令和４年４月２８日判決言渡

令和３年（行ケ）第１００６４号　審決取消請求事件

口頭弁論終結日　令和４年２月１日

判　　決

原　　告　　三星電子株式会社

同訴訟代理人弁理士　　佐藤英昭

吉田豊麿

丸山亮

林晴男

松本邦夫

被　　告　　特許庁長官

同指定代理人　　山崎慎一

田中秀人

中村則夫

冨澤美加

主　　文

１　原告の請求を棄却する。

２　訴訟費用は原告の負担とする。

３　この判決に対する上告及び上告受理申立てのための付加期間を３０日と定める。

事実及び理由

第１　請求

特許庁が不服２０１８－１５５５６号事件について令和２年１２月９日にし

た審決を取り消す。

第２　事案の概要

１　特許庁における手続の経緯等

⑴　エーサー・クラウド・テクノロジイ・インコーポレイテッド（以下「エーサー」という。）は、平成１９年９月１３日（優先日平成１８年１１月９日、同月１６日（以下「本願優先日」という。）、優先権主張国米国）を国際出願日とする特許出願（特願２００９－５３６２２７号）の一部を分割した特許出願（特願２０１３－２１４４４０号）の一部を更に分割した特許出願（特願２０１５－１４９２２４号）を更に分割して、平成２９年３月２７日、発明の名称を「サーバ」とする発明について、新たな特許出願（特願２０１７－６０５０４号。以下「本願」という。）をした（甲１）。

エーサーは、同年１０月３０日付けの拒絶理由通知（甲５）を受けた後、平成３０年２月１４日付けで、特許請求の範囲及び発明の名称について手続補正をした（上記手続補正後の発明の名称は「サーバとこのサーバにより認証されるクライアント装置」。甲１２）。

エーサーは、同年７月６日付けで、上記手続補正による特許請求の範囲の補正について却下決定（甲１４）を受けるとともに、拒絶査定（甲１３）を受けた。

⑵　エーサーは、平成３０年１１月２６日、拒絶査定不服審判（不服２０１８－１５５５６号事件。甲１５）を請求した。

エーサーは、令和元年８月１９日付けの拒絶理由通知（甲１９）を受けたため、令和２年１月２７日付けで特許請求の範囲について手続補正（以下「本件補正」という。甲２４）をした。

特許庁は、同年１２月９日、「本件審判の請求は、成り立たない。」との審決（以下「本件審決」という。甲３２）をし、その謄本は、令和３年１月１２日、エーサーに送達された。

その後、原告は、エーサーから、本願に係る特許を受ける権利の譲渡を受け、同年３月１８日付けで、その旨の出願人名義変更届をした（甲３４、３５）。

⑶　原告は、令和３年５月１２日、本件審決の取消しを求める本件訴訟を提起した。

２　特許請求の範囲の記載

本件補正後の特許請求の範囲の請求項１の記載は､次のとおりである(以下、請求項１に係る発明を「本願発明」という。甲２４)。

【請求項１】

数発生器と、

証明書リクエストモジュールと、

証明書検証モジュールと、

前記数発生器、前記証明書リクエストモジュール、及び前記証明書検証モジュールに接続するインターフェースとを備えるとともに、不揮発性メモリを有したクライアント装置を認証するためのサーバであって

動作において、

前記数発生器が第１の数を生成し、

前記証明書リクエストモジュールは、デバイス証明書のリクエストを生成し、前記第１の数と前記デバイス証明書のリクエストは前記インターフェースを介してクライアント装置に送られ、

前記第１の数と、

前記クライアント装置において該クライアント装置の製造中にプログラムされたプライベートキーと前記サーバの数発生器が作成した第１の数を使用して生成される第２の署名と、

前記クライアント装置の装置ＩＤ、発行者ＩＤ、前記プライベートキーの関数である公開鍵及び前記クライアント装置の不揮発性メモリから読み出さ

れた第１の署名の関数として生成されたデバイス証明書と

を含むレスポンスが前記インターフェースで受け取られ、

前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し、前記サーバの数発生器が発生した第１の数と前記クライアント装置からの第１の数が一致しているか否かを検証する

ことを特徴とするサーバ。

３　本件審決の理由の要旨

⑴　本件審決の理由は、別紙審決書（写し）記載のとおりである。

その要旨は、本願発明は、本願優先日前に頒布された刊行物である特開２００６－９２２８１号公報（以下「引用文献１」という。甲６）に記載された発明及び特開２００４－１３５３２５号公報（以下「引用文献２」という。甲２６）、特開２００６－１８７０９号公報（以下「引用文献３」という。甲２７）、特開２００３－３２３３４２号公報（以下「引用文献４」という。甲２８）に記載の技術事項に基づいて、当業者が容易に発明をすることができたものであり、特許法２９条２項の規定により特許を受けることができないから、本願は拒絶すべきものであるというものである。

⑵　本件審決が認定した引用文献１に記載された発明（以下「引用発明」という。）、本願発明と引用発明の一致点及び相違点は、次のとおりである。

なお、原告は、引用文献１に引用発明の記載があることを認めている。

ア　引用発明

証明書要求部と、

乱数生成部と、

証明書検証部を有し、フラッシュメモリ１５１を有するセキュリティデバイス１０２の認証を行う、ＣＰ３０３であって、

前記乱数生成部は、乱数を生成し、

前記証明書要求部は、前記乱数を含む、セキュリティデバイス証明書を

要求するリクエストを生成して、前記リクエストを、前記セキュリティデバイス１０２に送信し、

前記セキュリティデバイス１０２から､セキュリティデバイス証明書と、前記乱数に対して施した電子署名とを応答として受信し、

前記電子署名を前記セキュリティデバイス証明書を用いて検証する、ＣＰ３０３。

イ　本願発明と引用発明の一致点及び相違点

（一致点）

「数発生器と、

証明書リクエストモジュールと、

証明書検証モジュールとを備えるとともに、

不揮発性メモリを有したクライアント装置を認証するためのサーバであって、

前記数発生器が第１の数を生成し、

前記証明書リクエストモジュールは、証明書のリクエストを生成し、

前記第１の数と前記証明書のリクエストは前記クライアント装置に送られ、

前記クライアント装置において該クライアント装置の製造中にプログラムされたプライベートキーと前記サーバの数発生器が作成した第１の数を使用して生成される第２の署名と、証明書と

を含むレスポンスが受け取られ、

前記証明書検証モジュールは前記証明書と第２の署名とを認証する、サーバ。」である点

（相違点１）

本願発明は、「数発生器、前記証明書リクエストモジュール、及び前記証明書検証モジュールに接続するインターフェース」を備えるものであるの

に対して、

引用発明においては、「インターフェース」について、特に、言及されていない点。

（相違点２）

“証明書”に関して、

本願発明においては、「クライアント装置の装置ＩＤ、発行者ＩＤ、前記プライベートキーの関数である公開鍵及び前記クライアント装置の不揮発性メモリから読み出された第１の署名の関数として生成されたデバイス証明書」であるのに対して、

引用発明においては、「セキュリティデバイス証明書」の詳細については、特に、言及されていない点。

（相違点３）

“リクエスト”に関して、

本願発明においては、「リクエストは前記インターフェースを介してクライアント装置に送られ」るものであるのに対して、

引用発明においては、「リクエスト」が、「インターフェース」を介して送信されることについては、特に、言及されていない点。

（相違点４）

“レスポンス”に関して、

本願発明においては、「レスポンス」が、「第１の数」を含むものであるのに対して、

引用発明においては、「応答」が、「乱数」を含む点については、特に、言及されていない点。

（相違点５）

本願発明においては、「レスポンスが前記インターフェースで受け取られ」るものであるのに対して、

引用発明においては、「応答」が、「インターフェース」で受信されることについては、特に、言及されていない点。

（相違点６）

本願発明においては、「サーバの数発生器が発生した第１の数と前記クライアント装置からの第１の数が一致しているか否かを検証する」ものであるのに対して、

引用発明においては、「乱数」の一致に関しては、特に、言及されていない点。

４　取消事由

引用文献１を主引用例とする本願発明の進歩性の判断の誤り

第３　当事者の主張

１　原告の主張

⑴　一致点の認定の誤り

ア　「クライアント装置」に係る一致点の認定の誤り

本件審決は、引用発明の「セキュリティデバイス１０２」が本願発明の「クライアント装置」に相当するとの認定を前提に、本願発明と引用発明は、「前記第１の数と前記証明書のリクエストは前記クライアント装置に送られ」る点で一致すると認定した。

しかし、引用発明は、「セキュリティデバイス１０２」が「情報端末１０１」に装着されて「情報端末１０１」と通信するように構成され，本願発明の「サーバ」に相当する引用発明の「ＣＰ３０３」には「情報端末１０１」が無線ネットワークを介して接続される構成であることからすると、本願発明の「クライアント装置」に相当するのは、引用発明の「情報端末１０１」であって、「セキュリティデバイス１０２」でないから、本件審決の上記一致点の認定は誤りである。

イ　「第２の署名」に係る一致点の認定の誤り

本件審決は、引用発明の「乱数に施した電子署名」が本願発明の「クライアント装置において該クライアント装置の製造中にプログラムされたプライベートキーと前記サーバの数発生器が作成した第１の数を使用して生成される第２の署名」に相当するとの認定を前提に、本願発明と引用発明は、「レスポンス」が「該クライアント装置の製造中にプログラムされたプライベートキーと前記サーバの数発生器が作成した第１の数を使用して生成される第２の署名」を含む点で一致すると認定した。

しかし、引用発明の「乱数に施した電子署名」とは、その文言から、「電子署名を乱数に施した」ことを意味するものであり、電子署名自体には、変化がなく、「乱数に施したことで得られた電子署名」とは異なるものである。一方、本願発明の「第１の数を使用して生成される第２の署名」は、第１の数を使用して新たに生成されるものであり、「乱数に施したことで得られた電子署名」に対応する署名であることからすると、引用発明の「乱数に施した電子署名」は、本願発明の「クライアント装置において該クライアント装置の製造中にプログラムされたプライベートキーと前記サーバの数発生器が作成した第１の数を使用して生成される第２の署名」に相当するものではないから、本件審決の上記一致点の認定は誤りである。

⑵　相違点２の容易想到性の判断の誤り

ア　本件審決は、相違点２に関し、「デバイスＩＤ」、「署名」を含む「デバイス証明書」については、引用文献３及び４の記載のとおり、本願優先日前に、当業者に周知の技術事項であり、また、「証明書」に「発行者ＩＤ」を含ませることも、引用文献を提示するまでもなく、当業者に周知の技術事項であるから、引用発明において、「セキュリティデバイス証明書」に、「セキュリティデバイス１０２」のＩＤ、「ＣＰ３０３」のＩＤ等を含ませるよう構成すること（相違点２に係る本願発明の構成とすること）は、当業者が必要に応じて適宜なし得る事項である旨判断した。

しかし、「デバイス証明書」に「署名」を含むこと自体は、引用文献３及び４に開示された「公開鍵証明書」にあるように周知技術ではあるが、一方で、相違点２に係る本願発明の構成は、「クライアント装置の装置ＩＤ、発行者ＩＤ、前記プライベートキーの関数である公開鍵及び前記クライアント装置の不揮発性メモリから読み出された第１の署名の関数として生成されたデバイス証明書」というものであり、本願発明の「デバイス証明書」に含まれる「第１の署名」は、「第１の署名の関数」として「デバイス証明書」を生成するためのものであるから、引用文献３及び４記載のような「デバイス証明書」に単に「署名」を含むものと異なるものである。

また、引用文献１には、本願発明の「第１の署名の関数」に対応する記載はないし、引用文献３及び４に開示された「公開鍵証明書」に含まれる「署名」は、本願発明の「第１の署名」と同一視できるものではない。

したがって、相違点２に係る本願発明の構成は、引用発明及び引用文献２ないし４記載の技術事項に基づいて当業者が必要に応じて適宜なし得る事項であるとはいえないから、本件審決の上記判断は誤りである。

イ　これに対し被告は、相違点２に係る本願発明の構成である「クライアント装置の装置ＩＤ、発行者ＩＤ、前記プライベートキーの関数である公開鍵及び前記クライアント装置の不揮発性メモリから読み出された第１の署名の関数として生成されたデバイス証明書」とは、「デバイス証明書」が、「クライアント装置の装置ＩＤ、発行者ＩＤ、プライベートキーの関数である公開鍵」と、これらを暗号化して生成される「第１の署名」とを含み、「クライアント装置の装置ＩＤ、発行者ＩＤ、プライベートキーの関数である公開鍵」に「第１の署名」を付して生成されるものであることを特定するものであるとした上で、本願発明の「第１の署名」は、引用文献３及び４に開示された「電子署名」と同等のものといえるから、本件審決における相違点２の容易想到性の判断に誤りはない旨主張する。

しかしながら、本願の願書に添付した明細書（以下、図面を含めて「本願明細書」という。甲１）には「第１の署名」について「これらを暗号化して生成される」との記載はなく、【００６２】には、「デバイス証明書が、装置ＩＤ、発行者ＩＤ、公開鍵、署名、及び共通パラメータから作成される」こと（「デバイス証明書」に「署名」が含まれること）の記載があるのみであるから、本願明細書を参酌しても、本願発明の「デバイス証明書」が、「クライアント装置の装置ＩＤ、発行者ＩＤ、プライベートキーの関数である公開鍵」と、これらを暗号化して生成される「第１の署名」とを含むものと解釈することはできない。

したがって、被告の上記主張は、その前提において失当である。

⑶　相違点の看過

引用発明は、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」との構成を備えるものではない点で本願発明と相違するが、本件審決は、この点を相違点として認定していないから、本件審決には、かかる相違点を看過した誤りがある。

すなわち、本願明細書の【００１６】には「サーバ１０２における証明書検証モジュール１１２は、信頼できる証明書チェーン(trusted certificate chain)を用いて、証明書Ｃｅｒｔを認証し」との記載があること、証明書チェーンは、認証パスとも呼ばれ、クライアント、サーバなどの証明書から、中間認証局の証明書、ルート認証局の証明書までの連なりであり、チェーン内の各証明書が次の証明書よって署名されることでセキュリティを確保するように構成されていることは技術常識であることからすると、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」とは、「デバイス証明書」は「証明書チェーン」を用いて認証され、「第２の署名」は「デバイス証明書」に含まれる公開鍵によって認証されることを意味するものと解されるが、引用文献１には、引用発明における「セキュリティ

デバイス証明書を用いて検証する」との構成が、このような認証を意味することを示した記載はないから、引用発明は、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」との構成を備えるものでない点で本願発明と相違する。

これに対し被告は、引用文献１の【００５７】の「電子署名を…セキュリティデバイス証明書を用いて検証する」との記載は、「セキュリティデバイス」が「セキュリティデバイス秘密鍵」を保持していることを「検証」することを意味するものであり、また、セキュリティデバイス証明書を用いて検証するためには、当該セキュリティデバイス証明書が正当なものであることが確認できなければならないから、引用発明は、「セキュリティデバイス証明書」と「電子署名」とをそれぞれ認証するものであるとして、上記相違点の看過はない旨主張する。

しかし、「セキュリティデバイス証明書を用いて検証する」とは、あくまで「セキュリティデバイス証明書」に含まれている情報を検証することであって、「セキュリティデバイス証明書」そのものを認証するものとはいえないから、被告の上記主張は失当である。

⑷　小括

以上のとおり，本件審決には，一致点の認定の誤り、相違点２の容易想到性の判断の誤り及び相違点の看過があるから、本願発明は，引用発明及び引用文献２ないし４記載の技術事項に基づいて，当業者が容易に発明をすることができたものであるとした本件審決の判断は，誤りである。

したがって、本件審決は取り消されるべきものである。

２　被告の主張

⑴　一致点の認定の誤りの主張に対し

ア　「クライアント装置」に係る一致点の認定の誤りの主張に対し

本願発明の特許請求の範囲（請求項１）には、サーバとクライアント装

置との接続が直接であるか間接であるかについて特定がされておらず、サーバとクライアント装置との間に機器が介在する構成が排除されていないこと、引用発明の「セキュリティデバイス１０２」は、その機能を見ても、「ＣＰ３０３」の「証明書要求部」から「前記乱数を含む、セキュリティデバイス証明書を要求するリクエスト」が送信されてこれを受信し、「セキュリティデバイス証明書と、前記乱数に対して施した電子署名とを応答として」返信した上で、「ＣＰ３０３」において、「前記セキュリティデバイス証明書を用いて検証」されるものであり、「サーバ」によって認証される「クライアント装置」といい得ることからすると、引用発明の「セキュリティデバイス１０２」が本願発明の「クライアント装置」に相当することは明らかである。

したがって、引用発明の「セキュリティデバイス１０２」が本願発明の「クライアント装置」に相当するとした本件審決の一致点の認定に誤りはない。

また、仮に引用発明の「セキュリティデバイス１０２」と「情報端末１０１」とを合わせたものを、本願発明の「クライアント装置」に相当するものと対比したとしても、引用発明が「クライアント装置」を備える点で本願発明と一致することに変わりはないから、本件審決の結論に影響しない。

