

記事

Mihoko Iijima · 2021年10月12日 6m read

## いつも使用しているユーザで IRIS や Caché にアクセスできなくなった時の原因の探り方 (監査の使い方)

開発者の皆さん、こんにちは。

いつも使用しているユーザでアプリケーションや InterSystems 製品 (IRIS / Caché / Ensemble / HealthShare) にアクセスしたとき、セキュリティ設定変更などの影響で急にアクセスできなくなった! という場合に、調査に便利な監査ログの参照方法をご紹介します。

ここでは、%Allロールを持つシステム管理ユーザ (system や SuperUser) で管理ポータルにアクセスできる状態での確認方法をご紹介します。

監査ログですが、まずはシステムで監査が取られる設定になっているかご確認ください (通常無効化されている場合は、調査の時だけ有効に変更してください)。

**管理ポータル > システム管理 > セキュリティ > 監査 > 監査を有効に**

ようこそ, \_SYSTEM

表示: [ ]

クリックできない状態 = 監査は有効な状態です

|                  |          |               |             |
|------------------|----------|---------------|-------------|
| ホーム              | 構成 >     | ユーザ           | 監査を有効に      |
| Health           | セキュリティ > | ロール           | 監査を無効に      |
| Analytics        | ライセンス >  | リソース          | 監査データベースの閲覧 |
| Interoperability | 暗号化 >    | サービス          | システムイベントを構成 |
| システムオペレーション      |          | アプリケーション >    | ユーザイベントを構成  |
| システムエクスプローラ      |          | SSL/TLS 構成    | 監査ログのコピー    |
| システム管理           |          | X.509証明書      | 監査ログのエクスポート |
|                  |          | OAuth 2.0 >   | 監査ログの削除     |
|                  |          | 管理ファイル転送接続    |             |
|                  |          | システム・セキュリティ > |             |
|                  |          | 監査            |             |
|                  |          | セキュリティアドバイザ   |             |
|                  |          | 携帯電話          |             |

次に、アクセスできなくなった原因を探るため、以下のシステムイベントの監査を取得できるように変更します。

## 管理ポータル > システム管理 > セキュリティ > 監査 > システムイベントを構成

以下のイベントの「状態変更」をクリックし、Enabled にはい と表示されるようにします。

- %System/%Login/LoginFailure
- %System/%Security/Protect

ようこそ, \_SYSTEM

表示: [アイコン]

