(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-515214
(P2024-515214A)
(43)公表日　令和6年4月5日(2024.4.5)

(51)国際特許分類　FI
G06F 21/53 (2013.01)　G06F 21/53
G06F 21/55 (2013.01)　G06F 21/55
G06F 21/60 (2013.01)　G06F 21/60　360

審査請求　有　予備審査請求　有　（全36頁）

(21)出願番号　特願2023-565437(P2023-565437)
(86)(22)出願日　令和4年4月22日(2022.4.22)
(85)翻訳文提出日　令和5年12月15日(2023.12.15)
(86)国際出願番号　PCT/IL2022/050416
(87)国際公開番号　WO2022/224262
(87)国際公開日　令和4年10月27日(2022.10.27)
(31)優先権主張番号　63/177,998
(32)優先日　令和3年4月22日(2021.4.22)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,
最終頁に続く

(71)出願人　523400644
タロン サイバー セキュリティ リミテッド
イスラエル国 ６７１３８２７ テルアビブ デレク メナケム ベギン ８０ ２階
(74)代理人　100165157
弁理士　芝 哲央
(74)代理人　100205659
弁理士　齋藤 拓也
(74)代理人　100126000
弁理士　岩池 満
(74)代理人　100185269
弁理士　小菅 一弘
(72)発明者　ベン－ヌーン オフェル
イスラエル国 ６７８９０３６ テルアビ
最終頁に続く

(54)【発明の名称】　サイバーセキュリティシステム

(57)【要約】
通信ネットワークを介してアクセス可能なデジタルリソースのグループのデジタルリソースへのセキュアアクセスを提供するための通信システムであって、ＩＰ（インターネットプロトコル）アドレスを介してアクセス可能なデータ処理ハブと、前記通信ネットワークを介して通信するために使用可能な複数のユーザ機器（ＵＥ）であって、それぞれが、前記ＵＥ内のアンビエントソフトウェアから隔離され、セキュアウェブブラウザ（ＳＷＢ）を含むサイバーセキュア隔離環境（ＣＩＳＥ）を有するように構成される、ＵＥと、を含み、前記ハブ及びＣＩＳＥは、ＣＩＳＥの中で動作中及び静止中のデジタルリソースが前記ハブに可視であるように構成される、通信システム。
【選択図】図１

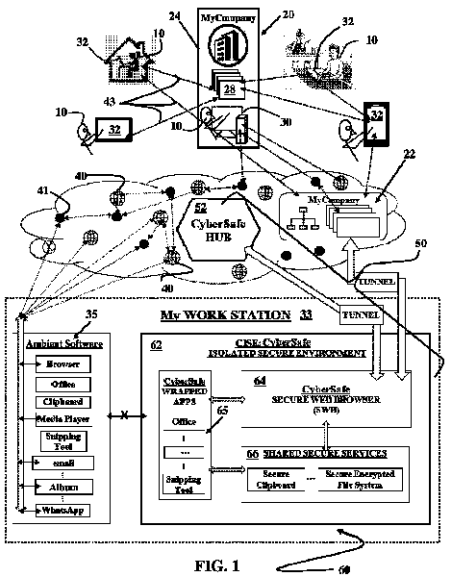


FIG. 1

【特許請求の範囲】
【請求項１】
通信ネットワークを介してアクセス可能なデジタルリソースのグループのデジタルリソースへのセキュアアクセスを提供するための通信システムであって、
ＩＰ（インターネットプロトコル）アドレスを介してアクセス可能なデータ処理ハブと、
前記通信ネットワークを介して通信するために使用可能な複数のユーザ機器（ＵＥ）であって、それぞれが、前記ＵＥ内のアンビエントソフトウェアから隔離され、セキュアウェブブラウザ（ＳＷＢ）を含むサイバーセキュア隔離環境（ＣＩＳＥ）を有するように構成される、ＵＥと、
を含み、
前記ハブ及びＣＩＳＥは、ＣＩＳＥの中で動作中及び静止中のデジタルリソースが前記ハブに可視であるように構成される、通信システム。
【請求項２】
前記セキュア環境は、前記システムのセキュリティポリシーによって定義されるセキュリティ制約に適合するようにラップされた少なくとも１つのソフトウェアアプリケーションを含む、請求項１に記載の通信システム。
【請求項３】
前記セキュア環境は、前記ＳＷＢによって使用可能な少なくとも１つのセキュアサービスアプリケーションと、前記少なくとも１つのラップされたアプリケーションと、を含む、請求項２に記載の通信システム。
【請求項４】
前記少なくとも１つのセキュアサービスアプリケーションは、セキュアクリップボードと、セキュア暗号化ファイルシステムと、を含む、請求項３に記載の通信システム。
【請求項５】
前記ＣＩＳＥ内のアプリケーション間の通信は、セキュア暗号化通信チャネルを介する、請求項２～４のいずれか一項に記載の通信システム。
【請求項６】
前記ＳＷＢと前記ＣＩＳＥ内のアプリケーションとの間の通信は、セキュア暗号化通信チャネルを介する、請求項２～５のいずれか一項に記載の通信システム。
【請求項７】
前記ＳＷＢから送信される通信は、前記ＳＷＢが前記通信を暗号化する前に、前記ハブに可視である、請求項１～６のいずれか一項に記載の通信システム。
【請求項８】
前記ＳＷＢに入る通信は、前記ＳＷＢが前記通信を復号した後に、前記ハブに可視である、請求項１～７のいずれか一項に記載の通信システム。
【請求項９】
ＵＥ内の前記ＳＷＢは、前記ＵＥのユーザの通信を監視して、前記ユーザ及び前記ユーザが訪問するウェブサイトの閲覧挙動を特徴付けるデータを取得する、請求項１～８のいずれか一項に記載の通信システム。
【請求項１０】
前記ハブ及び／又は前記ＳＷＢは、取得した前記データを処理して、前記ユーザがアクセスするウェブサイトとの前記ユーザの対話の通常パターンを決定する、請求項９に記載の通信システム。
【請求項１１】
前記ハブ及び／又は前記ＳＷＢは、取得した前記データを処理して、前記ユーザが前記ウェブサイトにアクセスすることに起因するリソースの前記グループのデジタルリソースに対するサイバー損傷のリスクを決定する、請求項１０に記載の通信システム。
【請求項１２】
前記ハブ及び／又は前記ＳＷＢは、決定された前記リスクに応答してグループリソース

を保護するためのウェブ閲覧セキュリティポリシーを構成する、請求項１１に記載の通信システム。
【請求項１３】
前記ＳＷＢは、前記ＳＷＢと前記ＳＷＢによってアクセスされるウェブサイトとの間の通信を監視して、前記ウェブ閲覧セキュリティポリシーを施行する、請求項１２に記載の通信システム。
【請求項１４】
前記閲覧セキュリティポリシーを施行することは、前記ＳＷＢを使用して前記ユーザの閲覧挙動を監視して、決定された通常閲覧挙動に応答して前記挙動における異常を識別することを含む、請求項１２に記載の通信システム。
【請求項１５】
前記異常は、決定された前記通常挙動及び／又は前記ポリシーの侵害を含む、請求項１４に記載の通信システム。
【請求項１６】
異常を識別することに応答して、前記ＳＷＢ及び／又は前記ハブは、前記侵害に起因するサイバー損傷の可能性を改善するアクションを行う、請求項１４又は１５に記載の通信システム。
【請求項１７】
異常を識別することに応答して、前記ＳＷＢ及び／又は前記ハブは、前記ハブの発生に対するアラートを生成する、請求項１４～１６のいずれか一項に記載の通信システム。
【請求項１８】
ＵＥ内の前記ＳＷＢは、前記ＵＥのユーザの通信を監視して、前記ユーザが使用するクラウドコンピューティングアズアサービス（ＣＣａａＳ）リソース及びＣＣａａＳリソースのユーザ使用を特徴付けるデータを取得するように構成される、請求項１～１７のいずれか一項に記載の通信システム。
【請求項１９】
前記ＳＷＢ及び／又は前記ハブは、取得した前記データを処理して、前記ユーザがアクセスするＣＣａａＳリソースのユーザ使用の通常パターンを決定する、請求項１８に記載の通信システム。
【請求項２０】
前記ＳＷＢ及び／又は前記ハブは、取得した前記データを処理して、前記ユーザが前記ＣＣａａＳリソースにアクセス及び／又は使用することから生じるリソースの前記グループのデジタルリソースに対するサイバー損傷のリスクを決定する、請求項１９に記載の通信システム。
【請求項２１】
前記ＳＷＢ及び／又は前記ハブは、前記ＣＣａａＳリソースにアクセス及び／又は使用するために決定されたリスクに応答して前記グループリソースを保護するためのＣＣａａＳセキュリティポリシーを構成する、請求項２０に記載の通信システム。
【請求項２２】
前記ＳＷＢは、前記ＳＷＢと前記ＳＷＢによってアクセスされるＣＣａａＳリソースとの間の通信を監視して、前記ＣＣａａＳセキュリティポリシーを施行する、請求項２１に記載の通信システム。
【請求項２３】
前記ＣＣａａＳセキュリティポリシーを施行することは、前記ＳＷＢを使用する前記ユーザによるＣＣａａＳリソースの使用を監視して、ＣＣａａＳのユーザ使用の決定された前記通常パターンに応答して前記使用における異常を識別することを含む、請求項２２に記載の通信システム。
【請求項２４】
前記異常は、決定された前記通常挙動及び／又は前記ポリシーの侵害を含む、請求項２３に記載の通信システム。

【請求項２５】
異常を識別することに応答して、前記ＳＷＢ及び／又は前記ハブは、前記侵害に起因するサイバー損傷の可能性を改善するアクションを行う、請求項２３又は２４に記載の通信システム。
【請求項２６】
異常を識別することに応答して、前記ＳＷＢ及び／又は前記ハブは、前記ハブの発生に対するアラートを生成する、請求項２３～２５のいずれか一項に記載の通信システム。
【請求項２７】
前記ＳＷＢがリソースの前記グループのリソースへのアクセスを要求するように動作する前に、前記ハブは、前記ＳＷＢが含むソフトウェアを調べるように動作する、請求項１～２６のいずれか一項に記載の通信システム。
【請求項２８】
ソフトウェアを調べることは、前記ＳＷＢを識別するブラウザＩＤ、Ｂ－ＩＤ、前記ＳＷＢを含む前記ＵＥを識別するユーザ機器ＩＤ、ＵＥ－ＩＤ、及び前記ＳＷＢを操作するユーザを識別するユーザＩＤ、Ｕ－ＩＤを含む拡張ＩＤを認証することを含む、請求項２７に記載の通信システム。
【請求項２９】
前記ソフトウェアを調べることは、前記ソフトウェアのソフトウェア完全性試験を実行することを含む、請求項２７又は請求項２８に記載の通信システム。
【請求項３０】
前記ソフトウェア完全性試験を実行することは、前記ハブが含むメモリ又はアクセスを有するメモリから完全性試験のセットを取り出すことを含む、請求項２９に記載の通信システム。
【請求項３１】
完全性試験の前記セットは、チャレンジ応答試験（ＣＲＴ）、挙動証明試験（ＢＡＴ）、抗ウイルスチェック（ＡＶ）、エンドポイント検出及び応答（ＥＤＲ）、又はバイナリデジタル署名（ＢＤＳ）チェックのうちの少なくとも１つ、又は２つ以上の任意の組み合わせを含む、請求項３０に記載の通信システム。
【請求項３２】
前記完全性試験を実行することは、前記セット内の試験を重み付けすることと、前記重み付けに応答して実行する少なくとも１つの試験を選択することと、を含む、請求項３１に記載の通信システム。
【請求項３３】
前記少なくとも１つの選択された完全性試験によって返された完全性の尺度に応答して、前記ソフトウェアの完全性の質（ＱｏＩ）を決定することを含む、請求項３２に記載の通信システム。
【請求項３４】
前記ＱｏＩ基準に基づいて、前記ＱｏＩが満足できるものであるか否かを決定することを含む、請求項３３に記載の通信システム。
【請求項３５】
前記ＱｏＩが許容できない場合、前記ＳＷＢ内のソフトウェアを修正するか否かを決定することを含む、請求項３４に記載の通信システム。
【請求項３６】
前記ＳＷＢがリソースの前記グループのリソースへのアクセスを要求するように動作する前に、前記ハブは、前記ＵＥが含むアンビエントソフトウェアを調べるように動作する、請求項１～３５のいずれか一項に記載の通信システム。
【請求項３７】
前記アンビエントＵＥソフトウェアのソフトウェア完全性試験を実行することを含む、請求項３６に記載の通信システム。
【請求項３８】

前記アンビエントソフトウェアの完全性の質（ＱｏＩ）を決定することを含む、請求項３７に記載の通信システム。
【請求項３９】
アンビエントソフトウェアの前記ＱｏＩが満足できるものであるか否かをＱｏＩ基準に基づいて決定することを含む、請求項３８に記載の通信システム。
【請求項４０】
前記アンビエントソフトウェアのＱｏＩが満足できない場合、前記ＳＷＢ内のソフトウェアを修正するか否かを決定することを含む、請求項３４に記載の通信システム。
【請求項４１】
前記ＵＥソフトウェアにおけるサイバー攻撃脆弱性特徴の存在を検出することと、前記脆弱性特徴に対するサイバー攻撃リスク推定値を決定することと、を含む、請求項３６～４０のいずれか一項に記載の通信システム。
【請求項４２】
前記アンビエントサイバー攻撃リスク推定値を処理して、ＣＩＳＥ及び／又はＳＷＢに含まれ、ＳＷＢ及び／又はリソースの前記グループ内のリソースをサイバー損傷から保護するソフトウェアが、前記脆弱性特徴と関連付けられる起こり得るサイバー損傷に対する許容可能な程度の保護を提供するかどうかを決定することを含む、請求項４１に記載の通信システム。
【請求項４３】
前記アンビエントソフトウェアのリスクにさらされたコンポーネントを検出することと、リスクにさらされた前記コンポーネントのサイバー攻撃リスク推定値を決定することと、を含む、請求項３６～４２のいずれか一項に記載の通信システム。
【請求項４４】
前記アンビエントソフトウェアリスク推定値を処理して、ＣＩＳＥ及び／又はＳＷＢに含まれ、ＳＷＢ及び／又はリソースの前記グループ内のリソースをサイバー損傷から保護するソフトウェアが、リスクにさらされた前記コンポーネントに関連する起こり得るサイバー損傷に対する許容可能な程度の保護を提供するかどうかを決定することを含む、請求項４３に記載の通信システム。
【請求項４５】
前記システム及び／又はリソースの前記グループのリソースをサイバー損傷にさらす前記ユーザの挙動特徴を特徴付けるユーザリスクコンポーネントを含む前記ユーザのためのプロファイルを取り出すことを含む、請求項３６～４４のいずれか一項に記載の通信システム。
【請求項４６】
前記リスクコンポーネントを処理して、ＣＩＳＥ及び／又はＳＷＢに含まれ、ＳＷＢ及び／又はリソースの前記グループ内のリソースをサイバー損傷から保護するソフトウェアが、前記ユーザリスクコンポーネントと関連付けられる起こり得るサイバー損傷に対する許容可能な程度の保護を提供するかどうかを決定することを含む、請求項４５に記載の通信システム。
【請求項４７】
ＣＩＳＥ及び／又はＳＷＢに含まれ、ＳＷＢ及び／又はリソースの前記グループ内のリソースをサイバー損傷から保護するソフトウェアが、許容可能な程度の保護を提供する場合、前記ＳＷＢを修正するか否かを決定することを含む、請求項４２、４４、及び４６のいずれか一項に記載の通信システム。
【請求項４８】
前記ＱｏＩが許容できない場合、前記ＳＷＢ内のソフトウェアを修正するか否かを決定することを含む、請求項４７に記載の通信システム。
【請求項４９】
前記ハブ、ＳＷＢ、及びＩＤＰは、リソースの前記グループのリソースへの前記ＳＷＢのアクセスを許可する際に協働するように構成される、請求項１～４８のいずれか一項に

記載の通信システム。
【請求項５０】
前記ハブ、ＳＷＢ、及びＩＤＰを構成することは、
前記ＳＷＢが前記リソースに提出するアクセスの要求に対して前記ハブをコピーするように前記ＳＷＢを構成することと、
前記ユーザアイデンティティを認証し、前記ハブが、前記ＳＷＢが前記リソースに提出したアクセスの前記要求のコピーを受信したかどうかについて前記ハブに問い合わせるように、前記ＩＤＰを構成することと、
前記ユーザアイデンティティが認証され、前記ハブがアクセスの前記要求のコピーの受信を肯定応答する場合、アクセスを許可するように前記ＩＤＰを構成することと、
を含む、請求項４９に記載の通信システム。
【請求項５１】
前記ハブ、ＳＷＢ、及びＩＤＰを構成することは、
前記ハブに、ＩＰアドレスを有するプロキシと、前記プロキシへのアクセスを保護する認証ファクタとを提供することと、
前記リソースへのアクセス要求を、前記要求が前記プロキシサーバの前記ＩＰアドレスから受信された場合にのみ、許可するように前記ＩＤＰを構成することと、
前記ウェブブラウザを、前記プロキシの前記ＩＰアドレス及び認証ファクタを前記ハブから要求して、受信するように、また前記プロキシＩＰアドレス及び認証ファクタを使用して前記プロキシにアクセスし、前記プロキシを介して前記リソースへのアクセスの要求を提出するように、構成することと、
を含む、請求項４９に記載の通信システム。
【請求項５２】
前記認証ファクタは、パスワードを含む、請求項５１に記載の通信システム。
【請求項５３】
前記ＳＷＢは、前記ＵＥを使用するユーザの閲覧アクティビティを監視し、前記閲覧アクティビティに対して前記システムの閲覧セキュリティポリシー及び／又はデジタルリソースの前記グループに関連する閲覧セキュリティポリシーを施行するように構成される、請求項１～５２のいずれか一項に記載の通信システム。
【請求項５４】
前記ＳＷＢは、サービスリソースとしてのクラウドコンピューティング（ＣＣａａＳ）と対話するために前記ＵＥを使用するユーザのアクティビティを監視し、前記システムのＣＣａａＳセキュリティポリシー及び／又は通信上のデジタルリソースの前記グループに関連するＣＣａａＳセキュリティポリシーを施行するように構成される、請求項１～５３のいずれか一項に記載の通信システム。
【請求項５５】
ＩＰアドレスを有する保護されたデジタルリソースへのアクセスを許可するための装置であって、前記装置は、
前記リソースの前記ＩＰアドレスにアクセスし、ユーザのためにリソースへのアクセスの要求を提出するように、前記ユーザによって動作可能なウェブブラウザと、
前記ウェブブラウザと通信し、前記ユーザが前記ブラウザを使用して前記リソースにアクセスするために行う要求の前記ブラウザによる通知を受信するように構成された信頼可能なセキュリティハブと、
前記リソースのユーザアイデンティティを検証するアイデンティティプロバイダ（ＩＤＰ）と、
を含み、
前記ブラウザによって提出された前記リソースへのアクセスの要求は、前記ＩＤＰが前記ユーザのＩＤを認証し、前記信頼可能なセキュリティハブが前記ブラウザから前記要求の通知を受信したという検証を前記信頼可能なセキュリティハブから受信する場合、許可される、装置。

