

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号
特開2016-206902
(P2016-206902A)

(43) 公開日 平成28年12月8日(2016.12.8)

(51) Int.Cl.

F I

テーマコード (参考)

G O 6 F 21/46 (2013.01)

G O 6 F 21/57 (2013.01)

G O 6 F 21/46

G O 6 F 21/57 3 7 0

審査請求 未請求 請求項の数 10 O L (全 14 頁)

(21) 出願番号	特願2015-86996 (P2015-86996)	(71) 出願人	000004226
(22) 出願日	平成27年4月21日 (2015. 4. 21)		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
		(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

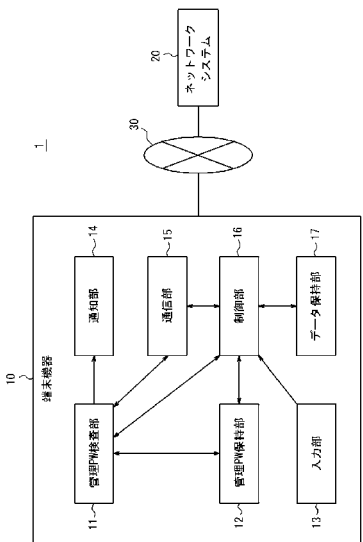
(54) 【発明の名称】 アクセス権限情報管理システム、端末機器及びアクセス権限情報管理方法

(57) 【要約】

【課題】 悪意ある第三者による端末機器への侵入を防止する。

【解決手段】 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30を通じて端末機器10と接続するネットワークシステム20とを備える。端末機器10は、ネットワークシステム20に接続する際に利用するアクセス権限情報を保持する管理PW保持部12と、管理PW保持部12のアクセス権限情報を検査する管理PW検査部11とを備える。管理PW検査部11は、アクセス権限情報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、その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する。

【選択図】 図1



【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、
ことを特徴とするアクセス権限情報管理システム。

10

【請求項 2】

前記検査情報は、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であり、前記検査部は、該パスワードリストに記載された文字列と前記アクセス権限情報とが一致性を有する場合、アクセス権限情報に脆弱性があると判定する、ことを特徴とする請求項 1 に記載のアクセス権限情報管理システム。

【請求項 3】

前記検査情報は、所定のルールであり、前記検査部は、前記端末機器の利用者の情報から、前記所定のルールに基づいて、文字列を作成し、該作成した文字列と前記アクセス権限情報とが一致性を有する場合、アクセス権限情報に脆弱性があると判定する、ことを特徴とする請求項 1 に記載のアクセス権限情報管理システム。

20

【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。

30

【請求項 5】

請求項 2 ~ 4 に記載のアクセス権限情報管理システムのうち、いずれか 2 以上を組み合わせたアクセス権限情報管理システム。

【請求項 6】

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、
ことを特徴とする端末機器。

40

【請求項 7】

前記検査情報は、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であり、前記検査部は、該パスワードリストに記載された文字列と前記アクセス権限情報とが一致性を有する場合、アクセス権限情報に脆弱性があると判定する、ことを特徴とする請求項 6 に記載の端末機器。

50

【請求項 8】

前記検査情報は、所定のルールであり、前記検査部は、前記端末機器の利用者の情報から、前記所定のルールに基づいて、文字列を作成し、該作成した文字列と前記アクセス権限情報とが一致性を有する場合、アクセス権限情報に脆弱性があると判定する、ことを特徴とする請求項 6 に記載の端末機器。

【請求項 9】

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、

10

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 10】

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、

前記ネットワークシステムから前記アクセス権限情報を検査するための検査情報を取得するステップと、

20

前記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】**

30

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。

40

【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

50

、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。

10

【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。

20

【課題を解決するための手段】

【００１０】

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、ことを特徴とする。

30

【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。

【００１２】

40

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、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

50

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、前記ネットワークシステムから前記アクセス権限情報を検査するための検査情報を取得するステップと、前記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。

