Guard の設定

この章では、Cisco Guard（Guard）の設定方法について説明します。これらの設定手順は、Guard の管理や宛先変更に関連する通信の基礎となります。

この章には、次の主要な項があります。

Guard のサービスのアクティブ化

Guard でアクティブにするサービスを定義することができます。正しい機能を有効にするためには、サービスを有効にして、そのサービスへのアクセスを許可する必要があります。ユーザは、Guard のサービスのアクティベーションを制御できます。目的の IP アドレスに対してアクセス権を付与または拒否することにより、Guard にアクセスし、制御するアドレスを制限することができます。

Guard のサービスには、次のものがあります。

- **ntp**：Network Time Protocol（NTP）サービス。Guard は、時刻同期サービスを提供します。この機能により、Guard を時刻同期サーバに同期させることができます。

  （注）　時刻の同期を可能にするには、NTP サーバを設定する必要があります。詳細については、表 3-8 および P.3-22 の「Guard のクロックと NTP サーバの同期」を参照してください。

- **snmp-server**：Simple Network Management Protocol（SNMP）サーバ サービス。SNMP を使用して Guard にアクセスすることにより、Riverhead 管理情報ベース（Riverhead の専用 MIB、MIB2、および UCDavis の MIB）で定義された情報を取得することができます。
- **snmp-trap**：SNMP トラップ サービス。snmp-trap サービスをアクティブにすると、Guard は SNMP トラップを生成します。詳細については、P.3-27 の「SNMP トラップの有効化」を参照してください。
- **ssh**：Secured Shell サービス（詳細については、P.3-26 の「ホスト名の変更」を参照）。
- **wbm**：Web ベース管理（WBM）サービス。ユーザは、Web ブラウザを使用して、Web 経由で Guard を制御できます。

Guard のサービスをアクティブにするには、次の手順を実行します。

ステップ 1　Guard のサービスを有効にします。次のように入力します。

```
service {ntp | snmp-server | snmp-trap | wbm}
```

（注）　デフォルトでは、SSH 以外、Guard のすべてのサービスは無効になっています。

ステップ 2　Guard のサービスに対するアクセス権を付与し、接続を可能にします。次のように入力します。

```
permit service ip-addr [ip-mask]
```

表 3-1 に、**permit** コマンドの引数を示します。

表 3-1　permit コマンドの引数

パラメータ	説明
service	アクセスと操作の対象となるサービス。
ip-addr	アクセスを許可する IP アドレス。すべての IP アドレスからのアクセスを許可するには、* を使用します。
ip-mask	（オプション）IP マスク。デフォルトのサブネット マスクは、255.255.255.255 です。

注意　セキュリティ上の理由から、初期設定後はすべての IP アドレスからのアクセスを許可すること（*）は推奨しません。

次の例を参考にしてください。

```
admin@GUARD-conf# service ntp
admin@GUARD-conf# permit ntp 192.168.10.35
```

アクセス コントロールの設定

アクセス コントロールは、ネットワーク サーバにアクセスできるユーザと、そのようなユーザがアクセスした後で使用することのできるサービスを制御する手段です。認証、認可、アカウンティング（AAA）のネットワーク セキュリティ サービスは、アクセスを設定するための基本的なフレームワークとなります。

- 認証:ユーザにシステムおよびシステム サービスへのアクセスを許可する前に、そのユーザを識別する方法。
- 認可：システムへのアクセスを取得した後で、ユーザが実行することのできる内容を決定するプロセス。通常、このプロセスは、ユーザが認証され、システムの操作を開始した後で実行されます。
- アカウンティング：ユーザが実行中または実行した内容を記録する処理。アカウンティングにより、ユーザがアクセスしているサービスを追跡することができます。

次の各項では、アクセス コントロールの設定方法について説明します。

認証の設定

ユーザが Guard にログインしようとするとき、または（**enable** コマンドを使用して）上位の特権レベルを要求するときに、Guard で使用する認証方式を設定することができます。Guard は、次の認証オプションを提供します。

- ローカル認証：ローカル認証では、ローカルに設定されたログイン名およびイネーブル パスワードが認証に使用されます。これがデフォルトの認証方式です。詳細については、P.3-6 の「ローカル認証の設定」を参照してください。
- TACACS+ 認証 ：TACACS+ 認証では、TACACS+ サーバまたは TACACS+ サーバのリストを使用してユーザが認証されます。

シーケンシャルな認証リストを設定することができます。認証リストでは、ユーザの認証に使用する認証方式を定義します。この定義により、認証に使用する 1 つ以上の方式を指定することができます。したがって、最初の方式が失敗した場合は、認証のバックアップ システムが提供されます。

