M-Drive

利用マニュアル

操作編（管理者ユーザ詳細編）[その他]

このたびはクラウドストレージサービスM-Driveをご利用いただきまして
誠にありがとうございます。
本マニュアルでは、本サービスのその他の設定に関する操作を説明いたします。

第9．0版

※一部画面イメージは開発中のものです。実際の画面とは一部異なる場合がありますのでご注意ください。
※本書に記載されている会社名、システム名、製品名は一般に各社の登録商標または商標です。
なお、本文および図表中では、「™」、「®」は明記しておりません。

利用マニュアルについて

①：サービス概要

本サービスの
サービスの概要や特長を説明

②：新規契約お申込み編

本サービスの
新規お申込み方法を説明

③：導入編【設定例】

本サービスの初期設定を設定例
から説明

④：操作編
（管理者ユーザ詳細）

管理者権限を持つ利用者様向け
の操作説明

⑤：操作編
（一般ユーザ詳細）

ユーザ向けの操作説明

⑥：ログイン・メールアドレス、
パスワード変更、
アカウントロック解除編

本サービスへのログイン、メール
アドレス・パスワード変更、
アカウントロック解除の操作説明

⑦：契約変更･解約申込編

ご契約情報確認方法や
変更について説明

⑧：電子帳簿保存法対応編

電子帳簿保存法に対応するため
の設定・操作方法を説明

改版履歴

版	年月	改訂内容	改訂箇所
1.0版	2022年2月	初版作成	
2.1版	2022年6月	管理コンソールのメニューに合わせて項目名を「使用量」に変更しました。 また、説明を更新し、使用量の更新に関する注釈を更新しました。	4
		承認者の一括編集機能について追記しました。	5
		フォルダテンプレート機能について追記しました。	6
		ファイルロック一覧機能について追記しました。	7
3.1版	2022年10月	属性機能、属性セット機能について追記しました。	8 9
4.0版	2022年11月	「利用マニュアルについて」に「⑧：電子帳簿保存法対応編」を追記しました。	-
		Active Directory設定機能について追記しました。	10
5.0版	2023年3月	属性画面のチェックボックス非表示化に伴い記載を更新しました。	8
5.1版	2023年7月	インシデント管理機能について追記しました。	11
		Driveアクティビティについて追記しました。	12
8.3版	2024年11月	「クォータ機能」に「フォルダ容量超過アラート」機能追加に伴い、記載を更新しました。	2-3
		メールテンプレート機能について記載を最新化しました。	3
9.0版	2025年10月	Active Directory設定機能の注釈を追記しました。	10

目次

1 ごみ箱

1．ごみ箱について

【全社共有】フォルダ配下のフォルダやファイルを削除すると、
管理コンソール内の**【ごみ箱】**に移動します。

誤って削除してしまったファイルやフォルダは、「復元」し、元の場所または任意の場所へ戻すことが可能です。

ここに注意

【パーソナルフォルダ】配下のフォルダやファイルを削除した場合は、【ツール】 – 【ごみ箱】に移動されます。

1 ごみ箱

2．ごみ箱からのファイル・フォルダの復元と削除

管理コンソールの内のごみ箱からファイルやフォルダを復元する方法と
削除する方法についてご案内いたします。

ごみ箱からファイルやフォルダを元に戻す

1. 本サービスのWebにログインします。

2. **【ツール】** - **【管理コンソール】**をクリックします。

3. **【編集を開始する】**をクリックし、閲覧モードから編集モードへ変更します。

4．**【ごみ箱】**をクリックします。
復元したいファイルを選択し(①) 、対象の項目をクリック(②)します。

2．ごみ箱からのファイル・フォルダの復元と削除

【元のフォルダに戻す】をクリックした場合、ファイルやフォルダが保管されていた場所に戻すことができます。元のフォルダに戻す旨メッセージが表示されますので「OK」ボタンをクリックします。

【指定したフォルダに戻す】をクリックした場合、ファイルやフォルダを指定した場所に戻すことができます。フォルダ指定画面が表示されます。復元先フォルダを指定し(①)、「リストア」ボタンをクリック(②)します。

2．ごみ箱からのファイル・フォルダの復元と削除

5．指定した復元先にファイルが保管されます。

6．「編集を終了する」ボタンをクリックし、編集モードから閲覧モードへ変更後、画面右上の×ボタンをクリックし、管理コンソール画面を閉じます。

参考

フォルダも同様の手順で復元することができます。

1 ごみ箱

2．ごみ箱からのファイル・フォルダの復元と削除

ごみ箱からファイルやフォルダを削除する

1．**【ツール】** – **【管理コンソール】** - **【ごみ箱】**をクリックします。
2．削除したいファイルを選択し、「ごみ箱から削除」ボタンをクリックします。

3．「OK」ボタンをクリックすると、ごみ箱からファイルが削除されます。

参考

フォルダも同様の手順で削除することができます。

2．ごみ箱からのファイル・フォルダの復元と削除

リストア時のエラーメッセージ一覧

リストアの際に表示される可能性のあるメッセージは、以下です。
エラーの理由を確認し、対処してください。

リストア先のフォルダが既に削除されているため、リストアに失敗しました。
エラーの理由：リストア先のフォルダが削除されていた場合に表示されます。

フォルダの階層の上限を超えるフォルダが存在するため、リストアに失敗しました。
エラーの理由：フォルダ数の上限を超えてしまう場合に表示されます。

フォルダパスの長さを超えるフォルダが存在するため、リストアに失敗しました。
エラーの理由：パス長が上限を超えてしまう場合に表示されます。

リストア先のフォルダ数が上限を超えたため、リストアに失敗しました。
エラーの理由：フォルダの階層が上限を超えてしまう場合に表示されます。

リストア先のファイル数が上限を超えたため、リストアに失敗しました。
エラーの理由：保管できるファイル数の上限を超えてしまう場合に表示されます。

2 ログ

1．共有リンク証跡

共有リンク証跡の利用方法について説明します。

共有リンク証跡とは

【全社共有】フォルダ内に保管しているファイルの発行済みの共有リンクの証跡が確認できる機能です。

共有リンクを発行した際の情報(宛先、共有したファイル等)を確認することができます。

共有リンク証跡の保管期間

証跡は管理コンソールの**【ポリシー設定】**で設定した期間、保管されます。

参考

共有リンク発行時に設定した【有効期間】後、何日保管するか設定することができます。

共有リンク発行時：

2 ログ

1．共有リンク証跡

共有リンク証跡の確認方法

1. 本サービスのWebにログインします。

2. **【ツール】 - 【管理コンソール】 - 【共有リンク証跡】**をクリックします。

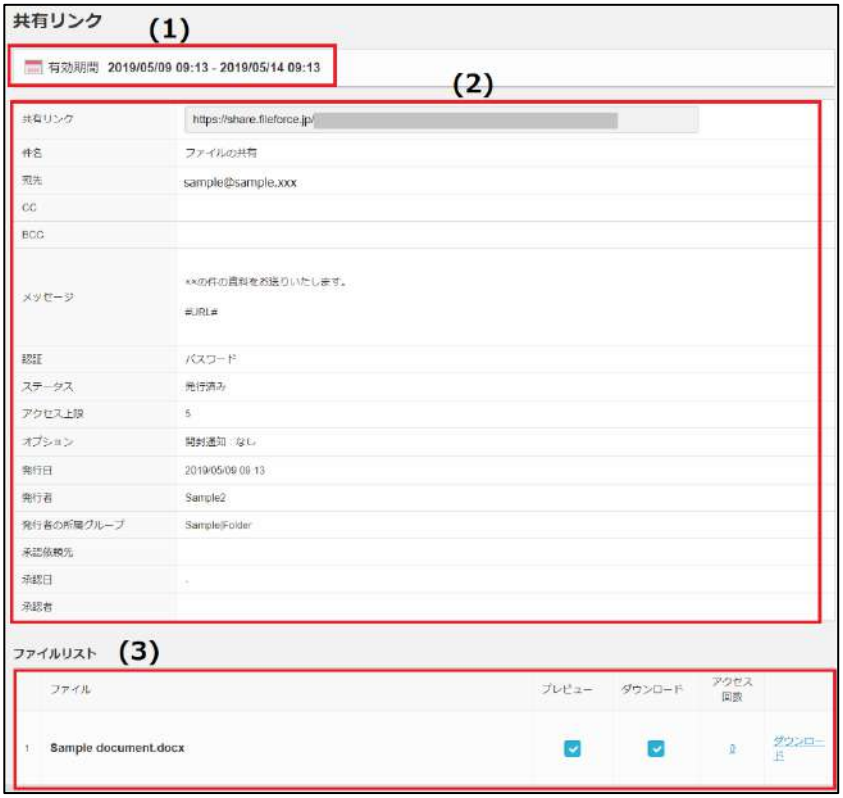
3. 期間やメールアドレス等、条件を入力し「検索」ボタンをクリックすると、
検索結果が画面右側に表示されます。

4．**【詳細】**をクリックします。

2 ログ

1．共有リンク証跡

5．発行した共有リンクの詳細を確認することができます。



(1) 共有リンクの有効期間が表示されます。
(2) 共有リンクの発行先、発行の際の設定が表示されます。

参考

「リンクをメールで送信」を選択した場合、宛先やメッセージが確認できます。

(3) 共有リンクを発行したファイルをダウンロードすることができます。
ファイルの内容は、共有リンクを発行時と同じ内容です。

2．管理ログ

【管理ログ】には、管理コンソールの操作ログが保存されています。
期間、ユーザ、操作内容で絞り込み、結果を表示することができます。

参考

管理コンソール以外の操作ログは、【ツール】 - 【ログ＆レポート】より確認することができます。

操作方法

1．管理コンソール内の**【管理ログ】**をクリックします。
2．検索条件を設定し 「検索」ボタンをクリックします。

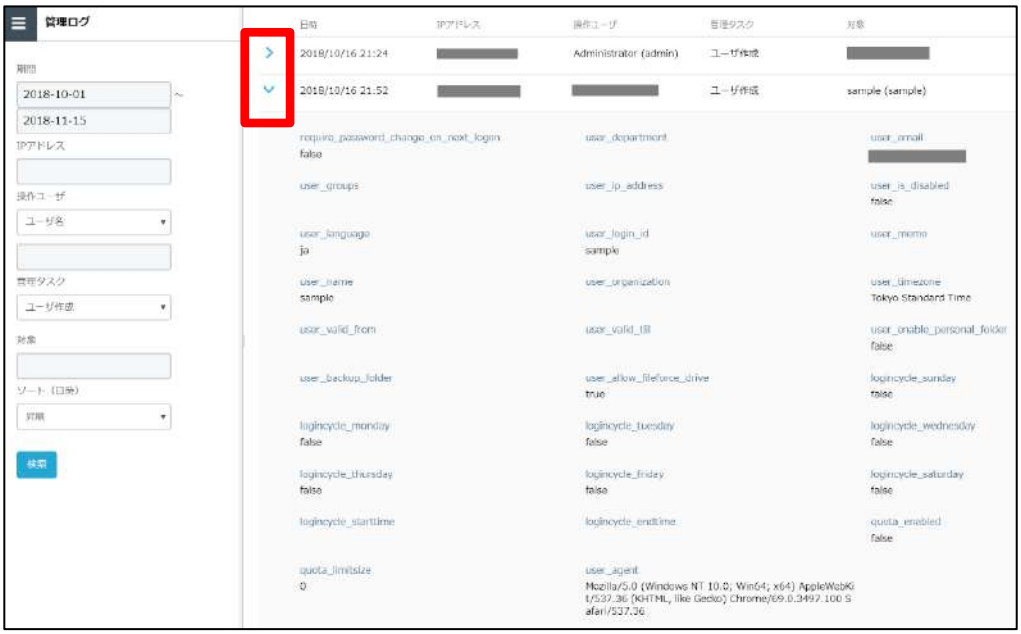
期間	出力したい期間(開始と終了)入力
操作ユーザ名	ユーザ名またはログインIDを選択し、下の欄に入力
管理タスク名	ユーザ作成やグループ削除等、検索したいタスク名を選択

