

特別版

できる

Microsoft 365

管理編

清水理史&できるシリーズ編集部



ライセンスからデバイスまでを一括管理
常に最新デスクトップ環境を安全に運用



インプレス

*1:当社調べ *2:大手書店チェーン調べ

本書の読み方

レッスン

見開き2ページを基本に、
やりたいことを簡潔に解説

●やりたいことが見つけやすいタイトル
「〇〇をするには」や「〇〇ってなに?」など、「やりたいこと」や
「知りたいこと」がすぐに見つけられるタイトルがついています。

●機能名で引けるサブタイトル

「あの機能を使うにはどうするんだっけ?」そんな時に便利。
機能名やサービス名などで調べやすくなっています。



右ページのつめでは、
知りたい機能で
ページが挟めます。

Point

操作の要点をていねいに解説。レッスンで解説している内容をより深く理解することで、確実に使いこなせるようになります。

※ここで紹介している紙面はイメージです。本書の内容と一部異なる場合があります。

ヒント

レッスンに関連した、さまざまな機能を紹介したり、一歩進んだ使いこなしのテクニックまで解説します。

●用語の使い方

本文中では、「Microsoft® Windows® 10」のことを「Windows 10」または「Windows」と記述しています。また、本文中では「Microsoft® Office 365」のことを「Office 365」、「Microsoft® Word® 2016」のことを「Word 2016」または「Word」、「Microsoft® Excel® 2016」のことを「Excel 2016」または「Excel」、「Microsoft® PowerPoint」のことを「PowerPoint」と表記しています。本文中で記述している用語は、基本的に実際の画面に表示される名称に則っています。

●本書の前提

本書では、「Windows 10」がインストールされているパソコンで、インターネットに常時接続されている環境を前提に画面を再現しています。

●本書に掲載されている情報について

本書に掲載されている情報は、2018年12月現在のものです。本書の発行後に、情報が変更されることもあります。

「できる」「できるシリーズ」は、株式会社インプレスの登録商標です。

Microsoft、Windows、Office 365、Word、Excel、PowerPointは、米国Microsoft Corporationの米国および/またはその関連会社の商標です。そのほか、本書に記載されている会社名、製品名、サービス名は、一般に各開発メーカーおよびサービス提供元の登録商標または商標です。

なお、本文中には™および®マークは明記していません。

まえがき

今、組織のシステムを取り巻く環境はとても複雑です。さまざまなデバイスを使って、さまざまな場所で、さまざまなツールを活用し、さまざまな人と、さまざまな目的で、さまざまな形態で一緒に働くことが要求される一方で、このような働き方を支えるためのシステムをスピーディかつ低成本に、しかもセキュリティやコンプライアンスに十分配慮した状態で整えなければなりません。

本書は、こうした現代ならではのシステム管理の悩みを、マイクロソフトが提供するクラウドサービス「Microsoft 365」によって改善するためのガイドブックです。最新のクラウドサービスと最新のデスクトップによって、従来のシステム管理者の大きな負担になっていた作業がどのように改善されるか、進化を続ける最新の脅威からどのようにシステムを保護するかをテーマに、Microsoft 365で提供される各種機能について、展開・更新、セキュリティといった分野ごとに、イラストを交えながら分かりやすく解説しています。

本書を手に取ることで、組織のシステム管理に携わる方々の負担が少しでも軽くなれば幸いです。

2018年12月

清水理史

目 次

できる Microsoft 365管理編

① Microsoft 365で何が変わるの？ <企業の働き方とセキュリティ改革>	2
② どんなプランやエディションがあるの？ <Microsoft 365プランの選択>	4
③ Microsoft 365を使い始めよう <Microsoft 365 テナントの準備>	6
④ パソコンの準備をしよう <OfficeとWindowsの展開>	8
⑤ より安全に活用するには 【外部脅威対策】 <統合ソリューション>	12
⑥ より安全に活用するには 【情報保護対策】 < Azure Information Protection, Azure AD Premium、Microsoft Cloud App Security、Microsoft Intune>	18
⑦ 安全性を維持するために必要な更新の管理 <WindowsとOffice 365 ProPlusの更新>	22

Microsoft 365で何が変わるの？

企業の働き方とセキュリティ改革

Microsoft 365は、「働き方改革」や「セキュリティ対策」など、今、組織が取り組むべき課題に、どう役立つのでしょうか？
その概要を見てみましょう。

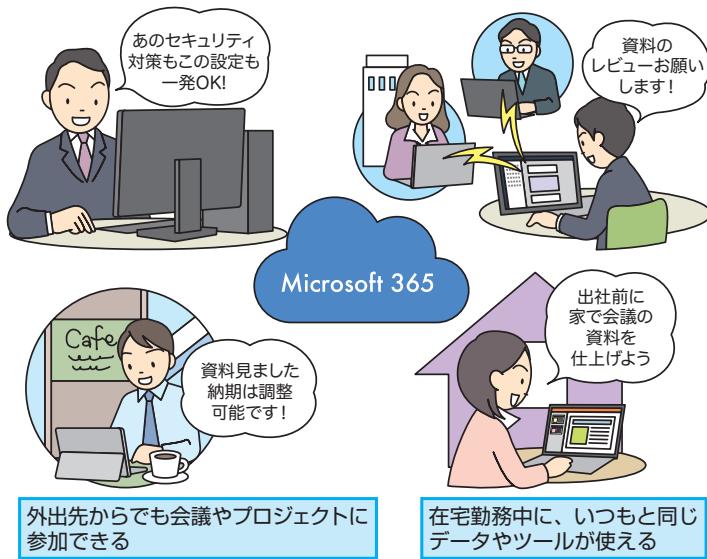
クラウドシフトで常に最新の生産性とセキュリティを実現

●働き方改革を促進

「どうすれば生産性を上げられるか？」「誰もが働きやすい環境をどう実現するか？」。「Microsoft 365」は、こうした課題に取り組む組織に最適なマイクロソフトのクラウドソリューションです。Windows 10やOffice 365 ProPlusなどをクラウドから社員に簡単に展開できるだけでなく、Microsoft Teamsなどの各種クラウドサービスを活用することで組織内の情報共有やコミュニケーションを活発化したり、AIによる新しいコンピューティングパワーを手軽に活用できます。

いろいろなサービスや端末を一元管理。
PCの展開も楽で、セキュリティも万全

社内外のメンバーとチャットで
共同作業や会議ができる



●Microsoft 365で働き方がこう変わる

- ・組織内の情報共有やコミュニケーションを活発化できる
- ・在宅勤務や外出先での作業など新しい働き方を実現できる
- ・Windows 10やOffice 365 ProPlusの組織内展開が楽になる



具体的に どう働き方が変わるの？

本書は、Microsoft 365を活用したクラウドアントの展開やセキュリティ対策など、主に管理機能に焦点を当てた小冊子です。Microsoft 365で何ができるのか？ 具体的にどのような仕事がどう変わらるのか？ といったことは『できるMicrosoft 365 活用編』で詳しく紹介していますので、そちらを参照してください。



Microsoft Teams って何？

Microsoft Teamsは、組織内、および外部の人と文字によるチャットやビデオ会議をしたり、ファイルなどのデータを共有したりできる新しいタイプのコミュニケーションツールです。プロジェクトや話題ごとに作成したチームごとに、リアルタイムに会話ができるため、情報を整理しやすく、素早い意志決定をすることができます。従来のメールによるコミュニケーションでは、大量の情報の中に重要な情報が埋もれてしまいかで、意思疎通にも時間がかかりますが、こうした組織の悩みを解決できます。

●モダンデスクトップの実現

設置したデバイスを組織向けにセットアップしたり、そのセキュリティ対策を施すことは、これまで組織のシステム担当者にとって大きな負担となっていました。こうした負担を軽くできるのが「モダンデスクトップ」という概念です。クラウドサービスを活用することで、常に最新のWindowsと最新のOfficeを利用できるようにしたり、マルウェアからの攻撃や情報漏えいを防止するセキュリティ対策を手間なく整えたりできます。モダンデスクトップによって、これまで組織で抱えていた次のような悩みを解決できます。

- ・Windowsを組織用にセットアップするのに手間がかかる
- ・WordやExcelなどのOfficeアプリのインストールに手間がかかる
- ・更新プログラムの適用タイミングや配信方法を制御できない
- ・デバイスのセキュリティ対策にコストと手間がかかる
- ・標的型攻撃などの高度な攻撃への対策ができていない
- ・情報漏えい対策をどうしたらいいかが分からない
- ・スマートフォンなどのデバイスの管理に、目が行き届かない
- ・社員が勝手にクラウドサービスを使っており、無法地帯
- ・組織内のクライアントを統合的に管理できない
- ・法令遵守をどう実現すればいいのかが分からない



