超サポ
愉快カンパニー
アシスト

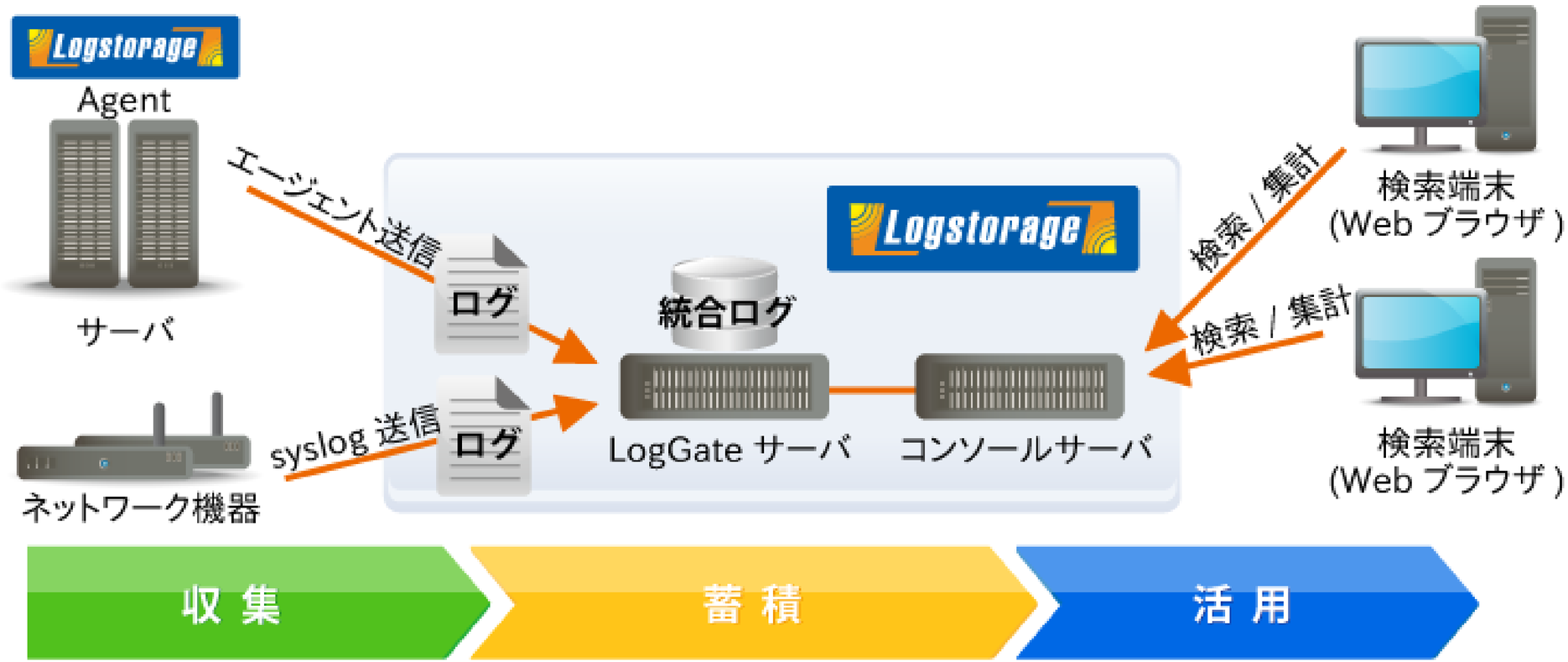
Logstorageのことが よくわかる紹介資料

文書番号：LS0001WG

目次

統合ログ管理システムLogstorage とは

Logstorageはインフォサイエンス社で開発された“国産“の統合ログ管理システムです。
標的型攻撃や内部不正への備え、PCIDSS/GDPR/監査への対応など、様々な目的に対して必要な機能を網羅しています。
国内導入企業は、2500社以上。金融・IT・公共・製造・サービス・官公庁・運輸・教育・食品あらゆる業種業態の
お客様にご利用いただいています。



アシスト+Logstorage

豊富な導入実績

アシストでは、2006年からログ管理製品の取り扱いを始め、現在では、
250社以上のユーザ様に対して、製品の導入・構築・運用サポートをご支援しています。

専任SEによる充実の導入支援サービス

クラスタ対応、他製品との連携、各種トレーニングなど、Logstorageの導入支援サービスを充実させており、お客様要件に沿ったサービスを提供しています。

スキルトランスファー型支援

アシストでは、これまで培ってきたノウハウをお客様へスキルトランスファーする事で、お客様自身で運用し活用いただく為のご支援をしています。検討・設計段階から運用に至るまで、万全の体制でサポートします。

アシストのLogstorageサポートサービス

安心、専任のサポート体制

導入メンバーから、専任サポートメンバーにお客様の環境情報を引き継ぐことで、問い合わせの際は即座に問題解決に取り掛かれます。専任サポートメンバーと導入メンバー相互に情報を連携し、導入後も安心してご利用いただけるサポート体制をとっております。

保守サービス内容

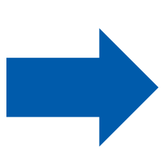
サポート専用のWebサイト/電子メール/電話を用意し、専任のサポートメンバーがきめ細かく対応致します。

・受付時間：24時間365日受付(サポート専用Webサイト/電子メール)
・回答時間：9:00～17:00 月曜日～金曜日(休日を除く)
・パッチ、バージョンアップメディアの無償提供

Logstorage 機能紹介

Logstorage 機能の概要

Logstorageは、ログを収集する、収集したログを蓄積する、蓄積したログを活用する3つの機能で構成されています。



あらゆる収集方法

独自データベース　インデックス

高速検索　表・グラフ　即時検知　定期レポート

テキスト形式の全てのログを収集します。ログの種類や収集のタイミングなど要件にあわせてあらゆる収集方法を提供し、200種類を超える収集実績があります。

ログの受信と蓄積を行います。インデックスを作成するので、高速検索が可能です。Logstorage独自のデータベースのため改竄不可で、ログの正当性を担保します。

蓄積したログを検索/分析します。Webブラウザがあれば、どこからでもアクセスし、検索/分析ができます。また、レポート作成や定期的なメール配信が可能です。

ログ収集機能について

あらゆる収集方法を提供

Logstorageは、テキストで出力されるログを全て収集できます。また、収集するログの種類や収集対象サーバへのLogstorageモジュール導入可否、ログ収集のタイミング(リアルタイムか、定期実行か)によって、あらゆる収集方法を提供しています。

収集方法名称	収集対象	モジュール導入有無	収集のタイミング	概要
LogstorageAgent	UNIX/Windowsサーバ上のテキストログ	有	リアルタイム	対象サーバのログファイルやイベントログをリアルタイム監視し、収集します。
SecureBatchTransfer	UNIX/Windowsサーバ上のテキストログ	有	定期実行	バッチ実行によりログをFTP/FTPSで収集します。圧縮転送、転送済ファイルの削除機能があります。
EventLogCollector	Windowsサーバイベントログ、VMwareイベントログ、NetApp/EMCストレージイベントログ	無	定期実行	**イベントログ専用**収集モジュールです。収集対象サーバへのモジュール導入は不要です。
クラウド専用モジュール	AWS、Azure、Box、Office365	無	定期実行	**クラウド専用**収集モジュールです。 ※クラウドサービス側での出力設定が必要です。

※収集可能なログ1行の最大長は約32KB(32,767Byte)となります。

Logstorageモジュール以外の収集方法

収集対象のサーバにモジュールを導入できない場合でも、収集対象側のOS標準機能などでログを転送することができれば、Logstorageに収集/蓄積が可能です。以下、OS標準機能を使った収集方法です。

収集方法名称	収集対象	モジュール導入有無	収集のタイミング	概要
Syslog	ネットワーク機器、syslog	無	リアルタイム	機器標準のSyslog転送を利用し、直接受信します。Syslogサーバとして利用が可能です。
FTP/フォルダ監視	UNIX/Windowsサーバ上のテキストログ	無	転送実行タイミングに依存	モジュールが導入できないサーバの標準機能など。FTPまたはファイル共有などでログを収集します。

ログ収集の実績（一部抜粋）

対象	実績	対象	実績	対象	実績	対象	実績
OSシステム・イベント	・Windows ・Solaris ・AIX ・HP-UX ・Linux ・BSD	Webサーバ／プロキシ	・Apache ・IIS ・Blue Coat ・i-Filter ・squid ・WebSense	メール	・MS Exchange ・sendmail ・Postfix ・qmail	クラウド	・AWS ・Azure ・Office365 ・BOX ・G Suite
クライアント操作	・秘文 ・Info Trace ・MyLogStar ・CWAT ・Malion ・SeP ・QND ・LanScope Cat ・SKYSEA Client View	ネットワーク機器	・Cisco PIX/ASA ・Cisco Catalyst ・NetScreen ・SSG ・VPN-1 ・Firewall-1 ・SSL-VPN ・Palo Alto ・FortiGate	サーバアクセス	・CA Priviredged Identity Manager ・VISUACT ・File Server Audit ・SecureCube/ AccessCheck ・Alogコンバータ	その他	・SAP　R/3（ERP） ・NetApp(NAS) ・IVEX Meta Logger
データベース	・Oracle ・SQLServer ・DB2 ・PostgreSQL ・MySQL	運用監視	・JP1 ・Systemwalker ・Open View	データベース監査ツール	・PISO ・SSDB監査 ・SecureSphere ・Chakra		

