(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6626095号
(P6626095)
(45)発行日　令和1年12月25日(2019.12.25)　(24)登録日　令和1年12月6日(2019.12.6)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62 354

請求項の数 22 (全 30 頁)

(21)出願番号　特願2017-512318(P2017-512318)
(86)(22)出願日　平成27年8月27日(2015.8.27)
(65)公表番号　特表2017-532649(P2017-532649A)
(43)公表日　平成29年11月2日(2017.11.2)
(86)国際出願番号　PCT/CN2015/088214
(87)国際公開番号　WO2016/034068
(87)国際公開日　平成28年3月10日(2016.3.10)
審査請求日　平成30年5月15日(2018.5.15)
(31)優先権主張番号　201410446695.6
(32)優先日　平成26年9月3日(2014.9.3)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所

最終頁に続く

(54)【発明の名称】機密情報処理方法、装置、及び、サーバ、ならびに、セキュリティ決定システム

(57)【特許請求の範囲】
【請求項１】
コンピュータが実行する機密情報処理方法であって、
前記コンピュータの情報収集ユニットによって、ページ内の処理対象情報を取得することと、
前記コンピュータの機密情報識別ユニットによって、予め設定された機密情報識別ストラテジーに従って、前記コンピュータの機密情報ライブラリ内に保存された機密情報に基づいて前記処理対象情報が機密情報であるかどうかを決定することと、
前記コンピュータの情報処理ユニットによって、前記処理対象情報が機密情報であるときに前記コンピュータの処理ストラテジー・ユニットによって保存され予め設定された機密情報処理ストラテジーに従って処理を行い、処理済機密情報を作成することと、
前記コンピュータの置換ユニットによって、前記ページ内の前記処理対象情報を、前記処理済機密情報によって置換して、前記処理済機密情報を有するページを作成することと、
を含み、
前記ページ内の処理対象情報を取得することは、
ＭＶＣフレームワーク構造におけるコントローラが呼び出された後であって、ビューが実行される前に、インターセプタを用いて前記ページ内の前記処理対象情報を取得すること、または、
ＭＶＣフレームワーク構造におけるＶｅｌｏｃｉｔｙが呼び出された後に、インターセ

プタを用いて前記ページ内の前記処理対象情報を取得すること、
を含む機密情報処理方法。
【請求項２】
コンピュータが実行する機密情報処理方法であって、
前記コンピュータの情報収集ユニットによって、ページ内の処理対象情報を取得することと、
前記コンピュータの機密情報識別ユニットによって、予め設定された機密情報識別ストラテジーに従って、前記コンピュータの機密情報ライブラリ内に保存された機密情報に基づいて前記処理対象情報が機密情報であるかどうかを決定することと、
前記コンピュータの情報処理ユニットによって、前記処理対象情報が機密情報であるときに前記コンピュータの処理ストラテジー・ユニットによって保存され予め設定された機密情報処理ストラテジーに従って処理を行い、処理済機密情報を作成することと、
前記コンピュータの置換ユニットによって、前記ページ内の前記処理対象情報を、前記処理済機密情報によって置換して、前記処理済機密情報を有するページを作成することと、
を含み、
前記処理対象情報は、
ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報、
を含む機密情報処理方法。
【請求項３】
予め設定された機密情報識別ストラテジーに従って、前記処理対象情報が機密情報であるかどうかを決定することは、
前記ページ・サーバの前記ＭＶＣフレームワーク構造における前記ＭｏｄｅｌＭａｐ内の前記変数情報の変数名を取得することと、
前記ＭｏｄｅｌＭａｐ内の前記変数情報の前記取得された変数名を、前記機密情報ライブラリ内に保存された機密情報と比較し、前記変数名が前記機密情報ライブラリ内にあるかどうかを決定することと、
前記変数名が前記機密情報ライブラリ内にあるかどうかの前記決定の結果により、前記処理対象情報が、前記機密情報であるかどうかを決定することと、
を含む請求項２に記載の機密情報処理方法。
【請求項４】
前記コンピュータの処理対象機密情報ユニットによって、前記ページ・サーバの前記ＭＶＣフレームワーク構造における前記ＭｏｄｅｌＭａｐ内の前記変数情報の値が処理対象機密情報であるどうかを、予め設定された機密情報モニタリング・ストラテジーに従って決定することと、
前記コンピュータの送信ユニットによって、前記変数情報の前記値が処理対象機密情報であると、前記機密情報モニタリング・ストラテジーに従って決定されるときには、前記変数情報の前記値に対応する変数名を前記機密情報ライブラリに送ることと、
を更に含む請求項３に記載の機密情報処理方法。
【請求項５】
予め設定された機密情報処理ストラテジーに従って処理を実行することは、
様々の変数名に対応する値に対する機密情報処理ストラテジーを、前記変数情報における前記様々の変数名に応じて設定すること、または、
同一の変数名に対応する値のための機密情報処理ストラテジーを、指定されたフィールド情報の特権により、前記同一の変数名において設定すること、
を含む請求項２に記載の機密情報処理方法。
【請求項６】
前記機密情報処理ストラテジーは、
処理無し、
所定の部分の表示、

マスキングの完遂、
特権に基づくマスキング、
変換後の表示、及び
誤報、
のうちの少なくとも１つを含む請求項５に記載の機密情報処理方法。
【請求項７】
ページ内の処理対象情報を取得する情報収集ユニットと、
機密情報を保存する機密情報ライブラリと、
前記処理対象情報が機密情報であるかどうかを、前記機密情報ライブラリに保存される前記機密情報に基づいて決定する機密情報識別ユニットと、
機密情報処理ストラテジーを保存する処理ストラテジー・ユニットと、
前記処理対象情報が機密情報であると前記機密情報識別ユニットが決定すると、前記処理ストラテジー・ユニットによって保存される前記機密情報処理ストラテジーに基づいて前記処理対象情報を処理して、処理済機密情報を作成する情報処理ユニットと、
を含み、
前記情報収集ユニットによって取得された前記処理対象情報は、
ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報、を含む、機密情報処理を実現するための装置。
【請求項８】
前記処理ストラテジー・ユニットによって保存される前記機密情報処理ストラテジーは、
様々の変数名に対応する値について、前記変数情報における前記様々の変数名に応じて設定される機密情報処理ストラテジー、または
指定されたフィールド情報の特権により、同一の変数名に対応する値のために、前記変数情報の前記同一の変数名において設定された、機密情報処理ストラテジー、
を含む、請求項７に記載の、機密情報処理を実現するための装置。
【請求項９】
前記処理ストラテジー・ユニットは、
所定の表示ルールに従って前記変数名に対応する値の特定のフィールドを表示する所定部分表示ユニット、
所定のマスキング・ルールに従って前記変数名に対応する前記値の全てのフィールドをマスクする完全マスキング・ユニット、
指定されたフィールドの特権によって、前記変数名に対応する前記値を処理する特権に基づくマスキング・ユニット、
所定の変換ルールに従って前記変数名に対応する前記値を変換し、前記変換された値を前記変数名の前記値として使用する変換・表示ユニット、及び
前記機密情報処理を実現するための装置内の構造化モジュールのうちの何れか１つが異常であるとき、または、前記機密情報識別ユニットによって識別された前記機密情報が、サードパーティ・モジュールによって設定された機密情報決定基準に従っていないときには、前記変数名に対応する前記値の処理をスキップし、誤報ログを生成する誤報ユニット、
のうちの少なくとも１つを含む、請求項８に記載の、機密情報処理を実現するための装置。
【請求項１０】
前記機密情報識別ユニットは、
前記ページ・サーバの前記ＭＶＣフレームワーク構造における前記ＭｏｄｅｌＭａｐ内の前記変数情報の変数名を取得するキー値取得ユニットと、
前記ＭｏｄｅｌＭａｐにおける前記変数情報の前記取得された変数名が前記機密情報ライブラリに保存された前記機密情報と同一であるかどうかについて比較を行う比較ユニットと、

前記比較ユニットの比較結果によって、前記処理対象情報が機密情報であるかどうかについて決定する第１の決定ユニットと
を含む、請求項７に記載の、機密情報処理を実現するための装置。
【請求項１１】
予め設定された機密情報モニタリング・ストラテジーを保存するモニタリング・ストラテジー・ユニットと、
前記予め設定された機密情報モニタリング・ストラテジーに従って、前記ページ・サーバの前記ＭＶＣフレームワーク構造における前記ＭｏｄｅｌＭａｐ内の前記変数情報の値が処理対象機密情報であるかどうかについて決定する処理対象機密情報ユニットと、
前記変数情報の前記値が処理対象機密情報であると前記処理対象機密情報ユニットが決定すると、前記変数情報の前記値に対応する変数名を前記機密情報ライブラリへ送る送信ユニットと
を更に含む、請求項７に記載の、機密情報処理を実現するための装置。
【請求項１２】
インターセプタを用いることにより、サーバ、または前記サーバの処理済機密情報受信ユニットへ前記処理済機密情報を直接送るリターン・ユニット、
を更に含む、請求項７に記載の、機密情報処理を実現するための装置。
【請求項１３】
前記ページ内の前記処理対象情報を前記処理済機密情報によって置き換える置換ユニット、
を更に含む、請求項７に記載の、機密情報処理を実現するための装置。
【請求項１４】
クライアント端末によって送られたＨＴＴＰ要求を受け取り、前記ＨＴＴＰ要求に従ってページ・テンプレートＭｏｄｅｌＭａｐを生成し、処理対象情報を前記生成されたページ・テンプレートＭｏｄｅｌＭａｐへ送り込み、前記ＨＴＴＰ要求に対応するページのレンダリングを完遂し、前記レンダリング済みのページを前記クライアント端末に送り、機密情報処理モジュールによって送られた処理済機密情報を受け取り、前記ページ・テンプレートＭｏｄｅｌＭａｐにおける、対応する処理対象情報を、前記処理済機密情報に置き換えるＭＶＣターゲット・システムと、
前記ページ・テンプレートＭｏｄｅｌＭａｐにおける処理対象情報を取得し、前記処理対象情報を前記機密情報処理モジュールへ送り、前記機密情報処理モジュールによって送られた処理済機密情報を受け取り、前記処理済機密情報を前記ＭＶＣターゲット・システムへ送るインターセプタと、
前記処理対象情報を受け取り、前記処理対象情報が機密情報かどうかを決定し、予め設定された機密情報処理ストラテジーに従って機密情報であると決定された前記処理対象情報を処理して処理済機密情報を作成する前記機密情報処理モジュールと、
を含む、機密情報処理を実現するためのサーバであって、
前記機密情報処理モジュールは、
処理対象情報を受け取る情報受信ユニットと、
機密情報を保存する第１の機密情報ライブラリと、
前記第１の機密情報ライブラリに保存された前記機密情報に基づいて、前記処理対象情報が機密情報であるかどうかを決定する第１の機密情報識別ユニットと、
前記機密情報処理ストラテジーを保存する第１の処理ストラテジー・ユニットと、
前記処理対象情報が機密情報であると前記第１の機密情報識別ユニットが決定すると、前記第１の処理ストラテジー・ユニットによって保存された前記機密情報処理ストラテジーに基づいて、前記処理対象情報を処理して処理済機密情報を作成する第１の情報処理ユニットと、
前記インターセプタへ前記処理済機密情報を送る第１のリターン・ユニットと、
を含む、機密情報処理を実現するためのサーバ。
【請求項１５】

