

JAPAN | JUNE 20, 2024

aws SUMMIT



BOOTH

AWS AppFabric のご紹介

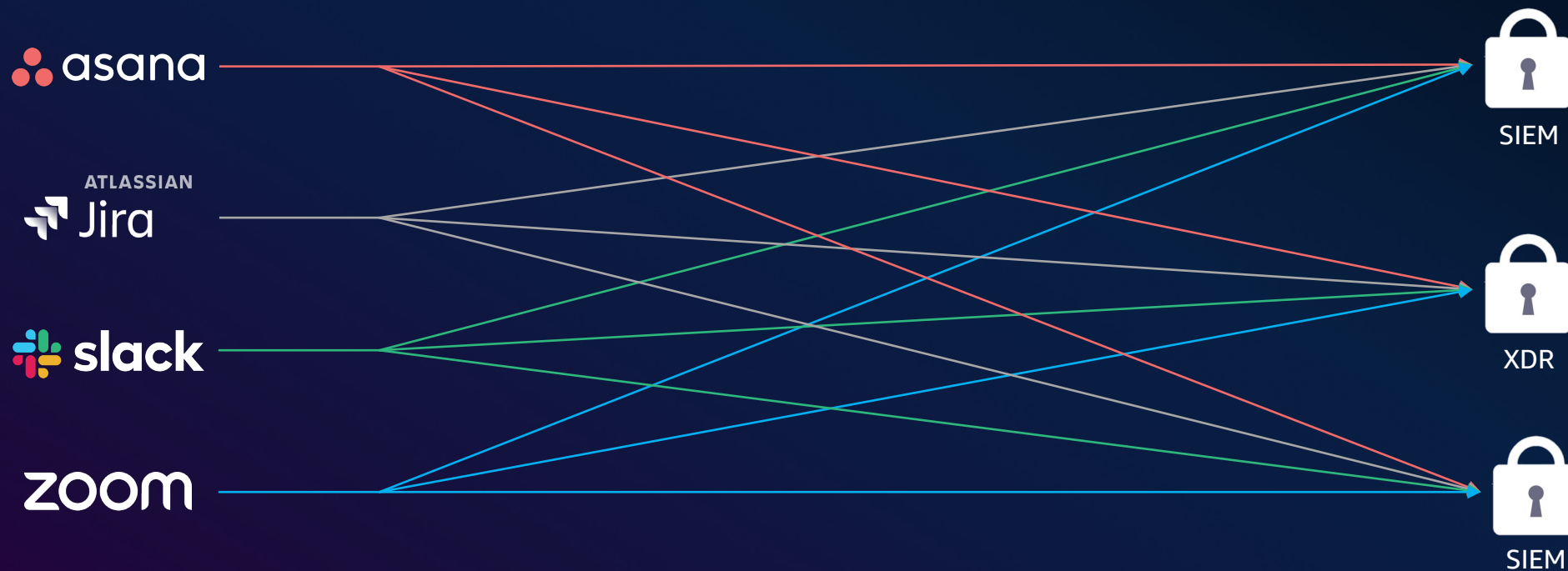


SaaS アプリケーションの採用が急増



SaaS を採用する組織が直面する課題

- セキュリティ可観測性（オブザーバビリティ）
- データの孤立（データ サイロ）
- P2P（ポイントツーポイント）の統合管理



AppFabric で正規化されたデータの単一のソースを提供

コーディングは不要



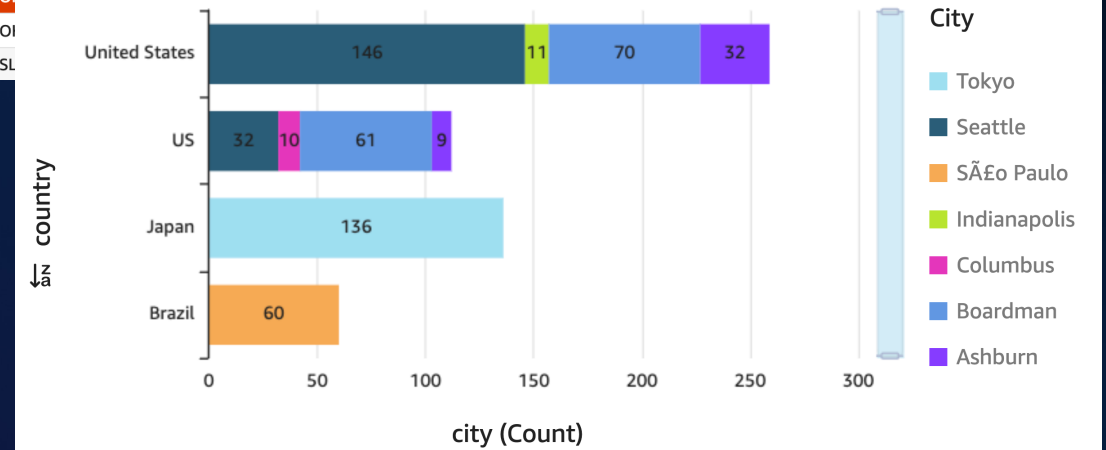
インサイトの種類

- セキュリティ
 - 異常なログイン場所
 - 権限の変更
 - 多数のログイン失敗
- Ad hoc 検索
 - インシデント調査と対応
 - ユーザーの活動追跡
- SaaSの利用頻度
 - トップアプリ、ユーザー、場所
 - ライセンスの最適化、アラート

Events Based On Timeline

timestamp	partition_4	category_name	type_name	status	message
Apr 30, 2024 5:01pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	User login to Okta
Apr 30, 2024 5:00pm	DROPBOX	Application	Web Resources Activity: Read	Success	Previewed files and/or folders
Apr 30, 2024 5:00pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	Authentication of user via MFA
Apr 30, 2024 4:59pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	User login to Okta
Apr 30, 2024 4:58pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	Authentication of user via MFA
Apr 30, 2024 4:57pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	User login to Okta
Apr 30, 2024 4:56pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	Authentication of user via MFA
Apr 30, 2024 4:55pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	User login to Okta
Apr 30, 2024 4:54pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	Authentication of user via MFA
Apr 30, 2024 4:53pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	User login to Okta
Apr 30, 2024 4:52pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	Authentication of user via MFA
Apr 30, 2024 4:51pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	User login to Okta
Apr 30, 2024 4:29pm	OKTA	Identity & Access Management	Authentication: Logon	Failure	User login to Okta
Apr 30, 2024 4:29pm	SL	Application	Web Resources Activity: Read	Success	Previewed files and/or folders