【請求項５６】
ＩＰアドレスを有する保護されたデジタルリソースへのアクセスを許可するための方法であって、
前記ＩＰアドレスに、前記リソースへのユーザアクセスの要求を提出するステップと、
前記要求を信頼可能なセキュリティハブにコピーするステップと、
前記ＩＤＰがユーザアイデンティティを検証し、前記信頼可能なセキュリティハブが前記要求上にコピーされたことを確認する場合、前記要求を許可するステップと、
を含む、方法。
【請求項５７】
ＩＰアドレスを有する保護されたデジタルリソースへのアクセスを許可するための装置であって、前記装置は、
認証ファクタで保護され、ＩＰアドレスを有するプロキシサーバと、
前記プロキシサーバＩＰアドレス及び認証ファクタを有する信頼可能なセキュリティハブと、
アクセス要求を、前記要求が前記プロキシサーバの前記ＩＰアドレスから受信された場合にのみ、許可するように構成されたアイデンティティプロバイダ（ＩＤＰ）と、
ウェブブラウザであって、ユーザによって、
前記信頼可能なセキュリティハブから、前記プロキシの前記ＩＰアドレス及び認証ファクタを要求及び受信することと、
前記プロキシＩＰアドレス及び認証ファクタを使用して前記プロキシにアクセスし、前記プロキシを介して前記リソースへのアクセスの要求を提出することと、
を行うように、動作可能なウェブブラウザと、
を含む、装置。
【請求項５８】
保護されたデジタルリソースへのアクセスを許可する方法であって、
前記リソースにアクセスするための要求を、所定のＩＰアドレスから前記要求が受信された場合にのみ、許可するようにＩＤＰを構成するステップと、
ブラウザから前記リソースへのユーザアクセスの要求を受信するステップと、
前記ブラウザに前記ＩＰアドレス及び前記ＩＰアドレスを有するプロキシの認証ファクタを提供するステップと、
前記プロキシＩＰアドレス及び認証ファクタを使用して前記ブラウザに応答するアクセスの要求を許可して、前記プロキシを介して前記要求を提出するステップと、
を含む、方法。
【請求項５９】
前記認証ファクタは、パスワードを含む、請求項５６又は５８に記載の方法。
【請求項６０】
前記認証ファクタは、パスワードを含む、請求項５５又は５７に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願）
本出願は、米国特許法第１１９条（ｅ）の下で、２０２１年４月２２日に出願された米国仮出願第６３／１７７，９９８号の利益を主張し、その開示は、参照により本明細書に組み込まれる。
【０００２】
本開示の実施形態は、通信ネットワーク及びデジタルリソースのためのサイバーセキュアアクセスチャネル及びワークスペースを提供することに関する。
【背景技術】
【０００３】
現代の通信ネットワーク及びインターネットを提供する様々なコンピュータ及び通信技

術は、通信ネットワークと、そのネットワークへのアクセスを提供する固定及び／又はモバイルユーザ機器（ＵＥ）の動作をサポートする多種多様な仮想及びベアメタルネットワーク要素（ＮＥ）を包含する。これらの技術は、今日の社会の基盤である情報技術（ＩＴ）及びオペレーション技術（ＯＴ）を可能にし、産業機器の制御、ビジネスオペレーションのサポート、並びにインターネットを介したデータ、音声、及びビデオコンテンツの生成及び伝搬のための多数の方法、デバイス、インフラストラクチャ、及びプロトコルを提供する。世界中のほとんどの人々は、あらゆる種類の情報を、物理的位置とは無関係に、インターネットを通じて、容易に入手することができる。今日、グローバルなコミュニティの大部分は自分のパーソナル、Ｂｒｉｎｇ Ｙｏｕｒ Ｏｗｎ Ｄｅｖｉｃｅ（ＢＹＯＤ）、ＵＥ、例えば、自分のパーソナルスマートフォン、ラップトップ、タブレット、及びホームデスクトップ等を使用して、自分の雇用者及び職場グループへの接続性を介して、自分の家庭、コーヒーショップ、及び休暇の場から定期的に遠隔で働いている。ネットワークは、情報の消費を脱階層化し、社会的インフラストラクチャの変化を加速してきた。

【０００４】

しかしながら、コンピュータ及び通信技術によって提供される利益には、そのコストが伴わないわけではない。同じ技術及び利益は、機密性に対する正当な個人及び集団の権利を提供して、維持することと、サイバー攻撃による妨害及び損害に対して技術が可能にした同一の産業及びビジネス運営の完全性及び安全性を保護することの難しさが大幅に増加している。

【０００５】

例えば、サイバー攻撃表面のフィンガープリントは、個人の空間的に繋がれていないＢＹＯＤであっても、企業の職場ユーザ機器（ＷＰＵＥ）であっても、各ＵＥを特徴付け、おそらくＵＥ上で、より頻繁にＵＥが接続するエンティティ及びシステム上で、悪意のあるハッカーによる悪用の脆弱性を提供し、大混乱をもたす。各ＵＥ、特にＢＹＯＤは、人の通信ノードとして機能することに加えて、ＵＥが接続する任意の通信ネットワークのための潜在的なサイバー攻撃ノードである。個人ＢＹＯＤを使用して遠隔作業に少なくとも部分的に移行したクライアント、ワーカ、及び／又はアソシエイトと連絡しなければならない企業の場合、サイバー攻撃に対する脆弱性は、多数のそれらの遠隔連絡先、連絡先のそれぞれのＢＹＯＤ内のソフトウェア構成、及び連絡先がＵＥを使用して関与する非企業通信の多様性によって増幅される。企業データ及び記憶リソースのクラウドに傾倒し、遠隔コンタクトがアクセス及び使用するインフラストラクチャ・アズ・ア・サービス（ＩａａＳ）、プラットフォーム・アズ・ア・サービス（ＰａａＳ）、及びソフトウェア・アズ・ア・サービス（ＳａａＳ）等の技術が普及したことでは、適切なサイバー保護を提供することが、ますます複雑になっている。

【発明の概要】

【０００６】

本開示の実施形態の態様は、以下では「ＣｙｂｅｒＳａｆｅ」とも呼ばれるサイバーセキュア通信システムを提供することに関し、サイバーセキュア通信システムは、システムによって伝搬される通信トラフィックに対する可視性の向上を提供し、リソースの本体のデジタルリソースに対するサイバー保護を提供し、リソースの本体に関連付けられたＵＥ（ＢＯＹＤ又はＷＰＵＥ）の認可されたユーザに対して、リソースの本体のデジタルリソースへのアクセスをセキュアにするように動作する。

【０００７】

提示の便宜上、デジタルリソースの本体は、任意選択で「ＭｙＣｏｍｐａｎｙ」と呼ばれる企業によって所有され、企業は、リソースの本体に関連付けられたＵＥを使用してＭｙＣｏｍｐａｎｙリソースにアクセスすることを認可されたユーザを採用するか、又はユーザとタスクに従事すると仮定する。リソースの本体に関連付けられたＵＥは、認可されたユーザがＭｙＣｏｍｐａｎｙリソースにアクセスすることを可能にするように、本開示の実施形態に従って構成されたＵＥである。リソースの本体に関連付けられたＵＥは、Ｍ

ｙＣｏｍｐａｎｙ　ＵＥと呼ばれることがあり、ＭｙＣｏｍｐａｎｙリソースにアクセスするためにＭｙＣｏｍｐａｎｙ　ＵＥを使用することを認可されたユーザは、ＭｙＣｏｍｐａｎｙユーザ又は単にユーザと呼ばれることがある。

【０００８】

デジタルリソースは、静止中又は動作中のデジタルフォーマットの任意の情報を含み、例として、実行可能なコード及び／又はデータを指す電子文書、画像、ファイル、データ、データベース、及び／又はソフトウェアを含む。デジタルリソースは、デジタルリソース上で動作し、又はデジタルリソースを生成するために使用され得る、任意のソフトウェア及び／又はハードウェアも含む。動作中のデジタルリソースは、通信システムのノード間で使用中、及び／又は動作中、及び／又は移動中のデジタルリソースである。静止中のデジタルリソースは、ストレージ内にあり、動作していないデジタルリソースである。

【０００９】

一実施形態では、ＣｙｂｅｒＳａｆｅは、ＣｙｂｅｒＳａｆｅハブとも称され、任意選択でクラウドベースのデータ及び処理セキュリティハブと、ＣｙｂｅｒＳａｆｅによって、又はそれに従って構成される、ＭｙＣｏｍｐａｎｙ　ＵＥのＣｙｂｅｒＳａｆｅ分離セキュア環境（ＣＩＳＥ）に常駐する、ＣｙｂｅｒＳａｆｅセキュアウェブブラウザ（ＳＷＢ）とも称される、ウェブブラウザとを備える。一実施形態では、ＣＩＳＥは、ＳＷＢ内及びＣＩＳＥ内に常駐し得る他のアプリケーション内に含まれるソフトウェア（コード及び／又はデータ）を、ＵＥアンビエントソフトウェアとも呼ばれ、ＭｙＣｏｍｐａｎｙリソースに関連付けられていないタスクのために使用され得るＵＥ内のソフトウェアから、及びＵＥの外部のソフトウェアから隔離するように動作する。一実施形態では、ＣＩＳＥへの、及びＣＩＳＥからの、またＣＩＳＥにおけるアプリケーション間の、それぞれデータの進入及び退出は、ＣＩＳＥ内への、及びＣＩＳＥから／へのデータのアクセス及び移動に関連する、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙセキュリティポリシーを施行するようにＣｙｂｅｒＳａｆｅによって構成される、ＳＷＢによって監視及び制御される。データの移動及びデータへのアクセスの分離及び制御、並びにポリシーの施行は、サイバー損傷に対する強化された保護、及びＭｙＣｏｍｐａｎｙ　ＵＥとの通信及びＭｙＣｏｍｐａｎｙ　ＵＥを介した通信から生じ得るＭｙＣｏｍｐａｎｙリソースからの及び／又はＭｙＣｏｍｐａｎｙリソースへのデータの漏出に対するセキュリティを提供するように動作する。

【００１０】

一実施形態では、データの進入及び退出を監視することは、ＳＷＢによってサポートされる通信を監視することと、監視された通信に含まれるデータを記憶及び処理することと、データをＣｙｂｅｒＳａｆｅハブ及びＭｙＣｏｍｐａｎｙ　ＩＴに利用可能にすることとを含む。一実施形態では、監視は、発信通信がＳＷＢによって暗号化される前にＣＩＳＥ及びＳＷＢから発信する通信に対して、及び着信通信がＳＷＢによって復号された後にＣＩＳＥに着信する通信に対して実行される。さらに、ＳＷＢとのユーザ対話は、ローカルに、又はＣｙｂｅｒＳａｆｅセキュリティハブによって監視されてもよい。その結果、ＵＥとＭｙＣｏｍｐａｎｙとの間の通信及びＵＥと対話するＭｙＣｏｍｐａｎｙユーザのアクションは、ＣｙｂｅｒＳａｆｅ及びＭｙＣｏｍｐａｎｙに実質的に完全に可視であり、ＳＷＢ、ハブ、及び／又はＭｙＣｏｍｐａｎｙと関連付けられる他の信頼可能なコンポーネントによって処理されてもよい。

【００１１】

本開示の実施形態によれば、ＳＷＢは、ＭｙＣｏｍｐａｎｙユーザによってＭｙＣｏｍｐａｎｙ　ＵＥから起動されると、ＣｙｂｅｒＳａｆｅセキュリティハブから、ＵＥから実行する許可を要求するように構成され、ＳＷＢをサイバー損傷から保護するように動作する、アンチインジェクション及び／又はアンチエクスプロイテーションソフトウェア等の、任意選択でクラッディングと呼ばれるソフトウェアを備える。許可の要求を受信すると、ＣｙｂｅｒＳａｆｅハブは、任意選択で、ＵＥユーザのＩＤをチェックし、ウェブブラウザソフトウェアの完全性及びＵＥのセキュリティ姿勢を調べる。ユーザＩＤが許容可

能であり、ソフトウェア完全性及び／又はクラッディングが無傷であること、及び／又はＵＥ環境のセキュリティ姿勢が満足できることが分かった場合、セキュリティハブは、ＵＥからのＳＷＢの動作を許可し、任意選択で、ＭｙＣｏｍｐａｎｙリソースにアクセスするための提示のためのセキュリティトークンをＳＷＢに発行してもよい。

【００１２】

一実施形態では、ＣｙｂｅｒＳａｆｅセキュリティハブであって、ＣｙｂｅｒＳａｆｅ　ＳＷＢと、ＭｙＣｏｍｐａｎｙのデジタルリソースへのアクセスを制御するように動作するアイデンティティプロバイダ（ＩＤＰ）とは、ＭｙＣｏｍｐａｎｙのデジタルリソースのリソースへのアクセスをＭｙＣｏｍｐａｎｙ　ＵＥの認可されたユーザに許可する際に協働するように構成される。ＣｙｂｅｒＳａｆｅは、ＭｙＣｏｍｐａｎｙリソースにアクセスするためにＣｙｂｅｒＳａｆｅ　ＳＷＢを使用するようにＭｙＣｏｍｐａｎｙユーザを制約するように動作してもよい。

【００１３】

一実施形態では、ＣｙｂｅｒＳａｆｅは、ＭｙＣｏｍｐａｎｙ　ＵＥのＭｙＣｏｍｐａｎｙユーザによってアクセスされるウェブサイト及びＭｙＣｏｍｐａｎｙユーザの閲覧挙動を特徴付けるデータを取得し、データをＣｙｂｅｒＳａｆｅハブにアップロードするようにＳＷＢを構成する。ＣｙｂｅｒＳａｆｅハブ及び／又はＳＷＢは、データを処理して、ウェブサイトへのアクセス及び／又はリソースをサイバー攻撃にさらし得るユーザ閲覧挙動から生じるＭｙＣｏｍｐａｎｙリソースへの損傷（以下、サイバー損傷とも呼ばれる）のリスクを推定する。ハブ及び／又はＳＷＢは、サイバー損傷のリスクを緩和するためにサイバー損傷リスク推定値に応答してＳＷＢ及び／又はＵＥを構成することができる。ＳＷＢを中程度のリスクに構成することは、ウェブサイトへのアクセスを制限又は防止するように、及び／又はウェブサイト、ＳＷＢ、ＵＥ、及び／又はユーザ閲覧挙動の機能性、及び／又はＳＷＢもしくはＣＩＳＥと他のアプリケーションとの間でデータを転送するための許可を制限するようにＳＷＢを構成することを含み得る。ＵＥを中程度のリスクに構成することは、パスワード、パッチング、ファイアウォール、ウェブサイト許可を更新すること、及び／又はリモートアクセスを無効にすることをＵＥのユーザに要求することを含み得る。

【００１４】

一実施形態では、ＣｙｂｅｒＳａｆｅは、ブラウザ拡張機能及び／又はブラウザ拡張機能の使用に対するユーザ閲覧挙動を特徴付けるデータを取得し、データを処理して、ブラウザ拡張機能をダウンロードし、ＳＷＢを修正してブラウザ拡張機能によって提供される機能性をＳＷＢに追加することに起因するＭｙＣｏｍｐａｎｙリソースのサイバーセキュリティに対するリスクを推定する。ＣｙｂｅｒＳａｆｅは、ブラウザ拡張機能によってもたらされるリスクを緩和するようにＳＷＢ及び／又はブラウザ拡張機能を構成した後に、ブラウザ拡張機能をＳＷＢと統合することを可能にし得る。

【００１５】

本開示の一実施形態によると、ＣｙｂｅｒＳａｆｅは、ＣｙｂｅｒＳａｆｅ　ＳＷＢを使用して、ＭｙＣｏｍｐａｎｙユーザによるＭｙＣｏｍｐａｎｙ　ＣＣａａＳ（サービスとしてのクラウドコンピューティング）リソースの使用を特徴付けるデータを監視及び取得し、データを処理し、ユーザによって証明されるサービスの通常使用パターンを決定する。ＣｙｂｅｒＳａｆｅは、ＭｙＣｏｍｐａｎｙユーザによって関与するＣＣａａＳセッションを監視し、セッション中に示されている通常使用パターン使用異常に応答して識別するように、ＣｙｂｅｒＳａｆｅ　ＳＷＢを構成することができる。ＣＣａａＳセッションにおける使用異常の識別に応答すると、ＳＷＢは、セッション中にリアルタイムでＣＣａａＳリソースの使用を制約し得る。使用を制約することは、ＣＣａａＳとユーザとの間のリアルタイムデータ転送を防止すること、及び／又はセッションをキャンセルすることを含んでもよい。異常を識別すると、ＳＷＢはアラートを生成し、分析のために異常に関連するデータをハブにアップロードすることができる。一実施形態では、ＣｙｂｅｒＳａｆｅは、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙポリシーによって義務付けら

