CHAPTER 10

Cisco IPICS のハイ アベイラビリティの設定と管理

Cisco IPICS には、単一障害点のないハイ アベイラビリティを提供するため、セカンダリのホット スタンバイ サーバを設定するオプションがあります。プライマリ サーバで障害が発生した場合は、そのセカンダリ サーバが自動的に、通信の中断なくサービスを引き継ぎます。この章では、ハイ アベイラビリティ機能について詳細に説明します。ここでは次のトピックを取り上げます。

概要

Cisco IPICS のハイ アベイラビリティ（HA）機能では、2 つの Cisco IPICS サーバを冗長ペアとして構成し、システム ユーザおよび接続されているデバイスを管理する 1 つの *アクティブ サーバ*と、アクティブ サーバに問題が発生したりオフラインになったりした場合に管理を引き継ぐため待機する 2 番目の *スタンバイ サーバ* を設定することができます。

アクティブ サーバとスタンバイ サーバの定義

初期設定の際、プライマリ サーバとスタンバイ サーバのロールは、サーバにインストールされているライセンス ファイルの種類によって決定されます。

- *IPICS ベース サーバ*ライセンスと*ポリシー エンジン基本*ライセンスは、プライマリ サーバとして指定するサーバにインストールします。このサーバが、アクティブのロールを担うことになります。
- セカンダリ サーバに指定するサーバには、*ハイ アベイラビリティ* ライセンスだけをインストールします。このサーバが、スタンバイのロールを担うことになります。

サーバのペアが HA モードで稼動を始めた後は、*アクティブ*と*スタンバイ*のロールをサーバ間で切り換えることができます。ユーザは Cisco IPICS Administration Console にログインすると、自動的に現在アクティブなサーバにログインされます。

ヒント　詳細については、『*Cisco IP Interoperability and Collaboration System Server Installation Guide*』の「Managing Your Licenses」の項を参照してください。

セキュア通信を使用するリモート サーバ ロケーション

冗長 Cisco IPICS サーバは、それぞれ REMOTE ロケーションに配置して、一方のロケーションにおける重大な障害が他方のサーバに影響しないようにすることができます。セキュア通信は初期設定の際に確立され、このときに両サーバが 1 回だけの SSH/TLS 証明書と公開キーの交換を行います。詳細については、「Cisco IPICS サーバでの HA の設定」（P.10-4）を参照してください。

ローカルの重要プロセスの障害によるサーバのフェールオーバー

ローカルの重要なプロセス（Tomcat など）に障害が発生すると、アクティブ サーバはスタンバイ サーバに対し、アクティブ ロールを担うようにと指示を出します。このプロセスには数分かかる場合があります。またこのプロセスは、スタンバイ サーバが準備完了状態で待機しており、到達可能であることを前提としています。

ハートビート メッセージの損失によるサーバのフェールオーバー

各冗長サーバは、交信を定期的なハートビート メッセージによっても維持します。アクティブ サーバが、設定された時間の経過後もこのメッセージに応答しない場合は、スタンバイ サーバがアクティブ ロールを担います。このハートビート通信の損失は、ネットワーク接続の切断やハードウェア障害によって発生することがあります。

デフォルトでは、プライマリ サーバとスタンバイ サーバはハートビート メッセージを 15 秒ごとに交換します。5 回のハートビート メッセージが失敗すると（計 75 秒間）、スタンバイ サーバがアクティブ ロールを担います。

必要に応じてデフォルトのハートビート時間を変更するには、「Cisco IPICS サーバでの HA の設定」（P.10-4）を参照してください。

IDC および接続されたデバイスへのフェールオーバーの影響

フェールオーバーが発生すると、切り替えが完了するまで IDC 接続が一時的に失われる場合があります。ただしコンソールはオフライン モードで動作を続け、ユーザが何も操作を行わなくても、自動的に新しいサーバに再接続されます。元のサーバがオンラインに戻りスタンバイ ロールを担っても、コンソールの接続は中断されません。詳細については、「IDC 接続に対する HA の影響」（P.10-10）を参照してください。

iPhone のような一部の接続デバイスも、フェイルオーバーの際に接続が途切れることはありません。Cisco Unified IP Phone や標準的な電話機などのその他のデバイスは、手動で再接続する必要があります。詳細については、「接続されたデバイスに対する HA の影響」（P.10-12）を参照してください。

スプリット ブレーン状況からの手動のフェールオーバーと復旧

アクティブ サーバからスタンバイ サーバへのフェールオーバーは、手動で強制することもできます。詳細については、「手動フェールオーバーの実行」（P.10-14）を参照してください。

プライマリとセカンダリのサーバ間の通信が切断された場合、両方のサーバが一時的にアクティブのロールを担うことがあります。この状況は、*スプリット ブレーンのシナリオ*と呼ばれています。通信が再度確立されたら、手動でセカンダリ サーバをスタンバイ ロールに移行させる必要があります。手順については、「スプリット ブレーンのシナリオの解決」（P.10-15）を参照してください。

