(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6169777号
(P6169777)

(45)発行日　平成29年7月26日(2017.7.26)　(24)登録日　平成29年7月7日(2017.7.7)

(51)Int.Cl.		F I		
G09C 1/00	(2006.01)	G09C	1/00	660D
G06F 21/60	(2013.01)	G06F	21/60	320
G06F 17/30	(2006.01)	G06F	17/30	120A

請求項の数 25　(全 25 頁)

(21)出願番号	特願2016-502658 (P2016-502658)
(86)(22)出願日	平成26年3月14日 (2014.3.14)
(65)公表番号	特表2016-519808 (P2016-519808A)
(43)公表日	平成28年7月7日 (2016.7.7)
(86)国際出願番号	PCT/US2014/027896
(87)国際公開番号	WO2014/143786
(87)国際公開日	平成26年9月18日 (2014.9.18)
審査請求日	平成29年3月14日 (2017.3.14)
(31)優先権主張番号	13/840,446
(32)優先日	平成25年3月15日 (2013.3.15)
(33)優先権主張国	米国(US)

早期審査対象出願

(73)特許権者　515160389
インフォマティカ　エルエルシー
アメリカ合衆国　カリフォルニア州　９４０６３、レッドウッド　シティ、シーポート　ブルバード　２１００
２１００　Ｓｅａｐｏｒｔ　Ｂｌｖｄ，Ｒｅｄｗｏｏｄ　Ｃｉｔｙ，ＣＡ　９４０６３　Ｕ．Ｓ．Ａ.
(74)代理人　100120662
弁理士　川上　桂子
(74)代理人　100112715
弁理士　松山　隆夫
(72)発明者　ブコブザ、　エリック
イスラエル国、６７７７８　テルアビブ　ヤド　ハルズティム　１４

最終頁に続く

(54)【発明の名称】データのトークン化方法および装置、並びにデータのトークン化のためのコンピュータ可読媒体

(57)【特許請求の範囲】

【請求項１】

データのトークン化のための、データベースネットワークルータ装置であって、前記装置は、

一または複数のプロセッサと、

前記一または複数のプロセッサの少なくとも一つと動作的に結合され、命令を保存する、一または複数のメモリとを備え、

前記命令は前記一または複数のプロセッサの少なくとも一つによって実行される時に、前記一または複数のプロセッサの少なくとも一つに、

一または複数のトークン化されたデータ値を保有するトークン化データベースを宛先とし、トークン化されたデータ値を含まない要求を受領し、

一または複数の規則を前記要求に適用し、

前記一または複数の規則の少なくとも一つに基づいて前記要求を書き換え、

前記書き換えられた要求を前記トークン化データベースへ送信する

ことを行わせ、

書き替えられた前記要求は、当該要求の結果としてデータが前記トークン化データベースに追加された場合に、当該要求において特定された一または複数のトークン化されていないデータ値を、前記トークン化データベースに存在するソフトウェアエージェントによりトークン化するよう構成され、

書き換えられた前記要求は、当該要求の結果としてデータが前記トークン化データベー

スから受領された場合、前記トークン化データベースに、トークン化されていないデータ値を返させるよう構成されている、データベースネットワークルータ装置。
【請求項２】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求がデータ検索要求である時に、検索規則を選択する工程と、
前記要求を書き換えて非トークン化コマンドを前記要求に挿入する工程であって、前記非トークン化コマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記要求の結果検索されたトークン化されたデータ値を前記データベースネットワークルータへ送信する前に非トークン化するよう信号を送るコマンドである、工程と、
を含む、請求項１に記載のデータベースネットワークルータ装置。
【請求項３】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が、一または複数の新たなデータ値をさらに含むデータ更新要求である時、更新規則を選択する工程と、
前記要求を書き換えてトークン化コマンドを前記要求に挿入する工程であって、前記トークン化コマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記一または複数の新たなデータ値を前記トークン化データベースへ追加する前にトークン化するよう信号を送るコマンドである、工程と、
を含む、請求項１に記載のデータベースネットワークルータ装置。
【請求項４】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が、一または複数の新たなデータ値をさらに含む挿入データ要求である時、挿入規則を選択する工程と、
前記要求を書き換えてトークン化コマンドを前記要求に挿入する工程であって、前記トークン化コマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記一または複数の新たなデータ値を前記トークン化データベースへ挿入する前にトークン化するよう信号を送るコマンドである、工程と、
を含む、請求項１に記載のデータベースネットワークルータ装置。
【請求項５】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が一または複数のフィルタデータ値を含む時、フィルタ項規則を選択する工程であって、前記一または複数のフィルタデータ値が、前記要求を、前記一または複数のフィルタデータ値に関連する一部の記録に限定するフィルタデータ値である、工程と、
前記要求を書き換えてトークン化コマンドを前記要求に挿入する工程であって、前記トークン化コマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記トークン化データベース上で前記要求を実行する前に前記一または複数のフィルタデータ値をトークン化するよう信号を送るコマンドである、工程と、
を含む、請求項１に記載のデータベースネットワークルータ装置。
【請求項６】
前記一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が不完全であると判断される時、不完全要求規則を選択する工程と、
欠落しているデータを求める要求を前記トークン化データベースへ送信する工程であって、前記欠落しているデータは、前記要求の不完全な部分である工程と、
前記トークン化データベースから前記欠落しているデータを受領する工程と、
欠落しているデータを含むよう前記要求を書き換える工程と、
を含む、請求項１に記載のデータベースネットワークルータ装置。
【請求項７】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求に関連付けられた認証レベルを、前記トークン化データベース内の一または複数のデータフィールドにアクセスするために必要な認証レベルと比較する工程と、

前記比較に基づいて、前記要求内の一または複数の認証されていないデータフィールドを識別する工程と、
前記要求内の認証されていないデータフィールド各々について、前記要求を書き換えて架空データコマンドを前記要求に挿入する工程であって、前記架空データコマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記要求が前記認証されていないデータフィールド内のデータ用のデータ検索要求である場合に前記要求に応答して架空のデータ値を返すか、または前記要求が前記認証されていないデータフィールド内のデータを含む更新または挿入要求である場合にソフトウェアエージェントに渡された前記データ値を架空値として無視するよう、信号を送るコマンドである、工程と、
をさらに含む、請求項１に記載のデータベースネットワークルータ装置。
【請求項８】
前記要求はセキュリティ認証情報を含み、前記セキュリティ認証情報は前記書き換えられた要求の一部として前記トークン化データベースへ送信される、請求項１に記載のデータベースネットワークルータ装置。
【請求項９】
一または複数の演算装置によるデータのトークン化のためのコンピュータ実行方法であって、
一または複数のトークン化されたデータ値を保有するトークン化データベースを宛先とし、トークン化されたデータ値を含まない要求を、前記一または複数の演算装置で受領する工程と、
一または複数の規則を、前記一または複数の演算装置によって前記要求に適用する工程と、
前記一または複数の規則の少なくとも一つに基づいて、前記一または複数の演算装置によって前記要求を書き換える工程と、
前記一または複数の演算装置によって、前記書き換えられた要求を前記トークン化データベースへ送信する工程と、を含み、
書き替えられた前記要求は、当該要求の結果としてデータが前記トークン化データベースに追加された場合に、当該要求において特定された一または複数のトークン化されていないデータ値を、前記トークン化データベースに存在するソフトウェアエージェントによりトークン化するよう構成され、
書き換えられた前記要求は、当該要求の結果としてデータが前記トークン化データベースから受領された場合、前記トークン化データベースに、トークン化されていないデータ値を返させるよう構成されている、コンピュータ実行方法。
【請求項１０】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求がデータ検索要求である時に、前記一または複数の演算装置によって検索規則を選択する工程と、
前記一または複数の演算装置によって前記要求を書き換えて非トークン化コマンドを前記要求に挿入する工程であって、前記非トークン化コマンドは、トークン化データベースに存在するソフトウェアエージェントに、前記要求の結果検索された前記トークン化されたデータ値を前記データベースネットワークルータへ送り返す前に非トークン化するよう信号を送るコマンドである、工程と、
を含む、請求項９に記載のコンピュータ実行方法。
【請求項１１】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が、一または複数の新たなデータ値をさらに含むデータ更新要求である時、前記一または複数の演算装置によって更新規則を選択する工程と、
前記一または複数の演算装置によって前記要求を書き換えてトークン化コマンドを前記要求に挿入する工程であって、前記トークン化コマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記一または複数の新たなデータ値を前記トー

クン化データベースへ追加する前にトークン化するよう信号を送るコマンドである、工程と、
を含む、請求項９に記載のコンピュータ実行方法。
【請求項１２】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が、一または複数の新たなデータ値をさらに含む挿入データ要求である時、前記一または複数の演算装置によって挿入規則を選択する工程と、
前記一または複数の演算装置によって前記要求を書き換えてトークン化コマンドを前記要求に挿入する工程であって、前記トークン化コマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記一または複数の新たなデータ値を前記トークン化データベースへ挿入する前にトークン化するよう信号を送るコマンドである、工程と、
を含む、請求項９に記載のコンピュータ実行方法。
【請求項１３】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が一または複数のフィルタデータ値を含む時、前記一または複数の演算装置の少なくとも一つによってフィルタ項規則を選択する工程であって、前記一または複数のフィルタデータ値は、前記要求を、前記一または複数のフィルタデータ値に関連する一部の記録に限定するフィルタデータ値である、工程と、
前記一または複数の演算装置の少なくとも一つによって前記要求を書き換えてトークン化コマンドを前記要求に挿入する工程であって、前記トークン化コマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記トークン化データベース上で前記要求を実行する前に前記一または複数のフィルタデータ値をトークン化するよう信号を送るコマンドである、工程と、
を含む、請求項９に記載のコンピュータ実行方法。
【請求項１４】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が不完全であると判断される時、前記一または複数の演算装置によって不完全要求規則を選択する工程と、
前記一または複数の演算装置によって、欠落しているデータを求める要求を前記トークン化データベースへ送信する工程であって、前記欠落しているデータは、前記要求の不完全な部分である工程と、
前記一または複数の演算装置によって、前記トークン化データベースから前記欠落しているデータを受領する工程と、
前記一または複数の演算装置によって、欠落しているデータを含むよう前記要求を書き換える工程と、
を含む、請求項９に記載のコンピュータ実行方法。
【請求項１５】
一または複数の規則を適用して前記要求を書き換える工程は、
前記一または複数の演算装置によって、前記要求に関連付けられた認証レベルを、前記トークン化データベース内の一または複数のデータフィールドにアクセスするために必要な認証レベルと比較する工程と、
前記一または複数の演算装置によって、前記比較に基づいて、前記要求内の一または複数の認証されていないデータフィールドを識別する工程と、
前記要求内の認証されていないデータフィールド各々について、前記一または複数の演算装置によって、前記要求を書き換えて架空データコマンドを前記要求に挿入する工程であって、前記架空データコマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記要求が前記認証されていないデータフィールド内のデータ用のデータ検索要求である場合に前記要求に応答して架空のデータ値を返すか、または前記要求が前記認証されていないデータフィールド内のデータを含む更新または挿入要求である場

