CISCO
SECURE

CISCO The bridge to possible

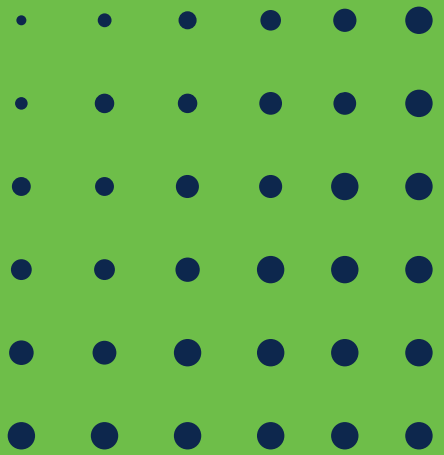
メールを開くその前に！
今だからこそ見直したい メールセキュリティ対策
～ランサムウェアはこう防ぐ！～

シスコシステムズ合同会社　セキュリティ事業
セキュリティアーキテクト　稲澤　敏
2022年4月22日

Agenda

- 始まりはEメール
- Eメールの偽装方法の理解
- Cisco Secureによるランサムウェア対策
- まとめとご参考情報

始まりはEメール



情報セキュリティ10大脅威 2022

■「情報セキュリティ10大脅威 2022」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	8位	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えい等の被害	9位

出典：IPA「情報セキュリティ10大脅威 2022」
（https://www.ipa.go.jp/security/vuln/10threats2022.html）

- 組織の脅威においては、ランサムウェアによる被害および標的型攻撃による機密情報の窃取が引き続き1位と2位
- サプライチェーンの弱点を悪用した攻撃が3位に

ランサムウェア被害状況
～2021年は日本国内でも被害多数～

CYBER SECURITY · NEWS · 4 MIN READ

Cyber Insurance Firm Suffers Sophisticated Ransomware Cyber Attack; Data Obtained May Help Hackers Better Target Firm's Customers

ALICIA HOPE · APRIL 5, 2021

Share Tweet Share Pin it

One of the largest insurance firms in the U.S. CNA Fin
"sophisticated cybersecurity attack" on March 21, 202
the company's employee and customer services for th
shut down "out of an abundance of caution" to preven

Founded in 1967, the Loews Corp subsidiary is
among the top 10 cyber ins
leading 15 casualty and pro
U.S. It employs about 5,800
annual revenue of over $10

Retailer FatFace pays $2m ransom to Conti cyber criminals

Retailer FatFace paid out a $2m ransom to restore its data following a January 2021 cyber attack by the Conti

hed: 26 Mar 2021 14:00

cessful cyber

Incident Of The Week: Garmin Pays $10 Million To Ransomware Hackers Who Rendered Systems Useless

It is believed that Garmin paid the $10 million ransom.

10NEWS

News Weather Sports Conn

APPALACHIAN UNSOLVED LIVE AT FIVE

TECH

As city computers held hostage, FBI warns of increase in ransomware attacks

sdxcentral SD-WAN SDN NFV CONTAINERS 5G SECURITY EDGE MULTI-CLOUD OPEN SOUR

Never face a dead-end job again.
Check out Career Content

News

Health-Care Providers See Surge in Ransomware Attacks in Europe, U.S.

By Ryan Gallagher | April 3, 2020

Amid COVID-19, Cyber Criminals Push Phishing, Ransomware Scams

June 16, 2020

Newsletter

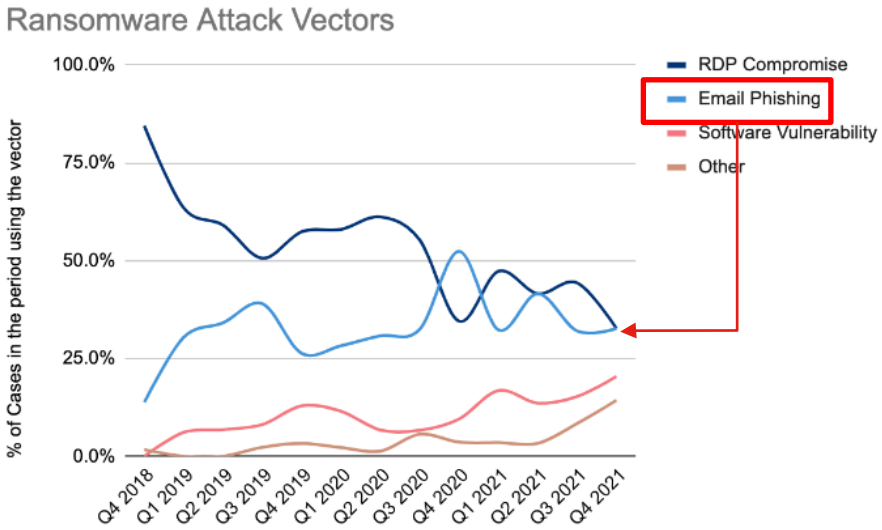
Honda Automobile Customer Service @HondaCustSvc

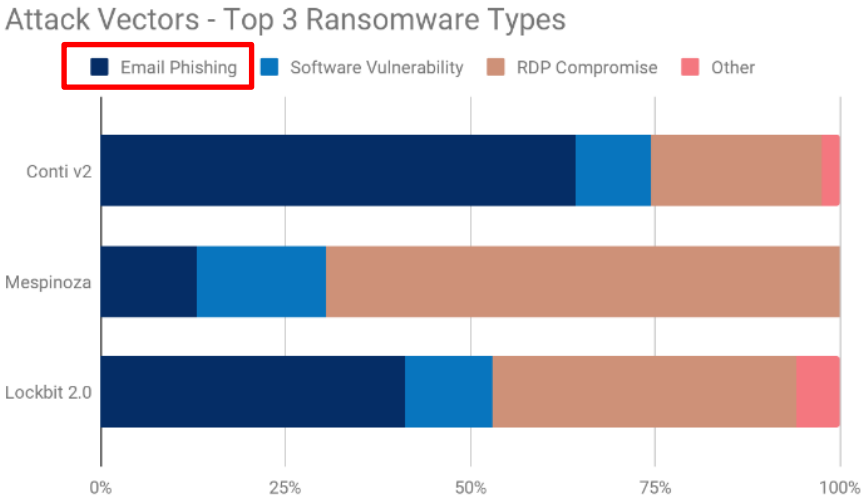
At this time Honda Customer Service and Honda Financial Services are experiencing technical difficulties and are unavailable. We are working to resolve the issue as quickly as possible. We apologize for the inconvenience and thank you for your patience and understanding.

1:43 PM · Jun 8, 2020

99 86 Share this Tweet

ランサムウェアの攻撃経路としては Emailフィッシング・RDP侵害がTop 2



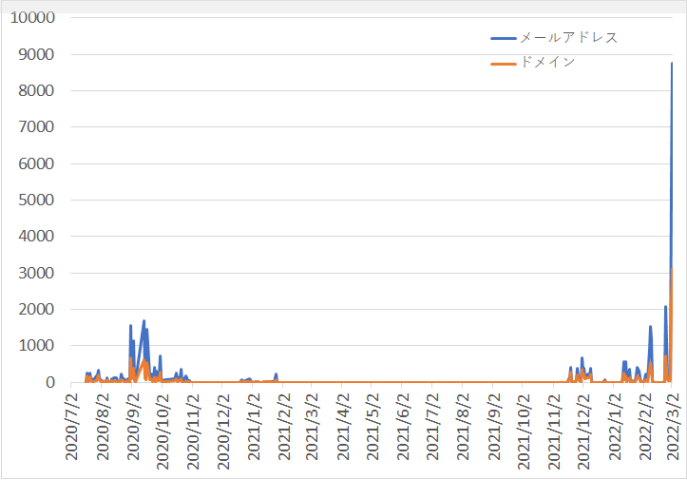


出典：https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021

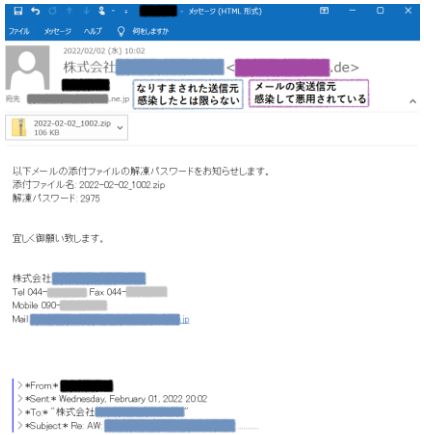
マルウェアEmotetの感染再拡大に関する注意喚起

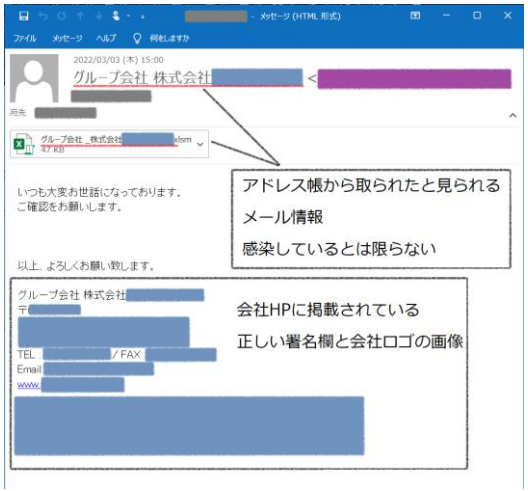
2022年2月10日にJPCERTからマルウェアEmotetの感染再拡大に関する注意喚起
（以下 https://www.jpcert.or.jp/at/2022/at220006.html から引用）

