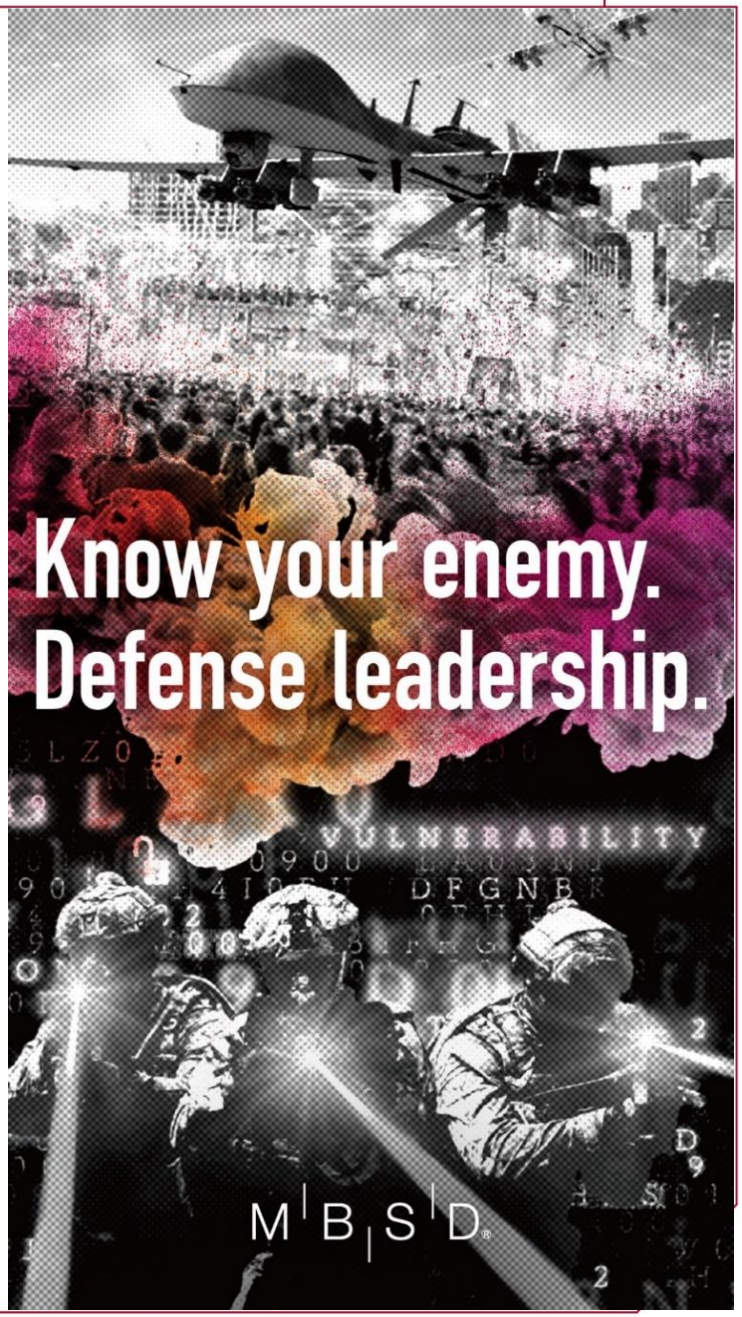
宇宙産業と
サイバーセキュリティ対策

２０２１年１１月１０日



関原　優　（Masaru Sekihara）

三井物産セキュアディレクション株式会社
執行役員（コンサルティングサービス事業本部・公共事業部管掌）
情報処理安全確保支援士（第000073号）

三井物産で情報セキュリティ専門会社である三井物産セキュアディレクションの設立に携わる。
20年程、IT・サイバーセキュリティのサービス事業に従事し、SOC構築、サイバー攻撃分析、
疑似攻撃によるWebサイトやネットワークの診断、自社SIEMなどのセキュリティツール開発、
官公庁やグローバル企業等に対するセキュリティコンサルティングなどを手掛ける。

配下部門には１５０名超のコンサルタント・セキュリティ技術者（高度なサイバー攻撃をログなどから発見するThreat Hunter、マルウェア解析技術者など）を擁し、顧客組織のセキュリティ対策にあたっている。

