

AWSのログ管理・分析ツールの決定版

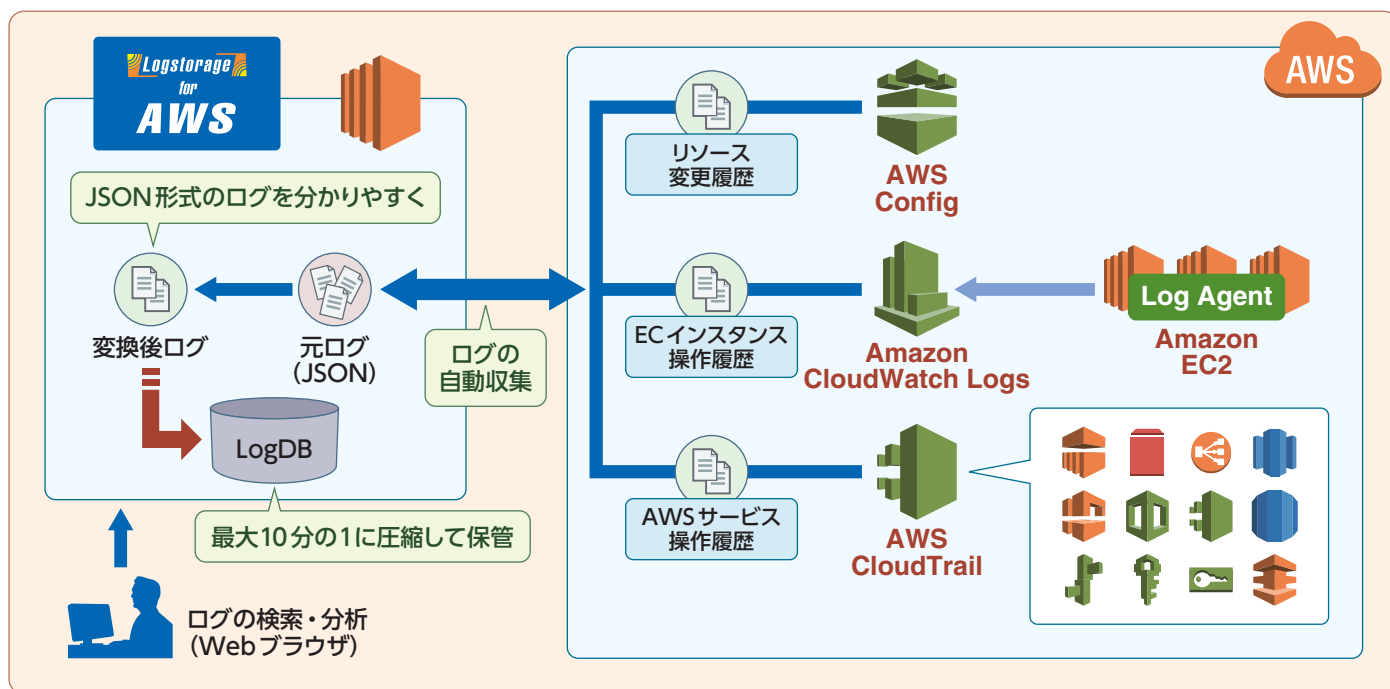


<http://www.logstorage.com/aws/>



○ Logstorage for AWSの特長

Logstorage for AWSは、AWS上で生成されるあらゆるログデータを「収集・解析」「保管」「検索・分析」「レポート」するための、統合ログ管理ツールです。AWS上のリソースのライフサイクルの管理、コンプライアンス準拠、セキュリティ分析、運用上のトラブルシューティングなど、幅広く活用することができます。