れ得るように、所与のＣＣａａＳリソース、リソースの通常のＣＣａａＳ使用パターン、ユーザの認可プロファイル、及び／又はユーザがＣＣａａＳセッションに携わるために使用する特定のＭｙＣｏｍｐａｎｙ　ＵＥに基づいて、ＭｙＣｏｍｐａｎｙユーザによる所与のＣＣａａＳリソースの使用を構成し、これは、使用のコンテキストに基づいて動的に変化し得る。本開示の実施形態によれば、ＣｙｂｅｒＳａｆｅは、ＣｙｂｅｒＳａｆｅ　ＳＷＢを使用して、ＣＣａａＳに自動的にサインインするためにＣＣａａＳが期待するユーザ及びパスワード入力を模倣することによって、シングルサインオン（ＳＳＯ）をネイティブにサポートしないＣＣａａＳへのＳＳＯアクセスを提供する。

【００１６】

この概要は、発明を実施するための形態において以下でさらに説明される概念の選択を簡略化された形で紹介するために提供される。この概要は、特許請求される主題の重要な特徴又は本質的な特徴を特定することを意図するものではなく、特許請求される主題の範囲を限定するために使用されることを意図するものでもない。

【図面の簡単な説明】

【００１７】

本発明の実施形態の非限定的な実施例について、本段落に続いて列挙される、本明細書に添付される図面を参照して、以下に説明する。複数の図に現れる同一の特徴は、概して、それらが現れる全ての図において同一のラベルでラベル付けされる。図面における本発明の実施形態の所与の特徴を表すアイコンをラベル付けするラベルは、所与の特徴を参照するために使用さることがある。図面に示される特徴の寸法は、提示の便宜及び明瞭さのために選択され、必ずしも縮尺通りに示されていない。

【００１８】

【図１】本開示の一実施形態に従って、ＭｙＣｏｍｐａｎｙと呼ばれる企業にサイバーセキュリティを提供するためにＣｙｂｅｒＳａｆｅ　ＣＩＳＥ及びＳＷＢを有するように構成されたＭｙＣｏｍｐａｎｙ　ＵＥを概略的に示す。

【図２Ａ】本開示の一実施形態に従って、図１に示すＳＷＢがＣｙｂｅｒＳａｆｅハブとのハンドシェイクに関与して、ＭｙＣｏｍｐａｎｙリソースにアクセスする際に使用するためのトークンを取得することができる手順の流れ図を示す。

【図２Ｂ】本開示の一実施形態に従って、図１に示すＳＷＢがＣｙｂｅｒＳａｆｅハブとのハンドシェイクに関与して、ＭｙＣｏｍｐａｎｙリソースにアクセスする際に使用するためのトークンを取得することができる手順の流れ図を示す。

【図２Ｃ】本開示の一実施形態に従って、図１に示すＳＷＢがＣｙｂｅｒＳａｆｅハブとのハンドシェイクに関与して、ＭｙＣｏｍｐａｎｙリソースにアクセスする際に使用するためのトークンを取得することができる手順の流れ図を示す。

【図３】は、本開示の一実施形態に従って、ＳＷＢがＭｙＣｏｍｐａｎｙリソースにアクセスするための許可を提供され得る手順の流れ図を示す。

【図４】本開示の実施形態に従って、ＳＷＢがＭｙＣｏｍｐａｎｙリソースにアクセスするための許可を提供され得る別の手順の流れ図を示す。

【図５Ａ】本開示の一実施形態に従って、ＣｙｂｅｒＳａｆｅがデータを取得及び処理して、ウェブサイトへのアクセスに関連するＭｙＣｏｍｐａｎｙリソースへの可能なサイバー攻撃リスクを推定し、ＳＷＢを使用してＭｙＣｏｍｐａｎｙユーザのウェブサイトへのアクセスを制御し得る手順の流れ図を示す。

【図５Ｂ】本開示の一実施形態に従って、ＣｙｂｅｒＳａｆｅがデータを取得及び処理して、ウェブサイトへのアクセスに関連するＭｙＣｏｍｐａｎｙリソースへの可能なサイバー攻撃リスクを推定し、ＳＷＢを使用してＭｙＣｏｍｐａｎｙユーザのウェブサイトへのアクセスを制御し得る手順の流れ図を示す。

【図５Ｃ】本開示の一実施形態に従って、ＭｙＣｏｍｐａｎｙユーザとウェブサイトとの相互作用のサンプルシナリオを監視することを図示する流れ図を示す。

【図６Ａ】本開示の一実施形態に従って、ＣｙｂｅｒＳａｆｅが、ＭｙＣｏｍｐａｎｙリソースにサイバーセキュリティを提供するために、ＭｙＣｏｍｐａｎｙＣＣａａＳリソー

スの使用を監視し、リアルタイム介入を提供するように動作し得る手順を図示する流れ図を示す。
【図６Ｂ】本開示の一実施形態に従って、ＣｙｂｅｒＳａｆｅが、ＭｙＣｏｍｐａｎｙリソースにサイバーセキュリティを提供するために、ＭｙＣｏｍｐａｎｙＣＣａａＳリソースの使用を監視し、リアルタイム介入を提供するように動作し得る手順を図示する流れ図を示す。
【発明を実施するための形態】
【００１９】
考察において、別段の記載がない限り、本開示の実施形態の１つ又は複数の特徴の条件又は関係特性を修飾する「実質的に」及び「約」等の形容詞は、その条件又は特性が、それが意図される用途に対する実施形態の動作に許容される許容範囲内に定義されることを意味すると理解される。本開示における一般的な用語が、例示的なインスタンス又は例示的なインスタンスのリストを参照することによって示される場合はいつでも、参照されるインスタンスは、一般的な用語の非限定的な例示的なインスタンスの目的であり、一般的な用語は、参照される特定の例示的なインスタンスに限定されることを意図しない。「一実施形態では」という語句は、「あり得る」、「任意選択で」、又は「例として」等の許容と関連付けられるか否かにかかわらず、例を考慮して紹介するために使用されるが、必ずしも本開示の可能な実施形態の必要な構成ではない。別段の指示がない限り、説明及び特許請求の範囲における「又は」という用語は、排他的ではなく包括的な「又は」であるとみなされ、それが結合するアイテムのうちの少なくとも１つ、又は複数のアイテムの任意の組み合わせを示す。
【００２０】
図１は、本開示の一実施形態に従って、ＭｙＣｏｍｐａｎｙ２０又は単にＭｙＣｏｍｐａｎｙとも呼ばれる企業２０の通信ネットワーク、及び通信ネットワークを使用するＭｙＣｏｍｐａｎｙユーザ１０のためのサイバーセキュア通信を提供するように動作するＣｙｂｅｒＳａｆｅシステム５０を概略的に示す。ＭｙＣｏｍｐａｎｙは、クラウドベースのデジタルリソース２２と、ＭｙＣｏｍｐａｎｙのオンプレミスデジタルリソース２８を記憶及び処理するためのオンプレミスサーバ（図示せず）を収容するプレミス２４と、ＭｙＣｏｍｐａｎｙビジネスを行うためにクラウドベース及びオンプレミスリソースにアクセスし、それを使用し、それを処理するためにオンプレミスのときに、ＭｙＣｏｍｐａｎｙユーザ１０によって使用するためのＷＰＵＥ３０とを有してもよい。ＭｙＣｏｍｐａｎｙによって、ユーザ１０は、オフプレミス時に、様々なタイプのＢＹＯＤ３２のいずれかを使用して様々な場所からＭｙＣｏｍｐａｎｙリソースにアクセスすることが可能になり得る。ＭｙＣｏｍｐａｎｙユーザ１０は、個人活動のために自分のそれぞれのＢＹＯＤ３２を使用することができ、ＭｙＣｏｍｐａｎｙユーザは、オンプレミス時に、ＭｙＣｏｍｐａｎｙポリシーによって定義された許可に従って、個人活動のためにＷＰＵＥ３０を使用することを許可され得ると仮定される。個人活動には、通信ノード４１及びウェブサイト４０のクラウドインフラストラクチャを介したウェブブラウジング、ソーシャルネットワーキング、アップロード、及びマテリアルのダウンロードを含んでもよい。ＭｙＣｏｍｐａｎｙネットワークは、両矢印の破線４３によって概略的に示されるように、ＭｙＣｏｍｐａｎｙのオンプレミスデジタルリソース２８、クラウドベースのデジタルリソース２２、ＭｙＣｏｍｐａｎｙのプレミス２４にインストールされたＷＰＵＥ３０を使用するオンプレミスユーザ１０、及び様々なオフプレミスロケーションにおいてＢＹＯＤ３２を使用するオフプレミスユーザ１０の様々な組み合わせのいずれかの間の通信をサポートすることが要求され得る。
【００２１】
本開示の一実施形態によれば、ＣｙｂｅｒＳａｆｅ５０は、任意選択でクラウドベースのＣｙｂｅｒＳａｆｅ処理及びデータハブ５２と、ＭｙＣｏｍｐａｎｙリソースにアクセスし使用するためにＭｙＣｏｍｐａｎｙユーザ１０によって使用される複数のＭｙＣｏｍｐａｎｙ　ＵＥ、ＢＹＯＤ３２及び／又はＷＰＵＥ３０の各々におけるＭｙＣｏｍｐａｎ

ｙ通信及びデジタルリソースをサイバー保護するように動作するソフトウェアアーキテクチャ６０とを備える。ＣｙｂｅｒＳａｆｅハブ５２は、ハブがＣｙｂｅｒＳａｆｅ５０及びＣｙｂｅｒＳａｆｅのコンポーネントに提供する機能性を可能にし、サポートするために必要とされるクラウドベース及び／又はベアメタル処理及びメモリリソースを備える、及び／又はそれへのアクセスを有する。

【００２２】

例として、図１は、休止時及び／又は動作中にＭｙＣｏｍｐａｎｙデジタルリソースを保護し、ＭｙＣｏｍｐａｎｙ　ＵＥ３３を使用し得るユーザ１０のためのリソースへのサイバーセキュアアクセスを提供するようにＭｙＣｏｍｐａｎｙ　ＵＥ３３を構成する、ＣｙｂｅｒＳａｆｅソフトウェアアーキテクチャ６０を概略的に示す。ＭｙＣｏｍｐａｎｙ　ＵＥ３３は、ＢＹＯＤ又はＷＰＵＥであってもよく、Ｍｙ－ＷｏｒｋＳｔａｔｉｏｎ３３と呼ばれることがある。

【００２３】

アーキテクチャ６０は、Ｍｙ－ＷｏｒｋＳｔａｔｉｏｎ３３に常駐するアンビエントソフトウェア３５から隔離されるＣｙｂｅｒＳａｆｅ隔離環境ＣＩＳＥ６２を備え、ＣＩＳＥ６２に常駐するＳＷＢ６４を含む。アンビエントソフトウェア３５は、典型的には、ＭｙＣｏｍｐａｎｙビジネスを行う際に使用することを意図していないデータ及びアプリケーションを含み得る。例として、アンビエントソフトウェア３５は、ブラウザ、アプリケーションのオフィススイート、クリップボード、ファミリー画像のアルバム、フォトアルバム及びＷｈａｔｓＡｐｐを含んでもよい。ＣＩＳＥ６２は、また、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙポリシー特徴によって要求されるサイバーセキュリティ特徴をアプリケーションと関連付けるために、アンビエントソフトウェア３５から任意選択でインポートされ、ＣｙｂｅｒＳａｆｅによってラップされ、任意選択でコンテナ化される、アプリケーションのセット６５を含んでもよい。一実施形態では、ＣＩＳＥは、ＳＷＢ６４によって、及びＳＷＢ６４を介してセット６５内のアプリケーションによって使用するためにアクセスされ得る共有セキュアサービス６６のアンサンブルを備える。共有セキュアサービス６６は、任意選択で、セキュアクリップボード及びセキュア暗号化ファイルシステムを含む。

【００２４】

ＣＩＳＥ６２は、ＳＷＢ６４、共有セキュアサービス６６、及びラップされたアプリケーション６５のラッピングのセキュリティアプリケーション、特徴、及び機能性によって生成され、サポートされる、実質的に連続的なセキュリティ周辺によって画定される、隔離されたセキュリティドメインを提供する。一実施形態によれば、ＣＩＳＥ６２は、ＰＣＩ　ＤＳＳ（支払カード産業データセキュリティ規格）、ＨＩＰＡＡ（医療保険の相互運用性と説明責任に関する法律）、及び／又はＳＯＣ２（米国公認会計士協会のサービス組織コントロール）等の規格の方法及びそれに準拠する方法を用いてサイバーセキュリティ及びアイソレーションを提供するように構成することができる。任意選択で、ＣＩＳＥ６２は、ネットワークレベルでアンビエントソフトウェアから隔離される。

【００２５】

一実施形態では、分離及びセキュリティを提供するために、ＳＷＢ６４は、ＣＩＳＥ６２への、及びそこからの、またＣｙｂｅｒＳａｆｅでラップされたアプリケーション、共有セキュアサービス６６、及び／又はＳＷＢ６４内のアプリケーション間の、それぞれデータの進入及び退出を監視及び制御するように構成される。ＳＷＢ６４は、ＣＩＳＥ内のデータ及びＣＩＳＥへのデータ及びＣＩＳＥからのデータに関連する、へのアクセス、及び移動のＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙセキュリティポリシーを施行するように、ＣｙｂｅｒＳａｆｅによって有利に構成される。データの移動及びデータへのアクセスの分離及び制御、ならびにポリシーの施行は、サイバー損傷に対する強化された保護、ならびにＭｙＣｏｍｐａｎｙ　ＵＥとの通信及びＭｙＣｏｍｐａｎｙ　ＵＥを介した通信から生じ得るＭｙＣｏｍｐａｎｙリソースからの及び／又はＭｙＣｏｍｐａｎｙリソースへのデータの漏出に対するセキュリティを提供するように動作する。

【００２６】
一実施形態では、データの進入及び退出を監視することは、ＳＷＢ６４によってサポートされる通信を監視することと、監視された通信に含まれるデータを記憶及び処理することと、データをＣｙｂｅｒＳａｆｅハブ及びＭｙＣｏｍｐａｎｙＩＴに利用可能にすることとを含む。一実施形態では、監視は、発信通信がＳＷＢｂによって暗号化される前にＣｙｂｅｒＳａｆｅ隔離環境ＣＩＳＥ６２（図１）から発信される通信に対して、及び着信通信がＳＷＢ６４によって復号された後にＣＩＳＥに着信する通信に対して実行される。その結果、ユーザのブラウジングは、ＣｙｂｅｒＳａｆｅ及びＭｙＣｏｍｐａｎｙにとって実質的に完全に可視であり、ローカル又はリモートで処理することができる。監視は、実質的に連続的、確率的、又は定期的であってもよい。確率的監視は、任意選択で所定の確率関数に従って、ランダムに決定された開始時間で開始する限定された持続時間の監視期間にわたって通信を監視することを含む。定期的な監視は、定期的な開始時間における監視期間中の通信の連続的な監視を含む。監視された通信は、ＳＷＢ６４によって、記憶及び／又は処理のために、ＣｙｂｅｒＳａｆｅハブ及び／又はＭｙＣｏｍｐａｎｙ内の宛先にミラーリングされてもよく、あるいは記憶及び／又は処理のために、ＣｙｂｅｒＳａｆｅハブ及び／又はＭｙＣｏｍｐａｎｙ内の宛先に送信される前に、関心のあるデータについてフィルタリングされてもよい。監視される通信がＳＷＢ６４によってどのように処理されるかを構成する特徴及び制約は、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙポリシーに基づいて決定してもよい。そのようなポリシーは、ローカルＳＷＢとＣｙｂｅｒＳａｆｅハブとの間でデータの処理がどのように共有されるかを指定してもよい。
【００２７】
一実施形態では、ＳＷＢ６４は、ＣｙｂｅｒＳａｆｅ特徴及び／又は機能を備える独立したアプリケーション、又はブラウザコードへの変更及び／又追加によって、及び／又はＣｙｂｅｒＳａｆｅ拡張と統合することによって、修正され、追加のＣｙｂｅｒＳａｆｅ特徴及び／又は機能が提供される、Ｇｏｏｇｌｅ（登録商標） Ｃｈｒｏｍｅ、Ｍｉｃｒｏｓｏｆｔ（登録商標） Ｅｄｇｅ、Ａｐｐｌｅ（登録商標） Ｓａｆａｒｉ、Ｍｏｚｉｌｌａ（登録商標） Ｆｉｒｅｆｏｘ（登録商標）、Ｏｐｅｒａ（登録商標）、もしくはＢｒａｖｅ（登録商標）等の既存のウェブブラウザであってもよい。特徴及び機能性は、既存のブラウザに組み込まれてもよく、ブラウザは、オペレーティングシステムフックを使用して既存のブラウザの入力及び出力とインターフェースすること、ブラウザの元のバイナリをパッチすること、ブラウザのＡＰＩ及び／又はＳＤＫの上に専用拡張を構築すること、及び／又はブラウザが動作しているときにブラウザのメモリを動的に変更することによってＣｙｂｅｒＳａｆｅＳＷＢに変換されてもよい。
【００２８】
例として、以下では機能性と総称される特徴及び／又は機能性は、ＳＷＢ６０が、ユーザ１０がＣＩＳＥ６２及びＭｙＣｏｍｐａｎｙリソースにアクセスすることを検証及び許可するために、ＭｙＣｏｍｐａｎｙ ＩＤＰと協働すること、ウェブサイトに関連するサイバーリスクを分類するために使用され得る、ＭｙＣｏｍｐａｎｙユーザによって訪問されたウェブサイトを特徴付けるデータを獲得すること、ＳＷＢ６４セキュリティ機能を損なう可能性があるブラウザ拡張を特徴付けるデータを獲得すること、グループ及び／又は個人としてのＭｙＣｏｍｐａｎｙユーザによるＭｙＣｏｍｐａｎｙリソースの通常の挙動及び使用を決定するために処理され得るデータを獲得すること、ＭｙＣｏｍｐａｎｙユーザのＭｙＣｏｍｐａｎｙリソースとの関与を監視し、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙセキュリティ制約を施行するように関与を制御することを行うことを可能にする機能性のうちの少なくとも１つ又は複数の任意の組み合わせを含んでもよい。
【００２９】
一実施形態では、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙセキュリティ制約を施行することは、ＵＥ３３とＭｙＣｏｍｐａｎｙリソースとの間の全ての通信が、ＳＷＢ６４及びＳＷＢをリソースに接続するＣｙｂｅｒＳａｆｅトンネルを介して伝搬されることを要求することと、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙ許可をリソー

