ログ管理　SIEM　パッケージソフト

Logstorage VER.10

統合ログ管理システム「ログストレージ」

統合ログ管理ツール分野シェア
No.1
18年連続

出典：デロイト トーマツ ミック経済研究所2025年3月発刊
内部脅威対策ソリューション市場の現状と将来展望 2024年度 （統合ログ管理ツール部門）
出荷本数でシェア51.2%を獲得　https://mic-r.co.jp/mr/03370/

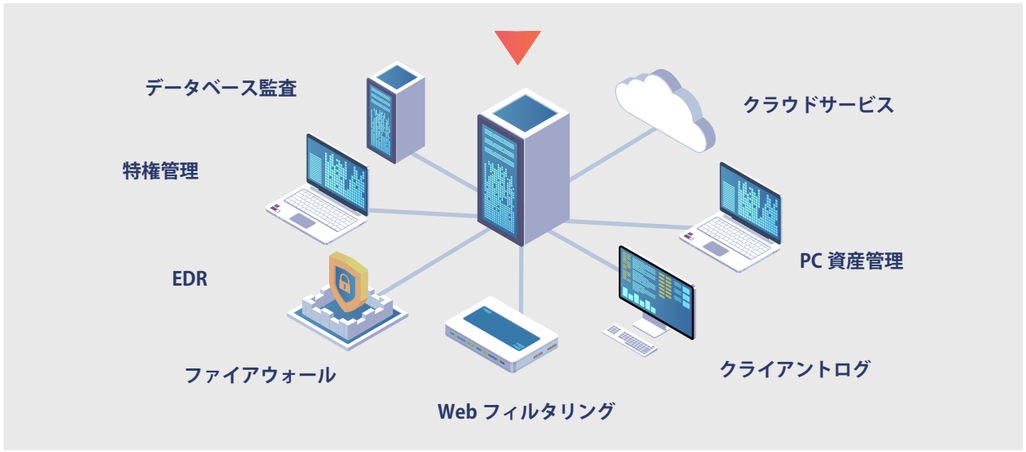
企業活動のあらゆるログを統合管理

なんでも 収集　安全に 保管　条件設定で 通知　すばやく 検索　わかりやすく 集計　自動で レポート

企業活動のあらゆるログを統合管理

Logstorage

情報システムのプロによる、情報システムのプロのための、ログの「収集・保管・分析」ソリューション



情報システムはビジネスの成長と安定を支える重要な経営基盤です。
Logstorageは、国内のさまざまな情報システムに導入され、その信頼性を支えてきました。

Security[560]: [7494782, 成功の監査, Thu Mar 14 13:52:54, YAMADA-WORK\yamada, YAMADA-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: D:\common\顧客リスト.xlsx ハンドル ID: 3460 操作 ID: {0,53699414} プロセス ID: 1908 イメージ ファイル名: C:\WINDOWS\explorer.exe プライマリ ユーザー名: yamada プライマリ ドメイン: YAMADA-WORK プライマリ ログオン ID: (0x0,0x284A4) 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_CON-

「意味がわからない」「使い方がわからない」専門性が求められるログ分析

"Logstorage" がログを 誰でも・カンタン・便利 に扱えるものにします

- なんでも“収集”
- 安全に“保管”
- 条件設定で“検知”

- すばやく“検索”
- わかりやすく“集計”
- 自動で“レポート”

"Logstorage" が選ばれ続ける理由

01 自由度の高い組み合わせで どんな環境にも使いやすく最適化できるから

- なんでも収集
- 組み合わせで カスタム
- 選べる購入形態

02 情報システムのプロが 使いやすさを重視して製品開発しているから

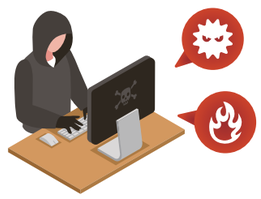
- 分かりやすい UIデザイン
- 専門スキルが いらない
- 低スペック環境 検証

