

LIVENESS AccessView

VERSION 3.0

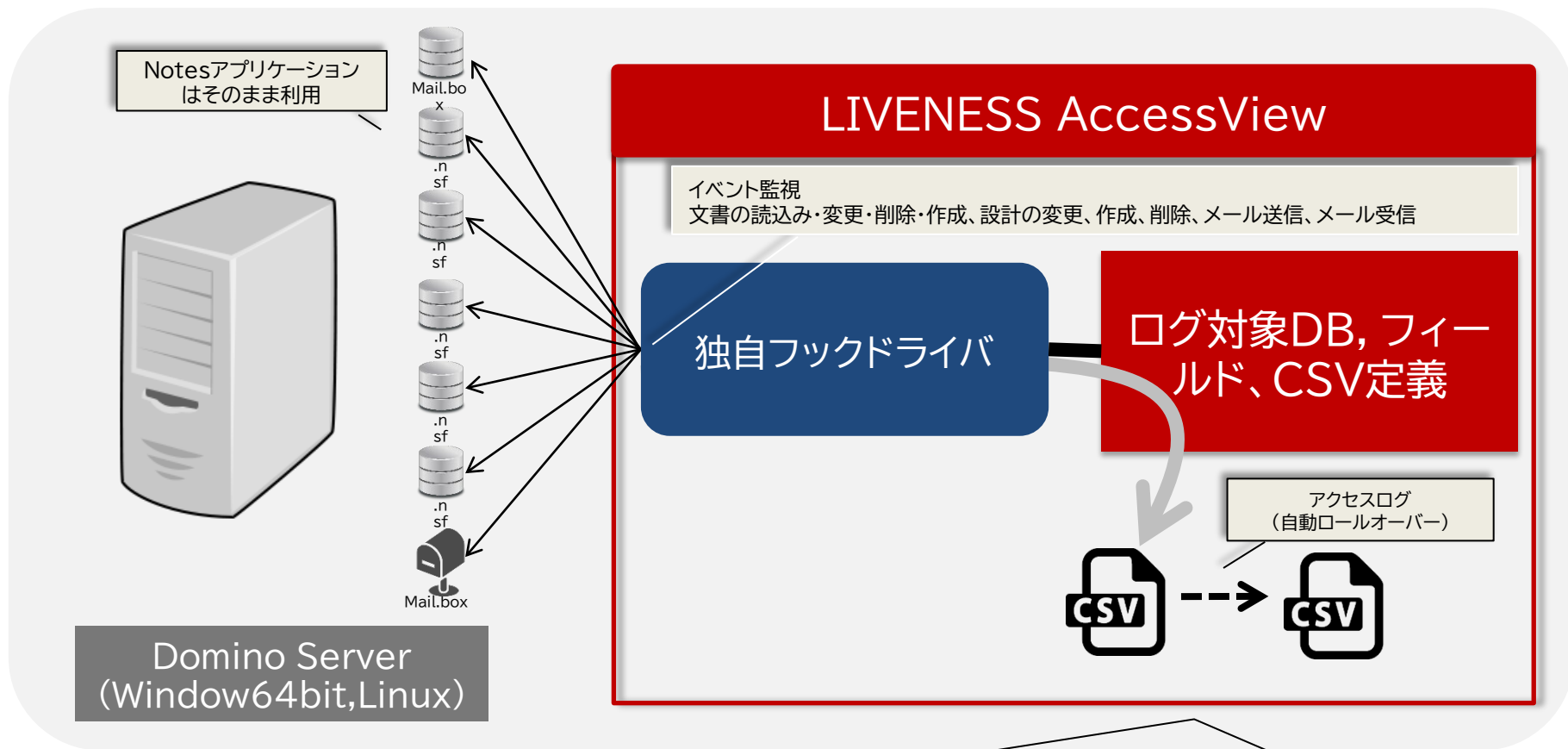
Notesアクセスログを文書単位で取得する。

LIVENESS AccessView とは

Notesログでは物足りない、Domlogではわかりづらい。サードパーティ製のアクセスログ取得ツールは高機能すぎて使いづらい、営業サポート終了している。などNotesアクセスログの管理に困っていませんか？監査や情報漏洩の抑止効果の観点からもアクセスログ取得は重要です。そんなノートユーザー様にお答えして、「LIVENESS AccessView」が誕生しました。