Guard は、最初にリストされた方式を使用してユーザを認証します。その方式が応答しない場合、Guard は 2 番目の認証方式を選択します。両方の認証方式を試してもうまくいかない場合、認証は失敗します。

分散認証方式を設定することもできます。Guard は、最初の TACACS+ サーバを使用してユーザを認証します。認証で拒否が返された場合、Guard は TACACS+ サーバ リスト、および、存在する場合は代替の認証方式（ローカル）をスキャンします。リストをすべて試してもうまくいかない場合、認証は失敗します。このオプションは、*first-hit* オプションを設定していない場合にのみ有効です。

注意　ユーザ データベースが、複数の TACACS+ サーバ、または TACACS+ サーバとローカル ユーザ データベースに分散している場合は、**no tacacs-server first-hit** コマンドを使用してください。

認証方式の設定

Guard で使用する認証方式を設定するには、次の手順を実行します。

ステップ 1　TACACS+ 認証が必要な場合は、TACACS+ サーバ接続を設定します。詳細については、P.3-15 の「TACACS+ サーバ接続の設定」を参照してください。

ステップ 2　認証方式を定義します。次のように入力します。

```
aaa authentication {enable | login} {local | tacacs+}
[tacacs+ | local]
```

表 3-2 に、**aaa authentication** コマンドの引数を示します。

表 3-2　aaa authentication コマンドのキーワード

パラメータ	説明
enable	Guard は、上位の特権レベルに入るときに認証を行います。
login	Guard へのログイン時に認証が行われます。
local	Guard は、ローカル データベースを使用してユーザを認証します。
tacacs+	TACACS+ サーバによってユーザが認証されます。
tacacs+ | local	設定された方式が失敗した場合の代替認証方式を設定します（オプション）。

次の例は、上位の特権レベルに入る際に認証を行うように設定する方法を示しています。最初の認証方式は TACACS+ に設定され、2 番目の認証方式はローカル ユーザ データベースに設定されています。

```
admin@GUARD-conf# aaa authentication enable tacacs+ local
```

ローカル認証の設定

Guard には、最初に管理者特権を持ったユーザ名が事前設定されており、このユーザを使用して新しいユーザを作成できるようになっています。ユーザ定義を使用すると、Guard のユーザ コミュニティをドメインに分割し、安全な管理アクセスのために必要に応じてパスワードを割り当てることができます。

TACACS+ サーバを使用した CLI ユーザの認証を有効にするには、P.3-4 の「認証の設定」を参照してください。

ユーザの追加

Guard のローカル データベースにユーザを追加するには、次のように入力します。

username *username* {**admin** | **config** | **dynamic** | **show**} [*password*]

表 3-3 に、**username** コマンドの引数とキーワードを示します。

表 3-3　username コマンドの引数とキーワード

パラメータ	説明
username	ユーザ名。英字で始まる英数字の文字列です。文字列にスペースを含めることはできません。また、長さは 63 文字までです。文字列にはアンダースコアを含めることができます。
admin | **config** | **dynamic** | **show**	ユーザの特権レベル。詳細については、表 2-4 を参照してください。
password	パスワード（オプション）。パスワードは、スペースを含まず、6 ～ 24 文字である必要があります。パスワードを入力しない場合、パスワードを要求されます。

次の例を参考にしてください。

```
admin@GUARD-conf# username Robbin config 1234
```

（注）　実行設定ファイルでは、**username** コマンドは、次のようにオプション *encrypted* とともに表示されます。

```
username Jose config encrypted 840xdMk3
```

encrypted オプションは、パスワードが暗号化されて保存されることを示します。Guard は、ログインのために入力されたパスワードではなく、暗号化されたパスワードを表示します。

Guard のユーザ リストからユーザを削除するには、次のように入力します。

no username *username*

ヒント　Guard のユーザのリストを表示するには、**show running-config** コマンドを使用します。現在 CLI にログインしているユーザのリストを表示するには、**show users** コマンドを使用します。

パスワードの変更

ユーザは、自分自身のパスワードを変更することができます。管理者は、自分自身のパスワードと、他のすべてのユーザのパスワードを変更できます。

自分自身のパスワードを変更するには、次の手順を実行します。

ステップ 1　次のように入力します。

password

ステップ 2　現在のパスワードを入力します。新しいパスワードの入力を求めるプロンプトが表示されます。

ステップ 3　新しいパスワードを入力します。パスワードは、スペースを含まず、6 ～ 24 文字である必要があります。新しいパスワードをもう一度入力し、確認するように求めるプロンプトが表示されます。

次の例を参考にしてください。

```
admin@GUARD# password
Old Password: <old-password>
New Password: <new-password>
Retype New Password: <new-password>
```

