

Cisco Email Security Advanced Phishing Protection v1 – インスタント デモ

最終更新日: 2018 年 8 月 9 日

このデモンストレーションについて

このデモンストレーションには、以下の内容が含まれます。

- [要件](#)
- [このソリューションについて](#)
- [トポロジ](#)
- [はじめに](#)
- [シナリオ 1: 電子メールの概要](#)
- [シナリオ 2: ドメイン スプーフィング](#)
- [シナリオ 3: アカウントの乗っ取り](#)
- [シナリオ 4: 表示名偽装によるビジネス メール詐欺](#)
- [シナリオ 5: ポリシー](#)
- [シナリオ 6: メッセージの分析](#)

要件

次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. 要件

必須	オプション
<ul style="list-style-type: none"> • ラップトップ • Google Chrome または Mozilla Firefox ブラウザの最新バージョン • Cisco Advanced Phishing Protection アプリケーションへの URL • Cisco Advanced Phishing Protection アプリケーション用のアカウント 	<ul style="list-style-type: none"> • Cisco AnyConnectR

このソリューションについて

今日のサイバー攻撃者は、ますます高度化する ID 偽装手法を駆使して、各社の従業員に攻撃を仕掛けてきます。しかし、どんな攻撃手法にも、適切なアプローチによって検出できる欠点が存在します。Cisco Advanced Phishing Protection によって、Cisco E メール セキュリティですでに実現されている送信者認証および BEC 検出機能が、さらに補強されます。

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

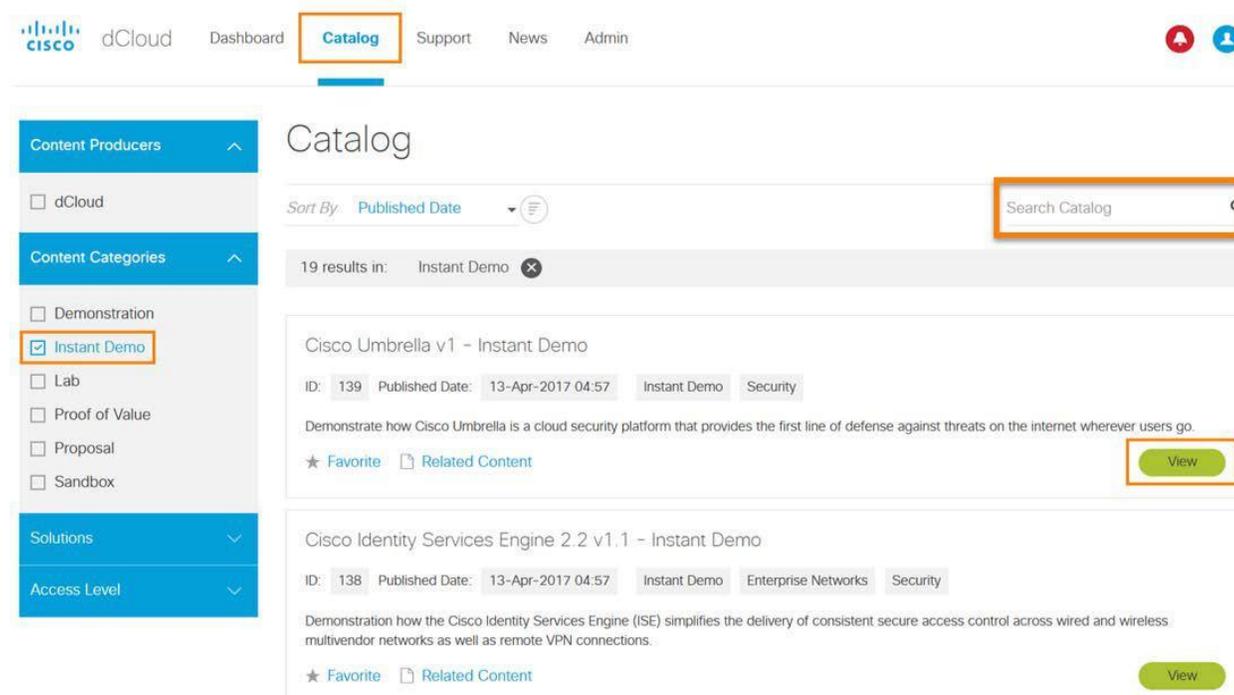
プレゼンテーションを成功させるためには、入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. [カタログ (Catalog)] をクリックして、サイド バーから [インスタント デモ (Instant Demo)] を選択します。これで、すべての dCloud インスタント デモが一覧表示されます。
2. 該当する [表示 (View)] ボタンをクリックします。

注: または、[カタログを検索 (Search Catalog)] ボックスを使用してインスタント デモの名前を検索することもできます。

図 1. インスタント デモ一覧



シナリオ 1. 電子メールの概要

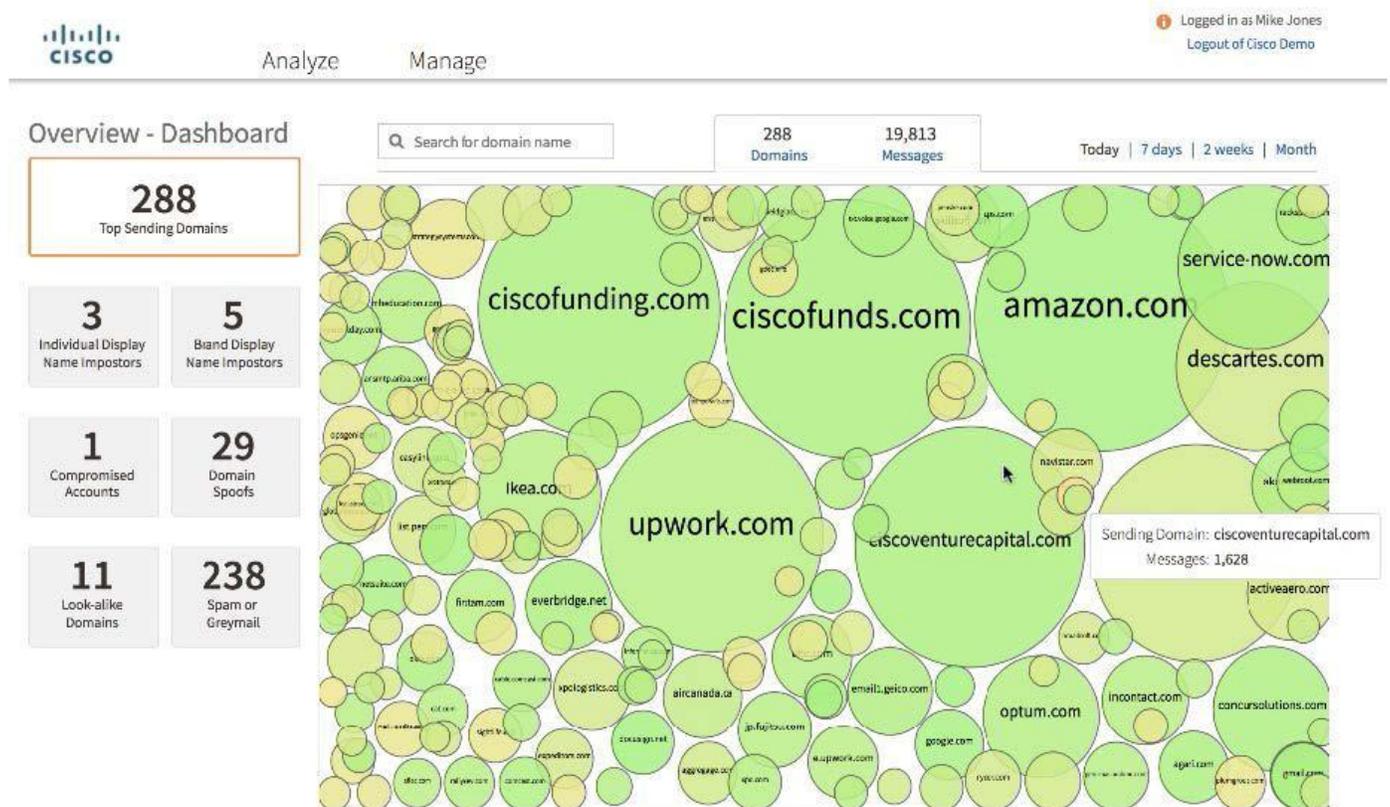
手順

アイデンティティ インテリジェンスは、本物の電子メール送信者の特徴を把握するための重要な情報となります。正当な電子メール送信者は、一貫性のある安定したパターンを示す傾向にあることが判明しています。これを把握して適切にモデル化すると、未知のメールも分類できるようになります。