スに施行することと、を含む。任意選択で、セキュリティ制約を施行することは、ＵＥ３３と企業リソースとの間の通信における異常を識別することと、識別された異常からの損傷を排除又は改善し、その発生に対する警告を生成するように動作することと、を含む。

【００３０】

図２Ａ～図６Ｂに提示される流れ図は、一実施形態に従って、ＣｙｂｅｒＳａｆｅシステム及びＳＷＢの機能性を示し、図示する、ＣｙｂｅｒＳａｆｅシステム５０及びＳＷＢ６４等のＣｙｂｅｒＳａｆｅシステム及びＳＷＢによって行われる手順の要素を示す。この議論は、ＣｙｂｅｒＳａｆｅシステムが、それぞれのユーザＩＤ、Ｕ－ＩＤ$_n$（１≦ｎ≦Ｎ）によって識別される複数のユーザＵ$_n$（１≦ｎ≦Ｎ）を有する所与のＭｙＣｏｍｐａｎｙ企業にサイバーセキュリティサービスを提供すると仮定する。ユーザは、ユーザ機器ＩＤ、ＵＥ－ＩＤ$_e$（１≦ｅ≦Ｅ）によって識別されるユーザ機器にアクセスし、それを使用することができ、ＣｙｂｅｒＳａｆｅは、それぞれ、ＳＷＢブラウザＩＤ、Ｂ－ＩＤｂによって識別されるインデックスｂによって参照される、ＣＩＳＥ及びＣｙｂｅｒＳａｆｅブラウザ、ＳＷＢを用いてＵＥを構成していると仮定する。

【００３１】

図２Ａ～図２Ｃは、ユーザ機器ＵＥ$_e$を使用する所与のユーザＵ$_n$が、ＣｙｂｅｒＳａｆｅセキュリティハブに連絡して、ＵＥ$_e$内のＣＩＳＥにアクセスし、それを使用する許可を要求し、ＣＩＳＥ内の常駐ＳＷＢ$_b$にＭｙＣｏｍｐａｎｙリソースへのアクセスのためのセキュリティトークンを発行させる、手順の流れ図１００を示す。

【００３２】

ブロック１０２において、ユーザＵ$_n$は、ＵＥ$_e$を操作して、ＣｙｂｅｒＳａｆｅセキュリティハブにサインインし、セキュリティトークンの要求を提出し、その要求は、ユーザＩＤ、Ｕ－ＩＤ$_n$、ユーザ機器ＩＤ、ＵＥ－ＩＤ$_e$、ＵＥ$_e$にインストールされたＳＷＢを識別するＳＷＢ$_b$　ＩＤ、Ｂ－ＩＤ$_b$を含む拡張ＩＤを含む。Ｕ－ＩＤ$_n$は、ユーザ名、パスワード、及び／又はユーザがＭｙＣｏｍｐａｎｙユーザとして最初に登録された日付等の、ユーザをＵＥ$_e$、ＳＷＢ$_b$、及び／又はＭｙＣｏｍｐａｎｙと関連付けるそのようなデータを含んでもよい。ＵＥ－ＩＤ$_e$は、ＭＡＣ（メディアアクセス）アドレス、ＵＵＩＤ（Ｕｎｉｖｅｒｓａｌ　Ｕｎｉｑｕｅ　Ｉｄｅｎｔｉｆｉｅｒ）、もしくはＩＭＳＩ（ｉｎｔｅｒｎａｔｉｏｎａｌ　ｍｏｂｉｌｅ　ｓｕｂｓｃｒｉｂｅｒ　ｉｄｅｎｔｉｔｙ）等の任意の適切な識別子、及び／又はＵＥ$_e$をユーザＵ$_n$、ＳＷＢ$_b$、及び／もしくはＭｙＣｏｍｐａｎｙに関連付ける情報を含んでもよい。Ｂ－ＩＤｂは、ブラウザユーザエージェント文字列、ＣｙｂｅｒＳａｆｅがＳＷＢ$_b$を割り当てる任意の好適な識別子、及び／又はＳＷＢ$_b$をＵＥ$_e$、Ｕ$_n$、及び／又はＭｙＣｏｍｐａｎｙと関連付ける情報を含んでもよい。

【００３３】

所与のユーザＵ$_n$は、複数のＵＥ$_e$及び／又は複数のＳＷＢ$_b$に関連付けられてもよく、ユーザＩＤ　Ｕ－ＩＤ$_n$は、関連付けを識別するデータを備えてもよいことに留意されたい。同様に、所与のユーザＵＥ$_e$は、複数のＵ$_n$及び／又は複数のＳＷＢ$_b$に関連付けられてもよく、所与のＳＷＢ$_b$は、複数のＵ$_n$及び／又は複数のＵＥ$_e$に関連付けられてもよく、それぞれのＩＤ、ＵＥ－ＩＤ$_e$、及びＢ－ＩＤ$_b$は、関連付けをマッピングするデータを備えてもよい。Ｕ$_n$、ＵＥ$_e$、及び／又はＳＷＢ$_b$のうちの１つ以上の任意の組み合わせは、ＣｙｂｅｒＳａｆｅへの少なくとも１つの以前のサインのそれぞれについての時刻（ＴｏＤ）を含んでもよい。

【００３４】

任意選択で、ブロック１０４において、ＣｙｂｅｒＳａｆｅセキュリティハブは、拡張ＩＤを認証する。拡張ＩＤを認証することは、ユーザＵ$_n$の３ファクタ認証に関与することと、Ｕ－ＩＤ$_n$、ＵＥ－ＩＤ$_e$、又はＢ－ＩＤ$_b$のうちの少なくとも１つとＩＤのうちの別の少なくとも１つとにおける関連付け及び／又はＴｏＤの整合性を決定することとを含んでもよい。

【００３５】

決定ブロック１０６において、拡張ＩＤがＯＫでない場合、ハブは、ブロック１４２に進み、要求されたトークンを拒否し、任意選択で拒否に対するアラートをＣｙｂｅｒＳａｆｅハブに送信する。他方、拡張ＩＤがＯＫである場合、ハブは、任意選択で決定ブロック１０８に進み、ＳＷＢ$_b$ソフトウェア上で完全性試験を実行するか否かを決定する。完全性試験を実行するか否かの決定は、ＭｙＣｏｍｐａｎｙ及び／又はＣｙｂｅｒＳａｆｅ試験ポリシーに依存し得る。ポリシーは、ＣｙｂｅｒＳａｆｅハブが、ＳＷＢ$_b$及び／又はＵＥ$_e$上で最後の完全性試験をいつ実行したか、ユーザＵ$_n$ブラウジング挙動及びインターネット使用パターンを特徴付けるユーザプロファイル、及び／又はサイバー攻撃ランドスケープの特徴に依存し得る。例えば、ＭｙＣｏｍｐａｎｙは、完全性試験の間の遅延が特定の下限遅延より短くなく、上限遅延より長くないというポリシーを有し得る。決定は、ユーザＵ$_n$が所定の頻度より高い頻度でリスクウェブサイトのリストにリストされたサイバーリスクウェブサイトをブラウズするかどうか、又はユーザがパスワードの更新又はアプリケーションのパッチングに従事する傾向があるかどうかに依存し得る。サイバー攻撃ランドスケープは、ＭｙＣｏｍｐａｎｙ又は他の企業によって最近経験されたサイバー攻撃の頻度及び／又は重症度、及び／又はどのようなタイプのサイバー攻撃に遭遇したかを含んでもよい。任意選択で、決定ブロック１０８における決定が完全性試験をスキップすることである場合、ハブはブロック１４０に進み、所望のトークンを発行する。決定が完全性試験を行うことである場合、ハブはブロック１１０に進み、ハブが含むか又はハブがアクセスを有するデータベースから、少なくとも１つのソフトウェア完全性試験「ｓｉｔ$_i$」のセット「ＳＩＴ」を検索することができ、ここで、ＳＩＴ＝｛ｓｉｔ$_i$｜１≦ｉ≦Ｉ｝であり、ＳＷＢ$_b$ソフトウェアの完全性を決定するために使用され得る。例示的なＳＩＴは、以下のうちの少なくとも１つ、又は複数の任意の組み合わせを含んでもよい。

ｓｉｔ$_1$＝ＣＲＴ（チャレンジ応答試験）、
ｓｉｔ$_2$＝ＢＡＴ（挙動証明試験）、
ｓｉｔ$_3$＝ＡＶ（抗ウイルスチェック）、
ｓｉｔ$_4$＝ＥＤＲ（エンドポイント検出及び応答）、
ｓｉｔ$_5$＝ＢＤＳ（バイナリデジタル署名）、
：
ｓｉｔ$_I$

【００３６】

ブロック１１２において、ＣｙｂｅｒＳａｆｅハブは、ＳＷＢ$_b$ソフトウェアの完全性を決定するために試験ｓｉｔ$_i$がどの程度適切であるかについての推定値を提供する各ｓｉｔ$_i$についての重みｗｉｔ$_i$を含む重みベクトルＷＩＴを決定する。一実施形態では、所与のｓｉｔ$_i$についてのｗｉｔ$_i$は、以下の関数である。

ＵＥ$_e$ハードウェアタイプ、例えば、ＵＥ$_e$がモバイルデバイス、タブレット、又はデスクトップである場合、所与のｓｉｔ$_i$のタイプを制限し得るＵＥ$_e$上で実行され得る、

感度（ｓｅｎｓｉｔｉｖｉｔｙ）、所与のｓｉｔ$_i$の真陽性率（ｔｒｕｅ　ｐｏｓｉｔｉｖｅ　ｒａｔｅ）、

特異性（ｓｐｅｃｉｆｉｃｉｔｙ）、所与のｓｉｔ$_i$の真陰性率（ｔｒｕｅ　ｎｅｇａｔｉｖｅ　ｒａｔｅ）、

迷惑レーティング、試験のパフォーマンスがユーザＵＥ$_e$に引き起こす不便さの尺度を提供する、

試験の過去のパフォーマンス、及び／又は

現在のサイバー攻撃コンテキスト、サイバー攻撃タイプの現在の有病率及び重症度を特定する。

【００３７】

ブロック１１４において、ＣｙｂｅｒＳａｆｅハブは、ＳＷＢ$_b$ソフトウェア上で、それらのそれぞれの重みｗｉｔ$_i$に応じて、試験ｓｉｔ$_i$の選択を実行するが、例えば、より大きい重みｗｉｔ$_i$は、それらのそれぞれの重みが中央値重みｗｉｔ$_i$より大きい完全

性試験ｓｉｔｉを選択することによって、より大きな関連性を示す。

【００３８】

ブロック１１６において、ＣｙｂｅｒＳａｆｅハブは、選択された試験ｓｉｔｉの各々によって返された完全性の尺度に応答して、ＵＥｅにおけるＳＷＢｂソフトウェアのＱｏＩ（ｅ，ｂ）（完全性の質）の尺度の値を決定する。一実施形態では、ＱｏＩ（ｅ，ｂ）は、それぞれの重みｗｉｔｉによって重み付けされたｓｉｔｉによって提供される完全性の尺度の平均である。任意選択で、決定ブロック１１８において、ＣｙｂｅｒＳａｆｅハブは、ＱｏＩ値が満足のいくものであるかどうかを決定する。ＱｏＩが満足いくものでない場合、ハブは、ブロック１４２に進み、トークンの発行を拒否し、任意選択でアラートを送信する。他方、ＱｏＩが満足のいくものである場合、ハブは、決定ブロック１２０に進み、ＵＥｅに対してアンビエントソフトウェア環境試験を実行するか否かを決定する。

【００３９】

ソフトウェア環境試験は、仮にあったとすれば、ＵＥｅ内のアンビエントソフトウェアがサイバー損傷によってどの程度リスクにさらされたか、又はサイバー損傷に対して不充分に保護されているかを決定するための試験である。ＵＥｅに対して環境試験を実行するか否かの決定は、完全性試験を実行するか否かの決定を行うときに重み付けされる同じ考慮事項の多くに基づき得る。例えば、その決定は、ＭｙＣｏｍｐａｎｙ及び／又はＣｙｂｅｒＳａｆｅポリシー、ならびにＵＥｅハードウェア、例えば、ＵＥｅが携帯電話又はラップトップであるかどうか、最後の環境試験がＵＥｅ上で実行されたとき、ユーザＵｎの閲覧挙動パターン、及び／又はサイバー攻撃ランドスケープの特徴等の要因に依存し得る。

【００４０】

任意選択で、決定ブロック１２０における決定がソフトウェア環境試験をスキップすることである場合、ＣｙｂｅｒＳａｆｅハブは、ブロック１４０に進み、所望のトークンを発行することができる。他方で、決定が環境試験を行うことである場合、ハブは、任意選択でブロック１１０に進み、データベースから、存在又は不在として判定される少なくとも１つのサイバー攻撃脆弱性特徴ｈｖｆｅ，ｊのセット「ＨＶＦ（ｅ）」を検索することができ、ここで、ＨＶＦ（ｅ）＝｛ｈｖｆｅ，ｊ｜１≦ｊ≦Ｊ｝である。ＨＶＦ（ｅ）は、静的及び／又は動的脆弱性特徴を備え得る。静的脆弱性特徴は、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙリソース等のアンビエントソフトウェアに含まれない周囲ソフトウェア及び／又はデジタルリソースをサイバー攻撃に脆弱にすると見なされる、ＵＥｅの周囲ソフトウェアに含まれるコード及び／又はデータ要素である特徴である。動的脆弱性特徴は、ＵＥｅがパブリックＷｉＦｉに接続されているか、サイバーリスクウェブサイトに接続されているか等の一時的脆弱性特徴であり、ＵＥｅの現在の使用を特徴付ける。例示的なＨＶＦ（ｅ）は、その存在又は不在が、任意選択で、以下のクエリに応答して判定され得る、脆弱性特徴のうちの少なくとも１つ、又は複数の任意の組み合わせを含んでもよい。

ｈｖｆｅ，１＝ＡＶ（抗ウイルス）／ＥＤＲ（エンドポイント検出及び応答）がインストールされているか？、

ｈｖｆｅ，２＝ファイアウォールがインストールされ、イネーブルになっているか？、

ｈｖｆｅ，３＝最新バージョンにパッチされたＯＳ（オペレーティングシステム）か？、

ｈｖｆｅ，４＝最新バージョンにパッチされたアプリケーションか？、

ｈｖｆｅ，５＝ＵＥｅへのアクセスが認証を必要とするか？、

ｈｖｆｅ，６＝リスクソフトウェアデフォルトが存在するか？、

ｈｖｆｅ，７＝パブリックＷｉ－Ｆｉが使用されているか？、

ｈｖｆｅ，８＝ＶＰＮ（仮想プライベートネットワーク）に接続されたＵＥｅか？、

ｈｖｆｅ，９＝接続されたネットワークのセキュリティレベルは？、

：

ｈｖｆｅ，Ｊ。

【００４１】

任意選択で、ブロック１２４において、ＣｙｂｅｒＳａｆｅハブは、ＵＥ$_{e}$アンビエントソフトウェア環境をスキャンして、各ｈｖｆ$_{e,j}$の存在を検出し、各ｈｖｆ$_{e,j}$に対するサイバー攻撃リスク推定値ｈｖｒ$_{e,j}$を含むリスクベクトルＨＶＲ（ｅ）を決定し、ここで、ＨＶＲ（ｅ）＝｛ｈｖｒ$_{e,j}$｜１≦ｊ≦Ｊ）｝である。所与の脆弱性ｈｖｆ$_{e,j}$についてのリスク推定値を決定することは、概して、脆弱性のタイプ及びサイバー攻撃ランドスケープに依存する。例えば、所与のパブリックＷｉ－Ｆｉのリスク推定値を決定することは、Ｗｉ－Ｆｉの物理的位置、推定が行われる時間にＷｉ－Ｆｉによって搬送される現在のトラフィック、及びＷｉ－Ｆｉを介して試みられたサイバー攻撃の最近の履歴に依存し得る。パッチングに関連するリスクは、要求又はインストールされるパッチングのタイプの関数であり得る。

【００４２】

ブロック１２６において、ＣｙｂｅｒＳａｆｅは、ＵＥ$_{e}$アンビエントソフトウェアをスキャンして、アンビエントソフトウェアにおけるリスクにさらされたコンポーネントｈｃｃ$_{k}$のセットＨＣＣ（ｅ）を決定することができ、ここで、ＨＣＣ（ｅ）＝｛ｈｃｃ$_{e,k}$｜１≦ｋ≦Ｋ）｝である。そして、ブロック１２８において、ＣｙｂｅｒＳａｆｅは、ＣｙｂｅｒＳａｆｅデータベースから、リスクコンポーネントｕｃｒ$_{n,r}$（１≦ｒ≦Ｒ）のセットＵＣＲ（ｎ）を任意選択で含むユーザのサイバーリスクプロファイルを特徴付けるユーザプロファイルを検索することができ、ここで、ＵＣＲ（ｎ）＝｛ｕｃｒ$_{n,r}$｜１≦ｒ≦Ｒ）｝であり、これは、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙをサイバー攻撃にさらすユーザＵ$_{n}$の挙動特徴を特徴付けるために使用され得る。

