NTT DATA

AWS Summitミニセッション

「A-gate®」
クラウドの情報流出リスクを即時修復！

2025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

庄司　武留（Shoji Takeru）
NTTデータ　第二金融事業本部　デジタルバンキング事業部

大手セキュリティサービスベンダーにて、法人営業に従事。
その後、ＮＴＴデータに入社し、A-gate営業として
金融業界を中心に幅広い顧客へ、ご提案を実施。

登壇者プロフィール

野口　陽平（Noguchi Yohei）
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、
プリセールス・お問い合わせ対応で、お客様のクラウド活用推進をサポート。
また、クラウドを使い始めるお客様向けのコンサルティングも行う。

登壇者プロフィール

谷崎　快斗（Tanizaki Kaito）
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・サポートの対応を行っており、
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

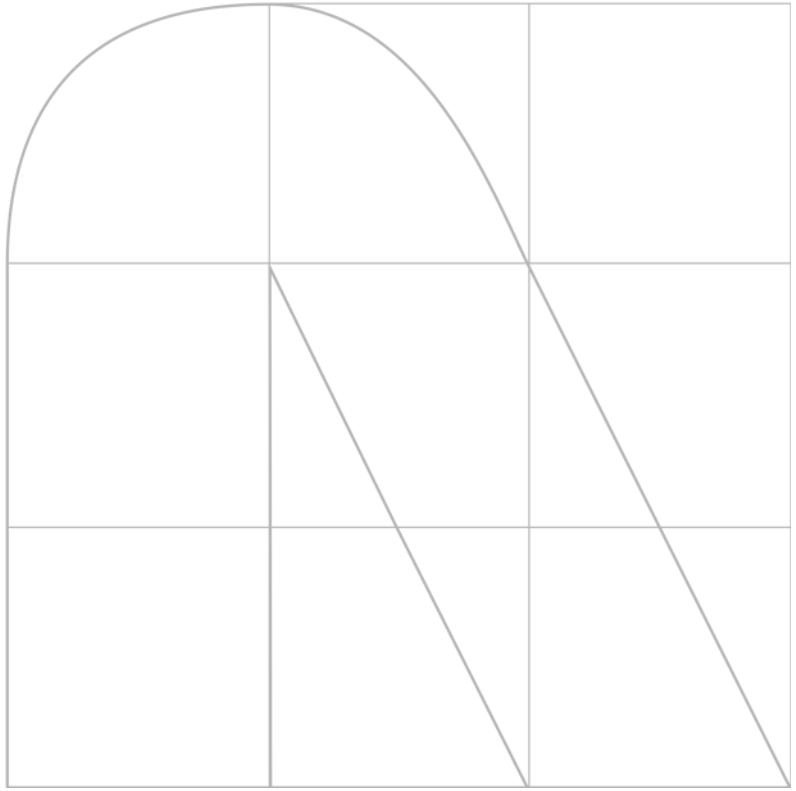
02　NTTデータが提供する「A-gate®」

03　「A-gate®」の強み

04　最後に

01

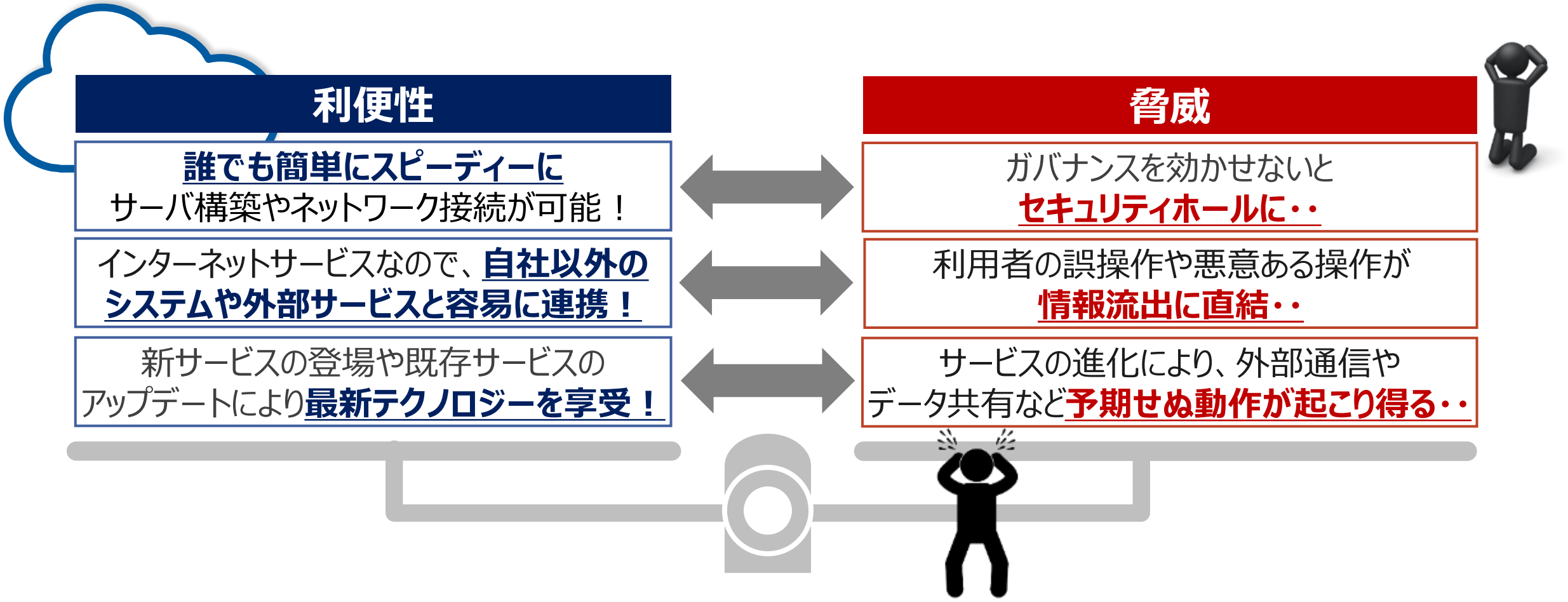
クラウドの脅威と向き合い方



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。

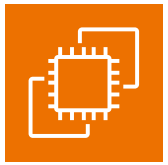
利便性	脅威
