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

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
1	利用範囲
2	利用対象者2
3	利用可能な端末
4	モバイル端末の装備品
5	利用機能
6	アクセスポイント
第4	モバイル端末の操作手順
1	管理者及び利用者による接続設定の操作等(貸出時)
2	利用者によるモバイル端末利用時の操作等(利用時)
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
1	貸出及び借用時等の管理
2	返却時及び返却後の管理
第6	利用申請手続
第7	利用終了後の手続
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
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6
2	ウイルスに感染した場合
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
 - 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

- 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
-	モバイル端末本体	<u> </u>		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
<i></i>	PHS通信カード	1		PHS通信カード
官	労働基準行政システム用トークン	」 甲 ⇒++		労働基準行政システム用トークン
埋土	統合ネットワーク用トークン	育		統合ネットワーク用トークン
有	 光学マウス	百		光学マウス
۲ <u>ب</u>	モバイルプリンタ本体	μ μ		モバイルプリンタ本体
よス	 モバイルプリンタ用ACアダプタ	よる		モバイルプリンタ用ACアダプタ
心	モバイルプリンタ用接続USBケーブル	引む		モバイルプリンタ用接続USBケーブル
月出	モバイルプリンタ用バッテリ	一切		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	1		マニュアル類
	キャリングバッグ	:		キャリングバッグ
	モバイル端末本体			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
甲	労働基準行政システム用トークン	官		労働基準行政システム用トークン
i 一述	統合ネットワーク用トークン	理业		統合ネットワーク用トークン
1)ア	光学マウス	伯 に		光学マウス
1	モバイルプリンタ本体	<i> </i>		モバイルプリンタ本体
4	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
周の	モバイルプリンタ用接続USBケーブル	山山		モバイルプリンタ用接続USBケーブル
留	モバイルプリンタ用バッテリ] 須		モバイルプリンタ用バッテリ
194	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
ł	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

7

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 <u>MC2</u>

No.	申請年月日	所属 氏名	申請理由	オ	借月 予望打	用 期間		許可 区分	貸与	年月	Ħ		貸 午可打	与 期間		返却	年月	日
	年月日		·	~	年 年	月 月	н Н	可否	年	月	Ħ	~	年 年	月月	日	年	月	日
	年月日	· ·		~	年 年	月 月	日日	可 否	年	月	Ħ	~	年 年	月 月	日 日	年	月	F
	年月日			~	年 年	月 月		可否	年	月	Ħ	~	年年	月 月	日日	年	月	ġ
	年月日			~	年 年	月 月	, В В	可 否	年	月	Ħ	~	年 年	月 月 、	日日	年	月	Ħ
	年月日			~	年 年	月 [,] 月	日日	可否	年	月	Ħ	~	年 年	月 月	日 日	年	月	в
	年月日			~	年 年	月 月	日日	可 否	 年	月	Ħ	~	年 年	月 月	日 日	年	月	Ħ
	年月日		C	~	年 年	月 月	田田	可 否	年	月	Ħ	~	年年	月 月	日日	年	月	目
	年月日	·		~	年 年	月 月	日日	可 否	年	月	ឝ	~	年 年	月 月	日 日	年	月	日
	年月日			~	年 年	月 月	日日	可 否	年	月	Ħ	~	年 年	月 月	日 日	年	月	日
	年月日			~	年年	月 月	H	可 否	年	月	Ħ	~	年年	月 月	日日	年	月	Ħ

8

0

	労働 労働基準部監督	局 課長 殿					 平成 労	、 年 働基準	月 日 臣 監督署長
					労働	局労働基	陸部		果・室長
	管理者(監督課長))					申請者所	所属課室署長	ž.
返去	印確認時印 借用・料	毕出許可時印					返却時印	借用・持	出申請時印
		-						•	
1	<u>モハシ</u> 借用・持出申 以下の。	イル端末借 請時 とおりモバイ	<u>用・持</u> ル端末を	出許可	「 申請書 新出したい	<u>兼</u> 返 ので、	法印確認 許可願い	浩 ます。	
			署		 労働局	労	働基準部	봌	≧・課
	氏名					,			
	申請理由								
	借用希望期間		年		Ħ	~	年	月	В
	持出先								. *
	許可・不許可年	月日	許可・不許可	ſ	年		月	Ħ	
管理	貸与 年 月日			年	月		Ħ		
百記入欄	貸与許可期間]	年	月	Ħ	~	年	月	日
	モバイル端末番 ※ [[] MC2~] の端末番号	涛 和C2							
2	返却確認時							<u> </u>	
	以下の。	とおりモバイ	ル端末を	返却いだ	こしました	ので、	確認願い	ます。	1
<u>1</u>	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	モバイル端末本	本に作成したこ 	ファイルの有 	*	有		無	
	××231年月日 ────────────────────────────────────	<u>م</u> يدر	역 	₩.dur B/- #X #	月		P		
※不用:	 文字は削除して使用す	・ ガ1 ること。	୬/ Ŋ 刀′割本 ¹	中印版省部	5 马泊				

