ALog V8 説明資料
～ 全般的な変更点～

日付： 2023/04/28
会社名： 株式会社網屋
部署名： 開発部

はじめに

ALog V8は、V7をベースにし、様々な機能拡張を行っております。
本資料ではV7とV8において異なる点をメインに解説します。
本資料の他に以下の資料も必要に応じてご確認ください。

① バージョンアップガイド …サポートサイトに掲載

②ユーザーガイド …製品に同梱

はじめに

- V7からV8へのバージョンアップは、「setup.exeを実行して上書きインストール」となります。V7のマイナーアップデート時の手順と同様です。
  - アーキテクチャに変更はありませんので大きな構築しなおしは発生しません。
  - 引き続き、ALog V8をインストールすることで、ALogの各製品すべてを管理することができます。
    （for Windows/for NetApp/for EMC/for PowerScale/for SQL Server/for Oracle/for Linux/ALog EVA/管理機能/検索機能）
  - 詳細は、バージョンアップガイドを参照してください。

- Webコンソールに大きな変更点はありません。
  - 管理画面のページはメニュー項目の増加に伴い、メニューの順番変更や再構成を行ないました。

- V6からV8へは直接移行できません。一度V7へ移行してからV8へバージョンアップしていただくか、V8を新規で構築していただく必要があります。

- 特別なオプションを使用しているお客様は、サポートへお問い合わせください。

目次

本文書は以下のとおり解説します。

V8では新機能を搭載しています。

1. AI リスクスコアリング機能

AIによるリスクスコアリング機能を搭載しました。
詳細は「ユーザーガイド」-「リスクスコアリングを使う」を参照してください。

2. WorkTime機能

別製品であったAttend ManagerをALog V8に搭載しました。
詳細は「ユーザーガイド」-「WorkTimeを使う」を参照してください。

1-1. AI リスクスコアリング機能

AI が過去のログから【普段】の行動モデルを自動生成し、【異常】の度合いをスコアリングします。また、ファイル名からも【異常】の度合いをスコアリングします。
スコアリングの対象としないパスを登録することでスコア調整を行うこともできます。

■ 異常が検知される例

① 普段アクセスが少ない時間帯にアクセスが多い。

時間帯毎のアクセス数の分布を過去のアクセスログからユーザー単位で解析します。そのデータを元に、
普段よりアクセスが多い時間帯が存在した時に異常と判断し、その度合をスコアとして出力します。

② 普段アクセスしないファイルにアクセスする。

ユーザー毎に普段どんなファイルにアクセスするかを過去のアクセスログから解析します。そのデータを元に、
そこから逸脱したファイルにアクセスした時に異常と判断し、その度合をスコアとして出力します。

1-2. WorkTime機能（勤怠管理）

「Attend Manager」をリニューアルしました。
主な変更点は以下のとおりです。

「WorkTime」はライセンスが必要です。
既に「Attend Manager」をご利用のお客様には新たにライセンスを発行いたしますのでお問合せください。

■ 主な変更点

① GUIによる設定及び結果の閲覧を可能に

GUIによる設定が可能になりました。また、勤怠の情報を画面から確認することも可能となり、可読性が向上するとともに、より効率的に管理できるようになりました。

② 出勤/退勤とみなすログを自由に設定可能に

出勤/退勤とみなすログの条件を自由に指定できるようにしました。これにより、ログオン/ログオフ以外にも入退室のログなどを出勤/退勤とみなしたりすることができるようになりました。

③ 様々なファイル出力を可能に

勤怠表やランキング等、様々な形式でファイルを出力することができるようになりました。
また、CSVだけでなく、Excel形式でも出力することが可能となりました。

2. システム要件

システム要件の主な変更点を記載します。
システム要件の詳細や、最新のOSの対応状況はV8の「ユーザーガイド」を参照してください。

※対応OSに関しては、各開発元のサポートが終了している場合、十分なサポートを提供できないため、サポート中のバージョンへのアップデートを強く推奨します。
※V7からV8にバージョンアップするにあたり、使用ポートに変更はありません。

マネージャーサーバ	対応OS	V7から変更あり Windows Server 2008/2008R2 のサポートを終了 Windows Server 2012 〜 に対応
	.Net Framework	V7から変更あり .NET Framework 4.8以上
	CPU	V7から変更あり 推奨：Quad Core以上→2.7GHz 8コア以上 最低：Dual Core以上→記載なし ※元々2.0GHz 4コア以上と記載していたが、それ以上必要なケースが多い
	メモリ	V7から変更あり 推奨：16GB以上→32GB以上 最低：8GB以上→記載なし ※8GBでは足りないケースが多い
	必要ブラウザ	V7から変更あり Internet Explorer10のサポートを終了 FireFox、Google Chrome、Microsoft Edgeに対応 ※IE11は2022/6/15サポート終了
	必要ソフトウエア	for SQL Serverの場合の作業用DBが不要に for Oracleの場合のOracle Clientが不要に
for Windows	対応OS	V7から変更あり Windows Server 2008/2008R2 のサポートを終了 Windows Server 2012 〜 に対応
	.Net Framework	エージェント方式の場合 2.0→4.5に変更
for NetApp	対応OS	V7から変更あり ※開発元サポートが終了しているバージョンを終了 [Data ONTAP] 全てのサポートを終了 [ONTAP] 9.1未満、9.2、9.4のサポートを終了 9.5〜 に対応
for EMC	対応OS	V7から変更あり ※開発元サポートが終了しているバージョンを終了 [DART] サポート終了 [VNX OE] サポートを終了 [VNXe OE]サポートを終了 [Unity] 5.0.3 〜 に対応 [PowerStore] 1.0 〜に対応

for PowerScale (旧 Isilon)	対応OS	V7から変更あり ※開発元サポートが終了しているバージョンを終了 OneFS 7.2.0未満のサポートを終了 9.0.0 〜 に対応
for SQL Server	対応OS	V7から変更あり Windows Server 2008/2008R2 のサポートを終了 Windows Server 2012 〜 に対応
	対応SQL Server	V7から変更あり SQL Server 2014未満のサポートを終了 SQL Server 2014 〜 に対応
	.Net Framework	エージェント方式の場合 2.0→4.5に変更
for Oracle	対応OS	V7から変更あり Windows Server 2008/2008R2 のサポートを終了 Windows Server 2012 〜 に対応
	対応Oracle Database	V7から変更あり Oracle Database 11g のサポートを終了 Oracle Database 12.2.x 〜 に対応
	.Net Framework	エージェント方式の場合 2.0→4.5に変更
for Linux	–	V7から変更あり RHEL 8〜 に対応 CentOS 6 のサポートを終了
ALog EVA	–	変更なし
Amazon FSx for Windows File Server	–	V8.4.0から製品群に追加
Amazon FSx for NetApp ONTAP	–	V8.5.0から製品群に追加

