統合ログ管理システム Logstorage Cloud Solutions ご紹介資料

Infoscience

インフォサイエンス株式会社
プロダクト事業部

Infoscience Corporation
www.infoscience.co.jp info@logstorage.com
Tel: 03-5427-3503 Fax: 03-5427-3889

会社概要

Infoscience

会社名	インフォサイエンス株式会社
代表者	宮 紀雄
設立	1995年10月
従業員	100名
URL	https://www.infoscience.co.jp/
所在地	東京都港区芝浦2丁目4番1号 インフォサイエンスビル
	ソフトウェア Logstorage シリーズの開発・販売 製品URL：https://logstorage.com/

統合ログ管理ツール
Logstorage

ログの収集・保管、高度な分析、高速な検索を行う
統合ログ管理ソフトです

DXプラットフォーム
Jimzen

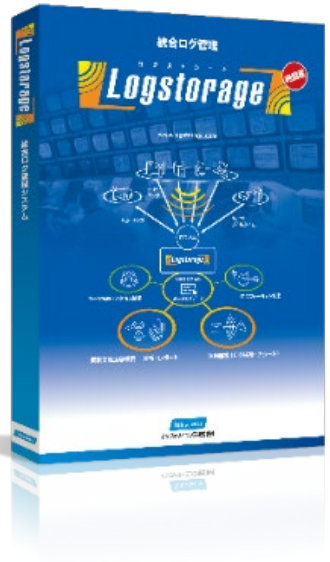
メンバーシップマネジメントを中心とするクラウド
サービスです

データセンター運用
DATA CENTER

独自の障害管理システムでサーバおよびネットワーク
機器の稼働状況を常に監視します

Logstorageシリーズ 製品概要

出荷本数シェアNo.1



Logstorage

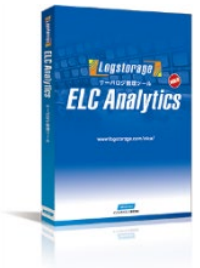
ログの収集・保管、高度な分析、高速な検索を行う、統合ログ管理ソフトです

★★★★★★★★★★★★★★★★

統合ログ管理ツール分野シェア

16年連続No.1

出典：デロイト トーマツ ミック経済研究所2023年1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 2022年度（統合ログ管理ツール部門）
出荷本数でシェア51.3%を獲得　https://mic-r.co.jp/mr/02620/



ELC Analytics

サーバのアクセスログや
ステータスログを管理します

Logstorage-X/SIEM

セキュリティ脅威を
リアルタイムで検知します

アライアンス・連携製品

各種管理ツールとの連携パッケージです

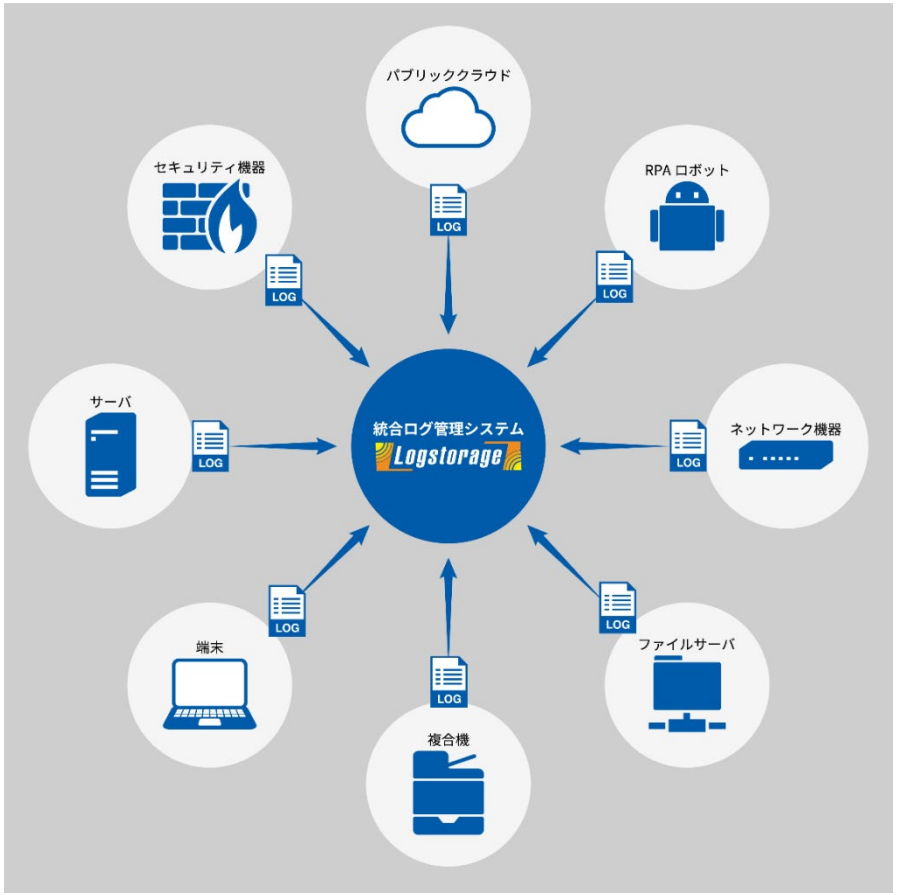
aws　Azure　Google Cloud
Microsoft 365　Google Workspace　box　cybereason
CWAT　LANSCOPE　MaLion　SKYSEA Client View
DEFESA Logger　MylogStar　paloalto　Access Check
iDoperation　PISO　SSDB監査　i-FILTER

統合ログ管理システム
「Logstorage」

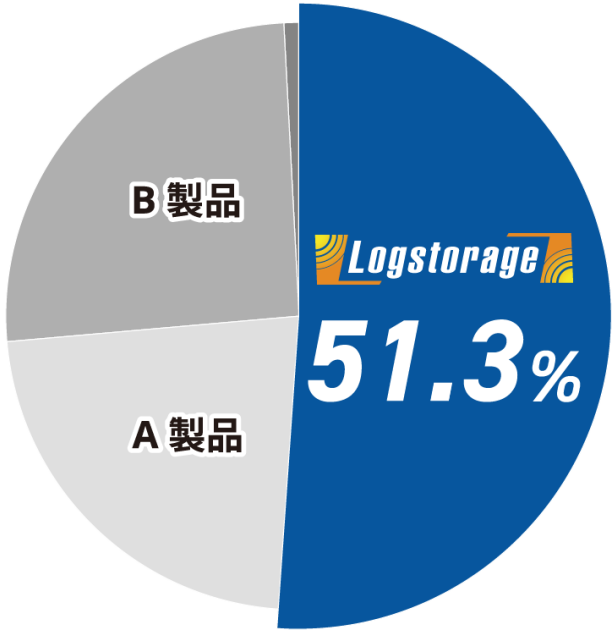
統合ログ管理システム「Logstorage」

「Logstorage」とは

様々なシステムに異なるフォーマットで散在するログを管理・分析する純国産の統合ログ管理システムです。
内部統制、情報漏えい対策、サイバー攻撃対策、システム運用監視、業務効率改善など多様な目的に対応できる、統合ログ分野でのデファクトスタンダード製品です。



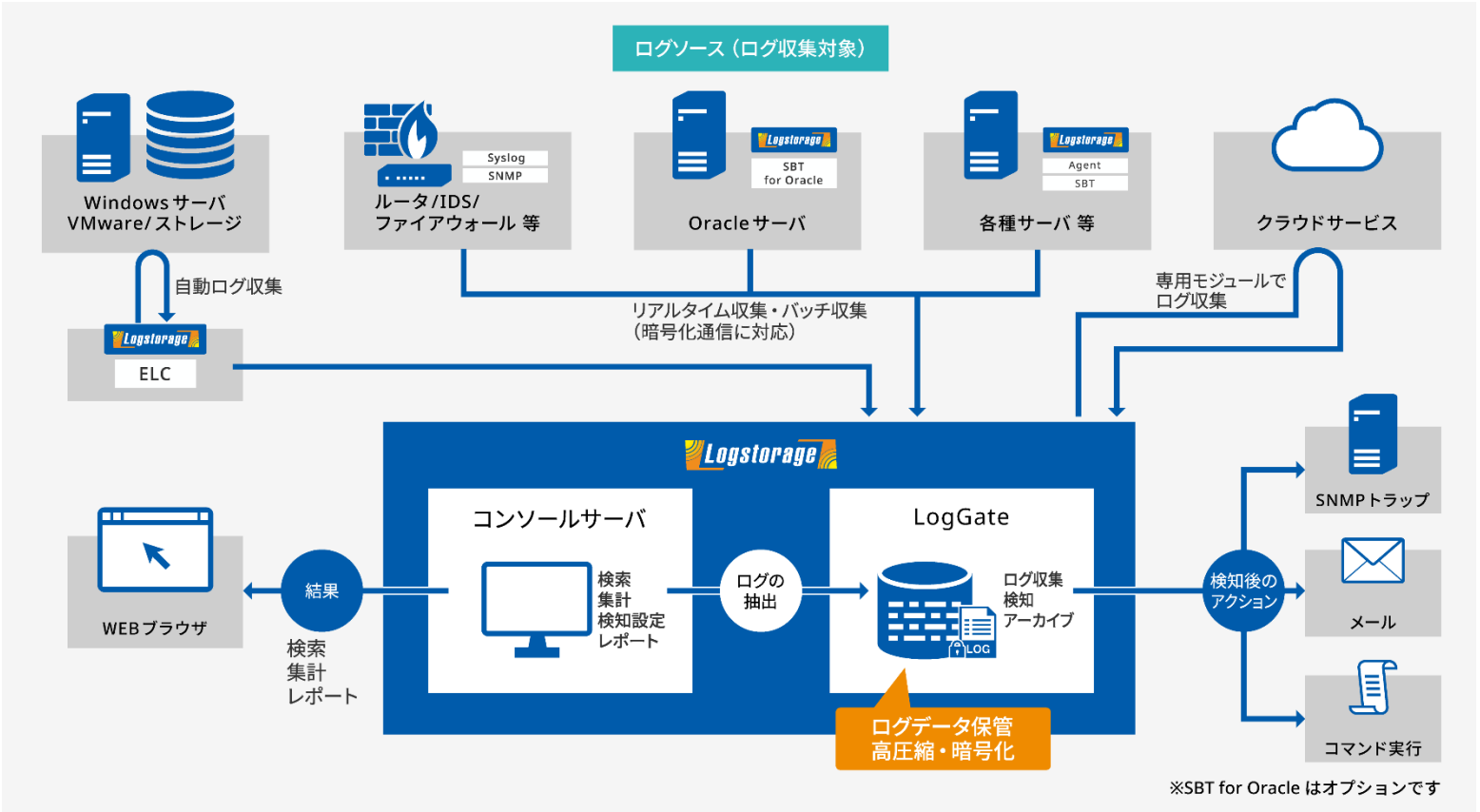
16年連続市場シェアNo.1
4,800社への導入実績



出荷本数シェア

※出典：デロイト トーマツ ミック経済研究所2023年1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 2022年度（統合ログ管理ツール部門）出荷本数でシェア51.3%を獲得 https://mic-r.co.jp/mr/02620/

統合ログ管理システム「Logstorage」



<Logstorage システム構成>

ログ収集機能

[受信機能]
- Syslog / FTP(S) / 共有フォルダ / SNMP

[ログ送信・取得機能]
- Agent
- ELC (EventLogCollector)
- SBT (SecureBatchTransfer)

ログ保管機能

- ログの圧縮保存 / 高速検索
- ログの改ざんチェック機能
- ログに対する意味（タグ）付け
- ログの暗号化保存
- 保存期間を経過したログを自動アーカイブ
- ログの保存領域管理機能

ログ検知機能

- ポリシーに合致したログのアラート
- ポリシーはストーリー的に定義可能
  (シナリオ検知)

検索・集計・レポート機能

- 複数ログの横断追跡とマウス操作による
  高度な絞込み
- インデックスによる大量ログの高速検索
- グラフ(円/折れ線/棒/表)によるログの
  サマリ表示
- レポート(HTML/PDF/CSV/TXT/XML)の
  自動メール通知

Logstorage 連携製品

各分野でトップシェアの製品と連携！

※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。

Logstorage 収集実績

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種以上のログ収集実績

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
IIS
BlueCoat
squid
WebSense
WebSphere
WebLogic
Apache Tomcat
Cosminexus
Trend Micro Cloud App Security
InterScan Web Security as a Service
Zscaler

サーバアクセス
ALog コンバータ
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
SQLServer
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 Vuris
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
Desk Net's
HP NonStop Server
System Answer

※順不同

パブリッククラウドのログ管理

クラウドについて

クラウドは、インフラやソフトウェアを管理することなく、インターネット通じて必要な時に必要な分だけ使用可能なサービスです。

クラウドの種類

IaaS **(Infrastructure as a Service)**	インフラを提供するクラウドサービス 例)Amazon EC2, Azure Virtual Machine, Google Compute Engine
PaaS **(Platform as a Service)**	プラットフォームを提供するクラウドサービス 例) Amazon Lambda, Azure Web Apps, Google App Engine
SaaS **(Software as a Service)**	ソフトウェアを提供するクラウドサービス 例) Dropbox, Box, Microsoft 365, Google Workspace