前記ページ・テンプレートＭｏｄｅｌＭａｐ内の処理対象情報を前記インターセプタによって取得することは、
前記ページ・テンプレートＭｏｄｅｌＭａｐ内の処理対象情報を、前記インターセプタのｐｏｓｔＨａｎｄｌｅまたはａｆｔｅｒＣｏｍｐｌｅｔｉｏｎ処理プログラムを用いて取得すること、
を含む、請求項１４に記載の、機密情報処理を実現するためのサーバ。
【請求項１６】
前記第１の処理ストラテジー・ユニットは、
所定の表示ルールに従って変数名に対応する値の特定のフィールドを表示する第１の所定部分表示ユニット、
所定のマスキング・ルールに従って前記変数名に対応する前記値の全てのフィールドをマスクする第１の完全マスキング・ユニット、
指定されたフィールドの特権によって前記変数名に対応する前記値を処理する第１の特権に基づくマスキング・ユニット、
所定の変換ルールに従って前記変数名に対応する前記値を変換し、前記変換された値を前記変数名の前記値として使用する第１の変換・表示ユニット、及び
機密情報処理を実現するための装置内の構造化モジュールのうちの何れか１つが異常であるとき、または、機密情報識別ユニットによって識別された前記機密情報が、サードパーティ・モジュールによって設定された機密情報決定基準に従っていないときには、前記変数名に対応する前記値の処理をスキップし、誤報ログを生成する第１の誤報ユニット、
のうちの少なくとも１つを含む、請求項１４に記載の、機密情報処理を実現するためのサーバ。
【請求項１７】
前記第１の機密情報識別ユニットは、
前記ＭＶＣターゲット・システム内の前記ＭｏｄｅｌＭａｐにおける変数情報の変数名を取得する第１のキー値取得ユニットと、
前記ＭｏｄｅｌＭａｐにおける前記変数情報の前記取得された変数名が前記第１の機密情報ライブラリに保存された前記機密情報と同一であるかどうかについて比較する第１の比較ユニットと、
前記第１の比較ユニットの比較結果によって、前記処理対象情報が機密情報であるかどうかを決定する第２の決定ユニットと、
を含む、請求項１４に記載の、機密情報処理を実現するためのサーバ。
【請求項１８】
予め設定された機密情報モニタリング・ストラテジーを保存する第１のモニタリング・ストラテジー・ユニットと、
前記ＭＶＣターゲット・システム内の前記ＭｏｄｅｌＭａｐにおける変数情報の値が処理対象機密情報であるどうかを、前記予め設定された機密情報モニタリング・ストラテジーに従って決定する第１の処理対象機密情報ユニットと、
前記変数情報の前記値が処理対象機密情報であると前記第１の処理対象機密情報ユニットが決定するときに、前記変数情報の前記値に対応する変数名を、前記第１の機密情報ライブラリへ送る第１の送信ユニットと、
を更に含む、請求項１４に記載の、機密情報処理を実現するためのサーバ。
【請求項１９】
機密情報を保存し、第２の処理対象機密情報ユニットによって送られた変数名を受け取り、前記保存された機密情報が前記受け取った変数名を含むかどうかを決定し、前記決定の結果が第２の機密情報ライブラリが前記受け取った変数名を含まないということであるときには、新規追加機密情報として前記変数名を保存する前記第２の機密情報ライブラリと、
ページ内の処理対象情報を取得し、前記処理対象情報が機密情報かどうかを前記第２の機密情報ライブラリに保存された前記機密情報に基づいて決定する第２の機密情報識別ユ

ニットと、
機密情報処理ストラテジーを保存し、更に、前記処理対象情報が機密情報であると前記第２の機密情報識別ユニットが決定するときには、前記保存された機密情報処理ストラテジーに基づいて前記処理対象情報を処理して処理済機密情報を作成する第２の情報処理ユニットと、
予め設定された機密情報モニタリング・ストラテジーを保存し、ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報の値が処理対象機密情報であるどうかを前記保存された機密情報モニタリング・ストラテジーに従って決定し、前記変数情報の前記値が処理対象機密情報であると決定するときには、前記変数情報の前記値に対応する変数名を前記第２の機密情報ライブラリへ送るモニタリング・ユニットと、
前記第２の機密情報ライブラリ内の新規追加機密情報の数を含む新規追加機密情報ログを生成する新規追加機密情報ログ・ユニットと、
前記モニタリング・ユニットによって決定された処理対象機密情報の数を含む処理対象機密情報ログを生成する処理対象機密情報ログ・ユニットと、
第１のターゲット・システムにおける前記新規追加機密情報ログまたは前記処理対象機密情報ログまたは前記第２の機密情報ライブラリ内のデータを取得し、前記第１のターゲット・システムが属するセキュリティ・レベルを、予め設定された決定ルールに従って決定する第１のセキュリティ決定ユニットと、
を有するセキュリティ決定システム。
【請求項２０】
前記第１のセキュリティ決定ユニットは、
第１の時間窓の範囲内における新規追加機密情報の数／前記第２の機密情報ライブラリ内に保存された前記機密情報の数によって、前記第１のターゲット・システムの前記セキュリティ・レベルを決定する第１の数決定ユニット、及び
第２の時間窓の範囲内における新規追加機密情報の数の前記処理対象機密情報の数に対する比によって、前記第１のターゲット・システムの前記セキュリティ・レベルを決定する第１の比決定ユニット、
のうちの少なくとも１つを含む、請求項１９に記載のセキュリティ決定システム。
【請求項２１】
予め設定された決定ルールに従って前記第１のターゲット・システムの前記セキュリティ・レベルを第２のターゲット・システムのそれと比較するマルチシステム決定ユニットを更に含み、
前記第１のセキュリティ決定ユニットは、前記新規追加機密情報ログ、または、処理対象機密情報ログ、または、前記第２のターゲット・システムの前記第２の機密情報ライブラリ内のデータを取得する請求項２０に記載のセキュリティ決定システム。
【請求項２２】
前記マルチシステム決定ユニットは、
前記第１の時間窓の範囲内における前記第１のターゲット・システム及び前記第２のターゲット・システムの前記新規追加機密情報の数／前記第２の機密情報ライブラリに保存された前記機密情報の数によって前記第１のターゲット・システム及び前記第２のターゲット・システムの前記セキュリティ・レベルを比較する第２の数決定ユニット、及び
前記第２の時間窓の範囲内における前記第１のターゲット・システムの前記新規追加機密情報の数の前記処理対象機密情報の数に対する比、及び、前記第２のターゲット・システムの前記新規追加機密情報の数の前記処理対象機密情報の数に対する比によって、前記第１のターゲット・システムの前記セキュリティ・レベル及び前記第２のターゲット・システムの前記セキュリティ・レベルを比較する第２の比決定ユニット、
のうちの少なくとも１つを含む請求項２１に記載のセキュリティ決定システム。
【発明の詳細な説明】
【技術分野】
【０００１】

本出願は、情報通信の分野に関し、特に、コンピュータ・ページ情報インタラクションにおける機密情報処理方法、装置、及び、サーバ、ならびに、セキュリティ決定システムに関する。

【背景技術】

【０００２】

情報技術が発達するにつれ、インターネットから情報を取得することは人々にとって重要な情報収集手段になった。そこでは、主要な手段は、クライアント端末のユーザが閲覧するために、サーバがＨＴＴＰ要求に応答し、要求されたページ情報をクライアント端末に返すように、クライアント端末上でブラウザを用いてＨＴＴＰページ要求をサーバに送信することを含む。

【０００３】

サーバによって返されるページは、一般に、ユーザに関連した機密情報（例えば、ユーザの、アカウント名、メール・アドレス、携帯電話番号、及び、身分証明カード情報）を含む。ページのソースコードを見ること、ウェブ上でウェブ・データ・パケットをクローリングさせること等によって、不法ユーザは容易にページ内の機密情報を取得することができ、結果としてユーザ情報の漏洩をもたらす。例えば、「ｍａｉｌｔｏ：」の後の情報または「@」の前後の情報はネットワーク・ツールを用いてページ情報から抽出され得、ページ内の電子メール情報を抽出する目的を達成し得る。

【０００４】

従来の技術では、機密情報を処理するための一般的な方法は、例えば、ページに埋め込まれたＪａｖａＳｃｒｉｐｔ（登録商標）のスクリプトを用いて機密を暗号化しマスクすることによる、或いは、不法ユーザが、サーバによって返されたページ内のパケットを取得することを防ぐことによるような処理方法を含む。例えば、電子メール機密情報は、ＡＳＣＩＩコード化された文字列に変換され、それから、ＪａｖａＳｃｒｉｐｔのスクリプト言語におけるｄｏｃｕｍｅｎｔ．ｗｒｉｔｅメソッドを用いてページに書き込まれ得る。こうして、電子メール機密情報の処理を完遂する。

【０００５】

しかし、従来の技術では、サーバによって返されたページ内の機密情報は、一般に、ＪａｖａＳｃｒｉｐｔのスクリプトによる列を有しないオリジナルの機密情報である。更に、もし、このページ内の機密情報に対してＪａｖａＳｃｒｉｐｔのスクリプトが実行されたならば、不法ユーザは、例えば、クライアント端末上のＪａｖａＳｃｒｉｐｔのスクリプトを削除する、または、対応するＪａｖａＳｃｒｉｐｔのスクリプトの実行を止めるというような容易な手段によって、依然として、このページ内の機密情報を取得し得る。したがって、従来の技術における、ページ機密情報の処理のための一般的な方法は、ページ内の機密情報のセキュリティ低下を引き起こす。

【発明の概要】

【０００６】

本出願の目的は、ページ内の機密情報のセキュリティを改善し得る、機密情報処理方法、装置、及び、サーバ、ならびに、セキュリティ決定システムを提供することである。

【０００７】

本出願において提供される、機密情報処理方法、装置、及び、サーバ、ならびに、セキュリティ決定システムは、以下のように実装される。

【０００８】

ページ内の処理対象情報を取得することと、

予め設定された機密情報識別ストラテジーに従って、前記処理対象情報が機密情報であるかどうかを決定することと、

前記処理対象情報が機密情報であるときに予め設定された機密情報処理ストラテジーに従って処理を行い、処理済機密情報を作成することと、

前記ページ内の対応する前記処理対象情報を、前記処理済機密情報によって置換して、前記処理済機密情報を有するページを作成することと、

を含む機密情報処理方法。
【０００９】
ページ内の処理対象情報を取得する情報収集ユニットと、
機密情報を保存する機密情報ライブラリと、
前記処理対象情報が機密情報であるかどうかを、前記機密情報ライブラリに保存される前記機密情報に基づいて決定する機密情報識別ユニットと、
機密情報処理ストラテジーを保存する処理ストラテジー・ユニットと、
前記処理対象情報が機密情報であると前記機密情報識別ユニットが決定すると、前記処理ストラテジー・ユニットによって保存される前記機密情報処理ストラテジーに基づいて前記処理対象情報を処理して、処理済機密情報を作成する情報処理ユニットと、
を含む、機密情報処理を実現するための装置。
【００１０】
クライアント端末によって送られたＨＴＴＰ要求を受け取り、このＨＴＴＰ要求に従ってページ・テンプレートＭｏｄｅｌＭａｐを生成し、処理対象情報を前記生成されたページ・テンプレートＭｏｄｅｌＭａｐへ送り込み、前記ＨＴＴＰ要求に対応するページのレンダリングを完遂し、前記レンダリング済みのページを前記クライアント端末に送り、機密情報処理モジュールによって送られた処理済機密情報を受け取り、前記ページ・テンプレートＭｏｄｅｌＭａｐにおける、対応する処理対象情報を、前記処理済機密情報に置き換えるＭＶＣターゲット・システムと、
前記ページ・テンプレートＭｏｄｅｌＭａｐにおける処理対象情報を取得し、この処理対象情報を前記機密情報処理モジュールへ送り、更に、前記機密情報処理モジュールによって送られた処理済機密情報を受け取り、前記処理済機密情報を前記ＭＶＣターゲット・システムへ送るインターセプタと、
前記処理対象情報を受け取り、この処理対象情報が機密情報かどうかを決定し、予め設定された機密情報処理ストラテジーに従って機密情報であると決定された前記処理対象情報を処理して処理済機密情報を作成する機密情報処理モジュールと、
を含む、機密情報処理を実現するためのサーバであって、
前記機密情報処理モジュールは、
処理対象情報を受け取る情報受信ユニットと、
機密情報を保存する第１の機密情報ライブラリと、
前記第１の機密情報ライブラリに保存された前記機密情報に基づいて、前記処理対象情報が機密情報であるかどうかを決定する第１の機密情報識別ユニットと、
前記機密情報処理ストラテジーを保存する第１の処理ストラテジー・ユニットと、
前記処理対象情報が機密情報であると前記第１の機密情報識別ユニットが決定すると、前記第１の処理ストラテジー・ユニットによって保存された前記機密情報処理ストラテジーに基づいて、前記処理対象情報を処理して処理済機密情報を作成する第１の情報処理ユニットと、
前記インターセプタへ前記処理済機密情報を送る第１のリターン・ユニットと、
を含む、機密情報処理を実現するための前記サーバ。
【００１１】
機密情報を保存し、第２の処理対象機密情報ユニットによって送られた変数名を受け取り、前記保存された機密情報が前記受け取った変数名を含むかどうかを決定し、前記決定の結果が、前記機密情報ライブラリが前記受け取った変数名を含まないということであるときには、新規追加機密情報として前記変数名を保存する第２の機密情報ライブラリと、
ページ内の処理対象情報を取得し、前記処理対象情報が機密情報かどうかを前記第２の機密情報ライブラリに保存された前記機密情報に基づいて決定する第２の機密情報識別ユニットと、
機密情報処理ストラテジーを保存し、更に、前記処理対象情報が機密情報であると前記第２の機密情報識別ユニットが決定するときには、前記保存された機密情報処理ストラテジーに基づいて前記処理対象情報を処理して処理済機密情報を作成する第２の情報処理ユ

