



## A

### AAA

- アカウントティング 4-17
- 設定 4-5
- 認可 4-14
- 認証 4-7

aaa accounting コマンド 4-17

aaa authentication コマンド 4-7

aaa authorization コマンド 4-14

action コマンド 7-30

add-service コマンド 7-16

admin 特権レベル 3-2

always-accept 7-31

always-ignore 7-31

### AP

アップグレード 11-9

アップグレード、インライン 11-16

～からのブート 2-14

設定の消去 11-20

パスワードの消去 11-20, 11-22

arp コマンド 10-34

auth パケットタイプ 7-18

## B

boot コマンド 2-14

## C

CFE 11-11, 11-17, 11-19

clear ap config コマンド 11-20

clear ap password コマンド 11-20, 11-22

clear log コマンド 10-11

### CLI

エラー メッセージ 3-5

コマンドのショートカット 3-7

コマンドの発行 3-3

使用 3-2

タブ補完 3-6

プロンプトの変更 4-38

ヘルプの取得 3-6

config 特権レベル 3-2

copy guard-running-config コマンド 5-42

copy コマンド

ftp running-config 11-4

packet-dump 10-21

running-config 11-2

ゾーンのログ 10-10

レポート 9-12

ログ 10-7, 10-10

copy-from-this 5-7

copy-policies コマンド 7-46

counters

history 10-4

CPU 使用率 10-33

## D

date コマンド 4-34

### DDoS

概要 1-2

deactivate コマンド 5-19, 5-52

default-gateway コマンド 3-11

description コマンド 5-10

detect learning コマンド 5-18

detect コマンド 5-52

diff コマンド 7-43, 7-44

disable コマンド 7-12

### Distributed Denial of Service

「DDoS」を参照

### DNS

TCP プロトコルフロー 9-8

TCP ポリシー テンプレート 7-5

検出された異常 9-3

dst トラフィック特性 7-19

dst-ip-by-ip アクティベーション形態 5-46, 5-53

dst-ip-by-name アクティベーション形態 5-53

dynamic 特権レベル 3-2

## E

### enable

password コマンド 4-13

コマンド 4-13, 7-12

entire-zone アクティベーション形態 5-53

event monitor コマンド 10-7

export packet-dump コマンド 10-20

export reports コマンド 9-11

export コマンド 10-9

packet-dump 10-19

## F

facility 10-8

first-hit 4-21

fixed-threshold 7-25

flash-burn コマンド 11-19

### fragments

ポリシー テンプレート 7-5

ftp-server コマンド 5-39

## G

global トラフィック特性 7-20

GUARD 設定、エクスポート 5-42

Guard 保護のアクティベーション方式 5-53

guard-conf コマンド 5-32

## H

histogram コマンド 7-33

### hostname

コマンド 4-38

変更 4-38

### HTTP

検出された異常 9-3

ポリシー テンプレート 7-5

hw-module コマンド 2-13, 11-10, 11-11, 11-13, 11-16, 11-22

- I
- in パケット タイプ 7-18
  - interactive
    - ポリシーのステータス 7-31
  - interactive-status コマンド 7-31
  - ip address コマンド
    - インターフェイス 3-9
    - ゾーン 5-9
  - IP アドレス
    - 変更、ゾーン 5-10
  - IP スキャン 9-8
    - 検出された異常 9-3
    - ポリシー テンプレート 7-6
- K
- key コマンド
    - add 4-33, 4-35
    - generate 4-26, 4-31, 4-37
    - remove 4-36
- L
- learning
    - policy-construction コマンド 5-16
    - threshold-tuning コマンド 5-19
    - コマンド 5-17, 5-21
    - プロセスの終了 5-17, 5-21
  - learning accept コマンド 5-16, 5-20
  - learning-params
    - periodic-action コマンド 5-17, 5-20, 5-23, 5-35
    - threshold-multiplier コマンド 7-26
    - threshold-selection コマンド 5-20, 5-24
    - threshold-tuned コマンド 5-10, 5-26
  - learning-params fixed-threshold コマンド 7-25
  - learning-params コマンド 5-34
  - LINK テンプレート 5-15
  - logging コマンド 10-8
- M
- max-services コマンド 7-10
  - MIB、サポートされている 4-2
  - min-threshold コマンド 7-11
  - MP
    - アップグレード 11-13
    - アップグレード、インライン 11-16
    - ～からのブート 2-14
  - mtu コマンド 3-9
- N
- netstat コマンド 10-36
  - no learning コマンド 5-17, 5-21
  - non\_estb\_conns パケット タイプ 7-18
  - notify ポリシー アクション 7-30
  - ns ポリシー テンプレート 7-8
- O
- other\_protocols
    - ポリシー テンプレート 7-6
  - out\_pkts パケット タイプ 7-18

