

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6217092号  
(P6217092)

(45) 発行日 平成29年10月25日 (2017.10.25)

(24) 登録日 平成29年10月6日 (2017.10.6)

(51) Int.Cl. F I  
**G O 6 F 21/62 (2013.01)** G O 6 F 21/62  
**G O 6 F 21/12 (2013.01)** G O 6 F 21/12 3 1 0

請求項の数 1 (全 35 頁)

(21) 出願番号	特願2013-43286 (P2013-43286)	(73) 特許権者	000005223
(22) 出願日	平成25年3月5日 (2013.3.5)		富士通株式会社
(65) 公開番号	特開2014-170501 (P2014-170501A)		神奈川県川崎市中原区上小田中4丁目1番1号
(43) 公開日	平成26年9月18日 (2014.9.18)	(74) 代理人	100103528
審査請求日	平成27年10月7日 (2015.10.7)		弁理士 原田 一男
		(72) 発明者	野田 敏達
			神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
		(72) 発明者	藤原 雪絵
			神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
		(72) 発明者	金谷 延幸
			神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

最終頁に続く

(54) 【発明の名称】 情報処理装置、システム、情報処理方法及びプログラム

(57) 【特許請求の範囲】

【請求項 1】

第1の情報処理装置と、前記第1の情報処理装置とW e bサーバとのデータ通信を中継する携帯型の第2の情報処理装置とを含み、

前記第1の情報処理装置は、

前記第2の情報処理装置を介して第1W e bサーバから受信した第1プログラムの実行中に、特定機能に係る呼び出しの発生を検出する検出部

を有し、

前記第2の情報処理装置は、

前記呼び出しの発生を検出すると、第2W e bサーバから受信した第2プログラムの動作状況に係るコンテキストを生成する生成部と、

前記コンテキストに基づいて、前記呼び出しの許否を判定する判定部と、

前記呼び出しを許容すると判定した場合に、前記第2の情報処理装置における前記特定機能呼び出し中継部

を有するシステム。

【発明の詳細な説明】

【技術分野】

【0001】

本技術は、プログラムによる機能呼び出し技術に関する。

【背景技術】

10

20

## 【 0 0 0 2 】

ある特許文献には、ユーザソフトウェアアプリケーションの能力を制御する技術が開示されている。この技術では、ユーザソフトウェアアプリケーションにおいて許可されていなかった付加的な機能の動作を、所定のコンテンツを受け取った場合に許可する。

## 【 0 0 0 3 】

また、別の特許文献には、サービス定義に基づいてW e b サービスへのアクセスに関する許可ポリシーを定義する技術が開示されている。

## 【 0 0 0 4 】

このように、ユーザソフトウェアアプリケーションの付加的な機能やW e b サービスへのアクセスを制限すれば、利用者による不当な使用を排除し、ユーザソフトウェアアプリケーションやW e b サービスの提供者側の利益が守られる面がある。

10

## 【 0 0 0 5 】

但し、機能の制限によって排除されるのは、利用者側の使用に限られない。例えば、あるオペレーティングシステムでは、W e b アプリケーションによって利用できる機能を予め設定し、特定のW e b アプリケーションによる特定機能の利用を制限するようにしている。このようにすれば、プログラムの提供者側で企図する処理を利用者の判断で制限することによって、利用者側の安全性が保たれる。

## 【 先行技術文献 】

## 【 特許文献 】

## 【 0 0 0 6 】

20

【 特許文献 1 】 特表 2 0 0 5 - 5 1 8 6 0 2 号公報

【 特許文献 2 】 特表 2 0 0 8 - 5 3 7 8 2 3 号公報

## 【 発明の概要 】

## 【 発明が解決しようとする課題 】

## 【 0 0 0 7 】

本技術の目的は、一側面では、プログラムによる特定機能の利用を、自動的に制限することを目的とする。

## 【 課題を解決するための手段 】

## 【 0 0 0 8 】

一態様に係る情報処理装置は、プログラムの実行中に、特定機能に係る呼び出しの発生を検出すると、自装置の状況に係るコンテキストを生成する生成部と、コンテキストに基づいて、呼び出しの許否を判定する判定部とを有する。

30

## 【 発明の効果 】

## 【 0 0 0 9 】

一側面としては、プログラムによる特定機能の利用を、自動的に制限できる。

## 【 図面の簡単な説明 】

## 【 0 0 1 0 】

【 図 1 】 図 1 は、機能制限システムの利用態様の例を示す図である。

【 図 2 】 図 2 は、機能制限システムの利用態様の例を示す図である。

【 図 3 】 図 3 は、機能制限システムの構成例を示す図である。

40

【 図 4 】 図 4 は、利用者端末のモジュール構成例を示す図である。

【 図 5 】 図 5 は、格納部と制限部と記憶部の構成例を示す図である。

【 図 6 】 図 6 は、生成ルールテーブルの例を示す図である。

【 図 7 】 図 7 は、判定ルールテーブル例を示す図である。

【 図 8 】 図 8 は、シーケンスの例を示す図である。

【 図 9 】 図 9 は、シーケンスの例を示す図である。

【 図 1 0 】 図 1 0 は、シーケンスの例を示す図である。

【 図 1 1 】 図 1 1 は、シーケンスの例を示す図である。

【 図 1 2 】 図 1 2 は、検出処理（エンジン監視型）フローの例を示す図である。

【 図 1 3 】 図 1 3 は、判定処理フローの例を示す図である。

50

- 【図 1 4】図 1 4 は、コンテキスト生成処理フローの例を示す図である。
- 【図 1 5】図 1 5 は、実施の形態 2 に係るシーケンスの例を示す図である。
- 【図 1 6】図 1 6 は、実施の形態 2 に係るシーケンスの例を示す図である。
- 【図 1 7】図 1 7 は、実施の形態 2 に係るシーケンスの例を示す図である。
- 【図 1 8】図 1 8 は、実施の形態 2 に係るシーケンスの例を示す図である。
- 【図 1 9】図 1 9 は、検出処理（API 監視型）フローの例を示す図である。
- 【図 2 0】図 2 0 は、実施の形態 3 に係る機能制限システムの構成例を示す図である。
- 【図 2 1】図 2 1 は、中継装置のモジュール構成例を示す図である。
- 【図 2 2】図 2 2 は、実施の形態 3 に係る格納部と制限部と記憶部の構成例を示す図である。
- 【図 2 3】図 2 3 は、実施の形態 3 に係る利用者端末のモジュール構成例を示す図である。
- 【図 2 4】図 2 4 は、実施の形態 3 に係るシーケンスの例を示す図である。
- 【図 2 5】図 2 5 は、実施の形態 3 に係るシーケンスの例を示す図である。
- 【図 2 6】図 2 6 は、実施の形態 3 に係るシーケンスの例を示す図である。
- 【図 2 7】図 2 7 は、実施の形態 3 に係るシーケンスの例を示す図である。
- 【図 2 8】図 2 8 は、実施の形態 4 に係る格納部と制限部と記憶部の構成例を示す図である。
- 【図 2 9】図 2 9 は、実施の形態 4 に係る利用者端末のモジュール構成例を示す図である。
- 【図 3 0】図 3 0 は、実施の形態 4 に係るシーケンスの例を示す図である。
- 【図 3 1】図 3 1 は、実施の形態 4 に係るシーケンスの例を示す図である。
- 【図 3 2】図 3 2 は、実施の形態 4 に係るシーケンスの例を示す図である。
- 【図 3 3】図 3 3 は、実施の形態 4 に係るシーケンスの例を示す図である。
- 【図 3 4】図 3 4 は、携帯型情報処理装置のハードウェア構成例を示す図である。

【発明を実施するための形態】

【0011】

[実施の形態 1]

本実施の形態では、状況に係るコンテキストに基づいて、Web アプリケーションに対して利用者端末のオペレーティングシステムで提供する API（Application Program Interface）の呼び出しを制限する。

【0012】

まず、図 1 及び 2 に基づいて、機能制限システムの利用態様について説明する。図 1 に示す機能制限システムの利用態様は、位置条件とネットワーク条件とに基づいて、コンテキストが判定される例を示している。つまり、この利用態様におけるコンテキストは、利用者端末 100 の位置と利用者端末 100 が接続するネットワークとによる状況を識別する情報である。また、この利用態様では、コンテキストに基づいて、アドレス帳機能に係る API と署名機能に係る API との利用可否が判定される例を示している。

【0013】

利用者端末 100 が社内ネットワークに接続している状況では、コンテキスト「CNT\_\_A」が生成される。そして、コンテキスト「CNT\_\_A」では、すべての Web アプリケーションにおいてアドレス帳機能に係る API についての判定結果が「利用可」となり、署名機能に係る API についての判定結果も「利用可」となる。

【0014】

つまり、利用者端末 100 は、その位置に関わらず、社内ネットワークに接続していれば、あらゆる Web アプリケーションにおいてアドレス帳の機能と署名の機能とが動作する。この場合には、例えば社員間の連絡や社用文書の発行などが許可される。

【0015】

利用者端末 100 が社内ネットワーク以外に接続し、且つ利用者端末 100 が会社敷地内（以下、社内という。）に位置している状況では、コンテキスト「CNT\_\_B」が生成

10

20

30

40

50

される。そして、コンテキスト「CNT\_\_B」では、すべてのWebアプリケーションにおいてアドレス帳機能に係るAPIについての判定結果が「利用可」となり、署名機能に係るAPIについての判定結果が「利用不可」となる。

【0016】

つまり、利用者端末100が社内で社内ネットワーク以外に接続していれば、あらゆるWebアプリケーションにおいてアドレス帳の機能は動作するが、署名の機能は動作しない。この場合には、例えば社員間の連絡は許可されるが、社用文書の発行は拒否される。

【0017】

利用者端末100が社内ネットワーク以外に接続し、且つ利用者端末100が会社敷地外（以下、社外という。）に位置している状況では、コンテキスト「CNT\_\_C」が生成される。そして、コンテキスト「CNT\_\_C」では、すべてのWebアプリケーションにおいてアドレス帳機能に係るAPIについての判定結果が「利用不可」となり、署名機能に係るAPIについての判定結果も「利用不可」となる。

10

【0018】

つまり、利用者端末100が社外で社内ネットワーク以外に接続していれば、あらゆるWebアプリケーションにおいてアドレス帳の機能も、署名の機能も動作しない。この場合には、例えば社員間の連絡も、社用文書の発行も拒否される。以上で、図1に示す機能制限システムの利用態様の説明を終える。

【0019】

図2に示す機能制限システムの利用態様の説明に移る。図2に示す機能制限システムの利用態様は、時刻条件とWebアプリケーション条件とに基づいて、コンテキストが判定される例を示している。つまり、この利用態様におけるコンテキストは、現在時刻と利用者端末100で動作しているWebアプリケーションとによる状況を識別する情報である。

20

【0020】

現在時刻が、勤務時間帯内であり、利用者端末100でWebアプリケーション「APL\_\_X」が動作している状況では、コンテキスト「CNT\_\_D」が生成される。そして、コンテキスト「CNT\_\_D」では、Webアプリケーション「APL\_\_Z」においてGPS（Global Positioning System）機能に係るAPIについての判定結果が「利用可」となり、復号機能に係るAPIについての判定結果も「利用可」となる。

30

【0021】

つまり、利用者端末100は、勤務時間帯内に、Webアプリケーション「APL\_\_X」を動作させていけば、Webアプリケーション「APL\_\_Z」においてGPSの機能と復号の機能とが動作する。この場合には、例えば所在位置に関連する秘密文書を閲覧することが許可される。

【0022】

現在時刻が、勤務時間帯内であり、利用者端末100でWebアプリケーション「APL\_\_X」が動作していない状況では、コンテキスト「CNT\_\_E」が生成される。そして、コンテキスト「CNT\_\_E」では、Webアプリケーション「APL\_\_Z」においてGPS機能に係るAPIについての判定結果が「利用可」となり、復号機能に係るAPIについての判定結果が「利用不可」となる。

40

【0023】

つまり、利用者端末100は、勤務時間帯内に、Webアプリケーション「APL\_\_X」を動作させていなければ、Webアプリケーション「APL\_\_Z」においてGPSの機能は動作するが、復号の機能は動作しない。この場合には、例えば所在位置に関連する一般文書を閲覧することは許可されるが、所在位置に関連する秘密文書を閲覧することは拒否される。

【0024】

現在時刻が、勤務時間帯外である状況では、コンテキスト「CNT\_\_F」が生成される。そして、コンテキスト「CNT\_\_F」では、Webアプリケーション「APL\_\_Z」に

50

においてGPS機能に係るAPIについての判定結果が「利用不可」となり、復号機能に係るAPIについての判定結果も「利用不可」となる。

【0025】

つまり、利用者端末100は、勤務時間帯外であれば、Webアプリケーション「APL\_Z」においてGPSの機能も、復号の機能も動作しない。この場合には、例えば所在位置に関連する一切の文書を閲覧することは許可されない。以上で、機能制限システムの利用態様についての説明を終える。

【0026】

次に、機能制限システムの構成について説明する。図3に、機能制限システムの構成例を示す。インターネットには、Webアプリケーションを提供するサービスを実現するWebアプリケーションサーバ301a乃至cが接続されている。利用者端末100は、Webアプリケーションサーバ301a乃至cと接続する場合には、インターネットを介してWebアプリケーションサーバ301a乃至cの各々にアクセスする。

10

【0027】

また、社内ネットワークは、ルータ303を介してインターネットに接続している。社内ネットワークには、社内サーバ305が設けられている。利用者端末100は、社内サーバ305と接続する場合には、インターネットと社内ネットワークとを介して社内サーバ305にアクセスする。但し、利用者端末100は、直接社内ネットワークを介して社内サーバ305にアクセスするようにしてもよい。

【0028】

20

社内サーバ305は、利用者端末100に対して社内サービスを提供する。また、社内サーバ305は、利用者端末100における動作に用いられるデータを配信するようにしてもよい。以上で、機能制限システムの構成についての説明を終える。

【0029】

次に、利用者端末100のモジュール構成について説明する。図4に、利用者端末100のモジュール構成例を示す。利用者端末100は、オペレーティングシステム(OS)401、Webブラウザ405、制限部407、格納部409、記憶部411、送信部413、受信部415、表示部417及び受付部419を有している。

【0030】

オペレーティングシステム401は、API群を備えるフレームワーク403を有している。この例で、API群には、GPS機能に係るAPI431a、署名機能に係るAPI431b、通信機能に係るAPI431c、復号機能に係るAPI431d、アドレス帳機能に係るAPI431e及び時計機能に係るAPI431fが含まれている。但し、他の機能に係るAPIを設けるようにしてもよい。

30

【0031】

Webブラウザ405は、スクリプトエンジン451を含んでいる。スクリプトエンジン451は、スクリプトを実行する。Webブラウザ405には、プラグイン453を追加される場合がある。本実施の形態における一部のモジュールを、プラグイン453により実現するようにしてもよい。

【0032】

40

制限部407は、WebアプリケーションによるAPIの利用を制限する。格納部409は、制限部407の処理に用いられるデータを予め格納する。記憶部411は、制限部407の処理により生じるデータを記憶する。送信部413は、データをインターネットに向けて送信する。受信部415は、インターネットからデータを受信する。表示部417は、例えば操作に係る画面を表示する。受付部419は、例えば利用者の操作によるデータ入力を受け付ける。

【0033】

更に、図5を用いて、格納部409と制限部407と記憶部411との詳細について説明する。格納部409は、この例では生成ルールテーブル、判定ルールテーブル及び検証データを格納する。

50

## 【 0 0 3 4 】

生成ルールは、コンテキストを生成するためのルールである。図 6 に、生成ルールテーブルの例を示す。図 6 のレコードは、コンテキストを生成するルールに相当する。レコードには、コンテキスト、時刻条件、位置条件、ネットワーク条件及び W e b アプリケーション条件のフィールドが設けられている。

