(19)日本国特許庁(JP)

(12)特許公報(B1)

(11)特許番号
特許第7547594号
(P7547594)

(45)発行日　令和6年9月9日(2024.9.9)

(24)登録日　令和6年8月30日(2024.8.30)

(51)国際特許分類

		FI	
Ｇ０６Ｑ	*10/0635(2023.01)*	Ｇ０６Ｑ	10/0635
Ｇ０６Ｆ	*21/57 (2013.01)*	Ｇ０６Ｆ	21/57

請求項の数　13　（全25頁）

(21)出願番号　特願2023-186227(P2023-186227)
(22)出願日　令和5年10月31日(2023.10.31)
審査請求日　令和5年10月31日(2023.10.31)
早期審査対象出願

(73)特許権者　521541734
株式会社アシュアード
東京都渋谷区渋谷２－１５－１
(74)代理人　110002815
ＩＰＴｅｃｈ弁理士法人
(72)発明者　鈴木 和幸
東京都渋谷区渋谷２－１５－１渋谷クロスタワー１２Ｆ 株式会社アシュアード内
(72)発明者　戸谷 慧
東京都渋谷区渋谷２－１５－１渋谷クロスタワー１２Ｆ 株式会社アシュアード内
(72)発明者　内山 陽介
東京都渋谷区渋谷２－１５－１渋谷クロスタワー１２Ｆ 株式会社アシュアード内
(72)発明者　ファン イーミン オリバー
最終頁に続く

(54)【発明の名称】　情報処理装置及び情報処理方法

(57)【特許請求の範囲】

【請求項１】

組織に属するユーザが利用するサービスに対するアクセス履歴を取得する取得部と、

前記アクセス履歴に基づいて、前記ユーザが利用するサービスを特定し、前記アクセス履歴に基づいて、特定された前記サービスに対する操作情報を特定し、特定されたサービス及び前記サービスに対応付けられた前記操作情報を含むサービス一覧を生成する制御部と、

前記サービス一覧を表示する出力部と、

前記サービスに関するリスク評価情報を前記サービスと対応付けて記憶する記憶部と、を備え、

前記出力部は、前記出力部によって表示される前記サービス一覧について、前記サービス一覧に含まれる前記サービスを前記ユーザが指定する操作を受け付けた場合に、前記ユーザによって指定された前記サービスに対する操作の内容であって、前記記憶部において前記サービスと対応付けて記憶されるリスク評価情報の開示の要求を少なくとも含む前記操作の内容を前記ユーザが選択可能に表示し、

前記制御部は、前記操作の内容を選択する操作を前記ユーザから受け付けた場合に、前記ユーザによって選択された前記操作の内容に応じた処理を実行する、情報処理装置。

【請求項２】

前記操作情報は、前記サービスにログインする情報、前記サービスに対してデータをアップロードする情報、前記サービスからデータをダウンロードする情報、前記サービスを

利用するユーザが増加した情報、前記サービスを利用するユーザが減少した情報、前記サービスが共有アカウントを用いて複数のユーザによって利用されている旨を示す情報、及び、前記サービスが指定されたIPアドレス以外からアクセスされた旨を示す情報の少なくともいずれか1つを含む、請求項１に記載の情報処理装置。

【請求項３】

前記制御部は、特定された前記サービスが有する特徴情報を特定し、

前記制御部は、特定された前記特徴情報を含む前記サービス一覧を生成する、請求項１に記載の情報処理装置。

【請求項４】

前記特徴情報をサービスと対応付けて記憶する記憶部を備え、

前記制御部は、前記記憶部を参照して、前記特徴情報を特定する、請求項３に記載の情報処理装置。

【請求項５】

前記特徴情報は、前記サービスがファイルのアップロードに対応する旨を示す情報、前記サービスがファイルのダウンロードに対応する旨を示す情報、前記サービスが仮想専用線に対応していない旨を示す情報、前記サービスが前記組織の外部に公開される旨を示す情報、前記サービスが他のサービスと連携する旨を示す情報、前記サービスがユーザ認証に対応していない旨を示す情報、及び、前記サービスがコミュニケーションツールである旨を示す情報の少なくともいずれか1つを含む、請求項３に記載の情報処理装置。

【請求項６】

前記組織で利用を制限する第1サービスの情報を記憶する記憶部を備え、

前記制御部は、特定された前記サービスの中から、前記第1サービスの情報に基づいて、前記第1サービスを特定し、

前記出力部は、前記第1サービスが特定されることにより、前記第1サービスの利用が検知された旨の通知を出力する、請求項１に記載の情報処理装置。

【請求項７】

前記サービス一覧の対象から除外される第2サービスの情報を記憶する記憶部を備え、

前記制御部は、前記アクセス履歴に基づいて、前記第2サービスの利用を検知しても、前記第2サービスを前記サービス一覧の対象から除外する、請求項１に記載の情報処理装置。

【請求項８】

前記制御部は、特定された前記サービスの中から、前記操作情報に基づいて、前記組織で対応が必要である第3サービスを特定し、特定された第3サービスが視覚的に強調された態様で前記サービス一覧を生成する、請求項１に記載の情報処理装置。

【請求項９】

前記制御部は、特定された前記サービスの中から、前記特徴情報に基づいて、前記組織で対応が必要である第3サービスを特定し、特定された第3サービスが視覚的に強調された態様で前記サービス一覧を生成する、請求項４に記載の情報処理装置。

【請求項１０】

前記制御部は、前記記憶部を参照し、特定された前記サービスの中から、前記リスク評価情報と対応付けられた第4サービスを特定し、特定された第4サービスについて前記リスク評価情報を含む態様で前記サービス一覧を生成する、請求項１に記載の情報処理装置。

【請求項１１】

前記リスク評価情報は、リスク評価に関する数値を含み、

前記制御部は、前記リスク評価に関する数値が閾値よりも低い前記第4サービスを特定し、特定された第4サービスが視覚的に強調された態様で前記サービス一覧を生成する、請求項１０に記載の情報処理装置。

【請求項１２】

前記リスク評価情報は、非公開情報に基づいた第1リスク評価情報と、公開情報に基づいた第2リスク評価情報と、を含む、請求項１１に記載の情報処理装置。

【請求項１３】
プロセッサを備えるコンピュータが実行する情報処理方法であって、前記プロセッサが、
組織に属するユーザが利用するサービスに対するアクセス履歴を取得するステップＡと、
前記アクセス履歴に基づいて、前記ユーザが利用するサービスを特定するステップＢと、
前記アクセス履歴に基づいて、特定された前記サービスに対する操作情報を特定するステップＣと、
特定された前記サービス及び特定された前記操作情報を含むサービス一覧を生成するステップＤと、
前記サービス一覧を表示するステップＥと、
前記サービスに関するリスク評価情報を前記サービスと対応付けて記憶するステップＦと、
前記ステップＥで表示される前記サービス一覧について、前記サービス一覧に含まれる前記サービスを前記ユーザが指定する操作を受け付けた場合に、前記ユーザによって指定された前記サービスに対する操作の内容であって、前記ステップＦにおいて前記サービスと対応付けて記憶されるリスク評価情報の開示の要求を少なくとも含む前記操作の内容を前記ユーザが選択可能に表示するステップＧと、
前記操作の内容を選択する操作を前記ユーザから受け付けた場合に、前記ユーザによって選択された前記操作の内容に応じた処理を実行するステップＨと、を実行する、情報処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置及び情報処理方法に関する。
【背景技術】
【０００２】
従来、クラウドサービスの利用を検知する手法が提案されている（例えば、特許文献１）。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開2021-77271公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
上述した手法によれば、利用が検知されたサービスに関する情報の提供が十分ではない場合がある。
【０００５】
そこで、本発明は、上述した課題を解決するためになされたものであり、検知したサービスに関する情報を提供することを可能とする情報処理装置及び情報処理方法を提供することを目的とする。
【課題を解決するための手段】
【０００６】
開示の態様は、組織に属するユーザが利用するサービスに対するアクセス履歴を取得する取得部と、前記アクセス履歴に基づいて、前記ユーザが利用するサービスを特定し、前記アクセス履歴に基づいて、特定された前記サービスに対する操作情報を特定し、特定されたサービス及び前記サービスに対応付けられた前記操作情報を含むサービス一覧を生成する制御部と、前記サービス一覧を出力する出力部と、を備える、情報処理装置である。
【０００７】
開示の態様は、組織に属するユーザが利用するサービスに対するアクセス履歴を取得するステップと、前記アクセス履歴に基づいて、前記ユーザが利用するサービスを特定する

ステップと、前記アクセス履歴に基づいて、特定された前記サービスに対する操作情報を特定するステップと、特定された前記サービス及び特定された前記操作情報を含む前記サービスの一覧を生成するステップと、前記サービスの一覧を出力するステップと、を備える、情報処理方法である。

【発明の効果】

【０００８】

本発明によれば、検知したサービスに関する情報を容易に把握するための情報を提供することを可能とする情報処理装置及び情報処理方法を提供することができる。

【図面の簡単な説明】

【０００９】

【図１】図１は、実施形態に係る情報処理システム100を示す図である。
【図２】図２は、実施形態に係る情報処理装置10を示す図である。
【図３】図３は、実施形態に係る表示態様300を示す図である。
【図４】図４は、実施形態に係る表示態様300を示す図である。
【図５】図５は、実施形態に係る表示態様300を示す図である。
【図６】図６は、実施形態に係る表示態様300を示す図である。
【図７】図７は、実施形態に係る情報処理方法を示す図である。
【図８】図８は、変更例1に係る表示態様300を示す図である。
【図９】図９は、変更例1に係る表示態様300を示す図である。
【図１０】図１０は、変更例2に係る表示態様300を示す図である。
【図１１】図１１は、変更例3に係る表示態様300を示す図である。