03 純国産メーカーとして 安心感のあるサービスを提供しているから

- 充実の販売・構築 パートナー
- 購入後の 保守サポート
- ISO/IEC 27001 取得企業

2002年の発売開始以来、5,500社以上の導入実績を重ね、18年連続で出荷本数シェア No.1*を獲得。

多様なセキュリティ課題の解決に "Logstorage" が活躍しています



脅威対策

脅威の検出（標的型攻撃／内部情報漏えい）
フォレンジック（攻撃を受けた際の証拠保全）

システム運用

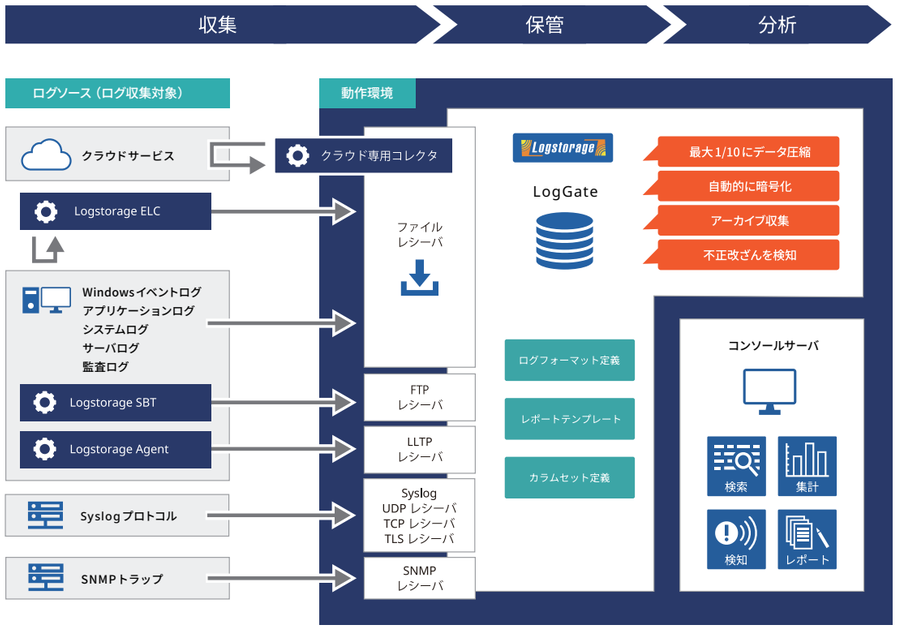
システムの状態把握
障害時の調査、解析

コンプライアンス

各種法令、業界／団体ガイドラインへの
ログ管理要件への充足

ログの収集

オンプレミスからクラウドまで膨大なログを自動収集。
収集先のログの出力方法に合わせて、さまざまなログ収集方式を選ぶことができます。



テキスト形式のログはすべて収集可能。

日本国内で利用されているソフトウェア・機器を中心に400種以上のログの収集実績があります。

ログ収集・管理実績製品（一部）

OS システム・イベント
Windows
Linux
Unix
Solaris
HP-UX
BSD
NetApp
EMC
VMware vCenter
VMware ESXi

Web ／プロキシ
Apache/Tomcat
IIS
Blue Coat
Squid
InfoCage PC検疫
Websense
WebSphere
WebLogic
Cosminexus
Trend Micro Cloud App Security
InterScan Web Security as a Service
Zscaler

サーバアクセス
ALog ConVerter
File Server Audit
CA Access Control
VISUACT

ICカード認証
SmartOn
ARCACLAVIS Revo

運用監視
Nagios
JP1
Systemwalker
OpenView
WebSAM

複合機
imageRUNNER
Apeos
SecurePrint!