収集・解析

- ・AWSの各サービスからのログ自動収集
- ・JSON形式のログの解析／変換

保管

- ・ログの圧縮保存／高速検索機能
- ・ログの暗号化／改ざんチェック機能
- ・ログの自動アーカイブ機能

検索・分析

- ・ログの検索／集計／レポート
- ・検索結果からクリック操作による絞込み
- ・レポートの定期自動出力

AWS上のログに関わる主要サービスに対応！

Logstorage for AWSは、AWS上のシステムの利用状況の把握や監査を行うために必要なデータを提供する、下記のサービスに対応しています。



AWS CloudTrail

AWS APIの呼び出しを記録し、ログファイルを提供するサービスです。



AWS Config

AWS上のリソースの構成変更の通知、構成履歴、インベントリーを提供するサービスです。



Amazon CloudWatch Logs

Amazon EC2インスタンス上のログ（イベントログ／syslogなど）を保存・提供するサービスです。



AWSのログを分かり易く！

AWSのサービスが出力するJSON形式のログは、そのままでは内容の理解が困難です。
ログを正しく分析・監査する為には、ログを適切に変換し、可視化するための仕組みが必須です。

```
"Records":[{"eventVersion":"1.02","userIdentity":
{"type":"IAMUser","principalId":"ABCDEFGHIJKLMNQRSTU","arn":"arn:aws:iam::999999999999:user/yamada","ac
countId":"999999999999","userName":"yamada"},"eventTime":"2015-04-27T00:03:14Z","eventSource":"signin.ama
zonaws.com","eventName":"ConsoleLogin","awsRegion":"us-east-1","sourceIPAddress":"192.168.0.1","userAgent
":"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90
Safari/537.36","requestParameters":null,"responseElements":
{"ConsoleLogin":"Success"},"additionalEventData":
{"LoginTo":"https://console.aws.amazon.com/console/home","MobileVersion":"No","MFAUsed":"No"},"eventID":"
a67bc106-0d0e-4fg2-hijk-514mn4op13q8","eventType":"AwsApiCall","recipientAccountId":"999999999999"}]}
```