2022年3月に入り、Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年の感染ピーク時の約5倍以上に急増しています。



［図1：Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数の新規観測の推移 (外部からの提供観測情報)（2022年3月3日更新）］



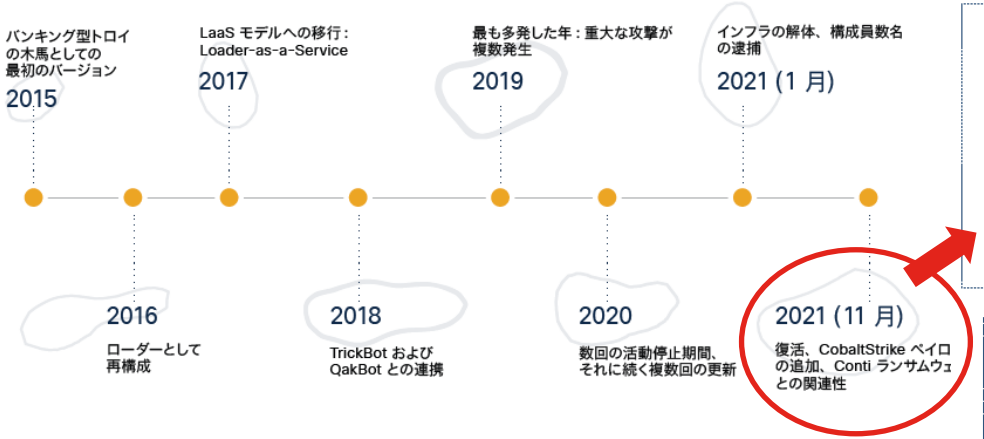


［図2, 図2-1：Emotetメールサンプル］

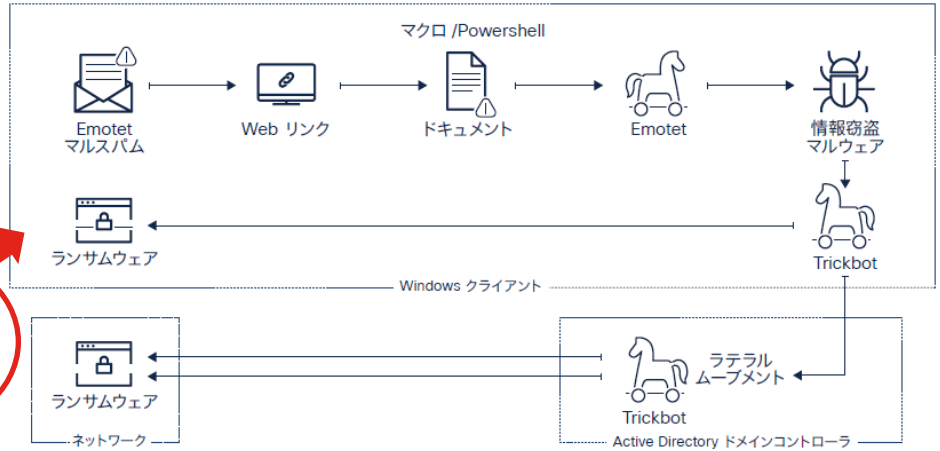
主にマクロ付きのExcelやWordファイル、あるいはこれらをパスワード付きZipファイルとしてメールに添付する形式で配信されており、ファイルを開封後にマクロを有効化する操作を実行することでEmotetの感染に繋がります。（中略）メール本文中のリンクをクリックすることで悪性なExcelやWordファイルがダウンロードされたり、アプリケーションのインストールを装いEmotet感染をねらうケースも観測しています。

今やEmotetはランサムウェアを運ぶ

Emotetの進化



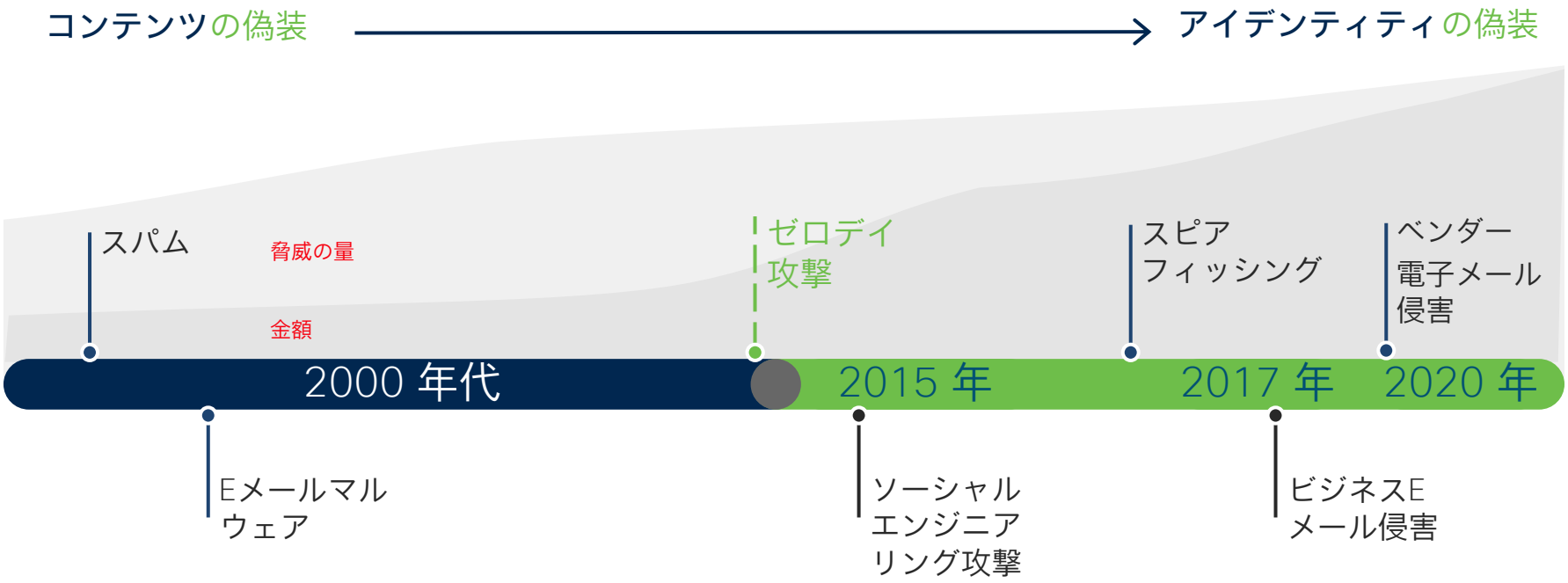
ランサムウェアのキルチェーンに変化をもたらした Emotet



出典：https://www.cisco.com/c/dam/global/ja_jp/products/collateral/security/threats-year-2022-report.pdf

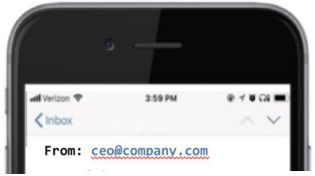
Eメールの偽装方法の理解

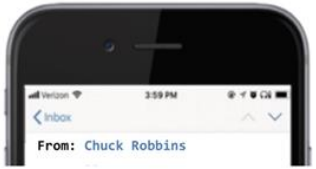
昨今のフィッシング攻撃はアイデンティティ偽装が当たり前

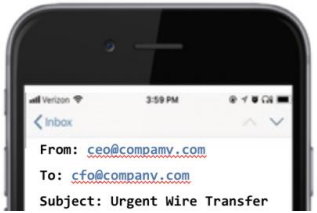


Emailなりすましのパターン

	なりすましの種類	概要
①	ドメインスプーフィング	エンベロープFromのドメインを受信者と同じドメインに偽装。レガシーな攻撃方法でSPFやDMARCでの対処が可能。
②	表示名詐欺	ヘッダFromの値を偽装し、経営層など受信者がよく知る人物名が表示される。
③	ブランド名偽造	技術的には②と同様だが、人物名ではなく受信者がよく知るブランドや会社名やドメインが表示される。件名にブランド名を記載することも
④	いとこドメイン/ 類似ドメイン	見分けのつきにくい・似せた形に模倣したドメインを使用したブランド偽装。エンベロープFrom、ヘッダFromのいずれのパターンも存在。 （例：c1sc0.com）
⑤	侵害されたアカウントを使用した攻撃	不正に取得したメールアカウントを使用して正当なメールアカウントの所有者として他の被害者にメールを送信