【 0 0 2 0 】

管理 P W 検査部 1 1 は、管理 P W 保持部 1 2 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 P W 検査部 1 1 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 2 0 から取得し保持する。そして、管理 P W 検査部 1 1 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 P W 保持部 1 2 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 P W 検査部 1 1 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 P W 検査部 1 1 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。

【 0 0 2 1 】

管理 P W 保持部 1 2 は、管理パスワードを保持する。管理 P W 保持部 1 2 は、暗号化された管理パスワードを保持してもよい。

10

【 0 0 2 2 】

入力部 1 3 は、利用者による入力を受け付ける。入力部 1 3 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 1 3 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 1 3 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。

【 0 0 2 3 】

通知部 1 4 は、管理 P W 検査部 1 1 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 1 0 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。

20

【 0 0 2 4 】

通信部 1 5 は、ネットワーク 3 0 を介して、ネットワークシステム 2 0 と通信する。

【 0 0 2 5 】

制御部 1 6 は、端末機器 1 0 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 1 6 は、端末機器 1 0 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 1 6 は、データ保持部 1 7 が保持しているデータ等を、通信部 1 5 を介して、ネットワークシステム 2 0 に送信する。なお、制御部 1 6 は、管理 P W 検査部 1 1 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 1 5 を介する端末機器 1 0 とネットワークシステム 2 0 との接続を遮断してもよい。

30

【 0 0 2 6 】

データ保持部 1 7 は、各種データを保持している。データ保持部 1 7 は、例えば、端末機器 1 0 がセンサである場合、端末機器 1 0 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 1 7 に保持されたデータは、制御部 1 6 によって、通信部 1 5 を介してネットワークシステム 2 0 に送信される。

【 0 0 2 7 】

[システム動作]

40

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。

【 0 0 2 8 】

工場出荷時等において、端末機器 1 0 の管理 P W 保持部 1 2 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 1 0 の購入者（利用者）は、この初期管理パスワードを端末機器 1 0 の入力部 1 3 から入力することで端末機器 1 0 のルート権限を保持し、端末機器 1 0 を、端末機器 1 0 の通信部 1 5 を介してネットワークシステム 2 0 に接続させる。端末機器 1 0 がネットワークシステム 2 0 に接続されると、管理 P W 検査部 1 1 は、端末機器 1 0 の利用が開始されたことを検知する。管理 P W 検査部 1 1 によって端末機器 1 0 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。

50

【 0 0 2 9 】

まず、管理 P W 検査部 1 1 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 S 1 0 1）。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 P W 検査部 1 1 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 S 1 0 1 : N o）、通知部 1 4 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 S 1 0 2）。さらに、ステップ S 1 0 2 の処理において、制御部 1 6 が、端末機器 1 0 とネットワークシステム 2 0 との接続を、直ちに遮断してもよい。またこの際、制御部 1 6 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 1 0 が利用できないようにしてもよい。一方、管理 P W 検査部 1 1 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 S 1 0 1 : Y e s）、ステップ S 1 0 3 の処理に進む。

10

【 0 0 3 0 】

次に、管理 P W 検査部 1 1 は、管理パスワードを検査するための検査情報を、通信部 1 5 を介して、ネットワークシステム 2 0 から取得し（ステップ S 1 0 3）、管理 P W 検査部 1 1 内に保持する。

【 0 0 3 1 】

そして、管理 P W 検査部 1 1 は、管理 P W 保持部 1 2 に保持されている管理パスワードの脆弱性を、ステップ S 1 0 3 の処理で取得した検査情報を用いて検査する（ステップ S 1 0 4）。

20

【 0 0 3 2 】

その後、管理 P W 検査部 1 1 は、ステップ S 1 0 4 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 S 1 0 5）。管理 P W 検査部 1 1 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 S 1 0 5 : N o）、処理を終了して次の検査まで待機する。一方、管理 P W 検査部 1 1 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 S 1 0 5 : Y e s）、ステップ S 1 0 6 の処理に進む。

