2017年6月9日(金)

資料１

衛星通信のセキュリティ強化に向けた量子暗号技術の研究開発 ～現状と展望～

参考資料
総務省、宇宙xICTに関する懇談会 第5回、2017年2月22日

http://www.soumu.go.jp/main_sosiki/kenkyu/space-times-ICT/index.html

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

衛星通信におけるセキュリティ脅威

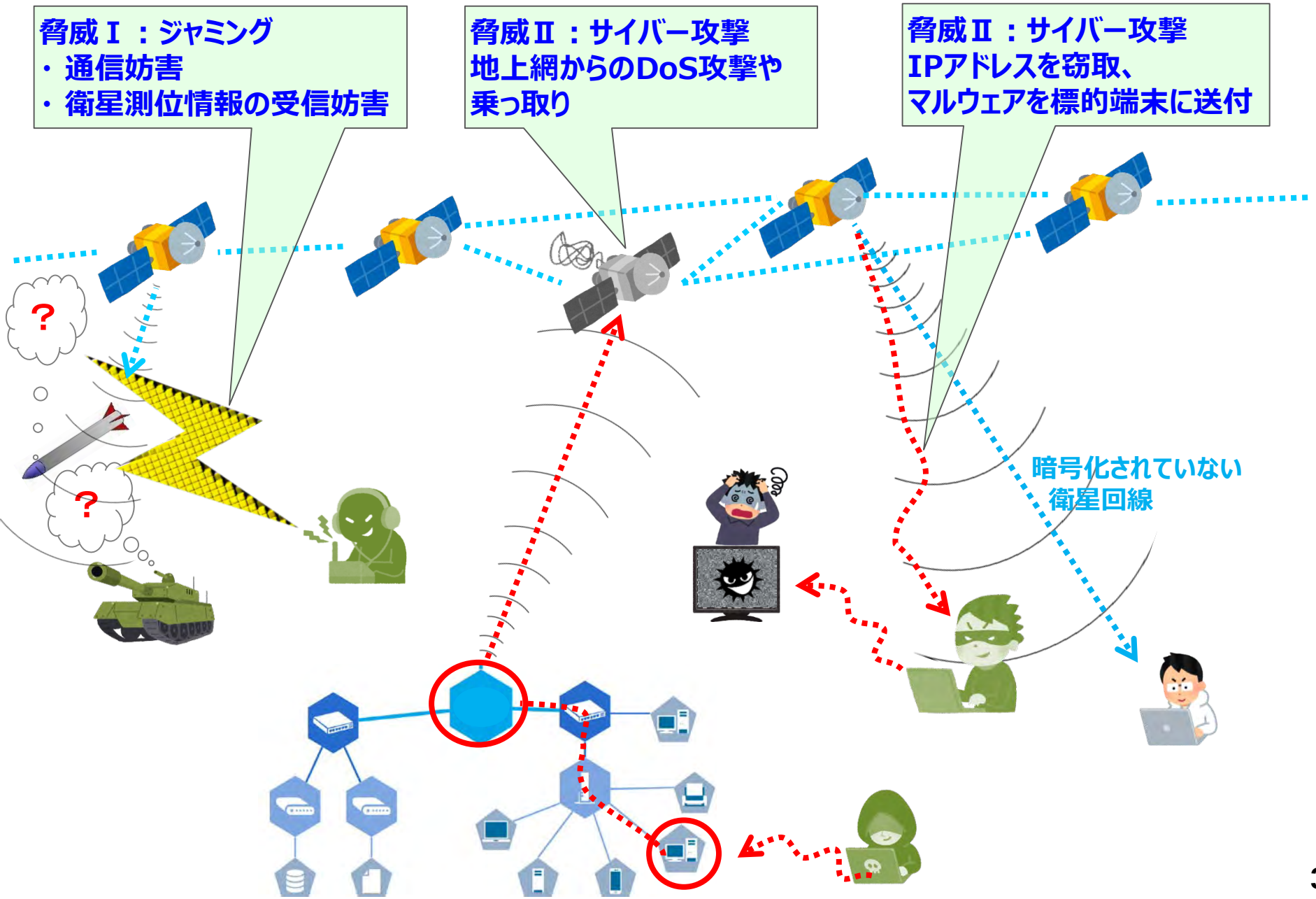
大きく3つの脅威

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（マルウェア送付、DoS攻撃など）

脅威 Ⅲ：盗聴、改竄

脅威Ⅰ及びⅡ


脅威Ⅰ：ジャミング
・通信妨害
・衛星測位情報の受信妨害
脅威Ⅱ：サイバー攻撃
地上網からのDoS攻撃や
乗っ取り
脅威Ⅱ：サイバー攻撃
IPアドレスを窃取、
マルウェアを標的端末に送付
暗号化されていない
衛星回線

脅威Ⅲ（盗聴、改竄）


脅威Ⅲ：盗聴
リモセン画像の解読
脅威Ⅲ：改竄
衛星測位情報の改竄（衛星、地上）
偽の信号
暗号化
傍 受
解 読
不正に航路を変更
偽の信号

・日々進化し多様化するサイバー攻撃や盗聴・改竄を一括して防ぐ万能策は無い
（個別の対策例については、補足資料１を参照）
・衛星上で実装できるセキュリティ対策には限界がある

・致命的な被害を防ぐための『最低限のセキュリティ』にフォーカス
・可能な限りの冗長系を組み込む（コスト vs 効果のトレードオフ）
・現在予見できない攻撃にも対処できる技術を取り入れる
・将来、共通プラットフォーム化できる汎用的な対策を考え抜く

トラストアンカー、トラストチェーンの明確なシステムは、ハッカーにとって攻撃しづらい！

・衛星通信装置を『オープン系』と『クローズ系』から構成
・2つの系を統合運用するための適切な『責任分界点』を設ける
・用途に応じて、2つの系を使い分ける
・クローズ系の中に、危殆化しない暗号技術、及び汎用的なインタフェースを実装
⇒これをコアとして**トラストアンカー、トラストチェーン**を構築