IBM Client Security Software バージョン 5.30
デプロイメント・ガイド

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 Version 5.30 Deployment Guide
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 2004.8

まえがき

IBM® Client Security Software のデプロイメントでは、IT 管理者はさまざまな要素を理解し、計画を立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・サブシステム、エンベデッド・セキュリティー・チップ、または Client Security Software の使用方法について説明するためのものではありません。本書では、エンベデッド・セキュリティー・チップを装着した社内のコンピューターにソフトウェアをデプロイメントする方法について説明します。

本書の対象読者

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 5.3 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。アプリケーション自体の使用法については、IBM が提供する「ユーザーズ・ガイド」、「管理者ガイド」、および Client Security Software のアプリケーション・ヘルプを参照してください。

製品の資料

Client Security Software バージョン 5.3 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 バージョン 5.3 管理者ガイド*

  Client Security Software で提供されているセキュリティー機能のセットアップおよび使用方法が記載されています。

- *Client Security Software バージョン 5.3 ユーザーズ・ガイド*

  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 5.3 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 ネットワーク・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。

- *Tivoli® Access Manager での Client Security Software バージョン 5.3 の使用法*

  Tivoli Access Manager での Client Security Software のセットアップについて記載されています。

その他の情報

その他の情報およびセキュリティー製品の更新がある場合は、IBM Web サイト http://www.ibm.com/jp/pc/security/ から取得できます。

目次

第 1 章 IBM Client Security Software をデプロイメントする前の考慮事項

IBM Client Security Software (CSS) は、さまざまな方法でデプロイメントできます。CSS は、IBM パーソナル・コンピューターに統合されている IBM エンベデッド・セキュリティー・サブシステム (ESS) ハードウェアを使用します。本書は、読者がご使用の環境に ESS をデプロイメントする方法を決定するのをサポートします。重要な点として、イメージ作成の方法から、エンド・ユーザーへの PC の支給方法まで、社内でのコンピューターのデプロイメントのプロセスを理解しておく必要があります。このプロセスにより、ESS をデプロイメントする方法が大きく異なってくるからです。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

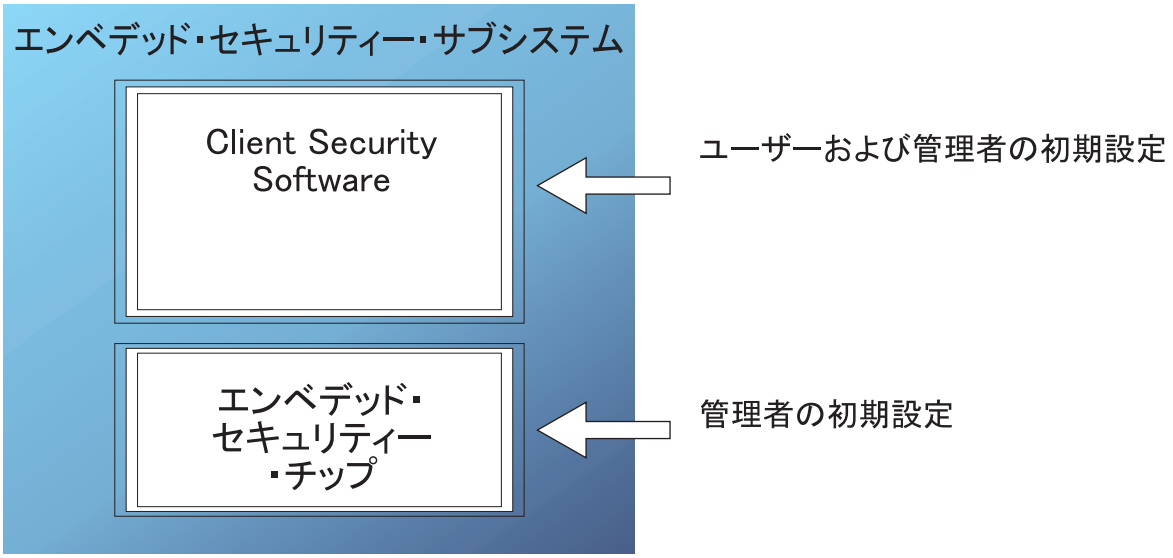

図 1. IBM Client Security System のコンポーネント

デプロイメントの要件および仕様

エンベデッド・セキュリティー・チップが装着されたコンピューターに IBM Client Security Software をインストールする場合は、サーバー記憶域、ダウンロードおよびインストールに関する以下の要件に注意してください。

1. IBM PC にエンベデッド・セキュリティー・チップが装着されている必要があります。
2. インストール可能なコードに必要なサーバー・ストレージは約 12 MB です。

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 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 つの主要コンポーネントで構成されています。

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

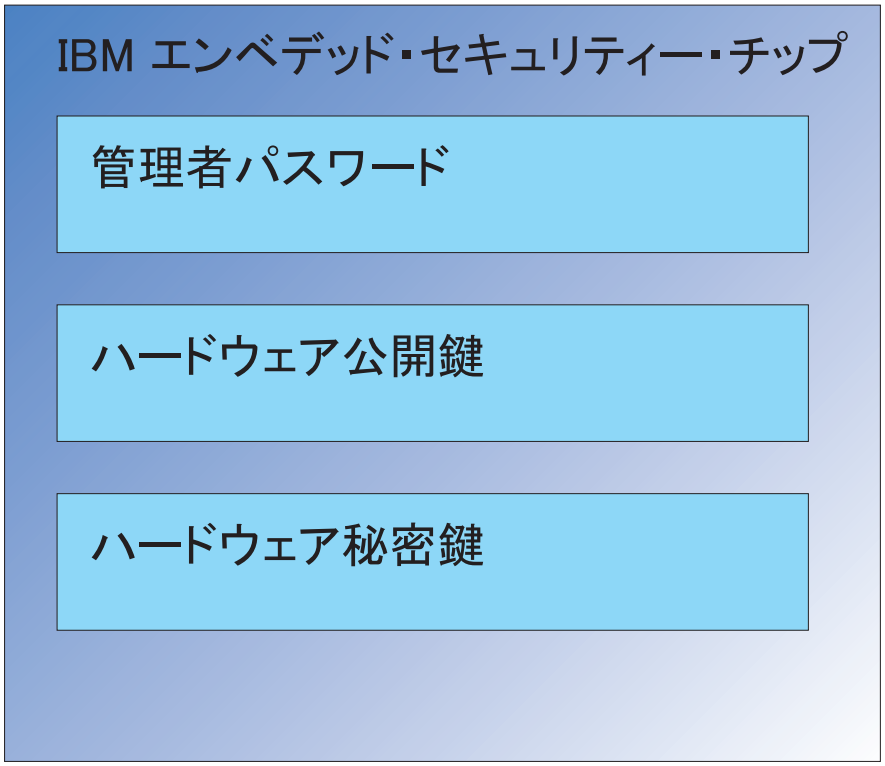

図 2. IBM エンベデッド・セキュリティー・チップに保持されるデータ

ハードウェア公開鍵および秘密鍵は、すべてのコンピューターの間で固有です。ハードウェア秘密鍵はチップから抽出することはできません。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

- 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、エンベデッド・セキュリティー・チップの機能を最大限に利用するために、追加のユーザーを使用可能にする場合があります。Client Security Software をインストールすると、管理者パスワードが設定されます。管理者パスワードが設定される方法とタイミングについては、本書で後ほど説明します。

重要: 管理者パスワードを管理するためのストラテジーを作成してください。このストラテジーは、ESS を最初に構成するときには確立されている必要があります。IT 管理者またはセキュリティー管理者が決定すれば、エンベデッド・セキュリティー・チップを搭載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ことができます。別の方法として、部門または建物ごとに別の管理者パスワードを割り当てることもできます。

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。

それぞれのコンピューターが固有のハードウェア公開鍵および固有の秘密鍵を持つようになります。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。

5 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。 5 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。以下では、公開鍵と秘密鍵の概要を説明します。

- 公開鍵と秘密鍵は、両方合わせて「鍵ペア」と呼ばれます。
- 公開鍵と秘密鍵は、以下のように数学的な関連があります。
  - 公開鍵で暗号化されたデータは、対応する秘密鍵でのみ復号化できます。
  - 秘密鍵で暗号化されたデータは、対応する公開鍵でのみ復号化できます。
  - 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、秘密鍵を引き出すことはできません。
  - 公開鍵は通常、すべての人が使用可能です。
- 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。

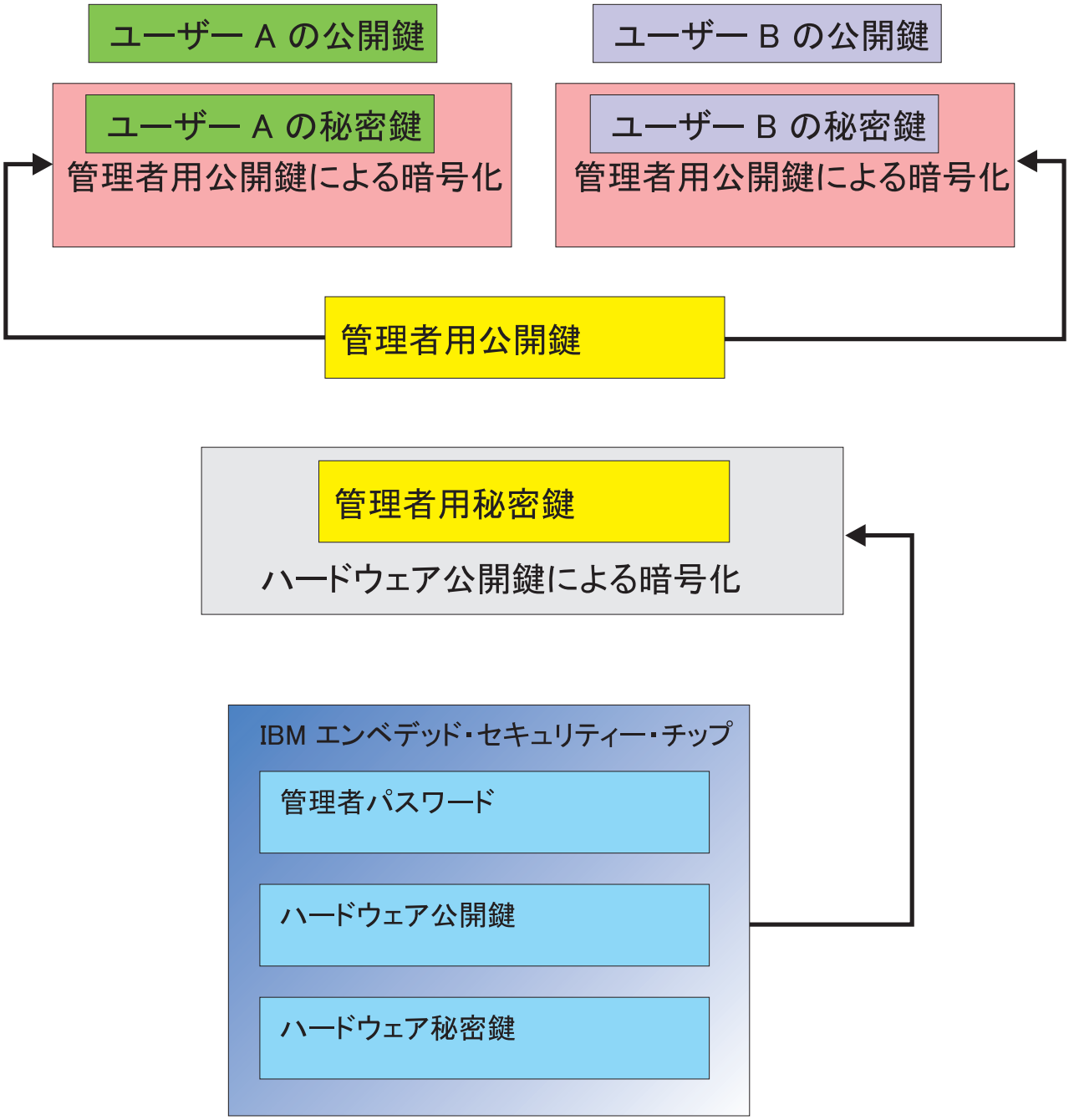

図 3. 複数の暗号化レイヤーによる強固なセキュリティー

鍵スワッピング階層

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。この仕組みの詳細は「*管理者ガイド*」に記載されていますが、マス・デプロイメント、デプロイメント、および管理に関係しているため、本書では概念について説明します。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。前述のとおり、これらの鍵は Client Security Software によって作成、それぞれのクライアント上で統計的に固有です。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。管理者公開鍵と秘密鍵のペアは、すべてのコンピューターの間で固有にすることも、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上で共通にすることもできます。それぞれの利点と欠点については、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。

- ユーザー公開鍵および秘密鍵を保護する
- ユーザー証明書のアーカイブおよび復元を使用可能にする
- ユーザー・クレデンシャル・ローミングを使用可能にする (「*管理者ガイド*」を参照)。

鍵のスワッピングを使用する理由

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。ここでは、各ユーザーが公開鍵と秘密鍵を持っている場合を考えます。ユーザーの秘密鍵は、管理者公開鍵によって暗号化されています。 5 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。このように、さまざまな秘密鍵について考える必要があるのはなぜでしょうか。

その理由を理解するには、前述の階層に注目する必要があります。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。この事例では、ハードウェア公開鍵および秘密鍵だけが、ブートからブートまでの持続鍵です。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内にスワッピングすると、チップ内の保護環境で秘密鍵を復号化し、使用できるようになります。

管理者秘密鍵は、ハードウェア公開鍵を使用して暗号化します。管理者秘密鍵を復号化するときは、チップ内で唯一使用可能なハードウェア秘密鍵を使用します。チップ内で管理者秘密鍵が暗号化されると、ユーザー秘密鍵 (管理者公開鍵によって暗号化) をハード・ディスクからチップ内に渡し、管理者秘密鍵を使用して復号化することができます。 5 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 3 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。

