資料５－４

宇宙×ICTの安心、安全対策

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

未来ICT研究所　主管研究員　佐々木雅英
Email: psasaki@nict.go.jp, Tel: 042-327-6524

背景

宇宙インフラは、社会活動に必須のものとなりつつあるが、同時に**脆弱性**も併せ持つ

・苛酷な環境（真空、宇宙線、弱い重力束縛）
・一度打上げられたら修理困難

（１）物理的脅威

・スペースデブリとの衝突
・衛星間の接近・衝突
・ミサイルやレーザー光による破壊

→ 補足資料を参照

（２）情報セキュリティ脅威

・電波やレーザ光によるジャミング
・サイバー攻撃
・盗聴、改竄、制御の乗っ取り

１個の破壊、攻撃が全地球規模に甚大な被害を及ぼす危険性

脅威の予測・分析、安心・安全への対策が必須

一国では対処しきれない問題が多く、国際的な連携が必須

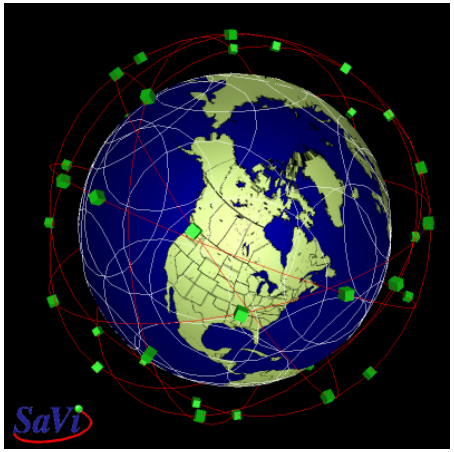
（２）情報セキュリティ脅威

・真の攻撃者がわかりにくい（攻撃者が圧倒的に有利）
・攻撃内容も見えにくい一方で、物理的被害を引き起こす

衛星コンステレーション計画

これまで政府主導の宇宙開発に、民間企業が積極参入し始め
新しい宇宙ビジネスが開花しつつある。

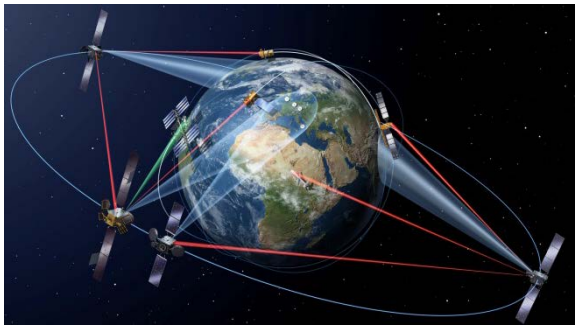
静止軌道や低軌道に多数の衛星を配備し**グローバル通信網**を構築



画像はオープンソースから引用

O3b Networks, SpaceX, OneWeb, eightyLEO, LeoSatなど
⇔背後にGoogleなどの巨大資本

低軌道の衛星コンステレーションにより高精度の**リアルタイム地球観測網**を構築



画像はESAのオープンソースから引用

海外：Terra Bella, Planet, Spire Global, OmniEarth
日本：アクセルスペース、キャノン電子、ウェザーニュース

将来的なサイバーリスクと脅威

リスク

① 衛星メガコンステレーション（4千機 ⇒ 1万機）

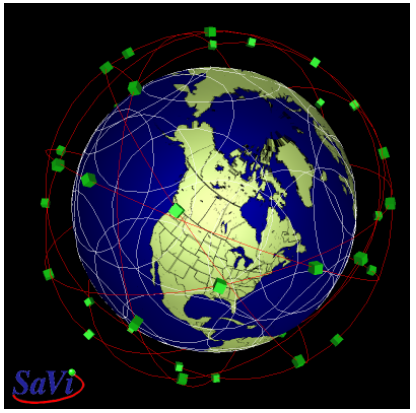
・リモートセンサーは長く使い続ける

・格好の標的として攻撃され続ける

地上でもウェブカメラの
ウィルス感染が急増中

・すべてが、ネットで繋がっている

・システム全体の安全性が、
脆弱な一箇所に依存してしまう



画像はオープンソースから引用

② 低コスト化への要請、広がるサプライチェーン

・廉価な部品を世界中から調達
⇒不正な罠（バックドア）が紛れ込む可能性が高まる

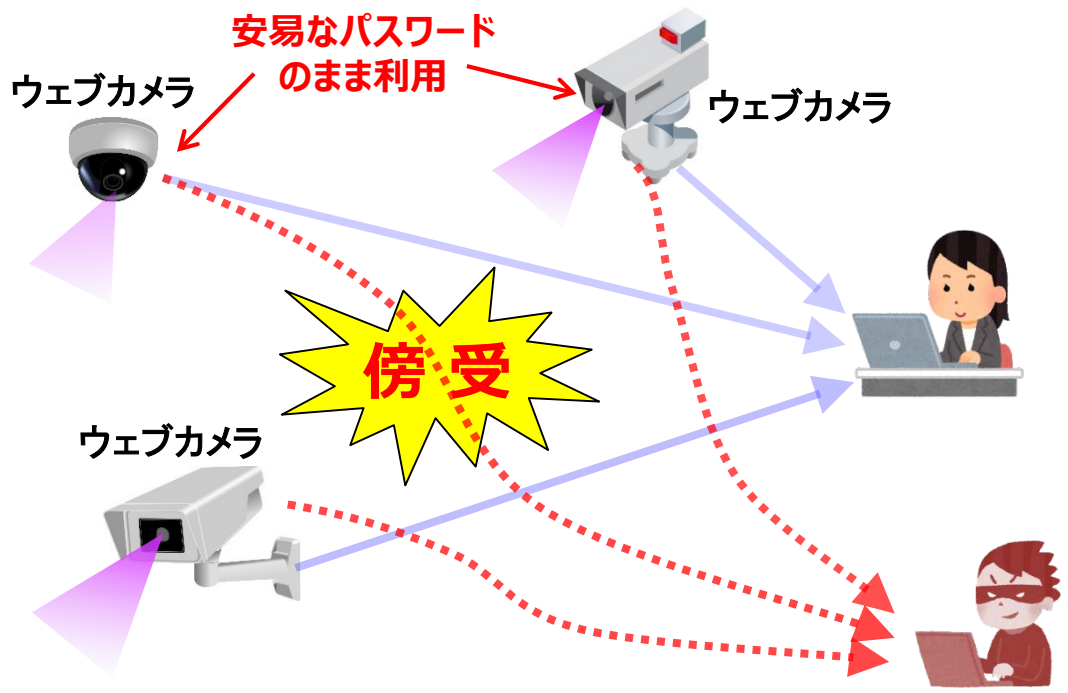
・設計開発段階からセキュリティ対策にコストを掛ける「security by design」が欠落しがち