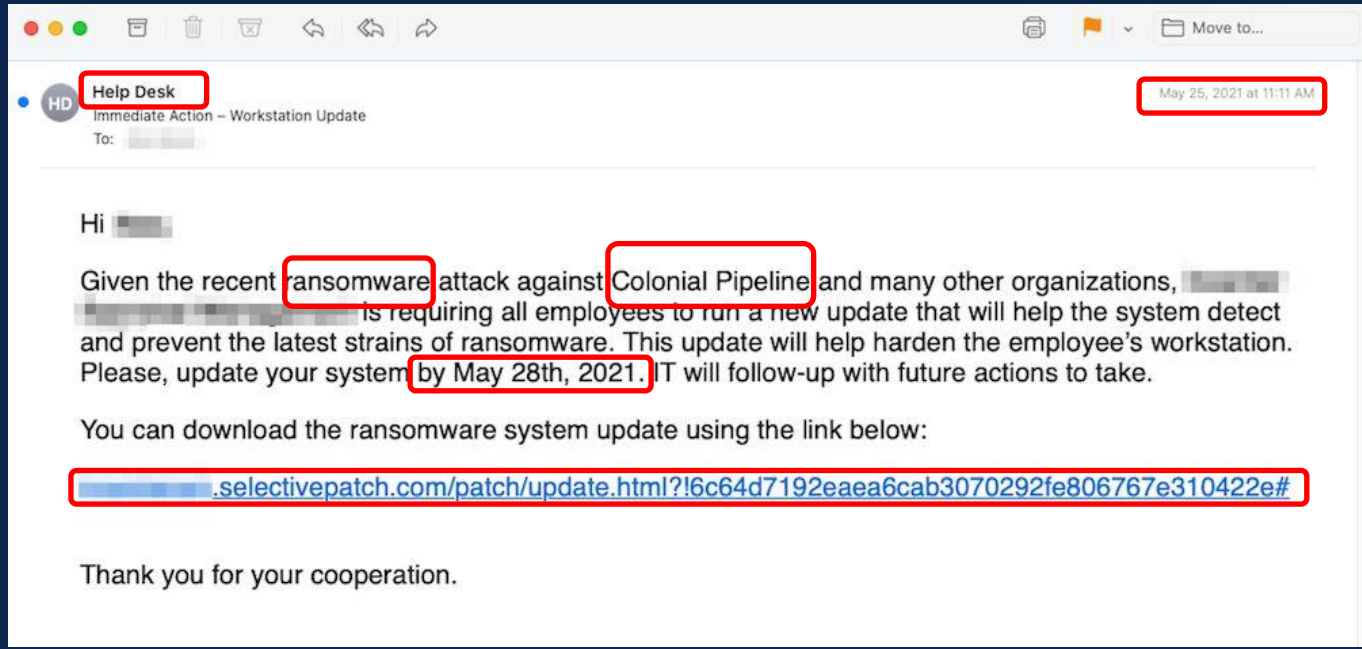






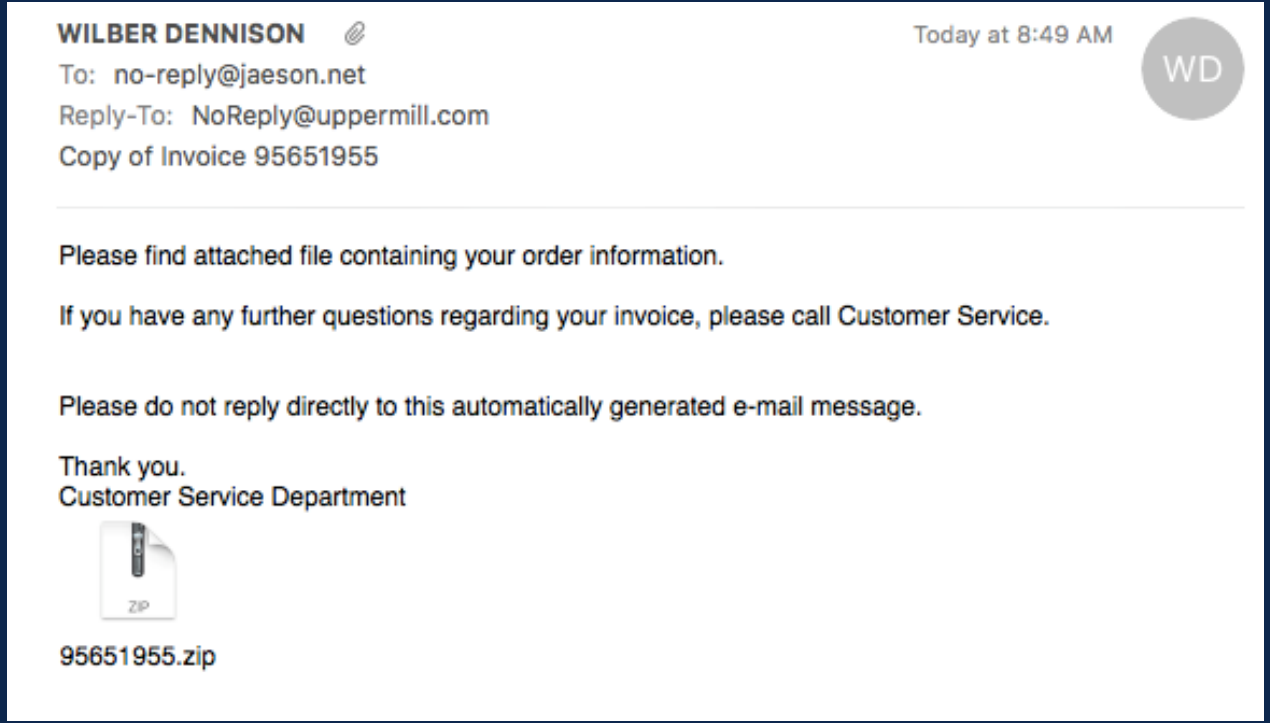
フィッシングEメールの例

- パッチ適用指示
- 緊急性
- 信頼された送信者
- URLリンク
- 流行りのワード



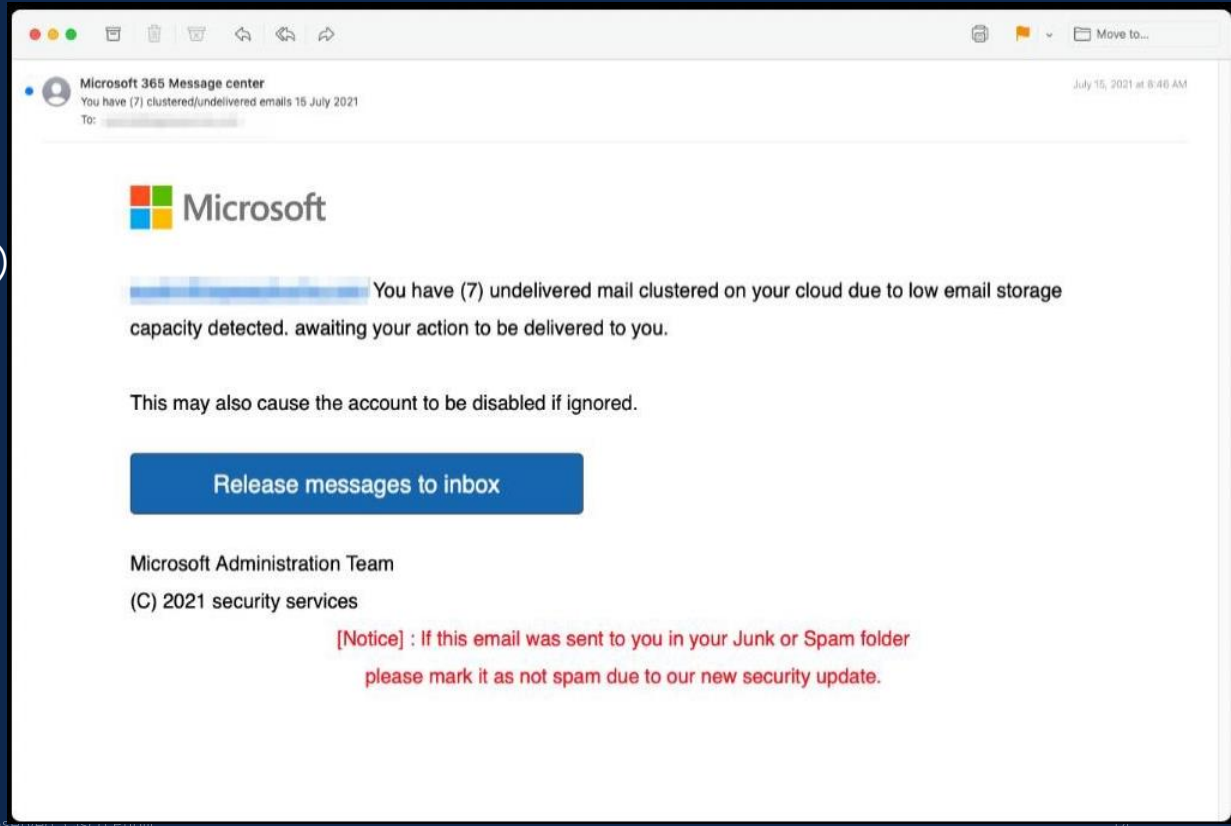
フィッシング Eメールの例

- 請求書
- 添付物
- 信頼性された送信者
- no-replyを利用



フィッシングEメールの例

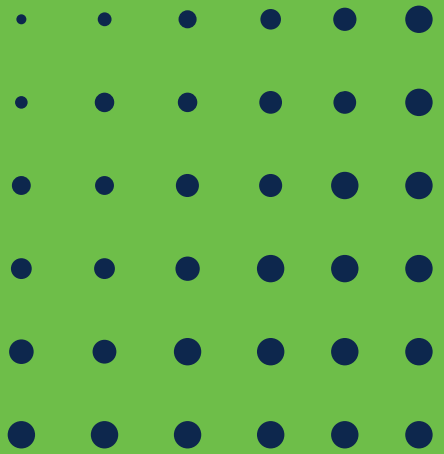
- 信頼された送信者
- 緊急性
- クリックボタン（URLを隠す）



Loading...

