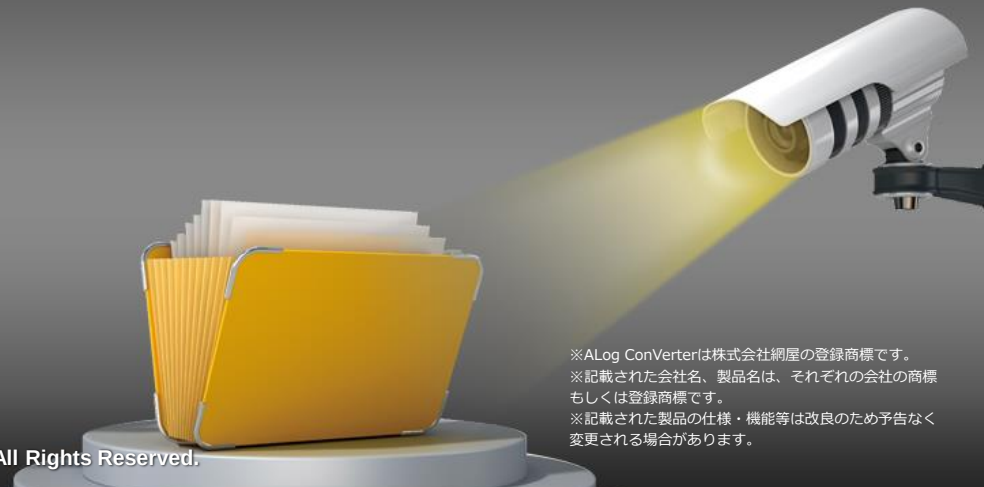
AMIYA

ALog

データベースサーバログ

ALog ConVerter® DB

for SQL Server／Oracle



※ALog ConVerterは株式会社網屋の登録商標です。
※記載された会社名、製品名は、それぞれの会社の商標もしくは登録商標です。
※記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。

ver. 7.3.0_3

ALogシリーズ

ALog ConVerter

サーバアクセスをOSレイヤから取得
複数サーバから統合的にログ管理を実現

エンタープライズ型

SMASH

専用サーバ不要＆簡単インストール
スタンドアロン型サーバログ

スタンドアロン型

ALog ConVerter DB

データベースアプリレイヤから取得
分散するDBログを一元的に保管

Resource Athlete

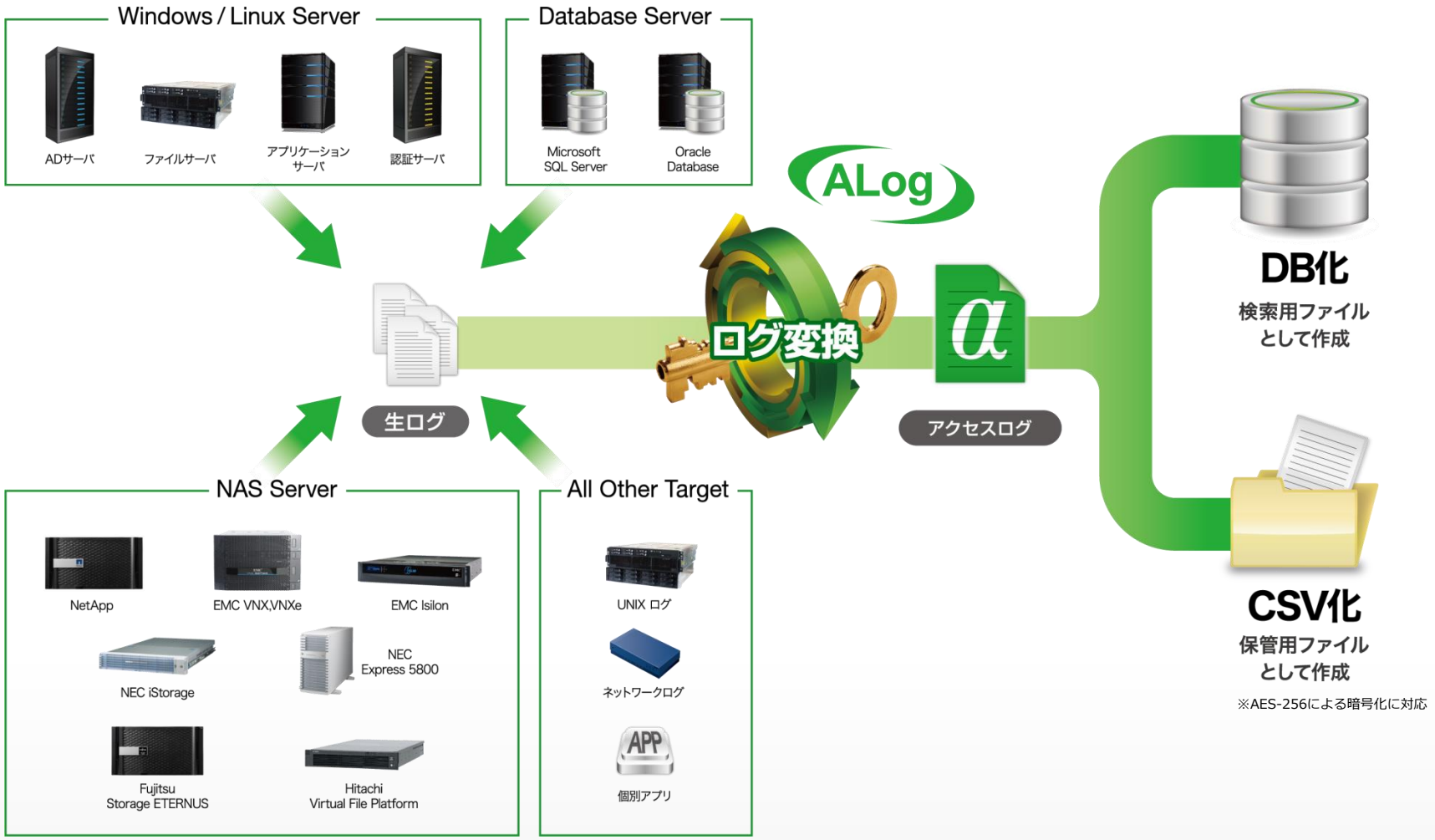
フォルダのアクセス権情報や
不要ファイルの洗い出しなど
マルチなサーバマネジメントツール

