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1回）

## 事務局説明資料

令和３年１月

経済産業省 製造産業局 宇宙産業室

# １．近年の宇宙産業の動向

２．近年のサイバー攻撃の動向

３．宇宙分野におけるセキュリティインシデント事例

４．海外における宇宙分野のセキュリティ対策

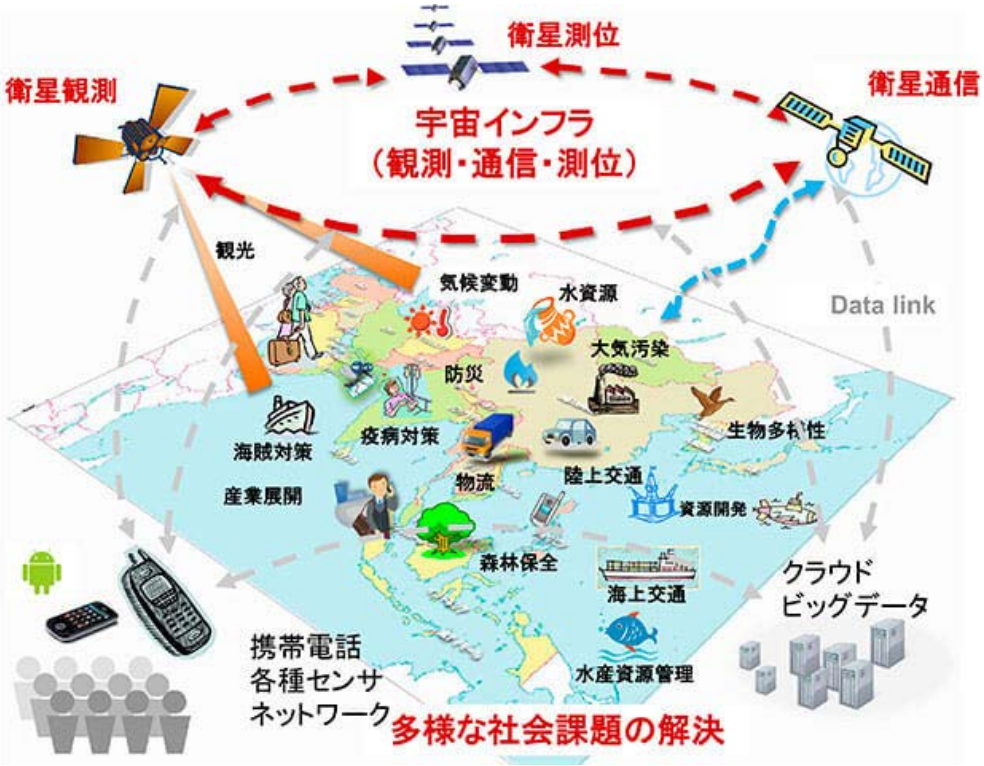
５．検討体制・検討方針

６．ガイドライン開発について

# 社会基盤としての宇宙システム

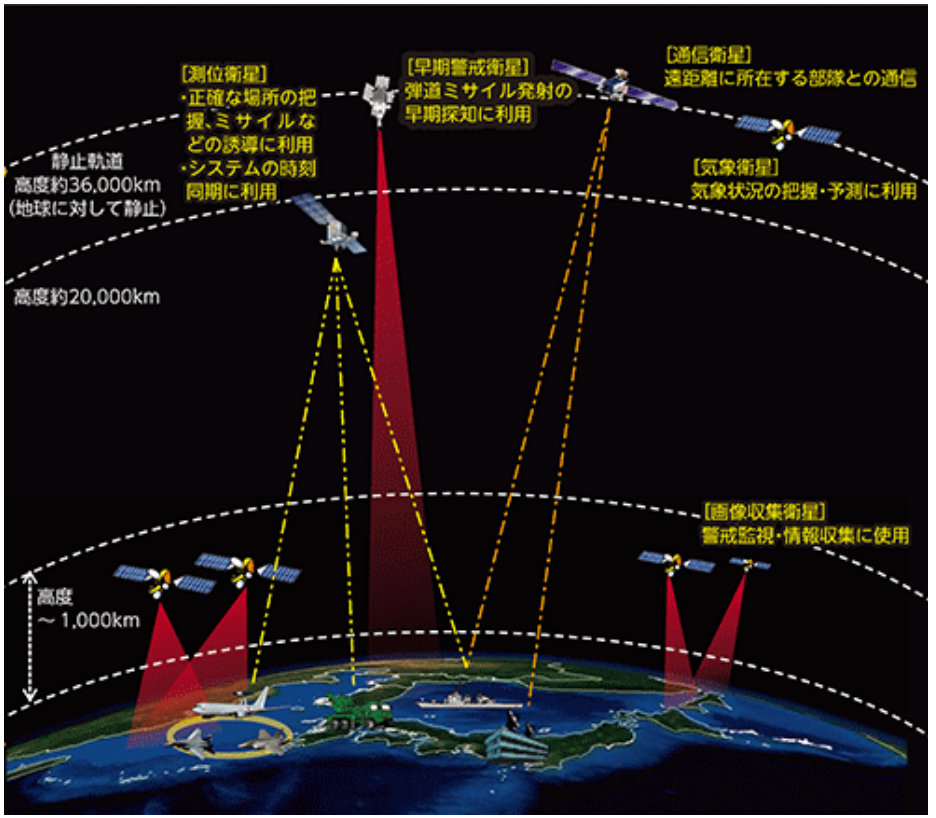
- 観測衛星、測位衛星、通信衛星、地上局、衛星データ利用システム等からなる**宇宙システムは、既に経済社会活動や安全保障分野における基盤**となっている。

## 経済社会活動における宇宙利用のイメージ




出典：慶應義塾大学神武直彦教授資料
https://r-tsushin.com/sdgs/conference_01_space.html

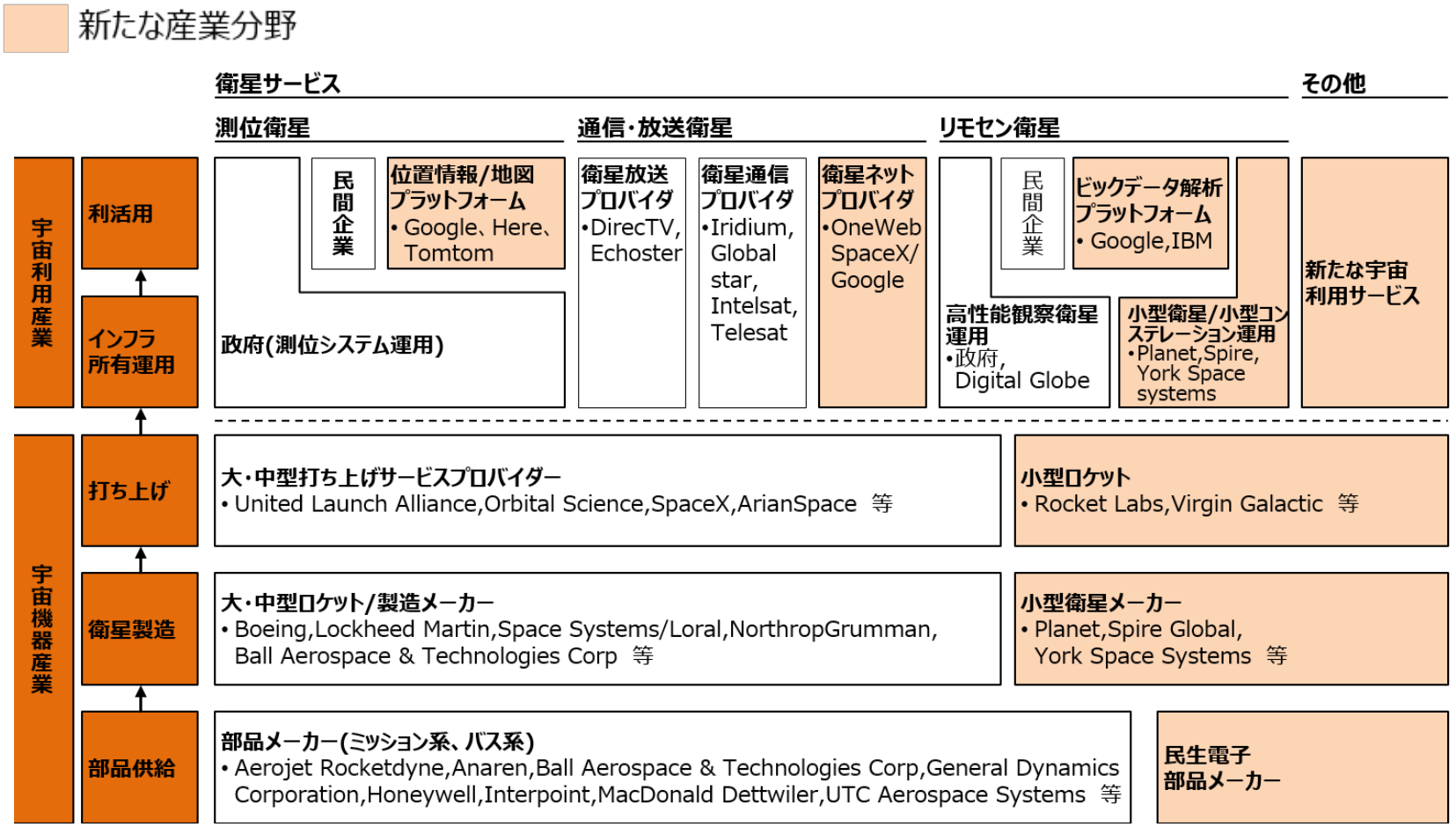
## 安全保障分野における宇宙利用のイメージ




出典：令和２年版防衛白書 図表III-1-3-1

# 宇宙ビジネスはベンチャー企業や巨大IT企業がけん引

- 民間企業による**商業ベースの宇宙ビジネスが活発化。ベンチャー企業が活躍。**
- **巨大IT企業**が小型通信衛星の運用や衛星データのクラウドサービスで**宇宙市場に参入。**




出典：内閣府「我が国の宇宙機器産業の課題、現状及び対応の方向性検討における論点」を基にベイカレント・コンサルティングが作成

# 超小型衛星コンステレーションによる衛星データ量の増大

- 超小型衛星は従来型衛星に比べ、１基当たりの**製造速度（数年→数カ月）及び製造コスト（数百億円→数千万～数億円）に優れ、コンステレーション（星団）化により観測頻度（日単位→分単位）や強靭性も向上。**
- また、AI等の解析技術を活用し、**新たな価値（ビジネス）を創出する企業が出てきている。**

**超小型衛星の例**

出典：アクセルスペース社 HP

**超小型衛星通信網の例**


出典：OneWeb社 HP

**主な超小型衛星打ち上げ計画**

| 企業名 | 種類 | 機数 |
|---|---|---|
| One Web社（米） | 通信 | 最大48,000機 |
| SpaceX社（米） | 通信 | 約12,000機 |
| Planet社（米） | 地球観測 | 100機超 |
| BlackSky Global社（米） | 地球観測 | 60機 |
| アクセルスペース社（日本） | 地球観測 | 50機 |