## 【 0 0 3 5 】

第 1 レコードには、時刻条件、位置条件及び W e b アプリケーション条件は設定されておらず、ネットワーク条件としては、利用者端末 1 0 0 が社内ネットワークに接続していることが定められている。従って、第 1 レコードによれば、現在時刻、利用者端末 1 0 0 の位置及び利用者端末 1 0 0 で動作している W e b アプリケーションの如何に関わらず、利用者端末 1 0 0 が社内ネットワークに接続していれば、コンテキスト「 C N T \_ A 」が生成される。

10

## 【 0 0 3 6 】

第 1 レコードの条件を、例えば条件式「ネットワーク = 社内ネットワーク」で表してもよい。

## 【 0 0 3 7 】

第 2 レコードには、時刻条件及び W e b アプリケーション条件は設定されておらず、位置条件としては、利用者端末 1 0 0 の位置が社内に含まれることが定められ、ネットワーク条件としては、利用者端末 1 0 0 が社内ネットワーク以外に接続していることが定められている。従って、第 2 レコードによれば、現在時刻及び利用者端末 1 0 0 で動作している W e b アプリケーションの如何に関わらず、利用者端末 1 0 0 が社内で社内ネットワーク以外に接続していれば、コンテキスト「 C N T \_ B 」が生成される。

20

## 【 0 0 3 8 】

第 2 レコードの条件を、例えば条件式「位置 = 社内    A N D    ネットワーク = N O T 社内ネットワーク」で表してもよい。

## 【 0 0 3 9 】

第 3 レコードには、時刻条件及び W e b アプリケーション条件は設定されておらず、位置条件としては、利用者端末 1 0 0 の位置が社外であることが定められ、ネットワーク条件としては、利用者端末 1 0 0 が社内ネットワーク以外に接続していることが定められている。

30

## 【 0 0 4 0 】

従って、第 3 レコードによれば、現在時刻及び利用者端末 1 0 0 で動作している W e b アプリケーションの如何に関わらず、利用者端末 1 0 0 が社外で社内ネットワーク以外に接続していれば、コンテキスト「 C N T \_ C 」が生成される。

## 【 0 0 4 1 】

第 3 レコードの条件を、例えば条件式「位置 = N O T    社内    A N D    ネットワーク = N O T    社内ネットワーク」で表してもよい。

## 【 0 0 4 2 】

第 4 レコードには、位置条件及びネットワーク条件は設定されておらず、時刻条件としては、現在時刻が業務時間帯内であることが定められ、 W e b アプリケーション条件としては、利用者端末 1 0 0 が「 x x x . j p / x x 」の U R L で特定される W e b アプリケーション（「 A P L \_ X 」という。）を動作させていることが定められている。従って、第 4 レコードによれば、利用者端末 1 0 0 の位置及び利用者端末 1 0 0 が接続しているネットワークの如何に関わらず、業務時間中に W e b アプリケーション「 A P L \_ X 」を動作させていれば、コンテキスト「 C N T \_ D 」が生成される。

40

## 【 0 0 4 3 】

第 4 レコードの条件を、例えば条件式「現在時刻 > 始業時刻    A N D    現在時刻 < 終業時刻    A N D    W e b アプリケーション = x x x . j p / x x 」で表してもよい。

## 【 0 0 4 4 】

第 5 レコードには、位置条件及びネットワーク条件は設定されておらず、時刻条件とし

50

ては、現在時刻が業務時間帯内であることが定められ、Webアプリケーション条件としては、利用者端末100が「xxx.jp/xx」のURLで特定されるWebアプリケーション(「APL\_X」という。)を動作させていないことが定められている。従って、第5レコードによれば、利用者端末100の位置及び利用者端末100が接続しているネットワークの如何に関わらず、業務時間中にWebアプリケーション「APL\_X」を動作させていなければ、コンテキスト「CNT\_E」が生成される。

【0045】

第5レコードの条件を、例えば条件式「現在時刻>始業時刻 AND 現在時刻<終業時刻 AND Webアプリケーション=NOT xxx.jp/xx」で表してもよい。

10

【0046】

第6レコードには、位置条件、ネットワーク条件及びWebアプリケーション条件は設定されておらず、時刻条件としては、現在時刻が業務時間帯外であることが定められている。従って、第6レコードによれば、利用者端末100の位置、利用者端末100が接続しているネットワーク及び利用者端末100で動作しているWebアプリケーションの如何に関わらず、業務時間外であれば、コンテキスト「CNT\_F」が生成される。

【0047】

第6レコードの条件を、例えば条件式「現在時刻<始業時刻 OR 現在時刻>終業時刻」で表してもよい。図6の例では、生成ルールをレコード形式で表したが、上述のように条件式形式で表してもよい。

20

【0048】

図5の説明に戻って、格納部409に格納されている判定ルールは、APIの利用可否の判定に用いられるルールである。

【0049】

図7に、判定ルールテーブルの例を示す。図7におけるレコードは、判定ルールに相当する。レコードには、コンテキスト、Webアプリケーション、アドレス帳機能に係るAPI、署名機能に係るAPI、GPS機能に係るAPI及び復号機能に係るAPIのフィールドが設けられている。

【0050】

Webアプリケーションのフィールドは、当該判定ルールを適用するWebアプリケーションを限定する場合に用いられる。具体的には、当該判定ルールを適用するWebアプリケーションを提供するサービスのURLが設定される。従って、このURLは、Webアプリケーションを特定する情報であるとともに、Webアプリケーションを提供するサービスを特定する情報でもある。

30

【0051】

アドレス帳機能に係るAPI、署名機能に係るAPI、GPS機能に係るAPI及び復号機能に係るAPIには、各APIの利用の可否が設定される。

【0052】

第1レコードは、コンテキスト「CNT\_A」に基づき、すべてのWebアプリケーションに対して、アドレス帳機能に係るAPIが、「利用可」であることを示している。同様に、署名機能に係るAPIは、「利用可」であるが、GPS機能に係るAPIは、「利用不可」であり、復号機能に係るAPIも、「利用不可」であることを示している。

40

【0053】

従って、第1レコードによれば、例えば任意のWebアプリケーションが、アドレス帳機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_A」に基づいて許可される。同様に、任意のWebアプリケーションが、署名機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_A」に基づいて許可され、一方、GPS機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_A」に基づいて拒否され、復号機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_A」に基づいて拒否される。

50

## 【 0 0 5 4 】

第2レコードは、コンテキスト「CNT\_\_B」に基づき、すべてのWebアプリケーションに対して、アドレス帳機能に係るAPIが、「利用可」であることを示している。同様に、署名機能に係るAPIは、「利用不可」であり、GPS機能に係るAPIも、「利用不可」であり、復号機能に係るAPIも、「利用不可」であることを示している。

## 【 0 0 5 5 】

従って、第2レコードによれば、例えば任意のWebアプリケーションが、アドレス帳機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_\_B」に基づいて許可される。同様に、任意のWebアプリケーションが、署名機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_\_B」に基づいて拒否され、GPS機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_\_B」に基づいて拒否され、復号機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_\_B」に基づいて拒否される。

10

## 【 0 0 5 6 】

第3レコードは、コンテキスト「CNT\_\_C」に基づき、すべてのWebアプリケーションに対して、アドレス帳機能に係るAPIが、「利用不可」であることを示している。同様に、署名機能に係るAPIも、「利用不可」であり、GPS機能に係るAPIも、「利用不可」であり、復号機能に係るAPIも、「利用不可」であることを示している。

## 【 0 0 5 7 】

従って、第3レコードによれば、例えば任意のWebアプリケーションが、アドレス帳機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_\_C」に基づいて拒否される。同様に、任意のWebアプリケーションが、署名機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_\_C」に基づいて拒否され、GPS機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_\_C」に基づいて拒否され、復号機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_\_C」に基づいて拒否される。

20

## 【 0 0 5 8 】

第4レコードは、コンテキスト「CNT\_\_D」に基づき、利用者端末100が「zzz.jp/zzz」のURLで特定されるWebアプリケーション(「APL\_\_Z」という。)に対して、アドレス帳機能に係るAPIが、「利用不可」であることを示している。同様に、署名機能に係るAPIも、「利用不可」であるが、GPS機能に係るAPIは、「利用可」であり、復号機能に係るAPIも、「利用可」であることを示している。

30

## 【 0 0 5 9 】

従って、第4レコードによれば、例えばWebアプリケーション「APL\_\_Z」が、アドレス帳機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_\_D」に基づいて拒否される。同様に、Webアプリケーション「APL\_\_Z」が、署名機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_\_D」に基づいて拒否されるが、GPS機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_\_D」に基づいて許可され、復号機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_\_D」に基づいて許可される。

40

## 【 0 0 6 0 】

第5レコードは、コンテキスト「CNT\_\_E」に基づき、利用者端末100が「zzz.jp/zzz」のURLで特定されるWebアプリケーションに対して、アドレス帳機能に係るAPIが、「利用不可」であることを示している。同様に、署名機能に係るAPIも、「利用不可」であるが、GPS機能に係るAPIは、「利用可」である。また復号機能に係るAPIは、「利用不可」であることを示している。

## 【 0 0 6 1 】

従って、第5レコードによれば、例えばWebアプリケーション「APL\_\_Z」が、アドレス帳機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_\_E」に基づいて拒否される。同様に、Webアプリケーション「APL\_\_Z」が、署名機能に係

50



るAPIを呼び出そうとした場合には、コンテキスト「CNT\_E」に基づいて拒否され、GPS機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_E」に基づいて許可される。また、復号機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_E」に基づいて拒否される。

【0062】

第6レコードは、コンテキスト「CNT\_F」に基づき、利用者端末100が「zzz.jp/zzz」のURLで特定されるWebアプリケーションに対して、アドレス帳機能に係るAPIが、「利用不可」であることを示している。同様に、署名機能に係るAPIも、「利用不可」であり、GPS機能に係るAPIも、「利用不可」であり、復号機能に係るAPIも、「利用不可」であることを示している。

10

【0063】

従って、第6レコードによれば、例えばWebアプリケーション「APL\_Z」が、アドレス帳機能に係るAPIを呼び出そうとした場合には、コンテキスト「CNT\_F」に基づいて拒否される。同様に、Webアプリケーション「APL\_Z」が、署名機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_F」に基づいて拒否され、GPS機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_F」に基づいて拒否され、復号機能に係るAPIを呼び出そうとした場合にも、コンテキスト「CNT\_F」に基づいて拒否される。

【0064】

図5の説明に戻って、格納部409に格納されている検証データは、Webアプリケーションを提供するWebアプリケーションサーバ301を検証する際に用いられるデータである。検証データは、例えば、ルート証明書である。

20

【0065】

制限部407は、生成ルール設定部501、判定ルール設定部503、検証データ登録部505、抽出部507、検証部509、Webアプリケーション登録部511、検出部513、コンテキスト生成部515及び判定部517を有している。

【0066】

生成ルール設定部501は、上述した生成ルールテーブルを格納部409に格納させる。生成ルール設定部501は、例えば、表示部417に生成ルールの入力画面を表示させ、生成ルール入力画面に対する入力の操作を受付部419で受け付けることによって、利用者に生成ルールを設定させる。あるいは、生成ルール設定部501は、インターネットを介して、生成ルールテーブルを配信する装置（例えば、社内サーバ305）から生成ルールテーブルをダウンロードするようにしてもよい。利用者は、例えば準備段階で生成ルール設定部501を起動し、生成ルールテーブルを用意する。

30

【0067】

判定ルール設定部503は、上述した判定ルールテーブルを格納部409に格納させる。判定ルール設定部503は、例えば、表示部417に判定ルールの入力画面を表示させ、判定ルール入力画面に対する入力の操作を受付部419で受け付けることによって、利用者に判定ルールを設定させる。あるいは、判定ルール設定部503は、インターネットを介して、判定ルールテーブルを配信する装置（例えば、社内サーバ305）から判定ルールテーブルをダウンロードするようにしてもよい。利用者は、例えば準備段階で判定ルール設定部503を起動し、判定ルールテーブルを用意する。

40

【0068】

検証データ登録部505は、検証データを所定の機関（例えば認証局）から取得し、格納部409に格納させる。利用者は、例えば準備段階で検証データ登録部505を起動し、検証データを用意する。

【0069】

抽出部507は、通信状況を監視し、通信に係る情報（接続先ネットワークのURLやWebアプリケーションを提供するサービスのURLなど）を抽出する。また、抽出部507は、接続先のネットワークのURLを記憶部411に記憶させる。

50

## 【 0 0 7 0 】

本実施の形態では、抽出部（プロキシ型）507aの例について説明する。抽出部（プロキシ型）507aは、Webブラウザ405とWebアプリケーションサーバ301との間の通信を中継する。そのため、Webブラウザ405は、抽出部（プロキシ型）507aをプロキシに設定しておく。尚、実施の形態2では、抽出部（API監視型）507bの例について説明する。

## 【 0 0 7 1 】

検証部509は、Webアプリケーションサーバ301からダウンロードされるWebアプリケーションを検証する。例えば、WebアプリケーションがHTML（HyperText Markup Language）5ファイル形式である場合、検証部509は、ダウンロードされるHTML5ファイルに相当するHTTP（HyperText Transfer Protocol）レスポンスの署名を検証する。検証部509は、Webアプリケーションサーバ301を認証するようにしてもよい。Webアプリケーション登録部511は、Webアプリケーションサーバ301のURLを記憶部411に記憶させる。検出部513は、APIの呼び出しの発生を検出する。本実施の形態に係る検出部（エンジン監視型）513aは、Webブラウザ405におけるスクリプトエンジン451への働きかけを監視し、APIの呼び出しを要する特定のスクリプトを検出することによって、APIの呼び出しの発生を検出する。尚、実施の形態2では、検出部（API監視型）513bの例について説明する。

10

## 【 0 0 7 2 】

コンテキスト生成部515は、コンテキストを生成する。判定部517は、コンテキストに基づき、APIの利用可否の判定を行う。

20

## 【 0 0 7 3 】

記憶部411は、例えば、ネットワークアドレスとWebアプリケーションリストとを記憶する。ネットワークアドレスは、接続先ネットワークのURLである。Webアプリケーションリストは、利用者端末100で動作しているWebアプリケーションを提供したサービスのURLのリストである。動作を終えたWebアプリケーションについても、当該URLが残されるようにしてもよい。以上で、機能制限システムのモジュール構成についての説明を終える。

## 【 0 0 7 4 】

続いて、図8乃至11に基づいて、シーケンスについて説明する。まず、図8のシーケンスの例について説明する。このシーケンスは、Webブラウザ405からWebアプリケーションサーバ301にアクセスすることを想定している。Webブラウザ405から送出されるHTTPリクエストは、Webブラウザ405におけるプロキシの設定に従って、抽出部（プロキシ型）507aに送られる（S801）。このHTTPリクエストは、Webアプリケーションサーバ301のURLへのアクセス要求に相当する。そして、抽出部（プロキシ型）507aは、HTTPリクエストをWebアプリケーションサーバ301に転送する（S803）。

30

## 【 0 0 7 5 】

HTTPリクエストに対するHTTPレスポンスは、Webアプリケーションサーバ301から抽出部（プロキシ型）507aへ返される（S805）。HTTPレスポンスは、例えばHTML5ファイルに相当する。

40

## 【 0 0 7 6 】

監視していたHTTPリクエストとHTTPレスポンスとに基づいて、抽出部（プロキシ型）507aは、ネットワークアドレスを抽出する処理を行う（S807）。具体的には、抽出部（プロキシ型）507aは、接続先ネットワークのURLを特定する。このとき、接続先ネットワークのURLは、Webアプリケーションサーバ301のURLと一致する。抽出した接続先ネットワークのURLは、前述の通り記憶部411に記憶される。この例では、Webアプリケーションサーバ301へのアクセスの例を示したが、他の装置にアクセスする場合にも、抽出部（プロキシ型）507aは、ネットワークアドレスを抽出するようにしてもよい。

