

まだ間に合う

企業が取り組むべきパブリッククラウドのセキュリティ対策



1. はじめに
2. パブリッククラウドを“安心・安全”に使うための“リスク対策”
(内部不正・設定ミスにどのように立ち向かうか)
3. A-gate[®]の機能・特長
4. A-gate[®]の実績・導入事例
5. A-gate[®]導入の流れ

はじめに



はじめに

DX(デジタルトランスフォーメーション)が進む中で、
鍵となるデジタル技術の活用を可能とし、さらにコスト削減にも寄与するパブリッククラウドを活用する企業が急増しています。

パブリッククラウドは、ビジネス面でもコスト面でもメリットをもたらす魅力あるサービスですが、
利便性が高い一方で、インターネット上に存在し、情報公開や他ユーザとの情報共有が簡単であるが故に、
操作・設定ミスが情報漏洩に直結してしまうというリスクがあります。

そのため、パブリッククラウドを安心・安全に使うためには、操作・設定ミスによる情報漏洩を防ぐための対策が必要です。
本ホワイトペーパーでは、操作・設定ミスによる情報漏洩を防ぐための対策について、「A-gate®」を例に用いながら解説します。

はじめに

パブリッククラウドの主なメリット

ビジネス上のメリットの一例

【柔軟性】

規模の拡大・縮小が可能なため
将来予測が不要

【データ連携】

社内外のシステムとの連携が
簡単

【アジリティ】

セルフサービスによる
リードタイムの減少

【技術革新】

先端技術と
日々の機能改善の享受

コスト上のメリットの一例

【更改・運用コスト】

ハード・OS更改と
運用からの解放

【センタコスト】

場所代・電気代などの
コスト削減

【リソース最適化】

ピークを基本とした
サイジングからの解放

【リソース最適化】

使わない時間は
停止して料金節約

はじめに

パブリッククラウドは、社内外のシステムとの連携がとても簡単であり、社外への情報公開や外部ユーザとの情報共有も簡単に行えます。
そのため社内でもさまざまなメンバーが情報共有を行うことがありますが、その簡単さゆえに起こりうるリスクも見落としてはいけません。

パブリッククラウド利用時のリスクが
特に高いとされるのは

- ・内部不正による情報漏洩
- ・うっかりミスによる情報漏洩

の2つで、社内での些細なミスから
思わぬ事故にもつながりかねません。

特にリスクが高い2点 設定ミスの発生率は 非常に高いとの報告あり		主なセキュリティリスク	クラウドではこうハイリスクになる
1	内部不正による情報漏洩		・簡単にインターネットや他アカウントへ情報漏洩可能
2	うっかりミスによる情報漏洩		・うっかりインターネットや他ユーザに情報を公開することがある ・クラウドの仕様変更を見落として情報が漏洩する
3	マルウェアに感染する	No.1,2を防ぐと、 自ずとNo.3~5も低リスクに	従来の感染経路に加えクラウド内のマーケットという経路が増える
4	OS・ソフトウェア等の脆弱性を突いた攻撃		インターネット非公開の場合は低リスクだったが、設定ミスでインターネットに繋がるため、従来よりハイリスクとなっている
5	インターネット上のサービスへの不正ログイン		クラウドの操作コンソールはインターネット上に公開されている

A-gate®で
対応！

パブリッククラウドを
“安心・安全”に使うための“リスク対策”

2

- パブリッククラウドにおけるセキュリティ脅威

パブリッククラウドが普及する一方で、利用者側の設定ミスや誤操作などを原因とする情報漏洩や不正アクセスが多発しています。例えば、顧客の個人情報が漏洩すると多大な被害を受けます。

また、パブリッククラウドの導入を決意してすぐにクラウド上に個別のシステムを作り始めることは、設定・操作に関するセキュリティポリシーが未適用の状態を利用することに繋がり、とても危険です。こうしたリスクを抑えるために、セキュリティを維持する万全の仕組みが必要です。



- パブリッククラウドにおけるセキュリティ脅威

パブリッククラウド利用におけるセキュリティ脅威として、代表的なものは以下のとおりです。
パブリッククラウドの各種サービスには情報漏洩に直結する設定(通信経路、データ共有、暗号化)が存在しますが、
これらを適切に設定・維持する必要があります。