Web上で操作可能なため利便性が高い反面、作業/操作内容が把握しづらいといった課題があります。ログを活用して見える化をし、監査できる仕組みを作ることが大切です。

クラウドのログ管理には課題が山積み

課題①ログの管理が複雑化

課題②参照したいログの特定が大変

課題③ログの可読性が低くフォーマットもバラバラ

課題④ログの保管期間が短い

課題⑤予期せぬ機能追加、変更が発生する可能性がある

課題① ログの管理が複雑化

どのログをどうやって管理すればいいの…

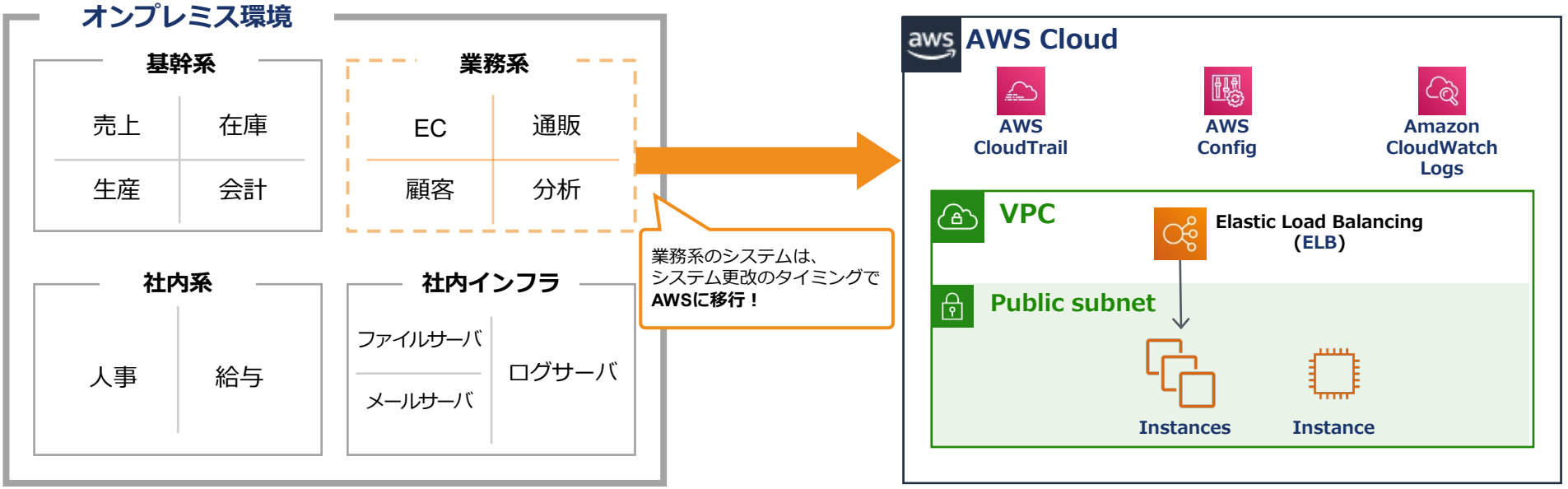
オンプレミス環境上で稼働するシステムのログ
- OSのイベントログ
- アプリケーションのログ

＋

クラウド基盤上で稼働するシステムのログ
- OSのイベントログ
- アプリケーションのログ

＋

クラウド利用者の操作ログ
- 管理コンソールのログイン
- 仮想サーバー作成のログ



システムは複雑化し、監査・管理対象は拡大します。

Logstorageで一元管理が可能です！！

課題② 参照したいログの特定が大変

サーバを停止したログはどれ…

例：AWS CloudTrail のログ（ Amazon EC2起動とEC2停止のログ）

{"Records": [{"eventVersion": "1.0","userIdentity": {"type": "IAMUser","principalId": "EX_PRINCIPAL_ID","arn": "arn:aws:iam::123456789012:user/Alice","accessKeyId": "EXAMPLE_KEY_ID","accountId": "123456789012","userName": "Alice"},"eventTime": "2014-03-06T21:22:54Z","eventSource": "ec2.amazonaws.com","eventName": **"StartInstances"**,"awsRegion": "us-east-2","sourceIPAddress": "205.251.233.176","userAgent": "ec2-api-tools 1.6.12.2","requestParameters": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]}},"responseElements": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2","currentState": {"code": 0,"name": "pending"},"previousState": {"code": 80,"name": "stopped"}}]}}},{"eventVersion": "1.0","userIdentity": {"type": "IAMUser","principalId": "EX_PRINCIPAL_ID","arn": "arn:aws:iam::123456789012:user/Alice","accountId": "123456789012","accessKeyId": "EXAMPLE_KEY_ID","userName": "Alice"},"eventTime": "2014-03-06T21:01:59Z","eventSource": "ec2.amazonaws.com","eventName": **"StopInstances"**,"awsRegion": "us-east-2","sourceIPAddress": "205.251.233.176","userAgent": "ec2-api-tools 1.6.12.2","requestParameters": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},"force": false},"responseElements": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2","currentState": {"code": 64,"name": "stopping"},"previousState": {"code": 16,"name": "running"}}]}}}]}

大量に存在するログの中から、参照したいログを特定するのは非常に困難であり、運用方法を検討する必要があります。

テンプレート条件を利用することで、簡単に参照することができます！！

課題③ ログの可読性が低くフォーマットもバラバラ

ログの内容がよくわからない…

AWS CloudTrail

```
"Records": [{
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            “arn”: “arn:aws:iam::123456789012:user/Alice”…
```

Azure Activity log


```
 "authorization": {
            "action": "Microsoft.Security/register/action",
            "scope": "/subscriptions/70435def-b7c2-45cb-
9258-f2d6a1835f34"
        },
        "caller": “user@domain.onmicrosoft.com",
        "channels": "Opera…
```

Amazon S3

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5
218e7cd47ef2be mybucket [06/Feb/2014:00:00:38
+0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5
218e7cd47ef2be 3E57427F3EXAMPLE
REST.GET.VERSIONING - “GET /mybucket?versioning
HTTP/1.1” 200 - 113 - 7 - “-” “S3Console/0.4” -
```

Box


