

【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29年10月19日 (2017.10.19)

【公表番号】特表2017-516240(P2017-516240A)

【公表日】平成29年6月15日 (2017.6.15)

【年通号数】公開・登録公報2017-022

【出願番号】特願2017-500803(P2017-500803)

【国際特許分類】

G 0 6 F 21/73 (2013.01)

G 0 6 F 21/55 (2013.01)

H 0 4 L 9/32 (2006.01)

【F I】

G 0 6 F 21/73

G 0 6 F 21/55

H 0 4 L 9/00 6 7 3 B

【手続補正書】

【提出日】平成29年9月11日 (2017.9.11)

【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】

装置のフィンガープリントを作成するコンピュータシステムであって、

装置管理システムに動作可能に接続される前記装置を備え、

前記装置管理システムは、

少なくとも 1 つのデータベースに動作可能に結合される少なくとも 1 つのプロセッサを含み、該少なくとも 1 つのプロセッサは、

第 1 のペイロードを前記装置から受信することであって、前記第 1 のペイロードは、特定の形式のデータと、前記装置を識別するのに使用される一意の識別子を含む装置指示子と、前記装置上で動作するファームウェアのバージョンの指示とを含む、前記受信すること、

前記装置のフィンガープリントを作成することであって、前記フィンガープリントは、特定の順序の前記特定の形式の 1 つ又は複数の別々のセクションのそれぞれのセクション形式と、前記装置上で動作するファームウェアのバージョンの指示とを含む、前記作成すること、

前記装置のフィンガープリントの記録及び前記一意の識別子を前記少なくとも 1 つのデータベースに記憶すること、

前記第 1 のペイロードの特定の形式を解析し、該特定の形式の 1 つ又は複数の別々のセクションにすること、

前記 1 つ又は複数の別々のセクションのそれぞれのセクション形式を判断すること、

前記特定の順序の前記 1 つ又は複数の別々のセクションのそれぞれのセクション形式の記録を作成すること、

前記装置から受信する各後続のペイロードの形式と前記装置のフィンガープリントとを比較し、前記装置が不正アクセスされたか否かを判断すること、を実行するように構成される、コンピュータシステム。

【請求項 2】

前記少なくとも1つのプロセッサは、前記装置が不正アクセスされたと判断すると、前記装置の状態を変更し、該装置が不正アクセスされたことを示すように更に構成されている、請求項1に記載のコンピュータシステム。

【請求項3】

前記少なくとも1つのプロセッサは、不正アクセスされていないことを示す状態を有する装置のペイロードのみを復号するように更に構成されている、請求項2に記載のコンピュータシステム。

【請求項4】

前記装置から受信する各後続のペイロードの形式と前記装置のフィンガープリントとを比較し、前記装置が不正アクセスされたか否かを判断することは、

第2のペイロードを前記装置から受信することであって、前記第2のペイロードは、第2の特定の形式の第2のデータ及び第2の装置指示子を含み、該第2の装置指示子は、前記装置を識別するのに使用される第2の一意の識別子を含む、前記受信すること、

前記第2の装置指示子に基づいて、前記フィンガープリントを前記少なくとも1つのデータベースから検索すること、

前記第2の特定の形式と前記フィンガープリントとを比較し、前記装置が不正アクセスされたか否かを判断すること、を含む、請求項1に記載のコンピュータシステム。

【請求項5】

前記第2の特定の形式と前記フィンガープリントとを比較し、前記装置が不正アクセスされたか否かを判断することは、

前記第2の特定の形式の1つ又は複数の別々のセクションのそれぞれの第2の形式と、前記フィンガープリントの1つ又は複数の別々のセクションのそれぞれのセクション形式とを比較することを含む、請求項4に記載のコンピュータシステム。

【請求項6】

前記少なくとも1つのプロセッサは、前記装置が不正アクセスされたと判断すると、ユーザに、前記装置が不正アクセスされたことを示すメッセージを送信するように更に構成されている、請求項5に記載のコンピュータシステム。

【請求項7】

前記少なくとも1つのプロセッサは、前記装置が不正アクセスされたと判断すると、いずれのデータも復号することなく前記第2のペイロードを無視するように更に構成されている、請求項6に記載のコンピュータシステム。

