【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成28年12月1日(2016.12.1)

【公表番号】特表2015-533444(P2015-533444A)
【公表日】平成27年11月24日(2015.11.24)
【年通号数】公開・登録公報2015-073
【出願番号】特願2015-540903(P2015-540903)
【国際特許分類】
Ｇ０６Ｆ　11/00　(2006.01)
Ｇ０６Ｆ　 9/445　(2006.01)
Ｇ０６Ｆ　21/57　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　 9/06　６３０Ａ
Ｇ０６Ｆ　 9/06　６１０Ｌ
Ｇ０６Ｆ　21/57　３２０

【手続補正書】
【提出日】平成28年10月14日(2016.10.14)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ニアフィールド通信（ＮＦＣ）デバイスにおいてアンチロールバック保護を与えるための方法であって、
前記ＮＦＣデバイスのための第１のファームウェアインスタレーションに関連するファームウェアバージョン番号（ＦＶＮ）を取得することと、ここにおいて、前記ＮＦＣデバイスが、不揮発性メモリを含まない基板上に実装される、
最低許容ファームウェアバージョン番号（ＬＡＦＶＮ）を取得することと、ここにおいて、前記ＬＡＦＶＮがセキュア要素環境に記憶され、ここにおいて、前記セキュア要素環境が、前記基板から分離されたメモリを利用する、
前記ＦＶＮと前記ＬＡＦＶＮとを比較し、ここにおいて、前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、前記第１のファームウェアインスタレーションを可能にしないことと
を備える方法。
【請求項２】
アンチロールバック保護を与えるためのニアフィールド通信（ＮＦＣ）デバイスであって、
１つまたは複数プロセッサと、
前記ＮＦＣデバイスのための第１のファームウェアインスタレーションに関連するファームウェアバージョン番号（ＦＶＮ）を取得するための手段と、ここにおいて、前記ＮＦＣデバイスが、不揮発性メモリを含まない基板上に実装される、
最低許容ファームウェアバージョン番号（ＬＡＦＶＮ）を取得するための手段と、ここにおいて、前記ＬＡＦＶＮがセキュア要素環境に記憶され、ここにおいて、前記セキュア要素環境が、前記基板から分離されたメモリを利用する、
前記ＦＶＮと前記ＬＡＦＶＮとを比較し、ここにおいて、前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、前記第１のファームウェアインスタレーションを可能にしないための手段と

を備えるＮＦＣデバイス。
【請求項３】
前記ＮＦＣデバイスがＮＦＣコントローラを備える、請求項１に記載の方法または請求項２に記載のＮＦＣデバイス。
【請求項４】
前記セキュア要素環境が、ソフトウェアおよびハードウェア攻撃から保護するスタンドアロンセキュア実行環境（ＳＥＥ）である、請求項１に記載の方法または請求項２に記載のＮＦＣデバイス。
【請求項５】
前記セキュア要素環境が、システムオンチップ（ＳｏＣ）のハードウェア保護パーティションにおける信頼実行環境（ＴＥＥ）である、請求項１に記載の方法または請求項２に記載のＮＦＣデバイス。
【請求項６】
前記ＬＡＦＶＮは、前記ＦＶＮが前記ＬＡＦＶＮよりも大きい場合、前記ＦＶＮに等しくなるように更新される、請求項１に記載の方法または請求項２に記載のＮＦＣデバイス。
【請求項７】
前記ＬＡＦＶＮがＧｌｏｂａｌＰｌａｔｆｏｒｍ機構を使用して更新される、請求項６に記載の方法または請求項６に記載のＮＦＣデバイス。
【請求項８】
前記ＬＡＦＶＮが制御当局によって更新される、請求項１に記載の方法または請求項２に記載のＮＦＣデバイス。
【請求項９】
前記第１のファームウェアインスタレーションが前記ＮＦＣデバイス上の既存のファームウェアの部分更新である、請求項１に記載の方法または請求項２に記載のＮＦＣデバイス。
【請求項１０】
前記第１のファームウェアインスタレーションが前記ＮＦＣデバイス上の既存のファームウェアの全更新である、請求項１に記載の方法または請求項２に記載のＮＦＣデバイス。