```
"created_at": "2017-02-02T16:50:51-08:00",
"event_id": "5dfbd9a7-d022-42a9-9b9a-00818d338686",
"event_type": "DOWNLOAD",
"ip_address": “XXX.XXX.XXX.XXX",
"type": "event",
…
```

サービスによってログのフォーマットは異なり、ログにどのような情報が入っているのかも、把握が難しい状態です。

テンプレート条件を利用することで、簡単に参照することができます！！

課題④ ログの保管期間が短い

いつまでログが保管できるの…

【各クラウドサービスのログ保管期間】

製品	ログ保管期間（※）
AWS	90日
Azure	90日
GCP	30日
Microsoft 365	90日
Google Workspace	180日

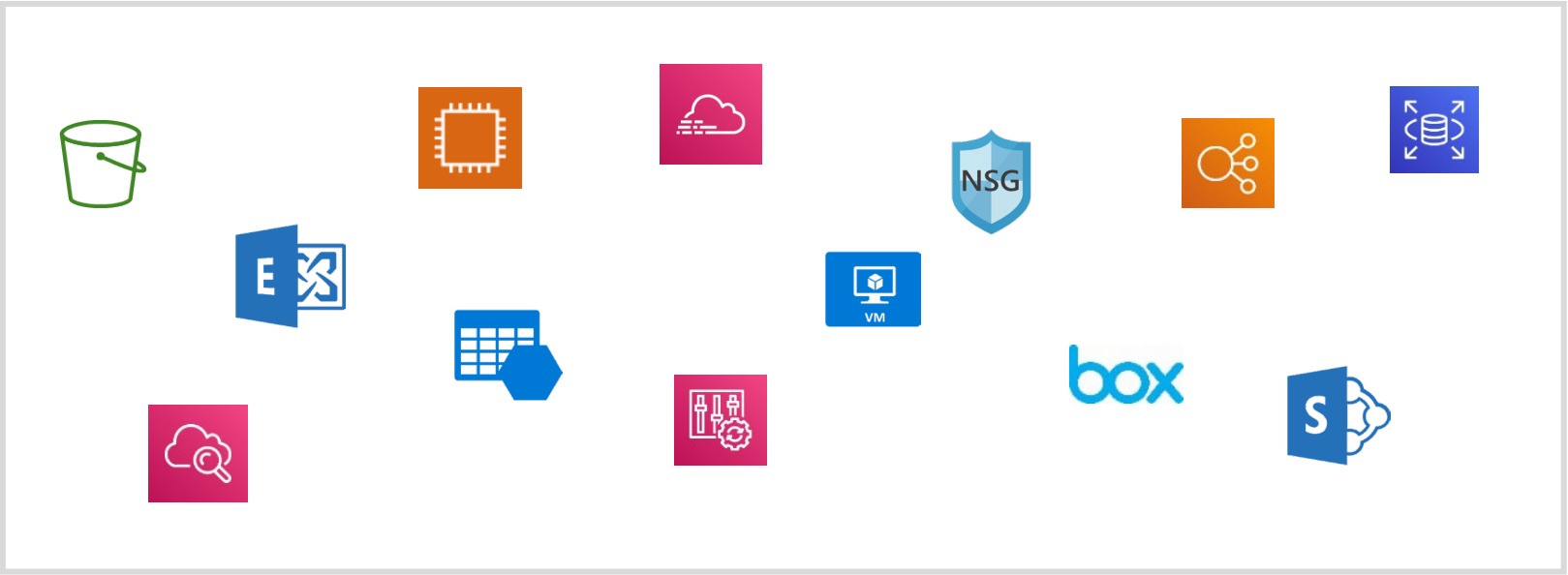
※ ログが保管される期間はログの種類により異なります。

1年以上のログの保管を義務付けている企業は多く、どのように管理するか検討が必要になります。

Logstorageでは、ログをセキュアに長期保管することが可能です！！

課題⑤ 予期せぬ機能追加、変更が発生する可能性がある

ログのフォーマットが変わった…



自らログ取得処理を開発・運用したり、フォーマット・意味付けの異なるログを
レビューしていては、運用コストの増大を招きかねません。

Logstorageクラウド対応製品では、運用コストがかかりません！

クラウドのログ管理には課題が山積み

Logstorage Cloud Solutionsで様々な課題に対応可能です！！

課題①　ログの管理が複雑 CLEAR

課題②　参照したいログの特定が大 CLEAR

課題③　ログの可読性が低くフォーマットもバラバ CLEAR

課題④　ログの保管期間が短い CLEAR

課題⑤　予期せぬ機能追加、変更が発生する可能性があ CLEAR

クラウド・各種サービスのログ収集

クラウドサービスのログを効率的に収集・分析

検索・集計・レポート条件テンプレートが用意されているので、ログ分析が容易に可能。
ログの長期保管・圧縮保管・暗号化・改ざん検出機能にも対応！

aws　Azure　Microsoft 365　Google Workspace　Google Cloud　box　cybereason

製品	対応サービス / 機能
AWS	AWS CloudTrail, AWS Config, Amazon CloudWatch Logs, Amazon CloudWatch Metrics, AWS Billing, Amazon S3, Amazon ELB, Amazon RDS, Amazon CloudFront,Amazon S3 オブジェクト
Azure	Azure Activity Log, Azure Virtual Machine, Azure Storage, Azure Network Security Group, Azure Active Directory
GCP	管理アクティビティ監査ログ, システムイベント監査ログ, データアクセス監査ログ, VPCフローログ, メトリックスデータ(仮想マシン)
Box	Enterprise Events
Microsoft 365	Microsoft 365 監査ログ (Azure Active Directory, Exchange, SharePoint, OneDrive for Business, Microsoft Teams) Microsoft 365 メッセージ追跡ログ (MessageTrace, MessageTraceDetail)
Google Workspace	管理コンソール, ログイン, SAML, OAuth トークン, ユーザーアカウント, グループ, ドライブ, デバイス
Cybereason	MALOP,マルウェア, 監査ログ

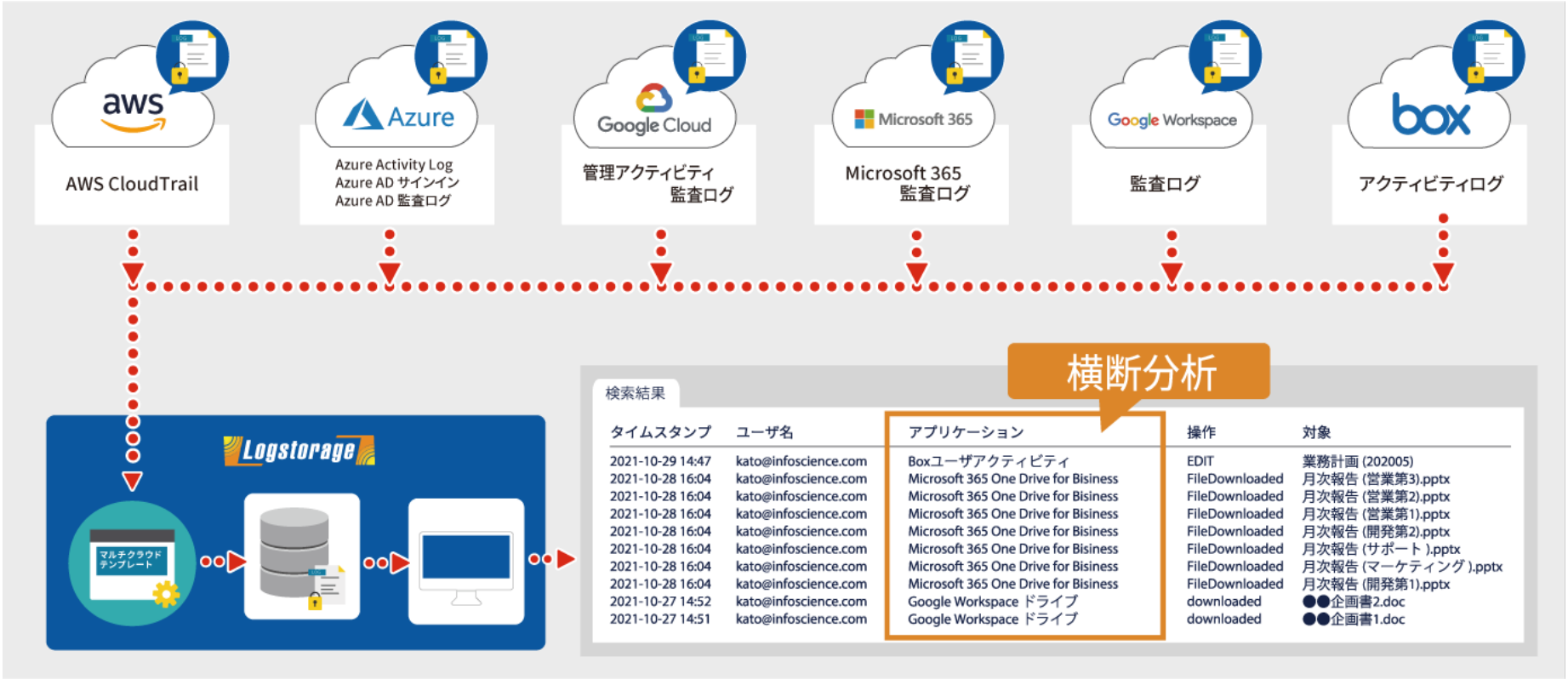
クラウド他、各種サービスのログも収集可能

他、各種サービスにも対応しています。

paloalto　iDoperation　HIBUN　SKYSEA Client View　CWAT　MylogStar　Access Check　SSDB監査　i-FILTER　PISO　On-premises LANSCOPE Endpoint Manager　DEFESA Logger　MaLion

Logstorage で収集したクラウドサービスログを横断的に分析・レポート

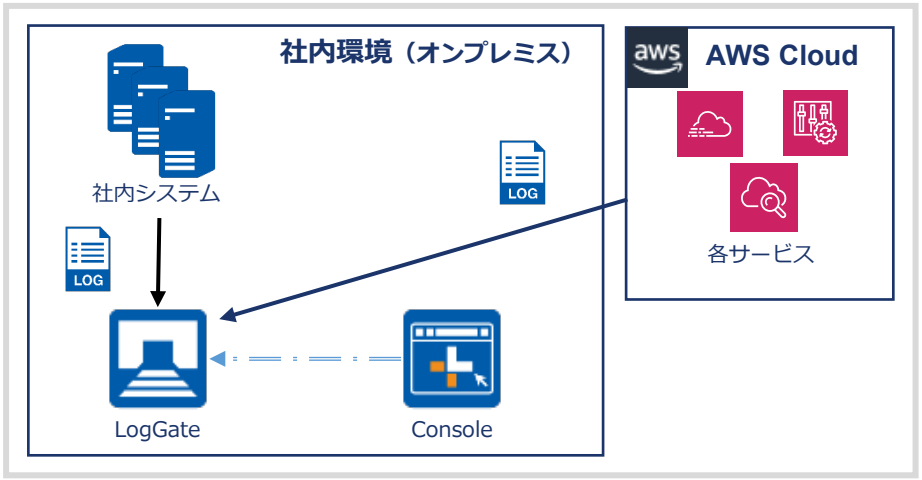
Logstorage Cloud Solutions に含まれる連携製品を横断分析できるテンプレートです。

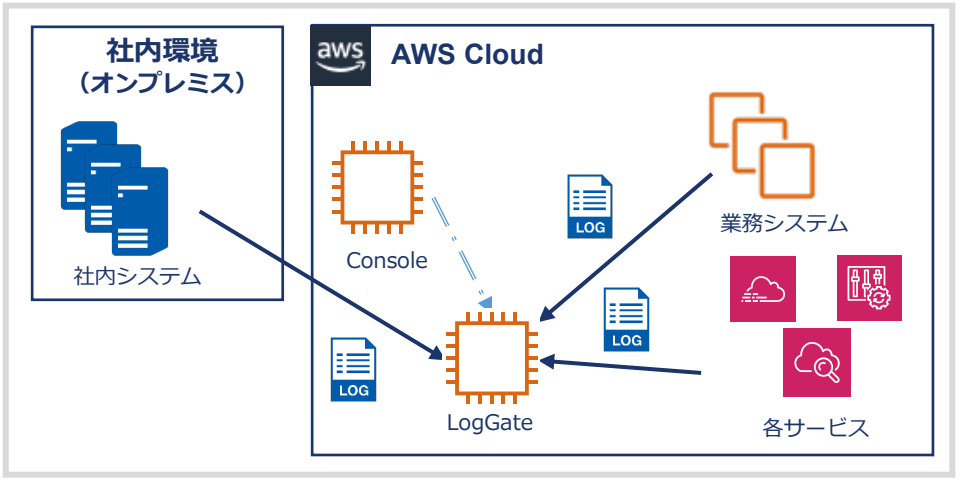


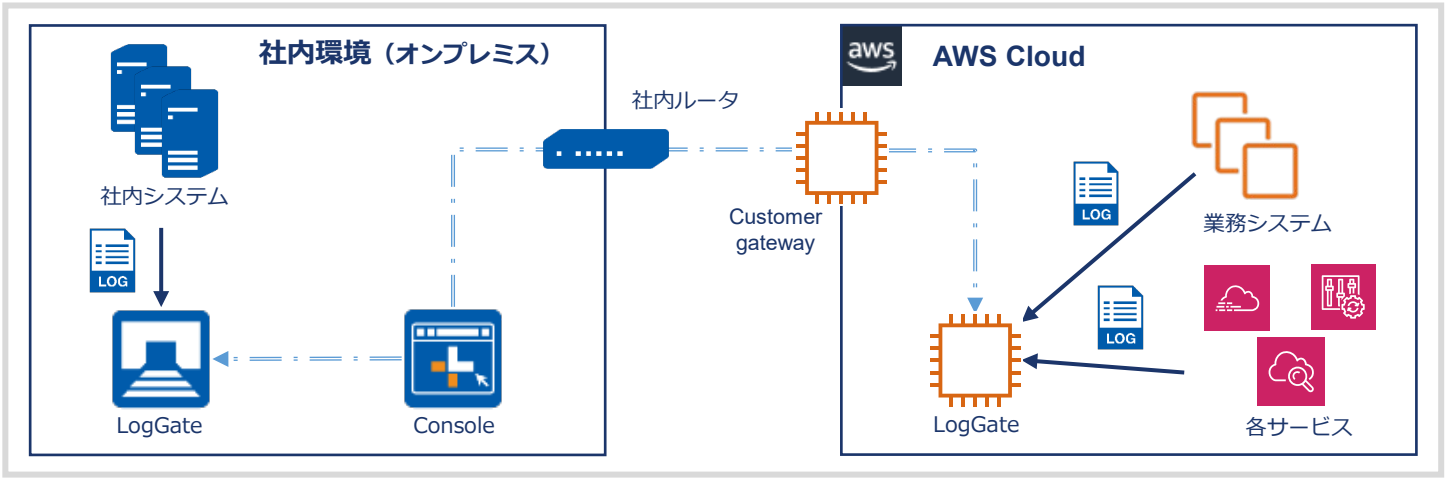
対応しているLogstorage Cloud Solutions 連携パックを2つ以上ご購入の方に
無償提供いたします。

Logstorage 構成例

Logstorageは、オンプレミス・クラウド・ハイブリット(※1)のいずれの環境においても構築可能です。





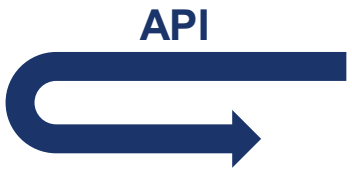


オンライン期間を過ぎたログをアーカイブして安価な Amazon S3 に転送することで

ストレージのコストを削減することができます

※1 ConsoleとLogGateが分かれるハイブリット環境の場合、環境間のネットワーク構成によって各拠点を跨った動作に遅延が発生する可能性があります。
お客様環境で事前に検証の上、ご利用いただくことを推奨いたします。

ログは自動で取得します！



クラウド専用
ログ収集モジュール

クラウド対応製品では、クラウドサービス毎に専用のログ収集モジュールを用意しています（※）。
タスク管理ツールを用いて、定期的に実行してログを収集します。

クラウドサービス側の設定、クラウド対応製品のインストールと設定をすることで
クラウド上のログを収集することが可能です。

※ Cybereason のログはsyslogで受信するため、ログ収集モジュールはありません。

Logstorage AWS 対応パック

- AWS上のログ管理 –

Logstorage Azure 連携パック

- Azure上のログ管理 –

Logstorage GCP 連携パック

- GCP上のログ管理 -

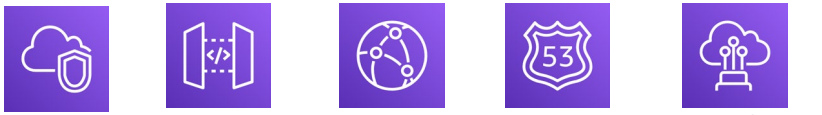
Amazon Web Services（AWS）

Logstorage

Amazon社が2004年から提供するクラウドサービスです。クラウドサービスの中では、最も長く利用されています。サービス系アプリやビッグデータ分析、ストレージなど、幅広い利用に適しています。

Compute

Networking



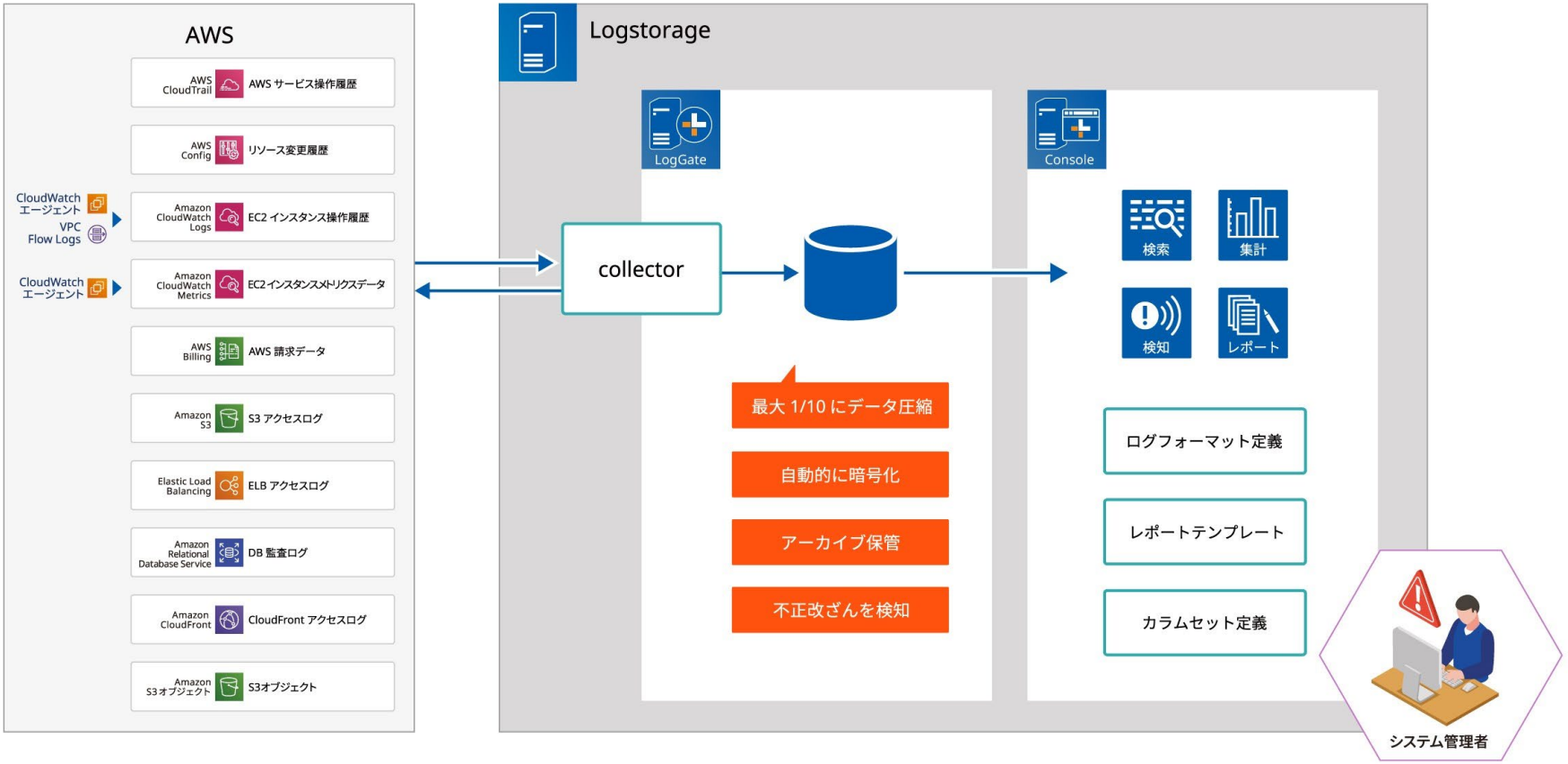
Storage

Security, Identity and Compliance

Database

Management & Governance

Logstorage 対応パック for AWS 概要



名称	詳細
AWS CloudTrail	AWS上の操作ログ（監査ログ）
AWS Config	リソースの構成変更履歴
Amazon CloudWatch Logs	EC2内のログ、VPC Flow Logs など
AWS Billing	AWS請求データ
Amazon S3	S3のアクセスログ

名称	詳細
Amazon CloudWatch Metrics	サーバーのメトリクス情報
Elastic Load Balancing	ELBのアクセスログ
Amazon RDS	SQLクエリーログ
Amazon CloudFront	CloudFrontのアクセスログ
Amazon S3（オブジェクト）	S3に配置された任意のログ

Microsoft Azure

Logstorage

