NTT東日本

おまかせクラウドアップセキュリティ

契約者管理コンソール利用マニュアル

東日本電信電話株式会社

変更履歴

年月	版	変更内容等
2021年08月30日	第1.0版	初版制定
2022年03月30日	第1.1版	手順追加
2022年06月21日	第1.2版	表紙記載の組織名を変更
2022年10月12日	第1.3版	一部システム名など文言追加
2023年02月27日	第1.4版	ヘルプページのURL変更に伴い修正
2023年07月12日	第1.5版	ExchangeOnline隔離プレビュー機能について追加
2023年11月28日	第1.6版	Gmail隔離プレビュー機能について追加

目次

【1】ダッシュボード操作手順

ダッシュボード操作手順（1）

1. コンソール画面ログイン

アカウントIDとパスワードを入力して「**ログイン**」を押下します。

①左図画面が表示された場合のみ、
「**2要素認証設定を行う**」を押下します。
※設定方法は別紙をご参照ください。

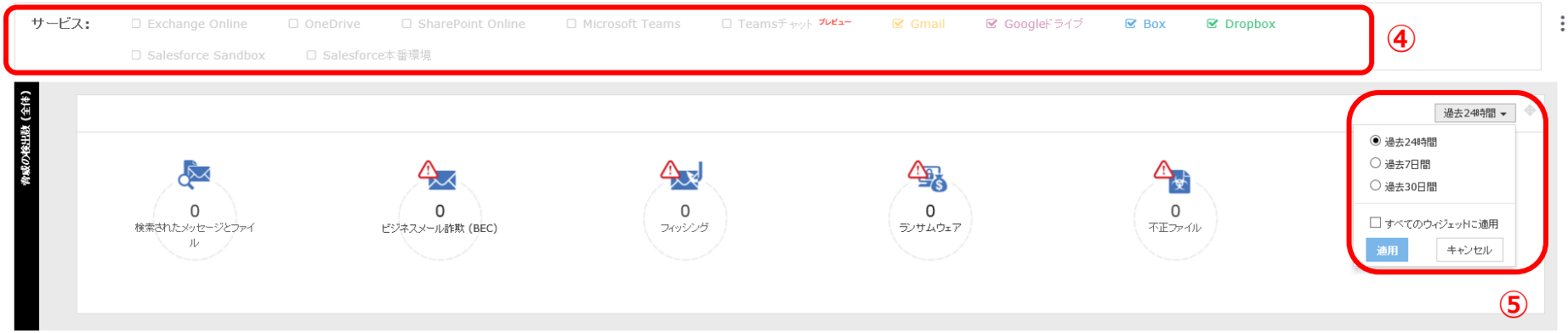
ダッシュボード操作手順（2）

②「**コンソールを開く**」を押下します。

③コンソール画面にログインできていることを確認します。

「**ダッシュボード**」が表示されていることを確認します。

ダッシュボード操作手順（3）



④画面中央部、「**サービス：**」より、連携済みで検知状況等を確認したいクラウドアプリケーションにチェックを入れます。

⑤プルダウンメニューから表示する期間を選択します。
画面を下にスクロールすると表示される各脅威検知情報等すべてに期間を適用する場合は、「**すべてのウィジェットに適用**」を選択し「**適用**」を押下します。

ダッシュボードでは以下項目の情報が表示されます。
・脅威の検出数 (全体)
・ランサムウェア対策
・ビジネスメール詐欺 (BEC)
・概要
・高度な脅威対策
・情報漏えい対策

各項目の詳細ごとに対象の表示期間を設定できます。

⑥画面中央部、「**サービス：**」右部のメニューより、現在のダッシュボードデータをエクスポートできます。

【2】ダッシュボードから取得可能なログの種類

管理コンソール画面より取得可能なセキュリティログの種類

ログの種類	ログ内容	ログからわかること(例)
①監査ログ	ユーザの実行処理	• 管理コンソール画面へのログイン時刻 • サービス連携完了有無 • ポリシー設定完了有無
②ランサムウェアログ	ランサムウェアと疑わしき脅威	• ランサムウェア名 • 受信者/送信者アドレス • メール件名
③隔離ログ	脅威度が高いと判定された隔離した脅威	• 検知対象の配置日時 • 検知された利用中クラウドアプリケーション名 • 検知対象のセキュリティリスク名 • 不審URLを含む各種ファイル名
④セキュリティリスクログ (②と③の情報を含みます)	不正URLやマルウェア、ランサムウェア等検知された脅威	• ファイル/メール件名 • ファイルの配置/メール送受信日時 • メール送受信者
⑤仮想アナライザログ	仮想アナライザ機能が働いた脅威(未知の脅威)	• リスクのレベル • 送受信者、 • ファイル名、URL、メール件名
⑥情報漏洩対策ログ	情報漏洩対策のポリシーで検知した脅威	• 違反したデータが何に該当したか ※金融コード、マイナンバーなど • ファイルの配置日時