生産性の向上、効率的な管理、
安心のセキュリティを
同時に実現

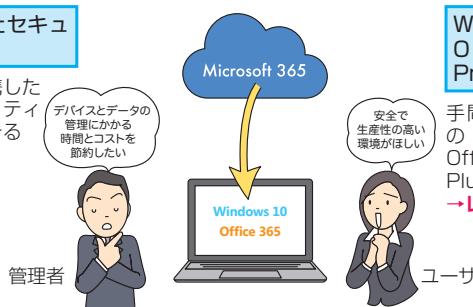
Microsoft 365は、組織に必要とされるさまざまなサービスを統合したソリューションです。Office 365 ProPlusとWindows 10だけでなく、チームでの生産性を高めたり、AIまで活用できる各種サービスやアプリケーション。組織内のシステムを管理するための各種サービス。エンタープライズ向けの高度なセキュリティを実現するセキュリティ対策機能など、トータルでソリューションを提供することで、現代のニーズにマッチした組織のIT化を手助けします。それぞれを個別に対策すると高額な費用がかかるうえ、個別に設定や管理が必要になりますが、リーズナブルな価格から始められるうえ、複数のサービスを統合的に管理することができます。

WindowsとOffice 365 ProPlusの展開

簡単に Windows や Office 365 ProPlus を
社内のクライアントに展開できる → レッスン①

統合化されたセキュリティ機能

クラウドと連携した
強力なセキュリティ
機能を利用できる
→ レッスン⑤、
レッスン⑥



Windows と Office 365 ProPlusの更新

手間なく常に最新
の Windows と
Office 365 ProPlus
に更新できる
→ レッスン⑦

Point

複雑化するシステムを Microsoft 365でシンプルに

組織のシステムに求められる要件は、今や、とても複雑です。例えば、働き方改革にともなって、社外ユーザーとのコミュニケーションを活性化しようとしたり、リモートワークを実現しようすれば、セキュリティ対策やコンプライアンス対策が不可欠になり、コストもシステム担当者の負担も大きくなる一方となります。そこで活用したいのがマイクロソフトが提供するMicrosoft 365です。デスクトップの管理から、クラウドサービスの活用、セキュリティ対策など、「今の時代」に合ったシステムをトータルで実現可能です。

●モダンデスクトップでPCの管理がこう変わる

- ・常に最新版のWindows 10、最新のOfficeを使える
- ・展開や更新の方法を選択できる
- ・組織内のセキュリティを強化できる

どんなプランやエディションがあるの？

Microsoft 365 プランの選択

Microsoft 365には、使える機能の違いによって複数のプランが用意されています。どのような用途に使うかを考えて最適なプランを選びましょう。

最適な用途のプランを選ぼう

Microsoft 365は、従来のOffice 365のサービスに、Windows 10、Enterprise Mobility and Securityの機能を統合したクラウドサービスです。Microsoft 365には、よく使う機能を絞り込んだBusinessと、より高度な機能を備えたEnterpriseのプランがあります。さらにEnterpriseにはE3とE5があり、E5ではより高度な脅威対策やコンプライアンス機能が提供されます。また、最前線で仕事をするユーザー向けのF1もあります。

◆ Microsoft 365 Enterprise E5

高度なセキュリティやコンプライアンス対策が必要な組織



◆ Microsoft 365 Enterprise F1

一般的な業務が少なく、常に現場において最小限の機能だけ使用できればよい組織



◆ Microsoft 365 Enterprise E3

一般的な業務の組織



◆ Microsoft 365 Business

一般的な業務の組織（300名以下）



最大ユーザー数だけで
プランを選ばないようにしよう

Microsoft 365のプランのうち、「Business」には最大ユーザー数300名以下という制限があります。これは、300名以下の場合は、必ずBusinessを選ばなければならないという意味ではありません。「Enterprise」は、「E3」「E5」とともに、規模に関係なく利用できるため、300名以下の場合でも、E3やE5の機能が必要な場合は、Microsoft 365 Enterpriseの契約を検討しましょう。



組み合わせて契約できる

Microsoft 365では、異なるプランを組み合わせて契約することもできます。例えば、E3とE5を一定数契約し、コンプライアンス機能が必要な部門のユーザーにはE5を、そうでない部門にはE3を割り当てることができます。これにより、無駄なくライセンスを購入できます。

● 最適なプランの選択で組織がこう変わる

- ・規模だけでなく、使いたい機能で契約できる
- ・組織の課題を解決するための機能を選んで使える
- ・使わないサービスに余計にコストをかけずに済む

▼もっと詳しく知りたいときはこちらへ！

<https://docs.microsoft.com/ja-jp/microsoft-365/enterprise/microsoft-365-overview>

エディションによる機能の違いを確認しよう

Microsoft 365のプランを選ぶときは、自社で実現したい機能が含まれているかどうかを確認することが重要です。例えば、Businessは、E3と使える機能はほぼ同じですが、脅威対策のDevice Guardやアクセス管理のCredential Guard、デバイス管理のWindows Analytics Device Healthといった高度な対策が使えません。

一方、E5には、Windows Defender ATP^{*}やOffice 365 ATPなどの高度なセキュリティ対策、Azure Information Protection P2やCloud App Securityなどの高度な情報保護機能に加え高度なコンプライアンス対策機能が利用可能です。

* ATP=Advanced Threat Protection

● Microsoft 365プラン主要機能比較表

		M365 F1	M365 E3	M365 E5	M365 Business
オペレーション システム のエディション	Windows 10 Enterprise	● ^{*1}	●	●	Windows 10 Business
Office アプリケーション	Office アプリケーション（ローカルにて Word、Excel、Outlook、PowerPoint、OneNote、Publisher、Access の利用が可能）		●	●	●
	Office Online（ブラウザーにて Word、Excel、PowerPoint、OneNote の利用が可能）	● ^{*2}	●	●	●
メールと予定表	Outlook、Exchange	● ^{*3}	●	●	●
チャットベースのワークスペース	Microsoft Teams	●	●	●	●
スケジュールとタスクの管理	Microsoft Teams、PowerApps、Flow	● ^{*4}	●	●	●
音声通信とビデオ会議	Microsoft Teams 電話会議、電話システム	● ^{*5}	●	●	●
ソーシャル & インターネット	SharePoint & Yammer	● ^{*6}	●	●	●
動画共有	Microsoft Stream	● ^{*7}	●	●	●
脅威対策	Windows Defender ウイルス対策、Device Guard	●	●	●	△ ^{*8}
	Windows Defender Advanced Threat Protection、Office 365 Advanced Threat Protection、Azure Advanced Threat Protection			●	
ID とアクセスの管理	Azure Active Directory プラン 1、Windows Hello、Credential Guard と DirectAccess	●	●	●	△ ^{*9}
	Azure Active Directory プラン 2			●	
デバイスとアプリの管理	Microsoft Intune	●	●	●	●
	Windows AutoPilot、Fine Tuned User Experience、Windows Analytics Device Health	●	●	●	△ ^{*10}
情報の保護	Windows 情報保護と BitLocker	●	●	●	●
	Azure Information Protection P1	●	●	●	●
高度なコンプライアンス	Azure Information Protection P2、Microsoft Cloud App Security、Office 365 Cloud App Security			●	
	Office 365 データ損失防止		●	●	●
分析	Advanced eDiscovery、カスタマー ロックボックス、アドバンスト データ ガバナンス、Customer Key、Office 365 特権 ID 管理			●	
	MyAnalytics	● ^{*11}	● ^{*11}	●	● ^{*11}
最大ユーザー数	Delve		●	●	●
	Power BI Pro			●	
最大ユーザー数		なし	なし	なし	300 名まで

*1 : ローカルのみ。詳細については、Microsoft 製品条項を参照してください。^{*2} : Office Mobile アプリを利用できるデバイスは本体画面の対角線長が 10.1 インチ以下のものに限定されます。^{*3} : 2GB 受信トレイ。ボイスメールはありません。

^{*4} : PowerApps はアプリの利用に限りられます。Flow は月 750 ユーザーまでとなります。^{*5} : 会議は参加のみ。1:1 音声/ビデオ通話はサポートされません。デスクトップやアプリの共有機能はありません。^{*6} : サイト管理者になることはできません。サイトメールボックスや個人用サイトは利用できません。フォームの作成はできません。^{*7} : 閲覧のみ、公開と共有は不可。^{*8} : Device Guard なし。^{*9} : Credential Guard なし。^{*10} : Windows Analytics Device Health なし。^{*11} : 今後順次展開予定。

▼もっと詳しく知りたいときはこちらへ！

<https://aka.ms/m365plans>



データセンターは日本にある

Microsoft 365のデータセンターは、世界中で100を超える場所で運用されていますが、日本で契約した場合は、原則、日本のデータセンターでデータが運用されます。このため、日本の法律に準拠した運用ができます。