収集モジュールの詳細説明

Logstorage Agentについて

UNIX/Windowsサーバ上のテキストログをリアルタイムに収集するLogstorage Agentの機能詳細です。

機能名	概要
ログのリアルタイム送信	ログファイルの更新を監視し、追記されたログをリアルタイムでLogGateに送信します。
ログの再送信	LogGateに送信できない場合に、一定量までのログをキャッシュして再送信できます。
送信先LogGateの自動切換	プライマリのLogGateに接続できない場合、送信先をセカンダリのLogGateに自動的に切り換えます。 （LogGateがプライマリーセカンダリ構成の場合）
システム高負荷時の動作抑制	ログソースが高負荷となったとき、サーバの稼働に影響しないよう、ログ送信を一時抑制します。
ブロックログの連結	複数行にまたがるログを解析し、1行のログとして送信できます。
ローテートログの追跡	ローテートされたログファイルを追跡し、ログを送信できます。
送信ログのフィルタ	キーワードによるログのフィルタリングを行い、必要なログのみ送信できます。
暗号化通信	独自プロトコル(LLTP)をSSL暗号化しセキュアにログを送信できます。

※ ローテーションの方式などによっては、ログの取りこぼしが発生する可能性がございます。

SecureBatchTransfer(SBT)について

UNIX/Windowsサーバ上のテキストログを定期的に収集するSecureBatchTransfer(SBT)の機能詳細です。

機能名	概要
ログファイルのバッチ転送	テキストログをファイル単位でLogGateに送信します。FTP／FTPSプロトコルを使用します。
送信対象ファイルの識別	ファイル更新日、またはファイル名に付与された日時情報から、送信対象のファイルを識別します。
ログファイルの圧縮転送	ログを圧縮してからLogGateへ送信できます。
暗号化通信	FTPSプロトコルによる暗号化通信に対応しています。
送信済みログファイルの削除	送信済みのログファイルを削除できます。
送信失敗時のリカバリ	LogGateへの送信に失敗したログファイルを再送信できます。
Oracleログの取得	XML形式に出力したOracle監査ログを収集できます（SBT for Oracle が別途必要です）

※ SBTはファイル単位での送信となります。ファイル内容の差分取得には対応していません。

EventLogCollector (ELC)について

Windowsサーバ、VMWare、NetApp/EMCストレージのイベントログをエージェントレスで収集するEventLogCollector（ELC）の機能詳細です。

機能名	概要
イベントログの定期自動収集	イベントログを定期的に自動収集します。収集間隔は最短1分です。
ログの解析機能	収集したログをELCが解析し、人にとって読みやすいコンパクトな解析ログを生成します。
元ログと解析ログの使い分け	【元ログのみ / 解析ログのみ / 両方】を選択して取り込むことが可能です。
解析ログの選択	解析する項目(ファイルアクセスやログインログオフ、管理者操作など)を選ぶことができます。
エージェントレス収集	専用コレクタにより、Windows/ V Mware/NetAPP/EMCのイベントログをエージェントレスで収集可能です。
ELCサーバの冗長構成	プライマリ、セカンダリのELCサーバが構築でき、プライマリが落ちた場合でもセカンダリが自動で収集を継続します。

EventLogCollectorのイベントログ解析機能

EventLogCollector (ELC)は、Windowsイベントログを、自動的に見やすくコンパクトに変換するログ解析機能があります。

複雑なイベントログを…

Windows EventLog(Security)	オブジェクトのオープン	Security[560]: [34127, 失敗の監査, Fri May 21 14:59:34, ENDO-WORK¥endo, ENDO-WORK] オブジェクトのオープン: オブジェクト サーバー: Security オブジェクトの種類: File オブジェクト名: C:¥test¥新規テキスト文書.txt ハンドル ID: - 操作 ID: {0,59559484} プロセス ID: 1404 イメージ ファイル名: C:¥WINDOWS¥explorer.exe プライマリ ユーザー名: endo プライマリ ドメイン: ENDO-WORK プライマリ ログオン ID: (0x0,0x1D733) クライアント ユーザー名: - クライアント ドメイン: - クライアント ログオン ID: - アクセス READ_CONTROL SYNCHRONIZE ReadData (または ListDirectory) ReadEA ReadAttributes 特権 - 制限された SID 数: 0
Windows EventLog(Security)	オブジェクトのオープン	Security[560]: [34128, 失敗の監査, Fri May 21 14:59:34, ENDO-WORK¥endo, ENDO-WORK] オブジェクトのオープン: オブジェクト サーバー: Security オブジェクトの種類: File オブジェクト名: C:¥test¥新規テキスト文書.txt ハンドル ID: - 操作 ID: {0,59559485} プロセス ID: 1404 イメージ ファイル名: C:¥WINDOWS¥explorer.exe プライマリ ユーザー名: endo プライマリ ドメイン: ENDO-WORK プライマリ ログオン ID: (0x0,0x1D733) クライアント ユーザー名: - クライアント ドメイン: - クライアント ログオン ID: - アクセス READ_CONTROL SYNCHRONIZE ReadData (または ListDirectory) ReadEA ReadAttributes 特権 - 制限された SID 数: 0
Windows EventLog(Security)	オブジェクトのオープン	Security[560]: [34130, 失敗の監査, Fri May 21 14:59:35, ENDO-WORK¥endo, ENDO-WORK] オブジェクトのオープン: オブジェクト サーバー: Security オブジェクトの種類: File オブジェクト名: C:¥test¥新規テキスト文書.txt ハンドル ID: - 操作 ID: {0,59564449} プロセス ID: 1404 イメージ ファイル名: C:¥WINDOWS¥explorer.exe プライマリ ユーザー名: endo プライマリ ドメイン: ENDO-WORK プライマリ ログオン ID: (0x0,0x1D733) クライアント ユーザー名: - クライアント ドメイン: - クライアント ログオン ID: - アクセス SYNCHRONIZE ReadAttributes 特権 - 制限された SID 数: 0

自動的に見やすいログに変換

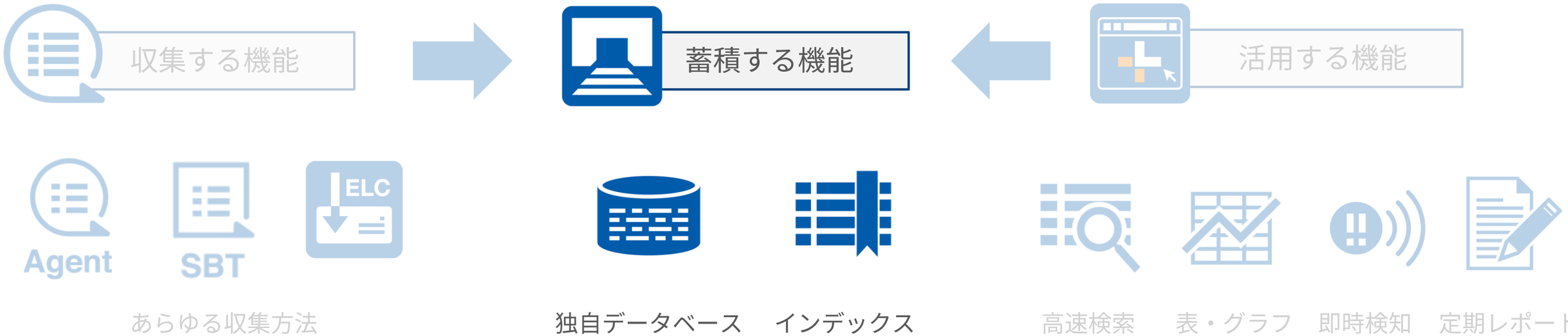
2010-05-21 14:59:34	localhost	ファイル読み込み	ENDO-WORK	endo	C:¥test¥	新規テキスト文書.txt	失敗
2010-05-21 14:59:35	localhost	ファイル書込み	ENDO-WORK	endo	C:¥test¥	新規テキスト文書.txt	失敗

イベント解析機能の解析対象

イベント解析機能では、以下のログ種別を解析し、見やすくすることができます。

ログ種別	内容
ローカルログオン	ローカルからのログオン／ログオン失敗
リモートログオン	リモートからのログオン／ログオン失敗
ファイルアクセス	ファイルの読み込み／書き込み／削除／名前変更／印刷
プロセス起動・終了	プロセスの起動／終了
管理者操作	管理者(Administrators)操作
Windowsファイアウォール	ファイアウォールの有効／無効、ルール作成／変更／削除、ポート許可／ブロック
システム設定変更	イベントログの削除／時刻変更／タスクスケジュール登録／サービス登録

ログ蓄積機能



ログ蓄積機能(LogGate)について

LogGateは、収集したログを構造化したデータとして圧縮保存し、ログの検索処理や、ログのリアルタイム検知を行います。ログ容量が増加した場合は、ライセンスの切り替えやLogGateを複数台で構成することで、ログの取り込みパフォーマンスを向上させることが可能です。

