(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6324344号
(P6324344)
(45)発行日　平成30年5月16日(2018.5.16)　(24)登録日　平成30年4月20日(2018.4.20)

(51)Int.Cl.　F I
G06F 21/46 (2013.01)　G06F 21/46
G06F 21/57 (2013.01)　G06F 21/57　３７０

請求項の数 4　(全 14 頁)

(21)出願番号　特願2015-86996(P2015-86996)
(22)出願日　平成27年4月21日(2015.4.21)
(65)公開番号　特開2016-206902(P2016-206902A)
(43)公開日　平成28年12月8日(2016.12.8)
審査請求日　平成29年6月23日(2017.6.23)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　100147485
弁理士　杉村　憲司
(74)代理人　100153017
弁理士　大倉　昭人
(72)発明者　神崎　賢一
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　山越　公洋
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】アクセス権限情報管理システム、端末機器及びアクセス権限情報管理方法

(57)【特許請求の範囲】
【請求項１】
端末機器と、ネットワークを通じて該端末機器と接続するネットワークシステムとを備えるアクセス権限情報管理システムであって、
前記端末機器は、
前記端末機器にアクセスして設定制御する際に利用するアクセス権限情報を保持する保持部と、
前記保持部のアクセス権限情報を検査する検査部と、を備え、
前記検査部は、前記アクセス権限情報の桁数及び文字種を検出し、該検出の結果に基づいて、総当たり攻撃に要する時間を算出し、該時間が所定時間内である場合、アクセス権限情報に脆弱性があると判定し、該判定を所定の時期に繰り返し実施する、
ことを特徴とするアクセス権限情報管理システム。
【請求項２】
前記検査部は、さらに、前記アクセス権限情報を検査するための検査情報を前記ネットワークシステムから取得し、該検査情報に基づいて、アクセス権限情報に脆弱性があるか否かを判定し、該判定を所定の時期に繰り返し実施する、請求項１に記載のアクセス権限情報管理システム。
【請求項３】
ネットワークシステムとネットワークを通じて接続する端末機器であって、
前記端末機器にアクセスして設定制御する際に利用するアクセス権限情報を保持する保

持部と、
前記保持部のアクセス権限情報を検査する検査部と、を備え、
前記検査部は、前記アクセス権限情報の桁数及び文字種を検出し、該検出の結果に基づいて、総当たり攻撃に要する時間を算出し、該時間が所定時間内である場合、アクセス権限情報に脆弱性があると判定し、該判定を所定の時期に繰り返し実施する、
ことを特徴とする端末機器。
【請求項４】
端末機器と、ネットワークを通じて該端末機器と接続するネットワークシステムとを備えるアクセス権限情報管理システムにおいて、該端末機器にアクセスして設定制御する際に利用するアクセス権限情報を検査するアクセス権限情報管理方法であって、
前記端末機器によって、
前記アクセス権限情報の桁数及び文字種を検出し、該検出の結果に基づいて、総当たり攻撃に要する時間を算出するステップと、
前記総当たり攻撃に要する時間が所定時間内である場合、アクセス権限情報に脆弱性があると判定するステップと、
前記判定するステップにおいて、アクセス権限情報に脆弱性があると判定した場合、前記端末機器の利用者に通知するステップと、を含み、
前記判定するステップを所定の時期に繰り返し実施する、
ことを特徴とするアクセス権限情報管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、端末機器にアクセスして設定制御する際に利用するアクセス権限情報の漏洩を防止するアクセス権限情報管理システム、端末機器及びアクセス権限情報管理方法に関する。
【背景技術】
【０００２】
近年、通信ネットワークの発展に伴い、身近な端末機器や、産業または交通に利用されている端末機器をネットワークに接続し、自動制御を行ったり、様々なサービスに利用する手法が、浸透しつつある。
【０００３】
それにより、端末機器が悪意ある第三者に侵入されて乗っ取られたり、端末機器にマルウェアを仕込まれたりするリスクが増加している。この場合、その端末機器の利用者に損害が発生したり、ネットワークが悪影響を受けることとなる。
【０００４】
このようなリスクの原因は、端末機器にアクセスして設定制御する際に利用する情報（以下、「アクセス権限情報」という）が、危殆化してしまい、悪意ある第三者による端末機器への侵入を許してしまうことにある。アクセス権限情報には、例えば、特権ＩＤ、システムＩＤ、管理者アカウント等がある。
【０００５】
端末機器への第三者の侵入を防ぐ対策としては、端末機器の管理者自らが、アクセス権限情報を定期的に変更する方法や、アクセス権限情報の原本とは別のアクセス権限情報を、派生導出させて利用する方法が知られている（例えば、特許文献１）。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００９－２５８８２０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】

しかしながら、端末機器の管理者自らが、アクセス権限情報を定期的に変更するとしても、アクセス権限情報が漏洩し悪意ある第三者が端末機器へ侵入してしまった場合に、管理者がその侵入に気付かなければ、次のアクセス権限情報の変更時まで、悪意ある第三者による端末機器への自由な侵入を許してしまうおそれがあった。

【０００８】

また、アクセス権限情報の原本とは別の派生導出させたアクセス権限情報を利用するとしても、原本が危殆化により流出してしまえば、悪意ある第三者による端末機器への侵入を許してしまうおそれがあった。

【０００９】

本発明の目的は、上述の問題に鑑みてなされたものであり、悪意ある第三者による端末機器への侵入を防ぎ、また、侵入された場合でも被害の甚大化を防ぐアクセス権限情報管理システム、端末機器及びアクセス権限情報管理方法を提供することにある。