rs1photography.com/compact

Cisco Secureによる
ランサムウェア対策

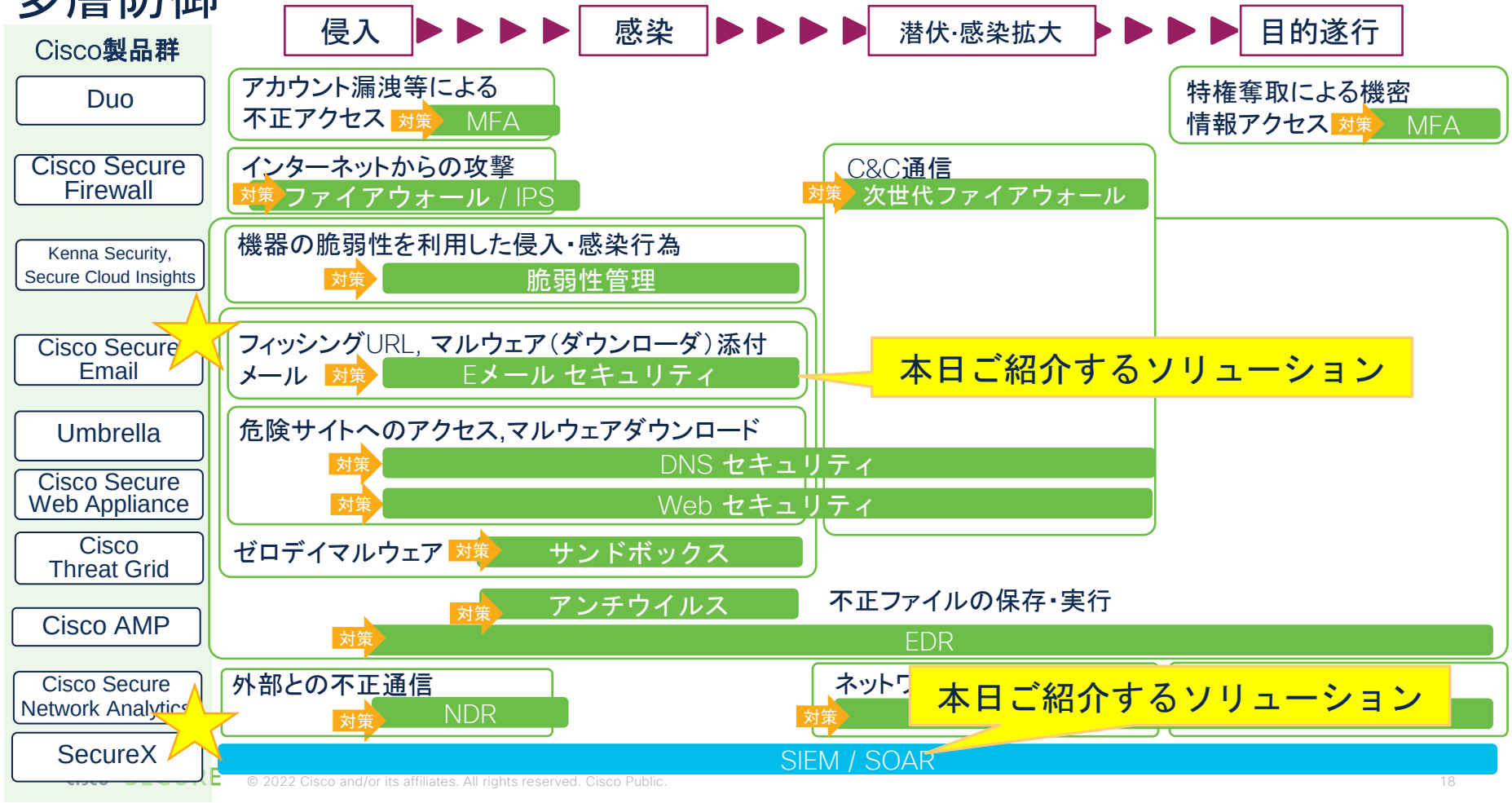


ランサムウェア対策におけるCiscoのアプローチ

- 考え方
  - ランサムウェアがネットワークに侵入するのを可能な限り防止
  - コマンドアンドコントロールを取得する前にシステムレベルで停止
  - ネットワークに存在するかどうかの検出
  - 更なるシステムやネットワークエリアへの感染拡大の封じ込め
  - インシデント対応を実行し、攻撃された脆弱性とエリアを修正

特効薬は存在しない！攻撃チェーンに沿った重要なステップをブロックするための多層型のアプローチが感染リスクを低減させるのに最も効果的！

多層防御



ランサムウェア対策としてEmail Securityに求められる要件

- 送信者のなりすましを検出するための多数の機能を備えていること
- 添付、または本文に存在するURLを分析し、悪意のある疑わしいURLからユーザを保護する機能を備えていること
- Eメールに添付されたファイルを静的・動的に分析し、マルウェアファイルからユーザを保護すること、またステルスマルウェアファイルも遡って検知が可能なこと
- 他製品と有機的に連携し、広範囲な脅威の可視性と迅速なインシデントレスポンスが提供可能なこと
- ユーザのセキュリティ意識向上のためのトレーニング機能

Cisco Secure Email

- Eメールに関わるあらゆる脅威からユーザーを保護
- 各製品間のシームレスな連携

Secure Email Gateway

包括的な脅威からの保護機能を提供するゲートウェイ型製品＆クラウドサービス

Domain Protection Phishing Defense

攻撃者がフィッシングキャンペーンで自社ドメインを使用するのを防ぐ

ID マッピングや行動分析から得たローカルインテリジェンスを使用して高度なフィッシングから保護

Cloud Mailbox

MS365の補足的なセキュリティ機能を提供するAPI型のクライドサービス

可視性、シンプルさ、ネイティブ統合を強化

内部メールスキャンが可能

Secure Awareness Training

ユーザのセキュリティ意識向上のためのトレーニングの提供

フィッシングシミュレーション

SecureX

Cisco Secureポートフォリオと既存インフラストラクチャを接続するクラウドネイティブのビルトインセキュリティプラットフォーム

ゲートウェイ型とAPI型の2つのクラウドサービスを用意

MXレコードの変更

実際のメッセージを
スキャンして
アクションを実施

メッセージを配信

MXレコードの変更不要

各メッセージのコピーを
Cloud Mailboxに送信

APIを利用したスキャンと
メールボックスへの修復

ゲートウェイ型

お客様のセキュリティ要件に応じた
きめ細やかなメッセージの
スキャンとコントロールを実現！

API型

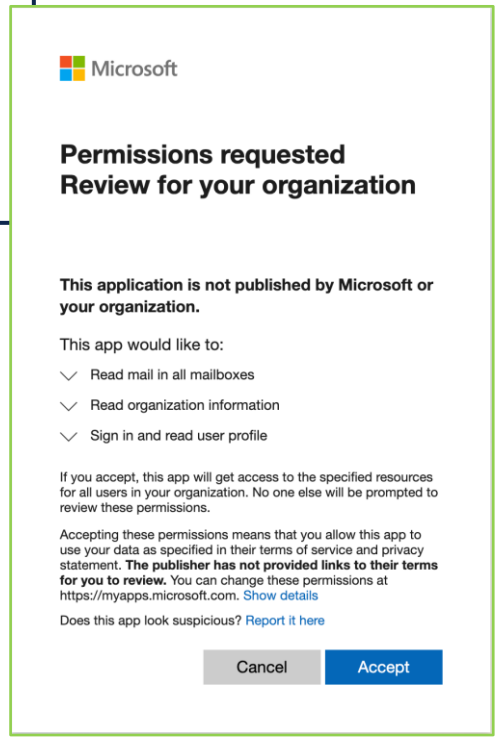
わずか5分のセットアップで
Talos脅威インテリジェンスによる
MS365への追加の脅威保護を提供！

Cloud MailboxはCloud Mailのセキュリティを補完

わずか2ステップ！MS365上で設定が完了！

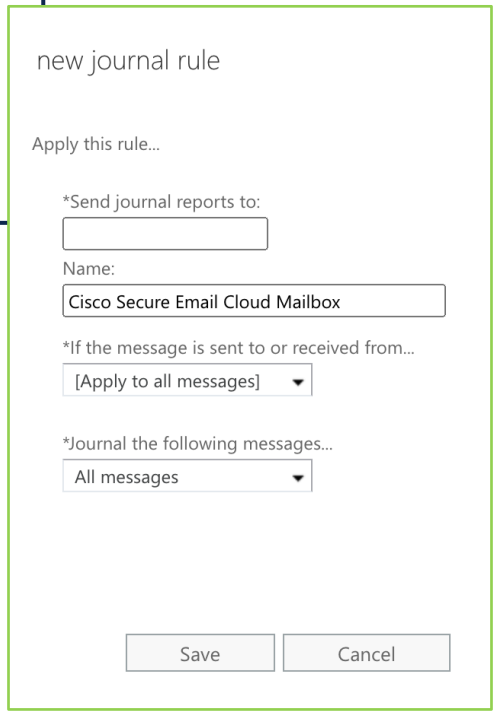
API の承認

ステップ 1



追加
ジャーナル
ルール

ステップ 2



Cloud MailboxはCloud Mailのセキュリティを補完

シンプルな管理と運用

接続の処理および
フィルタリング

DKIM 署名

ドメインのブロック/許可

受信者検証

クラウドプロバイダ

Cloud Mailboxは、管理を複雑にすることなく、既存のセキュリティ制御機能を補完します。

Cisco Secure Email パイプライン

送信者のなりすましを防げ！

詐欺メール検知（Forged Email Detection）

Business Email Compromise（BEC）対策

偽装電子メール検出

- 真の送信者アドレスの SMTP エンベロープを検査
- 送信者のアドレスと社員名簿を照合
- 偽装の可能性についてのユーザへの警告を付けて送信
- 攻撃と対応アクションのログを記録

