

 **IPGARD™**

Innovate | Protect | Gard

**IPGard Secure KVM**

**Administration and Security**

**Management Tool**

**設定ガイド**

V1.0

## 目次

1 管理機能の概要.....	4
2 システム要件 .....	4
3 システムセットアップ.....	5
4 管理操作の開始.....	6
5 ユーザー機能と設定 .....	6
5-1 ログイン.....	6
5-2 メニューの表示.....	7
5-3 登録済み CAC 機器の確認.....	7
5-4 CAC 機器の登録 .....	8
5-5 管理操作の終了.....	8
6 管理者機能.....	9
6-1 管理者ログイン.....	9
6-2 メニューの表示.....	9
6-3 ユーザー認証情報の変更 .....	10
6-4 管理者認証情報の変更.....	10
6-5 登録済み CAC 機器の確認.....	11
6-6 CAC ポートの設定（管理者） .....	11

6-7 イベントログの抽出 .....	12
6-8 初期化 .....	13
6-9 管理操作の終了.....	14

## 1 管理機能の概要

IPGARD 製「Administration and Security Management Tool」(以下、管理ツール)は、認証されたユーザーおよびシステム管理者が、IPGARD 製セキュア KVM スイッチに対して以下の管理操作を実行できるよう設計されています。

メニュー機能	管理者	ユーザー
ログイン	○	○
ユーザーアクセス認証情報の変更	○	-
管理者アクセス認証情報の変更	○	-
登録済み CAC デバイスの表示*	○	○
新規 CAC デバイスの登録*	○	○
監査ログの出力 (ダンプ)	○	-
工場出荷時設定へのリセット	○	-

※ ユーザー／管理者の機能権限

認証済みのユーザーおよび管理者は、いずれも本機が準拠する「Peripheral Sharing Switch (PSS) 用プロテクションプロファイル (PP) バージョン 3.0」においては「管理者」として扱われます。

本書では、上記の各機能を実行するために必要な情報について説明します。

## 2 システム要件

IPGARD 製セキュア KVM スイッチは、Windows や Linux などのオペレーティングシステムを搭載した一般的なパソコン、サーバー、またはシンクライアントと互換性があります。コンソールポートに接続可能な周辺機器については、以下の表をご参照ください。

※管理ツールは、Windows 環境でのみ動作します。対応 OS は Windows XP、7、8、10、11 です。

あわせて、.NET Framework バージョン 2.0 以降が必要です。

コンソールポート	対応デバイス
キーボード	有線接続のキーボードおよびテンキーに対応しています。 また、接続された機器が「HID キーボード」または「HID マウス」として PC に認識される必要があります。 ※内部に USB ハブ機能や複合デバイス機能を持つ機器には対応していません。 (※HID = Human Interface Device。標準的な入力機器として動作する USB デバイス)
ディスプレイ	セキュア KVM スイッチの DisplayPort 端子および HDMI 端子と物理的および論理的に互換性のあるインターフェースを使用する表示装置 (例: モニター、プロジェクター)
音声出力	アナログ接続のアクティブスピーカー、またはアナログヘッドホン

マウス/ポインティングデバイス	内部 USB ハブや複合デバイス機能を持たない有線マウスまたはトラックボール
CAC(Common Access Card)	ユーザー認証用の USB デバイス (USB ベースクラス 0Bh に分類されるスマートカードクラス) 例: スマートカードリーダー、PIV/CAC リーダー、トークン、生体認証リーダー

