IBM® Client Security Solutions

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

IBM® Client Security Solutions

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

本書および本書で紹介する製品をご使用になる前に、 109 ページの『付録 D. Client Security Software に関する米国の輸出規制』 および 111 ページの『付録 E. **特記事項および商標**』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 Solutions Client Security Software Version 5.4 Administrator and User 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 2004.10

この文書では、平成明朝体™W3、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™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

目次

第 1 部 Client Security の紹介

第 1 章 概要

一部の ThinkPad™ および ThinkCentre™ コンピューターでは、ダウンロード可能なソフトウェア・テクノロジーとともに機能する組み込みの暗号ハードウェアが標準装備されており、クライアント PC プラットフォームにおいて強力なセキュリティー・レベルを提供しています。このハードウェアとソフトウェアをまとめて、IBM エンベデッド・セキュリティー・サブシステム (ESS) と呼んでいます。ハードウェア・コンポーネントは IBM エンベデッド・セキュリティー・チップであり、ソフトウェア・コンポーネントは IBM Client Security Software (CSS) です。

Client Security Software は、IBM エンベデッド・セキュリティー・サブシステムを使用してファイルの暗号化と暗号鍵の格納を行う IBM コンピューター用に設計されています。このソフトウェアは、ローカル・ネットワーク、企業、またはインターネット全体にわたって、IBM クライアント・システムがクライアント・セキュリティー機能を使えるようにするためのアプリケーションとコンポーネントから構成されています。

IBM エンベデッド・セキュリティー・サブシステム

IBM ESS は、Public Key Infrastructure (PKI) などの鍵管理ソリューションをサポートしており、以下のローカル・アプリケーションから構成されています。

- File and Folder Encryption (FFE)
- Password Manager
- セキュア Windows ログオン
- 以下のような、複数の構成可能な認証方式
  - パスフレーズ
  - 指紋
  - スマート・カード

IBM ESS の機能を効果的に使用するためには、セキュリティー管理者はいくつかの基本的な概念を熟知している必要があります。次のセクションでは、基本的なセキュリティーの概念について説明しています。

IBM エンベデッド・セキュリティー・サブシステム

IBM エンベデッド・セキュリティー・サブシステムは、一部の IBM PC プラットフォームで特別なセキュリティー・レベルを提供するために組み込まれた暗号ハードウェア・テクノロジーです。このセキュリティー・サブシステムの出現により、暗号化と認証のプロセスは、傷つきやすいソフトウェアの環境から専用ハードウェアによるセキュアな環境へと移されます。これによって、セキュリティーは確実に強化されます。

IBM エンベデッド・セキュリティー・サブシステムは以下をサポートします。

- RSA3 PKI オペレーション (プライバシーのための暗号化および認証のためのディジタル署名など)

- RSA 鍵の生成
- 疑似乱数の生成
- 200 ミリ秒での RSA 機能の計算
- RSA 鍵ペア・ストレージ用の EEPROM メモリー
- TCG Main Specification バージョン 1.1 で定義されているすべての Trusted Computing Group (TCG) 機能
- Low Pin Count (LPC) バスを通じてのメインプロセッサーとの通信

IBM Client Security Software

IBM Client Security Software は、以下のソフトウェア・アプリケーションおよびコンポーネントから構成されています。

- **管理者ユーティリティー:** 管理者ユーティリティーは、管理者がエンベデッド・セキュリティー・サブシステムの有効化/無効化、鍵およびパスフレーズの作成、アーカイブ、再生成の目的に使用するインターフェースです。さらに、管理者はこのユーティリティーを使用して、Client Security Software で提供されているセキュリティー・ポリシーにユーザーを追加することもできます。
- **管理者コンソール:** 管理者は、Client Security Software の管理者コンソールを使用して、クレデンシャル・ローミング・ネットワークの構成、デプロイメントを可能にするためのファイルの作成と構成、非管理者の構成およびリカバリーのためのプロファイルの作成を行えます。
- **ユーザー構成ユーティリティー:** ユーザー構成ユーティリティーでは、クライアント・ユーザーは、UVM パスフレーズの変更、Windows パスワードの UVM による認識、アーカイブの更新、および指紋の登録を行うことができます。また、ユーザーは IBM エンベデッド・セキュリティー・サブシステムで作成されたディジタル証明書のバックアップ・コピーを作成することもできます。
- **ユーザー認証マネージャー (UVM):** Client Security Software は UVM を使用して、パスフレーズなどのシステム・ユーザー認証用のエレメントを管理します。たとえば、UVM はログオン認証用に指紋読取装置を使用できます。 Client Security Software で使用可能な機能は、以下のとおりです。
  - **UVM クライアント・ポリシー保護:** Client Security Software では、システム上でクライアント・ユーザーの認証方法を指図するためのクライアント・セキュリティー・ポリシーを、セキュリティー管理者が設定できます。

    ログオンに指紋が必要であるとポリシーに示されていて、ユーザーが指紋を登録していない場合は、ログオンの一部として指紋を登録することができます。また、Windows パスワードが UVM に登録されていない場合や、間違って登録されている場合にも、ユーザーはログオンの一部として正しい Windows パスワードを入力することができます。
  - **UVM ログオン・プロテクション:** Client Security Software では、セキュリティー管理者がログオン・インターフェースを介してコンピューター・アクセスを制御することができます。 UVM ログオン・プロテクションのもとでは、セキュリティー・ポリシーによって認識されたユーザーだけが確実にオペレーティング・システムにアクセスできます。

パスワードと鍵の関係

システム・ユーザーの身元を検証するために、他のオプションの認証装置に加えて、パスワードと鍵は一緒に機能します。 IBM Client Security Software の機能を理解するためには、パスワードと鍵の関係を理解しておくことが不可欠です。

管理者パスワード

管理者パスワードは、管理者を IBM エンベデッド・セキュリティー・サブシステムに対して認証するために使用します。このパスワードは、エンベデッド・セキュリティー・サブシステムの 機密保護機能のあるハードウェア領域内で維持され、認証されます。管理者は、認証されると、以下のアクションを行うことができます。

- ユーザーの登録
- ポリシー・インターフェースの起動
- 管理者パスワードの変更

管理者パスワードは、以下の方法によって設定することができます。

- IBM クライアント・セキュリティー・セットアップ・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
- BIOS インターフェースを使用して (ThinkCentre コンピューターのみ)

管理者パスワードを作成し、維持するためのストラテジーを持っておくことが重要です。管理者パスワードは、暗号漏えいがあったり、忘れてしまった場合は変更することができます。

Trusted Computing Group (TCG) の概念と用語をご存じの場合、管理者パスワードは所有者の権限の値と同じです。管理者パスワードは、IBM エンベデッド・セキュリティー・サブシステムと関連しているため、*ハードウェア・パスワード* と呼ばれることもあります。

ハードウェア公開鍵とハードウェア秘密鍵

IBM エンベデッド・セキュリティー・サブシステムは、クライアント・システムに対して絶大なる信頼の*ルート* を持っているということが大前提になっています。このルートは、他のアプリケーションおよび機能を保護するのに使用されます。信頼ルート確立の一部に、ハードウェア公開鍵およびハードウェア秘密鍵の作成があります。公開鍵と秘密鍵は、両方合わせて*鍵ペア* ともいいますが、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いずれも、対応する秘密鍵でのみ復号化が可能。
- 秘密鍵で暗号化されたデータはいずれも、対応する公開鍵でのみ復号化が可能。

ハードウェア秘密鍵は、セキュリティー・サブシステムの機密保護機能のあるハードウェア領域で作成され、格納され、使用されます。ハードウェア公開鍵は、いろいろな目的に利用されるので公開鍵という名前が付いていますが、セキュリティー・サブシステムの機密保護機能のあるハードウェア領域の外部に開示されることは決してありません。ハードウェア公開鍵およびハードウェア秘密鍵は、次のセクションで説明する IBM 鍵スワッピング階層の重要な一部です。

ハードウェア公開鍵およびハードウェア秘密鍵は、以下の方法で作成します。

- IBM クライアント・セキュリティー・セットアップ・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

Trusted Computing Group (TCG) の概念と用語をご存じの方には、ハードウェア公開鍵およびハードウェア秘密鍵は*ストレージ・ルート鍵* (SRK) として知られています。

管理者公開鍵と管理者秘密鍵

管理者の公開鍵および秘密鍵は、鍵スワッピング階層では不可欠な部分です。また、システム・ボードあるいはハード・ディスク障害の際には、これらによってユーザー固有のデータをバックアップし、復元することもできます。

管理者公開鍵および管理者秘密鍵は、全システムについて固有であっても、すべてのシステムまたはシステムのグループにわたって共通であっても構いません。これらの管理者鍵は管理する必要があるため、固有の鍵に対して既知の鍵を使用するストラテジーを持つことが重要です。

管理者公開鍵および管理者秘密鍵は、以下のいずれかの方法で作成できます。

- IBM クライアント・セキュリティー・セットアップ・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

アーカイブ

システム・ボードあるいはハード・ディスク障害の際には、公開鍵および秘密鍵によって、ユーザー固有のデータをバックアップし、復元することができます。

ユーザー公開鍵とユーザー秘密鍵

IBM エンベデッド・セキュリティー・サブシステムは、ユーザー固有のデータを保護するために、ユーザー公開鍵とユーザー秘密鍵を作成します。これらの鍵ペアは、ユーザーが IBM Client Security Software に登録されている場合に作成されます。これらの鍵は、IBM Client Security Software のコンポーネントであるユーザー認証マネージャー (UVM) によって、透過的に作成し、管理することができます。鍵は、どの Windows ユーザーがオペレーティング・システムにログオンされているかに基いて管理されます。

IBM 鍵スワッピング階層

IBM エンベデッド・セキュリティー・サブシステムの基本要素は、IBM 鍵スワッピング階層です。 IBM 鍵スワッピング階層のベース (またはルート) は、公開鍵および秘密鍵です。公開鍵および秘密鍵は、*鍵ペア* と呼ばれており、IBM Client Security Software によって作成され、それぞれのクライアント上で統計的に固有です。

次に高い「レベル」の階層 (ルートの上) は、管理者公開鍵および管理者秘密鍵 (*管理者鍵*ペア) です。管理者鍵ペアは、それぞれのマシン上で固有であるか、あるい

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上で同一であっても構いません。この鍵ペアを管理する方法は、ネットワークを管理する方法に依存します。管理者秘密鍵は、それが管理者定義のロケーション内のクライアント・システム (ハードウェア公開鍵によって保護されている) にある場合、固有です。

IBM Client Security Software は、エンベデッド・セキュリティー・サブシステム環境に Windows ユーザーを登録します。ユーザーが登録されると、ユーザー公開鍵とユーザー秘密鍵 (ユーザー鍵ペア) が作成され、新しい鍵「レベル」が作られます。ユーザー秘密鍵は、管理者公開鍵で暗号化されます。管理者秘密鍵は、ハードウェア公開鍵で暗号化されます。したがって、ユーザー秘密鍵を使用するためには、管理者秘密鍵 (ハードウェア公開鍵で暗号化されている) をセキュリティー・サブシステムにロードする必要があります。チップにロードされれば、ハードウェア秘密鍵は管理者秘密鍵を復号化します。これで、管理者秘密鍵はセキュリティー・サブシステム内部で使用できる準備ができたため、対応する管理者公開鍵で暗号化されたデータは、セキュリティー・サブシステム内部でスワップされ、復号化されて、使用することができます。現行の Windows ユーザーの秘密鍵 (管理者公開鍵で暗号化されている) がセキュリティー・サブシステムに渡されます。また、エンベデッド・セキュリティー・サブシステムに効力を持つアプリケーションが必要とするデータは、いずれもチップに渡されることになり、セキュリティー・サブシステムの機密保護機能のある環境内で復号化され、効力を持ちます。この例として、無線ネットワークの認証に使用される秘密鍵があります。

鍵が必要になればいつでも、セキュリティー・サブシステム内で鍵がスワップされます。暗号化された秘密鍵はセキュリティー・サブシステム内でスワップされ、その後、チップの保護された環境で使用することができます。このハードウェア環境の外側で、秘密鍵が公開されたり、使用されることはありません。これによって、データは IBM エンベデッド・セキュリティー・チップを通じて、ほぼ完全に保護されることになります。

秘密鍵は厳重に保護される必要があること、さらに IBM エンベデッド・セキュリティー・サブシステムのストレージ・スペースには限りがあることの理由により、秘密鍵は暗号化されます。ある時点でセキュリティー・サブシステムに格納できるのはいくつかの鍵のみです。ハードウェア公開鍵およびハードウェア秘密鍵のみが、ブートからブートまでの間セキュリティー・サブシステムに格納された状態にあります。複数の鍵と複数のユーザーを可能にするために、CSS は IBM 鍵スワップ階層を利用します。鍵が必要になればいつでも、IBM エンベデッド・セキュリティー・サブシステム内で鍵がスワップされます。関連する暗号化された秘密鍵はセキュリティー・サブシステム内でスワップされ、その後、チップの保護された環境で使用することができます。このハードウェア環境の外側で、秘密鍵が公開されたり、使用されることはありません。

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、セキュリティー・サブシステム内でのみ使用可能であり、管理者秘密鍵を復号化するために使用します。管理者秘密鍵がセキュリティー・サブシステム内で復号化されると、ユーザーの秘密鍵 (公開鍵で暗号化されている) をセキュリティー・サブシステムに渡し、管理者秘密鍵で復号化することができます。複数ユーザーの秘密鍵を、管理者公開鍵で暗号化することができます。そのため、IBM ESS を持つシステ

ムでは、実質的に無制限の数のユーザーを登録できますが、最良実例からすると、1台のコンピューターで登録するユーザー数を 25 人までに制限したほうがパフォーマンスを最適化できます。

IBM ESS は、セキュリティー・サブシステム内でハードウェア公開鍵およびハードウェア秘密鍵が使用されている鍵スワップ階層を利用して、チップの外部で保管されている他のデータを保護します。ハードウェア秘密鍵はセキュリティー・サブシステム内で生成され、この機密保護機能のある環境を離れることはありません。ハードウェア公開鍵はセキュリティー・サブシステムの外部で使用可能であり、秘密鍵などの他のデータ部分を暗号化したり、保護するのに使用されます。このデータは、一度ハードウェア公開鍵で暗号化されると、ハードウェア秘密鍵でしか復号化することはできません。ハードウェア秘密鍵はセキュリティー・サブシステムの機密保護機能のある環境でのみ使用可能であるため、暗号化されたデータはこの同じ機密保護機能のある環境でしか復号化し、使用することはできません。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ハードウェア秘密鍵を持つようになるという点に注目してください。 IBM エンベデッド・セキュリティー・サブシステムの乱数機能によって、それぞれの鍵ペアは統計的に固有であることが保証されます。

CSS 公開鍵インフラストラクチャー (PKI) 機能

Client Security Software には、企業での公開鍵インフラストラクチャー (PKI) の作成に必要とされるあらゆるコンポーネントが提供されています。たとえば、次のようなコンポーネントがあります。

- **管理者によるクライアント・セキュリティー・ポリシー制御** クライアント・レベルでのエンド・ユーザーの認証は、セキュリティー・ポリシー上重要な問題です。 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、ユーザー認証マネージャー (UVM) という認証ソフトウェアの一部となっています。
- **公開鍵暗号のための鍵の管理** 管理者は、Client Security Software を使用して、コンピューター・ハードウェアおよびクライアント・ユーザー用の暗号鍵を作成します。作成された暗号鍵は、鍵の階層を介して IBM エンベデッド・セキュリティー・チップにバインドされます。そこでは、ベース・レベルの鍵を使用して、上位の鍵 (クライアント・ユーザーに関連付けられた鍵など) が暗号化されます。IBM エンベデッド・セキュリティー・チップ上で鍵を暗号化して格納すると、コンピューター・ハードウェアに鍵が確実にバインドされるため、クライアント・セキュリティーにとって不可欠なレイヤーがさらに追加されることになります。
- **IBM エンベデッド・セキュリティー・サブシステムで保護されるディジタル証明書の作成および保管** 電子メール・メッセージのディジタル署名または暗号化に使えるディジタル証明書を申請することにより、Client Security Software では、Microsoft CryptoAPI を使用するアプリケーションの暗号化サービス・プロバイダーとして IBM エンベデッド・セキュリティー・サブシステムを選択できるようになります。そのようなアプリケーションとしては、たとえば Internet Explorer や Microsoft Outlook Express などがあります。これにより、ディジタル証明書の秘密鍵が、IBM エンベデッド・セキュリティー・サブシステムにあるユーザーの公開鍵によって確実に暗号化されます。Netscape ユーザーは、セキュリティーのために使われるディジタル証明書の秘密鍵生成装置として IBM エンベデッド・

セキュリティー・サブシステムも選択できます。PKCS (Public-Key Cryptography Standard) #11 を使用するアプリケーション (たとえば Netscape Messenger など) の場合、IBM エンベデッド・セキュリティー・サブシステムにより提供されている保護を利用できます。

- **IBM エンベデッド・セキュリティー・サブシステムへのディジタル証明書の転送機能** IBM Client Security Software の証明書転送ツールを使用すれば、デフォルトの Microsoft CSP で作成した証明書を IBM エンベデッド・セキュリティー・サブシステム CSP へ転送できます。これにより、証明書に関連付けられた秘密鍵は、機密性の低いソフトウェアではなく、安全な IBM エンベデッド・セキュリティー・サブシステムに格納されることになるため、秘密鍵の機密性が大幅に高まります。

  注: IBM エンベデッド・セキュリティー・サブシステム CSP によって保護されているディジタル証明書を別の CSP にエクスポートすることはできません。
- **アーカイブおよびリカバリー・ソリューション** オリジナルの鍵が破損または損傷した場合、アーカイブから鍵を復元することが可能であるため、アーカイブの作成は、重要な PKI 機能といえます。IBM Client Security Software では、鍵および IBM エンベデッド・セキュリティー・サブシステムで作成されたディジタル証明書のための鍵のアーカイブを設定したり、それらの鍵および証明書を必要に応じて復元するためのインターフェースが提供されています。
- **ファイルおよびフォルダの暗号化** ファイルおよびフォルダの暗号化機能により、クライアント・ユーザーはファイルまたはフォルダの暗号化や復号化を行うことができます。これにより、データ・セキュリティーのレベルも向上します。
- **指紋認証** IBM Client Security Software は、認証用の Targus 指紋読取装置、一部の IBM PC に装備されている内蔵指紋読取装置をサポートします。正しい操作を行うには、Targus の場合、Targus 指紋デバイス・ドライバーをインストールする前に Client Security Software をインストールする必要があります。内蔵指紋読取装置は、あらかじめドライバがインストールされていますので、そのまま Client Security Software をインストールします。
- **スマート・カード認証** IBM Client Security Software は、特定のスマート・カードを認証装置としてサポートします。Client Security Software では、スマート・カードを一時点における単一ユーザーの認証トークンとして使用できます。クレデンシャル・ローミングを使用していない場合、各スマート・カードはシステムに結合されます。このカードはパスワードとともに使用する必要があるため、スマート・カードを必要とするシステムはよりセキュアになりますが、暗号漏えいの恐れはあります。
- **クレデンシャル・ローミング** クレデンシャル・ローミングを使用すれば、登録されたネットワーク・ユーザーは、ネットワーク上のシステムを自分のワークステーションのように使用することができます。ユーザーは、任意の Client Security Software 登録済みクライアントの使用を許可されたならば、自分のパーソナル・データをクレデンシャル・ローミング・ネットワーク上の他の任意の登録済みクライアントにインポートすることができます。そのパーソナル・データは自動的に更新され、CSS アーカイブ上、およびそのパーソナル・データがインポートされている任意のコンピューター上で維持されます。このパーソナル・データ (新規の証明書、パスフレーズの変更など) の更新内容は、ローミング・ネットワークに接続された他のすべてのコンピューターで即時に使用可能になります。

- **FIPS 140-1 認証** Client Security Software は FIPS 140-1 認証済み暗号ライブラリーをサポートします。
- **パスフレーズ有効期限** 各ユーザーを UVM に追加すると、Client Security Software は、ユーザー固有のパスフレーズとパスフレーズ有効期限のポリシーを設定します。

第 2 部 ユーザー情報

第 2 章 クライアント・ユーザー向けの使用法

この章では、クライアント・ユーザーが以下の作業を行う際に役立つ情報を提供します。

- システム・ログオン用の UVM ログオン・プロテクションの使用
- ユーザー構成ユーティリティーの使用
- セキュア E メールと Web ブラウザーの使用
- UVM サウンド設定の構成

システム・ログオン用の UVM プロテクションの使用

この章には、システム・ログオン用の UVM ログオン・プロテクションの使用についての情報が記載されています。 UVM ログオン・プロテクションを使用できるようにするためには、まずそれをコンピューターで使用可能にしておく必要があります。

UVM ログオン・プロテクションによって、オペレーティング・システムへの アクセスをログオン・インターフェースを通じて制御することができます。 UVM ログオン・プロテクションは Windows のログオン・アプリケーションを置き換えるため、ユーザーがコンピューターをアンロックすると、「Windows ログオン」ウィンドウの代わりに「IBM ユーザー認証マネージャー (UMM) セキュア・ログオン」ウィンドウが開きます。 UVM プロテクションがコンピューターで使用可能になると、コンピューターの始動時に UVM ログオン・インターフェースが開きます。

コンピューターが実行中の場合は、「**Ctrl + Alt + Delete**」を押して、UVM ログオン・インターフェースにアクセスし、コンピューターのシャットダウンとロック、タスク・マネージャーのオープン、現行ユーザーのログオフなどを行うことができます。

クライアントのアンロック

UVM ログオン・プロテクションを使用している Windows クライアントをアンロックするには、次の手順を実行します。

1. ユーザー名と UVM パスフレーズを入力します。
2. ログオンするドメインを選択します。
3. 「**OK**」をクリックします。

   注: UVM は複数のドメインを認識しますが、ユーザー・パスワードはすべてのドメインで同一である必要があります。

注:

1. UVM パスフレーズが、入力されたユーザー名およびドメインと一致しない場合は、「IBM ユーザー認証マネージャー (UMM) セキュア・ログオン」ウィンドウが再び開きます。

2. クライアントの UVM ポリシー認証要件によっては、さらに認証プロセスが必要になる場合もあります。

ユーザー構成ユーティリティー

ユーザー構成ユーティリティーによって、クライアント・ユーザーは、管理者のアクセスを必要としない各種のセキュリティー保守作業を行うことができます。

ユーザー構成ユーティリティーの機能

ユーザー構成ユーティリティーによって、クライアント・ユーザーは以下のことを行うことができます。

- **パスワードとアーカイブの更新。** このタブによって、以下の機能が行えます。
  - **UVM パスフレーズの変更。** セキュリティーを高めるために、UVM パスフレーズを定期的に変更することができます。
  - **Windows パスワードの更新。** Windows ユーザー管理プログラムを使用して UVM 認証クライアント・ユーザーの Windows パスワードを変更する場合は、IBM Client Security Software のユーザー構成ユーティリティーを使用してパスワードも変更する必要があります。管理者ユーティリティーを使用して、管理者があるユーザーの Windows ログオン・パスワードを変更すると、そのユーザーに関して以前に作成されたユーザー暗号鍵はすべて削除され、関連するディジタル証明書も無効になります。
  - **Lotus Notes パスワードのリセット。**セキュリティーを高めるために、Lotus Notes のユーザーは Lotus Notes のパスワードを変更することができます。
  - **鍵アーカイブの更新。** ディジタル証明書を作成し、IBM エンベデッド・セキュリティー・チップに格納されている秘密鍵のコピーを作成したい場合、または鍵アーカイブを別のロケーションへ移動したい場合は、鍵アーカイブを更新します。
- **UVM サウンド設定。**このタブによって、認証の成功時と失敗時に再生されるサウンド・ファイルを選択することができます。
- **ユーザーの構成。** このタブによって、以下の機能が行えます。
  - **ユーザーのリセット。** この機能によって、セキュリティー構成をリセットすることができます。セキュリティー構成をリセットすると、以前の鍵や、証明書、指紋などがすべて消去されます。
  - **アーカイブからのユーザーのセキュリティー構成を復元。**この機能によって、アーカイブから設定値を復元することができます。これは、ファイルが破壊されてしまった場合、あるいは以前の構成に戻したい場合に便利です。
  - **CSS Roaming Server への登録。** この機能を使用すると、このシステムを CSS Roaming Server に登録することができます。システムが登録されると、現行構成をこのシステムにインポートすることができます。

Windows XP におけるユーザー構成ユーティリティーの制限

Windows XP ではアクセス制限が課されるため、特定の状況の下では、クライアント・ユーザーが使える機能が限定されます。

Windows XP Professional

Windows XP Professional の場合、クライアント・ユーザー制限が適用されるのは、次のような状況にある場合です。

- Client Security Software が、後で NTFS フォーマットに変換されるパーティション上にインストールされている
- Windows フォルダが、後で NTFS フォーマットに変換されるパーティション上にある
- アーカイブ・フォルダが、後で NTFS フォーマットに変換されるパーティション上にある