【発明を実施するための形態】

【００１０】

以下において、実施形態について図面を参照しながら説明する。なお、以下の図面の記載において、同一又は類似の部分には、同一又は類似の符号を付している。

【００１１】

但し、図面は模式的なものであり、各寸法の比率などは現実のものとは異なる場合があることに留意すべきである。従って、具体的な寸法などは以下の説明を参酌して判断すべきである。また、図面相互間においても互いの寸法の関係又は比率が異なる部分が含まれている場合があることは勿論である。

【００１２】

［開示の概要］

開示の概要に係る情報処理装置は、組織に属するユーザが利用するサービスに対するアクセス履歴を取得する取得部と、前記アクセス履歴に基づいて、前記ユーザが利用するサービスを特定し、前記アクセス履歴に基づいて、特定された前記サービスに対する操作情報を特定し、特定されたサービス及び前記サービスに対応付けられた前記操作情報を含むサービス一覧を生成する制御部と、前記サービス一覧を出力する出力部と、を備える。

【００１３】

開示の概要に係る情報処理方法は、組織に属するユーザが利用するサービスに対するアクセス履歴を取得するステップと、前記アクセス履歴に基づいて、前記ユーザが利用するサービスを特定するステップと、前記アクセス履歴に基づいて、特定された前記サービスに対する操作情報を特定するステップと、特定された前記サービス及び特定された前記操作情報を含む前記サービスの一覧を生成するステップと、前記サービスの一覧を出力するステップと、を備える。

【００１４】

開示の概要では、情報処理装置は、サービスに対するアクセス履歴に基づいて、サービスに対応する操作情報を特定した上で、特定されたサービス及び操作情報を含むサービス一覧を出力する。このような構成によれば、サービス一覧が操作情報を含むため、操作情報の内容に応じて対応の必要性を判断することが可能な形で、検知したサービスに関する情報を提供することができる。

【００１５】
開示の概要において、組織は、法人格を有する団体であってもよく、法人格を有していない団体であてもよい。ユーザは、組織と雇用関係を有する者であってもよく、組織と契約関係を有する者であってもよく、組織の構成員と読み替えられてもよい。具体的には、企業の従業員等が該当する。
【００１６】
［実施形態］
（情報処理システム）
以下において、実施形態に係る情報処理システムについて説明する。図１は、実施形態に係る情報処理システム100を示す図である。
【００１７】
図１に示すように、情報処理システム100は、情報処理装置10と、端末20と、端末30と、を有する。情報処理装置10、端末20及び端末40は、ネットワーク200によって接続される。特に限定されるものではないが、ネットワーク200は、インターネットによって構成されてもよい。ネットワーク200は、ローカルエリアネットワークを含んでもよく、移動体通信網を含んでもよく、VPN（Virtual Private Network）を含んでもよい。
【００１８】
情報処理装置10は、組織に属するユーザが利用するサービスに関する情報を処理する装置である。情報処理装置10の詳細については後述する（図２を参照）。
【００１９】
端末20は、組織に属するユーザによって用いられる端末である。例えば、端末20は、パーソナルコンピュータであってもよく、スマートフォンであってもよく、タブレット端末であってもよい。端末20は、表示部21を有してもよい。表示部21は、液晶パネル、有機EL（Electroluminescence）パネル、LED（Light Emitting Diode）などのディスプレイによって構成されてもよい。図１では、1つの端末20が例示されているが、実際には多数の端末20が存在してもよい。端末20は、ユーザ端末と称されてもよく、第1端末と称されてもよい。
【００２０】
実施形態では、表示部21に表示可能なブラウザを用いてサービスやアプリケーションが利用されるケースについて例示する。特に断らない限り、サービスは、アプリケーションを含むものと考えてもよい。サービスには、SaaS等のクラウドサービスが含まれる。端末20には、ブラウザ拡張機能がインストールされ、ブラウザ拡張機能によって、サービスに対するアクセス履歴が端末20から情報処理装置10に送信されてもよい。また、情報処理装置10は、クラウドサービス等のサービスが提供するAPI（Application Programming Interface）を利用し、API連携によりアクセス履歴を取得してもよい。また、情報処理装置10は、ユーザの利用する端末20にエージェントプログラムを導入したり、ゲートウェイを通過するトラフィックからアクセス履歴を取得したりしてもよいが、アクセス履歴を取得する手段は、特にこれらに限られない。組織の情報処理装置10は、受信したアクセス履歴情報に基づき、ユーザによるサービスの利用状況を検知し、利用しているサービス一覧のデータを生成する。ここで、ブラウザ拡張機能は、Webブラウザに特定の機能を追加するためのプログラムであり、アドオン、プラグイン又はエクステンションとも呼ばれる。アクセス履歴は、アクセスログと称されてもよく、HTML（Hyper Text Markup Language）、XML（Extensible Markup Language）などのマークアップ言語によって表されてもよいが、これに限られない。アクセス履歴は、ユーザの端末20からブラウザを介してアクセスしたサービスやウェブサイトの情報である。アクセス履歴は、アクセス元の情報（ユーザID、IPアドレス、ブラウザ名、OS名等）、アクセスされた日時、最後にアクセスされた日時、アクセス回数、アクセスされたファイル名、ユーザが行った操作、送信バイト数、受信バイト数、アクセス先の情報等の項目からなるログデータを含む。アクセス先の情報には、アクセス先のURL（Universal Resource Indicator）やタイトル、その他のキーワードの情報が含まれる。また、アクセス履歴には、ユーザが使用する端末の

起動、シャットダウン、ネットワークへの接続、ソフトウェアのインストールなどの操作ログが含まれてもよい。また、アクセス履歴には、ユーザが使用する端末とサーバとの間の送受信の内容や時間などの通信ログが含まれてもよい。また、アクセス履歴には、ユーザがネットワークやシステムへログインした履歴や、アプリケーションの動作等のアプリケーションログ、セキュリティに関する動作等のセキュリティログ、システムの動作等のシステムログ、システム等の設計変更に関する設計変更ログ、発生したエラーに関するエラーログを含んでもよい。

【００２１】

端末30は、組織のIT部門やその他の管理部門等、組織に属するユーザが利用するサービスに関する情報を管理する管理者によって用いられる端末である。例えば、端末30は、パーソナルコンピュータであってもよく、スマートフォンであってもよく、タブレット端末であってもよい。端末30は、表示部31を有してもよい。表示部31は、液晶パネル、有機ELパネル、LEDなどのディスプレイによって構成されてもよい。端末30は、管理者端末と称されてもよく、第2端末と称されてもよい。

【００２２】

実施形態では、表示部31は、情報処理装置10から受信する表示データに基づいて、組織に属するユーザが利用するサービスに関する情報を表示する。表示部31の表示態様の詳細については後述する（図３～図６を参照）。

【００２３】

（情報処理装置）

以下において、実施形態に係る情報処理装置10について説明する。図２は、実施形態に係る情報処理装置10を示す図である。なお、情報処理装置10は、クラウドサービスとして組織の外部のネットワークに設置されてもよいし、ユーザが所属する組織の内部のネットワークに設置されてもよい。

【００２４】

図２に示すように、情報処理装置10は、送信部11と、受信部12と、格納部13と、制御部14と、を有する。

【００２５】

送信部11は、通信モジュールによって構成されてもよい。通信モジュールは、IEEE802.11a/b/g/n/ac/ax、LTE、5G、6Gなどの規格に準拠する無線通信モジュールであってもよく、IEEE802.3などの規格に準拠する有線通信モジュールであってもよい。

【００２６】

送信部11は、組織に属するユーザが利用するサービスに関する情報を表示するための表示データを、組織のIT部門等が使用する端末30に送信する。サービスに関する情報は、サービス及びサービスに対応付けられた操作情報を含むサービス一覧を含んでもよい。サービス一覧は、ユーザによる利用が検知されたサービスを一覧で表示するものである。サービス一覧の詳細については後述する（図３～図６を参照）。

【００２７】

実施形態では、送信部11は、サービス一覧を出力する出力部を構成する。

【００２８】

受信部12は、通信モジュールによって構成されてもよい。通信モジュールは、IEEE802.11a/b/g/n/ac/ax、LTE、5G、6Gなどの規格に準拠する無線通信モジュールであってもよく、IEEE802.3などの規格に準拠する有線通信モジュールであってもよい。

【００２９】

受信部12は、組織に属するユーザが利用するサービスに対するアクセス履歴を端末20から受信する。受信部12は、端末20のブラウザにインストールされるブラウザ拡張機能からアクセス履歴を受信してもよい。上述したように、アクセス履歴は、HTML、XMLなどのマークアップ言語によって表されてもよい。受信部12は、アクセス履歴など、ネットワークを介して取得可能な情報を受信し、取得した情報に基づき、ユーザが利用しているサービスを検出する。

