【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成21年1月15日(2009.1.15)

【公表番号】特表2006-505062(P2006-505062A)
【公表日】平成18年2月9日(2006.2.9)
【年通号数】公開・登録公報2006-006
【出願番号】特願2004-550039(P2004-550039)
【国際特許分類】
Ｇ０６Ｆ　21/24　　(2006.01)
Ｇ０６Ｆ　12/00　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５６０Ａ
Ｇ０６Ｆ　12/00　　５３７Ｚ

【手続補正書】
【提出日】平成20年10月22日(2008.10.22)
【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】
データに対するセキュリティを実現する方法であって、
ユーザがデータベースに対して発行した照会を受領するステップと、
セキュリティに違反する傾向が存在するか否かを、
（ｉ）前記ユーザが以前に発行した少なくとも１つの他の照会を基準にして前記照会を実行前に比較分析するステップ、および、
（ｉｉ）前記照会の実行から戻された結果と、前記以前に発行された少なくとも１つの他の照会の実行から戻された結果とを実行後に比較分析するステップ
のうちの少なくとも１つのステップに基づいて判断するステップと
を備えた
方法。
【請求項２】
前記以前に発行された少なくとも１つの他の照会には当該ユーザの現在のログオン・セッションに属す照会だけが含まれる、
請求項１に記載の方法。
【請求項３】
セキュリティに違反する傾向が存在するか否かをステップ（ｉ）に基づいて判断する前記ステップが、
前記照会と前記以前に発行された少なくとも１つの他の照会との間の相対共通度を算出するステップ
を備えている、
請求項１に記載の方法。
【請求項４】
セキュリティに違反する傾向が存在するか否かをステップ（ｉ）に基づいて判断する前記ステップが、さらに、
前記相対共通度が所定値未満であるか否かを判断するステップと、
ＹＥＳの場合にセキュリティ規則を呼び出すステップと

を備えている、
請求項３に記載の方法。
【請求項５】
セキュリティに違反する傾向が存在するか否かをステップ（ｉｉ）に基づいて判断する前記ステップが、さらに、
前記照会の実行から戻された結果と、前記以前に発行された少なくとも１つの他の照会の実行から戻された結果との間の共通の結果の個数が低減しているか否かを判断するステップと、
ＹＥＳの場合に前記相対共通度が所定値未満であるか否かを判断し、ＹＥＳの場合にセキュリティ規則を呼び出すステップと
を備えた、
請求項３に記載の方法。
【請求項６】
セキュリティに違反する傾向が存在するか否かをステップ（ｉ）に基づいて判断する前記ステップが、
前記照会と前記以前に発行された少なくとも１つの他の照会との間の共通の照会条件が非重複の結果を戻すように構成されていることを探知するステップ
を備えている、
請求項１に記載の方法。
【請求項７】
セキュリティに違反する傾向が存在するか否かをステップ（ｉ）に基づいて判断する前記ステップが、
少なくとも部分的に非重複の結果を戻すように構成された、前記照会と前記以前に発行された少なくとも１つの他の照会との間に少なくとも１つの共通の照会条件が存在することを特徴とする、許可されていない量のデータベースを取得するユーザの試みを探知するステップ
を備えている、
請求項１に記載の方法。
【請求項８】
セキュリティに違反する傾向が存在するか否かをステップ（ｉ）に基づいて判断する前記ステップを、前記照会と前記以前に発行された少なくとも１つの他の照会とが共通の表の列にアクセスするように構成されている場合にだけ実行する、
請求項１に記載の方法。
【請求項９】
セキュリティに違反する傾向が存在するか否かをステップ（ｉｉ）に基づいて判断する前記ステップが、
前記照会の実行から戻された結果と前記以前に発行された少なくとも１つの他の照会の実行から戻された結果とが非重複であることを探知するステップ
を備えている、
請求項１に記載の方法。
【請求項１０】
セキュリティに違反する傾向が存在するか否かをステップ（ｉｉ）に基づいて判断する前記ステップが、
結果をサブセット化する傾向を探知するステップ
を備えている、
請求項１に記載の方法。
【請求項１１】
さらに、
セキュリティに違反する前記傾向が存在する場合、セキュリティ規則を呼び出すステップ