イ　「第２の署名」に係る一致点の誤りの主張に対し

「電子署名」は、乱数などの「情報Ａ」を公開鍵暗号方式で用いられる「公開鍵－秘密鍵」ペアの「秘密鍵」で暗号化して生成され、「公開鍵」を用いて「署名検証」されるものであることは、技術常識である（乙１，２）。

本願発明の特許請求の範囲（請求項１）には、「第２の署名」について、「前記クライアント装置において…プライベートキーと前記サーバの数発生器が作成した第１の数を使用して生成される」との記載があるところ、

本願明細書の【００１５】及び【００１６】記載の「署名Ｓｉｇ」及び「乱数Ｒ」は、それぞれ本願発明の「第２の署名」及び「第１の数」に対応するものである。そして、上記技術常識を踏まえると、本願発明の「第２の署名（署名Ｓｉｇ）」は、サーバから送られた「第１の数（乱数Ｒ）」を、クライアント装置の「プライベートキー」で暗号化して生成され、「証明書Ｃｅｒｔ」を用いて署名検証されるものと理解できる。

一方、引用文献１の【００５３】及び【００５４】の記載と上記技術常識によれば、引用発明の「電子署名」は、ＣＰ３０３から送られてきた「乱数」を「セキュリティデバイス１０２」の「秘密鍵」で暗号化して生成され、「セキュリティデバイス証明書」の「公開鍵」を用いて「署名検証」されるものと理解できる。

そうすると、引用発明の「電子署名」と本願発明の「第２の署名」とは、証明書に付された電子署名として、その生成についても署名検証についても相違するところはないから、引用発明の「電子署名」は、本願発明の「第２の署名」に相当するものといえる。

したがって、本願発明と引用発明は、「レスポンス」が「該クライアント装置の製造中にプログラムされたプライベートキーと前記サーバの数発生器が作成した第１の数を使用して生成される第２の署名」を含む点で一致するとした本件審決の一致点の認定に誤りはない。

⑵　相違点２の容易想到性の判断の誤りの主張に対し

本願発明の特許請求の範囲（請求項１）の「前記クライアント装置の装置ＩＤ、発行者ＩＤ、前記プライベートキーの関数である公開鍵及び前記クライアント装置の不揮発性メモリから読み出された第１の署名の関数として生成されたデバイス証明書」の記載（相違点２に係る本願発明の構成）の意味は直ちには明確とはいえない。

しかるところ、本願明細書の【００２３】の「デバイス証明書は公知のも

のである」との記載、セキュア証明書（デバイス証明書）の作成方法の例を示したフローチャートである図７のうちステップ７０８の記載及び【００６２】の記載を参酌するとともに、公開鍵証明書に関する技術常識（乙１，２）を踏まえれば、請求項１の上記記載は、「デバイス証明書」が、「クライアント装置の装置ＩＤ、発行者ＩＤ、プライベートキーの関数である公開鍵」と、これらを暗号化して生成される「第１の署名」とを含み、「クライアント装置の装置ＩＤ、発行者ＩＤ、プライベートキーの関数である公開鍵」に「第１の署名」を付して生成されるものであることを特定していると理解できる。

そうすると、本願発明の「第１の署名」は、「デバイス証明書」に含まれる、「プライベートキーの関数である公開鍵」によって署名検証がされると解されるので、引用文献３及び４に開示された「電子署名」と同等のものといえるから、本件審決における相違点２の容易想到性の判断に誤りはない。

⑶　相違点の看過の主張に対し

原告は、本願明細書の【００１６】の記載を根拠として、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」にいう「デバイス証明書」の「認証」とは、「証明書チェーン」を用いて認証することを意味するが、引用文献１には、引用発明における「セキュリティデバイス証明書を用いて検証する」との構成が、このような認証を意味することを示した記載はないから、引用発明は、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」との構成を備えるものでない点で本願発明と相違し、本件審決には、かかる相違点の看過がある旨主張する。

ア　しかし、本願発明の特許請求の範囲の請求項１には、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」にいう「認証」の具体的な認証方法について特定する記載がないこと、本願明細書の【００１６】には、サーバが受け取った証明書Ｃｅｒｔを，信頼

できる証明書チェーンを用いて認証することが記載されているが、これは、証明書Ｃｅｒｔ（デバイス証明書）の認証に係る一実施形態の記載にすぎないことからすると、当該「認証」が証明書チェーンを用いるものであると限定解釈する必要はない。

イ　引用文献１の【００５７】に、「アプリケーション発行要求８１３を受信したＣＰ３０３は、アプリケーション発行要求８１３に含まれていた電子署名（セキュリティデバイス証明書要求８０２または８１１に含まれていた乱数に対する電子署名）を同じくアプリケーション発行要求８１３に含まれていたＣＰ３０３が発行したセキュリティデバイス証明書を用いて検証して（署名検証８１４）、セキュリティデバイス１０２がＣＰ３０３が発行したセキュリティデバイス証明書に対応するセキュリティデバイス秘密鍵を保持していることを検証し」と記載されているように、引用発明のＣＰ３０３は、「電子署名」を「セキュリティデバイス証明書」を用いて「検証」することによって、「セキュリティデバイス秘密鍵」を保持していることを「検証」するものであり、これは、本願発明の「デバイス証明書」を「認証」することに対応する。

そして、「セキュリティデバイス証明書」を用いて「電子署名」を検証するためには、まず、当該「セキュリティデバイス証明書」が正当なものであることが確認できなければならないが、そのためには、当該「セキュリティデバイス証明書」が正当なものであることを検証することができる情報が含まれていなければならないこと、公開鍵証明書に関する技術常識を踏まえれば、当該「セキュリティデバイス証明書」には、「公開鍵」に加えて、当該「セキュリティデバイス証明書」が正当なものであることを保証する「署名（署名値）」が含まれることは、当業者にとって明らかである。

そうすると、引用発明のＣＰ３０３は、「セキュリティデバイス証明書」を受け取れば、当然に当該「署名（署名値）」を署名検証し、「セキュリテ

ィデバイス証明書」に含まれている情報が改ざんされていないことを確かめることになり、これは、「セキュリティデバイス証明書」を認証することにほかならないから、引用発明は、「セキュリティデバイス証明書」と「電子署名」とをそれぞれ認証するものである。

したがって、本件審決には、原告主張の相違点の看過はない。

⑷　小括

以上のとおり，本件審決における一致点の認定及び相違点２の容易想到性の判断に誤りはなく、また、本件審決に相違点の看過はないから、本願発明は，引用発明及び引用文献２ないし４記載の技術事項に基づいて，当業者が容易に発明をすることができたものであるとした本件審決の判断に誤りはない。

したがって、原告主張の取消事由は理由がない。

第４　当裁判所の判断

１　一致点の認定の誤りについて

⑴　本願明細書の記載事項

本願明細書（甲１）には、次のような記載がある（下記記載中に引用する図１、３、５ないし７については別紙１を参照）。

ア　【技術分野】

【０００１】

セキュアプロセッサは通常、ＩＤ、及び／又は格納された秘密鍵を含む。セキュリティレベルを高めるために、ある量(quantities)の秘密鍵などが、チップ内不揮発性メモリにプログラミングされて、セキュアプロセッサを作ることがある。ＩＤ及び秘密鍵のプログラミングは、チップのセキュア製造プロセスにおいて行われる。それぞれのＩＤは固有のものであり、プライベートキーも又固有のものである。これらの量(these quantities)は、デジタル権利管理や他のセキュリティ関連アプリケーションを実行する

ため、装置上のアプリケーションで使用される。通常、チップは、ネットワーク・プロトコル、秘密鍵などにおいて、使い捨てデータとして使用するために、暗号学的に強力な乱数を生成するメカニズムを含む。

【背景技術】

【０００２】

デジタル権利管理を実行するために使用される典型的なインフラにおいて、サーバは、装置に対する権利を有効にするため、デジタル的に署名されたチケットを供給するのに使用される。そのようなチケットは、装置にチケットを結びつけるために、かかる装置のアイデンティティ、及び／又は秘密鍵メカニズムを使用する。それぞれの装置ＩＤ／鍵の独自性を確実にするため、サーバは通常、セキュア・データベースを使って、製造された各チップに対応するＩＤ（及び／又は署名された証明書）を格納している。これらの証明書は、チップにプログラミングされた各秘密鍵（(プライベートキー、公開鍵）ペアのプライベートキー）に対応する公開鍵を含んでいる。データベースに証明書を投入するためには、データベースに関連するインフラを確実に製造プロセスに結び付け、製造されたチップとデータベース内の証明書の間で１対１対応を維持しなければならない。

【０００３】

上述したこれら関連技術の例や制限事項は、あくまで説明に役立つものとして例証したものであって排他的ではない。関連技術の他の制限事項は、当該技術者が本願明細書を読み、図面を検討することにより明らかになるであろう。

【発明が解決しようとする課題】

【０００４】

以下の実施形態とその特徴は、あくまで例証的であって範囲を制限しないことを意図したシステム、ツール、および方法に関連して記載、図示さ

れる。種々の実施形態では、上述した問題の１つ又はそれ以上が低減又は解消され、一方では他の実施形態がその他の改善に向けられる。

【０００５】

改善されたセキュア・プログラミング技術は、セキュアデバイスによってサポートされる典型的なセキュア・アプリケーションを可能とすると同時に、オンチップ秘密不揮発性メモリにプログラミングされるビットサイズを減少させることを含む。また、改善されたセキュア・プログラミング技術は、システムの製造プロセスを簡素化することを含む。一実施形態において、秘密事項のプログラミングは、オンチッププログラミングに対し分離されており、特にシステム統合やインフラ設定のプロセスからは分離される。

イ　【課題を解決するための手段】

【０００６】

セキュア・プログラミング技術は、チップの製造を、チケットを取得するために、チケットサーバに接続する後処理から分離させることを含む。この技術に沿った方法は、チケットを受け取るための如何なる通信に先だって、装置から（製造）サーバの署名が入った証明書を送ることを含んでも良い。この方法は、データベースを投入し、例えばちょうどチケットサービスが必要となる時など、後のチケットサービス実行を容易にすることを含んでも良い。

【０００７】

本技術に沿った装置は、製造プロセスにおいて、証明書をプライベートキーと共に格納するためのチップ内不揮発性メモリを含んでも良い。プライベートキーは、楕円カーブをベースとするプライベートキーであっても、またそうでなくとも良い。楕円カーブの暗号ベースの鍵の長所は、相対的な暗号強度にしては、多くの種類の鍵より小さいことである。更に、楕円

曲線アルゴリズムを使用し、無作為のプライベートキーを保存すると共に、ランタイム計算によって公開鍵を算出することが可能である。

【０００８】

有利な点としては、特にオンチップ・リアルエステートを考慮して、圧縮された証明書を不揮発性メモリ内に設けることが可能なことがある。（デバイス証明書を保存するために必要とされるものより）より小さなデータセットを使用して、かかる装置はデバイス上にダイナミックに証明書を作成し、それを要求するアプリケーションに提供する。デバイス証明書を複数回作っても、また作らなくとも良い。例えば、一旦デバイス証明書を作成し、更なる使用に備えてシステムの外部記憶装置に格納するようにしても良い。このことは証明書が公知データであるため、特に不安定なことではない（セキュアでない訳ではない)。

【０００９】

本技術によって構築された装置は、他の分野においても適用性を持つ可能性がある。例えば、ピア又は、第１のデバイス証明書を必要とする如何なるアプリケーションに対しても装置を認証することができる。またこれとは別に、不揮発性メモリにプログラミングするためのセキュアな製造プロセスを使い、不揮発性メモリは、装置のためのセキュアな乱数発生器を含んでも良い。

ウ　【発明を実施するための形態】

【００１１】

以下の説明では、本発明の実施形態の十分な理解を与えるために幾つかの特定の具体的な構成が提示される。しかし、当業者であれば、１つ以上のこれら特定の具体的な構成がなくとも、あるいは他の構成部などとの組み合わせにより、本発明を実施することが可能であることが理解されるであろう。また別の例では、様々な実施形態における本発明の側面を覆い隠

すことがないように、周知の具体的構成は、図示または詳細に説明されていない。

【００１２】

図１は、サーバにおいてクライアントを認証する(validating)ためのシステム１００の一例を示している。図１の例でシステム１００は、サーバ１０２、ネットワーク１０４、及びクライアント１０６を含む。サーバ１０２は、証明書リクエストモジュール１１０、証明書検証モジュール１１２、証明書データベース１１４、擬似乱数（ＰＲＮ）発生器１１６、及びインターフェース１１８を含む。クライアント１０６は、証明書作成モジュール１２０、不揮発性（ＮＶ）メモリ１２２、及びインターフェース１２４を含む。

【００１３】

サーバ１０２は、如何なる適用可能な公知の（又は手頃な）コンピュータであっても良い。ネットワーク１０４は、非限定的な例として、インターネットを含む如何なる通信ネットワークでも良い。クライアント１０６は、セキュア記憶装置(技術的に安全性が保証された記憶装置)を有する、如何なる適用可能な公知の（又は手頃な）コンピュータであっても良い。不揮発性メモリ１２２はセキュア鍵ストアを含んでもよく、一実施形態では同不揮発性メモリ１２２はオンチップメモリである。

【００１４】

図１の例では、動作において、レジストレーション(registration)用又はアクティベーション(activation)用プロトコルが、サーバ１０２によって起動される（或いは、クライアント１０６が、レジストレーション又はアクティベーションを起動するようにしても良い)。一実施形態では、プロトコルは、装置の同一性(a device identity)を登録(register)したり、証明書データベース１１４に証明書を与えたりする（certificate into）役

割を果たす。そのために、乱数発生器１１６は、乱数Ｒを生成し、サーバ１０２の証明書リクエストモジュール１１０は、デバイス証明書のリクエストを生成する。乱数Ｒとデバイス証明書のリクエストは、インターフェース１１８を介して、ネットワーク１０４へと送られる。

【００１５】

乱数Ｒとデバイス証明書のリクエストは、クライアント１０６のインターフェース１２４で受け取られる。クライアント１０６の証明書作成モジュール１２０は、証明書Ｃｅｒｔを作成する。証明書Ｃｅｒｔを作成するのに使用されるアルゴリズム例としては、図７を参照して以下に説明する。証明書作成モジュール１２０は、デバイス・プライベートキーを使用し、乱数Ｒ上の署名Ｓｉｇを算出する。オペランド(operands)は、不揮発性メモリ１２２に格納されているが、それらは例えばセキュリティカーネル（図５参照）にあるようにしても良い。また別の実施形態では、上記演算には、装置ＩＤ、シリアルナンバー、リージョンコード、或いはその他幾つかの数値を含む場合もある。クライアント１０６のインターフェース１２４は、ネットワーク１０４に対し、乱数Ｒや何らかの任意データ、証明書Ｃｅｒｔ、及び証明書Ｓｉｇを返す。

【００１６】

サーバ１０２Ｒは、インターフェース１１８で、乱数Ｒ、任意データ、証明書Ｃｅｒｔ、及び署名Ｓｉｇを受けとる。サーバ１０２における証明書検証モジュール１１２は、信頼できる証明書チェーン(trusted certificate chain)を用いて、証明書Ｃｅｒｔを認証し、証明書Ｃｅｒｔを用いて署名Ｓｉｇを認証し、更に乱数Ｒが、元々サーバ１０２によってクライアント１０６に送られた乱数Ｒと同じであるか否かを検証する。これらの認証及び検証が成功裏に完了したならば、サーバ１０２は、証明書データベース１１６に証明書Ｃｅｒｔを取り込む。この時点で、クライア

ント１０６が、サーバ１０２から（或いはクライアント１０６に許可を与える証明書を使用できる、その他幾つかのロケーションから）権利管理コンテンツ(rights managed content)やその他のオペレーションのためのデジタルライセンスを獲得することについて、推定上許可されることになる。

【００１７】

その他の実施形態としては､装置がＲＮＧを使って新しい鍵のペア{pvt1、pub1} を作成し、署名者としてプライベートキーがプログラミングされた装置を使用して、この新しい公開鍵 pub1 のために証明書が作成される場合もある。この新しい鍵 pvt1 は、乱数Ｒを持つメッセージに署名するのにつかわれる場合もある。

【００２３】

図３は、一回だけデバイス証明書を作成する方法の一例のフローチャート３００を示している。図３の例では、フローチャート３００は、モジュール３０２で始まり、ここでデバイス証明書がセキュアデバイスで作成される。次いでフローチャート３００は、モジュール３０４に進み、該デバイス証明書がシステムの外部記憶装置に格納される。装置はセキュア（技術的に安全性が保証されたもの）であるために、この変化(variation)は注目に値するが、デバイス証明書は公知のものである。従って、それはその都度、再生されないが、証明書は依然としてセキュアなものである。

エ　【００３９】

図５は、図１乃至図３を参照して上述した技術を実施するのに適していたセキュアシステム５００の一例を示している。代表的なセキュアシステム５００は、ゲーム機、メディアプレーヤー、埋め込み型(embedded)セキュアデバイス、セキュアプロセッサ付き“従来型”PC、或いはセキュアプロセッサを備える他のコンピュータ・システムを備えても良い。

【００４９】

図５の例では、チケットサービス５０６とセキュリティ API５１８は、システムセキュリティのための個々の実行スペースにおいて実行してもよい。データブロックを有効化するために、チケットサービス５０６は、ヘッダのデータを使ってチケットを有効にしても良い。そのチケットは、暗号化された鍵を含んでも良い。チケットサービス５０６は、セキュリティカーネル５１４におけるサービス（例えば、暗号化/復号化エンジン５１７）を利用して、鍵を復号化する。

