



CHAPTER 1

Cisco FireSIGHT システムの概要	1-1
管理対象デバイスの概要	1-2
シリーズ 2 およびシリーズ 3 管理対象デバイス	1-3
64 ビット仮想管理対象デバイス	1-3
Blue Coat X-Series 向け Cisco NGIPS	1-4
Cisco ASA with FirePOWER Services	1-4
Cisco ISA 3000	1-5
管理対象デバイスの各モデルでサポートされる機能の概要	1-6
Snort プロセスを再開する構成	1-8
Snort の再開によるトラフィックへの影響	1-9
防御センターの概要	1-10
防御センターの各モデルでサポートされる機能の概要	1-11
バージョン 5.4.X で提供される 防御センター とデバイス	1-13
FireSIGHT システム のコンポーネント	1-15
冗長性およびリソース共有	1-15
ネットワーク トラフィックの管理	1-16
FireSIGHT	1-17
アクセス制御	1-18
SSL インспекション	1-18
侵入検知と侵入防御	1-19
高度なマルウェア防御とファイル制御	1-19
アプリケーションプログラミング インターフェイス	1-20
ドキュメント リソース	1-21
表記法	1-22
ライセンスの表記規則	1-22
サポートされるデバイスと 防御センター の表記規則	1-23
アクセスの表記規則	1-24
IP アドレスの表記規則	1-24

CHAPTER 2

FireSIGHT システム へのログイン	2-1
アプライアンスへのログイン	2-1
アプライアンスからのログアウト	2-5
コンテキスト メニューの使用	2-5

再利用可能なオブジェクトの管理	3-1
オブジェクト マネージャの使用	3-2
オブジェクトのグループ化	3-2
オブジェクトの参照、ソート、およびフィルタ	3-3
ネットワーク オブジェクトの操作	3-4
セキュリティ インテリジェンス リストとフィードの操作	3-5
グローバル ホワイトリストおよびブラックリストの操作	3-7
インテリジェンス フィードの操作	3-9
カスタム セキュリティ インテリジェンス フィードの操作	3-10
手動によるセキュリティ インテリジェンス フィードの更新	3-11
カスタム セキュリティ インテリジェンスのリストの操作	3-11
ポート オブジェクトの操作	3-13
VLAN タグ オブジェクトの操作	3-14
URL オブジェクトの操作	3-15
アプリケーション フィルタの操作	3-16
変数セットの使用	3-19
定義済みのデフォルトの変数の最適化	3-20
変数セットについて	3-22
変数セットの管理	3-24
変数の管理	3-26
変数の追加および編集	3-27
変数のリセット	3-34
変数のネスト	3-35
変数セットを侵入ポリシーにリンクさせる	3-37
拡張変数について	3-37
ファイル リストの操作	3-38
ファイル リストに複数の SHA-256 値をアップロードする	3-39
個別のファイルをファイル リストにアップロードする	3-41
ファイル リストに SHA-256 値を追加する	3-41
ファイル リスト上のファイルの変更	3-42
ファイル リストからソース ファイルをダウンロードする	3-43
セキュリティ ゾーンの操作	3-44
暗号スイート リストの操作	3-45
識別名オブジェクトの操作	3-46
PKI オブジェクトの操作	3-48
内部認証局オブジェクトの使用	3-49
信頼できる認証局オブジェクトの使用	3-54
外部証明書オブジェクトの使用	3-56

内部証明書オブジェクトの使用	3-57
地理位置情報オブジェクトの操作	3-58

CHAPTER 4

デバイスの管理	4-1
管理の概念	4-2
防御センターで管理できるデバイス	4-2
ポリシーとイベント以外の機能	4-3
冗長な 防御センター の使用	4-4
管理インターフェイスについて	4-4
1つの管理インターフェイスの使用	4-5
複数の管理インターフェイスの使用	4-5
トラフィック チャンネルの使用	4-6
ネットワーク ルートの使用	4-7
NAT 環境での作業	4-8
ハイ アベイラビリティの設定	4-9
ハイ アベイラビリティの使用	4-10
ハイ アベイラビリティを実装する際のガイドライン	4-14
ハイ アベイラビリティのセットアップ	4-15
ハイ アベイラビリティ ステータスのモニタリングおよび変更	4-16
ハイ アベイラビリティの無効化とデバイスの登録解除	4-18
ペアにされた 防御センター 間での通信の一時停止	4-19
ペアにされた 防御センター 間での通信の再開	4-19
デバイスの操作	4-19
[デバイス管理 (Device Management)] ページについて	4-20
リモート管理の設定	4-21
防御センター へのデバイスの追加	4-25
デバイスへの変更の適用	4-27
デバイス管理のリビジョン比較レポートの使用	4-28
デバイスの削除	4-29
デバイス グループの管理	4-29
デバイス グループの追加	4-29
デバイス グループの編集	4-30
デバイス グループの削除	4-31
デバイスのクラスタリング	4-31
デバイス クラスタの設定	4-35
デバイス クラスタの編集	4-36
クラスタ内の個々のデバイスの設定	4-37
クラスタ内の個々のデバイス スタックの設定	4-38
クラスタを構成するデバイスでのインターフェイスの設定	4-38

クラスタ内のアクティブ ピアの切り替え	4-39	
クラスタを構成するデバイスのメンテナンス モードの開始		4-40
クラスタを構成するスタック内のデバイスの交換	4-40	
クラスタ状態共有の設定	4-41	
クラスタ状態共有のトラブルシューティング	4-43	
クラスタを構成するデバイスの分離	4-46	
スタック構成のデバイスの管理	4-47	
デバイス スタックの確立	4-49	
デバイス スタックの編集	4-51	
スタックに含まれる個々のデバイスの設定	4-51	
スタック構成のデバイスでのインターフェイスの設定		4-52
スタック構成のデバイスの分離	4-53	
スタック内のデバイスの交換	4-53	
デバイス設定の編集	4-54	
一般的なデバイス設定の編集	4-54	
デバイス ライセンスの有効化と無効化	4-55	
デバイス システム設定の編集	4-56	
デバイスのヘルスの確認	4-58	
デバイス管理設定の編集	4-58	
高度なデバイス設定について	4-59	
詳細なデバイス設定の編集	4-61	
高速パス ルールの設定	4-62	
センシング インターフェイスの設定	4-66	
HA リンク インターフェイスの設定	4-69	
管理対象デバイスの MTU の範囲	4-70	
Cisco ASA with FirePOWER Services インターフェイスの管理		4-71
インターフェイスの無効化	4-72	
重複する接続ロギングの防止	4-73	

CHAPTER 5

IPS デバイスの設定 5-1

パッシブ IPS 展開について	5-1
パッシブ インターフェイスの設定	5-2
インライン IPS 展開について	5-3
インライン インターフェイスの設定	5-3
インライン セットの設定	5-5
インライン セットの表示	5-7
インライン セットの追加	5-7
インライン セットの詳細オプションの設定	5-9

インライン セットの削除 5-12

Blue Coat X シリーズ インターフェイス用の Cisco NGIPS の設定 5-13

CHAPTER 6

仮想スイッチのセットアップ 6-1

- スイッチド インターフェイスの設定 6-2
 - 物理スイッチド インターフェイスの設定 6-2
 - 論理スイッチド インターフェイスの追加 6-4
 - 論理スイッチド インターフェイスの削除 6-5
- 仮想スイッチの設定 6-6
 - 仮想スイッチの表示 6-6
 - 仮想スイッチの追加 6-7
 - 仮想スイッチの詳細設定 6-8
 - 仮想スイッチの削除 6-10

CHAPTER 7

仮想ルータのセットアップ 7-1

- ルーテッド インターフェイスの設定 7-2
 - 物理ルーテッド インターフェイスの設定 7-2
 - 論理ルーテッド インターフェイスの追加 7-5
 - 論理ルーテッド インターフェイスの削除 7-8
- SFRP の設定 7-9
- 仮想ルータの設定 7-10
 - 仮想ルータの表示 7-11
 - 仮想ルータの追加 7-11
 - DHCP リレーのセットアップ 7-13
 - スタティック ルートのセットアップ 7-15
 - ダイナミック ルーティングのセットアップ 7-17
 - RIP 設定のセットアップ 7-18
 - OSPF 設定のセットアップ 7-23
 - 仮想ルータ フィルタのセットアップ 7-32
 - 仮想ルータ 認証プロファイルの追加 7-34
 - 仮想ルータ 統計情報の表示 7-35
 - 仮想ルータの削除 7-36

