

AWS Summit Japan 2026 ミニセッション

「A-gate[®]」 クラウドの情報漏洩リスクを即時修復！



2026年6月25,26日

株式会社NTTデータ 第二金融事業本部 デジタルバンキング事業部

登壇者プロフィール



安藤 耀将 (Yousuke Andou)

NTTデータ 第二金融事業本部 デジタルバンキング事業部

A-gate営業担当として、様々な業界のお客様へご提案。
グローバル案件の推進にも従事。

登壇者プロフィール



内堀 惣仁 (Nobuhito Uchibori)

NTTデータ 第二金融事業本部 デジタルバンキング事業部

大手銀行にて、法人企画等に従事。
その後、N T Tデータに入社し、BaselやALM関連の企画、営業や
大手金融機関向け開発案件に携わる。
現在はA-gate営業として、幅広い顧客へ、ご提案を実施。

登壇者プロフィール



菊地 雅仁 (Masahito Kikuchi)

NTTデータ 第二金融事業本部 デジタルバンキング事業部

A-gate開発担当として、
AWSに関するセキュリティソリューションの設計・構築を担当。
AWS環境におけるセキュリティ強化を通じて、お客様の安全なクラウド活用を支援している。

登壇者プロフィール



呉 雨可 (Yuke Wu)

NTTデータ 第二金融事業本部 デジタルバンキング事業部

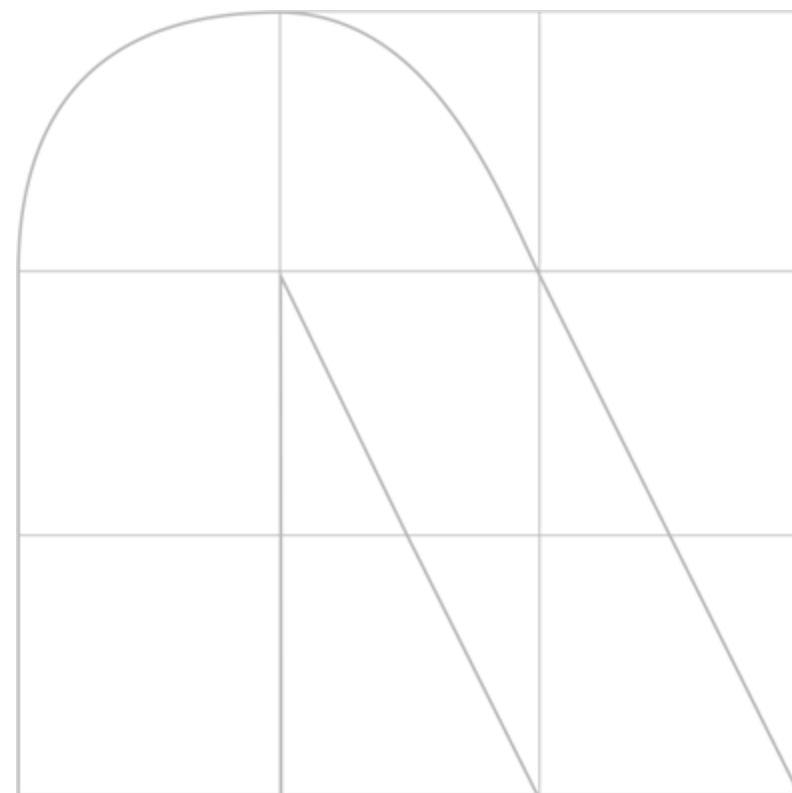
A-gate開発・運用担当として、
様々な業界のお客様にプリセールス・ご利用サポート対応しており、
お客様のクラウド活用推進に貢献している。

