システムセキュリティ

この章では、StarOS のセキュリティ機能について説明します。

この章は、次の内容で構成されています。

シャーシ別のキー識別子

ユーザーは、同じ設定情報を共有するシャーシまたはシャーシのセットに対してのみ機能する一意のシャーシキーを設定できます。

シャーシキーは、1 ～ 16 文字の英数字の ASCII 文字で構成されます。シャーシキーのプレーンテキスト値は、ユーザーには表示されません。インタラクティブに入力され、ユーザーにはエコーされません。

ASR5500 では、暗号化されたシャーシキーはミッドプレーン EEPROM に保存され、両方の MIO/UMIO で共有されます。

構成ファイルのヘッダーコメント行に保存されているシャーシキー識別子がシャーシキーと一致しない場合は、エラーメッセージがユーザーに表示されます。ユーザーは、シャーシキーを再度入力するだけで、シャーシキー値を変更できます。これまでのシャーシキーは新しいシャーシキーに置き換えられます。ユーザーはシャーシキーを入力する必要はありません。

ユーザーがシャーシキーを設定しない場合、システムはそのシャーシに固有の値を生成します。

重要 シャーシキーを変更すると、以前に生成された設定が無効になる可能性があります。これは、以前に生成された設定の秘密部分には、異なる暗号キーを使用されているためです。このため、設定を再作成して復元する必要があります。

重要 管理者がパスワードを簡単に設定できるようにするには、シャーシの初期設定時にシャーシキーを設定する必要があります。

構成ファイルには、シャーシキー（シャーシキー識別子）の一方向暗号化値と、コメントヘッダー行のバージョン番号が含まれています。この2つのデータは、設定内に保存されている暗号化されたパスワードが適切に復号化されるかどうかを決定します。

構成ファイルのロード中に、設定を生成するために使用されるシャーシキーは、保存されたシャーシキーと比較されます。一致しない場合、設定はロードされません。

ユーザーは、構成ファイルからシャーシキー識別子の値とバージョン番号のヘッダーを削除できます。また、ユーザーは構成ファイルを手動で作成することもできます。どちらの場合も、システムは、暗号化されたパスワードの暗号化に同じシャーシキーが使用されることを前提としています。そうでない場合は、印刷不可能な文字またはメモリサイズのチェックにより、パスワードが復号化されません。この状況は、シャーシキーを以前の値に戻し、暗号化された値を現在のシャーシキーと一致するように設定を編集したり、構成ファイルの設定ヘッダー行を下に移動したりすることによってのみ回復できます。

SHA2-256 アルゴリズムとそれに続く base36 エンコーディングを使用して、入力シャーシキーからシャーシ ID が生成されます。結果として得られる 44 文字のシャーシ ID は、フラッシュ内の同じ chassisid ファイルに保存されます。

MIO の同期

MIO/UMIO の起動時に、ASR 5500 ミッドプレーンに設定されているシャーシキーが自動的に読み込まれます。

パスワードの保護

インスペクタおよびオペレータの権限レベルを持つユーザーは、コマンドラインインターフェイス（CLI）を介して、構成ファイルに復号されたパスワードを表示できません。

セキュアなパスワードの暗号化

21.0 よりも前の StarOS リリースでは、デフォルトで、システムは MD5 ベースの暗号（オプション A）を使用してパスワードを暗号化します。これらのパスワードには、パスワードにラ

ンダムな64ビット（8バイト）のソルトが追加されています。シャーシキーは暗号キーとして使用されます。

シャーシキーを設定すると、暗号解読に「共有秘密」の知識が必要な暗号化方式がサポートされます。この共有秘密の知識を持つシャーシのみがパスワードにアクセスできます。パスワードを解読するために、シャーシキーを知っているハッカーは、暗号化内の 64 ビットのランダムなソルト値の場所を特定する必要があります。