Logstorage独自のデータベース。
生ログ(テキスト)から最大1/10まで圧縮。

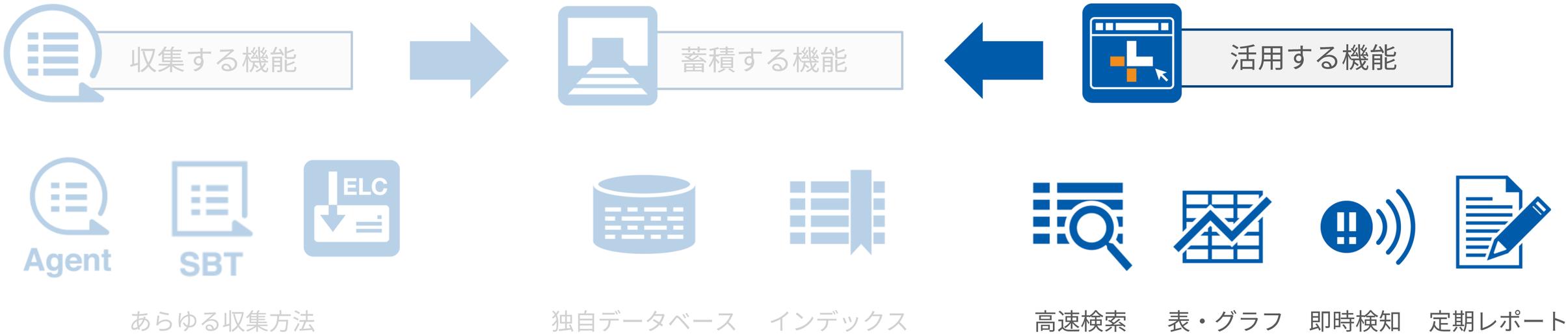
インデックスを作成し、高速検索を実現。1億件のログをわずか数秒で表示。

データは人の目では意味が
分かりづらいバイナリで保管。
さらにAES256で暗号化もかけられ、
よりセキュアに保管可能。

(備考)
1台あたりのLogGateがリアルタイムで収集できるログ量は以下の通りです。

- ワークグループ版(WG) 秒間 1,000行
- スタンダード版(ST)　秒間 2,000行　（※Enterprise版もLogGate1台あたりで同等）
- エンハンスト版(EH)　秒間 3,000行　（※Advanced版もLogGate1台あたりで同等）

ログ活用機能



ログ活用機能(コンソール)について

コンソールサーバは、Webサーバとして動作します。管理者はブラウザからアクセスし、ログの検索/集計/レポート出力や、その他各種設定を行います。

高速検索

大量ログからすぐに
検索結果を表示可能。
億単位のログから数秒で検索。

表・グラフ

様々な種類の表やグラフが
用意されており、
ログの俯瞰的な分析が可能。

即時検知

障害やセキュリティ
インシデントの予兆を
リアルタイムで検知。

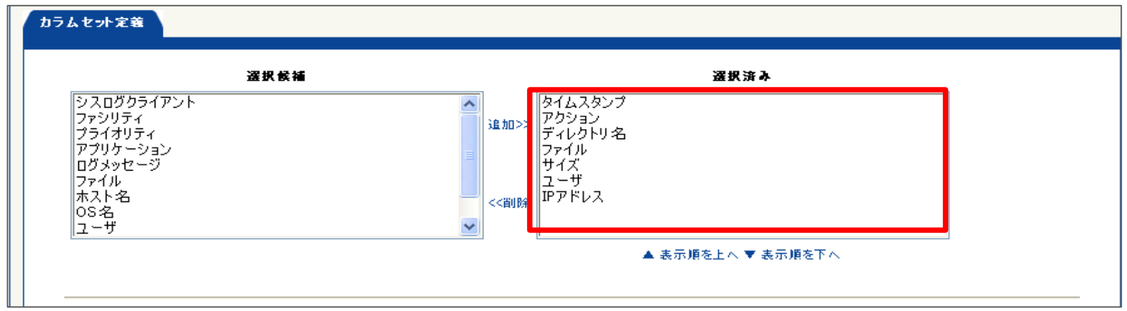
定期レポート

監査やセキュリティ用の
レポートを定期的に自動作成。
モニタリングの負荷を軽減。

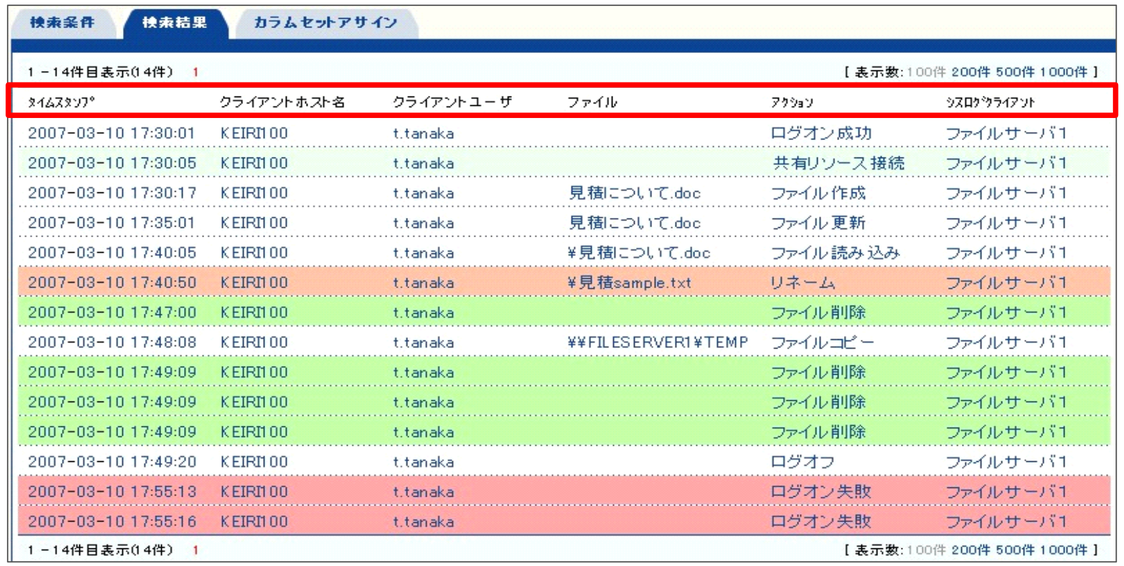
ログの高速検索

大量のログから、指定した条件で即座にログの検索/表示ができます。また、検索結果からクリック操作だけでログの詳細まで追跡できるので、直感的な操作で調査が可能です。

日時や特定のアカウント、アクション、対象アプリケーション名など様々な条件で検索可能



検索結果画面に表示したい項目を選択



検索結果画面が自由にカスタマイズ可能

ログの横断検索

複数のログを紐付けし、検索結果として表示します。単体のログだけでは疑わしくなくても、横断的に見ると疑わしい操作などがわかるようになります。

検索条件名：(2)社員行動追跡

概要：山田太郎さん 6/15の行動追跡

検索条件 | 検索結果 | カラムセットアサイン

1 - 26件目表示(26件) 1

ﾀｲﾑｽﾀﾝﾌﾟ	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	ユーザID	ログメッセージ
2008-06-15 12:49:00	e-SG	カード認証OK(入室)	yamada	e-SG: 8,カード認証OK ,2008/6/15 12:03,yamada 山田　太郎 ,ｶｰﾄﾞ操作記録,ｶｰ
2008-06-15 12:57:00	SmartOn	コンピュータロック解除	yamada	SmartOn: SOL,2008/06/15 12:57 ,2143,2 ,yamada,192.168.0.1,PC01,192.168.1
2008-06-15 13:04:10	CRM	ログイン	yamada	CRM: yamada,山田太郎,ログインしました。
2008-06-15 13:04:11	PISO	SQL監視情報	yamada	PISO(SQL): ""Server132 + Ora102"","server132","ora102","268370208",""
2008-06-15 13:04:13	CRM	顧客リスト選択	yamada	CRM: yamada,顧客リストを選択しました。
2008-06-15 13:04:14	PISO	SQL監視情報	yamada	PISO(SQL): ""Server132 + Ora102"","server132","ora102","268370208",""
2008-06-15 13:06:22	CRM	ログアウト	yamada	CRM: yamada,ログアウトしました。
2008-06-15 15:18:57	SmartOn	コンピュータロック	yamada	SmartOn: SmartOn,SOL,2008/06/15 15:18:57,2141,0,yamada,192.168.0.1,PC0
2008-06-15 15:19:00	e-SG	カード認証OK(退室)	yamada	e-SG: 8,カード認証OK ,2008/6/15 15:19,yamada 山田　太郎 ,ｶｰﾄﾞ操作記録,ｶｰ
2008-06-15 15:32:00	e-SG	カード認証OK(入室)	yamada	e-SG: 8,カード認証OK ,2008/6/15 15:32,yamada 山田　太郎 ,ｶｰﾄﾞ操作記録,ｶｰ
2008-06-15 15:32:00	SmartOn	コンピュータロック解除	yamada	SmartOn: SOL,2008/06/15 15:32 ,2143,2 ,yamada,192.168.0.1,PC01,192.168.1
2008-06-15 15:48:03	ApeosPort-Ⅱ	プリント	yamada	ApeosPort-Ⅱ","ApeosPort-Ⅱ C4300","1 of 1","FX MIB(SOAP)","FUJI XEROX A
2008-06-15 15:51:21	ApeosPort-Ⅱ	プリント	yamada	ApeosPort-Ⅱ","ApeosPort-Ⅱ C4300","1 of 1","FX MIB(SOAP)","FUJI XEROX A
2008-06-15 15:55:10	ApeosPort-Ⅱ	プリント	yamada	ApeosPort-Ⅱ","ApeosPort-Ⅱ C4300","1 of 1","FX MIB(SOAP)","FUJI XEROX A
2008-06-15 17:11:21	文録ﾞ	ワークシートの参照	yamada	BunLog:19808 2008/06/15 17:11:21 yamada DOMAIN1 PC001 192.168.0.1 A0
2008-06-15 17:11:35	文録ﾞ	ワークシートの内容変更	yamada	BunLog:19812 2008/06/15 17:11:35 yamada DOMAIN1 PC001 192.168.0.1 A0
2008-06-15 17:11:49	文録ﾞ	印刷(プレビュー含)	yamada	BunLog:19815 2008/06/15 17:11:49 yamada DOMAIN1 PC001 192.168.0.1 A0
2008-06-15 17:11:50	ApeosPort-Ⅱ	プリント	yamada	ApeosPort-Ⅱ","ApeosPort-Ⅱ C4300","1 of 1","FX MIB(SOAP)","FUJI XEROX A
2008-06-15 17:12:05	文録ﾞ	ブックの保存	yamada	BunLog:19818 2008/06/15 17:12:05 yamada DOMAIN1 PC001 192.168.0.1 A0