Agenda

- 01 クラウドの脅威と向き合い方
- 02 NTTデータが提供する「A-gate®」
- 03 「A-gate®」の強み
- 04 最後に

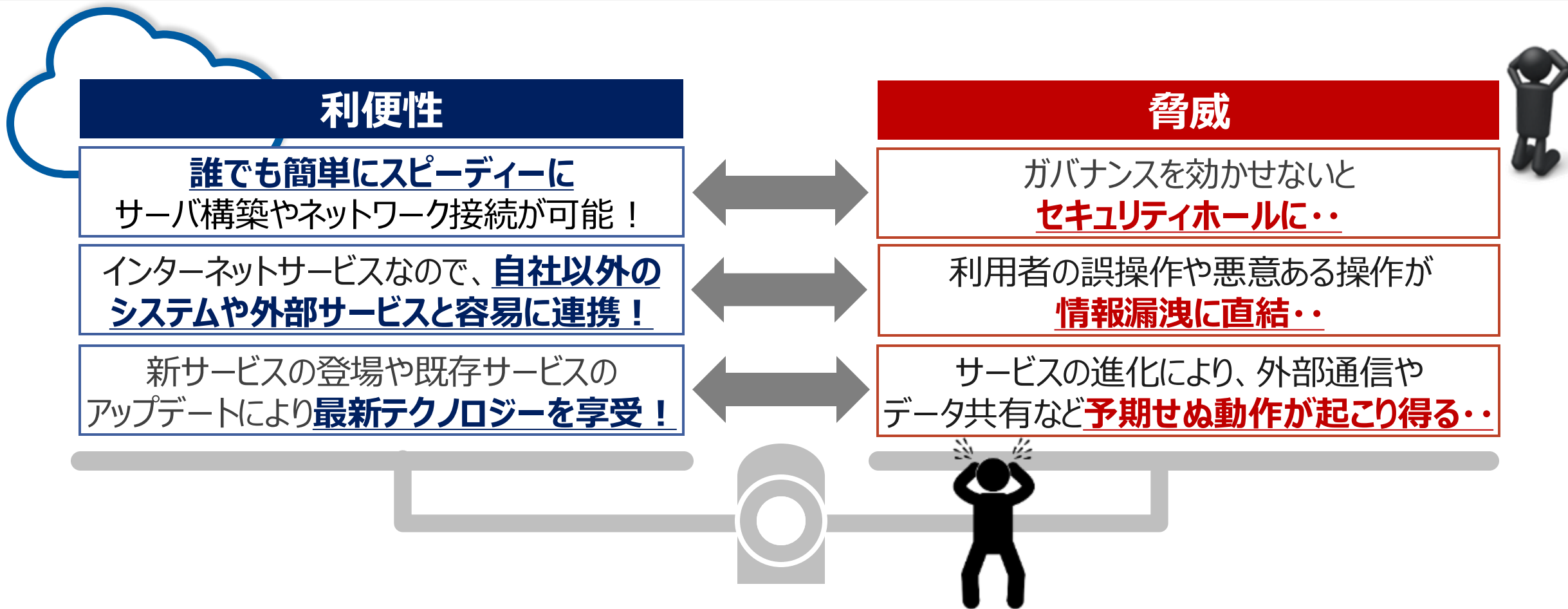
01

クラウドの脅威と向き合い方



クラウドの利便性と脅威

クラウドの利便性は**セキュリティの脅威の大きさ**とトレードオフ。
脅威を正しく理解し、対策することが重要。



クラウドの利便性と脅威

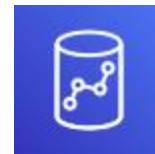
便利な反面、情報漏洩につながる設定がたくさん存在します。

アマゾン ウェブ サービス(AWS)の例



Amazon EC2

他アカウントへの
マシンイメージ共有を始め
数多のリスク有



Amazon Redshift

他アカウントへのイメージ
共有による漏洩リスク



AWS Lambda

VPC外に作成すると
Internet上のリソースに
アクセスし放題



Amazon RDS

他アカウントへのイメージ
共有による漏洩リスク

クラウドの情報漏洩リスクに対応するためには
「共有と公開を防御する仕組み」と「ガバナンスを効かせる体制」が必要です！

「A-gate®」のご提案

NTTデータは
AWSをセキュアに活用する

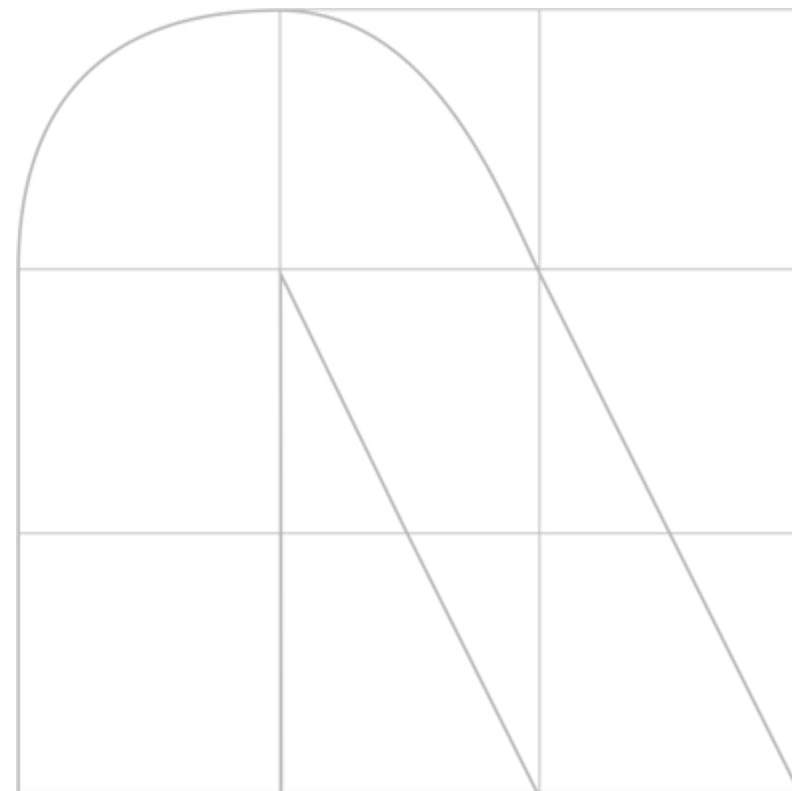
「A-gate®」

をご提案します



02

NTTデータが提供する「A-gate®」



「A-gate®」がご提供するもの

スタートアップコンサル

オプション



まずはクラウドのリスクを知り、
安全に利用するための社内ルールを整備する

クラウドセキュリティ基盤