CHAPTER 8

集約インターフェイスのセットアップ 8-1

- LAG の設定 8-2
 - ロード バランシング アルゴリズムの指定 8-3
 - リンク 選択ポリシーの指定 8-3
- LACP の設定 8-4
 - 集約スイッチド インターフェイスの追加 8-5

	集約ルーテッド インターフェイスの追加	8-8
	論理集約インターフェイスの追加	8-12
	集約インターフェイス統計情報の表示	8-14
	集約インターフェイスの削除	8-14
CHAPTER 9	ハイブリッド インターフェイスの設定	9-1
	論理ハイブリッド インターフェイスの追加	9-1
	論理ハイブリッド インターフェイスの削除	9-3
CHAPTER 10	ゲートウェイ VPN の使用	10-1
	IPSec について	10-1
	IKE について	10-2
	VPN 展開について	10-2
	ポイントツーポイントの VPN 展開について	10-3
	スター VPN 展開について	10-3
	メッシュ VPN 展開について	10-4
	VPN 展開の管理	10-5
	VPN 展開の設定	10-6
	高度な VPN 展開を設定する方法	10-14
	VPN 展開の適用	10-15
	VPN 展開のステータスの表示	10-16
	VPN の統計およびログの表示	10-17
	VPN 展開の比較ビューの使用	10-19
CHAPTER 11	NAT ポリシーの使用	11-1
	NAT ポリシーの計画と実装	11-2
	NAT ポリシーの設定	11-2
	NAT ポリシー ターゲットの管理	11-4
	NAT ポリシー内のルールの編成	11-5
	NAT ルールの警告とエラーの操作	11-7
	NAT ポリシーの管理	11-8
	NAT ポリシーの作成	11-9
	NAT ポリシーの編集	11-9
	NAT ポリシーのコピー	11-11
	NAT ポリシーの表示	11-11
	2つの NAT ポリシーの比較	11-12
	NAT ポリシーの適用	11-15
	NAT ルールの作成と編集	11-17

NAT ルール タイプについて	11-18	
NAT ルール条件と条件のしくみについて		11-20
NAT ルール条件について	11-21	
NAT ルールへの条件の追加	11-22	
NAT ルール条件リストの検索	11-24	
NAT ルールへのリテラル条件の追加	11-24	
NAT ルール条件でのオブジェクトの使用	11-25	
NAT ルールのさまざまな条件タイプの使用	11-25	
NAT ルールへのゾーン条件の追加	11-26	
ダイナミック NAT ルールへの送信元ネットワーク条件の追加		11-28
NAT ルールへの宛先ネットワーク条件の追加	11-29	
NAT ルールへのポート条件の追加	11-31	

CHAPTER 12

アクセス コントロール ポリシーの準備	12-1	
アクセス コントロールのライセンスおよびロール要件	12-2	
アクセス コントロールのライセンスおよびモデルの要件		12-3
カスタム ユーザ ロールによる展開の管理	12-4	
基本的なアクセス コントロール ポリシーの作成	12-6	
ネットワーク トラフィックに対するデフォルトの処理とインスペクションの設定	12-8	
アクセス コントロール ポリシーのターゲット デバイスの設定		12-10
アクセス コントロール ポリシーの管理	12-12	
アクセス コントロール ポリシーの編集	12-13	
失効したポリシーの警告について	12-16	
アクセス コントロール ポリシーの適用	12-17	
ポリシー全体の適用	12-19	
選択したポリシーの設定の適用	12-20	
アクセスコントロールポリシー適用中のトラフィックインスペクション		12-22
IPS または検出のみのパフォーマンスの考慮事項	12-23	
ネットワーク検出のみの展開の最適化	12-23	
検出なしの侵入検知と防御の実行	12-24	
アクセス コントロール ポリシーおよびルールのトラブルシューティング		12-25
パフォーマンスを向上させるためのルールの簡素化	12-26	
ルールのプリエンブションと無効な設定の警告について	12-27	
パフォーマンスを向上させプリエンブションを回避するためのルールの順序付け	12-28	
現在のアクセス コントロール設定のレポートの生成	12-30	
アクセス コントロール ポリシーの比較	12-31	

CHAPTER 13

セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録 13-1

セキュリティ インテリジェンス戦略の選択 13-2

セキュリティ インテリジェンスのホワイトリストおよびブラックリストの作成 13-4

ホワイトリストまたはブラックリストに追加するオブジェクトの検索 13-7

ホワイトリストまたはブラックリストに追加するオブジェクトの作成 13-8

CHAPTER 14

アクセス コントロール ルールを使用したトラフィック フローの調整 14-1

アクセス コントロール ルールの作成および編集 14-3

ルールの評価順序の指定 14-5

ルールが処理するトラフィックを指定するための条件の使用 14-6

ルール アクションを使用したトラフィックの処理とインスペクションの決定 14-8

ルールへのコメントの追加 14-14

ポリシー内のアクセス コントロール ルールの管理 14-15

アクセス コントロール ルールの検索 14-16

影響を受けるデバイス別のルールの表示 14-17

ルールの有効化と無効化 14-18

ルールの位置またはカテゴリの変更 14-19

CHAPTER 15

ネットワークベースのルールによるトラフィックの制御 15-1

セキュリティ ゾーンによるトラフィックの制御 15-2

ネットワークまたは地理的位置によるトラフィックの制御 15-4

VLAN トラフィックの制御 15-6

ポートおよび ICMP コードによるトラフィックの制御 15-8

CHAPTER 16

レピュテーションベースのルールによるトラフィックの制御 16-1

アプリケーション トラフィックの制御 16-2

トラフィックとアプリケーション フィルタの一致 16-4

個々のアプリケーションからのトラフィックの照合 16-5

アクセス コントロール ルールへのアプリケーション条件の追加 16-7

アプリケーション制御の制約事項 16-8

URL のブロッキング 16-10

レピュテーションベースの URL ブロッキングの実行 16-12

手動による URL ブロッキングの実行 16-15

URL の検出とブロッキングの制約事項 16-17

ユーザが URL ブロックをバイパスすることを許可 16-18

ブロックされた URL のカスタム Web ページの表示 16-21

CHAPTER 17

ユーザに基づくトラフィックの制御	17-1
アクセスコントロールルールへのユーザ条件の追加	17-3
アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得	17-4
ユーザ認識および制御のための LDAP サーバへの接続	17-5
オンデマンドによるユーザ制御パラメータの更新	17-9
LDAP サーバとの通信の一時停止	17-10
Active Directory のログインを報告するためのユーザ エージェントの使用	17-11

CHAPTER 18

侵入ポリシーおよびファイルポリシーを使用したトラフィックの制御	18-1
許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション	18-2
ファイルインスペクションおよび侵入インスペクションの順序について	18-5
AMPまたはファイル制御を実行するアクセスコントロールルールの設定	18-7
侵入防御を実行するアクセスコントロールルールの設定	18-8
侵入防御パフォーマンスの調整	18-10
侵入に対するパターン一致の制限	18-10
侵入ルールの正規表現制限のオーバーライド	18-11
パケットごとに生成される侵入イベントの制限	18-13
パケットおよび侵入ルール遅延しきい値の設定	18-14
侵入パフォーマンス統計情報のロギングの設定	18-20
ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整	18-21

CHAPTER 19

トラフィック復号の概要	19-1
SSL インスペクションの要件	19-2
SSL インスペクションをサポートするアプライアンスの展開	19-2
SSL インスペクションに必要なライセンスの特定	19-3
カスタム ユーザ ロールによる SSL インスペクション展開の管理	19-4
SSL ルールを設定するために必要な情報の収集	19-4
SSL インスペクションアプライアンス展開の分析	19-5
例:パッシブ展開でのトラフィック復号	19-6
例:インライン展開でのトラフィック復号	19-11

CHAPTER 20

SSL ポリシーの準備	20-1
基本 SSL ポリシーの作成	20-2
暗号化トラフィックに対するデフォルトの処理とインスペクションの設定	20-4
復号できないトラフィックのデフォルト処理の設定	20-5
SSL ポリシーの編集	20-8
アクセスコントロールを使用した復号設定の適用	20-10