【００５１】

矢印５２０～５２８を以て、システム５００のデータフローの例が例示を目的として供される。チケットサービス５０６での証明書リクエストの受取りは、呼出しアプリケーション５０８からチケットサービス５０６への証明書リクエスト矢印５２０によって表わされる。

【００５２】

チケットサービス５０６からセキュリティ API５１６への証明書リクエストの送りは、証明書リクエスト矢印５２２によって表されている。セキュリティカーネル５１４において、公開鍵／デバイス証明書・作成エンジン５１７は、鍵/署名ストア５１８からの鍵／署名データにアクセスする。このアクセスは、プライベートキー／署名アクセス矢印５２４によって表されている。セキュリティ API５１６は、デバイス証明書矢印５２６に示すように、デバイス証明書をチケットサービス５０６に返し、それは更にデバイス証明書矢印５２８に示すように、呼出しアプリケーション５０８に転送される。

オ　【００５３】

図６は、セキュアデバイスを製造する方法の例を示すフローチャート６００である。この方法、及び他の方法は、連続的に並べられたモジュールの形で表現される。しかしながら、これらの方法における各モジュールは、

並べ替えされたり、並列実行のために適当に並べられたりしても良い。図６の例において、フローチャート６００は、モジュール６０２でスタートし、ここで装置ＩＤが取得される。装置ＩＤは、シリアルナンバーであっても、或いは装置のための他の何らかの固有な識別子であっても良い。

【００５４】

図６の例で、フローチャート６００は、モジュール６０４に進み、ここでは装置のために小署名プライベートキー(a small-signature private key)として使用する目的で、擬似乱数が供される。今日に至るまで、本当の意味での乱数というものはコンピュータ上では生成できないが、当然のことながら、疑似乱数発生器や外部のセキュアなハードウェアにおける真性乱数発生器が、ここで意図する目的のために使用できるだろう。小署名プライベートキーは、これに限定されない例として、楕円カーブプライベートキーや比較的小さなフットプリント(footprint)を持った他の何らかのプライベートキーでも良い。

【００５５】

図６の例で、フローチャート６００は、モジュール６０６に進み、ここでは共通パラメータを使用してプライベートキーから公開鍵が算出される。例えば、スカラー倍数(scalar multiple)がプライベートキーとなるように、基点(base point)の倍数が算出されても良い。

【００５６】

図６の例で、フローチャート６００は、モジュール６０８に進み、ここでは一定の証明書構造(fixed certificate structure)が、証明書を作成するために使用される。証明書は、例えば楕円カーブＤＳＡなどの小署名アルゴリズム(small signature algorithm)を使用して署名される。一実施形態では、該一定の証明書構造は、少なくとも装置ＩＤ、発行者名、及びデバイス公開鍵を含むかもしれない。小署名アルゴリズムは、署名サイ

ズを最小限におさえるのに使用される。これに限定されない例として、楕円カーブ署名アルゴリズムが使用されても良い。

【００５７】

図６の例で、フローチャート６００は、モジュール６１０に進み、ここでは｛装置ＩＤ、プライベートキー、発行者ＩＤ、署名｝が、装置の不非揮発性メモリにプログラミングされる。このセットは、これらのアイテムが殆どの目的に対して充分セキュリティを提供するという理由でこれら４つのアイテムを含んでおり、また該セットは、比較的小さいサイズのプライベートキーと署名のおかげで比較的小さいフットプリントを有する（推定するに、装置ＩＤ及び発行者ＩＤも又、比較的小さいフットプリントを有している)。一実施形態では、例えば公開鍵など、デバイス証明書の作成(construct)に必要とされる如何なるデータも、要求に応じてプログラミングされた状態で生成されても良い。しかしながら、与えられた実施形態や実装に見合った形で、より多くのアイテム、又より少ないアイテムが不揮発性メモリにプログラミングされ得る。

【００５８】

図６の例では、フローチャート６００は、モジュール６１２に進み、秘密の乱数が装置のＲＯＭにプログラミングされる。この秘密乱数は、疑似乱数的に生成されても、また任意に割り当てられるようにしても良い。この秘密乱数は、セキュアな擬似乱数の生成をサポートするのに利用できる。また別の実施形態では、ＲＯＭが、他の公知の（又は手頃な）不揮発性記憶装置と置き換えられても良い。

カ　【００５９】

図７は、セキュア証明書の作成方法の例を示したフローチャート７００である。メリットとして、この方法は、不揮発性でプログラミングされた鍵と必要なソフトウェアを有する装置が、装置認証に使用可能な完全なデ

バイス証明書を作成することを可能にする。図７の例では、フローチャート７００は、モジュール７０２でスタートし、ここではデバイス証明書のリクエストが、呼出しアプリケーションから受け取られる。

【００６０】

図７の例で、フローチャート７００は、モジュール７０４に進み、ここでは｛装置ＩＤ、プライベートキー、発行者ＩＤ、署名｝が、不非揮発性メモリから読み込まれる。一実施形態では、セキュリティカーネル・モジュールが、不揮発性メモリにアクセスして読み込む。この目的のために適切なセキュリティカーネル・モジュールの例としては、Srinivasanらによって２００３年２月７日に出願された“信頼性や下位互換性のあるプロセッサ及びその上でのセキュアソフトウェア実行”というタイトルの米国出願第１０／３６０、８２７号や、Srinivasanらによって２００６年１０月２４日に出願された“セキュアデバイス認証システム及び方法”というタイトルの米国出願第１１／５８６、４４６号に記載されている。しかしながら、如何なる適用可能な公知の（又は手頃な）セキュリティカーネル・モジュールでも使用可能である。

【００６１】

図７の例で、フローチャート７００は、モジュール７０６に進み、ここでは公開鍵が、プライベートキーと（もしあるならば）共通パラメータとによって算出される。一実施形態では、この演算は、図６を参照して上述した方法のような製造プロセスに使用されたのと同じアルゴリズムを利用する。公開鍵は、セキュリティカーネルで算出されても良い。

【００６２】

図７の例で、フローチャート７００は、モジュール７０８に進み、ここではデバイス証明書が、装置ＩＤ、発行者ＩＤ、公開鍵、署名、及び共通パラメータから作成される。一実施形態において、セキュリティカーネル・

モジュールは、図６を参照して上述した方法のような製造プロセスで使用されおり、該デバイス証明書の構造を認識している。メリットとして、デバイス証明書は、要求に応じて作成できる。

【００６５】

ここで使用されたように、用語“実施形態”は、それに限定されない一例として説明を行うための実施例を意味している。

【００６６】

当業者であれば前述した実施例と実施形態は、代表的なものであり、本発明の範囲を限定するものでないことが理解されるであろう。当業者が明細書を考慮し、図面を検討したときに自明な置き換え、増強、均等物やそれらへの改良が、本発明の要旨と範囲に含まれることを意図している。したがって、添付された特許請求の範囲は、本発明の要旨と範囲内にあるこのような総ての変更、置き換え、均等物を含むことを意図している。

⑵　引用文献１の記載事項

引用文献１（甲６）には、次のような記載がある（下記記載中に引用する図１ないし４、８、２１については別紙２を参照）。

ア　【技術分野】

【０００１】

本発明は、データを盗聴、改竄等から安全に保持するＩＣカード等のセキュリティデバイスと、そのセキュリティデバイスを装着した携帯電話やＰＤＡ（Personal Digital Assistant）、パーソナルコンピュータなどの情報端末に関するもので、特に、電子マネーや電子チケット、音楽や画像、映像などのデジタルコンテンツ等の価値情報を扱う機器に関するものである。

【背景技術】

【０００２】

近年、ＣＰＵと耐タンパ性のある記憶領域を持つＩＣカード等のセキュリティデバイスは、カードアプリ（アプリはアプリケーションの略である。以下同様である）を動作させることが可能であり、電子マネーや定期券、電子チケット等のサービスに利用されている。

【０００３】

例えば、前述したセキュリティデバイスが携帯電話等の情報端末に内蔵されたものがある。これによれば、情報端末のキーボードやディスプレイをセキュリティデバイスに対するユーザインターフェイスとして使用することができる。また、セキュリティデバイスに書き込むデータや読み出したデータを、情報端末の通信機能を利用してネットワーク上で伝送することができるので、様々なサービスを利用することができる。この場合、それらのサービスを実行する際に情報端末が行うべき動作を規定した端末アプリが情報端末上で動作する。

【０００４】

従来、情報端末は、サービスプロバイダからネットワークを通じて端末アプリをダウンロードするなどして、この端末アプリを取得している。例えば、図２１に示すように、セキュリティデバイス２１１１に保持された電子マネーや電子チケット等の価値情報２１１３をオフライン環境下で表示する端末アプリ２１０８を、サービスプロバイダ２１２１からダウンロードする携帯端末２１０１が開示されている（特許文献１参照）。

【０００５】

この携帯端末２１０１は、端末アプリ２１０８のダウンロード及びそのダウンロードした端末アプリ２１０８を実行するプログラム制御部２１０２と、ダウンロードした端末アプリを記憶する格納部２１０３と、サービスプロバイダ２１２１との通信を行う通信部２１０４と、ユーザがサービスプロバイダ２１２１のＵＲＬを入力するユーザ入力部２１０５と、Ｌ

ＣＤ等の表示部２１０６と、を備えている。また、プログラム制御部２１０２には、さらに、ダウンロードした端末アプリを検証する検証部２１０７を備えている。一方、セキュリティデバイス２１１１は、内部のメモリに記憶されている価値情報２１１３を管理するカードアプリ２１１２を備えている。

【０００６】

このセキュリティデバイス２１１１に蓄積された価値情報２１１３を、オフライン環境下において携帯端末２１０１を用いて参照する場合、ユーザは、まず、ユーザ入力部２１０５にサービスプロバイダ２１２１のサーバに格納されている端末アプリ２１０８のＵＲＬを入力する。入力されたＵＲＬはプログラム制御部２１０２に渡され、プログラム制御部２１０２は渡されたＵＲＬに基づいて通信部２１０４を介してサービスプロバイダ２１２１のサーバと通信し、サービスプロバイダ２１２１から端末アプリ２１０８をダウンロードし（1）、検証部２１０７において端末アプリ２１０８の検証を行い（2）、問題がなければ端末アプリ２１０８を格納部２１０３に保存する（3）。

【０００７】

ユーザによって端末アプリ２１０８の起動操作が行われると、プログラム制御部２１０２は格納部２１０３から端末アプリ２１０８を読み出し、起動する（4）。起動された端末アプリ２１０８は、携帯端末２１０１に装着されたセキュリティデバイス２１１１のカードアプリ２１１２に価値情報２１１３を要求する（5）。カードアプリ２１１２は、内部のメモリに記憶されている価値情報２１１３を読み出して携帯端末２１０１側に送り（6）、端末アプリ２１０８は、取得した価値情報２１１３を携帯端末２１０１の表示部２１０６に表示する処理を行う（7）。

【発明が解決しようとする課題】

【０００８】

しかしながら、上記従来技術では、以下に示すような問題点があった。すなわち、セキュリティデバイス２１１１は、サービスプロバイダ２１２１から端末アプリケーション２１０８をダウンロードし、検証部２１０７において検証を行い、格納部２１０３に保存する。しかし、一度検証を経て保存された端末アプリケーション２１０８は再び検証される機会がない。そのため、一度検証を経て保存された端末アプリケーション２１０８に対して、価値情報２１１３へのアクセスの制限などを解除する改竄が施された場合は、セキュリティデバイス内の価値情報２１１３が不正に使用される恐れがあり、セキュリティの観点から好ましくない。また、サービスプロバイダからダウンロードしたコンテンツについても同様の問題が生じる。

【０００９】

本発明は、上記実情を鑑みてなされたものであり、改竄が加えられたアプリケーション等の実行を防ぐことができるセキュリティデバイスを提供することを目的とする。

イ　【課題を解決するための手段】

【００１０】

本発明のセキュリティデバイスは、内部に保持された価値情報を外部端末から参照するためのアプリケーションを記憶する記憶手段と、前記アプリケーションの同一性を保証する加工処理を行う加工手段と、加工処理したアプリケーションを記憶する記憶手段と、加工処理したアプリケーションを前記外部端末に対して発行する発行手段とを備える。また、本発明のセキュリティデバイスは、外部端末で再生するコンテンツを記憶する記憶手段と、前記コンテンツの同一性を保証する加工処理を行う加工手段と、加工処理したコンテンツを記憶する記憶手段と、加工処理したコンテンツ

を前記外部端末に対して発行する発行手段とを備える。また、本発明のセキュリティデバイスは、外部端末で再生するコンテンツを記憶する記憶手段と、前記コンテンツの同一性を保証する加工処理を行う加工手段と、加工処理したコンテンツを記憶する記憶手段と、加工処理したコンテンツを前記外部端末に対して発行する発行手段と、前記コンテンツを再生するアプリケーションを記憶する記憶手段と、前記アプリケーションの同一性を保証する加工処理を行う加工手段と、加工処理したアプリケーションを記憶する記憶手段と、加工処理したアプリケーションを前記外部端末に対して発行する発行手段とを備える。

【００１１】

上記構成によれば、セキュリティデバイスが保持する価値情報を外部端末で参照するアプリケーションや外部端末で再生するコンテンツに対してセキュリティデバイス側でアプリケーション、コンテンツの同一性を保証する加工処理を施した上で外部端末に発行することで、外部端末がアプリケーションの起動毎、コンテンツの再生毎にアプリケーション、コンテンツの同一性を検証することが可能となり、改竄したアプリケーションの実行、コンテンツの再生を防ぐことができる。

【発明の効果】

【００１２】

本発明によれば、セキュリティデバイスが保持する価値情報を外部端末で参照するアプリケーションや外部端末で再生するコンテンツに対してセキュリティデバイス側でアプリケーション、コンテンツの同一性を保証する加工処理を施した上で外部端末に発行することで、外部端末がアプリケーションの起動毎、コンテンツの再生毎にアプリケーション、コンテンツの同一性を検証することが可能となり、改竄したアプリケーションの実行、コンテンツの再生を防ぐことができる。

ウ　【発明を実施するための最良の形態】

【００１３】

以下、本発明の実施の形態を、図面を参照しながら説明する。

（実施の形態１）

図１に、本発明の第１の実施の形態におけるセキュリティデバイス１０２と情報端末１０１のシステム構成を示す。

【００１４】

セキュリティデバイス１０２は、耐タンパ機構を有し、その内部で安全なデータ処理を行う耐タンパデータ処理部１５０と、耐タンパデータ処理部１５０が処理したデータを格納するフラッシュメモリ１５１と、耐タンパデータ処理部１５０が情報端末１０１などのホスト機器との通信を制御するホスト機器通信手段１５７と、によって構成される。

【００１５】

耐タンパデータ処理部１５０は､内部にＣＰＵやＲＯＭ､ＥＥＰＲＯＭ、ＲＡＭ、更には、暗号処理用のコプロセッサを有し、ＲＯＭおよびＥＥＰＲＯＭに格納されたプログラムに基づいてＣＰＵがＲＡＭおよびフラッシュメモリ１５１を用いてデータ処理を行う。

【００１６】

耐タンパデータ処理部１５０には、ホスト機器通信手段１５７を介して外部から端末アプリケーションを受信するアプリケーション取得手段１５３と、

端末アプリケーションに対して、認証情報の埋め込みや、電子署名などの加工処理を施すアプリケーション加工手段１５２と、加工処理を施した端末アプリケーションを情報端末１０１に対して発行するアプリケーション発行手段１５４と、があり、これらは、実際には、耐タンパデータ処理部１５０の内部のＲＯＭやＥＥＰＲＯＭに格納されているプログラムを

耐タンパデータ処理部１５０のＣＰＵが実行することによって実現される。

【００１７】

また、フラッシュメモリ１５１には、アプリケーション取得手段１５３が外部から受信した加工処理を行う前の端末アプリケーションを格納する領域であるオリジナルアプリケーション記憶部１５５と、アプリケーション加工手段１５２が加工処理を施した後の端末アプリケーションを格納する領域である加工済みアプリケーション記憶部１５６と、がある。ＣＰＵが端末アプリケーションをオリジナルアプリケーション記憶部１５５または加工済みアプリケーション記憶部１５６に格納する場合、端末アプリケーションは、ＣＰＵおよびコプロセッサによって、暗号化されてそれぞれの記憶部に格納され、また、オリジナルアプリケーション記憶部１５５または加工済みアプリケーション記憶部１５６に暗号化された状態で格納されている端末アプリケーションをＣＰＵが読み出した場合、端末アプリケーションはＣＰＵおよびコプロセッサによって復号化される。

【００１９】

また、情報端末１０１は、プログラムに基づいてデータ処理を行うデータ処理部１１０と、セキュリティデバイス１０２との通信を制御するセキュリティデバイス通信手段１１６と、ネット上のサーバ機器や他の情報端末との無線通信を行う無線通信手段１１５と、キー入力スイッチなどの入力手段１１７と、データ処理部１１０が処理したデータを表示するＬＣＤなどの表示手段１１８と、によって構成される。

