

# SPACE DATA LINK SECURITY PROTOCOL EXTENDED PROCEDURES SUMMARY OF CONCEPT AND RATIONALE



## 「宇宙データリンクセキュリティプロトコル拡張手順概念の要約と根拠」

本解説資料は、推奨規格「Space Data Link Security Protocol – Extended Procedures」(CCSDS 355.1-B-1)に関連して、宇宙データリンクセキュリティ(SDLS)プロトコルの拡張手順の正当性、運用の概念および理論的根拠を示すものである。

SDLSプロトコルは、宇宙データリンク(SDL)プロトコルによって転送されるデータに対して、ユーザが選択したセキュリティサービスを実装するプロトコルであり、SDLおよびSpace Link Extension (SLE)サービスとの互換性制約を考慮して、SDLプロトコルによって転送されるサービスデータユニット(SDU)と、選択されたSDLプロトコルデータ構造を保護する。

推奨規格「Space Data Link Security Protocol – Extended Procedures (EP)」(CCSDS 355.1-B-1)は、SDLSプロトコルの実装を行うにあたり必要となる、標準化された補助的なサービスのセットを提供している。EPが提供するサービスは鍵管理、セキュリティアソシエーション(Security Association: SA)管理、およびSDLS監視と制御の3つに分類される。さらに、SDLプロトコル内でEPサービスメッセージを伝送するためのサービスインタフェースとデータ構造、並びにセキュリティユニットの状態報告メカニズムが規定されている。

(図1)

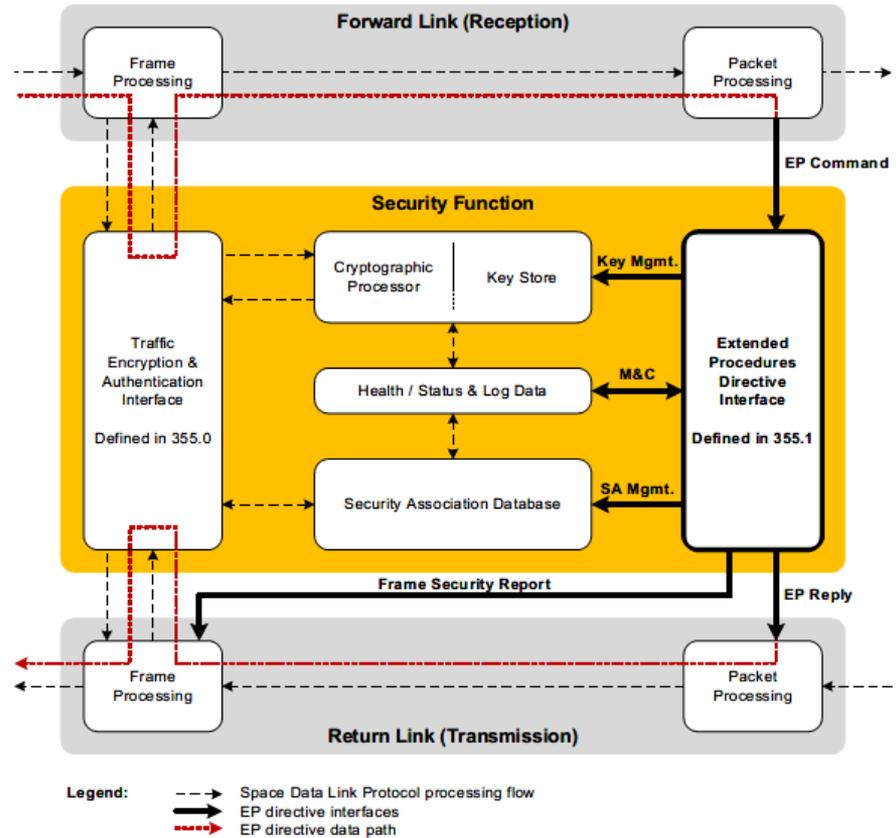


図1 SDLSプロトコル拡張手順のインタフェース