VVAULT® AUDIT

# ユーザーズマニュアル

Users Manual for VVAULT AUDIT 4.5

# はじめに

## 本文書のご利用にあたって

- 本文書の内容の一部または全部を著作者の許諾なしに複製、改変、および翻訳することは、著作権法下での許可事項を除き禁止されています。
- 本文書で使用している情報及び画像は本文書執筆時点のもので、最新版の製品および製品サイトと文言やデザイン等が異なる場合があります。
- 本文書内の社名、製品名は各社の商標又は登録商標です。

# 目次

# 1 VAビューアーへのアクセス

Users Manual for VVAULT AUDIT 4.5

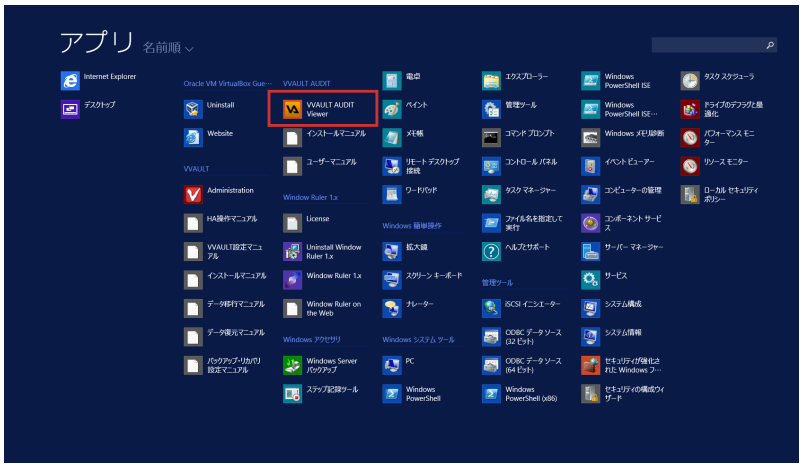
# 1-1
# VAビューアーの起動

本製品のVAビューアーを起動するには以下の手順に従ってください。

## 手順解説

①「スタートメニュー」を開き、表示された下方向の矢印をクリックします。


②「VVAULT AUDIT Viewer」をクリックすると、アプリケーションが起動し、VAビューアーのログイン画面が表示されます。

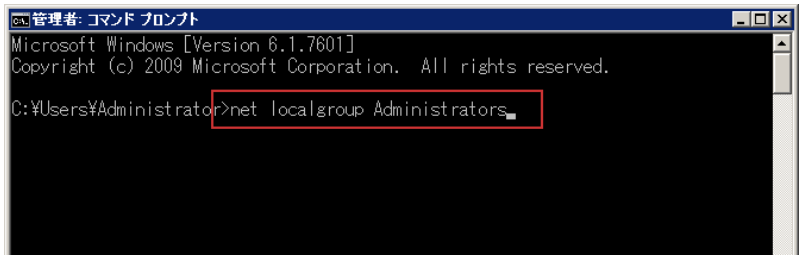


# 1-2
# 有効なアカウント名の確認

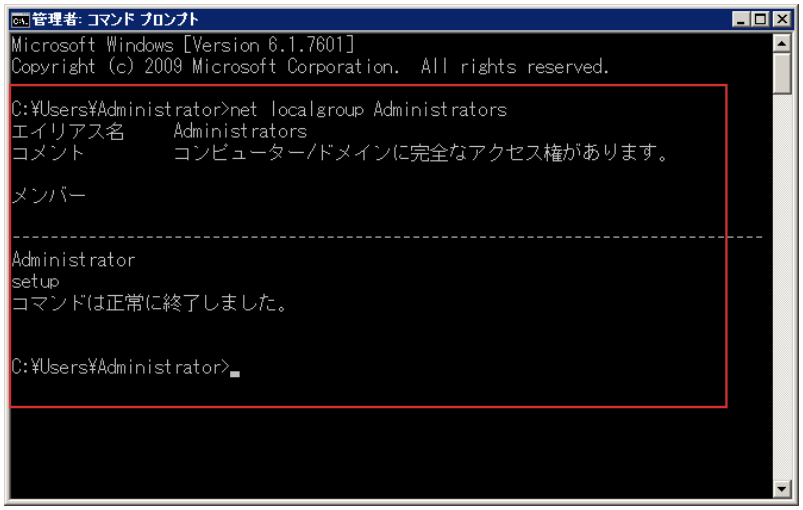
VAビューアーに接続するには、OSのAdministratorsグループに存在するアカウント名、およびパスワードが必要となります。ただし、実際のアカウント名と表示されている名称が異なる場合がありますので、以下の手順に従い、管理者の実際のアカウント名をご確認ください。

## 手順解説

① 「コマンドプロンプト」にて、「net localgroup Administrators」と入力し、実行します。




② 管理者アカウントの一覧が表示されますので確認します。この例では「Administrator」が実際のアカウント名となります。




**ワンポイント**

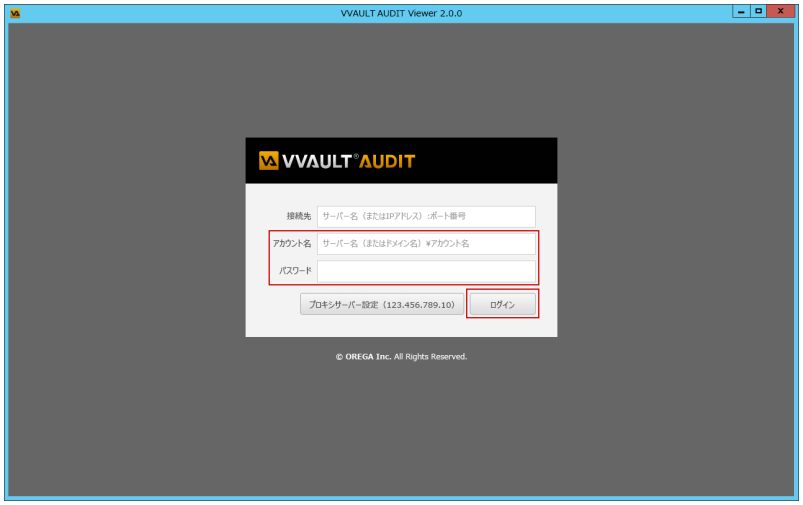
漢字名称の場合でもアカウント名として使用可能です。また、パスワードを設定していない場合は空白のままとしてください。

# 1-3
# VAビューアーの使用

VAビューアーを使用するには以下の手順で認証を行ってください。尚、認証画面へのアクセス方法は「1-1 VAビューアーの起動（P.6）」を、認証に失敗する場合は、「1-2 有効なアカウント名の確認（P.7）」をご覧ください。

## 認証の手順

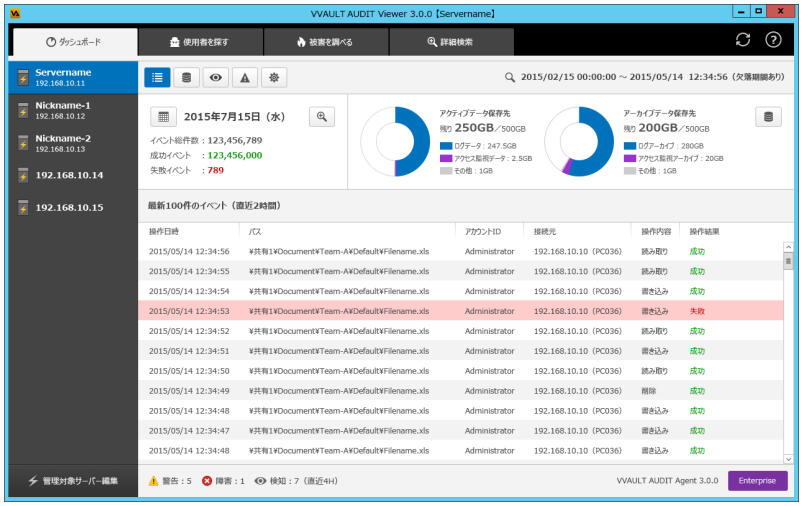
① OSのAdministratorsグループに存在するアカウント名とパスワードを入力し、「ログイン」ボタンをクリックします。




**ワンポイント**

接続先を変えることで別コンピューターにインストールされたVVAULT AUDITへ接続することも可能です。その際は接続先のコンピューターで有効なアカウントとパスワードを指定してください。
接続先のコンピューターに対してプロキシサーバーを利用する際は「プロキシサーバー設定」ボタンから設定してください。設定について「**インストールマニュアル**」「**3-2 各部の名称と設定**」を参照してください。

② 以下の画面に切り替わり、認証が完了します。

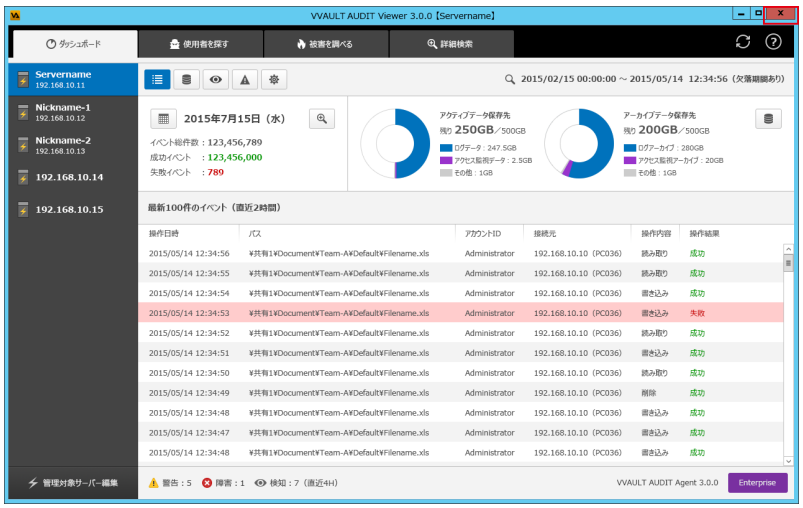



**ワンポイント**

エージェントサービスとの接続に失敗する場合は、Windowsサービス一覧より「VVAULT AUDIT Agent」が起動していることを確認し、起動している場合はサービスを再起動してください。