を備えた、
請求項１に記載の方法。
【請求項１２】
ステップ（ｉ）を実行した後に、セキュリティに違反する前記傾向が存在することを探知したときに前記セキュリティ規則を呼び出すステップが、
前記照会を終了させるステップ
を備えている、
請求項１１に記載の方法。
【請求項１３】
ステップ（ｉｉ）を実行した後に、セキュリティに違反する前記傾向が存在することを探知したときに前記セキュリティ規則を呼び出すステップが、
前記照会の実行から戻された結果を前記ユーザに供給しないでおくステップ
を備えている、
請求項１１に記載の方法。
【請求項１４】
データに対するセキュリティを実現する方法であって、
ユーザから複数の照会を受領するステップと、
前記複数の照会をデータベースに対して実行するステップと、
前記ユーザが前記データベースに対して引き続いて発行した照会を受領するステップと、
前記複数の照会および前記引き続いて発行された照会に基づいて、前記データベース中に存在するデータのうちの許可されていない量のデータにアクセスするユーザの試みが特定可能であるか否かをプログラムに基づいて判断するステップであって、該プログラムに基づいて判断する前記ステップが、前記引き続いて発行された照会と前記複数の照会との間の共通の照会条件が少なくとも複数の非重複の結果を戻すように構成されていることを探知するステップを備えているステップと、
を備えた
方法。
【請求項１５】
データに対するセキュリティを実現する方法であって、
ユーザから複数の照会を受領するステップと、
前記複数の照会をデータベースに対して実行するステップと、
前記ユーザが前記データベースに対して引き続いて発行した照会を受領するステップと、
前記引き続いて発行された照会を実行するステップと、
前記複数の照会および前記引き続いて発行された照会に基づいて、セキュリティ制約を迂回して一意の本人確認を回避するユーザの試みが特定可能であるか否かをプログラムに基づいて判断するステップと
を備えた
方法。
【請求項１６】
プログラムに基づいて判断する前記ステップが、
前記引き続いて発行された照会と前記複数の照会との間の相対共通度を算出するステップと、
前記引き続いて発行した照会の実行から戻された結果と前記複数の照会の実行から戻された結果と間の共通の結果の個数が低減したか否かを判断するステップと、
ＹＥＳの場合に前記相対共通度が所定値未満であるか否かを判断し、ＹＥＳならセキュリティ規則を呼び出すステップと
を備えている、
請求項１５に記載の方法。

【請求項１７】
プログラムに基づいて判断する前記ステップが、
結果をサブセット化する傾向を探知するステップ
を備えている、
請求項１５に記載の方法。
【請求項１８】
特定の物理データ表記を有するデータに対するセキュリティを実現する方法であって、
抽象照会を定義する複数の論理フィールドを備えた照会仕様を準備するステップと、
前記複数の論理フィールドを前記データの物理エンティティにマップするマッピング規則を準備するステップと、
セキュリティ規則を準備するステップと、
ユーザが前記データに対して発行した抽象照会を受領するステップであって、前記抽象照会は前記照会仕様に基づいて定義されているとともに、少なくとも１つの論理フィールドの値を用いて構成されている、ステップと、
前記ユーザから以前に受領した少なくとも１つの抽象照会を基準にして前記抽象照会を分析し、セキュリティ規則の呼び出しを引き起こす、セキュリティに違反するアクティビティの存在を探知するステップと
を備えた
方法。
【請求項１９】
前記ユーザから以前に受領した少なくとも１つの抽象照会を基準にして前記抽象照会を分析し、セキュリティ規則の呼び出しを引き起こす、セキュリティに違反するアクティビティの存在を探知する前記ステップが、
前記抽象照会と前記ユーザが以前に発行した少なくとも１つの他の抽象照会との比較分析を実行前に行うステップ
を備えている、
請求項１８に記載の方法。
【請求項２０】
前記ユーザから以前に受領した少なくとも１つの抽象照会を基準にして前記抽象照会を分析し、セキュリティ規則の呼び出しを引き起こす、セキュリティに違反するアクティビティの存在を探知する前記ステップが、
前記抽象照会の実行から戻された結果と以前に発行された少なくとも１つの他の抽象照会の実行から戻された結果との比較分析を実行後に行うステップ
を備えている、
請求項１８に記載の方法。
【請求項２１】
さらに、
前記セキュリティに違反するアクティビティの存在を探知するステップと、
前記セキュリティ規則を呼び出すステップと
を備えた、
請求項１８に記載の方法。
【請求項２２】
実行されると、セキュリティ違反を探知するオペレーションを行う命令群を含むプログラムであって、
コンピュータに、
ユーザがデータベースに対して発行した照会を受領するステップと、
セキュリティに違反する傾向が存在するか否かを、
（ｉ）前記ユーザが以前に発行した少なくとも１つの他の照会を基準にして前記照会を実行前に比較分析するステップ、および、
（ｉｉ）前記照会の実行から戻された結果と、前記以前に発行された少なくとも１つ

