CHAPTER 7

# ハードウェア キーストアおよびセキュリティ ワールドの使用

この章では、ハードウェア キーストアおよびハードウェア キーストアを使用するnCipher セキュリティ ワールドの設定方法について説明します。内容は次のとおりです。



## 7.1 キーストアの設定

ACE XML アプライアンスは、ハードウェアによる鍵の保管に nCipher nForce デバイスを使用するように設定できます。nCipher ハードウェア キーストアおよびセキュリティ ワールド モジュールは、ライセンスに基づいて提供される機能です。nCipher ハードウェア キーストアを使用するためのライセンスをお持ちでない場合は、代理店のサポート担当者に問い合わせてください。

**注：** nCipher カードは、ハードウェア キーストアを提供する以外に、暗号化 / 復号化のアクセラレーションも行います。この機能をイネーブルにする手順については、セクション 9.1「SSL アクセラレーションの有効化」を参照してください。

nCipher のハードウェアベースの鍵保管機能を使用するには、新規または既存の nCipher セキュリティ ワールドに ACE XML アプライアンスを追加する必要があります。「セキュリティ ワールド」は、nCipher セキュリティ モジュールが提供する、ハードウェアベースの鍵を使用するように設定された一連のアプライアンスです。これらのアプライアンスは、セキュア鍵情報を共有するとともに、鍵に対応する一連の設定ファイルとスマート カードを共有します。セキュリティ ワールドを作成するときには、セットに含まれるスマート カードの数、セキュリティ ワールドによって保護する鍵を回復可能にするかどうかなどのオプションを設定できます。

ハードウェアベースの鍵を使用する予定の各 ACE XML アプライアンスは、前もって nCipher カードをインストールしておく必要があります。このスマートカードは、アプライアンスのポートに物理的に取り付られける nCipher カードリーダに搭載します。スマート カードは、セキュリティ ワールドの設定、既存セキュリティ ワールドへのアプライアンスの追加といった nCipher の管理作業に使用するだけなので、nCipher の管理作業が完了すれば、カード リーダを ACE XML アプライアンスに搭載しておく必要はありません。したがって、1 つのカード リーダを使用して複数の ACE XML アプライアンスの nCipher 機能を設定できます。

クラスタ環境でハードウェア キーストアを使用するには、クラスタの各 ACE XML アプライアンスでハードウェア キーストアとハードウェア キーストアを使用するセキュリティ ワールドを設定する必要があります。

初期化プロセスには、ハードウェア スイッチの設定を変更する作業が含まれるので、キーストア ハードウェアを収容する ACE XML アプライアンスに物理的にアクセスできなければなりません。さらに、キーストアを再設定する端末ベースの nCipher ソフトウェア ツールを実行するために、管理権限が必要です。

キーストアとセキュリティ ワールドにアクセスするにはスマート カードの適切な運用が重要なので、スマート カードのバックアップ セットを作成し、離れた場所に保管することを推奨します。この章の例では、4 枚のカードからなるセットを作成しますが、そのうちの 2 枚をセキュリティ ワールドの編集に使用し、残りの 2 枚のカードは安全な場所に保管しておきます。

このマニュアルでは、ACE XML アプライアンスでの nCipher モジュールの使用に関するあらゆる作業を順を追って詳しく説明します。ただし、nCipher システムの詳細については、nCipher 搭載 ACE XML アプライアンスに付属している nCipher のマニュアルを参照してください。

# 7.2 新しいセキュリティ ワールドの作成

ここでは、新しい nCipher セキュリティ ワールドを作成し、Gateway を追加する方法について説明します。その後、セクション 7.3「既存セキュリティ ワールドへの追加」の手順に従って、このセキュリティ ワールドに Gateway をさらに追加できます。