【課題を解決するための手段】

【００１１】

また、上記課題を解決するため、本発明に係るアクセス権限情報管理システムは、端末機器と、ネットワークを通じて該端末機器と接続するネットワークシステムとを備えるアクセス権限情報管理システムであって、前記端末機器は、前記端末機器にアクセスして設定制御する際に利用するアクセス権限情報を保持する保持部と、前記保持部のアクセス権限情報を検査する検査部と、を備え、前記検査部は、前記アクセス権限情報の桁数及び文字種を検出し、該検出の結果に基づいて、総当たり攻撃に要する時間を算出し、該時間が所定時間内である場合、アクセス権限情報に脆弱性があると判定し、該判定を所定の時期に繰り返し実施する、ことを特徴とする。

【００１３】

また、上記課題を解決するため、本発明に係る端末機器は、ネットワークシステムとネットワークを通じて接続する端末機器であって、前記端末機器にアクセスして設定制御する際に利用するアクセス権限情報を保持する保持部と、前記保持部のアクセス権限情報を検査する検査部と、を備え、前記検査部は、前記アクセス権限情報の桁数及び文字種を検出し、該検出の結果に基づいて、総当たり攻撃に要する時間を算出し、該時間が所定時間内である場合、アクセス権限情報に脆弱性があると判定し、該判定を所定の時期に繰り返し実施する、ことを特徴とする。

【００１４】

また、上記課題を解決するため、本発明に係るアクセス権限情報管理方法は、端末機器と、ネットワークを通じて該端末機器と接続するネットワークシステムとを備えるアクセス権限情報管理システムにおいて、該端末機器にアクセスして設定制御する際に利用するアクセス権限情報を検査するアクセス権限情報管理方法であって、前記端末機器によって、前記アクセス権限情報の桁数及び文字種を検出し、該検出の結果に基づいて、総当たり攻撃に要する時間を算出するステップと、前記総当たり攻撃に要する時間が所定時間内である場合、アクセス権限情報に脆弱性があると判定するステップと、前記判定するステップにおいて、アクセス権限情報に脆弱性があると判定した場合、前記端末機器の利用者に通知するステップと、を含み、前記判定するステップを所定の時期に繰り返し実施する、ことを特徴とする。

【発明の効果】

【００１５】

本発明に係るアクセス権限情報管理システム、端末機器及びアクセス権限情報管理方法によれば、悪意ある第三者による端末機器への侵入を防止し、また、侵入された場合でも被害の甚大化を防ぐことができる。

【図面の簡単な説明】

【００１６】

【図１】本発明の一実施形態に係るアクセス権限情報管理システムの構成の一例を示す図

である。
【図２】本発明の一実施形態に係るアクセス権限情報管理システムの動作の一例を示すフローチャートである。
【図３】本発明に係るアクセス権限情報管理システムの実施例１の動作の一例を示すフローチャートである。
【図４】本発明に係るアクセス権限情報管理システムの実施例２の動作の一例を示すフローチャートである。
【図５】本発明に係るアクセス権限情報管理システムの実施例３の動作の一例を示すフローチャートである。
【発明を実施するための形態】
【００１７】
以下、本発明の一実施形態について、図面を参照して説明する。
【００１８】
[システム構成]
図１は、本発明の一実施形態に係るアクセス権限情報管理システムの構成の一例を示す図である。図１に示すアクセス権限情報管理システム１は、端末機器１０と、ネットワークシステム２０とを備える。端末機器１０及びネットワークシステム２０は、ネットワーク３０を介して、有線又は無線により、互いに接続される。端末機器１０をネットワークシステム２０に接続する際は、端末機器１０のルート権限を所有する利用者が、アクセス権限情報を利用して接続させる。以下では、アクセス権限情報として、利用者は、管理パスワードを用いるものとして説明する。
【００１９】
端末機器１０は、管理ＰＷ（パスワード）検査部１１（検査部）と、管理ＰＷ（パスワード）保持部１２（保持部）と、入力部１３と、通知部１４と、通信部１５と、制御部１６と、データ保持部１７とを備える。なお、本発明に係る端末機器１０の各機能を説明するが、端末機器１０が備える他の機能を排除することを意図したものではないことに留意する。
【００２０】
管理ＰＷ検査部１１は、管理ＰＷ保持部１２に保持されている管理パスワードの脆弱性を検査する。また、管理ＰＷ検査部１１は、管理パスワードを検査するための検査情報を、ネットワークシステム２０から取得し保持する。そして、管理ＰＷ検査部１１は、検査情報に基づき、管理パスワードに脆弱性があるか否か判定する。管理ＰＷ保持部１２に保持されている管理パスワードが暗号化されている場合、管理ＰＷ検査部１１は、暗号化された管理パスワードを復号してから管理パスワードの脆弱性の判定を行う。管理ＰＷ検査部１１による管理パスワードの脆弱性の判定の詳細については後述する。
【００２１】
管理ＰＷ保持部１２は、管理パスワードを保持する。管理ＰＷ保持部１２は、暗号化された管理パスワードを保持してもよい。
【００２２】
入力部１３は、利用者による入力を受け付ける。入力部１３は、例えば、タッチパネル、キーボード、マイク等であり、利用者から、文字、音声等で、入力を受け付ける。入力部１３は、例えば、利用者から、管理パスワードの入力を受け付ける。なお、入力部１３は、他の端末機器等を介して入力された管理パスワードを、有線通信や無線通信等を介して受け付けてもよい。
【００２３】
通知部１４は、管理ＰＷ検査部１１が管理パスワードに脆弱性があると判定した場合、管理パスワードを使用し続けることに危険性があることを、端末機器１０の利用者に通知する。通知は、例えば、アラーム、音声、管理パスワードを使用し続けることに危険性があり緊急に変更が必要である旨の表示、管理パスワードが漏洩する危険度を示すパーセント表示等により行うことができる。