3．検索結果が表示されます。

2．管理ログ

4．検索結果の › をクリックすると、詳細を確認することができます。

操作内容：ユーザ作成



3．クォータ

クォータの設定後の容量確認方法について説明します。

管理コンソール - フォルダにてクォータ制限値を設定したフォルダの使用状況を確認することが可能です。

【制限値を超えたフォルダのみ表示】をクリックすると、制限値を超えたフォルダの情報のみ表示されます。

3 メールテンプレート

メールテンプレート機能とそのカスタマイズ方法についてご案内いたします。

共有リンクのパスワード等、本サービスよりメールを送る際のテンプレートのカスタマイズが可能です。

テンプレート一覧

共有リンク	共有リンクパスワード	却下
	承認依頼	通知(リンク開封時)
	承認(リンク用)	通知(アクション実行時)
	承認(メール用)	
プロジェクト 共有フォルダ招待	社内メンバー招待（全社共通）	社外コラボレーター招待
	社内メンバー招待(パーソナルフォルダ)	社外コラボレーターパスコード
プロジェクト 共有フォルダ通知	アップロード	ファイル共有リンク作成
	コメント追加	フォルダ作成
	バージョン入れ替え	フォルダを空にする
	ファイル削除	フォルダ削除
	ダウンロード	フォルダ属性変更
	ファイル属性変更	フォルダ移動
	ファイル移動	フォルダ名変更
	プレビュー	ファイルアップロード通知
	ファイル名変更	

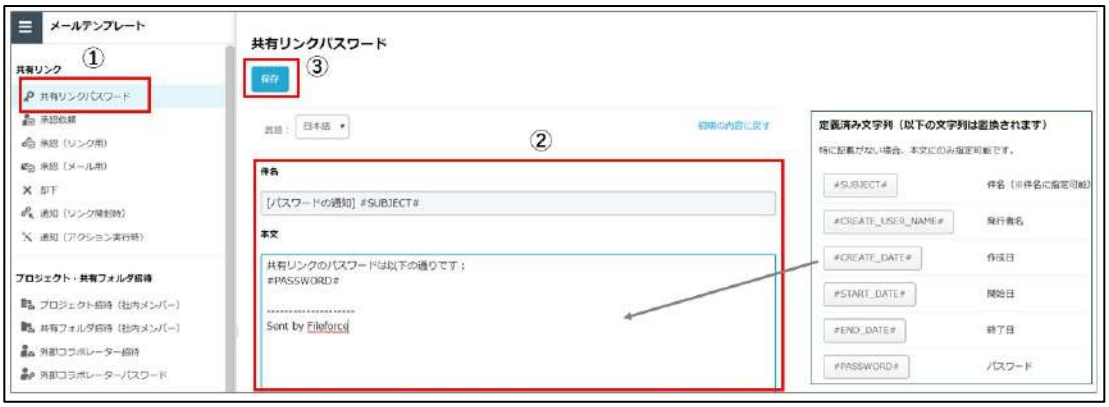
3 メールテンプレート

カスタマイズ方法

カスタマイズしたいメールテンプレートを選択してクリックし、件名・本文に追記または定義済みの文字列を追加後、「保存」ボタンをクリックします。

参考

【初期の内容に戻す】をクリックすると、編集前の状態に戻ります。



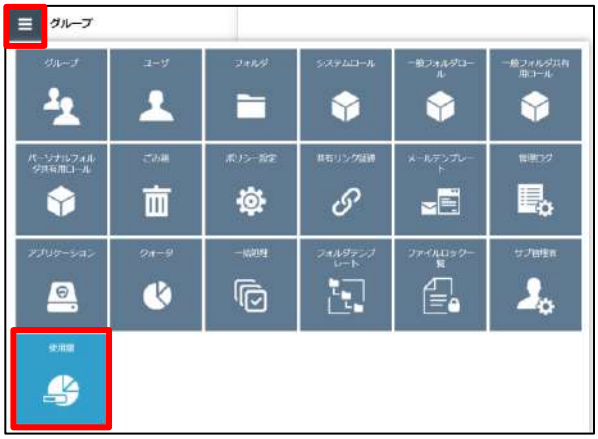
4 使用量

使用量の機能について説明します。

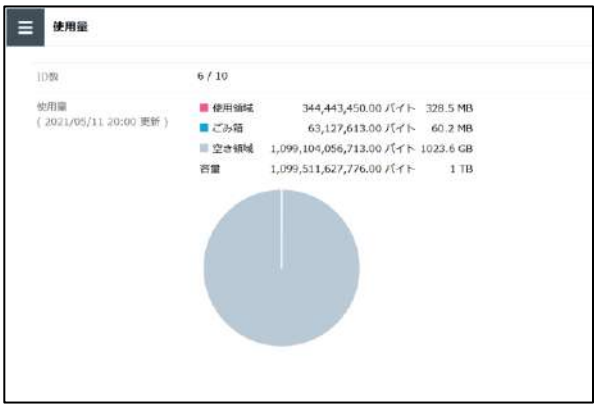
1. 本サービスのWebにログインします。

2. **【ツール】** - **【管理コンソール】**をクリックします。

3. 管理コンソールから**【使用量】**クリックします。



4. 使用量画面が表示され、下記が確認可能となります。
   - 契約ID
   - ID数
   - 使用領域
   - ごみ箱
   - 空き容量



ここに注意

ID数（ユーザ数）は作成のタイミングで反映されますが、使用量は1時間ごとで反映されます。
また、「使用量」にアクセスしたタイミングでも使用量は反映（更新）されます。

5 承認者の一括編集

承認者の一括編集の機能と操作方法について説明します。

一括編集では、現在本サービス上に登録されている承認者の情報のダウンロードと、一括で本サービス上の承認者情報を更新することができます。

承認者リストのダウンロード

1．承認者リストのダウンロード欄の「ダウンロード」ボタンをクリックします。

2．「OK」ボタンをクリックし、ファイルを保存します。

3．指定した保存先に保存されたCSVファイルを開くと、承認者情報が表示されます。

5 承認者の一括編集

承認者の一括更新

1．一括更新するため、まずは承認者リストのダウンロードが必要となります。　【承認者リストのダウンロード】欄の「ダウンロード」ボタンをクリックし、CSVファイルをダウンロードします。

2．CSVファイルを開き、内容を編集します。

ここに注意

group_name, email_address, is_deleteすべての項目の入力が必要です。
CSVファイルの文字エンコードはUTF-8ですので、UTF-8で保存してください。

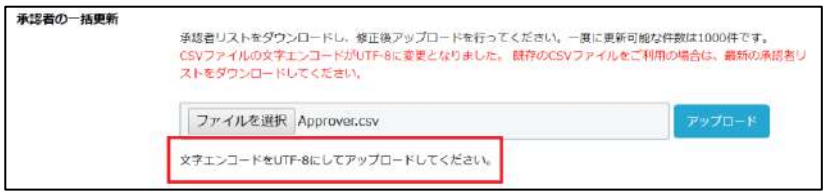
CSVファイル保存方法例 Excel2016をご利用の場合：
CSVファイルを編集後、保存の際には【名前を付けて保存】 をクリックし、
【CSV UTF-8(コンマ区切り)(*.csv)】を選択し、ファイルを保存します。

3．承認者を削除する場合は、is_delete 欄に “1”を入力します。

	A	B	C
1	group_name	email_address	is_delete
2	Sample	sample@xxxx.com	1

4．管理コンソールの【一括処理】をクリックし、「ファイルを選択」ボタンをクリックし、編集したCSVファイルを選択します。

5．アップロードするCSVファイルを選択後、「アップロード」ボタンをクリックします。



ここに注意

文字エンコードがUTF-8以外のファイルをアップロードした場合、「文字コードをUTF-8にしてアップロードしてください。」というメッセージが画面上に表示され、アップロードすることができません。