誰でも簡単にスピーディーに サーバ構築やネットワーク接続が可能！	ガバナンスを効かせないと **セキュリティホールに・・**
インターネットサービスなので、**自社以外のシステムや外部サービスと容易に連携！**	利用者の誤操作や悪意ある操作が **情報流出に直結・・**
新サービスの登場や既存サービスのアップデートにより**最新テクノロジーを享受！**	サービスの進化により、外部通信やデータ共有など**予期せぬ動作が起こり得る・・**



クラウドの利便性と脅威

便利な反面、情報流出につながる設定がたくさん存在します。

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
共有による情報流出リスク

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
共有による情報流出リスク

クラウドの情報流出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！

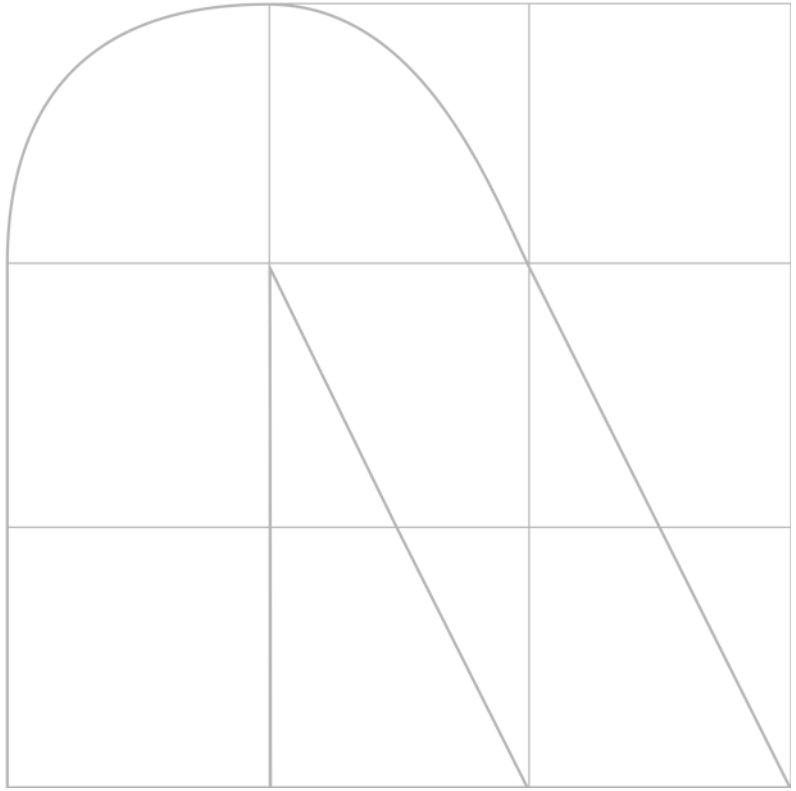
NTT DATA

「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随し、
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随し、
機能・仕組みを進化させていく

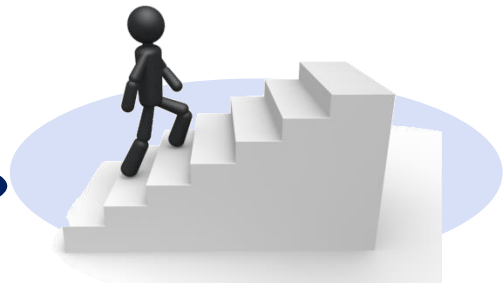
「A-gate®」がご提供するもの

クラウドセキュリティ基盤

違反検知・修復	情報流出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	クラウド上の情報流出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

