SPACE DATA LINK SECURITY PROTOCOL

「宇宙データリンクセキュリティプロトコル」

Blue Book
CCSDS 355.0-B-1
発行月：2015年9月
ISO　ISO21324

【概要】

本推奨規格は、データリンク層におけるセキュリティ方式を規定するものである。本推奨規格では、スペースリンクを伝送するフレーム（データ）の認証や守秘性確保のためのフレーム形式（セキュリティヘッダ、セキュリティトレーラ）を定義・推奨しており、データリンク層の3つのCCSDSプロトコルであるTM（Telemetry：テレメトリ）、TC（Telecommand：テレコマンド）、AOS（Advanced Orbiting System：将来型宇宙機システム）への適用が推奨される。本推奨規格は、いかなる宇宙ミッションが採用する暗号化アルゴリズムにも干渉せず、標準的なセキュリティ方式をデータリンク層に与えることを目的としている。また、宇宙機関間における相互運用の促進のため、CCSDSのその他のプロトコル群で推奨している伝送フレーム形式や、SLE（Space Link Extension)フォワード/リターンサービスに準拠したフレーム形式を採用している。

【内容】

本セキュリティプロトコルでは、セキュリティアソシエーション（SA）（通信を始める前に、送/受信側が、暗号化方式や暗号鍵などの情報を交換・共有し、安全な通信路を確立すること）を行うことで、認証、データ完全性、リプレイプロテクション、データ機密性等が確保される。SAが形成されると、「認証」、「暗号化」、「認証された暗号化」の3つの機能の内の1つが選択され、伝送フレームのフィールドに適用される。

本書が推奨する伝送フレームは、保護するフレームデータを「セキュリティヘッダ」と「セキュリティトレーラ」が囲む構造となる。「セキュリティヘッダ」にはセキュリティパラメータインデックス（SPI）、初期化ベクトル、アンチリプレイシーケンス番号等の情報が含まれ、「セキュリティトレーラ」にはメッセージ認証符号（MAC）が含まれる。第4章には「セキュリティヘッダ」「セキュリティトレーラ」の仕様及び認証/暗号化手順が定義されている。第5章にはTM、TC、AOSの各プロトコルにセキュリティプロトコルを適用する際の注意点、フレーム形式、セキュリティプロトコルが適用可能なサービスについて述べている。第6章にはセキュリティプロトコルとして管理すべきパラメータについて述べている。

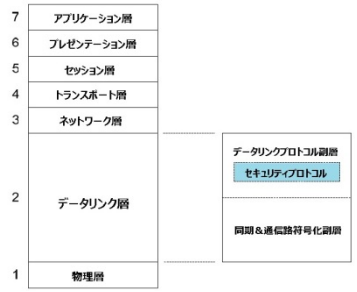

図1　OSI参照モデルにおける本セキュリティプロトコルの位置づけ

図2　セキュリティフレーム構造の比較

各国宇宙機関およびJAXAの動向

海外では、NASA（アメリカ航空宇宙局）、ESA（欧州宇宙機関）、CNES（フランス国立宇宙研究センター）、DLR（ドイツ航空宇宙センター）、CNSA（中国国家航天局）、INPE（ブラジル国立宇宙研究所）、UKSA（イギリス宇宙局）等の主な宇宙機関が本規格を採用している。JAXAでは、筑波宇宙センターと宇宙科学研究所（ISAS）が採用している。