

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～



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

26 Mar 2021 14:00

successful cyber

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

ALICIA HOPE · APRIL 5, 2021

10NEWS

News Weather Sports Conn

← APPALACHIAN UNSOLVED LIVE AT FIVE

Share Tweet Pin it + -

One of the largest insurance firms in the U.S. CNA Fin “sophisticated cybersecurity attack” on March 21, 2021 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

TECH

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

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

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

News

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

By Ryan Gallagher | April 3, 2020

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.

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

June 16, 2020



Newsletter

Facebook Twitter LinkedIn Email



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.

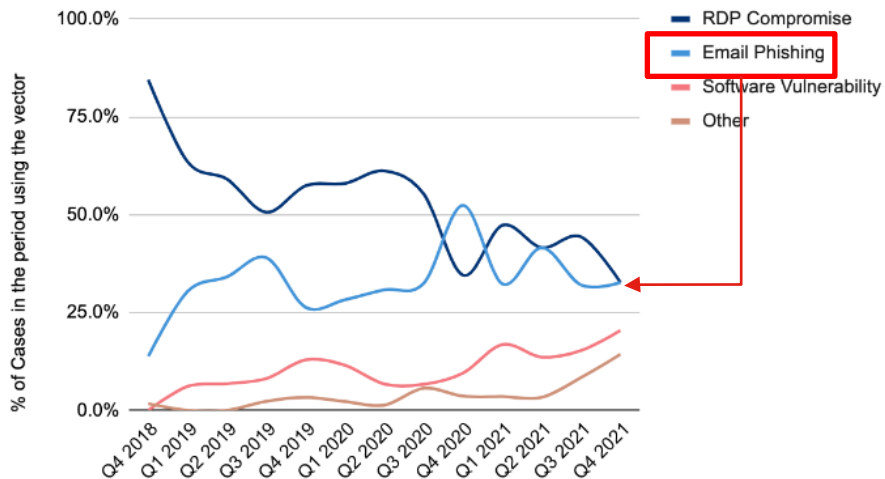
1:43 PM · Jun 8, 2020



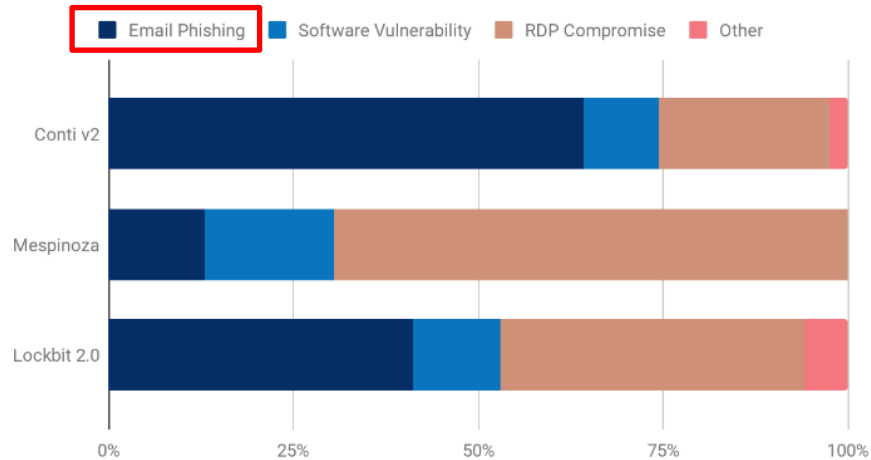
99 86 Share this Tweet

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

Ransomware Attack Vectors



Attack Vectors - Top 3 Ransomware Types

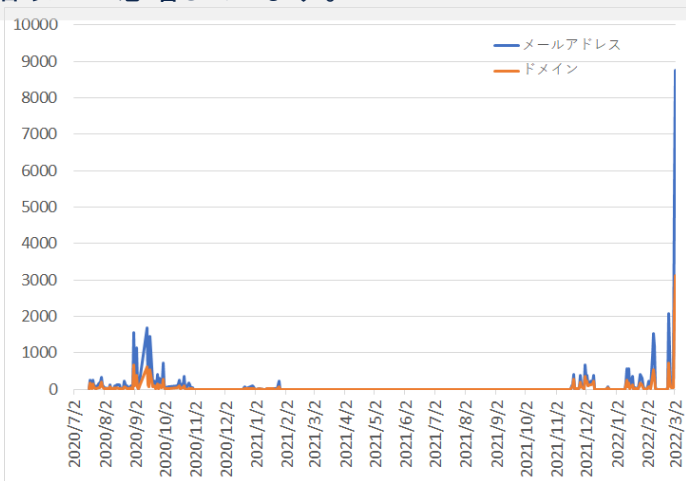


出典: <https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts>
<https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021>

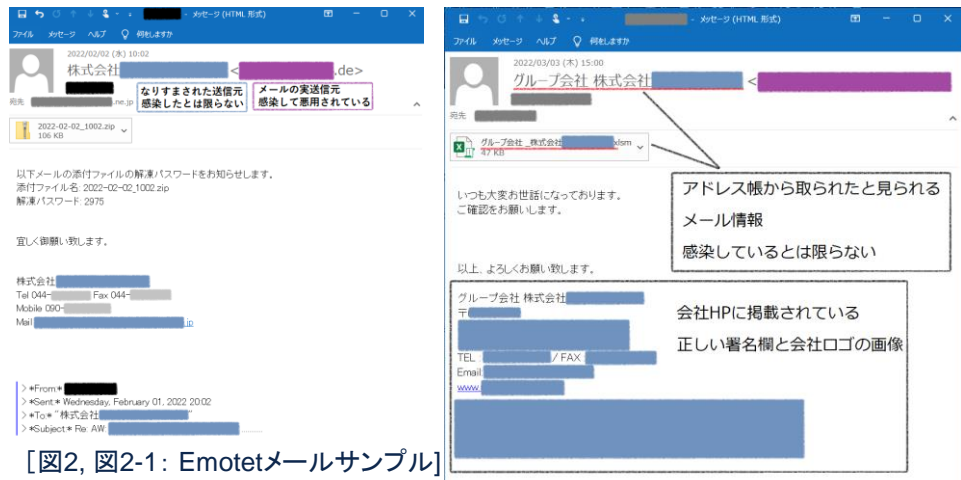
マルウェアEmotetの感染再拡大に関する注意喚起

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.jpccert.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。