6．承認者の情報が更新されます。

6 フォルダテンプレート

フォルダテンプレートの機能と操作方法について説明します。

フォルダテンプレートを設定することで、プロジェクトに対して「サブフォルダ」を予め設定したテンプレートから選択することが可能となります。

サブフォルダをまとめて作成したい場合や、テンプレートから作成する際に役立ちます。

プロジェクトの概要については、「利用マニュアル　操作編（管理者ユーザ詳細）「フォルダとプロジェクト」 」の「２．プロジェクトフォルダ」を参照ください。

操作方法

１．【ツール】 - 【管理コンソール】 - 【フォルダテンプレート】 をクリックします。

２．「新規作成」ボタンをクリックし、「名前」「説明」を入力し、サブフォルダを追加ください。

サブフォルダを追加しますと、以下のように表示されます。

「保存」すると、以下のように追加されます。

6 フォルダテンプレート

操作方法

3．【ツール】 - 【プロジェクト管理】 から対象のプロジェクトを開き、「テンプレートから作成」を選択すると、②で設定したテンプレートが選択可能となります。

4．該当のテンプレートを選択し、「次へ」ボタンをクリックください。

5．作成したテンプレートで「サブフォルダ」を選択し、「作成」ボタンをクリックします。

6 フォルダテンプレート

操作方法

6．作成が完了すると、該当のプロジェクト配下に「サブフォルダ」が表示されます。

7 ファイルロック一覧

ファイルロック一覧の機能と操作方法について説明します。

ファイルロック一覧にて、「全社共有」内のロックされているファイルが一覧で確認可能となります。

ファイルのロックについては 「利用マニュアル　操作編（一般ユーザ）「Webブラウザ」 」の「２．８．ファイルのロック」を参照ください。

操作方法

１．【ツール】 - 【管理コンソール】 - 【ファイルロック一覧】 をクリックします。

２．検索条件を設定し、「検索」ボタンをクリックします。
※条件を入れずに検索をすると、全ファイル表示されます。

３．検索結果が表示されます。

４．ロックを解除したい場合は、ロックを解除するファイルの「ロック解除」ボタンをクリックし、確認ダイアログで「OK」をクリックします。

8 属性

電子帳簿保存法対応のために、ファイルに付与できる属性情報を管理可能です。

属性機能の利用方法について説明します。

1. 本サービスのWebにログインします。

2. **【ツール】** - **【管理コンソール】**をクリックします。

3. **【編集を開始する】**をクリックし、閲覧モードから編集モードへ変更します。

4．管理コンソールから**【属性】**クリックします。

8 属性

5．属性画面が表示されます。

①	検索可能	チェックを付けた該当項目に対し、検索機能を有効にします。
②	インフォメーションパネルの表示	チェックを付けた該当項目に対し、本サービスのWebでファイル選択時にインフォメーションに表示することが可能です。
③	名前（日本語）、名前（英語）	属性の項目名を変更することが可能です。
④	リスト項目	リスト表示の項目に対し、事前に入力することで、属性セット時に選択が可能となります。（リスト項目は改行にて区切ります）
⑤	表示順序	属性の表示順序を変更可能です。

ここに注意

電子データによる保存は区分によって、ファイルに設定する属性情報の項目が異なります。
区分にあわせて、設定・操作方法をご参照ください。

・「電子取引」
利用マニュアル「電子帳簿保存法対応編　電子取引」をご参照ください。

・「電子帳簿等保存（電子書類）」
利用マニュアル「電子帳簿保存法対応編　電子書類」をご参照ください。
※電子帳簿等保存（電子帳簿）は本サービスとしては未対応です。

・「スキャナ保存」
利用マニュアル「電子帳簿保存法対応編　スキャナ保存」をご参照ください。

9 属性セット

ファイルに対して属性を入力する際の入力項目の表示/非表示を設定可能です。

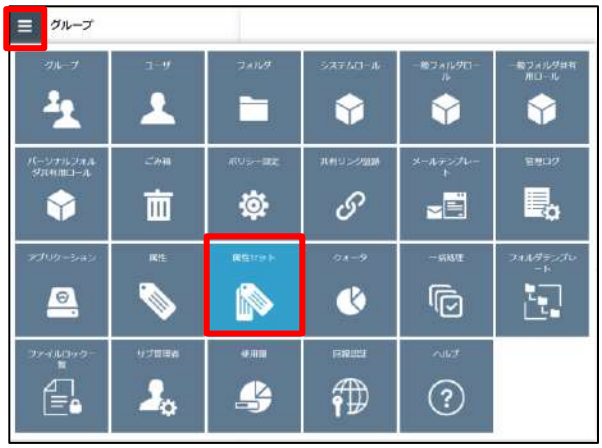
属性セット機能の利用方法について説明します。

1. 本サービスのWebにログインします。

2. **【ツール】** - **【管理コンソール】**をクリックします。

3. **【編集を開始する】**をクリックし、閲覧モードから編集モードへ変更します。

4．管理コンソールから**【属性セット】**クリックします。



5．属性セット画面が表示されます。
属性セットの新規作成、変更、削除が実施可能です。
（「既定」については、削除することはできません。）

9 属性セット

属性セットの新規作成

①属性一覧画面
表示したい「属性項目」をクリックし、「＞＞」をクリック

※以下に示す属性項目を表示するよう繰り返し実施してください。

②設定画面に
表示したい「属性項目」が表示

参考

・設定画面に誤った属性項目を選択した場合は、誤った属性項目をクリックし、「＜＜」をクリックすると削除できます。

・取引先をすべてテキスト入力する場合、属性項目「取引先リスト」は非表示可能です。

ここに注意

電子データによる保存は区分によって、ファイルに設定する属性情報の項目が異なります。
区分にあわせて、設定・操作方法をご参照ください。

・「電子取引」
利用マニュアル「電子帳簿保存法対応編　電子取引」をご参照ください。

・「電子帳簿等保存（電子書類）」
利用マニュアル「電子帳簿保存法対応編　電子書類」をご参照ください。
※電子帳簿等保存（電子帳簿）は本サービスとしては未対応です。

・「スキャナ保存」
利用マニュアル「電子帳簿保存法対応編　スキャナ保存」をご参照ください。

9 属性セット

属性セットの内容変更

属性セットを変更または削除したい場合は、 対象の属性セットをクリックし、変更の場合は変更内容を設定のうえ「保存」をクリックします。削除の場合は、「削除」ボタンをクリックします。

①変更したい属性セットをクリック

②変更したい設定内容に変更

③「保存」をクリック

属性セットの削除

属性セットを変更または削除したい場合は、 対象の属性セットをクリックし、「削除」ボタンをクリックします。

①変更したい属性セットをクリック

②「削除」をクリック

③削除確認画面が表示されます。「OK」をクリック

10 Active Directory設定

Active Directory設定を実施することで、ログイン方法として、Active Directory（以下、AD）のアカウントを選択可能です。

本書では、Active Directory設定を行ううえで必要な本サービスと認証連携するための Active Directory フェデレーション サービス（以下、ADFS）の設定と、本サービス内に実施するActive Directory設定について説明します。

ここに注意

■ADFSを構築するため、ADFSのサーバーをインターネットに公開することになります。
設定の際は、御社内のセキュリティルール等のご確認、NW管理担当者様等へのご相談をいただくのと、
設定内容についても、便宜ご確認いただき、御社内のルールに則った設定を実施するようにしてください。
なお、ADFSのSSLサーバー認証用の証明書について、自己署名証明書の利用は不可となりますので、ご注意下さい。

■本設定完了後、Active Directoryに参加しているPCからWebやストレージサービスDriveをご利用の場合、ログインの際に本サービスの認証（本サービスのログイン画面で、「Active Directoryアカウントでログイン」を選択）が必要になります。

■無料トライアルをご利用いただき、事前に動作検証いただくことを推奨します。

■次ページから、ADFSと本サービスの認証連携設定を説明しておりますが設定例となります。

10 Active Directory設定

1．ADFS認証連携設定

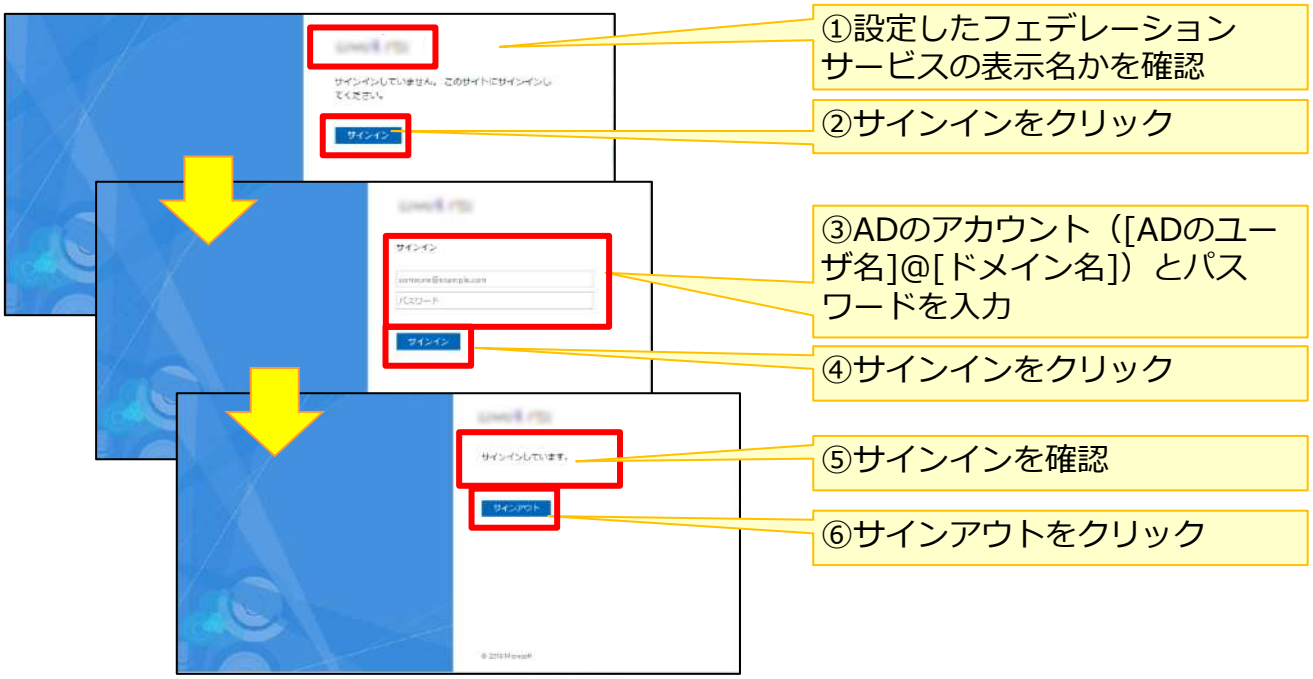
①ADFS構築確認

本サービスとADの認証連携するためには、ADFSを構築いただく必要があります。
※ADFSの構築に関しては、NW管理担当者様等にご確認をお願いいたします。

構築後の確認として、 ADに参加していないPCからインターネット経由で、下記URLにアクセスし、正常確認を実施してください。
※本書の<hostname>の部分は御社ADFSのホスト名に置き換えてください。

https://<hostname>/adfs/fs/federationserverservice.asmx
※以下のように、XMLの情報が表示されることを確認してください。

https://<hostname>/adfs/ls/idpinitiatedsignon.aspx

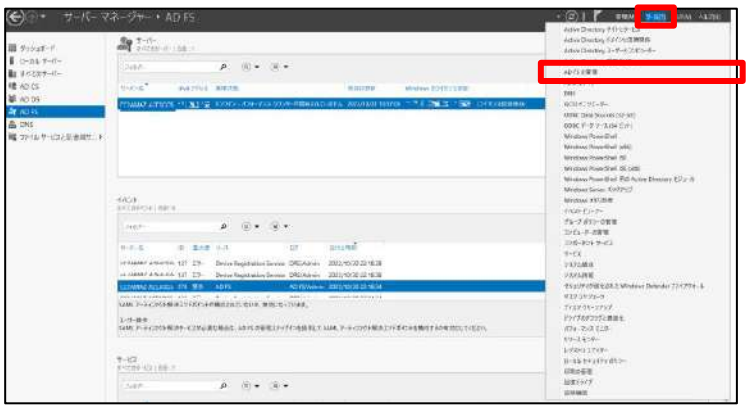


1．ADFS認証連携設定

②ADFSに本サービスの連携設定 - 証明書利用者信頼の追加

IdPのADFSと本サービスの連携設定で、本サービスの通信の許可を実施します。

1．サーバーマネージャー – AD FSで、ツールメニューから「AD FSの管理」をクリックします。



以下のURL分、２から１７までの操作を繰り返し実施します。

i. https://login.cloud-nas.net/login/callback
ii. https://login.cloud-nas.biz/login/callback
※ ii は、回線認証をご利用の場合に設定をお願いします。