オフィスへの入室カード認証　OK

顧客管理システム(CRM)へログイン

顧客管理システム(CRM)からログアウト

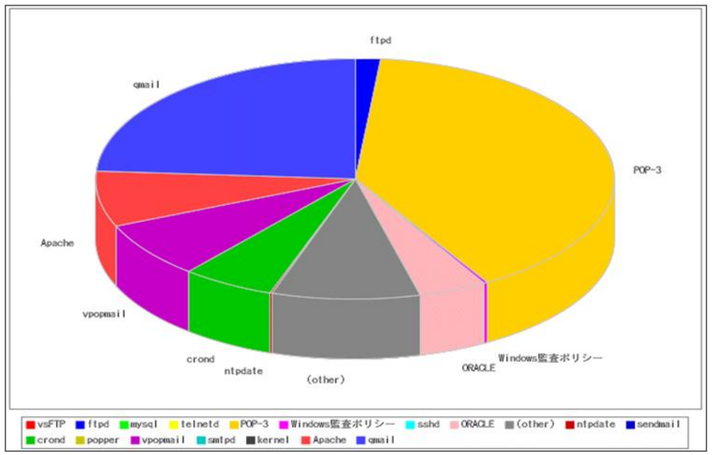
パートナーリストを印刷

パートナーリストデータを変更

入退室管理、Windows認証、CRMシステム、印刷などの複数ログを横串検索

ログの集計機能

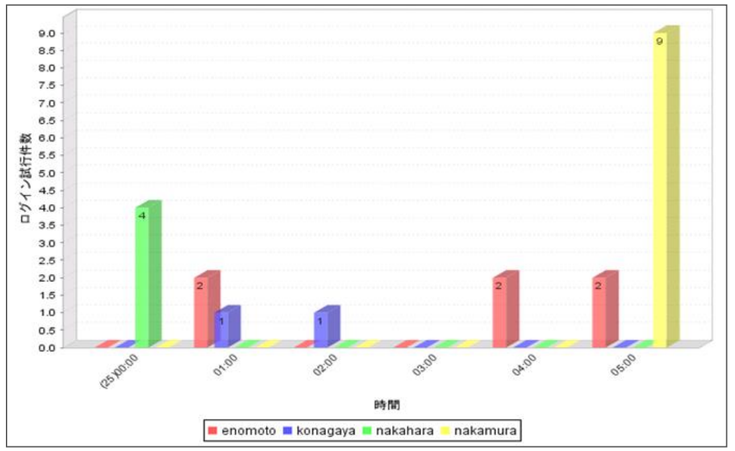
ユーザごとのログイン回数や日時別のアラート発生件数など、縦軸と横軸に任意の項目を設定し、あらゆる角度からログを分析できます。また、円グラフや折れ線グラフ、棒グラフなど様々な表示形式で、視覚的にもわかりやすく集計します。



ログイン回数の割合(ユーザ毎)

時間	ユーザID	アクセス回数
		件数
1/25	enomoto	10
	nakamura	5
	sone	5
	nakahara	3
	kawahara	1
	konagaya	1

時間帯別のログイン実行回数(ユーザ毎)



時間帯別のログイン実行回数(ユーザ毎)

即時検知機能

特定のログの発生頻度による検知や、あらかじめ指定した条件/シナリオにマッチするログの発生を検知するなど、
きめ細かい条件で検知できます。検知後のアクションも、メールやSNMPトラップ、コマンド実行があり、発生した事象をすばやく把握し、対策することが可能です。

即時検知の条件設定

- ログの発生頻度による検知
- 異なる種類の複数ログの組み合わせによる検知
- シナリオによる高度な検知
  (例)事象Aが1分間に5回起きた後に、事象Bが起きれば検知
- 時間や曜日別に検知

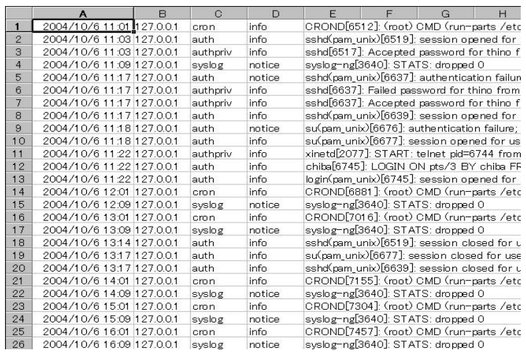
検知後のアクション

- メール
- SNMPトラップ
- 外部コマンドの実行

レポート作成機能

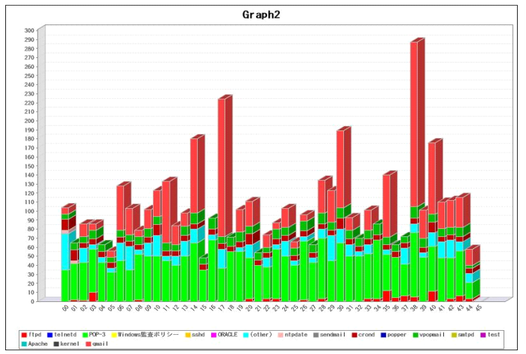
PCIDSSや内部統制、監査対応など、目的に合わせたレポートを作成します。また、検索/集計結果のレポートを定期的に作成し、メールで送付できるので、日々の継続的なモニタリングが容易になります。

- 定期的な実行 （時間毎、日毎、週毎、月毎）
- 多様な出力フォーマットに対応 （CSV、PDF、HTMLなど）
- 作成されたレポートのメール配信
- レポート出力条件を保管して作業を定型化
- XSLTによるカスタムレポート
- 外部レポートエンジンとの連携
- コマンドからのレポート作成

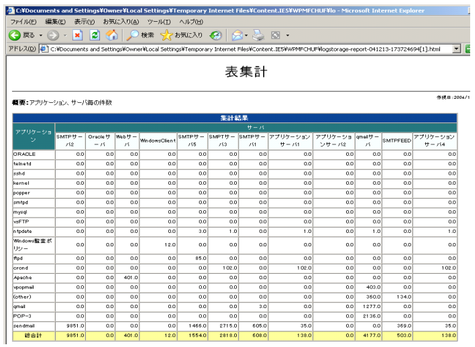


	A	B	C	D	E
1	2004/10/6 11:01	127.0.0.1	cron	info	CROND[6512]: (root) CMD (run-parts /etc
2	2004/10/6 11:03	127.0.0.1	auth	info	sshd(pam_unix)[6519]: session opened for
3	2004/10/6 11:03	127.0.0.1	authpriv	info	sshd[6517]: Accepted password for thino f
4	2004/10/6 11:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0
5	2004/10/6 11:17	127.0.0.1	auth	notice	sshd(pam_unix)[6637]: authentication failun
6	2004/10/6 11:17	127.0.0.1	authpriv	info	sshd[6637]: Failed password for thino from
7	2004/10/6 11:17	127.0.0.1	authpriv	info	sshd[6637]: Accepted password for thino f
8	2004/10/6 11:17	127.0.0.1	auth	info	sshd(pam_unix)[6639]: session opened for
9	2004/10/6 11:18	127.0.0.1	auth	notice	su(pam_unix)[6676]: authentication failure;
10	2004/10/6 11:18	127.0.0.1	auth	info	su(pam_unix)[6677]: session opened for us
11	2004/10/6 11:22	127.0.0.1	authpriv	info	xinetd[2077]: START: telnet pid=6744 from
12	2004/10/6 11:22	127.0.0.1	auth	info	chiba[6745]: LOGIN ON pts/3 BY chiba FF
13	2004/10/6 11:22	127.0.0.1	auth	info	login(pam_unix)[6745]: session opened for
14	2004/10/6 12:01	127.0.0.1	cron	info	CROND[6881]: (root) CMD (run-parts /etc
15	2004/10/6 12:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0
16	2004/10/6 13:01	127.0.0.1	cron	info	CROND[7016]: (root) CMD (run-parts /etc
17	2004/10/6 13:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0
18	2004/10/6 13:14	127.0.0.1	auth	info	sshd(pam_unix)[6519]: session closed for u
19	2004/10/6 13:17	127.0.0.1	auth	info	su(pam_unix)[6677]: session closed for use
20	2004/10/6 13:17	127.0.0.1	auth	info	sshd(pam_unix)[6639]: session closed for u
21	2004/10/6 14:01	127.0.0.1	cron	info	CROND[7155]: (root) CMD (run-parts /etc
22	2004/10/6 14:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0
23	2004/10/6 15:01	127.0.0.1	cron	info	CROND[7304]: (root) CMD (run-parts /etc
24	2004/10/6 15:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0
25	2004/10/6 16:01	127.0.0.1	cron	info	CROND[7457]: (root) CMD (run-parts /etc
26	2004/10/6 16:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0

