IBM Client Security Software デプロイメント・ガイド バージョン 5.4.0

更新日: 2004年11月18日

ご注意！

本書および本書で紹介する製品をご使用になる前に、『特記事項』に記載されている情報をお読みください。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原 典：	IBM Client Security Software Deployment Guide Version 5.4.0
発 行：	日本アイ・ビー・エム株式会社
担 当：	ナショナル・ランゲージ・サポート

第1刷 2004.12

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、
平成角ゴシック体™W3、平成角ゴシック体™W5、平成角ゴシック体™W7

© Copyright International Business Machines Corporation 2004. All rights reserved.

© Copyright IBM Japan 2004

まえがき

IBM® Client Security Software をデプロイする際、IT 管理者は多数の要素を理解し、計画をたてる必要があります。本書は、エンベデッド・セキュリティー・チップまたは Client Security Software の使用法について説明するものではありません。本書は、企業全体でエンベデッド・セキュリティー・チップを搭載したコンピューターにソフトウェアをデプロイする方法に関するガイドです。

対象読者

本書は、IT 管理者、または社内のコンピューターへの IBM Client Security Software バージョン 5.4 のデプロイメントの責任者を対象にしています。本書は、1 台または複数のコンピューターに IBM Client Security Software をインストールする際に必要な情報を提供します。この資料を参照する前に、「*IBM Client Security Software バージョン 5.4 管理者およびユーザー・ガイド*」を参照することをお勧めします。IBM は、アプリケーションの使用に関する情報として、「*IBM Client Security Software バージョン 5.4 管理者およびユーザー・ガイド*」とアプリケーション・ヘルプを用意しています。

製品の資料

Client Security Software バージョン 5.4 ライブラリーでは、以下の資料を入手することができます。

- *Client Security Software Version 5.4 管理者およびユーザー・ガイド*,

  Client Security Software のセキュリティー機能のセットアップおよび使用に関する情報に加え、 UVM ログオン・プロテクションの使用、Client Security スクリーン・セーバーのセットアップ、ディジタル証明書の作成、ユーザー構成ユーティリティーの使用など、Client Security Software で実行するタスクが記載されています。

- *Client Security Software バージョン 5.4 インストール・ガイド*

  IBM エンベデッド・セキュリティー・チップが装着されている IBM パーソナル・コンピューターへの Client Security Software のインストールについて記載されています。

その他の情報

追加の情報およびセキュリティー製品の更新が提供されている場合、IBM Web サイト (http://www.ibm.com/jp/pc/security/index.shtml) から入手できます。

© Copyright IBM Corp. 2004

目次

© Copyright IBM Corp. 2004

第 1 章 IBM Client Security Software のデプロイメント前の考慮事項

IBM Client Security Software バージョン 5.4.0 の一元的なデプロイメントは、IBM Client Security Software セットアップ・ウィザードの「拡張構成モード (Advanced Configuration Mode)」で実行できます。 IBM Client Security Software バージョン 5.4 は第 1 世代のセキュリティー・チップ (非 TCPA) をサポートしません。これらのシステムのユーザーは、Client Security Software バージョン 5.3 をご使用ください。

IBM Client Security Software (CSS) をデプロイするには、さまざまな方法があります。IBM Client Security Software は、IBM パーソナル・コンピューターに統合された IBM エンベデッド・セキュリティー・チップを使用します。本書は、お客様の環境における IBM エンベデット・セキュリティー・サブシステム (ESS) のデプロイメントの方法を決定する上で役立ちます。イメージ作成からエンド・ユーザーに PC を配布する方法まで、会社でコンピューターをデプロイするプロセスを検討することが重要です。このプロセスは、お客様の会社における ESS のデプロイメントの方法に多大な影響を与えます。IBM ESS は、図 1 のとおり 2 つの基本要素で構成されています。

1. Client Security Software
2. エンベデッド・セキュリティー・チップ

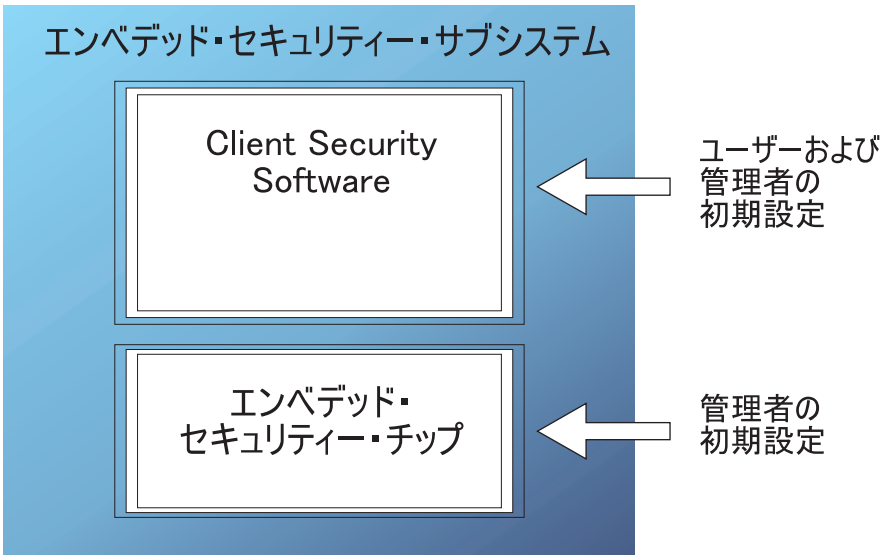

図 1. IBM Client Security System コンポーネント

© Copyright IBM Corp. 2004

デプロイメントの要件および仕様

IBM Client Security Software をエンベデッド・セキュリティー・チップ搭載のコンピューターにインストールすることを計画している場合、以下のサーバー・ストレージおよびダウンロードの要件、および設置時間について計画してください。

1. エンベデッド・セキュリティー・チップ搭載の IBM PC
2. インストール可能なコードのサーバー・ストレージ要件: およそ 20 MB
3. 各ユーザーの鍵アーカイブ・データに必要なサーバー・ストレージは、アーカイブを保存するユーザーごとに平均 200 KB です。

第 2 章 Client Security Software のインストール

この章では、Client Security Software をインストールするための 2 つの方法 (標準インストールと管理インストール) について説明します。

標準インストール

css540jp.exe ファイルは自己解凍型のインストール・パッケージであり、このファイルを実行するとインストール用のソース・ファイルが抽出され、インストールが開始されます。このファイルには、以下に説明する一連のコマンド行パラメーターを指定できます。パラメーターを必要とするコマンド行オプションは、オプションとパラメーターの間にスペースを入れずに指定する必要があります。たとえば、`css540jp.exe /s /v"/qn REBOOT="R""` は有効ですが、`css540jp.exe /s /v "/qn REBOOT="R""` は無効です (**“/qn REBOOT=”R””** はオプション **/v** のパラメーターです)。オプションのパラメーターにスペースが含まれている場合のみ、パラメーターの前後に引用符が必要です。

パラメーターを指定せずに css540jp.exe を実行する場合のインストールのデフォルトの動作では、インストールの実行の際にユーザー・インターフェースが表示され、インストールの最後にリブートのためのプロンプトが表示されます。ユーザー・インターフェースを表示せずにインストールを実行する場合、デフォルトでインストールの最後にリブートが実行されます。しかし、上記の例のセクションで示したように、REBOOT プロパティーを指定することによって、リブートを遅らせることができます。

/a このパラメーターを指定すると、実行可能ファイルは管理インストールを実行します。管理インストールでは、ユーザーによって指定されたディレクトリーにデータ・ファイルがコピーされますが、ショートカットの作成、COM サーバーの登録、アンインストール・ログの作成は行われません。

/x

このパラメーターを指定すると、実行可能ファイルは以前にインストールされた製品をアンインストールします。

/s このパラメーターを指定すると、実行可能ファイルはサイレント・モードで実行します。

/v **/v** パラメーターを使用すると、コマンド行スイッチとパブリック・プロパティーの値を Msiexec.exe に渡します。

/w このパラメーターを使用すると、実行可能ファイルはインストールが完了するまで終了するのを待ちます。このパラメーターをバッチ・ファイルで使用する場合、実行可能ファイルのコマンド行引き数全体の前に `start /WAIT` を置いてください。この使用法の正しい形式の例は以下のとおりです。

```
start /WAIT css540jp.exe /w
```

© Copyright IBM Corp. 2004

管理インストール

Microsoft® Windows®のインストーラーを使用すると、ワークグループによる使用またはカスタマイズのために、ネットワークに対するアプリケーションまたは製品の管理インストールを行うことができます。 Client Security Software インストール・パッケージの場合、管理インストールはインストール・ソース・ファイルを指定の位置に抽出します。管理インストールを実行するには、以下に示すように **/a** パラメーターを使用して、セットアップ・パッケージをコマンド行から実行する必要があります。

```
css540jp.exe /a
```

新しい抽出位置を選択できます。それには、C: 以外のドライブ (ローカル・ドライブ、マップされたネットワーク・ドライブなど) が含まれます。さらに、新しいディレクトリーもこのステップで作成されます。

管理インストールがサイレント・モードで実行される場合、以下に示すようにパブリック・プロパティー TARGETDIR をコマンド行に設定して、抽出位置を指定できます。

```
Setup.exe /s /v"/qn TARGETDIR=F:¥IBMCSS"
```

または

```
msiexec.exe /i "IBM Client Security Software.msi" /qn TARGERDIR=F:¥IBMCSS
```

カスタマイズを行った後、アンパックされたソース・ファイルからインストールするには、コマンド行から msiexec.exe を呼び出します。 『コマンド行パラメーター』は、msiexec.exe の使用法にとともに、指定できるコマンド行パラメーターを紹介しています。さらに、パブリック・プロパティーも、msiexec コマンド行呼び出しに直接設定できます。

コマンド行パラメーター

/i *package* **または** *product*

製品をインストールするには、以下の形式を使用します。

```
msiexec /i "C:¥WindowsFfolder¥Profiles¥UserName¥Personal¥MySetups¥Othello¥Trial
Version¥Release¥DiskImages¥Disk1¥productOthello Beta.msi"
```

製品コードは、製品のプロジェクト・ビューの製品コード・プロパティーで自動的に生成される GUID を指します。

注: 上記の例は、ページに収めるために 2 行に分かれています。このコマンドを入力するときは、1 行で入力してください。

/a *package*

/a パラメーターを指定すると、管理者権限を持つユーザーがネットワークに製品をインストールできるようになります。

/x *package* **または** *product code*

このパラメーターは製品をアンインストールします。

/L [i|w|e|a|r|u|c|m|p|v|+] *logfile*

このパラメーターは、ログ・ファイルのパスを指定します。以下に示すフラグは、ログ・ファイルに記録する情報を指定します。

- **i**

  状況メッセージをログに記録します。
- **w**

  重要でない警告メッセージをログに記録します。
- **e**

  すべてのエラー・メッセージをログに記録します。
- **a**

  アクション・シーケンスの開始をログに記録します。
- **r**

  アクション固有のレコードをログに記録します。
- **u**

  ユーザー要求をログに記録します。
- **c**

  最初のユーザー・インターフェース・パラメーターをログに記録します。
- **m**

  メモリー不足メッセージをログに記録します。
- **p**

  端末設定をログに記録します。
- **v**

  詳細な出力設定をログに記録します。
- **+**

  既存のファイルに追加します。
- *****

  詳細な出力設定を除く、すべての情報をログに記録するようにするワイルドカード文字です。

/? または /h

どちらのコマンドも、Windowsインストーラーの著作権情報を表示します。

TRANSFORMS

TRANSFORMS コマンド行パラメーターを使用すると、基本パッケージに適用するトランスフォームを指定できます。コマンド行トランスフォーム呼び出しの例を以下に示します。

```
msiexec /i "C:¥WindowsFolder¥Profiles¥UserName¥Personal¥MySetups¥Project Name¥
Trial Version¥My Release-1¥DiskImages¥Disk1¥ProductName.msi"
TRANSFORMS="New Transform 1.mst"
```

複数のトランスフォームをセミコロンで分けることができるため、Windows インストーラー・サービスが誤って解釈しないように、トランスフォームの名前にセミコロンを使用しないようにお勧めします。

注: 上記の例は、ページに収めるために 3 行に分かれています。このコマンドを入力するときは、1 行で入力してください。

Properties

すべてのパブリック・プロパティーは、コマンド行から設定または変更できます。パブリック・プロパティーは、すべて大文字で記述されることによって私用プロパティーと区別されます。たとえば、COMPANYNAME はパブリック・プロパティーです。

コマンド行からプロパティーを設定するには、構文 PROPERTY=VALUE を使用します。*COMPANYNAME* の値を変更するには、以下のように入力します。

```
msiexec /i "C:¥WindowsFolder¥Profiles¥UserName¥Personal¥MySetups¥Project Name¥
Trial Version¥My Release-1¥DiskImages¥Disk1¥ProductName.msi"
COMPANYNAME="InstallShield"
```

注: 上記の例は、ページに収めるために 3 行に分かれています。このコマンドを入力するときは、1 行で入力してください。

Client Security Software カスタム・パブリック・プロパティー

Client Security Software のインストール・パッケージには、インストールの実行時にコマンド行に設定できる、一連のカスタム・パブリック・プロパティーが含まれています。現在使用可能なカスタム・パブリック・プロパティーは以下のとおりです。

INSTALLPWM

これは、最初のインストールの際に Password Manager をインストールするかどうかを制御するために使用されます。1 に設定すると Password Manager はインストールされ、0 に設定すると Password Manager はインストールされません。デフォルト値は 1 です。

CFGFILE

このプロパティーは、サイレント・インストールの際に構成ファイルの位置を指定するために使用されます。構成ファイルには、セキュリティー・チップの既存のパスワードの値を含めることができます。これにより、チップにすでにパスワードが設定されている場合でも、ユーザーの対話なしにインストールを完了することができます。例:

```
CFGFILE=C:¥csec.ini
```

Client Security Software インストール機能

Client Security Software One-Click Installation には、*Security* (IBM Client Security Software) と *PWManager* (IBM Password Manager) の 2 つの機能が用意されています。デフォルトでは両方の機能がインストールされますが、インストールを実行するためのオプションがいくつか用意されており、 Security 機能だけがインストールされるようにすることができます (Security 機能が必要であれば、PWManager 機能は必要ありません)。ユーザー・インターフェースを表示せずにインストールを実行するときに、IBM Password Manager バージョン 1.3 以下がインストールされてい

ない場合、 IBM Client Security Software だけをインストールするか、IBM Client Security Software と IBM Password Manager の両方をインストールするかを選択する画面が表示されます。ユーザー・インターフェースを表示しないでインストールを実行する (サイレント) 場合、INSTALLPWM プロパティーを使用することによって、Password Manager をインストールするかどうかを制御できます (0 に設定すると Password Manager はインストールされません)。ユーザーが最初のインストール時には IBM Client Security だけをインストールすることを選択し、後から IBM Password Manager を追加することにする場合は、元のソース・パッケージを再度実行することによって行うことができます。ユーザー・インターフェースを表示する設定でインストールを再度実行すると、メンテナンス画面が表示されます。Password Manager がインストールされていない場合には、この画面で「Modify」ボタンを選択できます。このボタンを選択すると、Client Security だけを再インストールするか、IBM Client Security Software とIBM Password Manager の両方をインストールするように変更するかを選択できる画面が表示されます。ユーザーは、ソースからユーザー・インターフェースを表示せずに製品を再インストールして、IBM Password Manager を追加することもできます。これを行うコマンドの例を以下に示します。

Setup.exe の使用例

表 1 は css540jp.exe を使用したインストールの例を示しています。

表 1. css540jp.exe を使用したインストールの例

タイプ	例
サイレント・インストール (リブートし、インストールが終了する)	`css540jp.exe /s /v/qn`
サイレント・インストール (リブートなし)	`css540jp.exe /s /v"/qn REBOOT="R""`
サイレント・インストール (リブートなし、Password Manager はインストールされない)	`css540jp.exe /s /v"/qn REBOOT="R" INSTALLPWM=0"`
サイレント・インストール (リブートなし、インストール・ディレクトリーを指定)	`css540jp.exe /s /v"/qn REBOOT="R" INSTALLDIR=C:¥ibmcss"`
サイレント・インストール (リブートなし、構成ファイルを指定)	`css540jp.exe /s /v"/qn REBOOT="R" CFGFILE=C:¥csec.ini"`
サイレント管理インストール	`css540jp.exe /a`
サイレント管理インストール (抽出場所を指定)	`css540jp.exe /a /s /v"/qn TARGETDIR="F:¥CSS""`
インストール (リブートなし、インストール・ログを temp ディレクトリーに作成)	`css540jp.exe /v"REBOOT="R" /L*v %temp%¥css.log"`
Password Manager を追加するための製品のサイレント再インストール	`css540jp.exe /s /v"/qn ADDLOCAL=PWManager"`

表 2 は msiexec.exe を使用したインストールの例を示しています。

表 2. msiexec.exe を使用したインストール

タイプ	例
インストール (ログ・ファイルを作成)	`msiexec /i "C:¥IBM Client Security Software.msi" /L*v %temp%¥css.log`

表 2. *msiexec.exe* を使用したインストール *(続き)*

タイプ	例
サイレント・インストール (リブートなし)	`msiexec /i "C:¥IBM Client Security Software.msi" /qn REBOOT="R"`
サイレント・インストール (リブートなし、Password Manager はインストールされない)	`msiexec /i "C:¥IBM Client Security Software.msi" /qn REBOOT="R" INSTALLPWM=0`
Password Manager を追加するための製品のサイレント再インストール	`msiexec /i "C:¥IBM Client Security Software.msi" /qn ADDLOCAL=PWManager`

第 3 章 エンベデッド・セキュリティー・チップの機能

IBM エンベデッド・セキュリティー・チップの構図は図 2 のとおりです。3 つの主要なコンポーネントがあります。

1. 管理者パスワード
2. ハードウェア公開鍵
3. ハードウェア秘密鍵

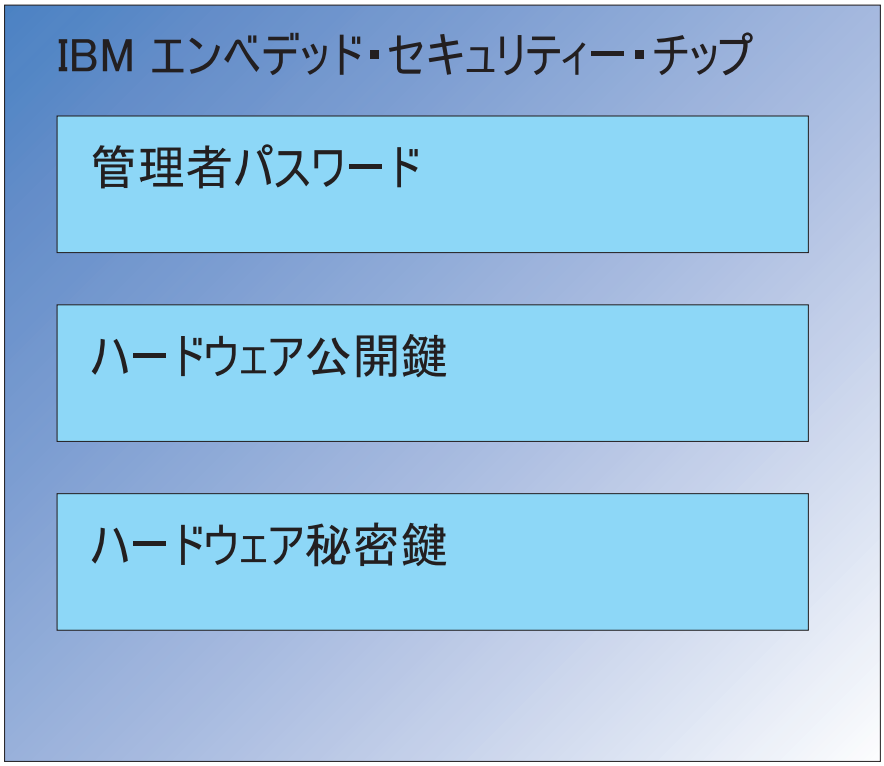

図 2. IBM エンベデッド・セキュリティー・チップに保持されるデータ

ハードウェアの公開鍵および秘密鍵は、各コンピューターごとに固有です。ハードウェア秘密鍵がチップから抽出されることは決してありません。新しい鍵ペアは、以下のいずれかの方法で作成することができます。

- Client Security Software ウィザードによって
- 管理者ユーティリティーによって
- スクリプトを使用して

ハードウェア鍵はチップから抽出することはできません。

管理者は、管理者パスワードを使用して、以下の機能にアクセスします。

- ユーザーの追加
- セキュリティー・ポリシーの設定
- パスフレーズ・ポリシーの設定

© Copyright IBM Corp. 2004

- スマートカードの登録
- バイオメトリック認証デバイスの登録

たとえば、管理者は追加ユーザーがエンベデッド・セキュリティー・チップの機構および機能を利用できるようにしなければならない場合があります。管理者パスワードは、Client Security Software のインストール時に設定されます。管理者パスワードが設定される方法およびタイミングについて詳しくは、本書で後ほど説明します。