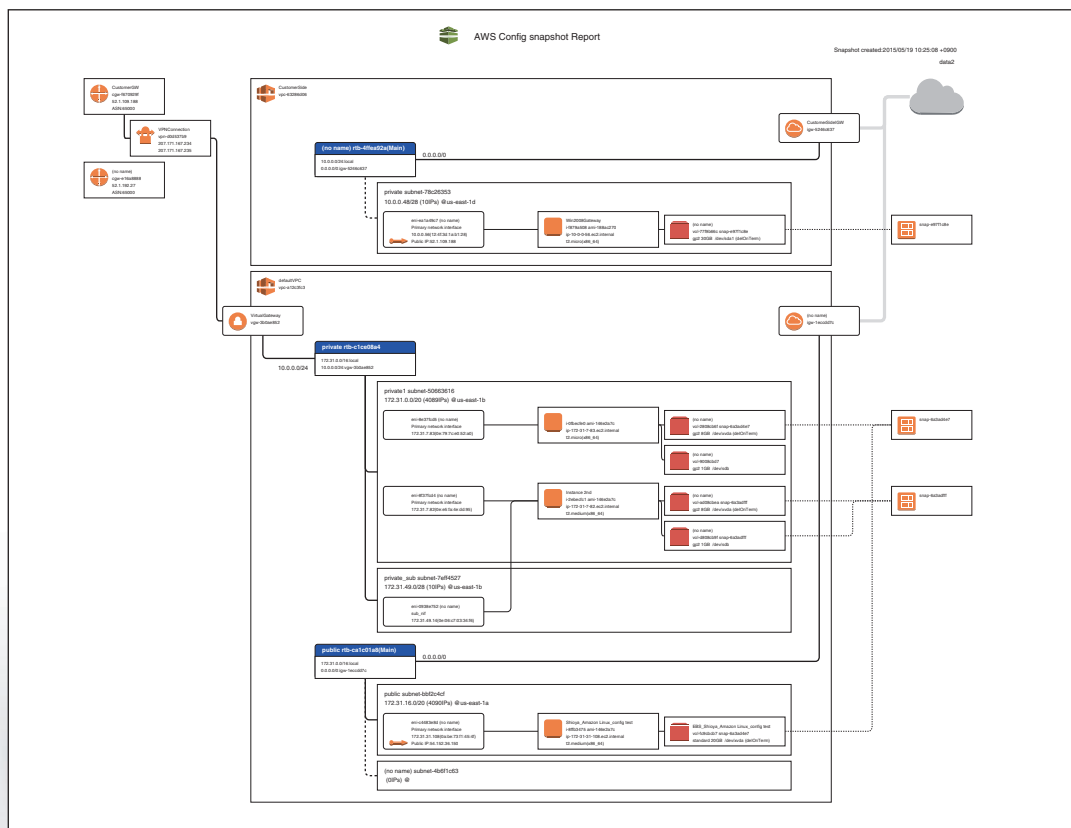


Logstorage for AWSはJSON形式のログを解析し、人間が理解できる形式に変換します

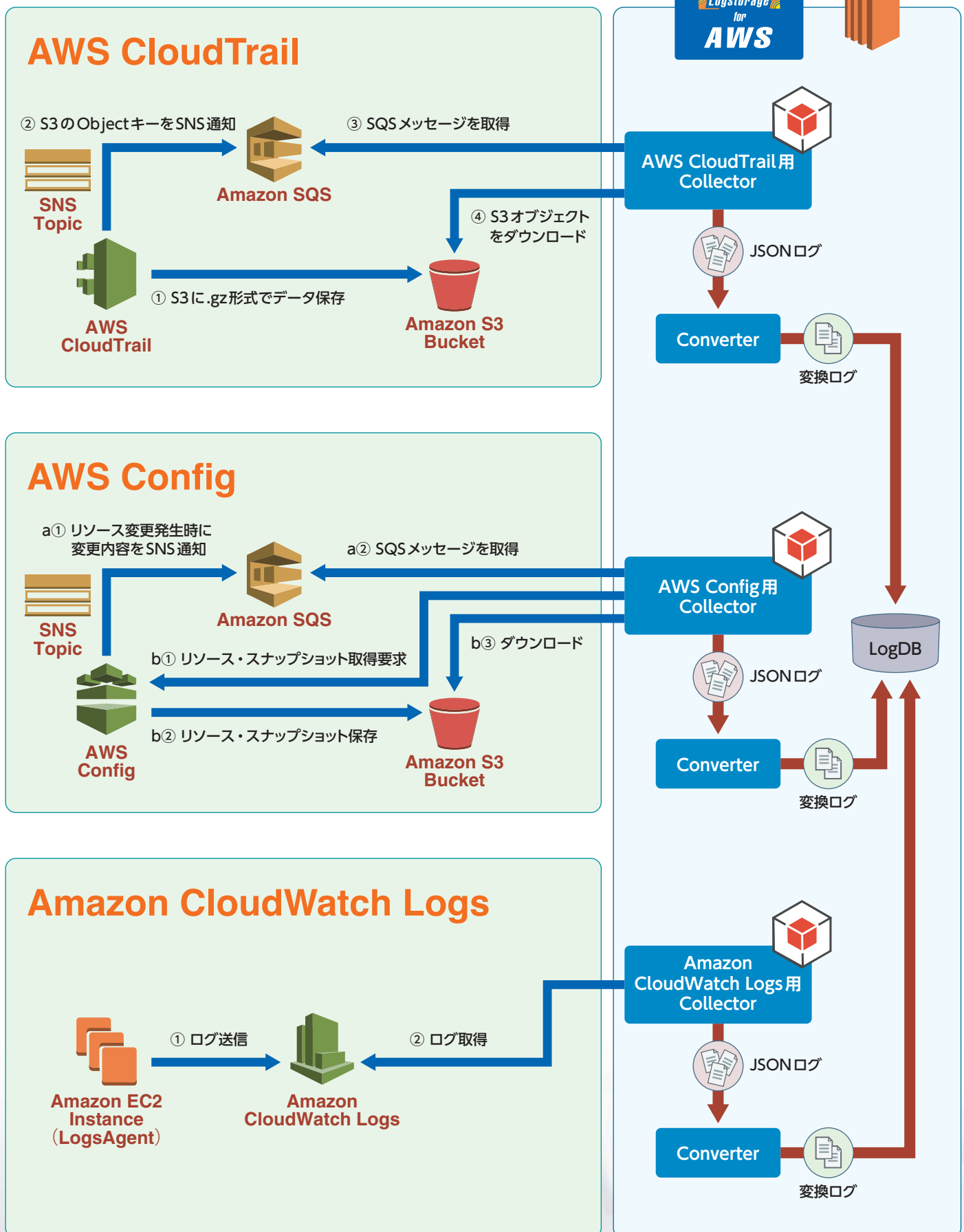
日時	サービス名	アクション	Type	ユーザ	イベント名	接続元IPアドレス	結果
2014-04-27 09:03:14	CloudTrail	Sign-In	IAM User	yamada	ConsoleLogin	192.168.0.1	成功

AWS上のリソース構成を可視化！

Logstorage for AWSは、AWS Configのログデータを活用し、AWS上に展開されているリソースの構成を可視化する機能を持っています。これにより、リソースが適正に利用されているか、また、セキュリティ上の問題が無いか、視覚的に分析する事が可能になります。