【００３０】
実施形態では、受信部12は、組織に属するユーザが利用するサービスに対するアクセス履歴を取得する取得部を構成する。
【００３１】
格納部13は、SSD（Solid State Drive）、HDD（Hard Disk Drive）などの記憶媒体によって構成されており、様々な情報を格納する。
【００３２】
格納部13は、端末20から受信するアクセス履歴を記憶してもよい。格納部13は、サービスが有する特徴情報をサービスと対応付けて記憶してもよい。例えば、格納部13は、サービスの名称と特徴情報とを対応付けたテーブル（サービスDB）を記憶してもよい。
【００３３】
格納部13は、組織でユーザによる利用を制限する又は禁止する第1サービスの情報を記憶してもよい。特に断らない限り、制限は、禁止を含むものと考えてもよい。第1サービスの情報は、第1サービスを識別する情報（例えば、サービスの名称）を少なくとも含めばよい。第1サービスは、セキュリティ上の懸念等に基づいて、ユーザによる利用が制限又は禁止されるサービスであり、第1サービスの情報のリストは、ブラックリストと称されてもよい。
【００３４】
格納部13は、サービス一覧の対象から除外される第2サービスの情報を記憶してもよい。第2サービスの情報は、第2サービスを識別する情報（例えば、サービスの名称）を少なくとも含めばよい。第2サービスは、セキュリティ上の懸念がない又は小さい等の理由から、ユーザによる利用が組織によって認められ、ユーザによる利用が検知された場合であっても、サービス一覧に表示する必要がないサービスであり、第2サービスの情報のリストは、ホワイトリストと称されてもよい。
【００３５】
格納部13は、サービスに関するリスク評価情報をサービスと対応付けて記憶してもよい。リスク評価情報は、リスク評価に関する数値を含んでもよい。リスク評価に関する数値は、100点を上限とした点数で表されてもよい。
【００３６】
リスク評価情報は、非公開情報に基づいた第1リスク評価情報を含んでもよい。第1リスク評価情報は、サービスを提供する提供者に対する調査結果に基づいて生成されてもよい。調査結果は、提供者に対するアンケートの結果を含んでもよく、具体的には、提供者によるセキュリティチェックシートの回答結果を含んでもよい。セキュリティチェックシートに含まれるチェックリストは、セキュリティ対策に関する複数の質問項目を含む。なお、チェックリストは、セキュリティ評価提供業者によって策定されたものであってもよい。リスク評価は、チェックリストに対する回答に基づいて取得されてもよく、各質問項目や回答の選択肢に割り当てられた点数の合計等によって算出されてもよい。
【００３７】
リスク評価情報は、公開情報に基づいた第2リスク評価情報を含んでもよい。第2リスク評価情報は、アクセス等が制限されないネットワーク上で収集可能な情報に基づいて生成されてもよい。アクセス等が制限されないネットワーク上で収集可能な情報は、公開情報の一例である。
【００３８】
例えば、ウェブ関連収集部は、サービスを利用するためのログインURLに基づいて、サービスに関するログインページにアクセスし、ウェブ関連の情報を収集してもよい。ウェブ関連の情報は、ウェブ関連のリスクの評価に用いられる情報であってもよい。例えば、ウェブ情報収集部は、ログインURLに基づいたアクセスによってサーバから発行されるCookieを収集してもよく、ログインURLに基づいたアクセスに対するサーバからのレスポンスに付与されるHTTPヘッダを収集してもよい。ウェブ関連収集部は、受信部12及び制御部14によって構成されてもよい。

【００３９】
例えば、評価機能部は、ウェブ関連収集部によって収集された情報に基づいて、サービスのリスク評価を算定する機能を有してもよい。具体的には、評価機能部は、ウェブ関連収集部によって収集された情報に基づいてリスク項目を特定し、特定されたリスク項目に基づいてリスク評価を算定してもよい。リスク評価は、特定されたリスク項目の総数及び対策済みのリスク項目の数によって表されてもよい。このようなケースにおいて、リスク評価は、対策網羅率と称されてもよい。評価機能部は、評価項目毎にリスク評価を算定してもよい。評価機能部は、制御部14によって構成されてもよい。
【００４０】
ここで、格納部13は、サービス（以下、登録サービス）に関する情報を登録する台帳を記憶してもよい。台帳には、組織内でユーザが利用中のサービスが組織によって登録され、サービスに関する個別の情報やリスク評価情報等を管理できる。例えば、登録サービスに関する情報は、登録サービスの名称、登録サービスの特徴情報、登録サービスのリスク評価情報などを含んでもよい。台帳は、情報処理装置10で管理されるユーザ（以下、登録ユーザ）に関する情報を登録していてもよい。登録ユーザに関する情報は、登録ユーザの名称、登録ユーザのメールアドレス、登録ユーザが用いるウェブブラウザの種類、登録ユーザが所属する組織及び部署の名称などを含んでもよい。
【００４１】
実施形態では、格納部13は、特徴情報をサービスと対応付けて記憶する記憶部を構成する。
【００４２】
制御部14は、少なくとも1つのプロセッサを含んでもよい。少なくとも1つのプロセッサは、CPU（Central Processing Unit）、MPU（Micro Processing Unit）、GPU（Graphics Processing Unit）、1以上のIntegrated Circuit、1以上のDiscrete Circuit、及び、これらの組合せによって構成されてもよい。
【００４３】
動作例1では、制御部14は、端末20から受信するアクセス履歴に基づいて、ユーザが利用するサービスを特定する。制御部14は、端末20から受信するアクセス履歴に基づいて、特定されたサービスに対する操作情報を特定する。例えば、制御部14は、サービス名とサービス識別子（例えば、URL）とを対応付ける情報を格納するサービスDBを参照して、アクセス履歴によって特定されるURLに対応するサービス名を特定する。
【００４４】
制御部14は、特定されたサービスについて、ブラウザ拡張機能等により取得できるアクセス履歴の解析によって操作情報を特定する。操作情報は、以下に示す情報を含んでもよい。例えば、制御部14は、アクセスログに含まれるアクセス先のURLがログインページ（例えば、・・・/login/など）である旨が検出された場合に、ログインする操作が行われたと判定してもよい。また、制御部14は、サービスへのログインの形式がパスワード認証である場合に、新規に認証用cookieが発行されたことが検出された場合に、ログインする操作が行われたと判定してもよい。制御部14は、データ送信量が閾値以上になった場合に、ファイル等のデータがアップロードされていると判定してもよく、アップロードページへのアクセスが検出された場合に、ファイル等のデータがアップロードされていると判定してもよい。
【００４５】
オプション1-1では、操作情報は、サービスにログインする情報（以下、ログイン操作）を含んでもよい。ログイン操作は、サービスを利用する際にログインを要求されるサービスについて、ユーザがサービスにログインする操作を示す情報である。
【００４６】
オプション1-2では、操作情報は、サービスに対して、ファイル等のデータをアップロードする情報（以下、ファイルアップロード）を含んでもよい。ファイルアップロードは、データのアップロードが可能なサービスについて、ユーザがファイル等のデータをアッ

プロードする操作を示す情報である。制御部14は、HTTP（Hyper Text Transfer Protocol）で規定された通信メソッドを含むリクエストの内容に基づきファイルアップロードを判定してもよい。例えば、リクエストメソッドがPOSTであり、かつ、ヘッダに「multipart/form-data」が含まれる場合に、ファイルアップロードと判定してもよい。

【００４７】

オプション1-3では、操作情報は、サービスからファイル等のデータをダウンロードする情報（以下、ファイルダウンロード）を含んでもよい。ファイルダウンロードは、データのダウンロードが可能なサービスについて、ユーザがデータをダウンロードする操作を示す情報である。

【００４８】

オプション1-4では、操作情報は、サービスを利用するユーザの数が増加した情報（以下、利用増加）を含んでもよい。利用増加は、単位期間（例えば、3日、7日、1ヶ月など）においてサービスを利用するユーザの増加数が閾値を超える旨を示す情報であってもよい。

【００４９】

オプション1-5では、操作情報は、サービスを利用するユーザの数が減少した情報（以下、利用減少）を含んでもよい。利用減少は、単位期間（例えば、3日、7日、1ヶ月など）においてサービスを利用するユーザの減少数が閾値を超える旨を示す情報であってもよい。

【００５０】

オプション1-6では、操作情報は、サービスが特定のアカウントを用いて複数の異なるユーザによって利用されている旨を示す情報（以下、共有アカウント利用）を含んでもよい。つまり、共有アカウント利用は、1つのアカウントを複数のユーザで共有して利用している旨を示す情報である。共有アカウント利用は、共有アカウントを用いて利用可能なサービスについて、複数の異なるユーザが共有アカウントを用いている旨を示す情報であってもよい。制御部14は、ブラウザ等からユーザのフィンガープリント等の情報を取得し、特定のアカウントから複数のユーザのフィンガープリント等が同時に検出された場合に、共有アカウント利用と判定してもよい。

【００５１】

オプション1-7では、操作情報は、サービスが指定されたIPアドレス以外からアクセスされた旨を示す情報（以下、指定外IP）を含んでもよい。指定外IPは、アクセス可能なIPアドレスが指定されたサービスについて、指定されたIPアドレス以外からアクセスされたことを示す情報であってもよい。例えば、指定されたIPアドレスは、組織のオフィス等で用いるIPアドレスや、組織が管理する機器に割り当てられたIPアドレスであってもよい。すなわち、指定外IPは、組織のオフィス等以外の場所からサービスにアクセスされたことや、組織外の危機からサービスにアクセスされたことを示す情報であってもよい。また、指定されたIPアドレスは、複数のIPアドレスを含んでもよく、IPアドレスの範囲で指定されてもよい。

【００５２】

オプション1-8では、操作情報は、メールアドレス等の情報の登録・変更、新規ユーザの招待、インターネットへの情報公開などを含んでもよい。

【００５３】

操作情報は、オプション1-1～オプション1-8の中から選択された2以上のオプションを含んでもよい。

【００５４】

制御部14は、サービス及びサービスに対応付けられた操作情報を含むサービス一覧を生成する。つまり、制御部14は、サービスの名称とともに当該サービスに関する操作情報を表示するための表示データを生成する。上述したように、サービス一覧を表示するための表示データ、つまり、サービスの名称と操作情報とを表示するための表示データは、送信部11によって端末30に送信される。

