改ざん検出

改ざん検出は、潜在的な改ざんイベントを特定するために Cisco 8000 シリーズ セキュアルータに実装されたセキュリティ機能です。各ルータは、シャーシカバーが安全に取り付けられた状態で製造元から出荷されます。出荷後にシャーシカバーが開かれた場合、ハードウェアは、デバイスの電源がオンになっているかオフになっているかに関係なく、すべてのシャーシカバーが開閉されたイベントを改ざん防止メモリに記録します。

起動時に、ソフトウェアは最新のイベントインデックスを読み取り、以前の既知のインデックスと比較します。不一致がある場合、ソフトウェアは起動時にSyslogメッセージを生成して、改ざんイベントを報告します。デバイスの電源が完全にオンになると、ソフトウェアはSyslogメッセージと SNMP トラップをただちに生成します。

利点

改ざん検出通知は、不正な物理アクセスやデバイスを侵害する試みを検出して、機密データとネットワークの完全性を保護します。

制限事項

改ざん検出機能は現在、SDWAN/SD ルーティングモードではサポートされていません。

改ざん検出の設定

改ざん検出はルータでデフォルトで有効になっています。シャーシカバーの開くまたは閉じるイベントが自動的に記録されます。

改ざんイベント通知は、config モードで以下のコマンドを使用して有効または無効にできます。

- 設定モードで次のコマンドを使用して、改ざん検出通知を有効にします（デフォルトで有効）。

```
Router(config)#platform tamper detection
```

- config モードで次のコマンドを使用して、改ざん検出通知を無効化します。

```
Router(config)#no platform tamper detection
```

改ざん検出イベントのマーク

改ざんイベントのマーキングは、

- 承認されたユーザーに対して特定のアクティビティが改ざんイベントとして表示されないようにし、
- システムが許可されたアクセスと不正なアクセスを区別できるようにすることで
- 改ざんイベントログの精度を維持する機能です。

改ざん検出イベントの設定

承認されたアクティビティがログで改ざんイベントとして表示されないようにする方法です。次の手順を実行します。

手順

ステップ 1 次のコマンドを使用して、同意トークンを取得するためのチャレンジを生成します。

例：

```
request consent-token generate-challenge tamper-auth auth-timeout <mins>
```

この手順により、承認ユーザーによってのみ同意トークンが生成されるようにできます。

ステップ 2 チャレンジが検証され、同意トークンが生成されたら、次のコマンドを使用して同意トークンを受け入れます。

例：

```
request consent-token accept-response tamper-auth <consent token>
```

ステップ 3 次のコマンドを使用して、改ざん検出イベントをマークします

例：

```
request platform hardware tamper-detection event-mark
```

request platform hardware tamper-detection event-mark コマンドは、Cisco IOS XE 17.17.1a からサポートされています。

最後の既知のイベントインデックスとタイムスタンプがマークされ、承認されたアクティビティがログに改ざんイベントとして表示されないようにします。

改ざん検出イベントの確認

```
Router# show platform tamper-detection event [power-off | power-on] [all | lastx | new]
```

オプション	説明
電源オフ	**電源オフ** オプションは、ルータに電源ケーブルが接続されていない場合に改ざんイベントを指定します。
電源の投入	**電源オン** オプションは、ルータの電源がオンになったときの改ざんイベントを指定します。
all	[**all**]オプションでは、記録されたすべての改ざんイベントが指定されます。システムは最大 500 エントリを表示できます。 500 エントリごとにロールオーバーカウンタが 1 つ増加します。
lastx	**lastx** オプションでは、表示するイベントの数を指定します。たとえば、「lastx 10」と入力すると、直近の 10 件のイベントが表示されます。
new	**new** オプションでは、最後の既知のイベントインデックス以降の新しい改ざんイベントを指定します。

show コマンドでは、以下の詳細を含むイベントログが提供されます。

- 現在のイベントインデックス
- 現在の時刻
- ロールオーバーステータスとロールオーバー回数：
  - 改ざんイベント数が 500 以下の場合、ロールオーバー数は 0、ロールオーバーステータス：No
  - 500 ログごとに、ロールオーバー数は 1 ずつ増加します：
  - 501 ～ 1000 が 1 ～ 500 を上書きする場合、ロールオーバー数は 1、ロールオーバーステータス：Yes
  - 1001 ～ 1500が 501～ 1000 を上書きする場合、ロールオーバー数は 2、ロールオーバーステータス：Yes
- イベントタイプとタイムスタンプを示すイベント

