Microsoft

ハイブリッドワークに不可欠な
ゼロトラスト・セキュリティ

Azure Active Directory による
新時代のセキュリティ

INDEX

第 1 章

ハイブリッドワーク時代の セキュリティとは？

数年前までは、企業のネット環境といえば、使用するデバイスは会社から支給された PC のみで、

ファイアウォールに守られた社内ネットワークだけで完結するのが一般的でした。

ですが最近は、リモートワークやクラウドサービス、BYOD（Bring your own device / 個人保有デバイスの業務への利用）の普及によって、

会社とその外側の境界線があいまいになっています。そんな新しい時代のセキュリティ対策は、

「全てのものを信用しない」ことを前提にしてあらゆる攻撃に備える「ゼロトラスト・セキュリティ」の考え方を持つことが大切です。

ゼロトラスト・セキュリティを支える基盤「Identity」

ゼロトラスト・セキュリティは、「何も信用せず、すべてを検証すること」が前提となります。

そのためには、一箇所ですべてのモノを管理するのが最も効率的です。

すなわち、デバイス、ユーザー、アプリなど、

検証すべき対象のすべてをひとつの基盤で管理・制御することで、

手間をかけずに高度なセキュリティ対策を施すことが可能となるのです。

HINT!

企業活動の土台となる Identity の担う役割とは？

ゼロトラストの世界では、Identity は企業活動で扱うすべての資本（アプリやユーザー、デバイスなど）を一箇所で管理し、企業活動の土台となる「制御プレーン」の役割を担います。その Identity ツールとしてマイクロソフトが提供しているのが、Azure Active Directory です。

POINT

境界型セキュリティの限界

これまでは、「社内と社外の接点からの脅威の侵入を防ぐ」ことを目的として、PC やサーバーを社内で結ぶネットワークと外部ネットワークとの境界線にファイアウォールなどを施す、「ネットワーク重視型」のセキュリティ対策が一般的でした。ですがこの対策だと、一度社内ネットワークへウイルスの侵入を許してしまうと、自由に社内情報にアクセスされてしまいます。社内ネットワーク内は安全であり、その境界線だけを守ろうとする境界方セキュリティの概念は、クラウド サービスや BYOD を取り入れたハイブリッドワーク時代には、そぐわなくなっているのです。

新時代のセキュリティ基盤「Azure Active Directory」

「Azure Active Directory (Azure AD)」は、
企業のアクセス コントロール基盤として、ゼロトラスト型のセキュリティ体制を実現します。
企業の IT 担当者であれば、マイクロソフトの Active Directory を
扱った経験のある方も多いかもしれません。
Active Directory が企業内認証に使われるのに対して、
Azure AD はクラウド サービスの認証に用いられるのが特徴です。

HINT!

Azure AD のクラウドならではのメリットとは？

クラウド サービスである Azure AD を導入すれば、独自でクラウド認証システムを構築する必要がなく、ゼロトラストに対応した最新のセキュリティ認証基盤を簡単に導入することができます。

MERIT 1

コストの低減

サーバー構築が不要のサブスクリプション型サービスなので、導入コストやランニングコストを抑えられる。

MERIT 2

運用の負担を低減

Active Directory では必要だった Windows Server のアップデート作業やパッチを当てる作業が必要なくなるため、運用の負担を減らせる。

MERIT 3

最新のセキュリティ対策

「Identity」に基づいた ID 統合管理で安全性を向上。世界で 2 番目にサイバー攻撃を受けているマイクロソフトが、自社への攻撃をベースにリスクを検知、脅威のトレンドにも対応。

MERIT 4

高い拡張性

自社アプリだけでなく、クラウド上のさまざまな外部アプリとも連携できるので、自社の使い方に合わせた運用が可能。

第 2 章

Azure AD 実践編

ゼロトラスト・セキュリティを実現するためには、誰がいつ、どのデバイスでどのアプリにアクセスしたかを正しく把握・管理し、

問題が起きた際には早急に対応できるようなアクセスコントロール基盤が必要です。

この章では、新時代の脅威に対して、アクセスコントロール基盤である

「Azure AD」がどのように有効に働くのかを、具体的に解説します。

「複雑なパスワードにすれば安全」は勘違い？

「数字とアルファベットの大文字、小文字、記号を混ぜた 8 文字以上の…」といった
複雑なパスワードであれば、安全性は高くなると思う方も多いのではないでしょうか。
実は、悪意を持ってパスワードを盗み出そうとする手口に対して、
パスワードの複雑さはあまり役に立ちません。また、フィッシング詐欺で偽サイトに誘導され、
パスワードを入力させられてしまえば相手に筒抜けになってしまいます。
そこで有効な対策になってくるのが、パスワード +α の「多要素認証」であり、
「パスワードレス認証」なのです。

HINT!