ALog ConVerter Any

様々なログをまとめて集約
障害ログなども統合して複合管理

ALogの守備範囲

Windowsに留まらず、Linux/NAS storageのサーバOSログやデータベースアプリケーションログ、ネットワークからのsyslog等、 ALogシリーズは広範囲のログを網羅します。

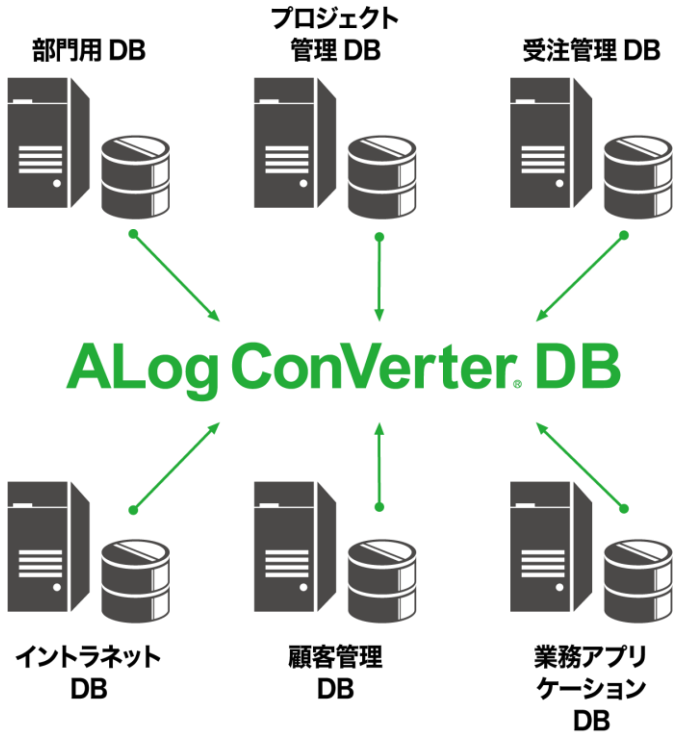


ALog DBの*Stylish* その1

ALog DBは、点在するデータベースのアクセスログを集中管理します。
マネージャーサーバ内でログを自動圧縮し、大量ログデータを長期間安全に保管します。

ログを集中管理

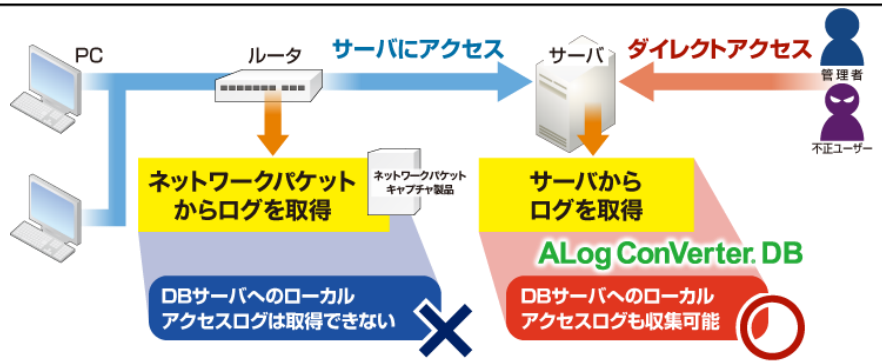
分散するデータベース環境において、それぞれからログを取得して
長期間保管し続けることは非常に面倒な運用管理方法です。
ALogでログを集約し、一元的なログの保管/監視体制を実現して下さい。



分かりやすく小さく

複雑なデータベースのログを解析処理し、分かりやすいログにまとめます。
その後自動圧縮機能にてログを小さくしてから継続保管します。

ローカルアクセスも

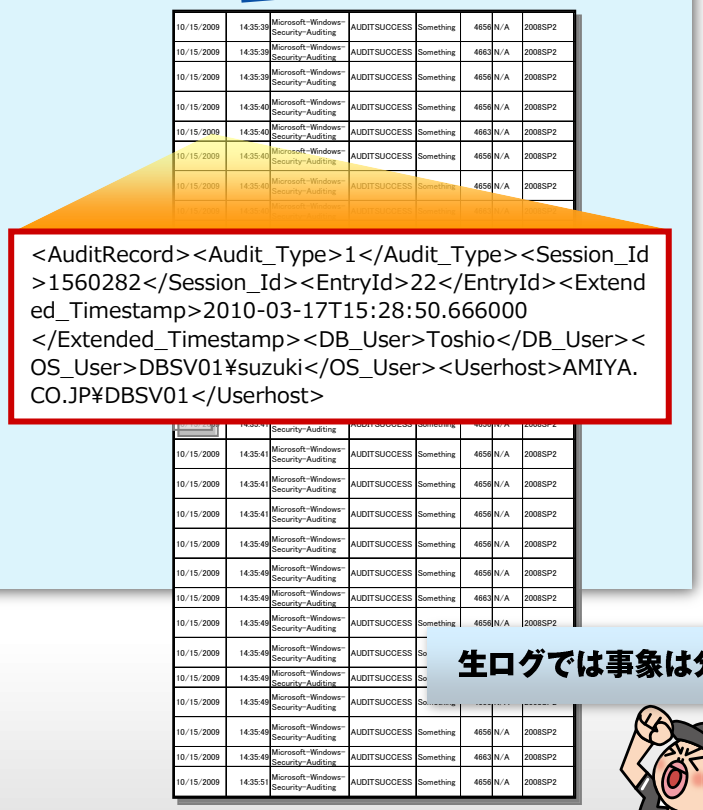


ネットワークパケット型だとデータベースに直接アクセスした記録が取得できません。
ALog ConVerter DB は、サーバのログを取得するのでダイレクトアクセスも取得できます。

ALog DBの*Stylish* その2

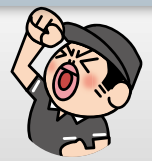
例：社員としおが、会計DBにログオンし、masterテーブルを参照した
ログは『LOGON』と『SELECT』と出てほしい

生ログだと…



<AuditRecord><Audit_Type>1</Audit_Type><Session_Id>1560282</Session_Id><EntryId>22</EntryId><Extended_Timestamp>2010-03-17T15:28:50.666000</Extended_Timestamp><DB_User>Toshio</DB_User><OS_User>DBSV01¥suzuki</OS_User><Userhost>AMIYA.CO.JP¥DBSV01</Userhost>