【００２０】

データ処理部１１０は、内部にＣＰＵやＲＯＭ、ＥＥＰＲＯＭ、ＲＡＭを有し、ＲＯＭおよびＥＥＰＲＯＭに格納されたプログラムに基づいてＣＰＵがＲＡＭおよびＥＥＰＲＯＭを用いてデータ処理を行う。

【００２１】

データ処理部１１０には、端末アプリケーションのプログラムコードを解釈して実行するアプリケーション実行手段１１１と、端末アプリケーションのセキュリティデバイス１０２へのダウンロード、および、セキュリティデバイス１０２に格納された端末アプリケーションの情報端末１０１へのロードを行うアプリケーション管理手段１１３と、情報端末１０１に次にロードされる端末アプリケーションを準備するアプリケーション準備手段１１２と、端末アプリケーションに施された電子署名を検証して、その有効性を検証するアプリケーション検証手段１１４と、があり、これらは、実際には、データ処理部１１０の内部のＲＯＭやＥＥＰＲＯＭに格納されているプログラムをデータ処理部１１０のＣＰＵが実行することによって実現される。

【００２２】

アプリケーション検証手段１１４には、電子署名を検証する際に利用するルートＣＡ証明書１１９（ＣＡは Certificate Authority を意味する）と、アプリケーション検証手段１１４が行う端末アプリケーションの検証処理の仕様を示す検証プロファイル１２０と、が保持されている。アプリケーション検証手段１１４はルートＣＡ証明書１１９を複数個、保持していても良い。

エ　【００２６】

端末アプリケーションをコンテンツプロバイダ（ＣＰ）のネット上のサーバからダウンロードする場合には、端末アプリケーションは、アプリケーション管理手段１１３によって、無線通信手段１１５を介してＣＰのサーバからダウンロードされ、セキュリティデバイス通信手段１１６およびホスト機器通信手段１５７を介してアプリケーション取得手段１５３に送信され、アプリケーション取得手段１５３が、受信した端末アプリケー

ションをオリジナルアプリケーション記憶部１５５に格納する。

【００２７】

この後、アプリケーション準備手段１１２によって、加工処理要求がアプリケーション加工手段１５２に送信され、加工処理要求を受信したアプリケーション加工手段１５２が、オリジナルアプリケーション記憶部１５５に格納されている端末アプリケーションに対して適当な加工処理を施し、加工済みアプリケーション記憶部１５６に格納する。

【００２８】

セキュリティデバイス１０２に格納された端末アプリケーションを実行する場合には、アプリケーション管理手段１１３によって、アプリケーション発行要求がアプリケーション発行手段１５４に送信され、アプリケーション発行要求を受信したアプリケーション発行手段１５４が、加工済みアプリケーション記憶部１５６から要求された端末アプリケーションを読出し、アプリケーション管理手段１１３に送信する。アプリケーション管理手段１１３は受信した端末アプリケーションをアプリケーション検証手段１１４に転送し、アプリケーション検証手段１１４が端末アプリケーションに施された電子署名を検証してその有効性を検証する。この時、アプリケーション検証手段１１４による検証をパスした端末アプリケーションだけが、アプリケーション実行手段１１１に転送され、アプリケーション実行手段１１１によって端末アプリケーションが起動される。

【００２９】

この後、アプリケーション実行手段１１１によって起動された端末アプリケーションは、まず、アプリケーション発行手段１５４によって、加工処理の際に埋め込まれた認証情報に基づいた認証処理が行われ、その認証処理にパスした場合のみ、その後の端末アプリケーションに固有の処理がアプリケーション実行手段１１１によって実行される。

【００３０】

このように、情報端末１０１において実行される端末アプリケーションを、情報端末１０１とセキュリティデバイス１０２とが認証することによって、不正な端末アプリケーションの実行が防止される。特に、端末アプリケーションがセキュリティデバイスのフラッシュメモリ１５１に格納された価値情報（図面には示されていない）を一定の制約のもとに利用するアプリケーションである場合には、それらの制約を不正に解除するなどの改竄が行われた端末アプリケーションの実行自体が防止されるので、価値情報は不正な利用から守られる。

【００３１】

次に、セキュリティデバイス１０２の内部のデータの詳細について説明する。図２は、アプリケーション加工手段１５２が内部に保持するデータの詳細と、セキュリティデバイス１０２に格納される端末アプリケーションのデータ構成を示している。アプリケーション加工手段１５２は、内部に、セキュリティデバイス１０２が装着されるホスト機器が行う端末アプリケーションの検証処理の仕様を示す検証プロファイル２２３と、端末アプリケーションに電子署名を行う際に用いるセキュリティデバイス秘密鍵２２１と、セキュリティデバイス秘密鍵２２１に対応するセキュリティデバイス証明書２２２と、ルートＣＡ証明書２２４とを保持する。

【００３２】

アプリケーション加工手段１５２は、検証プロファイル２２３とセキュリティデバイス秘密鍵２２１、セキュリティデバイス証明書２２２、ルートＣＡ証明書２２４を、それぞれ、複数個、保持していても良い。

【００３３】

検証プロファイル２２３のデータ構造は、検証プロファイル１２０のデータ構造と同様であり、セキュリティデバイス１０２を頻繁に装着するホ

スト機器としてセキュリティデバイス１０２に登録されたホスト機器の検証プロファイルがホスト機器ごとに保持される。この場合は、情報端末１０１の検証プロファイル１２０が検証プロファイル２２３として登録されている。

【００３４】

また、オリジナルアプリケーション記憶部１５５に格納されている端末アプリケーションは、それぞれ、実際のプログラムコードの部分であるアプリケーションコード２０１と、端末アプリケーションの発行者であるコンテンツプロバイダ（ＣＰ）によってアプリケーションコード２０１に施された電子署名である署名２０２と、署名２０２の有効性を証明する証明書チェーン２０３と、端末アプリケーションの属性情報２０４と、その端末アプリケーションに施されるべき加工処理の内容を規定した加工指示書２０５と、から構成される。

【００３５】

図４（ａ）は、オリジナルアプリケーション記憶部１５５に格納されている端末アプリケーションのアプリケーションコード２０１と署名２０２と証明書チェーン２０３の部分の一例を示しており、図３は、この場合のルートＣＡ３０１と中間ＣＡ３０２、コンテンツプロバイダ（ＣＰ）３０３、情報端末１０１、及びセキュリティデバイス１０２との間のシステム構成を示している。

【００３６】

この場合、証明書チェーン２０３は、ルートＣＡ３０１によって発行された中間ＣＡ３０２の中間ＣＡ証明書３２２と、中間ＣＡ３０２によって発行されたＣＰ３０３のＣＰ証明書３２２とから構成され、情報端末１０１とセキュリティデバイス１０２は、それぞれ、保有するルートＣＡ証明書を用いて、これらの証明書チェーン２０３を構成する証明書を検証する

ことによってＣＰ３０３によってアプリケーションコード２０１に施された署名２０２の有効性を検証することが出来る。

オ　【００４９】

次に、図８を用いて、ＣＰ３０３からセキュリティデバイス１０２に端末アプリケーションをダウンロードするシーケンス、及び、セキュリティデバイス証明書をダウンロードするシーケンスについて説明する。

【００５０】

まず、入力手段１１７から入力されたユーザ操作に基づいて、情報端末１０１が無線通信手段１１５を介し無線通信によってＣＰ３０３に端末アプリケーションを要求するメッセージを送信すると（アプリケーション要求８０１）、ＣＰ３０３は、情報端末１０１に装着されたセキュリティデバイス１０２に対して、セキュリティデバイス証明書を要求するメッセージを送信する（セキュリティデバイス証明書要求８０２または８１１）。

【００５１】

セキュリティデバイス証明書要求８０２（または８１１）には、ＣＰ３０３が生成した乱数が含まれており、情報端末１０１のセキュリティデバイス通信手段を介してセキュリティデバイス１０２に送信される。

【００５２】

セキュリティデバイス証明書要求８０２を受信したセキュリティデバイス１０２は、アプリケーション取得手段１５３がアプリケーション加工手段１５２に保持されているセキュリティデバイス証明書を調べ、ＣＰ３０３が発行したセキュリティデバイス証明書が保有されている場合には、アプリケーション取得手段１５３がアプリケーションの発行を要求するメッセージを生成して（アプリケーション発行要求生成８１３）ＣＰ３０３に送信し（アプリケーション発行要求８１３）、セキュリティデバイス証明書を保有していない場合には、アプリケーション取得手段１５３がＣＰに

セキュリティデバイス証明書の発行を要求するメッセージを生成して（証明書発行要求生成８０３）ＣＰ３０３に送信する（証明書発行要求８０４）。

【００５３】

この時、アプリケーション発行要求８１３には、ＣＰ３０３が発行したセキュリティデバイス証明書と、アプリケーション取得手段１５３がそのセキュリティデバイス証明書に対応するセキュリティデバイス秘密鍵を用いてセキュリティデバイス証明書要求８０２（または８１１）に含まれていた乱数に対して施した電子署名が含まれ、証明書発行要求８０４には、その他のセキュリティデバイス証明書と、アプリケーション取得手段１５３がそのセキュリティデバイス証明書に対応するセキュリティデバイス秘密鍵を用いてセキュリティデバイス証明書要求８０２に含まれていた乱数に対して施した電子署名が含まれる。

【００５４】

証明書発行要求８０４を受信したＣＰ３０３は、証明書発行要求８０４に含まれていた電子署名（セキュリティデバイス証明書要求８０２に含まれていた乱数に対する電子署名）を同じく証明書発行要求８０４に含まれていたセキュリティデバイス証明書を用いて検証して（署名検証８０５）、セキュリティデバイス１０２がセキュリティデバイス秘密鍵を保持していることを検証し、さらにＣＰ３０３は、そのセキュリティデバイス証明書に含まれるセキュリティデバイス公開鍵を用いて新たにセキュリティデバイス証明書を生成して（セキュリティデバイス証明書生成８０６）、セキュリティデバイス１０２に送信する（セキュリティデバイス証明書８０７）。仮に、署名検証８０５においてエラーが検出された場合には、ＣＰ３０３は、エラーメッセージを情報端末１０１に送信して処理を中止する（図には示していない）。

【００５５】

セキュリティデバイス証明書８０７は、情報端末１０１を介してセキュリティデバイス１０２に送信され、セキュリティデバイス証明書８０７を受信したセキュリティデバイス１０２は、アプリケーション取得手段１５３がセキュリティデバイス証明書８０７をアプリケーション加工手段１５２に保存して、セキュリティデバイス証明書８０７の取得を完了したことを示す応答メッセージを情報端末１０１に送信する（完了応答８０９）。

【００５６】

完了応答８０９を受信した情報端末１０１は、改めてＣＰ３０３に端末アプリケーションを要求するメッセージを送信する（アプリケーション要求８１０）。

【００５７】

アプリケーション発行要求８１３を受信したＣＰ３０３は、アプリケーション発行要求８１３に含まれていた電子署名（セキュリティデバイス証明書要求８０２または８１１に含まれていた乱数に対する電子署名）を同じくアプリケーション発行要求８１３に含まれていたＣＰ３０３が発行したセキュリティデバイス証明書を用いて検証して（署名検証８１４）、セキュリティデバイス１０２がＣＰ３０３が発行したセキュリティデバイス証明書に対応するセキュリティデバイス秘密鍵を保持していることを検証し、さらにＣＰ３０３は、そのセキュリティデバイス証明書に含まれるセキュリティデバイス公開鍵を用いて発行する端末アプリケーションを暗号化して（アプリケーション暗号化８１５）、セキュリティデバイス１０２に送信する（暗号化されたアプリケーション８１６）。

【００５８】

この時、暗号化する前の端末アプリケーションには、その有効性を示すためにＣＰ３０３による電子署名が施され、それを検証するための証明書が付加されている（図４（ａ）は暗号化する前の端末アプリケーションデ

ータ構造の一例を示している)。また仮に、署名検証８１４においてエラーが検出された場合には、ＣＰ３０３は、エラーメッセージを情報端末１０１に送信して処理を中止する（図には示していない)。

【００５９】

暗号化されたアプリケーション８１６は、情報端末１０１を介してセキュリティデバイス１０２に送信され、暗号化されたアプリケーション８１６を受信したセキュリティデバイス１０２は、アプリケーション取得手段１５３が、アプリケーション加工手段１５２が保持するセキュリティデバイス秘密鍵を用いて暗号を復号化し（暗号復号化８１７)、さらに、端末アプリケーションに施されたＣＰ３０３による電子署名を検証して端末アプリケーションの有効性を検証し（署名検証８１８)、端末アプリケーションをオリジナルアプリケーション記憶部１５５に保存して（アプリケーション保存８１９)、端末アプリケーションの取得を完了したことを示す応答メッセージを情報端末１０１に送信する（完了応答８２０)。

【００６０】

仮に、署名検証８１９においてエラーが検出された場合には、アプリケーション取得手段１５３は、端末アプリケーションを消去し、エラーメッセージを情報端末１０１に送信して処理を中止する（図には示していない)。

【００６１】

完了応答８２０を受信した情報端末１０１は、端末アプリケーションのダウンロードが完了したことを示すメッセージを表示手段１１８に表示して処理を終了する。

【００７０】

以上ように、情報端末１０１において実行される端末アプリケーションを、情報端末１０１とセキュリティデバイス１０２とが認証することによ

って、不正な端末アプリケーションの実行が防止される。

【００７１】

特に、端末アプリケーションがセキュリティデバイスのフラッシュメモリ１５１に格納された価値情報（図面には示されていない）を一定の制約のもとに利用するアプリケーションである場合には、それらの制約を不正に解除するなどの改竄が行われた端末アプリケーションの実行自体が防止されるので、価値情報は不正な利用から守られる。

⑶　「クライアント装置」に係る一致点の認定の誤りについて

原告は、本願発明の「クライアント装置」に相当するのは、引用発明の「情報端末１０１」であって、「セキュリティデバイス１０２」でないから、本件審決が、引用発明の「セキュリティデバイス１０２」が本願発明の「クライアント装置」に相当するとの認定を前提に、本願発明と引用発明は、「前記第１の数と前記証明書のリクエストは前記クライアント装置に送られ」る点で一致すると認定したのは誤りである旨主張する。

ア　本願発明の特許請求の範囲の請求項１には、本願発明の「サーバ」は、「数発生器」と「証明書リクエストモジュール」と、これらに「接続するインターフェース」を備えており、「数発生器」は「第１の数」を、「証明書リクエストモジュール」は「デバイス証明書のリクエスト」をそれぞれ生成し、「前記第１の数」と「前記デバイス証明書のリクエスト」は、「前記インターフェースを介してクライアント装置に送られ」るとの記載がある。これらの記載によれば、本願発明の「クライアント装置」は、「サーバ」が生成し、送信する「第１の数」及び「デバイス証明書のリクエスト」を受信する機能を有するものであると解される。

イ　引用文献１には、「ＣＰ３０３は、情報端末１０１に装着されたセキュリティデバイス１０２に対して、セキュリティデバイス証明書を要求するメッセージを送信する（セキュリティデバイス証明書要求８０２または８１

１)。」(【００５０】)、「セキュリティデバイス証明書要求８０２（または８１１）には、ＣＰ３０３が生成した乱数が含まれており、情報端末１０１のセキュリティデバイス通信手段を介してセキュリティデバイス１０２に送信される。」(【００５１】)、「セキュリティデバイス証明書要求８０２を受信したセキュリティデバイス１０２」(【００５２】) との記載があり、また、上記各段落の説明に用いられる図８には、「セキュリティデバイス証明書要求８０２」及び「セキュリティデバイス証明書要求８１１」について、それぞれ「ＣＰ３０３」から「情報端末１０１」を通過し「セキュリティデバイス１０２」を終点とする矢印が引かれている。引用文献１の上記記載及び図８から、引用発明の「ＣＰ３０３」は、「乱数」と「セキュリティデバイス証明書要求」を生成し、これらを「セキュリティデバイス１０２」に送信し、「セキュリティデバイス１０２」は、これらを受信するものと理解できる。そして、引用発明の「ＣＰ３０３」、「乱数」、「セキュリティデバイス証明書要求」は、それぞれ、本願発明の「サーバ」、「第１の数」、「デバイス証明書のリクエスト」に相当するから、引用発明の「セキュリティデバイス１０２」は、「サーバ」（ＣＰ３０３）が生成し、送信する「第１の数」（乱数）及び「デバイス証明書のリクエスト」（セキュリティデバイス証明書要求）を受信する機能を有するものと認められる。

したがって、引用発明の「セキュリティデバイス１０２」は、本願発明の「クライアント装置」に相当すると認められる。

ウ　これに対し、原告は、引用発明は、「セキュリティデバイス１０２」が「情報端末１０１」に装着されて「情報端末１０１」と通信するように構成され，本願発明の「サーバ」に相当する引用発明の「ＣＰ３０３」には「情報端末１０１」が無線ネットワークを介して接続される構成であることからすると、本願発明の「クライアント装置」に相当するのは、引用発明の「情報端末１０１」であって、「セキュリティデバイス１０２」でない旨主