また、パブリッククラウド自体が年間1,000回以上のスピードでアップデートされるため、これらのアップデートに追隨していく必要があります。

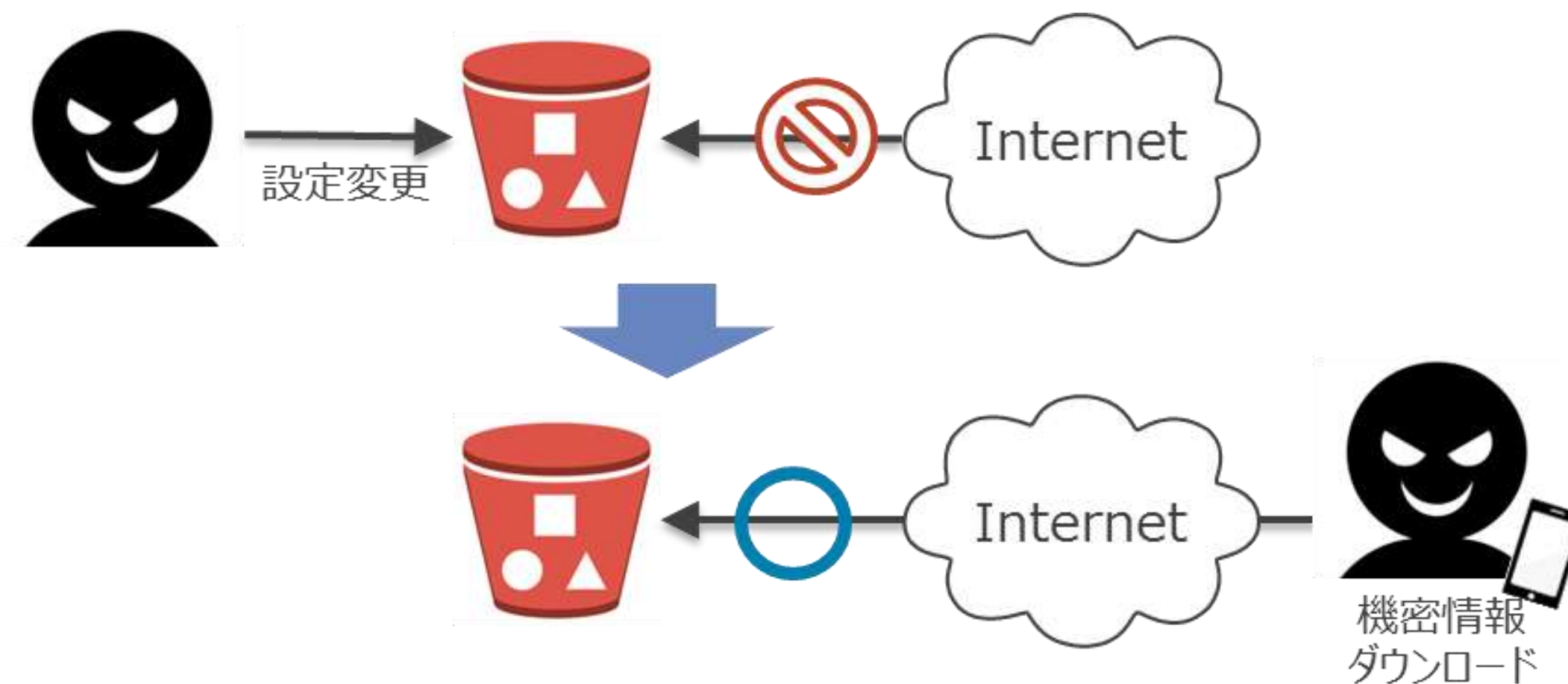
セキュリティ脅威	発生事象(例)	要因
通信経路	・外部アカウントとの接続によるデータ持ち出し ・外部からのアクセスによる情報漏洩	・利用者による故意、設定ミス ・悪意ある利用者の不正アクセス
データ共有	・外部アカウントとのデータ共有による情報漏洩 ・パブリック公開設定による情報漏洩	・アカウント共有の不適切な設定 ・パブリック公開の不適切な設定
暗号化	・リソース不正アクセスによる情報漏洩 ・通信の盗聴による情報漏洩	・クラウドレイヤの非暗号化
新サービス／機能追加	・パブリッククラウドの進化(新規サービスのリリース、既存サービスの機能追加)に伴う新たなセキュリティ脅威の自然発生による情報漏洩	・新サービスにおけるリスク未検証または、パブリッククラウドの進化への対策が未考慮

- セキュリティ脅威(内部不正・設定ミス)への対策

利用者の故意またはうっかりミスによって生じる情報漏洩は、企業にとって致命的なリスクになることから、パブリッククラウドの各種サービスにおける設定を、適切に設定・維持し続けることが必要です。

内部不正や設定ミスへの対策

これまで説明してきたインターネット公開・他アカウントとの不正な共有/接続、個人アカウントへの持ち出しは企業にとって致命的なリスクとなる



- セキュリティ脅威(内部不正・設定ミス)への対策

具体的には、パブリッククラウド上での他ユーザーとのデータ共有やインターネット公開機能、外部ネットワーク接続の機能を洗い出し、それらがしっかり制御されていることを継続的に確認する必要があります。

①共有／公開機能の特定

パブリッククラウドの各サービス単位(EC2／S3…)で、共有・公開機能の設定可能箇所を特定し続ける
→サービス自体の追加や機能追加にも対応し続ける

②構成変更時のチェック

作業時のミスへの対応として、
構成変更後に①でチェックした共有・公開設定がきちんと閉じられているかチェックする

③ユーザー利用時のチェック

特に大変！

内部不正への対応として、クラウドユーザー利用後に①でチェックした共有・公開設定がきちんと閉じられているか、また開けられた形跡がないかチェックする。(自動チェック機能がなければ漏洩後の発覚となってしまう)
→無数にあるクラウドの各サービスに精通し、かつ商用環境を操作するたびに全てのログを調査しなければならない