上記のような状況では、Windows XP Professional の制限ユーザーが、次のようなユーザー構成ユーティリティーのタスクを実行できない場合があります。

- UVM パスフレーズの変更
- UVM に登録済みのユーザーの Windows パスワードの更新
- アーカイブの更新

管理者が管理者ユーティリティーを始動して終了した後で、これらの制限がなくなります。

Windows XP Home

Windows XP Home の制限ユーザーは、次のいずれかの状況にある場合、ユーザー構成ユーティリティーを使用できません。

- Client Security Software が、NTFS フォーマットのパーティション上にインストールされている
- Windows フォルダが、NTFS フォーマットのパーティション上にある
- アーカイブ・フォルダが、NTFS フォーマットのパーティション上にある

ユーザー構成ユーティリティーの使用

ユーザー構成ユーティリティーを使用するには、次の手順を実行します。

1. **「スタート」→「プログラム」→ 「Access IBM」→「IBM Client Security Software」→ 「セキュリティー設定の変更」**をクリックします。

   IBM Client Security Software の「ユーザー構成ユーティリティー」メイン・スクリーンが表示されます。

2. 次のいずれかのタブを選択します。
   - **パスワードとアーカイブの更新。** このタブによって、UVM パスフレーズの変更、UVM 内の Windows パスワードの更新、UVM 内の Lotus Notes のパスワードのリセット、および暗号アーカイブの更新を行うことができます。
   - **UVM サウンド設定。** このタブによって、認証の成功時と失敗時に再生されるサウンド・ファイルを選択することができます。
   - **ユーザーの構成。** このタブによって、ユーザーは、アーカイブからユーザー構成を復元したり、セキュリティー構成をリセットしたり、(コンピューターをローミング・クライアントとして使用できる場合は) ローミング・サーバーに登録したりすることができます。
3. 「**OK**」をクリックして終了します。

それぞれの手順の特定のヘルプは、Client Security Software ヘルプ・システムから利用できます。

セキュア E メールと Web ブラウザーの使用

無保護のトランザクションをインターネット経由で送信すると、そのようなトランザクションは他人に傍受されたり、読まれたりする恐れがあります。インターネットのトランザクションに対する無許可アクセスは、ディジタル証明書を取得してそれによりディジタル署名を行い、E メール・メッセージを暗号化するか、あるいは Web ブラウザーを機密保護機能のあるものにすることによって、禁止することができます。

ディジタル証明書 (ディジタル ID またはセキュリティー証明書とも呼ばれる) は、認証局によって発行され、ディジタル署名される電子的な信任状です。ディジタル証明書が発行されると、証明書の所有者としての身元が認証局によって検証されます。認証局はディジタル証明書の信頼できる提供者です。 VeriSign などのサード・パーティーの発行者を認証局として利用することもできますが、認証局を社内のサーバーとしてセットアップすることもできます。ディジタル証明書には、名前および E メールなどのユーザー識別情報、証明書の有効期限、公開鍵のコピー、認証局の ID およびそのディジタル署名が含まれます。ディジタル証明書には、氏名や E メール・アドレスといったユーザー識別情報、証明書の有効期限、公開鍵のコピー、認証局の ID およびそのディジタル署名が含まれます。

Microsoft アプリケーションでの Client Security Software の使用

このセクションでは、Outlook Express などの Microsoft CryptoAPI をサポートするアプリケーションでの Client Security Software を使用したディジタル証明書の取得および使用方法について説明します。したがって、ここで示されている説明は、Client Security Software を使用した場合に限られます。

セキュリティー設定値の作成方法、および Outlook Express や Outlook などの E メール・アプリケーションの詳細については、これらのアプリケーションで用意されている資料を参照してください。

Microsoft アプリケーションのディジタル証明書の取得

Microsoft アプリケーションで使用するディジタル証明書の作成に認証局を利用する場合、証明書の暗号サービス・プロバイダー (CSP) を選択するようにプロンプトが出されます。

Microsoft アプリケーションで IBM エンベデッド・セキュリティー・チップの暗号機能を使用するには、ディジタル証明書を取得するときに暗号サービス・プロバイダーとして、必ず「**IBM Embedded Security Subsystem CSP**」を選択してください。これにより、ディジタル証明書の秘密鍵が IBM セキュリティー・チップに確実に格納されます。

また、可能であれば、特別なセキュリティー用に強力な (つまり、高度の) 暗号化を選択してください。 IBM エンベデッド・セキュリティー・チップは、ディジタル証明書の秘密鍵について 1024 ビットまでの暗号化が可能であるため、認証局のイ

ンターフェース内で使用できる場合にはこのオプションを選択します。1024 ビットの暗号化は、「強い暗号化」と呼ばれることもあります。

CSP として「**IBM Embedded Security Subsystem CSP**」 を選択した後、ディジタル証明書を取得する認証要件を満たすために、UVM パスフレーズの入力または指紋のスキャン (あるいはその両方) を行う必要がある場合があります。 認証要件は、コンピューターの UVM ポリシーに定義されています。

Microsoft CSP からの証明書の転送

IBM CSS 証明書転送ウィザードを使用すれば、デフォルトの Microsoft CSP で作成した証明書を IBM エンベデッド・セキュリティー・システム CSP へ転送できます。証明書を転送することにより、証明書に関連付けられた秘密鍵は、機密性の低いソフトウェアではなく、安全な IBM エンベデッド・セキュリティー・サブシステムによって格納されることになるため、秘密鍵の機密性が大幅に高まります。

転送できるセキュリティー証明書には 2 つのタイプがあります。

- **ユーザー証明書:** ユーザー証明書の目的は、ユーザーに許可を与えることです。一般には、cssdesk などの認証局 (CA) からユーザー証明書を取得します。認証局とは、証明書の保管、発行、公開を行う、信頼されているエンティティーです。ユーザー証明書を必要とする場面としては、E メールの署名、E メールの暗号化、特定のサーバーへのログオンなどがあります。
- **マシン証明書:** マシン証明書の目的は、特定のコンピューターを一意的に識別することです。マシン証明書を使用する場合の認証は、コンピューターを使用するユーザーではなく、そのコンピューター自体に基づいて行われます。

CSS 証明書転送ウィザード・アプリケーションは、エクスポート可能と設定されている Microsoft 証明書だけを転送し、対象になる証明書の鍵のサイズは 1024 ビット以下に制限されています。

ユーザーがマシン証明書を転送する必要があるときに、システムに対する管理者権限を持っていない場合、管理者は、そのユーザーが証明書を転送することを可能にするために、管理者構成ファイルを送信できます。そのようにすれば、管理者パスワードを提供する必要はありません。管理者構成ファイルを作成するには、(導入先フォルダ名)¥security フォルダーにある管理者コンソール (console.exe) を使用します。導入先フォルダーのデフォルトは、c:¥Program Files¥ibm です。

CSS 証明書転送ウィザードを使用するには、次の手順を実行します。

1. **「開始」→「Access IBM」→「IBM Client Security Software」→「証明書転送ウィザード」**をクリックします。

   IBM CSS 証明書転送ウィザードのウェルカム画面が表示されます。
2. 「**次へ**」をクリックして作業を開始します。
3. 転送する証明書のタイプを選択し、「**次へ**」をクリックします。 CSS 証明書転送ウィザードで転送できるのは、Microsoft 証明書ストアにあって、エクスポート可能と設定されている証明書だけです。
4. インターフェースの「発行先」領域に表示されている証明書の名前をクリックして、転送する証明書を選択し、「**次へ**」をクリックします。証明書が正常に転送されたことを示すメッセージが表示されます。

注: マシン証明書を転送するには、管理者パスワードまたは管理者構成ファイルが必要です。

5. 「**OK**」をクリックして、CSS 証明書転送ウィザードに戻ります。

証明書を転送すると、証明書は IBM エンベデッド・セキュリティー・サブシステム CSP に関連付けられ、秘密鍵は IBM エンベデッド・セキュリティー・サブシステムによって保護されます。この秘密鍵を使用したオペレーション (ディジタル署名の作成や E メールの復号化など) は、いずれも IBM エンベデッド・セキュリティー・サブシステムの保護された環境の中から実行されます。

Microsoft アプリケーションの鍵アーカイブの更新

ディジタル証明書を作成した後、鍵アーカイブを更新することによって、証明書のバックアップを取ります。鍵アーカイブの更新には、管理者ユーティリティーを使用します。

Microsoft アプリケーションのディジタル証明書の使用

Microsoft アプリケーションでセキュリティー設定値を使用して、ディジタル証明書を表示し、使用します。詳細については、Microsoft 提供の資料を参照してください。

ディジタル証明書を作成し、それを使用して E メール・メッセージに署名した後、最初に E メール・メッセージにディジタル署名するときに、UVM から認証要件のプロンプトが出されます。ディジタル証明書を使用する認証要件を満たすために、UVM パスフレーズの入力または指紋のスキャン (あるいはその両方) を行う必要がある場合があります。 認証要件は、コンピューターの UVM ポリシーに定義されています。

UVM サウンド設定

ユーザー構成ユーティリティーでは、提供されたインターフェースを使用して、サウンド設定を構成することができます。デフォルトのサウンド設定を変更するには、次の手順を実行します。

1. **「スタート」→「プログラム」→ 「Access IBM」→「IBM Client Security Software」→ 「セキュリティー設定の変更」**をクリックします。

   IBM Client Security Software のユーザー構成ユーティリティーのスクリーンが表示されます。

2. 「**UVM サウンド設定**」タブをクリックします。
3. 「UVM 認証音」領域で、認証が成功したときに関連付けたいサウンド・ファイルへのファイル・パスを「認証成功」フィールドに入力するか、あるいは「**参照...**」をクリックしてファイルを選択します。
4. 「UVM 認証音」領域で、認証が失敗したときに関連付けたいサウンド・ファイルへのファイル・パスを「認証失敗」フィールドに入力するか、あるいは「**参照...**」をクリックしてファイルを選択します。
5. 「**OK**」をクリックして、完了します。

第 3 章 IBM Password Manager

このセクションでは、IBM Password Manager の紹介と、一般的な IBM Password Manager 機能を実行する方法についての、ステップバイステップの手順を記載しています。

IBM Password Manager の紹介

IBM Password Manager では、ユーザー ID、パスワード、その他の個人情報など、重要で、忘れやすいログイン情報を、IBM Client Security を使って管理することができます。 IBM Client Security Password Manager は、すべての情報を IBM エンベデッド・セキュリティー・サブシステムによって保管するので、UVM ユーザー認証ポリシーは、ご使用のセキュア・アプリケーションと Web サイトへのアクセスを制御します。

これは、(それぞれ別個の規則に従い、別々の有効期日を持つ) 個々のパスワードを数多く覚えたり指定する必要がなくなり、必要なのは、1 つのパスフレーズを覚え、指紋、または任意の識別エレメントの組み合わせを提供するだけになることを意味します。

IBM Client Security Password Manager によって、以下の機能が実行できます。

- **IBM エンベデッド・セキュリティー・サブシステムによる保管されたすべての情報の暗号化**

  IBM Password Manager は、IBM エンベデッド・セキュリティー・サブシステムによってすべての情報を自動的に暗号化します。これによって、重要なすべてのパスワード情報は、IBM Client Security 暗号鍵によって保護されます。
- **単純な入力転送インターフェースを使用した、ユーザー ID およびパスワードの迅速かつ簡易な転送**

  IBM Password Manager の入力転送インターフェースを使用して、ご使用の Web ブラウザーまたはアプリケーションのログイン・ダイアログに情報を直接配置します。これは入力エラーを最小限にすることに役立ち、IBM エンベデッド・セキュリティー・サブシステムによってすべての情報を安全に保管することができます。
- **自動キーによるユーザー ID およびパスワード**

  IBM Password Manager によってログイン・プロセスは自動化され、IBM Password Manager に入力しておいたログイン情報が、Web サイトにアクセスするときに自動的に入力されます。
- **セキュア・ブラウザーへの機密ログイン情報のエクスポート**

  IBM Password Manager によって、機密ログイン情報をエクスポートし、それをコンピューター間で安全に移動させることができます。 IBM Password Manager からログイン情報をエクスポートする場合、取り外し可能メディアに保管でき

る、パスワードで保護されたエクスポート・ファイルが作成されます。ごのファイルは、自分のユーザー情報およびパスワードを利用するために使用できます。

- **ランダム・パスワードの生成**

  IBM Password Manager によって、それぞれの Web サイトまたはアプリケーションごとにランダム・パスワードを生成することができます。それぞれのアプリケーションは、さらに厳格なパスワード保護を使用可能にできるので、ランダム・パスワードによってデータのセキュリティーを向上させることができます。経験からすれば、たいていのユーザーは覚えやすい個人情報をパスワードに使用し、それらは比較的簡単にクラッキングされるので、ランダム・パスワードはユーザー定義のパスワードよりはるかに安全です。

- **Password Manager インターフェースを使用した項目の編集**

  IBM Password Manager によって、すべてのアカウント項目を編集し、オプションのすべてのパスワード機能を 1 つの使いやすいインターフェースでセットアップすることができます。これによって、パスワードおよび個人情報の管理は迅速かつ簡易になります。

- **Windows デスクトップ上のアイコン・トレイからの、または単純なキーボード・ショートカットによる、Password Manager へのアクセス**

  IBM Password Manager アイコンによって、ネットサーフィン時など、別のアプリケーションを Password Manager に追加する必要がある場合はいつでも、即時アクセスが可能になります。それぞれの Password Manager 機能も、単純なショートカットキーによって簡単にアクセスできます。

- **ログイン情報のアーカイブ**

  Client Security アーカイブ機能を使用して、IBM Password Manager は、ハード・ディスクまたはシステムの障害からの保護のために、Client Security アーカイブから機密ログイン情報を復元することができます。情報をアーカイブする方法の詳細については、「*Client Security Software* ユーザーズ・ガイド 」を参照してください。

IBM Password Manager の手順

IBM Client Security Password Manager によって、ユーザーは Password Manager インターフェースを使用して、Web サイトおよびアプリケーションに情報を入力することができます。 IBM Password Manager プログラムは、IBM エンベデッド・セキュリティー・サブシステムから該当のフィールドに入力した情報を、暗号化および保管します。この情報を Password Manager に一度保管すると、UVM ユーザー認証ポリシーに従って許可された Web サイトまたはアプリケーションにアクセスする場合はいつでも、このセキュア情報が自動的にこれらのフィールドに取り込まれます。

新しい登録の作成

パスワード情報を IBM Client Security Password Manager に入力するには、以下の手順を実行します。

1. アプリケーションまたは Web サイトのログオン画面を開きます。

2. システム・トレイで「**Password Manager**」アイコンをマウスの右ボタン・クリックして、「**作成**」を選択します。

   注: Password Manager の「作成」機能は、ショートカットキー **Ctrl + Shift + H** で使用することもできます。
3. 「IBM Password Manager - 新しい登録の作成」ウィンドウのフィールドに情報を入力します。

   注: このフィールドの情報は、長さが 260 文字未満でなければなりません。
4. 入力したテキストを表示したくない場合は、「**入力され文字を ″*″ で表示する**」チェック・ボックスにチェックをつけます。

   注: このチェック・ボックスが制御するのは、Password Manager 内でテキストを表示する方法だけです。テキストが Web サイトまたはアプリケーションにドロップされた後は、そのプロパティーはそのアプリケーションによって制御されます。
5. 「場所の選択」アイコンを使用して、テキストを Password Manager ユーティリティーから、Web サイトまたはアプリケーションの該当のフィールドにドラッグします。

   注: このアイコンによって、コンピューターのクリップボードまたは他の非セキュア・ロケーションを使用せずに、テキストをコピーすることができます。
6. 必要に応じて、それぞれのフィールドに対してステップ 3 からステップ 5 を繰り返します。
7. 「**新しい登録の保存**」をクリックします。
8. 新しい登録の記述名を入力します。
9. 再呼び出し後に Password Manager にログイン情報をサブミットさせたい場合は、「**登録が呼び出されたときに、自動で Enter キーを入力する**」チェック・ボックスをチェックします。

   注: 一部の Web サイトは、ログイン情報のサブミットに Enter キーを使用しません。ログインに失敗する場合は、この便利な機能は使用不可になります。
10. 「**新しい登録の保存**」をクリックして、完了します。

項目の再呼び出し

IBM Client Security Password Manager を使用したパスワードの再呼び出しは、単純かつ簡単です。

IBM Client Security Password Manager に保管された情報を再呼び出しするには、以下の手順を実行します。

1. 再呼び出しするアプリケーションまたは Web サイトのログオン画面を開きます。
2. システム・トレイで「**Password Manager**」アイコンをダブルクリックします。 Password Manager は、ログオン画面上のフィールドに、保管済みの情報を取り込みます。

   注: Password Manager の「再呼び出し」機能は、ショートカットキー **Ctrl + Shift + G** で使用することもできます。

3. UVM パスフレーズを入力するか、または UVM ユーザー認証ポリシーによって指定された認証プロセスを実行します。
4. **「登録が呼び出されたときに、自動で Enter キーを入力する」** チェック・ボックスにチェックマークが付いていない場合は、アプリケーションまたは Web サイトの「処理依頼」ボタンをクリックします。

   項目が再呼び出しされない場合、新規項目を作成するかどうかを尋ねるプロンプトが出されます。「**はい**」をクリックして、「IBM Password Manager - 新しい登録の作成」ウィンドウを起動します。

登録の管理

IBM Client Security Password Manager によって、ユーザーは Password Manager に保管された情報を処理することができます。「Password Manager- 管理」ウィンドウによって、Web サイトまたはアプリケーションのフィールドに取り込む、Password Manager に入力されたユーザー ID、パスワード、および他の情報を変更することができます。

IBM Client Security Password Manager に保管された情報を変更するには、以下の手順を実行します。

1. システム・トレイで「**Password Manager**」アイコンをマウスの右ボタン・クリックして、「**管理**」をクリックします。

   注: Password Manager の「管理」機能は、ショートカットキー **Ctrl + Shift + B** で使用することもできます。
2. UVM パスフレーズを入力するか、または UVM ユーザー認証ポリシーによって指定された認証プロセスを実行します。
3. 情報を編集します。以下のオプションから選択します。
   - 項目情報

     項目情報を編集するには、次の手順を実行します。
     a. 編集したい項目を右クリックします。
     b. 以下のアクションから選択します。
        – ″Enter キーを押す″ を追加

          「″Enter キーを押す″ を追加」を選択して、項目情報が Web サイトまたはアプリケーションに自動的に入力されるようにします。「″Enter キーを押す″ を追加」の起動時に、その機能の横にチェック・アイコンが表示されます。
        – 削除

          「削除」を選択して、項目全体を削除します。
     c. 「**変更の保存**」をクリックします。
   - 登録内容

     登録内容を編集するには、次の手順を実行します。
     a. 編集したいフィールドを右クリックします。
     b. 以下のアクションから選択します。

– 登録内容のの変更

「登録内容の変更」を選択して、このフィールドについて保管された情報を変更します。登録内容は、以下のいずれかの方法で変更できます。

- ランダム化された項目の作成によって

  ランダム化された項目を作成するには、「ランダム化する」を選択します。 Password Manager は、長さが 7、14、または 127 文字の、ランダム化された項目を作成します。

- 登録内容の手動での編集によって

  登録内容を手動で編集するには、「編集」を選択して、フィールドに適切な変更を加えます。

– 削除

「削除」を選択して、登録内容全体を削除します。

注: Password Manager でフィールドを変更しても、Password Manager 内のログイン情報が更新されるだけです。 Password Manager のランダム化機能を使用してパスワードのセキュリティーを向上させたい場合は、アプリケーションまたは Web サイトを、この機能によって生成された新規ランダム・パスワードと同期させる必要があります。簡便な Password Manager Transfer Field Tool を使用して、新規ランダム・パスワードを、アプリケーションまたは Web サイトの「パスワードの変更」フォームに転送します。新規パスワードがアプリケーションまたは Web サイトに対して有効であることを確認し、次いで「Password Manger - 管理 」ウィンドウの「変更の保存」を使用します。必要なすべての情報は保存されているので、新規パスワードを使用して項目を再作成する必要はありません。

c. 「**変更の保存**」をクリックします。

4. 「**変更の保存**」をクリックします。

ログイン情報のエクスポート

IBM Password Manager によって、機密ログイン情報をエクスポートし、それをコンピューター間で安全に移動させることができます。 IBM Password Manager からログイン情報をエクスポートする場合、取り外し可能メディアに保管できる、パスワードで保護されたエクスポート・ファイルが作成されます。ごのファイルは、自分のユーザー情報およびパスワードを利用するために使用できます。

IBM Client Security Password Manager に保管されたログイン情報をエクスポートするには、以下の手順を実行します。

1. システム・トレイで「**Password Manager**」アイコンを右クリックして、「**管理**」をクリックします。

   注: Password Manager の「管理」機能は、ショートカットキー **Ctrl + Shift + B** で使用することもできます。

2. UVM パスフレーズを入力するか、または UVM ユーザー認証ポリシーによって指定された認証プロセスを実行します。

3. 「**エクスポート**」をクリックします。「名前をつけて保存」ウィンドウが、デフォルト・パスおよび PwMgrExportReader ファイル名とともに表示されます。
4. エクスポート・ファイルを保管するロケーションを選択します。
5. 「**保管**」をクリックして、指定したロケーションとファイル名を受け入れます。エクスポート・ファイルに設定するパスフレーズの入力を求める画面が表示されます。
6. エクスポート・ファイルにパスフレーズを設定して、「**OK**」をクリックします。このパスフレーズは、エクスポートされたデータにアクセスするために必要になります。エクスポートが正常に完成したことを示すメッセージが表示されます。
7. 「**OK**」をクリックします。
8. IBM Password Manager を閉じます。
9. 指定したロケーションから、作成済みのエクスポート・ファイルを取り出し、それを取り外し可能メディアにコピーします。

このファイルを他のコンピューターで開く前に、前述の手順で設定したエクスポート・パスフレーズの入力が求められます。 IBM Password Manager は、セキュア・リーダーで機密情報を表示します。この情報は、印刷したりコンピューターのハード・ディスクに保管することはできません。「**OK**」をクリックして、エクスポート・リーダー・ファイルを閉じます。

第 4 章 クレデンシャル・ローミング

IBM Client Security Software のクレデンシャル・ローミング機能によって、UVM ユーザーのクレデンシャルをネットワーク内のすべての ESS 対応コンピューターで使用することができます。このネットワークは、ローミング・ネットワークと呼ばれ、ユーザーがネットワークの任意のコンピューターから容易に作業できるようにすることによって、ユーザーの柔軟性を強化し、アプリケーションの可用性を高めます。

クレデンシャル・ローミングのネットワーク要件

CSS クレデンシャル・ローミング・ネットワークは、以下の必要なコンポーネントで構成されています。

- ローミング・サーバー
- ローミング・クライアント
- ネットワーク・ドライブに割り当てられた共用のアーカイブ

注: ローミング・サーバーおよびローミング・クライアントとは、単に、IBM Client Security Software 5.1 以降がインストール済みで、管理者パスワードが設定されている ESS 対応コンピューターです。

ローミング・サーバーのセットアップ

クレデンシャル・ローミング・ネットワークを構成するには、1 つのコンピューターをローミング・サーバー (システム A と呼びます) として指定する必要があります。他のコンピューターは、いったんローミング・サーバーに登録されると、ローミング・クライアント になります。 (最初に登録されたローミング・クライアントをシステム B と呼びます。)

ローミング・サーバーに指定するコンピューターについては、何も特別なことはありません。ローミング・ネットワークの一部になり得るコンピューターであれば、いずれのコンピューターでも使用できます。ローミング・サーバーとは、単に、ローミング・ネットワークにより「信頼される」コンピューターを確立することを指定されたコンピューターに過ぎません。あるコンピューターがローミング・サーバーによって登録されると、そのコンピューターはネットワーク内のすべてのコンピューターによって信頼されることになります。

ローミング・ネットワークの構成は、2 つのステップのプロセスから成っています。

1. 鍵、アーカイブ、およびローミング・ユーザーを確立することによって、ローミング・サーバーを構成します。
2. 初期クライアント (システム B) およびローミング・クライアントにする他のすべてのコンピューターをローミング・ネットワークに登録します。

ローミング・サーバーは、ローミング・ネットワークを構成し、ローミング・クライアントの登録を開始します。ただし、クレデンシャル・ローミング・ネットワークのフォーカル・ポイントは、UVM ユーザーが格納されるネットワーク・ドライブに割り当てられた共用のドライブにあります。このアーカイブには、ユーザー・クレデンシャルに対するすべての更新が格納されます。このアーカイブをローミング・サーバーまたはいずれかのローミング・クライアントに配置するべきではありません。ローミング・サーバーは、ローミング・クライアントになるコンピューターにローミング・ネットワークへの登録を許可した後は、他の任意のローミング・クライアントのように行動します。