MD-5 で暗号化されたパスワードには、暗号化に使用される方法を識別するために、構成ファイルに「+ A」プレフィックスが付いています。

重要 デフォルトは Algorithm B です。

別のタイプの暗号化アルゴリズムを指定します。グローバル構成モードの **cli-encrypt-algorithm** コマンドを使用すると、オペレータはパスワード暗号化と秘密暗号化のアルゴリズムを設定できます。21.0 よりも前のリリースでデフォルトの暗号化とパスワードのアルゴリズムは、前述のように MD-5 です（オプション A）。2 番目のパスワード暗号化のアルゴリズム（オプション B）では、暗号化には AES-CTR-128、認証には HMAC-SHA1 が使用されます。暗号キーによってパスワードの機密性が保護され、認証キーによって整合性が保護されます。リリース 21.0 以降では、アルゴリズム B がデフォルトです。このキーで暗号化されたパスワードは、構成ファイルに「+ B」プレフィックスが付きます。

3 番目のタイプの暗号化アルゴリズムを指定できます（オプション C）。このアルゴリズムは、暗号化と認証に HMAC-SHA512 暗号アルゴリズムの使用を指定します。このキーで暗号化されたパスワードは、構成ファイルに「+ C」プレフィックスが付きます。

暗号キーはシャーシ ID と内部の乱数生成器から取得した 16 バイトの初期化ベクトル（IV）からハッシュされます。同じ暗号キーと IV のペアを使用して 2 つのパスワードが暗号化されることはありませんシャーシ ID と結果の暗号キーを生成するために、セキュリティ管理者はシャーシキーを設定する必要があります。ローカル MAC アドレスに基づくデフォルトのシャーシキーはサポートされなくなりました。

cli-encrypt-algorithm コマンドのシンタックスは次のとおりです。

```
config
   cli-encrypt-algorithm { A | B | C }
```

最新ではない暗号化および復号化のサポート

システムは、以前にフォーマットされた暗号化パスワードをサポートしています。暗号化されたパスワードのシンタックスは、暗号化に使用された方式を示しています。暗号化されたパスワードの前にプレフィックスが表示されない場合は、固定キーを使用した以前の暗号化方式が使用されます。暗号化されたパスワードに「+A」プレフィックスが含まれている場合、復号化方式はシャーシキーとランダムなソルトを使用します。

ユーザーが新しい設定を保存すると、生成されたファイルには常に最新の方式で暗号化されたパスワードが含まれます。ユーザーは、以前の DES ベースの暗号化値を生成できません。た

だし、将来のすべてのStarOSリリースでは、引き続き双方向で暗号化可能なすべてのパスワードのプレーンテキスト パスワード エントリをサポートします。

「ロックアウト」状態を引き起こすことなくシャーシキーを変更するための推奨プロセスは、次のとおりです。

- 前のシャーシキーを使用して、最後の正常な設定の設定ファイルをロードします。
- 必要な新しい値にシャーシキーを変更します。
- この新しいシャーシキーを使用して設定を保存します。

詳細については、「システム設定」の「シャーシキーの設定」を参照してください。

ICSR 設定のサポート

シャーシ間セッションリカバリ（ICSR）は、冗長性ペアとして同様に構成された 2 つの ASR 5500VPC-SI シャーシ/インスタンスを採用する冗長構成です。

ICSR ペアは同じシャーシキーを共有します。2 つのシャーシ/インスタンスに互換性のないシャーシキーがあることをISCRが検出した場合、エラーメッセージがログに記録されますが、ICSR システムは引き続き実行されます。一致するシャーシキーがないと、アクティブピアがアウトオブサービスなった場合に、スタンバイ ICSR ピアはサービスをリカバリできます。スタンバイピアは、暗号化された形式でパスワードに引き続きアクセスできます。

ICSR ピアは、サービス冗長性プロトコル（SRP）を使用して、冗長構成が暗号化されたパスワードまたは DES ベースの双方向暗号化文字列と一致するかどうかを定期的に確認します。設定はソフトウェアに内部的に生成されるため、ユーザーは ICSR の互換性をチェックするために使用される設定にアクセスできません。