管理者は、他のユーザのパスワードを変更できます。

特定のユーザのパスワードを変更するには、次の手順を実行します。

ステップ 1　グローバル プロンプトで、次のように入力します。

password *username-password*

引数 *username-password* は、変更対象のパスワードを持つユーザです。

ステップ 2　新しいパスワードを入力します。パスワードは、スペースを含まず、6 ～ 24 文字である必要があります。新しいパスワードをもう一度入力し、確認するように求めるプロンプトが表示されます。

この例では、管理者はユーザ *John* のパスワードを変更しています。

```
admin@GUARD# password Jose
New Password: <new-password>
Retype New Password: <new-password>
```

認可の設定

ユーザが使用できるサービスを制限することができます。認可が有効な場合、Guard はユーザのプロファイルでそのユーザのアクセス権を確認します。プロファイルは、ローカル ユーザ データベースまたは TACACS+ セキュリティ サーバにあります。ユーザは、そのユーザのプロファイル内の情報で許可されている場合にのみ、要求したサービスへのアクセス権を付与されます。

ユーザがコマンドを実行しようとするときに Guard で使用する認可方式を設定することができます。Guard では、次の認可オプションが提供されています。

- TACACS+ 許可：TACACS+ 許可では、TACACS+ サーバを使用してユーザが認可されます。後続のサーバが定義されている場合は、1 つのサーバとの通信が失敗した場合にのみ、そのサーバへのアクセスが開始されます。

  TACACS+ 許可では、2 種類がサポートされています。実行許可では、ユーザの認証時にユーザの特権レベルが決定されます。コマンド許可では、ユーザがコマンドに入ると、コマンドの許可を取得するために TACACS+ サーバに対して確認が行われます。

  TACACS+ 許可では、コマンドごとにアクセス権を指定することができます。

注意　**copy running-config ftp** コマンドへのアクセス権の付与には注意を払う必要があります。
このコマンドの実行を許可すると、設定ファイル内ですべてのコマンドにそれぞれ許可を設定しているかどうかに関係なく、すべての設定コマンドに対して許可が与えられます。

- ローカル許可：ローカル許可では、コマンド グループのアクセス コントロールにローカルで設定されたユーザ プロファイルが使用されます。許可は、指定された特権レベルのすべてのコマンドに対して定義されます。これがデフォルトの認可方式です。

シーケンシャルな認可リストを設定することができます。認可リストでは、ユーザの認可に使用する認可方式を定義します。この定義により、認可に使用する 1 つ以上の方式を指定することができます。したがって、最初の方式に対する通信が失敗した場合は、認可のバックアップ システムが提供されます。

Guard は、最初にリストされた方式を使用してユーザを認可します。その方式が応答しない場合、Guard は 2 番目の認可方式を選択します。両方の認可方式が成功しなかった場合、認可は失敗します。

Guard のローカル許可は、TACACS+ サーバへの通信に失敗した場合に実行することができます。

ローカル許可の設定

Guard のサービスにアクセスできるかどうかは、ユーザの特権レベルによって決まります。ユーザが使用できるサービスを制限することができます。Guard は、ユーザのプロファイルをチェックして、ユーザのアクセス権を確認します。認可されると、ユーザは、そのユーザのプロファイル内の情報で許可されている場合にのみ、要求したサービスへのアクセス権を付与されます。ユーザの特権レベルについては、表 2-4 を参照してください。

パスワードを使用した特権レベルの割り当て

管理者は、ユーザの特権レベルへのアクセスを制限するパスワードを設定できます。

ローカル パスワードを設定して特権レベルへのアクセスを制御するには、次のように入力します。

enable password [**level** *level*] [*password*]

表 3-4 に、**enable password** コマンドの引数とキーワードを示します。

表 3-4　enable password コマンドの引数

パラメータ	説明
level	（オプション）目的の特権レベル。このレベルには、admin、config、dynamic、show のいずれかを指定できます。詳細については、表 2-4 を参照してください。デフォルトのレベルは **admin** です。
password	（オプション）特権レベルのパスワード。パスワードは、スペースを含まず、6 ～ 24 文字である必要があります。パスワードを入力しない場合、パスワードを要求されます。

ユーザ特権レベル間の移動

認可されたユーザは、ユーザ特権レベル間を移動することができます。ユーザ特権レベル間を移動するには、次の手順を実行します。

ステップ 1　次のように入力します。

```
enable [level]
```

引数 *level* には、目的の特権レベルを指定します。このレベルには、admin、config、dynamic のいずれかを指定できます。デフォルトのレベルは **admin** です。詳細については、表 2-4 を参照してください。