【請求項8】

装置のフィンガープリントを作成するコンピュータシステムであって、

装置管理システムに動作可能に接続される前記装置を備え、

前記装置管理システムは、

少なくとも1つのデータベースに動作可能に結合される少なくとも1つのプロセッサを含み、該少なくとも1つのプロセッサは、

特定の装置からの複数のペイロードを受信することであって、各ペイロードは、或る形式の暗号化されたデータ及び暗号化されていないデータを含み、特定の装置からの第1のペイロードは、前記装置を識別するのに使用される一意の識別子を含む装置指示子と、前記装置上で動作するファームウェアのバージョンの指示とを含む、前記複数のペイロードを受信すること、

前記装置のフィンガープリントを作成することであって、前記フィンガープリントは、特定の順序の前記特定の形式の1つ又は複数の別々のセクションのそれぞれのセクション形式と、前記装置上で動作するファームウェアのバージョンの指示とを含む、前記作成すること、

前記特定の装置からの各ペイロードの形式と、前記特定の装置に関連するフィンガープリントとを比較すること、

前記特定の装置から受信したペイロードのうちの特定のペイロードの形式が、前記特定の装置に関連するフィンガープリントに一致しないと判断すると、前記特定のペイロード

の暗号化されたデータを復号することを拒否するとともに、暗号化されたデータを復号することを拒否する通知を、ユーザに関連するユーザコンピューティングシステムに送信すること、を実行するように構成され、

前記装置のフィンガープリントを作成することは、

前記第 1 のペイロードの特定の形式を解析し、該特定の形式の 1 つ又は複数の別々のセクションにすること、

前記 1 つ又は複数の別々のセクションのそれぞれの前記セクション形式を判断すること

、
前記特定の順序の前記 1 つ又は複数の別々のセクションのそれぞれの前記セクション形式の記録を作成すること、をさらに含む、コンピュータシステム。

【請求項 9】

前記少なくとも 1 つのプロセッサは、前記特定の装置から受信したペイロードのうちの特定のペイロードの形式が、前記特定の装置に関連するフィンガープリントに一致しないと判断すると、前記特定の装置に関連する状態をアクティブから改ざんに変更するように更に構成されている、請求項 8 に記載のコンピュータシステム。

【請求項 10】

前記特定の装置からの各ペイロードは、特定の順序のデータの 1 つ又は複数のセグメントを含む、請求項 8 に記載のコンピュータシステム。

【請求項 11】

前記特定の装置からのペイロードに含まれるデータの 1 つ又は複数のセグメントのそれぞれは、特定の形式である、請求項 10 に記載のコンピュータシステム。

【請求項 12】

前記 1 つ又は複数のセグメントの特定のセグメントの特定の形式は、文字形式である、請求項 11 に記載のコンピュータシステム。

【請求項 13】

前記 1 つ又は複数のセグメントの第 2 の特定のセグメントの特定の形式は、16 進形式である、請求項 12 に記載のコンピュータシステム。

【請求項 14】

前記少なくとも 1 つのプロセッサは、

第 2 の特定の装置からのペイロードを受信することであって、各ペイロードは、第 2 の形式の暗号化されたデータ及び暗号化されていないデータを含む、前記ペイロードを受信すること、

前記第 2 の特定の装置からの各ペイロードの第 2 の形式と、前記第 2 の特定の装置に関連する第 2 のフィンガープリントとを比較すること、

前記第 2 の特定の装置から受信したペイロードのうちの第 2 の特定のペイロードの形式が、前記第 2 の特定の装置に関連する前記第 2 のフィンガープリントに一致しないと判断すると、前記第 2 の特定のペイロードの暗号化されたデータを復号することを拒否するとともに、前記暗号化されたデータを復号することを拒否する通知を、第 2 のユーザに関連する第 2 のコンピューティングシステムに送信すること、を実行するように更に構成されている、請求項 8 に記載のコンピュータシステム。

【請求項 15】

前記フィンガープリント及び前記第 2 のフィンガープリントは同じフィンガープリントではない、請求項 14 に記載のコンピュータシステム。

【請求項 16】

装置のフィンガープリントを作成するコンピュータ実装方法であって、

データを暗号化可能な装置を準備すること、

前記装置に動作可能に結合されるコンピュータシステムを準備することであって、

前記コンピュータシステムは、

前記装置から受信したデータを復号する復号手段、

前記装置に関連するフィンガープリントを作成するフィンガープリント作成手段、

少なくとも1つのデータベース、

前記復号手段、前記フィンガープリント作成手段及び前記少なくとも1つのデータベースに動作可能に結合される少なくとも1つのプロセッサを含む、前記準備すること、

前記少なくとも1つのプロセッサが、前記装置から第1のペイロードを受信することであって、前記第1のペイロードは、特定の形式のデータと、前記装置を識別するのに使用される一意の識別子を含む装置指示子と、前記装置上で動作するファームウェアのバージョンの指示と、を含む、前記受信すること、