重要: ESS を最初に構成する際に設定する管理者パスワードを保守する計画を作成してください。IT 管理者またはセキュリティー管理者が、エンベデッド・セキュリティー・チップを装備した各コンピューターに同じ管理者パスワードを設定するように決定する場合、そのように設定することも可能です。または、それぞれの部門またはビルごとに異なる管理者パスワードを割り当てることも可能です。

IBM エンベデッド・セキュリティー・チップの他のコンポーネントは、ハードウェア公開鍵およびハードウェア秘密鍵です。この RSA 鍵ペアは、Client Security Software の構成時に生成されます。

各コンピューターには、固有のハードウェア公開鍵および固有の秘密鍵があります。IBM エンベデッド・セキュリティー・チップの乱数機能によって、それぞれのハードウェア鍵ペアは統計的に固有であることが保証されます。

11 ページの図 3 は、IBM エンベデッド・セキュリティー・チップの 2 つの追加コンポーネントを示しています。IBM エンベデッド・セキュリティー・サブシステム・インフラストラクチャーを効果的に管理するには、これら 2 つのコンポーネントについて理解する必要があります。 11 ページの図 3 は、管理者公開鍵と秘密鍵、およびユーザー公開鍵と秘密鍵を示しています。以下に、公開鍵および秘密鍵の概要を示します。

- 公開鍵および秘密鍵は、「鍵ペア」とみなされます。
- 秘密鍵および公開鍵は、以下のように数学的に関連しています。
  - 公開鍵で暗号化された内容は、秘密鍵でしか復号化できません。
  - 秘密鍵で暗号化された内容は、公開鍵でしか復号化できません。
  - 秘密鍵を知っていても、公開鍵を引き出すことはできません。
  - 公開鍵を知っていても、秘密鍵を派生させることはできません。
  - 通常、公開鍵は全員が使用できます。
- 秘密鍵は、確実に保護してください。
- 公開鍵と秘密鍵は、公開鍵インフラストラクチャー (PKI) の基盤です。

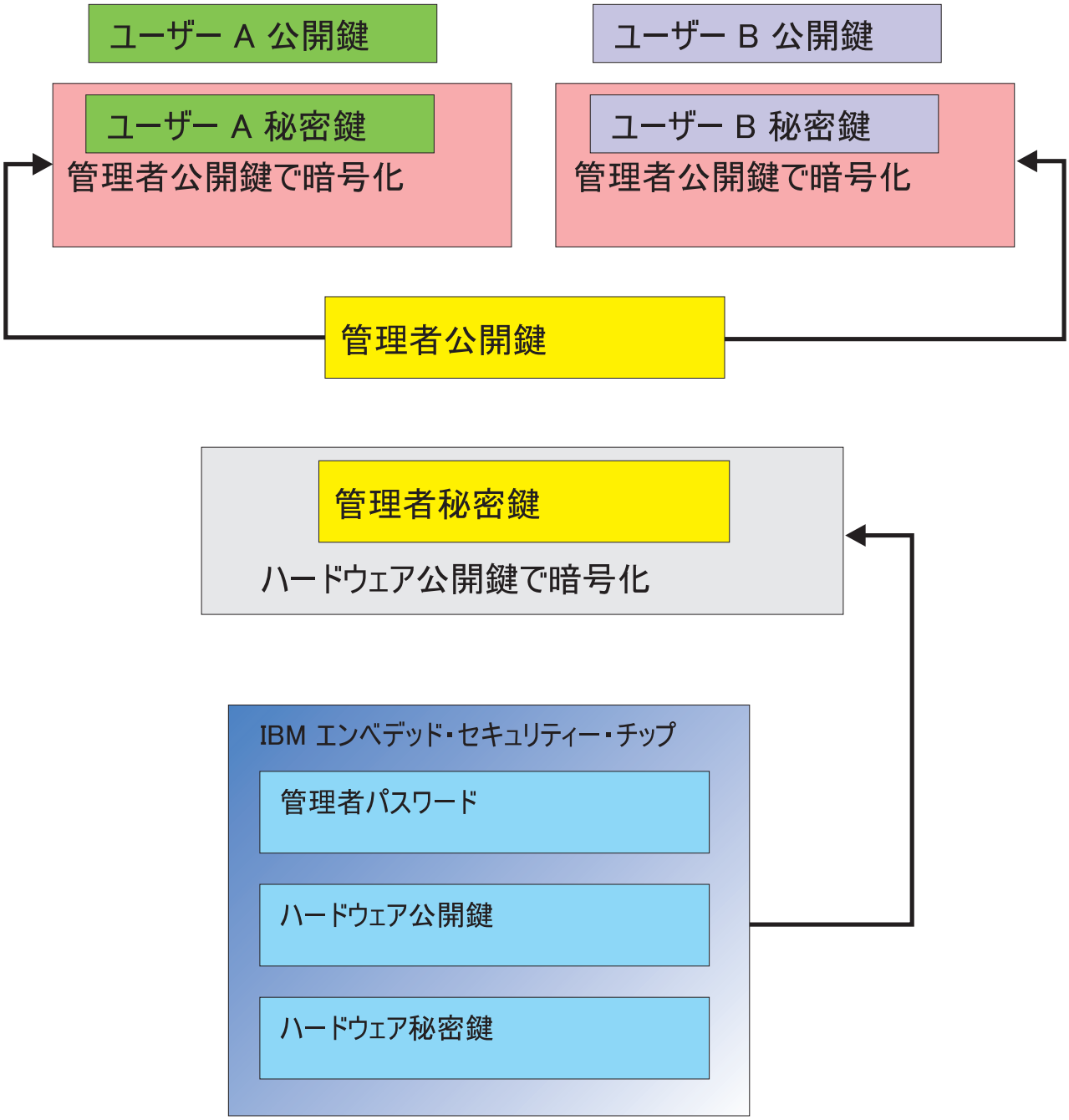

図 3. 複数の暗号化レイヤーによる強固なセキュリティー

鍵交換階層

IBM ESS アーキテクチャーの基本要素は、「鍵スワッピング」階層です。この機能の正確な詳細は「*IBM Client Security Software 管理者およびユーザー・ガイド*」で説明されていますが、ここでは、マス・デプロイメントによる設定、デプロイメント、および管理に適用される概念を紹介します。図 3 は、ハードウェア公開鍵およびハードウェア秘密鍵を示しています。前述したように、これらの鍵は Client Security Software により作成され、各クライアントごとに統計的に固有なもので

す。IBM エンベデッド・セキュリティー・チップの上に、管理者公開鍵と秘密鍵のペアが置かれています。管理者公開鍵および秘密鍵のペアは、各コンピューターごとに固有にすることも、またはすべてのクライアントまたはクライアントのサブセットに対して同一にすることもできます。利点および欠点は、本書で後ほど説明します。管理者公開鍵および秘密鍵は、次の操作を実行します。

- ユーザーの公開鍵および秘密鍵を保護する
- ユーザーの証明書のアーカイブおよびリストアを使用可能にする
- 「*IBM Client Security Software 管理者およびユーザー・ガイド*」に説明されているユーザー・クレデンシャル・ローミングを使用可能にする

なぜ鍵交換なのか?

以下のセクションでは、IBM ESS 環境のユーザーについて説明します。これらのユーザーを受け入れるために IBM Client Security Software および ESS をセットアップする方法について説明します。この場合、端的に説明すると、各ユーザーは公開鍵および秘密鍵を持っています。ユーザーの秘密鍵は、管理者公開鍵で暗号化されています。 11 ページの図 3 では、管理者秘密鍵がハードウェア公開鍵によって暗号化されていました。これらのさまざまな秘密鍵をわざわざ暗号化するのはなぜでしょうか?

その理由は、前述した階層にあります。IBM エンベデッド・セキュリティー・チップのストレージ・スペースには限りがあるため、どの時点でも、チップ内に置くことができる鍵の数には限界があります。このシナリオで、ハードウェア公開鍵および秘密鍵のみが永続的な (ブートからブートまでの) 鍵です。複数の鍵と複数のユーザーを使用可能にするために、IBM ESS は、鍵のスワッピング階層を実装します。鍵が必要になると、その鍵は IBM エンベデッド・セキュリティー・チップに「スワッピング」されます。暗号化された秘密鍵をチップに交換することにより、秘密鍵は復号化され、チップの保護された環境においてのみ使用されます。

管理者秘密鍵は、ハードウェア公開鍵で暗号化されます。ハードウェア秘密鍵は、チップ内でのみ使用でき、管理者秘密鍵を復号化するために使用されます。管理者秘密鍵がチップで復号化された後、ユーザーの秘密鍵 (管理者公開鍵で暗号化される) は、ハードディスクからチップへ受け渡され、管理者秘密鍵で復号化されます。 11 ページの図 3 では、複数のユーザー秘密鍵が管理者公開鍵によって暗号化されています。このように IBM ESS を使用すると、1 台のコンピューターに最大 100 人のユーザーをセットアップすることができます。

第 4 章 鍵のアーカイブに関する考慮事項

パスワードと鍵は、他のオプションの認証装置とも連動しながら、システム・ユーザーを認証します。

14 ページの図 4 は、IBM エンベデッド・セキュリティー・サブシステムと Client Security Software の連携を示したものです。Windows のログオンでは、ユーザー A がログオンするためのプロンプトが出され、ユーザー A はその指示に従ってログオンします。IBM Client Security System は、オペレーティング・システムが提供する情報に基づいて、現在のユーザーがだれかを判別します。ハードウェア公開鍵により暗号化された管理者秘密鍵が、エンベデッド・セキュリティー・チップにロードされます。

© Copyright IBM Corp. 2004

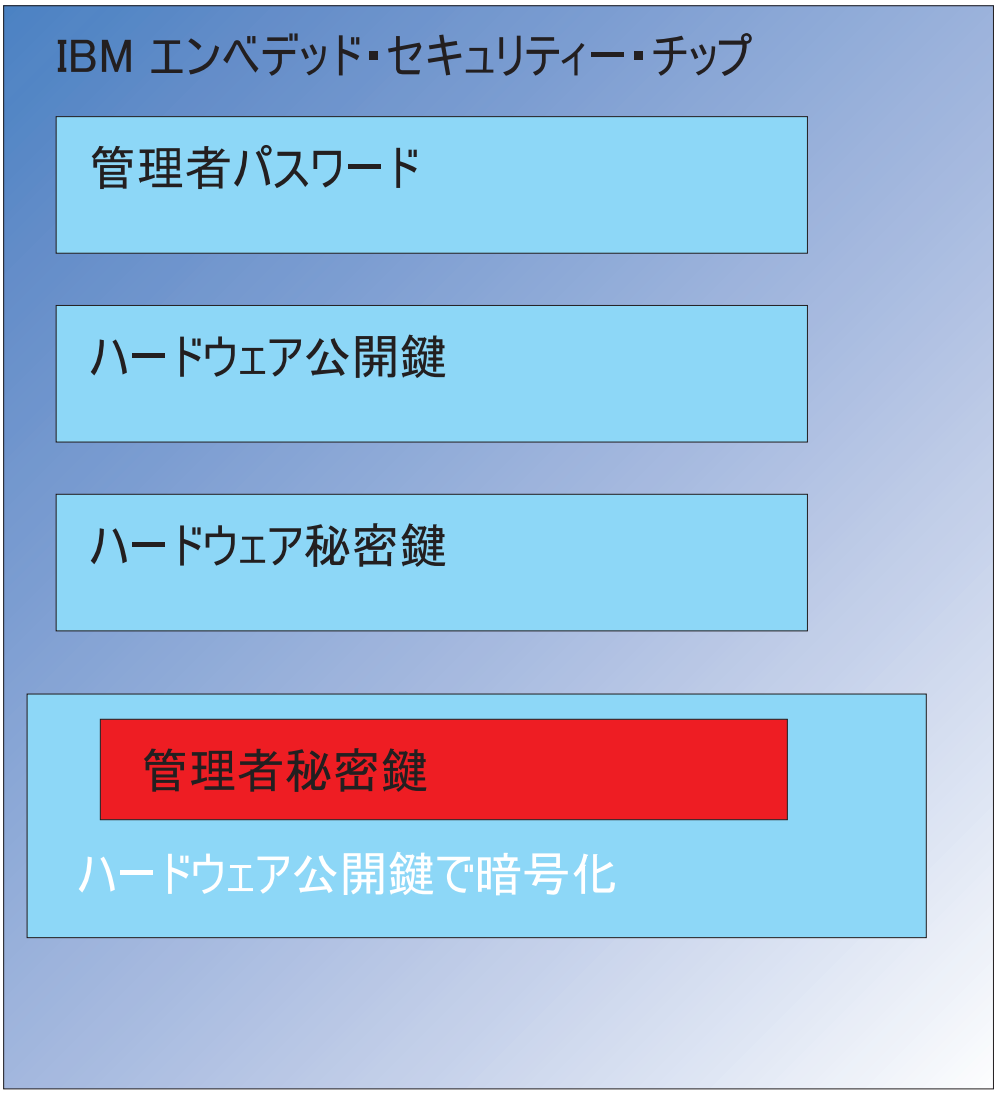

図 4. ハードウェア公開鍵により暗号化された管理者秘密鍵が、エンベデッド・セキュリティー・チップにロードされる

ハードウェア秘密鍵 (チップ内でのみ使用可能) は、管理者秘密鍵を復号化します。これで、管理者秘密鍵をチップで使用できます (15 ページの図 5 をご覧ください)。

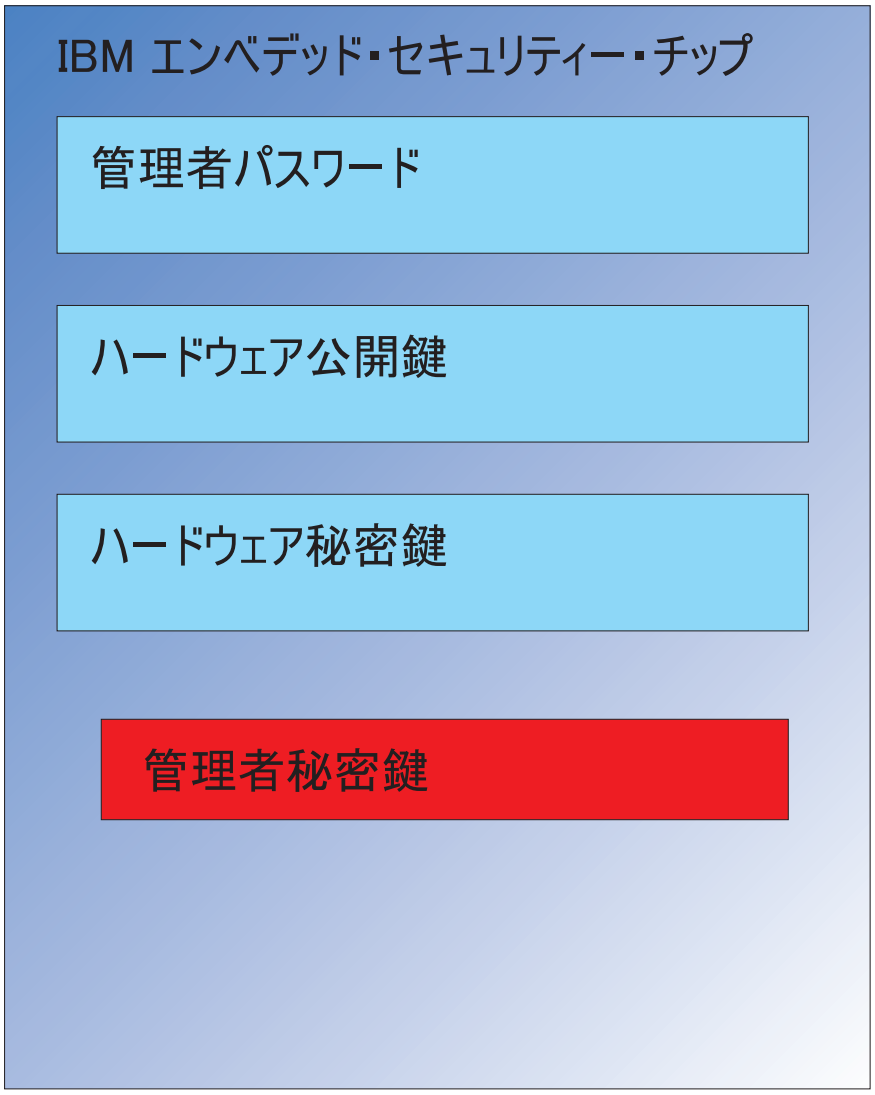

図 5. 管理者秘密鍵をセキュリティー・チップで使用できる。

ユーザー A はコンピューターにログオンしているため、ユーザー A の秘密鍵 (管理者公開鍵で暗号化) がチップに渡されます。 16 ページの図 6 をご覧ください。

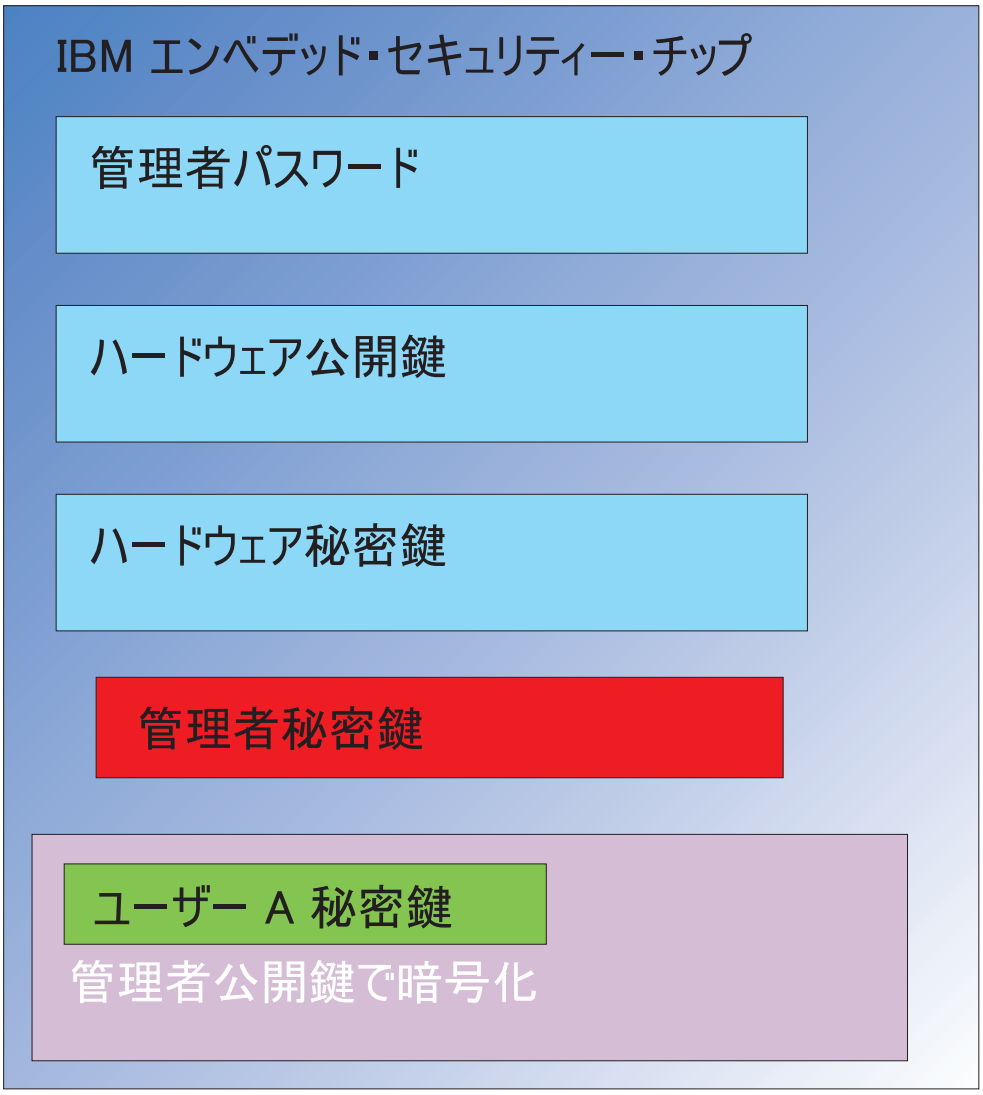

図 6. 管理者公開鍵で暗号化されているユーザー A の秘密鍵が、セキュリティー・チップに受け渡される。

管理者秘密鍵が、ユーザー A の秘密鍵を復号化するために使用されます。これで、ユーザー A の秘密鍵が使用可能になります。 17 ページの図 7 をご覧ください。

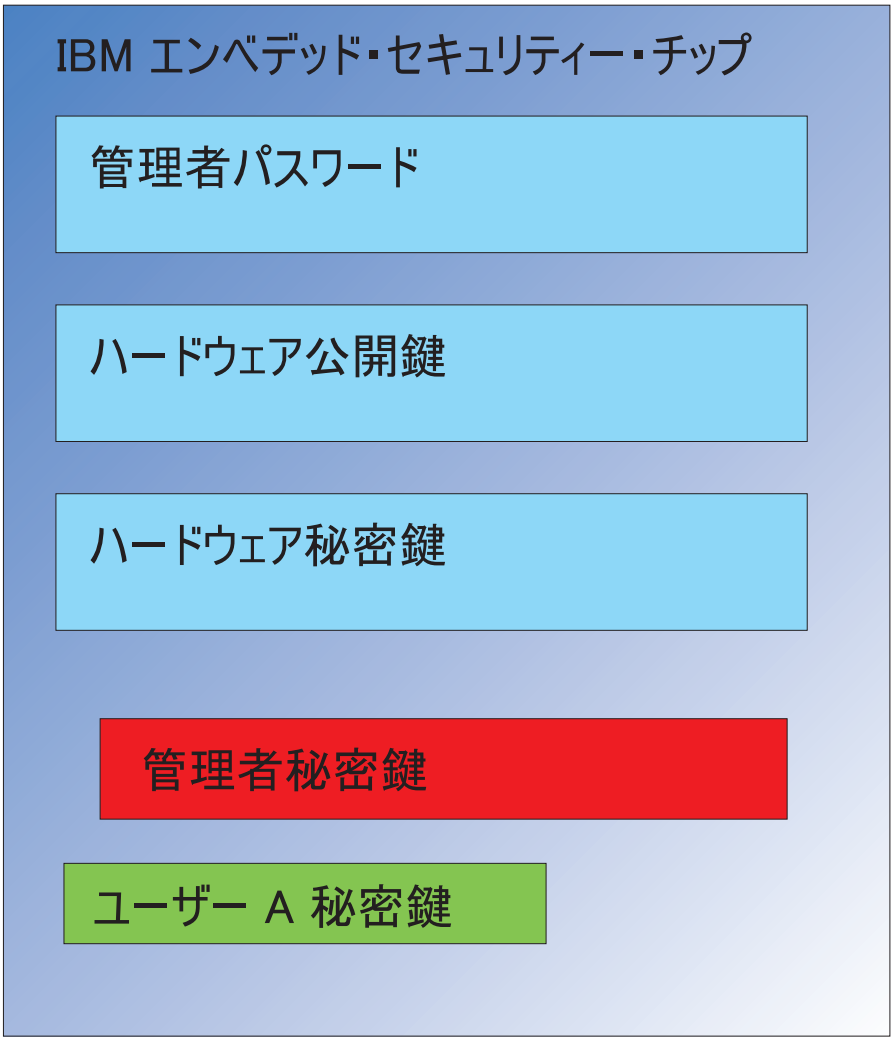

図 7. ユーザー A の秘密鍵を使用する準備ができた。

ユーザー A の公開鍵で暗号化できる鍵は、この他にいくつかあります。一例として、電子メールの署名に使用される秘密鍵があります。ユーザー A が署名付き電子メールを送信する場合、署名に使用される秘密鍵 (ユーザー A の公開鍵で暗号化されている) がチップに受け渡されます。ユーザー A の秘密鍵 (既にチップ内にある) は、ユーザー A の秘密署名鍵を復号化します。これで、ユーザー A の秘密署名鍵を希望の操作を実行するためにチップで使用できるようになります。この場合は、ディジタル署名の作成 (ハッシュの暗号化) です。ユーザー B がコンピューターにログオンする場合も、鍵をチップの内外に移動するために同じプロセスが使用されることに注意してください。

なぜ管理者鍵ペアなのか?

