

【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20年4月3日(2008.4.3)

【公開番号】特開2002-197065(P2002-197065A)

【公開日】平成14年7月12日(2002.7.12)

【出願番号】特願2000-396990(P2000-396990)

【国際特許分類】

G 0 6 F	21/20	(2006.01)
G 0 6 K	17/00	(2006.01)
G 0 8 B	25/04	(2006.01)
H 0 4 M	11/04	(2006.01)
G 0 6 K	19/10	(2006.01)
H 0 4 L	9/10	(2006.01)
H 0 4 L	9/30	(2006.01)
H 0 4 L	9/32	(2006.01)

【F I】

G 0 6 F	15/00	3 3 0 E
G 0 6 K	17/00	T
G 0 8 B	25/04	G
H 0 4 M	11/04	
G 0 6 K	19/00	R
H 0 4 L	9/00	6 2 1 A
H 0 4 L	9/00	6 6 3
H 0 4 L	9/00	6 7 1
H 0 4 L	9/00	6 7 3 E

【手続補正書】

【提出日】平成19年12月26日(2007.12.26)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

記録媒体に記録する照合データの数を、一個の真正データと複数個の囮データとを含む個数として、一個の真正データと複数個の囮データとが混在する照合データを有する本人認証データ記録媒体を設け、

前記本人認証データ記録媒体に、暗号鍵を含む機密情報を記録するに際して多数の照合データのうちの一個を特定して真正データを決定し、残余の照合データを囮データとして特定し、一個の真正データの示す情報を、本人認証データ記録媒体における、暗号鍵を含む機密情報を示す認証データとして特定し、

本人認証データ記録媒体を使用して認証データを入力するにあたり、本人認証データ記録媒体より一個の真正データを選択することで、真正な認証データが選択されたものとして本人認証を有効とし、

本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より一個の真正データを選択するに際し、少なくとも1個の囮データが含まれるとき盜難不正アクセスと判断し、本人認証を無効とするとともに、盜難警報を発生することを特徴とする、本人認証における盜難・監禁等の非常状態通報システム。

【請求項 2】

記録媒体に記録する照合データの数を、複数個の真正データと複数個の囮データとを含む個数として、複数個の真正データと複数個の囮データとが混在する照合データを有する本人認証データ記録媒体を設け、

前記本人認証データ記録媒体に、暗号鍵を含む機密情報を記録するに際して多数の照合データのうちの複数個を位置又は特徴および順序を特定して真正データを決定し、残余の照合データを囮データとして特定し、複数個の真正データの示す情報を、本人認証データ記録媒体における、暗号鍵を含む機密情報を示す認証データとして特定し、

本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より複数個の真正データを正しい順序で選択することで、真正な照合データが選択されたものとして本人認証を有効とし、

本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より複数個の真正データを選択するに際し、設定個数以上の囮データが含まれるとき盜難不正アクセスと判断し、本人認証を無効とするとともに、盜難警報を発生し、

盜難警報を発生を検知した管理センターは以後の当該本人認証データ記録媒体の使用を無効とすることを特徴とする、本人認証における盜難・監禁等の非常状態通報システム。

【請求項 3】

記録媒体に記録する照合データの数を、一個または複数個の真正データと複数個の囮データとを含む個数として、一個または複数個の真正データと複数個の囮データとが混在する照合データを有する本人認証データ記録媒体を設け、

前記本人認証データ記録媒体に、暗号鍵を含む機密情報を記録するに際して多数の照合データのうちの一個の真正データの決定 / または複数個の真正データおよび読み取り順序を決定し、残余の照合データを囮データとして特定し、一個の真正データ / または適正な読み取り順序による複数個の真正データの示す情報を、本人認証データ記録媒体における、暗号鍵を含む機密情報を示す認証データとして特定し、

さらに、囮データの一部を監禁通報データとして特定し、

本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体の照合データより一個の真正データの選択 / または複数個の真正データおよび読み取り順序を選択するとともに、前記監禁通報データを追加させることにより、

真正な認証データが選択されたものとして本人認証を有効とするとともに、真正データに追加して少なくとも 1 個の監禁通報データが含まれることで、本人が第 3 者の支配下にあると判断し、

管理センターは、本人認証を有効とするとともに、監禁通報警報を発生することを特徴とする、本人認証における盜難・監禁等の非常状態通報システム。

【請求項 4】

照合データ（パスワード）を記録した本人認証データ記録媒体の使用し、該本人認証データ記録媒体を有する認証端末機器と認証管理側機器との間で被承認者の入力操作による照合データの一一致により認証成立とする、本人認証システムにおいて、

照合データ（パスワード）を、その数を、複数個の真正データと複数個の囮データとを含む個数として、複数個の真正データと複数個の囮データとが混在し且つシンボル、記号、写真、二次元コード等で構成し、

照合データの記録媒体への記録に際して、被承認者は、

照合データを構成する多数の単位データのうち、複数個を位置又は特徴および順序を特定して真正データを決定し、残余の単位データを囮データとして特定し、

更に、囮データの一部を監禁通報データとして特定し、

本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より複数個の真正データを正しい順序で選択することで、真正な認証データが選択されたものとして本人認証を有効とし、

本人認証データ記録媒体の入力操作にあたり、囮データの選択個数が設定個数未満であるときは、再度の認証入力を有効とし、

本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より複数個の真正データを選択するに際し、設定個数以上の囲データが含まれるとき盜難不正アクセスと判断し、本人認証を無効とするとともに、盜難警報を発生し、盜難警報の発生を検知した管理センターは以後の当該本人認証データ記録媒体の使用を無効とし、

本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より複数個の真正データを選択するとともに、少なくとも一個の監禁警報データが含まれている場合には、真正な認証データが選択されたものとして本人認証を有効とし、更に、本人が第三者の支配下にあるものとして、管理センターは監禁通報警報を発生することを特徴とする本人認証における盜難・監禁等の非常状態通報システム。

