IBM® Client Security Solutions

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

IBM® Client Security Solutions

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

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

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

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

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

(URL は、変更になる場合があります)

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

原 典:	IBM Client Security Solutions Client Security Software Version 5.4 Installation 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

目次

まえがき

ここでは、本書の使用方法を説明します。

本書について

本書は、IBM ネットワーク・コンピューターに IBM Client Security Software をインストールする方法、さらに IBM エンベデッド・セキュリティー・サブシステムを搭載した IBM クライアントについて解説します。 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にする手順、およびセキュリティー・サブシステムの管理者パスワードの設定方法についても説明します。

本書は、次のように構成されています。

『第 1 章 概要』では、基本的なセキュリティー概念のアウトライン、このソフトウェアに組み込まれているアプリケーションおよびコンポーネントの概要、および Public Key Infrastructure (PKI) 機能について説明します。

『第 2 章 はじめに』では、コンピューターのハードウェアとソフトウェアのインストールに関する前提条件、およびソフトウェアのダウンロードについて説明します。

『第 3 章 ソフトウェアをインストールする前に』では、IBM Client Security Software のインストールに必要となる前提条件が記載されています。

『第 4 章 ソフトウェアのダウンロード、インストール、および構成』では、ソフトウェアのインストール、更新、およびアンインストールについて説明します。

『第 5 章 トラブルシューティング』では、本書に記載の指示を実行中に問題に遭遇したときの対応方法について役立つ情報が記載されています。

『付録 A. Client Security Software に関する米国の輸出規制』には、このソフトウェアに関する米国の輸出規制について情報が記載されています。

『付録 B. パスワードおよびパスフレーズの情報』では、UVM パスフレーズに適用できる基準、および管理者パスワードに対するルールについて説明します。

『付録 C. **特記事項および商標**』には、法的な特記事項と商標情報が記載されています。

本書の対象読者

本書は、IBM クライアント用のパーソナル・コンピューティング・セキュリティーをセットアップするネットワーク管理者またはシステム管理者を対象としています。ネットワーク環境内における公開鍵インフラストラクチャー (PKI) やディジタル証明書の管理などのセキュリティー概念に関する知識が必要です。

本書の使用法

本書を使用して、IBM クライアント上にパーソナル・コンピューティング・セキュリティーをインストールおよびセットアップしてください。本書は、*Client Security Software 管理者およびユーザー・ガイド* の姉妹書です。

本書およびその他のすべての Client Security 資料は、次の IBM Web サイトからダウンロードできます。http://www.ibm.com/jp/pc/security/css/security.html

「*Client Security Software 管理者およびユーザー・ガイド*」への参照

本書では、「*Client Security Software 管理者およびユーザー・ガイド*」を参考資料として使用します。「*管理者およびユーザー・ガイド*」には、ユーザー認証マネージャー (UVM) の使用方法、UVM ポリシーの処理方法、および管理者ユーティリティーとユーザー構成ユーティリティーの使用方法が記載されています。

ソフトウェアをインストール後、「*管理者およびユーザー・ガイド*」の説明を使用して、クライアントごとにセキュリティー・ポリシーのセットアップおよび保守をします。

その他の情報

その他の情報およびセキュリティー製品の更新がある場合は、次の IBM Web サイトから取得できます。http://www-6.ibm.com/jp/pc/security/

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・チップを使用してファイルの暗号化と鍵の格納を行う 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・チップ

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・サブシステムの登場により、暗号化と認証のプロセスは、ぜい弱なソフトウェア環境から、専用のハードウェアによる機密保護機能を備えた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、以下のことをサポートします。

- 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
- Trusted Computing Group (TCG) の TCG Main Specification version 1.1 で定義されている TCG のすべての機能
- 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:** Client Security Software 管理者コンソールによって、管理者はクレデンシャル・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ファイルの作成および構成、管理者以外のユーザーの構成の作成、およびプロファイルのリカバリーを行うことができます。
- **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を使用すると、クライアント・ユーザーは、UVM パスフレーズの変更、Windows ログオン・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することができます。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 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・チップ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、*鍵ペア* とも呼ばれますが、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・サブシステムのハードウェアによる機密保護機能のある領域で作成され、格納され、使用されます。また、ハードウェア公開鍵はさまざまな目的に利用できます (そのため公開鍵という名前が付けられてい

る) が、セキュリティー・サブシステムによる機密保護が機能しない領域に公開されることはありません。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、以下の方法で作成されます。

- 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、公開鍵および秘密鍵は*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、IBM 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。

公開鍵および秘密鍵は、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、以下いずれかの方法で作成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

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、管理者公開鍵および管理者秘密鍵によって、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づいて管理されます。

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。鍵スワッピング階層のベース (またはルート) は、ハードウェア公

開鍵および秘密鍵です。ハードウェア公開鍵および秘密鍵は、*ハードウェア鍵ペア*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、つまり*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ています。管理者秘密鍵は、それがクライアント・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、管理者定義のロケーションで固有です。

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、公開鍵と秘密鍵 (*ユーザー鍵ペア*) が作成され、新しい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・サブシステムによる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・サブシステムによって、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 鍵スワップ階層を使用します。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 (管理者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。 IBM ESS を持つシステムに登録できるユーザーの数には制限はありませんが、最良実例によると最適なパフォーマンスを得るためにはコンピューターごとのユーザー数を 25 人までにすることが推奨されます。

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、いったん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て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・サブシステム上の乱数機能によって、それぞれのハードウェア鍵ペアは統計的に固有であることが保証されます。

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暗号鍵の管理** 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・ユーザー用の鍵を作成します。作成された鍵は、鍵の階層を介して IBM エンベデッド・セキュリティー・サブシステムにバインドされます。そこでは、ベース・レベルのハードウェア鍵を使用して、上位の鍵 (クライアント・ユーザーに関連付けられたユーザー鍵など) が暗号化されます。 IBM エンベデッド・セキュリティー・サブシステム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は、ユーザーの公開鍵で暗号化され、IBM エンベデッド・セキュリティー・サブシステムに確実に格納されます。 Netscape ユーザーも、セキュリティーのための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・サブシステムを選択できます。 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 で保護されているディジタル証明書は、別の CSP にエクスポートできません。

- **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 指紋読取装置および一部の IBM PC に内蔵されている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。
- **Gemplus GemPC400 によるスマート・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、登録されているネットワーク・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 に登録されたクライアントでの UVM 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、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 章 はじめに

この章では、IBM Client Security Software を使用する場合のハードウェアとソフトウェアの互換性に関する要件について説明します。 IBM Client Security Software のダウンロードについても説明します。

ハードウェア要件

ソフトウェアをダウンロードおよびインストールする前に、お使いのコンピューターのハードウェアが IBM Client Security Software と互換性があることを確認します。

