

監査ログについて

株式会社ドリーム・アーツ



「SmartDB監査ログ」と「管理画面監査ログ」の2種類あります

SmartDB監査ログ

ログ保存期間: 5年間

主に**ユーザー操作**に関するログを出力

- バインダ操作
- プロセスエンジン操作
- REST API

など

管理画面監査ログ

ログ保存期間: 5年間

主に**管理画面**に関するログを出力

- 管理画面上の操作
- ユーザーによるユーザー・グループ情報の更新
- アカウントマスタ連携

など

システム管理 > ダッシュボード > 監査ログ からダウンロード

出力するログ種別と対象年月を選択し、ダウンロードを行ってください。

日毎のログが1ヶ月分まとめてダウンロードされます。

The screenshot displays the 'SmartDB 監査ログ' (SmartDB Monitoring Log) page. On the left, a user profile for '岡野 かわり' (Okano Kawaii) is visible, with a navigation menu where 'システム管理' (System Management) is highlighted. The main content area is titled '監査ログのダウンロード' (Download Monitoring Log). It contains the following elements:

- A header section with the title '監査ログのダウンロード'.
- A descriptive paragraph: '監査ログでは、前日までにいつ、だれが、なにを操作したのかが記録されています。対象となる ログ種別 と 対象年月 を指定して、ダウンロードすることが可能です。' (In the monitoring log, it is recorded when, by whom, and what was operated up to the previous day. You can specify the target log type and target year/month to download.)
- A 'ログ種別' (Log Type) section with two radio buttons: 'SmartDB監査ログ' (selected) and '管理画面監査ログ' (Management Screen Monitoring Log).
- An '対象年月' (Target Year/Month) section with dropdown menus for '年' (Year) set to '2022' and '月' (Month) set to '8'. A blue arrow points to the month dropdown.
- A prominent blue 'ダウンロード' (Download) button at the bottom.

ユーザ操作についていつ、どこから、誰が、何を行ったか 確認可能

ユーザーの操作(バイнда操作・プロセス操作・REST API)に関するログを、以下の項目を使って記録しています

ID	説明
when	操作した日時
where	リモートマシンのIPアドレス
who	操作したユーザのMID ※トークン利用時はトークンID
operation	操作の分類
objective	操作の対象 (binder-idなど ※operationにより変わります)
view	操作対象画面 (view-idなど ※operationにより変わります)
target	操作の付随対象 (record-id, filter-idなど ※operationにより変わります)
revision	変更内容を特定するための番号
result	操作結果
exception	例外発生時のメッセージ

※詳細は「[システム管理ガイド](#)」に掲載しています

ログは「システム管理ガイド」とつぎ合わせて確認することで、内容を把握することができます

文書削除ログ

ユーザ(MID)

when:2023-04-21 14:30:29 where:153.246.11.138 who:[100020] operation:docDelete
objective:15112 target:285 view:- revision:- result:OK exception:-

バインダID

文書ID

システム管理ガイド

バインダの操作別ログフィールドの値

操作	operation	objective	target	view
文書更新	docUpdate	binder-id	record-id	-
文書削除	docDelete	binder-id	record-id	-
文書閲覧	docView	binder-id	record-id	バージョン番号