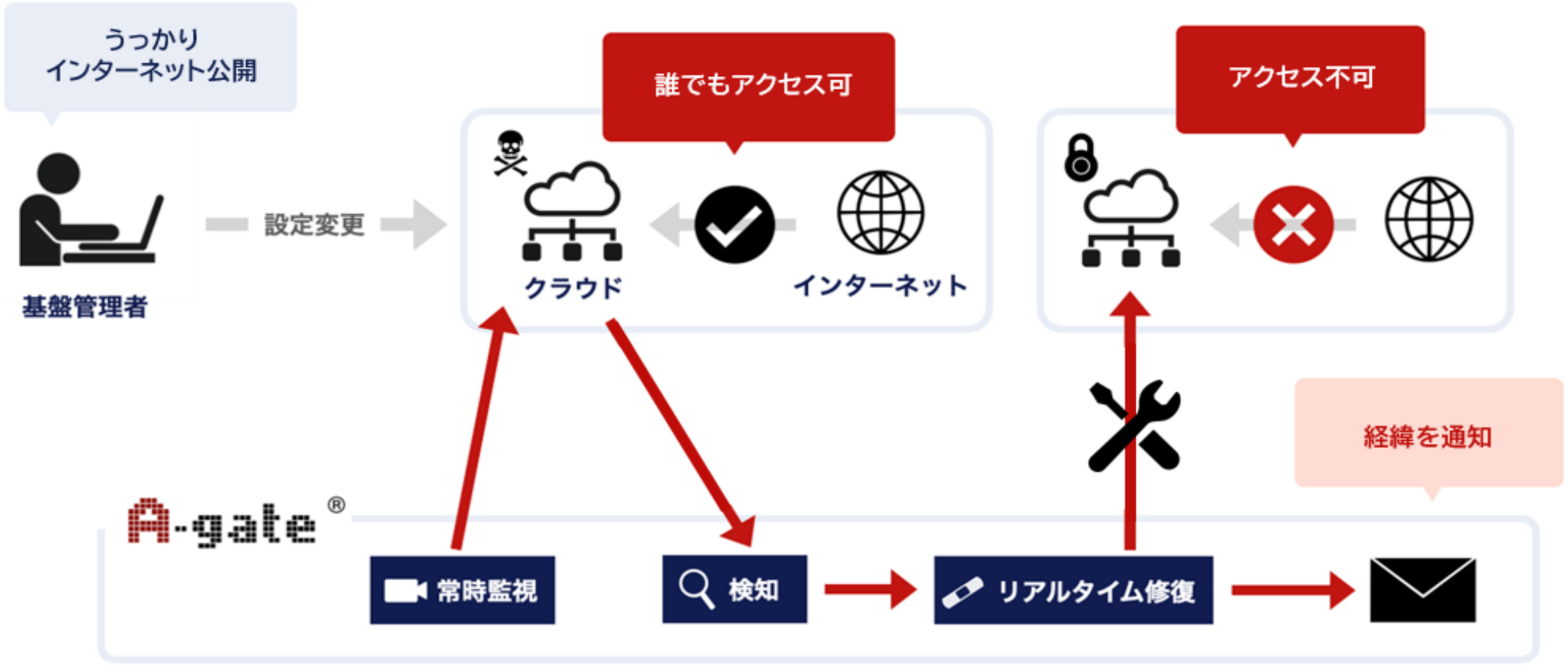
クラウドセキュリティ基盤



違反検知・修復	**情報流出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	クラウド上の情報流出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？

情報流出リスクのある設定を約2秒で検知＆修復します。



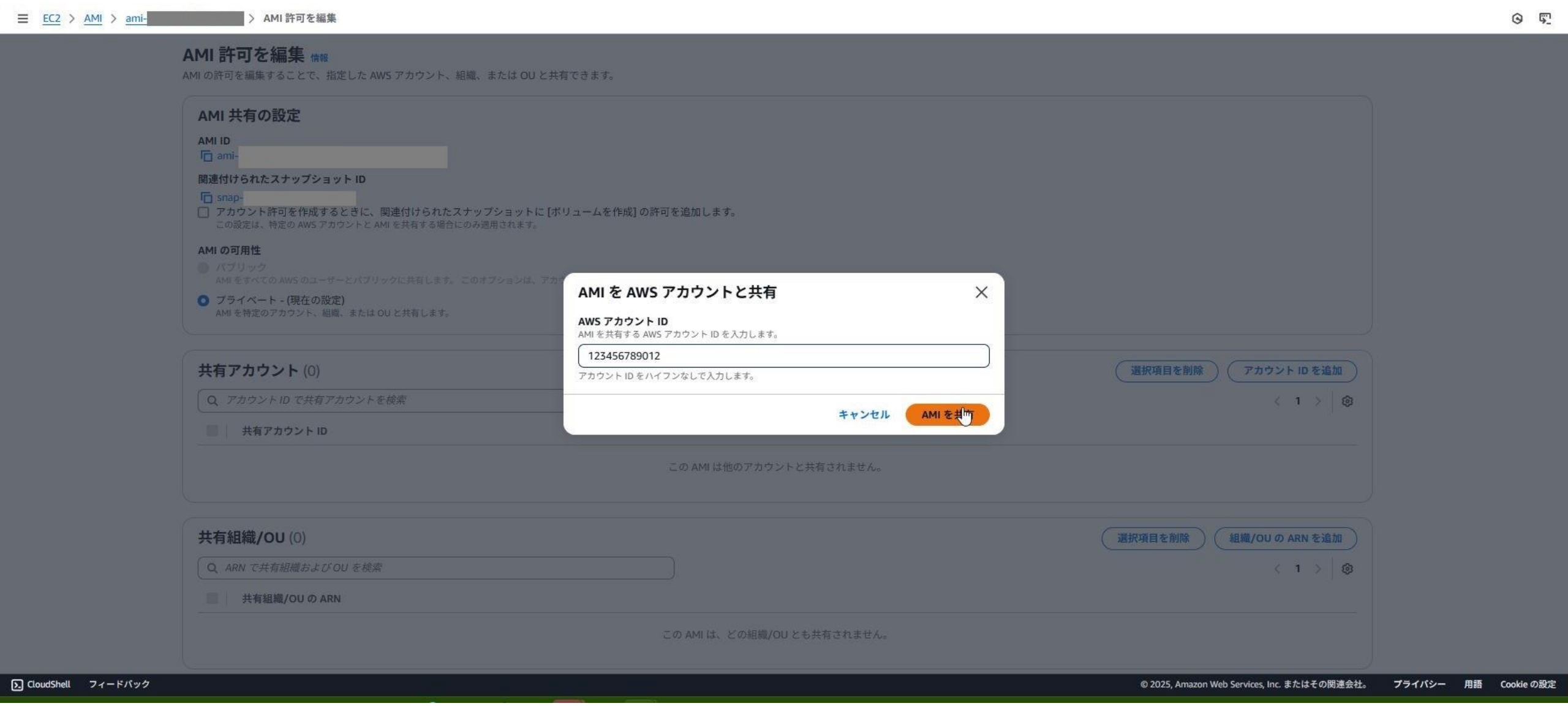
A-gate機能 を 継続してアップデート
～AWSを安全に利用するために、AWSの進化（新機能追加／更新）に追随～

