

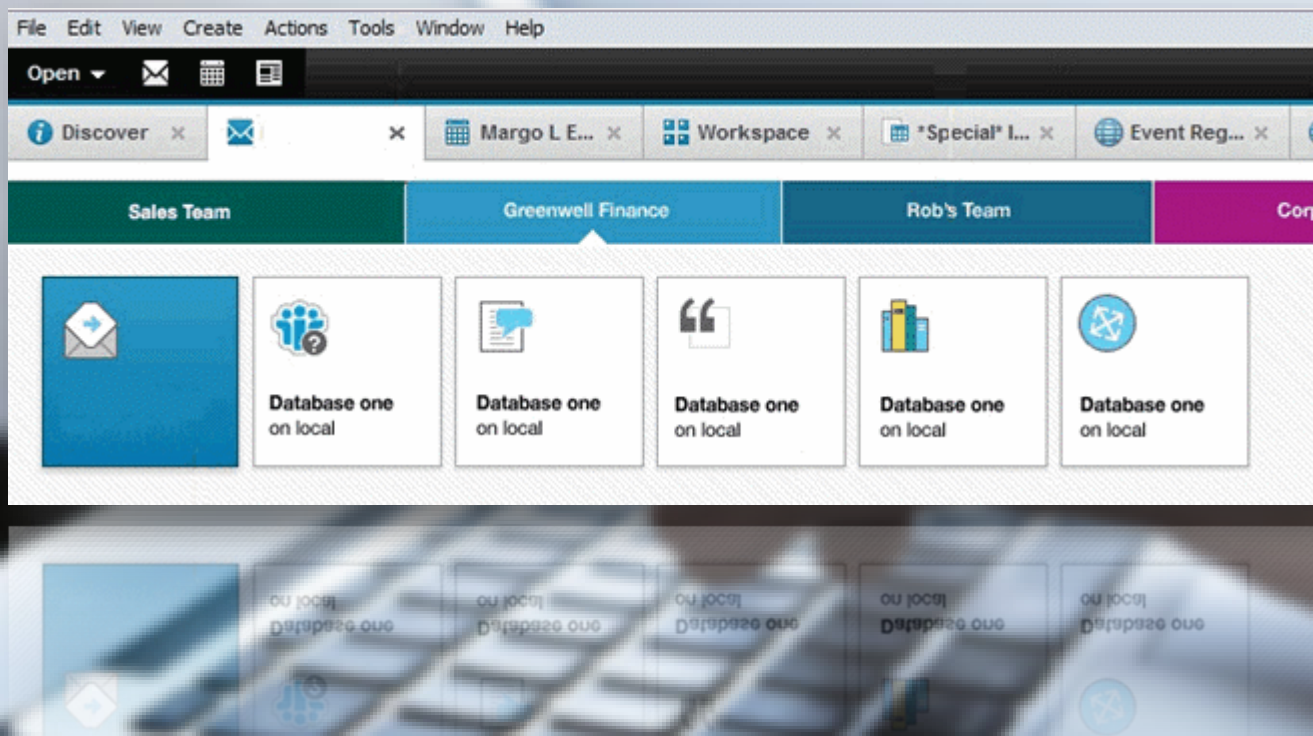
変わるスタイル、変えるスタイル。

LIVENESS SEREIS ご紹介

2019年8月



株式会社 ライブネス



LIVENESS AccessView

Notesアクセスログを文書単位で取得。

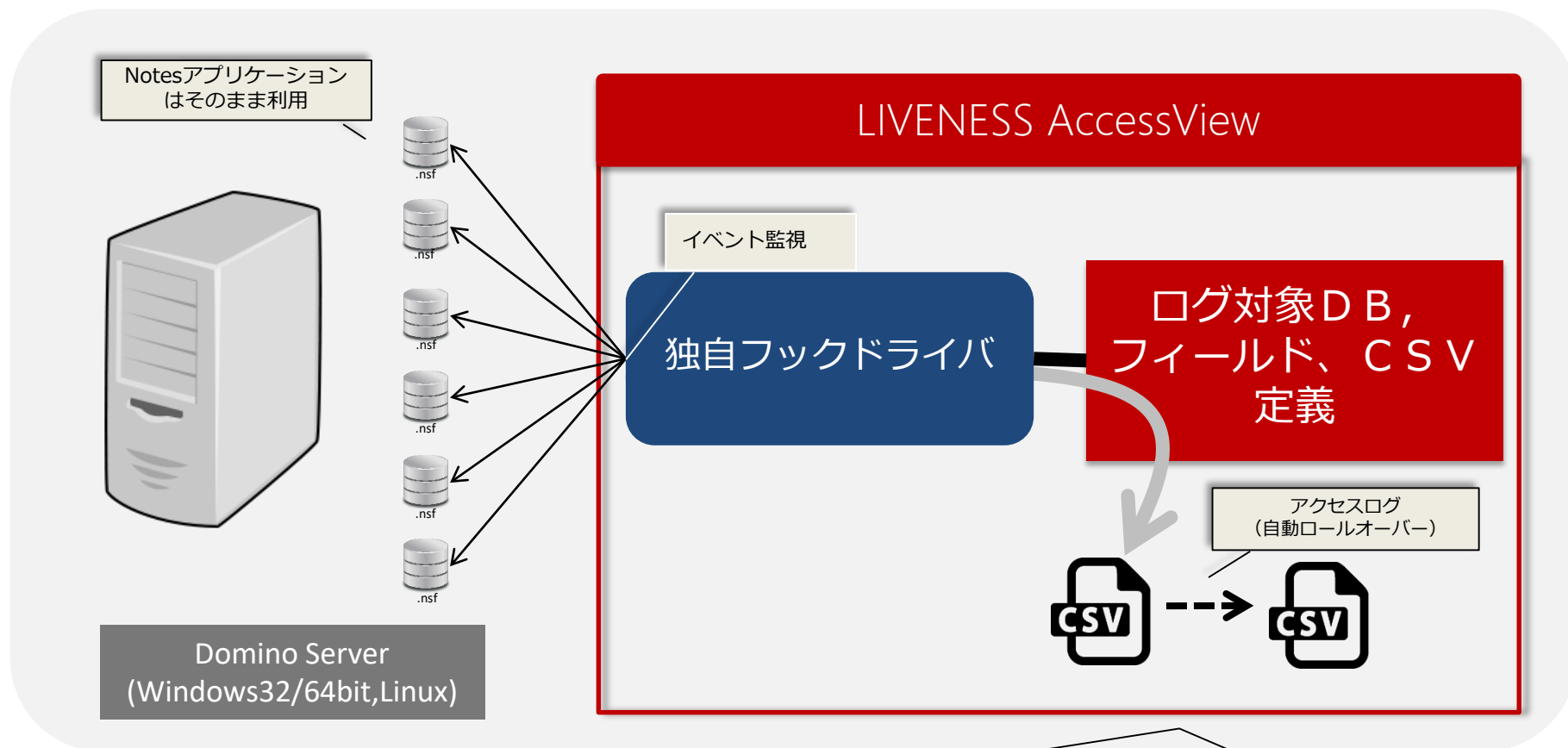
LIVENESS AccessView とは

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。