**セキュリティ上の理由により、以下の機器は本機ではサポートしていませんのでご注意ください。**

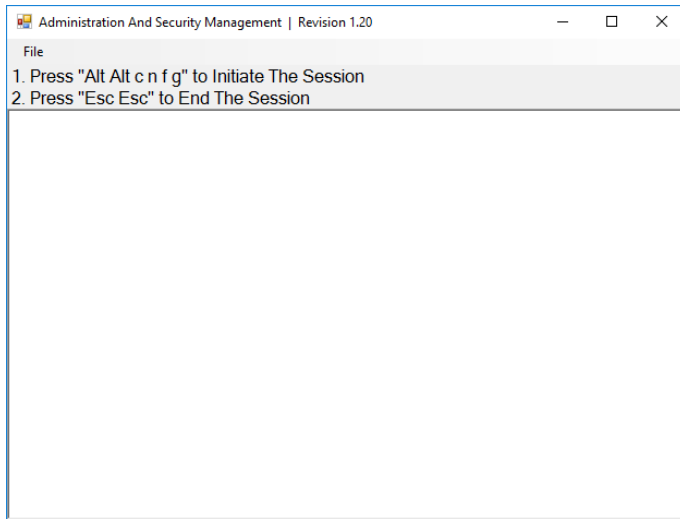
- ※ セキュア KVM スイッチはワイヤレスデバイスに対応していません。ワイヤレスキーボードやワイヤレスマウスは使用しないでください。
- ※ USB ハブ機能や USB ポートを内蔵したキーボードには対応していません。標準的な (HID) USB キーボードのみをご使用ください。
- ※ マイク音声入力やライン入力には対応していません。マイク付きヘッドセットやマイクは接続しないでください。
- ※ 外部電源を使用するユーザー認証デバイス (CAC) の接続は禁止されています。

### 3 システムセットアップ

※本操作には、セキュア KVM スイッチのポート 1 に接続したコンピューター 1 台のみで実行可能です。

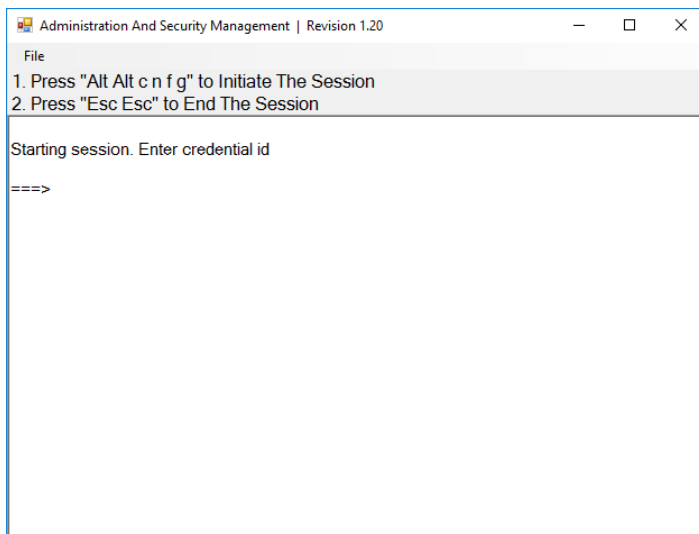
1. セキュア KVM スイッチおよびコンピューターの電源がオフになっている、または電源ケーブルが取り外されていることを確認してください。
2. USB Type-A to Type-B ケーブルを使用し、PC とセキュア KVM スイッチの K/M ポート 1 を接続してください。CAC ポートの設定が必要な場合は、もう 1 本の USB Type-A to Type-B ケーブルで PC とセキュア KVM スイッチの CAC ポートを接続してください。
3. USB キーボードおよび USB マウスを、セキュア KVM スイッチ背面の USB コンソールポートに接続してください。
4. PC とセキュア KVM スイッチのビデオ入力ポート 1 を、DisplayPort および HDMI ケーブルで接続してください。
5. モニターをセキュア KVM スイッチのコンソールビデオ出力ポートに DisplayPort および HDMI ケーブルで接続してください。
6. PC およびセキュア KVM スイッチの電源を入れてください。
7. 以下の URL より、管理ツール「Administration and Security Management Tool」を PC にダウンロードしてください：  
<http://ipgard.com/tools-software/>
8. ダウンロードした実行ファイルを起動してください。

