統合ログ管理システム Logstorage
AWS アライアンス版・対応パック 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

インフォサイエンス株式会社 概要

◆設立
1995年10月

◆代表者
宮 紀雄

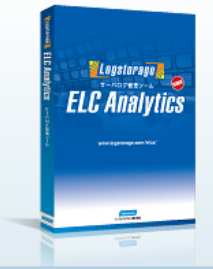
◆事業内容
- プロダクト事業
  パッケージソフトウェア「Logstorage」シリーズの開発
- SaaS事業
  メンバーシップマネジメントソリューション「Jimzen」の開発

◆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

パッケージラインナップ

統合ログ管理システム
Logstorage

サーバログ管理ツール
Logstorage ELC Analytics



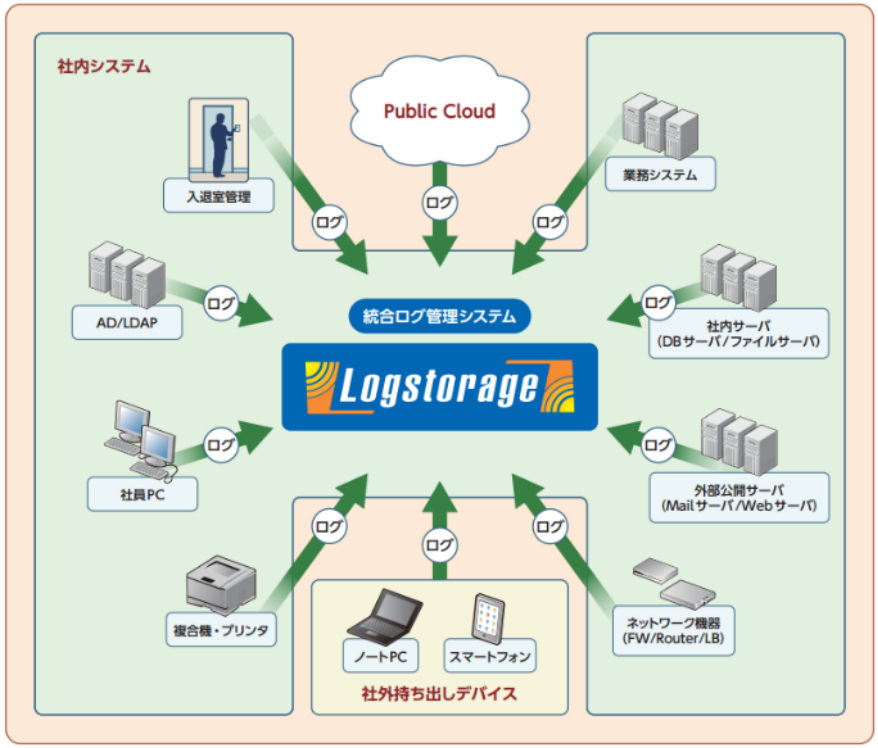
Logstorage：Cloud Solutions
Logstorage
aws
Microsoft Azure
Google Cloud
Microsoft 365
Google Workspace
box
cybereason

統合ログ管理システム「Logstorage」

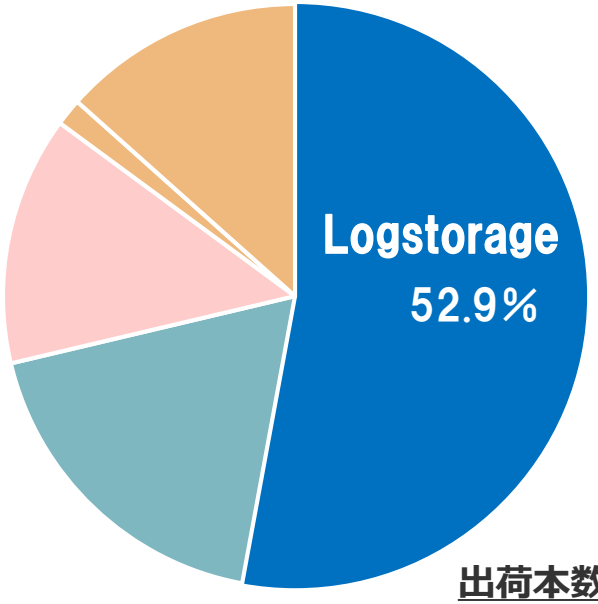
統合ログ管理システム「Logstorage」

「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。



14年連続市場シェアNo.1
4,100社への導入実績



出荷本数シェア

出典：デロイト トーマツ ミック経済研究所株式会社
「内部脅威対策ソリューション市場の現状と将来展望 2020年度版
(統合ログ管理ツール部門)」

統合ログ管理システム「Logstorage」

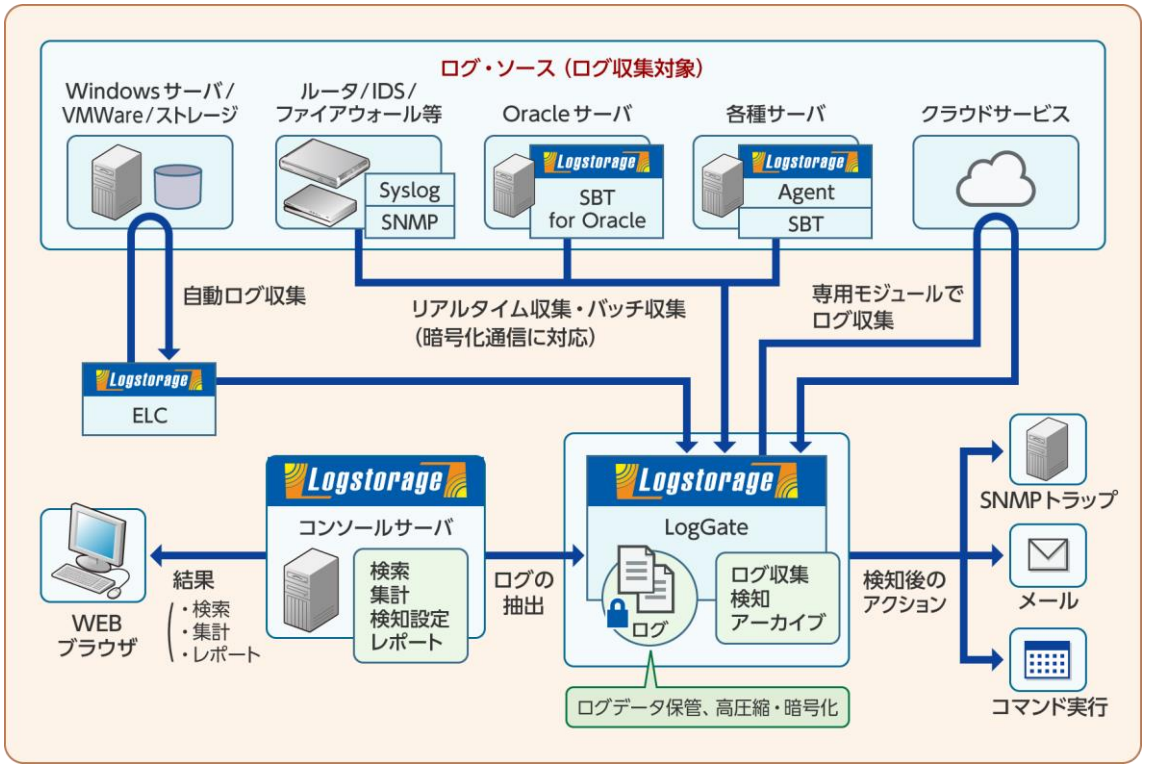
ログ収集機能

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

[ログ送信・取得機能]
- Agent
- EventLogCollector
- 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



<Logstorage システム構成>

ログ検知機能

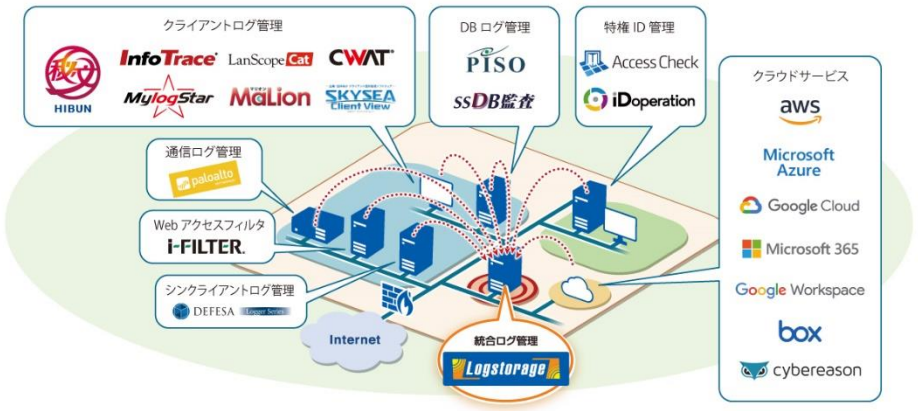
- ポリシーに合致したログのアラート
- ポリシーはストーリー的に定義可能(シナリオ検知)

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 ログ収集実績 / 連携製品

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



【Logstorage 連携製品】

LanScope Cat	SecureCube / AccessCheck
CWAT	InfoTrace
MylogStar	DEFESA Logger シリーズ
i-FILTER	MaLion
SSDB監査	PISO
SKYSEA Client View	Palo Alto Networks NGFW
秘文	iDoperation
Amazon Web Services (AWS)	Microsoft Azure
Google Cloud Platform (GCP)	Microsoft 365
Box	Google Workspace
Cybereason	

[OSシステム・イベント]
- Windows
- Solaris
- AIX
- HP-UX
- Linux
- BSD

[クライアント操作]
- LanScope Cat
- InfoTrace
- CWAT
- MylogStar
- DEFESA Logger
- 秘文
- SeP
- QND/QOH
- Malion
- SKYSEA Client View

[サーバアクセス]
- ALogコンバータ
- VISUACT
- File Server Audit
- CA Access Control
- SecureCube / AccessCheck

[運用監視]
- Nagios
- JP1
- Systemwalker
- OpenView
- WebSAM

[Lotus Domino]
- Lotus Domino
- Notes AccessAnalyzer2
- Auge AccessWatcher

[複合機]
- imageRunner
- Apeos
- SecurePrint!

[Web/プロキシ]
- Apache
- IIS
- BlueCoat
- i-FILTER
- squid
- WebSense
- WebSphere
- WebLogic
- Apache Tomcat
- Cosminexus
- Trend Micro Cloud App Security
- InterScan Web Security as a Service
- Zscaler

[データベース]
- Oracle
- SQLServer
- DB2
- PostgreSQL
- MySQL

[データベース監査]
- PISO
- Chakra
- SecureSphere DMG/DSG
- SSDB監査
- AUDIT MASTER
- IPLocks
- Guardium

[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

[ICカード認証]
- SmartOn
- ARCACLAVIS　Revo

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

[メール]
- MS Exchange
- sendmail
- Postfix
- qmail
- Exim
- GUARDIANWALL

[その他]
- VMware vCenter
- Vmware ESXi
- SAP R/3 (ERP)
- NetApp (NAS)
- ex-SG (入退室管理)
- MSIESER
- iSecurity
- Desk Net's
- HP NonStop Server
- System Answer
- AWS
- Microsoft Azure
- BOX
- Microsoft 365
- Google Workspace…その他

Logstorage AWS 対応製品

Amazon Web Services（AWS）

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


Amazon EC2


Amazon Elastic Container Service


Amazon Lambda


AWS Elastic Beanstalk


Elastic Load Balancing

Networking


Amazon VPC


Amazon API Gateway


Amazon CloudFront

Amazon Route 53


AWS Direct Connect

Storage


Amazon Elastic Block Store


Amazon Simple Storage Service


Amazon Glacier


AWS Storage Gateway


Amazon Elastic File System

Security, Identity and Compliance


AWS Identity and Access Management


AWS Key Management Service


AWS Single Sign-On


AWS WAF

Database


Amazon DynamoDB


Amazon RDS


Amazon ElastiCache


Amazon Redshift

Management & Governance


AWS Management Console


AWS CloudTrail


Amazon CloudWatch


AWS Config


AWS CloudFormation


AWS Auto Scaling

AWS上のログ管理の必要性

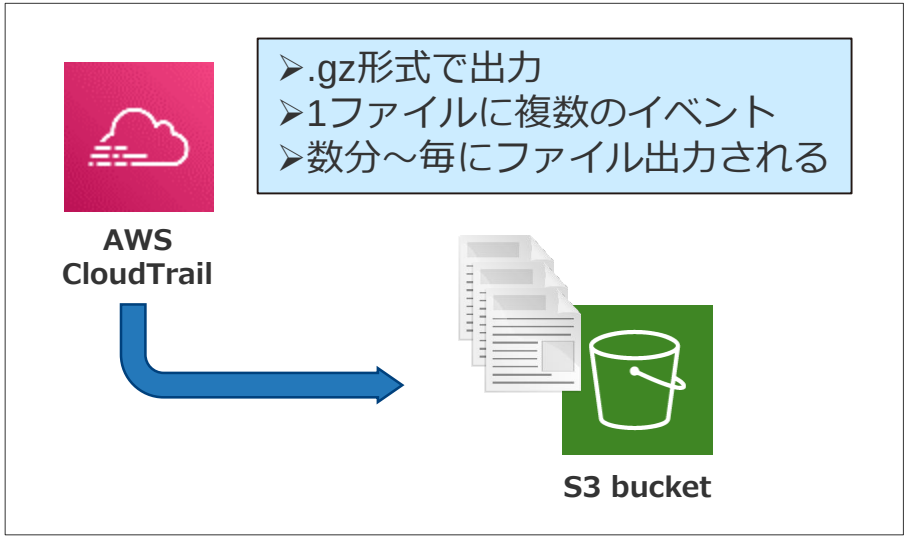
AWSは、Web上で操作でき利便性が高い反面で、作業や操作内容が把握しづらいといった課題があります。ログを活用して見える化をし、監査するための仕組みを作ることが大切です。

ただし、AWSのログ管理の実現には様々な課題に直面します。
一つ一つのサービスの仕様を把握しながら対応を進める必要があり、運用コストが増大する可能性があります。

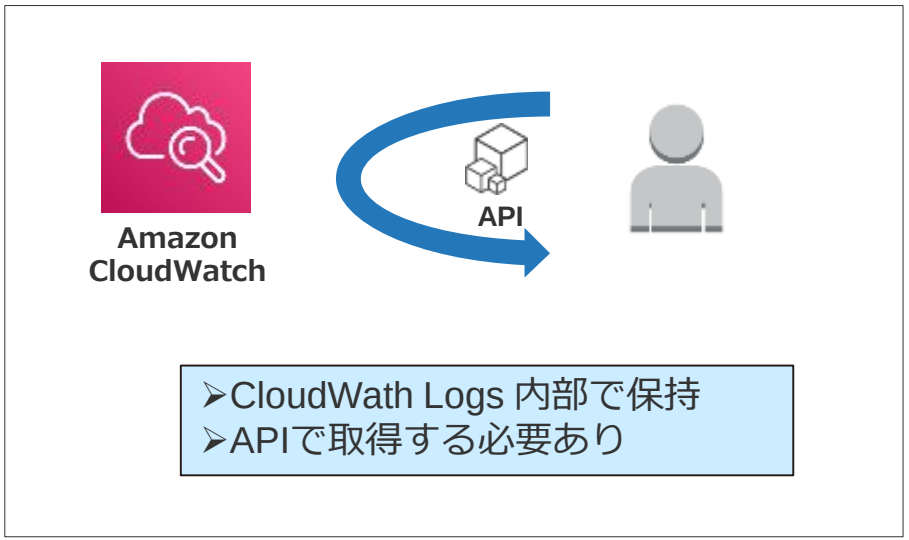
Logstorage と Logstorage 対応パック for AWS では、AWS上のログ管理の様々な課題に対処することが可能です!!