Cisco Advanced Phishing Protection の [概要(Overview)] ページは、サインインすると最初に表示されるページです。ここには、今日受信した電子メールの概要が図示されています。

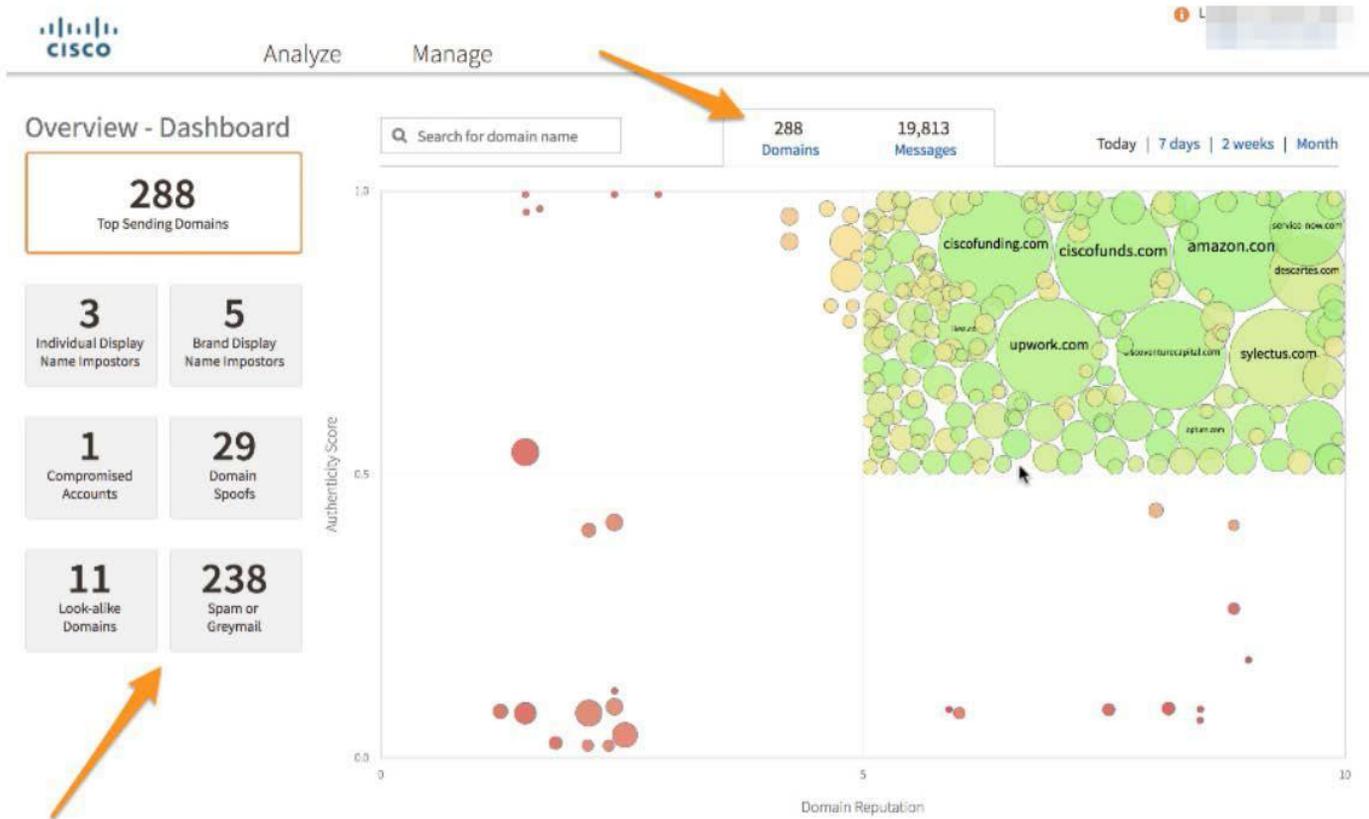
下記に示すのは、私たちの組織が今日受信した電子メールの概要です。

1. 右上の区画の空白部分をクリックすると、その区画が拡大されます。これらは、レピュテーションが高く、正規の電子メールを送信している、安定した正当な送信者です。



右上の区画を拡大すると、そこでは安定した正当な送信者を示しています。信頼できる電子メールが表示される右上の区画に、受信メールの大多数が表示されていることが、一目でわかります。

2. 空白部分をクリックすると、拡大前の表示に戻ります。



また、着信メッセージの送信元ドメインの総数と、受信メッセージの総数の概要も、簡単に把握できます。

左側のタイルでは、Advanced Phishing Protection によって識別された攻撃の種類が、わかりやすく示されています。

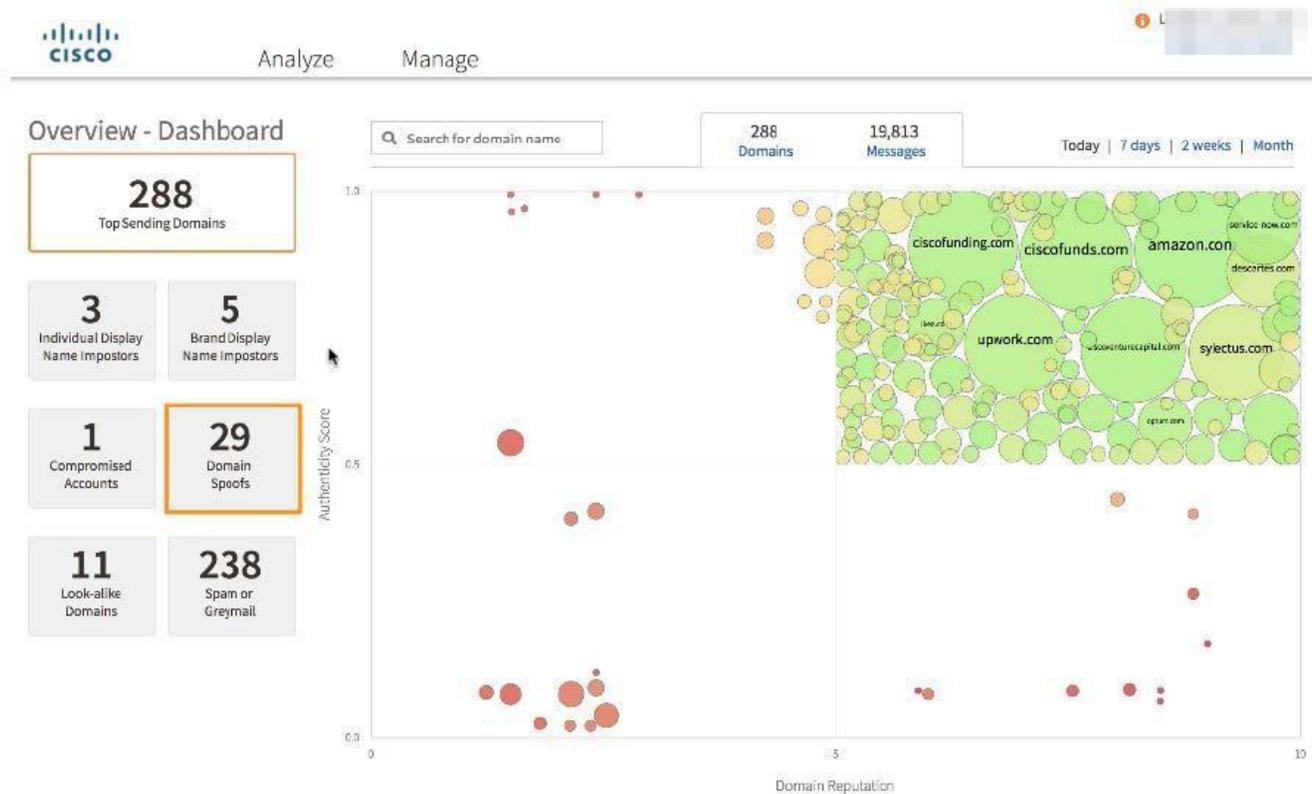
上部には、メール送信元ドメインの数と受信メッセージの数が表示されます。攻撃の種類と、それぞれに分類されるメッセージ数が、左側に示されます。

