CCSDS AUTHENTICATION CREDENTIALS
「CCSDS認証証明書」

Blue Book
CCSDS 357.0-B-1
発行月：2019年7月
ISO －

【概要】

本推奨規格は、CCSDSミッションや地上システムによる認証に使用される証明書の仕様を定義している。

【内容】

多くのCCSDSミッションは、機関間の通信で扱う情報を保護するためのセキュリティサービスを必要としている。複製や偽造が困難で、複雑なメカニズムである証明書方式として技術的に実績のあるX.509証明書（IETF（インターネット技術の標準化を推進する任意団体）で規定）と、保護簡易認証（ISO9594-8で規定）をCCSDSミッションへ適用することを目的として、本推奨規格が作成されている。

- X.509証明書
  X.509証明書は、保護簡易認証よりも安全なメカニズムを持っており、CCSDSミッション向けの主要な証明書として推奨している。1つのドメイン内でのIFや1対1の対向システムIFの場合は下記保護簡易認証の採用も選択肢の1つとしている。X.509証明書は、送信者と受信者の二者間認証ではなく、第三者機関として、認証局（公開鍵の証明などを行う）を含めた三者間認証でやり取りを行う。
  まず、送信者は個人鍵と公開鍵のペアを作成し、認証局に公開鍵の証明を依頼する。次に、認証局は証明書に署名し、その証明書を発行する。最後に、送信者から受信者へ証明書が送付される。認証局は、ユーザやデバイスに発行される証明書について、登録過程、証明書作成過程、証明書発行、証明書失効、鍵付け替えを行い、証明書や指示事項に署名を付与する。

- 保護簡易認証
  保護簡易認証は、ユーザの識別名（パスワード）を用いたローカル認証であり、下記に示す基本的なログオン時の認証である。
  a. 特定の関数を適用することで、ユーザの識別名、パスワード、無作為な数字と（あるいは）タイムスタンプの転送を保護する。
  b. 特定の関数を適用することで、無作為な数字と（あるいは）タイムスタンプとともに、aで表現した保護情報の転送を保護する。

本推奨規格では、2.2節にX.509証明書、2.3節に保護簡易認証、3.1節にX.509証明書の構文規則、3.2節に保護簡易認証の仕様を説明している。

各国宇宙機関及びJAXAの動向

新規文書につき、現在情報を収集中。