検査前

From: Chuck chuck.robbins@mail.com
Subject: [緊急]
送金支援のお願い

SMTP エンベロープアドレスを検査

```
$ telnet mail-smtp-in.l.mail.com 25
Trying 74.125.206.26...
Connected to mail-smtp-in.l.mail.com.
Escape character is '^]'.
220 mx.mail.com ESMTP i11si22058766wmh.67 – gsmtp
HELO mail.outside.com
250 mx.mail.com at your service
MAIL FROM: adam@outside.com
250 2.1.0 OK i11si22058766wmh.67 - gsmtp
```

受信者ドメイン
送信ドメイン
実際の送信者

検査後

実際の送信者に書き換え

From: adam@outside.com
Subject: {偽装の可能性あり} [緊急]
送金支援のお願い

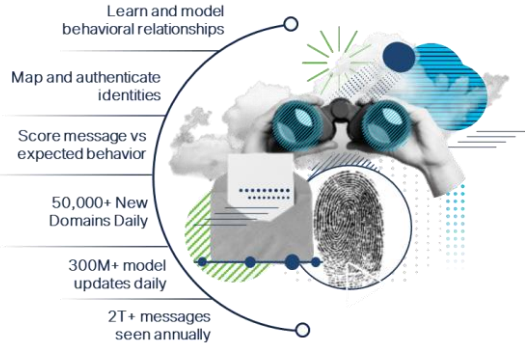
件名に警告追記

企業ディレクトリと比較

- Allison Johnson
- Barry Smith
- Chuck Robbins
- Dave Tucker

Cisco Secure Email Phishing Defense

メールの信頼度をAIと機械学習で判断（より高度な攻撃を検知）



3種のフェーズでメールを分析

- **送信元マッピング**

  送信元の情報（表示名/アドレス/ドメイン/件名など）を各パーツごとに分析し、関連性をマッピング

- **振る舞い解析**

  マッピングした送信元情報とそのメールの内容をベースに、そのメールが想定されたメールか判断。機械学習を用い、信頼できるメールを蓄積することで、より効果的に判断

- **信頼分析**

  マッピングした送信元情報と宛先の関連性を判断し、関連性が薄いメールに対しては基準値をより厳格化し、関連性が高いメールに対しては、信頼度スコアを高くするなどを実施

Phishing Defenseによる侵害されたアカウントの検知例

Message Details

Compromised Account: joe@

Trust Score 1

Authenticity Score	10.0	148.163.129.52 - (dispatch1-us1.ppe-hosted.com)
Domain Reputation	3.7	

Matched Policies:
Untrusted Messages
Compromised Account

Scoring Analysis

Compromised Account

Messages originating from a location not typically associated with th

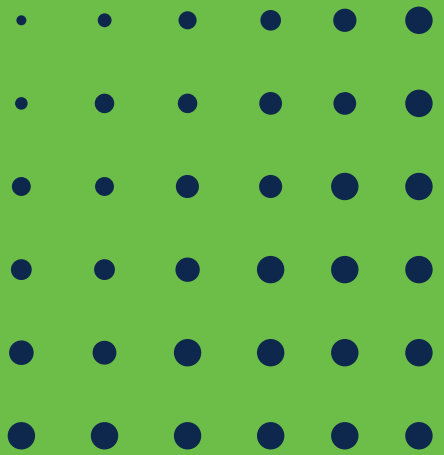
- Country of origin: Nigeria

Authenticity 10.0 Authenticity is a measure of whether the sending infrastructu
148.163.129.52 the domain.
(dispatch1-us1.ppe-hosted.com)

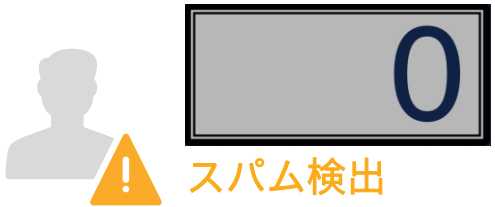
Email authentication checks:
SPF Pass Non-aligned DKIM Pass DMARC Pass

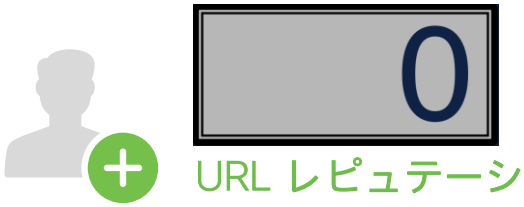
Show Less Always show more details Feedback

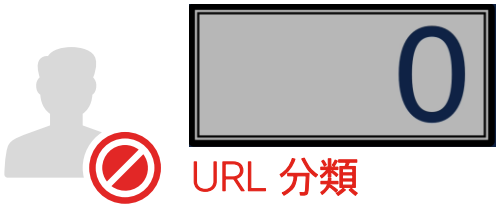
悪意のあるURLへのアクセスを防げ！

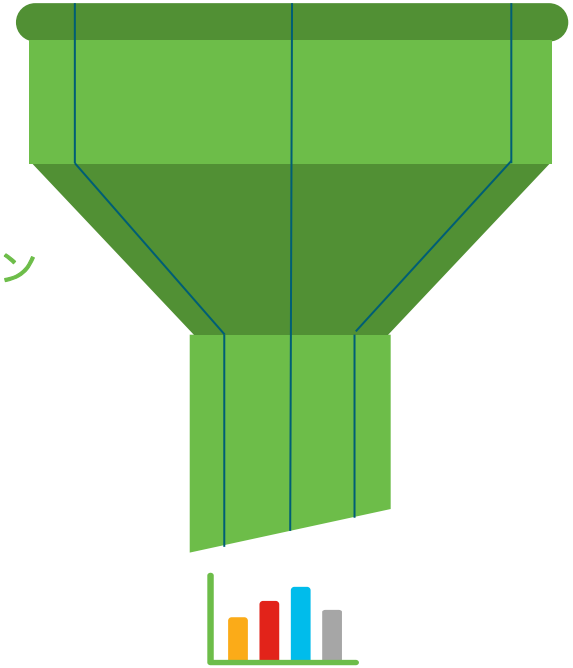


不正なURLを多層的に検出
ーURLフィルタリングー









標的型または混合型攻撃を自動的に検出
ーアウトブレイクフィルター

収集

10 万を超える組織と世界中の
電子メールトラフィックの
35% からデータをキャプチャ

検証

人間が異常を検証し、
自動生成された適応型
アウトブレイクルール

自動化

不審な URL を含むメッセージを動的に
隔離または書き換えて、きめ細かい
ルールに基づいて詳細な検査を実施

URL Rewrite (Outbreak Filters)

Instant block, do not proceed!

悪意のある
メール添付物を見抜け！

すり抜けたステルスマルウェアも遡って検出

Advanced Malware Protection（AMP）

Advanced Malware Protection

- 既知のマルウェアをブロック
- コンテキストドリブン分析でファイルを検査
- MS365のメールボックスに存在する脅威メールを自動的に削除
- ネットワークに出入りしようとしているメッセージを可視化

ファイルレピュテーション

ファジーフィンガープリンティング

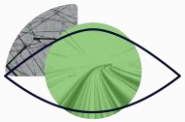
侵入の痕跡

既知のシグニチャ

ファイルサンドボックス

- 高度な分析
- 動的解析
- 846以上のインディケータ

ファイルレトロスペクション



パスワード保護された添付ファイルをスキャン！！

Password Protected File Analysis : PPFA

Supported file formats:
- アーカイブ: ZIP
- MS Office: DOC/X, PPT/X, XLS/X
- PDF

- Before PPFA

```
Fri Nov 13 19:06:44 2020 Info:   File reputation query initiating. File Name = 'malware.zip', MID = 735, File Size = 68
618 bytes, File Type = application/zip
Fri Nov 13 19:06:44 2020 Info:   Response received for file reputation query from Cache. File Name = 'malware.zip', MID
 = 735, Disposition = UNSCANNABLE, Malware = None, Analysis Score = 0, sha256 = 779dfe4503115733fd8296bb8593dd84c5a42b0
636d67c1c4723f59728ae58a0, upload_action = Recommended to send the file for analysis
Fri Nov 13 19:06:44 2020 Warning:   MID 735 reputation query failed for attachment 'malware.zip'. Extraction has failed
. Archive Error:  The file is password-protected
Fri Nov 13 19:06:44 2020 Info:   The attachment could not be scanned. File Name = 'malware.zip', MID = 735, SHA256 =779
dfe4503115733fd8296bb8593dd84c5a42b0636d67c1c4723f59728ae58a0, Unscannable Category = Message Error, Unscannable Reason
 = Archive Error:  The file is password-protected
```

