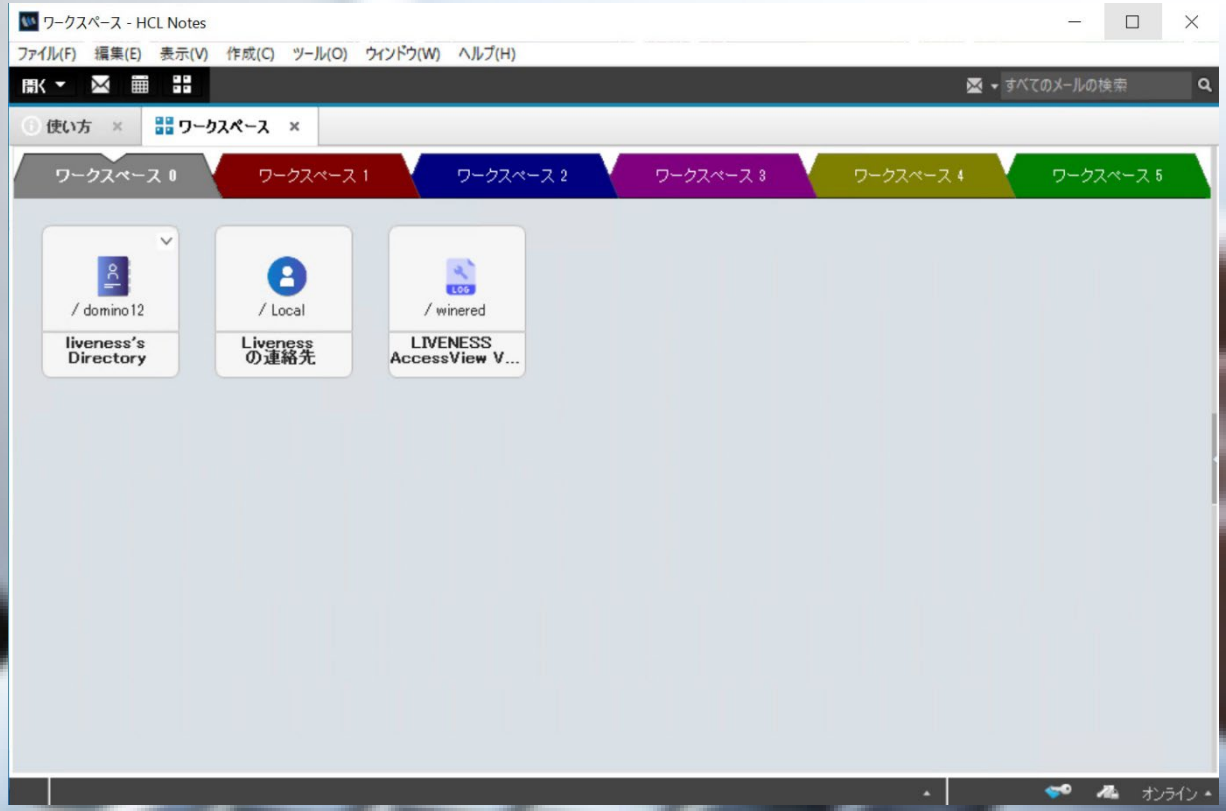


LIVENESS AccessView

VERSION 3.0

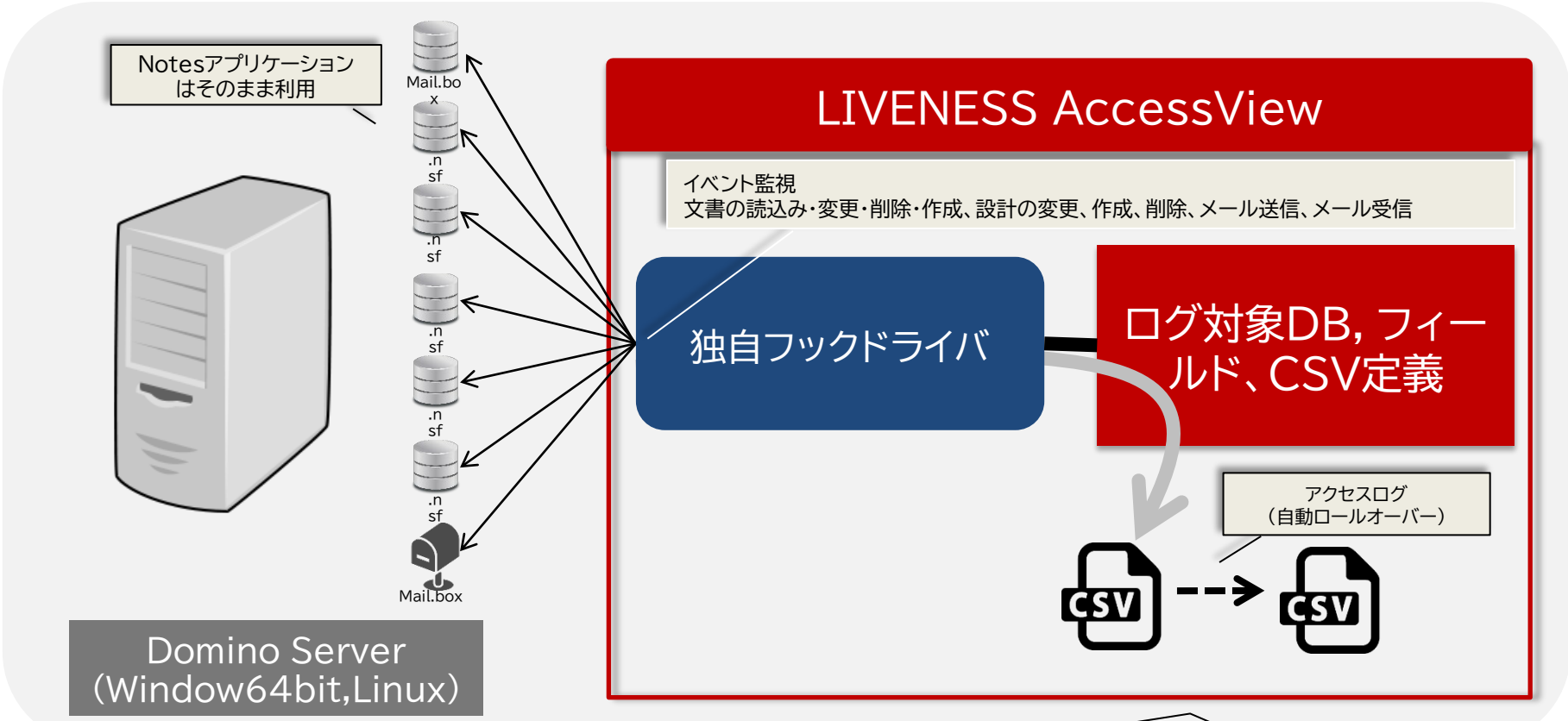
Notesアクセスログを文書単位で取得する。

LIVENESS AccessView とは

Notesログでは物足りない、Domlogではわかりずらい。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ずらい、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。そんなノーツ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。

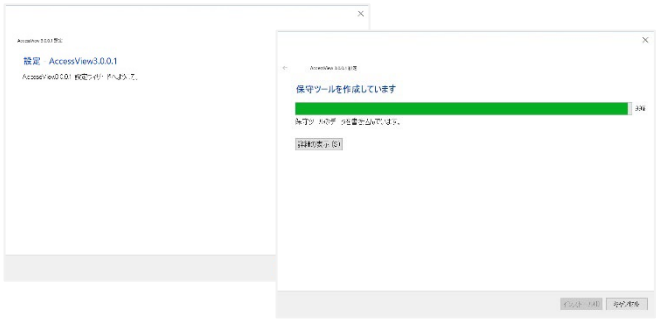
LIVENESS AccessView機能概要



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/I	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/I	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/I	demo¥old	B部門掲示	57:37.9	CN=admi	932	4D692932	Open	document	2015/5 新製品情報										
winered/I	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/I	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/I	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/I	demo¥old	B部門掲示	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										

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:¥PROGRA~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		◉ Windows ○ Linux	
フックドライバー除外DB	?	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	?	『』	
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	?	☐ オン	

CSVログ

保存フォルダ	?	『d:¥AccessView』	Dataフォルダ
ファイル名	?	『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	?	○ サイズ ◉ デイリー	
ローテーションファイル名	?	『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	『Note』	
	設計文書	『Design』	
	送信メール	『SendMailbox』	
	受信メール	『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) 標準 カスタム	設計文書(Design) 標準	送信メール(SendMailbox) 標準	受信メール(ReceiveMail) 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