ニットと、
予め設定された機密情報モニタリング・ストラテジーを保存し、前記ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報の値が処理対象機密情報であるどうかを前記保存された機密情報モニタリング・ストラテジーに従って決定し、前記変数情報の前記値が処理対象機密情報であると決定するときには、前記変数情報の前記値に対応する変数名を前記第２の機密情報ライブラリへ送るモニタリング・ユニットと、
前記第２の機密情報ライブラリ内の新規追加機密情報の数を含む新規追加機密情報ログを生成する新規追加機密情報ログ・ユニットと、
前記モニタリング・ユニットによって識別された処理対象機密情報の数を含む処理対象機密情報ログを生成する処理対象機密情報ログ・ユニットと、
第１のターゲット・システムにおける前記新規追加機密情報ログまたは前記処理対象機密情報ログまたは前記第２の機密情報ライブラリ内のデータを取得し、前記第１のターゲット・システムが属するセキュリティ・レベルを、予め設定された決定ルールに従って決定する第１のセキュリティ決定ユニットと、
を有するセキュリティ決定システム。
【００１２】
本出願は、機密情報処理方法、装置、及び、サーバ、ならびに、セキュリティ決定システムを提供する。処理対象情報はページ・サーバ端末上で取得される場合があり、処理対象情報が機密情報であるどうかを所定の機密情報識別ストラテジーに従って決定する。処理対象情報が機密情報であるときは、処理済機密情報は、予め設定された機密情報ストラテジーに従って処理され得る。それから、処理済機密情報はページへ戻され、処理済機密情報を有するページを作成する。クライアント端末によって受け取られたページは、機密情報がサーバ端末で処理されたページであり、クライアント端末の不法ユーザは、データ・パケットを捕えることによっても、ＪａｖａＳｃｒｉｐｔのスクリプトを削除することによっても、このページ内の本当の機密情報を取得することはできない。このように、このページの機密情報のセキュリティは改善される。
【００１３】
本出願の実施形態または従来の技術における技術的な解決策をより明確に記述するために、実施形態または従来の技術を記述するために必要な添付図面について以下に簡単に紹介する。明らかに、以下の説明において添付図面は単に本出願の幾つかの実施形態のみのものであり、当業者は、これらの添付図面によって創造的な努力無しで他の図面を得ることができる。
【図面の簡単な説明】
【００１４】
【図１】本出願によるユーザとサーバとの間のインタラクションの概略フロー図であり、サーバがＭＶＣフレームワーク・ページ構造を使用するものである。
【図２】本出願による機密情報処理方法の実施形態の方法のフロー図である。
【図３】本出願による機密情報処理方法の他の１つの実施形態のフロー図である。
【図４】本出願による機密情報処理を実現するための装置の１つの実施形態の概略モジュール構成図である。
【図５】本出願による機密情報処理を実現するための装置の機密情報識別ユニットの概略モジュール構成図である。
【図６】本出願による機密情報処理を実現するための装置の処理ストラテジー・ユニットの概略モジュール構成図である。
【図７】本出願による機密情報処理を実現するための装置の他の１つの実施形態の概略モジュール構成図である。
【図８】本出願による機密情報処理を実現するための装置の他の１つの実施形態の概略モジュール構成図である。
【図９】本出願による機密情報処理を実現するための装置の他の１つの実施形態の概略モ

ジュール構成図である。
【図１０】本出願による機密情報処理を実現するためのサーバの他の１つの実施形態の概略モジュール構成図である。
【図１１】本出願によるセキュリティ決定システムの実施形態の概略モジュール構成図である。
【図１２】本出願によるセキュリティ決定システムの他の１つの実施形態の概略モジュール構成図である。
【発明を実施するための形態】
【００１５】
当業者が本出願における技術的な解決策をより良く理解できるようにするために、本出願の実施形態の技術的な解決策は、本出願の実施形態の添付の図面を参照して、以下に明確、且つ、完全に記述されるであろう。明らかに、記述された実施形態は、本出願の実施形態のうちの幾らかだけであって、全てではない。本出願の実施形態に基づいて当業者によって創造的な努力無しで得られる他の全ての実施形態は、本出願の保護範囲に含まれる。
【００１６】
ＭＶＣフレームワークは、ウェブ・サーバにより一般に用いられるウェブ・アプリケーションの設計及び創造モードである。ここでは、ソフトウェアのサービス・ロジック、データ、及び、インターフェース表示がモデル・ビュー・コントローラ（ＭＶＣ）を用いて分離される。ここで、モデル（Ｍｏｄｅｌ）は、アプリケーションンのサービス・ロジックに関連したデータとデータ処理方法とをカプセル化するために用いられることができ、例えば、データベースにアクセスするというような、直接データにアクセスするという利点を一般に有する。ビュー（Ｖｉｅｗ）は、データを表示するために用いられることができ、一般に、アプリケーションの、ユーザ・インターフェース（例えば、ユーザが閲覧することができ、それと対話し得るページ・インターフェース）に関連する一部分である。一般に、ビューはモデル・データによって作られ得る。コントローラ（Ｃｏｎｔｒｏｌｌｅｒ）は、様々のレベルを組織するために機能し、イベントを処理して応答するために用いられ得る。ＭＶＣフレームワーク・モードの３つのモジュールは互いに独立していることができ、それらのうち１つが変更されても他の２つに影響を及ぼさないようにでき、１つのモデルが様々のビューによって繰り返し用いられ得る。例えば、ユーザＡはブラウザによって電子メールを送受信することを欲し、また、携帯電話によってメールボックスにアクセスすることを欲する。ＭＶＣフレームワーク設計モードは、サーバ端末上で使用されることができ、モデルは、ユーザの要求に応答して応答を返すことができ、ビューは、データをフォーマット化して、フォーマット化したデータをインターネット・インターフェース及びユーザ・ページのＷＡＰインターフェースへ提供し得る。
【００１７】
図１はユーザとサーバとの間のインタラクションの概略フロー図である。ここで、サーバはＭＶＣフレームワークのページ構造を使用する。図１に示すように、ユーザはクライアント端末のブラウザによって、ＨＴＴＰ要求をサーバに送信し得る。ＭＶＣフレームワーク・モードを使用するウェブ・サーバが、ブラウザを介してユーザによって送信されたＨＴＴＰ要求を取得すると、ウェブ・サーバはＨＴＴＰ要求に従って対応するページ・モデルを生成し、生成されたページ・モデルのレンダリングを行う。ページ・モデルは、一般に、ページ設計開発者によって前もって設計されたものか、または、システムに保存されたページ・テンプレート（ＭｏｄｅｌＭａｐ）であり得る。ページ・テンプレートは変数情報を含み得る。ページ・モデルのレンダリングは、コントローラを用いてページ・テンプレート内の変数情報を見つけることと、ページ・モジュール内の変数を、ユーザのＨＴＴＰ要求に従って、対応する実データによって置き換えることとを含み得る。ページ・テンプレート（ＭｏｄｅｌＭａｐ）のレンダリングを完遂した後、サーバは、レンダリングされたページをユーザに返すことができる。そして、ビュー・モジュール（Ｖｉｅｗ）は、ユーザのクライアント端末上で、レンダリングされたページの表示インターフェース

を制御し得る。

【００１８】

本出願は機密情報処理方法を提供する。この機密情報処理方法は、ユーザのクライアント端末によって受け取られるページに含まれる機密情報が、サーバ端末で対応して処理された機密情報であるように、サーバがユーザにページを返す前にユーザの機密情報を処理し得る。図２は、本出願による機密情報処理方法の実施形態の方法のフロー図である。図２に示すように、機密情報処理方法は、以下のものを含み得る。

【００１９】

Ｓ１：ページ内の処理対象情報が取得される。

【００２０】

処理対象情報はページ・サーバのフレームワーク構造に従って設定され得る。この実施形態における処理対象情報は、ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報を含み得る。ユーザ端末によって送信されたＨＴＴＰ要求を受け取ると、ページ・サーバは、空白のＭｏｄｅｌＭａｐのページ・テンプレートを作成し得る。ページ・テンプレートＭｏｄｅｌＭａｐは、ＭＶＣフレームワーク構造における保存構造であってよく、ユーザ端末へ戻されることが必要な情報をページに保存するために用いられ得る。上記の説明では、ページ・テンプレートＭｏｄｅｌＭａｐは変数を含んでよく、変数のデータフォーマットは、一般に、変数名（ｋｅｙ）と値とを含むキー・値対データフォーマットｍａｐ（ｋｅｙ：ｖａｌｕｅ）である。ここで、変数の値「ｖａｌｕｅ」は、一般に、初期値を表すために、ヌル値またはデフォルト文字列を使用する場合がある。コントローラ・フェーズにおいては、ＭｏｄｅｌＭａｐ．ｐｕｔ（）オペレーションを用いて、ＭｏｄｅｌＭａｐ内の変数にデータが入れられ得る。例えば、ＭｏｄｅｌＭａｐに設定される変数は（ｎａｍｅ１：ｖａｌｕｅ）であり、変数「ｎａｍｅ１」の値「Ｚｈａｎｇ　ｓａｎ」は、ＭｏｄｅｌＭａｐ．ｐｕｔ（"ｎａｍｅ１", "Ｚｈａｎｇ　ｓａｎ"）のようなオペレーションによって、ＭｏｄｅｌＭａｐ内の変数「ｎａｍｅ１」に入れられ得る。

【００２１】

この実施形態では、データがＭｏｄｅｌＭａｐ内の変数に入れられた後、ＭｏｄｅｌＭａｐのデータが取得され得る。このことは、この実施形態では、ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報を取得すること、及び、前記ページ内の処理対象情報としてＭｏｄｅｌＭａｐ内の変数情報を用いることとして言及する場合がある。本出願の機密情報処理方法では、ページ・サーバがデータをページ内の変数に入れている間に上記変数情報が取得され得ること、或いは、ページ・サーバが前記ページ内の全ての変数にデータを入れ終わった後にページ内の変数情報が取得され得ることに留意すべきである。この実施形態では、ＭＶＣフレームワーク構造を用いるページ・サーバにおいて、ＭＶＣフレームワークが全ての変数のデータをＭｏｄｅｌＭａｐに入れ終わった後で変数情報が取得され得、処理対象情報として用いられる。

【００２２】

本出願の他の１つの実施形態について、図３は本出願による機密情報処理方法の他の１つの実施形態の概略フロー図である。図３に示すように、機密情報処理方法においては、前記ページ内の処理対象情報を取得することは、インターセプタのｐｏｓｔＨａｎｄｌｅ処理プログラムを用いてＭＶＣフレームワークにおける変数情報を取得することと、この取得された変数情報を前記処理対象情報として使用することとを含み得る。具体的には、これは以下のことを含み得る。

【００２３】

ＭＶＣフレームワークのコントローラ・フェーズにおいて、ページ・サーバが変数情報を（変数名：値）の形でＭｏｄｅｌＭａｐ内の変数に入れる。ＭｏｄｅｌＭａｐ内の全ての変数に変数情報を入れ終わった後に、ＭＶＣフレームワークは、ＭｏｄｅｌＭａｐデータをインターセプタに送り得る。そして、インターセプタのｐｏｓｔＨａｎｄｌｅ処理プログラムは、ＭＶＣフレームワークによって送られたＭｏｄｅｌＭａｐデータを受け取る

。ｐｏｓｔＨａｎｄｌｅ処理プログラムは、ＭｏｄｅｌＭａｐ内の変数情報を吟味して、ＭｏｄｅｌＭａｐ内の変数を取得し、取得された変数情報を処理対象情報として用いてよい。

【００２４】

インターセプタは、一般に、アプリケーションの実行ステップまたはフィールドがアクセスされる前に、アクセス元をインターセプトするために用いられ得、インターセプトの前または後に特定の処理ステップを実行し得る。ＭＶＣフレームワーク構造では、インターセプタは３つの処理方法を含み得る。

【００２５】

ｐｒｅＨａｎｄｌｅ（）――コントローラが呼び出される前に呼び出され、初期化オペレーションのため、または、要求を前処理するために用いられ得る。

ｐｏｓｔＨａｎｄｌｅ（）――コントローラが呼び出された後であってビューが実行される前に呼び出され、モデル・データを処理するため、または、ビューのために用いられ得る。

ａｆｔｅｒＣｏｍｐｌｅｔｉｏｎ（）――ビューが提供された後で呼び出され、リソースをクリーンアップするために用いられ得る。

【００２６】

一般に、インターセプタの処理方法は、対応する処理ユニットによって実現され得る。例えば、ｐｒｅＨａｎｄｌｅ処理フェーズはインターセプタの物理的装置のｐｒｅＨａｎｄｌｅｒによって実行され得、当然、ｐｏｓｔＨａｎｄｌｅ処理フェーズはインターセプタの物理的装置のｐｏｓｔＨａｎｄｌｅｒによって実行され得る。

【００２７】

図３に示すように、一般に、ｐｒｅＨａｎｄｌｅフェーズではデータがＭｏｄｅｌＭａｐに入れられていないので、処理対象情報、すなわち、この実施形態のＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報、はｐｏｓｔＨａｎｄｌｅフェーズまたはａｆｔｅｒＣｏｍｐｌｅｔｉｏｎフェーズにおいて取得され得る。この実施形態では、好適な方法は以下の通りである。ＭＶＣフレームワーク構造のコントローラが呼び出された後であって、ビューが実行される前に、ページ内の処理対象情報がインターセプタを用いて取得され得、機密情報識別処理に割り込む。具体的には、この実施形態においては、変数データがＭｏｄｅｌＭａｐに入れられた後、インターセプタのｐｏｓｔＨａｎｄｌｅ処理プログラムはＭｏｄｅｌＭａｐ内の変数情報を取得し得る。ＭＶＣフレームワーク構造におけるレンダリング（Ｖｅｌｏｃｉｔｙ）が呼び出された後、確実に、ページ内の処理対象情報がインターセプタを用いて取得され得る。すなわち、処理対象情報はインターセプタのａｆｔｅｒＣｏｍｐｌｅｔｉｏｎフェーズにおいて取得される。