- セキュリティ脅威(内部不正・設定ミス)への対策の難しさ

しかし、①～③を人の力で対応しようとするとう困難を極めます。

①共有／公開機能の特定

パブリッククラウドの各サービス単位(EC2／S3…)で、共有・公開機能の設定可能箇所を特定し続ける
→パブリッククラウドは年間1,000件以上のアップデート(新規サービスのリリース、既存サービスの機能追加)があります。
膨大なアップデートの中から、自社で利用しているサービスに関するアップデートを抽出して内容を検証し、
利用中であるクラウド環境への影響を特定し続けなければいけません。

②構成変更時のチェック

作業時のミスへの対応として、
構成変更後に①でチェックした共有・公開設定がきちんと閉じられているかチェックする

③ユーザー利用時のチェック

特に大変！

内部不正への対応として、クラウドユーザー利用後に①でチェックした共有・公開設定がきちんと閉じられているか、また開けられた形跡がないかチェックする。
→悪意をもってクラウドの設定を変更し情報を持ち出す場合においては、情報の持ち出し後に設定を戻すことが想定されます。
これを捕捉するためには、無数にあるクラウドの各サービスに精通し、かつ商用環境を操作するたびにすべてのログを調査しなければなりません。(実質、機械的な仕組みがなければ漏洩後の発覚となってしまう)

⇒ ①～③をカバーする「A-gate®」を利用することで、万全な対策が可能となります！

A-gate®の機能・特長

3

- A-gate®とは

株式会社NTTデータが提供するクラウドセキュリティサービス「A-gate®」は、パブリッククラウド上で「情報漏洩リスクのある設定」が行われると即時に検知・修復し、クラウドを常に安全な状態に保ちます。

A-gate®は一貫したサポート体制でパブリッククラウド活用を支援します！
主な提供サービスは以下のとおりです。

①クラウドセキュリティ基盤



- ・権限分掌
- ・違反検知/修復

ポリシー違反検知・修復機能により、
情報漏洩リスクをシャットアウト

②マネージドCCoE



- ・新サービス研究
- ・アップデート

クラウドの進化へ追随し、
クラウドセキュリティ基盤を継続アップデート

スタートアップコンサル (※オプション)



- ・クラウド知見提供
- ・ガバナンス確立支援

クラウド活用体制を整える
コンサルティングサービス

- A-gate®とは - セキュアなクラウド環境の提供

A-gate®では、パブリッククラウドのセキュアな活用を実現し、クラウドの情報漏洩リスクから守るための機能・仕組みを提供します。

①クラウドセキュリティ基盤

→クラウドを安全に利用するための機能(権限分掌、ポリシー違反検知・修復)を提供します。

権限分掌

クラウド上の操作・設定に関する各種権限を役割に応じて適切に割り当て、権限セットとして提供
(システム開発におけるメンバーの役割に合わせて、クラウド権限のプリセットを提供します)

ポリシー違反検知・修復機能

クラウド上で情報漏洩リスクのある設定変更が行われた場合、自動的に修復
(セキュリティポリシー違反の設定をリアルタイムで監視し、検知時に自動修復する仕組みを提供します)

②マネージドCCoE

パブリッククラウドの進化に追随するため新サービスの検証を実施し、クラウドセキュリティ基盤を随時アップデートします。

- A-gate®とは - セキュアなクラウド環境の提供

権限分掌について

パブリッククラウドを安全に利用する上で必要と考えられる「権限セット」をA-gate®が提供し、システム開発における各役割に応じて「役割の遂行に必要な最小限のクラウド権限を付与した環境」を実現します。