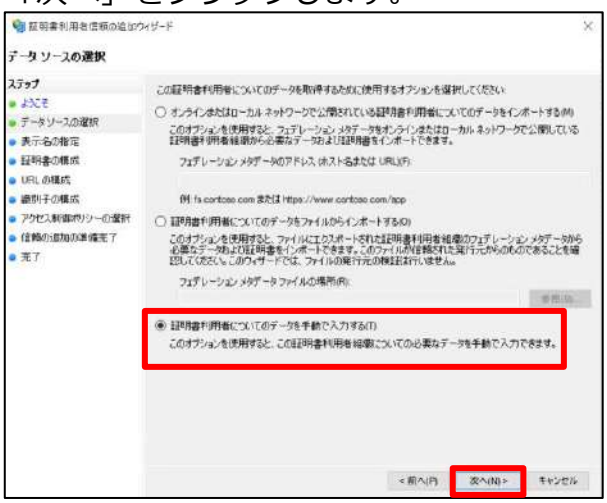
2．AD FSの管理画面で、「証明書利用者信頼の追加」をクリックします。

1．ADFS認証連携設定

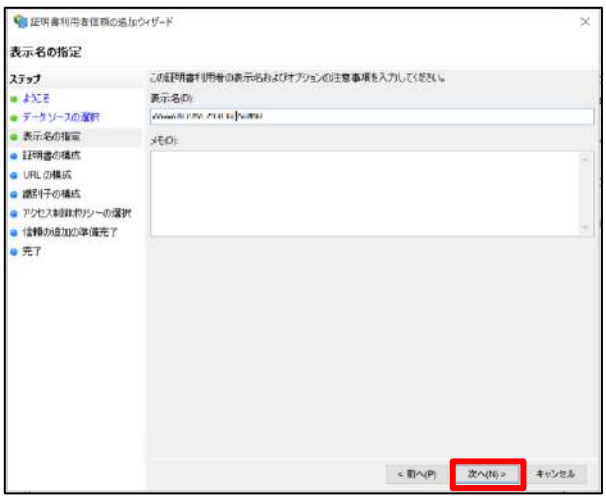
②ADFSに本サービスの連携設定 - 証明書利用者信頼の追加

3．証明書利用者信頼の追加ウィザード画面が表示されますので、「開始」をクリックします。

4．データソースの選択で、「証明書利用者についてのデータを手動で入力する」を選択し、「次へ」をクリックします。



5．表示名の指定で、 「表示名」に任意の表示名を入力し、「次へ」をクリックします。



10 Active Directory設定

1．ADFS認証連携設定

②ADFSに本サービスの連携設定 - 証明書利用者信頼の追加

6．証明書の構成で、証明書利用者信頼の追加ウィザード画面が表示されますので、「開始」をクリックします。

7．URLの構成で、「WS-Federationのパッシブプロトコルのサポートを有効にする」にチェックし、URLを入力のうえで、「次へ」をクリックします。

i. https://login.cloud-nas.net/login/callback
ii. https://login.cloud-nas.biz/login/callback
※ ii は、回線認証をご利用の場合に設定をお願いします。

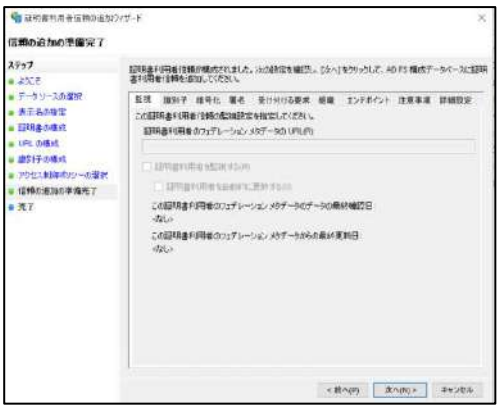
1．ADFS認証連携設定

②ADFSに本サービスの連携設定 - 証明書利用者信頼の追加

8．識別子の構成で、7．で入力したURLが設定されていることを確認し、「次へ」をクリックします。

9．アクセス制御ポリシーの選択で、「すべてのユーザーを許可」が選択されていることを確認し、「次へ」をクリックします。

１０．信頼の追加の準備完了で、「次へ」をクリックします。

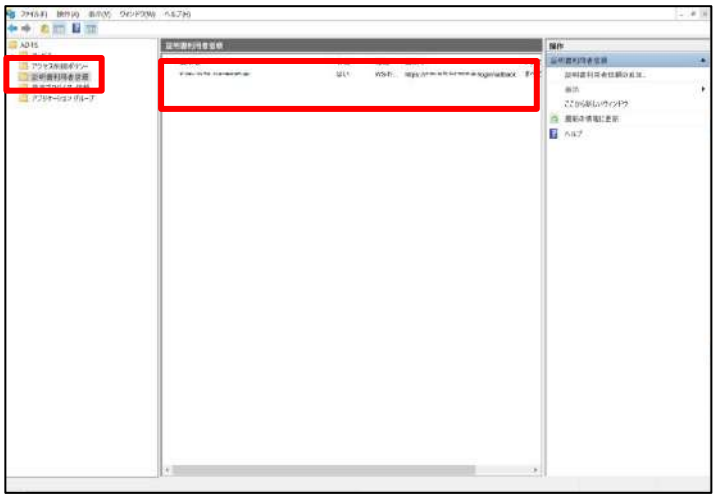


1．ADFS認証連携設定

②ADFSに本サービスの連携設定 - 証明書利用者信頼の追加

１１．完了画面で、「このアプリケーションの要求発行ポリシーを構成する」にチェックが入っていることを確認し、「閉じる」をクリックします。

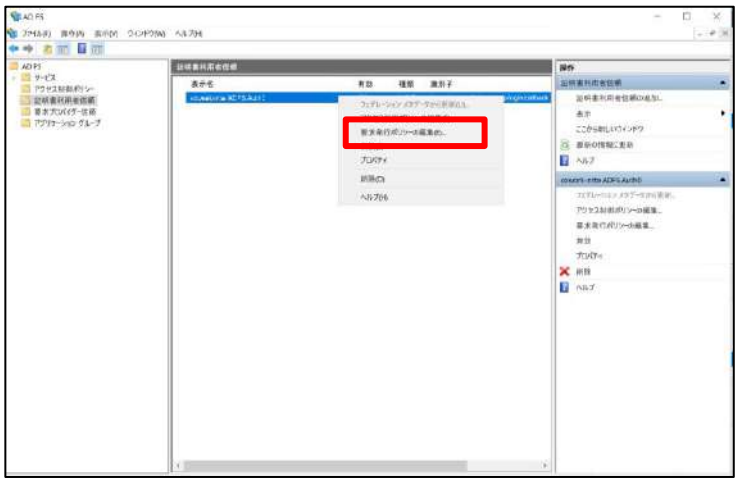
１２． AD FSの管理画面の「証明書利用者信頼」で、追加した証明書利用者信頼が表示されることを確認します。



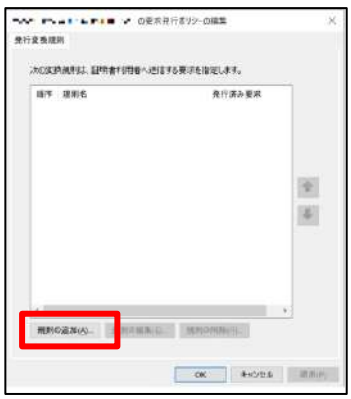
1．ADFS認証連携設定

②ADFSに本サービスの連携設定 - 証明書利用者信頼の追加

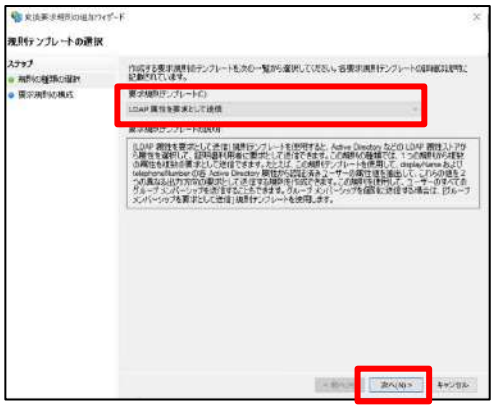
１３． AD FSの管理画面の「証明書利用者信頼」で、追加した証明書利用者信頼を右クリックし、「要求発行ポリシーの編集」をクリックします。



１４．要求発行ポリシーの編集画面で、「規則の追加」をクリックします。



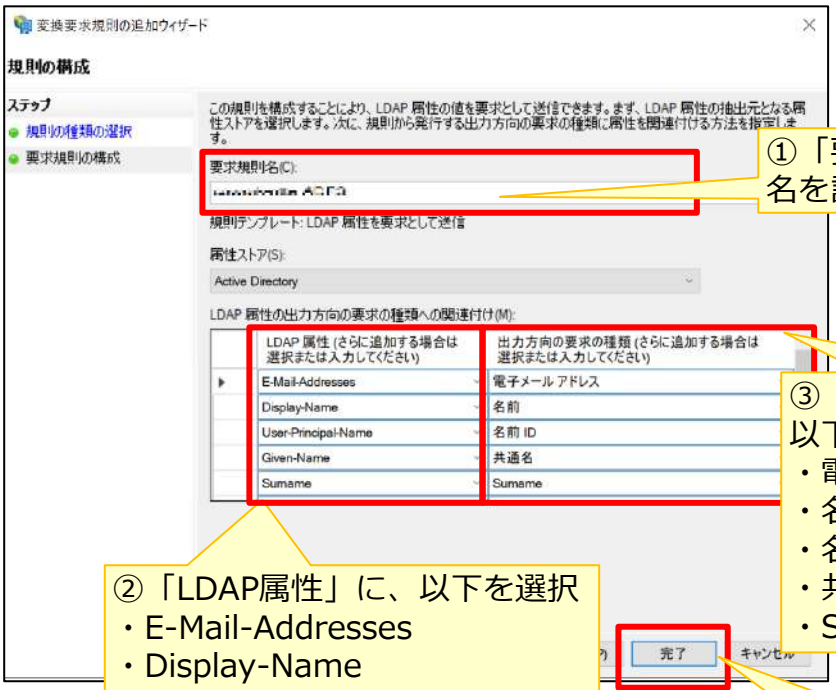
１５．変換要求規則の追加ウィザードの「規則の種類の選択」で、要求規則テンプレートに「LDAP 属性を要求して送信」が選択されていることを確認し、「次へ」をクリックします。