9

【別紙3 本省用】

	労働基準用	司労災補償 * 教会 E	部				•	योत	成年	月	Ē
	万 灭休(陕乡	长 傍至女	敗				1	ġ	労働基準	『局 課・	室長
	労災保険 返却確認時印 /	業務室長 借用 · 持出許可	4\$ED					申請 返却時印	者所属課室	長 持出申 諸	消時 印
	<u>+</u>	シバイル	端末借	<u>用</u> ・持	出許可	「申請書	÷兼ì	反却不能	2書		
1	借用・持 以	出申請時 下のとお	りモバイ	ル端末を	借用・扌	寺出したい	いので、	許可願W	います。		
	所属	I				課・論	Ĕ				
	氏名										
	申請理	<u>曲</u>									
	借用希望	—————————————————————————————————————		年	月	F	~	年	月		E
	持出好	ti			······,						
	許可・不	許可年月日	#	可・不許可	Ţ	年		月、	Ħ		
A E	音 貸与	年月日,			年	月		Ħ			
	者 記 入 貸与諸 欄	行期間		年	月	B	~	年	月		Ħ
	モバイハ ※ 「MC2~」	レ端末番号 の端末時を記入	MC 2								
2	返去「確認 い	時 下のとお	 りエバイル	 し端末を	仮知いた	-1.+1+	ので	確認願い	 \\$-{}-		
	返却時確認事	<u>- シレ40</u> 項 モ	バイル端末本体	に作成した	ファイルの有	<u></u>	<u>、</u> 有		。 無	ŧ	
	返却年月日			4	手	 月		/ 日		<u>_</u>	
	受領者		労災	~ 【補償部労	災保険業務	务室 氏名					
×7		て使用すること]

10

.

··· ·

(別添)

۳,

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。



.

.

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	
1	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	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	知範囲	管理者 ※1	利用者 ※2
BIOSパスワード			0	0
pointsec(HDD暗号化)ID/パ	スワード		0	о ^к
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)	0	×
	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	0	0

※1 管理者列の「〇」は、本省から通知される。

※2 利用者列の「〇」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。



第6 管理者による設定





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。

			56	C		
* * 711		<u>+1+ *+</u>	<u>v : e s</u>	<u>. 6 h f i</u>	<u> </u>	7
RADOTA	するためのコ	2-#102/120	>+*&>+UC	Vean.		
ユーザID: パスワード:	[,	0K 1120-113	ŒQ
L.	٦	المدر الم		and the second se	¢	J

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。

	RSA SecuriD [®] for Microsoft [®] Windo		r iD® rosoft* Window	with RSA* Security Center
	-			e Copyright 2005 RSA Security Inc.
RSA Sec 場合は、I	urID PAS PASSCOD	SCODE を使用 E の代わりに \	用してログオンします。 Windows パスワード	RSA SecurID トークンが発行されていない を使用します。
RSA Sec 場合は、I RSA Sec ユーザ名(urID PAS PASSCOD urID を初ば (い):	SCODE を使用 E の代わりにい めて使用する均 localmanager	用してログオンします。 Windows パスワード3 易合は、[ヘルプ] をク! 0100	RSA SecurID トークンが発行されていない を使用します。 リックして使い方を参照してください。

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(<u>Q</u>)」を選択する。



管理者





(管理者)

■ 自動更新クライアント X明	
均示表 么	いるデータはありません。
· · · · · · · · · · · · · · · · · · ·	
ウィルス対策ソフト	· · · · · · · · · · · · · · · · · · ·
Distributed Antivirus Corporate Edition 10,1	起動力で有しています。 ロフルカイナ (Seith (力からわでつ)
	パターンファイル更新指示を行いました。
	リアルタイム保護は既に有効に設定されています。
ف	セキュリティチェックで対象拡張子に関する警告が発生してい、
■ ファイアウォールソフト	
对象	1 2019月
お元表 化	1.るデータはありません。

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。



^{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。





OK

Cancel

Help

. .



