基発０１１８第　１号
平成２２年１月１８日

都道府県労働局長 殿

厚生労働省労働基準局長
(公印省略)

労働基準行政システムのモバイル端末の利用について

労働基準行政システムのモバイル端末（以下「モバイル端末」という。）の利用に関する利用手順書については、平成21年11月19日付け基発1119第10号「都道府県労働局及び労働基準監督署に設置する労働基準行政情報システム・労災行政情報管理システムの端末装置等の運用管理について」において、別途定めるとしていたところであるが、今般別添のとおり「労働基準行政システム「モバイル端末」利用手順書」を定め、下記のとおりモバイル端末を配備するので、当該手順書に基づいた適正な運用に遺漏なきを期されたい。

記

都道府県労働局（労働基準部監督課配備）各１台

※　配備日程等については、平成22年１月下旬から同年２月上旬を予定しているが、詳細については別途、労災補償部労災保険業務室から通知する。

労働基準行政システム「モバイル端末」利用手順書

平成 22 年 1 月

厚生労働省労働基準局

目次

第１　手順書の目的及び対象者 1
１　目的 1
２　対象者 1
第２　管理 1
１　モバイル端末の管理者等 1
２　管理 1
第３　利用範囲等 2
１　利用範囲 2
２　利用対象者 2
３　利用可能な端末 2
４　モバイル端末の装備品 2
５　利用機能 2
６　アクセスポイント 3
第４　モバイル端末の操作手順 3
１　管理者及び利用者による接続設定の操作等（貸出時） 3
２　利用者によるモバイル端末利用時の操作等（利用時） 3
３　利用者によるモバイル端末返却時の処理（返却時） 4
４　管理者によるモバイル端末返却時の処理（返却時） 4
第５　モバイル端末等の管理 4
１　貸出及び借用時等の管理 4
２　返却時及び返却後の管理 4
第６　利用申請手続 5
第７　利用終了後の手続 5
第８　モバイル端末利用時において遵守すべき事項 5
１　盗難・紛失及び情報漏えい等の防止 5
２　禁止事項 6
第９　緊急時の対応 6
１　モバイル端末等が損壊、紛失又は盗難にあった場合 6
２　ウイルスに感染した場合 6
３　機器の障害等の可能性がある場合 6

第１　手順書の目的及び対象者

１　目的

モバイル端末の開発については、平成 18 年 3 月 29 日に策定した「監督・安全衛生等業務の業務・システム最適化計画」において、「現場での情報検索、指導文書等の印刷、監督・指導結果の登録等が行えるようモバイル端末の導入を可能とする環境を整備し、基準システムの効果的な活用及び業務効率化を実現するための開発を実施する。」とし、その開発を行ったところである。

労働基準行政情報システム・労災行政情報管理システム（以下「労働基準行政システム」という。）の運用管理に関する具体的事項については、労働基準行政情報システム・労災行政情報管理システム運用管理要領（以下「要領」という。）、実際の業務については、各種機械処理手引等（以下「各種手引」という。）に定めているところであり、労働基準行政システム「モバイル端末」利用手順書（以下「手順書」という。）は、要領及び各種手引のほか、実際に労働基準行政システムのモバイル端末（以下「モバイル端末」という。）を利用する際の具体的利用手順を定め、もって、モバイル端末の適正な利用に資することを目的とする。

なお、手順書に定めるもののほか、モバイル端末の運用管理に関し必要な事項は要領等に基づくものとする。

２　対象者

手順書は、労働基準行政システムのＩＤが付与され、モバイル端末を利用できる都道府県労働局、各労働基準監督署及び厚生労働省労働基準局（以下「本省」という。）の職員を対象とする。

第２　管理

１　モバイル端末の管理者等

モバイル端末の管理者（以下「管理者」という。）は、都道府県労働局においては、労働基準行政情報システム・労災行政情報管理システム管理規程（以下「規程」という。）で定める局副管理者である労働基準部監督課長とし、また、本省においては、規程で定めるシステム運用管理者である労働基準局労災補償部労災保険業務室長とする。

なお、局副管理者は局副管理担当者に、システム運用管理者は運用管理担当者に、事務を補助させることができるものとする。

２　管理

モバイル端末は、要領に定める端末装置等に含まれるものであるため、管理に当たって手順書に定めのない事項は、要領に基づき管理するものとする。

第３　利用範囲等

１　利用範囲

モバイル端末を利用する際には、手順書で定める方法を遵守するものとする。

なお、手順書に定めのない事項は、要領を遵守し利用するものとする。

２　利用対象者

出張等の理由により、第６に規定するモバイル端末の借用・持出許可申請をした職員のうち、管理者がその必要性を認め、許可した職員に限るものとする。

なお、モバイル端末の利用対象者は、モバイル端末の借用・許可申請時より過去１年以内に労働基準行政システムのセキュリティ教育を受講した職員に限るものとする。

３　利用可能な端末

労働基準行政システムにおいて出張等で利用できる端末は、庁舎外で利用することを前提として配備したモバイル端末に限るものとする。

４　モバイル端末の装備品

モバイル端末の装備品は以下のものとする（以下「モバイル端末等」という。）。

（１）モバイル端末本体
（２）モバイル端末本体用ＡＣアダプタ、付属電源コネクタ
（３）ＰＨＳ通信カード
（４）労働基準行政システム用トークン（基準用(先)と書かれたシールが貼ってあるもの）
（５）統合ネットワーク用トークン（統合用(後)と書かれたシールが貼ってあるもの）
（６）光学マウス
（７）モバイルプリンタ本体
（８）モバイルプリンタ用ＡＣアダプタ
（９）モバイルプリンタ用接続ＵＳＢケーブル
(10) モバイルプリンタ用バッテリ
(11) ワイヤーロックケーブル、ワイヤーロックキー
(12) マニュアル類
①コンピュータの準備
②PIXUS iP90v 基本操作ガイド
③ピクサス純正用紙ガイド
④簡単スタートガイド
⑤ELECOM MOBI-LOCK 〈ご使用方法〉
⑥Kensington MicroSaver Computer Security Cable
(13) キャリングバッグ

５　利用機能

モバイル端末は労働基準行政システムの ThinClient と同等の機能を利用することが可能である(職員ポータルにおける業務メニューの労災タブ配下にあるサブシステム、申請・届出等処理支援

システム処理システム及び一部検索機能を除く。)。

また、TCS (ThinClient Server) 未接続状態であってもモバイル端末本体にインストールされているオフィス機能等は利用可能であるが、このオフィス機能等を利用しファイルを作成してもファイル保存ができるのはモバイル端末本体のみであり、外部記録媒体及び労働基準行政システムの個人用フォルダ等への移動は原則できないことから、セキュリティ確保等の観点からもモバイル端末本体にインストールされているオフィス機能等を利用したファイルの作成・保存は原則として行わないものとする。

6　アクセスポイント

モバイル端末からダイヤルアップで接続できるアクセスポイントは、統合ネットワークから提供されているアクセスポイントのみなので、ダイヤルアップ先の変更は行わないこと。

第４　モバイル端末の操作手順

モバイル端末の設定等操作手順は以下のとおりである。

なお、具体的なモバイル端末の操作方法については、別添「モバイル端末操作マニュアル」を参照すること。

1　管理者及び利用者による接続設定の操作等（貸出時）

（1）管理者による設定

管理者はLAN接続状態で以下の操作及び確認を行う。

ア　LAN接続状態で、モバイル端末の電源を投入後、BIOS (Basic Input/Output System) 及びPointsecのID及びパスワードを入力する。

イ　RSA SecurIDに管理者用のユーザ名及びPASSCODEを入力する。

ウ　タスクトレイのNOSiDEからAgentManagerを起動し、ウイルス対策ソフトのパターン定義ファイルをアップデートする。

エ　RSA Authentication Manager Remote Modeを起動し、利用者用IDに関連付けされたトークンが、次回接続時にPIN (Personal Identification Number) 設定を求める状態であること及びEnable状態であることを確認する。

（2）利用者による設定

利用者は上記（1）の設定終了後、引き続きLAN接続状態で以下の操作を行う。

ア　管理者から通知を受けたBIOS及びPointsecのID及びパスワードを入力する。

イ　労働基準行政システム用のトークンの生成数列を入力すると、PINの入力画面が出るので、6～8桁の任意の英数字を入力し、PINを設定する（設定後は、当該PINと労働基準行政システム用トークン生成数列の連続文字列がPASSCODEとなる。)。

2　利用者によるモバイル端末利用時の操作等（利用時）

（1）BIOS及びPointsecのID及びパスワードを入力する。

（2）RSA SecurIDに管理者から通知を受けたユーザ名及び上記1の（2）で設定したPINと労働

基準行政システム用トークンによる生成数列の連続文字列を入力する。

（3）ダイヤルアップ接続を起動し、管理者から通知を受けたユーザ名とパスワードに、管理者から通知を受けたPINと統合ネットワーク用トークンの生成数列を連続で入力する。

（4）ダイヤルアップ接続成功後、タスクトレイのNOSiDEからAgentManagerを起動し、構成情報の送信及びウイルス対策ソフトのパターン定義ファイルのアップデートを行う。

（5）スタートメニューからCitrixを起動し、労働基準行政システム用のIDとパスワードを入力し、タスクトレイのCitrixからTCS接続を選択する。

以上でモバイル端末によるThinClient機能の利用が可能となる。

なお、ThinClient機能の利用後はPHS接続を切断するか、ログオフを行うこと。

3　利用者によるモバイル端末返却時の処理（返却時）

モバイル端末の返却を行う場合には、モバイル端末を利用した職員はモバイル端末本体に作成したファイルを原則すべて削除してから返却を行うこと。

4　管理者によるモバイル端末返却時の処理（返却時）

（1）モバイル端末本体に保存されているモバイル端末利用者情報を削除するため、プロファイル削除を行うこと。

（2）RSA Authentication Manager Remote Modeを起動し、PINのクリア及びEnable状態であることの確認を行うこと。

第5　モバイル端末等の管理

1　貸出及び借用時等の管理

（1）管理者及びモバイル端末利用者は、借用・持出許可申請に関して第6の利用手続等を参照し利用手続を適正に行うこと。

（2）管理者及びモバイル端末利用者は、モバイル端末の貸出及び借用時に、別紙1「労働基準行政システムモバイル端末装備品一覧（チェックリスト）」（以下「チェックリスト」という。）を活用し、貸出物が一致しているかを確認すること。

（3）管理者は、申請の状況について申請の許可・不許可にかかわらず別紙2「労働基準行政システムモバイル端末管理簿」（以下「管理簿」という。）に記録すること。

2　返却時及び返却後の管理

（1）モバイル端末本体のオフィス機能等を利用した場合は、モバイル端末本体に作成したファイルを削除の上、返却すること。

（2）モバイル端末利用者及び管理者はモバイル端末の返却時に、チェックリストを活用し、返却物が貸出時のものと一致しているかを確認すること。

（3）管理者は、モバイル端末利用者から返却があった場合には、内容物及びモバイル端末の設定内容を確認し、管理簿を更新すること。

（4）返却後のモバイル端末については、施錠可能な保管場所に保管し、定期的にチェックリスト

を活用し、装備品の状況について確認を行うこと。

第６　利用申請手続

１　モバイル端末の利用を希望する職員は、原則貸出希望日の７日前までに別紙３「モバイル端末借用・持出許可申請書兼返却確認書」（以下「申請書兼確認書」という。）を作成し、都道府県労働局（労働基準監督署を含む。）職員にあっては労働基準部監督課長あて、本省職員にあっては労働基準局労災補償部労災保険業務室長あて、各所属長の申請許可押印を受けた上で申請すること。

なお、申請に当たっては所属する課室長等による申請許可押印を受けた上で申請すること。

２　利用申請に当たっては、１回の申請によるモバイル端末の借用希望期間を、原則として最長３０日以内とし、借用希望期間延長の必要が生じた場合には、期間終了までに再申請を行うこと。

３　申請書兼確認書による借用・持出申請があった場合、管理者は申請理由等を確認した上で申請書兼確認書の「借用・持出許可時印」欄に押印すること。また、申請の許可・不許可にかかわらず、管理簿に所定事項を記録し、受領した申請書兼確認書の写しを作成し、これを保管しておくこと。

４　管理者は上記３で押印した申請書兼確認書原本をモバイル端末等とともに利用者に交付すること。

第７　利用終了後の手続

１　モバイル端末利用後は、モバイル端末等とともに申請書兼確認書に返却日を記入し、「返却時印」欄への所属する課室長等による押印を受け、管理者にモバイル端末等とともに提出すること。

２　管理者は再度受領した申請書兼確認書の「返却確認時印」欄に押印し、これを管理簿とともに編てつ・保管すること。

第８　モバイル端末利用時において遵守すべき事項

１　盗難・紛失及び情報漏えい等の防止

モバイル端末を利用する職員は、以下の事項を遵守すること。

（１）モバイル端末を保管する場合は、必ず施錠可能な場所に保管すること。

なお、出張中等、施錠可能な場所に保管できない場合は、常に携帯するか、目の届くところに置き、駐車中の車中には、置かないこと。

（２）公共交通機関等での移動時における盗難防止、置き忘れ防止のため、網棚等に乗せないなど、置き場所に留意すること。

（３）各トークンとモバイル端末本体は分けて保管すること。

（4）庁舎外での利用に当たってモバイル端末を放置したままの離席機会を極力少なくすること。
（5）モバイル端末操作中にやむを得ず離席する際には、モバイル端末の操作をロックすること。
（6）IDやパスワードを入力する際には、周囲に配慮すること。

2　禁止事項
（1）行政事務の遂行以外の目的での情報作成、Webサイトへのアクセス等
（2）個人で別途契約しているプロバイダ、メールアドレス等の使用
（3）ソフトウェア（Winny等含む。）のインストール
（4）Webアクセス時等におけるセキュリティ設定の変更（＊）
（＊）セキュリティレベルの低下を防ぐ観点から、設定の変更を禁止する。
（5）システム及びソフトウェアの設定変更

第9　緊急時の対応
1　モバイル端末等が損壊、紛失又は盗難にあった場合
モバイル端末等の損壊、紛失又は盗難が判明した場合には要領に基づいた連絡等を行うこと。

2　ウイルスに感染した場合
モバイル端末等がウイルスに感染したことが判明した場合、直ちに接続しているネットワークを切断した上で、管理者に連絡・相談すること。

3　機器の障害等の可能性がある場合
モバイル端末を使用する上で「ホームページが閲覧できない」、「ローカルネットワークに接続できない」といった場合には、以下の項目を確認した上で対処すること。
なお、障害等の原因が不明な場合には、ヘルプデスクに問い合わせること。
（1）モバイル端末ログイン時に接続失敗する場合は、労働基準行政システム用トークンがロックされている可能性があるため、管理者による接続の再設定
（2）ＰＨＳ通信カードの正しい認識
・ＰＨＳ通信カードは正しく挿入されているか。
（3）ダイヤルアップの正しい設定
・アクセスポイントの電話番号は正しく設定されているか。
（ダイヤルアップ時に接続失敗する場合は、統合ネットワーク用トークンがロックしている可能性があるので、ヘルプデスクへ連絡すること）
（4）ユーザIDとパスワードの正しい入力

労働基準行政システムモバイル端末装備品一覧（チェックリスト）

貸出時			返却時		
管理者による貸出		モバイル端末本体	申請者による返却		モバイル端末本体
		モバイル端末本体用ＡＣアダプタ、付属電源コネクタ			モバイル端末本体用ＡＣアダプタ、付属電源コネクタ
		ＰＨＳ通信カード			ＰＨＳ通信カード
		労働基準行政システム用トークン			労働基準行政システム用トークン
		統合ネットワーク用トークン			統合ネットワーク用トークン
		光学マウス			光学マウス
		モバイルプリンタ本体			モバイルプリンタ本体
		モバイルプリンタ用ＡＣアダプタ			モバイルプリンタ用ＡＣアダプタ
		モバイルプリンタ用接続ＵＳＢケーブル			モバイルプリンタ用接続ＵＳＢケーブル
		モバイルプリンタ用バッテリ			モバイルプリンタ用バッテリ
		ワイヤーロックケーブル、ワイヤーロックキー			ワイヤーロックケーブル、ワイヤーロックキー
		マニュアル類			マニュアル類
		キャリングバッグ			キャリングバッグ
申請者による受領		モバイル端末本体	管理者による受領		モバイル端末本体
		モバイル端末本体用ＡＣアダプタ、付属電源コネクタ			モバイル端末本体用ＡＣアダプタ、付属電源コネクタ
		ＰＨＳ通信カード			ＰＨＳ通信カード
		労働基準行政システム用トークン			労働基準行政システム用トークン
		統合ネットワーク用トークン			統合ネットワーク用トークン
		光学マウス			光学マウス
		モバイルプリンタ本体			モバイルプリンタ本体
		モバイルプリンタ用ＡＣアダプタ			モバイルプリンタ用ＡＣアダプタ
		モバイルプリンタ用接続ＵＳＢケーブル			モバイルプリンタ用接続ＵＳＢケーブル
		モバイルプリンタ用バッテリ			モバイルプリンタ用バッテリ
		ワイヤーロックケーブル、ワイヤーロックキー			ワイヤーロックケーブル、ワイヤーロックキー
		マニュアル類			マニュアル類
		キャリングバッグ			キャリングバッグ