【請求項１１】
前記ＬＡＦＶＮが前記セキュア要素環境におけるアプリケーションに記憶される、請求項１に記載の方法または請求項２に記載のＮＦＣデバイス。
【請求項１２】
前記第１のファームウェアインスタレーションに関連するデジタル署名に基づいて前記第１のファームウェアインスタレーションを認証することをさらに備える、請求項１に記載の方法。
【請求項１３】
前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、ＬＡＦＶＮよりも大きいバージョン番号をもつ第２のファームウェアインスタレーションのアップロードを要求する、請求項１に記載の方法または請求項２に記載のＮＦＣデバイス。
【請求項１４】
前記第１のファームウェアインスタレーションに関連するデジタル署名に基づいて前記第１のファームウェアインスタレーションを認証するための手段をさらに備える、請求項２に記載のＮＦＣデバイス。
【請求項１５】
実行されたとき、請求項１から請求項１３に従って方法のステップを実行するためのコンピュータ実行可能命令を備える、コンピュータプログラム。
【手続補正２】
【補正対象書類名】明細書

【補正対象項目名】０１１１
【補正方法】変更
【補正の内容】
【０１１１】
[0126]いくつかの例示的な構成について説明したが、本開示の趣旨から逸脱することなく、様々な変更形態、代替構成、および等価物が使用され得る。たとえば、上記の要素は、より大きいシステムの構成要素であり得、他のルールが、本発明の適用よりも優先するかまたは他の方法で本発明の適用を変更し得る。また、上記の要素が考慮される前に、考慮されている間に、または考慮された後に、いくつかのステップが行われ得る。したがって、上記の説明は特許請求の範囲を制限しない。
以下に本願の出願当初の特許請求の範囲に記載された発明を付記する。
[Ｃ１]　デバイスにおいてアンチロールバック保護を与えるための方法であって、
前記デバイスのための第１のファームウェアインスタレーションに関連するファームウェアバージョン番号（ＦＶＮ）を取得することと、ここにおいて、前記デバイスが、不揮発性メモリを含まない基板上に実装される、
最低許容ファームウェアバージョン番号（ＬＡＦＶＮ）を取得することと、ここにおいて、前記ＬＡＦＶＮがセキュア要素環境に記憶され、ここにおいて、前記セキュア要素環境が、前記基板から分離されたメモリを利用する、
前記ＦＶＮと前記ＬＡＦＶＮとを比較し、ここにおいて、前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、前記第１のファームウェアインスタレーションを可能にしないこととを備える方法。
[Ｃ２]　前記デバイスがニアフィールド通信（ＮＦＣ）コントローラを備える、Ｃ１に記載の方法。
[Ｃ３]　前記セキュア要素環境が、ソフトウェアおよびハードウェア攻撃から保護するスタンドアロンセキュア実行環境（ＳＥＥ）である、Ｃ１に記載の方法。
[Ｃ４]　前記セキュア要素環境が、システムオンチップ（ＳｏＣ）のハードウェア保護パーティションにおける信頼実行環境（ＴＥＥ）である、Ｃ１に記載の方法。
[Ｃ５]　前記ＬＡＦＶＮは、前記ＦＶＮが前記ＬＡＦＶＮよりも大きい場合、前記ＦＶＮに等しくなるように更新される、Ｃ１に記載の方法。
[Ｃ６]　前記ＬＡＦＶＮがＧｌｏｂａｌＰｌａｔｆｏｒｍ機構を使用して更新される、Ｃ５に記載の方法。
[Ｃ７]　前記ＬＡＦＶＮが制御当局によって更新される、Ｃ１に記載の方法。
[Ｃ８]　前記第１のファームウェアインスタレーションが前記デバイス上の既存のファームウェアの部分更新である、Ｃ１に記載の方法。
[Ｃ９]　前記第１のファームウェアインスタレーションが前記デバイス上の既存のファームウェアの全更新である、Ｃ１に記載の方法。
[Ｃ１０]　前記ＬＡＦＶＮが前記セキュア要素環境におけるアプリケーションに記憶される、Ｃ１に記載の方法。
[Ｃ１１]　前記第１のファームウェアインスタレーションに関連するデジタル署名基づいて前記第１のファームウェアインスタレーションを認証することをさらに備える、Ｃ１に記載の方法。