【特許】

- 米国特許_第11159541号(2021年10月26日)/国内特許_第6219550号 発明者
  概要:ファイルマッピングによる暗号化に対するランサムウェア検知・防御技術
- 米国特許_第10264002号/国内特許_第5996145号 発明者
  概要:暗号化時のファイル特性を利用したランサムウェア検知・防御技術
- 国内特許_第5955475号 発明者
  概要:自己多重起動抑止特性を利用したマルウェア感染防御・無効化技術

【著書】

訴訟・コンプライアンスのためのサイバーセキュリティ戦略/NTT出版 など

はじめに

昨今、世界中でサイバー攻撃が多発しています。
サイバー犯罪による被害格は毎年数千億円にも上ると言われており、サイバー攻撃により窃取した身代金や、詐欺により奪った金銭は、さらに犯罪組織の活動を拡大させるという流れが活発化していると言えます。

規模や業種を問わず、あらゆる企業がサイバー攻撃の脅威に晒され、システムやネットワークの停止に伴う業務停止、大企業等の取引先への侵入の踏み台となり、さらには信用失墜や損害賠償といったリスクを抱える可能性があります。

昨年も、コロナ禍の中でリモートワークが急速に普及する一方で、セキュリティ対策が十分でないネットワーク機器等の脆弱性を突かれ、多くの企業・組織が攻撃の被害に遭っています。攻撃者が、対策が十分でなく容易に攻撃可能/利益を得る事ができる対象を狙ってくることは過去幾度も繰り返されている事実です。