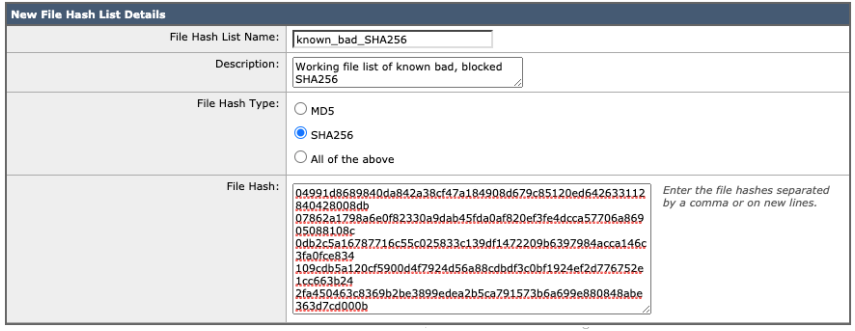
- After PPFA

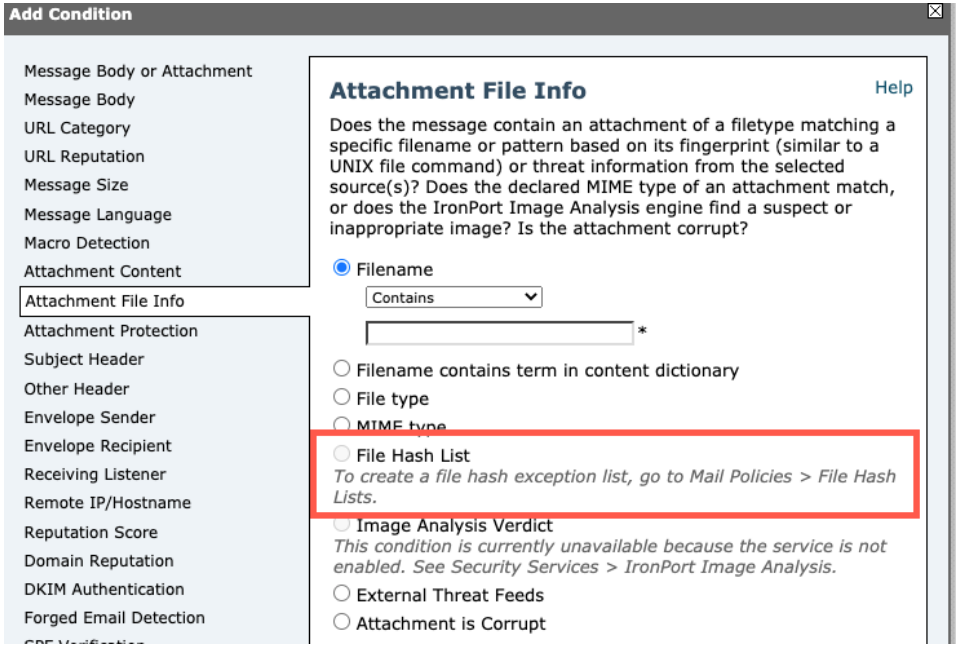
```
Fri Nov 13 19:07:42 2020 Info:   File reputation query initiating. File Name = 'malware.zip', MID = 736, File Size = 68
618 bytes, File Type = application/zip
Fri Nov 13 19:07:42 2020 Info:   Response received for file reputation query from Cache. File Name = 'malware.zip', MID
 = 736, Disposition = FILE UNKNOWN, Malware = None, Analysis Score = 0, sha256 = 779dfe4503115733fd8296bb8593dd84c5a42b
0636d67c1c4723f59728ae58a0, upload_action = Recommended to send the file for analysis
Fri Nov 13 19:07:42 2020 Info:   Compressed/Archive File: sha256 = 779dfe4503115733fd8296bb8593dd84c5a42b0636d67c1c4723
f59728ae58a0 MID = 736, Extracted File: File Name = 'malware.exe', File Type = 'application/x-dosexec', sha256 = 487906
3fd0ce8adb45c5310a8c937597957[illegible], Disposition = FILE UNKNOWN, Response received from = Cloud,
 Malware = None, Analysis Score = 0, upload_action = Recommended to send the file for analysis
Fri Nov 13 19:17:56 2020 Info:   File analysis complete. SHA256: 4879063fd0ce8adb45c5310a8c937[illegible], File name: malware.exe, Submit Timestamp: 1605323263, Update Timestamp: 1605323876, Disposition: 3, Score:
100, Analysis Id: '7aa29ee07af2317364ffeab34d6e154b', Details: W32.4879063FD0-100.SBX.TG
```

注：日本語は現状非サポート

カスタムでファイルハッシュのブラックリストを設定可！

- SHA256 (File Hash) for Filtering
  - 『添付ファイルの内容』条件及び『ファイル情報によって添付ファイルを削除』アクションにFile Hash Listオプションが追加
  - ハッシュ値が特定のSHA-256の添付ファイルに対しコンテンツフィルタ設定によるアクションを実施する際に利用可能
  - メッセージフィルタでも可能





脅威の可視性の強化と迅速なインシデントレスポンス

Cisco SecureX

無償 で利用可能! クラウドネイティブ な XDR プラットフォーム

ビルトインプラットフォーム エクスペリエンスを Cisco ポートフォリオで実現

SecureX　インテリジェンスの連携

Cisco Talos、
Cisco Threat Grid、
サードパーティの
アドバイザリ

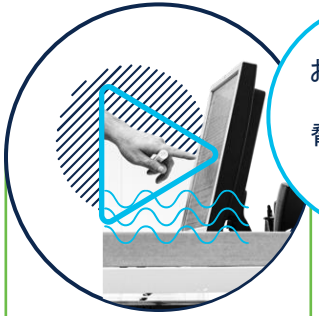
SECURE X

侵入の痕跡（IOC）

URL　IP　ホスト　SHA

Cisco Secure Email
Cloud または
Gateway

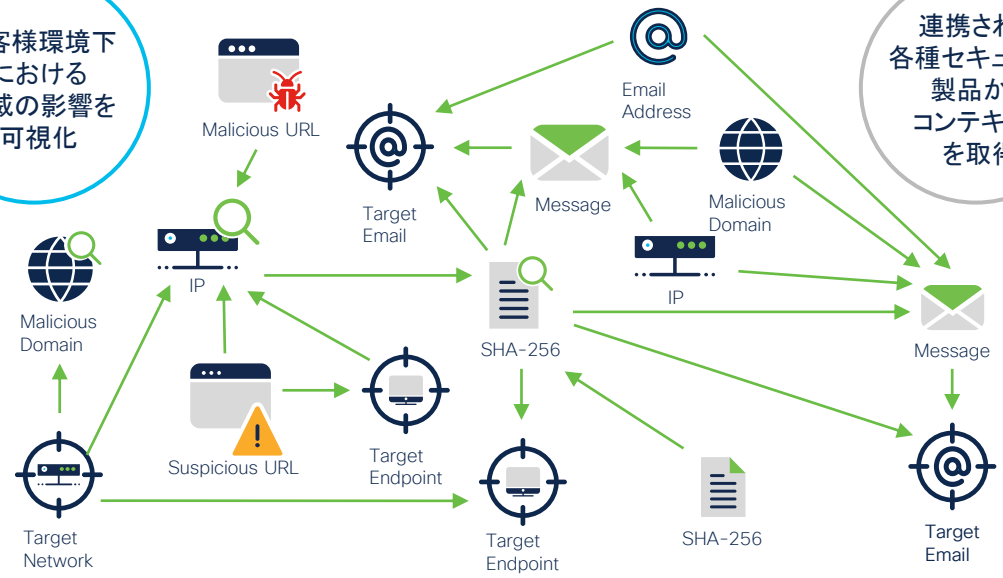
SecureX　インシデント調査



お客様環境下における脅威の影響を可視化

1クリックでブラウザコンテンツからオブザーバブルを抽出

- セキュリティブログ
- Cisco製品
- サードパーティ製品



ワークフローの自動化

連携された各種セキュリティ製品からコンテキストを取得

攻撃への対応と修復にかかる時間が85%短縮

- 対象ホストの隔離
- ファイルのブロック
- 宛先のブロック

SecureX Orchestration

コードがまったく/ほとんど不要なドラッグアンドドロップ インターフェイスによりプロセスの自動化がシンプルに

調査

ワークフローとプレイブックの自動化により、調査時間と対応時間が短縮

自動化

反復的なタスクが不要になり、MTTR が短縮されて生産性が向上するため、ミッションクリティカルなプロジェクトに注力可能

統合

独自のターンキーアプローチにより、他のシステムやソリューションと迅速に統合してツールボックスを拡張可能

拡張

際限なく拡張して常に機能する自動化により、常時同じレベルで SLA を実現

Threat Response | Investigate | Snapshots | Incidents | Intelligence | Robert Sherwin

Paste log entry, IP address, domain, etc

Investigate | Upload Snapshot | What can I search for? | on Auto Omit

Getting Started

Start by configuring integration modules in Cisco SecureX, which allows Threat Response to query your existing Cisco investments.


AMP for Endpoints


Email Security Appliance


Firepower


Orbital


SMA (Email)


SMA (Web)


Stealthwatch Enterprise


Threat Grid


Umbrella


Web Security Appliance

Don't own these products? Sign up for a free trial.

AMP for Endpoints | Email Security Appliance | Firepower | SMA (Email) | Stealthwatch Enterprise | Threat Grid | Umbrella

My First Investigation

Paste any combination of IOCs (IP, domains, SHAs, etc.) from security blogs, alerts from your SIEM, log files, and any other unstructured data. Threat Response will parse these IOCs for you! For a quick start, here are a few Cisco Talos posts - just **copy the entire set of IOCs at the end of each article:**

- Pylocky Unlocked: Cisco Talos releases PyLocky ransomware decryptor
- Fake Cisco Job Posting Targets Korean Candidates
- DNSpionage Campaign Targets Middle East

Need Help?