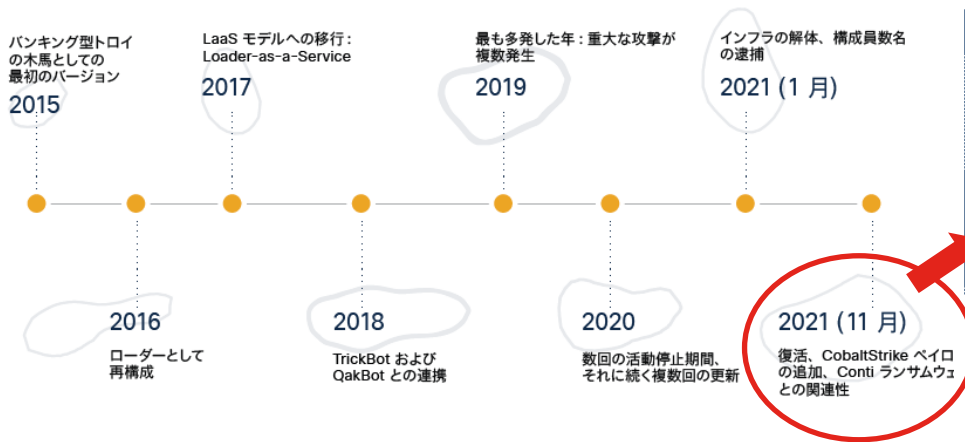
[図1: Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数の新規観測の推移 (外部からの提供観測情報) (2022年3月3日更新)]



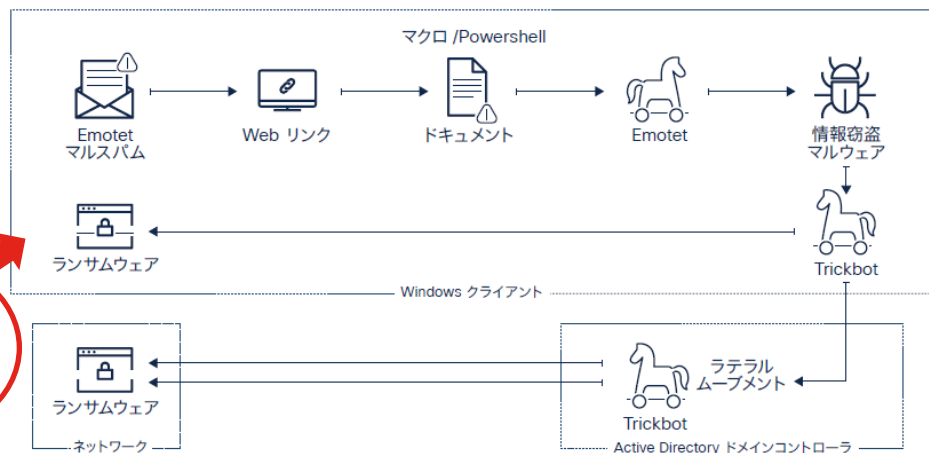
主にマクロ付きのExcelやWordファイル、あるいはこれらをパスワード付きZipファイルとしてメールに添付する形式で配信されており、ファイルを開封後にマクロを有効化する操作を実行することでEmotetの感染に繋がります。(中略)メール本文中のリンクをクリックすることで悪質なExcelやWordファイルがダウンロードされたり、アプリケーションのインストールを装いEmotet感染をねらうケースも観測しています。