CSV出力



PDF出力

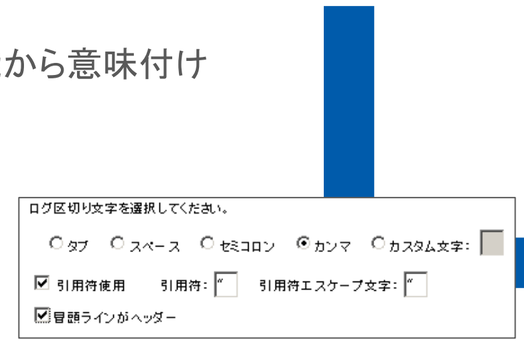


HTML出力

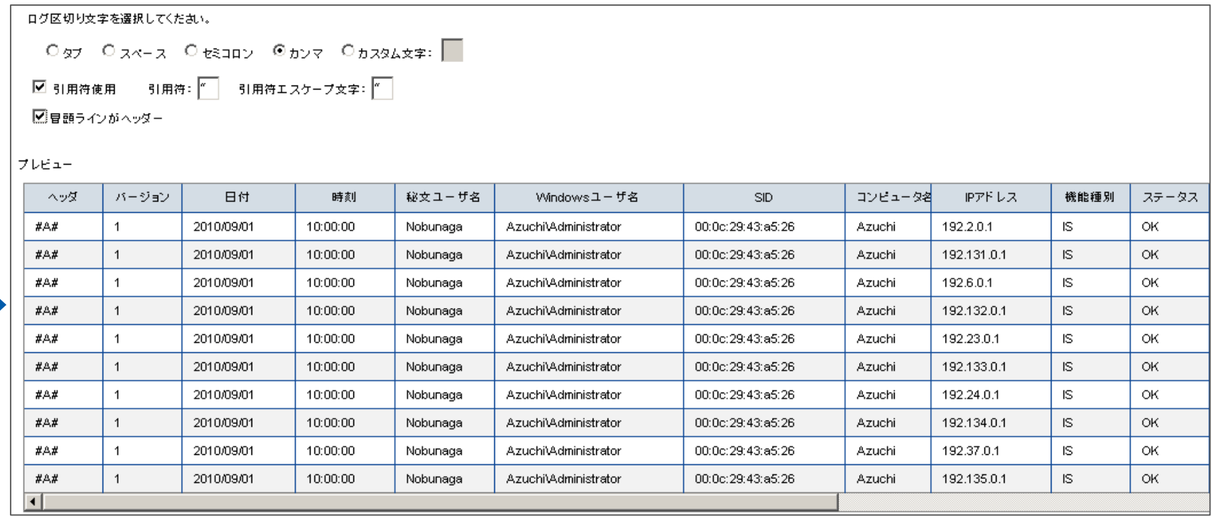
ログフォーマット管理機能

そのままではわかりづらいログを、意味のわかる形にする機能です。正規表現もしくは、ウィザード機能で簡単に定義することができます。

文字の羅列であるログを、
正規表現もしくはウィザード機能から意味付け



ウィザード機能



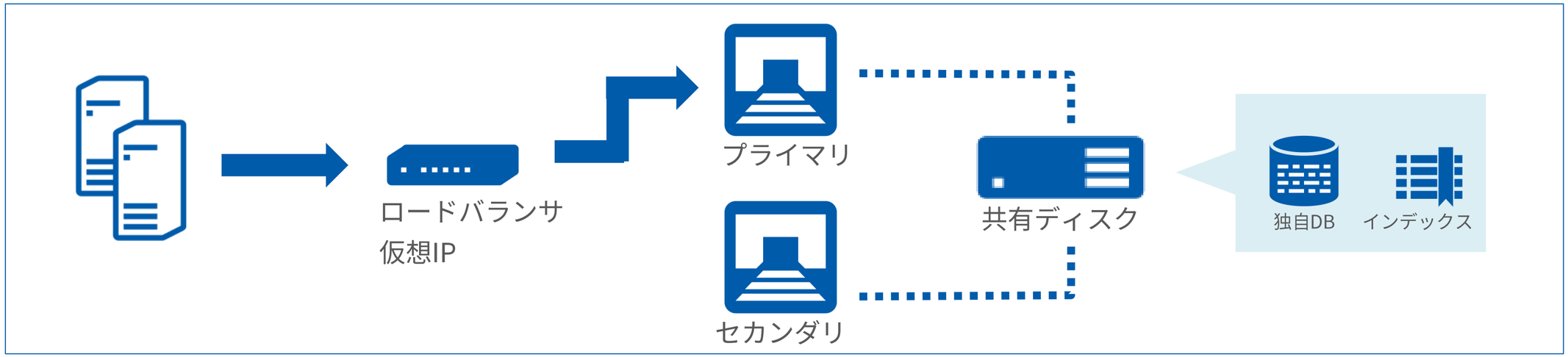
ヘッダ	バージョン	日付	時刻	秘文ユーザ名	Windowsユーザ名	SID	コンピュータ名	IPアドレス	機能種別	ステータス
#A#	1	2010/09/01	10:00:00	Nobunaga	Azuchi\Administrator	00:0c:29:43:a5:26	Azuchi	192.2.0.1	IS	OK
#A#	1	2010/09/01	10:00:00	Nobunaga	Azuchi\Administrator	00:0c:29:43:a5:26	Azuchi	192.131.0.1	IS	OK
#A#	1	2010/09/01	10:00:00	Nobunaga	Azuchi\Administrator	00:0c:29:43:a5:26	Azuchi	192.6.0.1	IS	OK
#A#	1	2010/09/01	10:00:00	Nobunaga	Azuchi\Administrator	00:0c:29:43:a5:26	Azuchi	192.132.0.1	IS	OK
#A#	1	2010/09/01	10:00:00	Nobunaga	Azuchi\Administrator	00:0c:29:43:a5:26	Azuchi	192.23.0.1	IS	OK
#A#	1	2010/09/01	10:00:00	Nobunaga	Azuchi\Administrator	00:0c:29:43:a5:26	Azuchi	192.133.0.1	IS	OK
#A#	1	2010/09/01	10:00:00	Nobunaga	Azuchi\Administrator	00:0c:29:43:a5:26	Azuchi	192.24.0.1	IS	OK
#A#	1	2010/09/01	10:00:00	Nobunaga	Azuchi\Administrator	00:0c:29:43:a5:26	Azuchi	192.134.0.1	IS	OK
#A#	1	2010/09/01	10:00:00	Nobunaga	Azuchi\Administrator	00:0c:29:43:a5:26	Azuchi	192.37.0.1	IS	OK
#A#	1	2010/09/01	10:00:00	Nobunaga	Azuchi\Administrator	00:0c:29:43:a5:26	Azuchi	192.135.0.1	IS	OK

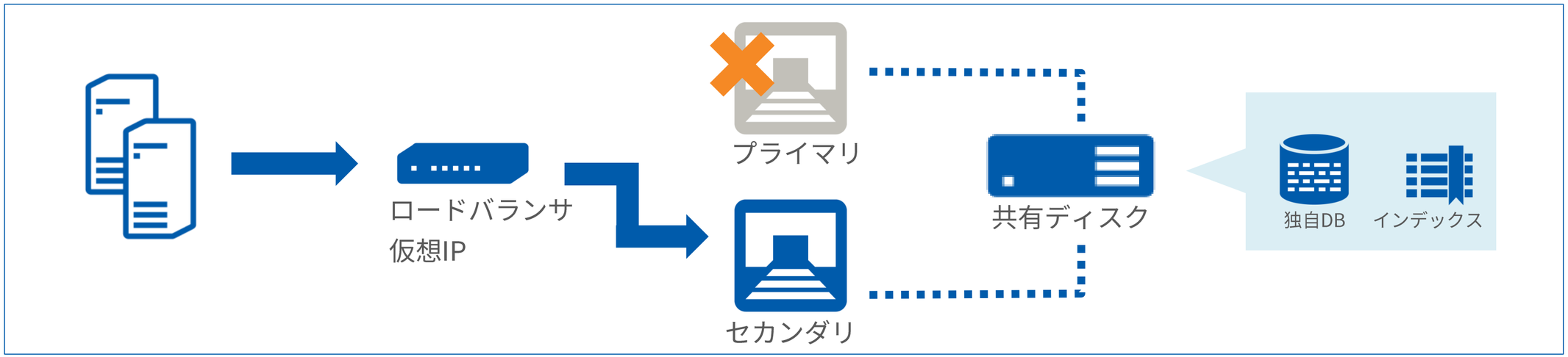
- アプリケーション(ログの種類)を識別
- アクション(アプリケーションの動作)を識別
- メッセージパラメータ(ログに出力されるIPアドレス、ユーザIDなど)を識別