【００２４】
通信部１５は、ネットワーク３０を介して、ネットワークシステム２０と通信する。
【００２５】
制御部１６は、端末機器１０全体を制御及び管理するものであり、例えばプロセッサにより構成することができる。制御部１６は、端末機器１０の各機能を実現する処理内容を記述したプログラムを、図示しない記憶部等に格納しておき、このプログラムを読み出して実行させることで実現することができる。制御部１６は、データ保持部１７が保持しているデータ等を、通信部１５を介して、ネットワークシステム２０に送信する。なお、制御部１６は、管理ＰＷ検査部１１が管理パスワードに脆弱性があると判定した場合、通信部１５を介する端末機器１０とネットワークシステム２０との接続を遮断してもよい。
【００２６】
データ保持部１７は、各種データを保持している。データ保持部１７は、例えば、端末機器１０がセンサである場合、端末機器１０がセンサとして収集したデータを保持している。データ保持部１７に保持されたデータは、制御部１６によって、通信部１５を介してネットワークシステム２０に送信される。
【００２７】
[システム動作]
図２は、本発明の一実施形態に係るアクセス権限情報管理システムの動作の一例を示すフローチャートである。
【００２８】
工場出荷時等において、端末機器１０の管理ＰＷ保持部１２には、予め初期管理パスワードが保持されている。端末機器１０の購入者（利用者）は、この初期管理パスワードを端末機器１０の入力部１３から入力することで端末機器１０のルート権限を保持し、端末機器１０を、端末機器１０の通信部１５を介してネットワークシステム２０に接続させる。端末機器１０がネットワークシステム２０に接続されると、管理ＰＷ検査部１１は、端末機器１０の利用が開始されたことを検知する。管理ＰＷ検査部１１によって端末機器１０の利用の開始が検知されると、アクセス権限情報管理システムの処理が開始される。
【００２９】
まず、管理ＰＷ検査部１１は、一定期間内に、利用者によって初期管理パスワードが変更されたか否か判定する（ステップＳ１０１）。一定期間は、例えば、数分、数時間、数日等である。一定期間、初期管理パスワードを、任意の管理パスワードへ変更せずに、使用し続けることは危険と判断される。そのため、管理ＰＷ検査部１１が一定期間内に利用者によって初期管理パスワードが変更されていないと判定した場合は（ステップＳ１０１：Ｎｏ）、通知部１４が、管理パスワードを使用し続けることに危険性があることを、例えばアラームとして、利用者に通知する（ステップＳ１０２）。さらに、ステップＳ１０２の処理において、制御部１６が、端末機器１０とネットワークシステム２０との接続を、直ちに遮断してもよい。またこの際、制御部１６は、利用者によって初期管理パスワードが変更されるまで、端末機器１０が利用できないようにしてもよい。一方、管理ＰＷ検査部１１が一定期間内に利用者によって初期管理パスワードが変更されたと判定した場合は（ステップＳ１０１：Ｙｅｓ）、ステップＳ１０３の処理に進む。
【００３０】
次に、管理ＰＷ検査部１１は、管理パスワードを検査するための検査情報を、通信部１５を介して、ネットワークシステム２０から取得し（ステップＳ１０３）、管理ＰＷ検査部１１内に保持する。
【００３１】
そして、管理ＰＷ検査部１１は、管理ＰＷ保持部１２に保持されている管理パスワードの脆弱性を、ステップＳ１０３の処理で取得した検査情報を用いて検査する（ステップＳ１０４）。
【００３２】
その後、管理ＰＷ検査部１１は、ステップＳ１０４の処理の検査結果に基づき、管理パ

スワードに脆弱性があるか否かを判定する（ステップＳ１０５）。管理ＰＷ検査部１１は、管理パスワードに脆弱性がないと判定した場合は（ステップＳ１０５：Ｎｏ）、処理を終了して次回の検査まで待機する。一方、管理ＰＷ検査部１１は、管理パスワードに脆弱性があると判定した場合は（ステップＳ１０５：Ｙｅｓ）、ステップＳ１０６の処理に進む。

【００３３】

ステップＳ１０６の処理では、通知部１４が、管理パスワードを使用し続けることに危険性があることを、例えばアラームとして、利用者に通知する。さらに、ステップＳ１０６の処理において、制御部１６が、端末機器１０とネットワークシステム２０との接続を、直ちに遮断してもよい。またこの際、制御部１６は、利用者によって、新たな管理パスワードが入力部１３から入力されるまで、端末機器１０が利用できないようにしてもよい。

【００３４】

その後、ステップＳ１０６の処理により管理パスワードを使用し続けることに危険性があることを認知した利用者によって、新たな管理パスワードが入力部１３から入力されると、管理ＰＷ保持部１２に、新たな管理パスワードが保持される（ステップＳ１０７）。すると、端末機器１０は、ステップＳ１０４からの処理を繰り返し行う。