管理者

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。

Login:	localmanager_010	0		
PASSCODE:				
ОК	Cancel He	ip		
				PASSCODE欄に入

h Ra	6A Auth	entica	ation b	lanager	6 1.1 Ada	nnistra	tion r	nobile_de	ma01				
Ede	System	<u>U</u> ser	Joken	Group	Agent Host	<u>R</u> ealm	Site	Radius	Fot	Report	Help		
		Add	User_										
¢	MG26E	Coc	i, Licer										
c	MG260	Let	Usere 11 Tuis										
		Dek	ete User	195 19 9029 S. .	~							•	
		. DA	ili içarı		,								
PT 3	hilere h												
	warn o	etore	cnanç	ing coi	nection								
					· • • • • • • • • • • • • •							 	· <u></u> ,.

「
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。

Select User by: 「First name 」「Last name 」「Default login 管理者による設定 利用者による設定 モムズ化比提主の利用	• •
管理者による設定 「First name 「Last name 「Default login 100cdluser_0100_01] Currently selected user: First Name: Last Name: Default Login: 利用者による設定 1 1 1 1	• • •
管理者による設定 利用者による設定	· · ·
管理者による設定	. <u>.</u>
Currently selected dser: First Name: Last Name: Default Login:	
利用者による設定	
利用者による設定	
ニーモバイル端本の知用 1 パート・ション しょうしょう しょうしょう しょうしょう パート	
OK Cancel Help	
First and Last Name, Jocakuser 0100_01	
Default Login: localuser_0100_01	
Default Shell:	
C Local User C Remote User	
Serial Number Token Type/Auth With Status	
ickens:	•
O: Original token R: Replacement for previous token	
Rale: <none></none>	
Assigned Profile:	
For Enderson Processing Processing States and State States and States and	
Start Date: 01/01/1986 09:00 End Date: 01/01/1986 09:00	
P Alloved to Create a AN	
Assign Joken., ddf: Assigned Token., Administrative Role.	
Assign Joken Group Memberships	
Assign Joken Edit Assigned Toten Administrative Role Group Memberships Agent Host Activations Edit User Extension, Data Set/Change User Password Remove User Password Edit Access Times	
Assign Joken Edif Assigned Totlen Artministrative Role Group Memberships Agent Hoet Activations Edif User Extension, Quilit Set/Change User Paissword Remove User Paissword. Edit Access Timesti Assign Profile: Remove Crófile Assignment Delete User Vere DiAb Source: Vere DiAb Source Char Weinere Presented.	

OK Cancel Apply L/S Changes Set All L/S Help



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。





→ 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。



く管理者

管理者

First and Last Name		Nocalijser, 0100 0	
		. Iocalosol_0100_0	
Lietauit Login: Iocalus	er_uiuu_ui		
Default Shell:			a sa sa sa sa sa
CLocal User C Remote Use	r see see se	오늘옷은	성 1978 2019 성 2018 2019
Serial Number Tok	en Type/Auth With	Status	
Tokens: 000201245243 Key F	ob/Passcode Enable	d;New PIN Mode	
· · · · · · · · · · · · · · · · · · ·		*	
O: Original token R: R	eplacement for previous to	Ken	
Role: <none></none>			
Assigned Profile:			
T. Temporary User			
Start Date: 01/01/1986	09:00 End Date: 01/	01/1986 09:00	
R Allowed to Create a PIN	Required to	Create a PIN 😳	
Assign Token	Edit Assigned Token		mustrafive, Role
Group Memberships	Agent Host Activation	ns li (dit-U	ser Extension Data.
Set/Change User Password	Remove User Pasow	prid Edi	t Access Times
	Remove Profile Assian	mènt.	Delete User
Assign Profile	1		
Assign Profile View I.DAP Source	Mew Emergency Passoo	ide	Windows Password

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

PINの削除

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。 利用申請 1. モバイル端末をLAN接続状態で以下の設定を行う。 利用者 (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。) 管理者による設定 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。 利用者 ※入力したパスワードは無表示となる。 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 POWER-ON PASSWORD

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。

			S	ec		
14 17 1 7	2. u 1	1.6. 7.6	* . / *	<u></u>	<u>. t y</u>	
10~07~/	するための	コーザヨンパスワ	ንትをእታኒ	てください		
ユーザ取 バスワート:	[0 /(29-1	<u>s</u> t
				•		
167 ·	¥	196 201, 1988	8			

利用者



ユーザ名(U):

PASSCODE(P):

OK.

localuser_0100_01

キャンセル

•

ヘルプ(日)



. . . .