生ログでは事象は分からず、、



ALog

ユーザ	対象	操作	詳細
Toshio_01	ユーザーがログオンしました	DB_LOGON	・・・・・・・・・・ ・・・・・・ Count:1　DB:会計DB
Toshio_01	master テーブルのデータが参照されました	DB_SELECT	・・・・・・・・・・ ・・・・・・ Count:1　DB:会計DB

Toshioが 会計DBに『ログオンして』 『参照した。』

分析して実操作に変換

ログの種類

アクセスログ

テーブルに対しての読み取りや更新などの操作を記録

時刻	ユーザー	サーバ	対象	操作	詳細
2015/7/23 20:03:32	Domain¥Kawasaki	DC001¥ins01	テーブル「t_user」のデータが参照されました。	DB_SELECT	AppName:Microsoft SQL Server Management Studio - クエリ ClientName:pc01

DBログオン・ログオフログ

ユーザーがいつDBログオン/ログオフしたかを記録

時刻	ユーザー	サーバ	対象	操作	詳細
2015/7/23 20:01:00	Domain¥Kawasaki	DC001¥ins01	pc1	DB_LOGON	AppName:Microsoft SQL Server Management Studio ・・・・・

管理者操作ログ

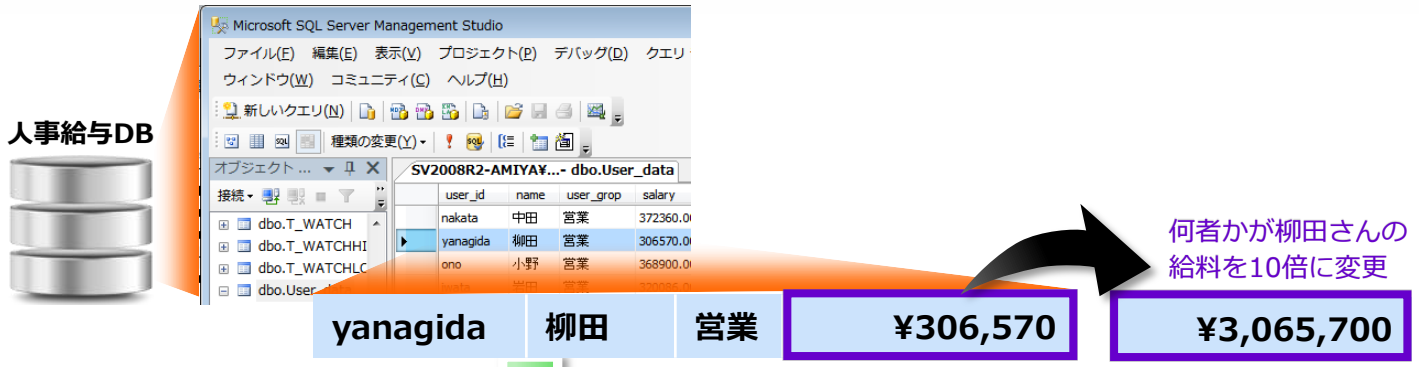
ユーザーの追加/削除やテーブルの変更など、DBの運用管理者が行う操作を記録

時刻	ユーザー	サーバ	対象	操作	詳細
2015/8/15 21:00:00	Domain¥Superman	DC011¥DB53	テーブル「t_user」が作成されました。	DB_ADMIN	AppName:OSQL-32 ClientName:pc01 Count:1　DB:master

※for OracleはSYSDBAユーザーの操作ログも取得可能

記録がなければあとで何も分からない

ケース１　何者かに給与額が改ざんされた



ALog DBで、ユーザー特定から操作内容まで把握

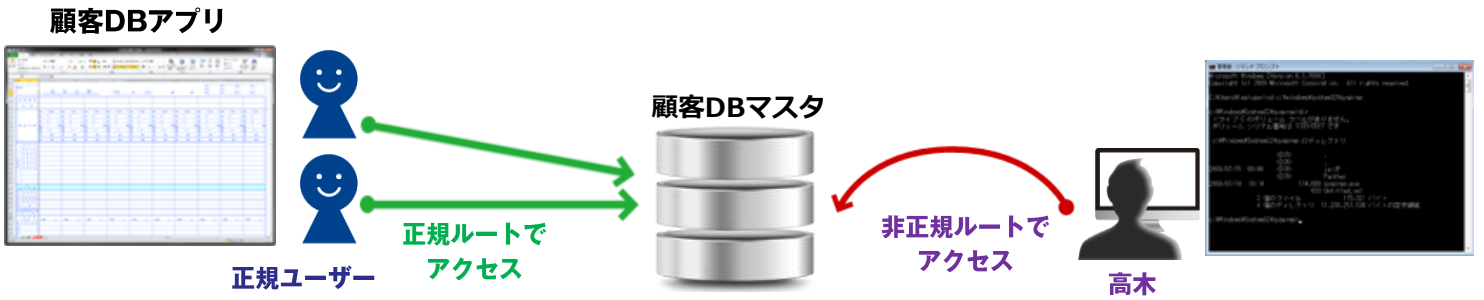
金子が

時刻	ユーザ	対象	操作	詳細
2014/3/15 22:15	Kaneko	人事給与DB テーブル[給与額]のデータが更新されました	DB_UPDATE	AppName:Microsoft SQL Server Management Studio ClientName:JINJI-PC
2014/3/15 22:15	Kaneko	UPDATE 給与額 SET salary WHERE @salary=3,065,700	DB_RAWSQL	・・・・・・・・・・・・・・・・・・・・

