

ファームウェア更新に対する IETF RATS 準拠リモートアテステーションの設計

A Design for Remote Attestation based on IETF RATS to protect firmware update

内匠真也 *
Shinya Takumi

藤松由里恵 *
Yurie Fujimatsu

金井遵 *
Jun Kanai

キーワード Remote Attestation (RA), IETF, RATS, RoT, ファームウェア更新

あらまし

本稿ではファームウェア更新の正常完了を検証可能なリモートアテステーションの設計を提案する。脆弱性の修正にはOTAアップデートが広く利用されているが、デバイスが点在するCPSにおいてはデバイスのファームウェア更新が正しく行われたことをサーバから確認できる必要がある。そこで本提案では標準化団体IETF(Internet Engineering Task Force)のRATS(Remote Attestation ProcedureS)ワーキンググループにおいて標準化が進むリモートアテステーション規格に注目し、デバイスのファームウェア更新後の状態をサーバからセキュアに確認するための設計を示す。本方式により多種多様なデバイスのファームウェア更新の正常完了を検証することが可能となり、CPSにおける確実な脆弱性対応を促進することができるようになる。

* (株)東芝研究開発センター 〒212-8582 神奈川県川崎市幸区小向東芝
町1. Corporate Research & Development Center, Toshiba Corporation.
1, Komukai-Toshiba-Cho, Saiwai-ku, Kawasaki-shi, Kanagawa
212-8582