Cisco IPICS サーバでの HA の設定

Cisco IPICS の HA を設定するには、プライマリ サーバとセカンダリ サーバをインストールして設定する必要があります。これらのサーバは、セキュアな暗号化された接続を使用して交信を行うため、別のロケーションに存在させることができます。

HA を設定する前に、次の説明に従って、両方のサーバに IP アドレス、NTP サーバ、および各サーバの正しいライセンスを設定する必要があります。

開始する前に

冗長 Cisco IPICS サーバを設定する前に、次の作業を行います。

- Cisco IPICS サーバの同期化に使用されるネットワーク タイム プロトコル（NTP）サーバのアドレスを取得します。詳細については、「HA サーバのサーバ時間の同期」（P.10-13）を参照してください。
- プライマリ サーバとセカンダリ サーバの IP アドレスを取得します。
- セカンダリ サーバの **ipicsadmin** ユーザ パスワードを取得します。
- プライマリ サーバ用の *IPICS ベース サーバ*ライセンスと*ポリシー エンジン基本*ライセンス、およびセカンダリ サーバ用の*ハイ アベイラビリティ*ライセンスを取得します。『*Cisco IP Interoperability and Collaboration System Server Installation Guide*』の「Managing Your Licenses」の項を参照してください。
- インストールされている HA サーバのペアが、『*Cisco IPICS Compatibility Matrix*』で定義されている、サポートされる設定のいずれかに一致することを確認します。

- いずれかの HA サーバ上に存在する既存のデータがすべてマージされることを確認するか、または IPICS ソフトウェアのクリーン インストールを実行します。
- 必要に応じて、IPICS サーバ ソフトウェアのクリーン インストールを実行します。サーバに HA を設定すると、いずれかのサーバに存在するデータはすべてマージされます。
  - 以前別の HA ペアでプライマリまたはセカンダリとして設定されていたサーバからのデータは、新しい HA 設定にマージされます。
  - サーバに以前 HA が設定されていなかった場合も、既存のデータはマージされます。
  - HA ペアの作成時に、サーバの既存データをマージしない場合は、IPICS サーバ ソフトウェアのクリーン インストールを実行して、そのデータを削除する必要があります。詳細については、『*Cisco IPICS Server Installation and Upgrade Guide*』を参照してください。

冗長 Cisco IPICS サーバに HA を設定するには、次の手順を実行します。

手順

ステップ 1　プライマリとセカンダリのサーバを物理的にインストールします。

手順については、『*Cisco IP Interoperability and Collaboration System Server Installation Guide*』を参照してください。

ステップ 2　（オプション）必要に応じて、IPICS サーバ ソフトウェアのクリーン インストールを実行し、プライマリまたはセカンダリのサーバから既存のデータを削除します。

（注）　サーバに HA を設定すると、いずれかのサーバに存在するデータはすべてマージされます。サーバ ソフトウェアのクリーン インストールを実行して、既存のデータを削除します。手順については、『*Cisco IPICS Server Installation and Upgrade Guide*』を参照してください。

ステップ 3　各サーバに IP アドレスを設定します。

手順については、『*Cisco IP Interoperability and Collaboration System Server Installation Guide*』を参照してください。

ステップ 4　プライマリとセカンダリの両サーバで、システム時間を同期するための NTP サーバを設定します。

（注）　HA サーバは、内部時刻設定を使用して HA ハートビートやデータを交換します。HA 設定は、両方のサーバで NTP が設定されていないと失敗します。

a. 両方のサーバで次のコマンドを入力して、NTP を有効化します。

```
ntpsetup -s enable <ntp-server> <backup-ntp-server>
```

次の例を参考にしてください。

```
ntpsetup -s enable ntp-sj1.cisco.com ntp-sj2.cisco.com
```

b. 両方のサーバで次のコマンドを入力して、システム設定を確認します。

```
ntpsetup -c
```

c. 両方のサーバで次のコマンドを入力して、ノード マネージャを再起動します。

```
service ipics_nm restart
```

ステップ 5　プライマリとセカンダリの各サーバで、次のソフトウェア ライセンスをインストールします。

a. プライマリ サーバで、*IPICS ベース サーバ*ライセンスと*ポリシー エンジン基本*ライセンスをインストールします。プライマリ サーバでは、HA ライセンスは必要ありません（HA ライセンスは絶対にプライマリ サーバにインストールしないでください）。

b. セカンダリ サーバでは、*ハイ アベイラビリティ* ライセンスだけをインストールします。セカンダリ サーバには、その他のライセンスは必要ありません。

『*Cisco IP Interoperability and Collaboration System Server Installation Guide*』の「Managing Your Licenses」の項を参照してください。