ネットワーク機器
FortiGate
SonicWall
BIG-IP
Cisco PIX/ASA
Cisco Catalyst
NetScreen/SSG
VPN-1
FireWall-1
Check Point IP
SSL-VPN
NOKIA IP
Alteon
IronPort
ServerIron
Proventia
CACHATTO

データベース
Oracle
SQL Server
Db2
PostgreSQL
MySQL
Chakra
SecureSphere DMG/DSG
AUDIT MASTER
IPLocks
Guardium

クライアント操作
SEP
QND/QOH

メール
MS Exchange
Sendmail
Postfix
qmail
Exim
GUARDIANWALL

アンチウィルス
Symantec AntiVirus
TrendMicro InterScan
McAfee VirusScan
HDE Anti-Virus
ESET
ウイルスバスター

その他
Lotus Domino
Notes AccessAnalyzer2
Auge AccessWatcher
SAP R/3 (ERP)
eX-SG (入退室管理)
MSIESER
iSecurity
desknet's
HP NonStop サーバー
System Answer

ログの保管

収集したログを安全に長期保管。高圧縮機能でストレージコストを削減。

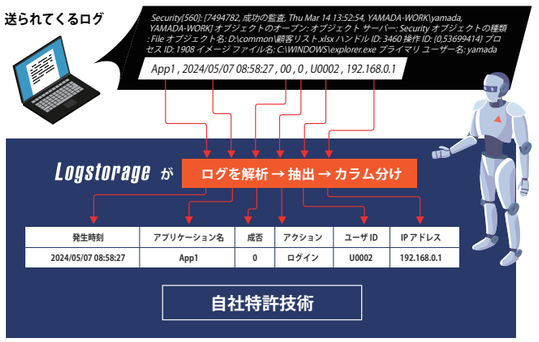
圧縮機能
収集したログを最大で10分の1に圧縮します。
保管用ストレージのコストを低減できます。

暗号化機能
ログを収集と同時に暗号化することで、
ログデータを守ります。

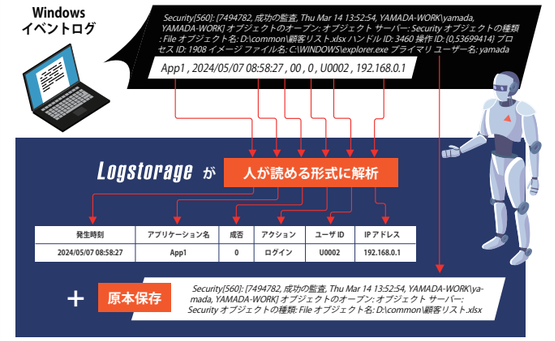
改ざん検出機能
ログのハッシュ値を管理しているため、
改ざん検出が可能です。

アーカイブ機能
OSのスケジューラー等に登録することで、
自動的にアーカイブ、自動削除が可能です。

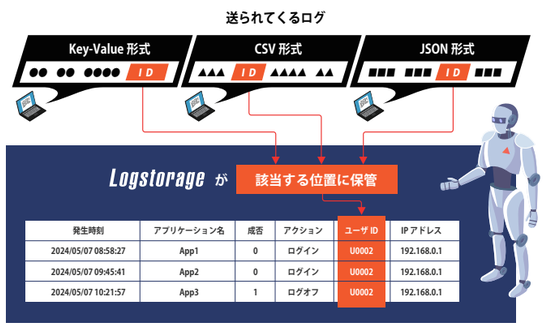
ログフォーマット定義機能
収集したログの項目に対して、意味付けを行う機能です。



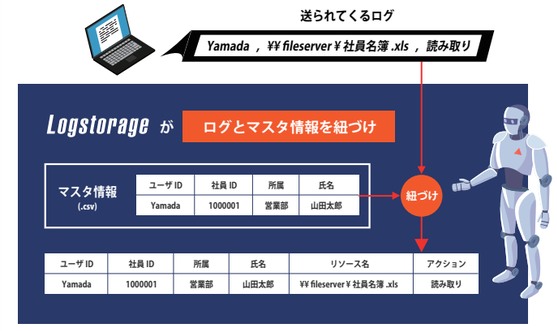
Windowsイベントログ 解析機能
可読性に乏しいWindowsイベントログを人が読める形式に解析します。