ハードウェアおよびソフトウェアの要件については、IBM Web サイト http://www.ibm.com/jp/pc/security/css/security.html で最新情報を参照できます。

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、IBM クライアントのシステム・ボードに埋め込まれた暗号マイクロプロセッサーです。この IBM Client Security の重要なコンポーネントによって、セキュリティー・ポリシーはぜい弱なソフトウェアから強固なハードウェアに移され、ローカル・クライアントのセキュリティーは大幅に強化されます。

IBM Client Security Software を使用できるのは、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 コンピューターとワークステーションのみです。IBM エンベデッド・セキュリティー・サブシステムを備えていないコンピューターに、このソフトウェアをダウンロードおよびインストールしても、ソフトウェアのインストールまたは実行は正しく行われません。

サポート対象の IBM モデル

Client Security Software は、多くの IBM デスクトップ・コンピューターやノートブック・コンピューターをサポートしています。サポートされるモデルの最新のリストは、Web ページ http://www.ibm.com/jp/pc/security/css/security.html をご覧ください。

ソフトウェア要件

ソフトウェアをダウンロードおよびインストールする前に、お使いのコンピューターのソフトウェアとオペレーティング・システムが、IBM Client Security Software と互換性があることを確認します。

オペレーティング・システム

IBM Client Security Software は、次のいずれかのオペレーティング・システムを必要とします。

- Windows XP

- Windows 2000 Professional 版

UVM 認識製品

IBM Client Security にはユーザー認証マネージャー (UVM) ソフトウェアが付属しており、これを使用すると、デスクトップ・コンピューターの認証方式をカスタマイズできます。この第 1 レベルのポリシー・ベースの制御により、資産保護を強化し、パスワード管理効率を高めます。 UVM は、会社全体に使用されているセキュリティー・ポリシー・プログラムと互換性があります。次のような UVM 認識製品を使用できます。

- **指紋読取装置などのバイオメトリック認証デバイス**

  UVM は、バイオメトリック認証デバイスについて、プラグ・アンド・プレイ・インターフェースを提供します。 IBM Client Security Software をインストールしてから、UVM 認識センサーをインストールする必要があります。UVM 認識センサーとしては、Targus 指紋読取装置および一部の IBM PC に内蔵されている内蔵型指紋読取装置があります。

  Targus の装置の場合、IBM クライアントにすでにインストールされている UVM 認識センサーを使用する場合は、その UVM 認識センサーをいったんアンインストールし、IBM Client Security Software をインストールしてから、UVM 認識センサーを再インストールする必要があります。内蔵型の場合は、既に認識センサーのドライバーがインストールされていますので、その状態で IBM Client Security Software のインストールを行ってください。

- **Tivoli Access Manager バージョン 5.1**

  UVM ソフトウェアは、Tivoli Access Manager などの中央化したポリシー・ベースのアクセス制御ソリューションとスムーズに統合することによって、ポリシー管理を単純化し、改善します。

  UVM ソフトウェアは、ネットワーク・システム (デスクトップ) およびスタンドアロン・システムの両者について、ポリシーをローカルで強化して、単一の一体化したポリシー・モデルを構築します。

- **Lotus Notes のバージョン 4.5 以降**

  UVM は、IBM Client Security Software と併用すると、Lotus Notes のログオン (Lotus Notes のバージョン 4.5 以降) でセキュリティーを改善できます。

- **Entrust Desktop Solutions 5.1、6.0、または 6.1**

  Entrust Desktop Solutions は、インターネットのセキュリティー機能をサポートし、重要な企業の各種処理をインターネットに移行できるようにします。 Entrust Entelligence は、識別や、プライバシー、検査、およびセキュリティー管理など、セキュリティーについて企業が必要とするすべての項目を 1 つのセキュリティー層で提供します。

- **RSA SecurID Software Token**

  RSA SecurID Software Token によって、従来からの RSA ハードウェア・トークンで使用するのと同じシードのレコードを既存のユーザー・プラットフォームに

組み込むことができます。その結果、専用の認証装置を使用せずに、組み込まれたソフトウェアにアクセスすることで、保護リソースへの認証をユーザーが得ることができます。

- **Gemplus GemPC400 スマート・カード読取装置**

  Gemplus GemPC400 スマート・カード読取装置を使用すれば、セキュリティー・ポリシーでスマート・カード認証を組み込んで、標準のパスフレーズ保護に対してさらにセキュリティー層を追加することができます。

Web ブラウザー

IBM Client Security Software は、ディジタル証明書を要求する際に次の Web ブラウザーをサポートします。

- Internet Explorer 5.0 またはそれ以降
- Netscape 4.8 および Netscape 7.1

ブラウザーの暗号化強化情報

強力な暗号化のサポートがインストールされている場合は、128 ビット・バージョンの Web ブラウザーを使用します。お使いの Web ブラウザーの暗号化強度をチェックするには、そのブラウザーに付属のヘルプ・システムを参照してください。

暗号化サービス

IBM Client Security Software は次の暗号化サービスをサポートします。

- **Microsoft CryptoAPI:** CryptoAPI は、Microsoft のオペレーティング・システムおよびアプリケーションに使用するデフォルトの暗号サービスです。 CryptoAPI サポートが組み込まれた IBM Client Security Software を使用すると、Microsoft アプリケーション用のディジタル証明書を作成する際に、IBM エンベデッド・セキュリティー・サブシステムの暗号操作を使用できます。
- **PKCS#11:** PKCS#11 は、Netscape、Entrust、RSA およびその他の製品に使用する暗号規格です。 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、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、PKCS#11 を使用する Netscape、Entrust、RSA、およびその他のアプリケーション用にディジタル証明書を生成できます。

E メール・アプリケーション

IBM Client Security Software は、セキュア E メールを使用して、次のアプリケーション・タイプをサポートします。

- Outlook Express および Outlook (サポート対象バージョンの Internet Explorer を使用した場合) など、暗号操作に Microsoft CryptoAPI を使用する E メール・アプリケーション
- Netscape Messenger (サポート対象バージョンの Netscape) など、暗号操作に公開鍵暗号化標準 #11 (PKCS#11) を使用する E メール・アプリケーション
- UVM ログオン・プロテクションによる Lotus Notes サポート

第 3 章 ソフトウェアをインストールする前に

この章では、IBM クライアントでインストール・プログラムを実行し、IBM Client Security Software を構成するのに必要な前提条件が記載されています。

Client Security Software のインストールに必要なすべてのファイルは、 IBM Web サイト http://www.ibm.com/jp/pc/security/css/security.html から入手できます。この Web サイトでは、システムに IBM エンベデッド・セキュリティー・サブシステムがあるかどうかを確認し、システムに適切な IBM Client Security オファリングを選択できるようにするための情報が提供されています。