超小型衛星の登場

↓ 低廉化・多数化

コンステレーション（星団）化

↓ 画像と通信量の増大及び高速化

衛星データの飛躍的な拡大

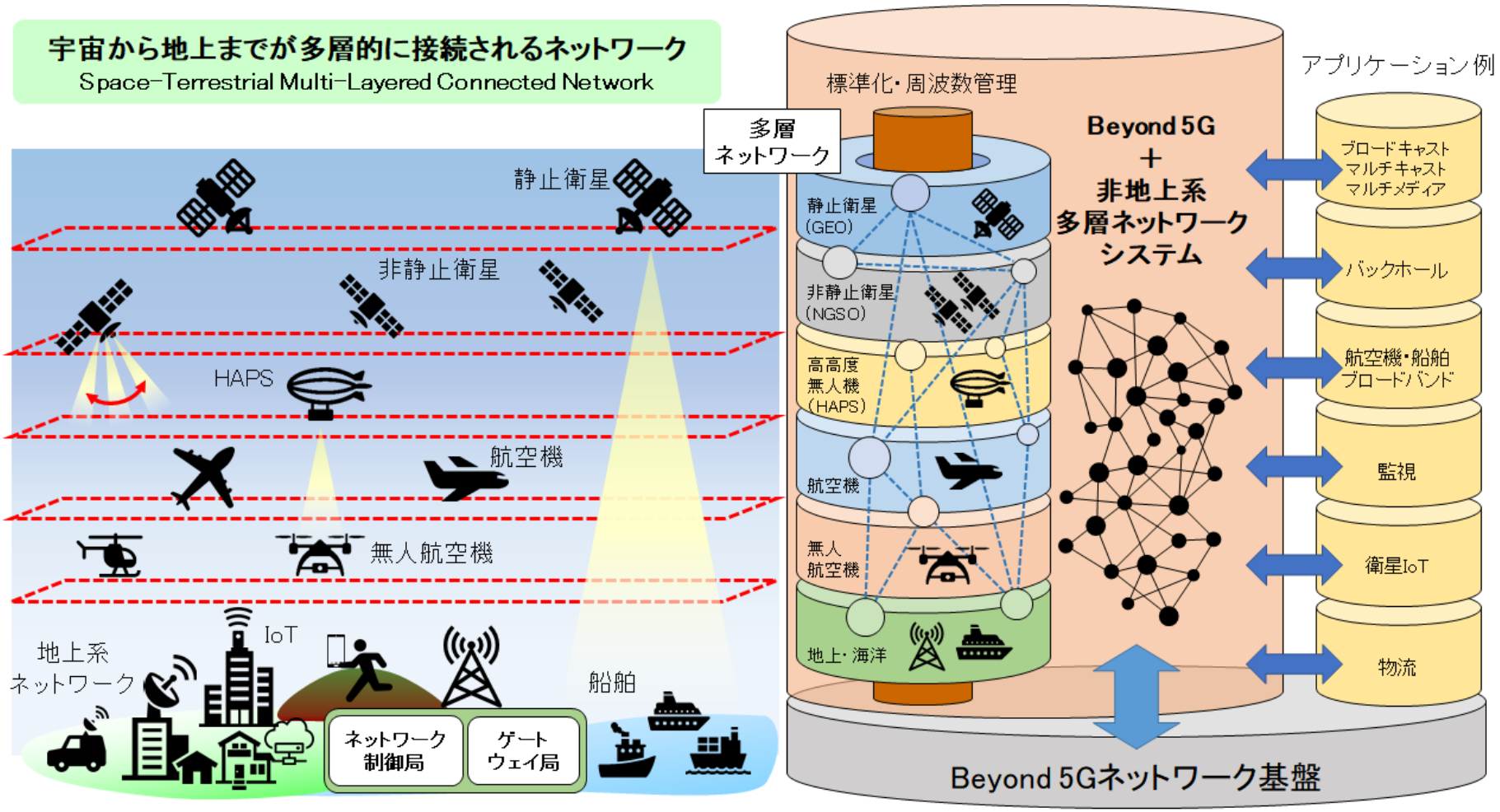
↓ ＡＩの活用

新たな価値創出

# 宇宙システムと5G/Beyond 5G

- 将来的には、宇宙システムは5GやBeyond 5Gにも組み込まれていく方向。

## Beyond 5G における通信ネットワークの概念




出典：国立研究開発法人情報通信研究機構（NICT）衛星通信と5G/Beyond 5Gの連携に関する検討会 報告書（2020年2月）https://www.nict.go.jp/info/topics/2020/02/14-1.html

１．近年の宇宙産業の動向

**２．近年のサイバー攻撃の動向**

３．宇宙分野におけるセキュリティインシデント事例

４．海外における宇宙分野のセキュリティ対策

５．検討体制・検討方針

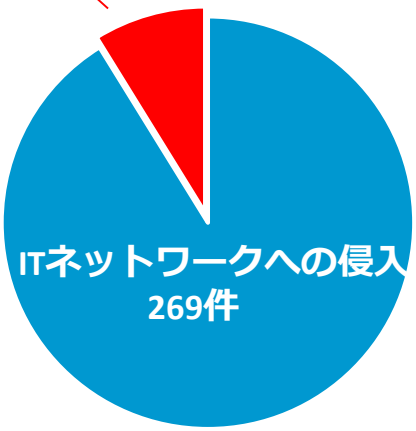
６．ガイドライン開発について

# 制御系システムへのサイバー攻撃の事例

- 米国ICS-CERTの報告では、**重要インフラ事業者等において、制御系にも被害が生じている。**
- ウクライナでは、2015年と2016年にサイバー攻撃による停電が発生。
  **2016年の攻撃(CrashOverRide)**では、**サイバー攻撃のみで、停電が起こされた。**

**米国の重要インフラへの**
**サイバー攻撃の深さ**

**攻撃のうち約一割は、**
**制御系までサイバー攻撃が到達**




（出典）NCCIC/ICS-CERT Year in Review FY2015
Homeland Security より経済産業省作成

**2016年に発生したウクライナの停電に係る攻撃**
**（CrashOverRide(Industryoyer)）**


(出典)https://www.jiji.com/jc/v2?id=20110311earthquake_25photo
(出典)www.chuden.co.jp/hekinan-pr/guide/facilities/thermalpower.html

# ランサムウェアによる生産設備停止の事例

- 2018年8月、半導体受託生産の世界最大手である**台湾積体電路製造（TSMC）において、主力工場内ネットワーク機器がマルウェア感染**。6日午後に復旧するまでの間、**生産が一時停止**。
- 生産停止による**損害額は最大190億円**。

## 本事案の詳細（原因・影響等）

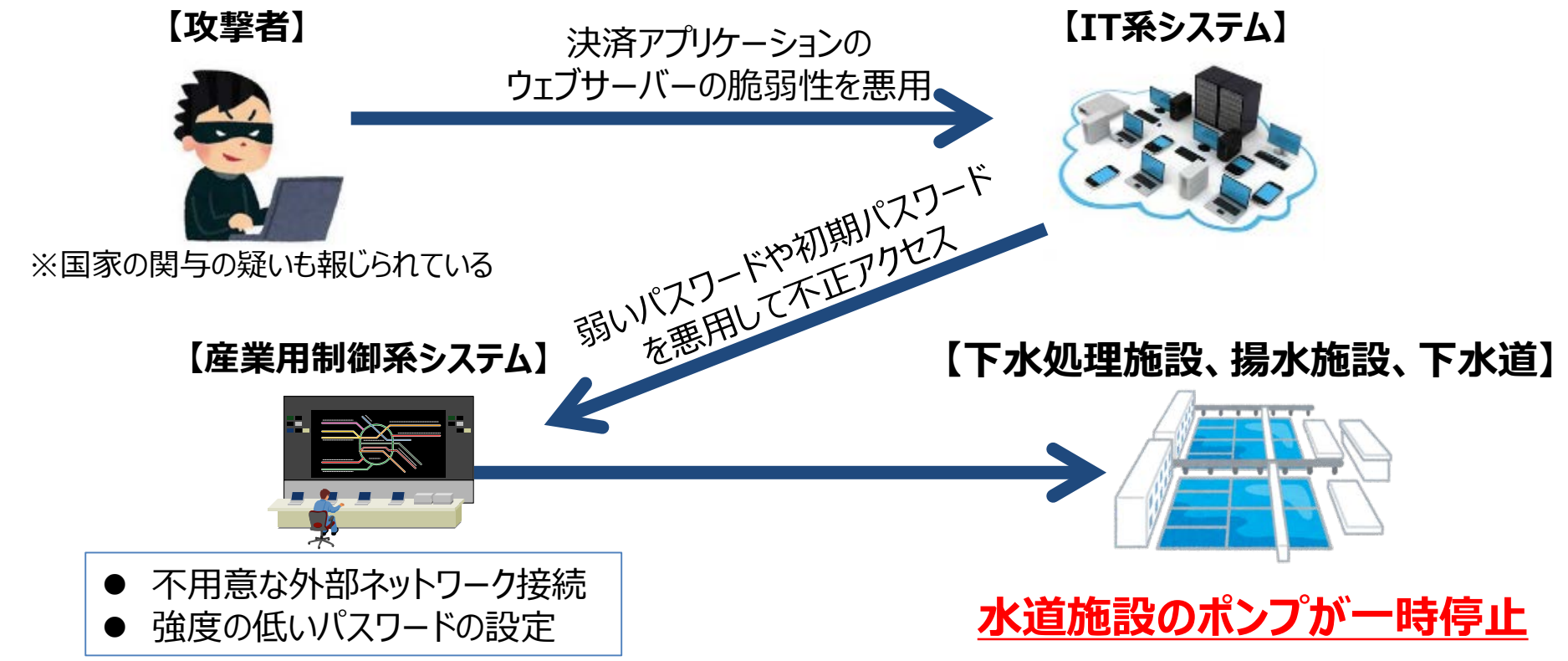
- 感染したマルウェアは、2017年5月に世界中で猛威を振るった「WannaCry」の亜種。金銭要求画面が出ずに機器を停止。
- 感染した新規追加機器を工場内ネットワークに接続したことで、ネットワーク内感染が発生。
- 本来、接続前に閉鎖環境でウィルススキャンする手順であったが、内部の作業ミスにより実施されなかった。
- 加えて、ネットワーク内機器がWindows7端末であったため、ネットワーク内で感染が拡大。

**３日間の生産停止により、損害額１９０億円**

## 感染イメージ

# 水道システムへのサイバー攻撃の事例

- 2020年4月、イスラエル政府は、**廃水処理場、ポンプ場、下水施設の監視制御・データ収集(SCADA)システムを狙った組織的な攻撃**があったとの報告を受けたと発表。
- 同国政府から、事前に制御システムや塩素制御装置のパスワードを変更するよう指示が出ていたが、適切な対策が取られていなかった水道施設のポンプが一時停止。**攻撃の最終目的は、同国の家庭用水道水に入る塩素量の増加**だった、との見方が一部メディアで紹介されている。




（出典）各種公開情報に基づき経済産業省作成

# 航空機システムの脆弱性の事例

- 2018年9月、大手航空機メーカーのサーバにおいて、航空機の**システム構成に関する情報がインターネット上に公開**されていることが発覚。IOActive社(I社)は、特定の脆弱性を用い、機内エンターテイメントシステム等から、**機器の操作に関わるネットワークに到達できることを発見**し、メーカーに報告。メーカーはI社に対して、報告されたのは**悪用可能な脆弱性ではなく、緩和策も実施済と回答するも、詳細は不開示**。
- これに失望したI社は2019年8月の**Black Hatで脆弱性の詳細を公開**。

