暗号プロトコル評価対象の概要

独立行政法人　情報通信研究機構

1.プロトコル名：Kerberos with forwardable ticket

2.関連する標準：RFC4120 (The Kerberos Network Authentication Service (V5)), July 2005. http://www.rfc-editor.org/rfc/pdfrfc/rfc4120.txt.pdf

3.暗号プロトコル仕様

Kerberos with forwardable ticketプロトコルについて解説する。

3.1.暗号プロトコルの概要と目的

クライアントのIPアドレスが変化する場合(別の端末へのリモートログイン等)のサーバ・クライアント間のネットワーク認証。FORWARDABLE(転送可能)なチケットを用いて、IPアドレスが変更された後でもサーバアクセス可能とする。(通常チケットでは IP アドレスが変更されると無効チケットとして取扱われる。)

シーケンス図

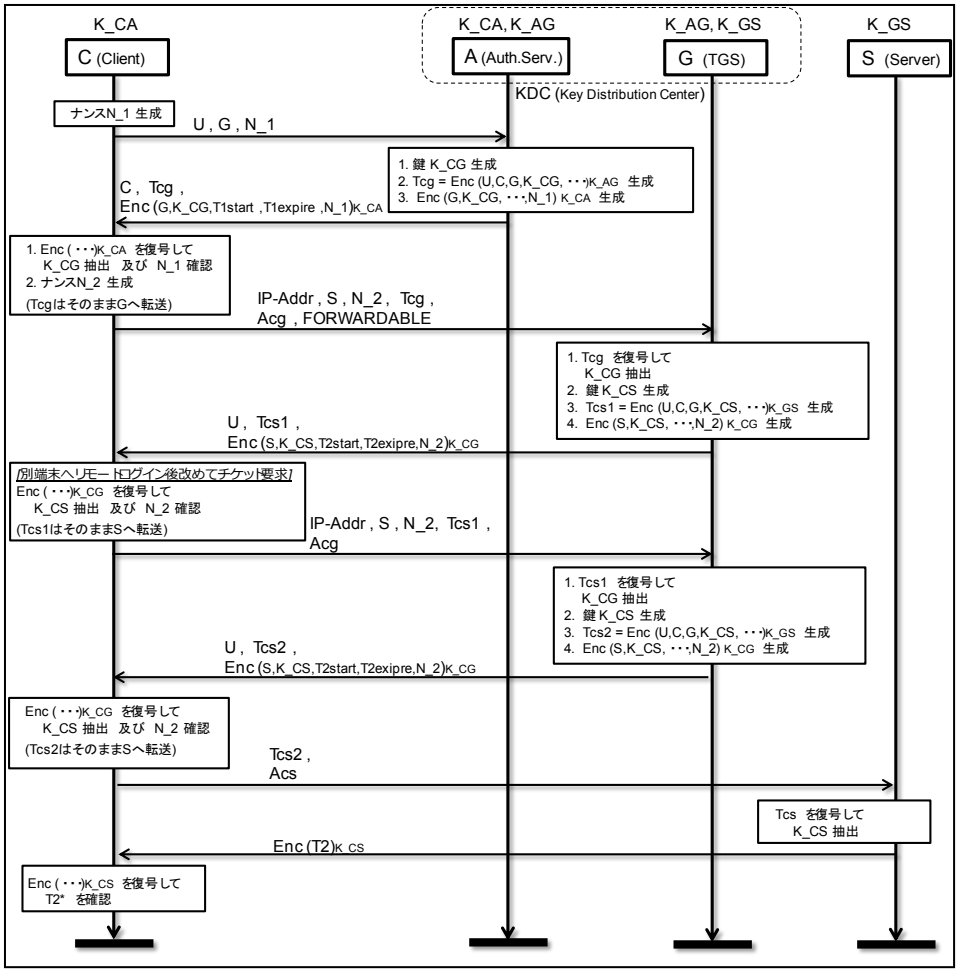

図 1. シーケンス図

4. 評価の環境

4.1. 攻撃者モデル（自然言語による記述）

攻撃者は参加者が送信するメッセージを横取りし、自らメッセージを構成して参加者に送信することができる。

4,2, セキュリティプロパティ（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。

4.3. 暗号プロトコルに関して知られている結果

○制限　第三者によるチケットの受取が可能であること。

○Formal Method 等による検証

- 文献 ： AVISPA による評価結果

http://www.avispa-project.org/library/Kerb-Forwardable.html

5.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。