ソフトウェアをインストールする前に

インストール・プログラムを使用すると、IBM クライアント上に IBM Client Security Software をインストールして、IBM エンベデッド・セキュリティー・サブシステムを使用できるようになりますが、インストール特性はさまざまな要因により異なります。

IBM Client Security Software をインストールするには、管理者権限を持つユーザーがログオンする必要があります。

Tivoli Access Manager を使用する場合のインストール

Tivoli Access Manager を使用してコンピューターの認証を制御する場合は、 IBM Client Security Software をインストールする*前*に、なんらかの Tivoli Access Manager コンポーネントをインストールしておく必要があります。詳しくは、「*Tivoli Access Manager での Client Security の使用法*」を参照してください。

スタートアップ機能に関する考慮事項

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方法や暗号鍵を生成する方法が、2 つの IBM スタートアップ機能により影響を受ける場合があります。そのような機能とは、BIOS 管理者パスワードおよび拡張セキュリティーであり、IBM コンピューターの構成/セットアップ・ユーティリティーからアクセスできます。 IBM Client Security Software には別個の管理者パスワードがあります。混乱を避けるために、 Client Security Software の資料では、 BIOS Setup Utility (BIOS セットアップ・ユーティリティー) で設定される管理者パスワードのことを *BIOS 管理者パスワード* と呼びます。

BIOS 管理者パスワード

BIOS 管理者パスワードは、許可されていない人が IBM コンピューターの設定内容を変更できないようにします。このパスワードは、 NetVista または ThinkCentre コンピューターの構成/セットアップ・ユーティリティー、または ThinkPad コンピューターの IBM BIOS セットアップ・ユーティリティーを使用して設定されます。コンピューターの始動時に Enter または F1 のキーを押すと、該当するプログラムにアクセスできます。このパスワードは、ThinkCentre 構成/セットアップ・ユーティ

リティーでは*管理者*パスワード、ThinkPad BIOS セットアップ・ユーティリティーではスーパーバイザー・パスワード と呼ばれるものです。

拡張セキュリティー

拡張セキュリティーは、始動シーケンスの設定に加えて、BIOS 管理者パスワードに対して追加の保護を提供します。拡張セキュリティーが使用可能になっているか、使用不可になっているかは、構成/セットアップ・ユーティリティーで確認できます。このユーティリティーは、システムの始動時に F1 キーを押すとアクセスできます。

パスワードと拡張セキュリティーの詳細については、ご使用のコンピューターの説明書を参照してください。

NetVista 6059、6569、6579、6649 モデルおよびすべての NetVista Q1x モデルの拡張セキュリティー: NetVista モデル (6059、6569、6579、6649 モデルおよびすべての Q1x モデル) に管理者パスワードを設定した場合は、管理者ユーティリティーを開いて、IBM エンベデッド・セキュリティー・サブシステムを有効にして、鍵を生成する必要があります。

これらのモデルで拡張セキュリティーが使用可能になっている場合、 IBM Client Security Software をインストールした後で、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・サブシステムを有効にし、鍵を生成する必要があります。拡張セキュリティーが使用可能になっていることをインストール・プログラムが検出すると、インストール・プロセスの最後で通知が表示されます。コンピューターを再始動し、管理者ユーティリティーを開いて IBM エンベデッド・セキュリティー・サブシステムを有効にして、鍵を生成してください。

その他のすべての NetVista のモデル (6059、6569、6579、6649 モデルおよび NetVista Q1x モデル以外) の拡張セキュリティー: その他の NetVista モデルで管理者パスワードが設定されている場合は、インストール・プロセスで管理者パスワードの入力が求められることはありません。

これらの NetVista モデルで拡張セキュリティーが使用可能になっている場合、インストール・プログラムを使用して、ソフトウェアをインストールできますが、IBM エンベデッド・セキュリティー・サブシステムを有効にするには構成/セットアップ・ユーティリティーが必要です。セキュリティー・サブシステムを有効にした後で、管理者ユーティリティーを使用して鍵を生成できます。

BIOS 更新情報

ソフトウェアをインストールする前に、使用するコンピューターについて、最新の基本入出力システム (BIOS) コードのダウンロードが必要になる場合があります。コンピューターの現在の BIOS レベルを確認するには、コンピューターを再起動し、F1 キーを押して構成/セットアップ・ユーティリティーを開始します。構成/セットアップ・ユーティリティーのメインメニューで「製品データ」を選択して、BIOS コードに関する情報を表示します。 BIOS コード・レベルは、EEPROM 改訂レベルとも呼びます。

NetVista モデル (6059、6569、6579、6649) で IBM Client Security Software 2.1 またはそれ以降を実行するには、BIOS レベル xxxx22axx 以降が必要です。 NetVista モデル (6790、6792、6274、2283) で IBM Client Security Software 2.1 またはそれ

以降を実行するには、BIOS レベル xxxx20axx 以降が必要です。詳しくは、ソフトウェアのダウンロードに含まれている README ファイルを参照してください。

使用しているコンピューター用の最新の BIOS コードの更新プログラムを見つけるには、IBM Web サイト http://www.pc.ibm.com/support で、検索フィールドに bios と入力し、ドロップダウン・リストからダウンロードを選択して、Enter キーを押してください。 BIOS コードの更新プログラムが表示されます。該当するモデル番号を選択して、Web ページの指示に従ってください。

管理者鍵ペアを使用した鍵の作成

鍵ペアとは、修復のために外部メディアに保管されている管理者鍵ペアのコピーのことです。アーカイブ鍵ペアを作成するためには管理者ユーティリティーを使用するため、初期状態の IBM クライアントに IBM Client Security Software をインストールしてから、鍵ペアを作成する必要があります。

第 4 章 ソフトウェアのダウンロード、インストール、および構成

この章では、IBM クライアントに IBM Client Security Software をダウンロードし、インストールし、構成する手順について説明します。さらに、ソフトウェアのアンインストール方法についても説明します。 Client Security の機能を拡張する各種のユーティリティーをインストールする前に、必ず IBM Client Security Software をインストールしてください。

重要: IBM Client Security Software 5.0 よりも前のバージョンからアップグレードする場合は、Client Security Software 5.1 以降をインストールする*前*に、すべての暗号化ファイルを復号する*必要*があります。ファイル暗号化の方法が変更されているため、IBM Client Security Software 5.0 より前のバージョンを使用して暗号化されたファイルは、Client Security Software 5.1 以降では復号できません。