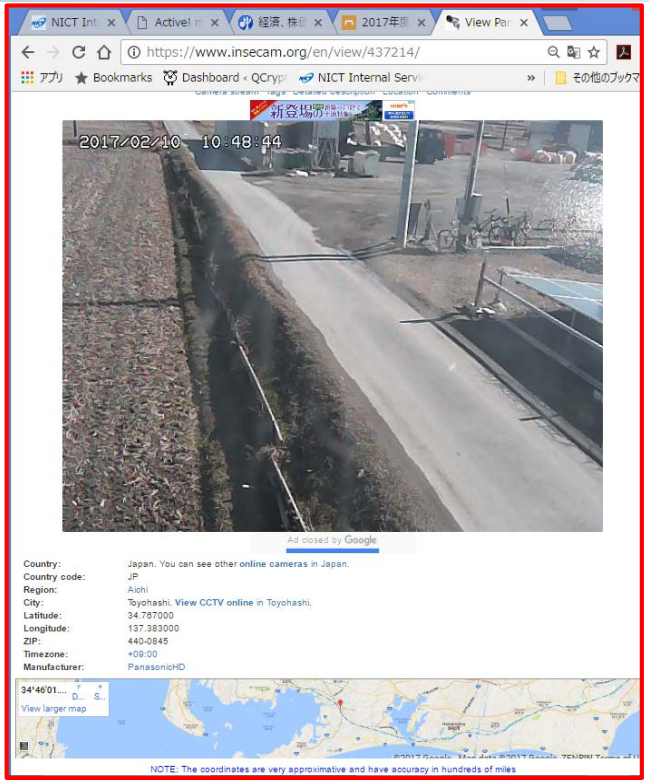
脅威

攻撃者は、防御の固い軍事衛星ではなく、対策の手薄な商用衛星を狙う

脆弱な一点を探し当て、そこから徐々に侵入範囲を拡大、最終的に
衛星コンステレーションと地上網まで含めたインフラ全体を乗っ取る

地上の脅威事例：監視カメラの盗聴





Insecam.org上で公開されている
映像と位置情報

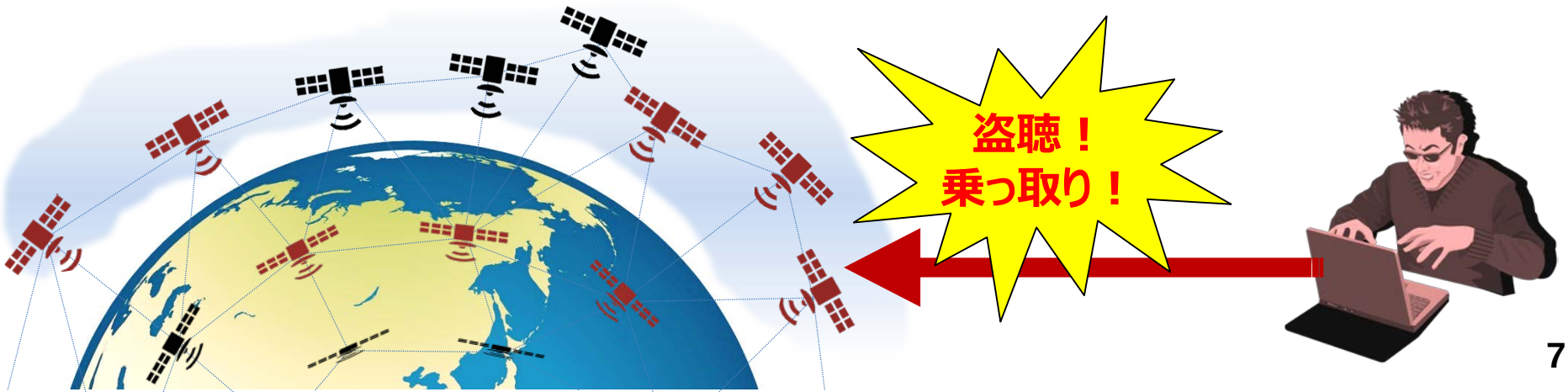
2014年～ ロシア（監視カメラの盗聴）

・ロシアにあるとされる匿名ウェブサイトInsecam.org上で、インターネット上の監視カメラの映像ストリーミングを傍受し、**ウェブサイト上で映像と場所を公開している。**

・出荷時パスワードのまま利用している監視カメラは、機種名などから比較的簡単にアクセス可能。米国で6000件以上、**日本で1800件以上の監視画像**が漏えい中(2017年2月10日時点)。

セキュリティ対策の脆弱なIoT機器は、簡単に盗聴され、乗っ取られる

衛星コンステレーション上のリモートセンサーや通信機器に対しても、同様の、あるいはさらに高度な盗聴リスクが懸念される



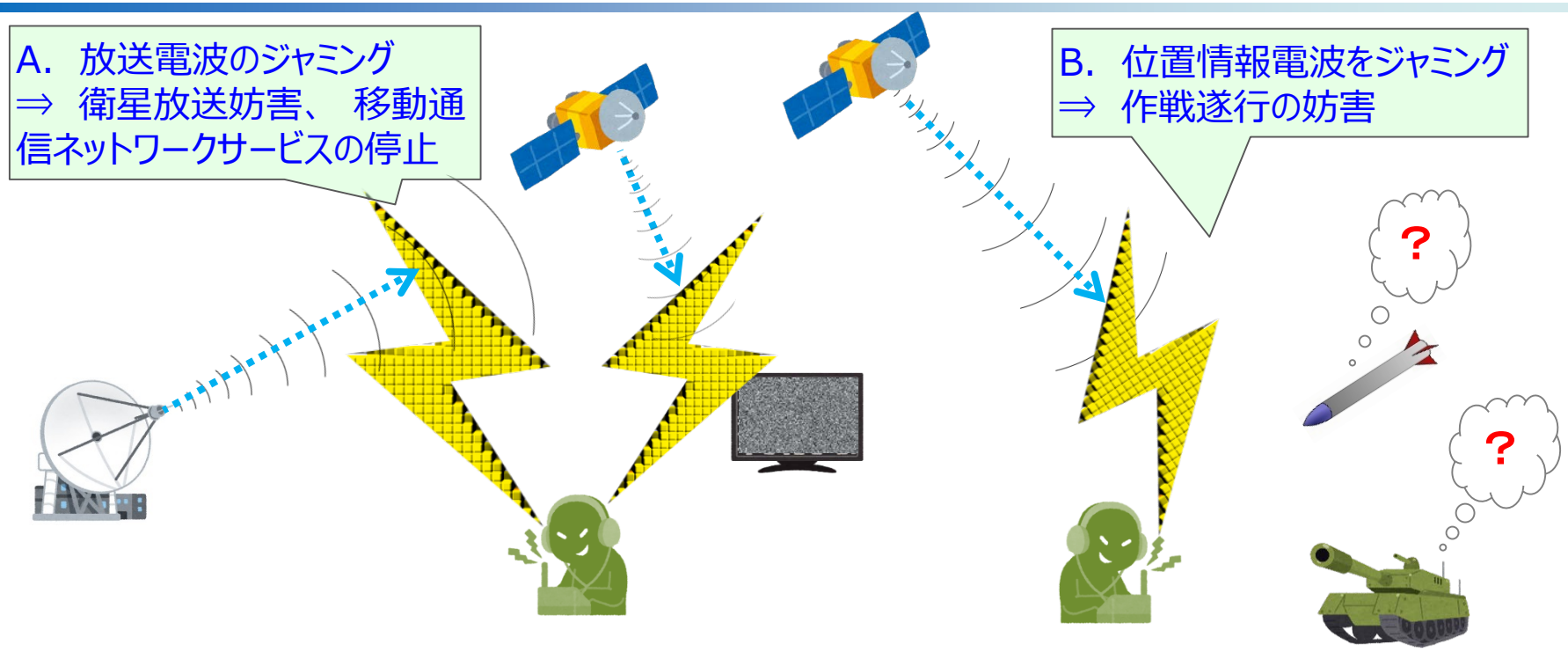
大きく3つの脅威にわけて分析

脅威 Ⅰ：ジャミング（電波やレーザ光の照射）

脅威 Ⅱ ：サイバー攻撃

脅威 Ⅲ ：盗聴、改竄、制御の乗っ取り

脅威Ⅰ：ジャミング



2003年～ イラン（衛星放送のジャミング）

イギリス人権団体のイラン向け衛星放送電波をイラン系企業がジャミング。

この放送に使われるカナダの静止衛星Telster 12は、2003年にキューバから、これが止んだ後は2005～2006年にリビアから、その後はイランからの妨害電波を受けている。