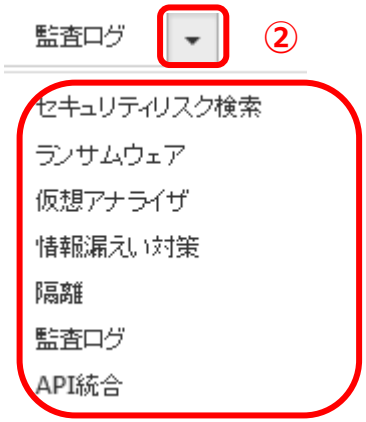
セキュリティログのカラム詳細

カラム名	説明
SHA-1	SHA-1ハッシュ値。
ウイルス名	検出したウイルスまたはそれに疑わしきものの名称。
ステータス	検出した脅威に対して処理を実行後のステータス。(隔離/削除　できた・できない)
セキュリティフィルタ	検知された脅威が該当しているフィルタの名称。
セキュリティリスク名	検知されたセキュリティリスク名称。
タイムスタンプ	リアルタイムスキャンで検知した日時。yyyy/mm/dd　hh:mm:ss形式で表示される。
ファイル名	検出されたファイルの名称。
ファイル更新時間	クラウドストレージ(Box,OneDriveなど)で検出した場合、検出したファイルの更新時間(配置時間)が記載される。
メッセージID	検出したメールに振り分けられているID。
メッセージ受信時刻	メールで検出した場合、メールの受信時刻が記載される。
ユーザ/ユーザ名	脅威を検出、ポリシー違反を検出したユーザー。メールアドレスで記載される。
リスクレベル	検出された脅威の危険度。
件名	メールで検出した場合、メールの件名が記載される。
処理	検出した脅威などに実行された処理内容。ポリシー設定で定める。「放置」「隔離」「削除」などが設定できる。
受信者	メールで検出した場合、メールの受信者アドレスが記載される。
場所	検出した脅威の配置されている場所。
実行されたテンプレート	検出する際に実行されたテンプレート名。情報漏洩対策で設定を行う金融コードやマイナンバー番号の設定が該当する。
実行されたポリシー	検出する際に実行されたポリシー名。初期設定では「初期設定の〇〇〇〇ポリシー」のように表示される。
検出の種類	検出された対象の種類。
検出方法	対象の脅威を検出した方法。
検索の種類	行われた脅威検索の種類。手動でない限り、「リアルタイム検索」が記載される。
検索元	スキャンを行った連携済みサービス。Gmail/Exchange Onlineなどが表示される。
概要レポート	レポートの管理ID。英数字の羅列が記載される。(例：c1a3425bbfdbfaebd36acad6f28fae28d4b13963)
詳細	ユーザーが行った処理が記載される。監査ログに表示される。
送信者	メールで検出した場合、メールの送信者アドレスが記載される。
違反コンテンツ	ポリシー・テンプレートの設定に違反するコンテンツの違反内容が記載される。
隔離タイプ	隔離で実施された処理のタイプ。隔離ログで使用される。