合にソフトウェアエージェントに渡された前記データ値を架空値として無視するよう信号を送るコマンドである、工程と、
をさらに含む、請求項９に記載のコンピュータ実行方法。
【請求項１６】
前記要求はセキュリティ認証情報を含み、前記セキュリティ認証情報は前記書き換えられた要求の一部として前記トークン化データベースへ送信される、請求項９に記載のコンピュータ実行方法。
【請求項１７】
コンピュータ可読命令を保存する少なくとも一つの非一時的なコンピュータ可読媒体であって、前記命令が一または複数の演算装置によって実行される時に前記一または複数の演算装置の少なくとも一つに、
一または複数のトークン化されたデータ値を保有するトークン化データベースを宛先とし、トークン化されたデータ値を含まない要求を受領し、
一または複数の規則を前記要求に適用し、
前記一または複数の規則の少なくとも一つに基づいて前記要求を書き換え、
前記書き換えられた要求を前記トークン化データベースへ送信する
ようにさせ、
書き替えられた前記要求は、当該要求の結果としてデータが前記トークン化データベースに追加された場合に、当該要求において特定された一または複数のトークン化されていないデータ値を、前記トークン化データベースに存在するソフトウェアエージェントによりトークン化するよう構成され、
書き換えられた前記要求は、当該要求の結果としてデータが前記トークン化データベースから受領された場合、前記トークン化データベースに、トークン化されていないデータ値を返させるよう構成されている、少なくとも一つの非一時的なコンピュータ可読媒体。
【請求項１８】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求がデータ検索要求である時に、検索規則を選択する工程と、
前記要求を書き換えて非トークン化コマンドを前記要求に挿入する工程であって、前記非トークン化コマンドは、トークン化データベースに存在するソフトウェアエージェントに、前記要求の結果検索された前記トークン化されたデータ値を前記データベースネットワークルータへ送り返す前に非トークン化するよう信号を送るコマンドである、工程と、
を含む、請求項１７に記載の少なくとも一つの非一時的なコンピュータ可読媒体。
【請求項１９】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求がデータ更新要求である時、更新規則を選択する工程であって、前記データ更新要求が一または複数の新たなデータ値をさらに含む工程と、
前記要求を書き換えてトークン化コマンドを前記要求に挿入する工程であって、前記トークン化コマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記一または複数の新たなデータ値を前記トークン化データベースへ追加する前にトークン化するよう信号を送るコマンドである、工程と、
を含む、請求項１７に記載の少なくとも一つの非一時的なコンピュータ可読媒体。
【請求項２０】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が、一または複数の新たなデータ値をさらに含む挿入データ要求である時、挿入規則を選択する工程と、
前記要求を書き換えてトークン化コマンドを前記要求に挿入する工程であって、前記トークン化コマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記一または複数の新たなデータ値を前記トークン化データベースへ挿入する前にトークン化するよう信号を送るコマンドである、工程と、
を含む、請求項１７に記載の少なくとも一つの非一時的なコンピュータ可読媒体。

【請求項２１】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が一または複数のフィルタデータ値を含む時、フィルタ項規則を選択する工程であって、前記一または複数のフィルタデータ値が、前記要求を、前記一または複数のフィルタデータ値に関連する一部の記録に限定する工程と、
前記要求を書き換えてトークン化コマンドを前記要求に挿入する工程であって、前記トークン化コマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記トークン化データベース上で前記要求を実行する前に前記一または複数のフィルタデータ値をトークン化するよう信号を送るコマンドである、工程と、
を含む、請求項１７に記載の少なくとも一つの非一時的なコンピュータ可読媒体。
【請求項２２】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求が不完全であると判断される時、不完全要求規則を選択する工程と、
欠落しているデータを求める要求を前記トークン化データベースへ送信する工程であって、前記欠落しているデータは、前記要求の不完全な部分である工程と、
前記トークン化データベースから前記欠落しているデータを受領する工程と、
欠落しているデータを含むよう前記要求を書き換える工程と、
を含む、請求項１７に記載の少なくとも一つの非一時的なコンピュータ可読媒体。
【請求項２３】
一または複数の規則を適用して前記要求を書き換える工程は、
前記要求に関連付けられた認証レベルを、前記トークン化データベース内の一または複数のデータフィールドにアクセスするために必要な認証レベルと比較する工程と、
前記比較に基づいて、前記要求内の一または複数の認証されていないデータフィールドを識別する工程と、
前記要求内の認証されていないデータフィールド各々について、前記要求を書き換えて架空データコマンドを前記要求に挿入する工程であって、前記架空データコマンドは、前記トークン化データベースに存在するソフトウェアエージェントに、前記要求が前記認証されていないデータフィールド内のデータ用のデータ検索要求である場合に前記要求に応答して架空のデータ値を返すか、または前記要求が前記認証されていないデータフィールド内のデータを含む更新または挿入要求である場合にソフトウェアエージェントに渡された前記データ値を架空値として無視するよう信号を送るコマンドである、工程と、
を含む、請求項１７に記載の少なくとも一つの非一時的なコンピュータ可読媒体。
【請求項２４】
前記要求はセキュリティ認証情報を含み、前記セキュリティ認証情報は前記書き換えられた要求の一部として前記トークン化データベースへ送信される、請求項１７に記載の少なくとも一つの非一時的なコンピュータ可読媒体。
【請求項２５】
コンピュータ可読命令を含むコンピュータプログラムであって、前記命令が一または複数の演算装置によって実行される時に前記一または複数の演算装置の少なくとも一つに、
一または複数のトークン化されたデータ値を保有するトークン化データベースを宛先とし、トークン化されたデータ値を含まない要求を受領し、
一または複数の規則を前記要求に適用し、
前記一または複数の規則の少なくとも一つに基づいて前記要求を書き換え、
前記書き換えられた要求を前記トークン化データベースへ送信する
ようにさせ、
書き替えられた前記要求は、当該要求の結果としてデータが前記トークン化データベースに追加された場合に、当該要求において特定された一または複数のトークン化されていないデータ値を、前記トークン化データベースに存在するソフトウェアエージェントによりトークン化するよう構成され、
書き換えられた前記要求は、当該要求の結果としてデータが前記トークン化データベー

スから受領された場合、前記トークン化データベースに、トークン化されていないデータ値を返させるよう構成されている、コンピュータプログラム。

【発明の詳細な説明】
【関連出願データ】
【０００１】
本願は、２０１３年3月１５日出願の米国特許出願第１３／８４０、４４６号に対して優先権を主張するものであり、この参照によりその全内容が本明細書に組み込まれるものである。
【背景技術】
【０００２】
企業データベースなどデータベースには、大量のデータが保存される。そのデータの多くは、機密の、または取扱いに注意が必要な情報を含んでいる。その結果、企業は、機密となりそうなデータの数値をそのデータベースに隠すためにトークン化をよく利用する。このトークン化プロセスは、データベースのデータ値をトークン値と置き換えることから構成できる。このトークン‐データ値関係は保管庫に保管されてもよく、認証されていないアクセスを防止し、許可されたユーザのみがデータベースのトークンの実際の数値にアクセスするようにするために、暗号化されてもよい。または、現実のデータ値をトークン保管庫に保管するのではなく、復号化プロセスを経てトークンに埋め込まれた実際のデータ値を抽出するためにトークン保管庫を使用してもよい。
【０００３】
認証されたユーザがアプリケーションからデータベース内のデータにアクセスしようとする時は、そのアプリケーションが認証されたユーザを識別し、トークンを実際の数値と置き換える作業を担当する。さらに、もし認証されたユーザが新たなデータをデータベースに追加しようとすれば、アプリケーションが新たなデータをデータベースに追加する前にそれをトークン化する作業を担当する。これにより、アプリケーションにさらなる負担がかかり、また、アプリケーションがトークン保管庫およびデータベースと通信することが求められる。例えば、ユーザが追加すべきデータ値をデータベースに入力すると、アプリケーションはまずデータ値をトークン化し、その後トークン－データ値関係を保管庫に追加し、それからトークン化されたデータ値をデータベースへ送信しなければならない。
【０００４】
トークン化に関連するタスクのほとんどをアプリケーションが担当する結果、各データベースプロバイダに用いられる特定のトークン化アプリケーション・プログラミング・インターフェース（ＡＰＩ）を組み込めるよう、アプリケーションをかなりカスタマイズしなくてはならず、他のデータベースプロバイダやトークン化プロバイダのＡＰＩと共には利用できなくなる。
【図面の簡単な説明】
【０００５】
【図１Ａ】図１Ａは、従来のトークン化スキームにおけるシステム構成部分の構成と、構成部分間のやりとりとを示したシステム図である。
【図１Ｂ】図１Ｂは、開示された実施形態にかかる、データトークン化用の装置の一例である。
【図２】図２は、開示された実施形態にかかる、多数のデータベース、アプリケーション、およびトークン化スキームを利用したデータトークン化のための装置の一例である。
【図３】図３は、開示された実施形態にかかる、データベースネットワークルータ（ＤＮＲ）からのデータベースアクセス要求を取り扱うための方法の一例を示すフローチャートである。
【図４】図４は、開示された実施形態にかかる、ＤＮＲからの要求に適用できる規則および規則群の多くを示す図である。
【図５】図５は、開示された実施形態にかかる、見本表を含む見本トークン保管庫および