新しいセキュリティ ワールドを設定する場合は、設定するスマート カードの数（n）を指定し、さらにセキュリティ ワールドに新しいアプライアンスを追加するために、物理的に存在していなければならないカード数（k）を指定する必要があります。ここで紹介する手順では、n=4、k=2 とします。すなわち、セキュリティ ワールドには 4 つの管理者カードがあり、セキュリティ ワールドに新しいモジュールを追加するには、そのうち 2 つのカードが存在していなければなりません。

**注：** nCipher コマンドを実行する前に、各自の IT 環境に応じたセキュリティ ワールドの要件を決定し、該当するセキュリティ ワールド オプションの詳細を nCipher のマニュアルで確認します。

## 7.2.1 準備

セキュリティ ワールドを設定する前に、次の準備が必要です。

- Gateway とその nCipher カード リーダへの物理アクセス
- Gateway の root パスワード
- 番号を割り当て、ラベルを付けた 4 枚の nCipher スマート カード（ラベルの形式は自由です）

## 7.2.2 新しいセキュリティ ワールドの作成

次の手順で、4 枚の管理者カードからなる単純なセキュリティ ワールドを作成します。

1. ACE XML アプライアンス上で、`root` ユーザとして `bash` シェルにアクセスします（メイン メニューから **Advanced Options**、**Run bash** の順に選択）。

   詳細については、セクション 4.5「bash シェルのアクセス」を参照してください。

2. Gateway のシャーシで、nCipher モジュールのスイッチを「I」の位置に切り替えます（カードはアプライアンス モデルによって、前面パネルにある場合と背面パネルにある場合があります）。

この動作によって、「事前初期化」モードへの切り替えを nCipher モジュールに指定します。ただし、スイッチの位置が変わっただけで、それ以外の変化はありません。スイッチの位置を変えるだけでは、モジュールのモードは変更されません。新しいモードにするには、モジュールをリセットする必要があります。

**重要：** 次の手順で、nCipher キーストアを初期化します。初期化によって、保管されている秘密鍵と秘密鍵を保護するハードウェア パスワードが破棄されます。これらの鍵が重要な場合は、これまで使用していたキーストアを初期化する前に、鍵を回復する手段を確保する必要があります。**キーストアの再初期化によって、キーストアのハードウェア パスワードを消失した場合、または消去した場合、そのハードウェア パスワードを回復することはできません。**キーストアに保管されているハードウェア パスワードと鍵の取り扱いについては、最新の注意が必要です。

3. 次のいずれかの手順でモジュールをリセットします。
   - モード スイッチの横にあるリセット ボタンを押します。

     リセット ボタンはペン、ピン、またはペーパー クリップを使用して押してください。

   または

   - ACE XML アプライアンス上で端末セッションの `root` ユーザとして、次のコマンドを実行します。

     ```
     /opt/nfast/bin/nopclearfail -ca
     ```

     `-ca` オプションは、`nopclearfail` コマンドで使用可能なすべての nCipher モジュールを初期化することを指定します。対応する番号を指定して特定のモジュールを初期化する場合は、代わりに `-m` および `-c` オプションを使用します。次の例を参照してください。

     ```
     /opt/nfast/bin/nopclearfail -c -m 1
     ```

     `-c` オプションは、`-m` オプションで指定された nCipher モジュールを `nopclearfail` コマンドでクリアすることを指定します。この例のオプションは、コマンドで 1 番のモジュールをクリアすることを指定しています。

   リセットが正常に完了すると、次のようなメッセージが標準出力に出力されます。

   ```
   module 1, command , clearunit: OK
   ```

   さらに、nCipher モジュールのブルーの LED が 1 回だけ短く点滅します（nCipher の LED は、nCipher カード上の、3 種類（M、I、O）の切り替えができるスイッチの横にあります）。この点滅は、コマンドラインまたはハードウェア リセット スイッチを使用してモジュールのモードを変更した場合に発生します。

4. モジュールの現在の動作モードを確認するために、コマンドラインから次のコマンドを実行します。

   ```
   /opt/nfast/bin/enquiry
   ```

   `enquiry` コマンドを使用すると、使用可能な各 nCipher モジュールの状態の要約情報が表示されます。事前初期化モードに正常に切り替わった場合は、リセットした各モジュールの要約情報の `mode` フィールドに `pre-initialization` と表示されます。