【3】ログの確認方法・取得手順

ログの確認方法・取得手順（1）

①画面上部タブより、「**ログ**」を選択します。

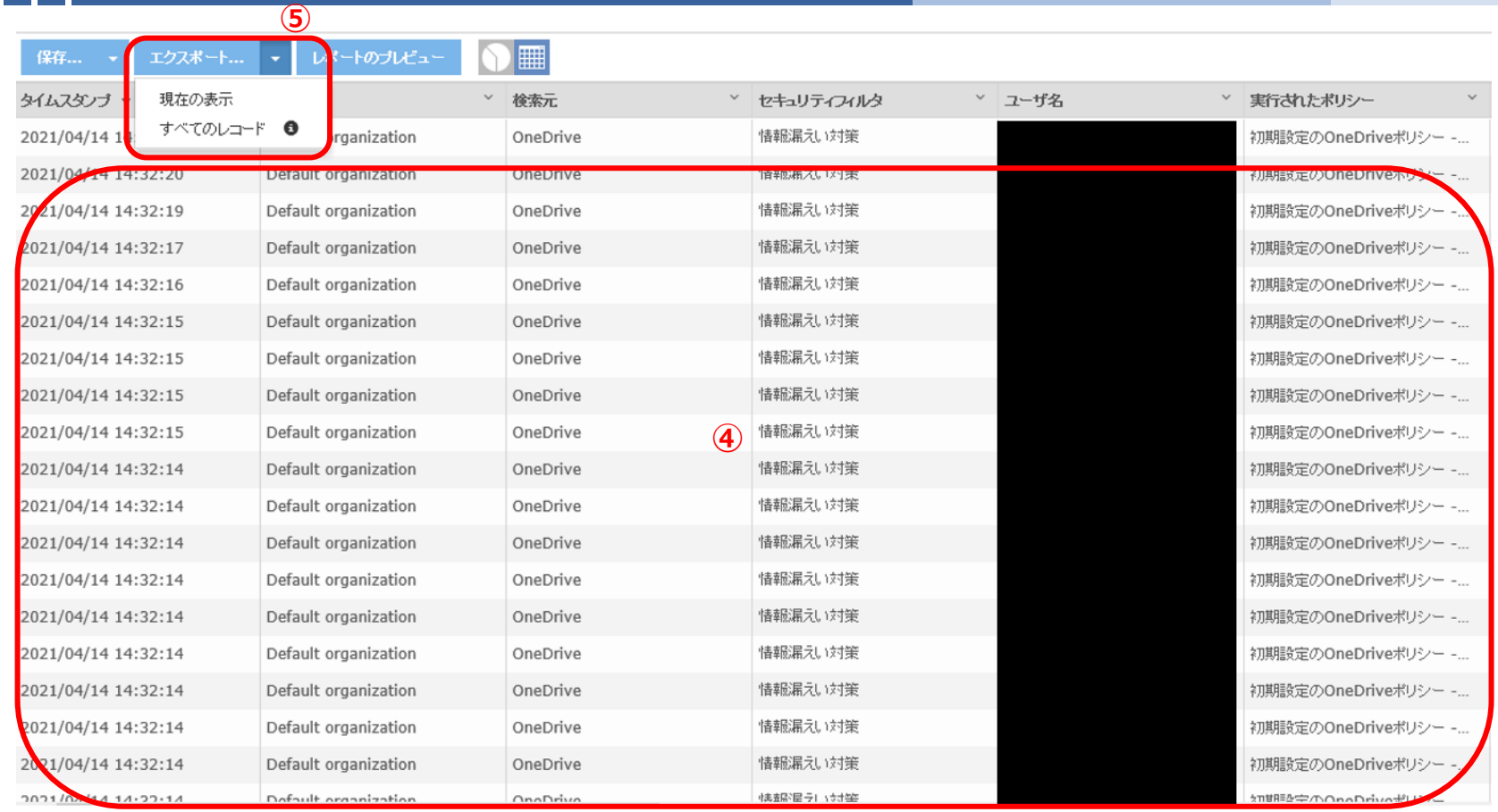


②画面中央左部、プルダウンメニューより閲覧したいログの種類を設定できます。

③画面上部右側、「**日付範囲の選択**」プルダウンからログを表示する期間を設定できます。
カレンダーから指定することで、指定開始日から指定終了日までの範囲を表示できます。(過去180日分のログを取得できます。)

指定後、「**検索**」を押下します。

ログの確認方法・取得手順（2）



④画面中央部の「**フィールド**」に選択した期間・種類のログが表示されます。

⑤設定したログをcsv形式でダウンロードできます。
「**エクスポート**」プルダウンから「**現在の表示**」または「**すべてのレコード**」を選択します。
ダウンロード実行時の出力結果は以下を参照ください。

現在の表示：フィールドに現在表示されているログが取得できます。
※スクロールしないと表示されない部分は出力されません。

すべてのレコード：選択した条件のログをすべて出力します。スクロールしないと表示されない部分も出力できます。
※出力可能な最大レコード数は10,000レコードとなります。

脅威の検知状況(ストレージ)確認例

■Googleストレージをご利用の場合(セキュリティリスクログを活用)