現在のトラフィック復号設定のレポートの生成	20-11
SSL ポリシーの比較	20-13

CHAPTER 21

SSL ルールの準備 21-1

サポートする検査情報の設定	21-3
SSL ルールの概要と作成	21-4
SSL ルールの評価順序の指定	21-6
条件を使用した、ルールによる暗号化トラフィックの処理の指定	21-7
ルールアクションを使用した暗号化トラフィックの処理と検査の決定	21-9
[モニタ (Monitor)] アクション: アクションの遅延とログの確保	21-10
[復号しない (Do Not Decrypt)] アクション: 暗号化トラフィックを検査なしで転送	21-11
[ブロック (Block)] アクション: 検査なしで暗号化トラフィックをブロック	21-11
[復号 (Decrypt)] アクション: さらに検査するためにトラフィックを復号	21-11
ポリシー内の SSL ルールの管理	21-14
SSL ルールの検索	21-15
SSL ルールの有効化と無効化	21-16
SSL ルールの位置またはカテゴリの変更	21-16
SSL ルールのトラブルシューティング	21-18
パフォーマンスを改善する SSL インスペクション設定	21-23

CHAPTER 22

SSL ルールを使用したトラフィック復号の調整 22-1

ネットワーク ベースの条件による暗号化トラフィックの制御	22-2
ネットワーク ゾーンによる暗号化トラフィックの制御	22-2
ネットワークまたは地理的位置による暗号化トラフィックの制御	22-4
暗号化された VLAN トラフィックの制御	22-6
ポートによる暗号化トラフィックの制御	22-7
ユーザ ベースの暗号化トラフィックの制御	22-9
レピュテーションによる暗号化トラフィックの制御	22-10
アプリケーションベースの暗号化トラフィックの制御	22-11
URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御	22-17
暗号化のプロパティに基づいたトラフィックの制御	22-22
証明書の識別名による暗号化トラフィックの制御	22-22
証明書による暗号化トラフィックの制御	22-24
証明書ステータスによる暗号化トラフィックの制御	22-26
暗号スイートによる暗号化トラフィックの制御	22-30
暗号化プロトコルのバージョンによるトラフィックの制御	22-32

CHAPTER 23	ネットワーク分析ポリシーおよび侵入ポリシーについて	23-1
	ポリシーが侵入についてトラフィックを検査する仕組み	23-2
	デコード、正規化、前処理:ネットワーク分析ポリシー	23-4
	アクセスコントロールルール:侵入ポリシーの選択	23-5
	侵入インスペクション:侵入ポリシー、ルール、変数セット	23-6
	侵入イベントの生成	23-7
	システム付属ポリシーとカスタムポリシーの比較	23-8
	システム付属のポリシーについて	23-9
	カスタムポリシーの利点	23-10
	カスタムネットワーク分析ポリシーの利点	23-11
	カスタム侵入ポリシーの利点	23-12
	カスタムポリシーに関する制約事項	23-13
	ナビゲーションパネルの使用	23-16
	競合の解決とポリシー変更の確定	23-17
CHAPTER 24	ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用	24-1
	レイヤスタックについて	24-1
	基本レイヤについて	24-3
	FireSIGHT推奨レイヤについて	24-6
	レイヤの管理	24-7
	レイヤの追加	24-9
	レイヤの名前および説明の変更	24-9
	レイヤの移動、コピー、および削除	24-10
	レイヤのマージ	24-10
	ポリシー間のレイヤの共有	24-11
	レイヤでの侵入ルールの設定	24-13
	レイヤ内のプリプロセッサと詳細設定の設定	24-16
CHAPTER 25	トラフィックの前処理のカスタマイズ	25-1
	アクセスコントロールのデフォルト侵入ポリシーの設定	25-1
	ネットワーク分析ポリシーによる前処理のカスタマイズ	25-3
	アクセスコントロールのデフォルトネットワーク分析ポリシーの設定	25-4
	ネットワーク分析ルールを使用して前処理するトラフィックの指定	25-5
	ネットワーク分析ルールの管理	25-10
CHAPTER 26	ネットワーク分析ポリシーの準備	26-1
	カスタムネットワーク分析ポリシーの作成	26-2
	ネットワーク分析ポリシーの管理	26-3

ネットワーク分析ポリシーの編集	26-4
インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する	26-6
ネットワーク分析ポリシーでのプリプロセッサの設定	26-7
現在のネットワーク分析設定のレポートの生成	26-10
2つのネットワーク分析ポリシーまたはリビジョンの比較	26-11

CHAPTER 27

アプリケーション層プリプロセッサの使用	27-1
DCE/RPC トラフィックのデコード	27-2
グローバル DCE/RPC オプションの選択	27-3
ターゲットベース DCE/RPC サーバポリシーについて	27-5
DCE/RPC トランスポートについて	27-6
DCE/RPC ターゲットベースポリシーオプションの選択	27-9
DCE/RPC プリプロセッサの設定	27-13
DNS ネームサーバ応答におけるエクスプロイトの検出	27-16
DNS プリプロセッサリソースレコードインスペクションについて	27-16
RData テキストフィールドに対するオーバーフローの試行の検出	27-18
古い DNS リソースレコードタイプの検出	27-18
試験的な DNS リソースレコードタイプの検出	27-19
DNS プリプロセッサの設定	27-19
FTP および Telnet トラフィックのデコード	27-20
グローバル FTP および Telnet オプションについて	27-21
グローバル FTP/Telnet オプションの設定	27-21
Telnet オプションについて	27-22
Telnet オプションの設定	27-23
サーバレベルの FTP オプションについて	27-24
サーバレベルの FTP オプションの設定	27-27
クライアントレベルの FTP オプションについて	27-30
クライアントレベル FTP オプションの設定	27-31
HTTP トラフィックのデコード	27-34
グローバル HTTP 正規化オプションの選択	27-34
グローバル HTTP 設定オプションの設定	27-36
サーバレベル HTTP 正規化オプションの選択	27-36
サーバレベル HTTP 正規化エンコードオプションの選択	27-45
HTTP サーバオプションの設定	27-47
追加の HTTP Inspect プリプロセッサルールの有効化	27-49
Sun RPC プリプロセッサの使用	27-50
Sun RPC プリプロセッサの設定	27-51
Session Initiation Protocol のデコード	27-52

SIP プリプロセッサ オプションの選択	27-53
SIP プリプロセッサの設定	27-55
追加の SIP プリプロセッサ ルールの有効化	27-55
GTP コマンド チャンネルの設定	27-57
IMAP トラフィックのデコード	27-58
IMAP プリプロセッサ オプションの選択	27-58
IMAP プリプロセッサの設定	27-60
追加の IMAP プリプロセッサ ルールの有効化	27-61
POP トラフィックのデコード	27-62
POP プリプロセッサ オプションの選択	27-62
POP プリプロセッサの設定	27-64
追加の POP プリプロセッサ ルールの有効化	27-65
SMTP トラフィックのデコード	27-65
SMTP デコードについて	27-65
SMTP デコードの設定	27-70
SMTP 最大デコード メモリ アラートの有効化	27-73
SSH プリプロセッサによるエクスプロイトの検出	27-73
SSH プリプロセッサ オプションの選択	27-74
SSH プリプロセッサの設定	27-77
SSL プリプロセッサの使用	27-77
SSL 前処理について	27-78
SSL プリプロセッサ ルールの有効化	27-79
SSL プリプロセッサの設定	27-80

CHAPTER 28

SCADA の前処理の設定 28-1

Modbus プリプロセッサの設定	28-1
DNP3 プリプロセッサの設定	28-3
CIP プリプロセッサの設定	28-5
CIP イベントについて	28-7

CHAPTER 29

トランスポート層およびネットワーク層の前処理の設定 29-1

トランスポート/ネットワークの詳細設定の構成	29-2
VLAN 見出しの無視	29-2
侵入廃棄ルールでのアクティブ応答の開始	29-3
トラブルシューティング:セッション終了メッセージのロギング	29-5
チェックサムの検証	29-6
インライン トラフィックの正規化	29-7
IP パケットの最適化	29-13

IP フラグメンテーションの 익스プロイトについて	29-13
ターゲットベースの最適化ポリシー	29-14
最適化オプションの選択	29-15
IP 最適化の設定	29-17
パケットのデコードについて	29-18
パケットのデコードの設定	29-21
TCP ストリームの前処理の使用	29-22
状態関連の TCP 익스プロイトについて	29-23
TCP グローバル オプションの選択	29-24
ターゲットベースの TCP ポリシーについて	29-24
TCP ポリシーのオプションの選択	29-26
TCP ストリームの再構成	29-30
TCP ストリームの前処理の設定	29-32
UDP ストリームの前処理の使用	29-35
UDP ストリームの前処理の設定	29-36

CHAPTER 30

パッシブ展開における前処理の調整	30-1
適応型プロファイルについて	30-1
プリプロセッサによる適応型プロファイルの使用	30-2
適応型プロファイルと FireSIGHT 推奨ルール	30-3
適応型プロファイルの設定	30-3