サイバー犯罪の高利益化
世界中で被害が拡大
想定被害額は毎年数千億円とも言われる
そして新たなマルウエア開発や
攻撃人材の採用へとビジネスが拡大

狙われるのは大企業だけではない
グループ企業や取引先など含めた
ターゲットと繋がりを持つ
サプライチェーンへの攻撃

新たな環境・仕組みなどセキュリティ対策が十分で無い対象を狙う
幾度も繰り返される/特に注意が必要

宇宙ビジネスの拡大

宇宙ビジネスの市場拡大

宇宙ビジネスの市場規模は世界で40兆円、2040年には100兆円規模に拡大すると言われている。

■衛星通信/観測
・宇宙インターネットによる世界規模の通信環境の整備
・小型化/低価格化する小型衛星などにより、衛星画像、観測データの利活用

■宇宙旅行
ヴァージン・ギャラクティック社、ブルーオリジン社、スペース・アドベンチャーズ社
スペースX社などが宇宙旅行サービスを展開している。

■調査研究/資源開発
宇宙環境を利用した開発、他惑星等の資源開発

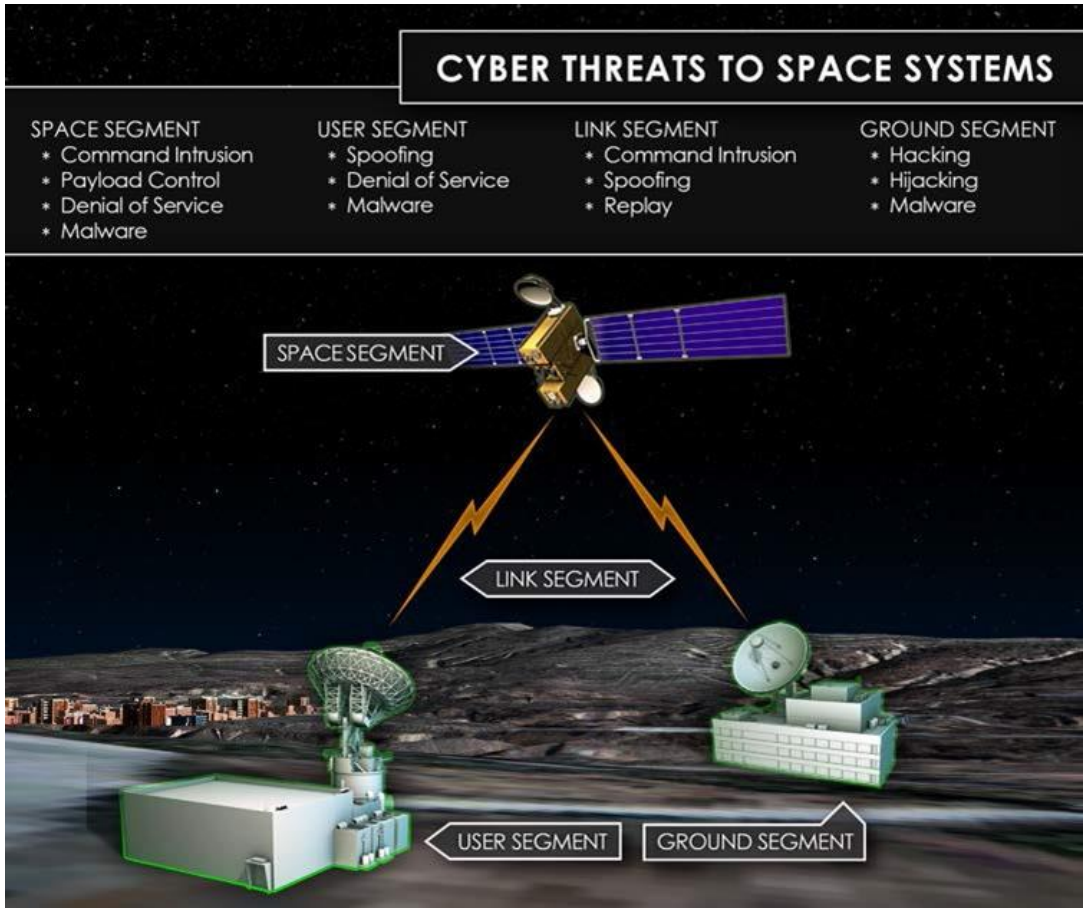
など

宇宙等の新たな領域での脅威

1. 宇宙システムにおけるサイバー脅威
2. GPSにおけるサイバー脅威
3. ドローンにおけるサイバー脅威

Ⅰ．宇宙システムにおけるサイバー脅威(1/2)

- **宇宙セグメント（人工衛星等）**
  - コマンド不正侵入
  - ペイロード制御
  - サービス妨害
  - マルウェア
- **ユーザーセグメント（利用者）**
  - スプーフィング（なりすまし）
  - サービス妨害
  - マルウェア
- **リンクセグメント（受信局）**
  - コマンド不正侵入
  - スプーフィング（なりすまし）
  - ジャミング
  - 盗聴（傍受）
- **地上セグメント（追跡管制局等）**
  - ハッキング
  - ハイジャック
  - マルウェア
- **その他**
  - サプライチェーンへの攻撃



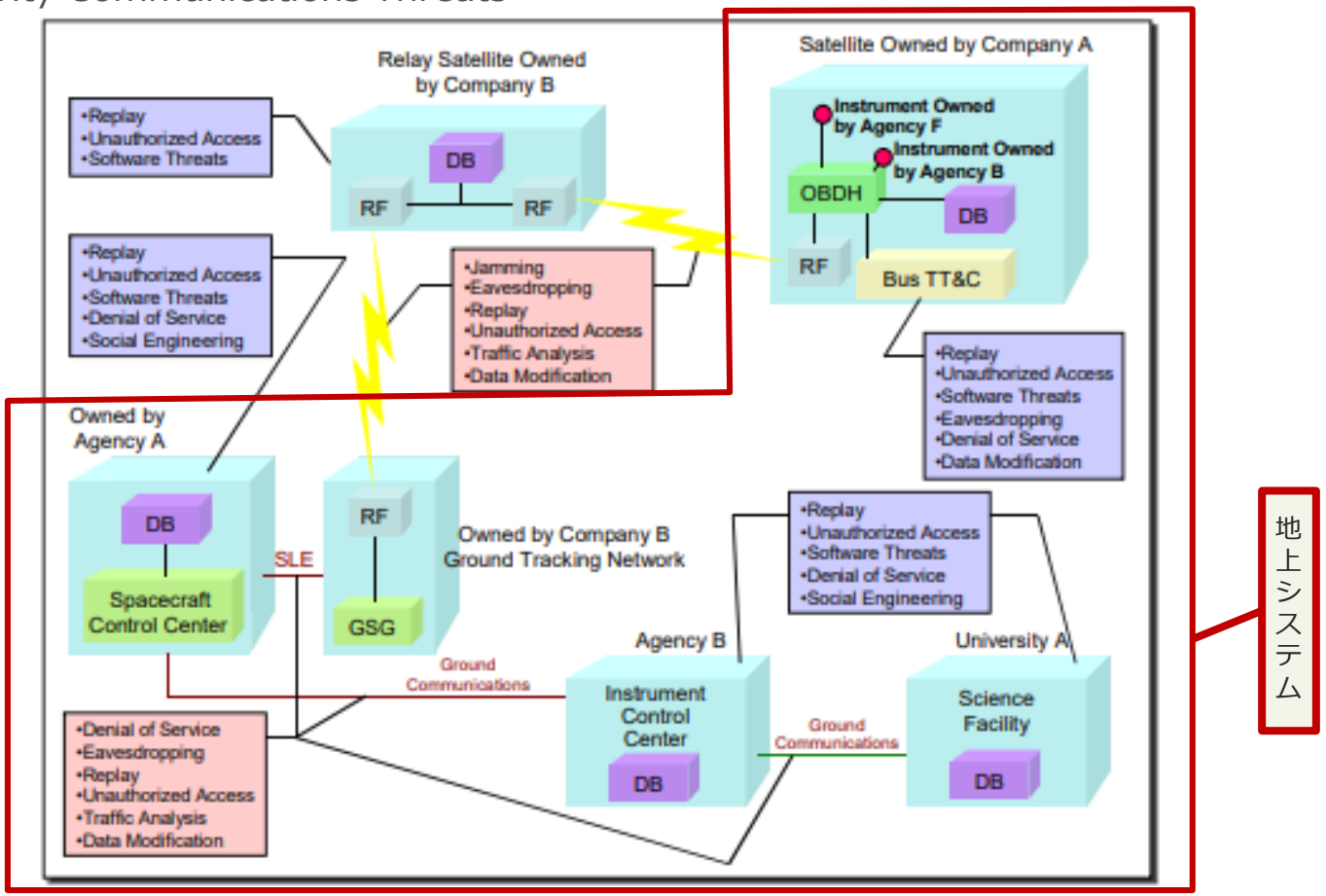
出典:AEROSPACE CRPORATION 『DEFENDING SPACECRAFT IN THE CYBER DOMAIN』November 2019