1．ADFS認証連携設定

②ADFSに本サービスの連携設定 - 証明書利用者信頼の追加

１６．変換要求規則の追加ウィザードの「要求規則の構成」で、本サービスと連携するADの情報を設定し、「完了」をクリックします。



①「要求規則名」に任意の規則名を記入

②「LDAP属性」に、以下を選択
・E-Mail-Addresses
・Display-Name
・User-Principal-Name
・Given-Name
・Sumame

③「出力方向の要求の種類」に、以下を選択
・電子メール アドレス
・名前
・名前 ID
・共通名
・Sumame

④「完了」をクリック

１７．要求発行ポリシーの編集画面で、今回追加した変換規則が追加されたことを確認し、「OK」をクリックします。

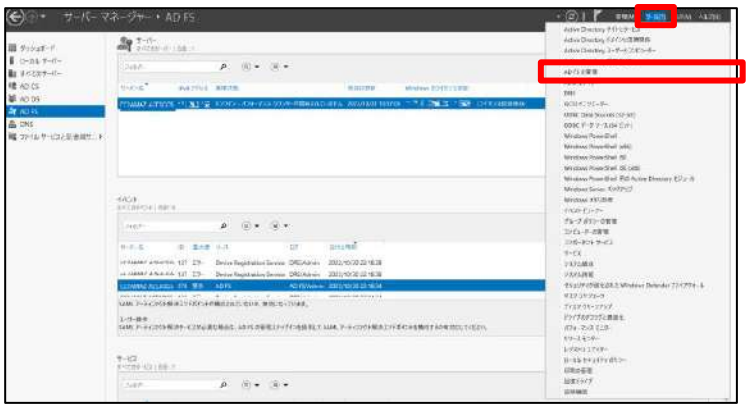
10 Active Directory設定

1．ADFS認証連携設定

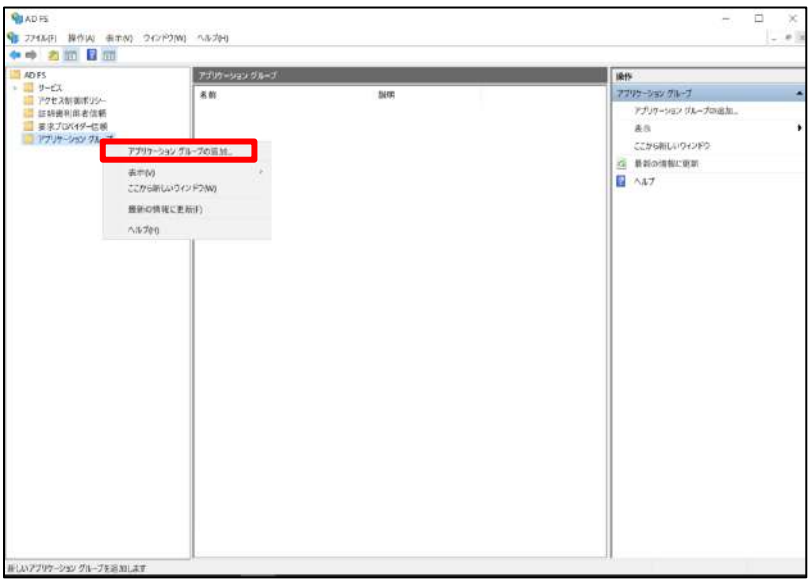
③ADFSに本サービスの連携設定 – アプリケーション グループの追加

IdPのADFSと本サービスの連携設定で、本サービスの通信を受け取る設定と、
本サービス上の「Active Directory設定」用設定値を取得します。

1．サーバーマネージャー – AD FSで、ツールメニューから「AD FSの管理」をクリックします。



2．AD FSの管理画面で、「アプリケーション グループ」を選択のうえ右クリックし、「アプリケーション グループの追加」をクリックします。

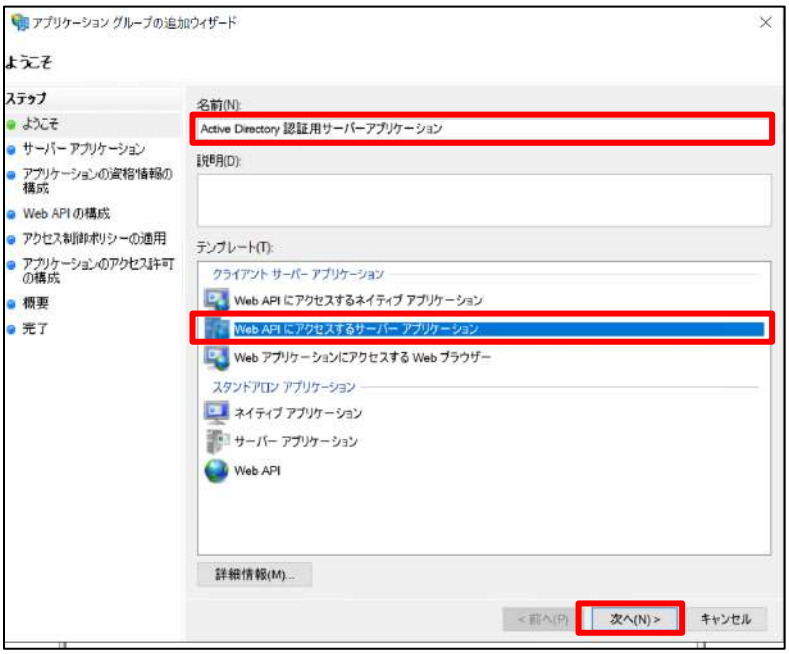


10 Active Directory設定

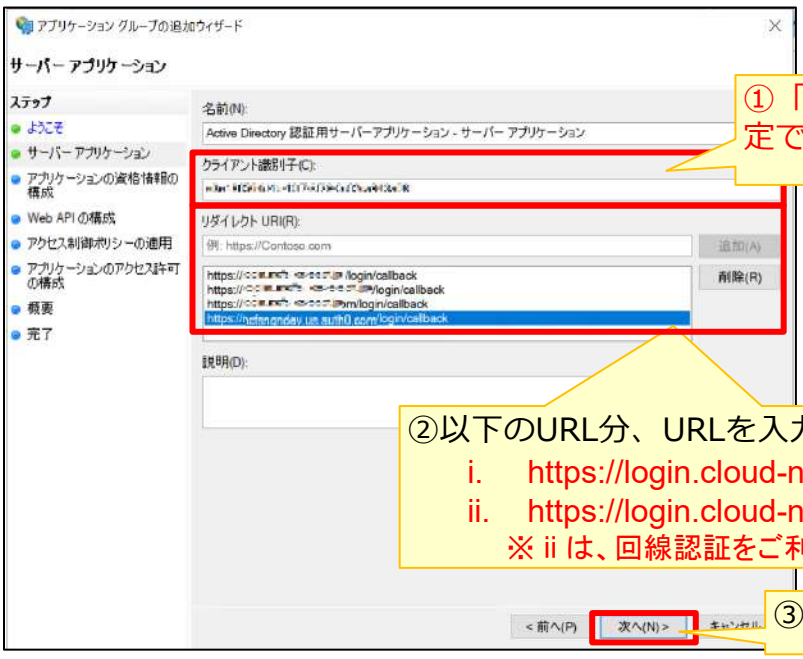
1．ADFS認証連携設定

③ADFSに本サービスの連携設定 – アプリケーション グループの追加

3．アプリケーション グループの追加ウィザードで、名前に任意のサーバーアプリケーション名を入力、テンプレートは「Web APIにアクセスするサーバー アプリケーション」を選択し、「次へ」をクリックします。



4．サーバーアプリケーションで、「クライアント識別子」は本サービスの「Active Directory設定」用設定で必要になる値のためテキストファイルへコピー＆ペーストなどを実施し、「リダイレクト URL」を設定のうえ、「次へ」をクリックします。



①「Active Directory設定」用設定で必要になる値のためメモ

②以下のURL分、URLを入力し「追加」をクリック
- i. https://login.cloud-nas.net/login/callback
- ii. https://login.cloud-nas.biz/login/callback