3. 製品（for XXX）ごとの変更点

製品ごとの機能追加/変更点についてまとめます。
表は、変更点の有無を示します。（変更のあるものは「●」）

	変換エンジン	監査設定	操作種別	詳細項目	ライセンス
Windows	●	–	●	●	–
NetApp	●	●	●	●	●
EMC	–	–	–	–	●
PowerScale	●	●	●	●	●
SQL Server	●	●	–	–	●
Oracle	●	●	–	–	●
Linux	–	–	–	●	–
ALog EVA	–	–	–	–	–

製品ごとの機能追加/仕様変更の詳細は以降のページを参照してください。
また、変換エンジンの変更等による詳細なファイルアクセスログ出力結果の変更については、
「ALogV8説明資料_ファイルアクセスログ編」をご確認ください。

3-1. for Windowsの変更点 （1/2）

- **変換エンジンの刷新**
  - 精度の高い変換を行なうため、新変換エンジンを開発
  - 変換エンジンが変わっているため出力が変更されている
    ※詳細は、「ALogV8説明資料_ファイルアクセスログ編」参照
  - 変換に使用するEventIDに変更はあるが、監査ポリシー/フォルダーの監査設定共に設定変更の必要はない
  - 要望の多いCOPYとMOVEを可能な限り出力できるよう対応
  - 今まで出力されていた余分なログも減らせるようにした、初期の除外フィルターに「.tmp」追加

- **任意EventIDを指定し収集変換する機能の追加**
  - for WindowsのAdvanced Editionライセンスが必要
  - ALogが変換対象としていないEventIDを監査対象とする必要がある場合、複雑でなければfor Windowsで対応可能に
    （複雑な場合は今までどおりALog EVAで対応）

3-1. for Windowsの変更点 （2/2）

■操作種別の変更

ログの種類	出力内容（操作）
ファイルアクセスログ	READ
	READ-Failure
	WRITE
	WRITE-Failure
	DELETE
	DELETE-Failure
	RENAME
	RENAME-Failure
	MOVE
	COPY
ログオンログ	LOGON
	LOGON-Failure
管理者操作ログ	ADMIN
	ADMIN-Failure
プリントログ	PRINT
ログオン/ログオフログ（スクリプト）	LOGON
	LOGOFF
アプリケーション起動ログ	CREATE
	EXIT
アクセス権変更ログ	P-ACCESS
	P-ACCESS-Failure

新規で追加

■詳細キーの変更

ログの種類	詳細項目
すべてのログ	Count
ファイルアクセスログ	ClientName / ClientIP / AppName / To
ログオンログ	AuthType / LogonType / ErrorCause / ClientIP / ClientName
管理者操作ログ	EventID / ClientIP / ClientName
プリントログ	Printer / Pages
ログオン/ログオフログ（スクリプト）	LogonType / ClientIP / ClientName
アプリケーション起動ログ	AppName / ClientIP / ClientName
アクセス権変更ログ	ClientName / ClientIP /AppName

新規で追加
RENAME/COPY/MOVE時に出力される

3-2. for NetAppの変更点 （1/2）

- **サポート終了に伴い、対象サーバ登録時の「7-mode」および「vFiler機能」の選択肢を撤廃**
- **変換エンジンの刷新（ONTAP）**
  - 精度の高い変換を行なうため、新変換エンジンを開発
  - 変換エンジンが変わっているため出力が変更されている
  - ※詳細は、「ALogV8説明資料_ファイルアクセスログ編」参照
  - 変換に使用するEventIDに変更はあるが、監査ポリシーに変更はなし
  - フォルダーの監査は「アクセス権変更ログ」の場合設定変更の必要あり
    - フルコントロール　→　必要な設定のみにする必要がある
  - MOVEは可能な限り出力できるよう対応
  - 初期の除外フィルターに「.tmp」を追加
- **画面からの「フォルダーの監査設定」機能追加（ONTAP）**
- **公開鍵認証を使用したSSH接続に対応（ONTAP）**
- **ALog経由で新規ボリューム作成する場合、サイズ指定を可能に（ONTAP）**
- **audit_<vserver_name>_<time_stamp>.partial.evtxを収集、変換対象に**
  - NetApp社との確認によりV7.4.0でpartial.evtxを収集、変換対象から除外したが、BURT#1084009の内容やNetApp社への再確認により上記ファイル名のログは通常のログにマージされずに残存することが判明したため。

3-2. for NetAppの変更点 （2/2）

- **ONTAP用出力形式オプション「PrefixType」の廃止**
  - PrefixTypeはアクセスログ「対象」欄に出力されるファイルパスの先頭にくるボリューム名の指定機能
    - 本オプションは資料「NetApp_Cluster-Modeの出力形式オプションの追加に関するお知らせ.pdf」によって解説されている
    - イベントログにボリューム名が出力されていないOS バージョンに対するフォロー機能であったが、該当バージョンがすべてサポート終了となったため、ALogでも対応を終了した
    - V8では「PrefixType」の設定がどのようになっていても参照せず、イベントログに記録されたボリューム名をそのまま出力する

パターン番号	初期状態	「対象」欄の出力結果
1 DSIDPrefix	V7.1.3以前にALogをインストールされたお客様	ObjectNameから()のボリューム名を省いたパスの先頭に、DSID番号を付与して出力します。DSID番号はイベントログのHandleIDの一部を10進数にした数字です。 <例> ¥1105¥02_開発部¥04_ALog¥01_pgXX¥要件定義.xlsx
2 NonePrefix	V7.1.4～V7.3.0の間にALogをインストールされたお客様	ObjectNameから()のボリューム名を省いたパスを出力します。 <例> ¥02_開発部¥04_ALog¥01_pgXX¥要件定義.xlsx
3 VolNamePrefix	V7.3.1でALogを新規インストールされたお客様	イベントログのObjectNameを()も含めたそのままの情報で出力します。 <例> (vol7);¥02_開発部¥04_ALog¥01_pgXX¥要件定義.xlsx

- **ライセンス表記を変更**
  - 「サーバライセンス」を「物理サーバライセンス」に変更
  - ライセンスカウント方法自体は変更なし

NetApp	正常 ライセンス種別: NetApp (カテゴリー S) 保守期限:2020/01/31 サーバライセンス: 5 (保有数) 論理サーバライセンス: 0/5 (消費数/保有数)	→	NetApp 正常 ライセンス種別: NetApp (カテゴリー S) 保守期限:2020/01/31 物理サーバライセンス: 5 (保有数) 論理サーバライセンス: 0/5 (消費数/保有数)