ローミング・サーバーの構成

ローミング・サーバーを構成するには、次の手順を実行します。

1. 管理者コンソールを起動し、「**クレデンシャル・ローミングの構成**」をクリックします。
2. 「**このコンピューターをローミング・サーバーとして構成する**」にチェックを付け、「**次へ**」をクリックします。
3. 「**構成**」をクリックします。
4. 「**新しい鍵ペアを作成する**」を選択する。
5. 鍵フォルダを指定し、「新しい鍵ペアを作成する」を選択してから、「**次へ**」をクリックします。
6. アーカイブ・フォルダを入力してから、「**次へ**」をクリックします。

   注: アーカイブ・フォルダと鍵フォルダは、ローミング用に登録した他のコンピューター (ローミング・クライアント) からアクセスできるものでなければなりません。このディレクトリーは、ネットワークに割り当てられた共用のドライブでなければなりません。

   現在、そのアーカイブにファイルがある場合は、このファイルの扱い方を尋ねるプロンプトが次のウィザード・ページに出されます。
7. 「**完了**」をクリックします。

ローミング・サーバーでのクライアントの登録

ローミング・サーバーでクライアントを登録するには、次の手順を実行します。

1. ローミング・サーバーの構成が完了すると、直ちに、クレデンシャル・ローミング・ネットワークの構成の画面が表示されます。「**ローミング・クライアントの登録を許可する**」を選択し、「**次へ**」をクリックします。
2. ローミング・クライアント登録を行うユーザーで、管理者権限を持つシステム B のユーザーの名前を入力します。
3. そのユーザーが使用するパスワードを入力し、確認します。 (このプロセスと、ユーザーの UVM 使用を許可するプロセス (後で出てきます) を混同しないでください。)
4. ユーザー構成ユーティリティーを使用してローミング・クライアントを登録する場合は、そのユーザー用の管理者構成ファイルを作成する必要があります。このプロセスでは、このユーザー固有のファイルを生成します。このファイルをそのユーザーおよびシステム B にアクセス可能なロケーションに格納します。

注: 管理者ユーティリティーを使用してローミング・クライアントを登録する場合は、このファイルは必要ありません。

ローミング・クライアントとして登録するシステム (システム B) の管理者パスワードを入力します。

5. 「**次へ**」をクリックします。
6. 管理者構成ファイルを作成した場合は、そのユーザーおよびシステム B にアクセス可能なロケーションにこのファイルを保管します。

前記の手順を完了すると、ローミング・サーバーが構成されたことになります。各ローミング・クライアントで登録を完了すると、ローミング・ネットワークを使用できる状態になります。

ローミング・クライアントの登録プロセスの完了

ローミング・サーバーで信頼できるシステムのリストを登録したら、クライアント・システムで以下のいずれかの手順を実行する必要があります。ローミング・サーバーを構成し、アーカイブに接続して、はじめてクライアントの登録プロセスを完了できます。

管理者ユーティリティーを使用したローミング・クライアントの登録

管理者ユーティリティーを使用してローミング・クライアントを登録するには、次の手順を実行します。

1. 「**鍵の設定**」をクリックします。
2. 鍵をアーカイブから復元するかと問われた場合は、「**いいえ**」をクリックします。
3. 「**このコンピューターをローミング・サーバーに登録する**」を選択し、「**次へ**」をクリックします。
4. システム A により作成されたアーカイブの場所と、システム A でこのユーザー用に指定されたローミング・クライアント登録のパスワードを入力し、「**次へ**」をクリックします。

この登録を完了するのに約 1 分かかります。

ユーザー構成ユーティリティーを使用したローミング・クライアントの登録

ユーザー構成ユーティリティーを使用してローミング・クライアントを登録するには、次の手順を実行します。

1. 「ユーザーの構成」タブから、「**ローミング・サーバーに登録**」をクリックします。
2. システム A で生成した管理者構成ファイルと、システム A でこのユーザー用に指定したローミング・クライアント登録のパスワードを入力し、「**次へ**」をクリックします。
3. システム A で作成されたアーカイブの場所を入力し、「**次へ**」をクリックします。

この登録を完了するのに約 1 分かかります。

大量展開によるローミング・クライアントの登録 (サイレント・インストール)

大量展開によってローミング・クライアントをサイレント・インストール方式で登録するには、次の手順を実行します。

1. csec.ini ファイルを作成します。 CSS .ini ファイルを作成するための詳細については、「*Client Security Software インストール・ガイド*」を参照してください。
2. そのファイルの csssetup セクションで、"enableroaming=1" を追加します。これは、コンピューターをローミング・クライアントとして登録することを示しています。
3. 同じセクションで、"username=OPTION" 項目を追加します。この値は、以下の 3 つのオプションが可能です。
   - **オプション 1: "[promptcurrent]" - 大括弧を含む。** この指定は、現在ログオンしているユーザーの .dat ファイルがローミング・サーバーで生成され、現行ユーザーがローミング・クライアント登録パスワードを知っている場合に使用してください。このオプションでは、展開の前にローミング・クライアント登録パスワード (sysregpwd) を入力するための画面が表示されます。
   - **オプション 2: "[current]" - 大括弧を含む。** この指定は、現在ログオンしているユーザーの .dat ファイルがサーバーで生成された場合に使用してください。 sysregpwd は、次のステップで説明するように扱います。
   - **オプション 3: 実際のユーザー名 (たとえば、"joseph")。** このような指定ユーザー名を使用する場合は、"joseph.dat" はローミング・サーバーで前もって生成されている必要があります。また、この場合の sysregpwd についても、次のステップで説明するように扱います。
4. 上記のオプション 2 または 3 を使用する場合は、さらに "sysregpwd=SYSREGPW" 項目を指定する必要があります。これは、現行ユーザー (オプション 2 をインプリメントする場合) または指定ユーザー (オプション 3 をインプリメントする場合) のいずれかと関連付けられたローミング・クライアント登録パスワードです。
5. ローミング・クライアントの登録を完了するには、ローミング・サーバーが設定したアーカイブにコンピューターを接続します。このアーカイブを csec.ini ファイルで指定します。 CSS クレデンシャル・ローミング・サーバーで設定した鍵フォルダも csec.ini ファイルで指定する必要があります。
6. 管理者コンソールを使用して、csec.ini ファイルを暗号化します。

csec.ini ファイルの例

以下の例はサンプルの csec.ini ファイルであり、選択したクレデンシャル・ローミング・オプションによってこのファイルがどのように変わるかを示しています。そのオプションとしては、次のようなものがあります。

- **ローミング値なし。** この基本ファイルは、クレデンシャル・ローミングでは使用できません。

- **ローミング・オプション 1** このファイルは、ローミング・クライアント登録用のオプション 1 を使用してローミングに使用できます。現行ユーザーは、展開の前にローミング・クライアント登録パスワードを入力する必要があります。
- **ローミング・オプション 2** このファイルは、ローミング・クライアント登録用のオプション 2 を使用してローミングに使用できます。現行ユーザーは、ini ファイルに指定されている自分のユーザー ID とローミング・クライアント登録パスワードを入力する必要があります。
- **ローミング・オプション 3** このファイルは、ローミング・クライアント登録用のオプション 3 を使用してローミングに使用できます。この .ini ファイルではユーザーを指定します。そのユーザーのローミング・クライアント登録パスワードもこの .ini ファイルで指定する必要があります。

以下に、個々の CSEC.INI ファイルの例を示します。

[CSSSetup]	**オプション 1**	**オプション 2**	オプション 3
	[CSSSetup]	[CSSSetup]	[CSSSetup]
suppw=bootup	suppw=bootup	suppw=bootup	suppw=bootup
hwpw=11111111	hwpw=11111111	hwpw=11111111	hwpw=11111111
newkp=1	newkp=1	newkp=1	newkp=1
keysplit=1	keysplit=1	keysplit=1	keysplit=1
kpl=c:¥jgk	kpl=c:¥¥ローミング・サーバーで作成された鍵ペアが保管されているコンピューター名¥jgk	kpl=c:¥¥ローミング・サーバーで作成された鍵ペアが保管されているコンピューター名¥jgk	kpl=c:¥¥ローミング・サーバーで作成された鍵ペアが保管されているコンピューター名¥jgk
kal=c:¥jgk¥archive	kal=c:¥¥ローミング・サーバーで作成されたアーカイブが保管されているコンピューター名¥archive	kal=c:¥¥ローミング・サーバーで作成されたアーカイブが保管されているコンピューター名¥archive	kal=c:¥¥ローミング・サーバーで作成されたアーカイブが保管されているコンピューター名¥archive
pub= c:¥jk¥admin.key	pub= c:¥jk¥admin.key	pub= c:¥jk¥admin.key	pub= c:¥jk¥admin.key
pri= c:¥jk¥private1.key	pri= c:¥jk¥private1.key	pri= c:¥jk¥private1.key	pri= c:¥jk¥private1.key
wiz=0	wiz=0	wiz=0	wiz=0
clean=0	**enableroaming=1**	**enableroaming=1**	**enableroaming=1**
	username= [promptcurrent]	**username= [current]**	**username= joseph**
		sysregpwd=12345678	**sysregpwd=12345678**
	clean=0	clean=0	clean=0
[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]
enrollall=0	enrollall=0	enrollall=0	enrollall=0
enrollusers=1	enrollusers=1	enrollusers=1	enrollusers=1
user1=joseph	user1=joseph	user1=joseph	user1=joseph
user1uvmpw= q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r
user1winpw=	user1winpw=	user1winpw=	user1winpw=
user1domain=0	user1domain=0	user1domain=0	user1domain=0
user1ppchange=0	user1ppchange=0	user1ppchange=0	user1ppchange=0
user1ppexppolicy=0	user1ppexppolicy=0	user1ppexppolicy=0	user1ppexppolicy=0

user1ppexpdays=184	user1ppexpdays=184	user1ppexpdays=184	user1ppexpdays=184
[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0

ローミング・ネットワークの管理

ローミング・ネットワークのネットワーク管理者は、ユーザーを登録し、ユーザーとクライアントのネットワーク・アクセスを管理する必要があります。そのような作業の中には、ユーザー情報のインポートやユーザー・データの同期が含まれます。そのように管理すれば、CSS ローミング・ネットワーク上のユーザーとクライアントの追加や削除を簡単に行えます。また、ローミング・ネットワークの復元、管理者鍵ペアの変更、アーカイブ・ロケーションの変更などの管理作業も実行できます。

ユーザーの登録

前記の手順を完了すると、クレデンシャル・ローミング・ネットワークが構成され、ローミング・クライアントがローミング用に登録されたことになります。これで、管理者ユーティリティーを使用してユーザーを許可することができます。次にローミング・ネットワークにユーザーを登録する方法を説明します。

ユーザー・データの同期化

それぞれのユーザーのデータは、アーカイブに格納されます。また、そのデータのコピーは、そのユーザーがローミングしたすべてのコンピューターにもローカルに格納されます。変更 (証明書の取得やパスフレーズの変更など) が行われると、そのローカル・データは更新されます。コンピューターがアーカイブに接続されている場合は、そのユーザーのデータも更新されます。ユーザーが別のコンピューターにログオンすると、そのコンピューターがアーカイブにも接続されている限り、更新内容がそのコンピューターに自動的にダウンロードされます。

ただし、アーカイブへの接続は常に保証されているわけではないため、ユーザーのデータがコンピューターとアーカイブの間で矛盾していることがよくあります。アーカイブに接続されていないコンピューターでユーザーのデータの変更が行われると、その変更はアーカイブには反映されず、その結果、他のコンピューターでも反映されません。いったんそのコンピューターがアーカイブに接続されると、変更内容がアーカイブで更新されます。ただし、変更を含んでいた最初のコンピューターがアーカイブに接続される前に、アーカイブに接続されていた別のコンピューターで変更が行われた場合は、修正不可能なデータ不整合の問題が生じます。つまり、アーカイブのデータには最初のコンピューターにはない変更内容が含まれているのに対して、そのコンピューターではアーカイブにはない変更内容が含まれています。このようなことが起こった場合は、ユーザーには 2 つの異なる構成が通知さ

れ、ローカルか、アーカイブか、いずれの構成を保存すべきか選択するようにとのプロンプトが出されます。選択されなかった構成の変更は失われてしまいます。したがって、ユーザーの構成に生じたいかなる変更も、その他のコンピューターに変更が生じる前に、必ずアーカイブに対して更新することが重要です。

ローミング環境での紛失したパスフレーズの回復

ユーザーがパスフレーズを紛失したり忘れたりした場合、管理者は、ローミング・サーバー上またはいずれかの登録済みクライアント上のユーザーのパスフレーズを変更できます。この変更は、基本的にネットワーク内のすべてのシステムに反映されますが、UVM ログオン・プロテクションが使用可能になっていて、ユーザーがパスフレーズをインポートしたシステムは*例外* です。そのような場合、そのコンピューターにはパスフレーズの更新が反映されません。ユーザーがそのコンピューターにアクセスするには、パスフレーズ・バイパス・ファイルが必要であり、UVM パスフレーズのバイパスを実行する必要があります。

ユーザー情報のインポート

ユーザー情報は、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、または UVM ログオン・インターフェースを使用して、ローミング・ネットワーク上の新しいコンピューターにインポートすることができます。 インポートしたいユーザーが、この新しいコンピューターに存在しない場合は、コントロール・パネルで Windows ユーザー・アカウントを作成します。新しいコンピューター上にユーザー・アカウントを持たないユーザーをインポートする場合は、Windows のコントロール・パネルで Windows のユーザー・アカウントを作成する必要があります。

注: ユーザーをローミング・ネットワークにインポートするためには、そのユーザーはローミング・ネットワーク上の別のコンピューターで許可されている必要があります。

ユーザー構成ユーティリティーを使用したユーザー情報のインポート

ユーザー構成ユーティリティーを使用してユーザー情報をローミング・ネットワーク上の新しいコンピューターにインポートするには、インポートしたいユーザーでログオンし、**「スタート」→「プログラム」→「Access IBM」→「IBM Client Security Software」→「セキュリティー設定の変更」**をクリックし、「ユーザーの構成」タブで**「アーカイブから現在のユーザーの構成をインポートする」**をクリックします。

管理者ユーティリティーを使用したユーザー情報のインポート

管理者ユーティリティーを使用してユーザー情報をローミング・ネットワーク上の新しいコンピューターにインポートするには、ユーザーを選択して、「**登録する**」をクリックします。ユーザーをアーカイブからインポートするのかを問われた場合は、「**はい**」をクリックします。

UVM ログオン・インターフェースを使用したユーザー情報のインポート

ユーザー情報は、UVM ログオン・インターフェースを使用して、ローミング・ネットワーク上の新しいコンピューターにインポートすることができます。このプロセスは、UVM ログオン画面から開始します。ネットワーク上の所定のシステムで

ユーザーが UVM の使用をまだ許可されていない場合は、アーカイブからインポートするかどうかを尋ねるメッセージ・ボックスが表示されます。

注:

1. 新しいコンピューター上にユーザー・アカウントを持たないユーザーをインポートする場合は、Windows のコントロール・パネルで Windows のユーザー・アカウントを作成してから作業を進める必要があります。
2. ローミング・サーバー上のアーカイブにアクセスするには、そのディレクトリーが、ネットワーク・ドライブに割り当てられている必要があります。

Windows 2000 を実行するコンピューター上で UVM ログオン・プロテクションを使用してユーザー情報をローミング・ネットワーク上の新しいコンピューターにインポートするには、以下の手順を実行します。

1. ログオン時に、インポートしたいユーザーのユーザー名と UVM パスフレーズを入力します。アーカイブからユーザー情報をインポートするかどうかを確認するためのメッセージが表示されます。
2. その画面で「**はい**」をクリックしてユーザーをインポートし、「**OK**」をクリックします。
3. アーカイブ・ロケーションがネットワーク・ドライブ上にある場合は、ネットワーク共用を指定する必要があることを示す画面で「**はい**」をクリックします。
4. 標準の Windows ログオン画面で自分の Windows パスワードを入力します。アーカイブのパスを指定するための画面が表示されます。
5. アーカイブのネットワーク・パスを入力します。
6. そのネットワーク・パスのためのユーザー名とパスワードを入力します。
7. 「**OK**」をクリックします。その操作が正しく完了したら、プロファイルが正常にインポートされたことを示すメッセージが表示されます。

Windows XP を実行するコンピューター上で UVM GINA を使用してユーザー情報をローミング・ネットワーク上の新しいコンピューターにインポートするには、以下の手順を実行します。

1. ログオン時に、インポートしたいユーザーのユーザー名と UVM パスフレーズを入力します。アーカイブからユーザー情報をインポートするかどうかを確認するためのメッセージが表示されます。
2. その画面で「**はい**」をクリックしてユーザーをインポートし、「**OK**」をクリックします。
3. アーカイブ・ロケーションがネットワーク・ドライブ上にある場合は、ネットワーク共用を指定する必要があることを示す画面で「**はい**」をクリックします。
4. Windows のネットワーク・ドライブの割り当てに関する標準画面で、アーカイブのネットワーク・パスを入力します。
5. 「**完了**」をクリックします。
6. そのネットワーク・パスのためのユーザー名とパスワードを入力し、「**OK**」をクリックします。その操作が正しく完了したら、ユーザー情報が正常にインポートされたことを示すメッセージが表示されます。

注: ユーザーをローミング・ネットワークにインポートするためには、そのユーザーはローミング・ネットワーク上の別のコンピューターで許可されている必要があります。

ユーザー情報をインポートした後は、UVM を用いた認証はそのコンピューターのセキュリティー・ポリシーに基づいて行われます。そのコンピューターのセキュリティー要件が正常に準備されてはじめて、ユーザーはログオンすることができるようになります。

ローミング・ネットワークでの UVM に登録されたユーザーの削除と復元

ローミング・ネットワークからユーザーを削除するには、ネットワーク管理者が以下の管理者コンソール手順を実行する必要があります。

1. 管理者コンソール・ユーティリティーを起動し、管理者パスワードを入力します。
2. 「**クレデンシャル・ローミングの構成**」をクリックします。
3. 「**UVM とクレデンシャル・ローミング・ネットワークからユーザーを削除する**」を選択し、「**次へ**」をクリックします。必要に応じて、この操作を繰り返します。
4. 削除するユーザーを選択し、「**削除**」をクリックします。

   注: ネットワークからユーザーを削除すると、そのユーザーに属するクレデンシャルはすべて永久的に失われます。

削除されたユーザーは、ネットワーク管理者によって復元されるまで、UVM とローミング・ネットワークの使用権限を持つことができません。

ローミング・ネットワークにユーザーを復元するには、ネットワーク管理者が以下の管理者コンソール手順を実行する必要があります。

1. ユーティリティーを開始し、管理者パスワードを入力します。
2. 「**クレデンシャル・ローミングの構成**」をクリックします。
3. 「**削除されたユーザーを復元する**」を選択し、「**次へ**」をクリックします。
4. 復元するユーザーを選択し、「**復元**」をクリックします。必要に応じて、この操作を繰り返します。

   ユーザーを復元したら、そのユーザーに UVM の使用権限を再び与えることが可能になります。ユーザーの復元によって、そのユーザーに UVM の使用権限が自動的に与えられるわけではありません。

ローミング・ネットワーク上のローミング・クライアントの削除と復元

ローミング・ネットワークから登録済みクライアントを除去するには、ネットワーク管理者が以下の管理者コンソール手順を実行する必要があります。

1. ユーティリティーを起動し、管理者パスワードを入力します。
2. 「**クレデンシャル・ローミングの構成**」をクリックします。

3. 「**ローミング・ネットワークからローミング・クライアントを削除する**」を選択し、「**次へ**」をクリックします。
4. 削除するシステムを選択し、「**削除**」をクリックします。必要に応じて、この操作を繰り返します。

   注: ネットワークからクライアントを削除すると、そのシステムに属するマシン・ベースのクレデンシャルはすべて永久的に失われます。

削除されたクライアントは、ネットワーク管理者によって復元されるまで、ネットワーク・ローミング・サーバーに登録することができません。

ローミング・ネットワークに登録済みクライアントを復元するには、ネットワーク管理者が以下の管理者コンソール手順を実行する必要があります。

1. ユーティリティーを起動し、管理者パスワードを入力します。
2. 「**クレデンシャル・ローミングの構成**」をクリックします。
3. 「**削除されたローミング・クライアントを復元する**」を選択し、「**次へ**」をクリックします。
4. 復元するクライアントを選択し、「**復元**」をクリックします。必要に応じて、この操作を繰り返します。

   クライアントを復元すると、そのクライアントをローミング・サーバーに再び登録することが可能になります。クライアントの復元によって、そのクライアントが自動的に再登録されるわけではありません。

注: クライアントを削除した時点で、そのシステムに自身のクレデンシャルが存在していたユーザーは、場合によっては、自身のクレデンシャルを再びインポートする必要があります。

ローミング・ネットワーク上のローミング・クライアントへのアクセスの管理

ネットワーク管理者は、特定の登録済みクライアントに対するアクセスを一部のユーザーに許可し、他のユーザーには許可しないという設定を行いたい場合があります。

ユーザーのアクセス権限を管理するには、ネットワーク管理者が以下の管理者コンソール手順を実行する必要があります。

1. ユーティリティーを起動し、管理者パスワードを入力します。
2. 「**クレデンシャル・ローミングの構成**」をクリックします。
3. 「**ローミング・クライアントへのユーザー・アクセスを管理する**」を選択し、「**次へ**」をクリックします。
4. 「**ローミング・ネットワーク上のコンピューターを選ぶ**」ボックスで、管理する登録済みクライアントを選択します。 2 つのリスト・ボックスに、アクセス権限のあるユーザーとアクセス権限のないユーザーがそれぞれ表示されます。
5. 次のいずれかを行います。
   - ユーザーに対してアクセスを制限するには、「**許可されたユーザー**」リストからユーザーを選択し、「**許可しない**」をクリックします。必要に応じて、この操作を繰り返します。

- 制限されているユーザーにアクセス権限を付与するには、「**許可されていないユーザー**」リストからユーザーを選択し、「**許可する**」をクリックします。必要に応じて、この操作を繰り返します。

ローミング・ネットワークのアクセス管理機能は、アーカイブ内に新しいフォルダを作成することを前提としています。その新しいフォルダは、ネットワーク管理者にとっては書き込み可能でなければならず、他のユーザーにとっては読み取り専用でなければなりません。ユーザーがこのフォルダに対する書き込みアクセス権限を持てば、自分自身や自分のシステムを手動で復元することができてしまいます。

ローミング・ネットワークの復元

ソフトウェアまたはハードウェアの障害が生じた場合には、ローミング・ネットワークを復元する必要がある場合があります。ローミング・サーバーが破壊された場合や、CSS が使用するデータが登録済みクライアント上で破壊された場合は、管理者ユーティリティーを使用して、ローミング環境以外の場合と同じ方法でデータを復元します。ローミング・ネットワークに登録されているローミング・クライアントの IBM エンベデッド・セキュリティー・サブシステムに障害が起こった場合や、そのサブシステムがクリアされた場合は、ローミング・クライアントをローミング・サーバーに再登録する必要があります。これ以外のアクションは不要です。

鍵ペアの変更

ローミング・ネットワークでは鍵ペアの変更は、それぞれのクライアントをローミング・サーバーで再登録することが必要になるので、お勧めできません。

ローミング・ネットワークで鍵ペアを変更する場合は、以下のステップをネットワークのすべてのコンピューターで実行する必要があります。

1. ローミング・サーバー上で、管理者ユーティリティーを使用して管理者鍵ペアを変更します。
2. ネットワーク内のすべてのローミング・クライアントをローミング・サーバーに再登録します。
3. メッセージが表示されたら、常に既存ファイルを保存します。

アーカイブ・フォルダの変更

ローミング・ネットワーク内のそれぞれのコンピューターは同一アーカイブにアクセスしているため、ローミング環境でアーカイブ・フォルダを変更するのと、ローミング環境以外で変更するのとでは若干異なります。

ローミング・ネットワークでアーカイブを変更するには、次の手順を実行します。

1. 以下の手順により、古いアーカイブ・フォルダから新しいアーカイブ・フォルダにファイルをコピーします。
   a. 管理者ユーティリティーを起動し、管理者パスワードを入力します。
   b. 「**鍵の設定**」をクリックします。
   c. 「アーカイブ・フォルダを変更する」を選択してから、「**次へ**」をクリックします。
   d. 新しいアーカイブ・フォルダを入力してから、「**次へ**」をクリックします。

e. すべてのファイルを古いフォルダから新しいフォルダへコピーするようにとのメッセージが表示されたら、「**はい**」をクリックします。

2. 以下の手順により、新しいアーカイブを使用するように、ネットワーク上の他のすべてのコンピューターを更新します。
   a. 管理者ユーティリティーを開始し、管理者パスワードを入力します。
   b. 「**鍵の設定**」をクリックします。
   c. 「アーカイブ・フォルダを変更する」を選択してから、「**次へ**」をクリックします。
   d. 新しいアーカイブ・フォルダを入力してから、「**次へ**」をクリックします。
   e. すべてのファイルを古いフォルダから新しいフォルダへコピーするようにとのメッセージが表示されたら、「**いいえ**」をクリックします。

ファイルおよびフォルダの暗号化 (FFE)

