CHAPTER 9

その他のシステム設定の構成

この章では、WAAS デバイスの基本設定を実行した後、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。

（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」は、WAE アプライアンスおよび WAE ネットワーク モジュール（NME-WAE デバイス ファミリ）を示します。

この章の構成は、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 GUI ナビゲーション ペインで、**[My WAN] > [Manage Devices]** を選択します。

ステップ 2　変更したいデバイスの横にある **[Edit]** アイコンをクリックします。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、*[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 4　[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。
  - 次の文字は違法と見なされ、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を解除します。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。

（注）　WAE が非透過モードで動作していて、プリント サービスが有効である場合、[Name] フィールドに入力するデバイスの NetBIOS 名およびホスト名には同一の名前を設定する必要があります。

ステップ 5　[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。このデバイス用の新しい位置を作成するには、「位置の作成」（p.3-17）を参照してください。

ステップ 6　[NAT Configuration] 見出しの下で、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。
- 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。

（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 7　[Comments] フィールドに、このデバイスに表示したいコメントを入力します。

ステップ 8　**[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 9-1 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 9-1　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、CIFS（WAFS）、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	バーチャライゼーション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 から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 GUI ナビゲーション ペインで、**[My WAN] > [Manage Devices]** を選択します。

ステップ 2　変更したいデバイスの横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [License Management]** を選択します。

ステップ 4　追加したい各ライセンスにの横にあるチェック ボックスを選択します。

ステップ 5　**[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 サービスの有効化

Remote Copy Protocol（RCP; リモート コピー プロトコル）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。User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用する TFTP と異なり、RCP は接続指向の 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 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 GUI ナビゲーション ペインで、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　RCP サービスを有効にしたいデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Inted RCP]** を選択します。[Inetd RCP Settings] ウィンドウが表示されます。

ステップ 4　**[Inetd Rcp Enable]** チェック ボックスを選択します。このオプションはデフォルトで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 5　**[Submit]** をクリックして、変更を保存します。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤い色で表示されます。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のみ表示されます。

Inetd FTP サービスの有効化

Inetd 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 GUI ナビゲーション ペインで、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　Inetd FTP サービスを有効にしたいデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Inted FTP]** を選択します。[Inetd FTP Settings] ウィンドウが表示されます。

ステップ 4　**[Inetd Enable FTP Service]** チェック ボックスを選択して、デバイスまたはデバイス グループで Inetd FTP サービスを有効にします。このオプションはデフォルトで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。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤い色で表示されます。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のみ表示されます。

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 Network Time Protocol（NTP; ネットワーク タイム プロトコル）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。

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 GUI ナビゲーション ペインで、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　設定したいデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーションペインで、**[Configure] > [Data/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 4　**[Enable]** チェック ボックスを選択して、NTP 設定を有効にします。このオプションはデフォルトで無効になっています。

ステップ 5　[NTP Server] フィールドに、ホスト名または IP アドレスを入力します。

ステップ 6　**[Submit]** をクリックします。

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 GUI ナビゲーション ペインで、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　時間帯を設定したいデバイスまたはデバイス グループの横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Configure]** > **[Data/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 4　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 9-2 を参照してください）。

ウィンドウがリフレッシュされ、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. 時間帯の領域を選択します。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 9-3 を参照してください。

ステップ 5　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 6　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. 絶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、複数年にわたって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、夏時間が開始し、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。必要なら、[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、夏時間が月の最初の週に開始し、**[last]** を選択すると、夏時間が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、夏時間が月の最初の週に終了し、**[last]** を選択すると、夏時間が月の最後の週に終了するように設定できます。

i. [End 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 7　[Start Time] ドロップダウン リストから、夏時間が開始する必要がある時（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、夏時間が終了する必要がある時（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 8　[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 9-3 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 9　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 10　**[Submit]** をクリックして、設定を保存します。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤い色で表示されます。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のみ表示されます。