システムの電源がオフになっているときのイベントの確認

システムの電源がオフになっている場合、ルータはバッテリ電源を使用して改ざんイベントを記録します。ルータは、最後の電源オフから次の電源オンまでの最初のシャーシカバーが開いたイベントを記録します。電源オフ中にシャーシカバーが何度も開いたり閉じたりした場合、最初の開いたイベントだけが記録されます。次に、システムの電源がオフになったときのイベントログを示します。

```
Router#show platform tamper-detection event power-off all
Current Time: 2025/04/25 19:55:03       Rollover Status: No     Rollover Count: 0
-------------------------------------------------------------------------------------------------
Tamper event index      |       Tamper event timestamp  |       Tamper events description
-------------------------------------------------------------------------------------------------

    #2                           2024/08/08 02:36:41             Chassis is opened
    #1                           2000/00/00 00:00:00             Battery not present or
used up
```

システムの電源が部分的にまたは完全にオンになっている場合のイベントの確認

システムの電源が使用できる場合、ルータはすべてのシャーシカバーの開閉イベントを記録します。次の例は、システムの電源が部分的にまたは完全にオンになっているときのイベントログを示しています。

```
Router show platform tamper-detection event power-on lastx 10
Current Time: 2025/04/25 19:54:46      Rollover Status: No     Rollover Count: 0
-------------------------------------------------------------------------------------------------
Tamper event index      |       Tamper event timestamp  |       Tamper events description
-------------------------------------------------------------------------------------------------

    #2                  025/04/24 22:10:14             Chassis is opened
    #1                   025/04/24 22:02:33             Chassis is closed
```

改ざん検出 SYSlog

ルータが起動すると、イベントログから現在のイベントインデックスが読み取られ、以前に保存されていた最後の既知のインデックスと比較されます。インデックス間に不一致がある場合、またはタイムスタンプが異なる場合、IOS は警告レベルの SYSlog メッセージを生成し、コントローラモードでコントローラに通知を送信します。

このセクションでは、SYSlog イベントの例を示します。

- 電源投入イベントの SYSlog

  改ざん検出が有効で、システムの電源がオンになっている場合、電源オンの SYSlog メッセージが起動中に表示されます。

  ```
  Apr 25 20:15:01.064: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
  was opened 0 times and closed 0 times during power up since last known event index
  7 at 2025/04/24 22:11:51
  ```

- 電源オフイベントの SYSlog

改ざん検出が有効になっていてシステムの電源がオフになっている場合、電源オフの SYSlog メッセージが起動中に表示されます。

```
Apr 25 20:15:01.064: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
was opened 0 times and closed 0 times during power down since last known event index
 5 at 2025/04/24 22:11:51
```

- ランタイムイベントの SYSlog

```
*Aug 29 06:56:34.560: %CMRP-4-INTRUSION_ALERT: R0/0: cmand: The system cover has
been opened !!
*Aug 29 06:56:36.130: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 2 times and closed 0 times during power down since last known event index
 50 at 2025/06/04 08:03:06
*Aug 29 06:56:36.130: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 20 times and closed 20 times during power up since last known event index
 1638 at 2025/06/05 07:08:12

*Aug 29 06:57:04.563: %CMRP-4-INTRUSION_ALERT: R0/0: cmand: The system cover has
been closed !!
*Aug 29 06:57:06.137: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 2 times and closed 0 times during power down since last known event index
 50 at 2025/06/04 08:03:06
*Aug 29 06:57:06.137: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 20 times and closed 21 times during power up since last known event index
 1638 at 2025/06/05 07:08:12
```

（注） 改ざん検出機能が無効になっている場合、SYSlog メッセージは起動時に表示されません。

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。

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。