中小規模向けのクラウドサービスの違いは？

Microsoftが中小規模の環境向けに提供しているクラウドサービスには、Microsoft 365 Businessに加えて、Office 365 Business Premiumもあります。大きな違いは、Microsoft 365には、Windows 10、Windows 10向けの管理機能（AutoPilotなど）、そしてEnterprise Mobility Suiteが含まれることです。詳細な機能の違いは、以下のWebページを参照してください。

▼ Microsoft 365 Businessサービスの説明

<https://aka.ms/m365bsdja>

Point

契約のための準備を進めよう

Microsoft 365を組織導入するには、事前に費用などを検討する必要がありますが、そのとき重要なのがプランの違いです。機能や費用の違いを検討し、どのプランをいくつ契約すればいいのかを検討しましょう。しかしクラウドサービスなら、後から契約を追加したり、逆に減らしたりすることが簡単にできるので、まずは小規模な単位で導入し、次第に組織全体に規模を拡大していくこともできます。

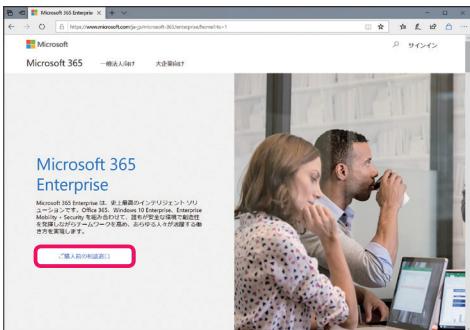
Microsoft 365を使い始めよう

Microsoft 365 テナントの準備

Microsoft 365を使えるようにしましょう。申し込み後、ユーザーを作成し、ライセンスを割り当てることで、各種サービスを使えるようになります。

Microsoft 365の申込み

●Webページから申込み



●Microsoft 365テナントの作成



●管理者ユーザーの作成



ソリューションプロバイダー経由でも購入できる

Microsoft 365は、各種ITサービスを提供するソリューションプロバイダー経由でも購入できます。取引がある会社に問い合わせてみたり、以下のサイトを利用してMicrosoft 365を取り扱っているソリューションプロバイダーを探してみるといいでしょう。

▼ソリューションプロバイダーの検索
<https://aka.ms/partnerja>



組織名を指定しよう

問い合わせ後、申し込みページからMicrosoft 365のテナントを作成します。担当者の氏名、連絡先メールアドレス、組織名などを入力して手順を進めましょう。



必要な設定をウィザードで実行できる

必要な設定がすべて完了していない場合、Microsoft 365の管理ポータルにアクセスすると、「Office 365 Enterprise E5（プラン名は契約に依存）のセットアップは完了していません」というメッセージが表示されます。[設定に移動]をクリックすると、必要な設定をウィザード形式で順番に実行できます。

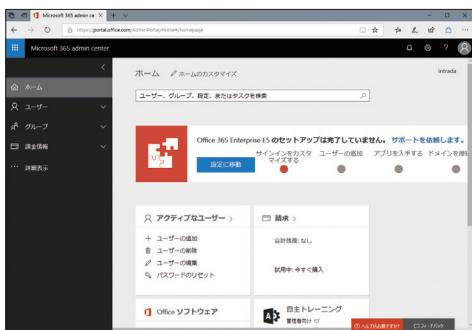
Microsoft 365は、マイクロソフトのから購入できます。まずは、Webページから問い合わせをして、見積もりを取得したり、申し込み方法について相談してみましょう。

問い合わせ後、申し込みページからMicrosoft 365のテナントを作成します。担当者の氏名、連絡先メールアドレス、組織名などを入力して手順を進めましょう。

管理者用のアカウントを作成します。管理者のメールアドレスとして使う名前、組織を識別するための名前、管理者アカウントのパスワードを指定しましょう。

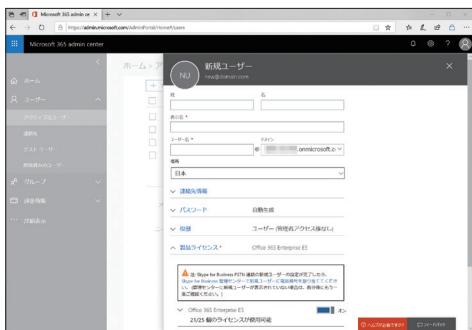
Office 365 のユーザーを作成する

● 管理ポータルへのアクセス



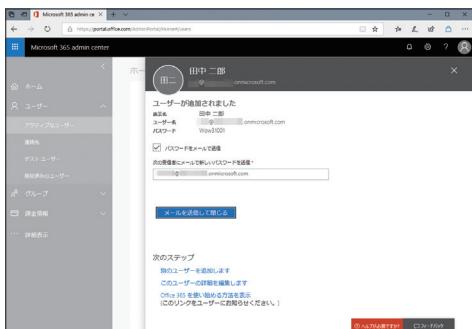
管理者アカウントを作成できたら、「<https://portal.office.com>」から管理ポータルにアクセスします。管理者アカウントでサインイン後、ホーム画面で [管理] をクリックしましょう。

● ライセンスの割り当て



[ユーザー] から新しいユーザーを追加します。ユーザー名などを設定後、[製品ライセンス] を開き、購入済みのライセンスのうち、どのプランを割り当てるかを選びましょう。

● アカウント情報の送信



作成したユーザーの情報はメールで送信できます。現在利用しているメールアドレスを指定してメールを送信しましょう。標準ではパスワードは自動生成された文字列が設定されます。

HINT! ユーザーをまとめて登録するには

[アクティブなユーザー] の画面で [その他] から [+複数のユーザーのインポート] を選択すると、ユーザー情報を記載した CSV ファイルから、複数のユーザーを一括で登録できます。CSV ファイルのサンプルをダウンロードすることもできるので、サンプルを参考にユーザー名などを記載した CSV ファイルを用意して登録しましょう。



HINT! PowerShellでもユーザーを作成できる

Microsoft 365 のアカウントは、PowerShell を使って作成することもできます。コマンドの構文や使い方については次の文書を参照してください。

▼ **Office 365 PowerShell を使用してユーザー アカウントを作成する**
<https://aka.ms/o365psshell>

HINT! ほかのシステムからメールを移行するには

すでに組織で利用しているメールシステムがある場合は、そのメールアカウントを Microsoft 365 に移行することもできます。移行方法については、次の文書を参照してください。

▼ **複数のメール アカウントを Office 365 に移行する方法**
<https://aka.ms/mailmove>

パソコンの準備をしよう

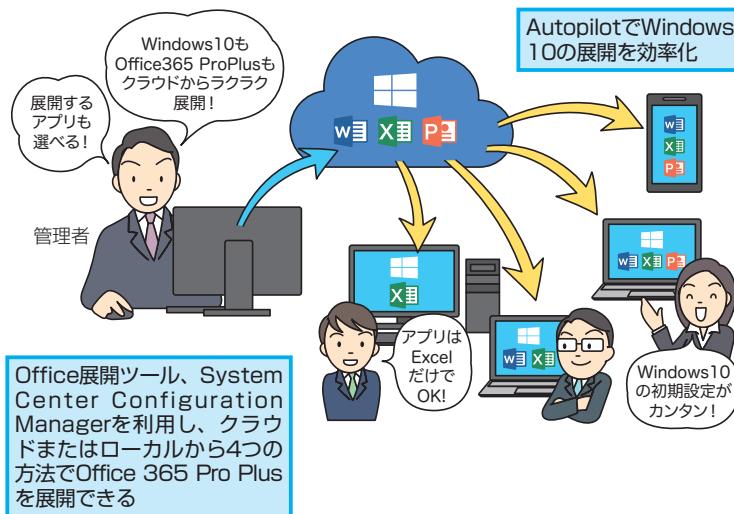
OfficeとWindowsの展開

組織内のPCにWindows 10やOffice 365 ProPlusを展開しましょう。さまざまなツールを使って、自社に合った方法で展開することができます。

デバイスへの展開

●自社に合わせた方法で展開できる

これまで、組織内のデバイスに、適切な設定でOSやアプリケーションを展開するのに大変な労力が必要でした。これに対して、Microsoft 365では、Windows 10やOffice 365 ProPlusを、クラウドなどから手軽に展開できます。Windows Autopilotを利用してWindows 10を組織に合わせて簡単にセットアップしたり、4種類の方法から自社の環境に合った方法を選んでOffice 365 ProPlusをインストールしたりできます。本書では、主にクラウドからのインストールに焦点を当てつつ、さまざまなサービスや展開オプションについて解説します（詳細は次ページ以降）。



●Microsoft 365でデバイスの準備がこう変わる

- ・最新のWindowsやOfficeを簡単に展開できる
- ・インストールソースやバージョンなどをカスタマイズできる
- ・ユーザーがインストールや初期設定を短時間かつ簡単にできる