段階を踏んで、より高度なセキュリティ対策を！

STEP 1

まずは組織全体に多要素認証を適用しよう

多要素認証は、過去にパスワードが漏れたことが原因で引き起こされた事件のほとんどが多要素認証で防げたといわれるほど、セキュリティ強度を向上させることができます。Azure AD は、SMS や電話、アプリケーション、ソフトウェアトークン、ハードウェアトークンといった 5 つの要素をパスワード +α の要素として提供しています。さらに、リスクベースの条件付アクセスでは、疑わしい行為を自動的に検出して多要素認証を有効化することもできます。

多要素認証を有効化できる条件

- 特殊な移動
- 匿名 IP アドレス
- 通常と異なるサインインプロパティ
- マルウェアにリンクした IP アドレス
- 視覚情報の漏えい
- Azure AD 脅威インテリジェンス

STEP 2

安全性も利便性も高いパスワードレス認証を検討しよう

パスワードレス認証とは、日ごろの業務でユーザーがパスワードを入力する必要がない運用のこと。パスワード以外の複数認証によって高いセキュリティ強度を保ちつつ、運用の手間を低減し、ユーザーの利便性も向上させることができます。

Microsoft が推奨するパスワードレス認証オプション

- Windows Hello For Business
- Microsoft Authenticator
- FIDO2 セキュリティキー

パスワード忘れへの対応が大変…

パスワードの複雑性を遵守する運用にすると、

「アカウントがロックされた」「パスワードを忘れた」といったケースが増えてきます。

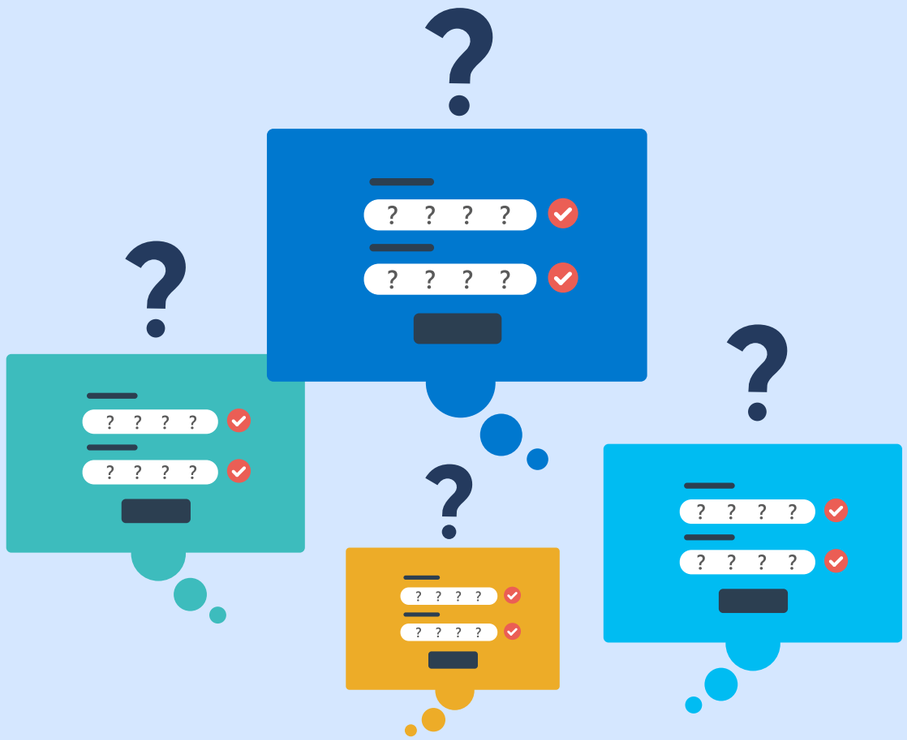
ある調査によれば、ヘルプデスクの問い合わせ内容で一番多いのは、パスワード変更依頼だそうです。

パスワードのリセットは、手続きが煩雑だったり、

リセットが完了するまではオンライン業務ができなくなってしまったりと、

生産性の低下につながります。ユーザーがパスワードを再設定できる、

Azure AD のセルフサービス パスワード リセット機能を有効に使って、この問題を解決しましょう。



HINT!