【００５５】
動作例2では、制御部14は、特定されたサービスについて、サービスが有する特徴情報を特定する。制御部14は、サービスを提供するサーバから特徴情報を取得することによって、特徴情報を特定してもよい。制御部14は、格納部13を参照して、特徴情報を特定してもよい。特徴情報は、以下に示す情報を含んでもよい。例えば、制御部14は、サービス名とURLとを対応付ける情報を格納するサービスDBを参照して、アクセス履歴によって特定されるURLに対応するサービス名を特定する。制御部14は、サービス名と特徴情報とを対応付けるサービスDBを参照して、特定されたサービス名に対応する特徴情報を特定し、特定された特徴情報を取得してもよい。サービスDBは、格納部13に格納されてもよい。
【００５６】
オプション2-1では、特徴情報は、サービスがファイル等のデータのアップロードに対応する旨を示す情報（以下、ファイルアップロード）を含んでもよい。ファイルアップロードは、サービスにおいてデータのアップロードが可能である旨を示す情報であってもよい。
【００５７】
オプション2-2では、特徴情報は、サービスがファイル等のデータのダウンロードに対応する旨を示す情報（以下、ファイルダウンロード）を含んでもよい。ファイルダウンロードは、サービスにおいてデータのダウンロードが可能である旨を示す情報であってもよい。
【００５８】
オプション2-3では、特徴情報は、サービスが仮想専用線に対応していない旨を示す情報（以下、VPN（Virtual Private Network）非対応）を含んでもよい。VPN非対応は、VPN以外の回線（例えば、公衆回線）でサービスを利用可能である旨を示す情報であってもよい。
【００５９】
オプション2-4では、特徴情報は、URLの共有等の機能により、サービスが組織の外部に公開される旨を示す情報（以下、外部公開）を含んでもよい。外部公開は、組織の外部からサービスにアクセス可能である旨を示す情報であってもよく、組織の外部に対してサービスがアクセス可能である旨を示す情報であってもよい。組織の外部は、組織のネットワーク（例えば、イントラネットワーク）の外部を意味してもよい。
【００６０】
オプション2-5では、特徴情報は、API連携等により、サービスが他のサービスと連携する旨を示す情報（以下、外部アプリ連携）を含んでもよい。他のサービスは、組織のネットワーク（例えば、イントラネットワーク）以外のネットワークで提供されるサービスを意味してもよい。他のサービスは、他のアプリケーションと読み替えられてもよい。
【００６１】
オプション2-6では、特徴情報は、サービスが、シングルサインオンやID連携等のユーザ認証に対応していない（SAML認証等の認証方式が利用できないサービスである）旨を示す情報（以下、SAML（Security Assertion Markup Language）非対応）を含んでもよい。SAMLは、ユーザ認証のための認証情報の一例であり、ユーザ認証は、SAML以外の方式であってもよい。
【００６２】
オプション2-7では、特徴情報は、サービスがコミュニケーションツールである旨を示す情報（以下、メール送信）を含んでもよい。メール送信は、コミュニケーションツールの一例であり、コミュニケーションツールは、メール受信、チャット送信、チャット受信、ビデオ会議ツールなどを含んでもよい。
【００６３】
特徴情報は、オプション2-1～オプション2-7の中から選択された2以上のオプションを含んでもよい。
【００６４】

制御部14は、サービス及びサービスが有する特徴情報を含むサービス一覧を生成する。上述したように、サービス一覧を表示するための表示データは、送信部11によって端末30に送信される。

【００６５】

動作例3では、動作例1及び動作例2が組み合わされてもよい。すなわち、サービス一覧は、操作情報及び特徴情報の双方を含んでもよい。

【００６６】

動作例4では、制御部14は、アクセス履歴に基づいて、第1サービスの利用を検知してもよい。このようなケースにおいて、制御部14は、第1サービスの利用が検知された旨の通知の出力を送信部11に指示してもよい。第1サービスの利用が検知された旨の通知は、上述したサービス一覧の表示とは別に出力されてもよい。第1サービスの利用が検知された旨の通知は、ブラックリストに含まれる第1サービスの利用が検知された場合に警告として出力されてもよい。

【００６７】

動作例5では、制御部14は、アクセス履歴に基づいて、第2サービスの利用を検知しても、第2サービスをサービス一覧の対象から除外してもよい。言い換えると、ホワイトリストに含まれる第2サービスは、サービス一覧の対象から除外される。

【００６８】

動作例6では、制御部14は、特定されたサービスの中から、操作情報に基づいて、組織で対応が必要である第3サービスを特定し、特定された第3サービスが視覚的に強調された態様でサービス一覧を生成してもよい。組織で対応が必要である第3サービスは、操作情報との関係で予め定義されたサービスであってもよい。例えば、セキュリティ上のリスクがあり、セキュリティの観点から対応が必要と考えられる操作が検知された第3サービスとして特定してもよい。例えば、操作情報がファイルアップロードであるサービスが第3サービスとして特定されてもよい。

【００６９】

視覚的に強調された態様は、第3サービスに関する文字列の色彩、フォント、サイズ、書体（太字、斜体、下線など）が第3サービス以外に関する文字列の色彩、フォント、サイズ、書体（太字、斜体、下線など）と異なる態様であってもよい。

【００７０】

動作例7では、制御部14は、特定されたサービスの中から、特徴情報に基づいて、組織で対応が必要である第3サービスを特定し、特定された第3サービスが視覚的に強調された態様でサービス一覧を生成してもよい。組織で対応が必要である第3サービスは、特徴情報との関係で予め定義されたサービスであってもよい。例えば、セキュリティ上のリスクがあり、セキュリティの観点から対応が必要と考えられる特徴を有するサービスを第3サービスとして特定してもよい。例えば、特徴情報が外部公開又は外部アプリ連携であるサービスが第3サービスとして特定されてもよい。

【００７１】

視覚的に強調された態様は、第3サービスに関する文字列の色彩、フォント、サイズ、書体（太字、斜体、下線など）が第3サービス以外に関する文字列の色彩、フォント、サイズ、書体（太字、斜体、下線など）と異なる態様であってもよい。

【００７２】

動作例8では、動作例6及び動作例7が組み合わされてもよい。すなわち、制御部14は、特定されたサービスの中から、操作情報及び特徴情報に基づいて、組織で対応が必要である第3サービスを特定し、特定された第3サービスが視覚的に強調された態様でサービス一覧を生成してもよい。組織で対応が必要である第3サービスは、操作情報及び特徴情報との関係で予め定義されたサービスであってもよい。例えば、操作情報がファイルアップロードであり、かつ、特徴情報が外部公開又は外部アプリ連携であるサービスが第3サービスとして特定されてもよい。

【００７３】

視覚的に強調された態様は、第3サービスに関する文字列の色彩、フォント、サイズ、書体（太字、斜体、下線など）が第3サービス以外に関する文字列の色彩、フォント、サイズ、書体（太字、斜体、下線など）と異なる態様であってもよい。

【００７４】

動作例9では、制御部14は、特定されたサービスの中から、アクセス履歴（例えば、サービスの名称など）に基づいて、リスク評価情報と対応付けられた第4サービスを特定し、特定された第4サービスについてリスク評価情報を含む態様でサービス一覧を生成してもよい。第4サービスは、第2リスク評価情報のみと対応付けられたサービスを含まずに、第1リスク評価情報と対応付けられたサービスを含んでもよい。第4サービスは、第1リスク評価情報及び第2リスク評価情報の双方と対応付けられたサービスであってもよい。

【００７５】

動作例9において、リスク評価情報がリスク評価に関する数値を含む場合には、制御部14は、リスク評価に関する数値が閾値よりも低い第4サービスを特定し、特定された第4サービスが視覚的に強調された態様でサービス一覧を生成してもよい。

【００７６】

リスク評価に関する数値は、第2リスク評価情報に含まれる数値ではなくて、第1リスク評価情報に含まれる数値であってもよい。リスク評価に関する数値は、第1リスク評価情報及び第2リスク評価情報の双方に含まれる数値の集計結果であってもよい。集計結果は、第1リスク評価情報及び第2リスク評価情報に含まれる数値の合計であってもよく、第1リスク評価情報及び第2リスク評価情報に含まれる数値に重付値を加味した集計結果であってもよい。第1リスク評価情報に含まれる数値の重付値は、第2リスク評価情報に含まれる数値の重付値よりも大きくてもよい。

【００７７】

実施形態では、制御部14は、アクセス履歴に基づいて、ユーザが利用するサービスを特定し、アクセス履歴に基づいて、特定されたサービスに対する操作情報を特定し、特定されたサービス及びサービスに対応付けられた操作情報を含むサービス一覧を生成する制御部を構成する。

【００７８】

（表示態様）

以下において、実施形態に係る表示態様について説明する。図３～図６は、実施形態に係る表示態様を示す図である。上述したように、表示態様は、端末30の表示部31に表示される態様であってもよい。表示態様は、情報処理装置10から送信される表示データに基づいて表示される態様であってもよい。

【００７９】

図３に示すように、表示態様300は、サービス一覧310及びアクションボタン320を含んでもよい。

【００８０】

サービス一覧310は、名称、検知操作、サービスの特徴を含んでもよい。

【００８１】

名称は、アクセス履歴に基づいて検知（特定）されたサービスの名称の一例である。

【００８２】

検知操作は、アクセス履歴に基づいて検知（特定）されたサービスに対する操作情報の一例である。操作情報としては、上述したオプション1-1～オプション1-8の中から選択された1以上の操作情報が考えられる。図３では、ログイン操作、ファイルアップロード、利用増加、指定外IP、利用減少、共有アカウント利用などが例示されている。

【００８３】

サービスの特徴は、アクセス履歴に基づいて検知（特定）されたサービスが有する特徴情報の一例である。特徴情報としては、上述したオプション2-1～オプション2-7の中から選択された1以上の特徴情報が考えられる。サービス一覧310は、サービス一覧310に含まれるサービスを選択するためのチェックボックス311を含んでもよい。