# 切断の手順

① VA ビューアーの右上端にある「×」ボタンをクリックします。




② 切断され、ウィンドウが閉じられます。

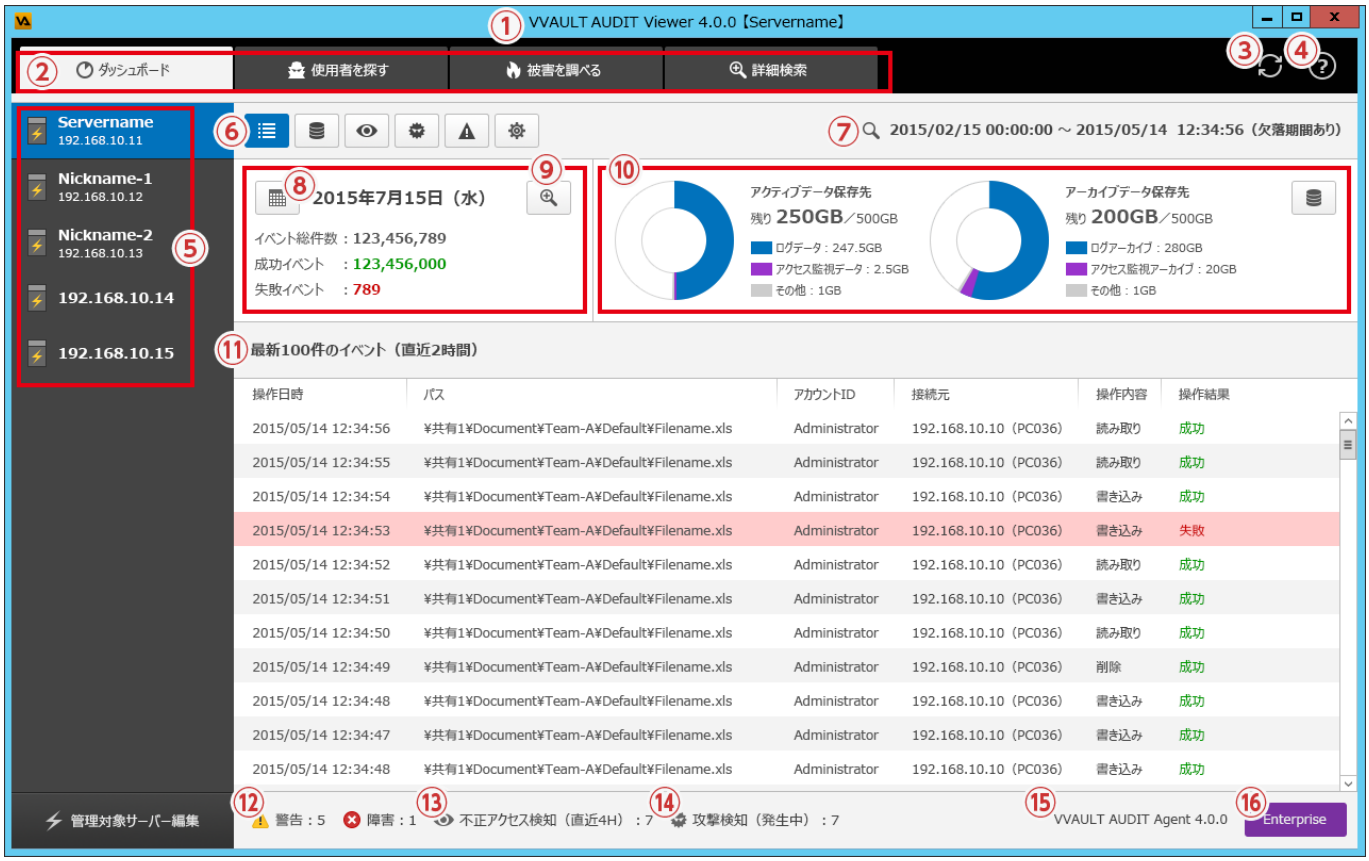
### ワンポイント

VA ビューアーは 120 分間「検索操作」が行われないと、セッションがタイムアウトします。セッションタイムアウトした際は、再度認証を実行してください。

# 1-4
# 各部の名称と役割

VAビューアーへの認証後に表示される「ダッシュボード サマリー画面」です。
ここではサーバーリストで選択された管理対象サーバーの日次で集計されたイベント件数、ストレージの使用量、最新の監査ログ100件などが確認できます。

ダッシュボードサマリー画面




## 名称と役割

① ビューアーバージョン
現在起動しているVVAULT AUDIT Viewerのバージョンと、接続先サーバー（コントローラー）のマシン名を表示します。

② メニュータブ
ダッシュボードと各種検索メニューがタブで表示されます。各種検索については「2-1 ログの検索について（P.14）」をご参照ください。

③ [リロード] ボタン
画面をリフレッシュします。

④ [ヘルプ] ボタン
VVAULT AUDITのマニュアルをダウンロードします。

⑤ **サーバーリスト**
最上部はコントローラー、それ以下は追加された管理対象サーバーの一覧を表示します。

⑥ **メニューボタン**
VVAULT AUDIT Viewerの各画面へ遷移するボタンです。
左から
・サマリー画面へ
・データ管理画面へ
・アクセス監視画面へ
・攻撃検知画面へ
・警告・障害画面へ
・システム設定画面へ

⑦ **検索可能期間**
DBデータに格納されているログテーブルから、最古と最新の日付を取得して表示します。

※この期間内で欠落したデータが検出された場合は「欠落データあり」という文言が表示されます。欠落している期間についてはデータ管理画面にて確認することができます。

⑧ **カレンダー**
検索可能期間を青字で表示します。

⑨ **日次集計データ**
[イベント件数]……対象日でVVAULT AUDITに記録されたイベントの総件数です。
[成功イベント]……対象日で操作結果が成功となったイベントの件数です。
[失敗イベント]……対象日で操作結果が失敗となったイベントの件数です。
[この日のログを見る]……対象日の条件を転記した状態で詳細検索画面を開きます。

⑩ **使用状況**
アクティブデータ（DBデータ）保存先およびアーカイブ保存先のストレージ情報を表示します。
（アーカイブ保存先の表示は、アーカイブ保存先設定時のみ）

※「その他」は対象ストレージの使用領域から、VVAULT AUDITでの使用サイズを差し引いた値です。

⑪ **最新100件のイベント（直近2時間）**
直近2時間で記録された監査ログのうち、最新の100件を表示します。

⑫ **警告・障害情報**
発生している警告・障害の総件数を表示します。

⑬ **検知件数**
全ルールで直近4時間に検知された検知件数の合計を表示します。

⑭ **攻撃検知（発生中）**
攻撃検知した履歴で終息していない件数の合計を表示します。

⑮ **エージェントバージョン**
エージェントサービスのバージョンを表示します

⑯ **ライセンス**
登録されたライセンス名を表示します。

# 2 ログの検索

Users Manual for VVAULT AUDIT 4.5

# 2-1
# ログの検索について

VVAULT AUDITは、Windowsイベントログに記録されたセキュリティログの中から、タスクのカテゴリが「詳細なファイル共有」(イベントID 5145) のみをデータベースに登録しています。

| コード | アクセス要求 | VVAULT AUDITでの日本語変換 | VVAULT AUDITでの操作分類 |
|---|---|---|---|
| 1537 | DELETE | 削除 | 削除 |
| 1538 | READ_CONTROL | セキュリティ情報の読み取り | その他 |
| 1539 | WRITE_DAC | アクセス権の変更 | その他 |
| 1540 | WRITE_OWNER | 所有者の変更 | その他 |
| 1541 | SYNCHRONIZE | 同期 | その他 |
| 1542 | ACCESS_SYS_SEC | アクセス システム セキュリティ | その他 |
| 1801 | Granted by | 許可元 | その他 |
| 1802 | Denied by | 拒否元 | その他 |
| 1803 | Denied by Integrity Policy check | インテグリティポリシーのチェックで拒否されました | その他 |
| 1804 | Granted by Ownership | 所有権によって許可されました | その他 |
| 1805 | Not granted | 許可されていません | その他 |
| 4416 | ReadData (or ListDirectory) | データの読み取り (またはフォルダー一覧の読み取り) | 読み込み |
| 4417 | WriteData (or AddFile) | データの書き込み (またはファイルの追加) | 書き込み |
| 4418 | AppendData (or AddSubdirectory or CreatePipeInstance) | データの追記 (またはサブフォルダーの追加 または パイプインスタンスの作成) | 書き込み |
| 4419 | ReadEA | 拡張属性の読み取り | その他 |
| 4420 | WriteEA | 拡張属性の書き込み | その他 |
| 4421 | Execute/Traverse | 実行／スキャン | その他 |
| 4422 | DeleteChild | 子要素の削除 | その他 |
| 4423 | ReadAttributes | 属性の読み取り | その他 |
| 4424 | WriteAttributes | 属性の書き込み | その他 |