【００２８】

この実施形態においては、インターセプタを用いてＭｏｄｅｌＭａｐ内の変数情報を取得して一部変更する方法は、（例えば、ｗｅｂｘフレームワーク構造のような）ＭＶＣフレームワークに基づく他のフレームワーク構造に適用できる点に留意すべきある。様々のインターセプタが、異なるページ・サーバ・フレームワークのために存在し得る。この実施形態では、ＭＶＣに基づくフレームワーク構造において、前記処理対象情報は、ページのレンダリング（Ｖｅｌｏｃｉｔｙ）の前であってコントローラが呼び出された後に、対応するインターセプタによって取得および処理されることができ、或いは、前記処理対象情報は、ページのレンダリング（Ｖｅｌｏｃｉｔｙ）の後で、対応するインターセプタによって対応するインターセプタによって取得および処理されることができる。好適な実装においては、処理対象情報は、ページのレンダリング（Ｖｅｌｏｃｉｔｙ）の前であってコントローラが呼び出された後に対応するインターセプタによって取得および処理される。

【００２９】

ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報が取得され、ページ内の処理対象情報として用いられる。

【００３０】
Ｓ２：予め設定された機密情報識別ストラテジーに従って、処理対象情報が機密情報であるかどうかが決定される。
【００３１】
機密情報識別ストラテジーは、前記処理対象情報が機密情報であるかどうかを決定するために予め設定された識別ルールまたは方法の組であってよい。例えば、処理対象情報がページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報である場合、機密情報識別ストラテジーは、機密情報を保存する機密情報ライブラリを含み得る。予め設定された機密情報識別ストラテジーに従って前記処理対象情報が機密情報であるかどうかを決定することは、以下のものを含み得る。
【００３２】
Ｓ２０１：ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報の変数名が取得される。
【００３３】
Ｓ２０２：ＭｏｄｅｌＭａｐ内の変数情報の取得された変数名は、機密情報ライブラリに保存された機密情報と比較され、この変数名が機密情報ライブラリにあるかどうかを決定する。
【００３４】
Ｓ２０３：前記変数名が機密情報ライブラリにあるかどうかの決定結果に従って、前記処理対象情報は機密情報であると決定される。
【００３５】
この実施形態では、予め定義された機密情報を含む機密情報ライブラリが設定され得る。例えば、ユーザの、ユーザ名、電話番号、電子メール、及び、ＩＤカード番号情報は、機密情報として予め定義され得る。ＭｏｄｅｌＭａｐにおける、それらの対応する変数名（キー）である、「Ｕｓｅｒ」、「Ｔｅｌ＿Ｎｕｍ」、「Ｅ－Ｍａｉｌ」、及び、「ＩＤ＿Ｎｕｍ」は、機密情報ライブラリに予め保存され得る。ＭｏｄｅｌＭａｐ内の変数情報の変数名が取得された後、取得された変数名は機密情報ライブラリに保存された機密情報と比較され得る。機密情報ライブラリが取得された変数名と同一の機密情報を含むならば、このことは、処理対象情報は機密情報であることを示し得る。すなわち、このことは、この変数名に対応するＭｏｄｅｌＭａｐ内の変数情報がこの実施形態の機密情報であることを示し得る。もし、上記の比較結果が、機密情報ライブラリが取得された変数名と同一の機密情報を含まないということであるならば、このことは、この処理対象情報は機密情報でないことを示し得る。すなわち、この変数名に対応するＭｏｄｅｌＭａｐ内の変数情報がこの実施形態の機密情報ではないことを示し得る。
【００３６】
機密情報ライブラリに保存された機密情報は、追加され得るか、削除され得るか、または、必要に応じて変更され得る。
【００３７】
ページ・サーバのフレームワーク構造が他のフレームワーク・モードに属する場合には、当然、取得された処理対象情報は、そのサーバのフレームワーク構造に対応する他のデータフォーマットを有する場合があり、機密情報識別ストラテジーもまた、処理対象情報及びフレームワーク構造に対応して設定され得る。例えば、処理対象情報のデータの全てが機密情報であるかどうかが直接決定される場合があり、或いは、暗号化対象情報が機密情報であるかどうかが、指定されたデータに基づいて決定される場合がある。
【００３８】
この実施形態のＭＶＣに基づくフレームワーク構造においては、処理対象情報が機密情報であるがどうかが、上記の予め設定された機密情報識別ストラテジーに従って決定される。
【００３９】
Ｓ３：処理対象情報が機密情報であると決定されると、予め設定された機密情報処理ス

トラテジーに従って処理が実行され、処理済機密情報を作成し得る。

【００４０】

決定の結果が、処理対象情報が機密情報であるということであるとき、その処理対象情報は予め設定された機密情報処理ストラテジーに従って処理され得る。機密情報処理ストラテジーは、機密情報として決定された処理対象情報を処理するための予め設定されたルールまたは方法の組を含み得る。この実施形態では、処理対象情報はＭｏｄｅｌＭａｐにおける変数（変数名：値）のデータフォーマットを有するとき、予め設定された機密情報処理ストラテジーに従って処理を実行することは、変数情報内の変数名に対応する値を処理することを含み得る。具体的には、機密情報処理ストラテジーは、非処理、所定の部分の表示、完全なマスキング、特権に基づくマスキング、変換後の表示、及び、誤報のうちの少なくとも１つを含み得る。

【００４１】

非処理は、変数名に対応する値についてマスキング、変換、及び、代入のような処理を実行しないことを含み得る。ここで、変数名に対応する値は変わらない。

【００４２】

所定の部分の表示は、所定の表示ルールに従って、変数名に対応する値の特定のフィールドを表示することを含み得る。例えば、処理対象情報は（Ｔｅｌ＿Ｎｕｍ：１５９１２３４４３２１）であり、所定の表示ルールは、変数名「Ｔｅｌ：Ｎｕｍ」に対応する値の第４～第８の桁を、文字「*」に置き換えることを含み得る。処理対象情報（Ｔｅｌ＿Ｎｕｍ：１５９１２３４４３２１）が、所定のフィールドを表示する前述の処理ストラテジーに従って処理された後に、処理済機密情報（Ｔｅｌ＿Ｎｕｍ：１５９*****３２１)が作成され得る.

【００４３】

完全なマスキングは、所定のマスキング・ルールに従って、変数名に対応する値の全てのフィールドをマスクすることを含み得る。例えば、変数名「Ｔｅｌ：Ｎｕｍ」に対応する値は１つ以上の文字「*」で置き換えられ得る。そして、作成された処理済機密情報は（Ｔｅｌ＿Ｎｕｍ：*）或いは（Ｔｅｌ＿Ｎｕｍ：**********)であり得る。

【００４４】

特権に基づくマスキングは、指定されたフィールドの特権によって、変数名に対応する値を処理することを含み得る。例えば、既知のフィールドは、クライアント端末のユーザの取得されたユーザ名であり、ユーザ名が属する様々のドメイン・グループの特権によって対応する処理方法が設定され得る。具体的には、以下の表１に示すように、ＨＴＴＰ要求を送信したクライアント端末のユーザの容認されている特権によって機密情報は処理され得る。具体的には、例えば、ＨＴＴＰ要求を送信するために受け取ったユーザ名がスーパー・アドミニストレータ・ドメイン・グループに属するときには機密情報の何れもが処理されないように設定され得る。ＨＴＴＰ要求を送信するためのユーザ名がアドミニストレータ・ドメイン・グループに属するときには指定された機密情報が部分的にマスクされるように設定され得る。ＨＴＴＰ要求を送信するためのユーザ名がユーザ・ドメイン・グループに属するときには指定された機密情報が完全にマスクされるか、部分的にマスクされるように設定され得る。

【００４５】

【表１】

表１　特権に基づくマスキング処理ストラテジーの概念テーブル

変数名	値	ドメイン・グループ	処理ストラテジー	処理後の値
Name1	Zhang san	スーパー・アドミニストレータ	非処理	Zhang san
Name2	Li si	アドミニストレータ	部分的な表示	Li*
Name3	Wang wu	ユーザ	マスキング	**
Tel_Num	15912344321	ユーザ	部分的な表示	159*****321
E-Mail	user1@163.com	ユーザ	部分的な表示	use**@163.com
ID_Num	320322198708081234	アドミニストレータ	マスキング	320****
Add_ID	Hangzhou, Zhejiang Province	ユーザ	部分的な表示	Zhejiang Province
Gender	Female	ユーザ	非処理	Female

【００４６】

変換後の表示は、所定の変換ルールに従って変数名に対応する値を変換して、変数名の値として変換された値を使用することを含み得る。例えば、ＭｏｄｅｌＭａｐ内の第４の変数（Ｎａｍｅ４：ｅｖｉｌ）の値「ｅｖｉｌ」は、所定のルールに従って「ｌｉｖｅ」に変換され、それから、第４の変数の処理された値として用いられる。すなわち、処理済機密情報は（Ｎａｍｅ４：ｌｉｖｅ）であり得る。

【００４７】

機密情報識別ルールが異常であるか、または、識別された機密情報が、他の条件に従って設定された機密情報決定基準に従わないときは、変数名に対応する値に対して処理オペレーションを実行しないこととして、誤報は表現され得る。この場合、誤報ログが生成され得る。誤報ログは、生成された誤報の数、各誤報の（例えば、元の変数名及び値のような）ターゲット・ソース、誤報の原因、ログ生成時間等を保存及び記録し得る。この実施形態では、生成された誤報ログが保存されることができ、その後の挙動の統計のために用いられ得る。

【００４８】

特定の実行の間、機密情報処理ストラテジーは、必要に応じて、組み合わせて、或いは、入れ子にして設定され得る。例えば、予め設定された機密情報処理ストラテジーに従って処理を実行することは、

変数情報における様々の変数名によって、これら様々の変数名に対応する値のために機密情報処理ストラテジーを設定すること、または、

指定されたフィールド情報の特権により、同一の変数名に対応する値のための機密情報処理ストラテジーを、変数情報の同一の変数名において設定すること、

を含み得る。

【００４９】

特定の例においては、ユーザのユーザ名、電話番号、電子メール、及び、アイデンティティ・カード番号情報は機密情報として予め定義されることができ、ＭｏｄｅｌＭａｐにおける、それらの対応する変数名（キー）は「Ｕｓｅｒ」、「Ｔｅｌ＿Ｎｕｍ」、「Ｅ－Ｍａｉｌ」、及び、「ＩＤ＿Ｎｕｍ」である。機密情報処理ストラテジーの設定の間、機密情報の予め設定されたセキュリティ・レベルに従って、ユーザ名の変数名「Ｕｓｅｒ」に対応する値の最初の２つの文字だけが、所定の部分を表示する処理ストラテジーに従って表示され得る。ここで、残りは文字「*」で置き換えられる。ユーザの電子メールの変数名「Ｅ－Ｍａｉｌ」に対応する値における文字「@」及び「@」の後の文字のみが、所

定の部分を表示する処理ストラテジーに従って表示される。比較的に重要である、ユーザのアイデンティティ・カード番号のために、アイデンティティ・カード番号の変数名「ＩＤ＿Ｎｕｍ」に対応する値の全ては、完全なマスキングの処理ストラテジーに従って４つの文字「*」で置き換えられ得る。

【００５０】

他の１つの実装においては、当然、指定されたフィールド情報の予め設定された特権によって、機密情報処理ストラテジーもまた、同一の変数名に対応する値のために変数情報の同一の変数において設定され得る。指定されたフィールドは、取得されたページにおける特定のフィールドに関する情報、例えば、ＨＴＴＰ要求を送信するユーザのユーザ名、を含み得る。具体的には、例えば、ＨＴＴＰ要求を送信するユーザの取得された特権によって機密情報が処理され得る。例えば、ＨＴＴＰ要求を送信するユーザがアドミニストレータ特権を有するとき、ユーザの電話番号の変数名「Ｔｅｌ＿Ｎｕｍ」に対応する値は処理されなくてよく、アドミニストレータは完全な電話番号情報を最後に返されたページにおいて見ることができる。ＨＴＴＰ要求を送信するユーザがレギュラーメンバーであるならば、ユーザの電話番号の変数名「Ｔｅｌ＿Ｎｕｍ」に対応する値の電話番号の最初及び最後の３桁のみが所定の表示ルールに従って表示され得る。残りは文字「*」で置き換えられる。