50

## 【 0 0 7 7 】

抽出部（プロキシ型）507aは、検証部509に、Webアプリケーションサーバ301のURLとHTTPレスポンスとを渡す（S809）。URLとHTTPレスポンスを受けると、検証部509は検証処理を行う（S811）。具体的には、検証部509は、HTTPレスポンスに付されている署名データを検証する。署名データの検証に成功した場合には、Webアプリケーションは真正であると判断される。署名データの検証に失敗した場合には、Webアプリケーションは不正であると判断される。

## 【 0 0 7 8 】

また、検証部509は、SSL（Secure Socket Layer）通信の開始時にWebアプリケーションサーバ301を認証するようにしてもよい。Webアプリケーションサーバ301の認証に成功した場合には、Webアプリケーションサーバ301は真正であり、Webアプリケーションサーバ301の認証に失敗した場合には、Webアプリケーションサーバ301は不正であると判断される。

10

## 【 0 0 7 9 】

検証部509は、抽出部（プロキシ型）507aへ検証結果を返す（S813）。検証結果が失敗である場合には、抽出部（プロキシ型）507aは処理を中断する。

## 【 0 0 8 0 】

検証結果が成功である場合には、抽出部（プロキシ型）507aは、Webアプリケーション登録部511にWebアプリケーションサーバ301のURLを渡す（S815）。Webアプリケーションサーバ301のURLを受けると、Webアプリケーション登録部511は、Webアプリケーション登録処理を行う（S817）。具体的には、Webアプリケーション登録部511は、Webアプリケーションサーバ301のURLを記憶部411に記憶されているWebアプリケーションリストに加える。

20

## 【 0 0 8 1 】

そして、抽出部（プロキシ型）507aは、Webブラウザ405へHTTPレスポンスを渡す（S819）。

## 【 0 0 8 2 】

図9に、続きのシーケンスの例を示す。HTTPレスポンスを受けると、Webブラウザ405は、HTML5のデータに対する構文解析や表示等の処理を行う。このとき、Webブラウザ405は、HTML5のデータ中のスクリプトを検出部（エンジン監視型）513aに渡す（S901）。

30

## 【 0 0 8 3 】

スクリプトが前述のAPI群のうちのいずれかのAPIの機能に関する記述を含む場合には、検出部（エンジン監視型）513aは、判定部517に当該APIについての利用可否の判定を求める。そのため、検出部（エンジン監視型）513aは、判定部517に判定リクエスト（API種別を含む。）を渡す（S903）。

## 【 0 0 8 4 】

判定リクエストを受けると、判定部517は、コンテキスト生成部515にコンテキストを生成するリクエストを渡す（S905）。

## 【 0 0 8 5 】

40

コンテキストを生成するリクエストを受けると、コンテキスト生成部515は、コンテキスト生成処理を行う（S907）。コンテキスト生成部515は、ネットワークアドレスの情報をを用いる場合に、記憶部411からネットワークアドレスを読み出す。また、コンテキスト生成部515は、動作しているWebアプリケーションの情報をを用いる場合に、記憶部411からWebアプリケーションリストを読み出す。更に、コンテキスト生成部515は、APIから取得する情報（例えば、位置情報や時間情報）を用いる場合に、API431を呼び出し（S909）、API431から戻り値（以下、API戻り値という。）を得る（S913）。そして、コンテキスト生成部515は、収集した情報と生成ルールとに基づいてコンテキストを生成する。

## 【 0 0 8 6 】

50

生成されたコンテキストは、コンテキスト生成部 5 1 5 から判定部 5 1 7 に返される ( S 9 1 5 )。

【 0 0 8 7 】

コンテキストを受けると、判定部 5 1 7 は、利用可否判定処理を行う ( S 9 1 7 )。具体的には、判定部 5 1 7 は、コンテキストと判定ルールとに基づいて、当該 A P I の利用可否を判定する。そして、判定部 5 1 7 は、検出部 ( エンジン監視型 ) 5 1 3 a に判定結果を返す ( S 9 1 9 )。

【 0 0 8 8 】

図 1 0 に、判定結果が成功である場合のシーケンスの例を示す。検出部 ( エンジン監視型 ) 5 1 3 a が成功の判定結果 ( S 1 0 0 1 ) を受けた場合には、検出部 ( エンジン監視型 ) 5 1 3 a は、スクリプトをスクリプトエンジン 4 5 1 に渡す ( S 1 0 0 3 )。スクリプトエンジン 4 5 1 は W e b ブラウザ 4 0 5 に含まれるが、便宜的に W e b ブラウザ 4 0 5 と分けて説明している。

【 0 0 8 9 】

スクリプトエンジン 4 5 1 は、当該機能に係る A P I 4 3 1 を呼び出す ( S 1 0 0 5 )。そして、A P I 4 3 1 は、スクリプトエンジン 4 5 1 に A P I 戻り値を返す ( S 1 0 0 7 )。スクリプトエンジン 4 5 1 は、検出部 ( エンジン監視型 ) 5 1 3 a に処理を戻す ( S 1 0 0 9 )。更に、検出部 ( エンジン監視型 ) 5 1 3 a は、W e b ブラウザ 4 0 5 に処理を戻す ( S 1 0 1 1 )。それぞれの処理の復帰において、A P I 戻り値が返されるようにしてもよい。

【 0 0 9 0 】

図 1 1 に、判定結果が失敗である場合のシーケンスの例を示す。検出部 ( エンジン監視型 ) 5 1 3 a が失敗の判定結果 ( S 1 1 0 1 ) を受けた場合には、検出部 ( エンジン監視型 ) 5 1 3 a は、W e b ブラウザ 4 0 5 に A P I 利用不可の通知を渡す ( S 1 1 0 3 )。以上でシーケンスについての説明を終える。

【 0 0 9 1 】

続いて、処理の詳細について説明する。まず、検出部 ( エンジン監視型 ) 5 1 3 a の処理について説明する。図 1 2 に、検出処理 ( エンジン監視型 ) フローの例を示す。検出部 ( エンジン監視型 ) 5 1 3 a は、W e b ブラウザ 4 0 5 からスクリプトを受ける ( S 1 2 0 1 )。この処理は、図 9 の S 9 0 1 に示したステップに相当する。

【 0 0 9 2 】

検出部 ( エンジン監視型 ) 5 1 3 a は、受け取ったスクリプトに前述の A P I 群のうちのいずれかの A P I の機能に関する記述が含まれているか否かを判定する ( S 1 2 0 3 )。スクリプトに前述の A P I 群のいずれの A P I の機能に関する記述も含まれていないと判定した場合には、検出部 ( エンジン監視型 ) 5 1 3 a は、スクリプトをスクリプトエンジン 4 5 1 に渡す ( S 1 2 0 5 )。検出部 ( エンジン監視型 ) 5 1 3 a は、スクリプトエンジン 4 5 1 におけるスクリプト処理の終了を待つ ( S 1 2 0 7 )。検出部 ( エンジン監視型 ) 5 1 3 a は、W e b ブラウザ 4 0 5 へ処理を戻す ( S 1 2 0 9 )。

【 0 0 9 3 】

受け取ったスクリプトに前述の A P I 群のうちのいずれかの A P I の機能に関する記述が含まれていると判定した場合には、検出部 ( エンジン監視型 ) 5 1 3 a は、判定部 5 1 7 に判定リクエストを渡す ( S 1 2 1 1 )。このとき、判定リクエストに当該 A P I の種別を含める。この処理は、図 9 の S 9 0 3 に示したステップに相当する。

【 0 0 9 4 】

検出部 ( エンジン監視型 ) 5 1 3 a は、判定部 5 1 7 から判定結果を受ける ( S 1 2 1 3 )。図 9 の S 9 1 9 に示したステップに相当する。

【 0 0 9 5 】

そして、検出部 ( エンジン監視型 ) 5 1 3 a は、判定結果が成功であるか、あるいは失敗であるかを判定する ( S 1 2 1 5 )。判定結果が成功であると判定した場合には、検出部 ( エンジン監視型 ) 5 1 3 a は、スクリプトエンジン 4 5 1 へスクリプトを渡す ( S 1

10

20

30

40

50

217)。この処理は、図10のS1003に示したステップに相当する。

【0096】

そして、検出部（エンジン監視型）513aは、スクリプトエンジン451におけるスクリプト処理の終了を待つ（S1219）。図10のS1009に示したステップに相当する。

【0097】

スクリプトエンジン451におけるスクリプト処理が終了すると、検出部（エンジン監視型）513aは、Webブラウザ405へ処理を戻す（S1221）。検出部（エンジン監視型）513aは、API戻り値を返すようにしてもよい。図10のS1011に示したステップに相当する。

10

【0098】

S1215において判定結果が失敗であると判定した場合には、検出部（エンジン監視型）513aは、Webブラウザ405へAPI利用不可の通知を渡す（S1223）。図11のS1103に示したステップに相当する。以上で、検出部513の処理についての説明を終える。

【0099】

次に、判定部517の処理について説明する。図13に、判定処理フローの例を示す。判定部517は、判定リクエストを待つ（S1301）。判定リクエストには、判定対象となるAPI種別が含まれている。判定リクエストを受けると、判定部517は、呼び出し元のWebアプリケーションを特定する（S1303）。判定部517は、例えば、抽出部（プロキシ型）507aからWebアプリケーションサーバ301のURLを取得し、当該URLによって呼び出し元のWebアプリケーションを特定する。あるいは、判定部517は、記憶部411に記憶されているWebアプリケーションリストに登録されているWebアプリケーションサーバ301のURLによって判定対象のWebアプリケーションを特定する。WebアプリケーションリストにWebアプリケーションサーバ301のURLが複数含まれている場合には、判定部517は、最も遅く登録されたWebアプリケーションサーバ301のURLによって呼び出し元のWebアプリケーションを特定するようにしてもよい。

20

【0100】

判定部517は、コンテキストを生成するリクエストを渡す（S1305）。この処理は、図9のS905に示したステップに相当する。

30

【0101】

そして、判定部517は、生成されたコンテキストを受ける（S1307）。この処理は、図9のS915に示したステップに相当する。

【0102】

判定部517は、判定ルールテーブルから、生成されたコンテキストに適合し、更に呼び出し元のWebアプリケーションにも適合するレコードを特定する（S1309）。判定部517は、当該レコードにおいて判定対象のAPI種別に対応する利用可否を読む（S1311）。S1309とS1311とは、図9のS917に示した利用可否判定処理に相当する。

40

【0103】

判定部517は、検出部（エンジン監視型）513aに判定結果を返す（S1313）。図9のS919に示したステップに相当する。以上で、判定部517の処理についての説明を終える。

【0104】

次に、コンテキスト生成部515の処理について説明する。図14に、コンテキスト生成処理フローの例を示す。コンテキスト生成部515は、コンテキストを生成するリクエストを待つ（S1401）。コンテキストを生成するリクエストを受けると、コンテキスト生成部515は、格納部409に格納されている生成ルールテーブルのうち、未処理のレコードを1つ特定する（S1403）。コンテキスト生成部515は、例えば順次レコ

50

ードを特定する。

【0105】

コンテキスト生成部515は、未処理の条件のフィールドを1つ特定する。コンテキスト生成部515は、例えば順次条件のフィールドを特定する(S1405)。コンテキスト生成部515は、当該条件のフィールドに条件があるか否かを判定する(S1407)。当該条件のフィールドに条件がないと判定した場合には、当該条件のフィールドについての判定を行わずに、S1413の処理に移る。

【0106】

当該条件のフィールドに条件があると判定した場合には、コンテキスト生成部515は、当該条件の対象データを取得する(S1409)。時刻条件であれば、時計機能に係るAPI431fから現在時刻を取得する。位置条件であれば、API431aから位置情報を取得する。ネットワーク条件であれば、記憶部411からネットワークアドレスを読み取る。Webアプリケーション条件であれば、記憶部411のWebアプリケーションリストから動作している他のWebアプリケーションのURLを読み取る。そして、コンテキスト生成部515は、対象データが条件に合致するか否かを判定する(S1411)。

10

【0107】

対象データが条件に合致すると判定した場合には、コンテキスト生成部515は、未処理の条件フィールドがあるか否かを判定する(S1413)。未処理の条件フィールドがあると判定した場合には、S1405の処理に戻る。未処理の条件フィールドがないと判定した場合には、合致しない条件が無いので、コンテキスト生成部515は、当該レコードのコンテキストを特定する(S1415)。

20

【0108】

一方、S1411で対象データが条件に合致しないと判定した場合には、コンテキストを生成しない。

【0109】

コンテキスト生成部515は、未処理のレコードがあるか否かを判定する(S1417)。未処理のレコードがあると判定した場合には、S1403の処理に戻る。

【0110】

未処理のレコードがないと判定した場合には、コンテキスト生成部515は、S1415で特定したコンテキストを判定部517に返す(S1419)。この処理は、図9のS915に示したステップに相当する。

30

【0111】

そして、S1401に戻り、次の生成リクエストを待つ。以上で、コンテキスト生成部515の処理についての説明を終える。

【0112】

本実施の形態によれば、Webアプリケーションによる特定機能の利用を、自動的に制限できる。例えば、利用者端末100で計測された情報(位置情報や時刻情報など)や秘密に符号処理された情報(暗号化されたデータ、復号されたデータ、署名データなど)が不正使用されることを防ぐことができる。

40

【0113】

また、Webアプリケーション又はWebアプリケーションを提供するサービスに応じて、Webアプリケーションによる特定機能の利用を制限できる。

【0114】

また、ネットワークとの接続状況に応じて、Webアプリケーションによる特定機能の利用を制限できる。

【0115】

また、他のWebアプリケーションの動作状況に応じて、Webアプリケーションによる特定機能の利用を制限できる。

【0116】

50

本実施の形態によれば、スクリプトエンジン 4 5 1 を監視するので、オペレーティングシステム 4 0 1 に依存しない。

【 0 1 1 7 】

[ 実施の形態 2 ]

実施の形態 1 で説明した抽出部 ( プロキシ型 ) 5 0 7 a に代えて、抽出部 ( A P I 監視型 ) 5 0 7 b を用いる例を説明する。また、実施の形態 1 で説明した検出部 ( エンジン監視型 ) 5 1 3 a に代えて、検出部 ( A P I 監視型 ) 5 1 3 b を用いる例についても併せて説明する。

【 0 1 1 8 】

抽出部 ( A P I 監視型 ) 5 0 7 b は、通信機能に係る A P I 4 3 1 c の呼び出しをフックすることによって、通信状況を監視し、通信に係る情報 ( 接続先ネットワークの U R L や W e b アプリケーションを提供するサービスの U R L など ) を抽出する。

【 0 1 1 9 】

また、検出部 ( A P I 監視型 ) 5 1 3 b は、各機能に係る A P I の呼び出しをフックすることによって、A P I 4 3 1 の呼び出しの発生を検出する。

【 0 1 2 0 】

図 1 5 乃至 1 8 に基づいて、実施の形態 2 に係るシーケンスについて説明する。まず、図 1 5 のシーケンスの例について説明する。この例では、ソケットを用いた通信を想定する。この図では、ソケットを用いた通信のシーケンスの一部を示している。例えば、W e b ブラウザ 4 0 5 によるソケットオープン抽出部 ( A P I 監視型 ) 5 0 7 b でフックし ( S 1 5 0 1 )、ソケットオープン通信機能に係る A P I 4 3 1 c に渡す ( S 1 5 0 3 )。データの送信も、抽出部 ( A P I 監視型 ) 5 0 7 b を介する ( S 1 5 0 5 , S 1 5 0 7 )。

【 0 1 2 1 】

そして、通信機能に係る A P I 4 3 1 c から W e b アプリケーションサーバ 3 0 1 へ H T T P リクエストが送出される ( S 1 5 0 9 )。W e b アプリケーションサーバ 3 0 1 から返された H T T P レスポンスは、通信機能に係る A P I 4 3 1 c から抽出部 ( A P I 監視型 ) 5 0 7 b に渡される ( S 1 5 1 1、S 1 5 1 3 )。