暗号化された SNMP コミュニティストリング

Simple Network Management Protocol（SNMP）は、ネットワーク要素のパスワードとしてコミュニティストリングを使用します。これらのコミュニティストリングは SNMP PDU のクリアテキストで送信されますが、値は構成ファイルで暗号化できます。

snmp community encrypted name コマンドは、SNMP コミュニティストリングの暗号化を有効にします。詳細については、『*Command Line Interface Reference*』の「*Global Configuration Mode Commands*」の章をご覧ください。

強化されたパスワード セキュリティ

合法的傍受の制約事項

この項では、合法的傍受（LI）のプロビジョニングに関連付けられている一部のセキュリティ機能について説明します。

LI サーバーアドレス

外部認証エージェント（RADIUS または Diameter など）は、access-accept の一部として LI サーバーアドレスのリストを送信します。そのサブスクライバにすでにインストールされている、またはこれからインストールされるすべての代行受信については、認証エージェントから受信したすべての LI アドレスと LI サーバーアドレスを照合するためのセキュリティチェックが実行されます。この基準を満たすアドレスのみが、そのサブスクライバの代行受信情報を取得します。

キャンプオントリガーを設定している間、ユーザーは、接続先の LI サーバーアドレスを入力する必要はありません。そのキャンプオントリガーに一致するコールが検出されると、認証エージェントから受信したリストを使用してセキュリティチェックが実行されます。LI関連の情報は、一致するアドレスが見つかった場合にのみ転送されます。

アクティブのみの代行受信が設定されている場合、一致するコールが検出されると、認証エージェントから受信した LI アドレスに対してセキュリティチェックが行われ、代行受信の設定は拒否されます。

そのサブスクライバの LI サーバーアドレスに関連する情報が受信されない場合、LI サーバーアドレスは制限されません。

重要 認証エージェントを介して、最大 5 つの LI サーバーアドレスがサポートされます。

重要 RADIUS 属性を使用した LI コンテンツおよびイベント配信の接続先アドレスを制限する機能は、PDSN および HA ゲートウェイでのみサポートされています。

代行受信の変更

1 人の LI 管理者は、別の LI 管理者が作成した代行受信にアクセスしたり、変更したりできます。代行受信が追加、削除、または変更されるたびに、変更に関するイベントログがすべての LI 管理者に表示されます。また、SNMP トラップも生成されます。

ユーザーの追加、変更、削除

システムに対するユーザーの追加または削除は一般には行われません。同じように、ユーザーの権限を変更することもまれです。ただし、システムが侵害された場合は、攻撃者が特権ユーザーを追加または削除したり、権限を上げたり、他のユーザーの権限を低くしたりすることがよくあります。

一般的なルールとして、権限の低いユーザーが権限を上げたり、権限の高いユーザーが入力したパスワードなどのセンシティブデータにアクセスしたりできないようにする必要があります。

重要 システムは、これらのユーザーがシステムを介して設定されている場合にのみ、ユーザーおよびユーザー属性（権限レベルなど）の変更を検出できます。

ユーザーの追加または削除の通知

承認レベルの低いユーザーは、承認レベルの高いユーザーを作成できません。ただし、悪意のある攻撃者が高レベルの権限を持つユーザーを作成できる場合は、他の高レベルの認可されたユーザーを削除して、システムからロックアウトすることができます。

次の SNMP トラップは、ユーザーが追加または削除されたときに管理者に通知します。

- **starLocalUserAdded**：新しいローカルユーザーアカウントがシステムに追加されたことを示します。
- **starLocalUserRemoved**：ローカルユーザーアカウントがシステムから削除されたことを示します。

権限レベル変更の通知

ユーザーの権限レベルが高くなるか低くなるたびに、SNMP 通知が送信されます。悪意のある攻撃者は、権限を何らかの方法で「昇格」させることで、より多くの権限を持つコマンドにアクセスする可能性があります。これが実行されると、他のすべてのユーザーの権限を「降格」させることができ、その結果、適切な管理者がシステムからロックアウトされます。

starLocalUserPrivilegeChanged トラップは、ローカルユーザーの権限レベルが変更されたことを示します。

オペレーティング システム シェルへのユーザーアクセス

starOsShellAccessed トラップは、ユーザーがオペレーティングシステムのシェルにアクセスしたことを示します。

Test-Commands

セキュリティ管理者または管理者権限を持つユーザーは、以前に非表示になっていた test-commands の表示を有効にすることができます。CLI test-commands では、既存のコマンドの新しいコマンドキーワード、および新しいコマンドが表示されます。