ローミング・ネットワークからクライアントマシンを削除した場合は、保護していたフォルダは一時的にアクセスできなくなりますので、注意が必要です。保護フォルダはコンピューターごとのベースで管理されます。例えば、フォルダがユーザー A によってシステム A で保護されている場合は、システム B に同じ名前のフォルダがあっても、ユーザーがそれをシステム B で保護しない限り、保護されません。

IBM Password Manager

IBM Password Manager を使用して保護されているすべてのパスワードは、ローミング・ネットワークのすべてのコンピューターで使用することができます。

ローミングの用語と定義

以下の用語は、ローミング・ネットワークのセットアップに関連した概念や手順を理解するのに役立ちます。

ローミング・クライアントの登録
コンピューターをローミング・サーバーに登録するプロセス。

ローミング・クライアント
ローミング・ネットワークにおけるすべての信頼できるコンピューター。

ローミング・サーバー
ローミング・ネットワークを開始するために使用する ESS コンピューター。

ローミング・クライアント登録のパスワード
コンピューターをローミング・サーバーに登録する際に使用するパスワード。

第 3 部 管理者情報

第 5 章 Client Security Software の使用法

管理者は、Client Security Software が提供する複数のコンポーネントを使用して、CSS クライアント・ユーザーに必要なセキュリティー機能をセットアップできます。次の例を参考にして、Client Security のポリシーと構成を計画してください。たとえば、Windows 2000 と Windows XP のユーザーは、システム・ログオン用の UVM プロテクションをセットアップすると、権限のないユーザーが CSS クライアントに ログオンするのを禁止することができます。

(例 1) ともに Outlook Express を使用する 1 つの Windows 2000 クライアントと 1 つの Windows XP クライアント

この例では、1 つの CSS クライアント (クライアント 1) に Windows 2000 と Outlook Express がインストールされ、もう 1 つのクライアント (クライアント 2) には Windows XP と Outlook Express がインストールされています。クライアント 1 で UVM の認証セットアップが必要なユーザーは 3 人、クライアント 2 で UVM の認証セットアップが必要なのは 1 人とします。すべてのクライアント・ユーザーが認証用の指紋を登録します。この例では、UVM 対応指紋センサーをインストールします。両方のクライアントとも Windows へのログオンには UVM ログオン・プロテクションを必要とすることにします。管理者は、UVM ポリシーの編集と使用を各クライアントで実行することに決めたとします。

Client Security をセットアップするには、次の手順を実行します。

1. クライアント 1 とクライアント 2 に Client Security Software をインストールします。詳しくは、「*Client Security Software インストール・ガイド*」を参照してください。
2. 各クライアントに UVM 対応指紋センサーおよび関連ソフトウェアをインストールします。

   UVM 対応製品については、Web サイトを参照してください (http://www.ibm.com/jp/pc/security/css/security.html)。
3. 各クライアント上で UVM でユーザー認証をセットアップします。以下のことを行います。
   a. ユーザーに UVM パスフレーズを割り当てることによって、ユーザーを UVM に登録します。クライアント 1 には 3 人のユーザーがいるので、すべてのユーザーを登録するまで、ユーザーを UVM に登録するプロセスを繰り返します。
   b. 各クライアントで UVM ログオン・プロテクションをセットアップします。
   c. ユーザーの指紋を登録します。 3 人のユーザーがクライアント 1 を使用するようにポリシーが設定されているので、3 人のユーザーがすべてクライアント 1 で指紋を登録する必要があります。クライアント 2 では 1 人のユーザーの指紋を登録する必要があります。

注: クライアントの UVM ポリシーの一部の認証要件として指紋を設定する場合は、各ユーザーが自分の指紋を登録する必要があります。

4. 次の操作についての認証を必要とする各クライアントで UVM ポリシーを編集および保存します。
   - Windows へのログオン
   - ディジタル証明書の獲得
   - Outlook Express 用のディジタル署名の使用
5. 各クライアントを再始動して、UVM ログオン・プロテクションを有効にします。
6. 設定した UVM パスフレーズと CSS クライアントの UVM ポリシーに設定した認証要件を UVM パスフレーズのユーザーに知らせます。

クライアント・ユーザーは、次のタスクを実行できるようになります。

- UVM ログオン・プロテクションを使用して、Windows をロックおよびアンロックする。
- ディジタル証明書を申請し、その証明書に関連した暗号サービス・プロバイダーとしてエンベデッド・セキュリティー・サブシステムを選択する。
- ディジタル証明書を使用して、Outlook Express で作成された E メール・メッセージを暗号化する。

(例 2) Lotus Notes を使用する 2 つの Windows 2000 CSS クライアント

この例では、2 つの CSS クライアント (クライアント 1 とクライアント 2) に Windows 2000 と Lotus Notes がインストールされています。クライアント 1 で UVM の認証セットアップが必要なユーザーは 2 人、クライアント 2 で UVM の認証セットアップが必要なのは 1 人とします。両方のクライアントは、UVM ログオン・プロテクションを必要とします。管理者は、クライアント 1 の UVM ポリシーを編集し、それをクライアント 2 にコピーすることにしました。

Client Security をセットアップするには、次の手順を実行します。

1. クライアント 1 とクライアント 2 に Client Security Software をインストールします。同じ UVM ポリシー・ファイルを使用するため、クライアント 1 とクライアント 2 にソフトウェアをインストールする際には同じ管理者公開鍵を使用する必要があります。このソフトウェアのインストールの詳細については、「*Client Security Software インストール・ガイド*」を参照してください。
2. 各クライアント上で UVM でユーザー認証をセットアップします。その後で、次の操作を実行します。
   a. ユーザーに UVM パスフレーズを割り当てることによって、ユーザーを UVM に登録します。クライアント 1 には 2 人のユーザーがいるので、すべてのユーザーを登録するまで、ユーザーを UVM に登録するプロセスを繰り返す必要があります。
   b. 各クライアントで UVM ログオン・プロテクションをセットアップします。
3. 両方のクライアントで UVM プロテクションの Lotus Notes サポートを有効にします。

4. クライアント 1 で UVM ポリシーを編集してからこのポリシーが保存されているファイルをクライアント 2 にコピーします。UVM ポリシーでは、スクリーン・セーバーの解除、Lotus Notes へのログオン、および Windows へのログオンにユーザー認証が必要です。詳しくは 63 ページの『UVM ポリシーの編集と使用』を参照してください。
5. 各クライアントを再始動して、UVM ログオン・プロテクションを有効にします。
6. UVM パスフレーズ、および各クライアントに設定されたポリシーをクライアント・ユーザーに知らせます。

(例 3) Tivoli Access Manager で管理され、E メールに Netscape を使用する複数の Windows 2000 CSS クライアント

次の例では、UVM ポリシーにより設定される認証オブジェクトの管理に Tivoli Access Manager の使用を計画する企業の管理者を対象としています。この例では、複数の CSS クライアントに Windows 2000 と Netscape がインストールされています。すべてのクライアントに、Tivoli Access Manager のコンポーネントである NetSEAT クライアントがインストールされています。 LDAP サーバーを使用するすべてのクライアントには、LDAP クライアントがインストールされています。UVM ポリシーにより Tivoli Access Manager がクライアント用に選択された認証オブジェクトを制御できます。

この例では、各クライアントで UVM の認証セットアップが必要なユーザーはそれぞれ 1 人です。すべてのユーザーが、認証用の指紋を登録します。この例では、UVM 対応指紋センサーをインストールし、Windows のログオンではすべてのクライアントで UVM ログオン・プロテクションが必要になります。

Client Security をセットアップするには、次の手順を実行します。

1. Tivoli Access Manager サーバーに Client Security コンポーネントをインストールします。詳しくは、「*Tivoli Access Manager での Client Security の使用法*」を参照してください。
2. すべてのクライアントに Client Security Software をインストールします。UVM ポリシーが使用されるため、このソフトウェアをインストールする際にはすべてのクライアントで同じ管理者公開鍵を使用する必要があります。ソフトウェアのインストールについては、「*Client Security Software インストール・ガイド*」をお読みください。
3. 各クライアントに UVM 対応指紋センサーおよび関連ソフトウェアをインストールします。使用可能な UVM 対応製品については、Web サイト (http://www-6.ibm.com/jp/pc/security/) を参照してください。
4. 各クライアント上で UVM でユーザー認証をセットアップします。詳しくは 44 ページの『ユーザーの登録』を参照してください。その後で、次の操作を実行します。
   a. ユーザーに UVM パスフレーズを割り当てることによって、ユーザーを UVM に登録します。
   b. 各クライアントで UVM ログオン・プロテクションをセットアップします。

c. 各クライアント・ユーザーの指紋を登録します。 CSS クライアントで指紋の認証が必要な場合は、そのクライアントのすべてのユーザーが指紋を登録する必要があります。

5. 各クライアントで Tivoli Access Manager セットアップ情報を構成します。詳しくは、「*Tivoli Access Manager での Client Security の使用法*」を参照してください。
6. いずれかのクライアントで UVM ポリシーを編集および保管してから、他のクライアントにその UVM ポリシーをコピーします。 Tivoli Access Manager が次の認証オブジェクトを制御するように UVM ポリシーを設定します。
   - Windows へのログオン
   - ディジタル証明書の獲得
   - Outlook Express 用のディジタル署名の使用

   詳しくは 63 ページの『UVM ポリシーの編集と使用』を参照してください。
7. 各クライアントを再始動して、UVM ログオン・プロテクションを有効にします。
8. 各クライアントに IBM エンベデッド・セキュリティー・サブシステム PKCS#11 モジュールをインストールします。このモジュールは、Netscape を使用して E メール・メッセージを送受信し、IBM エンベデッド・セキュリティー・サブシステムを使用してディジタル証明書を取得するクライアントに暗号サポートを提供します。詳しくは、「*Client Security Software インストール・ガイド*」を参照してください。
9. Tivoli Access Manager を使用して、Tivoli Access Manager 管理コンソールに表示される IBM Client Security Solutions オブジェクトを制御します。
10. 設定した UVM パスフレーズ、および各クライアントに設定されたポリシーをクライアント・ユーザーに知らせます。
11. クライアント・ユーザーに「*Client Security Software ユーザーズ・ガイド*」を参照して次のタスクを習得するようにアドバイスしてください。
    - UVM プロテクションを使用して、Windows をロックおよびアンロックする。
    - ユーザー構成ユーティリティーを使用する。
    - 証明書に関連した暗号サービス・プロバイダーとしてエンベデッド・セキュリティー・サブシステムを使用するディジタル証明書を申請する。
    - ディジタル証明書を使用して、Netscape で作成された E メール・メッセージを暗号化する。

第 6 章 ユーザーの許可

以下の情報は、Windows ユーザーをユーザー認証マネージャー (UVM) に登録する場合に役に立ちます。

クライアント・ユーザーの認証

クライアント・レベルでのエンド・ユーザーの認証処理は、コンピューターのセキュリティーにおける重要な考慮点です。 Client Security Software は、CSS 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。

CSS クライアントの UVM セキュリティー・ポリシーは、次の 2 とおりの異なる方法で管理することができます。

- CSS 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

最初のユーザーを追加すると、ハードウェア暗号鍵が生成されます。

認証エレメント

認証エレメント (たとえば、UVM パスフレーズやユーザーの指紋) は、CSS クライアントにユーザーを許可するのに使用されます。Windows ユーザーを UVM に登録するときは、クライアント・ユーザーに UVM パスフレーズを割り当てます。256 文字以内の UVM パスフレーズは、UVM が使用する主な認証エレメントです。UVM パスフレーズを割り当てる際に、ユーザー暗号鍵がそのクライアント・ユーザーに対して作成され、IBM エンベデッド・セキュリティー・サブシステムによって管理される 1 つのファイルに保管されます。 CSS クライアントが UVM 対応デバイスを認証に使用する場合は、ユーザーの指紋などの認証エレメントを UVM に登録しておく必要があります。

ユーザー認証のセットアップ時に、Client Security Software で使用する、次の機能を選択できます。

- **オペレーティング・システム・ログオン用の UVM プロテクション。** UVM プロテクションでは、UVM によって認識されたユーザーだけがオペレーティング・システムにアクセスできるようにします。システム・ログオンを行うために UVM プロテクションを使用可能にする前に、詳細について、「50 ページの『UVM ログオン・プロテクションのセットアップ』」を参照してください。
- **Client Security スクリーン・セーバー。** クライアント・ユーザーを追加した後、このユーザーは、Client Security スクリーン・セーバーをセットアップし、使用することができます。 Client Security スクリーン・セーバーは、Windows のコントロール・パネルの「画面」オプションを使用してセットアップされます。Client Security スクリーン・セーバーを使用するには、UVM ログオン・プロテクションを有効にする必要があります。

ユーザーを登録する前に

重要: Windows へのログオンに使用できるユーザー・アカウントのみを登録してください。Windows へのログオンに使用できないユーザー・アカウントを登録した場合、UVM ログオン・プロテクションを有効にすると、**すべての**ユーザーがシステムから締め出されます。

重要: UVM を使用するには、セットアップで少なくとも一人のクライアント・ユーザーを登録する**必要があります。** Client Security Software をはじめてセットアップするときに登録済みのユーザーがないと、目的のセキュリティー設定は適用**されず**、その情報は保護**されません**。

クライアント・ユーザーを許可する場合、管理者ユーティリティーに選択可能なユーザー名のリストが用意されます。リストに示される名前は、Windows を使用することによって追加されたユーザー・アカウントです。UVM にクライアント・ユーザーを追加する前に、Windows を使用して、それらのユーザーのユーザー・アカウントとプロファイルを作成します。Client Security Software は、Windows のセキュリティー機能と結合して動作します。

「ユーザーとパスワード」プログラムを使用して、新しいユーザー・アカウントを作成し、ユーザー・アカウントまたはグループを管理します。詳しくは、Microsoft の資料を参照してください。

注:

1. Windows を使用して新規ユーザーを作成する場合、各新規ユーザーのドメイン・パスワードは同一でなければなりません。
2. Windows ユーザー名が以前に変更されたユーザーは登録しないでください。UVM は以前のユーザー名を指しますが、Windows は新規のユーザー名しか認識しません。
3. 登録されたユーザー・アカウントが Windows から削除されると、UVM ログオン・プロテクション・インターフェースに、そのアカウントが Windows にログオンするために使用できるアカウントとして、誤ってリストされ続けます。このアカウントは、Windows へのログオンには使用できません。
4. ユーザーが登録された後は、その Windows ユーザー名を変更しないでください。変更すると、UVM で新しいユーザー名を許可し直し、すべての新しいクレデンシャルを要求する必要があります。

ユーザーの登録

ユーザーが管理者ユーティリティーを使用するには、管理者権限でログオンする必要があります。

ユーザーを UVM に登録するには、次の手順を実行します。

1. CSS クライアントの Windows デスクトップから、「**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**」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。
2. 管理者パスワードを入力し、「**OK**」をクリックします。

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. 「登録する Windows ユーザーの選択」領域で、リストからユーザー名を選択します。

   注: リスト内のユーザー名は、Windows で作成されたユーザー・アカウントによって定義されます。

4. 「**登録する**」をクリックします。

   「ユーザー認証設定」画面が表示されます。

5. 新規ユーザーのパスフレーズ有効期限の設定を検討および選択します。デフォルトでは、「**次回の使用時に、UVM パスフレーズを変更させる**」チェック・ボックスにチェックが入っており、パスフレーズは 184 日後に有効期限が切れるように設定されています。

6. 新規に登録するユーザーのパスフレーズを入力し、「**次へ**」をクリックします。

   パスフレーズが UVM パスフレーズ設定のルールに合致しない場合は、画面に入力したパスフレーズが無効であることが表示されます。その場合は、「**OK**」、次に「**UVM パスフレーズのルール**」をクリックして、有効なパスフレーズの満たすべきパラメーターを表示させます。

   パスフレーズが受け入れられると、操作が正常に完成したことを示すメッセージが表示されます。

7. 「**OK**」をクリックして続行します。

   「Windows ログオン・パスワード」画面が表示されます。セキュア UVM ログオンが使用可能になると、ユーザーがシステムにログオンできるようにユーザーの現在の Windows パスワードを保管する必要があります。この画面で、管理者は次のいずれかを行うことができます。

   - **ログオン時またはユーザー構成ユーティリティーを使用して、後でユーザーが Windows パスワードを登録させる。** ユーザー構成ユーティリティーを使用してユーザーに後で Windows パスワードを保管させるには、該当するラジオ・ボタンを選択して、「**次へ**」をクリックします。
   - **今、ユーザーの Windows パスワードを保存する。** ユーザーの現在の Windows パスワードを今すぐ保管するには、提示されたフィールドにユーザーの Windows パスワードを入力して確認し、「**次へ**」をクリックします。

     注: ここで入力するパスワードは、現在のユーザーの Windows パスワードと一致している必要があります。この設定は、Windows に保管されているパスワードには影響しません。

   操作が正常に完成したことを示すメッセージが表示されます。

8. 「**OK**」をクリックします。
9. 「**完了**」をクリックします。

ユーザーを削除する

ユーザーが管理者ユーティリティーを使用するには、管理者権限でログオンする必要があります。

UVM からユーザーの登録を取り消すには、次の手順を実行します。

1. CSS クライアントの Windows デスクトップから、「**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**」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。
2. 管理者パスワードを入力し、「**OK**」をクリックします。

   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. 「UVM に登録済みの Windows ユーザー」領域でリストからユーザー名を選択します。
4. 「**ユーザーの削除**」をクリックします。

   メッセージが表示されて、すべてのユーザーの既存の鍵、証明書、登録済みの指紋および保管済みのパスワードなどの、選択したユーザーのセキュリティー情報が失われることを警告します。
5. 「**はい**」をクリックして続行します。

   ユーザーのアーカイブ情報を除去するかどうかの確認メッセージが表示されます。この情報を除去すると、ユーザーは以前に保管したすべての設定値を、どのシステムにも復元できなくなります。
6. 「**はい**」をクリックして操作を完了します。

新規ユーザーを作成する

ユーザーが管理者ユーティリティーを使用するには、管理者権限でログオンする必要があります。

新規ユーザーを作成するには、次の手順を実行します。

1. CSS クライアントの Windows デスクトップから、「**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**」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。
2. 管理者パスワードを入力し、「**OK**」をクリックします。

   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. 「登録する Windows ユーザーの選択」領域で、「**新しい Windows ユーザーの作成**」をクリックします。

   「ユーザーとパスワード」画面が表示されます。
4. 「**追加**」をクリックします。

5. 提示されたフィールドに名前を入力して新規アカウントの名前を指定し、「**次へ**」をクリックします。パスワードを設定する場合は、パスワードを入力して「**次へ**」をクリックします。
6. 該当するラジオ・ボタンを選択して、アカウント・タイプを指定します。
7. 「**完了**」をクリックします。
8. 管理者ユーティリティーに戻ります。

   新規ユーザー・アカウントが、「登録する Windows ユーザーの選択」領域に表示されます。

第 7 章 追加の UVM 機能

登録されると、次のような Client Security 機能を使用できます。

- **UVM ログオン・プロテクション。** 詳しくは、『UVM ログオン・プロテクションの計画』を参照してください。
- **Lotus Notes ユーザー用の拡張認証プロテクション。**
- **PKCS#11 準拠のアプリケーションの使用可能化。**
- **パスフレーズの変更。**
- **ユーザーの指紋の登録。** 詳しくは、56 ページの『ユーザーの指紋を登録する』を参照してください。

  UVM にユーザーを追加する前に UVM 認識指紋センサーがインストールされている場合は、UVM にユーザーを追加するときに指紋を登録します。

UVM ログオン・プロテクション

UVM ログオン・プロテクションは、Windows のパスワード機能を拡張します。通常の Windows ログオンが UVM ログオン・インターフェースに置き換わります。したがって、ユーザーがシステムにログオンしようとするたびに、UVM ログオン・ウィンドウが開きます。

UVM ログオン・プロテクションの計画

Windows ログオン用の UVM プロテクションを設定および使用する前に、次の情報をお読みください。

- UVM ポリシーに Windows ログオンに指紋認証を使用するように示されていて、ユーザーが指紋を登録していない場合は、指紋を登録しないとログオンできません。

  また、UVM で Windows パスワードが登録されていない場合 (あるいは間違って登録されていると)、ログオンするときにもユーザーは正しい Windows パスワードを入力する必要があります。
- UVM プロテクションが使用可能になっている場合は、IBM エンベデッド・セキュリティー・チップをクリアしないでください。そのようなことを行うと、ロックアウトはされず、通常の Windows ログオンになります。詳しくは、79 ページの『付録 A. トラブルシューティング』の『管理者へのヒント』を参照してください。
- 管理者ユーティリティーの「**Windows ログオンを UVM ログオンに置き換える**」チェック・ボックスのチェックを外すと、システムは UVM ログオン・プロテクションを使用せずに Windows ログオン・プロセスに戻ります。
- UVM ログオン・プロテクションを有効にし、Cisco LEAP 機能を使用可能にする場合は、Cisco Aironet Client Utility (ACU) を再インストールする必要があります。

UVM ログオン・プロテクションのセットアップ

UVM ログオン・プロテクションをセットアップするには、次の手順を実行します。

1. IBM クライアントの Windows デスクトップから、「**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**」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。入力し、OK をクリックします。「管理者ユーティリティー」のメイン・ウィンドウが表示されます。
2. 「**アプリケーション サポートとポリシーの構成**」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。
3. 「**Windows ログオンを UVM ログオンに置き換える**」チェック・ボックスを選択します。
4. 「**OK**」をクリックします。
5. 「**終了**」をクリックします。
6. すべてのアプリケーションを閉じます。
7. コンピューターを再起動します。

コンピューターが再起動すると、コンピューターへのログオンを促すプロンプトが出されます。 UVM ログオン・プロテクションについては、 49 ページの『UVM ログオン・プロテクション』を参照してください。

UVM パスフレーズの回復

IBM クライアントのセキュリティー・ポリシーによって許可されるユーザーごとに、UVM パスフレーズが作成されます。パスフレーズは紛失したり、忘れたりする可能性や、クライアント・ユーザーによって変更される場合もあるため、管理者ユーティリティーでは、管理者は紛失や忘れられたパスフレーズを回復または変更することができます。

UVM パスフレーズの回復手順を開始するには、次の手順を実行します。

1. IBM クライアントの Windows デスクトップから、「**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**」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。パスワードを入力し、OK をクリックします。「管理者ユーティリティー」のメイン・ウィンドウが表示されます。
2. 「UVM に登録済みの Windows ユーザー」領域でユーザーを選択します。
3. 「**パスフレーズの変更**」をクリックします。

   「パスフレーズを変更してください」画面が表示されます。
4. アーカイブフォルダのパスとディレクトリー名を入力するか、「**参照**」をクリックしてディレクトリーを検索します。
5. 「秘密鍵ファイル」フィールドに管理者秘密鍵のパスとファイル名を入力するか、「**参照**」をクリックしてファイルを検索します。

6. 「**OK**」をクリックします。

   管理者秘密鍵が複数のファイルに分割されている場合、各ファイルのロケーションと名前を入力するように求めるメッセージが表示されます。「鍵ファイル」フィールドにファイルを入力するごとに、「**次の読込み**」をクリックしてください。
7. 「UVM パスフレーズ」フィールドにユーザーの新しい UVM パスフレーズを入力し、「UVM パスフレーズの確認」フィールドでパスフレーズを確認します。「**UVM パスフレーズのルール**」をクリックして、UVM セキュリティー・ポリシーによって実行される規則のリストを表示します。
8. 「パスフレーズの有効期限」領域で、パスフレーズの有効期限に関する使用可能な規則を選択して設定します。
9. 「**次へ**」をクリックします。操作が正常に完了したことを示すメッセージが表示されます。
10. 「**完了**」をクリックします。

Lotus Notes ユーザー用の拡張認証プロテクション

UVM は、Lotus Notes ユーザー用に拡張されたセキュリティー・プロテクションを提供します。

Lotus Notes ユーザー ID 用の UVM ログオン・プロテクションを使用可能にし、構成する

Lotus Notes で UVM ログオン・プロテクションを使用できるようにする前に、IBM クライアントに Lotus Notes をインストールし、ユーザーの Lotus Notes ユーザー ID とパスワードを設定し、Lotus Notes ユーザーによる UVM の使用を許可する必要があります。

Lotus Notes 用の UVM ログオン・プロテクションを有効にするには、次の手順を実行します。

1. IBM クライアントの Windows デスクトップから、「**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**」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。パスワードを入力し、OK をクリックします。「管理者ユーティリティー」のメイン・ウィンドウが表示されます。
2. 「**アプリケーション サポートとポリシーの構成**」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。
3. 「**Lotus Notes サポートを有効にする**」チェック・ボックスを選択します。

   Lotus Notes ユーザー ID の UVM プロテクションが使用可能になります。必要であれば、次のオプション・ステップを続行して Lotus Notes ログオンのポリシーを構成します。
4. 「**アプリケーション・ポリシー**」をクリックします。