[Ｃ１２]　前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、ＬＡＦＶＮよりも大きいバージョン番号をもつ第２のファームウェアインスタレーションのアップロードを要求する、Ｃ１に記載の方法。
[Ｃ１３]　アンチロールバック保護を与えるためのデバイスであって、
１つまたは複数のプロセッサと、
前記１つまたは複数のプロセッサによって実行されたとき、前記デバイスに、
前記デバイスのための第１のファームウェアインスタレーションに関連するファームウェアバージョン番号（ＦＶＮ）を取得することと、ここにおいて、前記デバイスが、不揮発性メモリを含まない基板上に実装される、

最低許容ファームウェアバージョン番号（ＬＡＦＶＮ）を取得することと、ここにおいて、前記ＬＡＦＶＮがセキュア要素環境に記憶され、ここにおいて、前記セキュア要素環境が、前記基板から分離されたメモリを利用する、
前記ＦＶＮと前記ＬＡＦＶＮとを比較し、ここにおいて、前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、前記第１のファームウェアインスタレーションを可能にしないことと
を行わせる、コンピュータ可読命令を記憶するメモリとを備えるデバイス。
[Ｃ１４] 前記デバイスがニアフィールド通信（ＮＦＣ）コントローラを備える、Ｃ１３に記載のデバイス。
[Ｃ１５] 前記セキュア要素環境が、ソフトウェアおよびハードウェア攻撃から保護するスタンドアロンセキュア実行環境（ＳＥＥ）である、Ｃ１３に記載のデバイス。
[Ｃ１６] 前記セキュア要素環境が、システムオンチップ（ＳｏＣ）のハードウェア保護パーティションにおける信頼実行環境（ＴＥＥ）である、Ｃ１３に記載のデバイス。
[Ｃ１７] 前記ＬＡＦＶＮは、前記ＦＶＮが前記ＬＡＦＶＮよりも大きい場合、前記ＦＶＮに等しくなるように更新される、Ｃ１３に記載のデバイス。
[Ｃ１８] 前記ＬＡＦＶＮがＧｌｏｂａｌＰｌａｔｆｏｒｍ機構を使用して更新される、Ｃ１７に記載のデバイス。
[Ｃ１９] 前記ＬＡＦＶＮが制御当局によって更新される、Ｃ１３に記載のデバイス。
[Ｃ２０] 前記第１のファームウェアインスタレーションが前記デバイス上の既存のファームウェアの部分更新である、Ｃ１３に記載のデバイス。
[Ｃ２１] 前記第１のファームウェアインスタレーションが前記デバイス上の既存のファームウェアの全更新である、Ｃ１３に記載のデバイス。
[Ｃ２２] 前記ＬＡＦＶＮが前記セキュア要素環境におけるアプリケーションに記憶される、Ｃ１３に記載のデバイス。
[Ｃ２３] 前記第１のファームウェアインスタレーションに関連するデジタル署名基づいて前記第１のファームウェアインスタレーションを認証するための前記デバイスをさらに備える、Ｃ１３に記載のデバイス。
[Ｃ２４] 前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、ＬＡＦＶＮよりも大きいバージョン番号をもつ第２のファームウェアインスタレーションのアップロードを要求する、Ｃ１３に記載のデバイス。
[Ｃ２５] 実行されたとき、デバイスに、
前記デバイスのための第１のファームウェアインスタレーションに関連するファームウェアバージョン番号（ＦＶＮ）を取得することと、ここにおいて、前記デバイスが、不揮発性メモリを含まない基板上に実装される、
最低許容ファームウェアバージョン番号（ＬＡＦＶＮ）を取得することと、ここにおいて、前記ＬＡＦＶＮがセキュア要素環境に記憶され、ここにおいて、前記セキュア要素環境が、前記基板から分離されたメモリを利用する、
前記ＦＶＮと前記ＬＡＦＶＮとを比較し、ここにおいて、前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、前記第１のファームウェアインスタレーションを可能にしないことと
を行わせる、コンピュータ実行可能命令を記憶するコンピュータ可読媒体。
[Ｃ２６] 前記デバイスがニアフィールド通信（ＮＦＣ）コントローラを備える、Ｃ２５に記載のコンピュータ可読媒体。
[Ｃ２７] 前記セキュア要素環境が、ソフトウェアおよびハードウェア攻撃から保護するスタンドアロンセキュア実行環境（ＳＥＥ）である、Ｃ２５に記載のコンピュータ可読媒体。