ログフォーマット自動解析機能
あらかじめファイル形式を指定しておくと、
収集したログの項目が自動で該当する位置に保管されます。



マスタ連携機能
ログ収集時にログとマスタ情報を紐づけ、ログに含まれない情報を付加できます。



原本性を保ちながら長期保管

ログの分析

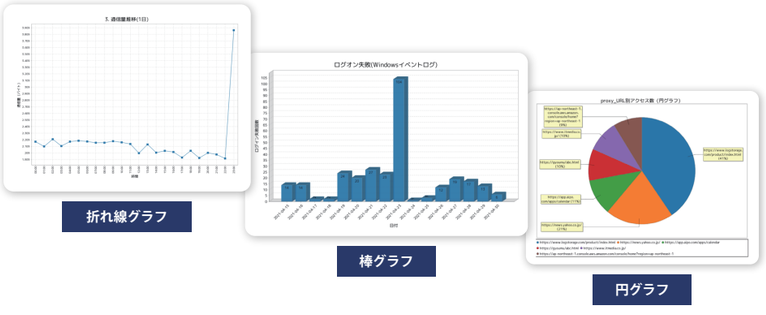
クリック操作で、誰でもカンタンにログ分析できます。

検索機能

検索機能は、収集したログに対して検索を行う
機能です。検索に使用できる条件は
AND/OR を組合わせて指定する事が可能です。
また、よく使われる条件は保存することができ、
その条件を集計やレポートで使う事も可能です。

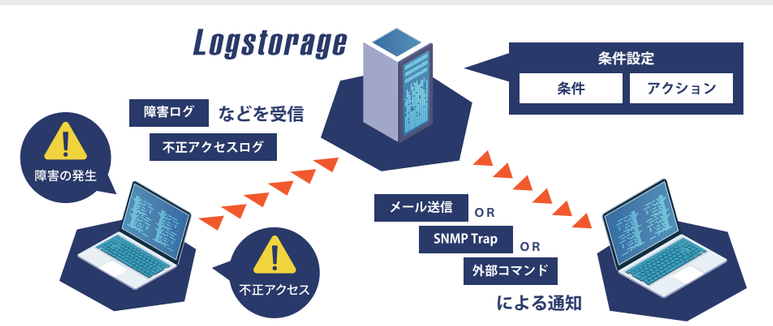
集計機能

集計機能は、収集したログに対して
「縦軸」「横軸」「系列」の3点を指定して、
様々な角度からログの分析を行う機能です。
軸や系列には、収集したログが持つ項目を
指定可能ですので、お客様のニーズに合った
集計条件を柔軟に設定できます。



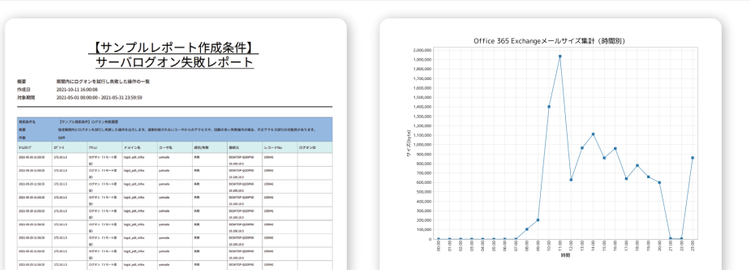
検知機能

検知機能は、システムの異常や不正処理を示すログを
リアルタイムに捉え、アラートを出す機能です。
シナリオに基づいたポリシー設定により誤検知を減らし、
本当に必要なログのみを検知する事が可能です。



レポート機能

レポート機能は、検索・集計・検知履歴をPDFや
HTML形式のレポートとして作成する機能です。
日次・月次などのタイミングで定期的・自動的に
出力できる他、作成したレポートをメールに
添付して自動送信することも可能です。