ステップ 6　プライマリ サーバの Cisco IPICS Administration Console にログインします。

手順については、「Administration Console へのアクセス」（P.1-15）を参照してください。

ステップ 7　Cisco IPICS Administration Console から、[Configuration] > [High Availability] > [Security] タブに移動します。

HA パートナーの信頼がまだ設定されていない場合は、ウィンドウに [Server Status] が [`Not Trusted`] であると表示されます。

ステップ 8　[High Availability] ウィンドウで次の手順を実行して、ハイ アベイラビリティ モードを有効化します。

a. [IP Address] フィールドに、HA パートナー サーバの IP アドレスを入力します。

HA パートナーは、セカンダリ Cisco IPICS サーバになります。[User Name] フィールドに、パートナー サーバの Linux 管理者のユーザ名（ipicsadmin）が表示されます。

b. [User Password] フィールドに、ipicsadmin ユーザのパスワードを入力します。

c. [Save] をクリックして HA パートナーの IP アドレスを保存し、冗長サーバ間の信頼を確立します。

信頼を確立するため、サーバ同士が公開キーと SSL 証明書を交換します。

成功すると、サーバのステータスが [Trusted] に変わり、[HA Configuration] タブが表示されます。

ステップ 9　[HA Configuration] タブをクリックします。

（注）

- [HA Configuration] ウィンドウは、ステップ 8 の説明に従ってハイ アベイラビリティ モードを有効化してから初めて表示されます。
- プライマリ サーバとセカンダリ サーバの IP アドレスは読み取り専用です。プライマリ サーバの IP アドレスは、現在ログインしている Cisco IPICS サーバになります。セカンダリ サーバの IP アドレスは、ステップ 8 でハイ アベイラビリティ モードを有効化するために入力したアドレスになります。
- ハイ アベイラビリティ モードが有効になっていても、HA がまだ設定されていない場合、[Standby Server Status] は [Not Ready] になります。

ステップ 10　（オプション）次の操作を行って、冗長サーバ間の接続の維持に使用されるデフォルトのハートビート設定を変更します。

a. [Heartbeat Port] フィールドに、HA ハートビート トラフィックの IP ポート番号を入力します。デフォルト値は 3444 です。

b. [Heartbeat Interval (seconds)] フィールドに、5 ～ 600 の数値を入力して、各ハートビート間の秒数を定義します。

各ハートビートでは、パートナー サーバのステータスと可用性が確認されます。デフォルト値は 15 秒です。

c. [Missed Heartbeat Count] フィールドに、5 ～ 30 の数値を入力して、アクティブ ロールがセカンダリ サーバに切り替えられるまでのハートビートの失敗回数を定義します。

デフォルトは、ハートビートの失敗 5 回（ハートビート間隔が 15 秒の場合は 75 秒間）です。切り替えプロセスにはおよそ 150 ～ 180 秒かかります。

d. [Update] をクリックして変更を保存します。

ステップ 11 [Configure] をクリックして、変更を保存し、ハイ アベイラビリティ（サーバ冗長性）をアクティブ化します。

短い遅延の後、HA 設定の処理が完了するまで自動的に IPICS システムからログアウトされます。

ステップ 12 [Standby Server Status] が [Ready] に変わることを確認します。

a. Cisco IPICS Administration Console にログインします。

b. [Configuration] > [High Availability] ウィンドウに移動します。

c. [HA Configuration] タブをクリックします。

d. [Standby Server Status] が [Ready] になっていることを確認します。

HA の設定解除

特定の状況においては、一時的に HA の設定を解除することが必要になります。こうした状況には、Cisco IPICS データベース バックアップからデータを復元する場合や、IPICS サーバの SSL 証明書を生成する場合などがあります。

Cisco IPICS サーバの HA を設定解除するには、次の手順を実行します。

手順

ステップ 1　アクティブ サーバの Cisco IPICS Administration Console から、[Configuration] > [High Availability] ウィンドウに移動します。

ステップ 2　[HA Configuration] タブをクリックします。

ステップ 3　[Unconfigure] ボタンをクリックします。

ステップ 4　アクティブ サーバからログアウトするには、[Logout] をクリックします。

ステップ 5　アクティブ サーバが再設定されるまで数分間待ちます。

ステップ 6　（オプション）パートナー サーバで使用されるセキュリティの信頼証明書を削除します。

（注）　HA セキュリティ証明書は、SSL 証明書を再生成または置換する必要があるときだけ削除します。デフォルトの IPICS サーバの SSL 証明書は、3 年間で有効期限切れとなり、その後は新しいものと置き換える必要があります。詳細については、付録 D「SSL 証明書の生成」を参照してください。

a. プライマリ サーバに再度ログインします。

b. [HA Security] ウィンドウに移動します（[Configuration] トレイを展開し、[High Availability] > [HA Security] を選択します）。

c. パスワードのフィールドにパートナー サーバのパスワードを入力して、[Delete] ボタンを有効化します。

   信頼証明書がパートナー サーバから削除されたことを保証するには、有効なパスワードが必要になります。

d. [Delete] をクリックして、パートナー サーバで使用される信頼証明書を削除します。

IDC 接続に対する HA の影響

ユーザが IDC にログインするときは、アクティブおよびスタンバイのすべてのサーバがログイン セレクタに表示されます。接続するには、アクティブなサーバを選択する必要があります。スタンバイのサーバを選択すると、接続は拒否され、自動的にアクティブなサーバにリダイレクトされます。