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（文書の読込み）
		Update（文書の読込み）
		Create（文書の読込み）
		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

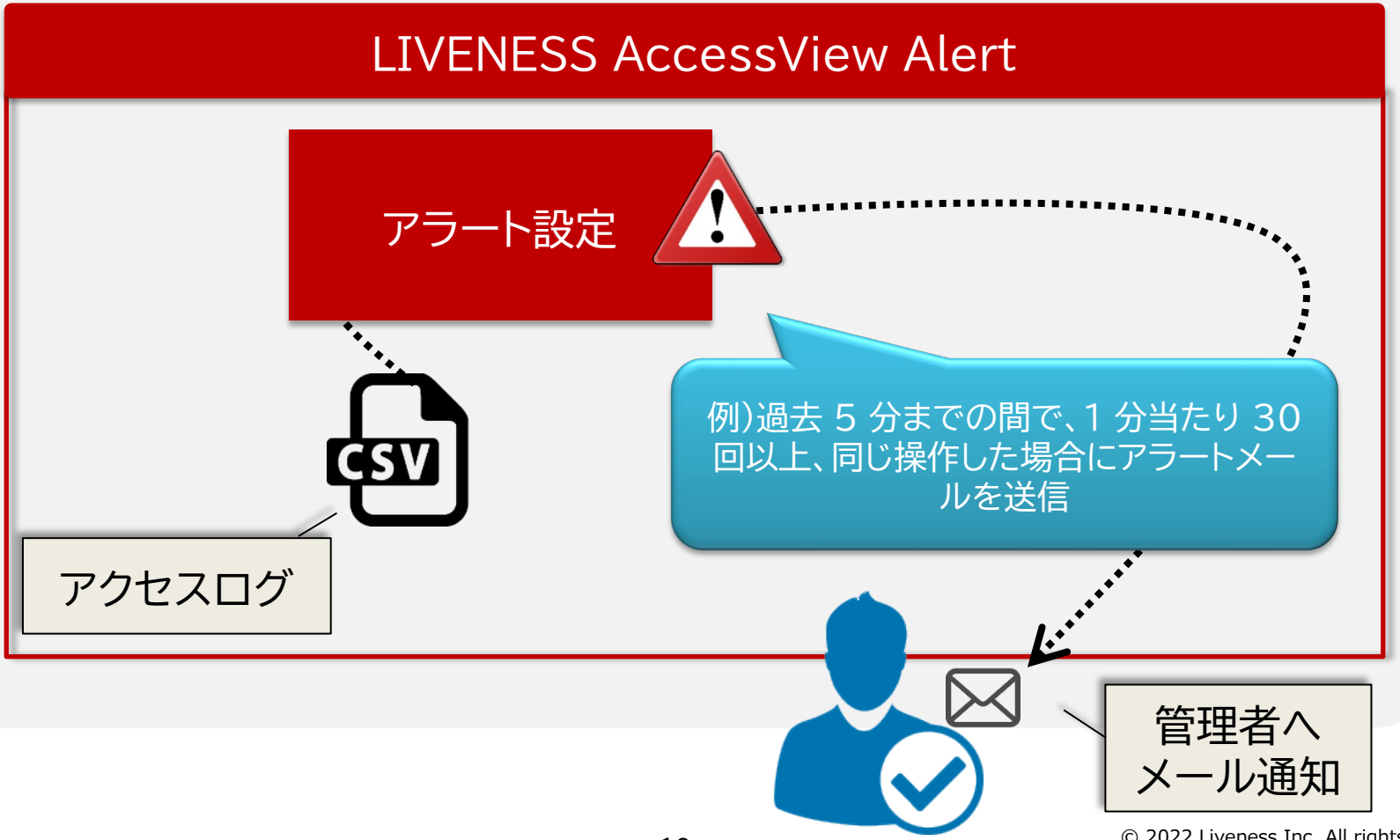
1	Dominoサーバー名
2	データベースパス
3	データベース名
4	ログ取得日時
5	メールサーバー名
6	ノーツ文書固有（Note ID）
7	ノーツ文書ID（UNID）
9	メール送信日時(受信日時)
10	メール送信元アドレス
11	メール送信先(To)アドレス
12	メール送信先(Cc)アドレス
13	メール送信先(Bcc)アドレス
14	メール件名
15	添付ファイル名