Microsoft社が提供するクラウドサービスです。Windows ServerやMicrosoft OfficeといったMicrosoft製品との親和性が高く、既存のActive Directoryとも容易に連携を行うことができ、ハイブリッドクラウド構成を実現する基盤として適しています。

Compute & Networking

Virtual Machines | Batch | Scheduler | RemoteApp | Virtual Network | load balancer | Express Route | Site Recovery

Storage & Content Delivery

Storage blob | Storage queue | Storage table | Media | Content Delivery Network

Deployment & Management

Active Directory | Automation | BizTalk | Backup | Activity Log | Search

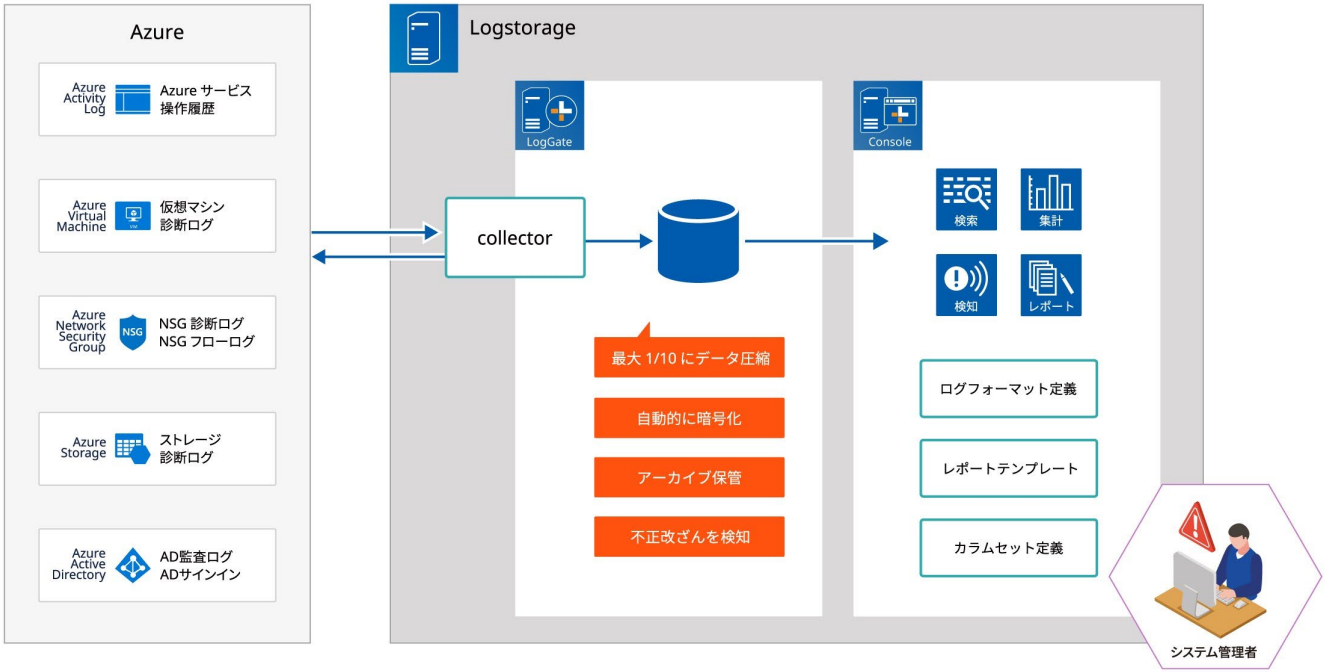
Database

SQL Database | DocumentDB | Redis Cache | Data Factory

Web & Mobile

Web App | Mobile App | API Management | Notification Hubs | Event Hubs

Logstorage Azure 連携パック 概要



・Azureポータルのログイン情報はサインインに記録されます。

・Azure サインインは、Azure のサブスクリプションとは別に、Azure Active Directory Premium P1 または P2 の契約が必要になります。

・監査ログは、Azure AD の様々な操作内容が記録されます。ユーザー、アプリ、グループ、ロール、ポリシーの追加や削除など、Azure AD 内のあらゆるリソースに加えられた変更が対象です。

名称	詳細	例
Activity logs	Azureサービスに対するアクセスログ	仮想マシンの作成/停止/削除
Azure Virtual machines	Azure仮想マシン内のアクセスログ	仮想マシン内のWindowsイベントログ/Linux syslog
Azure Active Directory	サインイン、監査ログ	
Azure Network Security Group	診断ログ（イベントログ、カウンタログ）、フローログ	
Azure Storage	Azureストレージへのアクセスログ	

Google Cloud Platform (GCP)

Logstorage

Google社が提供するクラウドサービスです。機械学習やビックデータ解析に優位性があります。
GmailやYouTube、Googleマップなどを稼働させる基盤としても利用されており、
安定したサービスの運用実績があります。

Compute

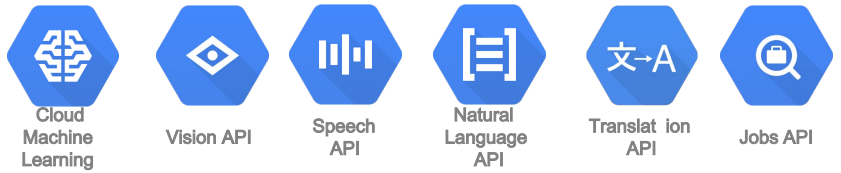
Identity & Security

Networking

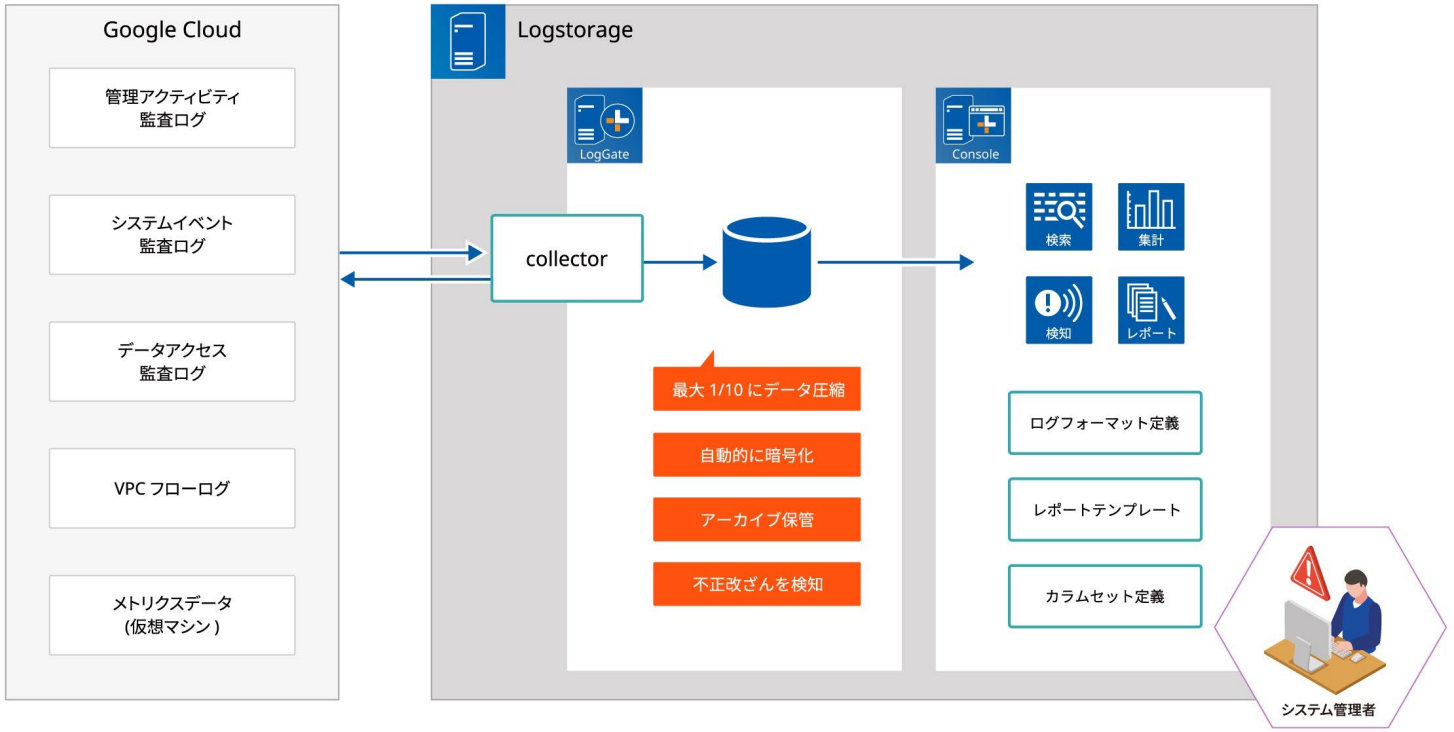
Big Data

Storage and Databases

Machine Learning



Logstorage GCP 連携パック 概要



名称	詳細	例
管理アクティビティ監査ログ	GCPリソースの構成変更などの管理操作が記録されます。デフォルトで有効であり、無効にはできません。	・仮想マシンの作成/停止/削除 ・GCPポータルへのログイン
データアクセス監査ログ	データを保持するGCPサービスについて、データの読み込みや書き込みがされた際に記録されます。デフォルトでは無効です。	・ストレージにあるファイルの読み込み
システムイベント監査ログ	ホストメンテナンスやライブマイグレーションといった、Google側でGCEに対して自動的に行った操作が記録されます。デフォルトで有効であり、無効にはできません。 ※システムイベント監査ログは、ログの詳細がGCPドキュメントに公開されていないためテンプレート条件は提供しておりません。	
VPCフローログ	VMインスタンスに送受信されたネットワークフローが記録されます。	
メトリクスデータ	システムのパフォーマンスに関するデータが記録されます。 ※ Logstorage GCP 連携パック では、仮想マシンのメトリクスデータ取得に対応しています。	

監査ログ / テンプレート例

Management Console ログイン履歴

概要　eventSource: signin.amazonaws.com
作成日　2014-10-03 16:14:29
対象期間　2014-08-01 00:00:00 - 2014-08-31 23:59:59

管理コンソールに、不正にアクセスされていないか?

検索条件名　Management Console ログイン履歴
概要　eventSource: signin.amazonaws.com
件数　65件

ﾀｲﾑｽﾀﾝﾌﾟ	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	Type	arn	userName	eventName	sourceIPAddress	responseElements
2014-08-20 16:59:01	CloudTrail	Sign-In	IAMUser		mori	ConsoleLogin		ConsoleLogin=Failure
2014-08-20 17:02:14	CloudTrail	Sign-In	IAMUser	arn:aws:iam::[redacted]:user/inamura	inamura	ConsoleLogin		ConsoleLogin=Success
2014-08-20 17:02:37	CloudTrail	Sign-In	IAMUser		mori	ConsoleLogin		ConsoleLogin=Failure
2014-08-20 17:25:04	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin		ConsoleLogin=Success
2014-08-21 08:16:09	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin		ConsoleLogin=Success
2014-08-21 13:43:13	CloudTrail	Sign-In	IAMUser	arn:aws:iam::[redacted]:user/inamura	inamura	ConsoleLogin		ConsoleLogin=Success
2014-08-21 13:44:45	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin		ConsoleLogin=Success
2014-08-22 08:23:18	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin		ConsoleLogin=Success
2014-08-22 16:31:23	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin		ConsoleLogin=Success
2014-08-22 17:06:30	CloudTrail	Sign-In	IAMUser	arn:aws:iam::[redacted]:user/mori	mori	ConsoleLogin		ConsoleLogin=Success
2014-08-22 17:12:50	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin		ConsoleLogin=Success
2014-08-25 08:07:53	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin		ConsoleLogin=Success
