Infinity Portal 操作方法

目次

[OVERVIEW 2](#_Toc117860526)

[EVENTS 7](#_Toc117860527)

[POLICY 18](#_Toc117860528)

[MAIL EXPLORER 26](#_Toc117860529)

[ANALYTICS & REPORTS 28](#_Toc117860530)

[USER INTERACTION 40](#_Toc117860531)

[AUDIT 47](#_Toc117860532)

[CONFIG 49](#_Toc117860533)

OVERVIEW

Infinity Portalへログイン後、最初に表示される画面です。

Harmony Email & Collaborationがお客様のメール環境で検知した有害なメールの件数や、その概要を確認できます。

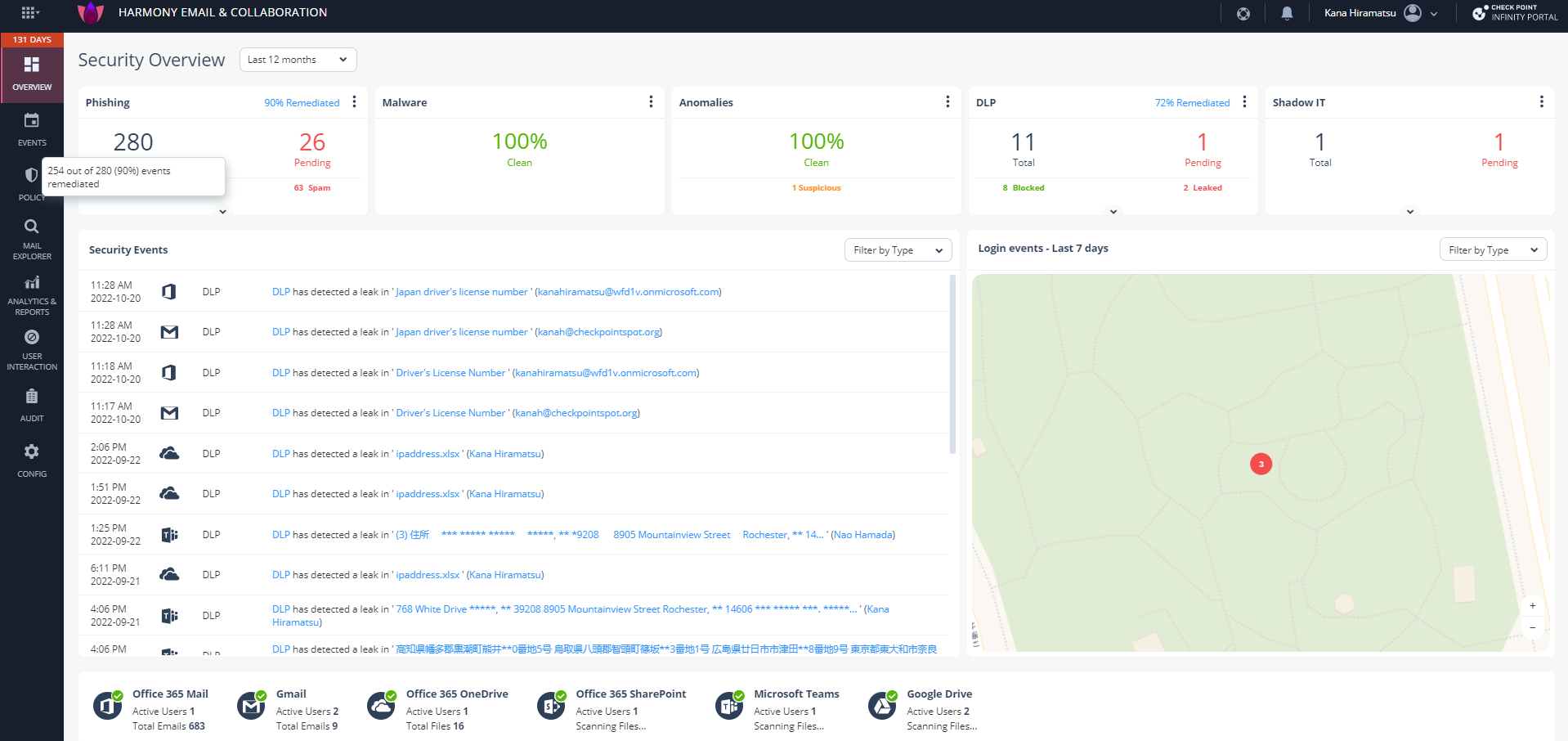
このOverviewは１分毎に自動更新されます。

1. 表示期間
2. Security Event
3. Phishing
4. Malware
5. Anomalies
6. DLP
7. Shadow IT

⑧Login events

1. 連携中の

SaaS一覧



■画面構成

1. 表示期間：

過去24時間、7日、30日、12カ月のなかから、Over viewに表示する期間を変更できます。

1. Phishing：期間中に検知された全てのフィッシング件数を表示します。

隔離などの対応をしていないメールがある場合、右側に赤字でPending件数として表示されます。

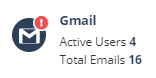
全てのフィッシング件数の下部には橙色の文字でsuspiciousイベント（Phishingと断定出来ないが、有害と疑われるイベント）の件数が表示されます（フィッシング件数には含まれていません）。

Phishing / Suspiciousイベントの振り分け基準は、Configタブより設定可能です。詳細手順は“Config”の項目をご参照ください。

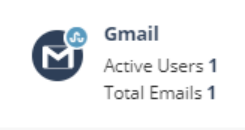
1. Malware：指定した期間中に検知されたマルウェアの件数を表示します。
2. Anomalies：普段とは異なる動きを検知をカウントします。普段とは異なる国からのメール受信、普段より数が多い受信者、脆弱性のあるブラウザの使用等の件数を表示します。
3. DLP：Configから定義したデータ型のデータ漏洩が検知された場合に表示されます。
4. Shadow IT: クラウドアプリケーションからユーザーへの、クラウドアプリケーションの利用を示唆するメールを特定します。例えば、「登録ありがとうございます」「通知が来ています」などのメッセージを含むメールは、ユーザーがクラウドアプリケーションを使用しているものと判断されます。このようなメールがメールボックスで見つかると、Shadow ITとしてセキュリティイベントが作成されます。
5. Security Events：直近で検知したフィッシング、マルウェア、Anomalies、DLP、Shadow ITを表示します。枠内右上のプルダウンメニューから、検知された脅威の種類を選択し、絞り込むことが可能です。この項目では、検知されたイベントに加え、隔離が実施されたイベントも一覧に表示されます。
6. Login events：アプリケーション毎にログインが実施された場所や、ログインの成功・失敗をマップ上で確認できます。
7. Harmony Email & Collaborationと連携されているSaaSアプリケーション一覧

緑のチェック= 正常に連携

赤いマーク= 連携エラーなので再度オンボーディングを実施する必要がある



青いマーク= オンボーディング直後でまだLearning Modeが走っている状態



■②～⑥に表示されるステータス表記について

* Clean: 正常であることを表す
* Remediated:セキュリティイベントが検知され、必要な対応が実施されたことを表す(手動での隔離、自動隔離）
* Pending:セキュリティイベントが検知され、それに対するアクションが未実施の状態を表す（対応方法については、p.4の「■セキュリティイベントへの対処」、ならびにp.7のEvent項目内「⑤Group Actions」をご参照ください）

■主な使い方

管理者は⑦Security Eventの内容を確認し、各メールを手動で隔離したり、Dismiss（イベントの無視）等の必要なアクションを実施して頂くことが可能です。②Phishingや⑥Shadow ITの各数字を押下すると、Event タブに遷移し、数字の内訳（セキュリティイベント一覧）を確認できます。

■セキュリティイベントへの対処

メールタイトルを押下すると、下図のようなメール詳細画面が表示されます。これは、まだPending 状態で何もアクションされていません。

この場合、「Quarantine Email」の黒いボタンを押下することで即時にメールが隔離されます。

※Detectモードでも手動での隔離が実行可能です。

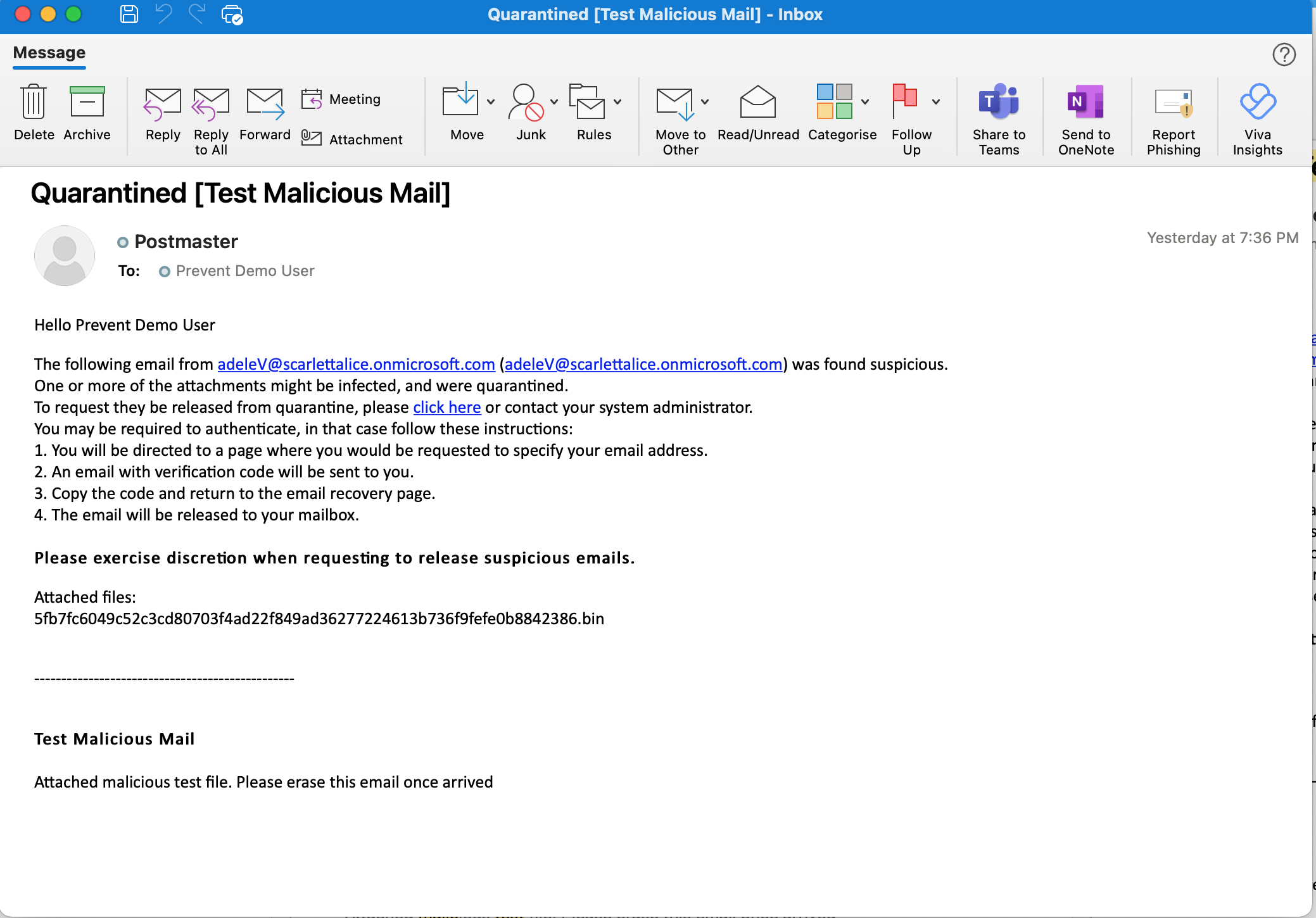


Quarantine Emailボタン

ン

「Quarantine Email」を実行すると、このメールを受信したユーザーのメールボックスからメールの隔離が実施された後、ユーザーに隔離された旨を通知するメール（「Quarantined [オリジナルメールの件名]」）が届きます。ユーザーは、そのメールをリストアしたい場合、ユーザー側で本通知メール内の‘Click Here’ボタンからリストア申請をします。その申請によって管理者へリクエストの通知メールが送信され、Infinity Portal上（User Interaction > Restore Requests）でリクエスト申請済みのメール一覧を確認できます。

・隔離された通知メール



Click hereボタン

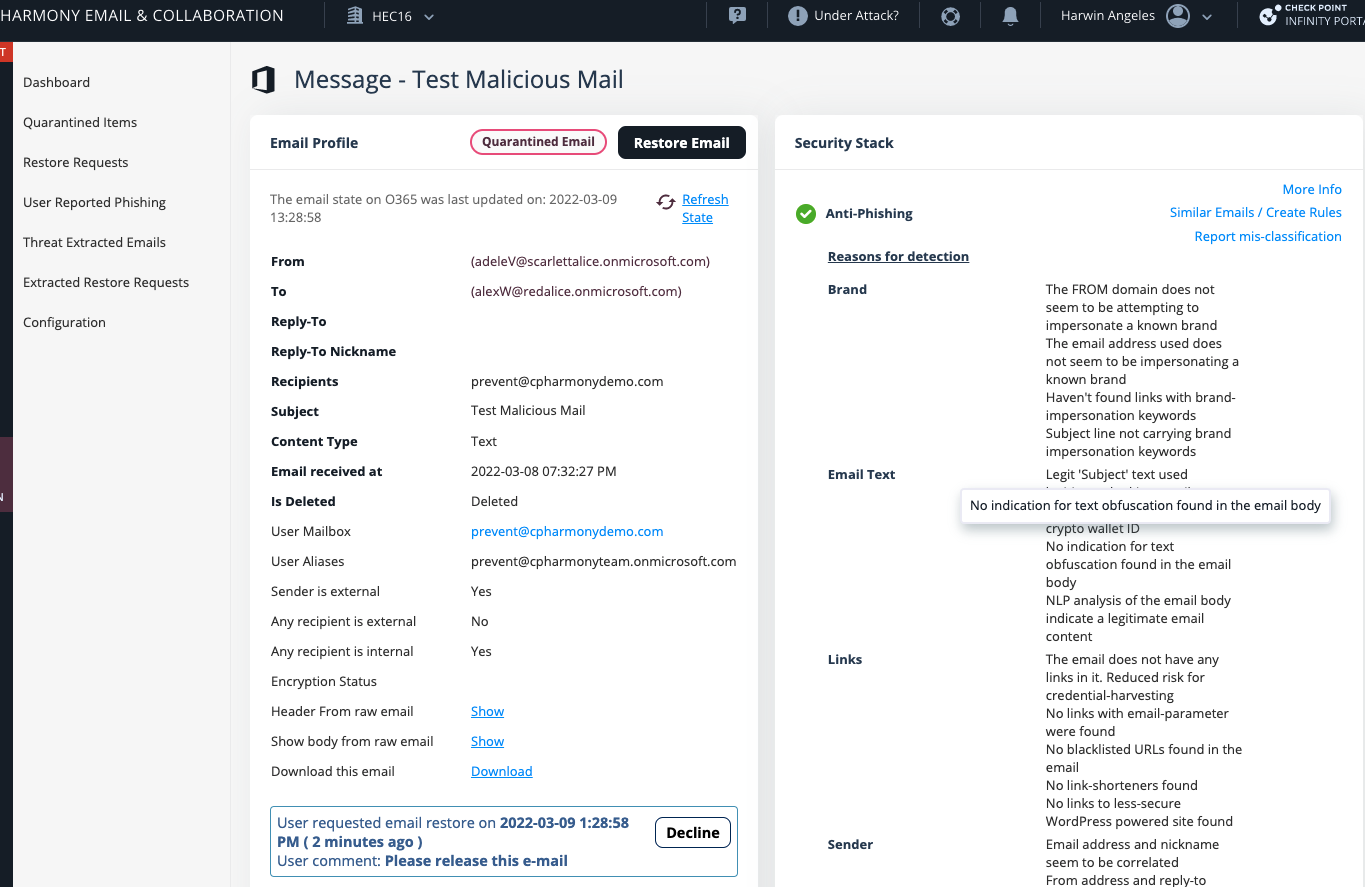
・管理者へ届くリストア申請リクエストメール

Graphical user interface, text, application, email

Description automatically generated

下記画像では、ピンクの枠線で囲まれている”Quarantined Email”と表示されており、このメールが既に隔離されていることを示しています。この画面上でリストアを許可する場合は画面上部のRestore Emailのボタン

を押下します。拒否する場合は画面下部のDeclineボタンを押下し、拒否理由を入力することで、ユーザーの申請を拒否します。



ピンクの枠線で囲まれたQuarantined Email。隔離済みであることを示しています。

Restore Emailボタン

Declineボタン

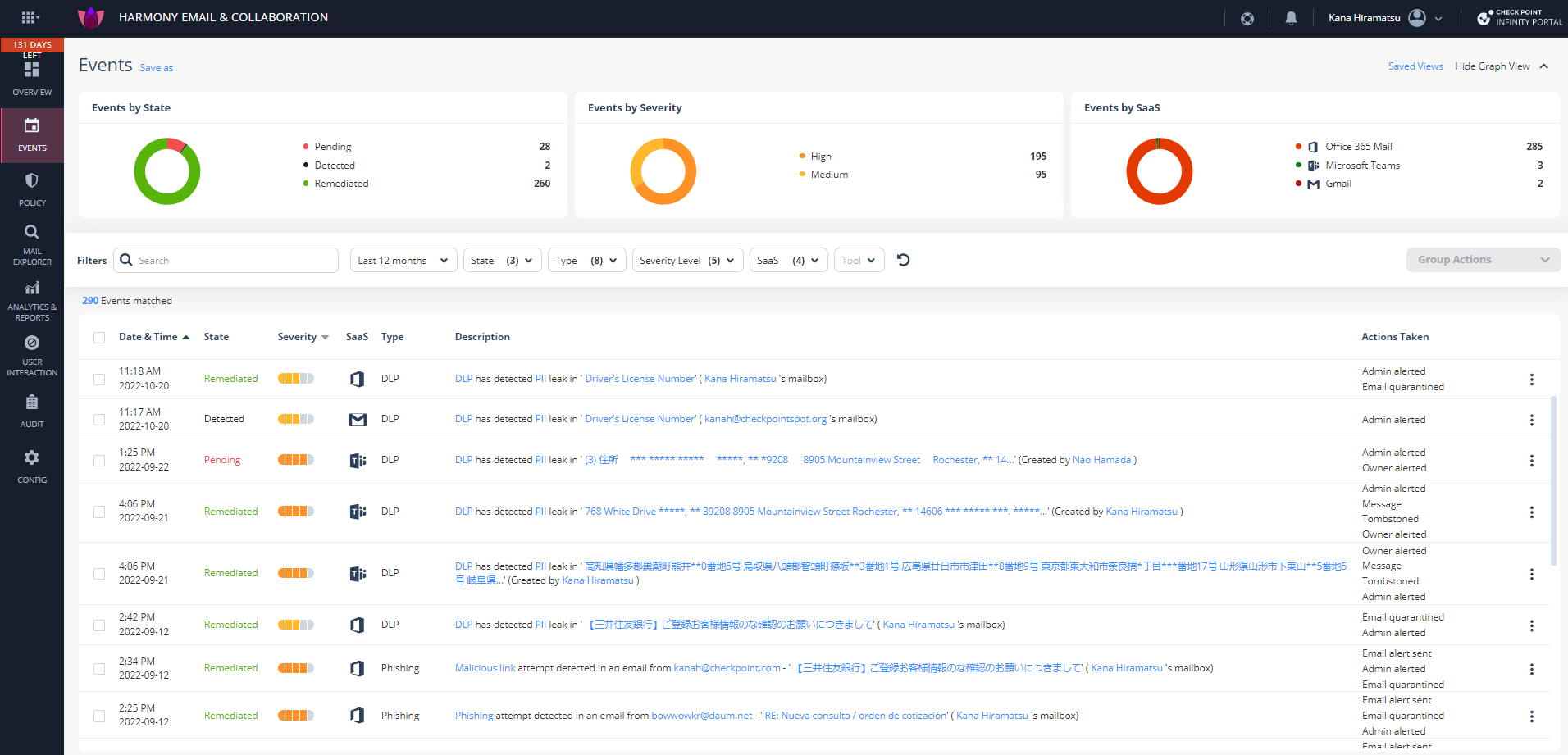
Quarantine（メール隔離）の他にも、Dismiss（セキュリティイベントの無視）、ユーザーへの通知、スパムへの移動、フィッシングではないとレポートする（過検知報告）が可能です。

詳細はp.7のEvent項目内の「⑤Group Actions」をご参照ください

# EVENTS

Eventsでは、有害なものとして検知されたメールの検索や絞り込みが可能です。

受信者や送信者、検知理由、攻撃の種類といった情報を確認できます。



1. Filters

⑤Group Actions

1. Events by SaaS
2. Events by Severity
3. Events by State

⑥Events matched (検索結果)

■画面構成

① Events by State：Eventとして検知されたメールについて、対応状況ごとに内訳を表示します。

* Pending:セキュリティイベントが検知され、それに対するアクションが未実施の状態を表す。
* Detected:外部向けの送信においてセキュリティイベントが検知されたものを表す。
* Remediated: セキュリティイベントが検知され、必要な対応が実施されたことを表す(手動での隔離、自動隔離）

② Events by Severity：Eventとして検知されたメールについて、重大度ごとに内訳を表示します。複数のセキュリティエンジンを活用し、総合的に判断した結果を、Critical、High、Medium、Low、Lowestの５段階の基準で評価しています。

③ Events by SaaS：Eventとして検知されたものについて、SaaSアプリケーションごとの内訳を表示します。

④ Filters：Eventとして検知されたものについて、検索したりフィルタリングをかけることが可能です。

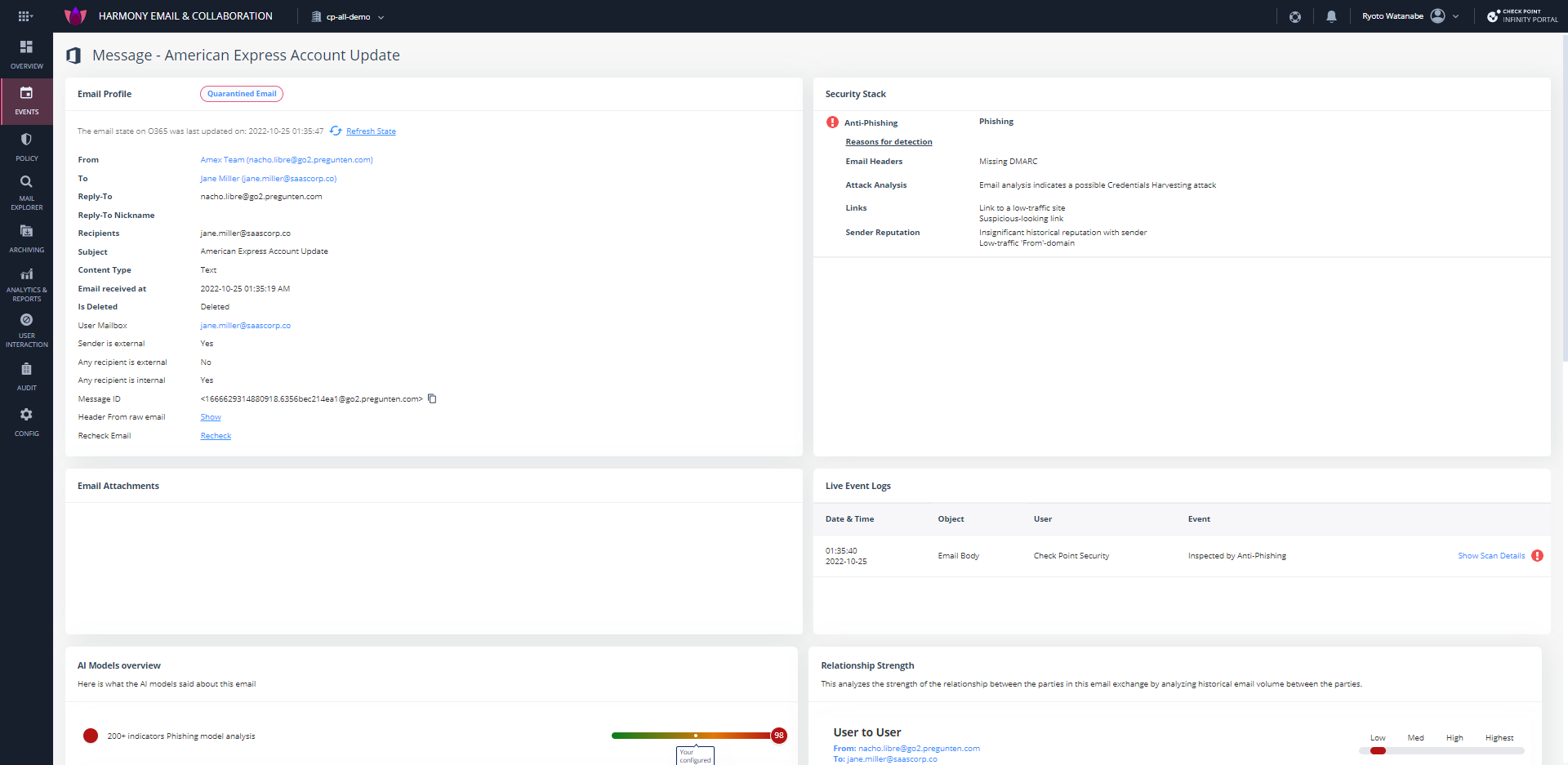
フィルターをかけられる項目：

* 表示期間（６０分、２４時間、７日、３０日、１２カ月）
* State：イベントのステータス
  + **All：**全て
  + **Pending：**セキュリティイベントが検知され、必要な対応が実施されていないもの
  + **Remediated：**セキュリティイベントが検知され、必要な対応が実施されたもの
  + **Detected：**外部向けの送信においてセキュリティイベントが検知されたもの
  + **Exception：Allow-list（**ホワイトリスト）に追加したアイテムで、受信されたもの
  + **Dismiss：**Pending状態のセキュリティイベントで、管理者によって問題ないと判断されたもの
* **Type：**セキュリティイベントの種類
* **Severity：**深刻度
* **SaaS：**連携済みのSaaSアプリケーション
* **Tool：**各Security Blade（=機能）
  + All
  + Threat Extraction: ファイル無害化
  + Anti-Malware
  + Anti-Phishing
  + URL Reputation
  + Click-Time Protection
  + DLP

⑤Group Actions：各セキュリティイベントに対して、一括での手動アクションが可能です。操作したいセキュリティイベントのチェックボックスを入力すると、Group Actionsのプルダウンメニューが使用可能となります。

* Remediatedのフィッシングメールを選択した場合（複数選択可能）、以下のアクションが可能です。
  + Alert user of phishing（Phishingメールとしてユーザーへアラート通知を出す）
  + Dismiss
  + Release email（一度隔離されたメールをユーザーへリリースし送信する）
  + Report as not phishing（Phishingではないとレポートする）
* Pendingのフィッシングメールを選択した場合（複数選択可能）、以下のアクションが可能です。
  + Alert user of phishing（Phishingメールとしてユーザーへアラートを送る）
  + Quarantine（隔離する)
  + Move to Spam（Spam boxへ移動させる）
  + Report as not phishing（Phishingではないとレポートする）
  + Dismiss（イベントを無視する）