表 9-2　時間帯地域の略号

時間帯	時間帯名
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
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	世界標準時
UTC	世界標準時
WET	西ヨーロッパ標準時
W-SU	中央ヨーロッパ標準時

表 9-3　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

表 9-3　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/Baku	+4
Asia/Bangkok	+7
Asia/Colombo	+6
Asia/Dacca	+6
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

表 9-3　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）
Japan	+9
Pacific/Auckland	+12
Pacific/Fiji	+12
Pacific/Guam	+10
Pacific/Kwajalein	–12
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 Greenwich Mean Time（GMT; グリニッジ標準時）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 ストアの設定

セキュア ストア暗号化は、WAAS システムのためのより強力な暗号化とキー管理を提供します。WAAS Central Manager と WAE デバイスは、パスワードの処理、暗号キーの管理、およびデータの暗号化にセキュア ストア暗号化を使用します。

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 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、CIFS パスワード、およびユーザ ログイン パスワードが含まれます。

セキュア ストア暗号化を有効にするには、Central Manager でパスワードを入力する必要があります。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、キー暗号化キーを使用して、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、WAFS ユーザ クレデンシャルの暗号化と保存などの WAAS 機能で使用されます。

セキュア ストアが Central Manager で有効な場合、データは、SHA1 ハッシュと AES 256-ビット アルゴリズムを使用して、入力されたパスワードから生成された 256-ビット キー暗号化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 キー暗号化キーを使用して暗号化されます。

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 Managers 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、次の手順に従います。

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）。

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）。

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）。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）　Central Manager をリブートした場合、セキュア ストア暗号化を手動で再有効化する必要があります。リモート WAE デバイスのディスク暗号化機能および CIFS 事前配置機能は、Central Manager でセキュア ストア パスワードを入力して、セキュア ストア暗号化を再度有効化するまで動作しません。

セキュア ストアが有効な場合、次のシステムの特性に影響します。

- 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。
- 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）。
- 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キーを使用して暗号化されます。
- バックアップ スクリプトは、バックアップの実行時に、デバイスのセキュア ストア モード ステータスをバックアップします。バックアップは、Central Manager 上でのみサポートされています。
- 復元スクリプトは、バックアップ ファイルのセキュア ストア モードが有効であるかどうかを確認します。バックアップ ファイルがセキュア ストア モードである場合は、デバイスを確認し復元するために、パス フレーズを入力する必要があります。復元は、Central Manager 上でのみサポートされています。
- 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 永続ストレージにストアされているデータにアクセスできるようになります。
- セキュア ストアがアクティブな場合、セキュア ストア モードをサポートしていない旧バージョンの WAAS ソフトウェアにはダウングレードできません。旧バージョンの WAAS ソフトウェアをインストールする前に、セキュア ストア モードを無効にする必要があります。
- 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（「ディスク暗号化の有効化」[p.15-31] を参照）。

Central Manager でのセキュア ストア暗号化の有効化

Central Manager でセキュア ストア暗号化を有効化するには、CLI を使用して、**cms secure-store init** EXEC モード コマンドおよび **cms secure-store open** EXEC モード コマンドを実行します。

ステップ 1　**cms secure-store init** コマンドを入力します。

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

ステップ 2　パスワードを入力し、Enter キーを押します。確認のため、プロンプトでパスワードを再度入力します。

セキュア ストアが起動します。ただし、Central Manager 上のデータはまだセキュア ストア暗号化では暗号化されていません。システムは引き続き、以前の暗号化モードを使用しています。

ステップ 3　**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。

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 キーを押します。

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）　Central Manager をリブートした場合は常に、セキュア ストア暗号化を手動で再有効化する必要があります。リモート WAE デバイスのディスク暗号化機能および CIFS 事前配置機能は、Central Manager でセキュア ストア パスワードを入力して、セキュア ストア暗号化を再度有効化するまで動作しません。