(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。

 利用申請
 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。

 管理者による設定
 ※入力したパスワードは無表示となる。

 利用者による設定
 POWER-ON PASSWORD

 PINの削除
 PINの削除

(_{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。

	Sec	
Stort C	/するためのつーザ加と/17ワードを入せして(だね、	? X
ユーザ ル パスワード:		xto
¥	t to a contract of a	

.





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。

 利用申請
 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。





PHS接続	に接続しています	
3	ユーザー名とパスワードを検証中	
	「キャンセル」	

Elles (c)

※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。







8. 結果画面が表示される。

(利用者)

Nosibit Hiventory Sub System	
ウィルス対策ソフト最適化結果	
免明	
	うるデータはありません。
···· ·· · · · · · · · · · · · · · · ·	•
ウィルス対策ソフト	•
- ウィルス対策ソフト 「象	· 我明
ウィルス対策ソフト す象 Symantec AntiVirus Corporate Edition 10.1	<u> 1 期 </u>
ウイルス対策ソフト 1象 Symantec AntiVirus Corporate Edition 10.1	<u>」 我明</u> 記動 だいます。 リアルタイム (保護は有効です。
ウイルス対策ソフト 操 Symantec AntiVirus Corporate Edition 10.1	<u>取明</u> 起動されています。 リアルタイム保護は有効です。 パターンファイル更新指示を行いました。
ウイルス対策ソフト 操 Symantec AntiVirus Corporate Edition 10.1	<u>説明</u> 記動されています。 リアルタイム(保護は有効です。 パターンファイル更新指示を行いました。 リアルタイム(保護は既に有効に設定されています。
ウイルス対策ソフト 1象 Symantec AntiVirus Corporate Edition 10.1	
ウィルス対策ソフト 1象 Symantec AntiVirus Corporate Edition 10.1	脱明 読むたれています。 リアルタイム(保護は有効です。 パターンファイル更新指示を行いました。 リアルタイム(保護は既に有効に設定されています。 セキュリティチェックで対象拡張子に関する警告が発生してい
ウイルス対策ソフト 気 Symantec AntiVirus Corporate Edition 10.1	IX0月 ご 記動されています。 リアルタイム(保護は有効です。 パターンファイル更新指示を行いました。 リアルタイム(保護は既に有効に設定されています。 セキュリティチェックで対象拡張子に関する警告が発生してい。 セキュリティチェックで対象拡張子に関する警告が発生してい。 ロー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
I ウイルス対策ソフト 「象 Sysmantec AntiVirus Corporate Edition 10.1 S D D コ I ファイアウォールソフト	IX9月 E動されています。 リアルタイム(保護は有効です。 パターンファイル更新指示を行いました。 リアルタイム(保護は既に有効に設定されています。 セキュリティチェックで対象拡張子に関する警告が発生してい

	セキュリティチェックで対象拡張子に関する警告が発生してい	•
ファイアウォールソフト		-
\$	<u>iXiii</u>	_
	⊥♪ 表示されるデータはありません。	
·		~ '

閉じる.

 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

 下要ファイルの削除

 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。

NOSIDE (nventory Sub System Agent Ag	Manager U. Kenton	· .	<u>, (C) × (</u>	
<u>برا مرد</u>	(Windows) (37/721-6)	現在3月1872年3月5日	時間6分長辺) はした。	~ るここを確認9る て
02144	状況 対象 セキュリティ情報	名		
	Ţ Ţ Ţ	示されるデータはありません。	-	
	Mindows Update	৫বেষ্ট্রেম &রেয়∺ছম		
ウィルス対策ソフトの最適化が売了しました。	······································			