「LIVENESS AccessView」は指定したDBを文書単位でアクセスログをテキスト形式にて出力します。

LIVENESS AccessView機能概要

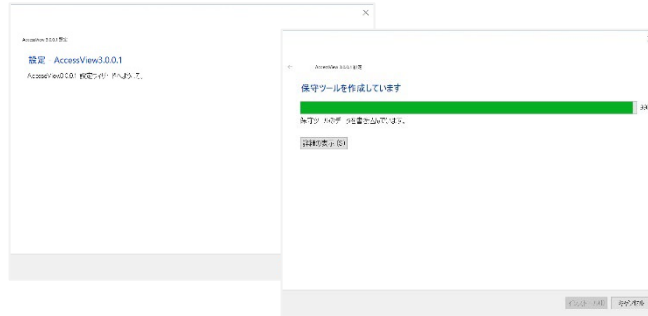


Server	Database	Database	Data/Tim	Username	Note ID	Universal	Level	Form	Field_1	Field_2	Field_3	Field_4	Field_5	Field_6	Field_7	Field_8	Field_9	Field_10	Attachments
winered/l	demo	old B部門	掲示	57:36.2	CN=admini	926	F6D61F1E	Open	document	当社製品が日経新聞に掲載されました。									ポータルご提案資料_20171017.pptx;PORTAL_top.pptx;ポータル利用イメージ.pptx
winered/l	demo	old B部門	掲示	57:37.5	CN=admini	0000092e	241BEFD	Open	document	News速報！！									FAX_20181012_1539329115_502.pdf
winered/l	demo	old B部門	掲示	57:37.9	CN=admini	932	4D692932	Open	document	2015/5 新製品情報									
winered/l	demo	old B部門	掲示	57:38.1	CN=admini	936	F398FB22	Open	document	人事部からのお知らせ									
winered/l	demo	old B部門	掲示	57:38.4	CN=admini	0000091a	18C1FBD	Open	document	新製品が発表されました！									
winered/l	demo	old B部門	掲示	57:38.6	CN=admini	0000091e	38D42B04	Open	document	売上高 営業利益 経常利益 四半期純利益？ 物流ニュースリリース (プレスリリース)									
winered/l	demo	old B部門	掲示	57:38.8	CN=admini	0000092a	C40A34E	Open	document	111迷走するカンジノ解禁、誤解流布で混乱する議論～反対派活発化で展開緊迫、公営でもリスク大									

導入設定は簡単！

Step1

Dominoサーバーにフックドライバーをインストール



Step2

DominoサーバーのNotes.iniに項目を追加(ログ取得プロセス指定)

```
EXTMGR_ADDINS=C:¥PROGRAM~1¥liveness¥ACCESS~1¥avhdrv
LIVENESS_AccessView3_LogSettings=ls_accessview.nsf
LIVENESS_AccessView3_EventKeys_nserver=2
LIVENESS_AccessView3_EventKeys_nhttp=2
LIVENESS_AccessView3_EventKeys_nrouter=1
```

Step3

ログ取得対象アプリケーションの定義



AccessViewアプリケーション設定

アプリケーション設定		更新日 : 2022/07/07 15:25
注意 : アプリケーション設定を反映するには、Dominoサーバーの再起動が必要です。		
サーバーOS	<input checked="" type="radio"/> Windows <input type="radio"/> Linux	
フックドライバー除外DB	<input type="text" value="log.nsf, domlog.nsf, names.nsf, admin4.nsf, catalog.nsf, schema.nsf, reports.nsf, events4.nsf, statrep.nsf, ddm.nsf"/>	デフォルト
フックドライバー除外ユーザー	<input type="text" value=""/>	
既読フラグを付ける時のみ文書オープンログ対象にする	<input type="checkbox"/> オン	
CSVログ		
保存フォルダ	<input type="text" value="d:¥AccessView"/>	Dataフォルダ
ファイル名	<input type="text" value="AccessViewLog-¥{process}-¥{type}.csv"/>	デフォルト
ファイルパス	d:¥AccessView¥AccessViewLog-¥{process}-¥{type}.csv	
ローテーション方法	<input type="radio"/> サイズ <input checked="" type="radio"/> デイリー	
ローテーションファイル名	<input type="text" value="d:¥AccessView¥AccessViewLog-¥{process}-¥{type}-¥{year}¥{month}¥{day}_¥{hour}¥{min}¥{sec}_¥{msec}.csv"/>	デフォルト
¥{type}(ログタイプ)	文書	<input type="text" value="Note"/>
	設計文書	<input type="text" value="Design"/>
	送信メール	<input type="text" value="SendMailbox"/>
	受信メール	<input type="text" value="ReceiveMail"/>

