二重マスの文字をA～Eの順に
並べ替えてできる言葉はなんでしょう?

縦のカギ

1. 物事を理解することです
2. _____の唐揚げ
3. これをしてはいけません
4. 安物買いの___失い

横のカギ

5. めでたいと喜ぶことです
6. 揺れ動くことを表す言葉です
7. 地中に打ち込んで、目印や支柱にする棒のことです
8. 必要以上に可愛がってしまうことです
9. ___と弟

A	B	C	D	E

https://www.networld.co.jp/product/alog/

株式会社ネットワールド　http://www.networld.co.jp/

お問い合わせ　alog-info@networld.co.jp

本　　社　〒101-0051 東京都千代田区神田神保町2-11-15 住友商事神保町ビル　TEL:03-5210-5020,5031,5095
関 西 支 店　〒530-0001 大阪市北区梅田3-3-20 明治安田生命大阪梅田ビル 24F　TEL:06-7664-5400
中 部 支 店　〒451-6008 愛知県名古屋市西区牛島町6-1 名古屋ルーセントタワー8F　TEL:052-588-7611
九 州 支 店　〒812-0013 福岡市博多区博多駅東 2-6-1 九勤筑紫通ビル 3F　TEL:092-461-7815

統合ログ管理ツール

ALog EVA

「行動の全掌握」を実現せよ。

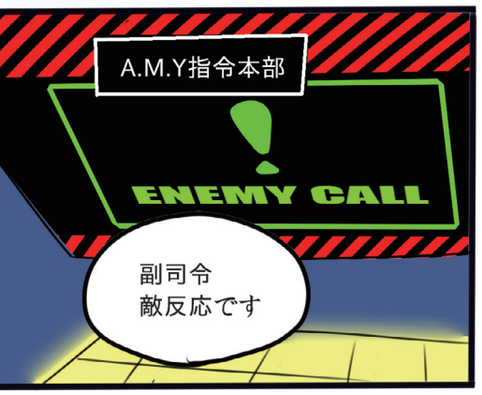
Networld

ALog

第1話 迫る魔の手！大都会に潜む恐怖

ここは世界的IT企業N社。――しかしそれは表の顔
裏では政府からの依頼を受け秘密組織A.M.Yを保有している。

それは、情報システム社員を
疲弊に追い込む、IT界に潜む魔物
DarkSideを撃退するためだった――



ALogシリーズに
「統合ログ管理ツール**ALog EVA**」が誕生

ALogシリーズは、情報セキュリティの基本かつ最大の対策とも言える「記録」の保持と監視を最も得意とする、エージェントを必要としないログ管理ツールです。
そのALogシリーズに、統合ログ管理ツールが加わりました。
ALog EVAで統合ログ管理を行うことで、全方位かつ活用型のログ管理を実現します。

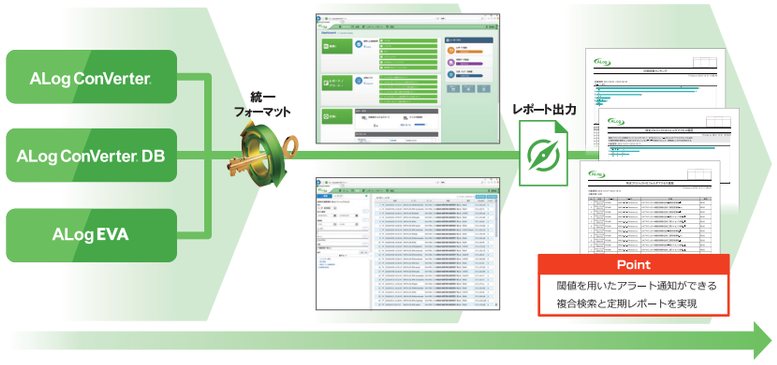
あらゆるデバイスの記録を保管する統合ログツール

ALog EVAはALogシリーズのログ範囲を飛躍的に拡大。
セキュリティ全般を全方位に統合管理し、サイバーアタックの検知、通信障害の原因探索、有事勃発時の事後追跡などのあらゆる記録を様々なデバイスから取得してセキュリティリスクの可視化と監視／レポートを行います。