前記フィンガープリント作成手段によって、前記装置のフィンガープリントを作成することであって、該フィンガープリントは、特定の順序の前記特定の形式の1つ又は複数の別々のセクションのそれぞれのセクション形式と、前記装置上で動作するファームウェアのバージョンの指示と、を含む、前記作成すること、

前記少なくとも1つのデータベースにおいて前記装置のフィンガープリント及び前記一意の識別子の記録を記憶するとともに、前記少なくとも1つのプロセッサによって前記装置の状態をアクティブに変更すること、

前記少なくとも1つのプロセッサによって、前記装置から受信する後続のペイロードの第2の特定の形式と、前記装置の前記フィンガープリントとを比較し、該装置が不正アクセスされたか否かを判断すること、

前記装置が不正アクセスされていないと判断すると、前記復号手段によって、前記後続のペイロードの暗号化されたデータを復号すること、を備え、

前記装置のフィンガープリントを作成することは、

前記第1のペイロードの特定の形式を解析し、該特定の形式の1つ又は複数の別々のセクションにすること、

前記1つ又は複数の別々のセクションのそれぞれのセクション形式を判断すること、

前記特定の順序の前記1つ又は複数の別々のセクションのそれぞれのセクション形式の記録を作成すること、をさらに含む、コンピュータ実装方法。

【請求項17】

前記少なくとも1つのプロセッサによって、前記装置から前記後続のペイロードを受信するステップであって、該後続のペイロードは前記第2の特定の形式のデータ及び前記装置指示子を含む、前記受信するステップ、

前記少なくとも1つのプロセッサによって、前記第2の特定の形式と前記フィンガープリントとを比較するように前記少なくとも1つのデータベースから前記フィンガープリントを検索するステップ、を更に備える、請求項16に記載のコンピュータ実装方法。

【請求項18】

前記装置が不正アクセスされたと判断すると、前記少なくとも1つのプロセッサによって、前記後続のペイロードの暗号化されたデータを復号することを拒否するステップを更に備える請求項17に記載のコンピュータ実装方法。