除外設定、CSVログファイル名の定義になります。

ログ対象アプリケーションの設定

CSVログフォーマット			
文書(Note) ?	設計文書(Design) ?	送信メール(SendMailbox) ?	受信メール(ReceiveMail) ?
<input type="button" value="標準"/> <input type="button" value="カスタム"/>	<input type="button" value="標準"/>	<input type="button" value="標準"/>	<input type="button" value="標準"/>
Server server Database Path dbpath Database Title dbtitle Date/Time now;yyyy/MM/dd HH:mm:ss.zzz Username user Note ID noteid Universal Note ID unid Level level Form form Field_1 field_1 Field_2 field_2 Field_3 field_3 Field_4 field_4 Field_5 field_5 Field_6 field_6 Field_7 field_7 Field_8 field_8 Field_9 field_9 Field_10 field_10 Attachments attachments_」	Server server Database Path dbpath Database Title dbtitle Date/Time now;yyyy/MM/dd HH:mm:ss.zzz Username user Note ID noteid Universal Note ID unid Level level Design Type noteclass Design Name fieldtitle_」	Server server Database Path dbpath Database Title dbtitle Date/Time now;yyyy/MM/dd HH:mm:ss.zzz Username user Note ID noteid Universal Note ID unid Level level Posted Date mail_posteddate From mail_from Send to mail_sendto Copy to mail_copyto Blind Copy to mail_blindcopyto Subject mail_subject Attachments attachments_」	Server server Database Path dbpath Database Title dbtitle Date/Time now;yyyy/MM/dd HH:mm:ss.zzz Username user Note ID noteid Universal Note ID unid Level level Posted Date mail_posteddate From mail_from Send to mail_sendto Copy to mail_copyto Blind Copy to mail_blindcopyto Subject mail_subject Attachments attachments_」

CSVログファイルフォーマット定義できます。

監視対象(ログ対象)アプリケーションの設定

The screenshot shows the 'LIVENESS AccessView V3.0' interface. On the left, there are buttons for 'アプリケーション設定' and '監視対象'. The main window displays a table of monitored applications with columns for '有効', 'DB名', 'ファイル名', and various actions. Below the table, the '監視アプリケーション' configuration panel is open, showing settings for '有効' (有効), '選択タイプ' (単一データベース), 'Notes DB' (demoYold_keiji.nsf), 'タイトル' (掲示板1), '受信メールログ' (受信メールログ), and '条件式' ('Form = "document"'). The 'フィールド' section contains 10 fields (Field_1 to Field_10) with selection buttons and values like 'Subject', 'Categories', and 'type'. At the bottom, there are checkboxes for '監視イベント' (観込, 変更, 作成, 削除, 設計変更, 設計作成) and '*アクセス集中アラート除外' (除外する).

フォルダ／DB単位で指定できます。
条件式、ログ取得するフィールド情報を定義可

CSV標準ログフォーマット

Notes/Webクライアントからのアクセスログ

1	Dominoサーバー名	
2	データベースパス	
3	データベース名	
4	ログ取得日時	
5	Notes ユーザー名	
6	ノーツ文書固有 (Note ID)	
7	ノーツ文書ID (UNID)	
8	監視イベント	Open (文書の読み込み)
		Update (文書の読み込み)
		Create (文書の読み込み)
		Delete (文書の削除)
9	フォーム名	
10	フィールド情報 (最大10個)	* カスタマイズにより追加可能
11	添付ファイル名	