安全に利用するための機能・仕組みを整える

マネージドCCoE



クラウドの進化に追従し、
機能・仕組みを進化させていく

「A-gate®」がご提供するもの

スタートアップコンサル



まずはクラウドのリスクを知り、
安全に利用するための社内ルールを整備する

クラウドセキュリティ基盤



安全に利用するための機能・仕組みを整える

マネージドCCoE



クラウドの進化に追従し、
機能・仕組みを進化させていく

「A-gate®」がご提供するもの



クラウドセキュリティ基盤



違反検知・修復

情報漏洩リスクのある設定を検知し、
自動で安全な設定に戻す機能

静的スキャン

クラウド上の情報漏洩リスクのある設定を
洗い出し、一覧化する機能

権限分掌

クラウドの操作権限を分掌するための
権限セット

「A-gate®」がご提供するもの



クラウドセキュリティ基盤



違反検知・修復

情報漏洩リスクのある設定を検知し、
自動で安全な設定に戻す機能

静的スキャン

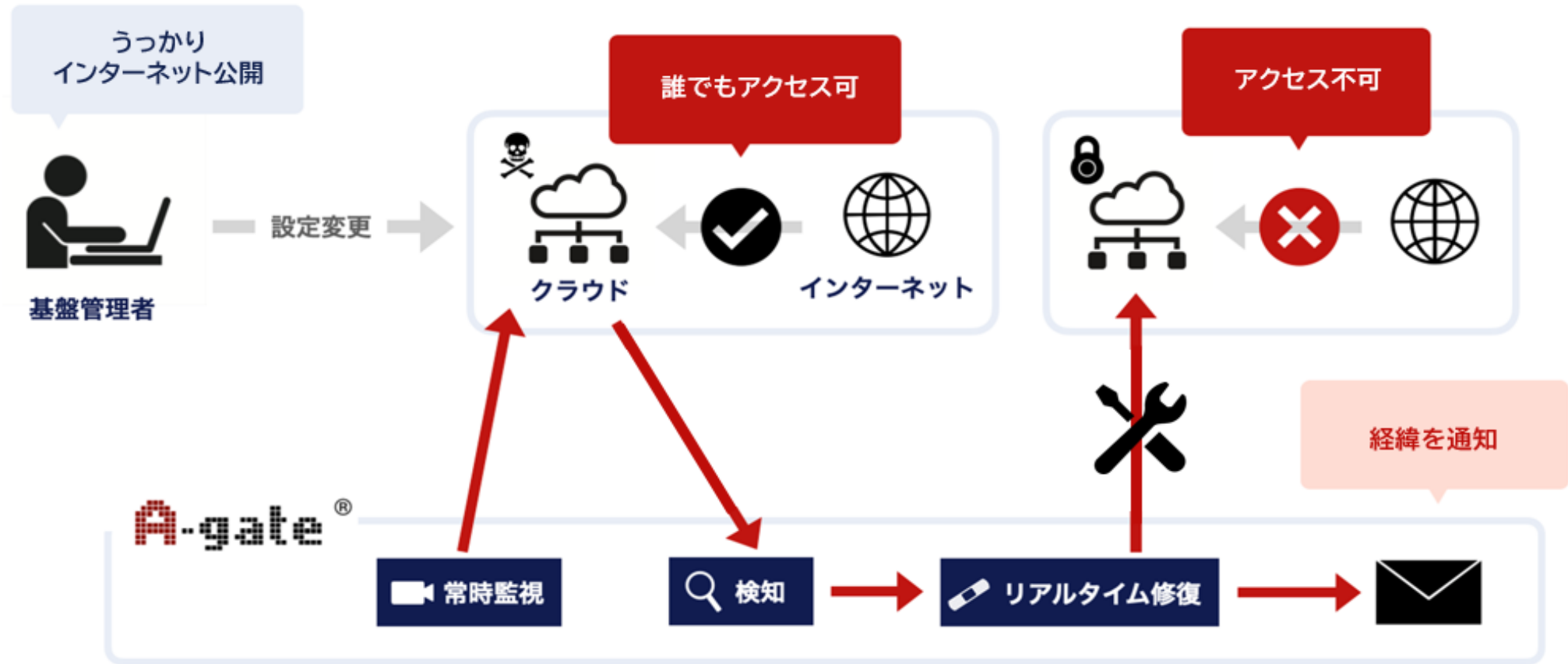
クラウド上の情報漏洩リスクのある設定を
洗い出し、一覧化する機能

権限分掌

クラウドの操作権限を分掌するための
権限セット

クラウドセキュリティ基盤：違反検知・修復とは？

情報漏洩リスクのある設定を**約2秒**で検知＆修復します。



A-gate機能を 継続してアップデート
～AWSを安全に利用するために、AWSの進化（新機能追加／更新）に追随～

クラウドセキュリティ基盤：違反検知・修復とは？

情報漏洩に直結する通信設定やデータ共有をポリシー違反と定義
(現在、AWS版では約150のルールがある) (2026年4月時点)