【００３５】

なお、端末機器１０は、ネットワークシステム２０から検査情報を取得する度ごとに、上記ステップＳ１０３からの処理を実施してもよい。また、端末機器１０は、端末機器１０のルート権限を所有する利用者によって、管理パスワードが任意の時に変更された場合には、その時ごとに上記ステップＳ１０３からの処理を開始してもよい。また、端末機器１０は、定期的に、上記ステップＳ１０３からの処理を繰り返し行ってもよい。

【００３６】

このように、外部から取得した検査情報を用いて、端末機器１０の内部で、端末機器１０の管理パスワードを検査し、管理パスワードの脆弱性を判定する。そして、管理パスワードに脆弱性があると判定した場合は、利用者に通知し、管理パスワードの変更を促すことによって、管理パスワードの脆弱性を解消する。そして、この脆弱性の判定を所定の時期に繰り返す。これにより、端末機器１０の管理パスワードの外部への漏洩を防止し、悪意ある第三者による端末機器１０への侵入を防止することができる。さらに、所定の時期に管理パスワードの検査を繰り返すことで、たとえ管理パスワードが外部に漏洩しても、悪意ある第三者による端末機器１０への侵入期間を短期化して被害の甚大化を防ぐことができる。

【００３７】

以下、上記のアクセス権限情報管理システムを基礎とした、３つの実施例を説明する。

【００３８】

[実施例１]

[システム構成]

管理ＰＷ検査部１１は、所定の間隔で、ネットワークシステム２０からパスワードリストを取得し保持する。そして、管理ＰＷ検査部１１は、取得したパスワードリストに記載された文字列と、管理ＰＷ保持部１２に保持されている管理パスワードとの一致性を検査する。さらに、管理ＰＷ検査部１１は、この一致性の検査結果に基づき、管理パスワードに脆弱性があるか否か判定する。パスワードリストについては後述する。

【００３９】

[システム動作]

図３は、本発明に係るアクセス権限情報管理システムの実施例１の動作の一例を示すフローチャートである。図３に示すステップＳ２０１，Ｓ２０２の処理は、図２に示すステップＳ１０１，Ｓ１０２と同様であるため、説明を省略する。

【００４０】

管理ＰＷ検査部１１は、所定の間隔で、ネットワークシステム２０からパスワードリス

ト（辞書）を取得し（ステップＳ２０３）、管理ＰＷ検査部１１内に保持する。所定の間隔は、例えば、数分、数時間、数日等である。ここで、パスワードリストとは、パスワードとして使用されることが多い文字列をリスト化したものである。パスワードとして使用されることが多い文字列は、時間と伴に変化する。そのため、ネットワークシステム２０上のパスワードリストも、パスワードとして使用されることが多い文字列が変化する度に更新される。管理ＰＷ検査部１１は、パスワードリストを定期的に更新するために、所定の間隔で、ネットワークシステム２０からパスワードリストを取得する。

【００４１】

次に、管理ＰＷ検査部１１は、ステップＳ２０３の処理で取得したパスワードリストに記載されている文字列と、管理ＰＷ保持部１２に保持されている管理パスワードとの一致性を検査する（ステップＳ２０４）。管理ＰＷ検査部１１は、例えば、パスワードリストに記載されている文字列と管理パスワードとが一致するか検査する。

【００４２】

その後、管理ＰＷ検査部１１は、ステップＳ２０４の処理結果に基づいて、管理パスワードに脆弱性があるか否か判定する（ステップＳ２０５）。管理ＰＷ検査部１１は、例えば、ステップＳ２０４の検査結果によりパスワードリストに記載されている文字列と管理パスワードとが一致すると評価した場合、管理パスワードに脆弱性があると判定する。

【００４３】

管理ＰＷ検査部１１が、管理パスワードに脆弱性がないと判定した場合（ステップＳ２０５：Ｎｏ）、処理を終了して次の検査まで待機する。一方、管理ＰＷ検査部１１が、管理パスワードに脆弱性があると判定した場合（ステップＳ２０５：Ｙｅｓ）、ステップＳ２０６の処理に進む。

【００４４】

ステップＳ２０６の処理では、図１に示すステップ１０６の処理と同様にして、通知部１４が、管理パスワードを使用し続けることに危険性があることを、例えばアラームとして、利用者に通知する。さらに、ステップＳ２０６の処理において、制御部１６が、通信部１５を介する端末機器１０とネットワークシステム２０との接続を、直ちに遮断してもよい。またこの際、制御部１６は、利用者によって、新たな管理パスワードが入力部１３から入力されるまで、端末機器１０が利用できないようにしてもよい。

【００４５】

ステップＳ２０７の処理は、図１に示すステップＳ１０７の処理と同様であるため、説明を省略する。

【００４６】

なお、ステップＳ２０４の処理において、管理ＰＷ検査部１１は、パスワードリストに記載されている文字列と管理パスワードとが完全に一致する場合だけでなく、部分一致する場合も、管理パスワードに脆弱性があると判定してよい。この場合、例えば、管理ＰＷ検査部１１が、管理パスワードの文字列のうち、３０％、５０％、７０％の文字列部分がパスワードリストに記載された文字列やその文字列部分と部分一致すると判定した場合に、通知部１４が、その一致する割合を、利用者に通知してもよい。さらに、部分一致を評価する場合、ステップＳ２０５の処理において、閾値を設けて管理パスワードの脆弱性を判定してもよい。例えば、管理パスワードの文字列の５０％がパスワードリストに記載されている文字列と部分一致することを閾値とした場合に、ステップＳ２０４の検査結果により管理パスワードの５０％以上がパスワードリストに記載された文字列と一致すると評価したとき、管理ＰＷ検査部１１は、管理パスワードに脆弱性があると判定する。

