# EAP-Archie 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

  The EAP Archie Protocol

- ✧ 機能

  PPP 接続において事前共有鍵を用いた相互認証・鍵交換プロトコル。

- ✧ 関連する標準

  Internet Draft (Intended status: Informational)

  http://tools.ietf.org/html/draft-jwalker-eap-archie-01

## 2. プロトコル仕様

EAP-Archie のプロトコル仕様の概要を解説する。

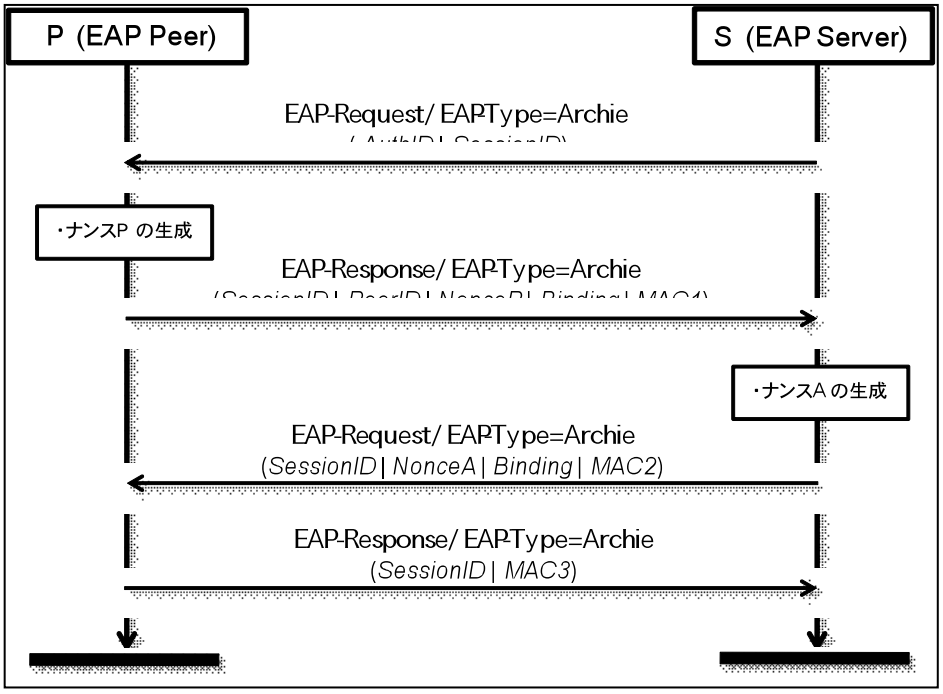


図 1. シーケンス図

### 2.1. 事前共有鍵

EAP-Archie では、3 種類の事前共有鍵 KCK (MAC 生成用)、KEK (鍵暗号化用)、KDK (セッ

ション鍵の生成）を用いる。

### 2.2. パケット

EAP-Archie では、EAP の Type フィールドが Archie に指定される。それ以降のデータが Archie パケットであるが、Archie パケットは以下のフィールドで構成される。

- ✧ MsgID:Archie パケットの種類を指定するフィールド。EAP-Archie では Archie-Request, Archie-Response, Archie-Confirm, Archie-Finish の 4 つの値が用いられる。
- ✧ Data：パケットに依存するペイロード。

### 2.3. ペイロード

ペイロードは以下のとおりである。

- ✧ AuthID：サーバの ID。
- ✧ SessionID：ランダムに生成されるナンス。
- ✧ PeerID：ピアの ID。
- ✧ NonceP：ピアが生成したナンス Np を KEK で暗号化したもの。
- ✧ NonceA：サーバが生成したナンス Na を KEK で暗号化したもの。
- ✧ Binding：ピアとサーバの MAC アドレスなどの対。
- ✧ MAC1：第 1 メッセージの Archie パケットからセッション ID を除いたものと、第 2 メッセージの Archie パケットから MAC1 自身を除いた値を連結し、KCK を用いて生成した MAC 値。
- ✧ MAC2：第 1 メッセージの Archie パケットからセッション ID を除いたものと、NonceP と、第 3 メッセージの Archie パケットから MAC2 自身を除いた値を連結し、KCK を用いて生成した MAC 値。
- ✧ MAC3：第 4 メッセージの Archie パケットから MAC3 自身を除いた値を連結し、KCK を用いて生成した MAC 値。

## 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）

RFC3748 では、暗号プロトコルの安全性について記述するためにいくつかの例を示しており、多くの場合これに従ってセキュリティ要件が記述される。EAP-Archie については、以下の性質を持つと主張されている。

- ➢ Conservative use of cryptography,

- Integrity protection,
- Replay protection,
- Man-in-the-middle resistance,
- Mutual authentication,
- Session formation,
- Consistent view,
- Peer liveness,
- Fresh key derivation,
- Key strength,
- Dictionary attack resistance, and
- Limited Denial-of-Service protection.

## 5. 安全性に関して知られている結果

### 5.1. 脅威/脆弱性

EAP-Archie 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

AVISPA による評価結果が http://www.avispa-project.org/library/EAP_Archie.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。