①検索元を「**Googleドライブ**」でフィルターをかけます

②リスク名を「**危険**」でフィルターをかけます

タイム	組織	検索元	セキュリティフィル	セキュリティリスク名	検出方	リスク	ユーザ名	実行さ	処理	場所	ファイル名
#######	初期設定の	Googleドライブ	Webレピュテーション	違法または禁止されたコンテンツ: [https]:	Webレピ	危険	*****@*****	初期設定の	放置	/マイドライブ/ファイル_000	ファイル_000
#######	初期設定の	Googleドライブ	Webレピュテーション	違法または禁止されたコンテンツ: [https]:	Webレピ	危険	*****@*****	初期設定の	放置	/マイドライブ/ファイル_000	ファイル_001

③「**場所**」や「**ファイル名**」を確認し、
許可している利用目的からずれていないか
ご確認をお願いいたします。
検閲したアイテムのファイル名を確認できます。

＜黄色く塗りつぶしたログの読み方＞
ユーザ*******のGoogleドライブに保存されたファイルの中に「**違法または禁止されたコンテンツ**」に分類される不正URLが含まれているため、おまかせクラウドアップセキュリティで「**危険**」と判定しています。

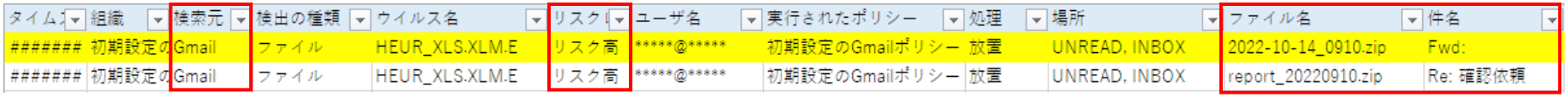
※Onedrive/Box/Dropboxでもカラムの内容が少し異なる場合がございますが同様に確認できます。

メールの脅威検知状況確認例

■Gmailをご利用の場合(仮想アナライザログを活用)

①検索元を**「Gmail」**で
フィルターをかけます

②リスクレベルを**「リスク高」**で
フィルターをかけます



タイム	組織	検索元	検出の種類	ウイルス名	リスク	ユーザ名	実行されたポリシー	処理	場所	ファイル名	件名
#######	初期設定の	Gmail	ファイル	HEUR_XLS.XLM.E	リスク高	*****@*****	初期設定のGmailポリシー	放置	UNREAD, INBOX	2022-10-14_0910.zip	Fwd:
#######	初期設定の	Gmail	ファイル	HEUR_XLS.XLM.E	リスク高	*****@*****	初期設定のGmailポリシー	放置	UNREAD, INBOX	report_20220910.zip	Re: 確認依頼