大項目	小項目	違反の例	修復の例
通信経路	パブリック	・InternetGatewayの設置	・InternetGatewayをVPCからデタッチ
	オンプレミス (自社以外)	・VpnGatewayの設置	・VpnGatewayをVPCからデタッチ
	他アカウント	・VPC Peeringの設置 ・PrivateLinkの共有設定 ・Gateway型のEndpointの設置 etc	・Peeringの切断 ・PrivateLinkの共有設定削除 ・Endpointの削除/Policyの修復
データ共有	パブリック公開	・Amazon S3のパブリック公開 ・非VPC型AWS Lambdaの設置 etc	・Amazon S3を非公開設定に変更 ・AWS Lambdaの削除
	他アカウントへ共有	・マシンイメージの共有 ・Amazon EMRの共有 etc	・共有設定を削除
非暗号化	データ	・Amazon S3、Amazon EMR、 Amazon RDS・・・etc	・暗号化 (Amazon EBSのブートディスクは例外)

EC2

ダッシュボード

EC2 グローバルレビュー

イベント

▼ インスタンス

インスタンス

インスタンスタイプ

起動テンプレート

スポットリクエスト

Savings Plans

リザーブドインスタンス

専有ホスト

キャパシティの予約

▼ イメージ

AMI

AMI カタログ

▼ Elastic Block Store

ボリューム

スナップショット

ライフサイクルマネージャ

▼ ネットワーク & セキュリティ

セキュリティグループ

Elastic IP

プレイスメントグループ

キーペア

ネットワークインターフェイス

CloudShell

フィードバック

EC2 > AMI > ami-

ami- のイメージの概要

AMI ID
ami-

AMI 名
111

ルートデバイス名
/dev/xvda

ブートモード
uefi-preferred

説明
-

最終起動時刻
-

ソース AMI ID
ami-

イメージタイプ
machine

所有者のアカウント ID
-

ステータス
利用可能

状態の理由
-

製品コード
-

ブロックデバイス
/dev/xvda=snap-015af9347ec9e256b:8:true:gp3

ソース AMI リージョン
ap-northeast-1

プラットフォームの詳細
Linux/UNIX

アーキテクチャ
x86_64

ソース
-

作成日
2024-06-04T05:15:43.000Z

RAM ディスク ID
-

登録解除保護
Disabled

ルートデバイスタイプ
EBS

使用オペレーション
RunInstances

仮想化タイプ
hvm

カーネル ID
-

非推奨化の時刻
-

許可された画像
-

EC2 Image Builder

アクション

AMI からインスタンスを起動

許可

ストレージ

タグ

イメージ共有の許可
プライベート
このイメージは、指定したアカウント ID、組織、または OU のみと共有されます。

① 画像を公開する際の制限は、以下を使用して管理されます: AMI へのパブリックアクセスをブロック 設定: データ保護とセキュリティ。

▼ 共有アカウント

Q アカウント ID で共有アカウントを検索

共有アカウント ID

共有アカウントはありません
この AMI は他のアカウントと共有されません。

アカウント ID を追加

AMI 許可を編集

< 1 >

▼

▼ 共有組織/OU

AMI 許可を編集 情報

AMI の許可を編集することで、指定した AWS アカウント、組織、または OU と共有できます。

AMI 共有の設定

AMI ID

ami-

関連付けられたスナップショット ID

snap-

☐ アカウント許可を作成するときに、関連付けられたスナップショットに [ボリュームを作成] の許可を追加します。
この設定は、特定の AWS アカウントと AMI を共有する場合にのみ適用されます。

AMI の可用性

☐ パブリック

AMI をすべての AWS のユーザーとパブリックに共有します。このオプションは、ア

☒ プライベート - (現在の設定)

AMI を特定のアカウント、組織、または OU と共有します。

共有アカウント (0)

🔍 アカウント ID で共有アカウントを検索

共有アカウント ID

この AMI は他のアカウントと共有されません。

選択項目を削除

アカウント ID を追加

< 1 > ⚙

キャンセル

AMI を共有

共有組織/OU (0)

🔍 ARN で共有組織および OU を検索

共有組織/OU の ARN

この AMI は、どの組織/OU とも共有されません。

選択項目を削除

組織/OU の ARN を追加

< 1 > ⚙

EC2 > AMI > ami-

EC2

ダッシュボード
EC2 グローバルビュー
イベント

▼ インスタンス
インスタンス
インスタンスタイプ
起動テンプレート
スポットリクエスト
Savings Plans
リザーブドインスタンス
専有ホスト
キャパシティの予約

▼ イメージ
AMI
AMI カタログ

▼ Elastic Block Store
ボリューム
スナップショット
ライフサイクルマネージャ

▼ ネットワーク & セキュリティ
セキュリティグループ
Elastic IP
プレースメントグループ
キーペア
ネットワークインターフェイス

CloudShell フィードバック

test-amiura-ami

ルートデバイス名
/dev/xvda

ブートモード
-

説明
-

最終起動時刻
-

ソース AMI ID
ami-

ステータス
利用可能

状態の理由
-

製品コード
-

ブロックデバイス
/dev/xvda=snap-0e2e736ec913f7495:8:true:gp2

ソース AMI リージョン
ap-northeast-1

xob_04

ソース
-

作成日
2023-02-14T05:01:32.000Z

RAM ディスク ID
-

登録解除保護
Disabled

instances

仮想化タイプ
hvm

カーネル ID
-

非推奨化の時刻
Fri Feb 14 2025 14:01:32 GMT+0900 (日本標準時)