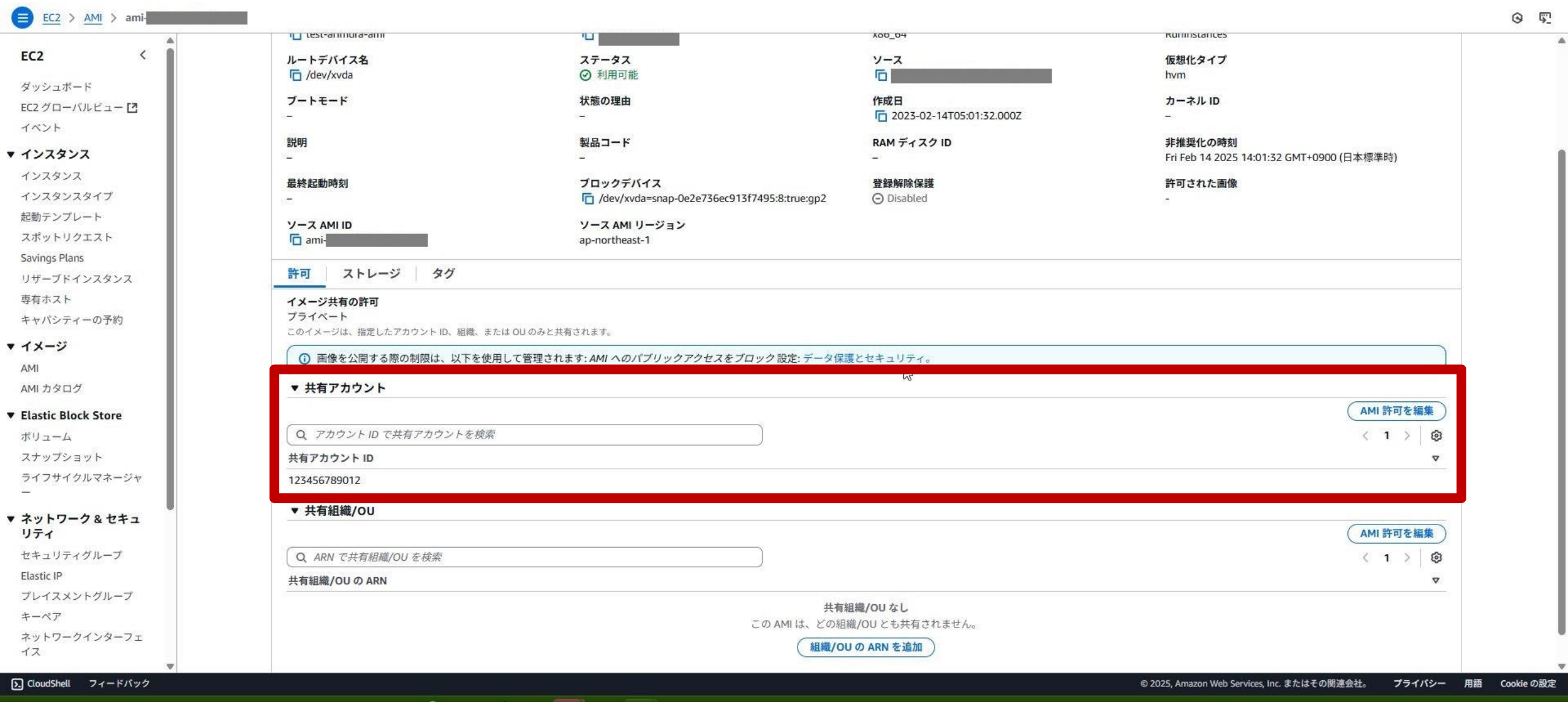
クラウドセキュリティ基盤 ：違反検知・修復 とは？

情報流出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）

大項目	小項目	違反の例	修復の例
通信経路	パブリック	・Internet Gatewayの設置	・Internet GatewayをAmazon VPCからデタッチ
	オンプレミス（自社以外）	・Vpn Gatewayの設置	・Vp Gate ayを Cからデタッチ
	他アカウント	・VPC Peeringの設置 ・Private Linkの共有設定 ・Gateway型のE point の設置 etc	・er の削 ・vat Linkの共有設定削除 ndpointの削除/Policyの修復
データ共有	パブリック公開	・Am azon のパブリック公開 ・非VPC上A azo Lambdaの設置 etc	・Amazon S3を非公開設定に変更 ・Amazon Lambdaの削除
	他アカウントへ共有	・ン ョンの共有 mazon EMRの共有 etc	・共有設定を削除
非暗号化	通信	・Amazon S3のhttp通信	・https通信に変更
	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）