5. アプライアンスの nCipher PCI カード インターフェイスに nCipher カード リーダを差し込みます。

   カード リーダの LED が点灯し、接続されていることを示します。カードが存在しない場合、またはカードを読み取れない場合、LED はレッドに点灯します。有効なスマート カードが存在している場合は、グリーンに点灯します。この時点ではまだ、リーダにカードを装着しません。

   旧バージョンの nCipher カード リーダと、カードを背面パネルに装着する ACE XML アプライアンス シャーシを併用する場合、プラグが短すぎてシャーシ背面パネルの被いから先へ届かない場合があります。nCipher カード リーダのプラグが短すぎてきちんと装着できない場合は、プラグにオスとメス両方のジェンダー変換器を取り付けて延長してください。

6. 新しいセキュリティ ワールドを作成するために、次のコマンドを実行します。

   ```
   /opt/nfast/bin/new-world -i
                  -Q cardsReqd/cardsInSet
                    -m moduleNum
   ```

   この場合

   - *cardsReqd* で、セキュリティ ワールドを編集するために物理的に存在しなければならないスマート カードの数を指定します。
   - *cardsInSet* で、セットに含まれるスマート カードの総数を指定します。
   - *moduleNum* で、初期化する nCipher モジュールを指定します。

   new-world コマンドでは、特定のインストレーションを記述する値を指定する必要があります。たとえば、4 枚のスマート カードを初期化し、セキュリティ ワールドを編集するためにはそのうちの 2 枚が存在していなければならないという場合は、*cardsReqd* 値として 2 を指定し、*cardsInSet* 値として 4 を指定します。次の例を参照してください。

   ```
   /opt/nfast/bin/new-world -i -Q 2/4 -m 1
   ```

   2 枚のスマート カードを初期化し、セキュリティ ワールドを編集するときに存在していなければならないカードが 1 枚だけの場合は、例の 2/4 の値を 1/2 に置き換えます。

   new-world ユーティリティは一度に 1 つずつ nCipher モジュールを初期化します。複数の nCipher モジュールを初期化する場合は、モジュールごとに new-world ユーティリティを実行し、-m オプションを使用して、new-world で初期化するモジュールを指定します。

   たとえば、前の例の場合、-m 1 引数は、new-world で 1 番のモジュールを初期化することを意味します。詳細については、nCipher 搭載 ACE XML アプライアンスに付属している nCipher のマニュアルを参照してください。

   しばらくすると、セットの最初のカードを挿入するようにシェル プロンプトで指示されます。

7. チップ側を上にして、カード リーダにカードを挿入し、カードが固定されるまで、静かにしっかり押し込みます。

   カード リーダのライトがグリーンに点灯し、カードを初期化する、またはカードのパスワードを設定するようにシェル プロンプトで指示されます。

8. **Module 1 slot contains an unrecognized card. Overwrite it?** というプロンプトが表示された場合は、**yes** を入力してから **Enter** キーを押します。

   カードに対応する新しいパスワードを設定するように要求されます。

   カードが認識できないことを示すプロンプトが表示されないかぎり、次のステップに進みます。

9. カードの新しいパスワードを入力し、プロンプトに従ってパスワードを確認します。2 度めに入力したパスワードが最初に入力したパスワードと完全に一致していなかった場合、パスワードを再度設定するように指示されます。

   **重要：** スマート カードのパスワードを紛失しないでください。セキュリティ ワールドに他のモジュールを追加する場合に、パスワードが必要になります。

   カードを取り外すように指示されます。

10. リーダからカードを取り出します。

11. プロンプトに従って前の手順を繰り返し、セットの残りのカードにパスワードを設定します。

    セットのすべてのカードにパスワードを設定すると、コマンドライン プロンプトに続いて、**security world created** というメッセージがコンソールに表示されます。