⑥Events matched：検索/フィルタリングした結果を表示します。表示されたメールのタイトルを押下すると、下記画面に遷移し、送信元や受信者、検知理由などの情報を確認することが可能です。



③　Security Stack

（検知理由と稼働したBlade（=機能））

⑤　Live Event Logs

　（稼働したBlade（=機能）と稼働日時）

⑦　Relationship Strength

ユーザー間、組織間でのメール送受信の関係性

⑥　AI Models overview

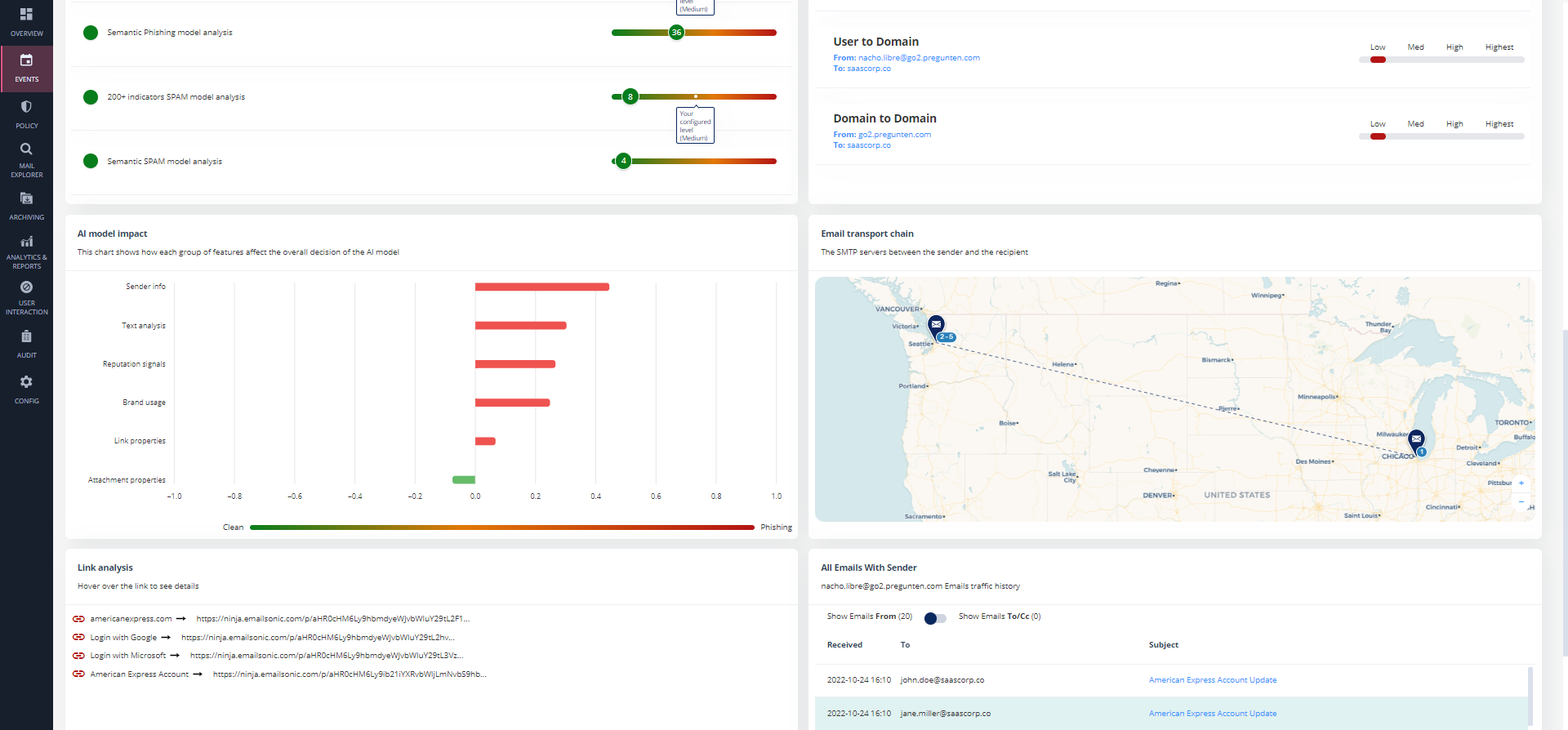
　（AIによる評価スコア概要）

④　Email Attachments

（添付ファイル）

②　Email Profile（メール概要）

1. Message（メール件名）



⑪　All Emails With Sender

（メールの受信者と送信者のメールの履歴）

⑩　Link analysis

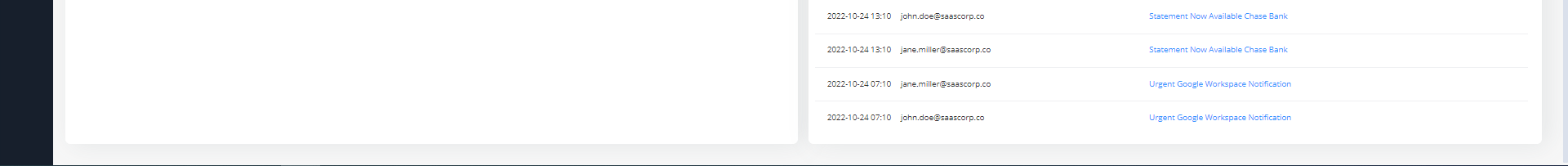
　（本文中のURL分析）

⑧　AI Models Impact

　（AIモデル影響）

⑧　Email transport chain

　（メールの転送経路）



■画面構成

① Message：該当のメールの件名を表示します。

② Email Profile：メールの基本情報を表示します。

　・From：送信者

　・To：受信者

　・Recipients：受信メールアドレス

　・Subject：件名

　・Content Type：メール本文内のタイプ（例：text）

　・Email received at：メール受信日、時間

　・Is Deleted：受信ボックスからメールが削除されているか

　・User Mailbox：受信者のメールボックス

　・Sender is external：送信者は外部からか

　・Any recipient is internal：受信者内に組織内の人が存在するか

　・Message ID：メッセージID

　・Header From raw email：メールヘッダ

　・Recheck Email：メールの再チェック

③ Security Stack：検知理由と稼働したBlade（=機能）

どのセキュリティ機能でどのような脅威を検知したかを表示します。１行目（上記画像であれば「Anti-phishing」）が稼働したBlade（=機能）となります。

**Reasons For Detection** :検知理由の詳細が記載されます。

**Email Headers :**メールヘッダ上で検知したリスクを表示します。

Non ASCII Info In Headers: メールヘッダにASCII情報が示されていない

Missing DMARC: DMARC認証の登録がされていない

**Domain Impersonation**: ドメインのなりすましが検知された場合に表示されます。

SPF check failed when checking sending IP: ○○ for domain ○○: 送信者のIPアドレスがドメインのDNSに登録された正規情報と一致しない(SPF認証されない)

**Sender Reputation :**メール送信者のレピュテーションによるリスクを表示します。

Insignificant Historical Reputation With Sender: 送信者のレピュテーション記録が好ましくない

Low-traffic 'From'-domain: 送信者のドメインからの通信が少ない

**Crypto Wallet Address:** 仮想通貨のウォレット情報が検知された場合に表示されます。

Email body contains a crypto wallet address: メール本文に仮想通貨ウォレットの情報が含まれる

**Attack Analysis:** 特定の種類の攻撃を検知した場合に表示されます。

Email analysis indicates a possible Extortion attack: 本文の内容から、該当メールが脅迫メールである可能性を検知

**Links :** メール内のリンクにリスクがある場合に表示されます。

Link To Newly Registered Domain: 登録されたばかりのドメインへのリンクが含まれる

Link To A Low-Traffic Site: アクセスの少ないWebサイトへのリンクが含まれる

Links with email-parameter: マーケティング分析などに利用されるパラメータがリンクに含まれる

Blacklisted URLs: 脅威として脅威データベースに登録されているURLが含まれる

Link-shorteners: 短縮URLが含まれる

Links to less-secure WordPress powered site: セキュリティが十分でないWordPressサイトへのリンクが含まれる

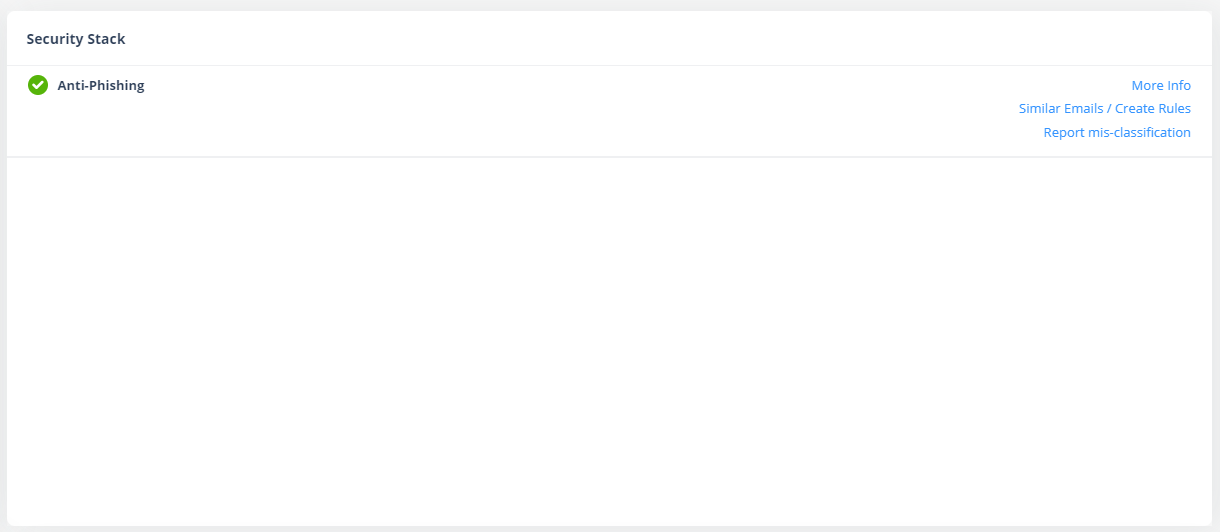
**Email Text :**メール本文の文章に疑わしい内容が見られる場合に表示されます。

Suspicious-Looking Email Text: メール本文の文章に悪意があると判断できる

Text obfuscation in the email HTML: HTMLメールの文章に難読化されたものが含まれる

Email Content Is Encoded: メール本文がエンコードされている

また、Security Stack内では以下の操作を行うことも可能です。



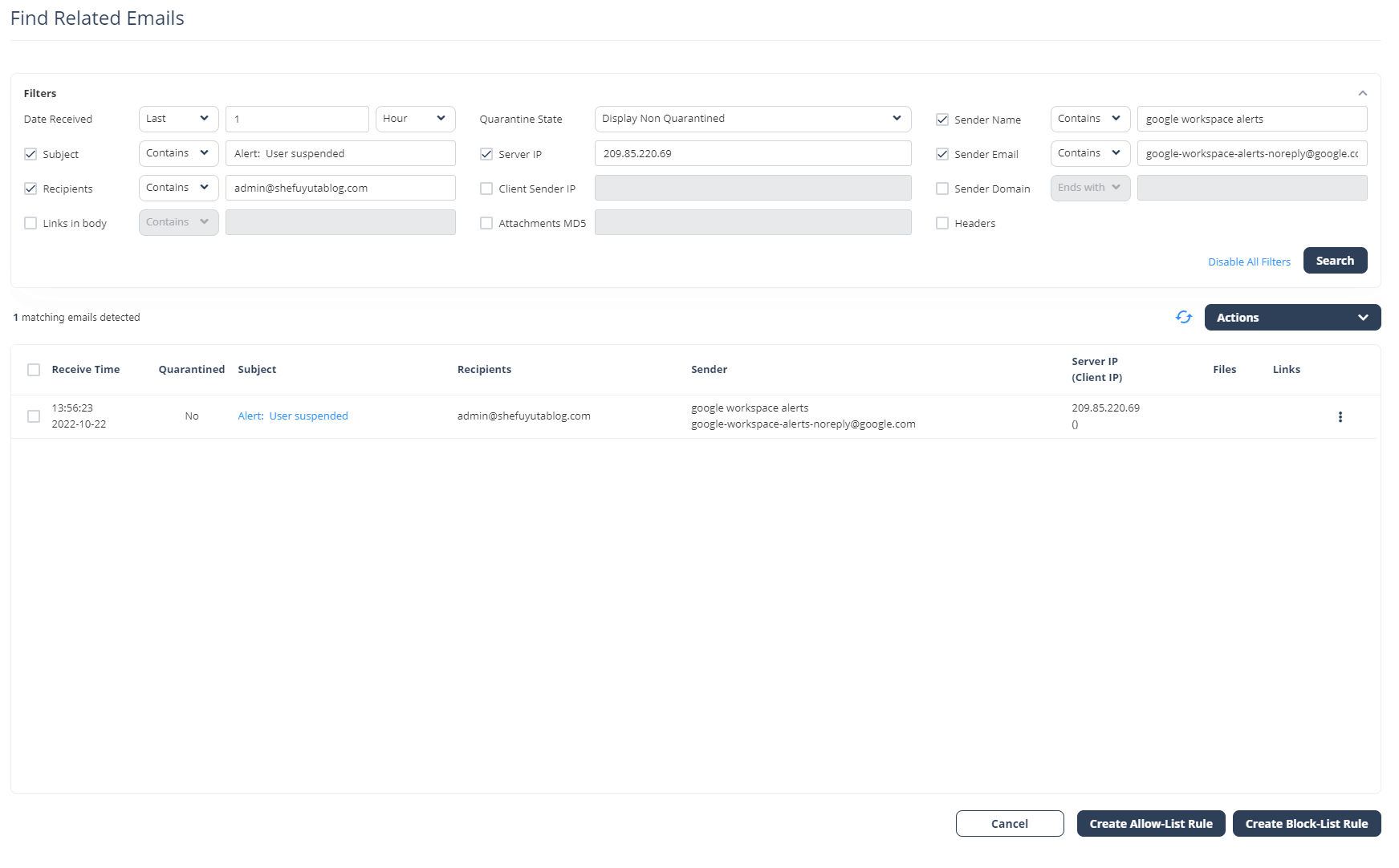
**More Info:** メールに含まれる脅威情報の詳細を確認するウィンドウがポップアップで表示されます。上記と同じReasons for detectionの他に以下の情報が記載されます。

**Phishing Status:** どの脅威として検知したのかを表示します。(例: Phishing)

**Detection Reason:** なぜ上記のPhishing Statusになったのかを表示します。(例: Phishing Confidence Level - Highest)

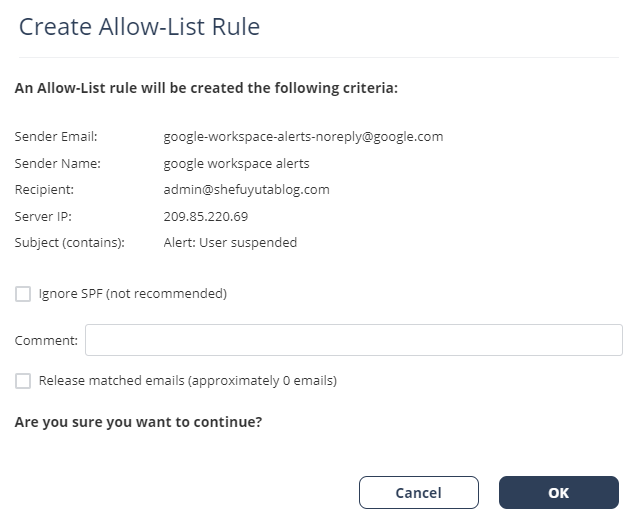
**Links:** メールに含まれるリンクの情報が記載されます。VirusTotalによるスキャンも可能です。

**Similar Emails / Create Rules:** MAIL EXPLORERのウィンドウがポップアップ表示され、同じ件名、受信者、サーバーIP、送信者名、送信者メールアドレスで自動的にメールが検索されます。MAIL EXPLORERのウィンドウではそのままその検索条件に合ったメールを許可/拒否するAllow/Blockリストを作成できます。



1. Filter: 検索条件の確認・変更ができます。Searchボタンを押下すると②のメールリストが更新されます。
2. Cancel: 検索操作を終了
3. Create Allow-List Rule: Filterの条件に合わせたAllow-Listの作成画面に進みます。
4. Create Block-List Rule: Filterの条件に合わせたBlock-Listの作成画面に進みます。
5. ○○matching emails detected: 検索条件にヒットしたメールがリストアップされます。

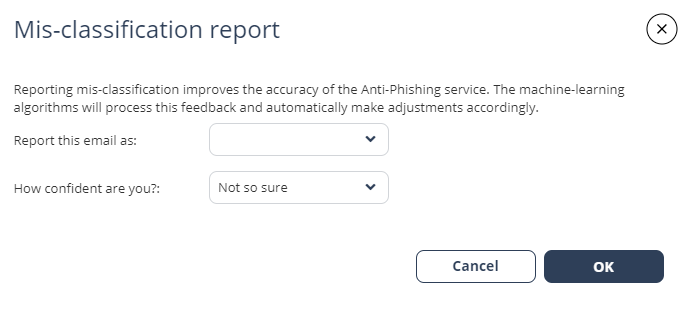
↓Create Allow-List Ruleを押下すると以下の様なウィンドウが表示されます。Block-List Ruleも同様です。



1. Cancel・OK: 設定をキャンセル、または確定します。
2. Release matched emails: 上記のAllow-Listにマッチしているメールが既にユーザーの隔離されている場合は隔離解除します。
3. Comment: Allow-Listに関するコメントです。Allow-List設定後、CONFIG > Anti-Phishing Allow-Listの項目にコメントが表示されます。(例: Allow-Listに設定した理由などを設定することで管理しやすくなります。)
4. Ignore SPF: デフォルトではAllow-List条件にマッチしていても、SPF認証を通らないメールに関しては検査対象になります。チェックを入れると、SPF認証の結果に関わらずAllow-List条件にマッチしたすべてのメールが検査を通過します。(チェックすることはセキュリティの観点から非推奨です。)
5. Criteria: 前画面のFilterで設定した条件でAllow-Listが作られるため、その内容をここで確認します。

※前画面のSearchを押下した・していないに関わらず、Filter上でチェックが入った項目が全て適用されます。

**Report mis-classification:** Harmony Email & Collaborationが下した判断は間違っているという場合に、AIの機械学習を進めるべくコンフィグミスのレポートを管理者から登録できます。登録用のウィンドウはポップアップで表示されます。



**Report this email as:** 該当メールがどのような種類の脅威であるか、管理者の判断を以下から選択します。

・Legit Marketing Email: 該当メールは正当なマーケティングメールである

・Clean Email: 該当メールは無害なメールである

・Spam: 該当メールはスパムメールである

・Phishing: 該当メールはフィッシングメールである

**How confident are you?:** Report this email asで選択した内容が正しいと言える確度を選択します。

・Not so sure: あまり自信はない

・Medium Confidence: ある程度の自信がある

・High Confidence: 間違いない

選択後、OKをクリックするとレポートは完了となり、Thanksのメッセージが表示されます。

④ Email Attachments：添付ファイルがメール内に送付されていた場合表示されます

⑤ Live Event Logs：稼働したSecurity Blade（=機能）の稼働日時を示します

⑥ AI Model overview：AIモデルによる評価結果概要を示します。

　・200+ indicators Phishing model analysis：ヘッダーや本文、レピュテーション、リンク、添付ファイル等の200以上の指標に関するAI分析に基づいたフィッシングスコアを示します。０から１００までの範囲が有り、スコアが高いほどフィッシングの危険性が高いと判断されます。

　・Semantic Phishing model analysis：メールのタイトルと本文のみを分析したフィッシングスコアをしめします。

　・200+ indicators SPAM model analysis：ヘッダーや本文、レピュテーション、リンク、添付ファイル等の200以上の指標に関するAI分析に基づいたスパムスコアを示します。０から１００までの範囲が有り、スコアが高いほどフィッシングの危険性が高いと判断されます。

　・Semantic SPAM model analysis：メールのタイトルと本文のみを分析したスパムスコアをしめします。

⑦ Relationship Strength：受信者と送信者の関係性。どの位の頻度でメールのやり取りがあるかを表現しています。Lowのほうがやり取りが少なく、Highestのほうがやり取りが多いことを示します。

　・User to User：受信者と送信者の間

　・User to Domain：受信者と送信者のドメインの間

　・Domain to Domain：受信者のドメインと送信者のドメインの間

⑧ AI model Impact：AIモデルの決定に関する影響度合いを示します。０を基準とし、1.0に近いほど危険度が高く、-1.0に近いほど危険度が小さいと判断したことを表します。

　・Attachment properties：添付ファイルの情報

　・Brand usage：署名部分にある会社のロゴなどの情報

　・Sender info：送信者情報

　・Link properties：リンク情報

　・Reputation signals：レピュテーション情報

　・Text analysis：メール本文

⑨ Email transport chain：SMTPサーバの場所を判断します。IPアドレスに基づいて、どこでメールのやり取りが実施されているかを判断します。

⑩ Link analysis：リンクの分析を表示します。プロトコル、ドメイン・ホスト、ディレクトリ、ファイル名等の分析を行っています。

⑪ All Emails With Sender：受信者と送信者の間のメールやりとり履歴を示します。。

**Messageページ内のアイコンの意味**

Security Stack

: 安全と判定

: 脅威と判定

AI Models over view

: 安全と判定

: 脅威と判定

Link Analysis

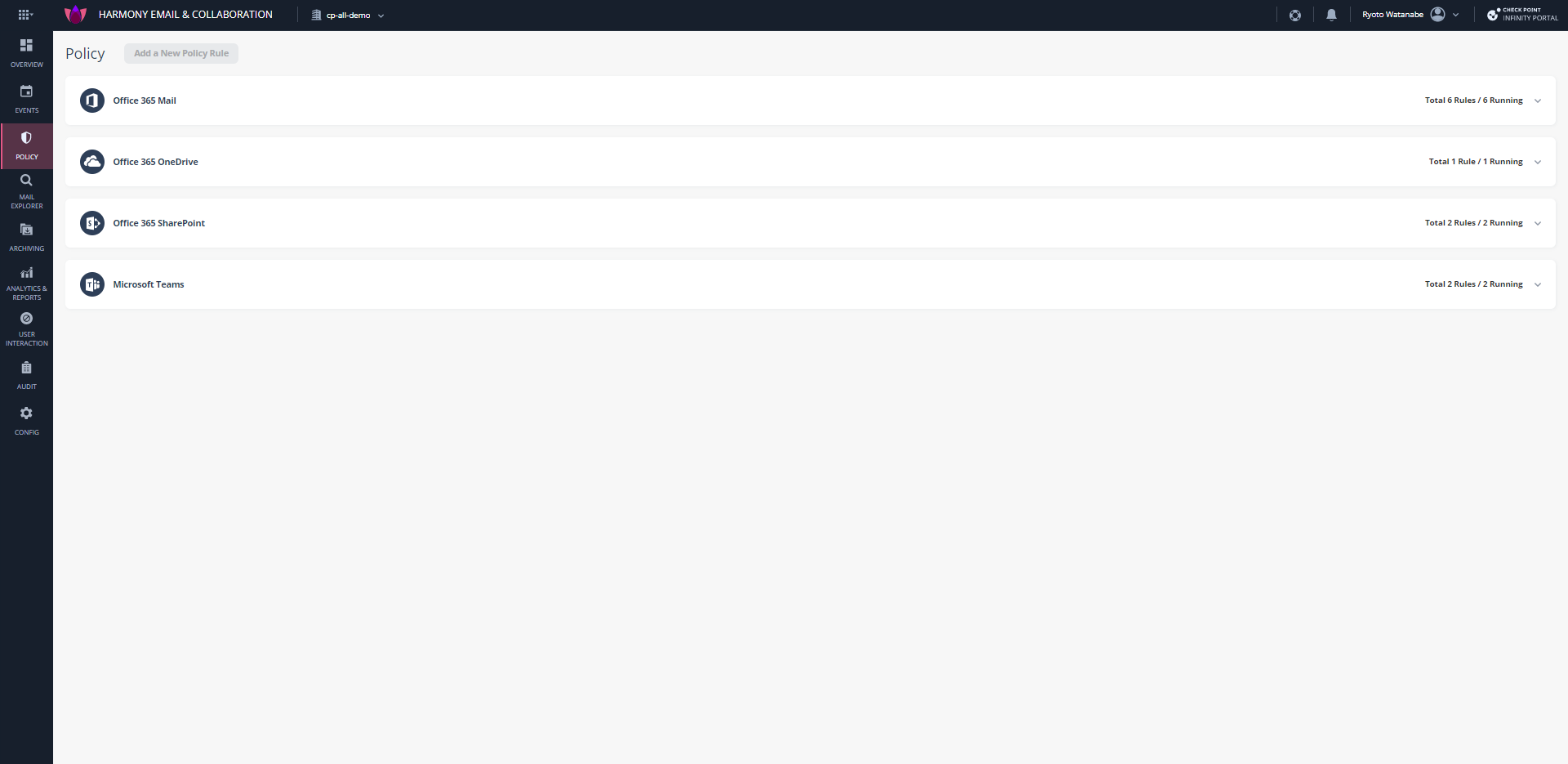
: 安全なリンク

: 疑わしいリンク

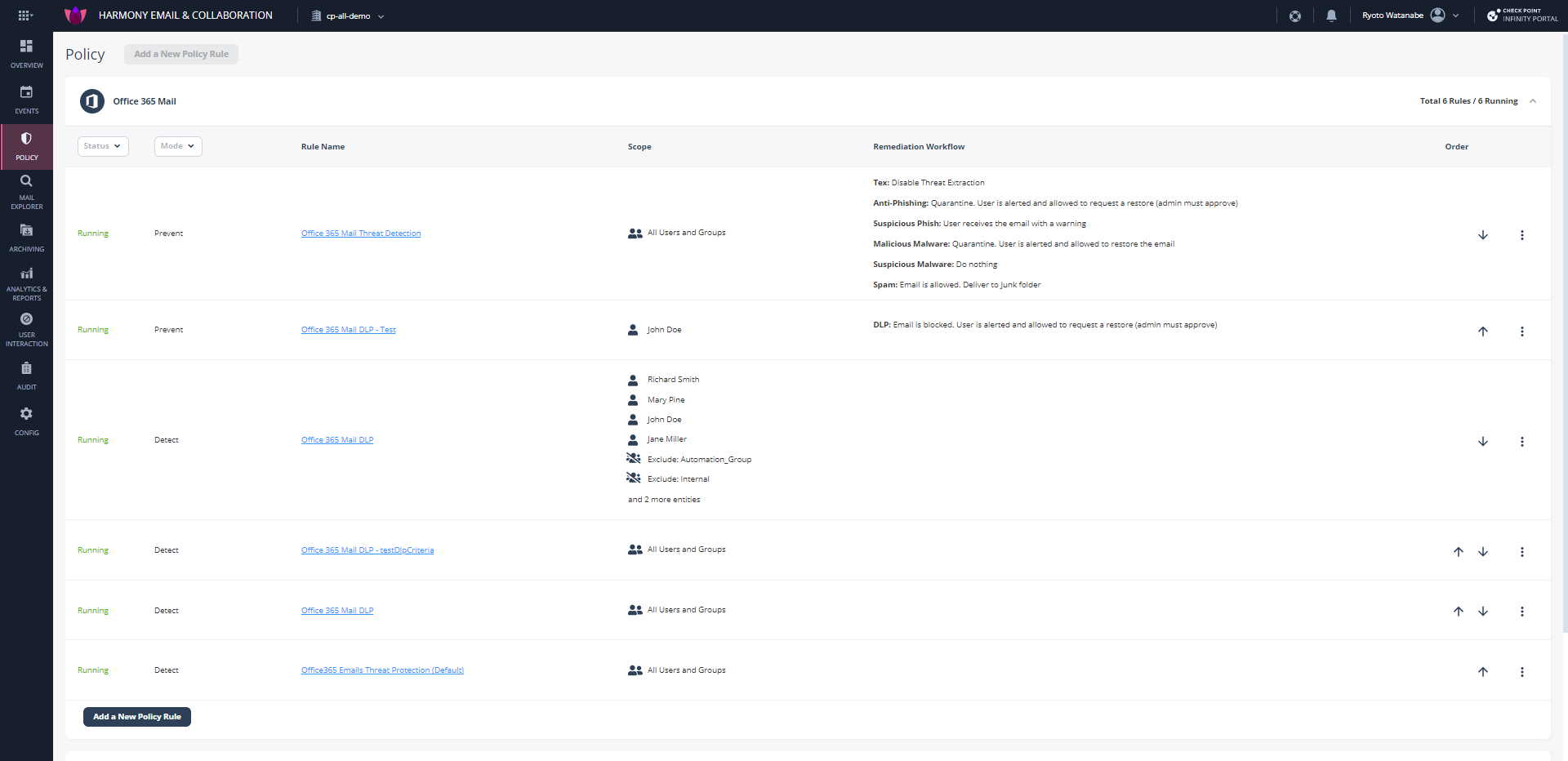
: 危険なリンク

# POLICY

Policyでは、すでにHarmony Email & Collaborationと連携しているSaaSアプリケーションの中から、有効化する機能の選択や、機能の適用範囲を設定することが出来ます。