▼もっと詳しく知りたいときはこちらへ！

<https://aka.ms/deployo365pp>



Macの場合は？

Microsoft 365には、Office for Macのライセンスも含まれています。Mac OSを搭載したクライアントデバイスにOffice for Macを展開するには、社員にインストーラーパッケージファイルを提供して、自分自身でインストールしてもらうか、インストーラーパッケージファイルをローカルネットワークにダウンロードしてから、ソフトウェア配布ツールを使用して組織内のMacに展開します。



インストールをカスタマイズできる

Office展開ツールを利用すると、Office 365 ProPlusのどのエディション（32ビット/64ビット）をインストールするか、WordやExcelなどのアプリをインストールすか、言語はどうするか、更新をどれくらいの頻度で実施するなどをカスタマイズできます。詳しくは次ページを参照してください。



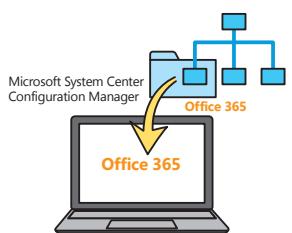
Office Mobileの商用利用もできる

スマートフォンやタブレット向けに提供されているOffice Mobileは、無料版も提供されていますが、無料版は商用利用が許可されてません。これに対して、Microsoft 365に加入している場合は、Office Mobileの商用利用ができるため、ビジネス文書を表示したり、編集ができます。外出先での作業や移動中の確認などに便利です。

Office 365 ProPlusの展開

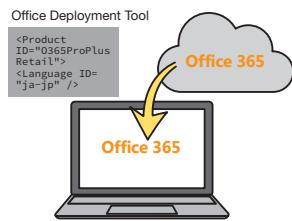
●4つの展開方法から選べる

Office 365 ProPlusを組織内のデバイスに展開する方法は4つあります。違いは、利用する展開ツールとインストールソース（どこからインストールするか）です。大規模な環境ではSystem Center Configuration Managerを利用する場合もありますが、使えない場合でもコマンドベースのOffice展開ツールで、インストールするエディションや言語、インストールソースなどをカスタマイズできます。インストールソースは、組織内の配布ポイント（共有フォルダーなど）、またはクラウドを選択できます。



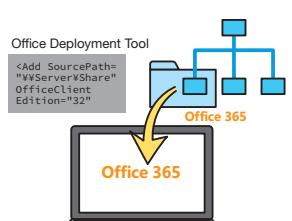
●System Center Configuration Managerでローカルソースから展開

System Center Configuration Managerを使用して展開を管理し、組織内ネットワークの配布ポイントからOffice 365 ProPlusを展開する



●Office展開ツールでクラウドから展開

Office展開ツールを使用して、クラウド（Office CDN）からデバイスにOfficeを直接インストールする



●Office展開ツールでローカルソースから展開

Office展開ツールを使用して、ネットワーク内の共有フォルダーなどからデバイスにOffice 365 ProPlusをインストールする



●クラウドからセルフインストール

ユーザーがMicrosoft 365のポータルから各自のデバイスにOffice 365 ProPlusをインストールする

▼もっと詳しく知りたいときはこちらへ！

<https://aka.ms/plano365pp>

HINT! System Center Configuration Managerって何？

System Center Configuration Managerは、デバイスの構成情報やソフトウェアの展開、更新管理、モバイルデバイスマネジメントなどを一元管理できるマイクロソフトのソリューションです。ほかの目的で導入済みの場合は、Microsoft 365と組み合わせて、Windows 10やOffice 365 Pro Plusの展開、更新管理に利用できます。

HINT! Office展開ツールって何？

Office展開ツールは、Office 365 Pro Plusのインストールを詳細に制御できるコマンドラインツールです。インストールソースの場所、アーキテクチャ(32ビット/64ビット)、更新チャネル(レッスン⑦参照)、言語、インストール時のユーザーインターフェース表示の有無、などを構成ファイル(xmlファイル)に記述することができます。

▼Office展開ツールの概要

<https://aka.ms/odtjp>

▼Office 365 ProPlus展開ガイド

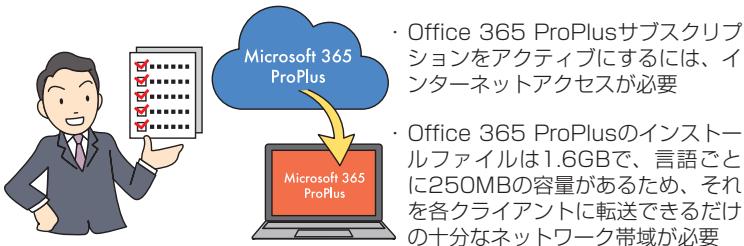
<https://aka.ms/odtman>

次のページに続く

展開の準備

●インフラストラクチャの確認

Office 365 ProPlusを展開するときは、デバイスの数や環境を確認することも大切ですが、組織内のネットワークに十分な帯域があるかを確認しておくことも重要です。特に、Office 365 ProPlusのインストールファイルはおおむね2GB弱あるため、クラウドからインストールする場合、複数台からの同時インストールで業務で必要なインターネットアクセスに支障が発生することもあります。



▼もっと詳しく知りたいときはこちらへ！

<https://docs.microsoft.com/ja-jp/deployoffice/assess-office-365-proplus>

●アプリケーション互換性の評価

デバイスにWindows 10やOffice 365 ProPlusをインストールしたときに、どのような影響があるかは慎重に評価する必要があります。Desktop Analyticsを利用すると、こうした作業の時間と労力を省くことができます。組織内で使われているアプリの一覧を作成したり、互換性を評価できるため、展開時のトラブルを減らし、安心してWindows 10やOffice 365 ProPlusを展開できます。

◆Desktop Analytics

アプリの調査

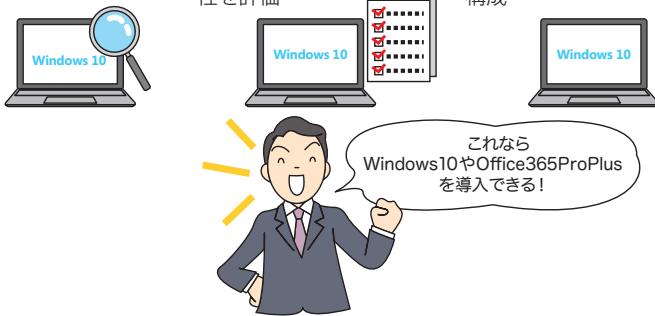
組織内で実行されているアプリの一覧表を作成

互換性の評価

Windows 10とOffice 365 ProPlusの最新の機能更新プログラムと既存アプリケーションの互換性を評価

パイロットグループの作成

最小限のデバイスで、すべてのアプリケーションとドライバーをカバーするパイロットグループを構成



▼もっと詳しく知りたいときはこちらへ！

<https://aka.ms/moderndesktopjp>

HINT! Office 365 ProPlusのインストール要件

Office 365 ProPlusのインストールには、次のスペックを満たすPCが必要です。インストール前に、組織内のPCのスペックも確認しておきましょう。

- 1.6 GHz 以上、2コアのプロセッサ
- 4GB RAM
- 4.0GBの使用可能ディスク領域
- 1280 x 768の画面解像度

HINT! Desktop Analyticsとは

Desktop Analyticsは、これまでに提供されていたWindows Analyticsを拡張したクラウドサービスです。これまでにも、アップグレード対象のWindowsから収集したデータを分析し、アップグレードの準備に関するレポートや問題点、推奨情報などを参照できましたが、Desktop Analyticsでさらにアプリの一覧作成や互換性を評価する機能などが追加されました。

HINT! Office 365 ProPlusの互換性をチェックできる

Office 365 ProPlusを組織内に展開するときは、あらかじめ互換性をチェックしておくことを推奨します。現在のバージョンで利用しているVBAマクロやアドインがOffice 365 ProPlusでも動作するかどうかは、「準備ツールキット」を利用することで確認できます。