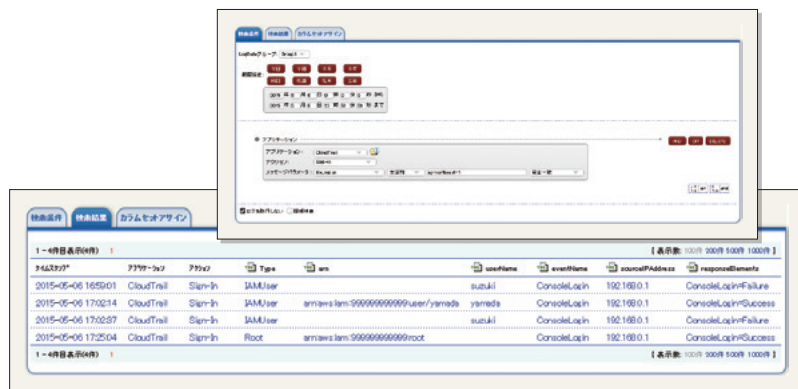
○ ログ収集の仕組み / 関連 AWS サービス



○ ログの分析機能

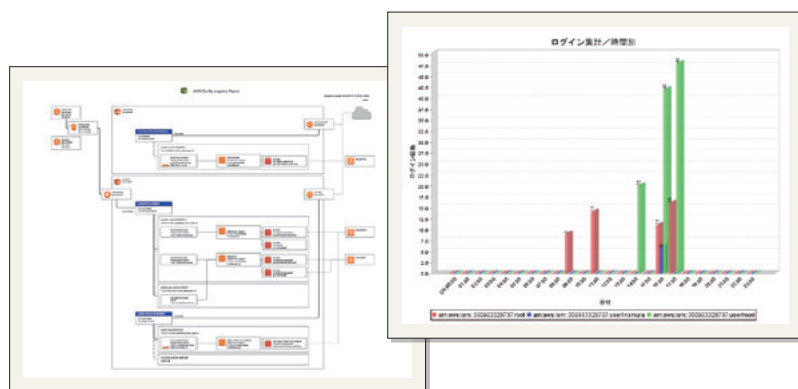
AWS 上のアクティビティを検索！

EC2 インスタンスを生成／停止したユーザは誰か、AWS Management Console にどの接続元からログインしてきたのか、ある AMI から生成された EC2 インスタンスはどれか、など、グラフィカルなユーザインターフェースにより、高度なスキル無しに検索することが可能になります。



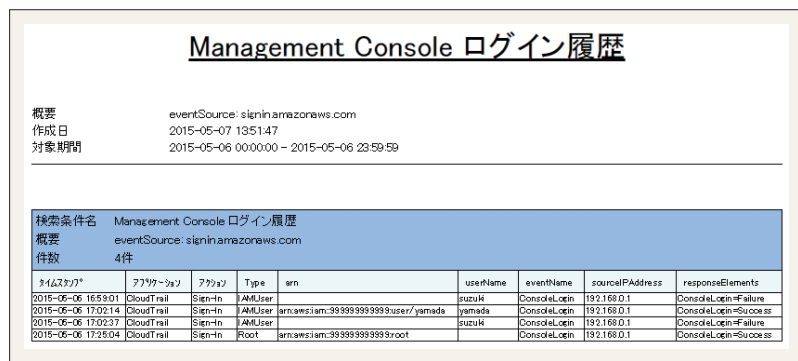
AWS の利用状況を視覚的に分析！

AWS Management Console へのユーザ毎のログイン回数や、EC2 インスタンスに対する接続元 IP アドレス毎のログイン回数、時間帯毎の EC2 インスタンスの起動数など、集計条件の縦軸、横軸に任意の項目を指定することで、様々な角度から、視覚的にログの分析を行うことが可能になります。



レポートを自動出力！

チェックしたい内容毎に、レポートを自動出力することが可能です。
作成されたレポートを自動的にメールに添付して送信することも可能ですので、AWS の利用状況の継続的な把握が容易になります。
レポートの出力間隔は、1 時間 / 1 日 / 1 週間 / 1 ヶ月 毎の指定が可能です。



○ ログの保管機能

暗号化機能

AES などの暗号化方式を用い、収集したログを暗号化して保管することが可能ですので、ログからの情報漏えいを防止できます。

改ざん検出機能

収集したログデータに対するハッシュ値を管理、チェックする機能により、ログが改ざんされていないことの証明が可能です。

圧縮機能

収集したログを最大で 10 分の 1 に圧縮して保管しますので、ログ保管に用いるストレージのコストを大幅にカットできます。

ユーザグループ管理機能

利用できる機能や閲覧できるログをユーザ、グループ毎に制限することができますので、権限に応じたアクセスコントロールが可能です。

○ Logstorage for AWS 動作環境

Amazon EC2 上で稼働させる場合

項目	推奨スペック
vCPU 数	2 以上
ECU 数	4 以上 (1vCPU 当たり 2ECU 以上)
メモリ	4GB 以上
推奨インスタンスタイプ	m3.large など
ストレージ (EBS)	プログラム領域 5GB 以上、別途ログ保管領域
OS	RedHat Enterprise Linux 6 / 7、Windows Server 2008 R2 / 2012 R2