（注）　アクティブとスタンバイのロールは、使用可能なサーバ間で切り替えることができます。ユーザは常に、アクティブなサーバにログインする必要があります。どちらのサーバでも、同じユーザ名とパスワードが使用されます。

アクティブ サーバがダウンするか、スタンバイ サーバとの接続が切断されると、フェールオーバーが発生します。この場合、IDC は自動的にスタンバイ サーバに切り替えられ、サービスは通常どおりに継続されます。IDC がスタンバイ サーバと接続を確立するまでの短時間、コンソールはその前にアクティブだったサーバから提供された設定を使用して、オフライン モードで動作します。コンソールには、オフライン ステータスをユーザに知らせるメッセージも表示されます。このオフラインの間に、コンソールのユーザが実行すべきアクションは特にありません。コンソールが自動的に新しいサーバに再接続すると、新しいメッセージが表示されます。

フェールオーバーの後、コンソールは元のサーバがオンラインに戻っても、新しいアクティブ サーバとの接続を維持します。復旧したサーバは新しいスタンバイ サーバになり、フェールオーバーが発生した際に管理を引き継ぐため待機します。コンソール ユーザがログアウトした場合は、再度アクティブ サーバ（ログイン サーバ セレクタに表示される）にログインできます。

ユーザがスタンバイ サーバにログインしようとすると、コンソールは自動的にアクティブ サーバにリダイレクトされます。

（注）

- フェイルオーバーの間、Cisco IPICS サーバの動作は短時間一時停止するため、すべてのデータがアクティブ サーバからスタンバイに同期されない可能性があります。この状況が発生すると、フェイルオーバーの直前に入力された一部の設定は失われることがあります。詳細については、下記の例を参照してください。

- フェールオーバーの少し前にインシデントにアップロードした写真やビデオは、再アップロードが必要になることがあります。これは、これらのファイルはサイズが大きい場合があり、システム データよりも低い優先度でレプリケートされるからです。

例

この例の Cisco IPICS システムには、「Cisco IPICS サーバでの HA の設定」（P.10-4）で説明する冗長サーバが設定されています。システムは 10 日間の間、問題なく動作しています。ディスパッチャ Dan が自分のシフトを開始し、ログインのダイアログでアクティブ サーバを選択してコンソールにログインします。昼食時に、局地的な地震が発生し、アクティブ サーバが棚から転落しました。Dan が使用しているコンソールは、サーバへのリンクが切断されたことを検出し、自動的にスタンバイ サーバに接続します。このプロセスにはおよそ 10 秒かかります。Dan はコンソールがすべてのサーバから接続解除されたことに気づきますが、コンソールはメディア リソースとの接続を維持しているため、Dan はコンソールの Push-to-Talk（PTT）チャネル機能を使用して、Adam（管理者）に局地的地震について知らせることができます。10 秒後、Dan が使用しているコンソールは自動的にスタンバイ サーバに接続します。コンソールに目に見える変化はありません。

サーバのフェールオーバーから 45 分後、管理者の Adam が地震に巻き込まれた元のサーバを再マウントし、サーバのネットワーク接続を回復します。ただし、ディスパッチャの Dan が使用しているコンソールは新しいアクティブ サーバとの接続を継続し、復旧したサーバが新しいスタンバイになります。

翌日、Dan は仕事に戻ると、コンソールにログインして新しいアクティブ サーバに接続します。このサーバは、ログイン サーバ セレクタによってアクティブ サーバと識別されます。

このプロセスの最中には、問題が 1 つ発生しました。地震の前は、Fire というチャネルが Ursula というユーザに割り当てられていました。コンソールがアクティブ サーバからのアップデートを受信したため、Ursula には新しいチャネルが表示されます。ただしアクティブ サーバは、チャネル割り当てがスタンバイ サーバに伝えられる前に、地震でネットワークから切断されました。新しい Fire チャネルはフェールオーバーの発生前にスタンバイに伝えられなかったため、Fire チャネルは新しいアクティブ サーバに表示されず、再設定が必要になります。

翌日、Amy がコンソールへのログインを試みます。彼女はフェールオーバー時にオンラインではなかったため、コンソールのログイン サーバ セレクタにはまだ元のアクティブ サーバが表示されます。Amy がこのサーバに接続しようとすると、このサーバは現在スタンバイになっているため、アプリケーションが 5 秒

