CHAPTER 10

その他のシステム設定の構成

この章では、Wide Area Application Service（WAAS）デバイスの基本設定を実行したあと、システム クロックの設定、デフォルトのシステム設定の変更、アラーム過負荷検出の有効化などのその他のシステム タスクを実行する方法について説明します。この章では、AppNav-XE および WAAS Express を実行する Cisco IOS ルータを登録および管理する方法についても説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE および WAVE アプライアンス、WAAS を実行する SM-SRE モジュール、および vWAAS インスタンスを示します。

この章の内容は、次のとおりです。

デバイス プロパティの変更

WAAS Central Manager GUI を使用すると、次のように WAE デバイスのプロパティを変更できます。

- デバイス名を変更する
- デバイスに新しい位置を割り当てる
- デバイスに管理トラフィックで使用される IP アドレスを割り当てる

- デバイスをアクティブまたは非アクティブにする

また、WAAS Central Manager GUI を使用して、デバイスのステータスがオンライン、保留状態、または非アクティブのいずれであるかを決定できます。

GUI では WAAS Central Manager デバイスの名前の変更しか実行できません。

デバイスのプロパティを変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*] を選択します。

ステップ 2　[*device-name*] > [Activation] を選択します。

選択したデバイスのプロパティを編集するためのフィールドがある [Device Activation] ウィンドウが表示されます。

WAAS Central Manager デバイスの場合、このウィンドウで変更できるフィールドは、デバイスの名前と NetBIOS 名だけです。さらに、デバイスの IP アドレスと役割が表示されます。

ステップ 3　[General Configuration] 見出しの下で、次のデバイス プロパティを設定または変更します。

- デバイスのホスト名を変更するには、[Name] フィールドに新しい名前を入力します。この名前は、次の規則に従う必要があります。
  - 名前には英数字とハイフン（-）だけを使用する。
  - 最初と最後の文字は、英数字である。
  - 長さは 30 文字以内。
  - 大文字と小文字を区別しない。
  - 次の文字は違反と見なされ、デバイス名に使用できない。
    @、#、$、%、^、&、*、()、|、\""/、<>
- デバイスをアクティブまたは非アクティブにするには、[Activate] チェックボックスを選択または選択解除します。このボックスを選択すると、デバイスは WAAS Central Manager GUI による集中管理用にアクティブになります。

  また、タスクバーの [Deactivate] アイコンをクリックして、デバイスを非アクティブにすることもできます。デバイスを非アクティブにすると、ハードウェアの障害時に、そのすべての設定を失うことなく、デバイスを交換できます。
- デバイスの NetBIOS 名を変更するには、提供されるフィールドにデバイスの新しい NetBIOS 名を入力します。NetBIOS 名は数字だけで構成できません。文字を含める必要があります。このフィールドは WAAS Express デバイスでは表示されません。

ステップ 4　[Locality] 見出しの下で、[Location] ドロップダウン リストから新しい位置を選択して、位置を設定または変更します。このデバイス用の位置を作成するには、「位置の作成」（P.3-11）を参照してください。

ステップ 5　[NAT] 見出しの [Management Interface Configuration] の下で、次のフィールドを使用して NAT 設定を構成します。

- [Use WAE's primary IP Address] チェックボックスを選択して、WAAS Central Manager が、デバイスのプライマリ インターフェイスに設定されている IP アドレスを使用して、NAT ファイアウォールの背後にある WAAS ネットワークでデバイスと通信できるようにします。このチェックボックスは WAAS Express デバイスでは表示されません。
- WAAS Central Manager が明示的に設定された IP アドレスを使用して、NAT ファイアウォールの背後にある WAAS ネットワークでデバイスと通信できるようにするには、[Management IP] フィールドにデバイスの IP アドレスを入力します。WAE のプライマリ インターフェイスがインライン グループ インターフェイスに設定されていて、管理トラフィックが個別の IP アドレス（同

じインライン グループ インターフェイスのセカンダリ IP アドレスまたは組み込みインターフェイスのセカンダリ IP アドレス）に設定されているシナリオでも、このアドレスを入力する必要があります。

- [Port] フィールドで、管理 IP アドレス用のポート番号を入力します。WAAS Express デバイスに設定されている HTTPS サーバがデフォルトの 443 以外のポートを使用している場合は、ここで同じポートを設定してください。

（注）　WAAS Central Manager は、プライマリ IP アドレスを使用してデバイスにアクセスできない場合、管理 IP アドレスを使用して通信を試みます。

ステップ 6　[Comments] フィールドに、このデバイスに表示するコメントを入力します。

ステップ 7　[Submit] をクリックします。

ソフトウェア ライセンスの管理

WAAS ソフトウェア バージョン 4.1.1 では、特定の WAAS 最適化機能およびアクセラレーション機能を有効にするソフトウェア ライセンスが導入されました。ソフトウェア ライセンスは、有効にする機能が動作する前に、インストールおよび設定される必要があります。

表 10-1 に、購入できるソフトウェア ライセンスおよび各ライセンスにより有効にされる機能を示します。

表 10-1　WAAS ソフトウェア ライセンス

ライセンス	説明
Transport	基本的な DRE、TFO、および LZ の最適化を有効にします。Enterprise ライセンスが設定されている場合は、設定できません。
Enterprise	EPM、HTTP、MAPI、NFS、SSL、CIFS、SMB、ICA、Window Print のアプリケーション アクセラレータ、WAAS Central Manager、および基本的な DRE、TFO、LZ 最適化を有効にします。Transport ライセンスが設定されている場合は、設定できません。
Video	ビデオ アプリケーション アクセラレータを有効にします。最初に Enterprise ライセンスを設定する必要があります。
Virtual-Blade	仮想化機能を有効にします。最初に Enterprise ライセンスを設定する必要があります。

ライセンスは、デバイス グループではなく個々の WAE デバイス上でインストールおよび管理されます。すべてのライセンスがすべてのデバイスでサポートされるわけではありません。WAAS Central Manager デバイスには Enterprise ライセンスだけが必要で、他のライセンスは設定できません。

（注）　WAAS Express ライセンスは、WAAS Central Manager からではなく、ルータの CLI コマンド **license install** を使用して管理されます。WAAS Express デバイスでは、WAAS デバイスで使用されるものと同じ種類のライセンスは使用されません。これらは WAAS Express 最適化機能を有効にする 1 つのライセンスを使用します。

WAAS Central Manager から WAE にライセンスを追加するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*] を選択します。(Central Manager 上のライセンスを管理するには CLI を使用する必要があるため、Central Manager デバイスを選択しないでください)。

ステップ 2　[Admin] > [History] > [License Management] を選択します。

ステップ 3　追加する各ライセンスの横にあるチェックボックスを選択します。

ステップ 4　[Submit] をクリックします。

CLI からライセンスを追加するには、**license add** EXEC コマンドを使用します。

CLI からライセンスを削除するには、**clear license** EXEC コマンドを使用します。

CLI からすべてのライセンスのステータスを表示するには、**show license** EXEC コマンドを使用します。

新しい WAAS デバイスを最初に設定する場合、セットアップ ユーティリティでもライセンスを設定します。

Inetd RCP および FTP サービスの有効化

リモート コピー プロトコル（RCP）を使用すると、リモート ホストとスイッチの間で設定ファイルをダウンロード、アップロード、およびコピーできます。コネクションレス型プロトコルのユーザ データグラム プロトコル（UDP）を使用する TFTP とは異なり、RCP はコネクション型の TCP を使用します。Inetd（インターネット デーモン）は、特定のポートに対する接続要求またはメッセージを聴取し、サーバ プログラムを起動して、それらのポートに関連付けられたサービスを実行します。RCP は、デバイス間でファイルをコピーします。

RCP は、UNIX ユーザがリモート UNIX システムでシェル コマンドを実行できる UNIX rshell サービスのサブセットです。RCP は、UNIX の組み込みサービスです。このサービスは、伝送プロトコルとして TCP を使用し、TCP ポート 514 で要求を聴取します。RCP サービスは、WAAS ソフトウェアを使用する WAAS デバイスで有効にできます。

WAAS デバイスで RCP および FTP サービスを有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Network] > [Network Services] を選択します。[Network Services] ウィンドウが表示されます。

ステップ 3　[Enable RCP] チェックボックスを選択して、Inetd RCP サービスを有効にします。デフォルトでは、このオプションは無効になっています。

（注）　Inetd デーモンは、FTP、RCP、および TFTP サービスを聴取します。Inetd が RCP 要求を聴取するには、RCP サービス用に明示的に有効にする必要があります。

ステップ 4　[Enable FTP] チェックボックスを選択して、Inetd FTP サービスを有効にします。デフォルトでは、このオプションは無効になっています。

ステップ 5　[Submit] をクリックして変更を保存します。

デフォルト設定またはデバイス グループ設定の適用後に保存されていない変更がある場合は、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。また、[Reset] ボタンをクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合にだけ表示されます。

日時設定の構成

このセクションでは、WAAS ネットワーク デバイス用の日時設定を構成する方法について説明します。内容は、次のとおりです。

NTP 設定の構成

WAAS Central Manager GUI を使用すると、ネットワーク上のネットワーク タイム プロトコル（NTP）ホストを使用して日時設定を構成できます。NTP を使用すると、WAAS ネットワーク内の異なる地域にあるデバイスの日時設定を同期化できます。これは正しいシステム動作とモニタリングのために重要です。各 WAAS デバイスで、必ずクロックの同期を維持するように NTP サーバを設定してください。

NTP 設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Date/Time] > [NTP] を選択します。[NTP Settings] ウィンドウが表示されます。

ステップ 3　[NTP Server] フィールドに、最大 4 つのホスト名または IP アドレスをスペースで区切って入力します。

ステップ 4　[Submit] をクリックします。

（注）　予期しない時間変更は、予期しないシステム動作の原因となる場合があります。NTP サーバの設定後またはシステム クロックの変更後に、システムをリロードすることを推奨します。

時間帯設定の構成

ネットワーク上に時刻サービスを提供する外部ソース（NTP サーバなど）がある場合は、システム クロックを手動で設定する必要はありません。手動でクロックを設定するときは、現地時間を入力します。

（注）　システムには 2 個のクロックがあります。ソフトウェア クロックとハードウェア クロックです。ソフトウェアは、ソフトウェア クロックを使用します。ハードウェア クロックは、ソフトウェア クロックを初期化するために、起動時にだけ使用されます。

デバイスまたはデバイス グループで時間帯を設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Date/Time] > [Time Zone] を選択します。[Time Zone Settings] ウィンドウが表示されます。