※「operation」によって「objective」「target」「view」の意味が変わります

ダウンロードしたcsvは文字が続くため、Excelに取り込むことで見やすくなります

① Excelを新規に開き
[データ]→[テキストまたはCSVから]
を選択し、履歴データを読み取る

② エクスプローラから
[すべてのファイル(*.*)]を選択
[インポート]で取り込む

③ 元のファイル[65001:Unicode(UTF-8)]を選択
区切り記号[コロン]を選択し読み込みを行う

名前	更新日時	種類	サイズ
audit.log	2021/06/10 15:04	テキストドキュメント	2 KB
audit.log.20210601	2021/06/01 14:59	20210601 ファイル	900 KB
audit.log.20210602	2021/06/02 14:59	20210602 ファイル	1,044 KB
audit.log.20210603	2021/06/03 14:59	20210603 ファイル	1,166 KB
audit.log.20210604	2021/06/04 14:56	20210604 ファイル	974 KB
audit.log.20210605	2021/06/05 14:56	20210605 ファイル	112 KB
audit.log.20210606	2021/06/06 14:57	20210606 ファイル	343 KB
audit.log.20210607	2021/06/07 14:56	20210607	
audit.log.20210608	2021/06/08 14:57	20210608	
audit.log.20210609	2021/06/09 14:59	20210609	
audit.log.20210610	2021/06/10 14:57	20210610	

Column1	Column2	Column3	Column4	Column5	Column6	Column7
when	2021-06-01 00	0	32 where	- who	- operation	restApiSynchronizeAccountCache obj
when	2021-06-01 00	5	32 where	- who	- operation	restApiSynchronizeAccountCache obj
when	2021-06-01 00	10	32 where	- who	- operation	restApiSynchronizeAccountCache obj
when	2021-06-01 00	15	32 where	- who	- operation	restApiSynchronizeAccountCache obj
when	2021-06-01 00	20	32 where	- who	- operation	restApiSynchronizeAccountCache obj
when	2021-06-01 00	24	39 where	192.168.0.20 who	素磨smith知総呂[1000208] operation	restApiGetSession objective
when	2021-06-01 00	24	39 where	192.168.0.20 who	素磨smith知総呂[1000208] operation	restApiGetSession objective
when	2021-06-01 00	31	31 where	192.168.0.20 who	SmartDB管理者[1000011] operation	restApiGetTimestampMonthlyCount
when	2021-06-01 00	35	32 where	- who	- operation	restApiSynchronizeAccountCache obj

主に管理画面・ユーザ情報等についていつ、どこから、誰が、何を行ったか 確認可能

管理画面の操作やユーザー・グループ情報の呼び出し・更新等に関するログを、以下の項目を使って記録しています

ID	説明
who	アクセスユーザーのMID
where	アクセス元クライアントIP
when	ログ出力時間(JST)
operation	オペレーションの種類
resource	リソースの種類
success	false: HTTPステータスが400以上, true: 左記以外
request	リクエスト情報(詳細は右記を参照)
objective	操作の付随対象 (ユーザーのMID, 認証プロバイダーなど ※operationにより変わります)
target	オブジェクトの付随情報

request内の情報

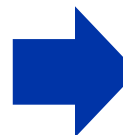
request内ID	説明
user.mid	アクセスユーザーのMID
path	リクエストパス
method	リクエストメソッド
params	リクエストURLパラメータ
query	リクエスト引数
body	リクエスト本文
response	レスポンス情報
statusCode	レスポンスステータスコード
message	レスポンスメッセージ
errCode	エラーコード

※詳細は「[システム管理ガイド](#)」に掲載しています

1行ごとにJSON形式でログ内容が出力されています。

整形することで内容を確認しやすくなります。

	A	B	C	D	E	F	G	H	I
1	{"level":"info","message":{"operation":"companyInfo","request":{"body":{"method":"GET","params":{"path":"/api/a								
2	{"level":"info","message":{"operation":"retrieveLastModify","request":{"body":{"method":"GET","params":{"path":"/								
3	{"level":"info","message":{"operation":"retrieveModifiedImageUsers","request":{"body":{"method":"GET","params":{"								
4	{"level":"info","message":{"operation":"hourly","request":{"body":{"method":"GET","params":{"path":"/api/system/								
5	{"level":"info","message":{"operation":"companyInfo","request":{"body":{"method":"GET","params":{"path":"/api/a								
6	{"level":"info","message":{"operation":"retrieveLastModify","request":{"body":{"method":"GET","params":{"path":"/								
7	{"level":"info","message":{"operation":"retrieveModifiedImageUsers","request":{"body":{"method":"GET","params":{"								
8	{"level":"info","message":{"operation":"companyInfo","request":{"body":{"method":"GET","params":{"path":"/api/a								
9	{"level":"info","message":{"operation":"hourlySync","request":{"body":{"method":"GET","params":{"path":"/api/sys								
10	{"level":"info","message":{"operation":"companyInfo","request":{"body":{"method":"GET","params":{"path":"/api/a								
11	{"level":"info","message":{"operation":"retrieveLastModify","request":{"body":{"method":"GET","params":{"path":"/								
12	{"level":"info","message":{"operation":"retrieveModifiedImageUsers","request":{"body":{"method":"GET","params":{"								
13	{"level":"info","message":{"operation":"companyInfo","request":{"body":{"method":"GET","params":{"path":"/api/a								
14	{"level":"info","message":{"operation":"companyInfo","request":{"body":{"method":"GET","params":{"path":"/api/a								



