このマニュアルについて

ここでは、このガイドを使用する方法について説明します。

各リリースでの変更点

セキュリティイベントの Syslog メッセージ

次のイベントタイプの syslog メッセージに対する変更については、「セキュリティイベントの Syslog メッセージの履歴」を参照してください。

- 侵入イベント
- 接続イベント
- セキュリティ インテリジェンス イベント
- ファイル イベント
- マルウェア イベント

その他のすべての Syslog メッセージ

この項では、次の Secure Firewall Threat Defense リリースで追加、変更、および廃止された syslog メッセージを示します。Syslog メッセージの詳細な説明については、それぞれ対応する章を参照してください。

- 表 1 : バージョン 7.2 で追加、変更、および廃止された Syslog メッセージ
- 表 2 : バージョン 7.1 で追加、変更、および廃止された Syslog メッセージ
- 表 3 : バージョン 7.0 で追加、変更、および廃止された Syslog メッセージ

表 *1* : バージョン *7.2* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	新しい syslog メッセージは追加されませんでした。
変更された Syslog メッセージ（ドキュメント）	なし
変更された syslog メッセージ（コード）	なし
廃止された Syslog メッセージ	なし

表 *2* : バージョン *7.1* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	709009、709010、709011、709012、709013
変更された Syslog メッセージ（ドキュメント）	なし
変更された syslog メッセージ（コード）	なし
廃止された Syslog メッセージ	なし

表 *3* : バージョン *7.0* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	なし
変更された syslog メッセージ（ドキュメント）	717009
変更された syslog メッセージ（コード）	なし
廃止された Syslog メッセージ	なし

表 *4* : バージョン *6.7* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	106029
変更された syslog メッセージ（ドキュメント）	105042、105003、105004、105043、305006、414004
変更された syslog メッセージ（コード）	302013、302014
廃止された Syslog メッセージ	なし

表 *5 :* バージョン *6.6* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	209006

表 *6 :* バージョン *6.5* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	748011、748012、302311、747042、747043、747044、769007、769009、852001、852002
変更された Syslog メッセージ	302014
廃止された Syslog メッセージ	

表 *7 :* バージョン *6.4* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	セキュリティイベント：430004、430005 その他：305017、308003、308004、408101、408102、409014、409015、409016、409017、419004、419005、419006、503002、503003、503004、503005、737038、737200-737206,737400-737407、747042、747043、747044、768003、768004
変更された Syslog メッセージ	737001 ～ 737019、737031 ～ 737036
廃止された Syslog メッセージ	

すべての Syslog メッセージ

表 *8 :* バージョン *6.3* の *Syslog* メッセージの変更

タイムスタンプロギング	バージョン 6.3 以降、Secure Firewall Threat Defense は、イベントの syslog で RFC 5424 に従ってタイムスタンプを有効にするオプションを提供します。このオプションを有効にすると、Syslog メッセージのすべてのタイムスタンプには、RFC 5424 形式に従って時刻が表示されます。次に、RFC 5424 形式の出力例を示します。 `<166>2018-06-27T12:17:46Z firepower : %FTD-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port` （注） 上記の例では、PRI 値 <166> は、ファシリティとアラートの重大度の両方を表すプライオリティ値です。RFC5424 形式の Syslog メッセージには、通常 PRI が表示されます。ただし、Management Center が管理する Threat Defense の場合、Management Center プラットフォーム設定を使用して EMBLEM 形式でのロギングを有効にした場合にのみ、PRI 値が syslog メッセージに表示されます。EMBLEM 形式を有効にする方法については、「Cisco Secure Firewall Management Center アドミニストレーション ガイド」を参照してください。PRI の詳細については、「RFC5424」を参照してください。
Syslog のプレフィックスの形式	Threat Defense オペレーティングシステムは、syslog ユーティリティを含む ASA オペレーティングシステムの一部を使用していました。したがって、この共有ユーティリティのため、Threat Defense の syslog メッセージはすべて「%ASA」から始まっていました。リリース 6.3 以降、Threat Defense の syslog メッセージは「%FTD」から始まります。