Ⅰ．宇宙システムにおけるサイバー脅威(2/2)

民間宇宙システムにおけるサイバーセキュリティ対策の主な国内外動向

2018：米国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』を改訂
2019：Orbital Security Alliance（OSA）が『Big Risk in Small Satellites』発表
2019：米国で民主体の『SPACE ISAC』立上げ
2020：経済産業省が『民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン』の検討開始
2021：米国NISTが『民間衛星向けのサイバーセキュリティ対策のガイドライン』ドラフト版を発行

CCSDS Security Communications Threats



出典：CCSDS『SECURITY THREATS AGAINST SPACE MISSIONS（INFORMATIONAL REPORT）, CCSDS 350.1-G-2』（2015年12月）

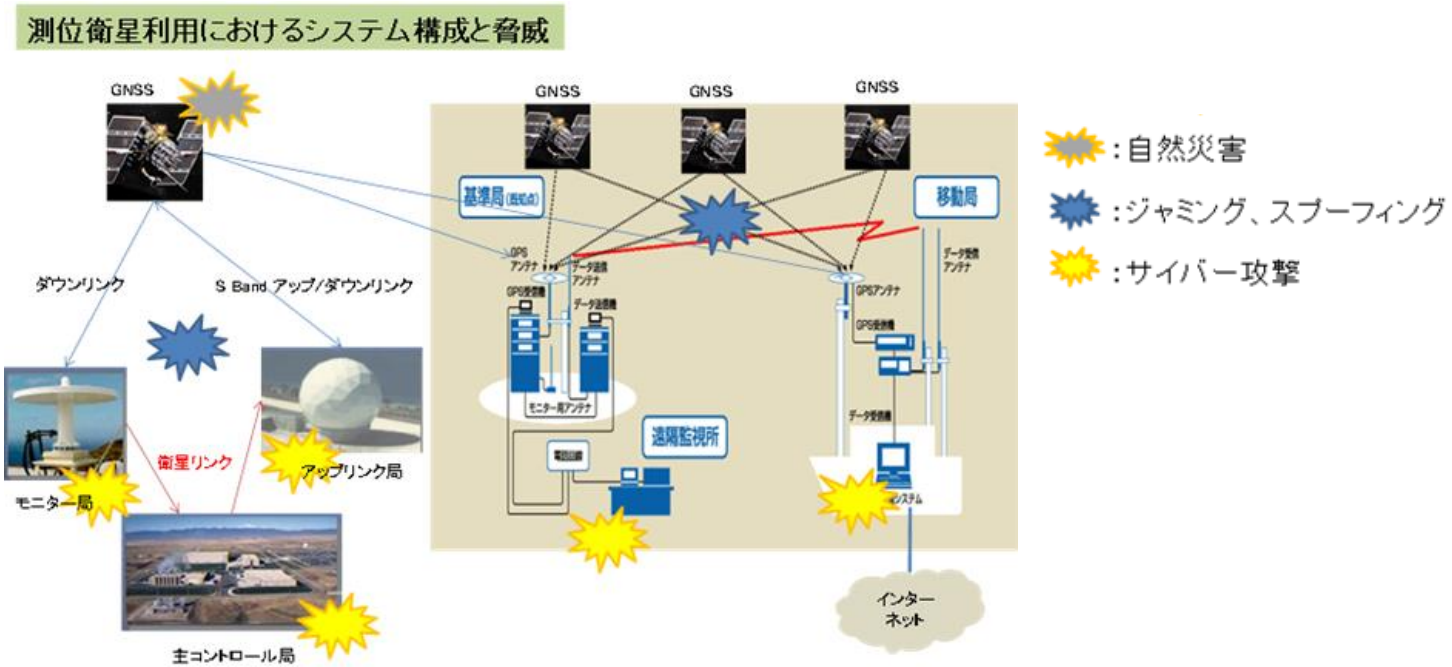
2．GPSにおけるサイバー脅威(1/2)

