



Cisco Domain Protection: 導入プロセス

公開日: 2018年7月22日

Cisco の導入は簡単で、明確に定義されたプロセスです。このプロセスは、大規模な組織を電子メールセキュリティイニシアティブによってサポートする数年間のエクスペリエンスに基づいて精緻化されています。2つの主要なプロジェクト要素が含まれます。1) Cisco と 2) 組織の DNS です。

これらの目標を達成します。

- DMARC レコードの導入
- サードパーティの送信者を含むメッセージストリームの認証
- DMARC でセキュリティ保護された1つのドメイン

Pre-requisite's	Introduction Call Week 1	Enabement call Week 2	Portal Overview Week 3	Authenticate Senders Week 4	Authenticate Senders Week 5	Enforcement Call Week 6	Transition call Week 7-8
<ul style="list-style-type: none">• Capture & share Messaging Architecture information• Identify target domain to secure• Publish DMARC record	<ul style="list-style-type: none">• Team introduction• Message Architecture overview• Project plan review	<ul style="list-style-type: none">• Start Sender identification• Start to identify business owners• Assist customer as needed	<ul style="list-style-type: none">• Overview of Agari Portal• Review best practices	<ul style="list-style-type: none">• Implement Authentication protocols• Complete Sender Identification• Continue business owner identification	<ul style="list-style-type: none">• Implement Authentication protocols• Complete business owner identification	<ul style="list-style-type: none">• Achieve 99%+ authentication• Secure domain• Monitor and confirm message traffic• Review best practices	<ul style="list-style-type: none">• Review overall project & deliverables• Review Agari Service offerings:• Technical Support• Customer Success Management• ESP Service

個別の追加ステップについては詳細に説明します。

主要なプロジェクト タスク

主要なオンボーディング タスクには次が含まれます。

- 対象ドメインの DMARC モニタレコードの発行。組織の送信メールストリームに対する完全な可視性の有効化。
- 認証プロトコルとして DMARC を実装した送信者の認証。
- 99% 以上のメッセージ認証の検証の有効性と外部の電子メール受信者に対するメッセージストリームの信頼性の実現。
- DMARC によるドメインの保護。
- ドメインを詐称したなりすまし電子メールからの顧客とパートナーの保護。