役割の定義



クラウドサービスの各操作に対するリスク種別の定義

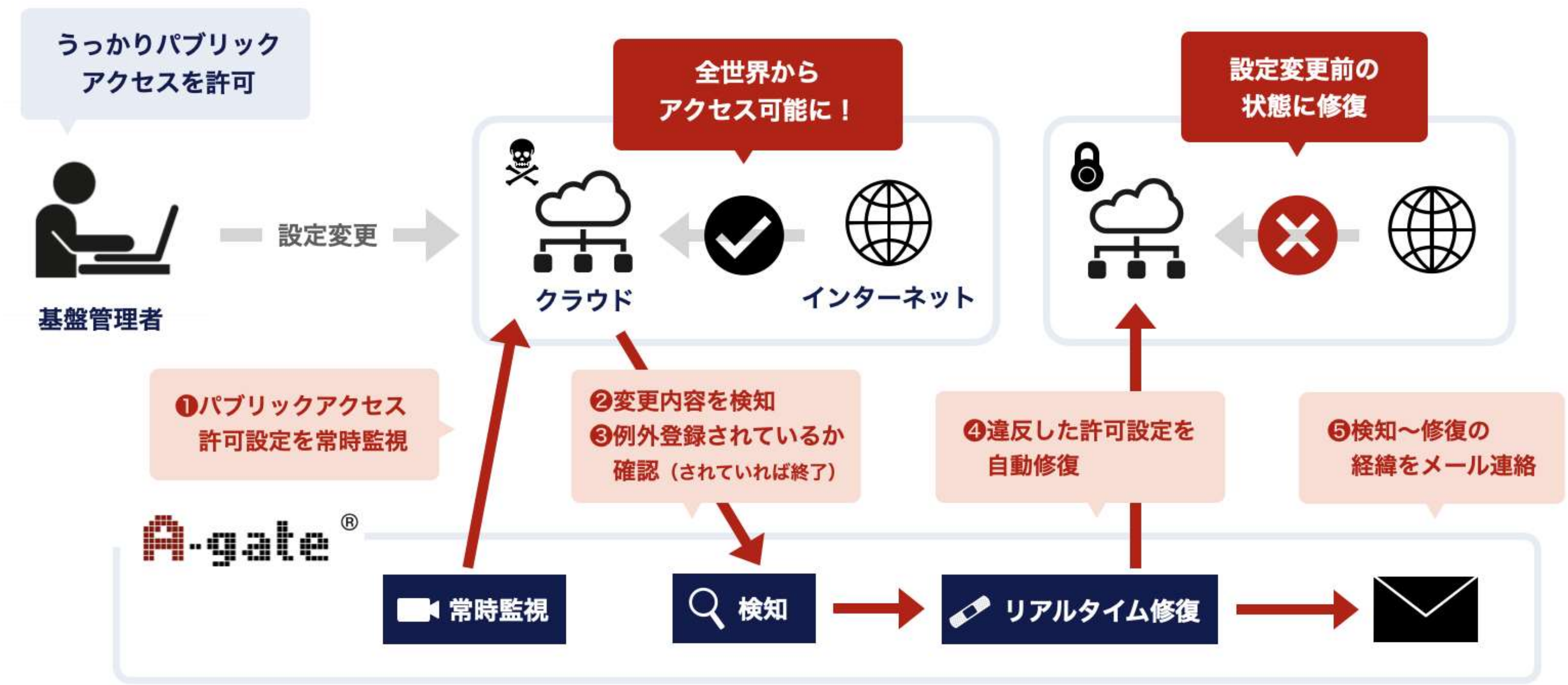
- ・ クラウドのユーザの作成・削除
- ・ クラウドのユーザへの**権限の付与・剥奪**
- ・ クラウド上の閉域NWと**外部NWの接続確立**
- ・ クラウド上の閉域NWと**オンプレミスの接続確立**
- ・ クラウド上への個別システムの構築(**他人へのデータ共有**などの操作権限あり)

権限セットを利用することでシステム開発のメンバーが役割に応じてそれぞれ実行してよい設定・操作を実施することとなり、適切な役割のメンバーのみが、**情報漏洩に直結する設定・操作**ができる状態にします。

- A-gate®とは - セキュアなクラウド環境の提供

ポリシー違反検知・
修復機能について

A-gate®では情報漏洩に直結する設定・操作(通信経路やデータ共有など)を「ポリシー違反」と定義しており、該当動作が行われていないかをリアルタイムで常時監視しています。
ポリシー違反に該当する操作や設定変更が行われた場合は、直ちに直前の状態に修復・削除し、クラウドを安全な状態に保ちます。



ポリシー違反の例

大項目	小項目
通信経路	パブリック
	オンプレミス (自社以外)
	他アカウント
データ共有	パブリック公開
	他アカウントへ共有
非暗号化	通信
	データ

必要となる操作については
A-gate提供の承認ワークフローで
「例外登録」を実施いただく事で
自動修復の対象外とできます。

- A-gate®とは - セキュアなクラウド環境の提供

ポリシー違反検知・
修復機能について

必要な通信経路やデータ共有の設定・操作を行う場合は、A-gate®のポータルサイトのワークフロー機能を用いて「例外登録」を実施することにより、該当リソースの修復処理を無効化することができます。
「担当者による申請」と「管理者の承認」のプロセスを経ることで、セキュリティ・ガバナンスを効かせた運用を実現します。

担当者により申請

例外申請の詳細入力

1. 対象アカウントID

s-nds2-pr-0000 (00D5j00000B8xyg)

2. 検知修復ルール

SFDCRule_0001_ファイルのインターネット公開リンク作成

3. 詳細パラメータ入力

3-1. ファイル名（タイトル） / ファイルサイズ

- 公開リンクの作成を許可するファイルのタイトル（拡張子無し）、ファイルサイズを指定してください。
- ファイルサイズは、アップロード元の端末で確認いただけるこちらのサイズを、カンマ無しで指定してください。
（ファイルサイズの確認方法は、[こちら](#)をご参照ください。）

※ 既存登録されている例外情報をマイナスボタンで非表示として登録を行うと、例外情報が削除されます。

インターネットに公開できるファイル.txt

5

-

+

4. 申請理由 【必須】

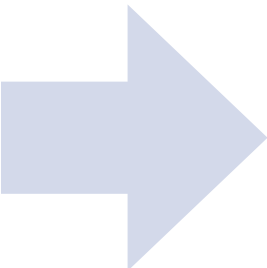
NextGenセミナーのため

5. コメント欄 （任意）

コメントを入力

戻る

確認



管理者の承認

申請の詳細

【申請対象のアカウント情報】

アカウントID	s-nds2-pr-0000 (00D5j00000B8xyg)
申請者	Toshiki.Ito@nttdata.com

【申請内容詳細】

ルール名	SFDCRule_0001_ファイルのインターネット公開リンク作成	
	新規追加分	削除分
ファイル名（タイトル） / ファイルサイズ	インターネットに公開できるファイル.txt, 5	dummy, 5

【申請理由】

申請理由	NextGenセミナーのため
コメント	(コメントなし)