ソフトウェアのダウンロード

Client Security Software のインストールに必要なすべてのファイルは、 IBM Web サイト http://www.ibm.com/jp/pc/security/css/security.html から入手できます。この Web サイトでは、システムに IBM エンベデッド・セキュリティー・サブシステムがあるかどうかを確認し、システムに適切な IBM Client Security オファリングを選択できるようにするための情報が提供されています。

適切なファイルをシステムにダウンロードするには、次の手順を実行します。

1. Web ブラウザーを使用して IBM Web サイト http://www.ibm.com/jp/pc/security/css/security.html にアクセスします。
2. Web ページの「エンベデッド・セキュリティー・サブシステムおよび IBM Client Security Software」セクションで、**「ソフトウェアのダウンロード」**をクリックします。
3. 「システムの選択」ボックスで、**「システムを検出して継続」**をクリックするか、またはマシンの 7 桁のタイプ・モデル番号を該当するフィールドに入力します。
4. E-mail アドレスを該当するフィールドに入力し、ドロップダウン・メニューから国/地域を選択します。
5. さまざまな他のオファリングに関する情報の送信を希望する場合は、該当するチェック・ボックスを選択します。
6. **「使用許諾契約書を表示」**をクリックして使用許諾契約書を確認してから、**「使用許諾契約書に同意する」**をクリックします。

   自動的に IBM Client Security ダウンロード・ページに転送されます。
7. Client Security Software 5.4 に対応するリンクを探し、**「ダウンロード」**をクリックします。

注: css54readme.html ファイルを見て、アップグレードや制限事項に関する特定の情報を確認します。

8. **「保管」**をクリックして、インストール用実行可能ファイルのコピーをハード・ディスクに保管します。
9. 保管場所を指定して**「保管」**をクリックします。ソフトウェアのインストールを開始するには、ダウンロード完了時に**「開く」**をクリックするか、または実行可能ファイルのアイコンをダブルクリックします。

ソフトウェアのインストール

適切なファイルをシステムにインストールするには、次の手順を実行します。

1. ダウンロードした実行可能ファイルをダブルクリックします。
2. 「IBM Client Security 用の Install Shield ウィザードへようこそ」の画面で「**次へ**」をクリックします。
3. 使用許諾契約書を読んでから、**「使用許諾契約書の条項に同意します」**ラジオ・ボタンを選択し、**「次へ」**をクリックします。

   「製品の選択」画面が表示されます。
4. 以下のラジオ・ボタンのうちいずれか 1 つを選択してから、**「次へ」**をクリックします。
   - **「IBM Client Security Software と IBM Password Manager をインストールする」**。これは、IBM Client Security Software と IBM Password Manager、および必要なすべてのデバイス・ドライバーをインストールまたはアップグレードする場合に選択します。
   - **「IBM Client Security Software のみインストールする」**。これは、IBM Client Security Software、および必要なすべてのデバイス・ドライバーをインストールまたはアップグレードする場合に選択します。

   「インストール先のフォルダ」画面が表示されます。
5. デフォルトのインストール先をそのまま使用する場合は**「次へ」**をクリックします。それとは異なるインストール先フォルダーを指定する場合は**「変更」**をクリックします。

   「プログラムをインストールする準備ができました」画面が表示されます。
6. インストールを開始するには、**「インストール」**をクリックします。インストールの設定値を確認したり変更したりする場合は、**「戻る」**をクリックします。

   ステータス・バーにインストールの進行状況が表示されます。その後、「InstallShield ウィザード完了」画面が表示されます。
7. **「終了」**をクリックして、ウィザードを終了します。

コンピューターに対してなされたインストール変更内容を有効にするには、コンピューターを再始動します。

構成オプションの選択

IBM Client Security セットアップ・ウィザードの最初の画面で、構成オプションを選択できます。構成オプションとして適切なものを選択することは非常に重要です。構成オプションを選択する前に、以下の情報を注意深くお読みください。セキュリティー・ユーザーとして初心者の場合は、*標準構成* オプションを選択してください。

標準構成

Client Security セットアップ・ウィザードで IBM Client Security Software の標準構成を選択すると、Client Security の機能のうち、以下に示すものを構成することになります。

- IBM Password Manager (インストール時に選択した場合)
- 右クリック・ファイル暗号化
- パスフレーズおよび指紋認証
- ディジタル署名のサポート

Client Security セットアップ・ウィザードで推奨されている*標準構成* オプションを使用した場合、構成処理はシンプルです。しかしこの構成が選択されている場合、Client Security Software の拡張機能のうちのいくつかは使用不可になり、CSS の機能の一部が利用できなくなります。

標準構成のデフォルト設定値

標準構成のハードコーディングされたデフォルト設定値は、以下のとおりです。

- **アーカイブの位置:** C:¥documents and settings¥all users¥application data¥ibm¥security¥archive
- **管理者鍵ペアの位置:** C:¥documents and settings¥all users¥application data¥ibm¥security¥keys

  管理者秘密鍵は分割されず、CSS 管理者パスフレーズによって暗号化されます。

その他の設定値としては、次のものがあります。

- IBM Password Manager のサポートは有効。
- セキュリティー・ポリシーは中: 使用可能な各認証方式が必要とされるのは、CSS の機能が初めて使用された場合だけ。
- パスフレーズ認証は常に必要。
- セットアップにおいて内蔵指紋読み取り装置が検出された場合は、指紋認証が必要。
- CSS をセットアップしたユーザーの UVM パスフレーズは、CSS *管理者パスワード* でもあります。 UVM パスフレーズを変更すると、CSS 管理者パスワードも変更されます。 CSS 管理者パスフレーズの有効期限は決して切れません。

標準構成のコンポーネントに関する制限事項

Client Security Software の機能のうち拡張構成後に有効になるものの中には、標準構成が選択された場合には無効になるものがあります。 CSS の標準構成でそれらの

機能を使用することはできません。それらの機能を有効にするには、構成を拡張構成に変換する必要があります。標準構成後の機能の差は、次のとおりです。

- **管理者ユーティリティー**

  次のアクションは、標準構成では実行できません。

  – ユーザーのリセット
  – ユーザーの削除
  – 「チップの設定」ボタンを使用して管理者パスワードを変更すること
  – 鍵構成機能

  ユーザーがこれらの操作のいずれかを実行しようとすると、CSS 拡張構成に変換するよう促されることになります。変換処理を実行すると、管理者の秘密鍵が暗号化解除され、管理者の鍵ペアがユーザーによって指定された場所に移されます。

- **管理者コンソール**

  標準構成の場合、使用法に関し、拡張構成の場合と比べ、以下の違いがあります。

  – アーカイブ・ディレクトリー、秘密鍵の場所、および公開鍵の場所のデータはハードコーディングされ、変更はできません。アーカイブの編集はローカル・コンピューター上でのみ可能です。
  – クレデンシャル・ローミングを構成するオプションは、標準構成では使用できません。標準構成を選択した場合、クレデンシャル・ローミングをセットアップするには、まず標準構成を通常の構成に変換する必要があります。
  – UVM パスフレーズ・バイパス操作を CSS 管理者に対して実行することはできません。