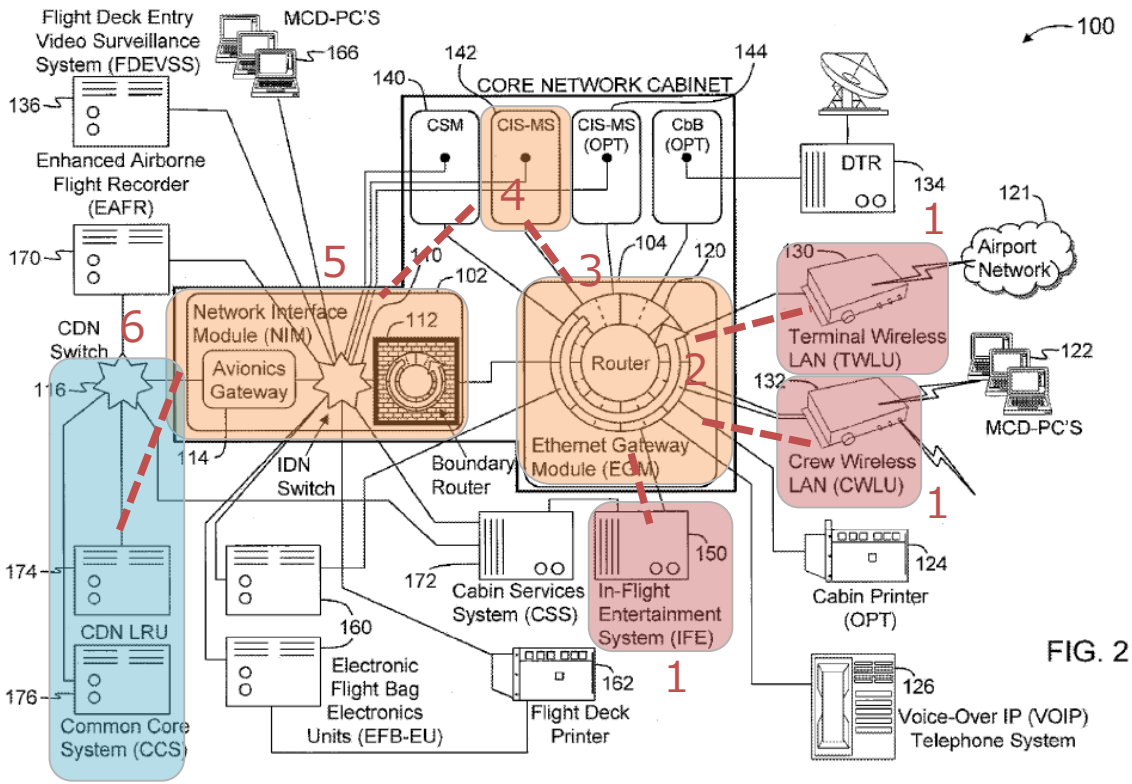



FIG. 2

●基本的な攻撃対象の解説図

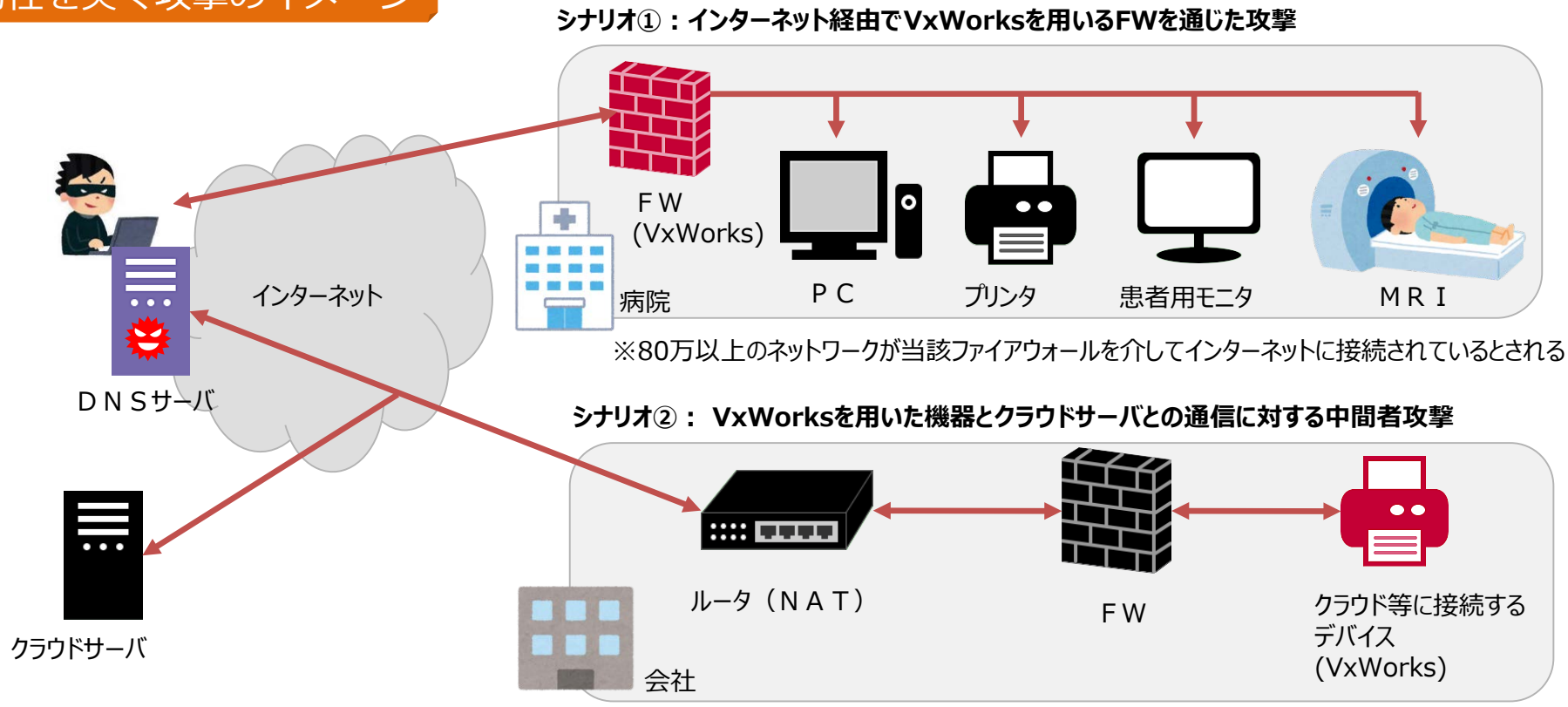
1の機内エンターテイメントシステムや外部ネットワークから、6の機体の操作やナビゲーションに関連するとされるネットワークに到達できると解説されている。

出典：https://ioactive.com/arm-ida-and-cross-check-reversing-the-787s-core-network/
https://www.wired.com/story/boeing-787-code-leak-security-flaws/

# 組み込みOSの脆弱性の事例

- 2019年7月、Armis Labは、**医療、自動車、航空機、防衛など幅広い産業において20億個以上のデバイスで採用されているWindRiver社のVxWorksに11個の脆弱性**があることを発表。
- 本脆弱性はVxWorksが採用するTCP/IPスタックに存在し、これを利用することでファイアウォール等の境界セキュリティを制御したりバイパスすることが可能となり、ネットワーク内外でマルウェアを伝搬させることができるようになるとされる。

## 本脆弱性を突く攻撃のイメージ




出典：https://www.armis.com/urgent11/

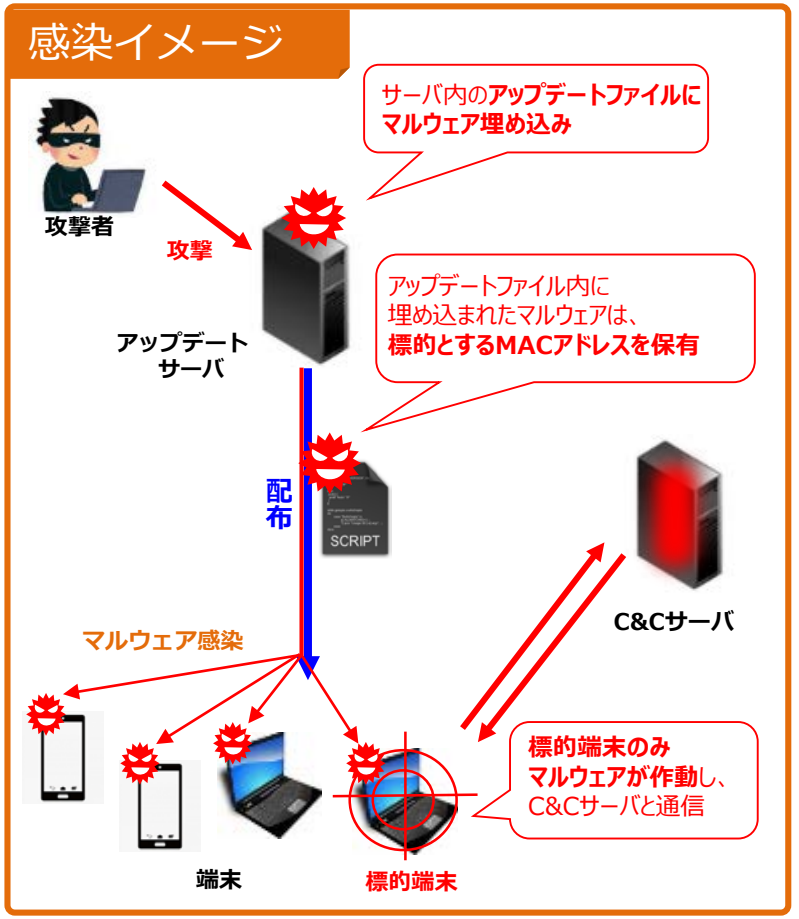
# アップデート機能を悪用したサイバー攻撃の事例

- 台湾のIT機器大手ASUSTeK社において、正規のアップデートサーバが攻撃を受け、当該サーバから**端末向けに配布されたアップデートファイルを介し、数十万の同社端末がマルウェアに感染**する事案が発生。

## 本事案の詳細（原因・影響等）

- 本攻撃は2018年6月から11月にかけて発生。「Shadow Hammer」と呼ばれる。
- 「ASUS Live Update Utility（アップデートサーバ）」によるソフトウェアアップデートを経由し、マルウェア（バックドアファイル）が数十万のASUS端末に感染。
- 本攻撃の大きな特徴として、マルウェアは標的とする端末のMACアドレスをあらかじめ保有しており、感染端末のMACアドレスを参照し、それが標的端末であるかを識別していた。
- 識別の結果、マルウェア感染端末が標的端末であった場合、C&Cサーバと通信を開始する攻撃手法。実際に標的端末が感染。
  - ✓ 標的端末以外ではマルウェアを作動させないことで、事案の発覚を遅らせる狙いがあるとみられる。
  - ✓ 攻撃者はMACアドレスにより、生産ロット等から標的とする特定の出荷先を絞り込んだものと推測される。

## 感染イメージ



# オープン・ソース・ソフトウェア（OSS）への攻撃事例

- OSSである仮想通貨（暗号資産）のウォレットアプリ「Copay」にユーザーの仮想通貨を盗み出すバックドアが仕掛けられて公開されていた。
- 攻撃者はCopay本体ではなく、Copayが利用する外部ライブラリの一つ（event-stream）を正規の権限で編集し、**悪意のあるコードが仕込まれた外部ライブラリ（flatmap-stream）に関連させることでバックドアを仕掛けた**。
- 悪意あるコードを追加する工程を複雑にし、かつ隠蔽を行うことで発覚を遅らせようとした。

2017.10 ・開発者によるevent-streamの最終更新

⋮

2018.8末 ・攻撃者がevent-streamの開発者に**「メンテナンスを引き継ぎたい」と持ちかけメンテナンス権限を取得**

2018.9.9 ・攻撃者がevent-streamを更新 → event-streamがflatmap-streamと関連

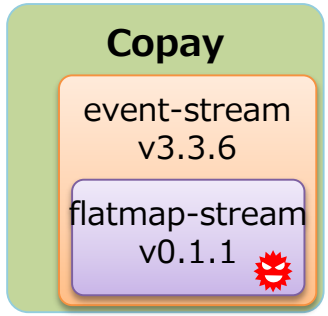
2018.10.5 ・攻撃者がflatmap-streamに**悪意のあるコードを追加**

2018.10.26 ・Copayが更新

**→ Copayが悪意のあるコードが仕込まれたflatmap-stream に関連するようになり、攻撃者がバックドアを利用できるように**

⋮

2018.11.26 ・ニュースになり、flatmap-streamは削除された



# クラウドサービスに対するサイバー攻撃の事例

- **クラウドサービスへのサイバー攻撃事案は絶えず発生**している状況。利用者側の設定不備を突く攻撃が多い。

## クラウドサービスにおける主なサイバー攻撃事例

- 米国配車サービス大手のウーバー・テクノロジーズにおいて、2017年11月、顧客とドライバー合わせて5,700万人の個人情報が流出したことが判明。原因はAWSへの不正アクセス。
- A社のインド子会社において、2018年5月、5万人以上の顧客情報が流出したことを発表。原因はAWSの公開設定ミス。

## 利用者の多いクラウドサービスにおけるサイバー攻撃の特徴

**「Office365」への不正アクセス**

- 攻撃者は、2要素認証が導入されていなかったり、単純なパスワードが設定されているようなアカウントを標的としている。
- 特にシステムアカウントについては、事業者内で共有する必要があることから単純なパスワードが設定されがちであり、使用頻度の低いものが放置されていることも多いため攻撃に気づきにくいという傾向がある。