下図は、管理ツール起動後に表示される画面です。



## 4 管理操作の開始

1. 接続されたキーボードを使用して、Alt → Alt → c → n → f → g の順にキーを押してください。
2. この操作を行うと、本機に接続されたマウスは一時的に操作できなくなります。
3. 下図は、コマンド入力後の開始画面です。

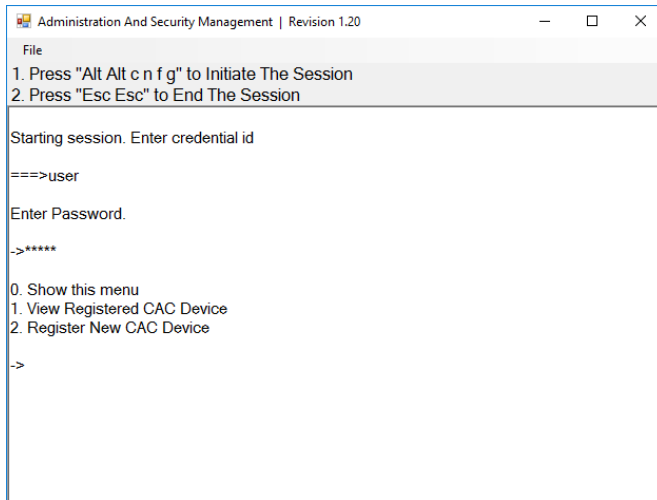


## 5 ユーザー機能と設定

### 5-1 ログイン

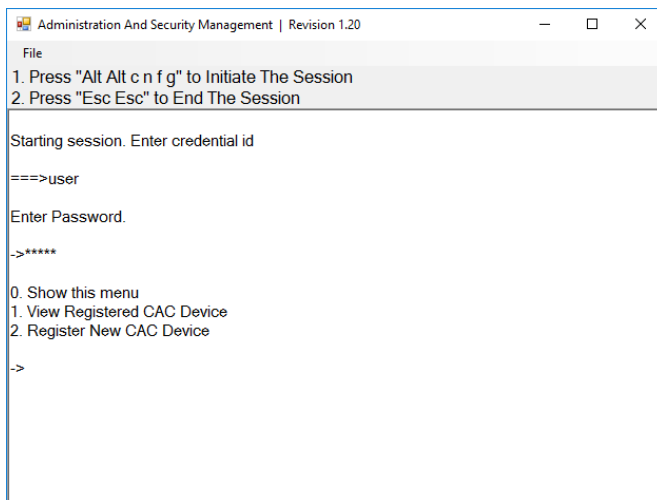
1. デフォルトのユーザー名 user を入力し、Enter キーを押します。
2. デフォルトのパスワード 12345 を入力し、Enter キーを押します。

3. 下図は、ログイン後に表示される画面です。



## 5-2 メニューの表示

1. メニュー画面で「0」を選択し、Enter キーを押します。
2. 下図のメニュー画面が表示されます。

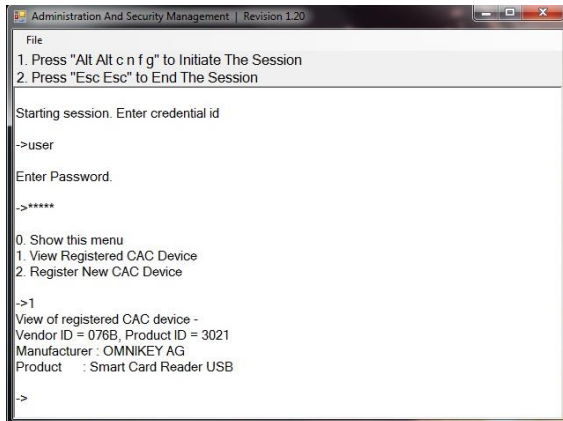


## 5-3 登録済み CAC 機器の確認

CAC (Common Access Card) ポートの設定はオプション機能です。特定の USB 周辺機器を本機に登録し、操作対象として使用できるようにします。同時に登録できる周辺機器は 1 台のみで、登録された機器のみがセキュア KVM スイッチと動作します。