- **ユーザー構成ユーティリティー**

  標準構成の場合、使用法に関し、拡張構成の場合と比べ、以下の違いがあります。

  – CSS をセットアップしたユーザーの UVM パスフレーズは、管理者パスワードでもあります。 UVM パスフレーズを変更すると、管理者パスワードも変更されます。
  – CSS 管理者ユーザーをリセットすることはできません。
  – クレデンシャル・ローミングを構成するオプションは、標準構成では使用できません。

標準構成から拡張構成への変換

Client Security Software の標準構成を拡張構成に変換するには、以下のようにします。

1. 管理者ユーティリティーを起動します。
2. CSS 管理者パスワードを入力します。
3. **「鍵の構成」**ボタンをクリックします。
4. **「OK」**をクリックして先へ進みます。

5. 暗号化解除した管理者鍵ペアの保管先を入力します。暗号化解除した鍵ペアは、ローカル・ハード・ディスク・ドライブには保管しないでください。これで変換処理は完了です。
6. アーカイブ位置を変更します。アーカイブは、ローカル・ハード・ディスク・ドライブには保管しないでください。

Client Security Software を拡張構成に変換したなら、それ以降にそれを標準構成に戻すことはできません。

拡張構成

IBM Client Security Software の*拡張構成* では、Client Security のうち以下に示す*付加的な* 機能が構成されます。

- **UVM ログオン保護**
- **鍵保管場所選択**
- **アプリケーション・サポート:** Entrust、FFE (ファイルとフォルダーの暗号化)、Lotus Notes
- **セキュリティ・レベルの設定**

IBM Client Security セットアップ・ウィザードの使用

IBM Client Security セットアップ・ウィザードは、Client Security Software をインストールし、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のに役立つインターフェースを提供します。 IBM Client Security Software セットアップ・ウィザードを使用して以下の手順を実行することにより、IBM クライアントでセキュリティー・ポリシーを設定するのに必要な作業を実行してください。

IBM Client Security セットアップ・ウィザードによって実行される一般的なステップは、以下のとおりです。実際のステップは、選択する構成オプションによって異なります。

- **セキュリティー管理者パスワードの設定**

  セキュリティー管理者パスワード (このマニュアルでは「管理者パスワード」と呼ぶ) は、IBM Client Security の管理者ユーティリティーへのアクセスを制御するために使用します。このユーティリティーは、このコンピューターのセキュリティー設定を変更するために使用します。

- **管理者セキュリティー鍵の作成**

  鍵は、コンピューター・ファイルに格納されている一連のディジタル鍵です。これらの鍵ファイルは、管理者鍵、管理者鍵ペア、またはアーカイブ鍵ペアとも呼ばれます。これらの重要な鍵は、取り外し可能なディスクまたはドライブに保管するようにお勧めします。管理者ユーティリティーでセキュリティー・ポリシーを変更する場合は、管理者鍵によってポリシーの変更が許可されていることを証明するように求めるプロンプトが表示されます。

  コンピューターのシステム・ボードまたはハード・ディスクを置換する必要がある場合のために、バックアップ・セキュリティー情報も保管されます。このバックアップ情報は、ローカル・システム以外の場所に保管してください。

- **IBM Client Security でのアプリケーションの保護**

  IBM Client Security で保護するアプリケーションを選択します。他の必要なアプリケーションをインストールしていない場合は、一部のオプションが使用できない場合があります。
- **ユーザーの許可設定**

  コンピューターにアクセスするには、ユーザーが UVM に登録されている必要があります。ユーザーを登録するときに、そのユーザーのパスフレーズを指定します。登録されていないユーザーはコンピューターを使用することはできません。
- **システム・セキュリティー・レベルの選択**

  コンピューターのセキュリティー・レベルを選択することによって、基本的なセキュリティー・ポリシーを簡単かつ直ちに設定することができます。後から IBM Client Security 管理者ユーティリティーでカスタム・セキュリティー・ポリシーを定義できます。

セットアップ・ウィザードによる標準構成

IBM Client Security セットアップ・ウィザードを使用して標準的な構成作業を実行するには、次のようにします。

1. **「スタート」→「プログラム」→「Access IBM」→「IBM Client Security Software」→「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」**をクリックします。

   「ようこそ IBM Client Security セットアップ・ウィザードへ」画面で、構成オプションを選択できます。
2. 「標準構成 (推奨)」構成のラジオ・ボタンを選択して、**「次へ」**を選択します。

   これを選択した場合、IBM Password Manager が有効になり、入力の必要なパラメーターはごくわずかです。標準構成を選択した場合は、CSS によりバックアップ情報とセキュリティー鍵がハード・ディスクに保管されます。セキュリティー・ユーザーとして初心者の場合は、標準構成オプションを使用してください。これはデフォルトの設定です。

   「パスフレーズの入力」画面が表示されます。
3. 以下の作業を実行します。
   a. 「UVM パスフレーズ」フィールドにパスフレーズを入力します。必要なら、**「UVM パスフレーズのルール」**ボタンをクリックして、有効なパスフレーズについてのヘルプを表示してください。

      注: 初期インストール時または IBM エンベデッド・セキュリティー・サブシステムのクリアの後は、「パスフレーズの確認入力」フィールドでパスフレーズを確認する必要があります。また、スーパーバイザー・パスワードを指定する必要がある場合もあります (適用できる場合)。
   b. 「パスフレーズ ヒント」フィールドに語句を入力します。
   c. **「次へ」**をクリックします。

コンピューター上に指紋読取装置が検出されているなら、「指紋の登録」画面が表示されます。**「はい、今指紋を登録します」**チェック・ボックスは、デフォルトでチェックされた状態になっています。

4. 以下のいずれかを実行します。
   - **「はい、今指紋を登録します」**チェック・ボックスのチェックをはずし、**「次へ」**をクリックします。
   - **「次へ」**をクリックし、画面上に表示される指示に従って指紋の登録作業を開始します。

   「許可ユーザーの追加」画面が表示されます。
5. 以下のいずれかを実行します。
   - **「他のユーザーを UVM に登録する (オプション)」**チェック・ボックスをチェックしてから、**「次へ」**をクリックします。
   - **「スキップ」**をクリックして、この作業をスキップします。

   「セキュリティーの設定値と機能の一覧」画面が表示されます。
6. **「終了」**をクリックすると、選択したセキュリティー設定値が有効になります。その処理には数分の時間がかかることがあります。コンピューターが IBM Client Security によって保護されるようになっ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。