冗長化/負荷分散構成

Logstorageの冗長化構成について

LogGateサーバはプライマリ/セカンダリ構成を取ることが可能です。プライマリのLogGateが障害などで停止した場合、
セカンダリがプライマリに昇格しログを受信します。システム全体でログを受信し続けられるような構成が可能です。

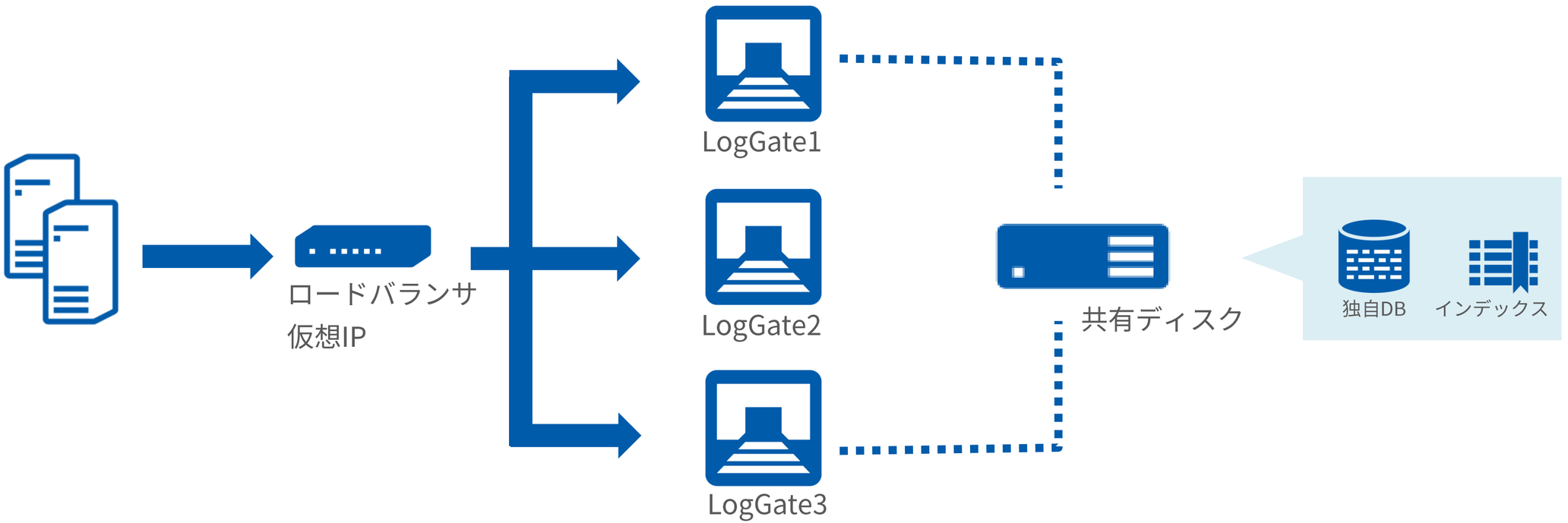




※ロードバランサ、仮想IP、共有ディスクは必須ではありません。それらを利用せずに冗長化構成をとることも可能です。

Logstorageの負荷分散構成について

Logstorageのエディションによっては負荷分散構成が可能です。LogGate1台あたり受信できるログ量は最大秒間3000行です。
それ以上の受信量となった場合はLogGateの台数を増やして負荷分散構成を取ります。

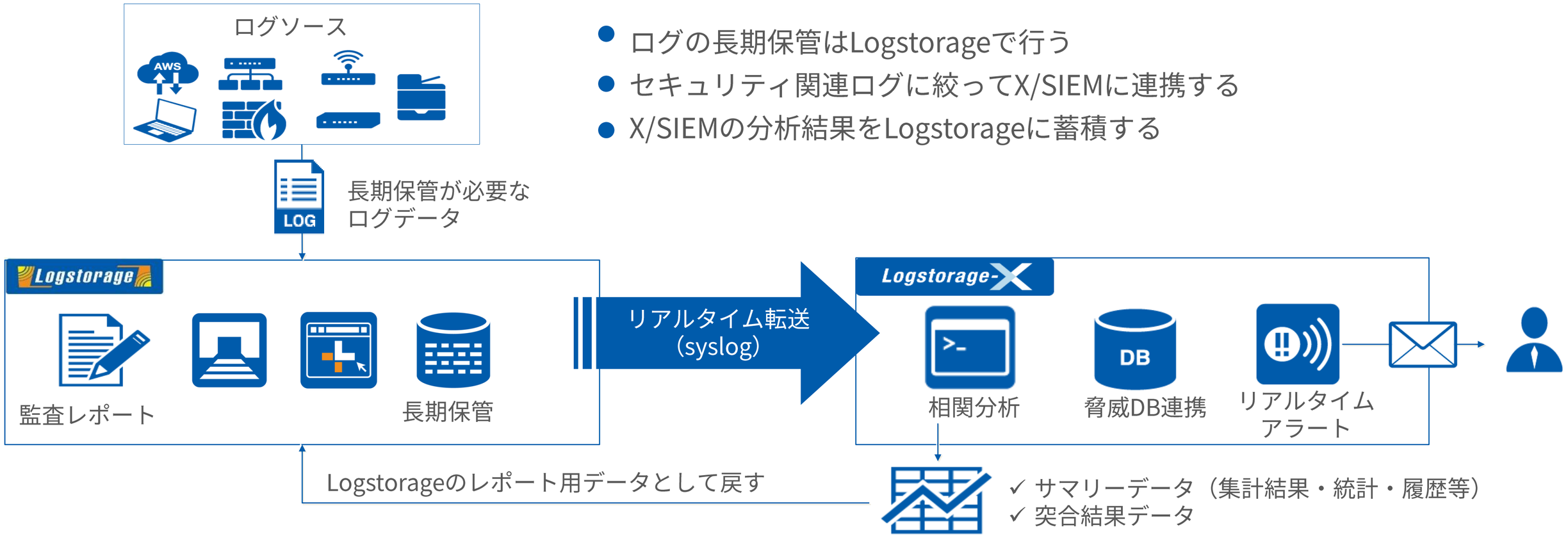


※ロードバランサ、仮想IP、共有ディスクは必須ではありません。それらを利用せずに負荷分散構成をとることも可能です。

SIEM製品との連携機能

LogGateは受信したログのSyslog転送やファイル出力が可能なため、SIEM製品や監視製品と連携できます。フィルタがかけられるため、必要なデータのみを連携します。

Logstorage　⇒　Logstorage X/SIEM の連携イメージ

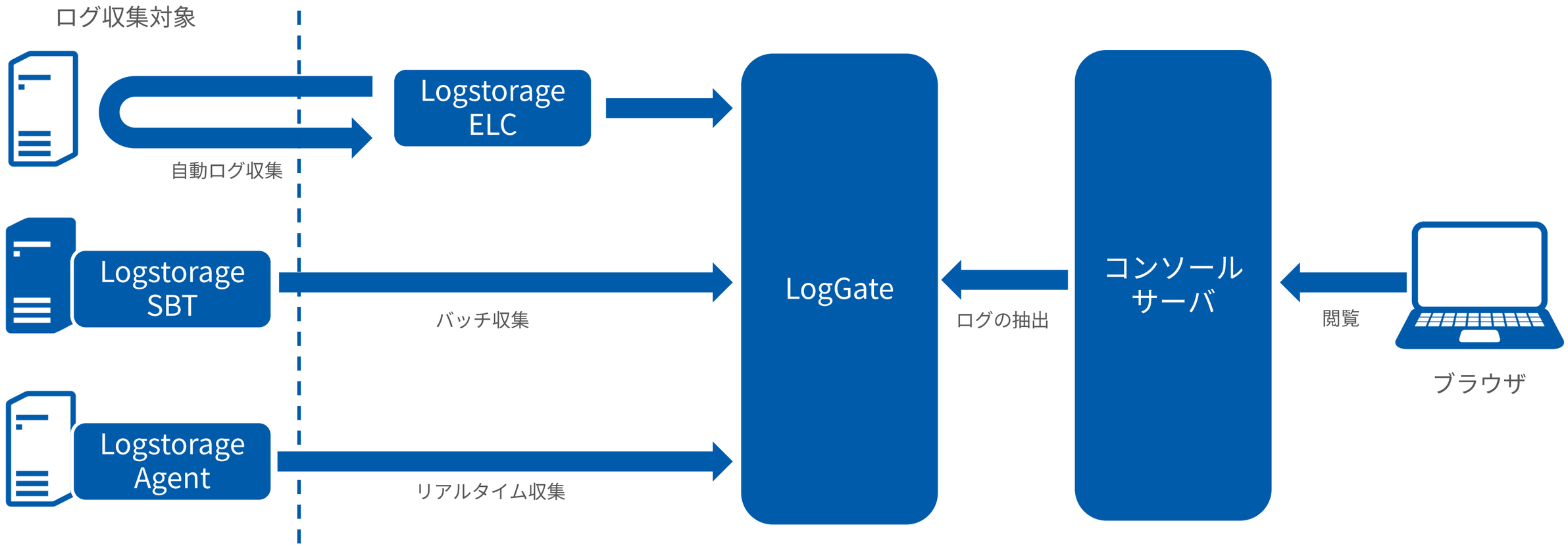


- ログの長期保管はLogstorageで行う
- セキュリティ関連ログに絞ってX/SIEMに連携する
- X/SIEMの分析結果をLogstorageに蓄積する