## 使用者を探す

特定のデータにアクセスしたユーザーを検索します。
（例）・ファイルやフォルダを削除したユーザーを検索調べたい。
・ファイルの操作履歴を調べたい。

## 被害を調べる

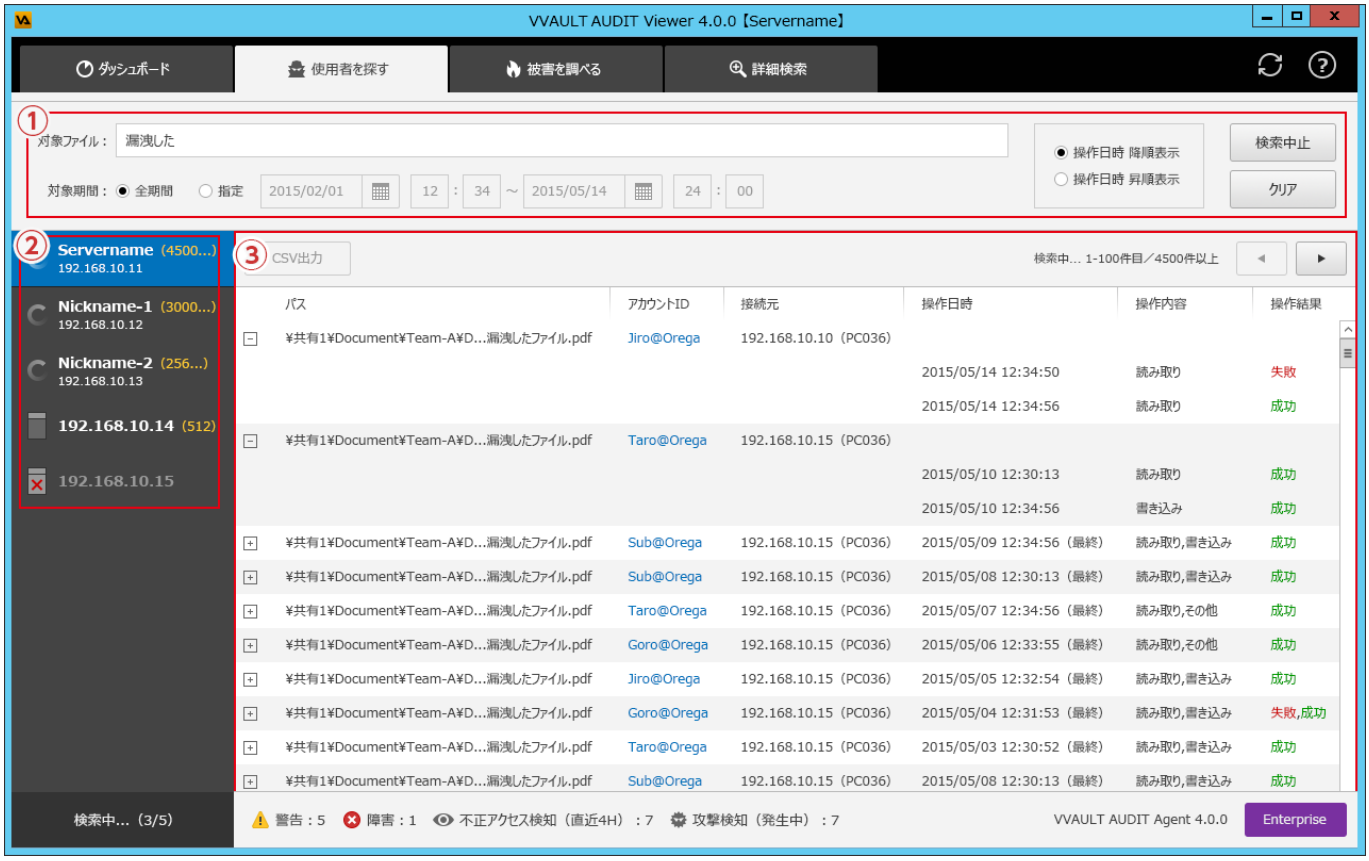
特定のユーザーがアクセスしたデータを検索します。
（例）・退職者の１ヶ月間の操作を調べたい。

## 詳細な条件で検索する

操作（読み取り、書き込み、削除）など、様々な条件でユーザーやデータを検索します。
（例）・権限のないデータにアクセスしようとしたユーザーを調べたい。
・特定のフォルダで最近削除されたファイルを調べたい。

# 2-2
# 基本構成と名称の役割

本製品は、複数のサーバーを対象にした「統合検索」に対応しており、すべての検索画面において以下のようなレイアウトになっています。




## 名称と役割

**① 検索条件**

検索条件を入力するエリアです。

**② サーバーリスト**

検索対象サーバーの一覧と検索ヒット数を表示します。検索中は下部に検索が完了したサーバー数がカウントされます。

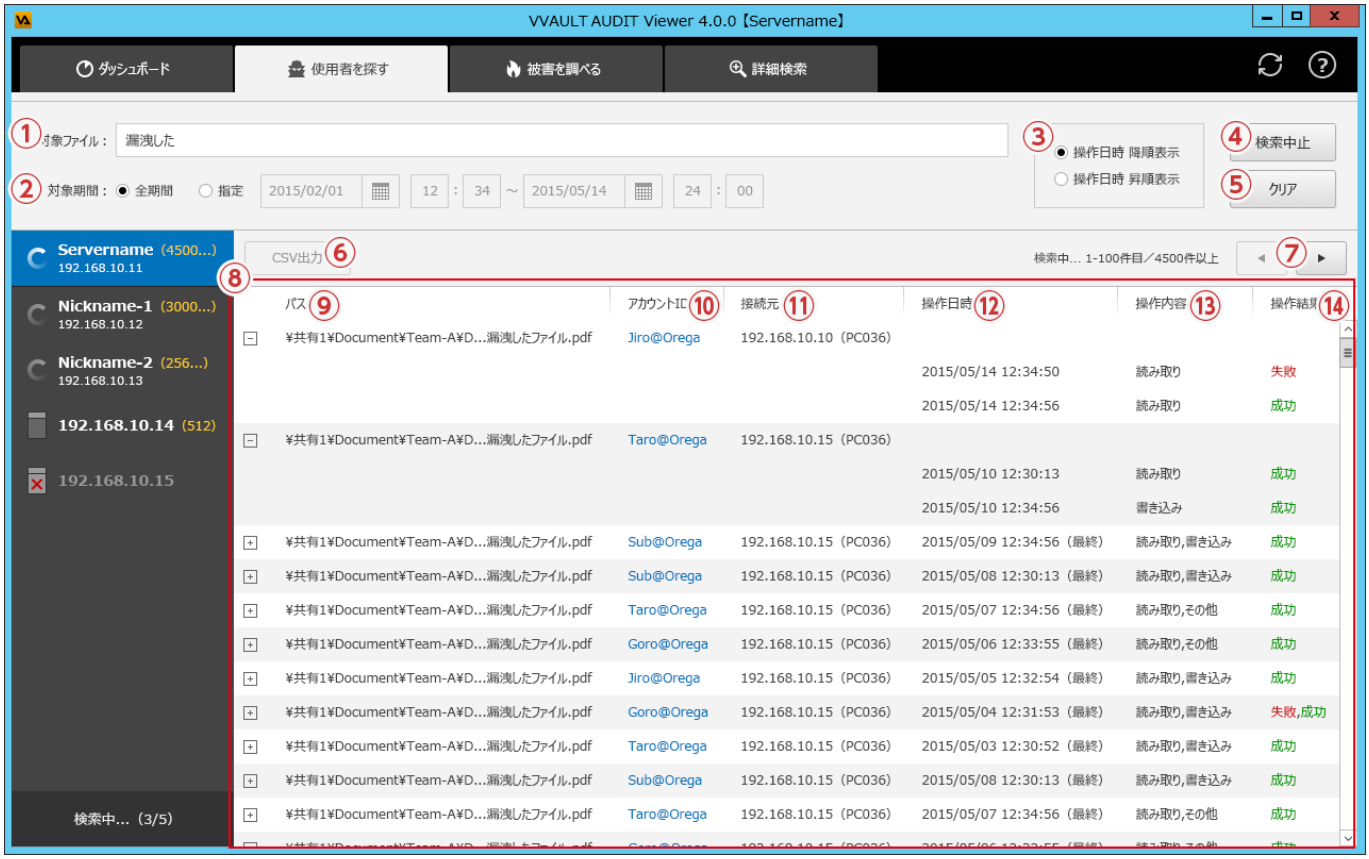
**③ 検索結果レコード**

検索にヒットしたレコードを表示します。

# 2-3
# 使用者を探す

特定のデータにアクセスしたユーザーを検索するための画面です。
※「読み取り」「書き込み」「削除」操作のみが検索対象となります。

## 「使用者を探す」画面




## 名称と役割

**① 対象ファイル**
検索したいファイル名、またはフォルダ名を入力します。(部分一致検索)

**② 対象期間**
検索の対象期間を選択します。「指定」の場合、任意の期間を入力します。

**③ ソート順**
検索結果のソート(昇順／降順)を選択します。

**④ [検索] ボタン**
指定した条件で検索を実行します。なお検索中は「キャンセル」ボタンをクリックすることで検索を中断することができます。

**⑤ [クリア] ボタン**
指定した条件と検索結果をクリアします。

**⑥ [CSV出力] ボタン**
検索結果から以下のフォーマットでCSVファイル(BOM付きUTF-8)を作成します。
”パス”／”アカウントID”／”グループID”／”接続元”／”操作日時”／”操作内容”／”操作結果”

**⑦ ページネーションボタン**
検索結果レコードのページ移動を行います。

**⑧ 検索結果レコード**
指定条件にヒットしたログレコードです。同じ「接続元」「アカウントID」「グループID」「パス」が連続するレコードをグループ化します。グループ化されたレコードにはサマライズした情報が表示されます。実際のログを見るには[+]ボタンをクリックして、ログレコードを表示させてください。ダブルクリックすると別ウィンドウが開き、ログの詳細を表示します。