許可された画像
-

許可 | ストレージ | タグ

イメージ共有の許可
プライベート
このイメージは、指定したアカウント ID、組織、または OU のみと共有されます。

① 画像を公開する際の制限は、以下を使用して管理されます: AMI へのパブリックアクセスをブロック 設定: データ保護とセキュリティ。

▼ 共有アカウント

AMI 許可を編集

1 1

Q アカウント ID で共有アカウントを検索

共有アカウント ID

123456789012

▼ 共有組織/OU

AMI 許可を編集

1 1

Q ARN で共有組織/OU を検索

共有組織/OU の ARN

共有組織/OU なし
この AMI は、どの組織/OU とも共有されません。

組織/OU の ARN を追加

EC2

ダッシュボード
EC2 グローバルビュー
イベント

▼ インスタンス

インスタンス
インスタンスタイプ
起動テンプレート
スポットリクエスト
Savings Plans
リザーブドインスタンス
専有ホスト
キャパシティの予約

▼ イメージ

AMI
AMI カタログ

▼ Elastic Block Store

ボリューム
スナップショット
ライフサイクルマネージャ

▼ ネットワーク & セキュリティ

セキュリティグループ
Elastic IP
プレースメントグループ
キーペア
ネットワークインターフェイス

ami- のイメージの概要

AMI ID
ami-

AMI 名
111

ルートデバイス名
/dev/xvda

ブートモード
uefi-preferred

説明
-

最終起動時刻
-

ソース AMI ID
ami-

イメージタイプ
machine

所有者のアカウント ID
-

ステータス
利用可能

状態の理由
-

製品コード
-

ブロックデバイス
/dev/xvda=snap-015af9347ec9e256b:8:true:gp3

ソース AMI リージョン
ap-northeast-1

プラットフォームの詳細
Linux/UNIX

アーキテクチャ
x86_64

ソース
-

作成日
2024-06-04T05:15:43.000Z

RAM ディスク ID
-

登録解除保護
Disabled

ルートデバイスタイプ
EBS

使用オペレーション
RunInstances

仮想化タイプ
hvm

カーネル ID
-

非推奨化の時刻
-

許可された画像
-

[EC2 Image Builder](#)[アクション](#)[AMI からインスタンスを起動](#)

許可 ストレージ タグ

イメージ共有の許可

プライベート

このイメージは、指定したアカウント ID、組織、または OU のみと共有されます。

画像を公開する際の制限は、以下を使用して管理されます: AMI へのパブリックアクセスをブロック 設定: データ保護とセキュリティ。

▼ 共有アカウント

Q アカウント ID で共有アカウントを検索

[AMI 許可を編集](#)

共有アカウント ID

共有アカウントはありません
この AMI は他のアカウントと共有されません。

[アカウント ID を追加](#)

クラウドセキュリティ基盤：違反検知・修復 とは？（補足）

要件上リスク有設定を行う必要がある場合、
「例外登録」により違反検知・修復を回避することが可能です。

A-gateポータル

メニュー

検知修復の例外登録

検知修復の動作モード変更

テナントの状態確認

検知修復履歴

AWS関連 (NEW)

Azure関連

Salesforce関連

A-gateポータル関連

通知先の管理

サポート問い合わせ

A-gateドキュメント

A-gate管理者メニュー

検知修復の例外申請

クラウド種別

AWS

アカウントID

検知修復ルール

EC2_AMIの共有

【注】 検知修復ルールに【工事中】と記載されている項目は、現在ポータルから例外申請できません。
例外申請が必要な場合は、A-gateポータルからリクエストを送信するか、下記メールアドレスにご依頼ください。

A-gate問い合わせ窓口：support@a-gate.zendesk.com

次へ

「A-gate®」がご提供するもの



クラウドセキュリティ基盤



違反検知・修復

情報漏洩リスクのある設定を検知し、
自動で安全な設定に戻す機能

静的スキャン

クラウド上の情報漏洩リスクのある設定を
洗い出し、一覧化する機能

権限分掌

クラウドの操作権限を分掌するための
権限セット

クラウドセキュリティ基盤：静的スキャンとは？

違反検知・修復のルールに則り、
AWSアカウント上の**リスクのある設定を洗い出し、一覧化**することが可能です。

すでにお使いの
AWSアカウントに対しても
情報漏洩リスクの有無を
チェック可能！

※「チェックした項目をまとめて例外申請する」は**担当者権限**でのみ実施可能です。

すべての行を展開する

🔄

チェックした項目をまとめて例外申請する

検知修復ルール		例外登録実施状況	
☐ すべての[例外申請する]にチェックする			
▼	Critical AppStream_ImagebuilderストリーミングURLの作成 ②	対象なし	
▼	Critical AppStream_StackストリーミングURLの作成 ②	対象なし	
▼	Critical Connect_インスタンスの作成 ②	すべて未登録	
▼	Critical EC2_AMIの共有 ②	すべて未登録	
リージョン AMIの共有を許可するAWSアカウント		例外登録状況	例外申請する
	東京 [redacted]	未登録	☐
	東京 [redacted]	未登録	☐
▼	Critical EC2_EBSスナップショットの共有 ②	対象なし	
▼	Critical FSx for Lustre_ファイルシステムにおけるデータリポジトリの書き込み先設定 ②	対象なし	
▼	Critical IAM_OpenIDConnectIDプロバイダの設定 ②	すべて登録済	
▼	Critical Kinesis_配信ストリームの他アカウント出力と非暗号化 ②	対象なし	