（注）　プライマリ Central Manager のセキュア ストアを有効にした場合は、同様にスタンバイ 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.9-15] を参照）。

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の取得を可能にするだけで、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。

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、最初にプライマリ Central Manager でセキュア ストアを有効にしてから、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.9-15] を参照）。

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 キーを押します。

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 ごとに手順 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、次の手順に従います。

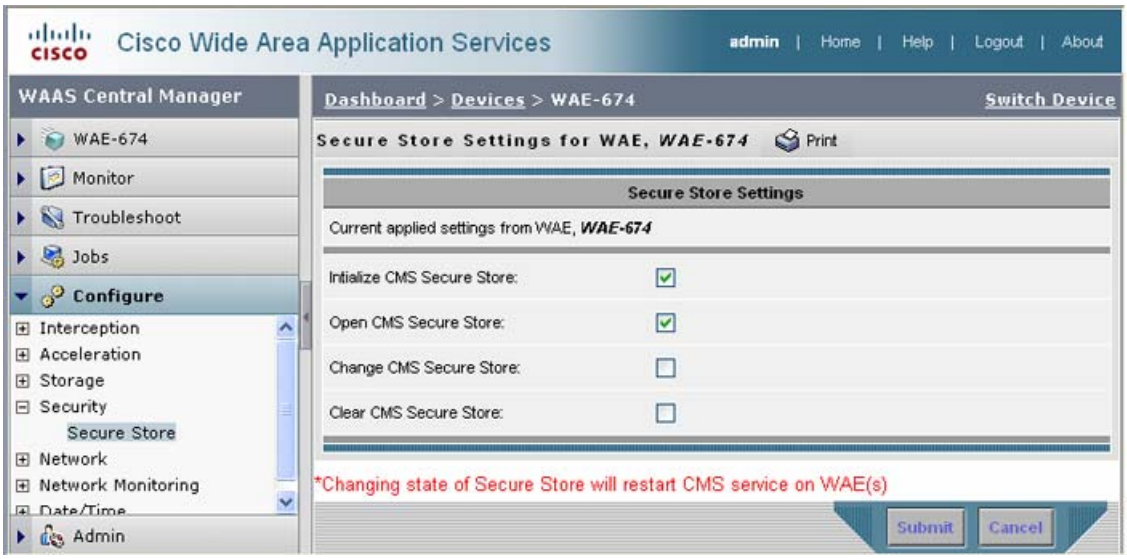
ステップ 1　WAAS Central Manager GUI から、**[Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　セキュア ストアを有効にしたいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

（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 グループの操作」[p.3-3] を参照）。

ステップ 3　ナビゲーション ペインで、**[Configure] > [Security] > [Secure Store]** を選択します。図 9-1 に示すように、[Secure Store Settings] ウィンドウが表示されます。

図 9-1　[Secure Store Settings] ウィンドウの例



ステップ 4　**[Initialize CMS Secure Store]** ボックスおよび **[Open CMS Secure Store]** ボックスを選択します。

ステップ 5　**[Submit]** をクリックして、セキュア ストア暗号化をアクティブ化します。

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 コマンドに続けて **cms secure-store open** 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アップデート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。セキュア ストア暗号化パスワードと暗号キーを変更するには、CLI EXEC モード コマンドの **cms secure-store change** を使用します。

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、次の手順に従います。

ステップ 1　**cms secure-store change** コマンドを入力します。

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

ステップ 2　新しいパスワードを入力し、Enter キーを押します。確認のため、プロンプトでパスワードを再度入力します。

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。

WAE デバイスの新しい暗号キーを生成するには、WAAS Central Manager GUI を使用して、次の手順に従います。

ステップ 1　WAAS Central Manager GUI から、**[Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　新しい暗号キーを生成するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Configure] > [Security] > [Secure Store]** を選択します。

ステップ 4　**[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 または WAE デバイスでのセキュア ストア暗号化の無効化

