・他組織の管理するデータ保管エリアに対する不正なエンティティの物理的侵入 ・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし ・自組織における悪意あるエンティティによる保護すべきデータの持出し	L3_1_a_ORG	**[ソシキ]** ・保護すべきデータの管理に関する組織内の責任が明確でない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
				L3_1_a_SYS	**[システム]** ・関係する他組織の保護すべきデータを格納するシステムにおいて、セキュアでない設定がなされている	・IoT 機器、サーバー等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する。	CPS.IP-1
						・IoT 機器、サーバー等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバー等の機能を必要最小限とする。	CPS.PT-2
					[システム] ・自組織のシステムにおいて、対処すべき脆弱性が放置されている	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・IoT 機器、サーバー等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10
						・IoT 機器、サーバー等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1
						・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えた IoT 機器を導入する。	CPS.MA-1

						・自組織の IoT 機器、サーバー等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・自組織の管理している IoT 機器、サーバー等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7
					[システム] 保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3
						・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発行、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・職務及び責任範囲（例：ユーザ／システム管理者)を適切に分離する 。	CPS.AC-5
						・特権を持つユーザのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する。	CPS.AC-6
						・IoT 機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
					[システム] ・IoT 機器、サーバー等の設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	・IoT 機器、サーバー等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	CPS.AC-2

						・無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバー等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	CPS.IP-5
						・IoT 機器、サーバー等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバー等の機能を必要最小限とする。	CPS.PT-2
						・IoT 機器、サーバー等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	CPS.CM-2
					[システム] ・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	CPS.PT-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	CPS.CM-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
				L3_1_a_PRO	**[プロシージャ]** ・他組織から管理を委託されるデータの機密区分および必要なセキュリティ対策について確認するプロシージャがない	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取り決める。	CPS.DS-1
				L3_1_a_DAT	**[データ]** ・他組織から管理を委託されているデータの保護に係る区分が明確になっていない	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	CPS.GV-3

					[データ] ・定められた機密区分に沿った情報の保護が実装されていない	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT 機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する。	CPS.AC-7
						・情報を適切な強度の方式で暗号化して保管する。	CPS.DS-2
						・IoT 機器、サーバー等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	CPS.DS-3
						・情報を送受信する際に、情報そのものを暗号化して送受信する。	CPS.DS-4
						・送受信する情報データ、保管データする情報の暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	CPS.DS-5
						・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	CPS.DS-9
		関係する他組織で管理している(データ保管)領域から自組織の保護すべきデータが漏洩する	・他組織の管理するデータ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・他組織の管理するデータ保管エリアに対する不正なエンティティの物理的侵入 ・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし ・自組織における悪意あるエンティティによる保護すべきデータの持出し	L3_1_c_ORG	**[ソシキ]** ・データを保管する組織、システム等の安全性を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6

						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L3_1_c_PEO	**[ヒト]** ・データの加工を委託する組織における要員の信頼性を契約前、契約後に確認していない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5
				L3_1_c_DAT	**[データ]** ・セキュリティ水準が統一されていない複数の組織、システム等に自組織の保護すべき情報が分散して所在している	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
		関係する他組織で保管中の自組織の保護すべきデータが改ざんされる	・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし	L3_2_a_DAT	**[データ]** ・保管中のデータに改ざんを検知するメカニズムがない	・送受信・保管する情報に完全性チェックメカニズムを使用する。	CPS.DS-11
3_3	データを送受信する機能 ・航路画定 ・航路予約 ・安全管理 ・離着陸場/機体管理 ・外部データ参照 ・ユーザ認証	関係する他組織で使用中の自組織の保護すべきデータが改ざんされる	・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし ・通信系路上でデータを改ざんする中間者攻撃等	L3_2_b_DAT	**[データ]** ・通信路上でデータが十分に保護されていない	・IoT 機器、サーバー等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	CPS.DS-3
						・情報を送受信する際に、情報そのものを暗号化して送受信する。	CPS.DS-4
					[データ] ・使用中のデータに改ざんを検知するメカニズムがない	・送受信・保管する情報に完全性チェックメカニズムを使用する。	CPS.DS-11
		(なりすまし等をした)ソシキ/ヒト/モノ等から不適切なデータを受信する	・不正な組織/ヒト/モノ/システムによる正規エンティティへのなりすまし ・改ざん等された正規なモノ/システムからの適切でないデータの受信	L3_3_a_ORG	**[ソシキ]** ・データ送信元となるデータの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	CPS.SC-3

						・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	CPS.SC-4
						・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	CPS.SC-6
						・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	CPS.SC-7
						・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	CPS.SC-8
				L3_3_a_PEO	**[ヒト]** ・自組織の保護すべきデータのセキュリティ上の扱いについて、外部委託先の担当者が十分に認識していない	・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	CPS.AT-2
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
				L3_3_a_SYS	**[システム]** ・データを収集・分析等するシステムにおいて、対処すべき脆弱性が放置されている	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	CPS.RA-2
						・IoT 機器、サーバー等の導入後に、追加するソフトウェアを制限する。	CPS.IP-2
						・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	CPS.IP-10
						・IoT 機器、サーバー等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。	CPS.MA-1