8 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。

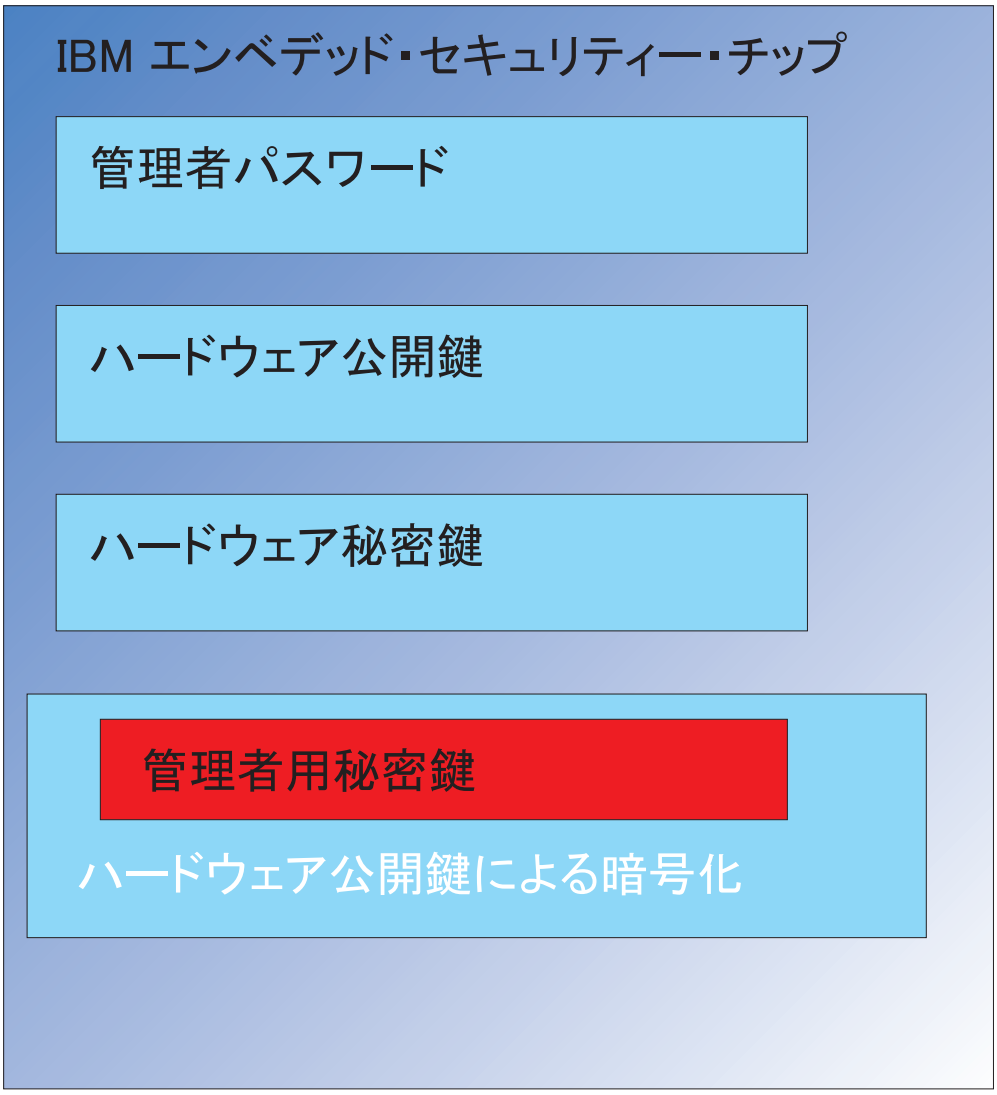

図 4. ハードウェア公開鍵により暗号化された管理者秘密鍵が、エンベデッド・セキュリティー・チップにロードされる

9 ページの図 5 のとおり、チップ上でのみ使用可能なハードウェア秘密鍵により管理者秘密鍵は復号化されます。これで、管理者秘密鍵は、チップ内で使用可能になります。

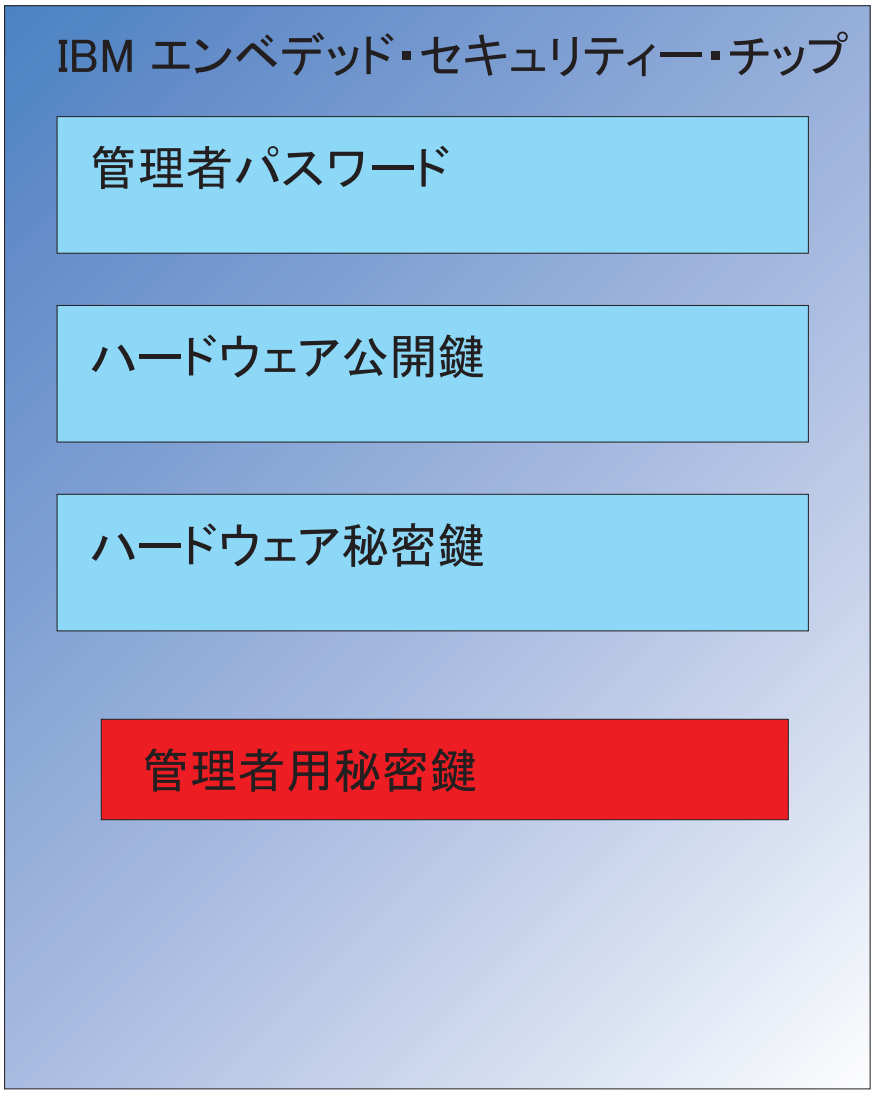

図 5. 管理者秘密鍵がセキュリティー・チップ内で使用可能になる

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。 10 ページの図 6 をご覧ください。

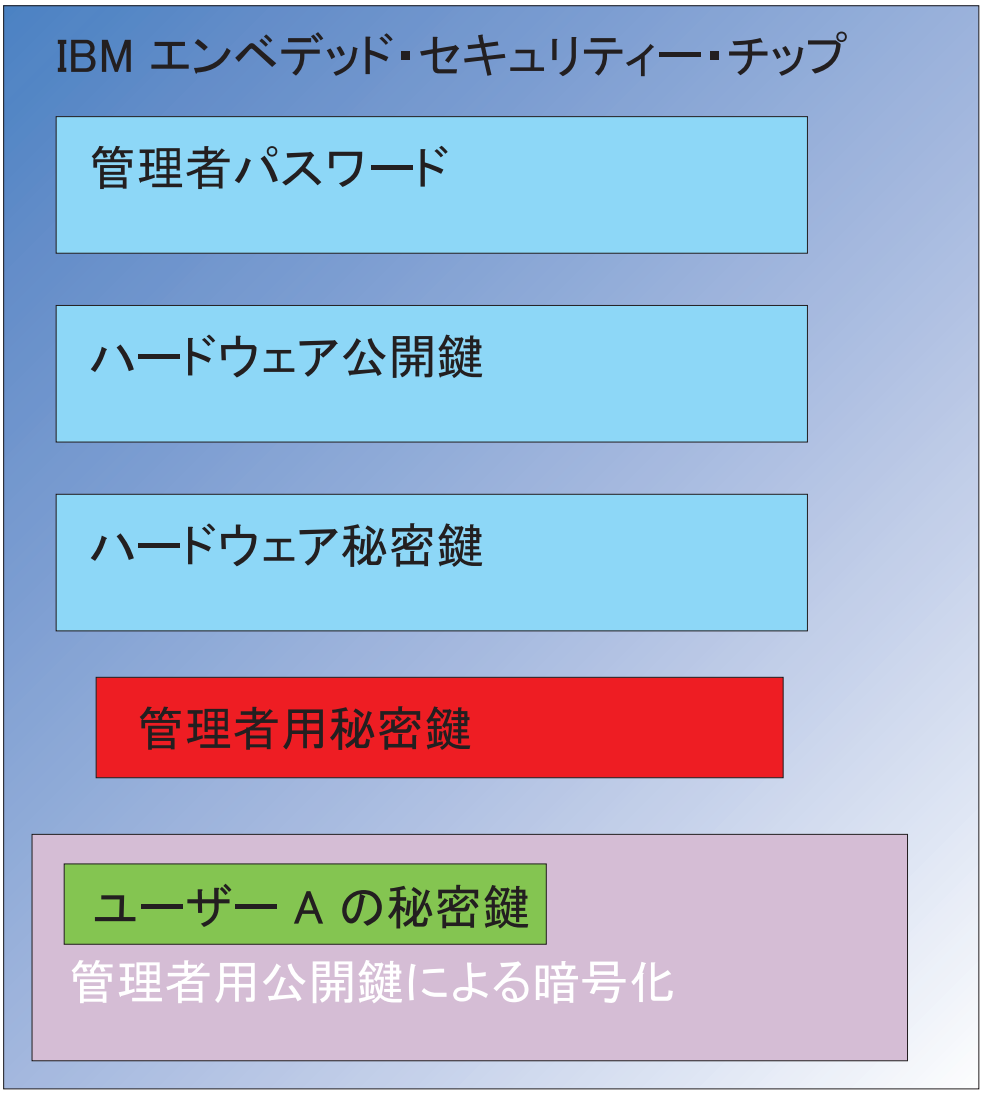

図 6. ユーザー A の秘密鍵 (管理者公開鍵で暗号化) がセキュリティー・チップに渡される

ユーザー A の秘密鍵を復号化するときは、管理者秘密鍵が使用されます。これで、ユーザー A の秘密鍵が使用可能になります。 11 ページの図 7 をご覧ください。

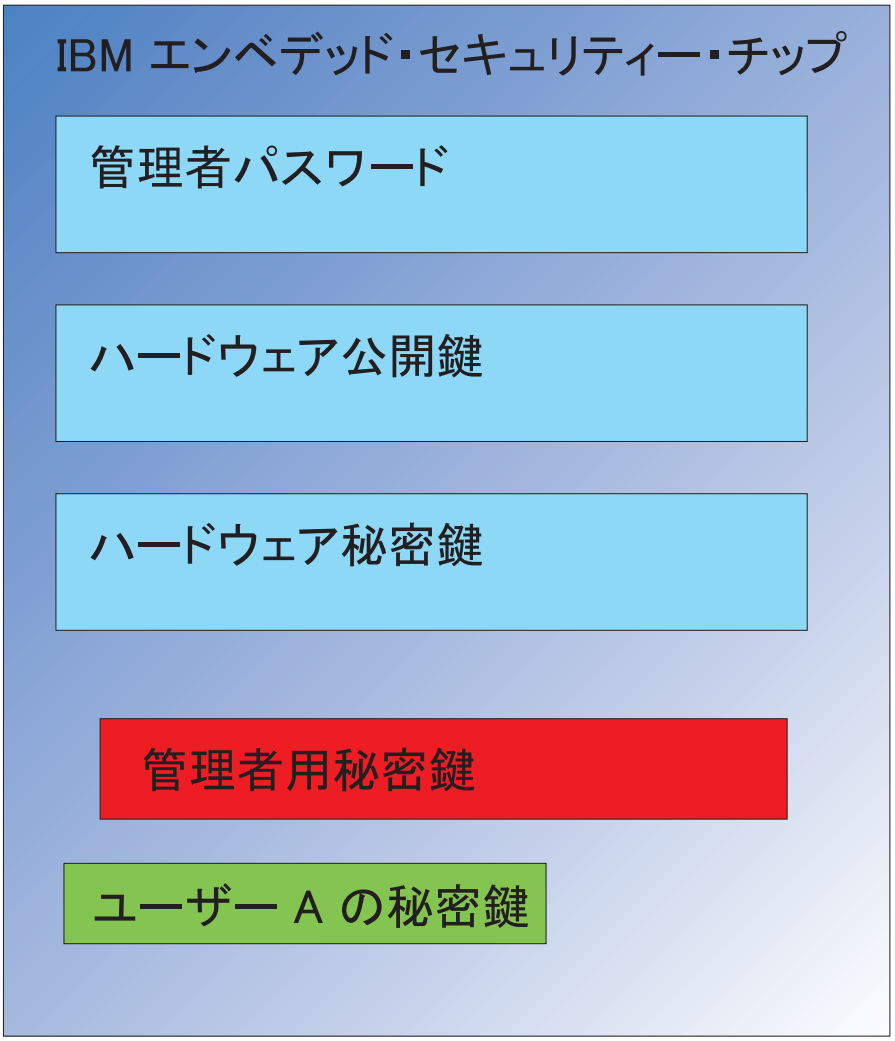

図 7. ユーザー A の秘密鍵が使用可能になる

他にも、ユーザー A の公開鍵を使用して暗号化できる鍵がいくつかあります。その 1 つは、電子メールの署名に使用する秘密鍵です。ユーザー A が署名済みの電子メールを送信する場合、署名するときに使用した秘密鍵 (ユーザー A の公開鍵で暗号化) がチップに渡されます。署名で使用されたユーザー A の秘密鍵を復号化するときは、チップ内のユーザー A の秘密鍵が使用されます。これで、チップ内のユーザー A の署名用の秘密鍵を使用して、目的の操作、つまりこの場合はディジタル署名の作成 (ハッシュを暗号化) を行うことができます。ユーザー B がコンピューターにログオンした場合も、同じプロセスで、チップへの鍵の出し入れが行われます。

