経済産業省

資料６

産業サイバーセキュリティ研究会WG１
宇宙産業SWG（第５回）

事務局説明資料

令和４年７月２１日

経済産業省 製造産業局 宇宙産業室

１．宇宙分野における海外のサイバーセキュリティ対策等

２．宇宙分野における近年のセキュリティインシデント事例

【米国】NISTIR 8270：商用衛星運用のためのセキュリティ入門書のドラフト第2稿

- 2022年2月、米国NISTは、**商用衛星運用のためのセキュリティ入門書であるNISTIR 8270のドラフト第2稿を発表**し、パブコメを開始した。パブコメは4月8日まで実施された。
- 文書では、NISTのCybersecurity Framework（CSF）を実践するための7つのステップに基づき、**商用衛星運用におけるサイバーセキュリティリスク管理の基本ステップを示している**ほか、本ステップに基づく具体的なリスク管理の例として、地球低軌道上の小型衛星に適用した場合のケーススタディも示されている。

NISTIR 8270における商用衛星運用におけるサイバーセキュリティリスク管理の基本ステップ

Step 1：優先順位付けを行い、範囲を決定する	● 商用衛星システムアーキテクチャの構成要素を把握する。 ● 組織のミッションや事業目標に応じたサイバーセキュリティプログラムの範囲を決定する。
Step 2：方向付けを行う	● 対象となるシステムに関連する資産及び規制要件や、全体的なリスクアプローチを特定する。 ● 対象となるシステムや資産に適用される脅威及び脆弱性を特定する。
Step 3：現在のプロファイル※を作成する	● 対象となるシステムや資産に対して既に実施している対策をCSFのサブカテゴリーに基づきリスト化する。 ● サブカテゴリーへの対応状況を踏まえ、CSFの5つの機能（識別・防御・検知・対応・復旧）に対する対策実施状況を評価する。
Step 4：リスクアセスメントを実施する	● 商用衛星システムの運用環境を分析し、新たなサイバーセキュリティリスクを特定する。 ● 内外のサイバー脅威情報を使用し、セキュリティインシデントの可能性や当該インシデントが組織に与える影響を分析する。
Step 5：目標のプロファイルを作成する	● 組織に期待されるサイバーセキュリティの成果について記述した目標となるプロファイルを作成する。 ● 組織固有のリスクに対処するために、組織独自のサブカテゴリーを追加することができる。
Step 6：ギャップを判断・分析し、優先順位付けを行う	● 現在のプロファイルと目標のプロファイルを比較し、サイバーセキュリティの取組に関するギャップを特定する。 ● 目標のプロファイルに記された成果を達成するための行動計画を策定する。
Step 7：行動計画を実施する	● Step 6で特定されたギャップに対して取るべき行動を決定する。 ● プロファイルの見直し、ギャップの再評価、行動計画の更新は、2年に一度、又は重大なインシデント等があった際に実施する。

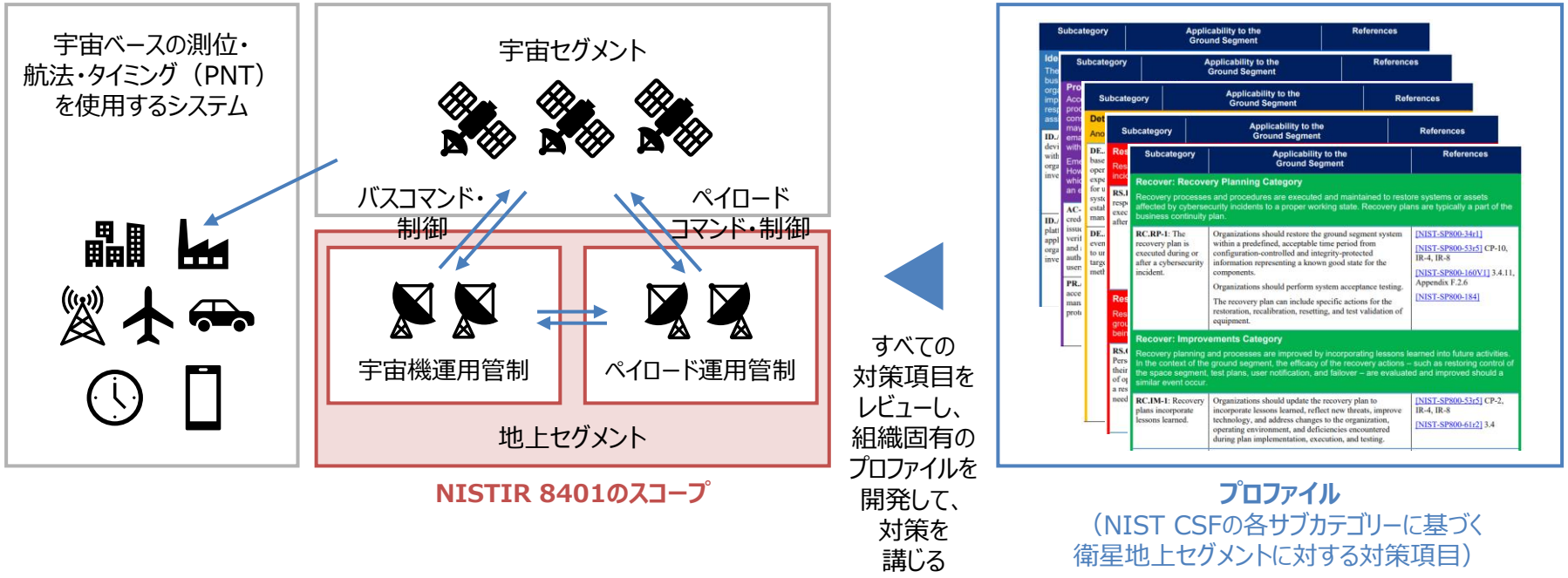
※ プロファイルとは、現在のセキュリティ対策と目指すべきセキュリティ対策を、自組織の事業上の要求事項やリスク許容度、割当可能なリソース等に踏まえて整理したもの。