【００５１】

処理対象情報が機密情報であると決定されると、少なくとも１つの予め設定された機密情報処理ストラテジーに従って処理が実行され、処理済機密情報を作成され得る。

【００５２】

Ｓ４：ページ内の対応する処理対象情報は処理済機密情報で置き換えられ、処理済機密情報を有するページを作成する。

【００５３】

処理済機密情報が、ページ内で取得された処理対象情報から作成された後、この処理済機密情報は、このページ内の対応する処理対象情報の対応する部分に送られ、このページ内の元の処理対象情報に取って代わり得る。例えば、この実施形態において、変数名に対応する値が機密情報処理ストラテジーに従って置き換えられた後、この値の置き換え後の変数はＭＶＣサーバ・フレームワーク構造におけるＭｏｄｅｌＭａｐに返され得る。そして、ページはＭＶＣフレームワークで値の置き換え後の上記変数を用いてレンダリングされる。具体的には、例えば、ＶＭページ・テンプレートのレンダリングの間、ＭｏｄｅｌＭａｐ内の変数情報の中で、その変数名が処理済機密情報の変数名と同一である変数情報における値は、処理済機密情報における変数名に対応する値によって置き換えられ得る。例えば、ＭｏｄｅｌＭａｐにおける変数（Ｎａｍｅ２：Ｌｉ　ｓｉ）の値「Ｌｉ　ｓｉ」は、処理済機密情報（Ｎａｍｅ２：Ｌｉ*）の値「Ｌｉ*」によって置き換えられ得る。当然、暗号化対象情報が機密情報でないと決定されるか、或いは、機密情報のための処理ストラテジーが非処理または誤報であると決定されるときは、暗号化対象情報は、処理される必要がない場合がある。具体的には、この実施形態において、ＭｏｄｅｌＭａｐ内の変数の値は置き換えられなくてもよい。

【００５４】

ページが処理済機密情報を用いてレンダリングされ、処理済機密情報を有するページを作成した後、この処理済機密情報を有するページはクライアント端末のブラウザへ戻され得る。処理済機密情報を有するページを受け取った後に、クライアント端末は、処理済機密情報を有するページをユーザに対して表示する。例えば、現在のログイン・ユーザ名を表示するためのモジュール表示領域では、ユーザ名「Ｌｉ　ｓｉ」が最初に示される。そして、機密情報が処理された後、クライアント端末のユーザに示されるユーザ名は「Ｌｉ*」であり得る。

【００５５】

この実施形態によって提供される機密情報処理方法においては、処理対象情報はページ・サーバ端末で取得され得る。そして、予め設定された機密情報識別ストラテジーに従っ

て、この処理対象情報が機密情報であるかどうかが決定される。この処理対象情報が機密情報であるときには、この機密情報は予め設定された機密情報処理ストラテジーに従って処理され得る。それから、処理された機密情報はページへ戻され、その結果、処理済機密情報を有するページが作成され得る。処理済機密情報を有するページに含まれる機密情報は、サーバ端末上で対応して処理された情報である。クライアント端末の不法ユーザは、もし、データ・パケットを捕獲しても、或いは、ＪａｖａＳｃｒｉｐｔの記述を削除しても、ページ内の本当の機密情報を取得することはできない。このように、ページ内の機密情報のセキュリティが改善される。

【００５６】

クライアント端末のユーザによって送られたＨＴＴＰ要求ページは、識別され処理されるべき複数個の機密情報を含み、これらの各々の機密情報は、様々の要求ページの様々の位置に出現し得、また、ＭＶＣフレームワーク構造のＭｏｄｅｌＭａｐ内の様々の変数に対応し得る。このことは、後に続く機密情報処理において機密情報を識別することの難しさを増す。様々のＭＶＣフレームワークに基づくページ・サーバ、または、様々の設計・開発人員が、例えば、ユーザの電子メールまたはアイデンティティ・カード番号のような、同一の機密情報に対して、様々の変数名をＭｏｄｅｌＭａｐ内に設定することがあり得る。例えば、１ページの要求のＭｏｄｅｌＭａｐにおいては、アイデンティティ・カード番号変数情報に対応する変数名は「ＩＤ＿Ｎｕｍ」であるが、別の１ページの要求においては、アイデンティティ・カード番号変数情報に対応する変数名はＭｏｄｅｌＭａｐにおいて「Ｎｕｍ＿００１」であり得る。本出願は動的な機密情報処理方法の他の１つの実施形態を提供する。この実施形態において、予め設定された機密情報モニタリング・ストラテジーに従って、機密情報識別ストラテジーはダイナミックに調節され得る。具体的には、機密情報処理方法は、以下のものを更に含み得る。

【００５７】

Ｓ５：予め設定された機密情報モニタリング・ストラテジーに従って、ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報の値が処理対象機密情報であるどうかが決定される。

【００５８】

Ｓ６：機密情報モニタリング・ストラテジーに従って変数情報の値が処理対象機密情報であると決定されるときには、この変数情報の値に対応する変数名が機密情報ライブラリに送られる。

【００５９】

この実施形態では、予め設定された機密情報モニタリング・ストラテジーに従って、ＭｏｄｅｌＭａｐ内の変数情報の値が処理対象機密情報であるかどうかが決定され得る。特定の実行アプリケーションにおいては、一般に、機密情報は特定のデータ構造フォーマットを有する。例えば、携帯電話番号は、一般に、ゼロ以外の数字から始まる１１桁の組合せであり得、電子メールは、一般に、文字「@」を含み得る。この場合、機密情報モニタリング・ストラテジーは、通常の照合によって、ＭｏｄｅｌＭａｐ内の変数情報の値が予め設定された１１桁の数字の組合せに一致するかどうかを決定してよく、或いは、機密情報モニタリング・ストラテジーは、ＭｏｄｅｌＭａｐ内の変数情報の値が文字「@」を含むかどうか、そして、文字「@」の前に少なくとも１つ非ヌル文字が存在するかどうかを決定し得る。もし、機密情報モニタリング・ストラテジーに従って、ＭｏｄｅｌＭａｐ内の変数情報の値が処理対象機密情報であると決定されると、この変数情報の値に対応する変数名「Ｐｈｏｎｅ＿Ｎｕｍ」または「Ｆｉｒｓｔ＿Ｃｏｎｔａｃｔ」は機密情報ライブラリに送られ得る。機密情報ライブラリは、変数情報の値に対応する変数名「Ｐｈｏｎｅ＿Ｎｕｍ」または「Ｆｉｒｓｔ＿Ｃｏｎｔａｃｔ」を受け取ってよく、機密情報ライブラリが変数名と同一の機密情報を保存したかどうかを確かめるために比較を行い得る。変数名と同一の機密情報が機密情報ライブラリに存在しないならば、この機密情報ライブラリに含まれず、それに対応する値が処理対象機密情報である変数名が、新規追加機密情報として機密情報ライブラリに保存され得る。このように、もし、この新規追加機密情報「Ｐ

ｈｏｎｅ＿Ｎｕｍ」または「Ｆｉｒｓｔ＿Ｃｏｎｔａｃｔ」が現在機密情報ライブラリに保存されていないならば、機密情報モニタリング・ストラテジーによって、変数名が「Ｐｈｏｎｅ＿Ｎｕｍ」または「Ｆｉｒｓｔ＿Ｃｏｎｔａｃｔ」である処理対象機密情報は、新規追加機密情報として機密情報ライブラリに追加され得る。次にユーザのＨＴＴＰ要求に応答される時に、変数名が「Ｐｈｏｎｅ＿Ｎｕｍ」または「Ｆｉｒｓｔ＿Ｃｏｎｔａｃｔ」である機密情報が識別され得、この変数名「Ｐｈｏｎｅ＿Ｎｕｍ」または「Ｆｉｒｓｔ＿Ｃｏｎｔａｃｔ」に対応する値は機密情報処理ストラテジーに従って処理され得る。

【００６０】

上記のＳ５において識別した処理対象機密情報に対応して、対応する処理対象機密情報ログが更に生成され得る。処理対象機密情報ログは、処理対象機密情報の数、この処理対象機密情報の値、この値に対応する変数名、この処理対象機密情報が機密情報ライブラリに送られたかどうか、各処理対象機密情報の処理時間、この処理対象機密情報ログの生成時間等を含むことができ、後に続くシステム・セキュリティ決定の間のデータ処理に用いられ得る。

【００６１】

機密情報ライブラリに保存される新規追加機密情報に対応して、対応する新規追加機密情報ログが更に生成され得る。新規追加機密情報ログは、新規追加機密情報の数、この新規追加機密情報の値、この値に対応する変数名、この新規追加機密情報が機密情報ライブラリに保存されたかどうか、その保存時刻、この新規追加機密情報ログの生成時間等を含んでよく、後に続くシステム・セキュリティ決定の間のデータ処理に用いられ得る。

【００６２】

本出願の機密情報モニタリング・ストラテジーを含む機密情報処理方法は、機密情報ライブラリの動的更新を実現し、処理対象情報内の機密情報をより正確に識別し、機密情報の処理を完遂し、ページ内の機密情報のセキュリティを改善し得る。

【００６３】

本出願の概念に基づいて、本出願は、機密情報処理を実行するための装置を提供する。図４は、本出願による機密情報処理を実行するための装置の実施形態の概略モジュール構成図である。図４に示すように、装置は、

ページ内の処理対象情報を取得する情報収集ユニット１０１、

機密情報を保存する機密情報ライブラリ１０２、

処理対象情報が機密情報であるかどうかを、機密情報ライブラリ１０２に保存されている機密情報に基づいて決定する機密情報識別ユニット１０３、

機密情報処理ストラテジーを保存する処理ストラテジー・ユニット１０４、及び

処理対象情報が機密情報であると機密情報識別ユニット１０３が決定すると、処理ストラテジー・ユニット１０４によって保存されている機密情報処理ストラテジーに基づいて処理対象情報を処理して処理済機密情報を作成する情報処理ユニット１０５、

を含み得る。

【００６４】

特定の実施形態において、情報取得ユニット１０１によって取得された処理対象情報は、ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報を含み得る。

【００６５】

特定の処理の間、処理ストラテジー・ユニット１０４によって保存される機密情報処理ストラテジーは、

変数情報内の様々の変数名によって様々の変数名に対応する値に対して設定される機密情報処理ストラテジー、または

同一の変数名に対応する値のために、指定されたフィールド情報の特権によって、変数情報の同一の変数名に対して設定される機密情報処理ストラテジー、

を含み得る。

【００６６】

図５は、本出願による機密情報処理を実現するための装置の機密情報識別ユニット１０３の実施形態の概略モジュール構成図である。図５に示すように、機密情報識別ユニット１０３は、

ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報の変数名を取得するキー値取得ユニット１０３１、

ＭｏｄｅｌＭａｐ内の変数情報の取得された変数名が機密情報ライブラリ１０２に保存された機密情報と同一であるかどうかについて比較を行う比較ユニット１０３２、及び

比較ユニット１０３２の比較結果により、処理対象情報が機密情報であるかどうかを決定する第１の決定ユニット１０３３、

を含み得る。

【００６７】

前述の第１の決定ユニット１０３３において、もし、比較ユニット１０３２の比較結果が、変数名が機密情報ライブラリ１０２に保存される機密情報と同一であるということであるならば、これに対応して、第１の決定ユニット１０３３は、情報取得ユニット１０１によって取得された情報は機密情報であると決定する。機密情報ライブラリ１０２に保存される機密情報を吟味した後に比較ユニット１０３２が変数名と同一である機密情報を見つけられないならば、比較結果は、変数名が同一でないということであり、この場合、第１の決定ユニット１０３３は、情報取得ユニット１０１によって取得された情報は機密情報でないと決定する。

【００６８】

図６は、本出願による機密情報処理を実現するための装置における処理ストラテジー・ユニットの実施形態の概略モジュール構成図である。図６に示すように、処理ストラテジー・ユニット１０４は、

所定の表示ルールに従って変数名に対応する値の特定のフィールドを表示する所定部分表示ユニット１０４１、

所定のマスキング・ルールに従って上記変数名に対応する値の全てのフィールドをマスクする完全マスキング・ユニット１０４２、

指定されたフィールドの特権によって上記変数名に対応する値を処理する、特権に基づくマスキング・ユニット１０４３（具体的には、例えば、高い特権を有するユーザに対しては、指定された機密情報がマスクされないか、或いは、部分的にマスクされるように設定され得る。そして、低い特権を有するユーザに対しては、この指定された機密情報が部分的にマスクされるか、或いは、完全にマスクされるように設定される）、