【手続補正2】

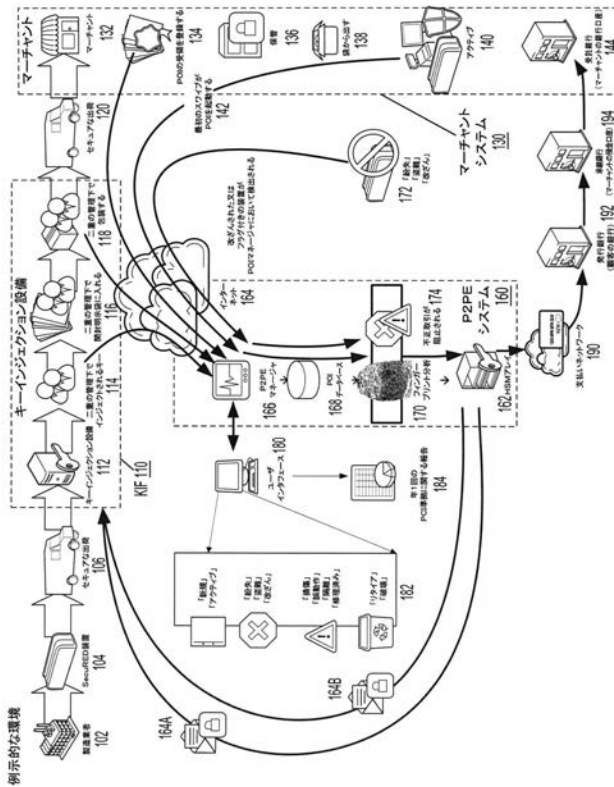
【補正対象書類名】図面

【補正対象項目名】全図

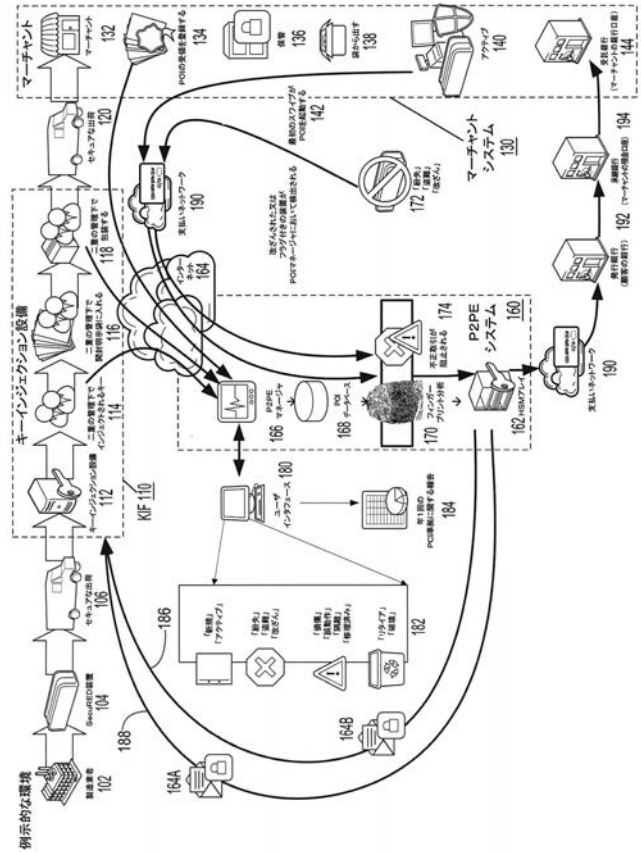
【補正方法】変更

【補正の内容】

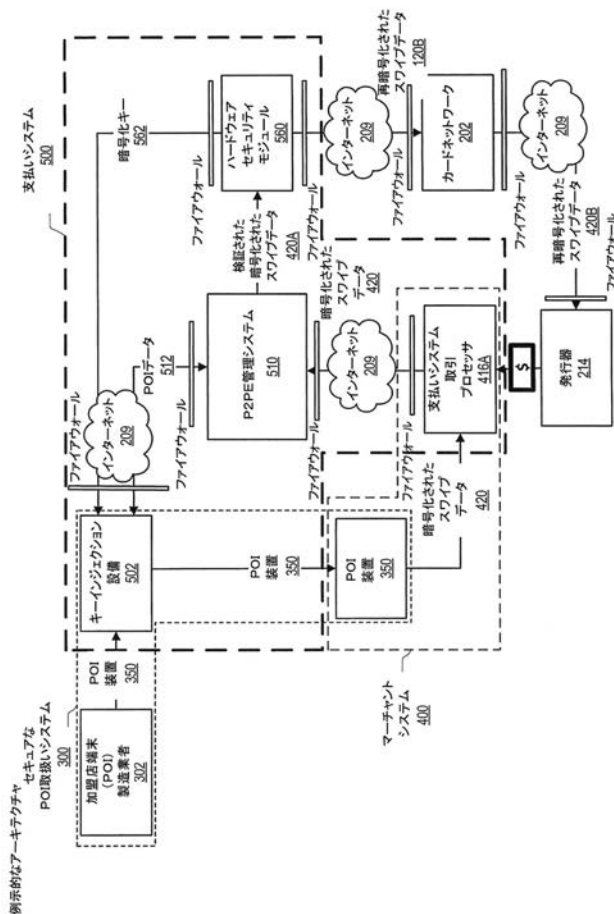
【図 1 A】



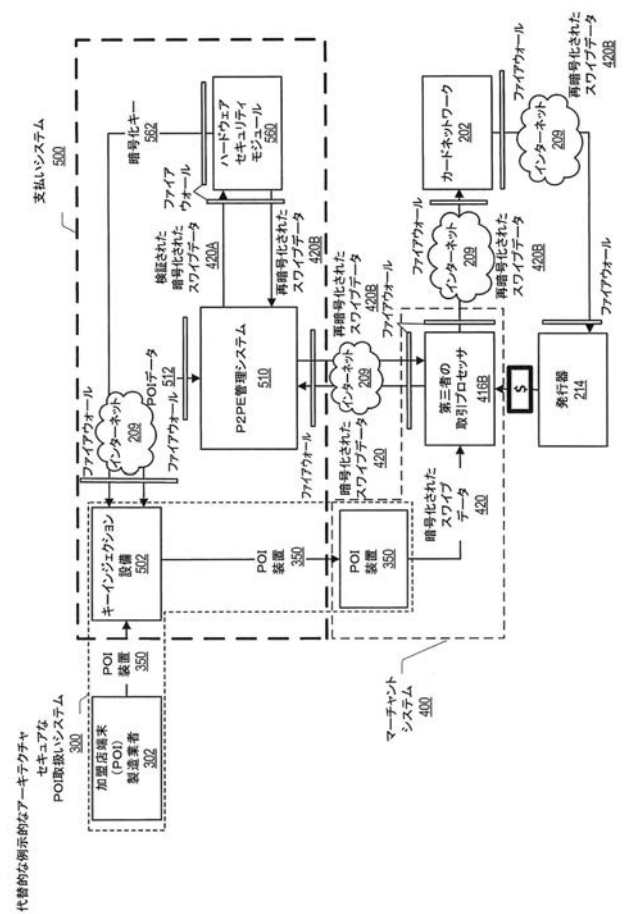