■操作種別の変更

ログの種類	出力内容（操作）
ファイルアクセスログ	READ
	READ-Failure
	WRITE
	WRITE-Failure
	DELETE
	DELETE-Failure
	RENAME
	MOVE
アクセス権変更ログ	P-ACCESS

新規で追加

■詳細キーの変更

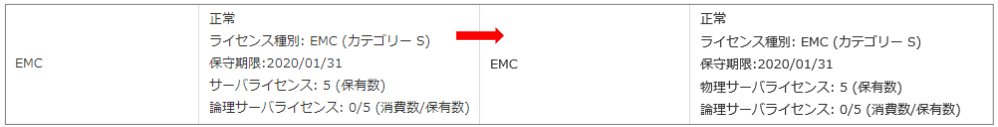
ログの種類	詳細項目
すべてのログ	Count / ClientIP
ファイルアクセスログ	To(RenameTo)

「RenameTo」を「To」に変更
MOVE時にも出力される(※)

※V7の「RenameTo」で出力されたアクセスログをインポートした場合、詳細項目にRenameToが出力されます。

3-3. for EMCの変更点

- **変換エンジンの変更なし（EMCではCOPY/MOVEは出ない）**
- **監査ポリシー、フォルダーの監査設定ともに変更なし**
- **変換に使用するEventIDに変更なし**
- **ライセンス表記を変更**
  - 「サーバライセンス」を「物理サーバライセンス」に変更
  - ライセンスカウント方法自体は変更なし



■操作種別

ログの種類	出力内容（操作）
ファイルアクセスログ	READ
	READ-Failure
	WRITE
	WRITE-Failure
	DELETE
	DELETE-Failure
	RENAME
	RENAME-Failure
アクセス権変更ログ	P-ACCESS
	P-ACCESS-Failure

変更なし

■詳細キー

ログの種類	詳細項目
すべてのログ	Count / ClientIP / ClientName

変更なし

3-4. for PowerScaleの変更点 （1/3）

- **製品の名称変更に伴いALog製品内での表記を変更 Isilon⇒PowerScale**
- **変換エンジンの刷新**
  - 精度の高い変換を行なうため、新変換エンジンを開発
  - 変換エンジンが変わっているため出力が変更されている
    ※詳細は、「 ALogV8説明資料_ファイルアクセスログ編」参照
  - 変換に使用するイベントを変更（closeイベントの使用を廃止）
    - 監査設定は変更の必要あり
  - MOVEは可能な限り出力できるよう対応
  - 不要なREADの削減（READ出力する判定を変更）
- **SID情報を取得する機能をPowerScaleの収集タスクから分離、AD情報取得タスクへ独立**
  - マネージャーサーバ経由のSID情報取得は「AD連携画面」＆「AD情報取得タスク」へ
  - PowerScale経由のSID情報取得の設定は今まで通りPowerScaleの対象サーバ編集画面にあり
    - PowerScale経由のSID情報取得の際、ゾーン指定が可能に
- **コンピューターアカウントはデフォルトで非表示に**
  - オプションで解除可能
- **初期の除外フィルターを設定**
  - Officeの「~$」を含むファイル、Officeの「.tmp」ファイルを除外

3-4. for PowerScaleの変更点 （2/3）

- **ライセンスカウント方法を変更**
  - V7ではノードを接続した際に作成されるフォルダー数をノード数としてカウントしていた
  - V8ではクラスタに含まれているノード数をライセンスとしてカウントする
- **ライセンス表記を変更**
  - 「サーバライセンス」の表示を削除、「ノードライセンス」の表示のみに

現在はPowerScale表記です

■操作種別の変更

ログの種類	出力内容（操作）
ファイルアクセスログ	READ
	READ-Failure
	WRITE
	WRITE-Failure
	DELETE
	DELETE-Failure
	RENAME
	RENAME-Failure
	MOVE
アクセス権変更ログ	P-ACCESS
	P-ACCESS-Failure

新規で追加

■詳細キーの変更

ログの種類	詳細項目
すべてのログ	Count / ClientIP / Protocol / To / Zone

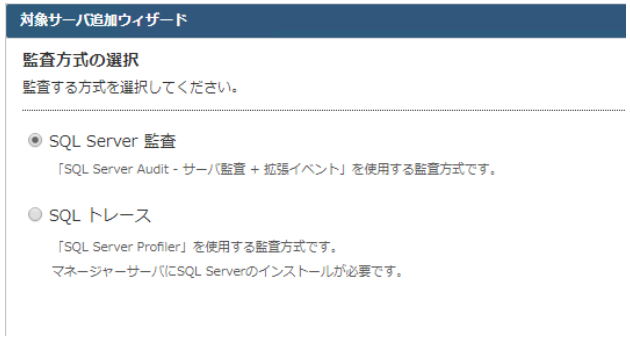
- 「Protocol」…新規追加。変換エンジンはCIFS領域用だが、NFS領域のログも変換する。
  NFS領域のログを変換したときにProtocolの項目にNFSと出力される。
- 「To」…名前変更や移動時に変更先のパスが出力される。RENAME/MOVE時に出力される。
- 「Zone」…アクセスゾーン名が出力される。

3-4. for PowerScaleの変更点 （3/3）

- **公開鍵認証を使用したSSH接続に対応**
- **「ユーザー」欄の形式指定オプション「UserNameFormat」の廃止**
  - 「ユーザー」欄の出力形式はV7では2種類存在していた
    ①UserPrincipalNameを利用したユーザー名(順番変更アリ)　　…例：ABC.co.jp¥ユーザー名
    ②NetBIOSドメイン名＋sAMAccountNameのユーザー名　　…例：ABC¥ユーザー名
    ※V7.1.3では②の出力形式をメインにしましたが、V7.1.3未満を利用中のユーザー向けに①の仕様も生かしていました。
    ReadmeV7.13 「- [Isilon] 新規インストールの場合、ユーザー名をuserprincipalnameではなく、NetBIOSドメイン名＋sAMAccountName　の組み合わせで変換するよう仕様変更」
  - V8では「ユーザー」欄は「②NetBIOSドメイン名＋sAMAccountNameのユーザー名」固定
  - 影響があるのは①の形式で出力していた場合