【００４３】

ブロック１３０において、ＣｙｂｅｒＳａｆｅは、ＨＶＲ（ｅ）、ＨＣＣ（ｅ）、ＵＣＲ（ｎ）、及び／又は、属性がＳＷＢ$_{b}$に提供するサイバーセキュリティの尺度をそれぞれ示すＳＷＢ$_{b}$のサイバークラッドソフトウェア属性のセットＣＰＡ（ｂ）を処理して、ＣＰＡ（ｂ）がサイバー攻撃に対する有利な保護をＳＷＢ$_{b}$に提供するかどうかを決定する。例えば、ＭｙＣｏｍｐａｎｙリソースへの高い特権を有するユーザについては、ＣＰＡ（ｂ）によって、ユーザがＭｙＣｏｍｐａｎｙリソースにアクセスできるようにするために、追加のセキュリティチェックを実行し、ＥＤＲ等の追加のセキュリティ制御をインストールすることが要求されることがある。さらに、サイバー攻撃に対するシステムの脆弱性に影響を及ぼすいくつかの能力は、ユーザが未知のウェブサイト又は低いセキュリティ評判（したがって、高いリスク）を伴うウェブサイトにアクセスしている場合、ＣＰＡ（ｂ）によって制約又は無効化されることもある。一実施形態では、処理は、ＨＶＲ（ｅ）、ＨＣＣ（ｅ）、ＵＣＲ（ｎ）、及び／又はＣＰＡ（ｂ）のコンポーネントに基づくコンポーネント特徴を備える入力特徴ベクトルに対して動作するように構成されたニューラルネットワークによって実行される。

【００４４】

任意選択で、ブロック１３２において、ＣｙｂｅｒＳａｆｅハブが、クラッド保護が有利であると判断した場合、ハブは、ブロック１４０に進み、要求されたトークンを発行する。他方、クラッド保護が有利でない場合、ハブは、ブロック１３４に進み、保護を改善するためにクラッド保護を修正するか否かを決定することができる。ハブが修正しないと決定した場合、ハブは、ブロック１４２に進み、トークンを拒否し、アラートを発することができる。他方、決定がクラッディングを修正することである場合、ハブは、ブロック１３６に進み、クラッディングを修正し、任意選択で決定ブロック１３８に進み、修正がサイバー保護の十分な改善をもたらしたかどうかを決定する。改善が十分でない場合、ＣｙｂｅｒＳａｆｅハブは、ブロック１４２に進み、トークンを拒否する。

【００４５】

図３は、本開示の一実施形態に従って、ＳＷＢ（ｎ，ｅ）$_{b}$を有するＵＥ$_{e}$を動作させるユーザＵ$_{n}$が、所与のＭｙＣｏｍｐａｎｙリソースにアクセスするための許可を提供され得る、手順１８０の流れ図を示す。ＳＷＢ（ｎ，ｅ）$_{b}$における括弧内参照（ｎ，ｅ）は、所与のＳＷＢ$_{b}$の構成が、所与のユーザＵ$_{n}$及び所与のユーザ機器ＵＥ$_{e}$との所与の

ＳＷＢ$_b$の関連付けに依存し得ることを、インデックスｂにおいて暗黙的に明示し、また、所与のＵＥ$_e$が、それぞれが異なるＭｙＣｏｍｐａｎｙユーザのために構成される、複数のＳＷＢ$_b$をホストし得ることも示す。

【００４６】

ブロック１８５において、ＣｙｂｅｒＳａｆｅは、所与のＭｙＣｏｍｐａｎｙリソース、例えば、クラウドベースのリソース２２又はオンプレミスリソース２８（図１）にアクセスするためにＵＥ$_e$を操作するユーザＵ$_n$を認証及び認可する際に協働するように、ＭｙＣｏｍｐａｎｙ　ＩＤＰ（識別プロバイダ）及びＣｙｂｅｒＳａｆｅハブ５２を構成する。

【００４７】

ブロック１８６において、ユーザＵ$_n$は、所与のＭｙＣｏｍｐａｎｙリソースにアクセスするための要求とともにＳＷＢ（ｎ，ｅ）$_b$のアイデンティティＢ－ＩＤｂを提出し、トンネル（図１）を介してＣｙｂｅｒＳａｆｅハブに要求を通知するようにＵＥ$_e$のＳＷＢ（ｎ，ｅ）$_b$を操作する。決定ブロック１８７では、所与のＭｙＣｏｍｐａｎｙリソースは、任意選択で、図２Ａ～図２Ｃに図示されるＣｙｂｅｒＳａｆｅプロシージャ１００に従って、任意選択で、ＳＷＢ（ｅ）$_b$がＣｙｂｅｒＳａｆｅハブによって発行されるＣｙｂｅｒＳａｆｅセキュリティトークンを有するかどうかを決定するようにチェックする。

【００４８】

ＳＷＢ（ｎ，ｅ）$_b$がＣｙｂｅｒＳａｆｅセキュリティトークンを保有しない場合、所与のＭｙＣｏｍｐａｎｙリソースは、ブロック１９４に進み、要求されたアクセスを拒否し、アラートを発する。他方、ＳＷＢ（ｎ，ｅ）$_b$がＣｙｂｅｒＳａｆｅセキュリティトークンを含む場合、任意選択でブロック１８８において、ＭｙＣｏｍｐａｎｙリソースは、ＳＷＢ（ｎ，ｅ）$_b$をＭｙＣｏｍｐａｎｙのＩＤＰにリダイレクトする。任意選択で、ブロック１８９において、ＩＤＰは、ユーザＵ$_n$に対してマルチファクタ認証（ＭＦＡ）ＩＤチェックを実行し、決定ブロック１９０において、マルチファクタチェックがＯＫでないと決定された場合、ブロック１９４に進み、要求されたアクセスを拒否する。

【００４９】

他方、ＭＦＡ　ＩＤチェックがＯＫである場合、ブロック１９１において、所与のＭｙＣｏｍｐａｎｙリソースは、ＳＷＢ（ｎ，ｅ）$_b$によって提出された要求をダブルチェックし、ＳＷＢ（ｎ，ｅ）$_b$がＣｙｂｅｒＳａｆｅハブに要求を通知したかどうか、及びＵ$_n$が所与のＭｙＣｏｍｐａｎｙリソースにアクセスすることを許可されているかどうかについて、ＣｙｂｅｒＳａｆｅハブ５２に問い合わせる。決定ブロック１９２において、ハブが要求を確証し、許可を確認する場合、任意選択でブロック１９３において、所与のＭｙＣｏｍｐａｎｙリソースは、要求されたアクセスを許可する。

【００５０】

図４は、本開示の一実施形態に従って、ＳＷＢ（ｎ，ｅ）$_b$を有するＵＥ$_e$を操作するユーザＵ$_n$が所与のＭｙＣｏｍｐａｎｙリソースにアクセスするための許可を提供され得る、別の手順、手順２００の流れ図を示す。

【００５１】

ブロック２０２において、ＣｙｂｅｒＳａｆｅは、任意選択で、ＭｙＣｏｍｐａｎｙリソースへのアクセスを提供するためのプロキシサーバをインスタンス化し、ブロック２０４において、プロキシのみからのＭｙＣｏｍｐａｎｙリソースへのアクセスを許可するようにＭｙＣｏｍｐａｎｙのＩＤＰを構成し、プロキシからのアクセスを要求するようにＳＷＢ（ｎ，ｅ）$_b$を構成する。

【００５２】

ブロック２０６において、ユーザＵ$_n$は、ＳＷＢ（ｎ，ｅ）$_b$を操作して、所与のＭｙＣｏｍｐａｎｙリソースへのアクセスを要求し、ＳＷＢ（ｎ，ｅ）$_b$は、ＣｙｂｅｒＳａｆｅセキュリティハブに接続してアクセスを要求する。ブロック２０８において、セキュリティハブは、プロキシのＩＰアドレス及びプロキシサービスへのアクセスのためのパス

ワードをＳＷＢ（ｎ，ｅ）$_b$に提供する。任意選択で、ブロック２１０において、ＳＷＢ（ｎ，ｅ）$_b$は、プロキシアドレス及びパスワードを使用して、プロキシを介して所与のＭｙＣｏｍｐａｎｙリソースへのアクセスを要求する。要求を受信すると、ＭｙＣｏｍｐａｎｙに関連付けられたＩＤＰは、任意選択で、要求に対してマルチファクタ認証（ＭＦＡ）チェックを実行する。マルチファクタチェックは、ユーザＵ$_n$に関するマルチファクタチェックに加えて、要求がプロキシのＩＰアドレスから受信されたかどうかに関するチェックを任意選択で含む。決定ブロック２１４において、ソースアドレスがプロキシのＩＰアドレスであり、ユーザアイデンティティに関連する認証ファクタが検証される場合、ブロック２１６において、所与のＭｙＣｏｍｐａｎｙリソースへのアクセスが許可される。一方、ＭＦＡが失敗した場合、ブロック２１８において、アクセスが拒否され、ＳＷＢ（ｎ，ｅ）$_b$は、拒否に対するアラートを発する。

【００５３】

図５Ａ及び図５Ｂは、ＣｙｂｅｒＳａｆｅが、ＭｙＣｏｍｐａｎｙユーザ閲覧活動の高い可視性監視を提供し、ユーザＵ$_n$の閲覧挙動に起因するサイバー損傷からＭｙＣｏｍｐａｎｙリソースを保護するように動作する、手順２５０の流れ図を示す。

【００５４】

ブロック２５２において、ＣｙｂｅｒＳａｆｅは、ＭｙＣｏｍｐａｎｙユーザの通信を監視し、ユーザ閲覧活動及びユーザが訪問するウェブサイトを特徴付けるデータを取得するようにブラウザＳＷＢ$_b$を構成する。任意選択で、ブロック２５４において、ブラウザＳＷＢ$_b$は、ユーザのセットＵ＝｛Ｕ$_n$｜（１≦ｎ≦Ｎ）｝からのＭｙＣｏｍｐａｎｙユーザＵ$_n$の閲覧を監視して、ユーザが訪問したウェブサイトのセットＷＳ＝｛ｗｓ$_w$｜（１≦ｗ≦Ｗ）｝の各ウェブサイト「ｗｓ$_w$」について、ユーザの閲覧挙動及びユーザが訪問するウェブサイトを特徴付けるために使用され得るデータを取得する。

【００５５】

一実施形態では、閲覧活動を監視することは、ＳＷＢ$_b$を介してユーザＵ$_n$とウェブサイトｗｓ$_w$との間の通信を監視することと、監視された通信に含まれるデータを記憶及び処理することと、ＣｙｂｅｒＳａｆｅハブ及びＭｙＣｏｍｐａｎｙ　ＩＴ及び／又はＣＩＳＥ内のアプリケーションによるローカル分析にデータを利用可能にすることとを含む。一実施形態では、監視は、発信通信がＳＷＢ$_b$によって暗号化される前にＣｙｂｅｒＳａｆｅ隔離環境ＣＩＳＥ６２（図１）及び／又はＳＷＢ６４（図１）から発信される通信に対して、また着信通信がＳＷＢ$_b$によって復号された後にＣＩＳＥに着信する通信に対して実行される。その結果、ユーザ閲覧は、ＣｙｂｅｒＳａｆｅ及びＭｙＣｏｍｐａｎｙに実質的に完全に可視であり、ローカル処理及びセキュリティ分析のために利用可能である。監視は、連続的、確率的、又は周期的であってもよい。連続的監視は、ユーザＵ$_n$とウェブサイトｗｓ$_w$との間のＳＷＢ$_b$を介して関与するセッションの持続時間の間の通信の実質的に連続的な監視を含む。確率的監視は、任意選択で所定の確率関数に従って、ランダムに決定された開始時間で開始する限定された持続時間の監視期間にわたって通信を監視することを含む。周期的監視は、周期的な開始時間における監視期間中の通信の連続的な監視を含む。監視された通信は、ＣｙｂｅｒＳａｆｅハブ及び／又はＭｙＣｏｍｐａｎｙ内の宛先にミラーリングされてもよく、又はＣｙｂｅｒＳａｆｅハブ及び／又はＭｙＣｏｍｐａｎｙ内の宛先に送信される前に、関心のあるデータについてフィルタリングされてもよい。監視される通信がＳＷＢ$_b$によってどのように処理されるかを構成する特徴及び制約は、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙポリシーに応答して決定され得る。

【００５６】

ブロック２５６において、取得したデータをＣｙｂｅｒＳａｆｅハブ５２（図１）にアップロードすることができる。任意選択で、ブロック２５８において、ＣｙｂｅｒＳａｆｅハブは、アップロードされたデータを処理して、ユーザがウェブサイトにアクセスするときにＭｙＣｏｍｐａｎｙユーザとウェブサイトｗｓ$_w$との通常の対話を特徴付けるか又は特徴付けるために使用され得る挙動プロファイルインジケータｗｐｉ$_{w,p}$のセットＷ

ＰＩ（ｗ）を決定する。任意選択で、ハブは、ウェブサイトws_wについて、ＷＰＩ（ｗ）を生成し、これは、各ＭｙＣｏｍｐａｎｙユーザU_nについて、ユーザ固有のＷＰＩ（ｗ）と呼ばれる。所与のユーザについて決定されたユーザ固有のＷＰＩ（ｗ）のプロファイルインジケータ$wpi_{w,p}$は、所与のユーザがウェブサイトにアクセスするときの所与のユーザの通常のウェブサイト挙動を特徴付ける。一実施形態では、ハブは、グループＷＰＩ（ｗ）と呼ばれるＷＰＩ（ｗ）を生成し、ＷＰＩ（ｗ）は、ＭｙＣｏｍｐａｎｙユーザのグループに対する通常のウェブサイト挙動を集合として特徴付ける。グループＷＰＩ（ｗ）のプロファイルインジケータ$wpi_{w,p}$は、任意選択で、ＭｙＣｏｍｐａｎｙユーザのグループの個々のメンバーについて決定されたユーザ固有のプロファイルインジケータ$wpi_{w,p}$の平均に重み付けすることができる。

【００５７】

例示的なユーザ固有のＷＰＩ（ｗ）及び／又はグループＷＰＩ（ｗ）は、以下のようなプロファイルインジケータ$wpi_{w,p}$のうちの少なくとも１つ、又は複数の任意の組み合わせを含んでもよい。

$wpi_{w,1}$＝アクセスの平均頻度、
$wpi_{w,2}$＝ウェブサイト上で費やされた平均時間、
$wpi_{w,3}$＝ウェブサイトに関連するウェブページをダウンロードするために転送されるデータの量、
$wpi_{w,4}$＝ウェブサイトからダウンロードされたウェブページリソースの数及びタイプ、
$wpi_{w,5}$＝ウェブサイトが使用するＨＴＭＬ５及びＤＯＭ　ＡＰＩ等のＡＰＩ、
$wpi_{w,6}$＝ウェブサイトの外へ向かうリンクの数及びタイプ、
$wpi_{w,7}$＝ウェブサイトがユーザから要求する情報（名前、性別、場所、クレジットカード、…）、
$wpi_{w,8}$＝ウェブサイトのコンテンツタイプ（ニュース、ソーシャルネットワーク、スポーツ、銀行、ポーン（ｐｏｒｎ）、ギャンブル、…）、
$wpi_{w,9}$＝許可、
：
$wpi_{w,P}$。

上記のいくつかのプロファイルインジケータは、複数の関連するインジケータを含む複合プロファイルインジケータであってもよいことに留意されたい。例えば、$wpi_{w,3}$＝リソースの数及びタイプは、概して、ウェブサイトページとバンドルされた複数の異なるリソースを含む。

【００５８】

任意選択で、ブロック２６０において、アップロードされたデータを処理して、ウェブサイトws_wに対するウェブサイト脆弱性特徴$wvf_{w,v}$のセットWVF_wを決定し、ここで、ＷＶＦ（ｗ）＝｛$wvf_{w,v}$｜（１≦ｖ≦Ｖ）｝であり、これは、ウェブサイトws_wに接続する結果として、SWB_b及び／又はSWB_bによってアクセスされるＭｙＣｏｍｐａｎｙリソースをサイバー損傷に対して脆弱にし得る。脆弱性特徴は、プロファイルインジケータ$wpi_{w,p}$の関数であり得る。例えば、所与のウェブサイトws_wに対するプロファイルインジケータ$wpi_{w,p}$の異常値は、サイバー攻撃に対する脆弱性及びサイバー攻撃による損傷のリスクが増大するウェブサイトの攻撃表面を示し得る。一実施形態に従うと、ウェブサイトの所与のプロファイルインジケータ$wpi_{w,p}$に関連付けられた脆弱性の尺度は、ウェブサイトの所与のプロファイルインジケータ$wpi_{w,p}$の値が$wpi_{w,p}$の平均値

【数１】

$$\overline{wpi}_{w,p}$$

から逸脱する程度によって提供することができる。平均

【数２】
$\overline{wpi}_{w,p}$

は、ＭｙＣｏｍｐａｎｙユーザについて決定された平均であっても、あるいはＭｙＣｏｍｐａｎｙを含み得る複数の異なる企業のユーザについて決定された平均であり得る「拡張平均」であってもよい。
【数３】
$\overline{wpi}_{w,p}$