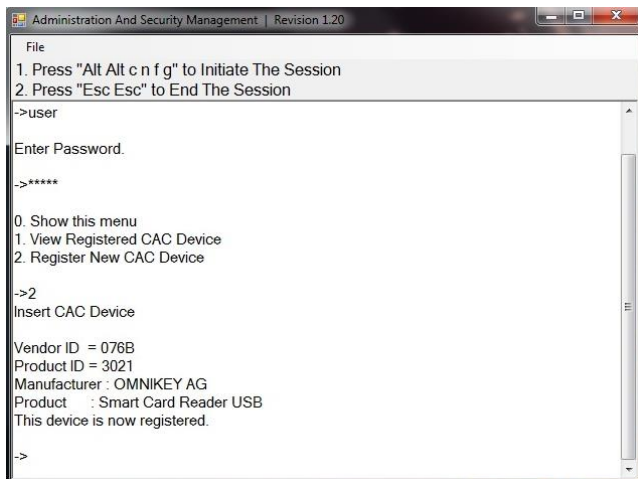
1. 画面のメニューから「1」を選択し、Enter キーを押します。

2. 下図は、登録したスマートカードリーダーの情報が表示されている画面です。



## 5-4 CAC 機器の登録

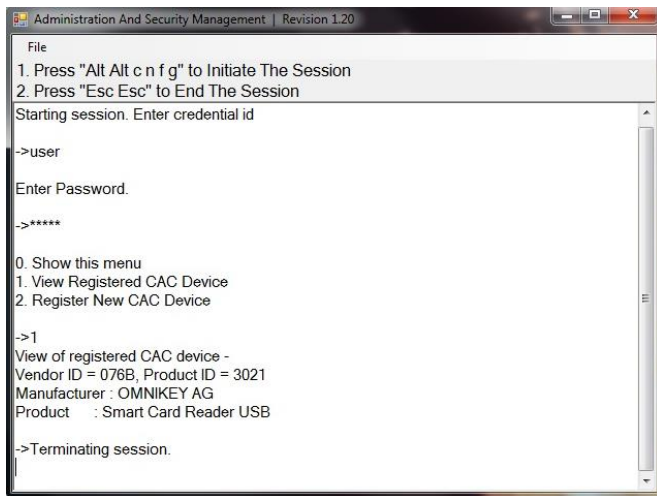
1. メニュー画面で「2」を選択し、Enter キーを押します。
2. 登録したい CAC 機器を、セキュア KVM スイッチのコンソール側にある CAC 用 USB ポートに接続します。機器の情報が読み取られるまでお待ちください。
3. 登録が完了すると、接続された周辺機器の情報が画面に表示され、3 回ブザー音を鳴らします。
4. 下図は、スマートカードリーダーを CAC ポートに登録した画面です。



