# IPSブロック設定によるCisco Secure Accessの警告アクションの上書き動作

## 内容

## お問い合わせ内容

IPSを有効にしたCisco Secure Accessのアクセスポリシー（インターネットアクセス）でWarn動作をテストすると、IPSブロック設定を上書きするように見えるWarn動作がユーザに予期せぬ動作を引き起こします。具体的には、IPSシグニチャをトリガーするURL(SERVER-WEBAPP /etc/passwd file access attempt, GID-SID: 1-1122)にアクセスすると、警告ページが表示され、ユーザ確認後、IPSがトラフィックをブロックするように設定されているにもかかわらず、URLへのアクセスが許可されます。

設定には次のものが含まれます。

- 操作：分離
- 侵入防御(IPS)：有効
- IPS/ブロック
- シグニチャ：SERVER-WEBAPP /etc/passwdファイルへのアクセス試行
- GID-SID: 1-1122

アクティビティ検索ログに競合するエントリが表示されます。

- IPS:（IPS：ブロック）
- WEB:（WEB：許可 – 警告ページが表示されます）
- WEB:（WEB：許可 – 警告アクセス後）

## 環境

- 製品：Cisco Secure Internet Access Advantage
- テクノロジー：セキュアなアクセス
- インターネットアクセスおよび警告アクションで設定されたアクセスポリシー
- 特定のシグニチャに対するブロックアクションを使用したIPSの有効化

# 解決策

この動作は、アクセスポリシーのWarnアクションがIPSブロック設定よりも優先されるCisco Secure Accessの不具合として認識されています。この問題は、アクセスポリシー警告アクションとIPSブロッキング機能の間のインタラクションに影響します。

## 確認手順

ご使用の環境でこの動作を確認するには、次の手順を実行します。

ステップ1:Warnアクションを含むアクセスポリシーを設定し、IPSブロッキングを有効にします。

- 警告の動作で分離するアクションの設定
- 侵入防御(IPS)の有効化
- ブロックアクションを使用したIPSの設定
- 特定の署名を適用する（例： SERVER-WEBAPP /etc/passwdファイルへのアクセスの試行、GID-SID: 1-1122）

ステップ2:IPSシグニチャをトリガーするURLにアクセスして設定をテストします

```
https://example.com/etc/passwd
```

ステップ3：動作の確認

- 警告ページが表示されます

- 警告を確認した後、続行できます
- IPSブロック設定にかかわらず、URLへのアクセスが許可される

ステップ4：アクティビティ検索ログを確認します。

- IPSブロックエントリとWEB許可エントリの両方の存在を確認します。
- 競合するログエントリが不具合を示していることを確認します

### 現状

この動作は、現在の実装では、設計上、警告アクションがIPSブロック設定を上書きする不具合として確認されています。GID-SID:1-1122以外のIPSシグニチャでも同じ動作が発生します。これは、Warnアクションが設定されているすべてのIPSシグニチャに影響するシステム上の問題であることを示しています。

この不具合の修正計画とスケジュールはまだ決定されていません。この問題が発生している組織では、セキュリティポリシーを評価し、厳密なIPSブロッキングが必要な場合は代替設定を検討する必要があります。

## 原因

根本的な原因は、Cisco Secure Accessの不具合です。この問題では、アクセスポリシーのWarnアクション処理がIPSブロックの適用よりも優先されます。この設計上の欠陥により、ユーザは警告確認メカニズムによるIPSセキュリティ制御をバイパスでき、警告アクションが設定されている場合にIPSブロック機能を事実上無効にすることができます。

Cisco Bug ID CSCwt39270（登録ユーザ専用）がこのケースに関連していますが、このバグと、確認されたWarnとIPSの動作との間の具体的な関係については、さらに調査が必要です。

## 関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。