2003年 イラク（GPSのジャミング）

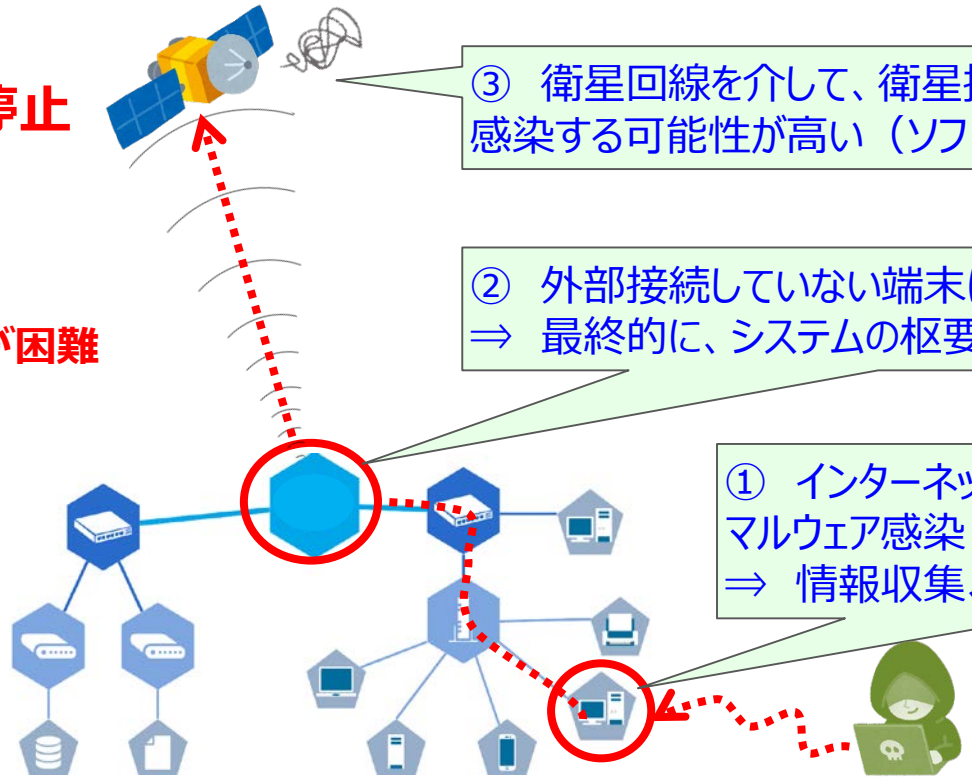
米軍が、イラク軍の対誘導兵器用GPS信号ジャミング装置６台を破壊。

2003年のイラク戦争中、このような装置によりGPS信号のジャミング事例多数。

脅威Ⅱ：サイバー攻撃（地上網からの侵入事例）

衛星サービスの停止

衛星回線では
攻撃場所の特定が困難



③ 衛星回線を介して、衛星搭載コンピュータも感染する可能性が高い（ソフト更新時など）

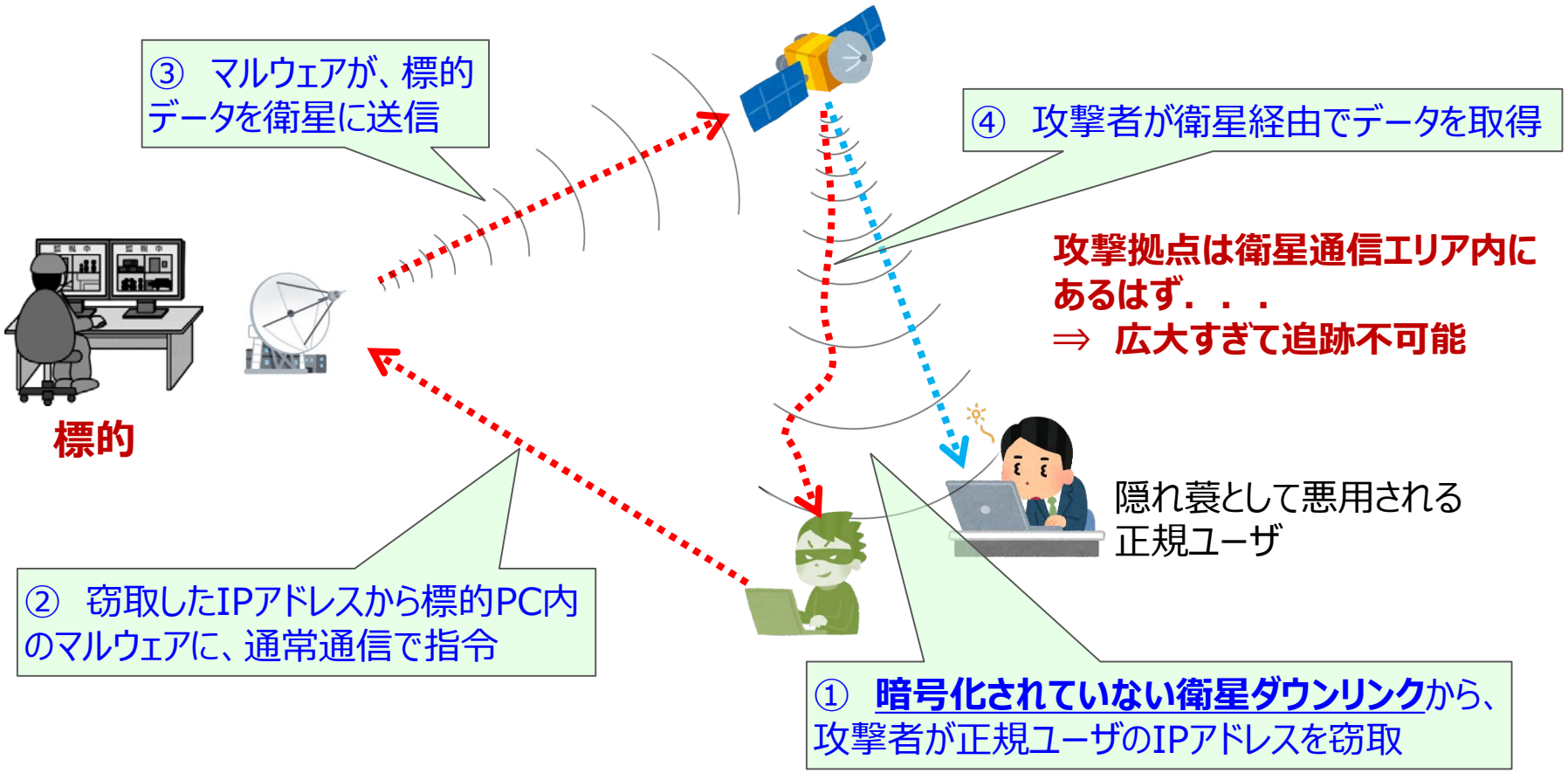
② 外部接続していない端末にもマルウェア感染が拡大
⇒ 最終的に、システムの枢要部にも感染

① インターネット経由で脆弱な端末を攻撃、マルウェア感染
⇒ 情報収集、外部操作

2014年 アメリカ（インターネットからの不正アクセス）

・アメリカ海洋大気庁(NOAA)の気象観測ネットワークが、中国系と思われるハッカーによりハッキングされ、一時閲覧不能になった。
・どのようなデータが盗まれたかは明かされていないが、NOAAの衛星から得られる気象データはハリケーンの予測などに用いられるほか各国にも配信される重要な情報を含む。

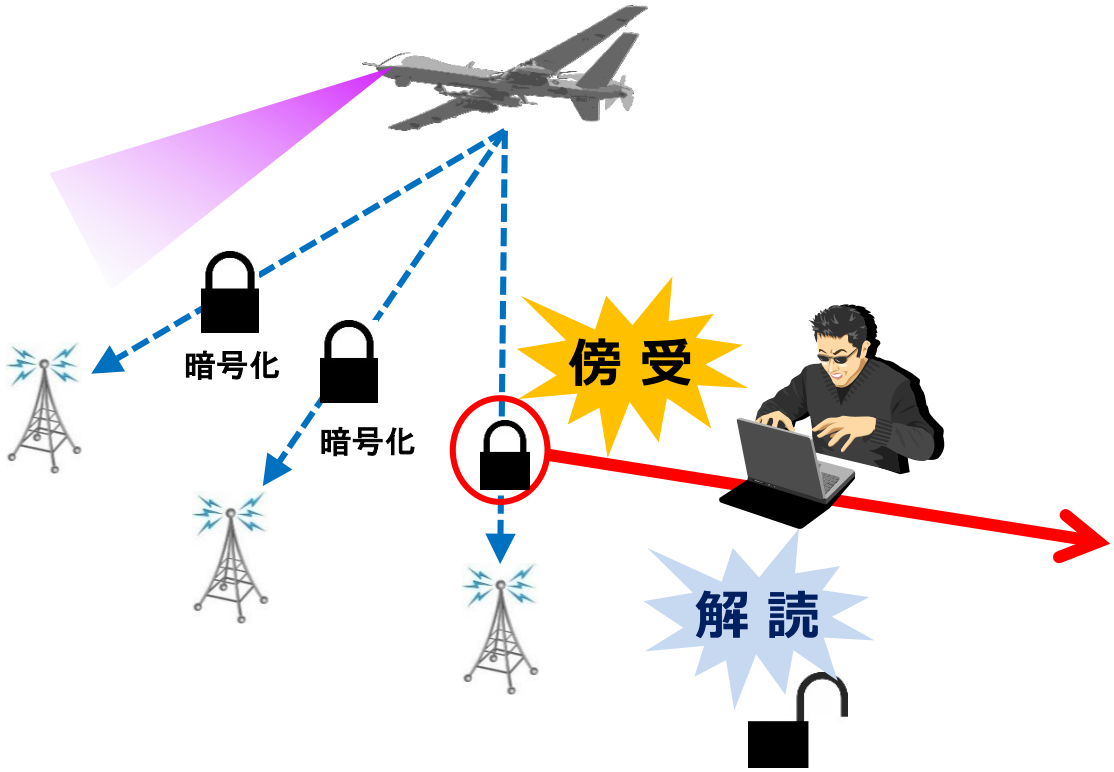
脅威Ⅱ：サイバー攻撃(衛星通信の悪用)



2015年～ ロシア（大規模スパイ活動）

・ロシア関係とみられるサイバースパイ集団 **Turla（トゥーラ）** によるサイバー攻撃と、その拠点隠ぺいに衛星ネットワークを悪用。
・45か国以上の政府機関、軍、教育研究機関、製薬企業などでマルウェア感染、そのネットワークに侵入、スパイ活動。

脅威 Ⅲ：盗聴、改竄、制御の乗っ取り（盗聴）

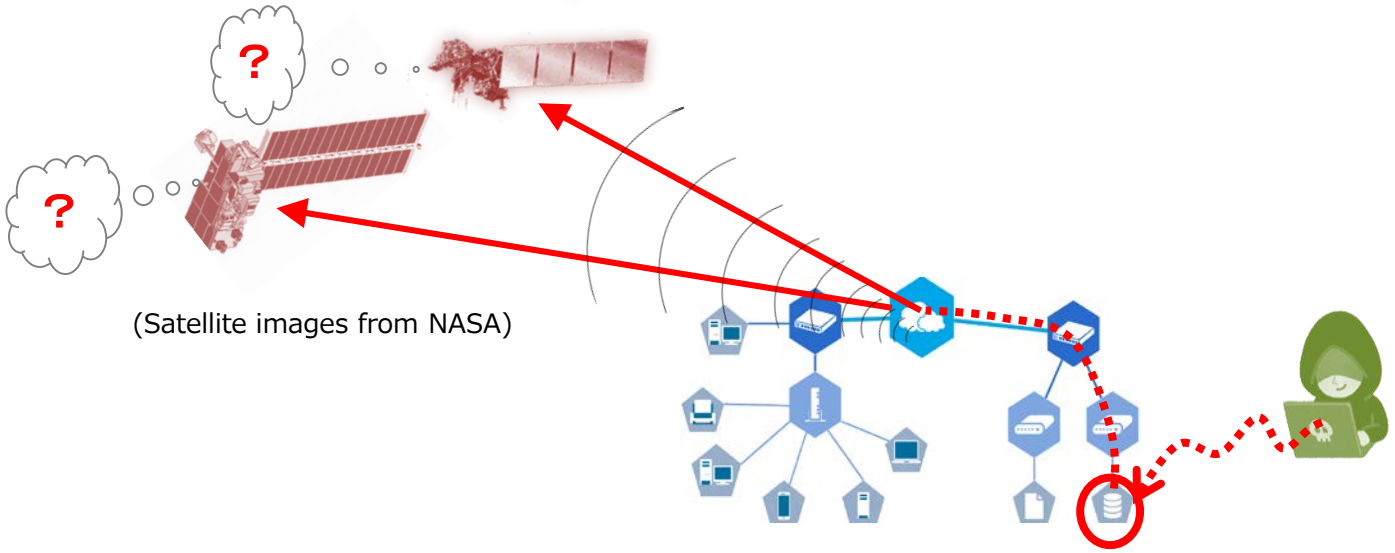


シリア軍無人機撮影とされる映像の傍受画像
（シリア西部　2012年3月11日）

1998~2016年　イギリス、アメリカ（諜報機関による盗聴）

イギリス通信本部（GCHQ)とアメリカ国家安全保障局（NSA）がキプロス島に傍受施設を建設し、中東・地中海地域の無人航空機の通信を傍受し、高性能コンピュータで解読。