CHAPTER 31

侵入ポリシーの準備	31-1
カスタム侵入ポリシーの作成	31-2
侵入ポリシーの管理	31-3
侵入ポリシーの編集	31-4
インライン展開でのドロップ動作の設定	31-6
侵入ポリシーの詳細設定の設定	31-7
侵入ポリシーの適用	31-9
現在の侵入設定のレポートの生成	31-10
2つの侵入ポリシーまたはリビジョンの比較	31-11

CHAPTER 32

ルールを使用した侵入ポリシーの調整	32-1
侵入防御ルールタイプについて	32-2
侵入ポリシー内のルールの表示	32-3
ルール画面のソート	32-5
ルール詳細の表示	32-5
侵入ポリシー内のルールのフィルタリング	32-11

	侵入ポリシー内のルール フィルタリングについて	32-11
	侵入ポリシー内のルール フィルタの設定	32-22
	ルール状態の設定	32-23
	ポリシー単位の侵入イベント通知のフィルタリング	32-26
	イベントしきい値の設定	32-26
	侵入ポリシー単位の抑制の設定	32-31
	動的ルール状態の追加	32-34
	動的ルール状態について	32-34
	動的ルール状態の設定	32-36
	SNMP アラートの追加	32-38
	ルール コメントの追加	32-39
CHAPTER 33	ネットワーク資産に応じた侵入防御の調整	33-1
	基本ルール状態推奨について	33-2
	高度なルール状態推奨について	33-3
	検査するネットワークについて	33-3
	ルール オーバーヘッドについて	33-3
	FireSIGHT 推奨の使用	33-4
CHAPTER 34	特定の脅威の検出	34-1
	Back Orifice の検出	34-2
	ポートスキャンの検出	34-3
	ポートスキャン検出の設定	34-5
	ポートスキャン イベントについて	34-7
	レート ベース攻撃の防止	34-10
	レート ベース攻撃の防止について	34-10
	レート ベース攻撃防止とその他のフィルタ	34-13
	レート ベース攻撃防止の設定	34-18
	センシティブ データの検出	34-20
	センシティブ データ検出の導入	34-21
	グローバルセンシティブ データ検出オプションの選択	34-21
	個別データ タイプ オプションの選択	34-22
	定義済みデータ タイプの使用	34-24
	センシティブ データ検出の設定	34-25
	モニタするアプリケーションプロトコルの選択	34-27
	特殊な場合:FTP トラフィックでのセンシティブ データの検出	34-29
	カスタム データ タイプの使用	34-29

CHAPTER 35	侵入イベント ロギングのグローバルな制限	35-1
	しきい値について	35-1
	しきい値のオプションについて	35-2
	グローバルしきい値の設定	35-3
	グローバルしきい値の無効化	35-4
CHAPTER 36	侵入ルールの理解と作成	36-1
	ルール構造について	36-2
	ルール ヘッダーについて	36-3
	ルールアクションの指定	36-4
	プロトコルの指定	36-5
	侵入ルールでの IP アドレスの指定	36-5
	侵入ルールでのポートの定義	36-9
	方向の指定	36-10
	ルールでのキーワードと引数について	36-11
	侵入イベント詳細の定義	36-12
	コンテンツ一致の検索	36-16
	コンテンツ一致の制約	36-20
	インライン展開でのコンテンツの置換	36-33
	Byte_Jump と Byte_Test の使用	36-34
	PCRE を使用したコンテンツの検索	36-39
	ルールへのメタデータの追加	36-46
	IP ヘッダー値の検査	36-51
	ICMP ヘッダー値の検査	36-54
	TCP ヘッダー値とストリーム サイズの検査	36-55
	TCP ストリーム再構築の有効化と無効化	36-60
	セッションからの SSL 情報の抽出	36-60
	アプリケーション層プロトコル値の検査	36-62
	パケット特性の検査	36-87
	パケットデータをキーワード引数の中に読み込む	36-90
	ルールキーワードを使用したアクティブ応答の開始	36-93
	イベントのフィルタリング	36-96
	攻撃後トラフィックの評価	36-98
	複数のパケットに及ぶ攻撃の検出	36-99
	HTTP エンコードのタイプと位置によるイベントの生成	36-104
	ファイルタイプとバージョンの検出	36-106
	特定のペイロードタイプを指し示す	36-108
	パケットペイロードの先頭を指し示す	36-109
	Base64 データのデコードと検査	36-110

ルールの構築	36-112
新しいルールの作成	36-112
既存のルールの変更	36-114
ルールへのコメントの追加	36-115
カスタム ルールの削除	36-116
ルールの検索	36-117
[ルール エディタ (Rule Editor)] ページでのルールのフィルタリング	36-119
ルール フィルタでのキーワードの使用	36-119
ルール フィルタでの文字列の使用	36-121
ルール フィルタでのキーワードと文字列の組み合わせ	36-121
ルールのフィルタリング	36-122

CHAPTER 37

マルウェアと禁止されたファイルのブロッキング	37-1
マルウェア防御とファイル制御について	37-2
マルウェア防御とファイル制御の設定	37-6
マルウェア防御とファイル制御に基づくイベントのロギング	37-7
FireAMP と FireSIGHT システムの統合	37-8
ネットワークベースの AMP とエンドポイント ベースの FireAMP の比較	37-9
ファイル ポリシーの概要と作成	37-11
ファイル ポリシーの作成	37-19
ファイル ルールの操作	37-20
ファイル ポリシーの詳細オプション([一般(General)])の設定	37-23
アーカイブ ファイルのインスペクション オプションの設定	37-24
2つのファイル ポリシーの比較	37-28
FireAMP 用のクラウド接続の操作	37-29
シスコ クラウド接続の作成	37-31
クラウド接続の削除または無効化	37-32
FireAMP プライベート クラウドの操作	37-33

CHAPTER 38

ネットワーク トラフィックの接続のロギング	38-1
どの接続をログに記録するか決定	38-2
クリティカルな接続のロギング	38-3
接続の開始または終了のロギング	38-5
Defense Center または外部サーバへの接続のロギング	38-6
アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて	38-7
接続ロギングのライセンスおよびモデル要件	38-11
セキュリティ インテリジェンス(ブラックリスト登録)の決定のロギング	38-13
暗号化された接続のロギング	38-15

SSL ルールによる復号可能接続のロギング	38-15
暗号化された接続および復号できない接続のデフォルトのロギング設定	38-16
アクセス コントロールの処理に基づく接続のロギング	38-18
アクセス コントロール ルールに一致する接続のロギング	38-18
アクセス コントロールのデフォルト アクションによって処理された接続のロギング	38-20
接続で検出された URL のロギング	38-22

CHAPTER 39

接続およびセキュリティ インテリジェンスのデータの使用	39-1
接続およびセキュリティ インテリジェンスのデータについて	39-2
接続サマリーについて	39-3
接続およびセキュリティ インテリジェンスのデータ フィールドについて	39-4
接続 イベントとセキュリティ インテリジェンス イベントで利用可能な情報	39-12
接続データとセキュリティ インテリジェンスのデータの表示	39-17
接続グラフの使用	39-18
グラフ タイプの変更	39-20
データセットの選択	39-22
集約された接続データに関する情報の表示	39-25
ワークフロー ページでの接続グラフの操作	39-26
接続データ グラフのドリルダウン	39-26
折れ線グラフのズームと再センタリング	39-27
グラフのデータを選択する	39-28
接続グラフの分離	39-29
接続データのエクスポート	39-30
接続およびセキュリティ インテリジェンスのデータ テーブルの使用	39-30
モニター ルールに関連付けられたイベントの使用	39-32
接続で検出されたファイルの表示	39-33
接続に関連付けられた侵入イベントの表示	39-34
暗号化接続に関連付けられた証明書の表示	39-34
接続およびセキュリティ インテリジェンスのデータの検索	39-35
接続サマリー ページの表示	39-42

CHAPTER 40

マルウェアとファイル アクティビティの分析	40-1
ファイル ストレージの操作	40-2
キャプチャ ファイル ストレージについて	40-3
保存されているファイルの別の場所へのダウンロード	40-4
動的分析の操作	40-5
Spero 分析について	40-6