出所）NIST, NISTIR 8270 (Draft) Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)に基づき三菱総合研究所作成
https://csrc.nist.gov/publications/detail/nistir/8270/draft

【米国】NISTIR 8401：衛星地上セグメントに対するNIST CSFプロファイルのドラフト

- 2022年4月、米国NISTは、**NIST CSFに基づく衛星地上セグメントのためのプロファイルに関する文書であるNISTIR 8401のドラフトを公開**し、パブコメを開始した。パブコメは6月20日まで実施された。
- 文書では、特に**宇宙機運用管制及びペイロード運用管制の2つに焦点**を当て、NIST CSFで規定されたサブカテゴリー毎に、**衛星地上セグメントに対する対策項目及び対策の参考となる文献が明記**されている。
- NISTは、本プロファイルを活用する組織に対し、**自組織のシステムに対して適用する際に、すべての対策項目をレビューすること**、組織の事業目標に基づくサイバーセキュリティ活動を実践するために、**各組織固有のプロファイルを開発すること**を奨励している。

NISTIR 8401のスコープ及びプロファイルの活用イメージ



出所）NIST, NISTIR 8401 (Draft) Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Controlに基づき三菱総合研究所作成
https://csrc.nist.gov/publications/detail/nistir/8401/draft

【米国】商用衛星システムに対するサイバーセキュリティ対策に関する法案の提出

- 2022年1月、ゲイリー・ピーターズ上院議員により、**CISAに対して、商用衛星システムの開発・保守・運用に関するサイバーセキュリティ勧告の策定を求める「衛星サイバーセキュリティ法」の法案**が上院に提出された。
- 同法案では、CISA長官に対し、**商用衛星システムのサイバーセキュリティに関する情報やシステムの安全な開発・運用・保守を支援する情報をオンラインで提供**する「商用衛星システムに関するサイバーセキュリティ情報センター」を**法案成立から180日以内に構築すること**を求めている。
- 加えて、米国会計検査院（GAO）に対して、**連邦政府による商用衛星産業に対するサイバーセキュリティ支援の状況を調査・報告すること**も求めている。
- 2022年4月には、トム・マリンノースキー下院議員及びアンドリュー・ガルバリーノ下院議員により、**同様の法案が下院にも提出**された。

注）いずれの法案も、上院・下院に提出された段階であり、審議中であることに留意。

出所）US Congress, S.3511 - Satellite Cybersecurity Act https://www.congress.gov/bill/117th-congress/senate-bill/3511,
H.R.7629 - Satellite Cybersecurity Act https://www.congress.gov/bill/117th-congress/house-bill/7629

【米国】国際衛星通信ネットワークへの脅威に対するセキュリティアドバイザリーの発表

- 2022年3月、米国CISA及びFBIは、**国際衛星通信のネットワークに対するサイバー攻撃の脅威に関する緩和策や関連情報をまとめたセキュリティアドバイザリーであるAA22-076Aを発表**した。
- 衛星通信ネットワークのプロバイダーに対し、**衛星通信機器における異常なトラフィックを検出するための追加監視を実施すること**、サイバー脅威活動を把握するために**ODNIレポート※を参照すること**を強く推奨した。
- また、衛星通信ネットワークのプロバイダー及び顧客に対して、**すべてのアカウントに対する安全な認証方法を使用すること**、**最小特権の原則を適用すること**、**ITサービスプロバイダーとの信頼関係を確認すること**等の緩和策の実施を強く推奨した。

