プライベートなAzure 環境で通信周りをあれこれ対応したお話

2024/06/22 第3回 Azure Travelers 勉強会 山形の旅

Kazuki Yamabe

アジェンダ

- 自己紹介
- サードパーティー製品を利用したAzure の閉塞環境
- 実際にあった問い合わせ
- まとめ
- 参考資料

アジェンダ

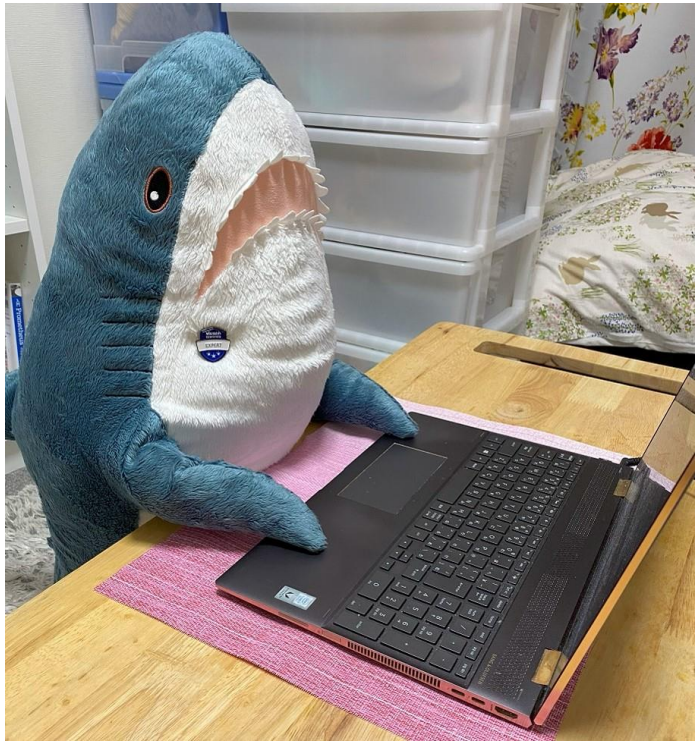
- 自己紹介
- サードパーティー製品を利用したAzure の閉塞環境
- 実際にあった問い合わせ
- まとめ
- 参考資料