**⑨ パス**
共有フォルダ上のフルパスを表示します。

**⑩ アカウントID**
「アカウント名」@「ドメイン名(ワークグループの場合はマシン名)」を表示します。クリックすることで条件を保持して詳細検索画面へ遷移します。

**⑪ 接続元**
アクセスしたマシンのIPアドレスとコンピューター名を表示します。

**⑫ 操作日時**
操作した日時を表示します。グループ化された親レコードでは、グループ内レコードの最終操作日時を表示します。

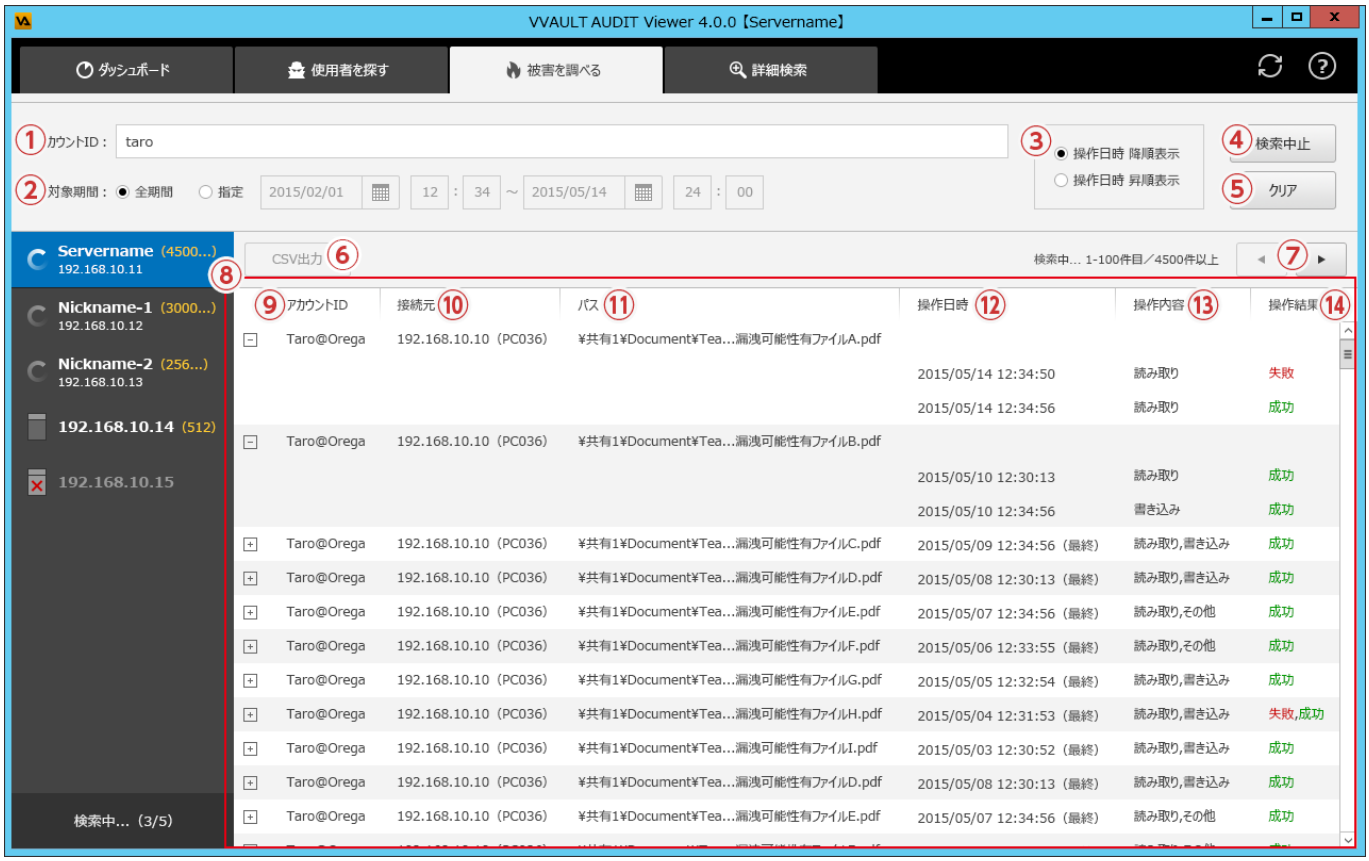
**⑬ 操作内容**
「読み込み」「書き込み」「削除」のいずれかの操作を表示します。

**⑭ 操作結果**
操作結果を「成功」または「失敗」で表示します。

# 2-4
# 被害を調べる

特定のユーザーがアクセスしたデータを検索する画面です。
※「読み取り」「書き込み」「削除」操作のみが検索対象となります。

## 「被害を調べる」画面




## 名称と役割

**① アカウントID**
検索したい「アカウント名」を入力します。(カンマ区切りで複数指定可能)
ドメイン名(ワークグループの場合はコンピューター名)も含めて検索する場合は「アカウント名@ドメイン名」のようにアットマークで区切ってください。ドメイン名のみで検索する場合は「@ドメイン名」のように先頭にアットマークを追加してください。

**② 対象期間**
検索の対象期間を選択します。「指定」の場合、任意の期間を入力します。

**③ ソート順**
検索結果のソート(昇順／降順)を選択します。

**④ [検索] ／ [検索中止] ボタン**
指定した条件で検索を実行します。なお検索中は[検索中止]ボタンをクリックすることで検索を中断することができます。

**⑤ [クリア] ボタン**
指定した条件と検索結果をクリアします。

⑥ **[CSV出力]ボタン**
検索結果から以下のフォーマットでCSVファイル(BOM付きUTF-8)を作成します。
”アカウントID”／”グループID”／”接続元”／”パス”／”操作日時”／”操作内容”／”操作結果”

⑦ **ページネーションボタン**
検索結果レコードのページ移動を行います。

⑧ **検索結果レコード**
指定条件にヒットしたログレコードです。同じ「アカウントID」「グループID」「接続元」「パス」が連続するレコードをグループ化します。グループ化されたレコードにはサマライズした情報が表示されます。実際のログを見るには[+]ボタンをクリックして、ログレコードを表示させてください。ダブルクリックすると別ウィンドウが開き、ログの詳細を表示します。

⑨ **アカウントID**
「アカウント名」@「ドメイン名(ワークグループの場合はコンピューター名)」を表示します。

⑩ **接続元**
アクセスしたコンピューターのIPアドレスとコンピューター名を表示します。

⑪ **パス**
共有フォルダ上のフルパスを表示します。

⑫ **操作日時**
操作した日時を表示します。グループ化された親レコードでは、グループ内レコードの最終操作日時を表示します。

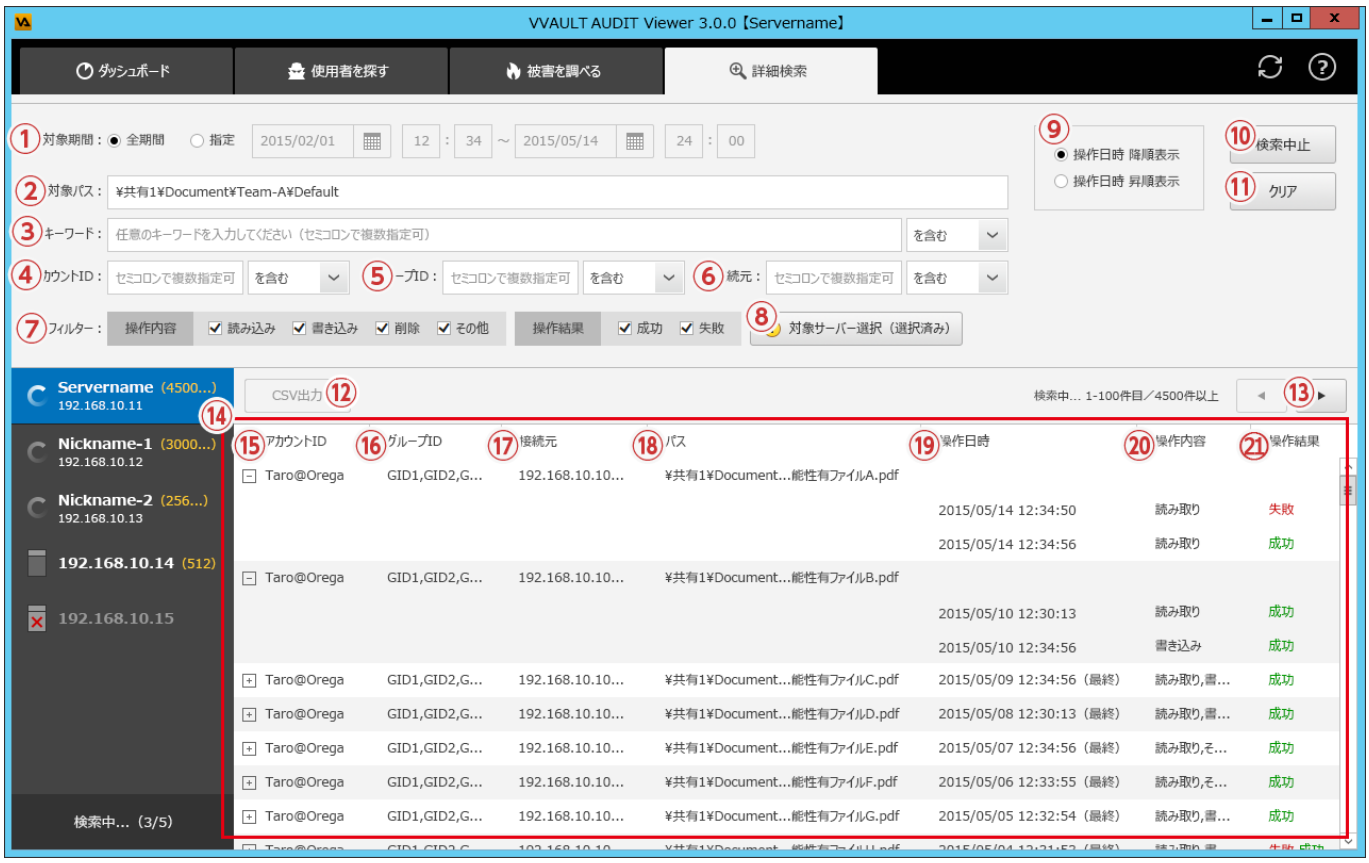
⑬ **操作内容**
「読み込み」「書き込み」「削除」のいずれかの操作を表示します。