※ Office of the Director of National Intelligence（米国国家情報長官官房）の"Annual Threat Assessment of the U.S. Intelligence Community"のこと。最新版は2022年3月8日に公開。

AA22-076Aにおいて衛星通信ネットワークのプロバイダー及び顧客に推奨される緩和策

衛星通信ネットワークのプロバイダーに対する推奨緩和策

- 通信衛星機器における異常なパケットを検出するための追加監視を行うこと
- 通信衛星ネットワークに関連するサイバー脅威活動を把握するために、ODNIレポートを参照すること
- 衛星通信ネットワークへのアクセス、管理、運用に使用される全てのアカウントに対して、多要素認証を含む可能な限り安全な認証方法を採用すること
- 認可ポリシーを確立し、最小権限の原則を適用すること
- ITサービスプロバイダーと適切な信頼関係にあることと、セキュリティに関して適切な契約条項（顧客システムへのアクセスの監視、ネットワーク上で発生したインシデントの通知等）が適用されていることを確認すること
- 衛星通信ネットワークにおける全ての通信に対して独立した暗号化を施すこと
- OS、ソフトウェア及びファームウェアに関するセキュリティを強化すること
- 衛星通信ネットワークにおけるログを監視し、不審なふるまいや不正なログイン試行等を監視すること
- インシデント対応、障害復旧及び運用継続に関する計画を作成、維持及び実行し、サービス中断時に重要な機能を継続運用できるようにすること

衛星通信ネットワークの顧客に対する推奨緩和策

- 衛星通信ネットワークへのアクセス、管理、運用に使用される全てのアカウントに対して、多要素認証を含む可能な限り安全な認証方法を採用すること
- 認可ポリシーを確立し、最小権限の原則を適用すること
- ITサービスプロバイダーと適切な信頼関係にあることと、セキュリティに関して適切な契約条項（必要なセキュリティ管理策の実施、顧客側のネットワークへのアクセスの監視等）が適用されていることを確認すること
- 衛星通信ネットワークにおける全ての通信に対して独立した暗号化を施すこと
- OS、ソフトウェア及びファームウェアに関するセキュリティを強化すること
- 衛星通信ネットワークにおけるログを監視して、不審なふるまいや不正なログイン試行等を監視すること
- インシデント対応、障害復旧及び運用継続に関する計画を作成、維持及び実行し、サービス中断時に重要な機能を継続運用できるようにすること

衛星通信ネットワークのプロバイダーと衛星通信ネットワークの顧客に共通して推奨される緩和策

出所）CISA, Alert (AA22-076A) Strengthening Cybersecurity of SATCOM Network Providers and Customersに基づき三菱総合研究所作成
https://www.cisa.gov/uscert/ncas/alerts/aa22-076a

【米国】国土安全保障に係る宇宙政策を示す文書の発表

- 2022年4月、米国DHSは、**国土安全保障に係る宇宙政策を示す文書である“DHS Space Policy”の更新版を発表**した。
- 同文書では、米国の国土安全保障において宇宙システムが果たす重要な役割と関連省庁間の取り組みにおけるDHSの役割を再定義しており、**DHSは以下の3つの分野で主導的役割を果たす**としている。
  - A) 宇宙システムのサイバーセキュリティの推進
  - B) 国土安全保障に係る機能保証（Mission Assurance）の計画と実行
  - C) 宇宙環境が破壊又は劣化した場合の国土への潜在的影響の対応と緊急時計画の策定
- 「A) 宇宙システムのサイバーセキュリティの推進」に関して、**宇宙システム関係企業に対するセキュリティ原則の採用を奨励**するとともに、**SPD-5に沿ったベストプラクティス、教育教材、標準を開発する旨を明記**している。

国土安全保障に係るDHSの宇宙政策（DHS Space Policy）の概要

A) 宇宙システムのサイバーセキュリティの推進	● DHSは、宇宙システムの設計、開発、取得、配備、運用の全ての段階において**サイバーセキュリティの原則を取り入れるよう企業に対して奨励**し、さらに多様な政府・産業界のパートナーとの密接な関係を維持し、**宇宙政策指令5（SPD-5）に沿ったベストプラクティス、教育材料、標準を開発**する。
B) 国土安全保障に係る機能保証（Mission Assurance）の計画と実行	● DHSは、意図的又は偶然の干渉や有害な操作に対し、NEF(National Essential Functions)やNCF(National Critical Functions)における**安全かつレジリエントな器材や能力の使用を奨励**し、連邦政府機関や民間セクターとの協力を重視する。 ● さらに、能力や機能が低下又は拒否された宇宙環境におけるNCF等の継続性を評価するため、**重要な宇宙システムの損失に対する手順と継続計画(Continuity Plan)を策定**し、**内部演習を実施**するとともに、宇宙システムの損失に対するDHSのレジリエンスを高めるため、**宇宙システムの代替案を検討する継続計画を策定**する。
C)宇宙環境が破壊又は劣化した場合の国土への潜在的影響の対応と緊急時計画の策定	● DHSは、原因の如何を問わず、宇宙環境が悪化した場合の**緊急時対応計画(Contingency Plan)を策定**し、宇宙空間における規範と責任ある国家の行動に関する**省庁間及び国際的な議論に参加**等を行う。