Insight

高度な分析を高速に実現するインサイト機能

コンソール画面のインサイト・ボードで、ログの統計情報を可視化。
ドリルダウンを始めとする各種機能で、直感的にログが分析できるようサポートします。

インサイト機能一覧

01 ドリルダウン
選択したデータの軸に従って、データの階層を1段階ずつ掘り下げる機能です。

02 タイムシフト比較
異なる期間のデータを同時に表示する機能です。

03 ハイライト
指定した項目のデータを強調表示させる機能です。

04 積み上げ
各項目のデータを1本の棒グラフに積み上げて表示させる機能です。

05 色設定
グラフの色を設定するための機能です。

06 グラフ設定
グラフの表示形式やデータ等を変更するための機能です。

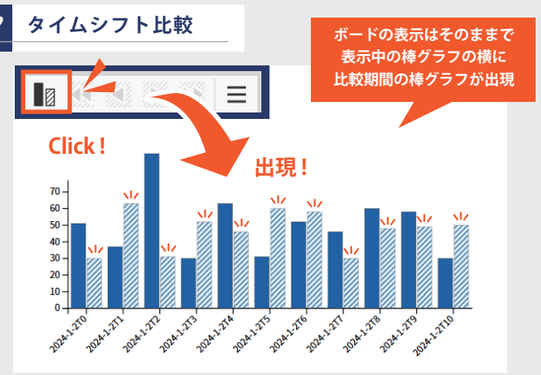
07 ドリルスルー
現在の分析期間・条件でログを検索する機能です。

08 タイトル・コメント編集
グラフのタイトルを編集する機能、グラフカードにコメントをつける機能です。

09 保存機能
インサイト・ボードの各種設定を保存する機能です。

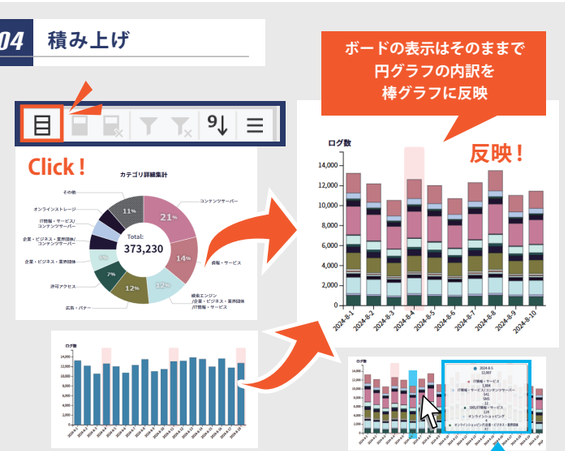
10 ボードリスト
登録したインサイト・ボードをリスト形式で表示します。

02 タイムシフト比較



[期間] の比較作業をカンタンに！

04 積み上げ