シナリオ 2. ドメイン スプーフィング

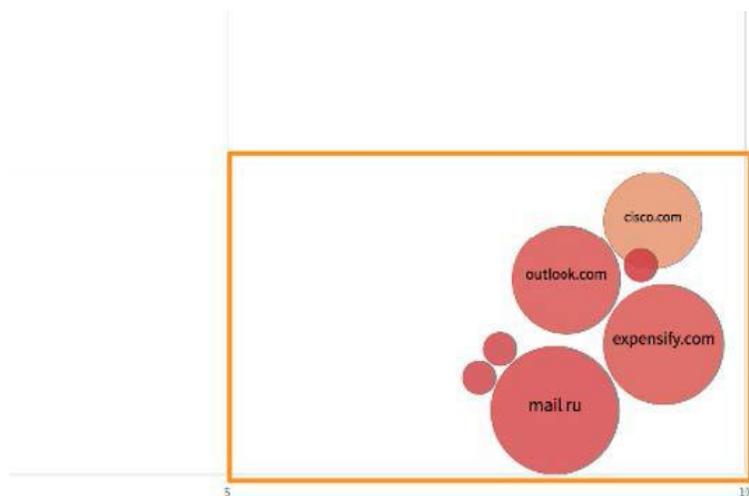
ドメイン スプーフィングとは、攻撃の一種です。このシナリオでは、ドメイン スプーフィングを確認する方法を紹介します。

手順

1. [ドメインスプーフィング(Domain Spoofs)] をクリックします。

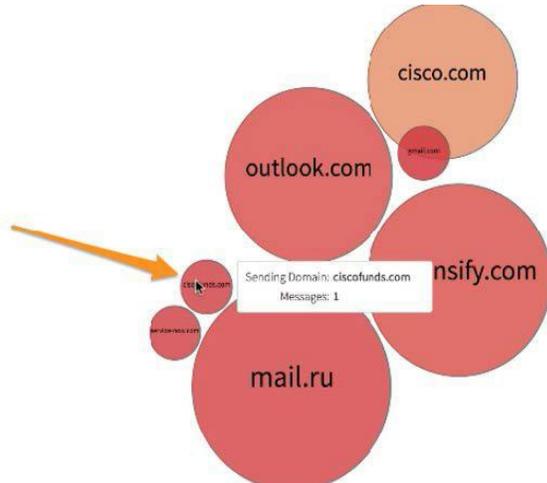


2. 右下の区画の空白部分をクリックします。



ここに表示されるのは、レピュテーションの高い送信者から着信したとされるメッセージですが、シスコの信頼性モデルに照らし合わせると、見かけと実態が異なる可能性が示唆されます。いずれかの赤い円をクリックすると、一連のメッセージを表示できます。今回は、ciscofunds.com から送信された 1 つのメッセージを見てみることにします。

3. [ciscofunds.com] の円をクリックします。



[メッセージの検索 (Search Messages)] ビューが表示されます。このビューでのフィルタリング条件は、クリックした円の条件に基づいて、あらかじめ設定されています。

4. メッセージをクリックすると、メッセージの詳細が表示されます。

To:

Reply-To:

Subject:

Attachment:

Received between: and

Authenticity Score Range:

Matched Policy:

Enforcement:

Message ID:

Attack Type:

Multiple attack types are logical ORs

Domain Reputation Range:

Domain Tags:

SBRS Range:

Sending Domain:

Hostname:

IP Address:

[Message Feedback](#)

[Create a Policy](#)

Displaying 1 - 1 of 1 Messages

Trust Score ▲	Date	From	To	Subject
0.8	29-Jun-2018	help@ciscofunds.com	rob.jenkins@ciscofunds.com	Please approve and forward expense report "June Expenses"

Displaying 1 - 1 of 1 Messages << Previous 1 Next >> Messages Per Page:

この詳細ビューでは、いくつかのスコアリング モデルの結果を確認できます。右上には、総合的なメッセージ信頼スコアが表示されます。0 ~ 10 点(10 点満点)の中 0.8 点という、非常に低いスコアになっています。このメッセージは、ciscofunds.com への送信元としては未知のサーバから着信しているため、[ドメインスプーフィング(Domain Spoof)] としても識別されていました。

Message Details

Date: 28-Jun-2018 19:05:27 PDT ⓘ

From: help@ciscofunds.com

To: rob.jenkins@ciscofunds.com

Subject: Please approve and forward expense report "June Expenses"

Message ID: <facade2c87954f9e91c755d17f1134cb@BY2PR12MB0064.ciscofunds.com>

Message Trust Score: 0.8 (Untrusted)

Domain Spoof
Message sent from a server not known to send mail for ciscofunds.com

Matched policies: Rapid DMARC

Message Trust Score Reasons

Authenticity Score: 0.1
Very low Authenticity Score

MAIL FROM: MAIL FROM does not match Header From: domain

DKIM 'd=' tag: Not available

Authentication results: SPF result not reported
DKIM result not reported
DMARC Fail

Sending Domain: ciscofunds.com
Domain Reputation: 8.5
Frequent, High Volume Sender
No Consistent Sending History

Sending IP Address: 203.26.100.17
SBRS: Not available

Search for similar messages

OK

5. ドメイン名である [ciscofunds.com] をクリックすると、このドメインに対する送信パターンが、さらに詳しく表示されます。

Message Details

Date: 28-Jun-2018 19:05:27 PDT ⓘ

From: help@ciscofunds.com

To: rob.jenkins@ciscofunds.com

Subject: Please approve and forward expense report "June Expenses"

Message ID: <facade2c87954f9e91c755d17f1134cb@BY2PR12MB0064.ciscofunds.com>

Message Trust Score: 0.8 (Untrusted)

Domain Spoof
Message sent from a server not known to send mail for ciscofunds.com

Matched policies: Rapid DMARC

Message Trust Score Reasons

Authenticity Score: 0.1
Very low Authenticity Score

MAIL FROM: MAIL FROM does not match Header From: domain

DKIM 'd=' tag: Not available

Authentication results: SPF result not reported
DKIM result not reported
DMARC Fail

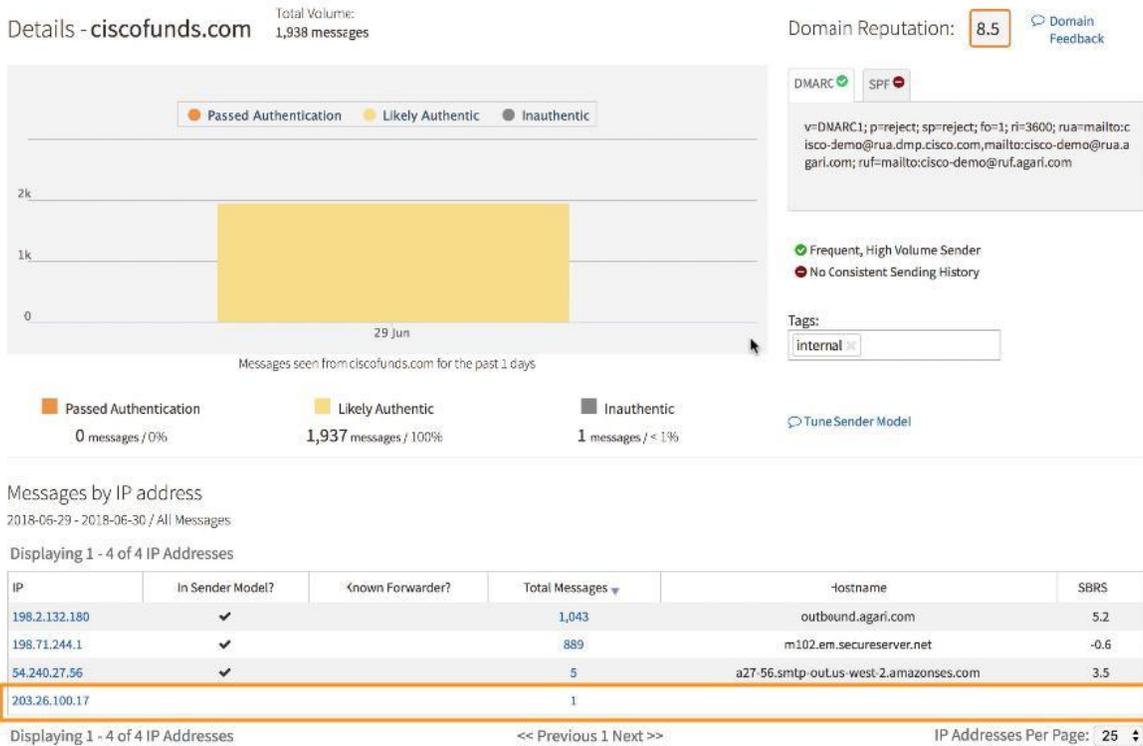
Sending Domain: ciscofunds.com
Domain Reputation: 8.5
Frequent, High Volume Sender
No Consistent Sending History