管理者鍵ペアを使用する理由

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の間で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。12 ページの図 8 をご覧ください。

重要: 管理者鍵ペアを管理するためのストラテジー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決定すれば、エンベデッド・セキュリティー・チッ

プを搭載した各コンピューターに同じ管理者鍵ペアを設定することができます。別の方法として、部門または建物ごとに別の管理者鍵ペアを割り当てることもできます。

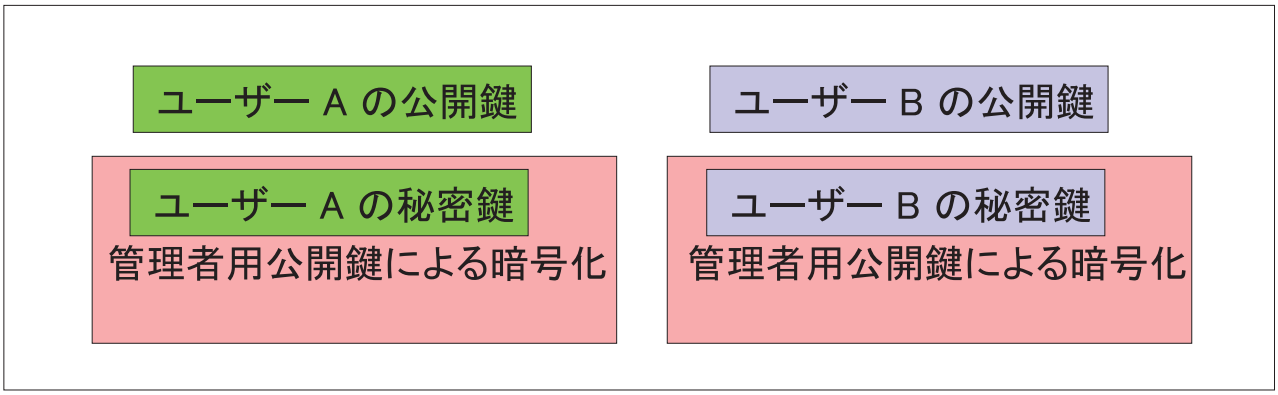

図 8. ユーザー固有の秘密鍵情報は管理者公開鍵によって暗号化される

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・ファイルを署名できることです。これにより、管理者以外の人がセキュリティー・ポリシーを変更するのを阻止できます。クライアント・セキュリティー・ポリシー・ファイルに高度なセキュリティーを適用するために、管理者秘密鍵を最大 5 人の間で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および暗号化するときは、秘密鍵の一部を持っている 5 名が全員揃う必要があります。これにより、1 人の人が管理者機能を一方的に実行するのを防ぐことができます。管理者秘密鍵の分割については、38 ページの表 4 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は、クライアントのインストール中に、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・ロケーションのユーザー・データは、管理者公開鍵により暗号化されます。ユーザーにデータのアーカイブを取らせても、管理者がデータをアンロックする管理者秘密鍵を持っていなければ意味がありません。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。アーカイブ秘密鍵は暗号化されないので注意してください。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

前述のとおり、管理者公開鍵および秘密鍵の重要な機能の 1 つは、ディスク内容のバックアップおよび復元機能です。この機能は、10 から15 で示されています。手順は以下のとおりです。

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。 14 ページの図 10 をご覧ください。

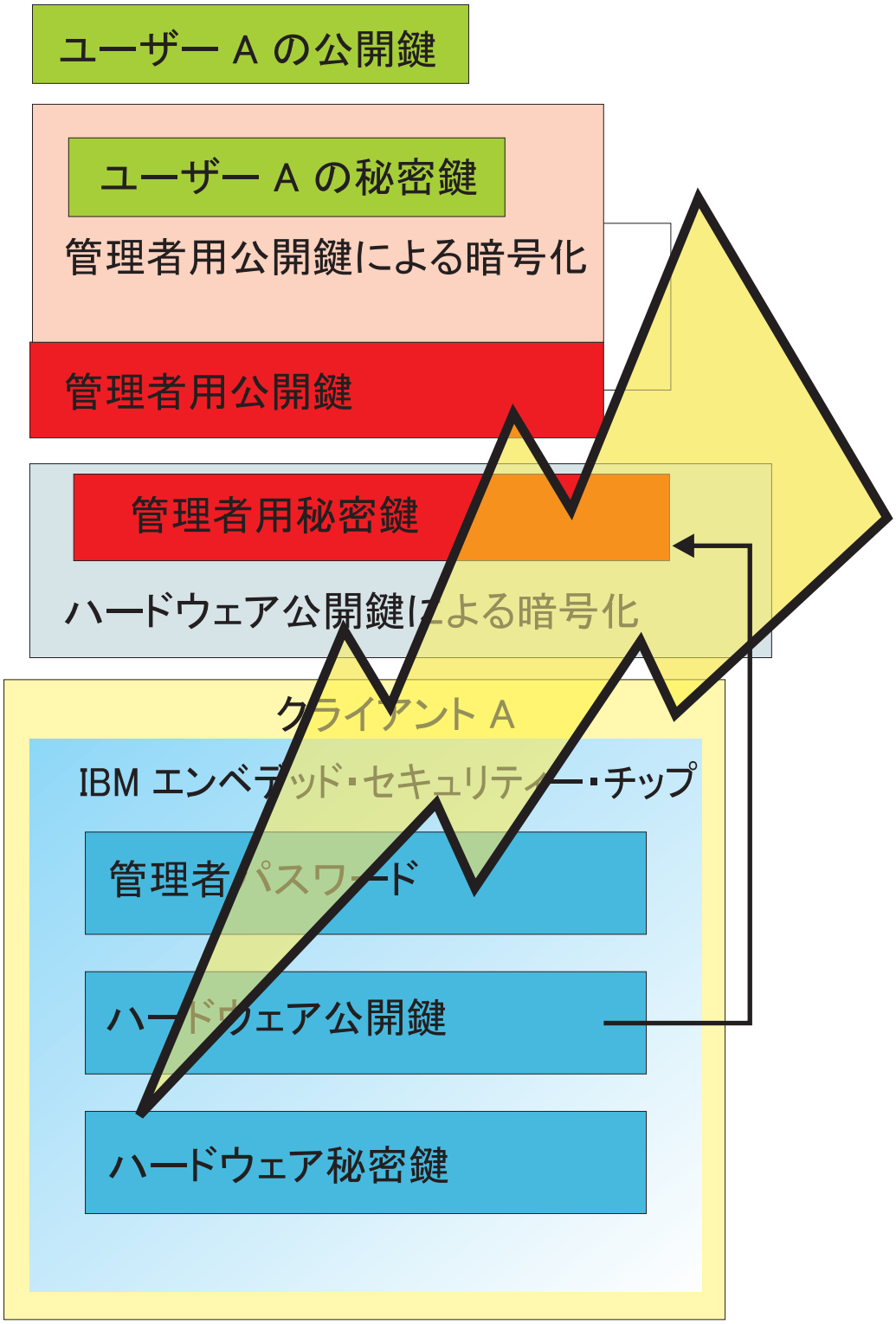

図 10. ユーザー A のコンピューターが落雷の影響で使用不可になる

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。 15 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。

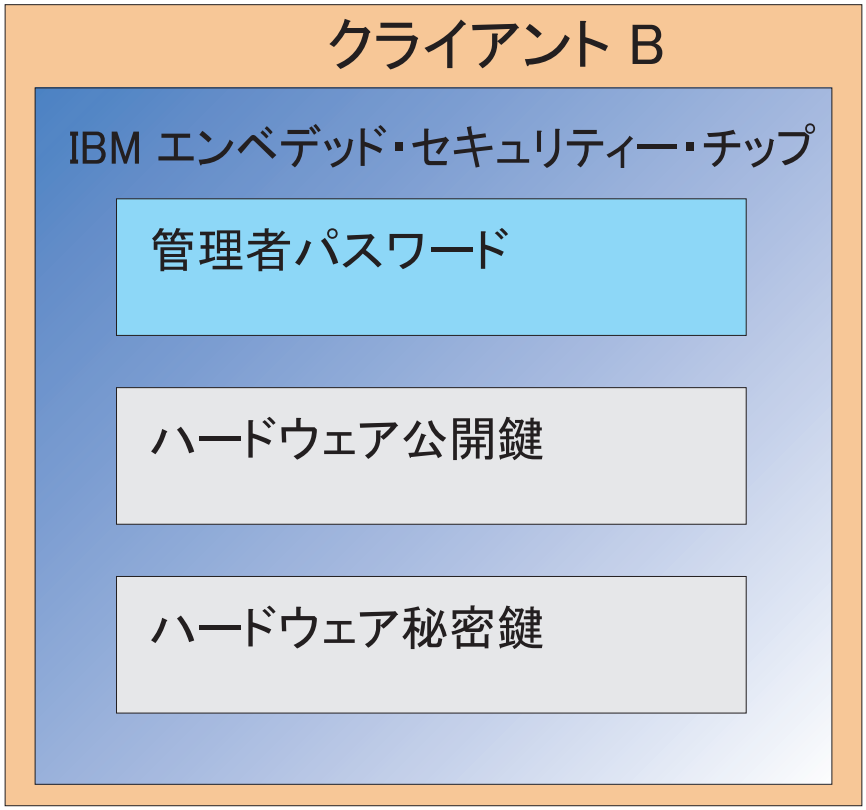

図 11. ユーザー A は、新しいエンベデッド・セキュリティー・チップを搭載した新しいコンピューター、クライアント B を受け取る

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。 12 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 で使用可能にするには、管理者公開鍵と秘密鍵をこのマシンに転送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。