所定の変換ルールに従って変数名に対応する値を変換して、この変数名の値として変換された値を使用する変換・表示ユニット１０４４、及び

機密情報処理装置の構造化モジュールのうちの何れか１つでも異常であるか、或いは、機密情報識別ユニット１０３によって識別される機密情報がサードパーティ・モジュールによって設定された機密情報決定基準に従わないときには、変数名に対応する値の処理をスキップし、誤報ログを生成する誤報ユニット１０４５、うちの少なくとも１つを含み得る。サードパーティ・モジュールの設定は、処理対象情報が機密情報であるかどうかを決定するために機密情報処理装置の内側または外側に設定される他の１つのモジュールを含み得る。この実施形態の機密情報処理を実現するための装置の機密情報識別方法が他の１つのモジュールの機密情報識別方法と矛盾するならば、ここの機密情報は誤報として設定され得る。そして、データ処理は機密情報に対しては実行されなくてよい。例えば、変数名に対応する値に含まれる文字「@」によって、対応する処理対象情報は機密情報、ユーザの電子メールであると決定される。一方、サードパーティ・モジュールにより、対応する処理対象情報が、設定された機密情報ではなく、ユーザによってテキストボックスに入られた商品についてのコメントであると決定され得る。この場合、機密情報処理装置の誤報ユニット１０４５は、処理対象情報に対するマスキングまたは変換のような処理を実行しなくてよく、現在の誤報のログを記録し得る。

【００６９】

この実施形態の機密情報処理を実現するための装置は、ページ内の処理対象情報を取得し、予め設定された機密情報識別ストラテジーに従って、この処理対象情報が機密情報であるかどうかを決定し得る。ｙｅｓであるならは、装置は、予め設定された機密情報処理ストラテジーに従って処理対象情報を処理して、機密情報の識別及び処理を完遂してよい。

【００７０】

本出願の他の１つの好適な実施形態において、機密情報処理を実現するための装置は、機密情報ライブラリ内に機密情報を維持するためのユニットを更に含み得る。図７は本出願による機密情報処理を実現するための装置の他の１つの実施形態の概略モジュール構成図である。図７に示すように、この装置は、

予め設定された機密情報モニタリング・ストラテジーを保存するモニタリング・ストラテジー・ユニット１０６、

処理対象機密情報、ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報の値が処理対象機密情報であるかどうかを予め設定された機密情報モニタリング・ストラテジーに従って決定する処理対象機密情報ユニット１０７、及び

変数情報の値が処理対象機密情報であると処理対象機密情報ユニット１０７が決定するとき、この変数情報の値に対応する変数名を機密情報ライブラリ１０２へ送る送信ユニット１０８、を含み得る。

【００７１】

これに対応して、機密情報ライブラリ１０２は、変数情報の値に対応する変数名を受け取って、この変数名と同一の機密情報が機密情報ライブラリ１０２に保存されるかどうかについて比較を行う。変数名と同一の機密情報が機密情報ライブラリ１０２に無いならば、この変数名は保存され得る。

【００７２】

図８は、本出願による機密情報処理を実現するための装置の他の１つの実施形態である。

図８に示すように、この装置は、ページ内の対応する処理対象情報を処理済機密情報に置き換える置換ユニット１０９を含み得る。

【００７３】

この実施形態では、機密情報処理を実現するための装置は、この装置内で、ページ内の対応する処理対象情報を処理済機密情報に置き換える。他の１つの実装においては、処理済機密情報はサーバへ送られ、このサーバは、対応する処理対象情報を処理済機密情報に置き換えて、この処理済機密情報を有するページを作成する。図９は本出願による機密情報処理を実現するための装置の他の１つの実施形態である。図９に示すように、この装置は、処理済機密情報を、サーバへ直接送る、あるいは、インターセプタを利用してこのサーバの処理済機密情報受信ユニットへ送るリターン・ユニット１１０を更に含み得る。

【００７４】

本出願は、機密情報処理を実現するためのサーバを更に提供する。このサーバは、ここまでに述べた機密情報処理を実現するための装置のうちの何れか１つを含み得る。

【００７５】

インターセプタを利用することなく、本出願により提供される機密情報処理を実現するためのサーバは、

クライアント端末によって送信されたＨＴＴＰ要求を受け取って、このＨＴＴＰ要求に従ってページ・テンプレートＭｏｄｅｌＭａｐを生成し、生成されたページ・テンプレートＭｏｄｅｌＭａｐへ処理対象情報を送り込み、上記ＨＴＴＰ要求に対応するページのレンダリングを完遂し、レンダリングされたページをクライアント端末に送り、機密情報処理モジュールによって送られた処理済機密情報を受け取り、ページ・テンプレートＭｏｄｅｌＭａｐ内の対応する処理対象情報を、上記処理済機密情報に置き換える第１のＭＶＣターゲット・システム、及び、

ページ・テンプレートＭｏｄｅｌＭａｐ内の処理対象情報を取得し、予め設定された機

密情報識別ストラテジーに従って、上記処理対象情報が機密情報かどうかを決定し、処理対象情報が機密情報であるとき、予め設定された機密情報処理ストラテジーに従って処理を実行して処理済機密情報を作成し、この処理済機密情報をＭＶＣターゲット・システムへ送る第１の機密情報処理モジュール、を含み得る。

【００７６】

図１０は、本出願による機密情報処理を実現するためのサーバの他の１つの実施形態の概略モジュール構成図である。このサーバは、ＭＶＣフレームワーク構造を含み得る。本出願の機密情報処理を実現するためのサーバは、機密情報処理を実現するための前述の装置のうちの何れか１つを含んでよく、好適な実装にはインターセプタを含み得る。具体的には、図１０に示すように、上記のサーバは、

クライアント端末によって送信されたＨＴＴＰ要求を受け取って、このＨＴＴＰ要求に従ってページ・テンプレートＭｏｄｅｌＭａｐを生成し、生成されたページ・テンプレートＭｏｄｅｌＭａｐへ処理対象情報を送り込み、ＨＴＴＰ要求に対応するページのレンダリングを完遂し、レンダリングされたページをクライアント端末に送り、機密情報処理モジュールによって送られた処理済機密情報を受け取り、ページ・テンプレートＭｏｄｅｌＭａｐ内の対応する処理対象情報を、処理済機密情報に置き換えるＭＶＣターゲット・システム１、

ページ・テンプレートＭｏｄｅｌＭａｐ内の処理対象情報を取得し、この処理対象情報を処理対象機密情報処理モジュール３へ送り、機密情報処理モジュール３によって送られた処理済機密情報を受け取り、この処理済機密情報をＭＶＣターゲット・システム１へ送るインターセプタ２、及び

処理対象情報を受け取り、この処理対象情報が機密情報であるどうかを決定し、予め設定された機密情報処理ストラテジーに従って機密情報と決定された処理対象情報を処理して処理済機密情報を作成する機密情報処理モジュール３、を含み得る。機密情報処理モジュールは、

処理対象情報を受け取る情報受信ユニット、

機密情報を保存する第１の機密情報ライブラリ、

第１の機密情報ライブラリに保存された機密情報に基づいて、この処理対象情報が機密情報であるかどうかを決定する第１の機密情報識別ユニット、

機密情報処理ストラテジーを保存する第１の処理ストラテジー・ユニット、

処理対象情報が機密情報であると、第１の機密情報識別ユニットが決定するときに、第１の処理ストラテジー・ユニットによって保存された機密情報処理ストラテジーに基づいて、この処理対象情報を処理して処理済機密情報を作成する第１の情報処理ユニット、及び

インターセプタに処理済機密情報を送る第１のリターン・ユニット、

を含み得る。

【００７７】

前述のＭＶＣターゲット・システム１は、特に、

クライアント端末によって送られたＨＴＴＰ要求を受け取り、このＨＴＴＰ要求に従ってページ・テンプレートＭｏｄｅｌＭａｐを生成するＭｏｄｅｌＭａｐモジュール１１、

生成されたページ・テンプレートＭｏｄｅｌＭａｐに処理対象情報を送り込み、インターセプタによって送られた処理済機密情報を受け取る情報Ｃｏｎｔｒｏｌｌｅｒモジュール１２、

ページ・テンプレートＭｏｄｅｌＭａｐ内の、対応する処理対象情報を、Ｃｏｎｔｒｏｌｌｅｒモジュール１２によって受け取られた処理済機密情報によって置き換え、更に、ＨＴＴＰ要求に対応するページのレンダリングを完遂するものであり得るＶｅｌｏｃｉｔｙモジュール１３、及び

クライアント端末にレンダリングされたページを送るリターン・モジュール１４、

を含み得る。

【００７８】

インターセプタは、一般に、ｐｒｅＨａｎｄｌｅｒ（２１）、ｐｏｓｔＨａｎｄｌｅＲ（２２）、及び、ａｆｔｅｒＣｏｍｐｌｅｔｉｏｎ（２３）を含み得る。本出願の機密情報処理を実現するためのサーバにおいて、ページ・テンプレートＭｏｄｅｌＭａｐ内の処理対象情報をインターセプタ２によって取得することは、インターセプタのｐｏｓｔＨａｎｄｌｅまたはａｆｔｅｒＣｏｍｐｌｅｔｉｏｎの処理プログラムを用いてページ・テンプレートＭｏｄｅｌＭａｐ内の処理対象情報を取得することを含み得る。

【００７９】

ＭＶＣターゲット・システムにおいて、処理対象情報はＭｏｄｅｌＭａｐ内の変数情報を含み得る。

【００８０】

前述の機密情報処理を実現するためのサーバにおいて、第１の処理ストラテジー・ユニットは、

所定の表示ルールに従って変数名に対応する値の特定のフィールドを表示する第１の所定部分表示ユニット、

所定のマスキング・ルールに従って変数名に対応する値の全てのフィールドをマスクする第１の完全マスキング・ユニット、

指定されたフィールドの特権によって変数名に対応する値を処理する、第１の特権に基づくマスキング・ユニット、

所定の変換ルールに従って、変数名に対応する値を変換し、この変換された値を変数名の値として使用する第１の変換・表示ユニット、及び

機密情報処理装置内の構造化モジュールのうちの何れか１つが異常であるとき、または、機密情報識別ユニットによって識別された機密情報が、サードパーティ・モジュールによって設定された機密情報決定基準に従っていないときには、変数名に対応する値の処理をスキップし、誤報ログを生成する第１の誤報ユニット、

の少なくとも１つを含む。

【００８１】

前述の機密情報処理を実現するためのサーバにおいては、第１の機密情報識別ユニットは、

ＭＶＣターゲット・システムにおけるＭｏｄｅｌＭａｐ内の変数情報の変数名を取得する第１のキー値取得ユニット、

ＭｏｄｅｌＭａｐ内の変数情報の取得された変数名が第１の機密情報ライブラリに保存された機密情報と同一であるかどうかについて比較を実行する第１の比較ユニット、及び、

第１の比較ユニットの比較結果により、処理対象情報が機密情報であるかどうかを決定する第２の決定ユニット、

を含む。

【００８２】

好適な実施形態において、前述の機密情報処理を実現するためのサーバは、更に、

予め設定された機密情報モニタリング・ストラテジーを保存する第１のモニタリング・ストラテジー・ユニット、

ＭＶＣターゲット・システムにおけるＭｏｄｅｌＭａｐ内の変数情報の値が処理対象機密情報であるかどうかを予め設定された機密情報モニタリング・ストラテジーに従って決定する第１の処理対象機密情報ユニット、及び

変数情報の値が処理対象機密情報であると第１の処理対象機密情報ユニットが決定するとき、この変数情報の値に対応する変数名を第１の機密情報ライブラリへ送る第１の送信ユニット、

を含み得る。

【００８３】

本出願により提供される機密情報処理を実現するためのサーバにおいては、ＭＶＣターゲット・システム１がユーザのＨＴＴＰ要求を受け取ると、ＭｏｄｅｌＭａｐモジュール

は、ページ・テンプレートＭｏｄｅｌＭａｐを生成し得る。それから、ＭＶＣターゲット・システムのＣｏｎｔｒｏｌｌｅｒモジュール１２が、生成されたＭｏｄｅｌＭａｐ内の変数に情報を送り込んだ後、インターセプタ２のｐｏｓｔＨａｎｄｌｅＲのｐｏｓｔＨａｎｄｌｅ処理プログラムは、ＭｏｄｅｌＭａｐ内の変数情報を取得し得る。更に、インターセプタは取得された変数情報を機密情報処理モジュール３へ送ることができ、機密情報処理モジュール３は、この変数情報が機密情報であるかどうかを決定し、予め設定された機密情報処理ストラテジーに従って、この機密情報を処理して処理済機密情報を作成し得る。ＭＶＣターゲット・システムは、機密情報処理モジュール３によって送られた処理済機密情報を受け取ってよく、ページ・テンプレートＭｏｄｅｌＭａｐ内の対応する処理対象情報を処理済機密情報に置き換えて、ページのレンダリングを完遂し得る。それから、サーバは、リターン・モジュール１４を用いて、処理済機密情報を有するページをユーザのクライアント端末へ返し得る。

【００８４】

本出願のＭＶＣフレームワークは、モデル・ビュー・コントローラ（ＭＶＣ）に基づいて設計され、作成されたウェブ・アプリケーション・モードの様々のＳｐｒｉｎｇＭＶＣフレームワーク、例えば、ｓｏｆａ２、ｓｏｆａ３，ｗｅｂｘのようなＭＶＣフレームワーク構造、を含む。