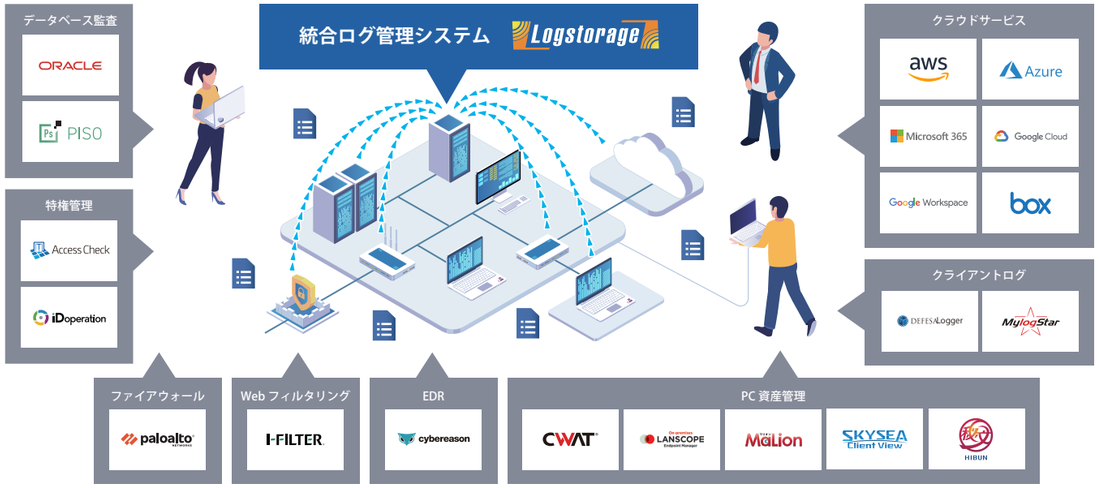
[内訳] の比較作業をカンタンに！

07 ドリルスルー

[詳細] の確認作業をカンタンに！

ログ管理をラクにする多数のオプション

連携製品



※Logstorageはインフォサイエンス株式会社の登録商標です。その他文中の社名、商品名は、各社の商標または登録商標です。

各分野のトップシェア製品と連携した「連携パック」で ログの管理技術を パッケージ提供

連携パック

連携パックは、各分野で人気の製品と連携して開発した「ログの収集・分析がすぐにスタートできる」Logstorageのオプション製品です。
連携パックを導入することで、各連携製品のログ管理のセットアップを簡略化できるほか、運用中に、収集対象のログのフォーマット(並び順や表示の仕方)や出力方法に変更があっても、各連携パックのバージョンアップで、変更を反映できます。

「消えてしまうログ」を 確実に残しておくために

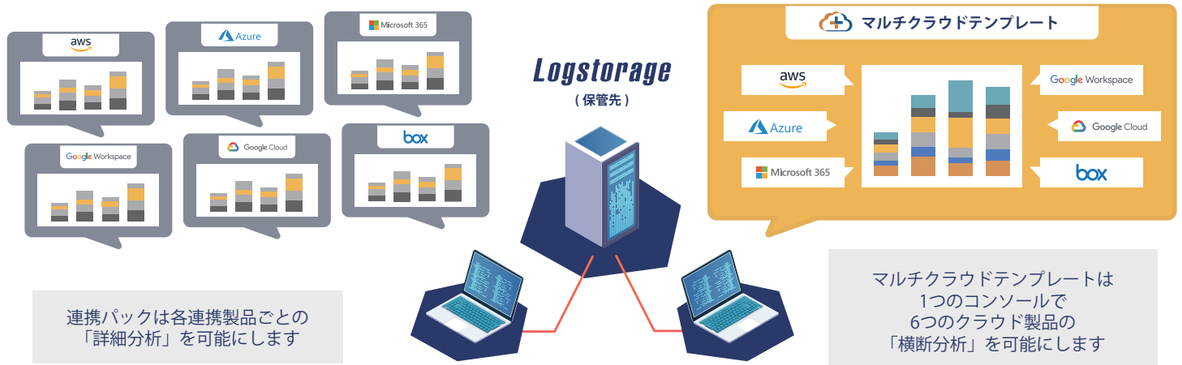
各クラウドのログ保管期間（参考値）
AWS…90日、Azure…90日、GCP…30日、
Microsoft 365…90日、Google Workspace…180日

「出力されるログの内容が変わった」
「アップデートでログの保管先が変わった」
「保管するログのサイズが増えた」
「仕様変更でログの種類が増えた」
「独自の収集プログラムが仕様変更で作り直し」