見本トークン化データベースの図である。
【図６】図６は、更新要求の前と後の見本トークン保管庫および見本表を示す図である。
【図７】図７は、挿入要求の前と後の見本トークン保管庫および見本表を示す図である。
【図８】図８は、開示された実施形態にかかる、ＤＮＲからの不完全な要求を取り扱うための方法の一例を示すフローチャートである。
【図９】図９は、開示された実施形態にかかる、ＤＮＲからのデータベースへの認証されていないアクセスを防ぐ方法の一例を示すフローチャートである。
【図１０】図１０は、開示された実施形態にかかるデータトークン化の方法を行うために使用できる、コンピューティング環境の一例を示す。
【発明を実施するための形態】
【０００６】
方法、装置、およびコンピュータ可読媒体が実施例および実施形態として本明細書に記載されているが、データトークン化用の方法、装置、およびコンピュータ可読媒体が、実施形態または図面に記載されたものに限定されないことを、当業者は認識する。図面および明細書が開示された特定の形態に限定されることを意図したものではないことを理解されたい。むしろ、添付の請求項の精神及び範囲から逸脱しないすべての変形、均等物、および代替物を包含することを意図している。本明細書中に使用された見出しはいずれも、整理するという目的のみのために使用されており、本明細書または請求項の範囲を制限することを企図していない。本明細書で使用されている通り、「～であってもよい／～だろう（may）」という表現は、必須の意味（すなわち、「～でなければならない（must）」という意味）ではなく、許容の意味（すなわち、可能性があるという意味）で用いられている。同様に、「含む」（「include」「including」、および「includes」）という用語は、「含む」ことを意味しており、それに限定されるという意味ではない。
【０００７】
図１Ａは、従来のトークン化スキームにおける構成部分の構成と、構成部分間のやりとりとを示したシステム図である。データベース１０２は、トークン化されたフォーマットのデータを保存する、トークン化データベースである。トークン－データ関係は、トークン保管庫１０１に保存されてもよい。アプリケーション１００は、トークン保管庫１０１と、トークン化されたデータを保存するデータベース１０２との間で、二方向通信をする。したがって、例えば、ユーザがトークン化データベース１０２に照会を行おうとすると、アプリケーション１００はまず、その照会中のフィルタ数値をトークン化し、照会をデータベース１０２へ送って照会を満足するトークン値を検索し、それからトークン値に対応する実際の数値をトークン保管庫１０１から検索しなければならない。同様に、もしユーザがデータベースを更新したいなら、アプリケーション１００が新たなデータ値をトークン化し、トークン化データベース１０２へそれらを送ったうえ、トークン保管庫１０１へ送らなければならない。
【０００８】
出願人は、トークン化の担当をアプリケーションから取り上げ、必要となるリソースを削減しインプリメンテーション（実現）を簡便にする中継ノードへ移すためのシステムを発見した。この変化によって、データベースプロバイダは、トークン化データベースを有するアプリケーションであれば、特定のトークン化ＡＰＩの要求に応ずるためにアプリケーションをカスタマイズする必要なく、いかなるアプリケーションも利用することができるようになった。さらに、中継ノードは、異なるトークン化技術を有する多数のデータベースプロバイダに対応して利用できるようになった。
【０００９】
図１Ｂは、上記のタスクを行いデータをトークン化するための、開示された実施形態にかかる装置の一例を示す。データベースネットワークルータ（ＤＮＲ）１０４は、アプリケーション１０３とトークン化データベース１０５との間の中継ノードとして機能する。ＤＮＲ１０４からのデータベースアクセス要求の一部として受領されたコマンドを解析し実行する、データベース上で作動するＤＮＲソフトウェアエージェント１０７を使用して

、データベース１０５は直接トークン保管庫１０６と通信する。ＤＮＲ１０４およびＤＮＲソフトウェアエージェント１０７を使用することにより、アプリケーション１０３はデータベース１０５から分離でき、かつ、トークン化ＡＰＩを統合しトークン化または非トークン化機能を実行する負担を、ＤＮＲ１０４およびＤＮＲソフトウェアエージェント１０７へ移すことができる。さらに、アプリケーションからトークン化および非トークン化機能を取り除くことにより、多数のトークン化ベンダーや会社がＤＮＲおよびＤＮＲソフトウェアエージェントを自身のデータベースとアプリケーションとの間のインターフェースとして利用することができる。

【００１０】

ＤＮＲを多数のデータベースとともに使用する方法の例が図２に示されている。アプリケーション２００Ａ、２００Ｂ、および２００Ｃは、異なるクライアントマシン（図示省略）上で作動してよく、３つの異なるトークン化データベース２０２Ａ、２０２Ｂ、および２０２Ｃと関連付けられてよい。各データベース２０４Ａ、２０４Ｂ、および２０４Ｃ上で作動するＤＮＲソフトウェアエージェントは各トークン保管庫２０３Ａ、２０３Ｂ、および２０３Ｃと通信する。もちろん、個別のトークン保管庫が各データベースに必須であるというわけではない。例えば、データベース２０２Ｂおよび２０２Ｃが同じトークン化スキームを使用し単一のトークン保管庫を共有することが、可能である。

【００１１】

ＤＮＲ２０１はアプリケーション２００Ａからの要求を受領またはインターセプトすることができ、アプリケーション、クライアントマシン、ユーザ本人証明、要求先、要求内容、またはその他いくつかのパラメータに基づいて、要求がデータベース２０２Ａと関連付けられていると判断することができる。要求はデータベース２０２Ａと関連付けられた規則に従って処理でき、下記に記載されたように、データベース２０２Ａ上へ送られる。データベース２０２Ａでは、いくつかのデータ値がトークン化の必要があると、またはいくつかのトークン化された数値が非トークン化（de-tokenize）の必要があると、ＤＮＲエージェント２０４Ａが判断するかもしれず、その時には、ＤＮＲ２０１および最終的にアプリケーション２００Ａへなんらかの結果を返す前に、トークン保管庫２０３Ａと通信して適切な演算を行うことができる。

【００１２】

図３を参照して、開示された実施形態のＤＮＲによるデータベースアクセス要求を取り扱う方法を以下に示す。ステップ３０１において、ＤＮＲはデータベースアクセス要求をアプリケーションから受領する。この要求は宛先を対象データベースとし、ＤＮＲへ行く先を変更することができ、または要求を前記ＤＮＲがインターセプトすることも可能である。または、要求は、目的地データベースを明示してＤＮＲへ送ることもできる。データベースアクセス要求をＤＮＲで受領することについては、色々な変更が可能である。

【００１３】

データベースアクセス要求としては、データ検索要求、データ更新要求、データ挿入要求、データ削除要求、またはその他同様のデータベースアクセス要求などを含む、様々なタイプの要求を含めることができる。さらに、要求の言語としては、構造化照会言語（ＳＱＬ）、コンテクスチュアル照会言語（ＣＱＬ）、ＸＱｕｅｒｙ、ＹＱＬ、Ｄａｔａｌｏｇ、ＯＱＬ、ＲＤＱＬ、およびその他多数の言語を含む、様々なタイプのデータベース照会言語を含めることができる。

【００１４】

ステップ３０２では、ＤＮＲは一または複数の規則を要求に適用することができる。これら規則は以下により詳しく記載されるが、様々な種別のデータベースアクセス要求、リクエストルーティング、トークン化規則、等に対する適切な取扱いに関連する規則を含めることができる。規則を適用した後、ステップ３０３で、要求が、一または複数の規則の少なくとも一つに基づいて書き換えられる。例えば、要求は書き換えられて一または複数のコマンドをデータベースアクセス要求に追加することができ、それはデータベース上で作動するＤＮＲエージェントによってその後解析され実行される。さらに、一または複数

のパラメータがＤＮＲエージェントへ渡され、これはＤＮＲエージェントへ一緒に渡されたデータの取り扱い方を指示するコマンドを伴う。例えば、パラメータは、使用する特定のトークン化スキーム、特定のユーザまたは装置の認証、コマンドを無視すべきかどうか、偽（ｆａｌｓｅ）の値は返されるべきかどうか、などを明示することができる。

【００１５】

一または複数の規則を使用して要求が書き換えられた後、ステップ３０４で書き換えられた要求を目的地データベースへ送信することができる。書き換えられた要求の実際の送信は、同様に、一または複数の規則に基づいて行うことができる。例えば、目的地データベースは、複数の場所（repository）にまたがって配置された分散データベースであってもよい。どの場所へ要求を送ればよいか判断するために、ＤＮＲは、データベースアクセス要求へ規則を適用してもよく、またはその内容に適用してもよい。同様に、もしＤＮＲが異なるトークン化スキームを有する多数の異なるデータベースへ要求を送信しているなら、ＤＮＲは書き換えられた要求の正しい送り先であるデータベースを判定するために規則を適用する必要があるだろう。または、もしＤＮＲが目的地データベースをすでに明示している要求をインターセプトするなら、ＤＮＲは、書き換えられた要求をその目的地データベースへ単に送信すればよい。

【００１６】

図４は、要求に適用できるいくつかの規則および規則群４００を示す。ＤＮＲは、受領された要求の種別に基づいて、データ検索要求規則４０１、データ更新要求規則４０２、およびデータ挿入要求規則４０３など、規則の群を適用する。さらに、図示は省略するが、ＤＮＲは同様に、データ削除要求に関連する規則群を適用する。実際には、これらはデータ更新要求と同様であるだろう。アクセス要求が一または複数のフィルタ項を含むとき、フィルタ項規則４０４が適用されうる。例えば、ＳＱＬ照会は、「select variable A where variable B=X（変数Ｂ＝Ｘであるような変数Ａを選択する）」と定めてもよい。このｗｈｅｒｅ節および関連の情報はフィルタ項であり、フィルタ項の取り扱い方を判断するために規則の群が用いられてもよい。

【００１７】

例えば、フィルタ項は、データベース上で作動しているＤＮＲエージェントへ渡された後にトークン化される必要がある、トークン化されていないデータを含んでもよい。ただし、トークン化ＡＰＩは、フィルタデータ値として渡されたデータ値のために新たなトークンが作り出されるべきではなく、トークン値（もし一つ存在すれば）はトークン保管庫から見つけ出すべきである、と指定してもよい。さらに以下に記載するように、渡された数値をトークン化すべきであって、新たなトークンをそのプロセスで作り出すべきではない、とＤＮＲエージェントに知らせるトークン化コマンドにパラメータを挿入するために、フィルタ項規則を用いることができる。

【００１８】

トークン化ＡＰＩ規則４０５は、様々なトークン化スキームを有するトークン化データベースからデータを検索するため、またはそこへデータを送付するために使用される色々な規則に関する。例えば、第一の要求が、そこに保存されているデータ値のすべてをトークン化するための第一トークン化アルゴリズムを使用する第一のデータベースを宛先とし、第二の要求が、そこに保存されている取扱いに注意が必要なデータのみをトークン化するための第二のトークン化アルゴリズムを使用する第二データベースを宛先としてもよい。したがって、例えば、ＤＮＲが第二のデータベースを宛先とするデータ検索要求を受領すると、ＤＮＲは、そのデータベースに関連付けられたトークン化ＡＰＩ規則を調べ、要求されたデータがトークンフォーマットで保存されているかどうかを判断することができる。もしトークンフォーマットで保存されていれば、ＤＮＲは非トークン化コマンドを要求に挿入することができ、そうでなければ、非トークン化コマンドは不要である。