【００８５】

本出願により提供される機密処理を実現するためのサーバでは、機密情報の識別はサーバ端末上で実行され得る。そして、機密情報として決定された情報は、サーバによってユーザのクライアント端末上のブラウザに送られるページに含まれる機密情報が処理済機密情報であるように、予め設定された機密情報処理ストラテジーに従ってサーバ端末上で処理される。不法ユーザは、データ・インターセプション、局所的なウェブ・ページの一部変更等によって本当の機密情報を取得することはできない。このように、ページ内の機密情報のセキュリティが提供される。

【００８６】

本出願の機密情報処理方法、装置、及び、サーバにおいて機密情報を識別し、処理するという概念により、本出願は更にセキュリティ決定システムを提供する。このセキュリティ決定システムは、ページ・サーバが安全かどうかを決定し、ページ・サーバのセキュリティ性能を決定するために用いられ得、更に、複数のサーバ・システムの間におけるセキュリティの比較、及び、低セキュリティのサーバの遅れの無いメンテナンスのために用いられ得、サーバのセキュリティを改善し得る。図１１は、本出願によるセキュリティ決定システムの概略モジュール構成図である。図１１に示すように、セキュリティ決定システムは、

機密情報を保存し、第２の処理対象機密情報ユニットによって送られた変数名を受け取り、保存された機密情報が受け取った変数名を含むかどうかを決定し、決定の結果が、受け取った変数名を機密情報ライブラリが含まないということであるとき、新規追加機密情報として変数名を保存する第２の機密情報ライブラリ２０１、

ページ内の処理対象情報取得し、第２の機密情報ライブラリ２０１に保存された機密情報に基づいて、処理対象情報が機密情報であるかどうかを決定する第２の機密情報識別ユニット２０２、

機密情報処理ストラテジーを保存し、処理対象情報が機密情報であると機密情報識別ユニット２０２が決定するとき、保存された機密情報処理ストラテジーに基づいて、処理対象情報を処理して、処理済機密情報を作成する第２の情報処理ユニット２０３、

予め設定された機密情報モニタリング・ストラテジーを保存し、保存した機密情報モニタリング・ストラテジーに従って、ページ・サーバのＭＶＣフレームワーク構造におけるＭｏｄｅｌＭａｐ内の変数情報の値が処理対象機密情報であるどうかを決定し、変数情報の値が処理対象機密情報であると決定するとき、変数情報の値に対応する変数名を第２の機密情報ライブラリ２０１へ送るモニタリング・ユニット２０４、

第２の機密情報ライブラリ２０１における新規追加機密情報の数を含み得る新規追加機

密情報ログ（を生成する新規追加機密情報ログ・ユニット２０５、
モニタリング・ユニット２０４によって決定された処理対象機密情報の数を含み得る処理対象機密情報ログを生成する処理対象機密情報ログ・ユニット２０６、及び
第１のターゲット・システムの新規追加機密情報ログまたは処理対象機密情報ログまたは第２の機密情報ライブラリのデータを取得し、予め設定された決定ルールによって、第１のターゲット・システムが属するセキュリティ・レベルを決定する第１のセキュリティ決定ユニット２０７、
を含み得る。
【００８７】
第１のセキュリティ決定ユニット２０７は、
第１の時間窓における新規追加機密情報の数／第１の時間窓における第２の機密情報ライブラリに保存された機密情報の数によって、第１のターゲット・システムのセキュリティ・レベルを決定する第１の数決定ユニット、及び
第２の時間窓における新規追加機密情報の数の処理対象機密情報の数に対する比によって、第１のターゲット・システムのセキュリティ・レベルを決定する第１の比決定ユニット、
のうちの少なくとも１つを含み得る。
【００８８】
具体的には、例えば、第１のターゲット・システムのセキュリティ・レベルが第１の時間窓における新規追加機密情報の数によって決定されるとき、様々のセキュリティ・レベルに対応する新規追加機密情報の数が予め定義され得る。例えば、新規追加機密情報の数は、第４のセキュリティ・レベルでは１００個未満、第３のセキュリティ・レベルでは１００～１０００個、第２のセキュリティ・レベルでは１００１～５０００個、第１のセキュリティ・レベルでは５０００個以上である場合である。他の１つの実装においては、第１のターゲット・システムのセキュリティ・レベルは、第２の時間窓における新規追加機密情報の数の処理対象機密情報の数に対する比によって決定され得る。上記の比がより大きな値であるほど、新しく設定された処理対象機密情報のうちで、より多くの処理対象機密情報が処理されたことを、或いは、新しく設定された処理対象機密情報のうちの処理対象機密情報が、より適時に処理されたことを示すが、そのシステムのセキュリティがより高いことを示し得る。これに対応して、上記の比の値が小さいほど、処理対象機密情報のうちで未処理のものがより多いことを示すが、そのシステムのセキュリティがより低いことを示し得る。確かに、対応するセキュリティ・レベルは上記の比によって定義され得るが、詳細については、上記の他の実施形態が参照され得る。詳細な記述は、ここでは繰り返さない。
【００８９】
図１２は、本出願によるセキュリティ決定システムの他の１つの好適な実施形態の概略モジュール構成図である。図１２に示すように、セキュリティ決定システムはマルチシステム決定ユニット２０８を更に含み得る。マルチシステム決定ユニット２０８は、予め設定された決定ルールに従って第１のターゲット・システムのセキュリティ・レベルを第２のターゲット・システムのセキュリティ・レベルと比較する。これに対応して、第１のセキュリティ決定ユニット２０７は、第２のターゲット・システムの新規追加機密情報ログまたは処理対象機密情報ログまたは第２の機密情報ライブラリのデータを取得し得る。
【００９０】
マルチシステム決定ユニット２０８は、
第１の時間窓における新規追加機密情報の数／第１のターゲット・システム及び第２のターゲット・システムの第２の機密情報ライブラリに保存された機密情報の数によって、第１のターゲット・システム及び第２のターゲット・システムのセキュリティ・レベルを比較する第２の数決定ユニット、及び
第２の時間窓における第１のターゲット・システム及び第２のターゲット・システムの、新規追加機密情報の数の処理対象機密情報の数に対する比によって、第１のターゲット

・システムと第２のターゲット・システムのセキュリティ・レベルを比較する第２の比決定ユニット、
のうちの少なくとも１つを含み得る。

【００９１】

具体的には、例えば、統計データによって、１週間における第１のターゲット・システムの新規追加機密情報の数が第２のターゲット・システムの新規追加機密情報の数より大きいということが得られるならば、このことは、第２のターゲット・システムのセキュリティが第１のターゲット・システムのセキュリティより高いことを示し得る。統計サイクルにおいて、第１のターゲット・システムにおける新規追加機密情報の数の処理対象機密情報の数に対する比が、第２のターゲット・システムにおける新規追加機密情報の数の処理対象機密情報の数に対する比より大きいならば、確かに、このことは、第１のターゲットが機密情報を遅れ無く処理し、高いセキュリティを有することを示す。上記の２つの方法において、システムのセキュリティ・レベルは様々の量の大きさから決定されることに留意されたい。例えば、１つのシステムでは、より多数の新規追加機密情報を含み得るが、比は大きく、このことは、システムの初期セキュリティは相対的に低いが、セキュリティは適時のメンテナンスにより著しく向上することを示し得る。

【００９２】

本出願において提供されるセキュリティ決定システムは、システムの脆弱性、更新が必要なパッチの数等によって、システムが安全かどうかを、そして、セキュリティ・レベルを決定する従来技術の方法からは独立している。本出願において提供される、機密情報の観点からシステム・セキュリティを決定するためのシステムは、ターゲット・システムにおいて識別され得る機密情報データによってターゲット・システムのセキュリティ性能を決定することができ、識別された機密情報が遅れ無く処理されるかどうかを決定することができ、システムのセキュリティ評価の本質という観点から、ターゲット・システムのためのより正確なセキュリティ決定をすることができる。例えば、もし、ターゲット・システムが、全体で１００，０００個の機密情報の間で、全ての機密情報を識別し処理することができるならば、あるいは、新しく処理対象であると認識された１００個中９９個の機密情報がオペレーションによって第２の機密情報ライブラリに追加されるならば、たとえ、適用されるべきＭ個のパッチまたはＮ個の脆弱性が上記ターゲット・システムに存在するために従来技術では上記ターゲット・システムのセキュリティが低いと判断されたとしても、上記ターゲット・システムは、機密情報の識別及び処理の本質という観点から実質的に非常に安全である。本出願のセキュリティ決定システムを用いて、ターゲット・システムのセキュリティは、より正確に決定され得る。本出願を用いて、様々のターゲット・システムのセキュリティは様々の許容度に基づいて比較され得る。そして、より安全でないターゲット・システムの機密情報が遅れ無く処理され得、或いは、ターゲット・システムを維持するために他の手段が取られ、システムのセキュリティを改善し得る。

【００９３】

ＨＴＴＰを含むプロトコルについての説明が本出願の内容において言及されるが、本出願は、ＨＴＴＰを含むプロトコルが完全に標準であることが必要である場合に限定されるものではない。プロトコル上の僅かな一部変更の後に得られる若干の送信機構、例えば、ＨＴＴＰＳまたはＨＴＴＰリリース２．０の伝送プロトコル、もまた、本出願の前述の実施形態の解決策を実装するために用いられ得る。確かに、ＨＴＴＰプロトコルを使用せずに私的なプロトコルを使用する場合においてさえ、そのプロトコルが本出願の前述の実施形態におけるページ情報インタラクションおよび情報の決定フィードバックの手法に合致する限り、依然として同じアプリケーションが実装され得る。詳細の記述は、ここでは繰り返さない。

【００９４】

前述の実施形態で例示される装置またはモジュールは、特に、コンピュータのチップまたは本体によって実装され得、或いは、特定の機能を有する製品によって実装され得る。説明の容易さのために、装置の記述は、機能に基づいて、様々のモジュールについての説

明に分けられている。当然、本出願の実装においては、モジュールの機能は１または複数のソフトウェアやハードウェアに実装され得、或いは、１つの機能を実装するモジュールが複数のサブモジュールまたはサブユニットの組合せによって実装されてもよい。

【００９５】

純粋なコンピュータで読取り可能なプログラムのコードを用いてコントローラを実装することに加えて、コントローラが同一の機能をロジック・ゲート、スイッチ、特定用途向け集積回路、プログラマブル・ロジック・コントローラ、及び、組込型マイクロコントローラの形で実装されるように、方法及びステップに関してロジック・プログラミングが実行され得ることについて当業者は承知している。したがって、この種のコントローラは、ハードウェア・コンポーネントと見なされ、様々の機能を実現するためにコントローラに含まれる装置もまたハードウェア・コンポーネントの内部構成と見なされ得る。また、様々の機能を実装するための装置でさえ、方法を実現するためのソフトウェア・モジュールと見なされ得、同様にハードウェア・コンポーネントの内部構成と見なされ得る。

【００９６】

本出願は、コンピュータ、例えば、プログラム・モジュール、で実行されるコンピュータ実行可能命令の一般的な文脈で記述され得る。一般に、プログラム・モジュールは、特定のタスクを実行するため、または、特定の抽象データ型を実装するための、ルーチン、プログラム、オブジェクト、コンポーネント、または、データ構造、クラス等を含む。本出願は、また、分散形コンピュータ環境において実現され得る。そのような分散形コンピュータ環境では、タスクは、通信ネットワークを介して接続される遠隔処理装置によって実行される。

分散形コンピュータ環境では、プログラム・モジュールは、記憶装置を含む、遠隔の局所的なコンピュータ保存媒体に配置され得る。

【００９７】

前述の実装の記述を通して、本出願がソフトウェアと必要な普遍的ハードウェア・プラットフォームとによって実装され得ることは、当業者には明確に理解できることである。そのような理解に基づいて、本出願の技術的な解決策は基本的に、或いは、従来の技術に寄与する部分は、ソフトウェア製品の形で具現化され得る。そのソフトウェア製品は、例えば、ＲＯＭ／ＲＡＭ、磁気ディスク、または、光ディスクのような、記憶媒体に保存され得、（パソコン、移動端末、サーバ、または、ネットワーク装置であり得る）コンピュータ装置が本出願の実施形態の前記方法または特定の部分を実行することを可能にする幾つかの命令を含み得る。