セルフ パスワード リセット機能で生産性を下げずに安全性も向上！

パスワードの変更には管理権限が必要で、ユーザーにとっても管理者にとっても手間がかかるものでした。Azure AD のセルフサービス パスワード リセット機能を有効にしておけば、ユーザー自身がパスワードをリセットできるため、諸手続きに伴う生産性の低下を防げることができます。また、推測しやすかったりよく利用されたりするパスワードを設定できないようにする機能も備えられているため、より安全な業務環境を実現できます。

セルフ パスワード リセット機能

ユーザー自身がパスワードのリセット可能！
安全性を高めるため推測しやすいパスワードは設定できない。

推測しやすいパスワード
1 2 3 4 5
NG

推測しずらいパスワード
9 a z W 7 5 q
OK

外部アプリが増えて、管理が煩雑に…

クラウドが主なビジネス基盤となったいま、企業は自社アプリだけではなく、
クラウド上に置かれた SaaS アプリを活用するようになりました。
当然、これらのアプリに対しても自社アプリと同程度のセキュリティ強度が必要になります。
ですが、セキュリティに気を遣うあまり、管理が煩雑になったりアプリを開くたびに
サインインを求められたりするのは、よい環境とは言えません。
Azure AD のアプリ連携機能を使えば、多様な SaaS アプリを安全に使えるようになります。

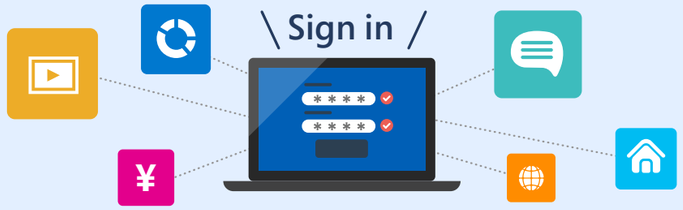
HINT!

Azure AD との連携で外部アプリも使いやすく!

Azure AD で ID を統合し、シングルルサインオン（SSO）を利用すれば、ユーザーが一度ログインした資格情報がほかのアプリにも使用されることになり、アプリにいちいちサインインする必要がなくなります。ID を一元管理できるようになるので、さまざまな外部アプリケーションの認証レベルの統一することもできます。ユーザーを集中的に管理して、アクセス状況を一元的に把握することも可能です。

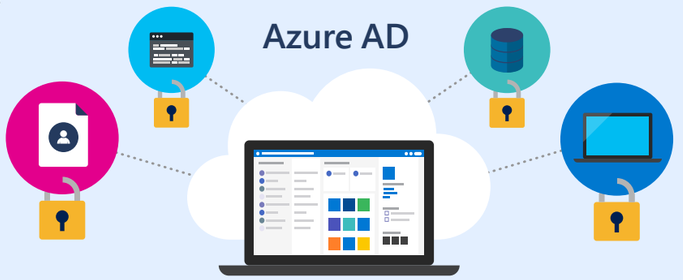
ユーザーのメリット

Azure AD 一度サインインするだけで、すべてのアプリを利用可能。



管理者のメリット

SaaS アプリケーションにも Office 365 と同じ強力な認証方式やアクセス コントロールが適用（セキュア リモートワーク、多要素認証、パスワードレス認証、デバイス ベースの認証、リスクベースの認証、など）されるので、SaaS 選定時に問題となる非機能要件対応を Azure AD に任せることが可能に。