[Ｃ２８] 前記セキュア要素環境が、システムオンチップ（ＳｏＣ）のハードウェア保護パーティションにおける信頼実行環境（ＴＥＥ）である、Ｃ２５に記載のコンピュータ可読媒体。
[Ｃ２９] 前記ＬＡＦＶＮは、前記ＦＶＮが前記ＬＡＦＶＮよりも大きい場合、前記ＦＶＮに等しくなるように更新される、Ｃ２５に記載のコンピュータ可読媒体。

[Ｃ３０] 前記ＬＡＦＶＮがＧｌｏｂａｌＰｌａｔｆｏｒｍ機構を使用して更新される、Ｃ２９に記載のコンピュータ可読媒体。
[Ｃ３１] 前記ＬＡＦＶＮが制御当局によって更新される、Ｃ２５に記載のコンピュータ可読媒体。
[Ｃ３２] 前記第１のファームウェアインスタレーションが前記デバイス上の既存のファームウェアの部分更新である、Ｃ２５に記載のコンピュータ可読媒体。
[Ｃ３３] 前記第１のファームウェアインスタレーションが前記デバイス上の既存のファームウェアの全更新である、Ｃ２５に記載のコンピュータ可読媒体。
[Ｃ３４] 前記ＬＡＦＶＮが前記セキュア要素環境におけるアプリケーションに記憶される、Ｃ２５に記載のコンピュータ可読媒体。
[Ｃ３５] 前記第１のファームウェアインスタレーションに関連するデジタル署名基づいて前記第１のファームウェアインスタレーションを認証するための前記デバイスをさらに備える、Ｃ２５に記載のコンピュータ可読媒体。
[Ｃ３６] 前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、ＬＡＦＶＮよりも大きいバージョン番号をもつ第２のファームウェアインスタレーションのアップロードを要求する、Ｃ２５に記載のコンピュータ可読媒体。
[Ｃ３７] アンチロールバック保護を与えるためのデバイスであって、
１つまたは複数のプロセッサと、
前記デバイスのための第１のファームウェアインスタレーションに関連するファームウェアバージョン番号（ＦＶＮ）を取得するための手段と、ここにおいて、前記デバイスが、不揮発性メモリを含まない基板上に実装される、
最低許容ファームウェアバージョン番号（ＬＡＦＶＮ）を取得するための手段と、ここにおいて、前記ＬＡＦＶＮがセキュア要素環境に記憶され、ここにおいて、前記セキュア要素環境が、前記基板から分離されたメモリを利用する、
前記ＦＶＮと前記ＬＡＦＶＮとを比較し、ここにおいて、前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、前記第１のファームウェアインスタレーションを可能にしないための手段とを備えるデバイス。
[Ｃ３８] 前記デバイスがニアフィールド通信（ＮＦＣ）コントローラを備える、Ｃ３７に記載のデバイス。
[Ｃ３９] 前記セキュア要素環境が、ソフトウェアおよびハードウェア攻撃から保護するスタンドアロンセキュア実行環境（ＳＥＥ）である、Ｃ３７に記載のデバイス。
[Ｃ４０] 前記セキュア要素環境が、システムオンチップ（ＳｏＣ）のハードウェア保護パーティションにおける信頼実行環境（ＴＥＥ）である、Ｃ３７に記載のデバイス。
[Ｃ４１] 前記ＬＡＦＶＮは、前記ＦＶＮが前記ＬＡＦＶＮよりも大きい場合、前記ＦＶＮに等しくなるように更新される、Ｃ３７に記載のデバイス。
[Ｃ４２] 前記ＬＡＦＶＮがＧｌｏｂａｌＰｌａｔｆｏｒｍ機構を使用して更新される、Ｃ４１に記載のデバイス。
[Ｃ４３] 前記ＬＡＦＶＮが制御当局によって更新される、Ｃ３７に記載のデバイス。
[Ｃ４４] 前記第１のファームウェアインスタレーションが前記デバイス上の既存のファームウェアの部分更新である、Ｃ３７に記載のデバイス。
[Ｃ４５] 前記第１のファームウェアインスタレーションが前記デバイス上の既存のファームウェアの全更新である、Ｃ３７に記載のデバイス。
[Ｃ４６] 前記ＬＡＦＶＮが前記セキュア要素環境におけるアプリケーションに記憶される、Ｃ３７に記載のデバイス。
[Ｃ４７] 前記第１のファームウェアインスタレーションに関連するデジタル署名基づいて前記第１のファームウェアインスタレーションを認証するための手段をさらに備える、Ｃ３７に記載のデバイス。
[Ｃ４８] 前記ＦＶＮが前記ＬＡＦＶＮよりも小さい場合、ＬＡＦＶＮよりも大きいバージョン番号をもつ第２のファームウェアインスタレーションのアップロードを要求する、Ｃ３７に記載のデバイス。