圧倒的な視認性と使いやすさ

統合ログ管理ツールのよく聞く失敗例
複雑な設計と難解なデータマッピング設定で導入時に極端に疲弊…

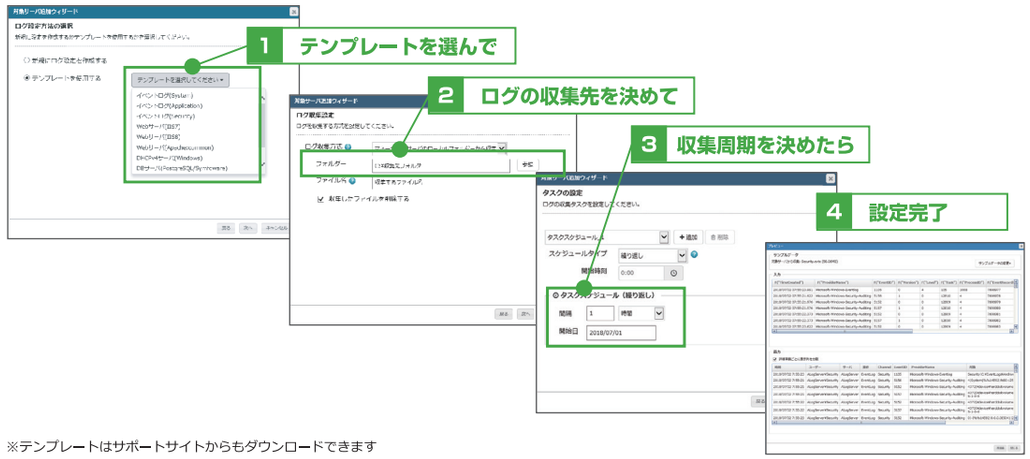
直観的に操作ができるシンプルなGUI、共通インターフェイスで「管理の一元化」が可能に



『非常に分かりにくい設定操作』という従来の問題点を一掃、ユーザー目線での「使いやすさ」を追求、実現しました。
ALog EVAが取得した情報は、シリーズ共通のインターフェースで管理されます。ひとつの管理画面で「不正操作の検出」と「セキュリティレポートの出力」を両立し、ログ管理で陥りがちな複合管理の深刻な煩わしさを解消します。