## 5-5 管理操作の終了

キーボードで Esc → Esc の順に押します。

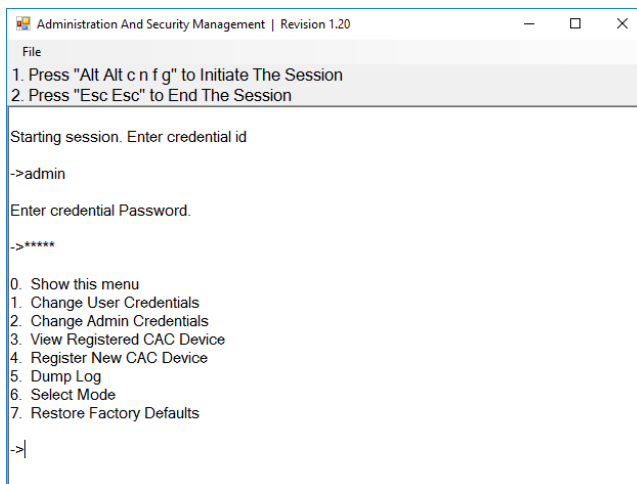
下図は、コマンド入力後に表示される画面です。



## 6 管理者機能

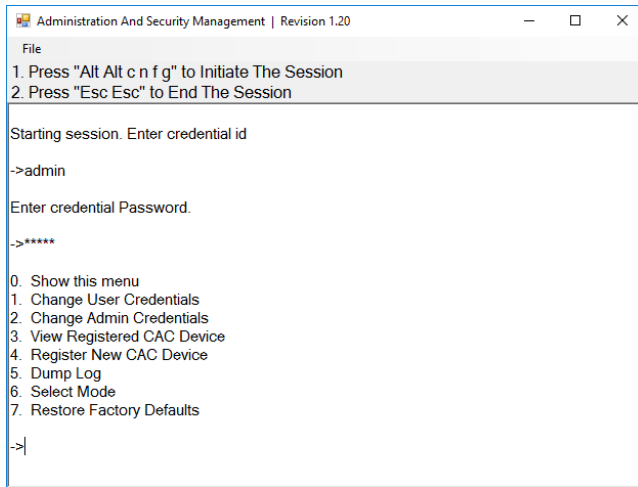
### 6-1 管理者ログイン

1. 項番 4 により、管理操作の開始を実施します。
2. デフォルトのユーザー名 admin を入力し、Enter キーを押します。
3. デフォルトのパスワード 12345 を入力し、Enter キーを押します。
4. 下図は、ログイン後に表示される画面です。



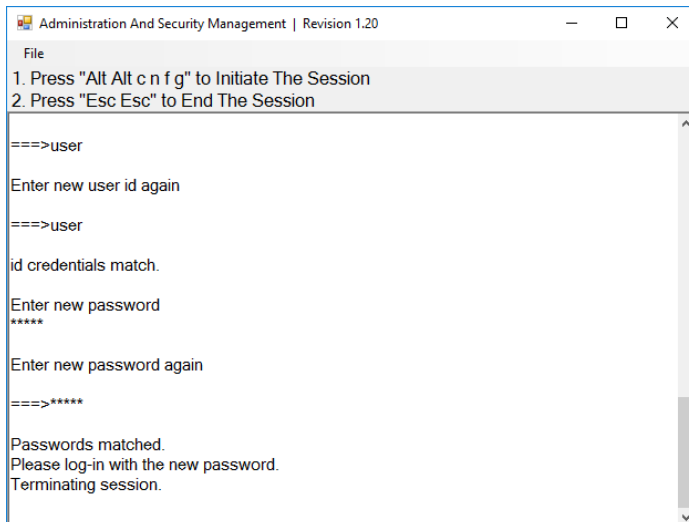
### 6-2 メニューの表示

1. メニュー画面で「0」を選択し、Enter キーを押します。
2. 下図のメニュー画面が表示されます。



### 6-3 ユーザー認証情報の変更

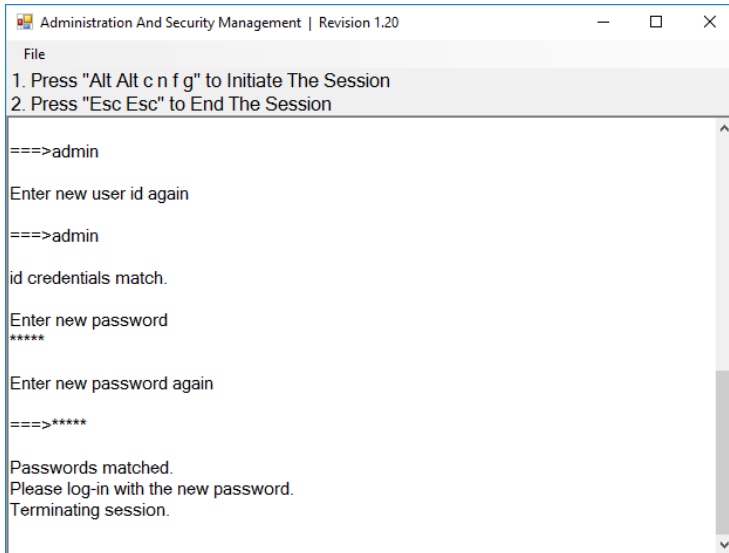
1. メニューから「1」を選択し、Enter キーを押します。
2. 新しいユーザーIDを入力し、Enter キーを押します。
3. 再度同じユーザーIDを入力し、Enter キーを押します。
4. 新しいユーザーパスワードを入力し、Enter キーを押します。
5. 再度同じパスワードを入力し、Enter キーを押します。
6. 下図は、変更操作中の画面です。