脅威 Ⅲ：盗聴、改竄、制御の乗っ取り（乗っ取り）



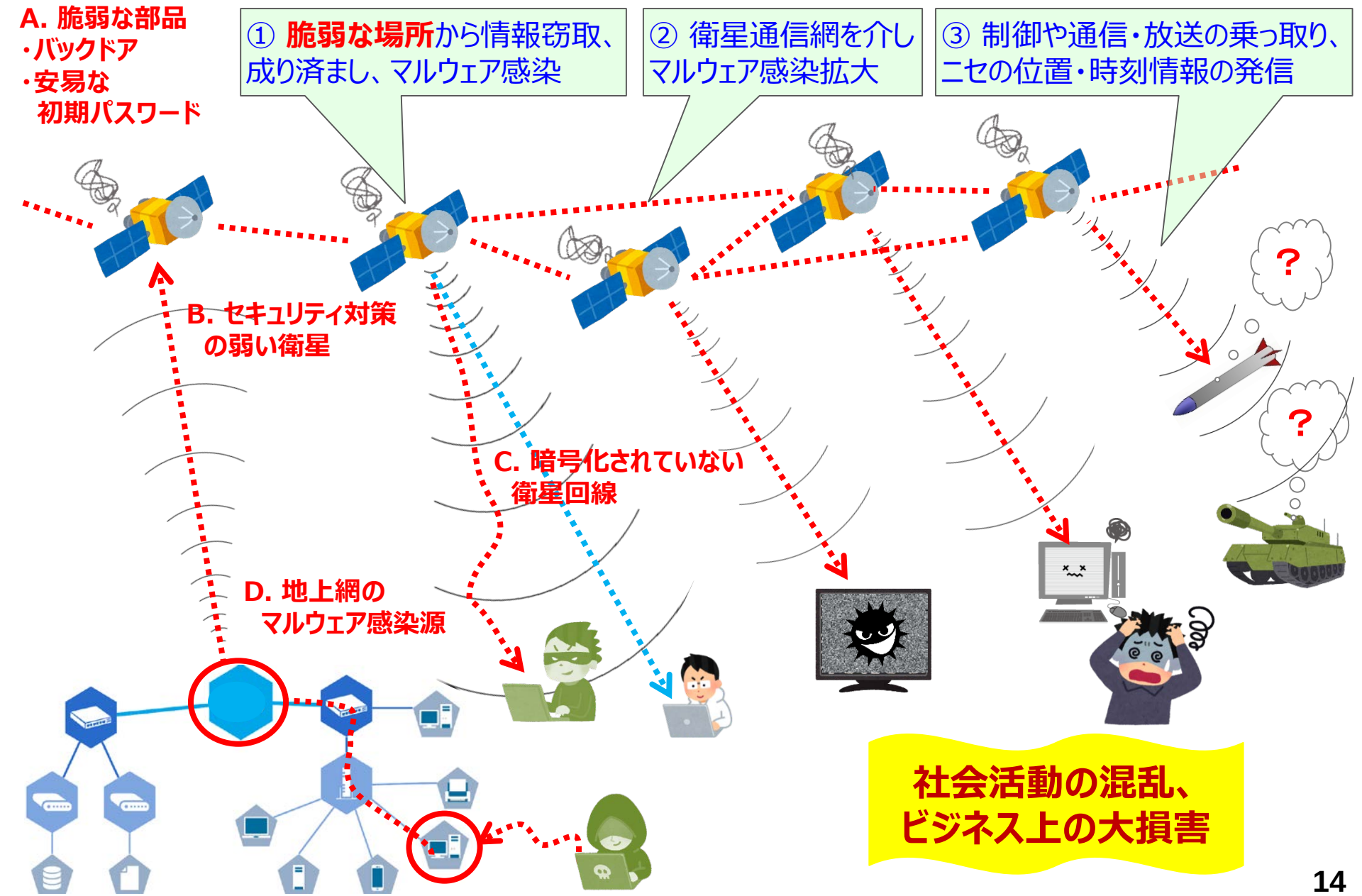
(Satellite images from NASA)

2007年、2008年　アメリカ（衛星制御の乗っ取り）

・NASAの地球観測衛星2機（Landsat-7、Terra AM-1）が、中国系と思われる
　ハッカー集団から計4回以上攻撃を受け、数分の間、制御不能となった。
・ノルウェーのスヴァールバル島にある衛星地上局に、インターネット回線から侵入したとみられる。

判明している制御不能時間；
　Landsat-7　：計12分間以上（ 2007年10月と、008年7月）
　Terra AM-1：2分間以上（2008年6月20日）
　　9分間以上（ 2008年10月22日）

衛星コンステレーション全体に被害が拡大



ジャミングへの対策

基本的にコストを掛けて、冗長性を導入するしかない

『逃げる』

① 複数の周波数チャネルを用意して適宜切り替える

② 通信経路の切り替え（他の衛星を経由等）、通信時刻の変更

③ 複数のGPSシステムから信号を受信 (Backup)

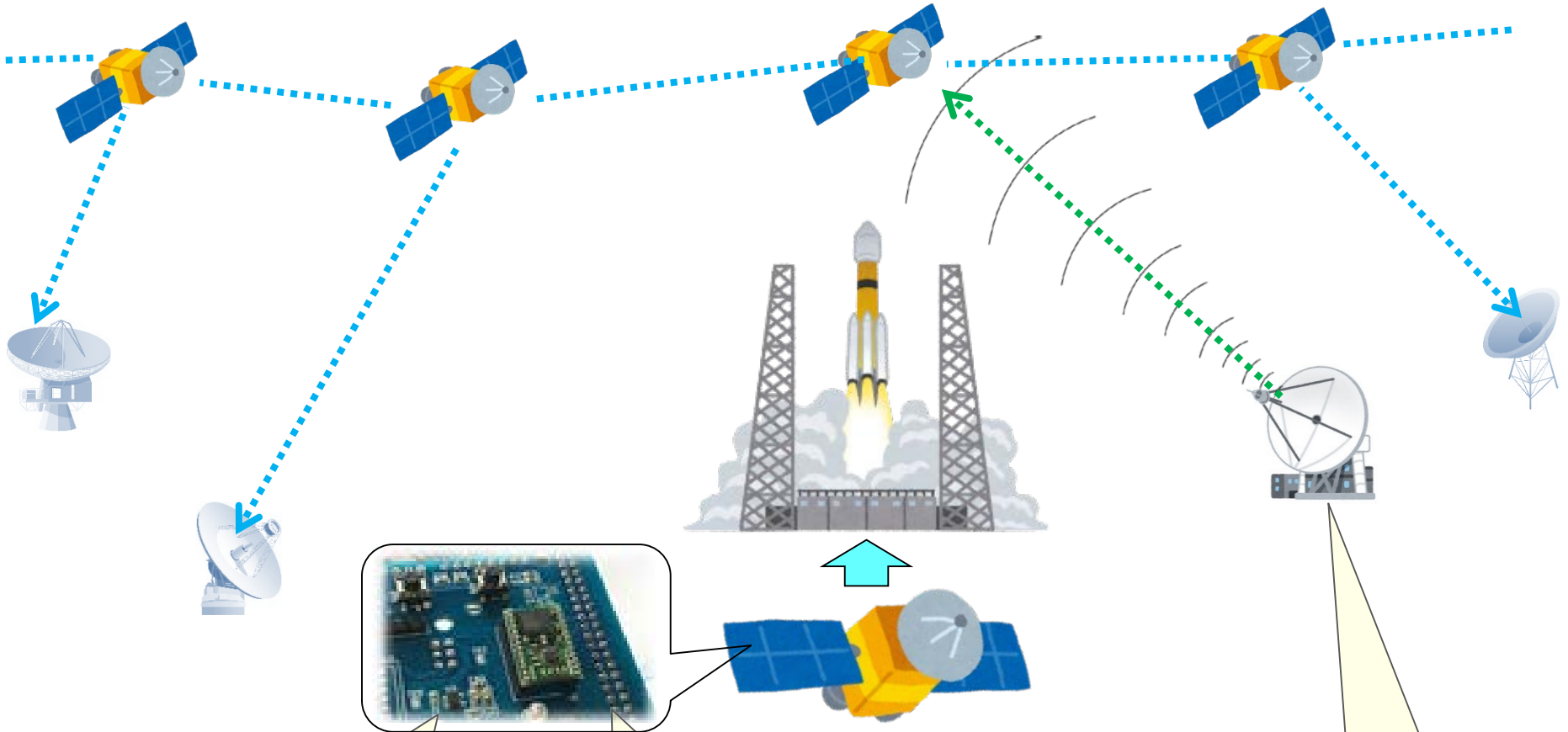
『耐える』

④ 特殊な相関構造を変調信号に埋め込み、ジャミングを排除 (Filtering)