▼準備ツールキット

<https://aka.ms/office365compatibility>

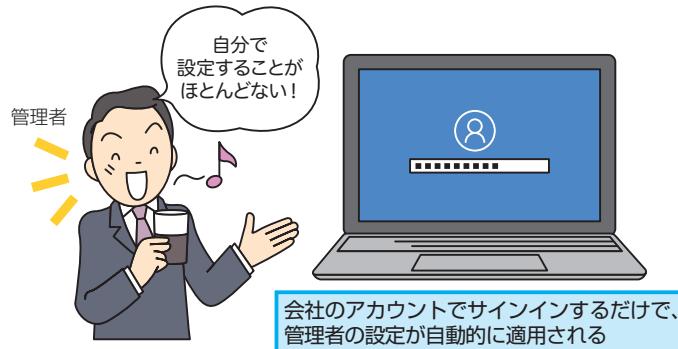
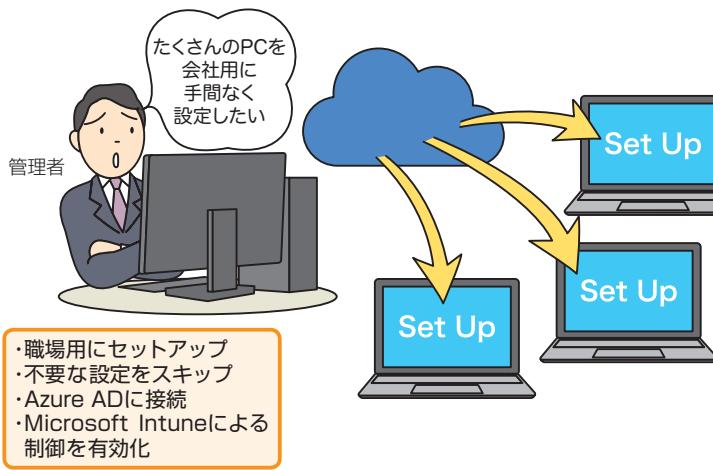
▼Office 365 ProPlus 展開ガイド

<http://aka.ms/odtman>

Windows AutopilotによるWindows 10の展開

●組織向けに自動的に構成できる

Windows Autopilotは、Windows 10を組織内に展開するための各種設定を自動的に構成できるクラウドベースのソリューションです。従来、組織内にデバイスを展開するには、あらかじめ組織向けにカスタマイズしておいたイメージを展開するなどの手間が必要でしたが、Windows Autopilotでは、クラウドから簡単な設定をするだけで、デバイスに組織向けの設定を自動的に適用することができます。管理者の手間を省けるだけでなく、ユーザーも、言語とキーボード、Microsoft 365のアカウントなど、最低限の情報を入力するだけで、セットアップを完了させることができます。



●Windows AutopilotでWindows 10の展開がこう変わる

- ・Windows 10の初期設定を自動的に組織向けに構成できる
- ・クラウドでの設定だけで簡単に組織向けの構成ができる
- ・ユーザーが初期設定で入力する項目を少なくできる

▼もっと詳しく知りたいときはこちらへ！

<https://docs.microsoft.com/ja-jp/microsoft-365/enterprise/windows10-deploy-autopilot>



どんな設定を構成できるの？

Windows Autopilotでは、次のような構成が可能となっています。また、初期設定の項目 (OOBE) のうち、組織に必要なないものをスキップすることもできます。

- ・デバイスをAzure Active Directory (Azure AD) に自動的に参加させる
- ・デバイスをMicrosoft IntuneなどのMicrosoft Intuneサービスに自動的に登録する(Azure AD Premium サブスクリプションが必要)
- ・管理者アカウントの作成を制限する
- ・構成グループごとにデバイスを管理できる
- ・初期設定で表示する項目(OneDrive、Cortana、プライバシー設定など)をカスタマイズできる



Windows 10が対象

Windows Autopilotで構成できるデバイスには、バージョン 1703以降のWindows 10 Professional、Enterprise、またはEducationがブレインストールされている必要があります。条件に当てはまらないデバイスがあるときは、あらかじめアップグレードしておきましょう。

Point

簡単に組織向けの構成ができる

Microsoft 365には、組織で使うデバイスを準備するためのさまざまな機能が用意されています。エディションや言語を指定してOffice 365 ProPlusをクラウドからインストールできるように構成したり、Azure Active Directoryに参加する構成でWindows 10をセットアップしたりと、本来、時間と手間が必要だった各種展開作業をクラウドベースで自動的に実行できます。デバイスの準備やセットアップに時間がかかるなくなることで、管理者はもちろん、ユーザーも、より生産的な仕事に時間を割けるようになるでしょう。

より安全に活用するには [外部脅威対策]

統合ソリューション

高度化するセキュリティ被害から、組織のデバイスを保護するはとても重要です。Microsoft 365でどのような対策ができるのかを見てみましょう。

マイクロソフト インテリジェント セキュリティ グラフ

●受け身的な対処から積極的な備えに

「本物と見分けが付かない巧妙な偽メール」「脆弱性を悪用した悪質な攻撃」など、日々、高度化する脅威に対抗するためにマイクロソフトが作り上げたのが「マイクロソフト インテリジェント セキュリティ グラフ」です。マイクロソフト インテリジェント セキュリティ グラフは、世界中の約12億台のWindowsデバイス、クラウドサービスから得られる毎月4,500億件の認証と4,000億通のメールなどを集約し、1日あたり6兆5,000億件以上のシグナルを人工知能(AI)や行動分析を活用しながら、セキュリティ脅威の状況をリアルタイムに分析した知見です。Microsoft 365はもちろんのこと、マイクロソフトの製品・サービスのセキュリティ強化に活用されています。



最新の脅威について学ぼう

マイクロソフトでは、マイクロソフト インテリジェント セキュリティ グラフの情報などを元に、最新の脅威について解説する「セキュリティインテリジェンスレポート」を公開しています。最新の脅威について知っておくことも重要なことで、目を通しておくといいでしょう。

▼セキュリティインテリジェンス レポート

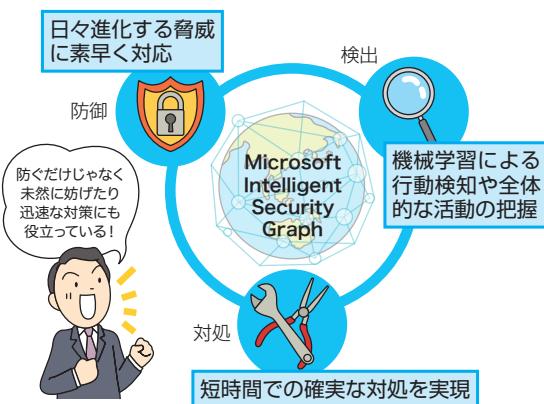
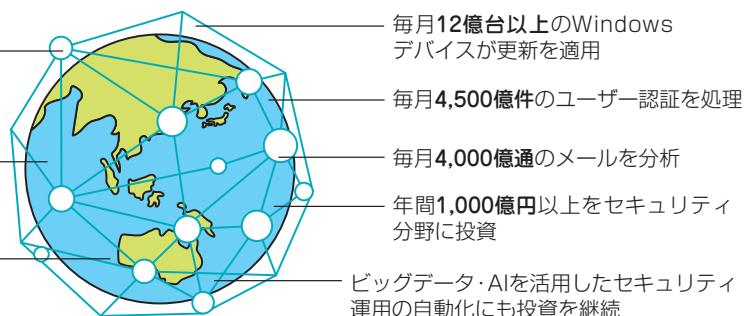
<https://aka.ms/sirja>

●地球規模でのセキュリティの知見 ~インテリジェント セキュリティ グラフ~

2,000万社以上の企業、10億人以上のユーザーなど、ビジネス・コンシューマ双方にクラウドサービスを提供

検索エンジンを通じて毎月18億以上のWebページをスキャン

マイクロソフト社としても、全世界13万ものユーザーを常に最新のセキュリティで保護



●マイクロソフト インテリジェント セキュリティ グラフでセキュリティ対策がこう変わる

- 日々進化する高度な脅威に常に最新のセキュリティ対策で対応
- 全世界のデータで守られるため、よりプロアクティブなセキュリティ対策が可能
- 発生したセキュリティ侵害に対して自動修復が可能