(_{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。







•

【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 SecurlD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。)。

with RSA* Security Center

RSA SecuriDを使用してWindowsへのログオン

RSA SecuriD®

1

RSA SecurID PASSCODE を使用してログオンします。RSA SocurID トークンが発行されていない 場合は、PASSCODE の代分ガビ Windows レベワードを使用します。 RSA SocurID を初めて使用する場合は、「ヘルプ」をグリックして使い方を参照してだだい。 ユーザ名(型): [localuse_0100_01	
PASSCODE(9) ******* 	

16. 業務終了後は「TCS接続(KC)」のスタートメニューから「ロクオフ」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





このコンピュータに格納されているプロファイル(P):

MC260100001¥Administrator MC260100001¥Iocaluser (1100 01

ユーザー ブロファイル

名前



PINの削除

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。

[?|X

ここでは例として「localuser_0100_01」を使用する。

サイズ 種類

種類の変更の

新しいユーザー アカウントを作成するには、コントロール パネルの [ユーザー アカウント] を聞いてください。

121 MB ローカル ローカル 255 MB ローカル ローカル

削除(D)

OK

状態

変... ł

2008.. 2008

コピー先の

キャンセル



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。



Name of Primary RS	A Authentication M	lanager	
MG2600000001			
·····			<u> </u>
OK	Cancel	<u>H</u> elp	



^{管理者} 3. RSA SecurlD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。





> 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。



Select Token				X .
Serial Nu	nber: 201245243			
Select T	oken from List			
- Auto Sele	cf:			
Unassigr	ned Token Sor	ted by: C Toke	n Import Date	
		C Toke	n Expiration C	jer Jate
ОК		,Help		



管理者 6.「Clear PIN」ボタンをクリックする。 Key Fob with 6 digits, changing every 60 seconds. Algorithm is AES. Serial Number: 000201245243 Assigned to: localuser_0100_01 Next Tokencode Mode: Off Lost Status: Not Lost Last Login Date-(UTC): 12/02/2009 Finabled 08:50 Token Start Date: 03/07/2008 09:00 □ New PIN: model Token Shutdown Date: 07/31/2012 09:00 Token Assignment Date (UTC): 11/02/2009 08:16 Offline Auth. Expiration (UTC): 01/01/2010 23:59 User Authenticates With: @ Passcode C Tokencode Only Resynchronize Token ... Clear PIN Set PIN to Next Tokencode ... Edit Assigned User,... Assign Token... Unassign Token Delete Token Edit Lost Status... Edit Token Extension Data... Assign Replacement Token... Re-Issue Software Token... View Emergency Tokencode Help OK Cancel

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。



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。

*・ローカル ユーザーとグループ			, 新しいユーザー	(?)[X]
ファイル(ビ) 操作(ビ) 表示(ビ) へルブ(◆ → □ 回 回 国。 (ビ) 【 ローカル ユーザーとグルーブ (ローカル)	ゆ 名前 7ルネーム		ユーザー名(<u>U)</u> ; フル ネーム(F);	localuser_0100_01
	Administrator Guest HelpAssistant Remote Desktop Help As SUPPORT 38	コンピュータ/ドメインの管理 コンピュータ/ドメインへのゲ. リモート アシスタンスを提供 ヘルプンサポート サード20	说明(<u>D</u>):	
· · · · · · · · · · · · · · · · · · ·			パスワード(P): パスワードの確認入 ()) ユーザーは次回 () ユーザーは次回 () ユーザーはパスワ () アカウントを無効	、力(Q): ログナノ4和レバスワードの変更が45要(M) ワードを変更できない(S) 期度(する(Q) 均にする(Q)
	Station and the second se	<u></u>		(作成(5)) (閉じる(2))



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「MG26000001」を選択し、「OK」ボタンをクリックする。

	Select Server to Administer
	Name of Primary RSA Authentication Manager
. .	OK Cancel Help
> 3. RSA Secur	D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、モバイル語

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

Administrator Authentication	(X)
Login: localmanager_0100	
PASSCODE:	
OK Cancel Help	

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

ile System	Add User	Arent Hott	<u>R</u> ealm	Site	RADIUS	Lot	Report	Help	
ଜ MG260 ሮ MG260	j gun user j gap User j tri fotostan gefete Users j LOAP Ljors	- sa 							
	LUGER ISSUE	'							
₩arn b	efore changing c	onnection							

(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。

and a second
J_01
· · · · · · · · · · · · · · · · · · ·
VAuth With Status
<u></u>
nent for previous token:
End Date: 01/01/1986 09:00
Required to C cale a PIN
Adaptine Ir stive Role.
gent Host Activations Full User Extension Date
Edit Access Times
Edit Access Times anaze Mattile Assignment: Delate User