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

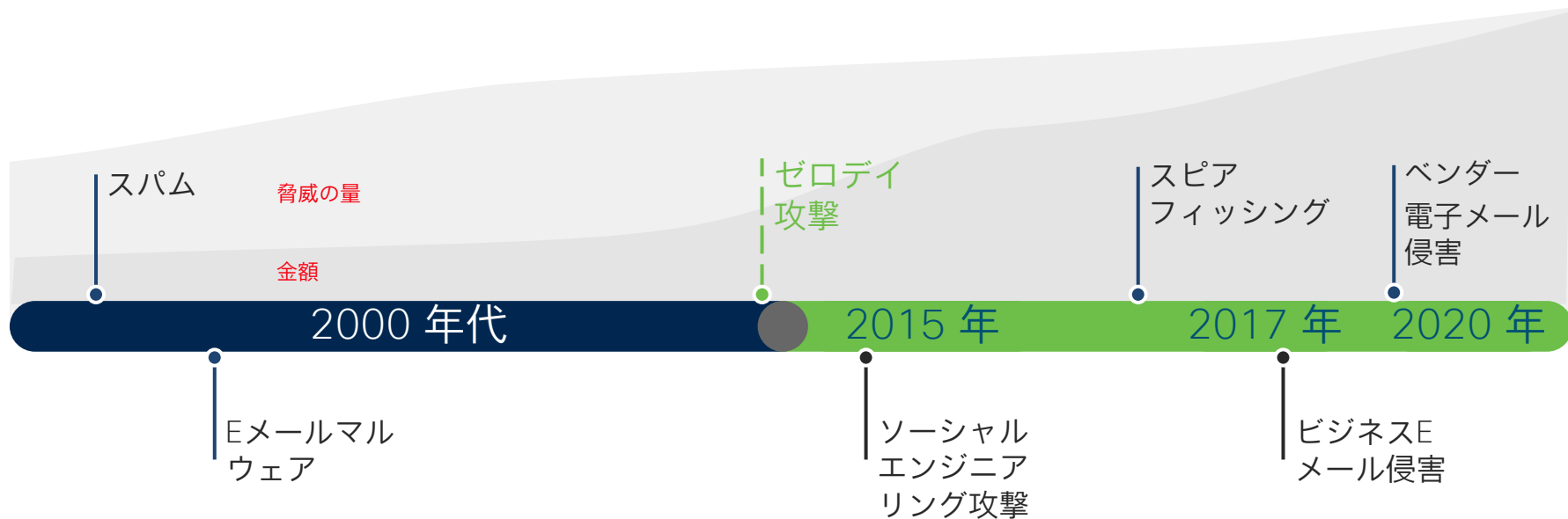
Eメールの偽装方法の理解



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

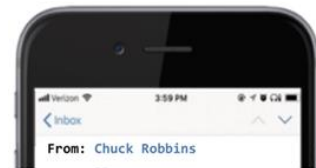
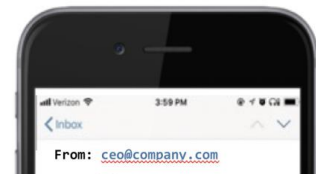
コンテンツの偽装

アイデンティティの偽装



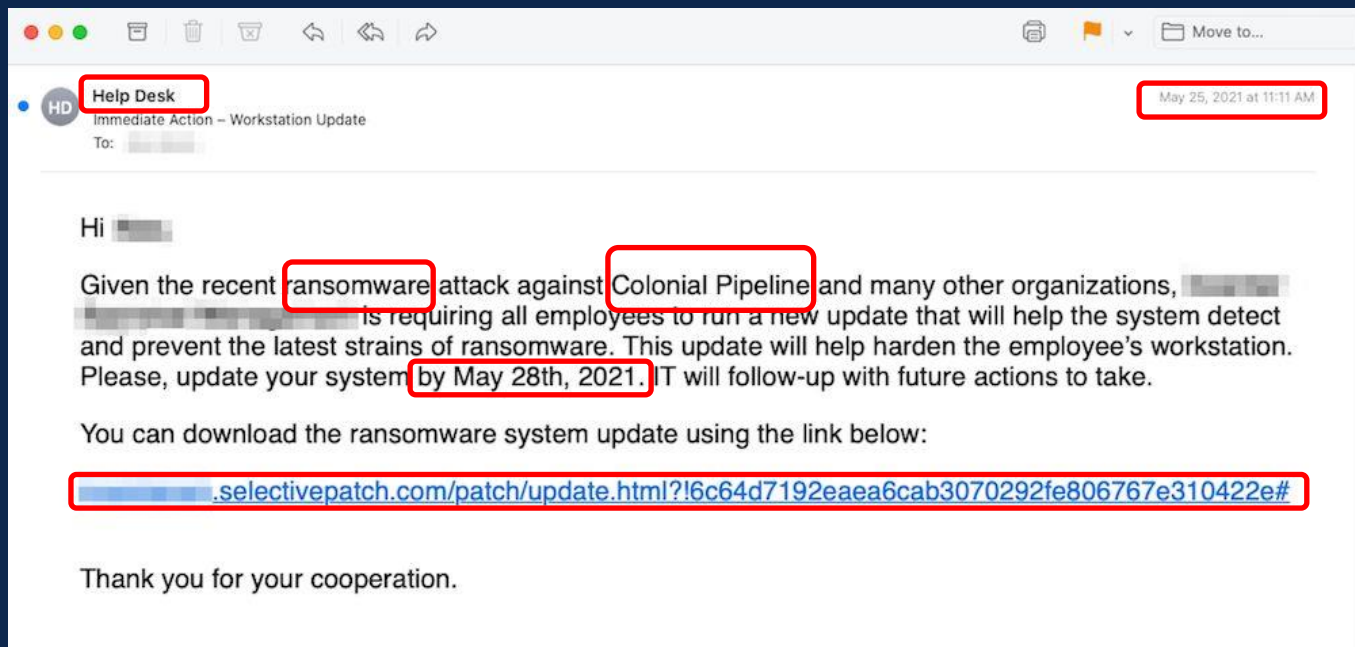
Emailなりすましのパターン

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ドレスを使用して正当なメールアドレス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

WILBER DENNISON  Today at 8:49 AM 


To: no-reply@jaeson.net
Reply-To: NoReply@uppermill.com
Copy of Invoice 95651955

Please find attached file containing your order information.

If you have any further questions regarding your invoice, please call Customer Service.

