# Kerberos with PA-ENC-TIMESTAMP pre-authentication method の概要

国立研究開発法人 情報通信研究機構

## 1. 基本情報

- ✧ 名前

  Kerberos with PA-ENC-TIMESTAMP pre-authentication method

- ✧ 機能

  信頼できる第三者機関（TTP, Trusted Third Party）の存在を前提とする、オープンなネットワークにおけるサーバ・クライアント間でのネットワーク認証・鍵交換プロトコル。 特徴は共通鍵暗号を利用した事前認証を行うこと。

- ✧ 関連する標準

  RFC6113 (https://tools.ietf.org/html/rfc6113)

## 2. プロトコル仕様

Kerberos with PA-ENC-TIMESTAMP pre-authentication method (以降 Kerberos preauth) のプロトコル仕様のシーケンスを図 1 に示す。最初のリクエストは、通常平文であるが、予め共有している鍵により共通鍵暗号を利用してタイムスタンプ等を暗号化したデータ送付することにより、事前認証の機能を付加している。

## 3. 攻撃者モデル（自然言語による記述）

攻撃者として Dolev-Yao モデルを想定する。すなわち、通信の盗聴、改ざん、遮断、再送が可能とする。

## 4. セキュリティ要件（自然言語による記述）

- ➢ サーバ (S) によるクライアント (C) の認証。
- ➢ クライアントによるサーバの認証。
- ➢ サーバとクライアントが共有した鍵 K_CS の秘匿性。

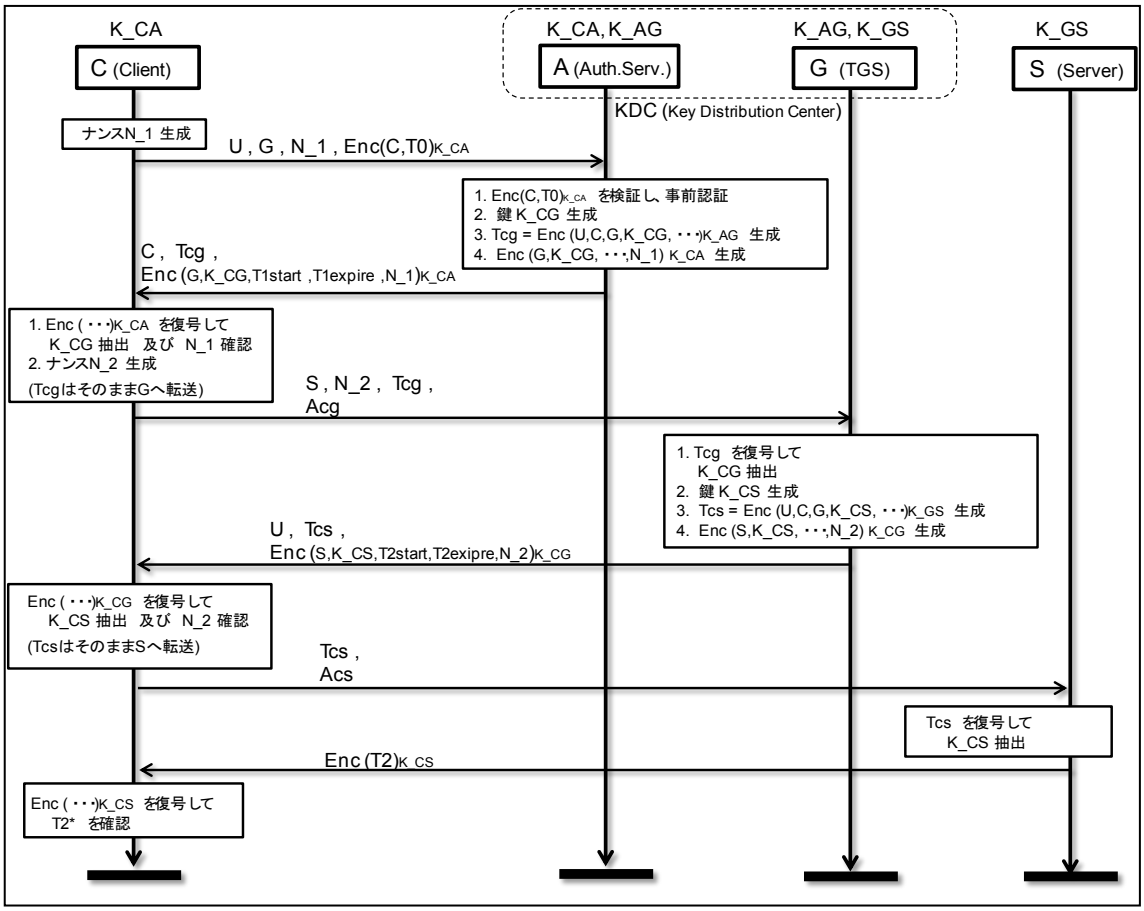


図 1. シーケンス図

## 5. 安全性に関して知られている結果

### 5.1. 制限

第三者によるチケットの受取が可能であること。

### 5.2. 脅威/脆弱性

K_CG の機密性。

### 5.3. 形式手法に基づく検証

AVISPA による評価結果が、http://www.avispa-project.org/library/Kerb-preauth.html に掲載されている。

## 6. 備考

本文書は、**総務省「暗号・認証技術等を用いた安全な通信環境推進事業に関する実証実験の請負　成果報告書」**からの引用である。