課題1：多様なログの出力方式

AWS CloudTrail



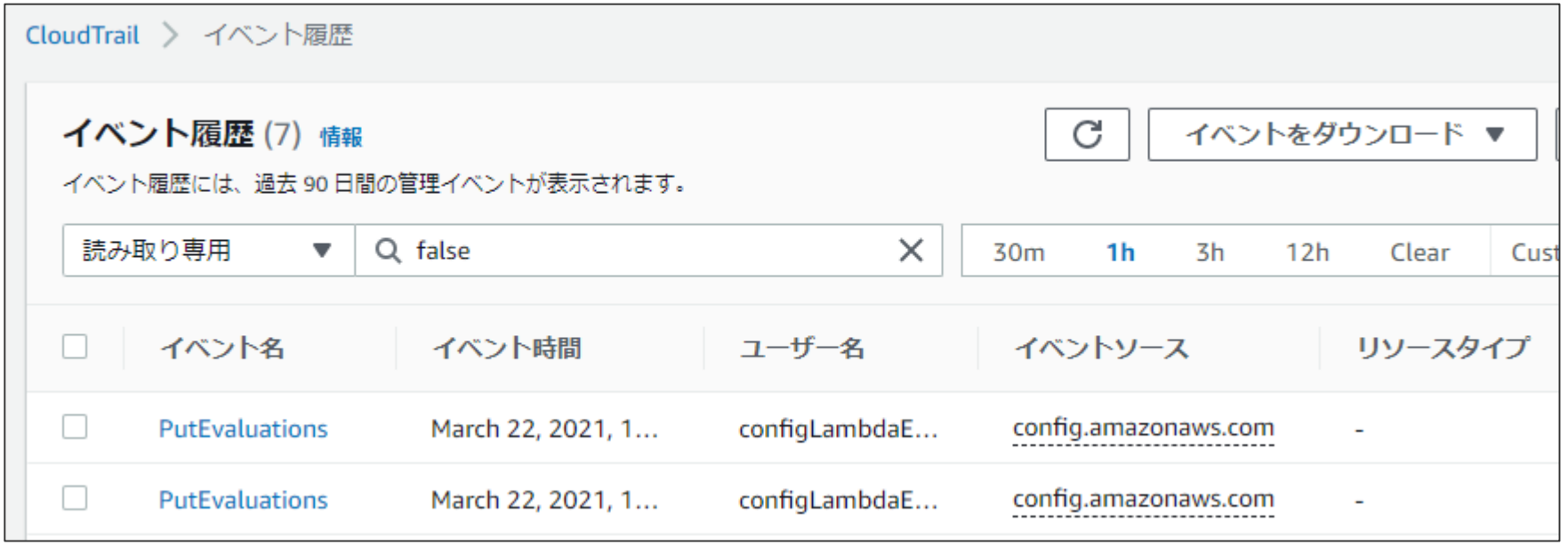
Amazon CloudWatch Logs



サービス毎に異なるログ出力方式に対応する必要があります。

サービス毎に専用のログ収集モジュールをご提供しています。

課題2：ログの参照期間が短い



AWS管理コンソールでは、過去90日間のCloudTrailイベント履歴を参照可能です。一方で、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は、ログをセキュアに長期保管することができます！！

課題3：特定のログを探すのが大変

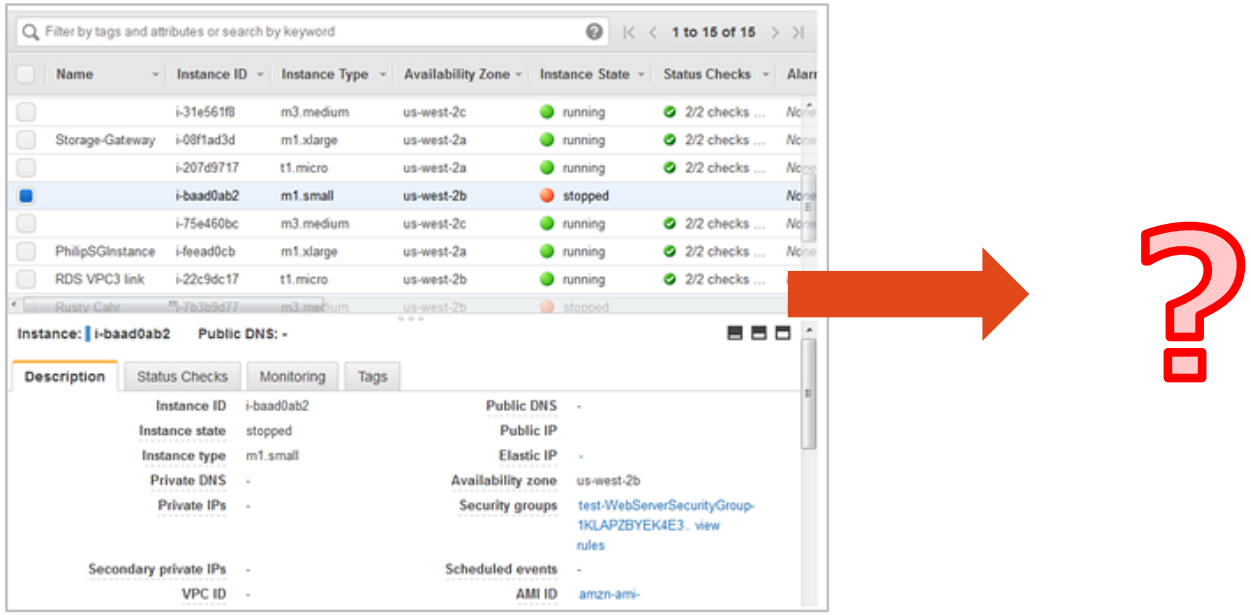
例：AWS CloudTrail のログ

{"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"}}]}}}]}

Amazon S3でログファイルの保存は可能ですが、各ファイルに点在したログの内容を把握することは容易ではありません。上記はAmazon EC2の起動とEC2停止の2操作のログです。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4：システム構成の把握が難しい



Amazon VPC などのネットワーク構成や Amazon EC2・Amazon EBS 等の関連性を把握することは、標準機能ではできません。

AWS Config スナップショットレポートで、システム構成図を確認することができます。

Logstorage 対応パック for AWS 概要

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

Amazon S3
・S3のアクセスログ

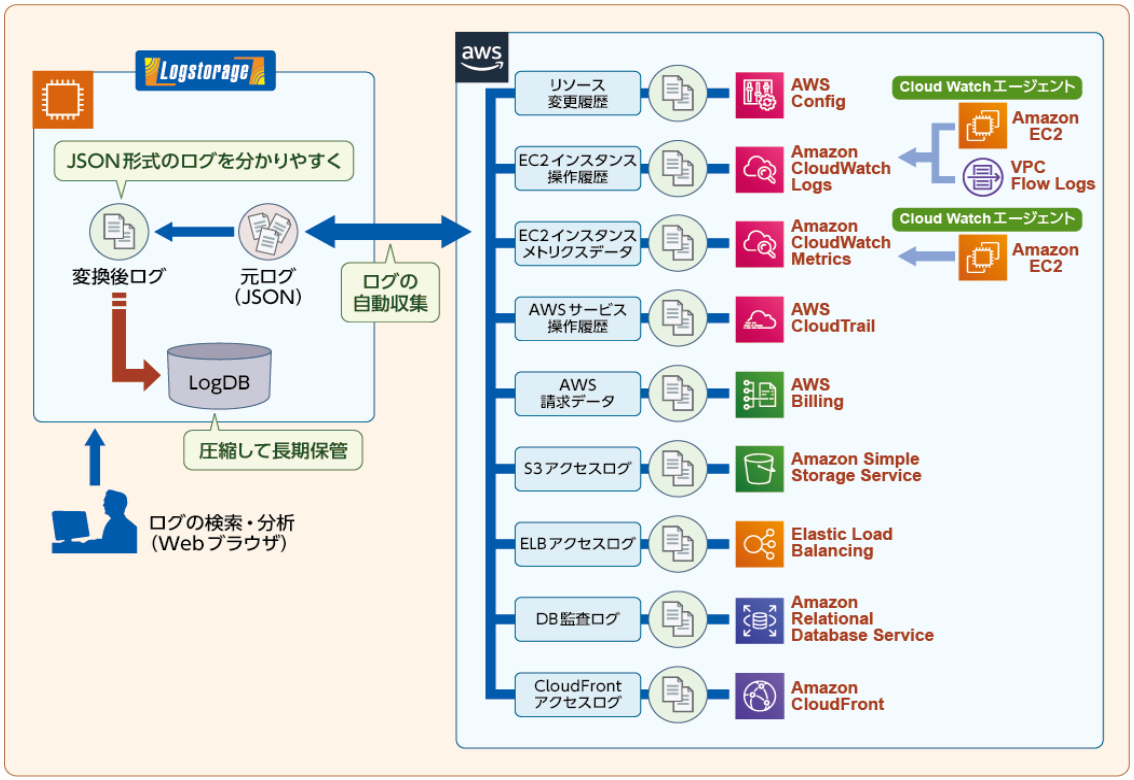
Elastic Load Balancing
・ELBのアクセスログ

Amazon RDS
・SQLクエリーログ

Amazon CloudFront
・CloudFrontのアクセスログ

Amazon CloudWatch Metrics
・サーバーのメトリクス情報

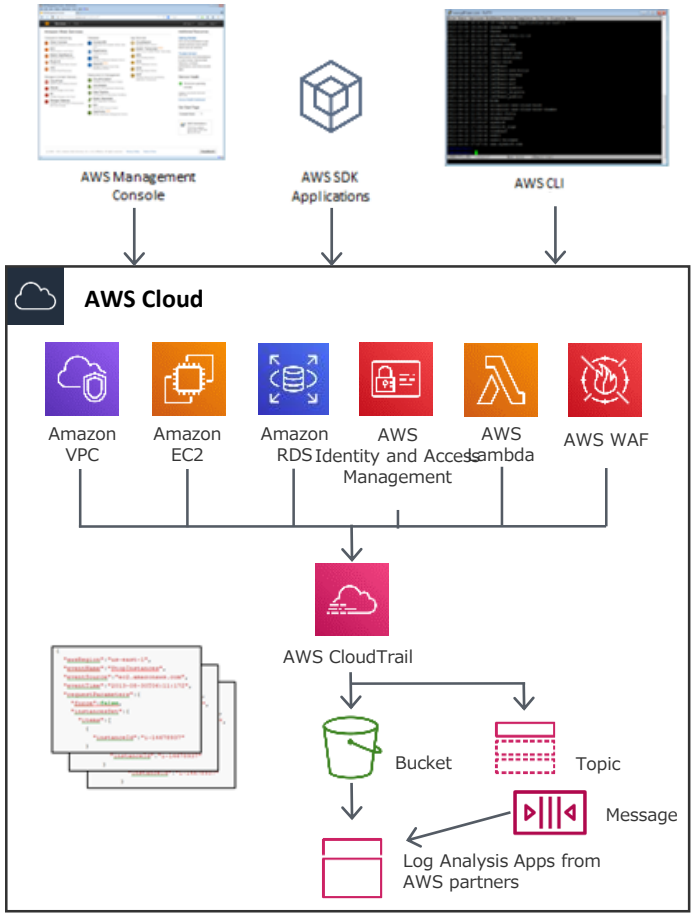
AWS Billing
・AWS請求データ



AWS CloudTrail 対応機能

AWSユーザーの操作やAPIコールを記録するサービス

コンプライアンス準拠	社内規定や規制基準に応じたAWSリソースの管理について説明するために、これらの情報を用いることができます。
リソースの ライフサイクル管理	あるAWSリソースの作成から削除まで追跡することができます。
運用上の トラブルシューティング	リソースに対して最近行われた変更を特定することができます。
セキュリティ分析	不適切な権限でのアクセスによる、拒否されたAPIコールを見ることができます。

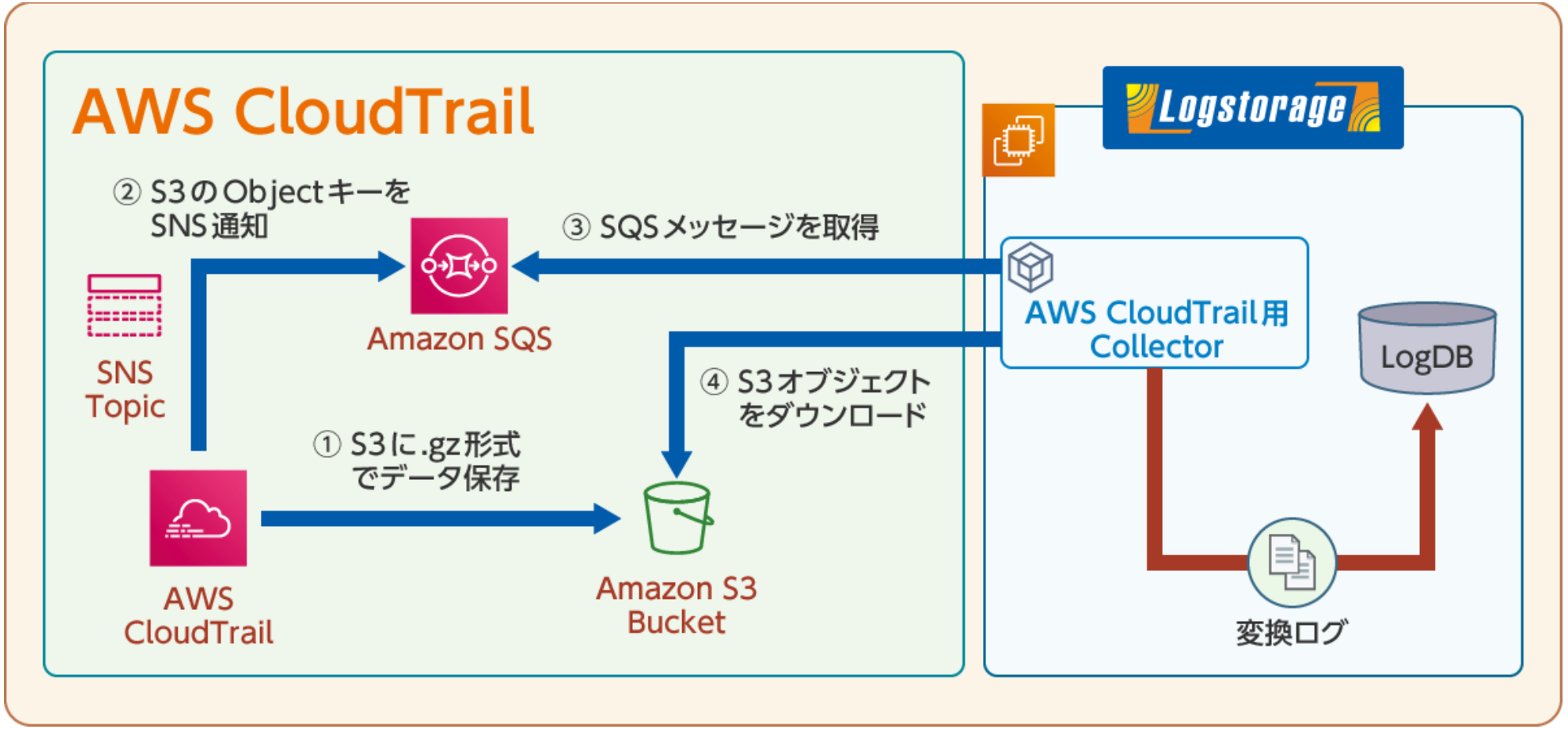


以下のような問いに答えることができます。

- ユーザーが、いつ、何を、どのように操作したか？
- 特定の期間に行われた操作は？
- どの接続元（IPアドレス）から行われた操作か？

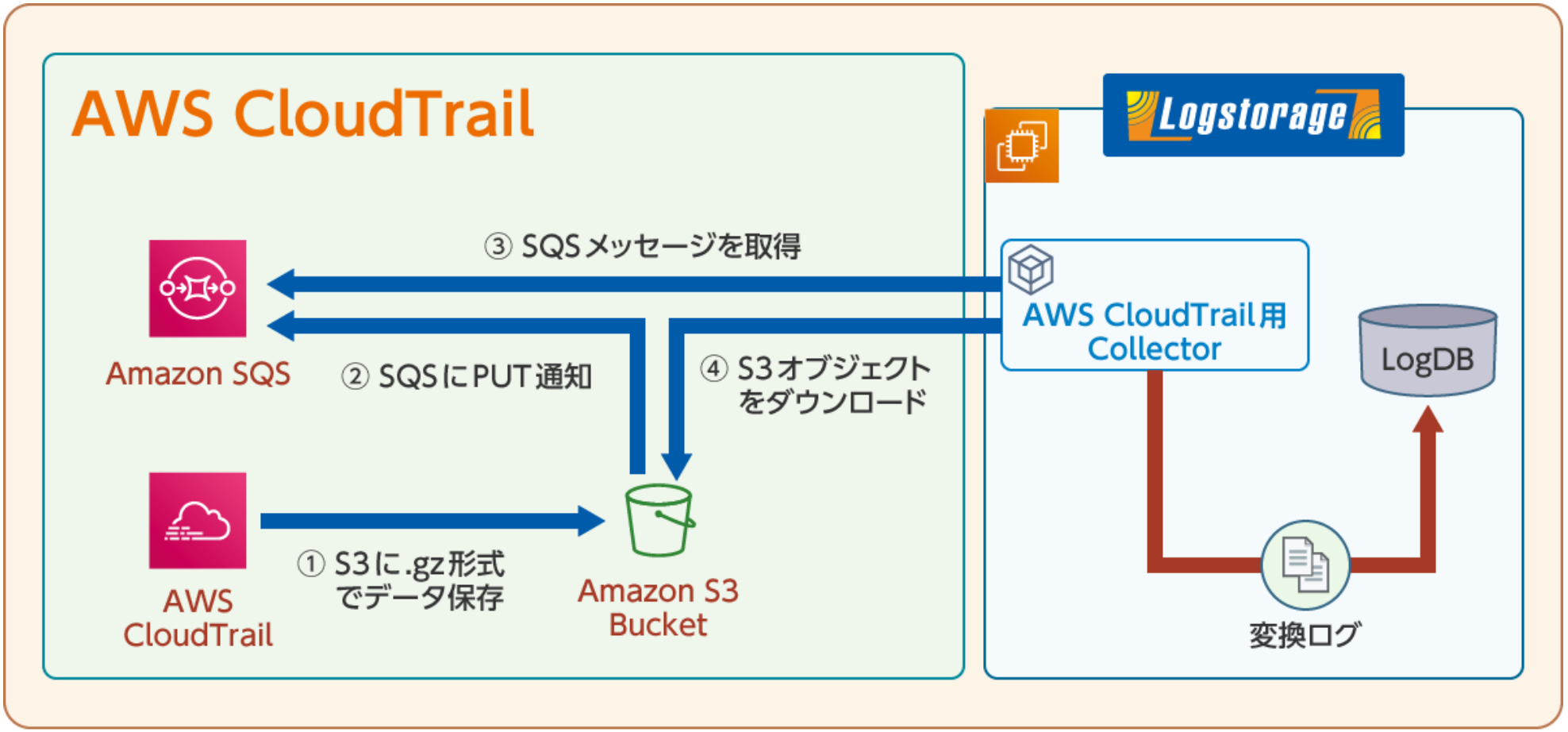
AWS CloudTrail ログ収集の仕組み（１）

AWS CloudTrail のイベント通知を利用



AWS CloudTrail ログ収集の仕組み（２）

Amazon S3 のイベント通知を利用



AWS CloudTrail レポート例

インスタンス削除履歴

概要　eventName: Terminate
作成日　2014-10-03 16:13:54
対象期間　2014-08-01 00:00:00 - 2014-08-31 23:59:59