Sending IP Address: 203.26.100.17
SBRS: Not available

Search for similar messages

OK

このドメイン宛での正当な送信元 IP アドレスから着信したあらゆるメッセージと比較すると、1 つだけスプーフィング IP アドレスから着信したメッセージが目につきます。



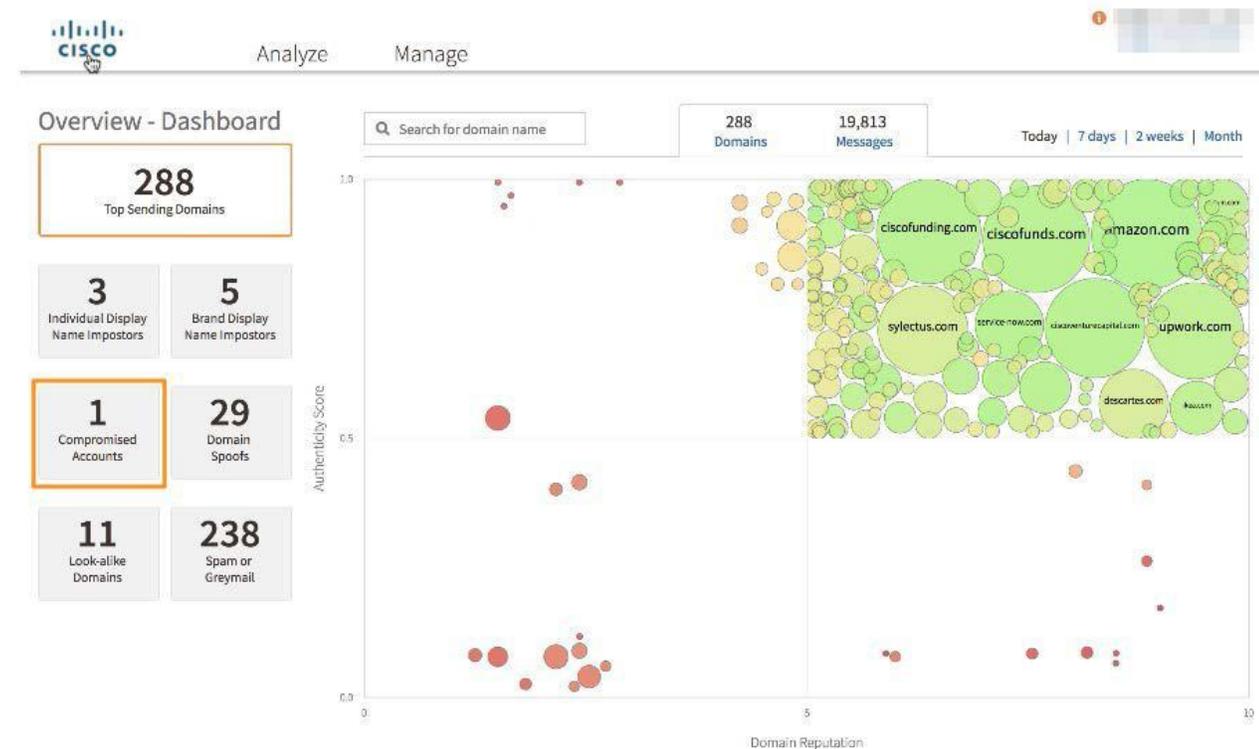
6. シスコのロゴをクリックして [概要 (Overview)] ページに戻ります。

シナリオ 3. アカウントの乗っ取り

急増している攻撃タイプの 1 つに、アカウントの乗っ取り (ATO) があります。信頼できるドメインのスプーフィングがだんだん困難になってきているため、より複雑な手法に乗り換える攻撃者が増えているのです。Advanced Phishing Protection は、さまざまなタイプの侵害を受けたアカウントからのメッセージを検出および分類します。

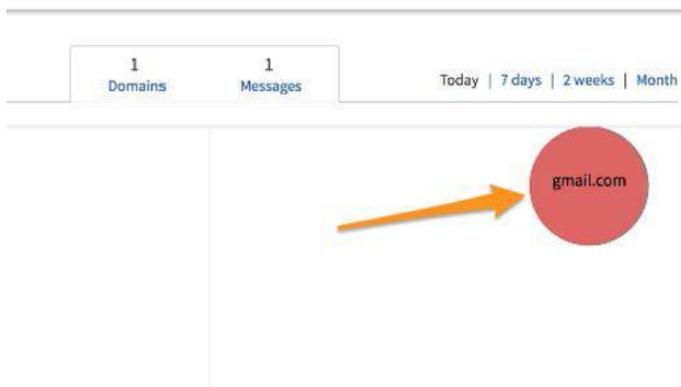
手順

1. [侵害を受けたアカウント (Compromised Accounts)] をクリックします。



このメッセージは実際には信頼できる区画に表示されています。その理由は、侵害されたアカウントがスプーフィングではなく、必ずしもなりすましとは断定されないからです。これは、実在のユーザから盗まれた ID です。

2. [gmail.com] の円をクリックします。



この例の場合、Cynthia Perdue というユーザの本物のアカウントであり、これまでは正当に使用されていたことが、シスコのモデルからわかります。

Attack Type: Multiple attack types are logical ORs

Domain Reputation Range: 5.0 10.0

Domain Tags:

SBRS Range: -10.0 10.0

Sending Domain:

Hostname:

IP Address:

Message Feedback
Create a Policy

Displaying 1 - 1 of 1 Messages

Trust Score ▲	Date	From	To	Subject
1	29-Jun-2018	Cynthia Perdue <cynthia.perdue528@gmail.com>	christopher.lutz@cisconfunding.com	Last Statement Enclosedd

Displaying 1 - 1 of 1 Messages << Previous 1 Next >> Messages Per Page: 25 ↓

3. メッセージをクリックします。

Message Feedback
Create a Policy

Displaying 1 - 1 of 1 Messages

Trust Score ▲	Date	From	To	Subject
1	29-Jun-2018	Cynthia Perdue <cynthia.perdue528@gmail.com>	christopher.lutz@cisconfunding.com	Last Statement Enclosedd

Displaying 1 - 1 of 1 Messages << Previous 1 Next >> Messages Per Page: 25 ↓

ここでは、信頼できない実行可能ファイルを含む添付ファイルを送信しているアカウントとして検出されています。このように、これまで良好だったアカウントから突然不正な動作が見られた場合、侵害の可能性が強いと言えます。

Message Details

Date: 28-Jun-2018 19:05:28 PDT ⓘ

From: Cynthia Perdue <cynthia.perdue528@gmail.com>

To: christopher.lutz@ciscofunding.com

Subject: Last Statement Enclosedd

Message ID: <006201d3b0b@aaattb86a05fee293e05@gmail.com> ⓘ

Message Trust Score: 1 (Untrusted)

- Compromised Account
cynthia.perdue528@gmail.com is a suspected compromised account
- Likely Malicious Attachment
Message contained likely malicious attachment(s):
files_2018-02-09_18-18-06_XTYXRD.zip
▶ Details

