TTC標準
Standard

JF-IETF-RFC3310

AKA を利用する場合の HTTP ダイジェスト認証方式

Hypertext Transfer Protocol (HTTP)
Digest Authentication Using
Authentication and Key Agreement (AKA)

第 1.0 版

2009 年 5 月 27 日制定

社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

目 次

＜参考＞

1. 国際勧告等との関係

本標準は、IETF において制定された RFC3310 に準拠している。

2. 上記国際勧告等に対する追加項目等

2.1. オプション選択項目

特になし

2.2. ナショナルマター項目

特になし

2.3. 原標準に対する変更項目

特になし

3. 改版の履歴

版数	制定日	改版内容
第 1.0 版	2009 年 5 月 27 日	制定

4. 工業所有権

TTC の「工業所有権等の実施の権利に係る確認書」の提出状況は、ＴＴＣホームページで公開されている。

5. その他

(1) 参照する主な勧告、標準

IETF RFC: RFC1889, RFC2119, RFC1890, RFC2327, RFC3047

3GPP 仕様 TS 33.102 (Rel4) (Dec 2001)

(2) 本出版は、具体的な規定内容を含んでいない。規定はすべて準拠元である IETF RFC によっている。
具体的な規定内容は RFC を参照する必要がある。

6. 標準作成部門

信号制御専門委員会

1. 標準の概要

本標準は、HTTP ダイジェストアクセス認証のためのワンタイムパスワード生成メカニズムを基礎にした認証/暗号鍵配送方式(AKA)を規定する。HTTP 認証のフレームワークは、ベーシックとダイジェストの２つの認証スキームを持つ。両スキームは、アクセス認証のために共有秘密鍵を基礎にした仕組みを用いる。

AKA の作用は、全世界共通移動体電話システム(UMTS)網においてユーザ認証とセッション鍵配送を実行する。AKA は、対称暗号を用いるチャレンジ-レスポンス方式のメカニズムである。

2. 本標準で規定する内容

本標準で規定する内容は下記の IETF RFC による。

IETF RFC3310：「Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)」