【００８４】
すなわち、サービス一覧310は、サービス及びサービスに対応付けられた操作情報を含むサービス一覧の一例である。サービス一覧は、サービス及びサービスが有する特徴情報を含むサービス一覧であると考えてもよい。ここで、サービス一覧は、検知（特定）されたサービスを全て含んでいる必要はなく、検知（特定）されたサービスの一部であってもよい。
【００８５】
アクションボタン320は、チェックボックス311によってチェックされたサービスに対する操作を指定するためのボタンである。アクションボタン320の詳細については後述する（図６を参照）。
【００８６】
図４に示すように、サービス一覧310は、検知人数/30日、検知人数/7日、アクセス数/30日、アクセス数/7日、ドメイン、送信バイト数、受信バイト数を含んでもよい。
【００８７】
検知人数/30日は、30日間においてサービスを利用したユーザの数である。検知人数/7日は、7日間においてサービスを利用したユーザの数である。30日及び7日は例示であり、ユーザの数を集計する期間は任意に設定することが可能であり、一定期間内にサービスを利用したユーザの数を示す指標であればよい。検知人数は、アクセス履歴（例えば、ブラウザ拡張機能にログインするユーザの識別情報）に基づいて特定可能である。
【００８８】
アクセス数/30日は、30日間におけるサービスに対するアクセスの数である。アクセス数/7日は、7日間におけるサービスに対するアクセスの数であり、一定期間内にサービスを利用したユーザの数を示す指標であればよい。30日及び7日は例示であり、アクセスの数を集計する期間は任意に設定することが可能である。アクセス数は、アクセス履歴に基づいて特定可能である。
【００８９】
ドメインは、サービスの所在を示すドメインである。ドメインは、IPアドレスによって代替されてもよく、IPアドレスと対応付けられてもよい。
【００９０】
送信バイト数は、任意の集計期間（例えば、7日、30日など）においてサービスに対して送信したデータのサイズである。データのサイズは、Byteで表されてもよく、K Byteで表されてもよく、M Byteで表されてもよい。
【００９１】
受信バイト数は、任意の集計期間（例えば、7日、30日など）においてサービスから受信したデータのサイズである。データのサイズは、Byteで表されてもよく、K Byteで表されてもよく、M Byteで表されてもよい。
【００９２】
図５に示すように、サービス一覧310は、セキュリティ評価及びウェブ評価を含んでもよい。
【００９３】
セキュリティ評価は、サービスを提供する提供者に対するセキュリティに関する調査結果に基づいて生成されるリスク評価情報であってもよい。セキュリティ評価は、非公開情報に基づいた第1リスク評価情報の一例である。セキュリティ評価は、サービスを提供する提供者が入力したセキュリティチェックシートの回答結果に基づいて算出されたスコアであってもよい。
【００９４】
ウェブ評価は、アクセス等が制限されないネットワーク（例えば、ウェブ）上で収集可能な情報に基づいて生成されるリスク評価であってもよい。ウェブ評価は、公開情報に基づいた第2リスク評価情報の一例である。ウェブ評価は、サービスに関するウェブサイト等の公開情報に基づいて算出されたスコアであってもよい。

【００９５】
図６に示すように、アクションボタン320の選択（例えば、クリック）に応じて、チェックボックス311によってチェックされたサービスに対する操作一覧（図６では、「評価開示を依頼」、「除外リストに追加」、「台帳に移す」など）が表示されてもよい。操作一覧の中から操作が選択された場合に、選択された操作がチェックボックス311によってチェックされたサービスに対して実行される。
【００９６】
特に限定されるものではないが、「評価開示を依頼」は、チェックボックス311によってチェックされたサービスについて、情報処理装置10に記憶されたリスク評価情報の開示を、サービスを提供する提供者又はリスク評価情報を管理するリスク評価業者に対して要求する操作であってもよい。開示が要求されるリスク評価情報は、第1リスク評価情報及び第2リスク評価情報の少なくともいずれか1つであってもよい。「除外リストに追加」は、チェックボックス311によってチェックされたサービスをホワイトリストに追加する操作であってもよい。「台帳に移す」は、チェックボックス311によってチェックされたサービスを台帳に移す操作であってもよい。
【００９７】
図３に示す表示態様は、上述した動作例1～動作例3の一例である。ここで、ブラックリストに含まれる第1サービスの利用が検知された場合には、サービス一覧310とは別に、第1サービスの利用が検知された旨の通知が出力されてもよい（動作例4）。ホワイトリストに含まれる第2サービスは、サービス一覧310の対象から除外されてもよい（動作例4）。さらに、操作情報及び特徴情報の少なくともいずれか1つに基づいて特定された第3サービス（例えば、図３に示すサービス”BBBB”）は、サービス一覧310において視覚的に強調された態様で表示されてもよい（動作例6～動作例8）。
【００９８】
図５に示す表示態様は、上述した動作例9の一例である。ここで、例えば、閾値が80であるケースを例示すると、リスク評価に関する数値が閾値よりも低い第4サービス（例えば、図５に示すサービス”AAAA”）は、サービス一覧310において視覚的に強調された態様で表示されてもよい。
【００９９】
（情報処理方法）
以下において、実施形態に係る情報処理方法について説明する。図７は、実施形態に係る情報処理方法を示す図である。
【０１００】
図７に示すように、ステップS10において、端末20のユーザは、サービスに対する操作を実行する。例えば、ブラウザにインストールされたブラウザ拡張機能は、サービスに対するアクセス履歴を取得する。
【０１０１】
ステップS11において、端末20は、アクセス履歴を情報処理装置10に送信する。例えば、ブラウザにインストールされたブラウザ拡張機能は、サービスに対するアクセス履歴を情報処理装置10に送信する。
【０１０２】
ステップS12において、情報処理装置10は、端末20から受信するアクセス履歴を記憶する。
【０１０３】
図７では、説明簡略化のために1つの端末20からアクセス履歴が取得されるケースが例示されているが、実際には多数の端末20からアクセス履歴が取得されてもよい。
【０１０４】
ステップS20において、端末30は、表示態様300を表示する要求を情報処理装置10に送信する。上述したように、表示態様300は、サービス一覧310を含んでもよい。
【０１０５】

ステップS21において、情報処理装置10は、表示態様300を表示するための表示データを生成し、生成された表示データを端末30に送信する。

【０１０６】

ステップS22において、端末30は、表示データに基づいて表示態様300を表示する。

【０１０７】

（作用及び効果）

実施形態では、情報処理装置10は、サービスに対するアクセス履歴に基づいて、サービスに対応する操作情報を特定した上で、特定されたサービス及び操作情報を含むサービス一覧310を出力する（例えば、動作例1、動作例3）。このような構成によれば、サービス一覧310により、企業等の組織が利用を許可していないサービスを特定することができるとともに、サービス一覧310が操作情報を含むため、操作情報の内容に応じて、セキュリティの観点等から、サービスやアプリケーションの利用停止やアカウントの削除等の対応の必要性を判断することが可能な形で、検知したサービスに関する情報を提供することができる。これにより、組織のIT部門等の管理部門による組織の利用サービスやアカウントの管理が容易になるとともに、セキュリティリスクを回避することが可能になる。

【０１０８】

実施形態では、情報処理装置10は、サービスに対するアクセス履歴に基づいて、サービスに対応する特徴情報を特定した上で、特定されたサービス及び特徴情報を含むサービス一覧310を出力してもよい（例えば、動作例2、動作例3）。このような構成によれば、サービス一覧310が特徴情報を含むため、特徴情報の内容に応じて、セキュリティの観点等から、対応の必要性を判断することが可能な形で、検知したサービスに関する情報を提供することができる。

【０１０９】

実施形態では、情報処理装置10は、ブラックリストに含まれる第1サービスの利用を検知した場合に、第1サービスの利用が検知された旨の通知を出力してもよい（動作例4）。このような構成によれば、管理者が不適切なサービスの利用を容易に把握することができ、サービスの利用停止等の対応を迅速に講じることができる

【０１１０】

実施形態では、情報処理装置10は、ホワイトリストに含まれる第2サービスの利用を検知しても、第2サービスをサービス一覧310の対象から除外してもよい（動作例5）。このような構成によれば、サービス一覧310において不要な情報を除外することができ、サービス一覧の視認性を向上させることができ、サービス一覧310で管理者が確認すべきサービスを容易に特定することができる。

【０１１１】

実施形態では、情報処理装置10は、操作情報及び特徴情報の少なくともいずれか1つに基づいて第3サービスを特定し、特定された第3サービスが視覚的に強調された態様でサービス一覧310を生成してもよい（動作例6～動作例8）。このような構成によれば、組織で対応が必要である第3サービスを管理者が容易に特定することができる。

【０１１２】

実施形態では、情報処理装置10は、アクセス履歴に基づいて、リスク評価情報と対応付けられた第4サービスを特定し、特定された第4サービスについてリスク評価情報を含む態様でサービス一覧310を生成してもよい（動作例9）。このような構成によれば、サービス一覧310がリスク評価情報を含むため、組織で対応が必要である第3サービスを管理者が容易に特定することができる。

【０１１３】

実施形態では、情報処理装置10は、リスク評価に関する数値が閾値よりも低い第4サービスを特定し、特定された第4サービスが視覚的に強調された態様でサービス一覧310を生成してもよい（動作例9）。このような構成によれば、組織で対応が必要である第4サービスを管理者が容易に特定することができる。