⑤ 独自の原子時計やポジショニング機構を衛星に搭載

⇒ジャミング発生下でも自立的に時空制御を維持

サイバー攻撃への対策（初期対策）



① 機器サプライチェーンの管理

・工場出荷時の脆弱性検証
バックドア検証法の開発
・IoT機器のセキュリティ検証
リストを導入、利用を推奨

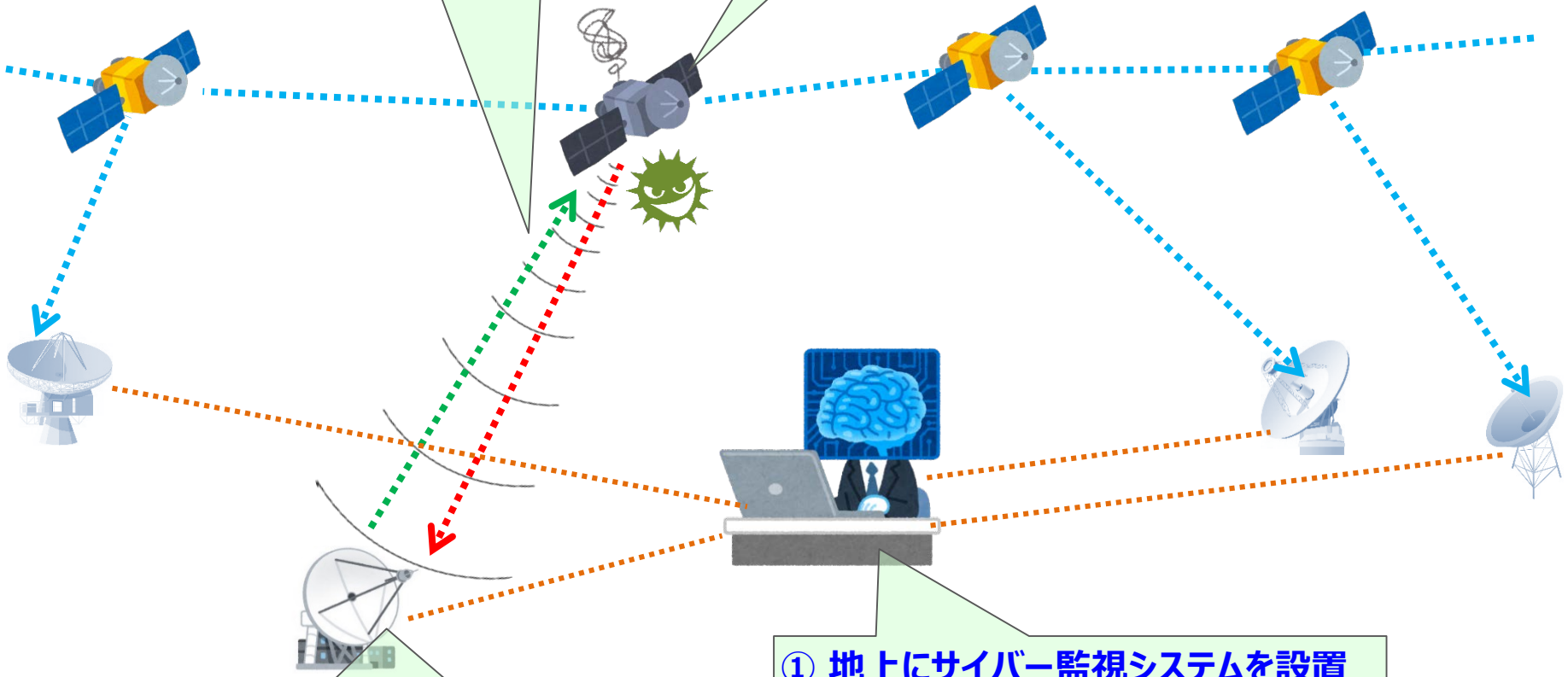
② 機器の初期パスワードの高セキュア化

・出荷時の初期パスワードのままでは起動しない仕組みを入れる

③ 打上げ後、安全に機器を起動し管理

・地上局から秘匿回線により
更新パスワードを送信
・定期的な機器認証

サイバー攻撃への対策（マルウェアの監視と駆除）



③ マルウェアの駆除とシステム修復作業

秘匿回線経由で初期化、
修復に必要な情報を送信

④修復不能なら衛星廃棄

遠隔の修復作業が困難と判断された場合、
廃棄 ⇒ デブリ化 ⇒ デブリ除去対策へ移行

① 地上にサイバー監視システムを設置

通信パケットのメタデータを収集
⇒AIで通信トラフィックを監視
⇒マルウェア感染をいち早く検知

② 感染検知後、通信を即時遮断

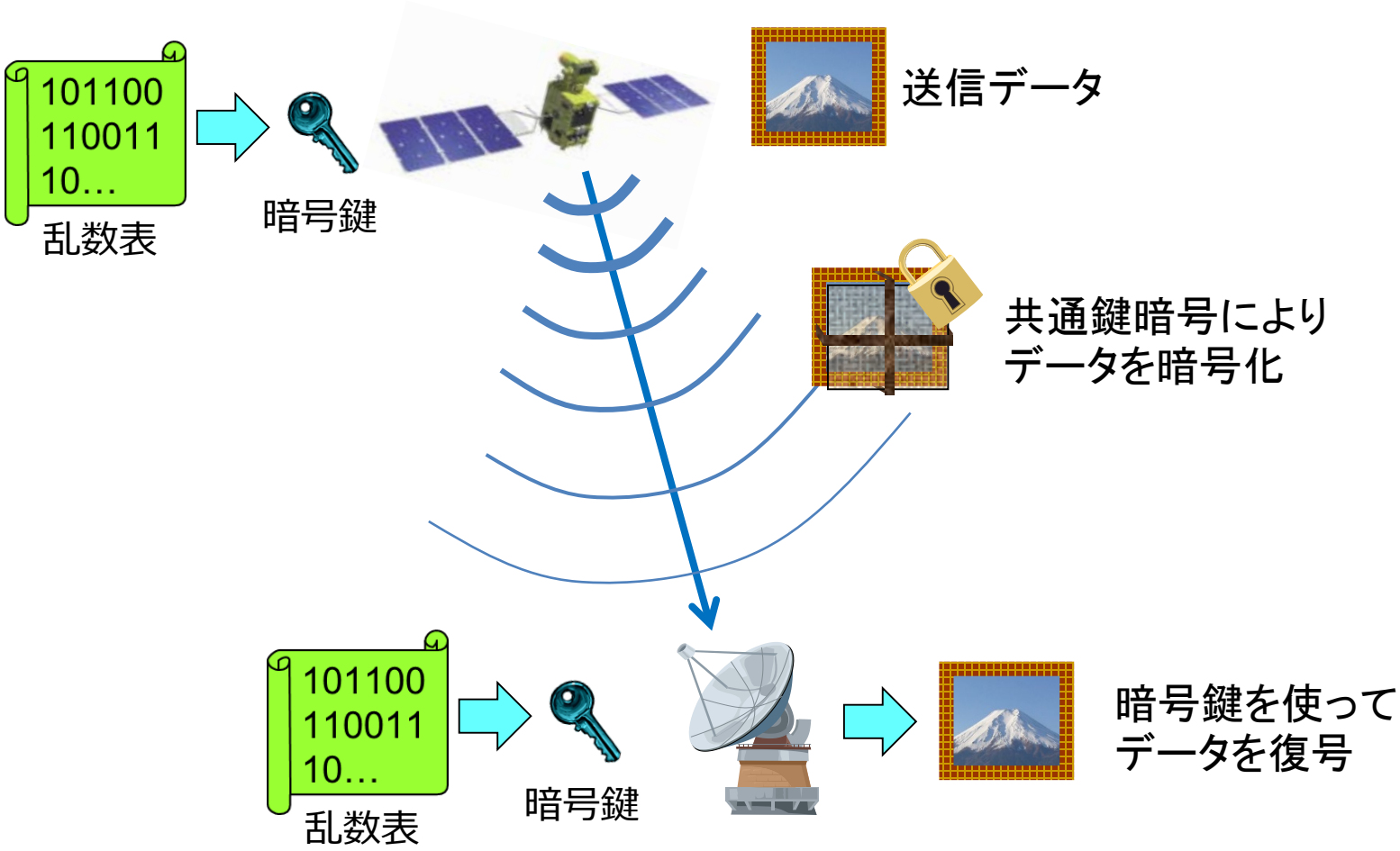
秘匿回線で地上局から即座に衛星通信
停止を指令、感染拡大を未然に防止

盗聴、改竄、制御の乗っ取りへの対策：暗号化

対策その１

現有技術活用

地上局と対になる乱数表を衛星のメモリに保存して打ち上げ、その乱数表を種鍵にして共通鍵暗号によりデータを暗号化（1対1の暗号化通信）



問題点：保存できる乱数表のメモリサイズが有限

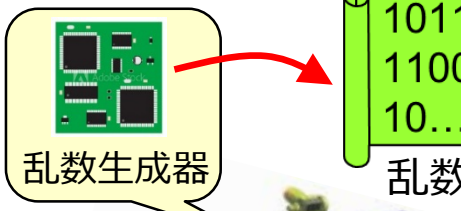
盗聴、改竄、制御の乗っ取りへの対策：暗号化

対策その２

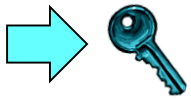
短期的開発目標

衛星光通信の利用を拡大する（すでに実用化は始まっている）

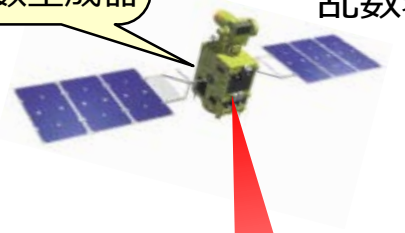
・ライセンスフリーの広い波長帯で
　大容量通信が可能
・レーザー光のビームは極めて細く、
　電波よりはるかに**傍受されにくい**