Logstorageのシステム要件

Logstorageのシステム要件

Logstorageのモジュールについて、それぞれのシステム要件を次のページより記載します。



※LogGateとコンソールサーバは同一筐体で動作可能です
※LogGateの導入OSがWindowsであれば、Logstorage EventLogCollector (ELC)も同一筐体で動作可能です
※Logstorage SecureBatchTransfer (SBT)とLogstorage Agentはログ収集対象に導入します
※Logstorage EventLogCollector (ELC)は、VMWare/ストレージ/Windows Serverのイベントログをリモートから収集します

LogGate 対応プラットフォーム

OS	バージョン
Windows	Windows Server 2008 R2 SP1版 (64bit版) Windows Server 2012 (64bit 版) Windows Server 2012 R2 (64bit版) Windows Server 2016 (64bit版) Windows Server 2019 (64bit版) ※Windows Server Core には対応しておりません。
Linux	Red Hat Enterprise Linux 5.5以上, 6.x , 7.x (64bit版)

※仮想化環境上で動作する場合も、仮想化環境固有の問題を除いてサポートをご提供致します。
※クラウド環境上でRed Hat EnterpriseLinuxを利用する場合、7.5以上をご利用ください。

コンソールサーバ対応プラットフォーム

OS	バージョン
Windows	Windows Server 2008 R2 SP1版 (64bit版) Windows Server 2012 (64bit 版) Windows Server 2012 R2 (64bit版) Windows Server 2016 (64bit版) Windows Server 2019 (64bit版) ※Windows Server Core には対応しておりません。
Linux	Red Hat Enterprise Linux 5.5以上, 6.x , 7.x (64bit版)

※仮想化環境上で動作する場合も、仮想化環境固有の問題を除いてサポートをご提供致します。
※クラウド環境上でRed Hat Enterprise Linuxを利用する場合、7.5以上をご利用ください。

種類	要件
対応Webブラウザ	Internet Explorer 11 Mozilla Firefox (製品リリース時点での最新版) Google Chrome (製品リリース時点での最新版) Microsoft Edge (製品リリース時点での最新版)

※ブラウザでcookie の設定を有効にする必要があります。

LogGate/コンソールサーバ 推奨スペック(共通)

種類	要件
CPU	インテル互換CPU 2.0GHｚ以上 コア数4コア以上
メモリ	2GB以上 (コンソールサーバ単体の場合) 8GB以上 (LogGate単体の場合) 2GB以上 (管理データベース単体の場合) 10GB以上 (コンソールサーバおよびLogGateを同居させる場合) 12GB以上 (コンソールサーバおよびLogGateを同居させ、かつ 管理データベースを同一サーバ上で外部起動する場合)
ディスク	OS領域 (Logstorageインストール領域)：10GB ※ログ蓄積領域：保管要件に依存

Agent対応プラットフォーム（Windows）

OS	バージョン
Windows	Windows 7 SP1 (32bit版/64bit版) Windows 8.1 (32bit版/64bit版) Windows 10 (32bit版/64bit版) Windows Server 2008 SP2 (32bit版/64bit版) Windows Server 2008 R2 SP1 (64bit版) Windows Server 2012 (64bit版) Windows Server 2012 R2 (64bit版) Windows Server 2016 (64bit版) Windows Storage Server 2008 R2 SP1(64bit版) Windows Storage Server 2012 (64bit版) Windows Storage Server 2012 R2 (64bit版) Windows Storage Server 2016 (64bit版) Windows Server 2019 (64bit版) ※ 各サーバOSのServer Coreインストールには対応していません。

※仮想化環境上で動作する場合も、仮想化環境固有の問題を除いてサポートをご提供致します。
※ Logstorage AgentはJREを使用します。使用するJREのバージョンは弊社 技術にお問い合わせください。

Agent対応プラットフォーム（Linux/UNIX）

OS	バージョン
Linux/Unix	Red Hat Enterprise Linux 5（32bit版/64bit版） Red Hat Enterprise Linux 6（32bit版/64bit版） Red Hat Enterprise Linux 7（64bit版） Ubuntu Linux 14.04 (32bit版/64bit版) HP-UX 11i v3 Oracle Solaris 10 (sparc) Oracle Solaris 10 (intel) Oracle Solaris 11 (sparc) Oracle Solaris 11 (intel)

※仮想化環境上で動作する場合も、仮想化環境固有の問題を除いてサポートをご提供致します。
※ Logstorage AgentはJREを使用します。使用するJREのバージョンは弊社 技術にお問い合わせください。

SecureBatchTransfer対応プラットフォーム

OS	バージョン
Windows	Windows 7 SP1 (32bit版/64bit版) Windows 8.1 (32bit版/64bit版) Windows 10 (32bit版/64bit版) Windows Server 2008 R2 SP1 (64bit版) Windows Server 2012 (64bit版) Windows Server 2012 R2 (64bit版) Windows Server 2016 (64bit版) Windows Storage Server 2008 R2 SP1 (64bit版) Windows Storage Server 2012 (64bit版) Windows Storage Server 2012 R2 (64bit版) Windows Storage Server 2016 (64bit版) Windows Server 2019 (64bit版) ※Server Coreインストールには対応していません。
Linux/Unix	Red Hat Enterprise Linux 5.5以上 (32bit版/64bit版) Red Hat Enterprise Linux 6 (32bit版/64bit版) Red Hat Enterprise Linux 7 (64bit版)

※仮想化環境上で動作する場合も、仮想化環境固有の問題を除いてサポートをご提供致します。

EventLogCollector 対応プラットフォーム

OS	バージョン
Windows	Windows Server 2008 R2 SP1 (64bit版) Windows Server 2012 (64bit版) Windows Server 2012 R2 (64bit版) Windows Server 2016 (64bit版) Windows Server 2019 (64bit版) ※ Windows Server Core には対応しておりません。

※仮想化環境上で動作する場合も、仮想化環境固有の問題を除いてサポートをご提供致します。

EventLogCollector 推奨スペック

種類	要件
CPU	Intel互換CPU 2.5GHz 以上 コア数4コア以上
メモリ	4GB以上
ディスク	EventLogCollectorインストール領域：1GB

EventLogCollector 対応ログソース（1/2）

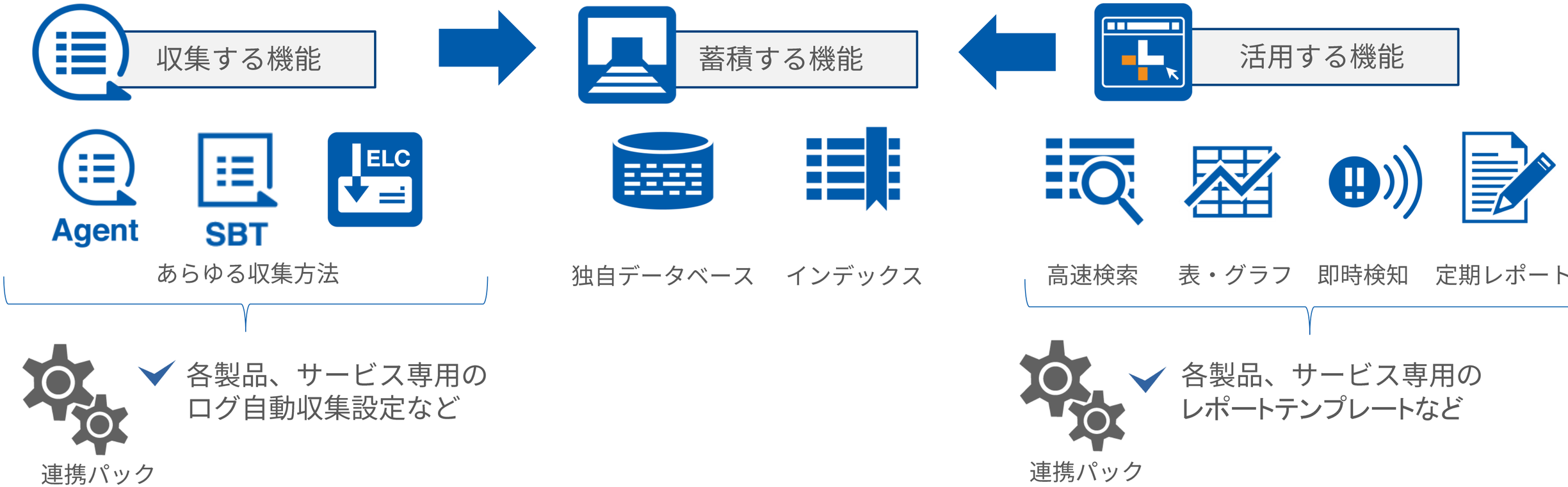
OS	バージョン
Windows	Windows 7 SP1 (32bit版/64bit版) Windows 8.1 (32bit版/64bit版) Windows 10 (32bit版/64bit版) Windows Server 2008 R2 SP1 (64bit版) Windows Server 2012 (64bit版) Windows Server 2012 R2 (64bit版) Windows Server 2016 (64bit版) Windows Storage Server 2008 R2 SP1 (64bit版) Windows Storage Server 2012 (64bit版) Windows Storage Server 2012 R2 (64bit版) Windows Storage Server 2016 (64bit版) Windows Server 2019 (64bit版) ※Server Coreインストールには対応していません。
NetApp イベント/ステータス (7モード)	Data ONTAP 8.2/8.2.1/8.2.2/8.2.3/8.2.4
NetApp (クラスタモード)	Data ONTAP 8.2.1/8.2.2/8.2.3/8.2.4 Data ONTAP 8.3/8.3.1/8.3.2※ Data ONTAP 9.0/9.1※ ※監査ログの解析はファイルアクセス(file-ops)にのみ対応しています。 その他監査ログには未対応です。