別紙２

労働局労働基準部監督課

労働基準行政システムモバイル端末管理簿

モバイル端末番号 MC２

No.	申請年月日	所属 氏名	申請理由	借用 希望期間	許可 区分	貸与年月日	貸与 許可期間	返却年月日
	年　月　日			年　月　日 ～　年　月　日	可　否	年　月　日	年　月　日 ～　年　月　日	年　月　日
	年　月　日			年　月　日 ～　年　月　日	可　否	年　月　日	年　月　日 ～　年　月　日	年　月　日
	年　月　日			年　月　日 ～　年　月　日	可　否	年　月　日	年　月　日 ～　年　月　日	年　月　日
	年　月　日			年　月　日 ～　年　月　日	可　否	年　月　日	年　月　日 ～　年　月　日	年　月　日
	年　月　日			年　月　日 ～　年　月　日	可　否	年　月　日	年　月　日 ～　年　月　日	年　月　日
	年　月　日			年　月　日 ～　年　月　日	可　否	年　月　日	年　月　日 ～　年　月　日	年　月　日
	年　月　日			年　月　日 ～　年　月　日	可　否	年　月　日	年　月　日 ～　年　月　日	年　月　日
	年　月　日			年　月　日 ～　年　月　日	可　否	年　月　日	年　月　日 ～　年　月　日	年　月　日
	年　月　日			年　月　日 ～　年　月　日	可　否	年　月　日	年　月　日 ～　年　月　日	年　月　日
	年　月　日			年　月　日 ～　年　月　日	可　否	年　月　日	年　月　日 ～　年　月　日	年　月　日

【別紙３　都道府県労働局用】

平成　　年　　月　　日

労働局
労働基準部監督課長　殿

労働基準監督署長
労働局労働基準部　　課・室長

管理者（監督課長）	
返却確認時印	借用・持出許可時印

申請者所属課室署長	
返却時印	借用・持出申請時印

モバイル端末借用・持出許可申請書 兼 返却確認書

1　借用・持出申請時

以下のとおりモバイル端末を借用・持出したいので、許可願います。

所属		署　　労働局　　労働基準部　　室・課
氏名		
申請理由		
借用希望期間		年　　月　　日　～　　年　　月　　日
持出先		
管理者記入欄	許可・不許可年月日	許可・不許可　　年　　月　　日
	貸与年月日	年　　月　　日
	貸与許可期間	年　　月　　日　～　　年　　月　　日
	モバイル端末番号 ※「MC２～」の端末番号を記入	MC２

2　返却確認時

以下のとおりモバイル端末を返却いたしましたので、確認願います。

返却時確認事項	モバイル端末本体に作成したファイルの有無	有	無
返却年月日	年　　月　　日		
受領者	労働局労働基準部監督課　氏名		

※不用文字は削除して使用すること。

【別紙３　本省用】

平成　　年　　月　　日

労働基準局労災補償部
労災保険業務室長　殿

労働基準局
課・室長

労災保険業務室長	
返却確認時印	借用・持出許可時印

申請者所属課室長	
返却時印	借用・持出申請時印

モバイル端末借用・持出許可申請書 兼 返却確認書

1　借用・持出申請時

以下のとおりモバイル端末を借用・持出したいので、許可願います。

所属		課・室
氏名		
申請理由		
借用希望期間		年　月　日　～　年　月　日
持出先		
管理者記入欄	許可・不許可年月日	許可・不許可　年　月　日
	貸与年月日	年　月　日
	貸与許可期間	年　月　日　～　年　月　日
	モバイル端末番号 ※「MC２～」の端末番号を記入	MC２

2　返却確認時

以下のとおりモバイル端末を返却いたしましたので、確認願います。

返却時確認事項	モバイル端末本体に作成したファイルの有無	有	無
返却年月日	年　月　日		
受領者	労災補償部労災保険業務室　氏名		

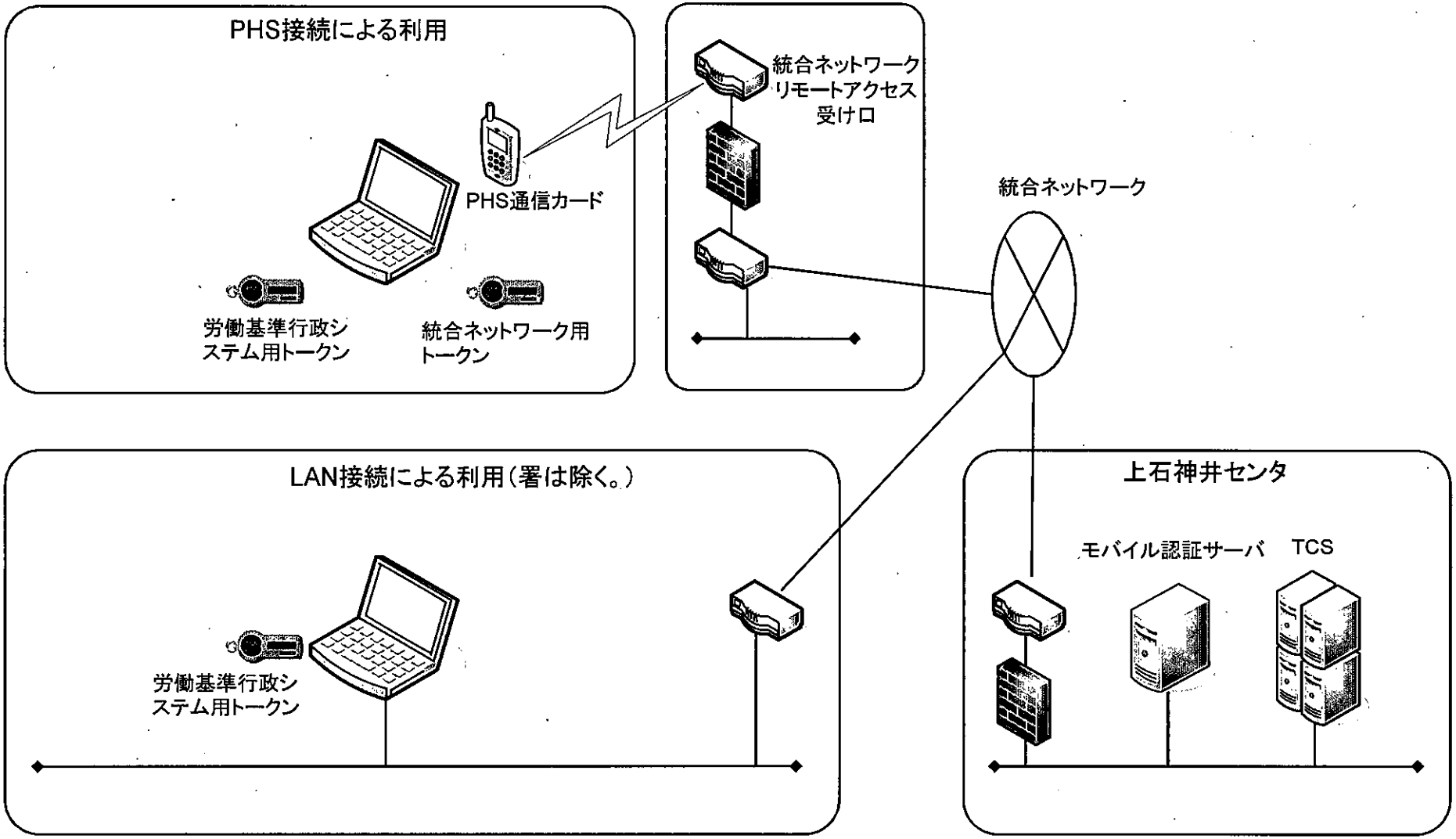
※不用文字は削除して使用すること。

（別添）

モバイル端末操作マニュアル

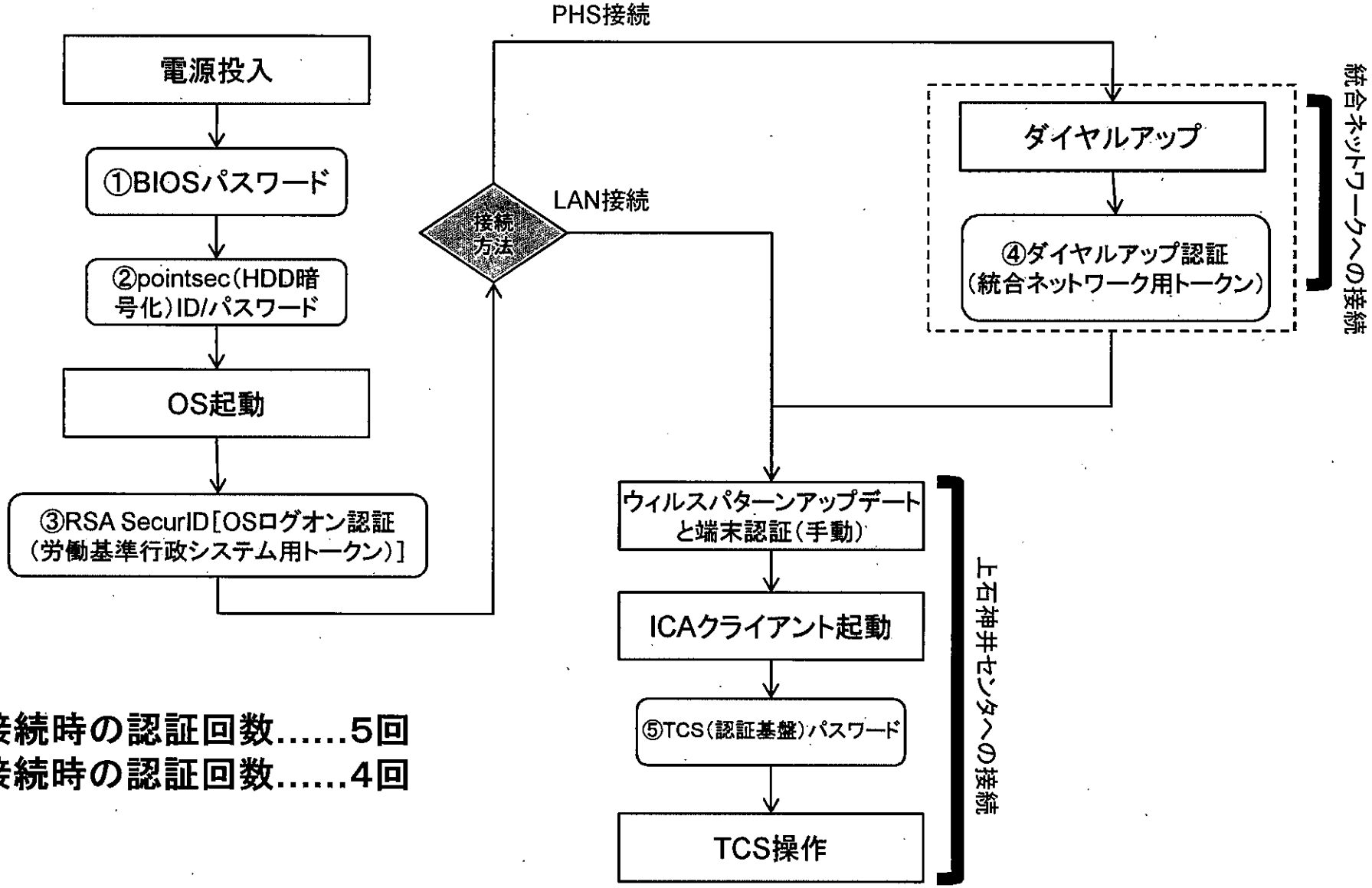
第1　モバイル端末の接続概要

モバイル端末の接続概要は以下のとおり。



第2　認証の流れ

モバイル端末を利用するために必要な認証の流れは以下のとおり。



①PHS接続時の認証回数……5回
②LAN接続時の認証回数……4回

第3　認証に必要な構成品

モバイル端末で認証を行うためには以下の構成品が必要となる。

項番	構成品		説明
1		モバイル端末本体	市販のノートPCをベースにOfficeアプリケーションを搭載し、HDD暗号化ソフトウェアを搭載した端末。統合ネットワークを経由することでTCSに接続し、労働基準行政システムを用いた業務を行うことが可能。
2		PHS通信カード	モバイル端末に接続し、統合ネットワークのダイヤルアップ接続を利用してTCSと通信を行う。
3		労働基準行政システム用トークン	モバイル端末のOSにログオンする際の認証に用いるワンタイムパスワードを生成する装置。 1分ごとにランダムな6ケタの数値が生成される。
4		統合ネットワーク用トークン	PHS通信カードを使用し、統合ネットワークにダイヤルアップ接続する際の認証に用いるワンタイムパスワードを生成する装置。 1分ごとにランダムな6ケタの数値が生成される。

第4　利用者及び管理者等の主な役割

利用者及び管理者等の主な役割は以下のとおり。

項番	関係者	役割
1	管理者 管理者	モバイル端末等の管理を行う。 管理者用IDとパスワードは本省より通知されるものを利用する。 返却時には不要なファイルや利用者情報を削除する。
2	利用者 利用者	モバイル端末の利用者。利用する際には管理者に利用申請を行い、管理者から通知されるID等を用いて認証を行う。 返却時には不要なファイルを原則全て削除する。
3	運用業者（ヘルプデスク）	システムに関する故障等の問い合わせ等の受付を行い、解決のための対応を行う。

各種ID/パスワードの通知範囲

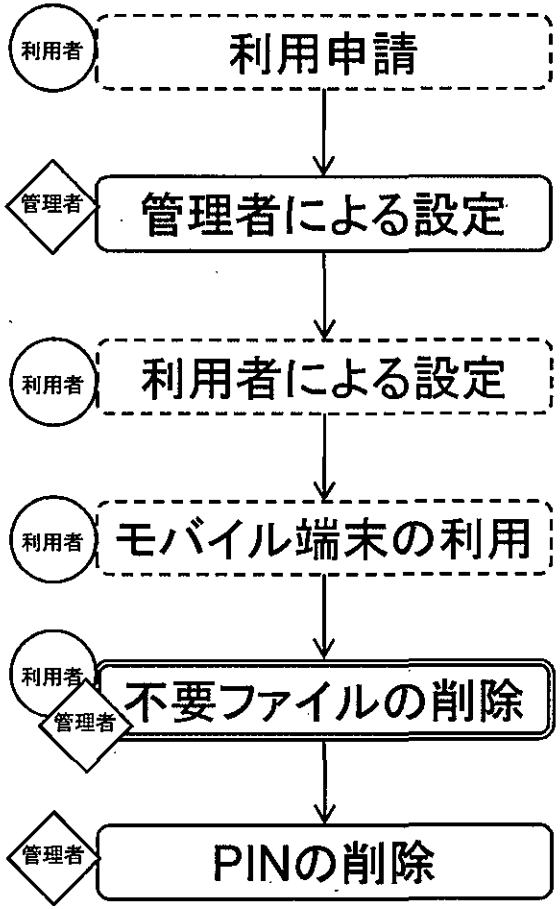
			管理者 ※1	利用者 ※2
BIOSパスワード			○	○
pointsec（HDD暗号化）ID/パスワード			○	○
RSA Secur（OSログオン） ID/パスワード	管理者用 （モバイル認証サーバアクセス時にも使用）		○	×
	利用者用	労働基準行政システム用トークン併用	△IDのみ通知	△IDのみ通知 （PINは利用者が設定）
ダイヤルアップID/パスワード		統合ネットワーク用トークン併用	○	○

※1　管理者列の「○」は、本省から通知される。

※2　利用者列の「○」は、管理者から通知される。

第5　モバイル端末の操作手順の流れ

モバイル端末の操作手順の流れは以下のとおり。



管理者に対してモバイル端末の利用を申請する。

モバイル認証サーバに対して、利用者と利用可能なモバイル端末の関連付けを行う。
登録されている利用者と利用可能な労働基準行政システム用トークン及びモバイル端末の関連付けを行う。
この時点でワンタイムパスワードを用いた認証が可能となる。

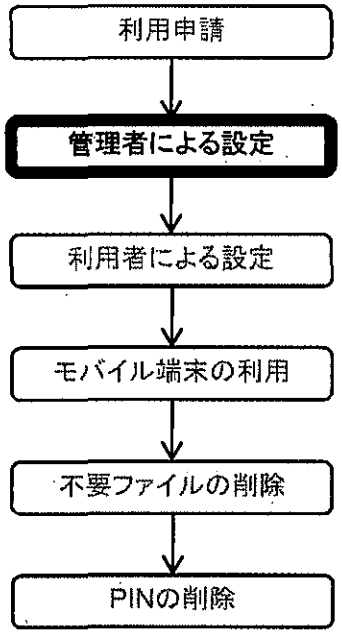
PASSCODEの一部となるPINを利用者が初期ログオン時に設定する。

モバイル端末を利用して労働基準行政システムを用いた業務を行う。

利用後不要となったファイルをモバイル端末から削除する。

次のユーザが使用できるように労働基準行政システム用トークンのPINの削除をする。

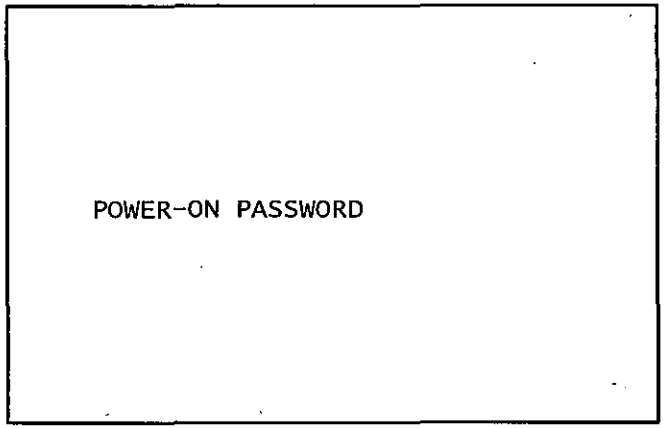
第6　管理者による設定

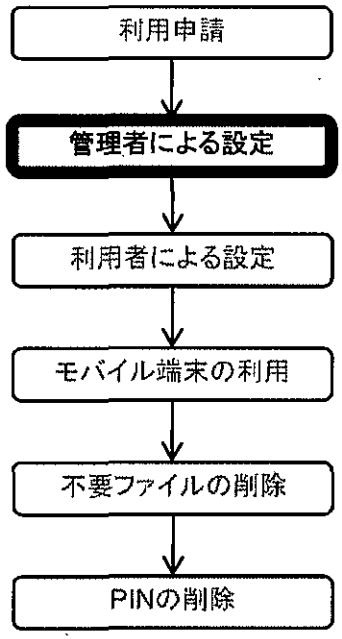


本手順は、管理者の所属課室におけるLANにて、モバイル認証サーバにアクセスできる状態で行う。

管理者　1. モバイル端末をLANに接続し、電源を投入する。

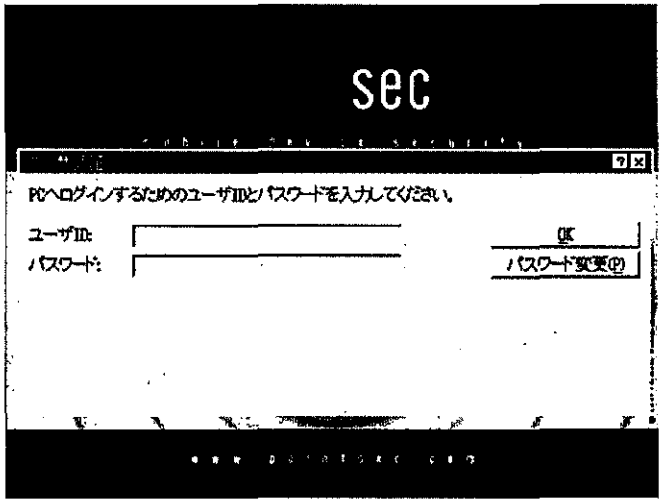
管理者　2. BIOSパスワードが求められるので、通知されたパスワードを入力する。
※入力したパスワードは無表示となる。