Central Manager または WAE デバイスでセキュア ストア暗号化を無効にするには、次の手順に従います。

ステップ 1　WAAS Central Manager GUI から、**[Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　セキュア ストアを無効にしたいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Configure] > [Security] > [Secure Store]** を選択します。図 9-1 に示すように、[Secure Store Settings] ウィンドウが表示されます。

ステップ 4　**[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。

CLI からセキュア 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）　プライマリ Central Manager のセキュア ストアを無効にした場合は、同様にスタンバイ Central Manager のセキュア ストアも無効にする必要があります。

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。これらのプロパティを変更するには、WAAS Central Manager GUI ナビゲーション ペインから、**[Configure] > [System Properties]** を選択します。

表 9-4 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 9-4　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	リモート 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、このリモート ユーザはデータベースから削除されます。デフォルトは、1 日です。リモート ユーザとは、WAAS Central Manager ではなく、外部 AAA サーバで定義されるユーザです。
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 グループに属すことができます）。
System.datafeed.pollRate	WAAS 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）を監視するための収集と送信の速度（秒）。速度を 0 に設定すると、状態の監視は無効になります。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、ローカルのデバイス 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 で実行された設定はローカル デバイスの設定を上書きします。
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）。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。

表 9-4　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.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	WAE 統計情報の監視（有効または無効）。デフォルトは true です。
System.monitoring.maxReports	カスタム レポートごとにストア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。これらの日付に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.print.driverFtpTimeout	FTP でプリンタ ドライバ ファイルが転送されるのを待つ最大秒数。指定できる範囲は、10 ～ 1800 秒です。デフォルトは 600 秒です。
System.registration.autoActivation	Central Manager に登録されている WAE デバイスを自動的にアクティブ化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。

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 GUI ナビゲーション ペインから、**[Configure] > [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　変更したいシステム 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　変更したいシステム 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。

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.9-24] 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 GUI ナビゲーション ペインから、**[Configure] > [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　**[Enable]** チェック ボックスを選択して、WAAS Central Manager がデバイスのオフライン ステータスを高速検出できるようにします。

ステップ 3　[Heartbeat Rate (Seconds)] 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] フィールドで、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 への送信中に削除できる UDP ハートビート パケットの個数を指定します。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、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 × 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; シスコ検出プロトコル）を受信すると、2 ×（ハートビート速度）×（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。

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 High Water Mark（HWM; 最高水準点）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、阻止されません。アラーム過負荷状態は、SNMP と Configuration Management System（CMS; 構成管理システム）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 Low Water Mark（LWM; 最低水準点）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）用のアラーム過負荷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 GUI ナビゲーション ペインで、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。[Devices]（または [Device Groups]）ウィンドウが表示されます。

ステップ 2　アラーム過負荷検出を設定したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーションペインで、**[Configure] > [Network 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 4　複数のアプリケーションがエラー条件を報告するときに、WAAS デバイス（またはデバイス グループ）がアラーム通知と解除動作を中止するように設定したくない場合は、**[Enable Alarm Overload Detection]** チェック ボックスの選択を解除します。デフォルトで、このチェック ボックスは選択されています。

ステップ 5　[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 6　[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 7　**[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** グローバル設定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を作成できます。レポートが生成されると、レポートへのリンクにより 1 人または複数の受信者への E メール送信が可能です（詳細は、「レポートの管理」[p.16-27] を参照）。

E メール通知を有効化するには、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 GUI ナビゲーション ペインで、**[My WAN] > [Manage Devices]** を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　E メール サーバ設定を構成したい WAAS Central Manager の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Configure] > [Notifier] > [Email Notification Server]** 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 4　[Mail Server Hostname] フィールドに、E メール送信に使用される E メール サーバのホスト名を入力します。

ステップ 5　[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 6　[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 7　[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 8　**[Submit]** をクリックします。