出所）DHS, DHS Space Policy, https://www.dhs.gov/sites/default/files/2022-06/DHS%20Policy%20Statement%20063-01%20Revision%2001%20-%20DHS%20Space%20Policy.pdf
SPACENEWS, Department of Homeland Security publishes space policy, https://spacenews.com/department-of-homeland-security-publishes-space-policy/

【米国】宇宙軍による商用衛星通信サービスの事前セキュリティ評価プログラムの試行

- 2022年5月、米宇宙軍宇宙システムコマンドは、**米国DoDが調達する商用衛星通信サービスのセキュリティ確保のための取組みであるIA-Pre（Infrastructure Asset Pre-Approval）の試行を開始したことを発表**した。2025年9月までにセキュリティ評価をIA-Preに完全に移行することを目指している。
- 従来のDoDの商用衛星通信サービス調達では、同一のサービスであっても、契約ごとにアンケート回答によるセキュリティ評価を実施していたが、IA-Preでは、**NIST SP 800-53に基づくセキュリティ管理策**を用いて、**商用衛星通信サービスごとの対策状況が事前に評価**される。評価を踏まえ、対策状況が承認された場合、**宇宙軍のサービスリストに登録され、以後は契約の都度のセキュリティ評価が不要**となる。

IA-Preの目的、現状及び今後の予定等

目的

- 統合運用の機会が増えた軍事用衛星通信（MilSatCom）と商用衛星通信（ComSatCom）のサイバーセキュリティ水準を同等にするため。
- 「承認済」サービスリストを維持することによって、政府、事業者双方のセキュリティ管理負担を軽減するため。

現状のステータスと今後の予定

- **2022年5月26日、CSCOがIA-Preの立ち上げを発表**。
- 2022年9月より事業者のセキュリティ評価を開始予定。
- 2023年1月に最初のサービスをIA-Preリストへ登録予定。
- 2023年9月まで従来のセキュリティ評価を用いて契約を受け入れ予定。その後、未対応の事業者に対して順次移行プログラムを実施。
- 2025年9月までにIA-Preに完全に移行予定。

IA-Preにおけるセキュリティ評価のフロー

Step 1：ベースラインの設定	AO※1から提供されるチェックリストを元に、NIST SP 800-53における“High Impact”のセキュリティ管理策を参照しつつ、CSCO※2がセキュリティ管理策のベースラインを設定。
Step 2：管理策の選定	CSCOが策定した管理策のベースラインに対してAO及びSCA※3がレビューを実施し、実装すべき管理策を選定。
Step 3：管理策の実装	商用衛星通信サービス事業者において、選定された管理策を実装。
Step 4：実装状況の評価	SCAが認定した第三者が管理策の実装状況を評価し、衛星通信サービス事業者と共同でレポートを作成。実装できない管理策については行動計画とマイルストーンを作成。
Step 5：官によるレビュー	AOとSCAにおいて、作成されたレポートのレビューを実施し、事前承認の合否を判断。

合格後、CSCOが管理するサービスリストへ登録

※1 Authorizing Official：システム運用の承認者
※2 Commercial Satellite Communications Office：宇宙軍における商用衛星通信サービス利用の統括者
※3 Security Controls Assessor：セキュリティ管理策の評価者

出所）SSC, “SSC CSCO reaches critical milestone for IA-Pre, roll-out begins today”等に基づき三菱総合研究所作成
https://www.ssc.spaceforce.mil/Portals/3/Documents/PRESS%20RELEASES/SSC%20PRESS%20RELEASE--IA%20PRE%20ROLLOUT_Final.pdf?ver=ixo3mKLNZMUvHfAbY2HPow%3d%3d
https://www.satellitetoday.com/government-military/2022/06/02/us-space-force-starting-tests-for-cybersecurity-initiative-ia-pre/
https://www.airforcemag.com/space-force-readies-cybersecurity-standards-commercial-satcom-providers/