⑭ **操作結果**
操作結果を「成功」または「失敗」で表示します。

# 2-5
# 詳細な条件で検索する

詳細な条件をログを検索する画面です。操作が「失敗」と記録されたレコードは背景色が赤くハイライトされます。

詳細検索画面




## 名称と役割

### ① 対象期間
検索の対象期間を選択します。「指定」の場合、任意の期間を入力します。

### ② 対象パス
検索したいデータのパスを入力します。（パスの前方一致検索）

### ③ キーワード
検索したデータのキーワードを入力します。

### ④ アカウントID
検索したい「アカウント名」を入力します。（セミコロン区切りで複数指定可能）
ドメイン名（ワークグループの場合はコンピューター名）も含めて検索する場合は「アカウント名@ドメイン名」のようにアットマークで区切ってください。ドメイン名のみで検索する場合は「@ドメイン名」のように先頭にアットマークを追加してください。

### ⑤ グループID
検索したい「グループ名」を入力します。（セミコロン区切りで複数指定可能）

### ⑥ 接続元
検索したい接続元のIPアドレスまたはコンピューター名を入力します。

⑦ **フィルター**
[操作内容]……検索したい操作内容(読み込み、書き込み、削除、その他)を選択します。
[操作結果]……検索したい操作結果(成功、失敗)を選択します。

⑧ **[対象サーバー選択]ボタン**
検索対象サーバー選択ウィンドウを表示します。

⑨ **ソート順**
検索結果のソート(昇順/降順)を選択します。

⑩ **[検索]/[検索中止]ボタン**
指定した条件で検索を実行します。なお検索中は[検索中止]ボタンをクリックすることで検索を中断することができます。

⑪ **[クリア]ボタン**
指定した条件と検索結果をクリアします。

⑫ **[CSV出力]ボタン**
検索結果から以下のフォーマットでCSVファイル(BOM付きUTF-8)を作成します。
"操作日時"/"パス"/"アカウントID"/"グループID"/"接続元"/"操作内容"/"操作結果"

⑬ **ページネーションボタン**
検索結果レコードのページ移動を行います。

⑭ **検索結果レコード**
指定条件にヒットしたログレコードです。ダブルクリックすると別ウィンドウが開き、ログの詳細を表示します。
なお、操作に失敗したログレコードは背景色が赤くなります。

⑮ **アカウントID**
「アカウント名」@「ドメイン名(ワークグループの場合はコンピューター名)」を表示します。

⑯ **グループID**
アカウントが属するグループ名をカンマ区切りで表示します。

⑰ **接続元**
アクセスしたコンピューターのIPアドレスとコンピューター名を表示します。

⑱ **パス**
共有フォルダ上のフルパスを表示します。

⑲ **操作日時**
操作した日時を表示します。

⑳ **操作内容**
「読み込み」「書き込み」「削除」「その他」のいずれかの操作を表示します。

㉑ **操作結果**
操作結果を「成功」または「失敗」で表示します。

## 検索対象サーバー選択ウィンドウ


## 名称と役割

① サーバーリスト
検索可能な管理対象サーバーの一覧を表示します。

②［全て選択］ボタン
サーバーリストを全て選択状態にします。

③［全ての選択を解除］ボタン
サーバーリストの選択状態を全て解除します。

④［決定］ボタン
検索対象サーバーの選択を確定します。

⑤［キャンセル］ボタン
設定値を保存せず、ウィンドウを閉じます。

## イベント詳細ウィンドウ


## 名称と役割

**① イベント詳細**

Windowsに記録された実際のログデータを表示します。
（表示されたデータを選択して値をクリップボードへコピーすることができます）

**② [閉じる] ボタン**

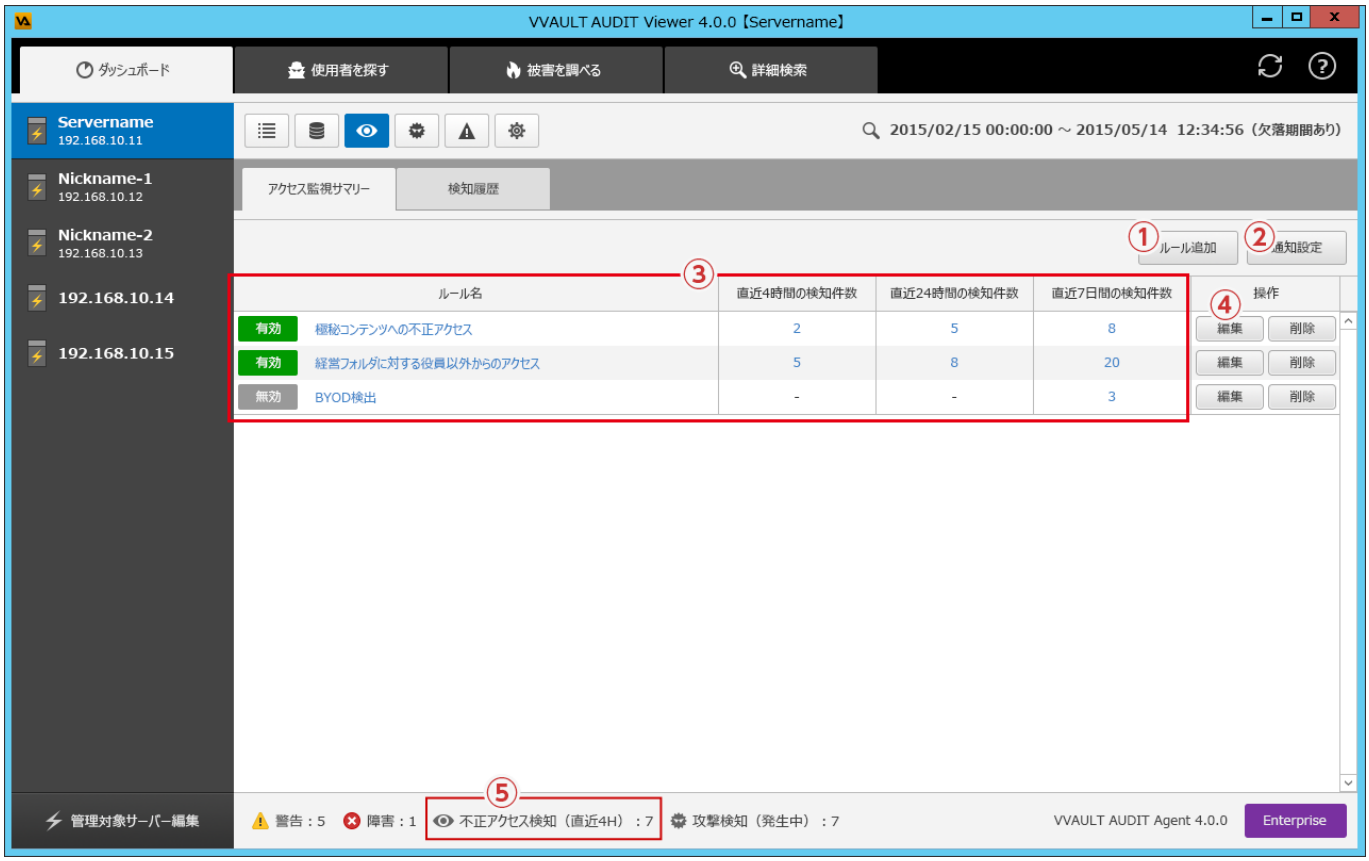
ウィンドウを閉じます。

# 3 アクセス監視

Users Manual for VVAULT AUDIT 4.5

# 3-1
# 各部の名称と役割

アクセス監視サマリー画面




## 名称と役割

① [ルール追加] ボタン
ルール追加ウィンドウを表示します。

② [通知設定] ボタン
通知設定ウィンドウを表示します。

③ アクセス監視サマリー
追加された全ルールに対して、直近４時間、直近２４時間、直近７日間の検知件数を表示します。

④ [編集] ボタン
ルール編集ウィンドウを表示します。

⑤ 検知件数
全ルールで直近４時間に検知された検知件数の合計を表示します。

## ルール追加ウィンドウ


## 名称と役割

**① 有効／無効**

ルールの有効／無効状態を設定する項目です。

**② ルール名**

ルールの名称を入力する項目です。

**③ 対象パス**

監視したいデータのパスを入力します。(パスの前方一致検索)
サーバー名は除いてください。
例）￥￥FILESEVER ￥共有￥Document でアクセス可能なパスを監視したい場合
対象パスには「￥共有￥Document」と入力してください。

**④ キーワード**

検索したデータのキーワードを入力します。

**⑤ アカウントID**

監視したい「アカウント名」を入力します。(セミコロン区切りで複数指定可能)
ドメイン名（ワークグループの場合はコンピューター名）も含めて監視する場合は「アカウント名＠ドメイン名」のようにアットマークで区切ってください。ドメイン名のみで監視する場合は「＠ドメイン名」のように先頭にアットマークを追加してください。

**⑥ グループID**

監視したい「グループ名」を入力します。(セミコロン区切りで複数指定可能)