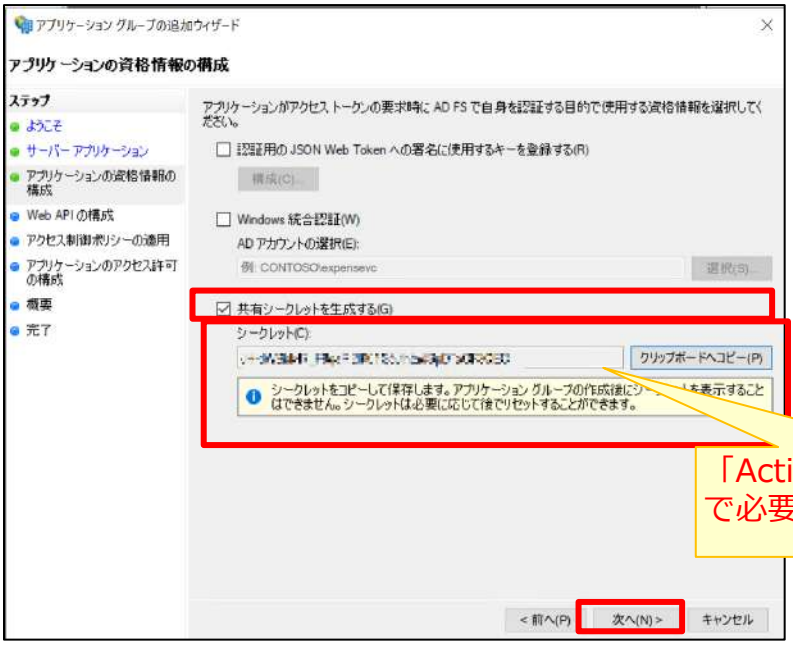
※ ii は、回線認証をご利用の場合に設定をお願いします。

③「次へ」をクリック

1．ADFS認証連携設定

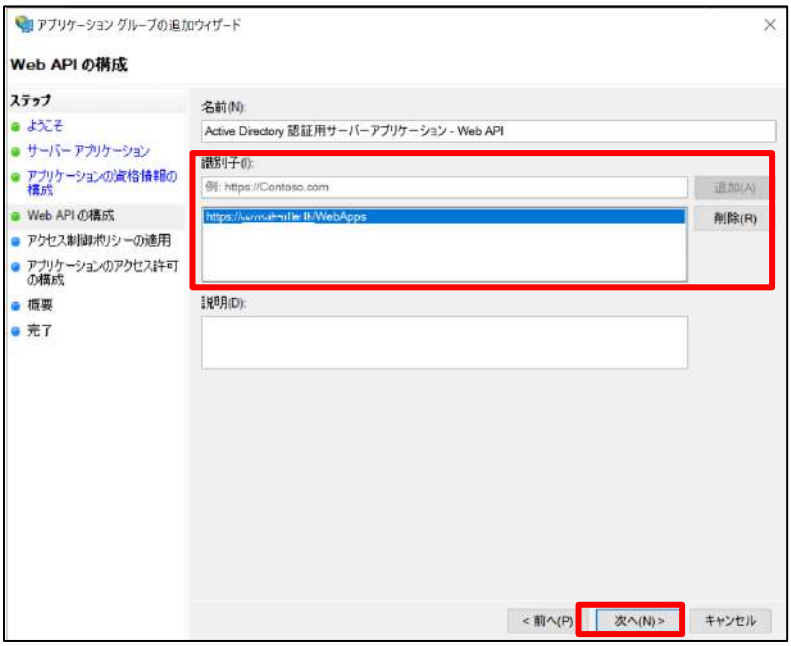
③ADFSに本サービスの連携設定 – アプリケーション グループの追加

5．アプリケーションの資格情報の構成で、「共有シークレットを生成する」をクリックすると「シークレット」が表示されます。
「シークレット」は本サービスの「Active Directory設定」用設定で必要になる値のためテキストファイルへコピー＆ペーストなどを実施し、「次へ」をクリックします。



「Active Directory設定」用設定で必要になる値のためメモ

6．Web APIの構成で、識別子に「https://<hostname>/WebApps」を設定し、「次へ」をクリックします。

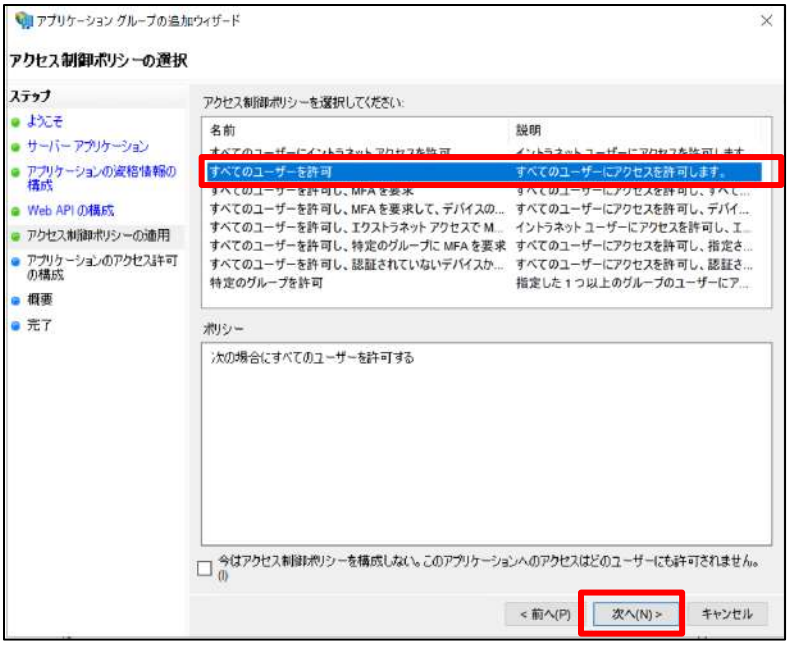


10 Active Directory設定

1．ADFS認証連携設定

③ADFSに本サービスの連携設定 – アプリケーション グループの追加

7．アクセス制御ポリシーの適用で、「すべてのユーザを許可」が選択されていることを確認し、「次へ」をクリックします。



8．アプリケーションのアクセス許可の構成で、「許可されているスコープ」を設定し、「次へ」をクリックします。

①以下にチェック
- Email
- openid
- profile

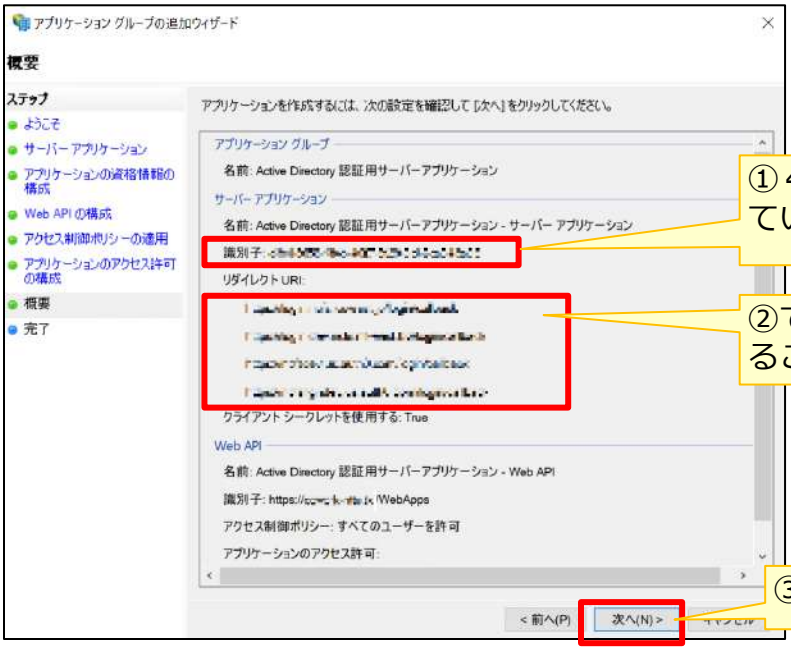
②「次へ」をクリック

10 Active Directory設定

1．ADFS認証連携設定

③ADFSに本サービスの連携設定 – アプリケーション グループの追加

9．概要で、これまで設定した値を確認し、「次へ」をクリックします。



8．アプリケーション グループの追加ウィザードでの完了画面が表示されます。
「閉じる」をクリックします。

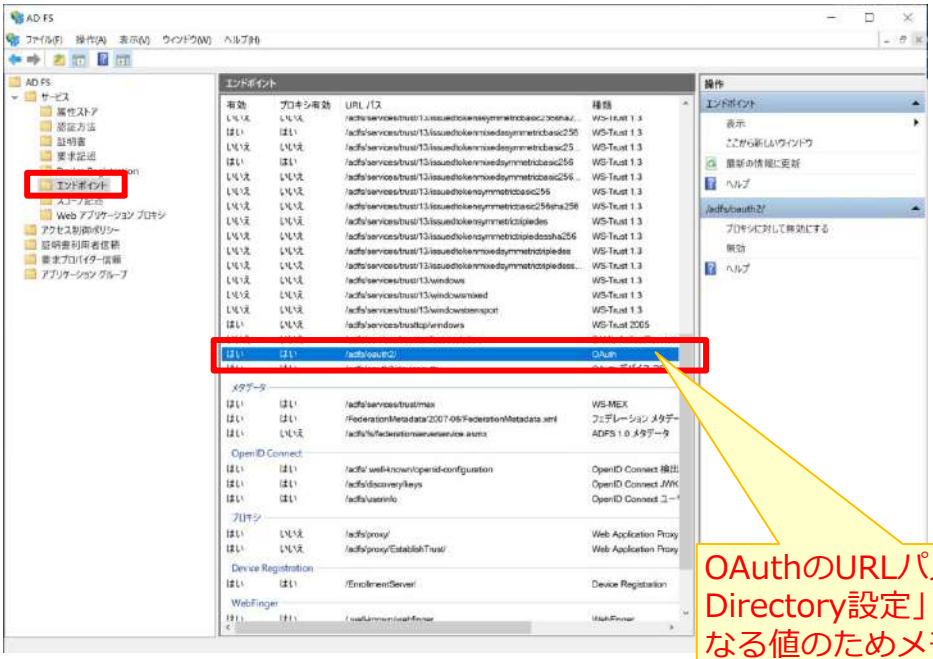
9．ADFSのサービスを再起動します。

10 Active Directory設定

1．ADFS認証連携設定

④ADFSに本サービスの連携設定 – エンドポイントURLの確認

AD FS管理画面で、サービス – エンドポイントを選択し、エンドポイントを表示します。



2．Active Directory設定

本サービス上で、Active Directory設定を実施します。
「１０．１．ADFS認証連携設定」で、下記の値が準備できているか確認してください。

- クライアント識別子（記載先「１０．１．ADFS認証連携設定」の「③」）
- 共有シークレット（記載先「１０．１．ADFS認証連携設定」の「③」）
- OAuthのURLパス（記載先「１０．１．ADFS認証連携設定」の「④」）

※準備できていない場合は、再度「１０．１．ADFS認証連携設定」をご確認ください。

Active Directory設定

１．ログイン画面にアクセスし、「パスワード変更、その他契約情報の変更はこちら」をクリックします。

パスワード変更、その他認証・契約情報の変更はこちらをクリック

2．Active Directory設定

Active Directory設定

2．認証・契約情報変更ログイン画面からログインします。

設定しているログイン方法でログイン

3．認証・契約情報変更メニューでActive Directory設定をクリックします 。

2．Active Directory設定

Active Directory設定

４．Active Directory設定画面で、「１０．１．ADFS認証連携設定」で取得した設定情報を入力し、設定をクリックします 。

①「Active Directoryサーバ OAuth2 認証エンドポイントURL 」に
https://<hostname>/OAuthのURLパス
を設定します。
例：https://<hostname>/adfs/oauth2

②「クライアントID」に
クライアント識別子を設定します。

③「クライアントシークレット」に
共有シークレットを設定します。

④「設定」をクリックします。

５．確認画面が表示されます。内容を確認のうえ、「」をクリックします。

2．Active Directory設定

Active Directory設定

6．Active Directory設定が完了し、再度Active Directory設定画面が表示されます。
また、契約者メールアドレスに、「Active Directoryアカウントのログイン用URL・接続ID通知」メールが届きます。

件名:【 M-Drive 】Active Directoryアカウントのログイン用URL・接続ID通知

本文：
〇〇　様
平素より、 M-Driveをご利用いただき誠にありがとうございます。
Active Directoryアカウントのログイン用URLおよび接続IDをご連絡いたします。
※契約者の方は、Active Directoryアカウントでログインをする利用者に対して、
事前に接続IDを通知してください。
利用者がログイン方法のActive Directoryアカウントに設定する際に、接続IDの入力が必要となります。