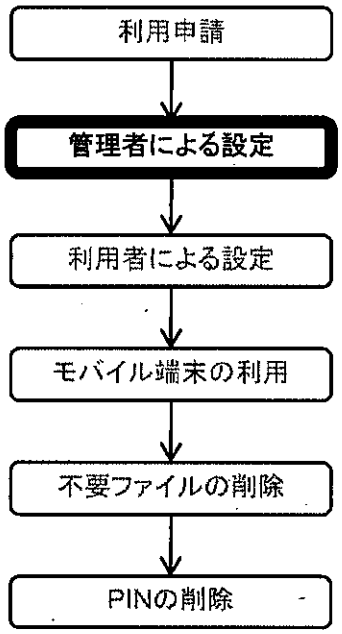
管理者

3. HDD暗号ソフトウェアの認証が求められるので、通知されたpointsecユーザID及びパスワードを入力し、「OK」ボタンをクリックする。続けてダイアログボックスが表示されるので、「続行」ボタンをクリックする。



管理者

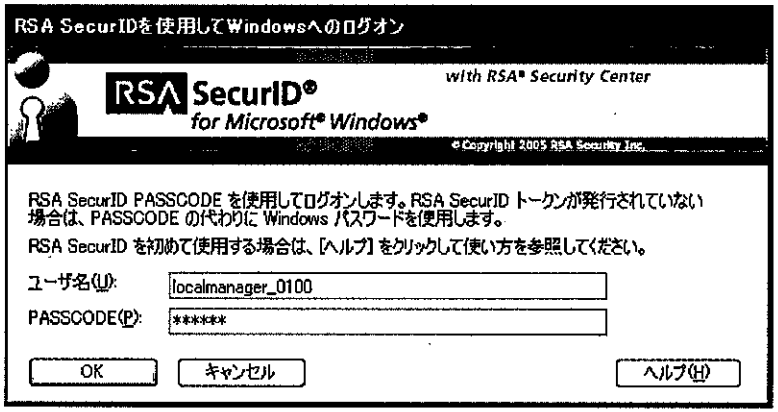
4. 正常に認証が行われるとOSが起動する。

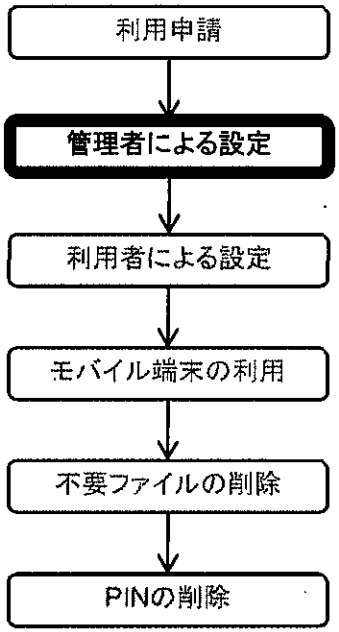


管理者

5. 通知されたRSA SecurID及びパスワード(管理者用)を入力し、「OK」ボタンをクリックする。
（管理者の認証ではワンタイムパスワード入力は不要。）

今回は例として管理者IDに「localmanager_0100」を使用する。

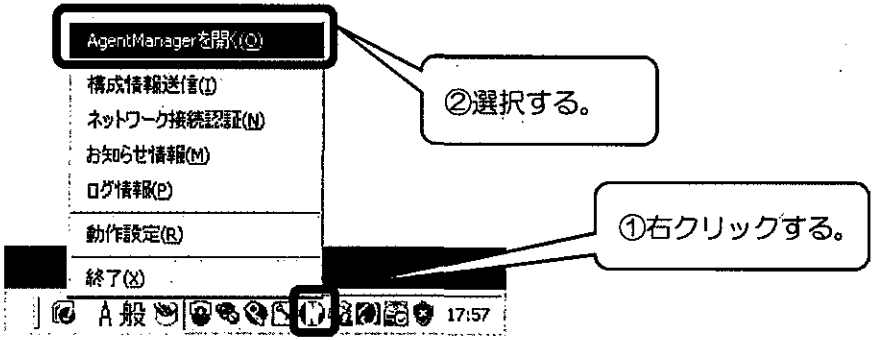




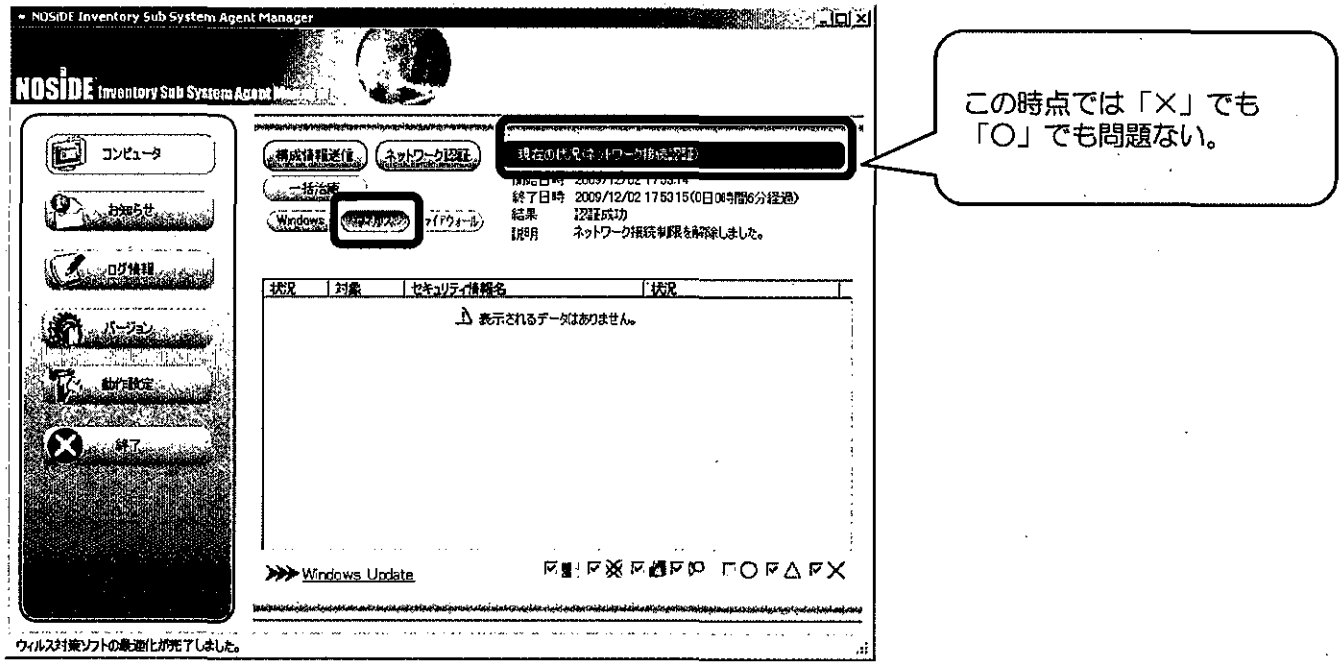
管理者

6. 画面右下タスクトレイのNOSiDEのアイコンを右クリックし、表示されたコンテキストメニューから「AgentManagerを開く(O)」を選択する。

※第6の6から8までの一連の操作を行っていない場合は労働基準行政システム側の接続が拒否される場合があるため、必ずこの一連の操作は行うこと。

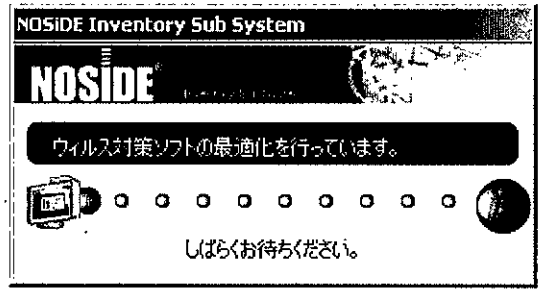


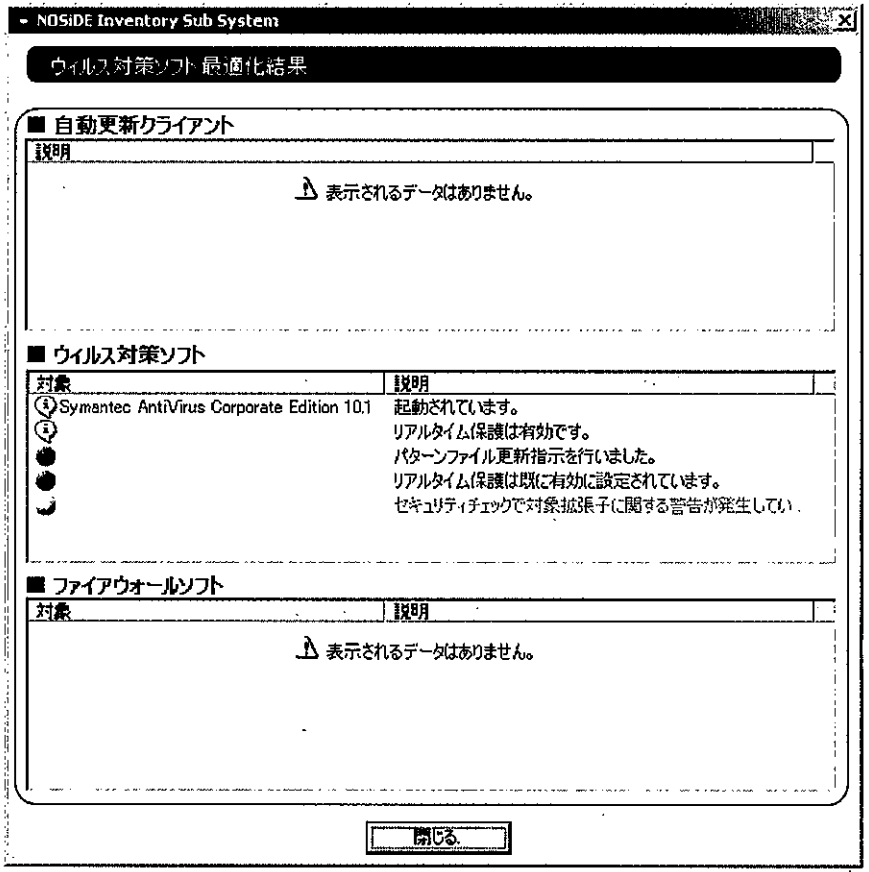
・表示されたNOSiDEメイン画面の、「ウィルス」ボタンをクリックする。



管理者

7. 結果画面が表示されるので「閉じる」ボタンをクリックする。





利用申請

管理者による設定

利用者による設定

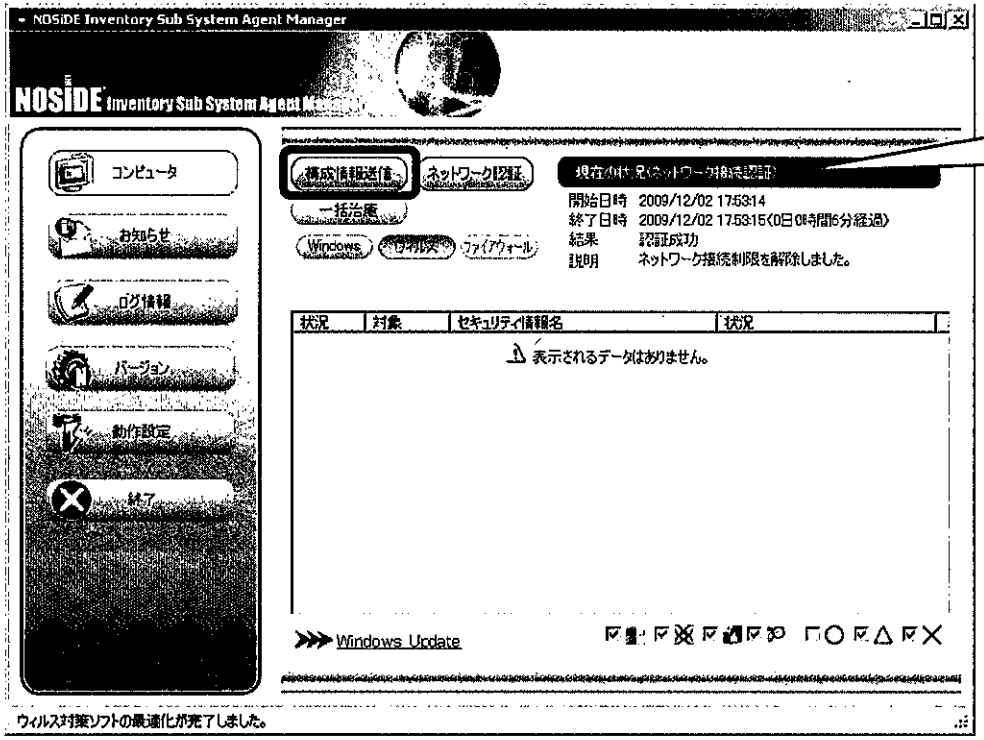
モバイル端末の利用

不要ファイルの削除

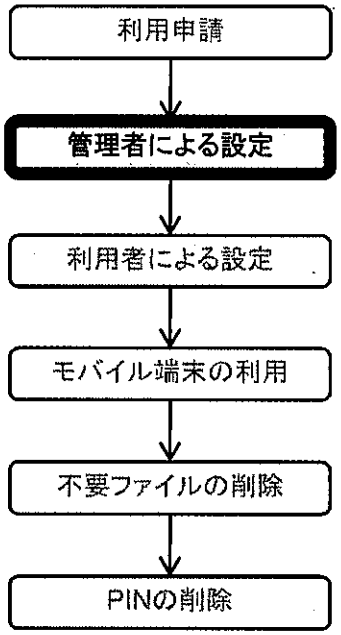
PINの削除

管理者

8. 表示されているNOSiDEのメイン画面の「構成情報送信」ボタンをクリックする。



「○」となっていることを確認する

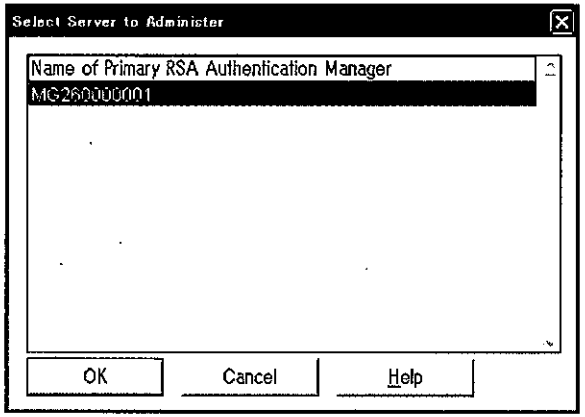


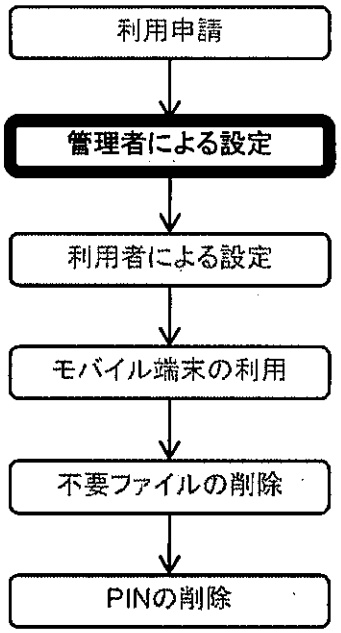
管理者

9. デスクトップ画面左下のスタートメニューから「マイコンピュータ」をクリックし、続けて「ローカルディスク(C:)」をダブルクリック、「soft_shortcut」をダブルクリック、「RSA Security」をダブルクリック、と進むと表示される「RSA Authentication Manager Remote Mode」をダブルクリックし起動する。