						・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT 機器を導入する。	CPS.MA-1
						・自組織の IoT 機器、サーバー等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	CPS.MA-2
						・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	CPS.CM-6
						・自組織の管理している IoT 機器、サーバー等に対して、定期的に対処が必要な脆弱性の有無を確認する。	CPS.CM-7
					[システム] ・通信路が適切に保護されていない	・IoT 機器、サーバー等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	CPS.DS-3
					[システム] ・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みが自組織のシステムに実装されていない	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	CPS.PT-1
						・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	CPS.AE-1
						・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	CPS.CM-1
						・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	CPS.CM-5
						・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	CPS.RP-1
					[システム] ・サイバー空間との通信開始時に、通信相手を識別・認証していない	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発行、管理、確認、取消、監査するプロシージャを確立し、実施する。	CPS.AC-1
						・無線接続先（ユーザや IoT 機器、サーバー等）を正しく認証する。	CPS.AC-3

						・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT 機器、サーバー等に対する不正ログインを防ぐ。	CPS.AC-4
						・IoT 機器、サーバー等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する。	CPS.AC-8
						・IoT 機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する。	CPS.AC-9
				L3_3_a_DAT	**[データ]** ・通信相手のエンドポイントから送信されるデータをフィルタリングする仕組みが導入・運用されていない	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行う IoT 機器を導入する。 ・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	CPS.CM-3
						・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	CPS.CM-4

付録 10：脆弱性一覧

第1層					
[ソシキ]	[ヒト]	[モノ]	[データ]	[プロシージャ]	[システム]
・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・自身が関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない	・モノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない	・自組織で管理しているデータの保護に係る区分が明確になっていない	・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない
・遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを策定・運用していない	・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	・情報システムや制御システムを構成しているモノのセキュリティ状況やネットワーク接続状況が適切に管理（例：資産の棚卸し、モニタリング）されていない	・定められた機密区分に沿った情報の保護が実装されていない	・組織内で規定されているプロシージャが関連する法規制等を遵守するような内容となっていない	・自組織のシステムにおいて、対処すべき脆弱性が放置されている
・セキュリティ事象を的確に検知するための体制が構築されていない	・遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを遵守していない	・法制度等で一定の保護を義務付けられている種のモノが、要求される水準の保護を適用されていない	・通信路及び通信路上のデータが十分に保護されていない	・自組織におけるセキュリティインシデントへの対応手順が策定されていない	・保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている
・セキュリティインシデントに的確に対応するための体制が構築されていない	・セキュリティインシデント発生時に適切なアクションを取ることができない	・セキュリティインシデントにより被害を受けた自組織の事業の範囲(製品等)を特定することができない	・取り扱うデータに改ざんを検知するメカニズムがない	・事業継続計画にセキュリティインシデントが位置づけられておらず、セキュリティインシデント発生時に自組織の事業継続に支障が生じる	保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない
・自組織のモノ/システム/データのサイバー空間における他組織との連携状況を把握していない	・他組織のヒトが自組織のセキュリティ事象発生時に適切なアクションを取ることができない	・セキュリティ事象による被害を受けたモノ(製品)・サービスが生じる	・法制度等で一定の保護を義務付けられている種のデータが、要求される水準の保護を適用されていない	・関係する他組織と連携したセキュリティ事象対応手順が策定されていない	・IoT機器、サーバー等の設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない
・自組織と他組織(サプライヤー等)とのフィジカル空間における連携状況および責任分界を把握していない	・自組織のヒトが他組織のセキュリティ事象発生時に適切なアクションを取ることができない	・自組織が提供する/されるモノ(製品)に関する記録(例：製造日/識別ナンバー/提供先)が保持されていない	・セキュリティインシデント発生時に事業を継続するために必要なデータが、適切に準備されていない、又は準備されてるが適切に機能しない	・製品・サービスの調達時に、調達品の適格性を確認するプロシージャが存在しない	・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない
・製品・サービスを調達する際、それが信頼できるものかを確認していない	・自組織の調達に関わる要員が、調達に係るセキュリティリスクを十分に認識していない	・調達する製品・サービスが十分な物理的保護を実施されていない			・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない
					・早期にネットワーク上での異常(例：なりすまし、メッセージの改ざん)を素早く検知し、対処するような仕組みがシステムに実装されていない
					・IoT、サーバー等に対する通信を適切に制御していない
					・IoT、サーバー等に対する物理的な妨害（例：妨害電波）に対処できていない
					・IoT機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない
					・法制度等で一定の保護を義務付けられている種のシステムが、要求される水準の保護を適用されていない
					・セキュリティインシデントを適切に検知するための機器等が導入されていないか、あるいは正しく運用されていない