【００４７】

なお、上述のようにパスワードとして使用されることが多い文字列が時間と伴に変化する度にパスワードリストは更新される。そのため、管理ＰＷ検査部１１が保持するパスワードリストが更新された際に、再度、上記ステップＳ２０４からの処理を繰り返し行ってもよい。また、端末機器１０のルート権限を所有する利用者によって任意の時に管理パスワードが変更された時ごとに、あるいは、所定の検査間隔（例えば、数分、数時間、数日

等）で、定期的に上記ステップＳ２０３からの処理を繰り返し行ってもよい。また、上記を組み合わせて、ステップＳ２０３またはＳ２０４からの処理を繰り返して行ってもよい。また、所定の検査間隔で管理パスワードを検査する場合、時期や一日の時間帯等によって、検査間隔を変更してもよい。

【００４８】

このように、実施例１では、パスワードとして使用されることが多い文字列をリスト化したパスワードリストを外部から取得し、端末機器１０の内部で、パスワードリストに記載されている文字列と、管理ＰＷ保持部１２に保持している管理パスワードの文字列との一致性を検査し、管理パスワードの脆弱性を判定する。そして、管理パスワードに脆弱性があると判定した場合は、利用者に通知し、管理パスワードの変更を促すことによって、管理パスワードの脆弱性を解消する。これにより、端末機器１０の管理パスワードの外部への漏洩を防止し、悪意ある第三者による端末機器１０への侵入を防止することができる。さらに、パスワードリストを所定の時期、または、定期的に更新し、管理パスワードを検査することで、たとえ管理パスワードが外部に漏洩しても、悪意ある第三者による端末機器１０への侵入期間を短期化して被害の甚大化を防ぐことができる。

【００４９】

[実施例２]

[システム構成]

管理ＰＷ検査部１１は、管理ＰＷ保持部１２に保持されている管理パスワードの桁数と文字種を検出し、管理パスワードについて総当たり攻撃を行うのに要する時間を算出する。さらに、管理ＰＷ検査部１１は、算出した総当たり攻撃に要する時間が所定時間内であるか否か判定する。

【００５０】

通知部１４は、管理ＰＷ検査部１１が算出した総当たり攻撃に要する時間が所定時間内であると判定した場合、管理パスワードを使用し続けることに危険性があることを、端末機器１０の利用者に通知する。

【００５１】

[システム動作]

図４は、本発明に係るアクセス権限情報管理システムの実施例２の動作の一例を示すフローチャートである。図４に示すステップＳ３０１，Ｓ３０２の処理は、図２に示すステップＳ１０１，Ｓ１０２と同様であるため、説明を省略する。

【００５２】

管理ＰＷ検査部１１は、管理ＰＷ保持部１２に保持されている管理パスワードの桁数と文字種を検出し（ステップＳ３０３）、総当たり攻撃に要する時間を算出する（ステップＳ３０４）。以下、総当たり攻撃に要する時間の算出について説明する。

【００５３】

例えば、ステップＳ３０３の処理により、管理パスワードの桁数が４桁であり、管理パスワードの文字種がアルファベットと数字の２種であると検出された場合、まず、管理ＰＷ検査部１１は、アルファベットと数字からなる４桁の文字列のパターン数を算出する。そして次に、管理ＰＷ検査部１１は、その算出したパターン数と、パスワードの照合等の処理にコンピュータが費やす時間から、総当たり攻撃に要する時間を算出する。なお、総当たり攻撃に要する時間は、演算を行うコンピュータの演算性能に依存する。そのため、総当たり攻撃に要する時間の算出に関し、一般的なコンピュータの演算性能を前提に算出してもよいし、また、利用者が予め設定した演算性能に基づいて算出してもよい。また、総当たり攻撃に要する時間の算出に関し、ネットワークシステム２０から計算資源の情報を定期的に入手して算出に用いてもよい。

【００５４】

その後、管理ＰＷ検査部１１は、ステップＳ３０４の処理により算出した総当たり攻撃に要する時間が、所定時間内であるか否か判定する（ステップＳ３０５）。所定時間は、管理ＰＷ検査部１１の処理能力、管理パスワードの検査時間、管理パスワードの検査間隔

等を考慮し、利用者又は製造者等により予め設定される。総当たり攻撃に要する時間が所定時間内であるとき、管理パスワードが総当たり攻撃により漏洩する危険性は高くなる。そのため、管理ＰＷ検査部１１は、総当たり攻撃に要する時間が所定時間内である場合は（ステップＳ３０５：Ｙｅｓ）、図１に示すステップＳ１０６の処理と同様にして、通知部１４が、管理パスワードを使用し続けることに危険性があることを、例えばアラームとして、利用者に通知する（ステップＳ３０６）。さらに、ステップＳ３０６の処理において、制御部１６が、通信部１５を介する端末機器１０とネットワークシステム２０との接続を、直ちに遮断してもよい。またこの際、制御部１６は、利用者によって、新たな管理パスワードが入力部１３から入力されるまで、端末機器１０が利用できないようにしてもよい。一方、管理ＰＷ検査部１１は、総当たり攻撃に要する時間が所定時間内でない場合は（ステップＳ３０５：Ｎｏ）、処理を終了して次回の検査まで待機する。