オンプレミス (物理サーバ) で稼働させる場合

項目	推奨スペック
CPU	Quad Core 以上
メモリ	4GB 以上
ストレージ	プログラム領域 5GB 以上、別途ログ保管領域
OS	RedHat Enterprise Linux 6 / 7、Windows Server 2008 R2 / 2012 R2

【備考】上記 OS をサポートする仮想環境にも対応しております。

○ Logstorage for AWS 対応サービス

- AWS CloudTrail
- AWS Config
- Amazon CloudWatch Logs

※2015年5月現在

○ Logstorage for AWS 価格

ライセンス費用: 65 万円～
(別途年間保守費用 13 万円～)



機能一覧

機能	詳細
ログの収集・解析機能	<ul style="list-style-type: none"> ・AWS CloudTrail / AWS Config / Amazon CloudWatch Logs が提供するログの自動収集 ・JSON形式のログの解析
ログの保管機能	<ul style="list-style-type: none"> ・大量ログの圧縮保管 ・保管ログの暗号化 (AES 128bit) ・保管ログの改ざんチェック ・保管ログのスナップショット ・指定期間を超えた保管ログのアーカイブ / 削除
検索機能	<ul style="list-style-type: none"> ・AWS CloudTrail / AWS Config / Amazon CloudWatch Logs 用の検索条件テンプレート (30 種類以上) ・AWS CloudTrail / AWS Config / Amazon CloudWatch Logs 用のカラムセット定義 ・大量ログに対する高速検索 ・タブを利用した複数ログの横断検索 ・AND/OR/ 正規表現などによる検索条件指定 ・検索条件の保存 ・検索結果からの絞り込み (トラッキング) ・検索の中断 ・特定ログのハイライト表示
集計・分析機能	<ul style="list-style-type: none"> ・AWS CloudTrail / AWS Config / Amazon CloudWatch Logs 用のログ分析テンプレート (30 種類以上) ・表、棒グラフ、折れ線グラフ、円グラフによる集計結果出力 ・ログの件数、最大、最小、平均、合計、標準偏差の出力 ・集計結果のトップ n 表示 ・集計条件の保存 ・集計の中断 ・集計結果の CSV ダウンロード
レポート機能	<ul style="list-style-type: none"> ・AWS 上のリソース構成レポートの出力 ・AWS CloudTrail / AWS Config / Amazon CloudWatch Logs 用のレポートテンプレート (30 種類以上) ・毎月、毎週、毎日、毎時の自動レポート作成 ・PDF、CSV、HTML、TXT、XML フォーマットでのレポート作成 ・レポートのメール添付送信 ・コマンドラインによるレポート作成実行
ログフォーマット管理機能	<ul style="list-style-type: none"> ・AWS CloudTrail / AWS Config / Amazon CloudWatch Logs 用のログフォーマット定義テンプレート ・ログフォーマット定義のインポート / エクスポート機能 ・タグ管理機能
ユーザ管理機能	<ul style="list-style-type: none"> ・グループ、ユーザ単位によるアクセス制御 ・LDAP / AD によるユーザ認証の連携
その他管理機能	<ul style="list-style-type: none"> ・コンソールとの SSL 通信 ・監査ログ出力 ・他のログサーバへのログ転送 ・各種設定条件のインポート、エクスポート ・Logstorage for AWS 自身の障害通知

「Logstorage」は、インフォサイエンス株式会社の登録商標です。

「アマゾン ウェブサービス」[Amazon Web Service] [AWS] は、Amazon.com, Inc. またはその関連会社の商標です。



AWSのログ管理・分析ツールの決定版



製品のお問い合わせ先

インフォサイエンス株式会社 プロダクト事業部

メール: info@logstorage.com 電話: 03-5427-3503

URL: <http://www.logstorage.com/aws/>

■ 開発元

Infoscience

インフォサイエンス株式会社

〒108-0023 東京都港区芝浦 2-4-1 インフォサイエンスビル
TEL. 03-5427-3503 FAX. 03-5427-3889
<http://www.infoscience.co.jp/> E-mail: info@logstorage.com

■ 販売代理店

※価格のお問い合わせは、販売店またはインフォサイエンスの営業まで。