③検閲されたアイテムの「**ファイル名**」や「**件名**」を
確認することができます。

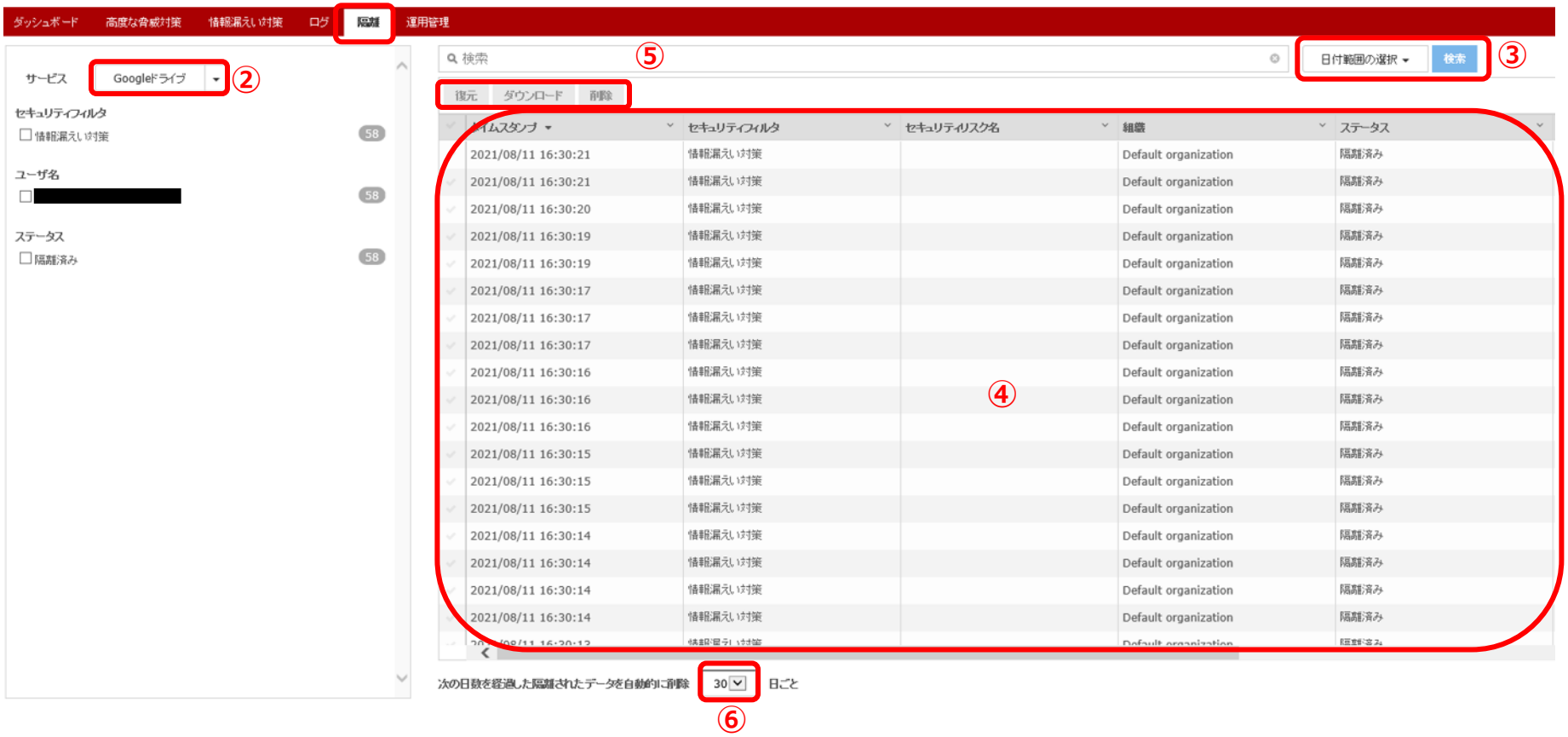
＜黄色く塗りつぶしたログの読み方＞
ユーザ*******のGmailで受信したメールの添付「**ファイル**」の中にウイルス付メールが含まれているため、
おまかせクラウドアップセキュリティで「**リスク高**」と判定しています。

※Exchange onlineでもカラムの内容が少し異なる場合がございますが同様に確認できます。

【4】隔離処理を実行したファイルの操作

隔離処理を実行したファイルの操作(1)

①画面上部タブより、「**隔離**」を選択します。



②画面中央左部、プルダウンメニューより操作したい
連携済みクラウドアプリケーションの種類を設定できます。

③画面上部右側、「**日付範囲の選択**」プルダウンからログを表示する期間を設定できます。
カレンダーから指定することで、指定開始日から指定終了日までの範囲を表示できます。

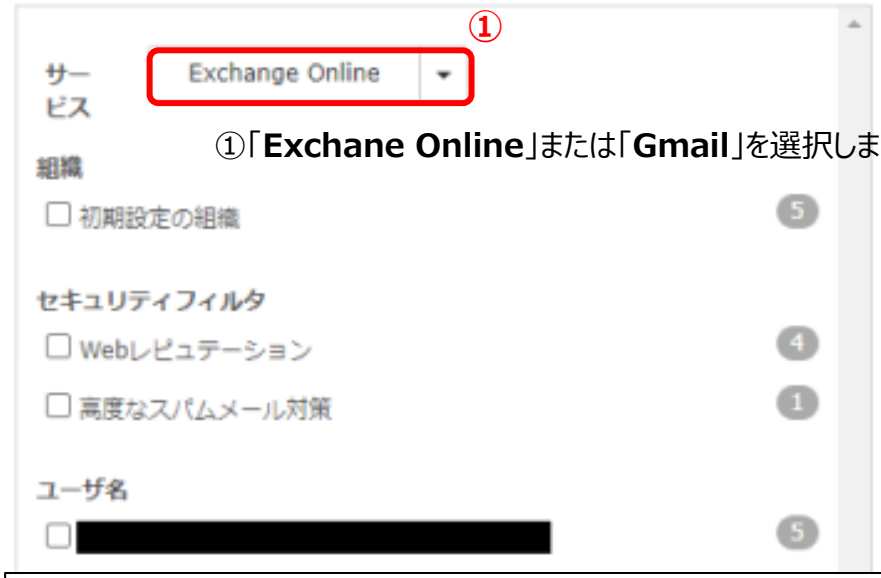
指定後、「**検索**」を押下します。

④画面中央部の「**フィールド**」に選択した期間・アプリごとに
隔離処理を実行されたデータが表示されます。
フィールド内左側のチェックを行うことでデータを選択できます。