- P**
- packet-dump 10-12
    - auto-capture コマンド 10-15
    - エクスポート 10-19, 10-20, 10-21
    - シグニチャ 10-27
    - 自動
      - アクティブ化 10-14
      - 非アクティブ化 10-16
  - packet-dump コマンド 10-17
  - permit
    - コマンド 3-12, 3-14, 4-3
  - ping コマンド 10-41
  - pkts パケットタイプ 7-19
  - policy set-timeout コマンド 7-29
  - policy-template add-service コマンド 7-16
  - policy-template remove service コマンド 7-16
  - policy-type アクティベーション形態 5-54
  - power enable コマンド 2-14
  - protect コマンド 5-52
  - protect-ip-state コマンド 5-54
  - protocol トラフィック特性 7-20
- R**
- rates
    - history 10-4
  - reactivate-zones 11-6
  - reload コマンド 11-6
  - remote-activate ポリシーアクション 7-30
  - remote-guard コマンド 5-47
  - remove service コマンド 7-16
  - reqs パケットタイプ 7-19
  - reset コマンド 2-13
  - running-config
    - copy 11-2
    - copy ftp 11-4
    - show 10-2
- S**
- scanners トラフィック特性 7-20
  - service
    - snmp-trap 4-39
  - set-action 7-30
  - show public-key コマンド 4-38
  - show コマンド
    - counters 10-4
    - cpu 10-33
    - diagnostic-info 10-31
    - dynamic-filters 6-21
    - host-keys 4-28, 4-33
    - log export-ip 10-9
    - memory 10-32
    - packet-dump signatures 10-27
    - policies statistics 5-21
    - rates 10-4
    - recommendations pending-filters 8-6
    - running-config 10-2
    - show 10-3
      - 公開鍵 4-28, 4-33, 4-37
      - 推奨事項 8-4, 8-5
      - ゾーンのポリシー 7-36
      - テンプレート 5-7
      - 動的フィルタのソート 6-21