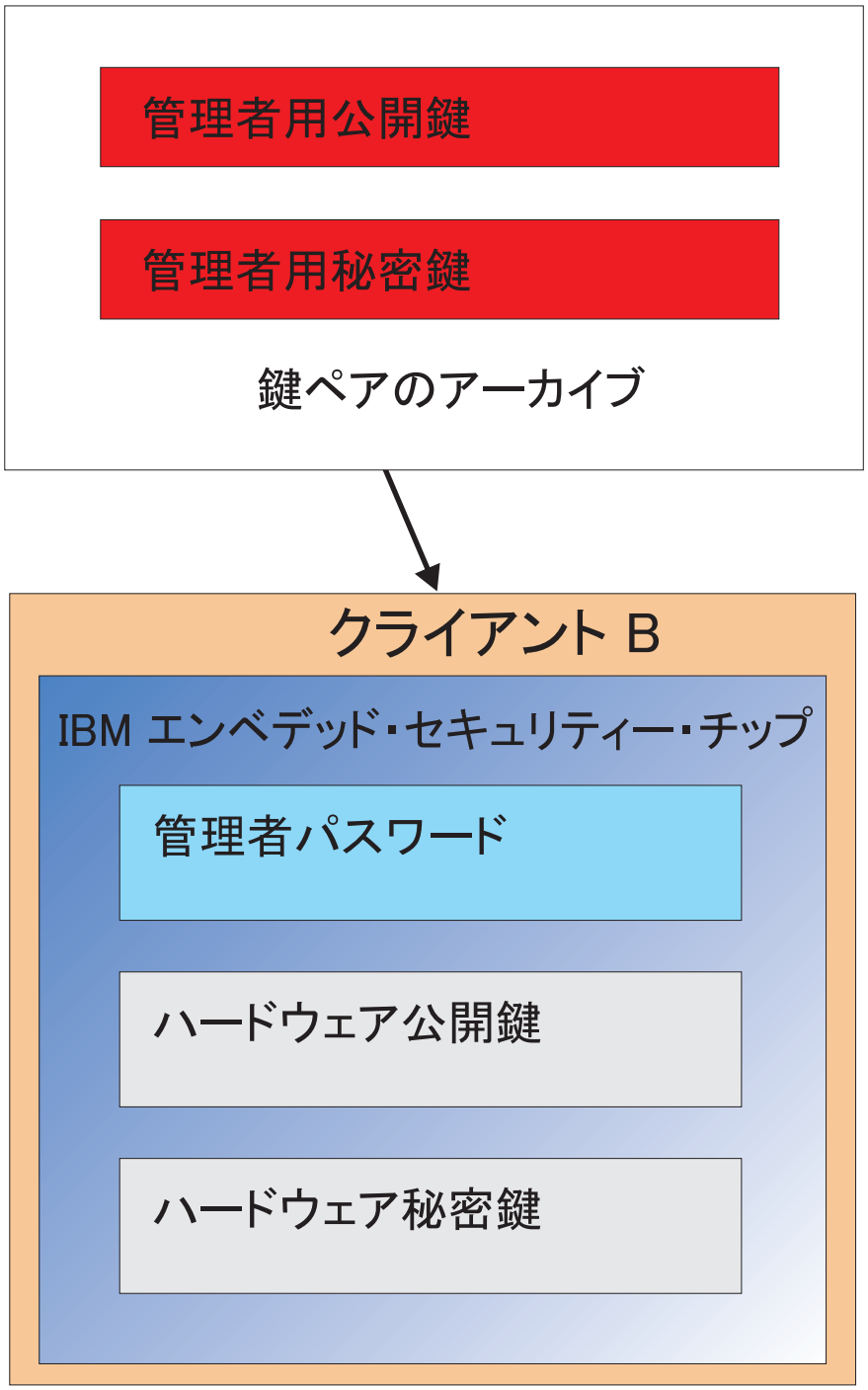

図 12. クライアント B はアーカイブ・ロケーションから管理者公開鍵と秘密鍵を取得する

4. 17 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。

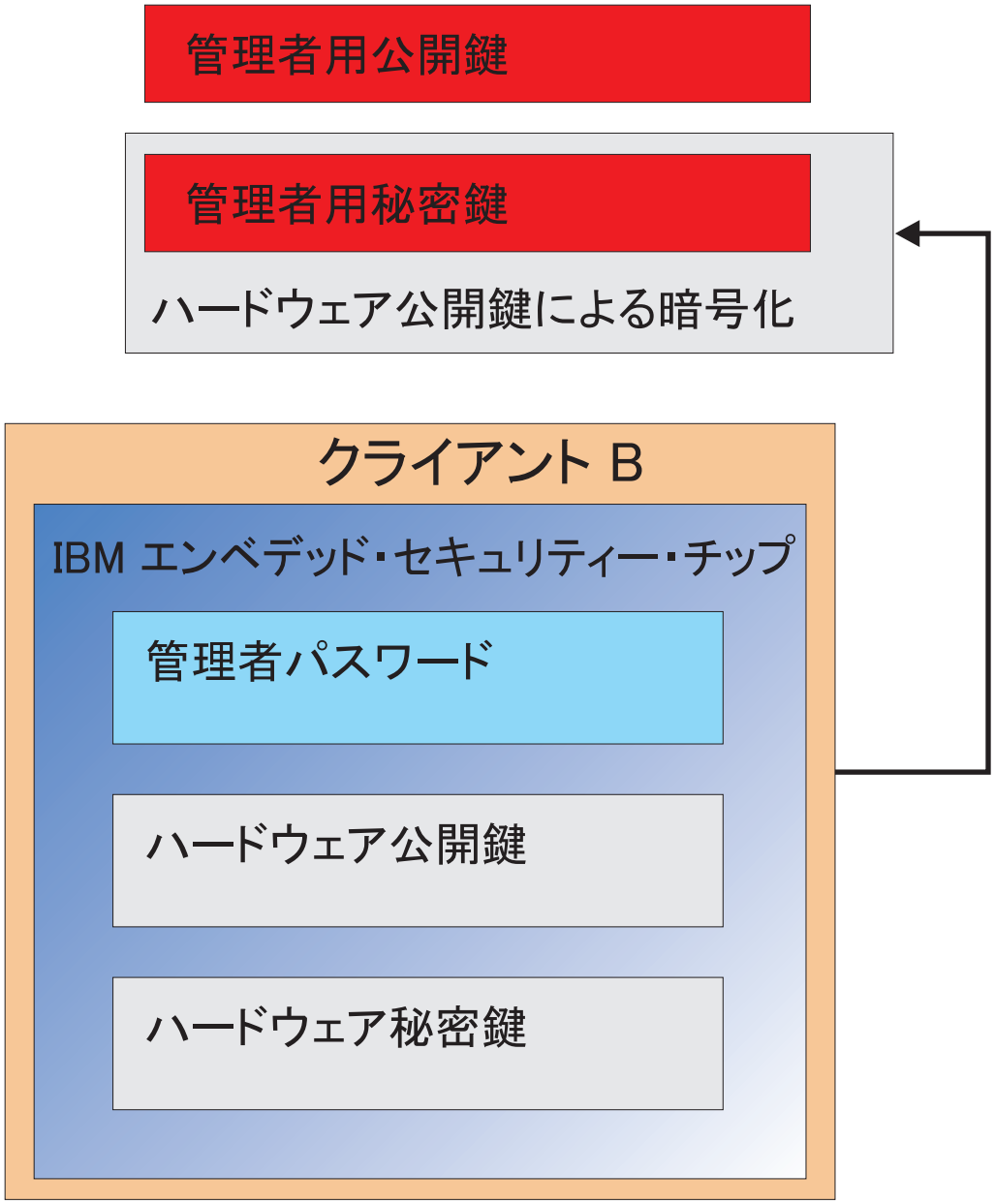

図 13. 管理者秘密鍵はクライアント B のハードウェア鍵により暗号化される

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、18 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。

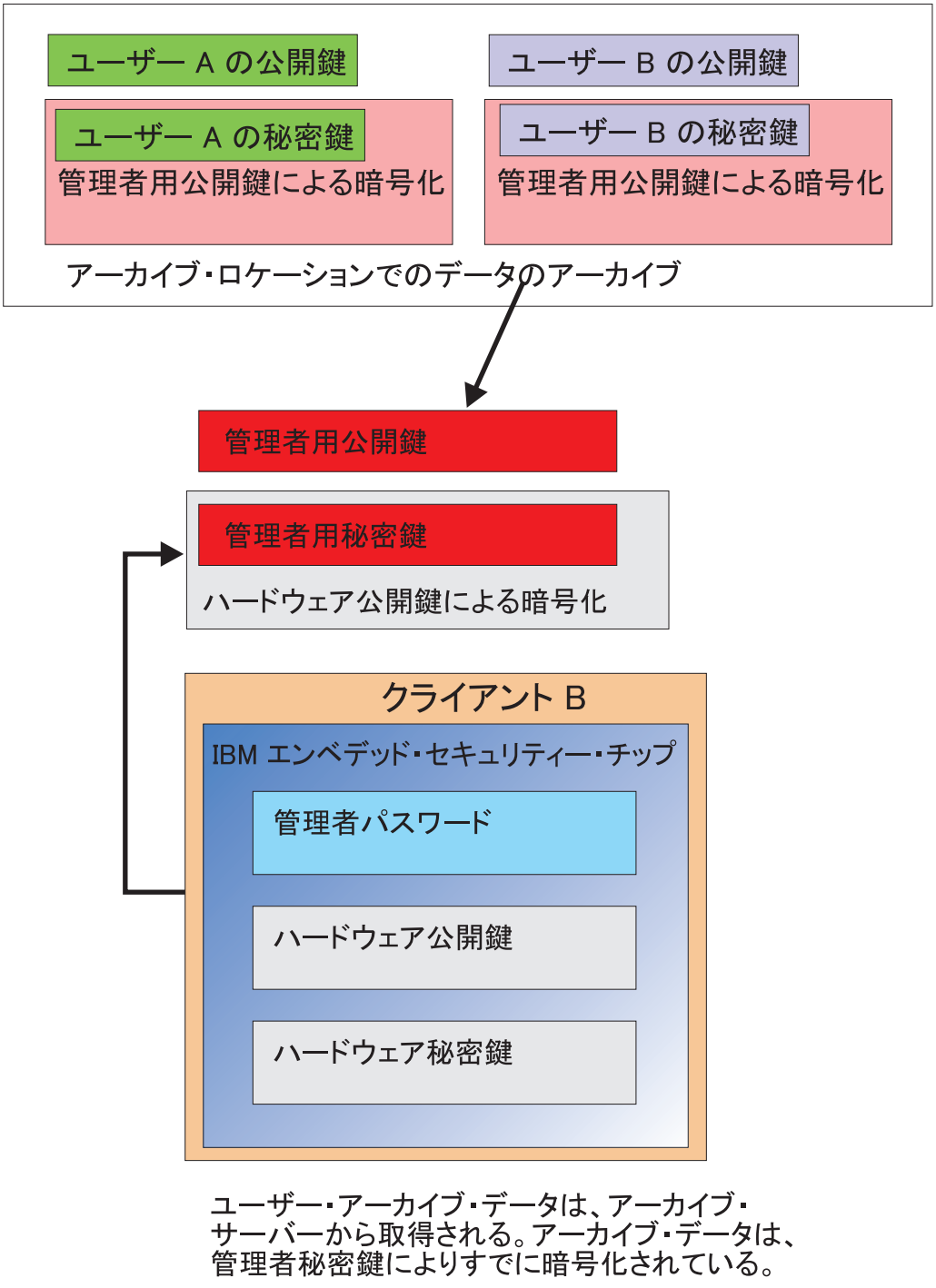

図 14. 管理者秘密鍵を暗号化した後、ユーザー A の証明書をクライアント B にロードできる

19 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、破ることはほぼ不可能です。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。つまり、アーカイブ鍵ペア (管理者公開鍵および秘密鍵)、特に管理者秘密鍵が安全に保

管されているかぎり、ユーザー証明書のアーカイブの場所はどこにあってもかまいません。

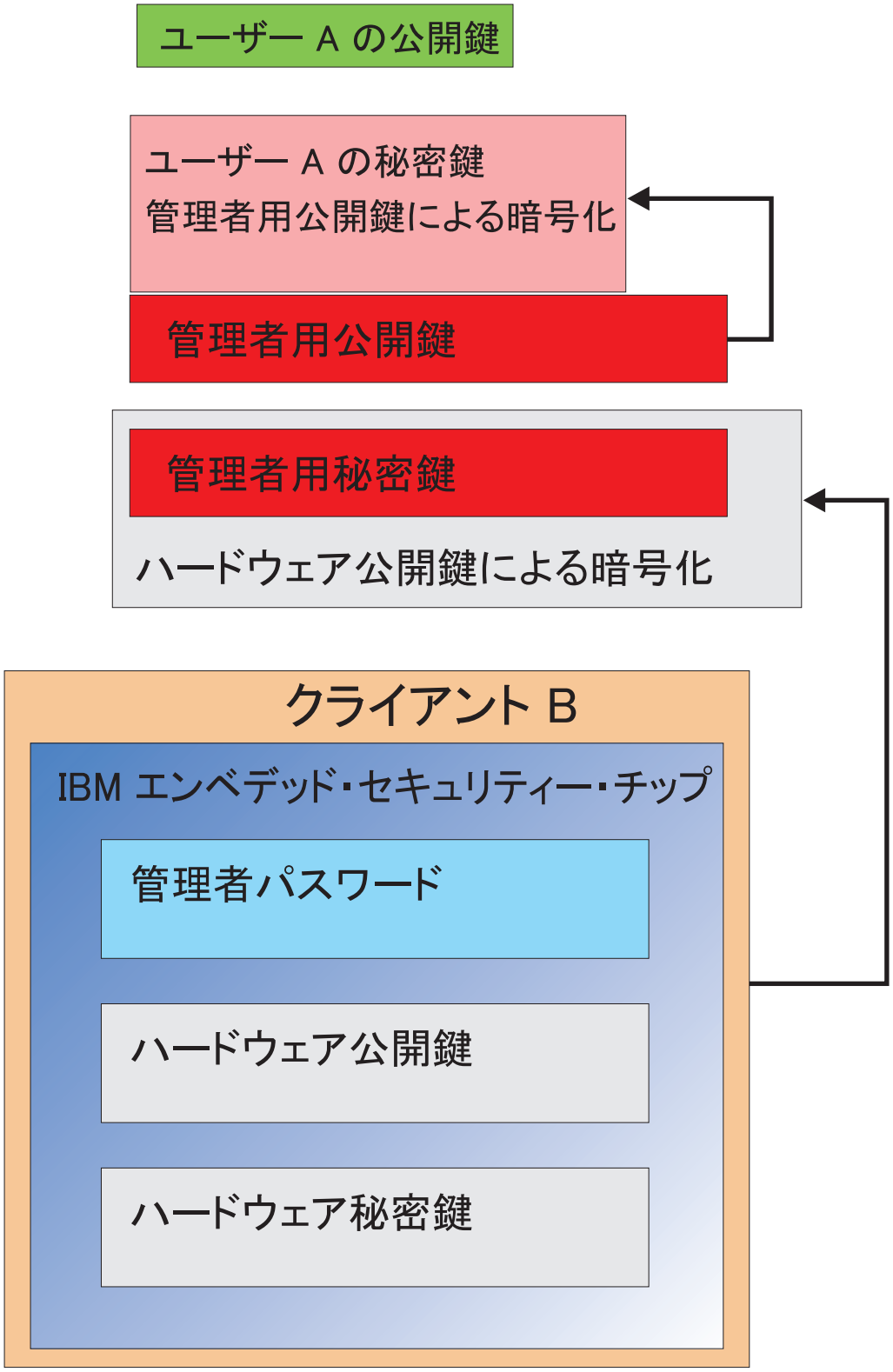

図 15. ユーザー A はクライアント B で完全に復元される

管理者パスワードの設定方法、およびアーカイブの場所の決定方法など、詳細については、ソフトウェアのインストールに関するセクションで説明します。図 16 は、ESS 環境でのコンポーネントの概要を示しています。重要な点として、各クライアントは、ハードウェア公開鍵および秘密鍵の側から見ると固有ですが、実際には共通の管理者公開鍵および秘密鍵を持っています。クライアントのアーカイブの場所はすべて共通ですが、このアーカイブの場所は、セグメントごとに定義することも、ユーザーのグループごとに定義することもできます。

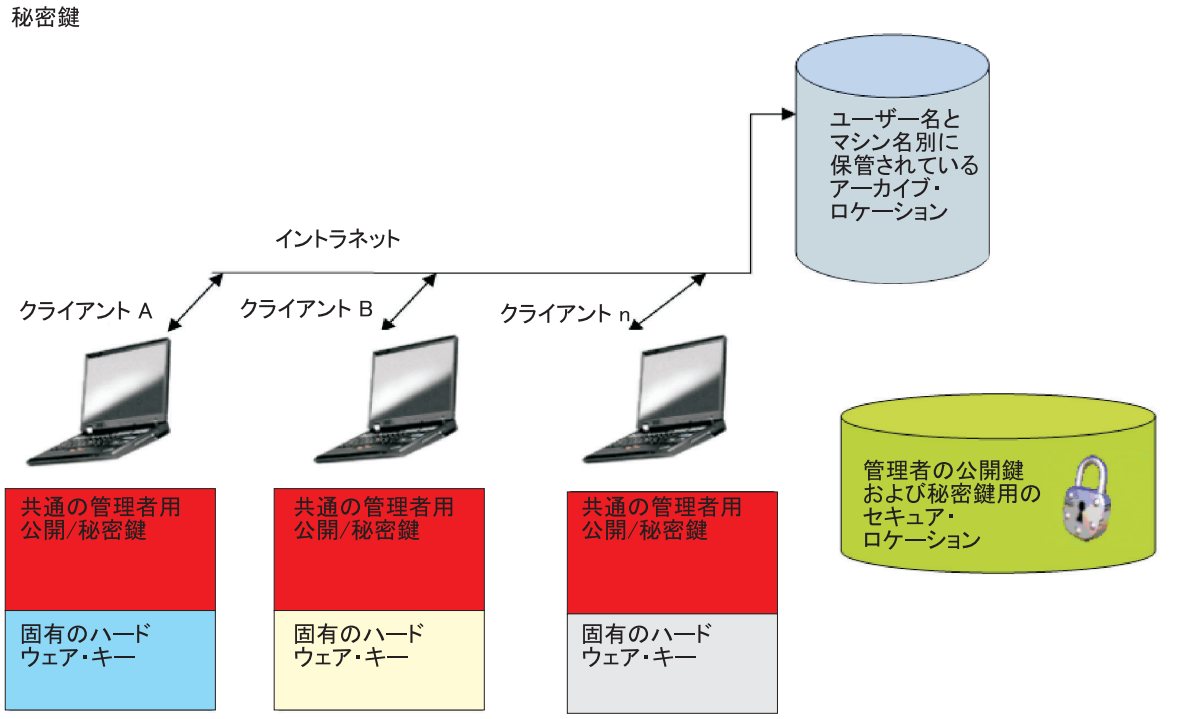

図 16. IBM Client Security System の主要コンポーネント

次の例を考えてください。人事部門は、技術部門とは別の場所に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: 同じ場所に保存するコンピューター名とユーザー名は、それぞれ固有でなければなりません。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 4 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
- セットアップ・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・ルールの設定
- 紛失したパスフレーズのリセット
- 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・ベースではなくマシン・ベースです。ポリシーは 1 台のコンピューター上のすべての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。ユーザーを登録する方法はいくつもありますが、その詳細については本書で後述します。このセクションでは、ユーザーが登録したときに行われる処理について説明します。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
- 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。最低でも 1 つのパスフレーズが必要です。ESS 環境の UVM コンポーネント (ユーザー側から見ると、UVM が認証を管理し、セキュリティー・ポリシーを適用する) 内のすべてのユーザーがパスフレーズを必要としており、このパスフレーズは少なくともコンピューターを開始するときに一度入力する必要があります。以下のセクションでは、パスフレーズの必要性、セットアップ方法、および使用方法について説明します。