NTT DATA

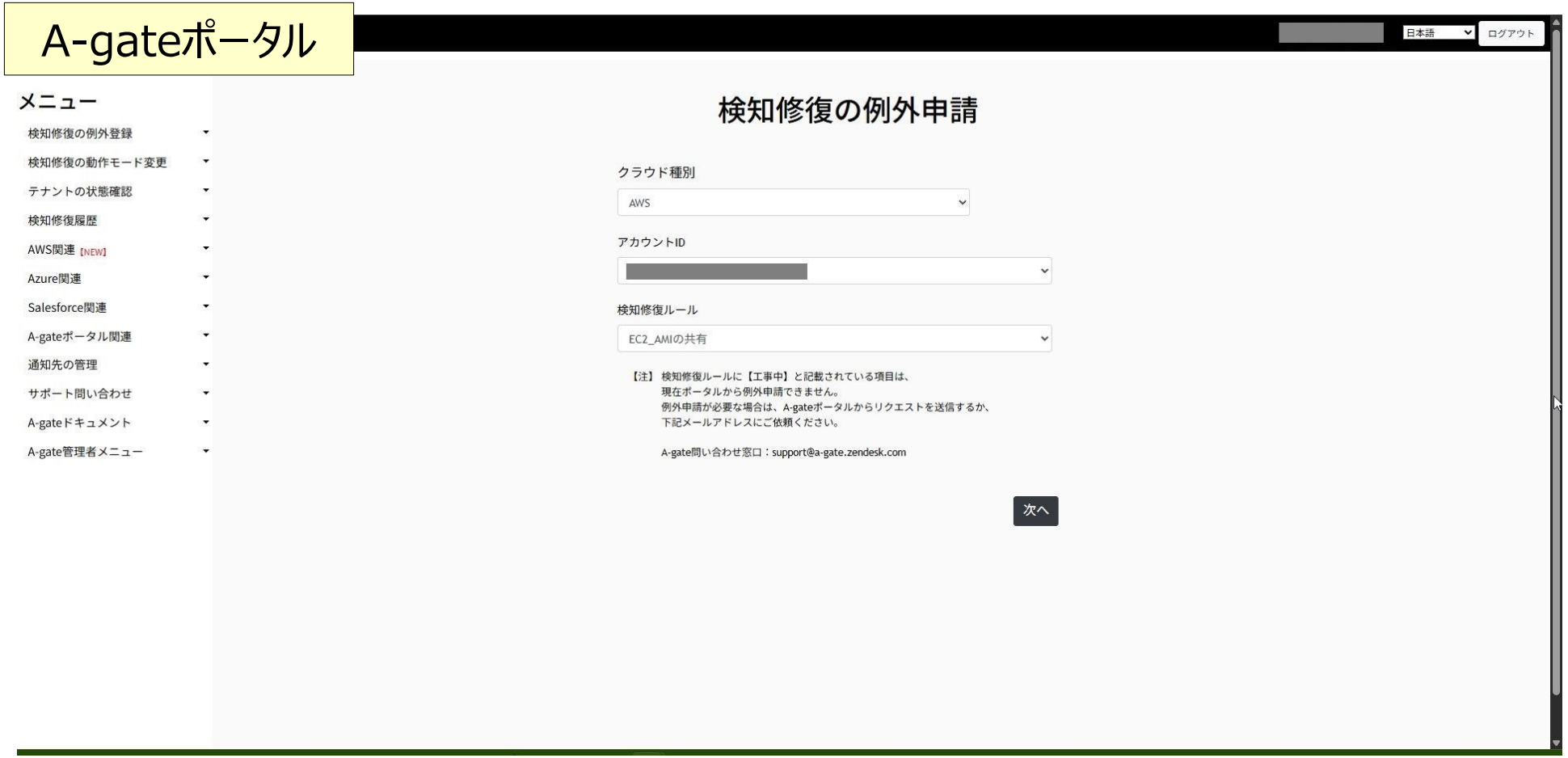




クラウドセキュリティ基盤：違反検知・修復　とは？（補足）

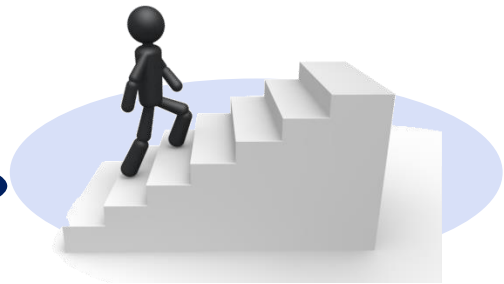
要件上リスク有設定を行う必要がある場合、
「例外登録」により違反検知・修復を回避することが可能です。