- ポリシー 7-36
  - ポリシーの統計情報 7-38
  - モジュール 2-3, 11-10, 11-13, 11-14
  - レポートの詳細 9-7
  - ロギング 10-9
  - ログ 10-9
  - show 特権レベル 3-2
  - shutdown コマンド 3-10
  - snapshot コマンド 7-40
  - SNMP、アクセス 4-2
  - snmp コマンド
    - community 4-41
    - trap-dest 4-39
  - SNMP、トラップ ジェネレータの設定 4-39
  - SPAN、設定 2-9
  - speed コマンド 3-9
  - src トラフィック特性 7-20
  - SSH
    - 鍵の削除 4-36
    - 鍵の生成 4-26, 4-31, 4-37
    - 公開鍵の表示 4-28, 4-33
    - サービス 3-14
    - 設定 3-14
    - ホスト鍵 4-27, 4-32
  - state コマンド 7-23
  - syn\_by\_fin パケットタイプ 7-19
  - sync コマンド 5-37, 5-38
  - syms パケットタイプ 7-19
  - syslog
    - エクスポートパラメータの設定 10-8
    - サーバの設定 10-9
    - メッセージの形式 10-8
- T
- TACACS+
    - 検索の設定 4-20
    - サーバの IP アドレス 4-19
    - サーバの暗号鍵 4-20
    - サーバの接続タイムアウト 4-21
    - サーバの設定 4-18
    - 統計情報の表示 4-22
    - 統計のクリア 4-22
    - 認証
      - key generate コマンド 4-25, 4-31
  - tacacs-server コマンド
    - clear statistics 4-22
    - first-hit 4-21
    - show statistics 4-22
    - timeout 4-22
    - 鍵 4-20
    - ホスト 4-19
- TCP
- 検出された異常 9-3, 9-8
  - プロキシが使用されない場合のポリシー テンプレート 7-8
  - ポリシー テンプレート 7-6
  - thresh-mult 7-27
  - threshold-list 7-28
  - threshold-selection 5-20
  - timeout コマンド 7-29
  - traceroute コマンド 10-39
  - trap 10-8
  - trap-dest 4-39

## U

## UDP

検出された異常 9-4

ポリシー テンプレート 7-7

unauth\_pkts パケット タイプ 7-19

upgrade コマンド 11-21

## username

暗号化されたパスワード 4-9

username コマンド 4-8

## V

VACL、設定 2-6

## W

## WBM

アクティブ化 3-12

## worm

ポリシー テンプレート 7-7

worm\_tcp ポリシー テンプレート 7-9

## X

XML スキーマ 9-11, 9-15, 10-19

## Z

## zone

コマンド 5-3, 5-7, 8-3

## あ

アカウントティング、設定 4-17

アクション フロー 9-10

## アップグレード

AP 11-9

MP 11-13

インライン 11-15

アプリケーション パーティション

「AP」を参照

## い

## 異常

検出された 9-3

フロー 9-5

イベント ログ 10-7

## インターフェイス

IP アドレスの設定 3-9

アクティブ化 3-8, 3-10

コマンド 3-9

## インタラクティブ

動作モード 8-3

インタラクティブ検出モード 1-7, 5-52

インタラクティブ保護モード 5-52

インライン アップグレード 11-15

## え

## エクスポート

設定ファイル 11-2

レポートを自動的に 9-11

ログ ファイル 10-10

エクスポート、GUARD 設定の 5-42

## か

カウンタ、表示 10-4

### 監視

ネットワーク トラフィック 10-12, 10-19,  
10-21

### 管理

SSH 3-14

VLAN 2-4

WBM 3-12

概要 3-12

ポート 2-4, 3-8, 3-9

## き

キャプチャ、パケット 10-17

## け

### 警告

記号の概要 xxv

### 検出

インタラクティブ モード 1-7, 5-52

自動モード 1-7, 5-52

### 検出された

異常 9-3

フロー 9-10

検出された攻撃 9-8

## こ

### 公開鍵

表示 4-37

### 攻撃のタイプ

検出された攻撃 9-8

### 攻撃レポート

エクスポート 9-11

エクスポート、自動的に 9-11

検出された異常 9-3

コピー 9-11, 9-12

タイミング 9-2

統計情報 9-3

表示 9-7

レイアウト 9-2

構築、ポリシー 5-15

コマンドのショートカット 3-7

コマンドライン インターフェイス

「CLI」を参照 3-2

## さ

### サービス

copy 7-46

wbm 3-12

アクセス権 4-3

イネーブル化 4-3

コマンド 3-12, 4-3

削除 7-16

追加 7-15

サービスのイネーブル化 4-3

## し

## しきい値

- 受け入れ前の乗算 7-26
- 固定値として設定 7-25
- コマンド 7-25
- 選択 7-41
- 調整 1-6, 5-13
- 調整済みのマーク付け 5-10, 5-26
- 特定の IP の設定 7-28
- ワーム 7-32