からの所与のｗｐｉ$_{w,p}$の偏差の程度は、
【数４】
$\overline{wpi}_{w,p}$

に関連する標準偏差σの単位で測定され得る。脆弱性特徴は、ウェブサイトプロファイルインジケータと見なされる特徴に、又は有利にはウェブサイトプロファイルインジケータとは別個に見なされる特徴に、直接依存しない特徴であり得る。例えば、所与のウェブサイトが悪意のあるウェブサイト又はサイバーリスクの高いウェブサイトに有し得るリンクの数は、ウェブサイトが他のウェブサイトに有するリンクの総数から独立していると有利に考慮されるウェブサイトの脆弱性特徴であり得る。
【００５９】
例示的なＷＶＦ（ｗ）は、以下に列挙される脆弱性特徴ｗｖｆ$_{w,v}$のうちの少なくとも１つ、又は複数の任意の組み合わせを含んでもよい。リストにおいて、対応するウェブサイトプロファイルｗｐｉ$_{w,v}$の平均からの偏差に依存すると考えられる脆弱性特徴は、関数
【数５】
$\mathcal{F}(\sigma, \overline{wpi}_{w,v})$

に等しいものとして記述される。
【数６】
$wvf_{w,1} = \mathcal{F}(\sigma, \overline{wpi}_{w,1})$

－アクセス頻度からの偏差の関数、
【数７】
$wvf_{w,2} = \mathcal{F}(\sigma, \overline{wpi}_{w,2})$

－ウェブサイト上で費やされた偏差時間の関数、
【数８】
$wvf_{w,3} = \mathcal{F}(\sigma, \overline{wpi}_{w,3})$

－転送されたデータ量からの偏差の関数、…、
ｗｖｆ$_{w,4}$＝ウェブサイトがブラックリスト化されたものか？、
ｗｖｆ$_{w,5}$＝悪意のあるウェブサイトへのリンクの数、
ｗｖｆ$_{w,6}$＝機密情報に対する要求の数及びタイプ（クレジットカード番号、社会保障番号）、

$wvf_{w,7}$＝コンテキスト外ウェブページコンテンツ、
$wvf_{w,8}$＝不必要な許可、
$wvf_{w,9}$＝フラッシュクッキー、
$wvf_{w,10}$＝ＵＲＬショートナーによってアドレス指定されるか、又はＵＲＬショートナーを含む、
$wvf_{w,11}$＝矛盾する特徴を有するＵＲＬ、
：
$wvf_{w,V}$。

【００６０】

ブロック２６２において、ＣｙｂｅｒＳａｆｅハブ５２は、任意選択で、ウェブサイト脆弱性リスク特徴ベクトルＷＶＦＲ（ｗ）＝｛$wvfr_{w,v}$｜１≦ｖ≦Ｖ）｝を決定し、ここで、$wvfr_{w,v}$、脆弱性$wvf_{w,v}$に関連付けられ得るサイバー損傷リスクレベルを定量化する。一実施形態では、ＣｙｂｅｒＳａｆｅは、ニューラルネットワークを使用して、リスクレベルを脆弱性に割り当てることができる。任意選択で、ＣｙｂｅｒＳａｆｅは、ヒューリスティック分類を使用して、リスクレベルを脆弱性に割り当てることができる。

【００６１】

任意選択で、ブロック２６４において、ＣｙｂｅｒＳａｆｅハブ５２は、アップロードされたデータを処理して、各ユーザU_nについて、任意選択でリスクコンポーネント$ucr_{n,r}$（１≦ｒ≦Ｒ）のセットＵＣＲ（ｎ）＝を含むユーザのサイバーリスクプロファイルを特徴付けるユーザプロファイルを決定し、ここで、ＵＣＲ（ｎ）＝｛$ucr_{n,r}$｜（１≦ｒ≦Ｒ）｝は、ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙをサイバー攻撃にさらすユーザU_nの挙動特徴を特徴付けるために使用され得る。リスクコンポーネント$ucr_{n,r}$を決定することは、任意選択で、閲覧挙動特徴のセットを決定することと、決定された閲覧特徴の各々について、挙動特徴がSWB_b及び／又はＭｙＣｏｍｐａｎｙリソースを露出するリスクの程度を推定することと、を含む。

【００６２】

例示的なＵＣＲ（ｎ）は、以下のようなプロファイルインジケータ$ucr_{n,r}$のうちの少なくとも１つ、又は複数の任意の組み合わせを含んでもよい。
$ucr_{n,1}$＝不注意なパスワード管理からのリスク、
$ucr_{n,2}$＝不注意な許可管理からのリスク、
$ucr_{n,3}$＝実行可能なコンテンツを無謀にクリックするからのリスクの推定値、
$ucr_{n,4}$＝フィッシング餌に対する感度不足からのリスク推定値、
$ucr_{n,5}$＝ＭｙＣｏｍｐａｎｙリソースにおいて高い特権を有するユーザについてのリスク推定値、
：
$ucr_{n,R}$。

【００６３】

ブロック２６６において、ユーザU_nは、SWB_bを使用してウェブサイトws_wへの接続を試み、SWB_bは、任意選択で、その試みをＣｙｂｅｒＳａｆｅハブ５２に通知する。通知に応答して、ハブは、任意選択でブロック２６８において、ＷＶＦＲ（ｗ）及びＵＣＲ（ｎ）を処理して、接続から生じ得るサイバー損傷リスクの推定値を提供するセキュリティリスクインジケータ（ＳＲＩ）の値を提供する。そして、ブロック２７０において、ハブ又はSWB_bは、ウェブサイトを検査して、ウェブサイトの変化及び／又はユーザU_nとウェブサイトws_wとの対話の現在の仮想モデルに応答するリアルタイムセキュリティリスクインジケータ（ＲＳＲＩ）を決定することができる。

【００６４】

ＲＳＲＩを決定するためにウェブサイトws_wを調べることは、ＷＶＦ（ｗ）の脆弱性特徴$wvf_{w,v}$に、したがってＳＲＩとＲＳＲＩとの間に統計的に有意な差を生成するリスク特徴ベクトルＷＶＦＲ（ｗ）に変化があるかどうかを決定することを含み得る。Ｒ

ＳＲＩウェブブラウザを決定する実施形態では、ＳＷＢ$_b$は、ウェブページをウェブサイトｗｓ$_w$からＣＩＳＥ内のセキュアサンドボックスにダウンロードし、ウェブページをウェブサイトからレンダリングする前に、ウェブページとバンドルされたリソースの挙動をチェックして、ウェブページ及びリソースが良性であるかどうかを決定することができる。任意選択で、ウェブブラウザＳＷＢ$_b$は、サイバー損傷をもたらす可能性がある、ユーザＵ$_n$がウェブサイトによって提示される実行可能コンテンツをクリックする確率を決定するために、ウェブサイトのエミュレーションと対話する際のユーザＵ$_n$の挙動をモデル化することができる。例えば、ＳＷＢ$_b$は、サンドボックスにおいて実験を実行して、ウェブサイトｗｓ$_w$のエミュレーションがフィッシングベイトを生成するかどうか、及びフィッシングベイトが生成される場合、ＵＣＲ（ｎ）に基づくＵ$_n$アバターがフィッシングベイトをクリックするかどうかを決定することができる。

【００６５】

一実施形態では、ＳＲＩ及び／又はＲＳＲＩの値は、セットＷＶＦ（ｗ）、ＷＶＦＲ（ｗ）、及び／又はＵＣＲ（ｎ）のうちの少なくとも１つ又は複数の任意の組み合わせからのコンポーネントであるか、又はそれに基づくコンポーネントを有する入力特徴ベクトルに対して動作するニューラルネットワークによって決定され得る。任意選択で、ＳＲＩ及び／又はＲＳＲＩの値は、ｗｓ$_w$及び／又はＵ$_n$のヒューリスティックモデルに基づいて決定される。

【００６６】

決定ブロック２７２において、ＣｙｂｅｒＳａｆｅブラウザＳＷＢ$_b$は、セキュリティリスクインジケータＳＲＩが所定の最大上限ＳＲＩ－ＵＢより大きいか、又はＲＳＲＩが所定の最大許容上限ＳＲＩ－ＵＢより大きいかどうかを決定することができる。リスクインジケータのいずれもそのそれぞれの上限よりも大きくない場合、ＳＷＢ$_b$はブロック２８２に進み、ウェブサイトｗｓ$_w$へのアクセスを可能にし、ユーザＵ$_n$とウェブサイトｗｓ$_w$との対話を監視するように動作することができる。

【００６７】

他方、ＳＲＩ又はＲＳＲＩの一方がそれぞれの上限よりも大きい場合、ＳＷＢ$_b$は決定ブロック２７４に進み、ユーザＵ$_n$とウェブサイトｗｓ$_w$との対話及び／又はウェブサイトｗｓ$_w$の機能性をサポートするためにＳＷＢ$_b$の構成を修正するかどうかを決定することができる。ブラウザＳＷＢ$_b$が修正しないと決定した場合、ブラウザはブロック２８０に進み、ウェブサイトｗｓ$_w$へのアクセスを防止し、拒否をＣｙｂｅｒＳａｆｅハブに警告することができる。

【００６８】

他方、ＳＷＢ$_b$が決定ブロック２７４において修正することを決定する場合、ブラウザは任意選択でブロック２７６に進み、ユーザＵ$_n$のためのブラウザ構成を修正し、及び／又はウェブサイトｗｓ$_w$の機能を修正する。例として、ユーザＵ$_n$のためのＳＷＢ$_b$の構成を修正することは、Ｕ$_n$がウェブサイトｗｓ$_w$を表示する特定の実行可能コンテンツをクリックすることを防止することを含むことができ、ウェブサイトｗｓ$_w$を修正することは、ウェブサイト許可を変更すること、及び／又はウェブサイトリンクを無効にすることを含むことができる。修正に続いて、ブラウザＳＷＢ$_b$は、決定ブロック２７８に進み、修正がＳＲＩ及び／又はＲＳＲＩを許容可能な値に低減することに成功したかどうかを決定することができる。ブロック２８２において修正が成功した場合、ブラウザＳＷＢ$_b$はユーザＵ$_n$をｗｓ$_w$に接続し、成功しなかった場合、ブラウザはブロック２８０に進み、ｗｓ$_w$へのＵ$_n$のアクセスを防止する。

【００６９】

一実施形態に従うと、ユーザＵ$_n$とウェブサイトｗｓ$_w$との対話を監視することは、図５Ｃに示す流れ図の２９０によって提供されるシナリオ例によって示されるセキュリティポリシーの侵害を防止するためにユーザアクティビティに介入することを含む。

【００７０】

一実施形態では、手順２５０の手順と同様の手順が、ＣｙｂｅｒＳａｆｅによって実行

され、ＭｙＣｏｍｐａｎｙがアクセス及びダウンロードすることを望み得るブラウザ拡張機能を調べる。ウェブサイトと同様に、ＳＷＢ$_{b}$は、ＭｙＣｏｍｐａｎｙのユーザが関心を証明する拡張のセットの各々についてのデータを蓄積する。データは、拡張子及び／又は拡張子と対話するユーザを修正するかどうか、及びどのように修正するか、また拡張子をダウンロードしてブラウザＳＷＢと統合することを可能にするかどうかを決定するために使用される脆弱性特徴及び脆弱性リスク推定値を決定するために使用され得る。

【００７１】

図６Ａ及び図６Ｂは、ＣｙｂｅｒＳａｆｅが、クラウドコンピューティングのＭｙＣｏｍｐａｎｙユーザの高可視性監視を提供し、ＭｙＣｏｍｐａｎｙクラウドコンピューティングリソースのセットＭｙ－ＣＣａａＳ＝｛Ｍｙ－ＣＣａａＳ$_{s}$｜（１≦ｓ≦Ｓ）｝のＭｙＣｏｍｐａｎｙクラウドコンピューティングリソースＭｙ－ＣＣａａＳ$_{s}$にＭｙＣｏｍｐａｎｙユーザがアクセスし、それを使用することから生じるサイバー損傷からＭｙＣｏｍｐａｎｙリソースを保護するように動作する、手順３００の流れ図を示す。クラウドコンピューティングリソースＭｙ－ＣＣａａＳ$_{s}$は、例として、サービスとしてのインフラストラクチャ（ＩａａＳ）リソース、サービスとしてのプラットフォーム（ＰａａＳ）リソース、又はサービスとしてのソフトウェア（ＳａａＳ）であり得る。

【００７２】

ブロック３０２において、ＣｙｂｅｒＳａｆｅは、ＭｙＣｏｍｐａｎｙユーザのクラウドコンピューティングアクティビティを監視し、ユーザが訪問するＭｙＣｏｍｐａｎｙユーザクラウドコンピューティングアクティビティ及びＭｙ－ＣＣａａＳ$_{s}$リソースを特徴付けるデータを取得するようにブラウザＳＷＢ$_{b}$を構成する。任意選択で、ブロック３０４において、ブラウザＳＷＢ$_{b}$は、クラウドコンピューティングリソースＭｙ－ＣＣａａＳのＭｙＣｏｍｐａｎｙ使用を監視し、所与のユーザＵ$_{n}$及びＭｙ－ＣＣａａＳ$_{s}$セッション（ＣＣＳＥＳＳ$_{n,s}$）について、ＳＷＢ$_{b}$は、任意選択で、キーパフォーマンスインジケータ（ＫＰＩ）のセットＣＣａａＳ－ＫＰＩ（ｎ，ｓ）、ＵＥ－ＫＰＩ（ｎ，ｓ）、Ｕ－ＫＰＩ（ｎ，ｓ）のためのデータと、セッションメタデータコンポーネントのセットＳＭＥＴＡ（ｎ，ｓ）のためのデータと、を蓄積する。

【００７３】

ＣＣａａＳ－ＫＰＩ（ｎ，ｓ）は、セッションＣＣＳＥＳＳ$_{n,s}$中のＭｙ－ＣＣａａＳ$_{s}$の動作を特徴付けるために使用され得るＫＰＩの値を含む。ＣＣａａＳ－ＫＰＩ（ｎ，ｓ）は、例として、ＣＰＵ使用量、メモリ使用量、帯域幅使用、ユーザの要求に対する応答時間、スループット、待ち時間、要求誤り率、アクセスされるリソース、許可変更、及び／又はネットワーク要求のうちの少なくとも１つ、又は複数の任意の組み合わせに対する値を提供するＫＰＩを含むことができる。ＵＥ－ＫＰＩ（ｎ，ｓ，ｅ）は、セッションＣＣＳＥＳＳ$_{n,s}$中にＣＣａａＳ$_{s}$と対話するためにユーザＵ$_{n}$が使用するユーザ機器ＵＥ$_{e}$の動作を特徴付けるために使用され得るＫＰＩの値を含む。ＵＥ－ＫＰＩ（ｎ，ｓ，ｅ）ＫＰＩは、例として、ｃｐｕ使用量、メモリ使用、スレッドカウント、タスク実行時間、ＵＥのセキュリティ制御、特定のＵＥに関連するデータの履歴、ＵＥのリスクスコア、及び／又はスループットのうちの少なくとも１つ、又は複数の任意の組み合わせに対する値を提供するＫＰＩを含むことができる。Ｕ－ＫＰＩ（ｎ，ｓ）は、セッションＣＣＳＥＳＳ$_{n,s}$中にユーザＵ$_{n}$のアクションを特徴付けるために使用され得るＫＰＩの値を含む。Ｕ－ＫＰＩ（ｎ，ｓ）は、例として、ユーザキーボードタイピングパターン、ユーザマウス活動パターン、ラップされたアプリの使用、共有セキュアサービスの使用、ＳＷＢにおいてローカルにタイプされたデータを含む、セッション中にユーザによって使用されるデータパターン、アップロード及びダウンロードされたファイル、ファイル名、及び／又は、アンビエントソフトウェアを使用する中断のうちの少なくとも１つ、又は複数の任意の組み合わせに対する値を提供するＫＰＩを含むことができる。ＳＭＥＴＡ（ｎ，ｓ）は、任意選択で、セッションＣＣＳＥＳＳ$_{n,s}$に対するインデックス付け及び記述データを含む。ＳＭＥＴＡ（ｎ，ｓ）は、例として、セッションＩＤ（Ｕ－ＩＤ$_{n}$、ＵＥ－ＩＤ$_{e}$、Ｂ－ＩＤ$_{b}$）、セッションＴｏＤ（時刻）、セッション持続時間、アップロ

ードされたデータ及びファイルのアイデンティティ、ダウンロードされたファイルのアイデンティティ及びデータ、及び／又は訪問したウェブサイト及びウェブサイト訪問持続時間のうちの少なくとも１つ、又は複数の任意の組み合わせに対する値を提供するデータコンポーネントを含むことができる。

【００７４】

任意選択で、ブロック３０６において、ブラウザＳＷＢ$_b$は、セットＣＣａａＳ－ＫＰＩ（ｎ，ｓ）、ＵＥ－ＫＰＩ（ｎ，ｓ）、Ｕ－ＫＰＩ（ｎ，ｓ）、及び／又はＳＭＥＴＡ（ｎ，ｓ）をＣｙｂｅｒＳａｆｅセキュリティハブ５２（図１）にアップロードする。そして、ブロック３０８において、ブラウザＳＷＢ$_b$及び／又はＣｙｂｅｒＳａｆｅハブは、ＣＣａａＳ－ＫＰＩ（ｎ，ｓ）、ＵＥ－ＫＰＩ（ｎ，ｓ）、Ｕ－ＫＰＩ（ｎ，ｓ）、及び／又はＳＭＥＴＡ（ｎ，ｓ）によって提供されるデータを処理して、セットのコンポーネントの期待値を決定する。期待値は、ユーザＵ$_n$及びＭｙ－ＣＣａａＳ$_s$についてのセッションＣＣＳＥＳＳ$_{n,s}$の複数のインスタンスについて、及び／又は集合として複数のＭｙ－ＣＣａａＳ$_s$セッションＣＣＳＥＳＳ$_{n,s}$及びＭｙＣｏｍｐａｎｙユーザＵ$_n$のグループについての期待値について決定され得る。一実施形態では、所与のユーザＭｙＣｏｍｐａｎｙユーザＵ$_n$に対する期待値は、ＣＣＳＥＳＳ$_{n,s}$に対するユーザ固有通常挙動パターンを決定し、ＭｙＣｏｍｐａｎｙのグループに対する期待値は、ＣＣＳＥＳＳ$_s$セッションに対するグループ通常挙動パターンを決定する。