ステップ 2　特権レベルのパスワードを入力します。

次の例を参考にしてください。

```
admin@GUARD> enable admin
Enter enable admin Password: <password>
```

下位の特権レベル（**show**）に戻る場合は、**disable** コマンドを使用します。

認可方式の設定

認可方式を設定するには、次の手順を実行します。

ステップ 1　TACACS+ 許可が必要な場合は、TACACS+ サーバ接続を設定します。詳細については、P.3-15 の「TACACS+ サーバ接続の設定」を参照してください。

ステップ 2　認可方式を定義します。次のように入力します。

```
aaa authorization {exec | commands level} {local | tacacs+} [local]
```

認可方式のシーケンシャルなリストを設定できます。各方式について、**aaa authorization** コマンドを入力します。

表 3-5 に、**aaa authorization** コマンドの引数とキーワードを示します。

表 3-5　aaa authorization コマンドの引数とキーワード

パラメータ	説明
exec	ユーザが EXEC シェルの実行を許可されているかどうかを判別するために認可が実行されます。Guard は、TACACS+ サーバに確認して、認証されたユーザの特権レベルを判別します。 ⚠ **注意**　認可を設定する前に、TACACS+ サーバにそのユーザを設定しておく必要があります。
commands	指定された特権レベルのすべてのコマンドに対して認可が実行されます。複数の特権レベルの認可を設定するには、認可が必要な特権レベルごとにこのコマンドを発行します。
level	指定された特権レベルの認可を定義します。有効なエントリは、show、dynamic、config、および admin です。ユーザの特権レベルについては、表 2-4 を参照してください。
local	Guard は、認可にローカル データベースを使用します。

表 3-5　aaa authorization コマンドの引数とキーワード（続き）

パラメータ	説明
tacacs+	TACACS+ サーバによってユーザのアクセス権が確認されます。
local	設定された方式が失敗した場合の代替の認可方式を設定します（オプション）。

（注）　コンソール セッションから入力されたコマンドには、TACACS+ 許可は実行されません。

次の例は、*config* 特権レベルを必要とするコマンドの認可を設定する方法を示しています。最初の認可方式は TACACS+ に設定され、2 番目の認可方式はローカル ユーザ データベースに設定されています。

```
admin@GUARD-conf# aaa authorization commands config tacacs+ local
```

（注）　設定コマンド モードにアクセスできるようにするには、dynamic ユーザ特権レベルに対するアクセス権を付与するか、**configure** コマンドへのアクセス権を指定する必要があります。

TACACS+ サーバの設定例

TACACS+ サーバのデータベースで、各コマンドの許可を指定することができます。

次の例を参考にしてください。

```
user=Zoe {
    cmd = protect {
        permit .*
    }
    cmd = "no protect" {
        permit .*
    }
    cmd = learning {
        deny policy*
    }
    cmd = "no learning" {
        deny .*
    }
    cmd = dynamic-filter {
        permit .*
    }
    cmd = "no dynamic-filter" {
        permit .*
    }
    cmd = flex-filter {
        deny .*
    }
    cmd = "no flex-filter" {
        deny .*
    }
}
```

アカウンティングの設定

アカウンティング管理により、Guard のリソースの使用状況を追跡することができます。ユーザがアクセスしているサービスを追跡し、TACACS+ サーバにアカウンティング情報を保存することができます。

アカウンティングを設定するには、次の手順を実行します。

ステップ 1　TACACS+ サーバ接続を設定します。詳細については、P.3-15 の「TACACS+ サーバ接続の設定」を参照してください。

ステップ 2　複数の特権レベルのアカウンティングを設定するには、アカウンティングが必要な特権レベルごとにこのコマンドを発行します。次のように入力します。

```
admin@GUARD-conf# aaa accounting commands {show | dynamic | config |
admin} stop-only {local | tacacs+}
```

表 3-6 に、**aaa accounting** コマンドの引数とキーワードを示します。

表 3-6　aaa accounting コマンドのキーワード

パラメータ	説明
show | dynamic | config | admin	指定された特権レベルのアカウンティングを定義します。ユーザの特権レベルについては、表 2-4 を参照してください。
stop-only	要求されたユーザ処理の最後にアカウンティング停止通知を送信します。
tacacs+	アカウンティングに TACACS+ サーバのデータベースが使用されます。
local	アカウンティング情報は保存されません。

次の例は、TACACS+ サーバ上で *config* 特権レベルを必要とするコマンドのアカウンティングを設定する方法を示しています。

```
admin@GUARD-conf# aaa accounting commands config stop-only tacacs+
```