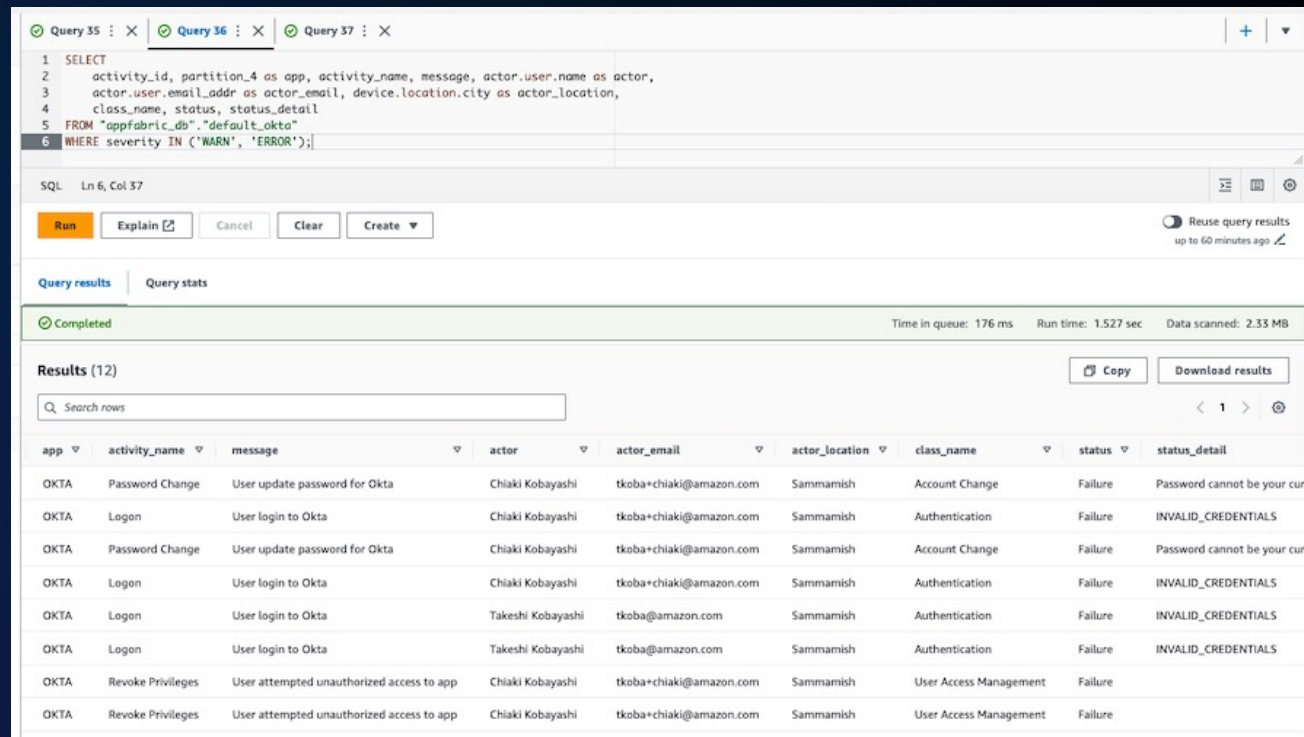
Geographic Locations



Amazon QuickSight を利用して「ログイン失敗」と「アクセス場所」を可視化したグラフ

インサイトの種類

- セキュリティ
 - 異常なログイン場所
 - 権限の変更
 - 多数のログイン失敗
- Ad hoc 検索
 - インシデント調査と対応
 - ユーザーの活動追跡
- SaaSの利用頻度
 - トップアプリ、ユーザー、場所
 - ライセンスの最適化、アラート



The screenshot shows the Amazon Athena console interface. At the top, there are three tabs for Query 35, Query 36, and Query 37. The active query is displayed in a text area with the following SQL code:

```
1 SELECT
2   activity_id, partition_4 as app, activity_name, message, actor.user.name as actor,
3   actor.user.email_addr as actor_email, device.location.city as actor_location,
4   class_name, status, status_detail