管理者鍵ペアを使用する主な理由は、アーカイブ機能と復元機能を利用できることです。管理者鍵ペアは、チップとユーザー証明書との間の抽象化層として機能します。ユーザー固有の秘密鍵情報は、管理者公開鍵を使用して暗号化されます。 18 ページの図 8 をご覧ください。

重要: 管理者鍵ペアを保守する計画を作成してください。IT 管理者またはセキュリティー管理者が、エンベデッド・セキュリティー・チップ搭載の各コンピューターごとに同じ管理者鍵ペアを使用するように決定する場合、そのように設定することも可能です。または、各部門またはビルごとに異なる管理者鍵ペアを割り当てることも可能です。

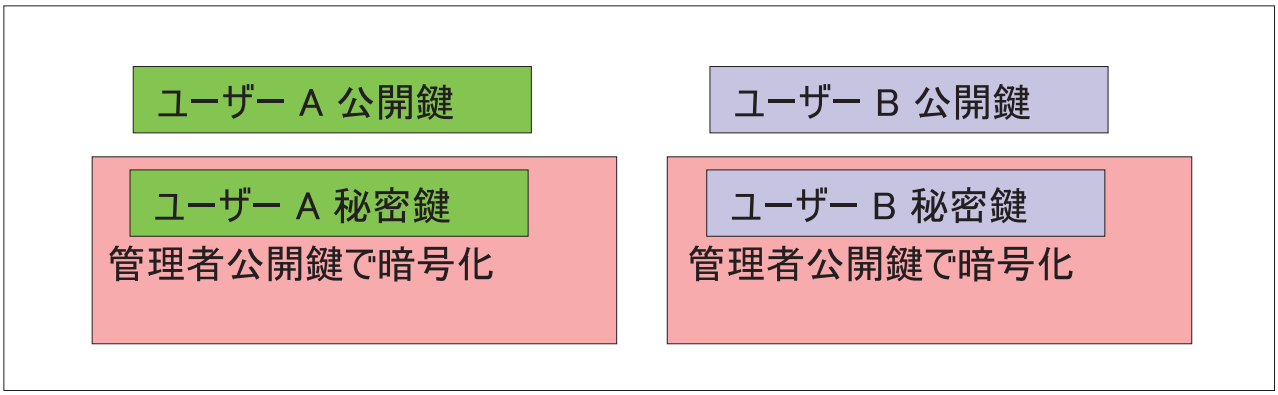

図 8. ユーザー固有の秘密鍵情報は、管理者公開鍵で暗号化される。

管理者鍵ペアを使用する別の理由は、クライアント・セキュリティー・ポリシー・ファイルに署名して、管理者以外のユーザーがセキュリティー・ポリシーを変更するのを防ぐためです。クライアント・セキュリティー・ポリシー・ファイルの高度なセキュリティーを実現するために、管理者秘密鍵を最大 5 人に分割することができます。そのような場合、クライアント・セキュリティー・ポリシー・ファイルなどのファイルを署名して暗号化するには、秘密鍵の一部を保持する 5 人の全員が揃う必要があります。これにより、1 人が一方的に管理者機能を実行することを防ぎます。管理者秘密鍵の分割については、42 ページの表 6 の Keysplit=1 設定を参照してください。

IBM Client Security Software の初期設定では、管理者鍵ペアはソフトウェアによって作成されるか、外部ファイルからインポートされます。共通の管理者鍵ペアを使用する場合、クライアントのインストール時に必要なファイルの場所を指定します。

図 8 のとおり、このユーザー固有の情報は、管理者が定義したアーカイブ・ロケーションにバックアップ (書き出し) されます。このアーカイブ・ロケーションには、クライアントと物理的または論理的に接続されている任意のタイプのメディアを指定できます。このアーカイブ・ロケーションに関する最良実例については、IBM Client Security System のインストールに関するセクションで説明します。

管理者公開鍵および秘密鍵はアーカイブされません。アーカイブの場所にあるユーザー・データは、管理者公開鍵で暗号化されます。ユーザー・アーカイブ・データのみを持っていても、管理者秘密鍵がなければデータを復号化できません。管理者の公開鍵と秘密鍵は、IBM Client Security Software 資料では、「アーカイブ鍵ペア」と呼ばれています。秘密鍵は暗号化されない点にご注意ください。アーカイブ鍵ペアを保管および保護するときは、特別な注意が必要です。

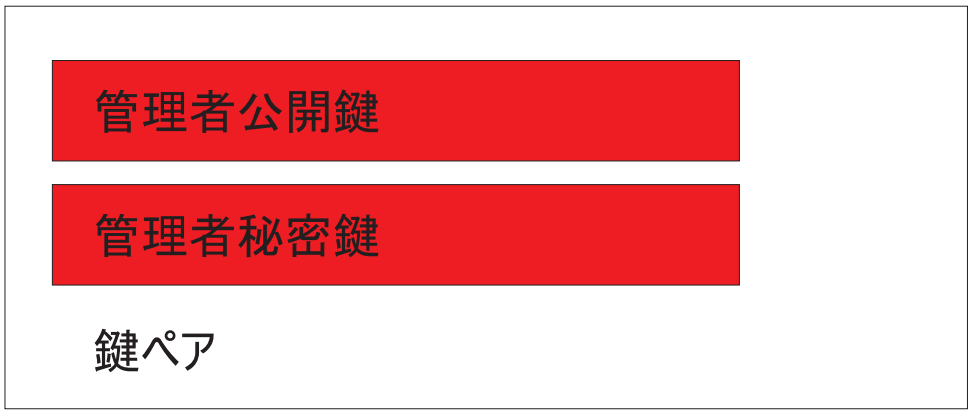

図 9. アーカイブ鍵ペアは管理者公開鍵と秘密鍵で構成される

前述したように、管理者公開鍵および秘密鍵の最も重要な機能は、ディスクの内容のバックアップと復元です。この機能は、10 から15 で示されています。ステップは次のとおりです。

1. クライアント A が、何らかの理由でユーザー A で使用不可になりました。この例では、クライアント A、つまりコンピューターが落雷の影響を受けたとします。 20 ページの図 10 をご覧ください。

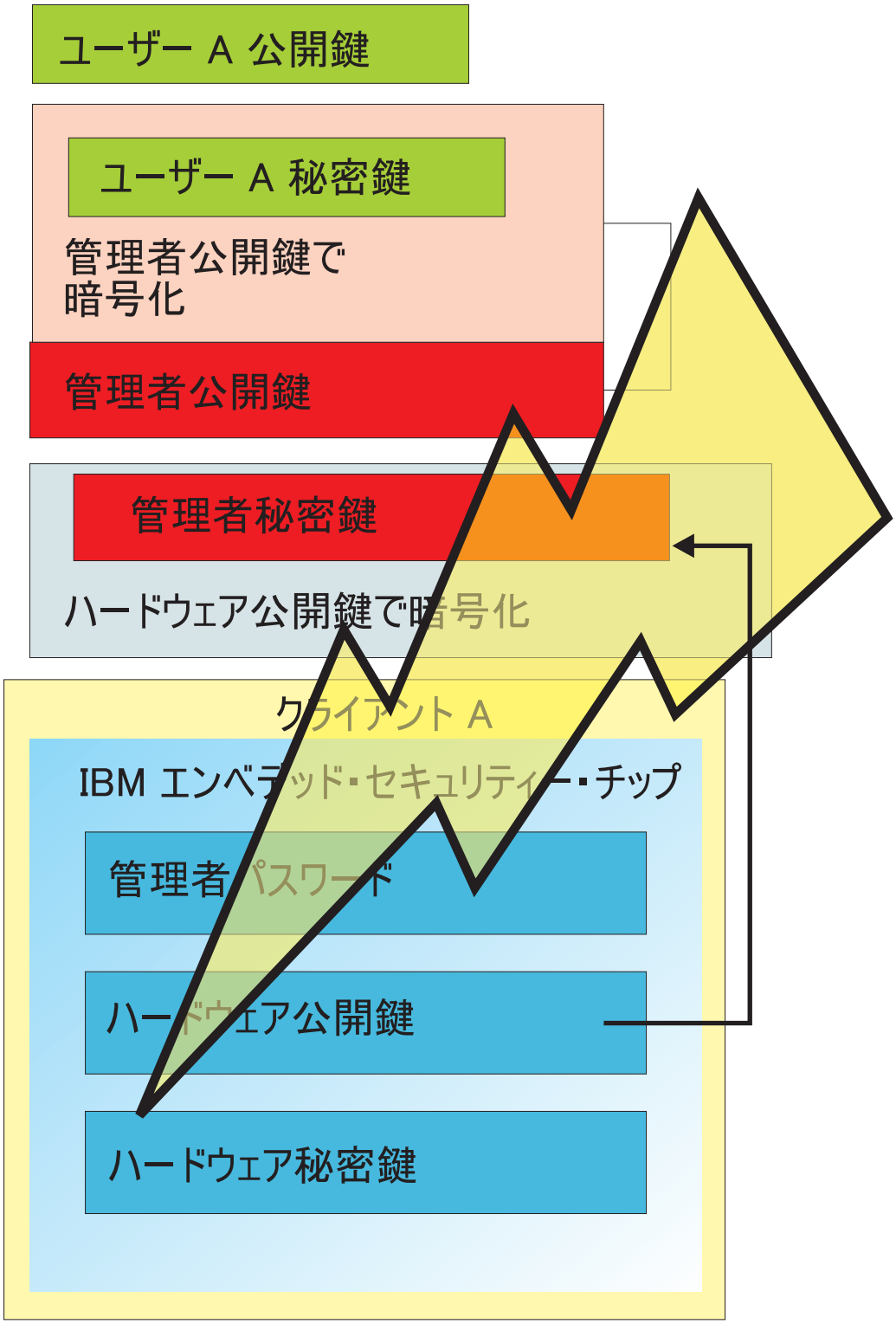

図 10. ユーザー A のコンピューターに落雷して使用不可能になった。

2. ユーザー A は、新しい改良型の IBM コンピューター、つまりクライアント B を入手します。 21 ページの図 11 をご覧ください。クライアント B がクライアント A と違うのは、ハードウェア公開鍵と秘密鍵が、クライアント A 上の鍵と異なるということです。この異なる部分は、クライアント B の灰色の部分

と、クライアント A の緑色の部分です。クライアント B の管理者パスワードは、クライアント A の管理者パスワードと同じですので注意してください。

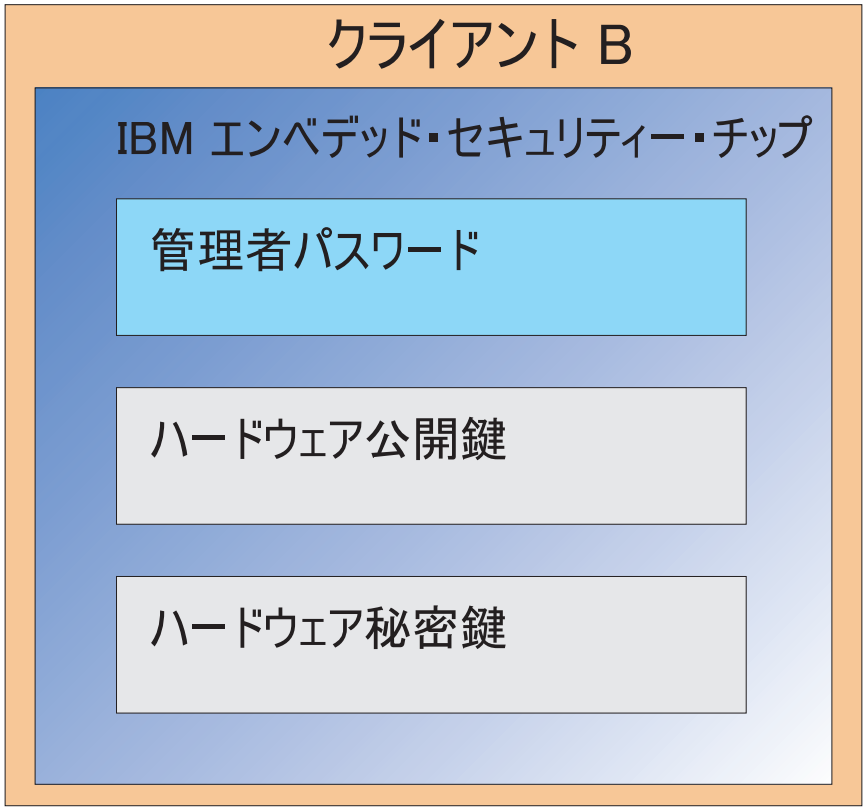

図 11. ユーザー A が、新規のエンベデッド・セキュリティー・チップを搭載した新規コンピューター、クライアント B を受け取る。

3. クライアント B には、クライアント A 上と同じユーザー証明書が必要です。この情報は、クライアント A からアーカイブされます。 18 ページの図 8 で示したとおり、ユーザー鍵は管理者公開鍵により暗号化され、アーカイブ・ロケーションに保管されます。ユーザー証明書をクライアント B で使用可能にするために、管理者公開鍵および秘密鍵をこのマシンに移行する必要があります。図 12 は、アーカイブ・ロケーションからユーザー・データをリカバリーするために、クライアント B が管理者公開鍵と秘密鍵を引き出す様子を示しています。

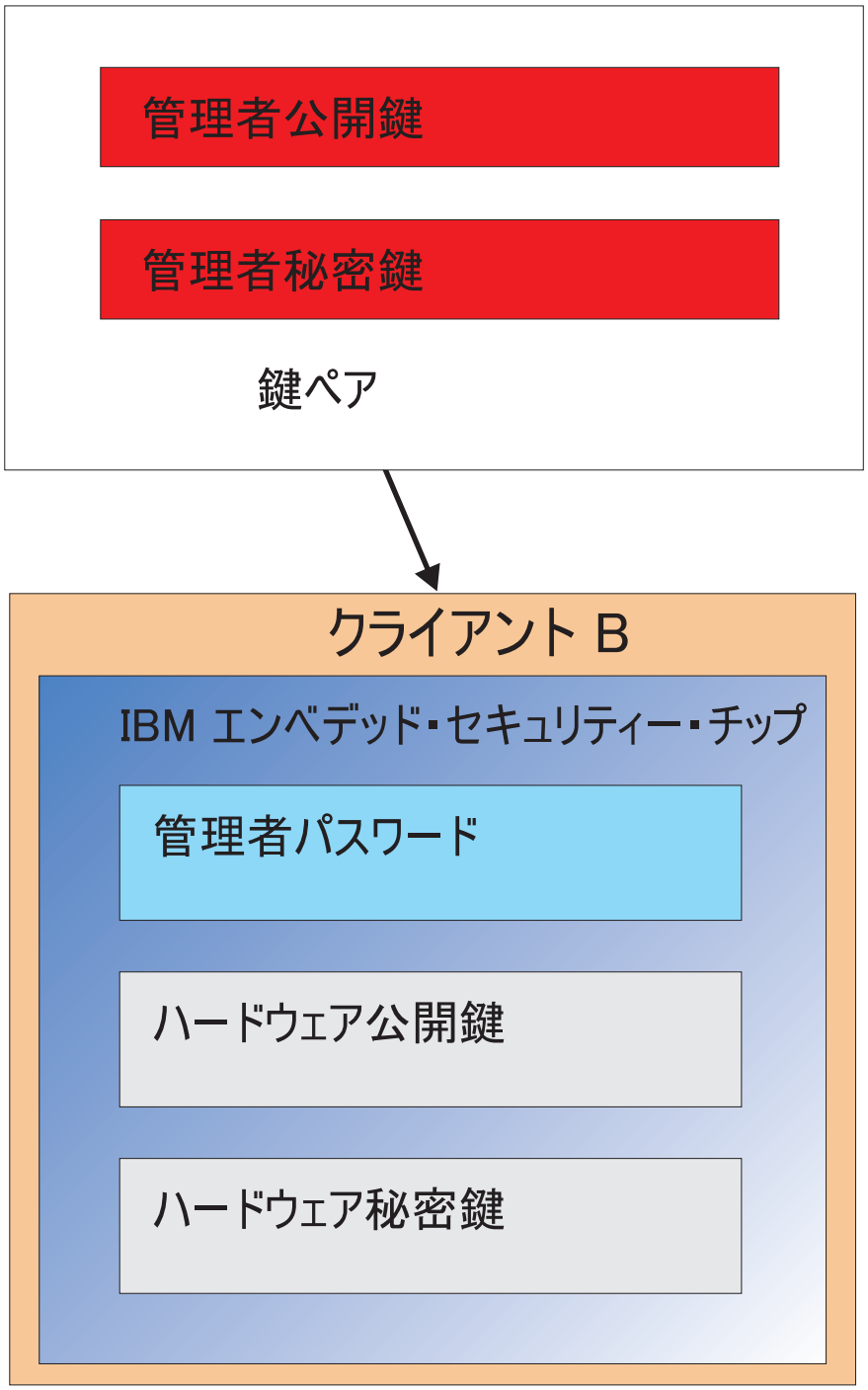

図 12. クライアント B がアーカイブの場所から管理者公開鍵および秘密鍵を検索する。

4. 23 ページの図 13 は、クライアント B のハードウェア公開鍵を使用して管理者秘密鍵を暗号化する様子を示しています。

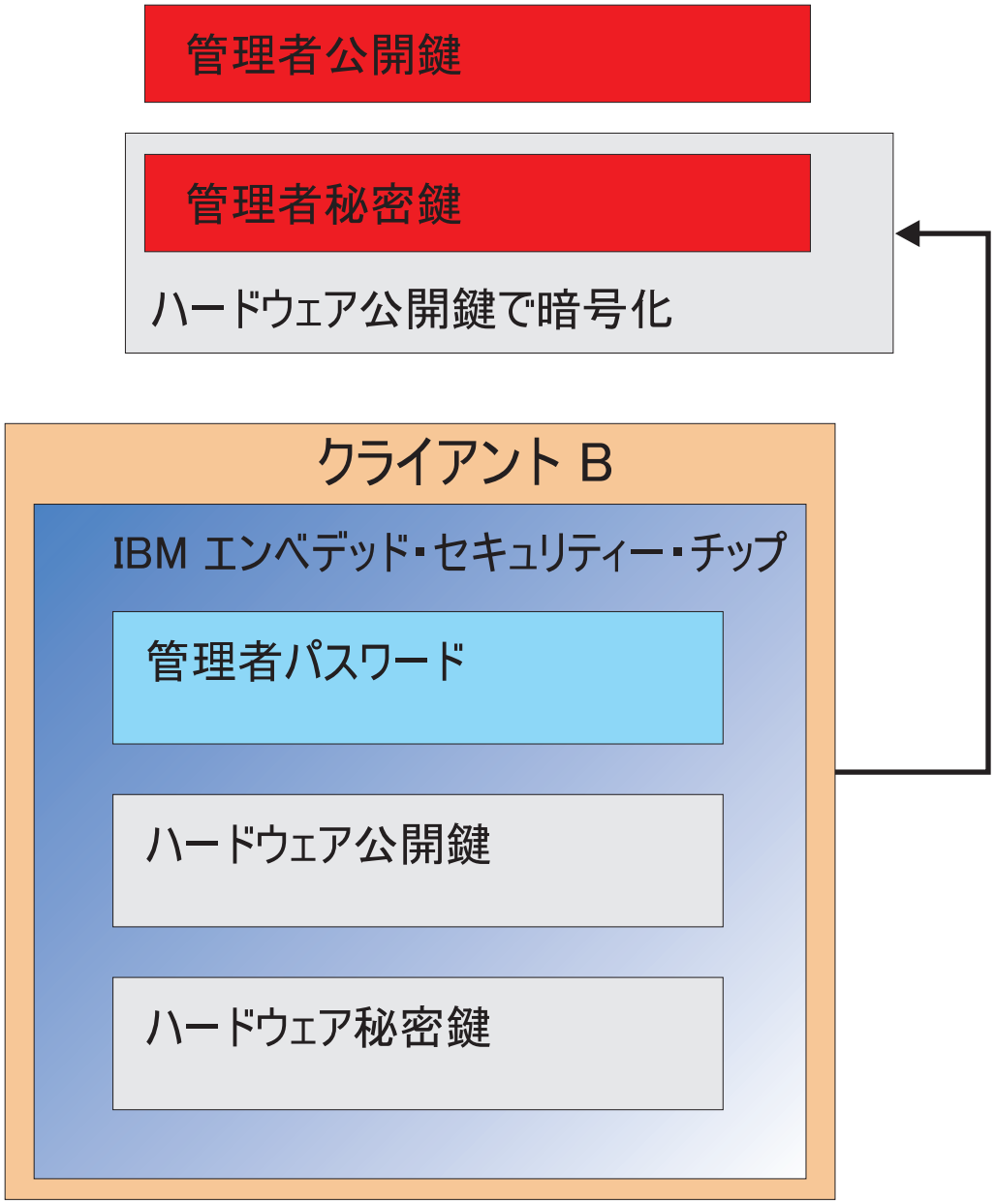

図 13. 管理者秘密鍵が、クライアント B のハードウェア鍵で暗号化される。

このように、管理者秘密鍵がハードウェア公開鍵により暗号化されているため、24 ページの図 14 に示すとおり、クライアント B 上のユーザー A のためにユーザー証明書を取得することができます。