動的分析のためのファイルの送信	40-6	
脅威スコアおよび動的解析のサマリーの確認	40-7	
ファイルイベントの操作	40-8	
ファイルイベントの表示	40-9	
ファイルイベントテーブルについて	40-10	
ファイルイベントの検索	40-14	
マルウェア イベントの操作	40-18	
マルウェア イベントの表示	40-20	
マルウェア イベントテーブルについて	40-22	
マルウェア イベントの検索	40-29	
キャプチャ ファイルの操作	40-33	
キャプチャ ファイルの表示	40-34	
キャプチャ ファイルテーブルについて	40-35	
キャプチャ ファイルの検索	40-37	
ネットワーク ファイル トラジェクトリの操作	40-39	
ネットワーク ファイル トラジェクトリの確認	40-40	
ネットワーク ファイル トラジェクトリの分析	40-42	

CHAPTER 41

侵入イベントの操作	41-1	
侵入イベントの統計の表示	41-2	
ホスト統計情報	41-3	
イベントの概要	41-4	
イベント統計情報	41-4	
侵入イベントのパフォーマンスの表示	41-5	
侵入イベントのパフォーマンス統計グラフの生成	41-5	
侵入イベント グラフの表示	41-10	
侵入イベントの表示	41-10	
侵入イベントについて	41-12	
侵入イベントと関連付けられた接続データの表示	41-17	
侵入イベントの確認	41-18	
侵入イベントのワークフロー ページについて	41-20	
ドリルダウン ページとテーブル ビュー ページの使用	41-21	
パケット ビューの使用	41-25	
イベント情報の表示	41-27	
フレーム情報の表示	41-35	
データリンク層情報の表示	41-36	
ネットワーク層情報の表示	41-36	
トランスポート層情報の表示	41-39	

パケット バイト情報の表示	41-41
影響レベルを使用してイベントを評価する	41-41
プリプロセッサ イベントの読み取り	41-43
プリプロセッサ イベントのパケットの表示について	41-44
プリプロセッサ ジェネレータ ID の読み取り	41-44
侵入イベントの検索	41-46
クリップボードの使用	41-54
クリップボードのレポートの生成	41-55
クリップボードからのイベントの削除	41-56

CHAPTER 42

インシデント対応	42-1
インシデント対応の基本	42-1
インシデントの定義	42-2
共通のインシデント対応プロセス	42-2
FireSIGHT システムのインシデント タイプ	42-5
インシデントの作成	42-5
インシデントの編集	42-6
インシデント レポートの生成	42-7
カスタム インシデント タイプの作成	42-8

CHAPTER 43

外部アラートの設定	43-1
アラート応答の使用	43-2
電子メール アラート応答の作成	43-3
SNMP アラート応答の作成	43-4
Syslog アラート応答の作成	43-5
アラート応答の変更	43-8
アラート応答の削除	43-8
アラート応答の有効化と無効化	43-8
影響フラグ アラートの設定	43-9
ディスカバ イベント アラートの設定	43-9
高度なマルウェア対策アラートの設定	43-10

CHAPTER 44

侵入ルールの外部アラートの設定	44-1
SNMP 応答の使用	44-2
SNMP 応答の設定	44-3
Syslog 応答の使用	44-4
syslog 応答の設定	44-6

電子メールアラートについて	44-7
電子メールアラートの設定	44-9

CHAPTER 45

ネットワーク検出の概要	45-1
検出データ収集について	45-2
ホスト データ収集について	45-3
ユーザ データ収集について	45-3
アプリケーション検出について	45-11
サードパーティ検出データのインポート	45-17
検出データの用途	45-17
NetFlow について	45-18
NetFlow と FireSIGHT データの違い	45-19
NetFlow データの分析準備	45-21
侵害の兆候(痕跡)について	45-22
侵害の兆候タイプについて	45-22
侵害の兆候(痕跡)データの表示と編集	45-24
ネットワーク検出ポリシーの作成	45-25
検出ルールの操作	45-26
ユーザ ログインの制限	45-33
高度なネットワーク検出オプションの設定	45-34
ネットワーク検出ポリシーの適用	45-42

CHAPTER 46

ネットワーク検出の拡張	46-1
検出戦略の評価	46-2
管理対象デバイスが正しく配置されているか	46-2
未確認のオペレーティング システムに一意的 TCP スタックがあるか	46-2
FireSIGHT システムがすべてのアプリケーションを識別できるか	46-3
脆弱性の修正パッチを適用したか	46-3
サードパーティの脆弱性を追跡するか	46-4
ネットワーク マップの拡張	46-4
パッシブ検出について	46-4
アクティブ検出について	46-5
現在の ID について	46-5
ID の競合について	46-7
カスタム フィンガープリントの使用	46-8
クライアントフィンガープリントの作成	46-9
サーバフィンガープリントの作成	46-12
フィンガープリントの管理	46-15
フィンガープリントのアクティブ化	46-15

フィンガープリントの非アクティブ化	46-16
フィンガープリントの削除	46-16
フィンガープリントの編集	46-17
アプリケーションディテクタの操作	46-19
ユーザ定義のアプリケーションプロトコルディテクタの作成	46-21
ディテクタの管理	46-26
ホスト入力データのインポート	46-32
サードパーティデータの使用の有効化	46-33
サードパーティ製品マッピングの管理	46-33
サードパーティの脆弱性のマッピング	46-37
カスタム製品マッピングの管理	46-38

CHAPTER 47

アクティブスキヤンの設定	47-1
Nmap スキャンの概要	47-1
Nmap 修復の概要	47-2
Nmap スキャン戦略の作成	47-6
サンプルの Nmap スキャンプロファイル	47-7
Nmap スキャンのセットアップ	47-10
Nmap スキャンインスタンスの作成	47-10
Nmap スキャンターゲットの作成	47-11
Nmap 修復の作成	47-13
Nmap スキャンの管理	47-17
Nmap スキャンインスタンスの管理	47-17
Nmap 修復の管理	47-18
オンデマンド Nmap スキャンの実行	47-19
スキャンターゲットの管理	47-20
スキャンターゲットの編集	47-21
スキャンターゲットの削除	47-21
アクティブスキヤンの結果での作業	47-22
スキャン結果の表示	47-22
スキャン結果テーブルについて	47-24
スキャン結果の分析	47-24
スキャンのモニタリング	47-24
スキャン結果のインポート	47-25
スキャン結果の検索	47-26

CHAPTER 48

ネットワークマップの使用	48-1
ネットワークマップについて	48-2
ホストのネットワークマップの操作	48-2

ネットワーク デバイスのネットワーク マップの操作	48-4
侵入の痕跡のネットワーク マップの操作	48-5
モバイルデバイスのネットワーク マップの操作	48-6
アプリケーションのネットワーク マップの操作	48-7
脆弱性のネットワーク マップの操作	48-8
ホスト属性のネットワーク マップの操作	48-10
カスタム ネットワーク トポロジの操作	48-11
カスタム トポロジの作成	48-12
カスタム トポロジの管理	48-16
CHAPTER 49	ホスト プロファイルの使用 49-1
ホスト プロファイルの表示	49-5
ホスト プロファイルの基本的なホスト情報の使用	49-6
ホスト プロファイルの IP アドレスの操作	49-8
ホスト プロファイルでの侵害の兆候の使用	49-9
単一ホストにおける侵害の兆候のルール状態の編集	49-10
侵害の兆候に対するソース イベントの表示	49-10
侵害の兆候を解決済みにする	49-11
ホスト プロファイルでのオペレーティング システムの使用	49-12
オペレーティング システムのアイデンティティの表示	49-14
オペレーティング システムの編集	49-14
オペレーティング システムのアイデンティティの競合を解決する	49-15
ホスト プロファイルでのサーバの使用	49-17
サーバの詳細	49-19
サーバのアイデンティティの編集	49-20
サーバアイデンティティの競合の解決	49-22
ホスト プロファイルでのアプリケーションの使用	49-22
ホスト プロファイルでのアプリケーションの表示	49-23
ホスト プロファイルからのアプリケーションの削除	49-24
ホスト プロファイルでの VLAN タグの使用	49-24
ホスト プロファイルでのユーザ履歴の使用	49-25
ホスト プロファイルでのホスト属性の使用	49-25
ホスト属性の値の割り当て	49-26
ホスト プロファイルでのホストプロトコルの使用	49-26
ホスト プロファイルにおけるホワイト リスト違反の使用	49-27
ホスト プロファイルからのホワイト リスト ホスト プロファイルの作成	49-28
ホスト プロファイルでのマルウェア検出の使用	49-29