2014-08-25 11:38:38	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin		ConsoleLogin=Success
2014-08-25 13:48:00	CloudTrail	Sign-In	IAMUser	arn:aws:iam::[redacted]:user/mori	mori	ConsoleLogin		ConsoleLogin=Success
2014-08-25 16:32:22	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin		ConsoleLogin=Success
2014-08-25 16:33:18	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin		ConsoleLogin=Success

接続元集計

概要　AWSサービスへの接続元IPアドレスの集計
作成日　2014-07-10 14:16:48
対象期間　2014-06-01 00:00:00 - 2014-06-30 23:59:59

管理外の接続はないか?

集計条件名　接続元集計
概要

リージョン	サービス	接続元	ログ件数
us-west-1	cloudtrail.amazonaws.com	[redacted]	114
	directconnect.amazonaws.com	[redacted]	3
	ec2.amazonaws.com	[redacted]	487
	ec2.amazonaws.com	[redacted]	29
	elasticloadbalancing.amazonaws.com	[redacted]	6
	elasticloadbalancing.amazonaws.com	[redacted]	108
	monitoring.amazonaws.com	[redacted]	150
us-east-1	cloudtrail.amazonaws.com	[redacted]	54
	ec2.amazonaws.com	[redacted]	120
	elasticloadbalancing.amazonaws.com	[redacted]	3
	sns.amazonaws.com	[redacted]	765
	monitoring.amazonaws.com	[redacted]	4
	sts.amazonaws.com	signin.amazonaws.com	130
us-west-2	cloudtrail.amazonaws.com	[redacted]	21
	ec2.amazonaws.com	[redacted]	300
	elasticloadbalancing.amazonaws.com	[redacted]	5
	elasticloadbalancing.amazonaws.com	signin.amazonaws.com	2
	monitoring.amazonaws.com	signin.amazonaws.com	37

仮想マシン削除履歴

概要
作成日　2017-08-10 14:05:14
対象期間　2017-07-01 00:00:00 - 2017-07-31 23:59:59

誤ったインスタンスの削除はないか？

検索条件名　仮想マシン削除履歴
概要　操作名: Microsoft.Compute/virtualMachines/delete or Microsoft.ClassicCompute/virtualmachines/delete, イベント名: Begin request で抽出
件数　8件

ﾀｲﾑｽﾀﾝﾌﾟ	要求_名前	呼び出し元	要求_IPアドレス	リソースプロバイダー名	操作名	リソースグループ名	リソース名
2017-07-20 18:13:24	shioya	shioya@[redacted].com	[redacted]	Microsoft.Compute	Microsoft.Compute/virtualMachines/delete	ShioyaTest	NewLogstWG2
2017-07-20 18:11:07	shioya	shioya@[redacted].com	[redacted]	Microsoft.Compute	Microsoft.Compute/virtualMachines/delete	ShioyaTest	XLogst3
2017-07-20 18:09:19	shioya	shioya@[redacted].com	[redacted]	Microsoft.Compute	Microsoft.Compute/virtualMachines/delete	ShioyaTest	LogstorageWG2
2017-07-20 18:08:43	shioya	shioya@[redacted].com	[redacted]	Microsoft.Compute	Microsoft.Compute/virtualMachines/delete	ShioyaTest	JumpBox
2017-07-20 18:07:53	shioya	shioya@[redacted].com	[redacted]	Microsoft.Compute	Microsoft.Compute/virtualMachines/delete	ShioyaTest	NewLogstWG
2017-07-13 15:34:46	shioya	shioya@[redacted].com	[redacted]	Microsoft.Compute	Microsoft.Compute/virtualMachines/delete	ShioyaTest	TestLogst
2017-07-13 14:40:22	kitagawa	kitagawa@[redacted].com	[redacted]	Microsoft.Compute	Microsoft.Compute/virtualMachines/delete	logstorageTest	Kitagawa-A3-WS2
2017-07-03 17:48:04	shioya	shioya@[redacted].com	[redacted]	Microsoft.Compute	Microsoft.Compute/virtualMachines/delete	ShioyaTest	LogstorageWG

Security ログオン失敗

仮想サーバーに、不正にアクセスされていないか?

監査ログ / テンプレート例

GCP VMインスタンス操作履歴

概要
作成日　2020-07-31 14:55:54
対象期間　2020-01-01 00:00:00 - 2020-12-31 23:59:59

1つのレポートに監査したい内容を
複数設定することができます。

検索条件名　GCP VMインスタンス作成履歴
概要　「beta.compute.instances.insert」で抽出
件数　3件

ﾀｲﾑｽﾀﾝﾌﾟ	ログレベル	ユーザー	ｱｸｼｮﾝ	メソッド名	リソース名	リソースタイプ	プロジェクトI
2020-07-14 17:07:54	NOTICE	user1@infoscience.com	Compute Engine	beta.compute.instances.insert	projects/gcp-test/zones/asia-northeast1-b/instances/logstorage-ws	gce_instance	gcp-test
2020-07-10 10:46:13	NOTICE	user1@infoscience.com	Compute Engine	beta.compute.instances.insert	projects/gcp-test/zones/asia-northeast1-b/instances/instance-rhel-e2	gce_instance	gcp-test