パスフレーズの必要性

簡単に説明すると、パスフレーズはセキュリティーを確保するために必要です。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。しかし、チップにアクセスするのに必要な認証が弱いと、ハードウェア・チップを追加してもさほど効果はありません。たとえば、セキュリティー機能を持つハードウェア・チップを導入したとします。ただし、チップによるアクションを呼び出すのに必要な認証は 1 桁です。この場合、ハッカーは、0 から 9 までの 1 桁の数字を当てるだけで、他人の証明書を使用してアクションを呼び出すことができます。認証が 1 桁だとチップのセキュリティーは弱いため、ソフトウェア・ベース・ソリューションにはほとんど利点がないことになります。ハードウェア保護に関連して強固な認証がないのであれば、セキュリティー上の効果は全くありません。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。 3 ページの『第 2 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。ユーザーの秘密鍵にも、1 つのパスフレーズが関連付けられています。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のものです。 23 ページの図 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。

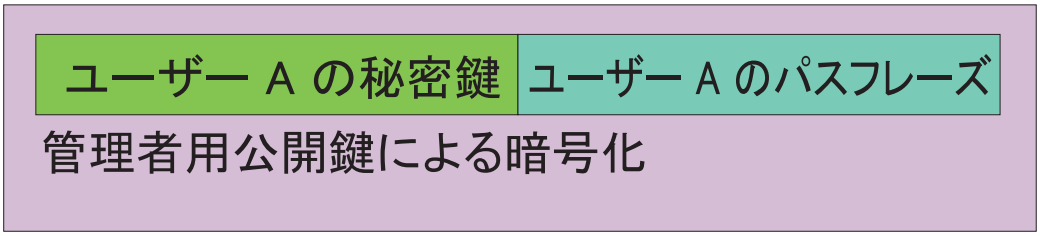

図 17. ユーザー A は、ユーザー A の秘密鍵を必要とする任意の機能を実行するためにパスフレーズを入力する必要がある

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規則のことです。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。

ユーザー A の秘密鍵は管理者公開鍵により暗号化され、秘密鍵の復号化には管理者の秘密鍵が必要です。そのため、ユーザー A のパスフレーズが紛失しても、管理者は新しいパスフレーズを再設定できます。

パスフレーズの使用

24 ページの図 18 から 26 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要です。必要に応じて認証装置を追加することができますが、いずれの場合も初期のユーザーのパスフレーズ要件が必要なくなることはありません。バイオメトリック・データまたは他の認証データは、ユーザーの公開鍵により暗号化されます。この追加のセキュリティー・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。

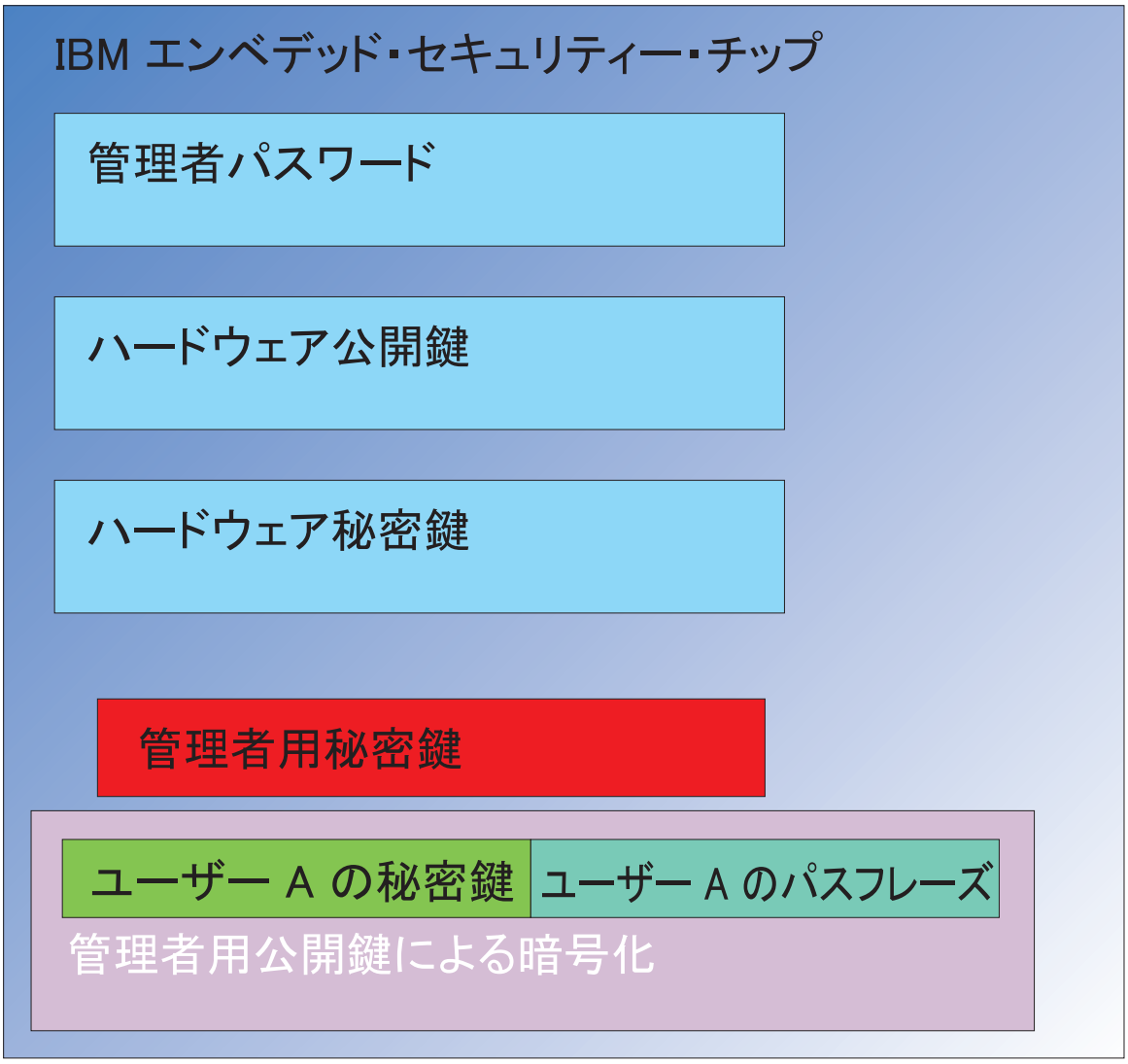

図 18. 管理者の秘密鍵はチップ内で復号化される

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。管理者の秘密鍵は、前述のとおり、チップ内ですでに復号化されています。 25 ページの図 19 は、証明書が渡される様子を示しています。

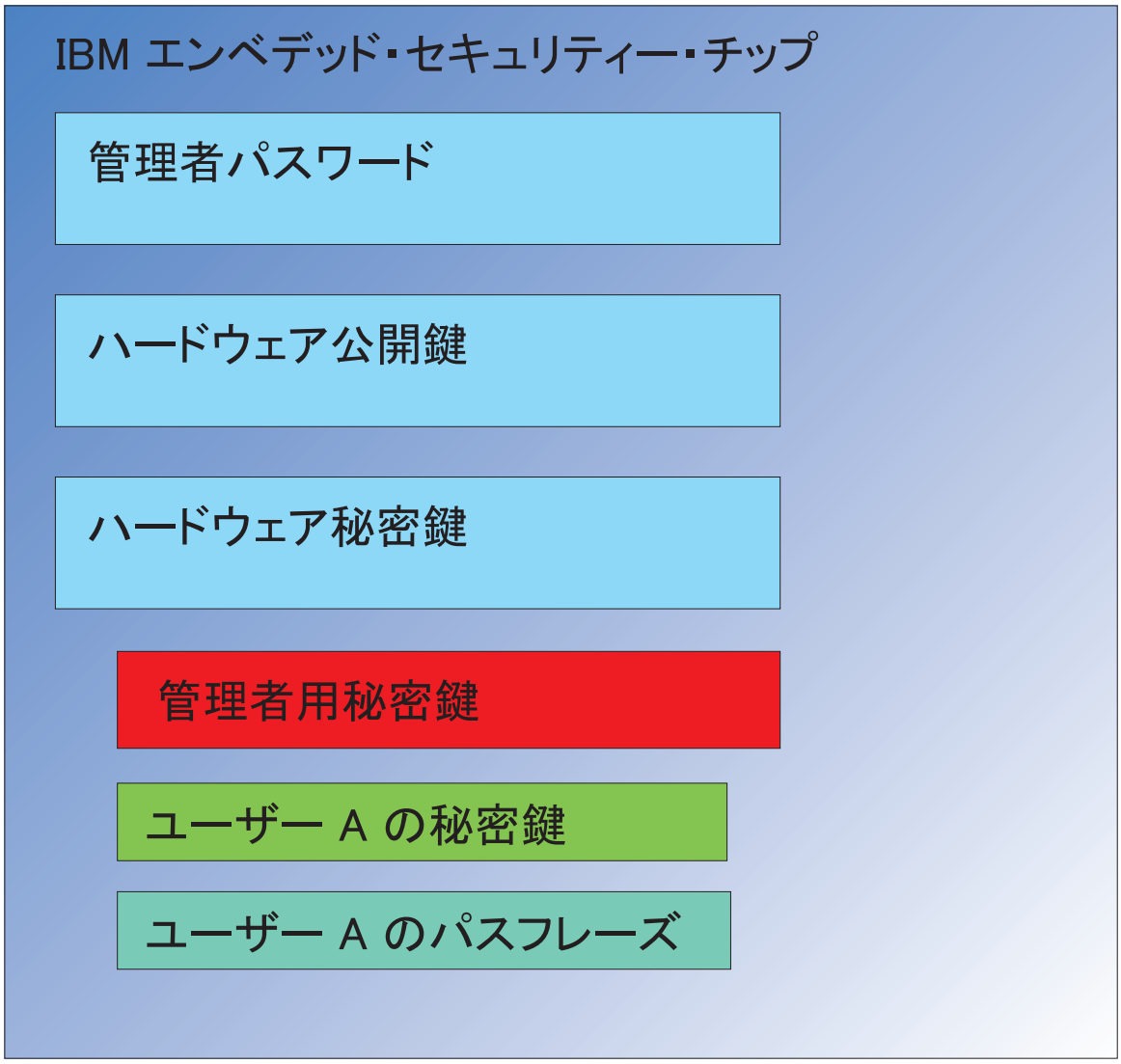

図 19. ユーザー A の秘密鍵およびパスフレーズがチップ内で使用可能になる

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、 26 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。