**Amazon Web Service（AWS）のクラウドストレージ「Amazon S3」への不正アクセス**

- ディレクトリの設定を「公開状態」にしていたり、パスワードが設定されていないといった、利用者側のAWS設定ミスが多くの原因。

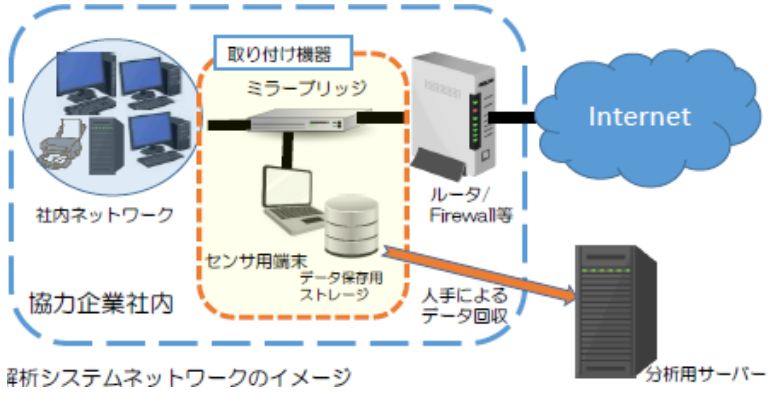
# 中小企業に対するサイバー攻撃の実態

- 地域の中小企業も、例外なくサイバー攻撃の脅威にさらされていることが明らかになってきている。

## 中小企業被害実態に関する調査

**■調査内容**

実証期間：平成30年9月～平成31年1月
実証内容：中小企業30社を対象に、ネットワーク上の通信データ等を一定期間収集。



解析システムネットワークのイメージ

**■ 調査結果**

- 調査した**30社全てでサイバー攻撃**を受けていたことを示す不審な通信が記録されていた。
- 少なくとも5社ではコンピューターウイルスに感染するなどして、**情報が外部に流出したおそれ**があることが分かった。

出典：大阪商工会議所「平成30年度中小企業に対するサイバー攻撃実情調査（報告）」共同研究実施者：神戸大学、東京海上日動火災保険（株）（2019年7月）

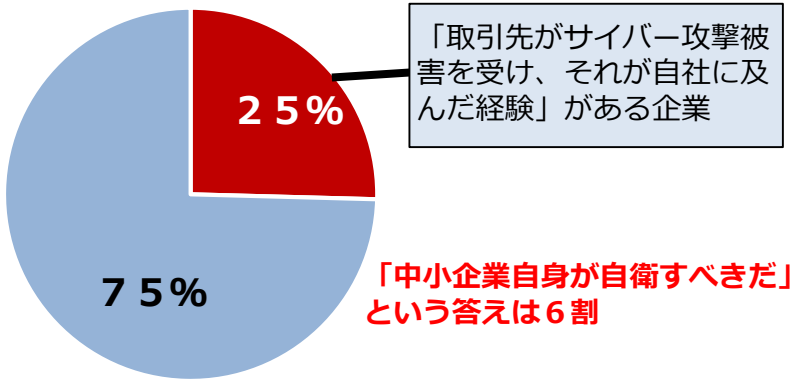
## 取引先経由の被害に関する調査

**■調査内容**

調査期間：平成31年2月～3月
調査内容：全国の従業員100人以上の企業を対象に、郵送、FAX、メール、Web、対面による依頼・回答

**■調査結果**

- 大企業・中堅企業118社に調査したところ、取引先がサイバー攻撃被害を受け、**影響が自社に及んだ経験**がある企業が30社あった（**25%**）




出典：大阪商工会議所「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査」（2019年5月）

# COVID-19に乗じたサイバー攻撃の事例

- 海外において、新型コロナウイルス対策を行っている医療関連機関に対するサイバー攻撃が確認されており、混乱に乗じたフィッシングメールや偽アプリ、フェイクニュースなども増加。

**WHO**へのサイバー攻撃が倍増

- WHOへのサイバー攻撃が倍増。攻撃の一つは、**DarkHotelと呼ばれるAPT攻撃**。

**スペイン**の病院で初のサイバー被害

- 3月上旬、スペインの病院が**ランサムウェア「NetWalker」**の攻撃を受けITインフラの一部が使用不能に。スペイン病院初のサイバー被害事例。

**英**ワクチン試験施設に攻撃

- 3月14日、COVID-19向けワクチンの試験施設が**ランサムウェア「Maze」**の攻撃を受け、個人情報窃取・同公開の被害。

**フランス**の医療機関に対するDDoS攻撃

- 3月22日、パリ周辺の大学病院等を統括するパリ公立病院連合（AP-HP)に**DDoS攻撃**。
- 攻撃は1時間続き、この間、外部との接続が遮断。

**チェコ**の大学病院にサイバー攻撃

- 3月12-13日、チェコ内でコロナ対応を担っていたBrno大学の病院がサイバー攻撃を受け、全コンピュータ停止。
- 急患を受け入れられなくなり、近隣病院に患者が送られた。

**米イリノイ州**郡公衆衛生局HPがダウン

- 3月10日、イリノイ州Champaign-Urbana地区の公衆衛生局のHPが**ランサムウェア攻撃**を受けダウン。

**米保健福祉省**（HHS）にDDoS攻撃

- 3月15日、米保健福祉省に**DDoS攻撃**。
- 同省当局者は外国勢力が関与したとの見方を示している。

感染状況をトラッキングする**偽アプリ**

- ダウンロードするとスマートフォンがロックされ、「**ロック解除したければビットコインで100ドル払え**」とのメッセージが表示。

米JH大学を装った**悪性ウェブサイト**

- 新型コロナウイルスの感染状況をリアルタイムで確認できるジョンズ・ホプキンス大学HPを装った悪性ウェブサイトが多数出現。HPを閲覧しようとリンクをクリックするとマルウェアに感染し、個人情報が窃取される。

**TV会議の招待を装う**偽メッセージ

- 招待メールに見せかけたメール中のボタンを押すと、攻撃者Webサイトに誘導
- 「会議はすでに始まっています」「あなたの参加を待機しています」など、焦らせるような文章が記載。

米NSCが**フェイクメッセージ**を否定

- 米軍所属の友人からの情報として「数日中にトランプ大統領が2週間の国家封鎖を実施する」とのテキストメッセージが急拡散。米NSCがツイッターでフェイクであると否定。

＜各種報道等に基づいて作成＞

１．近年の宇宙産業の動向

２．近年のサイバー攻撃の動向

**３．宇宙分野におけるセキュリティインシデント事例**

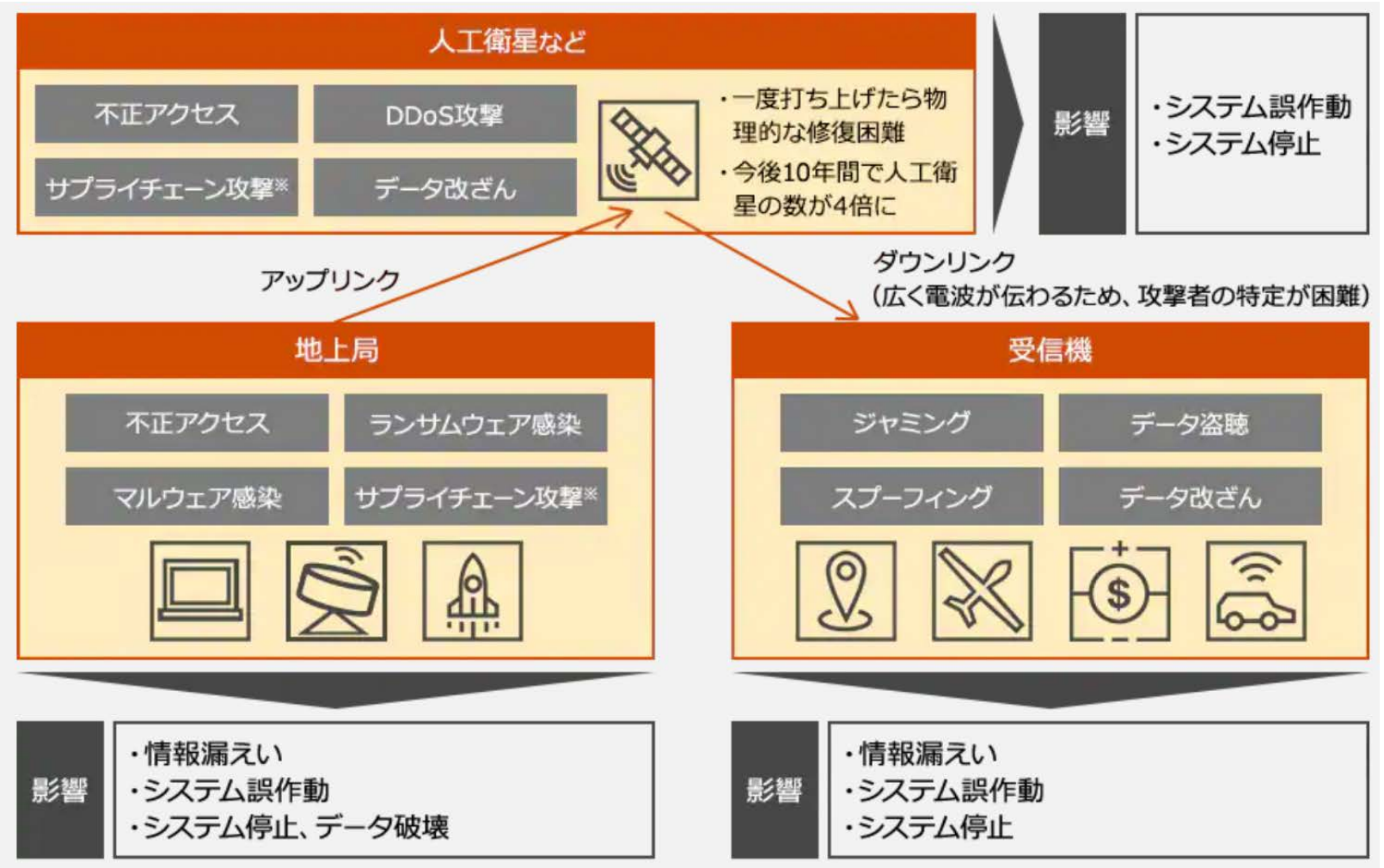
４．海外における宇宙分野のセキュリティ対策

５．検討体制・検討方針

６．ガイドライン開発について

# 宇宙システムにおけるサイバー攻撃の対象と影響の広がり

- 宇宙システムは、技術情報のオープン化、民生品の活用、オープン・ソース・ソフトウェア（OSS）の活用、地上局のクラウド化などにより、**サイバー攻撃の対象やその影響の範囲が広がっている。**




出典：PwC社 HP
https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting/space-cybersecurity-service.html

# 宇宙分野におけるセキュリティインシデントの概況①

- **宇宙分野では1986-2020年に国内外で90件以上のセキュリティインシデントが発生。**
- 詳細は次項以降。

**【MBSD調べ】**

**カテゴリー別のインシデント数推移**

| カテゴリー | サブカテゴリー | 発生年 | | | | | | 合計 |
|---|---|---|---|---|---|---|---|---|
| | | 1986-2000 | 2001-2005 | 2006-2010 | 2011-2015 | 2016-2020 | NA[*1)] | |
| セグメント | データ通信 | 4 | 7 | 10 | 12 | 9 | 2 | 44 |
| | 地上セグメント | 4 | 4 | 9 | 14 | 7 | 1 | 39 |
| | 宇宙セグメント | 2 | 0 | 6 | 1 | 3 | 0 | 12 |
| | 不明 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| セクター | 政府系 | 5 | 5 | 15 | 13 | 6 | 0 | 44 |
| | 商用 | 4 | 3 | 5 | 11 | 7 | 0 | 30 |
| | 軍事 | 2 | 2 | 5 | 0 | 3 | 0 | 12 |
| | 民間 | 0 | 3 | 2 | 2 | 4 | 0 | 11 |
| | NA[*2)] | 0 | 0 | 0 | 0 | 1 | 3 | 4 |
| テクニック | CNE[*3)] | 3 | 4 | 8 | 13 | 7 | 1 | 36 |
| | ジャミング[*4)] | 3 | 4 | 4 | 8 | 2 | 2 | 23 |
| | 乗っ取り[*5)] | 2 | 2 | 4 | 1 | 2 | 0 | 11 |
| | スプーフィング[*6)] | 0 | 0 | 0 | 2 | 4 | 1 | 7 |
| | 盗聴 | 0 | 1 | 3 | 1 | 1 | 0 | 6 |
| | 事故 | 1 | 0 | 2 | 0 | 1 | 0 | 4 |
| | サービス停止 | 1 | 0 | 2 | 1 | 0 | 0 | 4 |
| | ASAT | 0 | 0 | 2 | 0 | 1 | 0 | 3 |
| | コントロール | 1 | 0 | 2 | 0 | 0 | 0 | 3 |
| | ミーコニング[*7)] | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| | 盗難・紛失 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| インシデント数 | | 10 | 11 | 23 | 26 | 19 | 3 | 92 |