【００１９】

トークン化ＡＰＩ規則４０５は、どんな種別のデータまたはデータフィールドがトークン化されるべきか明示することができる。例えば、あるトークン化ＡＰＩはすべてのデー

タがトークン化されるべきであると明示し、別のトークン化ＡＰＩは、個人的または機密の情報を含むデータフィールドのみがトークン化されるべきであると明示してもよい。

【００２０】

不完全要求規則４０６も同様に以下により詳しく記載され、これはＤＮＲが特定のフィールドや他の何か必要な情報を欠いている要求を受領する際に適用することができる。

【００２１】

認証規則４０７およびセキュリティ規則４０８は、ユーザ、装置、またはユーザに関連付けられたセッションが、要求を行うための十分な認証情報を有しているかどうか判断するために使用でき、また、ユーザが十分な認証情報を有していない様々な状況においてどんなアクションを取るべきであるかを明示するために使用できる。例えば、消費者取引データベースにおいて、各消費者のみが非トークン化されたフォーマットで自身のクレジットカード情報を見ることができる、とセキュリティ規則で定めてもよい。もしシステム管理者が関連のフィールドすべてとの取引の一覧を求めるなら、セキュリティ規則を利用して、非トークン化されたフォーマットで保護されていないフィールドを返信し、トークンフォーマットで関連付けられたクレジットカード番号を返してもよい。または、セキュリティ規則を利用して、各クレジットカード番号について、偽の、または架空の番号を返すよう、データベースに指示することもできる。架空値は、なんらかのアルゴリズムを使用して生成することができ、または、架空値のプールから選択することもできる。認証規則は、異なる種別のユーザについて異なるレベルのアクセスを実現するために、用いられてもよい。例えば、管理者のみがデータベース中の記録の更新、挿入、または削除に必須の許可を有し、その他のユーザはすべて、照会をする許可のみを有してもよい。

【００２２】

最後に、上記のように、ルーティング規則４０９は、要求をどこに転送するかを判断するために利用されてもよい。ルーティング規則４０９は、インターセプトされた要求の目的地データベースアドレスを記録して、書き換えられた要求をそのアドレスへ送る、という規則のように簡略であってもよい。

【００２３】

規則はすべてＤＮＲの枠組みの中で説明されているが、規則の機能性のいくつか、またはすべては、データベース上で作動するＤＮＲソフトウェアエージェントによって実現することができることを理解されたい。例えば、もしユーザが要求を行えると認証されていなければ、かかる査定はＤＮＲでなされてもよく、ＤＮＲは、「not-authorized（認証されていない）」というトークンまたはメッセージを、データベースへ送られた書き換えられた要求に挿入することができる。データベースでは、ＤＮＲソフトウェアエージェントが「not-authorized（認証されていない）」というトークンを読み出すことができ、要求に応答してアクションすべきではないと判断する。さらに、当業者なら理解されるだろうが、これら規則すべてが、ここに開示するデータトークン化の方法を行うために必要なわけではない。

【００２４】

図５は、見本トークン化データベース５０１を示す。見本データベース５０１の表ＸＹＺ５０２には、名前（name）と社会保障番号（social security number, SSN）のトークン化されたリストが入っている。トークン値Ｔ１、Ｔ２、Ｔ３、およびＴ４は図示のための記載であって、実際のトークン値はデータベース所有者／管理者またはトークン化プロバイダに都合の良いなんらかの数字の列または英数字の列であってよい。

【００２５】

見本データベース５０１は同様に、ＤＮＲ５０４を介して受領された書き換えられた要求から解析されたコマンドを実現するＤＮＲソフトウェアエージェント５０５を備える。見本データベース５０１上で作動するＤＮＲエージェント５０５は、見本トークン化データベース５０１中のトークン値に対応するデータ値を含む見本トークン保管庫５０３と通信する。

【００２６】

ＤＮＲ５０４は、データベースアクセス要求を一または複数のアプリケーション５０６から受領し、要求を処理した／書き換えたのち、関連する書き換えられた要求を見本トークン化データベース５０１へ送る。もちろん、ＤＮＲ５０４は一度に多数のトークン化データベース（図示省略）および多数のアプリケーションと通信してもよく、図面に限定された構成部分が示されているのは、ただ図示と明瞭化のためである。

【００２７】

ＤＮＲ５０４によって、アプリケーション５０６がトークン化または非トークン化を担当することなく、アプリケーション５０６を使用しているユーザ（図示省略）が見本トークン化データベース５０１を宛先とするデータベースアクセス要求を入力し送信できるようになる。データベース要求が通常入力されるようなやり方で、ユーザはデータベース要求を入力でき、アプリケーション５０６はそれらを、トークン化および非トークン化関連の処理をすべて取り扱うＤＮＲ５０４へ転送することができる。

【００２８】

色々な種別の要求の演算および各要求の具体例を、見本トークン化データベース５０１中の表ＸＹＺ５０２および見本トークン保管庫５０３を参照しながら説明する。上記例の言語はＳＱＬに準拠しているが、これは説明のためにこのようにしているだけであって、いかなる照会言語も使用することができる。

【００２９】

ＤＮＲ５０４が見本トークン化データベース５０１を宛先とするデータ検索要求を受領すると、まずデータ検索要求用の適切な規則群をロードする。適切な規則群をロードしたのち、データ検索要求を評価し、書き換えて、それが見本トークン化データベース５０１へ送付された後に、その検索すべき数値が非トークン化された状態で返されるようにする。

【００３０】

例えば、データ検索要求が下記のようであったとする。

“SELECT Name FROM Table XYZ”（表ＸＹＺから名前を選択）

【００３１】

この照会が、変更なく、見本トークン化データベース中の表ＸＹＺ５０２上で作動していたら、返されるであろう結果群は下記のようになる。

Name:T1,T2（名前：Ｔ１、Ｔ２）

【００３２】

もちろん、これは、ユーザがこのような照会で検索しようとした情報ではない。ＤＮＲ５０４がこの照会を受領すると、適切な規則群を用いて照会を次のように書き換える。

“SELECT deToken(Name) FROM Table XYZ”（表ＸＹＺから非トークン（名前）を選択）

【００３３】

非トークン化関数（deToken function）は、見本トークン化データベース５０１上で作動するＤＮＲエージェント５０５に対し、結果群をＤＮＲ５０４へ返信する前に、検索された数値を非トークン化することを示す。したがって、書き換えられた照会の例を使用すると、見本データベース５０１は書き換えられた照会を実行してトークン値を名前欄で検索し、ＤＮＲエージェント５０５はそれらトークン値を見本トークン保管庫５０３へ送信して実際の数値を検索し、それがその後ＤＮＲ５０４へ返される。

【００３４】

非トークン化関数はただ一つのパラメータをとるものとして示されているが、これは単に明瞭化のためである。非トークン化関数は多数のパラメータをとることができる。例えば、非トークン化関数は照合用のＤＮＲ原本署名を含むパラメータをとることができ、ＤＮＲエージェントが直接アクセスを受けないようにする。関数は、使用中の特定のトークン化スキームに関連するパラメータをとることができ、または、ユーザセッション識別印など特定のユーザセッションに関連する情報を有するパラメータを含むことができる。関数は同様に、どの種別の数値が返されるべきかに関連するセキュリティデータを含むこと

ができる。このことは、架空値についてより詳しく記載される。

【００３５】

したがって、照会が見本トークン化データベース５０１へ送付される前にＤＮＲ５０４を通過して書き換えられる時にアプリケーション５０６のユーザへ返信されるであろう結果群は、以下のようになる。

Name: Miller, Sanchez （名前：Miller, Sanchez）

【００３６】

非トークン化関数は、セキュリティまたは許可の配慮から、選択的に適用でき、見本データベース５０１へ一または複数の追加の変数を渡すことができる。これらの変更は、セキュリティおよび架空値の特徴を参照して、さらに下記に記載する。

【００３７】

ＤＮＲ５０４が見本トークン化データベース５０１を宛先とするデータ検索要求を受領する時、まずデータ更新要求用の適切な規則群をロードする。適切な規則群をロードしたのち、ＤＮＲ５０４は、データ検索要求を評価し、見本トークン化データベース５０１へ送付された後にトークン化データベースに追加すべき数値がトークンフォーマットになり適切なトークン－データ関係が見本トークン保管庫に保存されるように、データ検索要求を書き換える。

【００３８】

したがって、見本トークン化データベース５０１に送付されＤＮＲ５０４によってインターセプトされたデータ更新要求が下記のようであれば、

UPDATE Table XYZ, SET SSN = 421-66-4567 （ＳＳＮ＝４２１－６６－４５６７をセットして、表ＸＹＺを更新）

【００３９】

書き換えられた要求は下記のようになる。

UPDATE Table XYZ, SET SSN = Tokenize(421-66-4567) （ＳＳＮ＝トークン化（４２１－６６－４５６７）をセットして、表ＸＹＺを更新）

【００４０】

トークン化関数（Tokenize function）は、見本トークン化データベース上で作動するＤＮＲエージェント５０５に対し、更新データのトークン値を作り出すよう指示することができる。トークン化関数はただ一つのパラメータをとるものとして示されているが、これは単に明瞭化のためである。トークン化関数は多数のパラメータをとることができる。例えば、トークン化関数は検証用のＤＮＲ原本署名を含むパラメータをとることができ、ＤＮＲエージェントが直接アクセスを受けないようにする。関数は、使用中の特定のトークン化スキームに関連するパラメータをとることができ、または、ユーザセッション識別印など特定のユーザセッションに関連する情報を有するパラメータを含むことができる。関数は同様に、どの種別の数値が返されるべきかに関連するセキュリティデータを含むことができる。架空値について、このことがより詳しく記載される。

【００４１】

ＤＮＲエージェント５０５がトークン化関数を受領する時、もし関数中に通過させたデータ値用のトークンが存在しなければ、新たなトークンを作り出すことができる。さらに、ＤＮＲエージェント５０５は、更新要求の明細に従って、トークン化されたデータ値で表ＸＹＺ５０２の関連する部分を更新し、トークン－データ値関係を保存用に見本トークン保管庫５０３へ送付することができる。もちろん、実際には、更新コマンドの多くが、どの部分を更新すべきか示したｗｈｅｒｅ節を含むであろう。フィルタ数値について、これらがより詳しく記載される。オプションとして、トークン化関数はまた、データ値から生成されたトークン値がトークン保管庫へ追加されるべきかどうかをＤＮＲエージェントに対して示すパラメータを含むこともできる。

【００４２】

図６には、更新要求を受領する前の時間Ｔ－０、６０３と、更新要求を受領した後の時間Ｔ－１、６０４との二つの時間で、見本トークン保管庫が示されている。さらに、表Ｘ

ＹＺも、二つの時間である、時間Ｔ－０、６０１および時間Ｔ－１、６０２で示されている。

【００４３】

上記に記載された特定の更新要求の例を使用して、表ＸＹＺおよびトークン保管庫の両方の推移を説明する。対応するトークンをまだ有さないデータ値である新たなＳＳＮナンバー「４２１－６６－４５６７」を更新要求が含むので、その数値のための新たなトークン値が生成される必要がある。ＤＮＲエージェントは、適切なトークン化規則を使用して、新たなトークン「Ｔ５」を生成する。トークン化規則は、インストール中にＤＮＲエージェントに前もってロードしてもよく、またはその後のいずれかの時点でトークン保管庫や、データベース、またはその他の適切なソースから受領してもよい。