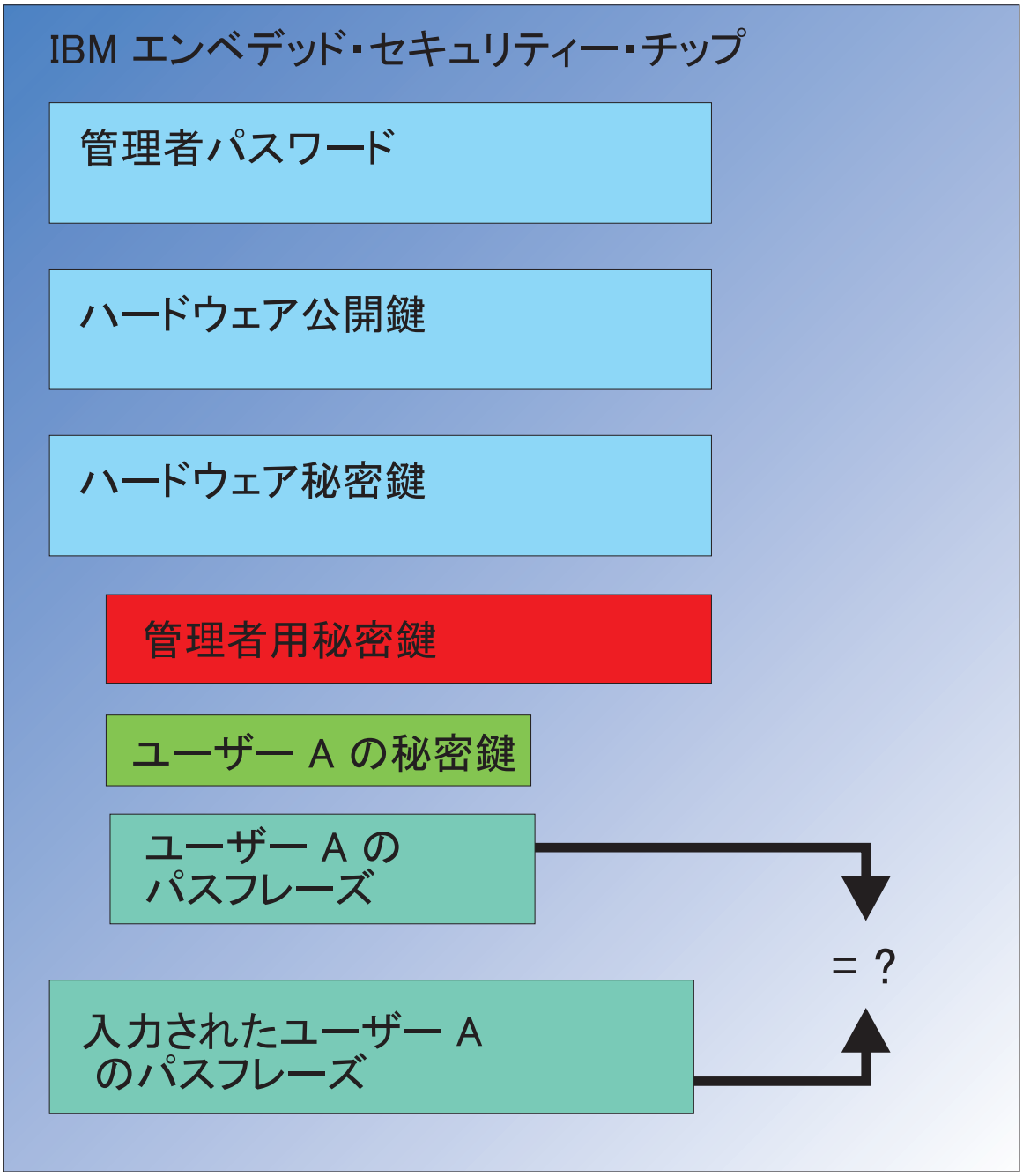

図 20. ユーザー A がユーザー A の証明書の使用を試みると、パスフレーズ・ダイアログが表示される

入力されたパスフレーズはチップに渡され、復号化されたパスフレーズ値と比較されます。両方が一致すれば、ユーザー A の証明書は、ディジタル署名や電子メールの復号化など、さまざまな機能で使用できるようになります。注目すべき点として、このパスフレーズの比較はチップのセキュア環境内で行われます。このチップには、失敗アクセスの繰り返し試行を検出するハンマーリング防止機能が備わっています。注目すべき別の点として、ユーザー A の登録済みパスフレーズが、チップ外で攻撃にさらされることはありません。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。ユーザー・パスフレーズの作成は、この登録プロセスの一部です。これ以降は、このパスフレーズの設定方法、およびパスフレーズ規則の適用方法について説明します。

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 Securiy Software と関連付けられています。これまでのセクションでは、初期設定の全体的な概念について説明しました。以降のセクションでは、初期設定の具体的なプロセスについて詳しく説明します。

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。次の表は、公開鍵と秘密鍵、および管理者パスワードを初期設定する方法を示したものです。

表 1. ハードウェアの初期設定方法

処置	BIOS での定義	管理者による CSS ソフトウェアでの手動定義	スクリプトでの定義
ハードウェア公開/秘密鍵の作成	不可	可	可
管理者パスワードの作成	一部の TCG と互換クライアントでは可。BIOS エントリーを確認してください。	可	可

表 1 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、ソフトウェアまたはスクリプトを使用して手動に開始する必要があります。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。ハードウェア公開鍵および秘密鍵の値はチップにより制御されるため、管理者が設定することはできません。チップ内の乱数機能により、統計的にランダムな公開鍵と秘密鍵のペアが生成されます。ただし、管理者パスワードは管理者が設定します。

ハードウェア鍵とは異なり、管理者パスワードは管理者が値を設定します。管理者パスワードについては、以下の点を考慮する必要があります。

- 管理者パスワードとして何を設定するか。
- さまざまなグループ用に複数の管理者パスワードを設定するか。その場合、どのコンピューターにどのパスワードを割り当てるかを、どのように論理的に決定するか。
- どの管理者に、パスワードへのアクセスを許可するか。いくつかのユーザー・グループ用に複数のパスワードを定義する場合、どの管理者にどのパスワードへのアクセスを許可するか。
- 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。

上記の項目について効果的な決定をするには、管理者パスワードで実行できる処理を理解する必要があります。次のとおりです。

- 管理者ユーティリティーへのアクセス権の取得
- 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

以降のセクションでは、ポリシー・ファイルと管理者秘密鍵の接続について説明します。ここでは、ポリシーを変更するのに管理者秘密鍵が必要であるということに注目してください。表 2 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 2. 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	管理者用秘密鍵
管理者ユーティリティーへのアクセス権の取得	可	不可
ユーザーの追加/削除/復元	可	不可
使用可能な CSS アプリケーション/機能の定義	可	不可
ポリシーの定義/変更	可	可
ユーザー・パスフレーズのリセット用ファイルの作成	可	可

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。上の表は、この鍵と関連付けられた機能を示しています。管理者公開鍵および秘密鍵の設定に注目してください。この鍵ペアは、コンピューターごとに固有にすることも、全マシンで共通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、人事部門の全コンピューター用に 1 つの管理者パスワードおよび管理者秘密鍵を設定し、技術部門用に別の管理者パスワードおよび管理者鍵を設定するという要領です。別の方法として、建物や所在地など、物理的に区別して異なる設定を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ときにどの管理者秘密鍵を使用するかは、どのユーザーがリセットを要求しているかに応じて簡単に判別できます。27 ページの表 1 および 31 ページの表 3 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 をデプロイメントする前のセキュリティー・ポリシーの設定

セキュリティーと認証に関する要求は、企業内のさまざまな関係者から出されます。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 7 章 新規または変更されたセキュリティー・ポリシー・ファイルのリモートでのデプロイメント』 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が、クライアントのハードディスクに保管されたり、人が読取可能な形式でエンベデッド・セキュリティー・チップに保管されることはありません。保管場所は、ユーザーの記憶を除けば他に 1 つのロケーションしかありません。それが、管理者鍵ペアで保護されているアーカイブです。管理者は、管理者秘密鍵を使用して、アーカイブに保管されている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、復号化されたパスフレーズをユーザーに提供します。

ユーザーがパスフレーズを変更すると、新しい情報は、指定されたアーカイブ・ロケーションにアーカイブされます。

認証装置が誤動作した場合、IBM Client Security Software では、「**パスフレーズまたはオーバーライドパスワードで認証する**」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。その後、ユーザーはセキュア・タスクを実行することができます。

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。また、c:¥jgk¥archive がネットワーク・ドライブの場合、パスフレーズをアーカイブするには、そのドライブがクライアント・コンピューターにマッピングされている必要があります。
2. アーカイブ・ロケーションを指定しないか、そのロケーションがクライアント・コンピューターにマッピングされていない場合、パスフレーズはリカバリーできません。

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は、2 つのプロセスで構成されていることに注目してください。

1. 登録
2. 個別設定

登録

登録とは、IBM Client Security Subsystem にユーザーを追加または登録する作業のことです。 30 ページの図 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管理し、ポリシーを適用します。

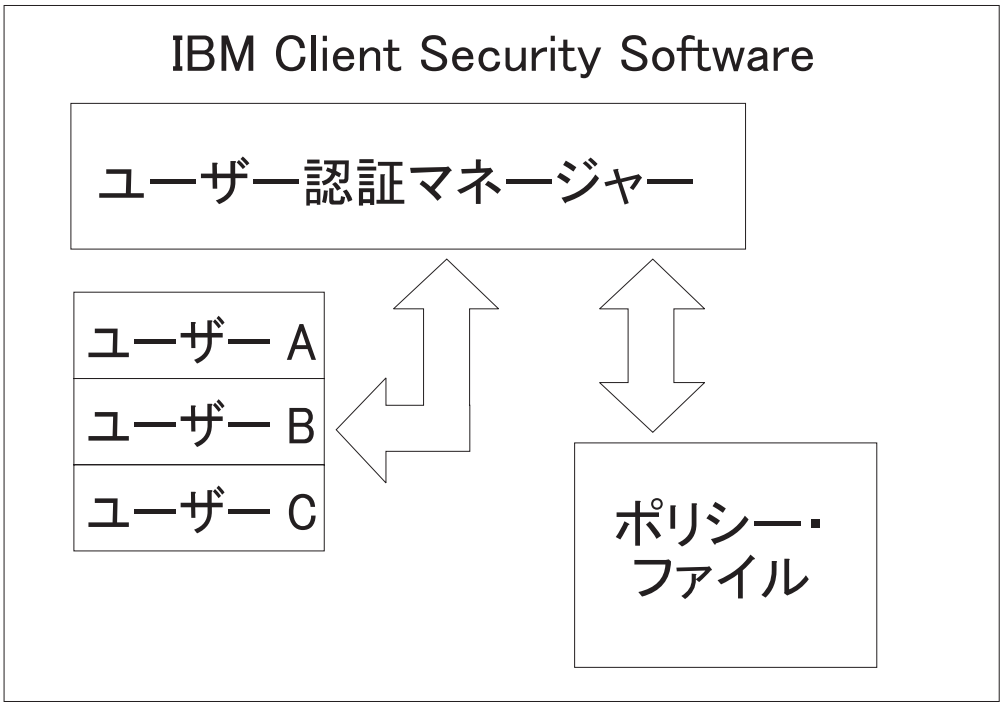

図 21. ユーザー認証マネージャーは、各ユーザーの証明書を管理し、セキュリティー・ポリシーを適用する

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とオペレーティング・システムに誰がログオンしているかに応じて、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、Microsoft® Outlook にアクセスして、ディジタル署名された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 では、操作の実行許可が与えられる前に、ポリシー・ファイルで定義されたポリシーが適用されます。この例の場合、操作を実行する前に、パスフレーズが認証を受ける必要があります。ユーザーがパスフレーズを入力するためのプロンプトが出され、それが正しく認証されると、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、その人だけが記憶している必要があります。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たとします。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保証するため、ユーザー A は、システムへのアクセス権を取得した後にそのパスフレーズをカスタマイズする必要があります。そうすれば、他の人が、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実行するのを防ぐことができます。

表 3. ユーザーの初期設定方法

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使用してユーザー用の CSS を手動で個別設定します。	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、管理者パスワードの暗号化ものが含まれる構成ファイルを作成します。このファイルはユーザーに送信され、ユーザーは、管理者の介入や立ち合いがなくても個別に登録することができます。	セットアップはユーザーが行います。
*.ini	管理者は、.ini ファイルを実行するスクリプトを作成して、デフォルトまたは個別設定されたパスワードを入力します。	管理者またはユーザーが立ち会うかどうかは任意です。

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。そのために、以下のいずれかのデプロイメント方法をとります。

- 各マシンをどのエンド・ユーザーが使用するかをすべて把握している場合。たとえば、マシン 1 は Bob が使用するため、マシン 1 には Bob を登録します。Bob は、コンピューターを受け取ったら、個別設定 (個人パスフレーズの設定) を行わなければなりません。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。
- 各マシンをどのエンド・ユーザーが使用するかを把握していない場合。この場合は、クライアント 1 をエンド・ユーザー X に発送します。

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、いくつかのデプロイメント・オプションがあり、そのため IBM ESS をより柔軟にデプロイメントすることができます。

次の図は、標準的な PC デプロイメントのフロー・チャートを示しています。

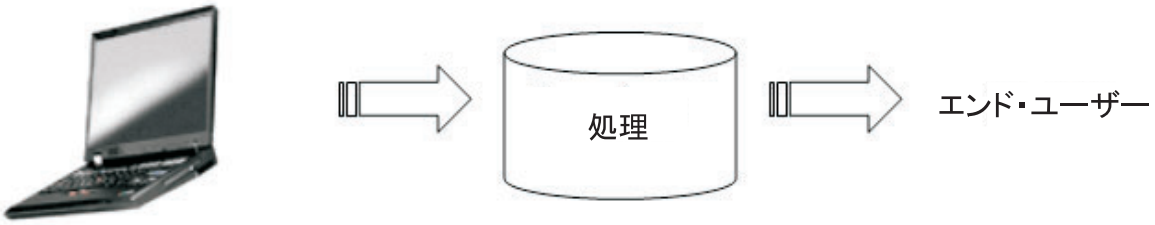

図 22. 標準的な PC デプロイメントのフロー・チャート

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 コードがディスク・イメージに含まれていません。インストール、初期設定、個別設定は、コンピューターがデプロイメントされた後に実行されます。
2. **イメージ・コンポーネント**—IBM Client Security Software コードはイメージに含まれていますが、インストールされていません。会社の個別設定およびユーザーの個別設定のいずれも開始されていません。(33 ページの図 23 を参照)
3. **単純インストール**—IBM Client Security Software はインストールされており、会社またはエンド・ユーザー用に個別設定されています。(34 ページの図 24 を参照。)
4. **部分的な個別設定**—IBM Client Security Software はインストールされており、会社の個別設定は完了しているが、エンド・ユーザーの個別設定は完了していません。(34 ページの図 24 を参照。)
5. **一時的な個別設定**—IBM Client Security Software はインストールされており、会社とユーザー両方の個別設定が完了しています。ユーザーは、ユーザー・パスフレーズを再設定する必要があり、場合によっては、指紋の登録やスマートカードの関連付けなど他の認証情報を提供する必要があります。(35 ページの図 25 を参照。)
6. **完全な個別設定**—IBM Client Security Software はインストールされており、会社とユーザー両方の個別設定が完了しています。管理者は、ユーザー・パスフレー

ズを設定します。指紋の登録またはその他の認証が必要な場合は、ユーザーが個別設定のための情報を提供します。(35 ページの図 25 を参照。)