A-gateポータル



「A-gate®」がご提供するもの

クラウドセキュリティ基盤



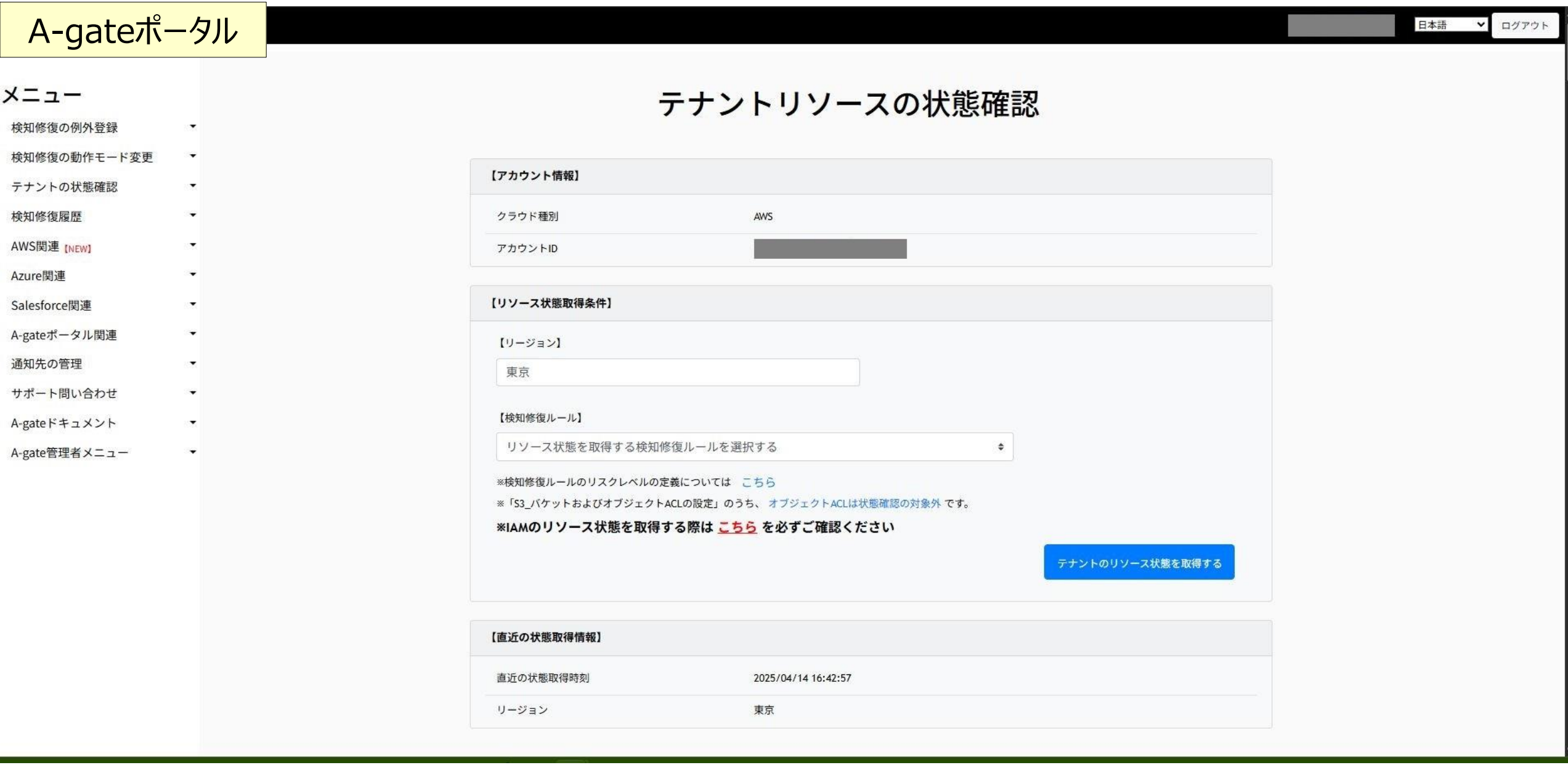
違反検知・修復	情報流出リスクのある設定を検知し、自動で安全な設定に戻す機能
静的スキャン	**クラウド上の情報流出リスクのある設定を洗い出し、一覧化する機能**
権限分掌	クラウドの操作権限を分掌するための権限セット