ほど一時停止します。接続が失敗すると、コンソールは自動的に他方のサーバにリダイレクトされます。コンソールは新しいアクティブ サーバに接続し、新しいサーバのステータスを反映するよう更新されます。

接続されたデバイスに対する HA の影響

Cisco IPICS サーバのフェールオーバーが発生すると、接続されているデバイスは次のような影響を受けます。

- モバイル クライアント：モバイル クライアントは自動的に新しいアクティブ サーバに切り替わります。
- Cisco Unified IP Phone : Cisco Unified IP Phone の管理者は、プライマリとセカンダリ両方の IPICS サーバに Cisco Unified Phone Service を設定する必要があります。この設定では、ユーザまたは管理者のいずれかが、両方のサーバでサービスに登録できます （詳細については、『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified Phone Services」の項を参照してください）。

  Cisco Unified IP Phone の使用中にアクティブ サーバがダウンした場合は、手動でアクティブ IPICS サーバに再接続する必要があります。[Services] メニューを開き、新しいアクティブ Cisco IPICS サーバを選択して、再度ログインします。
- 標準的な電話機：標準的なダイヤルイン電話コールは中断されますが、ユーザは短い遅延の後、システムに再度コールできます。

（注）
- Cisco IPICS が、フェールオーバーの発生時 VTG に参加していたダイヤルアウトしたユーザに、自動的に再コールすることはありません。
- 実行中だった外部通知またはポリシーはすべて、フェールオーバー後に再開されます。ユーザには、重複する通知が送信される場合があります。

HA サーバのサーバ時間の同期

サーバで HA を設定する前に、各サーバでネットワーク タイム プロトコル（NTP）を使用して内部時刻を設定する必要があります。HA サーバは、内部時刻設定を使用して HA ハートビートやデータを交換します。HA 設定は、両方のサーバで NTP が設定されていないと失敗します。

また、時刻設定はいずれの HA サーバでも手動で変更しないでください。時刻設定に 30 秒以上のずれがあると、サーバ間の HA 通信が失われ、*スプリット ブレーン*のシナリオが開始される可能性があります。詳細については、「スプリット ブレーンのシナリオの解決」（P.10-15）を参照してください。

プライマリまたはセカンダリ サーバの時刻設定を同期するには、次の手順を実行します。

手順

ステップ 1　プライマリとセカンダリの両サーバで、NTP サーバを設定します。

NTP サーバにより、システムの時刻が設定され、アクティブ サーバとスタンバイ サーバの時刻が同期されます。

a. 両方のサーバで次のコマンドを入力して、NTP を有効化します。

```
ntpsetup -s enable <ntp-server> <backup-ntp-server>
```

次の例を参考にしてください。

```
ntpsetup -s enable ntp-sj1.cisco.com ntp-sj2.cisco.com
```

b. 両方のサーバで次のコマンドを入力して、システム設定を確認します。

```
ntpsetup -c
```

（注）　両方のサーバに同じファイルまたは記録が存在し、それらのタイムスタンプが異なっている場合は、タイムスタンプが最新のファイルまたは記録だけが保持されます。古いほうのデータは上書きされます。

ステップ 2　両方のサーバで次のコマンドを入力して、ノード マネージャを再起動します。

```
service ipics_nm restart
```

ステップ 3　時刻設定の誤りによって両方のサーバがアクティブ状態になった場合は、セカンダリ サーバを強制的にスタンバイ モードに戻す必要があります。詳細については、「スプリット ブレーンのシナリオの解決」（P.10-15）を参照してください。

手動フェールオーバーの実行

現在のアクティブ サーバとスタンバイ サーバのロールを手動で切り替えるには、次の手順を実行します。アクティブ ロールはスタンバイ サーバに移されます。この手順は、アクティブ サーバをオフラインにし、サーバ間で安定したフェールオーバーを行いたい場合に必要になります。

開始する前に

- プライマリまたはセカンダリのいずれかのサーバを [Active] ステータスにできます。現在 [Standby] ステータスのサーバにアクティブ ロールを切り替えるには、次の手順を実行します。
- 手動フェールオーバーを実行するには、HA が設定済みであり、[Standby Server Status] が [Ready] になっている必要があります。詳細については、「Cisco IPICS サーバでの HA の設定」（P.10-4）を参照してください。
- 開始する前に、コンソールおよび接続されたデバイスへのフェールオーバーの影響を再確認してください。「IDC 接続に対する HA の影響」（P.10-10）および「接続されたデバイスに対する HA の影響」（P.10-12）を参照してください。