5 FROM "appfabric_db"."default_okta"
6 WHERE severity IN ('WARN', 'ERROR');
```

Below the query editor, there are buttons for "Run", "Explain", "Cancel", "Clear", and "Create". The "Run" button is highlighted in orange. To the right, there is a toggle for "Reuse query results up to 60 minutes ago".

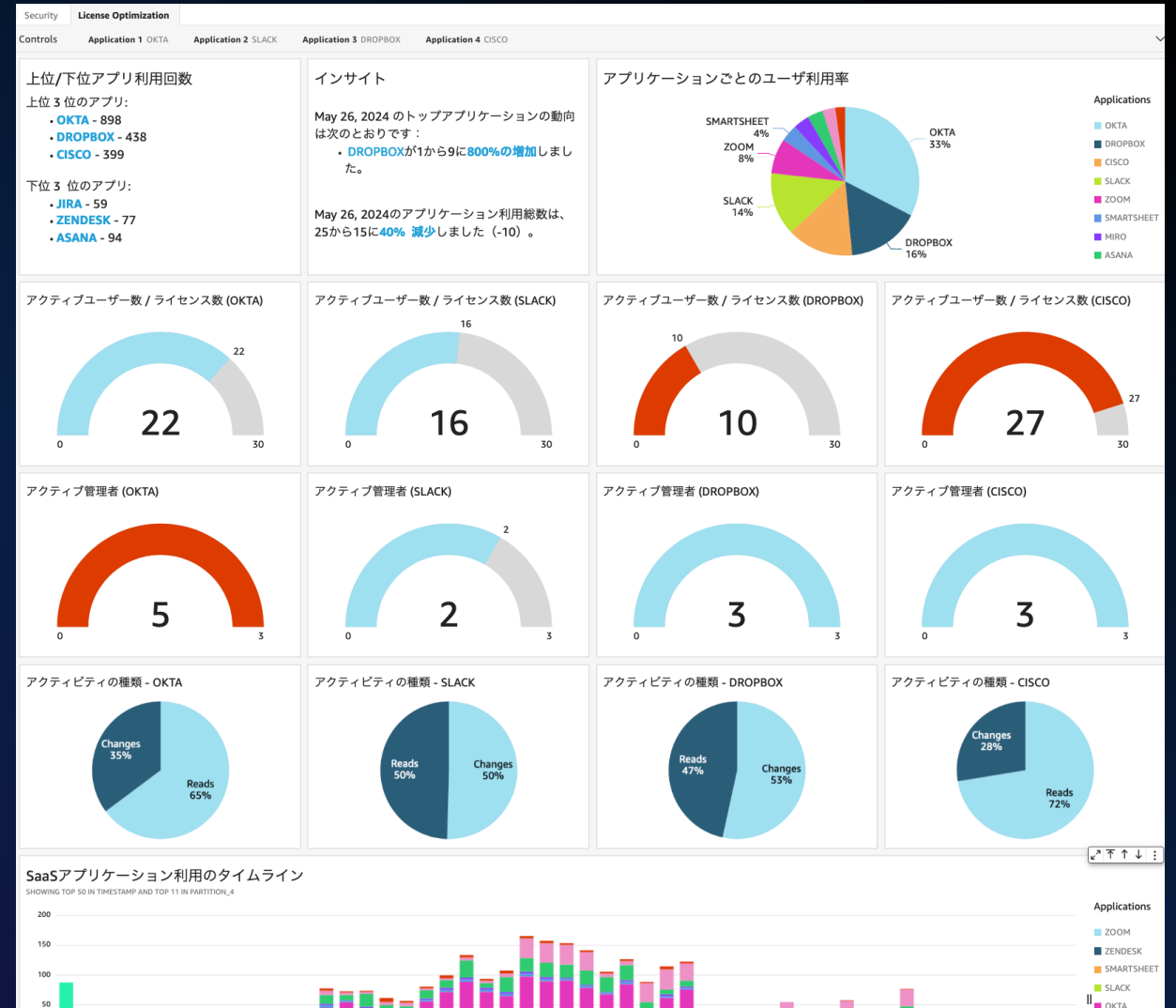
The "Query results" tab is active, showing a "Completed" status. Below this, there are buttons for "Copy" and "Download results". A search bar for rows is present. The main area displays a table with 12 rows of results. The table has the following columns: app, activity_name, message, actor, actor_email, actor_location, class_name, status, and status_detail.