ステップ 3　標準時間帯を設定するには、次の手順に従ってください。

a. [Time Zone Settings] セクションで、[Standard Time Zone] オプション ボタンをクリックします。夏時間を設定していない UTC（オフセット =0）がデフォルトです。標準時間帯を設定すると、システムは自動的に UTC オフセットを調整するので、UTC オフセットを指定する必要はありません。

時間帯の標準的な表記法は、*Location/Area* 形式を使用します。ただし、*Location* は世界の大陸または地域、*Area* はその地域内の時間帯領域です。

b. ドロップダウン リストから、時間帯の地域を選択します（このリストの略号については、表 10-2 を参照してください）。

ウィンドウが更新され、2 番めのドロップダウン リストに、選択した地域のすべての領域の時間帯が表示されます。

c. 時間帯の地域を選択します。UTC オフセットは自動的に標準時間帯に設定されます。

夏時間が組み込まれている標準時間帯もあります（米国の大半の時間帯が該当）。これらの地域では、夏時間のあいだは UTC オフセットが自動的に変更されます。設定可能な標準時間帯およびその UTC オフセットのリストについては、表 10-3 を参照してください。

ステップ 4　デバイスでカスタマイズされた時間帯を設定するには、次の手順に従ってください。

a. [Time Zone Settings] セクションで、[Customized Time Zone] オプション ボタンをクリックします。

b. [Customized Time Zone] フィールドで、時間帯の名前を指定します。時間帯項目は大文字と小文字を区別し、スペースを含めて最大 40 文字を使用できます。標準時間帯の名前を指定すると、[Submit] をクリックしたときにエラー メッセージが表示されます。

c. UTC オフセットについて、最初のドロップダウン リストから [+] または [-] 記号を選択して、設定された時間帯が UTC より進んでいるか、遅れているかを指定します。また、カスタマイズされた時間帯の UTC オフセット時間（0 ～ 23）と分（0 ～ 59）を選択します。UTC オフセットの範囲は、-23:59 から 23:59 です。デフォルトは 0:0 です。

ステップ 5　カスタマイズされた夏時間を設定するには、[Customized Summer Time Savings] セクションで次の手順に従ってください。

（注）　カスタマイズされた夏時間は、標準時間帯とカスタマイズされた時間帯の両方に指定できます。

a. 対夏時間を設定するには、[Absolute Dates] オプション ボタンをクリックします。

夏時間の開始日付と終了日付は、絶対日付または反復日付で設定できます。絶対日付設定は一度だけ適用され、毎年設定する必要があります。反復日付は何年間も繰り返し適用されます。

b. [Start Date] フィールドと [End Date] フィールドで、夏時間を開始し、終了する必要がある月（January ～ December）、日（1 ～ 31）、および年（1993 ～ 2032）を mm/dd/yyyy 形式で指定します。終了日付が常に開始日付よりあとにあることを確認します。

あるいは、[Start Date] フィールドと [End Date] フィールドの横にある [Calendar] アイコンをクリックして、[Date Time Picker] ポップアップ ウィンドウを表示します。デフォルトで、現在の日付が黄色で表示されます。必要に応じて、[Date Time Picker] ポップアップ ウィンドウで左矢印または右矢印を使用して、前の年または次の年を選択します。ドロップダウン リストから月を選択します。月の日をクリックします。選択した日付が青色で表示されます。[Apply] をクリックします。あるいは、[Set Today] をクリックして、現在の日付へ戻ります。選択した日付は、[Start Date] フィールドと [End Date] フィールドに表示されます。

c. 反復夏時間を設定するには、[Recurring Dates] オプション ボタンをクリックします。

d. [Start Day] ドロップダウン リストから、開始する曜日（[Monday] ～ [Sunday]）を選択します。

e. [Start Week] ドロップダウン リストから、開始する週を設定するオプション（[first]、[2nd]、[3rd]、または [last]）を選択します。たとえば、[first] を選択すると、夏時間を月の最初の週に開始し、[last] を選択すると、夏時間を月の最後の週に開始するように設定できます。

f. [Start Month] ドロップダウン リストから、開始する月（[January] ～ [December]）を選択します。

g. [End Day] ドロップダウン リストから、終了する曜日（[Monday] ～ [Sunday]）を選択します。

h. [End Week] ドロップダウン リストから、終了する週を設定するオプション（[first]、[2nd]、[3rd]、または [last]）を選択します。たとえば、[first] を選択すると、夏時間を月の最初の週に終了し、[last] を選択すると、夏時間を月の最後の週に終了するように設定できます。

i. [Start Month] ドロップダウン リストから、終了する月（[January] ～ [December]）を選択します。

ステップ 6　[Start Time] ドロップダウン リストから、夏時間を開始する時（0 ～ 23）と分（0 ～ 59）を選択します。[End Time] ドロップダウン リストから、夏時間を終了する時（0 ～ 23）と分（0 ～ 59）を選択します。

夏時間の [Start Time] フィールドと [End Time] フィールドは、夏時間を反映するためにクロックを変更する時刻です。デフォルトで、開始時刻と終了時刻の両方が 00:00 に設定されます。

ステップ 7　[Offset] フィールドで、UTC からのオフセット（0 ～ 1439 分）を指定します （表 10-3 を参照）。

夏時間のオフセットは、システム クロックを指定した開始時刻より進め、終了時刻より遅らせる時間（分）を指定します。

ステップ 8　対応する時間帯に夏時間を指定しないようにするには、[No Customized Summer Time Configured] オプション ボタンをクリックします。

ステップ 9　[Submit] をクリックして、設定を保存します。

デフォルト設定またはデバイス グループ設定の適用後に保存されていない変更がある場合は、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。また、[Reset] ボタンをクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合にだけ表示されます。

表 10-2　時間帯地域の略号

時間帯	説明
CET	中央ヨーロッパ標準時
CST6CDT	中部夏時間
EET	東ヨーロッパ標準時

表 10-2　時間帯地域の略号 （続き）

時間帯	説明
EST	東部標準時
EST5EDT	東部夏時間
GB	英国
GB-Eire	英国 / アイルランド
GMT	グリニッジ標準時
HST	ハワイ標準時
MET	中央ヨーロッパ標準時
MST	山岳部標準時
MST7MDT	山岳部夏時間
NZ	ニュージーランド
NZ-CHAT	ニュージーランド、チャタム諸島
PRC	中国
PST8PDT	太平洋夏時間
ROC	台湾
ROK	韓国
UCT	協定世界時
UTC	協定世界時
WET	西ヨーロッパ標準時
W-SU	中央ヨーロッパ標準時

表 10-3　時間帯、UTC からのオフセット

時間帯	UTC からのオフセット（時間）
Africa/Algiers	+1
Africa/Cairo	+2
Africa/Casablanca	0
Africa/Harare	+2
Africa/Johannesburg	+2
Africa/Nairobi	+3
America/Buenos_Aires	-3
America/Caracas	-4
America/Mexico_City	-6
America/Lima	-5
America/Santiago	-4
Atlantic/Azores	-1
Atlantic/Cape_Verde	-1
Asia/Almaty	+6
Asia/Baghdad	+3
Asia/Baku	+4
Asia/Bangkok	+7
Asia/Colombo	+6
Asia/Dacca	+6

表 10-3　時間帯、UTC からのオフセット （続き）

時間帯	UTC からのオフセット（時間）
Asia/Hong_Kong	+8
Asia/Irkutsk	+8
Asia/Jerusalem	+2
Asia/Kabul	+4.30
Asia/Karachi	+5
Asia/Katmandu	+5.45
Asia/Krasnoyarsk	+7
Asia/Magadan	+11
Asia/Muscat	+4
Asia/New Delhi	+5.30
Asia/Rangoon	+6.30
Asia/Riyadh	+3
Asia/Seoul	+9
Asia/Singapore	+8
Asia/Taipei	+8
Asia/Tehran	+3.30
Asia/Vladivostok	+10
Asia/Yekaterinburg	+5
Asia/Yakutsk	+9
Australia/Adelaide	+9.30
Australia/Brisbane	+10
Australia/Darwin	+9.30
Australia/Hobart	+10
Australia/Perth	+8
Australia/Sydney	+10
Canada/Atlantic	-4
Canada/Newfoundland	-3.30
Canada/Saskatchewan	-6
Europe/Athens	+2
Europe/Berlin	+1
Europe/Bucharest	+2
Europe/Helsinki	+2
Europe/London	0
Europe/Moscow	+3
Europe/Paris	+1
Europe/Prague	+1
Europe/Warsaw	+1
Japan	+9
Pacific/Auckland	+12
Pacific/Fiji	+12
Pacific/Guam	+10
Pacific/Kwajalein	-12

表 10-3　時間帯、UTC からのオフセット （続き）

時間帯	UTC からのオフセット（時間）
Pacific/Samoa	-11
US/Alaska	-9
US/Central	-6
US/Eastern	-5
US/East–Indiana	-5
US/Hawaii	-10
US/Mountain	-7
US/Pacific	-8

UTC は、かつてのグリニッジ標準時（GMT）です。表に示すオフセット時間（UTC との相対時間）は、実質的に冬時間のものです。夏時間中は、オフセットが表の値と異なる場合があり、システム クロックによって計算され、それに応じて表示されます。

セキュア ストア設定の構成

セキュア ストア暗号化によって、WAAS システムに対して強力な暗号化とキー管理が行われます。WAAS Central Manager および WAE デバイスはセキュア ストア暗号化を使用して、パスワードの処理、暗号化キーの管理、およびデータの暗号化を行います。

ここでは、次の内容について説明します。

セキュア ストアの概要

Central Manager または WAE デバイスでセキュア ストア暗号化を有効にすると、WAAS システムは強力な暗号化アルゴリズムとキー管理ポリシーを使用して、システム上の特定のデータを保護します。このデータには、WAAS システム内でアプリケーションが使用する暗号キー、事前配置用の CIFS パスワード、ユーザ ログイン パスワード、NAM クレデンシャル、および証明書キー ファイルが含まれます。

Central Manager でのセキュア ストア暗号化は常に有効に設定されており、自動生成されたパスワードかユーザが指定したパスワードが使用されます。このパスワードは、安全規格に従い *キー暗号キー*を生成するために使用されます。WAAS システムは、キー暗号キーを使用して、Central Manager または

WAE デバイス上で生成された他のキーを暗号化し保存します。これらのその他のキーは、ディスクの暗号化や SSL アクセラレーション、または CIFS アクセラレータのクレデンシャルやユーザ パスワードの暗号化と保存などの WAAS 機能で使用されます。

Central Manager 上のデータは、SHA 1 ハッシュと AES 256 ビット アルゴリズムを使用して、パスワードによって生成された 256 ビット キー暗号キーを使用して暗号化されます。セキュア ストアが WAE デバイスで有効な場合、データは、SecureRandom（暗号として強力な疑似乱数ジェネレータ）を使用して生成された 256 ビット キー暗号キーを使用して暗号化されます。