手順

ステップ 1　Cisco IPICS Administration Console にログインします。

手順については、「Administration Console へのアクセス」（P.1-15）を参照してください。

ステップ 2　[Configuration] > [High Availability] ウィンドウに移動します。

ステップ 3　[HA Configuration] タブをクリックします。

（注）　[HA Configuration] タブが使用可能でない場合は、ハイ アベイラビリティ モードが有効になっていません。「Cisco IPICS サーバでの HA の設定」（P.10-4）の手順を実行してください。

ステップ 4　次の事項を確認します。

- [Standby Server Status] が [Ready] になっている。
- スタンバイ モードのサーバがアクティブ ロールを担う必要がある。

[Standby Server Status] が [`Not Ready`] の場合は、ハイ アベイラビリティ モードが有効にはなっていますが、設定はされていません。「Cisco IPICS サーバでの HA の設定」（P.10-4）のステップ 9を実行してください。

ステップ 5　[Failover Now] ボタンをクリックして、アクティブ ステータスをスタンバイ サーバに移します。

スタンバイ サーバが新しいアクティブ サーバになり、アクティブ サーバがスタンバイ サーバになります。

スプリット ブレーンのシナリオの解決

*スプリット ブレーンのシナリオ*は、プライマリとセカンダリのサーバ間の通信が切断され、両方のサーバがそれぞれ独立してアクティブ サーバのロールを担ったときに発生します。この状況では、コンソールやデバイスは互いに接続して動作を続行できますが、各サーバに保存されているデータは、他方のサーバと同期されません。時間の経過につれて、サーバ間のデータの相違は大きくなります。

サーバ間の通信リンクが再度確立されても、両方のサーバがアクティブ ステータスのままになります。この状況は、スプリット ブレーンのシナリオと呼ばれています。この不正な設定を解消するには、一方のサーバをスタンバイ ステータスに戻し、2 つのサーバ上のデータを調整する必要があります。

（注）

- いずれのサーバをスタンバイ ステータスに戻しても構いませんが、シスコでは次の手順で説明するとおり、プライマリ サーバをアクティブ ステータスのままにしてセカンダリ サーバをスタンバイに戻すことをお勧めしています。
- *スプリット ブレーン*のシナリオは、両サーバの時刻設定に 30 秒以上のずれがあるときに発生します。NTP を使用してサーバ時間を同期する方法については、「HA サーバのサーバ時間の同期」（P.10-13）を参照してください。

調整方法の概要

各サーバのデータを調整し、サーバの冗長性を回復するには、次のような方法が使用されます。次の説明を参照して、どの方法を使用するかを決定してください。

- 「方法 1：セカンダリ サーバを強制的にスタンバイ ステータスにする」（P.10-17）：この方法は、サーバが短時間（5 日未満）の間、スプリット ブレーン モードであった場合に使用します。このプロセスでは、セカンダリ サーバを強制的にスタンバイ ステータスにし、その後 Linux コマンドを使用して 2 つのサーバのデータベースとファイル システムを同期します。この方法では、各サーバが自動的にハイ アベイラビリティの動作に戻り、ユーザはプライマリ サーバへのアクセスを続行できます。
- 「方法 2：ハイ アベイラビリティを再設定する」（P.10-20）：この方法は、サーバが 5 日以上の間スプリット ブレーン モードだった場合、またはセカンダリ サーバをスタンバイ ステータスにすると（方法 1）データの損失が懸念される場合に使用します。この方法を実行すると、セカンダリ サーバがダウンし、プライマリ サーバのハイ アベイラビリティ設定が解除され、その後両サーバに存在するファイルを手動で調整することになります。作業が完了したら、両サーバで HA を設定し直して、サーバの冗長性を回復する必要があります。
- 「方法 3：回避策」（P.10-21）：この方法は、方法 1 および 2 が機能しない場合にだけ使用します。この方法では、プライマリを強制的に唯一のアクティブ サーバとしますが、データの調整は行いません。

方法 1：セカンダリ サーバを強制的にスタンバイ ステータスにする

方法 1 は、セカンダリ サーバを手動でスタンバイ ステータスにするときに使用します。セカンダリ サーバがスタンバイ ステータスになったら、SSH クライアントを使用してサーバのデータベースとファイル システムを再同期します。

サーバ データベースを再同期すると、次のようなことが起こります。

- プライマリ サーバにあってセカンダリ サーバに存在しない記録は、プライマリ サーバからセカンダリ サーバにレプリケートされます。
- セカンダリ サーバにあってプライマリ サーバに存在しない記録は、セカンダリ サーバからプライマリ サーバにレプリケートされます。
- ある記録が両方のサーバに存在する場合は、プライマリ サーバにある記録がマスターとみなされ、セカンダリ サーバにある対応する記録は置換されます。