給与額を306万円に変更

記録がなければあとで何も分からない

ケース2　何者かに非正規なルートから顧客DBを持ち出された



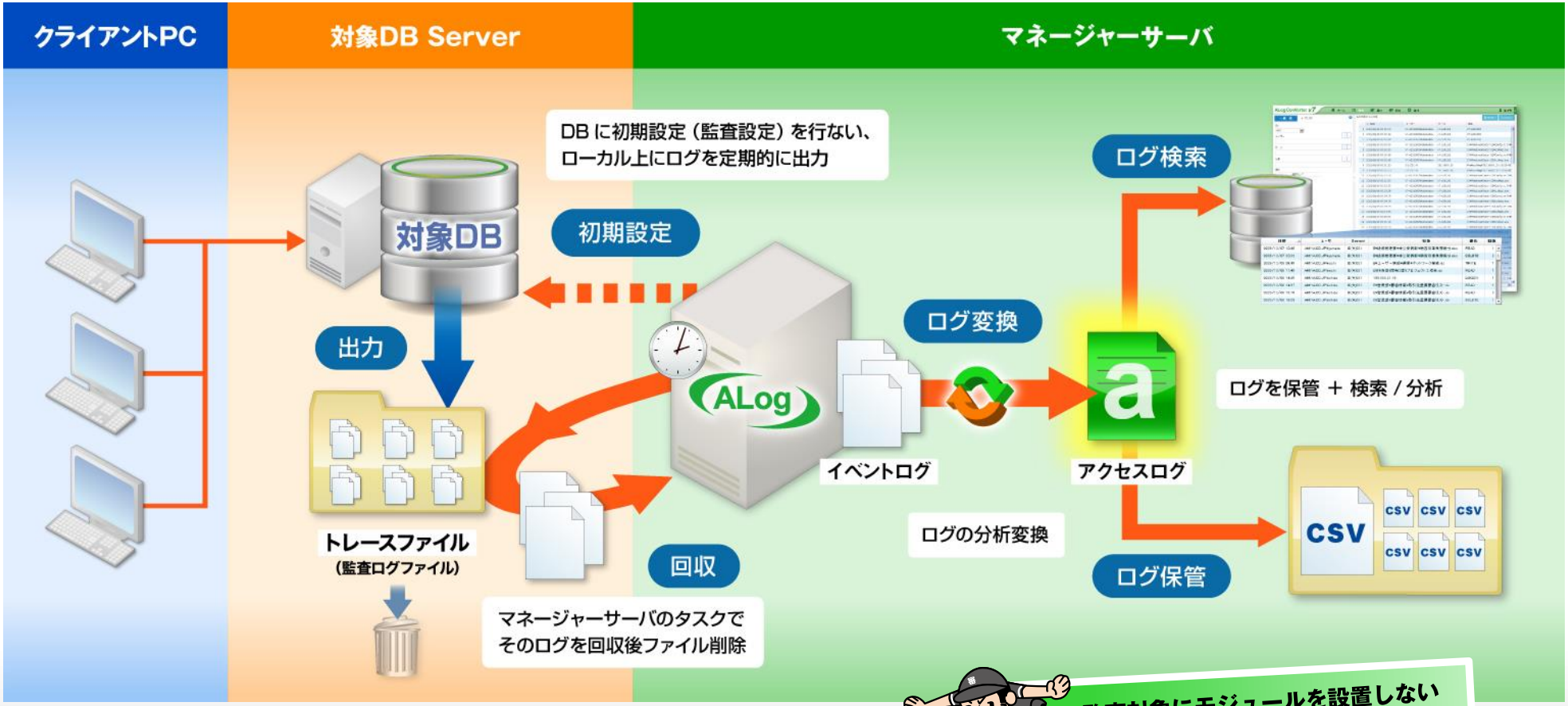
ALog DBで、非正規アクセスのみを記録

高木が

別アプリからDBアクセス

時刻	ユーザ	対象	操作	詳細
2015/7/7 18:02	Takagi	テーブル[会員登録情報]のデータが参照されました	DB_SELECT	AppName: Microsoft SQL Server Management Studio - クエリ ClientName:　Takagi-PC
2015/7/7 18:02	Takagi	SELECT * FROM 会員登録情報	DB_RAWSQL	・・・・・・・・・・・・・・・・・・・