【００５５】

ステップＳ３０７の処理は、図１に示すステップＳ１０７の処理と同様であるため、説明を省略する。

【００５６】

なお、端末機器１０のルート権限を所有する利用者によって任意の時に管理パスワードが変更された時ごとに、あるいは、所定の検査間隔（例えば、数分、数時間、数日等）で、上記ステップＳ３０３からの処理を繰り返し行ってもよいし、両者を組み合わせて行ってもよい。また、所定の検査間隔で管理パスワードを検査する場合、時期や一日の時間帯等によって、検査間隔を変更してもよい。

【００５７】

このように、実施例２では、端末機器１０は、管理ＰＷ保持部１２に保持されている管理パスワードの桁数と文字種を検出し、仮に総当たり攻撃をされた場合に管理パスワードが破られるまでにかかる総当たり攻撃に要する時間の推定時間を算出する。そして、算出した総当たり攻撃に要する時間が所定時間内であるか否か判定し、管理パスワードの脆弱性を判定する。さらに、管理パスワードに脆弱性があると判定した場合は、利用者に通知し、管理パスワードの変更を促すことによって、管理パスワードの脆弱性を解消する。これにより、端末機器１０の管理パスワードの外部への漏洩を防止し、悪意ある第三者による端末機器１０への侵入を防止することができる。さらに、所定の時期に繰り返し管理パスワードの検査を行うことで、管理パスワードの脆弱性が増した場合でも、悪意ある第三者による端末機器１０への侵入を防ぎ、また、侵入期間を短期化して被害の甚大化を防ぐことができる。

【００５８】

[実施例３]

[システム構成]

管理ＰＷ検査部１１は、ネットワークシステム２０から導出ルールを取得し保持する。そして、管理ＰＷ検査部１１は、取得した導出ルールに基づいて、パスワード候補を算出する。さらに、管理ＰＷ検査部１１は、算出したパスワード候補と、管理ＰＷ保持部１２に保持されている管理パスワードとが一致するか否か判定する。

【００５９】

通知部１４は、管理ＰＷ検査部１１が算出したパスワード候補と、管理ＰＷ保持部１２に保持されている管理パスワードとが一致すると判定した場合、管理パスワードを使用し続けることに危険性があることを、端末機器１０の利用者に通知する。

【００６０】

[システム動作]

図５は、本発明に係るアクセス権限情報管理システムの実施例３の動作の一例を示すフローチャートである。図５に示すステップＳ４０１，Ｓ４０２の処理は、図２に示すステップＳ１０１，Ｓ１０２と同様であるため、説明を省略する。

【００６１】

管理ＰＷ検査部１１は、ネットワークシステム２０から、利用者の情報からパスワード

候補を導出する導出ルールを取得し（ステップＳ４０３）、管理ＰＷ検査部１１内に保持する。さらに、管理ＰＷ検査部１１は、ステップＳ４０３の処理により取得した導出ルールに基づき、パスワード候補を算出する（ステップＳ４０４）。そして、管理ＰＷ検査部１１は、ステップＳ４０４の処理により算出したパスワード候補と、管理ＰＷ保持部１２に保持されている管理パスワードとが一致するか否か判定する（ステップＳ４０５）。

【００６２】

ここで、導出ルールの具体例について説明する。利用者は、自身に関する様々な情報（例えば、氏名、生年月日、電話番号、住所等）を用いて、パスワードを決めることが多い。導出ルールの一例として、例えば、「利用者の情報による文字列において、その文字列の各文字を、それぞれ、キーボード上のキーの位置から１つ右にずらす」というものが考えられる。この場合、利用者の情報（姓）が「ＳＡＴＯＵ」であるとすると、パスワード候補は「ＤＳＹＰＩ」と算出される。また、例えば、このようにして算出されたパスワード候補（上記の例では「ＤＳＹＰＩ」）に、所定の特殊文字（例えば、％、＄、＃等）をさらに付加するようなルールも、導出ルールの一例と考えられる。利用者の情報は、利用者が入力部１３から端末機器１０に直接入力してもよいし、管理ＰＷ検査部１１が、ステップ４０３の処理において、ネットワークシステム２０から取得してもよい。

【００６３】

管理ＰＷ検査部１１は、ステップＳ４０４の処理により算出したパスワード候補と管理パスワードとが一致しないと判定した場合（ステップＳ４０５：Ｎｏ）、処理を終了して次回の検査まで待機する。一方、管理ＰＷ検査部１１は、ステップＳ４０４の処理により算出したパスワード候補と管理パスワードが一致すると判定した場合（ステップＳ４０５：Ｙｅｓ）、ステップＳ４０６の処理に進む。算出するパスワード候補は複数であっても良い。

【００６４】

ステップＳ４０６の処理では、図１に示すステップ１０６の処理と同様にして、通知部１４が、管理パスワードを使用し続けることに危険性があることを、例えばアラームとして、利用者に通知する。さらに、ステップＳ４０６の処理において、制御部１６が、通信部１５を介する端末機器１０とネットワークシステム２０との接続を、直ちに遮断してもよい。またこの際、制御部１６は、利用者によって、新たな管理パスワードが入力部１３から入力されるまで、端末機器１０が利用できないようにしてもよい。