複合的インシデントを複数分類で重複カウントしたため、縦計はインシデント数と一致しない

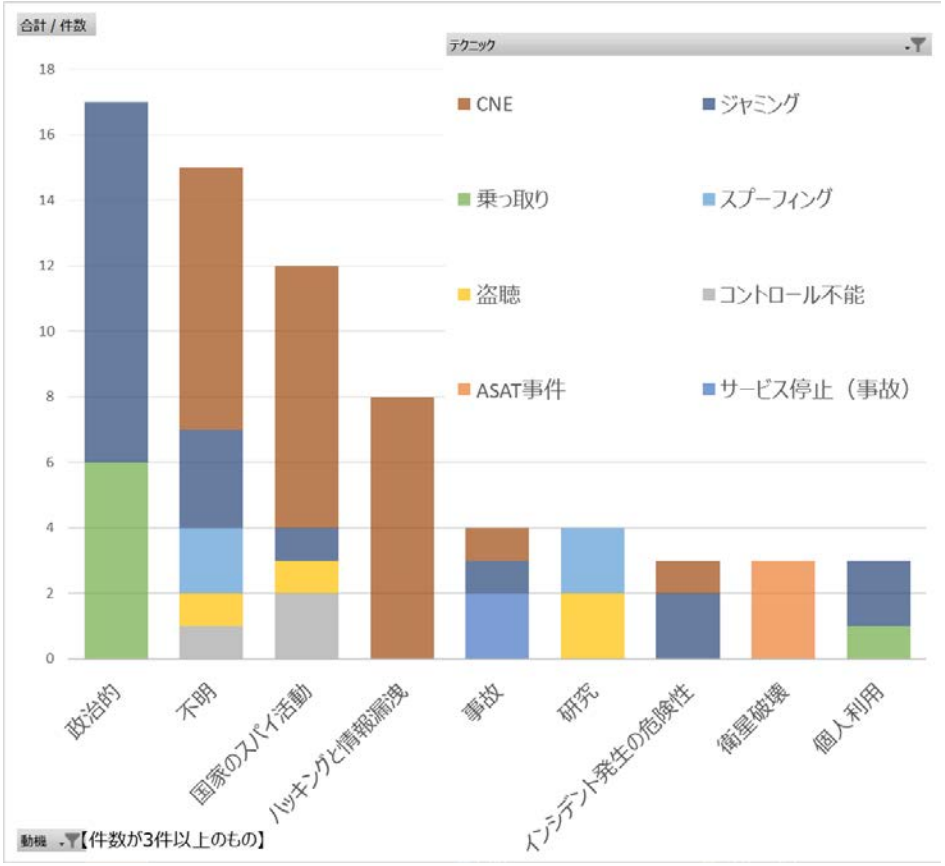
[*1)] 実インシデントは未発生であるが、インシデント発生の危険性が指摘(年度不明)されたもの

[*2)] 実インシデントは未発生であるが、インシデント発生の危険性が指摘されたもの

[*3)]Computer Network Exploitation, 諜報活動 [*4)]通信妨害

[*5)]CNE活動の延長で諜報活動に含まれる場合もあるが、電波ジャック（放送波の不正使用）や衛星ジャック（衛星の制御を不能にする）などを含む

[*6)]なりすまし[*7)]誤差混入させ再送信




【MBSD作成】

出典：

- Manulis M; Cyber Security In New Space,2020/5
- https://gigazine.net/news/20131112-iss-infected-malware-by-russian-usb/ Accessed 2020/11/25
- William J Malik; Attack Vectors in Orbit: The Need for IoT and Satellite Security; https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/13692/MBS-W03-Attack-Vectors-in-Orbit-The-Need-for-IoT-and-Satellite-Security.pdf
- PwC社 HP;https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting/space-cybersecurity-service.html
- NHKオンライン; 2020年8月6日 衛星通じたネット通信 “漏えいの危険性” 英の研究者が指摘 https://www3.nhk.or.jp/news/html/20200806/k10012554731000.html
- 内閣府宇宙開発戦略推進事務局;『宇宙システムの機能保証強化に関する調査』,2019/3
- IPA;制御システムのセキュリティリスク分析ガイド第二版,2020/3
- Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, Tyler Way, Makena Young; Space Threat Assessment 2020

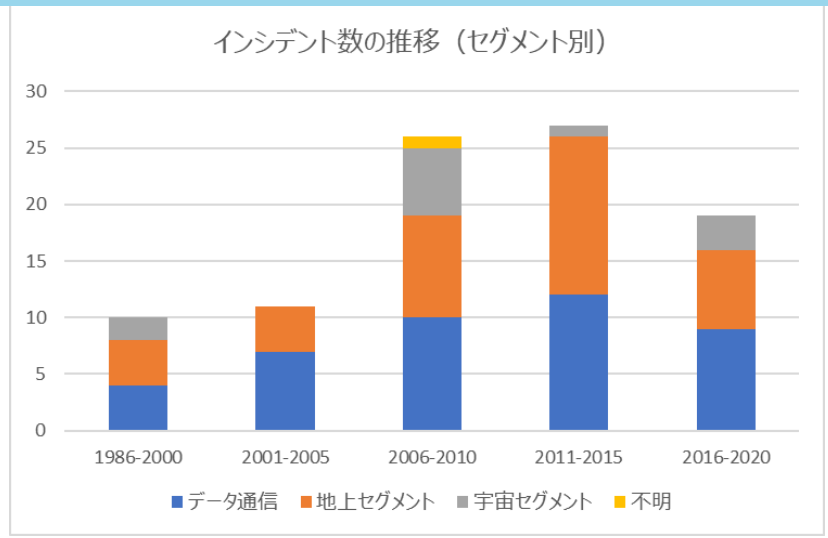
# 宇宙分野におけるセキュリティインシデントの概況②

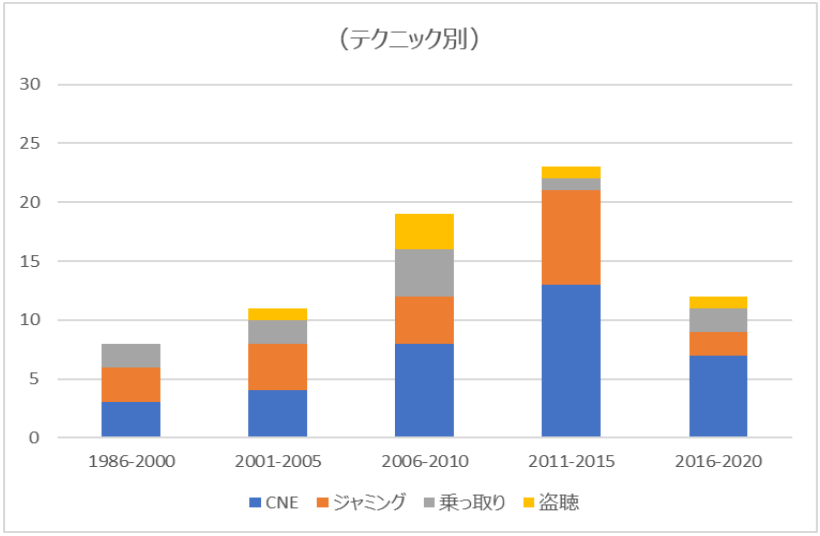
- セグメント別では、データ通信及び地上セグメントでのインシデントが多い。
- テクニック別では、諜報活動（Computer Network Exploitation：CNE）及びジャミングが多い。
- セクター別では、政府系および商用におけるインシデントが多い。

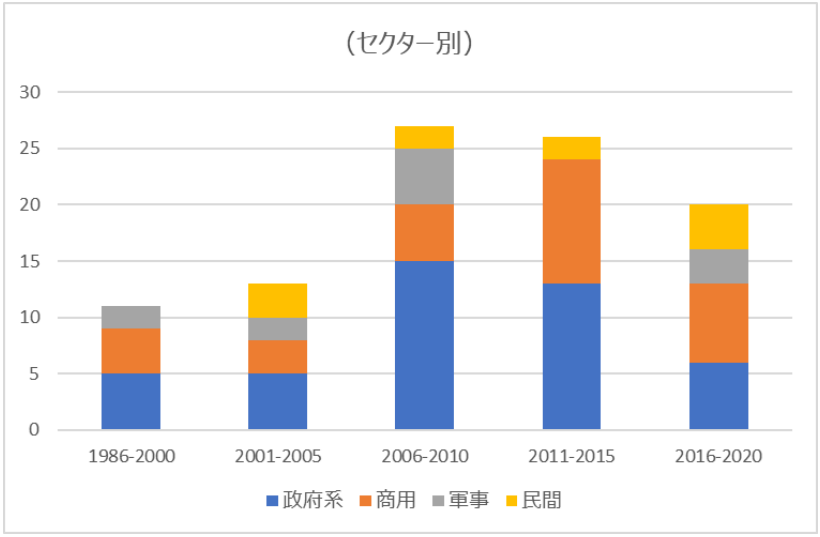
【MBSD調べ】

| カテゴリー | サブカテゴリー | 発生年 | | | | | | 合計 |
|---|---|---|---|---|---|---|---|---|
| | | 1986-2000 | 2001-2005 | 2006-2010 | 2011-2015 | 2016-2020 | NA[*1)] | |
| セグメント | データ通信 | 4 | 7 | 10 | 12 | 9 | 2 | 44 |
| | 地上セグメント | 4 | 4 | 9 | 14 | 7 | 1 | [illegible] |
| | 宇宙セグメント | 2 | 0 | 6 | 1 | 3 | 0 | |
| | 不明 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| セクター | 政府系 | 5 | 5 | 15 | 13 | 6 | 0 | 44 |
| | 商用 | 4 | 3 | 5 | 11 | 7 | 0 | 30 |
| | 軍事 | 2 | 2 | 5 | 0 | 3 | 0 | 12 |
| | 民間 | 0 | 3 | 2 | 2 | 4 | 0 | [illegible] |
| | NA | 0 | 0 | 0 | 0 | 1 | 3 | |
| テクニック | CNE | 3 | 4 | 8 | 13 | 7 | 1 | [illegible] |
| | ジャミング | 3 | 4 | 4 | 8 | 2 | 2 | 23 |
| | 乗っ取り | 2 | 2 | 4 | 1 | 2 | 0 | 11 |
| | スプーフィング | 0 | 0 | 0 | 2 | 4 | 1 | 7 |
| | 盗聴 | 0 | 1 | 3 | 1 | 1 | 0 | 6 |
| | 事故 | 1 | 0 | 2 | 0 | 1 | 0 | 4 |
| | サービス停止 | 1 | 0 | 2 | 1 | 0 | 0 | 4 |
| | ASAT | 0 | 0 | 2 | 0 | 1 | 0 | 3 |
| | コントロール | 1 | 0 | 2 | 0 | 0 | 0 | 3 |
| | ミーコニング | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| | 盗難・紛失 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| インシデント数 | | 10 | 11 | 23 | 26 | 19 | 3 | 92 |