### 6-4 管理者認証情報の変更

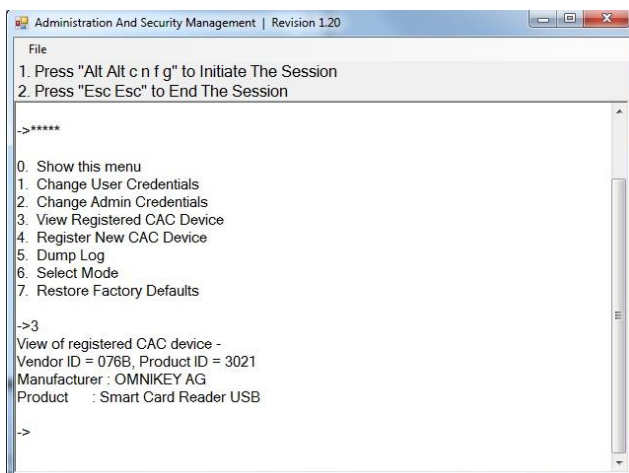
1. メニューから「2」を選択し、Enter キーを押します。
2. 新しい管理者 ID を入力し、Enter キーを押します。

3. 再度同じ ID を入力し、Enter キーを押します。
4. 新しいパスワードを入力し、Enter キーを押します。
5. 再度同じパスワードを入力し、Enter キーを押します。
6. 下図は、変更操作中の画面です。



## 6-5 登録済み CAC 機器の確認

1. 画面メニューから「3」を選択し、Enter キーを押します。
2. 下図は、登録したスマートカードリーダーの情報が表示されている画面です。

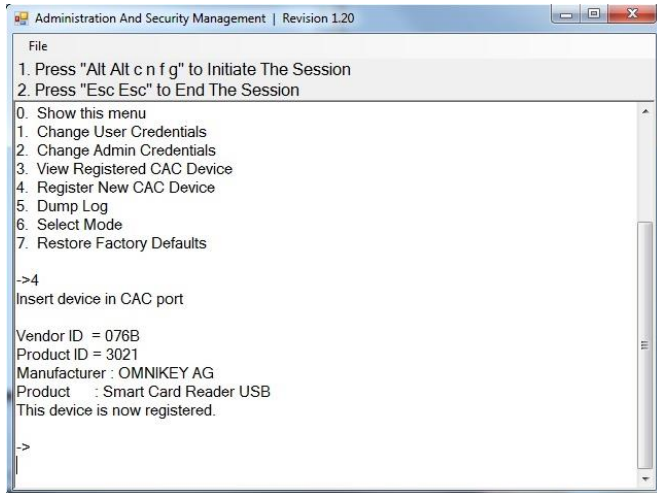


## 6-6 CAC ポートの設定 (管理者)

1. 画面のメニューから「4」を選択し、Enter キーを押します。
2. 登録したい CAC 機器を、セキュア KVM スイッチのコンソール側にある CAC 用 USB ポートに接続

します。機器の情報が読み取られるまでお待ちください。

3. 登録が完了すると、接続された周辺機器の情報が画面に表示され、3回ブザー音を鳴らします。
4. 下図は、スマートカードリーダーをCACポートに登録した画面です。