app	activity_name	message	actor	actor_email	actor_location	class_name	status	status_detail
OKTA	Password Change	User update password for Okta	Chiaki Kobayashi	tkoba+chiaki@amazon.com	Sammamish	Account Change	Failure	Password cannot be your cur
OKTA	Logon	User login to Okta	Chiaki Kobayashi	tkoba+chiaki@amazon.com	Sammamish	Authentication	Failure	INVALID_CREDENTIALS
OKTA	Password Change	User update password for Okta	Chiaki Kobayashi	tkoba+chiaki@amazon.com	Sammamish	Account Change	Failure	Password cannot be your cur
OKTA	Logon	User login to Okta	Chiaki Kobayashi	tkoba+chiaki@amazon.com	Sammamish	Authentication	Failure	INVALID_CREDENTIALS
OKTA	Logon	User login to Okta	Takeshi Kobayashi	tkoba@amazon.com	Sammamish	Authentication	Failure	INVALID_CREDENTIALS
OKTA	Logon	User login to Okta	Takeshi Kobayashi	tkoba@amazon.com	Sammamish	Authentication	Failure	INVALID_CREDENTIALS
OKTA	Revoke Privileges	User attempted unauthorized access to app	Chiaki Kobayashi	tkoba+chiaki@amazon.com	Sammamish	User Access Management	Failure	
OKTA	Revoke Privileges	User attempted unauthorized access to app	Chiaki Kobayashi	tkoba+chiaki@amazon.com	Sammamish	User Access Management	Failure	

Amazon Athena を利用してクエリー検索の例

インサイトの種類

- セキュリティ
 - 異常なログイン場所
 - 権限の変更
 - 多数のログイン失敗
- Ad hoc 検索
 - インシデント調査と対応
 - ユーザーの活動追跡
- SaaSの利用頻度
 - トップアプリ、ユーザー、場所
 - ライセンスの最適化、アラート