12. 新しいセキュリティ ワールドが作成されたことを確認するために、次のコマンドラインを実行します。

    ```
    ls -la /opt/nfast/kmdata/local
    ```

    シェルによって、指定したディレクトリの内容が表示されます。セキュリティ ワールドが正常に作成されている場合、ディレクトリにはワールド ファイルが 1 つと、1 つ以上の module_*X* ファイルが含まれています。次の出力例を参照してください。

    ```
    # ls -la /opt/nfast/kmdata/local
    total 32
    drwxrwsr-x 2 nfast nfast 4096 Jan 24 00:16 .
    drwxrwsr-x 8 nfast nfast 4096 Jan 23 23:09 ..
    -rw-r--r-- 1 root nfast 856 Jan 24 00:16
                        module_XXXX-XXXX-XXXX
    -rw-r--r-- 1 root nfast 16472 Jan 24 00:16
                        world
    ```

13. nCipher PCI カードからカード リーダを取り外します。

14. nCipher モジュールのスイッチを「O」の位置に切り替えます。

    この動作によって、「動作可能」モードへの切り替えを nCipher モジュールに指定します。

15. 次のいずれかの手順でモジュールをリセットします。

    - モード スイッチの横にあるリセット ボタンを押します。

      リセット ボタンはペン、ピン、またはペーパー クリップで押してください。

または

- ACE XML アプライアンス上で端末セッションの root ユーザとして、次のコマンドを実行します。

  ```
  /opt/nfast/bin/nopclearfail -ca
  ```

  リセットが正常に完了すると、次のようなメッセージが標準出力に出力されます。

  ```
  module 1, command , clearunit: OK
  ```

  -ca オプションは、nopclearfail コマンドで使用可能なすべての nCipher モジュールを初期化することを指定します。対応する番号を指定して特定のモジュールを初期化する場合は、代わりに -m および -c オプションを使用します。次の例を参照してください。

  ```
  /opt/nfast/bin/nopclearfail -c -m 1
  ```

  -c オプションは、-m オプションで指定された nCipher モジュールを nopclearfail コマンドでクリアすることを指定します。この例のオプションは、コマンドで 1 番のモジュールをクリアすることを指定しています。

nCipher モジュールをリセットして動作可能モードにすると、nCipher モジュールのブルーの LED が長い間隔で点滅します。

16. 次のコマンドラインを実行して、モジュールが動作可能になっていることを確認します。

    ```
    /opt/nfast/bin/enquiry
    ```

    enquiry コマンドを使用すると、使用可能な各 nCipher モジュールの状態の要約情報が表示されます。動作可能モードに正常に切り替わった場合は、リセットした各モジュールの要約情報の mode フィールドに operational と表示されます。

17. bash シェルを終了します。
18. **Advanced Options** メニューで **SSL Engine Configuration** を選択します。
19. **SSL Engine** 画面で **chil** を選択して、nCipher CHIL デバイスをイネーブルにします。

    **Advanced Options** メニューが表示されます。

20. **Return to Main Menu** を選択します。
21. **Main Menu** メニューで **Manage ACE XML Gateway Processes** を選択します。
22. **Restart All Services** を選択します。

シェルは現在指定されている構成でアプライアンスの再起動を試み、作業が完了すると、ステータス画面を表示します。

新しい構成でアプライアンスが正常に再起動すると、このセキュリティ ワールドで作成された秘密鍵を使用して、いつでも nCipher モジュールを使用できます。詳細については、ACE XML アプライアンスに付属している nCipher のマニュアルを参照してください。

# 7.3 既存セキュリティ ワールドへの追加

ここでは、既存の nCipher セキュリティ ワールドに Gateway を追加する方法について説明します。セキュリティ ワールドの概要およびセキュリティ ワールドの作成手順については、セクション 7.2「新しいセキュリティ ワールドの作成」を参照してください。さらに、ACE XML アプライアンスに付属している nCipher のマニュアルを参照してください。