「ポリシー構成の変更」画面が表示されます。

5. 「**ポリシー編集**」をクリックします。
6. 管理者パスワードを入力し、「**OK**」をクリックします。「IBM UVM ポリシー：」画面が表示されます。
7. 「オブジェクトの選択」タブで、「処理」ドロップダウン・メニューの「**Lotus Notes ログイン**」を選択します。
8. 「認証エレメント」タブで、Lotus Notes のログオンに必要な認証エレメントを選択します。
9. 「**適用**」をクリックして、選択内容を保管します。

「秘密鍵の要求」画面が表示されます。

10. 提示されたフィールドにパス名を入力するか、または「**参照**」をクリックし、該当するフォルダを選択して、秘密鍵のロケーションを指定します。
11. 「**OK**」をクリックします。

「オブジェクトの選択」タブをクリックしたときの IBM UVM ポリシー画面で「ポリシーの要約」をクリックすると、IBM ユーザー認証マネージャー (UVM)：ポリシーの要約画面にローカル・クライアント・ポリシーで制御されるオブジェクトの要約が表示されます。

12. Lotus Notes を開始します。

Lotus Notes サポートを有効にし、初めて Notes を起動する場合は、次に続く手順に従い、Lotus Notes パスワードを UVM に登録します。

Lotus Notes 内の UVM ログオン・プロテクションを使用する

Lotus Notes で UVM プロテクションを使用する前に、『Lotus Notes 内の UVM ログオン・プロテクションをセットアップする』のステップを実行します。

Lotus Notes 内の UVM ログオン・プロテクションをセットアップする

Lotus Notes 内で UVM プロテクションをセットアップするには、次の手順を実行します。

1. Lotus Notes にログインします。

「IBM ユーザー認証マネージャー」ウィンドウが表示されます。

2. Lotus Notes パスワードを該当のフィールドで入力および確認します。

これで Lotus Notes パスワードが UVM に登録されました。

Lotus Notes パスワードを変更する

Lotus Notes パスワードをリセットするには、次の手順を実行します。

1. Lotus Notes にログインします。
2. Lotus Notes のメニュー・バーから、「**ファイル**」→「**セキュリティ**」→「**ユーザー・セキュリティ**」の順にクリックします。

「IBM ユーザー認証マネージャー」ウィンドウが表示されます。

3. UVM パスフレーズを入力して、「**OK**」をクリックします。

   「ユーザー・セキュリティ」ウィンドウが表示されます。
4. 「**パスワードの変更**」をクリックします。

   「IBM ユーザー認証マネージャー」ウィンドウが表示されます。
5. 「**あなた自身のパスワードを作成**」ラジオ・ボタンを選択します。
6. 新しい Lotus Notes のパスワードを該当のフィールドで入力および確認し、「**OK**」をクリックします。

注: Lotus Notes 内でパスワードを以前に使用した値に変更するとき、Notes はパスワードの変更を拒否しますが、Client Security Software には通知しません。その結果、UVM は Notes が拒否したパスワードを変更します。

Lotus Notes 内でパスワードを変更する際に、パスワードが以前に使用されていたことを示すメッセージを受け取る場合、Lotus Notes を終了し、ユーザー構成ユーティリティーを始動して、Lotus Notes のパスワードを元の値に復元することが必要になります。

Lotus Notes パスワードがランダムに生成され、このエラーが出る場合、パスワードが何であったか知る方法はないので、パスワードを手作業でリセットする必要があります。管理者に新規 ID ファイルを要求するか、以前に保管していた ID ファイルのコピーを復元する必要があります。

Lotus Notes サポートを無効にする

Lotus Notes サポートを無効にするには、次の操作を実行します。

1. IBM クライアントの Windows デスクトップから、「**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**」をクリックします。

   管理者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・ウィンドウが表示されます。
2. 「**アプリケーション サポートとポリシーの構成**」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。
3. 「**Lotus Notes サポートを有効にする**」チェック・ボックスを選択解除します。
4. 「**OK**」をクリックします。

   「アプリケーション・サポート処理」画面に Lotus Notes のサポートが無効になっていることを示すメッセージが表示されます。

切り替えられた Lotus Notes ユーザー ID 用の UVM ログオン・プロテクションをセットアップする

UVM プロテクションが使用可能になっているユーザー ID から、別のユーザー ID に切り替えるには、次の操作を実行します。

1. Lotus Notes を終了します。

2. 現行ユーザー ID の Lotus Notes サポートを無効。詳しくは、 53 ページの『Lotus Notes サポートを無効にする』を参照してください。
3. Lotus Notes に入ると、ユーザー ID が切り替わります。ユーザー ID の切り替えについては、ご使用の Lotus Notes の資料を参照してください。
4. 切り替え先のユーザー ID の UVM プロテクションをセットアップするには、ユーザー構成ユーティリティーを使用し、 Lotus Notes パスワードの設定を行います。その後、管理ユーティリティーで Lotus Notes サポートを有効にします。

PKCS#11 準拠のアプリケーションを使用可能にする

ここに記載されている情報は、Client Security Software の使用に固有のものです。PKCS#11 をサポートするアプリケーション (Netscape や RSA SecurID Software) でのディジタル証明書の取得と使用に関連しています。

Netscape アプリケーションのセキュリティー設定の使用法について詳しくは、Netscape が提供する資料を参照してください。 IBM Client Security Software は、Netscape バージョン 4.8 および 7.1 のみをサポートします。

注: Client Security Software で 128 ビット・ブラウザーを使用するには、IBM エンベデッド・セキュリティー・チップが 256 ビット暗号をサポートしている必要があります。管理者ユーティリティーの「**セキュリティー・チップの設定**」ボタンをクリックすることで、Client Security Software によって提供される暗号化強度が分かります。

IBM エンベデッド・セキュリティー・チップ PKCS#11 モジュールをインストールする

ディジタル証明書を使用する前に、IBM エンベデッド・セキュリティー・チップ PKCS#11 モジュールをコンピューターにインストール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 PKCS#11 モジュールのインストールには、UVM パスフレーズが必要であるため、UVM に 1 人以上のユーザーが登録されている必要があります。

Netscape を使用して IBM エンベデッド・セキュリティー・チップ PKCS#11 モジュールをインストールするには、次の手順を実行します。

1. Netscape を開き、「**ファイル**」→「**ページを開く**」をクリックします。
2. `ibmpkcsinstallt.html` または `ibmpkcsinstalls.html` インストール・ファイルを見つけます。

   (ソフトウェアをインストールする際にデフォルトのディレクトリを受け入れた場合、ファイルは C:¥Program Files¥IBM¥Security に存在します。)
3. Netscape で `ibmpkcsinstallt.html` または `ibmpkcsinstalls.html` インストール・ファイルを開きます。

   このセキュリティー・モジュールのインストールを確認するメッセージが表示されます。
4. 「**OK**」をクリックします。

   「UVM パスフレーズ」ウィンドウが開きます。

5. UVM パスフレーズを入力して、「**OK**」をクリックします。

モジュールがインストールされたことを知らせるメッセージが表示されます。

ディジタル証明書を生成するために IBM エンベデッド・セキュリティー・サブシステムを選択する

ディジタル証明書作成時に、鍵を作成するカードまたはデータベースの選択を求められるので、「**IBM Embedded Security Subsystem Enhanced CSP**」を選択します。

ディジタル証明書の生成と、Netscape での使用について詳しくは、Netscape が提供する資料を参照してください。

鍵アーカイブを更新する

ディジタル証明書を作成した後、鍵アーカイブを更新することによって、証明書のバックアップを取ります。ユーザー構成ユーティリティーを使用すると、鍵アーカイブを更新できます。

PKCS#11 モジュールのディジタル証明書を使用する

ディジタル証明書の表示、選択、および使用には、アプリケーションのセキュリティー設定を使用します。たとえば、Netscape Messenger のセキュリティー設定では、E メール・メッセージにディジタル署名するか、暗号化するのに証明書を使用する前に、その証明書を選択しておかなければなりません。詳しくは、Netscape の説明書を参照してください。

IBM エンベデッド・セキュリティー・サブシステム PKCS#11 モジュールをインストールすると、UVM は、ディジタル証明書を使用するごとに認証要求画面が表示されます。認証要求の画面に従い、UVM パスフレーズの入力または指紋のスキャン、あるいはその両方が必要になります。認証要件は、コンピューターの UVM ポリシーに定義されています。

UVM ポリシーが設定する認証要件を満たさない場合は、エラー・メッセージが表示されます。このメッセージで「**OK**」をクリックすると、アプリケーションは開きますが、IBM エンベデッド・セキュリティー・サブシステムによって生成されたディジタル証明書を使用することはできません。アプリケーションを再始動し、正しい UVM パスフレーズまたは指紋、あるいはその両方を入力すると使用できるようになります。

パスフレーズを変更する

ユーザーが自分のパスフレーズを忘れてしまった場合、管理者はそのユーザーのパスフレーズを変更することができます。

リモート側でのパスフレーズの変更

リモート側でパスワードを変更するには、次の手順を実行します。

- **管理者**

  リモートの管理者は、以下のことを行う必要があります。

1. 一回限りのパスワードを新たに作成し、ユーザーに伝えます。
2. データ・ファイルをユーザーに送信します。

   このデータ・ファイルは、E メールでユーザーに送信することも、ディスケットなどの取り外し可能メディアにコピーすることも、あるいはユーザーのアーカイブ・ファイル (ユーザーがこのシステムにアクセスできるという前提) に直接書き込むことも可能です。この暗号化されたファイルを使用して、新しい一回限りのパスワードと突き合わせます。

- **ユーザー**

  ユーザーは、以下のことを行う必要があります。

1. コンピューターにログオンします。
2. パスフレーズの入力画面が出されたならば、「パスフレーズの代わりにテンポラリー・パスワードで認証する」のチェック・ボックスにチェックマークを付けます。
3. リモートの管理者から伝えられた一回限りのパスワードを入力し、管理者から送信されたファイルのロケーションを指定します。

   UVM が、ファイル内の情報と提供されたパスワードが一致することを検証した後、ユーザーはアクセスが認可されます。その後、ユーザーは直ちにパスフレーズを変更するようにプロンプトが出されます。

これが、紛失したパスフレーズを変更する際にお勧めできる方法です。

パスフレーズの手動変更

自分のパスフレーズを忘れたユーザーのシステムのところへ管理者が行ける場合は、管理者はユーザーのシステムで管理者としてログオンし、管理者ユーティリティーに対する秘密鍵を与え、ユーザーのパスフレーズを手動で変更することができます。パスフレーズを変更する際に、管理者はそのユーザーの元のパスフレーズを知っている必要はありません。

ユーザーの指紋を登録する

UVM ポリシーを編集して指紋認証を含めると、それぞれのユーザーは UVM に指紋を登録する必要があります。

UVM にユーザーの指紋を登録するには、次の管理者ユーティリティーの手順を実行します。

1. 「UVM に登録済みの Windows ユーザー」領域でリストからユーザー名を選択します。
2. 「**ユーザーの編集**」をクリックします。

   「ユーザー構成の変更 - UVM ユーザー属性の編集」ウィンドウが表示されます。
3. 「**指紋およびスマートカードの登録**」のチェック・ボックスを選択してから、「**次へ**」をクリックします。

「ユーザー構成の変更 - UVM で使用可能なデバイス」ウィンドウが表示されます。

4. 「**指紋の登録**」をクリックします。
5. 「手の選択」領域で、「**左**」または「**右**」をクリックします。
6. 「指の選択」領域で、スキャンして登録しようとする指をクリックして選択し、「**登録開始**」をクリックします。
7. UVM 対応指紋センサーに指を置き、画面の指示に従います。

   スキャナーのモデルによっては、1 つの指紋について 3 回のスキャンが必要になります。指紋スキャンを取り消すには、「**この指をキャンセル**」をクリックします。
8. 登録するほかの指を指定するか、または「**終了**」をクリックして終了します。

第 8 章 UVM ポリシーの処理

注: ローカル・クライアント用の UVM ポリシーを編集する前に、必ず、鍵が設定されていることを確認します。

ユーザーが UVM に登録された後、IBM クライアントごとにセキュリティー・ポリシーを編集し、保管する必要があります。Client Security Software が提供するセキュリティー・ポリシーは、UVM ポリシーと呼ばれます。これは、「ユーザーの登録」に指定した設定とクライアント・レベルの認証要件とを結合します。 UVM ポリシー・ファイルは、ネットワーク経由でクライアントにコピーできます。

管理者ユーティリティーには UVM ポリシー・エディターが組み込まれ、これを使用してクライアントの UVM ポリシーを編集して保管できます。IBM クライアントで実行されたタスク (たとえば、Windows へのログオンやスクリーン・セーバーのアンロックなど) は、認証オブジェクトと呼ばれます。これらのオブジェクトは、UVM ポリシー内で割り当てられた認証要件を持っています。たとえば、次の要求を行うように UVM ポリシーを設定できます。

- 各ユーザーは、Windows にログオンする際に、UVM パスフレーズを入力し、指紋認証を使用しなければならない。
- 各ユーザーは、ディジタル証明書を獲得するたびに UVM パスフレーズを入力しなければならない。

Tivoli Access Manager を使用して、UVM ポリシーで設定された個々の認証オブジェクトを制御することもできます。詳しくは、「*Tivoli Access Manager での Client Security Software の使用法* 」を参照してください。

UVM ポリシーは、個々のユーザーではなく、IBM クライアントに対して認証オブジェクトの要件を設定します。したがって、オブジェクト (たとえば、Windows のログオン) に指紋認証を必要とする UVM ポリシーを設定する場合、UVM の使用を許可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おく必要があります。

UVM ポリシーは、`globalpolicy.gvm` という名前のファイルに保管されます。ネットワーク経由で UVM を使用するには、UVM ポリシーを 1 つの IBM クライアントに保管してから、他のクライアントにコピーする必要があります。UVM ポリシー・ファイルを他のクライアントにコピーすると、それらのクライアントにUVM ポリシーをセットアップする時間を節約できます。

UVM ポリシーの編集

UVM ポリシーを編集し、それが編集されたクライアントでのみ使用します。デフォルトの位置に Client Security をインストールした場合、UVM ポリシー・ファイルは アーカイブ・フォルダの下の System フォルダの現在ログオンしているコンピューター名のフォルダの下に保存されます。¥archive¥systems¥コンピューター名¥globalpolicy.gvm として保管されます。 UVM ポリシー・ファイルを編集および保管するには、UVM ポリシー・エディターを使用します。UVM ポリシー・エディターのインターフェースは、管理者ユーティリティーで提供されます。

認証は、ポリシー・エディターで選択する内容に基づいて行われます。たとえば、Lotus Notes のログオンで「パスフレーズは最初の一回目だけ要求」を選択して Lotus Notes にログオンすると、UVM 認証画面が表示されます。その後は、リブートまたはログオフをするまでは、Lotus Notes にアクセスしてもパスフレーズは求められません。

認証オブジェクト (たとえば、Windows のログオン) に指紋を必要とする UVM ポリシーを設定すると、登録済みの各 UVM 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 ポリシーの編集時に、「**ポリシーの要約**」をクリックすると、ポリシー要約情報を表示できます。「**適用**」をクリックすると変更内容を保管することもできます。「**適用**」をクリックすると、秘密鍵を尋ねるメッセージが表示されます。管理者秘密鍵を入力して、「**OK**」をクリックし、変更内容を保管します。間違った管理者秘密鍵を入力すると、変更内容は保管されません。

オブジェクトの選択

UVM ポリシー・オブジェクトは、ユーザーのさまざまな動作に対応するセキュリティー・ポリシーを確立します。有効な UVM オブジェクトが、管理者ユーティリティーの「IBM UVM ポリシー」画面の「**オブジェクトの選択**」タブに指定されます。

有効な UVM ポリシー・オブジェクトは次のとおりです。

Windows へのログオン
このオブジェクトは、システムにログオンするときの認証要件を制御します。

スクリーン・セーバー解除
このオブジェクトは、Client Security スクリーン・セーバーを解除するときの認証要件を制御します。

Lotus Notes ログイン
このオブジェクトは、Lotus Notes へのログオンするときの認証要件を制御します。

Lotus Notes パスワード変更
このオブジェクトは、UVM を使用して Lotus Notes パスワードを変更する時、ランダム Lotus Notes パスワードを生成するときの認証要件を制御します。

Outlook メールの署名
このオブジェクトは、Microsoft Outlook または Outlook Express で「署名」ボタンをクリックするときの認証要件を制御します。

Outlook メールの復号化
このオブジェクトは、Microsoft Outlook または Outlook Express で「復号化」ボタンをクリックするときの認証要件を制御します。

ファイルとフォルダの保護
このオブジェクトは、右クリックによる暗号化と復号化を選択するときの認証要件を制御します。また IBM File and Folder Encryption でファイル・フォルダを保護/保護の解除するときの認証要件を制御します。

パスワード・マネージャー

このオブジェクトは、IBM Password Manager (IBM Web サイトから入手可能) を使用するときに必要な認証要件を制御します。 CSS 5.4 では、CSS 本体と同時に導入されます。

PKCS#11 ログイン

このオブジェクトは、PKCS#11 モジュールが PKCS#11 C_OpenSession の呼び出しを受けたときに必要となる認証要件を制御します。この設定を「パスフレーズは最初の一回目だけ要求」のままにしておくことをお勧めします。

Entrust ログイン

このオブジェクトは、Entrust が PKCS#11 モジュール向けに PKCS#11 C_OpenSession の呼び出しを発行するときに必要となる認証要件を制御します。この設定を「パスフレーズは最初の一回目だけ要求」のままにしておくことをお勧めします。

Entrust ログイン・パスワード変更

このオブジェクトは、Entrust ログオン・パスワードを変更するときの認証要件を制御します。Entrust は、PKCS#11 モジュール向けに PKCS#11 C_OpenSession の呼び出しを出してこれを行います。 この設定を「パスフレーズは最初の一回目だけ要求」のままにしておくことをお勧めします。

認証エレメント

UVM ポリシーにより、使用可能にする各オブジェクトに必要な使用可能な認証エレメントを設定します。これによりユーザーのさまざまな動作に対応するセキュリティー・ポリシーを設定できます。

管理者ユーティリティーの「IBM UVM ポリシー」画面の「**認証エレメント**」タブで選択できる認証エレメントには、次のものがあります。

パスフレーズの選択

これを選択すると、ユーザーの認証にパスフレーズを使用することができます。パスフレーズ要求の頻度を次の 3 つから選びます。

- 毎回パスフレーズ要求
- 最初の一回目だけパスフレーズ要求
- Windows ログオン時に認証したら、以後は要求しない

指紋の選択

これを選択すると、ユーザーの認証に指紋を使用することができます。指紋要求の頻度を次の 3 つから選びます。

- 毎回指紋要求
- 最初の一回目だけ指紋要求
- Windows ログオン時に認証したら、以後は要求しない

全体的な指紋の設定

これを選択すると、システムからユーザーがロックアウトされる前に行う、認証の最大再試行数を管理者が設定できます。また、ここで指紋認証を UVM パスフレーズでオーバーライドすることもできます。

スマートカードの選択
これを選択すると、ユーザーの認証にスマートカードを使用できます。

全体的なスマートカードの設定
これを選択すると、スマートカード認証をパスフレーズでオーバーライドできるようにポリシーを設定することができます。

UVM ポリシー・エディターを使用する

UVM ポリシー・エディターを使用するには、次の管理者ユーティリティー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。
2. 「**アプリケーション・ポリシー**」ボタンをクリックします。

   「ポリシー構成の変更」画面が表示されます。
3. 「**ポリシー編集**」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。
4. 管理者パスワードを入力し、「**OK**」をクリックします。

   「IBM UVM ポリシー」画面が表示されます。
5. 「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、認証要件を割り当てるオブジェクトを選択します。

   「処理」には、「Windows へのログオン」、「スクリーンセーバー解除」、「Outlook メールの復号化」などのオブジェクトが含まれています。オブジェクト・タイプの例としては「ディジタル認証の獲得」があります。
   - 「**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、選択したオブジェクトを Tivoli Access Manager が管理できるようにします。IBM クライアントの認証エレメントを Tivoli Access Manager に管理させる場合にのみ、このオプションを選択します。詳しくは、「*Tivoli Access Manager での Client Security の使用法*」を参照してください。

     重要: Tivoli Access Manager がオブジェクトを管理できるようにする場合、Tivoli Access Manager のオブジェクト・スペースに制御権を渡すことになります。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。
   - 「**選択したオブジェクトへの全アクセスを拒否**」を選択して、選択したオブジェクトのアクセスを拒否します。
6. 選択するオブジェクトごとに、次のいずれかを実行します。
   - 「**認証エレメント**」タブをクリックし、オブジェクトに割り当てたい使用可能な認証エレメントの設定を編集します。
7. 「**OK**」をクリックして、変更内容を保管して終了します。

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、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 ¥アーカイブフォルダ¥Systems¥コンピューター名 ¥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。

- ¥globalpolicy.gvm.sig¥globalpolicy.gvm
- ¥globalpolicy.gvm.sig¥globalpolicy.gvm.sig

globalpolicy.gvm globalpolicy.gvm.sig は、アーカイブ・フォルダ¥Systems¥現在ログオンしているコンピューター名¥ に保存されます。このファイルをクライアントの ¥アーカイブ・フォルダ¥Systems¥現在ログオンしているコンピューター名¥ にコピーする必要があります。

第 9 章 その他のセキュリティー管理者機能

IBM クライアントに Client Security Software をセットアップする場合、管理者ユーティリティーを使用して、IBM エンベデッド・セキュリティー・チップの有効化、管理者パスワードの設定、ハードウェア鍵の生成、およびセキュリティー・ポリシーのセットアップを行います。ここでは、管理者ユーティリティーの起動方法を説明します。

管理者ユーティリティーを開くには、次の手順を実行します。

1. IBM クライアントの Windows デスクトップから、「**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**」をクリックします。

   管理者ユーティリティーへのアクセスは管理者パスワードによって保護されているので、管理者パスワードを入力するように求めるメッセージが表示されます。
2. 管理者パスワードを入力し、「**OK**」をクリックします。

管理者コンソールの使用

Client Security Software 管理者コンソールを使用して、セキュリティー管理者は、自分のシステムから管理者特定タスクをリモート実行することができます。

管理者コンソール・アプリケーション (console.exe) は、`¥program files¥ibm¥security` ディレクトリーにインストールされています。管理者コンソール・アプリケーションは、そこから実行する必要があります。

管理者コンソールを使用すれば、セキュリティー管理者は次の機能を実行することができます。

- **認証エレメントのバイパスまたはオーバーライド** 管理者が実行できるバイパスまたはオーバーライド機能としては、次のものがあります。
  - **UVM パスフレーズのバイパス** この機能により、UVM パスフレーズをバイパスすることができます。この機能を使用すると、パスワード・ファイルと一緒にランダムな一時パスフレーズが作成されます。管理者は、このパスワード・ファイルをユーザーに送信し、他の手段を使用してパスワードを伝えます。このパスワードとファイルによってパスフレーズをバイパスし、新しいパスフレーズに変更することができます。
  - **指紋/スマートカード オーバーライド・パスワードの表示/変更** この機能により、管理者は、セキュリティー・ポリシーが指紋またはスマートカードをパスフレーズでオーバーライドできないように設定されている場合でも、セキュリティー・ポリシーをオーバーライドすることができます。この機能は、ユーザーの指紋読取装置が故障した場合、あるいはスマートカードが使用できない場合に必要になることがあります。セキュリティー管理者は、オーバーライド・パスワードを作成したり、ユーザーに E メール送信することができます。
- **アーカイブ情報へのアクセス** 管理者コンソールで操作を行うときは次のものが必要になります。

- **アーカイブ・フォルダ**
- **公開鍵**
- **秘密鍵**

- **その他のリモート管理者機能** 管理者コンソールを使用すれば、セキュリティー管理者はリモート側で次の機能を実行することができます。
  - **管理者構成ファイルの作成** この機能により、セキュリティー管理者は、管理者構成ファイルを生成することができます。管理者構成ファイルは、ユーザーが、クライアント・ユーティリティーを使用して、ユーザー自身を登録またはリセットする場合に必要となります。セキュリティー管理者は、通常、管理者構成ファイルをユーザーに E メールで送ります。
  - **セットアップ構成ファイルの暗号化/復号化** この機能により、セットアップ構成ファイルの暗号化が可能になり、セキュリティーがさらに向上します。この機能は、ファイルを復号化して編集可能にもします。
  - **クレデンシャル・ローミングの構成** ローミングの設定ができます。ローミング・ネットワークを設定すると、ネットワーク上のすべての UVM 認可ユーザーは、このシステムの自分のパーソナル・データ(パスフレーズ、証明書など)にアクセスすることができます。

アーカイブ・ロケーションの変更

アーカイブを初めて作成すると、すべての暗号鍵のコピーが作成されて、インストール時に指定したロケーションに保管されます。

注: クライアント・ユーザーは、ユーザー構成ユーティリティーを使用して、アーカイブを更新することもできます。詳しくは、13 ページの『第 2 章 クライアント・ユーザー向けの使用法』を参照してください。