注意 CLI test-commands は、診断の使用のみを目的としています。通常のシステム操作では、これらのコマンドへのアクセスは必要ありません。これらのコマンドは、Cisco TAC の担当者のみが使用することを目的としています。これらのコマンドの一部は、システムパフォーマンスの低下、サブスクライバの削除、および/またはシステムの動作不能の原因となることがあります。

cli test-commands モードの有効化

test-commands へのアクセスを有効にするには、セキュリティ管理者がグローバル構成モードにログインし、**cli hidden** を入力する必要があります。

次に、このコマンドシーケンスを示します。

```
[local]host_name# config
[local]host_name(config)# cli hidden
[local]host_name(config)#
```

デフォルトでは、**cli hidden** は無効になっています。

重要 低レベルの診断およびテストコマンドやキーワードは、管理者または上位の権限を持つユーザーに表示されるようになりました。CLI には、test-commands モードが有効になっていることを示すビジュアルインジケータはありません。

CLI テストコマンドにアクセスするためのパスワードの有効化

セキュリティ管理者は、CLI テストコマンドにアクセスするためのプレーンテキストのパスワードまたは暗号化されたパスワードを設定できます。*password* の値は、起動設定情報とともに **/flash** に保存されます。**show configuration** コマンドと **save configuration** コマンドがこの値をプレーンテキストで出力することはありません。

グローバル構成モード コマンドの **tech-support test-commands [encrypted] password** *new_password* **[old-password** *old_password* **]** は、CLI テストコマンドにアクセスするための暗号化されたパスワードまたはプレーンテキストのパスワードを設定します。

次に、このコマンドシーケンスを示します。

```
[local]host_name# config
[local]host_name(config)# tech-support test-commands password new_password [
```

```
old-password old_password ]
[local]host_name(config)#
```

新しいパスワードで既存のパスワードを置き換える場合は、変更を受け入れるために古いパスワードを入力する必要があります。

古いパスワードが入力されていない場合、または既存の設定値と一致しない場合は、「tech-support password is already configured」というエラーメッセージが表示されます。次に、古いパスワードのエントリを受け入れるように求めるプロンプト（「Enter old tech-support password:」）が表示されます。

old-password *old_password* を入力することで、古いパスワードの入力を求められることなく、既存のパスワードを置き換えることができます。古いパスワードを誤って入力した場合、または古いパスワードを入力しなかった場合は、「Failure: Must enter matching old tech-support password to replace existing password」というエラーメッセージが表示されます。

クイック セットアップ ウィザード（Exec モードの **setup** コマンド）でも、テクニカルサポートのテストコマンドパスワードの入力が求められます。古いテクニカルサポートのパスワードを忘れた場合は、コンソールポートから直接 **setup** を実行して、新しいテクニカルサポート パスワードを入力できます。

テストコマンドのパスワードが設定されている場合、グローバル構成モード コマンドの **cli test-commands [encrypted] password** *password* にはパスワードのキーワードを入力する必要があります。**encrypted** キーワードを指定した場合、*password* 引数は、パスワード値を含む暗号化された文字列として解釈されます。**encrypted** キーワードを指定しなかった場合、*password* 引数は実際のプレーンテキスト値として解釈されます。

重要 **tech-support test-commands password** が設定されていない場合は、StarOS が新しいパスワードを作成します。**cli test-commands** に **password** キーワードを入力しなかった場合は、パスワードの入力が求められます（エコーなし）。また、CLI テストコマンドにアクセスするには、管理者が **cli hidden** を有効にする必要があります。