## 7.3.1 準備

セキュリティ ワールドに別の ACE XML アプライアンスを追加する前に、次のものを準備します。

- セキュリティ ワールドが初期設定されている ACE XML アプライアンス。詳細については、セクション 7.2「新しいセキュリティ ワールドの作成」を参照してください。ここでは、このアプライアンスが始点システムであるものとして、手順を紹介します。
- セキュリティ ワールド ファイルのコピー。これは、セキュリティ ワールドの設定情報を定義する一連のファイルを含むディレクトリです。これらのファイルは通常、始点システムの `/opt/nfast/kmdata` ディレクトリにあります。
- 既存セキュリティ ワールドに含まれている管理者カード。セットとして何枚のカードが必要であるかは、作成時にセキュリティ ワールドをどのように設定したかによって決まります。
- セキュリティ ワールドに追加する ACE XML アプライアンスへの物理アクセス。ここでは、このアプライアンスを終点システムとして、手順を紹介します。
- 終点システムに取り付けた nCipher カード リーダ。
- 始点システムおよび終点システムの root パスワード。

## 7.3.2 セキュリティ ワールドへの ACE XML アプライアンスの追加

既存の nCipher セキュリティ ワールドに ACE XML アプライアンスを追加するには、次の手順で、始点アプライアンスからコピーしたファイルを使用して、終点システムの nCipher カードを初期化する必要があります。

1. 終点システムで、`root` ユーザとして `bash` シェルを実行します。
2. nCipher モジュールのスイッチを「I」の位置に切り替えます。
3. 次のいずれかの手順でモジュールをリセットします。
   - モード スイッチの横にあるリセット ボタンを押します。

     リセット ボタンはペン、ピン、またはペーパー クリップで押してください。

または

- 終点システムで次のコマンドラインを実行します。

  ```
  /opt/nfast/bin/nopclearfail -ca
  ```

  リセットが正常に完了すると、次のようなメッセージが標準出力に出力されます。

  ```
  module 1, command , clearunit: OK
  ```

  `-ca` オプションは、`nopclearfail` コマンドで使用可能なすべての nCipher モジュールを初期化することを指定します。対応する番号を指定して特定のモジュールを初期化する場合は、代わりに `-m` および `-c` オプションを使用します。次の例を参照してください。

  ```
  /opt/nfast/bin/nopclearfail -c -m 1
  ```

  `-c` オプションは、`-m` オプションで指定された nCipher モジュールを `nopclearfail` コマンドでクリアすることを指定します。この例のオプションは、コマンドで 1 番のモジュールをクリアすることを指定しています。

nCipher モジュールをリセットして事前初期化モードにすると、nCipher モジュールのブルーの LED が短く点滅します。

4. モジュールの現在の動作モードを確認するために、終点システム上で次のコマンドを実行します。

   ```
   /opt/nfast/bin/enquiry
   ```

   `enquiry` コマンドを使用すると、使用可能な各 nCipher モジュールの状態の要約情報が表示されます。事前初期化モードに正常に切り替わった場合は、リセットした各モジュールの要約情報の `mode` フィールドに `pre-initialization` と表示されます。

5. nCipher PCI カード インターフェイスに nCipher カード リーダを差し込みます。

   カード リーダの LED が点灯し、接続されていることを示します。カードが存在しない場合、またはカードを読み取れない場合、LED はレッドに点灯します。有効なスマート カードが存在している場合、LED はグリーンに点灯します。**この時点ではまだ、リーダにカードを装着しません。**

   旧バージョンの nCipher カード リーダと、カードを背面パネルに装着する ACE XML アプライアンス シャーシを併用する場合、プラグが短すぎて ACE XML アプライアンス シャーシ背面の被いから先へ届かない場合があります。nCipher カード リーダのプラグが短すぎてきちんと装着できない場合は、プラグにオスとメス両方のジェンダー変換器を取り付けて延長してください。