誤ったインスタンスの削除は無いか

検索条件名　EC2インスタンス削除履歴
概要　eventName: Terminate
件数　10件

タイムスタンプ	arn	awsRegion	sourceIPAddress	requestParameters
2014-08-20 16:50:59	arn:aws:iam::[redacted]:user/mori	ap-northeast-1	[redacted]	instancesSet/items/instanceId=i-f02848e8,instancesSet/items/instanceId=i-2b284832
2014-08-20 17:20:01	arn:aws:iam::[redacted]:user/mori	ap-northeast-1	[redacted]	instancesSet/items/instanceId=i-5db8db44,instancesSet/items/instanceId=i-5db8db44
2014-08-20 17:35:21	arn:aws:iam::[redacted]:root	ap-northeast-1	[redacted]	instancesSet/items/instanceId=i-6583e07f,instancesSet/items/instanceId=i-db82e1c2
2014-08-25 13:52:01	arn:aws:iam::[redacted]:user/mori	ap-northeast-1	[redacted]	instancesSet/items/instanceId=i-191c7e00
2014-08-25 15:14:20	arn:aws:iam::[redacted]:user/mori	ap-northeast-1	[redacted]	instancesSet/items/instanceId=i-e8c8e4ff
2014-08-26 14:23:38	arn:aws:iam::[redacted]:user/mori	ap-northeast-1	[redacted]	instancesSet/items/instanceId=i-c5ff36dc,instancesSet/items/instanceId=i-1f00ac06
2014-08-26 15:53:53	arn:aws:iam::[redacted]:user/mori	ap-northeast-1	[redacted]	instancesSet/items/instanceId=i-08b3d616
2014-08-28 13:16:41	arn:aws:iam::[redacted]:root	ap-northeast-1	[redacted]	instancesSet/items/instanceId=i-5f6ee146
2014-08-29 10:51:28	arn:aws:iam::[redacted]:user/mori	ap-northeast-1	[redacted]	instancesSet/items/instanceId=i-8a84eb93,instancesSet/items/instanceId=i-e1f698fb
2014-08-29 17:34:00	arn:aws:iam::[redacted]:root	ap-northeast-1	[redacted]	instancesSet/items/instanceId=i-6f553c96,instancesSet/items/instanceId=i-d8bdd4c1

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

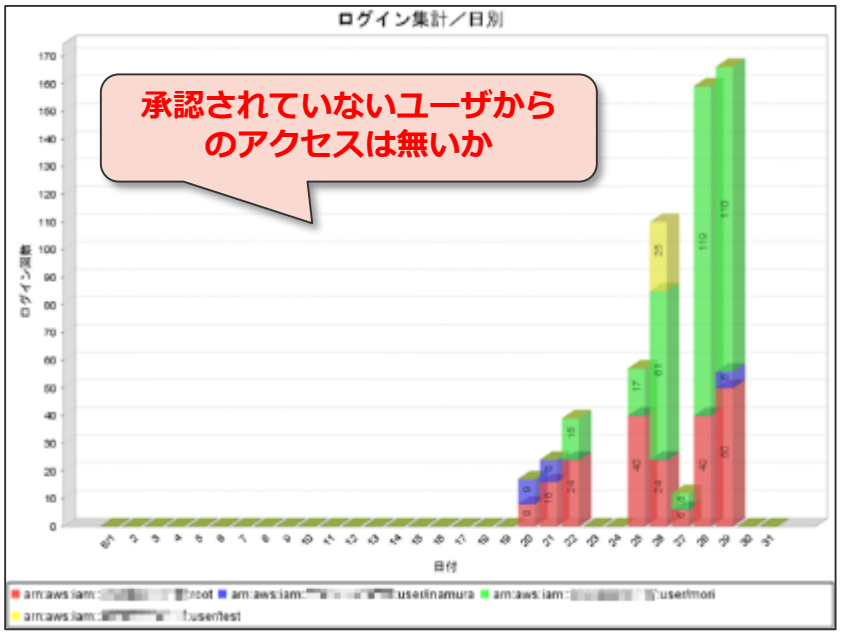
管理の接続は無いか?

検索条件名　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]	4873
	ec2.amazonaws.com	[redacted]	29
	elasticloadbalancing.amazonaws.com	[redacted]	6
	elasticloadbalancing.amazonaws.com	[redacted]	108
	monitoring.amazonaws.com	[redacted]	150
us-west-1	cloudtrail.amazonaws.com	[redacted]	64
	ec2.amazonaws.com	[redacted]	130
	elasticloadbalancing.amazonaws.com	[redacted]	3
	iam.amazonaws.com	[redacted]	760
	monitoring.amazonaws.com	[redacted]	4
	sts.amazonaws.com	signin.amazonaws.com	130
us-west-2	cloudtrail.amazonaws.com	[redacted]	31
	ec2.amazonaws.com	[redacted]	130
	elasticloadbalancing.amazonaws.com	[redacted]	5
		signin.amazonaws.com	3
	monitoring.amazonaws.com	[redacted]	27
		signin.amazonaws.com	1

ログイン集計／日別

承認されていないユーザからのアクセスは無いか



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

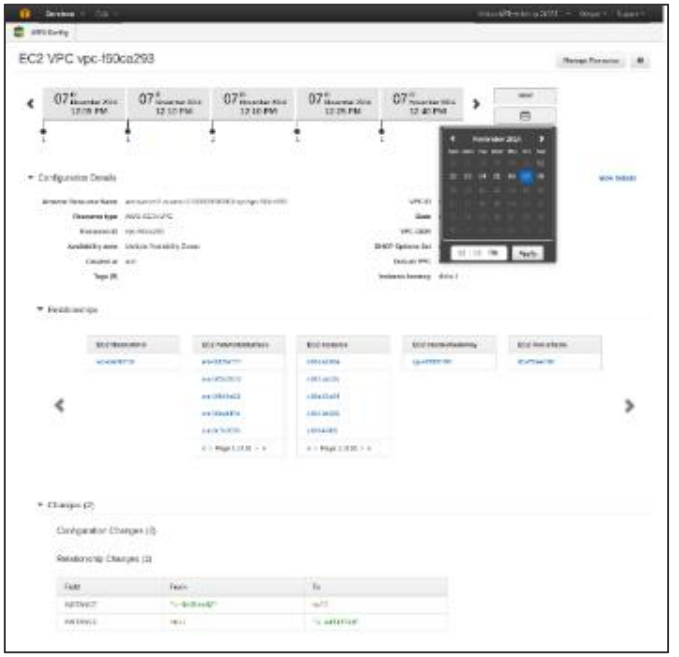
タイムスタンプ	アプリケーション	アクション	Type	arn	userName	eventName	sourceIPAddress	responseElements
2014-08-20 16:59:01	CloudTrail	Sign-In	IAMUser		mori	ConsoleLogin	[redacted]	ConsoleLogin=Failure
2014-08-20 17:02:14	CloudTrail	Sign-In	IAMUser	arn:aws:iam::[redacted]:user/inamura	inamura	ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-20 17:02:37	CloudTrail	Sign-In	IAMUser		mori	ConsoleLogin	[redacted]	ConsoleLogin=Failure
2014-08-20 17:25:04	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-21 08:16:09	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-21 13:43:13	CloudTrail	Sign-In	IAMUser	arn:aws:iam::[redacted]:user/inamura	inamura	ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-21 13:44:45	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-22 09:23:18	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-22 16:31:23	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-22 17:06:30	CloudTrail	Sign-In	IAMUser	arn:aws:iam::[redacted]:user/mori	mori	ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-22 17:12:50	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-25 09:07:59	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-25 11:39:38	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-25 13:48:00	CloudTrail	Sign-In	IAMUser	arn:aws:iam::[redacted]:user/mori	mori	ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-25 16:32:22	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin	[redacted]	ConsoleLogin=Success
2014-08-25 16:33:18	CloudTrail	Sign-In	Root	arn:aws:iam::[redacted]:root		ConsoleLogin	[redacted]	ConsoleLogin=Success

AWS Config 対応機能

AWS Config

AWSリソースの構成変更の通知、構成履歴やインベントリー情報を提供するサービス

リソースの管理	各リソースに対する呼び出しをポーリングして、リソースが作成、変更、削除されるたびに通知が送信されます。
監査とコンプライアンス	自社のポリシーやベストプラクティスに準拠していることを確認するために、リソースの設定履歴を利用できます。
設定変更の管理とトラブルシューティング	他のリソースとの関連性を確認することで、変更時の影響有無を判断できます。
セキュリティ分析	ユーザーに付与されている権限(IAM)の許可や、Amazon EC2 セキュリティグループのルールなどについて、設定履歴を用いてセキュリティの潜在的な脆弱性を分析することができます。



AWS Config 管理コンソール

以下のような問いに答えることができます。

・特定のリソースが、いつ、誰に、どのように操作されたか？
・特定の期間に行われた操作は？

AWS Config Partner / AWS Official Blog で紹介されました！！

AWS CONFIG PARTNERS

- AWS Config - 2nd Watch
- AWS Config - CloudCheckr
- AWS Config - Cloudnexa
- AWS Config - Evident.io
- AWS Config - Red Hat
- AWS Config - RedSeal
- AWS Config - Splunk
- AWS Config - Logstorage
- AWS Config - Service Now

Logstorage

Who we are and what we do

Logstorage, developed by Infoscience Corporation, Japan, offers an integrated log management system that allows you to consolidate your logs and manage them from a browser. You can create various complex searches, analyze statistics, set up alerts and reporting on AWS Config data. For example, you can search which instances are using approved AMIs, or which security groups were recently updated. You also get a visual report of the configuration snapshot delivered by
leading providers of integrated log management

Logstorage is not limited to collecting AWS Confi
in any format(eg. AWS Cloudtrail, Amazon Cloud

Get additional details at: http://www.logstorage.c

Support from LogStorage

The integrated log management application from AWS partner LogStorage now supports AWS Config. Of particular note is the ability to search on individual fields of the notification and to set alerts that are driven by the results. For example, you can easily watch for configuration changes that involve all of your EC2 instances which use a particular AMI. You can also detect when EC2 instances are launched and do not use a set of pre-approved AMIs; this allows you to easily detect usage that is not in accord with your internal standards and practices. Here is what it looks like:

Search Condition | Search Results | Column Set Assignment

Results 1 - 4 (of 4)

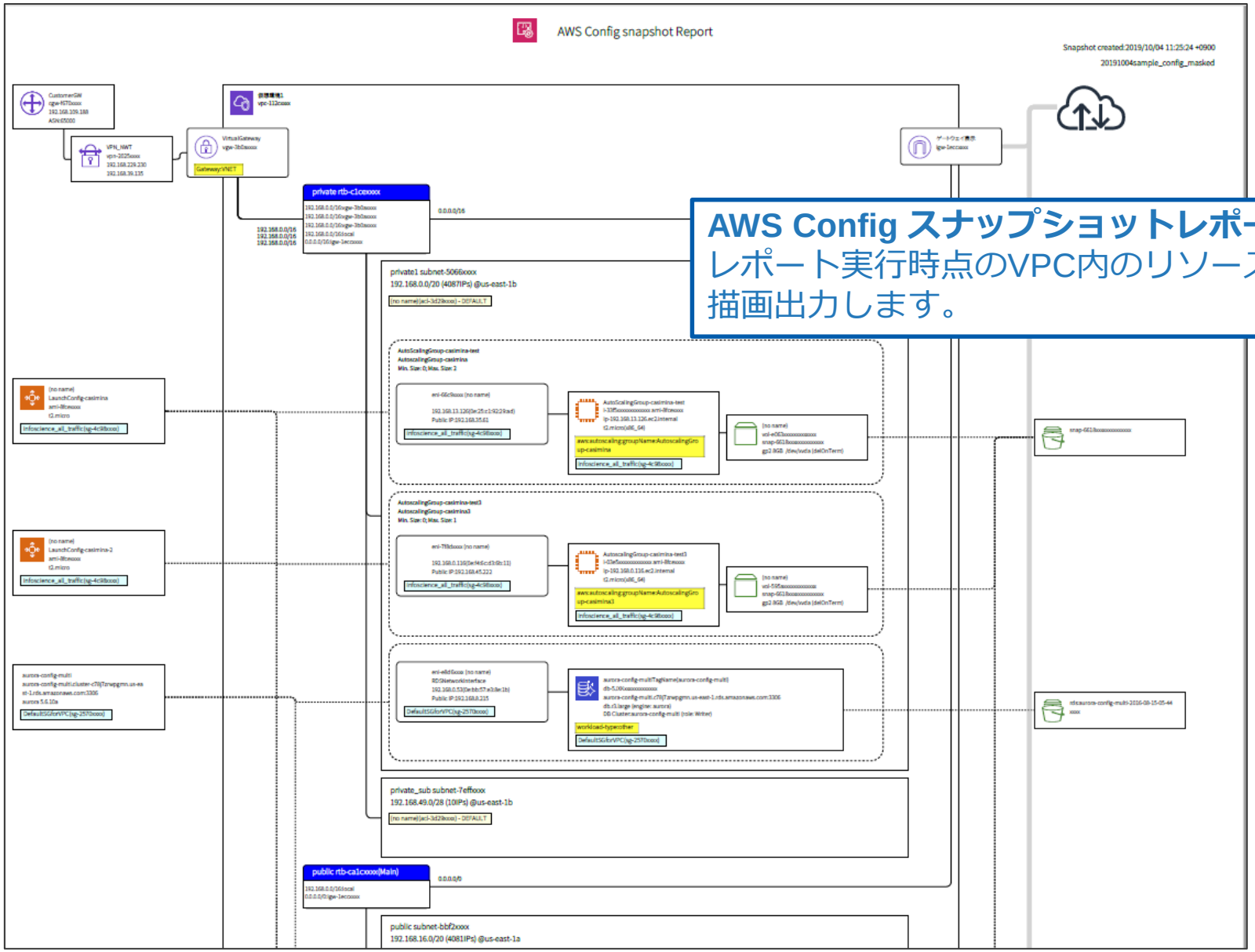
Timestamp	Action	aws_config_changeType	InstanceNameId	aws_resourceId	aws_name	aws_availabilityZone
2015-02-26 11:30:42	EC2:Instance	CREATE	ami-dfc39aef	i-689f9f84	i-689f9f84	us-west-2a
2015-02-27 13:10:38	EC2:Instance	CREATE	ami-dfc39aef	i-73c92b7e	i-73c92b7e	us-west-2b
2015-03-04 11:50:34	EC2:Instance	CREATE	ami-dfc39aef	i-f20114ff	開発:instance1_amazonlinux	us-west-2b
2015-03-06 12:05:46	EC2:Instance	CREATE	ami-dfc39aef	i-224ebf2f	prod.netserver.com	us-west-2b

Results 1 - 4 (of 4)

You can also display a diagram of your AWS resources and explore the relationships (as reported by AWS Config) between them:

URL: https://aws.amazon.com/jp/config/partners/logstorage/

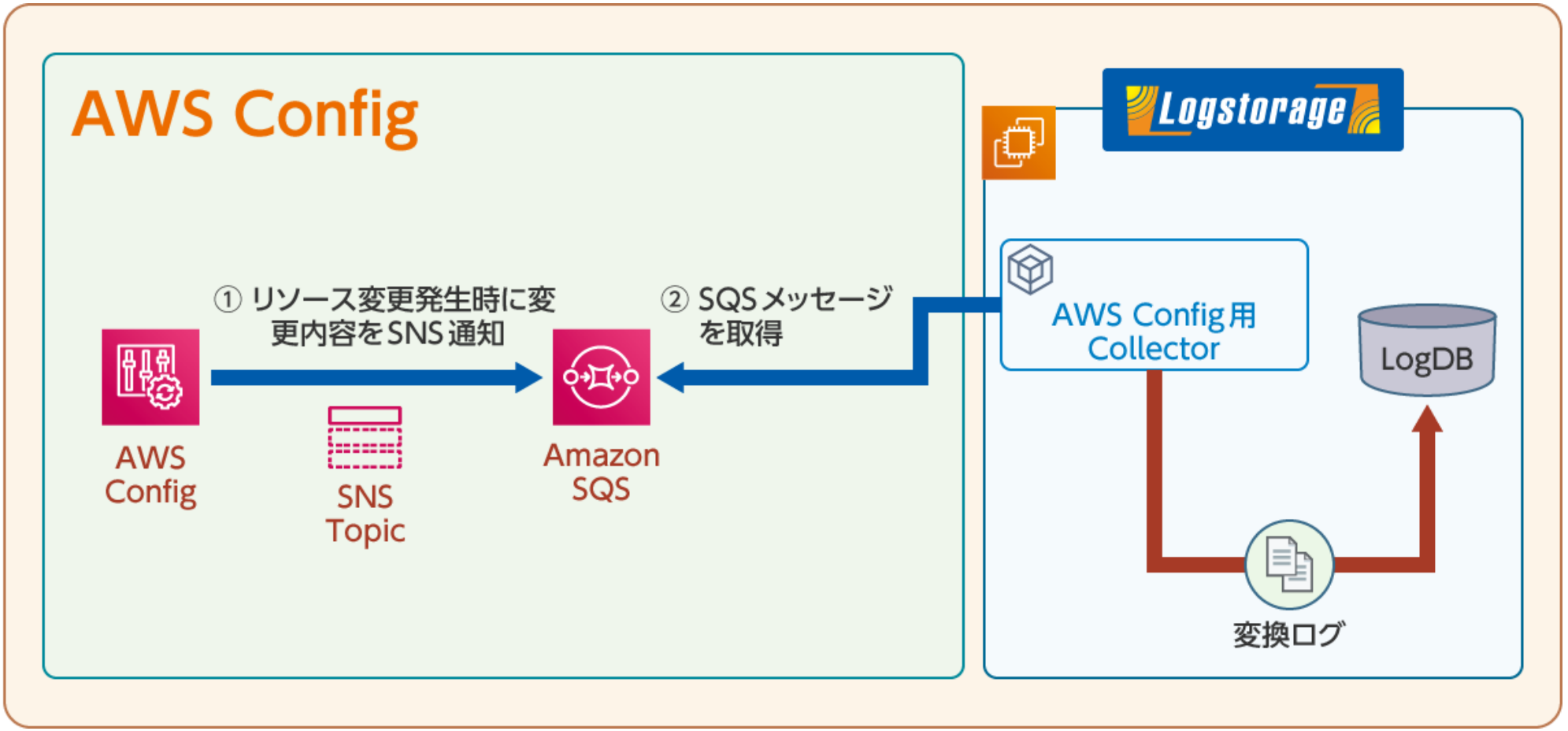
Configスナップショットレポート（構成図）



AWS Config スナップショットレポート では、レポート実行時点のVPC内のリソース構成を描画出力します。

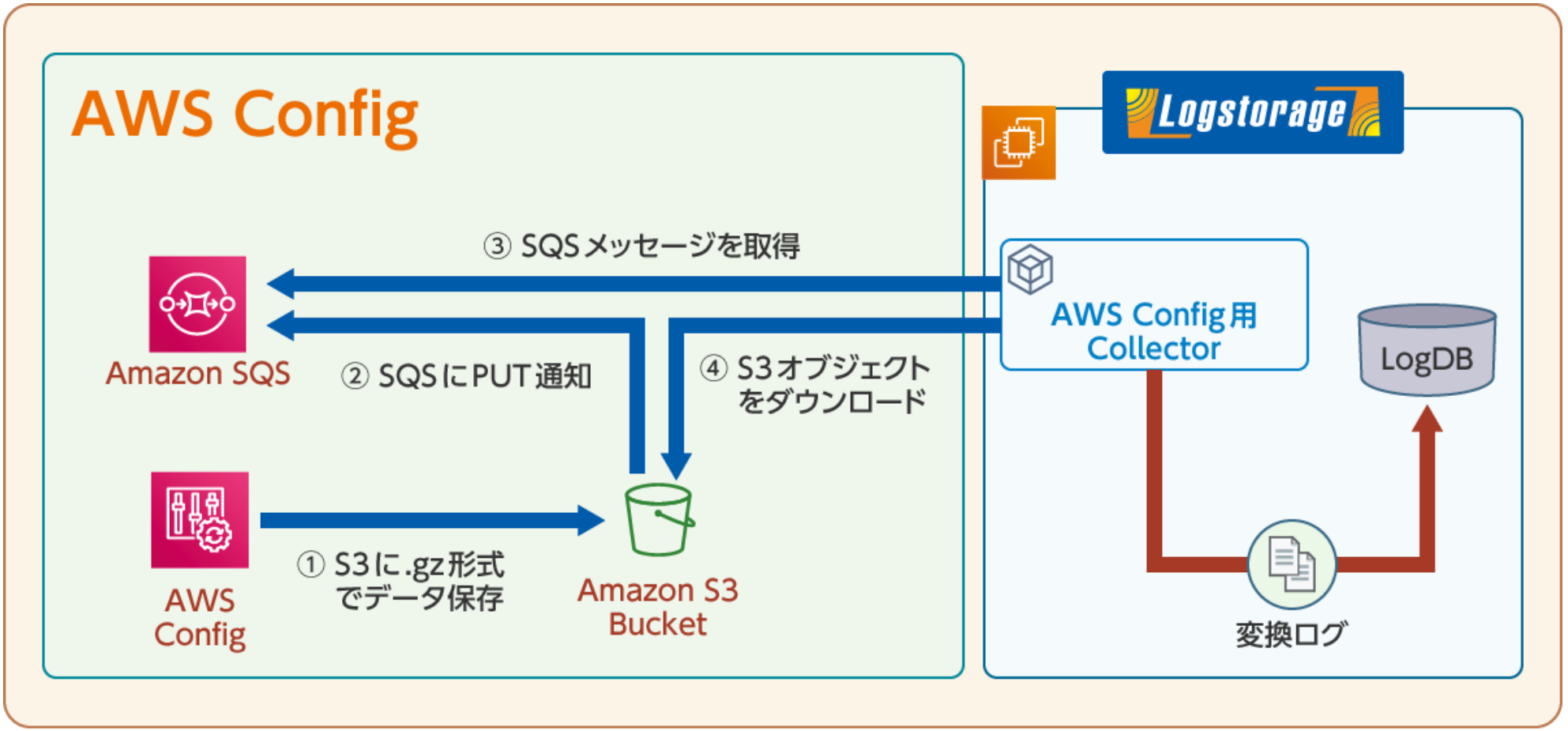
AWS Config ログ収集の仕組み（１）

AWS Config のイベント通知を利用

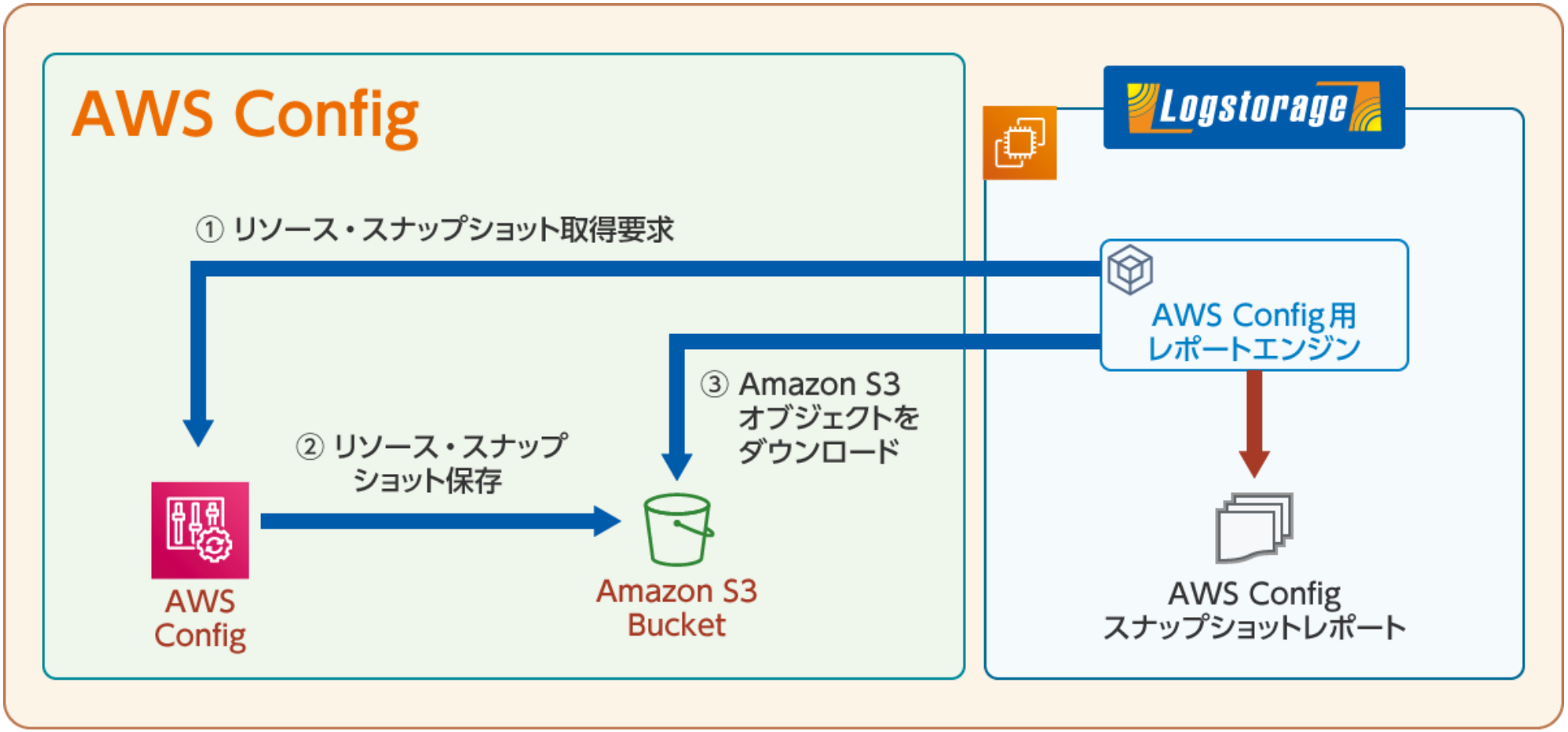


AWS Config ログ収集の仕組み（２）

Amazon S3 のイベント通知を利用



AWS Config レポート作成の仕組み

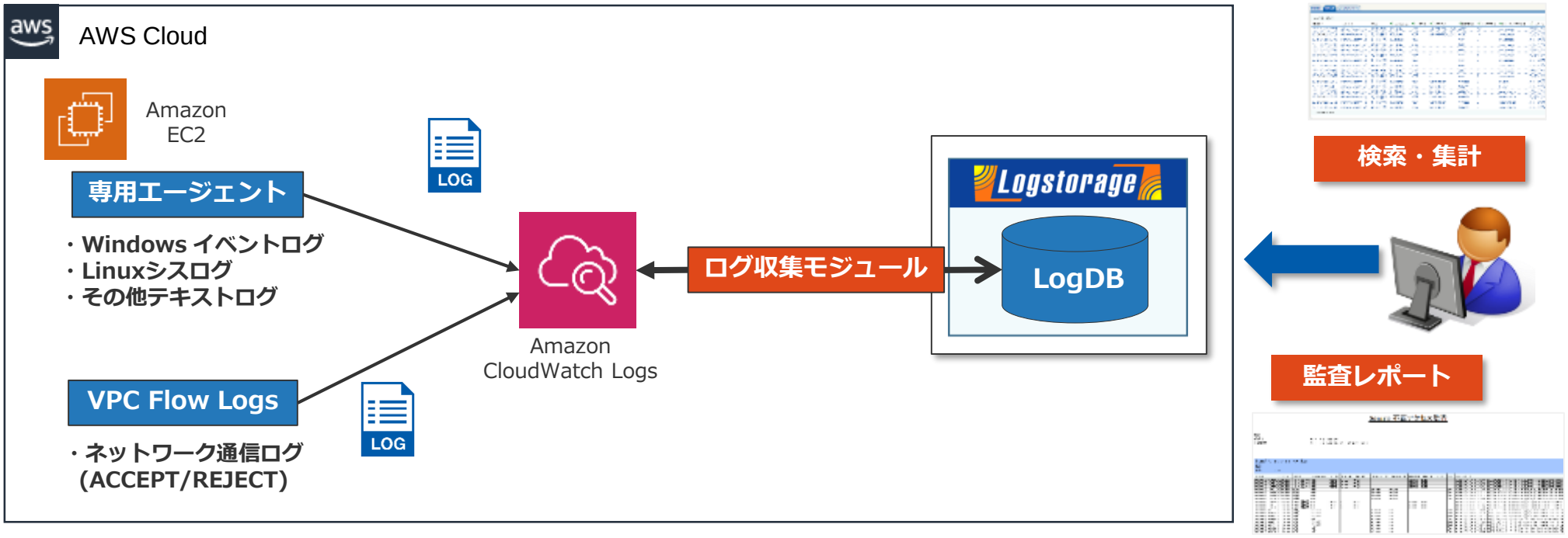


Amazon CloudWatch Logs 対応機能

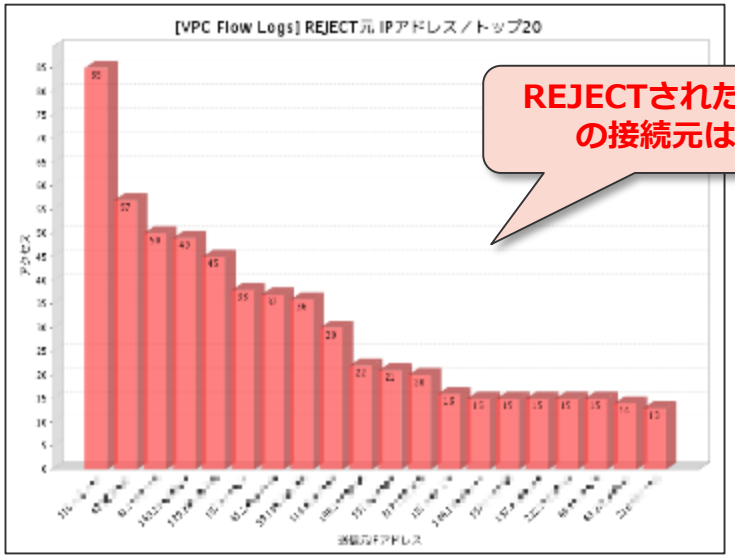
Amazon CloudWatch Logs とは

Amazon EC2インスタンス上のログやネットワーク上の通信ログなどを集約して可視化するサービスです。各EC2インスタンスに専用のエージェントをインストールすることで、Windowsイベントログ やLinux syslogなどの収集が可能です。また、VPC内のネットワークインターフェイス間で行き来するIPトラフィックの通信ログ(VPC Flow Logs)の収集が可能です。他にも、AWS上の様々なサービスに対応しています。

Amazon CloudWatch Logs 対応機能 構成

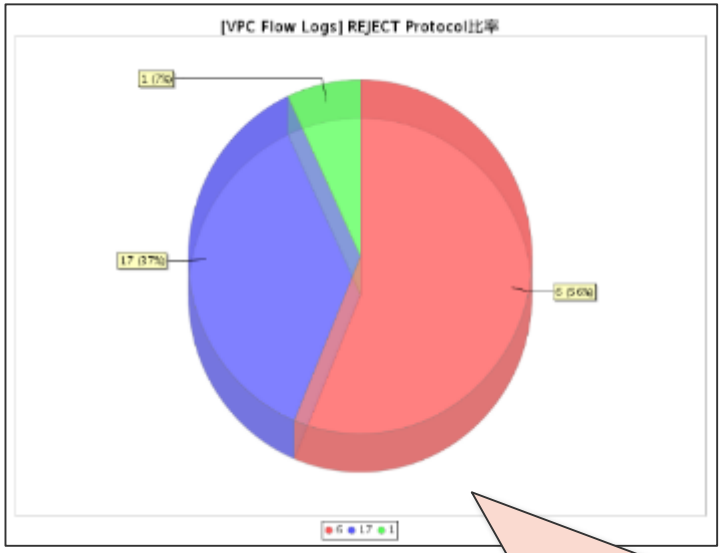


VPC Flow Logs レポート例／REJECT

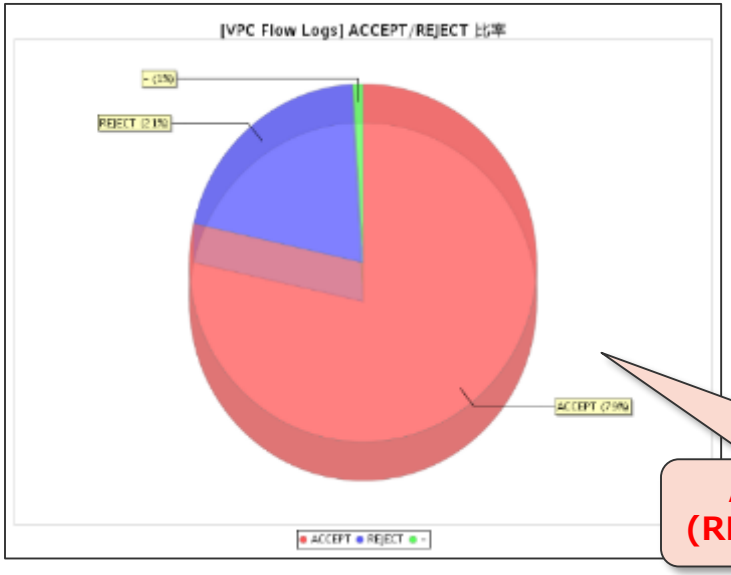


REJECTされた通信
の接続元は?

