第7章

セキュア・ブート/改ざん保護/暗号化

セキュリティ強化①…デバイスおよびデータの保護

小林 明

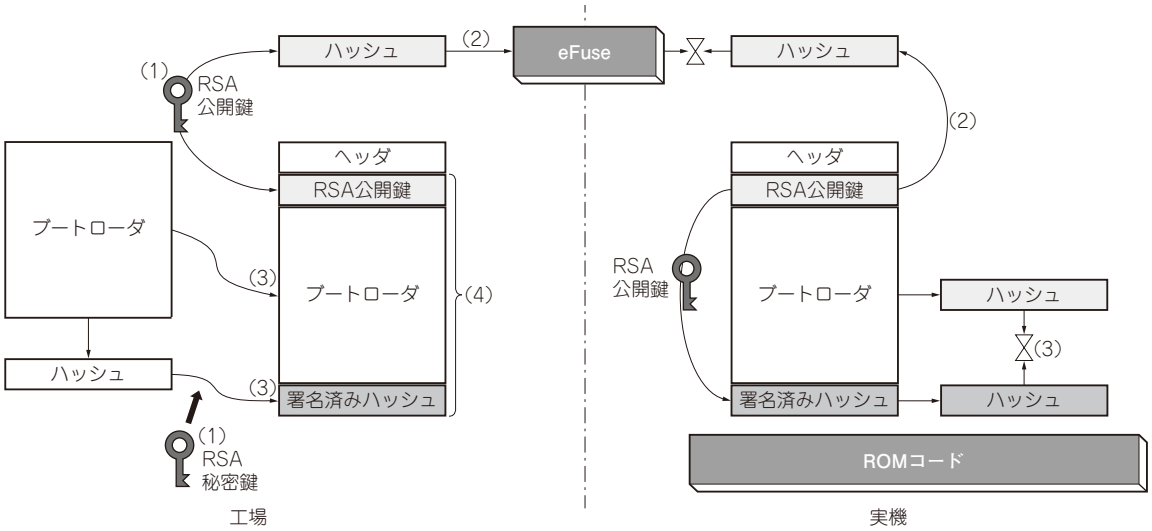

図1　セキュア・ブートにおける署名検証方式のしくみ
ブートローダに改ざんがあった場合，起動前に検知できるようになっている

最近は，サイバー・セキュリティによる被害が社会の深刻な問題となってきています．そのような中，サーバやPCに限らず，IoT機器についても，欧米をはじめとする各国でラベリング制度や法規制などの動きが活発になってきています．

この中で求められているのが，不正アクセスからの保護や脆弱性管理（製品リリース後も含む），脆弱性を取り除くためのソフトウェア・アップデートなどです．本章以降では，それらの方法について幾つか紹介します．

悪意あるソフトウェアの実行を未然に防ぐ…セキュア・ブート

チューニング術㊲

最近のSoCはセキュア・ブート機能を搭載しており，ブートローダ以降のトラスト・チェーンの作成を可能にしています．SoCによって機能実装は異なりますが，署名検証方式だけでなく，オブジェクトのAES（Advanced Encryption Standard）などの暗号化に対応しているものもあります．

署名検証方式の概要を**図1**に示します．暗号化の流れは次の通りです．

▶工場サイド

(1) SoCの機能に依存するが，RSA暗号化などで鍵のペア（公開鍵と秘密鍵）を作成する
(2) 公開鍵のハッシュ値をSoCの指定されたeFuse[注1]に書き込む
(3) ブートローダのハッシュ値を秘密鍵で署名する
(4) 公開鍵，ブートローダ，署名の3つをセットにする

▶実機サイド

(1) これ以降はSoCのROMコードで検証を実施
(2) 公開鍵を取り出し，ハッシュ値を作成し，eFuseに格納されているハッシュ値との一致をチェックする．
(3) 公開鍵を用いて署名を検証し，ブートローダの

注1：電気的にプログラム可能な不揮発性メモリのことです．一度書き込みを行うと元に戻すことはできません．