アーカイブ・ロケーションを変更するには、次の管理者ユーティリティーの手順を実行します。

1. 「**鍵の設定**」ボタンをクリックします。

   「鍵の構成の変更」画面が表示されます。
2. 「**アーカイブ・フォルダを変更する**」ラジオ・ボタンをクリックした後、「**次へ**」をクリックします。

   「鍵の構成の変更 - 新しいアーカイブ・フォルダ」画面が表示されます。
3. 新しいパスを入力するか、「**参照**」をクリックしてパスを選択します。
4. 「**OK**」をクリックします。

   操作が完了したことを示すメッセージが表示されます。
5. 「**完了**」をクリックします。

鍵ペアの変更

管理者鍵をアーカイブ・ロケーションに保管した場合、そのコピーした鍵のことを鍵ペアといいます。これらの鍵は、通常はディスケットまたはネットワーク・ディレクトリーに保管します。

注: 鍵ペアを変更する前に、必ずアーカイブを更新してください。

鍵ペアを変更するには、管理者ユーティリティーで次の手順を実行します。

1. 「**鍵の設定**」ボタンをクリックします。

   「鍵の構成の変更」画面が表示されます。
2. 「**鍵ペアの変更**」ラジオ・ボタンをクリックし、「**次へ**」をクリックします。

   「鍵構成の変更 - 公開鍵」画面が表示されます。
3. 「新しい鍵」領域の「公開鍵」フィールドに、新しい公開鍵のファイル名を入力します。「**作成**」をクリックして、新しい公開鍵を生成することもできます。

   注: 新しい公開鍵は、必ず、現在の鍵ファイルを格納しているロケーション以外のロケーションに作成してください。
4. 「新しい鍵」領域の「秘密鍵」フィールドに、新しい秘密鍵のファイル名を入力します。「**作成**」をクリックして、新しい秘密鍵を生成することもできます。

   注: 新しい秘密鍵は、必ず、現在の鍵ファイルを格納しているロケーション以外のロケーションに作成してください。
5. 「古い鍵」領域の「公開鍵」フィールドに、古い公開鍵のファイル名を入力するか、「**参照**」をクリックしてファイルを検索します。
6. 「古い鍵」領域の「秘密鍵」フィールドに、古い秘密鍵のファイル名を入力するか、「**参照**」をクリックしてファイルを検索します。
7. 「アーカイブの場所」領域で、格納されているファイル・パスを入力するか、「**参照**」をクリックしてパスを選択します。
8. 「**次へ**」をクリックします。

   注: 鍵ペアが複数のファイルに分割されている場合は、各ファイルの位置と名前を入力するように求めるメッセージが表示されます。フィールドにファイル名を入力するごとに、「**次の読込み**」をクリックしてください。

   操作が正常に完了したことを示すメッセージが表示されます。
9. 「**OK**」をクリックします。

   操作が完了したことを示すメッセージが表示されます。
10. 「**完了**」をクリックします。

アーカイブからの鍵の復元

システム・ボードを交換した場合や、ハード・ディスク障害によってユーザー鍵の完全性が損なわれた場合は、鍵を復元する必要があります。鍵を復元する場合、アーカイブから最新のユーザー鍵ファイルをコピーし、IBM エンベデッド・セキュリティー・サブシステムにそれらを保管します。鍵を復元すると、セキュリティー・チップに現在保管されている鍵をすべて上書きします。

コンピューター内の元のシステム・ボードを、IBM エンベデッド・セキュリティー・サブシステムを備えた新しいシステム・ボードに交換するときに、暗号鍵がハード・ディスク上で有効なままである場合、コンピューターに以前に関連づけられていた暗号鍵を復元することができます。これを行うには、新しいシステム・ボード上の IBM エンベデッド・セキュリティー・サブシステムを使用してそれらを「再暗号化」します。新しいチップを使用可能にし、管理者パスワードを設定した後で、鍵の修復を実行します。

新しいセキュリティー・サブシステムを使用可能にし、管理者パスワードを設定するための詳細については、74 ページの『IBM エンベデッド・セキュリティー・サブシステムを使用可能（有効）にし、管理者パスワードを設定する』を参照してください。

注: 鍵の修復後、UVM ログオンが自動的に使用可能になります。したがって、復元するシステムで UVM ログオンに指紋認証が必要な場合は、システムからロックアウトされないようにするために、復元の後再始動する*前*に、指紋ソフトウェアをインストールする必要があります。

次の説明では、管理者ユーティリティーがハード・ディスクの障害によって損傷していないものと想定します。ハード・ディスクの障害によりクライアント・セキュリティー・ファイルが損傷した場合、Client Security Software の再インストールが必要になる場合があります。

鍵の修復に関する要件

鍵の修復操作を正常に実行するには、以下の条件を満たす必要があります。

- 復元するシステムのコンピューター名は、元のシステムのコンピューター名と一致している必要があります。
- 復元するシステムは、鍵ペアと元のシステムのアーカイブ・ロケーションに対するアクセス権限を持っている必要があります。
- 復元するシステムは、クリアして使用可能にした状態の IBM セキュリティー・サブシステムを持っている必要があります。 (チップを使用可能にしてクリアするには、BIOS を使用します。)
- 復元するシステムは、元のシステムと同じレベルの IBM セキュリティー・サブシステム (つまり、TCG か、非 TCG かという点で同じサブシステム) を持っている必要があります。

修復のシナリオ

IBM Client Security の修復シナリオとして、以下の 3 つが考えられます。

- **システム・ボードの交換。** 元のシステム・ボードを交換しなければならない場合や、ハード・ディスクを新しいシステムに移す場合は、アーカイブに保管されている元のシステムの鍵を使用して、IBM セキュリティー・サブシステムを再確立する必要があります。
- **システム全体の交換。** 元のシステムが失われたり、盗まれたりした場合は、アーカイブ・ロケーションに保管されている情報に基づいて、IBM セキュリティー・サブシステムと IBM Client Security Software の両方を再確立する必要があります。
- **ハード・ディスクの交換。** 元のシステムでハード・ディスクに障害が起きた場合や、元のシステムに新しいハード・ディスクを取り付ける場合は、アーカイブから IBM Client Security Software を復元する必要があります。

システム・ボードの交換

IBM エンベデッド・セキュリティー・サブシステムが使用可能になっているコンピューターのシステム・ボードを交換するには、次の手順を実行します。

1. デスクトップから「**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**のアイコンをクリックします。
2. 管理者パスワードを入力し、確認し、「**OK**」をクリックします。
3. 元のシステムのアーカイブ・ロケーションと鍵ロケーションをそれぞれのフィールドに入力し、「**OK**」をクリックします。
4. 「**OK**」をクリックします。
5. 「**終了**」をクリックして、管理者ユーティリティーを閉じます。

   コンピューターは完全に復元されています。コンピューターをリブートしてから作業を進めてください。

システム全体の交換

新しいシステムに IBM Client Security Software をインストールした後、システムを再始動すると、CSS セットアップ・ウィザードが自動的に実行されます。システム全体の交換を開始し、アーカイブに保管されている情報を再確立するには、次の手順を実行します。

1. CSS セットアップ・ウィザードの開始ページで、「**拡張機械**」をクリックし「**次へ**」をクリックします。
2. 新しいシステムの管理者パスワードを入力し、確認し、「**次へ**」をクリックします。
3. 「**存在する鍵を使用する**」ラジオ・ボタンを選択し、アーカイブに保管されている元のシステムの公開鍵と秘密鍵のロケーションをそれぞれのフィールドに入力します。
4. アーカイブ・フォルダ領域で、一時的なアーカイブ・ロケーションを入力します。

   注:

   a. このロケーションは、後の手順で元のシステム・アーカイブからシステムを還元に復元した後の時点で、削除してください。

   b. 残りの情報は、元のアーカイブの復元処理で上書きされるので、デフォルト値を使用します。

5. 「**次へ**」をクリックします。
6. 「IBM エンベデッド・セキュリティー・サブシステムでアプリケーションを保護する」ページで、「**次へ**」をクリックします。
7. 「ユーザーを登録する」ページで、「**次へ**」をクリックします。
8. 「コンピューターのセキュリティー・レベルを選ぶ」ページで、「**次へ**」をクリックします。
9. 「セキュリティーの設定を確認してください」ページで、「**終了**」をクリックします。
10. 「**OK**」をクリックします。
11. 『ハード・ディスクの交換』 の手順に進みます。

ハード・ディスクの交換

ハード・ディスクの交換後に、アーカイブから IBM Client Security Software を復元するには、次の手順を実行します。

1. デスクトップより「**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**のアイコンをクリックします。
2. CSS セットアップ・ウィザードで設定した管理者パスワードを入力し、「**OK**」をクリックします。
3. 「**鍵の設定**」をクリックします。
4. 「**アーカイブから鍵を復元する**」ラジオ・ボタンを選択し、「**次へ**」をクリックします。
5. 元のシステムのアーカイブ・フォルダの場所と秘密鍵の場所をそれぞれのフィールドに入力し、「**次へ**」をクリックします。
6. 「**OK**」をクリックします。
7. 「**完了**」をクリックして、メインの構成ページに戻ります。
8. 「**終了**」をクリックして、管理者ユーティリティーを閉じます。

   コンピューターは完全に復元されています。コンピューターをリブートしてから作業を進めてください。

認証失敗カウンターのリセット

ユーザーの認証失敗カウンターをリセットするには、次の管理者ユーティリティーの手順を実行します。

1. 「UVM に登録済みの Windows ユーザー」領域で、ユーザーを選択します。
2. 「**失敗回数のリセット**」をクリックします。

   「ユーザーの失敗回数のリセット」画面が表示されます。
3. 選択したユーザーのアーカイブを該当のフィールドに入力するか、または「**参照**」をクリックしてアーカイブ・フォルダを入力します。
4. 選択したユーザーについて、秘密鍵ファイルの名前を該当のフィールドに入力するか、または「**参照**」をクリックして秘密鍵ファイルの保存されている場所を入力します。
5. 「**OK**」をクリックします。

操作が正常に終了したことを知らせるメッセージが表示されます。

6. 「**OK**」をクリックします。

Tivoli Access Manager 設定情報の変更

次の情報は、UVM セキュリティー・ポリシー用の認証オブジェクトの管理に Tivoli Access Manager の使用を計画しているセキュリティー管理者を対象にしています。詳しくは、「*Tivoli Access Manager での Client Security の使用法*」を参照してください。

クライアントでの Tivoli Access Manager の設定情報の構成

Tivoli Access Manager をローカル・クライアントにインストールすると、管理者ユーティリティーを使用して、アクセス・マネージャーの設定情報を構成できます。IBM クライアントで、Tivoli Access Manager 設定情報を構成するため、Client Security Software は、構成ファイルを使用します。この構成ファイルは、UVM ポリシーが、Tivoli Access Manager の制御に引き渡すオブジェクトに、Tivoli Access Manager を結合するために使用されます。

クライアントで Tivoli Access Manager の設定情報を構成するには、次の管理者ユーティリティー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。

2. 「**Windows ログオンを UVM ログオンに置き換える**」チェック・ボックスを選択します。
3. 「**アプリケーション・ポリシー**」ボタンをクリックします。「ポリシー構成の変更」画面が表示されます。
4. 「Tivoli Access Manager セットアップ情報」領域で、`TAMCSS.conf` 構成ファイルの絶対パスを選択します。 (たとえば、`C:¥TAMCSS¥TAMCSS.conf`。) Tivoli Access Manager をクライアントにインストールしていないと、この領域は使用可能になりません。「**参照**」をクリックして、構成ファイルを検索することも可能です。
5. 「**ポリシーの編集**」ボタンをクリックし、管理者パスワードを入力します。
6. 「処理」ドロップダウン・メニューで、Tivoli Access Manager によって制御したい処理を選択します。
7. 「**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、チェックを付けます。
8. 「**適用**」ボタンをクリックします。次回のキャッシュ・リフレッシュ時に、変更内容が有効になります。変更内容をすぐに有効にしたい場合は、「ポリシー構成の変更」画面の「**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・キャッシュのリフレッシュ

Tivoli Access Manager によって管理されるセキュリティー・ポリシー情報のローカル・レプリカが、IBM クライアントで保持されます。月数と日数の増分でローカル・キャッシュの更新頻度を設定するか、ボタンをクリックしてローカル・キャッシュをただちに更新することができます。

ローカル・キャッシュを設定または最新表示するには、次の管理者ユーティリティー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。
2. 「**アプリケーション・ポリシー**」ボタンをクリックします。「ポリシー構成の変更」画面が表示されます。
3. 「ローカル・キャッシュの更新間隔」領域で、次のどちらか 1 つを実行します。
   - ここでローカル・キャッシュを更新するには、「**ローカル・キャッシュの更新**」をクリックします。
   - 更新頻度を設定するには、指定されたフィールドに月数と日数を入力します。月数と日数の値は、スケジュールされた更新間隔を表します。

管理者パスワードの変更

IBM エンベデッド・セキュリティー・サブシステムを使用可能にするには、管理者パスワードを設定する必要があります。管理者パスワードの設定後、管理者ユーティリティーへのアクセスはこのパスワードで保護されます。セキュリティー強化のため、管理者パスワードを定期的に変更する必要があります。長期間変更されていないままのパスワードは、第三者の侵入を受ける危険性が高くなります。許可されていないユーザーが管理者ユーティリティーの設定値を変更できないようにするために、管理者パスワードを保護してください。管理者パスワードの規則については、101 ページの『付録 B. パスワードおよびパスフレーズの情報』を参照してください。

管理者パスワードを変更するには、次の管理者ユーティリティーの手順を実行します。

1. デスクトップより「**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**をクリックし、管理者ユーティリティーを起動します。「**セキュリティー・チップの設定**」ボタンをクリックします。

   「IBM セキュリティー・チップの設定変更」画面が表示されます。
2. 「**管理者パスワードを変更する**」をクリックします。

   「管理者パスワードの変更」画面が表示されます。
3. 「新しいパスワードを入力してください」フィールドに新しいパスワードを入力します。
4. 「新しいパスワードを確認してください」フィールドで、そのパスワードをもう一度入力します。
5. 「**OK**」をクリックします。

   操作が正常に終了したことを知らせるメッセージが表示されます。

   重要: 変更内容を保管するのに「Enter」または「Tab」→「Enter」を押さないでください。押した場合は、「セキュリティー・サブシステムを無効にする」ウィ

ンドウが表示されます。「サブシステムを無効にする」ウィンドウが開いても、チップを使用不可にせずに、ウィンドウを終了してください。

6. 「**OK**」をクリックします。

Client Security Software に関する情報の表示

Client Security Software に関する次の情報は、管理者ユーティリティーの「**セキュリティー・チップを無効にする**」ボタンをクリックして入手できます。

- Client Security Software と一緒に使用されるファームウェアのバージョン番号
- エンベデッド・セキュリティー・サブシステムの暗号化状況
- ハードウェア鍵の妥当性
- セキュリティー・チップの状況

IBM エンベデッド・セキュリティー・サブシステムを使用不可にする

管理者ユーティリティーを使用して、IBM エンベデッド・セキュリティー・サブシステムを使用不可にできます。管理者ユーティリティーを始動し、セキュリティー・サブシステムを使用不可にするには、管理者パスワードが必要になるので、権限のないユーザーがサブシステムを使用不可にするのを禁止するために、管理者パスワードを保護してください。

重要: UVM プロテクションが使用可能になっているときに、IBM エンベデッド・セキュリティー・サブシステムをクリアしないでください。 UVM ログオン・プロテクションを無効にするには、管理者ユーティリティーを開き、「**Windows ログオンを UVM ログオンに置き換える**」チェック・ボックスのマークを外します。コンピューターを再始動する必要があります。

エンベデッド・セキュリティー・サブシステムを使用不可にするには、次の管理者ユーティリティーの手順を実行します。

1. 「**セキュリティー・チップの設定**」ボタンをクリックします。
2. 「**セキュリティー・チップを無効にする**」ボタンをクリックし、画面の指示に従います。
3. ご使用のコンピューターで「拡張セキュリティー」が使用可能になっている場合にチップを使用不可にするには、構成/セットアップ・ユーティリティーで設定した BIOS 管理者パスワードの入力が必要になる場合があります。

セキュリティー・チップが無効になった後で、このサブシステムと暗号鍵を使用する場合には、セキュリティー・チップをもう一度使用可能（有効）にする必要があります。デスクトップより「**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**をクリックします。「セキュリティー・チップを有効にする」画面が表示されるので「はい」をクリックします。

IBM エンベデッド・セキュリティー・サブシステムを使用可能（有効）にし、管理者パスワードを設定する

システム・ボード交換後にアーカイブを復元したい場合や、IBM エンベデッド・セキュリティー・サブシステムを使用不可にしてある場合には、セキュリティー・サブシステムを使用可能にする必要があります。

セキュリティー・チップを有効にするには、次の手順を実行します。

1. IBM クライアントの Windows デスクトップから、「**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**」をクリックします。

   「セキュリティー・チップを有効にする」メッセージが表示され、IBM クライアントの IBM セキュリティー・チップを有効にするように求められます。
2. 「**はい**」をクリックします。

   コンピューターを再始動するように求めるメッセージが表示されます。IBM エンベデッド・セキュリティー・サブシステムを使用可能にするには、コンピューターを再始動する必要があります。コンピューターの「拡張セキュリティー」が使用可能になっている場合にサブシステムを使用可能にするには、構成/セットアップ・ユーティリティーで設定した BIOS 管理者パスワードまたはスーパーバイザー・パスワードの入力が必要になる場合があります。
3. 「**OK**」をクリックして、コンピューターを再始動します。

エントラスト・サポートを使用可能にする

IBM エンベデッド・セキュリティー・サブシステムは、Client Security Software とともに作動してエントラスト・セキュリティー機能を強化します。Client Security Software のあるコンピューターでエントラスト・サポートを使用可能にすると、エントラスト・ソフトウェア・セキュリティー・サブシステム機能を IBM セキュリティーに転送できます。

Client Security Software は、エントラスト・サポートを使用可能にするため、entrust.ini ファイルを自動的に検索しますが、entrust.ini ファイルが通常のパスに存在しない場合は、entrust.ini ファイルをユーザーが参照するためのダイアログが開きます。ファイルを見つけて、このファイルを選択すると、Client Security がエントラスト・サポートを使用可能にすることができます。管理者ユーティリティーの「**Entrust サポートを有効にする**」チェック・ボックスをクリックした後、エントラストが IBM エンベデッド・セキュリティー・サブシステムを利用する前に、リブートする必要があります。

エントラスト・サポートを使用可能にするには、次の手順を実行します。

1. IBM クライアントの Windows デスクトップから、「**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**」をクリックします。

   「管理者ユーティリティー」のメイン・ウィンドウが表示されます。
2. 「**アプリケーション サポートとポリシーの構成**」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。

3. 「**エントラスト サポートを有効にする**」チェック・ボックスを選択します。
4. 「**適用**」をクリックします。

「IBM クライアント・セキュリティー・エントラスト・サポート」画面にエントラスト・サポートが使用可能になっていることを示すメッセージが表示されます。

注: 変更内容を有効にするには、コンピューターの再始動が必要です。

第 4 部 付録

付録 A. トラブルシューティング

以下のセクションでは、Client Security Software の使用時に起こりうる問題の防止、またはそのような問題の識別と訂正に役立つ情報を提示します。

管理機能

ここには、Client Security Software のセットアップおよび使用の際に管理者の役に立つと考えられる情報が含まれています。

IBM Client Security Software は、IBM エンベデッド・セキュリティー・サブシステムを備えた IBM コンピューターでのみ使用できます。このソフトウェアには、IBM クライアントが、ぜい弱なソフトウェアではなく、セキュアなハードウェアによって機密情報を保護するためのアプリケーションやコンポーネントが含まれています。

ユーザーの登録

クライアントのユーザー情報を保護するには、クライアントに IBM Client Security Software をインストールする**必要があり**、ユーザーにそのソフトウェアの使用権限を与える**必要があります**。使いやすいセットアップ・ウィザードのガイドに従って、インストール・プロセス全体を実行できます。

重要: UVM を使用するには、セットアップで少なくとも一人のクライアント・ユーザーを登録する**必要があります**。 Client Security Software をはじめてセットアップするときに登録済みのユーザーがないと、目的のセキュリティー設定は適用**されず**、その情報は保護**されません**。

ユーザーを登録せずにセットアップ・ウィザードを終了し、コンピューターをシャットダウンしてから再始動した場合は、Windows の「スタート」メニューからクライアント・セキュリティーのセットアップ・ウィザードを実行し、UVM を使用する Windows ユーザーを登録します。これにより、IBM Client Security Software はセキュリティー設定を適用して機密情報を保護できるようになります。

ユーザーの削除

管理者ユーティリティーでユーザーを削除した場合、ユーザーのリストからそのユーザー名が削除されます。

BIOS 管理者パスワードの設定 (ThinkCentre)

管理者は BIOS セットアップ・ユーティリティーで使用可能なセキュリティー設定値を使用することにより、次の作業を行うことができます。

- IBM エンベデッド・セキュリティー・サブシステムの使用可能設定と使用不可設定
- IBM エンベデッド・セキュリティー・サブシステムのクリア

注意:

- IBM エンベデッド・セキュリティー・サブシステムをクリアすると、サブシステムに保管されている暗号鍵と証明書はすべて失われます。

セキュリティー設定値は、コンピューターの構成/セットアップ・ユーティリティーを介してアクセスできるため、管理者パスワードを設定し、許可されていないユーザーがこれらの設定値を変更できないようにします。

BIOS 管理者パスワードは、以下のように設定します。

1. コンピューターをシャットダウンして再始動します。
2. 画面上に構成/セットアップ・ユーティリティーのプロンプトが表示されたならば、**F1** キーを押します。

   構成/セットアップ・ユーティリティーのメインメニューが開きます。
3. 「**システム・セキュリティー**」を選択します。
4. 「**管理者パスワード**」を選択します。
5. パスワードを入力して、キーボード上の下矢印キーを押します。
6. もう一度パスワードを入力して、下矢印キーを押します。
7. 「**管理者パスワードの変更**」を選択して Enter キーを押した後、もう一度 Enter キーを押します。
8. **Esc** キーを押して終了すると、設定値が保管されます。

BIOS 管理者パスワードの設定後は、構成/セットアップ・ユーティリティーへのアクセスを試みるたびにプロンプトが表示されます。

重要: BIOS 管理者パスワードは安全な場所に記録しておいてください。 BIOS 管理者パスワードを紛失したり忘れてしまうと、構成/セットアップ・ユーティリティーへのアクセスができなくなります。さらに、コンピューターのカバーを取り外してシステム・ボード上のジャンパーを取り除かないと、BIOS 管理者パスワードの変更または削除を行うことはできません。詳しくは、ご使用のコンピューターに付属のハードウェア資料を参照してください。

スーパーバイザー・パスワードの設定 (ThinkPad)

管理者は、IBM BIOS セットアップ・ユーティリティーのセキュリティー設定値を用いて、次のタスクを実行することができます。

- IBM エンベデッド・セキュリティー・サブシステムの使用可能設定と使用不可設定
- IBM エンベデッド・セキュリティー・サブシステムのクリア

注意:

- Client Security Software のインストールまたはアップグレードの際には事前に、一部の ThinkPad モデルのスーパーバイザー・パスワードを一時的に無効にしておく必要があります。

Client Security Software をセットアップした後、許可されていないユーザーによってこれらの設定値が変更されないようにするために、スーパーバイザー・パスワードを設定します。

スーパーバイザー・パスワードを設定するには、次のいずれかの手順を実行します。

例 1

1. コンピューターをシャットダウンして再始動します。
2. 画面上にセットアップ・ユーティリティーのプロンプトが表示されたならば、F1 キーを押します。

   セットアップ・ユーティリティーのメインメニューが開きます。
3. 「**パスワード**」を選択します。
4. 「**スーパーバイザー・パスワード**」を選択します。
5. パスワードを入力して、Enter キーを押します。
6. もう一度パスワードを入力して、Enter キーを押します。
7. 「**続行**」をクリックします。
8. F10 キーを押すと、変更内容が保管されて終了します。

例 2

1. コンピューターをシャットダウンして再始動します。
2. 「通常の始動に割り込む場合は、青色の Access IBM ボタンを押す」メッセージが表示されたならば、青色の「Access IBM」ボタンを押します。

   「Access IBM」のデスクトップ領域が開きます。
3. 「**セットアップ・ユーティリティーの開始**」をダブルクリックします。
4. 矢印キーでメニューを下方にナビゲートして、「**セキュリティー**」 を選択します。
5. 「**パスワード**」を選択します。
6. 「**スーパーバイザー・パスワード**」を選択します。
7. パスワードを入力して、Enter キーを押します。
8. もう一度パスワードを入力して、Enter キーを押します。
9. 「**続行**」をクリックします。
10. F10 キーを押すと、変更内容が保管されて終了します。

スーパーバイザー・パスワードの設定後は、BIOS セットアップ・ユーティリティーへのアクセスを試みるたびにプロンプトが表示されます。

重要: スーパーバイザー・パスワードは安全な場所に記録しておいてください。スーパーバイザー・パスワードを紛失したり忘れてしまった場合は、IBM BIOS セットアップ・ユーティリティーへアクセスできなくなるため、パスワードの変更または削除を行うことができなくなります。詳しくは、ご使用のコンピューターに付属のハードウェア資料を参照してください。