管理者

10. 「MG260000001」を選択し、「OK」ボタンをクリックする。

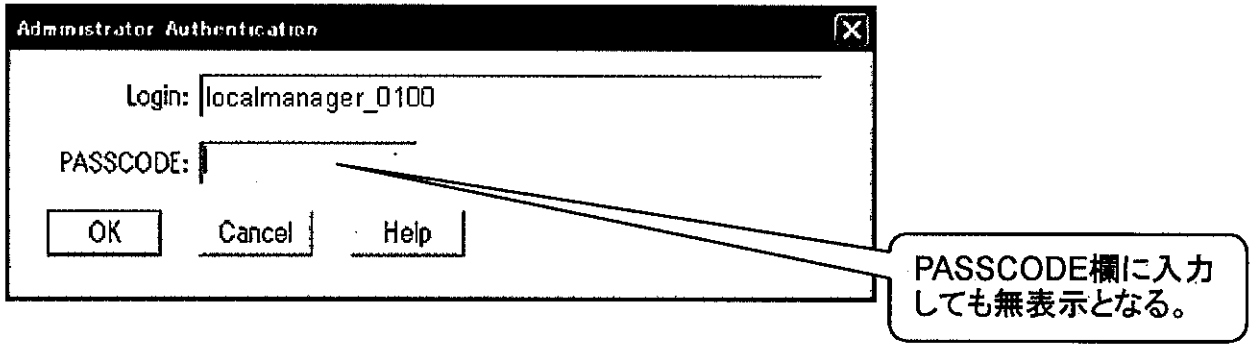




管理者

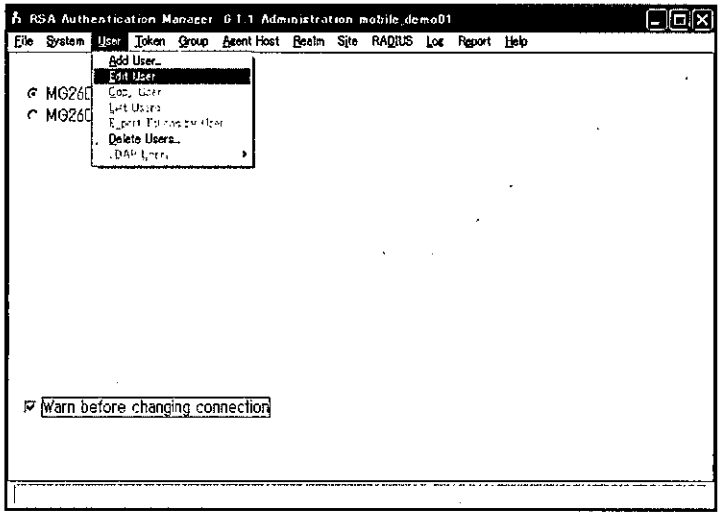
11. RSA SecurID及びパスワード(管理者用)と同じものを入力し、「OK」ボタンをクリックし、モバイル認証サーバの認証を行う。

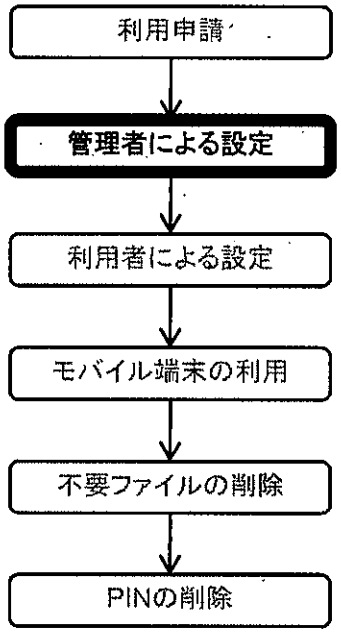
ここでは例としてログインIDに「 localmanager_0100 」を使用する。



管理者

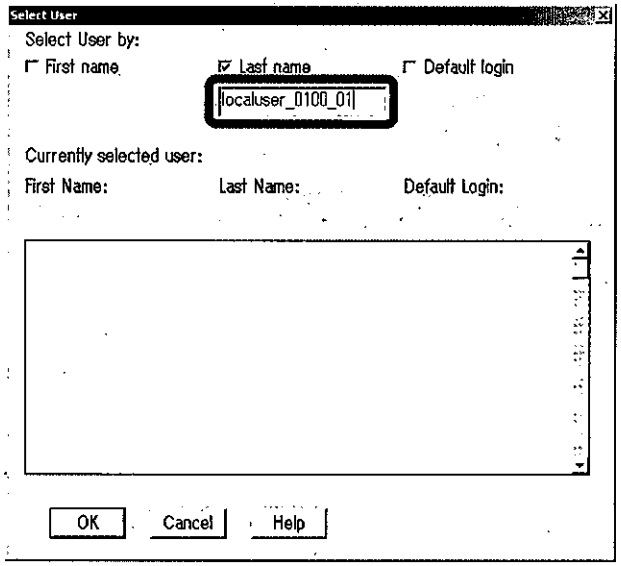
12. [User]メニューから「Edit User...」を選選択する。





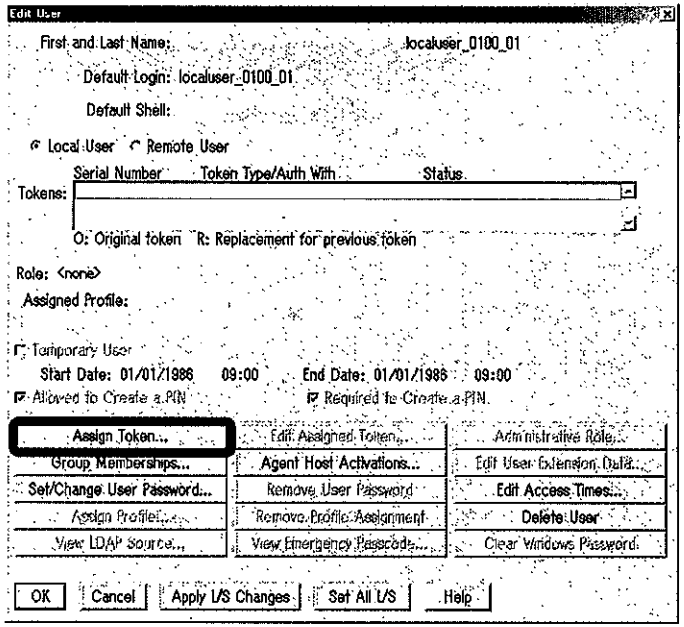
管理者

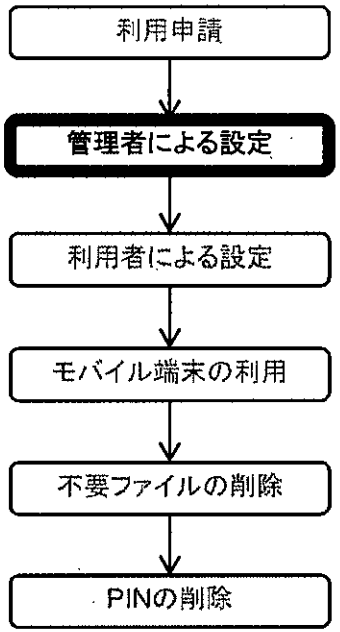
13. 表示される「Select User」ダイアログに通知されたユーザIDを入力し、「OK」ボタンをクリックする。
ここでは例として「localuser_0100_01」を使用する。



管理者

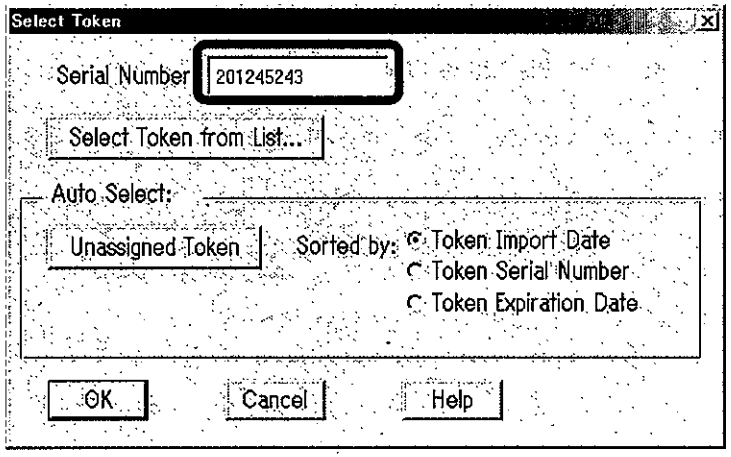
14. 表示された「Edit User」画面の「Assign Token...」ボタンをクリックする。

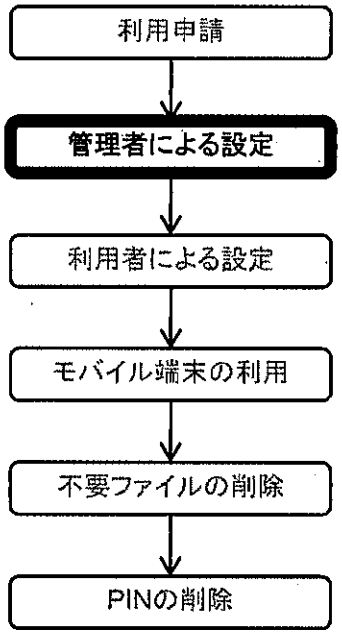




管理者

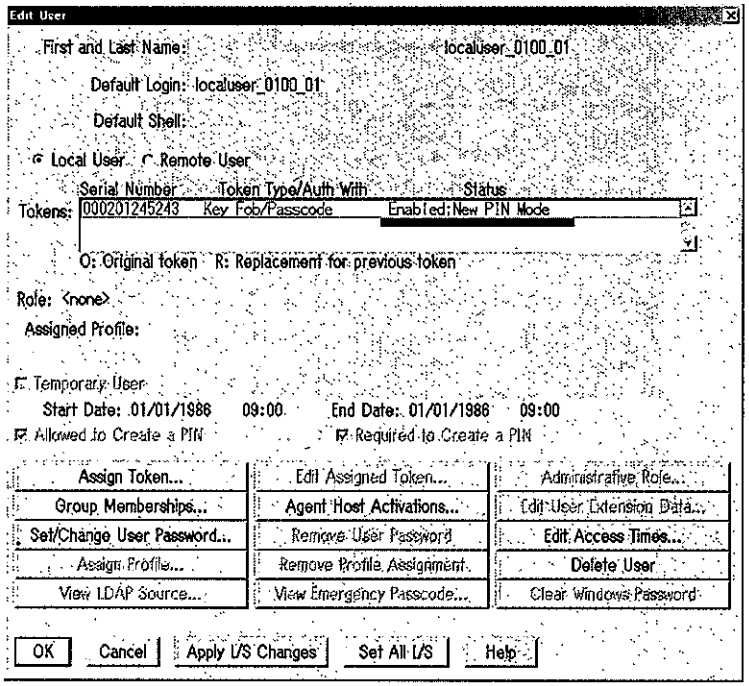
15. モバイル端末と一緒に配備した労働基準行政システム用トークンのシリアル番号（トークンの背面に書かれた数字）を入力し、「OK」ボタンをクリックする。
ここでは例としてシリアル番号「201245243」の労働基準行政システム用トークンを使用する。





管理者

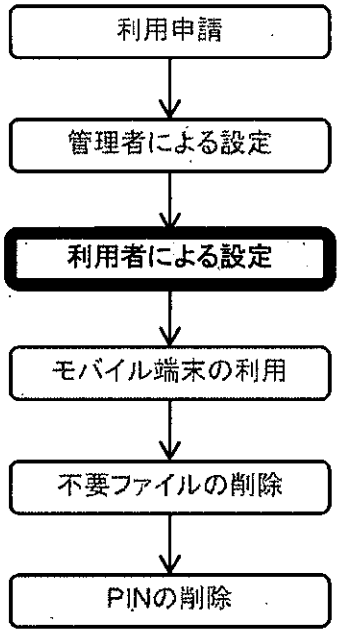
16. Tokensのステータス表示が、「New PIN Mode」になっていることを確認し、「OK」ボタンをクリックする。



管理者

17. 以上で管理者による設定が終了する。
管理者による設定が終了したら、次に利用者によりPINの任意設定を行う。

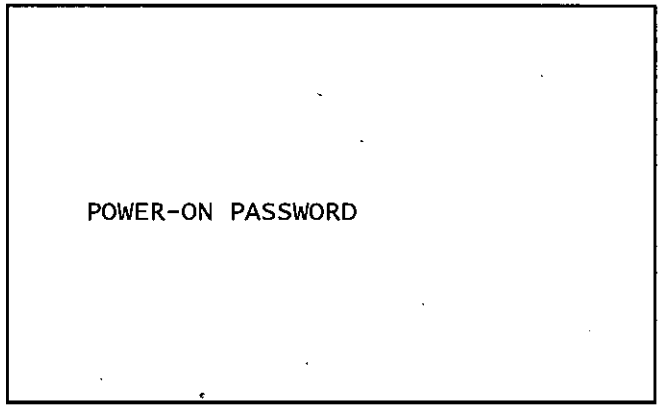
第7　利用者による設定



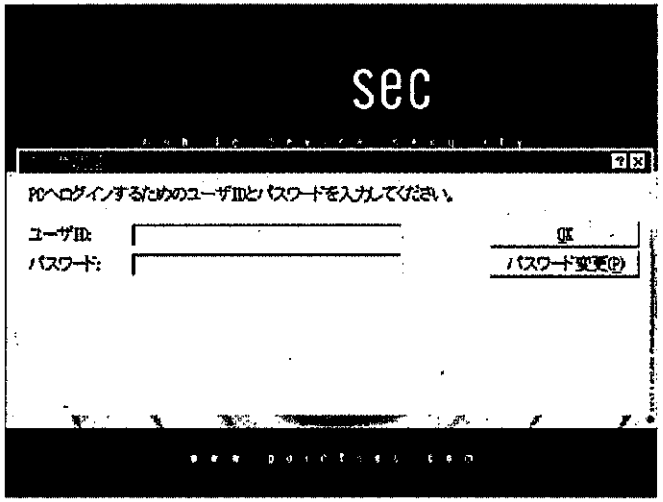
本手順は、第6の設定後に管理者の所属課室におけるLANにて、モバイル認証サーバにアクセスできる状態で行う。

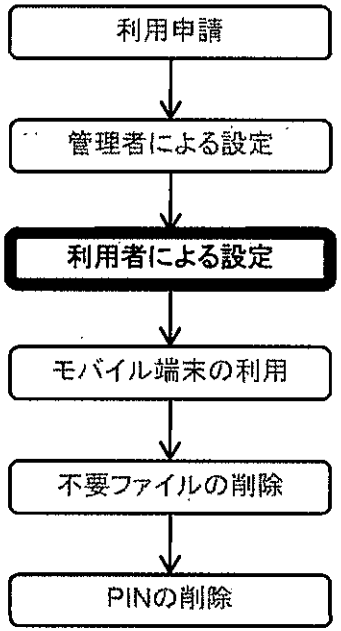
利用者　1. モバイル端末をLAN接続状態で以下の設定を行う。
（第6の操作後に電源を落とさずに続けて設定を行う場合は、WINDOWSからのログオフを行うことにより、第7の5からの開始となる。）

利用者　2. BIOSパスワードが求められるので、通知されたパスワードを入力する。
※入力したパスワードは無表示となる。



利用者　3. HDD暗号ソフトウェアの認証が求められるので、通知されたpointsecユーザID及びパスワードを入力し、「OK」ボタンをクリックする。



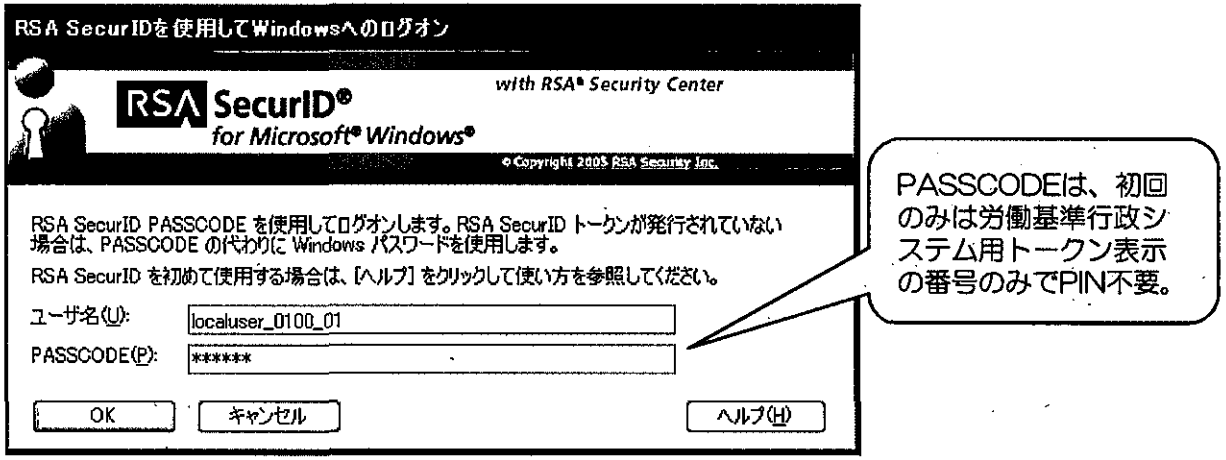


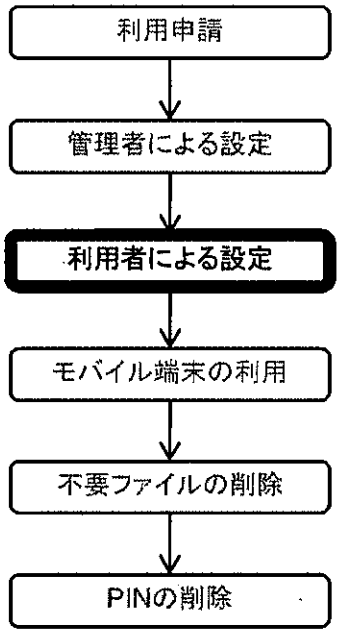
利用者 4. 正常に認証が行われるとOSが起動する。

利用者 5. ユーザ名にRSA SecurIDを入力し、PASSCODEに労働基準行政システム用トークンが生成する6桁の数字を入力し、「OK」ボタンをクリックする。

（<u>PINが設定されていない初期状態では労働基準行政システム用トークンの数字のみで入力</u>）

今回は例としてユーザIDに「localuser_0100_01」、
PASSCODEに労働基準行政システム用トークンが生成する6桁の数字（使う時間によって異なる値）を使用する。