【 0 0 3 3 】

ステップ S 1 0 6 の処理では、通知部 1 4 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 S 1 0 6 の処理において、制御部 1 6 が、端末機器 1 0 とネットワークシステム 2 0 との接続を、直ちに遮断してもよい。またこの際、制御部 1 6 は、利用者によって、新たな管理パスワードが入力部 1 3 から入力されるまで、端末機器 1 0 が利用できないようにしてもよい。

30

【 0 0 3 4 】

その後、ステップ S 1 0 6 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 1 3 から入力されると、管理 P W 保持部 1 2 に、新たな管理パスワードが保持される（ステップ S 1 0 7）。すると、端末機器 1 0 は、ステップ S 1 0 4 からの処理を繰り返し行う。

40

【 0 0 3 5 】

なお、端末機器 1 0 は、ネットワークシステム 2 0 から検査情報を取得する度ごとに、上記ステップ S 1 0 3 からの処理を実施してもよい。また、端末機器 1 0 は、端末機器 1 0 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 S 1 0 3 からの処理を開始してもよい。また、端末機器 1 0 は、定期的に、上記ステップ S 1 0 3 からの処理を繰り返し行ってもよい。

【 0 0 3 6 】

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 1 0 の内部で、端末機器 1 0 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

50

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]

10

[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 S 201, S 202 の処理は、図 2 に示すステップ S 101, S 102 と同様であるため、説明を省略する。

20

【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 S 203）、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。

30

【0041】

次に、管理PW検査部 11 は、ステップ S 203 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 S 204）。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を検査する。

【0042】

その後、管理PW検査部 11 は、ステップ S 204 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 S 205）。管理PW検査部 11 は、例えば、ステップ S 204 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。

40

【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 S 205：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 S 205：Yes）、ステップ S 206 の処理に進む。

【0044】

ステップ S 206 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 S 206 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

50

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)、処理を終了して次の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 P W 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 P W 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 P W 検査部 11 は、算出したパスワード候補と、管理 P W 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を判定する。

10

【0059】

通知部 14 は、管理 P W 検査部 11 が算出したパスワード候補と、管理 P W 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 S 401, S 402 の処理は、図 2 に示すステップ S 101, S 102 と同様であるため、説明を省略する。

20

【0061】

管理 P W 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 S 403）、管理 P W 検査部 11 内に保持する。さらに、管理 P W 検査部 11 は、ステップ S 403 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 S 404）。そして、管理 P W 検査部 11 は、ステップ S 404 の処理により算出したパスワード候補と、管理 P W 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を判定する（ステップ S 405）。

【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「S A T O U」とであるとすると、パスワード候補は「D S Y P I」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「D S Y P I」）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 P W 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。

30

【0063】

管理 P W 検査部 11 は、ステップ S 404 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 S 405：No）、処理を終了して次の検査まで待機する。一方、管理 P W 検査部 11 は、ステップ S 404 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 S 405：Yes）、ステップ S 406 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。

40

【0064】

ステップ S 406 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 S 406 の処理において、制御部 16 が、通信

50

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 S 407 の処理は、図 1 に示すステップ S 107 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 S 405 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 S 403 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 S 403 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、ステップ S 403 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。