⑤フィールドで選択したデータに対する操作を選択できます。

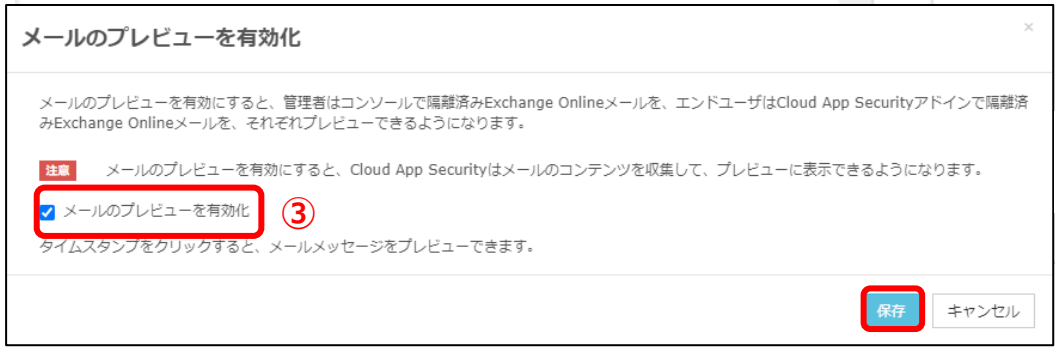
⑥隔離されたデータ自動削除日数をプルダウンメニューより設定できます。
30日,60日,90日から選択できます

隔離処理を実行したファイルの操作(2)



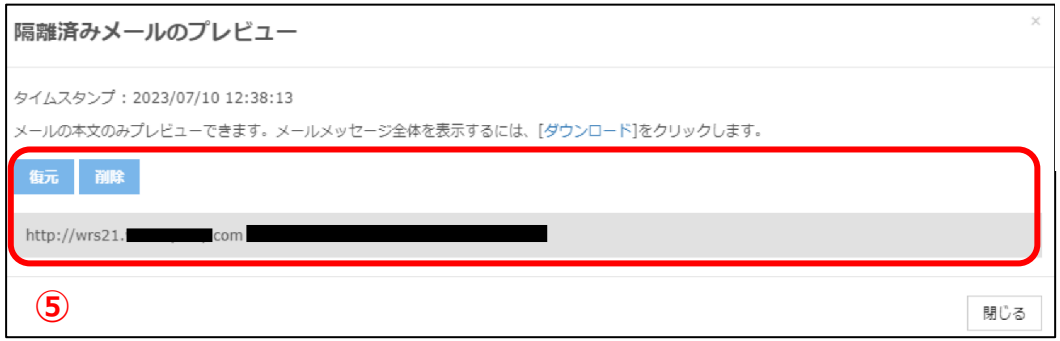
①「**Exchane Online**」または「**Gmail**」を選択します。