管理者パスワードの保護

管理者パスワードは、管理者ユーティリティーへのアクセスを保護します。許可されていないユーザーが管理者ユーティリティーの設定値を変更できないようにするために、管理者パスワードを保護してください。

IBM エンベデッド・セキュリティー・サブシステムのクリア (ThinkCentre)

IBM エンベデッド・セキュリティー・サブシステムからすべてのユーザーの暗号鍵を消去し、サブシステムの管理者パスワードをクリアしたい場合は、サブシステムをクリアする必要があります。 IBM エンベデッド・セキュリティー・サブシステムをクリアする前に、以下の情報をお読みください。

注意:

- IBM エンベデッド・セキュリティー・サブシステムをクリアすると、サブシステムに保管されている暗号鍵と証明書はすべて失われます。

IBM エンベデッド・セキュリティー・サブシステムをクリアするには、次の手順を実行します。

1. コンピューターをシャットダウンして再始動します。
2. 画面上にセットアップ・ユーティリティーのプロンプトが表示されたならば、F1 キーを押します。

   セットアップ・ユーティリティーのメインメニューが開きます。
3. 「**セキュリティー**」を選択します。
4. 「**IBM TCPA セキュリティー機能**」を選択し、Enter キーを押します。
5. 「**はい**」を選択します。
6. Enter キーを押して、選択内容を確認します。
7. F10 を押して変更内容を保管し、セットアップ・ユーティリティーを終了します。
8. 「**はい**」を選択し、Enter キーを押します。コンピューターが再始動します。

IBM エンベデッド・セキュリティー・サブシステムのクリア (ThinkPad)

IBM エンベデッド・セキュリティー・サブシステムからすべてのユーザーの暗号鍵を消去し、管理者パスワードをクリアしたい場合は、サブシステムをクリアする必要があります。 IBM エンベデッド・セキュリティー・サブシステムをクリアする前に、以下の情報をお読みください。

注意:

- IBM エンベデッド・セキュリティー・サブシステムをクリアすると、サブシステムに保管されている暗号鍵と証明書はすべて失われます。

IBM エンベデッド・セキュリティー・サブシステムをクリアするには、次の手順を実行します。

1. コンピューターをシャットダウンして再始動します。
2. 画面上にセットアップ・ユーティリティーのプロンプトが表示されたならば、F1 キーを押します。

   セットアップ・ユーティリティーのメインメニューが開きます。
3. 「**セキュリティー**」を選択します。

4. 「**IBM セキュリティー・チップ**」を選択し、Enter キーを押します。
5. Enter キーを押して、「**使用不可**」を選択します。
6. Enter キーを押して、選択内容を確認します。
7. 続行するには、Enter キーを押してください。
8. F10 を押して変更内容を保管し、セットアップ・ユーティリティーを終了します。
9. 「**はい**」を選択し、Enter キーを押します。コンピューターが再始動します。

CSS バージョン 5.4 に関する既知の問題と制限

Client Security Software バージョン 5.4 の機能を使用するときに役立つと考えられる情報を以下に示します。

ローミングに関する制限

CSS ローミング・サーバーの使用

だれかが CSS ローミング・サーバーにログオンしようとすると、CSS 管理者パスワードを入力するための画面が必ず表示されます。しかし、そのパスワードを入力しなくても、コンピューターを通常の方法で使用することは可能です。

ローミング環境での IBM Security Password Manager の使用

ローミング環境では、IBM Client Security Password Manager を使用して 1 つのシステムに保管したパスワードを別のシステムでも使用できます。ローミング・ネットワークでアーカイブが使用可能になっている場合、ユーザーが別のシステムにログオンすると、新しいエントリーが自動的にアーカイブから取り込まれます。したがって、ユーザーが 1 つのシステムにすでにログオンしている場合、ローミング・ネットワークで新しいエントリーを使用可能な状態にするには、いったんログオフしてからログオンし直す必要があります。

Internet Explorer の証明書とローミングのリフレッシュ遅延

Internet Explorer の証明書は、アーカイブで 20 秒ごとにリフレッシュされます。ローミング・ユーザーが Internet Explorer の新しい証明書を生成した場合、そのユーザーは少なくとも 20 秒待ってから、自分の CSS 構成を別のシステムにインポートしたり、別のシステムで復元したり変更したりする必要があります。 20 秒のリフレッシュ間隔の前にそれらの操作を実行しようとすると、証明書が失われてしまいます。また、証明書を生成した時点でユーザーがアーカイブに接続していなかった場合も、アーカイブに接続してから 20 秒待って、証明書がアーカイブで確実に更新されるようにする必要があります。

Lotus Notes のパスワードとクレデンシャル・ローミング

Lotus Notes のサポートが使用可能になっている場合、ユーザーの Lotus Notes パスワードは UVM によって保管されます。ユーザーが Lotus Notes にログオンするときに、Notes パスワードの入力は必要ありません。 Lotus Notes にアクセスするには、(セキュリティー・ポリシー設定に応じて) 自分の UVM パスフレーズ、指紋、スマート・カードなどが必要になります。

ユーザーが Lotus Notes 内で Notes パスワードを変更すると、Lotus Notes の ID ファイルはその新しいパスワードに合わせて更新され、新しい Notes パスワードの UVM コピーも更新されます。ローミング環境の場合、ユーザーの UVM クレデンシャルは、ユーザーがアクセスできるローミング・ネットワーク内の他のシステムでも使用可能になります。更新後のパスワードを保管した Notes ID ファイルがローミング・ネットワーク内の別のシステムで使用可能になっていない場合は、Notes パスワードの UVM コピーがその別のシステムの ID ファイルに保管されている Notes パスワードと一致しないという現象が起こりえます。その場合、ユーザーは Lotus Notes にアクセスできません。

更新後のパスワードを保管したユーザーの Notes ID ファイルが別のシステムで使用可能になっていない場合は、更新後の Notes ID ファイルをローミング・ネットワーク内の他のシステムにコピーして、ID ファイル内のパスワードが UVM コピーと一致するようにしてください。あるいは、「スタート」メニューから「セキュリティー設定の変更」を実行し、Notes パスワードを古い値に戻すという方法もあります。そのようにしてから、再び Lotus Notes で Notes パスワードを更新できます。

ローミング環境でのログオン時にクレデンシャルが使用可能になるかどうか

ネットワーク共用にアーカイブが置かれている場合、ユーザーがアーカイブにアクセスすると、最新のユーザー・クレデンシャルがアーカイブからただちにダウンロードされます。ログオン時には、ユーザーはまだネットワーク共用にアクセスしていないので、システム・ログオンが完了するまで、最新のクレデンシャルはダウンロードされません。たとえば、ローミング・ネットワーク内の別のシステムで UVM パスフレーズを変更した場合や、別のシステムで新しい指紋を登録した場合は、ログオン・プロセスが完了するまで、それらの更新内容は使用可能になりません。更新後のユーザー・クレデンシャルが使用可能になっていなければ、ユーザーは、以前のパスフレーズや他の登録済みの指紋でシステムへのログオンを試みる必要があります。ログオンが完了した時点で、ユーザーの更新後のクレデンシャルは使用可能になり、新しいパスフレーズや指紋が UVM に登録されます。

鍵の復元

鍵の復元操作を実行した場合は、コンピューターを再始動しなければ、Client Security Software を使用できません。

ローカル・ユーザー名とドメイン・ユーザー名

ドメイン・ユーザー名とローカル・ユーザー名が同じ場合は、両方のアカウントに同じ Windows パスワードを使用してください。 IBM ユーザー認証マネージャーは、1 つの ID につき 1 つの Windows パスワードしか保管しないので、ユーザーは、ローカル・ログオンとドメイン・ログオンに同じパスワードを使用する必要があります。そのようにしていない場合、IBM UVM セキュア Windows ログオン置換が使用可能になっていれば、ローカル・ログインとドメイン・ログインの切り替えを行うときに、IBM UVM Windows パスワードの更新を求める画面が表示されます。

CSS には、ドメインとローカルで別々のユーザーを同じアカウント名で登録する機能はありません。同じ ID をもつローカルとドメインのユーザーの登録を試みる

と、「選択されたユーザー ID は、すでに構成されています」というメッセージが表示されます。 CSS では、ドメインとローカルで共通する複数のユーザー ID を 1 つのシステムにそれぞれ登録して、一連の同じクレデンシャル、類似証明書、保管中の指紋などに共通 ID でアクセスできるようにすることは許可されません。

Targus 指紋ソフトウェアの再インストール

Targus 指紋ソフトウェアをいったん除去してから再インストールする場合は、指紋サポートを使用可能にするために、Client Security Software で指紋サポートを使用可能にするのに必要なレジストリー項目を手動で追加しなければなりません。必要な項目が入っているレジストリー・ファイル (atplugin.reg) をダウンロードして、ダブルクリックすると、そのレジストリー項目がレジストリーにマージされます。この操作を確認するための画面が表示されたら、「はい」をクリックしてください。Client Security Software が変更内容を認識して、指紋サポートを使用可能にするには、システムのリブートが必要です。

注: これらのレジストリー項目を追加するには、システムで管理者権限を持っている必要があります。

BIOS スーパーバイザー・パスフレーズ

IBM Client Security Software 5.4 とそれ以前のバージョンでは、一部の ThinkPad システムで利用できる BIOS スーパーバイザー・パスフレーズ機能をサポートしていません。 BIOS スーパーバイザー・パスフレーズを使用可能にした場合は、セキュリティー・サブシステムの使用可能設定や使用不可設定をすべて BIOS セットアップから実行する必要があります。

Netscape 7.x の使用

Netscape 7.x の動作は Netscape 4.x の動作とは異なり、Netscape を開始したときに、パスフレーズの画面がすぐには表示されません。 PKCS#11 モジュールは必要なときにのみロードされるので、PKCS#11 モジュールを必要とする操作を実行するときにはじめて、パスフレーズの画面が表示されることになります。

アーカイブ・ロケーションとしてのディスケットの使用

セキュリティー・ソフトウェアの構成時に、アーカイブ・ロケーションとしてディスケットを指定すると、構成プロセスがディスケットにデータを書き込むときに長い時間がかかります。アーカイブ・ロケーションとしては、ネットワーク共用や USB 鍵などのメディアのほうが優れています。

スマート・カードに関する制限

スマート・カードの登録

ユーザーがスマート・カードによる認証を正しく実行するには、まずスマート・カードを UVM に登録する必要があります。 1 枚のカードを複数のユーザーに割り当てている場合は、そのカードを最後に登録したユーザーだけがそのカードを使用できます。したがって、スマート・カードは 1 つのユーザー・アカウントについてのみ登録するべきです。

スマート・カードによる認証

認証にスマート・カードが必要な場合は、UVM によって、スマート・カードの挿入を求めるダイアログが表示されます。読取装置にスマート・カードを挿入すると、スマート・カードの PIN を入力するための画面が表示されます。ユーザーが間違った PIN を入力すると、UVM によって、スマート・カードを求める画面が再び表示されます。スマート・カードをいったん取り外してから挿入し直さないと、PIN の再入力はできません。スマート・カードの正しい PIN を入力するまで、ユーザーはスマート・カードの取り外しと挿入を繰り返す必要があります。

暗号化の後にフォルダにプラス記号 (+) が表示される場合

ファイルやフォルダを暗号化した後に、Windows エクスプローラーによって、フォルダ・アイコンの前に余計なプラス記号 (+) が表示されることがあります。この余計な記号は、エクスプローラーのウィンドウを最新の表示に更新すると消えます。

Windows XP の制限ユーザーに関する制限

Windows XP の制限ユーザーは、自分の UVM パスフレーズや Windows パスワードを更新できません。また、ユーザー構成ユーティリティーを使用して自分の鍵アーカイブを更新することもできません。

その他の制限

ここでは、Client Security Software に関連した他の既知の問題や制限について説明します。

Windows オペレーティング・システムでの Client Security Software の使用

全 Windows オペレーティング・システムの既知の制限: UVM に登録されているクライアント・ユーザーが自分の Windows ユーザー名を変更した場合、Client Security の機能がすべて失われます。そのユーザーは UVM で新規ユーザー名を再登録して、新規クレデンシャルをすべて要求しなければならなくなります。

Windows XP オペレーティング・システムの既知の制限: UVM に登録済みのユーザーは、以前に Windows ユーザー名を変更した場合、UVM に認識されなくなります。 UVM は以前のユーザー名を指しますが、Windows は新規のユーザー名しか認識しません。Client Security Software のインストール前に Windows ユーザー名を変更した場合にも、この制約が伴います。

Netscape アプリケーションでの Client Security Software の使用

許可に失敗した後で Netscape が開く: UVM パスフレーズ・ウィンドウが開いた場合、続行する前に UVM パスフレーズを入力し、その後「**OK**」をクリックする必要があります。不正な UVM パスフレーズを入力した場合 (または指紋スキャン用には適さない指紋を指定した場合)、エラー・メッセージが表示されます。
「**OK**」をクリックすると Netscape が開きますが、IBM エンベデッド・セキュリティー・サブシステムで生成されたディジタル証明書を使用することはできません。

IBM エンベデッド・セキュリティー・サブシステム証明書を使用する前に、Netscape を終了して再び入り、正確な UVM パスフレーズを入力する必要があります。

アルゴリズムが表示されない: IBM エンベデッド・セキュリティー・サブシステム PKCS#11 モジュールでサポートされているハッシュ・アルゴリズムはすべて、Netscape 内でそのモジュールが参照されているときには選択されません。次のアルゴリズムは、IBM エンベデッド・セキュリティー・サブシステム PKCS#11 モジュールでサポートされていますが、Netscape 内で参照されているときはサポート対象として認識されません。

- SHA-1
- MD5

IBM エンベデッド・セキュリティー・サブシステム証明書と暗号化アルゴリズム

以下の情報は、IBM エンベデッド・セキュリティー・サブシステム証明書で使用できる暗号化アルゴリズムに関する問題の識別に役立ちます。 電子メール・アプリケーションで使用されている暗号化アルゴリズムについては、Microsoft または Netscape の最新情報を参照してください。

ある Outlook Express (128 ビット) クライアントから別の Outlook Express (128 ビット) クライアントに電子メールを送信する場合: 128 ビット版 Internet Explorer 4.0 または 5.0 を備えた Outlook Express を使用して、Outlook Express (128 ビット) を使用している他のクライアント宛てに暗号化された電子メールを送信した場合、IBM エンベデッド・セキュリティー・サブシステム証明書で暗号化されたメッセージは 3DES アルゴリズムしか使用できません。

Outlook Express (128 ビット) クライアントと Netscape クライアント間で電子メールを送信する場合: Netscape クライアントから Outlook Express (128 ビット) クライアントに対する RC2(40)、RC2(64)、または RC2(128) 暗号化要求は、常に、RC2(40) アルゴリズムを使用する Netscape クライアントに戻されます。

Outlook Express (128 ビット) クライアントでは選択不可能な一部のアルゴリズム: ご使用のバージョンの Outlook Express (128 ビット) の構成またはアップデート方法によっては、一部のアルゴリズム (RC2 アルゴリズムなど) が IBM エンベデッド・セキュリティー・サブシステム証明書には使えないことがあります。ご使用のバージョンの Outlook Express に使用されている暗号化アルゴリズムについては、Microsoft の最新情報を参照してください。

Lotus Notes ユーザー ID に対する UVM プロテクションの使用

Notes セッション内でユーザー ID を切り替えた場合に UVM プロテクションが機能しない: UVM プロテクションは、Notes セッションの現行ユーザー ID に対してのみセットアップできます。 UVM プロテクションが有効になっているユーザー ID から別のユーザー ID に切り替えるには、次の手順を実行します。

1. Notes を終了します。
2. 現行ユーザー ID の UVM プロテクションを使用不可にします。

3. Notes に入りユーザー ID を切り替えます。ユーザー ID の切り替えについては、ご使用の Lotus Notes の資料を参照してください。

   切り替え先のユーザー ID に対する UVM プロテクションをセットアップする場合は、ステップ 4 に進みます。
4. Client Security Software が提供している Lotus Notes 構成ツールに入り、UVM プロテクションをセットアップします。

ユーザー構成ユーティリティーに関する制限

Windows XP ではアクセス制限が課されるため、特定の状況の下では、クライアント・ユーザーが使える機能が限定されます。

Windows XP Professional 版

Windows XP Professional の場合、クライアント・ユーザー制限が適用されるのは、次のような状況にある場合です。

- Client Security Software が、後で NTFS フォーマットに変換されるパーティション上にインストールされている
- Windows フォルダが、後で NTFS フォーマットに変換されるパーティション上にある
- アーカイブ・フォルダが、後で NTFS フォーマットに変換されるパーティション上にある

上記のような状況では、Windows XP Professional の制限ユーザーが、次のようなユーザー構成ユーティリティーのタスクを実行できない場合があります。

- UVM パスフレーズの変更
- UVM に登録済みの Windows パスワードの更新
- 鍵アーカイブの更新

Windows XP Home 版

Windows XP Home の制限ユーザーは、次のいずれかの状況にある場合、ユーザー構成ユーティリティーを使用できません。

- Client Security Software が、NTFS フォーマットのパーティション上にインストールされている
- Windows フォルダが、NTFS フォーマットのパーティション上にある
- アーカイブ・フォルダが、NTFS フォーマットのパーティション上にある

Tivoli Access Manager に関する制限

Tivoli Access Manager コントロールが選択されている場合、「**選択したオブジェクトへの全アクセスを拒否**」チェック・ボックスは有効です。 UVM ポリシー・エディターで、「**選択したオブジェクトを Tivoli Access Manager が管理する**」を選択して、Tivoli Access Manager での認証オブジェクトの制御を有効にした場合も、「**選択したオブジェクトへの全アクセスを拒否**」チェック・ボックスは有効です。「**選択したオブジェクトへの全アクセスを拒否**」チェック・ボックスがアクティブな状態のままでも、このチェック・ボックスを選択して Tivoli Access Manager コントロールを指定変更することはできません。

エラー・メッセージ

Client Security Software に関連したエラー・メッセージが、イベント・ログ内に生成される: Client Security Software で使用されるデバイス・ドライバーは、場合によってはイベント・ログ内にエラー・メッセージを生成することがあります。これらのメッセージに関連したエラーは、ユーザーのコンピューターの通常の運用には影響しません。

認証オブジェクトのアクセスが拒否された場合に、関連したプログラムが生成したエラー・メッセージが UVM によって呼び出される: UVM ポリシーが認証オブジェクトのアクセスを拒否する設定 (たとえば、電子メールの復号化など) が施されている場合、アクセスが拒否されたことを通知するメッセージは、使用されているソフトウェアによって異なります。たとえば、認証オブジェクトへのアクセスが拒否されたことを通知する Outlook Express からのエラー・メッセージは、アクセスが拒否されたことを通知する Netscape のエラー・メッセージとは異なります。

トラブルシューティングに関する図表

以下のセクションでは、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載せています。

インストールに関するトラブルシューティング情報

Client Security Software のインストール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
ソフトウェアのインストール中にエラー・メッセージが表示される	**処置**
ソフトウェアのインストール時には、選択したアプリケーションおよびその全コンポーネントを除去するかを尋ねるメッセージが表示されます。	「**OK**」をクリックして、ウィンドウから出ます。新しいバージョンの Client Security Software をインストールする場合は、再度インストール処理を開始します。
インストール中には、削除かアップグレードかの選択画面が表示されます。	次のいずれかを行います。 • Client Security Software 5.0 より前のバージョンがインストールされている場合は、「**削除**」を選択してそれらを削除します。次いでシステムを再起動し、IBM BIOS セットアップ・ユーティリティーを使用して、セキュリティー・サブシステムをクリアします。 • それ以外の場合は、「**アップグレード**」を選択し、インストールを続行します。
管理者パスワードが認識されないため、インストール・アクセスが拒否される	**処置**

問題の兆候	可能な解決策
IBM エンベデッド・セキュリティー・サブシステムが使用可能な IBM クライアント上にソフトウェアをインストールした場合、その IBM エンベデッド・セキュリティー・サブシステムの管理者パスワードが認識されません。	セキュリティー・サブシステムをクリアしてインストールを続行します。

管理者ユーティリティーに関するトラブルシューティング情報

管理者ユーティリティー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情報を、次に示します。

問題の兆候	可能な解決策
管理者ユーティリティーで UVM パスフレーズを入力して確認した後に、「次へ」ボタンが選択不可能になる	**処置**
UVM にユーザーを追加した場合、管理者ユーティリティーで UVM パスフレーズを入力して確認した後に「**次へ**」ボタンが選択不可能になります。	Windows タスクバー上の「**情報**」項目をクリックして、手順を続行します。
管理者公開鍵の変更の際にエラー・メッセージが表示される	**処置**
エンベデッド・セキュリティー・サブシステムをクリアして鍵アーカイブを復元した場合、管理者公開鍵を変更するとエラー・メッセージが表示されることがあります。	UVM にユーザーを追加します。適用可能な場合は、新規の証明書を要求します。
UVM パスフレーズのリカバリーを試みるとエラー・メッセージが表示される	**処置**
管理者公開鍵を変更してからユーザー用 UVM パスフレーズのリカバリーを試みると、エラー・メッセージが表示されることがあります。	次のいずれかを行います。 • ユーザー用 UVM パスフレーズが不要の場合、アクションは不要です。 • ユーザー用 UVM パスフレーズが必要な場合は、UVM にユーザーを追加する必要があります。適用可能な場合は、新規の証明書を要求します。
UVM ポリシー・ファイルを保管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**
「**適用**」または「**保存**」をクリックして UVM ポリシー・ファイル (globalpolicy.gvm) を保管しようとしたときに、エラー・メッセージが表示されます。	エラー・メッセージを閉じ、再度 UVM ポリシー・ファイルを編集して変更を行った後で、ファイルを保管します。
UVM ポリシー・エディターを開こうとするとエラー・メッセージが表示される	**処置**
カレント・ユーザー (オペレーティング・システムにログオン済み) が UVM に追加されていない場合、UVM ポリシー・エディターは開きません。	UVM にユーザーを追加して、UVM ポリシー・エディターを開きます。

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いるときにエラー・メッセージが表示される	**処置**
管理者ユーティリティーを使用しているときに、次のようなエラー・メッセージが表示される可能性があります。 IBM エンベデッド・セキュリティー・サブシステムへアクセスしようとしているときにバッファー入出力エラーが発生しました。リブートすると直るかもしれません。	エラー・メッセージを閉じて、コンピューターを再始動します。
管理者パスワードの変更時に、チップ無効のメッセージが表示される	**処置**
管理者パスワードの変更を行おうとして、確認のパスワードを入力した後に Enter キーまたは Tab → Enter キーを押すと、「**チップの無効化**」ボタンが使用可能になり、チップの無効化を確認するメッセージが表示されます。	次の操作を行います。 1. チップの無効化を確認するウィンドウを終了します。 2. 管理者パスワードを変更するには、新規のパスワードを入力し、確認のパスワードを入力して、「**変更**」をクリックします。確認のパスワードの入力後に Enter キーまたは Tab → Enter キーを押さないでください。

ユーザー構成ユーティリティーに関するトラブルシューティング情報

ユーザー構成ユーティリティー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情報を、次に示します。

問題の兆候	可能な解決策
Windows XP Professional では、制限ユーザーが特定のユーザー構成ユーティリティーの機能を実行できない	**処置**
Windows XP Professional の制限ユーザーは、以下のようなユーザー構成ユーティリティーのタスクを実行できない場合があります。 • UVM パスフレーズの変更 • UVM に登録済みの Windows パスワードの更新 • 鍵アーカイブの更新	これは、Windows XP Professional における既知の制限です。この問題に対する解決策はありません。
Windows XP Home では、制限ユーザーがユーザー構成ユーティリティーを使用できない	**処置**

問題の兆候	可能な解決策
Windows XP Home の制限ユーザーは、次のいずれかの状況にある場合、ユーザー構成ユーティリティーを使用できません。 • Client Security Software が、NTFS フォーマットのパーティション上にインストールされている • Windows フォルダが、NTFS フォーマットのパーティション上にある • アーカイブ・フォルダが、NTFS フォーマットのパーティション上にある	これは、Windows XP Home における既知の制限です。この問題に対する解決策はありません。

ThinkPad 特有のトラブルシューティング情報

ThinkPad コンピューター上で 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情報を、次に示します。

問題の兆候	可能な解決策
別の UVM 対応の指紋センサーが正常に動作しない	**処置**
IBM ThinkPad コンピューターでは、複数の UVM 対応指紋センサーの入れ替えがサポートされていません。	指紋センサー・モデルは、切り替えないでください。リモート側で作業するときには、ドッキング・ステーションから作業するときと同じモデルを使用します。

Microsoft に関するトラブルシューティング情報

次に示すトラブルシューティング一覧表には、Microsoft アプリケーションまたはオペレーティング・システムで 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情報が記載されています。