2020-07-10 09:55:10	NOTICE	user1@infoscience.com	Compute Engine	beta.compute.instances.insert	projects/gcp-test/zones/asia-northeast1-b/instances/instance-ws-e2	gce_instance	gcp-test

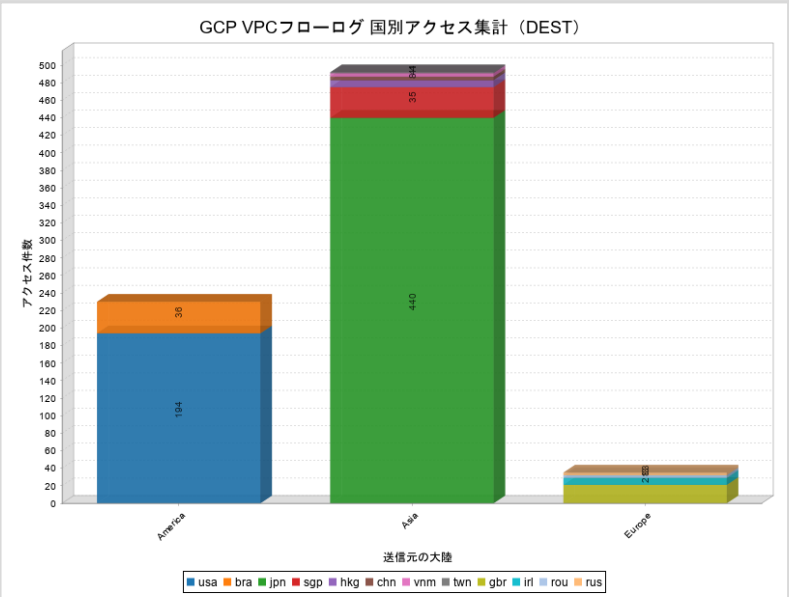
検索条件名　GCP VMインスタンス削除履歴
概要　「v1.compute.instances.delete」で抽出
件数　3件

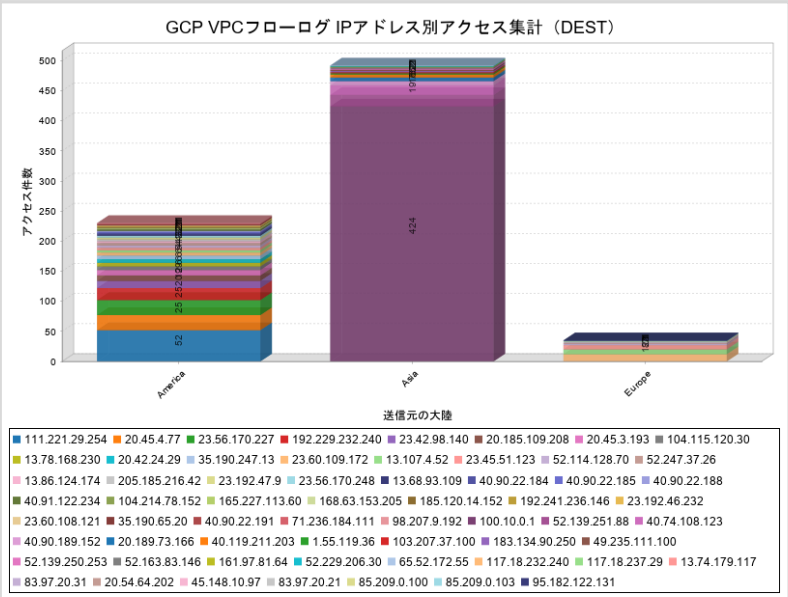
ﾀｲﾑｽﾀﾝﾌﾟ	ログレベル	ユーザー	ｱｸｼｮﾝ	メソッド名	リソース名	リソースタイプ	プロジェクトID
2020-07-10 17:06:14	NOTICE	user1@infoscience.com	Compute Engine	v1.compute.instances.delete	projects/gcp-test/zones/asia-northeast1-b/instances/instance-ws	gce_instance	gcp-test
2020-07-10 17:06:03	NOTICE	user1@infoscience.com	Compute Engine	v1.compute.instances.delete	projects/gcp-test/zones/asia-northeast1-b/instances/instance-ws-e2	gce_instance	gcp-test
2020-07-10 17:06:03	NOTICE	user1@infoscience.com	Compute Engine	v1.compute.instances.delete	projects/gcp-test/zones/asia-northeast1-b/instances/instance-rhel-e2	gce_instance	gcp-test

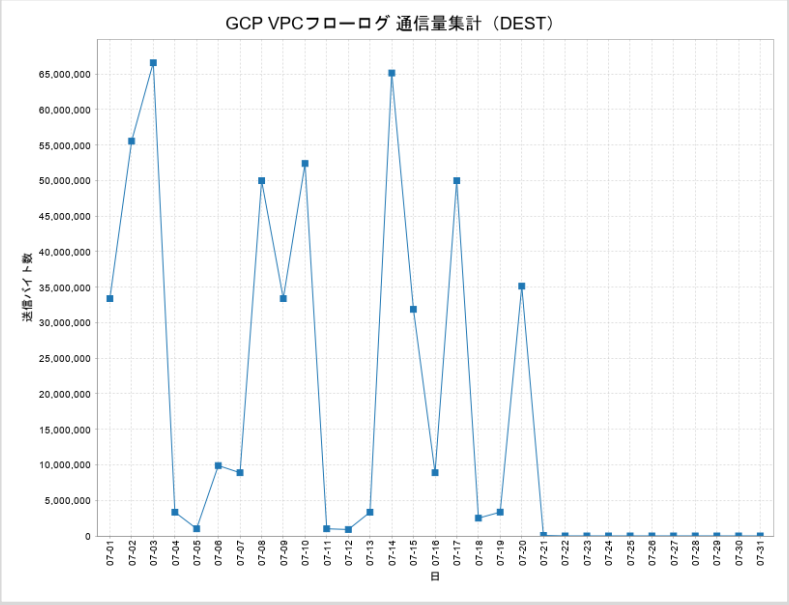
検索条件名　GCP VMインスタンス起動履歴
概要　「v1.compute.instances.start」で抽出
件数　4件

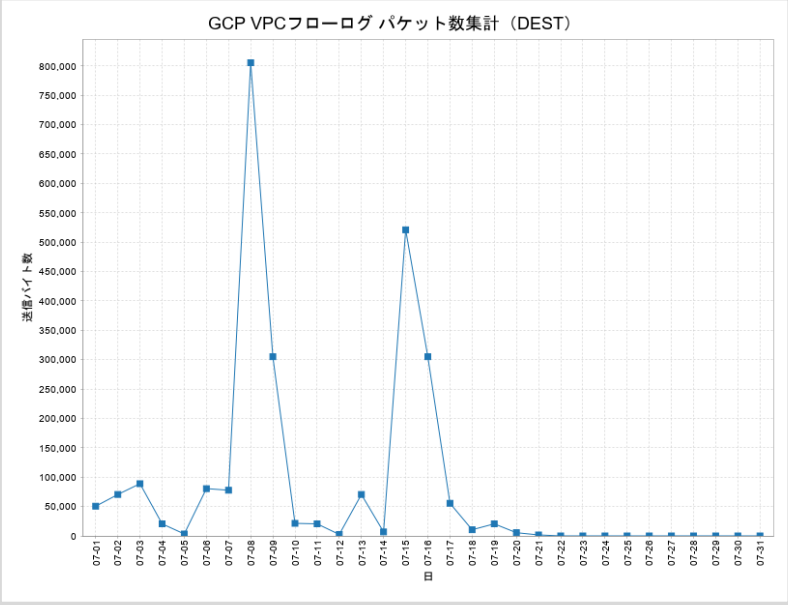
ﾀｲﾑｽﾀﾝﾌﾟ	ログレベル	ユーザー	ｱｸｼｮﾝ	メソッド名	リソース名	リソースタイプ	プロジェクトID	
2020-07-21 09:22:53	NOTICE	user1@infoscience.com	Compute Engine	v1.compute.instances.start	projects/gcp-test/zones/asia-northeast1-b/instances/logstorage-ws	gce_instance	gcp-test	1(
2020-07-20 16:10:45	NOTICE	sample1@logst.com	Compute Engine	v1.compute.instances.start	projects/gcp-test/zones/asia-northeast1-b/instances/logstorage-ws	gce_instance	gcp-test	1(
2020-07-15 09:24:06	NOTICE	sample1@logst.com	Compute Engine	v1.compute.instances.start	projects/gcp-test/zones/asia-northeast1-b/instances/logstorage-ws	gce_instance	gcp-test	1(

VPCフローログ / テンプレート例

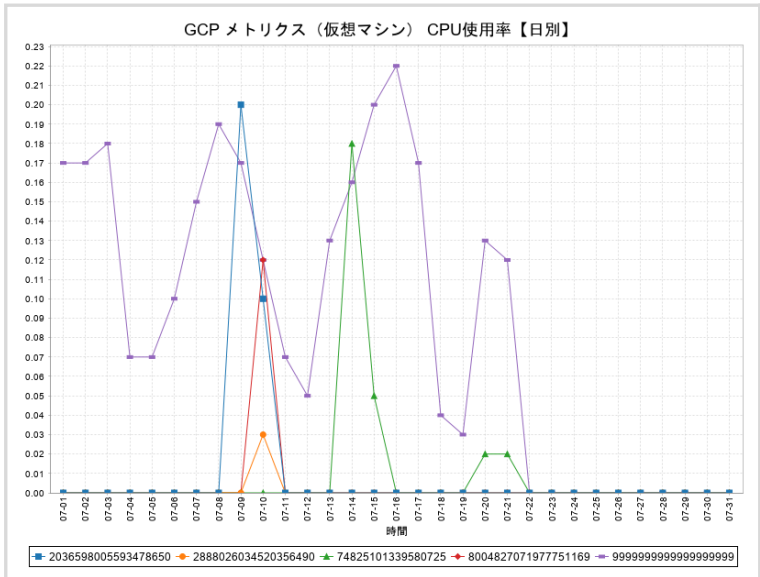


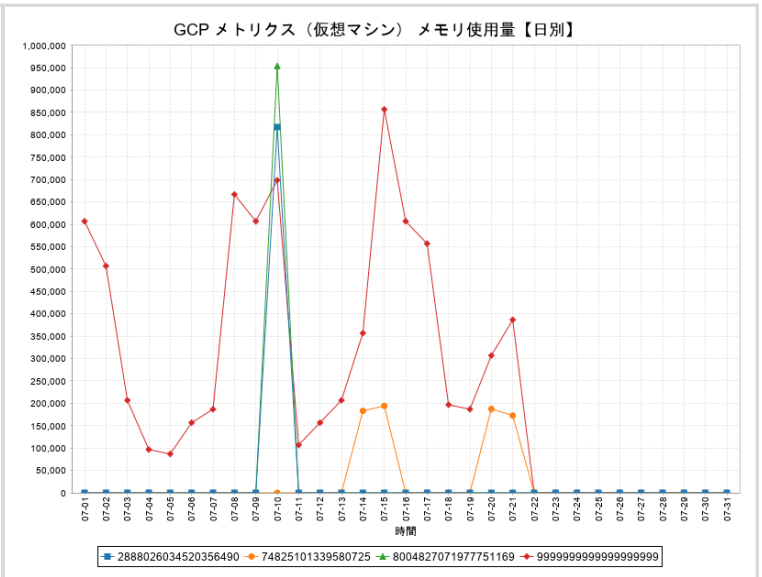


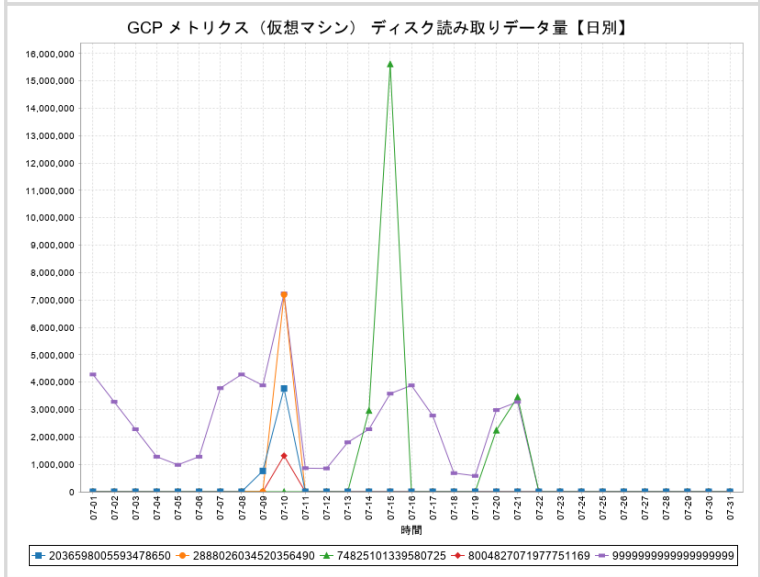


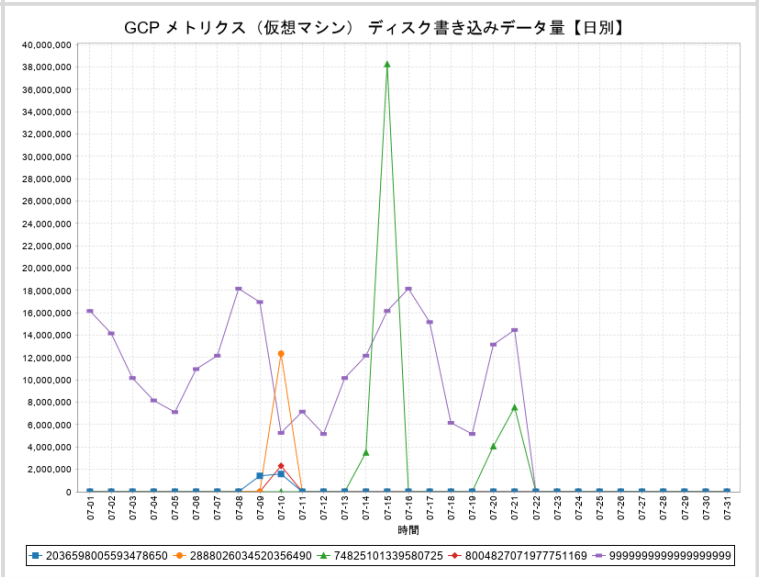


メトリクスデータ(仮想マシン) / テンプレート例





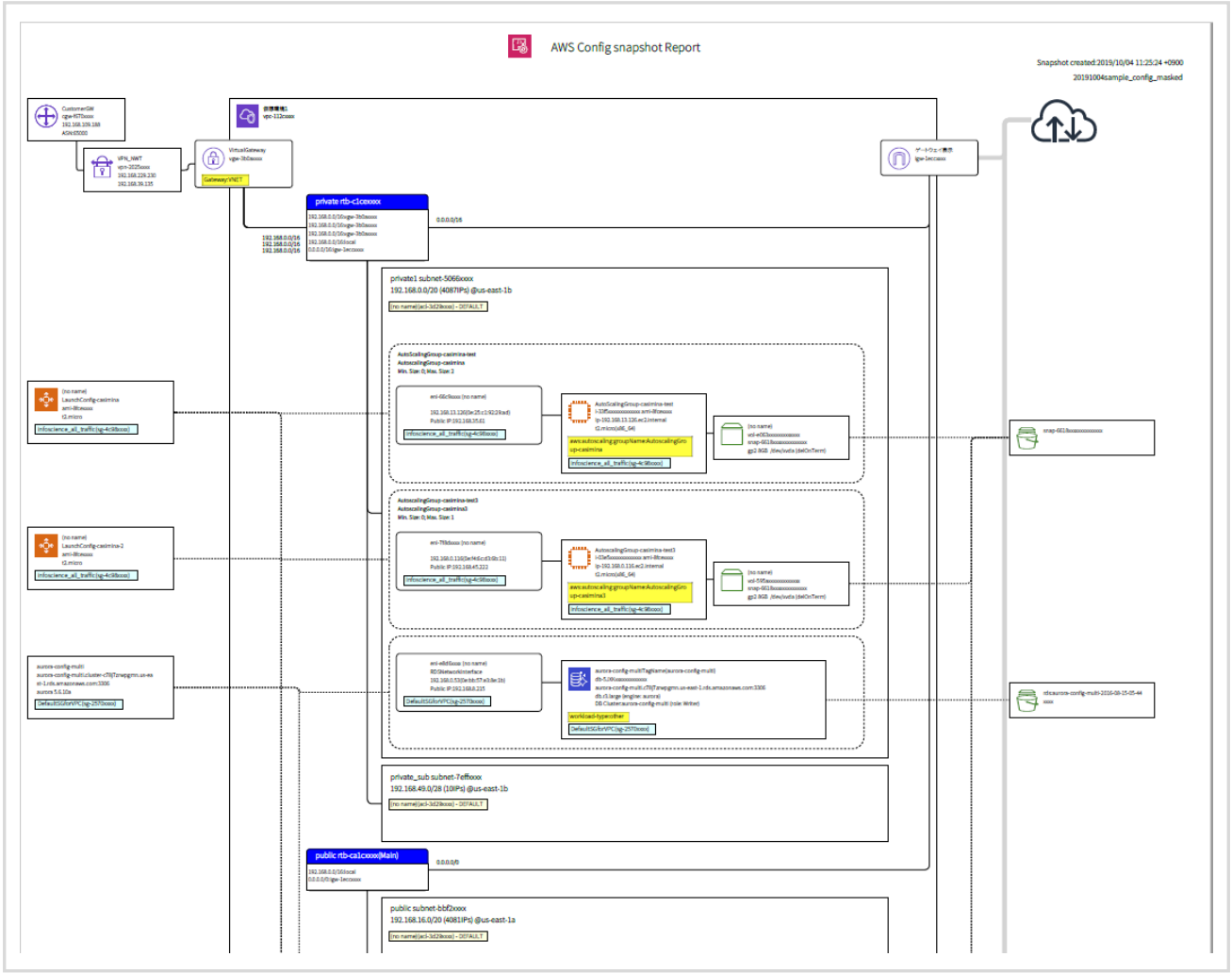




AWS Config スナップショットレポート

Logstorage

レポート実行時点のVPC内のリソース構成情報を出力します。



Logstorage Box 連携パック

- Box上のログ管理 -

Logstorage Microsoft 365 連携パック

- Microsoft 365上のログ管理 -

Logstorage Google Workspace 連携パック

- Google Workspace上のログ管理 -

Logstorage Cybereason 連携パック

- Cybereason上のログ管理 -

Box

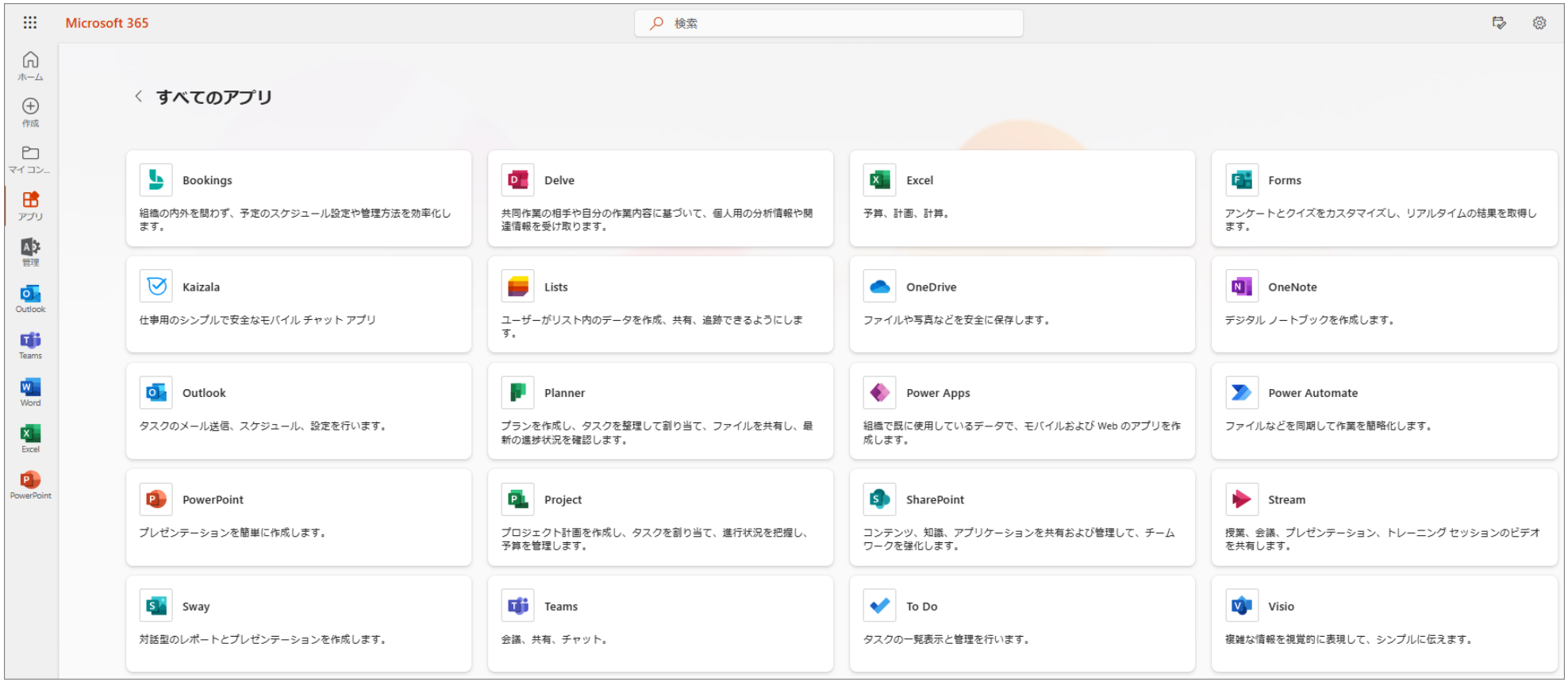
Box社が提供するセキュアなファイル共有とコラボレーションを実現したクラウドサービスです。
場所やデバイスを問わず、誰とでもファイル共有することが可能です。

Microsoft 365

Logstorage

Microsoft社が提供するクラウドサービスです。

Microsoft 365アプリ、ストレージ、最高水準のセキュリティを一つに纏めたソリューションとして展開しています。場所やデバイスを問わずに利用でき、常に最新のOfficeの機能とセキュリティが提供されることから、オンプレミス型のOffice製品からMicrosoft 365に切り替えて運用するケースが非常に増えています。

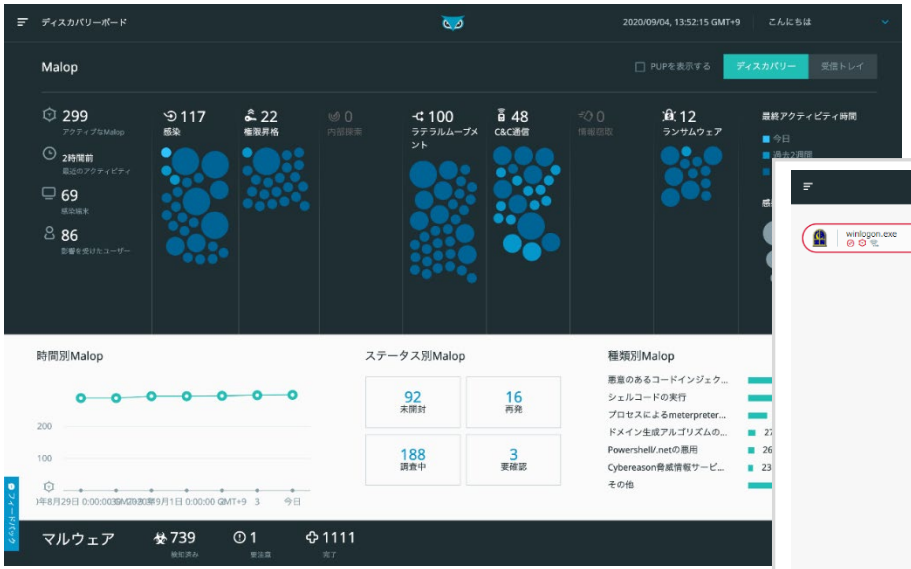


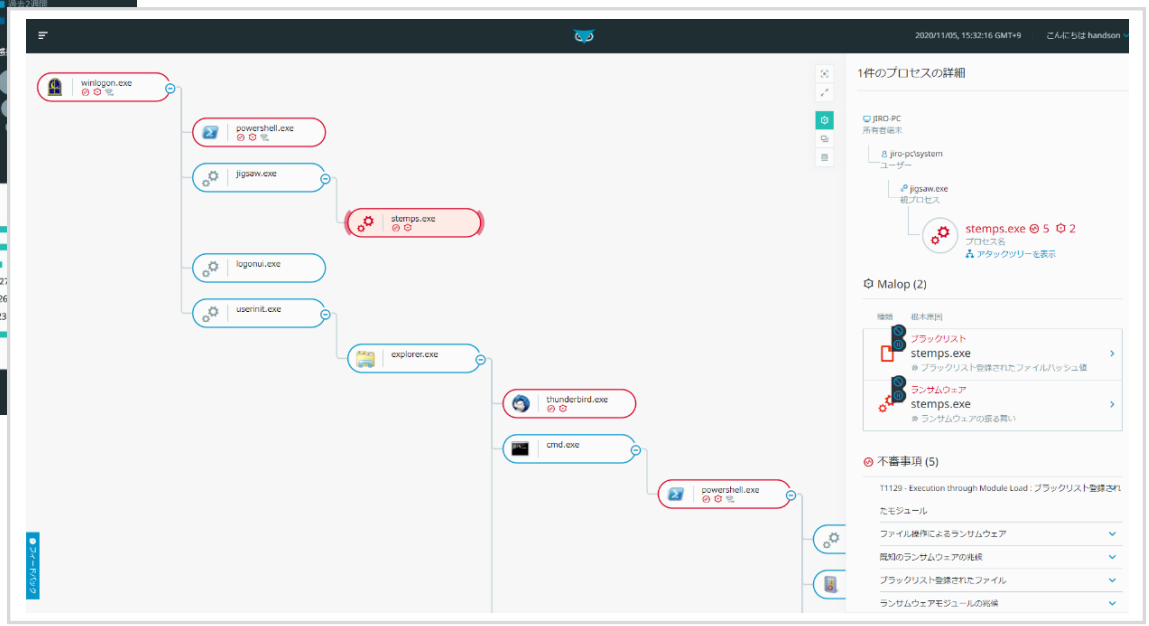
Google Workspace

Google社が提供するグループウェアのクラウドサービスです。
Gmail、ドキュメント、ドライブ、カレンダーなどの機能がスイート化して提供されています。

Cybereason

「Cybereason」は、AIを活用した独自のエンジンでエンドポイントの膨大なログを解析し、サイバー攻撃の兆候をリアルタイムに検知して対処する「Cybereason EDR」と、既知および未知のマルウエアやファイルレスマルウエアなどの侵入をブロックする次世代アンチウイルス「Cybereason NGAV」によって、企業のパソコンやサーバといったエンドポイントセキュリティ対策の強化を支援する、サイバー攻撃対策プラットフォームです。





SaaS との連携について

ユーザーの操作履歴が監査ログに記録されます。

⇒・いつ、誰が、何を、どのように操作したか？

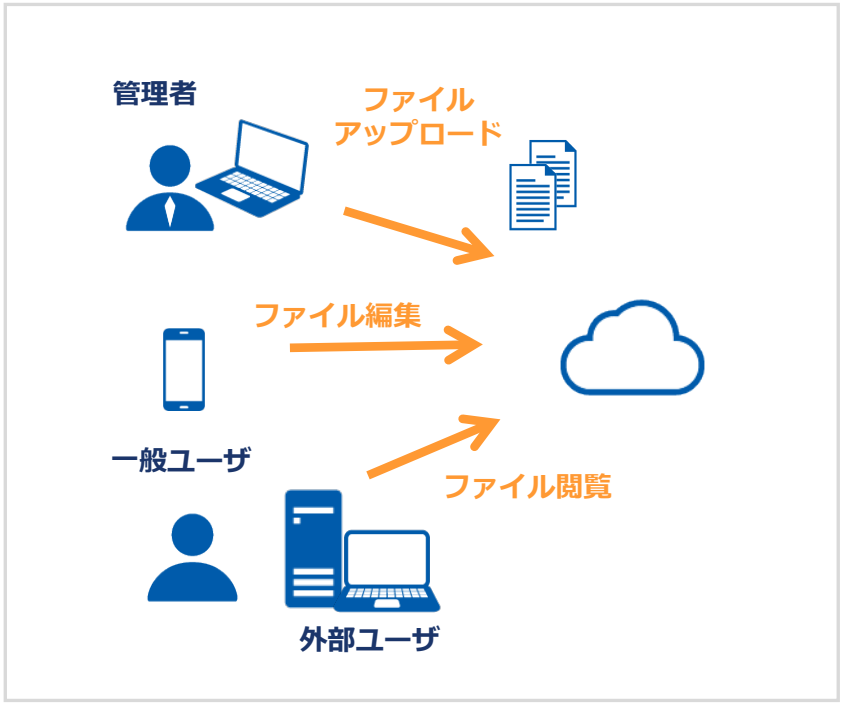
・特定ユーザがある期間に行った操作は？

・どの接続元(IPアドレス)から操作が行われたか？

Microsoft 365 のログ参照可能期間⇒90日

Google Workspace のログ参照可能期間⇒180日

より長い期間のログを保管するためには、別の仕組みを検討する必要があります。



Logstorageオプション機能は、SaaS の監査ログの収集に対応しています！

製品	対応サービス / 機能
Box	Enterprise Events
Microsoft 365	Microsoft 365 監査ログ (Azure Active Directory, Exchange, SharePoint, OneDrive for Business, Microsoft Teams) , Microsoft 365 メッセージ追跡ログ (MessageTrace, MessageTraceDetail)
Google Workspace	管理コンソール, ログイン, SAML, OAuth トークン, ユーザーアカウント, グループ, ドライブ, デバイス
Cybereason	MALOP,マルウェア, 監査ログ

Logstorage – SaaS 連携　テンプレート例

SaaS の操作履歴を可視化

⇒ いつ、誰が、何を、どのように操作したか？

検索条件名: Box 全ログ検索

概要:

検索条件 | 検索結果 | カラムセットアサイン

ログ | カラム　1-50件目 表示 (全69件)　1 2 > >>　[表示数: 100件]　拡張トラッキング　ログを折り込

タイムスタンプ	作成名	作成ログイン	アクション	ソース_項目名(フォルダ・ファイル名)	ソース_親名	IPアドレス	ソース_ログイン
2019-07-15 10:32:34	suzuki	suzuki@infoscience.co.jp	ログイン			192.168.0.123	suzuki@infoscience.co.jp
2019-07-15 10:33:18	suzuki	suzuki@infoscience.co.jp	プレビュー	7月売上情報.xls	売上情報	192.168.0.123	
2019-07-15 10:34:08	suzuki	suzuki@infoscience.co.jp	プレビュー	顧客名簿.doc	顧客情報	192.168.0.123	
2019-07-15 10:35:09	suzuki	suzuki@infoscience.co.jp	ダウンロード	顧客名簿.doc	顧客情報	192.168.0.123	
2019-07-17 17:11:54	Unknown User		ログイン失敗			192.100.0.1	inoue@aaa.co.jp
2019-07-17 17:12:10	inoue	inoue@aaa.co.jp	ログイン			192.100.0.1	inoue@aaa.co.jp
2019-07-17 17:13:57	inoue	inoue@aaa.co.jp	アップロード	20190718_A社様向け打ち合わせ資料	すべてのファイル	192.100.0.1	
2019-07-17 17:13:58	inoue	inoue@aaa.co.jp	外部共有招待	20190718_A社様向け打ち合わせ資料	すべてのファイル	192.100.0.1	
2019-07-17 17:16:26	inoue	inoue@aaa.co.jp	共有	20190718_A社様向け打ち合わせ資料	すべてのファイル	192.100.0.1	
2019-07-17 17:16:35	inoue	inoue@aaa.co.jp	共有項目更新	20190718_A社様向け打ち合わせ資料	すべてのファイル	192.100.0.1	
2019-07-17 17:18:44	inoue	inoue@aaa.co.jp	ログイン追加			192.100.0.1	inoue@aaa.co.jp
2019-07-17 17:22:48	inoue	inoue@aaa.co.jp	アップロード	会議資料.docx	20190718_A社様向け打ち合わせ資料	192.100.0.1	
2019-07-17 17:23:50	Unknown User		ダウンロード	会議資料.docx	20190718_A社様向け打ち合わせ資料	192.100.0.1	
2019-07-17 17:26:44	inoue	inoue@aaa.co.jp	アップロード	案件共有情報.xlsx	20190718_A社様向け打ち合わせ資料	192.100.0.1	
2019-07-17 17:27:11	inoue	inoue@aaa.co.jp	ダウンロード	案件共有情報.xlsx	20190718_A社様向け打ち合わせ資料	192.100.0.1	
2019-07-17 17:33:50	inoue	inoue@aaa.co.jp	外部共有招待	20190718_A社様向け打ち合わせ資料	すべてのファイル	192.100.0.1	
2019-07-18 08:42:24	kimura	kimura-k@gmail.com	ダウンロード	会議資料.docx	20190718_A社様向け打ち合わせ資料	10.66.0.1	
2019-07-18 08:42:24	kimura	kimura-k@gmail.com	ダウンロード	案件共有情報.xlsx	20190718_A社様向け打ち合わせ資料	10.66.0.1	
2019-07-18 08:42:27	kimura	kimura-k@gmail.com	プレビュー	会議資料.docx	20190718_A社様向け打ち合わせ資料	10.66.0.1	
2019-07-18 08:42:46	kimura	kimura-k@gmail.com	アップロード	無題のメモ 2019-07-18 08:42:44.boxnote	20190718_A社様向け打ち合わせ資料	10.66.0.1	

定期的にレポート出力し、ファイル操作履歴を確認することができます。

Box フォルダ・ファイル操作 日別集計レポート

概要　集計条件: Box フォルダ・ファイル操作 集計 で抽出
作成日　2016-08-03 15:56:24
対象期間　2016-07-01 00:00:00 - 2016-07-31 23:59:59

集計条件名　Box フォルダ・ファイル操作 集計
概要　アクション: アップロード／コピー／ダウンロード で抽出

日付	ユーザ	操作	操作対象	件数
2016-07-15	[redacted]	UPLOAD	見積書	1
2016-07-19	[redacted]	DOWNLOAD	外部ファイル	14
	[redacted]	DOWNLOAD	test1.txt	5
		UPLOAD	test1.txt	6
			サンプル.docx	1
			セールスチーム用フォルダ	2
			社内ルール.docx	1
2016-07-20	[redacted]	UPLOAD	Box Reports	1
			folder_tree_run_on_2016-07-19__19-59-35.xlsx	1
	[redacted]	UPLOAD	test001.txt	1
2016-07-22	[redacted]	UPLOAD	test001.txt	1
			テスト共有	1
2016-07-26	[redacted]	DOWNLOAD	外部ファイル	1
		UPLOAD	公開用フォルダ	1
2016-07-27	[redacted]	UPLOAD	test	1
			test2	1
2016-07-28	[redacted]	DOWNLOAD	usage_log_run_on_2016-07-27__21-48-20.xlsx	1
			外部ファイル	1
		UPLOAD	usage_log_run_on_2016-07-27__21-48-20.xlsx	1
2016-07-29	[redacted]	DOWNLOAD	サンプル.docx	1
			社内ルール.docx	2
		UPLOAD	サンプル.docx	1
			セールスチーム用フォルダ	1
			社内ルール.docx	1

Microsoft 365 MessageTrace

いつ、誰が、誰宛てにメールを送信したかを確認することができます。

検索条件名: Microsoft 365 メッセージ追跡

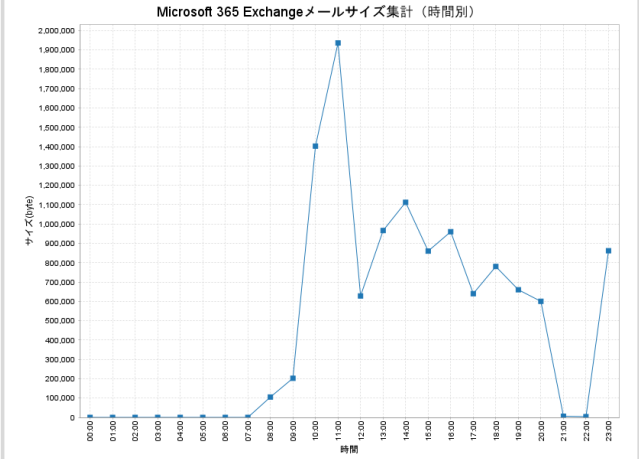
概要:

検索条件 | 検索結果 | カラムセットアサイン

ログ | カラム　1-18件目表示 (全18件)

タイムスタンプ	差出人アドレス	宛先アドレス	件名	アクション	送信元IP	サイズ
2022-12-10 10:48:17	ito@infoscience.com	sato@abc.com	○○案件:打ち合わせの日程調整	Delivered	100.10.0.1	2922015
2022-12-10 10:19:16	ito@infoscience.com	sato@abc.com	○○案件:打ち合わせの日程調整	Delivered	100.10.0.1	17697
2022-12-10 10:14:19	MicrosoftExchange329exxx@infoscience.com	ito@infoscience.com	配信不能: ○○案件:打ち合わせの日程調整	Delivered	null	40152
2022-12-10 10:14:18	ito@infoscience.com	kitagawa@infoscience2.co.jp	○○案件:打ち合わせの日程調整	Failed	100.10.0.1	13477