乱数表



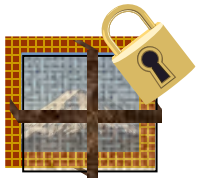
暗号鍵



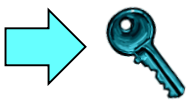
レーザー光

さらに

・衛星に乱数生成器を搭載し**常時、真性乱数を生成**
・光通信の際に、真性乱数も地上局へ送信
・共有した真性乱数を暗号鍵として通信を暗号化



乱数表



暗号鍵

問題点：依然として1対1の暗号通信

盗聴、改竄、制御の乗っ取りへの対策：暗号化

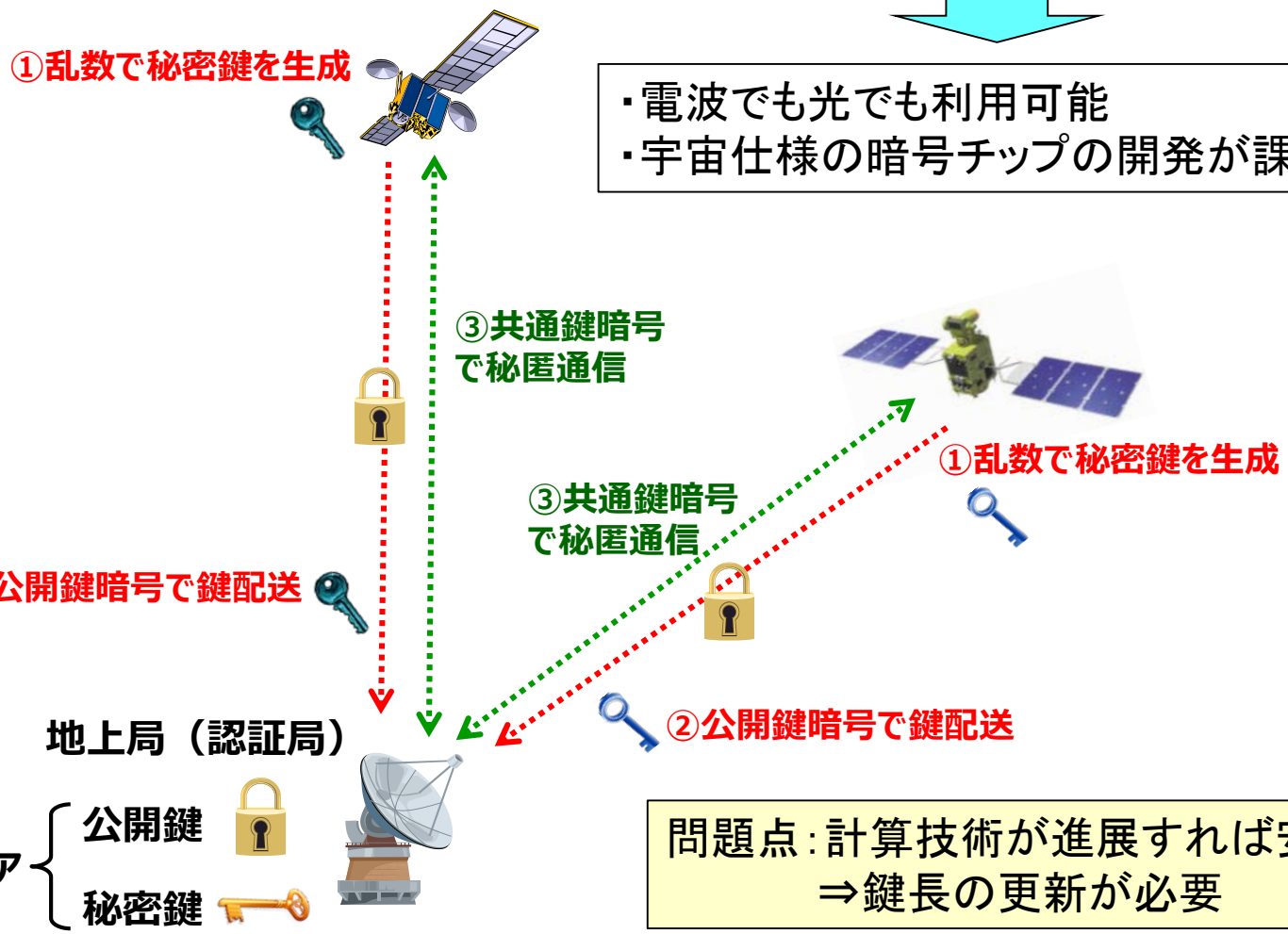
対策その３

中期的開発目標

地上インターネットで使われている暗号技術を衛星通信網に実装

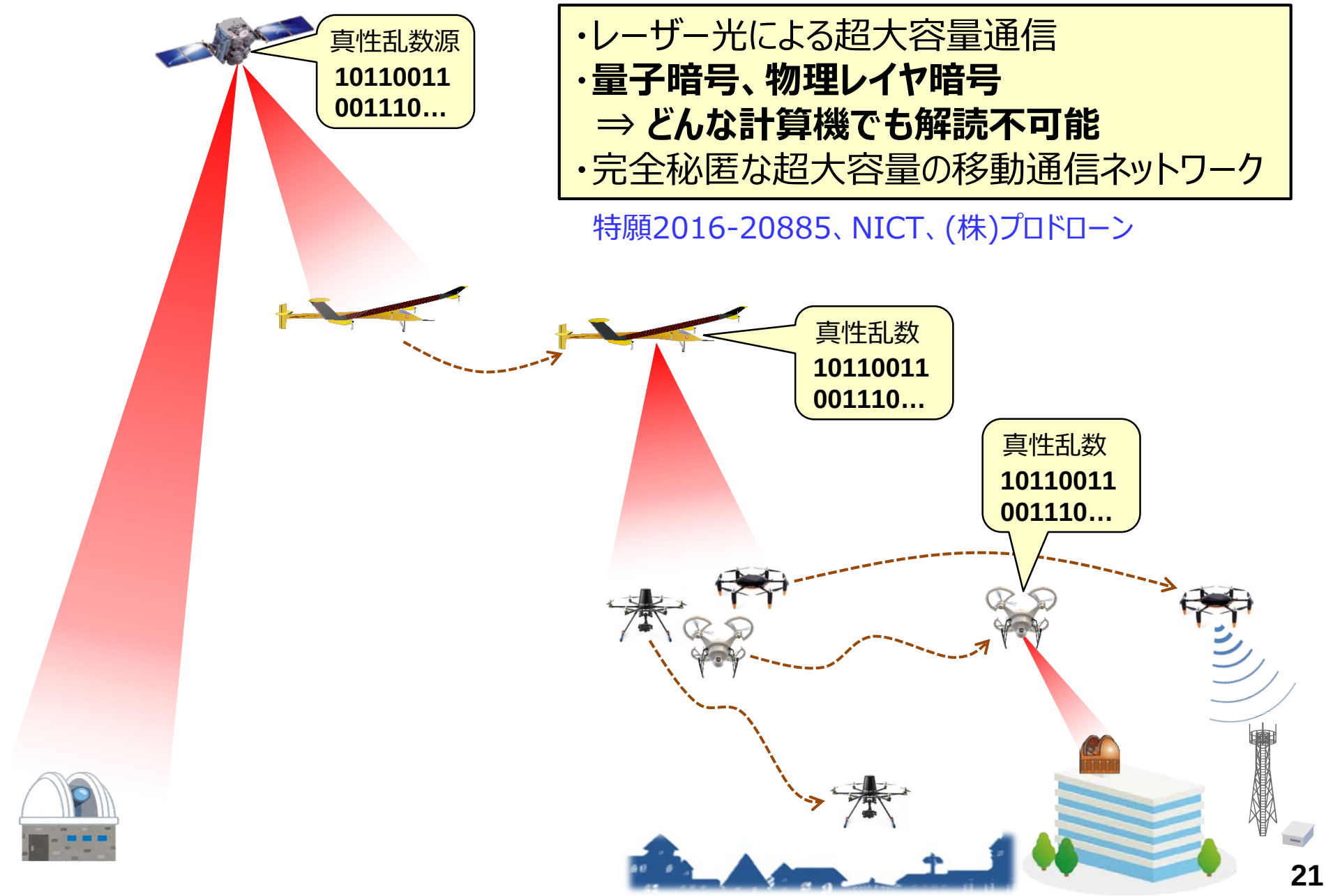
・公開鍵暗号による鍵配送（1対多、多対1）
・共通鍵暗号による通信の暗号化

・電波でも光でも利用可能
・宇宙仕様の暗号チップの開発が課題



問題点：計算技術が進展すれば安全性は危殆化
⇒鍵長の更新が必要

長期的開発目標：超大容量･超高秘匿グローバルネットワーク

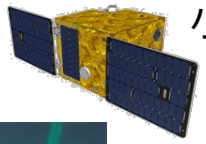


・レーザー光による超大容量通信
・**量子暗号、物理レイヤ暗号**
　⇒ **どんな計算機でも解読不可能**
・完全秘匿な超大容量の移動通信ネットワーク

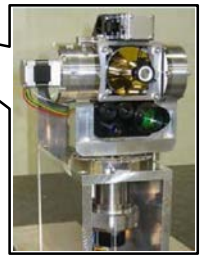
特願2016-20885、NICT、(株)プロドローン

CG動画
『高秘匿通信ネットワーク』

NICTにおける研究開発



小型衛星「SOCRATES」(50kg)　2014年5月14日打ち上げ



NICTが小型光送信機
SOTAを開発 (5.9kg)