Central Manager のセキュア ストア暗号化は、次のいずれかのモードを使用します。

- 自動生成パスフレーズ モード：Central Manager によってパスフレーズが自動的に生成されます。各システムが再起動した後、そのパスフレーズを使用してセキュア ストアが開かれます。これは、新しい Central Manager デバイスのデフォルト モード、またはシステムが再インストールされた後のデフォルト モードです。
- ユーザ指定パスフレーズ モード：パスフレーズはユーザが指定します。各システムが再起動した後、セキュア ストアを開くには、ユーザがパスフレーズを入力する必要があります。このモードに切り替えることができます。4.4.1 よりも前のバージョンからアップグレードされ、セキュア ストアが初期化されたシステムは、4.4.1 以降へのアップグレード後にこのモードに設定されます。

セキュア ストアを実装するには、システムが次の要件を満たしている必要があります。

- Central Manager がネットワークで使用できるように設定されている必要があります。
- WAE デバイスが、Central Manager に登録されている必要があります。
- WAE デバイスが Central Manager とオンラインになっている（アクティブ接続を確立している）必要があります。この要件は、セキュア ストアが WAE デバイスで有効な場合にのみ適用されます。
- すべての Central Manager と WAE デバイスで、WAAS ソフトウェア バージョン 4.0.19 以上を実行している必要があります。

強力なストア暗号化を実装するには、次の手順に従ってください。

ステップ 1　プライマリ Central Manager で強力なストレージ暗号化を有効にします Central Manager でのセキュア ストア暗号化の有効化を参照してください。

ステップ 2　スタンバイ Central Manager で強力なストレージ暗号化を有効にします スタンバイ Central Manager でのセキュア ストア暗号化の有効化を参照してください。

ステップ 3　WAE デバイスまたは WAE デバイス グループで強力なストレージ暗号化を有効にします WAE デバイスでのセキュア ストア暗号化の有効化を参照してください。セキュア ストアは、Central Manager で有効にしてから、WAE デバイスで有効にする必要があります）。

セキュア ストアは、Central Manager と WAE デバイスで独立して有効にすることができます。暗号化されたデータの完全な保護を保証するには、セキュア ストアを Central Manager と WAE デバイスの両方で有効にします。最初に、Central Manager 上でセキュア ストアを有効にする必要があります。

（注）　セキュア ストアがユーザ指定パスフレーズ モードになっている場合は、Central Manager を再起動するときに、セキュア ストア暗号化を手動で開く必要があります。リモート WAE デバイス上でセキュア ストア（ディスク暗号化、CIFS 事前配置、SSL アクセラレーション、AAA など）を使用するすべてのサービスは、ユーザが Central Manager のセキュア ストア パスワードを入力してセキュア ストア暗号化を開くまで、正しく機能しません。

セキュア ストアについて、次の考慮事項に注意してください。

- Central Manager データベースに保存されたパスワードは、強力な暗号化技術を使用して暗号化されます。
- CIFS 事前配置クレデンシャルは、Central Manager と WAE デバイスの強力な暗号化キーを使用して暗号化されます。
- 証明書キー ファイルは、Central Manager の強力な暗号キーを使用して暗号化されます。
- プライマリ Central Manager が失敗すると、セキュア ストア キー管理はスタンバイ Central Manager によって処理されます （スタンバイ Central Manager では、セキュア ストア モードを手動で有効にする必要があります）。
- バックアップ スクリプトによって、バックアップ時にデバイスのセキュア ストア パスフレーズ モード（ユーザ指定または自動生成）がバックアップされます。バックアップと復元は、Central Manager でのみサポートされます。
- セキュア ストアがユーザ指定パスフレーズ モードだったときにバックアップを行い、それをセキュア ストアが自動生成パスフレーズ モードになっているシステムに復元する場合は、復元を続行するためにユーザパスフレーズを入力する必要があります。復元後、システムはユーザ指定パスフレーズ モードになります。セキュア ストアが自動生成パスフレーズ モードだったときにバックアップを行い、それをセキュア ストアがユーザ指定パスフレーズ モードになっているシステムに復元する場合、パスワードを入力する必要はありません。復元後、システムは自動生成パスフレーズ モードになります。
- WAE デバイスでセキュア ストアを有効にすると、システムは Central Manager からの新しい暗号キーを初期化し取得します。WAE は、このキーを使用して、ディスク上の CIFS 事前配置クレデンシャルや情報などのデータを暗号化します（ディスク暗号化も有効な場合）。
- セキュア ストアを有効にしたあとで WAE をリブートすると、WAE は Central Manager からキーを自動的に取得します。これにより、WAAS 永続ストレージに保存されているデータにアクセスできるようになります。キーの取得に失敗した場合は、クリティカル アラームが発生し、セキュア ストアを手動で再オープンする必要があります。更新に CIFS 事前配置、ダイナミック共有、またはユーザ設定が含まれる場合、セキュア ストアが再オープンされるまで、WAE は Central Manager からの設定更新を拒否します。また、WAE から Central Manager に送信される更新には、事前配置設定は含まれません。
- セキュア ストアは特定のシステム情報を暗号化しますが、ハード ドライブ上のデータは暗号化しません。データ ディスクを保護するには、別途、ディスク暗号化を有効にする必要があります 「ディスクの暗号化の有効化」（P.16-31）を参照してください。

Central Manager でのセキュア ストア暗号化の有効化

新しい Central Manager では、デフォルトでセキュア ストアが有効に設定されており、システムの起動後に、システムで生成されたパスワードによってセキュア ストアが開かれます。セキュア ストアを有効にするために、何も行う必要がありません。

Central Manager がユーザ指定パスフレーズ モードで設定されている場合、システム起動後に手動でセキュア ストアを開く必要があります。Central Manager でセキュア ストア暗号化を開くには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Admin] > [Secure Store] を選択します。[Configure CM Secure Store] ウィンドウが表示されます。

ステップ 2　[Open Secure Store] の下にある [Current passphrase] フィールドに、セキュア ストアのパスフレーズを入力します。

ステップ 3　[Open] ボタンをクリックします。

セキュア ストアが開かれます。データはパスワードから派生したキーを使用して暗号化されます。

CLI からセキュア ストアを開くには、**cms secure-store open** EXEC コマンドを使用します。

（注） ユーザ指定パスフレーズ モードに設定されている Central Manager を再起動するたびに、セキュア ストアを手動で再度開く必要があります。リモート WAE デバイス上でセキュア ストア（ディスク暗号化、CIFS 事前配置、SSL アクセラレーション、AAA など）を使用するすべてのサービスは、ユーザが Central Manager のセキュア ストア パスワードを入力してセキュア ストアを再度開くまで、正しく機能しません。自動生成パスフレーズ モードに切り替えると、再起動するたびにセキュア ストアを再度開く必要がなくなります。

（注） プライマリ Central Manager のセキュア ストアをユーザ指定パスフレーズ モードで有効にした場合は、スタンバイ Central Manager のセキュア ストアも有効にする必要があります。「スタンバイ Central Manager でのセキュア ストア暗号化の有効化」（P.10-13）を参照してください。

セキュア ストア暗号化のステータスをチェックするには、**show cms secure-store** コマンドを入力します。

スタンバイ Central Manager でのセキュア ストア暗号化の有効化

（注） スタンバイ Central Manager では、暗号キー管理のサポートは限定されています。プライマリ Central Manager が失敗した場合、スタンバイ Central Manager は WAE デバイスに対して暗号キーを取得できるようにするだけで、新しい暗号キーの初期化は行いません。プライマリ Central Manager が使用不能な場合は、WAE デバイスのディスク暗号化またはセキュア ストアは有効にしないでください。

プライマリ Central Manager のセキュア ストアのパスフレーズ モードは、スタンバイ Central Manager に（標準複製時間内に）複製されます。プライマリ Central Manager が自動生成パスフレーズ モードに切り替えられると、スタンバイ Central Manager のセキュア ストアはオープン状態に変更されます。プライマリ Central Manager がユーザ指定パスフレーズ モードに切り替えられるか、パスフレーズが変更されると、スタンバイ Central Manager のセキュア ストアは初期化状態に変更されますが、オープン状態にはならず、アラームが出ます。スタンバイ Central Manager でセキュア ストアを手動で開く必要があります。

プライマリ Central Manager がユーザ指定パスフレーズ モードのときに、スタンバイ Central Manager でセキュア ストア暗号化を有効にするには、まず、プライマリ Central Manager でセキュア ストアを開いてから、CLI を使用して、スタンバイ Central Manager 上で **cms secure-store open** EXEC モード コマンドを実行します。

ステップ 1　プライマリ Central Manager でセキュア ストア暗号化を有効にします「Central Manager でのセキュア ストア暗号化の有効化」（P.10-12）を参照してください。

ステップ 2　スタンバイ Central Manager がプライマリ Central Manager からデータを複製するまで待ちます。

レプリケーション（複製）は、60 秒以内（デフォルト）に、またはシステムの設定に従って実行されます。

ステップ 3　スタンバイ Central Manager で **cms secure-store open** コマンドを入力して、セキュア ストア暗号化をアクティブにします。

スタンバイ Central Manager が、「please enter pass phrase」メッセージで応答します。

ステップ 4　パスワードを入力し、Enter を押します。

スタンバイ Central Manager が、セキュア ストア暗号化を使用してデータを暗号化します。

（注）　システム上のスタンバイ Central Manager ごとにステップ 3 ～ 4 を繰り返します。

セキュア ストア暗号化のステータスをチェックするには、**show cms secure-store** コマンドを入力します。

WAE デバイスでのセキュア ストア暗号化の有効化

WAE デバイスでセキュア ストア暗号化を有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

（注）　セキュア ストア ステータスは、デバイス グループ内のすべての WAE デバイスで同一である必要があります。グループ内のすべての WAE デバイスのセキュア ストアを有効にするか、すべての WAE デバイスのセキュア ストアを無効にする必要があります。WAE デバイスをデバイス グループに追加する前に、その WAE デバイスのセキュア ストア ステータスが他の WAE デバイスのステータスと一致するように設定する必要があります 「デバイス グループの使用」（P.3-2）を参照してください。

ステップ 2　[Configure] > [Security] > [Secure Store] を選択します。[Secure Store Settings] ウィンドウが表示されます。

ステップ 3　[Initialize CMS Secure Store] ボックスを選択します　（[Open CMS Secure Store] ボックスは自動的に選択されています）。