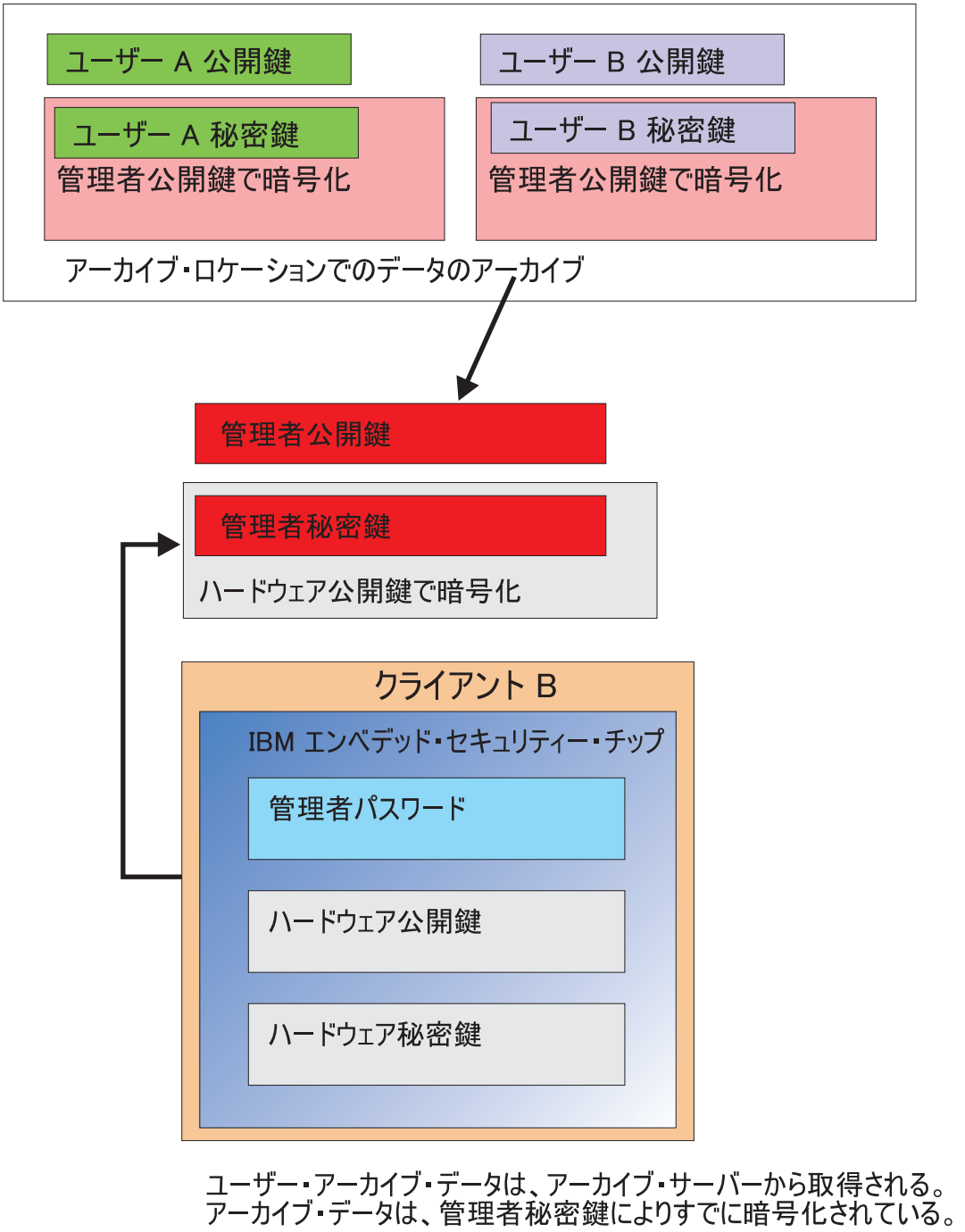

図 14. ユーザー A の証明書は、管理者秘密鍵が暗号化された後にクライアント B にロードできる。

25 ページの図 15 は、クライアント B に完全に復元されたユーザー A を示しています。ユーザー A の秘密鍵は、アーカイブ・サーバー上に置かれていたときに、管理者公開鍵により暗号化されたことに注目してください。管理者公開鍵は、2048 ビットの RSA 鍵であり、実質的に破ることは不可能です。つまり、アクセス制御を強化するために、必ずしもアーカイブの場所を保護する必要はないということです。鍵ペア (管理者公開鍵および秘密鍵)、厳密には管理者秘密鍵がセキュアに保持

されている限り、ユーザー証明書のアーカイブの場所は基本的にどこでも構いません。

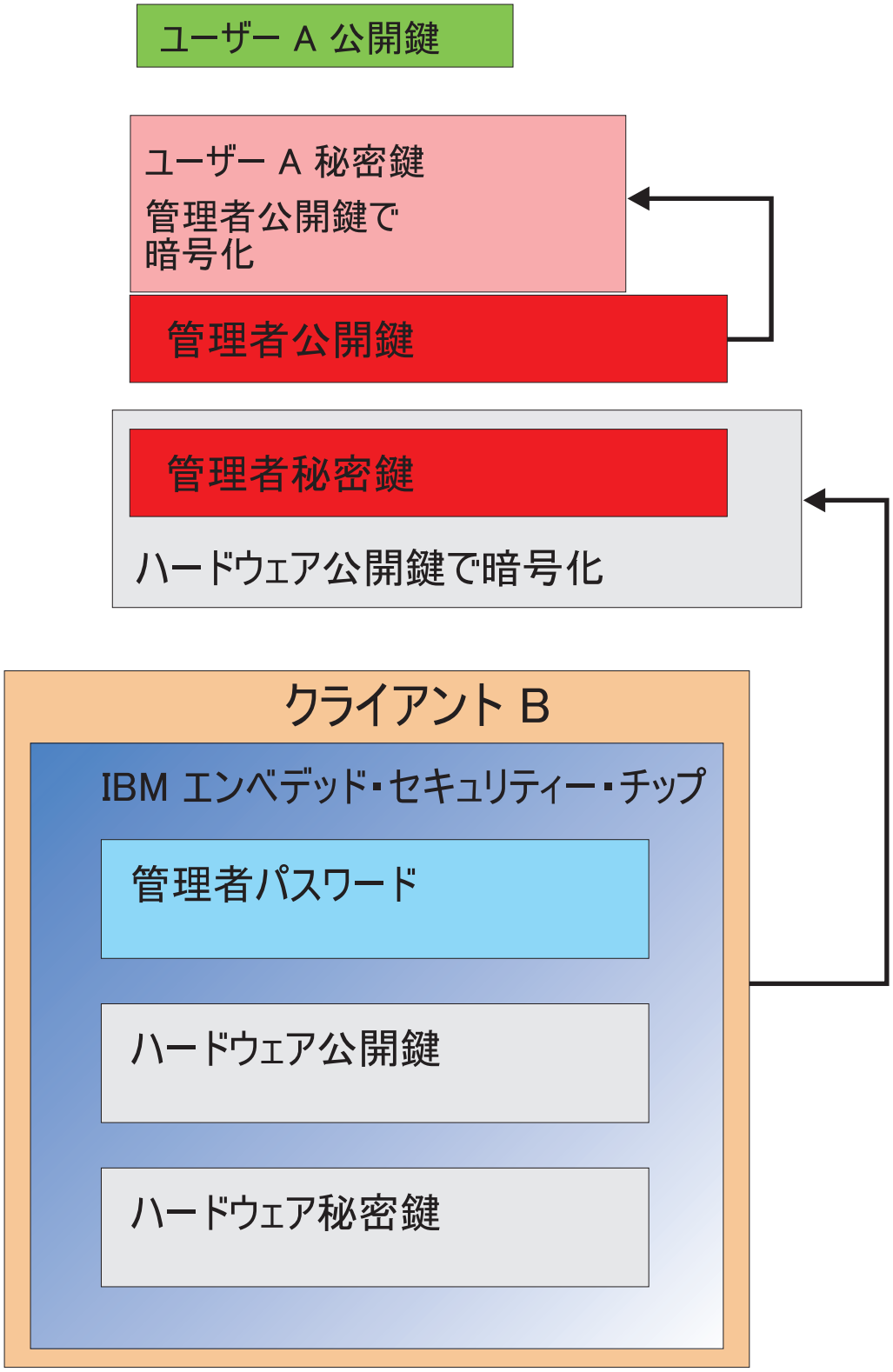

図 15. ユーザー A がクライアント B に完全に復元される。

管理者パスワードの設定方法、アーカイブの場所などについては、ソフトウェアのインストールに関するセクションで詳しく説明します。図 16 は、ESS 環境におけるコンポーネントの概要を示しています。最大のポイントは、各クライアントが、ハードウェア公開鍵および秘密鍵の点では固有ですが、共通の管理者公開鍵および秘密鍵を使用している点です。クライアントは、共通のアーカイブの場所を使用しますが、このアーカイブの場所はユーザーのセグメントまたはグループで使用できます。

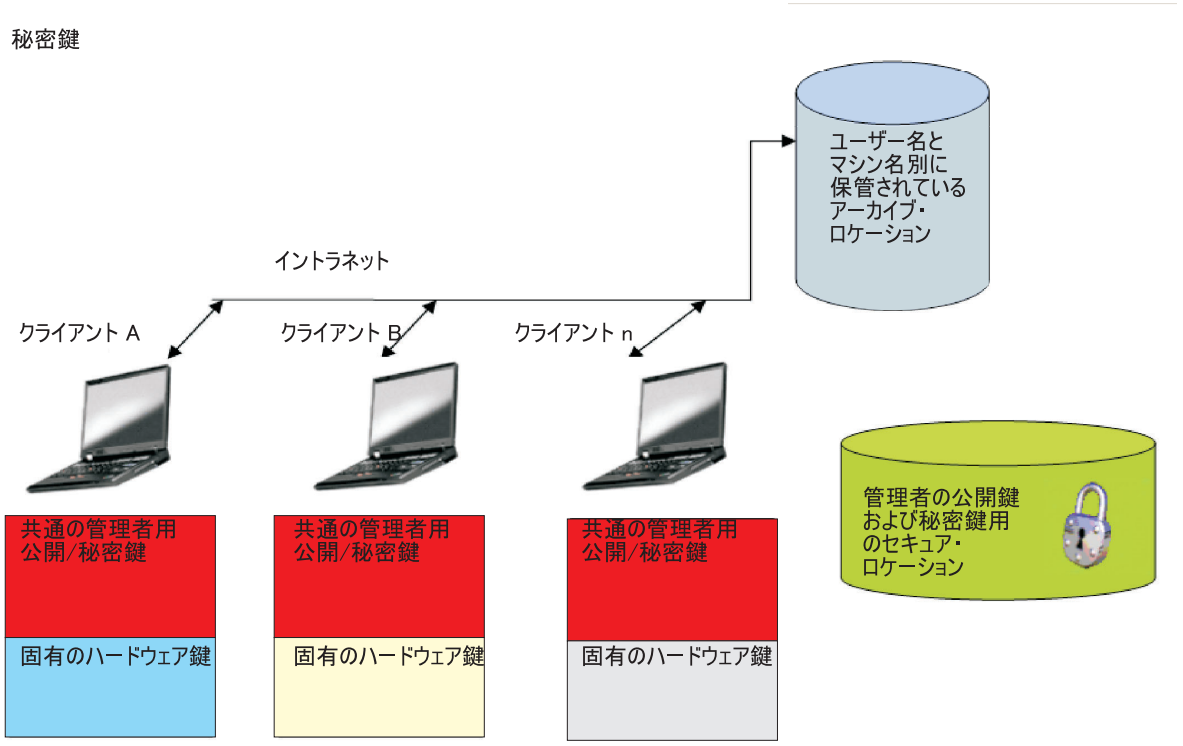

図 16. IBM Client Security System の主要コンポーネント

以下の例を検討してください。人事部門は、エンジニアリング部門と別のアーカイブの場所を持つことができます。アーカイブは、ユーザー名とコンピューター名を基に行われます。IBM Client Security Software は、前述のユーザー A およびユーザー B で示したとおり、ユーザー名とコンピューター名を基に、システムのユーザーを位置定義済みのアーカイブの場所にアーカイブします。また、管理者公開鍵および秘密鍵が安全な場所に置かれているかどうかも注意してください。

注: 同じ場所に保存される各コンピューター名とユーザー名は固有である必要があります。コンピューター名またはユーザー名が重複していると、同じ名前を持つ以前のアーカイブが上書きされてしまいます。

第 5 章 IBM Client Security Software

IBM Client Security Software は、アプリケーションと IBM エンベデッド・セキュリティー・チップを接続します。また、ユーザーの登録、ポリシーの設定、および基本的な管理機能の実行などの操作で、インターフェースとして機能します。IBM Client Security System は、基本的に以下のコンポーネントで構成されています。

- 管理者ユーティリティー
- ユーザー構成ユーティリティー
- 管理者コンソール
- インストール・ウィザード
- ユーザー認証マネージャー (UVM)
- 暗号化サービス・プロバイダー
- PKCS#11 モジュール

IBM Client Security System では、いくつかの主要な機能を実行できます。

- ユーザーの登録
- ポリシーの設定
- パスフレーズ・ポリシーの設定
- パスフレーズを忘れた場合のリセット
- ユーザー証明書の復元

たとえば、ユーザー A がオペレーティング・システムにログオンすると、IBM Client Security System は、ユーザー A がログオン状態であると仮定してすべての決定をします。 (**注:** セキュリティー・ポリシーはユーザー単位ではなくマシン単位です。ポリシーは、同一コンピューターの全ユーザーに適用されます。) ユーザー A が IBM エンベデッド・セキュリティー・サブシステムの利点を活用とすると、IBM Client Security System では、パスフレーズや指紋認証など、そのコンピューターでユーザー A のために設定されている セキュリティー・ポリシーが適用されます。ユーザー A としてログオンした人が正しいパスフレーズを入力できないか、指紋が正しく認証されない場合、IBM ESS は、そのユーザーの要求を拒否します。

ユーザーの登録および登録の管理

IBM ESS ユーザーとは、IBM ESS 環境に登録されている Windowsユーザーのことです。本書で後ほど詳しく説明しますが、ユーザーを登録するにはいくつかの方法があります。このセクションでは、ユーザーが登録する際に行われることを説明します。プロセス中にどのような処理が行われるかを理解しておくと、IBM ESS の仕組みや、実際の環境での管理方法に関する理解を深めることができます。

Client Security Software は、ユーザー認証マネージャー (UVM) を使用して、システム・ユーザーを認証するためのパスフレーズや他の要素を管理します。UVM ソフトウェアでは、次の機能が使用可能です。

- UVM クライアント・ポリシー保護

© Copyright IBM Corp. 2004

- UVM ログオン・プロテクション
- UVM Client Security スクリーン・セーバー・プロテクション

IBM ESS 環境の各ユーザーには、認証目的で使用する個別設定オブジェクトが少なくとも 1 つ関連付けられています。最小要件は、パスフレーズです。ESS (ユーザーの観点から見ると、UVM が認証を管理し、セキュリティー・ポリシーを実行する) 環境の UVM コンポーネントで、すべてのユーザーはパスフレーズを持つ必要があり、このパスフレーズはコンピューターを開始するたびに最小回数として 1 回は求められます。以下のセクションで、パスフレーズが使用される理由、セットアップ方法、および使用法について説明します。

パスフレーズの要求

パスフレーズはセキュリティー上の理由で必要です。 IBM エンベデッド・セキュリティー・サブシステムなどのハードウェア要素を導入すると、処理で使用するユーザー証明書を、自律型の安全なロケーションに保管できるため大きな利点があります。ただし、ハードウェア・チップが提供する保護は、チップにアクセスするために必要な認証が弱い場合はほとんど役に立ちません。たとえば、セキュリティー機能を実行するハードウェア・チップがあるとします。ただし、チップによりアクションを呼び出すために必要な認証は 1 桁とします。これにより、潜在的なハッカーがユーザー証明書を使用してアクションを呼び出すには、1 桁の数字 (0 から 9) を推測するだけですみます。1 桁の認証は、ソフトウェア・ベースのソリューションに利点をほとんど提供しないため、チップのセキュリティーを弱めます。ハードウェア保護と併せて強い認証を使用しない限り、セキュリティー上の利益はまったく得られません。IBM ESS で必要とされているパスフレーズは、ハードウェア上のユーザー証明書を使用していずれかのアクションを実行する前に、ユーザーを認証するために使用されます。UVM パスフレーズは、管理者鍵ペアでしかリカバリーできないので、システムが盗難にあっても、そのシステムから取り出すことはできません。

パスフレーズの設定

各ユーザーは、自らの証明書を保護するためにパスフレーズを選択します。 9 ページの『第 3 章 エンベデッド・セキュリティー・チップの機能』 では、ユーザーの秘密鍵は、管理者公開鍵により暗号化されています。また、ユーザーの秘密鍵にも関連したパスフレーズがあります。このパスフレーズは、ユーザー証明書を使用してユーザーを認証するために使用されます。図 17 は、パスフレーズ、および管理者公開鍵により暗号化された秘密鍵コンポーネントを示しています。

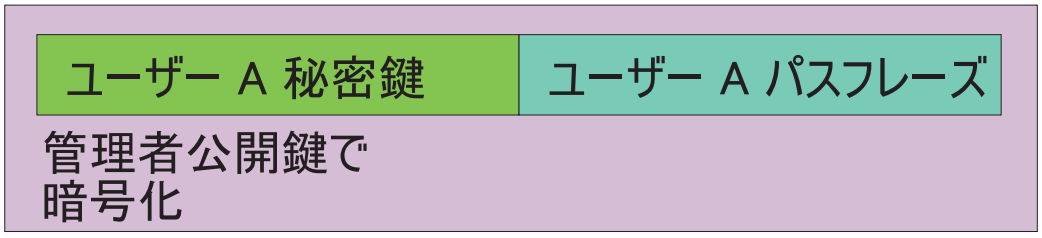

図 17. ユーザー A は、ユーザー A の秘密鍵を必要とする機能を実行するためにパスフレーズを提供する必要がある。

図 17 に示されているパスフレーズは、既存のポリシーに基づいてユーザーが選択したものです。既存のポリシーとは、パスワードの文字数や有効期限日数など、パス

ワードの作成を制御するためのルールのことです。パスフレーズは、ユーザーが UVM に登録されたときに作成されます。IBM Client Security Software を展開したときに、このプロセスがどのように行われるかについては、本書で後ほど詳しく説明します。