第2層					
[ソシキ]	[ヒト]	[モノ]	[データ]	[プロシージャ]	[システム]
・情報システムや産業用制御システムに接続している自組織のIoT機器のセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない	・自組織内外のヒトによるIoT機器に対する物理的な不正行為を防げない	・利用しているIoT機器が十分なセキュリティ機能を実装していない	・IoT機器の廃棄時に、データを削除（又は読み取りできない状態に）する手順がない	・調達時に、適切なレベルのセキュリティ機能が実装されているかを確認するプロシージャがない	・通信相手に対するアクセス制御が十分でない
・利用しているIoT機器に関わる脆弱性情報、脅威情報を収集・分析し、適切に対応していない。		・セキュリティの観点において強度が十分でない設定(パスワード、ポート等)がなされている		・IoT機器の誤動作を検知した後の対応手順が定義されていない	・システム管理権限に対するアクセス制御が十分でない
・ネットワークの適正利用を確認していない		・インプットされたデータを検証する仕組みが無い		・IoT機器のセキュリティ設定手順が定められていない	・システムにおいて対処すべき脆弱性が適切に対処されていない
・IoT機器を管理するシステムのセキュリティ対策状況（ソフトウェア構成情報、パッチ適用状況等）を把握できていない		・利用している機器に耐タンパー性がなく、物理的な改ざんを防げない		・IoT機器の停止を検知した後の対応手順が定義されていない	・IoT機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない
・機器を調達する際、安全性を実装しているかを確認していない				・安全に支障をきたしうる機器等の兆候を発見した際のプロシージャが定められていない	・稼動するシステムとして、安全計装が考慮されていない。
・機器を調達する際、改ざん検知機能及び改ざん防止機能を実装しているかを確認していない				・IoT機器を調達する際に、調達製品が信頼できるものかを確認するプロシージャがない	・定期的に接続機器の完全性を検証していない
・自組織の情報システムや産業用制御システムに接続している機器の状態を把握できていない					・不正な機器がネットワークに接続されたことを適切に検知できない。
・IoT機器を調達する際、調達製品が信頼できるものかを確認していない					・IoT機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない
・運用時にIoT機器やソフトウェアが正規品である（改ざんされていない）ことを確認していない					・不正な機器によるネットワーク接続（有線あるいは無線）を防止できない
・IoT機器を調達する際、調達製品が計測セキュリティを考慮しているものかを確認していない					・組織外部への不正な通信を適切に検知し、遮断する等の対応ができない
					・サイバー空間および正規の機器に接続する機器が正規のものかを確認する仕組みが実装されていない

第3層					
[ソシキ]	[ヒト]	[モノ]	[データ]	[プロシージャ]	[システム]
・データの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない		・複数の組織、システム等に個人情報等が分散して所在している	・データの取り扱いについて、必要なプロシージャを規定していない	・IoT機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない
・サービスサプライヤーに対して、組織、システム等の信頼性を契約前、契約後に確認していない	・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない		・自組織で扱うデータが保護が必要な特定の種類のデータであることが識別されていない	・データの取り扱いについて、必要なプロシージャを満たしているかを確認していない	・データを扱うシステムにおいてデータの秘匿性に応じた設計がなされていない
・保護すべきデータの管理に関する組織内の責任が明確でない	・データの加工・分析を委託する組織における要員の信頼性を契約前、契約後に確認していない		・セキュリティ水準が統一されていない複数の組織、システム等に自組織の保護すべき情報が分散して所在している	・他組織から管理を委託されるデータの機密区分および必要なセキュリティ対策について確認するプロシージャがない	・データを加工・分析するシステムにおいて、セキュアでない設定がなされている
・対応が必要なデータ保護に関する法規制等を十分に認識してない	・データの加工を委託する組織における要員の信頼性を契約前、契約後に確認していない		・他組織から管理を委託されているデータの保護に係る区分が明確になっていない		・データを加工・分析するシステムにおいて、対処すべき脆弱性が放置されている
・データを加工・分析する組織、システム等の安全性・信頼性を契約前、契約後に確認していない	・自組織の保護すべきデータのセキュリティ上の扱いについて、外部委託先の担当者が十分に認識していない		・定められた機密区分に沿った情報の保護が実装されていない		・システム上でデータが十分に保護されていない
・データを保管する組織、システム等の安全性を契約前、契約後に確認していない			・保管中のデータに改ざんを検知するメカニズムがない		・インプットとなるデータを十分に確認していない
・データ送信元となるデータの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない			・通信路上でデータが十分に保護されていない		・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない
			・使用中のデータに改ざんを検知するメカニズムがない		・関係する他組織の保護すべきデータを格納するシステムにおいて、セキュアでない設定がなされている
			・通信相手のエンドポイントから送信されるデータをフィルタリングする仕組みが導入・運用されていない		・自組織のシステムにおいて、対処すべき脆弱性が放置されている
					・保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない
					・IoT機器、サーバー等の設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない
					・データを収集・分析等するシステムにおいて、対処すべき脆弱性が放置されている
					・通信路が適切に保護されていない
					・サイバー空間との通信開始時に、通信相手を識別・認証していない