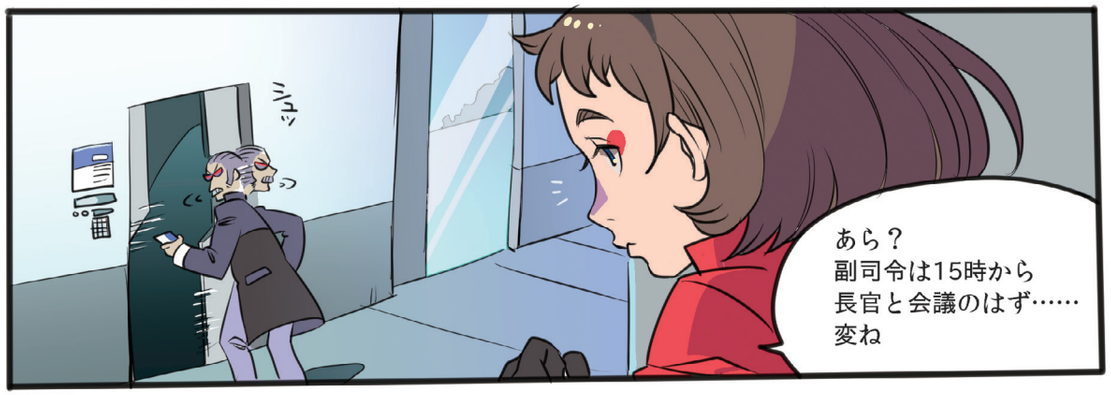
専用テンプレートを標準装備、スピーディーなログマッピングを実現

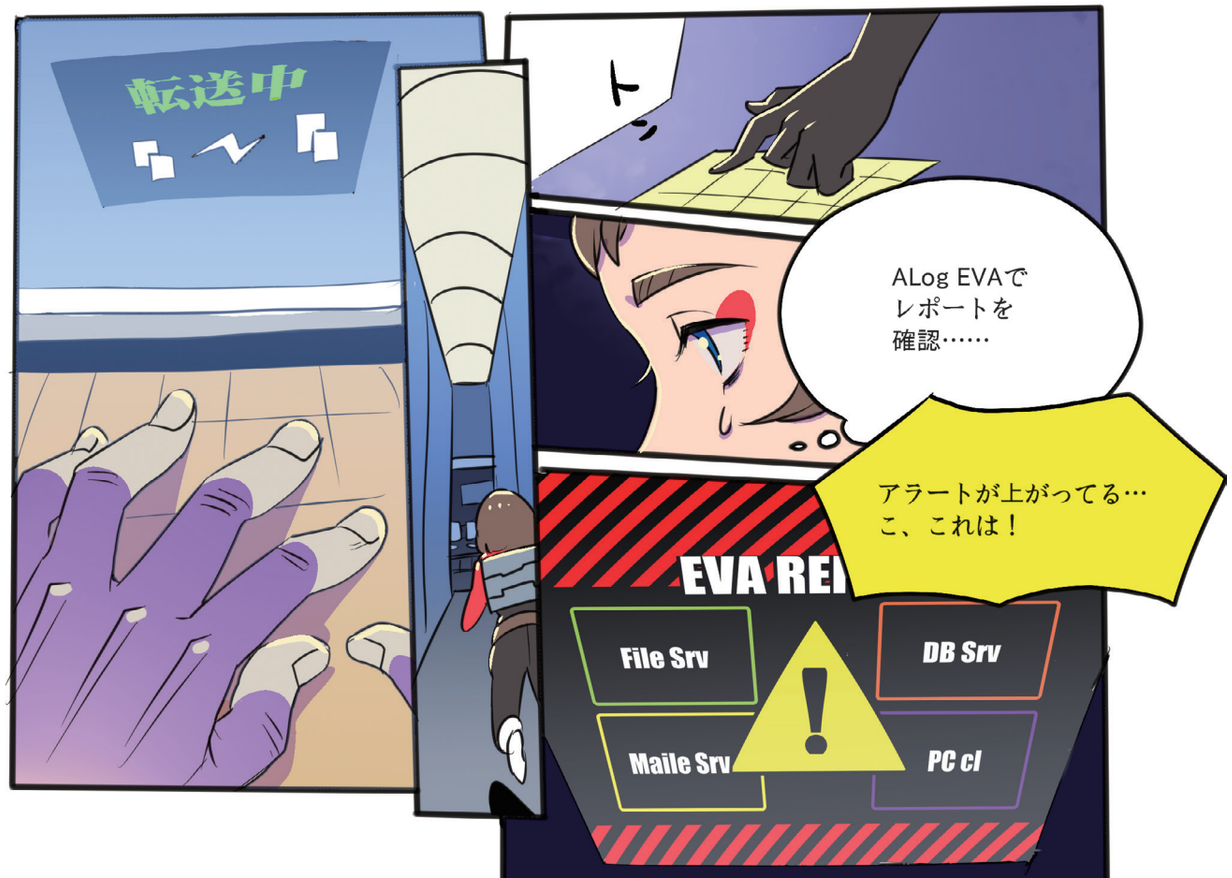
テンプレートを選ぶだけで設定完了、従来製品の導入障壁である”専門的技術がないと構築できない”を払拭しました。
テンプレートを使わない場合も、シンプルで使いやすいGUIで簡単に設定できます。スクリプト言語による複雑な定義を書かなくても、マッピング設定が可能です。