3-5. for SQL Serverの変更点 （1/4）

- **SQLの監査に利用する方式を変更**
  - これまで使用していた監査方式は「トレースの監査」（SQL Server Profiler）。この監査方式はMicrosoft側で途中から非推奨となっており、いつ廃止されるか不明な状態であった。ALogとしてはいつか他の方式にする必要があったが、取得するログが変わると影響があるため簡単には出来なかった。
  - V8では新たに「SQL Server監査」(RAWSQL以外)と「拡張イベント」(RAWSQL)を監査方式として採用。
    - 取得するログの拡張子やフォルダー名等変更あり
  - 対象サーバ追加時に、V7までの監査方式とV8で新対応した監査方式を選択できる
  - SQL Server Auditを使用する方式ではSQL Server側の都合で2012～2016ではアプリケーション名（AppName）が出力されていないため、SQL Server 2017以降にするのがベスト
    - 詳細については後述
  - ベストエフォートとしたSQL Server 2008/R2はeditionにより上記方式に対応していない、且つ対応しているeditionでも監査の範囲やフィルター機能が実装されたばかりのバージョンのため制限が多い。そのため、元のSQL Server Profiler方式で取得する



3-5. for SQL Serverの変更点 （2/4）

- **SQL Server監査使用時、マネージャーサーバ内の作業用DBを廃止**
  - 導入が簡単に（ライセンスも不要に）

	監査方法	作業用DBの要否	
2008/R2	SQL Server Profiler（.trc）	必要	ベストエフォート
2012～2016	SQL Server Audit（.sqlaudit）＋ 拡張イベント（.xel）	不要	SQL監査の仕様により アプリケーション名に制約あり
2017～	SQL Server Audit（.sqlaudit）＋ 拡張イベント（.xel）	不要	アプリケーション名に制約なし

- **ライセンス形態の変更**
  - 追加インスタンスライセンスを廃止　※ 詳細は「ライセンス定義書」をご確認ください
  - V7時に発行されたライセンスは使用可能
- **ライセンス表記を変更**
  - 「サーバライセンス」の表示を削除し、「インスタンスライセンス」を「データベースライセンス」に変更

3-5. for SQL Serverの変更点 （3/4）

■操作種別

ログの種類	出力内容（操作）
DBアクセスログ	DB_SELECT
	DB_SELECT-Failure
	DB_INSERT
	DB_INSERT-Failure
	DB_DELETE
	DB_DELETE-Failure
	DB_UPDATE
	DB_UPDATE-Failure

ログの種類	出力内容（操作）
DBログオン/ログオフログ	DB_LOGON
	DB_LOGON-Failure
	DB_LOGOFF
DB管理者操作ログ	DB_ADMIN
	DB_ADMIN-Failure
RAWSQLログ	DB_RAWSQL
	DB_RAWSQL-Failure

変更なし

■詳細キー

ログの種類	詳細項目
すべてのログ	Count / AppName / DB
RAWSQLログ以外	ClientIP
RAWSQLログ	ClientName / RowCounts

- **SQL Server監査使用時の出力に関する変更（3点）**

①RAWSQL以外でアプリケーション名「AppName」が出力されない（SQL Server 2012～2016のみ）

SQL Serverが2012～2016の場合、元のログにアプリケーション名が出力されないため。

■アクセスログ例

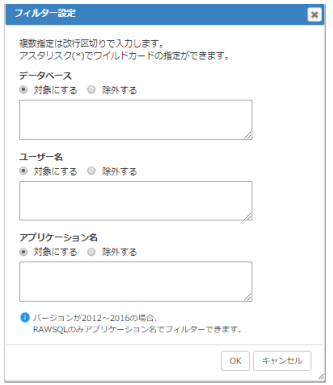
V7の出力結果：詳細欄

AppName:Microsoft SQL Server Management Studio ClientName:12R2-SQL12 Count:1 DB:master

V8(2012～2016)の出力結果：詳細欄

ClientName:12R2-SQL12¥WS2016K01 Count:1 DB:master RowCounts:0

※これにより、フィルター設定画面の「アプリケーション名」欄も2012～2016の場合機能しません。
SQL Server 2017からアプリケーション名を出力するように改善されているため、バージョンアップを推奨します。
※RAWSQLに使用している「拡張イベント」には2012～2016間もアプリケーション名が出力されています。
そのためアクセスログにアプリケーション名を出力すること、フィルター設定で除外すること、共に可能です。



3-5. for SQL Serverの変更点 （4/4）

②細かな文言の差異

新しい監査方式で使用している「SQL Server Audit」では今までより詳細な情報が付与されています。
その結果、以下の例のような細かな文言の差異があります。

V7の出力結果：対象欄
データベースがバックアップされました
V8の出力結果：対象欄
データベース**[ALogDB]**がバックアップされました

③SQL Serverの内部操作と思われるログの出力の差異

V7では『実際にクエリを実行した際のログ』の他、DB内部に関する監査ログが出力されていました。
この内部操作と思われるログの出力が、監査方式の変更により変わっています。
（出力されていたものが出力されない、出力されていなかったものが出力される、双方のケースがありえます）

3-6. for Oracleの変更点

- **統合監査対応（Oracle12c以降から使用可能）**
  - 統合監査方式にも対応したが、標準監査も引き続き使用可能
- **マネージャーサーバへのOracle Client導入を不要化（導入が簡単に）**
- **ライセンス形態の変更**
  - 追加インスタンスライセンスを廃止し、データベース数のみでライセンスカウントを行なうよう変更
  - V7時に発行されたライセンスは使用可能
- **ライセンス表記を変更**
  - 「サーバライセンス」の表示を削除、「インスタンスライセンス」を「データベースライセンス」に変更

■操作種別

ログの種類	出力内容（操作）
DBアクセスログ	DB_SELECT
	DB_SELECT-Failure
	DB_INSERT
	DB_INSERT-Failure
	DB_DELETE
	DB_DELETE-Failure
	DB_UPDATE
	DB_UPDATE-Failure

ログの種類	出力内容（操作）
DBログオン/ログオフログ	DB_LOGON
	DB_LOGON-Failure
	DB_LOGOFF
DB管理者操作ログ	DB_ADMIN
	DB_ADMIN-Failure
SYSDBAログ	DB_SYSDBA
RAWSQLログ	DB_RAWSQL
	DB_RAWSQL-Failure

変更なし

■詳細キー

ログの種類	詳細項目
すべてのログ	Count / ClientName / AppName / Schema
	SesId / OSUser / DBID
DBログオンログ	Count / ClientIP / ClientName / AppName / Schema / SesId / OSUser / DBID

変更なし

3-7. for Linuxの変更点

- **他製品との統一性のため5秒マージの規則を変更**
  5秒以内であっても間に同じファイルに対する別の操作が含まれていればマージされないように変更
- **Syslogの変換タスクでのパフォーマンス向上**
- **公開鍵認証を使用したSSH接続に対応**
- **アクセスログ出力結果の変更点　詳細項目「RenameTo」が「To」に変更**

V7の詳細項目

“AppName:/usr/bin/mv ClientIP:10.255.101.254 ClientName:RHEL74 Count:1 RenameTo:/home/amiya/renameFileA.csv Tty:pts0“