【 0 1 2 2 】

H T T P レスポンスに相当するデータを受信すると、抽出部 ( A P I 監視型 ) 5 0 7 b は、ネットワークアドレスを抽出する処理を行う ( S 1 5 1 5 )。具体的には、抽出部 ( A P I 監視型 ) 5 0 7 b は、接続先ネットワークの U R L を特定する。このとき、接続先ネットワークの U R L は、W e b アプリケーションサーバ 3 0 1 の U R L と一致する。抽出した接続先ネットワークの U R L は、前述の通り記憶部 4 1 1 に記憶される。この例では、W e b アプリケーションサーバ 3 0 1 へのアクセスの例を示したが、他の装置にアクセスする場合にも、抽出部 ( A P I 監視型 ) 5 0 7 b は、ネットワークアドレスを抽出するようにしてもよい。

【 0 1 2 3 】

抽出部 ( A P I 監視型 ) 5 0 7 b は、検証部 5 0 9 に、W e b アプリケーションサーバ 3 0 1 の U R L と H T T P レスポンスとを渡す ( S 1 5 1 7 )。U R L と H T T P レスポンスを受けると、検証部 5 0 9 は検証処理を行う ( S 1 5 1 9 )。具体的には、検証部 5 0 9 は、H T T P レスポンスに付されている署名データを検証する。署名データの検証に成功した場合には、W e b アプリケーションは真正であると判断される。署名データの検証に失敗した場合には、W e b アプリケーションは不正であると判断される。

【 0 1 2 4 】

また、検証部 5 0 9 は、S S L 通信の開始時に W e b アプリケーションサーバ 3 0 1 を認証するようにしてもよい。W e b アプリケーションサーバ 3 0 1 の認証に成功した場合には、W e b アプリケーションサーバ 3 0 1 は真正であり、W e b アプリケーションサーバ 3 0 1 の認証に失敗した場合には、W e b アプリケーションサーバ 3 0 1 は不正であると判断される。

10

20

30

40

50

## 【 0 1 2 5 】

検証部 5 0 9 は、抽出部 ( A P I 監視型 ) 5 0 7 b へ検証結果を返す ( S 1 5 2 1 ) 。検証結果が失敗である場合には、抽出部 ( A P I 監視型 ) 5 0 7 b は処理を中断する。

## 【 0 1 2 6 】

検証結果が成功である場合には、抽出部 ( A P I 監視型 ) 5 0 7 b は、Web アプリケーション登録部 5 1 1 に Web アプリケーションサーバ 3 0 1 の URL を渡す ( S 1 5 2 3 ) 。 Web アプリケーションサーバ 3 0 1 の URL を受けると、Web アプリケーション登録部 5 1 1 は、Web アプリケーション登録処理を行う ( S 1 5 2 5 ) 。具体的には、Web アプリケーション登録部 5 1 1 は、Web アプリケーションサーバ 3 0 1 の URL を記憶部 4 1 1 に記憶されている Web アプリケーションリストに加える。

10

## 【 0 1 2 7 】

そして、抽出部 ( A P I 監視型 ) 5 0 7 b は、Web ブラウザ 4 0 5 へ HTTP レスポンスを渡す ( S 1 5 2 7 ) 。

## 【 0 1 2 8 】

図 1 6 に、続きのシーケンスの例を示す。Web ブラウザ 4 0 5 から A P I が呼び出されると、検出部 ( A P I 監視型 ) 5 1 3 b は当該 A P I 呼び出しをフックする ( S 1 6 0 1 ) 。フックする箇所によって、呼び出される A P I の種別は特定される。

## 【 0 1 2 9 】

A P I 呼び出しをフックすると、検出部 ( A P I 監視型 ) 5 1 3 b は、判定部 5 1 7 に当該 A P I についての利用可否の判定を求める。そのため、検出部 ( A P I 監視型 ) 5 1 3 b は、判定部 5 1 7 に判定リクエスト ( A P I 種別を含む。 ) を渡す ( S 1 6 0 3 ) 。

20

## 【 0 1 3 0 】

判定リクエストを受けると、判定部 5 1 7 は、コンテキスト生成部 5 1 5 にコンテキストを生成するリクエストを渡す ( S 1 6 0 5 ) 。

## 【 0 1 3 1 】

コンテキストを生成するリクエストを受けると、コンテキスト生成部 5 1 5 は、コンテキスト生成処理を行う ( S 1 6 0 7 ) 。コンテキスト生成部 5 1 5 は、ネットワークアドレスの情報をを用いる場合に、記憶部 4 1 1 からネットワークアドレスを読み出す。コンテキスト生成部 5 1 5 は、動作している Web アプリケーションの情報をを用いる場合に、記憶部 4 1 1 から Web アプリケーションリストを読み出す。コンテキスト生成部 5 1 5 は、A P I から取得する情報 ( 例えば、位置情報や時間情報 ) を用いる場合に、A P I 4 3 1 を呼び出し ( S 1 6 0 9 ) 、A P I 戻り値を得る ( S 1 6 1 3 ) 。そして、コンテキスト生成部 5 1 5 は、収集した情報と生成ルールとに基づいてコンテキストを生成する。

30

## 【 0 1 3 2 】

生成されたコンテキストは、コンテキスト生成部 5 1 5 から判定部 5 1 7 に返される ( S 1 6 1 5 ) 。

## 【 0 1 3 3 】

コンテキストを受けると、判定部 5 1 7 は、利用可否判定処理を行う ( S 1 6 1 7 ) 。具体的には、判定部 5 1 7 は、コンテキストと判定ルールに基づいて、当該 A P I の利用可否を判定する。そして、判定部 5 1 7 は、検出部 ( A P I 監視型 ) 5 1 3 b に判定結果を返す ( S 1 6 1 9 ) 。

40

## 【 0 1 3 4 】

図 1 7 に、判定結果が成功である場合のシーケンスの例を示す。検出部 ( A P I 監視型 ) 5 1 3 b が成功の判定結果 ( S 1 7 0 1 ) を受けた場合には、検出部 ( A P I 監視型 ) 5 1 3 b は、A P I 4 3 1 を呼び出す ( S 1 7 0 3 ) 。検出部 ( A P I 監視型 ) 5 1 3 b は、A P I 4 3 1 から戻り値を受けると ( S 1 7 0 5 ) 、Web ブラウザ 4 0 5 にその戻り値を渡す ( S 1 7 0 7 ) 。

## 【 0 1 3 5 】

図 1 8 に、判定結果が失敗である場合のシーケンスの例を示す。検出部 ( A P I 監視型 ) 5 1 3 b が失敗の判定結果 ( S 1 8 0 1 ) を受けた場合には、検出部 ( A P I 監視型 )

50



5 1 3 bは、Webブラウザ4 0 5にAPI利用不可の通知を渡す(S 1 8 0 3)。以上でシーケンスについての説明を終える。

【0 1 3 6】

続いて、処理の詳細について説明する。まず、検出部(API監視型)5 1 3 bの処理について説明する。図1 9に、検出処理(API監視型)フローの例を示す。検出部(API監視型)5 1 3 bは、API呼び出しをフックする(S 1 9 0 1)。図1 6のS 1 6 0 1に示したステップに相当する。このとき、検出部(API監視型)5 1 3 bは、APIの種別も特定する。

【0 1 3 7】

検出部(API監視型)5 1 3 bは、判定部5 1 7に判定リクエストを渡す(S 1 9 0 3)。このとき、判定リクエストに当該APIの種別を含める。図1 6のS 1 6 0 3に示したステップに相当する。

【0 1 3 8】

検出部(API監視型)5 1 3 bは、判定部5 1 7から判定結果を受ける(S 1 9 0 5)。図1 6のS 1 6 1 9に示したステップに相当する。

【0 1 3 9】

そして、検出部(エンジン監視型)5 1 3 aは、判定結果が成功であるか、あるいは失敗であるかを判定する(S 1 9 0 7)。判定結果が成功であると判定した場合には、検出部(API監視型)5 1 3 bは、種別に応じてAPI 4 3 1を呼び出す(S 1 9 0 9)。図1 7のS 1 7 0 3に示したステップに相当する。

【0 1 4 0】

そして、検出部(API監視型)5 1 3 bは、API 4 3 1から戻り値を受ける(S 1 9 1 1)。図1 7のS 1 7 0 5に示したステップに相当する。

【0 1 4 1】

検出部(API監視型)5 1 3 bは、API戻り値をWebブラウザ4 0 5に返す(S 1 9 1 3)。図1 7のS 1 7 0 7に示したステップに相当する。

【0 1 4 2】

S 1 9 0 7において判定結果が失敗であると判定した場合には、検出部(API監視型)5 1 3 bは、API利用不可の通知を渡す(S 1 9 1 5)。図1 8のS 1 8 0 3に示したステップに相当する。以上で、検出部(API監視型)5 1 3 bの処理についての説明を終える。

【0 1 4 3】

抽出部(プロキシ型)5 0 7 aと検出部(API監視型)5 1 3 bとを組み合わせる形態としてもよい。また、抽出部(API監視型)5 0 7 bと検出部(エンジン監視型)5 1 3 aとを組み合わせる形態としてもよい。

【0 1 4 4】

本実施の形態によれば、API呼び出しをフックするので、Webブラウザ4 0 5に依存しない。更に、プロセス単位で通信を監視することができる。

【0 1 4 5】

[実施の形態3]

上述の実施の形態では、Webブラウザを有する利用者端末1 0 0内でAPI 4 3 1の利用を制限する処理を行う例について説明したが、本実施の形態では、Webブラウザを有する利用者端末1 0 0とは別に設けた中継装置2 0 0においてAPIの利用を制限する例について説明する。

【0 1 4 6】

図2 0に、実施の形態3に係る機能制限システムの構成例を示す。中継装置2 0 0は、インターネットに接続する機能を有している。そして、中継装置2 0 0は、Webアプリケーションサーバ3 0 1 a乃至c、利用者端末1 0 0及び社内サーバ3 0 5とインターネットを介して通信する。尚、中継装置2 0 0と利用者端末1 0 0との間は、近距離無線通信や無線LANなどの他の通信媒体によって接続されるようにしてもよい。

10

20

30

40

50

## 【 0 1 4 7 】

中継装置 2 0 0 は、利用者端末 1 0 0 と W e b アプリケーションサーバ 3 0 1 a 乃至 c との間の通信を中継する。また、中継装置 2 0 0 は、利用者端末 1 0 0 に A P I の機能を提供する。そして、利用者端末 1 0 0 に A P I の機能を提供する前に、コンテキストを生成し、A P I の利用可否判定を行い、利用可と判定された A P I の機能を提供するように動作する。

## 【 0 1 4 8 】

図 2 1 に、中継装置 2 0 0 のモジュール構成例を示す。中継装置 2 0 0 は、オペレーティングシステム ( O S ) 2 1 0 1、制限部 2 1 0 7、格納部 2 1 0 9、記憶部 2 1 1 1、送信部 2 1 1 3、受信部 2 1 1 5、表示部 2 1 1 7 及び受付部 2 1 1 9 を有している。

10

## 【 0 1 4 9 】

オペレーティングシステム 2 1 0 1 は、A P I 群を備えるフレームワーク 2 1 0 3 を有している。この例で、A P I 群には、G P S 機能に係る A P I 2 1 3 1 a、署名機能に係る A P I 2 1 3 1 b、通信機能に係る A P I 2 1 3 1 c、復号機能に係る A P I 2 1 3 1 d 及び時計機能に係る A P I 2 1 3 1 f が含まれている。但し、他の機能に係る A P I を設けるようにしてもよい。

## 【 0 1 5 0 】

図 2 2 を用いて、格納部 2 1 0 9 と制限部 2 1 0 7 と記憶部 2 1 1 1 との詳細について説明する。格納部 2 1 0 9 は、この例では生成ルールテーブル、判定ルールテーブル及び検証データを格納する。

20

## 【 0 1 5 1 】

制限部 2 1 0 7 は、生成ルール設定部 2 2 0 1、判定ルール設定部 2 2 0 3、検証データ登録部 2 2 0 5、抽出部 ( プロキシ型 ) 2 2 0 7 a、検証部 2 2 0 9、W e b アプリケーション登録部 2 2 1 1、コンテキスト生成部 2 2 1 5、判定部 2 2 1 7 及び中継部 2 2 1 9 を有している。

## 【 0 1 5 2 】

生成ルール設定部 2 2 0 1 は、上述した生成ルールテーブルを格納部 2 1 0 9 に格納させる。生成ルール設定部 2 2 0 1 は、例えば、表示部 2 1 1 7 に生成ルールの入力画面を表示させ、生成ルール入力画面に対する入力操作を受付部 2 1 1 9 で受け付けることによって、利用者に生成ルールを設定させる。あるいは、生成ルール設定部 2 2 0 1 は、インターネットを介して、生成ルールテーブルを配信する装置 ( 例えば、社内サーバ 3 0 5 ) から生成ルールテーブルをダウンロードするようにしてもよい。利用者は、例えば準備段階で生成ルール設定部 2 2 0 1 を起動し、生成ルールテーブルを用意する。

30

## 【 0 1 5 3 】

判定ルール設定部 2 2 0 3 は、上述した判定ルールを格納部 2 1 0 9 に格納させる。判定ルール設定部 2 2 0 3 は、例えば、表示部 2 1 1 7 に判定ルールの入力画面を表示させ、判定ルール入力画面に対する入力操作を受付部 2 1 1 9 で受け付けることによって、利用者に判定ルールを設定させる。あるいは、判定ルール設定部 2 2 0 3 は、インターネットを介して、判定ルールテーブルを配信する装置 ( 例えば、社内サーバ 3 0 5 ) から判定ルールテーブルをダウンロードするようにしてもよい。利用者は、例えば準備段階で判定ルール設定部 2 2 0 3 を起動し、判定ルールテーブルを用意する。

40

## 【 0 1 5 4 】

検証データ登録部 2 2 0 5 は、検証データを所定の機関 ( 例えば認証局 ) から取得し、格納部 2 1 0 9 に格納させる。利用者は、例えば準備段階で検証データ登録部 2 2 0 5 を起動し、検証データを用意する。

## 【 0 1 5 5 】

抽出部 ( プロキシ型 ) 2 2 0 7 a は、通信状況を監視し、通信に係る情報 ( 接続先ネットワークの U R L や W e b アプリケーションを提供するサービスの U R L など ) を抽出する。また、抽出部 ( プロキシ型 ) 2 2 0 7 a は、接続先のネットワークの U R L を記憶部 2 1 1 1 に記憶させる。

50

## 【 0 1 5 6 】

検証部 2 2 0 9 は、W e b アプリケーションサーバ 3 0 1 からダウンロードされる W e b アプリケーションを検証する。例えば、W e b アプリケーションが H T M L 5 ファイル形式である場合、検証部 2 2 0 9 は、ダウンロードされる H T M L 5 ファイルに相当する H T T P レスポンスの署名を検証する。検証部 2 2 0 9 は、W e b アプリケーションサーバ 3 0 1 を認証するようにしてもよい。W e b アプリケーション登録部 2 2 1 1 は、W e b アプリケーションサーバ 3 0 1 の U R L を記憶部 2 1 1 1 に記憶させる。

## 【 0 1 5 7 】

コンテキスト生成部 2 2 1 5 は、コンテキストを生成する。判定部 2 2 1 7 は、コンテキストに基づき、A P I の利用可否の判定を行う。

10

## 【 0 1 5 8 】

中継部 2 2 1 9 は、利用者端末 1 0 0 からの A P I 利用を中継する。

## 【 0 1 5 9 】

記憶部 2 1 1 1 は、例えば、ネットワークアドレスと W e b アプリケーションリストとを記憶する。ネットワークアドレスは、接続先ネットワークの U R L である。W e b アプリケーションリストは、利用者端末 1 0 0 で動作している W e b アプリケーションを提供したサービスの U R L のリストである。動作を終えた W e b アプリケーションについても、当該 U R L が残されるようにしてもよい。

## 【 0 1 6 0 】

図 2 3 に、実施の形態 3 に係る利用者端末のモジュール構成例を示す。利用者端末 1 0 0 は、検出部（エンジン監視型）2 3 0 1 a を有している。検出部（エンジン監視型）2 3 0 1 a は、スクリプトエンジン 4 5 1 を監視する。