自己紹介

名前：Kazuki Yamabe

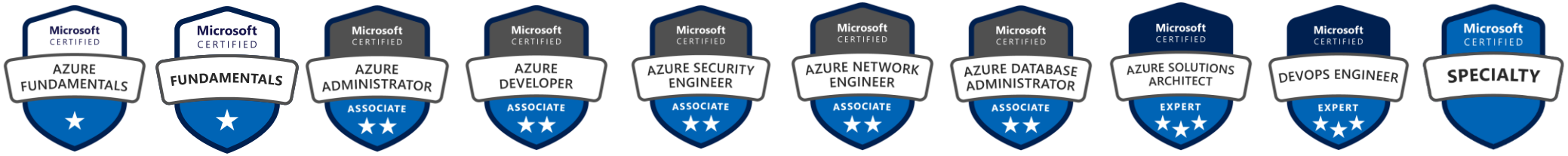
所属：株式会社エーピーコミュニケーションズ

職種：インフラエンジニアっぽい何でも屋のサメエンジニア



■ ブログ・SNS

- ブログ：https://www.kdkwakaba.com/
- X：@kdk_wakaba
- Linkedin：kdk-wakaba

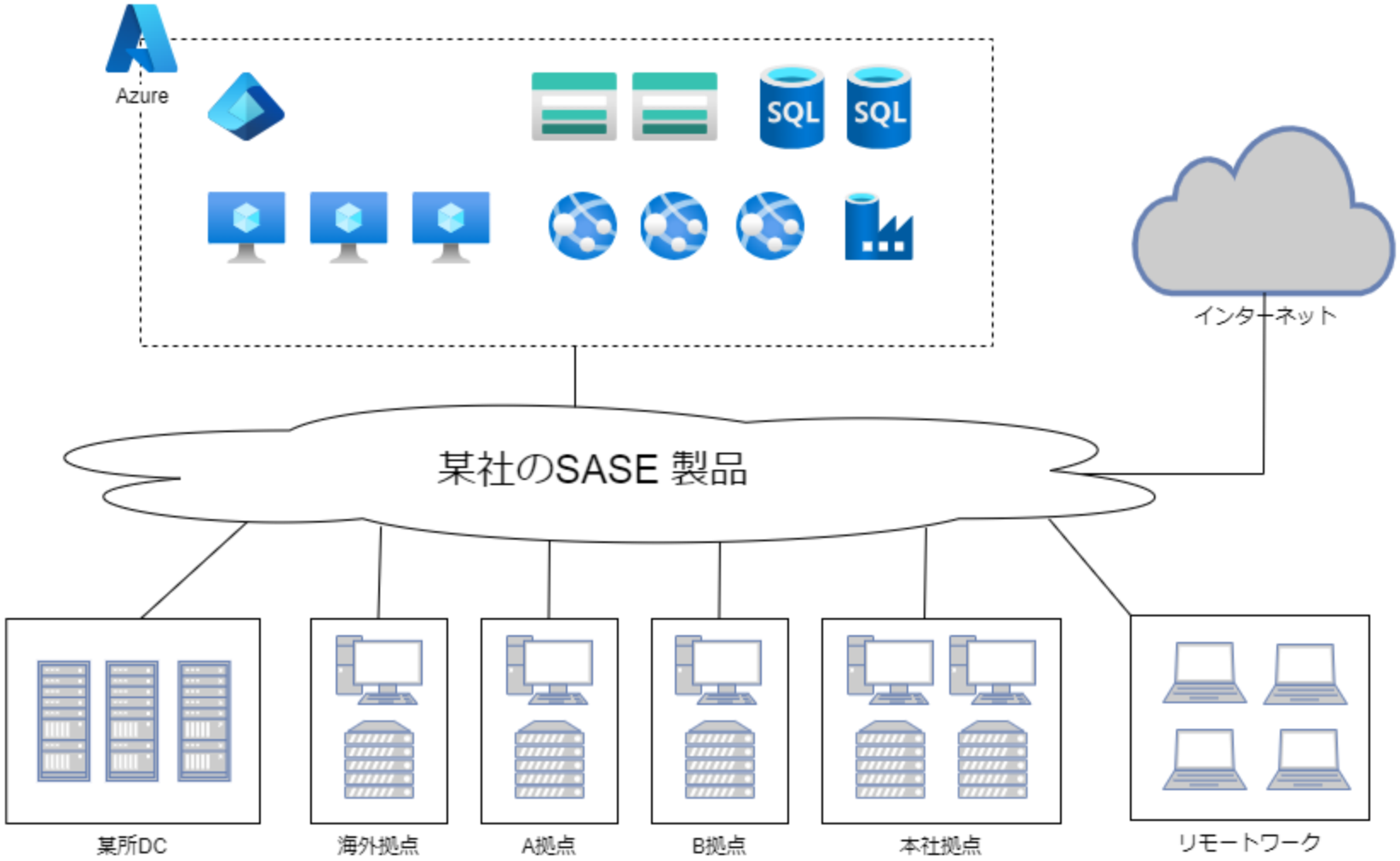


アジェンダ

- 自己紹介
- サードパーティー製品を利用したAzure の閉塞環境
- 実際にあった問い合わせ
- まとめ
- 参考資料

サードパーティー製品を利用したAzure 閉塞環境

複数拠点やリモートワークのアクセス管理をするためにSASE 製品を使うケースで問い合わせで調査したお話。



アジェンダ

- 自己紹介
- サードパーティー製品を利用したAzure の閉塞環境
- 実際にあった問い合わせ
- まとめ
- 参考資料

実際にあった問い合わせ – Azure Portal で情報が見れない

■ 問い合わせ内容

Azure Portal からIoT Hub を利用する時、デバイスが表示されずエラーとなってしまう。

※ IoT Hub はプライベートエンドポイントを利用している

■ 原因・対処

ローカルPC からプライベートなIoT Hub に443番ポートの通信遮断および名前解決が原因。Azure 前段のSASE 製品で443番ポートの通信許可、プライベートDNS ゾーンのフォワード設定追加で事象は解決。