Policyを設定したいSaaSアプリケーションを押下します



②Policyの新規作成

①SaaSアプリケーションに設定している内容一覧

■画面構成

①SaaSアプリケーションに設定しているポリシー一覧

　・Status：そのルールがRunning（適用中）か、Stopped（停止中）か、が表示されます。

　・Mode：そのルールのモード（Prevent, Detect and Remediate, Detect）が表示されます。

　・Rule Name：そのルールの名前が表示されます。押下すると、詳細を確認したり、内容を変更することが出来ます。

「

＊＊直近のPoCでは操作不要のため、設定変更手順については改めてご案内いたします＊＊

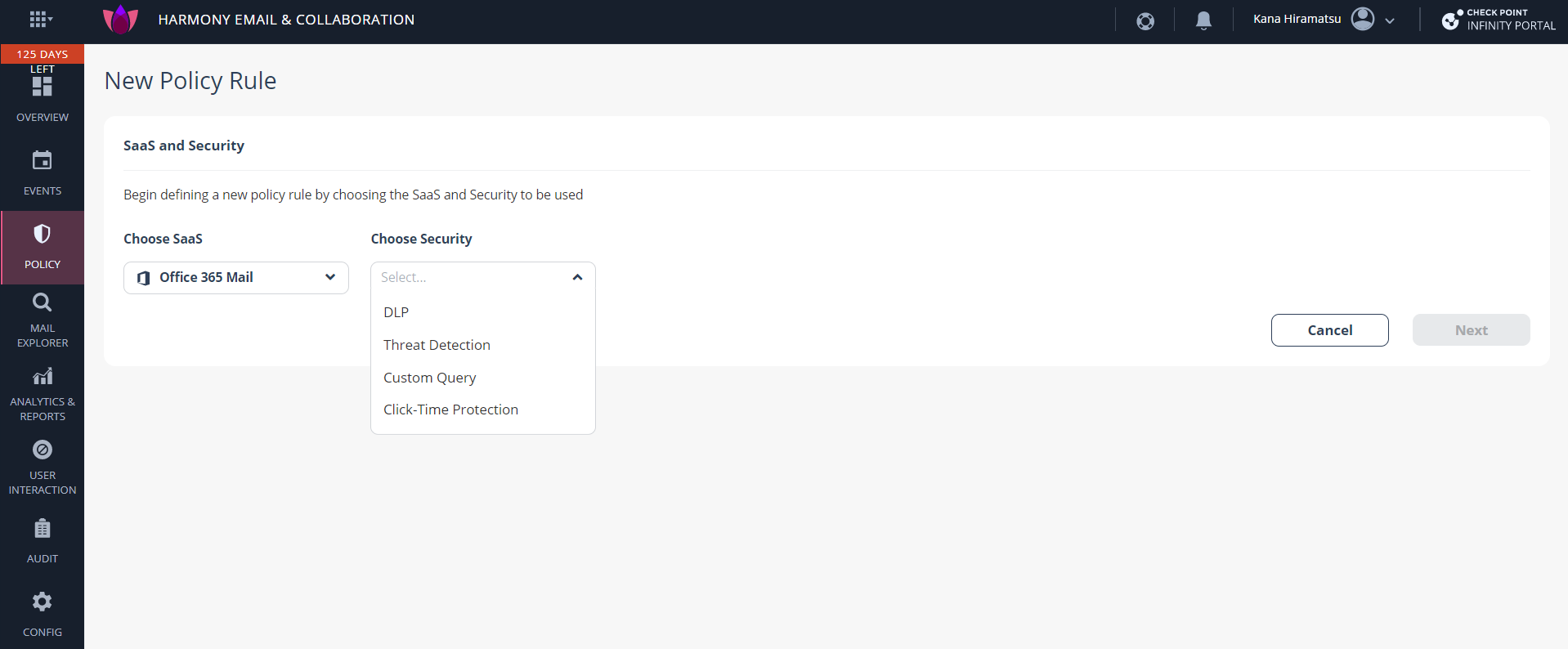
　」

　・Scope：そのルールの対象として設定されているメンバーやグループが表示されます。

　・Remediation Workflow：各機能が動作した際のワークフローが表示されます。

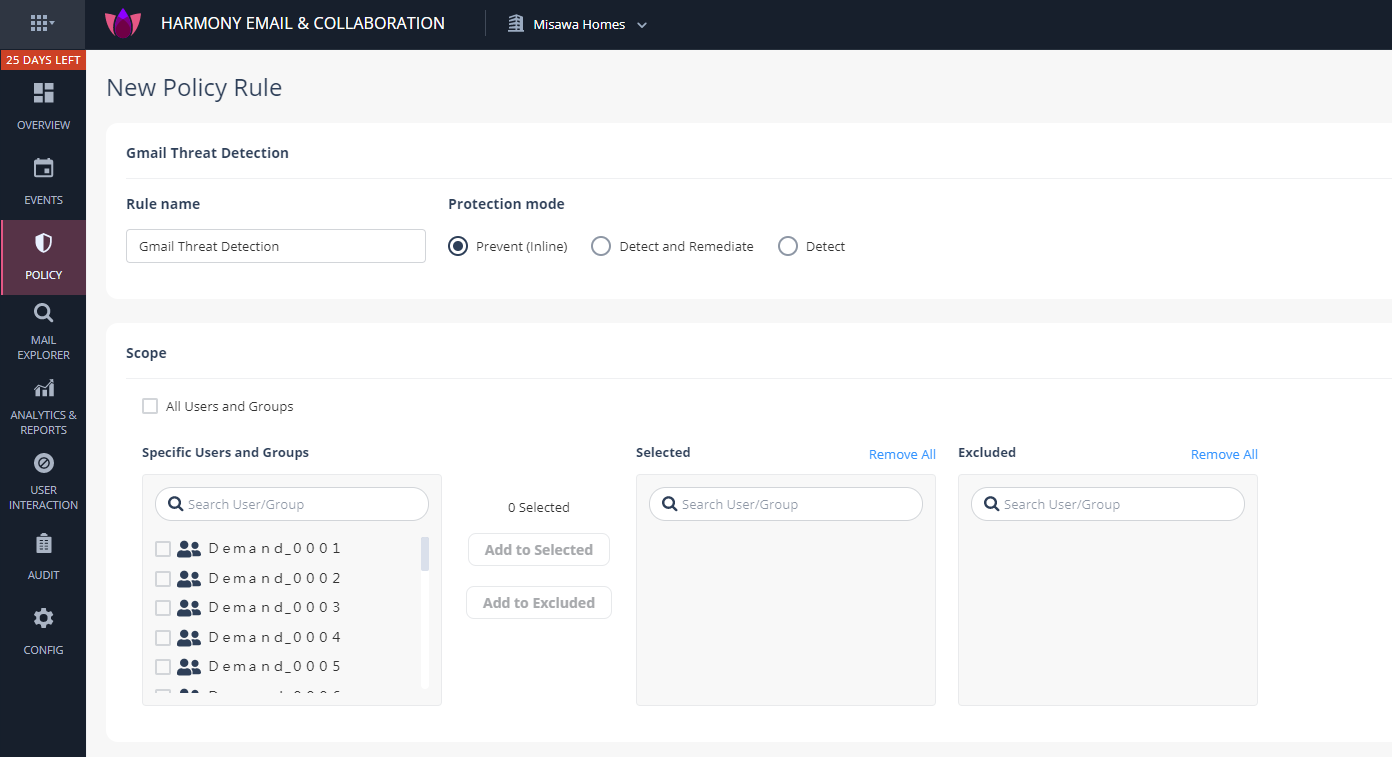
　・Order：ポリシーの優先順位が表示されます。

②Policyの新規作成：ポリシーを新しく作成することが出来ます。作成手順は下記のとおりです。



　作成したいポリシーのセキュリティを選択します。

* **DLP:** データ漏洩の保護
* **Threat Detection:** フィッシング、マルウェア、スパムメール等からの保護
* **Custom Query:** Allow-list, Block-list, 等クエリをカスタマイズ
* **Click-Time Protection:** メール本文内と添付ファイル内に含まれるURLリンクを置き換え、CPの検査エンジンでサイトがフィッシングサイトでないことを確認 (URL Reputation, URL Emulation エンジンを使用)
* URLはhttps://protect.checkpoint.com/v2/ \_\_\_<オリジナル url>\_\_\_<encrypted blob>に変更されます。ドメインがprotect.checkpoint.com/v2/と変更される



①Rule name

②Protection mode

③Scope

■画面構成

①Rule name: ルール名を設定します。

②Protection mode: Protectionモードを選択します。ProtectionモードにはPrevent、Detect and Remediate、Detect モードの３つがあります。

**Preventモード:** Inlineモードでユーザーのメールボックスにメールが配信される前に脅威が検知され、隔離が実行されます。

**Detect and Remediateモード:** ユーザーのメールボックスには一度配信がされ、即時にスキャンと隔離が実施されます。

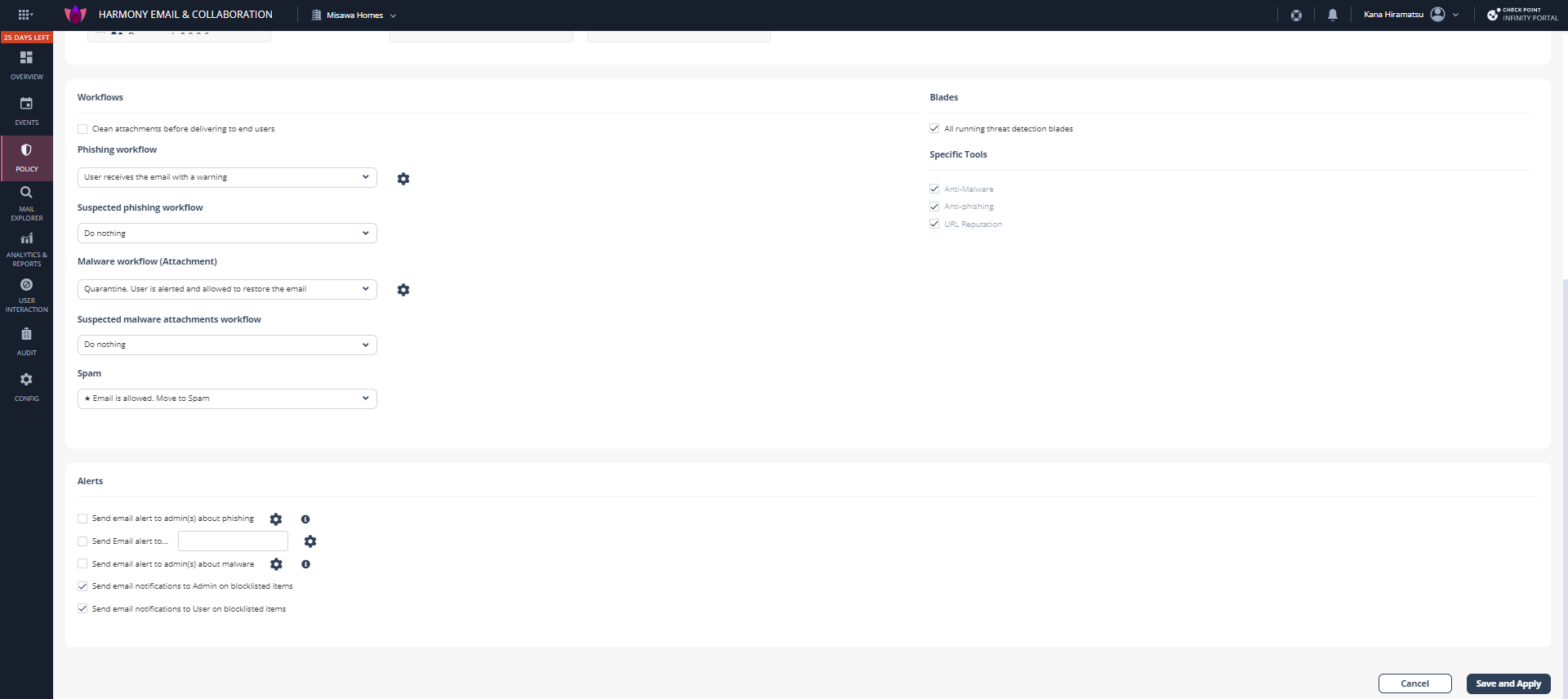
**Detectモード:** 監視のモードのみのため、隔離等の自動アクションは実施されません（手動での隔離は可能）。お客様のメールが隔離・ブロックされることは一切ありません。

※Preventモード、またはDetect and Remediateモードを選択すると、ページ下部に“Workflow”が表示されます。

Threat Extraction機能（ファイル無害化機能）はPreventモードでのみ対応しております。

**③Scope:** ポリシーを適用したいユーザー、グループを選択します。SaaSアプリケーション側で既に設定されているグループ、ユーザーが引き継がれるため、特定のユーザー/グループを追加、除外することができます。

・Workflowの設定（Prevent, Detect and Remediateのいずれかを選択した際に表示されます）



②Blades/ Specific Tools

①Workflows

③Alerts

■画面構成

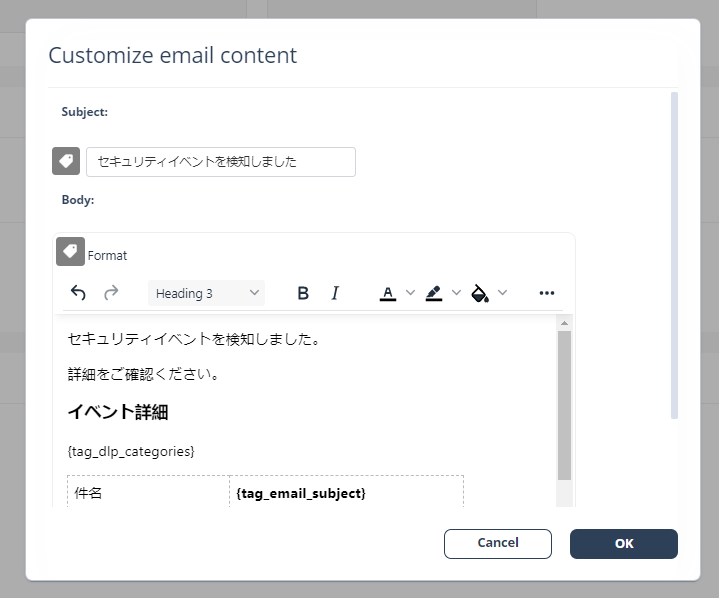
①Workflows：有害なメールを受信した際、各Blade（セキュリティ機能）がどのようにアクションをするか、設定することが出来ます。各設定項目については、次ページの“＊Workflow”をご参照ください。

②Blades/ Specific Tools：各Blade（セキュリティ機能）の有効化/非有効化を設定できます。

“All running threat detection blades”のチェックボックスに記入すると、全てのBladeを一括で有効化出来ます。

All running threat detection bladesのチェックボックスを外すと、Specific Toolsの一覧から有効化したい機能を個別に選択することが出来ます。

③Alerts：各Bladeがセキュリティイベントを検知した際に、どのように通知するかを設定することが出来ます。詳細については下記“＊Alerts”をご参照ください。



アラート通知メールに関しては、日本語での設定も⚙から実施頂けます。「Format」からタグを選択できます。

＊Workflow:

“Clean attachments before delivering to end users”のチェックボックスにチェックを入れることで、Threat Extraction(ファイル無害化)機能が有効化されます。

上記設定を行うと、Clean機能(無害化のみ：URLやマクロ等の除去)とConvert機能(無害化した上でPDF化)のいずれの設定を行うか、下記の選択肢から選択が可能となります。

選択肢：None（実行しない）, All file types（すべてのメールに実行する）,All file types except（除外するファイルタイプを指定）, Only（適用するファイルタイプを指定）

※All file types exceptとOnlyを選択した場合、ファイル拡張子を入力

TEX Workflow:

■**User is allowed to request a restore for any attachment (admin must approve)**

添付ファイルは無害化されたものに置き換えられてメールに添付される。メール内のリンクからオリジナルファイルのリクエストを送ることができ、管理者側で許可すればオリジナルファイルのリストアができる。

**■User is allowed to restore benign attachments only**

添付ファイルは無害化されたものに置き換えられてメールに添付される。メール内のリンクからオリジナルファイルのリクエストを送ることができ、 そのファイル内で脅威が検知されなかった場合に限り管理者側の許可なしにオリジナルファイルをリストアできる。

**■User is allowed to restore any attachment**

添付ファイルは無害化されたものに置き換えられてメールに添付される。メール内のリンクからオリジナルファイルのリクエストを送ることができ、 脅威検知の有無に関わらず管理者側の許可なしにオリジナルファイルをリストアできる。

Threat Extraction 対象ファイル

|  |  |
| --- | --- |
| **ファイルの種類** | **ファイル拡張子** |
| Adobe FDF | FDF |
| Adobe PDF (すべてのバージョン) | PDF |
| Microsoft Excel 2007 以降 | XLSX, XLSB, XLSM, XLTX, XLTM, XLAM |
| Microsoft Excel 2007 Binary | XLSB |
| Microsoft Excel 97 - 2003 | XLS |
| Microsoft PowerPoint 2007 以降 | PPTX, PPTM, POTX, POTM, PPAM, PPSX, PPSM |
| Microsoft PowerPoint 97 - 2003 | PPT, PPS, POT, PPA |
| Microsoft Word 2007 以降 | DOCX, DOCM, DOTX, DOTM |
| Microsoft Word 97 - 2003 | DOC, DOT |

“TEX workflow”より下の項目では、Threat Extraction以外の機能について設定することが可能です。

■**User receives the email with a warning（Phishing, Suspected phishingのみ）**

脅威として検知されたメールの件名に[Phishing Alert!]が追加され、ユーザーに届く。本文の最後には警告文とともに警告文不要というリクエストを管理者に出すためのリンクが追加される。

**■Quarantine. User is alerted and allowed to restore the email（Suspected phishing以外）**

脅威として検知されたメールはユーザーに届かず隔離される。「Quarantined[そのメールの件名]」という件名の隔離通知メールが届く。セキュリティイベントのアラート通知メール、フィッシング・マルウェアアラートメールの内容は管理者側でカスタマイズ可能。ユーザーは自身で隔離通知メール内のリンクから該当メールの解放ができる。

**■Quarantine. User is alerted and allowed to request a restore（admin must approve）（Spam以外）**

脅威として検知されたメールはユーザーに届かず隔離される。「Quarantined[そのメールの件名]」という件名の隔離通知メールが届く。セキュリティイベントのアラート通知メール、フィッシング・マルウェアアラートメールの内容は管理者側でカスタマイズ可能。隔離通知メールには隔離メールの解放リクエスト用リンクが含まれる。管理者がそのリクエストを受け取り許可をすれば、ユーザーに該当メールが届く。

**■Quarantine. User is not alerted (admin can restore)（全て対象）**

脅威として検知されたメールはユーザーに届かず隔離される。その通知もユーザーには届かない。管理者によるメール開放は可能。

**■Email is allowed. Deliver to junk folder（全て対象）**

脅威として検知されたメールもユーザーに届く。その際そのメールはユーザーのジャンクフォルダに格納される。

**■Do nothing（全て対象）**

脅威として検知されたメールも特に他のメールと変わらずにユーザーのメールボックスに届く。

**■Email is allowed. Header is added to the email（全て対象）**

脅威として検知されたメールは他のメールと変わらずにユーザーのメールボックスに届く。その際にカスタマイズ可能なヘッダーが本文に追加される。

**■Add [Spam] to the subject（Spamのみ）**

[Spam]と件名に追加する。

＊Blades（有効化する機能の選択）：

* **Anti-Malware:** メールの添付ファイルや共有ファイルにマルウェアが含まれているかを判断。既知のマルウェアを含むファイルを検出するためにCPの ThreatCloud を使用し（アンチウイルス）、回避可能なゼロデイマルウェアを検出するためにCPの高度なサンドボックス（Threat Emulation）を使用。
* **Anti-Phishing:** フィッシングメールやフィッシングの疑いのあるメールを検出。添付ファイル、リンク、送信者レピュテーション、ドメイン分析、OCR等、メールのさまざまなコンポーネントを分析。
* **URL Reputation:** URLが悪意のあるものであることが知られているか、または悪意のある参照を保持しているか確認。

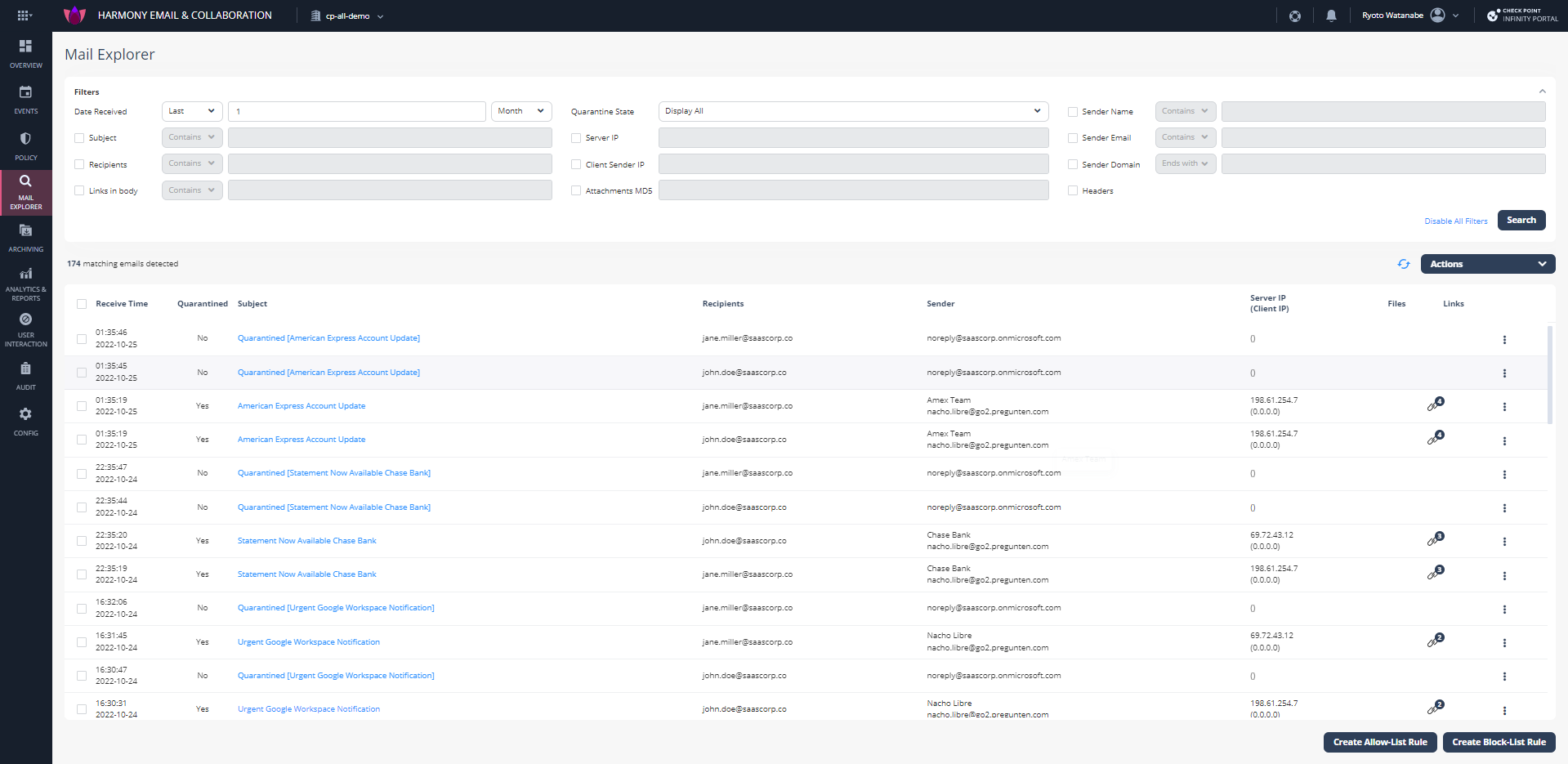
＊Alerts:

アラートメールの送信者設定、アラートメールのカスタマイズが可能です。

1. **Send Email alert to…：**管理者以外の特定のユーザーもアラート通知を受け取りたい場合、メールアドレスをボックス内に記入
2. **Send email alert to admin(s) about malware：**管理者へマルウェアのアラート通知を送信
3. **Alert Recipient about Malware：**マルウェアの可能性あるメールを受け取った管理者、ユーザー両者ともアラート通知を送信
4. **Send email alert to admin(s) about phishing：**管理者へフィッシングのアラート通知を送信
5. **Send email notifications to Admin on blocklisted items：**除外設定（Block-list Rule）で設定されている項目が検知された場合、管理者へアラートを送信
6. **Send email notifications to User on blocklisted items:** 除外設定（Block-list Rule）で設定されている項目が検知された場合、ユーザーへアラートを送信

# MAIL EXPLORER

Mail explorerでは、受信した全てのメールを閲覧することが可能です。Harmony Email & Collaboration でセキュリティイベントとして検知されていないメールも含まれます。