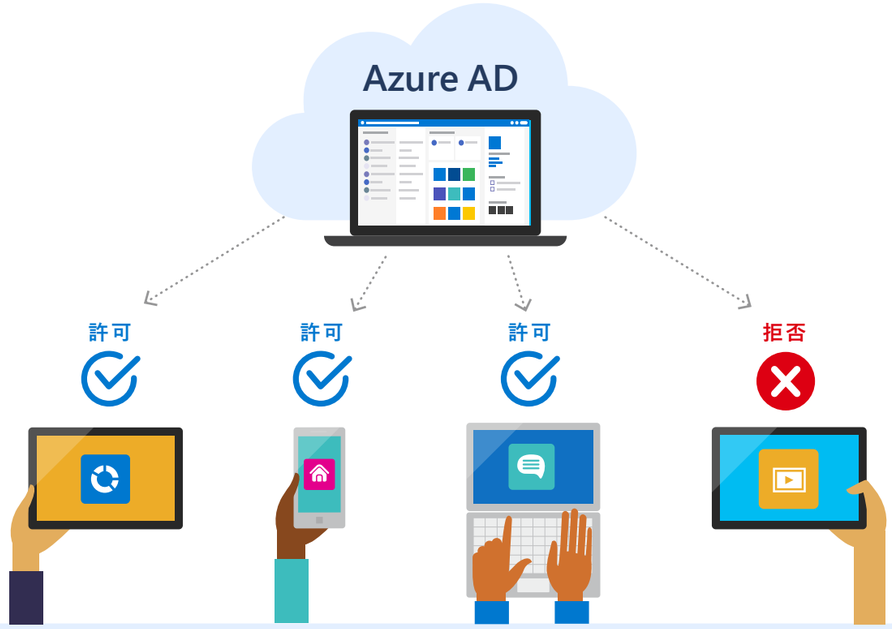
リモートワークや BYOD、セキュリティは大丈夫？

リモートワークや BYOD を導入した企業では、さまざまなデバイスから、
さまざまな経路で会社のネットワークへアクセスが行われます。
ネットワークの安全を保つためには、これらのユーザーがどこにいるのか、
なんのデバイスを使っているのか、どこにアクセスをするのか、
更にそのユーザーにリスクがあるのかをすべて検証したうえでアクセス可否の判断を行い、
セキュリティ強度をどの程度にセットするかをそれぞれに割り当てる必要があります。
Azure AD の「条件付きアクセス」を使えば、高度なセキュリティ対策を、
手軽に、しかも自動的に適用することができます。

HINT!

自動的にリスクを検出し、デバイスからのアクセスを制御！

条件付きアクセス機能によって、ユーザーの状況や使用しているデバイスの状態に応じてアプリにサインインする際の認証強度を変えたり、アクセスを拒否・許可したりすることができます。さらに、Azure AD に登録したデバイスなら、会社支給の端末でも、BYOD 端末でも、MDM (モバイル デバイス マネジメント) 機能によってそのデバイスが安全かどうかを自動的に判断し、アクセスを禁止したり、多要素認証による本人確認を強制したりできます。



条件付きアクセスで検出できる ID ベースのリスク

- 特殊な移動
- 短時間に別の国からサインインを試みる
- 匿名 IP アドレス
- 通常とは異なるサインインプロパティ
- マルウェアにリンクした IP アドレス
- ユーザーに対するセキュリティ侵害を確認
- パスワード スプレー
- 資格情報の漏洩
- Azure AD 脅威インテリジェンス
（マイクロソフトに集積された世界中の不正アクセス情報）