【０１１４】

［変更例1］
以下において、実施形態の変更例1について説明する。以下においては、実施形態に対する相違点について主として説明する。
【０１１５】
変更例1では、表示態様300のバリエーションについて説明する。
【０１１６】
第1に、表示態様300は、アクセス履歴に基づいて情報処理装置10によって検知された結果の概要に関する情報を含んでもよい。結果の概要は、図８に示す情報を含んでもよい。
【０１１７】
結果の概要は、表示態様300は、アクセス履歴に基づいて情報処理装置10によって検知されたユーザの数（図８では、検知ユーザ数）を含んでもよい。
【０１１８】
結果の概要は、アクセス履歴に基づいて情報処理装置10によって検知されたアクセスの数（図８では、検知アクセス数）を含んでもよい。
【０１１９】
結果の概要は、アクセス履歴に基づいて情報処理装置10によって検知されたサービスの数（図８では、検知サービス数）を含んでもよい。
【０１２０】
結果の概要は、アクセス履歴に基づいて情報処理装置10によって検知されたサービスの内訳を含んでもよい。内訳は、ドーナツ型の円グラフによって表されてもよい。但し、グラフの形態は、ドーナツ型の円グラフに限定されるものではない。
【０１２１】
登録サービスは、情報処理装置10が有するサービスDBで管理されるサービスである。なお、登録サービスの数に加え、登録サービスの内、組織の台帳に登録されているサービスの数を表示してもよい。その他ウェブサイトは、ユーザによってアクセスされたサービス以外のウェブサイトであってもよい。不明サービスは、サービスの内容を特定することができなかったサービスであってもよい。その他は、登録サービス、その他ウェブサイト、不明サービスのいずれにも該当しないサービスであってもよい。
【０１２２】
表示態様300は、ユーザのアクセスが検知されたサービスの総数（図８に示すyy件）を含んでもよい。表示態様300は、内訳を構成する項目毎のサービスの数（図８に示すxx件）を含んでもよい。さらに、サービスの内訳を表示する条件（図８では、アクセス数50件以上）が設定されてもよい。
【０１２３】
第2に、表示態様300は、検知されたサービスの一覧（以下、検知サービス一覧）を含んでもよい。
【０１２４】
図９に示すように、検知サービス一覧330は、名称、検知人数/30日、アクセス数/30日、最終検知日、可用性、機密性、調査実績などを含んでもよい。名称、検知人数/30日、アクセス数/30日、最終検知日については、上述した内容と同様であるため、その詳細については省略する。
【０１２５】
可用性は、ユーザがサービスに安全にアクセス可能であるかという観点が重要であるサービスか否かを示す情報である。可用性の欄においては、可用性が重要であるサービスについては、重要といった情報が表示され、可用性が重要でないサービスについては、何の情報も表示されなくてもよい。
【０１２６】
機密性は、権限を有するユーザのみがサービスにアクセス可能であるかという観点が重要であるサービスか否かを示す情報である。機密性の欄においては、機密性が重要であるサービスについては、重要といった情報が表示され、機密性が重要でないサービスについ

ては、何の情報も表示されなくてもよい。
【０１２７】
調査実績は、リスク評価情報に関する調査の実績があるか否かを示す情報である。調査の実績は、非公開情報に基づいた第1リスク評価情報に関する調査の実績であってもよい。調査の実績は、非公開情報に基づいた第1リスク評価情報及び公開情報に基づいた第2リスク評価情報の双方に関する調査の実績であってもよい。調査実績の欄には、調査実績があるサービスについては、ありといった情報が表示され、調査実績があるサービスについては、何の情報も表示されなくてもよい。
【０１２８】
特に限定されるものではないが、検知サービス一覧330は、上述したサービス一覧310に組み込まれてもよい。
【０１２９】
［変更例2］
以下において、実施形態の変更例2について説明する。以下においては、実施形態に対する相違点について主として説明する。
【０１３０】
変更例2では、サービス一覧310に含まれるサービスの絞り込みについて説明する。
【０１３１】
図１０に示すように、表示態様300は、サービス一覧310とともに、サービス一覧310に含まれるサービスの絞り込みに用いるフィルタ340を含む。特に限定されるものではないが、フィルタ340で選択可能な項目は、操作情報や特徴情報としてサービス一覧310に含まれる項目を含んでもよい。フィルタ340で選択可能な項目は、管理者によって任意に設定可能であってもよい。また、フィルタ340には、絞り込みに用いる項目を示す名称と、サービス一覧310に含まれるサービスの内、当該項目に該当するサービスの数とが表示されている。
【０１３２】
例えば、図１０の上段に示す状態において、フィルタ340のログイン操作が選択された場合には、図１０の下段に示すように、情報処理装置10は、サービス一覧310において、操作情報としてログイン操作が検知されていない（ログイン操作に該当しない）サービスを除外し、ログイン操作が検知された（ログイン操作に該当する）サービスを含めるように絞り込みが行われ、サービス一覧310の表示が更新される。また、例えば、セキュリティに関するインシデント（不正アクセス、情報漏洩など）の履歴を、サービス名と対応付けてサービスDBに記憶しておき、フィルタ340の項目として「インシデント履歴あり」を選択することで、インシデントの履歴のあるサービスへの絞り込みが行えるようにしてもよい。
【０１３３】
［変更例3］
以下において、実施形態の変更例3について説明する。以下においては、実施形態に対する相違点について主として説明する。
【０１３４】
変更例3では、表示態様300のバリエーションについて説明する。表示態様300は、ユーザ一覧350を含んでもよい。
【０１３５】
図１１に示すように、ユーザ一覧350は、メールアドレス、NGサービス、検知サービス数、最終検知日、ユーザ登録、ブラウザなどを含んでもよい。
【０１３６】
メールアドレスは、ユーザを識別する情報の一例である。メールアドレスは、ユーザの名称などと置き換えられてもよい。
【０１３７】
NGサービスは、組織で確認すべきサービスの有無を示す情報である。組織で確認すべき

サービスがあるユーザについては、アイコン360が表示されてもよい。例えば、アイコン360は、ユーザによるNGサービスへのアクセスが検知された場合に表示され、ユーザによるNGサービスへのアクセスが検知されなかった場合に表示されなくてもよい。組織で確認すべきサービスは、ブラックリストに含まれる第1サービス（動作例4）であってもよく、組織で対応が必要である第3サービス（動作例6～動作例8）であってもよく、リスク評価に関する数値が閾値よりも低い第4サービス（動作例9）であってもよい。

【０１３８】

最終検知日は、サービスに対するユーザのアクセスが最後に検知された日である。最終検知日は、時、分、秒などを含んでもよい。

【０１３９】

ユーザ登録は、情報処理装置10の台帳にユーザが登録されているか否かを示す情報である。例えば、登録済みは、ユーザが台帳に登録されている旨を示しており、招待済みは、台帳への登録を要求している旨を示していてもよい。

【０１４０】

ブラウザは、ユーザが用いるウェブブラウザの種類を示す情報である。

【０１４１】

ここで、NGサービスの欄においてアイコン360が選択された場合に、情報処理装置10は、組織で確認すべきサービスの詳細情報を表示してもよい。サービスの詳細情報は、実施形態で説明したサービス一覧310であってもよい。

【０１４２】

［その他の実施形態］

本発明は上述した実施形態によって説明したが、この開示の一部をなす論述及び図面は、この発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施形態、実施例及び運用技術が明らかとなろう。

【０１４３】

上述した開示において、アクセス履歴の受信は、アクセス履歴の取得と相互に読み替えられてもよい。サービス一覧310の出力は、サービス一覧310の表示、サービス一覧310を表示するための表示データの送信と相互に読み替えられてもよい。

【０１４４】

上述した開示では、表示態様300を表示するための表示データの生成が情報処理装置10によって実行されるケースについて例示した。しかしながら、上述した開示はこれに限定されるものではない。例えば、表示データの生成は、端末30上のアプリケーションによって実行されてもよい。このようなケースにおいて、表示データの生成に必要な情報は、情報処理装置10から端末30に送信されてもよい。

【０１４５】

上述した開示では特に触れていないが、表示は、物理現実における表示を含んでもよく、AR（Artificial Reality）などの拡張現実における表示を含んでもよく、VR（Virtual Reality）などの仮想現実における表示を含んでもよく、Metaverseなどの仮想空間における表示を含んでもよい。

【０１４６】

上述した開示では、情報処理装置10は、表示態様300を表示するための表示データを端末30に送信する。このようなケースにおいて、表示データの送信は、表示態様300（例えば、サービス一覧310）の出力の一例であると考えてもよい。

【０１４７】

上述した開示では特に触れていないが、情報処理装置10は、表示態様300を表示する表示部を有してもよい。表示部は、液晶パネル、有機ELパネル、LEDなどのディスプレイによって構成されてもよい。このようなケースにおいて、表示態様300の表示は、表示態様300（例えば、サービス一覧310）の出力の一例であると考えてもよい。

【０１４８】

実施形態では特に触れていないが、情報処理装置10及び端末30が行う各処理をコンピ

ュータに実行させるプログラムが提供されてもよい。また、プログラムは、コンピュータ読取り可能媒体に記録されていてもよい。コンピュータ読取り可能媒体を用いれば、コンピュータにプログラムをインストールすることが可能である。ここで、プログラムが記録されたコンピュータ読取り可能媒体は、非一過性の記録媒体であってもよい。非一過性の記録媒体は、特に限定されるものではないが、例えば、CD-ROMやDVD-ROM等の記録媒体であってもよい。

【０１４９】

或いは、情報処理装置10及び端末30が行う各処理を実行するためのプログラムを記憶するメモリ及びメモリに記憶されたプログラムを実行するプロセッサによって構成されるチップが提供されてもよい。

【０１５０】

［付記］

第1の特徴は、組織に属するユーザが利用するサービスに対するアクセス履歴を取得する取得部と、前記アクセス履歴に基づいて、前記ユーザが利用するサービスを特定し、前記アクセス履歴に基づいて、特定された前記サービスに対する操作情報を特定し、特定されたサービス及び前記サービスに対応付けられた前記操作情報を含むサービス一覧を生成する制御部と、前記サービス一覧を出力する出力部と、を備える、情報処理装置である。