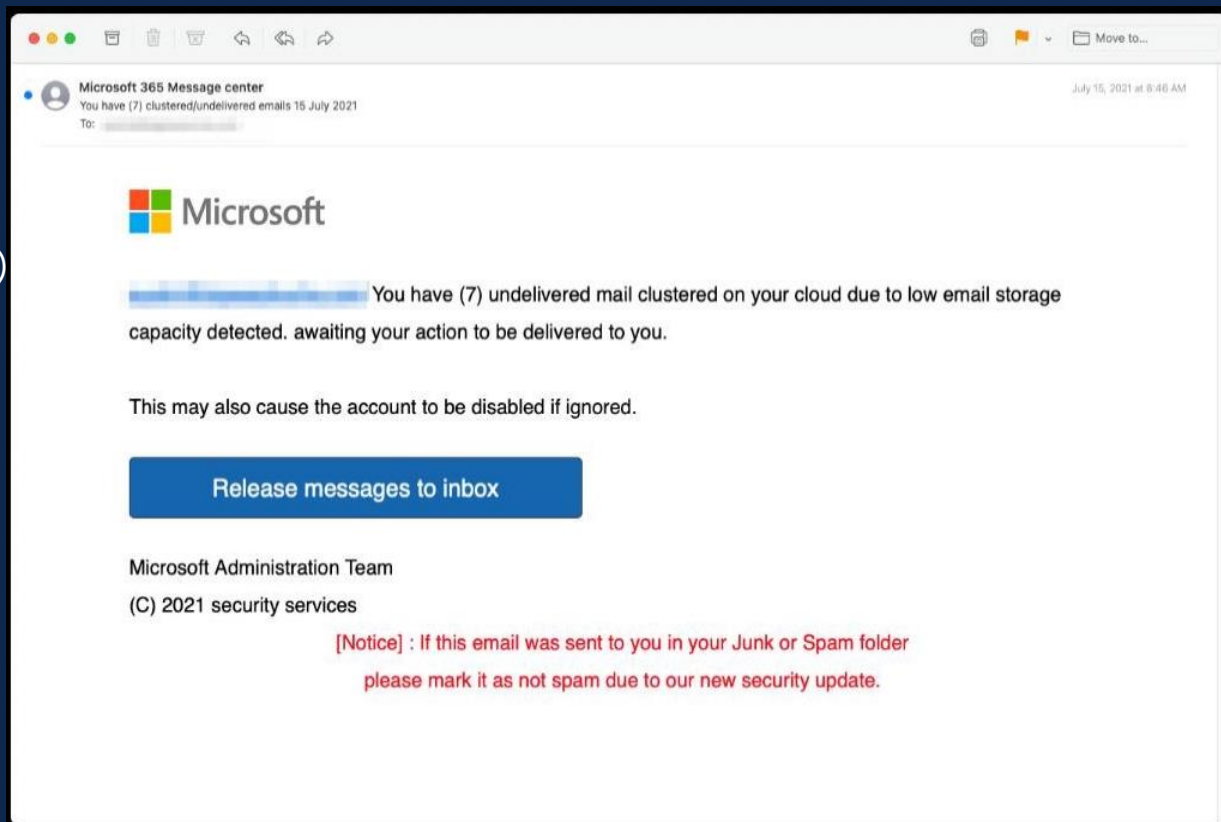
Please do not reply directly to this automatically generated e-mail message.

Thank you.
Customer Service Department


95651955.zip

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...

x +

- □ x

← → X

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！

Attack Chain

TARGET



COMPROMISE



BREACH

Recon

Stage

Launch

Exploit

Install

Callback

Persist

多層防御



- Cisco製品群
 - Duo
 - Cisco Secure Firewall
 - Kenna Security, Secure Cloud Insights
 - Cisco Secure Email
 - Umbrella
 - Cisco Secure Web Appliance
 - Cisco Threat Grid
 - Cisco AMP
 - Cisco Secure Network Analytics
 - SecureX

侵入

感染

潜伏・感染拡大

目的遂行

アカウント漏洩等による不正アクセス 対策 MFA

インターネットからの攻撃 対策 ファイアウォール / IPS

機器の脆弱性を利用した侵入・感染行為 対策 脆弱性管理

フィッシングURL, マルウェア(ダウンロード)添付メール 対策 Eメール セキュリティ

危険サイトへのアクセス, マルウェアダウンロード 対策 DNS セキュリティ

対策 Web セキュリティ

ゼロデイマルウェア 対策 サンドボックス

不正ファイルの保存・実行 対策 アンチウイルス

対策 EDR

外部との不正通信 対策 NDR

ネットワーク 対策

特権奪取による機密情報アクセス 対策 MFA

C&C通信 対策 次世代ファイアウォール

本日ご紹介するソリューション

本日ご紹介するソリューション

SIEM / SOAR

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**のクラウドサービス

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

ユーザー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



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



Permissions requested Review for your organization

This application is not published by Microsoft or your organization.

This app would like to:

- ✓ Read mail in all mailboxes
- ✓ Read organization information
- ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

ステップ 1 >



追加
ジャーナル
ルール

new journal rule

Apply this rule...

*Send journal reports to:

Name:

Cisco Secure Email Cloud Mailbox

*If the message is sent to or received from...

[Apply to all messages] ▾

*Journal the following messages...

All messages ▾

Save

Cancel

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

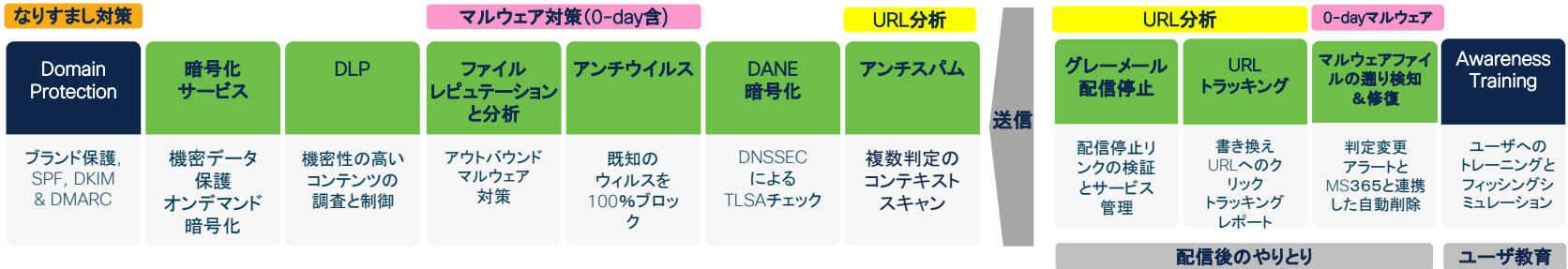
受信者検証

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。

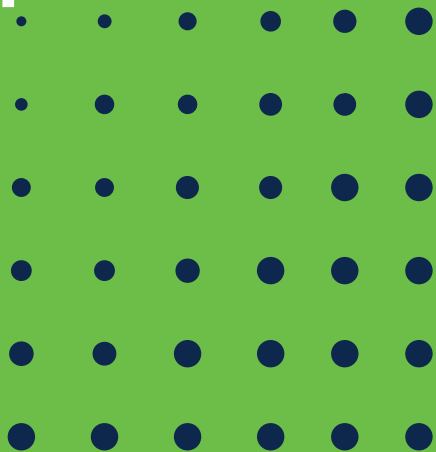
Cisco Secure Email パイプライン



- : Secure Email Gateway
- : Cloud Mailbox
- : 連携オプションサービス

SecureX : 可視性・インシデントレスポンス・ワークフロー(XDR)