メニュー

- 検知修復の例外登録
- 検知修復の動作モード変更
- テナントの状態確認
- 検知修復履歴
- AWS関連 **【NEW】**
- Azure関連
- Salesforce関連
- A-gateポータル関連
- 通知先の管理
- サポート問い合わせ
- A-gateドキュメント
- A-gate管理者メニュー

テナントリソースの状態確認

【アカウント情報】

クラウド種別	AWS
アカウントID	

【リソース状態取得条件】

【リージョン】

東京

【検知修復ルール】

リソース状態を取得する検知修復ルールを選択する

※検知修復ルールのリスクレベルの定義については [こちら](#)※「S3_バケットおよびオブジェクトACLの設定」のうち、[オブジェクトACL](#)は状態確認の対象外です。※IAMのリソース状態を取得する際は [こちら](#) を必ずご確認ください

テナントのリソース状態を取得する

【直近の状態取得情報】

直近の状態取得時刻	2025/04/14 16:42:57
リージョン	東京

メニュー

- 検知修復の例外登録
- 検知修復の動作モード変更
- テナントの状態確認
- 検知修復履歴
- AWS関連 **【NEW】**
- Azure関連
- Salesforce関連
- A-gateポータル関連
- 通知先の管理
- サポート問い合わせ
- A-gateドキュメント
- A-gate管理者メニュー

Search

- ☐ すべての検知修復ルール
- ☐ リスクレベル：Critical
 - ☐ AppStream_ImageBuilderストリーミングURLの作成
 - ☐ AppStream_StackストリーミングURLの作成
 - ☐ Client_VPN_クライアントVPNエンドポイントへのターゲットネットワークの関連付け
 - ☐ Cloud9_リモートサーバを利用する開発環境（SSH環境）の作成
 - ☐ CloudSearch_ドメインのアクセス許可設定
 - ☐ CodeArtifact_ドメインのアクセスポリシー設定
 - ☐ CodeArtifact_リポジトリのアクセスポリシー設定
 - ☐ Cognito_アプリクライアントの作成
 - ☐ Connect_インスタンスの作成
 - ☐ Direct_Connect_Direct Connectゲートウェイに対する接続承認
 - ☐ EC2_AMIの共有

リソース状態を取得する検知修復ルールを選択する

※検知修復ルールのリスクレベルの定義については [こちら](#)※「S3_バケットおよびオブジェクトACLの設定」のうち、[オブジェクトACL](#)は状態確認の対象外です。※IAMのリソース状態を取得する際は [こちら](#) を必ずご確認ください

テナントのリソース状態を取得する

【直近の状態取得情報】

直近の状態取得時刻	2025/04/14 16:42:57
リージョン	東京

※「チェックした項目をまとめて例外申請する」は**担当者権限**でのみ実施可能です。

すべての行を展開する



チェックした項目をまとめて例外申請する

検知修復ルール		例外登録実施状況	
☐ すべての[例外申請する]にチェックする			
▼	Critical AppStream_ImagebuilderストリーミングURLの作成 ②	対象なし	
▼	Critical AppStream_StackストリーミングURLの作成 ②	対象なし	
▼	Critical Connect_インスタンスの作成 ②	すべて未登録	
▼	Critical EC2_AMIの共有 ②	すべて未登録	
	リージョンAMIの共有を許可するAWSアカウント	例外登録状況	例外申請する
	東京	未登録	☐
	東京	未登録	☐
▼	Critical EC2_EBSスナップショットの共有 ②	対象なし	
▼	Critical FSx for Lustre_ファイルシステムにおけるデータリポジトリの書き込み先設定 ②	対象なし	
▼	Critical IAM_OpenIDConnectIDプロバイダの設定 ②	すべて登録済	
▼	Critical Kinesis_配信ストリームの他アカウント出力と非暗号化 ②	対象なし	