ホーム

Health

Analytics

Interoperability

システムオペレーション

システムエクスプローラ

システム管理

構成

- ユーザ
- セキュリティ
- ライセンス
- 暗号化

ロール

リソース

サービス

アプリケーション

SSL/TLS 構成

X.509証明書

OAuth 2.0

管理ファイル転送接続

システム・セキュリティ

監査

セキュリティアドバイザ

携帯電話

監査を有効に

監査を無効に

監査データベースの閲覧

システムイベントを構成

ユーザーイベントを構成

### システム監査イベント

以下がシステム監査イベントの一覧

フィルタ: ページサイズ: 0

| イベント名   | 状態  | 有効 | 無効 | リセット | 状態変更 |
|---|-----|----|----|------|------|
| %Ensemble%Message/ViewContents                | はい  | 0  | 0  | リセット | 状態変更 |
| %Ensemble%Production/ModifyConfiguration      | はい  | 0  | 0  | リセット | 状態変更 |
| %Ensemble%Production/StartStop                | はい  | 0  | 0  | リセット | 状態変更 |
| %Ensemble%Schema/Modify                       | はい  | 0  | 0  | リセット | 状態変更 |
| %System%DirectMode/DirectMode                 | いいえ | 0  | 0  | リセット | 状態変更 |
| %System%Login/JobEnd                          | いいえ | 49 | 0  | リセット | 状態変更 |
| %System%Login/JobStart                        | いいえ | 57 | 0  | リセット | 状態変更 |
| %System%Login/Login                           | いいえ | 33 | 0  | リセット | 状態変更 |
| %System%Login/LoginFailure                    | はい  | 9  | 9  | リセット | 状態変更 |
| %System%Login/Logout                          | いいえ | 14 | 0  | リセット | 状態変更 |
| %System%Login/TaskEnd                         | いいえ | 21 | 0  | リセット | 状態変更 |
| %System%Login/TaskStart                       | いいえ | 0  | 0  | リセット | 状態変更 |
| %System%SQL/PrivilegeFailure                  | いいえ | 0  | 0  | リセット | 状態変更 |
| %System%SQL/XDBCStatement                     | いいえ | 0  | 0  | リセット | 状態変更 |
| %System%Security/ApplicationChange            | はい  | 0  | 0  | リセット | 状態変更 |
| %System%Security/AuditChange                  | はい  | 3  | 2  | リセット | 状態変更 |
| %System%Security/AuditReport                  | はい  | 10 | 10 | リセット | 状態変更 |
| %System%Security/DBEncChange                  | はい  | 0  | 0  | リセット | 状態変更 |
| %System%Security/DocDBChange                  | はい  | 0  | 0  | リセット | 状態変更 |
| %System%Security/DomainChange                 | はい  | 0  | 0  | リセット | 状態変更 |
| %System%Security/KMIPServerChange             | はい  | 0  | 0  | リセット | 状態変更 |
| %System%Security/LDAPConfigChange             | はい  | 0  | 0  | リセット | 状態変更 |
| %System%Security/OpenAMIdentityServicesChange | はい  | 0  | 0  | リセット | 状態変更 |
| %System%Security/PhoneProvidersChange         | はい  | 0  | 0  | リセット | 状態変更 |
| %System%Security/Protect                      | はい  | 2  | 1  | リセット | 状態変更 |
| %System%Security/ResourceChange               | はい  | 0  | 0  | リセット | 状態変更 |

状態変更 をクリックすると Enabledの列の状態が「はい」「いいえ」に変わります。  
イベントの記録を追加する場合はEnabledを「はい」に設定します。

表示省略

この状態で、アクセスできない操作をもう1度試し、試した後で「監査データベースの閲覧」ページでエラーの内容を確認します。

## 管理ポータル > システム管理 > セキュリティ > 監査データベースの閲覧

ようこそ, \_SYSTEM

表示: [ ] [ ] [ ] [ ]