TACACS+ サーバ接続の設定

TACACS+ 認証方式を適用する前に、TACACS+ サーバのパラメータを設定しておく必要があります。TACACS+ サーバの設定には、次の内容が含まれます。

- サーバのアドレス（複数も可）：P.3-16 の「TACACS+ サーバの IP アドレスの設定」を参照してください。
- サーバの暗号キー：P.3-17 の「TACACS+ サーバの暗号キーの設定」を参照してください。
- 検索：P.3-17 の「TACACS+ の検索の設定」を参照してください。

- サーバのアクセス タイムアウト：P.3-18 の「TACACS+ サーバの接続タイムアウトの設定」を参照してください。

Guard のユーザ特権レベルは、TACACS+ の特権番号に次のように対応しています。

- admin = 15
- config = 10
- dynamic = 5
- show = 0

TACACS+ サーバの IP アドレスの設定

AAA に使用する TACACS+ サーバのシーケンシャルなリストを設定することができます。Guard は、リストされた TACACS+ サーバを使用してユーザを認証します。そのサーバが応答しない場合、Guard は 2 番目のサーバを選択します。リストされたすべてのサーバを試してもうまくいかない場合、AAA は失敗します。

または、Guard がリストの最初の TACACS+ サーバだけを使用してユーザを認証するように設定することもできます（詳細については、P.3-17 の「TACACS+ の検索の設定」を参照）。

リストには、各 TACACS+ サーバの IP アドレスを定義する必要があります。最大 9 つの TACACS+ サーバを定義できます。

リストに TACACS+ サーバを追加し、IP アドレスを割り当てるには、次のように入力します。

tacacs-server host *ip-address*

引数 *ip-address* には、TACACS+ サーバの IP アドレスを指定します。

TACACS+ サーバは、入力した順序でリストに追加されます。リストには、最大 9 つのサーバを追加できます。

次の例を参考にしてください。

```
admin@GUARD-conf# tacacs-server host 192.168.33.45
```

TACACS+ サーバの暗号キーの設定

TACACS+ サーバにアクセスするには、暗号キーを設定する必要があります。コマンドの一部として入力されるキーは、TACACS+ サーバ上のキーと一致している必要があります。キーにスペースを含めることはできません。

サーバの暗号アクセス キーを設定するには、次のように入力します。

tacacs-server key *tacacs-key*

引数 *tacacs-key* は、英数字の文字列です。

（注）　複数の TACACS+ サーバを使用している場合に定義できる暗号キーは 1 つだけです。このキーがすべての TACACS+ サーバとの通信の暗号化に使用されます。

次の例は、TACACS+ サーバの暗号キーを *MyTacacsKey* に設定する方法を示しています。

```
admin@GUARD-conf# tacacs-server key MyTacacsKey
```

TACACS+ の検索の設定

Guard が、1 つの認証拒否を最終的なものと見なし、他の TACACS+ サーバやローカル認証方式を使用したそれ以上の検索を中止するように設定することができます。この場合、Guard はローカルの認証方式にフォールバックせず、設定されている次の TACACS+ サーバ（存在する場合）にも移りません。

TACACS+ の検索方式は、認証にのみ適用されます。

Guard がリストの最初の TACACS+ サーバだけを使用してユーザを認証するように設定するには、次のように入力します。

tacacs-server first-hit

次の例を参考にしてください。

```
admin@GUARD-conf# tacacs-server first-hit
```

（注）　TACACS+ の検索方式を first-hit に設定しない場合、Guard はデフォルトでリスト内のすべての TACACS+ サーバでユーザを認証しようとします。

TACACS+ サーバの接続タイムアウトの設定

Guard が TACACS+ サーバの応答を待つ場合のタイムアウトを設定することができます。タイムアウトが終了すると、Guard は次の TACACS+ サーバ（そのようなサーバが設定されている場合）との接続を確立しようとするか、ローカルの AAA にフォールバックします（そのようなフォールバックが設定されている場合）。フォールバックの方式が設定されていない場合、認証と認可は失敗します。

（注）　すべての TACACS+ サーバとの通信に同じサーバ タイムアウトが使用されます。

TACACS+ サーバの接続タイムアウトを設定するには、次のように入力します。

tacacs-server timeout *timeout*

引数 *timeout* には、タイムアウトを秒単位で指定します。

次の例を参考にしてください。

```
admin@GUARD-conf# tacacs-server timeout 600
```

ヒント　ネットワークに問題がある場合や、小さいタイムアウト値を使用していて、TACACS+ サーバの応答が遅いためにタイムアウトが継続的に発生する場合には、タイムアウトの値を大きくすることができます。