【A-gateからの注意喚起 例外登録時に生じるリスク】

当該ルールが対応しているリスク	公開リンクを作成すると、該当ファイルをダウンロード可能なURLが発行される。 当該URLはインターネット上の誰でもアクセス可能であり、URL流出による情報漏洩リスクがある。 また、URLは一定の「ターン」で生成されるため、URL押定による情報漏洩リスクもある。
-----------------	--

コメント 【0/50】（承認または却下理由をご記入ください。）

コメントを入力

名前 【0/50】 名前を入力

確認 「確認しました」と入力

却下

承認

承認一覧へ戻る

- A-gate®とは - セキュアなクラウド環境の提供

ポリシー違反検知・修復機能について

以下はAWSにおける違反検知・修復対象の一例です。2023年2月時点で約130のルールがあります。

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	・S3のパブリック公開 ・非VPC型Lambdaの設置 etc	・S3を非公開設定に変更 ・Lambdaの削除
	他アカウントへ共有	・マシンイメージの共有 ・EMRの共有 etc	・共有設定を削除
非暗号化	通信	・S3のhttp通信	・https通信に変更
	データ	・S3、EMR、RDS・・・etc	・暗号化(EBSのブートディスクは例外)

- A-gate[®]とは - セキュアなクラウド環境の提供

ポリシー違反検知・修復機能について

違反検知・修復のイメージ

例:AWS上でインターネットゲートウェイを
アタッチすると情報漏洩リスクがあるが、約2秒で修復

The image displays three sequential screenshots of the AWS Management Console's 'Internet Gateways' page, illustrating a security incident and its resolution.

Top Screenshot: Shows the 'Internet Gateways (1/3)' page. The 'tx-policy-test' gateway is in an 'Attached' state, connected to VPC 'vpc-02999bd90c49ce845'. An 'アクション' (Action) dropdown menu is open, showing options like 'VPC にアタッチ' (Attach to VPC) and 'インターネットゲートウェイの削除' (Delete Internet Gateway).

Middle Screenshot: Shows the same page after the 'tx-policy-test' gateway has been detached. The status is 'Detached'. A red box highlights the 'Detached' status, and a red callout bubble labeled 'ハイリスク' (High Risk) points to it, indicating the security vulnerability.

Bottom Screenshot: Shows the same page after a repair action. The 'tx-policy-test' gateway remains 'Detached', but a blue callout bubble labeled 'ノーリスク' (No Risk) points to the status, indicating that the security risk has been mitigated by the A-gate system.

- A-gate[®]とは - セキュアなクラウド環境の提供

マネージドCCoEについて

パブリッククラウド自体が年間1,000回以上のスピードでアップデートされるため、これらのアップデートに追隨していく必要があります。
A-gate[®]では、パブリッククラウドの新サービスの検証やクラウドセキュリティ基盤へのアップデートを行う「マネージドCCoE」を実施。

パブリッククラウドが進化(新規サービスのリリース、既存サービスの機能追加)した際には安全に利用する方法の検証を行い、検証結果に応じてクラウドセキュリティ基盤を随時アップデートし、安全な状態を保ちます。

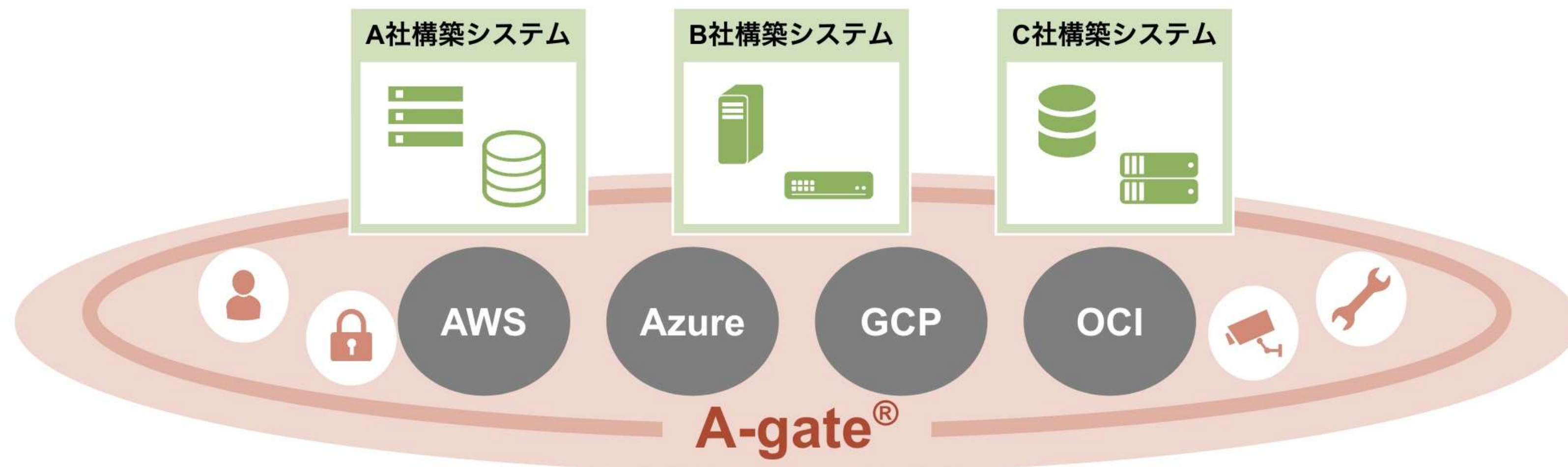
マネージドCCoE	新サービスの検証と審査	新機能や新サービスを安全に利用する方法の検証と、 検証結果を審査するスキーム
	セキュリティ基盤の アップデート	検証結果に応じてセキュリティ基盤を随時アップデート