【００７５】

任意選択で、ＣｙｂｅｒＳａｆｅハブ及び／又はブラウザＳＷＢ$_b$によって決定されたユーザ固有通常挙動パターン及びグループ通常挙動パターンは、ＣｙｂｅｒＳａｆｅハブに関連付けられたクラウドベースのメモリ等のメモリに、又はＣＩＳＥ６２（図１）内の共有セキュアサービス６６のセキュア暗号化ファイルシステムのメモリ等のＳＷＢ$_b$に関連付けられたメモリに記憶される。

【００７６】

任意選択で、ブロック３１０において、ＳＷＢ$_b$及び／又はＣｙｂｅｒＳａｆｅハブは、ＣＣａａＳ－ＫＰＩ（ｎ，ｓ）、ＵＥ－ＫＰＩ（ｎ，ｓ）、Ｕ－ＫＰＩ（ｎ，ｓ）、及び／又はＳＭＥＴＡ（ｎ，ｓ）によって提供されるデータを処理して、Ｍｙ－ＣＣａａＳ$_s$を使用するＭｙＣｏｍｐａｎｙユーザ、及び／又はＭｙ－ＣＣａａＳ$_s$を使用する特定のＭｙＣｏｍｐａｎｙユーザに関連するサイバー脆弱性を決定する。任意選択で、ブロック３１２において、ＣｙｂｅｒＳａｆｅハブ及び／又はＳＷＢ$_b$は、決定されたサイバー脆弱性に応答して、ＳＷＢ$_b$及び／又はＭｙ－ＣＣａａＳ$_s$の特徴を修正して、Ｍｙ－ＣＣａａＳ$_s$セッション中のサイバー損傷のリスクを中程度にする。例として、Ｍｙ－ＣＣａａＳ$_s$の修正は、特定のリソースへのアクセスを許可しないこと、許可変更を防止すること、及び／又はネットワーク要求を制限することを含むことができる。ＳＷＢ$_b$への修正は、特定のファイル及び／又はデータのアップロード及び／又はダウンロードを防止するように、及び／又はＭｙ－ＣＣａａＳ$_s$セッションの持続時間を制限するようにＳＷＢ$_b$を構成することを含むことができる。

【００７７】

任意選択で、ブロック３１４において、所与のＵＥ$_e$において所与のブラウザＳＷＢ$_b$を使用する特定のユーザＵ$_n$は、特定のＭｙ－ＣＣａａＳ$_s$へのアクセス及びその使用を要求し、許可され、Ｍｙ－ＣＣａａＳ$_s$との「現在の」セッションＣＣＳＥＳＳ$_{n',s'}$に従事する。ブロック３１６において、所与のＳＷＢ$_b$は、現在のセッションＣＣＳＥＳＳ$_{n',s'}$を監視して、ＣＣａａＳ－ＫＰＩ（ｎ’，ｓ’）、ＵＥ－ＫＰＩ（ｎ’，ｓ’，ｅ’）、Ｕ－ＫＰＩ（ｎ’，ｓ’）、ＳＭＥＴＡ（ｎ’，ｓ’）についてのデータを蓄積し、ローカルに処理し、アップロードして、現在のセッションについて、既に蓄積されているデータに追加する、任意選択で、所与のＳＷＢ$_b$以外のＳＷＢ$_b$によって、Ｍｙ－ＣＣａａＳ$_s$との以前のセッションからの処理のために、ＭｙＣｏｍｐａｎｙ及び／又はＣｙｂｅｒＳａｆｅポリシーを施行し、及び／又は異常イベントの発生を検出する。

【００７８】

一実施形態では、異常イベントは、通常挙動を侵害するイベント、又はＭｙＣｏｍｐａｎｙ及び／又はＣｙｂｅｒＳａｆｅポリシーを侵害するイベントである。例として、通常パターンの侵害は、所与のＳＷＢ$_b$によって監視される所与のＫＰＩの、ＫＰＩの期待値からの、ＫＰＩについて確立された標準偏差に所定の係数を乗じた値より大きい量の偏差を含み得る。任意選択で、イベントが通常挙動及び／又はポリシーの侵害であると決定するための条件は、ユーザ依存及び／又はＭｙ－ＣＣａａＳ$_s$依存である。例えば、経験のないＭｙＣｏｍｐａｎｙユーザの場合、侵害の定義は、経験のあるＭｙＣｏｍｐａｎｙユーザの場合よりも許容性が低く、その結果、ＫＰＩ係数は、経験のあるＭｙＣｏｍｐａｎｙユーザの場合よりも小さい場合がある。ＣｙｂｅｒＳａｆｅ及び／又はＭｙＣｏｍｐａｎｙポリシーの施行は、例として、ＭｙＣｏｍｐａｎｙユーザが特定のＭｙＣｏｍｐａｎｙファイル又はデータをアップロード、ダウンロード、及び／又は修正すること、ウェブサイト及び／又はＭｙＣｏｍｐａｎｙリソースにアクセスすることを防止することを伴い得る。防止することは、ユーザがユーザＵＥから通信を送信することを管理する前に、ＭｙＣｏｍｐａｎｙユーザによって作成された通信のドラフトを傍受することを含んでもよい。ポリシーを施行することは、許可を変更すること、又は現在のセッションＣＣＳＥＳＳ$_{n,s}$をキャンセルすること、ＣＩＳＥにおける、及びＣＩＳＥと他のＵＥコンポーネントとの間のいくつかのローカルアクセス許可をブロックすることを伴い得る。

【００７９】

ブロック３１８において、所与のＳＷＢ$_b$によって異常イベントが検出されない場合、所与のＳＷＢ$_b$は、決定ブロック３２８に続き、セッションＣＣＳＥＳＳ$_{n,s}$が終了したかどうかを決定することができる。セッションが終了していない場合、所与のＳＷＢ$_b$は、ブロック３１６に戻り、セッションの監視を続けることができる。セッションが終了している場合、所与のＳＷＢ$_b$は、ブロック３３０に進み、監視を終了する。他方、異常イベントが検出された場合、任意選択で決定ブロック３２０において、所与のＳＷＢ$_b$は、ＣｙｂｅｒＳａｆｅハブ５２（図１）及び／又はＭｙＣｏｍｐａｎｙポリシーに基づいて、異常イベントが応答を保証するかどうかを決定する。応答が保証されない場合、所与のＳＷＢ$_b$は、決定ブロック３２８に続き、セッションＣＣＳＥＳＳ$_{n,s}$が終了したかどうかを決定することができ、セッションが終了していない場合、ブロック３１６に戻り、セッションの監視を継続する。他方、応答が保証される場合、所与のＳＷＢ$_b$は、ブロック３２２に進み、応答を行うことができる。応答は、ＭｙＣｏｍｐａｎｙ及び／又はＣｙｂｅｒＳａｆｅポリシーを施行することと、前の段落で述べられたアクションを行うこととを含み得る。応答がキャンセルではなく、ＭｙＣｏｍｐａｎｙ及び／又はＣｙｂｅｒＳａｆｅポリシーの下で十分であると考えられる場合、所与のＳＷＢ$_b$は、決定ブロック３２８に続き、セッションＣＣＳＥＳＳ$_{n,s}$が終了したかどうかを決定することができ、セッションが終了していない場合、ブロック３１６に戻り、セッションの監視を継続する。他方、異常応答が十分でない場合、又はキャンセルを含む場合、所与のＳＷＢ$_b$はブロック３２６に進み、セッションＣＣＳＥＳＳ$_{n,s}$を終了する。

【００８０】

上記の説明では、様々なアクションが、ＣｙｂｅｒＳａｆｅハブ５２及びＣｙｂｅｒＳａｆｅブラウザＳＷＢ$_b$６４の一方又は他方によって実行されるものとして説明されていることに留意されたい。しかしながら、本開示の実施形態によれば、ＣｙｂｅｒＳａｆｅハブ５２及びＣｙｂｅｒＳａｆｅブラウザＳＷＢ$_b$の一方によって実行されるアクションは、他方によって実行されてもよく、あるいはＣｙｂｅｒＳａｆｅハブ５２及びブラウザＳＷＢ$_b$が協働することによって実行されてもよい。

【００８１】

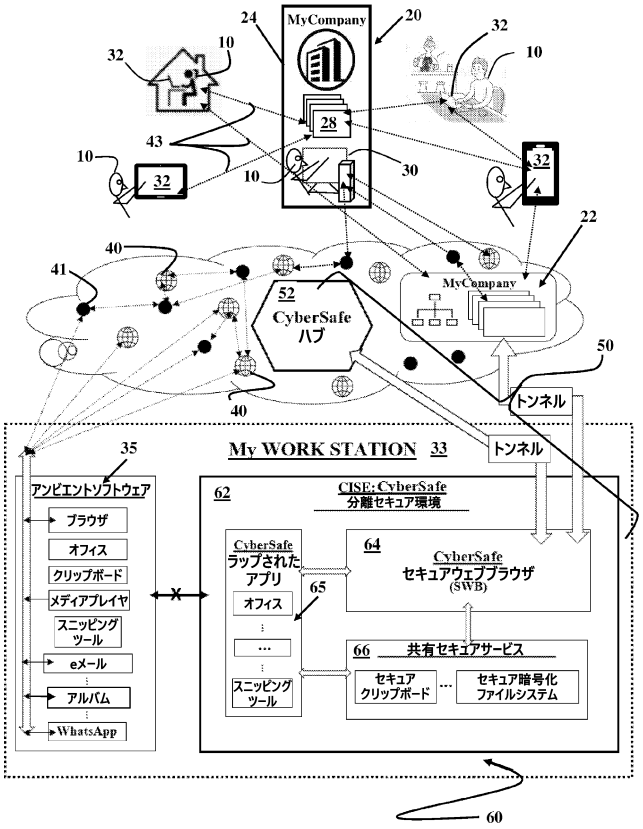
本出願の明細書及び特許請求の範囲では、「備える（ｃｏｍｐｒｉｓｅ）」、「含む（ｉｎｃｌｕｄｅ）」、及び「有する（ｈａｖｅ）」という動詞のそれぞれ、及びそれらの活用形は、動詞の１つ以上の主語が、必ずしも動詞の１つ以上の主語のコンポーネント、要素、又は部分の完全なリストではないことを示すために使用される。

【００８２】

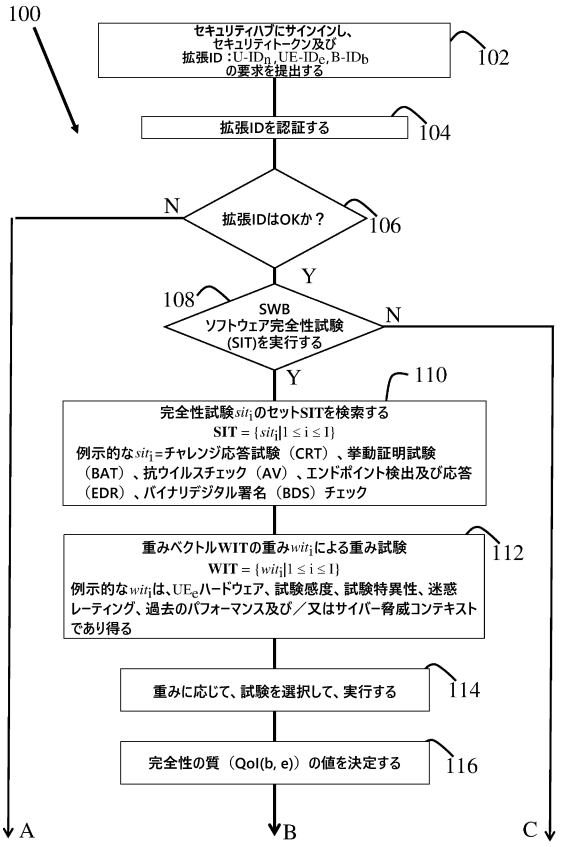
本出願における本発明の実施形態の説明は、例として提供され、本発明の範囲を限定することを意図しない。説明される実施形態は、異なる特徴を備え、その全てが本発明の全ての実施形態において必要とされるわけではない。いくつかの実施形態は、特徴のうちのいくつかのみ、又は特徴の可能な組み合わせを利用する。記載される本発明の実施形態の変形、及び記載される実施形態に記載される特徴の異なる組み合わせを含む本発明の実施形態は、当業者に思い浮かぶであろう。本発明の範囲は、特許請求の範囲によってのみ限定される。

【図面】

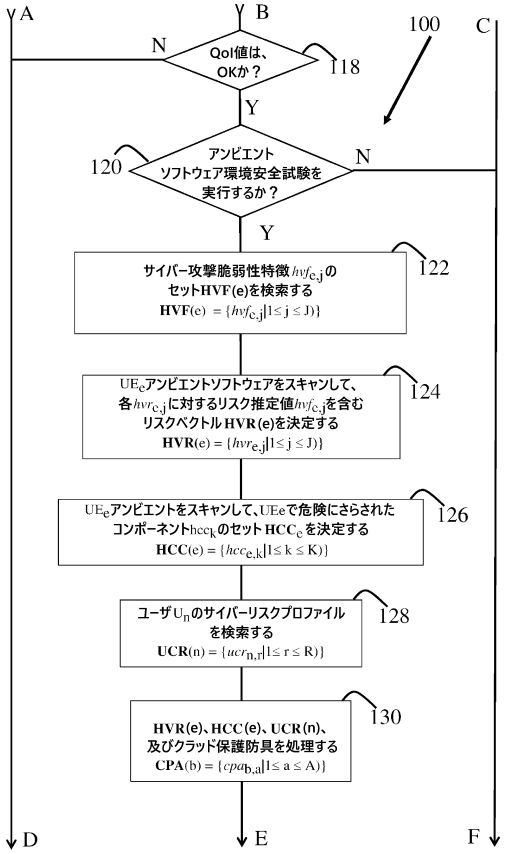
【図１】



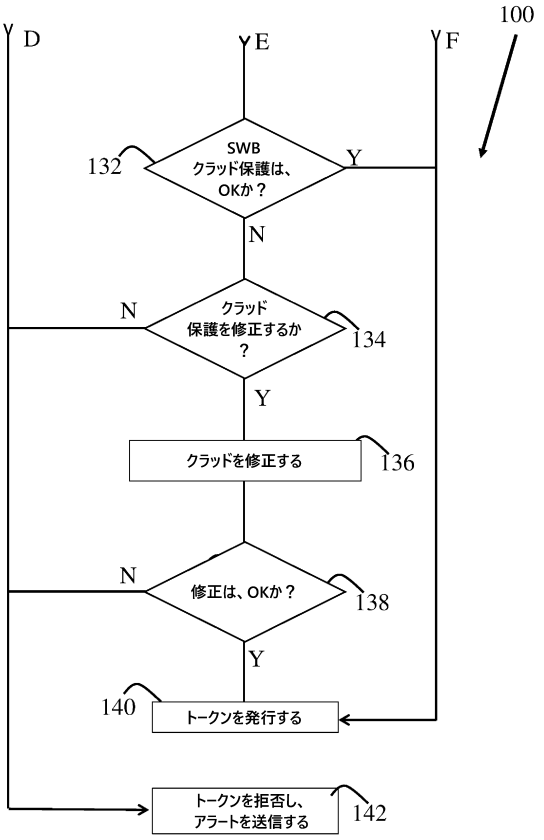
【図２Ａ】



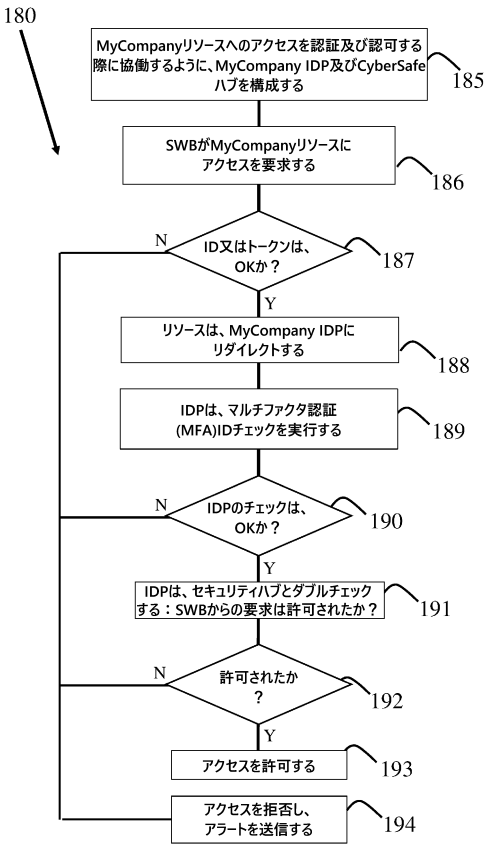
【図２Ｂ】


A
B
C
D
E
F
100
N
QoI値は、OKか？
118
Y
120
アンビエントソフトウェア環境安全試験を実行するか？
N
Y
サイバー攻撃脆弱性特徴 $hvf_{e,j}$ のセットHVF(e)を検索する
HVF(e) $= \{hvf_{e,j} | 1 \le j \le J\}$
122
UE_eアンビエントソフトウェアをスキャンして、各$hvr_{e,j}$に対するリスク推定値$hvf_{e,j}$を含むリスクベクトルHVR(e)を決定する
HVR(e) $= \{hvr_{e,j} | 1 \le j \le J\}$
124
UE_eアンビエントをスキャンして、UEeで危険にさらされたコンポーネントhcc_kのセット HCC_e を決定する
HCC(e) $= \{hcc_{e,k} | 1 \le k \le K\}$
126
ユーザ U_n のサイバーリスクプロファイルを検索する
UCR(n) $= \{ucr_{n,r} | 1 \le r \le R\}$
128
HVR(e)、HCC(e)、UCR(n)、及びクラッド保護防具を処理する
CPA(b) $= \{cpa_{b,a} | 1 \le a \le A\}$
130