CSV標準ログフォーマット

アプリケーション設計変更のアクセスログ

1	Dominoサーバー名	
2	データベースパス	
3	データベース名	
4	ログ取得日時	
5	Notes ユーザー名	
6	ノーツ文書固有 (Note ID)	
7	ノーツ文書ID (UNID)	
8	監視イベント	CreateDesignOpen (設計の作成)
		UpdateDesign (設計の修正)
		DeleteDesign (設計の削除)
9	設計要素(フォーム名、ビュー名など)	

CSV標準ログフォーマット

メール送受信のアクセスログ

1	Dominoサーバー名
2	データベースパス
3	データベース名
4	ログ取得日時
5	メールサーバー名
6	ノーツ文書固有 (Note ID)
7	ノーツ文書ID (UNID)
9	メール送信日時(受信日時)
10	メール送信元アドレス
11	メール送信先(To)アドレス
12	メール送信先(Cc)アドレス
13	メール送信先(Bcc)アドレス
14	メール件名
15	添付ファイル名

LIVENESS AccessView Alert

*オプションライセンス

アラート機能

アクセスログを監視して管理者へアラートメールを送信できます。
例えば、同一DBを短時間に大量アクセスするイベントが発生するとそのDBはローカルDBなどにコピーされている可能性があります。このようなイベントを監視することが出来ます。

LIVENESS AccessView Alert

アラート設定



アクセスログ

例)過去 5 分までの間で、1 分当たり 30 回以上、同じ操作した場合にアラートメールを送信



管理者へ
メール通知

アラート設定

アラートメール設定

アラートメールの使用	<input checked="" type="checkbox"/> 使用する
アラート対象ログ	nserver-notes (*指定ですべて対象) <ログファイル一覧> nserver-Note Notesクライアントからのログ nserver-Design 設計変更ログ nserver-SendMailbox メール送信ログ nRouter-ReceiveMail メール受信ログ nHTTP-Note Webクライアントからのログ
アラートのタイミング	過去 15 分までの間で、1 分当たり 50 回以上、同じ操作した場合にアラートメールを送信する。
アラート除外ユーザ	(除外ユーザなし) ※複数指定する場合は半角カンマが区切りです。
アラート除外イベント	<input type="checkbox"/> 誘込 <input checked="" type="checkbox"/> 変更 <input checked="" type="checkbox"/> 作成 <input checked="" type="checkbox"/> 削除
送信先	CN=admin liveness/O=liveness,CN=001 Ehime/O=liveness ※複数指定する場合は半角カンマが区切りです。
メールタイトル	【AccessView】NotesDB例外処理が発生
メール本文	AccessViewアラートメール 解析の結果、以下の条件でアラートが発生しましたので通知します。 計測開始時間: #{acc_time} から #{integ_min} 分間 アクセス数: #{acc_count} 回 データベース/ス: #{db_path} ユーザID: #{user_id} 操作: #{event}

アラート設定

アクセスログ参照

The screenshot shows the LIVENESS AccessView V2.00 interface. The main window displays a list of log files with columns for 'ログファイル名' (Log File Name) and 'ログ取得日' (Log Acquisition Date). A modal window titled 'AccessLog参照' is open, showing details for a selected log file.

ログファイル名	ログ取得日
AccessViewLog.csv	2021/01/19 09:11:19
AccessViewLog-nserver-SendMailbox.csv	2021/01/19 14:28:41
AccessViewLog-nserver-Note.csv	2021/01/19 14:28:42
AccessViewLog-nserver-Design.csv	2021/01/19 14:01:55
AccessViewLog-nRouter-ReceiveMail.csv	2021/01/19 14:28:41
AccessViewLog-nHTTP-Note.csv	2021/01/19 12:50:10
AccessViewLog-20210119_042919_000.csv	2021/01/18 15:58:11

AccessLog参照	
ログファイル名	AccessViewLog.csv
ログファイル	- AccessViewLog.csv
最終更新日時	2018/04/06 12:51:58

アクセスログ参照

動作環境

- サーバー
 - HCL Notes/Domino 9.0.1/v10/v11/v12
 - OS Windows Server 64bit ,
Linux(RHEL 7/8)
- アクセスログ対象アプリケーション
 - Notes アプリケーション (Notesシステム管理DBは対象外)

お問い合わせ

<https://www.liveness.co.jp/contact>

✉ info@liveness.co.jp