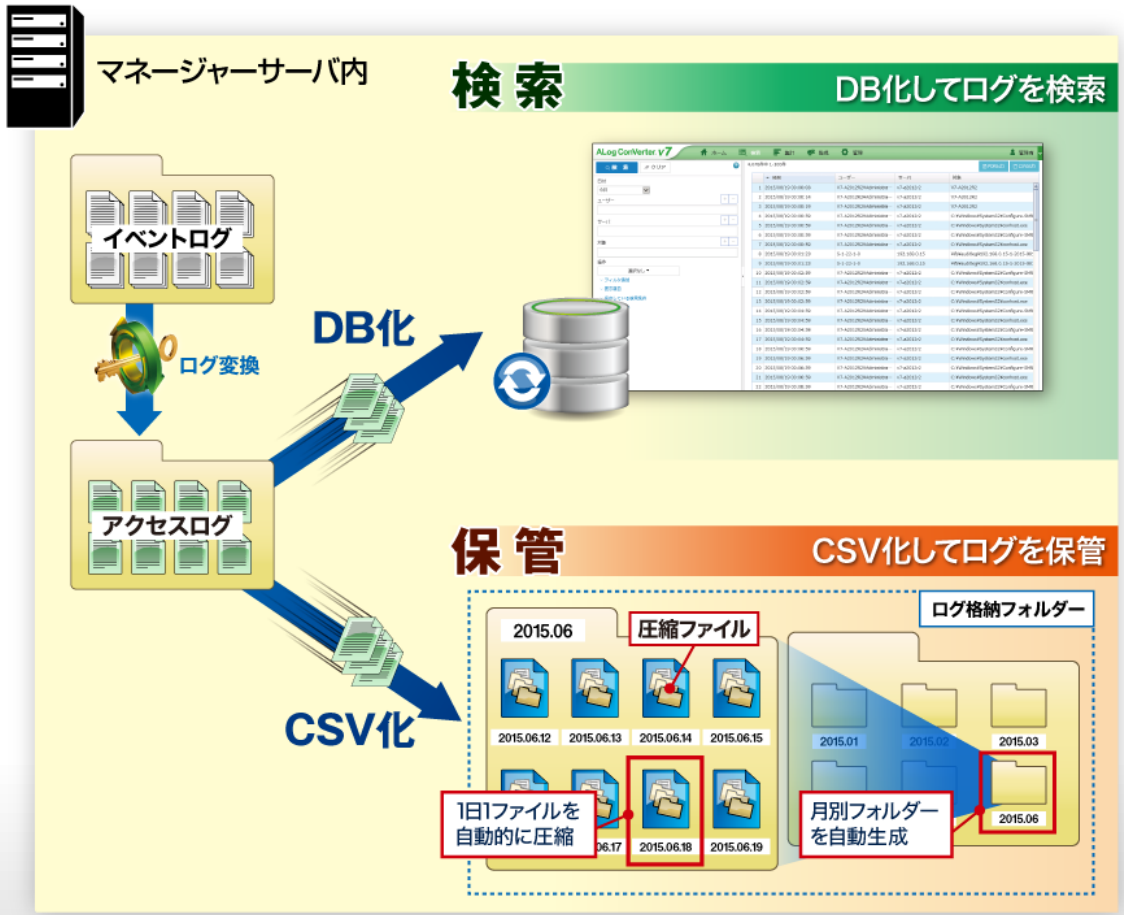
処理の流れ【 for SQL Server / for Oracle 】

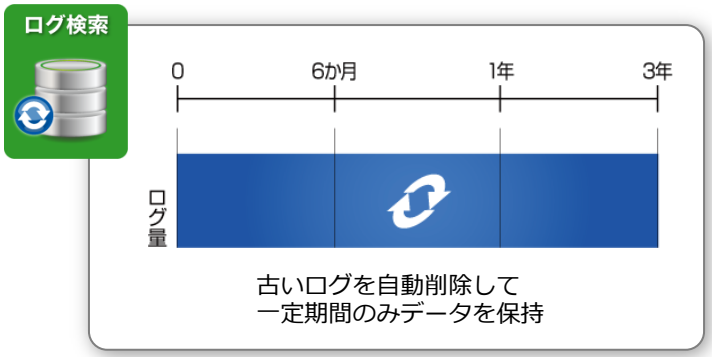


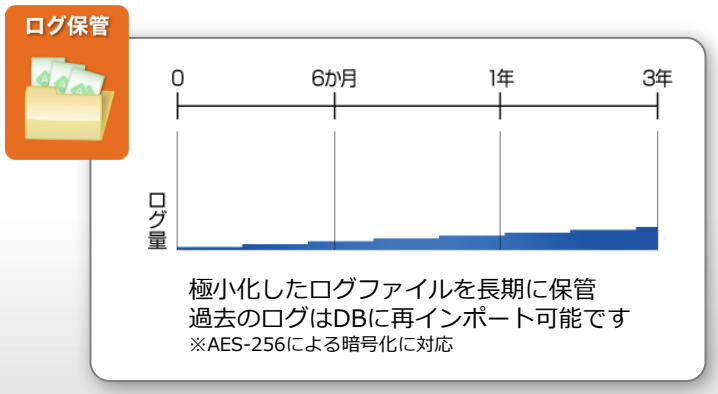
監査対象にモジュールを設置しない
エージェントレスタイプです

マネージャーサーバ内の仕組み

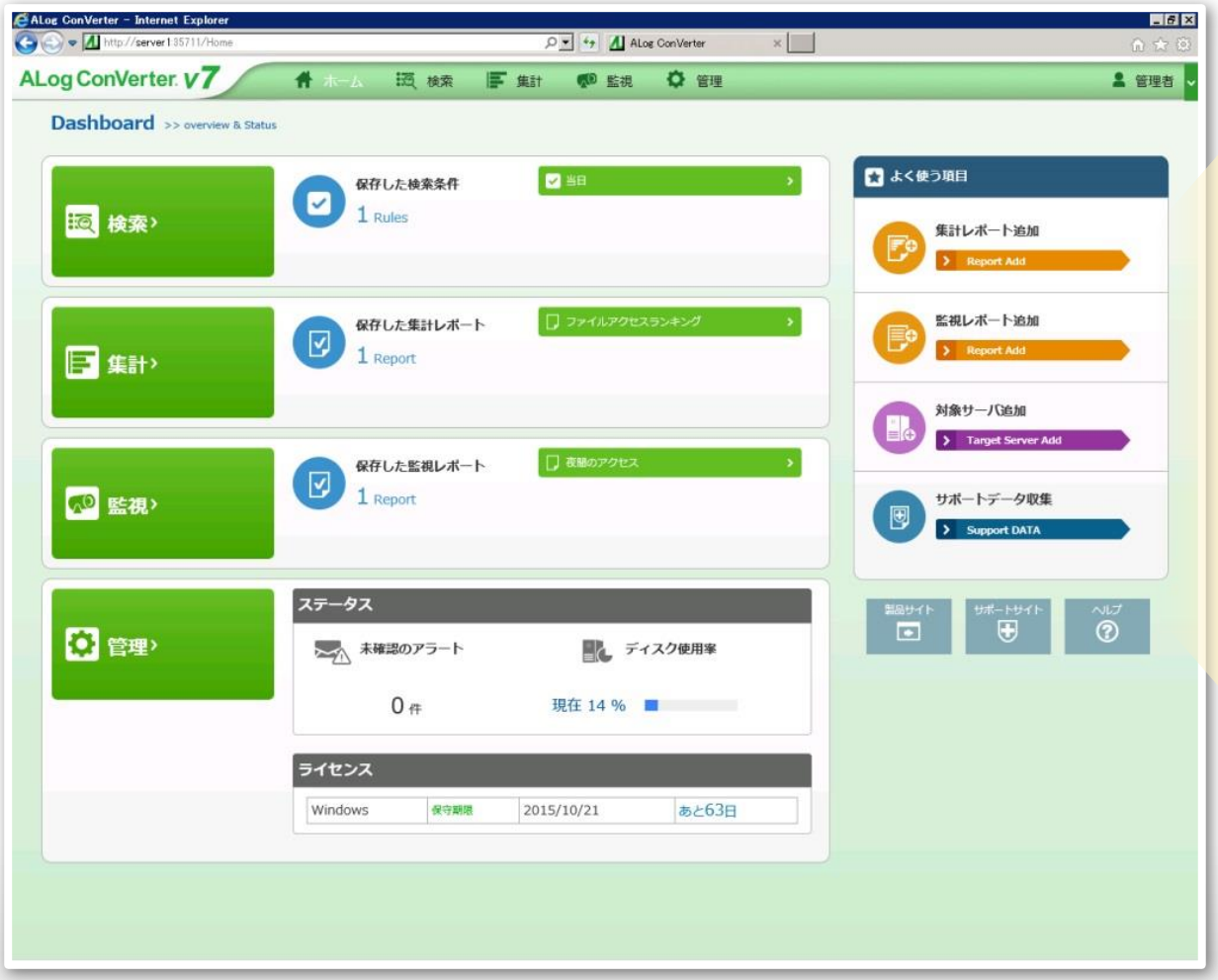
マネージャーサーバは、大量に蓄積されたログを長期に渡って保持できるように設計されています。
アクセスログをDBファイルとCSVファイルの2方向に作成し、高速検索と大容量の保管を実現します。