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 - gsmtpp
HELO mail.outside.com
250 mx.mail.com at your service
MAIL FROM: adam@outside.com
250 2.1.0 OK i11si22058766wmh.67 - gsmtpp
```

受信者ドメイン

送信ドメイン

実際の送信者

検査後

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

実際の送信者を書き換え

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

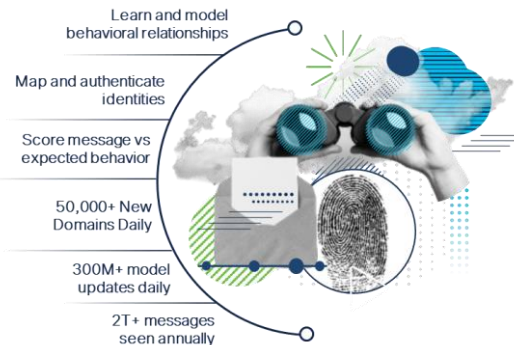
送信元の情報（表示名/アドレス/ドメイン/件名など）を各パーツごとに分析し、関連性をマッピング

- 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@ [redacted]

 Trust Score	1	
Authenticity Score	10.0	148.163.129.52 - (dispatch1-us1.ppe-hosted.com)
Domain Reputation	3.7	[redacted]

Matched Policies:
[Untrusted Messages](#)
[Compromised Account](#)

Scoring Analysis




 Compromised Account

Messages originating from a location not typically associated with the domain:

- Country of origin: Nigeria

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

Email authentication checks:

-  SPF Pass
-  Non-aligned DKIM Pass
-  DMARC Pass

Show Less

Always show more details

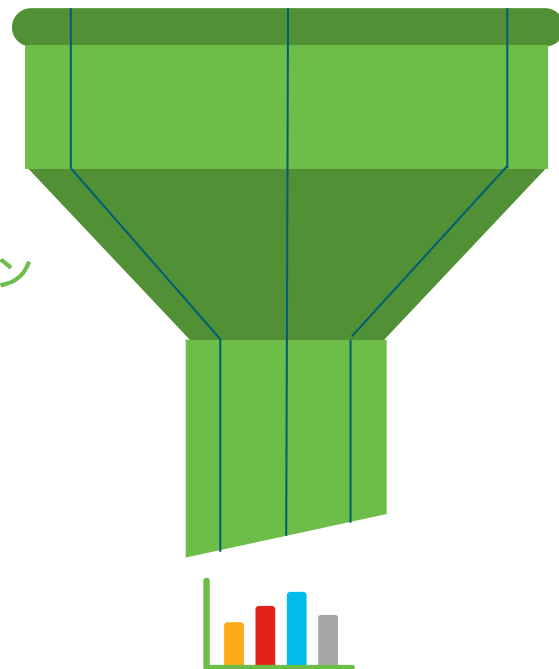
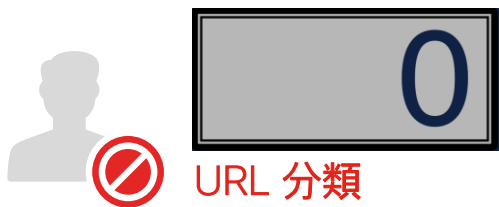
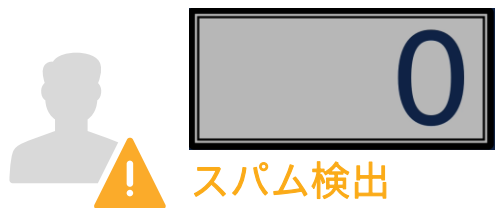
 Feedback



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 —URLフィルタリング—



標的型または混合型攻撃を自動的に検出 —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

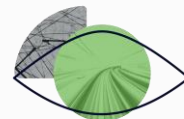
ファイルサンドボックス



- 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 = 68618 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 = 779dfe4503115733fd8296bb8593dd84c5a42b0636d67c1c4723f59728ae58a0, 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 = 779dfe4503115733fd8296bb8593dd84c5a42b0636d67c1c4723f59728ae58a0, 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 = 68618 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 = 779dfe4503115733fd8296bb8593dd84c5a42b0636d67c1c4723f59728ae58a0, upload_action = Recommended to send the file for analysis
Fri Nov 13 19:07:42 2020 Info: Compressed/Archive File: sha256 = 779dfe4503115733fd8296bb8593dd84c5a42b0636d67c1c4723f59728ae58a0 MID = 736, Extracted File: File Name = 'malware.exe', File Type = 'application/x-dosexec', sha256 = 4879063fd0ce8adb45c5310a8c9375979370be7ecc8417ba50fd0ba9aa8a8cc6, 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: 4879063fd0ce8adb45c5310a8c9375979370be7ecc8417ba50fd0ba9aa8a8cc6, File name: malware.exe, Submit Timestamp: 1605323263, Update Timestamp: 1605323876, Disposition: 3, Score: 100, Analysis Id: '7aa29ee07af2317364ffeab34d6e154b', Details: W32.4879063FD0-100.SBX.TG
```