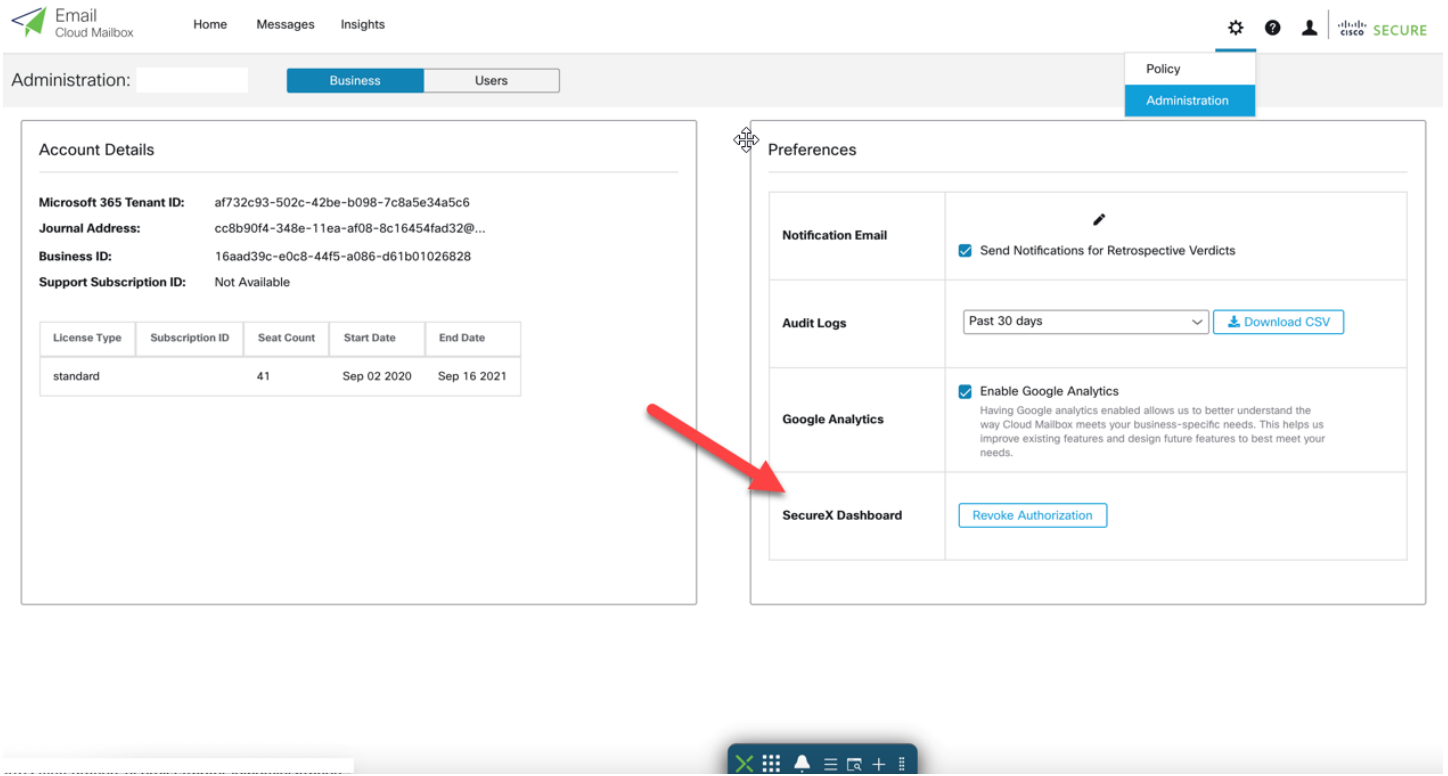
- Browse the help topics, which include definitions, FAQs, and much more
- Understand the Relations Graph with this 3-min video
- See real investigations with Threat Response with our HowTo series

Speed up your investigations with SecureX Orchestration

You can add custom response workflows into the pivot menu to seamlessly run actions and execute workflows on observables found virtually anywhere...for no additional cost! Check out this new 2 minute video to see this in action and learn how to get started with Orchestration today.


SecureX Orchestration

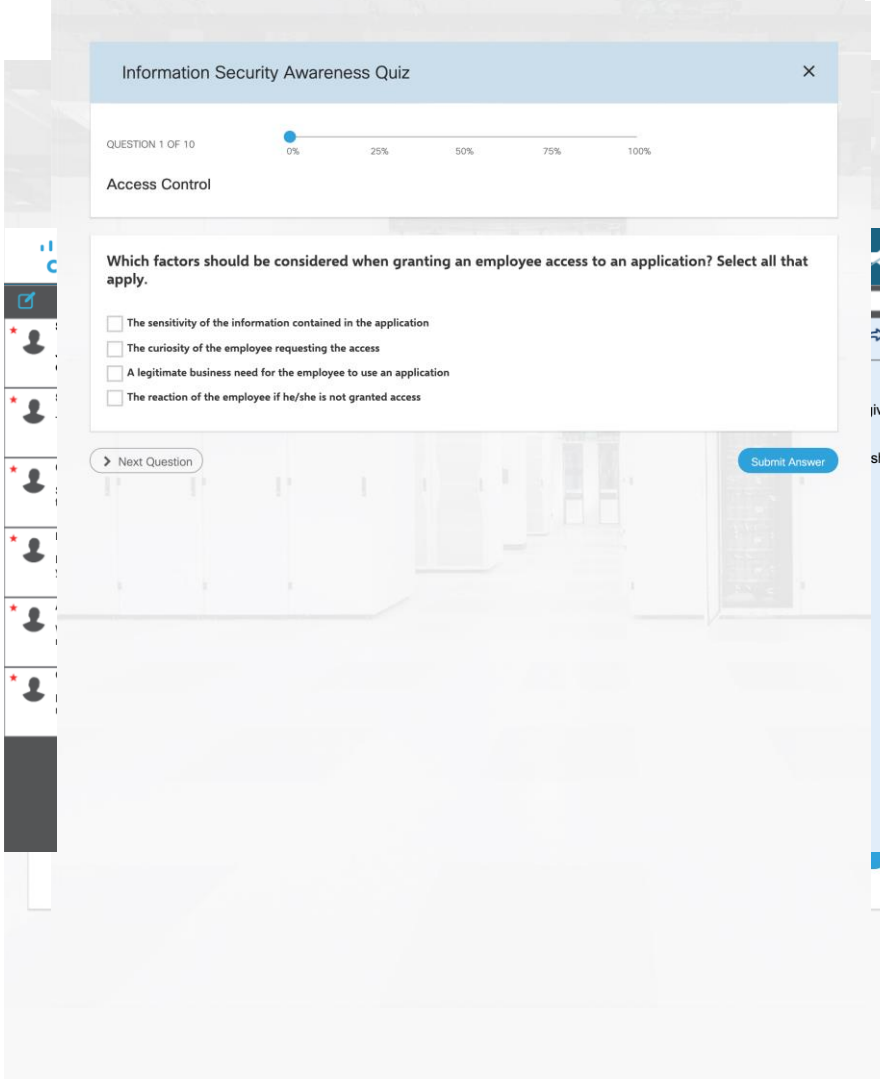
Cloud MailboxもワンクリックでSecureXと簡単連携！



ユーザのセキュリティへの意識を高める

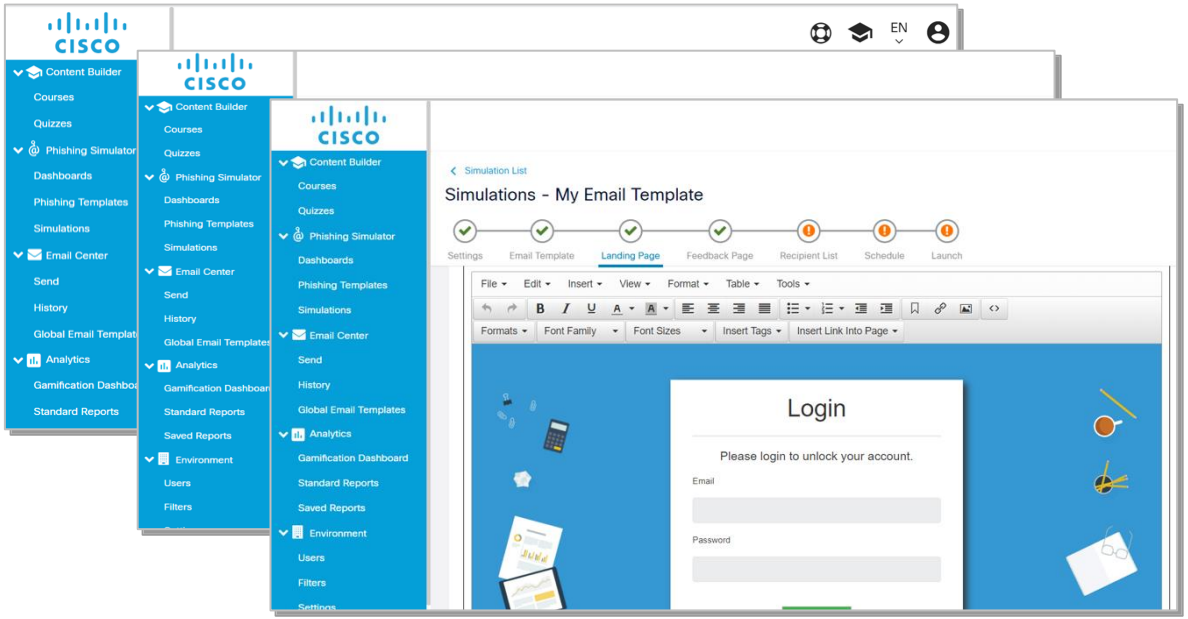
Cisco Secure Awareness Training

- 効果的なフィッシング シミュレーションや意識向上トレーニングを柔軟に行えるように必要なサポートを提供し、結果を計測してレポート
- セキュリティ運用チームがエンドユーザへの対応に追われなくなるため、リアルタイムの脅威に集中することが可能
- セキュリティトレーニングを通じてよりスマートかつ安全に働けるように従業員を教育