ホーム

Health

Analytics

Interoperability

システムオペレーション

システムエクスプローラ

システム管理

構成

セキュリティ

ライセンス

暗号化

ユーザ

ロール

リソース

サービス

アプリケーション

SSL/TLS 構成

X.509証明書

OAuth 2.0

管理ファイル転送接続

システム・セキュリティ

監査

セキュリティアドバイザ

携帯電話

監査を有効に

監査を無効に

監査データベースの閲覧

システムイベントを構成

ユーザーイベントを構成

監査ログのコピー

監査ログのエクスポート

監査ログの削除

システム > セキュリティ管理 > 監査データベースの閲覧

## 監査データベースの閲覧

イベントソース: \* ページサイズ: 1000 結果: 1000+ ページ: 1 の 1

| 時間                      | イベントソース | イベントタイプ   | イベント        | PID   | CSPセッション   | ユーザ     | 説明                                     | 詳細 |
|-------------------------|---------|-----------|-------------|-------|------------|---------|--|----|
| 2021-10-11 11:47:00.919 | %System | %Security | AuditReport | 21428 | SEwatCb9Sb | _SYSTEM | クエリリスト                                 | 詳細 |
| 2021-10-11 11:46:15.653 | %System | %Security | AuditReport | 21428 | SEwatCb9Sb | _SYSTEM | クエリリスト                                 | 詳細 |
| 2021-10-11 11:23:15.397 | %System | %Security | AuditReport | 21428 | SEwatCb9Sb | _SYSTEM | クエリリスト                                 | 詳細 |
| 2021-10-11 11:23:09.822 | %System | %Security | AuditReport | 21428 | SEwatCb9Sb | _SYSTEM | クエリリスト                                 | 詳細 |
| 2021-10-11 11:22:59.326 | %System | %Security | AuditReport | 21428 | SEwatCb9Sb | _SYSTEM | クエリリスト                                 | 詳細 |
| 2021-10-11 11:22:47.973 | %System | %Security | Protect     | 18772 |            | test    | Attempt to access a protected resource | 詳細 |
| 2021-10-11 11:22:35.166 | %System | %Security | UserChange  | 21428 | SEwatCb9Sb | _SYSTEM | ユーザ test を変更                           | 詳細 |

以下例では、ターミナルにログインした時の監査ログの記録をご紹介します。

ログインに使用するユーザ名は test、パスワード test、ロールに %Operator が設定されていて、管理ポータル [システムオペレーション] メニューが利用できるユーザとします。



### 1) パスワードが異なるとき

ターミナルにアクセスしたときの表示は以下の通りです。

```
?????:test  
?????:****  
???????????????
```

監査データベースの閲覧画面を再表示した時の一覧には、「プログラマモード ログイン失敗」と表示されています。

|                         |         |        |              |       |      |                 |
|-------------------------|---------|--------|--------------|-------|------|-----------------|
| 2021-10-11 11:48:36.248 | %System | %Login | LoginFailure | 15336 | test | プログラマモード ログイン失敗 |
|-------------------------|---------|--------|--------------|-------|------|-----------------|

詳細を確認するため、「詳細」のリンクをクリックします。

システム > セキュリティ管理 > 監査データベースの閲覧

## 監査データベースの閲覧

ページサイズ: 1000 結果: 1000+ ページ: 1 の 1

| 時間                      | イベントソース | イベントタイプ   | イベント         | PID   | CSPセッション   | ユーザ     | 説明              |                    |
|-------------------------|---------|-----------|--------------|-------|------------|---------|-----------------|--------------------|
| 2021-10-11 11:48:57.432 | %System | %Security | AuditReport  | 21428 | SEwatCb9Sb | _SYSTEM | クエリリスト          | <a href="#">詳細</a> |
| 2021-10-11 11:48:36.248 | %System | %Login    | LoginFailure | 15336 |            | test    | プログラマモード ログイン失敗 | <a href="#">詳細</a> |
| 2021-10-11 11:47:00.919 | %System | %Security | AuditReport  | 2     |            |         |                 | <a href="#">詳細</a> |

監査詳細:

|            |  |
|------------|--|
| 説明         | プログラマモード ログイン失敗  |
| タイムスタンプ    | 2021-10-11 11:48:36.248  |
| UTCタイムスタンプ | 2021-10-11 02:48:36.248  |
| イベントソース    | %System  |
| イベントタイプ    | %Login   |
| イベント       | LoginFailure   |
| ユーザ名       | test   |
| Pid        | 15336  |
| JobId      | 327707   |
| ジョブ番号      | 27   |
| IPアドレス     | 127.0.0.1  |
| 実行形式       |  |
| システムID     | ijima-letsn2:IRISHEALTH3   |
| インデックス     | 6790   |
| ロール        |  |
| 認証         | パスワード  |
| ネームスペース    | %SYS   |
| ルーチン       |  |
| ユーザ情報      |  |
| O/S ユーザ名   | ijima  |
| ステータス      |  |
| イベントデータ    | エラーメッセージ: エラー #798: パスワード 認証が失敗しました<br>エラー #952: パスワードが不正です<br>サービス名: %Service_Console<br>ログインルーチン: プログラマモード<br>\$!:  TRM :15336<br>\$P:  TRM :15336 |

「イベントデータ」の行にエラーメッセージが記録されています。

```
?????????: ??? #798: ?????? ??????????
???? #952: ????????????
```

