【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】令和2年2月6日(2020.2.6)

【公表番号】特表2019-501461(P2019-501461A)
【公表日】平成31年1月17日(2019.1.17)
【年通号数】公開・登録公報2019-002
【出願番号】特願2018-535112(P2018-535112)
【国際特許分類】
Ｇ０６Ｆ　21/31　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/31

【手続補正書】
【提出日】令和1年12月17日(2019.12.17)
【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】
スマートカードアプリケーションのセキュリティを検証する方法であって：
前記スマートカードアプリケーションによって実行される現在のサービスのプロンプトを受信するステップ（３０３）と；
前記現在のサービスの関連データを取得するステップ（１０１）と；
前記現在のサービスの前記関連データとセキュリティパラメータとを特定するステップ（１０２）と；
前記現在のサービスの前記関連データが前記セキュリティパラメータと一致しているかどうかを検証するステップ（１０３）と；
前記スマートカードアプリケーションにサービス指示を送信するステップ（３０５）と；を備える、
セキュリティを検証する方法。
【請求項２】
前記現在のサービスの前記関連データが前記セキュリティパラメータと一致する場合に前記現在のサービスの継続を許可するステップ、又は、前記現在のサービスの前記関連データが前記セキュリティパラメータに一致していない場合に前記現在のサービスを終了するステップを更に備える、
請求項１に記載の方法。
【請求項３】
前記現在のサービスの前記関連データが、現在地情報、現在時刻情報、取引情報のうちの少なくとも１つ、又はこれらの組み合わせを含む、
請求項１又は２に記載の方法。
【請求項４】
前記現在のサービスの前記関連データは、前記現在地情報を備え、現在のサービスの前記関連データが前記セキュリティパラメータと一致しているかどうかを検証するステップは、前記現在地情報をある位置範囲と比較するステップを備える、
請求項３に記載の方法。
【請求項５】
前記スマートカードアプリケーションが外部との前記サービス処理を実行するときに、

前記現在のサービスの前記関連データを取得するステップは：
埋め込み型セキュリティチップに組み込まれたスマートカードアプリケーションが近距離通信（ＮＦＣ）コントローラと通信するときに、前記両者間での通信を監視して、前記現在のサービスの前記関連データを取得するステップを更に備える、
請求項１乃至請求項４のいずれか１項に記載の方法。
【請求項６】
前記スマートカードアプリケーションが外部との前記サービス処理を実行するときに、前記現在のサービスの前記関連データを取得するステップは：
前記仮想スマートカードアプリケーションが前記ＮＦＣコントローラと通信するときに、前記仮想スマートカードアプリケーションにおける前記両者間の通信を監視し、前記現在のサービスの前記関連データを取得するステップを更に備える、
請求項１乃至請求項５のいずれか１項に記載の方法。
【請求項７】
前記現在のサービスの前記関連データとセキュリティパラメータとを特定するステップの前に：
ユーザにより入力された前記セキュリティパラメータを受信し、格納するステップと；
ユーザの関連データに基づく解析を通してサーバにより得られたセキュリティパラメータを受信し、格納するステップと；を更に備える、
請求項１乃至請求項６のいずれか１項に記載の方法。
【請求項８】
前記セキュリティパラメータは、前記ユーザの動作履歴の解析に基づく、
請求項１乃至請求項７のいずれか１項に記載の方法。
【請求項９】
前記セキュリティパラメータは、あるエリアに対する前記ユーザの動作履歴の統計解析に基づく、
請求項８に記載の方法。
【請求項１０】
請求項１乃至請求項９のいずれか１項に記載の方法を実行するように構成された複数のモジュールを備える、
スマートカードアプリケーションのセキュリティを検証するためのデバイス。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００８５
【補正方法】変更
【補正の内容】
【００８５】
本願は実施を用いて表されているが、当業者は、本願がその主旨から逸脱しない多くの変形及び変更を含み、添付の特許請求の範囲が本願の主旨から逸脱しないこれらの変形及び変更を含むことを理解する。
以下、本発明の実施の態様の例を列挙する。
［第１の局面］
スマートカードアプリケーションのためのセキュリティ検証方法であって：
前記スマートカードアプリケーションが外部とのサービス処理を実行するときに、現在のサービスの関連データを取得するステップと；
前記現在のサービスの前記関連データとセキュリティパラメータとを特定するステップと；
前記現在のサービスの前記関連データが前記セキュリティパラメータと一致しない場合、前記現在のサービスを終了するステップと；を備える、
セキュリティ検証方法。
［第２の局面］