Secure Firewall Threat Defense Syslog メッセージについて

（注） このトピックの情報は、セキュリティイベントに関連するメッセージには適用されません。

次の表に、メッセージのクラスおよび各クラスに関連付けられているメッセージ ID の範囲を示します。メッセージ ID の有効な範囲は 100000 ～ 999999 です。

（注） 番号が連番から抜けている場合、そのメッセージは Threat Defense デバイスコードにはありません。

ほとんどの ISAKMP メッセージには、トンネルの識別に役立つ追加オブジェクトの共通セットがあります。これらのオブジェクトは、使用可能なときに、メッセージの説明テキストの前に付加されます。メッセージの生成時にオブジェクトが未知の場合、特定の **heading = value** の対は表示されません。

これらのオブジェクトは次の形式で追加されます。

Group = **groupname**, Username = **user**, IP = **IP_address**,...

ここで、Group はトンネル グループを特定し、username はローカル データベースまたは AAA サーバーのユーザー名、IP アドレスはリモート アクセス クライアントまたは L2L ピアのパブリック IP アドレスです。

通常、Syslog メッセージのトラフィック セッションに各フローの接続番号/ID が表示されます。ただし、一部の接続については、接続 ID は増加しますが、Syslog メッセージには ID が表示されません。そのため、後続のメッセージの接続 ID でシーケンス番号の欠落が見られる場合があります。たとえば、TCP トラフィック フローで、Syslog メッセージに各フローの接続 ID が 201、202、203、204 と表示されたとします。ICMP フローが開始されると、接続 ID は内部的に 205 および 206 に増えますが、Syslog メッセージには番号が表示されません。別の TCP フローが続くと、その接続番号は 207、208 などと表示され、シーケンスをスキップしているように見えます。

表 *9 : syslog* メッセージのクラスおよび関連付けられているメッセージ *ID* 番号

ロギング クラス	定義	Syslog メッセージ ID 番号
auth	User Authentication	109、113
—	アクセス リスト	106
—	アプリケーション ファイアウォール	415
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 認証局	717
citrix	Citrix Client	723
—	クラスタ	747
—	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロールの EAP または EAPoUDP	333、334

ロギング クラス	定義	Syslog メッセージ ID 番号
eigrp	EIGRP ルーティング	336
email	電子メール プロキシ	719
—	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709、727
—	Identity-Based ファイアウォール	746
ids	侵入検知システム	400、733
—	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレス割り当て	735
ips	侵入防御システム	400、401、420
—	IPv6	325
—	ブロックリスト、許可リスト、およびグレーリスト	338
—	ライセンス	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
nacpolicy	NAC ポリシー	731
nacsettings	NAC ポリシーを適用する NAC 設定	732
—	ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
—	NP SSL	725
ospf	OSPF ルーティング	318、409、503、613
—	パスワードの暗号化	742
—	電話プロキシ	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321

ロギング クラス	定義	Syslog メッセージ ID 番号
—	セキュリティ イベント （このトピックの情報は、これらのイベントには適用されません）	430
—	Smart Call Home	120
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL スタック	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
—	脅威の検出	733
tre	トランザクション ルール エンジン	780
—	UC-IME	339
tag-switching	サービス タグ スイッチング	779
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
—	VXLAN	778
webfo	WebVPN フェールオーバー	721

ロギング クラス	定義	Syslog メッセージ ID 番号
webvpn	WebVPN と AnyConnect Client	716
—	NAT および PAT	305

Syslog メッセージを送信するためのシステムの設定

トリガーするイベントが発生するとすぐに、syslog が生成されます。Threat Defense が syslog メッセージを送信できる最大レートは、syslog のレベルと使用可能な CPU リソースによって異なります。Management Center に保存できるイベントの数はモデルによって異なります。システムパフォーマンスを向上させるために、イベント生成制限、しきい値制限を構成でき、一部のイベントタイプのストレージを無効にすることもできます。外部の syslog、SNMP トラップサーバー、またはその他の外部ツールにイベントを記録することもできます。これらのシステムロギング設定の詳細については、ご使用のリリースの『Cisco Secure Firewall Management Center デバイス構成ガイド』または『Cisco Secure Firewall Device Manager Configuration Guide』を参照してください。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。