【００４４】

新たな番号４２１－６６－４５６７に対応するトークンＴ５を生成した後、新たなトークンおよび関連付けられたデータ値が見本トークン保管庫６０４に保存される。さらに、表ＸＹＺ６０２中の記録の各々のＳＳＮすべてが新たなトークンＴ５と共に更新される。上記のように、これは更新要求がｗｈｅｒｅ限定を含まなかったからである。

【００４５】

非トークン化関数と同様に、セキュリティまたは許可の配慮から、トークン化関数は選択的に適用でき、見本データベースへさらに一または複数の変数を通過させることができる。これらの変更を、セキュリティおよび架空値の特徴を参照して、さらに下記に記載する。

【００４６】

挿入データ要求は、更新データ要求と同様に取り扱われ、そこでトークン化関数は新たなデータのために利用される。したがって、例えば、ユーザが「Ｊａｃｋｓｏｎ」という名前の人物の社会保障名を含む記録を表ＸＹＺに追加したい場合、その挿入要求は以下のように書き込むことができるだろう。

INSERT INTO TABLE XYZ, VALUES (Jackson, 162-97-2441) （値（Ｊａｃｋｓｏｎ、１６２－９７－２４４１）を表ＸＹＺに挿入）

【００４７】

この要求がＤＮＲにインターセプトされトークン化コマンドを含むように書き換えられた後に、下記のように、見本トークン化データベースへ送付できる。

INSERT INTO TABLE XYZ, VALUES (Tokenize(Jackson), Tokenize(162-97-2441)) （値（トークン化（Ｊａｃｋｓｏｎ）、トークン化（１６２－９７－２４４１）を表ＸＹＺに挿入）

【００４８】

これは、見本トークン化データベース上で作動するＤＮＲエージェントに、新たなデータ値の各々のために新たなトークン値を作り出しそれに従ってデータベースおよびトークン保管庫を更新するよう、注意を促すだろう。

【００４９】

図７は、上記に挙げられた挿入コマンドの結果を示す。時間Ｔ－０の表ＸＹＺ７０１は、挿入データ要求がデータベースに送付される前の表であり、時間Ｔ－１の表ＸＹＺ７０２は、挿入データ要求が送付された後の表である。同様に、時間Ｔ－０のトークン保管庫７０３は、挿入データ要求がデータベースへ送付される前のトークン保管庫であり、時間Ｔ－１のトークン保管庫７０４は、挿入データ要求がデータベースに受領された後のトークン保管庫である。時間Ｔ－１の表ＸＹＺ７０２および時間Ｔ－１の見本トークン保管庫７０４は、二つの新たなトークン、Ｔ５およびＴ６の追加を示している。これら二つの新たなトークンは、新たなデータ値Ｊａｃｋｓｏｎおよび１６２－９７－２４４１に対応している。

【００５０】

多くの要求はフィルタ項、すなわち、要求が適用されるデータ群の範囲およびサイズを小さくするかまたはフィルタ処理する項、を含んでもよい。図５の上述の表ＸＹＺ５０２

の例を使用すると、ユーザは誰かの姓を使ってその社会保障番号を検索しようとしてもよいが、表になっている全員のＳＳＮについて検索することはできない。ある人のＳＳＮが探されていて、その人の名前が「Ｍｉｌｌｅｒ」なら、通常、下記の照会をデータベースに送り、ＭｉｌｌｅｒのＳＳＮを検索する。

SELECT SSN FROM Table XYZ WHERE Name=Miller　（名前＝Ｍｉｌｌｅｒの条件で、表ＸＹＺからＳＳＮを選択）

【００５１】

もちろん、もしこの照会がそのままトークン化データベース中のトークン化された表ＸＹＺへ送信されれば、名前Ｍｉｌｌｅｒは見つからず、何の結果も返信されないだろう。なぜならこの照会は、トークン化されていないデータベース用だからである。トークン化データベースに対応させるため、照会はＤＮＲによって以下のように書き換えられる。

SELECT deToken(SSN) FROM Table XYZ WHERE Name=Tokenize(Miller)　（名前＝トークン化（Ｍｉｌｌｅｒ）の条件で、表ＸＹＺから非トークン化（ＳＳＮ）を選択）

【００５２】

上記のデータ検索要求についての説明にあるように、要求に対する第一の変更は、非トークン化関数の挿入の中にある。要求に対する第二の変更は、フィルタデータ値「Ｍｉｌｌｅｒ」用のトークン化関数の挿入である。これは、データベース上で作動するＤＮＲエージェントに対し、「Ｍｉｌｌｅｒ」に対応するトークン値を見つけてＳＳＮを選択する時のフィルタとしてそのトークン値を使用するように注意を促している。

【００５３】

この場合、「Ｍｉｌｌｅｒ」に対応するトークン値はＴ１であるので、照会の結果、Ｔ１に対応するトークン化されたＳＳＮを選択することになり、それはＴ３である。ＤＮＲエージェントは非トークン化関数をＴ３に適用して「０４５－２２－１２４６」というＳＳＮを生成し、これがユーザへ返される。

【００５４】

または、トークン化関数は、それが挿入データ値、更新データ値、またはフィルタデータ値に関連付けられているのかどうかを示すパラメータを通過させてもよい。これは、そのデータ値のために新たなトークンを生成する必要があるのかどうかをＤＮＲエージェントが判断する際に有用である。例えば、挿入データ値または更新データ値と共にトークン化関数が用いられる時、ＤＮＲエージェントは、そのデータ値用にトークン値が存在するかどうかを見るためにトークン保管庫を調べ、それが存在しなければ、新たなトークン値を生成してもよい。トークン化関数がフィルタデータ値と共に用いられる時、選択されたデータ値群をフィルタ処理するためにフィルタデータ値が用いられ、データ表には追加されないので、ＤＮＲエージェントは新たなトークンが生成されなくてもよいと判断する。この状況では、ＤＮＲエージェントはトークン保管庫中のフィルタデータ値に対応する適切なトークン値を見つけるだけでよく、もしトークン値が存在していなければ、ＤＮＲエージェントはどの記録もそのフィルタデータ値に対応していないと正確に判断することができる。なぜなら、もし以前に表に挿入されるか追加されていれば、そのデータ値用にトークンが作り出されていたはずだからである。または、関連付けられたトークン値がまだ無い、渡された全てのデータ値についてトークン値を作り出すために、トークン化関数を使用できる。

【００５５】

データ検索コマンドと共に用いられることに加えて、データベース中に保存されているデータ値を更新するために、フィルタを利用することができる。例えば、図５の表ＸＹＺ５０２を参照し、ユーザが「Ｓａｎｃｈｅｚ」という名前に関連付けられたＳＳＮを更新したいとすると、そのためには、下記の要求を送信すればよい。

UPDATE Table XYZ, SET SSN = 123-45-6789 WHERE Name=Sanchez　（名前＝Ｓａｎｃｈｅｚの条件でＳＳＮ＝１２３－４５－６７８９をセットして、表ＸＹＺを更新）

【００５６】

もしデータベースがトークン化されていなかったら、これによって「Ｓａｎｃｈｅｚ」という名前に関連付けられたＳＳＮが「１２３－４５－６７８９」に変更されるだろう。しかしながら、データベースはトークン化されているので、要求はＤＮＲによって下記のように書き換えられる。

UPDATE Table XYZ, SET SSN=Tokenize(123-45-6789) WHERE Name = Tokenize(Sanchez)　（名前＝トークン化（Ｓａｎｃｈｅｚ）の条件でＳＳＮ＝トークン化（１２３－４５－６７８９）をセットして、表ＸＹＺを更新）

【００５７】

書き換えられた要求は、新たなデータ値用の新たなトークンがデータベースに追加されるよう、かつ、名前がトークン値Ｔ２に等しいようなトークン値を追加するよう、ＤＮＲエージェントに対して指示する。前述のように、Ｓａｎｃｈｅｚという名前に対応するトークン値が、ＤＮＲエージェントによって用いられたのと同じトークン化規則を適用するＤＮＲによって決定される。

【００５８】

ＤＮＲは、本明細書で具体的に例示しないさらに別の種別のデータベースアクセス要求を取り扱ったり書き換えたりしてもよい。例えば、ユーザは特定のデータ記録の削除要求を出すことができる。もちろん、記録を削除する時、トークン化しないこと、または非トークン化が必要であるが、ＤＮＲが、ＤＮＲエージェントに記録だけでなくトークン－データ関係をもトークン保管庫から除去するように指示するトークン除去（removeToken）関数を追加するために要求を書き換えることにより、データをわたすことも可能である。ＤＮＲによってトークン化データベースに合わせて改変されうる要求およびパラメータ種別には、他に、「select distinct」変更子や「order by」変更子がある。

【００５９】

ＤＮＲは不完全な要求を扱うための一または複数の規則を有してもよい。図８を参照すると、ＤＮＲはステップ８０１でデータベースアクセス要求を受領し、ステップ８０２で要求が不完全な要求であるかどうか査定してもよい。不完全な要求は、一または複数の規則によって必要な情報を欠いていると判断された要求、と分類されうる。図５の表ＸＹＺ５０２の上記例を使用すると、要求は下記のようになる。

SELECT * FROM Table XYZ　（表ＸＹＺから＊を選択）

【００６０】

この例では、アステリスク、すなわちスター演算子は、ユーザが、表ＸＹＺ中の可能性のあるフィールドをすべて選択しようとしていることを示すために使用されている。しかしながら、非トークン化関数を適切に利用するためには、実際のカラム名の一覧が必要だろう。したがってＤＮＲはステップ８０２で、要求が不完全であると判断し、ステップ８０３へ進行してもよく、そこで、欠落しているデータを求める要求を送付する。この要求は、データベース、データベース上のＤＮＲエージェント、またはカラム名を追跡できるその他の場所へ送付することができる。さらに、欠落した情報もまた、ＤＮＲ上のなんらかのメモリに保存されてもよい。

【００６１】

上記の例では、ＤＮＲは表ＸＹＺ上の全カラムの一覧をステップ８０３で要求する。その結果、名前およびＳＳＮのカラム識別子がＤＮＲで受領される。ステップ８０４では、ＤＮＲは他に欠落した情報が無いか検証し、もし無ければ、ステップ８０５へ進む。もしまだ欠落した情報があれば、ＤＮＲは、欠落した情報と同じまたは異なるソースへ、もう一つ要求を送ることができる。