秘密鍵の復号化には管理者の秘密鍵が必要であるため、ユーザー A の秘密鍵は管理者公開鍵で暗号化されます。したがって、ユーザー A のパスフレーズを忘れた場合、管理者は新しいパスフレーズにリセットできます。

パスフレーズの使用

30 ページの図 18 から 32 ページの図 20 は、チップ上でユーザーのパスフレーズがどのように処理されるかを示しています。パスフレーズは必ず、操作の最初に、少なくともセッションに 1 回は使用します。パスフレーズは常に必須です。認証デバイスを追加することもできますが、最初のユーザー・パスフレーズ要件と置き換えることはできません。簡潔に説明すると、バイオメトリックまたはその他の認証データは、ユーザーの公開鍵で暗号化されます。この追加セキュリティー・データを復号化するには、秘密鍵へのアクセスが必要になります。

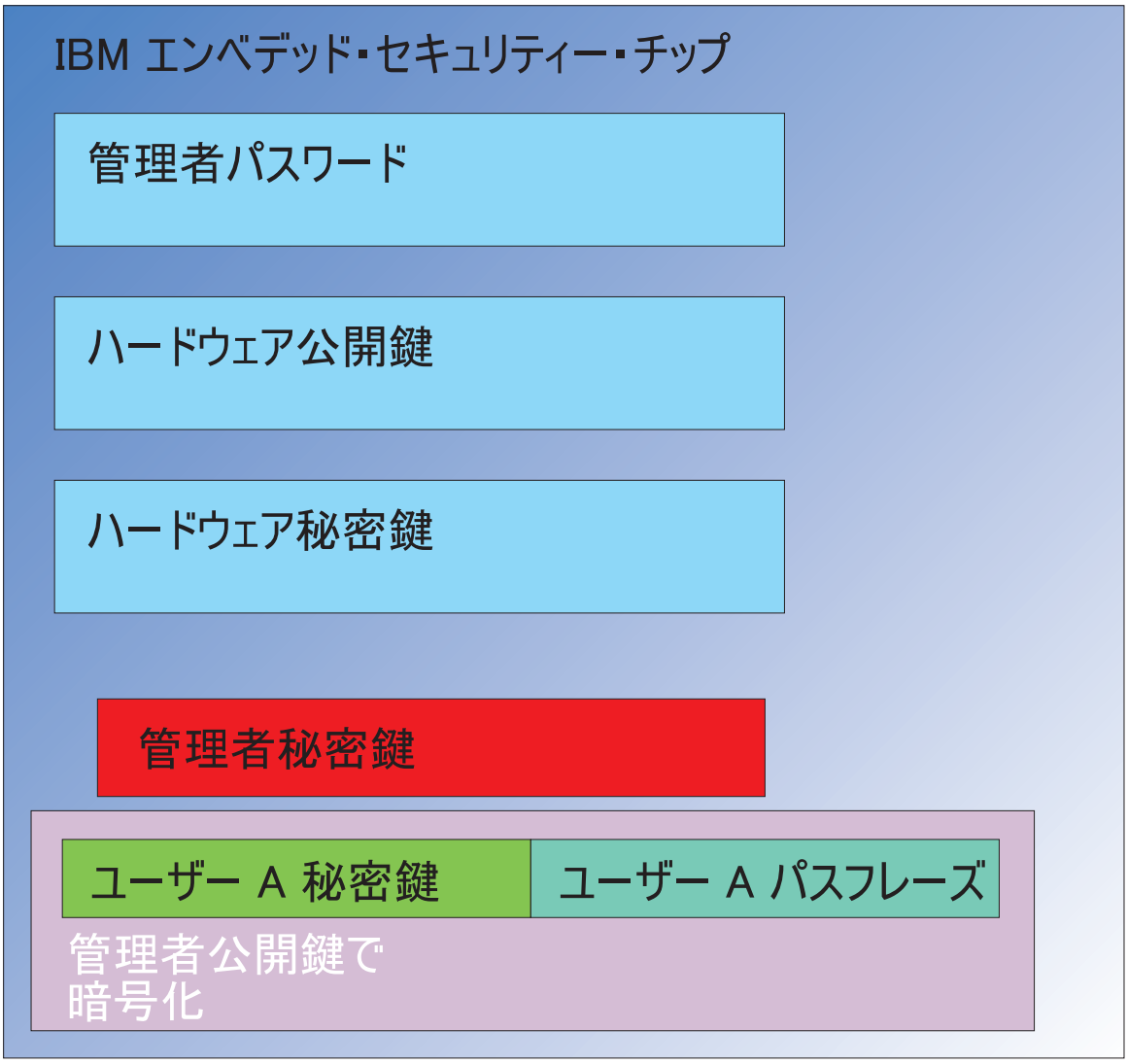

図 18. 管理者の秘密鍵はチップ内で復号化される

このため、追加のデータを復号化する場合は、少なくとも各セッションで 1 回はパスフレーズを入力する必要があります。管理者公開鍵により暗号化されたユーザー A の秘密鍵とパスフレーズを構成する証明書は、IBM エンベデッド・セキュリティー・チップに渡されます。前述したように、管理者の秘密鍵はチップで既に復号化されています。 31 ページの図 19 は、証明書が渡される様子を示しています。

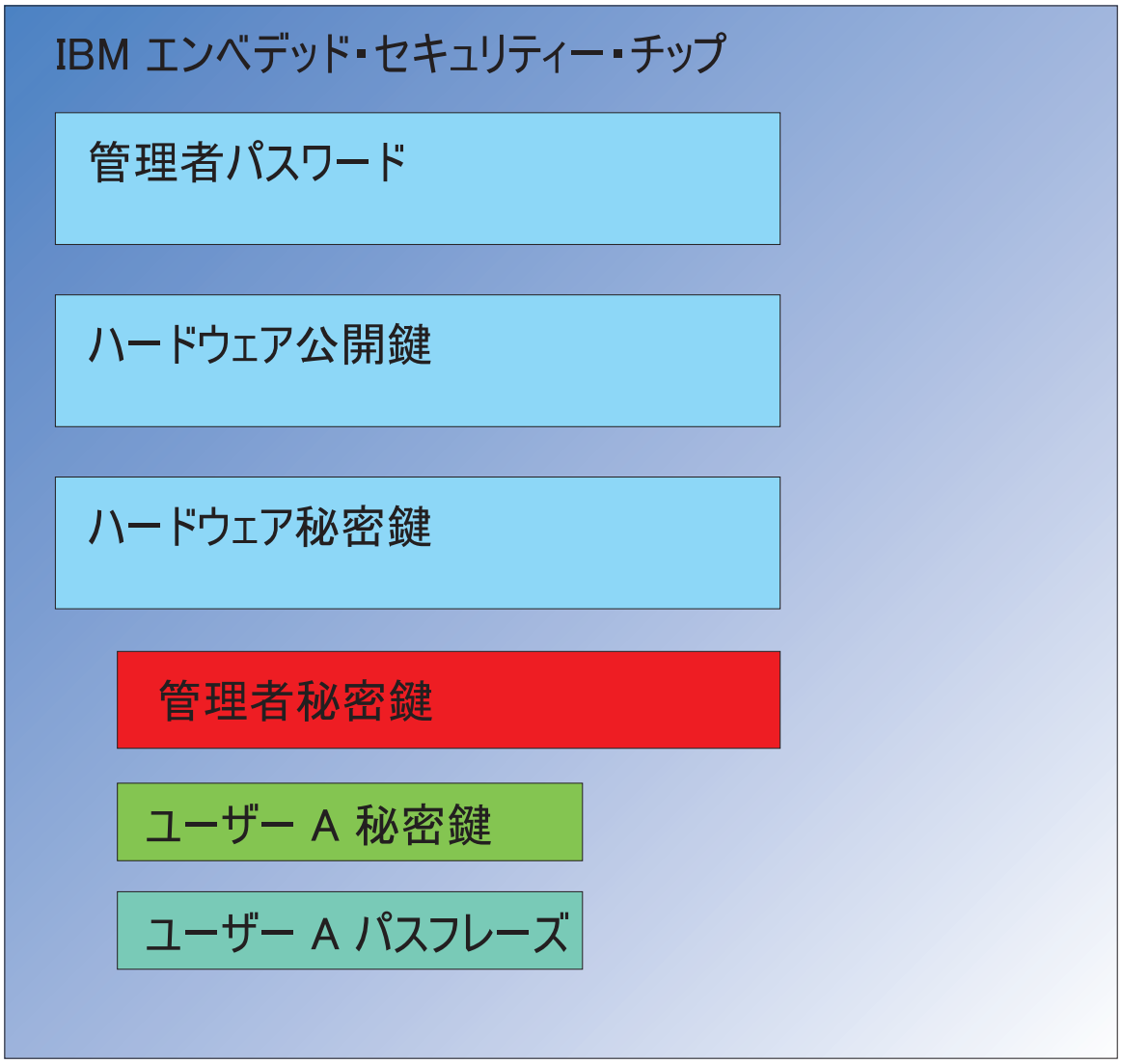

図 19. ユーザー A の秘密鍵とユーザー A のパスフレーズはチップで使用できる。

証明書は復号化され、ユーザー A の秘密鍵およびパスフレーズがチップ内で使用可能になります。IBM Client Security System によりユーザー A として識別されたログイン済みのユーザーが、ユーザー A の証明書の使用を試みると、 32 ページの図 20 に示されているパスフレーズ・ダイアログが表示されます。

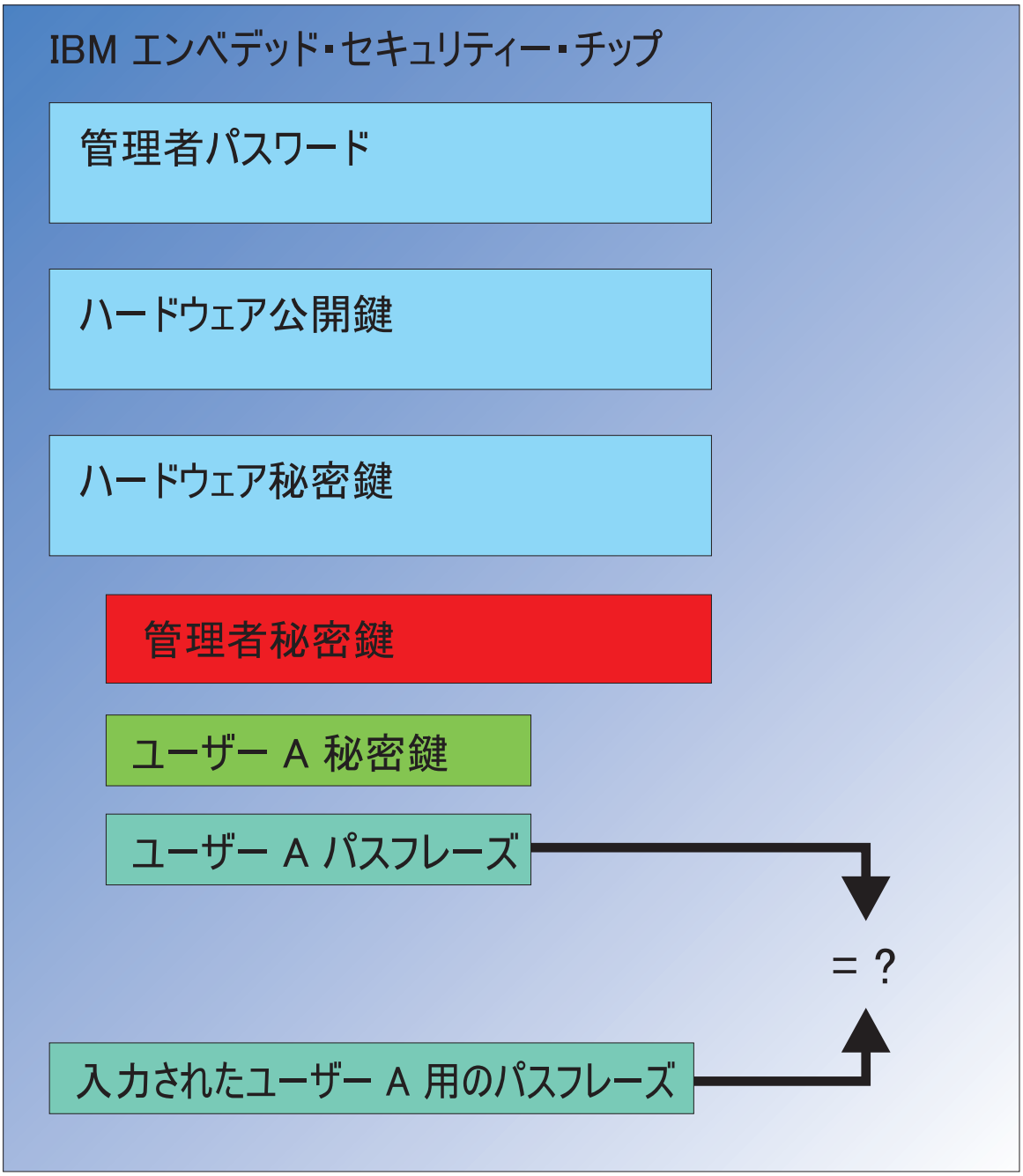

図 20. ユーザー A がユーザー A の証明書を使用しようと試みると、パスフレーズ・ダイアログがオープンする。

入力されたパスフレーズがチップに受け渡され、復号化されたパスフレーズ値と比較されます。一致する場合、ユーザー A の証明書はディジタル署名または電子メールの復号化などさまざま機能に使用できます。このパスフレーズの比較は、チップのセキュアな環境で実行されることにご注意ください。チップには攻撃に対する機能があり、失敗を繰り返すアクセスの試行を検出します。また、ユーザー A の登録されたパスフレーズが決してチップの外部に公開されることがない点にもご注意ください。ユーザーの登録は、IBM Client Security Software のインストールの一部で行われます。この登録プロセスの一部として、ユーザーのパスフレーズの作成があります。このパスフレーズの設定方法およびパスフレーズ・ルールの実行については、後で説明します。

1 ページの図 1 は、IBM エンベデッド・セキュリティー・チップ、および IBM Client Security System を示しています。 1 ページの図 1 は、会社の初期設定およびユーザーの初期設定も示しています。会社の初期設定はエンベデッド・セキュリティー・サブシステムと関連付けられており、ユーザーの初期設定は IBM Client Security Software と関連付けられています。前のセクションでは、一般的な概念を理解するための初期設定について説明しました。次のセクションでは、初期設定のプロセスについて、さらに詳しく説明します。

TPM の初期設定

基本的に、TPM 初期設定とは、ハードウェア公開鍵および秘密鍵、および管理者パスワードを追加するプロセスのことです。つまり、このプロセスにより、IBM から出荷された状態の汎用マシンは、企業にとって固有のマシンになります。次の表では、公開鍵および秘密鍵、および管理者パスワードの初期設定の方法を示しています。

表 3. ハードウェア初期設定の方法

処置	BIOS で作成可能	CSS ソフトウェアで管理者により手動で作成可能	スクリプトで作成可能
ハードウェア公開鍵/秘密鍵の作成	いいえ	はい	はい
管理者パスワードの作成	一部の TCPA と互換性のあるクライアント: はい。BIOS エントリーを確認してください。	はい	はい

表 3 は、ハードウェア公開鍵および秘密鍵が、ソフトウェアのインストール時に自動的に作成されないことを示しています。ハードウェア公開鍵および秘密鍵の作成は、ソフトウェアで手動により、またはスクリプトにより開始される必要があります。管理者パスワードは、BIOS、IBM Client Security Software アプリケーション、またはスクリプトのいずれかの方法で作成できます。チップが、ハードウェア公開鍵および秘密鍵に設定された値を制御します。ユーザーは値を設定できません。チップの乱数機能が使用されて、統計的に無作為な公開鍵および秘密鍵のペアが作成されます。ただし、管理者パスワードは管理者が設定します。

管理者パスワードが異なるのは、管理者が値を設定する必要がある点です。管理者パスワードに関するいくつかの問題に対応する必要があります。

- 管理者パスワード (複数可) として何を設定しますか?
- 複数の異なるグループがありますか?その場合、各コンピューターに対するパスワードはどのような方法で論理的に判別しますか?
- どの管理者がパスワードへのアクセス権を持ちますか? 異なるグループのユーザーに対して複数のパスワードを設定する場合、どのユーザーがどのパスワードに対してアクセス権をもちますか?
- 自己管理型のエンド・ユーザーには、管理者パスワードへのアクセスを許可するか。

上記の項目に対して有効な判断を下すには、管理者パスワードによって使用可能になる以下の機能について理解することが重要です。

- 管理者ユーティリティーへのアクセスの取得
- ユーザーの追加/削除
- 使用可能な IBM Client Security Software アプリケーション/機能の定義

後続のセクションで、ポリシー・ファイルと管理者秘密鍵の関連付けについて説明します。現時点では、ポリシーを変更するために管理者秘密鍵が必要である点にご注意ください。表 4 は、管理者パスワードおよび管理者秘密鍵で実行可能な機能を示しています。

表 4. パスワードおよび秘密鍵に基づいた管理者のアクション

処置	管理者パスワード	管理者秘密鍵
管理者ユーティリティーへのアクセスの取得	はい	いいえ
ユーザーの追加/削除/復元	はい	いいえ
使用可能な CSS アプリケーション/機能の定義	はい	いいえ
ポリシーの定義/変更	はい	はい
ユーザーのパスフレーズをリセットするファイルの作成	はい	はい

TPM の初期設定でも、管理者公開鍵および秘密鍵が参照されます。上図で、この鍵と関連付けられた機能が分かります。管理者公開鍵および秘密鍵の設定について検討してください。この鍵ペアは、それぞれのコンピューターごとに固有にすることも、すべてのマシンに対して同一にすることもできます。IBM Client Security Software を初期設定すると、管理者は、既存の鍵ペアを使用するか、クライアント用に新しい鍵ペアを作成するかを選択することができます。企業にとって何が最善かは、実装する使用モデルによって異なります。

最良実例

企業の規模が大きければ、マシンごとに固有の鍵を与えるか、部門ごとに固有の鍵を与えることができます。たとえば、人事部門で使用されているすべてのコンピューターに管理者パスワードおよび/または管理者秘密鍵を設定して、エンジニアリング部門には別の管理者パスワードおよび/または管理者秘密鍵を設定する例などがあります。また、ビルまたは立地など物理的な要素をもとに区別することもできます。パスフレーズ・リセット・ファイルを作成する際に、使用する管理者秘密鍵を判別できると、リセットを要求するユーザーに基づいて簡単に処理できます。 33 ページの表 3 および 37 ページの表 5 で示されているとおり、ユーザーと会社、またはハードウェアの初期設定を実行する必要があります。

CSS をデプロイする前にセキュリティー・ポリシーを設定する

企業や組織においては、セキュリティーおよび認証についての設定が重要です。管理者アクセス権を持っている人であれば、ポリシーを変更し、そのポリシーをクライアント・コンピューターに「push」することができますが (59 ページの『第 8 章 リモート側で新規または改訂されたセキュリティー・ポリシー・ファイルをデプロイする』 を参照)、ポリシー設定は、デプロイメントの前に構成するのが最善で

す。ポリシーの設定の詳細については、「*Client Security Software 管理者ガイド*」の「UVM ポリシーの処理」を参照してください。

パスフレーズの紛失や認証装置の誤動作に備える

ユーザーがパスフレーズを紛失し、指紋読取装置やスマートカードなどの認証装置が正しく動作しない事態が頻繁に生じます。

パスフレーズの紛失: ユーザーのパスフレーズは、クライアント・ハードディスクまたはエンベデッド・セキュリティー・チップのどこにも、人が読める形式では保存されていません。ユーザー自身の頭の中か、管理者鍵ペアで保護された他の場所に保管しておくことが安全です。管理者は、管理者秘密鍵を使用して、アーカイブ内のユーザー情報を復号化する必要があります。それから、管理者はユーザーに、新しいパスフレーズを提供します。

ユーザーがパスフレーズを変更すると、指定したアーカイブに新しい情報が保存されます。

認証装置が誤動作した場合、IBM Client Security Software の設定を変更して、「**Click here to bypass**」ボタンを表示するように構成することができます。ボタンをクリックすると、パスフレーズを正しく入力するようにという要求がユーザーに出されます。セキュアなタスクを続行することができます。

CSS でバイパス・ボタンを表示するように設定するには、以下の手順を行います。

1. CSEC.INI ファイル (ルート・ディレクトリに位置) 内で、`AllowBypass= 0` エントリーを検索します。デフォルトでは、値が `0` に設定されており、CSS ではバイパス・ボタンは非表示になります。
2. `AllowBypass` 値を 1 に設定します。CSS ウィンドウで、パスフレーズに加えて認証を提供するようにユーザーに要求するときに、バイパス・ボタンが表示されます。
3. CSEC.INI ファイルを保存します。

注:

1. この情報をアーカイブするには、セットアップ構成ファイル (csec.ini) の保存先ディレクトリ名を `kal=`”保存先ディレクトリ名”にアーカイブ・ロケーションを指定する必要があります。さらに、保存先ディレクトリ名がネットワーク・ドライブの場合、そのドライブはパスフレーズを保存するために、クライアント・コンピューター上でマップされていなければなりません。
2. アーカイブを指定しないでクライアント・コンピューター上もマップされない場合、パスフレーズはリカバリーされません。