公共および民間、航空宇宙および防衛、スマートシティ、IoT、金融、産業、自動車、ITS、モビリティ、放送および通信、クラウドなど、世界中の重要インフラが常時GPSのPNT（Positioning,Navigation,Timing）情報に直接依存している。

GNSS 衛星の信号は電波としては微弱であり、またその仕様が公開されているため、以下の様な妨害が可能。

スプーフィング（SPOOFING）：人為的に偽のGNSS 衛星を模倣した信号を作り出し、目標とするGNSS 受信機に受信させ、その使用者が認知する位置（もしくは時刻）情報 を誤らせる。

ミーコニング（MEACONING）：実際のGNSS 衛星の信号をもとに、遅延や一部改ざんなどの手を加えて再放送した信号を目標とする GNSS 受信機に受信させ、その使用者が認知する位置（もしくは時刻）情報を誤らせる。



GNSS(Global Navigation Satellite System / 全球測位衛星システム)：
米国のGPS、日本の準天頂衛星システム、ロシアのGLONASS、EUのGalileoなどの衛星測位システムの総称

2．GPSにおけるサイバー脅威(2/2)

経済損失例：

- GPS / GNSSが5日間使用できなくなった場合、英国では5B£（50億ポンド）の経済的損失になると試算している。
  【参考：London Economics『The economic impact on the UK of a disruption to GNSS』June 2017】

事例：

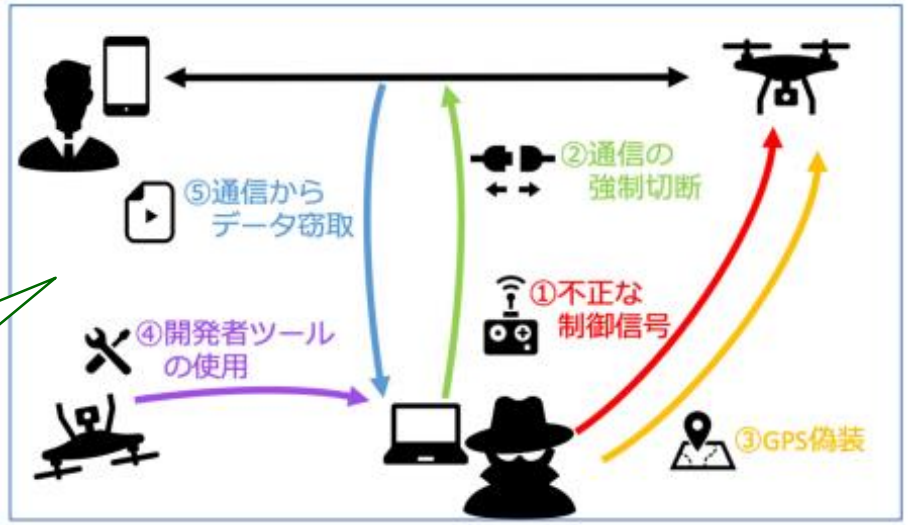
- 地上デジタルネットワークで正確な時刻が利用できないと、テレビ画面にフリーズした画像が表示

