産業サイバーセキュリティ研究会
ワーキンググループ1(制度・技術・標準化)
宇宙産業SWG(第2回)
議事概要

1. 日時・場所

日時:令和3年3月3日(水) 15時30分～17時30分

場所:経済産業省別館101-2会議室／オンライン併催

2. 出席者

委員 :坂下委員(座長)、鹿志村委員、片岡委員、木下委員、栗原委員(欠席)、小山委員、佐々木委員、名和委員、丸山委員、満永委員、吉松委員

オブザーバ:内閣官房 内閣サイバーセキュリティセンター、内閣官房 衛星情報センター、内閣府 宇宙開発戦略推進事務局、総務省、文部科学省、防衛省、国立研究開発法人宇宙航空研究開発機構(JAXA)
宇宙産業SWG作業部会コアメンバー及び拡大メンバー

経済産業省:製造産業局宇宙産業室室長 是永基樹、製造産業局宇宙産業室室長補佐(総括) 伊奈康二
商務情報政策局サイバーセキュリティ課課長補佐 入江奨

3. 配付資料

資料1 議事次第・配付資料一覧

資料2 委員等名簿

資料3 宇宙システムのデータ構成 -データの流れ-

資料4 制御システムのセキュリティリスク分析とインシデント事例

資料5 事務局説明資料(非公表)

4. 議事概要

1)宇宙産業SWG開催挨拶

- 事務局から、現下の状況を踏まえて、会議室に出席の座長とオンライン出席の委員及びオブザーバ参加の関係者によるハイブリッド形式で開催との説明があった。

2)情報提供

- 小山委員から『宇宙システムのデータ構成』の紹介があった
- 木下委員から『制御システムにおけるセキュリティリスク分析とインシデント事例』の紹介があった

3)ガイドラインの開発 について

- 事務局から第1回SWG及び第1回作業部会での主なコメント、及びガイドラインの開発についての検討結果の説明があった。

4)自由討議

① 宇宙システムのデータフローについて

- 衛星と地上間の通信形態については、インターネットプロトコルはまだ本格的に採用されておらず、専用のフォーマット(CCSDS 準拠)が使われている。コマンドやテレメトリの回線は数百 bps～数 kbps 程度であるが、ミッションデータの通信の場合、通信衛星では数百 Gbps、観測衛星では数百 Mbps の通信速度である。
- 通信衛星ではデジタル化が進んでいる。打ち上げ後、通信に係る方式等を自由に変えられるということで活用され

ている。平易に使えるという観点では、デジタル化というよりも、超小型衛星コンステレーションの登場により、小さな端末を搭載して通信するという動向にあり、最終的には携帯電話位のサイズを目指している。ただし、大型の衛星については、専用の送信局が必要となっているのが現実である。

② ガイドラインのスコープに関して

- スコープで小型衛星を対象にしていることから、必然的に規模の小さい企業が主な対象と考えられる。成長段階にある小規模の企業の場合、ビジネス先行になる可能性が高いと考えられる。大企業が先行して行っているセキュリティ対策、何かあった場合のレジリエンスを目的とした事業継続のための仕組みが急所となる。
- ビジネスを守っていくという姿勢が必要であり、サイバーインシデントあるいはセキュリティにかかる事故が発生した場合に、最小コストで原因究明ができたり、所管官庁に迅速に報告ができたりする仕組みであれば、小規模の事業者でも遵守可能と期待できる。
- 原因究明可能なログを積極的に残す仕組みを記述することが重要と考える。事故が発生した後に迅速に原因を究明できれば、結果的にシステムを守ることになると考えられる。目的についても、発生を防止・抑止・回避するだけでなく迅速に対処するということも含めるべきと考える。
- 開発段階のセキュリティの重要性に注目されているが、先ず運用に焦点を置くというアプローチが良いと思うので、その旨を明示しておくと良い。

③ 宇宙システムを取り巻くセキュリティに係る状況について

- 民生分野ではないかもしれないが、SolarWinds の事件は事例に加えても良いのではないか。現段階で、小型衛星がクリティカルな部分にデータを送信するということはないかもしれないが、将来的にはクリティカルなシステムにデータを供給するようになると、ゼロトラストの技術が重要となってくる。将来的な課題として、ガイドラインに記載するとなると、宇宙事業者がサプライヤーに対してゼロトラストを要求する考え方を盛り込むことになると考えられる。
- 対象システムを解析する場合、サーバ単位にしたり、類似する機能の代表を取り扱ったりするが、資産の数が多いのでモデル化が必要である。ブレークダウンする場合も、すべて一律ではなく、メリハリをつけて、特に重要なところは掘り下げ、そうでなければ大きな粒度で取り扱うこともある。但し、粒度によって対策も変わってくる。
- 衛星だけで 70 万点も部品があるため、対象システムはあまり細かくせず、本ガイドラインでは概念的な整理を優先すべきと考える。システムにおけるインプット／アウトプット等を整理し、抽象化した形でガイドラインを作成すべきと考える。突き詰めると標準的な対策・要件になり、宇宙システムに特有の話ではなくなってしまうことも想定される。そのため、システムで肝となるリスクに対しては、具体的な対策を事例として補足する形でメリハリをつけたガイドラインとし、衛星の大小による影響を受けないということであれば、全般的に使えるガイドラインとするのが良い。

④ 民間宇宙システムにおけるセキュリティ対策のポイント

- ベンチャー事業者等ではコンステレーションが増えてきている。資産を守るという観点では、事業者を守ることとなる。一方、被害から守るという観点では、衛星の制御が乗っ取られた場合、第三者に被害が与える攻撃があるとすると、コンステレーションでは影響度が大きいように感じられる。事業者だけでなく第三者も守るという観点も考慮して検討できれば良いと思う。
- CIA（機密性・完全性・可用性）以外にも HSE（健康・安全・環境）を含めて事業被害を評価する場面も増えてきている。そういった視点を考慮して分析するのは良いことだと考える。
- 事業被害を考える際は、単にお金の問題に留まる話ではない。例えば、制御プラントから有害な溶液が流出して海洋汚染につながったり、人体に影響したりすることが、制御分野での最大の関心事項である。データの完全性を担保するといった IT の範疇に留まらない。工場の場合、生産したデータの改ざんより、生産するデータのレシピを改ざんされることがより危惧されている。
- 内部犯行の論点があったが、脅威を考える上では、環境要因、過失、故意の 3 つで整理すれば、外部・内部は関係なくなる。データセキュリティの改ざんの取扱いはリスク分析次第で整備できるものと考える。

- 安全という意味で、フェールセーフ機能を搭載したものを調達することで最終的に安全が確保されれば良いという考え方で整備をしないと、セキュリティだけで考えると過剰になる可能性がある。
- 脅威源について実際に発生したものを記述するのが良い。制御技術についてはオープン技術を使ったところから入り込む攻撃が増えている。マイクロソフトのポータルにもあるように、コロナ禍でアカウントハイジャックも急増し、また、マルウェア感染は前年比 430%と昨年とは異質な動向・変化がある。

5) その他

最後に事務局から、今後のスケジュールについて以下のとおり連絡を行った後、閉会した。

- 4 月以降に作業部会を 1 回又は 2 回程度開催後、第 3 回検討会の実施を予定している。
- 詳細については後日連絡する。

お問合せ先

製造産業局　宇宙産業室
電話：03-3501-1512