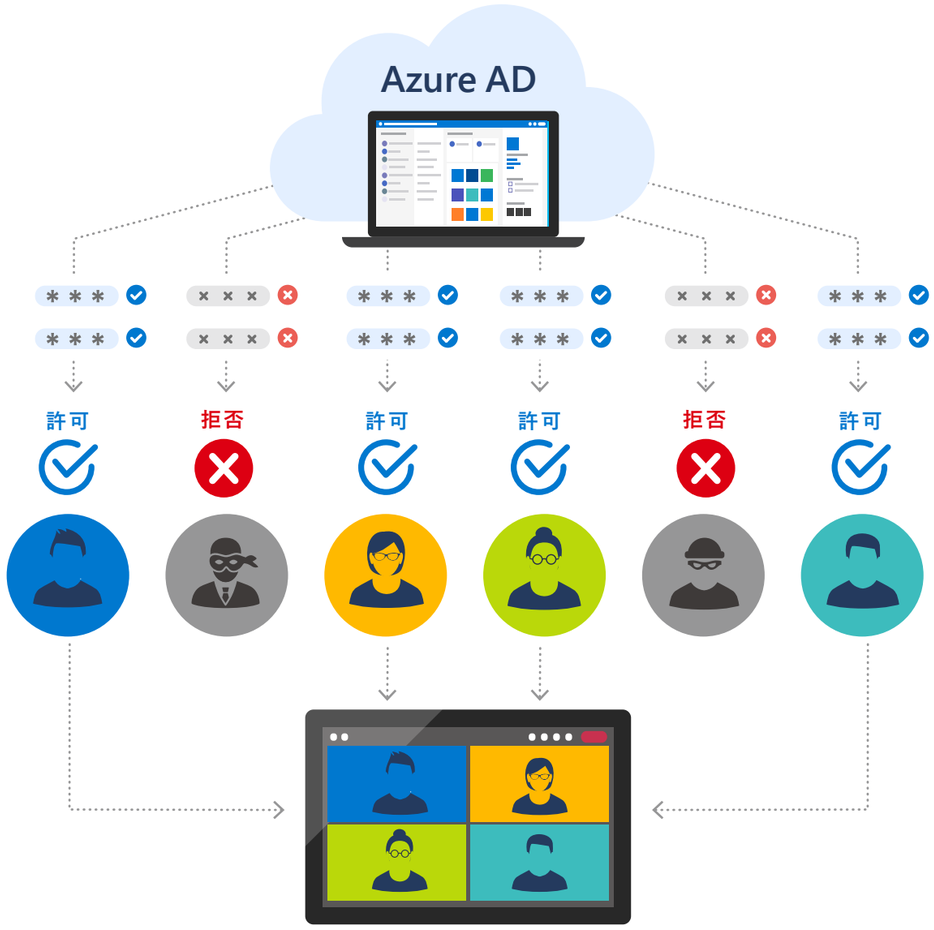
Web 会議で外部ユーザーと安全にやり取りするには？

リモートワークの普及に伴って、Web 会議ツールの利用は一般的になりました。
Web 会議ツールを通じて機密情報を扱う場面も増えています。
しかし、外部の人のアカウント管理はその人自身に任せるしかなく、
ツールによっては、全く関係ない人が勝手に参加できたり、
外部にパスワードや会議内容が漏洩したりしてしまうのではないか、といった
セキュリティリスクが指摘されることもあります。
「Microsoft Teams」なら、安全に情報をやりとりしながら、
組織やチームのコラボレーションを活性化できます。

HINT!

安心して使えるコラボレーションツール「Microsoft Teams」

Microsoft Teams では、Azure AD の「条件付きアクセス」を利用できるので、外部のユーザーにも多要素認証を要求したり、普段とは違うアクセスなどのリスクを検知してパスワードの変更を求めたりと、組織内ユーザーと同様の高度なセキュリティを適用できます。このため、安心して外部の人とコラボレーションできます。また、Microsoft Teams 内で機密情報を扱ったり、組織内だけで留めたい内容の資料を利用したりする場合は、外部アクセスやゲストアクセスをオフにすることもできます。



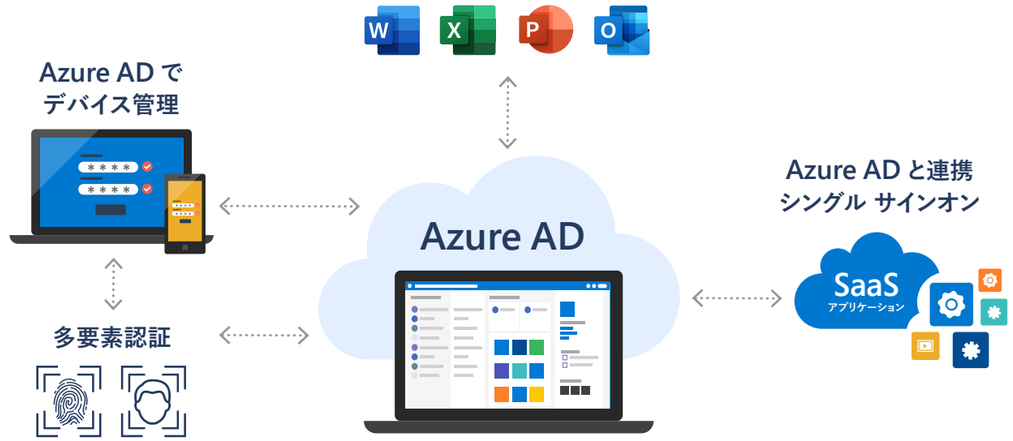
ゼロトラスト時代のパートナー、Azure AD

これから私たちが進もうとしている「ゼロトラスト」の世界では、
リモートワークやハイブリットワークが進み、いろんな場所からさまざまなデバイスで
社内ネットワークにアクセスするようになります。自社アプリだけでなく、
クラウドに置かれたサードパーティアプリの活用も、これまで以上に進んでいくでしょう。
一方で、パスワードはもはや安全ではなく、多様化するサイバー攻撃への対応が求められます。
Azure AD を活用して、新時代の脅威にも負けない万全なセキュリティ対策を手に入れましょう。

HINT!