ステップ 4　[Submit] をクリックして、セキュア ストア暗号化をアクティブにします。

新しい暗号キーが Central Manager で初期化され、WAE はセキュア ストア暗号化を使用してデータを暗号化します。

CLI からセキュア ストアを有効にするには、**cms secure-store init** EXEC コマンドを使用します。

（注）　**cms secure-store** コマンドを実行する前に、WAE 上でデータ入力ポール レート間隔（デフォルトは 5 分）以内にその他の CLI 設定に変更を行った場合、これらの先行する設定変更は失われるため、再度実行する必要があります。

（注）　デバイス グループのセキュア ストアを有効または無効にしても、変更内容はすべての WAE デバイスに同時に反映されません。WAE デバイスを表示した際には、Central Manager が各 WAE デバイスのステータスを更新するまで十分な時間を確保してください。

セキュア ストアのパスフレーズ モードの変更

セキュア ストアは、ユーザ指定パスフレーズ モードまたは自動生成パスフレーズ モードのいずれかで動作できます。また、これらのモードを切り替えることができます。

ユーザ指定パスフレーズ モードから自動生成パスフレーズ モードに変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Admin] > [Secure Store] を選択します。

ステップ 2　[Switch to CM auto-generated passphrase mode] エリアで、[Current passphrase] フィールドにパスワードを入力します。

ステップ 3　[Switch] ボタンをクリックします。

ステップ 4　表示される確認メッセージで [OK] をクリックします。

セキュア ストアが自動生成パスフレーズ モードに変わり、オープン状態のままになります。

自動生成パスフレーズ モードからユーザ指定パスフレーズ モードに変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Admin] > [Secure Store] を選択します。

ステップ 2　[Switch to User-provided passphrase mode] エリアで、[New passphrase] フィールドにパスワードを入力してから、[Confirm passphrase] フィールドにパスワードをもう一度入力します。

パスワードは、次の規則に従う必要があります。

- 長さは 8 ～ 64 字
- 許可される文字セット（A-Za-z0-9~%'!#$^&*()|;:,"<>/）だけを使用
- 数字を少なくとも 1 文字含める
- 大文字と小文字を少なくとも 1 文字ずつ含める

ステップ 3　[Switch] ボタンをクリックします。

ステップ 4　表示される確認メッセージで [OK] をクリックします。

セキュア ストアがユーザ指定パスフレーズ モードに変わり、オープン状態のままになります。スタンバイ Central Manager がある場合は、そのセキュア ストアを手動で開く必要があります（「スタンバイ Central Manager でのセキュア ストア暗号化の有効化」（P.10-13）を参照）。

CLI からセキュア ストアのパスフレーズ モードを変更するには、**cms secure-store mode** EXEC コマンドを使用します。

（注）　ユーザ指定パスフレーズ モードに設定されている Central Manager を再起動するたびに、セキュア ストアを手動で再度開く必要があります。リモート WAE デバイス上でセキュア ストア（ディスク暗号化、CIFS 事前配置、SSL アクセラレーション、AAA など）を使用するすべてのサービスは、ユーザが Central Manager のセキュア ストア パスワードを入力してセキュア ストアを再度開くまで、正しく機能しません。自動生成パスフレーズ モードに切り替えると、再起動するたびにセキュア ストアを再度開く必要がなくなります。

セキュア ストア暗号キーおよびパスワードの変更

セキュア ストア暗号化パスワードは、Central Manager が暗号化されたデータ用の暗号キーを生成するために使用されます。Central Manager がユーザ指定パスフレーズ モードに設定されている場合は、パスワードを変更できます。

Central Manager でパスワードを変更し新しい暗号キーを生成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Admin] > [Secure Store] を選択します。

ステップ 2　[Change Secure Store passphrase] エリアの [Current passphrase] フィールドに現在のパスワードを入力します。

ステップ 3　[New passphrase] フィールドに新しいパスワードを入力します。

パスワードは、次の規則に従う必要があります。

- 長さは 8 ～ 64 字
- 許可される文字セット（A-Za-z0-9~%'!#$^&*()|;:,"<>/）だけを使用
- 数字を少なくとも 1 文字含める
- 大文字と小文字を少なくとも 1 文字ずつ含める

ステップ 4　[Confirm passphrase] フィールドに、もう一度新しいパスワードを入力します。

ステップ 5　[Change] ボタンをクリックします。

WAAS デバイスは、新しいパスワードから派生した新しい暗号キーを使用して、保存されているデータを暗号化し直します。

CLI から Central Manager のパスワードを変更し新しい暗号キーを生成するには、**cms secure-store change** EXEC コマンドを使用します。

WAAS Central Manager から WAE デバイスの新しい暗号化キーを生成するには、次の手順に従います。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Security] > [Secure Store] を選択します。

ステップ 3　[Change CMS Secure Store] チェックボックスを選択し、[Submit] をクリックします。

Central Manager 内で新しい暗号キーが生成されます。Central Manager が、WAE 内の暗号キーを新しいキーで置き換えます。WAE は、新しい暗号キーを使用して保存されているデータを暗号化し直します。

CLI からセキュア ストア暗号キーを設定するには、**cms secure-store change** EXEC コマンドを使用します。

Central Manager でのセキュア ストア暗号化のリセット

Central Manager をリロードしたときに、それがユーザ指定パスフレーズ モードで設定されており、セキュア ストアのパスワードを忘れてしまったためセキュア ストアを開けないときは、セキュア ストアをリセットできます。この処理により、すべての暗号化されたデータ、証明書ファイルとキー ファイル、およびキー マネージャのキーが削除されます。セキュア ストアは再度初期化され、自動生成パスフレーズ モードに設定されて開かれます。

Central Manager でセキュア ストア暗号化をリセットするには、次の手順に従ってください。

ステップ 1　プライマリ Central Manager CLI で、**cms secure-store reset** コマンドを入力してセキュア ストア暗号化をリセットします。

ステップ 2　スタンバイ Central Manager がプライマリ Central Manager からデータを複製するまで待ちます。

レプリケーション（複製）は、60 秒以内（デフォルト）に、またはシステムの設定に従って実行されます。

ステップ 3　セキュア ストアが初期化され、オープンされた状態の場合は、スタンバイ Central Manager で **cms secure-store reset** コマンドを入力します。

ステップ 4　プライマリ Central Manager から、すべてのユーザ アカウント パスワード、CIFS クレデンシャル、および NAM クレデンシャルをリセットします。

ユーザ パスワードをリセットする方法については、「別のアカウントのパスワードの変更」（P.8-7）を参照してください。ダイナミック共有パスワードをリセットする方法については、「CEFS アクセラレータのダイナミック共有を作成」（P.12-10）を参照してください。事前配置パスワードをリセットする方法については、「新しい事前配置ディレクティブの作成」（P.12-13）を参照してください。NAM クレデンシャルをリセットする方法については、「基本セットアップの設定」（P.15-4）を参照してください。

ステップ 5　Central Manager に登録されている各 WAE で、次の手順を実行します。

a. セキュア ストアが初期化され、オープンされている場合は、Central Manager から、セキュア ストアをクリアします（「WAE デバイスでのセキュア ストア暗号化の無効化」（P.10-18）を参照）。または、CLI から、**cms secure-store clear** EXEC コマンドを入力します。

b. Central Manager からセキュア ストアを初期化するか（「WAE デバイスでのセキュア ストア暗号化の有効化」（P.10-14）を参照）、CLI から **cms secure-store init** EXEC コマンドを入力します。（この手順は ステップ 5a を実行したときのみ必要です）。

c. **crypto pki managed-store initialize** コマンドを入力し、SSL アクセラレータを再起動します。

d. ディスク暗号化が有効な場合は、Central Manager からディスク暗号化を無効にするか（「ディスクの暗号化の有効化」（P.16-31）を参照）、CLI から **no disk encrypt enable** グローバル コンフィギュレーション コマンドを入力します。

e. ディスク暗号化が ステップ 5d の前に有効になっている場合は、デバイスをリロードします。リロード後、ディスク暗号化を再度有効にし、デバイスをもう一度リロードします。

（注）　ステップ 5 を実行する前に WAE がリロードされた場合、ディスク暗号化、SSL アクセラレーション、およびセキュア ストアは正しく機能しません。このような場合は、WAE を工場出荷時のデフォルト設定に戻す必要があります。

ステップ 6　プライマリ Central Manager から、WAE で設定されているすべての高速化およびピアリング サービス用に、すべての証明書およびキー ファイルを再インポートします。

WAE デバイスでのセキュア ストア暗号化の無効化

WAE デバイスでセキュア ストア暗号化を無効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Security] > [Secure Store] を選択します。[Secure Store Settings] ウィンドウが表示されます。

ステップ 3　[Clear CMS Secure Store] チェックボックスを選択し、[Submit] をクリックすると、セキュア ストア暗号化は無効になり、標準の暗号化に戻ります。

また、**cms secure-store clear** コマンドを入力しても、セキュア ストア暗号化を無効にし、標準の暗号化に戻すことができます。

（注）　暗号化されたサービスのユーザ アカウント ドメイン アイデンティティを含むデバイスのセキュア ストアはクリアできません。ユーザ アカウント ドメイン アイデンティティの詳細については、「暗号化 MAPI アクセラレーションの設定」の項を参照してください。