EventLogCollector 対応ログソース（2/2）

OS	バージョン
EMC	DART 6.0/7.1 DART(VDM) 7.1 VNX 7.0/7.1/8.1 VNX(VDM) 7.1 VNXe OE 2.1/2.4 Unity 4.0.0/4.0.1/4.0.2/4.1.0/4.1.2※ ※Unity全シリーズ(All Flush/Hybrid/UnityVSA)をサポートしています。
VMware	vCenter Server Ver.5.0/Ver.5.1/Ver.5.5 vCenter Server Ver.6.0 /Ver.6.5 ESXi Ver.5.0/Ver.5.1/Ver.5.5 ESXi Ver.6.0 /Ver.6.5

Logstorage連携パック

Logstorageには、代表的な製品やサービス向けに、簡易にログ収集/分析ができる連携パックが用意されています。
各製品、サービス専用のログ自動収集設定やなど、ログの管理や活用に必要な定義や設定がセットになっています。
連携パックを利用することで、構築や設定の手間を省くことができます。



Logstorage連携パック製品一覧（2020/4時点）

種類	連携パック	販売元 / 開発元
Amazon Web Service(AWS)ログ収集	AWS	Amazon.com,Inc.
Azure Activity Log収集	Azure	Microsoft Corporation
データベースアクセスログ収集	PISO	株式会社インサイトテクノロジー
データベースアクセスログ収集	SSDB監査	株式会社システムエグゼ
シンクライアント操作ログ収集	IVEX Meta Logger	日本ナレッジ株式会社
ファイルサーバアクセスログ収集	VISUACT	セキュリティフライデー株式会社
クライアント操作ログ・アラートログ収集	LanScope Cat	エムオーテックス株式会社
クライアント操作ログ・アラートログ収集	SKYSEA Client View	Sky株式会社
クライアント操作ログ収集	MylogStar	株式会社ラネクシー
クライアント操作ログ収集	InfoTrace	株式会社ソリトンシステムズ
クライアント操作ログ収集	CWAT	インテリジェント ウェイブ株式会社
クライアント操作ログ収集	Malion	株式会社インターコム
Webアクセスログ収集	i-FILTER	デジタルアーツ株式会社
アクセス管理ログ収集	SecureCube / Access Check	NRIセキュアテクノロジーズ株式会社
ファイアウォールログ収集	Palo Alto Networks next-generation firewalls	パロアルトネットワークス株式会社
G Suiteアクセスログ収集	G Suite	Google LLC

ライセンスの考え方と種類

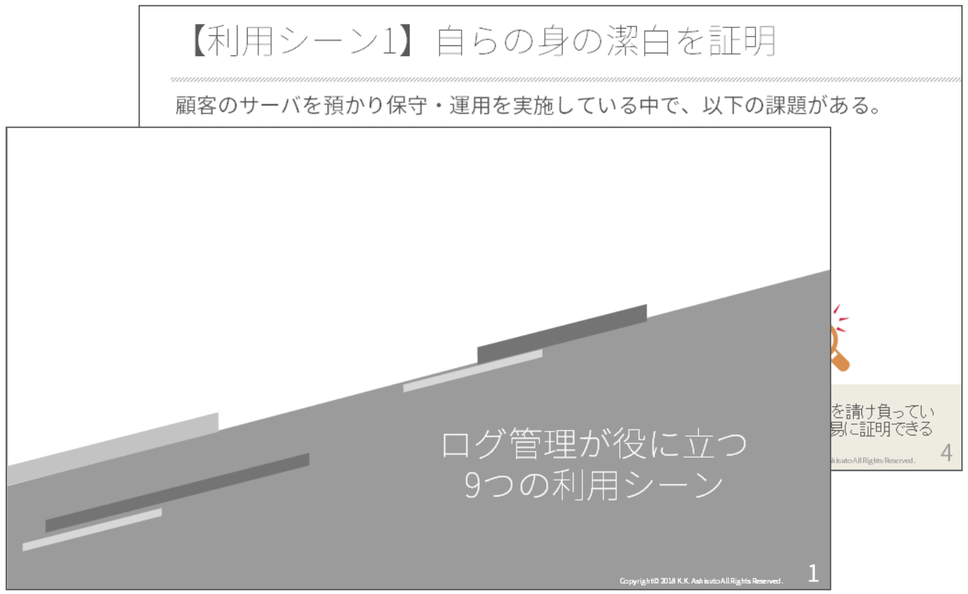
規模に応じて選べる5種類のライセンス

Logstorageは、ログ収集の対象となるサーバ台数と、ログ量に応じてライセンスを選択します。1つのサーバ内に複数種類のログがあり、それぞれ収集方法が違ったとしてもライセンス価格には影響しません

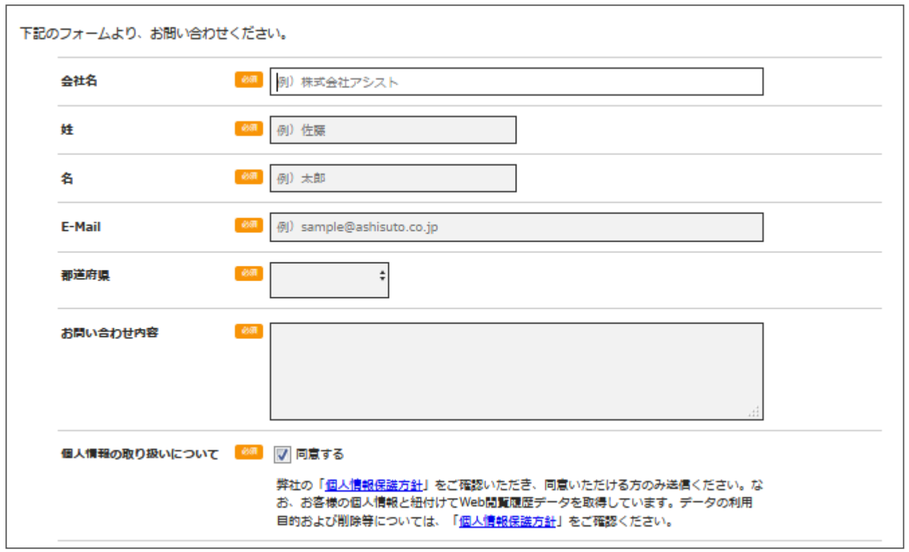
エディション名	LogGate1台が処理できるログ量(1日)	ライセンスに含まれるLogGate台数	ログ収集対象のサーバ台数	集計・検知・レポート機能
ワークグループ	5GB	1台	5台(5台以上は追加ライセンス)	オプション
スタンダード	10GB	1台	5台(5台以上は追加ライセンス)	オプション
エンハンスト	15GB	1台	5台(5台以上は追加ライセンス)	オプション
エンタープライズ	10GB	2台	無制限	込み
アドバンスト	15GB	2台	無制限	オプション

関連資料/概算見積もりサービスのご案内

Logstorageでは、別途、下記のような資料・概算見積もりのサービスをご用意しています。
お気軽にご利用ください。



全てのダウンロード資料を
確認する



概算見積もりを
依頼する

各種お問い合わせ

本資料に関するお問い合わせや、Logstorageに関するご質問、導入のご相談、製品デモンストレーション、お見積りのご依頼など、お気軽にご連絡ください。お客様のご要望に応じて、専任のスタッフが対応させていただきます。

株式会社アシスト　Logstorage　お問い合わせ窓口

＜問い合わせページ＞
https://www.ashisuto.co.jp/pa/contact/logstorage.html