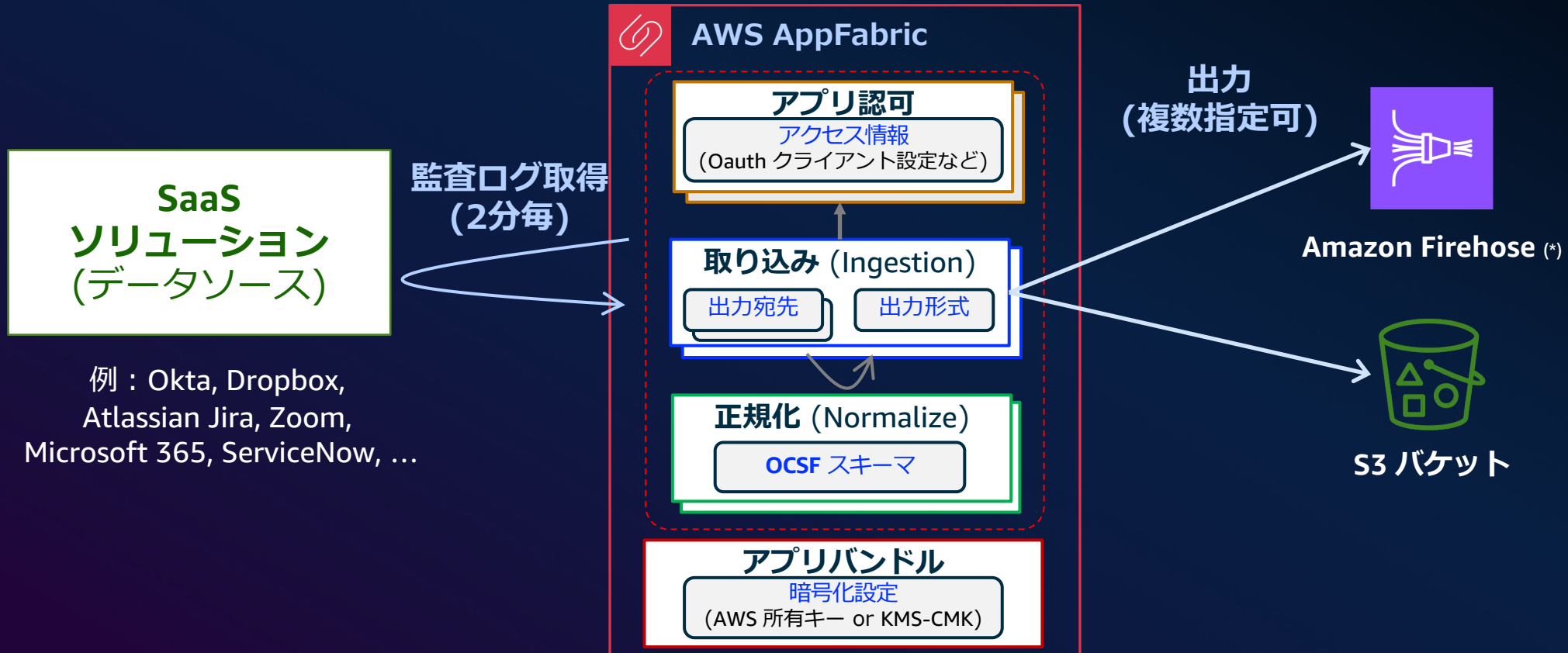


Amazon QuickSight を利用して利用頻度を可視化したダッシュボード

AWS AppFabric - 概要

東京リージョン
利用可能

SaaS の監査ログ(アクセスログ)を定期的に収集し、
所定のデータ形式で Amazon Firehose または S3 バケットに出力する



AWS AppFabric - アプリケーション

AppFabricと統合されたアプリケーション

SaaS アプリケーション (データ元)