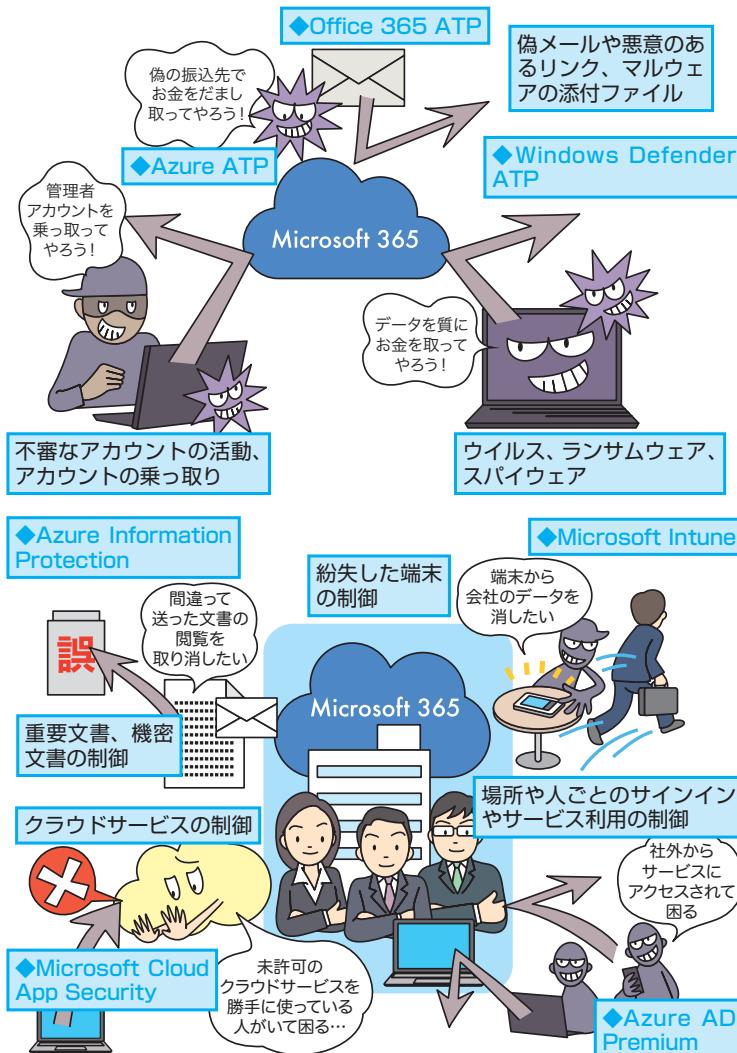
▼もっと詳しく知りたいときはこちらへ！

<https://aka.ms/intelisec>

Microsoft 365のセキュリティ対策機能

●統合的なソリューションを提供

Microsoft 365では、組織に必要なセキュリティ対策機能をトータルで提供することで、複雑になりがちなセキュリティ対策をシンプルに利用することができます。外部からの脅威に対抗するための機能だけでなく、内部からの情報漏えいやコンプライアンス違反を防ぐための機能も備え、全方位で組織の安全性を確保できます。



●Microsoft 365でセキュリティ対策がこう変わる

- ・エンドポイントデバイスからアプリ、IDまでトータルで対策可能
- ・拡散範囲が広く、しかもスピードの速い最新の脅威にも対応可能
- ・生産性を犠牲にせずに高い安全性を実現できる

▼もっと詳しく知りたいときはこちらへ！

<https://www.microsoft.com/ja-jp/security/>

HINT! セキュリティ被害が大きな損失を招くことも

セキュリティ被害は、ときに組織にとって大きな損失を招くこともあります。国内の組織でも、実際に取引先からを装った偽メールで巨額の費用を偽口座に振り込ませた事例や、大量の個人情報の流出によって謝罪や賠償に発展した事例も多くあります。他人事と考えず、冷静に現在のセキュリティ対策状況を見直すことが重要です。

HINT! 生産性とのバランスが重要

セキュリティ対策は、生産性とのバランスを考慮して導入しましょう。情報漏えい対策を防ぐために、文書の保護設定を厳しくし過ぎると、情報の共有や外部とのやりとりがしにくくなります。バランスを考慮して、実際に利用する機能や設定の検討が重要です。

HINT! 拡散の範囲とスピードが拡大

近年のセキュリティ被害は、その被害が拡散する範囲が広く、スピードも速いのが特徴です。1台の被害が、複数台へと広がり、さらにサーバーなどの基幹部分にも短時間で拡散します。被害をなるべく早く発見し、その拡散を食い止めることが重要です。

次のページに続く

Microsoft 365の多層防御

●Office 365 ATP + Windows Defender ATP + Azure ATP

Microsoft 365では、複数のセキュリティ対策を組み合わせた多層防御を実現できます。例えば、標的型攻撃のように、偽メールによる誘導から、デバイスへのマルウェア感染を経て、別のユーザーアカウントを乗っ取りながら、さらにネットワークの奥深くへと侵入しようとする手口に対しても、Office 365 ATPでメールを利用した攻撃を防御し、Windows Defender ATPでデバイスへの攻撃を防御し、Azure ATPでIDへの攻撃を防御するといったように、複数の機能を使って、それぞれの段階で侵入を防げます。



●多層防御で高度な攻撃への対処がこう変わる

- ・メール、デバイス、IDのそれぞれを保護
- ・被害の拡大を段階的に防げる
- ・高度な攻撃への対処が可能

HINT! 多層防御って何？

多層防御は、幾重もの対策によって段階的にセキュリティ被害を防ぐ方法のことです。単に、セキュリティ対策を複数設置するのではなく、それぞれの段階で視点の異なる対策（メール、デバイス、IDなど）を実施することで、仮に1つの壁を突破されたとしても、次の壁で阻止することで、攻撃が成功する確率を下げることができます。攻撃の手口が高度化する現代に必要とされるセキュリティ対策の考え方となっています。

HINT! 一部の被害しか見えていないケースも

仮に今、組織にあるデバイスの1台で、ウイルスが発見されたとしましょう。これは、単にそのデバイスだけが感染したものでしょうか？ それとも段階的な攻撃の一部でしょうか？ また、このデバイス1台だけでしょうか？ それともほかのデバイスにも広がっているのでしょうか？ 個別のセキュリティ対策ソリューションでは、こうした被害の全体像を把握するのは困難です。これに対して、Microsoft 365では、組織全体の対策状況や被害の状況を把握できるため、発生したインシデントに対して、より確実な対処を実施することができます。

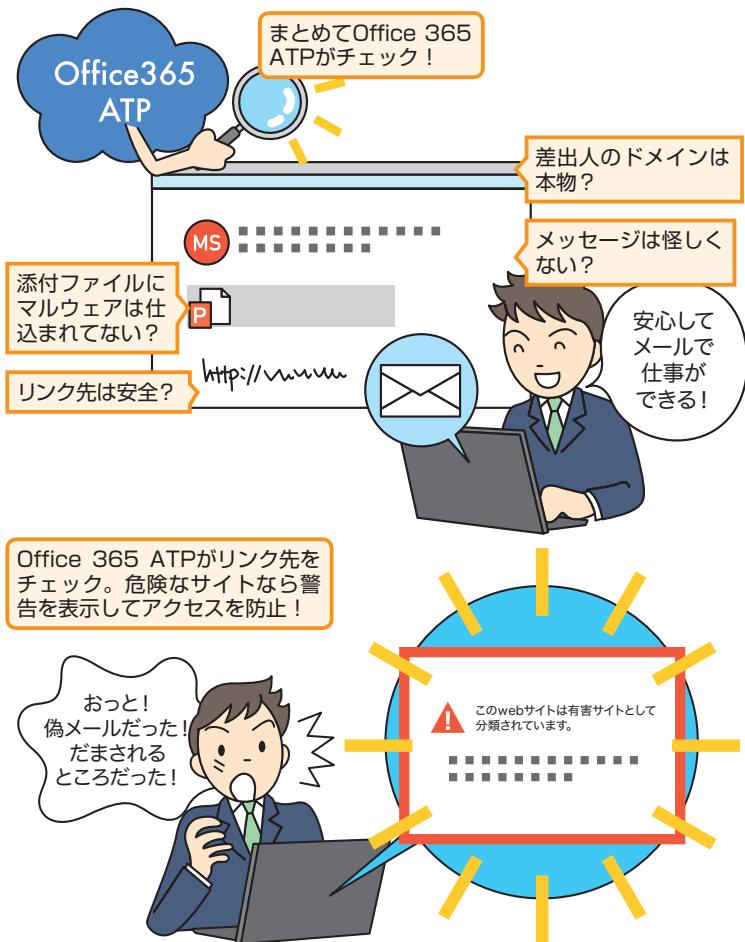
HINT! 人の目では判断が難しい巧妙な手口

「偽メールであることくらい見れば分かるだろう……」。そう思う人も少なくないかもしれません。しかし、実際に見破ることは簡単ではありません。過去の被害の例では、犯人が偽メールを送る前から、システムへと侵入し、実際に何通ものメールのやりとりを盗み見することで、取引先の人物になりました例もありました。人の目だけで判断することは難いため、リンク先がどこにつながるのか、添付ファイルの中身は何かを確実にチェックできる仕組みが必要です。

Office 365 ATPによる保護

●メールのリンクや添付ファイルをチェック

多層防御の言わば「入り口」を守る役割を担うのがOffice 365 ATPです。メールの安全性を確保するための機能となっており、メール内のリンクや添付ファイルを事前にチェックしたり、なりすましを検知する技術によって偽メールや偽装されたドメインを検知できます。サンドボックスを利用したチェックが実行可能なため、未知の脅威も検知できるのが特徴です。



●Office 365 ATPでメールの安全性がこう変わる

- ・本物そっくりの偽メールも判断可能
- ・リンクや添付ファイルをユーザーが開く前にチェック
- ・未知の脅威にも対応可能

▼もっと詳しく知りたいときはこちらへ！

<https://docs.microsoft.com/ja-jp/office365/securitycompliance/office-365-atp>

HINT! サンドボックスって何？

Office 365 ATPでは、添付ファイルのチェックなどにサンドボックスを利用します。サンドボックスは、セキュリティチェック用の隔離された環境です。仮想環境で稼働するOS上で、実際に添付ファイルを実行することによって、添付ファイルに危険がないかを確かめることができます。これにより、まだ定義ファイルがない未知のマルウェアなども検知できます。

