PANA 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

  Protocol for Carrying Authentication for Network Access (PANA)

- ✧ 機能

  UDP/IP 上でのネットワークアクセス認証・鍵交換プロトコルであり、Extensible Authentication Protocol (EAP) のメッセージを運ぶ。

- ✧ 関連する標準

  RFC5191 (https://tools.ietf.org/html/rfc5191)

2. プロトコル仕様

PANA のプロトコル仕様のシーケンスを図 1 に示す。本文書では、EAP-AKA が利用されているとする。

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）

- ➢ 認証：エンティティ PaC とエンティティ PAA はお互いに通信相手が誰であるかを正しく確認でき、攻撃者によりなりすまされない。
- ➢ 鍵交換：エンティティ PaC とエンティティ PAA の共有するセッション鍵が想定されていないエンティティに対して秘匿されている

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

PANA について現時点で知られている脆弱性はない。

5.2. 形式手法に基づく検証

PANA について現時点で知られている形式手法に基づく検証はない。

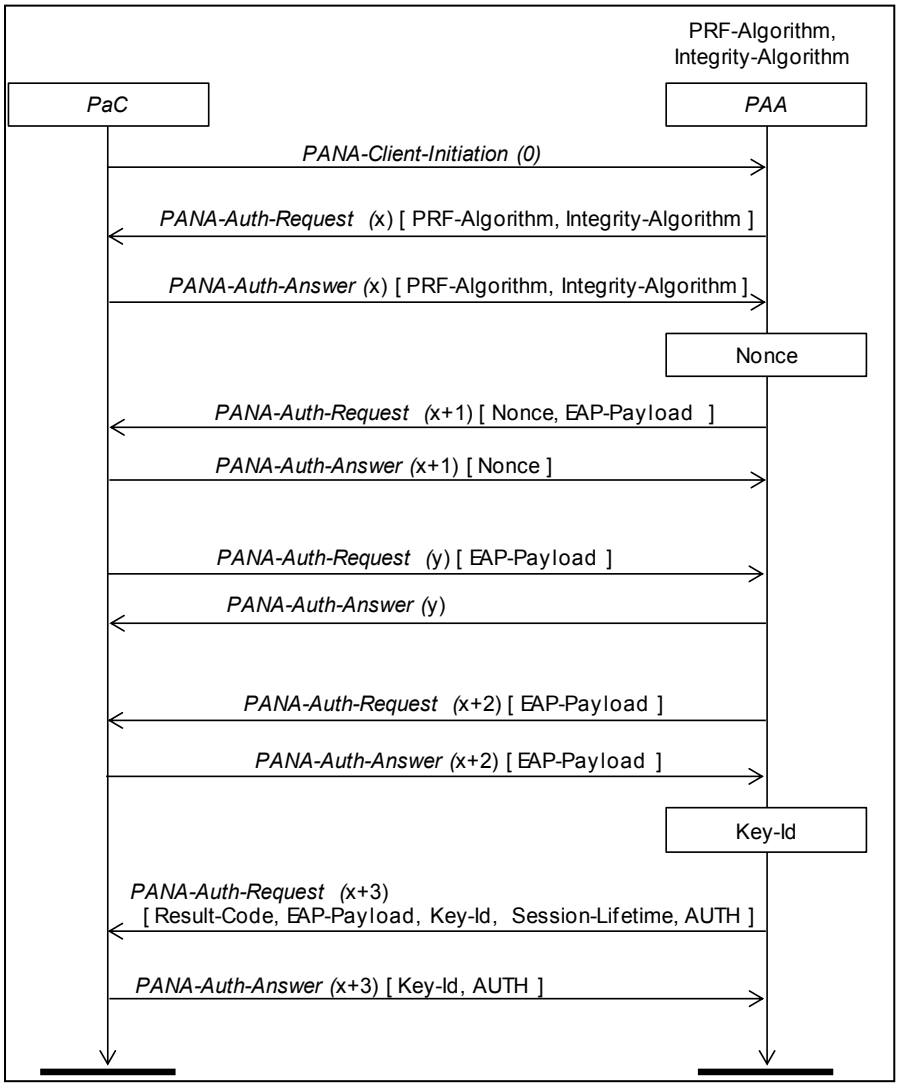

図 1. シーケンス図

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。