

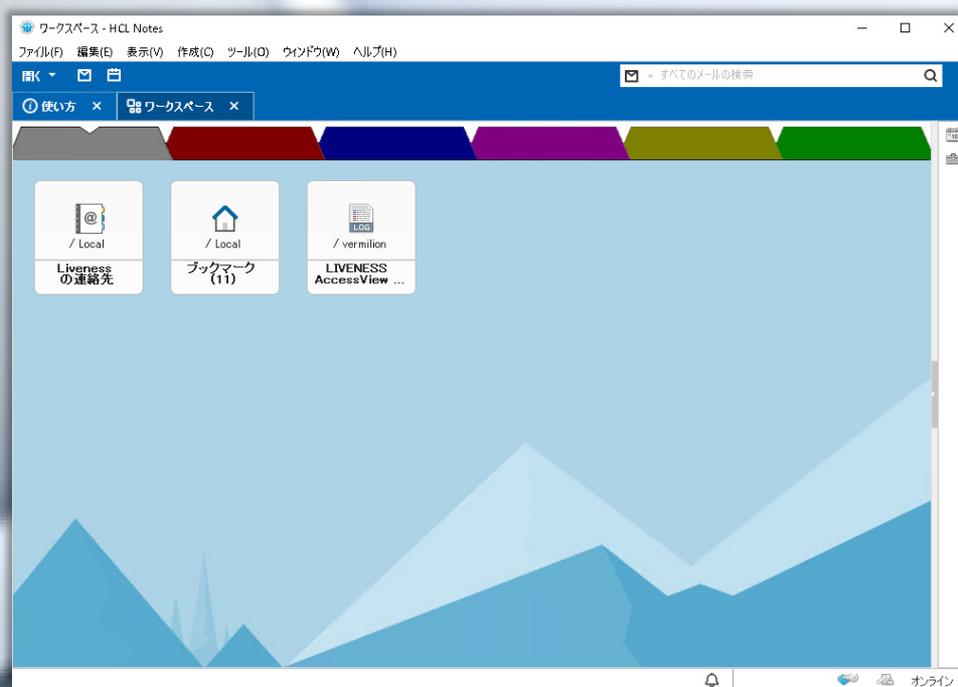
変わるスタイル、変えるスタイル。

LIVENESS SEREIS ご紹介

2021年3月



株式会社 ライブネス



LIVENESS AccessView

VERSION 2.0

Notesアクセスログを文書単位で取得。

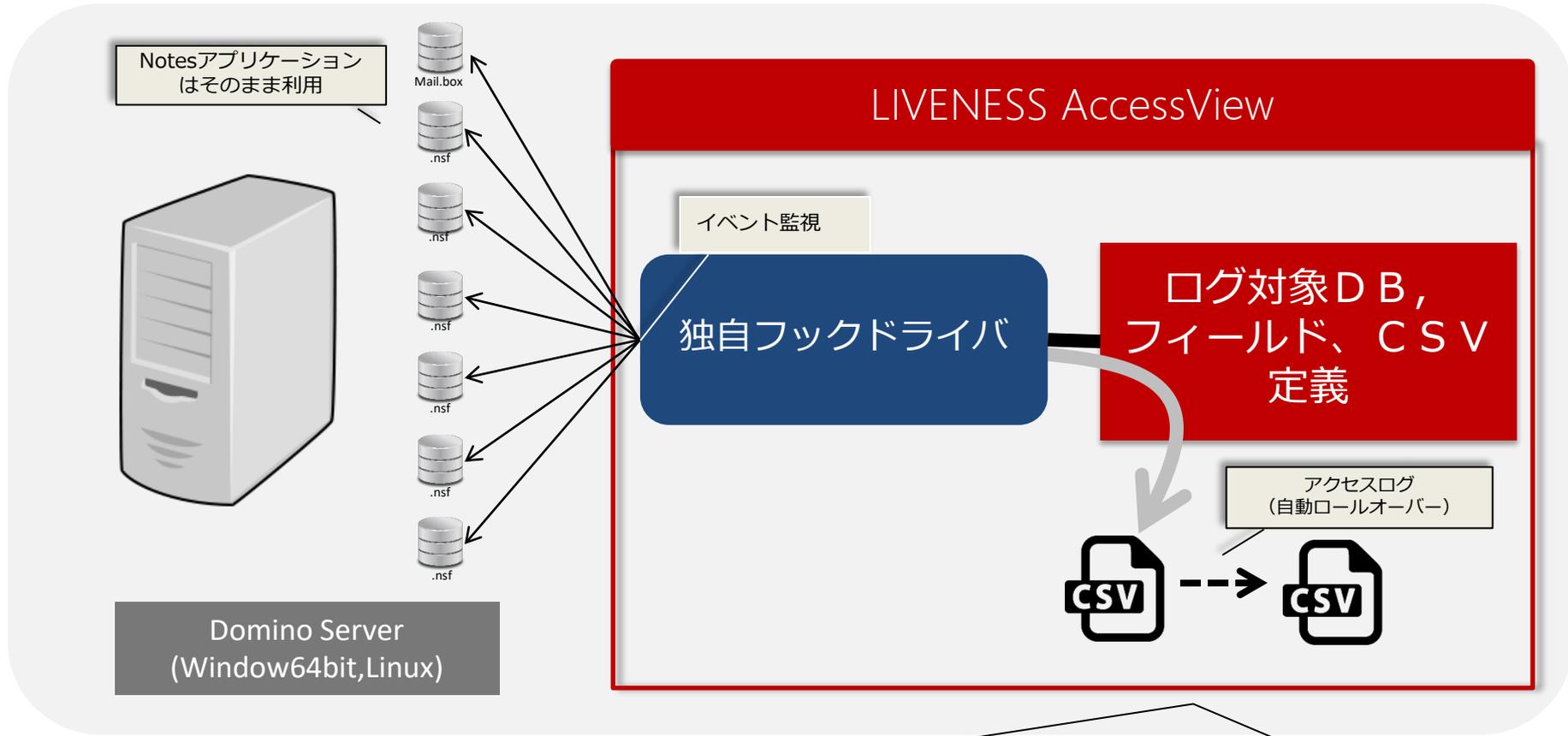
LIVENESS AccessView とは

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で使いづらい、営業サポート終了している。など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 誕生しました。

LIVENESS AccessView は指定したDBの文書単位でアクセスログをテキスト形式で出力します。



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=admi	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=admi	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=admi	932	4D692932	Open	document	2015/5 新製品情報										
winered/l/	demo¥old	B部門掲示	57:38.1	CN=admi	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=admi	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=admi	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=admi	0000092a	C40A34EE	Open	document	111迷走するカン？ 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										

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

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

ログ対象アプリケーションの設定

The screenshot displays the '監視アプリケーション' (Monitoring Application) configuration page in LIVENESS AccessView V2.00. The page is divided into several sections:

- 監視アプリケーション (Monitoring Application):** Includes options for '有効' (Enabled) and '無効' (Disabled), '選択タイプ' (Selection Type) set to '単一データベース' (Single Database), 'Notes DB' set to 'demo#event.nsf', 'タイトル' (Title) set to 'イベント案内', and '取得済ログの参照' (Reference to Retrieved Logs) set to '取得メールログ' (Retrieved Email Log).
- フィールド (Fields):** A list of 11 fields (Field_1 to Field_10) with selection buttons and values like 'e_Body', 'e_Time_Stat', and empty strings.
- 監視イベント (Monitoring Events):** Checkboxes for '読込' (Load), '作成' (Create), '変更' (Change), and '削除' (Delete).
- アクセス集中アラート除外 (Exclude Access Concentration Alerts):** A checkbox for '除外する' (Exclude).
- 設計削除 アラート除外 条件式 (Design Deletion Alert Exclusion Conditions):** A table on the right side of the screen.