TACACS+ サーバの統計の表示

TACACS+ サーバに関連する統計情報を表示することができます。統計データは、各サーバ対して提供されます。統計データには、次のフィールドがあります。

- **PASS**：サービスが TACACS+ サーバに正常にアクセスし、アクセス権を付与された回数。
- **FAIL**：サービスが TACACS+ サーバに正常にアクセスし、アクセス権を拒否された回数。
- **ERROR**：サービスが TACACS+ サーバにアクセスできなかった回数。

TACACS+ 関連の統計を表示するには、**show tacacs statistics** コマンドを使用します。

TACACS+ の統計をクリアするには、**clear tacacs statistics** コマンドを使用します。

Guard の設定の表示

Guard の設定ファイルを表示することができます。このファイルには、インターフェイスのアドレス、Guard のプロキシ アドレス、デフォルト ゲートウェイ アドレスなど、Guard の設定に関する情報が含まれています。

Guard の設定ファイルを表示するには、次のように入力します。

show running-config [all | Guard | interfaces *interface-name* | router | self-protection | zones]**]**

表 3-7 に、**show running-config** コマンドの引数とキーワードを示します。

表 3-7　show running-config コマンドの引数とキーワード

パラメータ	説明
all	Guard のすべてのモジュール（Guard、ゾーン、インターフェイス、ルータ、および自己保護）の設定ファイルを表示します。
Guard	Guard の設定ファイルを表示します。
interfaces	Guard のインターフェイスの設定ファイルを表示します。インターフェイス名を入力します。
router	ルータの設定を表示します。
self-protection	Guard の自己保護の設定を表示します。
zones	すべてのゾーンの設定ファイルを表示します。

次の例を参考にしてください。

```
admin@GUARD# show running-config guard
```

設定ファイルは、Guard を現在の設定値で設定するために実行されるコマンドで構成されています。Guard の設定ファイルをリモート FTP サーバにエクスポートして、バックアップ用にしたり、別の Guard にその Guard の設定パラメータを実装できるようにすることができます。詳細については、P.10-6 の「ログ ファイルの表示」を参照してください。

日付と時刻の設定

時刻と日付を設定するには、次のように入力します。

date *MMDDhhmm*[[*CC*]*YY*][*.ss*]

表 3-8 に、**date** コマンドの引数とキーワードを示します。

表 3-8　date コマンドの引数

パラメータ	説明
MM	数字で表した月。
DD	月の日付。
hh	24 時間表記の時間。
mm	分。
CC	（オプション）年の最初の 2 桁。
YY	（オプション）年の最後の 2 桁。
.ss	（オプション）秒。ピリオドが付いている必要があります。

次の例は、日付を *2003* 年 *10* 月　*8* 日に設定し、時刻を午後 *5* 時 *10* 分（17 時 10 分）*17* 秒に設定する方法を示しています。

```
admin@GUARD-conf# date 1008171003.17
Wed Oct  8 17:10:17 EDT 2003
```

Guard のクロックと NTP サーバの同期

Guard のシステム クロックとタイム サーバが同期するように設定することもできます。Guard のクロックが NTP サーバと同期するように設定するには、次の手順を実行します。

ステップ 1　日付と時刻をローカルに設定します。次のように入力します。

```
date MMDDhhmm[[CC]YY][.ss]
```

詳細については、P.3-21 の「日付と時刻の設定」を参照してください。

ステップ 2　Guard のシステムの時間帯を設定します。次のように入力します。

```
timezone timezone-name
```

引数 *timezone-name* には、目的の時間帯の名前を指定します。名前は、*陸地 / 都市* で構成されます。

陸地には、次のオプションがあります。

- Africa、America、Antarctica、Arctic、Asia、Atlantic、Australia、Europe、Indian、Pacific
- Etc：目的の時間帯のワイルド カード

ヒント　時間帯の名前では、大文字と小文字が区別されます。目的の陸地名を入力し、Tab キーを 2 回押すと、関連する都市のリストが表示されます。

ステップ 3　NTP サービスを有効にします。次のように入力します。

```
service ntp
```

ステップ 4　ネットワーク アドレスから NTP サービスへのアクセス権を付与します。次のように入力します。

```
permit ntp ip-address
```

ステップ 5　目的の NTP サーバの IP アドレスを設定します。次のように入力します。

```
ntp server ip-address
```

引数 *ip-address* には、NTP サーバの IP アドレスを指定します。

Guard の設定をリロードする必要があります。

次の例を参考にしてください。

```
admin@GUARD-conf# date 1008171003.17
admin@GUARD-conf# timezone Africa/Timbuktu
admin@GUARD-conf# service ntp
admin@GUARD-conf# permit ntp 192.165.200.224
admin@GUARD-conf# ntp server 192.165.200.224
```