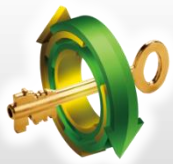
ALog V7 インターフェース



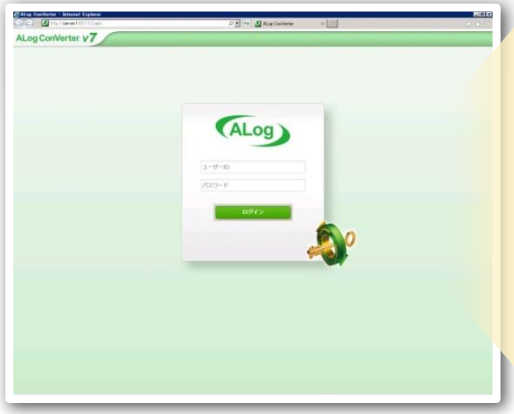
◆統一インターフェース◆
検索、集計、監視、管理、全ての機能を集約。
TOPページをダッシュボード化しました。

◆設定条件保存機能◆
一度定義した「検索のフィルタ条件」や
「監視レポート」などを記憶して
TOP画面から呼び出せるようになりました。

◆サポートデータ収集機能◆
障害発生時にサポートセンターに送る必要な
設定ファイルを自動的に生成します。



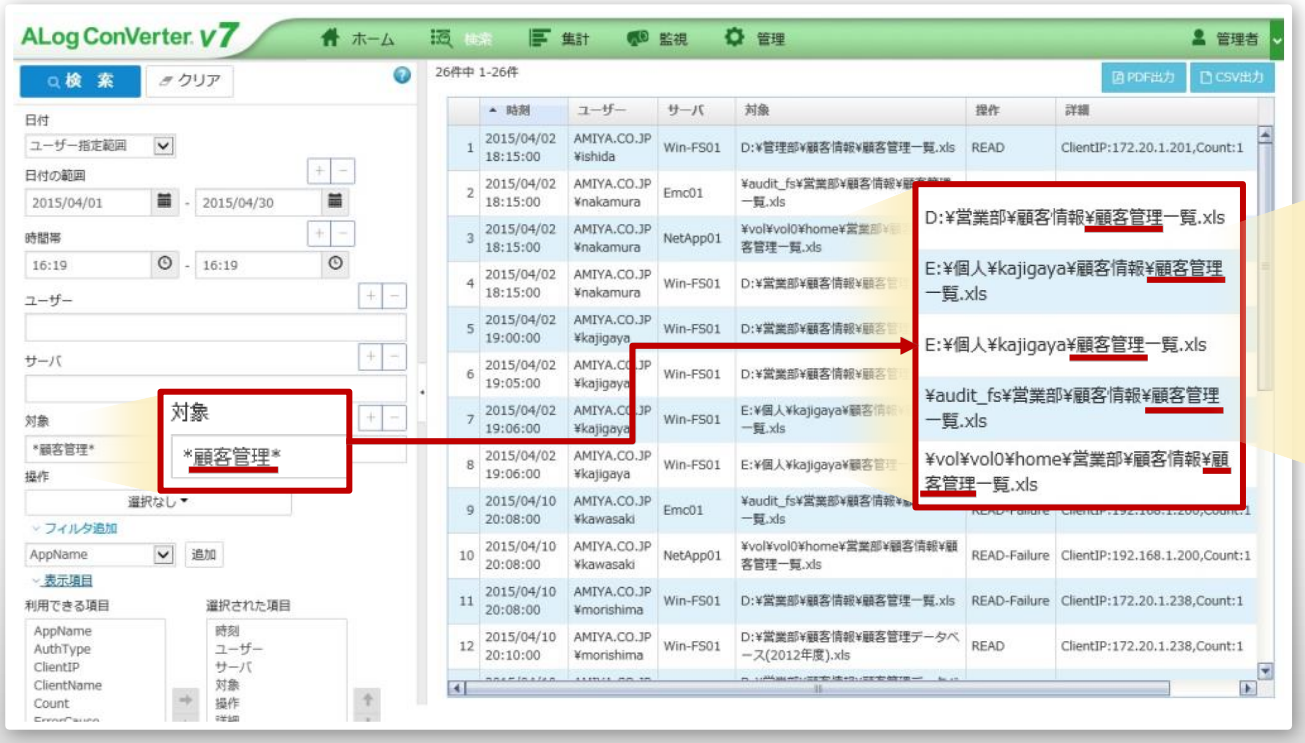
ALog V7 インターフェース



◆閲覧ユーザー制限機能◆
例：支店長Aに築地支店フォルダ
以下のアクセスログのみを参照させたい

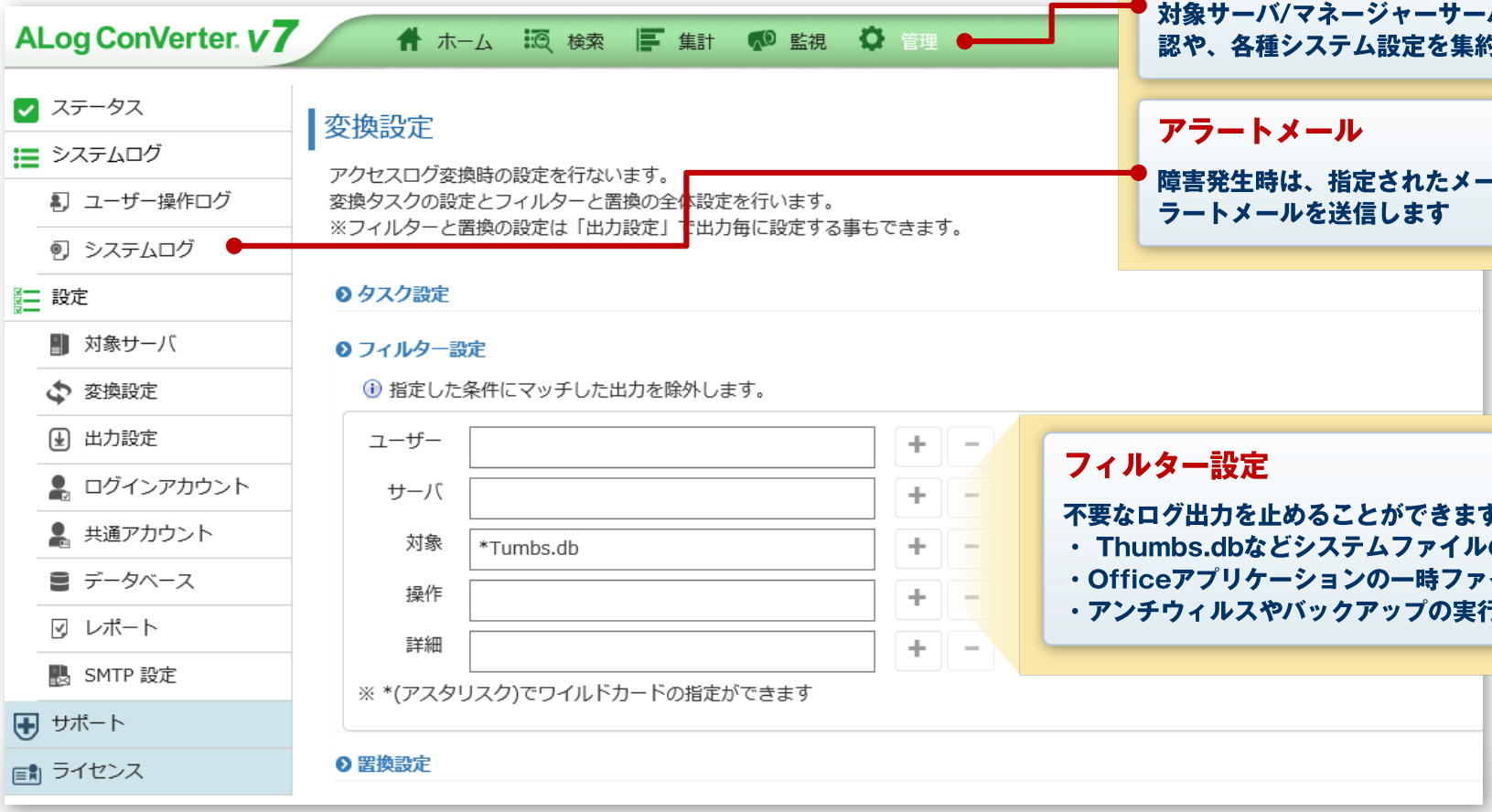
◆AD連携機能◆
ログインする認証ユーザーを
Active Directoryと連携可能に