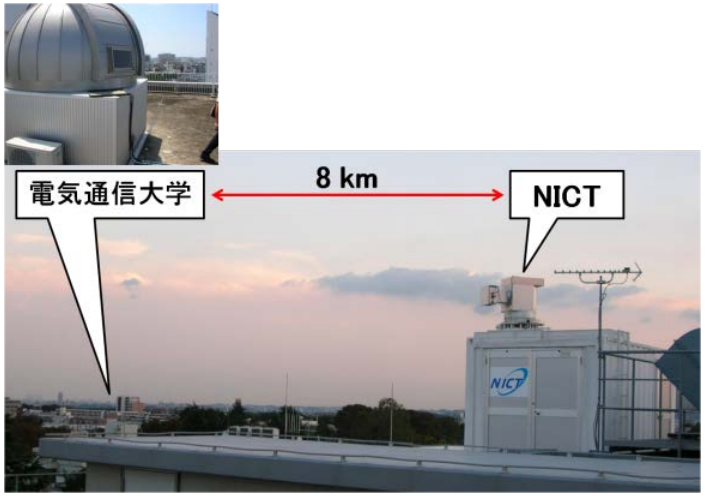
・2015年、低軌道600kmと地上間で10Mbps
でのセンサー画像伝送に成功

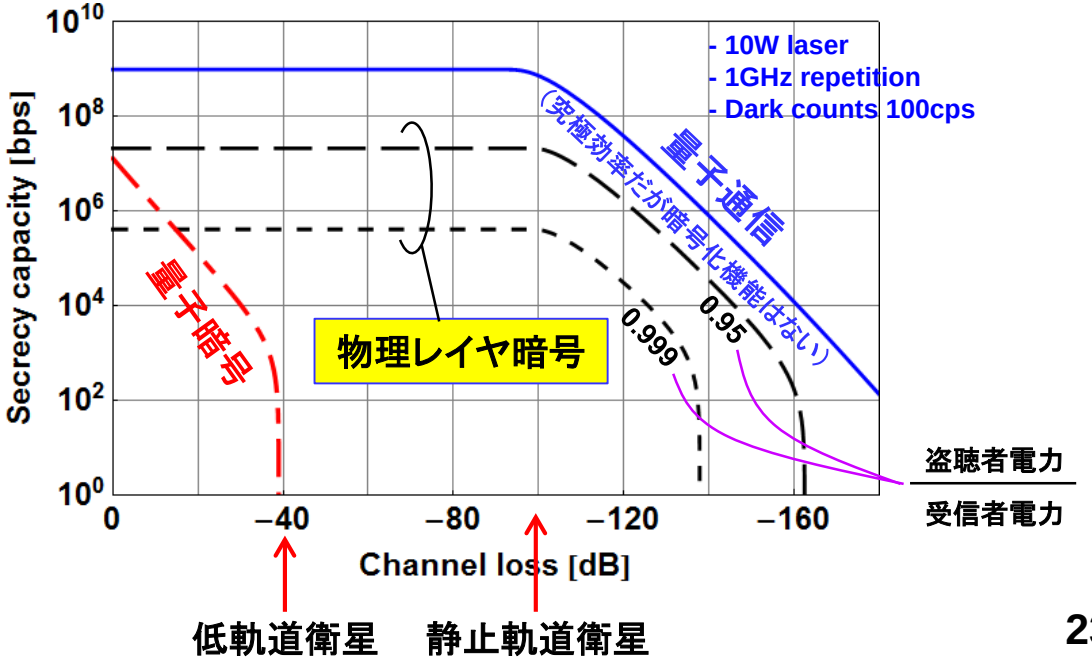
http://www.nict.go.jp/press/2015/06/03-2.html
A. C.-Casado, et al., Opt. Express. 24(11), 12254 (2016).

・2016年、量子暗号の予備実験

Paper in preparation

光空間テストベッドで量子暗号、物理レイヤ暗号の研究開発、技術試験衛星の設計

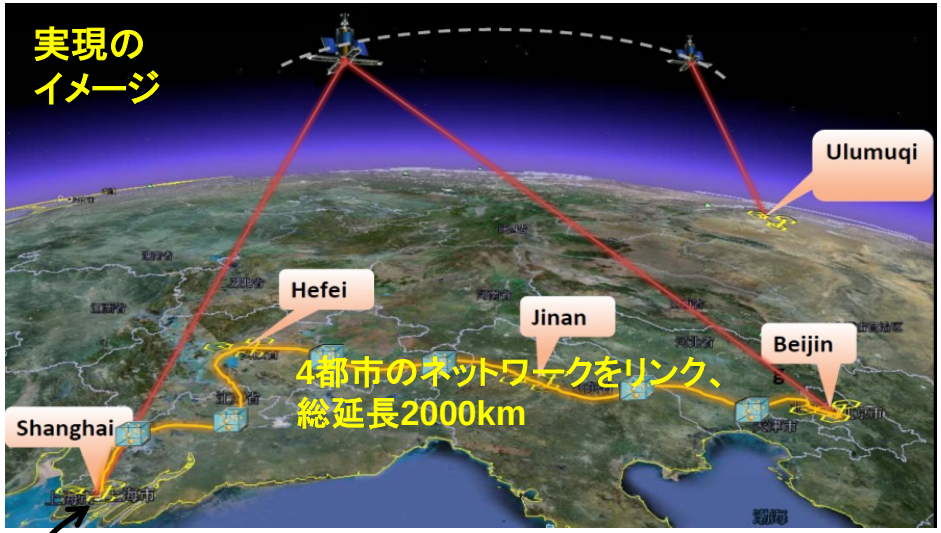




録画映像
『ドローン通信』

研究開発動向：中国

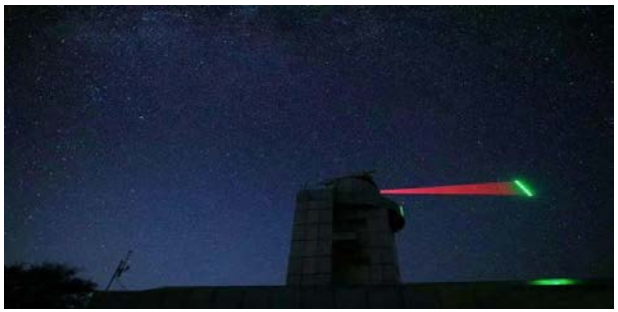
- 世界最大の量子暗号ネットワークを構築：北京－上海間2000kmのバックボーン
- 量子科学技術衛星を打ち上げ（2016年8月）
- 次の量子暗号衛星の打ち上げ計画もあり