**⑦ 接続元**

監視したい接続元のIPアドレスまたはコンピューター名を入力します。

**⑧ 操作内容**

監視したい操作内容（読み込み、書き込み、削除、その他）を選択します。

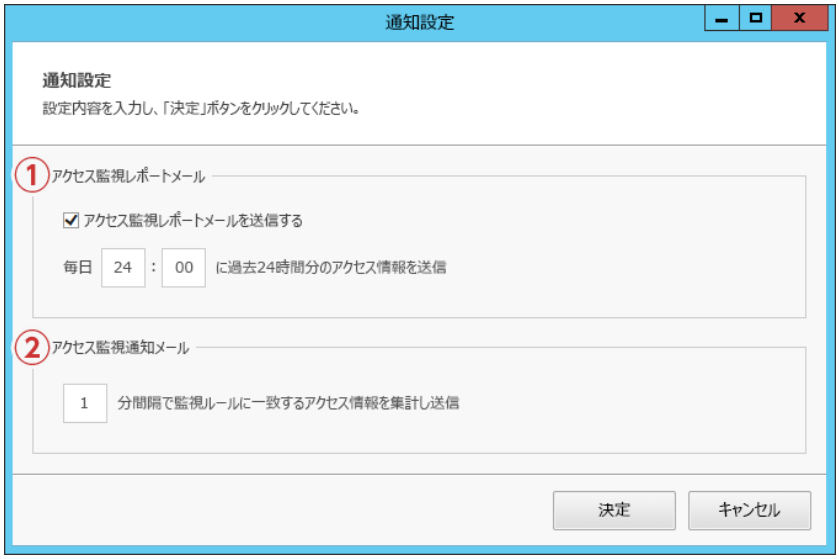
⑨ **操作結果**
監視したい操作結果（成功、失敗）を選択します。

⑩ **通知設定**
検知した場合の通知先を設定する項目です。
・イベントに記録……Windowsのイベントログに記録します。
・管理者に通知……レポートメールに設定された管理者用メールアドレスに通知メールを送信します。
・指定したメールに通知……任意のメールアドレスに通知メールを送信します。

⑪ **［決定］ボタン**
入力された設定値を保存します。

⑫ **［キャンセル］ボタン**
入力値を保存せず、ウィンドウを閉じます。

## 通知設定ウィンドウ




## 名称と役割

**① アクセス監視レポートメール**

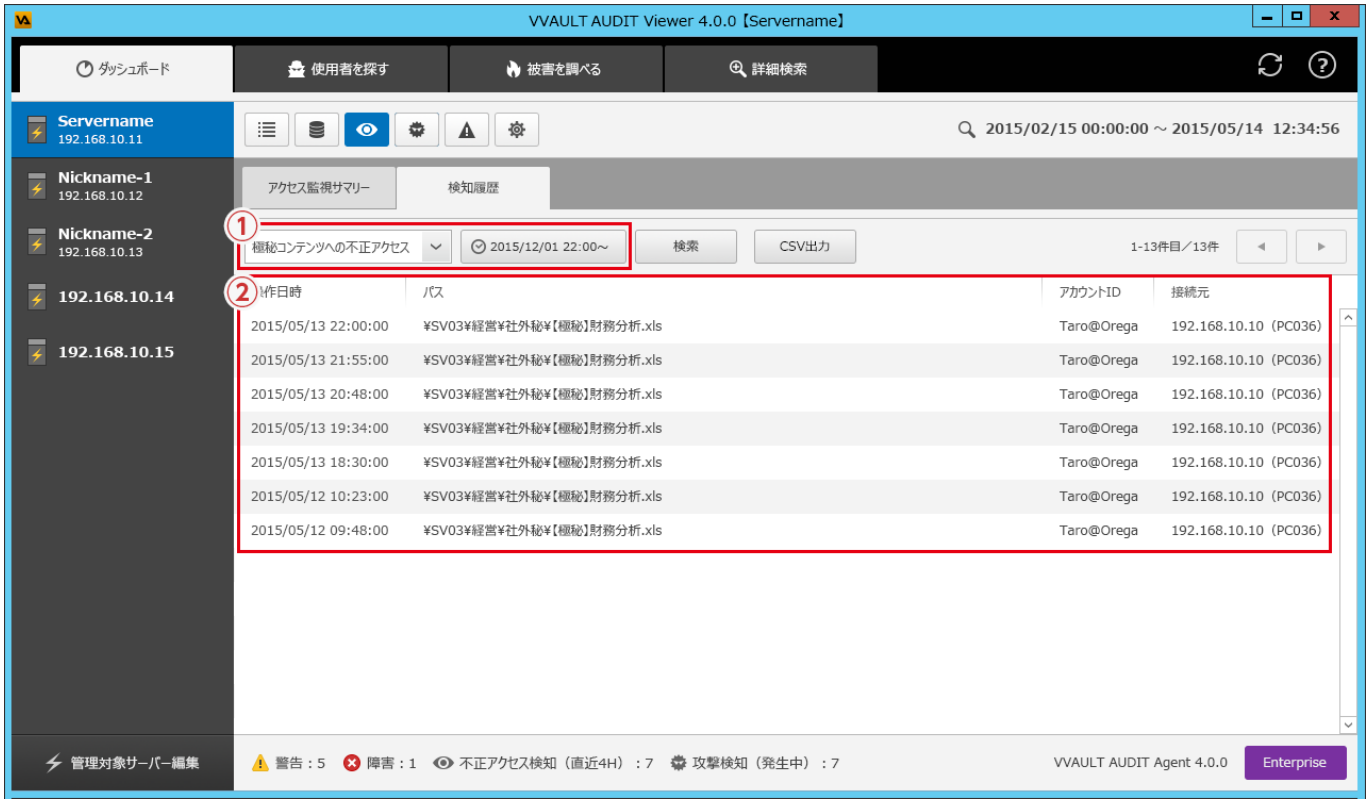
アクセス監視レポートメールを送信する場合はチェックを入れ、送信時刻を入力してください。

**② アクセス監視通知メール**

アクセス監視通知メールを送信する間隔を入力してください。

※該当するアクセスが検知されなかった場合、通知メールは送信されません。

# 検知履歴画面




## 名称と役割

### ① フィルター条件

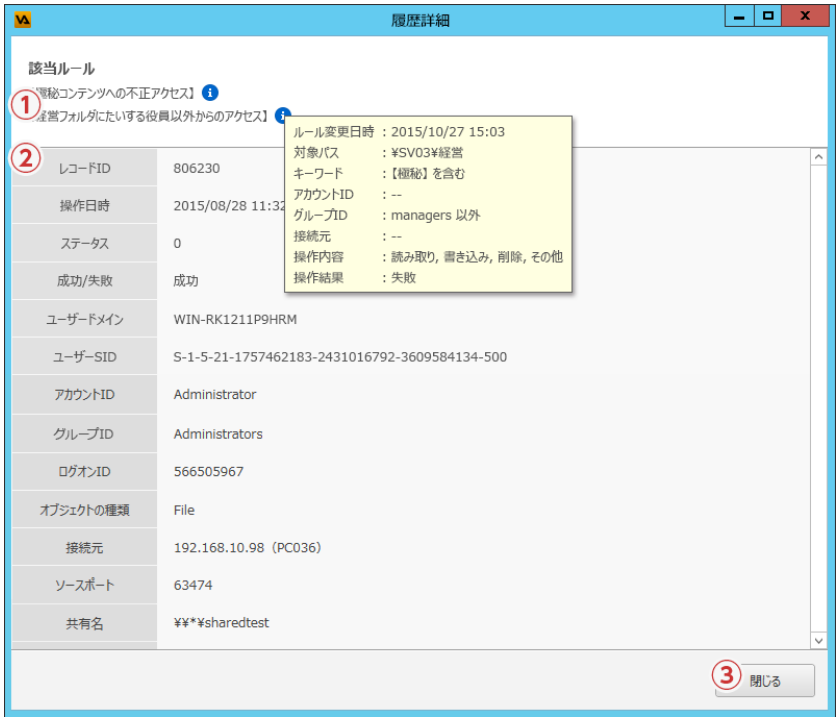
検知履歴を絞り込むための条件を入力するエリアです。

### ② 検索結果レコード

条件にヒットしたレコードを表示します。

※このデータは、「ログデータ」と「アクセス検知データ」を結合して表示します。もしどちらか欠落している場合は、データ管理画面より任意のデータを復元してアクティブデータにしてください。