どのような通信先/ポートに
REJECTされた通信があったか



REJECTされた通信のプロトコルは?
(1-ICMP / 6-TCP / 17-UDP)

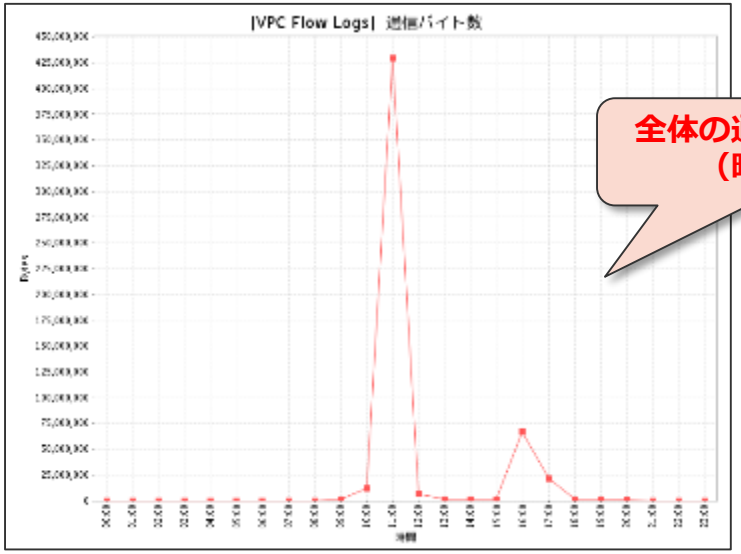


ACCEPT/REJECTの比率は?
(REJECT通信が異常に多く無いか)

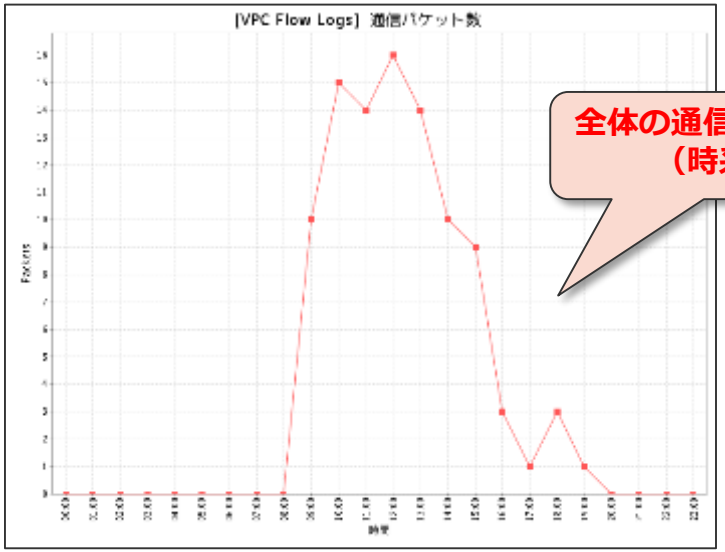
REJECTされた通信

通信元IPアドレス	通信先IPアドレス	通信先ポート	アクセス件数
116	10.	8080	8
		8118	7
		8888	9
	10.	8080	7
		8118	7
		8888	7
	10.	8118	8
		8888	8
	10.	8080	8
		8118	8
		8888	8
42.	10.	3306	15
	10.	3306	14
	10.	3306	14
	10.	3306	14
61.	10.	8080	2
		8118	3
		8888	4
	10.	8080	3
		8118	4
		8888	3
	10.	8080	4
		8118	3
		8888	3
	10.	8080	3
		8118	3
		8888	3
	10.	8118	2
		8888	4
	10.	8080	2
		8118	2
		8888	2
169	10.	514	49
129	10.	123	45
157	10.	123	38

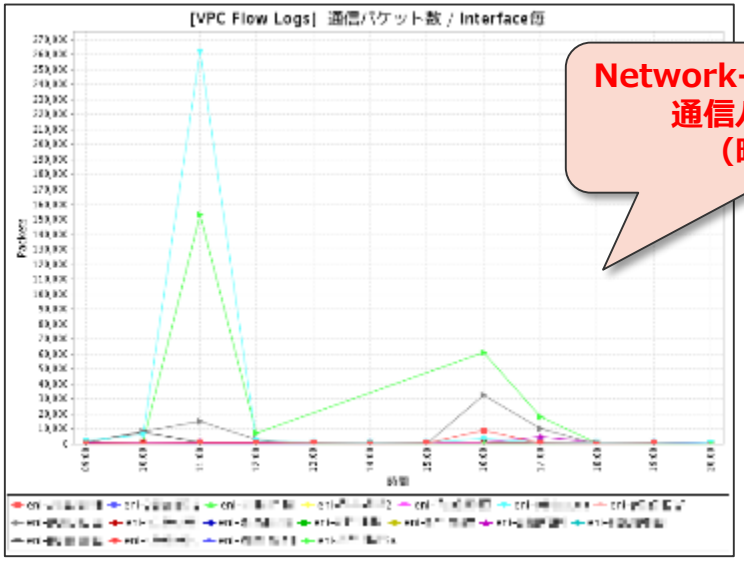
VPC Flow Logs レポート例／通信量



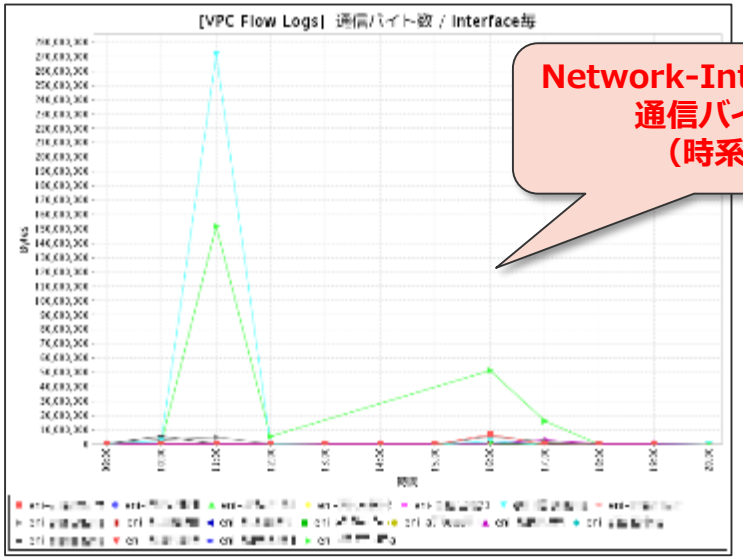
全体の通信バイト数
（時系列）



全体の通信パケット数
（時系列）

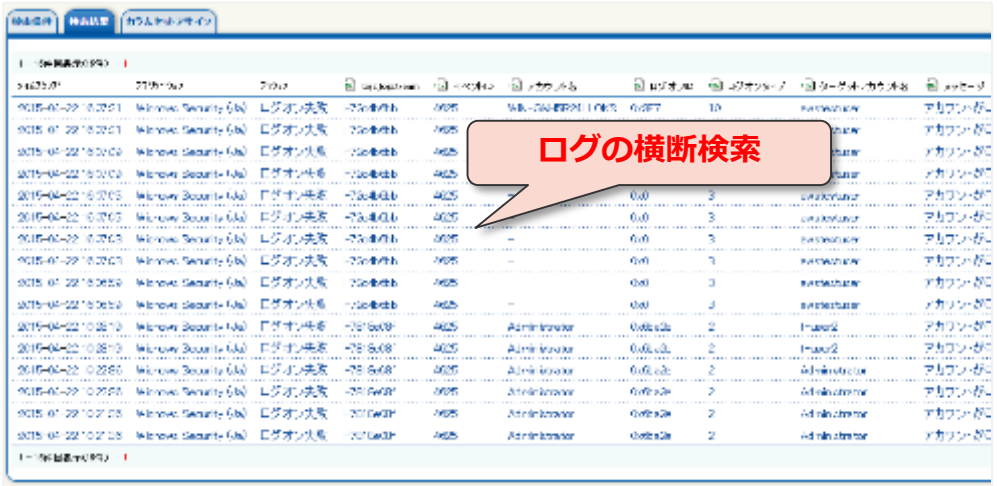


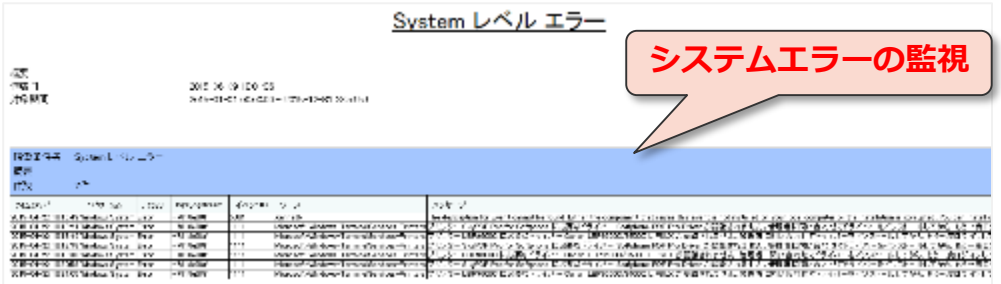
Network-Interface毎の
通信パケット数
（時系列）

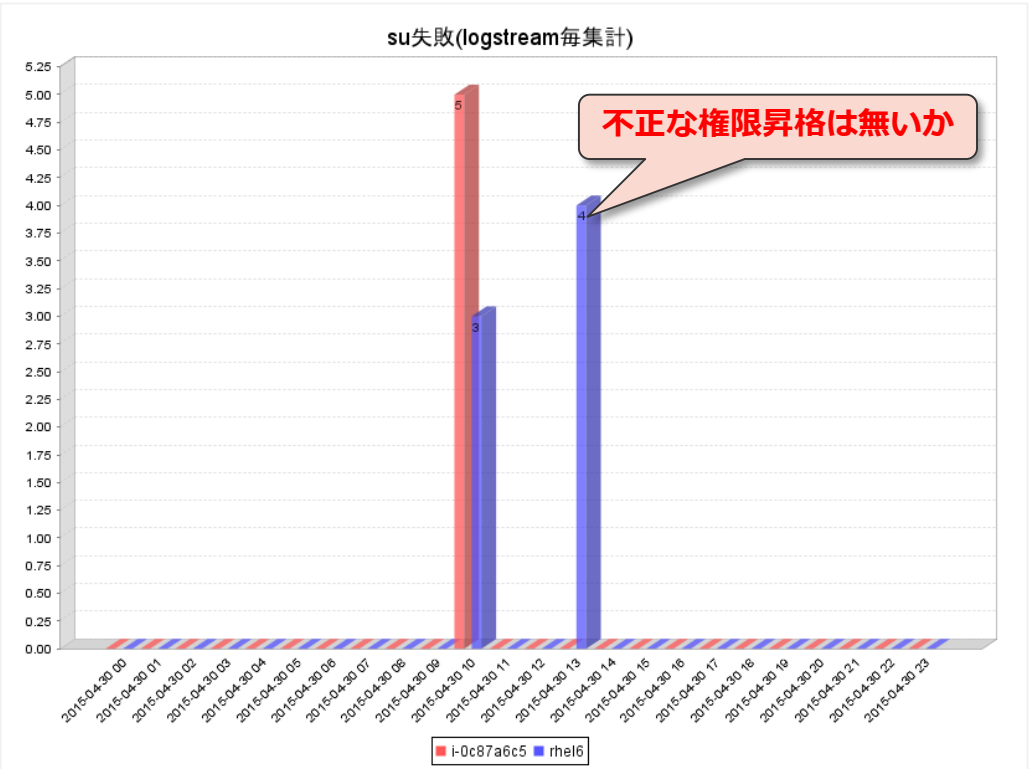


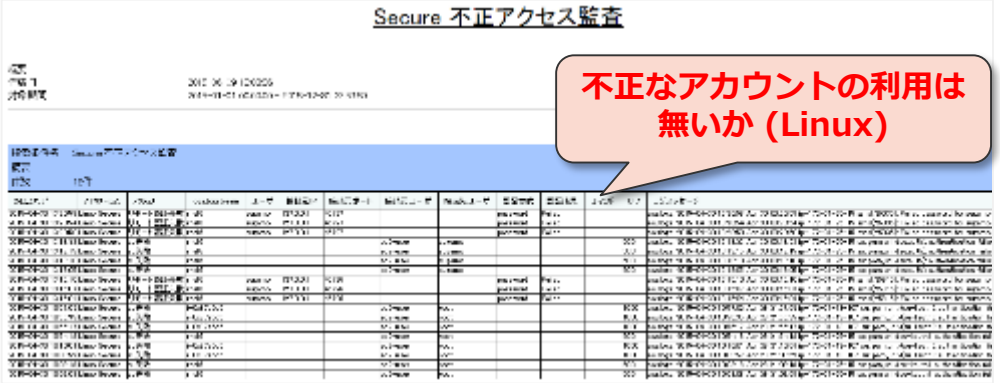
Network-Interface毎の
通信バイト数
（時系列）

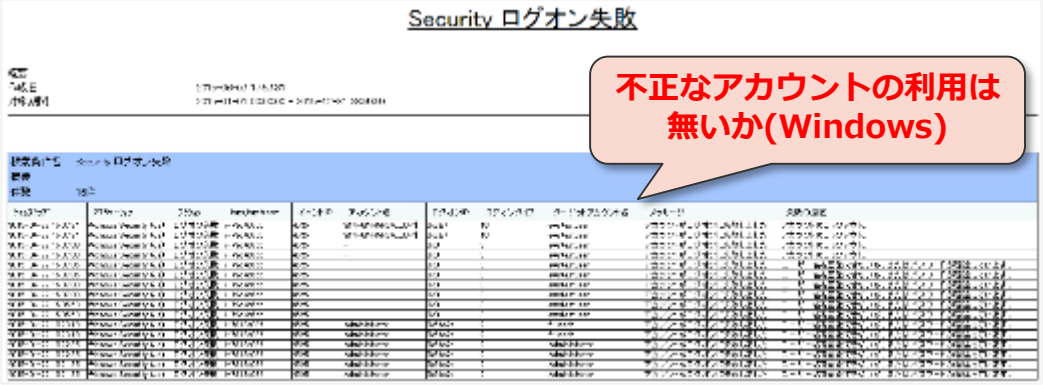
Amazon EC2 イベントログ / syslog レポート例











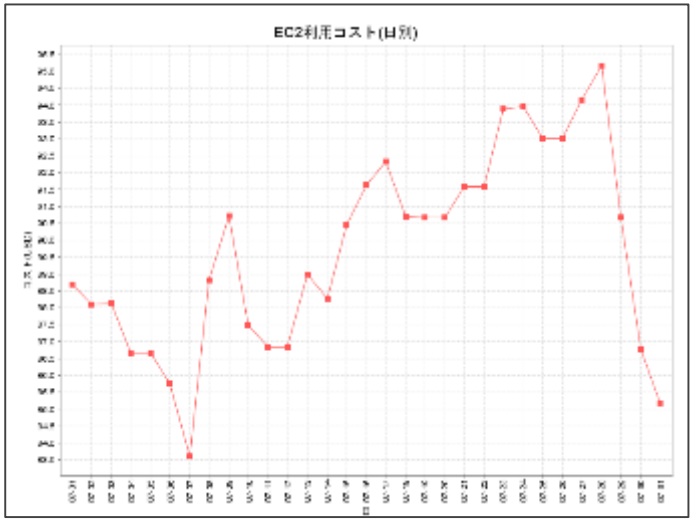
その他の機能

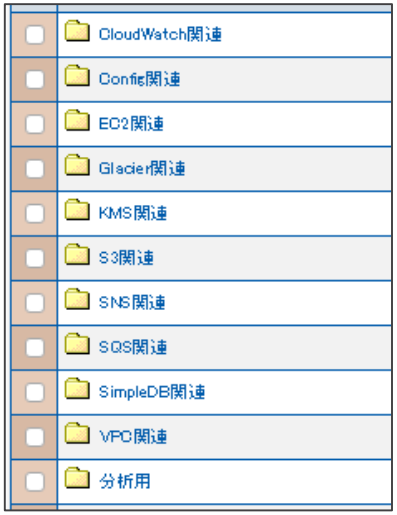
- AWS Billing
- Amazon S3
- ELB
- Amazon RDS
- Amazon CloudWatch Metrics
- Amazon CloudFront
- Amazon S3/Glacier へのログアーカイブ