ファイル システムのファイルを再同期すると、次のようなことが起こります。

- プライマリ サーバにあってセカンダリ サーバに存在しないファイルは、プライマリ サーバからセカンダリ サーバにコピーされます。
- セカンダリ サーバにあってプライマリ サーバに存在しないファイルは削除されます。
- 同じファイルが両方のサーバに存在する場合は、タイムスタンプが新しいほうのファイル（世界標準時（UTC）を基準とする）が保持され、他方の HA サーバにコピーされます。古いバージョンのファイルは上書きされます。古いほうのファイルを削除する代わりにファイルをマージしたい場合は、Linux のシステム管理者に問い合わせて、**scp** または **sftp** を使用してファイルの相違を調整する方法を確認してください。

このプロセスでは、各サーバが自動的にハイ アベイラビリティの動作に戻り、ユーザはプライマリ サーバへのアクセスを続行できます。

手順

ステップ 1　（オプション）同期の際にレプリケートされたファイルおよびフォルダを表示します。

次の場所にあるファイルを表示します。

```
/opt/cisco/ipics/conf/fileDirectory
```

このファイルには、ローカルのソース ディレクトリとリモートの宛先ディレクトリが含まれています。

```
/idspri/backup/
/idspri/backup
/opt/cisco/ipics/tomcat/current/webapps/ipics_files/
/opt/cisco/ipics/tomcat/current/webapps/ipics_files
/opt/cisco/ipics/tomcat/current/webapps/ipics_server/pmclogs/
/opt/cisco/ipics/tomcat/current/webapps/ipics_server/pmclogs
/idspri/archive/
/idspri/archive
/idspri/db_table_archive/
/idspri/db_table_archive
/opt/cisco/ipics/tomcat/current/webapps/documents/
/opt/cisco/ipics/tomcat/current/webapps/documents
```

（注）　このファイルは、レプリケートする内容を決定するために使用されます。このファイルは一切変更しないでください。

ステップ 2　セカンダリ サーバを強制的にスタンバイ ステータスにします。

a. どちらのサーバがセカンダリ サーバとして設定されているかを確認します。

「Cisco IPICS サーバでの HA の設定」（P.10-4）を参照してください。

b. セカンダリ サーバの Cisco IPICS Administration Console にログインします。

手順については、「Administration Console へのアクセス」（P.1-15）を参照してください。

c. [Configuration] > [High Availability] ウィンドウに移動します。

d. [HA Configuration] タブをクリックします。

（注）　ウィンドウ上部に、スプリット ブレーンのシナリオが発生したというメッセージが表示されます。

e. [Standby Server Status] が [Not Ready] になっていることを確認します。

f. ウィンドウ下部にある [Go Standby] ボタンをクリックします。

[Go Standby] ボタンは、両方のサーバがアクティブ モードになっており、両サーバ間の通信が再確立されているときにだけ有効になります。

g. 確認メッセージが表示されたら、[OK] をクリックします。

セカンダリ サーバから、現在のすべてのユーザ セッションがログアウトされます。

h. スプリット ブレーンの修復プロセスが完了するまで待ちます。

修復プロセスでは、アクティブとスタンバイのサーバ設定を備えた HA サーバ ペアが再確立されます。

プロセスの完了後は、セカンダリ サーバへのログインを試みると、プライマリ サーバにリダイレクトされます。詳細については、「IDC 接続に対する HA の影響」（P.10-10）を参照してください。

ステップ 3　プライマリ サーバとセカンダリ サーバのデータベースを再同期します。

a. SSH クライアントを使用して、ユーザ名 [Informix] でプライマリまたはセカンダリの HA サーバにログインします。コマンドはどちらのサーバでも同じように機能します。

b. 次のコマンドを入力して、データベースの同期プロセスを開始します。

```
server> /opt/cisco/ipics/database/bin/ipicsedr_control_repl
REPAIR
```

c. 次のコマンドを入力して、データベースの同期プロセスを監視します。

```
server> /sbin/service ipics ha-status
```

（注） データベース レプリケーションの修復プロセスは、バックグラウンドで同時実行されます。さまざまなプロセスのステータスは、[Pending Database Replication Synchronization Processes] の下に一覧表示されます。修復プロセスは、セクションに未処理のエントリがなくなると終了します。

ステップ 4　ファイル システムのファイルを再同期します。

a. SSH クライアントを使用して、ユーザ名 [ipicsadmin] でプライマリ サーバにログインします。

（注） プライマリ サーバでは、次のコマンドを実行する必要があります。

b. 次のコマンドを入力して、ファイル システムの同期プロセスを開始します。

```
server> /opt/cisco/ipics/database/bin/ipicsrsync run ipicsadmin
```

c. 次のコマンドを入力して、同期プロセスを監視します。

```
server> /opt/cisco/ipics/database/logs/rsync.log
```

ステップ 5　プライマリ サーバの Cisco IPICS Administration Console にログインして、プライマリ サーバがアクティブ ステータスであり、セカンダリ サーバがスタンバイ ステータスであることを確認します。