■ 注意点・気づき

- プライベートなサービスを見る時、ローカルPC (ブラウザ) から対象サービスへの443番通信許可が必要
- ポートの許可だけでなく、必要に応じてDNS フォワード設定で拠点からの名前解決も追加する

実際にあった問い合わせ – PaaS 系サービスが正常に動作しない

■問い合わせ内容

Azure Machine Learning などのPaaS 系サービスをデプロイ後、各種機能が正常に動作しない。

■原因・対処

サービスに必要な一部URL、ポートが許可されていなかったため正常に動作していなかった。サードパーティーのSASE 製品ではサービスタグ、FQDN タグは利用できないため、必要なURL、プロトコル、ポートを直接許可することで事象は解消。

■注意点・気づき

- サードパーティーのSASE 製品ではサービスタグ、FQDN タグは利用できないので直接許可が必要
- 公式ドキュメントに掲載されていない情報はSR で問い合わせをして確認する

実際にあった問い合わせ – クエリエディターのEntra ID 認証が失敗

■ 問い合わせ内容

プライベートエンドポイントを繋いだAzure SQL Database でクエリエディターでMicrosoft Entra ID 認証が失敗する。SSMS の認証では問題なくログインできるしユーザーへの必要なロールも付与している。

■ 原因・対処

SQL Database に対し443番ポートや1433番ポートは許可していたが1443番ポートが許可していなかった。SASE 製品で1443番ポートの許可設定を追加し事象は解消。

■ 注意点・気づき

- SQL Database のクエリエディターとSSMS の接続は別物となるため注意
- 1443番ポートは事前に予約しているポートのため、SQL Server = 1433番ポートでの決め打ちは注意

実際にあった問い合わせ – 特定の拠点からアクセスできない

■ 問い合わせ内容

本社拠点からAzure リソースへのアクセスはできるが、A 拠点からAzure リソースにアクセスできない。ユーザー間のRBAC はどちらも同じはずなのに…。

■ 原因・対処

最小限のアクセスに絞りすぎたために、A 拠点のIP アドレス帯がサードパーティー製品のSaaS のホワイトリストに入っていなかった。また、プライベートDNS のフォワード設定も本社拠点しか入れていなかった。A 拠点に各種設定を追加し解消。

■ 注意点・気づき

- 最小限のアクセス制限は大事だが、複数の拠点がある場合は許可設定の差異を意識する

アジェンダ

- 自己紹介
- サードパーティー製品を利用したAzure の閉塞環境
- 実際にあった問い合わせ
- まとめ
- 参考資料

まとめ

- Azure の各種サービスでは様々な通信があるため、各種ネットワーク要件は事前に確認する
- 一部PaaS サービスではOutbound のFQDN、プロトコル、ポートの許可が必要なため、適宜許可する
  - サードパーティー製品のSaaS だとサービスタグ、FQDN タグはそのまま利用できない
  - MSのドキュメントに掲載されていないものはSR で問い合わせして確認する
- 最小限のアクセスは大事だが、複数拠点での利用を行う時は環境差異に注意する

参考資料

- 仮想ネットワーク サービス タグ
  - https://learn.microsoft.com/ja-jp/azure/virtual-network/service-tags-overview
- FQDN タグの概要
  - https://learn.microsoft.com/ja-jp/azure/firewall/fqdn-tags
- Azure SQL DB Connectivity Troubleshooting
  - https://techcommunity.microsoft.com/t5/azure-database-support-blog/azure-sql-db-connectivity-troubleshooting/ba-p/1158677

ご清聴ありがとうございました。