ホスト プロファイルでの脆弱性の使用	49-29
脆弱性の詳細の表示	49-31
脆弱性の Impact Qualification の設定	49-32
脆弱性に対するパッチのダウンロード	49-33
個々のホストに対する脆弱性の設定	49-34
事前定義のホスト属性の使用	49-34
ユーザ定義のホスト属性の使用	49-35
ユーザ定義のホスト属性の作成	49-36
ユーザ定義ホスト属性の編集	49-38
ユーザ定義ホスト属性の削除	49-39
ホスト プロファイルでのスキャン結果の使用	49-39
ホスト プロファイルからのホストのスキャン	49-40

CHAPTER 50

ディスクバリ イベントの使用	50-1
ディスクバリ イベントの統計情報の表示	50-2
統計情報のサマリ	50-3
イベント分類 (Event Breakdown)	50-4
プロトコル分類 (Protocol Breakdown)	50-5
アプリケーションプロトコル分類 (Application Protocol Breakdown)	50-5
OS 分類 (OS Breakdown)	50-5
ディスクバリのパフォーマンス グラフの表示	50-6
ディスクバリ イベントのワークフローについて	50-7
ディスクバリ イベントとホスト入力イベントの使用	50-9
ディスクバリ イベントのタイプについて	50-10
ホスト入力イベントのタイプについて	50-14
ディスクバリ イベントおよびホスト入力イベントの表示	50-16
ディスクバリ イベント テーブルについて	50-17
ディスクバリ イベントの検索	50-18
ホストの使用	50-21
ホストの表示	50-21
ホスト テーブルについて	50-22
選択したホストのトラフィック プロファイルの作成	50-26
選択したホストに基づいたコンプライアンスのホワイト リストの作成	50-26
ホストの検索	50-27
ホスト属性の使用	50-30
ホスト属性の表示	50-30
ホスト属性のテーブルについて	50-31
選択したホストのホスト属性の設定	50-32
ホスト属性の検索	50-33

侵入の痕跡の使用	50-35	
侵入の痕跡の表示	50-36	
侵害の痕跡テーブルについて	50-37	
侵害の痕跡の検索	50-37	
サーバの使用	50-39	
サーバの表示	50-40	
サーバのテーブルについて	50-41	
サーバの検索	50-43	
アプリケーションの使用	50-45	
アプリケーションの表示	50-46	
アプリケーションテーブルについて	50-46	
アプリケーションの検索	50-48	
アプリケーションの詳細の使用	50-49	
アプリケーションの詳細の表示	50-50	
アプリケーションの詳細テーブルについて	50-51	
アプリケーションの詳細の検索	50-52	
脆弱性の処理	50-54	
脆弱性の表示	50-55	
脆弱性テーブルについて	50-56	
脆弱性の非アクティブ化	50-58	
脆弱性の検索	50-58	
サードパーティの脆弱性の処理	50-60	
サードパーティの脆弱性の表示	50-61	
サードパーティの脆弱性テーブルについて	50-62	
サードパーティの脆弱性の検索	50-63	
ユーザの使用	50-65	
ユーザの表示	50-66	
ユーザテーブルについて	50-67	
ユーザの詳細とホストの履歴について	50-68	
ユーザの検索	50-69	
ユーザ アクティビティの使用	50-71	
ユーザ アクティビティ イベントの表示	50-73	
ユーザ アクティビティ テーブルについて	50-73	
ユーザ アクティビティの検索	50-74	
CHAPTER 51		
関連ポリシーおよび関連ルールの設定	51-1	
関連ポリシーのルールの作成	51-3	
ルールの基本情報の指定	51-5	
関連ルール トリガー条件の指定	51-6	

ホスト プロファイル限定の追加	51-24	
経時的な接続データを使用した関連ルールの制約		51-28
ユーザ限定の追加	51-38	
スヌーズ期間および非アクティブ期間の追加		51-40
ルールの作成メカニズムについて	51-41	
関連ポリシーのルールの管理	51-49	
ルールの変更	51-49	
ルールの削除	51-50	
ルール グループの作成	51-50	
関連応答のグループ化	51-51	
応答グループの作成	51-51	
応答グループの変更	51-52	
応答グループの削除	51-53	
応答グループのアクティブ化と非アクティブ化		51-53
関連ポリシーの作成	51-53	
ルールとホワイト リストを関連ポリシーに追加する		51-55
ルールおよびホワイト リストのプライオリティの設定		51-56
ルールとホワイト リストに応答を追加する	51-57	
関連ポリシーの管理	51-58	
関連ポリシーのアクティブ化と非アクティブ化		51-59
関連ポリシーの編集	51-60	
関連ポリシーの削除	51-60	
関連イベントの操作	51-60	
関連イベントの表示	51-61	
関連イベント テーブルについて		51-63
関連イベントの検索	51-64	
CHAPTER 52	FireSIGHT システムのコンプライアンス ツールとしての使用	52-1
コンプライアンス ホワイト リストについて	52-2	
ホワイト リスト ターゲットについて	52-3	
ホワイト リスト ホスト プロファイルについて		52-4
ホワイト リストの評価について	52-6	
ホワイト リスト違反について	52-7	
コンプライアンス ホワイト リストの作成	52-8	
ネットワークの調査	52-10	
基本的なホワイト リスト情報の提供	52-11	
コンプライアンス ホワイト リスト ターゲットの設定		52-12
コンプライアンス ホワイト リスト ホスト プロファイルの設定		52-15
コンプライアンス ホワイト リストの管理	52-26	

コンプライアンス ホワイト リストの変更	52-27
コンプライアンス ホワイト リストの削除	52-27
共有ホスト プロファイルの操作	52-28
共有ホスト プロファイルの作成	52-28
共有ホスト プロファイルの変更	52-30
共有ホスト プロファイルの削除	52-32
組み込みホスト プロファイルの工場出荷時の初期状態へのリセット	52-33
ホワイト リスト イベントの操作	52-34
ホワイト リスト イベントの表示	52-34
ホワイト リスト イベント テーブルについて	52-36
コンプライアンス ホワイト リスト イベントの検索	52-37
ホワイト リスト 違反の処理	52-39
ホワイト リスト 違反の表示	52-39
ホワイト リスト 違反 テーブルについて	52-41
ホワイト リスト 違反の検索	52-42

CHAPTER 53

トラフィック プロファイルの作成	53-1
基本的なプロファイル情報の指定	53-3
トラフィック プロファイル条件の指定	53-3
トラフィック プロファイル条件の構文	53-4
ホスト プロファイル限定の追加	53-5
ホスト プロファイル限定の構文	53-6
プロファイル オプションの設定	53-9
トラフィック プロファイルの保存	53-10
トラフィック プロファイルのアクティブ化と非アクティブ化	53-10
トラフィック プロファイルの編集	53-11
条件の作成手順について	53-11
単一の条件の作成	53-12
条件の追加と結合	53-14
複数の値を条件で使用する	53-17
トラフィック プロファイルの表示	53-17

CHAPTER 54

修復の設定	54-1
修復の作成	54-1
Cisco IOS ルータ用修復の設定	54-3
Cisco PIX ファイアウォール用修復の設定	54-8
Nmap 修復の設定	54-12
セット属性修復の構成	54-17

修復ステータス イベントの使用	54-18
修復ステータス イベントの表示	54-19
修復ステータス イベントの使用	54-21
修復ステータス テーブルについて	54-21
修復ステータス イベントの検索	54-23

CHAPTER 55

ダッシュボードの使用 55-1

ダッシュボード ウィジェットについて	55-4
ウィジェットの可用性について	55-5
ウィジェットのプリファレンスについて	55-8
事前定義されたウィジェットについて	55-8
[アプライアンス情報 (Appliance Information)] ウィジェットについて	55-9
Appliance Status ウィジェットについて	55-10
Correlation Events ウィジェットについて	55-11
[現在のインターフェイス ステータス (Current Interface Status)] ウィジェットについて	55-12
Current Sessions ウィジェットについて	55-13
Custom Analysis ウィジェットについて	55-13
Disk Usage ウィジェットについて	55-31
インターフェイス トラフィック ウィジェットについて	55-32
Intrusion Events ウィジェットについて	55-33
Network Compliance ウィジェットについて	55-35
[製品ライセンス (Product Licensing)] ウィジェットについて	55-37
[製品アップデート (Product Updates)] ウィジェットについて	55-38
RSS Feed ウィジェットについて	55-39
[システム負荷 (System Load)] ウィジェットについて	55-40
[システム時刻 (System Time)] ウィジェットについて	55-40
White List Events ウィジェットについて	55-41
ダッシュボードの操作	55-42
カスタム ダッシュボードの作成	55-42
ダッシュボードの表示	55-44
ダッシュボードの変更	55-46
ダッシュボードの削除	55-50