【００６５】

ステップＳ４０７の処理は、図１に示すステップＳ１０７の処理と同様であるため、説明を省略する。

【００６６】

なお、ステップＳ４０５の処理において、管理ＰＷ検査部１１は、パスワード候補と管理パスワードとが完全に一致する場合だけでなく、部分一致する場合も、管理パスワードに脆弱性があると判定してよい。この場合、例えば、管理ＰＷ検査部１１が、管理パスワードの文字列のうち、３０％、５０％、７０％の文字列部分がパスワード候補と部分一致すると判定した場合に、通知部１４が、その一致する割合を、利用者に通知してもよい。さらに、部分一致を評価した場合、ステップ４０５の処理において、閾値を設けて管理パスワードの脆弱性を判定してもよい。例えば、管理パスワードの文字列の５０％がパスワードリストに記載されている文字列と部分一致することを閾値とした場合に、管理パスワードの５０％以上がパスワード候補と一致すると評価したとき、管理ＰＷ検査部１１は、管理パスワードに脆弱性があると判定する。

【００６７】

なお、端末機器１０のルート権限を所有する利用者によって任意の時に管理パスワードが変更された時ごとに、あるいは、新しい導出ルールが追加された場合に、上記ステップＳ４０３からの処理を繰り返し行ってもよい。また、所定の検査間隔（例えば、数分、数時間、数日等）で、上記ステップＳ４０３からの処理を繰り返し行ってもよい。また、上記を組み合わせて、ステップＳ４０３からの処理を繰り返して行ってもよい。所定の検査

間隔で管理パスワードを検査する場合、時期や一日の時間帯等によって、検査間隔を変更してもよい。

【００６８】

このように、実施例３では、導出ルールを外部から取得し、端末機器１０の内部で、導出ルールに基づき、パスワード候補を算出する。そして、算出したパスワード候補と、管理ＰＷ保持部１２に保持されている管理パスワードとが一致するか否か判定し、管理パスワードの脆弱性を判定する。そして、管理パスワードに脆弱性があると判定した場合は、利用者に通知し、管理パスワードの変更を促すことによって、管理パスワードの脆弱性を解消する。これにより、端末機器１０の管理パスワードの外部への漏洩を防止し、悪意ある第三者による端末機器１０への侵入を防止することができる。さらに、所定の時期に繰り返し管理パスワードの検査を行うことで、たとえ管理パスワードが外部に漏洩しても、悪意ある第三者による端末機器１０への侵入期間を短期化して被害の甚大化を防ぐことができる。

【００６９】

なお、上記の実施例１～３の方法は、自由に組み合わせて実行することができる。また、上記の実施例１～３の方法は、それぞれ並列に実行してよく、また、１つずつ順に実行してもよい。また、例えば、実施例１と実施例２を実行する場合、実施例１の方法は１時間ごとに実行し、実施例２の方法は２日ごとに実行する、というように実行時間の間隔に差を付けて、実施例１と実施例２を並列に実行してもよい。

【００７０】

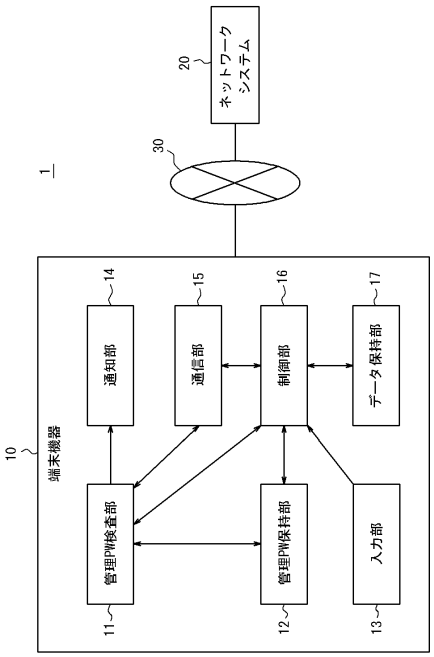
本発明を諸図面や実施例に基づき説明してきたが、当業者であれば本開示に基づき種々の変形や修正を行うことが容易であることに注意されたい。従って、これらの変形や修正は本発明の範囲に含まれることに留意されたい。例えば、各構成部、各ステップ等に含まれる機能等は論理的に矛盾しないように再配置可能であり、複数の構成部やステップ等を１つに組み合わせたり、或いは分割したりすることが可能である。また、本発明について装置を中心に説明してきたが、本発明は装置が備えるプロセッサにより実行される方法、プログラム、又はプログラムを記録した記憶媒体としても実現し得るものであり、本発明の範囲にはこれらも包含されるものと理解されたい。

【符号の説明】

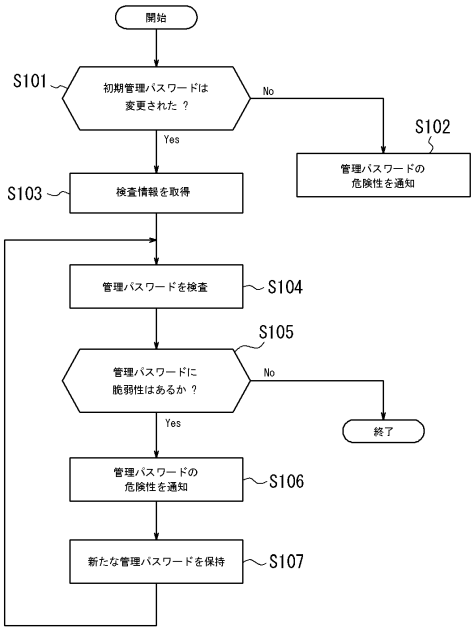
【００７１】

１　アクセス権限情報管理システム
１０　端末機器
１１　管理ＰＷ検査部
１２　管理ＰＷ保持部
１３　入力部
１４　通知部
１５　通信部
１６　制御部
１７　データ保持部
２０　ネットワークシステム
３０　ネットワーク