Exec モードの cli test-commands

Exec モードコマンドは、Exec モードから **cli テストコマンド**を入力する特権ユーザーが使用できます。

```
[local]host_name# cli test-commands [encrypted] password password
Warning: Test commands enables internal testing and debugging commands
USE OF THIS MODE MAY CAUSE SIGNIFICANT SERVICE INTERRUPTION
```

重要 ユーザーが CLI テストコマンドモードを開始するたびに、SNMP トラップ（starTestModeEntered）が生成されます。

構成モードの cli test-commands

低レベルのソフトウェアパラメータにアクセスできるようにするための構成コマンドには、権限を持つユーザーがグローバルコ ンフィギュレーション モードでコマンド **cli test-commands** を入力した後にのみアクセスできます。

```
[local]host_name# config
[local]host_name(config)# cli test-commands [encrypted] password password
Warning: Test commands enables internal testing and debugging commands
USE OF THIS MODE MAY CAUSE SIGNIFICANT SERVICE INTERRUPTION
```

重要 ユーザーがCLIテストコマンドモードを開始するたびに、SNMPトラップ（starTestModeEntered）が生成されます。

暗号化のための COTS ハードウェアの使用

StarOS VPC インスタンスは、ソフトウェア内でパケットの暗号化とトンネリングを実行します。ただし、市販（COTS）のサーバーがIntel Communicationsのチップセット89xxを使用し、このチップセットにパススルーするようにVPC仮想マシンを設定した場合、VPCインスタンスは自動的にこのハードウェアチップを使用してパケットの暗号化と復号を実行します。Intel Communicationsのチップセット89xxは、Coleto Creekとも呼ばれています。

（注） VPCが暗号化と復号にハードウェアチップセットを使用するためには、サービス機能（SF）VMのすべてでIntel Communicationsのチップセットを使用する必要があります。

COTSサーバーがこのチップセットを使用しているかどうかを確認するには、**show hardware** コマンドを使用してすべてのスロットの情報を表示します。次に、 Coleto Creek 暗号化アクセラレータを使用するハードウェア上のVPC SIインスタンスに対する **show hardware** コマンドの出力例を示します。

```
[local]swch32# show hardware
System Information:
  Platform                : KVM Guest
  UUID/Serial Number      : 014A4D4F-7644-4CF1-C408-8ABB631B3E34
  CPU Packages            : 1 [#0]
  CPU Nodes               : 1
  CPU Cores/Threads       : 16
  Memory                  : 16384M (qvpc-si-medium)
  Crypto Accelerator      : Coleto Creek A0
Storage Devices:
  Virtual Flash           : Present
    Type                  : 4096M disk
    Model                 : ATA-QEMUHARDDISK
    Serial Number         : QM00001
  Hard Drive 1            : Present
    Type                  : 16384M disk
    Model                 : ATA-QEMUHARDDISK
    Serial Number         : QM00002
```

```
  Hard Drive 2            : Not Present
  USB 1                   : Not Present
  USB 2                   : Not Present
  CDROM 1                 : Present
    Type                  : cdrom
    Model                 : QEMU-QEMUDVD-ROM
Network Interfaces:
  loeth0   addr 52:54:00:ae:b7:72 at virtio1, 1af4:0001 (virtio_net)
    RxQ(s)/RINGSZ/COALESCE: 1/256/-NA-
    TxQ(s)/RINGSZ/COALESCE: 1/256/-NA-
    NODE-ID               : -NA-
  port1_10 addr 00:1b:21:87:14:ac at 0000:00:06.0, 8086:10fb (ixgbe)
    RxQ(s)/RINGSZ/COALESCE: 16/4096/500
    TxQ(s)/RINGSZ/COALESCE: 16/4096/0
    NODE-ID               : -NA-
  port1_11 addr 00:1b:21:87:14:ad at 0000:00:07.0, 8086:10fb (ixgbe)
    RxQ(s)/RINGSZ/COALESCE: 16/4096/500
    TxQ(s)/RINGSZ/COALESCE: 16/4096/0
    NODE-ID               : -NA-
```