CLI から WAE のセキュア ストアを無効にするには、**cms secure-store clear** EXEC コマンドを使用します。

（注）　セキュア ストアは、Central Manager では無効にできません。

デフォルトのシステム設定プロパティの変更

WAAS ソフトウェアではすでにシステム プロパティが設定済みですが、システムのデフォルト動作を変更するために変更できます。

表 10-4 で、変更できるシステム設定プロパティについて説明します。

表 10-4　システム設定プロパティの説明

システム プロパティ	説明
cdm.remoteuser.deletionDaysLimit	外部ユーザが最後にログインしてから、WAAS Central Manager データベースから削除されるまでの最大日数。たとえば、cdm.remoteuser.deletionDaysLimit が 5 に設定されている場合、最後のログイン時と現在の時間の差が 5 日を超えると、この外部ユーザはデータベースから削除されます。デフォルトは、60 日です。外部ユーザとは、WAAS Central Manager ではなく、外部 AAA サーバで定義されているユーザです。そのようなユーザによってスケジュール設定されているすべてのレポートも、ユーザが削除されると削除されます。
cdm.session.timeout	WAAS Central Manager GUI セッションのタイムアウト（分）。デフォルトは 10 分です。セッションがこの長さの時間アイドル状態である場合、ユーザは自動的にログアウトされます。
DeviceGroup.overlap	デバイスが複数のデバイス グループに属することが可能かどうかを示すステータス。デフォルトは true です（デバイスは複数のデバイス グループに属することができます）。
System.datafeed.pollRate	WAAS（または WAAS Express）デバイスと WAAS Central Manager 間のポール レート（秒）。デフォルトは 300 秒です。
System.device.recovery.key	デバイス ID の復旧キー。このプロパティを使用すると、WAAS ネットワーク内の別のノードでデバイスを交換できます。
System.guiServer.fqdn	Device Manager GUI を起動するために使用する方式（IP アドレスまたは FQDN）。
System.healthmonitor.collectRate	CMS デバイスの状態（またはステータス）をモニタするための収集と送信の速度（秒）。速度を 0 に設定すると、状態のモニタは無効になります。デフォルトは 120 秒です。
System.lcm.enable	ローカルと中央の管理機能（有効または無効）。このプロパティを使用すると、ローカル デバイスの CLI または WAAS Central Manager GUI を使用して構成した設定を WAAS ネットワーク設定データの一環として保存できます。デフォルトは true です。このプロパティが false（無効）に設定されている場合、ローカル デバイスで実行された設定変更は Central Manager に伝達されず、Central Manager で実行された設定がローカル デバイスの設定を上書きします。この設定は、WAAS と WAAS Express デバイスの両方に適用されます。
System.monitoring.collectRate	WAE がモニタリング レポートを収集し、WAAS Central Manager へ送信する速度（秒）。WAAS Express デバイスの場合、これが、WAAS Express デバイスから Central Manager がモニタリング データを収集する速度になります。デフォルトは 300 秒（5 分）です。この間隔を減らすと、WAAS Central Manager デバイスのパフォーマンスに影響します。
System.monitoring.dailyConsolidationHour	WAAS Central Manager が 1 時間ごとおよび 1 日ごとにモニタリング レコードを集計する時刻。デフォルトは 1（午前 1 時）です。
System.monitoring.enable	WAAS および WAAS Express 統計情報のモニタリング（有効または無効）。デフォルトは true です。

表 10-4　システム設定プロパティの説明 （続き）

システム プロパティ	説明
System.monitoring.maxDevicePerLocation	ロケーション レベル レポートでモニタリングがサポートされるデバイスの最大数。デフォルトは 25 です。
System.monitoring.maxReports	カスタム レポートごとに保存する、成功または失敗したレポート インスタンスの最大数。デフォルトは、10 個のレポート インスタンスです。
System.monitoring.monthlyConsolidationFrequency	WAAS Central Manager が日単位のモニタリング レポートを月次レポートに集計する回数（日単位）。この設定を 1 に設定すると、WAAS Central Manager は、毎日集計を実行する必要があるかどうかを検査し、集計に十分なデータがある場合のみ集計を実行します。デフォルトは、14 日です。 毎月のデータ レコードを作成すると、対応する毎日のレコードはデータベースから削除されます。集計は、少なくとも 2 か月分のデータと集計周期日数分のデータが存在する場合のみ実行されます。そのため、WAAS Central Manager は、常に先月の毎日のデータ レコードを保持し、先週のデータを 1 日単位で表示できます。 たとえば、データ収集が 2006 年 2 月 2 日に開始し、System.monitoring.monthlyConsolidationFrequency が 14 に設定されている場合、WAAS Central Manager は、2 月 16 日、3 月 2 日、3 月 16 日、および 3 月 30 日に過去 2 か月分のデータがあるかどうかを検査します。これらの日には十分なデータが存在しないため、集計は実行されません。 ただし、4 月 13 日には、2 か月分のデータが存在します。WAAS Central Manager は、2 月のデータを集計し、2 月の毎日のデータ レコードを削除します。
System.monitoring.recordLimitDays	システムに保持するモニタリング データの最大日数。デフォルトは、1825 日です。
System.monitoring.timeFrameSettings	すべてのチャートを示すのに使用されるデフォルトの期間。ユーザが保存するデータは変更されません。デフォルトは、Last Hour です。
System.registration.autoActivation	Central Manager に登録されている WAAS および WAAS Express デバイスを自動的にアクティブにする自動アクティベーション機能のステータス。デフォルトは、true です（デバイスは自動的に登録されます）。
System.rpc.timeout.syncGuiOperation	Central Manager の WAE 接続との GUI 同期操作のタイムアウト（秒）。デフォルトは、50 秒です。
System.security.maxSimultaneousLogins	ユーザに許可される WAAS Central Manager の最大同時セッション数。同時セッションを無制限に許可する場合は 0（ゼロ、デフォルト）を指定します。セッションを終了するには、Central Manager からログオフする必要があります。ユーザがログオフせずにブラウザを閉じた場合、セッションは 120 分後にタイムアウトするまで閉じられません（タイムアウトは設定できません）。許可される並列セッションの数を超えた場合も、タイムアウトになるまで Central Manager GUI に再びアクセスできません。この設定は CLI から Central Manager デバイスへのアクセスには影響を及ぼしません。

表 10-4　システム設定プロパティの説明 （続き）

システム プロパティ	説明
System.security.webApplicationFilter	JavaScript、SQL、または制限された特殊文字の入力を拒否する Web アプリケーション フィルタのステータス。デフォルトは false です。
System.standby.replication.maxCount	スタンバイ Central Manager に複製される統計データ レコードの最大数（1,000 単位）。範囲は、10 ～ 300 です。デフォルトは、200（200,000 レコード）です。この数字を増やすことは推奨できません。
System.standby.replicationTimeout	スタンバイ Central Manager への複製を待つ最大秒数。範囲は、300 ～ 3600 秒です。デフォルトは、900 秒です。このタイムアウトを減らすことは推奨できません。

システム プロパティの値を表示または変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Configure] > [Global] > [System Properties] を選択します。[Config Properties] ウィンドウが表示されます

ステップ 2　変更するシステム プロパティの横にある [Edit] アイコンをクリックします。[Modifying Config Property] ウィンドウが表示されます。

ステップ 3　変更するシステム プロパティに応じて、ドロップダウン リストから、新しい値を入力するか、新しいパラメータを選択します。

ステップ 4　[Submit] をクリックして、設定を保存します。

Web アプリケーション フィルタの設定

Web アプリケーション フィルタは、WAAS Central Manager GUI をクロスサイト スクリプティング（XSS）攻撃から保護するセキュリティ機能です。XSS セキュリティ問題は、事前にコンテンツの検証またはエンコードを行わずに、ユーザから発信されたデータを Web ブラウザに送信すると生じる可能性があります。これにより、悪意のあるスクリプティングがクライアント ブラウザで実行され、データベースの整合性が損なわれる可能性があります。

このセキュリティ機能により、WAAS ユーザが送信するすべてのアプリケーション パラメータは、HTML ページに読み込まれる前に検査および/または符号化されることが確認されます。

ここでは、次の内容について説明します。

- 「Web アプリケーション フィルタの有効化」（P.10-21）
- 「セキュリティ検査」（P.10-22）

Web アプリケーション フィルタの有効化

Web アプリケーション フィルタを有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Configure] > [Global] > [System Properties] を選択します。[Config Properties] ウィンドウが表示されます

（注）　CLI を使用してこの機能を有効にすることはできません。この機能はデフォルトで無効に設定されています。

ステップ 2　system.security.webApplicationFilter 項目の横にある [Edit] アイコンをクリックします。

[Modifying Config Property] ウィンドウが表示されます。

ステップ 3　[Value] ドロップダウン リストから [true] を選択して、この機能を有効にします。

Central Manager および Device Manager ユーザに対し、この機能を有効にした後、ログアウトしてから再度ログインすることを勧める確認メッセージが表示されます。

ステップ 4　[OK] をクリックし、[Submit] をクリックします。

ステップ 5　ログアウトしてから再度ログインします。

セキュリティ検査

Web アプリケーション フィルタ機能では、入力検査とサニタイズという 2 つの方法を使用してセキュリティを検証します。入力検査では、データを受け入れる前にすべての入力データを検査します。サニタイズは、データ内にすでに存在する悪意のある設定やスクリプトが実行されることを防止します。

ここでは、次の内容について説明します。

- 「入力検査」（P.10-22）
- 「サニタイズ」（P.10-22）

入力検査

入力検査は、Central Manager および Device Manager データベースに入力されるすべてのデータをスキャンするもので、admin ユーザだけが設定できます。

Central Manager GUI を使用して送信されたデータに XSS の疑いがある場合はすべてブロックされます。入力がブロックされると、警告が表示されます

入力データは次の XSS フィルタ ルールと照合されます。

- セミコロン（;）が含まれる場合、入力は拒否されます。
- 山カッコ（<>）で囲まれている場合、入力は拒否されます。
- 上記のタグ（&#60、&#62、%3c、%3e）の生成に間接的に使用される可能性がある場合、入力は拒否されます。

サニタイズ

サニタイザは、データベースに対して XSS 攻撃があったときに、悪意のある設定やスクリプトがブラウザで実行されるのを防止します。ユーザはサニタイズを設定することはできません

Central Manager から送信された設定データに XSS の疑いがある場合は、[Device Groups] > [All Device Groups] ページに赤色で表示されます。

オフライン WAAS デバイスの高速検出の設定

オフライン デバイスの高速検出を有効にすると、オフライン WAAS デバイスを高速に検出できます。WAAS デバイスは、2 回以上のポーリング期間にわたって getUpdate（get configuration poll）要求で WAAS Central Manager にアクセスできない場合、オフラインとして宣言されます（この機能の詳細については、「オフライン デバイスの高速検出について」（P.10-24）を参照してください）。

オフライン WAAS デバイスの高速検出を設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Configure] > [Global] > [Fast Device Offline Detection] を選択します。[Configure Fast Offline Detection] ウィンドウが表示されます。

（注）　オフライン デバイス高速検出機能は、WAAS Central Manager がデバイスから最初の UDP ハートビート パケットと getUpdate 要求を受信するときだけ有効です。

ステップ 2　WAAS Central Manager でデバイスのオフライン ステータスをすばやく検出できるようにするには、[Enable Fast Offline Detection] チェックボックスをオンにします。

ステップ 3　[Heartbeat Rate] フィールドで、デバイスが UDP ハートビート パケットを WAAS Central Manager へ送信する必要がある頻度を秒で指定します。デフォルトは 30 秒です。

ステップ 4　[Heartbeat Fail Count] フィールドに、デバイスがオフラインと宣言される前にデバイスから WAAS Central Manager への送信中にドロップできる UDP ハートビート パケットの数を指定します。デフォルトは 1 です。

ステップ 5　[Heartbeat UDP Port] フィールドで、デバイスが UDP ハートビート パケットをプライマリ WAAS Central Manager へ送信するために使用するポート番号を指定します。デフォルトは、ポート 2000 です。