■Active Directoryアカウントのログイン用URL
・インターネット用：https://・・・
・回線認証用： https://・・・

■Active Directoryアカウントのログイン設定に必要な接続ID
・Active Directoryの接続ID adfs-XXXXXXXXXXXXXXX
M-Driveへログイン時に、
接続IDの入力画面が表示された場合、上記の接続IDを入力してください。

利用者のログイン方法の設定を「Active Directoryアカウント」に設定する際に、
「Active Directoryの接続ID」が必要となりますので、
ログイン方法の設定を「Active Directoryアカウント」に設定することを希望している利用者へ、「Active Directoryの接続ID」と
AD認証時、アカウントには[ADのユーザ名]@[ドメイン名]の形式での入力が必要であることを通知してください。

ここに注意

■契約者は、ADの設定変更が発生しますと、ADFSと本サービスと認証連携ができなくなる可能性があり、そのことにより本サービスへ「Active Directoryアカウント」によるログインができなくなる恐れがありますので、ログイン方法で「Active Directoryアカウント」は選択できません。

参考

Active Directory設定後、Active Directory設定が確認可能となります。
（利用者はActive Directory設定の変更は不可で確認のみです。）

1. 認証・契約情報変更ログイン画面からログイン
2. 認証・契約情報変更メニューでActive Directory設定をクリック
3. Active Directory設定の「Active Directoryの接続ID」を確認

11 インシデント管理

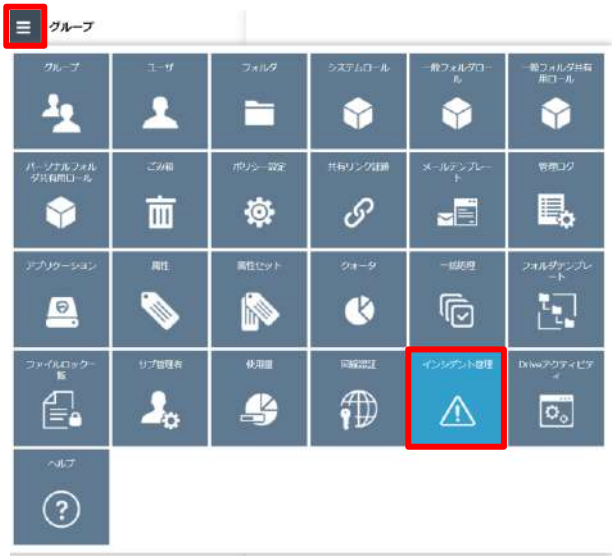
ランサムウェア検知･予防から被害ファイルの特定と復旧までが可能な
インシデント管理機能の利用方法について説明します。

1. 本サービスのWebにログインします。

2. **【ツール】** - **【管理コンソール】**をクリックします。

3. **【編集を開始する】**をクリックし、閲覧モードから編集モードへ変更します。

4．管理コンソールから**【インシデント管理】**クリックします。

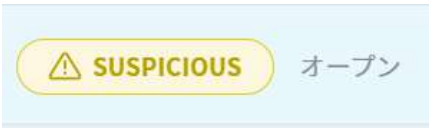


5．インシデント画面が表示されます。

11 インシデント管理

1．メイン画面

ストレージサービスDriveが疑わしい挙動として検知したインシデントがプロセス単位で一覧表示されます。
表示される種類としては以下の４種類です。



SUSPICIOUS（サスピシャス）：不審なプロセス検知・オープン状態・未処理
”疑わしい”として検知された状態です。「インシデントを見る」からインシデントの詳細を確認し、
このインシデントを”悪意のあるプロセスである”か”信頼されたプロセスである”かを判断する必要があります。

参考

検知したプロセスからのファイル更新が中断され、クラウド上のデータ更新がされない状態です。

MALICIOUS（マリシャス）：悪意のあるプロセスとして判断済み・オープン状態
”悪意のあるプロセスである”と判断され対処中の状態です。
（以降「悪意のあるプロセス」タブにも登録されます。）
該当プロセスが操作した他のファイルを”影響範囲の調査”で一覧を抽出、確認したうえで”ファイルの復旧”にて復旧させる必要があります。

ここに注意

悪意のあるプロセスとして判断すると、以降、組織内の全てのストレージサービスDriveで、このプロセスによって行われた未同期の変更は破棄されます。
慎重に確認・判断検討してください。

11 インシデント管理

1．メイン画面

TRUSTED（トラステッド）：信頼されたプロセスとして判断済み・オープン状態
”信頼されたプロセスである”と判断され対処中の状態です。
（以降「信頼されたプロセス」タブにも登録されます。）
問題がなければクローズしてインシデントを完了してください。

参考

検知したプロセスから通常利用と同様にクラウド上のデータ更新がされます。

ランサムウェアを誤って信頼済みプロセスと判断したとしても
このプロセスを信頼済みプロセスから削除し、
再度手動でインシデントとして起票しなおすことで
改めて悪意のあるプロセスと判断、ファイル復旧といった作業が可能です。

クローズ：処理済み・クローズ状態
インシデントの判断と対処が完了した状態です

11 インシデント管理

1．メイン画面

インシデントを起票

ストレージサービスDriveが検知していないプロセスを手動でインシデントとして登録することができます。

一度クローズしてしまったインシデントのプロセスを改めて処理したい時、
別途特定のプロセスをインシデントとして対応したい時　などに利用します。

「インシデントを起票」ボタンを押すと下記画面に遷移します。

インシデントの登録には、一覧に表示される”名前”と”実行ファイルのSHA256ハッシュ値”の入力が必要です。

”実行ファイルのSHA256ハッシュ値”について
過去にインシデントとして登録されたことがあるプロセスの場合、
「インシデントを見る」から”全般情報”内の”実行ファイルのSHA256”から確認できます。

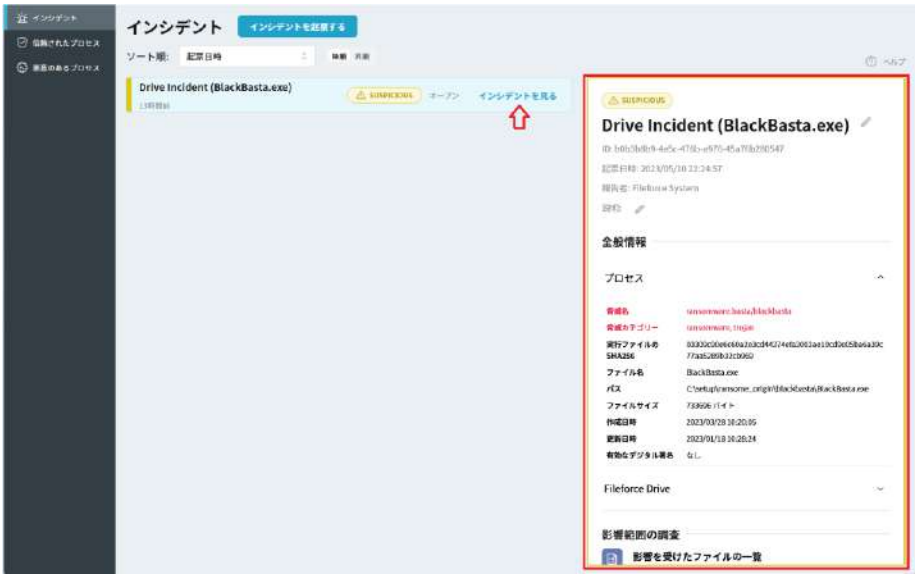
インシデントとして登録されたことのないプロセスのハッシュ値を取得する場合は
一般的な方法として下記ドキュメントを参照してください。

■Get-FileHash　（Microsoftドキュメント）※外部サイト

https://learn.microsoft.com/ja-jp/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-7.3

2．インシデントを見る（インシデントの詳細）

「インシデントを見る」からインシデントの詳細の確認と対応ができます。



全般情報
検知したプロセスの詳細と検知元のストレージサービスDriveの詳細を確認できます。

影響範囲の調査
このプロセスによって影響を受けたファイルを”過去にさかのぼって”一覧が作成できます。

「影響を受けたファイルを抽出する」を押すとリスト作成が始まります。
作成が完了すると以下のように画面が変わり、CSV形式のファイルで影響を受けたファイル一覧をダウンロード、確認ができます。

2．インシデントを見る（インシデントの詳細）

解決
このインシデントを”悪意のあるプロセス”か”信頼されたプロセス”かを判定します。

判定の際に、各々判定理由が必要になります。

・悪意のあるプロセスである　→　MALICIOUS（マリシャス）

・信頼されたプロセスである　→　TRUSTED（トラステッド）

2．インシデントを見る（インシデントの詳細）

ファイルの復旧
「影響を受けたファイルを抽出する」の結果をもとに復旧する範囲を指定してファイルを復旧します。完了すると下記のように結果がダウンロードできるようになります。

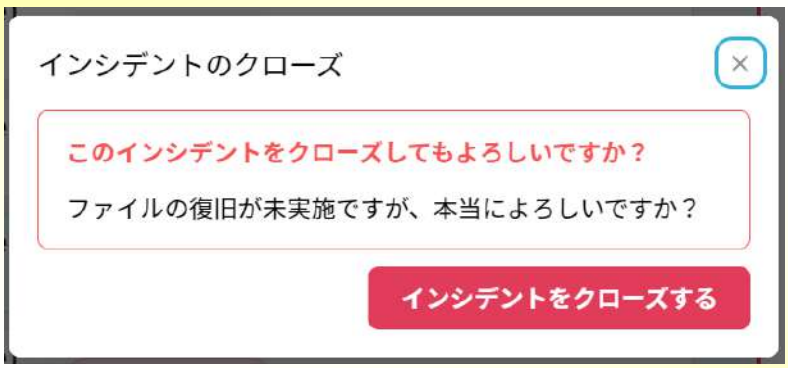
参考

復旧対象のファイル数などにより時間がかかる場合があります。

クローズ
インシデントをクローズします。

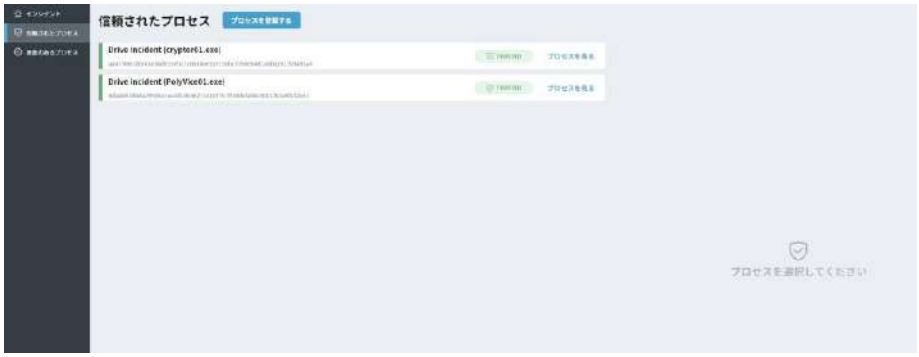
ここに注意

ファイル復旧を行っていない場合、下記メッセージが表示されます。クローズ後に復旧が必要な場合、改めて「インシデント起票」から
インシデントを作成する必要があります。



