2018 年 1 月 10 日

日本マイクロソフト株式会社
カスタマーサービスアンドサポート統括本部

Azure 計画メンテナンスに関するご報告

平素は格別のご高配を賜り、厚くお礼申し上げます。
本年 1 月 4 日より急遽、開始いたしました Azure メンテナンスにつきまして、以下の通りご報告いたします。脆弱性への対応とは言え、本メンテナンスの実施により、貴社の Azure 上のシステムへご不便とご迷惑をお掛けしましたことを深くお詫び申し上げます。

尚、公表されている脆弱性に対しては、今回の Azure インフラストラクチャの更新にて、ハイパーバイザー レベルでの修正を行っており、Windows もしくは Linux 仮想マシンイメージの更新は不要でございます。しかしながら、今回の件に関係なく、弊社では常に最新のパッチレベルにしておくことを推奨しております。
各ゲスト OS については以下サイトにてガイダンスを提供しておりますので、参考にしていただければ幸いです。

ADV180002|Guidance to mitigate speculative execution side-channel vulnerabilities
https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/ADV180002

Guidance for mitigating speculative execution side-channel vulnerabilities
https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/mitigate-se

目次

1. 今回のメンテナンス内容

Azure においては信頼性・パフォーマンス・セキュリティの向上のためメンテナンスを行っております。多くの更新は、仮想マシンの再起動を行わず、一時停止状態にして行われますが、一部のメンテナンス内容によって再起動が必要となります。

今回のメンテナンスは仮想マシンが稼働するホストサーバーの BIOS やファームウェアの更新及び、ホスト OS のアップグレードが必要となるメンテナンスであったため、お客様の仮想マシンの再起動が必要でございました。

＜Azure のメンテナンスの種類＞

■ インフラストラクチャの一部コンポーネントのメンテナンス

Azure の制御プレーンやストレージおよびネットワーク インフラストラクチャの更新につきましては、仮想マシンへの影響はございません。

■ パッチの適用

Azure ホストへのセキュリティやコンプライアンス等のパッチの適用につきましては、「インプレース仮想マシン移行（in-place virtual machine migration）」機能で、ローカルの一時ディスクとメモリーステートが保管された状態にし、最大 30 秒だけ仮想マシンの動作を一時停止させますが、仮想マシンの再起動は行いません。

■ ハードウェアメンテナンスとホスト OS のアップグレード

ハードウェアのメンテナンスまたは使用停止、ホスト OS のアップグレードにつきましては、仮想マシンの再起動が必要となります。このように再起動を伴うメンテナンスの場合は、サブスクリプション管理者へメンテナンスの予定が通知されます。また、都合に応じて自分自身でメンテナンスを開始できる時間枠(セルフサービス期間)が提供されます。

2. 今回の経緯

記載は日本時間となります。

■ 2017 年中 - 脆弱性の認識と対策の開始

弊社内において、CPU 脆弱性に関して認識し、計画メンテナンスの対策を講じておりました。

■ 2017 年 12 月 19 日 - 計画メンテナンスの通知

本脆弱性の問題が公にはなっておりませんでしたが、重大な問題であったため、急遽、今回の計画メンテナンスを以下のスケジュールにて実施することが決定いたしました。

通知	2018 年 1 月 2 日
セルフサービス期間	2018 年 1 月 2 日から 2018 年 1 月 9 日
予定メンテナンス期間	2018 年 1 月 10 日 午前 3 時から 2018 年 1 月末日(日本時間)

■ 2017 年 12 月 27 日 - 計画メンテナンスのセルフサービス期間延長

多くのお客様からのご要望に応え、セルフサービス期間を可能な限り長く用意させていただくべく、今回の計画メンテナンスのスケジュールを以下のように変更することが決定いたしました。

通知	2017 年 12 月 28 日午前 9 時
セルフサービス期間	2017 年 12 月 28 日午前 9 時から 2018 年 1 月 9 日午後 9 時
予定メンテナンス期間	2018 年 1 月 10 日午前 9 時から 2018 年 1 月末日

なお、Azure 管理ポータルより各仮想マシンのメンテナンススケジュールが表示されるようになりましたが、脆弱性対策の重要性から、時間的制約が大きく、一部リージョンの一部仮想マシンにおいてはセルフサービスのメンテナンスが提供できない状態となっておりました。

■ 2018 年 1 月 4 日

2018 年初より、マスメディアにおいて当脆弱性が明らかとされました。続いて、2018 年 1 月 4 日に Google の Project Zero チームより上述の脆弱性が公表されました。公表された情報には、実証コードが含まれており、今回の脆弱性を悪用したプログラムが作成されるまでの猶予期間が全くない状況となったため、当初のメンテナンス スケジュールを前倒しせざるを得ないという判断結果に至りました。これにより 2018 年 1 月 4 日午前 8:30 より順次、脆弱性への対応を適用するとともに本対応の反映のため、お客様の仮想マシンの再起動を実施、同時にお客様への通知の準備が行われ、順次、電子メールでの通知が行われました。

通知	2018 年 1 月 4 日午後
セルフサービス期間	2018 年 1 月 4 日午前 8 時 30 ※脆弱性情報の一般公表により急きょ打ち切り
予定メンテナンス期間	2018 年 1 月 4 日午前 8 時 30 から 2018 年 1 月 11 日午前 9 時

上記予定メンテナンス期間の完了予定日より早期にメンテナンスを終えることが出来、2018 年 1 月 9 日午前 11 時頃、全リージョンで完了済みとなっております。

弊社からの公開声明については、以下をご参照ください。

Securing Azure customers from CPU vulnerability
https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/

抄訳:
https://blogs.technet.microsoft.com/jpaztech/2018/01/04/securing-azure-customers-from-cpu-vulnerability/

以上