前頁の表



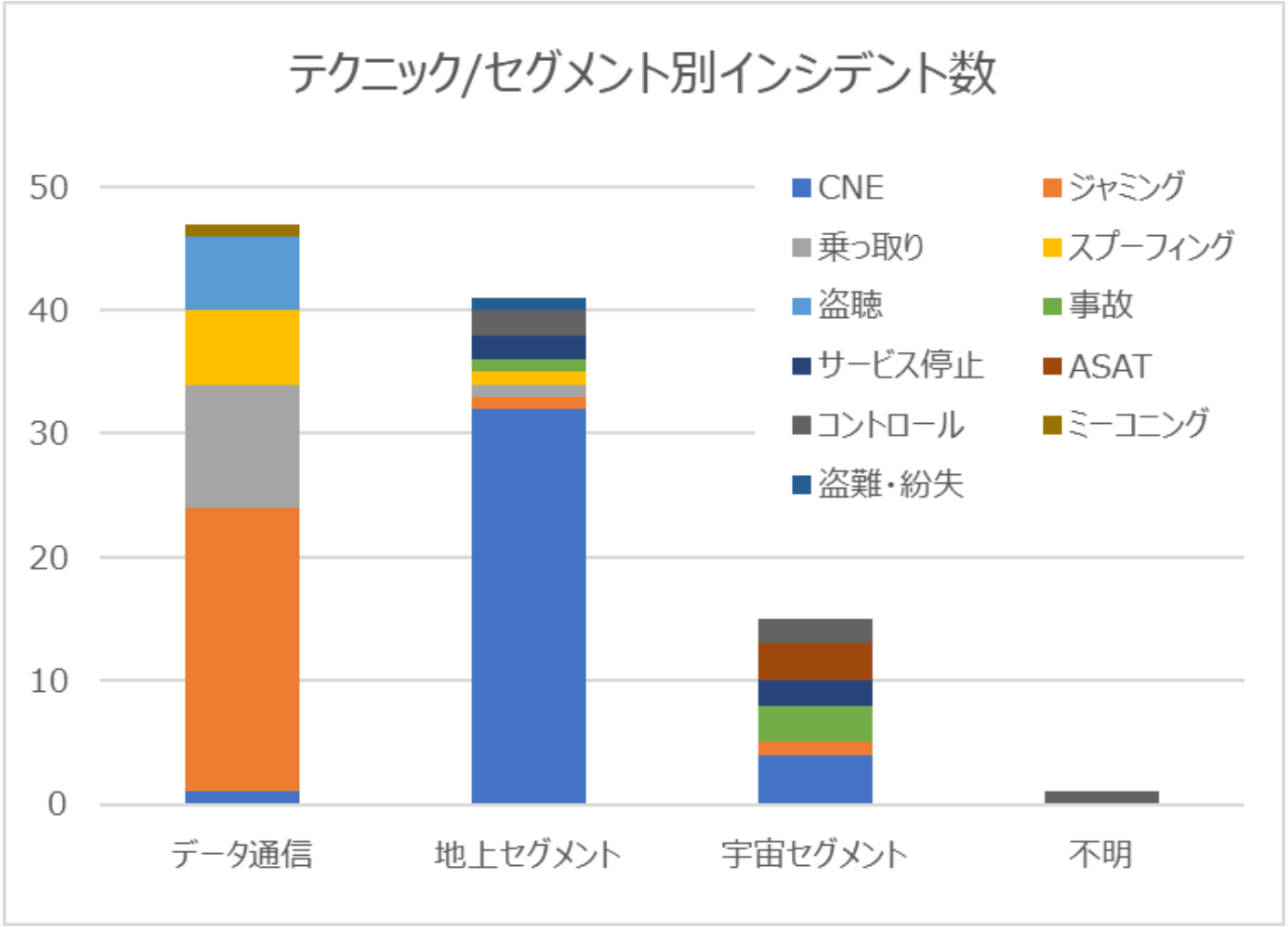



# 宇宙分野におけるセキュリティインシデントの概況③

- データ通信セグメントでは、ジャミング（通信妨害）や乗っ取りが多い。
- 地上セグメント及び宇宙セグメントでは、諜報活動（CNE）が多い。

【MBSD調べ】



１．近年の宇宙産業の動向

２．近年のサイバー攻撃の動向

３．宇宙分野におけるセキュリティインシデント事例

**４．海外における宇宙分野のセキュリティ対策**

５．検討体制・検討方針

６．ガイドライン開発について

# 米国における宇宙システムのセキュリティに係る施策等の概要

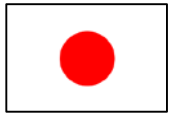
- 2007年、国家安全保障システム委員会（CNSS）が、「安全保障任務に用いられる宇宙システムのための国家情報保証方針（CNSSP 12）」を発行。
- **この２～３年は、商用衛星に係る民を中心とする取組が進展。**

凡例　●官、●民、●官民

| | | |
|---|---|---|
| 1990.7 | ● | • NSD-42（国家安全保障電気通信及び情報システムのセキュリティに係る国家方針）を発行。<br>• NSD-42に基づき、国家安全保障電気通信及び情報システムセキュリティ委員会（NSTISSC）を設立。 |
| 2001.10 | ● | • 大統領令13231**“情報時代における重要インフラの保護”**において、NSTISSCを**国家安全保障システム委員会（CNSS）**に再指定。CNSSは国防総省（DoD）、中央情報局（CIA）、国防情報局（DIA）、司法省（DOJ）、連邦捜査局（FBI）、国家安全保障局（NSA）、国家安全保障会議（NSA）等から構成される。 |
| 2005.6 | ● | • 国防総省が**DoDI 8581.01 “国防総省が使用する宇宙システムにおける情報保証方針”**を発行。（2010.6改訂） |
| 2007.3 | ● | • NSD-42を受け、CNSSが**CNSSP 12 ”安全保障任務に用いられる宇宙システムのための国家情報保証方針“**を発行。（2012.1改訂、2018.2改訂） |
| 2009.2 | ● | • NSD-42を受け、CNSSが**CNSSP 22 “国家安全保障システムのための情報保証リスク管理”**を発行。（2012.1.改訂、2016.8.サイバーセキュリティリスク管理方針に改訂） |
| 2012.3 | ● | • NSD-42を受け、CNSSが**CNSSD 505 ”サプライチェーンリスク管理”**を発行。（2017.7.26改訂） |
| 2017.1 | ● | • エアロスペースコーポレーションが“NAVIGATING THE POLICY COMPLIANCE ROADMAP FOR SMALL SATELLITE”で**衛星オーナーのDoDI 8581.01及びCNSSP 12への対応ついて解説。** |
| 2018.8 | ● | • 米国航空宇宙学会（AIAA）小型衛星カンファレンスで“No Encryption, No Fly”のルールが提案される。 |
| 2019.4 | ● | • **宇宙情報共有分析センター**（Space ISAC）の設立。（NASA、米国宇宙軍、国家偵察局が立ち上げ。） |
| 2019.4 | ● | • **Orbital Security Alliance (OSA)**が**“Big Risk in Small Satellites”**を発表。 |
| 2020.2 | ● | • 大統領令13905 ”測位・航法・時刻 サービスの責任ある使用による国家のレジリエンスの強化”発行。<br>PNTサービスに関連したセキュリティプロファイルに関する文書（NISTIR 8323）作成中。 |
| 2020.5 | ● | • OSAが民主導による**“商用宇宙システムセキュリティガイドライン”**を発行。 |
| 2020.9 | ● | • 大統領令SPD-5 “**宇宙システムにおけるサイバーセキュリティ原則**”（宇宙システムは悪意のあるサイバー活動による攻撃を考慮して設計・開発されるべきこと、地上システム・運用技術・情報処理システムの保護等が盛り込まれた）を発行。 |

# 安全保障任務に用いられる宇宙システムのための国家情報保証方針（CNSSP 12）の概要①

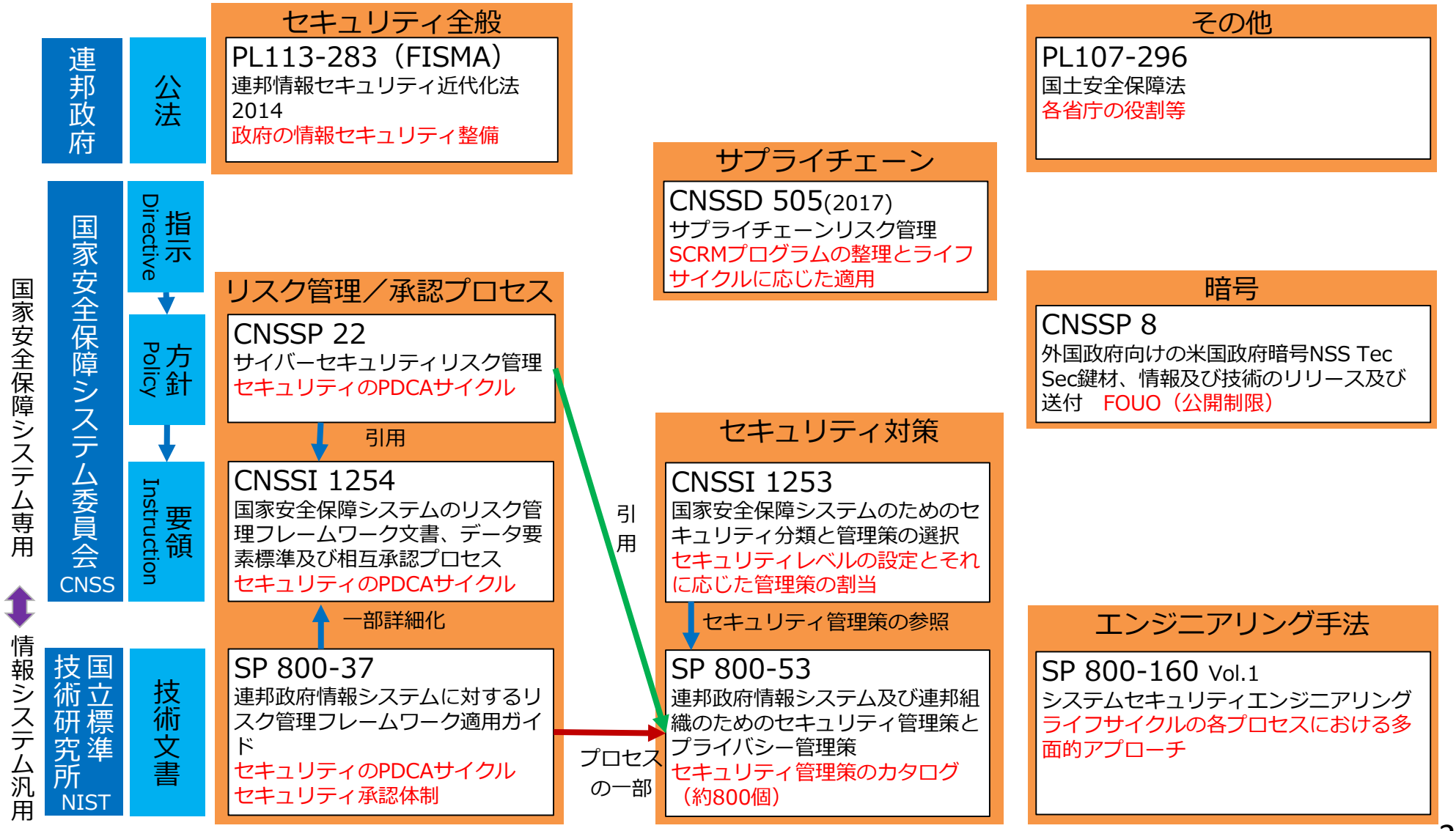
- CNSSP 12は、国家安全保障ミッションをサポートするために使用される宇宙システムのサイバーセキュリティに適用するように設計されたポリシー。

| | |
|---|---|
| 対象組織 | 米国政府  OR 米国政府  契約  事業者  OR 米国政府  合意  外国政府  |
| 対象システム等<br><br>※NIST SP 800-59 “情報システムの国家安全保障システム識別ガイドライン”も合わせて参照 | （対象システムの例）<br>打ち上げシステム  出典：Wikimedia Commons<br>試験場  出典：NASA / Robert Guere（ドライデン航空試験場）<br>宇宙プラットフォーム<br>バス機器<br>ミッション機器  <br>ペイロード  出典：NASA (Payload Systems)<br>運用センタ  <br>ユーザモデム／端末／機器  <br>AND<br>（取り扱う任務、情報等）<br>安全保障に係る情報<br>秘 注意  OR<br>国家安全保障に関わる宇宙プラットフォームへのペイロード輸送  OR<br>国家安全保障システムに係る技術・機構の実験・試験・実証  出典：JAXA(こうのとりのデブリ回収実験) |

出典：Committee on National Security Systems（February 2018）， CNSSP no.12 CYBERSECURITY POLICY FOR SPACE SYSTEMS USED TO SUPPORT NATIONAL SECURITY MISSIONS