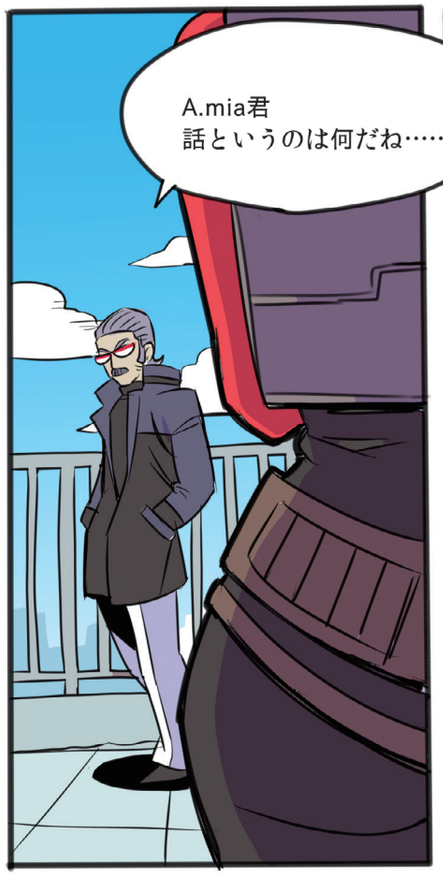


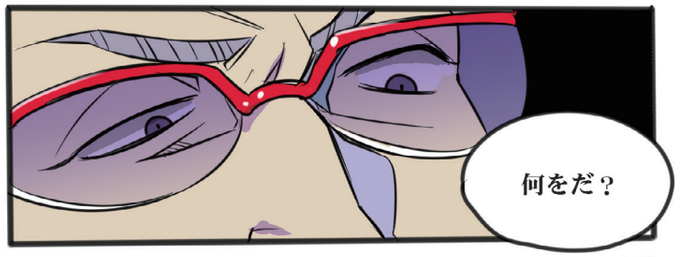
※テンプレートはサポートサイトからもダウンロードできます

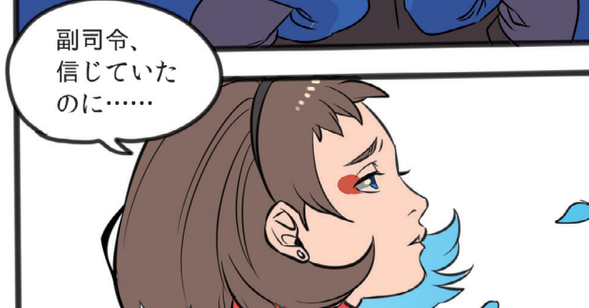
第2話 ボスの反乱、涙の別れ











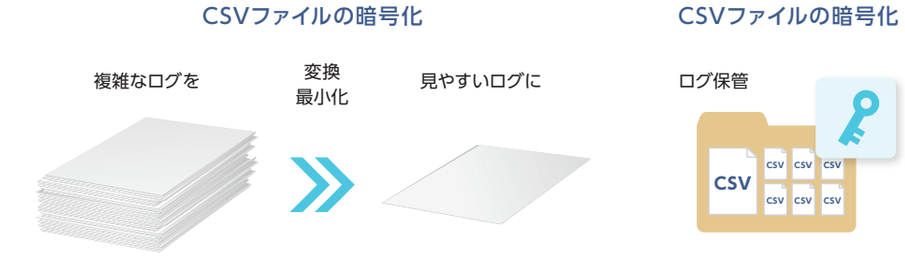
分かりやすく最小化、“活用型ログ”の長期保管を実現

統合ログ管理ツールのよく聞く失敗例

ログ量が膨大で、視認性がなく解読困難。ただ溜めているだけの状態。

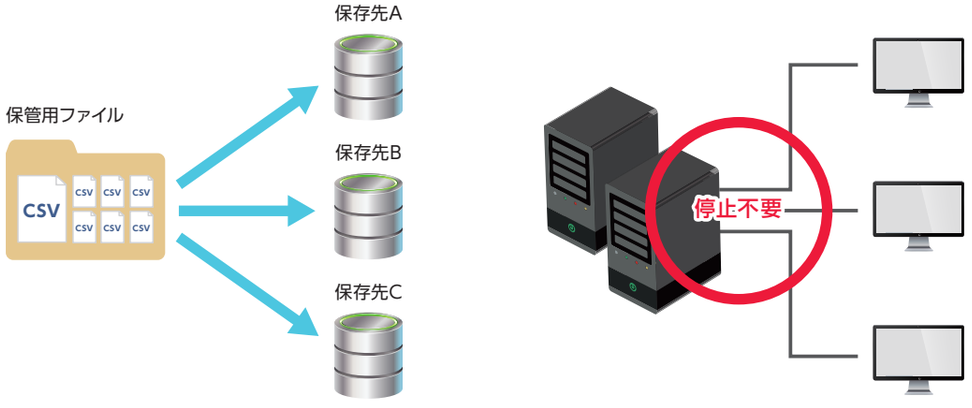
“役に立つログ”で長期保存

マッピング後ログ変換により最小化したログを圧縮保管する事で、記憶領域の節約を実現し長期保管を可能にします。
また、変換したログはCSV暗号化が可能なため改ざんの心配もありません。DBの保管期間は任意に設定が可能です。



保管用に変換・出力されたCSVファイルがバックアップファイルに

CSVファイル（暗号化可能）は、複数の保存先を指定することができます。
保存期間についても保存先ごとに指定が可能です。
従って、バックアップ用にファイルの変換や圧縮などの操作は必要ありません。
また、その都度詳細な指定・設定をする必要がなく、システムの停止も不要です。