Azure AD があれば怖くない！

Azure AD なら、新時代の脅威に備えた高度なセキュリティ対策ができるだけでなく、自動化によって管理者の負担を減らすこともできます。



認証
課題　サイバー攻撃の多様化、パスワードが最大の弱点に。
Azure AD　多要素認証やパスワードレス認証で認証プロセスを強化＆簡略化。

アクセス
課題　リモートワークが一般化し、アクセス経路が複雑化。
Azure AD　さまざまな経路からアクセスするすべてのデバイスを安全に制御。

アプリケーション
課題　クラウド サービス利用が進み、SaaS アプリの利用が増加。
Azure AD　多様なアプリと安全に連携。シングルルサインオンでアクセスも簡略化。

高度なセキュリティ機能をオールインワンで提供

Microsoft 365 E5 では、新時代のビジネス環境に必要な
「ID 保護」「脅威対策」「情報保護」「クラウドセキュリティ」の
4 つのセキュリティ機能がまとめて提供されます。
あとから機能を追加しなくても、Azure AD をはじめとする
さまざまなセキュリティ機能を提供するサービスを常に最新の状態で利用できるため、
各機能を連携させて包括的に組織全体を守ることができます。
同時に、自動化によって管理者の負担も軽減できます。

	Microsoft 365 E3	Microsoft 365 E5
ユーザー / 月	詳しくは、販売パートナー様へお問合せください	
含まれる Office アプリ	Outlook, Word, Excel, PowerPoint, Access, Publisher（Access、Publisher は Windows PC のみ）	
含まれるクラウドサービス	Exchange, OneDrive, SharePoint, Teams, Bookings, Sway, Lists, Yammer, Stream, Power Apps, Power Automate, Planner, ToDo, MyAnalytics	
1 ライセンスでのインストール	最大 5 台の Windows PC / Mac （Web・モバイル版と合わせて最大 15 台のデバイス）	
デバイスとアプリの管理	○	○
アイデンティティとアクセスの管理	△ ※	○
脅威対策	△ ※	○
情報保護	△ ※	○
セキュリティ管理	○	○
コンプライアンス管理	△ ※	○

※詳しくはこちらをご確認ください。https://www.microsoft.com/ja-jp/microsoft-365/compare-microsoft-365-enterprise-plans

Microsoft

お役立ち情報　Azure AD に関する情報を、ブログや映像でわかりやすくご案内しています。知りたいことや困ったことがあったときに、ぜひお役立てください。

Azure AD Webinar

Azure AD の基礎から導入・運用ノウハウまでを学べるウェビナーのアーカイブを公開中です。
YouTube チャンネル「Azure AD Japan」でもご覧いただけます。

http://aka.ms/azureadwebinar

EMS Blog

Azure AD (EMS) 開発チームメンバーが新機能などの最新情報をいち早くお届けするブログです。
Azure AD 管理者がおさえておきたいポイントをまとめた「セキュリティ ホワイトペーパー」もダウンロードできます。

http://aka.ms/emsblog/

Japan Azure Identity Support Blog

国内の Azure ユーザーのサポートを担当している現役の「Azure Identity サポート エンジニア」によるブログです。
新機能に関する情報や皆様に役立つ情報をお届けします。

https://github.com/jpazureid/blog

ご購入前のご相談は「セキュア リモートワーク相談窓口」

0120-167-400

（営業時間：9:00 ～17:30 土日祝日、弊社指定休業日を除く）

詳しくはこちらから

https://www.microsoft.com/ja-jp/microsoft-365

© 2021 Microsoft Corporation. All rights reserved.
※ 記載されている会社名および製品名は商標または各社の登録商標または商標です。※ 製品の仕様は、予告なく変更することがあります。予めご了承ください。※使用している画像はイメージです。※ 記載の内容は、2021 年 8 月現在のものです。

日本マイクロソフト株式会社　〒108-0075 東京都港区港南 2 - 16 - 3 品川グランドセントラルタワー