設計削除	アラート除外	条件式
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	@all
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	@all
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	@all
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Form = ""
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Form = "rouge"
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	@all
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	@all
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Form = "event"
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	@all
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Form = ""
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Form="Main T
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	@all

Ver 2.00

監視アプリケーションの設定

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で区切りします。
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 Etime/O=liveness ※複数指定する場合は半角カンマで区切りします。
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 top bar displays 'LIVENESS AccessView V2.00' and 'admin liveness'. The left sidebar contains navigation items: '監視アプリケーション' (Monitoring Applications), 'アラートメール設定' (Alert Mail Settings), and '取得済ログの参照' (Reference of Retrieved Logs). The main area shows a table of log files with columns 'ログファイル名' (Log File Name) and 'ログ取得日' (Log Retrieval Date). A modal window titled 'AccessLog参照' is open, displaying the following information:

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

A callout box points to the modal with the text 'アクセスログ参照'.

アプリケーションアクセスログ取得項目

Notes/Webアクセスごとにアクセスログを文書単位で取得します。

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)	
11	添付ファイル名	

アプリケーション設計変更ログ取得項目

設計要素の変更ログを取得します。

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)	

メール送信・受信ログ取得項目

メールの送受信ログを取得します。

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

動作環境

- **サーバー**

- HCL Notes/Domino 9.0.1以上 (v10/v11動作検証済)
- 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

株式会社 ライブネス

info@liveness.co.jp

担当：赤松