### 2) ユーザが存在しない時

存在しないユーザ (abc) でログインした場合は、以下のエラーが記録されます (この時も「プログラマモード ログイン失敗」と一覧に表示されます)。

|                         |         |        |              |       |     |                 |
|-------------------------|---------|--------|--------------|-------|-----|-----------------|
| 2021-10-11 11:55:16.644 | %System | %Login | LoginFailure | 19192 | abc | プログラマモード ログイン失敗 |
|-------------------------|---------|--------|--------------|-------|-----|-----------------|

詳細のリンクから「イベントデータ」を確認すると、以下のエラーメッセージが記録されています。

```
?????????: ??? #798: ?????? ??????????
???? #838: ??? abc ??????????
```

### 3) ユーザ名とパスワードはあっているのにターミナルにアクセスできない時 (アクセス拒否 と出るとき)

ユーザ名、パスワードの指定はあっていそうなのに、ターミナルにアクセスできないエラーが出ているときの状態です。

以下のエラーが記録されます (この時も「プログラマモード ログイン失敗」と一覧に表示されます)。

|                         |         |        |              |       |      |                 |
|-------------------------|---------|--------|--------------|-------|------|-----------------|
| 2021-10-11 11:57:48.305 | %System | %Login | LoginFailure | 21048 | test | プログラマモード ログイン失敗 |
|-------------------------|---------|--------|--------------|-------|------|-----------------|

詳細を確認します。

今回は、「エラーメッセージ: エラー #836: プログラマーアクセスの権限が不十分です」を出ています。

|         |   |
|---------|---|
| イベントデータ | エラーメッセージ: エラー #836: プログラマーアクセスの権限が不十分です<br>サービス名: %Service_Console<br>ログインルーチン: プログラマモード<br>\$:  TRM : 21048<br>\$P:  TRM : 21048 |
|---------|---|

テストに使用しているユーザは %Operator ロールを持ちますが、ターミナルのアクセスに必要な %Developer ロールを持っていません。そのため、アクセス権限不十分とエラーが出ています。

この他、**使用しているユーザが「無効」**になっている場合もアクセス拒否となり「プログラマーモード ログイン失敗」と表示され、詳細には以下のエラーメッセージが表示されます。

|         |  |
|---------|--|
| イベントデータ | エラーメッセージ: エラー #798: パスワード 認証が失敗しました<br>エラー #828: ユーザ test アカウントが無効です<br>サービス名: %Service_Console<br>ログインルーチン: プログラマモード<br>\$:  TRM : 19588<br>\$P:  TRM : 19588 |
|---------|--|

#### 4) ターミナルにアクセスできるけど、特定のネームスペースにアクセスできない状態

ユーザ test の役割が変わり、開発者としてターミナルにアクセスできるユーザに変更する必要があるとします。

ここで、管理者がユーザ test から %Operator ロールを削除し、%Developer ロールを付与したとします。

**管理ポータル > システム管理 > セキュリティ > ユーザ > test を選択 > ロール > %Developer 付与**

システム > セキュリティ管理 > ユーザ > ユーザ編集 - (セキュリティの設定)

## ユーザ編集

保存

プロフィール

キャンセル

### ユーザ test の定義編集:

General

Roles

SQL Privileges

SQL Tables

ユーザ test には以下のロールが割り当てられています:

| ロールの名前     | 付与特権オプション                |    |
|------------|--------------------------|----|
| %Developer | <input type="checkbox"/> | 削除 |

```
????:test  
?????:****
```

USER>

やっとターミナルにアクセスできました！

管理ポータルの [システムオペレーション] メニューの操作をルーチンで試そうと %SYS  
ネームスペースに移動します。

```
USER>set $namespace="%SYS"  
  
SET $NAMESPACE="%SYS"  
^  
<PROTECT> *c:\intersystems\irishealth3\mgr\  
USER>
```