「技術者のリソースがログ管理に取られすぎる課題」を解決

マルチクラウドテンプレート

クラウドサービスの横断的な管理・分析を可能にします。

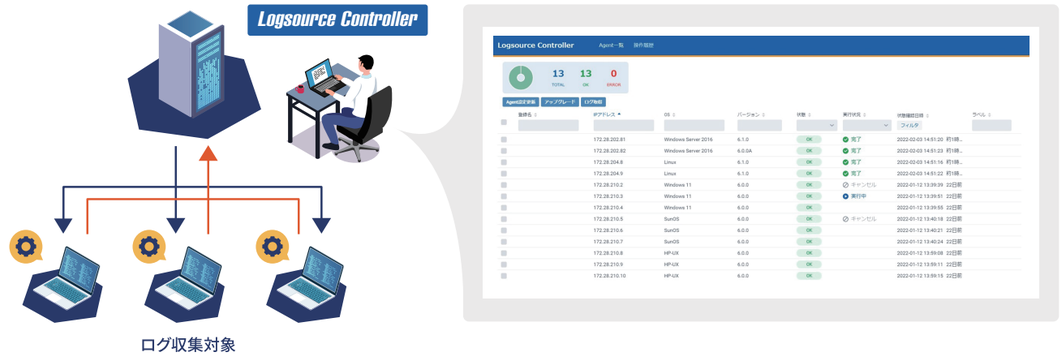


連携パックは各連携製品ごとの「詳細分析」を可能にします

マルチクラウドテンプレートは1つのコンソールで6つのクラウド製品の「横断分析」を可能にします

エージェント集中管理ツール

ログの収集対象に設置するプログラム(エージェント)の情報を、GUIで一括管理できるツールです。



ログ診断レポートサービス

国内トップクラスのホワイトハッカーが、企業の情報システムをサイバー攻撃から守ります。

Logstorageが収集したログを、国内トップクラスのホワイトハッカーが分析。サイバー攻撃をおこなうハッカーの目線で、情報システムのセキュリティの対策状況・脆弱性をレポートするサービスです。

製品導入に関するサポート

販売・構築パートナー

情報システムの課題にトータルで応える販売・構築パートナー

Logstorageは、国内の主要なSIerを販売・構築パートナーとしています。貴社の情報システムで関連する課題にもトータルで応えることができます。

アイビーシー株式会社	株式会社アシスト	株式会社アトミテック
NECソリューションイノベータ株式会社	エヌ・ティ・ティ・アドバンステクノロジ株式会社	NTTテクノクロス株式会社
キヤノンマーケティングジャパン株式会社	ケー・イー・エルテクニカルサービス株式会社	株式会社シーイーシー
CTCエスピー株式会社	株式会社システムエグゼ	大興電子通信株式会社
ダイワボウ情報システム株式会社	TIS株式会社	東芝デジタルエンジニアリング株式会社
日鉄ソリューションズ株式会社	日本ヒューレット・パッカード合同会社	株式会社ネットワールド
PCIソリューションズ株式会社	株式会社日立システムズ	富士電機ITソリューション株式会社
ユニアデックス株式会社		※50音順

試用版ライセンスの提供

Logstorageの試用版ライセンスをHPで受付中。Logstorageを1ヵ月無料でお試しいただけます。

インストールと設定作業をわかりやすくする「チュートリアル動画」でスピーディに検証いただけます。

参考資料の提供

日々変化を続けるセキュリティ要件、導入事例、活用事例のなかで、製品選定の参考に使える情報をまとめてHP上で提供しています。

ホワイトペーパー　導入事例　活用事例

購入後の保守サポート

製品導入後もサポートセンターが運用を支援。

サポートセンターによる対応をはじめ、製品の最新バージョンやパッチ提供、最新のシステム環境に対応する技術情報の提供により、Logstorageのご利用を幅広くご支援いたします。

オンラインセミナー [オンデマンド配信] による製品紹介

Logstorageの実際の製品デモ画面を使ったLogstorage製品ご紹介セミナー、Logstorageによる最新のセキュリティガイドラインへの対応セミナーを、HP上でオンデマンド配信しています。

オンラインセミナー

01 Logstorage製品紹介セミナー

本セミナーでは、統合ログ管理製品の導入目的を踏まえた上で、Logstorageの製品概要をご説明いたします。
実際のデモ画面にて、検索・集計・レポート出力の流れをご覧いただけます。