問題の兆候	可能な解決策
スクリーン・セーバーが、ローカル・スクリーン上にしか表示されない	**処置**
Windows 拡張デスクトップ機能を使用しているときは、システムおよびそのキーボードへのアクセスが保護されていても、Client Security Software のスクリーン・セーバーは、ローカル・スクリーン上にしか表示されません。	機密情報が表示されているときには、拡張デスクトップ上のウィンドウを最小化してから、Client Security スクリーン・セーバーを呼び出します。
UVM 登録済みユーザー用の Client Security が、正しく機能しない	**処置**
登録済みクライアント・ユーザーが、自分の Windows ユーザー名を変更した可能性があります。そのようなことが起きた場合、Client Security 機能はすべて失効します。	UVM で新規ユーザー名を再登録して、新規クレデンシャルをすべて要求します。

問題の兆候	可能な解決策
注: Windows XP では、UVM に登録済みのユーザーは、以前に Windows ユーザー名を変更した場合、UVM に認識されません。Client Security Software のインストール前に Windows ユーザー名を変更した場合にも、この制約が伴います。	
Outlook Express を使用して、暗号化された電子メールを読み取っているときの問題	**処置**
Web ブラウザーの暗号化強度は、送信側と受信側とで異なるため、暗号化された電子メールは復号化できません。	次のことを検証します。 1. 送信側で使用されている Web ブラウザーの暗号化強度が、受信側で使用されている Web ブラウザーの暗号化強度と互換していること 2. Web ブラウザーの暗号化強度が、Client Security Software のファームウェアにより提供される暗号化強度と互換していること
複数の証明書が関連付けられたアドレスからの証明書を使用しているときの問題	**処置**
Outlook Express では、1 つの電子メール・アドレスに関連付けられている複数の証明書をリストすることができますが、これらの証明書のいずれかが無効になる可能性があります。証明書が無効になるのは、証明書に関連付けられた秘密鍵が、証明書の生成元である送信側コンピューターの IBM エンベデッド・セキュリティー・サブシステム上には存在しなくなった場合です。	受信側にディジタル証明書の再送を依頼してから、Outlook Express のアドレス帳でその証明書を選択します。
電子メール・メッセージへのディジタル署名を試みたときの失敗時メッセージ	**処置**
電子メール・メッセージのコンポーザーが、自分の電子メール・アカウントに証明書を関連付けていない場合は、電子メール・メッセージへのディジタル署名を試みたときにエラー・メッセージが表示されます。	Outlook Express のセキュリティー設定を使用して、ユーザー・アカウントに関連付ける証明書を指定します。詳しくは、Outlook Express 用に提供された資料を参照してください。
Outlook Express (128 ビット) では、3DES アルゴリズムを使用した場合にしか電子メールを暗号化できない	**処置**
128 ビット・バージョンの Internet Explorer 4.0 または 5.0 と Outlook Express を併用しているクライアント間で、暗号化された電子メールを送信しているときには、3DES アルゴリズムしか使用できません。	Outlook Express に使用されている暗号化アルゴリズムについては、Microsoft の最新情報を参照してください。
Outlook Express クライアントが、別のアルゴリズムを使用して電子メール・メッセージを戻す	**処置**

問題の兆候	可能な解決策
RC2(40)、RC2(64)、または RC2(128) アルゴリズムで暗号化された電子メール・メッセージが、Netscape Messenger を使用しているクライアントから Outlook Express (128 ビット) を使用しているクライアントに送信されます。 Outlook Express クライアントから戻される電子メール・メッセージは、RC2(40) アルゴリズムで暗号化されます。	アクションは不要です。 Netscape クライアントから Outlook Express (128 ビット) クライアントに対する RC2(40)、RC2(64)、または RC2(128) 暗号化要求は、常に、RC2(40) アルゴリズムを使用する Netscape クライアントに戻されます。ご使用のバージョンの Outlook Express に使用されている暗号化アルゴリズムについては、Microsoft の最新情報を参照してください。
ハード・ディスク・ドライブの障害後、Outlook Express で証明書を使用しているときのエラー・メッセージ	**処置**
管理者ユーティリティーでは、鍵の修復機能の使用による証明書の復元が可能になっていますが、一部の証明書 (VeriSign によって提供されている無償の証明書など) は、鍵の修復後に復元されない可能性があります。	鍵の修復後に、次のいずれかを行います。 • 新規の証明書の取得 • Outlook Express で、再び証明書の権限を登録します。
Outlook Express が、証明書に関連付けられた暗号化強度を更新しない	**処置**
送信側が Netscape で暗号化強度を選択して、署名付き電子メール・メッセージを、Outlook Express と Internet Explorer 4.0 (128 ビット) を併用しているクライアントに送信した場合、戻された電子メールの暗号化強度が一致しない可能性があります。	関連付けられている証明書を Outlook Express のアドレス帳から削除します。再び署名付き電子メールを開いて、証明書を Outlook Express のアドレス帳に追加します。
Outlook Express で、復号化のエラー・メッセージが表示される	**処置**
Outlook Express では、メッセージをダブルクリックして開くことができます。場合によっては、暗号化されたメッセージをあまりにも素早くダブルクリックした場合は、復号化のエラー・メッセージが表示されます。	メッセージを閉じて、暗号化された電子メール・メッセージをもう一度開きます。
暗号化されたメッセージを選択したときに、復号化のエラー・メッセージが、プレビュー画面区画に表示されることもあります。	プレビュー・ウィンドウ画面区画にエラー・メッセージが表示された場合、アクションは不要です。
暗号化された電子メールにカーソルを合わせて「送信」ボタンを 2 回クリックすると、エラー・メッセージが表示される	**処置**
Outlook Express を使用中に、暗号化された電子メール・メッセージを送信しようとして「送信」ボタンを 2 回クリックした場合、メッセージの送信不能を通知するメッセージが表示されます。	エラー・メッセージを閉じて、「**送信**」ボタンを 1 回クリックします。
証明書を要求中に、エラー・メッセージが表示される	**処置**

問題の兆候	可能な解決策
Internet Explorer を使用している場合、IBM エンベデッド・セキュリティー・サブシステム CSP を使用する証明書を要求したときに、エラー・メッセージを受け取る可能性があります。	ディジタル証明書をもう一度要求します。

Netscape アプリケーションに関するトラブルシューティング情報

次に示すトラブルシューティング一覧表には、Netscape アプリケーションで 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情報が記載されています。

問題の兆候	可能な解決策
暗号化された電子メールを読み取っているときの問題	**処置**
Web ブラウザーの暗号化強度は、送信側と受信側とで異なるため、暗号化された電子メールは復号化できません。	次のことを検証します。 1. 送信側で使用されている Web ブラウザーの暗号化強度が、受信側で使用されている Web ブラウザーの暗号化強度と互換していること 2. Web ブラウザーの暗号化強度が、Client Security Software のファームウェアにより提供される暗号化強度と互換していること
電子メール・メッセージへのディジタル署名を試みたときの失敗時メッセージ	**処置**
Netscape Messenger で IBM エンベデッド・セキュリティー・サブシステム証明書が選択されていない場合、電子メール・メッセージの作成者が証明書付きメッセージに署名しようとしたときに、エラー・メッセージが表示されます。	Netscape Messenger のセキュリティー設定を使用して、証明書を選択します。 Netscape Messenger が開いているときは、ツールバー上のセキュリティー・アイコンをクリックします。「セキュリティー情報」ウィンドウが開きます。左パネル内の「**Messenger**」をクリックし、「**IBM エンベデッド・セキュリティー・チップ証明書**」を選択します。詳しくは、Netscape の説明書を参照してください。
別のアルゴリズムを使用しているクライアントに、電子メール・メッセージが戻される	**処置**
RC2(40)、RC2(64)、または RC2(128) アルゴリズムで暗号化された電子メール・メッセージが、Netscape Messenger を使用しているクライアントから Outlook Express (128 ビット) を使用しているクライアントに送信されます。 Outlook Express クライアントから戻される電子メール・メッセージは、RC2(40) アルゴリズムで暗号化されます。	アクションは不要です。 Netscape クライアントから Outlook Express (128 ビット) クライアントに対する RC2(40)、RC2(64)、または RC2(128) 暗号化要求は、常に、RC2(40) アルゴリズムを使用する Netscape クライアントに戻されます。ご使用のバージョンの Outlook Express に使用されている暗号化アルゴリズムについては、Microsoft の最新情報を参照してください。

問題の兆候	可能な解決策
IBM エンベデッド・セキュリティー・サブシステムで生成されたディジタル証明書を使用できない	**処置**
IBM エンベデッド・セキュリティー・サブシステムで生成されたディジタル証明書は、使用の目的に提供されるものではありません。	Netscape が開いたときに、正確な UVM パスフレーズが入力されていることを検査します。不正な UVM パスフレーズを入力した場合、認証の失敗を通知するエラー・メッセージが表示されます。「**OK**」をクリックすると Netscape が開きますが、IBM エンベデッド・セキュリティー・サブシステムで生成された証明書を使用することはできません。Netscape を終了して再度開いてから、正しい UVM パスフレーズを入力する必要があります。
Netscape 内部では、同じ差し出し人からのディジタル証明書が新しいものに置き換わらない	**処置**
ディジタル署名付き電子メールを同じ差し出し人が複数回受信した場合、その電子メールに関連付けられた最初のディジタル証明書は上書きされません。	電子メールのディジタル証明書を複数受信した場合でも、1 つの証明書のみがデフォルトの証明書です。 Netscape のセキュリティー機能を使用して最初の証明書を削除してから 2 つ目の証明書を再度開くか、差し出し人にもう 1 つ署名付き電子メールを送信するよう依頼してください。
IBM エンベデッド・セキュリティー・サブシステム証明書をエクスポートできない	**処置**
Netscape では、IBM エンベデッド・セキュリティー・サブシステム証明書のエクスポートはできません。 Netscape のエクスポート機能は、証明書のバックアップを取る目的に用いることができます。	管理者ユーティリティーまたはユーザー構成ユーティリティーに移動して、鍵アーカイブを更新します。鍵アーカイブを更新すると、IBM エンベデッド・セキュリティー・サブシステムに関連付けられた全証明書のコピーが作成されます。
ハード・ディスク・ドライブの故障後に、復元された証明書を使おうとしたときのエラー・メッセージ	**処置**
管理者ユーティリティーでは、鍵の修復機能の使用による証明書の復元が可能になっていますが、一部の証明書 (VeriSign によって提供されている無償の証明書など) は、鍵の修復後に復元されない可能性があります。	鍵の修復後に、新しい証明書を取得します。
Netscape エージェントが開いてしまい、Netscape が失敗する	**処置**
Netscape エージェントは開いたときに Netscape を終了させてしまいます。	Netscape エージェントをオフにします。
Netscape を開こうとしても、すぐには開かない	**処置**

問題の兆候	可能な解決策
IBM エンベデッド・セキュリティー・サブシステム PKCS#11 モジュールを追加した後で Netscape を開こうとした場合、少し時間がたってからでないと Netscape が開きません。	アクションは不要です。これは情報提供目的にのみ記載したものです。

ディジタル証明書に関するトラブルシューティング情報

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始動して、証明書をもう一度取得します。

Tivoli Access Manager に関するトラブルシューティング情報

Client Security Software と Tivoli Access Manager の併用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
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へのアクセス不能	**処置**

問題の兆候	可能な解決策
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 のクライアント上に 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**」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 に関するトラブルシューティング情報

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 プロテクションが有効化された後には、Notes 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、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 の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。それでもエラーが生じる場合は、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**

問題の兆候	可能な解決策
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。

暗号化に関するトラブルシューティング情報

Client Security Software 3.0 またはそれ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
以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 またはそれ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 またはそれ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 では復号化できません。

UVM 対応デバイスに関するトラブルシューティング情報

UVM 対応デバイス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情報を、次に示します。

問題の兆候	可能な解決策
UVM 対応デバイスが正常に動作しなくなった	**処置**

問題の兆候	可能な解決策
UVM 対応セキュリティー・デバイス (スマート・カード、スマート・カード読取装置、指紋読取装置など) が正常に動作しなくなりました。	デバイスがシステムで正しく構成されているか確認してください。デバイスを構成した後、サービスが正しく開始されるように、システムをリブートする必要がある場合があります。 デバイスのトラブルシューティング情報については、そのデバイスの資料を参照するか、またはそのデバイスのベンダーに連絡してください。
UVM 対応デバイスが正常に動作しなくなった	**処置**
UVM 対応デバイスは、USB (Universal Serial Bus) ポートから切断した後で USB ポートに再接続すると、正常に動作しなくなる可能性があります。	デバイスを USB ポートに再接続した後で、コンピューターを再始動してください。

付録 B. パスワードおよびパスフレーズの情報

この付録では、パスワードおよびパスフレーズについて説明します。

パスワードとパスフレーズの規則

セキュア・システムを取り扱う場合には、さまざまなパスワードとパスフレーズが存在します。パスワードが異なれば、規則も異なります。このセクションでは、管理者パスワードと UVM パスフレーズについて説明します。

管理者パスワードの規則

管理ユーティリティーのインターフェースにより、セキュリティー管理者は、単純なインターフェースを介してパスワードの基準を管理できます。このインターフェースによって、管理者は以下の管理者パスワード規則を設定できます。

注: 以下のリストでは、各パスフレーズ基準のデフォルト設定値を括弧で示しています。管理者パスワードは有効期限が切れることはありません。

- 英数字の許容最小文字数を設定するかどうか (はい、6 文字)

  たとえば、「6」文字が許容されるように設定されている場合、1234567xxx は無効なパスワードです。
- 数字の許容最小文字数を設定するかどうか (はい、1 文字)

  たとえば、「1」に設定されている場合、thisismypassword は無効なパスワードです。
- スペースの許容最小数を設定するかどうか (最小数なし)

  たとえば、「2」に設定されている場合、i am not here は無効なパスワードです。
- パスフレーズの先頭文字として数字を使用可能にするかどうか (いいえ)

  たとえば、1password は、デフォルトでは無効なパスワードです。
- パスフレーズの末尾文字として数字を使用可能にするかどうか (いいえ)

  たとえば、password8 は、デフォルトでは無効なパスワードです。

以下の一般規則は管理者パスワードに関係するものです。

長さ パスワードの長さは、最大で 256 文字です。

文字 パスワードには、スペースや英数字以外の文字など、キーボードから入力できる任意の文字を組み合わせて使用できます。

プロパティー
管理者パスワードは、オペレーティング・システムへのログオン時に使用するパスワードとは異なります。管理者パスワードは、他の認証装置 (UVM 対応の指紋センサーなど) と合わせて使用できます。

誤入力 セッション時に管理者パスワードの誤入力を複数回行ってしまった場合、コンピューターは一連の攻撃対応型の遅延を実行します。

UVM パスフレーズの規則

IBM Client Security Software によって、セキュリティー管理者はユーザーの UVM パスフレーズを取り決める規則を設定することができます。セキュリティーを向上させるため、UVM パスフレーズは、従来のパスワードより長く、かつその独自性を高めることができます。 UVM パスフレーズ・ポリシーは、管理者ユーティリティーによって管理されています。

管理ユーティリティーの UVM パスフレーズ・ポリシー・インターフェースにより、セキュリティー管理者は、単純なインターフェースを介してパスフレーズの基準を管理できます。UVM パスフレーズ・ポリシー・インターフェースでは、管理者が以下のパスフレーズ規則を制定できます。

注: 以下のリストでは、各パスフレーズ基準のデフォルト設定値を括弧で示しています。

- 英数字の許容最小文字数を設定するかどうか (はい、6 文字)

  たとえば、「6」文字が許容されるように設定されている場合、1234567xxx は無効なパスワードです。
- 数字の許容最小文字数を設定するかどうか (はい、1 文字)

  たとえば、「1」に設定されている場合、thisismypassword は無効なパスワードです。
- スペースの許容最小数を設定するかどうか (最小数なし)

  たとえば、「2」に設定されている場合、i am not here は無効なパスワードです。
- パスフレーズの先頭文字として数字を使用可能にするかどうか (いいえ)

  たとえば、1password は、デフォルトでは無効なパスワードです。
- パスフレーズの末尾文字として数字を使用可能にするかどうか (いいえ)

  たとえば、password8 は、デフォルトでは無効なパスワードです。
- ユーザー ID を含むパスフレーズを許可するかどうか (いいえ)

  たとえば、UserName は、デフォルトでは無効なパスワードです。ここで、UserName はユーザー ID です。
- 新しいパスフレーズが直近に使用した x 種類のパスフレーズとは異なることを確認するかどうか (はい、3 種類)

  たとえば、最後の 3 つのパスワードのいずれかが mypassword であれば、mypassword は、デフォルトでは無効なパスワードです。
- パスフレーズの任意の位置に、以前のパスワードに使用した文字と同一の文字が連続して 4 文字以上含まれることを可能にするかどうか (いいえ)

  たとえば、前のパスワードが pass または word であれば、paswor は、デフォルトでは無効なパスワードです。

管理ユーティリティーの UVM パスフレーズ・ポリシー・インターフェースにより、セキュリティー管理者は、パスフレーズの有効期限も管理することができます。 UVM パスフレーズ・ポリシー・インターフェースを使用すれば、管理者は、以下のパスフレーズ有効期限規則から選択することができます。

- 所定の日数を過ぎたら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設定する (はい、184 日)

  たとえば、パスフレーズは、デフォルトでは 184 日で有効期限が切れます。新規のパスフレーズは、設定されたパスフレーズ・ポリシーに従わなければなりません。
- 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設定する (はい)

  このオプションを選択すると、パスフレーズの有効期限は切れません。

パスフレーズ・ポリシーは、ユーザーが登録されると、管理者ユーティリティーによって検査されます。また、ユーザーがクライアント・ユーティリティーを使用してパスフレーズを変更したときにも検査されます。以前のパスワードに関連している 2 つのユーザー設定はリセットされ、パスフレーズ・ヒストリーはすべて削除されます。

以下の一般的な規則は、UVM パスフレーズに関係するものです。

長さ パスフレーズの長さは、最大で 256 文字です。

文字 パスフレーズには、スペースや英数字以外の文字など、キーボードから入力できる任意の文字を組み合わせて使用できます。

プロパティー
UVM パスフレーズは、オペレーティング・システムへのログオン時に使用するパスワードとは異なります。UVM パスフレーズは、ほかの認証装置 (UVM 対応の指紋センサーなど) と合わせて使用できます。

誤入力 セッション時に UVM パスフレーズの誤入力を複数回行ってしまった場合、コンピューターは一連の攻撃対応型の遅延を実行します。このような遅延は、次のセクションで指定します。

National TPM を使用するシステムでの失敗回数

次の表は、National TPM システムの攻撃対応型の遅延の設定値です。

回数	次の失敗の場合の遅延
7-13	4 秒ごと
14-20	8 秒ごと
21-27	16 秒ごと
28-34	32 秒ごと
35-41	64 秒ごと (1.07 分ごと)
42-48	128 秒ごと (2.13 分ごと)
49-55	256 秒ごと (4.27 分ごと)
56-62	512 秒ごと (8.53 分ごと)
63-69	1,024 秒ごと (17.07 分ごと)

回数	次の失敗の場合の遅延
70-76	2,048 秒ごと (34.13 分ごと)
77-83	68.26 分ごと (1.14 時間ごと)
84-90	136.52 分ごと (2.28 時間ごと)
91-97	273.04 分ごと (4.55 時間ごと)
98-104	546.08 分ごと (9.1 時間ごと)
105-111	1,092.16 分ごと (18.2 時間ごと)
112-118	2,184.32 分ごと (36.4 時間ごと)

National TPM システムでは、ユーザー・パスフレーズと管理者パスワードを区別していません。 IBM エンベデッド・セキュリティー・チップを使用する認証は、いずれも同じポリシーに従っています。最大タイムアウトはありません。試行が失敗するごとに、上記の遅延が開始されます。攻撃対応型の遅延は、118 回目の試行でも終了せず、上記の方法で無限に継続します。

Atmel TPM を使用するシステムでの失敗回数

次の表は、Atmel TPM システムの攻撃対応型の遅延の設定値です。

回数	次の失敗の場合の遅延
15	1.1 分
31	2.2 分
47	4.4 分
63	8.8 分
79	17.6 分
95	35.2 分
111	1.2 時間
127	2.3 時間
143	4.7 時間

Atmel TPM システムでは、ユーザー・パスフレーズと管理者パスワードを区別していません。 IBM エンベデッド・セキュリティー・チップを使用する認証は、いずれも同じポリシーに従っています。最大タイムアウトは 4.7 時間です。 Atmel TPM システムは、4.7 時間を超えて遅延することはありません。

パスフレーズの変更

ユーザーが自分のパスフレーズを忘れてしまった場合、管理者はそのユーザーのパスフレーズを変更することができます。

リモート側でのパスフレーズの変更

リモート側でパスワードを変更するには、次の手順を実行します。

- **管理者**

リモートの管理者は、以下のことを行う必要があります。

1. 一回限りのパスワードを新たに作成し、ユーザーに伝えます。
2. データ・ファイルをユーザーに送信します。

   このデータ・ファイルは、E メールでユーザーに送信することも、ディスケットなどの取り外し可能メディアにコピーすることも、あるいはユーザーのアーカイブ・ファイル (ユーザーがこのシステムにアクセスできるという前提) に直接書き込むことも可能です。この暗号化されたファイルを使用して、新しい一回限りのパスワードと突き合わせます。

- **ユーザー**

  ユーザーは、以下のことを行う必要があります。

  1. コンピューターにログオンします。
  2. パスフレーズのプロンプトが出されたならば、「パスフレーズを忘れました」のチェック・ボックスにチェックマークを付けます。
  3. リモートの管理者から伝えられた一回限りのパスワードを入力し、管理者から送信されたファイルのロケーションを指定します。

     UVM が、ファイル内の情報と提供されたパスワードが一致することを検証した後、ユーザーはアクセスが認可されます。その後、ユーザーは直ちにパスフレーズを変更するようにプロンプトが出されます。

これが、紛失したパスフレーズを変更する際にお勧めできる方法です。

パスフレーズの手動変更

自分のパスフレーズを忘れたユーザーのシステムのところへ管理者が行ける場合は、管理者はユーザーのシステムで管理者としてログオンし、管理者ユーティリティーに対する秘密鍵を与え、ユーザーのパスフレーズを手動で変更することができます。パスフレーズを変更する際に、管理者はそのユーザーの元のパスフレーズを知っている必要はありません。

付録 C. システムへのログオン時に UVM プロテクションを使用するための規則

UVM プロテクションでは、特定の IBM クライアントの UVM に登録されたユーザーのみがオペレーティング・システムにアクセスできるようになります。Windows オペレーティング・システムには、ログオン時の保護機能を提供しているアプリケーションがあります。UVM プロテクションは、こうした Windows ログオン・アプリケーションと並行して機能するように設計されていますが、UVM プロテクションはオペレーティング・システムごとに異なります。

UVM ログオン・インターフェースが、オペレーティング・システムのログオンに置き換わります。したがって、ユーザーがシステムにログオンしようとするたびに、UVM ログオン・ウィンドウが開きます。

UVM プロテクションを設定して、システムへのログオン時にこの機能を使用するには、事前に次のヒントをお読みになってください。

- UVM プロテクションが使用可能になっている場合は、IBM エンベデッド・セキュリティー・チップをクリアしないでください。そのようなことを行うと、ハード・ディスクの内容が使用不能になるため、ハード・ディスク・ドライブを再フォーマットして、ソフトウェアをすべて再インストールしなければならなくなります。
- 管理者ユーティリティーの「**Windows ログオン置換を有効にする** 」チェック・ボックスのチェックを外すと、システムは UVM ログオン・プロテクションなしに Windows ログオン・プロセスに戻ります。
- Windows ログオン・アプリケーションに正しいパスワードを入力するための最大試行回数を指定することができます。このオプションは UVM ログオン・プロテクションには適用されません。UVM パスフレーズの入力試行回数には、限度を設定することはできません。

付録 D. Client Security Software に関する米国の輸出規制

IBM Client Security Software パッケージは、IBM Export Regulation Office (ERO) によって審査されておりますが、米国政府より輸出規制を要求されていることから、IBM では、これに該当する資料を提出致しました。この結果、米国政府による輸出禁止措置の対象国を除く各国への販売を目的として、最大 256 ビットの暗号化サポートに関する小売分類の承認を米国商務省から得ています。米国およびその他の国における規制は、当該国によって変更されることがあります。

Client Security Software パッケージをダウンロードできない場合は、最寄りの IBM 製品販売店に連絡し、担当の IBM Country Export Regulation Coordinator (ERC) による調査を依頼してください。

付録 E. 特記事項および商標

この付録には、IBM 製品に関する特記事項および商標を記載します。

特記事項

本書は製造元が提供する製品およびサービスについて作成したものです。

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

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 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。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム（本プログラムを含む）との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。 IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. 本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

商標

IBM、SecureWay および Tivoli は、IBM Corporation の商標です。

Tivoli は、Tivoli Systems, Inc. の商標です。

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などはそれぞれ各社の商標または登録商標です。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12