ユーザーの初期設定

IBM ESS は、複数のユーザーが 1 台のコンピューター上で独立してセキュア・トランザクションを実行するための機能を備えています。これらのユーザーには、1 つのパスフレーズが関連付けられており、その他にも指紋読取装置やスマートカードなどの認証装置が導入されている場合があります。このような仕組みは、*複数要因認証* と呼ばれています。ユーザーの初期設定は、IBM ESS を使用するためにクライアント・コンピューターを構成するときの、重要なステップです。ユーザーの初期設定には、2 つの部分のプロセスがあることにご注意ください。

1. 登録
2. 個人情報設定

登録

登録とは、IBM Client Security System にユーザーを追加または登録する作業のことです。図 21 は、IBM Client Security Software のユーザー認証マネージャー (UVM) コンポーネントを示しています。UVM は、各ユーザーの証明書を制御し、ポリシーを実行します。

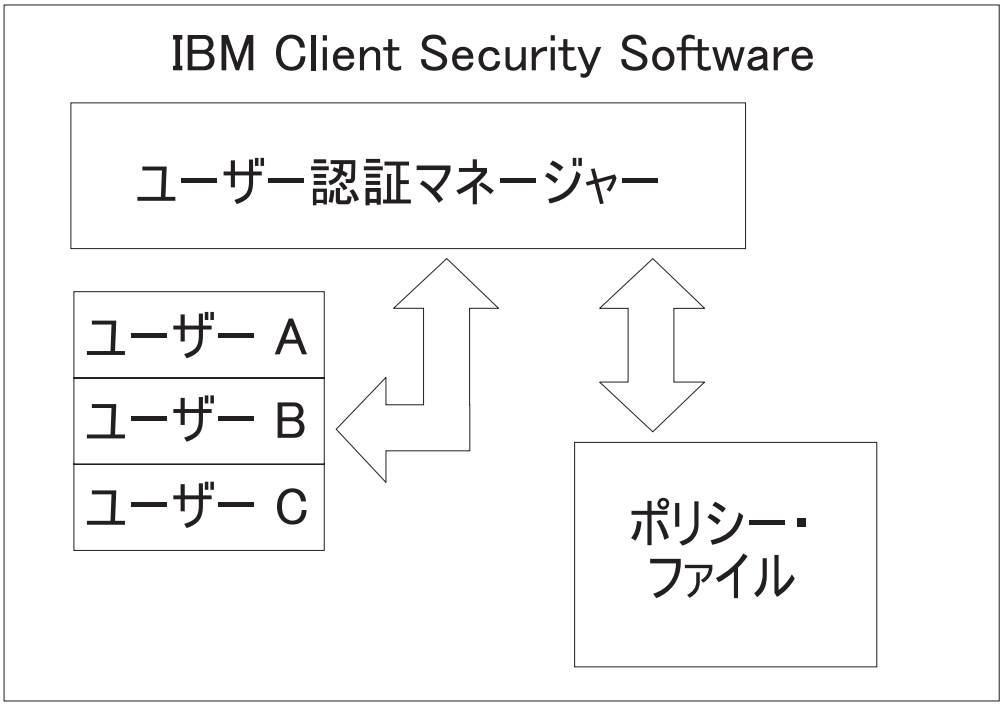

図 21. ユーザー認証マネージャーは、各ユーザーの証明書を制御し、セキュリティー・ポリシーを実行する。

図 21 に示されているようなポリシー・ファイルには、UVM が管理する各ユーザーに関する認証要求が定義されています。UVM のユーザーは、Windows ユーザー (ローカルまたはドメイン) に過ぎないことに注目してください。UVM は、現在コンピューターおよびオペレーティング・システムにログオンしているユーザーに基づいて証明書を管理します。たとえば、ユーザー A が Windows にログインしたときに、ユーザー A が UVM ユーザーでもある場合、ユーザー A が証明書が必要な操作を実行しようとすると、UVM によりポリシーが適用されます。別の例として、ユーザー A がコンピューターにログオンした場合を考えます。ユーザー A は、次に Microsoft Outlook を起動して、ディジタル署名付きの電子メールを送信します。ディジタル署名された電子メールを送信するときに使用した秘密鍵は、IBM エンベデッド・セキュリティー・サブシステムにより保護されます。UVM は、操作の実行を許可する前に、ポリシー・ファイルで定義されているポリシーを実行します。この例における要件は、操作が実行される前に、パスフレーズが認証されることです。UVM は、ユーザーにパスフレーズを求めるプロンプトを出し、正確に認証された場合、秘密鍵の操作がチップ内で実行されます。

個人の初期設定

個人の場合、初期設定とは個人用 UVM パスフレーズを設定することを指します。登録プロセスのさまざまな部分を、異なる人が実行することができます。個人の UVM パスフレーズは、本人のみに知らされます。ただし、各個人が初期設定プロセスを実行しない場合は、その個人が追加のステップを実行しなければならない場合があります。UVM では、ユーザーが初めてログオンしたときに、パスフレーズの変更を強制するように構成することもできます。

たとえば、ユーザー A が IT 管理者により初期設定されるとします。IT 管理者は、Windows のユーザー・リストからユーザー A を (たとえば、ドメインから) 選択します。UVM では、UVM パスフレーズをユーザー A に関連付けるように要求されます。そこで、IT 管理者は、「IT 管理者パスフレーズ」の「デフォルト値」を入力します。システムのセキュリティーを確実にするため、ユーザー A はシステムを受け取った後に、パスフレーズをカスタマイズして、他者がデフォルトのパスフレーズを使用してセキュア・トランザクションを行えないようにします。

表 5. ユーザーの初期設定の方法

方法	コマンド・プロセス	プロセス要件
手動	管理者は、管理者ユーティリティーを介して手動でユーザー用に CSS の個人情報設定を行える。	各コンピューターのセットアップには管理者が立ち合います。
管理者構成ファイル	管理者は、構成ファイルを作成できる。構成ファイルには、管理者パスワードの暗号化されたものが含まれる。そのファイルがユーザーに送信され、ユーザーは管理者の介入または立ち会いなしに個人で登録できる。	ユーザーが、セットアップ・プロセスを実行する。
*.ini	管理者が、.ini ファイルを実行するスクリプトを作成し、デフォルトまたは個別設定したパスワードを設定する。	管理者またはユーザーの立ち会いはオプションです。

デプロイメントのシナリオ

ここでは、1,000 個のエンド・ユーザーのために 1,000 個のクライアントをデプロイメントします。デプロイメントの方法は、以下のいずれかです。

- どのマシンがどのエンド・ユーザーに配布されるか正確に把握している場合。たとえば、マシン 1 がボブに配布されるため、ボブをマシン 1 に登録します。ボブは、コンピューターを受け取ると、個人情報設定 (彼の個人用パスフレーズの設定) を行う必要があります。Bob はコンピューターを受け取り、IBM Client Security Software を開始し、自分のパスフレーズを設定します。
- どのマシンがどのユーザーに配布されるのか把握していない場合。クライアント 1 をエンド・ユーザー X に配送します。

これら 2 つの要素があるため、IBM ESS のデプロイメント方法は、通常のアプリケーションとは異なります。ただし、IBM の ESS をデプロイする上で柔軟性を提供するデプロイメント・オプションがいくつかあります。

会社における PC 送達の標準的なフロー・チャートは以下のようになります。

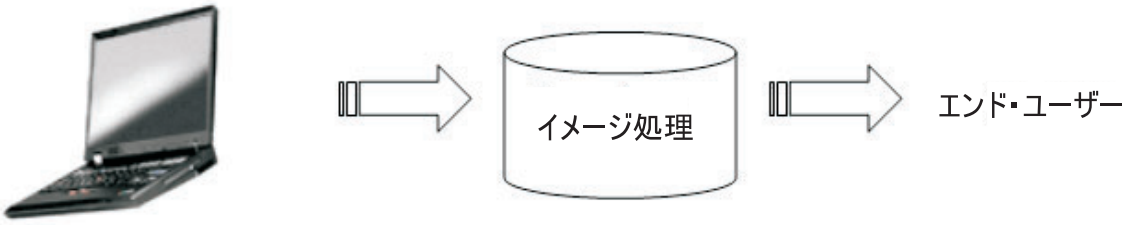

図 22. 標準的な PC デプロイメントのフロー・チャート

6 通りのデプロイメント・シナリオ

IBM Client Security Software をデプロイメントする方法は 6 通りあります。

1. **追加コンポーネント**—IBM Client Security Software のコードはディスク・イメージの一部ではありません。コンピューターがデプロイされた後に、インストール、初期設定、および個人情報設定が行われます。
2. **イメージ・コンポーネント**—IBM Client Security Software のコードはイメージの一部ですが、インストールされていません。会社およびユーザーの個人情報設定は開始されていません。 (39 ページの図 23 を参照)
3. **シンプル・インストール**—IBM Client Security Software はインストールされ、会社またはエンド・ユーザー用に個人情報設定が行われています。(40 ページの図 24 を参照。)
4. **部分的な個人情報設定**—IBM Client Security Software はインストールされ、会社の個人情報設定は行われていますが、エンド・ユーザーの個人情報設定は行われていません。(40 ページの図 24 を参照。)
5. **一時的な個人情報設定**—IBM Client Security Software はインストールされ、会社およびユーザーの個人情報設定は設定されています。ユーザーはユーザーのパス

フレーズをリセットし、必要に応じて、指紋スキャンまたはスマートカードの関連性など他の認証情報を提供します。(41 ページの図 25 を参照。)

6. **完全な個人情報設定**—IBM Client Security Software はインストールされ、会社およびユーザーの個人情報設定は設定されています。管理者はユーザーのパスフレーズを設定します。指紋スキャンまたは他の認証が必要である場合、ユーザーはその個人情報設定を提供する必要があります。(41 ページの図 25 を参照。)

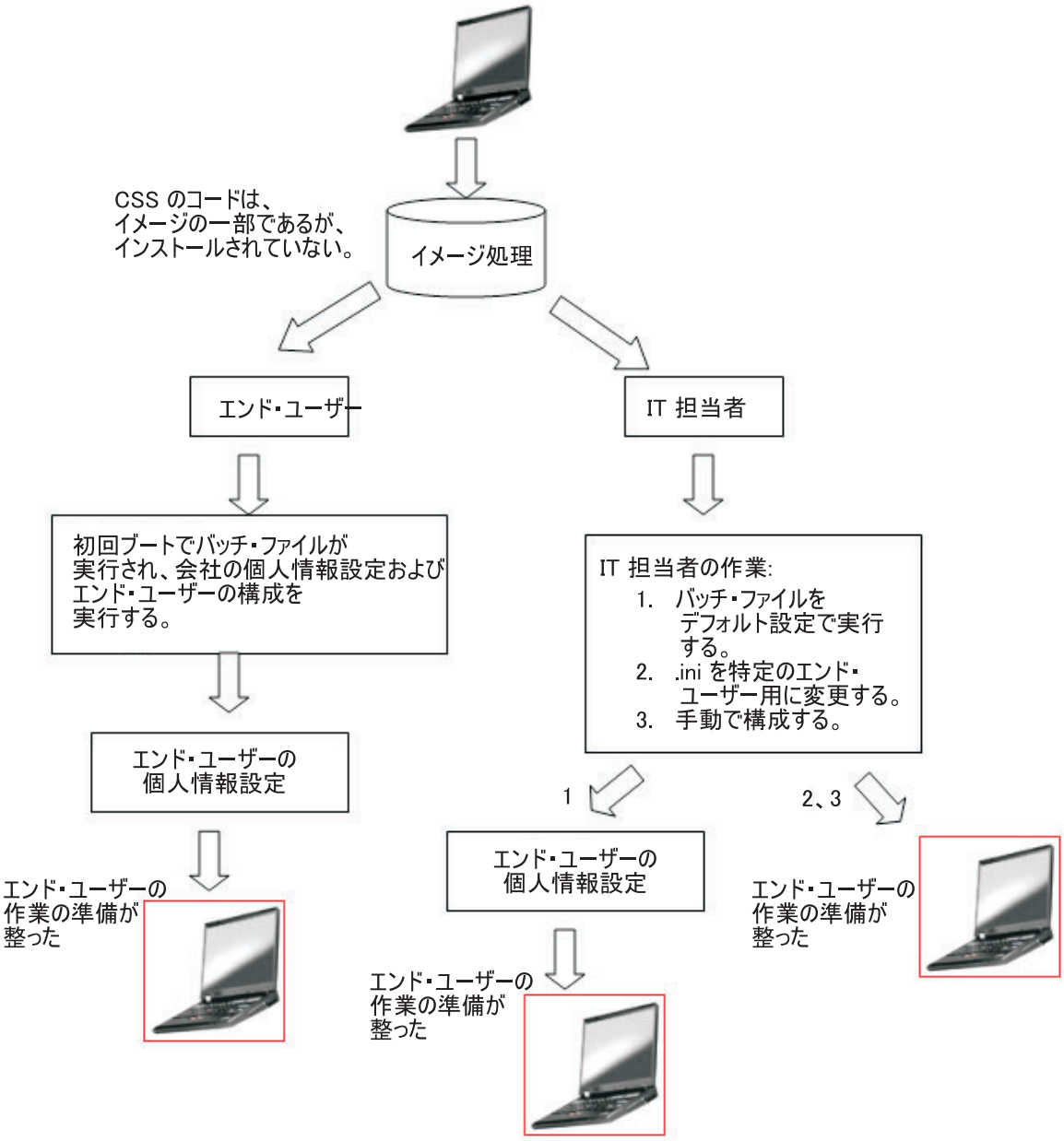

図 23. IBM Client Security Software コードはイメージに含まれているが、インストールされていない

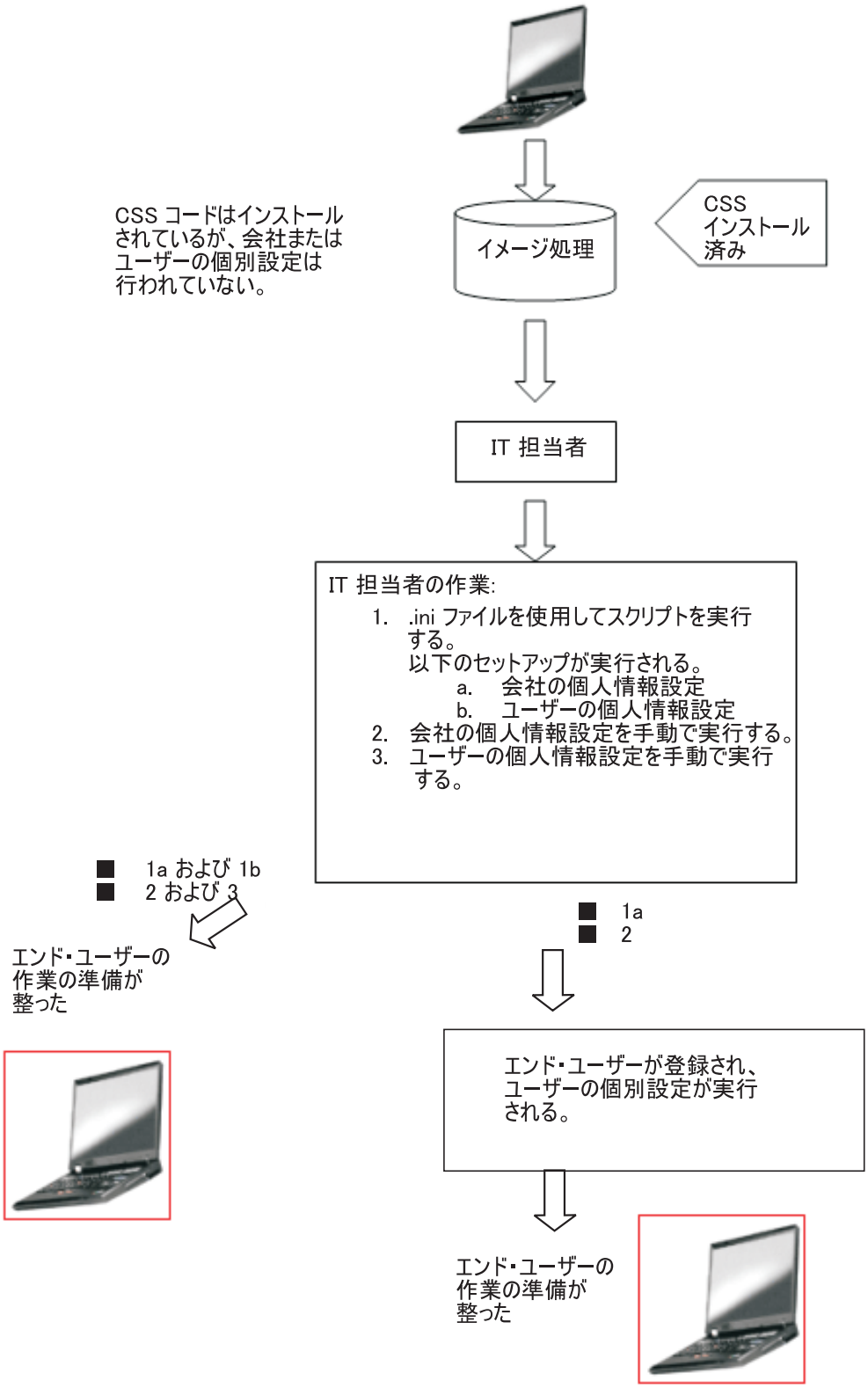

図 24. IBM Client Security Software コードはインストールされているが、会社またはユーザーの個別設定は行われていない

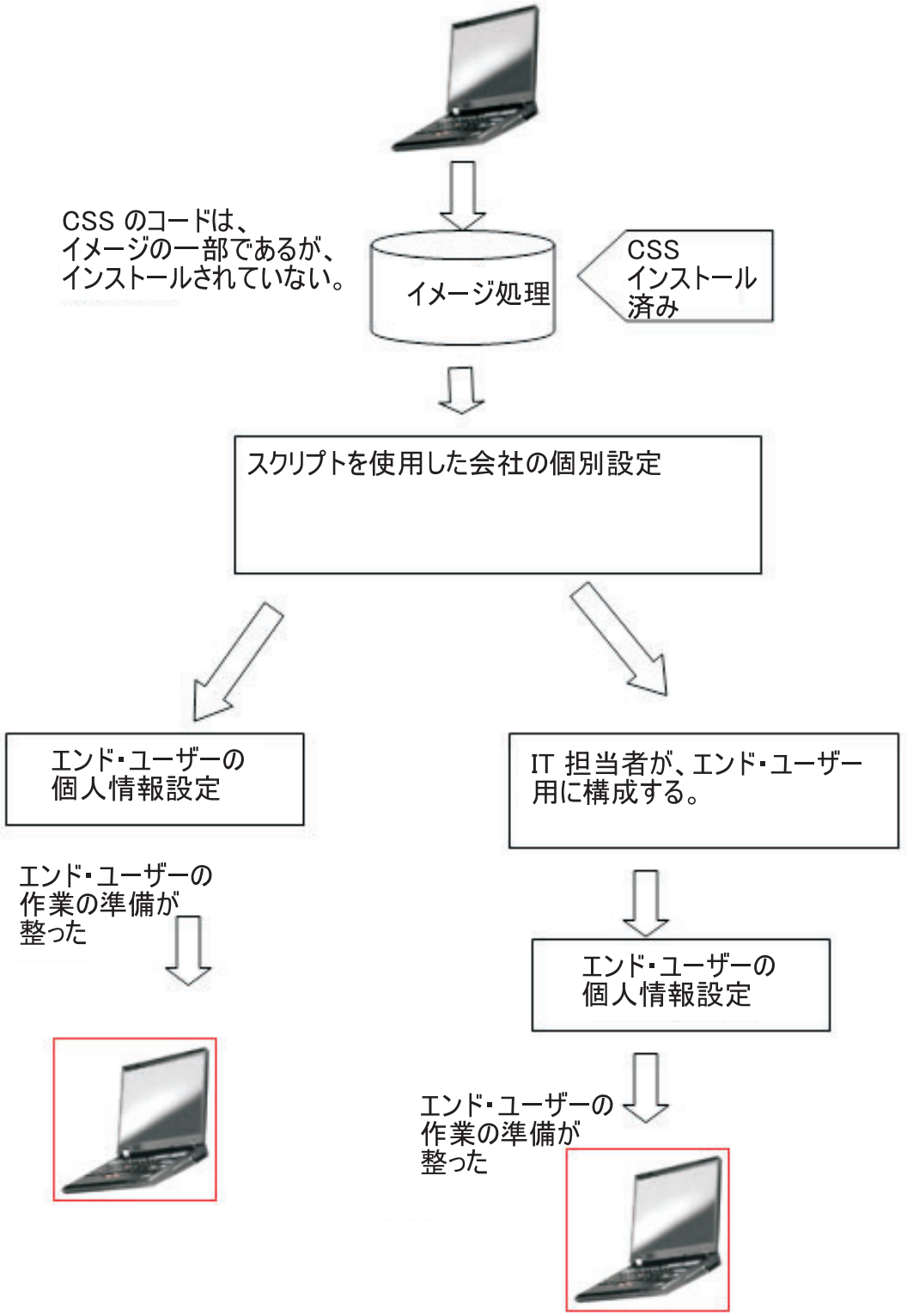

図 25. IBM Client Security Software はインストールされており、会社とユーザーの個別設定が完了している

シナリオ 1 では、ディスク・イメージがコンピューターに置かれた後に、IBM Client Security Software がデプロイメントされます。ディスク・イメージがインス