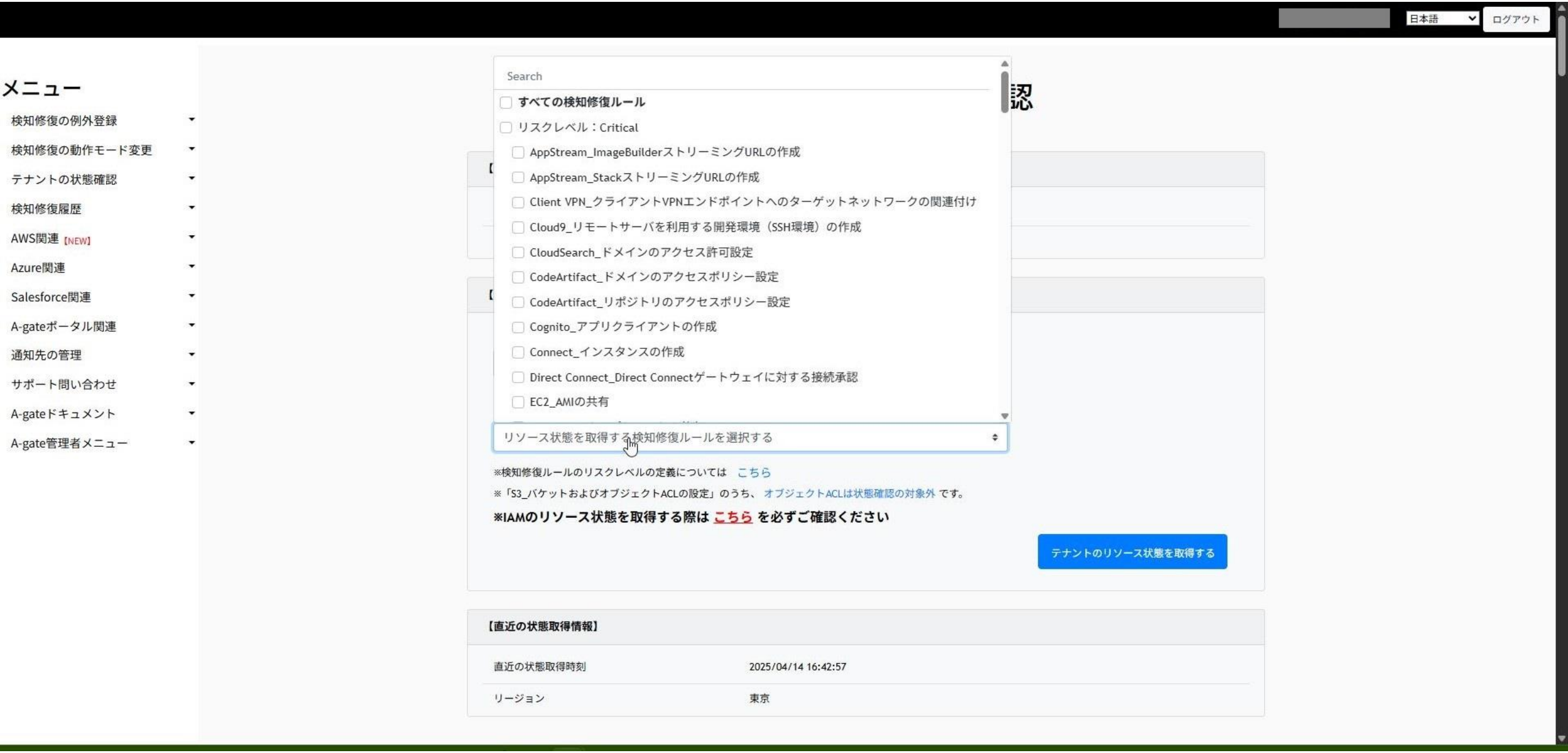
クラウドセキュリティ基盤　：静的スキャン　とは？

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
情報流出リスクの有無を
チェック可能！**

A-gateポータル





※「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。

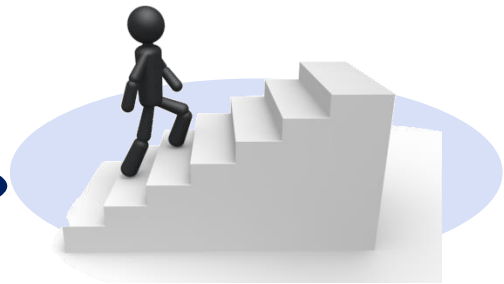
すべての行を展開する

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	対象なし	
▼	Critical	AppStream_Stackストリーミングの作成	対象なし	
▼	Critical	Connect_インスタンスの作成	すべて未登録	
▼	Critical	EC2_AMIの共有	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	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込み先設定	対象なし	
▼	Critical	IAM_OpenIDConnectIDプロバイダの設定	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	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	情報流出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	クラウド上の情報流出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**

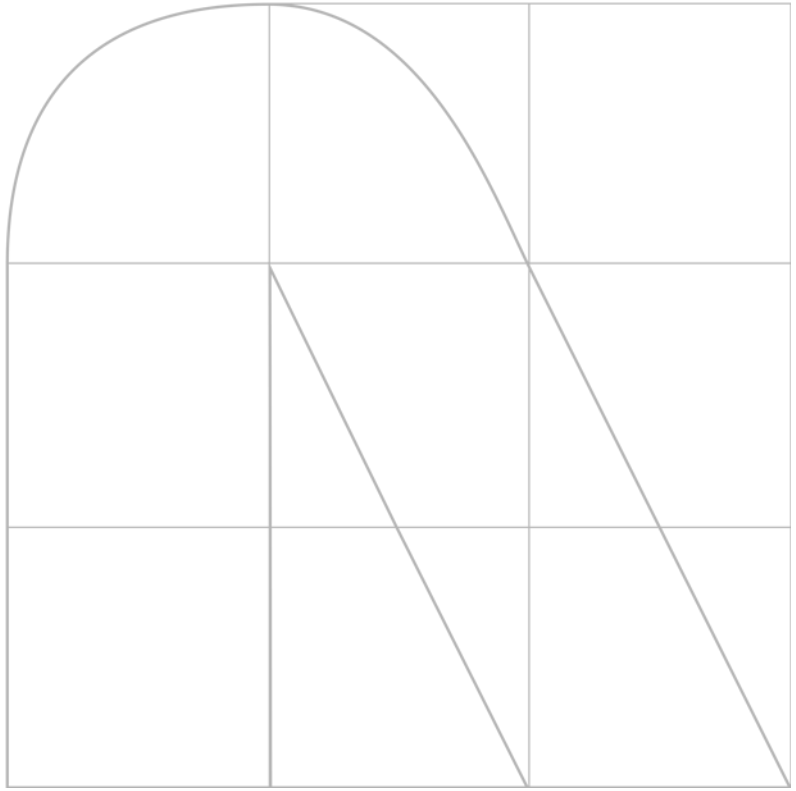
クラウドセキュリティ基盤 「権限分掌」とは？

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

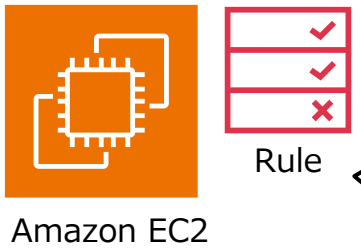
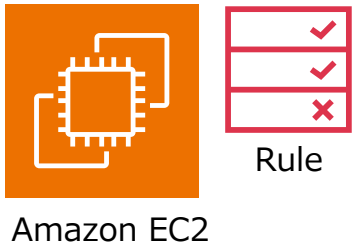
	A-gate®	他社CSPM
 Amazon S3  Permissions **任意のアカウント**からの読み取りを許可	✓	✓
 Amazon S3  Permissions **アカウントID「1111…」**からの読み取りを許可	✓	✗