張する。

しかし、前記イのとおり、引用文献１の図８において「ＣＰ３０３」から発せられた「セキュリティデバイス証明書要求８０２」及び「セキュリティデバイス証明書要求８１１」が、「情報端末１０１」を通過して「セキュリティデバイス１０２」に到達するように矢印が引かれていることに照らすと、引用発明の「セキュリティデバイス１０２」が「ＣＰ３０３」から送信された「乱数」及び「セキュリティデバイス証明書要求」の送受信は、「ＣＰ３０３」と「セキュリティデバイス１０２」との間で行われ、「情報端末１０１」は通過点にすぎないものと解される。

したがって、引用発明の「情報端末１０１」が本願発明の「クライアント装置」に相当するとの原告の上記主張は理由がない。

エ　以上によれば、本願発明と引用発明は、「前記第１の数と前記証明書のリクエストは前記クライアント装置に送られ」る点で一致するとした本件審決の認定の誤りをいう原告の主張は理由がない。

⑷　「第２の署名」に係る一致点の認定の誤りについて

原告は、本件審決は、引用発明の「乱数に施した電子署名」が本願発明の「クライアント装置において該クライアント装置の製造中にプログラムされたプライベートキーと前記サーバの数発生器が作成した第１の数を使用して生成される第２の署名」に相当するとの認定を前提に、本願発明と引用発明は、「レスポンス」が「該クライアント装置の製造中にプログラムされたプライベートキーと前記サーバの数発生器が作成した第１の数を使用して生成される第２の署名」を含む点で一致すると認定したが、本願発明の「第１の数を使用して生成される第２の署名」は、第１の数を使用して新たに生成されるものであり、「乱数に施したことで得られた電子署名」に対応する署名であるのに対し、引用発明の「乱数に施した電子署名」とは、その文言から、「電子署名を乱数に施した」ことを意味するものであり、電子署名自体には、変

化がなく、「乱数に施したことで得られた電子署名」とは異なるものであるから、本件審決の上記一致点の認定は誤りである旨主張する。

ア　本願発明の特許請求の範囲の請求項１の記載によれば、本願発明の「第１の数を使用して生成される第２の署名」とは、「プライベートキー」（秘密鍵）と「第１の数」を用いて生成される電子署名であると解される。このような理解は、本願明細書の「証明書作成モジュール１２０は、デバイス・プライベートキーを使用し、乱数Ｒ上の署名Ｓｉｇを算出する。」（【００１５】）との記載にも合致する。

イ　引用文献１には、「証明書発行要求８０４には、…セキュリティデバイス秘密鍵を用いてセキュリティデバイス証明書要求８０２に含まれていた乱数に対して施した電子署名が含まれる。」（【００５３】）、「証明書発行要求８０４を受信したＣＰ３０３は、証明書発行要求８０４に含まれていた電子署名（セキュリティデバイス証明書要求８０２に含まれていた乱数に対する電子署名）を同じく証明書発行要求８０４に含まれていたセキュリティデバイス証明書を用いて検証して（署名検証８０５）」（【００５４】）との記載がある。これらの記載及び図８によれば、引用発明の「乱数に対して施した電子署名」は、「プライベートキー」（セキュリティデバイス秘密鍵）と「第１の数」（乱数）を用いて生成される署名であるといえるから、本願発明の「第１の数を使用して生成される第２の署名」に相当すると認められる。

ウ　これに対し、原告は、引用発明の「乱数に施した電子署名」とは、その文言から、「電子署名を乱数に施した」ことを意味するものであり、「乱数に施したことで得られた電子署名」とは異なる旨主張する。

　しかし、引用発明の「乱数に対して施した電子署名」（乱数に施した電子署名）が乱数に対してセキュリティデバイス秘密鍵を用いて生成される電子署名を意味すると解されることは前記イのとおりであって、原告の上記

主張の解釈は、文言解釈として不自然であり、採用することができない。

エ　以上によれば、本願発明と引用発明は、「レスポンス」が「該クライアント装置の製造中にプログラムされたプライベートキーと前記サーバの数発生器が作成した第１の数を使用して生成される第２の署名」を含む点で一致するとした本件審決の認定の誤りをいう原告の主張は理由がない。

２　相違点２の容易想到性の判断の誤りについて

⑴　本願優先日当時の技術常識について

ア　各文献の記載事項

（ア）　乙１（「暗号技術入門　秘密の国のアリス」第３版、８頁～１０頁、２２７頁～２２８頁、２０１６年３月１８日発行、ＳＢクリエイティブ株式会社）

「暗号アルゴリズム

…平文から暗号文を作る手順、すなわち暗号化の手順のことを「暗号化のアルゴリズム」と呼び、復号化の手順のことを「復号化のアルゴリズム」と呼びます。暗号化・復号化のアルゴリズムを合わせて暗号アルゴリズムと呼びます。」

「鍵

…暗号化を行うときも、復号化を行うときも、いずれの場合にも鍵が必要になります。」

「対称暗号と公開鍵暗号

暗号は、鍵の使い方によって、対称暗号と公開鍵暗号の２種類に分類できます。

対称暗号（…）は、暗号化と復号化で同じ鍵を使う方式です。…

それに対して公開鍵暗号（…）は、暗号化と復号化で異なる鍵を使う方式です。…

Ｆｉｇ．１－８●対称暗号と公開鍵暗号」

「公開鍵暗号とデジタル署名

…デジタル署名の実現には、…公開鍵暗号の仕組みを利用します。公開鍵暗号では、公開鍵とプライベート鍵の鍵ペアを使い、公開鍵で暗号化して、プライベート鍵で復号化しました（…）。

デジタル署名でも、同じように公開鍵とプライベート鍵の鍵ペアを使います。しかし、２つの鍵の使い方は公開鍵暗号とは逆になります。メッセージをプライベート鍵で暗号化することが署名の作成に相当し、その暗号文を公開鍵で復号化することが署名の検証に相当します。２つの図を比較して公開鍵暗号を「逆に使っている」様子を理解してください（…）。

…つまり、ある公開鍵を使って暗号文が正しく復号化できたなら、その暗号文は、その公開鍵と対になったプライベート鍵で暗号されたはず、ということがいえます。

Ｆｉｇ．９－２●プライベート鍵による暗号化（デジタル署名）

プライベート鍵で暗号化するというのは、そのプライベート鍵を使える人にしか実現できない行為ですから、この事実から「プライベート鍵による暗号文」を「署名」として扱おうというのです（…）。

公開鍵は一般に公開できますから、公開鍵による復号化は誰にでもできることになります。これは、誰でもデジタル署名の検証が行えるという大きなメリットになります。」

（「Ｆｉｇ．１－８」及び「Ｆｉｇ．９－２」については別紙３を参照）

（イ） 乙２（「暗号技術のすべて」、５９８頁～５９９頁、２０１７年９月１５日発行、株式会社翔泳社）

「８．５．１　電子証明書とは

電子証明書（…）は、公開鍵がその証明書に書かれた所有者のものであることを証明するために用いられます。ここでいう公開鍵と

は、公開鍵暗号の公開鍵や、デジタル署名の検証鍵を指します。」

「８．５．２　証明書のフォーマット

証明書のフォーマットは、国際標準化団体のＩＴＵ（国際電気通信連合）により、標準化されており、その代表的なものがＸ．５０９です。Ｘ．５０９では、証明書の論理的構造を規定しています。…Ｘ．５０９証明書は、「署名前証明書」「署名アルゴリズム」「署名値」から構成されます（表８．６）。署名前証明書は、基本領域と拡張領域に分けられます。基本領域には、証明書の所有者の公開鍵に関する情報が記載されます。拡張領域には、基本領域を補足する情報が追加されます。例えば、「検証鍵情報」「鍵使用目的（署名検証・否認防止・暗号化など)」「ポリシー情報」などが含まれます。署名値は、署名前証明書に対する認証局のデジタル署名です。

証明書は使用する形式によって、ＰＫＣＳ＃１１（ＩＣカードなど）やＰＫＣＳ＃１２（データファイルなど）で保存されます。」

（「表８．６」については別紙４を参照）

（ウ）　引用文献３（甲２７）

【０１１０】

クライアントＩＤが登録済みである場合は、ステップＳ１４５に進み、サーバは、クライアントの保持するコピーコンテンツに対応するコンテンツＩＤリストの送信をクライアントに要求する。なお、この要求をクライアントに送信する際、サーバは、サーバクライアント間で転送されるコンテンツＩＤリストの安全性、正当性を確保するために適用するデータとして、乱数値（Ｒａｎｄｏｍ　ｃｈａｌｌｅｎｇｅ）とサーバの保持するデバイス証明書（公開鍵証明書）をクライアントに送信する。

【０１１１】

クライアントは、ステップＳ２４４において、乱数値とデバイス証明

書を伴ったコンテンツＩＤリスト要求を受信し、ステップＳ２４５において、利用期間の更新要求対象としたコンテンツを受領したサーバのサーバＩＤに対応付けられたコピーコンテンツのコンテンツＩＤからなるリストを生成して、サーバに送信する。このリスト送信に際して、クライアントは、クライアントが生成した乱数値と、クライアントのデバイス証明書（公開鍵証明書）を送信する。

【０１１４】

図９（ｂ）に、リストに併せて送信されるデバイス証明書（公開鍵証明書）のデータ構成例を示す。デバイス証明書（公開鍵証明書）は以下のデータを含む。

デバイスＩＤ［Ｄｅｖｉｃｅ　ＩＤ］＝クライアントＩＤ

デバイス公開鍵［Ｄｅｖｉｃｅ　Ｐｕｂｌｉｃ　Ｋｅｙ］

発行元電子署名［Ｓｉｇｎａｔｕｒｅ　ｂｙ　ＬＡ］

【０１１５】

図９（ｂ）に示す公開鍵証明書は、一般的な公開鍵証明書の構成であり、デバイスＩＤ、デバイス公開鍵と、発行元の電子署名を含む。例えばクライアントの公開鍵を格納したクライアントデバイス公開鍵証明書を受領したサーバは、受領した公開鍵証明書に設定された署名に基づく検証を実行して、証明書の改竄のないことの確認を行なった後に、格納されたクライアントの公開鍵を取得する。サーバは、取得したクライアント公開鍵を適用して、図９（ａ）に示すコンテンツＩＤリストに設定された電子署名、すなわちクライアント秘密鍵を適用して生成された署名の検証を実行することができる。

(エ)　引用文献４（甲２８）

【００８０】不揮発メモリ１００には、このアクセス制御部６０を搭載したデバイスが、正当なデバイスであることを証明するデバイス証明書

１０１と、アクセス制御部６０の公開鍵暗号用秘密鍵であるデバイス秘密鍵１０５と、デバイス証明書１００を発行した認証機関の公開鍵１０６とが格納されている。

【０１０５】デバイス証明（図２の１０１）には、デバイスＩＤ（図２の１０２）と、デバイス公開鍵（図２の１０３）と、これらの記述に対する電子署名（図２の１０３）（認証機関の秘密鍵により作成さえた）を含む。デバイス証明の正当性は、その電子署名を認証機関の公開鍵（図２の１０６）で正しく復号できるかどうかにより確認される。第三者がデバイス証明を偽造しようとしても､認証機関の秘密鍵を知らないので、正しい電子署名（図２の１０３）を作成することができない。

イ　デバイス証明書等に関する技術常識について

前記アの記載事項を総合すると，①「デバイス証明書」は、正当なデバイス（クライアント）であることを証明する電子証明書であり､「公開鍵証明書」が､「デバイス証明書」として用いられること（前記ア(ウ)、(エ)）、②電子署名は、公開鍵とプライベート鍵（秘密鍵）の鍵ペアを使い、メッセージをプライベート鍵（秘密鍵）で暗号化することが「署名」の「作成」に相当し、その暗号文を公開鍵で復号化することが「署名」の「検証」に相当すること（前記ア(ア)）、③「公開鍵証明書」は、電子署名が、秘密鍵を保有するものでなければ生成できないという性質を利用して、秘密鍵を保有する者とその者の公開鍵とを結びつけ、公開鍵が、その公開鍵とペアとなる秘密鍵を保有する者のものであること等を証明する手段であること（前記ア(ア)）、④「公開鍵証明書」の代表的なフォーマットは、別紙４のような論理的構造で規定されており､「署名前証明書」､「署名アルゴリズム」及び「署名値」から構成されていること（前記ア(イ)）、⑤「署名前証明書」の「基本領域」には、証明書の所有者の公開鍵に関する情報（「主体者」､「主体者公開鍵情報（アルゴリズム、主体者公開鍵)」､「発行者ユニー

ク識別子」、「主体者ユニーク識別子」等）が、「拡張領域」には、基本領域を補足する情報が記載されており、また、「署名値」は、「署名前証明書」部分について電子署名したものであること（前記ア(ア)、(イ)）、⑤「公開鍵証明書」を受け取った者は、「公開鍵証明書」に含まれる「公開鍵」で「署名（署名値)」を「検証」することによって、「公開鍵証明書」に含まれる情報（「署名前証明書」部分に含まれる情報）が改ざんされておらず、「公開鍵」が確かに主体者のものであることを確認することができること（前記ア(ア)、(ウ)、(エ)）は，本願優先日当時の技術常識であったことが認められる。

⑵　本願発明の「前記クライアント装置の装置ＩＤ、発行者ＩＤ、前記プライベートキーの関数である公開鍵及び前記クライアント装置の不揮発性メモリから読み出された第１の署名の関数として生成されたデバイス証明書」の意義について

ア　本願発明の特許請求の範囲の請求項１の「前記クライアント装置の装置ＩＤ、発行者ＩＤ、前記プライベートキーの関数である公開鍵及び前記クライアント装置の不揮発性メモリから読み出された第１の署名の関数として生成されたデバイス証明書」との記載から、本願発明の「第１の署名」は、「クライアント装置の不揮発性メモリから読み出された」ものであることを理解できるが、請求項１には、「第１の署名」の構成や生成方法等について規定した記載はない。

また、本願明細書には、本願発明の「第１の署名」について定義した記載はない。

一方で、本願明細書には、「デバイス証明書」に関し、①「クライアント１０６の証明書作成モジュール１２０は、証明書Ｃｅｒｔを作成する。…証明書作成モジュール１２０は、デバイス・プライベートキーを使用し、乱数Ｒ上の署名Ｓｉｇを算出する。」（【００１５】）、「図３は、一回だけデ

バイス証明書を作成する方法の一例のフローチャート３００を示している。図３の例では、フローチャート３００は、モジュール３０２で始まり、ここでデバイス証明書がセキュアデバイスで作成される。…デバイス証明書は公知のものである。」(【００２３】)、②「図６は、セキュアデバイスを製造する方法の例を示すフローチャート６００である。…図６の例において、フローチャート６００は、モジュール６０２でスタートし、ここで装置ＩＤが取得される。装置ＩＤは、シリアルナンバーであっても、或いは装置のための他の何らかの固有な識別子であっても良い。」(【００５３】)、「図６の例で、フローチャート６００は、モジュール６０４に進み、ここでは装置のために小署名プライベートキー(a small-signature private key)として使用する目的で、擬似乱数が供される。…小署名プライベートキーは、これに限定されない例として、楕円カーブプライベートキーや比較的小さなフットプリント(footprint)を持った他の何らかのプライベートキーでも良い。」(【００５４】)、「図６の例で、フローチャート６００は、モジュール６０６に進み、ここでは共通パラメータを使用してプライベートキーから公開鍵が算出される。」(【００５５】)、「図６の例で、フローチャート６００は、モジュール６０８に進み、ここでは一定の証明書構造(fixed certificate structure)が、証明書を作成するために使用される。証明書は、例えば楕円カーブＤＳＡなどの小署名アルゴリズム(small signature algorithm)を使用して署名される。一実施形態では、該一定の証明書構造は、少なくとも装置ＩＤ、発行者名、及びデバイス公開鍵を含むかもしれない。」(【００５６】)、「図６の例で、フローチャート６００は、モジュール６１０に進み、ここでは｛装置ＩＤ、プライベートキー、発行者ＩＤ、署名｝が、装置の不非揮発性メモリにプログラミングされる。…一実施形態では、例えば公開鍵など、デバイス証明書の作成(construct)に必要とされる如何なるデータも、要求に応じてプログラミングされた状態

で生成されても良い。」(【００５７】)、③「図７は、セキュア証明書の作成方法の例を示したフローチャート７００である。メリットとして、この方法は、不揮発性でプログラミングされた鍵と必要なソフトウェアを有する装置が、装置認証に使用可能な完全なデバイス証明書を作成することを可能にする。図７の例では、フローチャート７００は、モジュール７０２でスタートし、ここではデバイス証明書のリクエストが、呼出しアプリケーションから受け取られる。」(【００５９】)、「図７の例で、フローチャート７００は、モジュール７０４に進み、ここでは｛装置ＩＤ、プライベートキー、発行者ＩＤ、署名｝が、不非揮発性メモリから読み込まれる。」(【００６０】)、「図７の例で、フローチャート７００は、モジュール７０６に進み、ここでは公開鍵が、プライベートキーと（もしあるならば）共通パラメータとによって算出される。一実施形態では、この演算は、図６を参照して上述した方法のような製造プロセスに使用されたのと同じアルゴリズムを利用する。公開鍵は、セキュリティカーネルで算出されても良い。」(【００６１】)、「図７の例で、フローチャート７００は、モジュール７０８に進み、ここではデバイス証明書が、装置ＩＤ、発行者ＩＤ、公開鍵、署名、及び共通パラメータから作成される。一実施形態において、セキュリティカーネル・モジュールは、図６を参照して上述した方法のような製造プロセスで使用されおり、該デバイス証明書の構造を認識している。」(【００６２】) との記載がある。