「A-gate[®]」がご提供するもの



クラウドセキュリティ基盤



違反検知・修復

情報漏洩リスクのある設定を検知し、
自動で安全な設定に戻す機能

静的スキャン

クラウド上の情報漏洩リスクのある設定を
洗い出し、一覧化する機能

権限分掌

クラウドの操作権限を分掌するための
権限セット

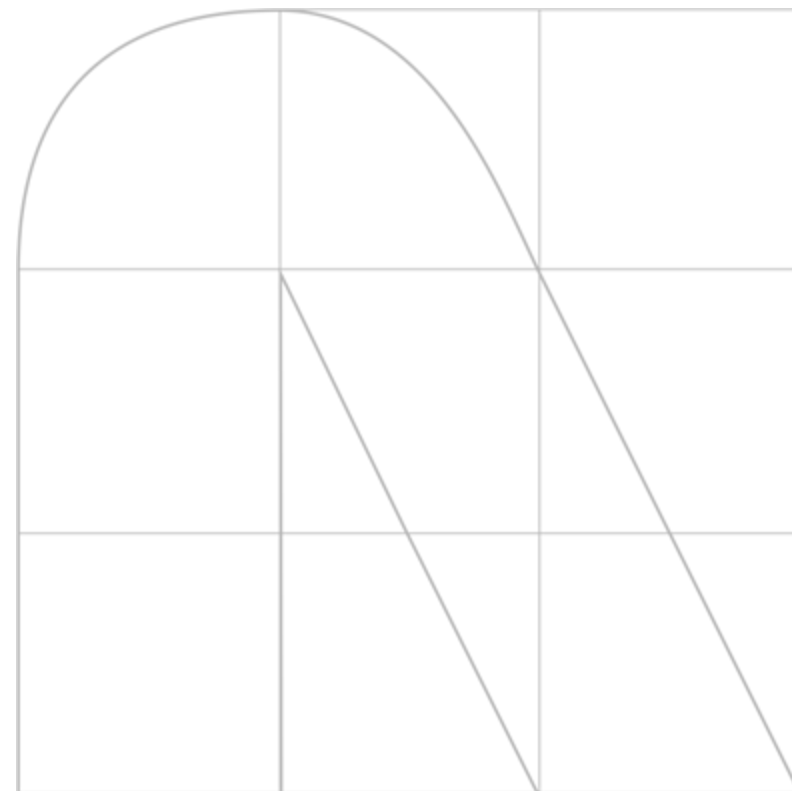
クラウドセキュリティ基盤 「権限分掌」とは？

A-gate[®]では、一般的な**システム開発に必要な権限セット**もご提供しています

役割	付与する権限・役割イメージ
 ID管理者	・ クラウドのユーザの作成・削除 ・ クラウドのユーザへの権限の付与・剥奪
 NW管理者	・ クラウド上の閉域NWと外部NWの接続確立 ・ クラウド上の閉域NWとオンプレミスの接続確立
 開発担当者	・ クラウド上への個別システムの構築 (他人へのデータ共有などの危険な操作権限なし)
 開発管理者	・ クラウド上への個別システムの構築 (他人へのデータ共有などの危険な操作権限あり)
⋮	

03

「A-gate®」の強み



「A-gate®」の強み

A-gate®は一般的なCSPM製品と比較して、
以下の点に強みがあります

1

一般的なCSPM製品では見落とされる
限定的な共有／公開設定を検出可能

2

違反を検知してから修復するまでの
スピードが速く、**内部不正を逃さない**

3

**数多くのサービスに対応し、
APIレベルでの網羅性も担保**

「A-gate[®]」の強み

1

一般的なCSPM製品では見落とされる
限定的な共有／公開設定を検出可能

例) S3バケットポリシーの設定



Amazon S3



任意のアカウントからの
読み取りを許可

A-gate[®]



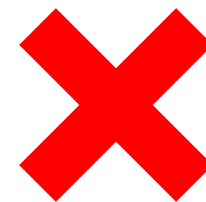
他社CSPM



Amazon S3



アカウントID「1111…」
からの読み取りを許可



「A-gate®」の強み

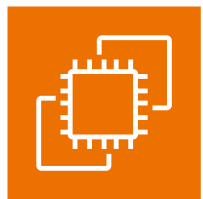
1

一般的なCSPM製品では見落とされる
限定的な共有／公開設定を検出可能

例) セキュリティグループの設定

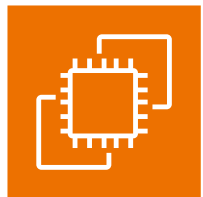
A-gate®

他社CSPM



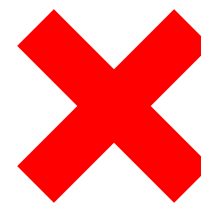
Amazon EC2

全世界 (0.0.0.0/0) からの
インバウンドアクセスを許可



Amazon EC2

世界の半分 (0.0.0.0/1) からの
インバウンドアクセスを許可



「A-gate[®]」の強み

2

違反を検知してから修復するまでの
スピードが速く、**内部不正を逃さない**



Amazon S3

情報持出し



設定戻し

自分の個人アドレスだけ
アクセス可にして
すぐに元に戻して証拠を
隠滅しよう

「A-gate®」の強み

2

違反を検知してから修復するまでの
スピードが速く、**内部不正を逃さない**



Amazon S3

情報持出し



設定戻し

自分の個人アドレスだけ
アクセス可にして
すぐに元に戻して証拠を
隠滅しよう



A-gate®は設定変更から約2秒で検知・自動修復！
(一般的なCSPMでは通知のみ、パトロールも1時間に1回)
通知メールも届くため不正にすぐ気付ける！

「A-gate®」の強み

3

数多くのサービスに対応し、
APIレベルでの網羅性も担保

対応するAWSサービスの数

A-gate®

100以上
(2026/04現在)

他社CSPM

30～50程度

「A-gate[®]」の強み

3

数多くのサービスに対応し、
APIレベルでの網羅性も担保

A-gate[®]では各アクション（API）に対してリスクチェックを行い、
検知・自動修復機能を具備。
一般的なCSPM製品では、以下のリスクからは守ってくれない…

【例】 Amazon EC2/ Amazon VPC	ModifyImageAttribute	AMIの共有が可能
	ModifySnapshotAttribute	Amazon EBSスナップショットの共有が可能
	ModifyVpcEndpoint	VPCエンドポイントポリシーの変更が可能 （情報持ち出しの抜け穴になりうる）
	...	...