③matching emails detected（検索結果）

②Actions

①Filter

④Create Allow-List Rule / Create Block-List Rule

■画面構成

①Filter：表示するメールついて、受信時間や件名、受信者、送信者など、様々な条件で絞り込むことが出来ます。条件を指定後、欄内右下の“Search”を押下し、検索を実行します。

フィルターをかけられる項目：

* Date Received（受信した期間）
* Quarantine State（隔離されたメール、隔離されていないメール）
* Subject（メール件名）
* Sender Name / Sender Email / Sender Domain（送信者名、メール、ドメイン）
* Recipients（受信者のメールアドレス）
* Links in body（本文内のURL）
* Server IP
* Client Server IP
* Attachments MD5
* Headers（メールヘッダー）

②Actions：検索結果に表示されたものの中で、チェックボックスを入れたメールに対し、一括で隔離やリストアの操作が可能です。

　・Restore selected emails：選択したメールを一括でリストア（ユーザーに解放）します。まだ隔離されていないもののみに適用されます。

　・Quarantine selected emails：選択したメールを一括で隔離します。すでに隔離されたもののみに適用されます。

　・Export to CSV：選択したメールをCSVファイルに出力します。押下すると、すぐにダウンロードが開始されます。

③matching emails detected（検索結果）：フィルターで指定した条件を満たすメール一覧を表示します。

　・Received Time：受信時刻を示します。

　・Quarantined：Yes（隔離済み）/No（未隔離）を示します。

　・Subject：メール件名を示します。押下すると、メールの検知理由等の情報が閲覧できます。

　　　　　（詳細の見方については、p.7のEventsの該当項目をご参照ください。）

　・Recipients：受信者のメールアドレスを示します。

　・Sender：送信者のメールアドレスを示します。

　・Sender IP（Client IP）：送信者のIPを示します。（）内はClient IPを示します。

　・Files：添付ファイルの有無を示します。

　・Links：本文中のURL有無と件数を示します。押下すると、実際のURLが表示されます。

④Create Allow-List Rule / Create Block-List Rule：Allow-List Rule（ホワイトリスト）、およびBlock-List Rule（ブラックリスト）を作成することが可能です。Configのタブから同様の設定が可能ですので、設定が必要な場合はそちらをご利用いただくことを推奨します。後述のConfigの項目をご参照ください。

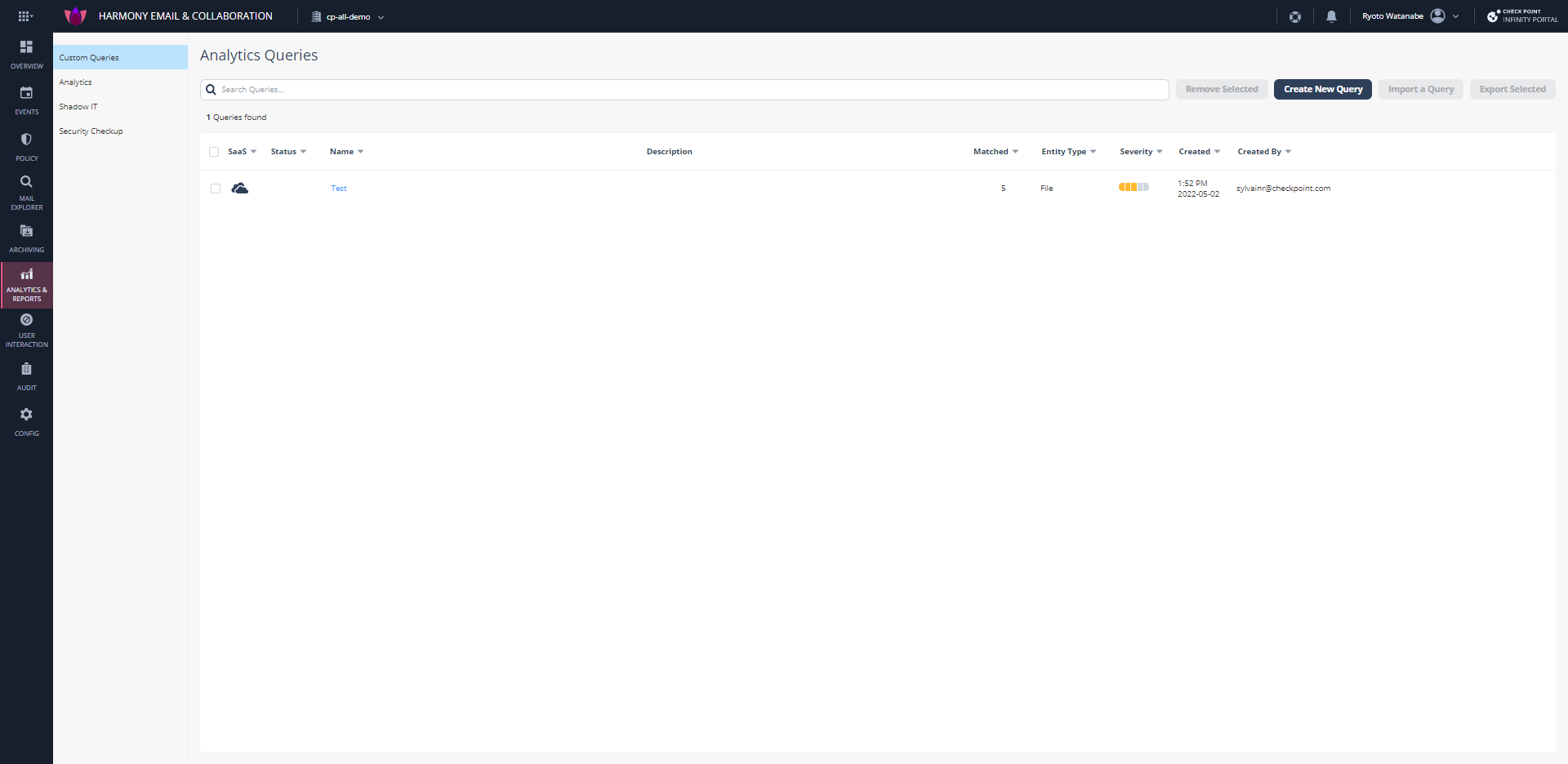
# ANALYTICS & REPORTS

Analytics & Reportsでは、Harmony Email & Collaborationによる各分析データを確認したり、自らクエリを設定して自由にデータを分析することが可能です。

Custom Queries, Analytics, Shadow IT, Security Checkupの項目があります。

**Custom Queries**

新しくカスタムクエリを作成したり、既存のクエリを活用して、様々な条件でメール攻撃の傾向を調べることが出来ます。



②Queries found（クエリ情報一覧）

③各アクション

①Search（クエリの検索）

■画面構成

①Search（クエリの検索）：作成済みのクエリを検索することが出来ます。

②Queries found（クエリ情報一覧）：作成済みのクエリ一覧を表示します。Searchした場合、対象のクエリのみが表示されます。

③各アクション：

　・Remove Selected：チェックボックスで選択したクエリを削除します。

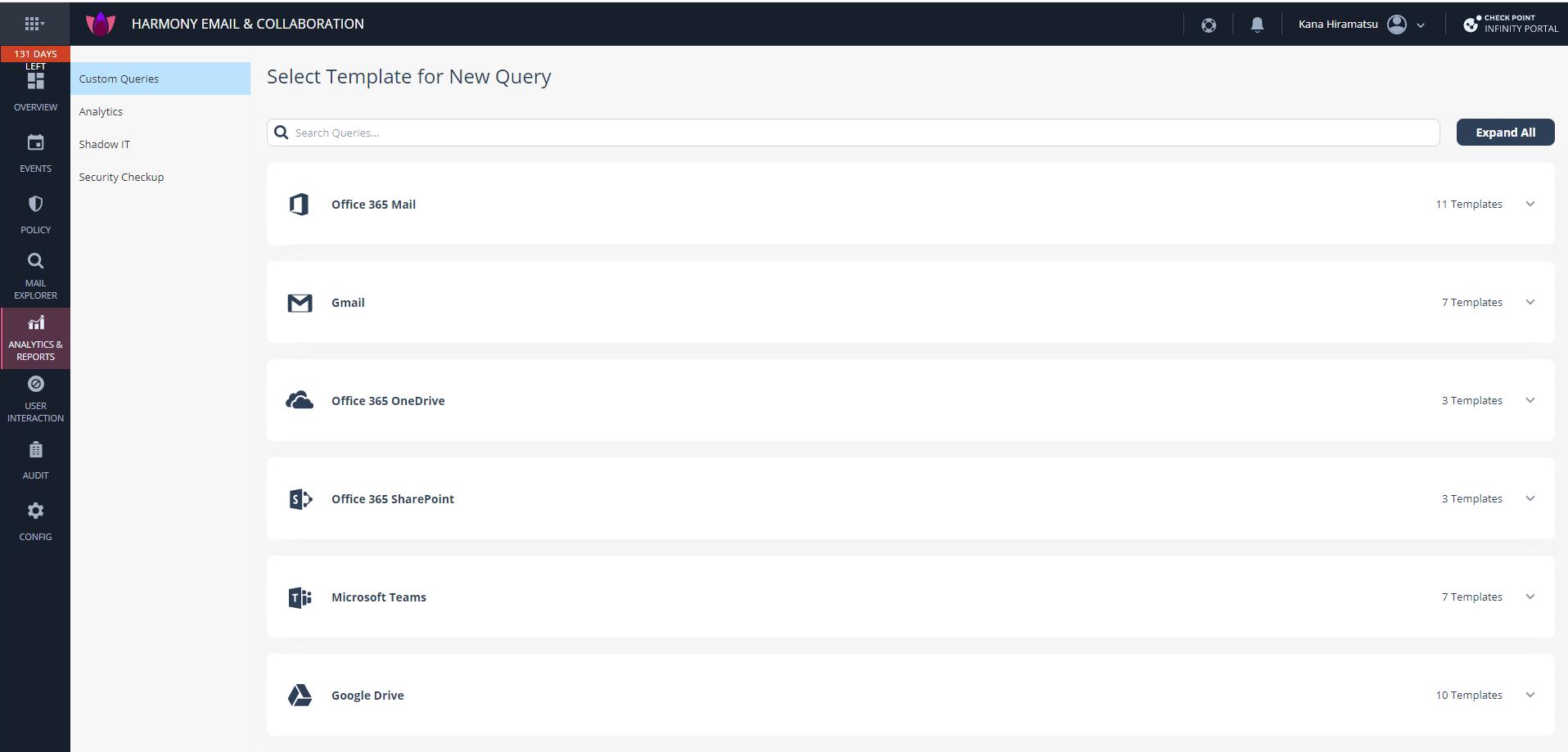
　・Create New Query：新しいカスタムクエリを作成することが出来ます。作成手順は次の項目をご参照ください。

　・Import a Query：.json形式のファイルをインポートしてQuery作成が出来ます。

　・Export Selected：チェックボックスで選択したクエリを.json形式で出力します。その場でダウンロードが開始されます。

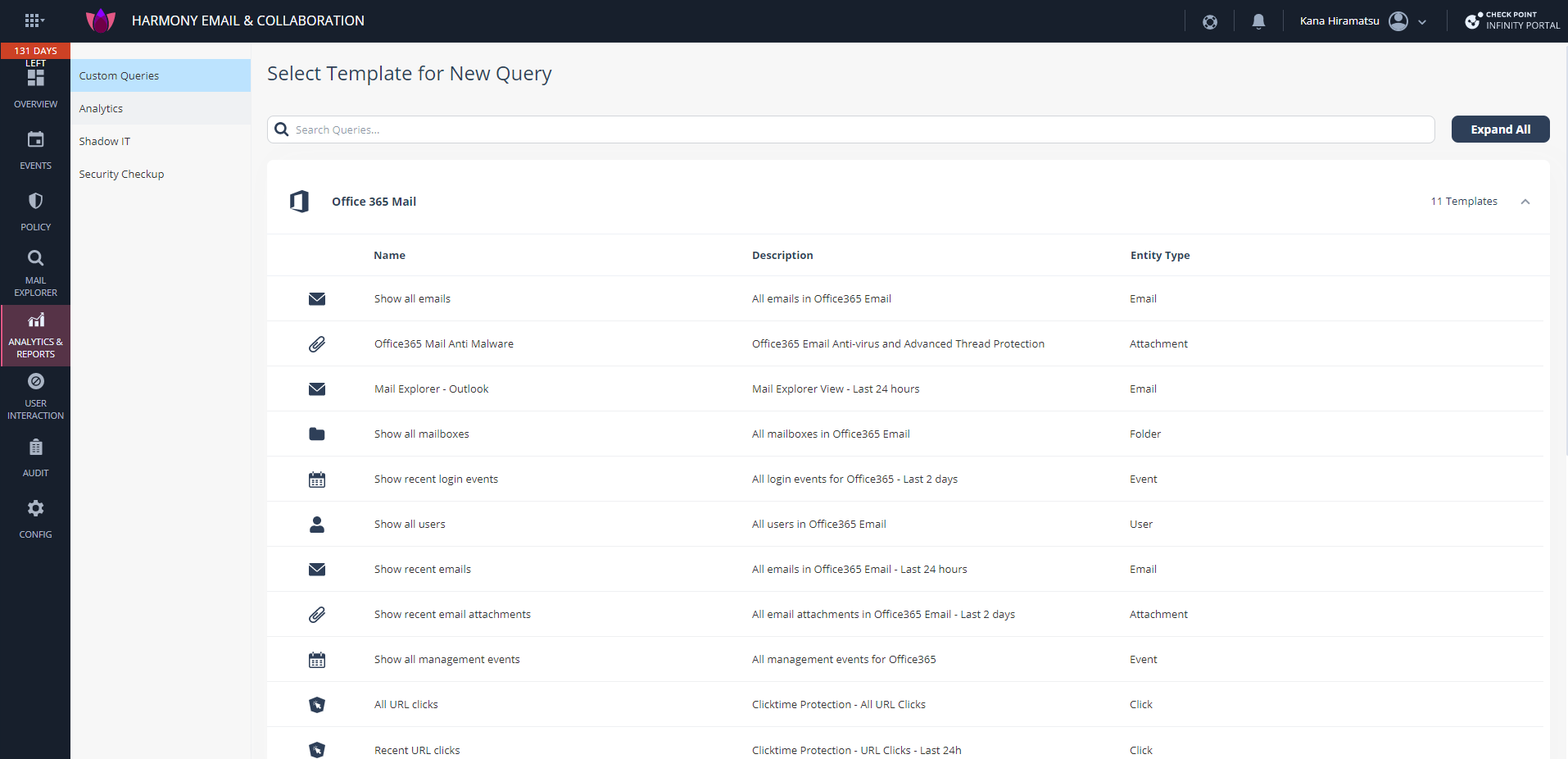
・Create New Queryによるカスタムクエリの新規作成

↓Image1



カスタムクエリを作成したいSaaSアプリケーションを選択します。

↓Image2



使用できるテンプレート一覧

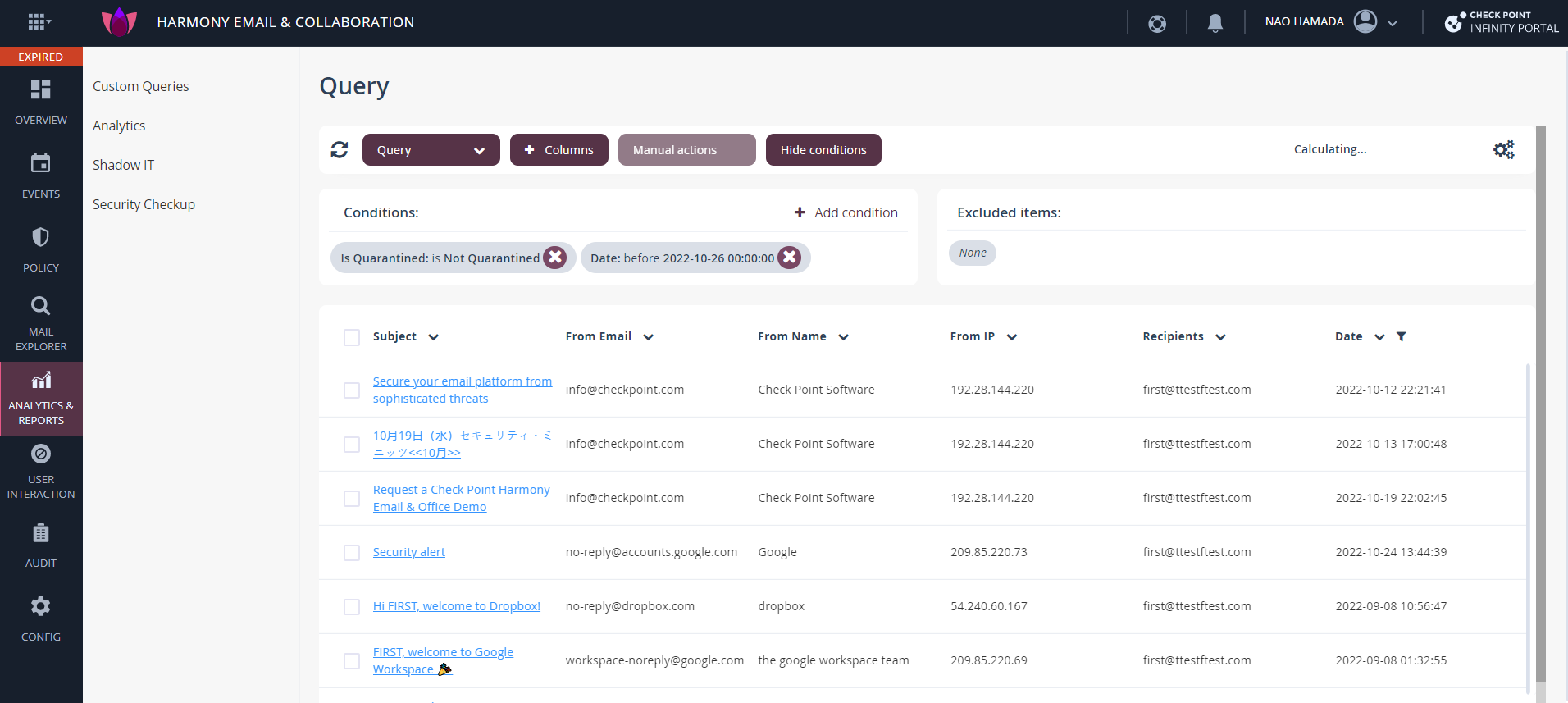
■Create New Queryによるカスタムクエリの新規作成手順

１．Image1のSaaSアプリケーション一覧から、クエリを作成したいものを選択します。

２．Image2クエリ作成のベースとするテンプレートを選択します。

　ー最上段のShow all emailsを選択すると、初めからからクエリを作成することが可能です。

例：“隔離されていないメール”と“10月26日以前受信したメール”を条件として表示



①Conditions

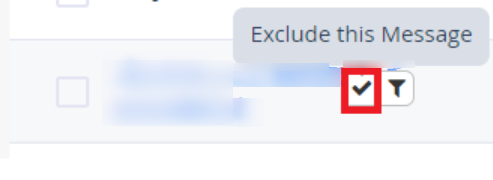
②Excluded items

③結果一覧

■画面構成

①Conditions：クエリに適用している条件を表示しています。枠内右上の「+ Add condition」から、条件を追加することが可能です。

②Excluded items：クエリ結果から除外する条件を表示しています。Queryの結果一覧から、除外したい項目（送信元情報やタイトル、受信者等）にマウスオンし、☑を押下すると、追加することができます。



③結果一覧：クエリを適用した結果一覧を表示します。

　・Subject：メール件名を表示します。

　・From Email：送信元メールアドレスを表示します。

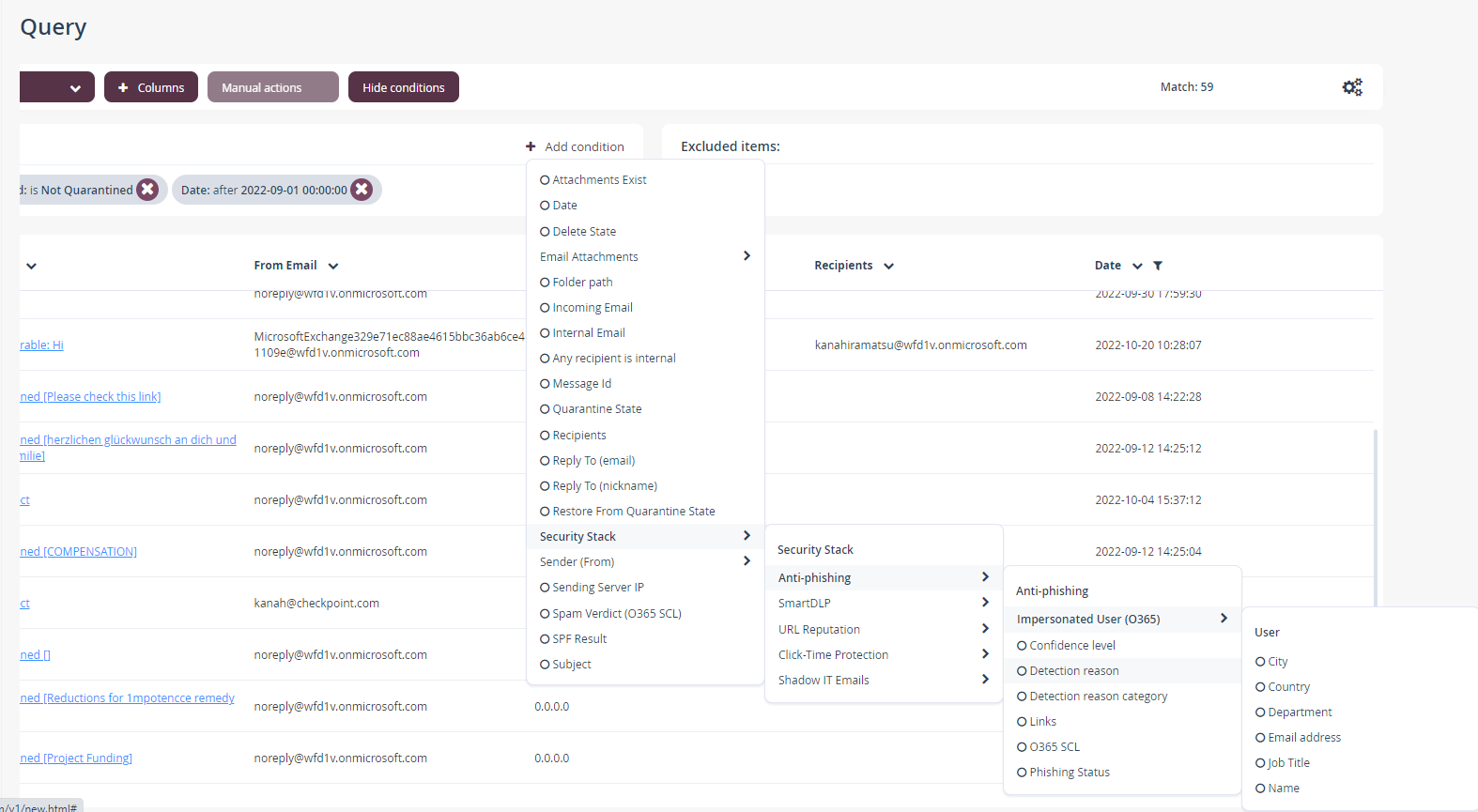
　・From Name：送信元名を表示します。

　・From IP：送信元IPを表示します。

　・Recipients：受信者のメールアドレスを表示します。

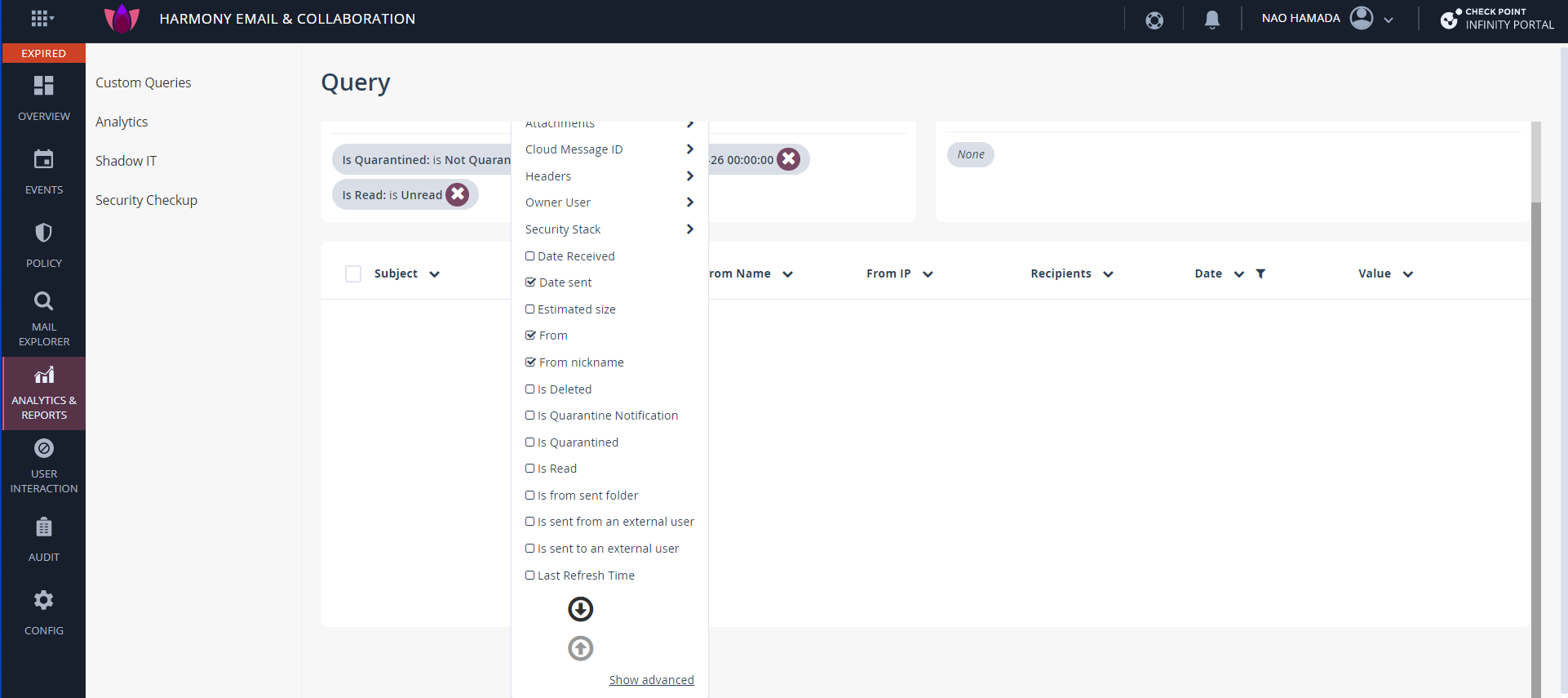
　・Date：受信日時を表示します。

・「+ Add condition」による条件の追加



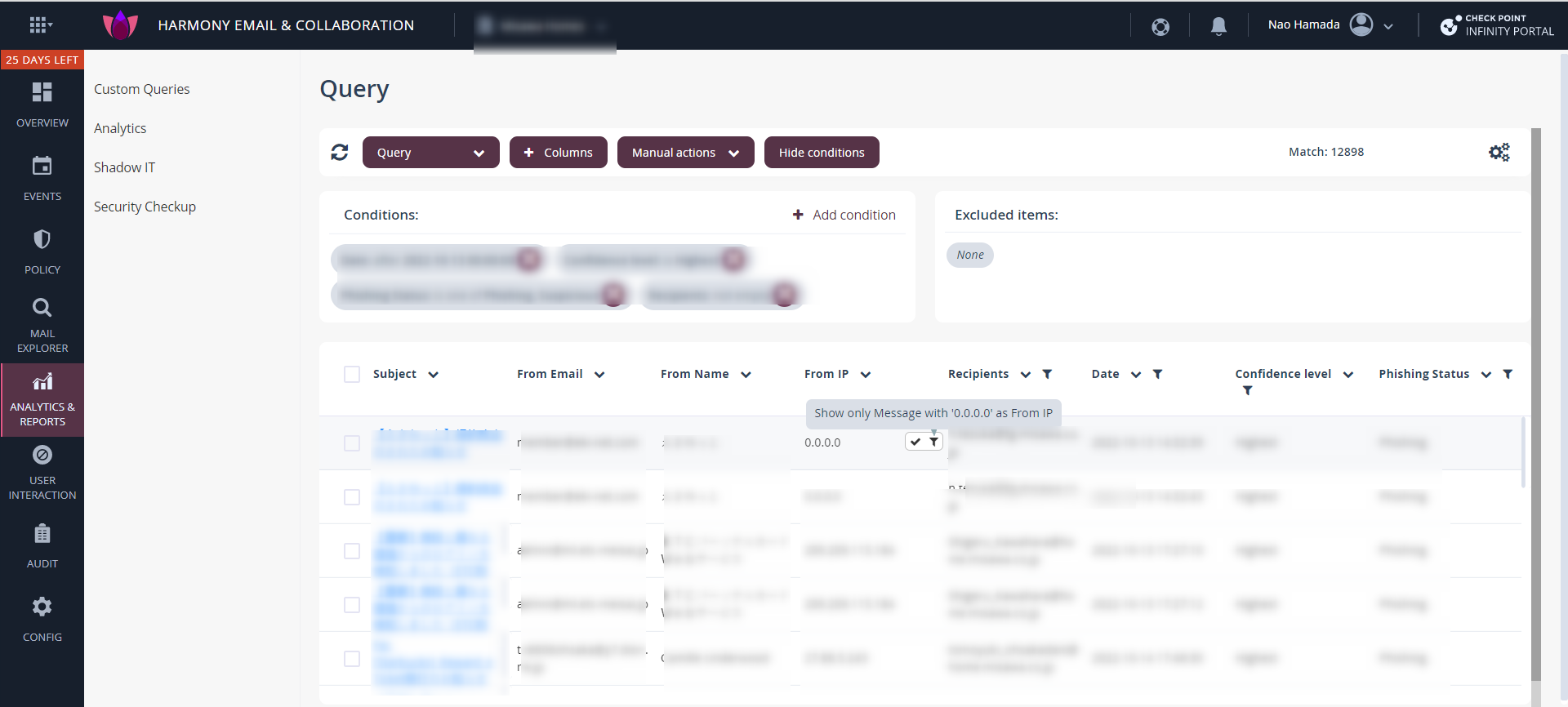
受信者や返信相手、どのセキュリティ機能で検知したか、等幅広い条件を設定可能です。