これらの記載と図６及び７を総合すると、本願明細書には、本願発明の「デバイス証明書」の実施形態として、「装置ＩＤ、発行者ＩＤ、公開鍵、署名」の証明書構造からなるデバイス証明書が開示されており、このデバイス証明書は、「公開鍵証明書」であること、上記「装置ＩＤ、発行者ＩＤ、公開鍵、署名」のうちの「署名」は、小署名アルゴリズム(small signature algorithm)を使用して算出された電子署名であり、本願発明の「第１の署

名」に相当することを理解できる。

そして、本願明細書には、上記「署名」の具体的内容についての記載はないが、「デバイス証明書は公知のものである。」（【００２３】）との記載及び前記⑴イ認定の本願優先日当時の技術常識を踏まえると、本願発明の「デバイス証明書」は、「公開鍵証明書」の代表的なフォーマット（別紙４参照）に基づくものであり、上記「署名」は、「公開鍵証明書」の「署名値」（証明書の所有者の公開鍵に関する情報（「主体者」、「主体者公開鍵情報（アルゴリズム、主体者公開鍵）」、「発行者ユニーク識別子」、「主体者ユニーク識別子」等）を含む「署名前証明書」部分について電子署名したもの）に相当するものと理解できる。

以上の本願発明の特許請求の範囲の請求項１の記載、本願明細書の上記記載及び前記⑴イ認定の本願優先日当時の技術常識を総合すると、本願発明の「デバイス証明書」の「第１の署名」とは、「デバイス証明書」に含まれる「前記プライベートキーの関数である公開鍵」にいう「プライベートキー」を用いて「前記クライアント装置の装置ＩＤ」、「発行者ＩＤ」及び「公開鍵」を暗号化した「署名値（署名）」を意味するものと解される。

そうすると、本願発明の「前記クライアント装置の装置ＩＤ、発行者ＩＤ、前記プライベートキーの関数である公開鍵及び前記クライアント装置の不揮発性メモリから読み出された第１の署名の関数として生成されたデバイス証明書」とは、「前記クライアント装置の装置ＩＤ、発行者ＩＤ、前記プライベートキーの関数である公開鍵」及びこれらを前記プライベートキーを用いて暗号化した署名（署名値）から構成される公開鍵証明書であると解される。

イ　これに対し原告は、本願明細書には、「第１の署名」について「これらを暗号化して生成される」との記載はなく、【００６２】には、「デバイス証明書が、装置ＩＤ、発行者ＩＤ、公開鍵、署名、及び共通パラメータから

作成される」こと（「デバイス証明書」に「署名」が含まれること）の記載があるのみであるから、本願明細書を参酌しても、本願発明の「デバイス証明書」が、「クライアント装置の装置ＩＤ、発行者ＩＤ、プライベートキーの関数である公開鍵」と、これらを暗号化して生成される「第１の署名」とを含むものと解釈することはできない旨主張する。

しかしながら、前記アで説示したとおり、本願発明の特許請求の範囲の請求項１の記載、本願明細書の記載及び前記⑴イ認定の本願優先日当時の技術常識を総合すると、本願発明の「デバイス証明書」の「第１の署名」とは、「デバイス証明書」に含まれる「前記プライベートキーの関数である公開鍵」にいう「プライベートキー」を用いて「前記クライアント装置の装置ＩＤ」、「発行者ＩＤ」及び「公開鍵」を暗号化した「署名値（署名）」を意味するものと解されるから、原告の上記主張は採用することができない。

⑶　相違点２の容易想到性について

ア　引用文献１には、「次に、図８を用いて、ＣＰ３０３からセキュリティデバイス１０２に端末アプリケーションをダウンロードするシーケンス、及び、セキュリティデバイス証明書をダウンロードするシーケンスについて説明する。」（【００４９】）、「まず、入力手段１１７から入力されたユーザ操作に基づいて、情報端末１０１が無線通信手段１１５を介し無線通信によってＣＰ３０３に端末アプリケーションを要求するメッセージを送信すると（アプリケーション要求８０１）、ＣＰ３０３は、情報端末１０１に装着されたセキュリティデバイス１０２に対して、セキュリティデバイス証明書を要求するメッセージを送信する（セキュリティデバイス証明書要求８０２または８１１）」（【００５０】）、「証明書発行要求８０４を受信したＣＰ３０３は、証明書発行要求８０４に含まれていた電子署名（セキュリティデバイス証明書要求８０２に含まれていた乱数に対する電子署名）

を同じく証明書発行要求８０４に含まれていたセキュリティデバイス証明書を用いて検証して（署名検証８０５）、セキュリティデバイス１０２がセキュリティデバイス秘密鍵を保持していることを検証し、さらにＣＰ３０３は、そのセキュリティデバイス証明書に含まれるセキュリティデバイス公開鍵を用いて新たにセキュリティデバイス証明書を生成して（セキュリティデバイス証明書生成８０６）、セキュリティデバイス１０２に送信する（セキュリティデバイス証明書８０７）。」（【００５４】）との記載がある。

これらの記載及び図８によれば、引用文献１記載の「証明書発行要求８０４に含まれていたセキュリティデバイス証明書」（引用発明の「セキュリティデバイス証明書」に相当するもの）は、セキュリティデバイス１０２がセキュリティデバイス秘密鍵を用いて生成した公開鍵を含む公開鍵証明書であることを理解できる。

イ　一方で、引用文献１には、「証明書発行要求８０４に含まれていたセキュリティデバイス証明書」の証明書構造に関する記載はない。

しかるところ、「公開鍵証明書」の代表的なフォーマットは、別紙４のような論理的構造で規定されており、「署名前証明書」、「署名アルゴリズム」及び「署名値」から構成されていることは、本願優先日当時の技術常識であったことを踏まえると、引用文献１に接した当業者は、引用発明の「セキュリティデバイス証明書」に上記「公開鍵証明書」の論理的構造を適用して、セキュリティデバイス１０２の装置ＩＤ、発行者ＩＤ、セキュリティデバイス秘密鍵を用いて生成した公開鍵及びこれらを上記セキュリティデバイス秘密鍵を用いて暗号化した署名（署名値）から構成される公開鍵証明書（相違点２に係る本願発明の構成）とすることを容易に想到することができたものと認められる。

これに反する原告の主張は、採用することができない。

３　相違点の看過について

原告は、①本願明細書の【００１６】には「サーバ１０２における証明書検証モジュール１１２は、信頼できる証明書チェーン(trusted certificate chain)を用いて、証明書Ｃｅｒｔを認証し」との記載があること、証明書チェーンは、認証パスとも呼ばれ、クライアント、サーバなどの証明書から、中間認証局の証明書、ルート認証局の証明書までの連なりであり、チェーン内の各証明書が次の証明書よって署名されることでセキュリティを確保するように構成されていることは技術常識であることからすると、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」とは、「デバイス証明書」は「証明書チェーン」を用いて認証され、「第２の署名」は「デバイス証明書」に含まれる公開鍵によって認証されることを意味するものと解される、②引用文献１には、引用発明における「セキュリティデバイス証明書を用いて検証する」との構成が、このような認証を意味することを示した記載はないから、引用発明は、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」との構成を備えるものでない点で本願発明と相違するが、本件審決は、この点を相違点として認定していないから、本件審決には、かかる相違点を看過した誤りがある旨主張する。

⑴　本願発明の特許請求の範囲の請求項１の記載から、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」との構成は、「サーバ」が備える「前記証明書検証モジュール」が「前記デバイス証明書」と「第２の署名」を認証することを規定したものと理解できるが、請求項１には、上記構成中の「認証」の認証方法について規定した記載はない。

また、本願明細書には、上記構成中の「認証」を特定の認証方法に限定することを述べた記載はない。

次に、本願明細書には、「サーバ１０２Ｒは、インターフェース１１８で、乱数Ｒ、任意データ、証明書Ｃｅｒｔ、及び署名Ｓｉｇを受けとる。サーバ

１０２における証明書検証モジュール１１２は、信頼できる証明書チェーン(trusted certificate chain)を用いて、証明書Ｃｅｒｔを認証し、証明書Ｃｅｒｔを用いて署名Ｓｉｇを認証し、更に乱数Ｒが、元々サーバ１０２によってクライアント１０６に送られた乱数Ｒと同じであるか否かを検証する。」（【００１６】）との記載があり、「証明書チェーン(trusted certificate chain)を用いて、証明書Ｃｅｒｔを認証し、証明書Ｃｅｒｔを用いて署名Ｓｉｇを認証」した実施形態が開示されているが、一方で、「当業者であれば前述した実施例と実施形態は、代表的なものであり、本発明の範囲を限定するものでないことが理解されるであろう。当業者が明細書を考慮し、図面を検討したときに自明な置き換え、増強、均等物やそれらへの改良が、本発明の要旨と範囲に含まれることを意図している。」（【００６６】）との記載に照らすと、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」との構成にいう「認証」は、【００１６】記載の「証明書チェーン」を用いた認証方法に限定すべきものと解することはできない。

これに反する原告の主張は、採用することができない。

⑵　引用文献１の【００５４】には「証明書発行要求８０４を受信したＣＰ３０３は、証明書発行要求８０４に含まれていた電子署名（セキュリティデバイス証明書要求８０２に含まれていた乱数に対する電子署名）を同じく証明書発行要求８０４に含まれていたセキュリティデバイス証明書を用いて検証して（署名検証８０５）、セキュリティデバイス１０２がセキュリティデバイス秘密鍵を保持していることを検証し」との記載がある。この記載及び図８から、引用発明において、「ＣＰ３０３」は、「乱数に対する電子署名」をセキュリティデバイス１０２からの証明書発行要求８０４に含まれていた「セキュリティデバイス証明書」を用いて検証する構成を有することが理解できる。そして、引用発明の「乱数に対する電子署名」が本願発明の「第２の署名」に対応すること（前記１⑷イ）からすると、引用発明の上記構成は、本

願発明のサーバが備える「前記証明書検証モジュールは…第２の署名とを認証する」構成に相当する。

次に、前記２⑴イのとおり、「公開鍵証明書」を受け取った者は、「公開鍵証明書」に含まれる「公開鍵」で「署名（署名値）」を検証することによって、「公開鍵証明書」に含まれる情報（「署名前証明書」部分に含まれる情報）が改ざんされておらず、「公開鍵」が確かに主体者のものであることを確認することができることは、本願優先日当時の技術常識であること、引用発明の「セキュリティデバイス証明書」は、「公開鍵証明書」であること（前記２⑶ア）からすると、引用発明の「セキュリティデバイス証明書」を用いて同証明書に含まれる署名を検証することによって同証明書に含まれる情報が改ざんされていないことを確認することは自明である。

そうすると、引用発明の「ＣＰ３０３」においても、「セキュリティデバイス証明書」を認証する構成を備えていると認められ、上記構成は、本願発明のサーバが備える「前記証明書検証モジュールは前記デバイス証明書…を認証し」との構成に相当する。

以上によれば、引用発明は、本願発明の「前記証明書検証モジュールは前記デバイス証明書と第２の署名とを認証し」との構成を備えるものと認められるから、上記構成が相違点であることを理由に本件審決における相違点の看過をいう原告の主張は、採用することができない。

⑶　その他原告は、本件審決における本願発明と引用発明の一致点の認定の誤りないし相違点の看過について縷々主張するが、いずれも本願発明の発明特定事項との関係が明確とはいえず、本件審決の結論に影響を及ぼすものといえないから、理由がない。