- A-gate®とは - 全体像

A-gate®はマルチクラウド対応 & ベンダーフリー

A-gate®は主要なパブリッククラウドに対応しており、各クラウドの特性に応じたクラウドセキュリティ基盤(権限分掌・検知修復)をご利用いただけます。
A-gate®上でのテナントシステムについては、NTTデータ以外のベンダーでも開発できます。
例えば、自社で所有している現行システムをパブリッククラウドへ移行する際に、現行ベンダーにてご対応いただけます。

実際にA-gate®をご利用中のお客様では、内製化による開発や案件に応じた開発ベンダーの採用などを実現しています。



- セキュリティ脅威対策は、A-gate®で！

パブリッククラウド利用におけるセキュリティ脅威を、A-gate®はカバーします。

セキュリティ脅威	発生事象(例)	要因	
通信経路	- 外部アカウントとの接続によるデータ持ち出し - 外部からのアクセスによる情報漏洩	- 利用者による故意、設定ミス - 悪意ある利用者の不正アクセス	クラウドセキュリティ 基盤がカバー
データ共有	- 外部アカウントとのデータ共有による情報漏洩 - パブリック公開設定による情報漏洩	- アカウント共有の不適切な設定 - パブリック公開の不適切な設定	
暗号化	- リソース不正アクセスによる情報漏洩 - 通信の盗聴による情報漏洩	クラウドレイヤの非暗号化	
新サービス／ 機能追加	クラウドサービスの進化(新規サービスのリリース、既存サービスの機能追加)に伴う新たなセキュリティ脅威の自然発生による情報漏洩	新サービスにおけるリスク未検証または、クラウドサービスの進化への対策が未考慮	マネージドCCoEがカバー

- A-gate®ならではの強み - まとめ

A-gate®だからこそ実現できる強みをご紹介します。

①強固なセキュリティ基盤を実現
(内部不正や設定ミスの防止)

人が管理するのではなく「ツールが自動化する」ので格段にミスが減らせます

②マネージドCCoEによる研究とアップデート

クラウドの新機能や新サービスを随時検証し、
クラウドセキュリティ基盤をアップデートし続けます。

③マルチクラウド対応

主要なメガクラウド(AWS、Azure、GCP、OCI)に対応！
①・②を各クラウドそれぞれの特性・仕様に合わせて対応

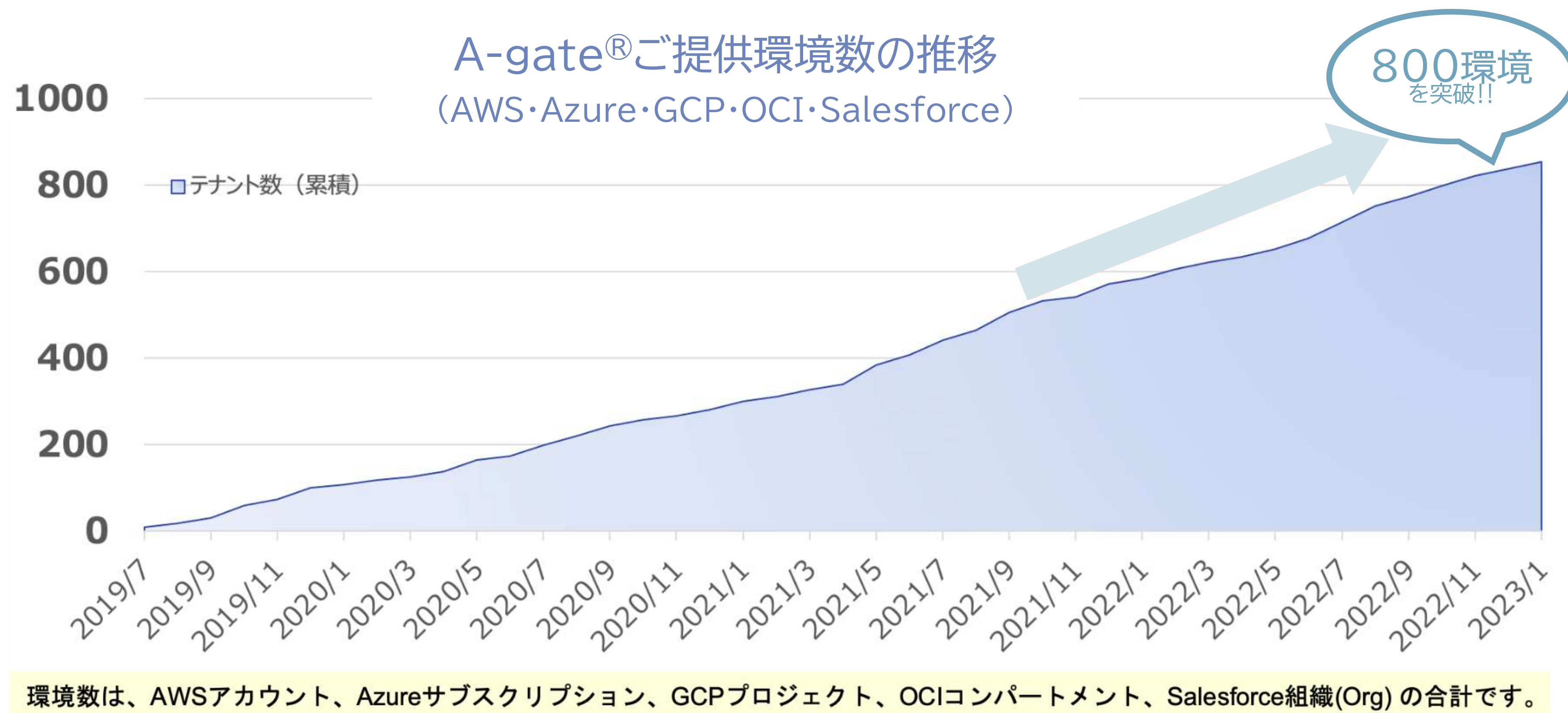
パブリッククラウドの利用規模を問わず、スピーディーかつ安心・安全にパブリッククラウドが活用できるようになります。