・「Show Advanced」による条件の追加



「+ Add condition」の最下部にある「show advanced」を押下すると、さらに細かい条件を設定可能です。

・クエリの検索結果から条件を追加する方法（Excluded itemsの手順と一部重複。）

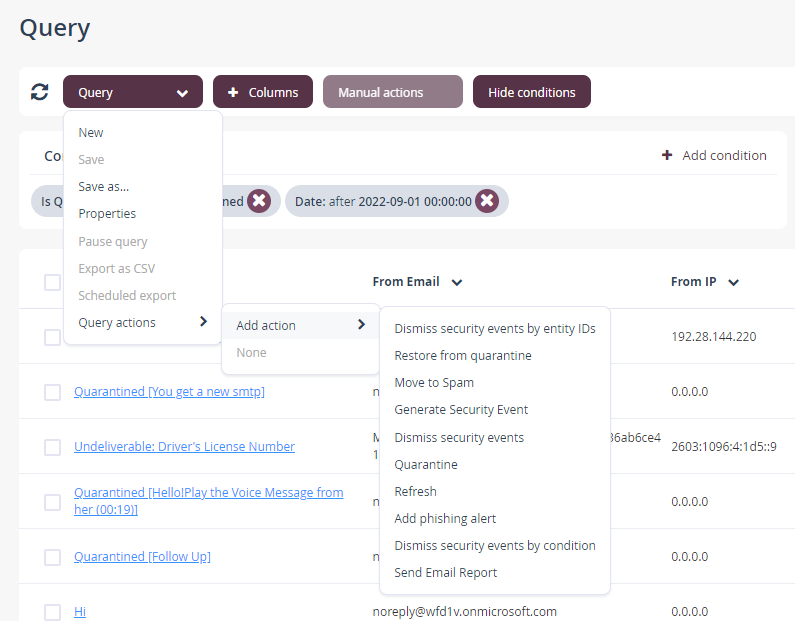


Queryの検索結果から、Queryの条件をさらに追加することも可能です。

✓を押下するとその数値（IPや送信者名、アドレスなど）を除外し、

漏斗マークを押下するとその数値を条件として追加します。

・クエリの保存とその他のアクションについて



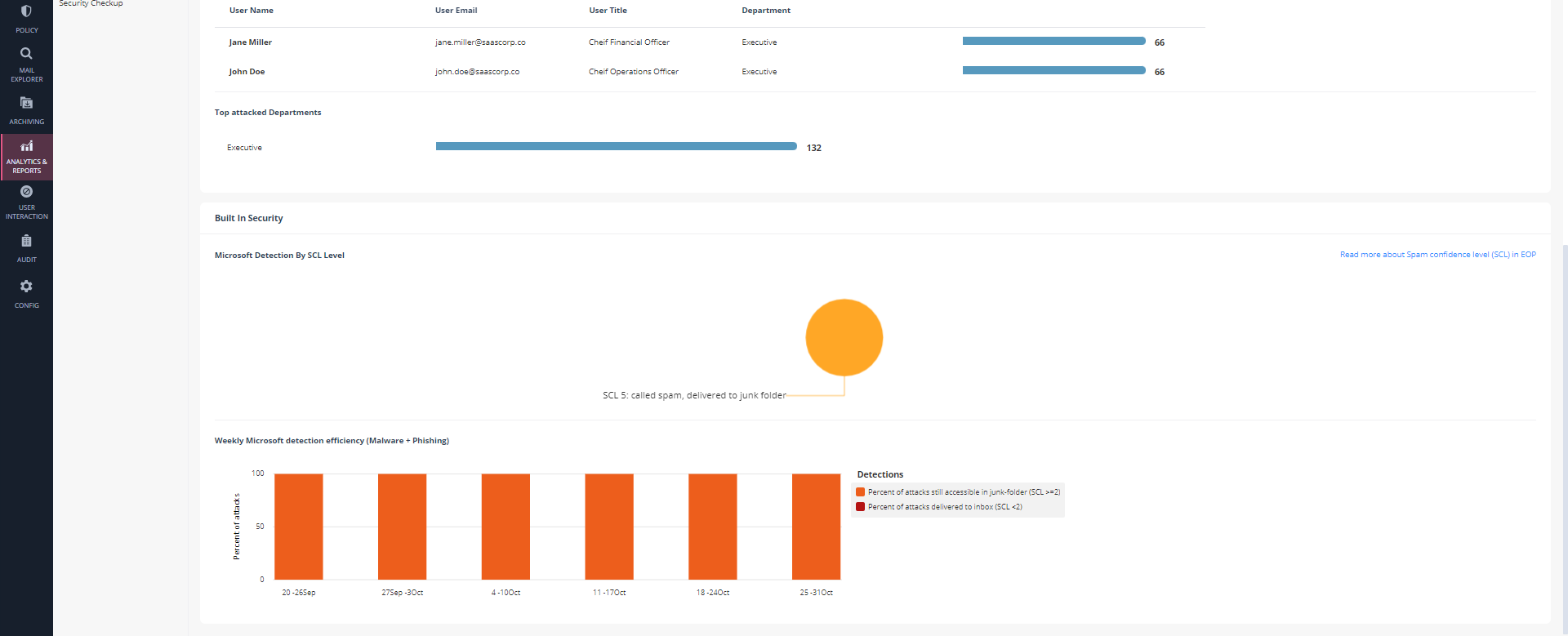
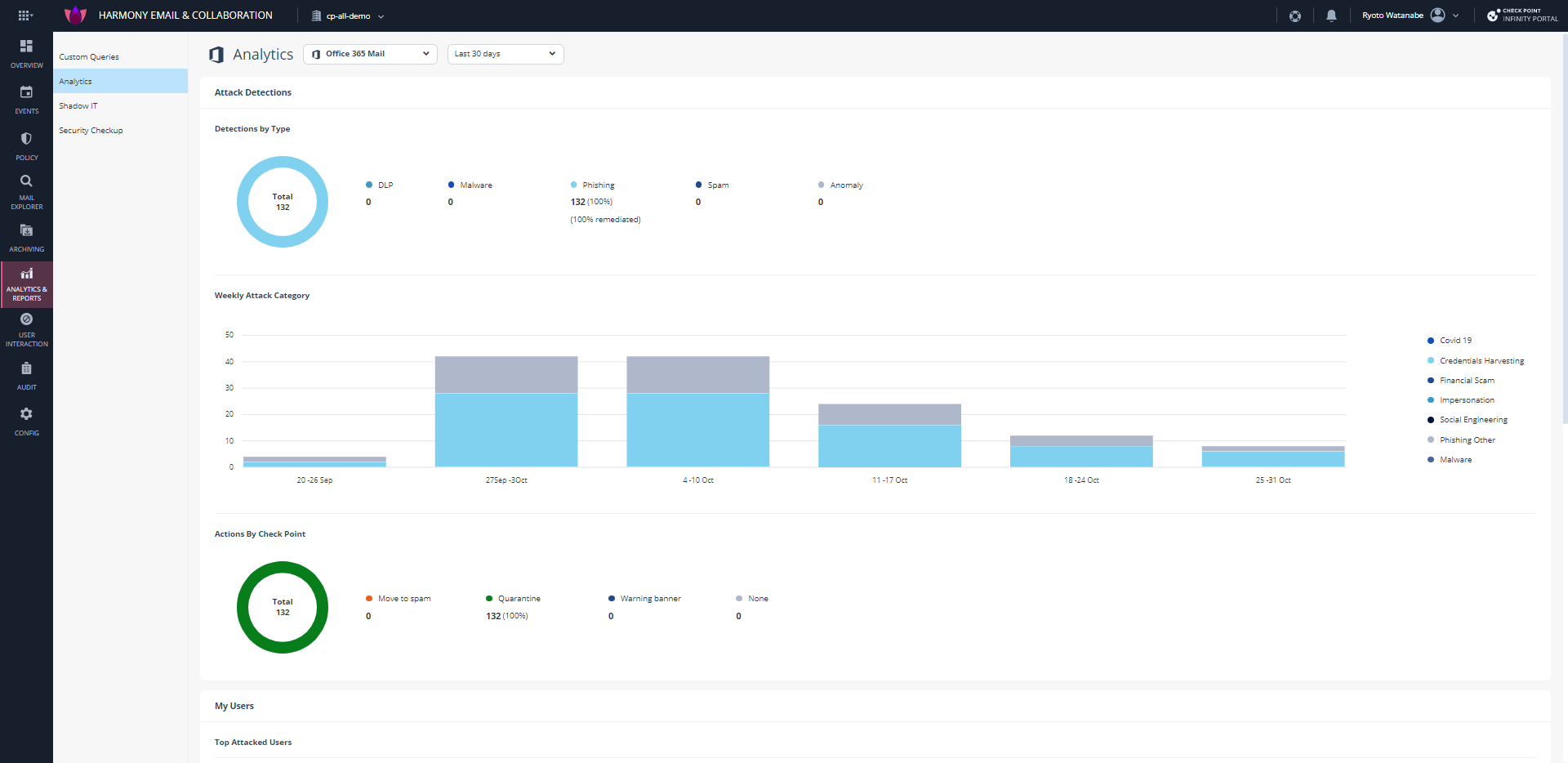
Save asから作成したクエリを保存することも可能です。

Query actionsから実施できるアクション：

* セキュリティイベントのentity IDを選択してDismiss（無視）する
* 隔離されたメールをリストア
* Spamボックスへ移動させる
* Security Event の生成
* メールの隔離
* フィッシングアラートメールの送信
* 条件をさらに追加し、セキュリティイベントを一回でDismiss（無視）する
* Email レポートの送信

**Analytics**

検知された攻撃の種類やユーザーごとに、グラフで表示することが出来ます。

■Gmail画面構成

③My Users

* Top Attacked Users
* Top attacked Departments

①SaaSアプリケーションの選択と期間の設定

①SaaSアプリケーションの選択と期間の設定：分析結果を表示させるSaaSアプリケーションの選択と、期間の指定が可能です。過去２４時間、７日、３０日、６０日、９０日から選択できます。

②Attack Detections

　・Detections by Type：検知された攻撃の種類ごとの件数を、円グラフで表示します。

　・Weekly Attack Category：１週間当たりの攻撃カテゴリを積み上げ棒グラフで表示します。

　・Actions by Check Point：Harmony Email & Collaborationによって実施されたアクションの種類と件数を円グラフで表示します。

③My Users

　・Top Attacked Users：期間中に最も攻撃メールを受信したユーザーと、その件数を表示します。

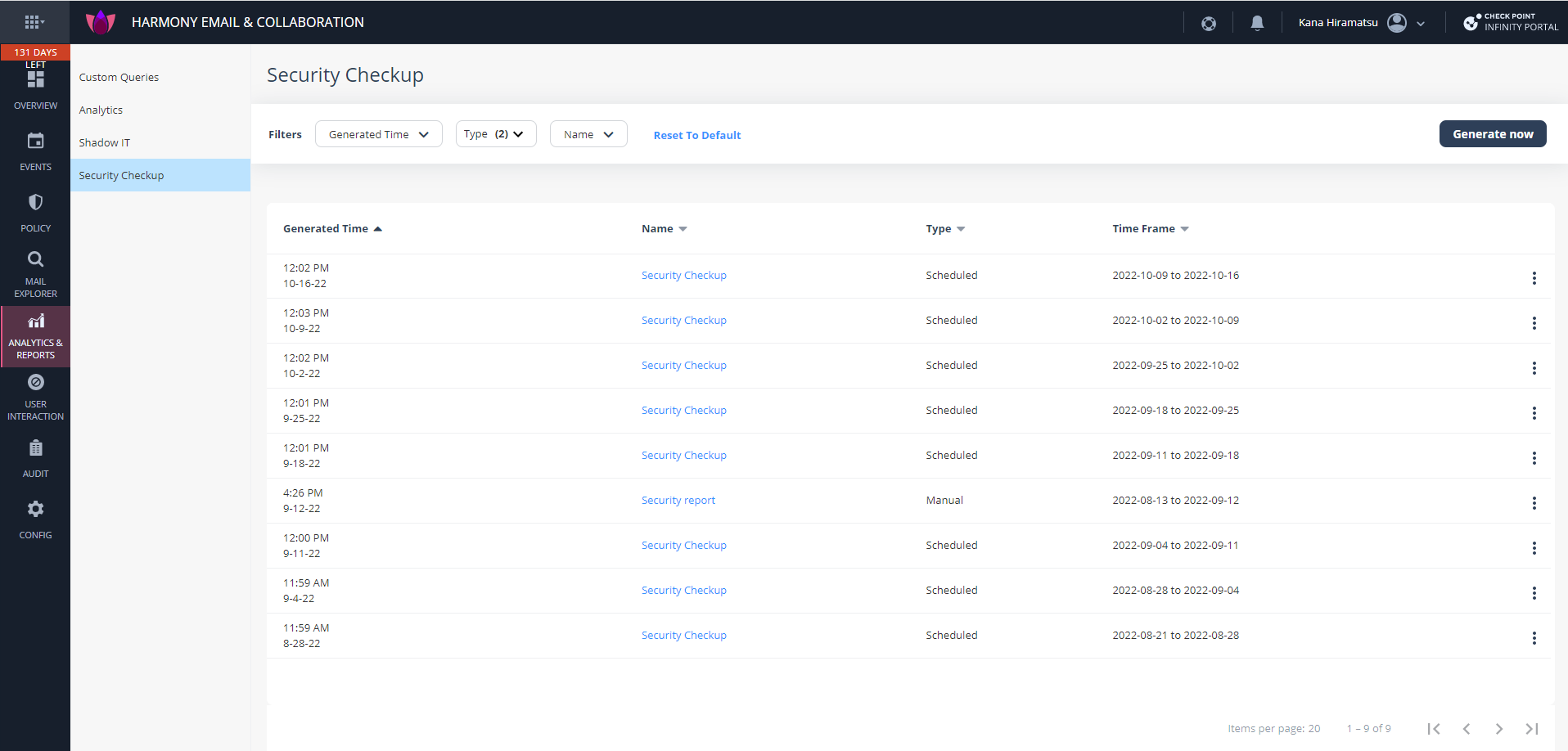
　・Top attacked Departments：期間中に最も攻撃メールを受信した部門とその件数を表示します。

**Shadow IT**

＊＊今回のPoCでは評価対象外のため、後日改めてご案内いたします＊＊

**Security Checkup**

過去に発行されたセキュリティレポートを確認したり、新たにレポートを作成することが出来ます。



②Generate now（レポートの手動作成）

③過去に作成されたレポート一覧

①Filters（レポートの検索と絞り込み）

■画面構成

①Filters：過去に作成したレポートの検索に使用します。作成時間や種類（手動/自動作成）で絞り込んだり、レポートの名前で検索することが可能です。

②Generate now：レポートを手動で新規作成することが出来ます。レポートの名前と期間を指定すると、この一覧に追加されるようになります。

③過去に作成されたレポート一覧：過去に作成されたレポートが表示されます。Filtersで絞り込みをした結果も、この一覧に表示されます。

　・Generated Time：作成時間が表示されます。過去1週間、2週間、1ヵ月の期間を指定可能です。

　・Name：レポートの名前が表示されます。押下することでブラウザ上でレポートを閲覧したり、PDFデータでダウンロードすることが可能です。

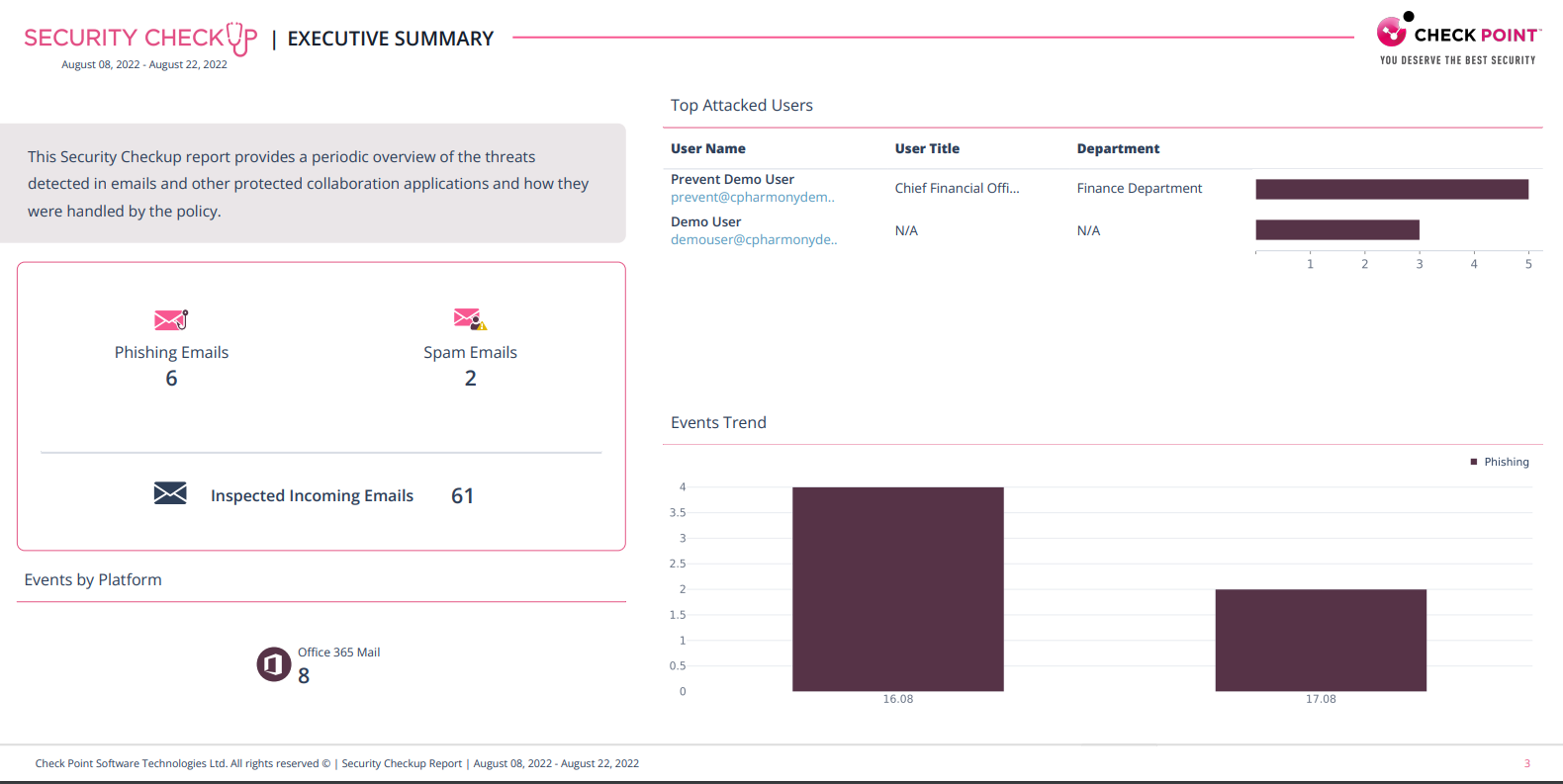
　・Type：レポートの種類（手動作成/スケジュールに基づいた自動作成）が表示されます。

　・Time Frame：レポートの期間が表示されます。

※レポートに表示されるセキュリティイベントの保管期間はデフォルトで１年間のため、過去１年間の中から１週間、２週間、１ヵ月の期間を選択してレポートを生成できます。

※１１月リリース予定機能：現在は１週間、２週間、１ヵ月のみ表示期間を選択し、レポートの生成が可能ですが、今後自由に表示期間をカスタマイズ頂けるよう、Custom Queryに本機能が追加されます。