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

New File Hash List Details	
File Hash List Name:	<input type="text" value="known_bad_SHA256"/>
Description:	<input type="text" value="Working file list of known bad, blocked SHA256"/>
File Hash Type:	<input type="radio"/> MDS <input checked="" type="radio"/> SHA256 <input type="radio"/> All of the above
File Hash:	<input type="text" value="04991d8689840da842a38cf47a184908d679c85120ed642633112840428008db07862a1798a5e0f82330a9dab45fda0af820ef3fe4dcca57206a86905088108c0db2c5a16787716c55c025833c139df1472209b6397984acca146c3fa0fce834109c0b5a120cf5900d4f7924d56a88c0bd13c0b1924ef2d726752e1cc663b242feaf59463c8369b2be3899edea2b5ca791573b6a699e880848abe363d7cd000b"/> <small>Enter the file hashes separated by a comma or on new lines.</small>

Add Condition

Message Body or Attachment
Message Body
URL Category
URL Reputation
Message Size
Message Language
Macro Detection
Attachment Content
Attachment File Info
Attachment Protection
Subject Header
Other Header
Envelope Sender
Envelope Recipient
Receiving Listener
Remote IP/Hostname
Reputation Score
Domain Reputation
DKIM Authentication
Forged Email Detection
SPF Verification

Attachment File Info [Help](#)

Does the message contain an attachment of a filetype matching a specific filename or pattern based on its fingerprint (similar to a UNIX file command) or threat information from the selected source(s)? Does the declared MIME type of an attachment match, or does the IronPort Image Analysis engine find a suspect or inappropriate image? Is the attachment corrupt?

Filename
 *

Filename contains term in content dictionary
 File type
 MIME type
 File Hash List
To create a file hash exception list, go to Mail Policies > File Hash Lists.
 Image Analysis Verdict
This condition is currently unavailable because the service is not enabled. See Security Services > IronPort Image Analysis.
 External Threat Feeds
 Attachment is Corrupt

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
アドバイザー



Cisco Secure Email
Cloud または
Gateway



SecureX インシデント調査



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

Paste log entry, IP address, domain, etc

Investigate Upload Snapshot What can I search for?

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
- DNSspionage 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！

The screenshot displays the Cisco SecureX administration interface for a Cloud Mailbox tenant. The top navigation bar includes 'Email Cloud Mailbox', 'Home', 'Messages', and 'Insights'. On the right, there are icons for settings, help, and user profile, along with the 'cisco SECURE' logo. Below the navigation, there are tabs for 'Business' and 'Users', and a 'Policy Administration' dropdown menu.

Account Details

Microsoft 365 Tenant ID: af732c93-502c-42be-b098-7c8a5e34a5c6
Journal Address: cc8b90f4-348e-11ea-af08-8c16454fad32@...
Business ID: 16aad39c-e0c8-44f5-a086-d61b01026828
Support Subscription ID: Not Available

License Type	Subscription ID	Seat Count	Start Date	End Date
standard		41	Sep 02 2020	Sep 16 2021

Preferences

- Notification Email**
 Send Notifications for Retrospective Verdicts
- Audit Logs**
Past 30 days (dropdown) [Download CSV](#)
- Google Analytics**
 Enable Google Analytics
Having Google analytics enabled allows us to better understand the way Cloud Mailbox meets your business-specific needs. This helps us improve existing features and design future features to best meet your needs.
- SecureX Dashboard**
[Revoke Authorization](#)

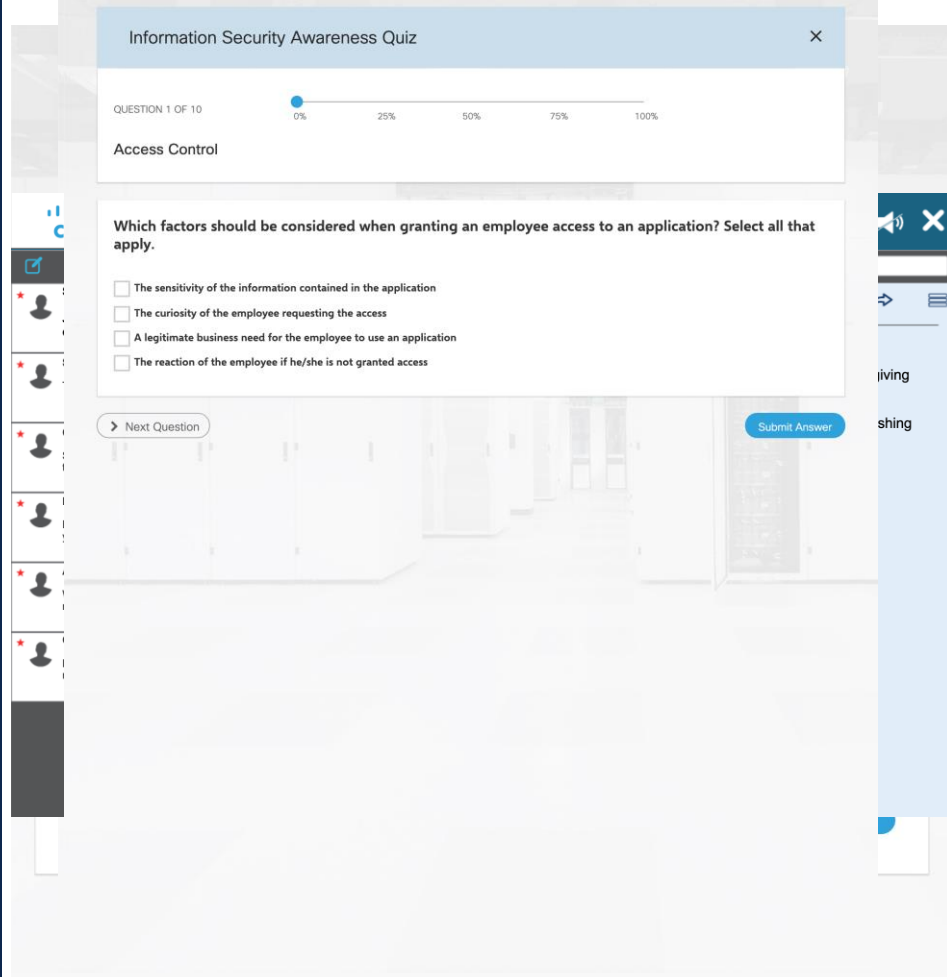
A red arrow points from the 'Account Details' section to the 'SecureX Dashboard' section in the 'Preferences' panel.