20

## 【 0 1 6 1 】

図 2 4 に、実施の形態 3 に係るシーケンスの例を示す。利用者端末 1 0 0 の W e b ブラウザ 4 0 5 から送出される H T T P リクエストは、利用者端末 1 0 0 の W e b ブラウザ 4 0 5 におけるプロキシの設定に従って、中継装置 2 0 0 の抽出部（プロキシ型）2 2 0 7 a に送られる（S 2 4 0 1）。この H T T P リクエストは、W e b アプリケーションサーバ 3 0 1 の U R L へのアクセス要求に相当する。そして、中継装置 2 0 0 の抽出部（プロキシ型）2 2 0 7 a は、H T T P リクエストを W e b アプリケーションサーバ 3 0 1 に転送する（S 2 4 0 3）。

30

## 【 0 1 6 2 】

H T T P リクエストに対する H T T P レスポンスは、W e b アプリケーションサーバ 3 0 1 から中継装置 2 0 0 の抽出部（プロキシ型）2 2 0 7 a へ返される（S 2 4 0 5）。H T T P レスポンスは、例えば H T M L 5 ファイルに相当する。

## 【 0 1 6 3 】

監視していた H T T P リクエストと H T T P レスポンスとに基づいて、中継装置 2 0 0 の抽出部（プロキシ型）2 2 0 7 a は、ネットワークアドレスを抽出する処理を行う（S 2 4 0 7）。具体的には、中継装置 2 0 0 の抽出部（プロキシ型）2 2 0 7 a は、接続先ネットワークの U R L を特定する。このとき、接続先ネットワークの U R L は、W e b アプリケーションサーバ 3 0 1 の U R L と一致する。抽出した接続先ネットワークの U R L は、前述の通り記憶部 2 1 1 1 に記憶される。この例では、W e b アプリケーションサーバ 3 0 1 へのアクセスの例を示したが、他の装置にアクセスする場合にも、中継装置 2 0 0 の抽出部（プロキシ型）2 2 0 7 a は、ネットワークアドレスを抽出するようにしてもよい。

40

## 【 0 1 6 4 】

中継装置 2 0 0 の抽出部（プロキシ型）2 2 0 7 a は、中継装置 2 0 0 の検証部 2 2 0 9 に、W e b アプリケーションサーバ 3 0 1 の U R L と H T T P レスポンスとを渡す（S 2 4 0 9）。U R L と H T T P レスポンスを受けると、中継装置 2 0 0 の検証部 2 2 0 9 は検証処理を行う（S 2 4 1 1）。具体的には、中継装置 2 0 0 の検証部 2 2 0 9 は、H T T P レスポンスに付されている署名データを検証する。署名データの検証に成功した場

50

合には、Webアプリケーションは真正であると判断される。署名データの検証に失敗した場合には、Webアプリケーションは不正であると判断される。

【0165】

また、中継装置200の検証部2209は、SSL通信の開始時にWebアプリケーションサーバ301を認証するようにしてもよい。Webアプリケーションサーバ301の認証に成功した場合には、Webアプリケーションサーバ301は真正であり、Webアプリケーションサーバ301の認証に失敗した場合には、Webアプリケーションサーバ301は不正であると判断される。

【0166】

中継装置200の検証部2209は、中継装置200の抽出部(プロキシ型)2207aへ検証結果を返す(S2413)。検証結果が失敗である場合には、中継装置200の抽出部(プロキシ型)2207aは処理を中断する。

【0167】

検証結果が成功である場合には、中継装置200の抽出部(プロキシ型)2207aは、中継装置200のWebアプリケーション登録部2211にWebアプリケーションサーバ301のURLを渡す(S2415)。Webアプリケーションサーバ301のURLを受けると、中継装置200のWebアプリケーション登録部2211は、Webアプリケーション登録処理を行う(S2417)。具体的には、中継装置200のWebアプリケーション登録部2211は、Webアプリケーションサーバ301のURLを記憶部2111に記憶されているWebアプリケーションリストに加える。

【0168】

そして、中継装置200の抽出部(プロキシ型)2207aは、利用者端末100のWebブラウザ405へHTTPレスポンスを渡す(S2419)。

【0169】

図25に、続きのシーケンスの例を示す。利用者端末100の検出部(エンジン監視型)2301aは、利用者端末100のWebブラウザ405から受けたスクリプトに前述のAPI群のうちのいずれかのAPIの機能に関する記述が含まれている場合に、中継装置200の中継部2219に当該APIの利用を求める。そのため、利用者端末100の検出部(エンジン監視型)2301aは、インターネットを介して中継装置200の中継部2219にAPI利用リクエストを送る(S2501)。このとき、インターネットに代えて、近距離無線通信や無線LANなどの他の通信媒体が用いられるようにしてもよい。

【0170】

中継装置200の中継部2219は、中継装置200の判定部2217に判定リクエスト(API種別を含む。)を渡す(S2503)。

【0171】

判定リクエストを受けると、中継装置200の判定部2217は、中継装置200のコンテキスト生成部2215にコンテキストを生成するリクエストを渡す(S2505)。

【0172】

コンテキストを生成するリクエストを受けると、中継装置200のコンテキスト生成部2215は、コンテキスト生成処理を行う(S2507)。中継装置200のコンテキスト生成部2215は、ネットワークアドレスの情報をを用いる場合に、記憶部2111からネットワークアドレスを読み出す。また、中継装置200のコンテキスト生成部2215は、動作しているWebアプリケーションの情報をを用いる場合に、記憶部2111からWebアプリケーションリストを読み出す。更に、中継装置200のコンテキスト生成部2215は、APIから取得する情報(例えば、位置情報や時間情報)を用いる場合に、中継装置200のAPI2131を呼び出し(S2509)、中継装置200のAPI2131から戻り値を得る(S2513)。そして、中継装置200のコンテキスト生成部2215は、収集した情報と生成ルールとに基づいてコンテキストを生成する。

【0173】

生成されたコンテキストは、中継装置 200 のコンテキスト生成部 2215 から中継装置 200 の判定部 2217 に返される (S2515)。

【0174】

コンテキストを受けると、中継装置 200 の判定部 2217 は、利用可否判定処理を行う (S2517)。具体的には、中継装置 200 の判定部 2217 は、コンテキストと判定ルールとに基づいて、当該 API の利用可否を判定する。そして、中継装置 200 の判定部 2217 は、中継装置 200 の中継部 2219 に判定結果を返す (S2519)。

【0175】

図 26 に、判定結果が成功である場合のシーケンスの例を示す。中継装置 200 の中継部 2219 が成功の判定結果 (S2601) を受けた場合には、中継装置 200 の中継部 2219 は、中継装置 200 における当該機能に係る API 2131 を呼び出す (S2603)。そして、中継装置 200 の API 2131 は、中継装置 200 の中継部 2219 に API 戻り値を返す (S2605)。そして、中継装置 200 の中継部 2219 は、インターネットを介して利用者端末 100 の検出部 (エンジン監視型) 2301a に API 利用結果を送る (S2607)。API 利用結果は、API 戻り値を含んでいる。利用者端末 100 側は、API 戻り値を用いて処理を続行する。このとき、インターネットに代えて、近距離無線通信や無線 LAN などの他の通信媒体が用いられるようにしてもよい。

【0176】

図 27 に、判定結果が失敗である場合のシーケンスの例を示す。中継装置 200 の中継部 2219 が失敗の判定結果 (S2701) を受けた場合には、中継装置 200 の中継部 2219 は、インターネットを介して利用者端末 100 の検出部 (エンジン監視型) 2301a に API 利用不可の通知を送る (S2703)。このとき、インターネットに代えて、近距離無線通信や無線 LAN などの他の通信媒体が用いられるようにしてもよい。

【0177】

本実施の形態によれば、プログラムを実行する装置とは別の装置の状況に応じて、プログラムによる特定機能の利用を制限できる。

【0178】

[実施の形態 4]

利用者端末 100 で監視する API の呼び出しに基づいて、利用者端末 100 と中継装置 200 とが連携する形態について説明する。

【0179】

図 28 に、実施の形態 4 に係る格納部 2109 と制限部 2107 と記憶部 2111 の構成例を示す。図 22 の抽出部 (プロキシ型) 2207a に代えて、抽出部 (API 監視型) 2207b を有している。

【0180】

図 29 に、実施の形態 4 に係る利用者端末 100 のモジュール構成例を示す。利用者端末 100 は、図 23 に示した検出部 (エンジン監視型) 2301a に代えて、検出部 (API 監視型) 2301b を有している。更に、利用者端末 100 は、転送部 2901 を有している。

【0181】

図 30 に、実施の形態 4 に係るシーケンスの例を示す。この例では、ソケットを用いた通信を想定する。この図では、ソケットを用いた通信のシーケンスの一部を示している。例えば、利用者端末 100 の Web ブラウザ 405 からのソケットオープンをフックした利用者端末 100 の転送部 2901 は、インターネットを介してソケットオープンの中継装置 200 の抽出部 (API 監視型) 2207b に送る (S3001)。中継装置 200 の抽出部 (API 監視型) 2207b は、ソケットオープンの中継装置 200 における通信機能に係る API 2131c に渡す (S3003)。データ送信の場合も、利用者端末 100 の転送部 2901 と中継装置 200 の抽出部 (API 監視型) 2207b とを介して送られる (S3005, S3007)。このとき、インターネットに代えて、近距離無線通信や無線 LAN などの他の通信媒体が用いられるようにしてもよい。

10

20

30

40

50

## 【 0 1 8 2 】

そして、中継装置 2 0 0 における通信機能に係る A P I 2 1 3 1 c から W e b アプリケーションサーバ 3 0 1 へ H T T P リクエストが送出される ( S 3 0 0 9 )。W e b アプリケーションサーバ 3 0 1 から返された H T T P レスポンスは、中継装置 2 0 0 における通信機能に係る A P I 2 1 3 1 c から中継装置 2 0 0 の抽出部 ( A P I 監視型 ) 2 2 0 7 b に渡される ( S 3 0 1 1、S 3 0 1 3 )。

## 【 0 1 8 3 】

H T T P レスポンスに相当するデータを受信すると、中継装置 2 0 0 の抽出部 ( A P I 監視型 ) 2 2 0 7 b は、ネットワークアドレスを抽出する処理を行う ( S 3 0 1 5 )。具体的には、中継装置 2 0 0 の抽出部 ( A P I 監視型 ) 2 2 0 7 b は、接続先ネットワークの U R L を特定する。このとき、接続先ネットワークの U R L は、W e b アプリケーションサーバ 3 0 1 の U R L と一致する。抽出した接続先ネットワークの U R L は、前述の通り記憶部 2 1 1 1 に記憶される。この例では、W e b アプリケーションサーバ 3 0 1 へのアクセスの例を示したが、他の装置にアクセスする場合にも、中継装置 2 0 0 の抽出部 ( A P I 監視型 ) 2 2 0 7 b は、ネットワークアドレスを抽出するようにしてもよい。

## 【 0 1 8 4 】

中継装置 2 0 0 の抽出部 ( A P I 監視型 ) 2 2 0 7 b は、中継装置 2 0 0 の検証部 2 2 0 9 に、W e b アプリケーションサーバ 3 0 1 の U R L と H T T P レスポンスとを渡す ( S 3 0 1 7 )。U R L と H T T P レスポンスとを受けると、中継装置 2 0 0 の検証部 2 2 0 9 は検証処理を行う ( S 3 0 1 9 )。具体的には、中継装置 2 0 0 の検証部 2 2 0 9 は、H T T P レスポンスに付されている署名データを検証する。署名データの検証に成功した場合には、W e b アプリケーションは真正であると判断される。署名データの検証に失敗した場合には、W e b アプリケーションは不正であると判断される。

## 【 0 1 8 5 】

また、中継装置 2 0 0 の検証部 2 2 0 9 は、S S L 通信の開始時に W e b アプリケーションサーバ 3 0 1 を認証するようにしてもよい。W e b アプリケーションサーバ 3 0 1 の認証に成功した場合には、W e b アプリケーションサーバ 3 0 1 は真正であり、W e b アプリケーションサーバ 3 0 1 の認証に失敗した場合には、W e b アプリケーションサーバ 3 0 1 は不正であると判断される。

## 【 0 1 8 6 】

中継装置 2 0 0 の検証部 2 2 0 9 は、中継装置 2 0 0 の抽出部 ( A P I 監視型 ) 2 2 0 7 b へ検証結果を返す ( S 3 0 2 1 )。検証結果が失敗である場合には、中継装置 2 0 0 の抽出部 ( A P I 監視型 ) 2 2 0 7 b は処理を中断する。

## 【 0 1 8 7 】

検証結果が成功である場合には、中継装置 2 0 0 の抽出部 ( A P I 監視型 ) 2 2 0 7 b は、中継装置 2 0 0 の W e b アプリケーション登録部 2 2 1 1 に W e b アプリケーションサーバ 3 0 1 の U R L を渡す ( S 3 0 2 3 )。W e b アプリケーションサーバ 3 0 1 の U R L を受けると、中継装置 2 0 0 の W e b アプリケーション登録部 2 2 1 1 は、W e b アプリケーション登録処理を行う ( S 3 0 2 5 )。具体的には、中継装置 2 0 0 の W e b アプリケーション登録部 2 2 1 1 は、W e b アプリケーションサーバ 3 0 1 の U R L を記憶部 2 1 1 1 に記憶されている W e b アプリケーションリストに加える。

## 【 0 1 8 8 】

そして、中継装置 2 0 0 の抽出部 ( A P I 監視型 ) 2 2 0 7 b は、インターネットを介して利用者端末 1 0 0 の転送部 2 9 0 1 へ H T T P レスポンスに相当するデータを送信する ( S 3 0 2 7 )。このとき、インターネットに代えて、近距離無線通信や無線 L A N などの他の通信媒体が用いられるようにしてもよい。

## 【 0 1 8 9 】

図 3 1 に、続きのシーケンスの例を示す。利用者端末 1 0 0 の W e b ブラウザ 4 0 5 からの A P I 呼び出しをフックした利用者端末 1 0 0 の検出部 ( A P I 監視型 ) 2 3 0 1 b は、インターネットを介して中継装置 2 0 0 の中継部 2 2 1 9 に A P I 利用のリクエスト

10

20

30

40

50

を送る（Ｓ３１０１）。このとき、インターネットに代えて、近距離無線通信や無線ＬＡＮなどの他の通信媒体が用いられるようにしてもよい。

【０１９０】

中継装置２００の中継部２２１９は、中継装置２００の判定部２２１７に当該ＡＰＩについての利用可否の判定を求める。そのため、中継装置２００の中継部２２１９は、中継装置２００の判定部２２１７に判定リクエスト（ＡＰＩ種別を含む。）を渡す（Ｓ３１０３）。

【０１９１】

判定リクエストを受けると、中継装置２００の判定部２２１７は、中継装置２００のコンテキスト生成部２２１５にコンテキストを生成するリクエストを渡す（Ｓ３１０５）。 10

【０１９２】

コンテキストを生成するリクエストを受けると、中継装置２００のコンテキスト生成部２２１５は、コンテキスト生成処理を行う（Ｓ３１０７）。中継装置２００のコンテキスト生成部２２１５は、ネットワークアドレスの情報をを用いる場合に、記憶部２１１１からネットワークアドレスを読み出す。中継装置２００のコンテキスト生成部２２１５は、動作しているＷｅｂアプリケーションの情報をを用いる場合に、記憶部２１１１からＷｅｂアプリケーションリストを読み出す。中継装置２００のコンテキスト生成部２２１５は、ＡＰＩから取得する情報（例えば、位置情報や時間情報）を用いる場合に、中継装置２００のＡＰＩ２１３１を呼び出し（Ｓ３１０９）、ＡＰＩ戻り値を得る（Ｓ３１１３）。そして、中継装置２００のコンテキスト生成部２２１５は、収集した情報と生成ルールとに基づいてコンテキストを生成する。 20