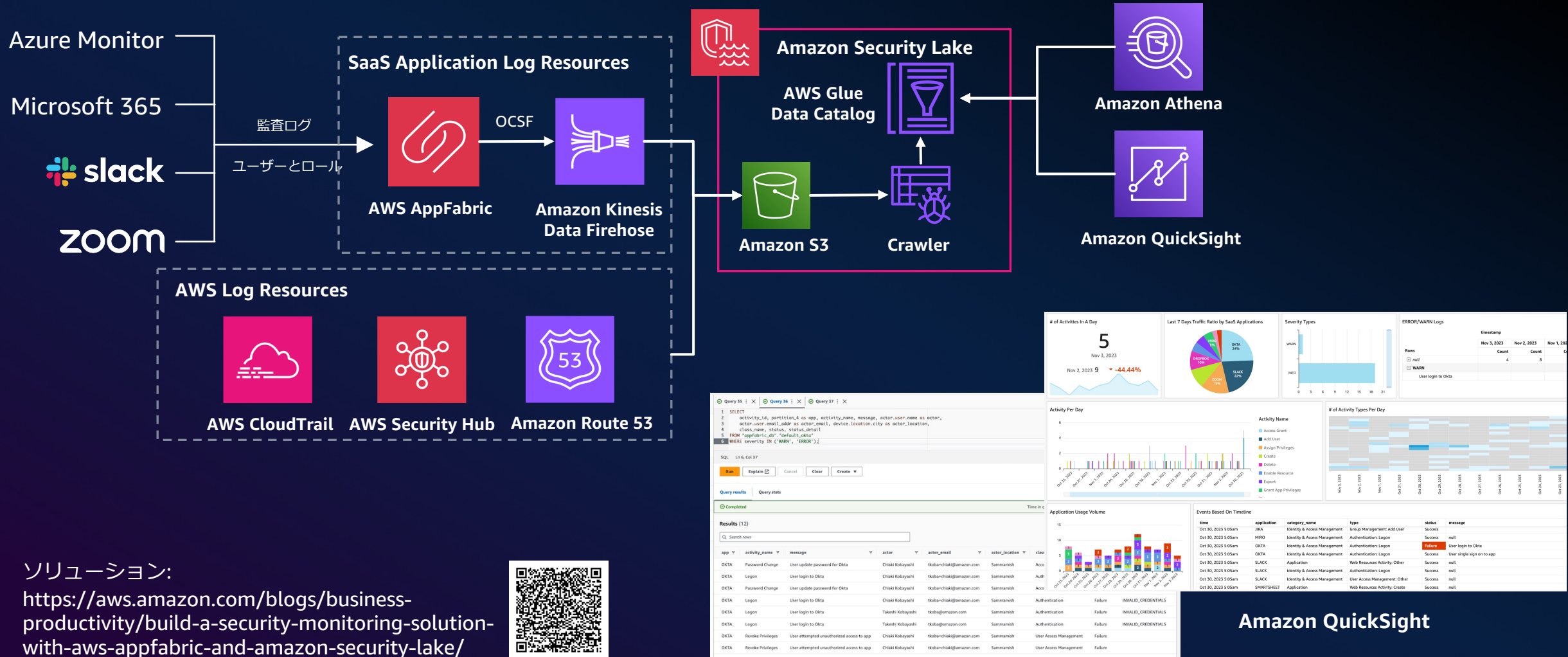


セキュリティ アプリケーション (データ宛先)



AWS AppFabric - セキュリティ監視

SaaSアプリとAWSリソースのセキュリティ監視

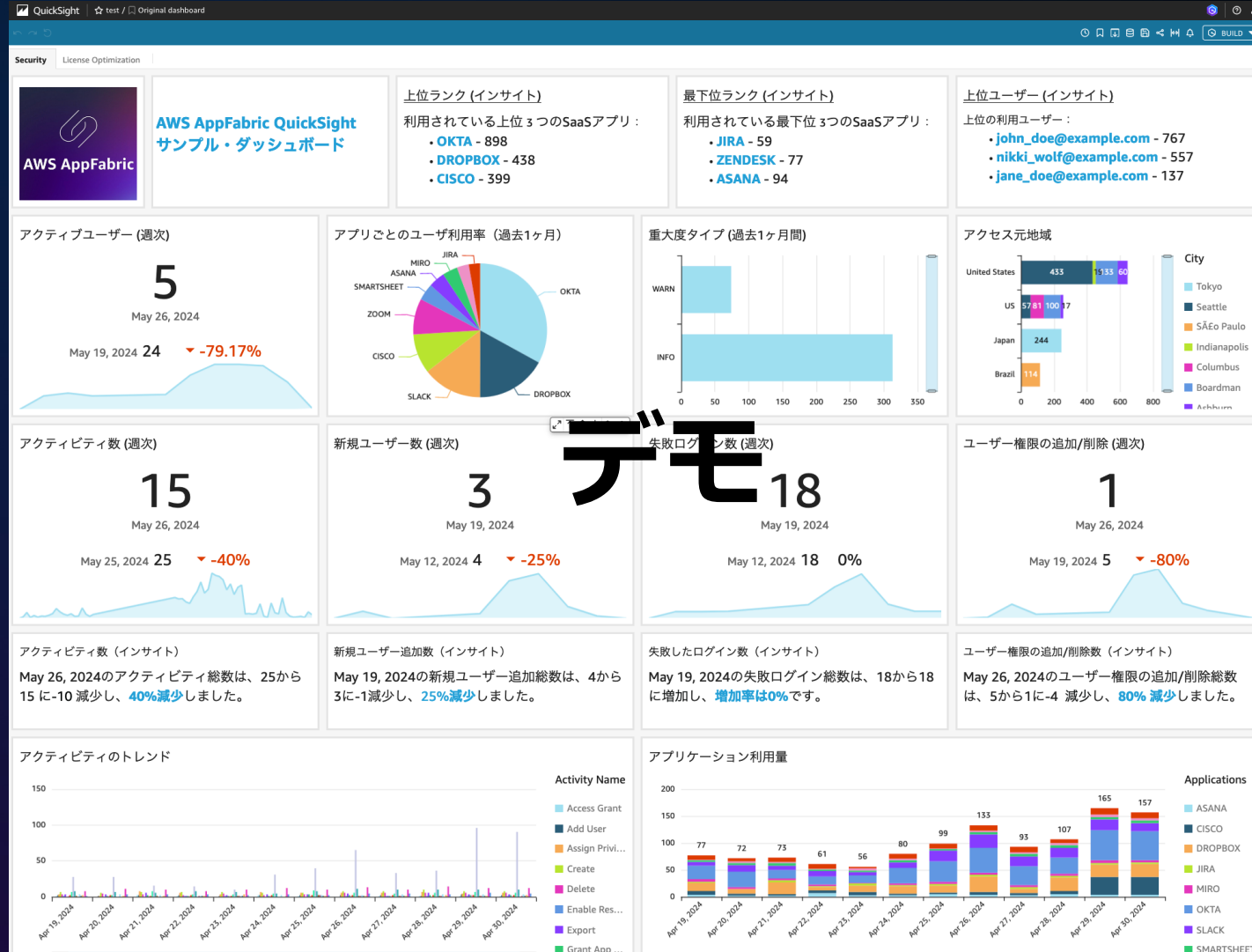


ソリューション:

<https://aws.amazon.com/blogs/business-productivity/build-a-security-monitoring-solution-with-aws-appfabric-and-amazon-security-lake/>



AWS AppFabric - セキュリティ監視



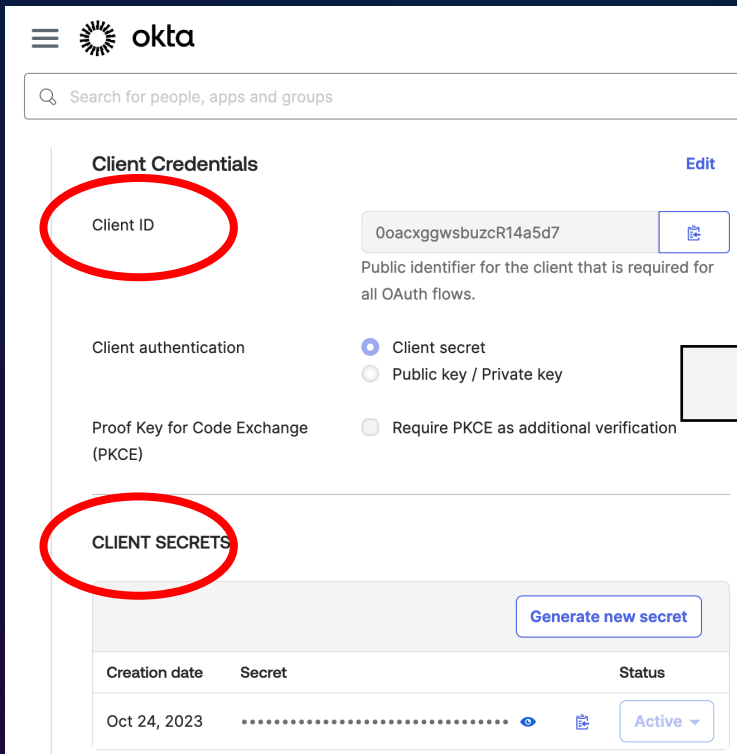
デモ

<https://github.com/aws-samples/appfabric-data-analytics/>

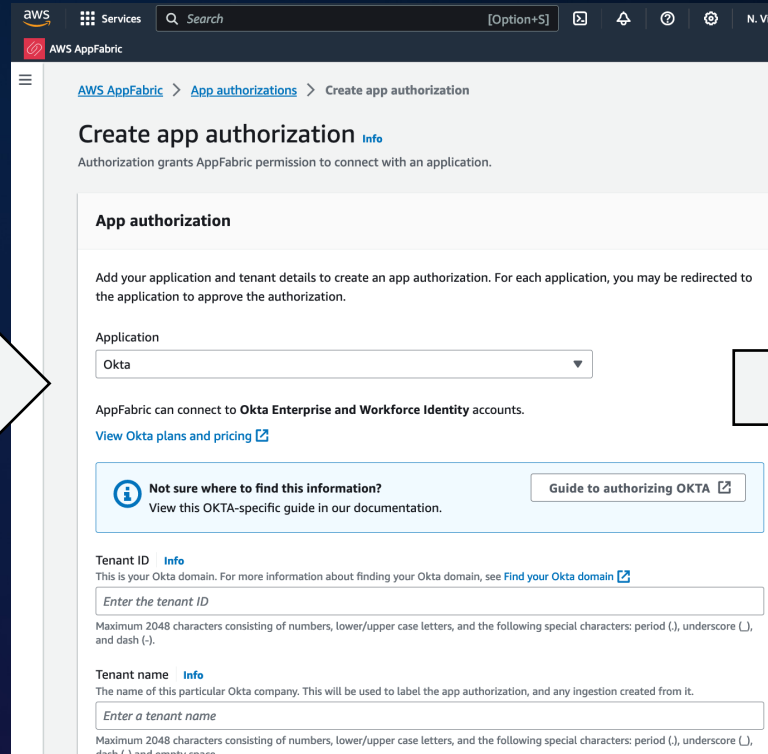


AWS AppFabric - 設定

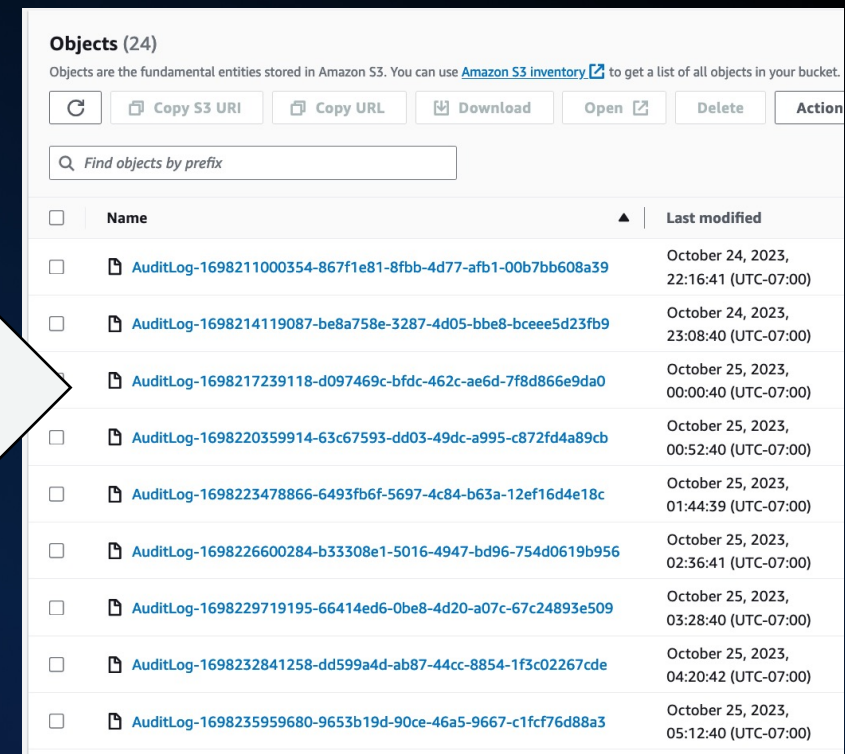
AWSマネージメントコンソールで簡単な3ステップ



The screenshot shows the Okta 'Client Credentials' page. The 'Client ID' field is circled in red. Below it, the 'CLIENT SECRETS' section is also circled in red, showing a table with one entry for 'Oct 24, 2023' with an 'Active' status. A large arrow points from this page to the AWS AppFabric console.



The screenshot shows the AWS AppFabric 'Create app authorization' page. The 'Application' dropdown menu is set to 'Okta'. A large arrow points from this page to the S3 console.



The screenshot shows the AWS S3 'Objects' page with a list of 24 objects. The objects are all named 'AuditLog-' followed by a long alphanumeric string. The table includes columns for 'Name' and 'Last modified'.

Name	Last modified
AuditLog-1698211000354-867f1e81-8fbb-4d77-afb1-00b7bb608a39	October 24, 2023, 22:16:41 (UTC-07:00)