# 履歴詳細ウィンドウ




## 名称と役割

① **該当ルール**
検知したルールを表示します。インフォメーションアイコンにカーソルを乗せると、検知時点のルール条件がツールチップに表示されます。

② **イベント詳細**
Windowsに記録された実際のログデータを表示します。（表示されたデータを選択して値をクリップボードへコピーすることができます）

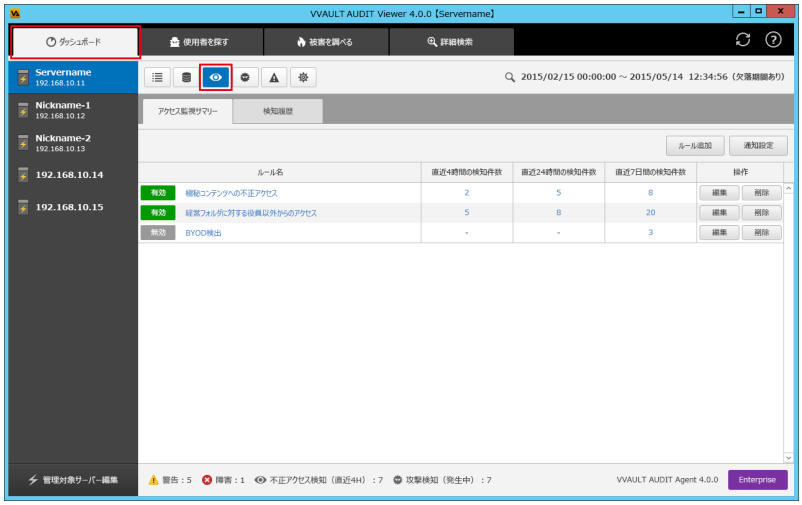
③ **[閉じる]ボタン**
ウィンドウを閉じます。

# 3-2
# 不正アクセスを監視する

ファイルサーバーにて不正なアクセスを監視する手順を説明します。

## 認証の手順

① 「ダッシュボードタブ」＞「アクセス監視」ボタンをクリックします。




**ワンポイント**

アクセス監視を利用するにはEnterpriseライセンスが必要です。

② 「ルール追加」ボタンをクリックし、監視したい条件を入力します。

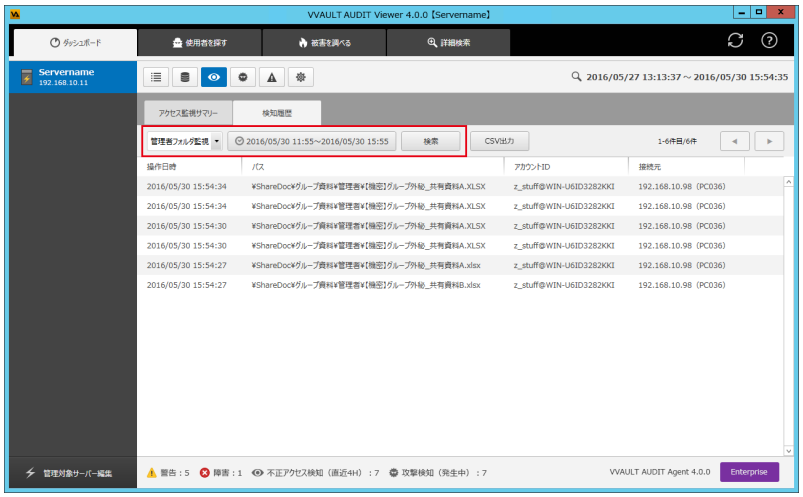

**ワンポイント**

入力値で正しくヒットするか、事前に詳細検索画面にてテストしておくことをおすすめします。

## 手順解説

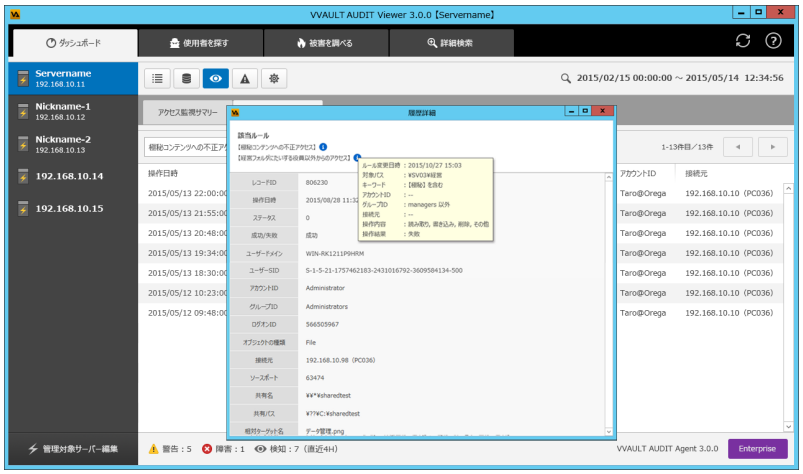
③ ルール追加後、条件にヒットするアクセスがあった場合は指定したアドレスに通知メールが送信されます。


④「検知履歴」一覧にてルールと期間を指定し、対象のログを検索します。



## 手順解説

⑤ 表示されたレコードをダブルクリックし「詳細表示」からアクセスの履歴詳細を確認します。



# 4 攻撃検知

Users Manual for VVAULT AUDIT 4.5

# 4-1
# 攻撃検知とは

一定間隔でサーバー内のファイルへのアクセスを集計・解析し、急激なアクセスの増加など攻撃的な挙動を検知した場合に予め設定されている通知先へ通知します。この「攻撃検知機能」を活用することで、ランサムウェアなどによるファイルサーバーの暗号化攻撃を早期に検知し、攻撃を実施した感染PCを特定することが可能となります。また攻撃検知後の自動ブロックを有効にすることで検知時点で攻撃元からのアクセスをブロックし、被害を最小限に抑えることができます。

## 【検知ジョブの実行間隔と通知条件】

・攻撃検知を有効にすると、5分間隔で検知ジョブが実行されます。
・検知ジョブは実行時点から遡った30分間の操作ログを、ユーザー／端末ごとに集計します。
・集計したログから異常な操作（攻撃）を検知すると、指定された通知先へ通知を行います。
※連続で～回検知したら通知する、という設定も可能です。

## 【検知条件について】

集計されたログにおいて、①～③の条件をすべて満たす操作がある場合、そのユーザー／端末から何らかの攻撃を受けているものとしてカウントを行います。
① 30分間に50,000回以上の「読み込み」操作を行った。
② 30分間に1,000回以上の「書き込み」操作を行った。
③ 30分間に1,000回以上の「 削除」操作を行った。

なお本機能はファイル作成、コピー、移動、名称変更など、大量に操作を行った際にも攻撃として検知する場合があります。
またファイルサーバーのファイル数が設定値より少ない場合は、攻撃を受けても検知できません。

## 【各種パラメーターについて】

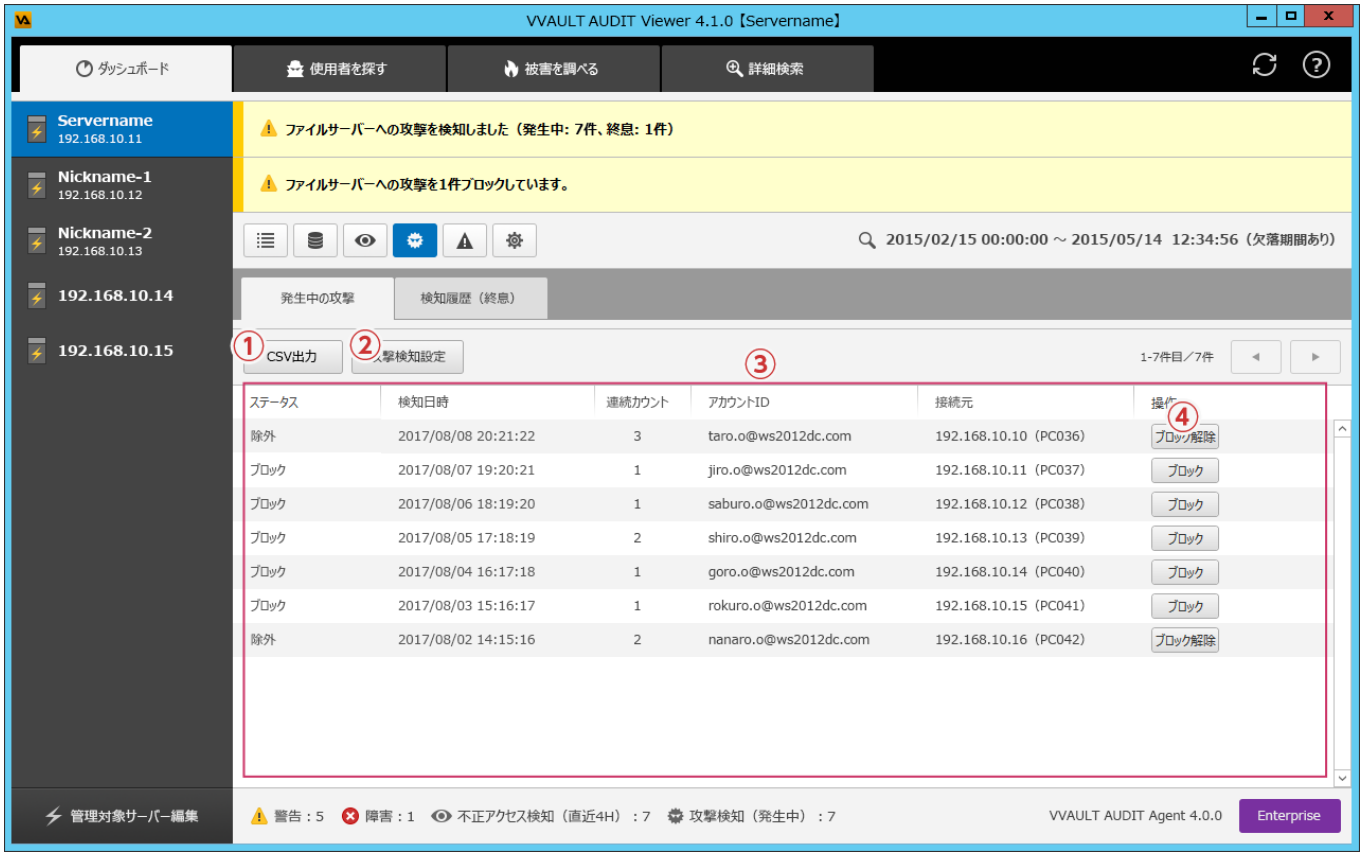
設定変更については「**インストールマニュアル**」の「**7 高度な設定**」を参照してください。

## 【攻撃のブロックについて】

Windowsファイアウォールを利用することで攻撃元からのアクセスをブロックすることができます。
Windowsファイアウォール規則に設定されるブロックの条件は「IPアドレス」です。そのため、ブロックされた端末においても「IPアドレス」が別になれば、別の端末としてアクセスが可能となります。IPv4 ／ IPv6を共用していたり、DHCPを利用されている環境など、端末の「IPアドレス」が変動するような状況ではご注意ください。
なお、自動でブロックが解除されることはありません。ブロックを解除する場合は、必ず端末からのアクセスが正常かご確認のうえ、手動で解除してください。
自動ブロックを無効、または特定端末からの攻撃を除外したい場合は、「**インストールマニュアル**」の「**7 高度な設定**」を参照してください。

# 4-2
# 各部の名称と役割

発生中の攻撃画面




## 名称と役割

**① [CSV出力] ボタン**

以下のフォーマットでCSVファイル（BOM付きUTF-8）を作成します。
”アカウントID”や”接続元”等／”ステータス”／”検知日時”／”検出範囲”／”検出件数（読み込み）”／”検出件数（書き込み）”／”検出件数（削除）”