セットアップ・ウィザードによる拡張構成

IBM Client Security セットアップ・ウィザードを使用して標準的な構成作業を実行するには、次のようにします。

1. **「スタート」→「プログラム」→「Access IBM」→「IBM Client Security Software」→「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」**をクリックします。

   「ようこそ IBM クライアント・セキュリティー・セットアップ・ウィザードへ」画面で、構成オプションを選択できます。
2. **「拡張構成」**ラジオ・ボタンを選択して、**「次へ」**をクリックします。

   これを選択した場合は、鍵の保管場所やセキュリティー・レベルなどの構成情報を自分で指定することが必要になります。また、CSS ログオン・プロテクション、Lotus Notes 保護、および IBM Password Manager を有効にすることが可能になります。

   「管理者パスワードを設定する」の画面が表示されます。
3. 「管理者パスワードを入力してください」フィールドに管理者パスワードを入力し、「**次へ**」をクリックします。

   注: 初期インストール時または IBM エンベデッド・セキュリティー・サブシステムのクリアの後は、「管理者パスワードをもう一度入力してください」

フィールドでセキュリティー管理者パスワードを確認する必要があります。また、スーパーバイザー・パスワードを指定する必要がある場合もあります (適用できる場合)。

「鍵を作成する」の画面が表示されます。

4. 以下のいずれかを実行します。
   - **新しい鍵を作成する**

     新しい鍵を作成するには、次の手順を行います。

     a. 「**新しい鍵を作成する**」ラジオ・ボタンをクリックする。
     b. パス名をフィールドに入力するか「**参照**」をクリックして適切なフォルダを選択することによって、鍵の保管先を指定します。
     c. 保護を強化するために鍵を分割する場合は、**「安全性の向上のためにアーカイブ鍵を分割する (5 分割まで)」**チェック・ボックスをクリックしてボックスにチェックマークを表示させ、矢印を使用して**「分割する数」**スクロール・ボックスで必要な番号を選択します。

   - **存在する鍵を使用する**

     既存の鍵を使用するには、次の手順を行います。

     a. 「**存在する鍵を使用する**」ラジオ・ボタンをクリックします。
     b. パス名をフィールドに入力するか、あるいは「**参照**」をクリックして該当するフォルダを選択することによって、公開鍵のロケーションを指定します。
     c. 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。
5. 提示されたフィールドにパス名を入力するか、あるいは「**参照**」をクリックして該当するフォルダーを選択することによって、セキュリティー情報のバックアップ・コピーの保管先となる鍵アーカイブ位置を指定します。
6. 「**次へ**」をクリックします。

「IBM エンベデッド・セキュリティー・サブシステムでアプリケーションを保護する」の画面が表示されます。

7. 適切なチェック・ボックスを選択してチェックマークを付け、「**次へ**」をクリックすると、IBM Client Security の保護が使用可能になります。使用可能な Client Security 選択項目は次のとおりです。
   - **ログオン・プロテクションを有効にする**

     通常の Windows ログオンをクライアント・セキュリティーの UVM ログオンで置き換える場合は、このボックスを選択します。これによりご使用のシステムのセキュリティーが向上し、IBM エンベデッド・セキュリティー・サブシステムおよびオプションの装置 (指紋読取装置またはスマート・カードなど) で認証を行った後でしかログオンできなくなります。

   - **IBM File and Folder Encryption を有効にする**

     ハードディスクのファイルを IBM エンベデッド・セキュリティー・サブシステムで保護する場合は、このボックスを選択します。 (IBM File and Folder Encryption ユーティリティーをダウンロードする必要があります。)

- **IBM Password Manager のサポートを有効にする**

  IBM Password Manager を使用して Web サイトのログオンおよびアプリケーションに対するパスワードを簡単かつ安全に格納したい場合は、このボックスを選択します。

- **Lotus Notes ログインを UVM ログオンに置き換える**

  IBM エンベデッド・セキュリティー・サブシステムによって Lotus Notes ユーザーを認証させる場合は、このボックスを選択します。

- **Entrust のサポートを有効にする**

  Entrust セキュリティー・ソフトウェア製品との統合を使用可能にする場合は、このボックスを選択します。

- **Microsoft Internet Explorer を保護する**

  この保護により、Microsoft Internet Explorer による電子メール通信と Web ブラウズを機密保護することが可能になります (別途、ディジタル証明書の取得が必要です)。 Microsoft Internet Explorer のサポートはデフォルトで使用可能になっています。

適切なチェック・ボックスを選択すると、「ユーザーを登録する」画面が表示されます。

8. 次のいずれかの手順を行うことによって、ユーザーの登録を行います。
   - ユーザーが IBM Client Security 機能を実行するのを許可するには、以下のことを行います。
     a. 「登録されていないユーザー」領域でユーザーを選択します。
     b. 「**ユーザーの登録**」をクリックします。
     c. 表示されているフィールドに IBM Client Security のパスフレーズを入力して確認し、「**次へ**」をクリックします。

        「UVM のパスフレーズの有効期限」画面が表示されます。
     d. ユーザーのパスフレーズ有効期限を設定して、「**終了**」をクリックします。
     e. **「次へ」**をクリックします。
   - 一度登録したユーザーに IBM Client Security 機能の実行を許可しない場合には、次のように行います。
     a. 「登録済みのユーザー」領域でユーザーを選択します。
     b. 「**ユーザー登録の取消**」をクリックします。

        「登録をやめますか?」というメッセージが表示されます。
     c. 「**はい**」をクリックします。
     d. **「次へ」**をクリックします。

   「コンピューターのセキュリティー・レベルを選ぶ」の画面が表示されます。
9. 適切なチェック・ボックスをクリックすることによって、ユーザーを確認する方法を選択します。複数の確認方法を選択できます。

- 指紋読取装置とスマート・カードの読取装置に関して IBM Client Security セットアップ・ウィザードを実行する前に、それらのデバイス・ドライバーをインストールして、セットアップ・ウィザードで認識されるようにする必要があります。
- スライド・セレクターを所定のセキュリティー・レベルまでドラッグし、「**次へ**」をクリックすることによって、コンピューターのセキュリティー・レベルを選択します。

  注: 後から管理者ユーティリティーのポリシーの編集を使用して、ウィザードでの設定内容を変更し、カスタム・セキュリティー・ポリシーを定義することができます。

「セットアップ完了 - セキュリティー設定値の確認」画面が表示されます。

10. セキュリティーの設定を確認し、次のどちらか 1 つの操作を行います。
    - 設定を受け入れるには、「**終了**」をクリックします。
    - 設定を変更するには、「**戻る**」をクリックし、適切な変更を行ってからこの画面に戻り、「**終了**」をクリックします。