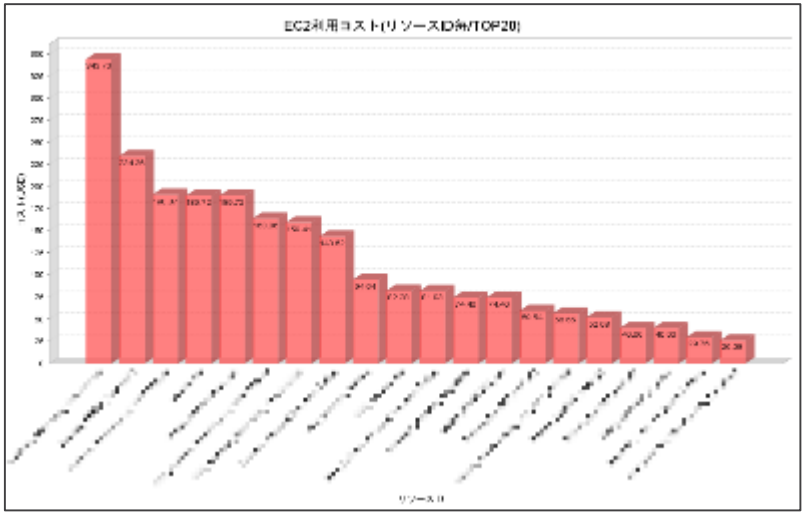
AWS Billing ～請求情報の可視化・分析～

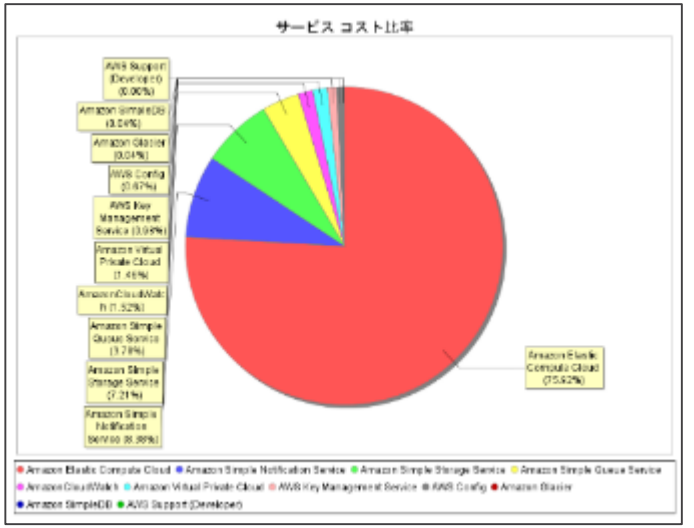
請求情報を可視化、長期的な分析が可能に

AWSのBillingデータを利用し、利用金額の観点から、AWSサービスの利用状況を把握します。
- 既に利用していないサービスで料金が発生していないか把握し不要なサービスを止める。
- EC2毎の利用コストを把握し、スポットインスタンス／リザーブドインスタンスの切替を検討する。
- 部署／ユーザ単位での利用金額を把握し、適切な費用配賦を行う。

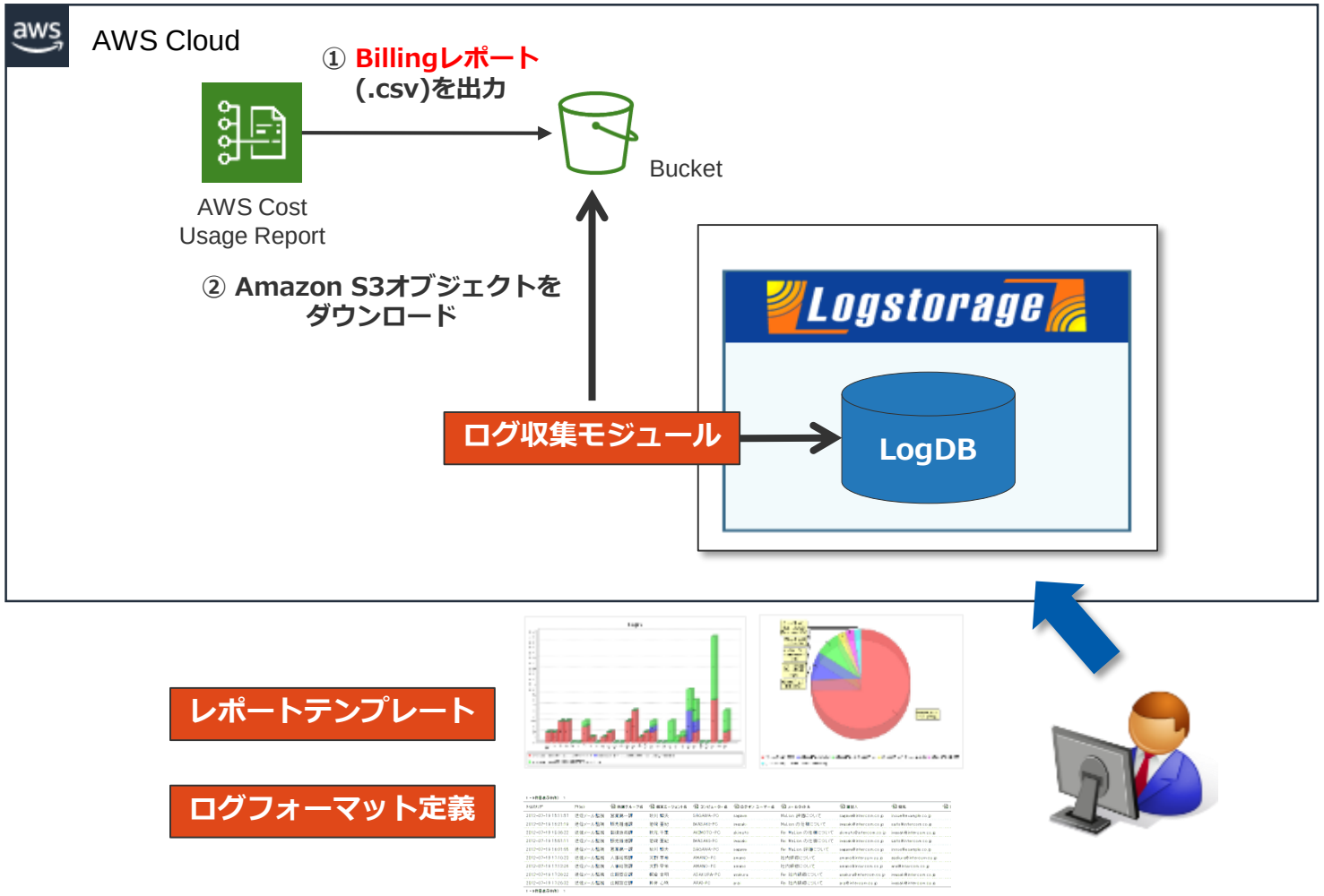




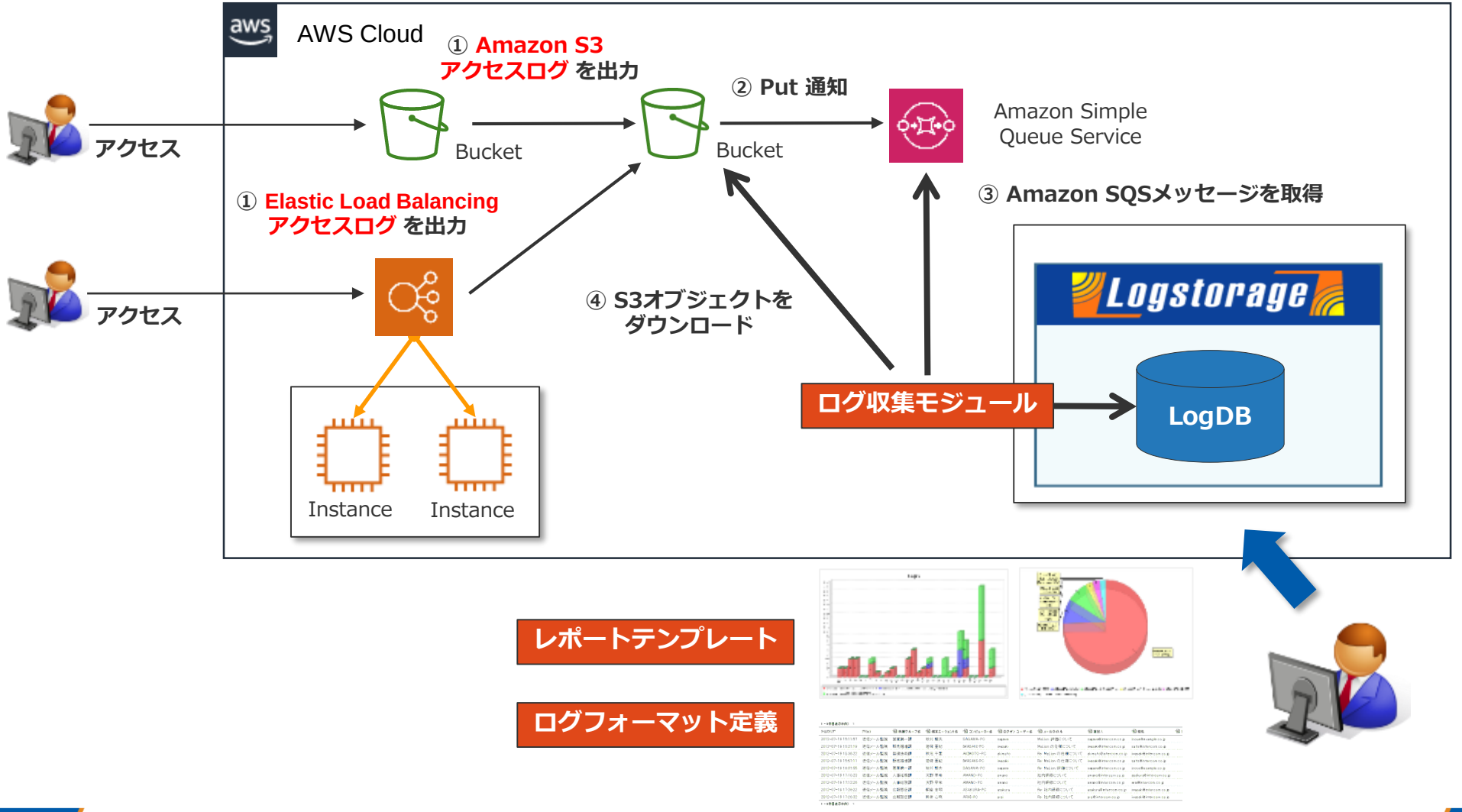




AWS Billing　連携機能 構成



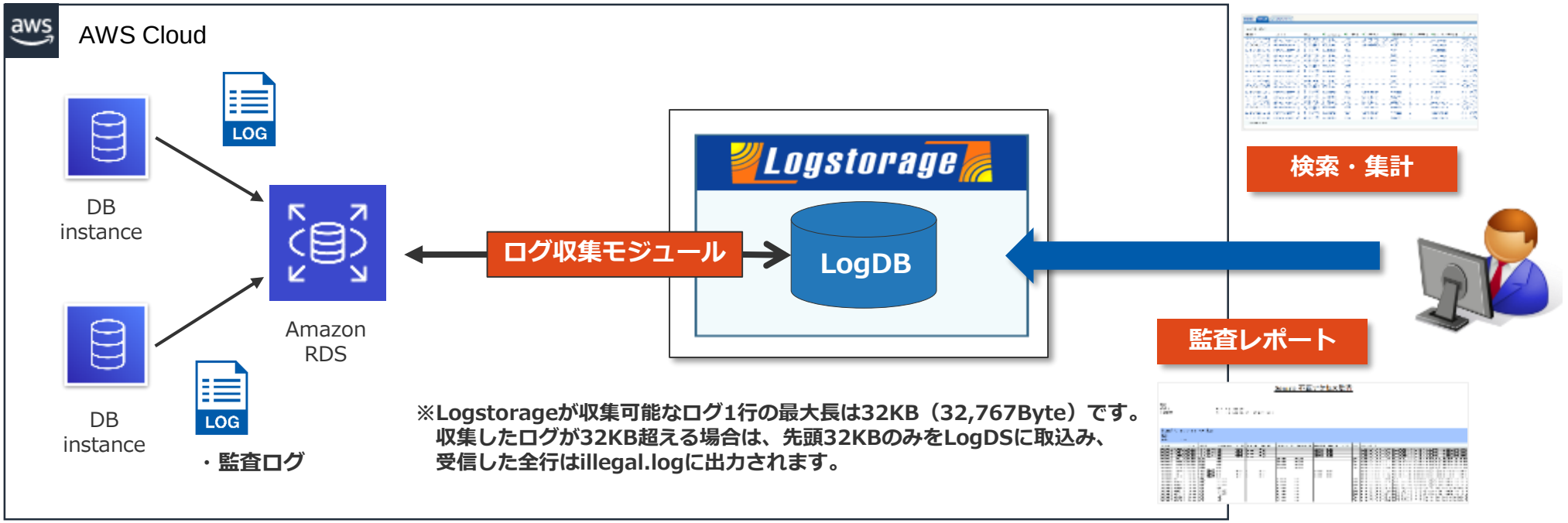
S3アクセスログ／ELB通信ログ 対応機能 構成



Amazon RDS とは

マネージド型リレーショナルデータベースサービスです。
Oracle 、Amazon Aurora、MySQL、MariaDB、Microsoft SQL Server、PostgreSQL といった一般的な 6 種類のデータベースエンジンから選択可能です。
柔軟にスケーラビリティができ、自動バックアップ 、スナップショットによるバックアップ、マルチAZ配置など、高い可用性と耐久性を容易に実現することが可能です。

Amazon RDS連携機能 構成



Amazon RDS(Oracle) 検索イメージ

データベースへのログイン、
テーブルへのSQLクエリ操作
などが把握可能

検索条件 | 検索結果 | カラムセットアサイン

1-100件目表示 (全 130件) 1 2 > >>

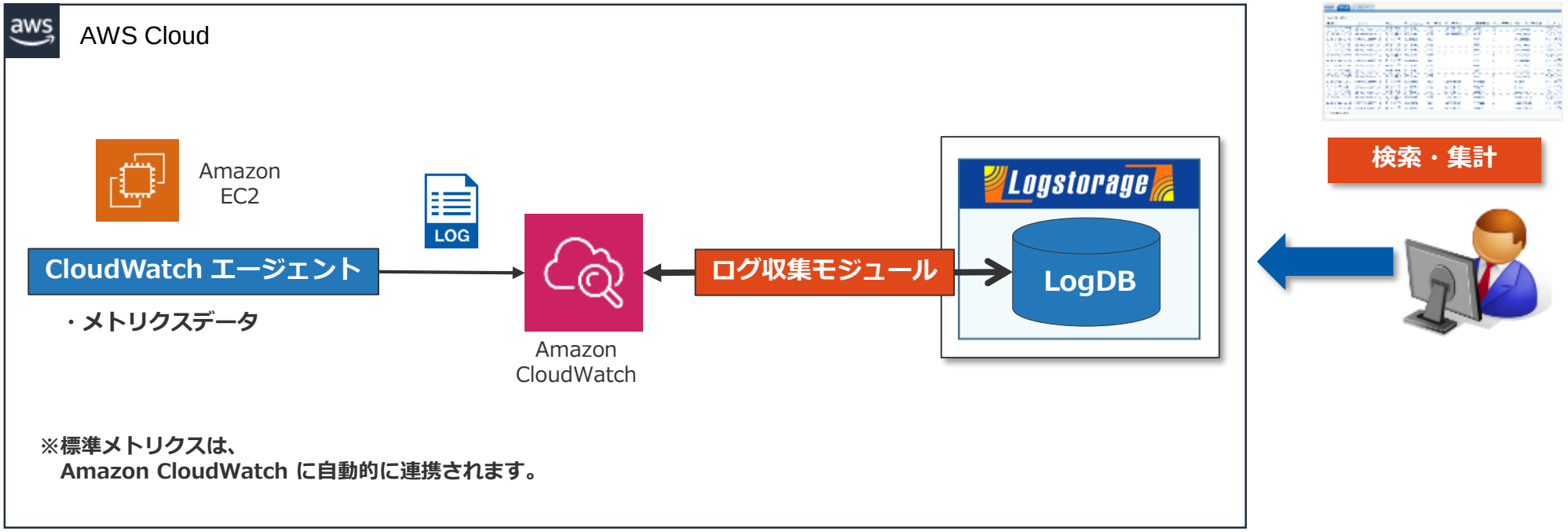
[表示数: 100件 ▼] 拡張トラッキング ログを改行しない

タイムスタンプ	ログソース	アプリケーション	Audit_Type_Name	Action_Name	DB_User	Sql_Text
2011-08-11 15:34:37	OraServ01	Oracle	標準監査	LOGON	SCOTT	
2011-08-11 15:42:06	OraServ01	Oracle	標準監査	LOGON	INAMURA	
2011-08-11 15:45:19	OraServ01	Oracle	標準監査	LOGON	INAMURA	
2011-08-11 15:45:37	OraServ01	Oracle	標準監査	LOGOFF	INAMURA	
2011-08-11 15:53:44	OraServ01	Oracle	標準監査	LOGON	INAMURA	
2011-08-11 15:56:27	OraServ01	Oracle	標準監査	LOGOFF	INAMURA	
2011-08-11 15:59:03	OraServ01	Oracle	標準監査	LOGON	INAMURA	
2011-08-11 15:59:03	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT USER FROM DUAL
2011-08-11 15:59:03	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,DATE_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER('SQL*Plus') LIKE UPPER(PR
2011-08-11 15:59:03	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,DATE_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER('SQL*Plus') LIKE UPPER(PR
2011-08-11 15:59:03	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER('SQL*Plus') LIKE UPPER(PRODUCT)) AND ((USER LIKE USERID) OR (USERID =
2011-08-11 15:59:03	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER('SQL*Plus') LIKE UPPER(PRODUCT)) AND ((USER LIKE USERID) OR (USERID =
2011-08-11 15:59:03	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT DECODE('A','A','1','2') FROM DUAL
2011-08-11 15:59:08	OraServ01	Oracle	標準監査	SELECT	INAMURA	select * from emp
2011-08-11 16:36:53	OraServ01	Oracle	標準監査	LOGOFF BY CLEANUP	INAMURA	
2011-08-12 11:45:56	OraServ01	Oracle	標準監査	LOGON	YAMADA	
2011-08-12 11:47:12	OraServ01	Oracle	標準監査	LOGON	YAMADA	
2011-08-12 11:47:40	OraServ01	Oracle	標準監査	LOGOFF	YAMADA	
2011-08-12 11:47:44	OraServ01	Oracle	標準監査	LOGON	INAMURA	
2011-08-12 11:47:44	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT USER FROM DUAL
2011-08-12 11:47:44	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,DATE_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER('SQL*Plus') LIKE UPPER(PR
2011-08-12 11:47:44	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,DATE_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER('SQL*Plus') LIKE UPPER(PR
2011-08-12 11:47:44	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER('SQL*Plus') LIKE UPPER(PRODUCT)) AND ((USER LIKE USERID) OR (USERID =
2011-08-12 11:47:44	OraServ01	Oracle	標準監査	SELECT	INAMURA	SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER('SQL*Plus') LIKE UPPER(PRODUCT)) AND ((USER LIKE USERID) OR (USERID =