第５　結論

以上のとおり、原告主張の取消事由は理由がなく、本件審決にこれを取り消すべき違法は認められない。

したがって、原告の請求は棄却されるべきものであるから、主文のとおり判決する。

知的財産高等裁判所第１部

裁判長裁判官　　大　　鷹　　一　　郎

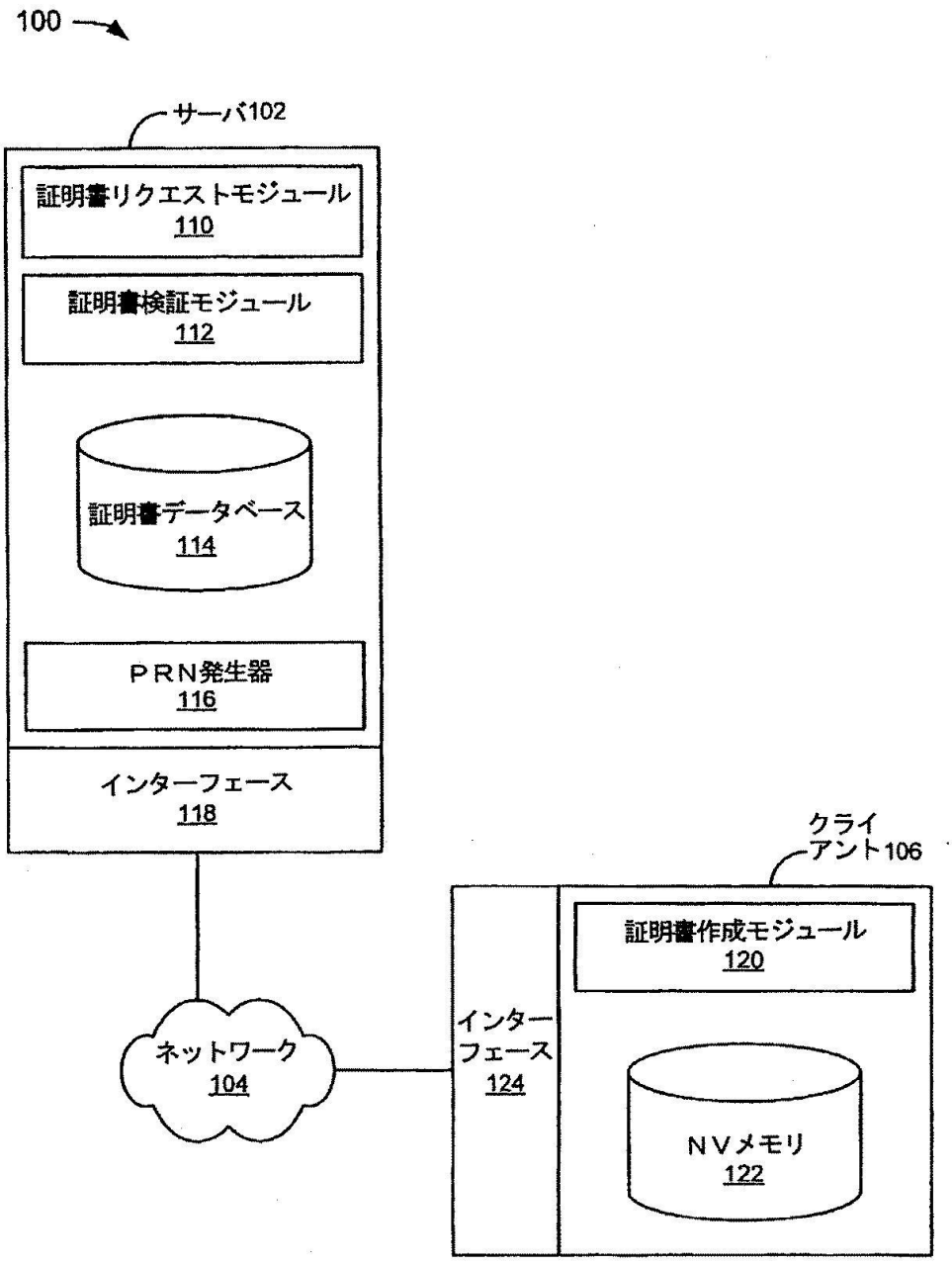
裁判官　　小　　川　　卓　　逸

裁判官小林康彦は、転補のため署名押印することができない。

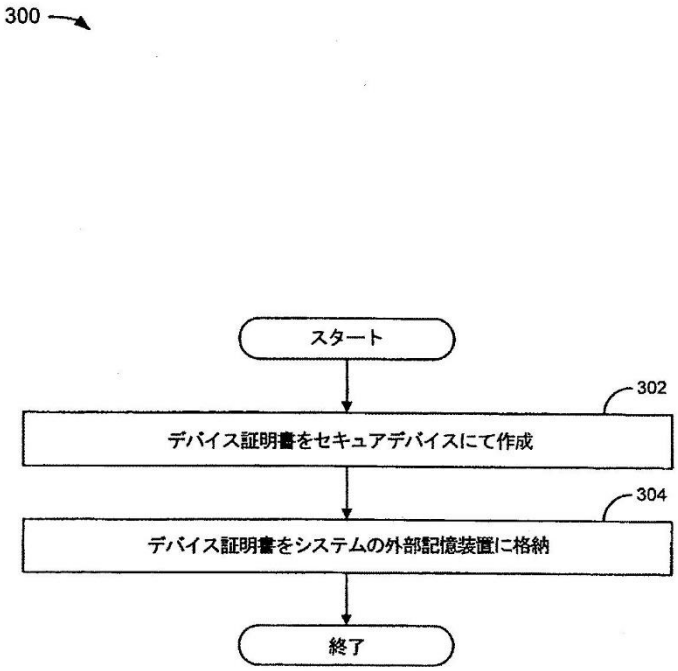
裁判長裁判官　　大　　鷹　　一　　郎

（別紙１）

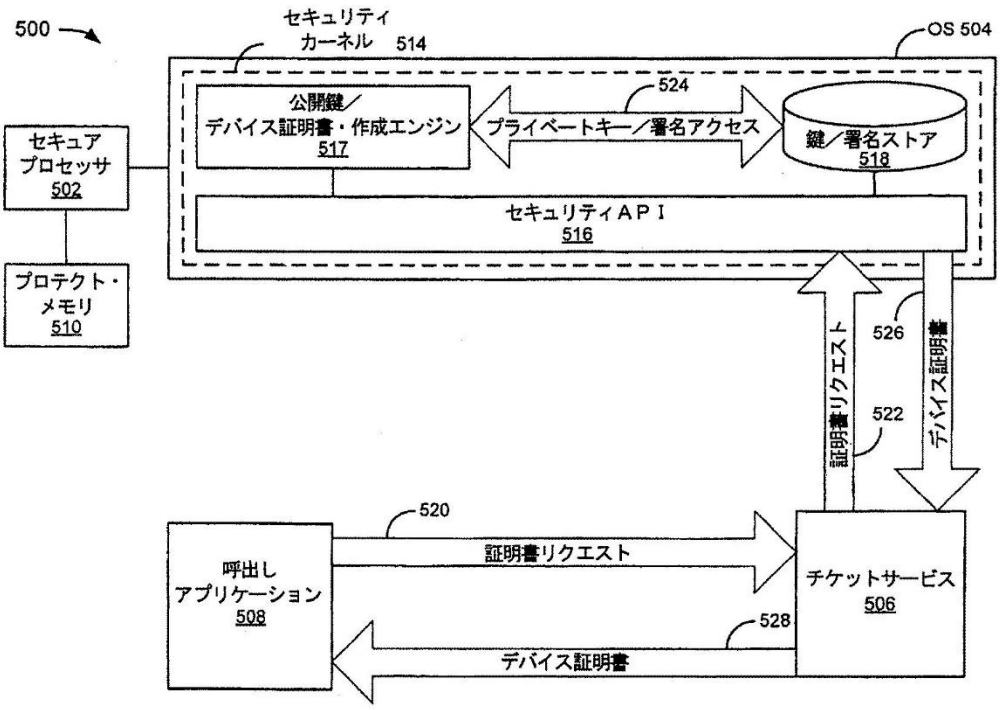
【図１】


100
サーバ102
証明書リクエストモジュール
110
証明書検証モジュール
112
証明書データベース
114
PRN発生器
116
インターフェース
118
クライアント106
証明書作成モジュール
120
インターフェース
124
NVメモリ
122
ネットワーク
104

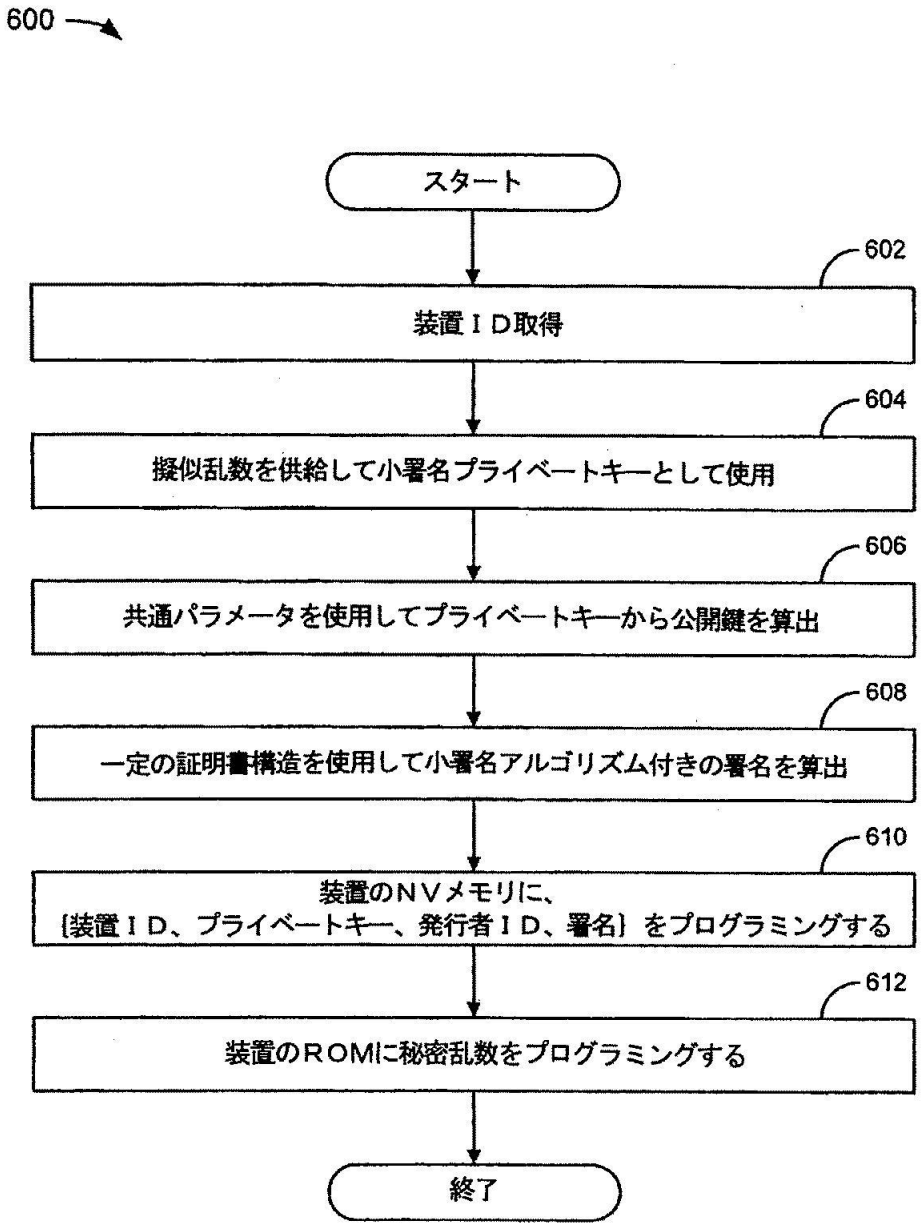
【図３】


300
スタート
302
デバイス証明書をセキュアデバイスにて作成
304
デバイス証明書をシステムの外部記憶装置に格納
終了

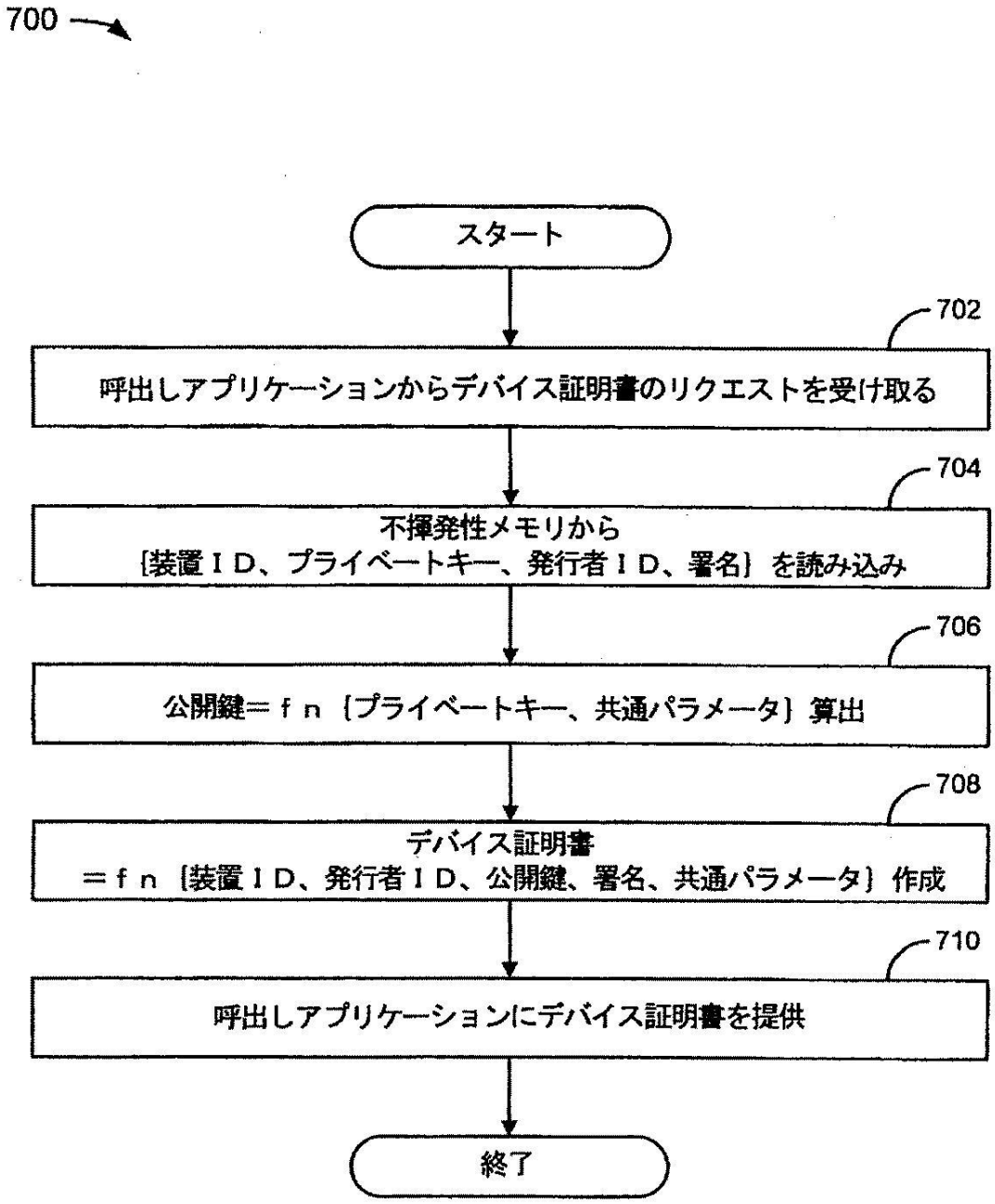
【図５】


500
セキュリティ
カーネル 514
OS 504
公開鍵
デバイス証明書・作成エンジン
517
524
プライベートキー／署名アクセス
鍵／署名ストア
518
セキュアプロセッサ
502
セキュリティＡＰＩ
516
プロテクト・メモリ
510
526
証明書リクエスト
522
デバイス証明書
520
証明書リクエスト
呼出しアプリケーション
508
チケットサービス
506
528
デバイス証明書

【図６】

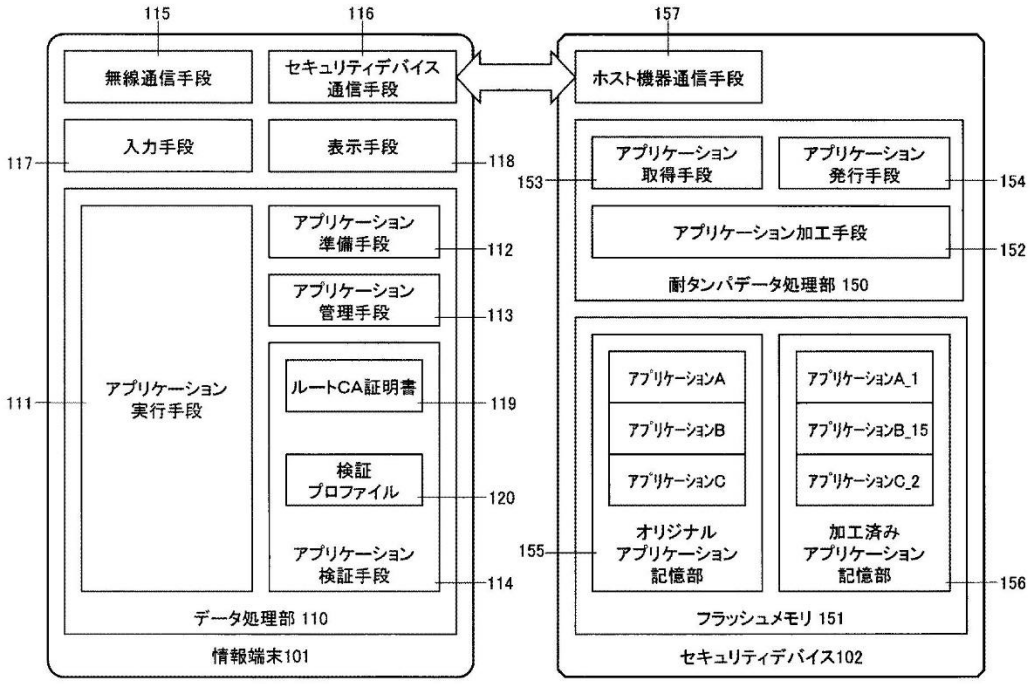

600
スタート
602
装置ＩＤ取得
604
擬似乱数を供給して小署名プライベートキーとして使用
606
共通パラメータを使用してプライベートキーから公開鍵を算出
608
一定の証明書構造を使用して小署名アルゴリズム付きの署名を算出
610
装置のＮＶメモリに、
{装置ＩＤ、プライベートキー、発行者ＩＤ、署名} をプログラミングする
612
装置のＲＯＭに秘密乱数をプログラミングする
終了

【図７】

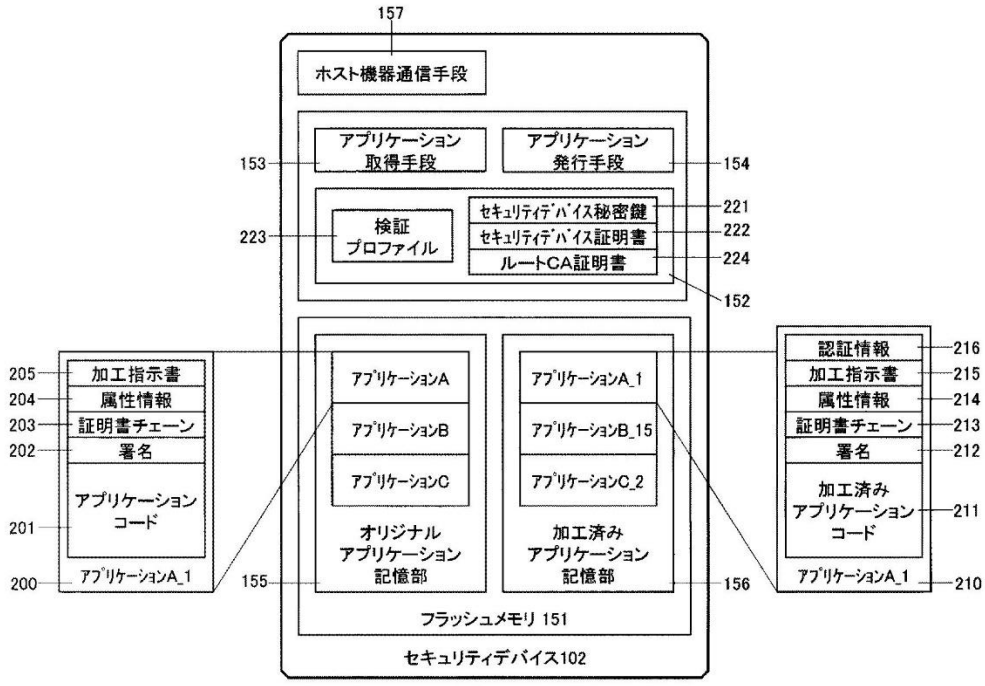

700
スタート
702
呼出しアプリケーションからデバイス証明書のリクエストを受け取る
704
不揮発性メモリから
〔装置ＩＤ、プライベートキー、発行者ＩＤ、署名〕を読み込み
706
公開鍵＝ｆｎ〔プライベートキー、共通パラメータ〕算出
708
デバイス証明書
＝ｆｎ〔装置ＩＤ、発行者ＩＤ、公開鍵、署名、共通パラメータ〕作成
710
呼出しアプリケーションにデバイス証明書を提供
終了