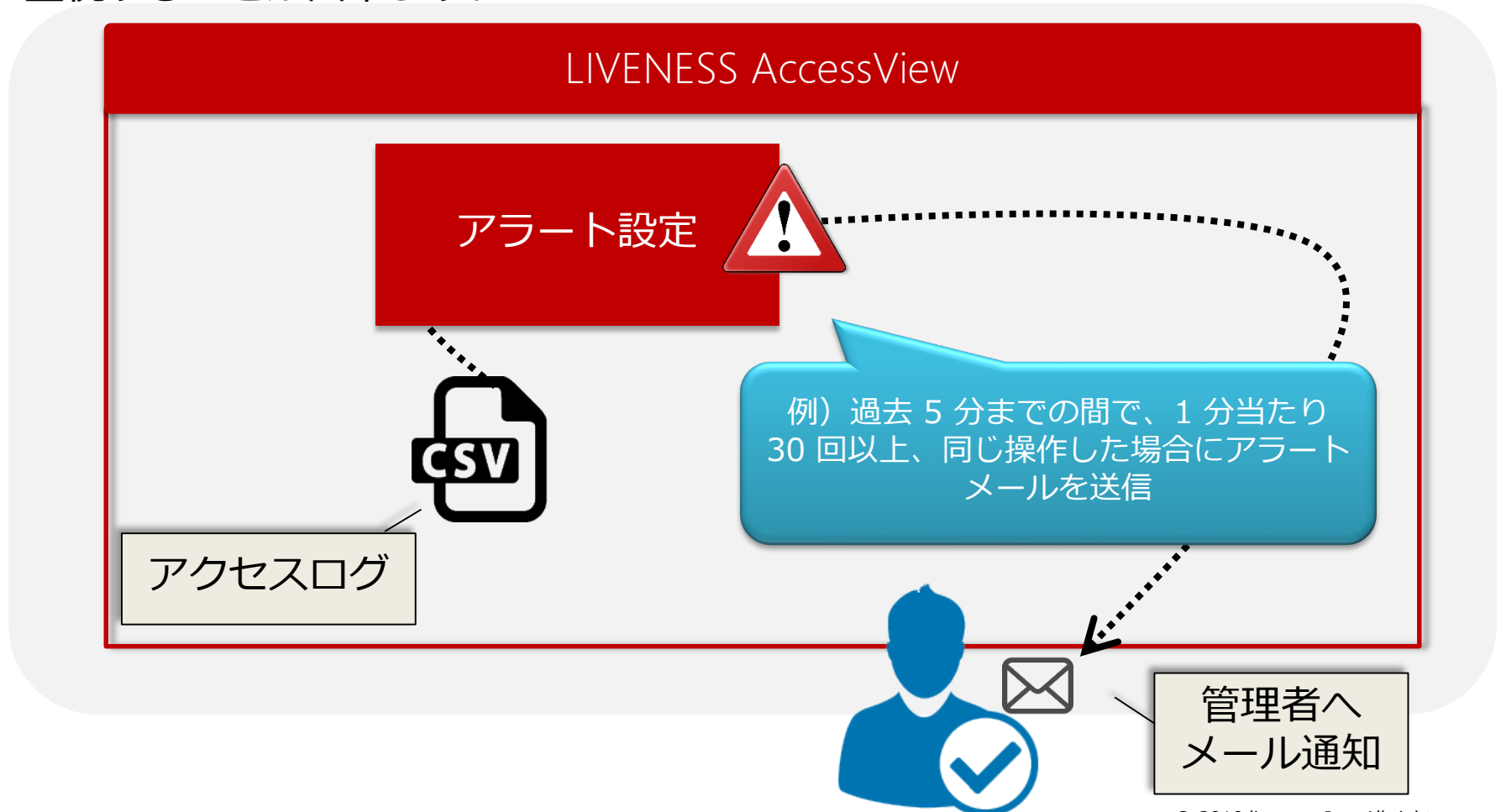
LIVENESS AccessView機能概要



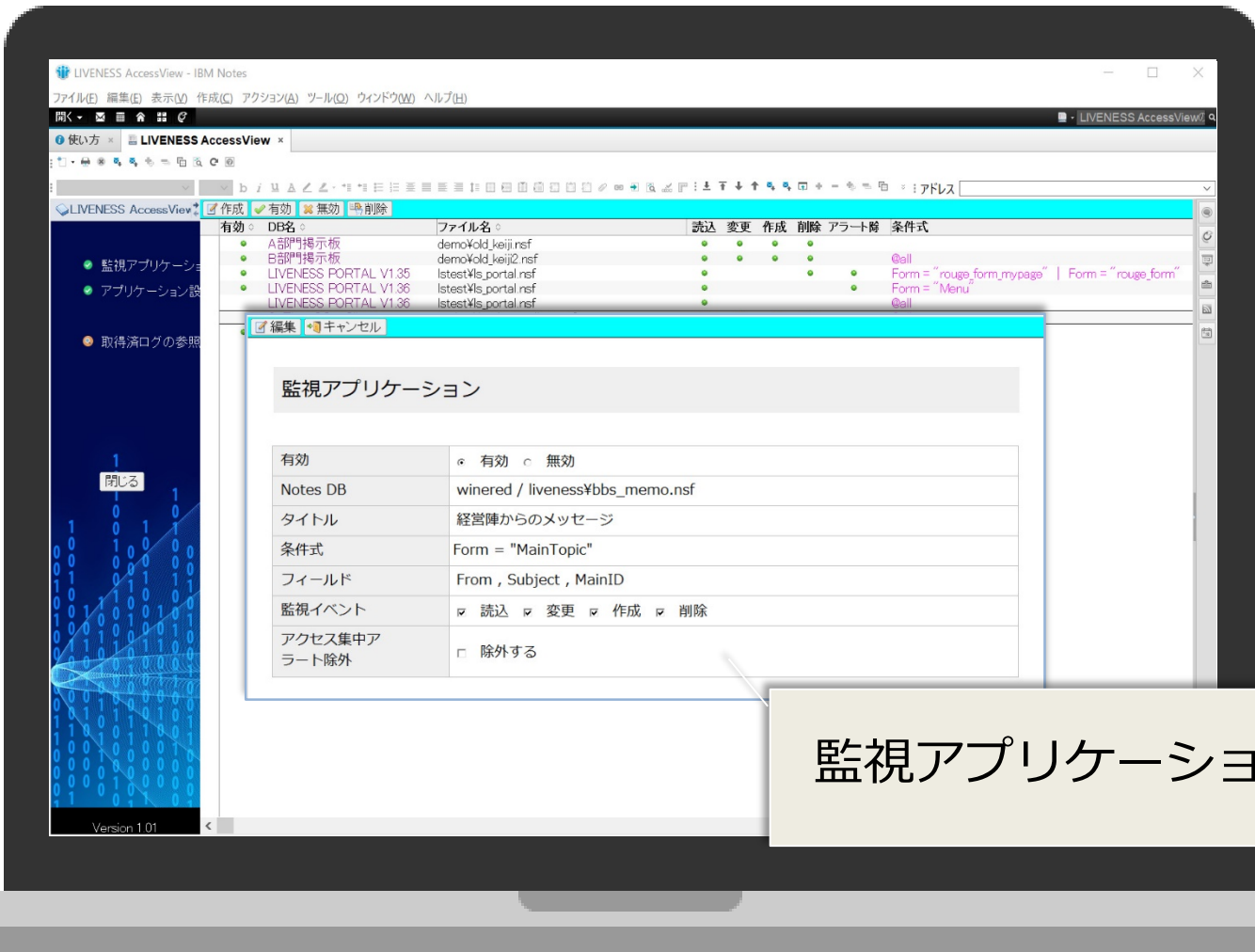
Server	Database	Database	Data/Tim	Username	Note ID	Universal	Level	Form	Field_1	Field_2	Field_3	Field_4	Field_5	Field_6	Field_7	Field_8	Field_9	Field_10	Attachments
winered/l	demo¥old	B部門掲	57:36.2	CN=admi	926	F6D61F1E	Open	document	当社製品が日経新聞に掲載されました。										ポータルご提案資料_20171017.pptx;PORTAL_top.pptx;ポータル利用イメージ.pptx
winered/l	demo¥old	B部門掲	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	57:37.9	CN=admi	932	4D692932	Open	document	2015/5 新製品情報										
winered/l	demo¥old	B部門掲	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	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	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	57:38.8	CN=admi	0000092a	C40A34EE	Open	document	111迷走するカジノ解禁、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										