    IBM Client Security Software は、IBM エンベデッド・セキュリティー・サブシステムで設定を構成します。コンピューターが IBM Client Security によって保護されるようになったことを確認するメッセージが表示されます。
11. **「OK」**をクリックします。

IBM セキュリティー・サブシステムの有効化

IBM セキュリティー・サブシステムが有効でなければ、 Client Security Software は使用できません。セキュリティー・サブシステムが有効になっていない場合は、管理者ユーティリティーを使用して有効にすることができます。

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・サブシステムを有効にするには、次の手順を実行します。

1. **「スタート」→「設定」→「コントロール パネル」→「IBM エンベデッド・セキュリティー・サブシステム」**をクリックします。

   IBM セキュリティー・サブシステムが無効になっていることを示すメッセージが画面に表示され、セキュリティー・サブシステムをすぐに有効にするかどうかを確認するメッセージが表示されます。
2. 「**はい**」をクリックします。

   スーパーバイザー・パスワードまたは BIOS 管理者パスワードが使用可能になっている場合は BIOS セットアップ・ユーティリティーでスーパーバイザー・パスワードを使用不可にしてから続行するように求めるメッセージが表示されます。
3. 以下のいずれかを実行します。
   - スーパーバイザー・パスワードが使用可能になっている場合は、「**キャンセル**」をクリックしてそのスーパーバイザー・パスワードを使用不可にしてからこの手順を実行します。
   - スーパーバイザー・パスワードが使用不可の場合は、「**OK**」をクリックして続行します。

4. 開いているアプリケーションをすべてクローズし、「**OK**」をクリックしてコンピューターを再始動します。
5. コンピューターの再起動後、「**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**」をクリックして、管理者ユーティリティーを開きます。

   IBM セキュリティー・サブシステムが構成されていないか、クリアされていることを示すメッセージが表示されます。この時点では新規パスワードが必要です。
6. 適切なフィールドに新しい管理者パスワードを入力して確認し、「**OK**」をクリックします。

   操作が完了し、管理者ユーティリティーのメイン画面が表示されます。

Client Security Software のバージョンのアップグレード

クライアントに以前のバージョンの Client Security がインストールされている場合は、Client Security の新しい機能を利用するためには、ソフトウェアを最新のバージョンに更新する必要があります。

重要: IBM Client Security Software バージョン 4.0x 以前のバージョンがインストールされているシステムでは、その IBM Client Security Software をアンインストールし必ずチップをクリアしてから IBM Client Security Software の最新のバージョンをインストールしてください。そのようにしないと、インストールに失敗するか、ソフトウェアからの応答がなくなる恐れがあります。

新しいセキュリティー・データを使用したアップグレード

Client Security Software を完全に削除してやり直す場合は、次の手順を行います。

1. コントロール・パネルの「アプリケーションの追加と削除」を使用し、旧バージョンの Client Security Software をアンインストールします。
2. システムをリブートします。
3. BIOS セットアップ・ユーティリティーで IBM エンベデッド・セキュリティー・チップをクリアします。
4. システムをリブートします。
5. Client Security Software の最新バージョンをインストールし、IBM Client Security Software セットアップ・ウィザードを使用してそれを構成します。

既存のセキュリティー・データを使用した CSS 5.0 以降からのアップグレード

既存のセキュリティー・データを使用して Client Security Software バージョン 5.0 以降からアップグレードする場合は、次のようにします。

1. 次のステップに従い、アーカイブを更新します。
   a. **「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。
   b. 「パスワードとアーカイブの更新」タブを選択し、「**アーカイブの更新**」ボタンをクリックし、バックアップ情報を更新します。

アーカイブ・ディレクトリーを確認します。

c. ユーザー構成ユーティリティーを終了します。

2. 次のステップに従い、既存のバージョンの Client Security Software をアップグレードします。

   a. Windows のデスクトップで、「**スタート**」→「**ファイル名を指定して実行**」の順にクリックします。

   b. 「ファイル名を指定して実行」フィールドに、ダウンロードした最新の IBM Client Security Software のファイル名を入力します。

   c. 「**アップグレード**」を選択します。

   d. システムをリブートします。

Client Security Software のアンインストール

必ず Client Security の機能を拡張する、IBM File and Folder Encryption (FFE) ユーティリティーをアンインストールしてから、IBM Client Security Software をアンインストールしてください。 Client Security Software をアンインストールするには、管理者権限を持つユーザーがログオンする必要があります。

注: 必ずすべての FFE、およびすべての UVM 認識のセンサー・ソフトウェアをアンインストールしてから、IBM Client Security Software をアンインストールしてください。Client Security Software をアンインストールするには、管理者パスワードが必要です。

注: IBM Client Security Software バージョン 5.4 より古いバージョンでは、Password Manager は、別にインストールされていました。もし「アプリケーションの追加と削除」に IBM Password Manager が表示されている場合は、IBM Client Security Software を削除する前に、Password Manager を削除してください。

Client Security Software をアンインストールするには、次の手順を実行します。

1. すべての Windows プログラムをクローズします。
2. Windows のデスクトップで、「**スタート**」→「**設定**」→「**コントロール・パネル**」をクリックします。
3. 「**アプリケーションの追加と削除**」アイコンをクリックします。
4. ソフトウェアのリストで、「**IBM Client Security Software**」を選択します。
5. 「**変更と削除**」をクリックします。
6. 「**削除**」ラジオ・ボタンを選択します。
7. 「**次へ**」をクリックして、ソフトウェアをアンインストールします。
8. 確認ウィンドウで「**OK**」をクリックします。
9. 表示されるインターフェースに管理者パスワードを入力して、「**OK**」をクリックします。
10. 以下のいずれかを実行します。
    - 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 Netscape にインストールした場合は、IBM エンベデッド・セキュリティー・

サブシステム PKCS#11 モジュールを使用不可にするプロセスを開始するように求めるメッセージが表示されます。「**はい**」をクリックして処理を続けます。

一連の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 PKCS#11 モジュールが削除されるまで、各メッセージで「**OK**」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 PKCS#11 モジュールを Netscape にインストールしていない場合は、Client Security Software と一緒にインストールされた共用 .DLL ファイルを削除したいかどうかをたずねるメッセージが表示されます。

  これらのファイルをアンインストールするには「**はい**」、ファイルをそのままにしておくには「**いいえ**」をクリックします。これらのファイルをインストールしたままにしても、コンピューターの通常の動作には影響はありません。

「アーカイブからこのコンピューターの情報を削除しますか?」と表示されます。「**いいえ**」を選択した場合は、新しいバージョンの IBM Client Security Software を再度インストールするときに情報をアーカイブから復元できます。