Message Trust Score Reasons

Authenticity Score: 1.0 Very high Authenticity Score	Sending Domain: gmail.com Domain Reputation: 9 Frequent, High Volume Sender No Consistent Sending History
MAIL FROM: gmail.com	Sending IP Address: 96.233.123.167 — [static-96-233-123-167.bstnma fios.verizon.net]
DKIM 'd=' tag: gmail.com	SBRS: Not available IP address is in Sender Model for this domain
Authentication results: SPF Pass DKIM Pass DMARC Pass	

Search for similar messages

OK

4. [詳細(Details)] をクリックします。

@gmail.com>

Message Trust Score: 1 (Untrusted)

- Compromised Account
cynthia.perdue528@gmail.com is a suspected compromised account
- Likely Malicious Attachment
Message contained likely malicious attachment(s):
files_2018-02-09_18-18-06_XTYXRD.zip
▶ Details

file_path: testFile3.txt
type: MIME entity
tags: Untrusted Executable, Malicious File Execution
reasons:

Sending Domain: gmail.com
Domain Reputation: 9
Frequent, High Volume Sender
No Consistent Sending History

添付ファイルは、[悪意のあるファイルの実行 (Malicious File Execution)] を伴う [信頼できない実行可能ファイル (Untrusted Executable)] と分類されています。

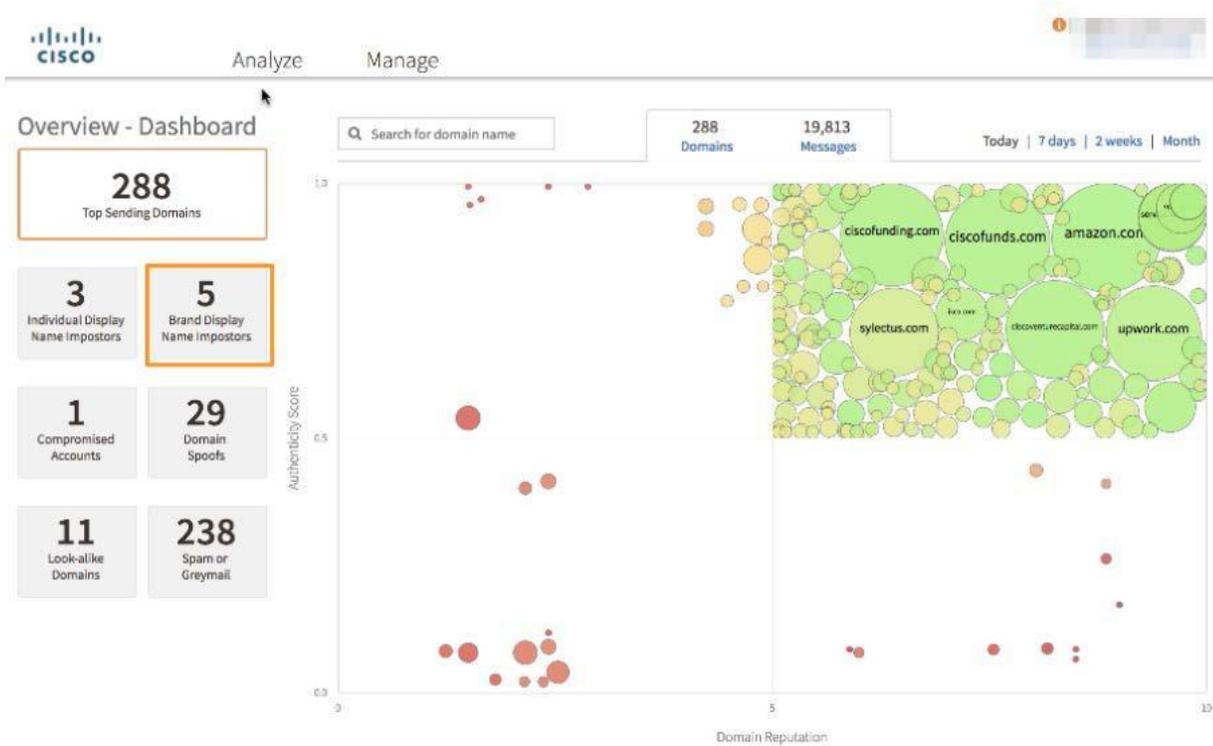
5. シスコのロゴをクリックして [概要 (Overview)] ページに戻ります。

シナリオ 4. 表示名偽装によるビジネス メール詐欺

ビジネス メール詐欺(BEC)は、多くの場合、表示名偽装を利用して実行されます。表示名偽装は、各社の役員や有名ブランドになりすますために犯罪者が使用する、一般的な手口です。Advanced Phishing Protection では、この両方の種類の攻撃を特定することができます。

手順

1. [ブランド表示名なりすまし(Brand Display Name Imposters)]をクリックします。



現在、5件のブランド表示名なりすましが確認されています。ここでは、その送信元ドメインの簡単な概要を表示します。

2. [メッセージの表示(Show Messages)]をクリックします。



ここに表示されている HSMC、Amazon、Wells Fargo、Apple、eBay という大手ブランドはすべて、現在なりすましの対象になっています。

Attachment: Message ID:

Received between: and

Attack Type:
 Multiple attack types are logical ORs

Domain Reputation Range: to Domain Tags: SBRS Range: to

Sending Domain: Hostname: IP Address:

[Message Feedback](#)
[Create a Policy](#)

Displaying 1 - 5 of 5 Messages

Trust Score ▲	Date	From	To	Subject
0.5	29-Jun-2018	HSBC <bank-director@post.com>	fiona.ying@ciscofunding.com	[URGENT] Your Department Director needs your input- Ref. BH5418470218
0.5	29-Jun-2018	Amazon Services <aws-amazonid@noreply.com>	susan.ammerlangen@cisco.com	Problems with your Amazon Account - Confirm Now*
0.5	29-Jun-2018	Wells Fargo <superian.jenkins@gmail.com>	susan.ammerlangen@cisco.com	Account Problem
0.5	29-Jun-2018	Apple Support <apple_support_online@gmail.com>	cadenza.erhardt@ciscofunds.com	Issue with your Account
0.5	29-Jun-2018	eBay <payments4ebay@consultant.com>	darlene.hubbard@ciscofunds.com	eBay Buyer Protection Program - Item ID # 743862017153 - 2007 Ford F-150 Lariat

Displaying 1 - 5 of 5 Messages << Previous 1 Next >> Messages Per Page: 25 ▾

3. [Apple Support] のメッセージをクリックします。

Displaying 1 - 5 of 5 Messages

Trust Score ▲	Date	From	To	Subject
0.5	29-Jun-2018	HSBC <bank-director@post.com>	fiona.ying@ciscofunding.com	[URGENT] Your Department Director needs your input- Ref. BH5418470218
0.5	29-Jun-2018	Amazon Services <aws-amazonid@noreply.com>	susan.ammerlangen@cisco.com	Problems with your Amazon Account - Confirm Now*
0.5	29-Jun-2018	Wells Fargo <superian.jenkins@gmail.com>	susan.ammerlangen@cisco.com	Account Problem
0.5	29-Jun-2018	Apple Support <apple_support_online@gmail.com>	cadenza.erhardt@ciscofunds.com	Issue with your Account
0.5	29-Jun-2018	eBay <payments4ebay@consultant.com>	darlene.hubbard@ciscofunds.com	eBay Buyer Protection Program - Item ID # 743862017153 - 2007 Ford F-150 Lariat

Displaying 1 - 5 of 5 Messages << Previous 1 Next >> Messages Per Page: 25 ▾

このメッセージは、レピュテーションの高い送信者である Gmail から着信したものであり、Gmail のインフラストラクチャから正当に送信されていますが、Apple サポートが gmail.com アドレスのアカウントを使って受信者アカウントの問題を通知するとは、通常は考えられません。

Message Details

Date: 28-Jun-2018 19:05:27 PDT ⓘ

From: **Apple Support** <apple_support_online@gmail.com>

To: cadenza.erhardt@cisconfunds.com

Subject: Issue with your Account

Message ID: <ca8b7017011108234739f881df70b55@gmail.com>

Message Trust Score: 0.5 (Untrusted)

Brand Display Name Impostor
apple_support_online@gmail.com is not expected to send for apple