オプション不要、検索やレポートは標準装備

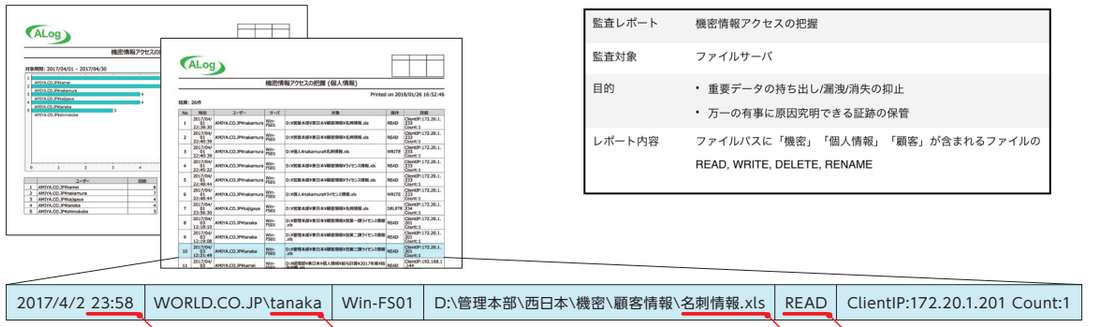
統合ログ管理ツールのよく聞く失敗例

検索ツールやレポーティングツールは別製品または別オプション…
複数導入しないと実用に至らない。

レポートは定期的に自動作成

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。

レポートサンプル



内部不正対策を目的とした場合の例

監査レポート	機密情報アクセスの把握
監査対象	ファイルサーバ
目的	• 重要データの持ち出し/漏洩/消失の抑止 • 万一の有事に原因究明できる証跡の保管
レポート内容	ファイルパスに「機密」「個人情報」「顧客」が含まれるファイルの READ, WRITE, DELETE, RENAME

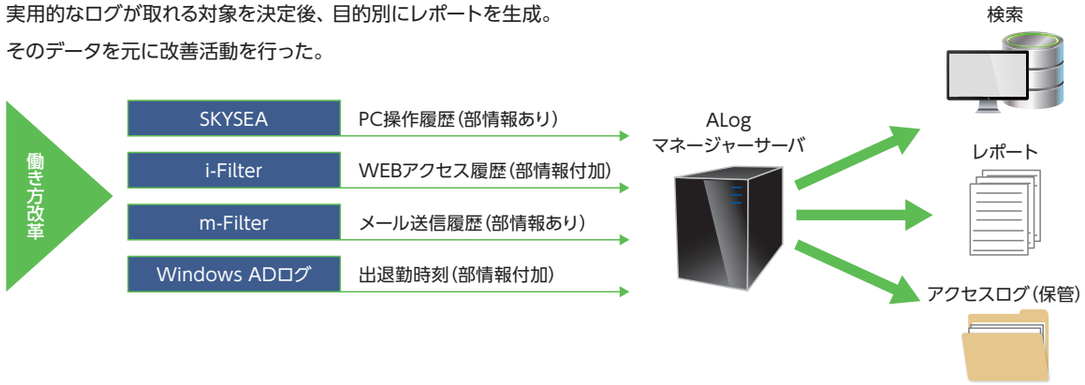
監査 ▶		事象／対象／行動 ▶	出力
機密情報アクセスの把握	事象	持ち出し、漏洩、消失の防止、操作の記録保管	機密ワード 月度レポート
	対象	ファイルサーバ	個人情報ワード 月度レポート
	行動	ファイル名（機密／個人情報）へのR／W／R／Dを取得	
管理者操作の正当証明	事象	管理者による不正行為の防止、正当性証明	ADサーバ特権管理者　月度レポート
	対象	ADサーバ／DBサーバ	DBサーバ特権管理者　月度レポート
	行動	ドメインコントローラ上／DB上の管理操作を取得	
要注意人物の監視（特定者のみ）	事象	退職予定者の監督（情報の売買防止）	ユーザーAの全ファイルアクセス　月度レポート
	対象	ファイルサーバ／メールサーバログ	ユーザーAの全メール送受信　月度レポート
	行動	ユーザーAのファイル利用／メールの履歴を取得	
不正ファイルアップロードの監視	事象	ストレージサイト等への業務ファイルのアップロード禁止	Upload回数上位者をランキング表示
	対象	WebProxyログ	時間外Upload実行上位者をアラート通知
	行動	外部アップロードファイル／接続先の履歴を取得	
不正コピー／保管履歴の監視	事象	外部デバイスを介した漏洩の防止	全ての外部デバイスコピー　日次レポート
	対象	クライアントPC	開発部門の外部デバイスコピー　日次レポート
	行動	外部デバイス（E／F drive）にコピーした履歴を取得	