の他の照会の実行から戻された結果とを実行後に比較分析するステップ
のうちの少なくとも１つのステップに基づいて判断するステップと
を実行させる命令群を有する、
プログラム。
【請求項２３】
前記以前に発行された少なくとも１つの他の照会には当該ユーザの現在のログオン・セッションに属す照会だけが含まれる、
請求項２２に記載のプログラム。
【請求項２４】
セキュリティに違反する傾向が存在するか否かをステップ（ｉ）に基づいて判断する前記ステップが、
前記照会と前記以前に発行された少なくとも１つの他の照会との間の相対共通度を算出するステップ
を備えている、
請求項２２に記載のプログラム。
【請求項２５】
セキュリティに違反する傾向が存在するか否かをステップ（ｉ）に基づいて判断する前記ステップが、さらに、
前記相対共通度が所定値未満であるか否かを判断するステップと、
ＹＥＳの場合にセキュリティ規則を呼び出すステップと
を備えている、
請求項２４に記載のプログラム。
【請求項２６】
セキュリティに違反する傾向が存在するか否かをステップ（ｉｉ）に基づいて判断する前記ステップが、さらに、
前記照会の実行から戻された結果と、前記以前に発行された少なくとも１つの他の照会の実行から戻された結果との間の共通の結果の個数が低減しているか否かを判断するステップと、
ＹＥＳの場合に前記相対共通度が所定値未満であるか否かを判断し、ＹＥＳの場合にセキュリティ規則を呼び出すステップと
を備えた、
請求項２４に記載のプログラム。
【請求項２７】
セキュリティに違反する傾向が存在するか否かをステップ（ｉ）に基づいて判断する前記ステップが、
前記照会と前記以前に発行された少なくとも１つの他の照会との間の共通の照会条件が非重複の結果を戻すように構成されていることを探知するステップ
を備えている、
請求項２２に記載のプログラム。
【請求項２８】
セキュリティに違反する傾向が存在するか否かをステップ（ｉ）に基づいて判断する前記ステップが、
少なくとも部分的に非重複の結果を戻すように構成された、前記照会と前記以前に発行された少なくとも１つの他の照会との間に少なくとも１つの共通の照会条件が存在することを特徴とする、許可されていない量のデータベースを取得するユーザの試みを探知するステップ
を備えている、
請求項２２に記載のプログラム。
【請求項２９】
セキュリティに違反する傾向が存在するか否かをステップ（ｉ）に基づいて判断する前

記ステップを、前記照会と前記以前に発行された少なくとも１つの他の照会とが共通の表の列にアクセスするように構成されている場合にだけ実行する、
請求項２２に記載のプログラム。
【請求項３０】
セキュリティに違反する傾向が存在するか否かをステップ（ｉｉ）に基づいて判断する前記ステップが、
前記照会の実行から戻された結果と前記以前に発行された少なくとも１つの他の照会の実行から戻された結果とが非重複であることを探知するステップ
を備えている、
請求項２２に記載のプログラム。
【請求項３１】
セキュリティに違反する傾向が存在するか否かをステップ（ｉｉ）に基づいて判断する前記ステップが、
結果をサブセット化する傾向を探知するステップ
を備えている、
請求項２２に記載のプログラム。
【請求項３２】
さらに、
セキュリティに違反する前記傾向が存在する場合、セキュリティ規則を呼び出すステップを備えた、
請求項２２に記載のプログラム。
【請求項３３】
ステップ（ｉ）を実行した後に、セキュリティに違反する前記傾向が存在することを探知したときに前記セキュリティ規則を呼び出すステップが、
前記照会を終了させるステップ
を備えている、
請求項３２に記載のプログラム。
【請求項３４】
ステップ（ｉｉ）を実行した後に、セキュリティに違反する前記傾向が存在することを探知したときに前記セキュリティ規則を呼び出すステップが、
前記照会の実行から戻された結果を前記ユーザに供給しないでおくステップ
を備えている、
請求項３２に記載のプログラム。
【請求項３５】
セキュリティを確認するオペレーションを行うセキュリティ確認命令群をコンピュータに実行させるもつプログラムであって、
前記コンピュータに、
ユーザから複数の照会を受領するステップと、
前記複数の照会をデータベースに対して実行するステップと、
前記ユーザが前記データベースに対して引き続いて発行した照会を受領するステップと、
前記複数の照会および前記引き続いて発行された照会に基づいて、前記データベース中に存在するデータのうちの許可されていない量のデータにアクセススするユーザの試みが特定可能であるか否かをプログラムに基づいて判断するステップであって、該プログラムに基づいて判断する前記ステップが、前記引き続いて発行された照会と前記複数の照会との間の共通の照会条件が少なくとも複数の非重複の結果を戻すように構成されていることを探知するステップを備えている、ステップ、
を実行させるプログラム。
【請求項３６】
セキュリティを確認するオペレーションを行うセキュリティ確認命令群をコンピュータ