Matched policies: General Imposters

Message Trust Score Reasons

Authenticity Score: 1.0
Very high Authenticity Score

MAIL FROM: gmail.com

DKIM 'd=' tag: gmail.com

Authentication results:
 ✓ SPF Pass
 ✓ DKIM Pass
 ✓ DMARC Pass

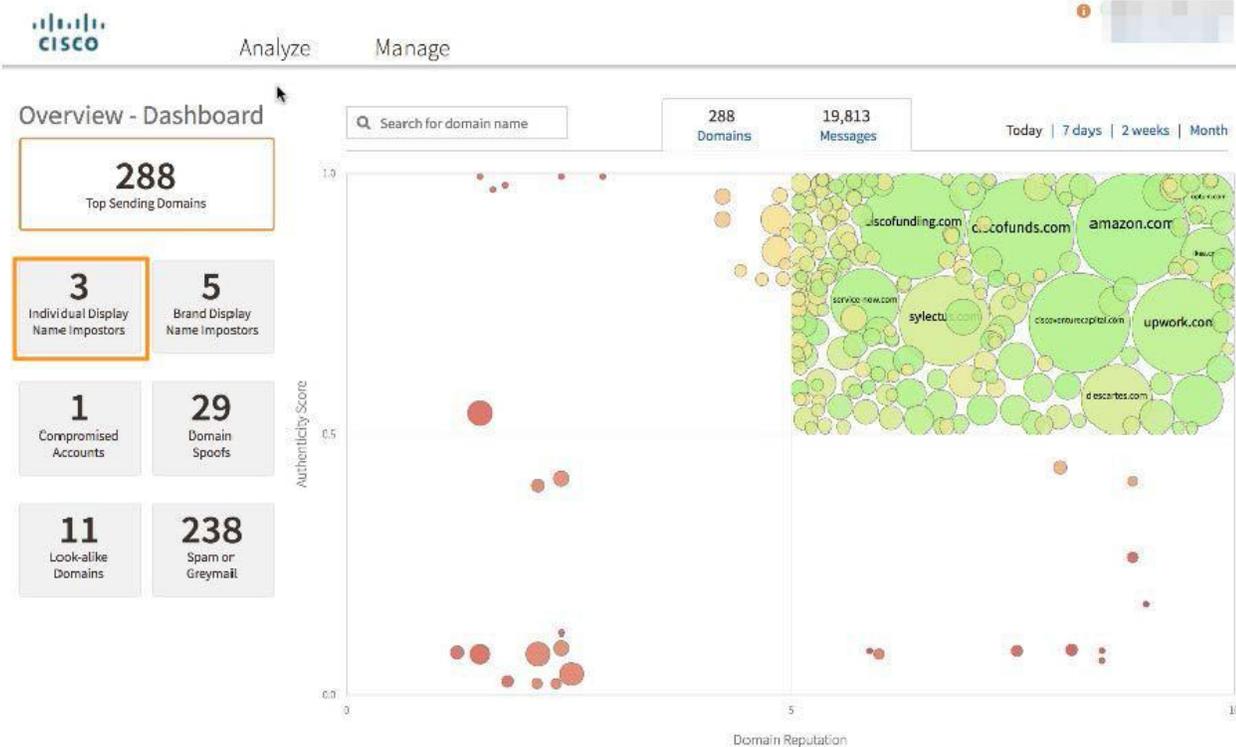
Sending Domain: gmail.com
 Domain Reputation: 9
 ✓ Frequent, High Volume Sender
 ✗ No Consistent Sending History

Sending IP Address: 209.85.223.188 -- (mail-io0-f188.google.com)
 SBRS: 3.5
 ✓ Very high SBRS
 ✓ IP address is in Sender Model for this domain

Search for similar messages

OK

4. [OK] をクリックします。
5. シスコのロゴをクリックして [概要 (Overview)] ページに戻ります。
6. [個々の表示名なりすまし (Individual Display Name Imposters)] をクリックします。



7. [メッセージの表示 (Show Messages)] をクリックします。



よくあるように、最高責任者がターゲットになっています。

8. CEO のメッセージ (Chuck Robbins へのなりすまし) をクリックします。

Create a Policy

Displaying 1 - 3 of 3 Messages

Trust Score ▲	Date	From	To	Subject
1.2	29-Jun-2018	Chuck Robbins <chet@alumni.com>	esther.topiaria@ciscofunds.com	Acquisition Terms, can we get it back quickly?
1.2	29-Jun-2018	Kelly Kramer <cfo_exec@alumni.com>	eugene.fetterbang@ciscofunds.com	W-2 copies for Audit
1.4	29-Jun-2018	Chuck Robbins <ceo_home@innocent.com>	robert.fennick@ciscofunds.com	A quick request

Displaying 1 - 3 of 3 Messages << Previous 1 Next >> Messages Per Page: 25 ↓

このなりすましメッセージの詳細を見るときは、[合致するポリシー (Matched policies)] に特に着目してください。この例でのポリシー名は、[役員のみなりすまし (Executive Impostors)] です。

Message Details

Date: 28 Jun 2018 19:05:27 PDT
From: Chuck Robbins <ceo_home@innocent.com>
To: robert.fennick@ciscofunds.com
Subject: A quick request
Message ID: <ca8b2017011108154899E881DF7DB55@aol.com>

Message Trust Score: 1.4 (Suspicious)
Individual Display Name Impostor
ceo_home@innocent.com is an impostor of chuck robbins
Matched policies: [Executive Impostors](#)

Message Trust Score Reasons

Authenticity Score: 1.0 Very high Authenticity Score	Sending Domain: innocent.com Domain Reputation: 2.8 Frequent, High Volume Sender No Consistent Sending History
MAIL FROM: innocent.com	Sending IP Address: 77.238.177.83 — (sonic305-21.consmr.mail.ir2.yahoo.com) SBRS: 1.6 IP address is in Sender Model for this domain
DKIM 'd=' tag: innocent.com	
Authentication results: SPF Pass DKIM Pass DMARC Pass	

[Search for similar messages](#)

OK

9. [OK] をクリックしてからシスコのロゴをクリックして [概要 (Overview)] ページに戻ります。

シナリオ 5. ポリシー

悪意のあるメッセージを識別するには、信頼スコアと攻撃の分類が使用されます。ポリシーとは、これらに基づいてどのようなアクションを行うか指定するルールです。使用可能なアクションの種類としては、セキュリティ管理者または SOC に対するアラート、メッセージの本来の受信者に対するアラート、メッセージの削除、受信トレイから別フォルダ（迷惑メールなど）へのメッセージの移動などの機能があります。

手順

1. [管理(Manage)] > [ポリシー(Policies)] の順に移動します。

The screenshot displays the Cisco dCloud interface. At the top, there are two tabs: 'Analyze' and 'Manage'. The 'Manage' tab is selected and highlighted with an orange box. A dropdown menu is open under 'Manage', with 'Policies' selected and highlighted with an orange box. Below the tabs, there is a 'Search Messages' section with various filters. On the right side, there are several sliders and dropdown menus for configuring search criteria. At the bottom, there are 'Search' and 'Reset' buttons.

Search Messages

Search and filter mail that has been sent to you.

From: From:

To: To:

Reply-To: Reply-To:

Subject: Subject:

Attachment:

Received between: and

Trust Score Range: 0.0 10.0

Authenticity Score Range: 0.0 1.0

Matched Policy:

Enforcement:

Message ID:

Attack Type:

Multiple attack types are logical ORs

Domain Reputation Range: 0.0 10.0

Domain Tags:

SBRs Range: -10.0 10.0

Sending Domain:

Hostname:

IP Address:

[Message Feedback](#)

[Create a Policy](#)

下記に示しているのは、メッセージの信頼スコアと攻撃の種類を使用した、最も一般的な攻撃の条件をカバーするデフォルト ポリシー セットです。

Configure Policies based on message content.