【０１９３】

生成されたコンテキストは、中継装置２００のコンテキスト生成部２２１５から中継装置２００の判定部２２１７に返される（Ｓ３１１５）。

【０１９４】

コンテキストを受けると、中継装置２００の判定部２２１７は、利用可否判定処理を行う（Ｓ３１１７）。具体的には、中継装置２００の判定部２２１７は、コンテキストと判定ルールに基づいて、当該ＡＰＩの利用可否を判定する。そして、中継装置２００の判定部２２１７は、中継装置２００の中継部２２１９に判定結果を返す（Ｓ３１１９）。 30

【０１９５】

図３２に、判定結果が成功である場合のシーケンスの例を示す。中継装置２００の中継部２２１９が成功の判定結果（Ｓ３２０１）を受けた場合には、中継装置２００の中継部２２１９は、中継装置２００のＡＰＩ２１３１を呼び出す（Ｓ３２０３）。中継装置２００の中継部２２１９は、中継装置２００のＡＰＩ２１３１から戻り値を受けると（Ｓ３２０５）、インターネットを介して利用者端末１００の検出部（ＡＰＩ監視型）２３０１ｂにＡＰＩ利用結果を送る（Ｓ３２０７）。ＡＰＩ利用結果には、ＡＰＩ戻り値が含まれる。このとき、インターネットに代えて、近距離無線通信や無線ＬＡＮなどの他の通信媒体が用いられるようにしてもよい。利用者端末１００側は、ＡＰＩ戻り値を用いて処理を続行する。 40

【０１９６】

図３３に、判定結果が失敗である場合のシーケンスの例を示す。中継装置２００の中継部２２１９が失敗の判定結果（Ｓ３３０１）を受けた場合には、中継装置２００の中継部２２１９は、インターネットを介して利用者端末１００の検出部（ＡＰＩ監視型）２３０１ｂにＡＰＩ利用不可の通知を送る（Ｓ３３０３）。このとき、インターネットに代えて、近距離無線通信や無線ＬＡＮなどの他の通信媒体が用いられるようにしてもよい。以上でシーケンスについての説明を終える。

【０１９７】

本実施の形態によれば、プログラムを実行する装置とは別の装置の状況に応じて、プログラムによる特定機能の利用を制限できる。

【０１９８】

以上本技術の一実施の形態を説明したが、本技術はこれに限定されるものではない。例えば、上述の機能ブロック構成は実際のプログラムモジュール構成に一致しない場合もある。

【0199】

また、上で説明した各記憶領域の構成は一例であって、上記のような構成でなければならないわけではない。さらに、処理フローにおいても、処理結果が変わらなければ処理の順番を入れ替えることも可能である。さらに、並列に実行させるようにしても良い。

【0200】

利用者端末100と中継装置200とは、例えば携帯型情報処理装置である。図34に、携帯型情報処理装置のハードウェア構成例を示す。携帯型情報処理装置は、RAM(Random Access Memory)3403、スピーカ3405、LCD(Liquid Crystal Display: 液晶ディスプレイ)3407、タッチパネル3409、マイク3411、NAND(Not AND)メモリ3413、通信CPU(Central Processing Unit)3415、アプリCPU3417、近距離通信デバイス3419、GPSセンサー3421、無線LAN(Local Area Network)デバイス3423、DSP(Digital Signal Processor)3425、ISP(Image Signal Processor)3427、カメラ3429、バス3431、サブプロセッサ3433、地磁気センサー3435、ジャイロセンサー3437及び加速度センサー3439を有している。そのうち、RAM3403、スピーカ3405、LCD3407、タッチパネル3409、マイク3411、NANDメモリ3413、通信CPU3415、アプリCPU3417、近距離通信デバイス3419、GPSセンサー3421、無線LANデバイス3423、DSP3425、ISP3427及びカメラ3429は、バス3431を介して接続されている。LCD3407は、表示装置の例である。

【0201】

RAM3403は、例えばプログラムやデータを記憶する。スピーカ3405は、音声出力する。LCD3407は、画像や画面を表示する。タッチパネル3409は、接触状態と接触位置などを検出する。マイク3411は、音声を入力する。NANDメモリ3413は、不揮発性記憶素子のフラッシュメモリである。このNANDメモリ3413は、例えばプログラムやデータを記憶する。通信CPU3415は、通信処理に係る演算処理を行う。アプリCPU3417は、アプリケーションソフトを実行する演算装置である。近距離通信デバイス3419は、近距離通信を制御するデバイスである。GPSセンサー3421は、位置を測定する装置である。無線LANデバイス3423は、無線LANの通信を制御するデバイスである。DSP3425は、デジタル信号処理を行うプロセッサである。ISP3427は、画像処理を行うプロセッサである。カメラ3429は、撮影する装置である。また、アプリCPU3417は、サブプロセッサ3433と接続している。サブプロセッサ3433は、地磁気センサー3435、ジャイロセンサー3437、及び加速度センサー3439に接続している。サブプロセッサ3433は、地磁気センサー3435、ジャイロセンサー3437、及び加速度センサー3439を制御する。

【0202】

この例では、アプリCPU3417は、サブプロセッサ3433を介して地磁気センサー3435、ジャイロセンサー3437、及び加速度センサー3439の計測結果を取得するが、アプリCPU3417は、直接に地磁気センサー3435、ジャイロセンサー3437、及び加速度センサー3439の計測結果を取得するようにしてもよい。

【0203】

以上述べた本発明の実施の形態をまとめると、以下のようになる。

【0204】

本実施の形態に係る情報処理装置は、プログラムの実行中に、特定機能に係る呼び出しの発生を検出すると、自装置の状況に係るコンテキストを生成する生成部と、コンテキストに基づいて、呼び出しの可否を判定する判定部とを有する。

【0205】

このようにすれば、プログラムによる特定機能の利用を、自動的に制限できる。



## 【 0 2 0 6 】

また、上記判定部は、更に、プログラム又はプログラムを提供するサービスに対応するルールに従って、呼び出しの許否を判定するようにしてもよい。

## 【 0 2 0 7 】

このようにすれば、プログラム又はプログラムを提供するサービスに応じて、プログラムによる特定機能の利用を制限できる。

## 【 0 2 0 8 】

また、上記自装置の状況は、情報処理装置におけるネットワークとの接続状況であってもよい。

## 【 0 2 0 9 】

このようにすれば、ネットワークとの接続状況に応じて、プログラムによる特定機能の利用を制限できる。

## 【 0 2 1 0 】

また、上記自装置の状況は、情報処理装置における他のプログラムの動作状況であってもよい。

## 【 0 2 1 1 】

このようにすれば、他のプログラムの動作状況に応じて、プログラムによる特定機能の利用を制限できる。

## 【 0 2 1 2 】

本実施の形態に係るシステムは、プログラムの実行中に、特定機能に係る呼び出しの発生を検出する検出部を有する第1の情報処理装置と、呼び出しの発生を検出すると、自装置の状況に係るコンテキストを生成する生成部と、コンテキストに基づいて、呼び出しの許否を判定する判定部とを有する第2の情報処理装置とを含む。

## 【 0 2 1 3 】

このようにすれば、プログラムを実行する装置とは別の装置の状況に応じて、プログラムによる特定機能の利用を制限できる。

## 【 0 2 1 4 】

なお、上で述べた処理をコンピュータに行わせるためのプログラムを作成することができ、当該プログラムは、例えばフレキシブルディスク、CD-ROM、光磁気ディスク、半導体メモリ、ハードディスク等のコンピュータ読み取り可能な記憶媒体又は記憶装置に格納されるようにしてもよい。尚、中間的な処理結果は、一般的にメインメモリ等の記憶装置に一時保管される。

## 【 0 2 1 5 】

以上の実施例を含む実施形態に関し、さらに以下の付記を開示する。

## 【 0 2 1 6 】

## (付記1)

プログラムの実行中に、特定機能に係る呼び出しの発生を検出すると、自装置の状況に係るコンテキストを生成する生成部と、

前記コンテキストに基づいて、前記呼び出しの許否を判定する判定部とを有する情報処理装置。

## 【 0 2 1 7 】

## (付記2)

前記判定部は、更に、前記プログラム又は前記プログラムを提供するサービスに対応するルールに従って、前記呼び出しの許否を判定する

付記1記載の情報処理装置。

## 【 0 2 1 8 】

## (付記3)

前記自装置の状況は、前記情報処理装置におけるネットワークとの接続状況である

付記1又は2記載の情報処理装置。

## 【 0 2 1 9 】

(付記 4)

前記自装置の状況は、前記情報処理装置における他のプログラムの動作状況である  
付記 1 乃至 3 のいずれか 1 つ記載の情報処理装置。

【 0 2 2 0 】

(付記 5)

プログラムの実行中に、特定機能に係る呼び出しの発生を検出する検出部  
を有する第 1 の情報処理装置と、

前記呼び出しの発生を検出すると、自装置の状況に係るコンテキストを生成する生成部  
と、

前記コンテキストに基づいて、前記呼び出しの許否を判定する判定部と  
を有する第 2 の情報処理装置と  
を含むシステム。

10

【 0 2 2 1 】

(付記 6)

プログラムの実行中に、特定機能に係る呼び出しの発生を検出すると、自装置の状況に  
係るコンテキストを生成する処理と、

前記コンテキストに基づいて、前記呼び出しの許否を判定する処理と  
を含む情報処理方法。

【 0 2 2 2 】

(付記 7)

プログラムの実行中に、特定機能に係る呼び出しの発生を検出すると、自装置の状況に  
係るコンテキストを生成する処理と、

前記コンテキストに基づいて、前記呼び出しの許否を判定する処理と  
をコンピュータに実行させるためのプログラム。

20

【符号の説明】

【 0 2 2 3 】

1 0 0	利用者端末	2 0 0	中継装置
3 0 1	W e b アプリケーションサーバ	3 0 3	ルータ
3 0 5	社内サーバ	4 0 1	オペレーティングシステム
4 0 3	フレームワーク	4 0 5	W e b ブラウザ
4 0 7	制限部	4 0 9	格納部
4 1 1	記憶部	4 1 3	送信部
4 1 5	受信部	4 1 7	表示部
4 1 9	受付部	4 3 1	A P I
4 3 1 a	G P S 機能に係る A P I	4 3 1 b	署名機能に係る A P I
4 3 1 c	通信機能に係る A P I	4 3 1 d	復号機能に係る A P I
4 3 1 e	アドレス帳機能に係る A P I	4 3 1 f	時計機能に係る A P I
4 5 1	スクリプトエンジン	4 5 3	プラグイン
5 0 1	生成ルール設定部	5 0 3	判定ルール設定部
5 0 5	検証データ登録部	5 0 7	抽出部
5 0 7 a	抽出部 (プロキシ型)	5 0 7 b	抽出部 (A P I 監視型)
5 0 9	検証部	5 1 1	W e b アプリケーション登録部
5 1 3	検出部	5 1 3 a	検出部 (エンジン監視型)
5 1 3 b	検出部 (A P I 監視型)	5 1 5	コンテキスト生成部
5 1 7	判定部	2 1 0 1	オペレーティングシステム
2 1 0 3	フレームワーク	2 1 0 7	制限部
2 1 0 9	格納部	2 1 1 1	記憶部
2 1 1 3	送信部	2 1 1 5	受信部
2 1 1 7	表示部	2 1 1 9	受付部
2 1 3 1	A P I	2 1 3 1 a	G P S 機能に係る A P I

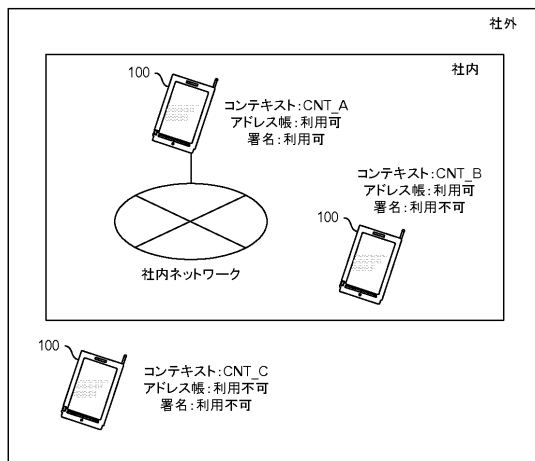
30

40

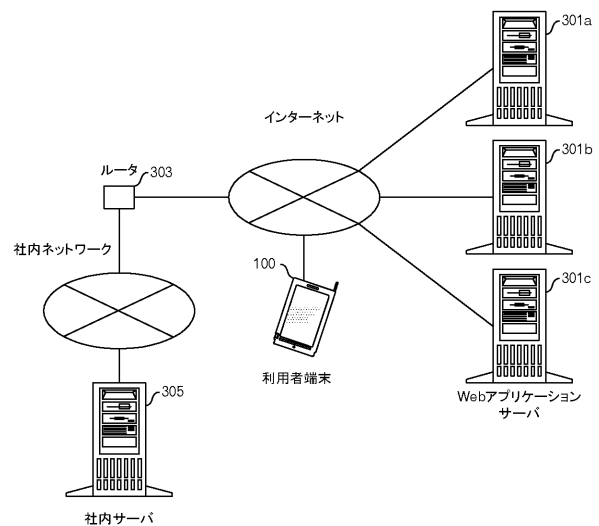
50

2 1 3 1 b	署名機能に係る A P I	2 1 3 1 c	通信機能に係る A P I
2 1 3 1 d	復号機能に係る A P I	2 1 3 1 f	時計機能に係る A P I
2 2 0 1	生成ルール設定部	2 2 0 3	判定ルール設定部
2 2 0 5	検証データ登録部	2 2 0 7	抽出部
2 2 0 7 a	抽出部 (プロキシ型)	2 2 0 7 b	抽出部 (A P I 監視型)
2 2 0 9	検証部	2 2 1 1	Webアプリケーション登録部
2 2 1 5	コンテキスト生成部	2 2 1 7	判定部
2 2 1 9	中継部	2 3 0 1 a	検出部 (エンジン監視型)
2 3 0 1 b	検出部 (A P I 監視型)	2 9 0 1	転送部