V8の詳細項目

“AppName:/usr/bin/mv ClientIP:10.255.101.254 ClientName:RHEL74 Count:1 To:/home/amiya/renameFileA.csv Tty:pts0"

「RenameTo」を「To」に変更
他製品との統一性のため(※)

■操作種別

ログの種類	出力内容（操作）
ファイルアクセスログ	READ
	READ-Failure
	WRITE
	WRITE-Failure
	DELETE
	DELETE-Failure
	RENAME
	RENAME-Failure

ログの種類	出力内容（操作）
アクセス権変更ログ	P-ACCESS
	P-ACCESS-Failure
コマンド実行ログ	EXEC
	EXEC-Failure
ログオン/ログオフログ	LOGON
	LOGON-Failure
	LOGOFF
syslog	SYSLOG

変更なし

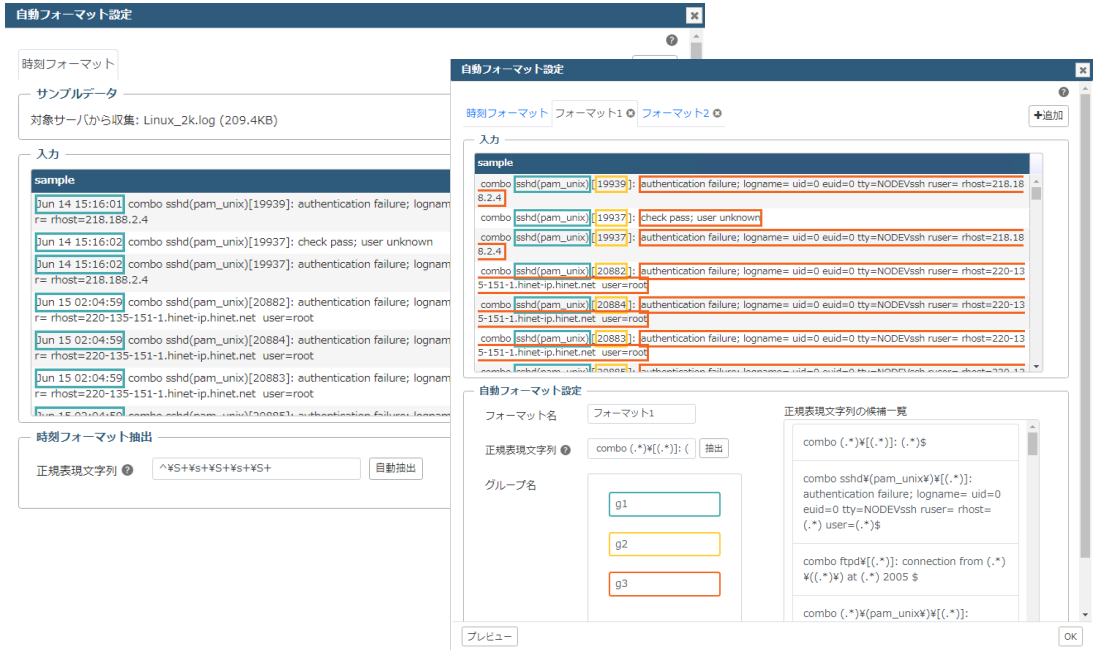
■詳細キーの変更

ログの種類	詳細項目
すべてのログ	Count
ファイルアクセスログ	AppName / AuditUser / ClientIP / ClientName / ErrorCause / To(RenameTo) / Tty
アクセス権変更ログ	AppName / AuditUser / ClientIP / ClientName / ErrorCause / Tty
コマンド実行ログ	AppName / AuditUser / ClientIP / ClientName / ErrorCause / CurrentDir / Tty
ログオンログオフログ	AppName / AuditUser / ClientIP / ClientName / ErrorCause

※V7で「RenameTo」で出力されたアクセスログをインポートした場合、
詳細項目にRenameToが出力されます。

3-8. for ALog EVAの変更点 （1/2）

- **サンプルデータから自動でフォーマットを判定し、各カラムを抽出するための正規表現文字列を提案する機能を追加**
  - 自分で正規表現を書くことが難しい場合にもALogが自動で提案するため、簡単に設定できる
  - 1つのサンプルデータに複数のフォーマットが存在するケースも対応可能に

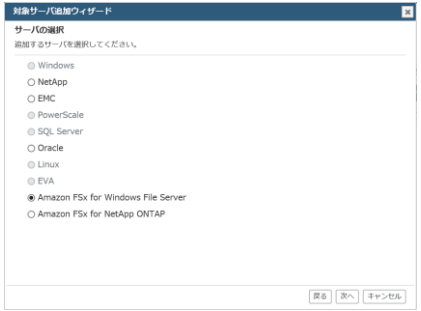


3-8. for ALog EVAの変更点 （2/2）

- **標準テンプレートの一部を削除**
  - 削除した標準テンプレートはサポートサイトでの配布に切り替え
  - 削除対象は3点 「Webサーバ(IIS7)」「Webサーバ(IIS8)」「NetApp (NFSv4)」
- **「Apache」用の標準テンプレートを変更**
  - Commonだけでなくcombinedのログにも簡単に対応できるようにするため
- **詳細キーの別名対応、グループ化対応（横串検索可能に）**
  - 複数の詳細キーをグループ化し、まとめて検索可能に
    - 詳細は「ユーザーガイド」参照
- **詳細キーのタイプ設定対応**
  - 文字列型以外に、数値型、時刻型、日付型で検索可能に
    - 詳細は「ユーザーガイド」参照
- **SCP接続して収集時に公開鍵認証を使用したSSH接続に対応**
- **ALog Syslog Receiverを提供**
  - ALog Syslog Receiverを別途インストールすることで、Syslog形式のログを直接受信可能に
  - 詳細はALog Syslog Receiver ユーザーガイド参照
- **入力マッピング設定に空のフィールドを除外するオプションを追加**
  - マッピング入力設定においてCSV/TSV/DSVファイル形式の場合、「空のフィールドを除外」を選択することで、分割したフィールドの内容を評価し、その内容が空だった場合に除外される。

3-9. Amazon FSx for Windows File Server を対応製品に追加

- **V8.4.0より製品群に新規追加**
- **ファイルアクセスしたログが「オブジェクトアクセス」として出力**
  - 書き込み、削除などのファイルアクセス時の操作が全て操作欄に「ObjectAccess」として出力
  - ファイルアクセスに失敗時は「ObjectAccess-Failure」として出力



■動作条件

1. Amazon Kinesis Data Firehoseに監査イベントログ出力用の配信ストリームが作成済みであること
2. Amazon FSx for Windows File Serverの監査イベントログ出力先が1の配信ストリームに設定されていること
3. Amazon S3に監査ログ出力用のバケットが作成済みであること
4. 1の配信ストリームの出力先が3のバケットに設定されていること