^{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。



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。

管理者

and the second	· · · · · · · · · · · · · · · · · · ·	
First and Last Name.		iser_0100_01
Default Login: loca	luser_0100_01	
Default Shell:	<u>an an an an ann an an ann an ann an an a</u>	a salada a sa a sa a sa a sa a sa a sa a
🕝 Local User 🔭 Remote U	Jšer	
Serial Number 1	Token Type/Auth With Sta	ntus
Tokens:		- <u>1</u>
O: Original foken R	Replacement for previous token	a a serie de la companya de la compa
Role: <none> Assigned Profile:</none>		
Primporary Uper		
Start Date: 01/01/1986	09:00 End Date: 01/01/198	6 09:00
	and the second	
Rectiliowed to Create a RIN	In Creat	е а.PIN
R: Allowed to Create a RN Assign Token.	Edir Assigned Token	é a filn Administrative. kole
R. Allowed to, Croate, a.RN Assign Token Group Memberships	Edir Assigned Totern Agent Host Activations.	e a.PIN Administrative. Kole Edit. User. Educosion Data,
P: Allowed to Create a RIN Assign Token Group Memberships SeVChange User Password.	Edit Assigned Token.	e ac ^P IN Administrative: Kole Edit User Eduction Data Edit Access Times.
R. Allowed to Croate a.RN Assign Token Group Meinberships Sel/Change User Password. Assign Profile	Agent Host Activations Agent Host Activations Remove User Reserved	e a.Bh Administrative. Kole Edit User, Edunsion Data Edit Access Times Defoto User

OKを決すと、追加する利用言を 自然が自己する心気タループに追 加するかの多イアロクが出るので 「YES」とする。

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。



 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。

Edit User			
First and Last Name:	localus	ær_0100_01	
Default Login: localuse	r_0100_01	· .	
Default Shell:	· · ·		
🦷 🤄 Local User 🦿 Remote User		·	7
Tokens 000201245243 Key Fo	T, Alt with Oto W/Passcode Enabled		
U: Uriginal token K: Ke	placement for previous token		
Role: <none></none>			
Assigned Profile:			
🗂 Temporary User		Å	
Start Date: 01/01/1986 0	19:00 End Date: 01/01/1986	3 09 : 00	
🕫 Allowed to Create a PIN	🕫 Required to Create	a PIN	
Assign Token	Edit Assigned Token	Administrative Role	
Group Memberships	Agent Host Activations	Edit User Extension Data.	
Set/Change User Password	Remove User Password	Edit Access Times	
Assign Profile,	Remove Profile Assignment	Delete User	
View LDAP Source	View Emergency Passcode	Clear Windows Password	1
OK Cancel Apply L/S	Schanges Set All U/S	Help	

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。

t Taken	
Key Fob with 6 digits, changing every 60 seco	nds. Algorithm is AES.
Serial Number: 000201245243	
Assigned to: localuser_0100_01	
Next Tokencode Mode: Off	
	· · ·
Lost Status: Not Lost	、
	
Last Login Date (UTC): 12/02/2009	08:50 F Enabled
Token Start Date: 03/07/2008	09:00
Token Shutdown Date: 07/31/2012	09:00 T New PIN mode
Token Assignment Date (UTC): 11/02/2009	D8:16
Offline Auth. Expiration (UTC): 01/01/2010 .	23:59
User Authenticates With: 🤗 Passcode	C Tokencode Only
Resynchronize Token	Clear PIN
Set PIN to Next Tokencode	Edit Assigned User
Assign Token	Unassign Token
Deiete Token	Edit Lost Status
Edit Token Extension Data	Assign Replacement Token
Re-Issue Software Token	View Emergency Tokencode.,,
OK	Help

.

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。

.

17 3	問いるより内容(仕執)	作業分担			
- 現金	同い合わせ内谷(抜件)	管理者	運用業者(ヘルプデスク)		
1	BIOSパスワード忘れ	0	_		
2	PointsecのID及びパスワード忘れ	0	<u> </u>		
3	RSA SecurIDのID忘れ	0	_		
4	PIN忘れ、RSA SecurlDロック (PIN初期化依頼、ロック解除依頼)	0	—		
5	ダイヤルアップできない(故障、ロック)	_	0		

· · · ·

-