[Maximum Offline Detection Time] フィールドには、失敗したハートビート カウントとハートビート速度の積が表示されます。

最大オフライン検出時間 = 失敗したハートビート カウント X ハートビート速度

オフライン デバイスの高速検出機能を有効にしていない場合、WAAS Central Manager は、デバイスがオフラインと宣言される前に、デバイスが getUpdate 要求でアクセスされるまで 2 回以上のポーリング期間を待ちます。ただし、オフライン デバイスの高速検出機能を有効にすると、WAAS Central Manager は、[Maximum Offline Detection Time] フィールドに表示される値を超えるまで待ちます。

WAAS Central Manager がデバイスから Cisco Discovery Protocol（CDP）を受信すると、2 X（ハートビート速度）X（失敗したハートビート カウント）の期間の後で、WAAS Central Manager GUI にデバイスがオフラインとして表示されます。

ステップ 6　[Submit] をクリックします。

（注）　Central Manager で、Fast WAE 設定のオフライン検出ページを変更すると、デバイスが一時的にオフラインとして表示される場合があります。設定の変更がデバイスに反映されると、デバイスはオンラインとして再度表示されます。

オフライン デバイスの高速検出について

WAAS デバイスと WAAS Central Manager の通信に UDP を使用すると、オフラインになったデバイスをより高速に検出できます。UDP ハートビート パケットは、指定した間隔で WAAS ネットワーク内の各デバイスからプライマリ WAAS Central Manager へ送信されます。プライマリ WAAS Central Manager は、各デバイスから UDP ハートビート パケットを受信した最後の時刻を追跡します。WAAS Central Manager は、指定した個数の UDP パケットを受信しない場合、応答しないデバイスのステータスをオフラインとして表示します。UDP ハートビートは getUpdate 要求より必要な処理量が少ないため、より頻繁に送信でき、WAAS Central Manager はより高速にオフライン デバイスを検出できます。

この機能を有効または無効にする、2 個の UDP パケット間の間隔を指定する、および失敗したハートビート カウントを設定することができます。ハートビート パケット速度は、2 個の UDP パケットの間隔として定義されます。WAAS Central Manager GUI は、指定したハートビート パケット速度と失敗したハートビート カウントの値を使用して、ハートビート速度と失敗したハートビート カウントの積としてオフライン検出時間を表示します。オフライン デバイスの高速検出を有効にすると、WAAS Central Manager は、UDP をサポートしていないネットワーク セグメントに存在するデバイスを検出し、getUpdate（get configuration poll）要求を使用してオフライン デバイスを検出します。

デフォルトで、オフライン デバイスの高速検出機能は無効になっています。

アラーム過負荷検出の設定

WAAS デバイスは、Node Health Manager からの着信アラーム レートを追跡できます。着信アラーム レートが最高水準点（HWM）を超えると、WAAS デバイスはアラーム過負荷状態になります。この状況は、複数のアプリケーションがエラー条件を報告するために同時にアラームを上げると発生します。WAAS デバイスがアラーム過負荷状態になると、次の状況が発生します。

- それ以降のアラーム発信およびクリア動作に関する SNMP トラップは、一時停止されます。raise alarm-overload アラームと clear alarm-overload アラームに対応するトラップが送信されます。ただし、raise alarm-overload アラームが発信されてから clear alarm-overload アラームが発信されるまでの間に行われたアラーム動作に関するトラップは一時停止されます。
- アラーム過負荷発信およびクリア通知は、ブロックされません。アラーム過負荷状態は、SNMP と構成管理システム（CMS）に伝達されます。ただし、アラーム過負荷状態では、SNMP と CMS に個々のアラームは通知されません。情報は、CLI を使用しないと入手できません。
- アラーム レートが最低水準点（LWM）を下回るレベルまで減少するまで、WAAS デバイスはアラーム過負荷状態のままです。
- 着信アラーム レートが LWM より下がると、WAAS デバイスはアラーム過負荷状態から出て、アラーム カウントを SNMP と CMS に報告し始めます。

WAAS デバイスがアラーム過負荷状態にある場合、Node Health Manager は、WAAS デバイスで上げられるアラームを記録し、着信アラーム レートを追跡し続けます。WAAS デバイスで上げられるアラームは、『*Cisco Wide Area Application Services Command Reference*』に説明されている **show alarm** CLI コマンドを使用して表示できます。

WAAS デバイス（またはデバイス グループ）のアラーム過負荷検出を設定するには、次の手順を実行します。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Monitoring] > [Alarm Overload Detection] を選択します。[Alarm Overload Detection Settings] ウィンドウが表示されます。

ステップ 3　複数のアプリケーションがエラー条件を報告したときに、WAAS デバイス（またはデバイス グループ）がアラーム発信とクリア動作を一時停止するように設定しない場合は、[Enable Alarm Overload Detection] チェックボックスの選択を解除します。このチェックボックスは、デフォルトでオンになっています。

ステップ 4　[Alarm Overload Low Water Mark (Clear)] フィールドで、それより下がると WAAS デバイスがアラーム過負荷状態から出る 1 秒あたりの着信アラーム数を入力します。

最低水準点とは、アラームを再起動する前にアラームの数が下がる必要がある最低水準です。デフォルト値は、1 です 最低水準点は、最高水準点値未満でなければなりません。

ステップ 5　[Alarm Overload High Water Mark (Raise)] フィールドで、それを超えると WAAS デバイスがアラーム過負荷状態に入る 1 秒あたりの着信アラーム数を入力します。デフォルト値は 10 です。

ステップ 6　[Submit] をクリックして、設定を保存します。

CLI からアラーム過負荷検出を設定するには、**alarm overload-detect** グローバル コンフィギュレーション コマンドを使用します。

E メール通知サーバの設定

レポートを定期的に生成するようスケジュールし、レポートが生成されたときに、レポートへのリンクを 1 人または複数の受信者に E メール送信することが可能です （詳細については、「レポートの管理」（P.17-45）を参照してください）。

E メール通知を有効にするには、次の手順に従って、WAAS Central Manager に E メール サーバ設定を構成する必要があります。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*] を選択します。Central Manager デバイスを選択する必要があります。

ステップ 2　[Configure] > [Monitoring] > [Email Notification] を選択します。[Configure Email Server Details] ウィンドウが表示されます

ステップ 3　[Mail Server Hostname] フィールドに、E メール送信に使用される SMTP E メール サーバのホスト名を入力します。

（注）　SMTP メール サーバだけがサポートされています。他の種類のメール サーバを設定した場合、E メール通知は失敗します。

ステップ 4　[Mail Server Port] フィールドに、ポート番号を入力します。デフォルトは、ポート 25 です。

ステップ 5　[Server Username] フィールドに、有効な E メール アカウントのユーザ名を入力します。

ステップ 6　[Server Password] フィールドに、E メール アカウントのパスワードを入力します。

ステップ 7　[From Address] フィールドに、E メール通知の送信者として表示される E メール アドレスを入力します。

ステップ 8　[Submit] をクリックします。

IPMI over LAN の使用

インテリジェント プラットフォーム管理インターフェイス（IPMI）over LAN は、WAVE-294/594/694/7541/7571/8541 アプライアンスのリモート プラットフォーム管理サービスを提供します。IPMI は、管理者がハードウェアおよびセンサーをモニタし、システム コンポーネントを制御し、重要なシステム イベントのログを取得してリモート管理およびリカバリを実行する方法を定義する、オープンな標準テクノロジーです。IPMI はベースボード管理コントローラ（BMC）上で実行され、WAAS とは独立して動作します。IPMI over LAN を設定し、WAAS 上で有効にすると、WAAS が応答不能になった場合やデバイスの電源がオフになっている（ただし、電源に接続されている）場合であっても、許可されたユーザは BMC にリモートからアクセスできます。IPMI v2 準拠の管理ユーティリティ（ipmitool、OSA SMbridge など）を使用して BMC にリモートから接続して、IPMI の操作を実行できます。

IPMI over LAN 機能は、次のリモート プラットフォーム管理サービスを提供します。

- WAAS アプライアンスの電源オン、電源オフ、および電源再投入のサポート。
- 現場交換可能ユニット（FRU）の情報を調べ、センサーの値を読み取ることによる、WAAS ハードウェア コンポーネントのヘルスのモニタ。
- 重要なシステム イベントのログを取得して、リモート管理およびリカバリを実行。
- IPMI セッションを介した、WAAS アプライアンスへのシリアル コンソール アクセスのサポート。
- IPMI Serial over LAN（SoL）のサポート：IPMI SoL は、リモート ユーザが IPMI セッションでシリアル コンソールを使用して WAAS アプライアンスにアクセスすることを可能にします。

IPMI over LAN 機能および IPMI SoL 機能は CLI コマンドを使用して設定することができ、以下を含みます。

- IPMI LAN インターフェイスの設定
- IPMI LAN ユーザの設定
- リモート IPMI アクセスのためのセキュリティ設定
- IPMI over LAN の有効化 / 無効化
- IPMI SoL の有効化 / 無効化
- BMC LAN チャネルのデフォルト設定の復元
- 現在の IPMI over LAN 設定および IPMI SoL 設定の表示

IPMI over LAN の設定の詳細については、「BMC の設定によるリモート プラットフォーム管理」（P.10-27）を参照してください。

BMC ファームウェア アップデート

IPMI over LAN を使用するには、特定の BMC ファームウェア バージョンがデバイスにインストールされている必要があります。サポートされる最小 BMC ファームウェア バージョンは、次のとおりです。

- WAVE-294/594/694—48a
- WAVE-7541/7571/8541—26a

WAAS バージョン 4.4.5 以降とともに工場から出荷された WAAS アプライアンスには、正しいファームウェアが必ずインストールされています。以前のバージョンの WAAS ソフトウェアとともに出荷されたデバイスを更新する場合は、BMC ファームウェアを更新する必要があります（以前に更新されていない限り）。

正しいファームウェア バージョンを実行しているかどうかを判断するには、**show bmc info** コマンドを使用します。次の例では、デバイス（ここでは 48a）に最新の BMC ファームウェア バージョンがインストールされていることが表示されています。

```
wave# show bmc info
Device ID                 : 32
Device Revision           : 1
Firmware Revision         : 0.48                    <<<<< version 48
IPMI Version              : 2.0
Manufacturer ID           : 5771
Manufacturer Name         : Unknown (0x168B)
Product ID                : 160 (0x00a0)
Product Name              : Unknown (0xA0)
Device Available          : yes
Provides Device SDRs      : no
Additional Device Support :
    Sensor Device
    SDR Repository Device
    SEL Device
    FRU Inventory Device
Aux Firmware Rev Info     :
    0x0b
    0x0c
    0x08
    0x0a                                            <<<<< a
. . .
```

BMC ファームウェア アップデートが必要な場合は、cisco.com の [Wide Area Application Service (WAAS) Firmware] ダウンロード ページ（登録済みのお客様のみ）からダウンロードできます。ファームウェアのバイナリ イメージの名前は waas-bmc-installer-48a-48a-26a-k9.bin です。あるいは、新しいバージョンを使用できる場合があります。使用可能な最新のファームウェア更新を使用してください。

