（日本語抄訳）

RCA - 複数の Microsoft サービスで発生した認証エラー (Tracking ID LN01-P8Z)

影響の概要:

2021 年 3 月 15 日の 19:00 UTC（日本時間 3 月 16 日 AM 4:00）から 2021 年 3 月 16 日の 09:37 UTC（日本時間 3 月 16 日 18:37）の間で、認証を Azure Active Directory (Azure AD) に依存する Microsoft サービスおよびサードパーティ アプリケーションにおいて、認証処理を行う際にエラーが発生した可能性があります。Azure AD サービスに対する対処策は、2021 年 3 月 15 日 21:05 UTC（日本時間 3 月 16 日　6:05）に完了しました。これにより各サービスへのトラフィックが順次回復しました。以下に、主なサービスとその回復までの時間を示します。

2021 年 3 月 15 日 22:39 UTC（日本時間 3 月 16 日 7:39): Azure Resource Manager が回復しました。
2021 年 3 月 16 日 01:00 UTC（日本時間 3 月 16 日 10:00): Azure Key Vault（ほとんどのリージョン）が回復しました。
2021 年 3 月 16 日 01:18 UTC（日本時間 3 月 16 日 10:18): セーフ デプロイメント プロセス (SDP) の一環として、Azure Storage の構成アップデートを最初の運用テナントに適用しました。
2021 年 3 月 16 日 01:50 UTC（日本時間 3 月 16 日 10:50): Azure Portal の機能が完全に回復しました。
2021 年 3 月 16 日 04:04 UTC（日本時間 3 月 16 日 13:04): Azure Storage の構成変更がほとんどのリージョンに適用されました。
2021 年 3 月 16 日 04:30 UTC（日本時間 3 月 16 日 13:30): 残りの Azure Key Vault リージョン (West US、Central US、East US 2) が回復しました。
2021 年 3 月 16 日 09:25 UTC（日本時間 3 月 16 日 18:25): Azure Storage が復旧を完了し、障害が完全に解消したことを報告しました。

根本原因と緩和策:

Azure AD は、OpenID およびその他の ID 標準プロトコルの利用をサポートするために、暗号鍵を使用して暗号的な署名処理を行います。セキュリティを高める標準的な対策の一環として、自動化されたシステムが、スケジュールに従い使用されなくなった鍵を自動的に削除します。過去数週間にわたり、複雑な複数のクラウドにまたがる移行を行うために、特定の鍵を通常よりも長い期間にわたり「保持」とマークしてい

ました。この対応において、自動化処理がその「保持」状態を誤って無視してしまう不具合が顕在化し、その特定の鍵が削除される状態が生じました。

署名鍵に関するメタデータは、インターネットの ID 標準プロトコルに沿い、Azure AD によってインターネット上でアクセス可能な場所に公開されます。この公開されたメタデータが 2021 年 3 月 15 日 19:00 UTC（日本時間 3 月 16 日 AM 4:00）に変更されたことにより、Azure AD と連携してこれらのプロトコルを使用するアプリケーションは、順次新しいメタデータを取得し始めました。結果として、削除された鍵で署名されたトークン/アサーションが信頼されなくなりました。この時点で、エンドユーザーはこれらのアプリケーションにアクセスすることができなくなりました。

サービスのテレメトリによって問題が検知され、エンジニアリング チームが問題の対応を開始しました。2021 年 3 月 15 日 19 時 35 分 UTC（日本時間 3 月 16 日 AM 4:35）に、進行中だった直近のバックエンドの基盤変更を元の状態に戻しました。鍵の削除処理が根本的な原因であることが判明したため、21:05 UTC（日本時間 AM 6:05）に鍵のメタデータを以前の状態にロールバックしました。

アプリケーションはロールバックされたメタデータを取得し、正しいメタデータでキャッシュを更新する必要があります。キャッシュの処理方法が様々なサーバーでそれぞれ異なって実装されているため、個々のアプリケーションが復旧するまでの時間もそれぞれ異なるものとなりました。一部のストレージ リソースでは、キャッシュされたメタデータによる影響が長く続きました。このため、これらのキャッシュを無効化して更新するための更新プログラムを展開しました。このプロセスが完了し、2021 年 3 月 16 日 9:37 UTC（日本時間 3 月 16 日 18:37）に、残存する影響を受けたお客様に対しても問題の解消が報告されました。

Azure AD は、この問題を含む一連のリスクを防ぐため、バックエンドのセーフ デプロイメント プロセス（SDP）システムに追加の保護を適用するという複数フェーズの取り組みを進めていました。第 1 フェーズでは、新しい鍵の追加を保護する対応を行いましたが、鍵の削除への対応は第 2 フェーズにあり、今年半ばまでに完了する予定でした。以前の Azure AD の障害は 2020 年 9 月 28 日に発生しており、複数フェーズの SDP の取り組みが完了すれば、どちらの障害も再発を防止できる類いのリスクとなります。

次のステップ:
今回の障害がどれほどの深刻な影響を与えたか、また容認しがたいものであったか弊社としても認識しており、深く陳謝いたします。今後このような問題が発生しないように、Microsoft Azure プラットフォームとプロセスの改善に継続的に取り組んでまいります。9 月の障害では、「今回確認された一連の問題を防ぐため、Azure AD サービスのバックエンド SDP システムに追加の保護機能を適用する」という計画を示しました。

- この SDP の変更の第 1 段階は終了し、第 2 段階は非常に慎重かつ段階的に展開を進めており、今年半ばに終了する予定です。初期の分析では、このシステムが完全に導入されれば、今回起きたような障害や 2020 年 9 月に起きた関連する障害も防止が可能です。それまでは、SDP の第 2 フェーズが完了するまでの間、鍵の削除プロセスに追加の保護措置を講じます。

- 9 月に発生した障害では、Azure AD バックアップ認証システムの導入についても言及しました。この取り組みは順調に進んでいます。しかし、残念ながら今回のケースでは、Azure AD バックアップ認証システムはトークンの発行を保護できても、トークンの検証までは保護できませんでした。これはトークンの検証処理が今回影響を受けたメタデータのエンドポイントに依存しているためです。

- 本障害では、Azure Active Directory を使用しているお客様にはサービス正常性を通じて通知を行いました。しかし、影響を受けた関連するサービスすべてに対しての通知を行うことができませんでした。この点については、ツールの不備があると判断し、今後適切に通知が行われるよう対応していく予定です。

- 調査と進捗状況について、お客様により最新の情報を提供すべきでした。今回、Azure、Microsoft 365、Dynamics 365 の間で情報提供の詳細やタイミングに差異があったことを確認しており、複数の Microsoft サービスを利用しているお客様の混乱を招きました。このためサービス間で一貫性と透明性を高めるために、修復項目を設けています。

フィードバックのお願い:
Azure カスタマー・コミュニケーション・エクスペリエンスの向上のためのアンケートにご協力ください: https://aka.ms/AzurePIRSurvey