方法 2：ハイ アベイラビリティを再設定する

方法 2 は、必要に応じて 2 つのサーバ間のデータ整合性を手動で点検し、データを調整するために使用します。詳細については、「調整方法の概要」（P.10-16）を参照してください。

手順

ステップ 1　SSH を使用してセカンダリ サーバにログインします。

ステップ 2　次のコマンドを入力して、セカンダリ サーバへのアクセスを停止します。

- `server> /sbin/service ipics stop`
- `server> /sbin/service ipics_nm stop`

ステップ 3　次の操作を行って、プライマリ サーバの HA 設定を解除します。

a. プライマリ サーバの Cisco IPICS Administration Console にログインします。

手順については、「Administration Console へのアクセス」（P.1-15）を参照してください。

b. [Configuration] トレイを展開して、[High Availability] をクリックします。

c. [HA Configuration] タブをクリックします。

d. [Unconfigure] ボタンをクリックします。

e. [Logout] をクリックして、アクティブ サーバからログアウトします。

f. プライマリ サーバが再設定されるまで数分間待ちます。

g. プライマリ サーバに再度ログインします。

h. もう一度 [HA Security] 画面に移動します（[Configuration] トレイを展開し、[High Availability] をクリックして、[HA Security] タブをクリックします）。

i. [HA Security] 画面で [Delete] をクリックして、HA セキュリティ証明書を削除し、HA モードを無効化します。

ステップ 4　両サーバの次のディレクトリを点検して、両方のサーバのファイルが同じであることを確認します。

- /idspri/backup
- /opt/cisco/ipics/tomcat/current/webapps/ipics_files
- /opt/cisco/ipics/tomcat/current/webapps/ipics_server/pmclogs
- /idspri/archive
- /idspri/db_table_archive
- /opt/cisco/ipics/tomcat/current/webapps/documents

（注）　/documents ディレクトリには、アップロードされたすべての iPhone および IDC コンテンツが含まれており、これは重要データとみなされます。

ステップ 5　ファイルが同じでない場合は、正しいファイルをプライマリ サーバのディレクトリに移動します。

ステップ 6　プライマリとセカンダリのサーバでハイ アベイラビリティを再設定します。

「Cisco IPICS サーバでの HA の設定」（P.10-4）を参照してください。

（注）　元のプライマリ サーバのロールをセカンダリ ロールに変更する場合は、新しい HA ライセンスが必要になります。

方法 3：回避策

方法 1 と方法 2 のどちらを実行してもスプリット ブレーンのシナリオを修復できない場合は、次の回避策を使用して、プライマリ サーバを強制的に唯一のアクティブ ステータスのサーバとします。

手順

ステップ 1　セカンダリ サーバをシャットダウンします。

a. SSH を使用してセカンダリ サーバにログインします。

b. 次のコマンドを使用して、サーバをシャットダウンします。

```
shutdown -h now
```

c. マシンの電源を切ります。

ステップ 2　プライマリ サーバ上のすべてのサービスを、一度停止してから再起動します。

a. SSH を使用してプライマリ サーバにログインします。

b. 次のコマンドを使用して、IPICS サービスを再起動します。

```
service ipics stop-all
service ipics start-all
```

ステップ 3　(オプション) プライマリ サーバで `stop-all` および `start-all` のコマンドを使用できない場合は、次の代替コマンドを入力します。

```
service ipics_nm stop
service ipics stop
service ipics start
```

(10 秒待ちます)

```
service ipics_nm start
```

ステップ 4　セカンダリ サーバの電源を入れます。

長時間のサーバ ダウンタイム後の HA 設定の再確立

HA サーバ ペアのいずれか一方のサーバが長時間にわたりダウンした場合は、残ったアクティブ サーバがデータベースの更新内容をトランザクション ログに保存します。通常の動作状況では、ダウンした HA サーバがオンラインに戻ると、データベースの更新内容がこのサーバに復元されます。

ただし、2 番目のサーバが長時間にわたってオフラインになり、さらにシステム上で過剰なアクティビティが行われると、データベース ログに空きスペースがなくなる場合があります。データベース ログの内容が容量の 100 % に達すると、データベース レプリケーションのブロック状態（DDRBLOCK 状態）が発生することがあり、この場合はこれをクリアするまでデータベースのすべての更新がブロックされます。

この状況を防止するため、Cisco IPICS システムでは使用率が容量の 90 % を超えると、自動的に HA 設定が解除されます。また、使用率が容量の 75 % に達するとエラー メッセージも表示され、90 % に達したときにも再度エラー メッセージが表示されて、同時に HA 設定が解除されます。

いずれかのサーバにおける長時間のダウンタイム後に HA 設定が解除された場合は、「Cisco IPICS サーバでの HA の設定」（P.10-4）の説明に従って、アクティブ サーバで HA を再設定する必要があります。