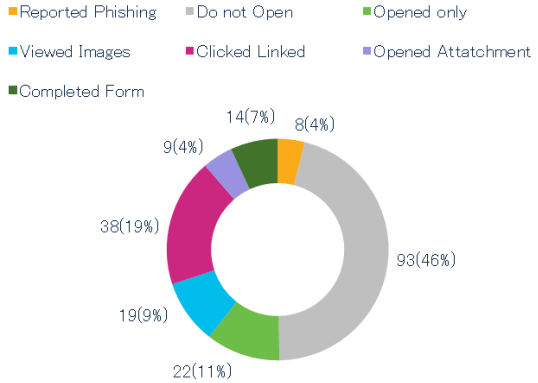


Phishing Simulation

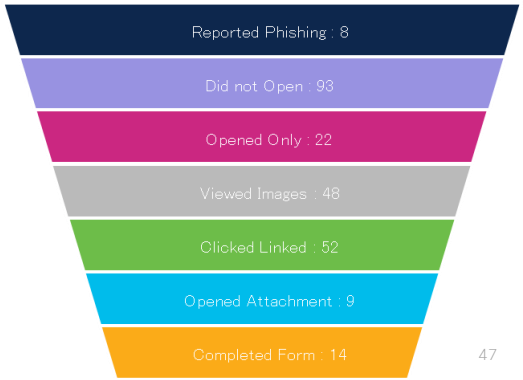
- テンプレートを使用して簡単に訓練メールを作成可能



Recipient Action Summary

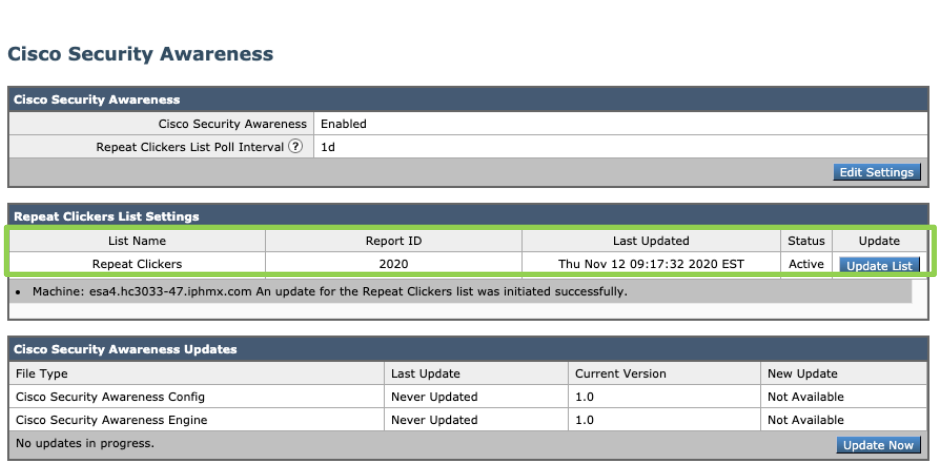


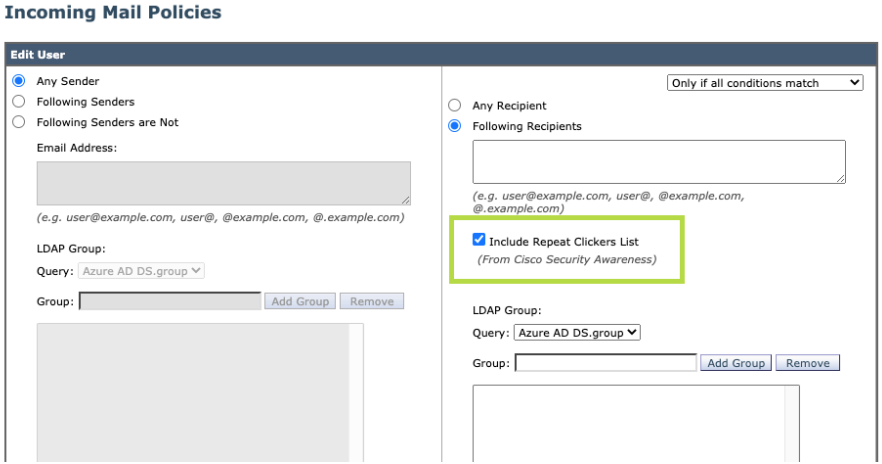
Total Action Performed



Secure Email GatewayとAwareness Trainingの統合

- Awareness Trainingはリピートクリッカーリスト（シミュレーションテストに何度も引っかかるユーザのリスト）をEmail Gatewayに提供
- Email Gatewayではリピートクリッカーリストのユーザを対象にした厳格なポリシー適用が可能
  - URLの無効化、書き換え、添付ファイルのマクロ除去、無効化（PDF化）、暗号化ファイルのブロック　など



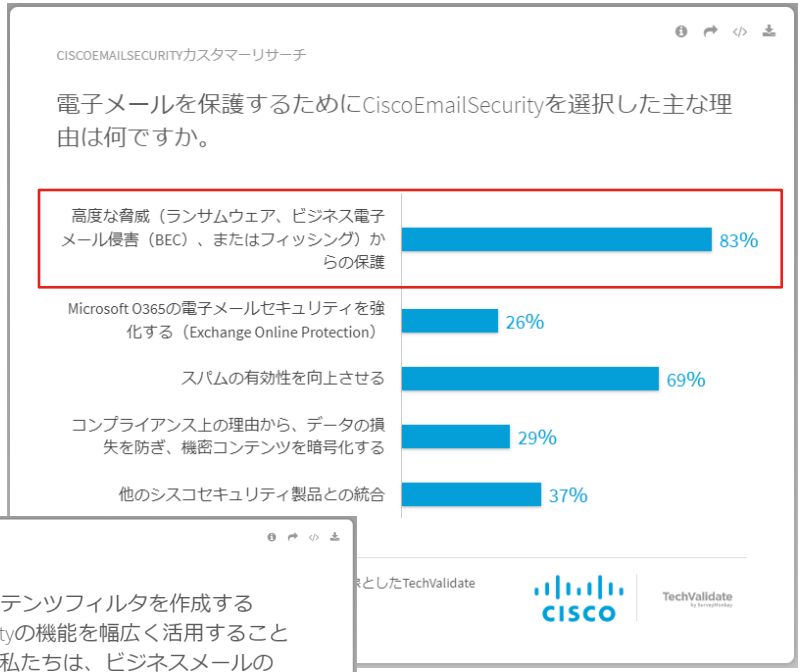


まとめとご参考情報

Key Takeaway！

- Eメールは依然として最も危険な感染ルート、
  ランサムウェアも例外ではない
- 昨今のEメールセキュリティ求められる三大対策は、
  なりすまし・URLリンク・添付ファイル
- Cisco Secure Email Gateway, Cloud Mailboxはこれら最新の脅威に基本のライセンスでしっかりと対応
- さらにPhishing Defense、SecureX（無償）、Awareness Trainingがシームレスに連携して、Eメールに関わる全ての脅威に包括的に対応

Cisco Secure Emailをご利用中のお客様の声

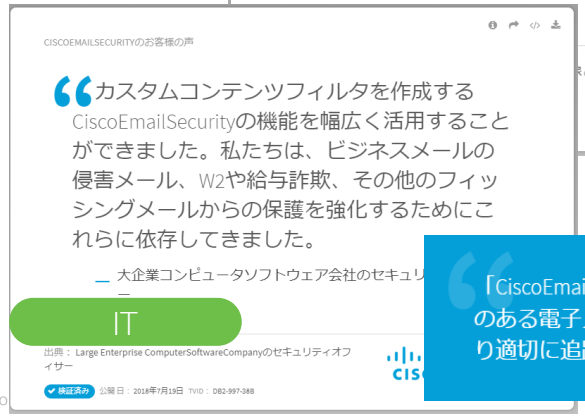


「CiscoEmailSecurityでAdvancedMalwareProtection（AMP）を導入することで、組織はステルスマルウェアから保護し、より迅速に修正することができました。」

「スパムは80%減少し、フィッシングメールはほとんどなくなりました。」

「サンドボックス環境で悪意のある添付ファイルを分析する製品の機能のために割り当てられた評価。」

製造業



IT

「CiscoEmailSecurityを使用すると、洞察を得て、スパム/悪意のある電子メールを制御できます。また、すべてのメールをより適切に追跡できるようになります。」

保険業

まずは無料トライアルをお試しください

- Cisco Secure Cloud Email Gateway　：　45日間利用可能
  - MXレコードを変更せず、既存のEmail Gateway機器からのBCCやジャーナリング送信にて容易に検証可能です（実通信への影響は御座いません！）
- Cisco Secure Cloud Mailbox　：　30日間利用可能
  - わずか5分の簡単設定
  - MS365利用中のお客様
  - モニタモードでお試し可能です（ユーザ様への実影響なし！アセスメント目的で是非！）

詳細はCisco代理店様、またはCisco担当営業まで
お気軽にお問合せください

シスコ サイバーセキュリティ

特に中堅中小企業において、
いっそう深刻化するサイバーセキュリティの問題

どこから始めたらよいのか？

誰に相談すればよいのか？

自社のセキュリティ状態がどうなっているのか？

セキュリティ対策にどのくらいの費用が必要なのか？

CISCO

サイバーセキュリティ対策
ンター

Cisco セキュリ
販売パートナー


cisco
SECURE