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できます。



ログ対象アプリケーションの設定



The screenshot displays the LIVENESS AccessView application configuration interface. The main window shows a table of monitored applications. A modal dialog titled "監視アプリケーション" (Monitoring Application) is open, showing configuration details for a specific application.

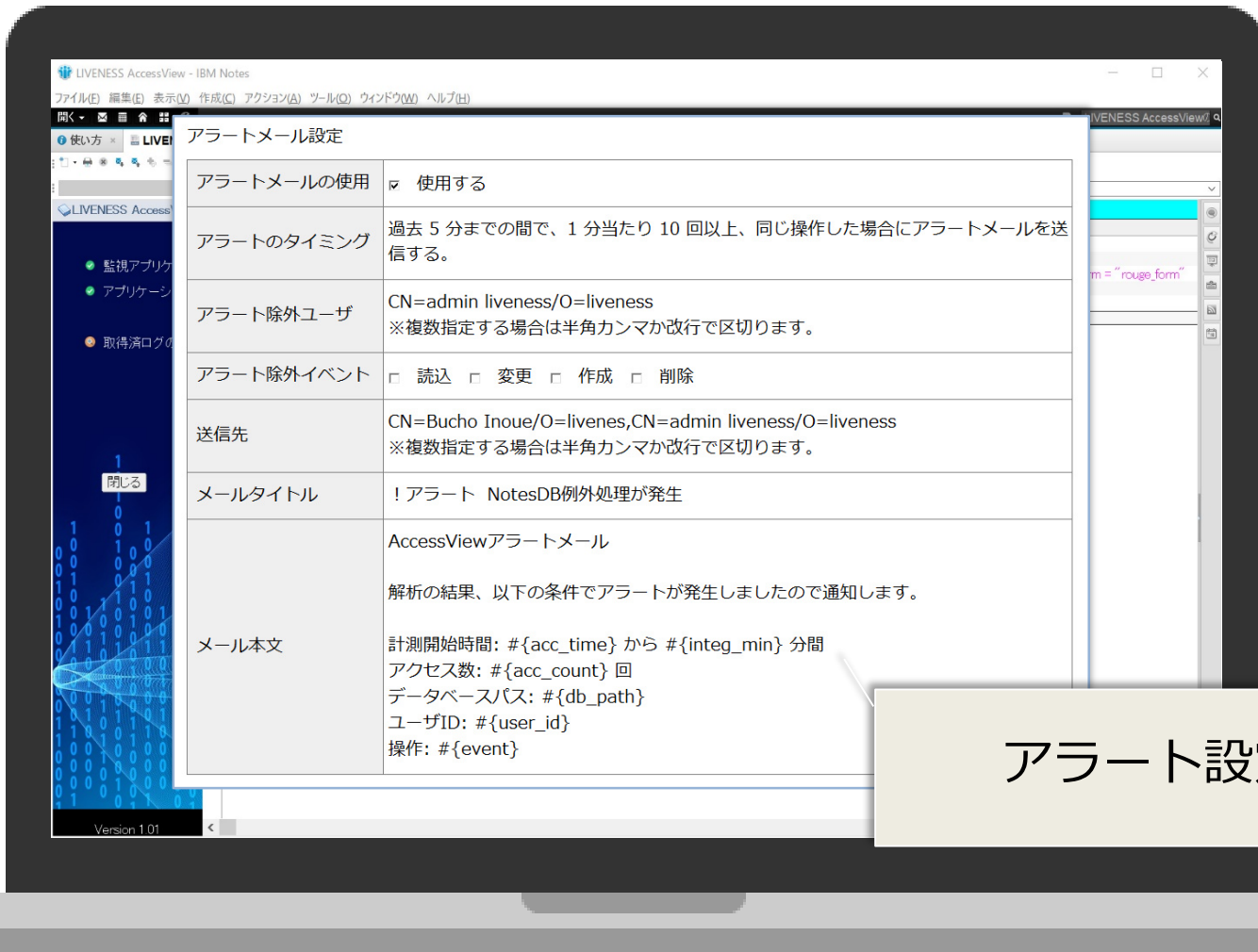
有効	DB名	ファイル名	読込	変更	作成	削除	アラート	条件式
☒	A部門掲示板	demoVold_keiji.nsf	☒	☒	☒	☒		@all
☒	B部門掲示板	demoVold_keiji2.nsf	☒	☒	☒	☒		Form = "rouge_form_mypage" Form = "rouge_form"
☒	LIVENESS PORTAL V1.35	lsteetVls_portal.nsf	☒	☒	☒	☒		Form = "Menu"
☒	LIVENESS PORTAL V1.36	lsteetVls_portal.nsf	☒	☒	☒	☒		@all