【独国】BSIによる衛星システムに対するサイバーセキュリティ対策ベースラインの発表（1）

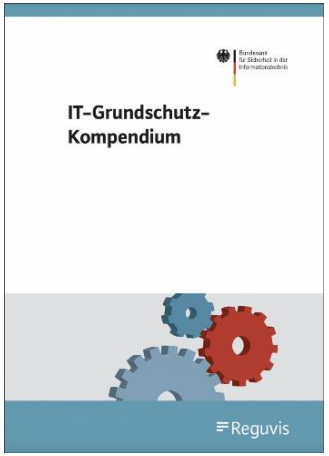
- 2022年6月、ドイツ情報セキュリティ庁（BSI）は、衛星システムに対するサイバー攻撃対策のベースラインを定めた**“IT-Grundschutz-Profil für Weltrauminfrastrukturen (Basic IT Protection Profile for Space Infrastructures)”を発表**した。
- 文書では、一般的な衛星システムのアーキテクチャを定めた上で、典型的な衛星システムのミッションと脅威シナリオに基づくリスク分析を実施し、**衛星システムが実装すべきセキュリティ管理策（推奨事項）**を規定している。
- セキュリティ管理策は、サイバーセキュリティ対策のベースラインを示したBSIの既存フレームワーク“IT-Grundschutz (Basic IT Protection)”を参照している。

IT-Grundschutz-Profil für Weltrauminfrastrukturenの概要

策定の背景	2016年に採択されたドイツの国家サイバーセキュリティ戦略において、BSIに対し、宇宙システムのサイバーセキュリティとして推奨される最小要件を2022年末までに開発することを指示
策定WGへの主な参加組織	● 情報セキュリティ庁（BSI） ● OHB Digital Connect社 ● Airbus Defense and Space社 ● ドイツ航空宇宙センター（DLR）
対象システム	● 一般的な衛星システムのアプリケーション、ITシステム及びインフラ ● 衛星システム単体を対象とし、衛星とのインターフェース部分は含まれるが、地上システム（地上管制センター、打上げシステム等）は含まれない
対象者	● 衛星システム製造・運用のプロジェクトマネージャ及び情報セキュリティ責任者
今後の予定	● セキュリティ機能の実装に向けた技術ガイドラインの策定

IT-Grundschutzとは

- BSIが整備するITシステムのセキュリティ管理策のベースラインを定めたフレームワーク。
- BSIは具体的な管理策を整理した文書である“IT-Grundschutz-Kompendium”を毎年更新・発行している。

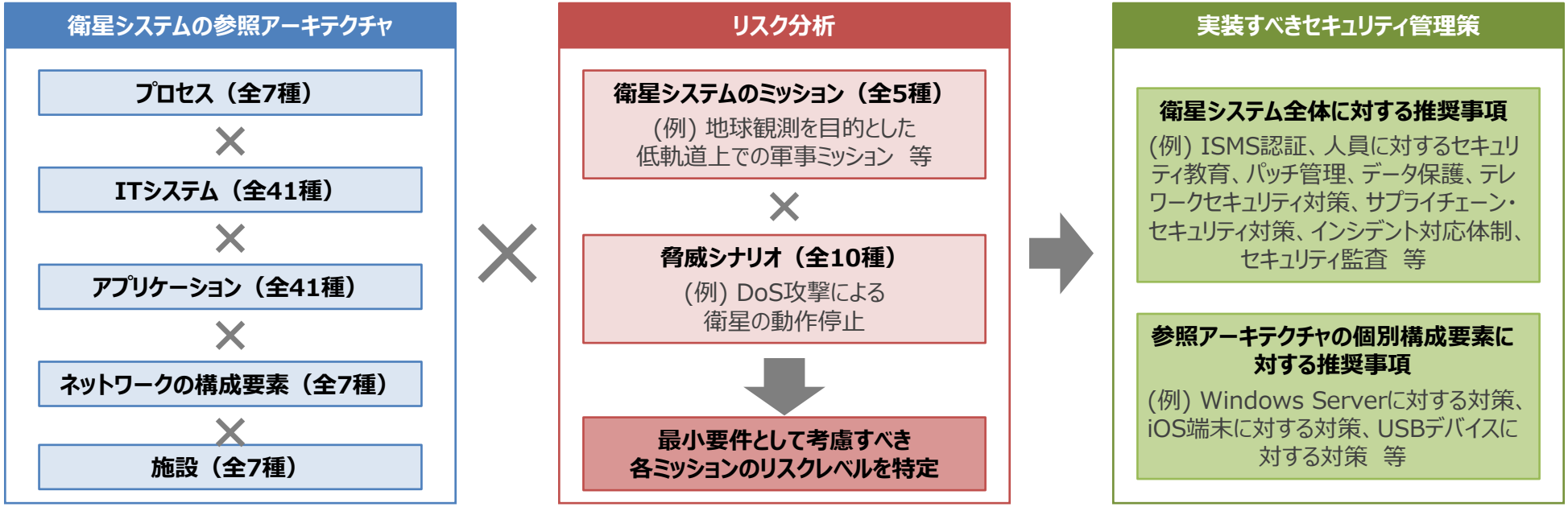


出所）BSI, “IT-Grundschutz-Profil für Weltrauminfrastrukturen”、“IT-Grundschutz-Kompendium”等に基づき三菱総合研究所作成
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.pdf?__blob=publicationFile&v=2
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf?__blob=publicationFile&v=3#download=1