次のコマンドを使用して、ネットワーク上の FTP を介して使用可能なイメージ ファイルから、ファームウェアを更新できます。

copy ftp install *ip-address remotefiledir* **waas-bmc-installer-48a-48a-26a-k9.bin**

アップデート プロセスが BMC ファームウェアのヘルス ステータスを自動的に確認します。BMC ファームウェアの破損が検出された場合、BMC は BMC ファームウェア アップデート手順中に回復されます。更新プロセスは全体で数分かかります。デバイスは応答不能として表示される場合がありますが、プロセスを中断したり、デバイスの電源を再投入しないでください。更新が完了した後には、デバイスをリロードする必要があります。

デバイスがリブートしたら、**show bmc info** コマンドを使用して、ファームウェア バージョンを確認できます。

BMC のリカバリおよび BMC ファームウェアの更新を行うと、BMC の出荷時の初期状態が復元され、現在のすべての IPMI over LAN 設定が消去されます。

BMC ファームウェアの破損が起こった場合は、クリティカル アラームが発生します。

BMC の設定によるリモート プラットフォーム管理

この項では、IPMI over LAN および IPMI SoL を有効にしてリモート プラットフォーム管理を実行するために必要な最小限の手順について説明します。この項では、次のトピックについて取り上げます。

- IPMI over LAN の有効化
- IPMI SoL の有効化

IPMI over LAN の有効化

IPMI over LAN を有効にするには、**bmc lan** コマンドを使用して次の手順を実行します。

ステップ 1　デフォルトの BMC LAN IP アドレスを変更します。

ステップ 2　BMC デフォルト ユーザ（user 2）のパスワードを変更します。

ステップ 3　IPMI over LAN を有効にします。

ステップ 4　番号 2 のユーザのユーザ名およびパスワードを使用し、IPMI セッション v2.0 を介してリモート クライアントから BMC にアクセスします。BMC へのアクセスに使用されるデフォルトの暗号スイートは 3 です。これは、RAKP-HMAC-SHA1 認証アルゴリズム、HMAC-SHA1-96 整合性アルゴリズム、および AES-CBC-128 暗号化アルゴリズムを指定します。

ステップ 5　BMC over a IPMI セッション v1.5 にアクセスするには、user 2 の IPMI セッション バージョン設定を v2.0 から v1.5 に変更します。

IPMI SoL の有効化

IPMI SoL を有効にするには、次の手順を実行します。

ステップ 1　WAAS デバイス上で IPMI over LAN（IoL）を設定し、有効にします。

ステップ 2　リモート クライアント上で、BMC ユーザが IPMI セッション v2.0 を介して IoL 操作を正常に実行できることを確認します。

ステップ 3　リモート クライアント上で、WAAS コンソールのボー レートの 9600 bps と一致するように、端末のボー レートを変更します。

ステップ 4　WAAS デバイス上で IPMI SoL を有効にします。

ステップ 5　IPMI 管理ツールが ipmitool の場合は、リモート クライアント上で次のコマンドを使用して、特定の BMC ユーザの SoL ペイロード ステータスを確認します。
ipmitool -I lanplus -H *bmc-ip-address* **-U** *bmc-user-name* **sol payload status 1** *bmc-user-userid*

次に例を示します。

```
# ipmitool -I lanplus -H 2.1.4.70 -U user3 sol payload status 1 3
Password:
User 3 on channel 1 is disabled
```

ステップ 6　このユーザの SoL ペイロードが無効になっている場合は、次のコマンドを使用して、このユーザの SoL ペイロードを有効にします。
ipmitool -I lanplus -H *bmc-ip-address* **-U** *bmc-user-name* **sol payload enable 1** *bmc-user-userid*

次に例を示します。

```
# ipmitool -I lanplus -H 2.1.4.70 -U user3 sol payload enable 1 3
Password:
# ipmitool -I lanplus -H 2.1.4.70 -U user3 sol payload status 1 3
Password:
User 3 on channel 1 is enabled
```

ステップ 7　リモート クライアント上で次のコマンドを使用して、WAAS デバイスへのシリアル コンソールを開きます。
ipmitool -I lanplus -H *bmc-ip-address* **-U** *bmc-user-name* **sol activate**

ステップ 8　これで、リモート クライアント上で WAAS デバイスのコンソール セッションを開始しました。終了したら、~. の エスケープ文字を使用して、接続を終了します。

Cisco IOS ルータ デバイスの管理

WAAS Central Manager を使用して、WAAS Express および AppNav-XE デバイスを管理できます。これらは、両方とも WAAS 関連ソフトウェアを使用して展開された Cisco IOS ルータです。[Central Manager] メニューは、これらのデバイスが WAAS アプライアンス機能のサブセットを実装する際に、WAAS Express または AppNav-XE デバイスがコンテキストとして選択されたときに、フル メニューのサブセットを表示します。

Central Manager と Cisco IOS Express デバイスは HTTPS プロトコルを使用して通信します。WAAS Central Manager と Cisco IOS ルータ デバイス間の通信を確立するには、Cisco IOS ルータ デバイスを Central Manager に登録する必要があります。Central Manager GUI を使用して Cisco IOS ルータ デバイスを登録するのが最も簡単な方法です。

この項では、次のトピックについて取り上げます。

Central Manager GUI を使用した Cisco IOS ルータ デバイスの登録

Cisco IOS ルータ デバイスを登録するには、次の手順に従ってください。

ステップ 1　[WAAS Central Manager] メニューから、[Admin] > [Registration] > [Cisco IOS Routers] を選択します。[Cisco IOS Router Registration] ウィンドウが表示されます。

（注）　Central Manager GUI を使用して Cisco IOS ルータ デバイスを登録するには、SSH がルータで有効になっている必要があります。

ステップ 2　[IP Address（es）] フィールドに、登録するルータの IP アドレスをカンマで区切って入力します。IP アドレス、ホスト名、ルータのタイプ、およびステータスが、[Registration Status] テーブルに表示されます。

また、登録する IP アドレスのリストを含む CSV ファイルをアップロードすることもできます。リストをアップロードするには、[Import CSV file] オプション ボタンをクリックし、[Choose File] ボタンをクリックし、ファイルを参照して [Open] クリックします。各 IP アドレスは別々の行にある必要があります。

ステップ 3　ユーザ名、パスワード、および有効化パスワードを入力して、ルータのログイン クレデンシャルを設定します。ルータでユーザを作成する必要がある場合は、「ユーザの設定」（P.10-31）を参照してください。

ステップ 4　[HTTP Authentication Type] で、[local] または [AAA] を選択します。

ステップ 5　Central Manager の [IP Address] フィールドに、Central Manager に使用するルータの IP アドレスを入力します。このフィールドは、当初は現在の Central Manager の IP アドレスが入力されますが、NAT 環境ではこの設定を変更する必要がある場合があります。

ステップ 6　[Register] ボタンをクリックし、登録ステータスが成功になったことを確認します。

結果はログ ファイル（/local/local1/errlog/waasx-audit.log）で表示できます。

Cisco IOS ルータ デバイスが正しく登録されると、Central Manager は、そのデバイスを登録ステータス テーブルとすべてのデバイス リストに表示します。

Cisco IOS ルータ デバイスにソフトウェア ライセンスをインストールする必要がある場合があります。詳細については、「ルータでのライセンスのインストール」（P.10-34）を参照してください。

ルータ クレデンシャルの設定

Central Manager が Cisco IOS ルータ デバイスにアクセスする場合は、Central Manager でルータ クレデンシャルを設定する必要があります。

Central Manager では、すべての Cisco IOS ルータ デバイスに適用されるグローバル クレデンシャルを定義できます。あるいは [Admin] > [Authentication] > [WAAS Express Credentials/AppNav-XE Credentials] メニュー項目を使用することにより、デバイス グループまたは個々のデバイス レベルでクレデンシャルを定義できます。デバイス グループまたは個々のデバイスのクレデンシャルを設定するには、まず Cisco IOS ルータ登録プロセスを完了してから、ルータ デバイス グループまたはデバイスのクレデンシャルを設定する必要があります。デバイスのクレデンシャルとデバイス グループのクレデンシャルは、グローバル クレデンシャルよりも優先されます。

グローバル ルータ クレデンシャルを設定するには、次の手順に従ってください。

ステップ 1　[WAAS Central Manager] メニューから、[Admin] > [Security] > [Cisco IOS Router Global Credentials] を選択します。[Cisco IOS Router Global Credentials] ウィンドウが表示されます。

ステップ 2　[Username] フィールドに、Cisco IOS ルータで定義されているユーザ名を入力します。ルータでユーザを作成する必要がある場合は、「ユーザの設定」（P.10-31）を参照してください。

（注）　Cisco IOS ルータ デバイスで HTTP サーバに対してローカルまたは AAA 認証を使用していない場合、つまり、デフォルトの HTTP サーバ設定である **ip http authentication enable** を使用する場合、[Username] フィールドの指定は任意です。（「ルータでの HTTP セキュア サーバの有効化」（P.10-34）を参照）。

ステップ 3　[Password] フィールドに、指定したユーザ名のパスワードを入力します。

ステップ 4　[Submit] をクリックします。

（注）　Central Manager でルータ クレデンシャルを変更しても、ルータ デバイス自体の設定値は変更されません。影響を受けるのは、Central Manager に保存されているルータ クレデンシャルだけです。

CLI を使用した Cisco IOS ルータの登録

表 10-5 に示されている手順を実行することにより、CLI を使用して Central Manager に Cisco IOS ルータ デバイスを登録することもできます。この手順は、WAAS Express と AppNav-XE の両方を実行する Cisco IOS ルータに適用されます。

表 10-5　CLI を使用して Cisco IOS ルータを登録するためのチェックリスト

作業	追加情報と手順
1. ユーザ名とパスワードを設定します。	ルータと Central Manager に同じユーザ名とパスワードが設定されるので、Central Manager は管理目的でルータにログインできます。 詳細については、「ユーザの設定」（P.10-31）を参照してください。
2. プライマリ Central Manager 管理サーバ証明書をルータにインポートします。	ルータはセキュア HTTPS サーバの通信に Central Manager 証明書が必要です。 詳細については、「Central Manager 証明書のインポート」（P.10-32）を参照してください。
3. ルータ証明書を設定します。	Central Manager デバイスは、セキュア HTTPS サーバの通信用にこのルータ証明書を要求します。 詳細については、「ルータ証明書の設定」（P.10-33）を参照してください。
4. ユーザ認証を使用して、セキュア HTTP サーバを有効にします。	Central Manager とルータの通信を有効にします。 詳細については、「ルータでの HTTP セキュア サーバの有効化」（P.10-34）を参照してください。
5. 永久 WAAS ソフトウェア ライセンスをインストールします。	WAAS Express ソフトウェアがルータ上で動作できるようになります。 詳細については、「ルータでのライセンスのインストール」（P.10-34）を参照してください。
6. NTP サーバを設定します。	ルータと Central Manager の間で時間の同期を維持します。 詳細については、「NTP サーバの設定」（P.10-35）を参照してください。
7. ルータを Central Manager に登録します。	ルータを Central Manager に登録します。 詳細については、「ルータの登録」（P.10-35）を参照してください。