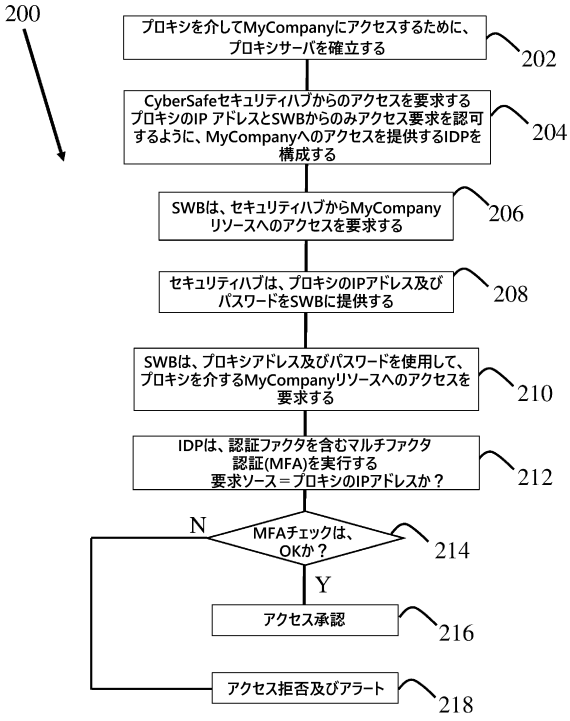
【図２Ｃ】


D
E
F
100
SWBクラッド保護は、OKか？
132
Y
N
N
クラッド保護を修正するか？
134
Y
クラッドを修正する
136
N
修正は、OKか？
138
Y
140
トークンを発行する
トークンを拒否し、アラートを送信する
142

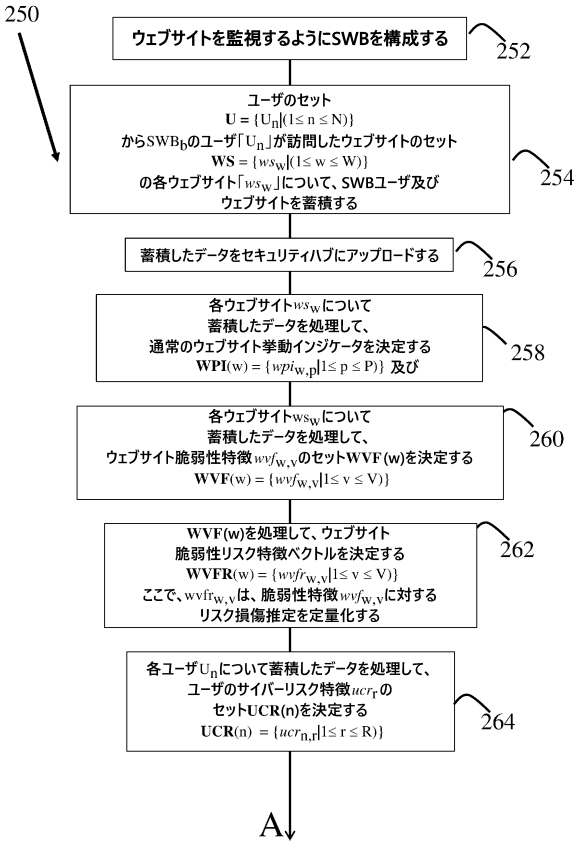
【図３】


180
MyCompanyリソースへのアクセスを認証及び認可する際に協働するように、MyCompany IDP及びCyberSafeハブを構成する
185
SWBがMyCompanyリソースにアクセスを要求する
186
N
ID又はトークンは、OKか？
187
Y
リソースは、MyCompany IDPにリダイレクトする
188
IDPは、マルチファクタ認証(MFA)IDチェックを実行する
189
N
IDPのチェックは、OKか？
190
Y
IDPは、セキュリティハブとダブルチェックする：SWBからの要求は許可されたか？
191
N
許可されたか？
192
Y
アクセスを許可する
193
アクセスを拒否し、アラートを送信する
194

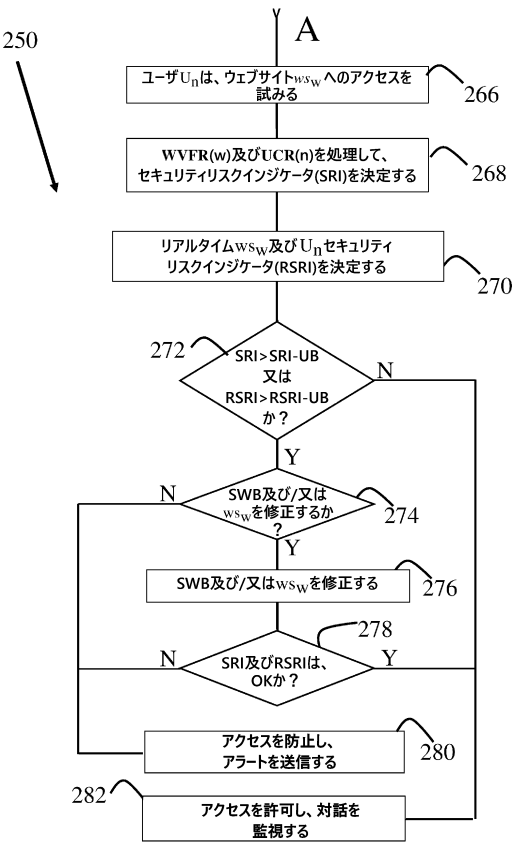
【図４】


200
プロキシを介してMyCompanyにアクセスするために、プロキシサーバを確立する
202
CyberSafeセキュリティハブからのアクセスを要求するプロキシのIP アドレスとSWBからのみアクセス要求を認可するように、MyCompanyへのアクセスを提供するIDPを構成する
204
SWBは、セキュリティハブからMyCompanyリソースへのアクセスを要求する
206
セキュリティハブは、プロキシのIPアドレス及びパスワードをSWBに提供する
208
SWBは、プロキシアドレス及びパスワードを使用して、プロキシを介するMyCompanyリソースへのアクセスを要求する
210
IDPは、認証ファクタを含むマルチファクタ認証(MFA)を実行する
要求ソース＝プロキシのIPアドレスか？
212
N
MFAチェックは、OKか？
214
Y
アクセス承認
216
アクセス拒否及びアラート
218

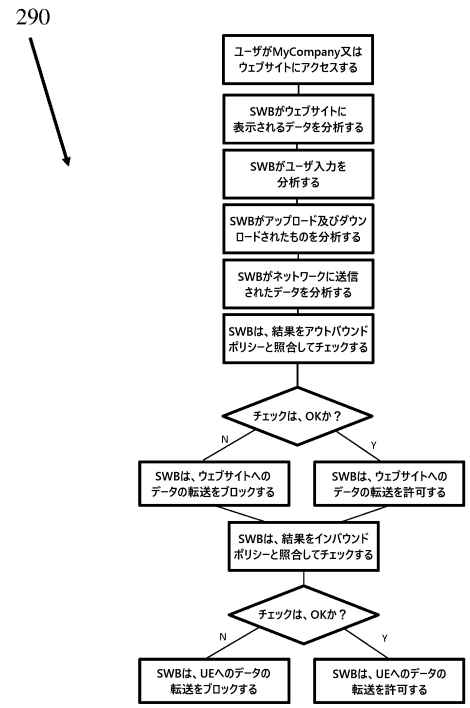
【図５Ａ】



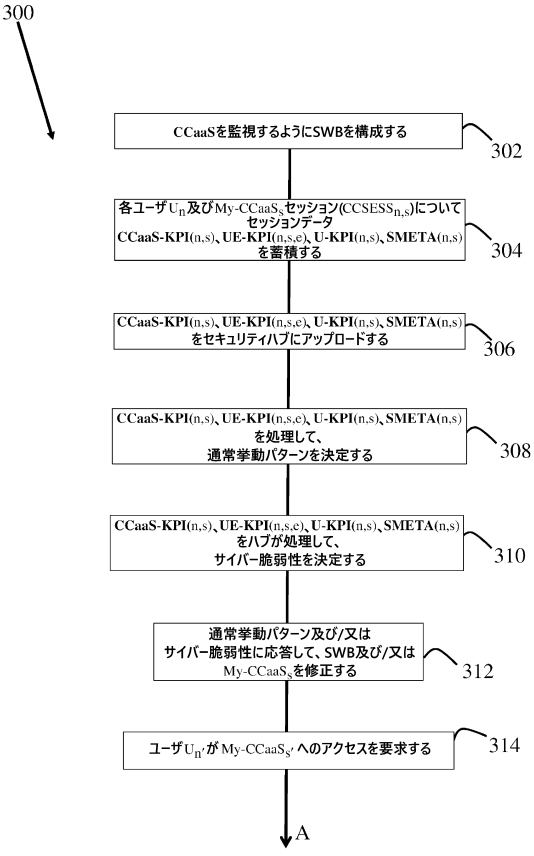
【図５Ｂ】



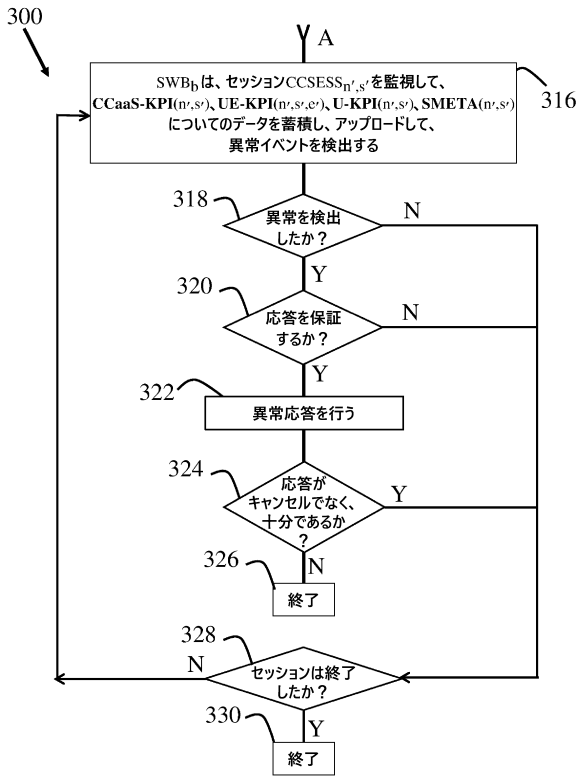
【図５Ｃ】



【図６Ａ】



【図６Ｂ】


300
A
SWBbは、セッションCCSESSn′,s′を監視して、
CCaaS-KPI(n′,s′)、UE-KPI(n′,s′,c′)、U-KPI(n′,s′)、SMETA(n′,s′)
についてのデータを蓄積し、アップロードして、
異常イベントを検出する
316
318
異常を検出したか？
N
Y
320
応答を保証するか？
N
Y
322
異常応答を行う
324
応答がキャンセルでなく、十分であるか？
Y
N
326
終了
328
N
セッションは終了したか？
330
Y
終了

【手続補正書】
【提出日】令和5年12月15日(2023.12.15)
【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】
通信ネットワークを介してアクセス可能なデジタルリソースのグループのデジタルリソースへのセキュアアクセスを提供するための通信システムであって、
ＩＰ（インターネットプロトコル）アドレスを介してアクセス可能なデータ処理ハブと、
前記通信ネットワークを介して通信するために使用可能な複数のユーザ機器（ＵＥ）であって、それぞれが、前記ＵＥ内のアンビエントソフトウェアから隔離され、セキュアウェブブラウザ（ＳＷＢ）を含むサイバーセキュア隔離環境（ＣＩＳＥ）を有するように構成される、ＵＥと、
を含み、
前記ハブ及びＣＩＳＥは、ＣＩＳＥの中で動作中及び静止中のデジタルリソースが前記ハブに可視であるように構成される、通信システム。
【請求項２】
前記セキュア環境は、前記システムのセキュリティポリシーによって定義されるセキュリティ制約に適合するようにラップされた少なくとも１つのソフトウェアアプリケーションを含む、請求項１に記載の通信システム。
【請求項３】
前記セキュア環境は、前記ＳＷＢによって使用可能な少なくとも１つのセキュアサービスアプリケーションと、前記少なくとも１つのラップされたアプリケーションと、を含む、請求項２に記載の通信システム。
【請求項４】
前記少なくとも１つのセキュアサービスアプリケーションは、セキュアクリップボードと、セキュア暗号化ファイルシステムと、を含む、請求項３に記載の通信システム。
【請求項５】
前記ＣＩＳＥ内のアプリケーション間の通信は、セキュア暗号化通信チャネルを介する、請求項２に記載の通信システム。
【請求項６】
前記ＳＷＢと前記ＣＩＳＥ内のアプリケーションとの間の通信は、セキュア暗号化通信チャネルを介する、請求項２に記載の通信システム。
【請求項７】
前記ＳＷＢから送信される通信は、前記ＳＷＢが前記通信を暗号化する前に、前記ハブに可視である、請求項１に記載の通信システム。
【請求項８】
前記ＳＷＢに入る通信は、前記ＳＷＢが前記通信を復号した後に、前記ハブに可視である、請求項１に記載の通信システム。
【請求項９】
ＵＥ内の前記ＳＷＢは、前記ＵＥのユーザの通信を監視して、前記ユーザ及び前記ユーザが訪問するウェブサイトの閲覧挙動を特徴付けるデータを取得する、請求項１に記載の通信システム。
【請求項１０】
前記ハブ及び／又は前記ＳＷＢは、取得した前記データを処理して、前記ユーザがアクセスするウェブサイトとの前記ユーザの対話の通常パターンを決定する、請求項９に記載

の通信システム。
【請求項１１】
前記ハブ及び／又は前記ＳＷＢは、取得した前記データを処理して、前記ユーザが前記ウェブサイトにアクセスすることに起因するリソースの前記グループのデジタルリソースに対するサイバー損傷のリスクを決定する、請求項１０に記載の通信システム。
【請求項１２】
前記ハブ及び／又は前記ＳＷＢは、決定された前記リスクに応答してグループリソースを保護するためのウェブ閲覧セキュリティポリシーを構成する、請求項１１に記載の通信システム。
【請求項１３】
前記ＳＷＢは、前記ＳＷＢと前記ＳＷＢによってアクセスされるウェブサイトとの間の通信を監視して、前記ウェブ閲覧セキュリティポリシーを施行する、請求項１２に記載の通信システム。
【請求項１４】
前記閲覧セキュリティポリシーを施行することは、前記ＳＷＢを使用して前記ユーザの閲覧挙動を監視して、決定された通常閲覧挙動に応答して前記挙動における異常を識別することを含む、請求項１２に記載の通信システム。
【請求項１５】
前記異常は、決定された前記通常挙動及び／又は前記ポリシーの侵害を含む、請求項１４に記載の通信システム。
【請求項１６】
前記ＳＷＢがリソースの前記グループのリソースへのアクセスを要求するように動作する前に、前記ハブは、前記ＳＷＢが含むソフトウェアを調べるように動作する、請求項１に記載の通信システム。
【請求項１７】
前記ソフトウェアを調べることは、前記ソフトウェアのソフトウェア完全性試験を実行することを含む、請求項１６に記載の通信システム。
【請求項１８】
前記ＳＷＢがリソースの前記グループのリソースへのアクセスを要求するように動作する前に、前記ハブは、前記ＵＥが含むアンビエントソフトウェアを調べるように動作する、請求項１に記載の通信システム。
【請求項１９】
前記アンビエントＵＥソフトウェアのソフトウェア完全性試験を実行することを含む、請求項１８に記載の通信システム。
【請求項２０】
前記アンビエントソフトウェアの完全性の質（ＱｏＩ）を決定することを含む、請求項１９に記載の通信システム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/IL2022/050416

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/44 G06F21/53 G06Q20/40 H04W12/06 H04W12/08
H04L9/40 H04L67/02
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
G06F G07G G06Q H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/007291 A1 (MILLER KARL FREDERICK [US]) 1 January 2015 (2015-01-01) abstract paragraph [0002] paragraphs [0007] - [0010] paragraph [0015] -----	1-60
X	US 2018/359244 A1 (COCKERILL AARON [US] ET AL) 13 December 2018 (2018-12-13) abstract paragraph [0017] - paragraph [0020] -----	1-60
A	US 9 521 032 B1 (WORSLEY TIMOTHY CRAIG [US]) 13 December 2016 (2016-12-13) abstract -----	1-60

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 July 2022	12/08/2022

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	San Millán Maeso, J

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IL2022/050416

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015007291 A1	01-01-2015	US 2015007291 A1	01-01-2015
		US 2017250984 A1	31-08-2017
US 2018359244 A1	13-12-2018	EP 3635985 A1	15-04-2020
		IL 259467 A	28-06-2018
		US 2018359244 A1	13-12-2018
		US 2019141030 A1	09-05-2019
		US 2021258304 A1	19-08-2021
		WO 2018227024 A1	13-12-2018
US 9521032 B1	13-12-2016	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

ブ スデロト ハハスカラ ストリート １７エー

(72)発明者 ボブロフ オハド

イスラエル国 ６３４２６２０ テルアビブ バル コチヴァ ６

(72)発明者 ロス ギラド

イスラエル国 ７１７０９１４ モディイン マカビム－レウト エメク ハフラ ３１

(72)発明者 ハルパク ガイ

イスラエル国 ５２９０４４４ ラマット ガン ハルドゥフ ラマット－エファル １６

(72)発明者 サロモン イド

イスラエル国 ６９４１５０５ テルアビブ ネイサン アルターマン ５