3．信頼されたプロセス

”信頼されたプロセスである”と判定されたプロセスが一覧表示されます。



「プロセスを見る」を押すと、該当プロセスのハッシュ値を確認できます。

オープン中のインシデント（未クローズのインシデント）は「プロセスを削除する」ボタンがグレーアウトしていますが、クローズされたインシデントは「プロセスを削除する」が有効になり削除ができるようになります。

誤ってインシデントを”信頼されたプロセスである”と判定してしまった場合、
一度インシデントをクローズして削除を行ってください。

3．信頼されたプロセス

プロセスを登録する

手動でプロセスを登録できます。

インシデントの登録には、一覧に表示される”名前”と”実行ファイルのSHA256ハッシュ値”の入力が必要です。

”実行ファイルのSHA256ハッシュ値”について
過去にインシデントとして登録されたことがあるプロセスの場合、インシデント一覧から「インシデントを見る」から”全般情報”内の”実行ファイルのSHA256”から確認できます。

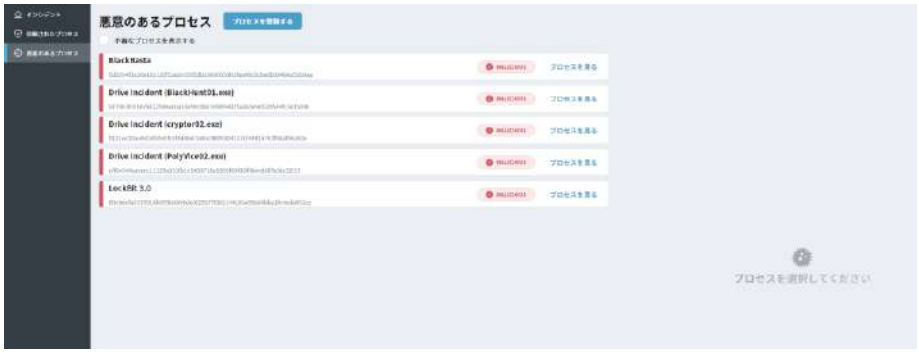
インシデントとして登録されたことのないプロセスのハッシュ値を取得する場合は一般的な方法として下記ドキュメントを参照してください。

■Get-FileHash　（Microsoftドキュメント）※外部サイト

https://learn.microsoft.com/ja-jp/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-7.3

4．悪意のあるプロセス

”悪意のあるプロセスである”と判定されたプロセスが一覧表示されます。



参考

「不審なプロセスを表示する」をチェックすると
SUSPICIOUS（サスピシャス）となったプロセスも表示されます。

「プロセスを見る」を押すと、該当プロセスのハッシュ値を確認できます。

オープン中のインシデント（未クローズのインシデント）は「プロセスを削除する」ボタンがグレーアウトしていますが、クローズされたインシデントは「プロセスを削除する」が有効になり削除ができるようになります。

誤ってインシデントを”悪意のあるプロセスである”と判定してしまった場合、
一度インシデントをクローズして削除を行ってください。

4．悪意のあるプロセス

プロセスを登録する

手動でプロセスを登録できます。

インシデントの登録には、一覧に表示される”名前”と”実行ファイルのSHA256ハッシュ値”の入力が必要です。

”実行ファイルのSHA256ハッシュ値”について
過去にインシデントとして登録されたことがあるプロセスの場合、インシデント一覧から「インシデントを見る」から”全般情報”内の”実行ファイルのSHA256”から確認できます。

インシデントとして登録されたことのないプロセスのハッシュ値を取得する場合は一般的な方法として下記ドキュメントを参照してください。

■Get-FileHash　（Microsoftドキュメント）※外部サイト

https://learn.microsoft.com/ja-jp/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-7.3

5．【参考】検知されたインシデントの調べ方

検知されたインシデントが悪意のあるプロセスであるかどうかの調べ方について一例を記載します。

プロセスハッシュからの確認

インシデント管理の全般情報から、検知された疑わしいプロセスのハッシュ値を確認することができます。
（”**実行ファイルのSHA256**”が該当の項目です）

このハッシュ値を、以下のような複数のアンチウイルスエンジンで検査可能なサイトで検索することで、検知されたプロセスがランサムウェアかどうかの判断に使用することができます。

«参考サイト»
VirusTotal　※外部サイト
https://www.virustotal.com/gui/home/search

参考

プロセスのハッシュ値とは
プロセスを一意に識別するために使用される固定長の値です。
プロセスのデータから生成され、プロセスが異なる場合は異なる値が生成されます。

5．【参考】検知されたインシデントの調べ方

プロセスハッシュからの確認

判断ポイントとして、たとえば以下の情報をランサムウェアかどうかの判断に活用することができます。

・アンチウイルスエンジンの検出数
レポートの先頭に、スキャンに使用された各アンチウイルスエンジンでどのように判定されたかの統計が表示されます。
検出数が多いほど、ランサムウェアとしての疑いが高いと考えられます。

・検出されたランサムウェアの名称
検出されたランサムウェアの名称を確認してください。
もしその名称が既知のランサムウェアである場合、ファイルやURLがランサムウェアである可能性が高いです。

・セキュリティ ベンダーの検出情報
各セキュリティ ベンダーにどのように判定されたかを確認することができます。

！ ここに注意

インシデント検知の際に自動的にプロセスのハッシュの確認を行っています。
脅威情報であった場合、

脅威名
脅威カテゴリー

に記載されています。”ransomware”（ランサムウエア）、”trojan”（トロイの木馬）といった 記載があった場合、他のセキュリティ ベンダーでも脅威とみなされたものとして”危険性が高い”と判断できます。

※すべてのランサムウェアが脅威名、脅威カテゴリーが表示されるわけではないため
「表示されていない=問題がない」というわけではありません。
影響を受けたファイルの確認や、端末の操作者への確認など総合的に確認してください。

5．【参考】検知されたインシデントの調べ方

”影響を受けたファイルの一覧”の確認

プロセスのハッシュ値からは判断できなかった場合、もしくはランサムウェアではない可能性が高い場合でも、プロセスによって操作されたファイルの一覧を確認してください。
検知されたDriveのユーザに対して、意図したファイル操作かどうかを確認し操作がユーザによって意図されたものであるかを確認してください。

その他、有名なランサムウエアの関連プロセスは
すでにインターネット上で情報が公開され警戒が呼びかけられている場合があります。
プロセス名をインターネット上で検索し脅威情報として周知されているものではないか確認してください。

«参考サイト»
・公的機関運営サイト
ランサムウエア対策特設サイト
https://www.jpcert.or.jp/magazine/security/nomore-ransom.html

情報処理推進機構（IPA）
ランサムウェア対策特設ページ
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

・民間企業運営サイト
ランサムウェア対策2023
https://cybersecurity-jp.com/ransomware/column/93/

12 Driveアクティビティ

プロセス、ユーザごとの動作が期間別の統計としてグラフ化されます。

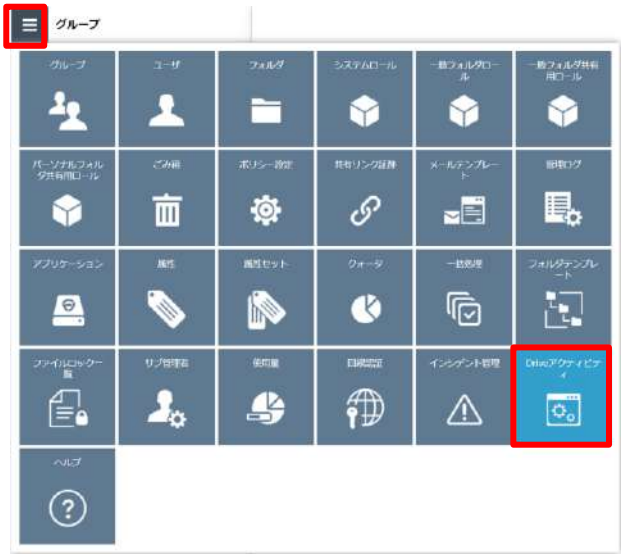
Driveアクティビティについて説明します。

1. 本サービスのWebにログインします。

2. **【ツール】** - **【管理コンソール】**をクリックします。

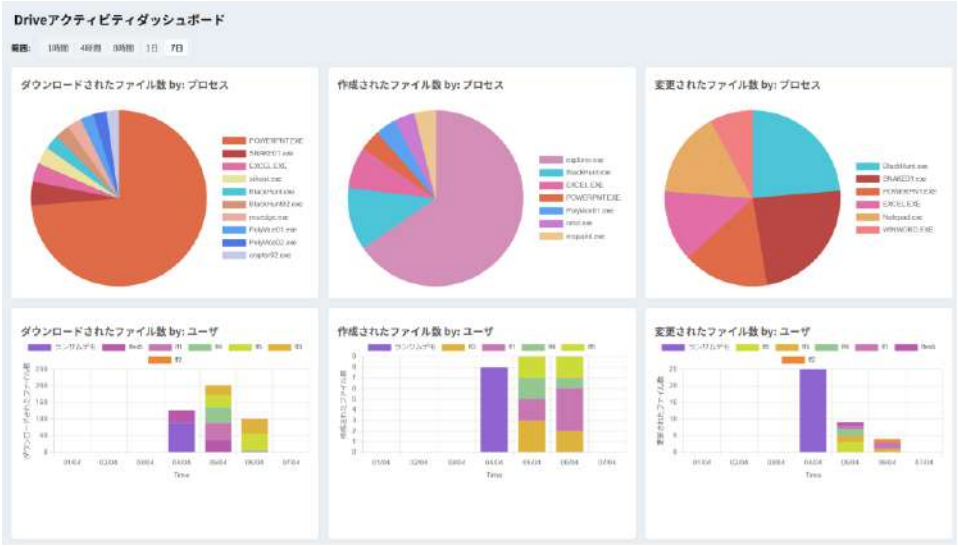
3. **【編集を開始する】**をクリックし、閲覧モードから編集モードへ変更します。

4．管理コンソールから**【Driveアクティビティ】**クリックします。



5．Driveアクティビティ画面が表示されます。

12 Driveアクティビティ



画面上部の「期間」を切り替えることで、集計範囲を選択できます。

参考

■グラフに表示されるデータサンプリングについての補足

基本的にユーザ、プロセスともに数が多いものが優先的に表示されます。
そのため範囲の指定によっては表示対象外となるユーザ、プロセスがある場合があります。