02 Logstorage クラウド対応 連携製品紹介セミナー

本セミナーでは、クラウド（ AWS, Azure, Box, Microsoft 365, GCP, Google Workspace, Cybereason）のログ監視・可視化に役立つ
Logstorageの活用方法をご紹介いたします。※Logstorage製品紹介セミナーを視聴済みの方を対象としています。

03 PCI DSS v 4.0で求められるログの管理要件に準拠するには

セミナー前半では、PCI DSSv4.0の基礎知識をはじめ、ログの収集、保管、活用に対する課題と対応策について解説いたします。
セミナー後半では、ログ管理と深い関わりを持つ「要件10」について詳しく解説いたします。

04 自工会/部工会 サイバーセキュリティガイドライン対策セミナー

本セミナーでは、自工会/部工会 サイバーセキュリティガイドラインが策定された理由をはじめ、なぜログ管理が重要視されるのか、
ガイドライン中のログ管理要求事項に対して、Logstorageがどのように応えることができるのかについて解説していきます。

05 医療情報システムの安全管理に関するガイドライン対策セミナー

本セミナーでは、医療業界における近年のセキュリティ脅威をはじめ、医療情報システムの安全管理に関するガイドラインの概要、
ガイドライン中のログ要件に対するLogstorageの対応状況などを解説します。

会社概要

会社名：	インフォサイエンス株式会社
所在地：	東京都港区芝浦2-4-1 インフォサイエンスビル
設立：	1995年10月
資本金：	1億円
事業内容：	・セキュリティ関連ソフトウェア製品開発 ・SaaS型クラウドサービス ・データセンター運用
代表者：	代表取締役社長　宮 紀雄

会社沿革

1995年	品川区北品川にて会社を設立。システム運用サービスを開始
1996年	受託システム開発を開始
1999年	メールフィルタリングシステム「Spamghetti」をリリース
2001年	統合ログ管理システム「Logstorage」をリリース
2001年	本社ビルを取得し、本社を港区芝浦に移転
2002年	ネットワークオペレーションズセンター（データセンター）を 北品川から芝浦に移転
2004年	セキュリティ認証「ISMS(Ver.2.0)」と「BS7799-2」を取得
2006年	ISO27001を取得
2008年	資本金を1億円に増資 英賽（大連）信息技術有限公司設立
2013年	Infoscience USA, Inc.設立
2025年	「Logstorage」が18年連続シェアNo.1を獲得*

*市場調査会社「デロイト トーマツ ミック経済研究所株式会社」が発刊した
『内部脅威対策ソリューション市場の現状と将来展望 2024年度（統合ログ管理ツール部門）』において、
18年連続シェアNo.1を達成
（出典：デロイト トーマツ ミック経済研究所2025年3月発刊：内部脅威対策ソリューション市場の
現状と将来展望 2024年度（統合ログ管理ツール部門）出荷本数でシェア51.2%を獲得
https://mic-r.co.jp/mr/03370/）

*市場調査会社「富士キメラ総研」が発刊した
『2024 ネットワークセキュリティ ビジネス調査総覧《市場編》』において、14年連続シェアNo.1を達成
（出典：富士キメラ総研 2011-2024 ネットワークセキュリティ ビジネス調査総覧《市場編》
統合ログ管理ツール（SIM/SIEM）、市場占有率、SIM、金額ベース、2023年度実績、
2010年度-2023年度連続シェアNo.1）

ISO/IEC 27001 を
取得しています。

QUALITY ASSURANCE JIC REGISTERED ORGANIZATION I028-ISO/IEC 27001

ISMS-AC ISMS ISR002

登録組織：ネットワークオペレーションズセンター、プロダクト事業部、アドミニストレーション本部

Logstorage 製品のお問い合わせ先

TEL 03-5427-3503　Mail info@logstorage.com

URL https://logstorage.com/

Infoscience 〒108-0023 東京都港区芝浦 2-4-1 インフォサイエンスビル
インフォサイエンス株式会社（https://www.infoscience.co.jp/）

お問い合わせ先