【００６２】

ステップ８０５では、ＤＮＲはさらに、要求に基づく規則に従うのみならず、検索された欠落した情報を取り込むよう、データベースアクセス要求の書き換えを進める。したがって、上記例では、要求はまず、下記のように書き換えることができる。

SELECT Name, SSN FROM Table XYZ　（表ＸＹＺから名前、ＳＳＮを選択）

【００６３】

この後、要求はさらに下記のように書き換えることができる。

SELECT deToken(Name), deToken(SSN) FROM Table XYZ （表ＸＹＺから非トークン化（名前）、非トークン化（ＳＳＮ）を選択）

【００６４】

これによって確実に、表ＸＹＺ中の、トークン値ではなく、データ値が、ユーザに返される。照会は、書き換えられた後、ステップ８０６でデータベースへ送付される。

【００６５】

図９を参照して、データベースへの認証されていないアクセスを防止するＤＮＲセキュリティプロセスについて説明する。上記のように、ＤＮＲにおいて適用される一または複数のセキュリティ規則として、プロセスが実現される。ステップ９０１で要求が受領された後、ＤＮＲはステップ９０２で、ユーザが要求を行うために認証されているかどうか判断する。これには、ユーザがなんらかの要求を行うために認証されているかどうか判断することが含まれており、例えば、認証されていないシステムユーザではないか調べる、ユーザが更新要求など特定の種別の要求を行うために認証されているかどうか調べる、などである。したがって、例えば、読み出し専用の権利を有するユーザは選択要求を行えると認証されるかもしれないが、更新要求については認証されないだろう。ユーザがデータベースへのどのようなアクセスについても認証されていないと判断される場合もあるだろう。

【００６６】

もしユーザが要求を行えると認証されていなければ、ステップ９０４で、セキュリティ動作がＤＮＲによって行われる。セキュリティ動作は、様々なセキュリティ動作から選択される。例えば、ＤＮＲは、更新または挿入の場合はデータベースにその要求を無視するよう指示するフラグを、選択要求の場合は架空値を返すよう指示するフラグを設定するように、要求を書き換えてもよい。例えば、トークン化関数は多数の変数を通過させるように構成でき、そのうちのひとつをTokenize(value, fictive_value?)のような架空値フラグとしてもよい。ユーザが更新することを認証されておらず、下記の更新要求を入力したとする。

UPDATE Table XYZ, SET SSN = 123-45-6789 （ＳＳＮ＝１２３－４５－６７８９をセットして、表ＸＹＺを更新）

【００６７】

すると、セキュリティ規則を考慮に入れて書き換えられた要求は下記のようになる。

UPDATE Table XYZ, SET SSN = Tokenize(123-45-6789, true) （ＳＳＮ＝トークン化された（１２３－４５－６７８９、正）をセットして、表ＸＹＺを更新）

【００６８】

これは、トークン化関数の数値が架空であること、更新は無視すべきであることをＤＮＲエージェントに知らせるだろう。同様に、要求が選択要求であれば、非トークン化関数は架空値フラグを通過させることができる。ユーザが認証されておらず、下記のような選択要求を入力したとする。

SELECT Name FROM Table XYZ （表ＸＹＺから名前を選択）

【００６９】

すると、セキュリティ規則を考慮に入れて書き換えられた要求は下記のようになる。

SELECT deToken(Name, true) FROM Table XYZ （表ＸＹＺから非トークン化（名前、正）を選択）

【００７０】

これは、実際の非トークン化された数値ではなく、架空値を選択要求に応答して返すべきであると、ＤＮＲに対して注意を促すだろう。これは様々な方法で達成できる。例えば、乱数発生器が、トークン値をシードとして使用し、ユーザへの返信用に架空値を生成してもよい。非トークン化またはトークン化関数中の架空値フラグは、デフォルト値をｆａｌｓｅ（誤）とすることができるが、認証されていないユーザが検出された時にｔｒｕｅ（正）へ変更することができる。

【００７１】
トークン化および非トークン化関数中に架空値フラグを設けることの他に、データ値を通過させるために架空値関数が利用できる。例えば、データ値を通過させるために非トークン化関数を用いるのではなく、架空値返信（returnFictiveValue）関数を用いて、データ要求に応答して架空値を返すようＤＮＲエージェントへ指示することができる。
【００７２】
さらに、架空値は、認証されていないユーザや要求を扱う唯一の方法ではない。ユーザが認証されていない場合、空の値、すなわちナル（ＮＵＬＬ）値を返すようにＤＮＲエージェントに指示するフラグ、または非トークン化された数値の代わりにトークン値を返すようにＤＮＲエージェントに指示するフラグ、を非トークン化関数に含めることができる。さらに、ユーザが認証されていない場合、ＤＮＲは、更新、挿入、または選択要求をブロックするためにセキュリティ規則を利用することもできる。様々な変更が可能である。
【００７３】
ユーザが要求を行う権限を有していなければ、ステップ９０３で、ＤＮＲが、要求の中に保護されたデータフィールドがあるかどうか判断する。例えば、データベース中の表がいくつかのデータフィールドを含んでもよく、そのうちの一または複数が、そのデータベースまたは表へのアクセスを有するユーザの一部にのみ限定されていてもよい。したがって、前述の例の表ＸＹＺにおいて、「名前」というフィールドが全ユーザにとってアクセス可能な標準のデータフィールドである一方、「ＳＳＮ」というデータフィールドを、管理者など一部のユーザに限定することができる。異なる種別のデータフィールドについて異なる認証レベルが利用されてもよく、また、認証レベルの数は２に限らず、データベースに多数の階層の認証と関連付けられたデータフィールドが含まれていてよい。
【００７４】
保護されたデータフィールドが無ければ、ステップ９０５で、認証されたユーザ用の通常の処理と同様に、要求が処理される。もし保護されたデータフィールドがあれば、ステップ９０６で、ＤＮＲが保護されたデータフィールド各々についてユーザ認証レベルを検査し、要求が明示した方法でそのデータフィールドへアクセスする認証をユーザが有しているかを判断する。これは、ユーザの許可／認証を、保護されたデータフィールド上で要求が指定した関数を実行するために必要な許可／認証と比較することにより、達成できる。例えば、保護されたデータフィールドは、どのデータであれそれを参照するためには、ユーザは「レベル５の認証」を有しなければならないという必要条件を有していてもよい。もし要求しているユーザがレベル５よりも低い認証を有していれば、保護されたデータフィールド上の要求について認証を欠くと判断される。同様に、同じ保護されたデータフィールドが、どのデータであれそれを編集するためにはユーザが「レベル７の認証」を有しなければならないという必要条件を有していてもよい。この場合、参照アクセス権を有するレベル５のユーザであっても、保護されたデータフィールド内のデータを変更することはできないだろう。したがって、前記の表ＸＹＺの例を使用すると、「SELECT SSN FROM Table XYZ（表ＸＹＺからＳＳＮを選択）」という要求は許可されるかもしれないが、同じユーザによる「UPDATE Table XYZ, SET SSN = 123,45,6789　（ＳＳＮ＝１２３，４５，６７８９をセットして、表ＸＹＺを更新）」という要求は認証されないであろう。もちろん、認証は、レベルで整理されなくともよい。例えば、認証はユーザの役割や条件、または認証されたアクセスと認証されていないアクセスとを区別するためのその他のベースに従って、整理できる。
【００７５】
ユーザが特定の保護されたデータフィールドへのアクセスの認証を有していないようなら、ステップ９０８で、ＤＮＲは、その保護されたデータフィールドのためにセキュリティ動作を行うことができる。このセキュリティ動作は、ステップ９０４で記載された架空値フラグを含むセキュリティ動作と同様でもよいが、ユーザがアクセスを認証されていない保護されたデータフィールドのために限定的に適用することもできる。したがって、表ＸＹＺの例で、ユーザがＳＳＮフィールドではなく名前フィールドへのアクセスの認証を

有しており、下記の要求を出すとする。

SELECT Name, SSN FROM Table XYZ （表ＸＹＺから名前、ＳＳＮを選択）

【００７６】

すると、要求は、架空値フラグを含むよう下記のように書き換えられる。

SELECT detoken(Name, false), deToken(SSN, true) FROM table XYZ （表ＸＹＺから、非トークン化（名前、誤）、非トークン化（ＳＳＮ、正）を選択）

【００７７】

この書き換えられた要求がＤＮＲに指摘するのは、名前フィールド用の非トークン化関数は架空値ではなく非トークン化された名前値を返信し、かつ、ＳＳＮフィールド用の非トークン化関数は架空値を返信すべきである、ということである。さらに、上記のように、認証されていないデータフィールド用のセキュリティ動作は、そのフィールド用のナル値を返すこと、非トークン化された数値の代わりにトークン値を返すこと、または要求の該当部分をブロックすることをも、含むことができる。

【００７８】

ステップ９０７において、ＤＮＲはさらに保護されたデータフィールドがあるかどうかを判断し、もしあれば、さらに判断および処理を行うためにステップ９０６へ戻る。保護されたデータ値が他に無ければ、通常通り、要求の残りの処理がステップ９０９で継続する。

【００７９】

前述のセキュリティプロセスに使用されたように、認証は、異なる多数の種別のセキュリティ認証情報および認証スキームを参照することができる。例えば、認証が特定のユーザではなく、なんらかの装置の識別子に基づいてもよく、受領した要求の出所である装置のネットワーク情報に認証が基づいてもよく、異なるレベルの許可または権利などの認証スキームが用いられてもよく、また、セキュリティトークン、証明書（certificate）、またはその他の形態の承認（authentication）や認証が用いられてもよい。さらに、架空値フラグはデフォルト値としてｆａｌｓｅに設定されていると述べたが、フラグはデフォルト値としてｔｒｕｅに設定されてもよく（例えば、デフォルト値は認証されていないユーザまたは要求をとってもよい）、要求認証が確認された時にｆａｌｓｅに変更されてもよい。様々な変形が可能であり、セキュリティ規則は、ここに開示する承認や認証の具体例に限定されない。

【００８０】

データ値を受領しデータベースへ渡すことに加え、ＤＮＲはまた、セキュリティトークンまたは認証情報を受領しデータベースへ渡すことができる。ＤＮＲは、要求とともにセキュリティトークンをアプリケーションから受領する。セキュリティトークンは、ＤＮＲがユーザを確認し、かつユーザが認証されていることを確認できるようにする、パスワードなどの認証情報や、証明書、またはその他のデータであればよい。

【００８１】

ＤＮＲは、書き換える前にセキュリティトークンまたは認証情報を承認するかまたは確認して、要求をデータベースへ送付することができる。もしセキュリティトークンが有効であれば、ＤＮＲは、前述した架空値フラグと同様のフラグを利用して、要求が安全で認証されていることをＤＮＲエージェントに示すことができる。例えば、トークン化（または非トークン化）関数は、Tokenize (data value, valid_security_credential?)のように、一つはデータ値、もう一つはセキュリティトークンの有効性を示す、二つのパラメータを通過させてもよい。