## 6-7 イベントログの抽出

イベントログとは、セキュアKVMスイッチ内に記録された操作履歴です。  
認証された管理者のみが確認できます。

1. メニューから「5」を選択し、Enterキーを押します。
2. 最新の10件のイベントが画面に表示されます。

```
=====LOG DATA=====
```

No	Event	Date & Time	Pass/Fail
9.	ALO	10/26/16 15:58:49	PASS
10.	P01	10/26/16 15:59:10	PASS
11.	PWU	10/26/16 15:59:11	PASS
12.	STS	10/26/16 15:59:11	PASS
13.	ALO	10/26/16 15:59:41	PASS
14.	AFD	10/26/16 15:59:47	PASS
15.	ALF	10/26/16 16:00:12	PASS
16.	PWU	10/26/16 16:00:26	PASS
17.	STS	10/26/16 16:00:26	PASS
18.	ALO	10/26/16 16:00:47	PASS

3. Enterキーを押すことで、過去の10件が順に表示されます（最大100件まで）。
4. ログのヘッダーには以下の情報が含まれます
  - ・製品型番

- ・シリアル番号
- ・改ざん防止スイッチの状態
- ・製造拠点
- ・製造日
- ・改ざん防止システムの有効化日
- ・現在の記録数

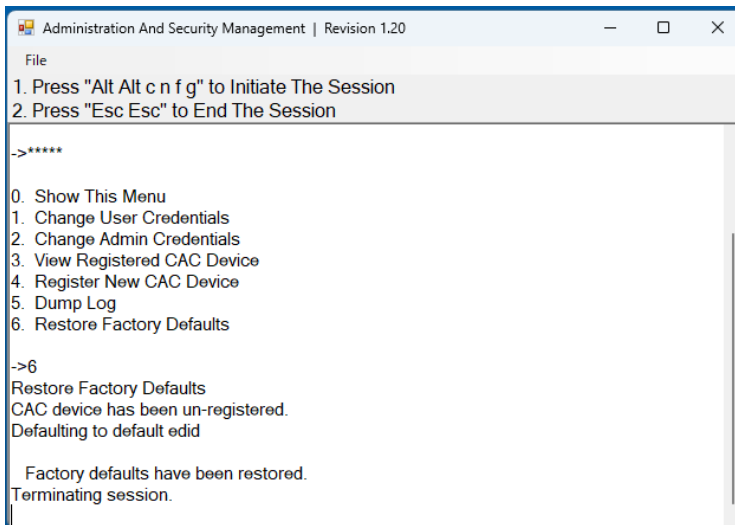
5. ログに記録されるイベントコードの一覧は以下のとおりです

No	コード	内容
1	ALO	管理者ログオン
2	ALF	管理者ログオフ
3	ARM	管理者権限の更新
4	CAC	CAC の構成
5	EDL	EDID 情報の取得
6	LGD	ログ出力
7	PWU	起動
8	PXX	モードの選択:01(KVM)、02(KM)、 03(カスタム)・・・アップロード済み
9	RCA	CAC デバイスが拒否されました
10	AFD	工場出荷時の設定に戻す
11	RKM	キーボードまたはマウスが拒否されました
12	STS	セルフテスト
13	TMP	機器の改ざんが検出されました。 メーカーのみ確認可能です。
14	ULO	ユーザーログオン
15	ULF	ユーザーログオフ

## 6-8 初期化

初期化を実行すると、自動的に電源がリセットされ、すべてのシステム設定が工場出荷状態に戻ります。  
登録された CAC 機器もすべて削除されます。

1. メニューから「6」を選択し、Enter キーを押します。
2. 自動的にセキュア KVM スイッチが初期化され、再起動します。



## 6-9 管理操作の終了

キーボードで Esc → Esc の順に押します。

下図は、コマンド入力後に表示される画面です。