6. 始点システムで、`root` ユーザとして `bash` を実行します。

   詳細については、セクション 4.5「bash シェルのアクセス」を参照してください。

7. 始点システムの `/opt/nfast/kmdata` ディレクトリから終点システムの同じディレクトリ パスに、既存のセキュリティ ワールド ファイルをコピーします。

   終点システムにデータをコピーするために、`scp` プログラムが必要になる場合があります。

8. 終点システム上で、次のコマンドラインを実行し、セキュリティ ワールドに終点システムを追加します。

   ```
   /opt/nfast/bin/new-world -l -s 0 -m 1
   ```

   パスワード、および管理者カード セットのスマート カードが要求されます。指示に従ってパスワードを入力し、カードを挿入します。

   new-world コマンドの引数はカスタマイズ可能です。詳細については、nCipher 搭載 ACE XML アプライアンスに付属している nCipher のマニュアルを参照してください。

9. nCipher PCI カードからカード リーダを取り外します。

10. nCipher モジュールのスイッチを「O」の位置に切り替えます。

    この動作によって、動作可能モードへの切り替えを nCipher モジュールに指定します。この時点で、nCipher カード背面のブルーのライトが短く点滅し続けており、カードがまだ事前初期化モードであることを示します。スイッチの位置を変えるだけでは、モジュールのモードは変更されません。新しいモードにするには、モジュールをリセットする必要があります。

11. 次のいずれかの手順でモジュールをリセットします。

    - モード スイッチの横にあるリセット ボタンを押します。

      リセット ボタンはペン、ピン、またはペーパー クリップで押してください。

    または

    - ACE XML アプライアンス上で端末セッションの root ユーザとして、次のコマンドを実行します。

      ```
      /opt/nfast/bin/nopclearfail -ca
      ```

      リセットが正常に完了すると、次のようなメッセージが標準出力に出力されます。

      ```
      module 1, command , clearunit: OK
      ```

      -ca オプションは、nopclearfail コマンドで使用可能なすべての nCipher モジュールを初期化することを指定します。対応する番号を指定して特定のモジュールを初期化する場合は、代わりに -m および -c オプションを使用します。次の例を参照してください。

      ```
      /opt/nfast/bin/nopclearfail -c -m 1
      ```

      -c オプションは、-m オプションで指定された nCipher モジュールを nopclearfail コマンドでクリアすることを指定します。この例のオプションは、コマンドで 1 番のモジュールをクリアすることを指定しています。

    nCipher モジュールをリセットして動作可能モードにすると、nCipher モジュールのブルーの LED が長い間隔で点滅します。

12. 次のコマンドラインを実行して、モジュールが動作可能になっていることを確認します。

    ```
    /opt/nfast/bin/enquiry
    ```

`enquiry` コマンドを使用すると、使用可能な各 nCipher モジュールの状態の要約情報が表示されます。動作可能モードに正常に切り替わった場合は、リセットした各モジュールの要約情報の `mode` フィールドに `operational` と表示されます。

13. `bash` シェルを終了します。
14. **Advanced Options** メニューで **SSL Engine Configuration** を選択します。

    **SSL Engine** 画面が表示されます。
15. **chil** を選択して、nCipher CHIL デバイスをイネーブルにします。

    **Advanced Options** メニューが表示されます。
16. **Return to Main Menu** を選択します。
17. **Main Menu** メニューで **Manage ACE XML Gateway Processes** を選択します。

    **Manage ACE XML Gateway Processes** メニューが表示されます。
18. **Restart All Services** を選択します。

    シェルは現在指定されている構成でアプライアンスの再起動を試み、作業が完了すると、ステータス画面を表示します。

新しい構成でアプライアンスが正常に再起動すると、既存のセキュリティ ワールドが提供する秘密鍵を使用して、いつでも nCipher モジュールを使用できます。詳細については、ACE XML アプライアンスに付属している nCipher のマニュアルを参照してください。