残念・・・。エラーです。

エラーの原因を監査ログを参照して確認します。

|                         |         |           |         |      |      |  |
|-------------------------|---------|-----------|---------|------|------|--|
| 2021-10-11 12:17:02.329 | %System | %Security | Protect | 9684 | test | Attempt to access a protected resource |
|-------------------------|---------|-----------|---------|------|------|--|

Protect のイベントが記録され「Attempt to access a protected resource」と表示されています。

詳細を確認します。



この記録は、mgr以下にある IRIS.dat (= IRISYSデータベース) に対する <PROTECT>  
エラーが発生したことを意味します。

これは、ユーザ test から %Operator ロールを削除することで、IRISYS データベースに対する READ と WRITE  
の許可がなくなったことが原因です。

%Developer ロールだけでは、アクセスしたいデータベースに対する許可が不足するため、追加でユーザ test  
に適切なデータベースの許可を付与する必要があります。

例のように、%SYS ネームスペースにアクセスしたい場合は、IRISYSのデータベースロール (%DBIRISYS)  
を付与することでデータベースに対してREAD / WRITE の許可が追加できます。

システム > セキュリティ管理 > ユーザ > ユーザ編集 - (セキュリティの設定)

## ユーザ編集

保存

プロフィール

キャンセル

### ユーザ test の定義編集:

General

Roles

SQL Privileges

SQL Tables

ユーザ test には以下のロールが割り当てられています:

| ロールの名前                     | 付与特権オプション                |                    |
|----------------------------|--------------------------|--------------------|
| <a href="#">%DB_IRISYS</a> | <input type="checkbox"/> | <a href="#">削除</a> |
| <a href="#">%Developer</a> | <input type="checkbox"/> | <a href="#">削除</a> |

再度、ターミナルにユーザ test でログインし直してから %SYS  
ネームスペースに移動し、試しにユーティリティを実行してみます。

```
?????:test  
?????:****  
USER>set $namespace="%SYS"
```

```
%SYS>do ^TASKMGR
```

- 1) ??????
- 2) ??????
- 3) ??????
- 4) ??????
- 5) ????????
- 6) ??????
- 7) ??????
- 8) ????????
- 9) ????????????????
- 10) ??

```
???????
```

うまく行きました。

いかがでしたでしょうか。

今まで使用していたユーザで急にアクセスできない！という状況になった時、セキュリティ設定に変更がなかったかどうかご確認ください。

もし変更した後アクセスできなくなった場合は、この記事で試したように、監査を使用してどんなエラーが発生しているか確認することができます。

監査についての[ドキュメント](#)もあります。ぜひご参照ください。

最後に、  
普段監査を使用されて  
いない環境は、  
**調査が終わったら「無効化」することをお忘れなく！**

[#システム管理](#) [#セキュリティ](#) [#ヒントとコツ](#) [#Caché](#) [#Ensemble](#) [#HealthShare](#) [#InterSystems IRIS](#)  
[#InterSystems IRIS for Health](#)

---

ソースURL:

<https://jp.community.intersystems.com/post/%E3%81%84%E3%81%A4%E3%82%82%E4%BD%BF%E7%94%A8%E3%81%97%E3%81%A6%E3%81%84%E3%82%8B%E3%83%A6%E3%83%BC%E3%82%B6%E3%81%A7-iris-%E3%82%84-cach%C3%A9-%E3%81%AB%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E3%81%A7%E3%81%8D%E3%81%AA%E3%81%8F%E3%81%AA%E3%81%A3%E3%81%9F%E6%99%82%E3%81%AE%E5%8E%9F%E5%9B%A0%E3%81%AE%E6%8E%A2%E3%82%8A%E6%96%B9%EF%BC%88%E7%9B%A3%E6%9F%BB%E3%81%AE%E4%BD%BF%E3%81%84%E6%96%B9%EF%BC%89>

---