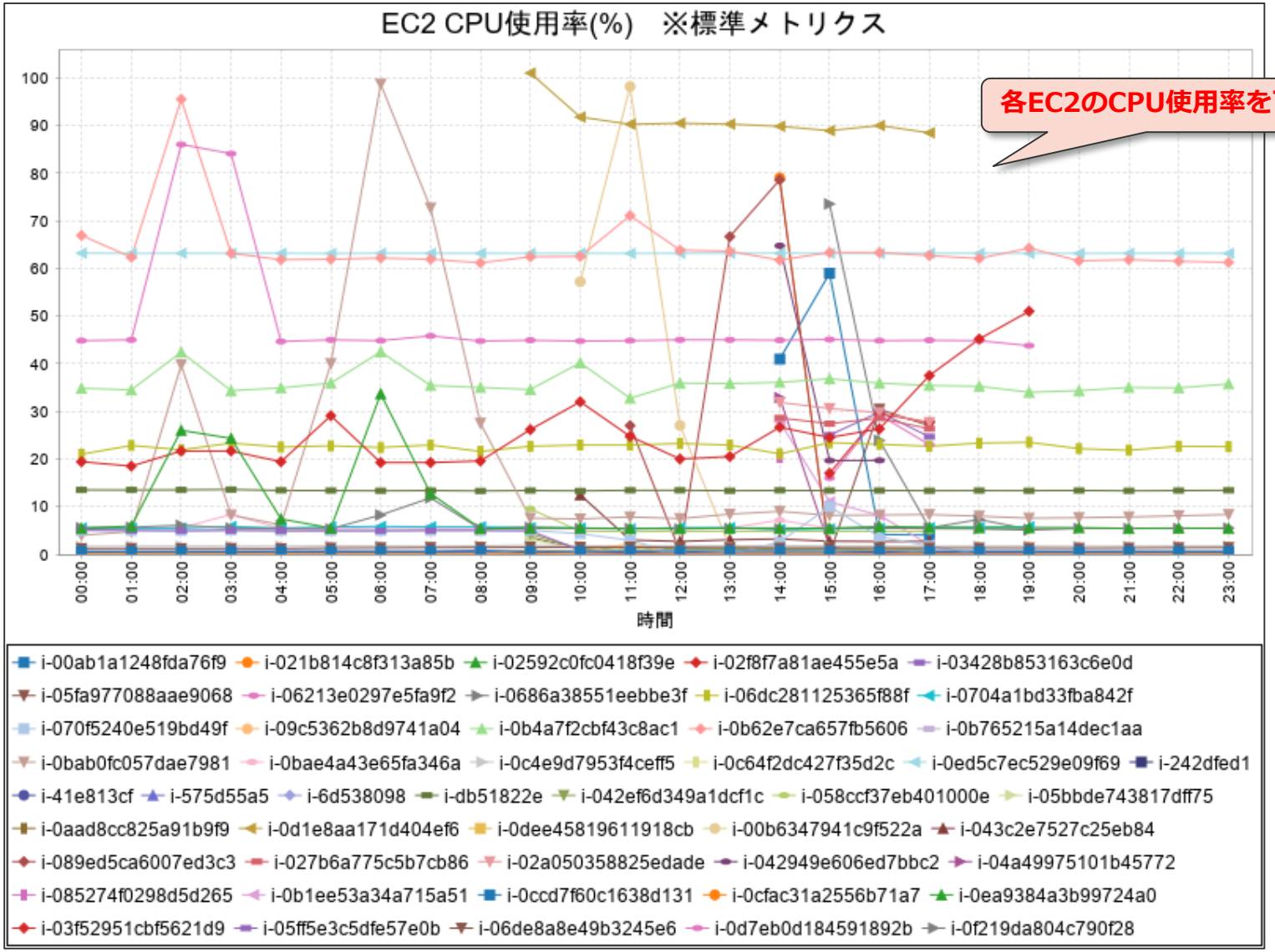
Amazon CloudWatch Metrics とは

Amazon CloudWatch サービス（AWSの各種リソースを監視するマネージドサービス）の一機能です。
AWS の各リソースとアプリケーションのモニタリングが可能。例えば、EC2のCPU、ディスクIOといった性能情報を参照することができます。オンプレミスのサーバのメトリクスも取得可能です。
（CloudWatchエージェントのインストールが必要です。）

Amazon CloudWatch Metrics 対応機能 構成



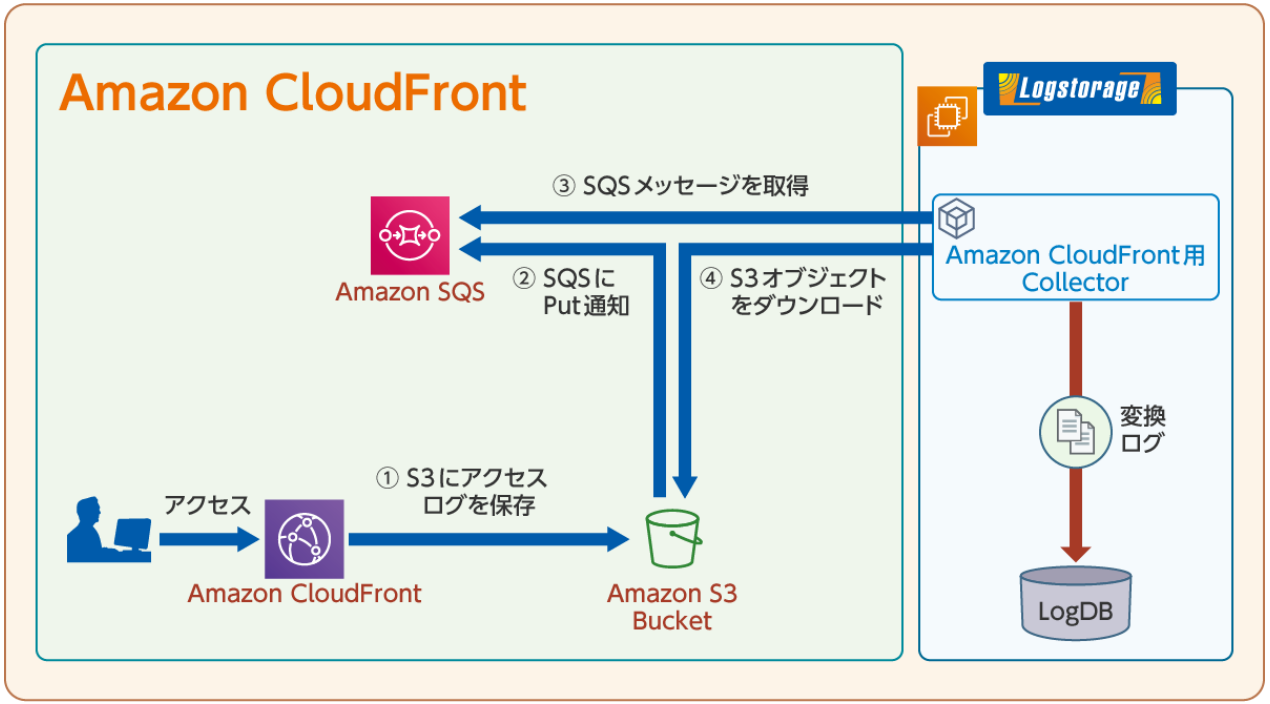
Amazon CloudWatch Metrics 集計イメージ



Amazon CloudFront とは

CDN（コンテンツデリバリネットワーク）サービスです。
サーバからコンテンツを直接配信せず、CloudFrontを介して、静的ファイルおよび動的コンテンツを配信するため、負荷分散やネットワークレイテンシの低減に役立ちます。コンテンツを配信するオリジンサーバは、Amazon EC2やS3などの他にオンプレミスサーバも指定することが可能です。

Amazon CloudFront 対応機能 構成



Amazon CloudFront 検索イメージ

検索条件名: Webディストリビューション アクセスログ

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　1-42件目表示 (全42件)　1　[表示数:100件 ▼] 拡張トラッキング ログを

Webディストリビューション のアクセスログ

タイムスタンプ	リクエスト元のIP アドレス	エッジロケーション	リファラー	URI	URIクエリ	HTTPメソッド	HTTPステータスコード	ユーザエージェント
2019-01-23 14:09:11	10.0.0.1	SEA19-C2	-	/index.html	-	GET	504	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
2019-01-23 14:09:41	10.0.0.1	SEA19-C2	http://dn9v2wkjjbhi9.cloudfront.net/index.html	/favicon.ico	-	GET	504	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
2019-01-23 14:09:46	10.0.0.1	SEA19-C2	-	/iOS+proxy.mp4	-	GET	304	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
2019-01-23 14:09:46	10.0.0.1	SEA19-C2	http://dn9v2wkjjbhi9.cloudfront.net/iOS+proxy.mp4	/iOS+proxy.mp4	-	GET	206	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
2019-01-23 14:39:13	10.0.0.1	SEA19-C2	-	/iOS+proxy.mp4	-	GET	304	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
2019-01-31 09:52:47	10.0.0.1	HIO50-C1	-	/	-	GET	504	PostmanRuntime/7.19.0
2019-01-31 09:54:14	10.0.0.1	HIO50-C1	-	/index.html	-	GET	504	PostmanRuntime/7.19.0
2019-01-31 09:54:45	10.0.0.1	HIO50-C1	-	/index.html	-	POST	403	PostmanRuntime/7.19.0
2019-01-31 09:54:59	10.0.0.1	HIO50-C1	-	/video.mp4	-	POST	403	PostmanRuntime/7.19.0
2019-01-31 09:55:03	10.0.0.1	HIO50-C1	-	/video.mp4	-	PUT	403	PostmanRuntime/7.19.0

検索条件名: RTMPディストリビューション アクセスログ

概要:

検索条件 | 検索結果 | カラムセットアサイン

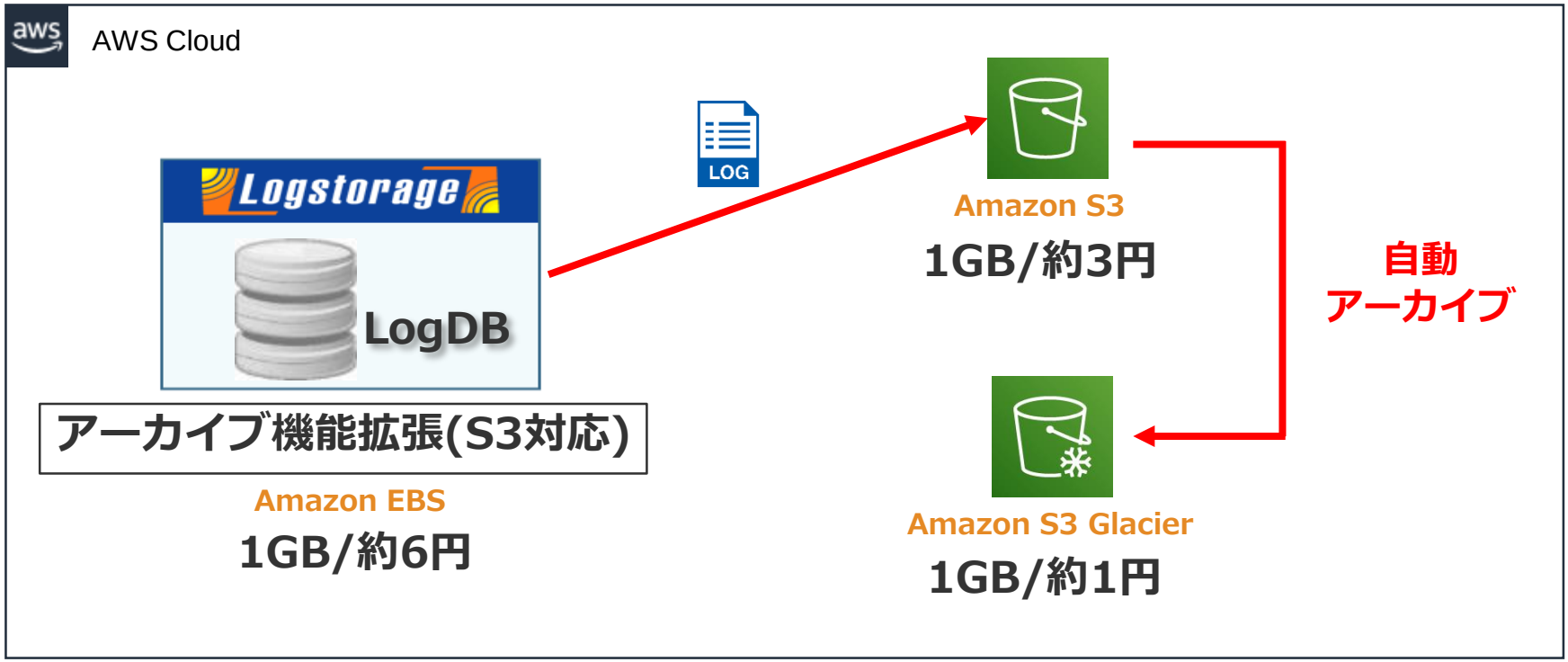
ログ | カラム　1-100件目表示 (全115件)　1 2 ≥ ≫　[表示数:100件 ▼] 拡張トラッキング ログを折り

RTMPディストリビューション のアクセスログ

タイムスタンプ	リクエスト元のIP アドレス	エッジロケーション	リファラー	URI	ストリーム名	イベントタイプ	イベント
2019-01-23 14:55:46	10.0.0.1	PHL50	https://vjs.zencdn.net/swf/5.4.2/video-js.swf	rtmp://s1qj4pyk840fb8.cloudfront.net/	-	connect	OK
2019-01-23 15:10:59	10.0.0.1	PHL50	http://d1k5ny0m6d4zlj.cloudfront.net/diag/CFStreamingDiag.swf	rtmp://s1qj4pyk840fb8.cloudfront.net:1935/cfx/st	-	connect	OK
2019-01-23 15:11:00	10.0.0.1	PHL50	http://d1k5ny0m6d4zlj.cloudfront.net/diag/CFStreamingDiag.swf	rtmp://s1qj4pyk840fb8.cloudfront.net:1935/cfx/st	video.mp4	play	OK
2019-01-23 15:12:05	10.0.0.1	PHL50	-	rtmp://s1qj4pyk840fb8.cloudfront.net:1935/cfx/st	-	connect	OK
2019-01-23 15:12:06	10.0.0.1	PHL50	-	rtmp://s1qj4pyk840fb8.cloudfront.net:1935/cfx/st	video.mp4	play	OK
2019-01-23 15:12:20	10.0.0.1	PHL50	-	rtmp://s1qj4pyk840fb8.cloudfront.net:1935/cfx/st	video.mp4	stop	OK
2019-01-23 15:12:20	10.0.0.1	PHL50	-	rtmp://s1qj4pyk840fb8.cloudfront.net:1935/cfx/st	-	disconnect	OK
2019-01-23 15:12:52	10.0.0.1	PHL50	http://d1k5ny0m6d4zlj.cloudfront.net/diag/CFStreamingDiag.swf	rtmp://s1qj4pyk840fb8.cloudfront.net:1935/cfx/st	video.mp4	stop	OK
2019-01-23 15:13:32	10.0.0.1	PHL50	https://vjs.zencdn.net/swf/5.4.2/video-js.swf	rtmp://s1qj4pyk840fb8.cloudfront.net:1935/cfx/st/	-	connect	OK
2019-01-23 15:13:32	10.0.0.1	PHL50	https://vjs.zencdn.net/swf/5.4.2/video-js.swf	rtmp://s1qj4pyk840fb8.cloudfront.net:1935/cfx/st/	video.mp4	play	OK