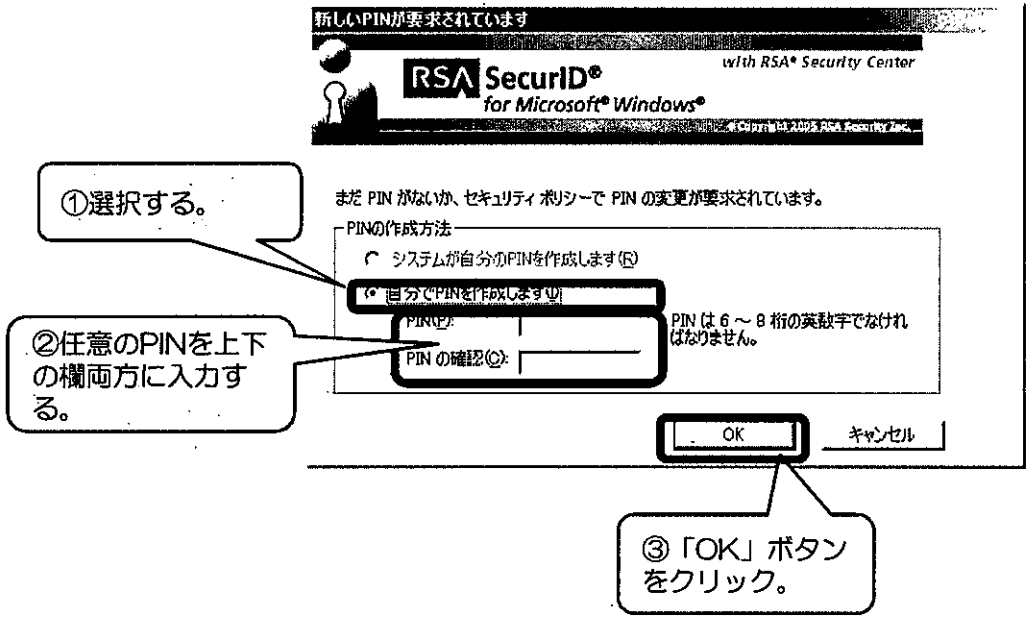




利用者

6. PINを設定するよう求められるので、「自分で作成します」を選択し、6～8桁の任意の英数字を入力し、PIN設定を行う。

（注）このPINを忘れるとモバイル端末にログオンできなくなるため、その場合は管理者に依頼をして再度PINの初期化を行う必要がある。

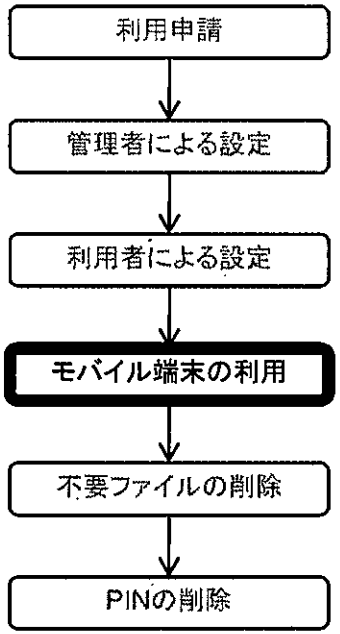


利用者 7. ユーザ名に通知されたRSA SecurIDを入力し、PASSCODEに設定したばかりのPIN（6～8桁）＋労働基準行政システム用トークンが生成する6桁の数字を入力し、「OK」ボタンをクリックする。

利用者 8. デスクトップ画面が表示される。

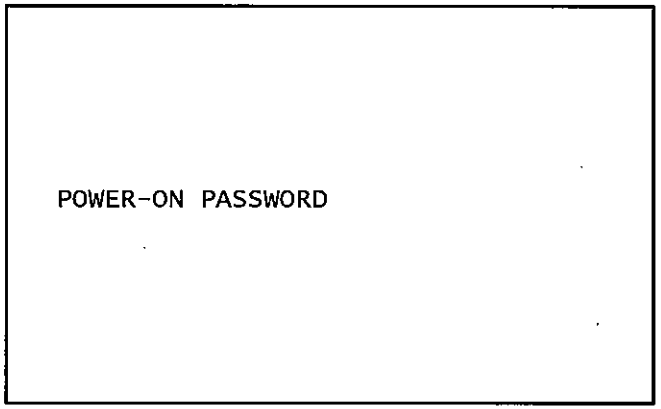
利用者 9. 以上でモバイル端末をPHS接続で利用することができる。

第8 モバイル端末の利用

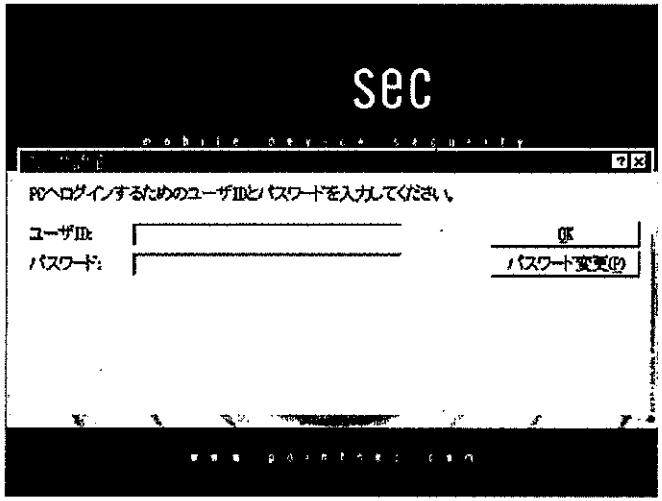


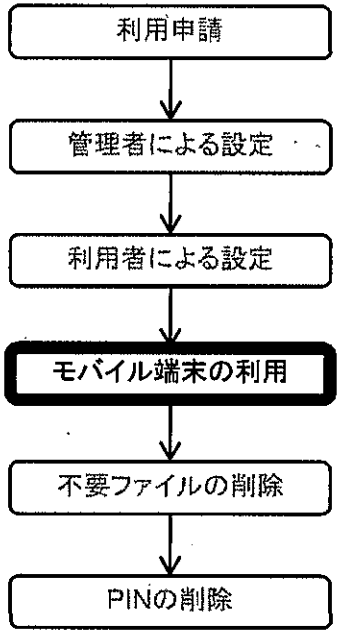
利用者 1. モバイル端末に電源を投入する。

利用者 2. BIOSパスワードが求められるので、通知されたパスワードを入力する。
※入力したパスワードは無表示となる。



利用者 3. HDD暗号ソフトウェアの認証が求められるので、通知されたpointsecユーザID及びパスワードを入力し、「OK」ボタンをクリックする。

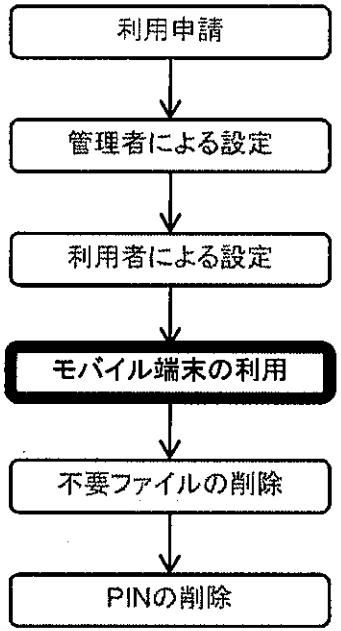




利用者 4. 正常に認証が行われるとOSが起動する。

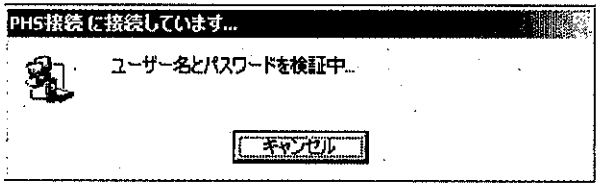
利用者 5. ユーザ名に通知されたRSA SecurIDを入力し、PASSCODEに第7の6で設定したPIN（6～8桁）＋労働基準行政システム用トークンが生成する6桁の数字を入力し、「OK」ボタンをクリックする。
これ以降、利用者は、PHSを使用した接続が可能となる。

※この認証において、10回以上連続して認証が失敗した場合、労働基準行政システム用トークンが使用できない状態となる。この場合に使用可能な状態に戻すためには、管理者による設定変更が必要となる。



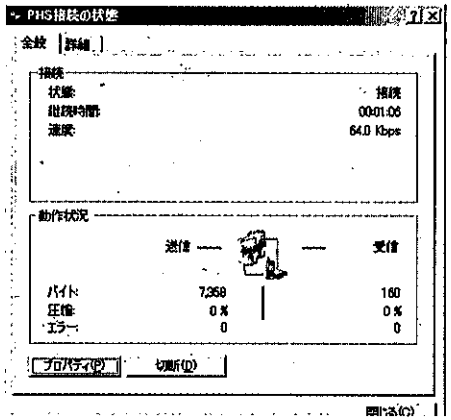
利用者

6. OSログオン後、デスクトップ上の「PHS接続」のアイコンをダブルクリックし、表示される「PHS接続 へ接続」画面に管理者から通知されたダイヤルアップID及びパスワード＋統合ネットワーク用トークン表示の数字を入力し、「ダイヤル(D)」ボタンをクリックする。



※1 この認証において、5回以上連続して認証が失敗した場合、統合ネットワーク接続用トークンができない状態となる。この場合に使用可能な状態に戻すためには、統合ネットワーク側での解除操作が必要となるため、ヘルプデスクへの連絡が必要となる。

※2 接続されると画面右下のタスクトレイにアイコンが表示される。また、デスクトップ上の「PHS接続」アイコンをダブルクリックすると「PHS接続の状態」画面が表示され、接続状態を確認することができる。

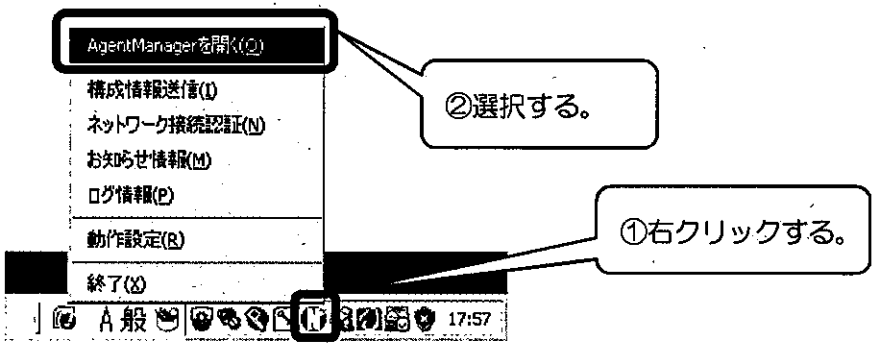


利用申請
↓
管理者による設定
↓
利用者による設定
↓
モバイル端末の利用
↓
不要ファイルの削除
↓
PINの削除

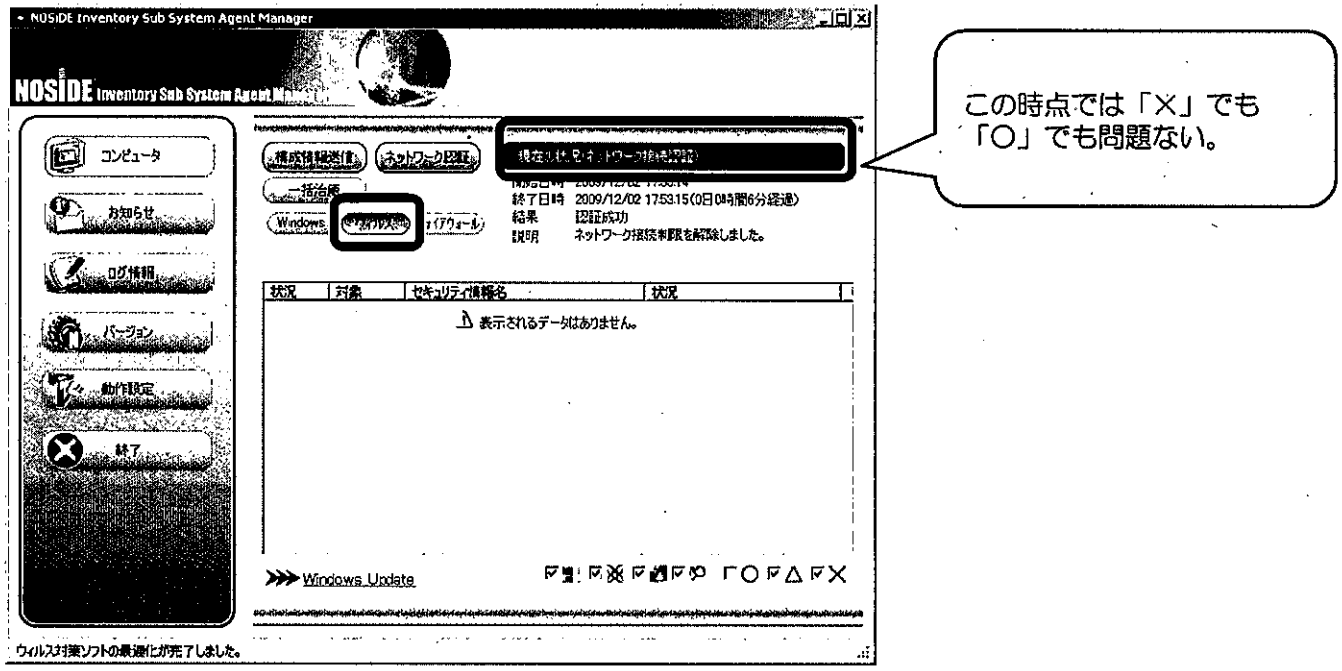
利用者

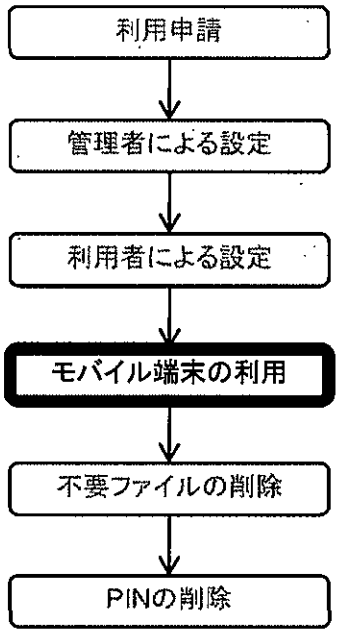
7. 画面右下タスクトレイのNOSiDEのアイコンを右クリックし、表示されたコンテキストメニューより「AgentManagerを開く(O)」を選択する。

