SPACE DATA LINK SECURITY PROTOCOL – SUMMARY OF CONCEPT AND RATIONALE

「宇宙データリンクセキュリティプロトコル – コンセプトと論理的根拠の概要」

Green Book
CCSDS 350.5-G-2
発行月：2024年1月

本解説資料は、宇宙データリンクセキュリティ(SDLS)プロトコルの核となる部分や、SDLSプロトコルの拡張手順(鍵管理、SA管理、監視制御)に関するコンセプト及び論理的根拠について説明しており、推奨規格「Space Data Link Security Protocol」(CCSDS 355.0-B-2)の内容を解説している。

データリンク層に、TC（Telecommand：テレコマンド）、TM（Telemetry：テレメトリ）、AOS（Advanced Orbiting System：将来型宇宙機システム）、USLP（Unified Space Data Link Protocol：統合的宇宙データリンクプロトコル）の各サービスを適用する際には、SDLSプロトコルを使用することでデータユニットの保護が可能となる。 例えば図1に示すようなミッション制御センター－地上局－衛星間の通信においては、ミッション制御センター－衛星間でSDLSプロトコルを利用することで安全な通信を確立することが可能となる。

本文書の第3章では、セキュリティサービス(認証、データ機密性、データ完全性及びそれらの組み合わせ)の選択に対する理論的根拠を説明している。また、SDLSプロトコルで保護できる範囲(バーチャルチャネル)や、保護できない範囲(マスターチャネル)についても説明している。図2は、OSI参照モデル及びCCSDSのプロトコル階層における、SDLSプロトコルの位置づけを示しており、SDLSプロトコルがデータリンク層のTM、TC、AOS、USLPそれぞれに対してどのような機能を果たすかを説明している。

第4章では、セキュリティアソシエーション(SA)の切り替えによる暗号鍵更新を実現することで、より安全な暗号通信を確立することを説明している。そして、効率的なSDLSプロトコル運用のために、送受信者間の暗号化鍵や初期化ベクトル、シーケンスカウンタ等の同期及び管理についても説明している。また、地上局やオンボードの実装シナリオについて説明している。

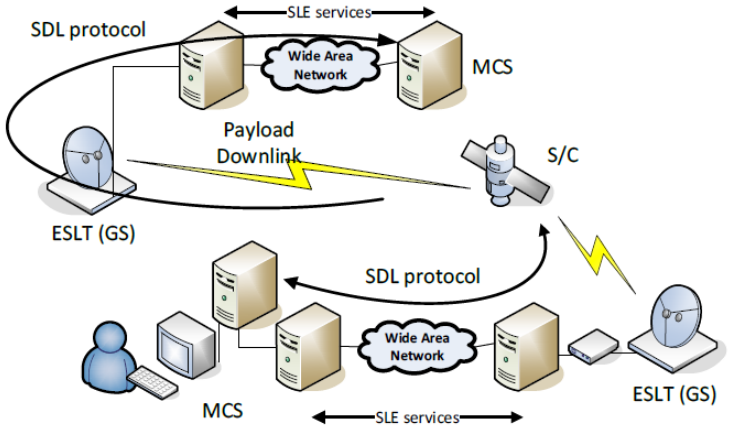

図1:ネットワークトポロジ例

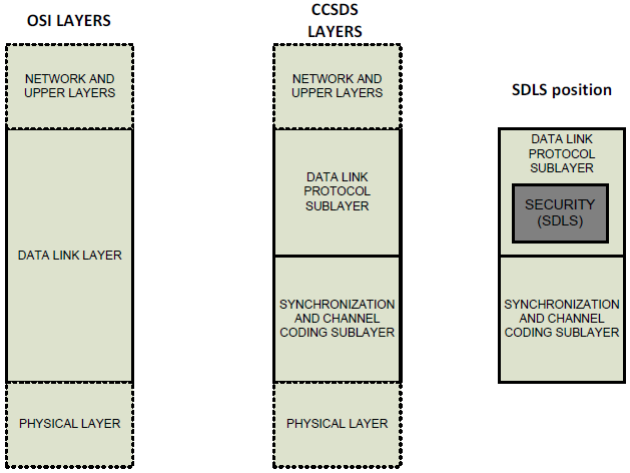

図2: OSI参照モデル及びCCSDSのプロトコル階層における SDLSプロトコルの位置づけ