【図 1 B】



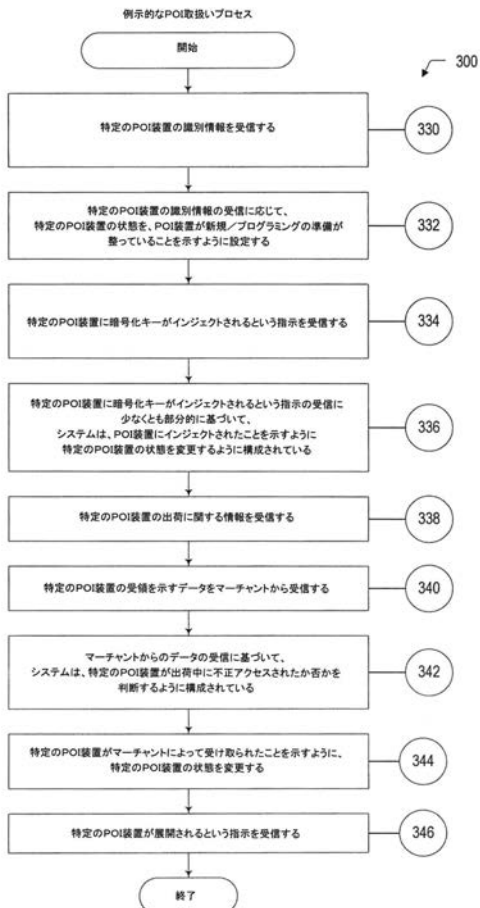
【図 2 A】



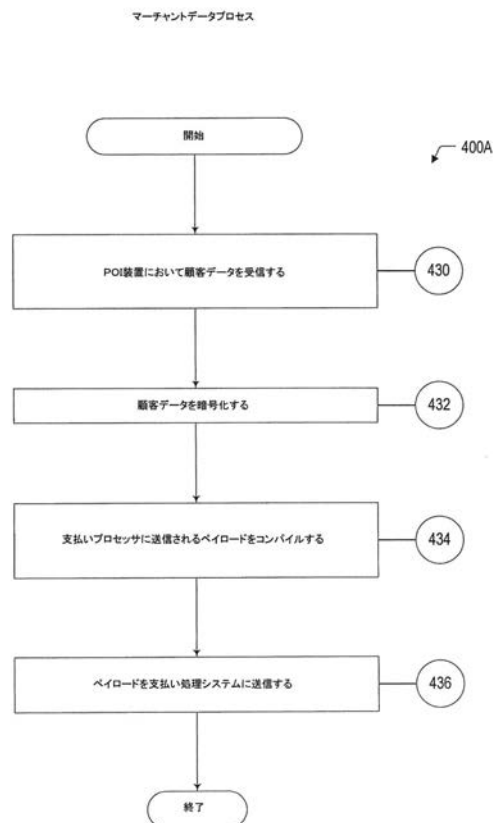
【図 2 B】



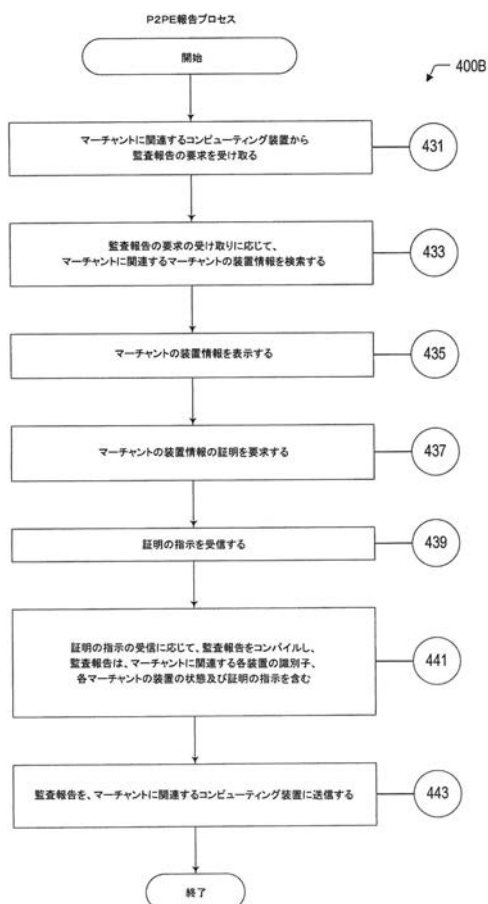
【図 3】



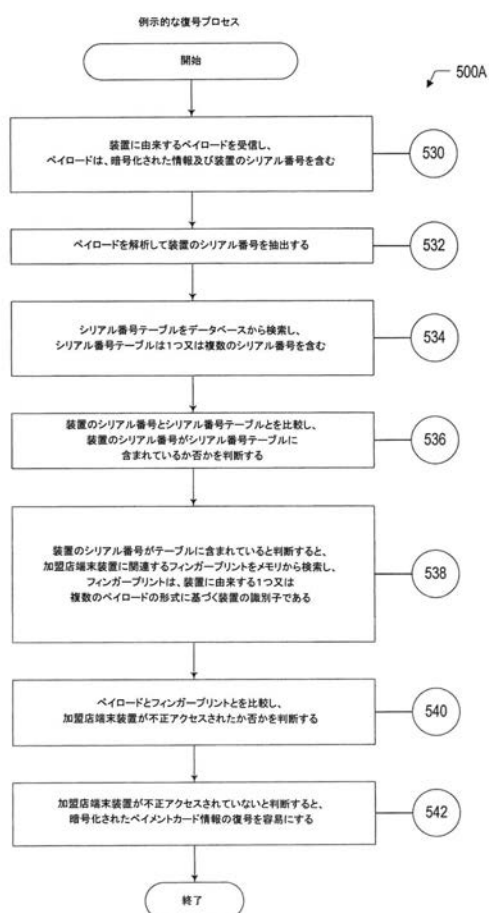