整形

```

{
  "message":{
    "who":1000000,
    "where":"::ffff:192.168.0.9",
    "when":"2020-08-01 19:08:49",
    "operation":"companyInfo",
    "resource":"company",
    "success":true,
    "request":{
      "user":{
        "mid":1000000
      },
      "path":"/api/admin/company",
      "method":"GET",
      "params":{},
      "query":{},
      "body":{}
    },
    "response":{
      "statusCode":200,
      "message":"OK",
      "errCode":""
    }
  },
  "level":"info",
  "timestamp":"2020-08-01T10:31:49.277Z"
}
    
```

ログは「システム管理ガイド」とつぎ合わせて確認することで、内容を把握することができます

ユーザ削除ログ

```
{
  "message": {
    "objective": "1000466",
    "operation": "userDelete",
    "request": { "params": { "id": "1000466" }, "user": { "mid": 1000288, (中略) }, (中略) },
    "resource": "user",
    "response": { "statusCode": 204, (中略) },
    "success": true,
    "when": "2023-04-03 16:48:10",
    "where": "35.76.130.98:63642, 35.76.130.98",
    "who": 1000288
  },
  "level": "info",
  "timestamp": "2023-04-03T07:48:10.787Z"
}
```

削除されたユーザ(MID)

削除したユーザ(MID)

システム管理ガイド

操作	operation	objective	target
ユーザ情報更新	userUpdate	ユーザのMID	
ユーザ削除	userDelete	ユーザのMID	
ユーザ個人情報/業務情報取得	userExtensionGet	ユーザのMID	

※「operation」によって「objective」「target」の意味が変わります

個人情報保護の観点から監査ログにはMIDでのみ記録されます。

個人を特定するためにはMIDからユーザー情報を割り出す必要があります

アカウントマスタ連携 > 付加情報連携 > CSV出力から
ユーザ付加情報(user_ext_ids.csv)をダウンロード

ダウンロードしたcsvにある「mid(read only)」の列から、該当のMIDを
探すと、ユーザー情報を割り出すことができます

user_ext_ids.csv

	A	B	C	D	E	F	G	H
1	namespace	id	new_namespace	new_id	mid(read only)	login_id(read only)	name(read only)	primary_gname(read only)
2	smartdb	1000012			1000012	@dreamarts.co.jp	業師丸 直輝	SmartDB運用グループ
3	smartdb	1000013			1000013	@dreamarts.co.jp		マーケティンググループ
4	smartdb	1000014			1000014	@dreamarts.co.jp		株式会社DAdemo
5	smartdb	1000015			1000015	@dreamarts.co.jp		AEグループ2
6	smartdb	1000016			1000016	@dreamarts.co.jp		エンゲージメントリード
7	smartdb	1000018			1000018	@dreamarts.co.jp		D関連会社
8	smartdb	1000020			1000020	@dreamarts.co.jp		エンゲージメントリード
9	smartdb	1000021			1000021	@dreamarts.co.jp		CTサービス1グループ
10	smartdb	1000023			1000023	@dreamarts.co.jp		事業基盤開発本部

DreamArts

<https://www.dreamarts.co.jp/>

