CCSDS CRYPTOGRAPHIC ALGORITHMS

「CCSDS暗号アルゴリズム」

Blue Book
CCSDS 352.0-B-1
発行月：2012年11月
ISO20215

【概要】

本推奨規格は、宇宙機関間で使用するCCSDS用セキュリティ暗号アルゴリズムを定義するものである。

【内容】

データ、音声、画像、テレメトリ、コマンド等、衛星から地上に至る宇宙ミッションで利用できる、共通鍵を用いた暗号アルゴリズムや、認証アルゴリズムを推奨しており、以下が説明されている。

- CCSDSに適用したセキュリティアルゴリズムの暗号化についての概要
- セキュリティ暗号の概要
- 共通鍵を用いたMACアルゴリズム
- 公開鍵/秘密鍵を用いた認証
- 認証アルゴリズムとして知られているAEAD（Authenticated Encryption with Associated Data）の概要
- 暗号アルゴリズムで使用するモードや鍵サイズ等
- 認証アルゴリズムとして推奨するHMAC（Hash Message Authentication Code）の概要

<u>各国宇宙機関およびJAXAの動向</u>

海外では、DLR（ドイツ航空宇宙センター）がCCSDS暗号アルゴリズムを使用している。JAXAではCCSDS推奨規格は使用していない。

© 2017 宇宙航空研究開発機構（JAXA）