■操作種別

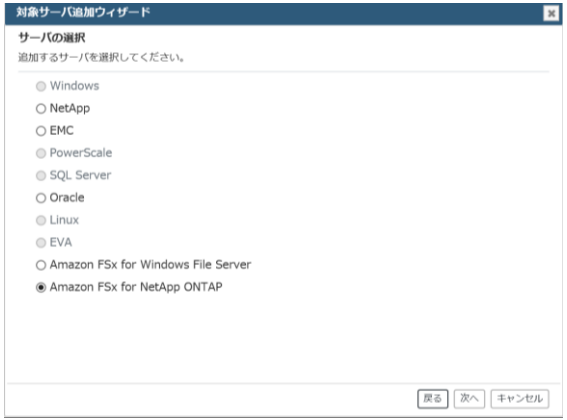
ログの種類	出力内容（操作）
オブジェクトアクセス	ObjectAccess
	ObjectAccess-Failure

■詳細キー

ログの種類	詳細項目
すべてのログ	AccessList / AccessMask /Count

3-10. Amazon FSx for NetApp ONTAP を対応製品に追加

- **V8.5.0より製品群に新規追加**
- **for NetApp (ONTAP)と同じアクセスログを出力**



■動作条件

1.ファイルアクセスログの出力対象となるファイル領域がCIFS領域であること
（NFS領域には対応していません）

2.マネージャーサーバから対象サーバに対してsshコマンドが実行できること

3.ログのフォーマットがevtx形式であること(XML形式には対応していません)

4.ストレージ仮想マシンの設定を「Active Directoryへの参加」にしていること

■操作種別

ログの種類	出力内容（操作）
ファイルアクセスログ	READ
	READ-Failure
	WRITE
	WRITE-Failure
	DELETE
	DELETE-Failure
	RENAME
	MOVE
アクセス権変更ログ	P-ACCESS

■詳細キー

ログの種類	詳細項目
すべてのログ	Count / ClientIP
ファイルアクセスログ	To(RenameTo)

4. 機能追加/仕様変更 （1/2）

ALogの各機能に対し、機能追加や仕様変更があります。

ホーム	ユーザーがカスタマイズできる機能を追加
検索	検索ボックスを追加し、全カラム検索も可能に
	検索結果のハイライト機能を追加
	検索結果表示時に最新のログ情報を表示（検索結果のソート順初期値が降順）
	秒指定の検索、時間帯の絞り込み検索が可能に
	UIをレポート画面と共通化し、明示的な除外指定欄を追加 これにより、将来的には「-」による除外指定を廃止予定（V8時点では「詳細キーのグループ化」以外では使用可能）
	タブによる条件指定により複雑な検索を可能に
	時刻以外の列でソート可能に
	EVA用：表示項目の切り替えによる詳細項目名の「_」をカットしたCSVの出力に対応
	EVA用：詳細項目を別名にする、詳細項目をグループ化する機能を追加
	EVA用：詳細項目の検索タイプを変更する機能を追加
レポート	変換エンジンに合わせてCOPYとMOVEをテンプレートの初期選択に追加
	集計レポートと監視レポートの機能差を撤廃 アラート機能：監視レポートのみで使用できたが集計レポートでも使用可能に
	タブによる条件指定により複雑な検索を可能に
	「高度な設定」を新設 ・表示形式（ランキング形式/時系列形式）が選択可能に ・集計キー＆集計方法の設定を整理 ・明示的な「時系列形式」の選択可能化に伴い、テンプレート名の変更「総ファイルアクセス」→「時間別アクセス」
	詳細キーでのソート機能対応
	しきい値の仕様変更 ・「ユーザー毎でカウントする」項目を廃止 ・代わりに「高度な機能」にチェックをいれると「しきい値の詳細項目」が表示され、その中で同等の設定が可能に