AuditLog-1698214119087-be8a758e-3287-4d05-bbe8-bceee5d23fb9	October 24, 2023, 23:08:40 (UTC-07:00)
AuditLog-1698217239118-d097469c-bfdc-462c-ae6d-7f8d866e9da0	October 25, 2023, 00:00:40 (UTC-07:00)
AuditLog-1698220359914-63c67593-dd03-49dc-a995-c872fd4a89cb	October 25, 2023, 00:52:40 (UTC-07:00)
AuditLog-1698223478866-6493fb6f-5697-4c84-b63a-12ef16d4e18c	October 25, 2023, 01:44:39 (UTC-07:00)
AuditLog-1698226600284-b33308e1-5016-4947-bd96-754d0619b956	October 25, 2023, 02:36:41 (UTC-07:00)
AuditLog-1698229719195-66414ed6-0be8-4d20-a07c-67c24893e509	October 25, 2023, 03:28:40 (UTC-07:00)
AuditLog-1698232841258-dd599a4d-ab87-44cc-8854-1f3c02267cde	October 25, 2023, 04:20:42 (UTC-07:00)
AuditLog-1698235959680-9653b19d-90ce-46a5-9667-c1fcf76d88a3	October 25, 2023, 05:12:40 (UTC-07:00)

SaaSアプリ・管理ページ

AppFabricのコンソール

S3のコンソール

AppFabric の始め方

1

AWS アカウントでログインします

無料で AWS アカウントを作成し、AWS AppFabric を選択してください¹

2

SaaS アプリケーションを接続します

IT 管理者は、SaaS アプリケーションを AppFabric に接続するための認証情報と承認トークンを提供します。

3

AppFabric の使用を開始しましょう

AppFabric の機能を使用して、セキュリティと生産性を向上させるのを始めましょう。

はじめましょう



aws.amazon.com/console

AppFabric について



aws.amazon.com/appfabric

Thank you!