【００８２】

状況により、このセキュリティトークンフラグを、架空値フラグに加えて、通過させることもできる。例えば、ユーザに関連付けられたセキュリティトークンが有効であっても、ユーザが特定のデータフィールドにアクセスするには不適切な許可を有する場合、トークン化または非トークン化関数中のデータ値に加えて、二つのフラグを通過させることができる。

【００８３】
セキュリティフラグは、要求の取り扱い方を判断するために、データベースまたはデータベース上で作動するＤＮＲエージェントによって用いられる。例えば、ｆａｌｓｅに設定されたセキュリティフラグと共に非トークン化関数が受領されると、非トークン化ステップを省略してもよく、その結果、トークン値がユーザへ返される。同様に、ｆａｌｓｅに設定されたセキュリティフラグと共にトークン化関数が受領されると、ＤＮＲエージェントは一緒に渡されたデータ値をトークン化する代わりに、関数を無視することができる。deToken(Name, fictive_value?, valid_security credential?)のような非トークン化関数は、セキュリティ認証情報が有効であるが名前を検索するための適切な許可をユーザが有していないといった場合には、名前用の架空値を返し、セキュリティ認証情報が有効ではない場合には、数値を返さない。

【００８４】
さらに、ＤＮＲに受領されたセキュリティトークン／認証情報は、関数のうちの１つにおける引数として、ＤＮＲエージェントに渡される。このシナリオにおいて、セキュリティトークン／認証情報の有効性は、ＤＮＲではなく、ＤＮＲエージェントで直接査定される。

【００８５】
一または複数の上記の技術は、一または複数のコンピュータシステム中で実現されることができ、もしくは、一または複数のコンピュータシステムを含むことができる。図１０は、コンピューティング環境１０００の一般化された例を示す。コンピューティング環境１０００は、記載された実施形態の用途や機能の範囲について限定を示唆するものではない。

【００８６】
図１０を参照すると、コンピューティング環境１００は少なくとも一つの処理ユニット１０１０およびメモリ１０２０を含む。処理ユニット１０１０は、コンピュータ実行可能な命令を実行し、現実のまたは仮想のプロセッサであってもよい。多重処理システムにおいては、多数の処理ユニットがコンピュータ実行可能な命令を実行して処理パワーを増加させている。メモリ１０２０は、一時的なメモリ（例えば、レジスタ、キャッシュ、ＲＡＭなど）、非一時的なメモリ（例えば、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリなど）、またはその二つの組合せであってもよい。メモリ１０２０は、上記技術を実現するソフトウェア１０８０を記憶していてもよい。

【００８７】
コンピューティング環境は、さらに追加の構成を有していてもよい。例えば、コンピューティング環境１０００は、記憶装置１０４０、一または複数の入力装置１０５０、一または複数の出力装置１０６０、および一または複数の通信接続部１０９０を備える。バス、制御器、またはネットワークなどの相互接続機構１０７０は、コンピューティング環境１０００の構成部分を相互接続する。通常、オペレーティングシステムソフトウエアまたはファームウェア（図示省略）は、コンピューティング環境１０００で作動するその他のソフトウェア用の操作環境を提供し、コンピューティング環境１０００の構成部分の動作を調整する。

【００８８】
記憶装置１０４０は着脱可能であっても、着脱不可であってもよく、磁気ディスク、磁気テープ、カセット、ＣＤ－ＲＯＭ、ＣＤ－ＲＷ、ＤＶＤなど、情報を記憶するために用いることができ、コンピューティング環境１０００中でアクセスすることができる媒体を含む。記憶装置１０４０は、ソフトウェア１０８０への命令を記憶してもよい。

【００８９】
入力装置（複数も可）１０５０は、キーボード、マウス、ペン、トラックボール、タッチ画面、またはゲーム制御器などのタッチ入力装置、音声入力装置、走査装置、デジタルカメラ、遠隔制御、コンピューティング環境１０００に入力を行う他の装置であってもよい。出力装置（複数も可）１０６０は、表示器、テレビ、モニタ、プリンタ、スピーカ、

コンピューティング環境１０００からの出力を行う他の装置であってもよい。

【００９０】

通信接続部（複数も可）１０９０は、通信媒体を介して別のコンピューティングエンティティへの通信を可能にする。通信媒体は、コンピュータ実行可能な命令、音声または画像情報、変調データ信号のデータ、等の情報を伝達する。変調データ信号は、信号の特徴の一つまたは複数が信号中の情報を暗号化するように設定または変更された信号である。例であって限定ではないが、通信媒体としては、電気、光学、ＲＦ、赤外線、音響などのキャリアによって実現される有線または無線技術などがある。

【００９１】

インプリメンテーション（実現）は、コンピュータ可読媒体の一般的なコンテキストで説明できる。コンピュータ可読媒体は、コンピューティング環境内でアクセスできる媒体であれば、いずれの媒体であってもよい。例であって限定ではないが、コンピューティング環境１０００内においては、コンピュータ可読媒体としては、メモリ１０２０、記憶装置１０４０、通信媒体、および上記のいずれかの組み合わせなどが挙げられる。

【００９２】

図１０は、コンピューティング環境１０００、表示装置１０６０、および入力装置１０５０を個別の装置として示しているが、これは識別のしやすさのためである。コンピューティング環境１０００、表示装置１０６０、および入力装置１０５０は個別の装置（例えば、モニタやマウスに有線で接続されたパーソナルコンピュータなど）でもよく、単一の装置に統合されたもの（例えば、スマートフォンやタブレットなどタッチディスプレイを備えたモバイル装置など）でもよく、または装置の組み合わせ（例えば、タッチ－スクリーン表示装置と動作的に連結される演算装置、単一の表示装置および入力装置に取り付けられた複数の演算装置など）であってもよい。コンピューティング環境１０００はセットトップボックスや、パーソナルコンピュータ、または、一または複数のサーバであってよく、例えばネットワーク接続されたサーバ、クラスタ化サーバ環境、または演算装置のクラウドネットワークであってもよい。

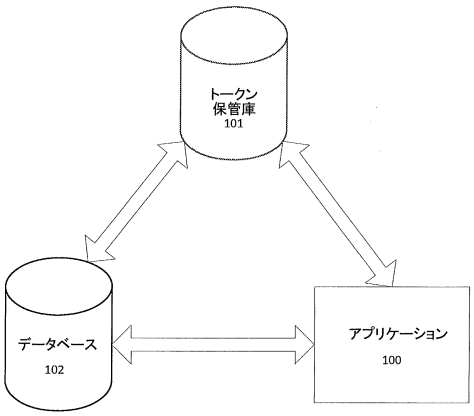
【００９３】

記載された実施形態を参照して本発明の原理を記載し説明したが、記載された実施形態は、構成や詳細においてかかる原理から逸脱することなく変更できることは、認識されるであろう。特段の記載の無い限り、本明細書に記載されたプログラム、プロセス、または方法は、特定の種別のコンピューティング環境に関連するわけではなく、限定もされないことを、理解されたい。各種の汎用のまたは特殊なコンピューティング環境は、本明細書に記載された教示に従って、使用されたり操作が実行されたりしてもよい。ソフトウェアに示される本実施形態の要件は、ハードウェアで実現されてよく、その逆も可である。

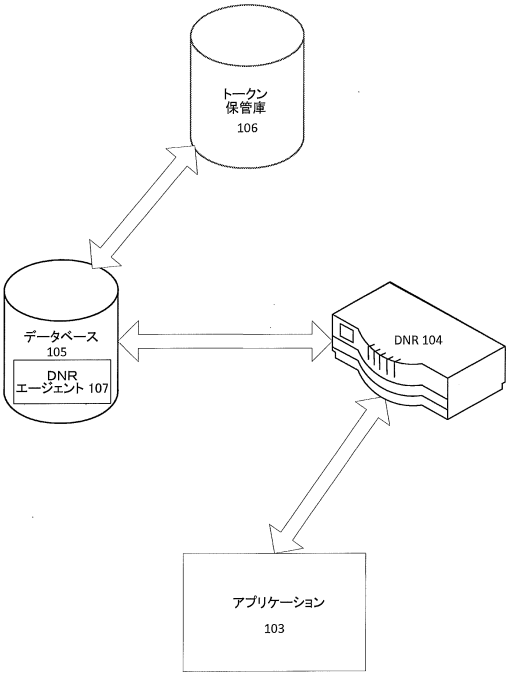
【００９４】

本発明の原理が適用できる、考えられうる多くの実施形態を鑑み、以下の請求項および均等物の範囲および精神に該当するような実施形態はすべて、本発明であると主張する。

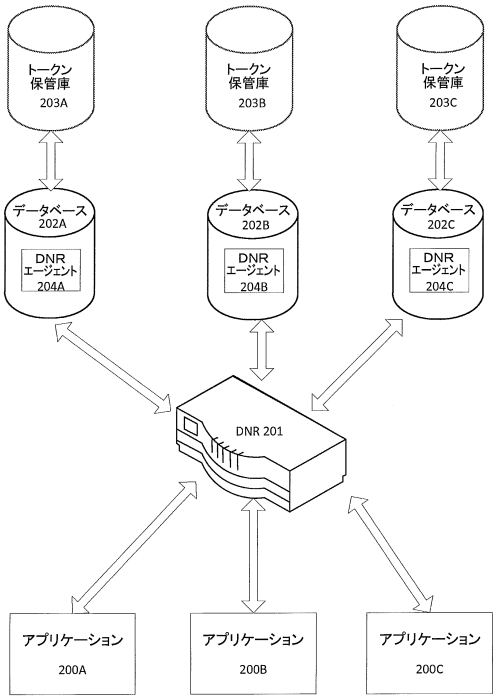
【図１Ａ】


トークン
保管庫
101
データベース
102
アプリケーション
100

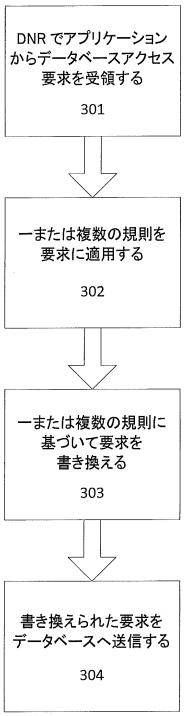
【図１Ｂ】


トークン
保管庫
106
データベース
105
DNR
エージェント 107
DNR 104
アプリケーション
103

【図２】


トークン
保管庫
203A
トークン
保管庫
203B
トークン
保管庫
203C
データベース
202A
DNR
エージェント
204A
データベース
202B
DNR
エージェント
204B
データベース
202C
DNR
エージェント
204C
DNR 201
アプリケーション
200A
アプリケーション
200B
アプリケーション
200C