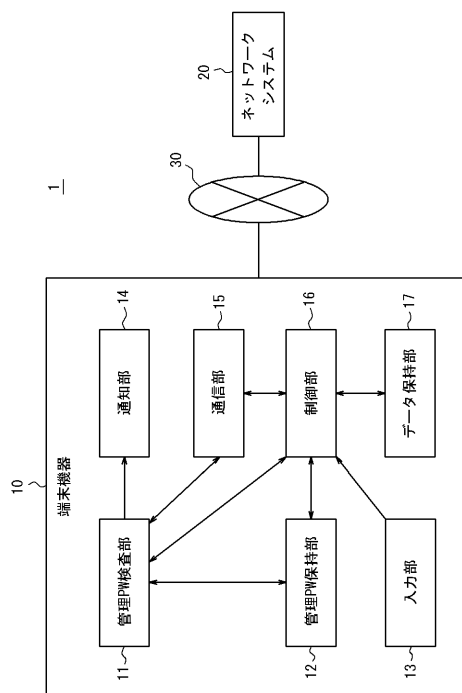
【符号の説明】

【0071】

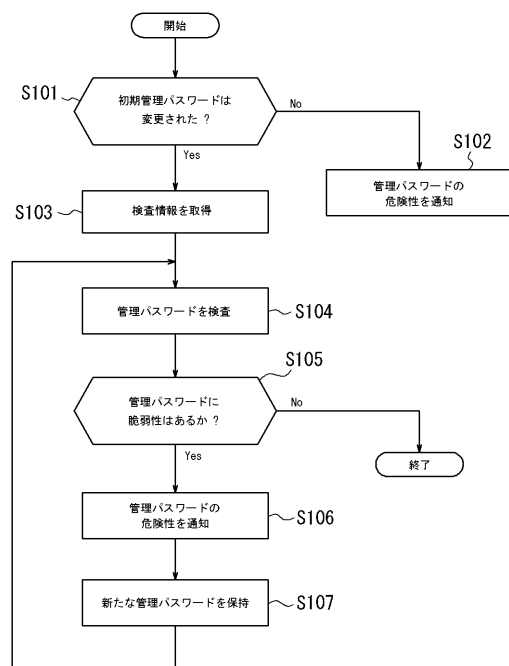
- 1 アクセス権情報管理システム
- 10 端末機器
- 11 管理PW検査部
- 12 管理PW保持部
- 13 入力部
- 14 通知部
- 15 通信部
- 16 制御部
- 17 データ保持部
- 20 ネットワークシステム
- 30 ネットワーク

10

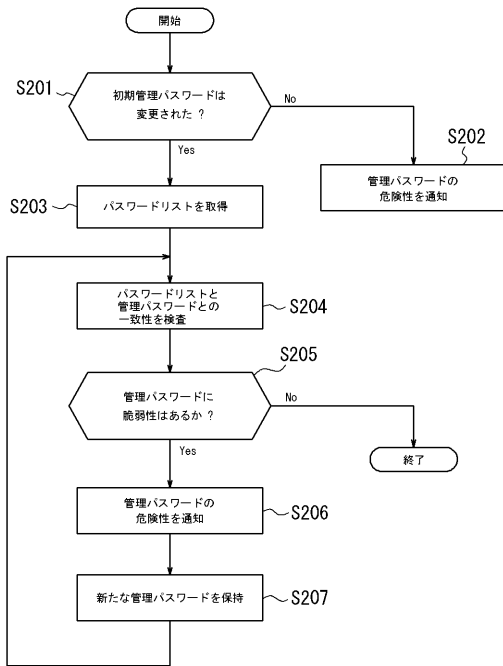
【図1】



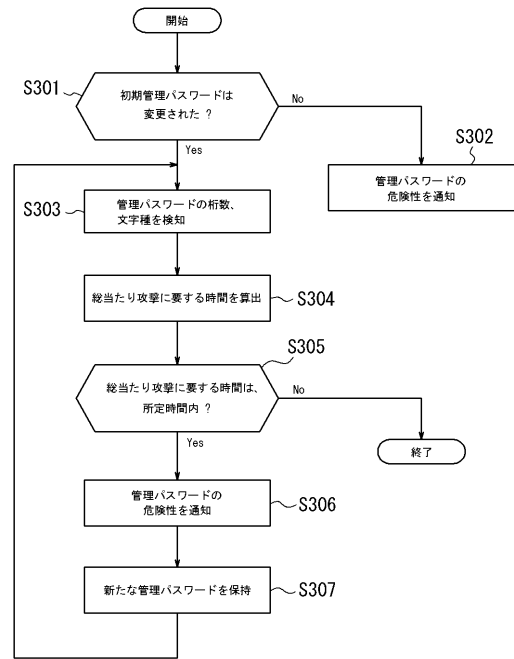
【図2】



【図 3】



【図 4】



【図 5】