【図 4 A】



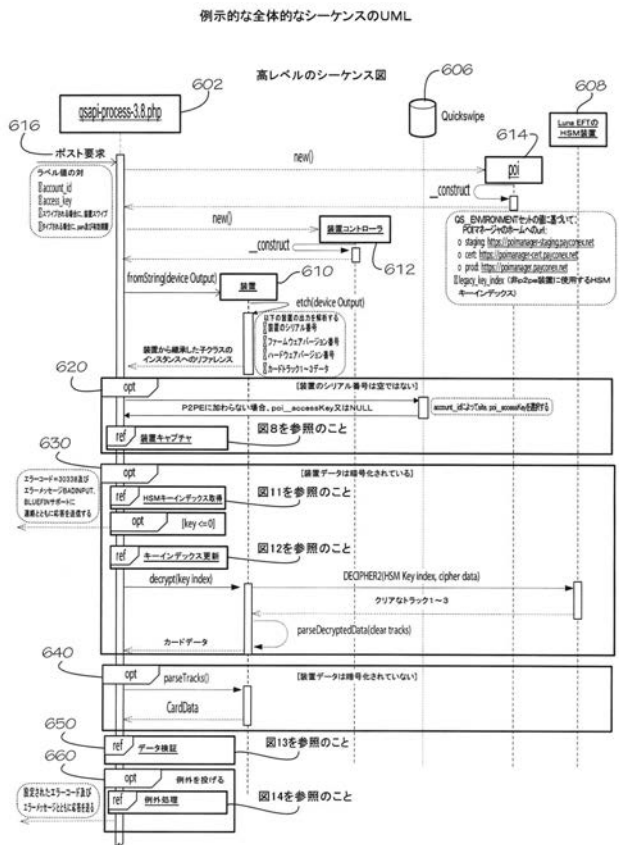
【図 4 B】



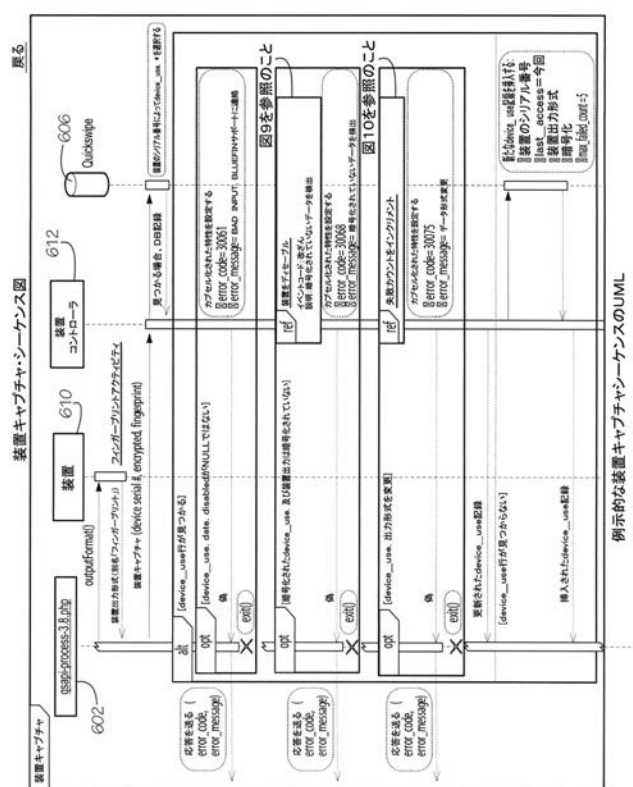
【図 5 A】



【図 6】

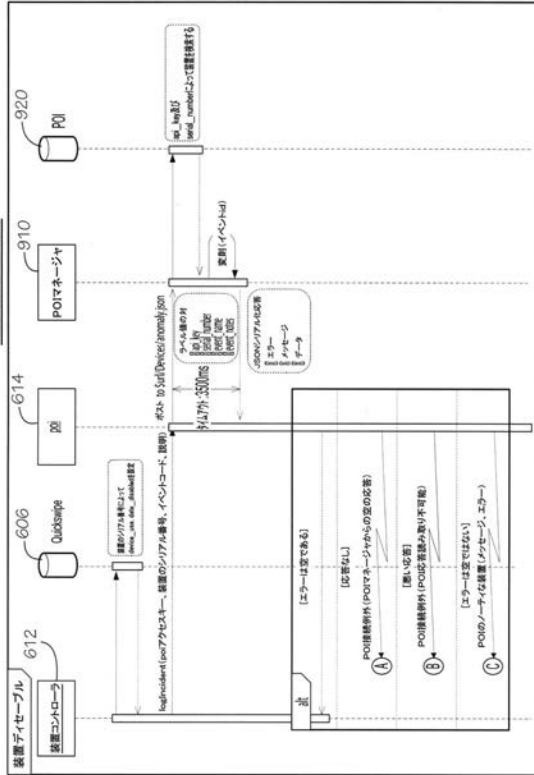


【図 8】



例示的な出力評価のUML