次に、暗号アクセラレータがインストールされていないハードウェア上の VPC SI インスタンスに対する **show hardware** コマンドの出力例を示します。

```
[local]swch81# show hardware
System Information:
  Platform                : KVM Guest
  UUID/Serial Number      : E0A26495-F822-4AC0-914D-B51332177C4D
  CPU Packages            : 1 [#0]
  CPU Nodes               : 1
  CPU Cores/Threads       : 16
  Memory                  : 32768M (qvpc-si-medium)
  Crypto Accelerator      : None
Storage Devices:
  Virtual Flash           : Present
    Type                  : 4096M disk
    Model                 : ATA-QEMUHARDDISK
    Serial Number         : QM00001
  Hard Drive 1            : Present
    Type                  : 16384M disk
    Model                 : ATA-QEMUHARDDISK
    Serial Number         : QM00002
  Hard Drive 2            : Not Present
  USB 1                   : Not Present
  USB 2                   : Not Present
  CDROM 1                 : Present
    Type                  : cdrom
    Model                 : QEMU-QEMUDVD-ROM
Network Interfaces:
  loeth0   addr 52:54:00:e9:70:05 at virtio1, 1af4:0001 (virtio_net)
    RxQ(s)/RINGSZ/COALESCE: 1/256/-NA-
    TxQ(s)/RINGSZ/COALESCE: 1/256/-NA-
    NODE-ID               : -NA-
  port1_10 addr 52:54:00:22:f7:85 at virtio2, 1af4:0001 (virtio_net)
    RxQ(s)/RINGSZ/COALESCE: 8/256/-NA-
    TxQ(s)/RINGSZ/COALESCE: 8/256/-NA-
    NODE-ID               : -NA-
  port1_11 addr 52:54:00:3e:67:f9 at virtio3, 1af4:0001 (virtio_net)
    RxQ(s)/RINGSZ/COALESCE: 8/256/-NA-
    TxQ(s)/RINGSZ/COALESCE: 8/256/-NA-
    NODE-ID               : -NA-
```

OS とプラットフォームの乱数生成器のサポート

機能の概要と変更履歴

要約データ

該当製品または機能エリア	すべて
該当プラットフォーム	• VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *VPC-DI* システム管理ガイド • *VPC-SI System* アドミニストレーション ガイド

マニュアルの変更履歴

重要 リリース 21.2 および N5.1 よりも前に導入された機能の改訂履歴の詳細は示していません。

改訂の詳細	リリース
最初の導入。	21.13

機能説明

ASR 5500 および VPC プラットフォームに展開されているいくつかの機能には、特定のタスクを実行するための乱数が必要です。これらのタスクにはカーネル乱数生成器が使用されていますが、生成される数値は、セキュリティ標準規格に従って十分にランダムである場合とそうでない場合があります。ただし、ハードウェアまたはホストが提供する乱数は、信頼性が高く、セキュリティ標準規格に準拠していると見なされます。

OS およびプラットフォームの乱数生成器のサポート機能は、このセキュリティ コンプライアンス要件に対応しています。これにより、システム管理者は、ホストマシン上でハードウェア乱数生成器（HWRNG）を設定できます。

設定されている場合、システムはハードウェアの乱数生成器を使用します。

（注） この機能は、HWRNG サポートがホストで使用可能な場合にのみ機能します。

HWRNGサポートが使用可能な場合は、ホスト上の `libvirt xml` ファイルに次の設定を追加します。これにより、クライアント（StarOS）に `virtio_rng` サポートが追加されます。

```
<rng model='virtio'>
      <backend model='random'>/dev/random</backend>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x07' function='0x0'/>
</rng>
```

（注） （前述の設定に示すように）設定でスロット番号7を使用して競合がある場合、次に使用可能なスロットを使用します。

この設定は、それぞれの展開設定に基づいてサポートされているプラットフォームに適用する必要があります。

クライアントでの設定変更は必要ありません。クライアント（StarOS）は、ホストでサポートが有効になっている場合、自動的に `virtio_rng` を選択します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。