※第7の7から9までの一連の操作を行っていない場合は労働基準行政システム側の接続が拒否される場合があるため、必ずこの一連の操作は行うこと。



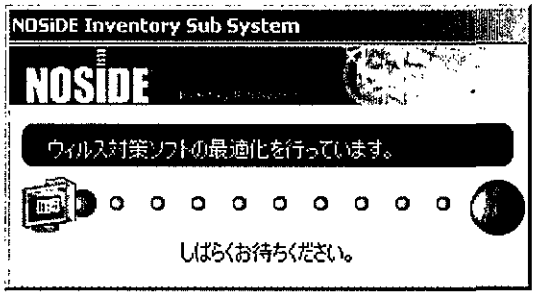
・表示されたNOSiDEメイン画面より、「ウィルス」ボタンをクリックする。

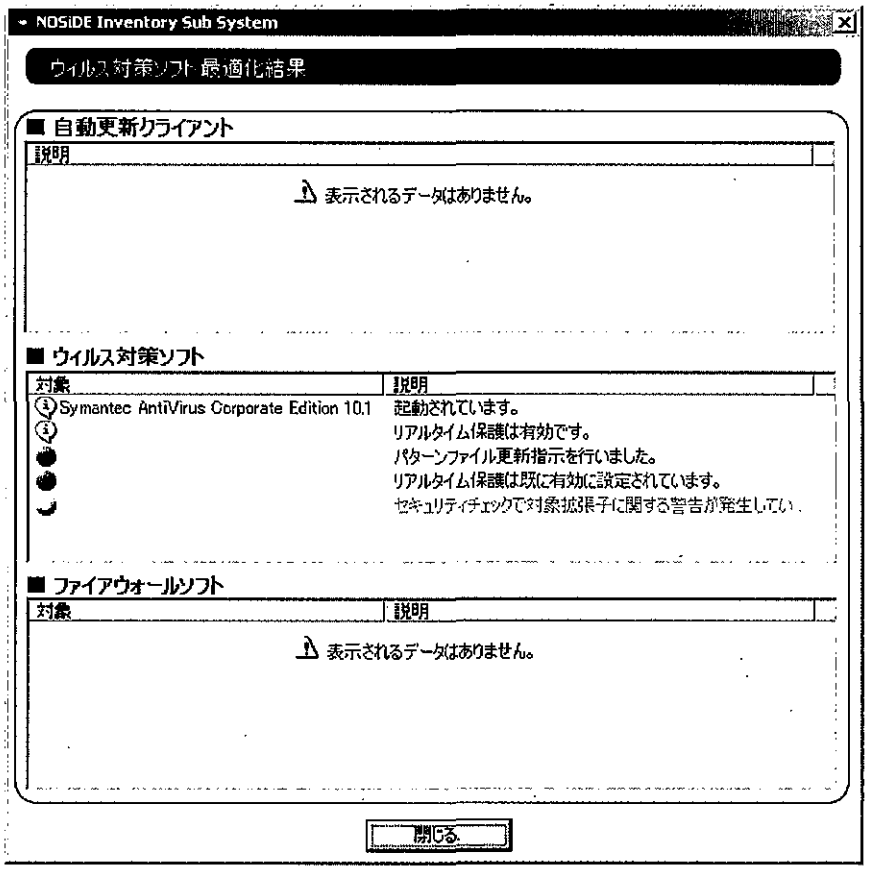




利用者

8. 結果画面が表示される。





利用申請

↓

管理者による設定

↓

利用者による設定

↓

モバイル端末の利用

↓

不要ファイルの削除

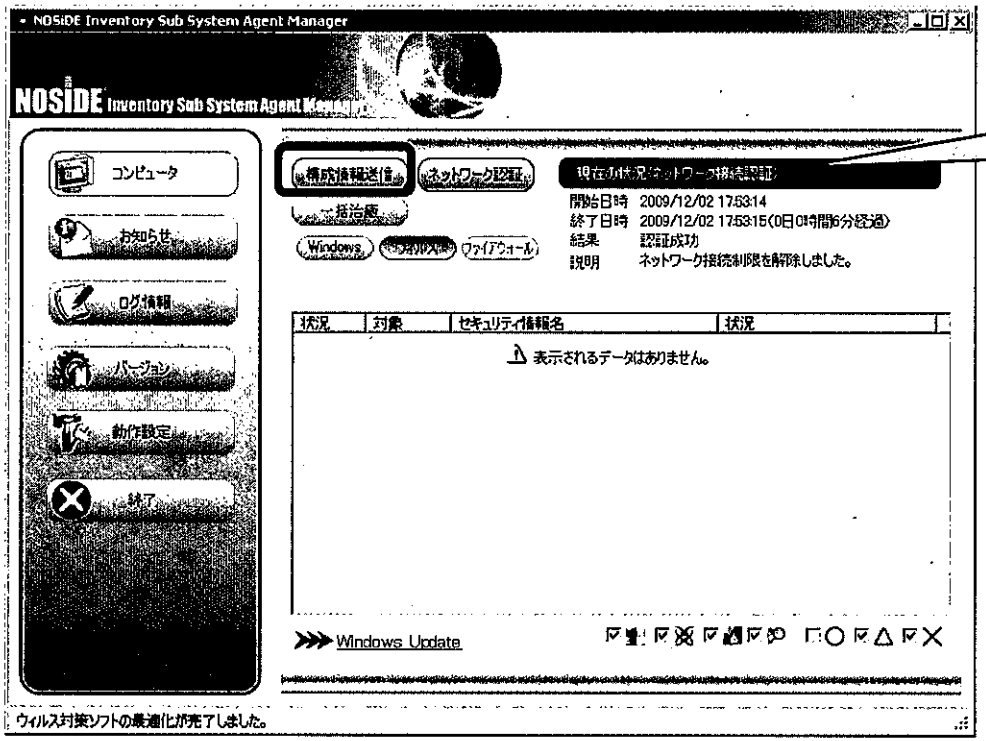
↓

PINの削除

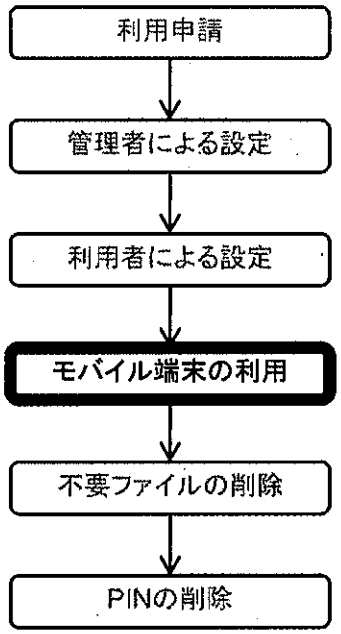
利用者

9. 表示されているNOSiDEのメイン画面を起動し、「構成情報送信」ボタンをクリックする。

※OSにログオンし、NOSiDEによる端末の認証も完了した時点でThin Clientと同様に上石神井センタへ接続された状態となる。

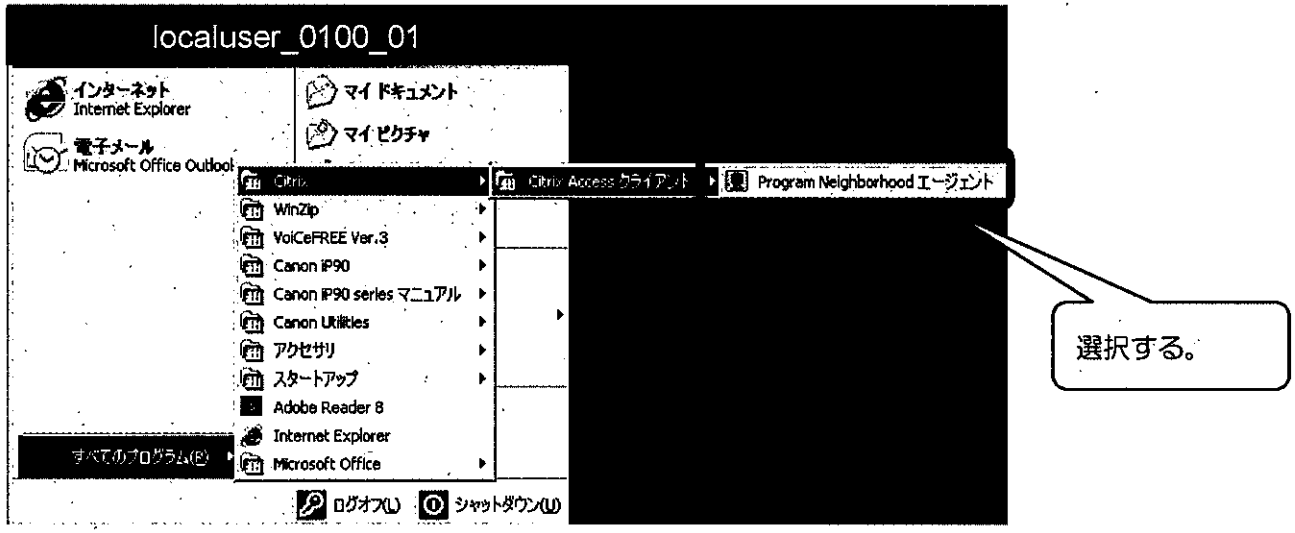


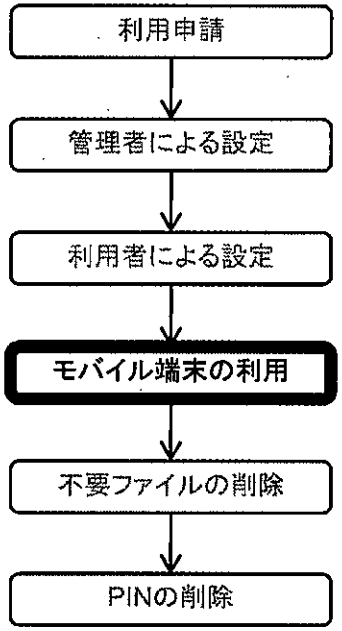
「○」となっていることを確認する



利用者

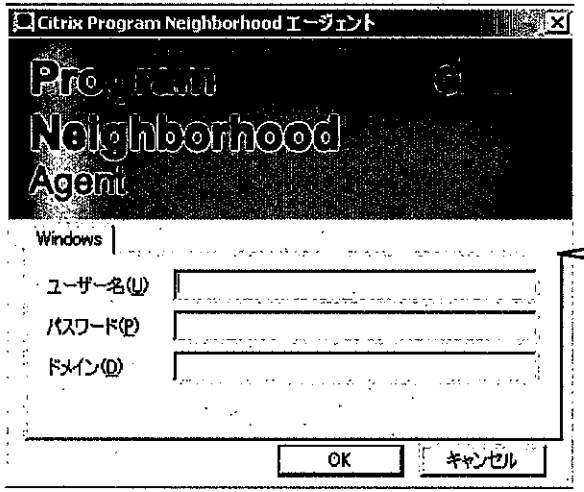
10. Windowsのスタートメニューより、Citrixの「Program Neighborhood エージェント」を起動する。





利用者

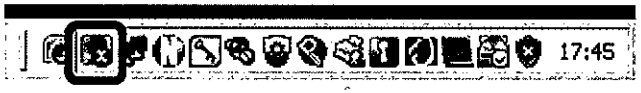
11. 利用者がThinClient、Fat Clientを使用するときと同じユーザ名、パスワード、ドメイン名を入力し、「OK」ボタンをクリックする。
（すでにThinClientにログオンしている状態での 多重ログオンはできない。）



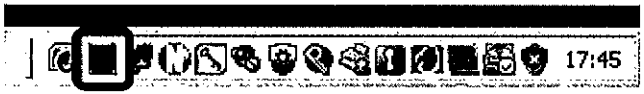
ThinClient、FatClientで入力しているユーザ名、パスワード、ドメイン（KRDN）を入力

利用者

12. 画面右下タスクトレイの「Citrix」アイコンより、正常ログオンされたことを確認する。



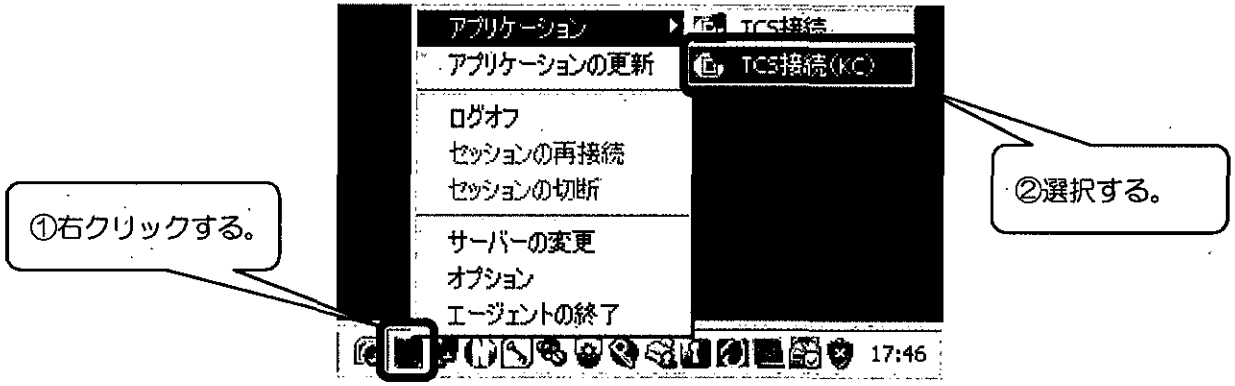
ログオン前の状態



正常ログオン後の状態

利用者

13. 画面右下タスクトレイの「Citrix」アイコンを右クリックし、「TCS接続(KC)」を選択する。



利用者

14. 「TCS接続(KC)」が開始されたことを確認する。

利用者

15. 以上でThinClientと同等の機能が利用可能となる。

利用申請

↓

管理者による設定

↓

利用者による設定

↓

モバイル端末の利用

↓

不要ファイルの削除

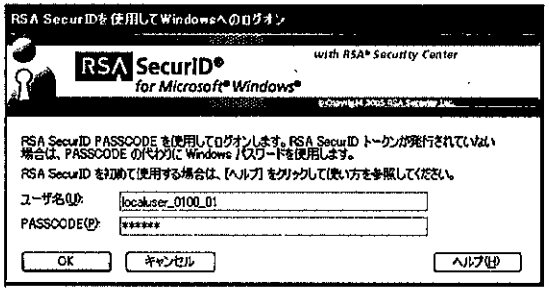
↓

PINの削除

【その他】

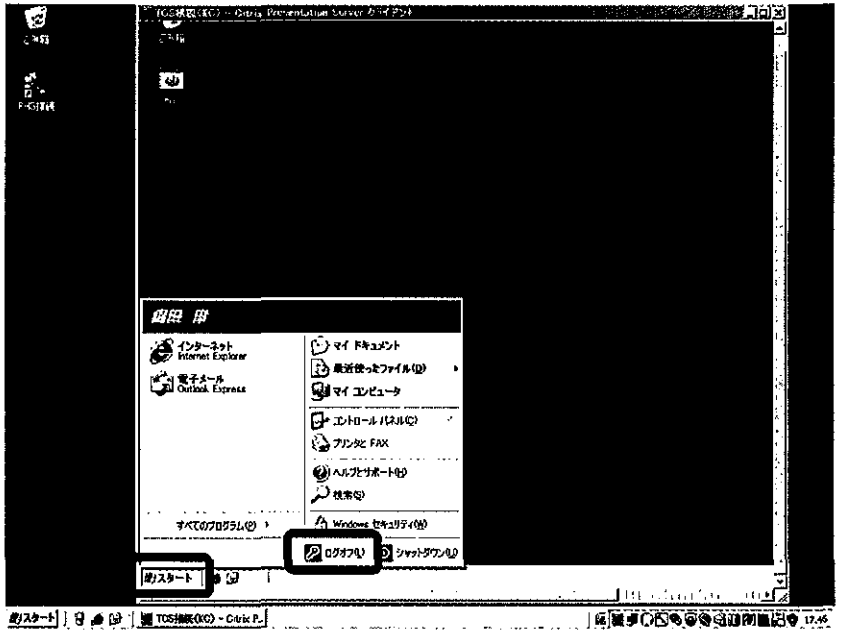
モバイル端末は一定時間操作がされない状態が続いた場合は、操作のロックがかかる。

ロックを外すにはRSA SecurID及びパスワード（利用者用）による再度の認証を行う（第8の5参照。）。

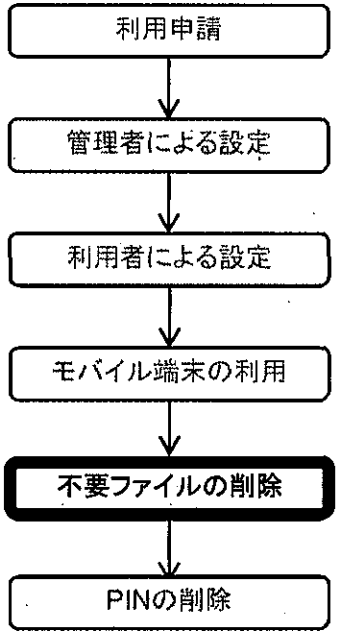


利用者

16. 業務終了後は「TCS接続（KC）」のスタートメニューから「ログオフ」を行う。
※この状態ではまだPHSによる接続状態が続いているので、OSからのログオフを行うか、「PHS接続」のアイコンをダブルクリックし「PHS接続の状態」画面で「切断」をクリックすること。



第9　不要ファイルの削除

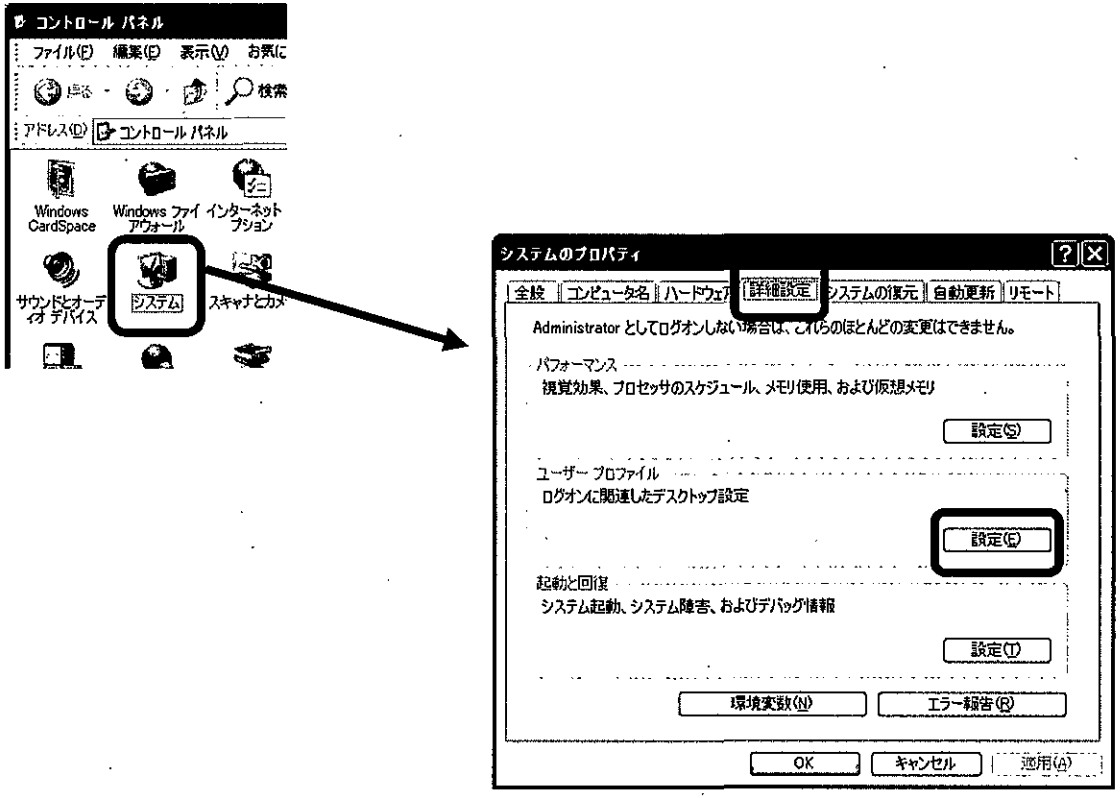


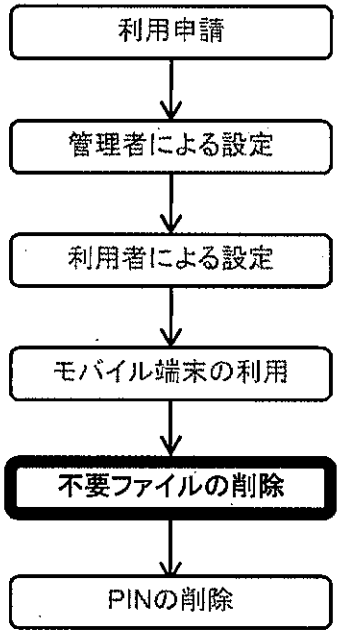
利用者はモバイル端末返却時に、本体の不要なファイルを削除する。
管理者は、利用者からモバイル端末が返却された際にモバイル端末本体の前の利用者が保存したファイルの削除と、前の利用者の行った各種設定の初期化を行うためにユーザプロファイルの削除操作を行う。