◆検索の高速処理化◆
V7から新たに高速検索処理を実現
従来よりも更に速く、使いやすくなりました



◆ログフィルタ機能◆
- 顧客管理というファイル名のみを検索したい
- Bさんの1ヶ月間のアクセス履歴を知りたい
- Cファイルを削除したユーザーを探したい

ALog V7 インターフェース



管理機能

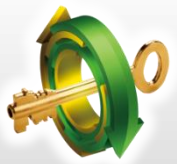
対象サーバ/マネージャーサーバのステータス確認や、各種システム設定を集約

アラートメール

障害発生時は、指定されたメールアドレスにアラートメールを送信します

フィルター設定

不要なログ出力を止めることができます
- Thumbs.dbなどシステムファイルのログ
- Officeアプリケーションの一時ファイルのログ
- アンチウィルスやバックアップの実行ユーザーのログ

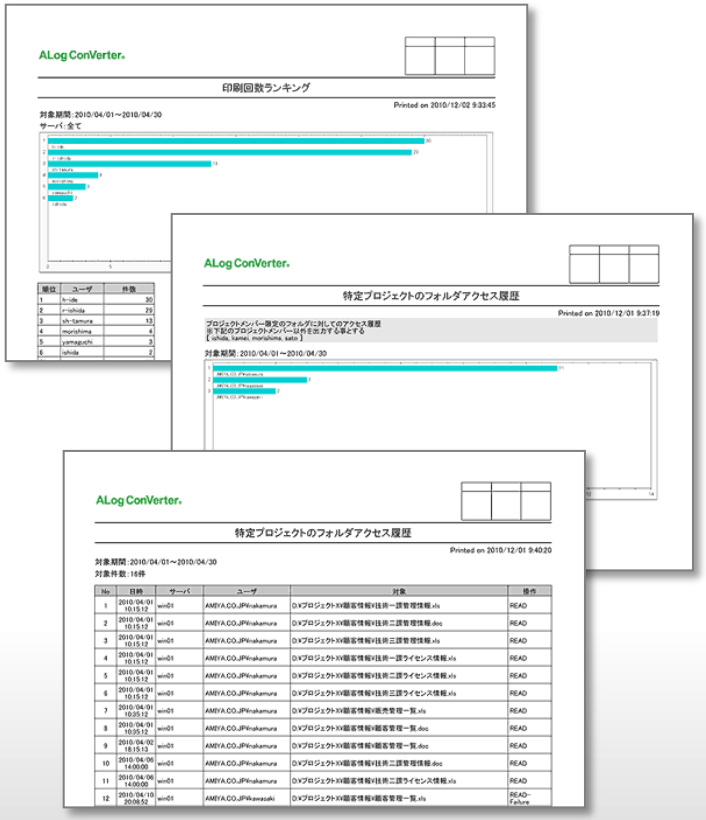


自動レポート作成機能

あらかじめ監視したい内容を設定しておけば、レポートが定期的に自動作成されます。
作成されたレポートをメールに添付して運用者に送付することもできます。

事前にセットしておけば

レポートが定期的に送られてくる



動作環境 – マネージャーサーバ

for SQL Server、for Oracle 共通

対応OS：	Windows Server 2008 (x64) / 2008R2 / 2012 / 2012R2 / 2016 ※32bit版OSには非対応 ※各OS のサービスパック（SP）に対応 ※各エディション（Standard / Enterprise / Datacenter）に対応 ※仮想環境、クラウド環境に対応
CPU：	Dual Core以上 （推奨：Quad Core 以上）
メモリ：	4GB 以上(推奨16GB 以上)
HDD：	500GB以上の空き容量（**「HDD試算例」参照**） ※対象サーバの台数やアクセスログの保管期間の長さによってはさらに空き容量が必要な場合があります
ソフトウェア：	.NET Framework 4.5以上 **※1** 以下のいずれかのWebブラウザ Internet Explorer10以降 Firefox バージョン40以降 Google Chrome バージョン44 以降 Microsoft SQL Server（対象サーバがSQL Serverの場合のみ）**※2** Oracle Client（対象サーバがOracle Databaseの場合のみ）

HDD試算例（for Oracle例）

前提 ・1日20万クエリ実行する (100MB)
・1年間分ログを保持する（約365日と仮定）
・検索用にDBデータを1年分保持する
・ RAWSQLログ/SYSDBログは取得しない