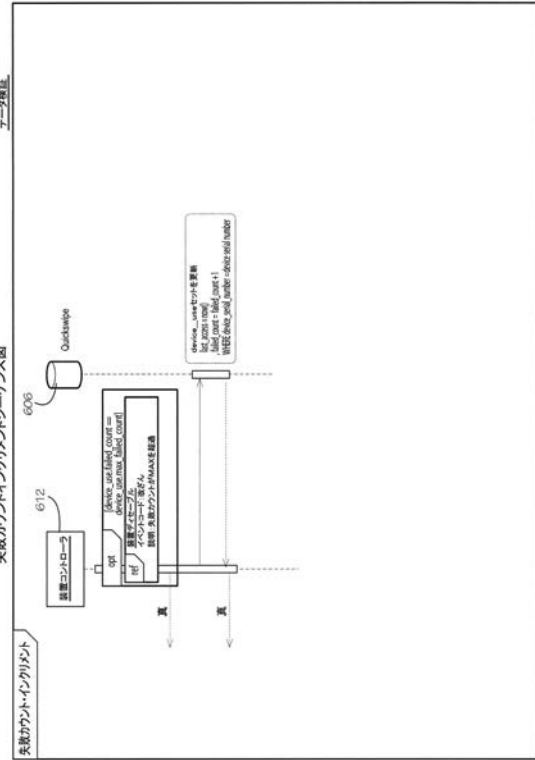
【図 9】

装置ディセーブルシーケンス図
失敗カウント・インクリメント
キーインデックス更新

【図 10】

装置ディセーブル
シーケンス

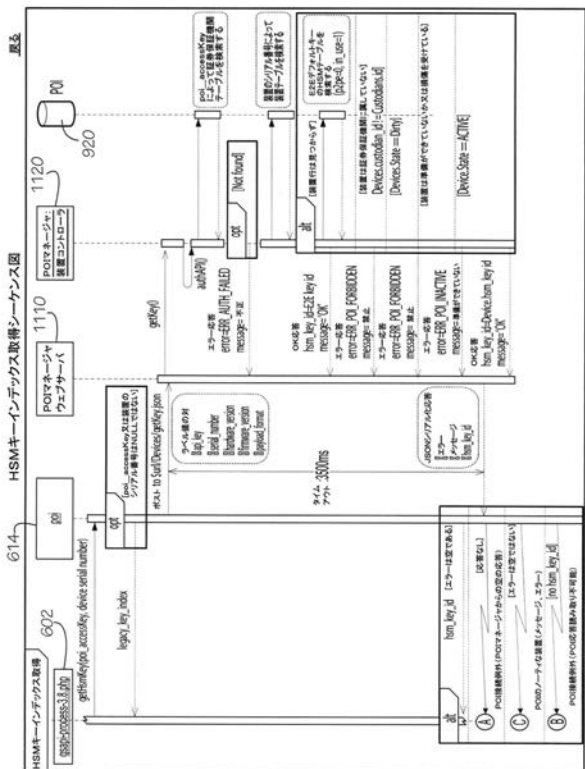
失敗カウント・インクリメントシーケンス図



例示的な失敗カウント・シーケンスのUML

【図 11】