【独国】BSIによる衛星システムに対するサイバーセキュリティ対策ベースラインの発表 (2)

- BSIの文書では、衛星システムの参照アーキテクチャを**「衛星システムのプロセス」、「各プロセスを実施するためのアプリケーション」、「アプリケーションが搭載されるITシステム」、「ネットワークの構成要素」及び「システムが展開される施設」の5つの観点**で整理している。
- この参照アーキテクチャに対して**衛星システムの典型的な5つのミッション**及び**10種の脅威シナリオ**を想定し、**各ミッションにおける脅威のレベルを分析**している。
- リスク分析の結果を元に、**「衛星システム全体に対して実装すべき推奨事項」**及び**「参照アーキテクチャの個別構成要素に対して実装すべき推奨事項」**を示している。
- セキュリティ管理策はあくまで推奨事項であるが、BSIは、**具体的なセキュリティ対策の検討や、複数ステークホルダー間でのセキュリティ対策の合意に当たって本文書を活用することを推奨**している。

IT-Grundschutz-Profil für Weltrauminfrastrukturenにおけるセキュリティ管理策導出の流れ



出所）BSI, “IT-Grundschutz-Profil für Weltrauminfrastrukturenに基づき三菱総合研究所作成
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.pdf?__blob=publicationFile&v=2