【０１５１】

第2の特徴は、第1の特徴において、前記操作情報は、前記サービスにログインする情報、前記サービスに対してデータをアップロードする情報、前記サービスからデータをダウンロードする情報、前記サービスを利用するユーザが増加した情報、前記サービスを利用するユーザが減少した情報、前記サービスが共有アカウントを用いて複数のユーザによって利用されている旨を示す情報、及び、前記サービスが指定されたIPアドレス以外からアクセスされた旨を示す情報の少なくともいずれか1つを含む、情報処理装置である。

【０１５２】

第3の特徴は、第1の特徴又は第2の特徴において、前記制御部は、特定された前記サービスが有する特徴情報を特定し、前記制御部は、特定された前記特徴情報を含む前記サービス一覧を生成する、情報処理装置である。

【０１５３】

第4の特徴は、第3の特徴において、前記特徴情報をサービスと対応付けて記憶する記憶部を備え、前記制御部は、前記記憶部を参照して、前記特徴情報を特定する、情報処理装置である。

【０１５４】

第5の特徴は、第3の特徴又は第4の特徴において、前記特徴情報は、前記サービスがファイルのアップロードに対応する旨を示す情報、前記サービスがファイルのダウンロードに対応する旨を示す情報、前記サービスが仮想専用線に対応していない旨を示す情報、前記サービスが前記組織の外部に公開される旨を示す情報、前記サービスが他のサービスと連携する旨を示す情報、前記サービスがユーザ認証に対応していない旨を示す情報、及び、前記サービスがコミュニケーションツールである旨を示す情報の少なくともいずれか1つを含む、情報処理装置である。

【０１５５】

第6の特徴は、第1の特徴乃至第5の特徴の少なくともいずれか1つにおいて、前記組織で利用を制限する第1サービスの情報を記憶する記憶部を備え、前記制御部は、前記アクセス履歴に基づいて、前記第1サービスの利用を検知し、前記出力部は、前記第1サービスの利用が検知された旨の通知を出力する、情報処理装置である。

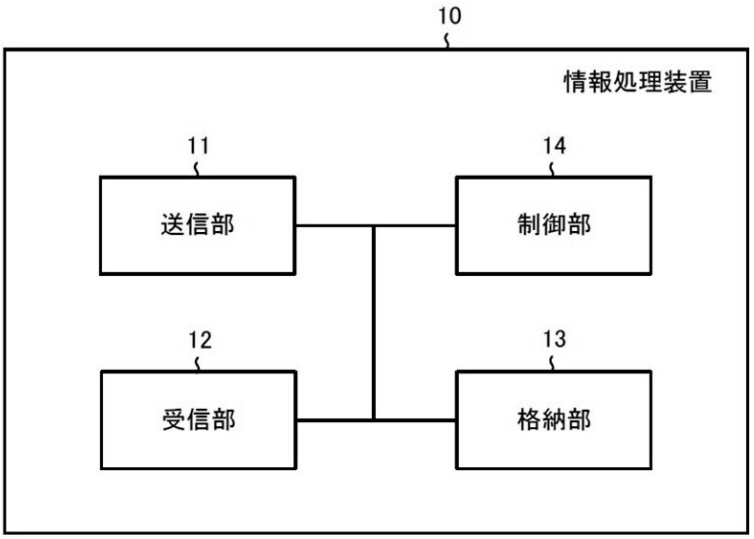
【０１５６】

第7の特徴は、第1の特徴乃至第6の特徴の少なくともいずれか1つにおいて、前記サービス一覧の対象から除外される第2サービスの情報を記憶する記憶部を備え、前記制御部は、前記アクセス履歴に基づいて、前記第2サービスの利用を検知しても、前記第2サービスを前記サービス一覧の対象から除外する、情報処理装置である。

【０１５７】
第8の特徴は、第1の特徴乃至第7の特徴の少なくともいずれか1つにおいて、前記制御部は、特定された前記サービスの中から、前記操作情報に基づいて、前記組織で対応が必要である第3サービスを特定し、特定された第3サービスが視覚的に強調された態様で前記サービス一覧を生成する、情報処理装置である。
【０１５８】
第9の特徴は、第1の特徴乃至第8の特徴の少なくともいずれか1つにおいて、前記制御部は、特定された前記サービスの中から、前記特徴情報に基づいて、前記組織で対応が必要である第3サービスを特定し、特定された第3サービスが視覚的に強調された態様で前記サービス一覧を生成する、情報処理装置である。
【０１５９】
第10の特徴は、第1の特徴乃至第9の特徴の少なくともいずれか1つにおいて、前記サービスに関するリスク評価情報を前記サービスと対応付けて記憶する記憶部を備え、前記制御部は、特定された前記サービスの中から、前記アクセス履歴に基づいて、前記リスク評価情報と対応付けられた第4サービスを特定し、特定された第4サービスについて前記リスク評価情報を含む態様で前記サービス一覧を生成する、情報処理装置である。
【０１６０】
第11の特徴は、第10の特徴において、前記リスク評価情報は、リスク評価に関する数値を含み、前記制御部は、前記リスク評価に関する数値が閾値よりも低い前記第4サービスを特定し、特定された第4サービスが視覚的に強調された態様で前記サービス一覧を生成する、情報処理装置である。
【０１６１】
第12の特徴は、第10の特徴又は第11の特徴において、前記リスク評価情報は、非公開情報に基づいた第1リスク評価情報と、公開情報に基づいた第2リスク評価情報と、を含む、情報処理装置である。
【０１６２】
第13の特徴は、組織に属するユーザが利用するサービスに対するアクセス履歴を取得するステップと、前記アクセス履歴に基づいて、前記ユーザが利用するサービスを特定するステップと、前記アクセス履歴に基づいて、特定された前記サービスに対する操作情報を特定するステップと、特定された前記サービス及び特定された前記操作情報を含む前記サービスの一覧を生成するステップと、前記サービスの一覧を出力するステップと、を備える、情報処理方法である。
【符号の説明】
【０１６３】
10…情報処理装置、11…送信部、12…受信部、13…格納部、14…制御部、20…端末、30…端末、100…情報処理システム、200…ネットワーク

【要約】
【課題】　組織のセキュリティが害されているか否かを容易に把握するための情報を提供することを可能とする情報処理装置及び情報処理方法を提供する。
【解決手段】　情報処理装置は、組織に属するユーザが利用するサービスに対するアクセス履歴を取得する取得部と、前記アクセス履歴に基づいて、前記ユーザが利用するサービスを特定し、前記アクセス履歴に基づいて、特定された前記サービスに対する操作情報を特定し、特定されたサービス及び前記サービスに対応付けられた前記操作情報を含むサービス一覧を生成する制御部と、前記サービス一覧を出力する出力部と、を備える。
【選択図】　図２