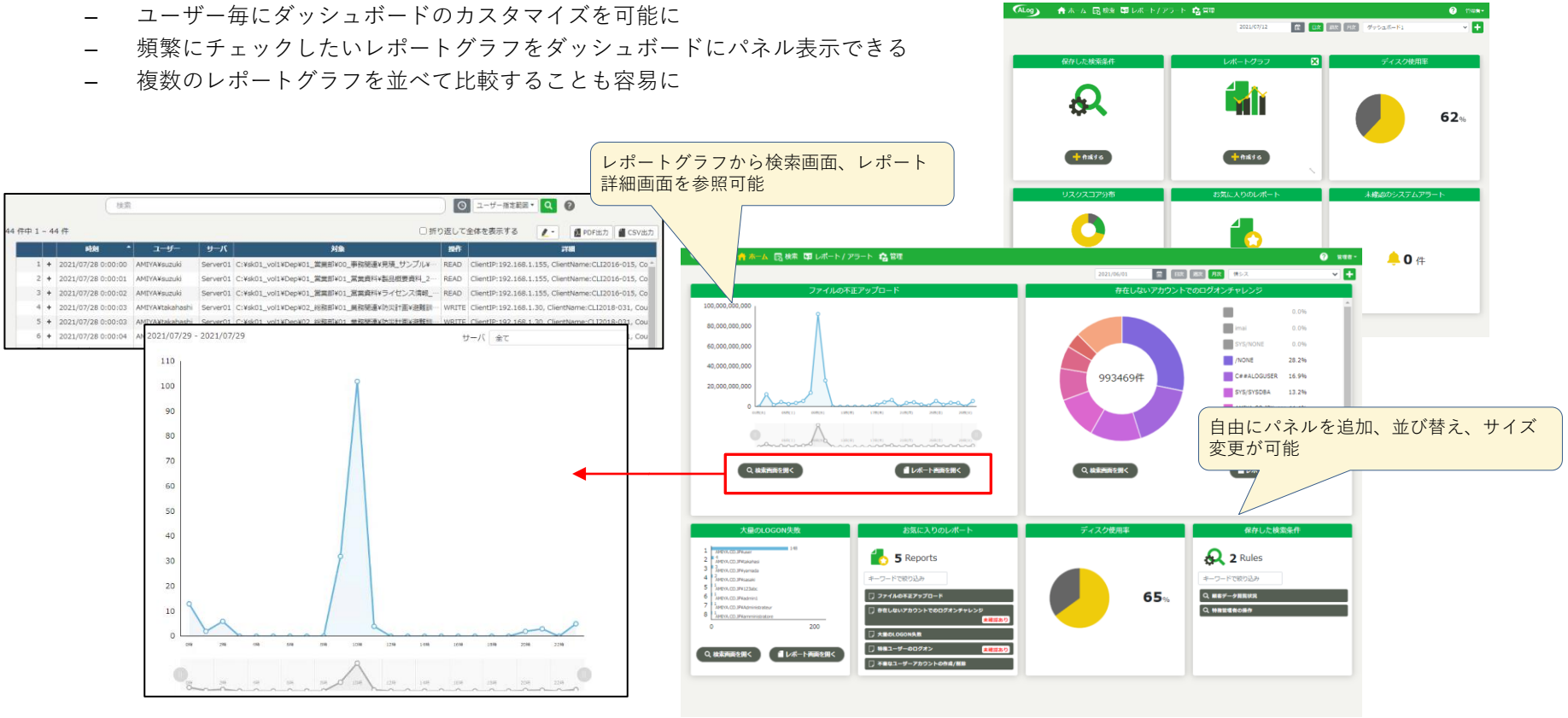
4. 機能追加/仕様変更 （2/2）

レポート	EVA用：詳細項目を別名にする、詳細項目をグループ化する機能を追加
	EVA用：詳細項目の検索タイプを変更する機能を追加
	レポートのテンプレート種類の追加
	アラート時に外部連携する機能を追加(syslog送信やプロセス起動が可能に)
管理	メール送信機能の強化（暗号化方式「SMTP over SSL」に対応）
	ALogの一時ファイル作成先として、常にALogのデータフォルダー配下が使用されるように変更
	イベントログバックアップ機能の強化（ (パスワード付) ZIPに対応）
	システムログのメール通知を複数設定できるように変更
	ALog Cloud連携機能を追加
AD連携機能強化	目的1：Windows/PowerScaleの変換エンジンでの変換時、ユーザー名の置換処理に利用する 目的2：WorkTime機能でアカウント名から氏名情報への置換処理に利用する 目的3：リスクスコアリング機能でアカウント名から氏名情報への置換処理に利用する 目的4：検索、レポートで表示名、グループ名で検索時に利用する
検索用DB	過去ログの高速インポートモードと検索/レポートタスク実行の排他処理を解除
その他	レポート共通設定の削除期間の初期値を3か月から1年に変更

各バージョンの機能詳細については、Readmeおよびユーザーガイドを参照してください。

4-1. ホーム画面の変更点（ダッシュボード）

- **ダッシュボード画面をリニューアル**
  - ユーザー毎にダッシュボードのカスタマイズを可能に
  - 頻繁にチェックしたいレポートグラフをダッシュボードにパネル表示できる
  - 複数のレポートグラフを並べて比較することも容易に



4-2. 検索/レポートの変更点 （1/6）

- **[検索] 直感的操作で使える検索ボックスの追加**
  - カラムを意識せずに検索ワードを入力するだけで検索が可能に
  - 「サーバ:localhost」のようにカラム名を指定して検索も可能
  - 検索結果からドリルダウンして簡単に絞り込みが可能に
  - 検索結果をハイライトして検索結果から見たい箇所を一目瞭然に

4-2. 検索/レポートの変更点 （2/6）

- **[検索/レポート]タブによる条件指定により複雑な検索を可能に**
  - フィルター項目間のAND/ORを複雑に組み合わせた検索を行ないたいと要望をいただいていたため、その要望に対応した機能です。
  - 指定画面が複雑になりすぎると使い難くなってしまうため、できる限り分かりやすく使っていただきたいと考えて「タブ」化しました。
    - 1つのタブで検索可能なことを複数タブを使って検索しようとする必要はありません。1つのタブで検索しきれない場合に複数タブでの検索をしてください。
  - タブ間をAND/OR指定可能、最大で5つのタブを追加可能

4-2. 検索/レポートの変更点 （3/6）

- **[レポート]集計レポートと監視レポートの機能差を撤廃**
- **[レポート]「高度な設定」を新設**

(2つまとめて説明)

– V7.4.0でレポートの高機能化と集計/監視レポートの画面統一を行なってきましたが、V8.0.0で集計/監視レポートの機能差を撤廃しました。
– 複雑なレポート設定をしたいという要望がある一方で、簡単にレポートを使いたいユーザーの操作性の維持も必要なため、「高度な設定」を用意し、必要なユーザーのみが複雑な設定をするような画面としました。
– アラート機能：監視レポートからのみ → 集計レポートでも可能に
– 一部のレポートテンプレートを選択したときにしか設定できなかった「集計キー」はどのテンプレートからでも設定可能に
(「高度な設定」内に配置)
– 「総ファイルアクセス」のテンプレート名を「時間別アクセス」に変更
– 「高度な設定」内に「表示形式」を新設。これにより今まで「総ファイルアクセス」テンプレートでしかできなかった「時系列」形式のレポートを自由に作成可能に。
– レポート結果の表示も読みやすくなるよう調整

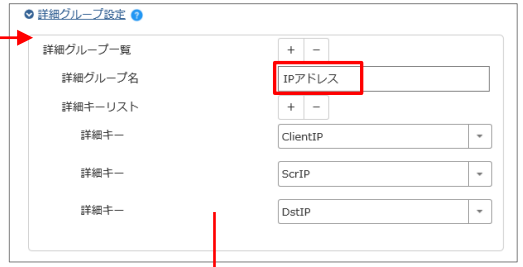
4-2. 検索/レポートの変更点 （4/6）

- **[検索/レポート]詳細項目を別名にする、詳細項目をグループ化する機能を追加**
  - 管理-詳細設定内に「詳細グループ設定」機能を新設
  - 同じ意味を持つ詳細項目が複数作成されてしまっている環境において、複数の詳細を横串で検索したい場合等に使用
    （本来であれば同じ意味を持つものは同じ項目にマッピングされるのが最も望ましい形です）

別の詳細項目だがどれもIPアドレスを示すものである

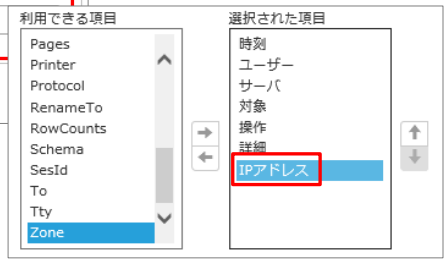
これらをグループとして登録する

ClientIP	SrcIP	DstIP	IPアドレス(グループ)
10.255.255.1			ClientIP:10.255.255.1
	10.255.255.2	10.255.255.3	SrcIP:10.255.255.2,DstIP:10.255.255.3
	10.255.255.1	10.255.255.3	SrcIP:10.255.255.1,DstIP:10.255.255.3



