



Stealthwatch System v6.9.0 内部アラーム ID

著作権および商標

© 2017 Cisco Systems, Inc. All rights reserved.

NOTICE

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハードコピーおよびソフトコピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト (www.cisco.com/go/offices) をご覧ください。

Stealthwatch System V6.9.0 内部アラーム ID

(注) 以前に使用されていたいくつかのアラームは使用されなくなり、このファイルにリストされなくなりました。

1	ホスト ロック違反
5	SYN フラッド
6	UDP フラッド
7	ICMP フラッド
8	パケット フラッド
9	大容量のメール
10	メールリレー
11	スパム送信元
12	メール拒否
13	アクティブなポートを表示
14	新規ホストがアクティブ状態
15	上位のターゲット インデックス
16	上位の合計 インデックス
17	最大フローを開始
18	新規フローを開始
19	SYN 受信済み
20	上位のファイル共有 インデックス
24	疑わしいUDP アクティビティ
25	MAC アドレス違反
26	ハーフオープン攻撃
28	アクセス
29	低トラフィック
30	高トラフィック
31	ホストのアクティブを確認
32	懸念事項 インデックス
33	疑わしい長いフロー
34	トラップされたホスト
35	ワーム アクティビティ

36	ワーム伝播
37	最大フローの提供
38	新規フローの提供
39	ホストに対してビーコンを実行
40	データ損失
41	ボット感染ホスト : C&C 活動の試行 (部分一致)
42	ボット感染ホスト : C&C 活動の成功 (完全一致)
43	ボット コマンド & コントロール サーバ (制御される)
44	低速接続フラッド
45	データ漏洩
46	コマンド & コントロール
47	ポリシー違反
48	疑わしい静かな長いフロー
49	受信された UDP
50	受信された ICMP
51	偵察
52	データホーディング
53	高 DDoS 攻撃ターゲット インデックス
54	高 DDoS ソース インデックス
55	ポート スキャン
56	エクスプロイト
57	異常
58	ブルート フォース ログイン
59	ファントムとの通信
60	過大な SMB ピア
61	SSH リバース シェル
62	疑わしいアプリケーションの検出
63	スキャナ通信
257	Ping
258	ICMP タイムアウト
259	タイムアウト UDP
260	タイムアウト TCP

261	リセット UDP
262	リセット TCP
263	不正なフラグすべて
264	不正なフラグ SYN FYN
265	不正な予約済みのフラグ(Sflowのみ)
266	不正なフラグ RST
267	不正なフラグ ACK
268	不正なフラグ URG
269	不正なフラグ フラグなし
271	ステルス スキャン UDP
272	ステルス スキャン TCP
273	SRC=DES
276	Addr スキャン TCP
277	Ping スキャン
278	特大サイズの Ping パケット
281	フラグ Pkt が短すぎる
282	フラグ Pkt が長すぎる
283	フラグのサイズが異なる
286	Addr スキャン UDP
289	ICMP ネット到達不能
290	ICMP ホスト到達不能
291	ICMP プロトコル到達不能
292	ICMP ポート到達不能
293	ICMP フラグが必要
294	ICMP SRC ルート失敗
295	ICMP 宛先ネットワーク不明
296	ICMP 宛先ホスト不明
297	ICMP 送信元ホスト孤立
298	ICMP 宛先ネット管理者
299	ICMP 宛先ホスト管理者
300	ICMP ネット到達不能 TOS
301	ICMP ホスト到達不能 TOS

302	ICMP 通信管理者
303	ICMP ホスト優先順位
304	ICMP 優先順位の遮断
310	フロー拒否
315	疑わしいデータホーディング
316	ターゲット データホーディング
317	TOR からの接続試行
318	TOR からの接続成功
319	内部 TOR 終了の検出
513	TOR への接続試行
514	TOR への接続成功
515	内部 TOR エントリの検出
516	Bogon アドレスへの接続成功
517	Bogon アドレスからの接続成功
518	Bogon アドレスへの接続試行
519	Bogon アドレスからの接続試行
4010	フローコレクタのフローデータ損失
4020	インターフェイス使用率がインバウンドを超過
4030	インターフェイス使用率がアウトバウンドを超過
5010	FlowSensor VE 設定エラー
5011	FlowSensor トラフィック損失
5012	FlowSensor RAID 障害
5013	FlowSensor RAID の再構築
5998	FlowSensor 時間のミスマッチ
5999	FlowSensor の管理チャンネルダウン
6010	新規 VM
6020	V-Motion
7001	リレーションシップ高トラフィック合計
7002	リレーションシップ高トラフィック
7003	リレーションシップ低トラフィック
7004	リレーションシップ最大フロー
7005	リレーションシップ新規フロー

7006	リレーションシップ ラウンドトリップ時間
7007	リレーションシップ サーバ応答時間
7008	リレーションシップ TCP 再送率
7009	リレーションシップ SYN フラッド
7010	リレーションシップ UDP フラッド
7011	リレーションシップ ICMP フラッド
9021	フローコレクタのデータ削除
9022	フローコレクタのデータベース使用不可
9023	フローコレクタのデータベースのチャンネルダウン
9040	フローコレクタ ログの保存期間削減
9050	フローコレクタ エクスポート カウントの超過
9051	フローコレクタ FlowSensor VE カウントの超過
9052	フローコレクタ フロー率の超過
9053	フローコレクタ インターフェイス カウントの超過
9100	フローコレクタ RAID 障害
9102	フローコレクタ RAID の再構築
9998	フローコレクタ パフォーマンスの低下
9999	フローコレクタ停止
60000	フローコレクタ タイム mismatches
60001	Cisco ISE 管理チャンネルダウン
60002	フローコレクタ 管理チャンネルダウン
60003	SMC RAID 障害
60005	SMC RAID の再構築
60007	SMC ディスク容量低下
60008	SMC プライマリの重複
60012	Stealthwatch フローライセンスの超過
60013	ライセンスの破損
60014	ライセンスされていない機能
60015	SLIC チャンネルダウン
600016	ID チャンネルダウン
600017	SMC フェールオーバー チャンネルダウン
600018	ID コンセントレータ チャンネルダウン