2022-12-10 10:07:24	MicrosoftExchange329exxx@infoscience.com	ito@infoscience.com	配信不能: ○○案件:打ち合わせの日程調整	Delivered	null	59885
2022-12-10 10:07:23	ito@infoscience.com	kato@infoscience.com	○○案件:打ち合わせの日程調整	Failed	100.10.0.1	13315
2022-12-09 11:14:30	MicrosoftExchange329exxx@infoscience.com	kato@infoscience.com	配信不能: 情報共有ミーティング (2022年12月)	Resolved	null	90052
2022-12-09 11:14:30	MicrosoftExchange329exxx@infoscience.com	kato-11@gmail.com	配信不能: 情報共有ミーティング (2022年12月)	Failed	null	90052

時間	サイズ(byte) 合計
2022-11-21 00	0
2022-11-21 01	0
2022-11-21 02	0
2022-11-21 03	0
2022-11-21 04	0
2022-11-21 05	0
2022-11-21 06	0
2022-11-21 07	0
2022-11-21 08	105098
2022-11-21 09	202466
2022-11-21 10	1402466
2022-11-21 11	1936284
2022-11-21 12	628064
2022-11-21 13	965976
2022-11-21 14	1112114
2022-11-21 15	860000
2022-11-21 16	960000
2022-11-21 17	640000
2022-11-21 18	780000
2022-11-21 19	660000
2022-11-21 20	600000
2022-11-21 21	6000
2022-11-21 22	4000
2022-11-21 23	861668



時間別のメールサイズを可視化、

表やグラフ(棒グラフ、折れ線グラフ等)で

出力できます。

組織外のユーザーからアクセスされたフォルダ・ファイルの一覧が確認できます。

集計条件名: Google Workspace ドライブ 組織外からアクセスされたフォルダ・ファイル

概要: ※抽出条件の「@infoscience¥.co¥.jp」は自ドメインに変更してください。

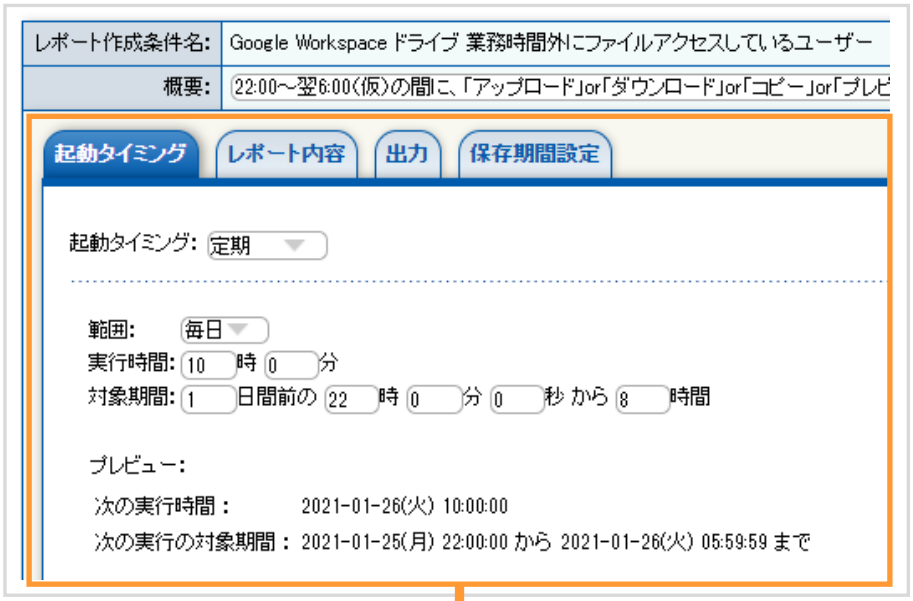
集計対象設定　集計条件設定　集計結果

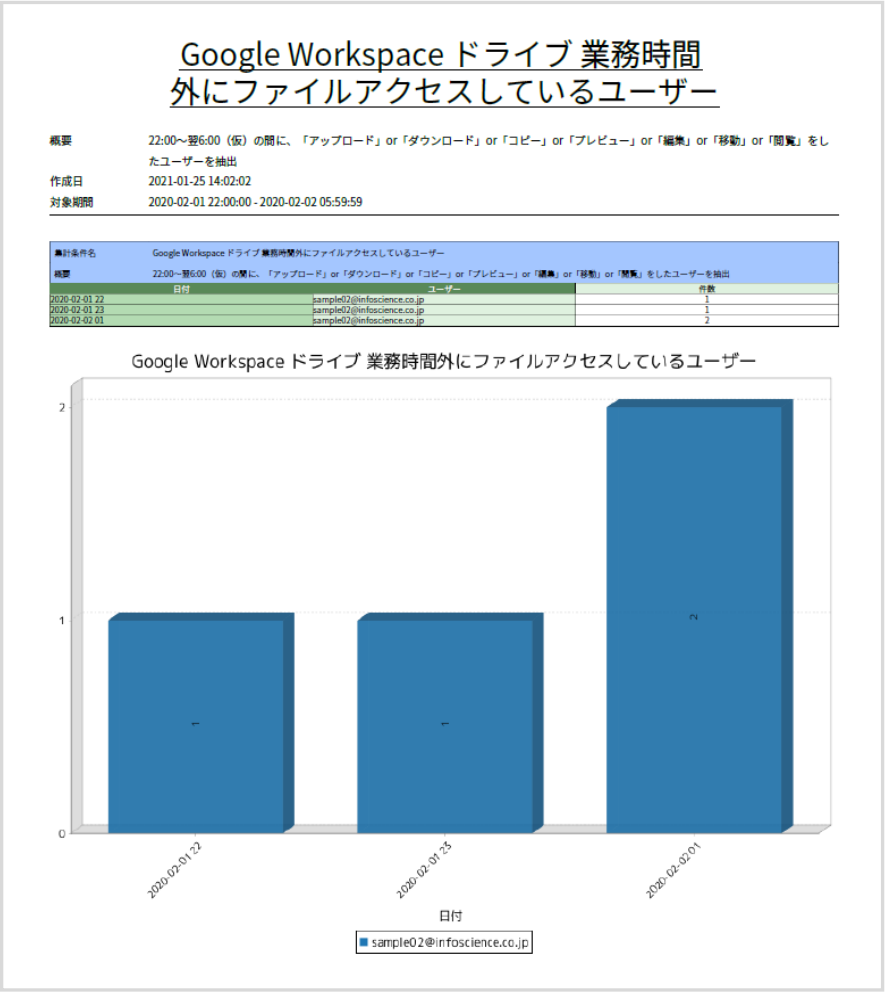
表を表示

時間	アイテム名	ユーザー	件数
2020-02-09	20200209_打ち合わせ	sample01@infoscience.com	3
	nsw_share	sasaki@aaa.com	7
		yamamoto@aaa.com	1
	打ち合わせ議題候補	nakamura@ccc.com	2
		sasaki@aaa.com	2
	製品リスト(2020年版)	ito@aaa.com	1
		kato@aaa.com	1
		sasaki@aaa.com	1
		sasaki@ccc.com	1
		sato@infoscience.com	1
		suzuki@aaa.com	1
		takahashi@aaa.com	1
		watanabe@aaa.com	1
	開発議事録(202001xx)	sasaki@aaa.com	1
2020-02-14	view.txt	tanaka@bbb.com	1
	セミナー候補.txt	suzuki@aaa.com	2
	打ち合わせ議題候補	sasaki@aaa.com	3
		sasaki@infoscience.com	1
		yamaguti@ccc.com	1
2020-02-21	パートナー様向け説明会資料		56
		sasaki@aaa.com	1
2020-02-29	20200129〇△様案件議事録.txt	tanaka@bbb.com	2
総合計			91

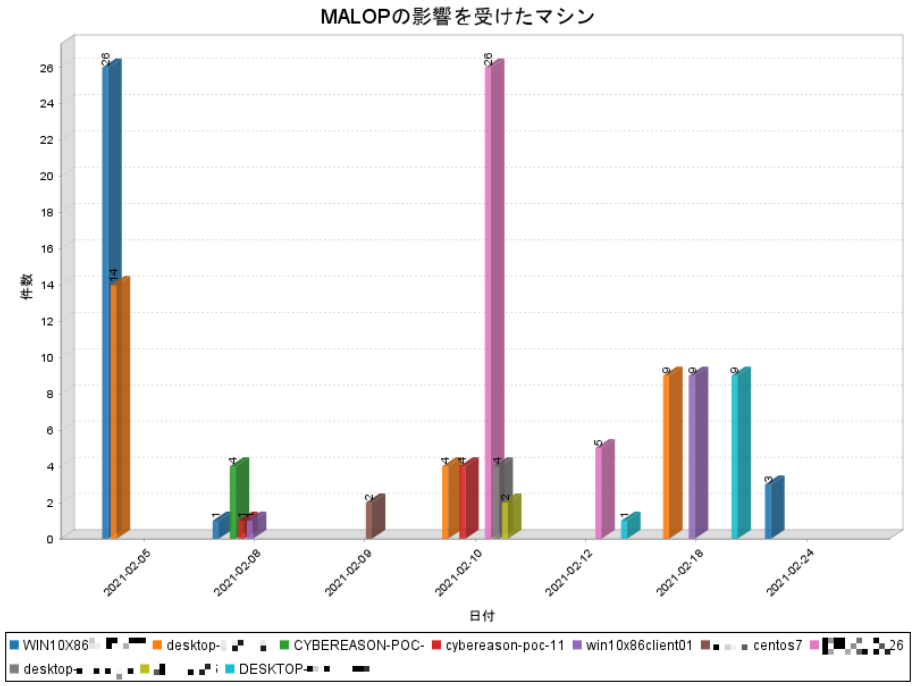
Logstorage – SaaS 連携　テンプレート例

業務時間外でのファイルアクセス状況を定期的に把握することができます。

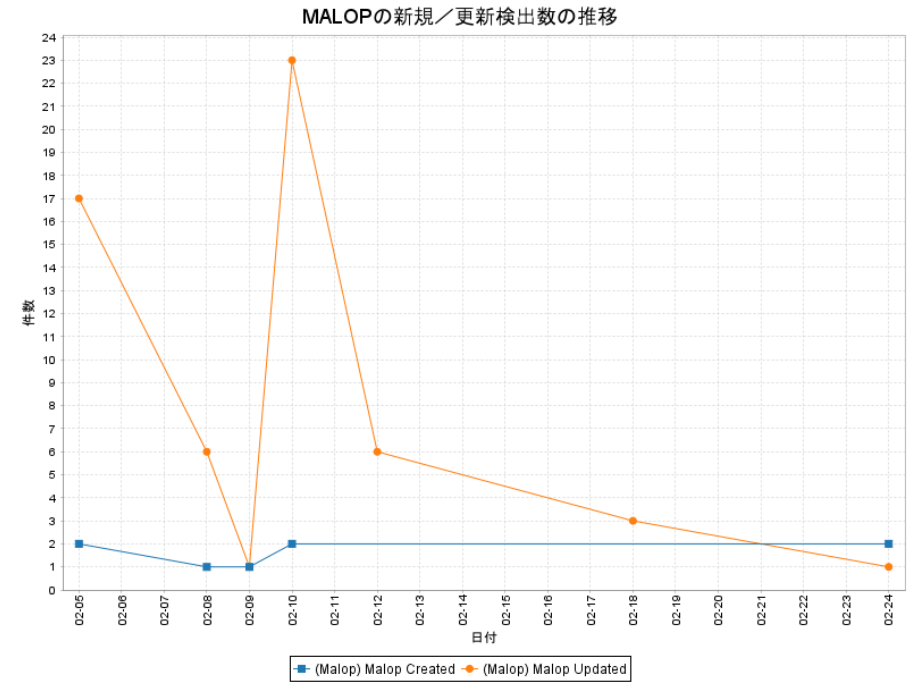




Cybereason



Cybereason EDR で検出された
MALOPの件数（新規／更新）を確認できます。



Cybereason EDR で検出された
MALOPの出現元のマシン情報を確認できます。

ライセンス

ライセンス内容	
製品名称	Logstorage対応パック for AWS Logstorage Azure 連携パック Logstorage GCP 連携パック Logstorage Box 連携パック Logstorage Microsoft 365 連携パック Logstorage Google Workspace 連携パック Logstorage Cybereason 連携パック
含まれる機能	**ログ収集モジュール** ⇒各サービスのログ・データを収集するためのモジュール。 ※Cybereason 連携パックには含まれません。
	ログフォーマット定義・タグ定義 ⇒各サービスのログフォーマット定義とタグ定義。
	検索／集計／レポートテンプレート ⇒各サービスのログを分析するためのテンプレート。
ライセンス価格	※別紙参照

木曜セミナーのご案内

随時、Logstorageのご紹介セミナーを開催しております。

■**第1部『Logstorageのご紹介』**

ログ活用の事例を交えながら、統合ログ管理システムLogstorageの機能をご紹介致します。

■**第2部『Logstorage クラウド対応製品紹介』**

クラウド(AWS, Azure, Box, Microsoft 365, GCP, Google Workspace, Cybereason)のログ監視、リソースの可視化に役立つLogstorageの活用方法をご紹介いたします。

アジェンダ	・セキュリティとログ管理 ・ログ管理の問題点とLogstorageによる解決 ・Logstorageの機能紹介 ・最新版Logstorageのデモ ・質疑応答 ※内容は予告なく変更になる場合がございます。ご了承ください。
タイムテーブル	14：00～14：30　第1部　Logstorage 本体製品紹介 14：30～14：35　休憩 14：35～15：00　第2部　Logstorage クラウド対応製品紹介
開催日程	木曜日（不定期） ※詳しくは https://logstorage.com/webinar/ をご覧ください。
参加費	無料
お申し込み方法	お申込みフォームより必要事項をご記入の上、お申込みください。
注意事項	本ウェビナーはGoToWebinarを利用して開催いたします。 GoToWebinarのシステム要件や接続方法等については、 https://logstorage.com/pdf/webinar_guide.pdf をご確認ください。 同業他社様からのお申し込みをお断りさせて頂いております。 当フォームは法人向けの為、フリーメールアドレスで申し込まれた場合は 当社からの回答をお送りできない場合がございます。ご了承ください。 企業でご利用のメールアドレスをご利用ください。
お問い合せ	E-mail：seminar@logstorage.com Tel：03-5427-3503

開発元

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
https://www.infoscience.co.jp/

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
TEL 03-5427-3503　　FAX 03-5427-3889
https://logstorage.com/
mail : info@logstorage.com