HINT! レポートで被害状況を確認できる

Office 365 ATPでは、保護状況をレポートで表示することもできます。マルウェアやフィッシングと考えられるメールが何通やりとりされ、そのうちのどれくらいを破棄したか、組織内の誰が標的となっているか、誰がいつ危険なリンクをクリックしたなどを確認することができます。

HINT! 攻撃シミュレーターも利用できる

Microsoft 365では、攻撃シミュレーターと呼ばれるサービスも利用できます。Office 365脅威インテリジェンスに含まれる攻撃シミュレーターは、フィッシング攻撃やパスワード攻撃などが、実際にどのように実行されるのかを体験できるシミュレーターです。組織のセキュリティ対策状況をチェックしたり、攻撃に対する訓練をしたいときなどに活用できます。

▼攻撃シミュレーター

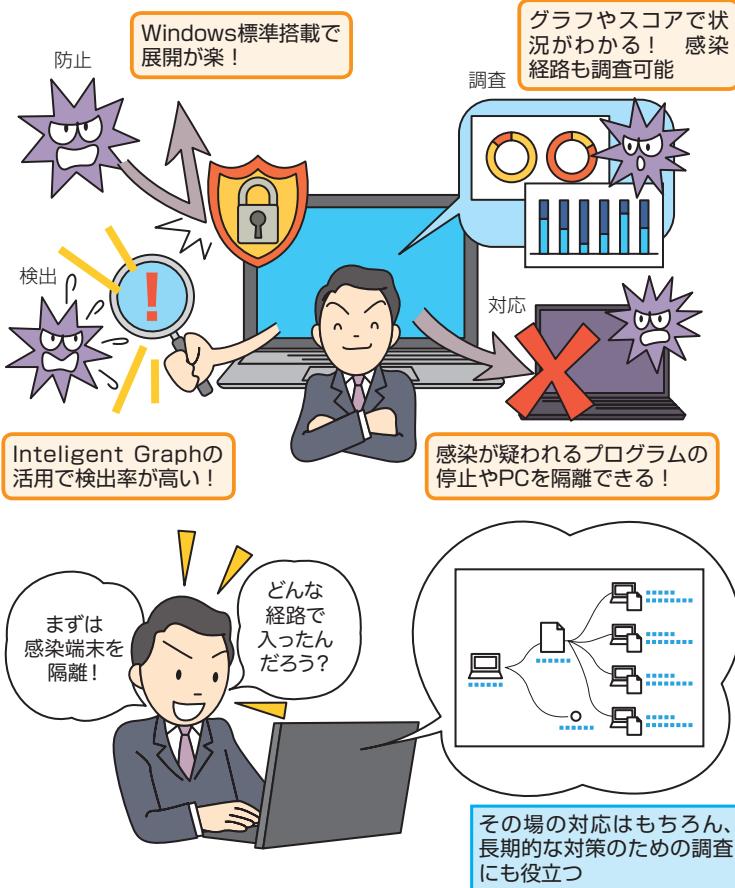
<https://aka.ms/o365attacksimm>

次のページに続く

Windows Defender ATP

●マルウェア対策+インシデント対処が可能

ユーザーが利用するデバイスを保護する役割を担うのがWindows Defender ATPです。Windows 10には、デバイスをマルウェアから保護するWindows Defenderが標準搭載されていますが、Microsoft 365では、さらに高度な対策が可能なWindows Defender ATPを利用可能となっており、組織内のデバイスの挙動を監視し、セキュリティインシデントが発生したデバイスの隔離や停止などの対策もできるようになっています。



●Windows Defender ATPでエンドポイント対策がこう変わる

- ・Windows 10標準機能で高度な対策が可能
- ・対策状況やインシデントの状況を把握できる
- ・発生したインシデントに対して自動的な対処（隔離など）が可能

▼もっと詳しく知りたいときはこちらへ！

<https://aka.ms/wdatpja>



エンドポイントって何？

エンドポイントは、ネットワークにつながれたデバイスの総称です。一般的には、組織内に設置されたPCやユーザーが使うスマートフォンなどを指します。



インシデントって何？

インシデントは、情報の安全性を脅かす確率の高い事象のことです。マルウェアへの感染、不正アクセスなどはもちろんのこと、端末の紛失や盗難、重要な情報の誤送信などを指します。



対策を自動化できる

セキュリティ対策は、さまざまな機能を導入することも大切ですが、導入後に、正常性を監視したり、万が一のインシデントに実際に対応したりすることの方が重要です。しかしながら、日常業務の中で、管理社自らが、大量的ログやアラートをチェックするのは困難です。Windows Defender ATPでは、このような監視や対処を管理者の代わりに実行する自動化機能を備えており、マルウェアに感染した端末を検知するだけでなく、修復するまでを自動化することもできます。

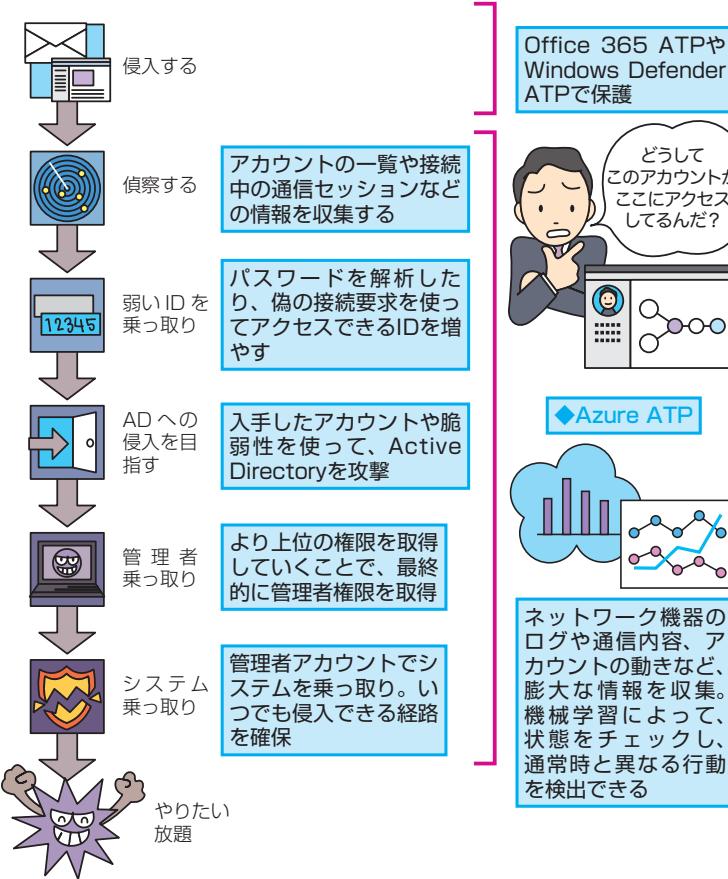
▼自動調査機能の詳細

<https://aka.ms/wdatpauto>

Azure ATPによる保護

●IDの保護

Azure ATPは、組織のシステムのより深い部分を保護することができるソリューションです。メールなどからデバイスへの侵入を果たした攻撃者は、サーバーやデータベースなどにあるより重要な情報を狙って活動します。侵入したデバイスから、組織内の環境を丹念に調査し、次々とユーザー アカウントやデバイスを乗っ取りながら、最終的には管理者権限を取得してシステムを乗っ取り、いつでも外部から侵入できる経路を開いておくなどの工作をします。Azure ATPでは、ネットワークの通信やアカウントの行動を監視、AIによる分析によって、不審な活動を検知することができます。メールやデバイスへの攻撃が、さらなる深刻な被害に達することを防止できます。



HINT! 被害状況を見やすく表示できる

通常、深い階層への攻撃を検知したり、万が一、攻撃された場合の原因を探るには、ネットワーク機器のログや通信内容、サーバーのログなど、個別の機器の情報を大量にチェックする必要があります。しかし、Azure ATPでは、こうした情報を自動的に収集し、見やすく表示できます。これにより、攻撃経路をタイムラインで表示するなど、被害状況を用意に把握できます。

HINT! どのような攻撃を検知できるの?