## シグニチャ

- 生成 10-26
- シグニチャの生成 10-26
- シグニチャの抽出 10-26
- 時刻、設定 4-34
- 自動検出モード 1-7, 5-52
- 自動保護モード 5-52

## す

## 推奨事項

- アクティブ化 8-3, 8-7
- 受け入れ 8-8
- 概要 8-2
- 決定の変更 7-31
- コマンド 8-7
- 通知の受信 8-2
- 非アクティブ化 8-3
- 表示 8-2, 8-4
- 保留フィルタの表示 8-6
- 無視 8-8

## スーパーバイザ モジュール

- サポートされているバージョン 11-7
- シャットダウン 2-13
- 設定 2-1
- 設定の確認 2-15
- 設定の保存 2-2
- 電源の切断 2-14
- ブート 2-14
- リセット 2-13
- スナップショット
- コマンド 7-41
- 比較 7-43
- 表示 7-44
- ポリシーのバックアップ 5-13, 7-42

## せ

## 設置

- 確認 2-2

## 設定

- スーパーバイザへの保存 2-2
- ファイル
- インポート 11-4
- エクスポート 11-2
- コピー 11-2
- 表示 10-2
- 設定コマンド 3-8

## そ

## ゾーン

- IP アドレス 5-9



- IP アドレスの変更 5-10
  - LINK テンプレート 5-15
  - オフラインでの同期 5-43
  - 検出 5-50
  - コピー 5-7
  - 再設定 5-9
  - 削除 5-7
  - 作成 5-3
  - 自動的な同期 5-34
  - ステータスの表示 10-3
  - 設定の同期 5-28
  - 設定の表示 5-11
  - 設定モード 5-9
  - 定義 1-4
  - テンプレート 5-5
  - 動作モード 5-4
  - 比較 7-44
  - 複製 5-7
  - ポリシーの表示 7-36
  - ラーニング 5-12
  - リモート Guard リスト 5-48
  - ゾーンのポリシー
    - 調整済みのマーク付け 5-10, 5-26
- た**
- 断片化 9-8
    - 検出された異常 9-3
- ち**
- 注意
    - 記号の概要 xxiv
- て**
- デフォルト設定、～に戻す テンプレート 11-20
    - LINK 5-15
    - ゾーン 5-5
    - ポリシーの表示 5-7
- と**
- 動的フィルタ 6-2
    - 概要 6-21
    - コマンド 6-24
    - 削除 6-24
    - ソート 6-21
    - 定義 1-8
    - ～の作成の防止 6-24
    - 表示 6-21
    - ワーム 7-35
  - 特定の IP しきい値 7-28
  - 特権レベル 3-2
    - ～の間の移動 4-13
    - パスワードの割り当て 4-13
  - トラフィック
    - 監視 10-12, 10-19, 10-21
    - トラフィックのキャプチャ 10-12
    - トラフィックの記録 10-12
    - トラフィックの送信元
      - SPAN 2-5
      - VACL 2-5
      - キャプチャ 2-5
      - 設定 2-5