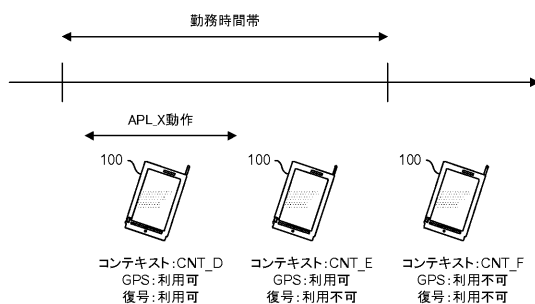
【図 1】



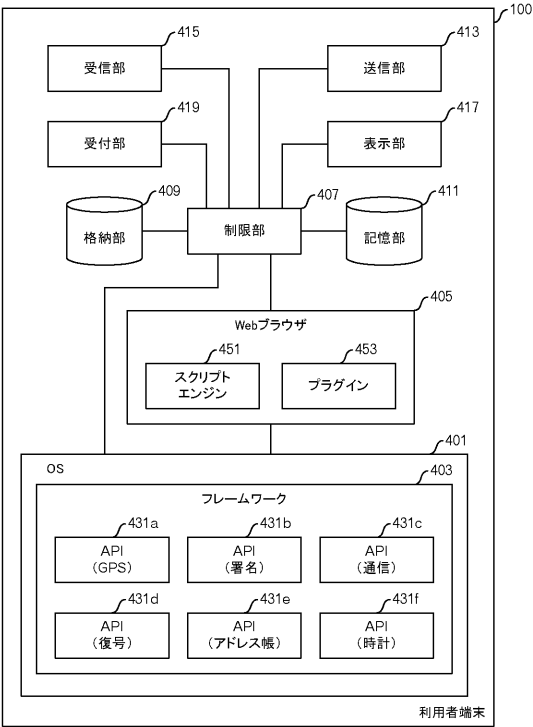
【図 3】



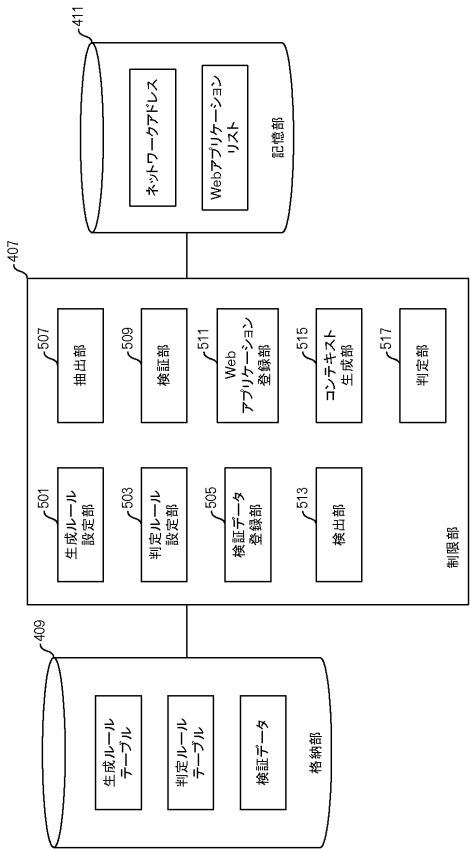
【図 2】



【図 4】



【図 5】



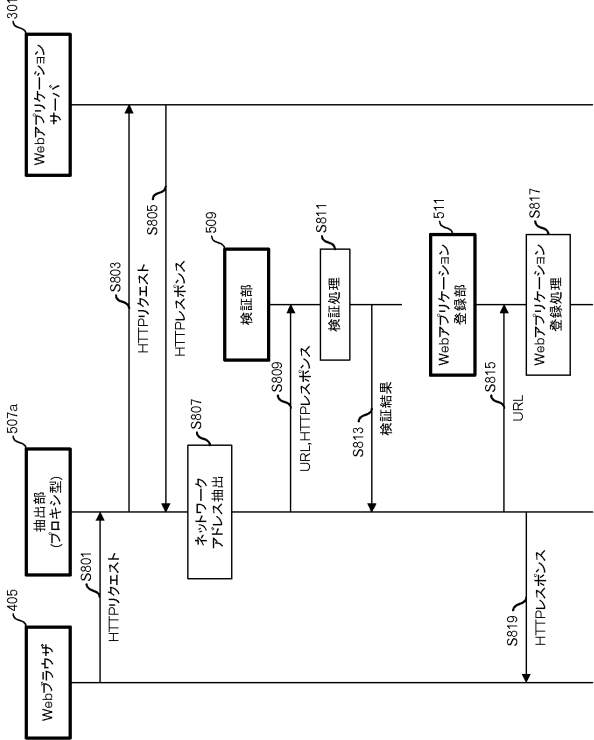
【図 6】

コンテキスト	時刻条件	位置条件	ネットワーク条件	Webアプリケーション条件
CNT_A	なし	なし	社内ネットワーク	なし
CNT_B	なし	社内	社内ネットワーク以外	なし
CNT_C	なし	社外	社内ネットワーク以外	なし
CNT_D	業務時間帯内	なし	なし	xxx.jp/xx 動作
CNT_E	業務時間帯内	なし	なし	xxx.jp/xx 非動作
CNT_F	業務時間帯外	なし	なし	なし

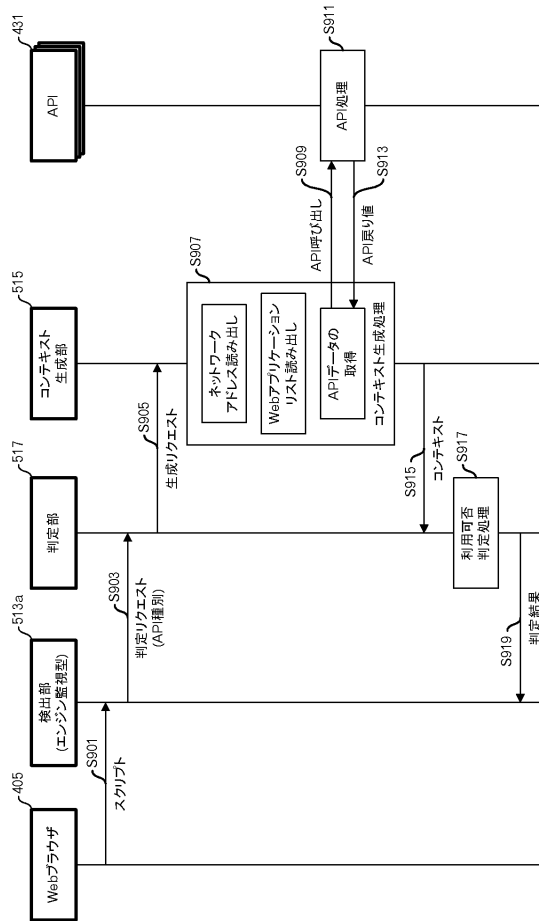
【図 7】

コンテキスト	Webアプリケーション	API(アドレス帳)	API(署名)	API(GPS)	API(復号)
CNT_A	すべて	利用可	利用可	利用不可	利用不可
CNT_B	すべて	利用可	利用不可	利用不可	利用不可
CNT_C	すべて	利用不可	利用不可	利用不可	利用不可
CNT_D	zzz.jp/zz	利用不可	利用不可	利用可	利用可
CNT_E	zzz.jp/zz	利用不可	利用不可	利用可	利用不可
CNT_F	zzz.jp/zz	利用不可	利用不可	利用不可	利用不可