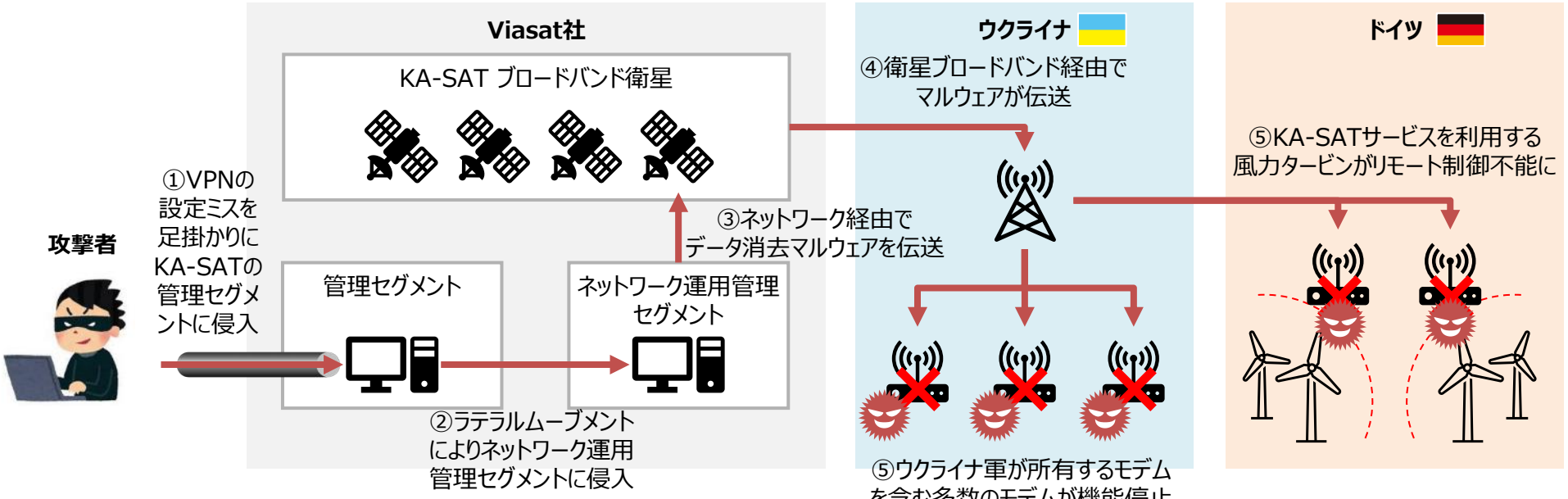
１．宇宙分野における海外のサイバーセキュリティ対策等

２．宇宙分野における近年のセキュリティインシデント事例

【ウクライナ・欧州】衛星通信大手Viasatのブロードバンドサービスに対するサイバー攻撃

- 2022年2月24日、衛星ブロードバンドサービス大手**Viasatの通信衛星「KA-SAT」サービスに利用する数万の通信モデムが標的型DoS攻撃**を受け、当該サービスを利用するウクライナや欧州の組織からの**衛星ブロードバンドへの接続が一時的に不能**となった。
- このサイバー攻撃は**ロシアがウクライナに侵攻を開始する1時間前に発生**したため、**ウクライナ軍の指揮系統に対しても混乱を巻き起こした**とされている。
- また、ドイツでは、当該モデムを使用する複数の風力タービンが攻撃の影響を受け、複数の発電事業者が管理する**7,800基を超える風力タービンのリモート制御が不能**となった。
- 2022年5月10日、**EU、英国、米国、カナダ、エストニア、オーストラリア、ニュージーランド等は**、当該攻撃がロシアによるものであると正式に発表し、**ロシアの行動を強く非難する声明をそれぞれ発表**した。

KA-SATへのサイバー攻撃のイメージ

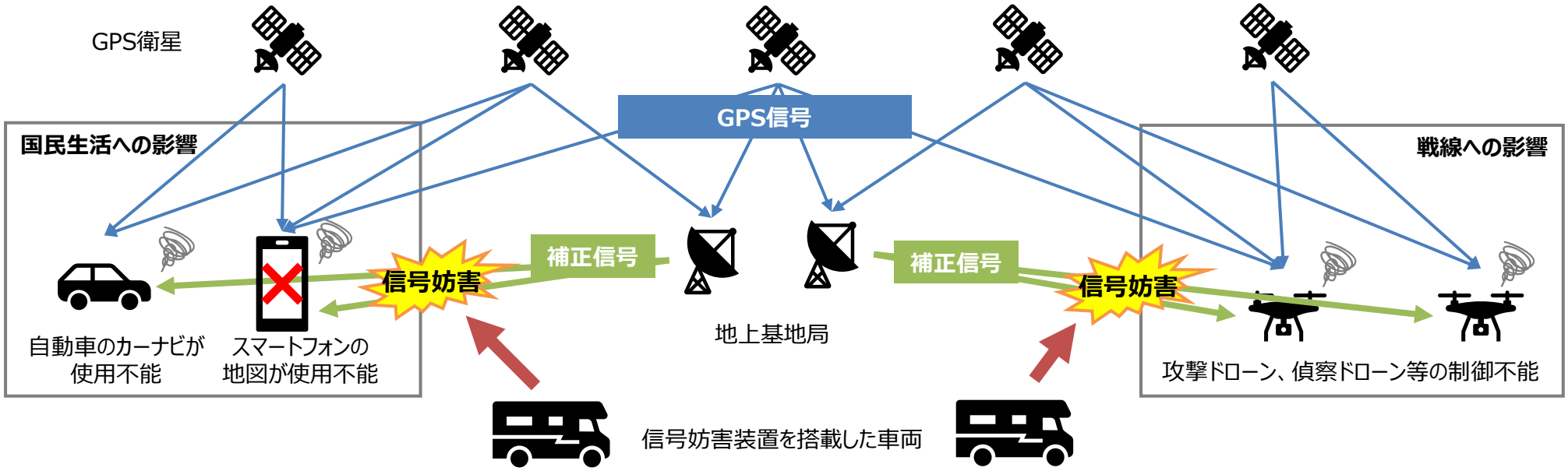


出所）Viasat社等の公開情報に基づき三菱総合研究所作成
https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/
https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000

【ウクライナ】ロシアによるGPSの地上基地局信号の妨害

- 2022年4月12日、米宇宙軍の作戦担当副本部長を務めるデイヴィッド・トンプソン大将は米NBCの番組に出演し、アメリカが提供している**ウクライナのGPS信号がロシアから妨害**を受けている可能性があると述べた。
- ロシアは、大型トラックのような妨害用車両を開発し、**地上基地局側がGPS精度向上のため発信している電波を妨害**しているとみられる。
- 米シンクタンクCSISは、**同様の妨害が2014年前後から断続的に行われている**としている。
- GPSが機能不全に陥った場合、**自動車のカーナビやスマートフォンの地図等が使用不能**となり、国民の生活への影響が出るのみならず、ウクライナ軍が使用している**攻撃ドローンや偵察用の市販ドローンの飛行制御が困難**となり、戦線への影響も懸念される。