ユーザのセキュリティへの
意識を高める



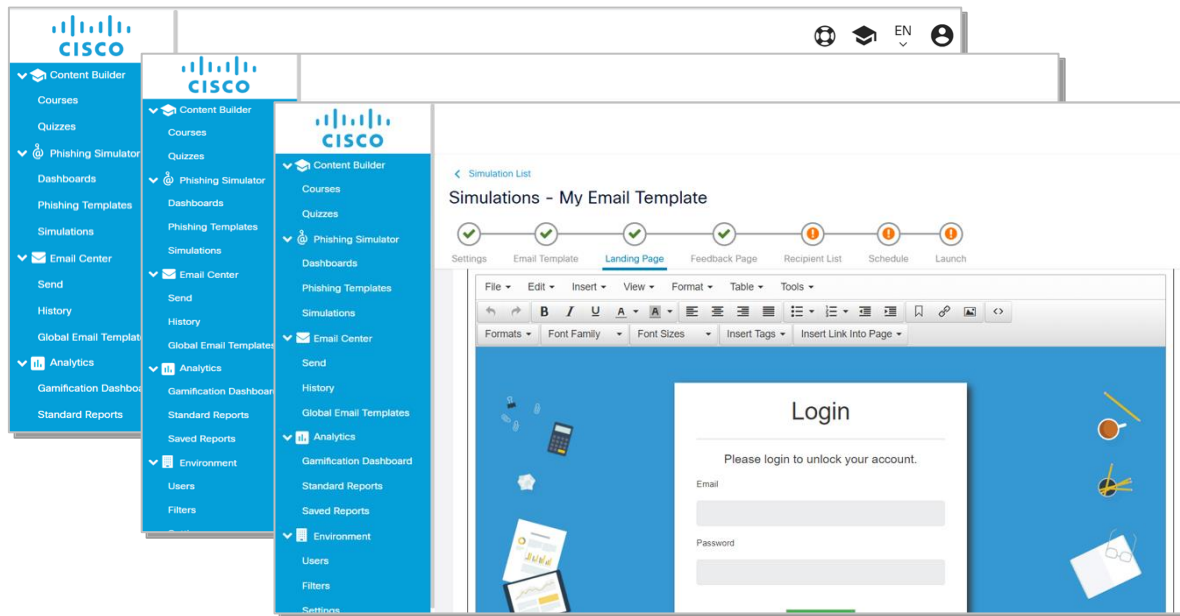
Cisco Secure Awareness Training

- 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



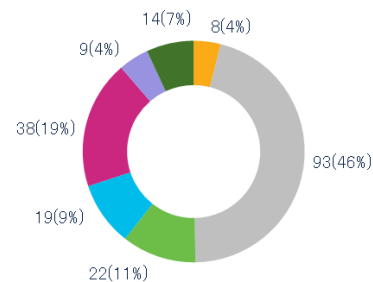
Phishing Simulation

- テンプレートを使用して簡単に訓練メールを作成可能

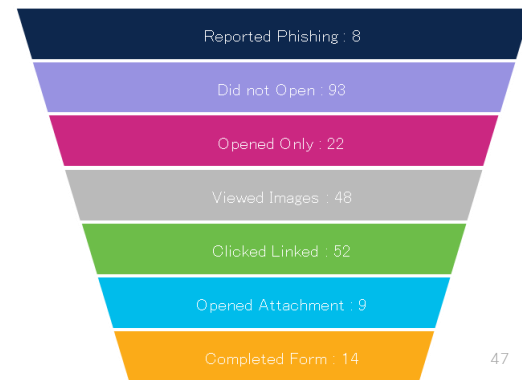


Recipient Action Summary

- Reported Phishing
- Do not Open
- Opened only
- Viewed Images
- Clicked Linked
- Opened Attachment
- Completed Form



Total Action Performed



Secure Email GatewayとAwareness Trainingの統合

- Awareness Trainingはレポ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ではレポ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

Cisco Security Awareness

Cisco Security Awareness	
Cisco Security Awareness	Enabled
Repeat Clickers List Poll Interval ?	1d
Edit Settings	

Repeat Clickers List Settings

List Name	Report ID	Last Updated	Status	Update
Repeat Clickers	2020	Thu Nov 12 09:17:32 2020 EST	Active	Update List
Machine: esa4.hc3033-47.iphmx.com An update for the Repeat Clickers list was initiated successfully.				

