

# Cisco Secure Access Control Systemのパスワード変更の脆弱性



アドバイザリーID : Cisco-SA-20110330-[CVE-2011-0951](#)  
初公開日 : 2011-03-30 16:24  
バージョン 1.0 : Final  
CVSSスコア : [5.0](#)  
回避策 : No Workarounds available  
Cisco バグ ID :

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

## 概要

Cisco Secure Access Control System(ACS)には、認証されていないリモートの攻撃者がユーザパスワードを変更できる可能性のある脆弱性が存在します。

この脆弱性は、Cisco Secure ACSアプリケーションのWebベース管理インターフェイスにおけるユーザパスワード変更機能に対する不適切なセキュリティ制限に起因します。認証されていないリモートの攻撃者は、悪意のある要求をシステムに送信することで、この脆弱性を不正利用する可能性があります。成功すると、攻撃者はユーザアカウントのパスワードを変更する可能性があります。

シスコはこの脆弱性をセキュリティアドバイザリで確認し、更新されたソフトウェアをリリースしました。

この脆弱性を不正利用するには、攻撃者は悪意のある要求をターゲットシステムに送信する必要があります。攻撃者が悪用を実行するには、内部ネットワークへのアクセスが必要になる可能性があります。

シスコはCVSSスコアを通じて、機能的なエクスプロイトコードが存在することを示していますが、このコードが一般に公開されることは確認されていません。

## 該当製品

シスコは、次のリンクでCisco Bug ID [CSCti77440](#)のセキュリティアドバイザリをリリースしてい

ます。 [cisco-sa-20110330-ac](#)s

## 脆弱性のある製品

次のバージョンのCisco Secure ACSがこの脆弱性の影響を受けます。 ハードウェアアプライアンスとソフトウェアのみのバージョンの両方に脆弱性が存在します。

- パッチ3、4、5のいずれか ( またはこれらのパッチの任意の組み合わせ ) がインストールされ、パッチ6以降がインストールされていないCisco Secure ACSバージョン5.1
- パッチがインストールされていないCisco Secure ACSバージョン5.2
- パッチ1または2 ( あるいは両方 ) がインストールされ、パッチ3以降がインストールされていないCisco Secure ACSバージョン5.2

## 脆弱性を含んでいないことが確認された製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

## 回避策

使用可能なソフトウェアアップデートを適用することを推奨します。

管理者は、IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけが該当システムのWebベースの管理インターフェイスにアクセスできるようにすることを検討できます。

管理者は重要なシステムを監視することを推奨します。

Cisco Applied Intelligenceチームは、管理者がこの脆弱性を悪用しようとする試みを識別して緩和するために、更新されたソフトウェアを適用する前に、次の関連ドキュメントを作成しました。

[cisco-amb-20110330-ac](#)s

## 修正済みソフトウェア

契約が有効なシスコのお客様は、 [Cisco](#) のSoftware Centerからアップデートを入手できます。 契約をご利用でないお客様は、 1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)に連絡するか、 [tac@cisco.com](mailto:tac@cisco.com) のEメールでアップグレードを入手できます。

## 推奨事項

```
$propertyAndFields.get("recommendations")
```

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team ( PSIRT ) は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20110330-CVE-2011-0951>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2011年3月30日

## 利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

## 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。