TTC標準
Standard

JF-IETF-RFC3853

SIP における S/MIME での AES 利用

S/MIME Advanced Encryption Standard (AES)
Requirement for
the Session Initiation Protocol(SIP)

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 RFC3853 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: RFC2119 , RFC2246 , RFC3261 , RFC3369 , RFC3565 , RFC3394 , RFC3851

米国国立標準技術研究所(NIST): FIPS 197 (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

RFC3261 は現在、セッション開始プロトコル(SIP)における S/MIME の実装の為に実装必須な暗号方式として 3DES を規定している。 本標準は S/MIME のために次世代標準暗号化方式(AES)を必要とするために RFC3261 の規定内容を更新するものである。

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 RFC3853 : 「S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)」