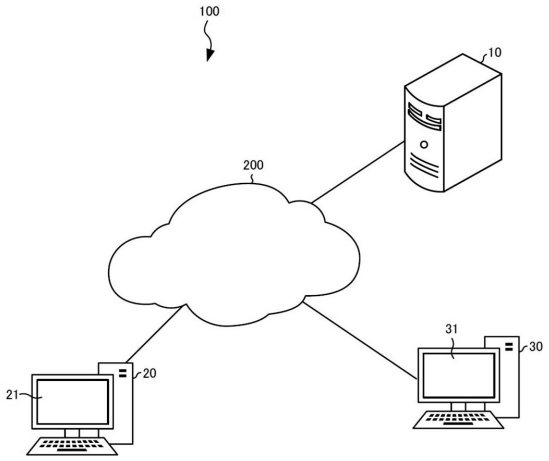
図2



【図面】

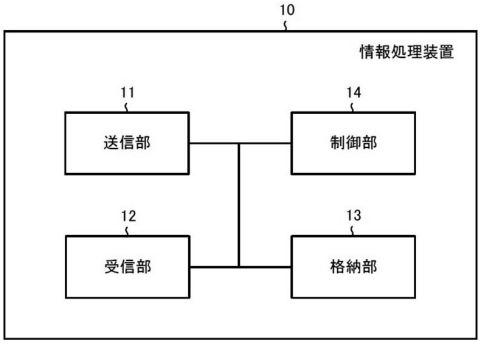
【図１】

図1



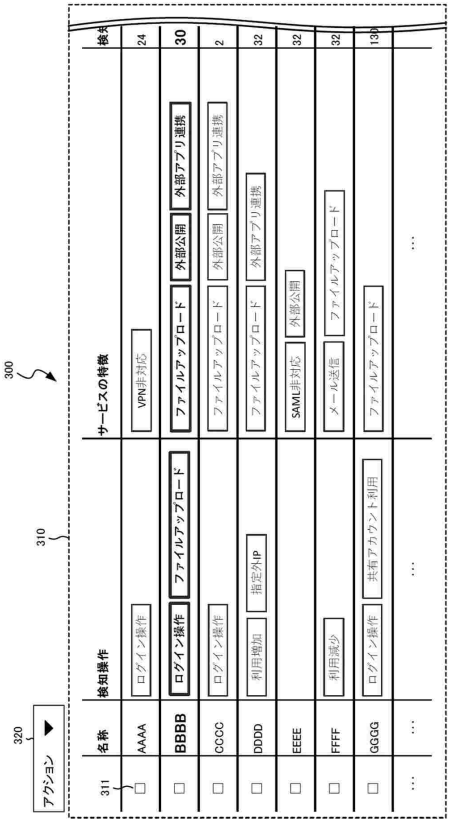
【図２】

図2



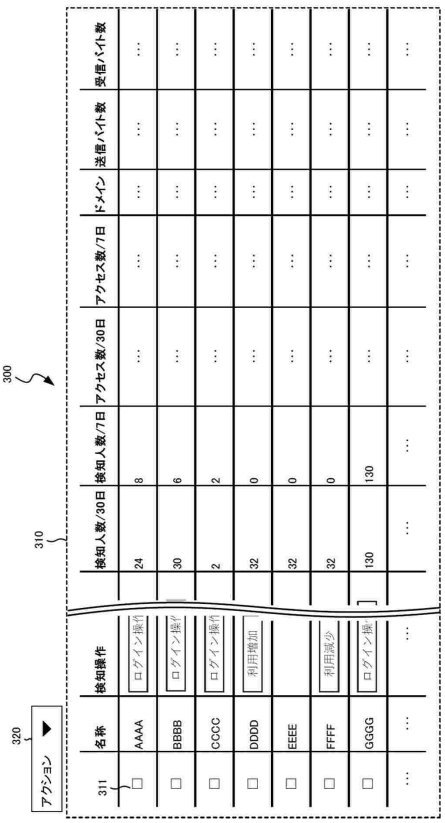
【図３】

図3

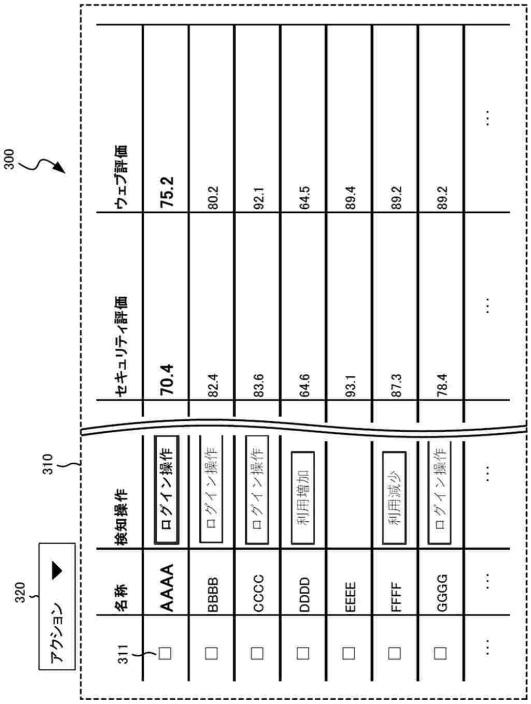


【図４】

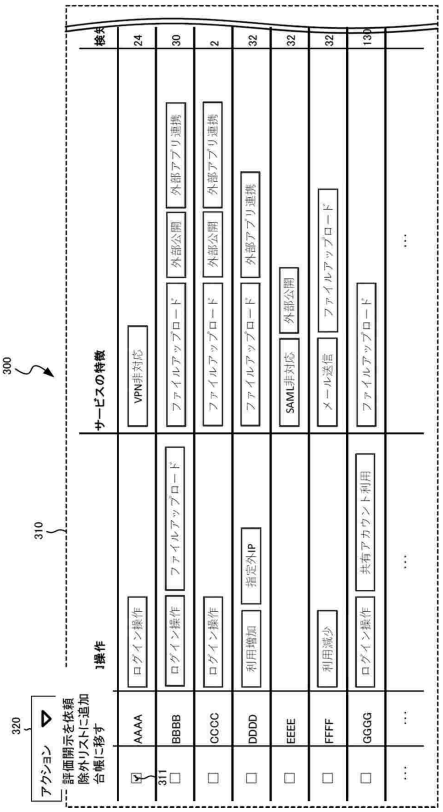
図4



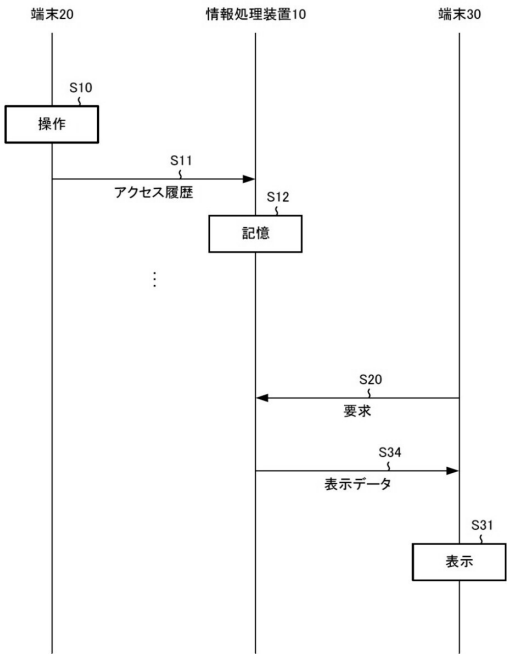
【図５】
図5



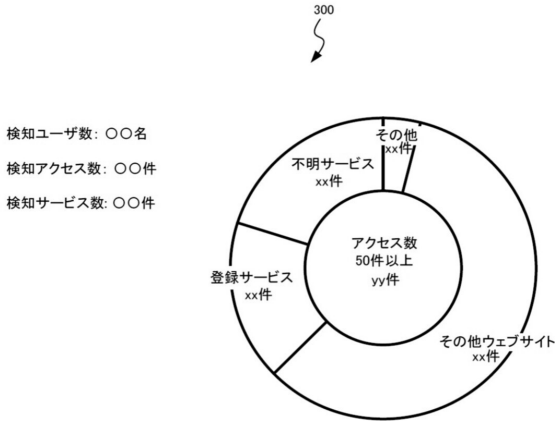
【図６】
図6



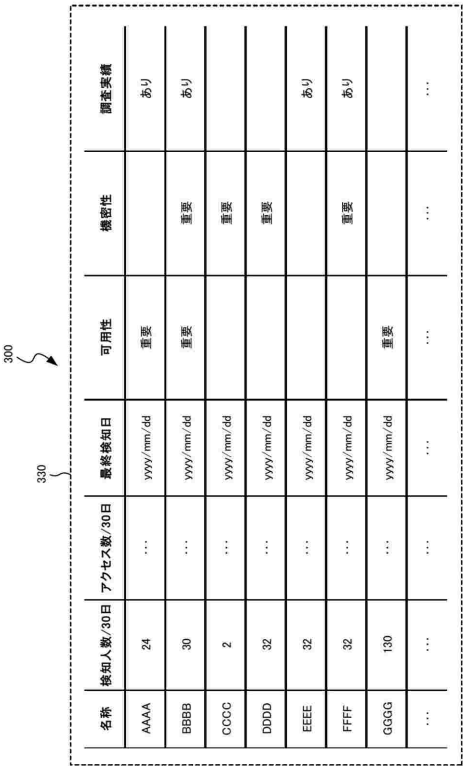
【図７】
図7



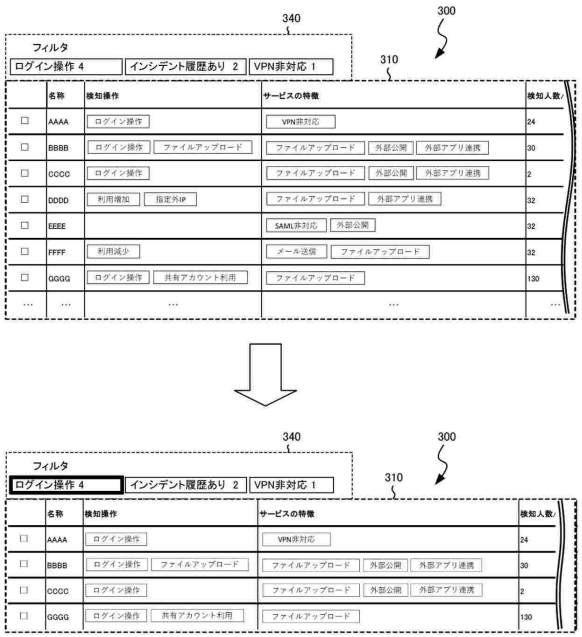
【図８】
図8



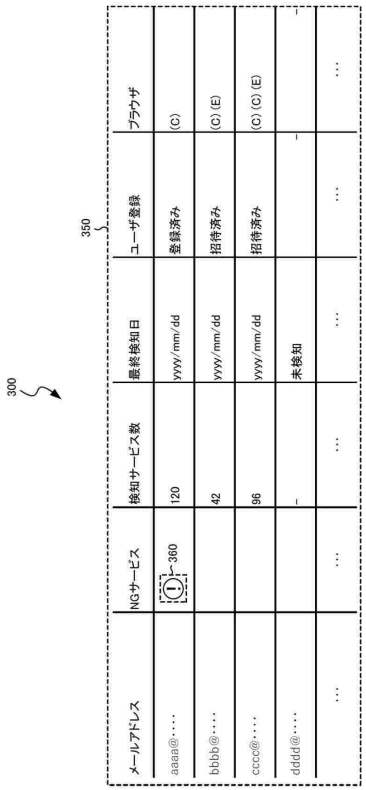
【図９】
図9



【図１０】
図10



【図１１】
図11



フロントページの続き

東京都渋谷区渋谷２－１５－１渋谷クロスタワー１２Ｆ　株式会社アシュアード内

審査官　久宗 義明

(56)参考文献

特開２０２２－０５０４６２（ＪＰ，Ａ）
特開２００９－２３７６５９（ＪＰ，Ａ）
特開２０１１－１８６９３３（ＪＰ，Ａ）
再公表特許第２０２０／２０４１４４（ＪＰ，Ａ１）
国際公開第２０１７／０３８２２１（WO，Ａ１）
特許第７３５７８１９（ＪＰ，Ｂ１）
特開２０１７－１０７３４８（ＪＰ，Ａ）
株式会社ディー・オー・エス，ＰＣ操作ログ，ＰＣ操作ログ－ログ管理｜ＩＴ資産管理ソフトＳＳ１の機能 [online]，日本，株式会社ディー・オー・エス，2022年08月13日，[令和6年2月6日検索], インターネット＜URL: https://web.archive.org/web/20220813204839/https://www.dos-osaka.co.jp/ss1/kinou/log/ss1_kinou_sousa.html＞

(58)調査した分野　(Int.Cl.，ＤＢ名)

Ｇ０６Ｑ　１０／００－９９／００
Ｇ０６Ｆ　２１／５７