トールされた後、IBM Client Security Software がインストールおよび構成され、エンベデッド・セキュリティー・チップが構成されます。

シナリオ 2 から 6 は、ソフトウェアのデプロイメントおよび構成、およびチップの構成のさまざまなオプションを表しています。お客さまのニーズおよび環境に応じて、要件に最適なシナリオおよびインストールの方法を選択できます。

構成ファイルの詳細

CSEC.INI ファイルは、Client Security のウィザード (Security ディレクトリーの CSECWIZ.EXE) を使用して作成できます。ウィザードを完了した後、**「セットアップ・ウィザードで行った設定をセットアップ構成ファイル (C:¥CSEC.INI) に保存します。」の横にあるチェック・ボックスにチェックマークを付けます。ただし、サブシステムは構成しないでください。(設定は、C:¥CSEC.INI に保管されます)。**

設定

マス・デプロイメントによる設定を開始する場合は cscc.ini ファイルが必要です。拡張子が .ini であればファイル名は任意です。次のリストは、作成する .ini ファイルの設定および設定の説明を示しています。CSEC.INI ファイルを開いて変更する前に、最初に Security フォルダーの CONSOLE.EXE を使用して復号化する必要があります。

表 6. Client Security System 構成設定

[CSSSetup]	CSS セットアップのセクション・ヘッダー。
suppw=bootup	BIOS 管理者/スーパーバイザーのパスワード。 不要な場合はブランクのままにしてください。
hwpw=11111111	CSS ハードウェア・パスワード。8 文字でなければなりません。常に必須です。ハードウェア・パスワードがすでに設定されている場合は、正しい値でなければなりません。
newkp=1	新しい管理者鍵ペアを生成する場合は 1。 既存の管理者鍵ペアを使用する場合は 0。
keysplit=1	newkp が 1 の場合は、秘密鍵コンポーネントの番号を決定します。 **注:** 既存の鍵ペアが複数の秘密鍵パーツを使用する場合は、すべての秘密鍵パーツを同じディレクトリーに格納しなければなりません。
kpl=c:¥jgk	newkp が 1 の場合の管理者鍵ペアの場所。ネットワーク・ドライブの場合はマップする必要があります。
kal=c:¥jgk¥archive	ユーザー鍵アーカイブの場所。 ネットワーク・ドライブの場合はマップする必要があります。
pub=c:¥jk¥admin.key	既存の管理者鍵ペアを使用する場合の管理者公開鍵の場所。 ネットワーク・ドライブの場合はマップする必要があります。
pri=c:¥jk¥private1.key	既存の管理者鍵ペアを使用する場合の管理者秘密鍵の場所。 ネットワーク・ドライブの場合はマップする必要があります。
wiz=0	このファイルが CSS セットアップ・ウィザードによって生成されたかどうかを識別します。このエントリーは必須ではありません。ファイルに含める場合には、値は必ず 0 にします。
clean=0	初期化後に .ini ファイルを削除する場合は 1、 初期化後も .ini ファイルを残しておく場合は 0。

表 6. Client Security System 構成設定 (続き)

enableroaming=1	クライアントのローミングを有効にする場合は 1、 クライアントのローミングを無効にする場合は 0。
username= [promptcurrent]	[promptcurrent] に設定すると、現在のユーザーにシステム登録パスワードの入力を求めるプロンプトを表示します。 [current] に設定すると、sysregpwd エントリーで指定されたシステム登録パスワードが現在のユーザーに与えられ、ユーザーはシステムをローミング・サーバーに登録することを許可されます。 指定したユーザーがローミング・サーバーへのシステムの登録を許可されており、そのユーザーのシステム登録パスワードを sysregpwd 項目で指定する場合は [<specific user account>]。 enableroaming 値が 0 の場合や、enableroaming エントリーが存在しない場合は、このエントリーを使用しないでください。
sysregpwd=12345678	システム登録パスワード。この値は、システムがローミング・サーバーに登録されるための正しいパスワードを設定してください。username 値が [promptcurrent] に設定されている場合や、username エントリーが存在しない場合は、このエントリーを含めないでください。
[UVMEnrollment]	ユーザー登録のセクション・ヘッダー。
enrollall=0	ローカル・ユーザー・アカウントをすべて UVM に登録する場合は 1、 特定のユーザー・アカウントを UVM に登録する場合は 0。
defaultuvmpw=top	enrollall が 1 の場合は、すべてのユーザーに対する UVM パスフレーズです。
defaultwinpw=down	enrollall が 1 の場合、すべてのユーザー用に UVM に登録された Windows パスワード。
defaultppchange=0	enrollall が 1 の場合に、すべてのユーザーに対する UVM パスフレーズ変更ポリシーを設定します。 値を 1 に設定した場合、ユーザーの次回のログオン時に UVM パスフレーズの変更が要求されます。 値を 0 に設定した場合、ユーザーの次回のログオン時に UVM パスフレーズの変更は要求されません。
defaultppexppolicy=1	enrollall が 1 の場合に、すべてのユーザーに対する UVM パスフレーズ有効期限ポリシーを設定します。 値を 0 に設定した場合、UVM パスフレーズの有効期限が設定されます。 値を 1 に設定した場合、UVM パスフレーズの有効期限を設定しません。
defaultppexpdays=0	enrollall が 1 の場合は、すべてのユーザーに対し UVM パスフレーズの有効期限が切れるまでの日数を設定します。 ppexppolicy が 0 に設定される場合、この値で UVM パスフレーズの有効期限が切れるまでの日数を設定してください。
enrollusers=*x*、ここで x はコンピューターに登録するユーザーの総数を示します。	このステートメントの値は、登録するユーザーの総数を指定します。 enrollall が 0 の場合は、UVM に登録されたユーザーの数です。

表 6. Client Security System 構成設定 (続き)

user1=jknox	登録するユーザーの情報を、ユーザー 1 から順に提供します。(ユーザー 0 は存在しません。)ユーザー名はアカウント名でなければなりません。XP の実際のアカウント名を取得するには、次を行います。 1. コンピューター管理 (Computer Management) (Device Manager) を開始します。 2. 「Local Users and Groups (ローカル・ユーザーおよびグループ)」ノードを展開します。 3. 「Users (ユーザー)」フォルダーをオープンします。 「Name (名前)」列にリストされた項目がアカウント名です。
user1uvmpw=chrome	ユーザー 1 UVM の UVM パスフレーズを指定します。
user1winpw=spinning	UVM に登録するユーザー 1 の Windows パスフレーズを指定します。
user1domain=0	ユーザー 1 のアカウントがローカルであるのか、またはドメインにあるのかを指定します。 このアカウントがローカルであることを示す場合は 0、 このアカウントがドメインにあることを示す場合は 1。
user1ppchange=0	ユーザー 1 の次回のログオン時に UVM パスフレーズの変更を要求するかどうかを指定します。 値を 1 に設定した場合、ユーザーの次回のログオン時に UVM パスフレーズの変更が要求されます。 値を 0 に設定した場合、ユーザーの次回のログオン時に UVM パスフレーズの変更は要求されません。
user1ppexppolicy=1	ユーザー 1 の UVM パスフレーズの有効期限を設定するかどうかを指定します。 値を 0 に設定した場合、UVM パスフレーズの有効期限が設定されます。 値を 1 に設定した場合、UVM パスフレーズの有効期限を設定しません。
user1ppexpdays=0	user1ppexppolicy=0 の場合、この値で UVM パスフレーズの有効期限が切れるまでの日数を設定してください。
各ユーザーに対して、表の影付き部分で指定された順に従って、完全な構成設定を提供します。1 名のユーザーにすべてのパラメーターを提供してから、次のユーザーにパラメーターを提供します。たとえば、enrollusers が 2 に設定される場合、以下のグループの構成設定を追加することができます。	
user2=chrome	
user2uvmpw=left	
user2winpw=right	
user2domain=0	
user2ppchange=1	
user2ppexppolicy=0	
user2ppexpdays=90	
[UVMAppConfig]	UVM 認識アプリケーションのセットアップおよび UVM 認識モジュールのセットアップに関するセクション・ヘッダー。

表 6. Client Security System 構成設定 (続き)

uvmlogon=0	UVM ログオン・プロテクションを使用する場合は 1、 Windows ログオンを使用する場合は 0。
entrust=0	Entrust 認証に UVM を使用する場合は 1、 Entrust 認証を使用する場合は 0。
notes=1	Lotus Notes に VM プロテクションを使用する場合は 1、 Notes のパスワード保護を使用する場合は 0。
netscape=0	IBM PKCS#11 モジュールによる 電子メールの署名と暗号化を行う場合は 1。 IBMPKCS#11 モジュールによる 電子メールの署名と暗号化を行わない場合は 0。
passman=0	パスワード・マネージャーを使用する場合は 1、 パスワード・マネージャーを使用しない場合は 0。
folderprotect=0	ファイルおよびフォルダー暗号化を使用する場合は 1、 ファイルおよびフォルダー暗号化を使用しない場合は 0。

注:

1. IBM Client Security Software が拡張および更新されると、*.ini のパラメーターは変更することがあります。
2. いずれかのファイルまたはパスがネットワーク・ドライブ上にある場合、そのドライブはドライブ名にマッピングされている必要があります。
3. ソフトウェアがコンテンツをロードできるようにするには、CSEC.ini ファイルが暗号化されている必要があります。このファイルは、Security ディレクトリー内の CONSOLE.EXE を使用して暗号化します。スクリプトを使用して INI ファイルを暗号化する場合、次のコマンドを使用することもできます。(長いパス名を使用するには、引用符が必要です): *CSS インストール・フォルダー*¥console.exe /q /ini: *暗号化されていない ini ファイルの絶対パス*
4. マス・デプロイメント設定をマス・デプロイメント・インストールとともに実行しない場合は、次のコマンドでコマンド行から ini. ファイルを実行します。

   CSS installation folder¥acamucli /ccf:c:¥csec.ini
5. INI ファイルでは、サブシステムを構成した後に、新しいユーザーを追加する機能がサポートされています。この機能は、ユーザーを登録するのに便利です。INI ファイルは前述の方法で実行しますが、「pub=」および「pri=」値は含めないでください。このコードは、ユーザー登録のみを目的としており、サブシステムの再初期設定は想定していません。

IBM Client Security Software では、すでにインストールされている現在の Client Security Software に影響することなく、CSEC.INI ファイルを再度実行することができます。このファイルを再度実行すると、追加のユーザー登録などの操作を実行できます。

表 7. 2 回目の実行時の Client Security Software 構成設定

[CSSSetup]	CSS セットアップのセクション・ヘッダー。
suppw=	BIOS 管理者/スーパーバイザーのパスワード。 不要な場合はブランクのままにしてください。

表 7. 2 回目の実行時の Client Security Software 構成設定 (続き)

hwpw=11111111	CSS ハードウェア・パスワード。8 文字でなければなりません。常に必須です。ハードウェア・パスワードがすでに設定されている場合は、正しい値でなければなりません。
newkp=0	既存の管理者鍵のペアを使用する場合は 0。
keysplit=1	newkp が 1 の場合は、秘密鍵コンポーネントの番号を決定します。 **注:** 既存の鍵ペアが複数の秘密鍵パーツを使用する場合は、すべての秘密鍵パーツを同じディレクトリーに格納しなければなりません。
pub=	ブランクのままにしてください。
pri=	ブランクのままにしてください。
kal=c:¥archive	ユーザー鍵アーカイブの場所。 ネットワーク・ドライブの場合はマップする必要があります。
wiz=0	このファイルが CSS セットアップ・ウィザードによって生成されたかどうかを識別します。このエントリーは必須ではありません。ファイルに含める場合には、値は必ず 0 にします。
clean=0	初期設定後も .ini ファイルを残しておく場合は 0。
enableroaming=0	クライアントでローミングを無効にする場合は 0。
[UVMEnrollment]	ユーザー登録のセクション・ヘッダー。
enrollall=0	ローカル・ユーザー・アカウントをすべて UVM に登録する場合は 1、 特定のユーザー・アカウントを UVM に登録する場合は 0。
enrollusers=1	このステートメントの値は、登録するユーザーの総数を指定します。
user1=*eddy*	登録する新しいユーザーの名前。
user1uvmpw=pass1word	ユーザー 1 UVM の UVM パスフレーズを指定します。
user1winpw=	UVM に登録するユーザー 1 の Windows パスフレーズを指定します。
user1domain=0	ユーザー 1 のアカウントがローカルであるのか、またはドメインにあるのかを指定します。 このアカウントがローカルであることを示す場合は 0、 このアカウントがドメインにあることを示す場合は 1。
user1ppchange=0	ユーザー 1 の次回のログオン時に UVM パスフレーズの変更を要求するかどうかを指定します。 値を 1 に設定した場合、ユーザーの次回のログオン時に UVM パスフレーズの変更が要求されます。 値を 0 に設定した場合、ユーザーの次回のログオン時に UVM パスフレーズの変更は要求されません。
user1ppexppolicy=1	ユーザー 1 の UVM パスフレーズの有効期限を設定するかどうかを指定します。 値を 0 に設定した場合、UVM パスフレーズの有効期限が設定されます。 値を 1 に設定した場合、UVM パスフレーズの有効期限を設定しません。
user1ppexpdays=0	user1ppexppolicy=0 の場合、この値で UVM パスフレーズの有効期限が切れるまでの日数を設定してください。

第 6 章 Tivoli Access Manager サーバーへの Client Security コンポーネントのインストール

クライアント・レベルでのエンド・ユーザーの認証処理は、セキュリティー上の重要な問題です。Client Security Software は、IBM クライアントのセキュリティー・ポリシーの管理に必要なインターフェースを備えています。このインターフェースは、Client Security Software の主要コンポーネントである認証ソフトウェアのユーザー認証マネージャー (UVM) に組み込まれています。

IBM クライアントの UVM セキュリティー・ポリシーは、次の 2 通りの異なる方法で管理できます。

- IBM クライアントに置かれているポリシー編集を使用して、ローカル側から管理する
- Tivoli® Access Manager を使用して全社的に管理する

Client Security を Tivoli Access Manager と一緒に使用する前に、Tivoli Access Manager の Client Security コンポーネントをインストールしておく必要があります。このコンポーネントは、IBM Web サイト (http://www.ibm.com/jp/pc/security/index.shtml) からダウンロードできます。

前提条件

IBM クライアントと Tivoli Access Manager サーバーとの間の保護接続を確立する前に、次のコンポーネントを IBM クライアントにインストールしておく必要があります。

- IBM Global Security Toolkit
- IBM SecureWay® Directory クライアント
- Tivoli Access Manager Runtime Environment

Tivoli Access Manager のインストールと使用の詳細については、http://www.tivoli.com/products/index/secureway_policy_dir/index.htm の Web サイトにある資料を参照してください。

Client Security のコンポーネントのダウンロードとインストール

Client Security コンポーネントは、IBM Web サイトから無料でダウンロードできます。

Client Security コンポーネントをダウンロードして、Tivoli Access Manager サーバーと IBM クライアントにインストールするには、以下の手順を実行します。

1. Web サイト上の情報を使用して、システムに IBM 統合セキュリティー・チップが搭載されていることを確認します。この確認を行うには、モデル番号をハードウェア要件のテーブルと照合して、「**続行**」をクリックします。

© Copyright IBM Corp. 2004

2. マシン・タイプと一致するラジオ・ボタンを選択して、「**続行**」をクリックします。
3. ユーザー ID を作成し、オンライン・フォーム記入により IBM に登録して、使用許諾契約書を確認した上で「**使用許諾契約書に同意**」をクリックします。

   自動的に Client Security ダウンロード・ページに転送されます。
4. ダウンロード・ページ上のステップに従って、デバイス・ドライバー、readme ファイル、ソフトウェア、参照資料、追加のユーティリティーなど、必要なものをすべてインストールします。
5. 次の手順を実行して、Client Security Software をインストールします。
   a. Windows のデスクトップで、「**スタート**」 > 「**ファイル名を指定して実行**」の順にクリックします。
   b. 「ファイル名を指定して実行」フィールドに「`d:¥directory¥css54xjp.exe`」と入力し、「**OK**」をクリックします。ここで、d:¥directory¥ は、ダウンロードしたファイルが保管されているドライブとディレクトリーです。ファイル名中の「X」は、省略されるか、英数字が入ります。適切なファイル名を入力します。
   c. 「**OK**」をクリックします。画面の指示に従って、インストールを続けます。
6. コンピューターが再起動したら、Windows のデスクトップから、「**スタート**」 > 「**ファイル名を指定して実行**」の順にクリックします。
7. 「ファイル名を指定して実行」フィールドに「*d:¥directory*¥TAMCSS.exe」(*d:¥directory*¥ はファイルが格納されているドライブ名およびディレクトリー) を入力するか、「**参照**」をクリックしてファイルを位置指定します。
8. 「**OK**」をクリックします。
9. 宛先フォルダーを指定して、「**解凍**」をクリックします。

   ウィザードによって、指定されたフォルダーにファイルが抽出されます。ファイルが正常に解凍されたことを示すメッセージが出されます。
10. 「**OK**」をクリックします。

Client Security コンポーネントを Tivoli Access Manager サーバーに追加

pdadmin ユーティリティーは、管理者が大部分の Tivoli Access Manager 管理タスクの実行に使用できるコマンド行ツールです。複数コマンドの実行により、管理者は、複数の pdadmin コマンドが入っているファイルを使用して、1 つのタスクまたは一連のタスクを実行できます。pdadmin ユーティリティーと管理サーバー (pdmgrd) 間の通信は、SSL を介して保護されます。pdadmin ユーティリティーは、Tivoli Access Manager Runtime Environment (PDRTE) パッケージの一部としてインストールされます。

pdadmin ユーティリティーは、このようなファイルの位置を指定するファイル名引き数を受け入れます。たとえば、次のとおりです。

```
MSDOS>pdadmin [-a admin-user][-p password ]file-pathname
```

次のコマンドは、IBM Solutions オブジェクト・スペース、Client Security Actions、および個々のACL 項目を Tivoli Access Manager サーバー上に作成する方法の一例です。

```
MSDOS>pdadmin -a sec_master -p password C:¥TAM_Add_ClientSecurity.txt
```

pdadmin ユーティリティーおよびそのコマンド構文の詳細については、「*Tivoli Access Manager Base Administrator Guide*」を参照してください。

IBM クライアントと Tivoli Access Manager サーバー間の保護接続の確立

IBM クライアントから Tivoli Access Manager 許可サービスに許可決定を要求するためには、Tivoli Access Manager セキュア・ドメイン内に独自の認証 ID を設定する必要があります。

Tivoli Access Manager セキュア・ドメイン内でアプリケーション用に固有の ID を作成する必要があります。認証 ID が認証検査を実行するには、アプリケーションが remote-acl-users グループのメンバーでなければなりません。アプリケーションがセキュア・ドメイン・サービスのいずれかとコンタクトしたい場合、まず、セキュア・ドメインにログインする必要があります。

IBM Client Security アプリケーションは、svrsslcfg ユーティリティーを使用することによって、Tivoli Access Manager 管理サーバーおよび許可サーバーとの通信を可能にしています。

IBM Client Security アプリケーションは、svrsslcfg ユーティリティーを使用することによって、Tivoli Access Manager 管理サーバーおよび許可サーバーとの通信を可能にしています。

svrsslcfg ユーティリティーは、次のタスクを実行します。

- アプリケーション用のユーザー ID を作成する。例: DemoUser/HOSTNAME
- そのユーザー用の SSL キー・ファイルを作成する。例: DemoUser.kdb と DemoUser.sth
- ユーザーを remote-acl-users グループに追加する。

次のパラメーターが必要です。

- **-f cfg_file** 構成ファイルのパスおよび名前。TAMCSS.conf を使用します。
- **-d kdb_dir** サーバー用の鍵リング・データベース・ファイルが入るディレクトリー。
- **-n server_name** 対象の IBM クライアント・ユーザーの実際の Windows ユーザー名/UVM ユーザー名。
- **-P admin_pwd** Tivoli Access Manager の管理者パスワード。
- **-s server_type** remote として指定する必要がある。
- **-S server_pwd** 新たに作成されたユーザーのパスワード。このパラメーターは必須です。

- **-r port_num** IBM クライアント用の listen ポート番号。これは、Tivoli Access Manager Runtime 変数の PD 管理サーバー用 SSL サーバー・ポートで指定されるパラメーターです。
- **-e pwd_life** パスワードの有効期間 (日数)。

IBM クライアントと Tivoli Access Manager サーバーとの間の保護接続を確立するには、次の手順を実行します。

1. ディレクトリーを作成し、この新しいディレクトリーに TAMCSS.conf ファイルを移動します。

   例: `MSDOS> mkdir C:¥TAMCSS MSDOS> move C:¥TAMCSS.conf C:¥TAMCSS¥`
2. svrsslcfg を実行してユーザーを作成します。