The modal dialog "監視アプリケーション" (Monitoring Application) shows the following configuration details:

有効	☒ 有効 ☐ 無効
Notes DB	winered / liveness¥bbs_memo.nsf
タイトル	経営陣からのメッセージ
条件式	Form = "MainTopic"
フィールド	From , Subject , MainID
監視イベント	☒ 読込 ☒ 変更 ☒ 作成 ☒ 削除
アクセス集中アラート除外	☐ 除外する

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	☒ 使用する
アラートのタイミング	過去 5 分までの間で、1 分当たり 10 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	CN=admin liveness/O=liveness ※複数指定する場合は半角カンマで改行で区切ります。
アラート除外イベント	☐ 読込 ☐ 変更 ☐ 作成 ☐ 削除
送信先	CN=Bucho Inoue/O=liveness,CN=admin liveness/O=liveness ※複数指定する場合は半角カンマで改行で区切ります。
メールタイトル	！アラート 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 データベースパス: #{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 displays the LIVENESS AccessView application interface. On the left, a sidebar contains navigation options: 監視アプリケーション (Monitoring Application), アプリケーション設定 (Application Settings), and 取得済みログの参照 (Reference of Retrieved Logs). The main window shows a table 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 dialog box titled 'AccessLog参照' (AccessLog Reference) is open, showing details for the selected file 'AccessViewLog.csv'. The dialog includes fields for ログファイル名 (Log File Name), ログファイル (Log File), and 最終更新日時 (Last Updated Date). A callout box points to a specific log entry in the table, and a large yellow box at the bottom right contains the text 'アクセスログ参照' (AccessLog Reference).

ログファイル名	ログ取得日
AccessViewLog.csv	2018/04/06 12:51:58
AccessViewLog_20171213_145443_892.csv	2017/12/13 14:54:43
AccessViewLog_20171215_144313_046.csv	2017/12/15 14:43:13
AccessViewLog_20171219_153024_788.csv	2017/12/19 15:30:24
AccessViewLog_20171222_133829_942.csv	2017/12/22 13:38:29
AccessViewLog_20171224_175909_280.csv	2017/12/24 17:59:09
AccessViewLog_20180109_204418_398.csv	2018/01/09 20:44:18
AccessViewLog_20180112_180924_910.csv	2018/01/12 18:09:24
AccessViewLog_20180116_203300_574.csv	2018/01/16 20:33:00

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

ログ取得項目

アクセスした文書レベルでログを取得します。

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	アクセス日時	
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	

動作環境

- **サーバー**

- IBM Notes/Domino 9.0.1以上 (10.0.1動作検証済)
- OS Windows Server 32/64bit ,
Linux(CentOS 7.0,RedHat 7.0)

- **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 (メール、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