# 安全保障任務に用いられる宇宙システムのための国家情報保証方針（CNSSP 12）の概要②

- CNSSP 12においては以下に示す法令、文書に準拠することが求められている。




出典：Committee on National Security Systems（February 2018）， CNSSP no.12 CYBERSECURITY POLICY FOR SPACE SYSTEMS USED TO SUPPORT NATIONAL SECURITY MISSIONS

１．近年の宇宙産業の動向

２．近年のサイバー攻撃の動向

３．宇宙分野におけるセキュリティインシデント事例

４．海外における宇宙分野のセキュリティ対策

**５．検討体制・検討方針**

６．ガイドライン開発について

# 経済産業省における産業サイバーセキュリティに関する検討体制

- 経済産業省では、サイバーセキュリティ課が設置した産業サイバーセキュリティ研究会の下、産業分野別のセキュリティ対策の具体化・実装を推進中。今回、**新たに「宇宙産業SWG」を新設。**

## 産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
第３回：平成31年　4月19日　開催
第４回：令和2年　　4月17日　開催（電話開催）
第５回：令和2年　　6月30日　開催

**構成員**

※2020年6月開催時点

| | |
|---|---|
| **泉澤　清次** | 三菱重工業株式会社取締役社長 |
| **遠藤　信博** | 日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社取締役会長等 |
| **大林　剛郎** | 日本情報ｼｽﾃﾑ・ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長 |
| **櫻田　謙悟** | 経済同友会代表幹事、ＳＯＭＰＯホールディングス グループＣＥＯ取締役　代表執行役社長 |
| **篠原　弘道** | 日本電信電話株式会社取締役会長 |
| **中西　宏明** | 株式会社日立製作所取締役会長 |
| **船橋　洋一** | アジア・パシフィック・イニシアティブ理事長 |
| **村井　純(座長)** | 慶應義塾大学教授 |
| **渡辺　佳英** | 日本商工会議所特別顧問、大崎電気工業株式会社取締役会長 |

**オブザーバー**

NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

**WG 1**
**制度・技術・標準化**
（計6回開催）

**WG 2**
**経営・人材・国際**
（計6回開催）

**WG 3**
**ビジネス化**
（計5回開催）

## 標準モデル（CPSF）

**Industry by Industryで検討**
（分野ごとに検討するためのSWGを設置）

- **ビルSWG** → ガイドライン第1版の策定
- **電力SWG** → 既存ガイドラインの強化
- **防衛産業SWG** → 検討中
- **自動車産業SWG** → ガイドラインを公表
- **スマートホームSWG** → ガイドライン原案の作成
- **宇宙産業SWG** → 来年度中のガイドライン開発を目指す
- ・・・

# 宇宙産業SWGでの検討事項（案）

- 本SWGでは、以下の事項について検討したい。

## 検討事項（案）

**（１）ガイドラインの開発**

- 以下を基本的なフレームワークとして活用しつつ、民間事業者向けの宇宙システムに係るサイバーセキュリティ対策のガイドラインを令和３年度中を目標に開発する。
  - 「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）Ver1.0」（2019年4月 METI）
  - 「制御システムのセキュリティリスク分析ガイド 第2版」（2020年3月 IPA）

**（２）情報共有の枠組みに関する検討**

- 宇宙業界におけるサイバーセキュリティに関する情報共有の枠組みについて検討する。

**（３）その他の必要な施策に関する検討**

- その他、宇宙業界におけるサイバーセキュリティの向上に必要な施策について検討する。

# 宇宙産業SWGでの検討に係る基本方針（案）

- 本SWGでの検討に当たっては、以下を基本方針としたい。

## 基本方針（案）

**（１）開発するガイドラインは自主的な対策を促すためのもの**

- 本SWGで開発するガイドラインは、自主的な対策を促すためのものとする。ただし、規制官庁が当該ガイドラインを参照することは妨げない。

**（２）関係府省庁・関係機関との連携**

- 本SWGにおける議論次第では、必要に応じて関係府省庁・関係機関との合同開催も視野に入れる。

**（３）他の取組との調和を図る**

- JAXA、他業界（防衛産業等）、海外等の取組との調和を念頭に置く。

**（４）「宇宙×サイバー」のコミュニティへの発展を目指す**

- 本SWG及び作業部会には、宇宙分野の専門家、産業サイバーセキュリティの専門家の両方に参加していただき、お互いの専門領域について理解を深めることを通じ、「宇宙×サイバー」のコミュニティへと発展させることを目指す。また、その延長として情報共有の枠組みついても検討する。

**（５）継続的な見直し**

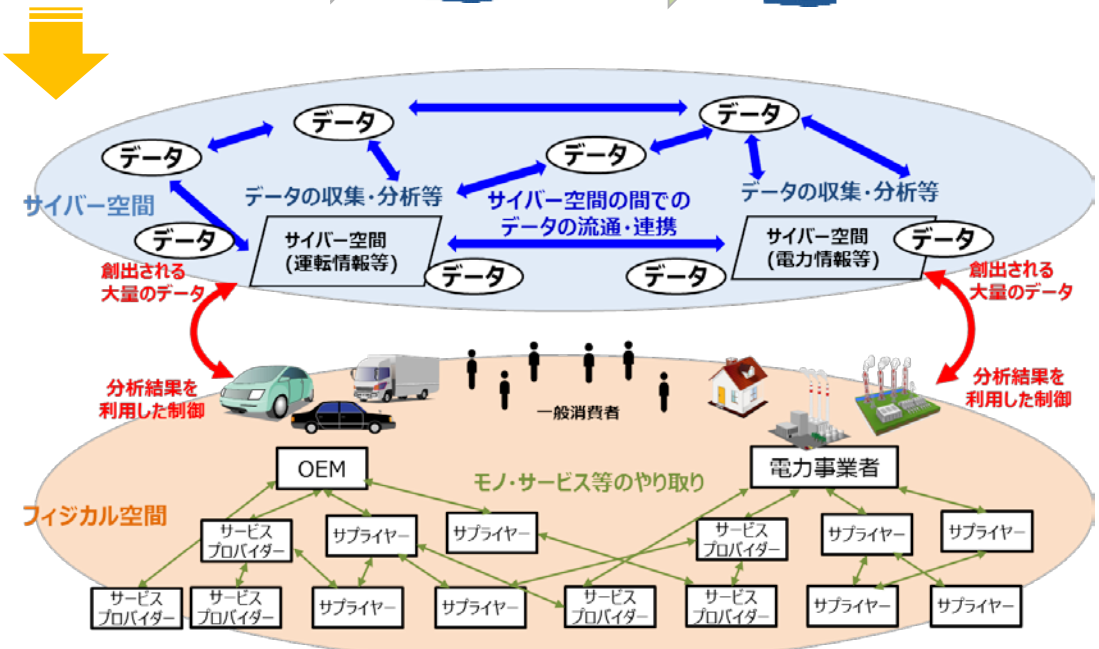
- 開発したガイドラインについては、海外や民間の最新の知見を取り入れつつ継続的な見直しを図る。

# （参考）Society5.0におけるサプライチェーン構造の変化

- 我が国では、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」の実現を提唱。
- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**となる。

**「Society5.0」以前**

**個々の企業主体の定型的なつながりで価値を生み出す**




**Society5.0の社会におけるモノ・データ等の繋がりのイメージ**

**サイバー空間で大量のデータの流通・連携**
**⇒データの性質に応じた管理の重要性が増大**

**フィジカル空間とサイバー空間の融合**
**⇒フィジカル空間までサイバー攻撃が到達**

**企業間が複雑につながるサプライチェーン**
**⇒影響範囲が拡大**

# （参考）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）（2019年4月 経済産業省サイバーセキュリティ課）

- CPSFでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデル（**三層構造**と**６つの構成要素**）を提示。

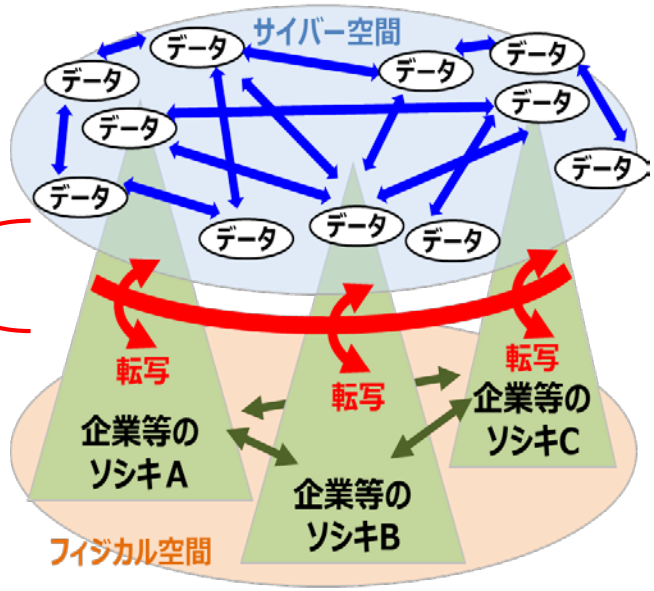
## 三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

**サイバー空間におけるつながり**
**【第３層】**
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

**フィジカル空間とサイバー空間のつながり**
**【第２層】**
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

**企業間のつながり**
**【第１層】**
適切な**マネジメントを基盤に各主体の信頼性**を確保



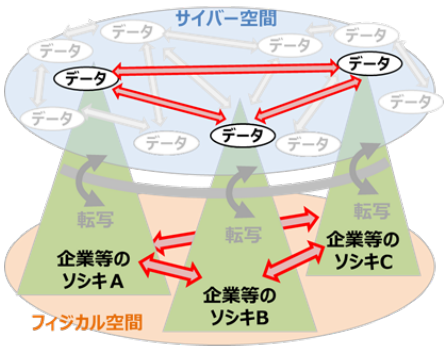
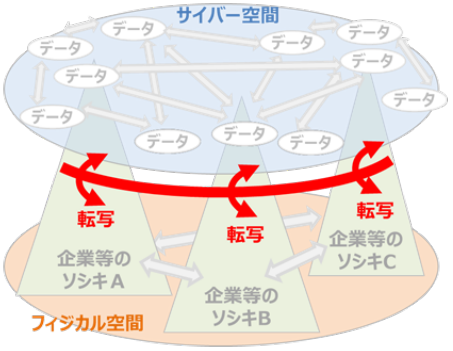
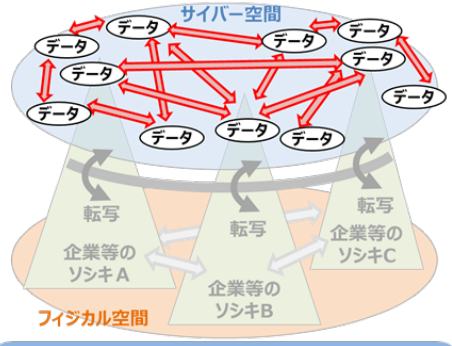

## ６つの構成要素

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６つに整理**

| 構成要素 | 定義 |
|---|---|
| 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・組織 |
| 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<br>操作する機器を含む |
| データ | • フィジカル空間にて収集された情報及び共有・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の一連の活動の手続き |
| 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 |

# （参考）CPSFの全体概要（リスク源と対応する方針の整理）

- 各層における機能、セキュリティインシデント、リスク源、対策要件を整理。

| | 企業間のつながり【第１層】 | フィジカル空間とサイバー空間のつながり【第２層】 | サイバー空間におけるつながり【第３層】 |
|---|---|---|---|
| 新たなサプライチェーン構造の整理 |  |  |  |
| 機能（守るべきもの） | • 平時及び緊急時のリスク管理・対応体制の構築と運用<br>• 企業内及び企業間のリスク管理・対応体制の構築と運用 | • フィジカル空間とサイバー空間の境界における情報の正確な転写及び正確な転写の証明 | • データの加工・分析<br>• データの保管<br>• データの送受信 |
| セキュリティインシデント | • 保護すべき資産の棄損<br>• 他組織のセキュリティ事象発生に起因する事業停止 | • 不正確なデータの送信<br>• 安全に支障をきたす動作 | • 保護すべきデータの漏えい<br>• なりすまし等による不正な組織からのデータ受信 |
| リスク源（構成要素ごとに整理） | • セキュリティリスクに対するガバナンスの欠如<br>• 他組織との連携状況の未把握 | • 不正なIoT機器との接続<br>• 許容範囲外の入力データ | • 通信経路が保護されていない<br>• 通信相手を識別していない |
| 対策要件 | ■ マネジメントルールの徹底<br>■ 関係者との役割分担 | ■ 接続相手の認証<br>■ 安全なIoT機器の導入 | ■ 暗号化によるデータ保護<br>■ データの提供者の信頼性確認 |