Cisco Security Awareness Updates

File Type	Last Update	Current Version	New Update
Cisco Security Awareness Config	Never Updated	1.0	Not Available
Cisco Security Awareness Engine	Never Updated	1.0	Not Available
No updates in progress. Update Now			

Incoming Mail Policies

Edit User

Any Sender
 Following Senders
 Following Senders are Not

Email Address:

(e.g. user@example.com, user@, @example.com, @.example.com)

LDAP Group:
Query: Azure AD DS.group

Group: [Add Group](#) [Remove](#)

Any Recipient
 Following Recipients

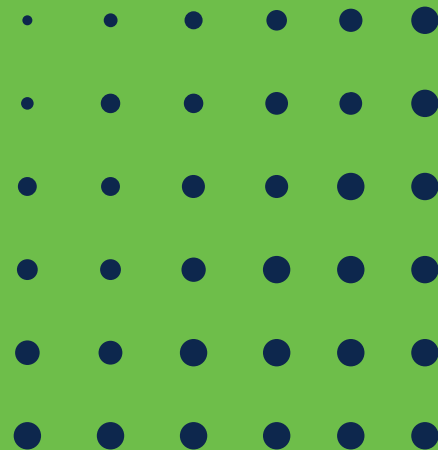
(e.g. user@example.com, user@, @example.com, @.example.com)

Include Repeat Clickers List
(From Cisco Security Awareness)

LDAP Group:
Query: Azure AD DS.group

Group: [Add Group](#) [Remove](#)

まとめとご参考情報



Key Takeaway !



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

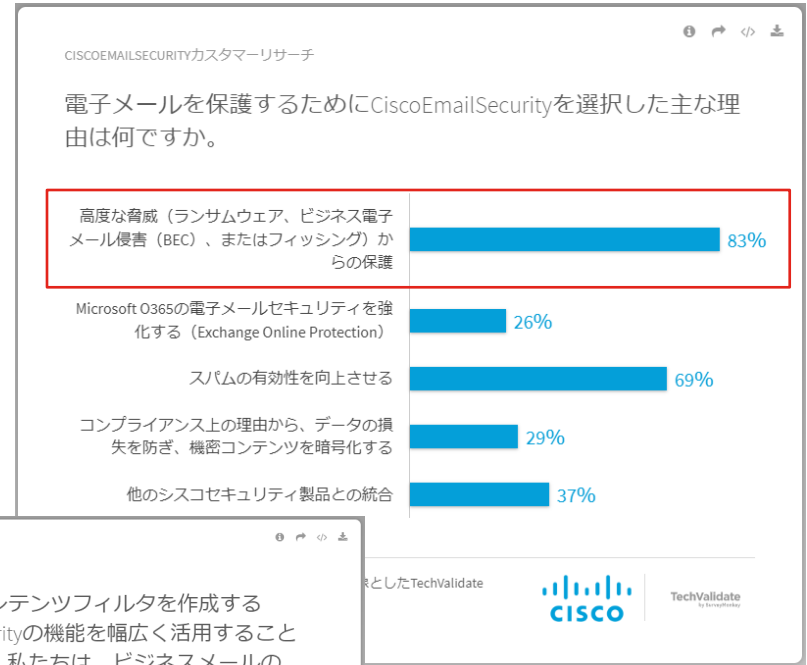


Cisco Secure Email Gateway, Cloud Mailboxはこれら最新の脅
威に**基本のライセンス**でしっかりと対応



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

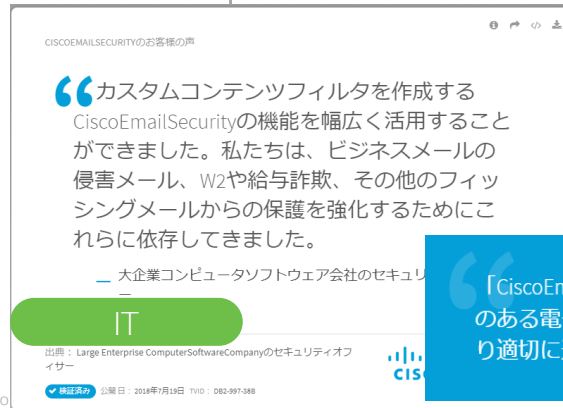


「CiscoEmailSecurityでAdvancedMalwareProtection（AMP）を導入することで、組織はステルスマルウェアから保護し、より迅速に修正することができました。」

「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



「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下さい

- 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？



サイバーセキュリティ対策
センター



Cisco セキュリ
ティ 販売パートナー

企業規模に関わらずサイバーセキュリティ対策の重要性がますます高ま
ってきており、中でも中堅中小企業はかつてないほどのサイバー攻撃の脅威
にさらされ、サイバーセキュリティの問題が一層深刻化しています。

シスコは、中堅中小企業を主な対象として、あらゆる角度でセキュリティに
関する課題を支援するための、サイバーセキュリティ対策支援セン
ターを設けました。

[お申し込みはこちら](#)



[支援内容](#) [申請フォーム](#) [製品](#)

支援内容

- サイバーセキュリティ対策ご相談受付
- サイバーセキュリティ対策指南ガイドの提供
- 専門家によるセキュリティ対策セミナー
- シスコセキュリティソフトウェア 無償トライアル提供 ※
- セキュリティに特化した販売パートナーの紹介
- 販売パートナーと連携したセキュリティヘルスチェック提供（一部有償）、対策費用見積りのお見積り

*支援提供について：シスコシステムズ合同会社による提供を原則といたしますが、シスコ販売パートナー企業からの提供となる場合もあります。

*無償トライアル提供製品：Cisco Umbrella, Cisco Secure Access by Duo, Cisco Secure Endpoint, Cisco Secure Email

*保守およびサポートについて：無料トライアル期間中の保守サポートは原則提供いたしません。利用ガイドをご覧ください。

ご相談・お申し込み

- 平日の日中に連絡のつきやすい電話番号のご入力をお願いします。
- 弊社のパートナー企業からご連絡する場合があります。あらかじめご了承ください。

【個人情報取り扱い】を必ずご確認の上、必要事項をご入力ください
*ご入力が必要な項目です

メールアドレス*

所在地*

選択してください

正式会社名*

姓*

名*

役職*

電話番号*

ご希望の最新鋭の情報を選択して、下記の欄にご記入ください*

- 資料のダウンロードがほしい
- 最新のヘルスチェックを実施する
- 多要素認証(MFA)について知りたい
- メールセキュリティ対策を強化したい



SECURE