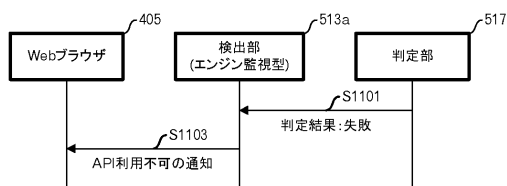
【図 8】



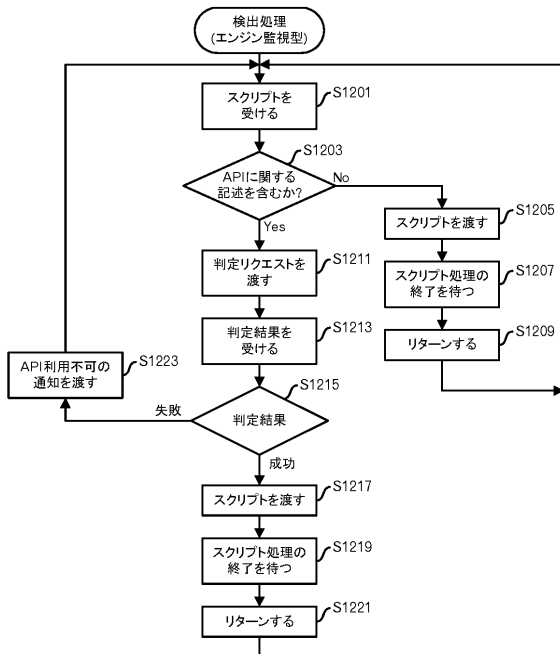
【図 9】



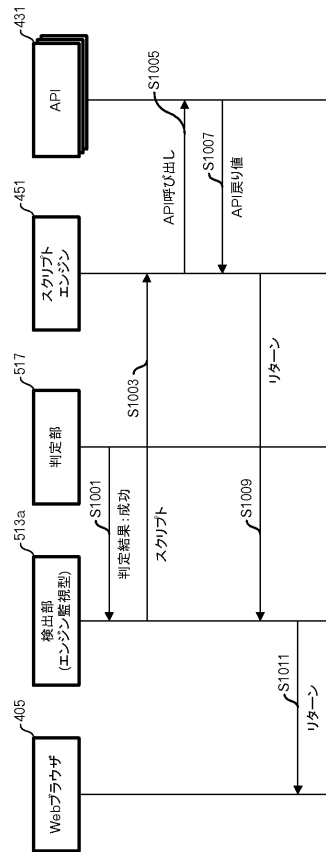
【図 11】



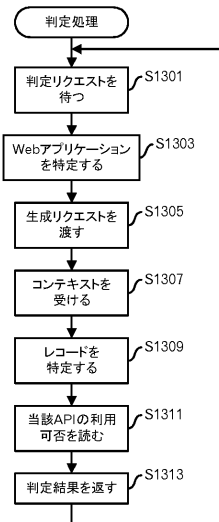
【図 12】



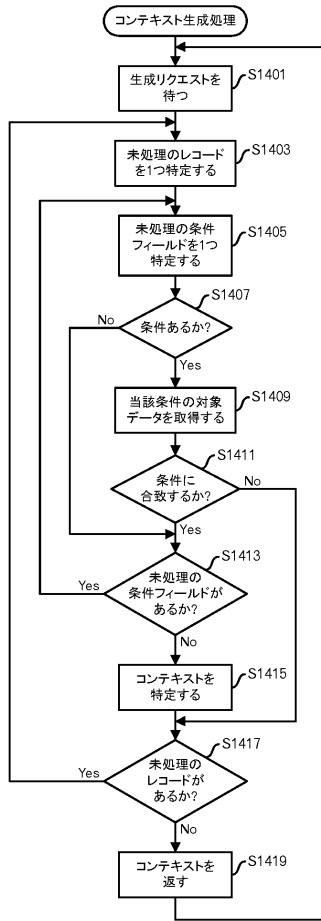
【図 10】



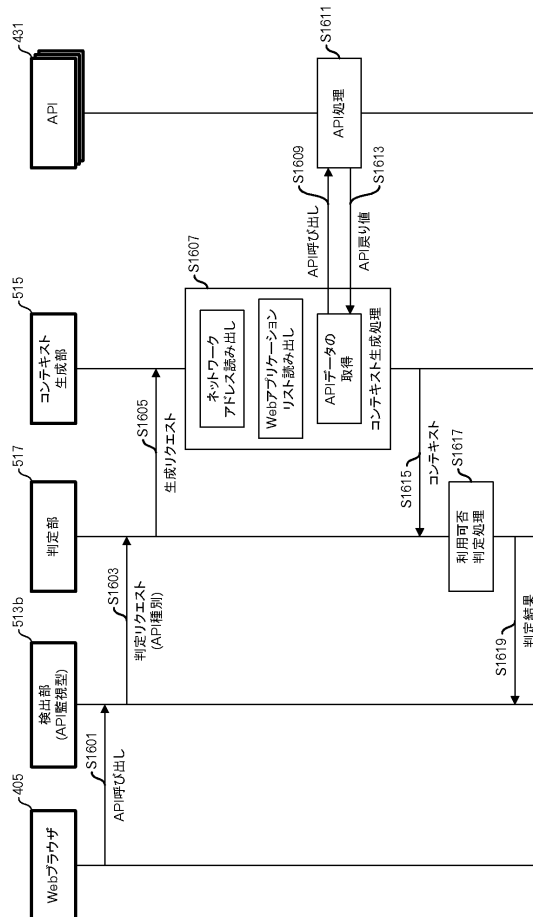
【図 13】



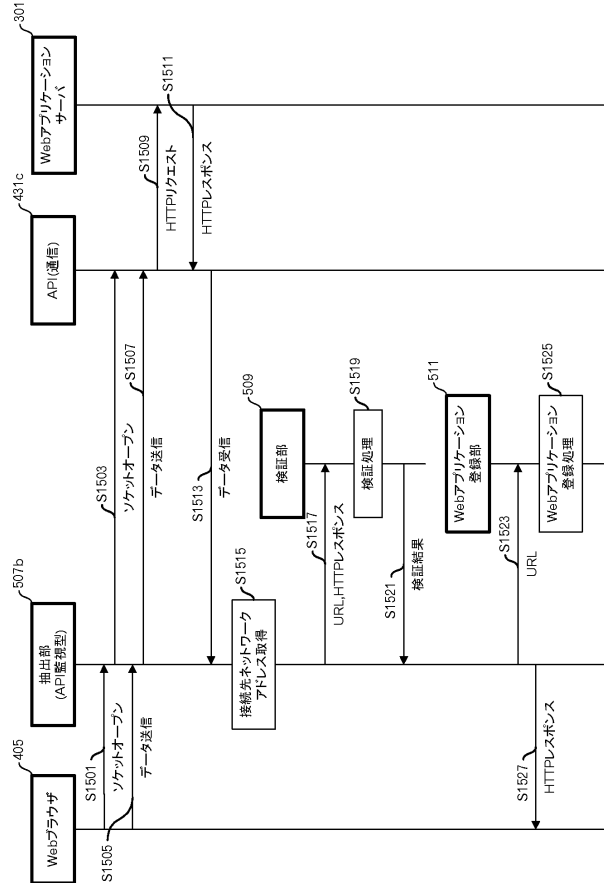
【図 14】



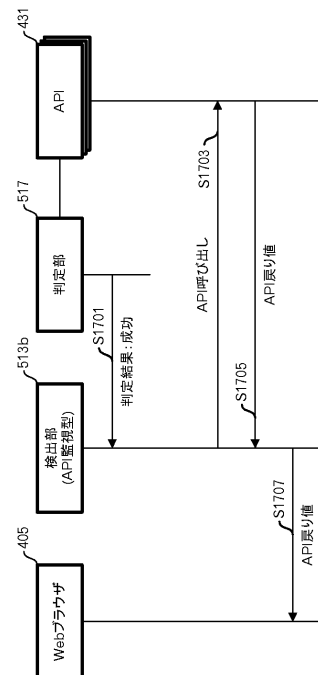
【図 16】



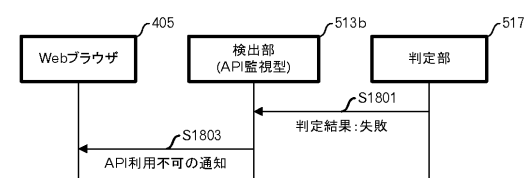
【図 15】



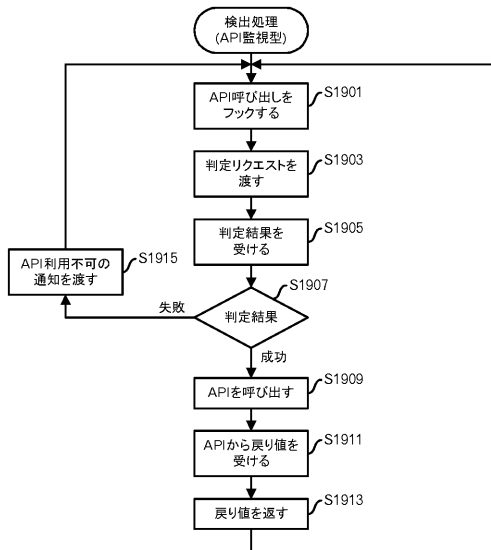
【図 17】



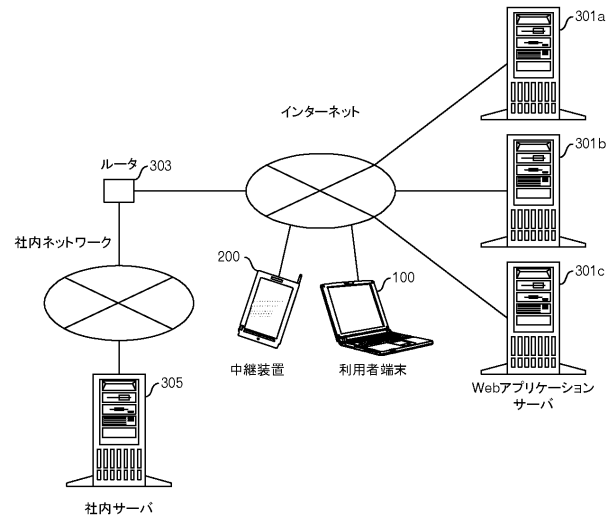
【図 18】



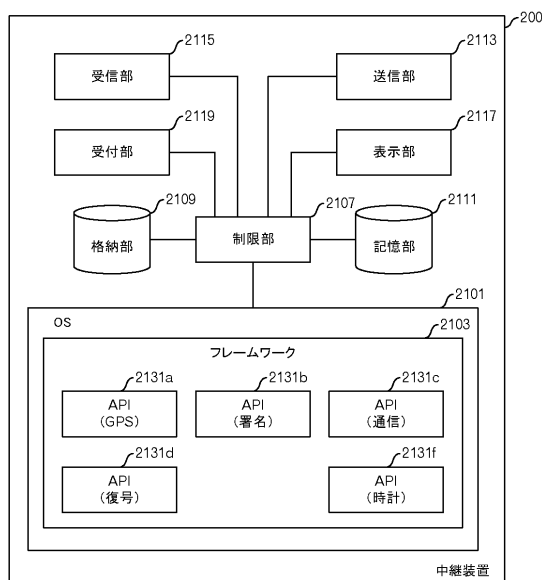
【図 19】



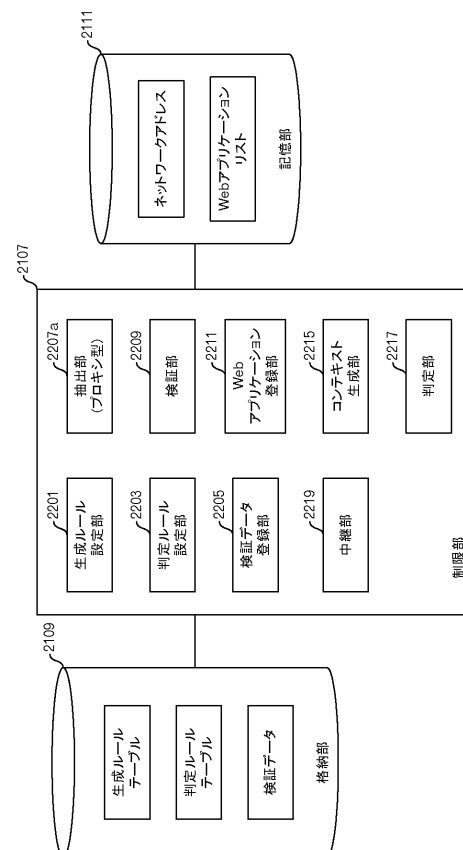
【図 20】



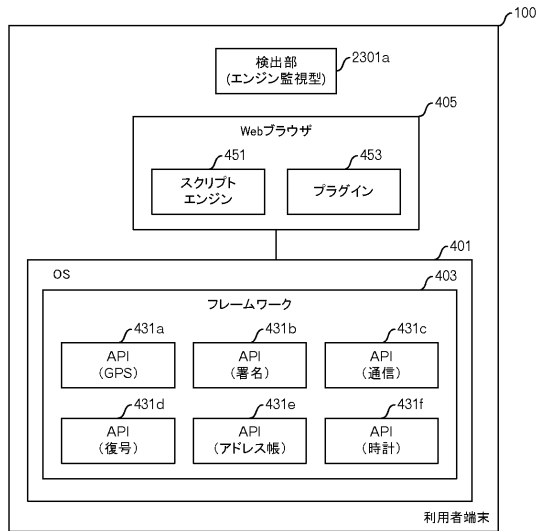
【図 21】



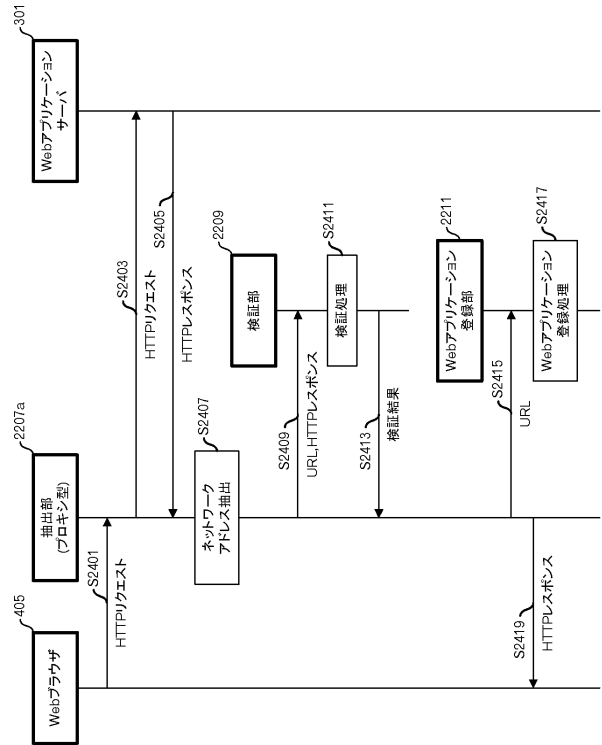
【図 22】



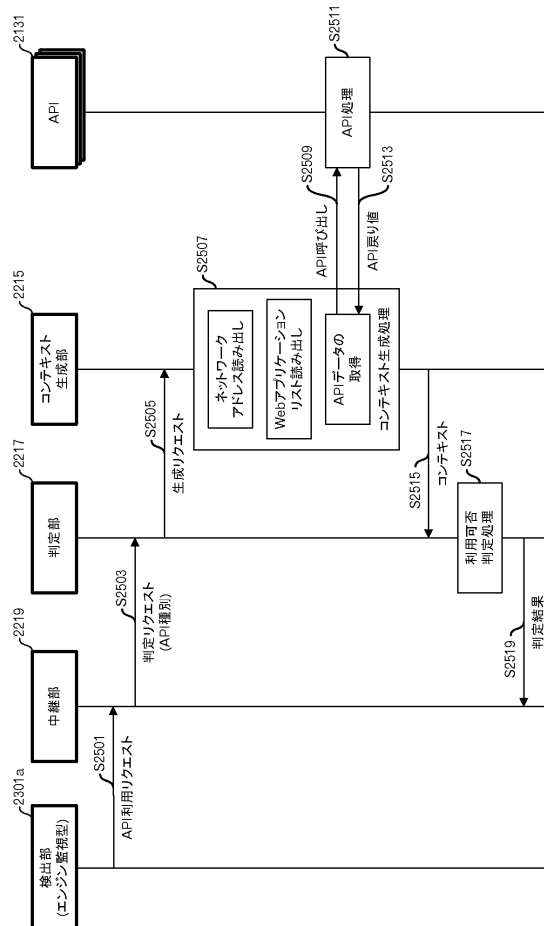
【図 23】



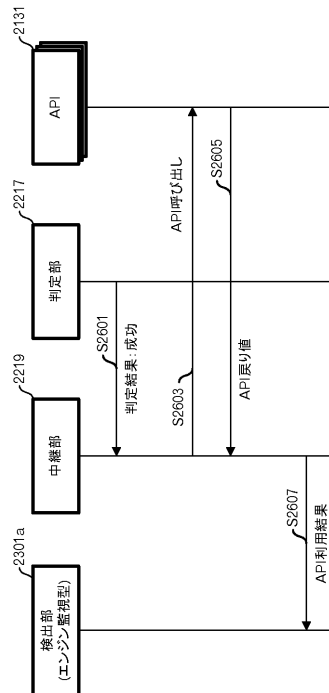
【図 24】



【図 25】

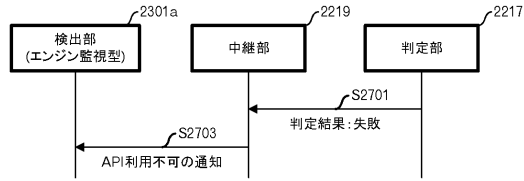


【図 26】

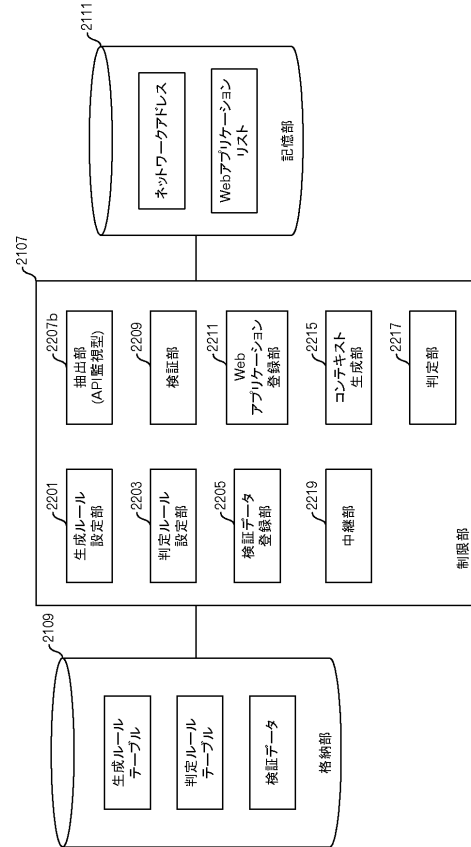




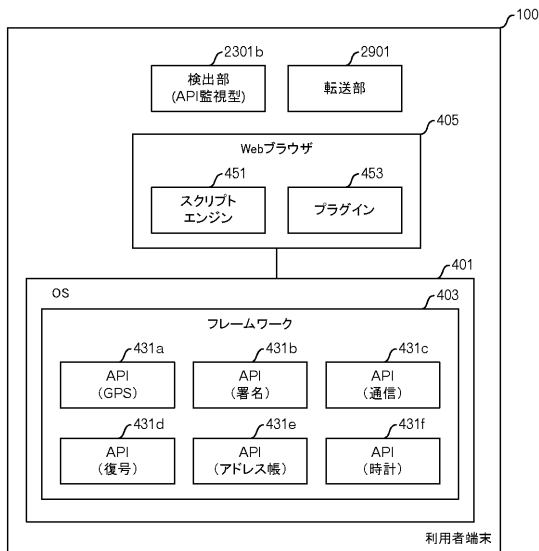
【図 27】



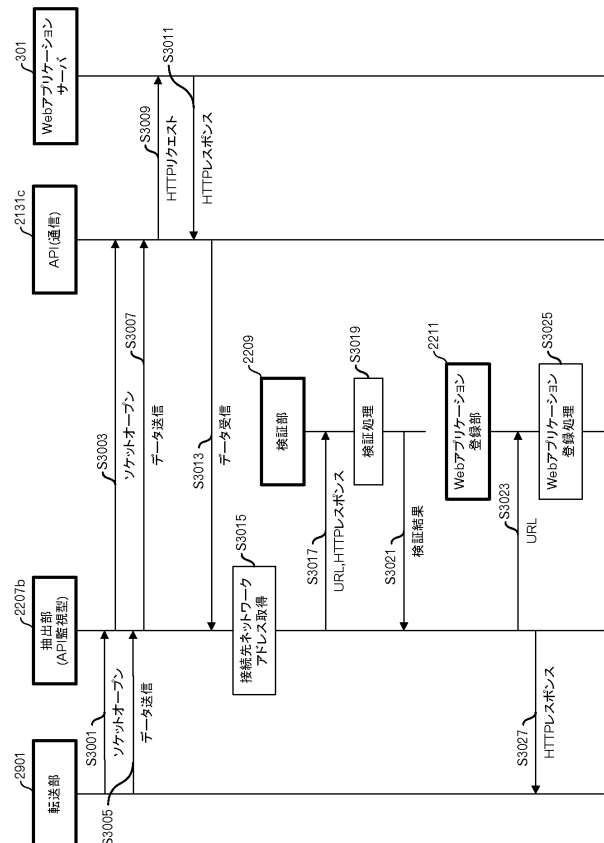
【図 28】



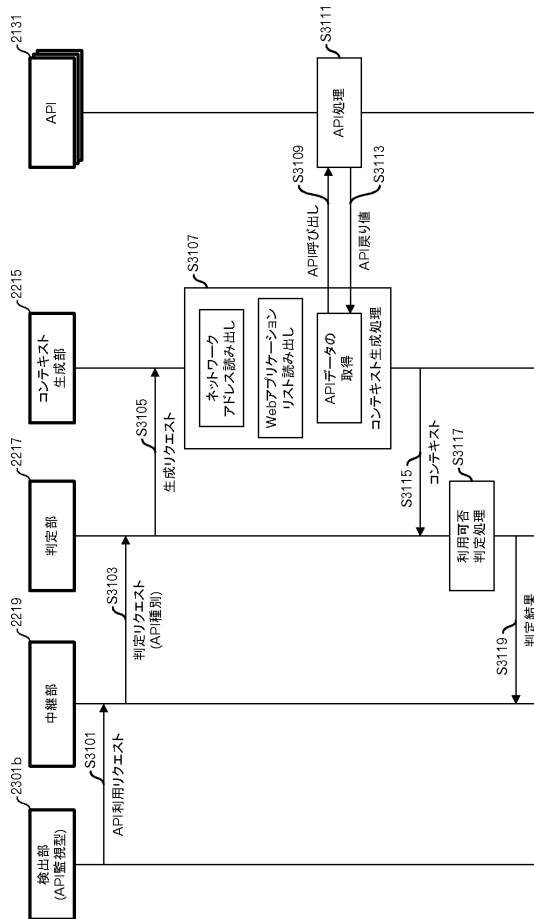
【図 29】



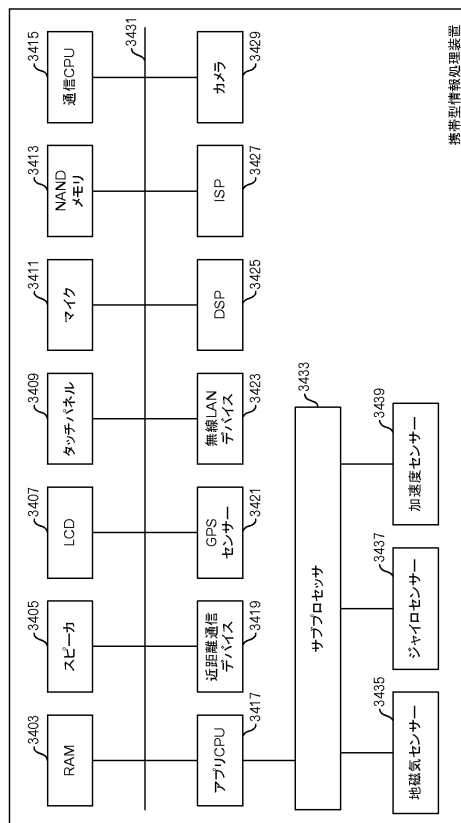
【図 30】



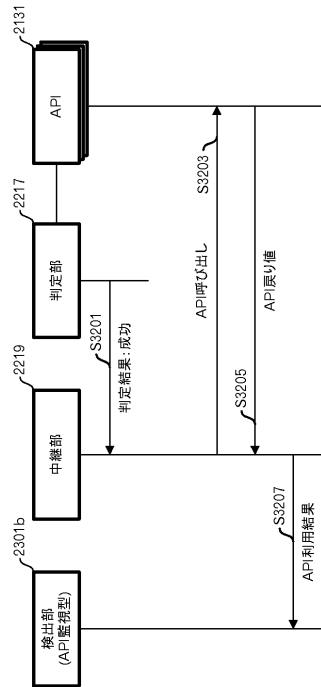
【 図 3 1 】



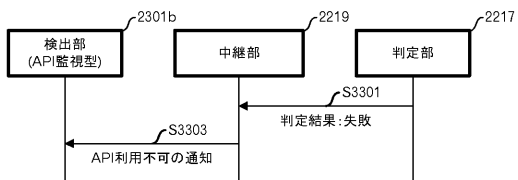
【 図 3 4 】



【 図 3 2 】



【 図 3 3 】



---

フロントページの続き

(72)発明者 大久保 隆夫  
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

審査官 金木 陽一

(56)参考文献 特開平6-131301(JP,A)  
特開2004-46666(JP,A)  
特開2008-165325(JP,A)  
特開2007-328757(JP,A)  
特表2009-521191(JP,A)  
特開2010-11101(JP,A)  
特開2009-130856(JP,A)  
国際公開第2008/050512(WO,A1)  
米国特許出願公開第2009/0183227(US,A1)