# （参考）CPSFにおける他の国際規格等との対応関係

- 第Ⅲ部、添付C及び添付Dにおいて、主要な国際規格等との対応関係を記載。
- NIST Cybersecurity Framework、NIST SP800-171、ISO/IEC 27001付属書Aについては、**各規格等から見た場合の対応関係も整理。**

## <添付C> CPSF ⇒ 他の国際規格等

| 対策要件ID | 対策要件 | 対応する脆弱性ID | 対策例 | 対策例を実行する主体 | NIST SP800-171 | NIST SP800-53 | ISO/IEC 27001 付属書A | IEC 62443 |
|---|---|---|---|---|---|---|---|---|
| CPS.AM-1 | ・・・ | L1_1_a_COM, L1_1_b_COM, | <High-Advanced> ・・・ | O/S | ○ | ○ | ○ | ― |
| | | | <Advanced> ・・・ | O/S | ○ | ○ | ○ | ○ |

## <添付D> 他の国際規格等 ⇒ CPSF

| NIST Cybersecurity Framework Ver1.1 | | | サイバー・フィジカル・セキュリティ対策フレームワーク | |
|---|---|---|---|---|
| 機能 | サブカテゴリID | サブカテゴリ | 対策要件ID | 対策要件 |
| 特定(ID) | AM-1 | ・・・ | CPS.AM-1 | ・・・ |

| NIST SP 800-171 | | | NIST SP800-171 から参照される NIST SP800-53 | サイバー・フィジカル・セキュリティ対策フレームワーク | | |
|---|---|---|---|---|---|---|
| ファミリ | 管理策ID | 要求事項 | 管理策名称 | 対策要件ID | 対策要件 | 対策例 |
| アクセス制御 | 3.1.1 | ・・・ | ・AC-2 アカウント管理 ・・・ | CPS.AC-9 | ・・・ | ・・・ |

| ISO/IEC 27001:2013 附属書A | | サイバー・フィジカル・セキュリティ対策フレームワーク | | |
|---|---|---|---|---|
| 管理策ID | 要求事項 | 対策要件ID | 対策要件 | 対策例 |
| A.5.1.1 | ・・・ | CPS.BE-2 | ・・・ | ・・・ |

１．近年の宇宙産業の動向

２．近年のサイバー攻撃の動向

３．宇宙分野におけるセキュリティインシデント事例

４．海外における宇宙分野のセキュリティ対策

５．検討体制・検討方針

**６．ガイドライン開発について**

# ガイドライン開発の進め方について

- CPSFで提示されている以下の流れを踏まえてガイドライン開発を進める。

## セキュリティ・リスクマネジメントの流れ

**（１）分析対象の明確化**

- 分析範囲の決定と資産の明確化
- システム構成の明確化
- 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**

- 事業被害レベルの定義
- 想定されるセキュリティインシデントの具体化および事業被害レベルの割り当て

**（３）リスク分析の実施** ※ここでは一例として事業被害ベースの手法を想定

- 自組織に対する攻撃シナリオの検討
- 事業被害レベルの評価
- 脅威の特定および評価
- 対策/脆弱性の特定および評価　等

**（４）リスク対応の実施**

- 改善箇所の抽出、選定
- リスクの低減
- リスク低減効果の把握　等

# 当面の作業：分析対象の明確化①

- 当面の作業として、分析対象の明確化を行いたい。
- 本SWGの下位に設置をする、民間企業を中心とする作業部会において、分析対象の明確化・モデル化を行う。

## 分析対象の考え方

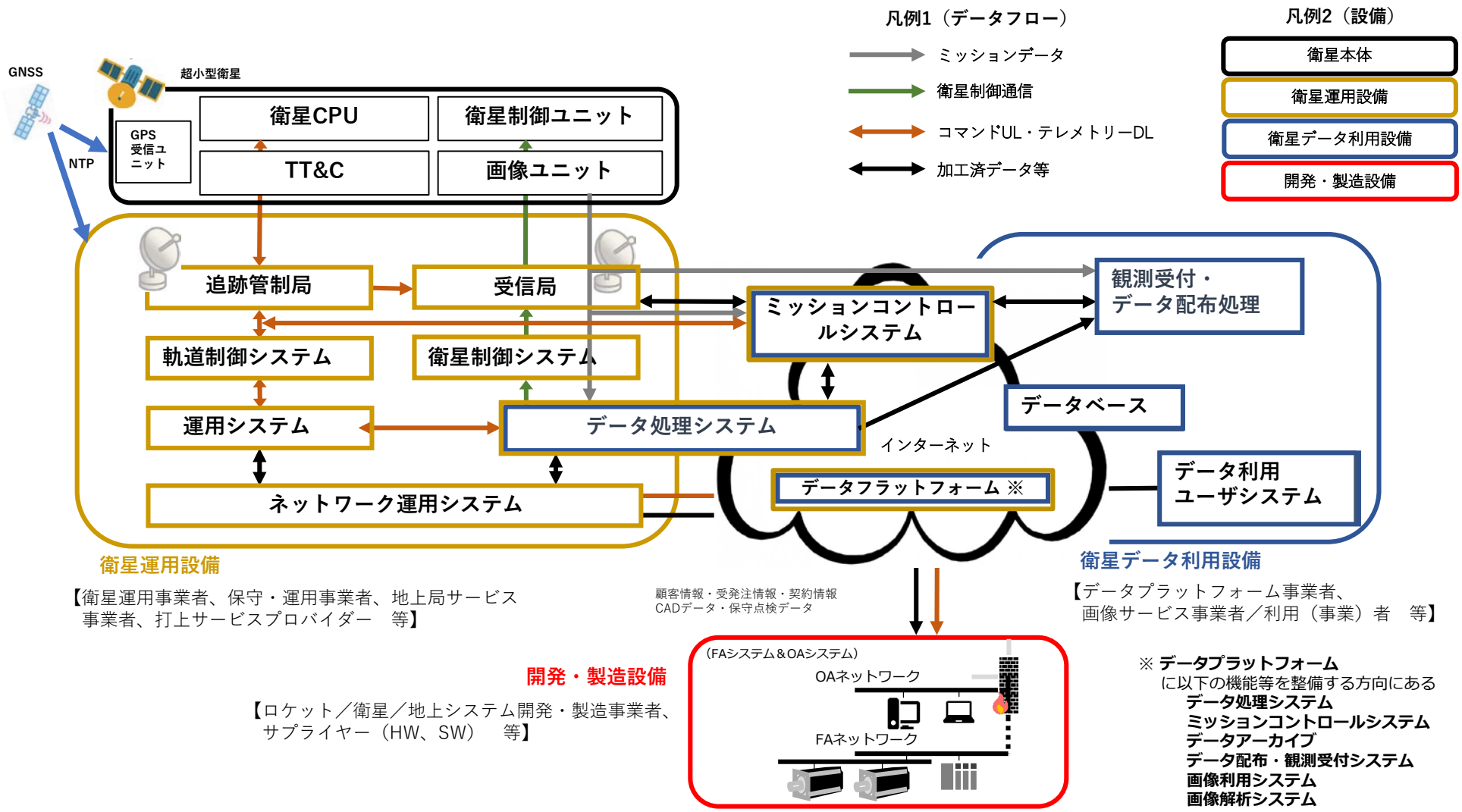
- 本SWGでは、複数の典型的な民間ビジネスのための宇宙システムを分析対象とする。
- まずは6Uサイズの超小型衛星など、今後、開発・製造が加速化する領域を例として整理・分析を進める。
- 地上局システム及び衛星データ利用のためのシステム（クラウド化されたものを含む）も分析対象に加える。

## 検討の進め方

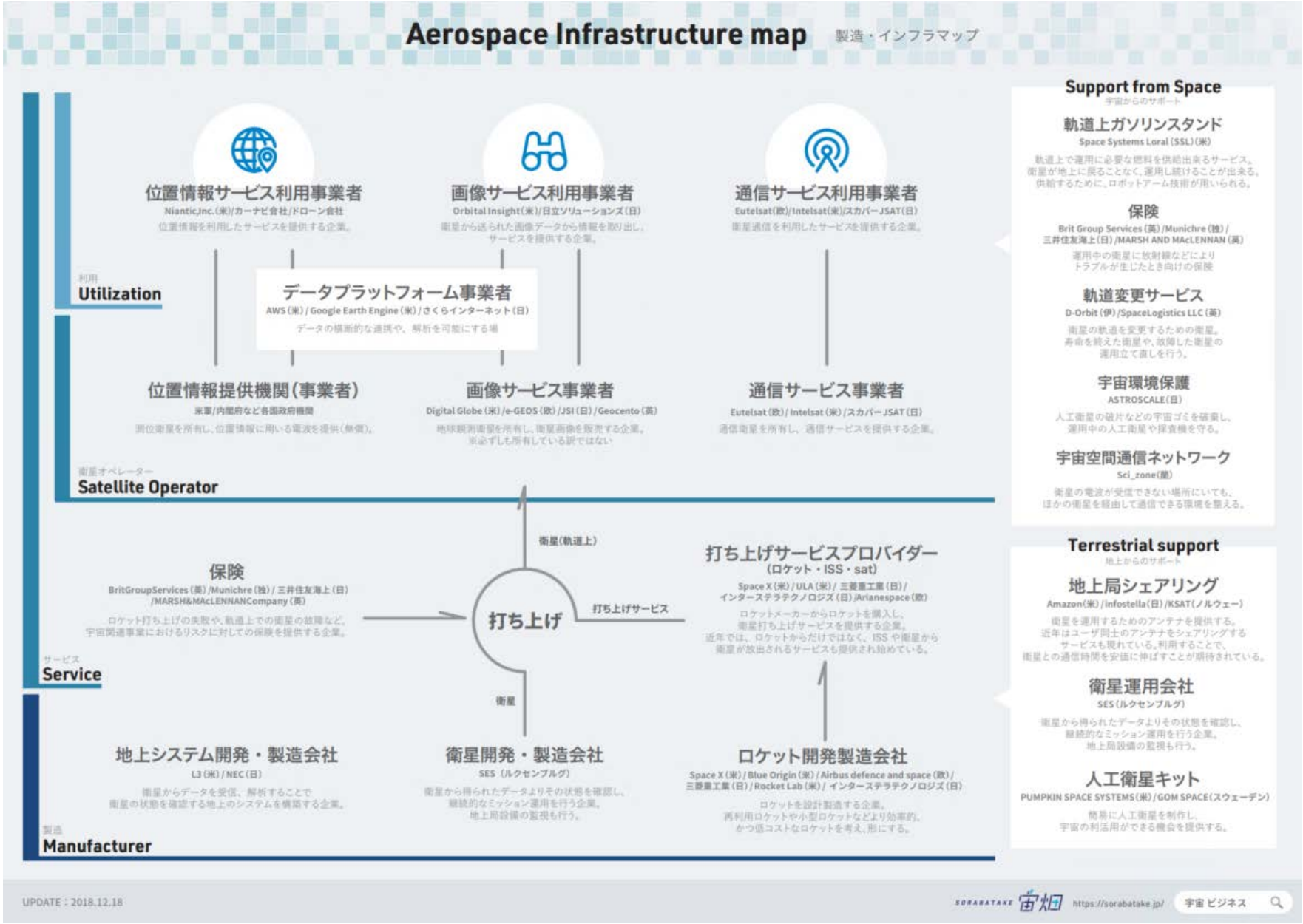
- SWGの下位に実務者を中心とする作業部会を設置し、整理・分析を進める。

# 当面の作業：分析対象の明確化②

- 分析対象の全体像の素案（イメージ）は以下。作業部会を通じて整理・分析を進める。



# （参考）宇宙基盤マップ (2019)




出典：宙畑HP ～宇宙ビジネスとは~業界マップ、ビジネスモデル、注目企業、市場規模~ https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting/space-cybersecurity-service.html