ロシアによるGPSへの攻撃とその影響のイメージ

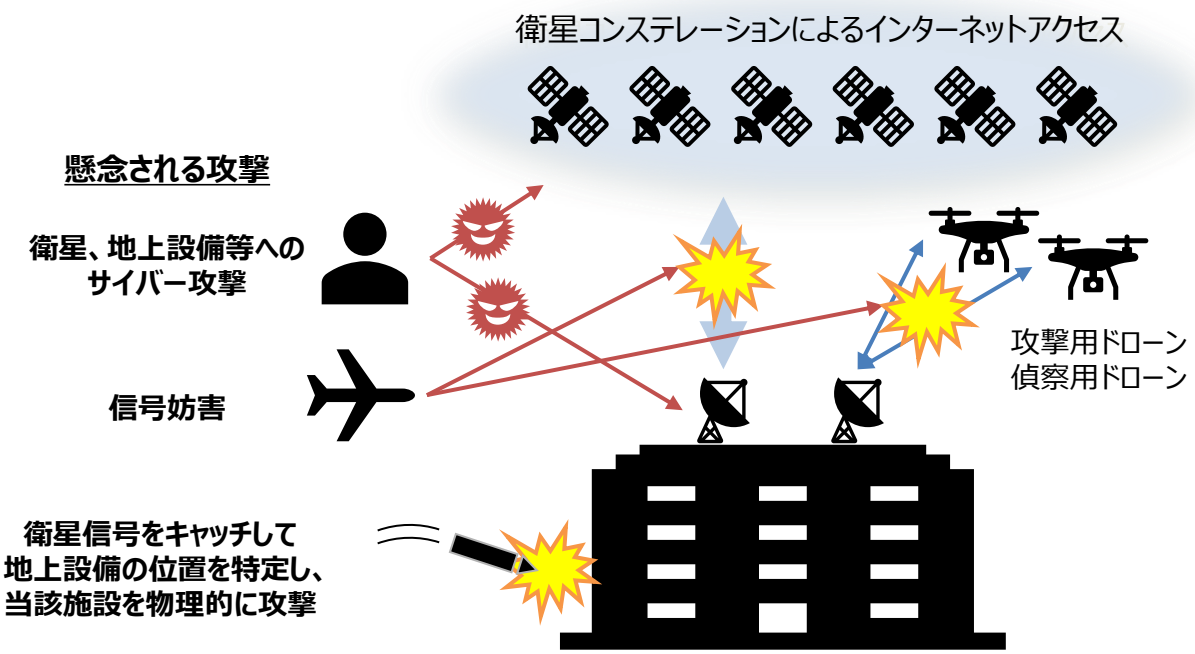


出所）Newsweek記事等に基づき三菱総合研究所作成
https://www.newsweekjapan.jp/stories/world/2022/04/gps-5_1.php

【ウクライナ】SpaceX社の衛星インターネットへの攻撃

- 米SpaceX社は、ロシアのウクライナ侵攻直後より、ウクライナ政府の依頼に応じる形で**衛星コンステレーションを用いたインターネット接続サービスであるStarlinkのサービスをウクライナで提供**している。
- 地上設備の設置により利用できるStarlinkは、侵攻によって**地上ネットワーク回線が断絶した地域においてもインターネット接続を確立**できるほか、**攻撃用ドローンや偵察用ドローンとの通信にも活用**することができる。
- 他方で、衛星信号を探知することにより、 Starlinkの地上設備の位置を特定できるため、**ロシアによる攻撃対象となりうる可能性が指摘**されており、同社のイーロン・マスクCEOも**Starlinkの通信に対する電波妨害やハッキングの試みが増加**していることを明かしている。

Starlinkへの攻撃イメージ



Starlinkのサービス提供と被攻撃に関する状況の経緯

- 2022年2月24日、ロシアによるウクライナ侵攻が開始
- 同年2月26日、ウクライナのミカイロ・フェドロフ副首相兼デジタル担当大臣がSpaceX社のイーロン・マスクCEOにTwitter上でStarlinkの提供を依頼
- 同年2月27日、マスク氏がフェドロフ氏の依頼に応える形でウクライナでのStarlinkサービス開始及び地上設備提供をTwitter上で表明
- 同年3月1日、ウクライナにStarlinkの地上設備が到着し、運用開始
- 同年3月4日、マスク氏がStarlinkの地上設備がロシアの攻撃対象となる可能性が高いことをTwitter上で注意喚起
- 同年3月8日、マスク氏がウクライナのStarlinkが電波妨害を受けているとTwitter上で発言
- 同年3月25日、マスク氏がロシアによるStarlinkへの全てのハッキング及びジャミング行為を防いだとTwitter上で発言
- 同年5月11日、マスク氏がロシアによるStarlinkに対するサイバー攻撃が強まっているとTwitter上で発言

出所）CNN記事等に基づき三菱総合研究所作成
https://edition.cnn.com/2022/03/03/tech/spacex-starlink-ukraine-internet-security-risks-scn/
https://www.reuters.com/world/europe/spacex-chief-musk-warns-that-its-starlink-system-could-be-targeted-ukraine-2022-03-03/
https://www.appbank.net/2022/05/11/technology/2233958.php