● **検索用DBデータ** ＝ 59GB /年

● **圧縮後アクセスログCSV** ＝ 730MB /年

計 ＝約60GB/年

※1
ALog ConVerter Anyをご利用になる場合は4.6以上が必要です

※2
for SQL Serverをご利用の場合は、トレースログを変換するためにSQL Server の機能を利用するため、ログ収集対象のSQL Server と同等以上のバージョンのSQL Server が必要です（例： SQL Server 2008 のログを収集する場合、マネージャーサーバにはSQL Server 2008 以上をインストールする必要があります）

動作環境 – 対象サーバ (for SQL Server)

対象サーバ　MS SQL Server

対応OS：	Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 ※各OS のサービスパック（SP）に対応 ※各エディション（Standard / Enterprise / Datacenter）に対応 ※仮想環境（VMWare, Hyper-V, Citrix XenServer）に対応
SQL Server：	Microsoft SQL Server 2005 / 2008 / 2008R2 / 2012 / 2014 / 2016 ※各エディション（Workgroup, Standard, Enterprise, Business Intelligence）に対応 ※32bit版、64bit版ともに対応
必要ソフトウェア：	.NET Framework 2.0 SP1 以上

動作条件

・マネージャーサーバから対象サーバのSQL Serverに対しリモート接続が出来ること
・「ストアドプロシージャの自動実行」が許可されていること
・AWE 機能が有効になっている場合、SQL Server を起動するWindowsユーザーアカウントに「lock pages in memory」権限が付与されていること
・ログの収集方式がエージェント方式の場合、対象サーバからマネージャーサーバの共有フォルダーへファイルの書き込みができること
・対象サーバの管理共有へアクセスできること

対象サーバ Oracle

対応OS：	Windows Server 2008 / 2008R2 / 2012 / 2012R2 / 2016 Red Hat Enterprise Linux 5 / 6 / 7 Oracle Linux 6.8 ※UKEに対応
対応Oracle Database：	Oracle Database 10.1.x / 10.2.x /11.1.x / 11.2.x / 12c
必要ソフトウェア：	.NET Framework 2.0 SP1 以上（OSがWindows Serverの場合のみ）

※Solarisまたは、MIRACLE LINUXをお使いの場合は、お問い合わせください。
※ALog ConVerter for Oracleは、RACによるクラスタ構成に対応しています。その他のクラスタ構成をご利用の場合はお問い合わせください。
※メーカーサポートが終了している製品・バージョンは十分なサポートをご提供できない恐れがあるため、メーカーサポート中の製品・バージョンをご利用いただくことを推奨します。

バージョンごとのログ出力形式

バージョン	ログ出力
Oracle 10.1.x, 10.2.X	**OS/DB**
Oracle 11.1.x, 11.2.X	**OS/XML/DB**
Oracle 12c	**OS/XML/DB**

※ ログ出力が「OS」の場合はミリ秒単位の時刻の出力および一般ユーザーのRAWSQL ログ収集ができません。

動作条件

・「AUDIT_TRAIL」によるデータベースの監査が利用できること（既に設定されている場合は、既存の監査設定が変更されることがあります）
・ログの収集方式がエージェント方式（OSがWindows Serverの場合のみ）の場合、対象サーバからマネージャーサーバの共有フォルダーへファイルの書き込みができること
・WindowsOSの場合、対象サーバの管理共有へアクセスできること

ALogシリーズ価格表

ALog ConVerter for SQL Server

製品名	数量	価格	年間保守
ALog ConVerter for SQL Server	1 SQL Server	¥600,000	¥108,000
	2 SQL Server	¥880,000	¥158,400
	3 SQL Server	¥1,130,000	¥203,400
	4 SQL Server	¥1,370,000	¥246,600
	5 SQL Server	¥1,580,000	¥284,400
	6 SQL Server	¥1,780,000	¥320,400
	7 SQL Server	¥1,960,000	¥352,800
	8 SQL Server	¥2,120,000	¥381,600
	9 SQL Server	¥2,260,000	¥406,800
	10 SQL Server	¥2,390,000	¥430,200
	11台以降	¥120,000	¥21,600
SQL Server 追加インスタンス	1 インスタンス	¥120,000	¥21,600

◆対象はMicrosoft SQL Serverになります。
◆ライセンスは対象のデータベースサーバ数でカウントします。
◆インスタンスごとにログを取得したい場合、別途「SQL Server追加インスタンス」が必要です。
◆保守は初年度必須でご加入下さい。次年度以降の保守金額も同額となります。
◆追加購入時の累積ボリュームディスカウントはありません。

ALogシリーズ価格表

ALog ConVerter for Oracle

製品名	数量	価格	年間保守
ALog ConVerter for Oracle	1 Oracle Database	¥780,000	¥140,400
	2 Oracle Database	¥1,130,000	¥203,400
	3 Oracle Database	¥1,460,000	¥262,800
	4 Oracle Database	¥1,760,000	¥316,800
	5 Oracle Database	¥2,040,000	¥367,200
	6 Oracle Database	¥2,300,000	¥414,000
	7 Oracle Database	¥2,530,000	¥455,400
	8 Oracle Database	¥2,740,000	¥493,200
	9 Oracle Database	¥2,920,000	¥525,600
	10 Oracle Database	¥3,080,000	¥554,400
	11台以降	¥160,000	¥28,800
Oracle 追加インスタンス	1 インスタンス	¥160,000	¥28,800

◆対象はOracle Database Serverになります。
◆ライセンスは対象のデータベースサーバ数でカウントします。
◆インスタンスごとにログを取得したい場合、別途「Oracle Server追加インスタンス」が必要です。
◆クラスタ構成の場合、クラスタ台数分のライセンスが必要です。
◆保守は初年度必須でご加入下さい。次年度以降の保守金額も同額となります。
◆追加購入時の累積ボリュームディスカウントはありません。

保守サポート

年間保守契約内容

- ○ テクニカルサポート
  （メール・電話での回答。年末年始を除く平日の9時～17時）
- ○ オンラインサポートセンターの利用
- ○ メジャーバージョンの無償利用
- ○ パッチ版（ログ変換プログラム）の無償利用

※ソフトウェア保守にはオンサイトのサービスは含まれません。
障害発生時には、メールや電話による問い合わせに対してサポートを行います。
現地での設定変更や再インストール作業は保守料金には含まれません。

オンラインサポートセンター

ALog ConVerter は、対象のサーバOSやDBのバージョンに
合わせてログ変換ロジックを随時更新しています。保守の継続更新を当初よりご想定下さい。