A-gate®の実績・導入事例

4

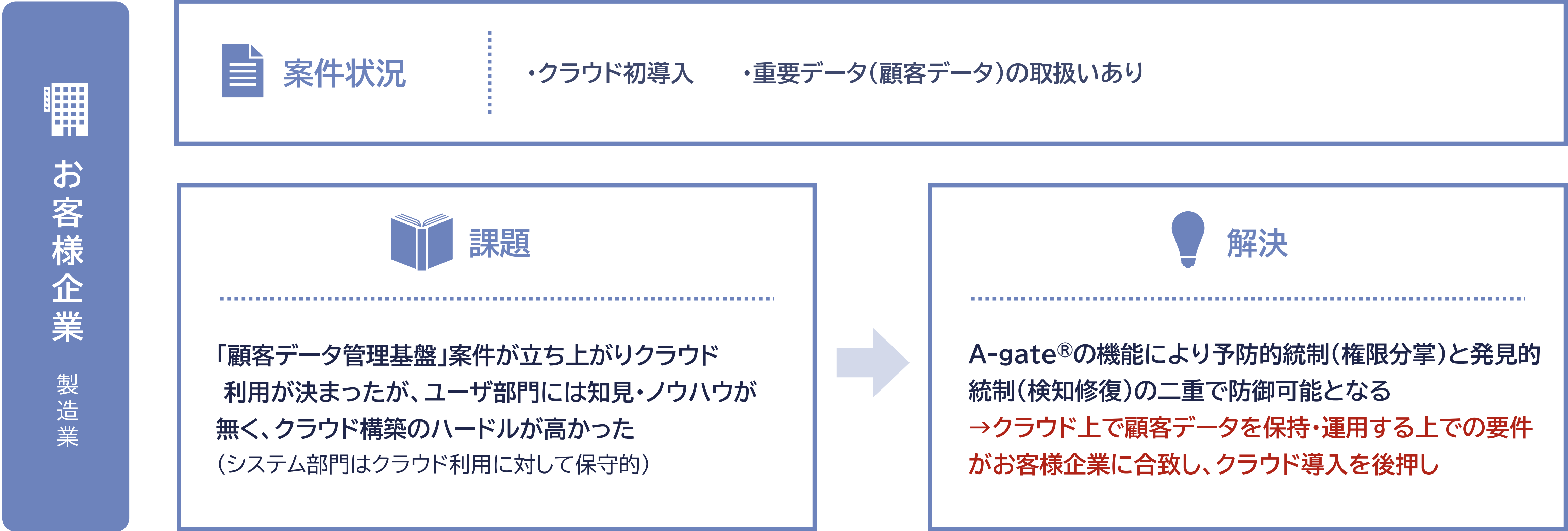
- A-gate®の導入実績

セキュリティに厳格な金融機関向けにサービスを提供開始した「A-gate®」ですが、多種多様な業界のお客様にご評価いただき、利用環境数は800を超えました。(2023年1月時点)



- A-gate®の導入事例 ①

パブリッククラウド利用に慎重だったお客様に対する導入サポート



- A-gate®の導入事例 ②

クラウド上のDX基盤を全社展開する上でのセキュリティ強化を実現



お客様企業

製造業



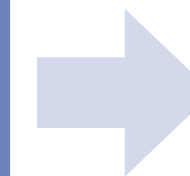
案件状況

- ・クラウド導入済
- ・部門横断のDX案件が発足



課題

- ・セキュリティ基盤を構築する枠組みはできていたものの、全社展開するための体制づくりが間に合っていなかった
- ・「DX基盤構築」の案件主導でクラウドを活用するにあたり、自社のグループ本体の企業ですら活用できていなかった
- ・クラウドを各部署でバラバラに利用することで縦割り状態になっており、ガバナンスを効かせることが困難となっていた