Amazon S3 / Amazon S3 Glacier へのログバックアップ

過去ログをS3/Gracierにバックアップ



運用例

・LogDB上に1年間保存
　⇒ 1年以上3年未満のログはS3上に保存
　　⇒　 3年以上前のログはGlacier上に保存

ログ保管ストレージの
コストを大幅にカット

Logstorage / AWS連携 導入事例

[事例1] cloudpack(アイレット株式会社)様

[事例2] ハンズラボ株式会社様

[事例3] GMOフィナンシャルホールディングス株式会社様

[事例4] データセンター事業者様

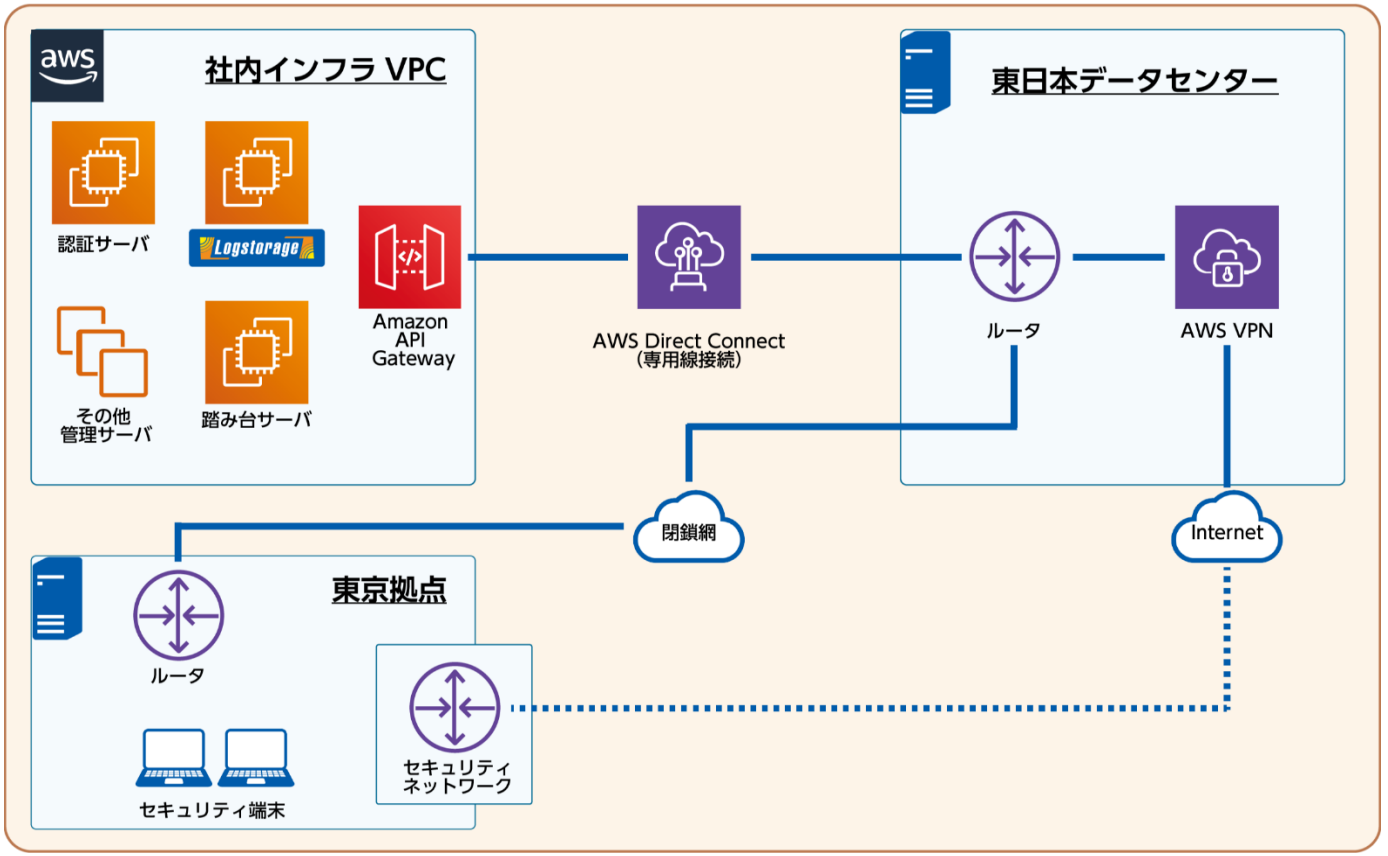
[事例1] cloudpack(アイレット株式会社)様

Logstorage導入目的

・各種セキュリティ認証の取得
(PCI DSS / ISO27001)
・SOC2 への取り組み
・上記への対応を通じ、セキュリティへの取り組みについて客観的な評価に基づく透明性の確保、高度なセキュリティ体制の実現

ログ収集対象

ログ収集対象
ルータ
スイッチ
認証サーバ
踏み台サーバ
NATインスタンス
セキュリティ端末
その他、セキュリティ管理サーバ
全顧客の AWS CloudTrail ログ
全顧客の AWS Config ログ



Logstorage導入環境

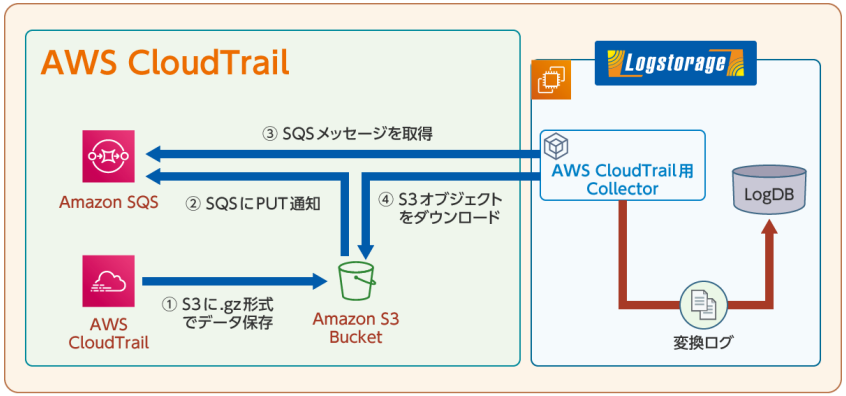
[事例1] cloudpack様のコメント

○PCI DSS認証

『無償で提供されるLogstorageのPCI DSSテンプレートには、テンプレートが対応するPCI DSS要件番号が記載されており、監査がスムーズに進んだ。』
『Logstorageは、PCI DSSで求められるログの暗号化と改ざん検出に標準機能で対応しており、別の製品と組み合わせる必要なく対応できた。』
『結果、PCI DSS認証取得において、ログに関する指摘事項はなかった。』

[Windows] 監査ポリシーの変更の一覧	PCI 10.2.2
ログイン失敗一覧	PCI 10.2.4
ログイン成功一覧	PCI 10.2.4
[Linux] パスワードの変更履歴一覧	-
[Linux] 特権権限への昇格の一覧 / sudo	PCI 10.2.4
[Linux] 特権権限への昇格失敗の一覧 / su	PCI 10.2.4
[Linux] 特権権限への昇格成功の一覧 / su	PCI 10.2.4
[Linux] 管理者権限のログイン履歴	PCI 10.2.2

【PCI DSSレポートテンプレート（一部）】



【S3 Put Eventを利用したCloudTrailログの収集】

○SOC 2報告書

『Logstorageを利用したログの一元管理はSOC2対応でも踏襲した。AWSを対象としたフルマネージドサービス事業で、国内で初めてSOC 2報告書を受領した。』

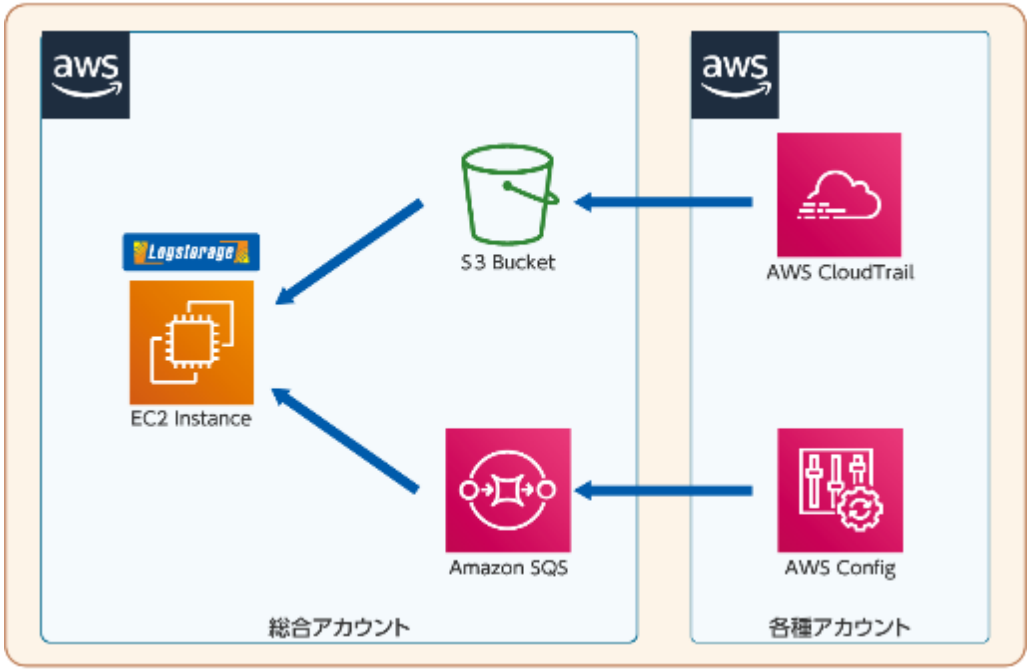
○その他

『LogstorageはAMIでも提供されるため、インストールには殆ど手間が掛からなかった。』
『多くのお客様のCloudTrailのログを効率的に収集するために必要としていた S3 Put Event に対応してもらえたのは助かった。』

[事例2] ハンズラボ株式会社様

Logstorage導入目的

・内部統制、PCI DSS対応が主な目的で、AWS上のログデータを素早く検索できるようにするため
・エンジニア全員がAWSを使用しており、だれが／いつ／どこで／何をしたのか 監視する必要がある
・全てのログを一箇所で統合管理するため



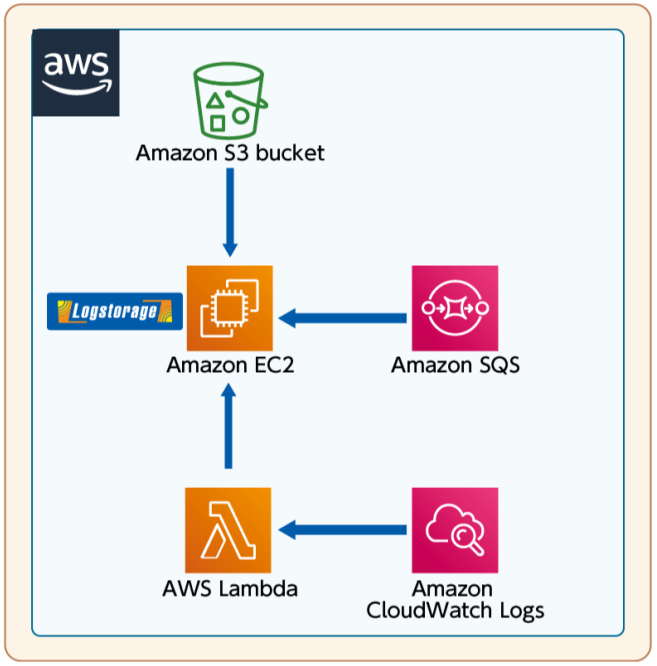
Logstorage導入環境

HANDS LAB × Logstorage

詳細は以下URLをご確認ください。
↓↓↓
https://logstorage.com/case/case_handslab.html

Logstorage導入目的

・AWS上にある環境の【見える化】のため
・構成図の作成から担当者へメール送信の運用フェーズを自動化できる機能を兼ね備えていた為、導入を決定
・AWS LambdaとAmazon CloudWatchを使用し、インスタンスの起動・停止の自動化を実現



Logstorage導入環境

GMOフィナンシャルHD

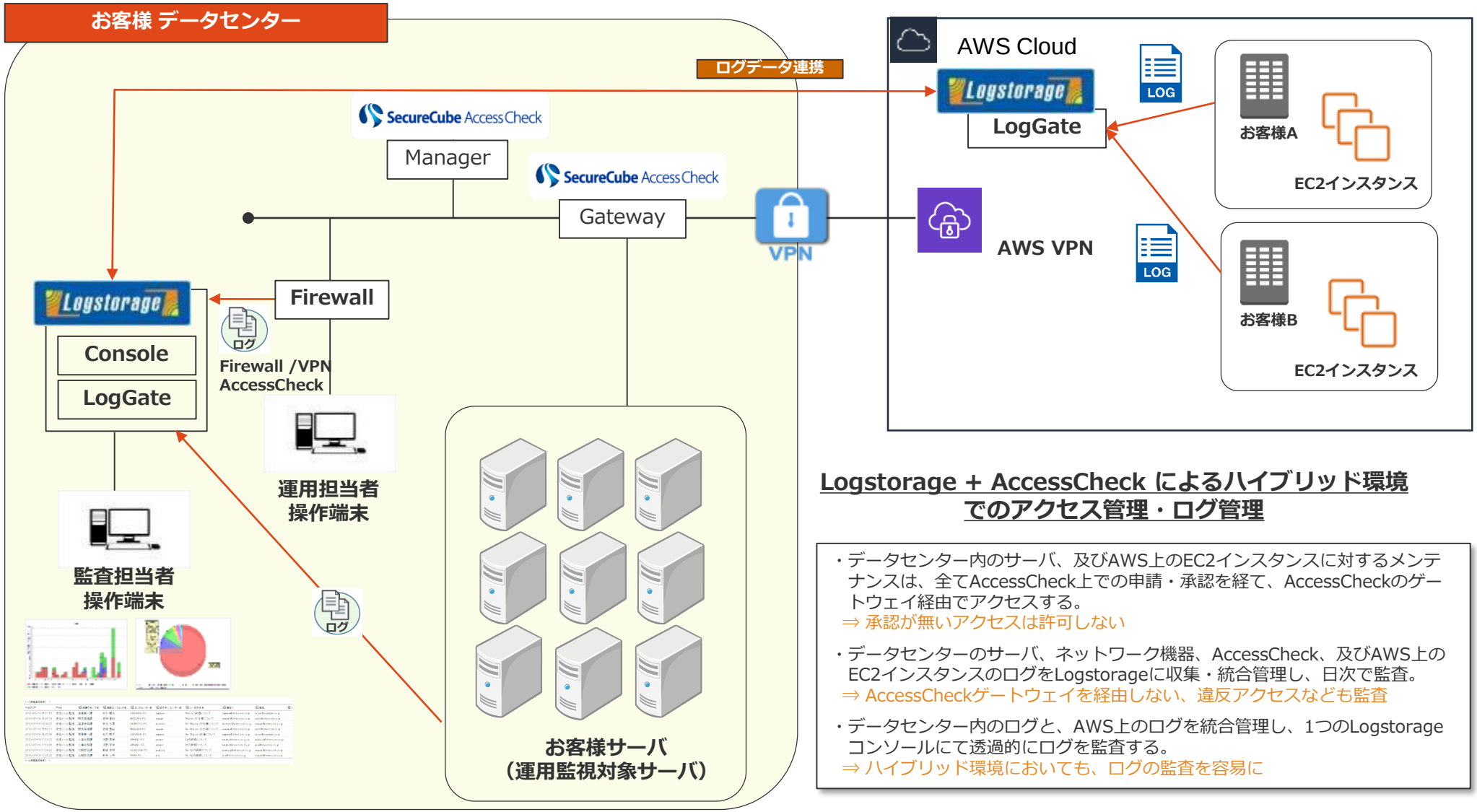
✖

Logstorage

詳細は以下URLをご確認ください。
↓↓↓
https://logstorage.com/case/case_gmofh.html

[事例4] データセンター事業者様

お客様(DC事業者様)が提供する「包括的システム運用サービス」。 SecureCube AccessCheck + Logstorageを導入する事で、DC事業者様が自社データセンター内で預かるお客様サーバ、及びAWS上のEC2インスタンス等の運用をより安全に、セキュアに行うことで、各種コンプライアンス要求に対応



Logstorage + AccessCheck によるハイブリッド環境でのアクセス管理・ログ管理

・データセンター内のサーバ、及びAWS上のEC2インスタンスに対するメンテナンスは、全てAccessCheck上での申請・承認を経て、AccessCheckのゲートウェイ経由でアクセスする。
⇒ 承認が無いアクセスは許可しない

・データセンターのサーバ、ネットワーク機器、AccessCheck、及びAWS上のEC2インスタンスのログをLogstorageに収集・統合管理し、日次で監査。
⇒ AccessCheckゲートウェイを経由しない、違反アクセスなども監査

・データセンター内のログと、AWS上のログを統合管理し、1つのLogstorageコンソールにて透過的にログを監査する。
⇒ ハイブリッド環境においても、ログの監査を容易に

ライセンス

ライセンス

ライセンス内容	
製品名称	**Logstorage対応パック for AWS**
対応サービス	**AWS CloudTrail, AWS Config, Amazon CloudWatch Logs, Amazon CloudWatch Metrics, AWS Billing, Amazon S3**(アクセスログ), **Amazon ELB, Amazon RDS, Amazon CloudFront**
含まれる機能	**AWS ログ収集モジュール** AWS 各サービスのログ・データを収集するためのモジュール。
	AWS ログフォーマット定義・タグ定義 AWS 各サービスのログフォーマット定義とタグ定義。
	AWS 検索／集計／レポートテンプレート AWS 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
出荷開始日	2015年6月1日

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