Create Policy

Configure Policy Text for Original Recipients

Show policies: All Policies

Displaying 1 - 9 of 9 Policies

Name	Conditions	Enabled?	Action	Notify Recipients?	Last Triggered	Number of Times Triggered (in last 7d)
Rapid DMARC [Manage Senders]	<ul style="list-style-type: none"> Attack types include <code>spoof</code> Domain's Tags include <code>internal</code> 	Y	None	N	29-Jun-2018 0:05:28 UTC	12,060
Executive Imposters	<ul style="list-style-type: none"> From: address: <ul style="list-style-type: none"> matches a Display Name in <code>Executives</code> 	Y	None	N	29-Jun-2018 0:05:29 UTC	29
C-Level Imposters	<ul style="list-style-type: none"> From: address: <ul style="list-style-type: none"> matches a Display Name in <code>C-Level Executives</code> 	Y	None	N	29-Jun-2018 0:05:29 UTC	11
Spoof of Partner Domains	<ul style="list-style-type: none"> Attack types include <code>spoof</code> Domain's Tags include <code>partner</code> 	Y	None	N	29-Jun-2018 0:05:29 UTC	10
Look-alike Domains	<ul style="list-style-type: none"> Attack types include <code>lookalike_domain</code> 	Y	None	N	Never	0
Brand Display Name Imposters	<ul style="list-style-type: none"> Attack types include <code>dnj</code> 	Y	None	N	Never	0
Suspicious Messages to C-Level	<ul style="list-style-type: none"> To: address: <ul style="list-style-type: none"> matches a Display Name in <code>C-Level Executives</code> Message Trust Score is between 0.0 and 3.1 	Y	None	N	Never	0
Untrusted Messages	<ul style="list-style-type: none"> Message Trust Score is between 0.0 and 1.1 	Y	None	N	Never	0
Low Message Trust and Low Server Reputation	<ul style="list-style-type: none"> Message Trust Score is between 0.0 and 2.5 SBRs is between -10.0 and -2.0 	Y	None	N	Never	0

Displaying 1 - 9 of 9 Policies

<< Previous 1 Next >>

Policies Per Page: 25

Rapid DMARC ポリシーは、パブリック DMARC 拒否ポリシーを発行するよりも短時間のうちに、自ドメインを着信スプーフィングから保護できる、特別なポリシーです。ポリシー条件が社内ドメインのスプーフィングを特定する設定になっていることに注目してください。ポリシーの横にある [送信者の管理(Manage Senders)] リンクをクリックすると、Advanced Phishing Protection の信頼モデルをガイドとして使用し、すべての送信者をすばやく簡単にカタログ化することができます。送信者のカタログ化を行わない場合でも、ポリシーはデフォルトで、Advanced Phishing Protection 信頼モデルを使用して機能します。

2. ポリシー名 **Rapid DMARC** の横にある [送信者の管理(Manage Senders)] リンクをクリックします。

Create Policy

Configure Policy Text for Original Recipients

Show policies: All Policies

Displaying 1 - 9 of 9 Policies

Name	Conditions	Enabled?	Action
Rapid DMARC [Manage Senders]	<ul style="list-style-type: none"> Attack types include <code>spoof</code> Domain's Tags include <code>internal</code> 	Y	Non
Executive Imposters	<ul style="list-style-type: none"> From: address: <ul style="list-style-type: none"> matches a Display Name in <code>Executives</code> 	Y	Non
C-Level Imposters	<ul style="list-style-type: none"> From: address: <ul style="list-style-type: none"> matches a Display Name in <code>C-Level Executives</code> 	Y	Non

これらは、シスコの社内ドメイン ciscofunds.com に対する送信者です。

Senders

Review senders to internal domains

Show senders for internal domain:

Today | 7 days | 2 weeks | Month

Senders Unassigned IP Addresses

Displaying 1 - 3 of 3 Senders

Sender	Inbound		Authenticity		Action
	Messages	IP addresses	Score	Reason	
amazon SES	5	1	1.0	Manual	✓ Approved Undo
MailChimp	1043	1	1.0	Manual	✓ Approved Undo
GoDaddy	889	1	0.8	Model	+ Approve - Deny

Displaying 1 - 3 of 3 Senders << Previous 1 Next >> Senders Per Page: 25

この例では、Amazon SES および Mail Chimp の 2 つの送信者が [承認済み (Approved)] となっています。つまり、これらはすでに、このドメイン向けの正当な送信者としてカタログ化されています。もう 1 つの送信者、GoDaddy については、信頼できるものとしてモデリングされていますが、カタログには追加されていません。これを追加すべきでしょうか。判断するには、詳細を確認する必要があります。

3. GoDaddy のロゴをクリックします。

Senders Unassigned IP Addresses

Displaying 1 - 3 of 3 Senders

Sender	Mess:
amazon SES	5
MailChimp	1043
GoDaddy	889

Displaying 1 - 3 of 3 Senders <<

メッセージはすべて、下記に示す GoDaddy の 1 つのサーバから発信されています。

Sender Details - GoDaddy Email Marketing

Sending IP addresses for internal domain:

2018-06-29 - 2018-06-30

Today | 7 days | 2 weeks | Month

Displaying 1 - 1 of 1 IP Addresses

IP	Hostname	SBRS	Total Messages
198.71.244.1	m102.em.secureserver.net	-0.6	889

Displaying 1 - 1 of 1 IP Addresses << Previous 1 Next >> IP Addresses Per Page: 25

© Copyright 2018, Cisco and/or its affiliates. All rights reserved. | Support

このサーバの SenderBase レピュテーション スコア (SBRS) は、あまり良好ではありません。メッセージ数をクリックすると、より詳しい情報を確認できます。

4. メッセージ数をクリックします。

Sender Details - GoDaddy Email Marketing

Sending IP addresses for internal domain:

2018-06-29 - 2018-06-30

Today | 7 days | 2 weeks | Month

Displaying 1 - 1 of 1 IP Addresses

IP	Hostname	SBRS	Total Messages
198.71.244.1	m102.em.secureserver.net	-0.6	889

Displaying 1 - 1 of 1 IP Addresses << Previous 1 Next >> IP Addresses Per Page: 25

© Copyright 2018, Cisco and/or its affiliates. All rights reserved. | Support

クリックすると、その一連のメッセージが示された [メッセージの検索 (Search Messages)] ページが表示されます。リストを調べて、認識している送信者かどうか確認できます。件名または送信元詳細をコンテキスト上の手がかりとして、信頼できるメッセージかどうかを確認できます。インベントリに追加したい送信者であることが確認できた場合は承認し、そうでない場合では拒否することができます。

5. ブラウザの [戻る (Back)] ボタンを 2 回をクリックして [送信者 (Senders)] ページに戻ります。
6. **送信者を承認または拒否**します。
 - 正当な送信者と思われる場合は、GoDaddy の [承認 (Approve)] リンクをクリックします。

Senders Unassigned IP Addresses

Displaying 1 - 3 of 3 Senders

Sender	Inbound		Authenticity		Action
	Messages	IP addresses	Score	Reason	
amazon SES	5	1	1.0	Manual	✓ Approved Undo
MailChimp	1043	1	1.0	Manual	✓ Approved Undo
Go Daddy	889	1	0.8	Model	+ Approve Deny

Displaying 1 - 3 of 3 Senders << Previous 1 Next >> Senders Per Page: 25

- 正当ではないと思われる場合は、GoDaddy の [拒否 (Deny)] リンクをクリックします。

Senders Unassigned IP Addresses

Displaying 1 - 3 of 3 Senders

Sender	Inbound		Authenticity		Action
	Messages	IP addresses	Score	Reason	
amazon SES	5	1	1.0	Manual	✓ Approved Undo
MailChimp	1043	1	1.0	Manual	✓ Approved Undo
Go Daddy	889	1	0.8	Model	+ Approve Deny

Displaying 1 - 3 of 3 Senders << Previous 1 Next >> Senders Per Page: 25

7. どちらの場合も、**選択を確定**します。

ここで選択したオプションによって、今後この送信者から ciscofunds.com 宛てにメッセージが送信された場合に、正当と見なされるのかスプーフイングと見なされるのが左右されます。