サンプルセキュリティレポート：

****

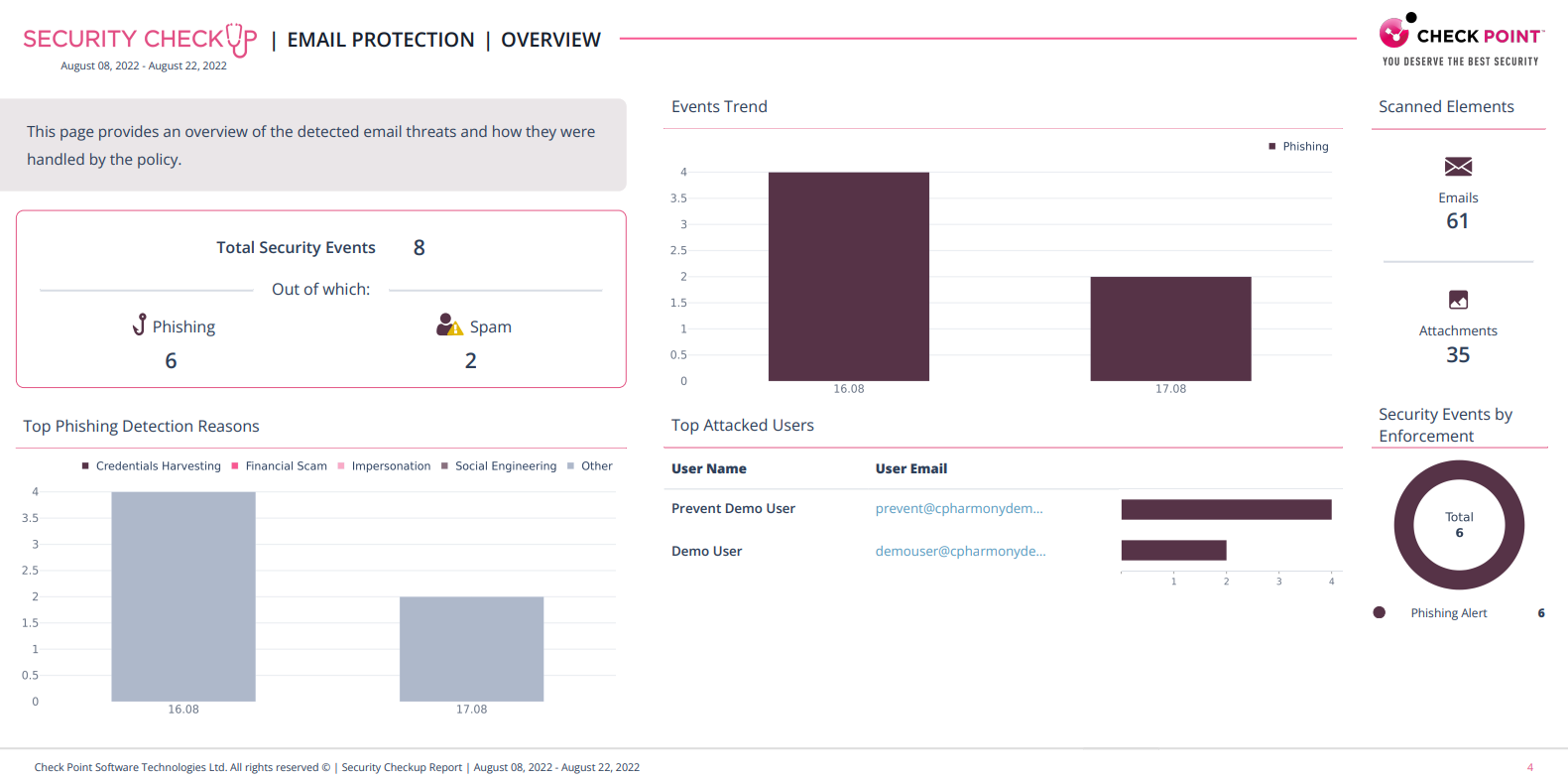
最も攻撃を受けたユーザーとその部署

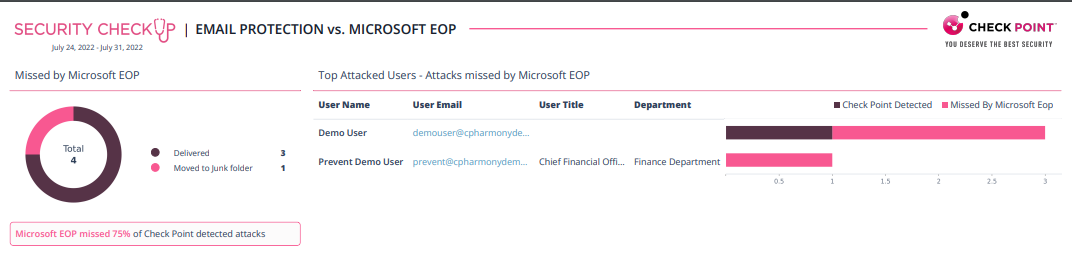
セキュリティイベント毎の

トレンド

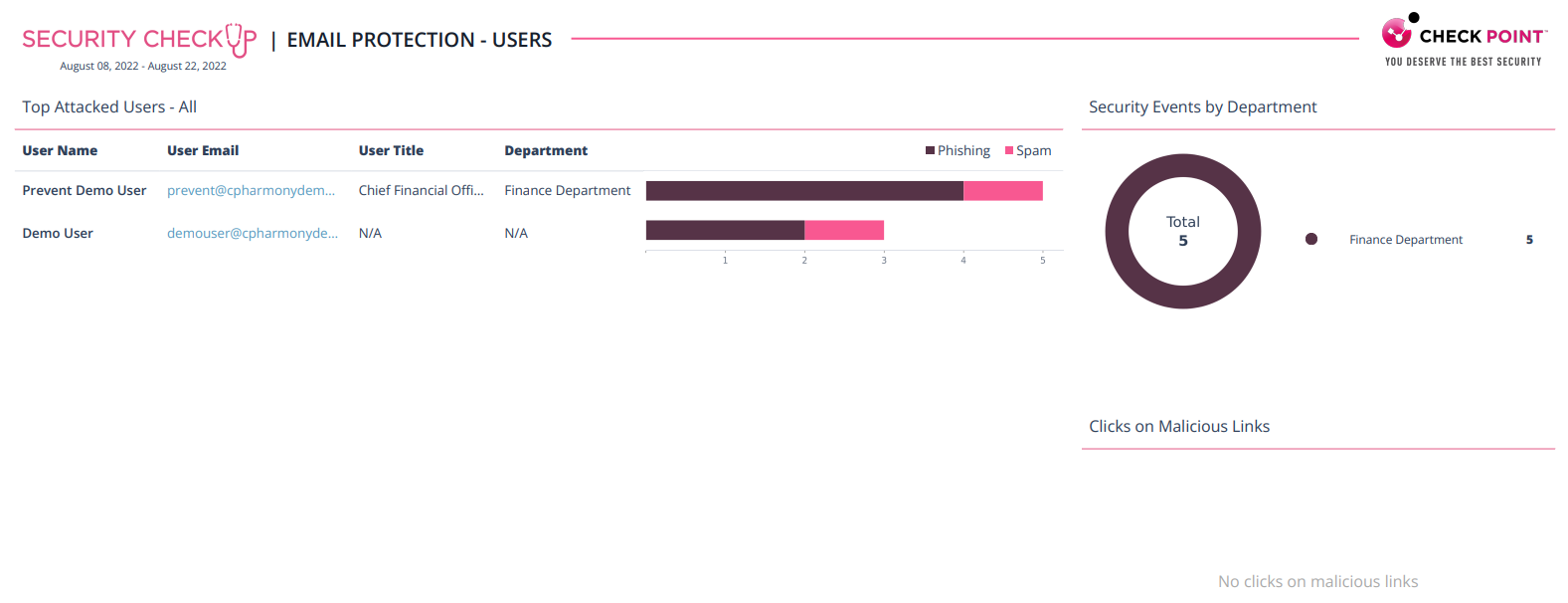
セキュリティイベントが検知された

プラットフォーム

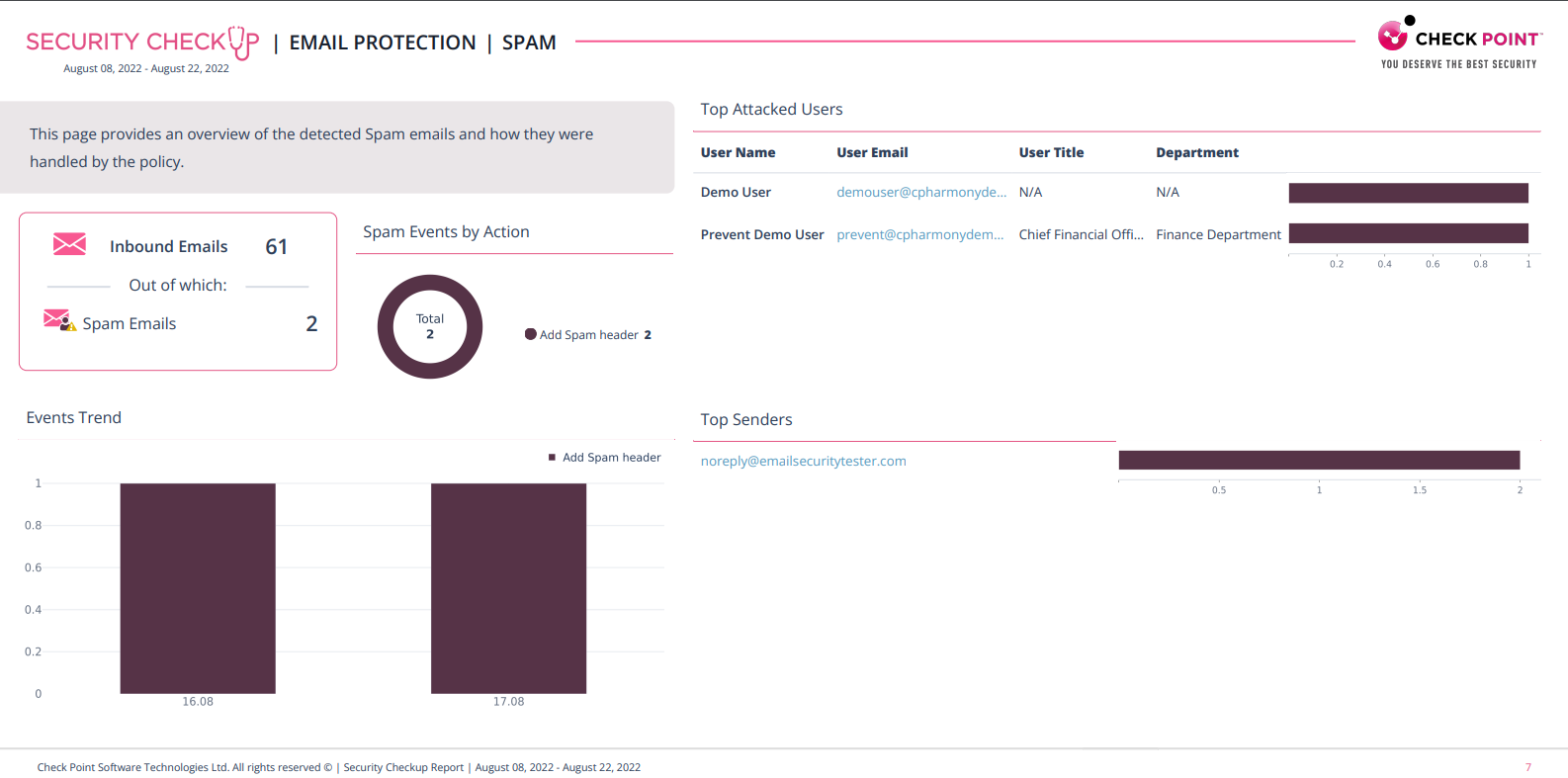
****

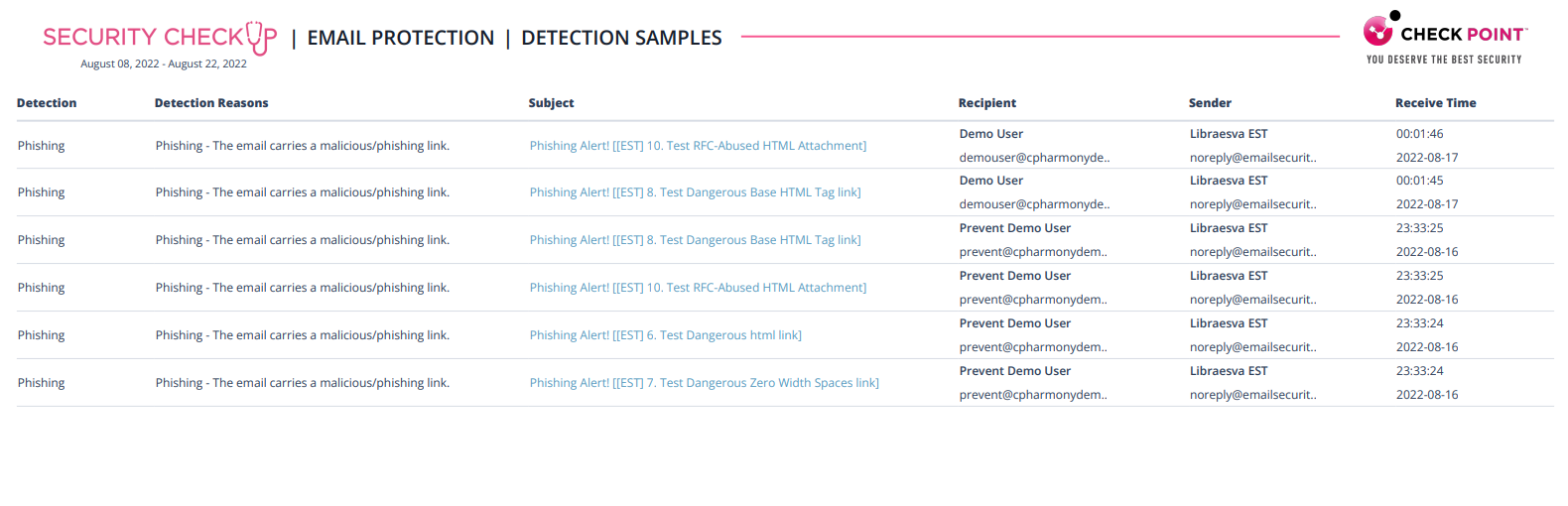
****

本製品とマイクロソフトプロテクションとの比較

****

このレポートの例ではマイクロソフトEOPを使っていた場合、75%ものセキュリティインシデントが検出できていないことを示しています

****

****

検知されたフィッシングメールの例

**■各項目の内容について**

|  |  |
| --- | --- |
| **Executive Summary** | **詳細** |
| Events by Platform | どのSaaS アプリケーションでセキュリティイベントが検知されたか |
| Top Attacked Users | 最も攻撃を受けたユーザーとそのユーザーに紐づく部署 |
| Events Trend | 攻撃の割合：マルウェア攻撃、フィッシング攻撃がどのくらい受けているか |

|  |  |
| --- | --- |
| **Email Protection** | **詳細** |
| Total Security Events | 検知されたセキュリティイベントの数：各マルウェア、フィッシング攻撃の数の割合 |
| Top Phishing Detection Reasons | HECで最も検知したフィッシング攻撃の理由 |
| Events Trend | 攻撃の割合：マルウェア攻撃、フィッシング攻撃がどのくらい受けているか |
| Top Attacked Users | 最も攻撃を受けたユーザーとそのユーザーに紐づく部署 |
| Scanned Elements | HECでスキャンを実施した要素　例：メール、添付ファイル |
| Security Events by Enforcement | HECで実施されたアクションに対してのセキュリティイベントの数（例：隔離がされたイベントの数等） |

|  |  |
| --- | --- |
| **Email Protection vs.**  **Microsoft EOP** | **詳細** |
| Missed by Microsoft EOP | MS EOPですり抜けてしまったメールの数（上記の例：75%ものセキュリティインシデントが検出できていない） |
| Top Attacked Users –  Attacks Missed by Microsoft EOP | EOPですり抜けたメールに対して最も攻撃を受けたユーザーとそのユーザーに紐づく部署 |

|  |  |
| --- | --- |
| Email Protection- Users | **詳細** |
| Top Attacked Users- All | 最も攻撃を受けたユーザーとそのユーザーに紐づく部署 |
| Security Events by Department | 最も攻撃を受けた部署 |
| Clicks on Malicious Links | 有害なリンクをクリックした回数 |

|  |  |
| --- | --- |
| Email Protection  Malware | **詳細** |
| Malware Trend | マルウェア攻撃を受けた割合 |
| Top Attacked Users | 最も攻撃を受けたユーザーとそのユーザーに紐づく部署 |
| Malware Events by Enforcement | マルウェア編：HECで実施されたアクションに対してのセキュリティイベントの数（例：隔離がされたイベントの数等） |
| Top File Types | 攻撃を最も受けたファイルタイプ |

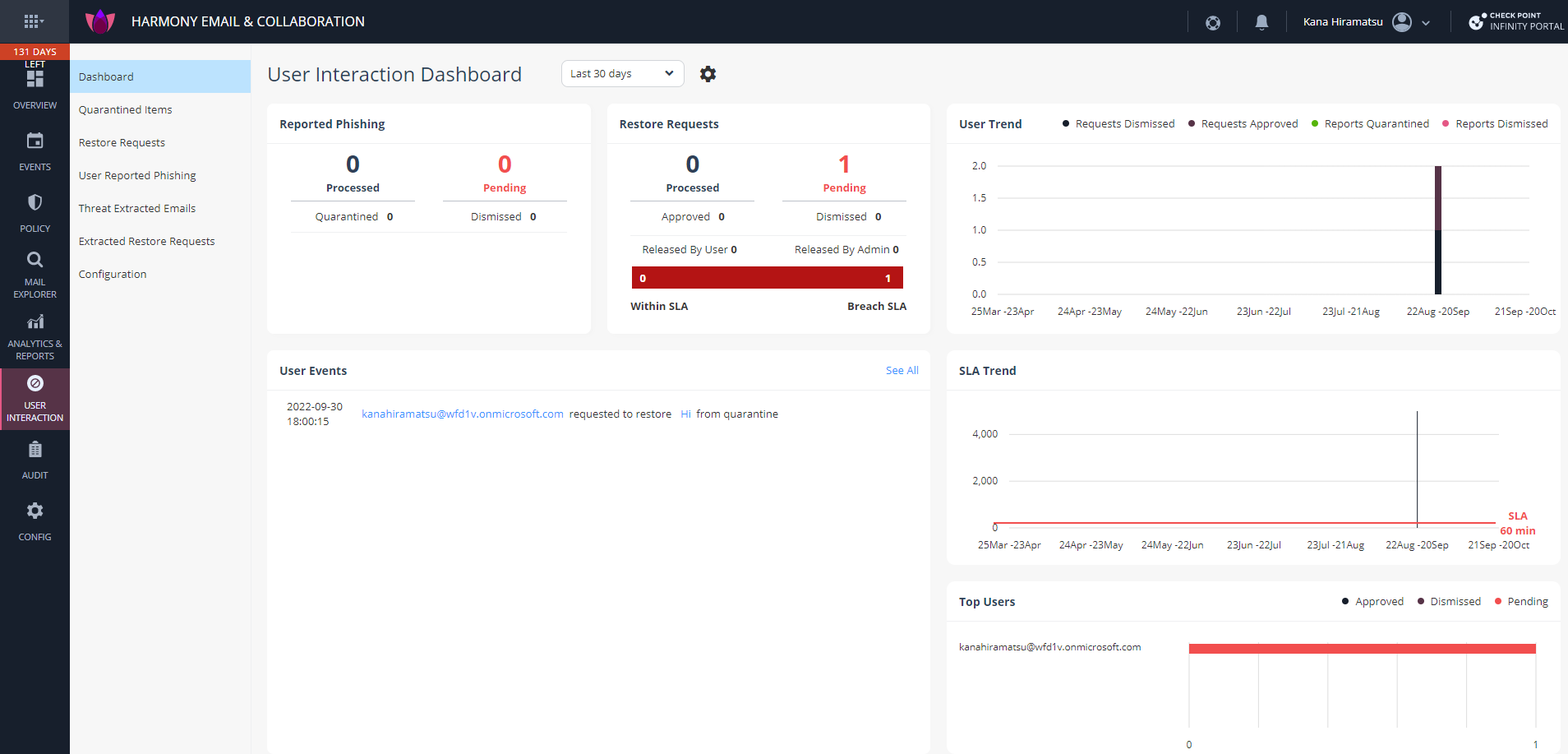
|  |  |
| --- | --- |
| Email Protection  Detection Samples | **詳細** |
| Detection Samples | セキュリティイベントとして検知されたメールサンプルの  攻撃タイプ、検知理由、メールの件名、送信者、受信者、受信時間 |

# USER INTERACTION

ユーザーからのフィッシング報告や、リストア（解放）リクエストに関する情報を確認できます。

＊＊Preventモードでの運用中に使用する機能となります。＊＊

**Dashboard**

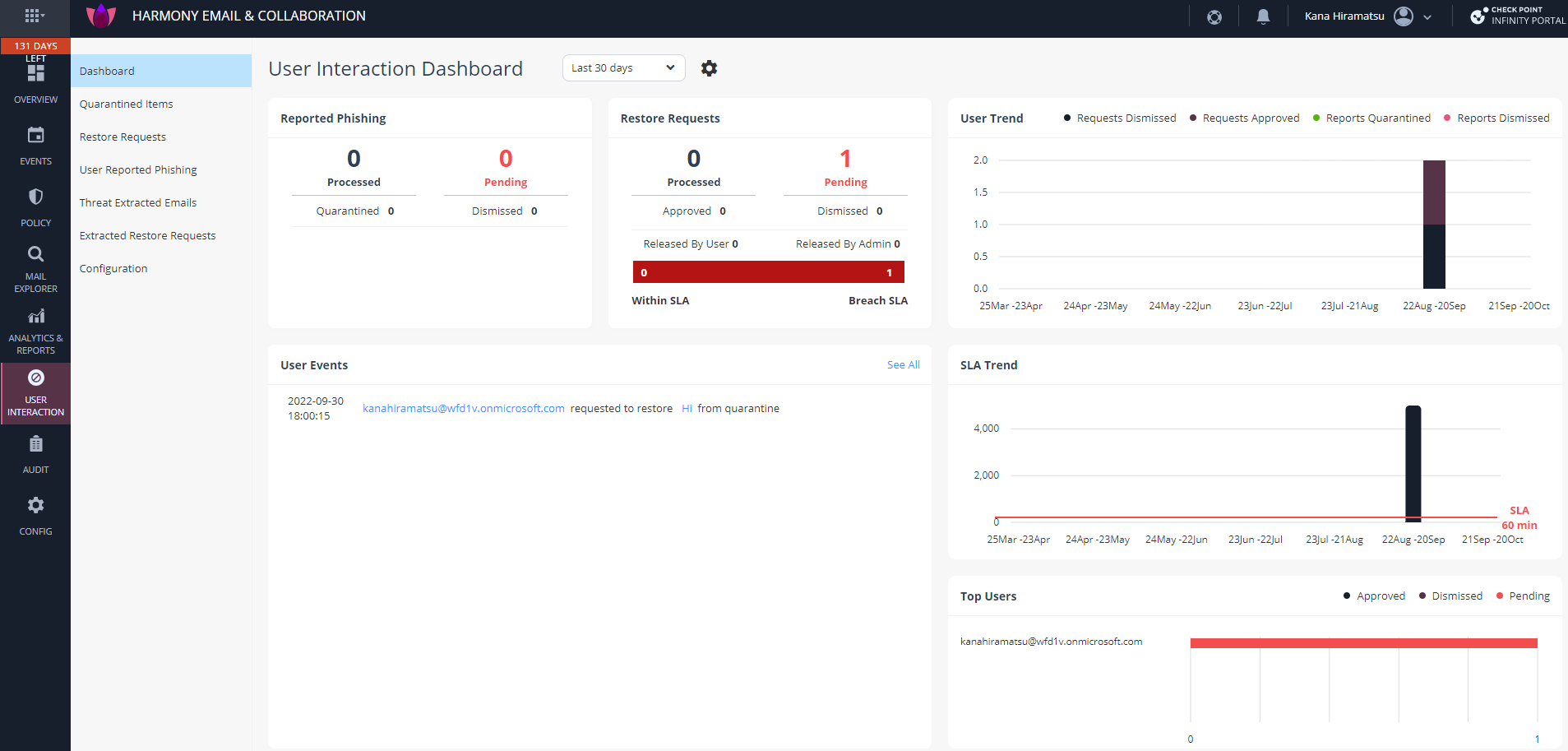


Dashboardからユーザーの操作歴のレポートをご確認頂けます。

* **Reported Phishing:** ユーザーが何件フィッシングであるとレポートし、それに対して管理者は隔離をした件数、まだPending状態の件数
* **Restore Requests:** 一度隔離されたメールに対して、ユーザーが何件自分でメールをリストアしたか、管理者がリストアを実施したかの件数、ユーザーが申請したリクエストに対して管理者がSLA内に必要なアクションを実施したか等

※SLA時間はデフォルトで１時間と設定されておりますが、自由にカスタマイズも⚙から変更可能です。

* **User Events:** ユーザーがメールのリストアをリクエストした場合、フィッシングとレポートした場合一覧として表示されます。



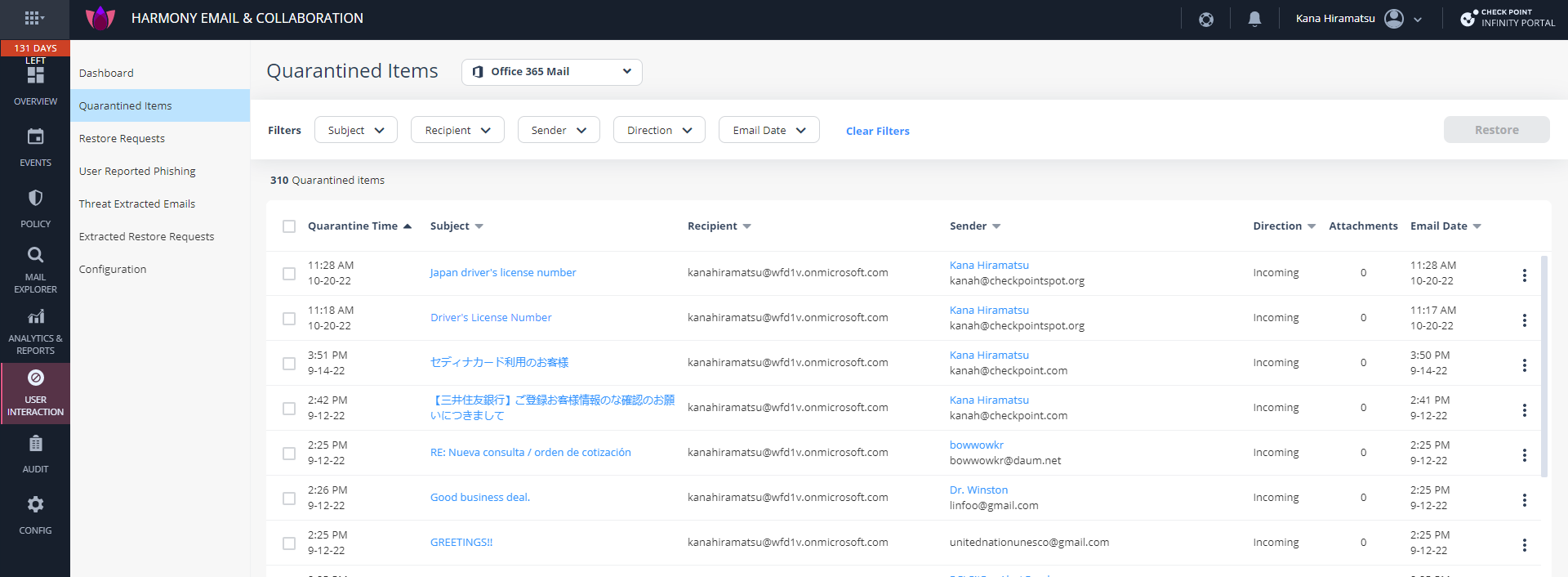
User Trend:

* **Requests Dismissed:** ユーザーが申請したリストアのリクエストが拒否された数
* **Requests Approved:** ユーザーが申請したリストアのリクエストが承認された数
* **Reports Quarantined:** フィッシングとしてユーザーがレポートしたメールに対して管理者が隔離した数
* **Reports Dismissed:** フィッシングとしてユーザーがレポートしたメールに対して管理者がDismissした数

SLA Trend: 各ユーザーが取ったアクションに対して、管理者は必要な対応がSLA内に実施しているかご確認頂けます。

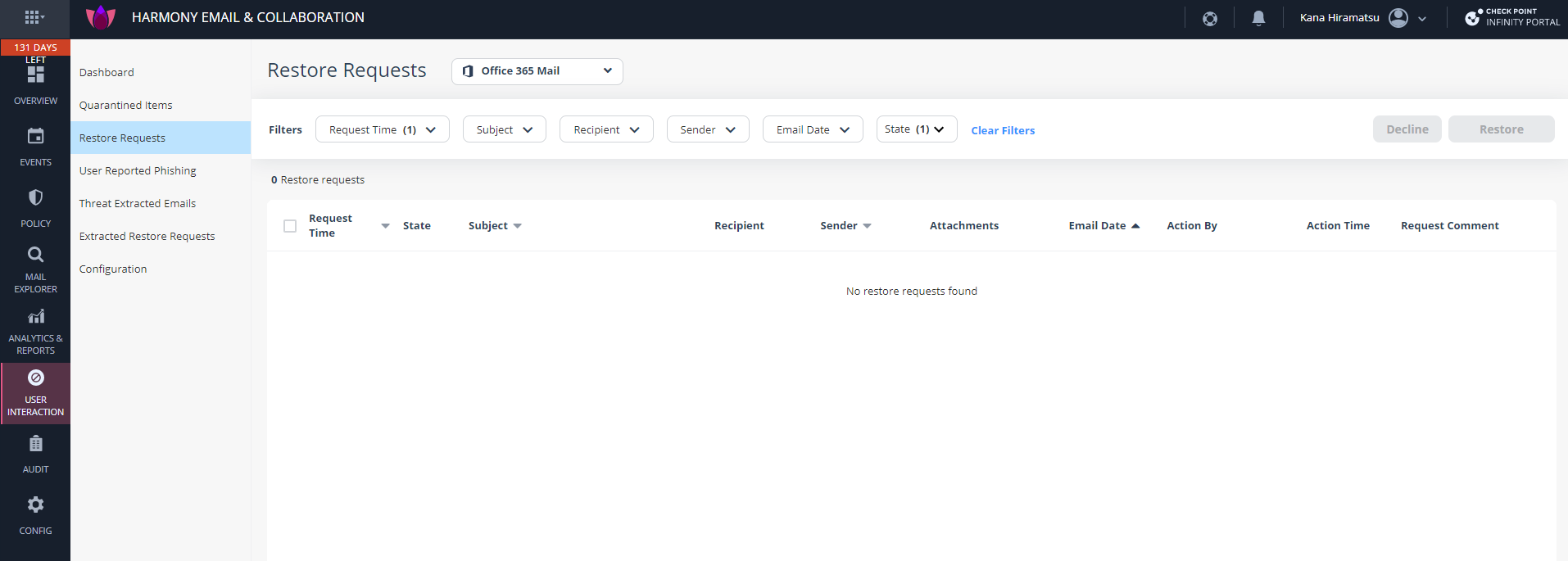
Top Users: 最もアクションを実施している管理者が、ユーザーのリクエストに対してどのような対応を実施しているかご確認頂けます。