SSH キーの管理

次の各項では、Guard の SSH キー リストの操作方法について説明します。

- SSH キーの追加
- SSH キーの削除

SSH キーの追加

ログイン名とパスワードを入力せずに SSH 接続を有効にするには、Guard の SSH キー リストにリモート接続の SSH 公開キーを追加します。

次のように入力します。

key add [user-*name*] {**ssh-dsa** | **ssh-rsa**} *key-string comment*

表 3-9 に、**key add** コマンドの引数とキーワードを示します。

表 3-9　key add コマンドの引数とキーワード

パラメータ	説明
user-name	（オプション）指定されたユーザの SSH キーを追加します。他のユーザの SSH キーを追加できるのは管理者だけです。 デフォルトは、現行ユーザの SSH キーの追加です。
ssh-dsa | **ssh-rsa**	SSH キーのタイプ。Guard は、SSH2-DSA と SSH2-RSA をサポートします。
key-string	Detector またはリモート端末で作成された公開 SSH キー。キーストリングは、8,192 ビットまでに制限されています。 キー タイプの識別（ssh-rsa または ssh-dsa）を除いた完全なキーをコピーする必要があります。
comment	デバイスの説明。コメントの形式は、通常、キーの生成に使用されるユーザとマシンを表す user@hostname になります。たとえば、Detector で生成される SSH 公開キーに使用されるデフォルトのコメントは、**root@DETECTOR** です。

次の例を参考にしてください。

```
admin@GUARD-conf# key add ssh-rsa 14513797528175730. . .user@Guard.com
```

SSH キーの削除

リストから SSH キーを削除できます。SSH キーを削除すると、次に Guard と SSH セッションを確立するときには認証を受ける必要があります。

Guard から SSH キーを削除するには、次のように入力します。

key remove [*user-name*] *key-string*

表 3-10 に、**key remove** コマンドの引数とキーワードを示します。

表 3-10　key remove コマンドの引数

パラメータ	説明
user-name	（オプション）指定のユーザの SSH キーを削除します。 他のユーザの SSH キーを削除できるのは管理者だけです。デフォルトは、現行ユーザの SSH キーの削除です。
key-string	削除する公開 SSH キー。 KEY プロンプトに SSH 公開キーをペーストします。識別フィールドは除き、キーだけをペーストしてください。

次の例を参考にしてください。

```
admin@GUARD-conf# show keys Lilac
ssh-rsa 2352345234523456... user@Guard.com
admin@GUARD-conf# key remove Lilac ssh-rsa 2352345234523456...
```

ホスト名の変更

Guard のホスト名を変更できます。この変更は、すぐに反映され、新しいホスト名は自動的にプロンプト ストリングに組み込まれます。

変更は、CLI プロンプトにも反映されます。

Guard のホスト名を変更するには、次のように入力します。

hostname *name*

引数 *name* には、新しいホスト名を指定します。

次の例を参考にしてください。

```
admin@GUARD-conf# hostname CiscoGuard
admin@CiscoGuard-conf#
```

SNMP トラップの有効化

Guard が SNMP トラップを送信し、Guard で発生する重大なイベントを管理者に通知するように設定することができます。Guard の SNMP Trap Generator を設定して、トラップ情報のスコープを定義することができます。

Guard が SNMP トラップを送信するように設定するには、次の手順を実行します。

ステップ 1　SNMP トラップ ジェネレータ サービスを有効にします。次のように入力します。

```
service snmp-trap
```

ステップ 2　SNMP Trap Generator のパラメータ（トラップの宛先アドレスとトラップ情報のスコープ）を設定します。次のように入力します。

```
snmp trap-dest ip-address [community-string-dest [min-severity]]
```

表 3-11 に、**snmp trap-dest** コマンドの引数を示します。

表 3-11　snmp trap-dest コマンドの引数

パラメータ	説明
ip-address	宛先ホストの IP アドレス。
community-string	（オプション）トラップとともに送信されるコミュニティ ストリング。このストリングは、宛先ホスト用に定義されたコミュニティ ストリングと一致する必要があります。デフォルトのコミュニティ ストリングは、*public* です。

表 3-11　snmp trap-dest コマンドの引数（続き）

パラメータ	説明
min-severity	（オプション）トラップ情報のスコープ。重大度レベルの範囲の下限を指定してスコープを定義します。この定義により、トラップは指定された重大度レベル以上のすべてのイベントを表示します。たとえば、重大度レベル *Warnings* を指定すると、トラップは *Warnings* から *Emergencies* までのすべての重大度レベルのイベントを表示します。重大度レベルのオプションを次に示します。 • **Emergencies**：システムは使用不能（重大度 = 0） • **Alerts**：即時のアクションが必要（重大度 = 1） • **Critical**：危険な状態（重大度 = 2） • **Errors**：エラー状態（重大度 = 3） • **Warnings**：警告状態（重大度 = 4） • **Notifications**：正常ではあるが、重要な状態（重大度 =5） • **Informational**:情報通知のためのメッセージ(重大度 = 6） • **Debugging**：デバッグ メッセージ（重大度 = 7） デフォルトでは、レポートにはすべての重大度レベルのイベントが表示されます。