前記現在のサービスの前記関連データが前記セキュリティパラメータと一致する場合、前記現在のサービスの継続を許可するステップを更に備える、
第１の局面に記載のセキュリティ検証方法。
［第３の局面］
前記現在のサービスの前記関連データが、現在地情報、現在時刻情報、取引情報のうちの少なくとも１つ、又はこれらの組み合わせを含む、
第１の局面に記載のセキュリティ検証方法。
［第４の局面］
前記スマートカードアプリケーションが外部との前記サービス処理を実行するときに、前記現在のサービスの前記関連データを取得する前記ステップは：
埋め込み型セキュリティチップに組み込まれたスマートカードアプリケーションがＮＦＣコントローラと通信するときに、前記両者間での通信を監視して、前記現在のサービスの前記関連データを取得するステップを更に備える、
第１の局面に記載のセキュリティ検証方法。
［第５の局面］
前記スマートカードアプリケーションが外部との前記サービス処理を実行するときに、前記現在のサービスの前記関連データを取得する前記ステップは：
前記仮想スマートカードアプリケーションが前記ＮＦＣコントローラと通信するときに、前記仮想スマートカードアプリケーションにおける前記両者間の通信を監視し、前記現在のサービスの前記関連データを取得するステップを更に備える、
第１の局面に記載のセキュリティ検証方法。
［第６の局面］
前記現在のサービスの前記関連データとセキュリティパラメータとを特定する前記ステップの前に：
ユーザにより入力されたセキュリティパラメータを受信し、格納するステップと；
ユーザの関連データに基づく解析を通してサーバにより得られたセキュリティパラメータを受信し、格納するステップと；を更に備える、
第１の局面に記載のセキュリティ検証方法。
［第７の局面］
スマートカードアプリケーションのためのセキュリティ検証デバイスであって：
前記スマートカードアプリケーションが外部とのサービス処理を実行するときに、現在のサービスの関連データを取得するように構成された取得ユニットと；
前記現在のサービスの前記関連データとセキュリティパラメータとを特定するように構成された特定ユニットと；
前記現在のサービスの前記関連データが前記セキュリティパラメータと一致しない場合、前記現在のサービスを終了するように構成された処理ユニットと；を備える、
セキュリティ検証デバイス。
［第８の局面］
前記処理ユニットは、前記現在のサービスの前記関連データが前記セキュリティパラメータと一致する場合、前記現在のサービスの継続を許可するように更に構成される、
第７の局面に記載のセキュリティ検証デバイス。
［第９の局面］
前記現在のサービスの前記関連データは、現在地情報、現在時刻情報、及び取引情報のうちの少なくとも１つ、又はこれらの組み合わせを含む、
第７の局面に記載のセキュリティ検証デバイス。
［第１０の局面］
前記取得ユニットは、埋め込み型セキュリティチップに組み込まれたスマートカードアプリケーションとＮＦＣコントローラとの間の通信を監視し、前記現在のサービスの前記関連データを取得する、
第７の局面に記載のセキュリティ検証デバイス。

［第１１の局面］
前記取得ユニットは、仮想スマートカードアプリケーションに組み込まれ、前記仮想スマートカードアプリケーションとＮＦＣコントローラとの間の通信において前記現在のサービスの前記関連データを取得する、
第７の局面に記載のセキュリティ検証デバイス。
［第１２の局面］
セキュリティパラメータ受信ユニットを更に備え、前記セキュリティパラメータ受信ユニットは：
ユーザが入力したセキュリティパラメータを受信し、格納するように構成される；又は
サーバがユーザの関連データに基づく解析を通して取得したセキュリティパラメータを受信し、格納するように構成される；
第７の局面に記載のセキュリティ検証デバイス。