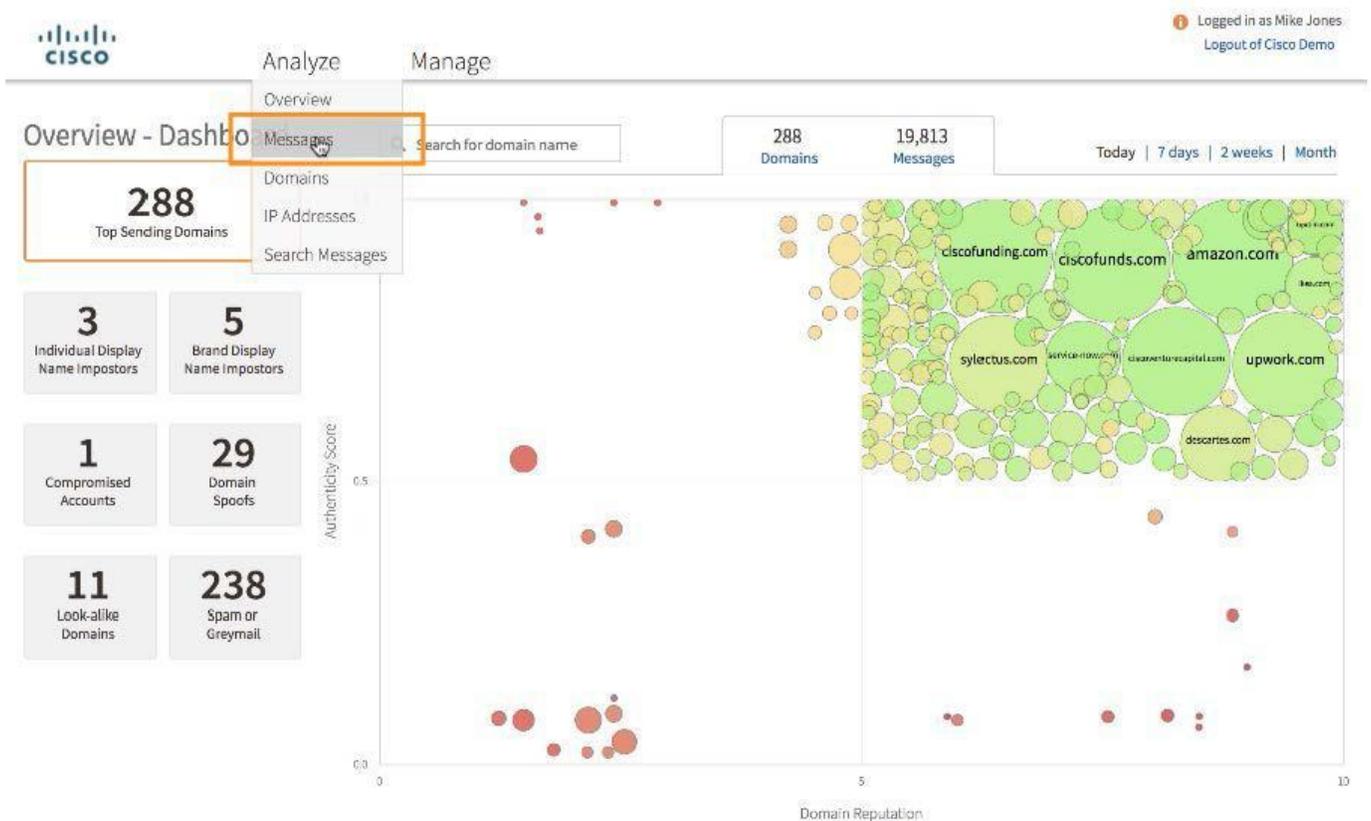
8. **シスコのロゴ**をクリックして [概要 (Overview)] ページに戻ります。

シナリオ 6. メッセージの分析

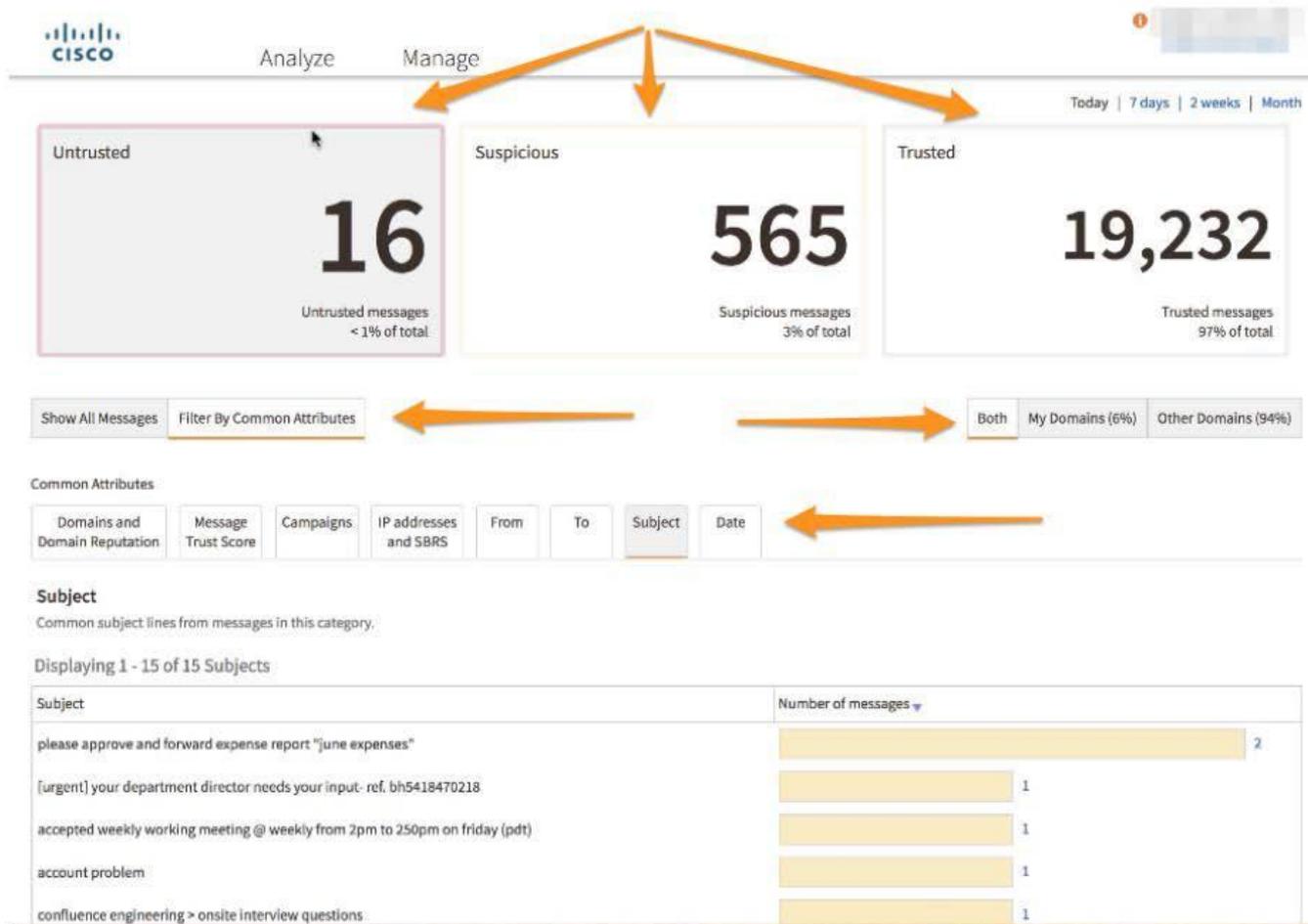
Advanced Phishing Protection では、電子メールトラフィックについて把握するための分析ビューが数多く提供されています。信頼できないメッセージ、疑わしいメッセージ、信頼できるメッセージの概観をつかむ方法として、[メッセージ(Messages)] ビューが一般的に利用されています。

手順

1. [分析(Analyze)] > [メッセージ(Messages)] の順に移動します。



これらの信頼性範囲それぞれについて、さまざまな一般的属性に基づくビューのフィルタリングを選択し、分析することができます。



2. [一般的属性でフィルタリング (Filter By Common Attributes)] をクリックしてから [件名 (Subject)] をクリックし、続いて [疑わしいメッセージ (Suspicious)] をクリックします。
3. **シスコのロゴ** をクリックして [概要 (Overview)] ページに戻ります。

本書は Cisco Advanced Phishing Protection の機能についての簡単なデモ資料ですが、皆様にとって有益なものとなることを願っています。Cisco Advanced Phishing Protection を利用すれば、現在最も複雑な BEC および ATO 攻撃で使用されている ID 偽装手法をも阻止することが可能です。

©2018 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は2018年8月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先