「A-gate®」の強み

3

数多くのサービスに対応し、
APIレベルでの網羅性も担保

A-gateによりリスクチェックされた
アクションを組み合わせ、
ユーザが自由に権限セットを作れる機能も
ご提供しています

「マネージドCCoE」として、
A-gateが随時
リスクチェックを実施！

A-gateポータル関連
通知先の管理
サポート問い合わせ
A-gateドキュメント
A-gate管理者メニュー

お好みA-gate 申請

5. A-gate推奨アクションセット付与の選択

・A-gateによるリスクチェックが行われており、各役割に対して推奨される権限セットを付与します。

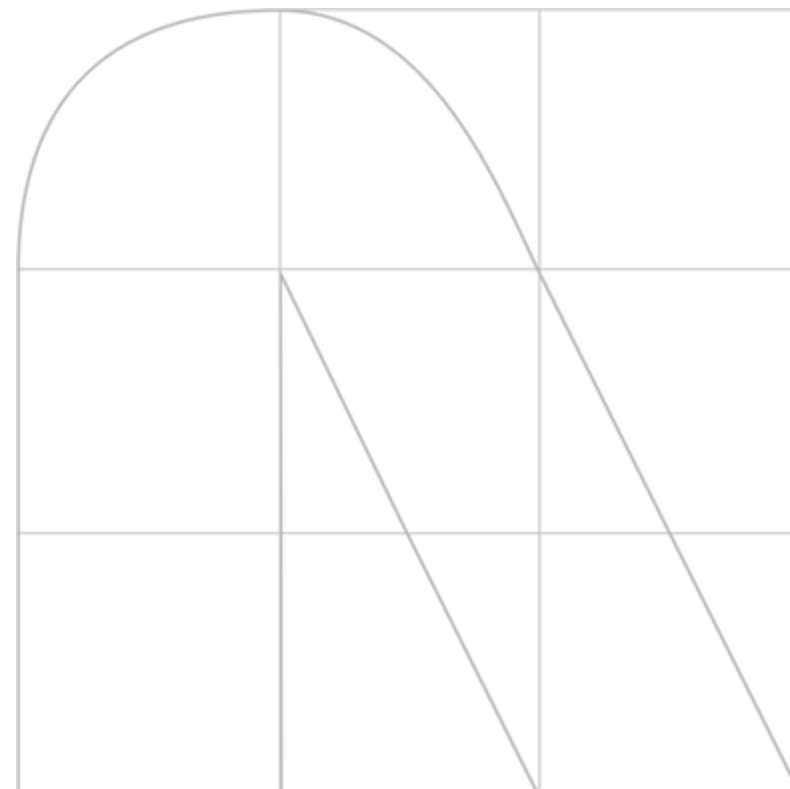
※ 設定可能なアクションには文字数の上限があります。
「確認」ボタンで文字数チェックおよび、付与予定アクションの確認を行ってください。

※ 各役割で利用可能なアクションについては、以下からご確認ください。
[「AWS_ガイド_A-gateの使い方_IAM・テナント開発編_【別紙】」のダウンロードはこちら](#)

サービス \ 権限	参照	サービス/ NW管理者	テナント 担当者	テナント 管理者
サービスを検索				
すべてのサービス	☐			
AmazonAPIGateway	☐	☐	☐	☐
AmazonAPIGatewayManagement	☐	☐	☐	☐
AmazonAppFlow	☐	☐	☐	☐
AmazonAppStream2.0	☐	☐	☐	☐
AmazonAthena	☐	☐	☐	☐
AmazonCloudFront	☐	☐	☐	☐
AmazonCloudSearch	☐	☐	☐	☐
AmazonCloudWatch	☐	☐	☐	☐
AmazonCloudWatchLogs	☐	☐	☐	☐
AmazonCloudWatchSynthetics	☐	☐	☐	☐
AmazonCognitoIdentity	☐	☐	☐	☐

04

最後に



まとめ

**「A-gate®」は、ベンチマークにとらわれず
情報漏洩に直結するかどうかという観点で
設定をつぶさにチェックします！**

**NTTデータの知見で、
情報漏洩に繋がる設定ミス・内部不正を
即時検知し、約 2 秒で修復します！**

まとめ

**「A-gate®」は、ベンチマークにとらわれず
情報漏洩に直結するかどうかという観点で
設定をつぶさにチェックします！**

ベンチマークも同時にカバーできる
進化版A-gateも現在企画中！
乞うご期待！

不正を
即時検知し、約2秒で修復します！

お問い合わせ

A-gate営業

株式会社 NTTデータ
第二金融事業本部 デジタルバンキング事業部
オフリング統括部 コンサルティング&セールス担当

A-gate(IaaS/PaaS)公式サイト



公式サイトのお問い合わせフォームからお気軽にお問い合わせください！



A-gate®