- 黒海でGPSスプーフィングが発生、その結果、海軍艦艇は相互の位置認識能力を喪失したとされる。

3．ドローンにおけるサイバー脅威(1/2)

- 空中セグメント
  - コマンド不正侵入
  - ペイロード制御
- ユーザーセグメント（操作端末）
  - スプーフィング
  - サービス妨害
  - マルウェア
- リンクセグメント
  - コマンド不正侵入
  - スプーフィング
  - リプレイ
  - ジャミング
  - 盗聴（傍受）
- その他
  - サプライチェーンへの攻撃

ドローンに対するサイバー攻撃の影響例



ドローンに対する主なサイバー攻撃の経路例

①ドローンへの不正な制御信号の送信
②ドローンと操作端末との接続断
③不正なGPS信号の送信
④開発者ツールの目的外用途使用
⑤通信盗聴による撮影映像/画像の窃取

出典：IPA『ドローンセキュリティハンドブック』2021年6月
https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/drone.html

3. ドローンにおけるサイバー脅威(2/2)

- 模擬攻撃による脆弱性の検証例

			ドローンA	ドローンB	ドローンC
ドローン仕様	種類		トイドローン	汎用ドローン	産業用ドローン
	離陸重量		約130g	約320g	約1,400g
	スマートフォンからの操作		○ Wi-Fi Password:無	○ Wi-Fi Password:有 (SSID固定/PW変更可)	--
	プロポ(2.4GHz無線)		○	○	○
	GPS搭載		--	○	○
模擬攻撃プログラム	不正操作	不正な制御信号	✓ 緊急停止	×	×
		通信の強制切断	✓ 不時着	✓ ホバリング維持	--
		GPSの偽装	--	×	✓ 位置情報の偽装
		開発者ツールの使用	✓ 緊急停止	✓ 緊急停止	×
	データ漏えい	通信からデータ窃取	✓ パケットキャプチャ復元	✓ リアルタイム	--

【凡例】○：装備あり　✓：模擬攻撃成功　×：模擬攻撃失敗　--：装備なし/未実施

出典：IPA『ドローンセキュリティハンドブック』2021年6月
https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/drone.html

新たな領域　脅威への対応

宇宙関連のシステムにおいても様々な脅威が挙げられています。
リスクを想定していれば、システム開発時にチェック機構を設ける、
開発委託先への依頼内容に、セキュリティ要件を含めるなどを検討できる場合があります。

■セキュリティの考慮
　新しいシステムやITを用いた利便化が進む際、セキュリティの考慮が不足しがちになります。

　開発体制にセキュリティチェックを行うための枠組みや、知見が十分に用意される前に、
システム化や整備が進むことで改修コストが大きくなったり、リスクが顕在化することが懸念されます。