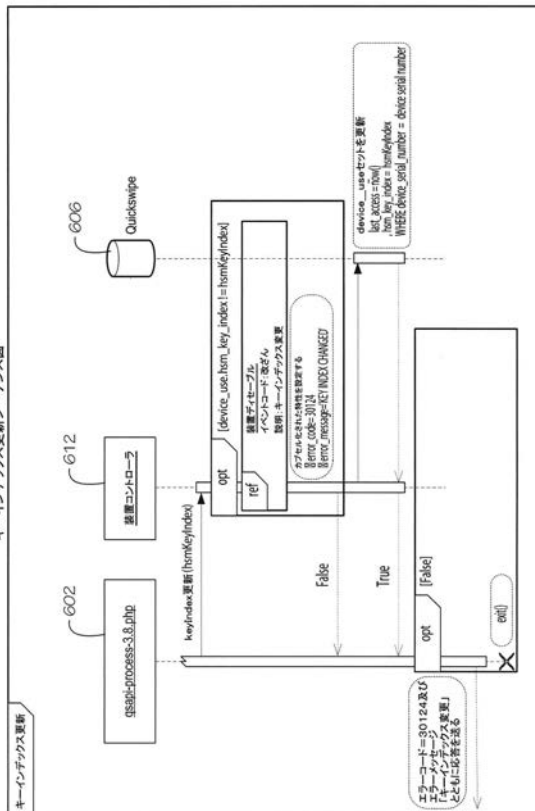
HSMキーインデックス取得シーケンス図



例示的なHSMキーインデックスシーケンスのUML

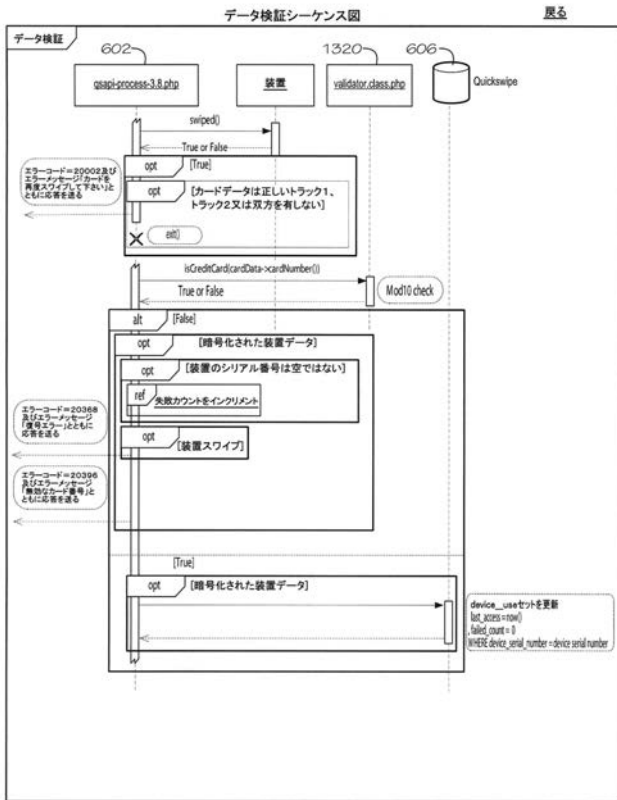
【図 12】

キーインデックス更新シーケンス図



例示的なキーインデックス更新シーケンスのUML

【図 13】



例示的な検証シーケンスのUML

【図 14】