LIVENESS AccessView Alert

＊オプションライセンス

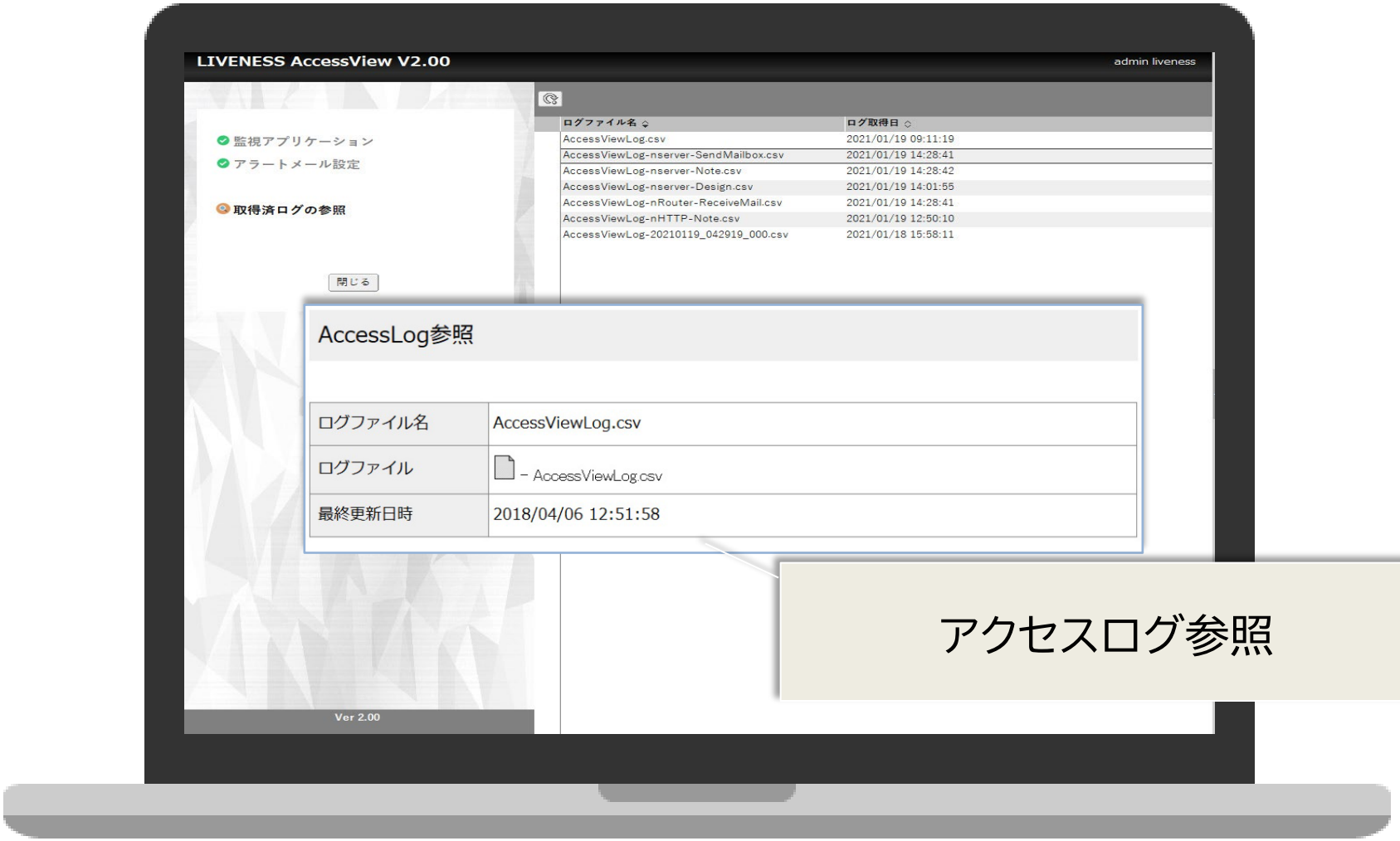
アラート機能

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。



アラート設定

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