**Quarantined Items**



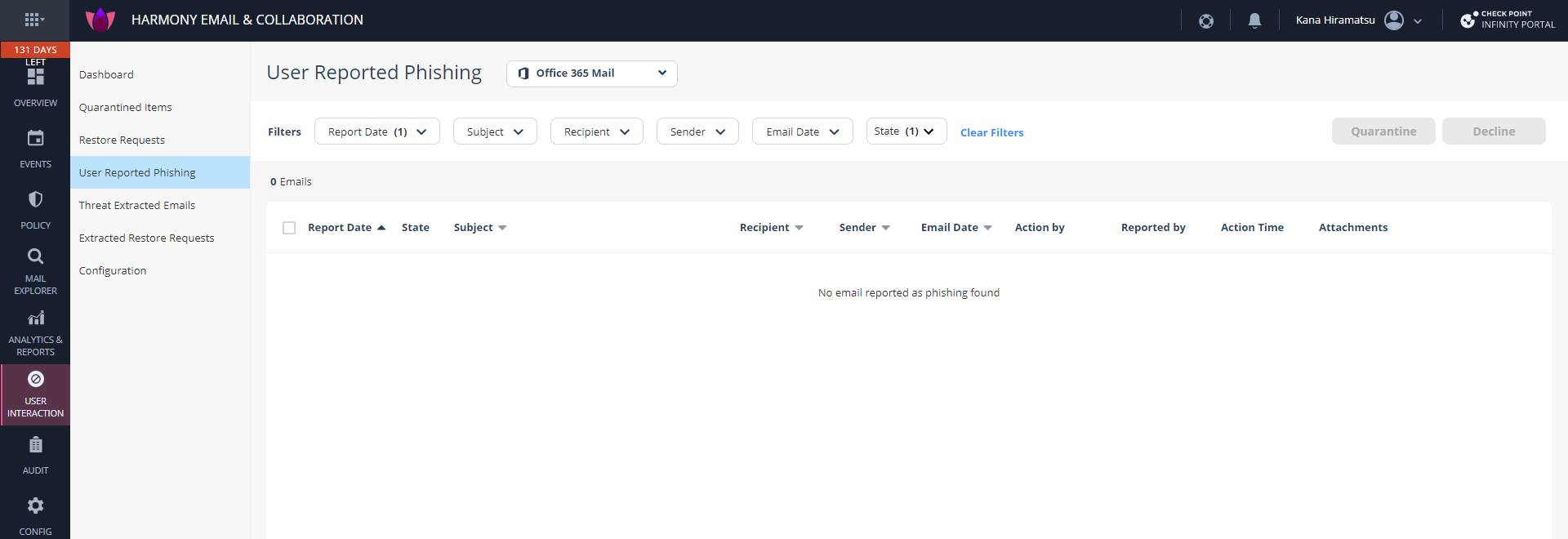
各SaaSアプリケーション毎に隔離済みのItemをご確認頂けます。囲まれている部分では隔離されているItemの中からフィルタで条件を絞って調べることができます。また、Itemを複数選択し、それらをリストアすることも可能です。選択すると、グレーアウトされているRestoreボタンを押下できるようになります。

**Restore Requests**



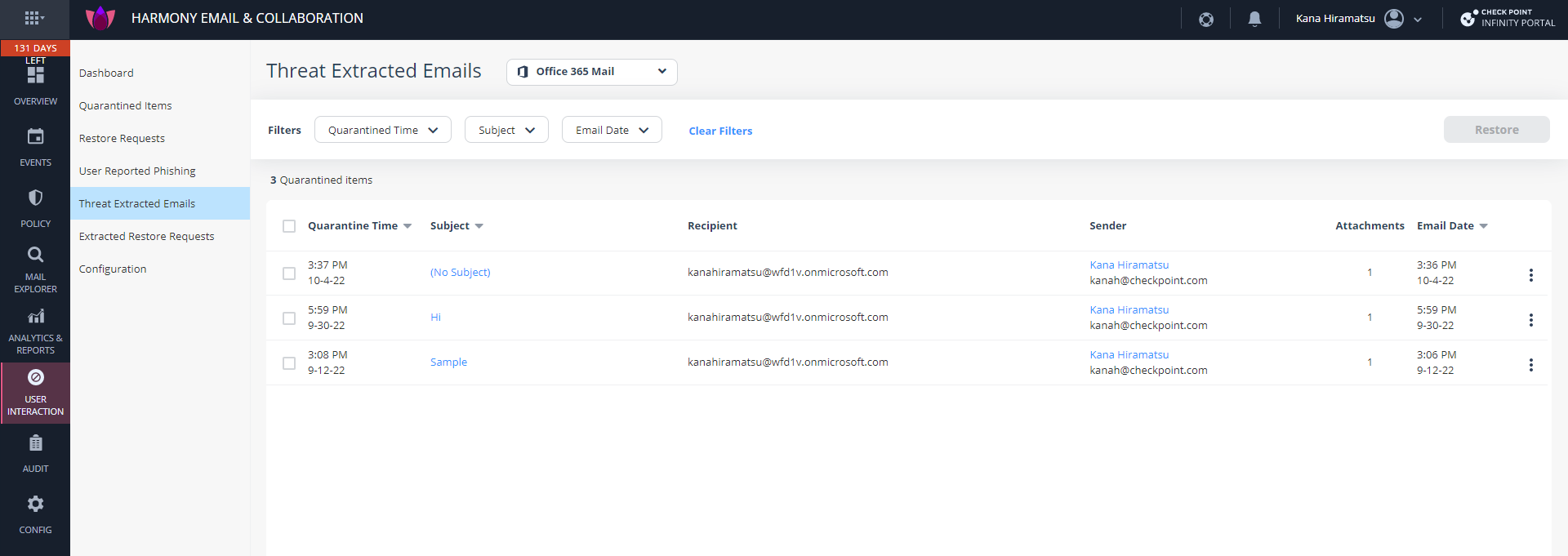
ユーザーがリクエストを申請した場合、一覧として表示されます。こちらはポリシー上、Quarantine. User is alerted and allowed to request a restore（admin must approve）のWorkflowを設定している場合のみ、表示される。ここから管理者は必要なアクションを実施して頂く。

**User Reported Phishing**

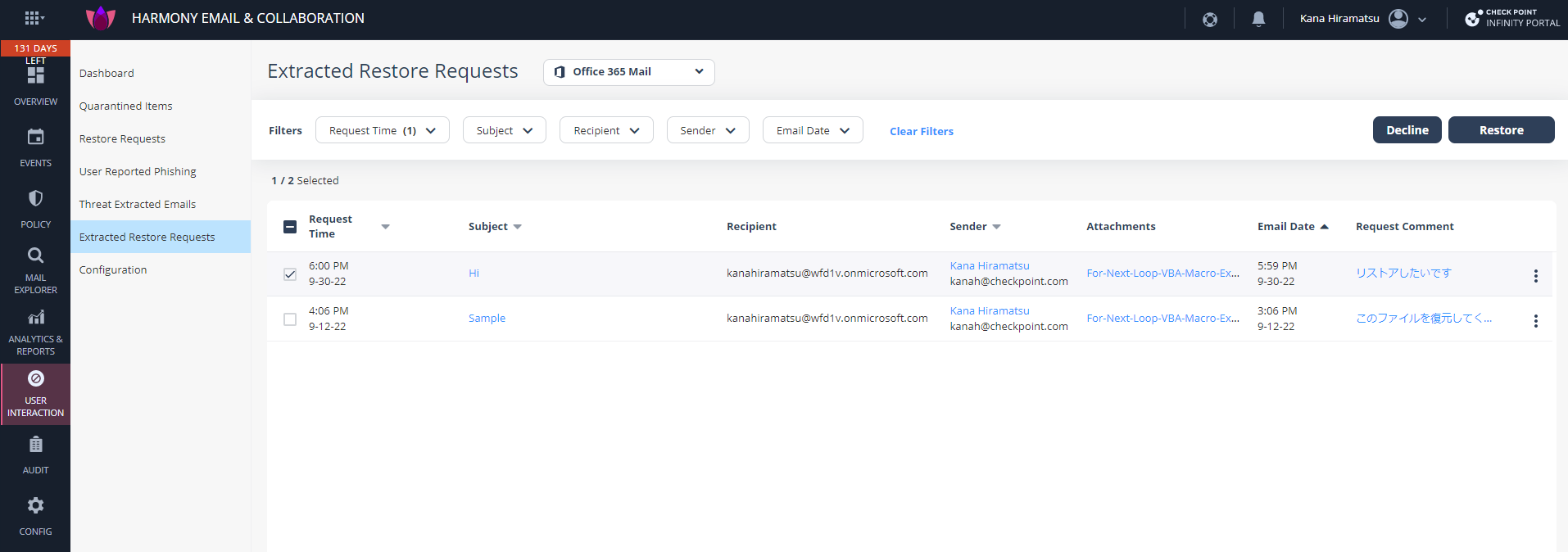


ユーザーがメールをフィッシングとしてレポートした際に一覧として表示される。ここから管理者はレポートされたメールの中身を確認し、隔離するか、レポートをDismissするか必要なアクションを実施頂きます。

**Threat Extracted Emails**

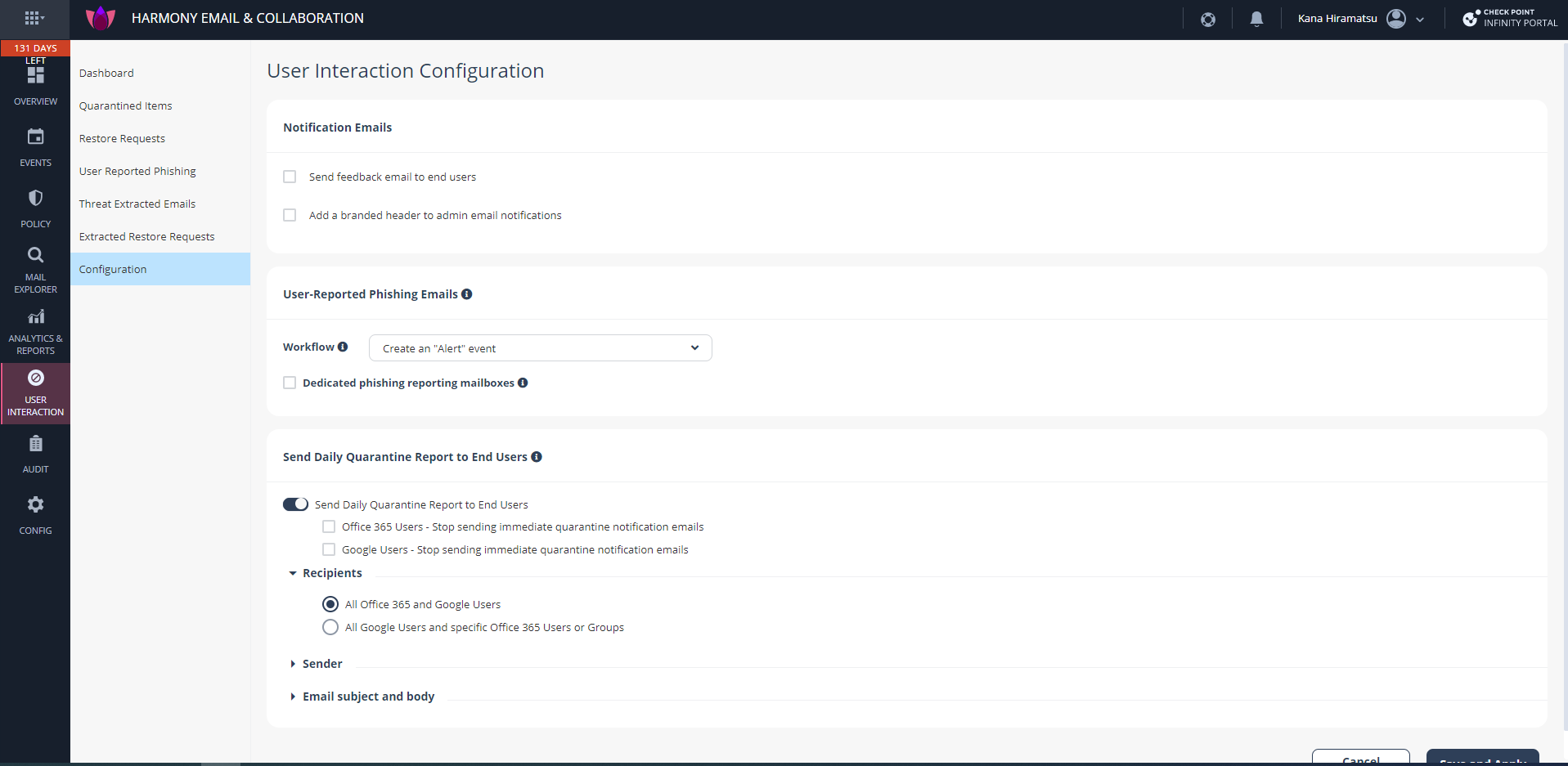


ファイル無害化がされたメールの一覧が表示されます。ここでも、メールのリストアは可能です。



一度ファイルは無害化されましたが、ユーザーの方でオリジナルファイルをリストアしたい場合、リストア申請を管理者側に送った場合に表示されます。ユーザーが記載したリストアの理由もRequest Commentセクションからご確認頂けます。また、こちらはポリシー上User is allowed to request a restore for any attachment (admin must approve)のWorkflowとして設定されている場合、一覧として表示されます。

**Configuration**



* Notification Emails

□Send feedback email to end users

チェックを入れると、管理者によるリクエスト承認または拒否が行われた際にユーザー側に通知メールが送られます。通知メールの内容はCONFIG > SaaS Applications > 該当アプリケーションのConfigureから編集できます。(Config参照)

□Add a branded header to admin email notifications

チェックを入れると、予め設定されたメールヘッダ・フッタ、ロゴ、コンタクト情報がユーザーへの通知メールに記載されます。

* User-Reported Phishing Emails

Gmail/M365のPhishing ReportやMark as Phishingの機能が使用された際のHarmony Email & Collaboration側の挙動を設定します。

-Do nothing

-Create an “Alert” event

-Create a “Phishing” event

□Dedicated phishing reporting mailboxes

チェックを入れると、メールアドレスの入力欄が表示され、入力したメールアドレスのメールボックスに届いたメールは全てPhishing Reportが発生したとみなすようになります。

* Send Daily Quarantine Report to End Users

ユーザーへ隔離メールに関する日次レポートを送ることができます。

Send Daily Quarantine Report to End Users(有効/無効)

→有効にするとさらに以下の設定項目が表示されます。

□Stop sending immediate quarantine notification emails

チェックを入れると、メール一件一件に関する日次レポートは送られなくなります。

-Recipients

日次レポートを受信するユーザーを全ユーザー、特定のユーザーまたはグループから選択できます。

-Sender

-Friendly-From name

日次レポートの送信者名を設定します。

-From address

日次レポートの送信者メールアドレスを設定します。デフォルトはno-reply@[受信者

のドメイン]となります。

-Reply-to address

日次レポートにユーザーが返信した場合の返信先メールアドレスを設定します。

-Email subject and body

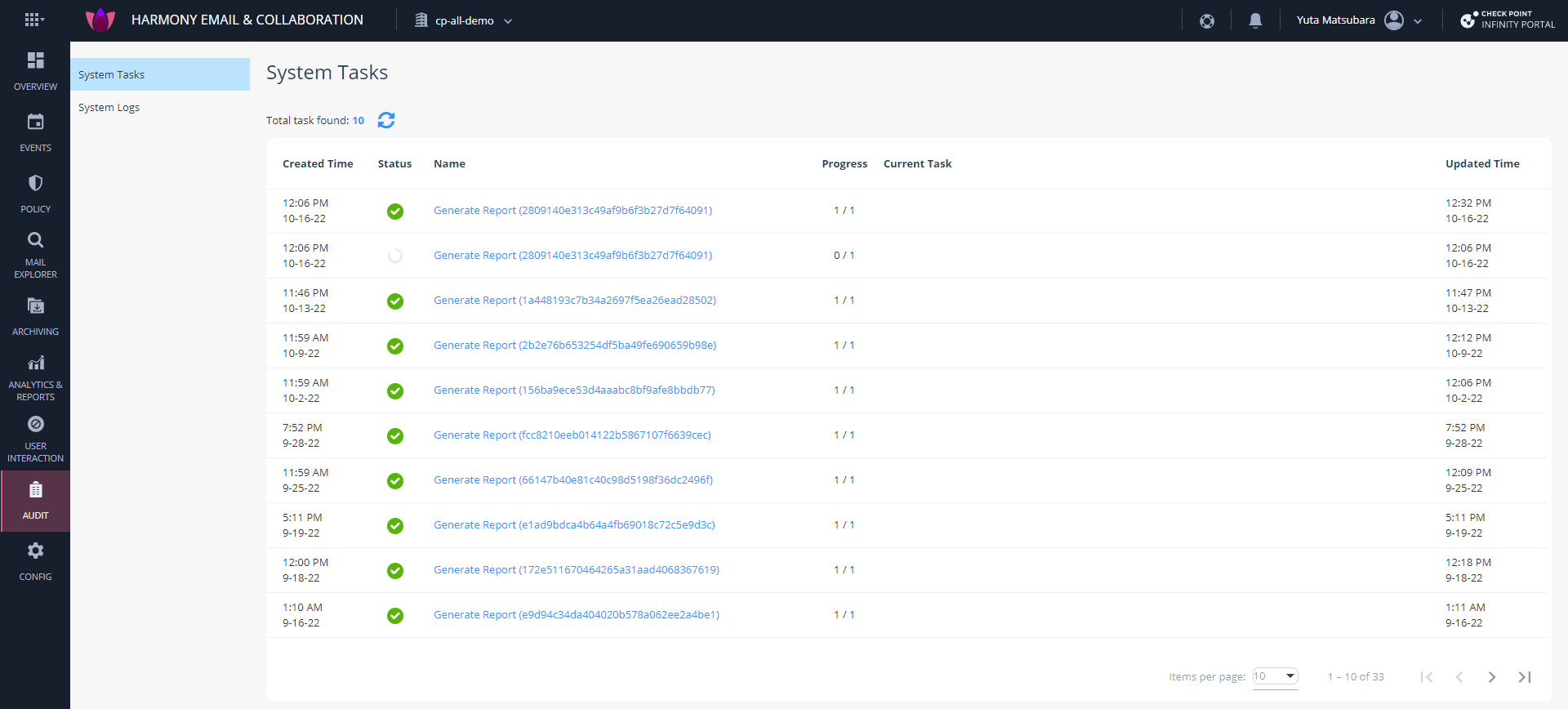
日次レポートの件名、本文をそれぞれ編集できます。

# AUDIT

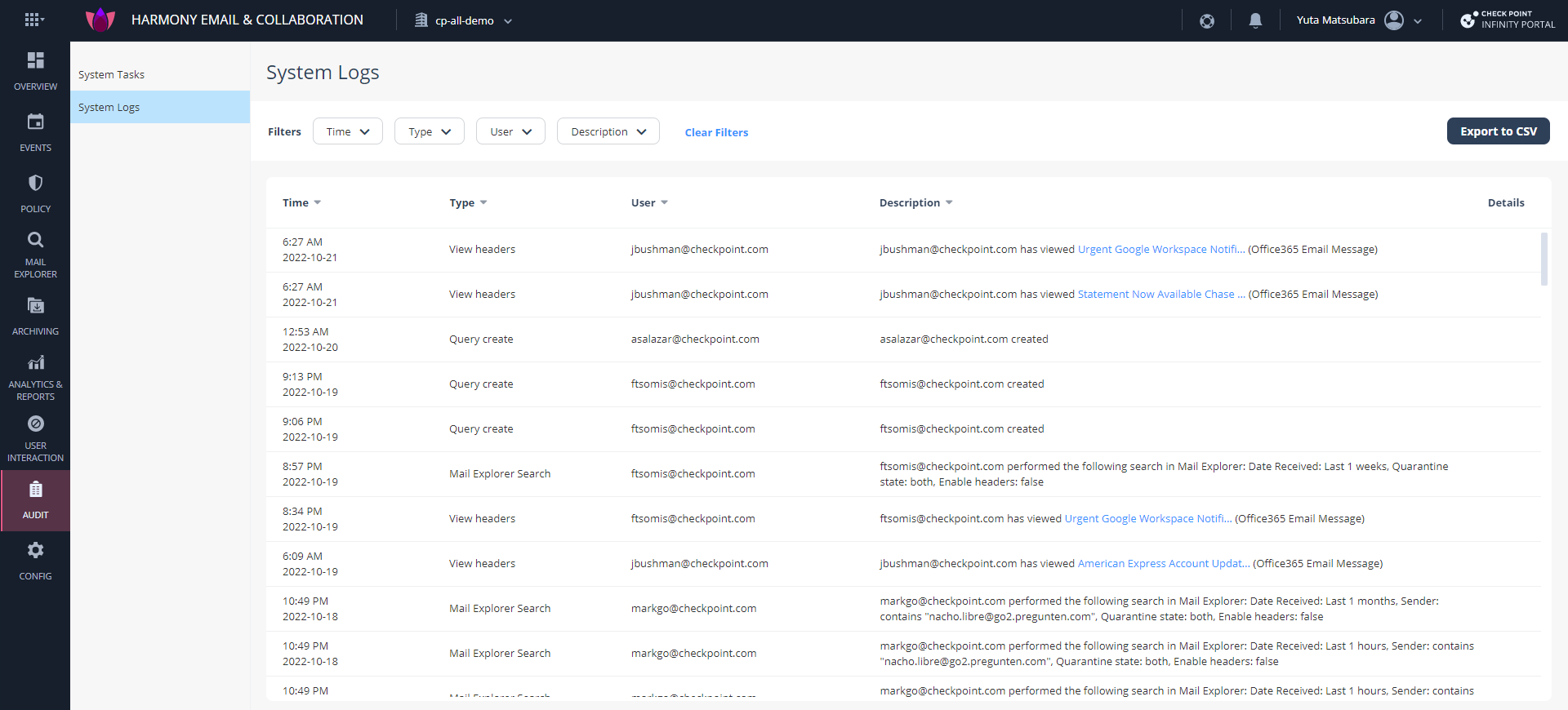
システムログを確認できます。

**System Tasks**

レポートの出力など、所要時間が長いタスクに関してその進捗状況を確認することができます。



**System Logs：**どの管理ユーザーがどのような操作を行ったのかを確認できます。



③システムログ一覧

②Export to CSV

①Filters（ログの検索と絞り込み）

■画面構成

①Filters：システムログについて、時間別、行動種別、ユーザー別、内容別にフィルタリングできます。

②Export to CSV：表示されているシステムログ一覧をCSV形式で出力します。押下すると、すぐにダウンロードが開始されます。

③システムログ一覧：Filtersの条件に一致するシステムログ一覧が表示されます。

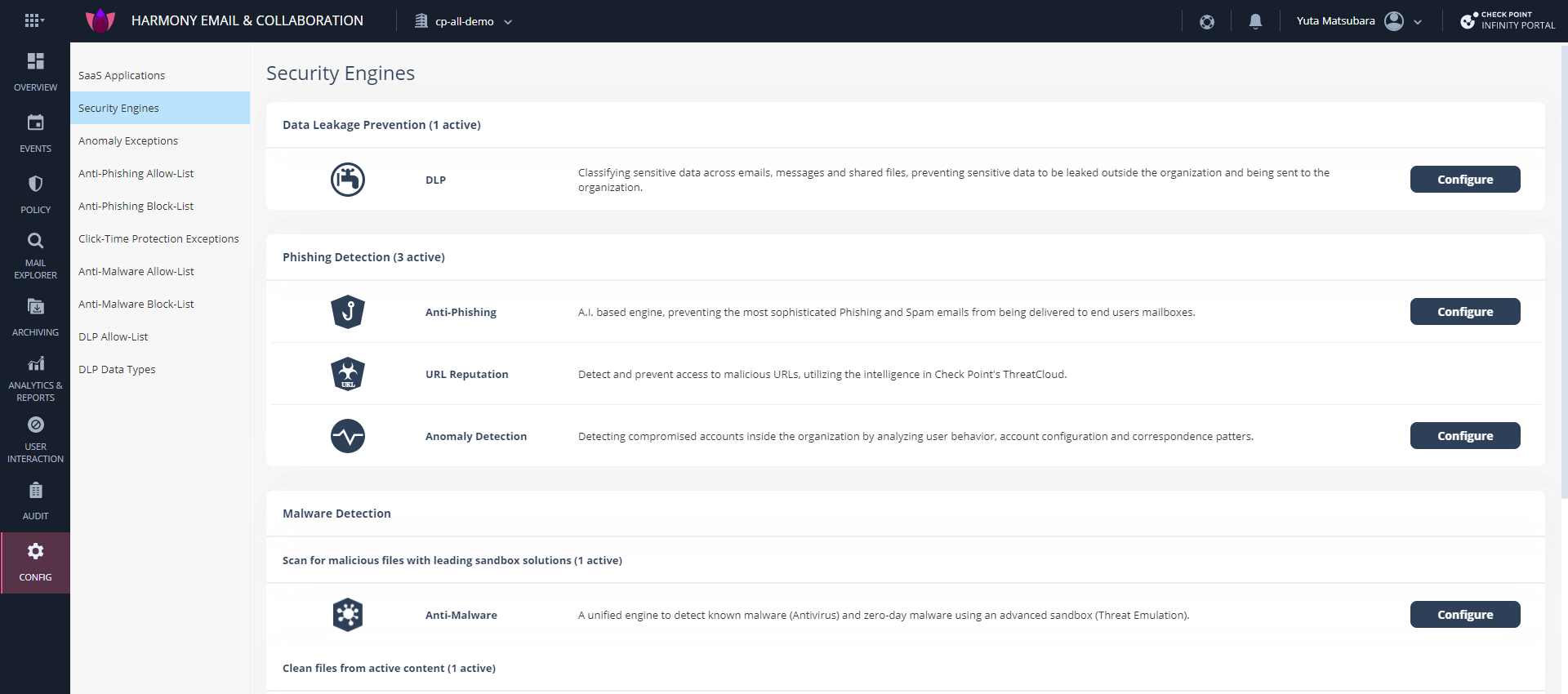
# CONFIG

各種設定を確認・変更することが可能です。

＊＊PoC期間中は、予期せぬ設定変更や誤操作を防ぐため、基本的には弊社にて承ります＊＊

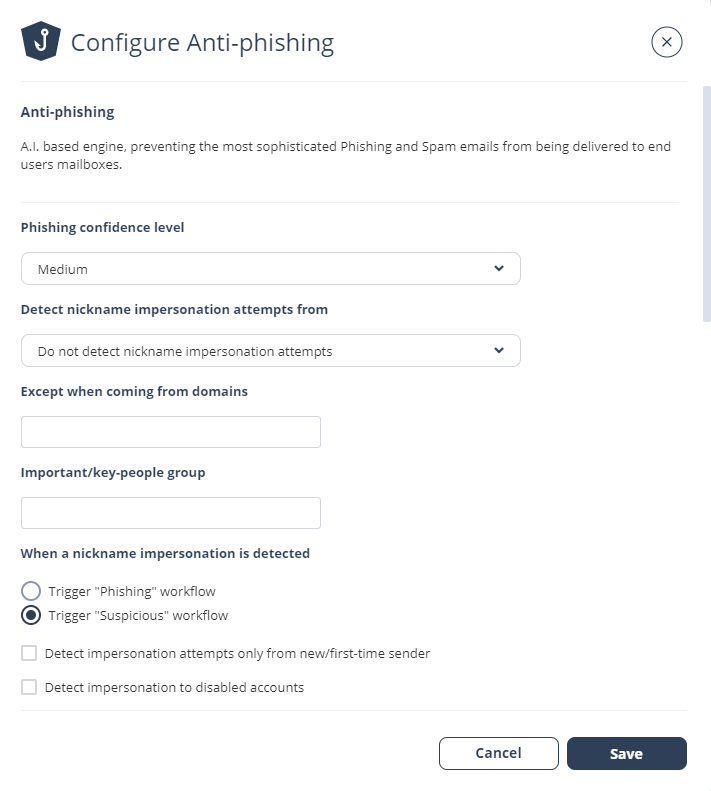
**Security Engines > Phishing Detection > Anti-Phishing**