働き方改革に乗り出したA市。残業解消や不適切労働の実態把握を目的にログ管理を行うことになった。

ALog EVA選定Point

- ☑ 複数のログを一気通貫でレポーティングできる
- ☑ ログから勤怠表が自動作成される
- ☑ 部署ごとに閲覧できるログやレポートの範囲が制限できる

実用的なログが取れる対象を決定後、目的別にレポートを生成。
そのデータを元に改善活動を行った。



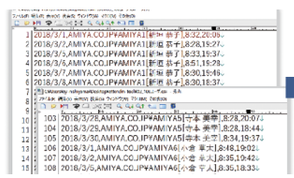
目的別 ー監視対象とレポートー

目的 ▶	ログの種類 ▶	レポート
過度な残業／サービス残業の把握	Windowsログオン／オフ タイムカードのログ	勤怠票表の出力
時間外労働の把握	ファイルサーバログ メールログ	退職予定者のファイル利用／ メール利用一覧
不適切行為の把握	WebProxyログ	SNS利用ヘビーユーザーランキングTOP10
	PCログ	有害サイト閲覧数ランキングTOP10

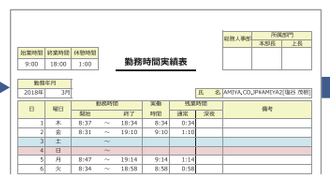
データを元に改善活動

運用例 ータイムカードのログから残業時間を確認ー

タイムカードのログ



ALogで勤怠帳票を自動化



累計残業時間をランキング

Rank	ユーザー名	累計残業時間
1	AMIYA.CO.JP¥AMIYA77[谷 きみ]	33:32
2	AMIYA.CO.JP¥AMIYA71[井川 さやか]	33:12
3	AMIYA.CO.JP¥AMIYA43[柴咲 恭子]	32:35
4	AMIYA.CO.JP¥AMIYA6[小倉 草太]	32:34
5	AMIYA.CO.JP¥AMIYA44[柳原 三省]	32:34
6	AMIYA.CO.JP¥AMIYA55[長岡 人志]	32:17
7	AMIYA.CO.JP¥AMIYA83[小川 優一]	32:11
8	AMIYA.CO.JP¥AMIYA33[大平 早織]	32:07

品名	ライセンス価格	型番	年間保守価格	型番
S（5GB／day）	¥800,000	AL-EVAS	¥144,000	M-AL-EVAS
M（20GB／day）	¥2,750,000	AL-EVAM	¥495,000	M-AL-EVAM
L（50GB／day）	¥5,000,000	AL-EVAL	¥900,000	M-AL-EVAL
NL（No Limit）	¥8,750,000	AL-EVANL	¥1,575,000	M-AL-EVANL

※ レンジはALog EVAが1日に収集するログの総容量に応じてご選択します。
※ ログの総容量が保有ライセンスの上限値を超えた場合、上位レンジのライセンスへの切替えが差額分の購入で可能です。
※ 保守は初年度必須です。
※ 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。

レンジ選択の例

Windows DHCPサーバの場合
- ログ収集対象のサーバ：1台
- クライアント端末数：2000台
- ➡ 0.2GB／日
- ➡ Sレンジ

ファイアウォール機器の場合
- ログ収集対象の機器：2台
- クライアント端末数：1000台
- ネットワーク拒否と許可の双方を取得
- ➡ 1.5GB/日×2台 ＝ 3GB／日
- ➡ Sレンジ

※この例は、ALog EVAをご利用中のお客様の環境を元にしたサンプルデータです。お客様の環境によりログ出力量が異なりますのでご注意ください。
詳しくはお問い合わせください。

ネットワールドの有償サービス

弊社エンジニアが現地にお伺いして、作業いたします。日頃、製品を担当しているスペシャリストなので安心！ お客様のニーズに合わせて、様々なサービスをご提供いたします。

対象製品	ALog EVA
標準作業	導入前設計支援、導入前準備、環境構築、基本動作確認、 基本トレーニング、設定シート作成
価格・作業条件	弊社担当営業までお問い合わせ下さい。

ALog EVAの他、ALog ConVerter for Windows、for NetApp、for EMCの導入サービスもございます。
是非ご利用ください。