CHAPTER 56

Context Explorer の使用 56-1

Context Explorer について	56-2
[トラフィックと侵入イベント カウント タイム (Traffic and Intrusion Event Counts Time)] グラフについて	56-3
[侵入の痕跡 (Indications of Compromise)] セクションについて	56-4
[ネットワーク情報 (Network Information)] セクションについて	56-6

[アプリケーション情報 (Application Information)] セクションについて	56-12
[セキュリティ インテリジェンス (Security Intelligence)] セクションについて	56-17
[侵入情報 (Intrusion Information)] セクションについて	56-20
[ファイル情報 (Files Information)] セクションについて	56-26
[地理位置情報 (Geolocation Information)] セクションについて	56-32
[URL 情報 (URL Information)] セクションについて	56-36
Context Explorer の更新	56-39
Context Explorer の時間範囲の設定	56-40
Context Explorer のセクションの最小化および最大化	56-40
Context Explorer データのドリルダウン	56-41
Context Explorer でのフィルタの操作	56-43
フィルタの追加および適用	56-43
コンテキスト メニューを使用したフィルタの作成	56-47
フィルタのブックマーク	56-48

CHAPTER 57

レポートの操作 57-1

レポート テンプレートについて	57-2
レポート テンプレートの作成と編集	57-4
新しいレポート テンプレートの作成	57-4
既存のテンプレートからのレポート テンプレートの作成	57-6
イベント ビューからのレポート テンプレートの作成	57-10
ダッシュボードまたはワークフローのインポートによるレポート テンプレートの作成	57-11
レポート テンプレートのセクションの編集	57-13
レポート テンプレート セクションの検索設定の操作	57-19
入力パラメータの使用法	57-20
レポート テンプレート内のドキュメント属性の編集	57-25
表紙のカスタマイズ	57-26
ロゴの管理	57-26
レポートの生成と表示	57-29
レポート生成オプションの使用法	57-31
スケジューラを使用したレポートの生成	57-32
レポートの生成時の電子メール配布	57-32
レポート用のリモートストレージの使用法	57-33
レポート テンプレートとレポート ファイルの管理	57-34
レポート テンプレートのエクスポートとインポート	57-34
レポート テンプレートの削除	57-36
レポートのダウンロード	57-36

レポートの削除 57-37

CHAPTER 58

ワークフローの概要と使用	58-1
ワークフローのコンポーネント	58-2
事前定義ワークフローとカスタム ワークフローの比較	58-3
事前定義テーブルとカスタム テーブルのワークフローの比較	58-4
事前定義の侵入イベント ワークフロー	58-4
事前定義のマルウェア ワークフロー	58-7
事前定義のファイル ワークフロー	58-7
事前定義されたキャプチャ ファイル ワークフロー	58-8
事前定義の接続データ ワークフロー	58-8
事前定義のセキュリティ インテリジェンス ワークフロー	58-10
事前定義のホスト ワークフロー	58-10
事前定義の侵入の痕跡ワークフロー	58-11
事前定義のアプリケーション ワークフロー	58-11
事前定義のアプリケーション詳細ワークフロー	58-12
事前定義のサーバ ワークフロー	58-13
事前定義のホスト属性ワークフロー	58-13
事前定義のディスカバリ イベント ワークフロー	58-14
事前定義のユーザ ワークフロー	58-14
事前定義の脆弱性ワークフロー	58-14
事前定義のサードパーティの脆弱性ワークフロー	58-15
事前定義の関連およびホワイトリスト ワークフロー	58-15
事前定義のシステム ワークフロー	58-16
保存済みのカスタム ワークフロー	58-16
ワークフローの使用	58-18
ワークフローの選択	58-19
ワークフローのツールバーについて	58-21
ワークフローのページの使用	58-21
イベント時間の制約の設定	58-27
イベントの制約	58-35
複合的な制約の使用	58-38
テーブル ビュー ページのソートおよびレイアウトの変更	58-38
ドリルダウン ワークフロー ページのソート	58-39
ワークフロー ページの行の選択	58-40
ワークフロー内の他のページへのナビゲート	58-40
ワークフロー間のナビゲート	58-41
ブックマークの使用	58-42
カスタムワークフローの使用	58-44

カスタム ワークフローの作成	58-44	
カスタム接続データ ワークフローの作成		58-46
カスタム ワークフローの表示	58-48	
カスタム ワークフローの編集	58-49	
カスタム ワークフローの削除	58-50	

CHAPTER 59

カスタム テーブルの使用	59-1	
カスタム テーブルについて	59-1	
可能なテーブルの結合について	59-2	
カスタム テーブルの作成	59-6	
カスタム テーブルの変更	59-9	
カスタム テーブルの削除	59-9	
カスタム テーブルに基づいたワークフローの表示		59-10
カスタム テーブルの検索	59-10	

CHAPTER 60

イベントの検索	60-1	
検索設定の実行と保存	60-1	
検索の実行	60-2	
保存済み検索設定のロード	60-4	
保存済み検索設定の削除	60-4	
検索でのワイルドカードと記号の使用	60-5	
検索でのオブジェクトとアプリケーションフィルタの使用		60-5
検索での時間制約の指定	60-6	
検索での IP アドレスの指定	60-6	
検索でのデバイスの指定	60-7	
検索でのポートの指定	60-8	
実行時間が長いクエリの停止	60-8	

CHAPTER 61

ユーザの管理	61-1	
シスコユーザ認証について	61-1	
内部認証について	61-3	
外部認証について	61-3	
ユーザ特権について	61-4	
認証オブジェクトの管理	61-5	
LDAP 認証	61-6	
RADIUS 認証	61-34	
認証オブジェクトの削除	61-45	
ユーザ アカウントの管理	61-46	

ユーザ アカウントの表示	61-46
新しいユーザ アカウントの追加	61-47
コマンドライン アクセスの管理	61-49
外部認証ユーザ アカウントの管理	61-50
ユーザ ログイン設定の管理	61-51
ユーザ ロールの設定	61-53
カスタム ユーザ ロールの管理	61-56
ユーザ特権とオプションの変更	61-59
制限付きユーザ アクセス プロパティについて	61-59
ユーザ パスワードの変更	61-60
ユーザ アカウントの削除	61-60
ユーザ アカウント特権について	61-61
ユーザ ロール エスカレーションの管理	61-71
エスカレーション ターゲット ロールの設定	61-72
エスカレーションに使用するカスタム ユーザ ロールの設定	61-72
ユーザ ロールのエスカレーション	61-74
シスコ Security Manager からのシングル サインオンの設定	61-74

CHAPTER 62

タスクのスケジュール	62-1
定期タスクの設定	62-2
バックアップ ジョブの自動化	62-3
証明書失効リストのダウンロードの自動化	62-4
Nmap スキャンの自動化	62-5
Nmap スキャン用にシステムを準備する	62-6
Nmap スキャンのスケジュール	62-6
侵入ポリシーの適用の自動化	62-7
レポートの生成を自動化する方法	62-9
位置情報データベースの更新の自動化	62-10
FireSIGHT 推奨の自動化	62-11
ソフトウェア更新の自動化	62-12
ソフトウェア ダウンロードの自動化	62-13
ソフトウェア プッシュの自動化	62-14
ソフトウェア インストールの自動化	62-15
脆弱性データベースの更新の自動化	62-17
VDB 更新のダウンロードの自動化	62-18
VDB 更新のインストールの自動化	62-19
URL フィルタリング更新の自動化	62-20
タスクの表示	62-21

カレンダーの使用法	62-21
タスク リストの使用法	62-22
スケジュール済みタスクの編集	62-23
スケジュール済みタスクの削除	62-23
定期タスクの削除	62-24
ワнтаイム タスクの削除	62-24

CHAPTER 63

システム ポリシーの管理	63-1
システム ポリシーの作成	63-2
システム ポリシーの編集	63-3
システム ポリシーの適用	63-4
システム ポリシーの比較	63-5
システム ポリシーの削除	63-7
システム ポリシーの設定	63-8
アクセス コントロール ポリシー設定の構成	63-8
アプライアンスのアクセス リストの設定	63-9
監査ログの設定	63-11
外部認証の有効化	63-13
ダッシュボードの設定	63-15
データベース イベント制限の設定	63-16
DNS キャッシュ プロパティの設定	63-19
メール リレー ホストおよび通知アドレスの設定	63-20
ネットワーク解析ポリシーの設定の構成	63-21
侵入ポリシー設定の構成	63-22
別の言語の指定	63-23
カスタム ログイン バナーの追加	63-24
SNMP ポーリングの設定	63-25
STIG コンプライアンスの有効化	63-27
時間の同期	63-28
ユーザ インターフェイスの設定	63-31
サーバの脆弱性のマッピング	63-33