   MSDOS> svrsslcfg -config -f C:¥TAMCSS¥TAMCSS.conf -d C:¥TAMCSS¥ -n <server_name> - s remote -S <server_pwd> -P <admin_pwd> -e 365 -r 199

   注: <server_name> を、IBM クライアントの対象 UVM ユーザー名とホスト名に置き換えてください (例: -n DemoUser/MyHostName)。IBM クライアント・ホスト名は、MSDOS プロンプトで「hostname」と入力して見つけることができます。svrsslcfg ユーティリティーは、Tivoli Access Manager サーバー内に有効な項目を作成し、暗号化された通信用に固有の SSL キー・ファイルを提供します。
3. svrsslcfg を実行して、ivacld の位置を TAMCSS.conf ファイルに追加します。

   デフォルトでは、PD Authorization server はポート 7136 で listen します。これは、Tivoli Access Manager サーバー上の ivacld.conf ファイルの ivacld スタンザにある tcp_req_port パラメーターを調べることによって確認できます。ivacld ホスト名が正しいことが重要です。この情報を取得するには、pdadmin server list コマンドを使用します。サーバー名は **server_name-host_name** です。次は、pdadmin server list の実行例です。

```
MSDOS> pdadmin server list   ivacld-MyHost.ibm.com
```

その後で、次のコマンドを使用して、上で表示された ivacld サーバーのレプリカ・エントリーを追加します。ivacld は、デフォルト・ポート 7136 上で listen していることを前提とします。

```
svrsslcfg -add_replica  -f config file path -h host_name MSDOS>svrsslcfg
-add_replica  -f C:¥TAMCSS¥TAMCSS.conf -h MyHost.ibm.com
```

IBM クライアントの構成

Tivoli Access Manager を使用して IBM クライアントの認証オブジェクトを管理するには、Client Security Software に付属のコンポーネントである管理者ユーティリティーを使用して、あらかじめ各クライアントを構成しておく必要があります。このセクションでは、IBM クライアントを構成する場合の前提条件と手順について説明します。

前提条件

必ず、表示されている順に次のソフトウェアを IBM クライアントにインストールしてください。

1. **サポートされている Microsoft Windows オペレーティング・システム。**Tivoli Access Manager を使用すると、Windows XP、Windows 2000、Windows NT® Workstation 4.0 のいずれかが稼動している IBM クライアントの認証要件を管理することができます。
2. **Client Security Software バージョン 5.3 以上。** このソフトウェアをインストールして IBM エンベデッド・セキュリティー・チップを使用可能にすると、Client Security 管理者ユーティリティーを使用して、ユーザー認証を設定し、UVM セキュリティー・ポリシーを編集することができます。Client Security Software のインストールと使用についての包括的な説明は、「*Client Security Software インストール・ガイド*」および「*Client Security Software 管理者ガイド*」を参照してください。

Tivoli Access Manager セットアップ情報の構成

Tivoli Access Manager をローカル・クライアントにインストールしたら、Client Security Software が備えているソフトウェア・コンポーネントである管理者ユーティリティーを使用して、Access Manager のセットアップ情報を構成できます。Access Manager のセットアップ情報は、次の設定値で構成されています。

- 構成ファイルへの絶対パスの選択
- ローカル・キャッシュ・リフレッシュ間隔の選択

IBM クライアントの Tivoli Access Manager セットアップ情報を構成するには、次の手順を実行します。

1. 「**スタート**」 > 「**設定**」 > 「**コントロール パネル**」 > 「**IBM エンベデッド・セキュリティー・サブシステム**」の順にクリックします。
2. 管理者パスワードを入力して、「**OK**」をクリックします。

   パスワードを入力すると、管理者ユーティリティーのメインウィンドウが開きます。
3. 「**アプリケーション・サポートとポリシーの構成**」ボタンをクリックします。

   「UVM アプリケーションとポリシーの構成」画面が表示されます。
4. 「**標準の Windows ログオンを UVM のセキュア・ログオンに置き換える**」チェック・ボックスにチェックマークを付けます。
5. 「**アプリケーション・ポリシー**」ボタンをクリックします。
6. 「 Tivoli アクセス・マネージャー・セットアップ情報」の領域で、TAMCSS.conf 構成ファイルへの絶対パスを選択します。たとえば、`C:¥TAMCSS¥TAMCSS.conf` とします。

   この領域を使用可能にするには、 Tivoli Access Manager をクライアントにインストールする必要があります。
7. 「**ポリシーを編集**」ボタンをクリックします。

   「管理者パスワードの入力」画面が表示されます。

8. 指定のフィールドに管理者パスワードを入力して、「**OK**」をクリックします。

   「IBM UVM ポリシー」画面が表示されます。
9. 「処理」ドロップダウン・メニューから、Tivoli Access Manager を使用して管理するための動作を選択します。
10. 「選択したオブジェクトをアクセス・マネージャーが管理する」チェック・ボックスを選択して、チェック・ボックスの中にチェックマークが表示されるようにします。
11. 「**適用**」ボタンをクリックします。

    変更は次回のキャッシュ・リフレッシュ時に反映されます。変更を即時に反映する場合は、「**ローカル・キャッシュの更新**」ボタンをクリックします。

ローカル・キャッシュ機能の設定および使用

Tivoli Access Manager 構成ファイルを選択したら、ローカル・キャッシュのリフレッシュ間隔を設定できます。セキュリティー・ポリシー情報のローカル・レプリカが、Tivoli Access Manager によって管理された状態で IBM クライアントで保持されます。ローカル・キャッシュの自動リフレッシュは、月数 (0 から 12) または日数 (0 から 30) の増分でスケジュールできます。

ローカル・キャッシュを設定またはリフレッシュするには、以下の手順を実行します。

1. 「**スタート**」 > 「**設定**」 > 「**コントロール パネル**」 > 「**IBM エンベデッド・セキュリティー・サブシステム**」の順にクリックします。
2. 管理者パスワードを入力して、「**OK**」をクリックします。

   「管理者ユーティリティー」ウィンドウが開きます。管理者ユーティリティーの使用法の詳細については、「*Client Security Software 管理者ガイド*」を参照してください。
3. 管理者ユーティリティーで、「**アプリケーション・サポートとポリシーの構成**」ボタンをクリックしてから、「**アプリケーション・ポリシー**」ボタンをクリックします。

   「クライアント・セキュリティー・ポリシー構成の変更」画面が表示されます。
4. 次のいずれかを実行します。
   - この時点でローカル・キャッシュをリフレッシュするには、「**ローカル・キャッシュの更新**」をクリックします。
   - 自動リフレッシュの頻度を設定するには、指定のフィールドに月数 (0 から 12) および日数 (0 から 30) を入力して、「**ローカル・キャッシュの更新**」をクリックします。ローカル・キャッシュがリフレッシュされ、ローカル・キャッシュ・ファイルの有効期限が更新されて、次回の自動リフレッシュの実行期日が表示されます。

Tivoli Access Manager による IBM クライアント・オブジェクトの管理

UVM ポリシーは、1 つのグローバル・ポリシー・ファイルを通じて管理されます。グローバル・ポリシー・ファイル(UVM ポリシー・ファイルと呼びます) に

は、IBM クライアント・システムで実行される処理(たとえば、システムへのログオン、スクリーン・セーバーの消去、電子メール・メッセージの署名) の認証要件が記載されています。

Tivoli Access Manager によって IBM クライアントの認証オブジェクトを管理するには、その前に UVM ポリシー編集を使用してUVM ポリシー・ファイルを編集します。UVM ポリシー編集は管理者ユーティリティーに含まれています。

重要: Tivoli Access Manager によってオブジェクトを管理すると、Tivoli Access Manager のオブジェクト・スペースにオブジェクトの制御権が渡されます。これを行う場合は、Client Security Software を再インストールして、そのオブジェクトに対するローカル制御権を再設定する必要があります。

ローカル UVM ポリシーの編集

ローカル・クライアントの UVM ポリシーを編集する場合は、必ず事前に1 人以上のユーザーが UVM に登録されていることを確認してください。登録がない場合は、ポリシー編集でローカル・ポリシー・ファイルを開くときにエラー・メッセージが表示されます。

ローカル UVM ポリシーを編集し、それが編集されたクライアントにのみ使用します。デフォルトの位置に Client Security をインストールした場合、ローカル UVM ポリシーは ¥Program Files¥IBM¥Security¥UVM_Policy¥globalpolicy.gvm として保管されます。UVM に追加されたユーザーのみが、UVM ポリシー編集を使用できます。

注: 認証オブジェクト(たとえば、オペレーティング・システムのログオン) に指紋を必要とするUVM ポリシーを設定する場合、UVM に追加される各ユーザーは、そのオブジェクトを使用するには指紋を登録していなければなりません。

UVM ポリシー編集を始動するには、管理者ユーティリティーで次の手順を実行します。

1. 「**アプリケーション・サポートとポリシーの構成**」ボタンをクリックしてから、「**アプリケーション・ポリシー**」をクリックします。

   「クライアント・セキュリティー・ポリシー構成の変更」画面が表示されます。
2. 「**ポリシーを編集**」ボタンをクリックします。

   「管理者パスワードの入力」画面が表示されます。
3. 指定のフィールドに管理者パスワードを入力して、「**OK**」をクリックします。

   「IBM UVM ポリシー」画面が表示されます。
4. 「オブジェクトの選択」タブで、「**処理**」または「**オブジェクト・タイプ**」をクリックし、認証要件の割り当て対象にするオブジェクトを選択します。

   有効なアクションの例としては、「システムへのログオン」、「システムのアンロック」、「電子メールの復号化」があります。オブジェクト・タイプの例としては、「ディジタル証明書の獲得」があります。
5. 選択したオブジェクトごとに、「**選択したオブジェクトをアクセス・マネージャーが管理する**」を選択して、そのオブジェクトに対して Tivoli Access Manager を使用可能にします。

重要: Tivoli Access Manager によってオブジェクトを管理すると、Tivoli Access Manager のオブジェクト・スペースにオブジェクトの管理権を移すことになります。後でオブジェクトに対するローカル制御権を再設定するには、Client Security Software を再インストールする必要があります。

注: UVM ポリシーの編集時に「**ポリシーの要約**」をクリックすると、ポリシーの要約情報を表示できます。

6. 「**適用**」をクリックして、変更内容を保管します。
7. 「**OK**」をクリックして終了します。

リモート・クライアント用の UVM ポリシーの編集と使用

複数の IBM クライアントにまたがって UVM ポリシーを使用するには、リモート・クライアント用の UVM ポリシーを編集し保管してから、UVM ポリシー・ファイルを他の IBM クライアントにコピーします。デフォルトの位置に Client Security をインストールした場合、UVM ポリシー・ファイルは ¥Program Files¥IBM¥Security¥UVM_Policy¥remote¥globalpolicy.gvm として保管されます。

この UVM ポリシーを使用する他のリモート IBM クライアントに、次のファイルをコピーします。

- ¥IBM¥Security¥UVM_Policy¥remote¥globalpolicy.gvm
- ¥IBM¥Security¥UVM_Policy¥remote¥globalpolicy.gvm.sig

デフォルトの位置にClient Security Software をインストールした場合、上記のパスのルート・ディレクトリーは ¥Program Files です。リモート・クライアントの ¥IBM¥Security¥UVM_Policy¥ ディレクトリー・パスに両方のファイルをコピーする必要があります。

トラブルシューティングの図

以下の項は、Client Security Software を使用しているときに問題が生じた場合に役立つと考えられるトラブルシューティングの一覧表を示しています。

ディジタル証明書のトラブルシューティングに関する情報

ディジタル証明書の取得中に問題が生じた場合に役立つと考えられるトラブルシューティング情報を、次に示します。

問題の兆候	可能な解決策
ディジタル証明書の要求中に、UVM パスフレーズ・ウィンドウまたは指紋認証ウィンドウが繰り返し表示される	**処置**
ディジタル証明書が取得される前に、UVM セキュリティー・ポリシーは、ユーザーに UVM パスフレーズまたは指紋認証を要求します。ユーザーが証明書を取得しようとすると、UVM パスフレーズまたは指紋スキャンを要求する認証ウィンドウが繰り返し表示されます。	認証ウィンドウが開くたびに、UVM パスフレーズを入力するか、指紋をスキャンします。

問題の兆候	可能な解決策
VBScript または JavaScript™ のエラー・メッセージが表示される	**処置**
ディジタル証明書を要求したときに、VBScript または JavaScript に関連したエラー・メッセージが表示される可能性があります。	コンピューターを再起動して、証明書をもう一度取得します。

Tivoli Access Manager のトラブルシューティングに関する情報

Client Security Software と Tivoli Access Manager の併用による問題が生じた場合に役立つと考えられるトラブルシューティング情報を、次に示します。

問題の兆候	可能な解決策
ローカルのポリシー設定値が、サーバー上のポリシー設定値と対応しない	**処置**
Tivoli Access Manager では、UVM でサポートされていない特定のビット構成ができます。このため、PD サーバーの構成中に、管理者によって行われた設定値がローカルのポリシー要件で上書きされる可能性があります。	これは、既知の制限です。
Tivoli Access Manager のセットアップ設定値にアクセスできない	**処置**
管理者ユーティリティーの「ポリシー・セットアップ」ページ上では、Tivoli Access Manager のセットアップ、およびローカル・キャッシュ・セットアップ設定値にアクセスできません。	Tivoli Access Manager Runtime Environment をインストールします。IBM クライアント上に Runtime Environment がインストールされていない場合、「ポリシー・セットアップ」ページ上の Tivoli Access Manager 設定値が使用可能になりません。
ユーザー用のコントロールが、ユーザーおよびグループの両方に対して有効になってしまう	**処置**
「**ビットのトラバース(Traverse bit)**」がオンの場合、Tivoli Access Manager サーバーの構成中にユーザーをグループに定義すると、ユーザー用のコントロールがユーザーとグループの両方に対して有効になってしまいます。	アクションは不要です。

Lotus Notes のトラブルシューティングに関する情報

Client Security Software と Lotus Notes® の併用による問題が生じた場合に役立つと考えられるトラブルシューティング情報を、次に示します。

問題の兆候	可能な解決策
Lotus® Notes に対する UVM 保護が有効化された後、Notes が自身のセットアップを終了できなくなる	**処置**

問題の兆候	可能な解決策
管理者ユーティリティーを使用して UVM プロテクションを有効化した後には、Lotus Notes がセットアップを終了できなくなります。	これは、既知の制限です。 管理者ユーティリティーで Lotus Notes のサポートを有効にするには、事前に Lotus Notes を構成して稼働の状態にする必要があります。
Notes パスワードを変更しようとしたときにエラー・メッセージが表示される	**処置**
Client Security Software の使用中に Notes パスワードを変更すると、エラー・メッセージが表示される可能性があります。	パスワードの変更を再試行します。それでも解決されない場合は、クライアントを再始動します。
パスワードを無作為に生成した後で、エラー・メッセージが表示される	**処置**
エラー・メッセージが表示されるのは、次のようなことを行った場合です。 • Lotus Notes 構成ツールを使用して、Notes ID に対する UVM プロテクションを設定したとき • Notes を開き、Notes で提供されている機能を使用して Notes ID ファイルのパスワードを変更したとき • パスワードを変更した直後に Notes を閉じたとき	「**OK**」をクリックして、エラー・メッセージを閉じます。これ以外のアクションは不要です。 エラー・メッセージに反して、パスワードは変更されています。新しいパスワードは Client Security Software によって作成される、ランダム生成のパスワードです。Notes ID ファイルは現在、ランダム生成のパスワードで暗号化されるため、新規のユーザー ID ファイルはユーザーにとって必要ありません。エンド・ユーザーがもう一度パスワードを変更すると、UVM は Notes ID 用に新たにランダム生成のパスワードを生成します。

暗号化のトラブルシューティングに関する情報

Client Security Software 3.0 以降を使用してファイルを暗号化しているときに問題が生じた場合に役立つと考えられるトラブルシューティング情報を、次に示します。

問題の兆候	可能な解決策
前に暗号化したファイルが、復号化されない	**処置**
Client Security Software 3.0 以降へのアップグレード後、以前のバージョンのClient Security Software で暗号化されたファイルは、復号化されません。	これは、既知の制限です。 Client Security Software 3.0 以降をインストールする*前*に、以前のバージョンの Client Security Software を使用して暗号化されたファイルをすべて、復号化する必要があります。以前のバージョンの Client Security Software を使用して暗号化されたファイルは、そのファイルの暗号のインプリメンテーションが変更されてしまっているため、Client Security Software 3.0 では復号化できません。

第 7 章 IBM Client Security Software を補完するためのサード・パーティーのハードウェア・デバイス・ドライバーのインストール

Client Security にサード・パーティー・ソリューションをインストールすると、社内のコンピューター環境に合わせてプロテクションのレベルを調整するための追加の機能を統合して、インフラストラクチャー全体を保護することができます。

IBM エンベデッド・セキュリティー・サブシステムは、以下の製造元のセキュリティー認証ハードウェアに適合していることがテストにより確認済みです。

- Targus 製の指紋読取装置
- Gemplus 製のスマート・カード・ソリューション

上記の製造元の製品の詳細については、製造元へのリンクが含まれている http://www.ibm.com/jp/pc/security/css/css.html にアクセスしてください。

ディスク・イメージの一部となる多くのコンポーネントと同様に、インストールの順序が非常に重要です。上記の認証装置や関連ドライバー、および他のソフトウェアをデプロイメントする予定の場合、最初に IBM Client Security Software をインストールする必要があります。デバイス・ドライバーより以前に CSS がハードディスクに存在しないと、認証デバイスのドライバーおよびソフトウェアが正常にインストールされません。

認証デバイスのソフトウェアおよびドライバーのインストール方法と最新情報については、デバイスに付属のマニュアルをお読みください。

© Copyright IBM Corp. 2004

第 8 章 リモート側で新規または改訂されたセキュリティー・ポリシー・ファイルをデプロイする

セキュリティー・ポリシーを更新する場合でも、異なるコンピューター用に異なるポリシーを作成する場合でも、署名の権限を持つ IT 管理者はポリシー・ファイルを改訂してデプロイできます。ポリシー・ファイルを、ACAMUCLI.EXE を使用して編集してください。(「コントロール パネル」で IBM Security Subsystem アイコンをダブルクリックして、ポリシーを編集することもできます。)

「適用」をクリックした後に、表示中の指示に従ってポリシー・ファイルに署名します。(**注:** 管理者秘密鍵が分割されている場合、ポリシー・ファイルに署名するには、すべてのコンポーネントを入力する必要があります。) 編集したファイルは、GLOBALPOLICY.GVM および GLOBPOLICY.GVM.SIG になります。これらのファイルを適切なユーザーに分散して、Security¥UVM_Policy フォルダーに保管されていることを確認します。

デプロイメントの後に、パスフレーズ・ポリシーをリモート側で更新できます。ユーザーが次回パスフレーズを変更する場合に、パスフレーズ・ポリシー・ファイルを更新してパスフレーズ要件を変更できます。管理者は、ユーザーにパスフレーズ変更を強制した後の期間を定義できます。この有効時間は、ユーザーの登録時に定義します。たとえば、管理者がユーザー Jane を登録したときの初期のポリシーでは、パスワードの長さが 8 文字、有効期限が 30 日に設定されていたとします。管理者は、ポリシー・ファイルを更新して、Jane がパスフレーズを次に変更するときに、新しいパスフレーズの長さを 12 文字にするよう要求することができます。また、管理者は有効期限の期間を変更することもできます。たとえば、管理者はジェーンにパスフレーズを 30 日ごとではなく 15 日ごとに変更するよう要求できます。次のシナリオではどうなるでしょうか? 30 日間のパスフレーズの「寿命」のうち、10 日目になります。新しいパスフレーズ・ポリシー・ファイルは、クライアント・コンピューターに送信され、パスフレーズを 15 日ごとに変更するよう要求します。パスフレーズの有効期限は、5 日後または 20 日後のどちらで切れるでしょうか。パスフレーズは、オリジナルのポリシーに従って 20 日後に有効期限が切れます。パスフレーズの有効期限ポリシーは、パスフレーズが設定された時点で有効になります。15 日間に変更するポリシーは、ジェーンが 20 日後にパスフレーズを変更した時点から開始します。

要求されたパスフレーズの特性を変更する場合は、上記の指示に従ってください。次に、SECURITY¥UVM_POLICY フォルダーから UVM_PP_POLICY.DAT および UVM_PP_POLICY.DAT.SIG ファイルを配布します。

© Copyright IBM Corp. 2004

付録. 特記事項

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書で説明される製品は、誤動作により人的な傷害または死亡を招く可能性のある移植またはその他の生命維持アプリケーションで使用されることを意図していません。本書に記載される情報が、IBM 製品仕様または保証に影響を与える、またはこれらを変更することはありません。本書の内容は、IBM またはサード・パーティーの知的所有権のもとで明示または黙示のライセンスまたは損害補償として機能するものではありません。本書に記載されている情報はすべて特定の環境で得られたものであり、例として提示されるものです。他の稼働環境では、結果が異なる場合があります。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

© Copyright IBM Corp. 2004

IBM 以外の Web サイト

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

商標

以下は、IBM Corporation の商標です。

IBM
ThinkPad
ThinkCentre
Tivoli

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。