- に
- 認可、設定 4-11, 4-12
  - 認識モジュール 10-32
  - 認証、設定 4-7
  - 認証されていない TCP の検出された異常 9-4
- は
- バークリー パケット フィルタ 6-13
  - バージョン、アップグレード 11-21
  - バイパス フィルタ
    - コマンド 6-19
    - 削除 6-20
    - 設定 6-19
    - 定義 6-2
    - 表示 6-20
    - 定義 1-8
  - ハイブリッド 9-8
  - パケット、キャプチャ 10-17
  - パスワード
    - 暗号化された 4-9
    - イネーブル化 4-13
    - 復旧 11-20, 11-22
    - 変更 4-10
  - パスワード、復旧 11-22
- ふ
- フィルタ
    - 概要 6-2
    - 動的 1-8, 6-2, 6-21
    - バイパス 1-8, 6-19
    - フレックスコンテンツ 1-8, 6-6
  - フラッシュの焼き付け 11-19
  - フレックスコンテンツ フィルタ
    - 設定 6-6
    - 定義 1-8, 6-2
    - 番号変更 6-7
    - 表示 6-15
  - フレックスコンテンツ フィルタの番号変更 6-7
  - プロキシ
    - プロキシが使用されない場合のポリシー テンプレート 7-8
    - プロキシが使用されない場合のポリシー テンプレート 7-8
  - 分析検出モジュール 7-18
- ほ
- ポート
    - 管理 3-8, 3-9
    - データ 3-8, 3-9
  - ポート スキャン 9-8
    - 検出された異常 9-3
    - ポリシー テンプレート 7-6
  - 他のプロトコル
    - 検出された異常 9-3
  - 保護
    - アクティベーション方式 5-53
    - 非アクティブ化 5-52
  - ホスト、ロギング 10-9
  - ホスト鍵
    - 削除 4-29, 4-33
  - ポリシー
    - action 7-30

- copy-policies 7-46
  - learning-params fixed-threshold コマンド 7-25
  - timeout 7-29
  - アクション 7-22, 7-30
  - アクティブ化 7-22
  - 現在の～のバックアップ 5-13, 7-42
  - 構造 7-2
  - 構築 1-6, 5-13, 5-15, 7-4
  - コマンド 7-21
  - サービスの削除 7-16
  - サービスの追加 7-15
  - しきい値 7-4, 7-22, 7-25
  - しきい値の乗算 7-27
  - しきい値の調整 1-6, 5-13, 5-18, 7-4
  - しきい値を固定 7-25
  - 状態 7-22
  - タイムアウト 7-22
  - 調整済みのマーク付け 5-10, 5-26
  - ディセーブル化 7-22
  - 統計情報の表示 5-21, 7-38
  - トラフィック特性 7-19
  - ナビゲーションパス 7-21
  - パケットタイプ 7-18
  - パラメータのコピー 7-46
  - 非アクティブ化 7-22
  - ポリシー テンプレート
    - max-services 7-10
    - min-threshold 7-11
    - worm\_tcp 7-9
    - 概要 7-5
    - コマンド 7-8, 7-9, 7-12
    - 状態 7-11
    - 設定コマンド レベル 7-9
    - パラメータ 7-9
    - ポリシーのしきい値の調整 5-18
    - 保留動的フィルタ 8-2
      - 表示 8-6
- め
- メモリ消費量 10-32
  - メンテナンス パーティション
    - 「MP」を参照
- も
- モジュール
    - 概要 7-18
    - 認識 10-32
    - 分析 7-18
- ゆ
- ユーザ
    - Admin 2-12
    - riverhead 2-12
    - 新しい～の追加 4-8
    - 検出された異常 9-4
    - 削除 4-9
    - 追加 4-8
    - 特権レベル 3-2, 4-12
    - 特権レベルの割り当て 4-8
  - ユーザ フィルタ
    - コマンド 6-7

## ら

## ラーニング

- 概要 5-12
- 結果の同期 5-14
- しきい値の調整 5-18
- ポリシーの構築 5-15

## り

## リポート

- パラメータ 11-6

## リモートの Guard

- アクティブ化 5-45
- コマンド 5-49
- デフォルト リスト 5-47
- リスト 5-48
- リストのアクティベーション順序 5-48

## れ

- レート、表示 10-4

## レポート

- 「攻撃レポート」を参照 9-2
- 詳細 9-7

## ろ

- ロギング、設定の表示 10-9

## ログ ファイル

- エクスポート 10-7, 10-10
- クリア 10-11
- 表示 10-9

## わ

## ワーム

- 概要 7-32
- 攻撃の識別 7-34
- しきい値 7-32, 7-33
- 動的フィルタ 7-35
- ポリシー 7-18, 7-20
- ポリシー テンプレート 7-33