NTT DATA

「A-gate®」の強み

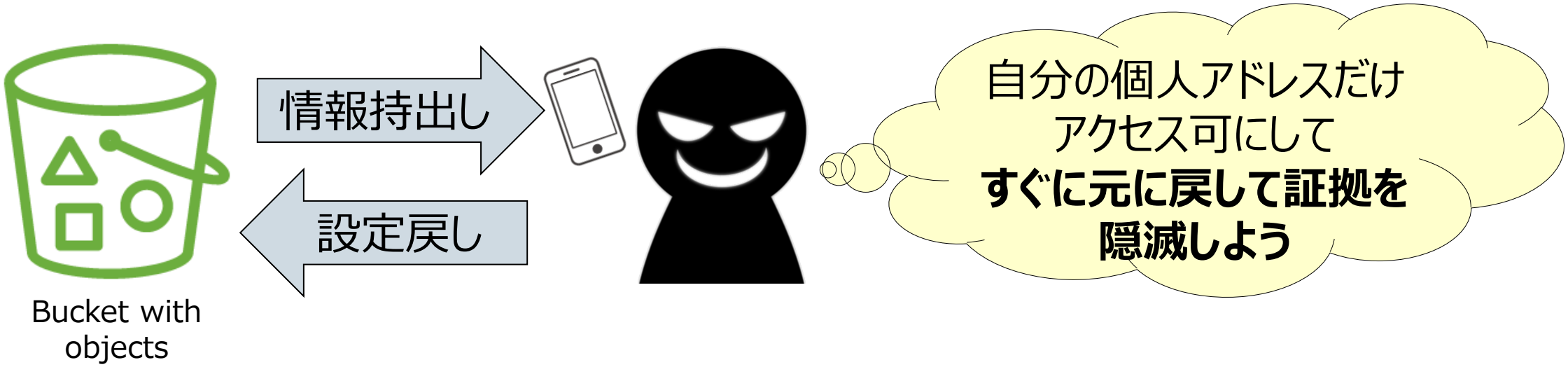
1 一般的なCSPM製品では見落とされる
限定的な共有／公開設定を検出可能

例）セキュリティグループの設定

	A-gate®	他社CSPM
 **全世界（0.0.0.0/0）**からのインバウンドアクセスを許可	✓	✓
 **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

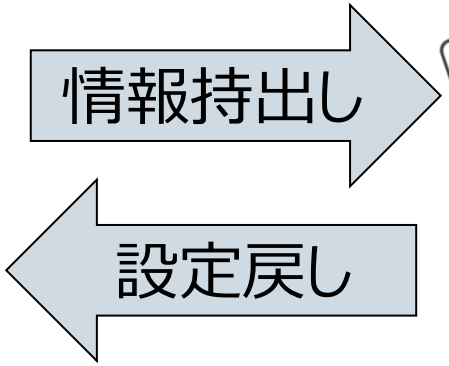


「A-gate®」の強み

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

Bucket with objects



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®	他社CSPM
100以上 **（2025/04現在）**	**30～50**

「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】EC2/VPC	ModifyImageAttribute	AMIの共有が可能
	ModifySnapshotAttribute	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

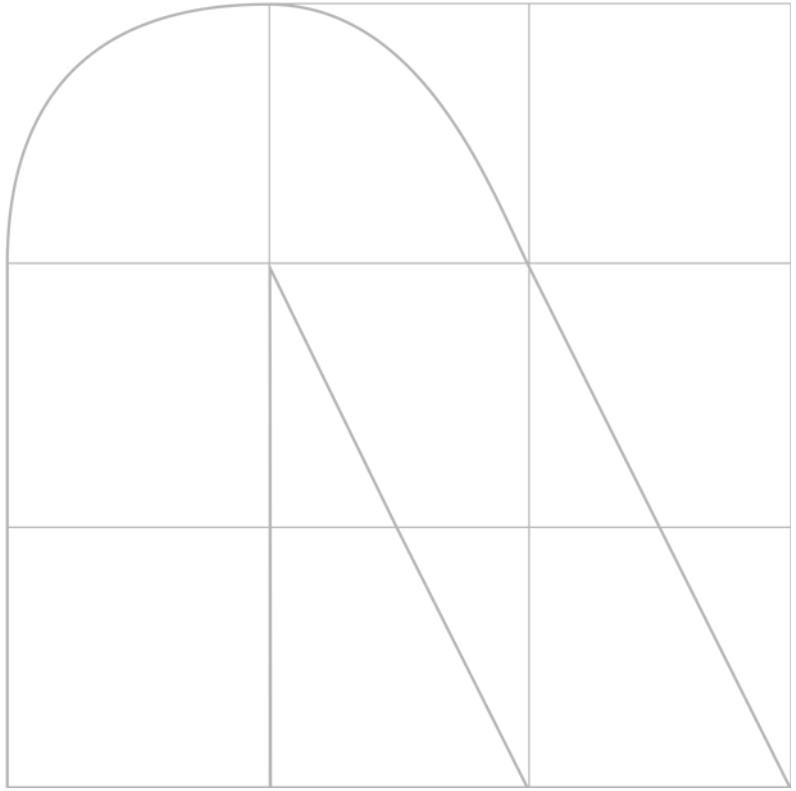
数多くのサービスに対応し、
APIレベルでの網羅性も担保

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！

04

最後に



まとめ

「A-gate®」は、ベンチマークにとらわれず
情報流出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、
情報流出に繋がる設定ミス・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！

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
オファリング統括部　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®

NTT DATA


NTT DATA