このユーザプロファイルの削除操作は、管理者権限でモバイル端末にログオンしている状態で行う。

管理者

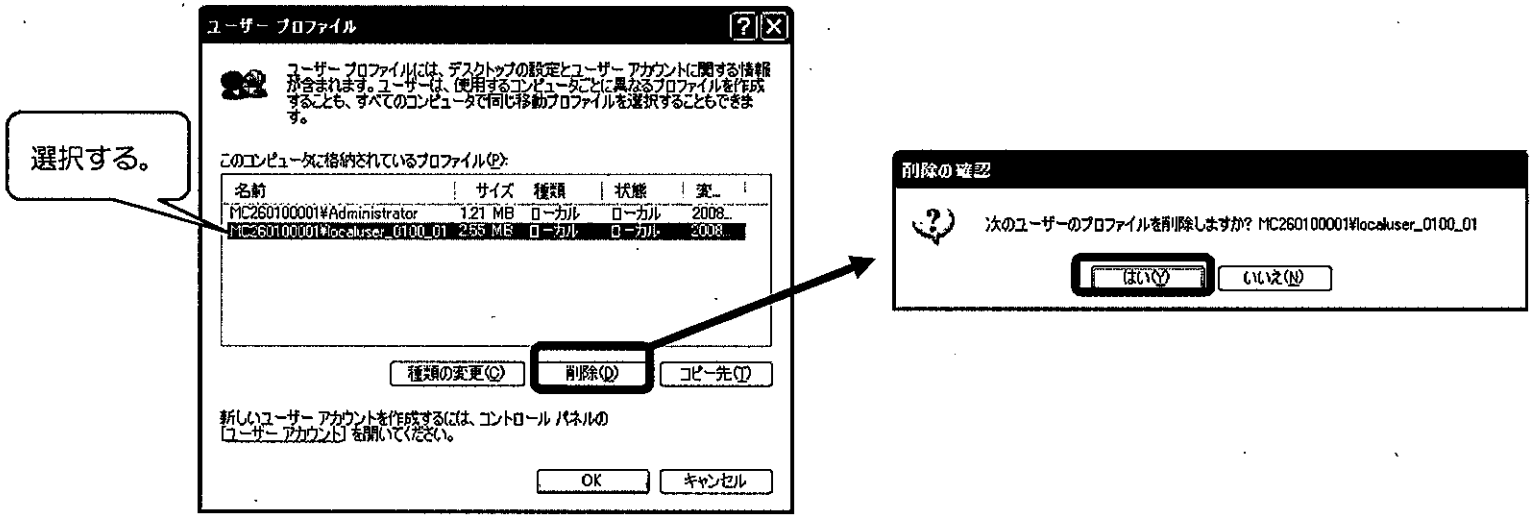
1.　第6の1から5の操作を行った後、Windowsのスタートメニューより「コントロールパネル」を起動し、「システム」をダブルクリックする。
「システムのプロパティ」画面が開くので、上部の「詳細設定」タブをクリックし、「ユーザプロファイル」の「設定」ボタンをクリックする。





管理者

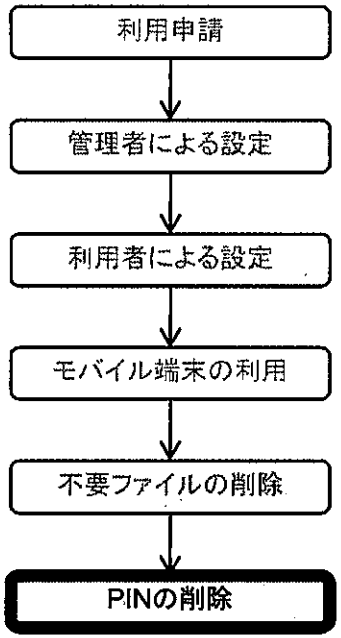
2. 「ユーザープロファイル」画面が開く。
削除したい利用者を選択し、「削除」ボタンを押す。「削除の確認」ポップアップで「はい」ボタンをクリックする。
ここでは例として「localuser_0100_01」を使用する。



第10　PINの削除

次のユーザに貸し出すため労働基準行政システム用トークンに設定されたPINを削除する。

この削除操作は、管理者権限でモバイル端末にログオンしている状態で行う。



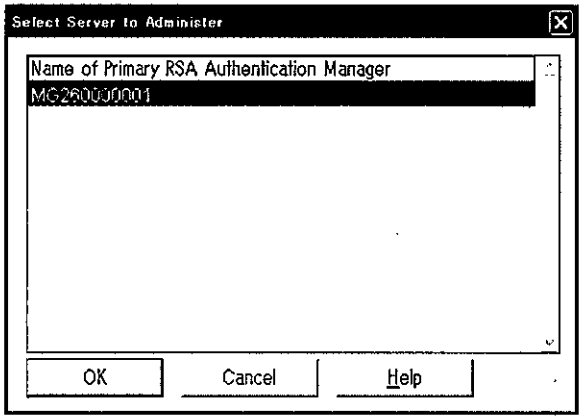
管理者

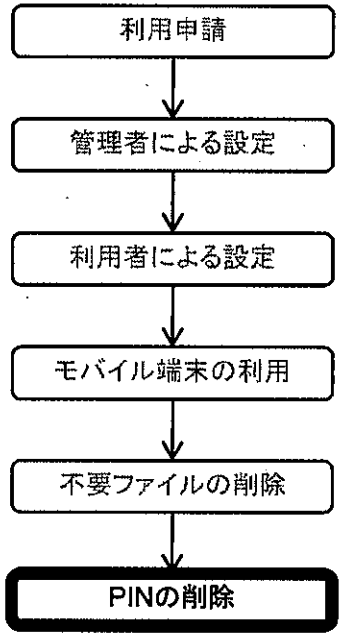
1. 第9の不要ファイルの削除を行った後、デスクトップ画面左下のスタートメニューから「マイコンピュータ」をクリックし、続けて「ローカルディスク(C:)」をダブルクリック、「soft_shortcut」をダブルクリック、「RSA Security」をダブルクリック、と進むと表示される「RSA Authentication Manager Remote Mode」をダブルクリックし起動する。

管理者

2. 利用者(サーバ)を登録するためRSA Authentication Manager Remote Mode (C:¥soft_shortcut¥RSA Security にある)を起動する。

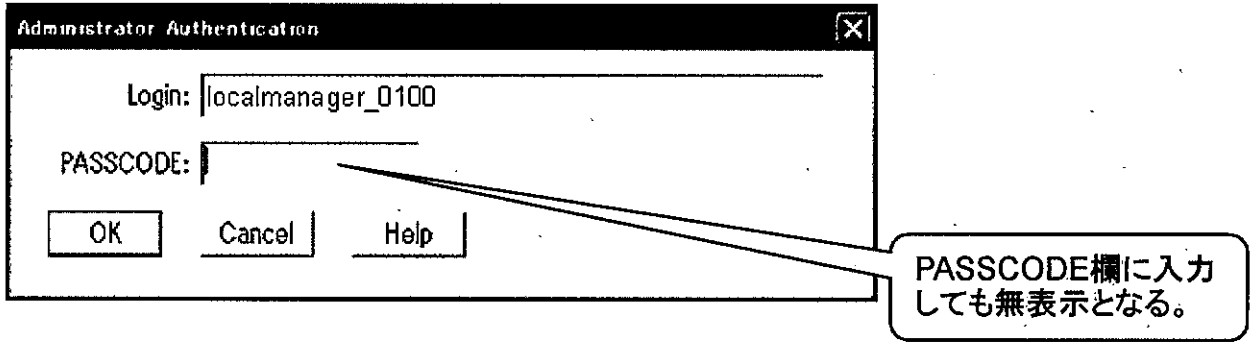
「MG260000001」を選択し、「OK」ボタンをクリックする。



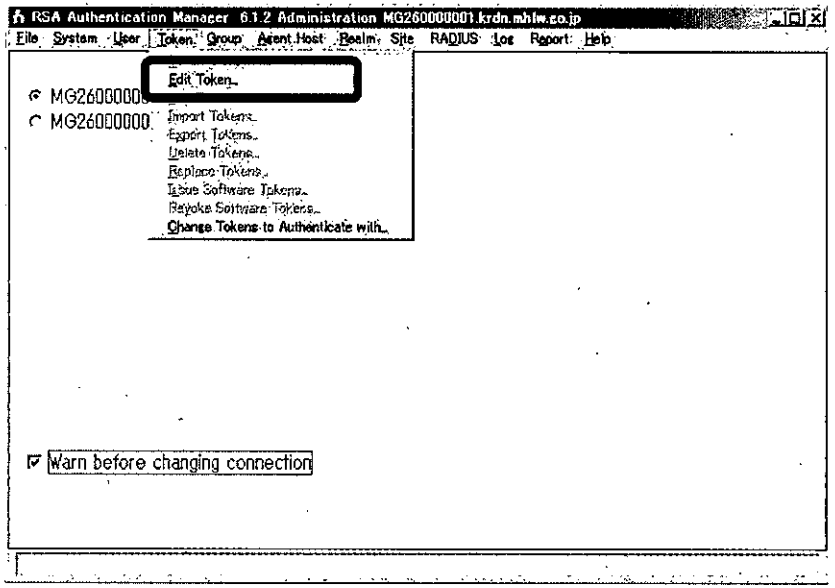


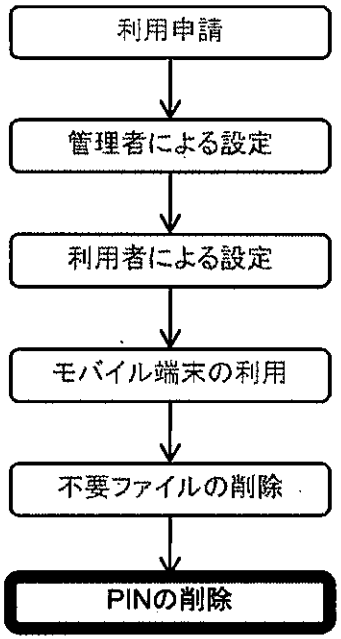
管理者 3. RSA SecurID及びパスワード(管理者用)と同じものを入力し、「OK」ボタンをクリックし、モバイル認証サーバの認証を行う。

ここでは例としてログインIDに「 localmanager_0100 」を使用する。



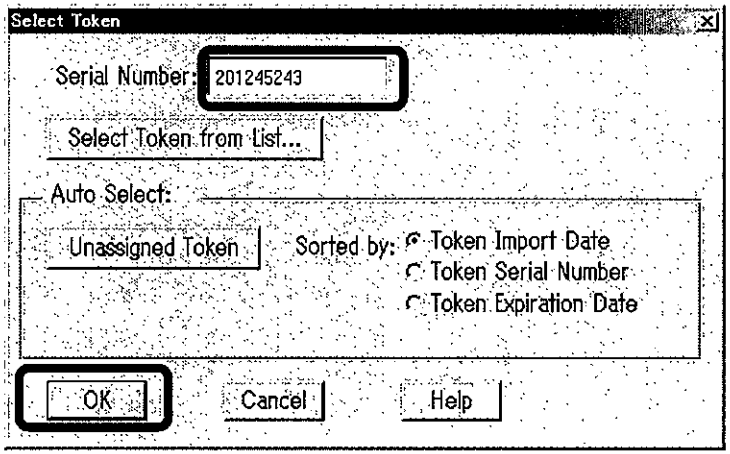
管理者 4. [Token]メニューから「Edit Token...」を選択する。

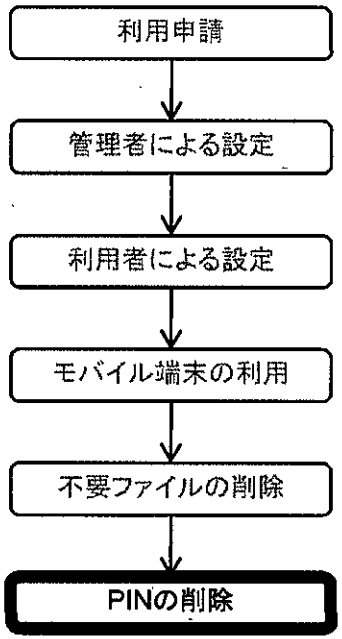




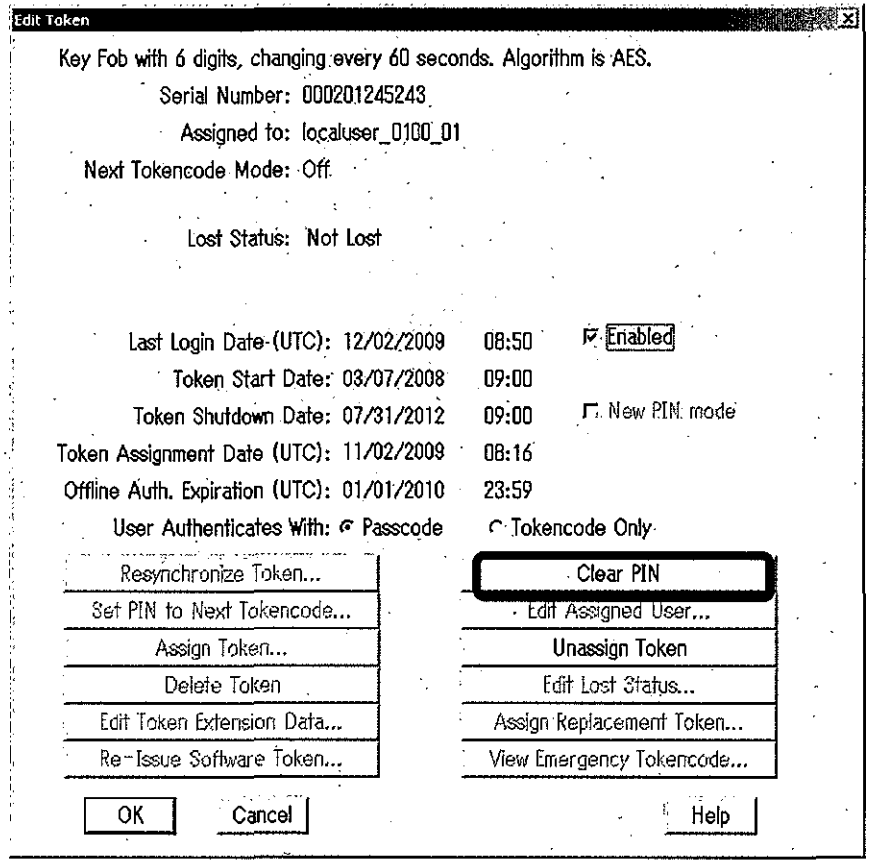
管理者

5. 「Serial Number」欄に労働基準行政システム用トークンのシリアル番号を入力し、「OK」ボタンをクリックする。
ここでは例として「201245243」のシリアル番号を持つ労働基準行政システム用トークンを使用する。





管理者 6.「Clear PIN」ボタンをクリックする。



参考

※1 ユーザがPINを忘れた場合の初期化においては、第6の1から5の操作を行った後、第10の操作を行う。

※2 RSA SecurID認証において、10回以上連続して認証を失敗した場合、労働基準行政システム用トークンが使用できない状態となる。この場合は上記画面の「Enabled」のチェックを付けることにより回復する。

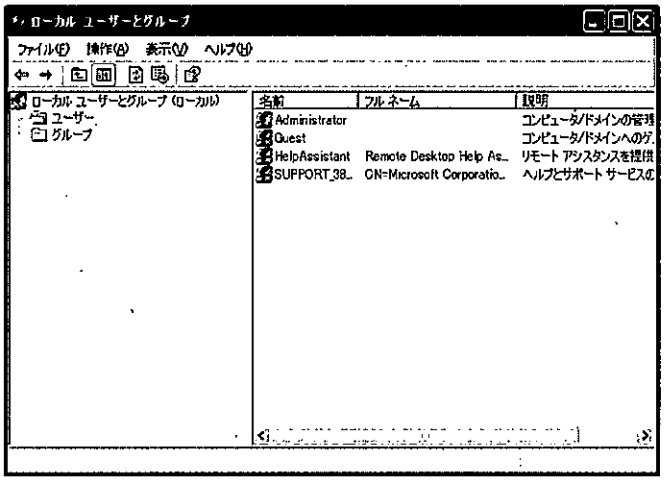
第11　利用者情報の再登録

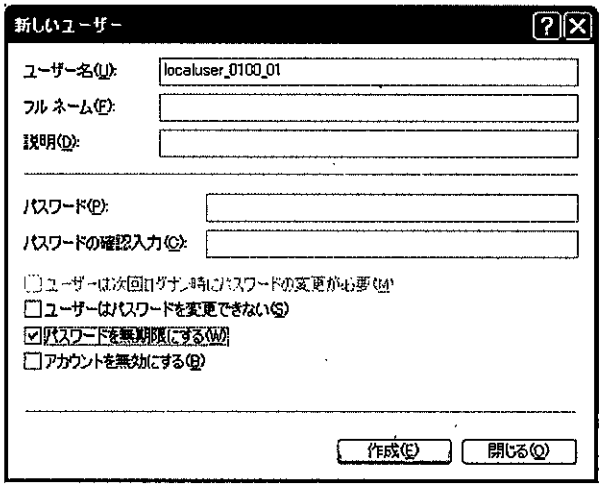
利用者（ローカル）情報については、モバイル端末配備時は初期設定を行っているが、各種設定において、利用者情報を削除した場合のモバイル端末へのローカルユーザの再登録手順は以下のとおりである。