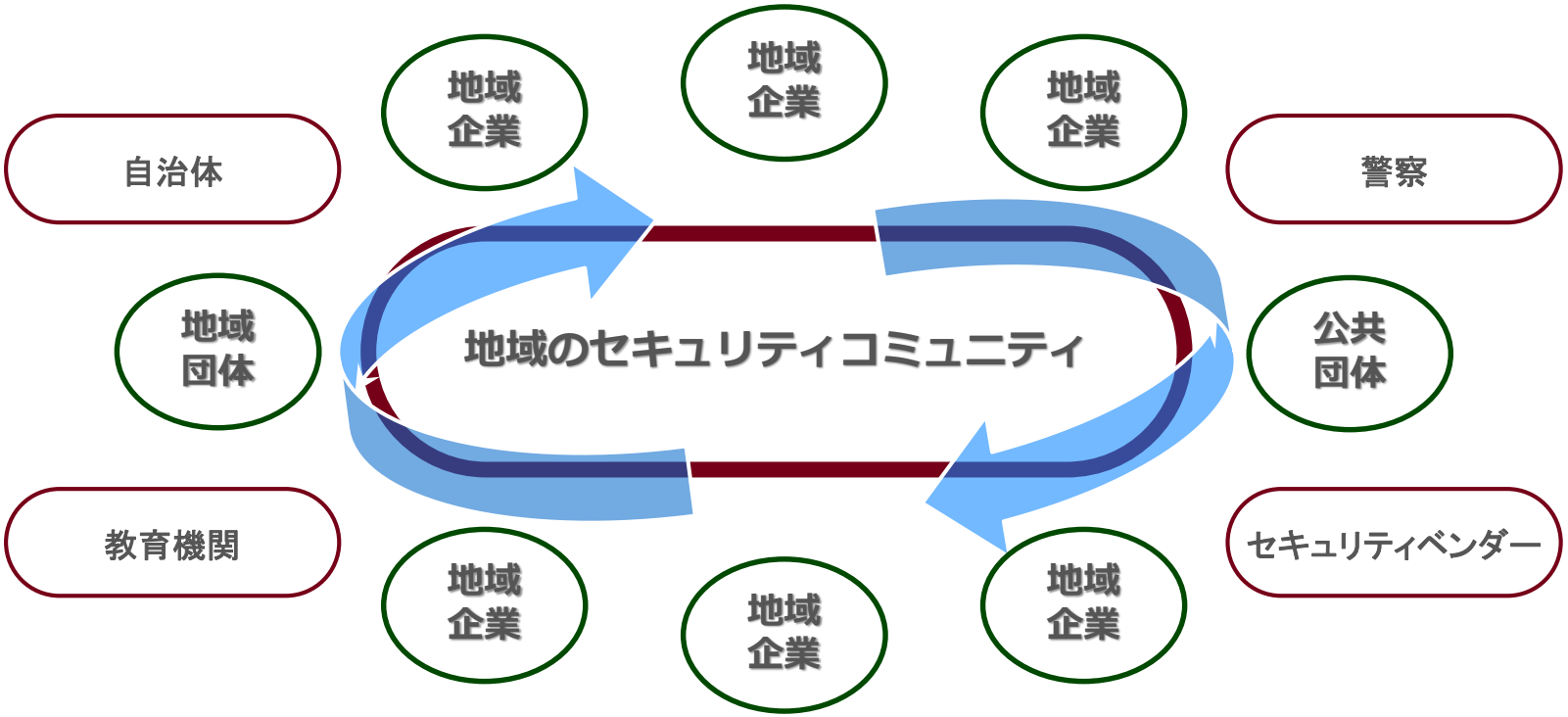
　これは宇宙関連システムに特化したことでなく、また連携する既存のITシステムとの間でも
セキュリティリスクの考慮が不足することが良くあります。

技術的に、個社で対応出来ない脅威もありますが、
まずは、自社で取り組むビジネスや開発するシステム、連携する企業とのサプラチェーンなど、
どのようなリスクが想定されるか検討し、必要に応じた対策を検討されることをお勧めします。

地域のセキュリティコミュニティ

地域のセキュリティコミュニティ

個々の企業・組織だけで対策を強化するのは難しい。
身近にセキュリティについて聞ける関係先を持ち、
できることから実施、協力できるコミュニティの形成が進みつつある。



体験の共有	交流	情報の共有
・自分のできたこと/できなかったこと ・同業種、取引先同士のビジネス上のセキュリティ要求状況	・企業同士の交流から新たなビジネスも ・企業と学生の交流から新たな雇用も	・費用をかけずにできること ・費用をかけて実施したこと ・国や公共団体、セキュリティベンダーなどの有用情報

最後に

サイバーセキュリティは特別な難しいものと考えない。

新たな仕組みが広がる、利便性が向上するようなとき
セキュリティの考慮が不足した脆弱なシステムや環境が生まれることが
多くあります。

セキュリティ対策のためにかけられるコストは限られています。
安価に作りこまなければビジネスとして成り立たない、
一方、リスクが顕在化すればビジネスが成り立たなくなるかもしれません。

どのようなリスクがあるのか把握し、自分ごとと捉えられれば
費用の大小問わず、自身で対策や対応することは、普段からやっている
ことと変わりません。

地域の方々との交流を通して、取り組まれている対策を把握したり、
公開情報などを活用して社内教育をしたりなど、単独ではリスクが
わからない場合でも、先に取り組まれている方々と話すことで様々な
気づきがあります。
できるところから取り組んで頂ければ幸いです。

三井物産セキュアディレクション株式会社