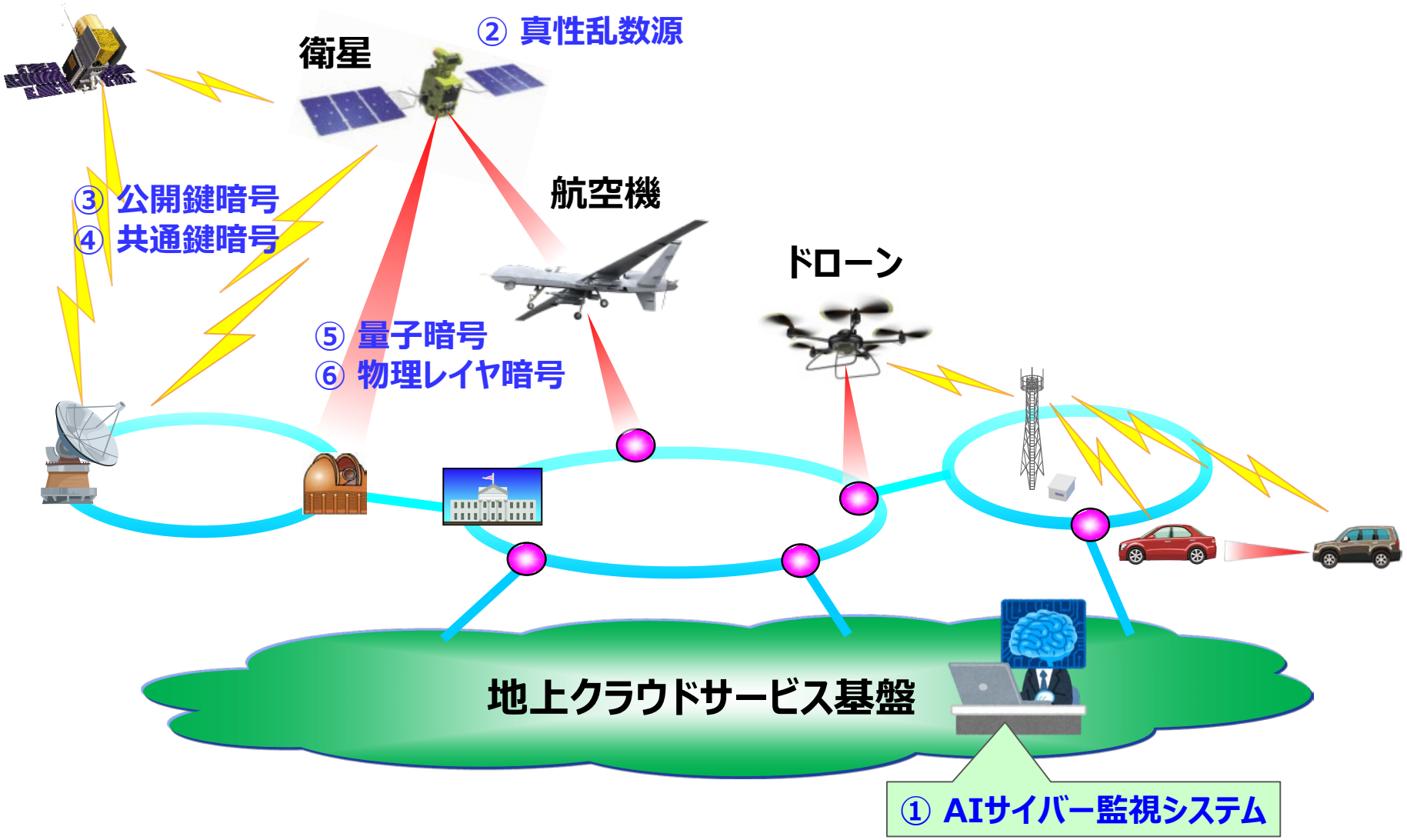
50ノード級の都市圏量子暗号ネットワーク

Qiang Zhang氏 (中国科学技術大学) のご好意による

量子科学技術衛星 600kg



セキュア移動通信ネットワークの将来像



まとめ

宇宙×ICTが進歩するほど、**リスクと脅威、被害規模**が増加する

宇宙×ICTによるイノベーションの実現には、安心・安全対策への取り組みが必須

（１）物理的脅威

・デブリ化防止機能の実装（位置情報発信機能、軌道変更機能）
・打上げ軌道調整（衛星ベンダーの自主的連携、国際的取り決め）

（２）情報セキュリティ脅威

Ⅰ ジャミング対策
・複数の通信回線、GPSシステムを利用し冗長化
Ⅱ サイバー攻撃対策
・機器サプライチェーンの管理
・衛星通信トラフィックを地上局で監視、AIでマルウェアの検知、駆除
Ⅲ盗聴、改竄、乗っ取り対策
・乱数チップと暗号化チップを衛星搭載（公開鍵暗号、共通鍵暗号）
・レーザー光通信、量子暗号、物理レイヤ暗号
⇒ 完全秘匿な超大容量の移動通信ネットワーク

競争力のあるビジネス展開、究極の超大容量・超高秘匿グローバルネットワーク

Thank you for your attention

補足資料

物理的脅威の事例と対策

2009年、米国・イリジウム衛星とロシア・コスモス衛星が低軌道上で衝突、最初にして最大量のデブリを発生

平成21年:米国衛星と寿命を終えたロシア衛星が衝突

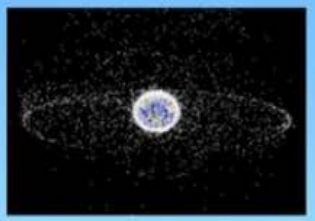
米国小型実証衛星

キラー衛星

接近して妨害・攻撃・捕獲等

スペースデブリ

高速で周回しており、衝突により衛星損傷



デブリの分布状況

米国
平成17年:他衛星に接近・撮像可能な小型実証衛星打上げ
中国
平成22年:衛星同士の接近実験

レーザー照射

衛星攻撃ミサイル（地上／空中発射式）

電磁パルス攻撃を含む

通信妨害

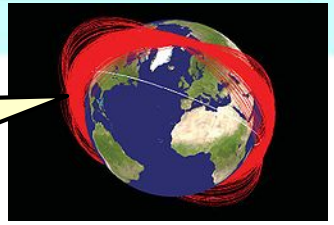
ロシア製GPSジャマー

ロシア
2000年代:GPSジャマーを世界中で販売
中国
平成20年:米国地球観測衛星に通信妨害の疑い

米国
平成 9年:レーザー照射に対する衛星脆弱性評価試験
中国
平成18年:米国衛星にレーザー照射の疑い

2007年、中国が弾道ミサイルで高度850kmの軌道の老朽化した気象衛星を破壊

2011年、破片がISSと6.1kmまで接近



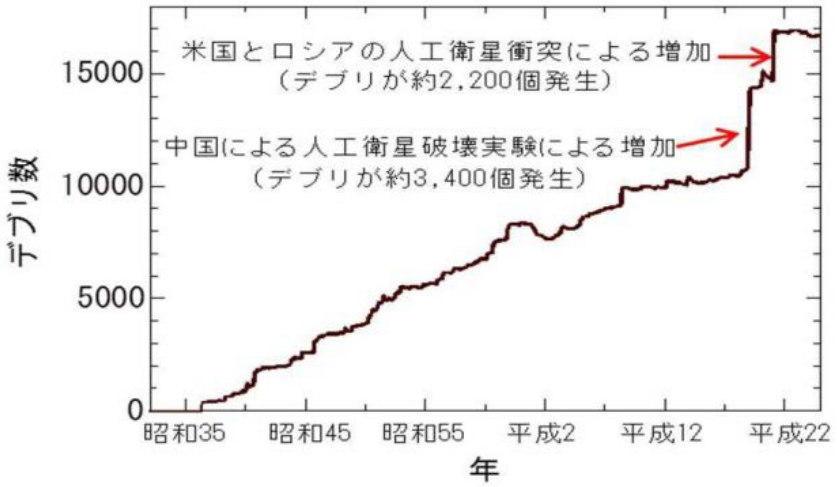
科学技術・学術審議会　研究計画・評価分科会　宇宙開発地用部会
ISS・国際宇宙探査小委員会（第8回）、資料8-1「防衛省における宇宙開発利用の取り組みについて（平成26年10月17日　防衛省）」から引用

問題点と対策

問題点

・一旦生成されたデブリは半永久的に周回
⇒遠い未来までリスクとして残り続ける
・将来、衛星数が爆発的に増加
⇒1回の衝突から雪崩的にデブリが大量発生

スペースデブリの増加の推移
（NASA公表資料をもとに防衛省作成）



対策

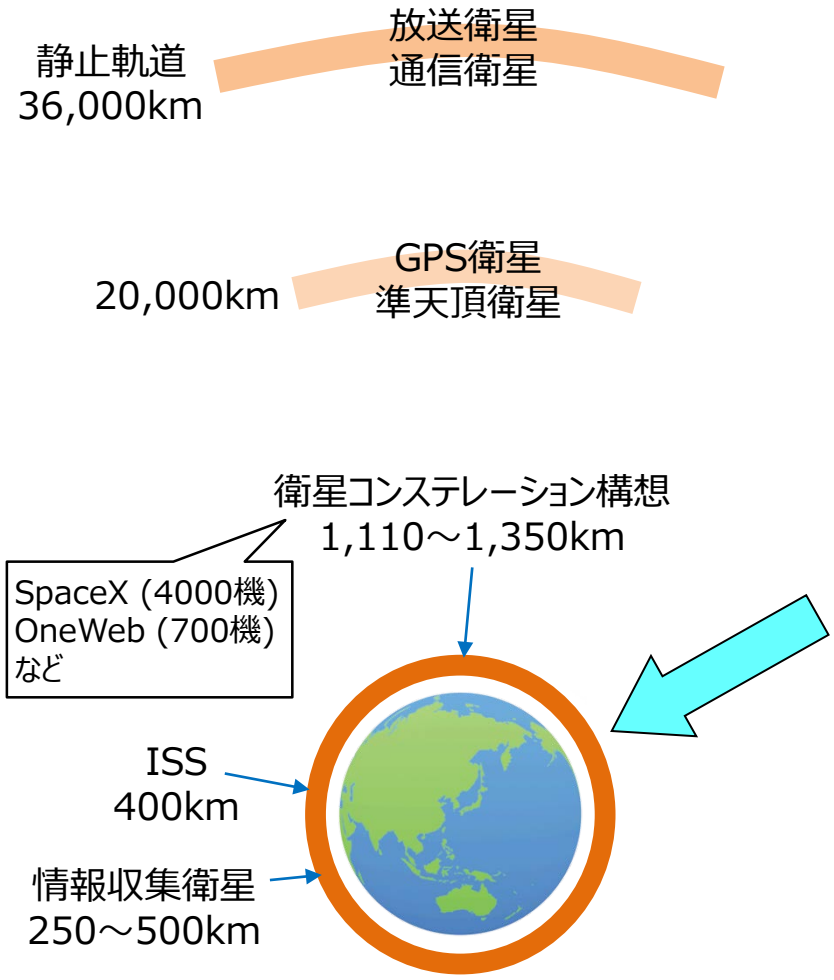
・デブリの発生禁止ルール
2007年、国連宇宙空間平和利用委員会で「宇宙デブリ低減ガイドライン」採択（罰則なし）

・デブリ発見・回避のための体制作り
・宇宙状況監視に関する日米協力(2013年以降、相互に情報提供)
・米国：宇宙監視ネットワークが、地上25カ所、衛星1機（高度約900km）から、直径10cm以上のものを監視
・日本：JAXAが、地上2か所（美星、上斎原：岡山県）から、直径1m以上のものを監視

・デブリ除去
・帯電・減速させ大気圏突入
・墓場軌道への移動(静止軌道の上空)
・高強度レーザにより溶かす

⇒ 実用化は今後の課題 ⇒ 稼働中の衛星除去も可能なため、悪意のない透明性の高い実施体制が必要

衛星の所有者、利用者側の対策（案）



・利益第一主義は、脆弱性を助長する
・安全対策を伴った成長戦略を

1．デブリ化防止機能の実装

1）衛星機能停止後も位置情報を発信し続ける機能
2）軌道変更に必要な燃料の保持
⇔衛星寿命低下とのトレードオフ

2．打上げ軌道調整

1）衛星ベンダー(産業界)が自主的に連携して、打上げ軌道を事前に調整
2）我が国では内閣府が中心になって法制化を推進中
3）国連では条約化を各国で折衝中