CHAPTER 64

アプライアンス設定の構成	64-1
アプライアンス情報の表示と変更	64-2
カスタム HTTPS 証明書の使用	64-3
現在の HTTPS サーバ証明書の表示	64-4
サーバ証明書要求の生成	64-5
サーバ証明書のアップロード	64-6
ユーザ証明書の要求	64-6

データベースへのアクセスの有効化	64-8
管理インターフェースの構成	64-9
管理インターフェースのオプションについて	64-10
管理インターフェースの編集	64-13
システムのシャットダウンと再起動	64-14
手動による時刻の設定	64-16
リモートストレージの管理	64-17
ローカルストレージの使用	64-18
リモートストレージでの NFS の使用	64-18
リモートストレージでの SSH の使用	64-19
リモートストレージでの SMB の使用	64-20
変更調整について	64-22
リモートコンソールアクセスの管理	64-23
アプライアンス上のリモートコンソール設定の構成	64-24
Lights-Out 管理ユーザアクセスの有効化	64-25
Serial over LAN 接続の使用	64-27
Lights-Out 管理の使用	64-28
クラウド通信の有効化	64-30
VMware ツールの有効化	64-34

CHAPTER 65

FireSIGHT システムのライセンス	65-1
ライセンスについて	65-1
ライセンスのタイプと制約事項	65-2
サービスサブスクリプション	65-8
ハイアベイラビリティペアのライセンス	65-9
スタック構成デバイスおよびクラスタ構成デバイスのライセンス	65-9
シリーズ 2 アプライアンスのライセンス付与	65-9
FireSIGHT ホストおよびユーザライセンスの制限について	65-10
ライセンスの表示	65-12
Defense Center へのライセンスの追加	65-13
ライセンスの削除	65-14
デバイスのライセンス付き機能の変更	65-15

CHAPTER 66

システムソフトウェアの更新	66-1
更新のタイプについて	66-1
ソフトウェア更新の実行	66-2
更新の計画	66-3
更新プロセスについて	66-4

防御センターの更新	66-7
管理対象デバイスの更新	66-9
メジャーな更新のステータスのモニタリング	66-11
ソフトウェアアップデートのアンインストール	66-12
脆弱性データベースの更新	66-14
ルールの更新とローカルルールファイルのインポート	66-16
ワнтаイムルール更新の使用	66-18
再帰的なルール更新の使用	66-21
ローカルルールファイルのインポート	66-22
ルール更新ログの表示	66-24
位置情報データベースの更新	66-32

CHAPTER 67

システムのモニタリング	67-1
ホスト統計情報の表示	67-2
システムステータスとディスク領域使用率のモニタ	67-4
システムプロセスステータスの表示	67-5
実行中のプロセスについて	67-7
システムデーモンについて	67-7
実行可能ファイルおよびシステムユーティリティについて	67-8

CHAPTER 68

ヘルスモニタリングの使用	68-1
ヘルスモニタリングについて	68-2
正常性ポリシーについて	68-3
ヘルスマジュールについて	68-3
ヘルスモニタリング設定について	68-6
正常性ポリシーの設定	68-7
デフォルト正常性ポリシーについて	68-8
正常性ポリシーの作成	68-9
正常性ポリシーの適用	68-34
正常性ポリシーの編集	68-35
正常性ポリシーの比較	68-37
正常性ポリシーの削除	68-40
ヘルスマニタブラックリストの使用	68-40
正常性ポリシーまたはアプライアンスのブラックリストへの登録	68-41
個別のアプライアンスのブラックリストへの登録	68-42
個別の正常性ポリシーモジュールのブラックリストへの登録	68-43
ヘルスマニタアラートの設定	68-43
ヘルスマニタアラートの作成	68-44

ヘルス モニタ アラートの解釈	68-45
ヘルス モニタ アラートの編集	68-45
ヘルス モニタ アラートの削除	68-46
ヘルス モニタの使用	68-46
ヘルス モニタ ステータスの解釈	68-47
アプライアンス ヘルス モニタの使用	68-48
ステータス別のアラートの表示	68-49
アプライアンスのすべてのモジュールの実行	68-49
特定のヘルス モジュールの実行	68-50
ヘルス モジュール アラート グラフの生成	68-51
ヘルス モニタを使用したトラブルシューティング	68-52
ヘルス イベントの操作	68-54
ヘルス イベント ビューについて	68-55
ヘルス イベントの表示	68-55
ヘルス イベント テーブルについて	68-61
ヘルス イベントの検索	68-62

CHAPTER 69

システムの監査

69-1

監査レコードの管理	69-1
監査レコードの表示	69-2
監査レコードの抑制	69-5
監査ログ テーブルについて	69-8
監査ログを使って変更を調査する	69-9
監査レコードの検索	69-9
システム ログの表示	69-11
システム ログ メッセージのフィルタリング	69-12

CHAPTER 70

バックアップと復元の使用

70-1

バックアップ ファイルの作成	70-2
バックアップ プロファイルの作成	70-7
ローカル ホストからのバックアップのアップロード	70-8
バックアップ ファイルからのアプライアンスの復元	70-8

CHAPTER 71

ユーザ設定の指定

71-1

パスワードの変更	71-1
期限切れのパスワードの変更	71-2
ホームページの指定	71-2
イベント ビュー設定の設定	71-3

	イベント設定	71-4
	ファイル設定	71-5
	デフォルトの時間枠	71-6
	デフォルトのワークフロー	71-8
	デフォルトのタイムゾーン設定	71-8
	デフォルトのダッシュボードの指定	71-9
APPENDIX A	設定のインポートおよびエクスポート	A-1
	設定のエクスポート	A-1
	設定のインポート	A-5
APPENDIX B	データベースからの検出データの消去	B-1
APPENDIX C	実行時間が長いタスクのステータスの表示	C-1
	タスク キューの表示	C-1
	タスク キューの管理	C-2
APPENDIX D	コマンドライン リファレンス	D-1
	基本的な CLI コマンド	D-2
	configure password	D-2
	end	D-3
	exit	D-3
	help	D-3
	history	D-4
	logout	D-4
	? (疑問符)	D-4
	?? (二重の疑問符)	D-5
	Show コマンド	D-5
	access-control-config	D-7
	alarms	D-7
	arp-tables	D-7
	audit-log	D-8
	bypass	D-8
	clustering	D-8
	cpu	D-9
	database	D-10
	device-settings	D-11
	disk	D-11
	disk-manager	D-12

dns	D-12
expert	D-12
fan-status	D-12
fastpath-rules	D-13
gui	D-13
hostname	D-13
hosts	D-14
hyperthreading	D-14
iab	D-14
inline-sets	D-15
interfaces	D-15
ifconfig	D-15
lcd	D-16
link-aggregation	D-16
link-state	D-17
log-ips-connection	D-17
managers	D-17
memory	D-18
model	D-18
mpls-depth	D-18
NAT	D-18
netstat	D-20
network	D-21
network-modules	D-21
network-static-routes	D-21
ntp	D-22
perfstats	D-22
portstats	D-22
power-supply-status	D-23
process-tree	D-23
processes	D-23
route	D-24
routing-table	D-24
serial-number	D-24
ssl-policy-config	D-25
stacking	D-25
summary	D-25
time	D-26
traffic-statistics	D-26
user	D-26

users	D-27	
version	D-28	
virtual-routers	D-28	
virtual-switches	D-28	
vmware-tools	D-29	
VPN	D-29	
コンフィギュレーション コマンド		D-31
clustering	D-31	
bypass	D-31	
gui	D-32	
iab	D-32	
lcd	D-34	
log-ips-connections	D-35	
manager	D-35	
mpls-depth	D-36	
network	D-36	
password	D-43	
stacking disable	D-43	
user	D-43	
vmware-tools	D-46	
system コマンド		D-47
access-control	D-47	
disable-http-user-cert	D-48	
file	D-49	
generate-troubleshoot	D-50	
ldapsearch	D-50	
lockdown-sensor	D-51	
nat rollback	D-51	
reboot	D-51	
restart	D-52	
shutdown	D-52	
<hr/>		
APPENDIX E	セキュリティ、インターネット アクセス、および通信ポート	E-1
	インターネット アクセス要件	E-2
	通信ポートの要件	E-3
<hr/>		
APPENDIX F	サードパーティ製品	F-1
<hr/>		
GLOSSARY		