（別紙２）

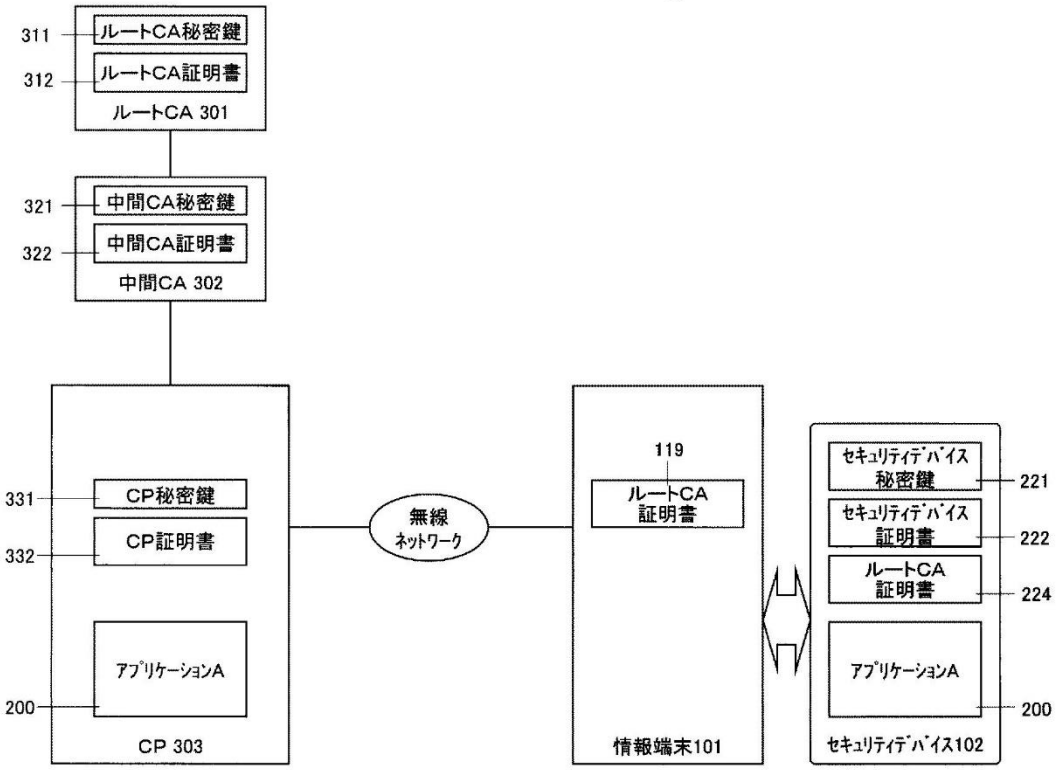
【図１】


115
116
157
無線通信手段
セキュリティデバイス通信手段
ホスト機器通信手段
入力手段
表示手段
117
118
153
アプリケーション取得手段
アプリケーション発行手段
154
アプリケーション加工手段
152
アプリケーション準備手段
112
アプリケーション管理手段
113
耐タンパデータ処理部 150
111
アプリケーション実行手段
ルートCA証明書
119
検証プロファイル
120
アプリケーション検証手段
114
アプリケーションA
アプリケーションB
アプリケーションC
アプリケーションA_1
アプリケーションB_15
アプリケーションC_2
155
オリジナルアプリケーション記憶部
加工済みアプリケーション記憶部
156
データ処理部 110
フラッシュメモリ 151
情報端末101
セキュリティデバイス102

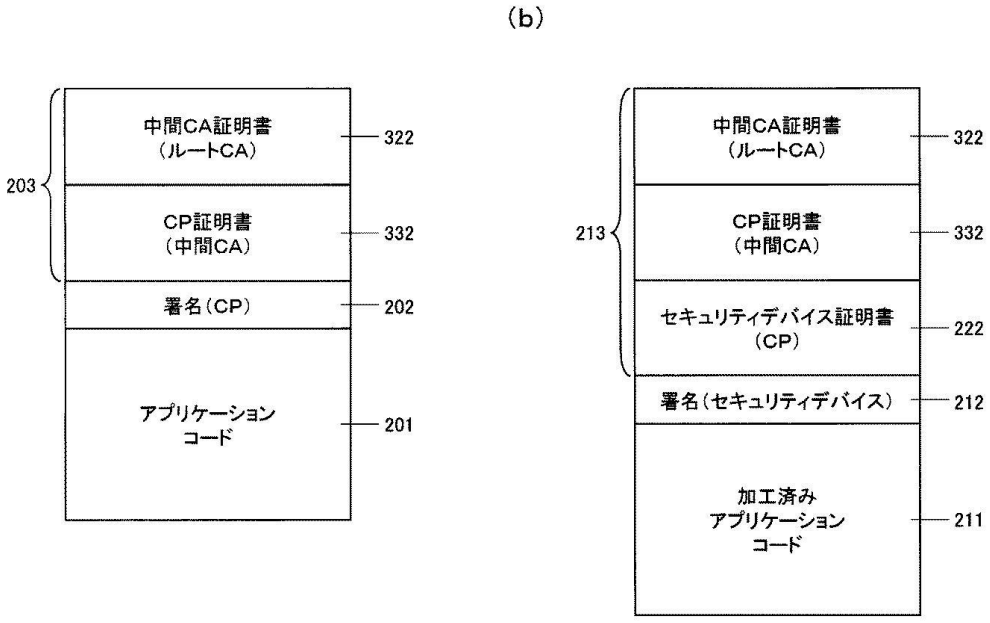
【図２】


157
ホスト機器通信手段
153
アプリケーション取得手段
アプリケーション発行手段
154
223
検証プロファイル
セキュリティデバイス秘密鍵
221
セキュリティデバイス証明書
222
ルートCA証明書
224
152
205
加工指示書
204
属性情報
203
証明書チェーン
202
署名
201
アプリケーションコード
200
アプリケーションA_1
アプリケーションA
アプリケーションB
アプリケーションC
アプリケーションA_1
アプリケーションB_15
アプリケーションC_2
155
オリジナルアプリケーション記憶部
加工済みアプリケーション記憶部
156
フラッシュメモリ 151
セキュリティデバイス102
認証情報
216
加工指示書
215
属性情報
214
証明書チェーン
213
署名
212
加工済みアプリケーションコード
211
アプリケーションA_1
210

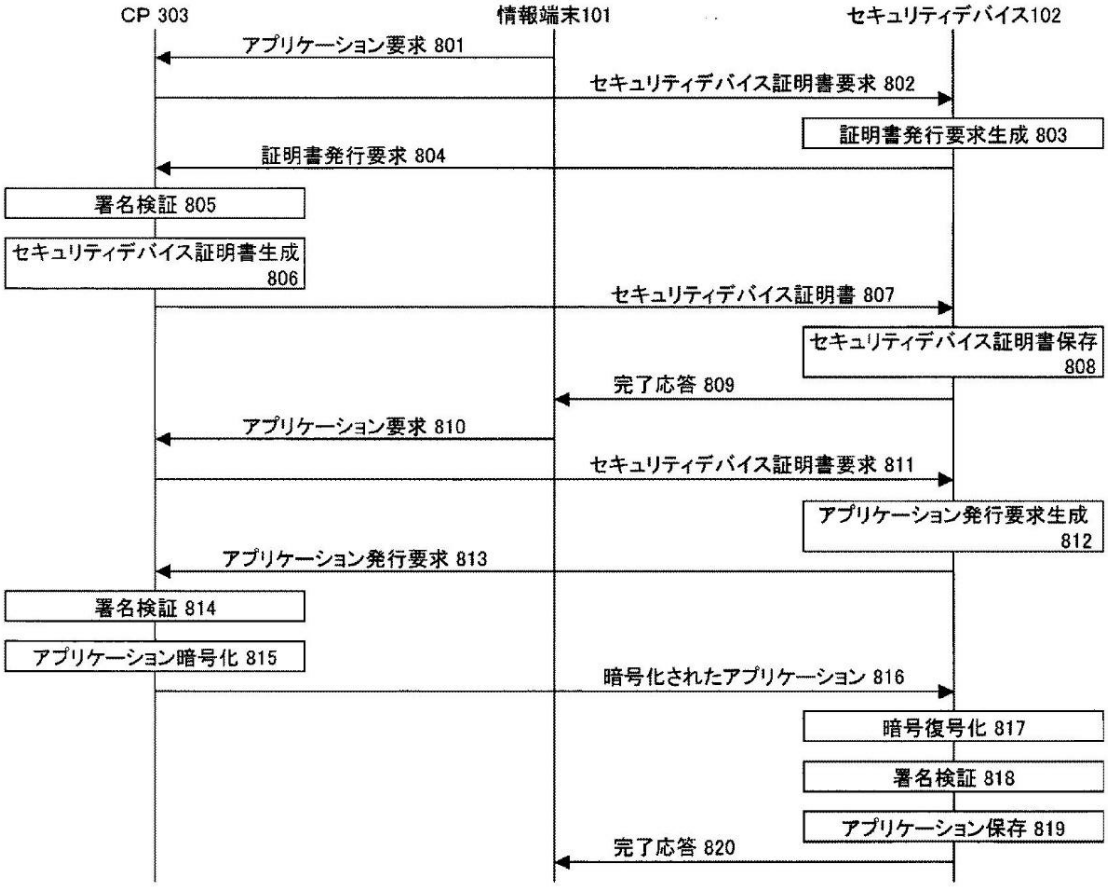
【図３】


311
ルートCA秘密鍵
312
ルートCA証明書
ルートCA 301
321
中間CA秘密鍵
322
中間CA証明書
中間CA 302
331
CP秘密鍵
332
CP証明書
アプリケーションA
200
CP 303
無線
ネットワーク
119
ルートCA
証明書
情報端末101
セキュリティデバイス
秘密鍵
221
セキュリティデバイス
証明書
222
ルートCA
証明書
224
アプリケーションA
200
セキュリティデバイス102

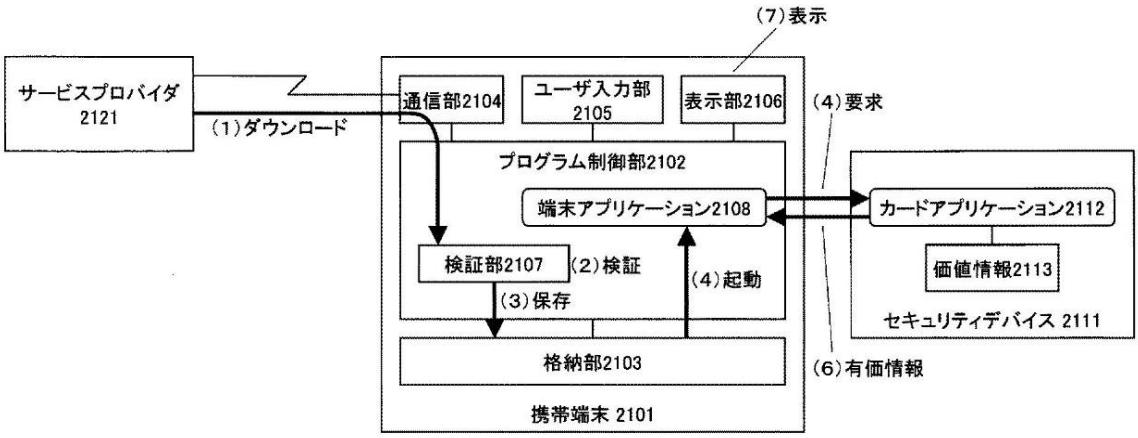
【図４】


(a)
(b)
203
中間CA証明書
(ルートCA)
322
CP証明書
(中間CA)
332
署名(CP)
202
アプリケーション
コード
201
213
中間CA証明書
(ルートCA)
322
CP証明書
(中間CA)
332
セキュリティデバイス証明書
(CP)
222
署名(セキュリティデバイス)
212
加工済み
アプリケーション
コード
211

【図８】

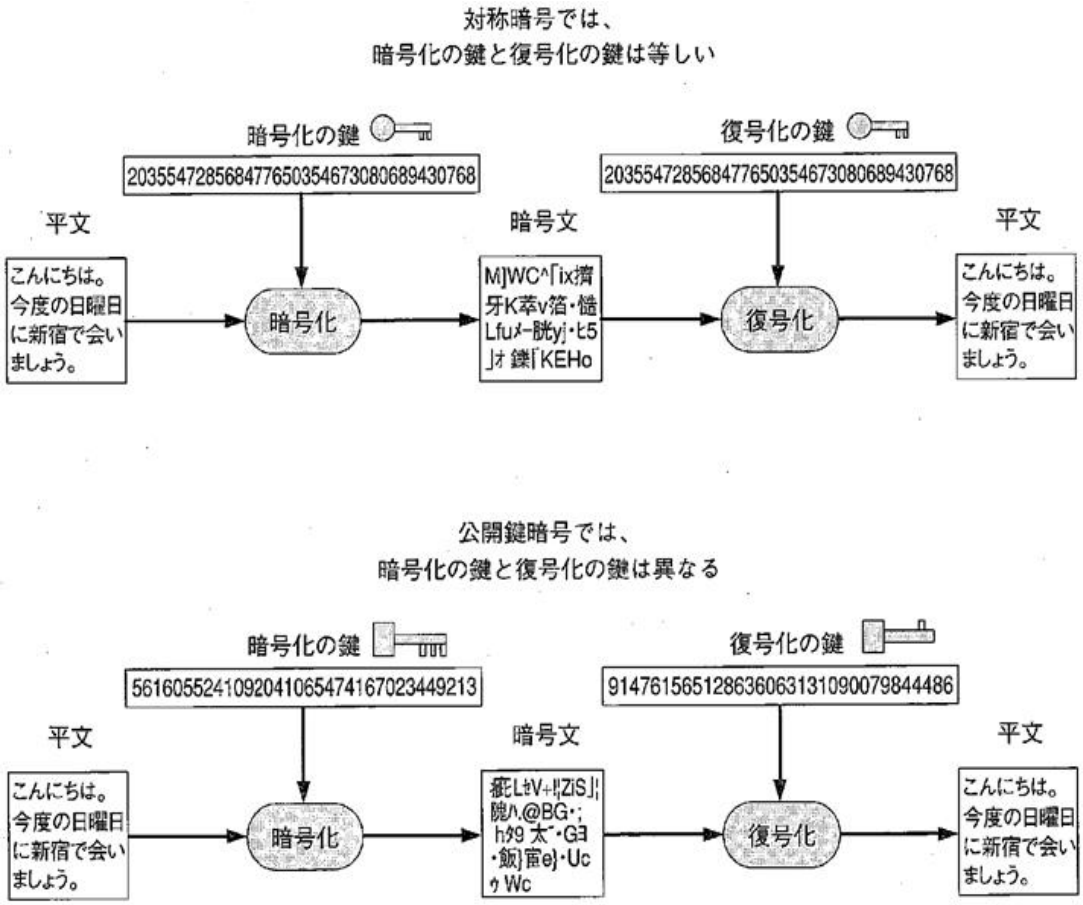

CP 303
情報端末101
セキュリティデバイス102
アプリケーション要求 801
セキュリティデバイス証明書要求 802
証明書発行要求生成 803
証明書発行要求 804
署名検証 805
セキュリティデバイス証明書生成 806
セキュリティデバイス証明書 807
セキュリティデバイス証明書保存 808
完了応答 809
アプリケーション要求 810
セキュリティデバイス証明書要求 811
アプリケーション発行要求生成 812
アプリケーション発行要求 813
署名検証 814
アプリケーション暗号化 815
暗号化されたアプリケーション 816
暗号復号化 817
署名検証 818
アプリケーション保存 819
完了応答 820

【図２１】

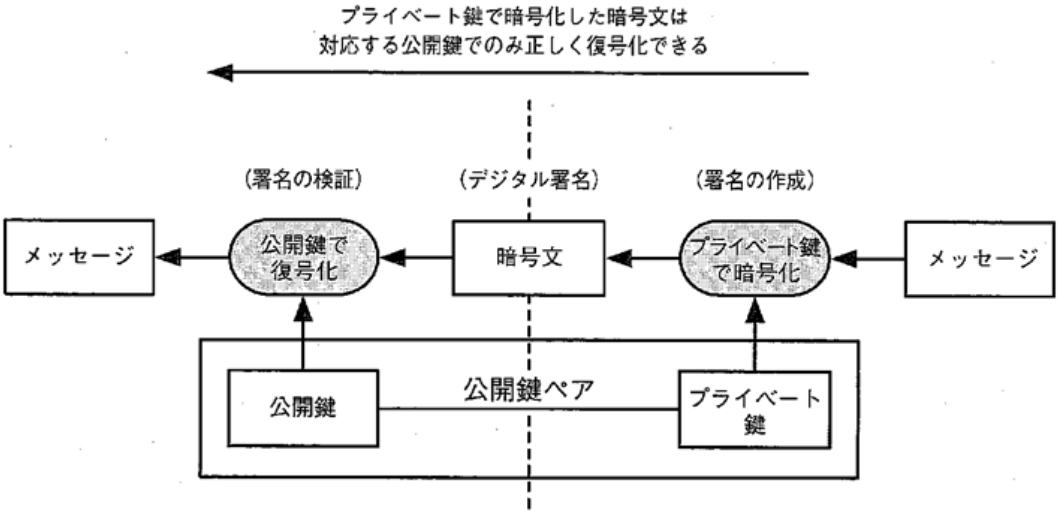

(7)表示
サービスプロバイダ 2121
(1)ダウンロード
通信部2104
ユーザ入力部 2105
表示部2106
(4)要求
プログラム制御部2102
端末アプリケーション2108
カードアプリケーション2112
検証部2107
(2)検証
(4)起動
価値情報2113
(3)保存
セキュリティデバイス 2111
格納部2103
(6)有価情報
携帯端末 2101

（別紙３）

Ｆｉｇ．１－８●対称暗号と公開鍵暗号



Ｆｉｇ．９－２●プライベート鍵による暗号化（デジタル署名）



（別紙４）

表8.6 X.509証明書の構造

証明書	署名前証明書	バージョン	
		シリアル番号	
		アルゴリズム識別子	
		発行者	
		有効期間	開始時刻
			終了時刻
		主体者	
		主体者公開鍵情報	アルゴリズム
			主体者公開鍵
		発行者ユニーク識別子	
		主体者ユニーク識別子	
		拡張領域	識別子
			重要度
			拡張値
	署名アルゴリズム		
	署名値		