次に、*errors* 以上の重大度レベルのトラップが、SNMP コミュニティ ストリング *tempo* とともに宛先 IP アドレス *192.168.100.52* に送信される例を示します。

```
admin@GUARD-conf# snmp trap-dest 192.168.100.52 tempo errors
```

（注）　トラップのログは、Guard のイベント ログに記録され、トラップ条件が発生すると、SNMP エージェントがトラップを送信するかどうかに関係なく、イベント モニタに表示されます。

SNMP コミュニティ ストリングの設定

Guard の SNMP コミュニティ ストリングを設定して、異なる組織のクライアントがそれぞれ異なるコミュニティ ストリングを使用して SNMP エージェントにアクセスできるようにすることができます。

SNMP コミュニティ ストリングを追加するには、次のように入力します。

snmp community *community-string*

引数 *community-string* には、目的の Guard のコミュニティ ストリングを指定します。このストリングは最大 15 文字の英数字で、スペースを含めることはできません。

（注）　Guard のデフォルトのコミュニティ ストリングは *riverhead* です。

Guard の自己保護

独立した IP アドレスを持つネットワーク要素としての Guard は、潜在的な DDoS 攻撃の危険にさらされています。デフォルトの設定では、このような攻撃に対する保護が提供されます。ユーザは、この自己防衛保護設定にアクセスし、変更することができます。

注意　Guard の自己防衛保護のデフォルト設定は変更しないことを強くお勧めします。不要な設定の結果として、Guard の自己保護機能に大きな支障をきたす場合があります。

Guard の自己防衛保護設定を変更するには、自己保護設定モードに入ります。次のように入力します。

self-protection

Guard の自己防衛保護に使用できるコマンドのセットは、通常のゾーンで使用できるものと同じです。ゾーンの設定の詳細については、第 5 章「ゾーンの設定」、第 6 章「ゾーンのフィルタの設定」、第 7 章「ポリシー テンプレートとポリシーの設定」、および第 8 章「インタラクティブ推奨モード」を参照してください。

Guard の自己保護設定ファイルを表示するには、**show running-config** コマンドを使用します。詳細については、「Guard の設定の表示」を参照してください。

フレックス フィルタのデフォルト設定

Guard のフレックス フィルタは、明示的な指定がない限り、デフォルトですべてのトラフィック フローをブロック（ドロップ）するように設定されています。表 3-12 に、Guard が適切に機能するために必要な通信を可能にするためのフレックス フィルタのデフォルト設定を示します。

表 3-12　フレックス フィルタのデフォルト設定

サービス	IP プロトコル	送信元ポート	宛先ポート	同期の許可
bgp	6	179	*	no
telnet	6	23	*	no
ftp-control	6	21	*	no
ftp-data	6	20	*	yes
tacacs	6	49	*	yes
ssh	6	22	*	no
ssh	6	*	22	yes
https	6	*	443	yes
icmp	1	*	*	—
snmp	17	*	161	—
ntp	17	*	123	—
ntp	17	123	*	—
ospf	89	*	*	—
rip	17	520	*	—
rip	17	*	520	—
gre	47	*	*	—

フレックス フィルタのデフォルト設定は、次の内容で構成されます。

- ポート 179 で、Guard によって開始される BGP 通信を有効化し、送信元ポート 179 の着信 SYN パケットをブロックする。この設定により、Guard によって開始される宛先変更元ルータへの BGP 接続が可能になります。
- ポート 23 で、Guard によって開始される telnet 通信を有効化し、送信元ポート 23 の着信 SYN パケットをブロックする。この設定により、Guard によって開始される宛先変更元ルータへの telnet 接続が可能になります。
- Guard によって開始される FTP サーバとの FTP 通信を有効化し、送信元ポート 21 で着信 FTP 制御 SYN パケットをブロックする。
- TACACS+ サーバとの TACACS 通信を有効化し、送信元ポート 49 からの着信 SYN パケットをブロックする。この設定により、認証、認可、アカウンティングのための TACACS+ サーバとの通信が可能になります。
- 着信および発信 SSH 通信を有効にする。
- 着信 HTTPS 通信を有効にする。
- ICMP 通信を有効にする。
- SNMP 通信を有効にする。
- NTP 通信を有効にする。
- OSPF 通信を有効にする。
- RIP 通信を有効にする。
- GRE 通信を有効にする。