以降では、これらの手順について詳しく説明します。

ユーザの設定

ルータと Central Manager が通信するために設定する最初の手順は、ルータと Central Manager で同じユーザを設定することです。

ユーザを設定するには、次の手順を実行します。

ステップ 1　ルータ CLI にログインします。

ステップ 2　**username** IOS コンフィギュレーション コマンドを使用して、ルータ上で特権レベル 15 を持つローカル ユーザを設定します。

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#username cisco privilege 15 password 0 cisco
router(config)#exit
```

あるいは、外部 TACACS+ または RADIUS ユーザを設定することができます。詳細はこの手順の後の説明を参照してください。

ステップ 3　実行コンフィギュレーションを保存します。

```
router#write memory
Building configuration...
[OK]
```

ステップ 4　WAAS Central Manager で、「ルータ クレデンシャルの設定」（P.10-30）に記載されている説明に従って、ルータ クレデンシャルを設定します。

ルータで外部 TACACS+ ユーザを設定するには、ルータで次のコンフィギュレーション コマンドを使用します。

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login default group tacacs+
router(config)#aaa authorization exec default group tacacs+
router(config)#tacacs-server host host-ip
router(config)#tacacs-server key keyword
```

ルータで外部 RADIUS ユーザを設定するには、ルータで次のコンフィギュレーション コマンドを使用します。

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login default group radius
router(config)#aaa authorization exec default group radius
router(config)#radius-server host host-ip
router(config)#radius-server key keyword
```

TACACS+ または RADIUS の外部認証サーバは Cisco ACS 4.x または 5.x の必要があります。

Central Manager 証明書のインポート

次の手順では、Central Manager からルータに証明書をインポートします。

証明書をインストールするには、次の手順を実行します。

ステップ 1　Central Manager CLI にログインします。

ステップ 2　次のように show crypto EXEC コマンドを使用して、管理証明書を表示します。

```
waas-cm#show crypto certificate-detail admin

...
-----BEGIN CERTIFICATE-----
TIICezCCAeSgAwIBAgIEVwMK8zANBgkqhkiG9w0BAQUFADCBgTELMAkGA1UEBhMC
VVMxEzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMQ0wCwYD
VQQLEwRDTkJVMRswGQYDVQQKExJDaXNjbyBTeXN0ZW1zLCBJbmMxHjAcBgNVBAMT
FWRvYy13YWFzLWNtLmNpc2NvLmNvbTAeFw0wODA3MjQxOTMwMjNaFw0xMzA3MjMx
OTMwMjNaMIGBMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTERMA8G
A1UEBxMIU2FuIEpvc2UxDTALBgNVBAsTBENOQlUxGzAZBgNVBAoTEkNpc2NvIFN5
c3RlbXMsIEluYzEeMBwGA1UEAxMVZG9jLXdhYXMtY20uY2lzY28uY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQCy10xBfsUDTh5imYwkkterx/IqkNQO7KB/
M0wqIK2j4zj4BpR1ztKaFyEtGjqGpxPBQ54V9EHGmGUljx/Um9PORk3AXyWoUsDf
o0T2Z94FL5UoVUGzUia6/xiUrPCLNf6BLBDGPQg970QtZSU+DYUqjYHzDgv6yXFt
```

```
viHARbhZdQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADKF7aIeQ+Uh4Y2zZJwlaIF7
ON+RqDvtyy4DNerEN9iLI4EFO/QJ+uhChZZU8AKR8u3OnLPSNtNck33OWwMemcOd
QGhnsMtiUq2VuSh+A3Udm+sMLFguCw5RmJvqKTrj3ngAsmDBW3uaK0wkPGp+y3+0
2hUYMf+mCrCOwBEPfs/M
-----END CERTIFICATE-----
```

ステップ 3　証明書テキストの、出力の BEGIN CERTIFICATE と END CERTIFICATE 行の間の部分をコピーします。

ステップ 4　ルータ CLI にログインします。

ステップ 5　次のようにして、Central Manager の証明書を設定します。

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#crypto pki trustpoint wcm

router(ca-trustpoint)#enrollment terminal pem
router(ca-trustpoint)#exit
router(config)#crypto pki authenticate wcm

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

ステップ 6　ステップ 3 で Central Manager からコピーした証明書を貼り付けます。

ルータ証明書の設定

ルータは、HTTPS 通信の確立時に Central Manager によって要求される証明書が必要です。この手順ではルータに永続的な自己署名証明書を設定する方法を説明していますが、CA 署名付き証明書を使用することもできます。

ルータ証明書を設定するには、次の手順に従ってください。

ステップ 1　ルータ CLI にログインします。

ステップ 2　ルータの自己署名証明書を作成します。

（注）　CSCsy03412 により、証明書を登録する前に、**ip domain name** *name* を設定する必要があります。**ip domain name** を設定しなかった場合、IOS はリロード時に自己署名証明書を再生成します。これは、WAAS Central Manager との通信に影響を及ぼします。

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#crypto pki trustpoint local
router(ca-trustpoint)#enrollment selfsigned
router(ca-trustpoint)#subject-alt-name routerFQDN
router(ca-trustpoint)#exit
router(config)#crypto pki enroll local
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 10.10.10.25
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

ルータが Central Manager に登録された後にルータ証明書を変更した場合は、Central Manager に証明書を再インポートする必要があります。詳細については、「ルータ デバイス証明書の再インポート」（P.10-35）を参照してください。

ルータでの HTTP セキュア サーバの有効化

Central Manager とルータは HTTPS プロトコルを使用して通信します。ルータで HTTP セキュア サーバを有効にする必要があります。

HTTP セキュア サーバを有効にするには、次の手順を実行します。

ステップ 1　ルータで、HTTP セキュア サーバを有効にします。

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip http secure-server
```

ステップ 2　次のようにして、ローカル ユーザの HTTP サーバ用認証を設定します。

```
router(config)#ip http authentication local
```

外部 TACACS+ または RADIUS のユーザ認証を使用している場合、次のようにして HTTP サーバの認証を設定します。

```
router(config)#ip http authentication aaa
```

（注）　HTTP サーバにローカルまたは AAA 認証を設定しなかった場合は、有効化パスワードのみが認証に使用されます。（デフォルトは **ip http authentication enable** であり、有効化パスワードのみを使用し、ユーザ名は使用しません）。このデフォルト設定が使用されている場合、Central Manager 上のルータにユーザ名クレデンシャルを定義する必要はありません。（「ユーザの設定」（P.10-31）を参照）。

ルータでのライセンスのインストール

ルータには、WAAS Express または AppNav-XE ソフトウェアを実行するために 1 つ以上のライセンスが必要です。詳細については、ルータのマニュアルを参照してください。

ライセンスをインストールするには、次の手順に従ってください。

ステップ 1　ルータ上の **license** コマンドにアクセス可能な場所に、適切なライセンスを取得してコピーします。

ステップ 2　ルータで、ライセンスをインストールします。

```
router#license install ftp://infra/licenses/FHH122500AZ_20100811190225615.lic
```

この例ではライセンスの取得とインストールに FTP を使用していますが、このコマンドにはさまざまなオプションを使用できます。展開に最適なオプションを選択してください。

ステップ 3　実行コンフィギュレーションを保存します。

```
router#write memory
Building configuration...
[OK]
```

NTP サーバの設定

WAAS ネットワーク内のデバイス間で時刻の同期を保つことが重要です。すでに Central Manager 用に設定された NTP サーバがある必要があります（「NTP 設定の構成」（P.10-5）を参照）。

ルータに対して NTP サーバを設定するには、次のようにルータで **ntp server** グローバル コンフィギュレーション コマンドを使用します。

```
router#config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ntp server 10.10.10.55
```

ルータの登録

Central Manager を使用したルータの設定の最後の手順は、デバイスの登録です。Central Manager の IP アドレスを確認しておく必要があります。

ルータを Central Manager に登録するには、次の手順に従ってください。

ステップ 1　WAAS-Express ルータの場合、次のように Central Manager に登録します。

```
router#waas cm-register https://CM_IP_Address:8443/wcm/register
```

AppNav-XE ルータの場合、次のように Central Manager に登録します。

```
router#appnav cm-register https://CM_IP_Address:8443/wcm/register
```

このコマンドの URL に、示されているとおりに Central Manager IP アドレスを指定します。必ず、コロンとポート番号 8443 を指定してください。

永久 WAAS ライセンスがルータにインストールされていない場合は、評価ライセンスを継続する条項に同意する必要があります。評価ライセンスの有効期限は 60 日間です。

ステップ 2　実行コンフィギュレーションを保存します。

```
router#write memory
Building configuration...
[OK]
```

Central Manager にルータを正しく登録すると、Central Manager は、最初に管理ステータスが [Pending] で、ライセンス ステータスが [Active] であるデバイスを [Manage Devices] ページに表示します。Central Manager がデバイスの設定とステータスを取得すると、管理ステータスは [Online] に変わり、ライセンス ステータスは [Permanent]（または [Evaluation]、[Expires in x weeks y days]）に変わります。

ルータ デバイス証明書の再インポート

Central Manager にルータ デバイスを登録した後に、ルータ デバイス証明書を変更した場合は、一致する証明書を Central Manager に再インポートする必要があります。

ルータ デバイス証明書を再インポートするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*] を選択します。

ステップ 2　[Admin] > [Authentication] > [Identity Certificate] を選択します。[Certificate] ウィンドウが表示されます。

[Certificate Info] タブに、デバイスの証明書情報が表示されます。[Certificate in PEM Encoded Format] タブに、PEM 形式の証明書が表示されます。このタブから証明書をコピーして、次の手順の貼り付け操作で使用できます。

ステップ 3　タブの上部に表示されている次のオプション ボタンのいずれかを選択して、選択した証明書を Central Manager にインポートします。

- [Upload PEM file] : [Choose File] をクリックし、証明書を含む PEM ファイルを検出します。
- [Manual] : 表示されるテキスト フィールドに PEM エンコード証明書を貼り付けます。

ステップ 4　[Submit] をクリックします。