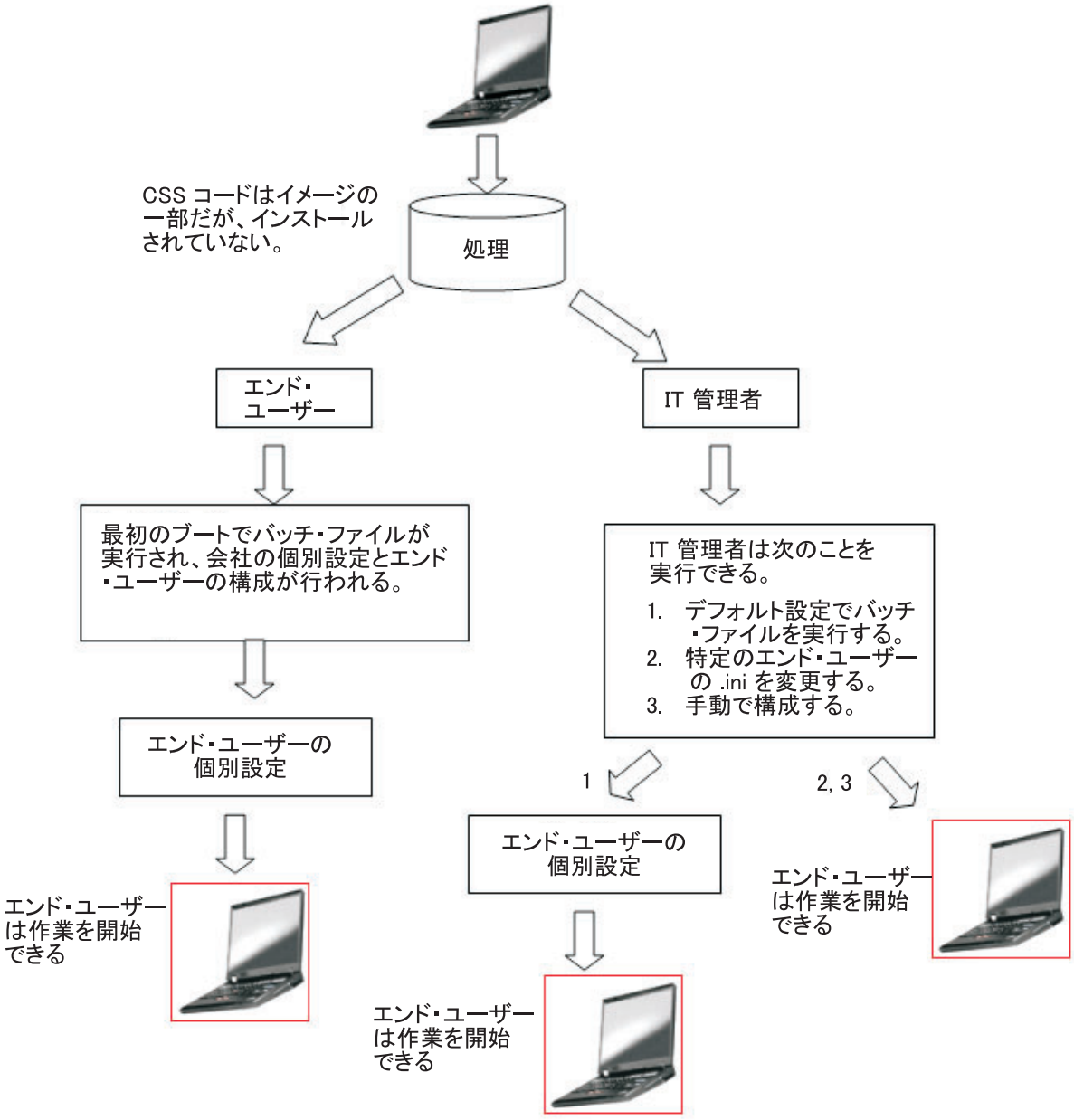

図 23. IBM Client Security Software コードはイメージに含まれているが、インストールされていない

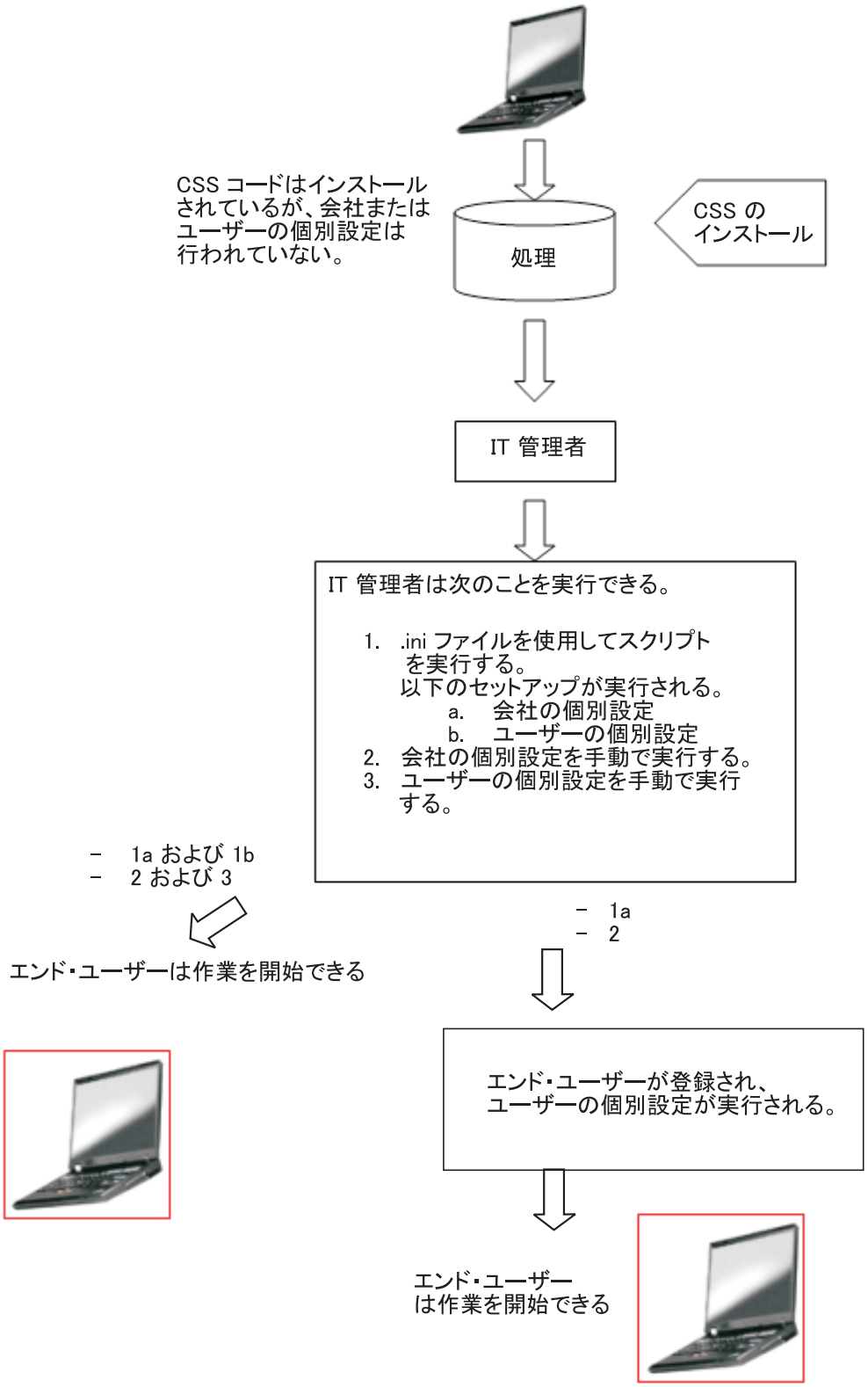

図 24. IBM Client Security Software コードはインストールされているが、会社またはユーザーの個別設定は行われていない

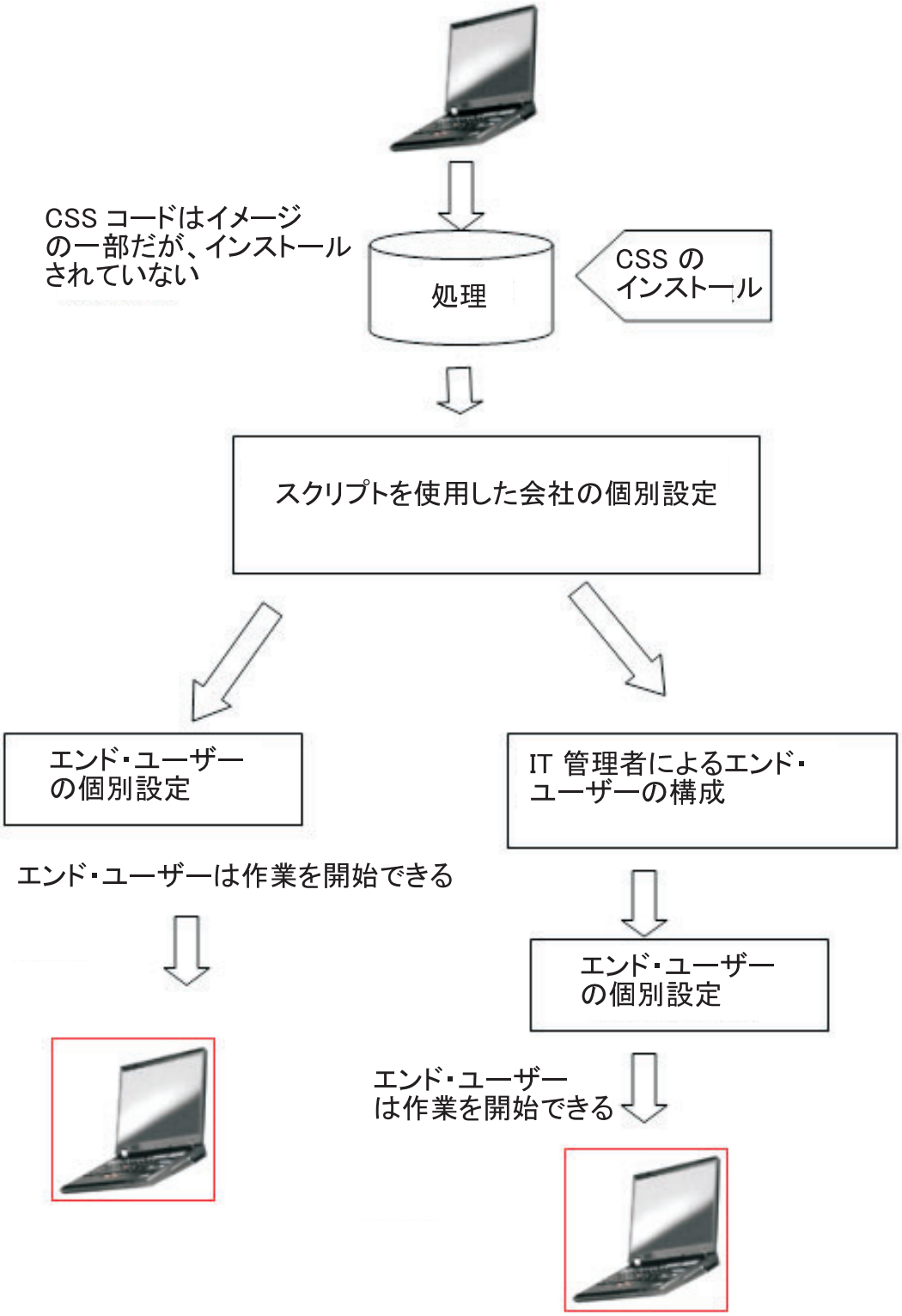

図 25. IBM Client Security Software はインストールされており、会社とユーザーの個別設定が完了している

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と構成、およびチップの構成で選択できるさまざまなオプションを示しています。実際の必要と環境に応じて、要件を満たす最善のシナリオおよびインストール方法を選択してください。インストール方法の詳細については、「インストールおよび初期設定」を参照してください。

インストールおよび初期設定

IBM Client Security Software のインストールは、インストールと初期設定という 2 つのプロセスに分けられます。インストール・プロセスは、通常のソフトウェアのインストール方法とほとんど同じです。このインストールは、以下の 2 つの方法で実行できます。

1. Client Security Software を、デプロイメント済みのコンピューターに追加する。(シナリオ 1 (32 ページ) を参照。)
2. Client Security Software は、ベース・イメージの一部です。(シナリオ 2 (32 ページ) からシナリオ 6 (32 ページ) を参照。)

インストール

1 番目の方法では、IBM Client Security Software は、IBM ImageUltra™ Builder などのプログラムにより全コンピューターに追加されたイメージに追加されます。

2 番目の方法では、IBM Client Security Software は、ベース・イメージが置かれているコンピューターをデプロイメントした後に、エンド・ユーザーの PC に追加されます。この方法は、次の 2 つの方法で実行できます。

1. **ユーザーによる実行**— ユーザーがインストールを開始し、ダイアログをクリックしたり必要な情報を入力しながらインストールを完了します。
2. **サイレント・インストール**—ユーザーの介入を必要とすることなく、インストール・プロセスを開始し、完了します。

初期設定

初期設定には 2 つの方式があります。

1. マス・デプロイメントによる設定
2. 個別の初期設定

マス・デプロイメントによる設定オプションでは、CSS.ini ファイルを使用する必要があります。このファイルには、システム上のすべてのユーザーを登録したり、すべてのユーザーに設定済みパスフレーズを付与するためのパラメーターがあります。個別の初期設定では、エンド・ユーザーが自らを登録し、ユーザー定義のパスワードを定義するためのファイルをエンド・ユーザーに提供することができます。

セキュリティー・チップを搭載したデプロイメント済みコンピューターへの IBM Client Security Software の追加

管理者は、IBM Client Security Software (ベース・イメージ上) の配布のみを実行し (個別設定や構成を行わない)、それからクライアントを構成することができます。別の方法として、管理者は、IBM Client Security Software をマス・デプロイメントに

より、構成を自動的に実行することもできます。どちらの場合でも、最初にソフトウェアをインストールし、次に構成を行うという手順は変わりません。

IBM Client Security Software のインストール: ベースのイメージに IBM Client Security Software を追加するには、以下のコンポーネントが含まれている必要があります。

1. ドライバー: LPC (TCPA システム用) および SMBus

   注:

   a. SMBus には自動インストール用のコードがありますが、このドライバーは Microsoft によって署名されていないため、このドライバーをインストールするときは、管理者の立ち会いが必要です。現在、この制約を解消する方向で準備が進められています。

   b. デプロイメント用に Sysprep ドナー・イメージを作成する場合、このドライバーのインストールでは、ドナー・イメージの作成時のみ管理者の立ち合いが必要です。

   c. IBM ImageUltra Builder を使用するには、Portable Sysprep Image を準備する必要があります。SMBus は、ベース・イメージの一部でなければなりません。すべてのコンピューターについて、SMBus をベース・イメージの一部として含めない場合は、2 つのベース・イメージを作成する必要があります。