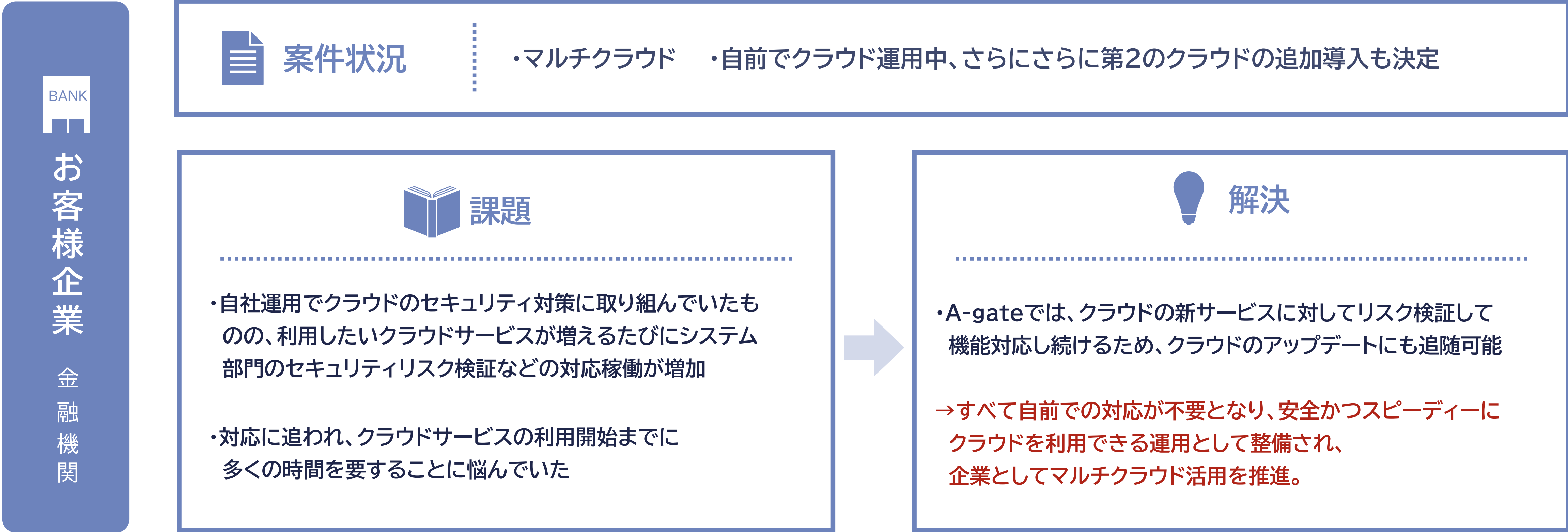
解決

A-gate推奨の、クラウド利用における社内運用ルールを全社に展開

→案件ごとにセキュリティのルールがバラつくことなく全社でセキュリティを強化し、統制を効かせた上でクラウド活用できるように

- A-gate®の導入事例 ③

クラウド利用拡大・アップデートにおけるセキュリティリスク検証の負荷を軽減



A-gate®導入の流れ

5

A-gate®導入の流れ

ステップ1

お問い合わせ(お客様)

→A-gate公式サイト経由にてお申し込みください。(ご検討のサービスをお知らせください)

ステップ2

A-gate概要紹介(お客様・A-gate)

→お打ち合わせにて、A-gateの概要説明をさせていただきます。(ご検討のサービスに関する機能概要、料金、申込方法等をご説明します)

ステップ3

お申し込み(お客様)

→ご利用開始の1ヶ月前が目安となります

ステップ4

ご契約(お客様・A-gate)

ステップ5

ご提供準備(A-gate)

→お客様が既にご利用中のクラウド環境に対して導入する場合、お客様環境の事前確認(&必要に応じてお客様側での事前作業)を実施します。(新規利用の場合は不要です)
※A-gateの場合は、全利用者が共通仕様でご利用いただくサービスとなるため、ご利用開始にあたって、お客様との要件定義・個別カスタマイズ検討等はございません。

ステップ6

ご利用開始

お問い合わせ

パブリッククラウドを安心・安全に利用するにあたり欠かせないセキュリティ対策。
クラウドを活用しながら自社のセキュリティをより強化したい方、自社のセキュリティ対策に不安を感じている方は、
ぜひクラウドセキュリティサービス「A-gate®」の導入をご検討ください。
公式サイトのお問い合わせボタンより、お気軽にお問い合わせください。

A-gate®に関するお問い合わせ



A-gate

「A-gate」は、株式会社NTTデータの登録商標です。

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

[公式サイトリンク](#)

お問い合わせ
ボタン
から！

A-gate(IaaS/PaaS)公式サイト



クラウドのリスクとその対策方法を
マンガでわかりやすくご紹介！

<https://agate.nttdata.com/>

A-gate(Salesforce)公式サイト



Salesforceの潜在リスクとその対策方法を
マンガでわかりやすくご紹介！

<https://agate.nttdata.com/salesforce/>

The image features a low-angle, upward-looking perspective of a modern city skyline. Two prominent skyscrapers with curved, glass-and-steel facades dominate the center. The sky is a clear, deep blue. In the foreground, the tops of trees and streetlights are visible, suggesting an urban environment. The overall tone is professional and tech-oriented.

NTT Data