アンチフィッシングエンジンは、Phishing、Suspicious Phishing、およびSpamの検出を担っています。この項目ではアンチフィッシングエンジンの検出における閾値などの設定を行います。



Anti-PhishingのConfigureをクリックすると、以下のウィンドウが表示されます。

Image41



以下の項目についてそれぞれ設定していきます。

* Phishing confidence level

LowestからHighestの5段階で設定します。どのconfidence levelでメールを検知した場合にPhishingとして表示するかの設定です。設定したconfidence level未満の検知についてはSuspicious Phishingとなります。デフォルトはHighです。

* Detect nickname impersonation attempts from

メール送信者名のなりすましを、どの範囲で検知するかを設定します。

-Important/key-people only

ネットワーク内の重役にのみ適用(Gmail/M365内の役職情報、および以下で指定したSecurity Group)

-Any internal user

ネットワーク内のユーザーのみに適用

-Do not detect nickname impersonation attempt

なりすましの検知はしない

* Except when coming from domains

送信者名なりすまし検知におけるホワイトリストの設定です。ドメイン名を指定します。”,”で区切ることで複数のドメインを指定できます。(大文字、小文字は区別されます)

例) domain1.co.jp, domain2.co.jp

* Important/key-people group

デフォルトでGmail/M365内の役職情報を引き継ぎますが、Security Groupを指定することもできます。Security GroupはGroup名もしくはGroupアドレスで指定できます。(大文字、小文字は区別されます)

* When a nickname impersonation is detected

送信者名のなりすましを検知した場合の挙動について、POLICYで設定したPhishing、またはSuspicious Phishingのどちらかのworkflowを選択します。

-Trigger “Phishing” workflow

-Trigger “Suspicious” workflow

□Detect impersonation attempts only from new/first-time sender

チェックを入れると初めて検出された送信者のみが検知されます。過検知を防ぐことに役立ちます。

□Detect impersonation to disabled accounts

チェックを入れると無効にしたGmail/M365アカウントのなりすましも検知されます。

□Detect impersonation to deleted accounts

チェックを入れると削除されたGmail/M365アカウントのなりすましも検知されます。

□Include suspected self-impersonation in impersonation-detection algorithm

受信者と同じ名前の送信者名はなりすましでない可能性が高いため、デフォルトでは検知しないようになっています。チェックを入れると受信者と送信者名が同じ場合も検知対象となります。

□Allow end users to whitelist senders they trust via in-mail link

チェックを入れると、POLICY内のworkflow設定で「User receives the email with a warning」が選択されている場合に、受信者はメール本文内の「Do you trust this sender – Yes/No」の項目でYesをクリックすることで、その受信者用のホワイトリストを作成できるようになります(SPFチェックを通過したメールのみ対象) 。また、このユーザーのYes/Noの選択はHarmony Email & Collaborationの機械学習に用いられます。

* SMTP host/s acting as Mail Transfer Agent/s (MTA)

Gmail/M365の前に置いているMTAのDNS名、またはIPアドレスを入力することで、送信者IPアドレスをより正確に認識し、SPFチェックをより正確に行うことができます。”,”で区切ることで複数の入力が可能です。

□ Enable phishing protection for disabled email accounts

チェックを入れると、無効にしたGmail/M365アカウントへのメールも検知するようになります。

* When a newly registered domain sends an email, apply the following workflow

新たに登録されたドメインからメールが送られてきた場合の挙動をPOLICY内のPhishing、Suspicious Phishing、または動作なしという選択肢から指定します。

-Do nothing

-Trigger “Suspicious” workflow

-Trigger “Phishing” workflow

* Minimum age of newly registered domain (in days)

何日以内に登録されたドメインを上記のnewly registered(新たに登録された)として判断するのかを、日単位で指定します。

* Allow-List Settings(Microsoftのみ対象)

□ Allow-List emails that are allow-listed by Microsoft (SCL = -1) also in Check Point

Microsoftでは、ホワイトリストで指定された対象のメールのメールヘッダにplacing SCL=-1と記載されます。チェックを入れることでSCL=-1となっているメールを全て自動的に許可するようになります。Microsoft上で厳重な設定を敷いている場合に有用な設定項目です。

* Enforce the following workflow on DMARC failed emails, with action = reject/quarantine

DMARCのメール認証を通過できず、且つaction=reject/quarantineとなっている場合にHarmony Email & Collaborationが取る挙動を指定します。POLICY内で設定したSuspicious Phishing、Phishing、または何もしないという選択肢から指定します。

-No extra action

-Trigger “Suspicious” workflow

-Trigger “Phishing” workflow

* Mark incoming emails with encrypted attachment as

暗号化された添付ファイル付きのメールについては別途Confidence levelを設定することができます。他のメールと同じConfidence levelに設定することもできます。

-Normal mode – act according to confidence level

-“Phishing” for all such emails

-“Suspicious” for all such emails

-“Phishing” if confidence level is ”Lowest” or “above”

-“Suspicious” if confidence level is ”Lowest” or “above”

-“Phishing” if confidence level is ”Low” or “above”

-“Suspicious” if confidence level is ”Low” or “above”

-“Phishing” if confidence level is ”Medium” or “above”

-“Suspicious” if confidence level is ”Medium” or “above”

□Enable phishing detection for internal-to-internal emails

チェックを入れると、ネットワーク内部間のメールも検査します。

□Follow file sharing links

チェックを入れると、ファイル共有用URLリンクも検査するようになります。

* Mark emails from your domain(s) as phishing when

受信者と同じドメインから送信されてきたメールを、特定のSFPチェック結果に応じて必ずフィッシングとして検知できるようにします。どのようなSFPチェック結果の場合にフィッシングとして検知するかを以下から指定します。

-No extra action

-SPF=Softfail OR SPF=Fail

-SPF=Fail

-SPF<>Pass

* Spam confidence level

スパムメールに対するConfidence levelを設定します。指定したConfidence levelを超えた場合にスパムメールとして判断されます。

□Match nicknames by email address

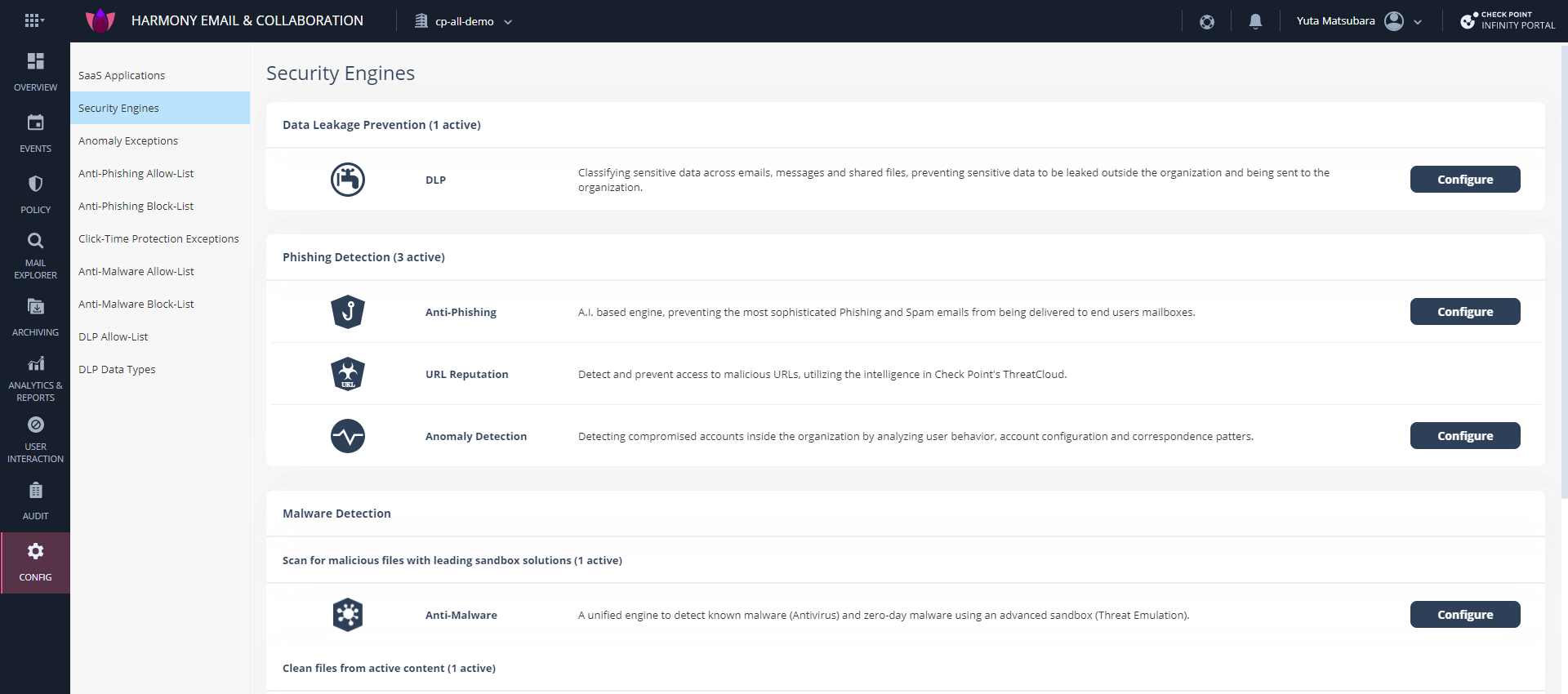
チェックを入れると、受信メールのFrom項目に送信者名の情報が入っていない場合に、メールアドレスと一致する送信者名情報が過去のメールから紹介できればそれを表示させます。

□Treat marketing emails as spam

チェックを入れると、マーケティングメールを識別してそれをスパムメールとして扱います。

**Security Engines > Phishing Detection > Anomaly Detection**

異常検知エンジンは、組織内部で乗っ取られてしまったアカウントを、振る舞いなどのパターンマッチングによって検知します。



□Email anomaly alerts to admins

チェックを入れると、異常検知エンジンが脅威を検知した場合に管理者にメールで通知します。

□Allow distribution list massive emails

チェックを入れると、Distribution List・Mailing Listを使用した多数のメールに関しては異常検知エンジンによるけんさを行わないようになります。

□Enable Intra-Country geo-suspicious events

チェックを入れると、不可能な距離間でログインが短期間に連続して発生した場合、その複数の位置情報が同じ国内であっても異常として検知します。

**Anti-Phishing Allow-List**

アンチフィッシングエンジンは、許可リストとブロックリストの定義をサポートしています。

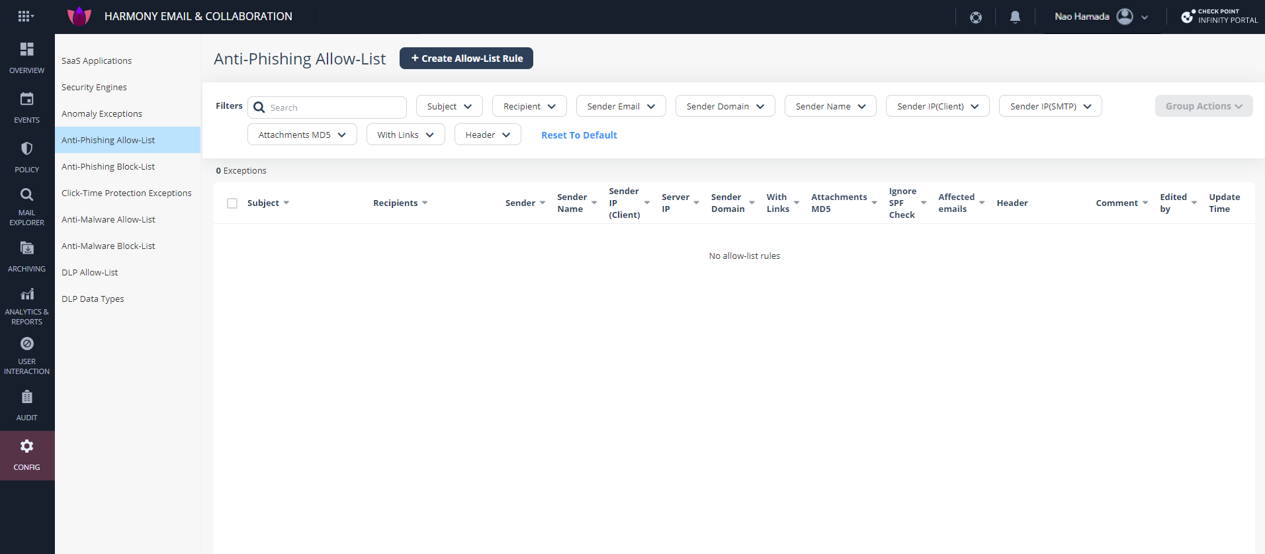
アンチフィッシングエンジンは、Allow-ListまたはBlock-Listのルールに一致するメールのスキャンを停止します。アンチフィッシングの判定は、自動的にクリーン（Allow-Listの場合）またはフィッシング／フィッシングの疑い／スパム（Block-Listの場合）になります。

注 - フィッシング対策の許可リストとブロックリストのメールは、マルウェア対策やDLPなど、他のセキュリティエンジンによって評価されます。

Allow-List、Block-Listのルールは以下の方法から追加できます。

* Anti-Phishing Allow-List / Block-List

CONFIG > Anti-Phishing Allow-List もしくは CONFIG > Anti-Phishing Block-List  
Filterから、メールをフィルタリングするための基準を定義し、検索をクリックします。  
フィルタリングの条件を絞り込んでから、［Create Allow-List Rule］をクリックして許可リスト規則を作成するか、［Create Block-List Rule］をクリックしてブロックリスト規則を作成します。必要に応じて、「コメント」にルールの説明を入力し、「OK」をクリックします。



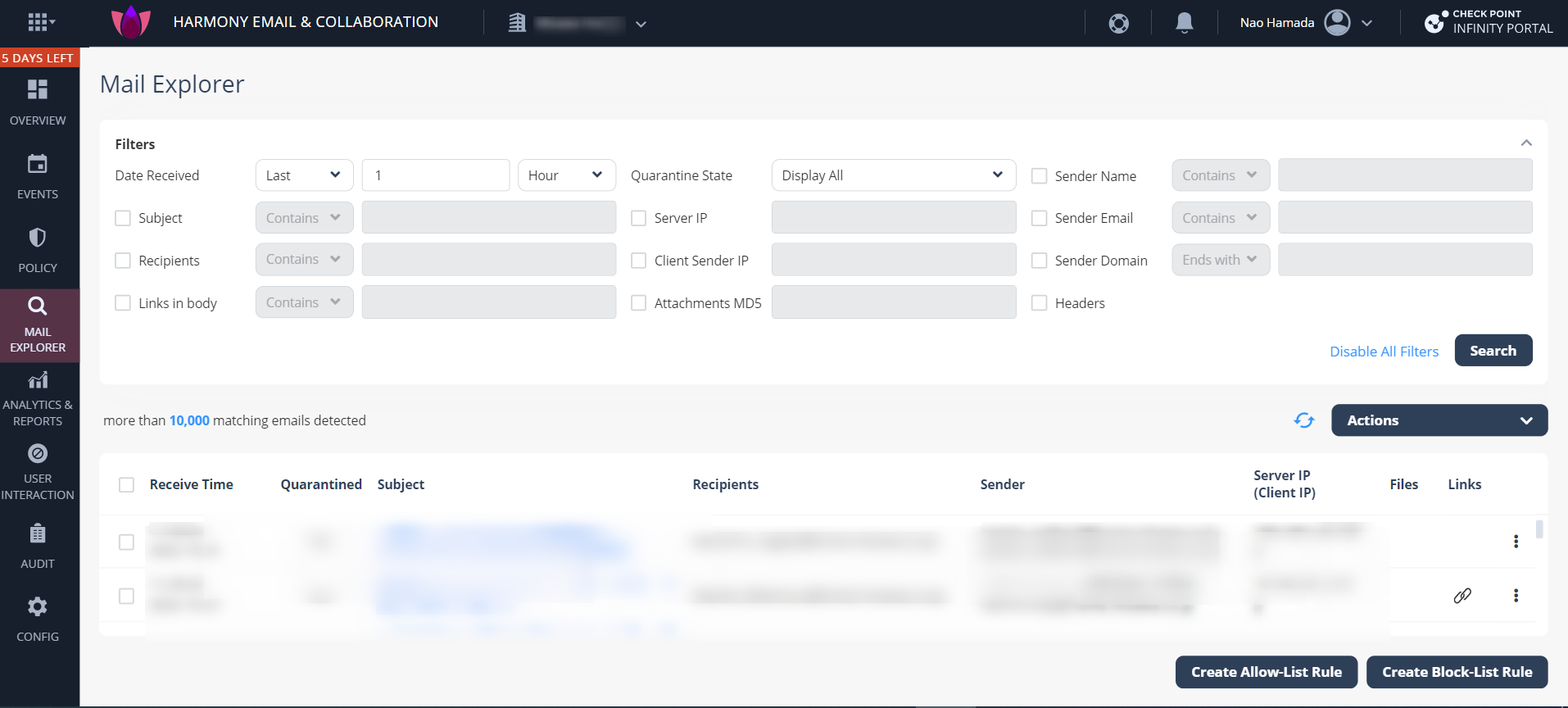
* Emailプロフィールページから  
  設定したいメールプロフィールを開きます。  
  「セキュリティスタック (**Security Stack**) 」で、「類似メール／ルールの作成 (**Similar Emails / Create Rules**) 」を選択します。

「フィルタ (**Filters)** 」で、メールをフィルタリングする条件を定義し、「検索(**Search**)」をクリックします。

メールの条件を絞り込んでから、「許可リスト規則の作成 (**Create Allow-List Rule)** 」をクリックして許可リスト規則を作成するか「ブロックリスト規則の作成 (**Create Block-List Rule)** 」をクリックしてブロックリスト規則を作成します。

必要に応じて、「コメント (**Comment)** 」にルールの説明を入力し、「OK」をクリックします。

* MAIL EXPLORERから

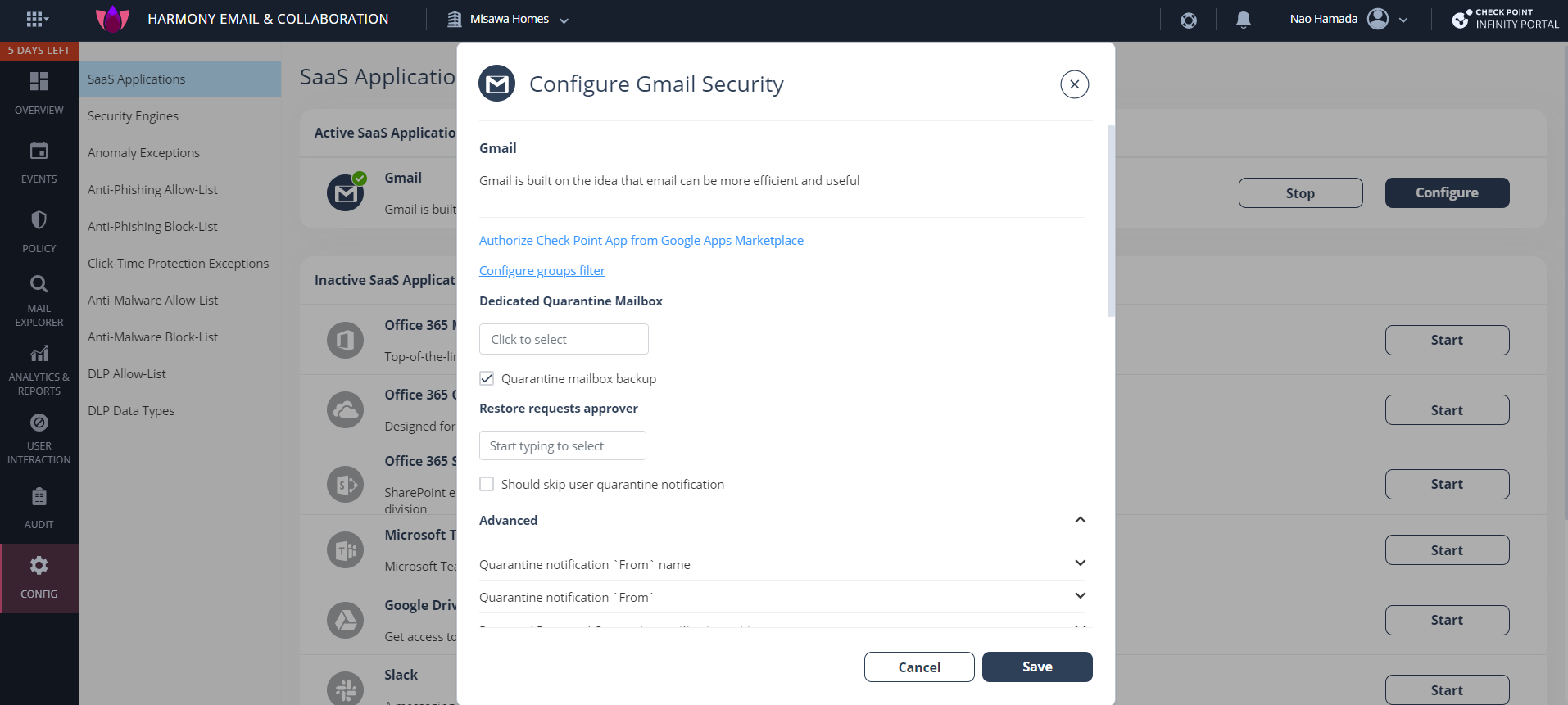


定義された条件に一致するメールをクリーンとマークするAllow-Listルールを作成するには、フィルターを選択し、Allow-Listルールの作成をクリックします。

定義された条件に一致するメールをブロックするBlock-Listルールを作成するには、フィルターを選択し、Create Block-List Ruleをクリックします。

※受信日および、隔離状態のフィールドで定義された検索条件は、どのルールにも適用されません。  
フィッシング対策のAllowListに入っていても、メールはマルウェアやDLPのためにはスキャンされます。

**SaaS Applications > Configure**

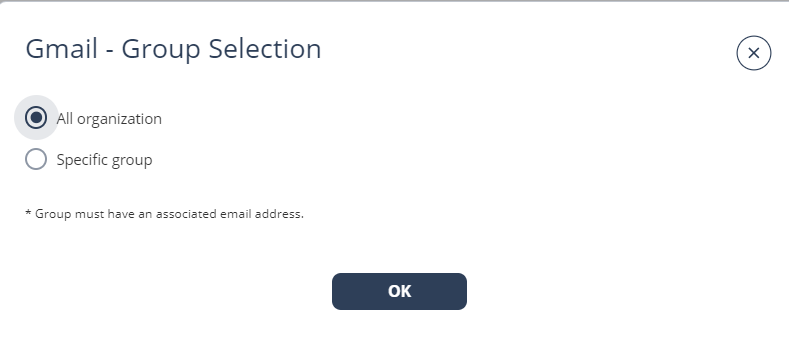


SaaSアプリケーションそれぞれの詳細設定や、Onboardに失敗した際の再認証ができます。

Authorize Check Point App from Google Apps Marketplace

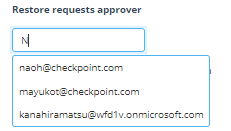
注: Linkは、新しいタブで開いてください。Googleのログイン画面が開きます。

Gmail - Group Selection



選択したユーザーグループに含まれる全てのユーザーが、課金対象としてカウントされます。

* Restore Requests Approver



メールのリストアの承認者のメールをここから追加できます。

* Advanced

ユーザーへの通知メールに関する詳細の設定ができます。

|  |  |
| --- | --- |
| **Advanced** | **詳細** |
| Quarantine notification `From` name | メールが隔離された際のお知らせメールの送信者名 |
| Quarantine notification `From` | メールが隔離された際のお知らせメールの送信メールアドレス |
| Password Protected Quarantine notification subject | PPAPメールが隔離された際の件名 |
| Quarantine notification subject | メールが隔離された際の件名 |
| Password Protected Quarantine notification body | PPAPメールが隔離された際のメールの本文 |
| Quarantine notification body | メールが隔離された際のメールの本文 |
| Require password to release encrypted file notification body | PPAPメールが隔離された際の通知メールの本文 |
| Quarantined notification (admin restore request): | メールが隔離された際の通知メール（Adminにリストアを要求する際） |
| Restore request subject | リストア要求メールの件名 |
| Restore request body | リストア要求メールの本文 |
| Decline message subject | リストア拒否のメールの件名 |
| Decline message body | リストア拒否のメールの本文 |
| Threat extracted message format | ThreatExtraction（無害化）をした際のメールのフォーマット |
| Threat extracted attachment name template | ThreatExtraction（無害化）をした際の添付ファイルの名前 |
| Phishing quarantine notification subject | フィッシングメール隔離の通知メールの件名 |
| Phishing quarantine notification body | フィッシングメール隔離の通知メールの本文 |
| Phishing decline message subject | フィッシングメール拒否のメールの件名 |
| Phishing decline message body | フィッシングメール拒否のメールの本文 |
| Spam quarantine notification body | スパムで隔離されたメールの本文 |
| Spam quarantine notification subject | スパムで隔離されたメールの件名 |
| Report Phishing approve subject | フィッシングメールを報告した際に、フィッシングメールと認められた際の件名 |
| Report Phishing approve body | フィッシングメールを報告した際に、フィッシングメールと認められた際の本文 |
| Report Phishing simulation subject | フィッシングメールシュミレーションの報告の件名 |
| Report Phishing decline subject | フィッシングメールシュミレーションの報告が拒否された時の件名 |
| Report Phishing simulation body | フィッシングメールの報告の本文 |
| Report Phishing decline body | フィッシングメールの報告の件名 |