に実行させるもつプログラムであって、
前記コンピュータに、
ユーザから複数の照会を受領するステップと、
前記複数の照会をデータベースに対して実行するステップと、
前記ユーザが前記データベースに対して引き続いて発行した照会を受領するステップと、
前記引き続いて発行された照会を実行するステップと、
前記複数の照会および前記引き続いて発行された照会に基づいて、セキュリティ制約を迂回して一意の本人確認を回避するユーザの試みが特定可能であるか否かをプログラムに基づいて判断するステップと
を実行させる、
プログラム。
【請求項３７】
プログラムに基づいて判断する前記ステップが、
前記引き続いて発行された照会と前記複数の照会との間の相対共通度を算出するステップと、
前記引き続いて発行した照会の実行から戻された結果と前記複数の照会の実行から戻された結果と間の共通の結果の個数が低減したか否かを判断するステップと、
ＹＥＳの場合に前記相対共通度が所定値未満であるか否かを判断し、ＹＥＳならセキュリティ規則を呼び出すステップと
を備えている、
請求項３６に記載のプログラム。
【請求項３８】
プログラムに基づいて判断する前記ステップが、
結果をサブセット化する傾向を探知するステップ
を備えている、
請求項３６に記載のプログラム。。
【請求項３９】
その上に情報が格納されたコンピュータ読み取り可能な媒体であって、
前記情報が、
抽象照会を定義する複数の論理フィールドを備えた照会仕様と、
前記複数の論理フィールドを前記データの物理エンティティにマップするマッピング規則と、
複数のセキュリティ規則と、
ユーザが前記データに対して発行した抽象照会を受領することに対応して、セキュリティに違反するアクティビティを探知するオペレーションを行いうるように実行可能な実行時コンポーネントであって、
前記抽象照会は前記照会仕様に基づいて定義されているとともに、少なくとも１つの論理フィールドの値を用いて構成されており、
セキュリティに違反するアクティビティを探知する前記オペレーションが、
ユーザが前記データに対して発行した抽象照会を受領するステップであって、前記抽象照会は前記照会仕様に基づいて定義されているとともに、少なくとも１つの論理フィールドの値を用いて構成されている、ステップと、
前記ユーザから以前に受領した少なくとも１つの抽象照会を基準にして前記抽象照会を分析し、セキュリティ規則の呼び出しを引き起こす、セキュリティに違反するアクティビティの存在を探知するステップと
を備えている、
実行時コンポーネントと
を備えている、
コンピュータ読み取り可能な媒体。

【請求項４０】
前記ユーザから以前に受領した少なくとも１つの抽象照会を基準にして前記抽象照会を分析し、セキュリティ規則の呼び出しを引き起こす、セキュリティに違反するアクティビティの存在を探知する前記ステップが、
前記抽象照会と前記ユーザが以前に発行した少なくとも１つの他の抽象照会との比較分析を実行前に行うステップ
を備えている、
請求項３９に記載のコンピュータ読み取り可能な媒体。
【請求項４１】
前記ユーザから以前に受領した少なくとも１つの抽象照会を基準にして前記抽象照会を分析し、セキュリティ規則の呼び出しを引き起こす、セキュリティに違反するアクティビティの存在を探知する前記ステップが、
前記抽象照会の実行から戻された結果と以前に発行された少なくとも１つの他の抽象照会の実行から戻された結果との比較分析を実行後に行うステップ
を備えている、
請求項３９に記載のコンピュータ読み取り可能な媒体。
【請求項４２】
さらに、
前記セキュリティに違反するアクティビティの存在を探知するステップと、
前記セキュリティ規則を呼び出すステップと
を備えた、
請求項３９に記載のコンピュータ読み取り可能な媒体。
【請求項４３】
前記セキュリティ規則は前記抽象照会を実行させないようにする、
請求項３９に記載のコンピュータ読み取り可能な媒体。
【請求項４４】
前記セキュリティ規則は前記ユーザが発行する前記抽象照会を受領したことを記録するように定義されている、
請求項３９に記載のコンピュータ読み取り可能な媒体。