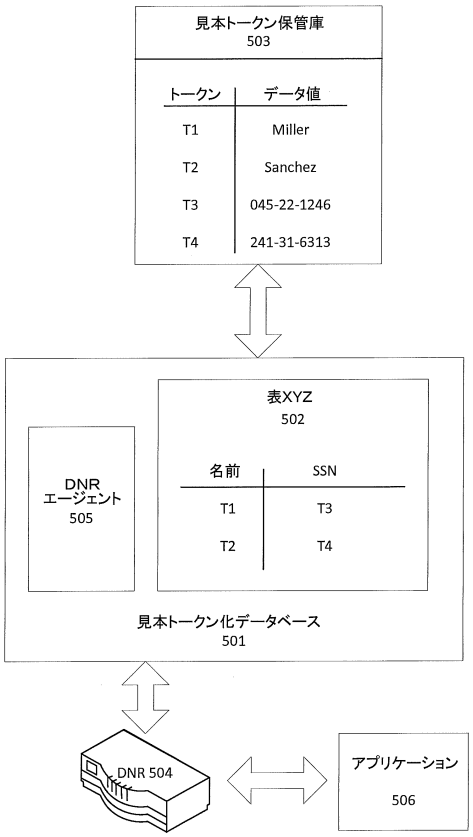
【図３】


DNR でアプリケーション
からデータベースアクセス
要求を受領する
301
ーまたは複数の規則を
要求に適用する
302
ーまたは複数の規則に
基づいて要求を
書き換える
303
書き換えられた要求を
データベースへ送信する
304

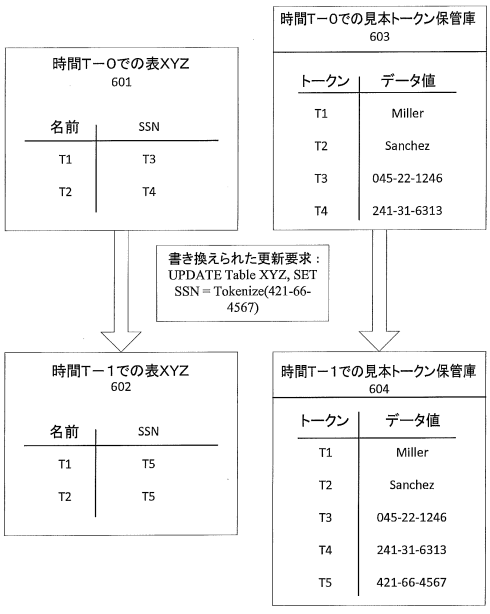
【図４】


規則
400
データ検索
要求規則
401
データ更新
要求規則
402
データ挿入
要求規則
403
アクセス要求
フィルタ項規則
404
トークン化
API規則
405
不完全
要求規則
406
認証規則
407
セキュリティ規則
408
ルーティング規則
409

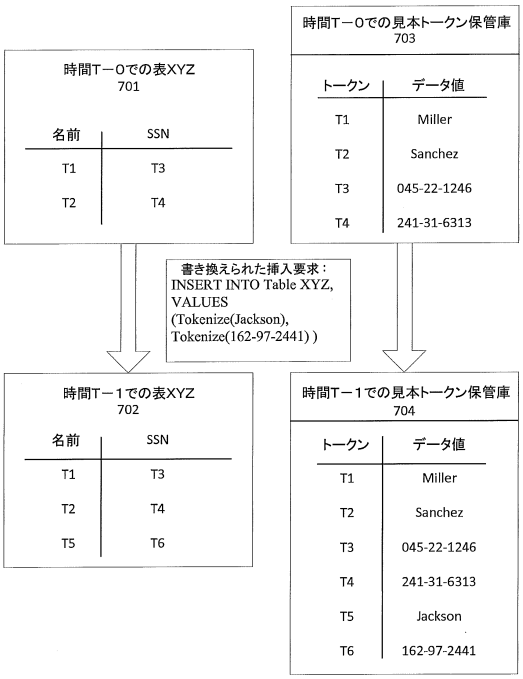
【図５】


見本トークン保管庫
503
トークン
データ値
T1
Miller
T2
Sanchez
T3
045-22-1246
T4
241-31-6313
表XYZ
502
名前
SSN
T1
T3
T2
T4
DNR
エージェント
505
見本トークン化データベース
501
DNR 504
アプリケーション
506

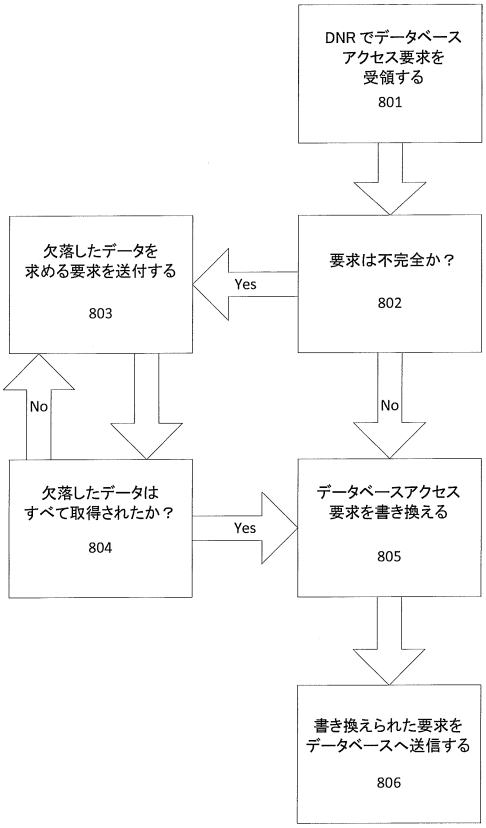
【図６】


時間T－0での表XYZ
601
名前
SSN
T1
T3
T2
T4
時間T－0での見本トークン保管庫
603
トークン
データ値
T1
Miller
T2
Sanchez
T3
045-22-1246
T4
241-31-6313
書き換えられた更新要求：
UPDATE Table XYZ, SET
SSN = Tokenize(421-66-4567)
時間T－1での表XYZ
602
名前
SSN
T1
T5
T2
T5
時間T－1での見本トークン保管庫
604
トークン
データ値
T1
Miller
T2
Sanchez
T3
045-22-1246
T4
241-31-6313
T5
421-66-4567

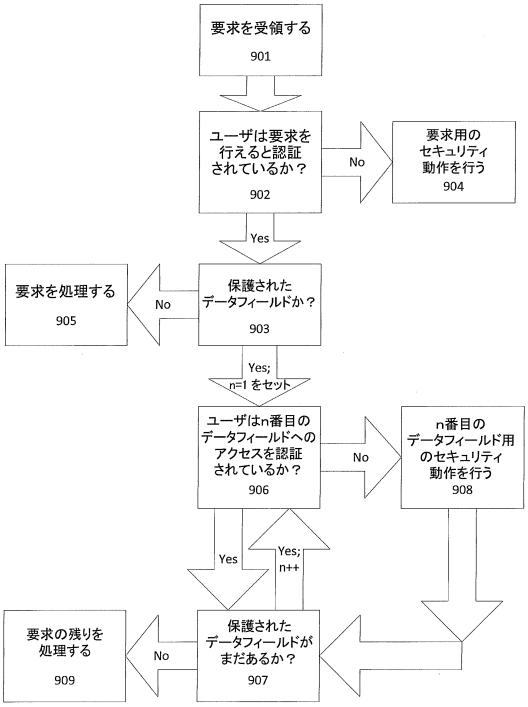
【図７】


時間T－0での表XYZ
701
名前
SSN
T1
T3
T2
T4
時間T－0での見本トークン保管庫
703
トークン
データ値
T1
Miller
T2
Sanchez
T3
045-22-1246
T4
241-31-6313
書き換えられた挿入要求：
INSERT INTO Table XYZ,
VALUES
(Tokenize(Jackson),
Tokenize(162-97-2441))
時間T－1での表XYZ
702
名前
SSN
T1
T3
T2
T4
T5
T6
時間T－1での見本トークン保管庫
704
トークン
データ値
T1
Miller
T2
Sanchez
T3
045-22-1246
T4
241-31-6313
T5
Jackson
T6
162-97-2441

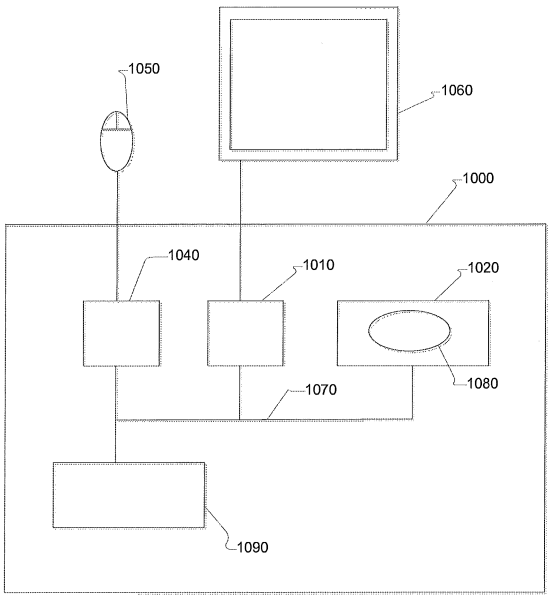
【図８】


DNR でデータベース
アクセス要求を
受領する
801
要求は不完全か？
802
Yes
欠落したデータを
求める要求を送付する
803
No
No
欠落したデータは
すべて取得されたか？
804
Yes
データベースアクセス
要求を書き換える
805
書き換えられた要求を
データベースへ送信する
806

【図９】


要求を受領する
901
ユーザは要求を
行えると認証
されているか？
902
No
要求用の
セキュリティ
動作を行う
904
Yes
要求を処理する
905
No
保護された
データフィールドか？
903
Yes;
n=1 をセット
ユーザはn番目の
データフィールドへの
アクセスを認証
されているか？
906
No
n番目の
データフィールド用
のセキュリティ
動作を行う
908
Yes
Yes;
n++
要求の残りを
処理する
909
No
保護された
データフィールドが
まだあるか？
907

【図１０】


1050
1060
1000
1040
1010
1020
1080
1070
1090

フロントページの続き

審査官　脇岡　剛

(56)参考文献　米国特許第８４５８４８７（ＵＳ，Ｂ１）
米国特許出願公開第２０１３／０１９１６５０（ＵＳ，Ａ１）
米国特許出願公開第２００５／００８６２５６（ＵＳ，Ａ１）
特開２００９－０９９１５１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　１７／３０
Ｇ０６Ｆ　２１／６０