11. ソフトウェアが削除された後、「**終了**」をクリックします。

    Client Security Software をアンインストールした後、コンピューターを再起動する必要があります。

Client Security Software をアンインストールすると、インストール済みの Client Security Software のコンポーネント、すべてのユーザー鍵、ディジタル証明書、登録済みの指紋、および格納されているパスワードが削除されます。

輸出規制

IBM Client Security Software には、北米内および国際的にダウンロードできる暗号化コードが入っています。米国の Web サイトからの暗号化ソフトウェアのダウンロードが禁止されている国では、IBM Client Security Software をダウンロードできません。 IBM Client Security Software に関する輸出規制については 37 ページの『付録 A. Client Security Software に関する米国の輸出規制』を参照してください。

第 5 章 トラブルシューティング

以下のセクションでは、Client Security Software をインストールまたは構成する際に発生する可能性のある問題の防止、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

ユーザーの登録

クライアント・ユーザー情報を保護するには、クライアントに IBM Client Security Software をインストールして、ソフトウェアを使用できるようにユーザーを登録する**必要があります**。使いやすいセットアップ・ウィザードが用意されており、このウィザードによってインストール・プロセスを実行できます。

重要: セットアップ時に、少なくとも 1 人のクライアント・ユーザーが UVM の使用を許可され**なければなりません**。 Client Security Software の初期設定の際にユーザーが登録されないと、セキュリティー設定は適用**されず**、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・ウィザードを完了した場合、コンピューターを終了してから再始動し、 Windows の「スタート」メニューから Client Security セットアップ・ウィザードを実行して、 Windows ユーザーが UVM を使用できるように登録してください。このようにすると、 IBM Client Security Software によってセキュリティー設定が適用され、ユーザーの重要な情報が保護されるようになります。

BIOS 管理者パスワードの設定 (ThinkCentre)

管理者は構成/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・サブシステムの有効化または無効化
- 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、サブシステム上に格納されている暗号鍵および証明書はすべて消失します。

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. 「**System Security**」を選択します。
4. 「**Administrator Password**」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. 「**Change Administrator password**」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・サブシステムの有効化または無効化
- 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ら、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. 「**Password**」を選択します。
4. 「**Supervisor Password**」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. 「**Continue**」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. 「**Start setup utility**」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、**「Security」**を選択します。
5. 「**Password**」を選択します。
6. 「**Supervisor Password**」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. 「**Continue**」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。

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、チップ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、サブシステム上に格納されている暗号鍵および証明書はすべて消失します。

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ら、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. 「**Security**」を選択します。

4. **「IBM TCPA Security Feature」**を選択して Enter キーを押します。
5. 「**はい**」を選択します。
6. Enter を押して、選択を確定します。
7. F10 を押して変更内容を保存し、セットアップ・ユーティリティーを終了します。
8. **「Yes」**を選択して、Enter キーを押します。コンピューターは再始動します。

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、サブシステム上に格納されている暗号鍵および証明書はすべて消失します。

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ら、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. 「**Security**」を選択します。
4. **「IBM Security Chip」**を選択して、Enter キーを押します。
5. Enter キーを押し、**「Disabled」**を選択します。
6. Enter を押して、選択を確定します。
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存し、セットアップ・ユーティリティーを終了します。
9. **「Yes」**を選択して、Enter キーを押します。コンピューターは再始動します。

CSS バージョン 5.4 の既知の問題または制限

以下の情報は、Client Security Software バージョン 5.4 をインストールまたは構成する際に役立ちます。

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削除して再インストールする場合、Client Security Software で指紋サポートを可能にするためには、必要なレジストリー項目を手動で追加する必要があります。必要な項目の入ったレジストリー・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、レジストリー項目をレジストリーにマージできます。プロンプトが出されたら、「はい」をクリックし

て、この操作を確定します。 Client Security Software が変更を認識して、指紋サポートを有効にするために、システムをリブートする必要があります。

注: これらのレジストリー項目を追加するために、対象システムで管理者特権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 (およびそれ以前) は、ThinkPad システムで BIOS スーパーバイザー・パスフレーズ機能をサポートしない場合があります。 BIOS スーパーバイザー・パスフレーズを有効にするには、 BIOS セットアップからセキュリティー・サブシステムの使用可能および使用不可の設定を行う必要があります。

スマート・カードの制限

スマート・カードの登録

スマート・カードの使用に関して認証を受ける前に、そのカードを UVM に登録する必要があります。 1 つのカードが複数のユーザーに割り当てられている場合、最後にそのカードを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・アカウントにのみ登録してください。

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。
インストールの際に、プログラムをアップグレードまたは削除する必要があることを示すメッセージが表示されます。	以下のいずれかを実行します。 • バージョン 5.0 より前の Client Security Software がインストールされている場合、**「削除」**を選択して、それを削除します。次にコンピューターを再起動し、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てください。 • そうでない場合、**「アップグレード」**を選択してインストールを続けてください。

問題の兆候	可能な解決策
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**
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。
Client Security の管理者機能を実行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 の管理者機能を実行すると、エラー・メッセージが表示される。	Crypto 1 (非 TCG) システムでハードウェア鍵ペアを生成するためには、ThinkPad スーパーバイザー・パスワードまたは ThinkCentre BIOS 管理者パスワードが使用不可になっていなければなりません。 CSS インストール処理では、該当するパスワードが使用不可になるまで 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ことはできません。

付録 A. 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 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

管理者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管理者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を使用することにより管理者は、次のような管理者パスワード規則を確立できます。

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。管理者パスワードの有効期限は決して切れません。

- 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、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 を使用した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	それぞれ 4 秒
14-20	それぞれ 8 秒
21-27	それぞれ 16 秒
28-34	それぞれ 32 秒
35-41	それぞれ 64 秒 (1.07 分)
42-48	それぞれ 128 秒 (2.13 分)
49-55	それぞれ 256 秒 (4.27 分)
56-62	それぞれ 512 秒 (8.53 分)
63-69	それぞれ 1,024 秒 (17.07 分)

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

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・サブシステムを使用する認証は、いずれも同じポリシーに従っています。タイムアウトの最大値はありません。試行が失敗するごとに、上記の遅延が発生します。 118 回目の試行でも攻撃対応型の遅延は終了しません。むしろ、上記の方法で無限に続けられます。

Atmel TPM を使用した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・サブシステムを使用する認証は、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。

パスフレーズのリセット

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リセットすることができます。

パスフレーズのリモート側でのリセット

リモート側でパスワードをリセットするには、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リセットする際にお勧めできる方法です。

パスフレーズの手動リセット

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. 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。 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、IBM Corporation 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等はそれぞれ各社の商標です。

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