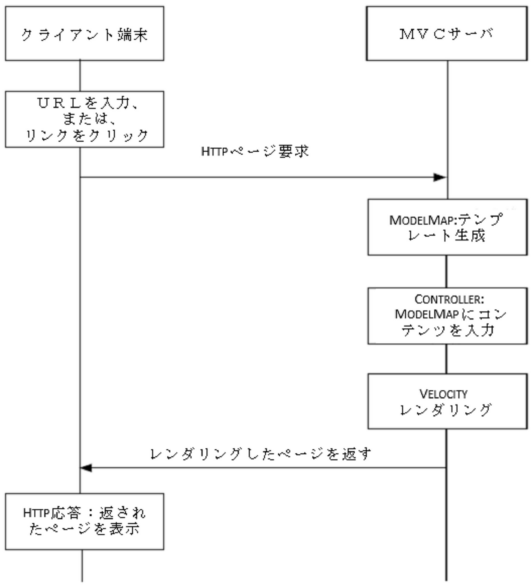
【００９８】

本明細書における様々の実施形態は段階的に記述されている。実施形態の間の同一または類似する部分は互いに参照され得る。各実施形態において、他の実施形態と異なる部分については集中的に記述されている。本出願は、例えば、パソコン、サーバ・コンピュータ、携帯用装置または携帯機器、タブレット型装置、マルチプロセッサ・システム、マイクロプロセッサ・ベースのシステム、セットトップ・ボックス、プログラム可能な電子装置、ネットワークＰＣ、ミニコンピュータ、メインフレーム・コンピュータ、及び、上記のシステムまたは装置の何れかを含む分散コンピューティング環境のような、多くの普遍的または専用のコンピュータ・システム環境または構成に適用され得る。

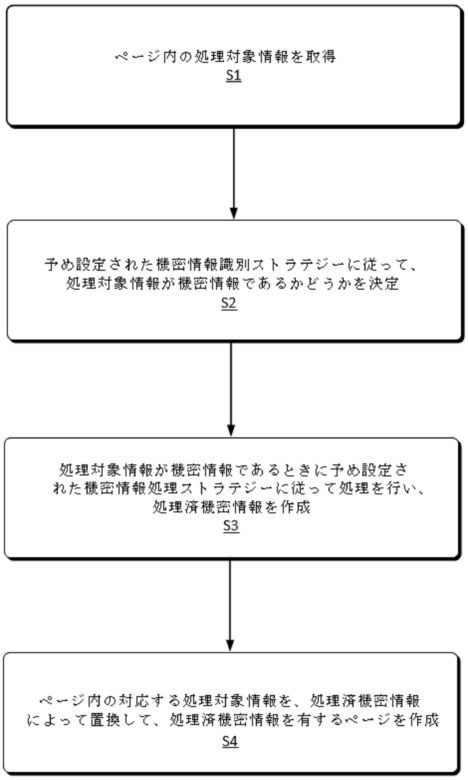
【００９９】

本出願は実施形態を通して記述されているが、本出願が、本出願の趣旨を逸脱しない範囲で多くの変形及び変更を有することが当業者には理解される。そして、添付の請求の範囲が本出願の趣旨を逸脱しない範囲でこれらの変形及び変更を包含することを意図している。

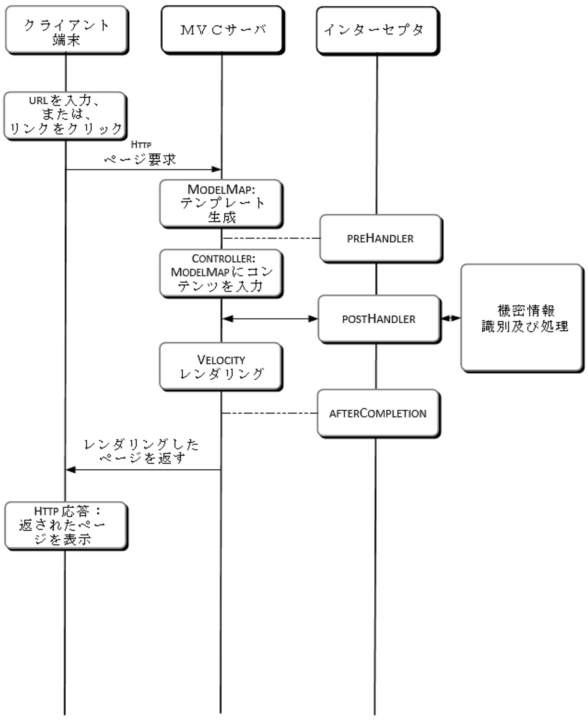
【図１】


クライアント端末
ＭＶＣサーバ
ＵＲＬを入力、
または、
リンクをクリック
HTTPページ要求
MODELMAP:テンプレート生成
CONTROLLER:MODELMAPにコンテンツを入力
VELOCITYレンダリング
レンダリングしたページを返す
HTTP応答：返されたページを表示

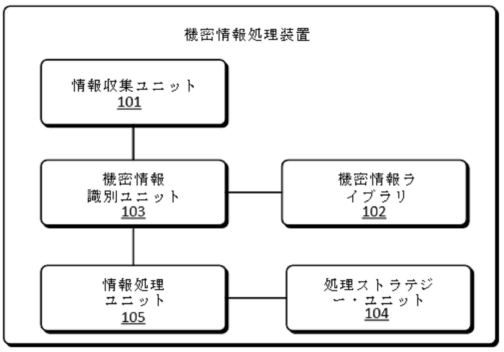
【図２】


ページ内の処理対象情報を取得
S1
予め設定された機密情報識別ストラテジーに従って、処理対象情報が機密情報であるかどうかを決定
S2
処理対象情報が機密情報であるときに予め設定された機密情報処理ストラテジーに従って処理を行い、処理済機密情報を作成
S3
ページ内の対応する処理対象情報を、処理済機密情報によって置換して、処理済機密情報を有するページを作成
S4

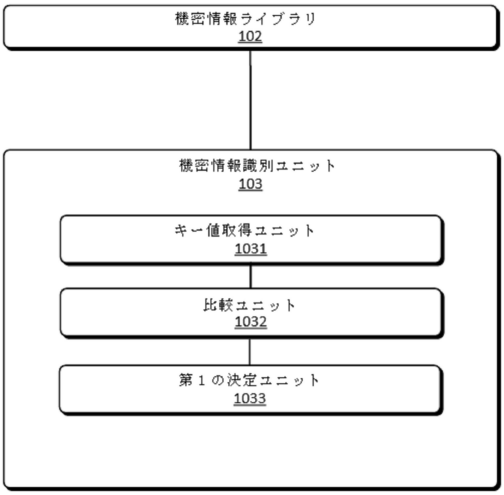
【図３】


クライアント端末
ＭＶＣサーバ
インターセプタ
URLを入力、または、リンクをクリック
HTTPページ要求
MODELMAP:テンプレート生成
PREHANDLER
CONTROLLER:MODELMAPにコンテンツを入力
POSTHANDLER
機密情報識別及び処理
VELOCITYレンダリング
AFTERCOMPLETION
レンダリングしたページを返す
HTTP応答：返されたページを表示

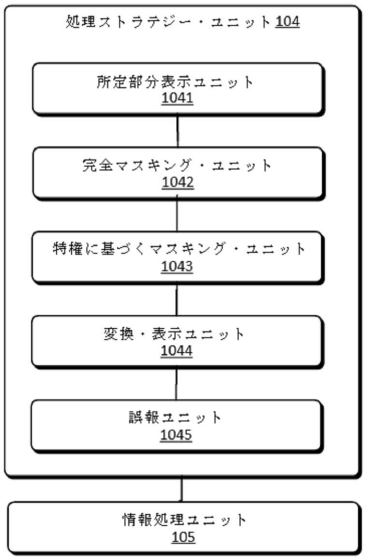
【図４】


機密情報処理装置
情報収集ユニット
101
機密情報識別ユニット
103
機密情報ライブラリ
102
情報処理ユニット
105
処理ストラテジー・ユニット
104

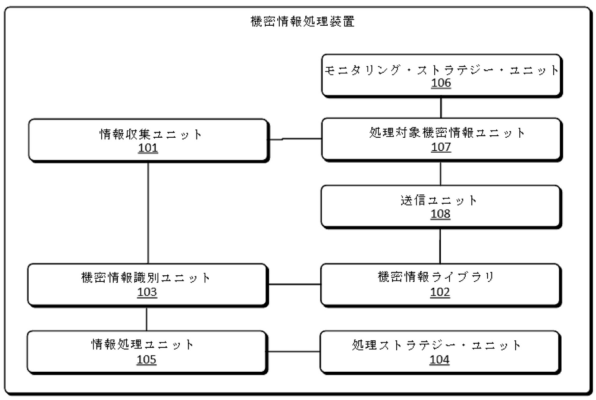
【図５】


機密情報ライブラリ
102
機密情報識別ユニット
103
キー値取得ユニット
1031
比較ユニット
1032
第１の決定ユニット
1033

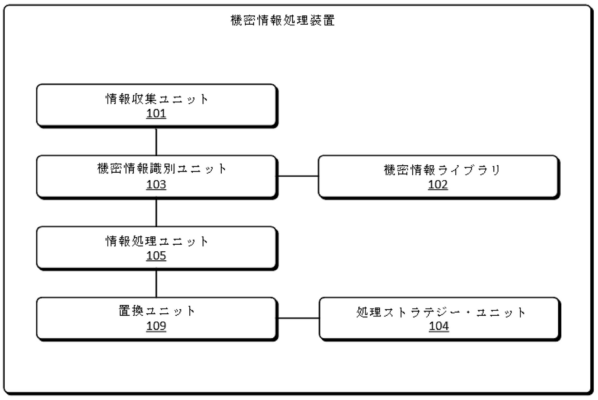
【図６】



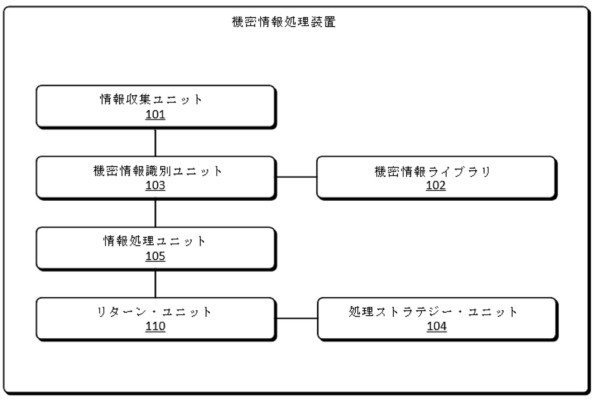
【図７】



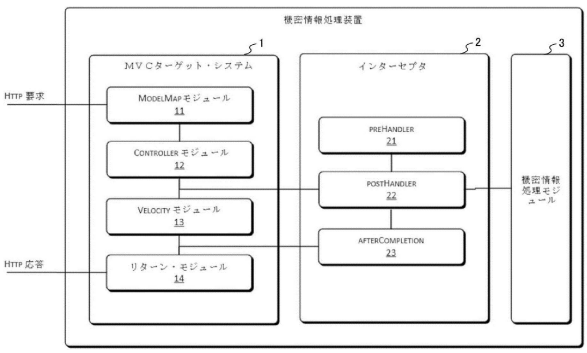
【図８】



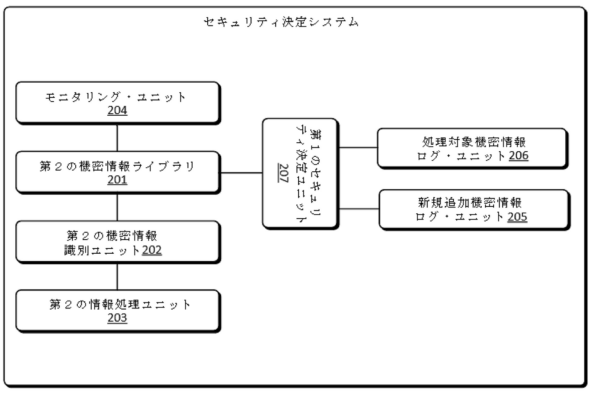
【図９】



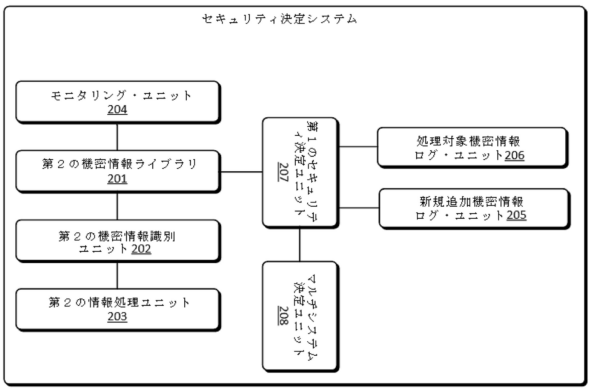
【図１０】



【図１１】



【図１２】



フロントページの続き

(72)発明者 ジャン シアン
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 リュー ジエンピン
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 チェン ジョンロン
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 ヤン コー
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 シュー フイチン
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 モウ ウェイ
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 ワン シンガン
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 スン チャオ
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 ユー シアオシュエ
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 ジアン チンフェイ
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内
(72)発明者 シアオ ハンシアオ
中華人民共和国 ３１１１２１ ゼァージアン ハンチョウ ユー ハン ディストリクト ウェスト ウェン イー ロード ナンバー９６９ ビルディング ３ ５／エフ アリババ グループ リーガル デパートメント内

審査官 青木 重徳

(56)参考文献 米国特許出願公開第２００９／０１４４８２９（ＵＳ，Ａ１）

特開２０１２－２５２４２５（ＪＰ，Ａ）
特開２００５－０９２８９１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２