2. IBM Client Security Software コード
3. 定義済みの管理者パスワードおよび秘密鍵—
4. Install IBM Client Security Software アプレット (ポリシー・ファイルで必要な場合は、File and Folder Encryption および Password Manager をインストールする必要があります。これらのアプレットのサイレント・インストールについては、「*IBM Client Security インストール・ガイド*」を参照してください。)

上にリストした 3 つのコンポーネントをドナー・システムに追加した後、エンベデッド・セキュリティー・サブシステム・ハードウェア (セキュリティー・チップ) を初期設定する必要があります。大量インストールを開始するには、以下の手順を実行します。

1. CSEC.INI ファイルを作成します。(CSEC.INI ファイルは、クライアント・セキュリティー・ウィザード、つまり Security ディレクトリー内の CSECWIZ.EXE を使用して作成できます。ウィザードが完了したら、**「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。このコンピュータの設定には影響しません。」**のチェック・ボックスにチェックマークを付けます。
2. フォルダー名を指定して Winzip を実行し、IBM Client Security Software インストール・パッケージ (csecxxxx_00xx.exe) の内容を抽出します。
3. SETUP.ISS ファイルの szIniPath および szDir 項目を編集します。これらは、マス・デプロイメントに必要です。マス・デプロイメントを行う場合は、szIniPath パラメーターが必要です。(完全な SETUP.ISS ファイルについては、以下を参照してください。)
4. ターゲット・システムにファイルをコピーします。

5. ¥setup -s コマンド行ステートメントを作成します。このコマンド行ステートメントは、管理者権限を持っているユーザーのデスクトップから実行する必要があります。Startup プログラム・グループ、または Run キーがこれを行うのに適しています。
6. 次のブート時に、このコマンド行ステートメントを除去します。

setup.iss ファイルの全内容を、若干の説明をつけてリストします。

```
[InstallShield Silent] Version=v6.00.000 File=Response File szIniPath=d:¥csec.ini
```

(上記のパラメーターは、マス・デプロイメントに必要な .ini ファイルの名前とロケーションです。.ini ファイルがネットワーク・ドライブにある場合は、そのドライブがマッピングされている必要があります。サイレント・インストールでマス・デプロイメントを使用しない場合は、このエントリーを削除します。IBM Client Security Software のインストールのみを実行する場合は、上のコード行から szIniPath=d:¥csec.ini を削除してください。インストールだけでなく構成も実行する場合は、コマンドをそのまま残して、パスを確認してください。)

```
[FileTransfer] OverwrittenReadOnly=NoToAll [{7BD2CFF6-B037-47D6-A76BD941EE13AD96}-
DlgOrder] Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdLicense-0 Count=4 Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdAskDestPath-0 Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdSelectFolder-0 Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdFinishReboot-0 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0]
Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0]
szDir=C:¥Program Files¥IBM¥Security
```

(上記のパラメーターは、Client Security のインストールに使用するディレクトリーです。これはコンピューターに対してローカルである必要があります。)

```
Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0] szFolder=IBM Client Security Software
```

(上記のパラメーターは、Client Security のプログラム・グループです。)

```
Result=1 [Application] Name=Client Security Version=5.00.002f
Company=IBM Lang=0009 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdFinishReboot-0] Result=6 BootOption=3
```

構成: マス・デプロイメントを開始するには次のファイルも必要です。拡張子が .ini であれば、ファイル名は任意です。以下では、作成する必要がある .ini ファイルの設定およびその説明をリストします。CSEC.INI ファイルを開いて変更する前に、まず Security フォルダー内の CONSOLE.EXE を使用してこのファイルを復号化する必要があります。

大量インストール時にマス・デプロイメントを実行しない場合は、コマンド行から次のコマンドで .ini ファイルを実行します。

```
<CSS installation folder>¥acamucli /ccf:c:¥csec.ini
```

表 4. Client Security のシステム構成の設定

[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 ハードウェアのパスワード。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。

表 4. Client Security のシステム構成の設定 (続き)

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数を決定します。 **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する必要があります。
kpl=c:¥jgk	newkp が 1 の場合の管理者鍵ペアのロケーション。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ロケーション。 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ロケーション。 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ロケーション。 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表します。この項目は不要ですが、このファイルに含める場合は、値は 0 にしておきます。
clean=0	初期設定後に .ini ファイルを削除する場合は 1。 初期設定後に .ini ファイルを残しておく場合は 0。
enableroaming=1	クライアントでローミングを使用可能にする場合は 1。 クライアントでローミングを使用不可にする場合は 0。
username= [promptcurrent]	現行ユーザーにシステム登録パスワードを要求する場合は [promptcurrent]。 現行ユーザーがローミング・サーバーへのシステムの登録を認可されており、現行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 [current]。 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 の値が 0 の場合、または enableroaming 項目がない場合は、この項目を指定しないでください。
sysregpwd=12345678	システム登録パスワード。システムをローミング・サーバーに登録するための正しいパスワードを設定します。username の値が [promptcurrent] の場合、または username 項目がない場合は、この項目を指定しないでください。
[UVMEnrollment]	ユーザー登録のセクション・ヘッダー。
enrollall=0	すべてのローカル・ユーザー・アカウントを 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、すべてのユーザー用の UVM パスフレーズ。

表 4. Client Security のシステム構成の設定 (続き)

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、すべてのユーザーに適用される UVM パスフレーズ変更ポリシー。 ユーザーに次回のログオンで UVM パスフレーズの変更を要求する場合は 1。 ユーザーに次回のログオンで UVM パスフレーズの変更を要求しない場合は 0。
defaultppexppolicy=1	enrollall が 1 の場合、すべてのユーザーに適用される UVM パスフレーズ有効期限ポリシー。 UVM パスフレーズの有効期限が切れるように設定する場合は 0。 UVM パスフレーズの有効期限を無期限にする場合は 1。
defaultppexpdays=0	enrollall が 1 の場合、すべてのユーザーに適用される、UVM パスフレーズの有効期限が切れるまでの日数。 ppexppolicy が 0 の場合、UVM パスフレーズの有効期限が切れるまでの日数。
enrollusers=*x*。x はコンピューターに登録するユーザーの合計数です。	この値は、登録されるユーザーの合計数を設定します。 enrollall が 0 の場合、この値は UVM に登録されるユーザーの数を設定します。
user1=jknox	登録するユーザーの情報を 1 から順に列挙します (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。Windows XP の実際のアカウント名を取得するには、次の手順を行います。 1. 「コンピューターの管理」(デバイス・マネージャー) を開始します。 2. 「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. 「ユーザー」フォルダーを開きます。 「名前」列にリストされた項目がアカウント名です。
user1uvmpw=chrome	UVM のユーザー 1 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かドメインかを指定します。 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 に次回のログオンで 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。 ユーザーに次回のログオンで UVM パスフレーズの変更を要求する場合は 1。 ユーザーに次回のログオンで UVM パスフレーズの変更を要求しない場合は 0。

表 4. Client Security のシステム構成の設定 (続き)

user1ppexppolicy=1	ユーザー 1 の UVM パスフレーズの有効期限が切れるようにするかどうかを指定します。 UVM パスフレーズの有効期限が切れるように設定する場合は 0。 UVM パスフレーズの有効期限を無期限にする場合は 1。
user1ppexpdays=0	user1ppexppolicy が 0 の場合、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。
ユーザーごとに、表内の陰影部分の順序に従って一連の構成設定を行います。1 人のユーザーのすべてのパラメーターを設定した後、次のユーザーのパラメーターを設定します。たとえば、enrollusers が 2 に設定されている場合、次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 対応アプリケーションのセットアップおよび UVM 対応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。
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	ロータス ノーツに UVM プロテクションを使用する場合は 1。 ノーツ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	Password Manager を使用する場合は 1。 Password Manager を使用しない場合は 0。
folderprotect=0	FFE を使用する場合は 1。 FFE を使用しない場合は 0。

注:

1. 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。
2. 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。
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. 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。

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 5. 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。
hwpw=11111111	CSS ハードウェアのパスワード。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数を決定します。 **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する必要があります。
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ロケーション。 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表します。この項目は不要ですが、このファイルに含める場合は、値は 0 にしておきます。
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使用不可にする場合は 0。
[UVMEnrollment]	ユーザー登録のセクション・ヘッダー。
enrollall=0	すべてのローカル・ユーザー・アカウントを 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	この値は、登録されるユーザーの合計数を設定します。
user1=*eddy*	登録する新しいユーザーの名前。
user1uvmpw=pass1word	UVM のユーザー 1 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。

表 5. 2 回目の実行時の Client Security Software 構成設定 (続き)

user1domain=0	ユーザー 1 のアカウントがローカルかドメインかを指定します。 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 に次回のログオンで 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。 ユーザーに次回のログオンで UVM パスフレーズの変更を要求する場合は 1。 ユーザーに次回のログオンで UVM パスフレーズの変更を要求しない場合は 0。
user1ppexppolicy=1	ユーザー 1 の UVM パスフレーズの有効期限が切れるようにするかどうかを指定します。 UVM パスフレーズの有効期限が切れるように設定する場合は 0。 UVM パスフレーズの有効期限を無期限にする場合は 1。
user1ppexpdays=0	user1ppexppolicy が 0 の場合、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。

第 5 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・エディターを使用して、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.pc.ibm.com/us/security/index.html) 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 ディレクトリー・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。

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¥csec53Xjp.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。
   d. 「**Unzip**」をクリックします。2 つのファイルが展開されたことを示すウィンドウが表示されます。
   e. 「**OK**」をクリックします。元のウィンドウの「**Close**」をクリックします。展開先 (デフォルトは、`C:¥Temp_css`) に 2 つのファイル (CSSISU53X.exe、csec53Xjp_00XX_X.exe) が展開されます。ここで、ファイル名中の「X」は、省略されるか、英数字が入ります。
   f. 「スタート」>「ファイル名を指定して実行」をクリックします。「ファイル名を指定して実行」フィールドに「d:¥directry¥CSSISU53Xjp.exe」と入力し、「OK」をクリックします。ここで、d:¥directry は、10 で展開された先の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。
   g. 「**インストールの開始**」をクリックします。

      ドライバーのインストールが正常に終了した後は、画面の指示に従って、「**OK**」をクリックし、インストールを続けます。
   h. すぐにコンピューターを再起動するオプションを選択し、「**OK**」をクリックします。

      コンピューターが再起動すると、IBM Client Security Software セットアップ・ウィザードが開きます。「キャンセル」をクリックしてください。
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、This is the 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・エディターを使用してUVM ポリシー・ファイルを編集します。UVM ポリシー・エディター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・エディターでローカル・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・エディターを使用できます。

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・エディターを始動するには、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。
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。

問題の兆候	可能な解決策
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。

ロータス ノーツのトラブルシューティングに関する情報

Client Security Software とロータス ノーツ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
ロータス ノーツに対する UVM 保護が有効化された後、ロータス ノーツが自身のセットアップを終了できなくなる	**処置**
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、ロータス ノーツ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ロータス ノーツのサポートを有効にするには、事前にロータス ノーツを構成して稼働の状態にする必要があります。
ノーツ・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 の使用中にノーツ・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。 • ロータス ノーツ構成ツールを使用して、ノーツ ID に対する UVM プロテクションを設定したとき • ノーツを開き、ノーツで提供されている機能を使用してノーツ 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ノーツを閉じたとき	「**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。ノーツ 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 はノーツ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 6 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.pc.ibm.com/us/security/index.html にアクセスしてください。

ディスク・イメージの一部になっている多くのコンポーネントと同様、製品をインストールする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・ファイルをインストールする前に CSS がハード・ディスクに置かれていないと、これらの装置のドライバーおよびソフトウェアは正しくインストールされません。

認証ハードウェアを正しく使用できるよう、ソフトウェアおよびドライバーのインストールに関する最新の情報を入手するには、デバイスに付属のマニュアルを参照してください。

第 7 章 新規または変更されたセキュリティー・ポリシー・ファイルのリモートでのデプロイメント

セキュリティー・ポリシーを更新したり、コンピューター別に異なるポリシーを作成したりする場合、署名権限を持つ IT 管理者はポリシー・ファイルを変更してデプロイメントすることができます。ポリシー・ファイルを編集するには、ACAMUCLI.EXE を使用します。(「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、画面上に表示される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。)編集済みのファイルは、GLOBALPOLICY.GVM と GLOBPOLICY.GVM.SIG です。これらのファイルを適切なユーザーに配布し、それらのファイルが Security¥UVM_Policy フォルダーに保管されていることを確認します。

デプロイメントした後は、パスフレーズ・ポリシーをリモート側で更新できます。パスフレーズ・ポリシー・ファイルを更新すると、ユーザーが次にパスフレーズを変更するときのパスフレーズ要件が変更されます。管理者は、ユーザーにパスフレーズの変更を強制するまでの時間を定義できます。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、管理者は有効期限も変更できます。たとえば、管理者は 30 日ごとではなく 15 日ごとにパスフレーズを変更するように Jane に要求することができます。次の例を考えてみましょう。パスフレーズの有効期限が 30 日で、現在その 10 日目だとします。そこで、パスフレーズを 15 日ごとに変更するように要求する新しいパスフレーズ・ポリシー・ファイルがクライアント・コンピューターに送られてきました。パスフレーズは残り 5 日で期限切れになるのでしょうか。それとも 20 日後でしょうか。この場合、パスフレーズは元のポリシーの定義どおり 20 日後に期限切れになります。パスフレーズ有効期限ポリシーは、パスフレーズを設定したときから適用されます。15 日に変更されたポリシーは、20 日後に Jane がパスフレーズを変更したときに開始します。

パスフレーズの必須特性を変更するには、上記の手順を実行します。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。

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。

本書で説明されている製品は、臓器移植、あるいは製品の誤動作が身体の損傷や死亡につながるような生命維持を目的とした用途に使用することはできません。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。

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。