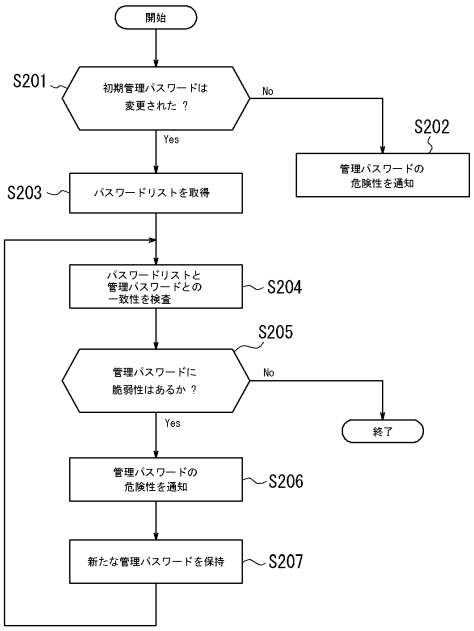
【図１】


1
20
ネットワーク
システム
30
10
端末機器
14
通知部
15
通信部
16
制御部
17
データ保持部
11
管理PW検査部
12
管理PW保持部
13
入力部

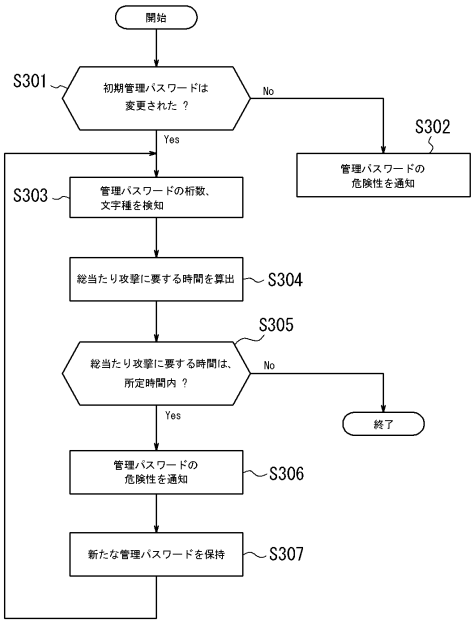
【図２】


開始
S101
初期管理パスワードは
変更された ？
No
S102
管理パスワードの
危険性を通知
Yes
S103
検査情報を取得
管理パスワードを検査
S104
S105
管理パスワードに
脆弱性はあるか ？
No
終了
Yes
管理パスワードの
危険性を通知
S106
新たな管理パスワードを保持
S107

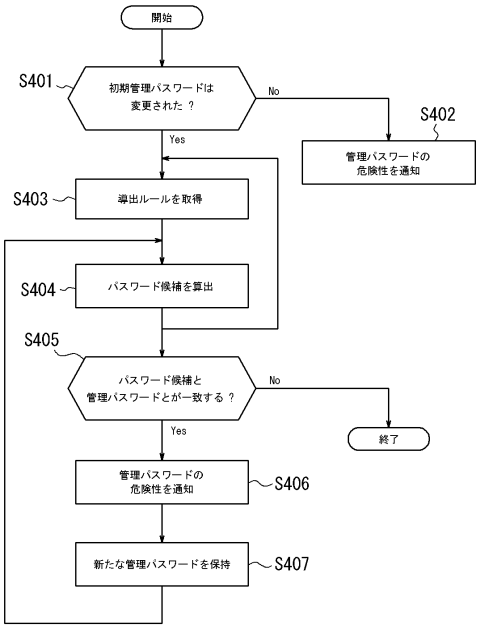
【図３】


開始
S201
初期管理パスワードは
変更された ？
No
S202
管理パスワードの
危険性を通知
Yes
S203
パスワードリストを取得
パスワードリストと
管理パスワードとの
一致性を検査
S204
S205
管理パスワードに
脆弱性はあるか ？
No
終了
Yes
管理パスワードの
危険性を通知
S206
新たな管理パスワードを保持
S207

【図４】


開始
S301
初期管理パスワードは
変更された ？
No
S302
管理パスワードの
危険性を通知
Yes
S303
管理パスワードの桁数、
文字種を検知
総当たり攻撃に要する時間を算出
S304
S305
総当たり攻撃に要する時間は、
所定時間内 ？
No
終了
Yes
管理パスワードの
危険性を通知
S306
新たな管理パスワードを保持
S307

【図５】


開始
S401
初期管理パスワードは
変更された ？
No
S402
管理パスワードの
危険性を通知
Yes
S403
導出ルールを取得
S404
パスワード候補を算出
S405
パスワード候補と
管理パスワードとが一致する ？
No
終了
Yes
管理パスワードの
危険性を通知
S406
新たな管理パスワードを保持
S407

フロントページの続き

(72)発明者　田中　政志
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

審査官　宮司　卓佳

(56)参考文献　特開２０１２－０７３９０４（ＪＰ，Ａ）
特開２０１５－００３４０７（ＪＰ，Ａ）
米国特許出願公開第２０１４／０３７３０８８（ＵＳ，Ａ１）
園田道夫，パワーアップ講座　こちらセキュリティ相談室　第３回　失敗しないパスワード管理，日経ＮＥＴＷＯＲＫ　第８６号，日本，日経ＢＰ社，２００７年　５月２２日，第８６号，p.122-p.127

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４６
Ｇ０６Ｆ　２１／５７