再登録は、管理者権限でモバイル端末にログオンしている状態で行う。

管理者

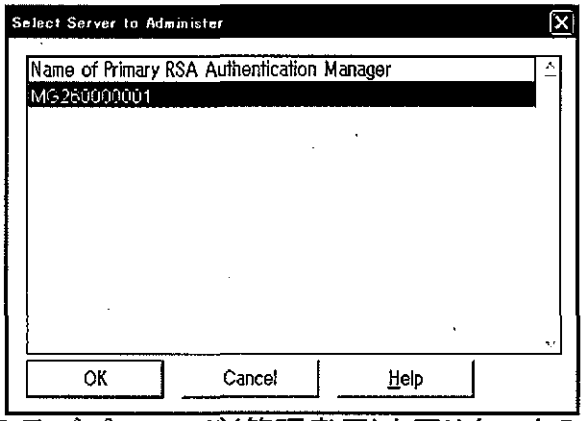
1. スタートメニューから「コントロールパネル」を選択し、その中にある「管理ツール」を選択すると表示されるウィンドウの中から「コンピュータの管理」をクリックすると「コンピュータの管理」が立ち上がる。画面中の「ローカルユーザーとグループ」から「ユーザー」にカーソルを合わせ右クリックを行うと、「新しいユーザー」画面が立ち上がる。
   通知されたユーザIDのみを入力し、4つのチェックボックス中「パスワードを無期限にする」にのみチェックを行い「作成」ボタンをクリックする。
   今回は例としてユーザIDに「localuser_0100_01」を使用する。





管理者

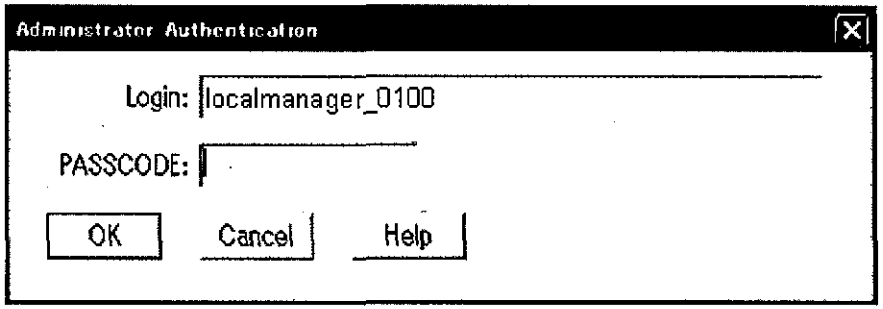
2. デスクトップ画面左下のスタートバーから「マイコンピュータ」をクリックし、続けて「ローカルディスク(C:)」をダブルクリック、「soft_shortcut」をダブルクリック、「RSA Security」をダブルクリック、と進むと表示される「RSA Authentication Manager Remote Mode」をダブルクリックし起動する。表示された「MG260000001」を選択し、「OK」ボタンをクリックする。



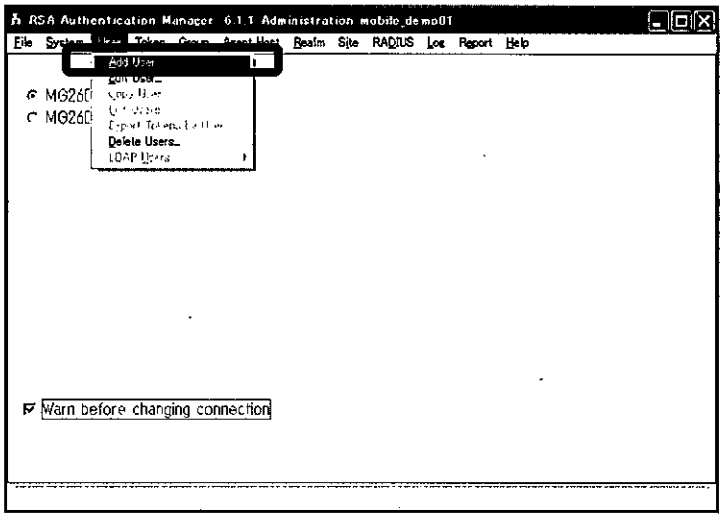
管理者

3. RSA SecurID及びパスワード(管理者用)と同じものを入力し、「OK」ボタンをクリックし、モバイル認証サーバの認証を行う。

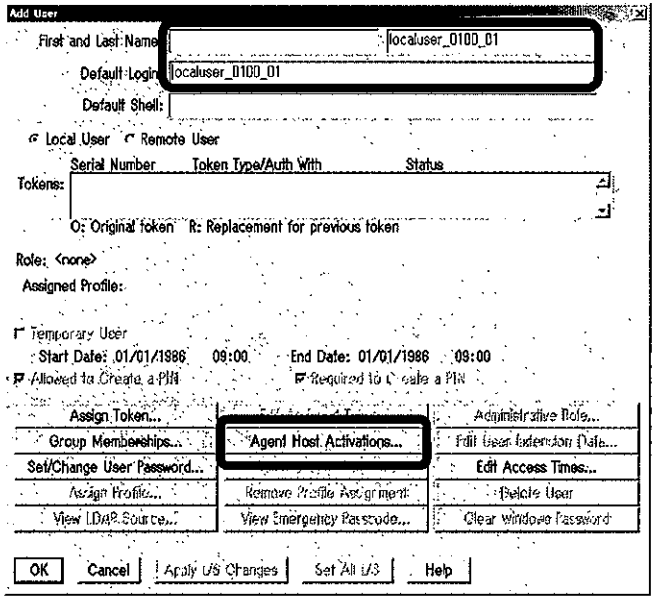
ここでは例としてログインIDに「 localmanager_0100 」を使用する。



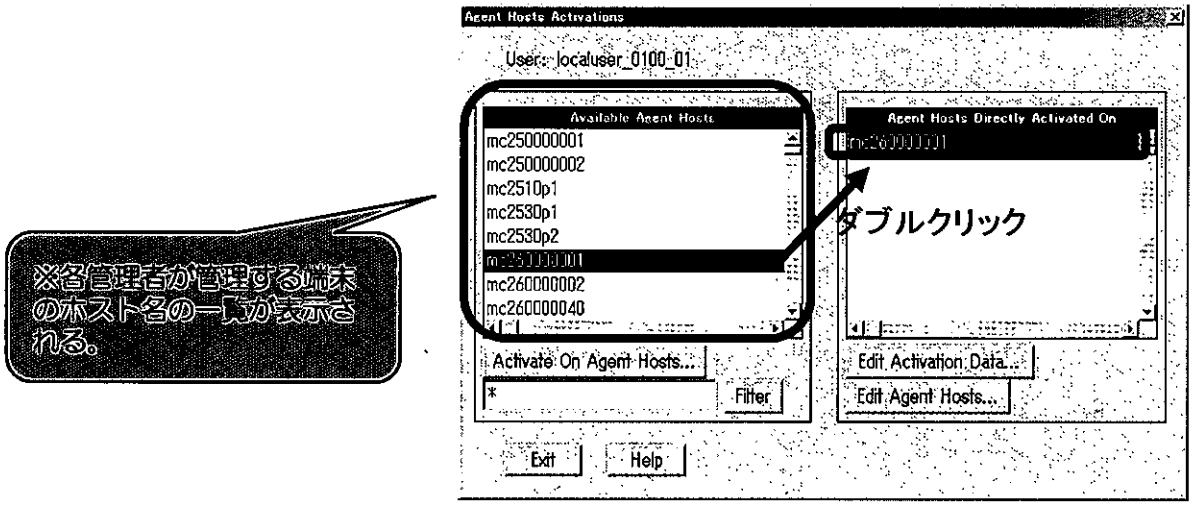
管理者 4. [User]メニューから「Add User...」を選択する。



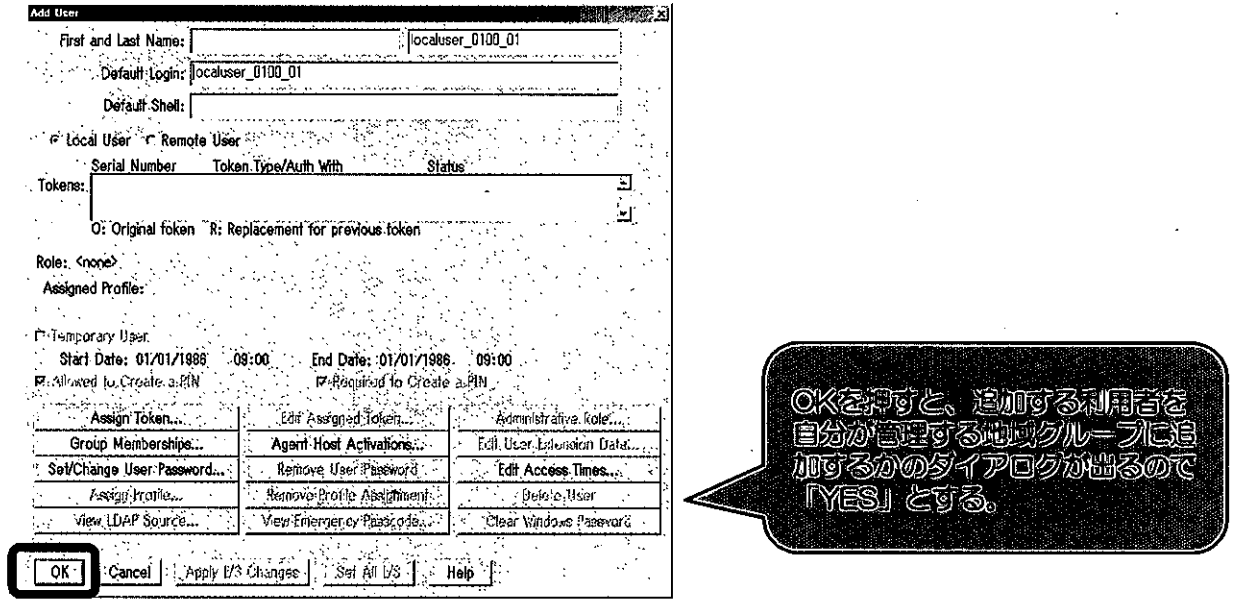
管理者 5. 第11の1でモバイル端末に登録した利用者と同じIDを入力し、「Agent Host Activations ...」ボタンをクリックする。
ここでは例として「localuser_0100_01」を使用する。



管理者 6.「Agent Host Activations」に表示された端末のホスト名をダブルクリックし、「Exit」ボタンをクリックする。
ここでは例として「localuser_0100_01」利用者に、モバイル端末「MC260000001」を選択する。



管理者 7. 第7の5の「Add User」画面に戻るので「OK」ボタンをクリックし登録を完了する。



第12 トークン(労働基準行政システム用)交換時の設定

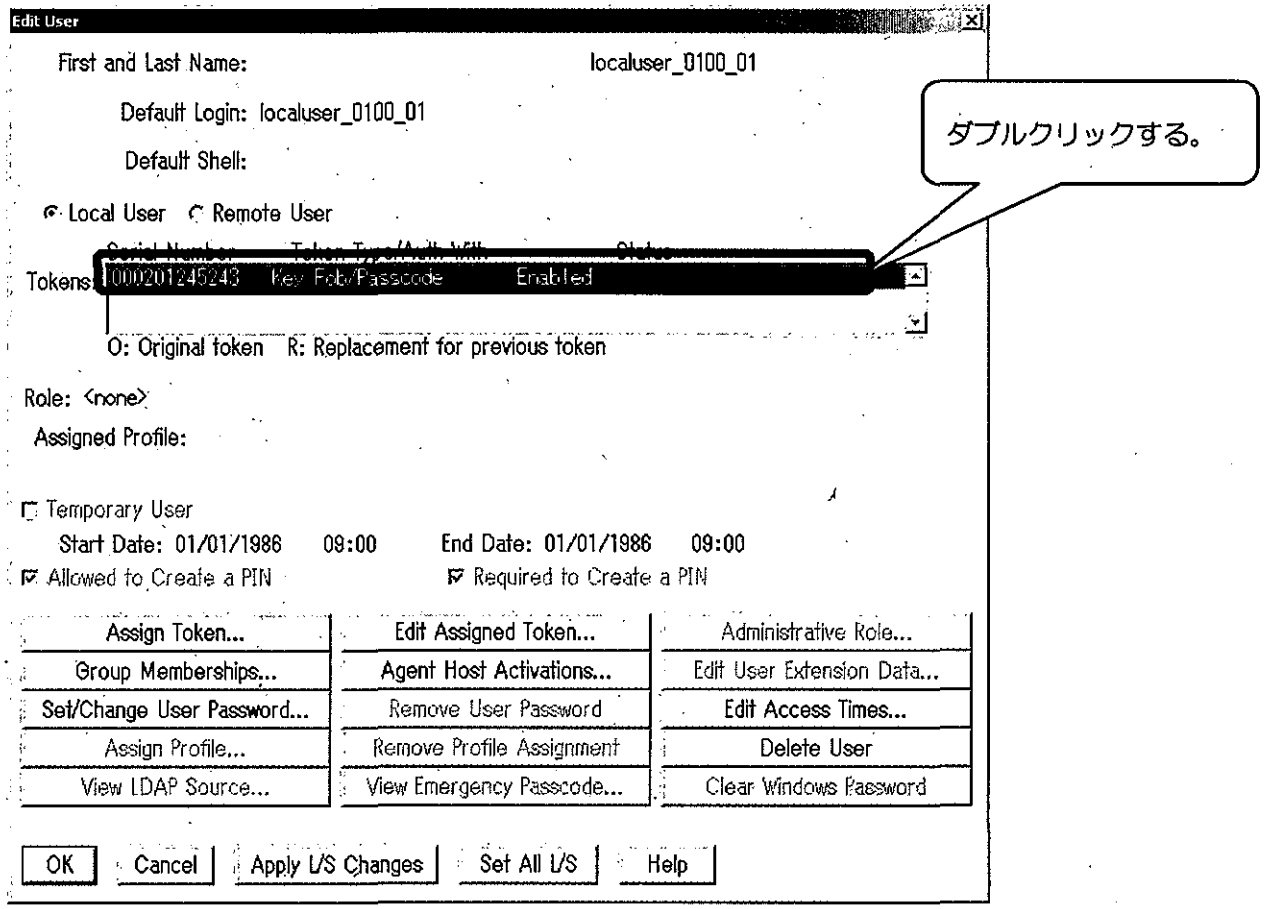
1つの労働基準行政システム用トークンには1つのユーザIDしか関連付けられないため、労働基準行政システム用トークン交換時には労働基準行政システム用トークンの関連付けを行う。その手順は以下のとおりである。

本手順は、管理者権限でモバイル端末にログオンしている状態(第6の5まで終了した状態)で行う。

なお、統合ネットワーク用トークンについては本省で設定することとなる。

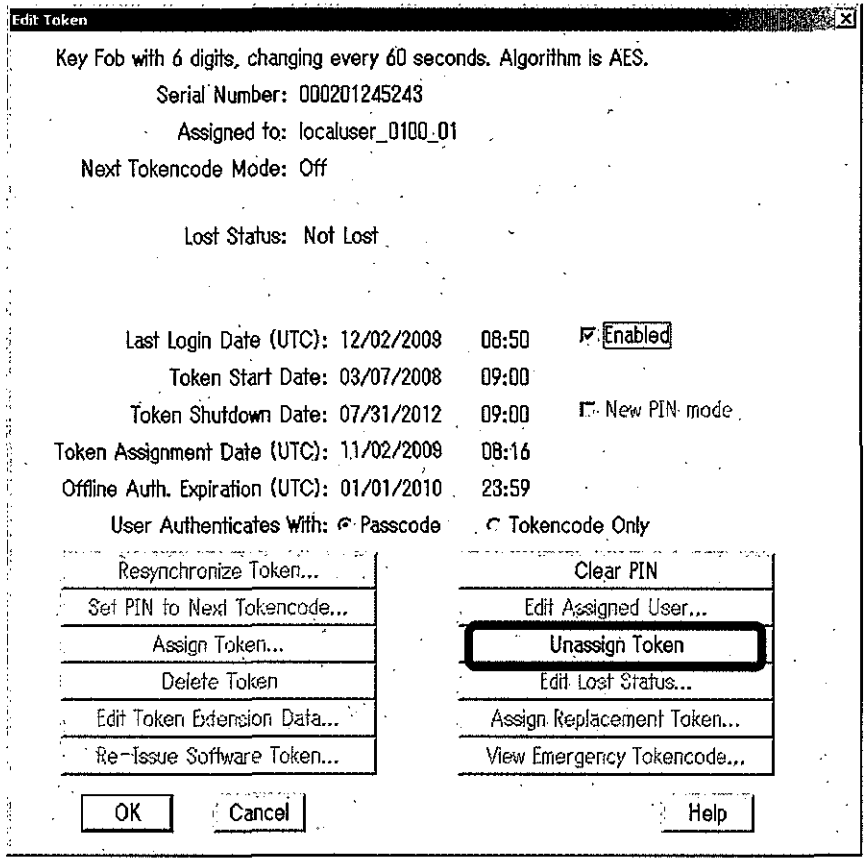
管理者

1. 第6の9から13までを行った後、表示された「Edit User」画面の「Tokens」をダブルクリックする。ここでは例として「localuser_0100_01」に割り当てられた労働基準行政システム用トークン「(000)201245243」を指定する。



管理者

2.「Unassign Token」ボタンをクリックし、労働基準行政システム用トークンの関連付けを解除する。
解除後は、交換後のトークンを用いた第6及び第7の作業を行うことにより交換後の労働基準行政システム用トークンが使用できる状態になる。



第13 問い合わせ先

主な問い合わせ先は以下のとおり。
その他についてはヘルプデスクに問い合わせをすること。

項番	問い合わせ内容(抜粋)	作業分担	
		管理者	運用業者(ヘルプデスク)
1	BIOSパスワード忘れ	○	―
2	PointsecのID及びパスワード忘れ	○	―
3	RSA SecurIDのID忘れ	○	―
4	PIN忘れ、RSA SecurIDロック (PIN初期化依頼、ロック解除依頼)	○	―
5	ダイヤルアップできない(故障、ロック)	―	○