IPアドレスの検索で
「10.255.255.1」を検索すると

詳細グループを作成すると、
フィルター追加や表示項目の
選択肢に表示されるようになる



ClientIP	SrcIP	DstIP	IPアドレス(グループ)
10.255.255.1			ClientIP:10.255.255.1
	10.255.255.2	10.255.255.3	SrcIP:10.255.255.2,DstIP:10.255.255.3
	10.255.255.1	10.255.255.3	SrcIP:10.255.255.1,DstIP:10.255.255.3

ClientIP、SrcIP、DstIPという異なる詳細項目に対して「10.255.255.1」を検索し、ヒットしたものが検査結果になる

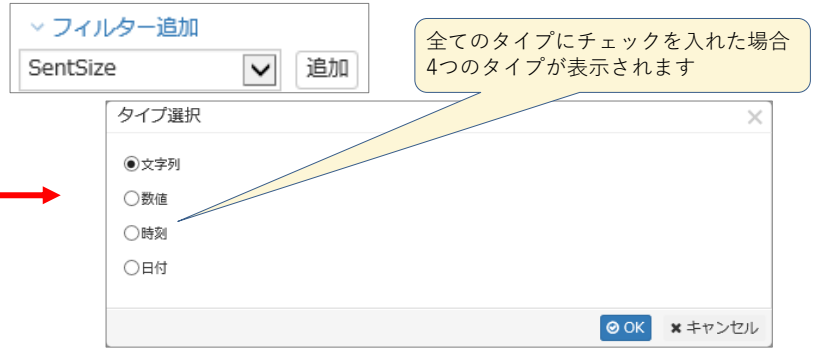
ALog EVAをご利用のユーザーで使用する機会を想定して実装した機能ですがその他製品をご利用の場合も機能を使うことが可能です。機能詳細はユーザーガイドに記載されています。

4-2. 検索/レポートの変更点（5/6）

- **[検索/レポート]詳細項目の検索タイプを変更する機能を追加**
  - 管理-詳細設定内に「詳細キータイプ設定」機能を新設
  - EVAのマッピングによって定義された詳細項目は、すべて文字列型(タイプ)でしか検索ができませんでした。
  - 数値や日付として検索したいという要望があるためこれに対応しています。
  - 本機能が動作するためには条件があるためユーザーガイドを参照してください。

文字列以外のタイプで検索したい詳細キーを指定し、使いたいタイプにチェックをいれます。

検索やレポート画面で詳細キーを選択すると、どのタイプで検索するかの選択肢が表示されます。
最初の設定でチェックをいれたタイプが選択肢になります。



ALog EVAのライセンスを適用した環境でのみ使用できる機能です。
機能詳細はユーザーガイドに記載されています。

4-2. 検索/レポートの変更点（6/6）

- **[レポート]レポートのテンプレート種類を追加**
  - [基本監査パック]タブにはADサーバ/ファイルサーバ/DBなど、用途に合わせた具体的な監査を想定しテンプレート化しました。
  - [サイバー攻撃自動検知パック][Microsoft 365 パック]タブ用のテンプレートは必要に応じて使えるようサポートサイトからダウンロードしたテンプレートをインポートする仕組みとなっています。

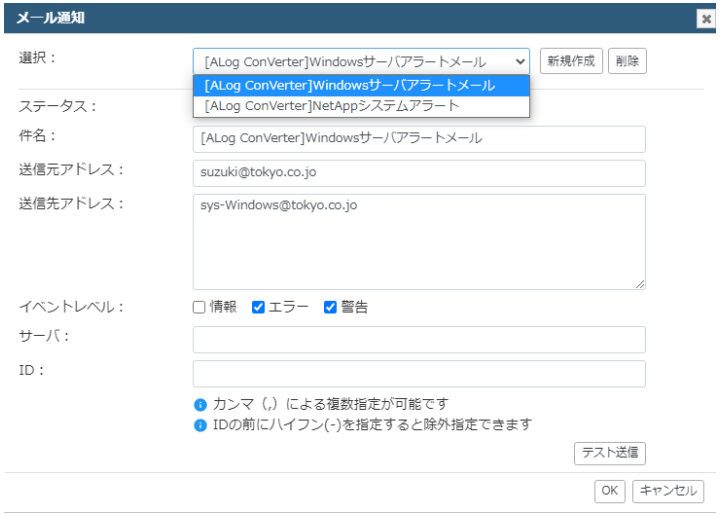
- **[レポート]アラート時の外部連携機能を追加**
  - アラートの設定において外部連携を設定できます
  - アラート検知時、Syslog送信やプロセス起動をする設定ができます

4-3. 管理機能の変更点（1/2）

- **メール送信機能強化**
  - 暗号化方式に「SMTP over SSL」を追加
  - より多くの認証方式に対応

4-3. 管理機能の変更点（2/2）

- **イベントログバックアップ機能の強化**
  - イベントログバックアップの保存形式にパスワード付(ZIP)を追加
- **システムログのメール通知を複数設定できるように変更**
  - システムログ発生時のメール通知が複数設定できるように変更



4-4. AD連携機能強化

これまでのALogでは、ActiveDirectoryから情報を取得するのは、for PowerScaleのみでした。
今回V8では、その処理をPowerScaleの収集タスクから分離し、「AD情報取得タスク」として独立させることで、取得したAD情報を他のALog製品でも利用できるようにしました。

- **アクセスログへの変換時に「ユーザー名」を置換**
  - for Windows
    - イベントログに含まれるSIDとADのユーザーオブジェクトのSIDを紐づけ、 AD上のユーザーログオン名に置換
  - for PowerScale
    - 収集タスクから分離することで、AD情報の取得に時間がかかる環境で収集タスクが影響を受けていた問題を解消
    - 従来どおり、監査ログのSIDを置換
- **検索/レポートでAD情報を利用**
  - ADに登録された表示名で検索可能に
  - AD情報を利用してグループを作成しておくと、グループでの検索も可能に
- **WorkTime機能でユーザー名の置換やグループ化に利用**
  - AD情報を使用して、氏名（漢字）で勤怠情報を確認可能に
  - AD情報の組織構造（OU）や部署情報をもとにグループ化、グループ化した状態でWorkTime情報を閲覧可能に
- **リスクスコアリング機能でユーザー名の置換や、写真を利用**
  - ADのユーザーオブジェクトに登録された属性や画像を利用してリスクスコアリング解析結果画面にユーザー情報として表示

4-5. ALog Cloud連携機能追加

- **ALog Cloud連携機能を新設**
  - アクセスログをALog Cloudへ連携する機能を新設
  - V8で変換したアクセスログをALog Cloudへアップロードし、ALog Cloud側で参照できます
  - 連携するには、ALog Cloudで発行したクレデンシャルファイルを参照し、アクティベーションする必要があります

詳細はALog Cloudユーザーガイドに記載されています。