【請求項 5】

照合データ（パスワード）を記録した本人認証データ記録媒体の使用し、該本人認証データ記録媒体を有する認証端末機器と認証管理側機器との間で被承認者の入力操作による照合データの一一致により認証成立とする、本人認証システムにおいて、

照合データ（パスワード）を、その数を、複数個の真正データと複数個の囲データとを含む個数として、複数個の真正データと複数個の囲データとが混在し且つシンボル、記号、写真、二次元コード等で構成し、

照合データの記録媒体への記録に際して、被承認者は、

照合データを構成する多数の単位データのうち、複数個を位置又は特徴および順序を特定して真正データを決定し、残余の単位データを囲データとして特定し、

更に、囲データの一部を監禁通報データとして特定し、

本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より複数個の真正データを正しい順序で選択することで、真正な認証データが選択されたものとして本人認証を有効とし、

本人認証データ記録媒体の入力操作にあたり、囲データの選択個数が設定個数未満であるときは、再度の認証入力を有効とし、

本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より複数個の真正データを選択するに際し、設定個数以上の囲データが含まれるとき盜難不正アクセスと判断し、本人認証を無効とするとともに、盜難警報を発生し、盜難警報の発生を検知した管理センターは以後の当該本人認証データ記録媒体の使用を無効とし、

本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より複数個の真正データを選択し、さらに監禁警報データが存在しない場合には、真正な認証データが選択されたものとして本人認証を有効とし、更に、本人が第三者の支配下にあることを管理センターに通報する

ことを特徴とする本人認証における盜難・監禁等の非常状態通報システム。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0 0 0 4

【補正方法】変更

【補正の内容】

【0 0 0 4】

【課題を解決するための手段】

本願請求項 1 の発明は、記録媒体に記録する照合データの数を、一個の真正データと複数個の囲データとを含む個数として、一個の真正データと複数個の囲データとが混在する照合データを有する本人認証データ記録媒体を設け、前記本人認証データ記録媒体に、暗号鍵を含む機密情報を記録するに際して多数の照合データのうちの一個を特定して真正データを決定し、残余の照合データを囲データとして特定し、一個の真正データの示す情報を、本人認証データ記録媒体における、暗号鍵を含む機密情報を示す認証データとして特定し、本人認証データ記録媒体を使用して認証データを入力するにあたり、本人認証データ記録媒体より一個の真正データを選択することで、真正な認証データが選択されたものとして本人認証を有効とし、本人認証データ記録媒体の入力操作にあたり、本人認証デー

タ記録媒体より一個の真正データを選択するに際し、少なくとも1個の囲データが含まれるとき盜難不正アクセスと判断し、本人認証を無効とともに、盜難警報を発生することを特徴とする、本人認証における盜難・監禁等の非常状態通報システムを提供する。

本願請求項2の発明は、請求項1の発明において、前記本人認証データ記録媒体における真正データを複数個とする。即ち、多数の照合データのうちの複数個を位置および順序を特定して真正データを決定し、残余の照合データを囲データとして特定し、複数個の真正データの示す情報を、本人認証データ記録媒体の認証データとする。

よって、本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より複数個の真正データを正しい順序で選択することで、真正な照合データが選択されたものとして本人認証を有効とすることを特徴とする。

本願請求項3および本願請求項4の発明は、請求項1または請求項2の発明において、囲データの一部を監禁通報データとして特定し、真正データに追加して少なくとも1個の監禁通報データが含まれることで、本人が第3者の支配下にあると判断し、本人認証とともに監禁通報警報を発生することを特徴とする。

即ち、真正な認証データが選択されたものとして本人認証を有効とするとともに、真正データに追加して少なくとも1個の監禁通報データが含まれることで、本人が第3者の支配下にあると判断し、管理センターは、本人認証を有効とするとともに、監禁通報警報を発生することを特徴とする。

本願請求項5の発明は、請求項3の発明において、本人認証データ記録媒体の入力操作にあたり、本人認証データ記録媒体より複数個の真正データを選択し、さらに監禁警報データが存在しない場合には、真正な認証データが選択されたものとして本人認証を有効とし、更に、本人が第三者の支配下にあることを管理センターに通報する。

即ち、請求項3の発明においては、監禁警報データは、第三者の支配下にある本人認証者が、付加データ（付加信号）として入力操作することで、本人が第三者の支配下にあることを管理センターに通報する。

しかし、請求項4の発明においては、監禁警報データは、付加データ（付加信号）として常に入力操作するが、第三者の支配下にあるときは、付加データ（付加信号）である監禁警報データの入力操作を欠くことで、監禁警報データを不存在として、本人が第三者の支配下にあることを管理センターに通報する。

したがって、常時は付加データ（付加信号）として常に入力操作を必要とするが、第三者の支配下にある緊急時には、第三者に感知されることなく緊急通報することができる。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0019

【補正方法】変更

【補正の内容】

【0019】

【発明の効果】

本願発明は、多数の類似した照合データを記録した本人認証データ記録媒体1を使用しつつ多数の類似した照合データより正データを本人記憶により選択指示することで、認証データの他人による本人認証を確実に阻止することができる。

且つ、認証データの送り込みに際し、囲データが含まれている場合には、盜難警報を発生することで、本人認証データ記録媒体の紛失・盜難による不正アクセスに対する対策を強化することができる。

本願発明は、本人認証について、悪意の第3者の支配下におかれたユーザーからのアクセスに対し、ユーザーとシステムの双方の保護・保全をはかることができる効果を有する。

また、悪意の第3者の支配下において、悪意の第3者に感知されることなく、監禁通報を発信することができる。