セキュリティクラウド制御のドメインを確認 – CUI更新

内容

概要

このドキュメントでは、Cisco Unified Identity(CUI)の更新後に、Security Call Control(SCC)で新しいドメインを検証する方法について説明します。

背景

Cisco Security Cloud Control(SCC)でドメインを要求および検証する際、管理者はドメインの所有権を証明するためにDNS TXTレコードを公開する必要があります。

問題

検証を成功させるために必要なDNSレコードの配置に変更があります。シスコのドキュメントで参照されている前述の手順では、専用の検証サブドメインを使用します。

_cisco-sxso-verification.example.com

ただし、現在の検証プロセスでは、専用の検証サブドメインではなく、ルートドメインの直下で、シスコが提供するTXT検証トークンを公開する必要があります。

変更点を教えてください。

以前の構成（現在の検証ワークフローには適用されなくなりました）:

DNSフィールド	値
レコード タイプ	テキスト
ホスト/名前	_cisco-sxso-verification.example.com

値	Cisco検証トークン

新しい構成（必須）:

DNSフィールド	値
レコード タイプ	テキスト
ホスト/名前	@
値	Cisco検証トークン

解決方法

実装ステップ

1. ドメインのDNSプロバイダー（GoDaddy、Cloudflare、Route 53、Azure DNSなど）にログインします。
2. ドメインのDNS管理に移動します。
3. 新しいTXTレコードを作成します。
4. レコードを次のように設定します。
   タイプ： TXT
   ホスト/名前： @
   値：Cisco SCCによって生成された検証トークンを貼り付けます。
   TTL：デフォルト値。
5. DNSレコードを保存し、DNS伝播の時間を許可します。
6. Cisco SCCに戻り、Verifyをクリックします。

確認

次のコマンドを使用すると、TXTレコードが正しくパブリッシュされたことを確認できます。

```
dig TXT example.com
```

応答には、シスコの検証トークンを含める必要があります。

レコードがDNSに表示されたら、SCCに戻り、ドメインの検証を再試行します。

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。