**② [攻撃検知設定] ボタン**

攻撃検知設定ウィンドウを表示します。

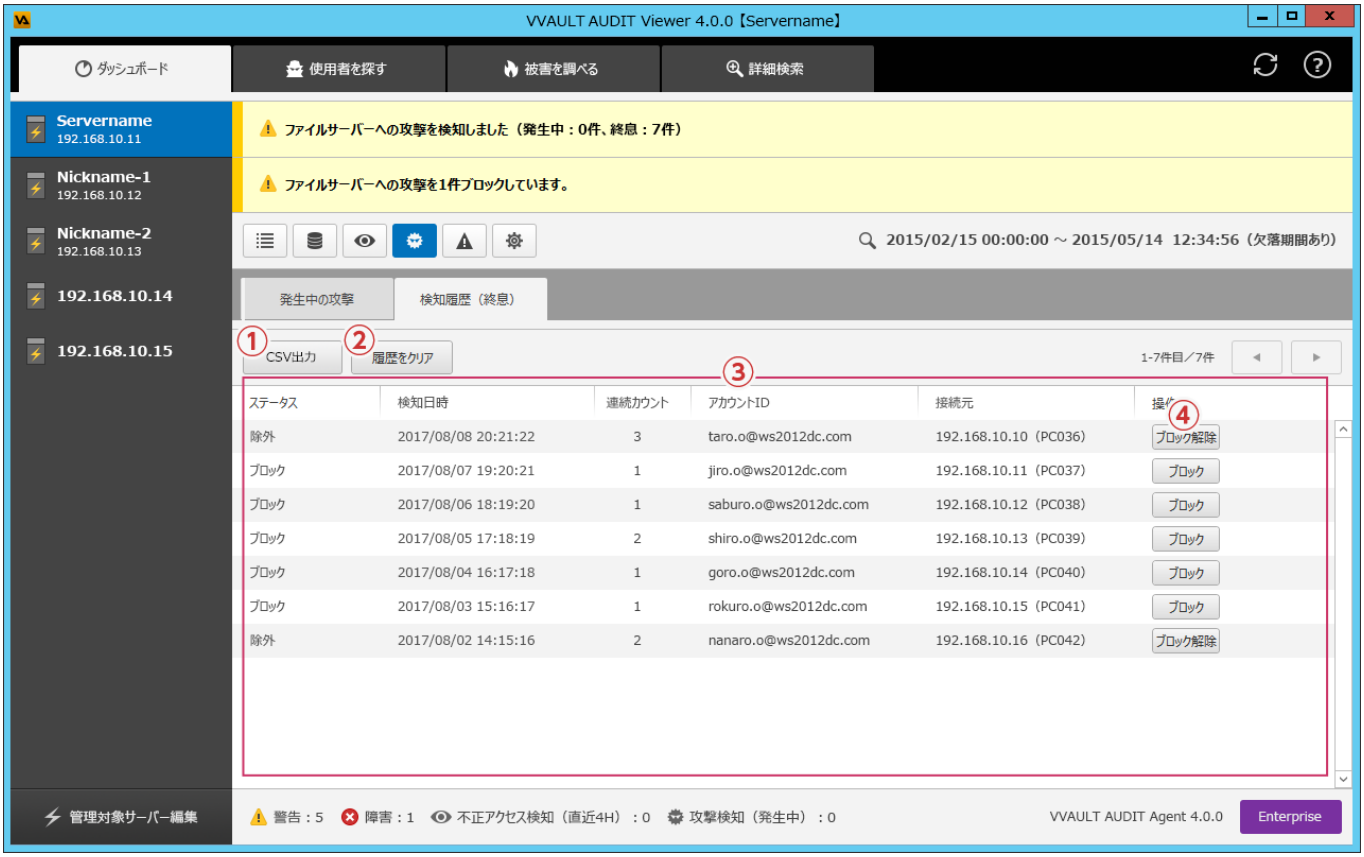
**③ 検索結果レコード**

攻撃検知したレコードを表示します。

**④ [ブロック／ブロック解除] ボタン**

ブロックをクリックすると、接続元の「IPアドレス」をWindowsファイアウォール設定に追加し、接続元からのアクセスを遮断します。ブロック解除をクリックすると、追加したファイアウォールの設定を削除します。解除する前には、必ず攻撃が終息していることを確認してください。またはこの攻撃が必要なアクセスである場合は、「**インストールマニュアル**」の「**7 高度な設定**」にて接続元のIPアドレスを「除外設定」に登録してください。

# 検知履歴（終息）画面




## 名称と役割

**① [CSV出力]ボタン**

以下のフォーマットでCSVファイル（BOM付きUTF-8）を作成します。
”アカウントID”や”接続元”等／”ステータス”／”検知日時”／”検出範囲”／”検出件数（読み込み）”／”検出件数（書き込み）”／”検出件数（削除）”

**② [履歴をクリア]ボタン**

終息した検知履歴をクリアします。

**③ 検索結果レコード**

攻撃検知したレコードを表示します。

**④ [ブロック／ブロック解除]ボタン**

ブロックをクリックすると、接続元の「IPアドレス」をWindowsファイアウォール設定に追加し、接続元からのアクセスを遮断します。ブロック解除をクリックすると、追加したファイアウォールの設定を削除します。解除する前には、必ず攻撃が終息していることを確認してください。またはこの攻撃が必要なアクセスである場合は、「**インストールマニュアル**」の「**7 高度な設定**」にて接続元のIPアドレスを「除外設定」に登録してください。

## 攻撃検知設定ウィンドウ


## 名称と役割

**① 攻撃検知機能**

攻撃検知の有効／無効状態を設定する項目です。

**② 通知先**

検知した場合の通知先を設定する項目です。

・イベントに記録……Windowsのイベントログに記録します。

・管理者に通知……レポートメールに設定された管理者用メールアドレスに通知メールを送信します。

・指定したメールに通知……任意のメールアドレスに通知メールを送信します。

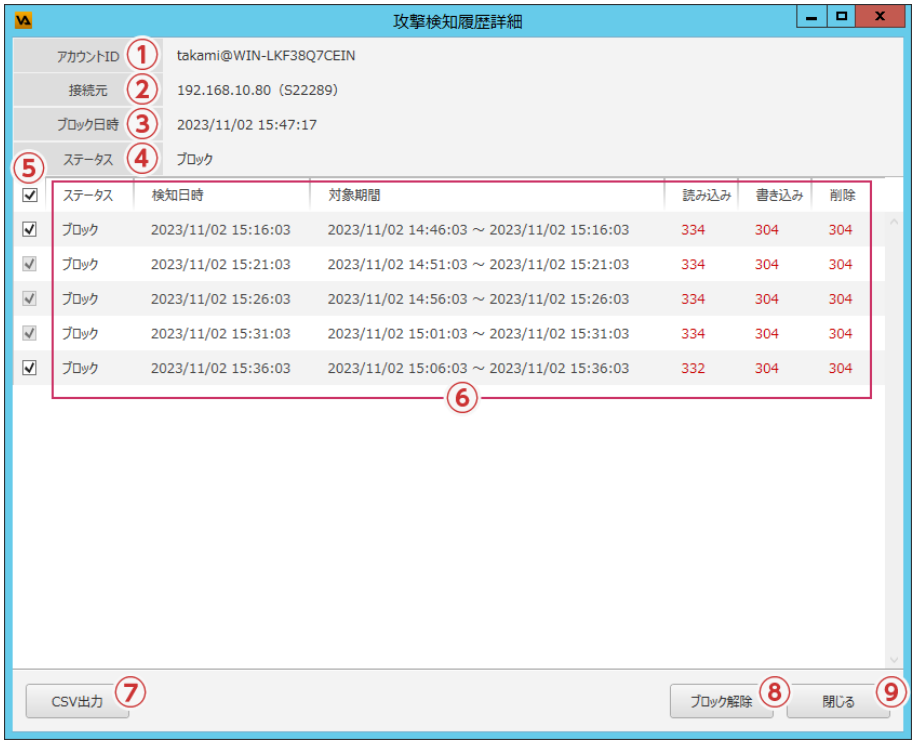
**③［決定］ボタン**

入力された設定値を保存します。

**④［キャンセル］ボタン**

入力値を保存せず、ウィンドウを閉じます。

# 攻撃検知履歴詳細ウィンドウ




## 名称と役割

**① アカウントID**
検知されたユーザーのアカウントIDを表示します。

**② 接続元**
検知されたユーザーの接続元を表示します。

**③ ブロック日時**
攻撃を検知し、接続元からのアクセスをブロック（Windowsファイアウォールに登録）した日時を表示します。

**④ ステータス**
攻撃に対してブロック状態の最新ステータスを表示します。

**⑤ チェックボックス**
CSVを出力する対象を指定します。

**⑥ 検知レコード一覧**
連続で検知された履歴の一覧を表示します。

**⑦ [CSV出力]ボタン**
チェックボックスで選択した範囲を対象とした詳細検索の結果をCSVファイルに出力します。

**⑧ [ブロック／ブロック解除]ボタン**
ブロックをクリックすると、接続元の「IPアドレス」をWindowsファイアウォール設定に追加し、接続元からのアクセスを遮断します。ブロック解除をクリックすると、追加したファイアウォールの設定を削除します。解除する前には、必ず攻撃が終息していることを確認してください。またはこの攻撃が必要なアクセスである場合は、「**インストールマニュアル**」の「**7 高度な設定**」にて接続元のIPアドレスを「除外設定」に登録してください。

**⑨ [閉じる]ボタン**
ウィンドウを閉じます。

Soliton® 株式会社ソリトンシステムズ
https://www.soliton.co.jp/

Users Manual for VVAULT AUDIT 4.5 VAUSM-231110