②画面上段中央部、「**メールプレビューの有効化**」を押下します。



③「**メールプレビューを有効化**」ウィンドウが表示されます。
「**メールのプレビューを有効化**」にチェックを入れ、「**OK**」を押下します。

④設定後に検知した隔離メールの「**タイムスタンプ**」がリンクになるため、プレビューを閲覧したい対象のリンクをクリックします。

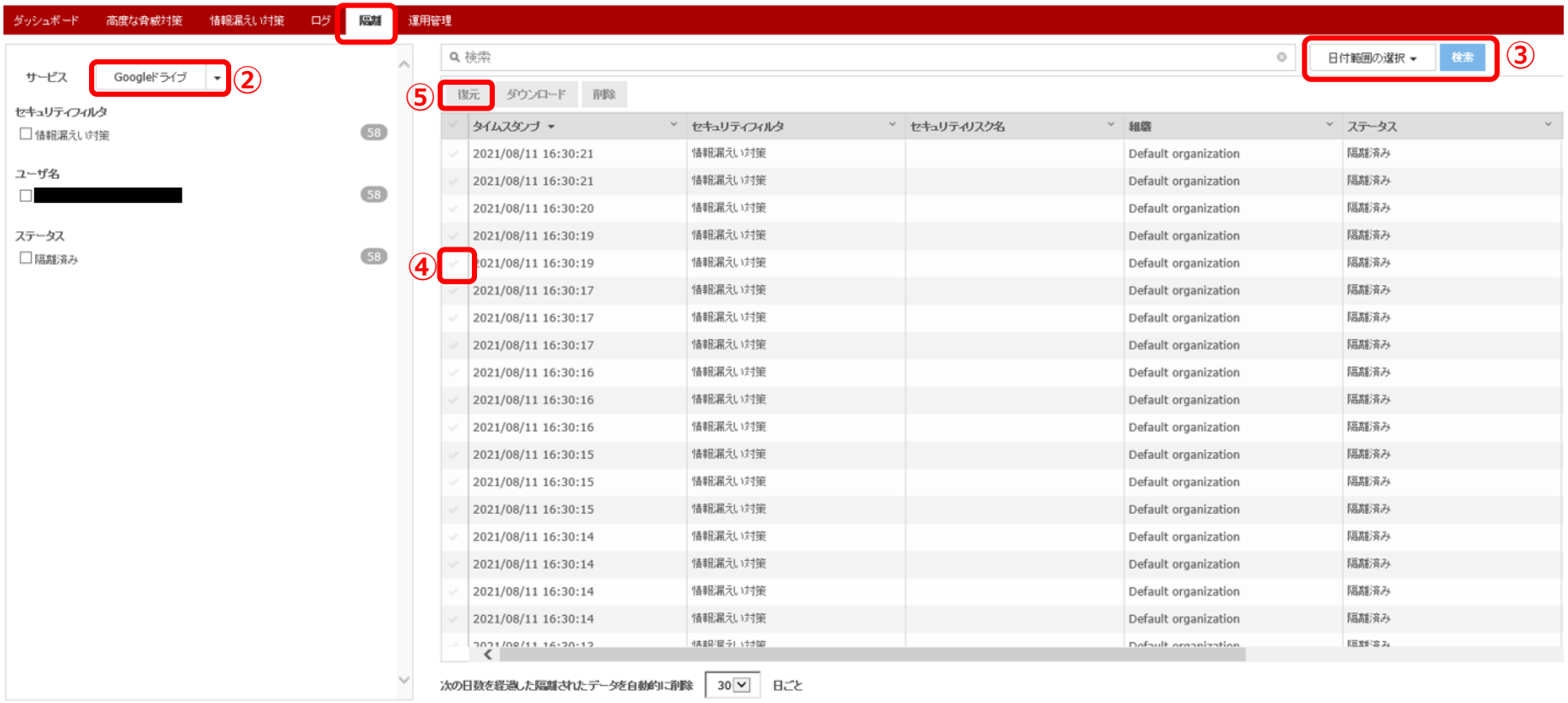


⑤対象の隔離メールの本文プレビューがウィンドウで表示されます。
必要に応じ、「**復元**」や「**削除**」を実施します。
※メール全体(件名や添付ファイル)などを確認する場合は、
隔離されたメールの「**ダウンロード**」を実施してください。

【5】隔離処理を実行したファイルの復元方法

隔離処理を実行したファイルの復元方法

①画面上部タブより、「**隔離**」を選択します。



②画面中央左部、プルダウンメニューより操作したい
連携済みクラウドアプリケーションの種類を設定できます。

③画面上部右側、「**日付範囲の選択**」プルダウンからログを表示する期間を設定できます。
カレンダーから指定することで、指定開始日から指定終了日までの範囲を表示できます。

指定後、「**検索**」を押下します。

④表示された隔離済みアイテムの中から復元したいアイテムのチェックボックスにチェックを入れます。

⑤「**復元**」を押下します。
※受信者の受信するべきだった領域へアイテムが復元されます。

参考サイト

その他の操作方法やご不明点については以下サイトに接続しご確認ください

オンラインヘルプセンタへアクセスします。(トレンドマイクロ社オンラインヘルプセンタ)

・コンソールからアクセス（下図参照）
1.「**はじめに**」にある「**オンラインヘルプの表示**」リンクをクリック。
2.「**はじめに**」部分がない場合、右上「**？**」アイコンにカーソルをあわせた後、「**よくある質問**」をクリック。