Cisco Advanced Phishing Protection：導入プロセス（オンプレミス型）

発行日：2018 年 6 月 22 日

Cisco Advanced Phishing Protection の導入

Cisco Advanced Phishing Protection は簡単で明確なプロセスで導入できます。このプロセスは、大規模組織の E メール セキュリティ戦略をサポートしてきた長年の経験に基づいて改良が重ねられました。次の 3 つの主要なプロジェクト エレメントが含まれます：1) Cisco E メール セキュリティ ゲートウェイ 2) オンプレミス型 Cisco Advanced Phishing Protection センサー 3) Cisco Advanced Phishing Protection。

これらの目標を達成します。

- メッセージング アーキテクチャの理解
- Cisco Advanced Phishing Protection センサーの導入
- メッセージ トラフィックの確認
- 正確なメッセージ スコアリングの検証
- 適用モードでの 1 つの Cisco Advanced Phishing Protection ポリシー

追加の個別の手順を詳しく説明します。

主要なプロジェクト タスク

主要なオンボーディング タスクは以下で構成されています。

- Cisco Advanced Phishing Protection センサーへすべてのメッセージをデュアル配信するための Cisco E メール セキュリティ アプライアンスの設定。組織の受信メール ストリームに対する完全な可視性の有効化。
- オンプレミス型 Cisco Advanced Phishing Protection センサーの導入。Cisco Advanced Phishing Protection の E メール トラスト プラットフォームに必要なメッセージの詳細（認証ヘッダー）を提供。

Cisco Systems, Inc.
www.cisco.com

- ポリシー & データ モデルを調整。組織への有効なメッセージを正確に識別するための調整。悪意のあるメッセージ（BEC）を効果的に識別するためのポリシーの調整。
- ポリシーの適用の有効化。
- 悪意のあるメッセージ（フレンドリ名のスプーフィング）をブロックするポリシーの実行。