Azure ATPでは、Active Directoryに対する攻撃や、それに関連する不審な活動を検知できます。例えば、メモリーに残る過去の認証情報を悪用する「Pass-The-Hash」や「Pass-The-Ticket」、半永久的に有効な管理権限の認証チケットを悪用する「ゴールデンチケット」などの攻撃を検知できます。また、攻撃の調査のために実施されるディレクトリサービス列挙、SMBセッション列挙、DNS偵察などを検知したり、乗っ取ったデバイスからさらに別のデバイスへと攻撃範囲を広げるための水平・垂直ブルートフォース攻撃なども検知できます。

Point

誰もが使いこなせる高度なセキュリティ対策

現代の高度化した脅威の状況を考えると、外部の攻撃から組織を守るには、複数の対策を組み合わせた多層防御が不可欠です。しかし、こうした対策は、コストが高く、導入も管理も難しいというのが、これまでの常識でした。Microsoft 365では、メール、デバイス（エンドポイント）、IDと多層的な防御を実現しながら、それらの設定をクラウド上のポータルから一元管理でき、インシデントを素早く検知したり、その対応の自動化まで可能です。高度でありながら、誰もが使いこなせます。

●Azure ATPでID保護がこう変わる

- ・アカウントの不審な活動を検知
- ・より深い階層への攻撃や深刻な被害を未然に防げる

▼もっと詳しく知りたいときはこちらへ！

<https://docs.microsoft.com/ja-jp/azure-advanced-threat-protection/what-is-atp>

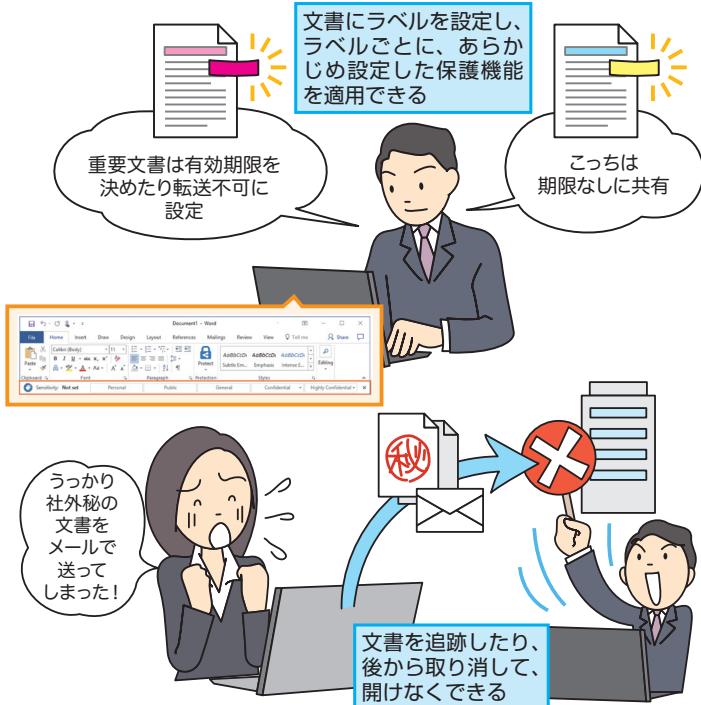
より安全に活用するには 【情報保護対策】

Azure Information Protection、Azure AD Premium、
Microsoft Cloud App Security、Microsoft Intune

Azure Information Protection

●ラベルで分類して重要な文書を追跡

組織で扱われる文書の中には、外部に出すことができない重要な文書が少なからず存在します。こうした文書を保護できるのがAzure Information Protectionです。普段使っているWordやExcelで「Confidential」などのラベルを文書に設定すると、その情報を元にクラウド上で設定したルールが文書が適用され、組織外に送信されることを防いだり、内容をコピーすることを禁止できます。うっかりメールで送信してしまった重要な文書を後から開けなくすることもできるので、情報をしっかりと保護できます。



●Azure Information Protectionで文書管理がこう変わる

- ・ラベルを設定するだけで情報保護のルールを文書に適用できる
- ・文書を追跡したり、送信したメールの閲覧を後から禁止できる

▼もっと詳しく知りたいときはこちらへ！

<https://docs.microsoft.com/ja-jp/azure/information-protection/what-is-information-protection>

組織の大切な情報を守ることができるのも、Microsoft 365のメリットの1つです。どのように情報を守れるのかを見てみましょう。



どんな制限ができるの？

Azure Information Protectionでは、さまざまな制限を設定できます。例えば、表示、保存、印刷、コピー、転送などのアクセス許可を設定できます。また、文書にアクセスできる期限を設定したり、文書に「社外秘」などのヘッダーやフッター、透かしを自動的に追加することなどもできます。



ユーザーの操作は簡単

ラベル設定などの操作は、WordやExcel、PowerPoint、Outlookなどのアプリに加えて、エクスプローラーからも設定できます。このため、ファイルを開くことなく、文書を保護することもできます。



ラベルを自動的に設定できる

文書の中に含まれるキーワードを指定することで、文書に自動的にラベルを設定することもできます。例えば、クレジットカード情報が含まれる文書を保存するだけで、自動的「Confidential」のラベルを設定することなどもできます。



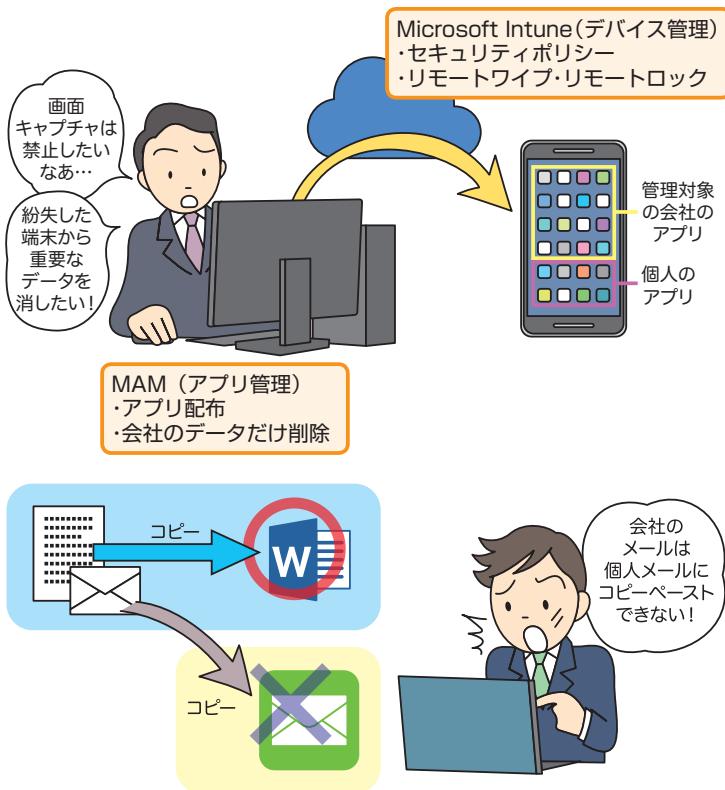
文書を取り消しても削除されるわけではない

Azure Information Protectionは、文書に対するアクセス権限をクラウド上で管理するサービスです。このため、メールで送信した文書を後から取り消したとしても、その文書自体が削除されるわけではなく、アクセスが禁止されるという動作になります。

デバイス管理

●デバイスの紛失や情報漏えいに備える

スマートフォンやモバイルPCは、外出先でも仕事ができる便利な道具ですが、その一方で盗難や紛失によって、組織の情報が危険にさらされる可能性が常に潜んでいます。こうした危機に備えることができるのが、Microsoft 365に含まれるMicrosoft Intune機能です。デバイスにパスワードを強制したり、万が一の盗難時に遠隔操作でデータを削除することができます。さらに、アプリの管理ができるのも特徴で、アプリを配布したり、端末内のデータを組織のデータと個人のデータに区別することで、組織のデータが個人のアプリにコピーされることを防いだり、組織のデータだけを遠隔操作で削除することもできます。



●Microsoft Intuneでデバイスの管理がこう変わる

- ・スマートフォンやモバイルPCを一元管理できる
- ・紛失や盗難時に遠隔操作でデータを削除できる
- ・組織のデータと個人のデータを区別してさまざまな管理ができる

▼もっと詳しく知りたいときはこちらへ！

<https://aka.ms/msintunejp>

HINT! 組織のデータの削除って どういうこと？

組織によっては、個人が所有するスマートフォンを業務に利用している場合もあります。このような場合でも、業務で使う組織のアプリを区别して管理できるのがMicrosoft Intuneの特徴です。紛失時はもちろんのこと、退職した場合などでも、個人のデータは残したまま組織のアプリだけを削除できます。

HINT! リモートロックや リモートワイプができる

スマートフォンやモバイルPCを紛失した場合、物質的な損失よりも深刻なのが、情報漏えいの被害です。万が一、大量の顧客情報などが含まれていれば、組織の存続を揺るがす深刻なインシデントにもなりかねません。遠隔操作でデバイスを操作できないようにロック「リモートロック」やデバイスのデータを削除できる「リモートワイプ」の機能を活用しましょう。

HINT! デバイスの制限や Wi-Fiの設定などもできる

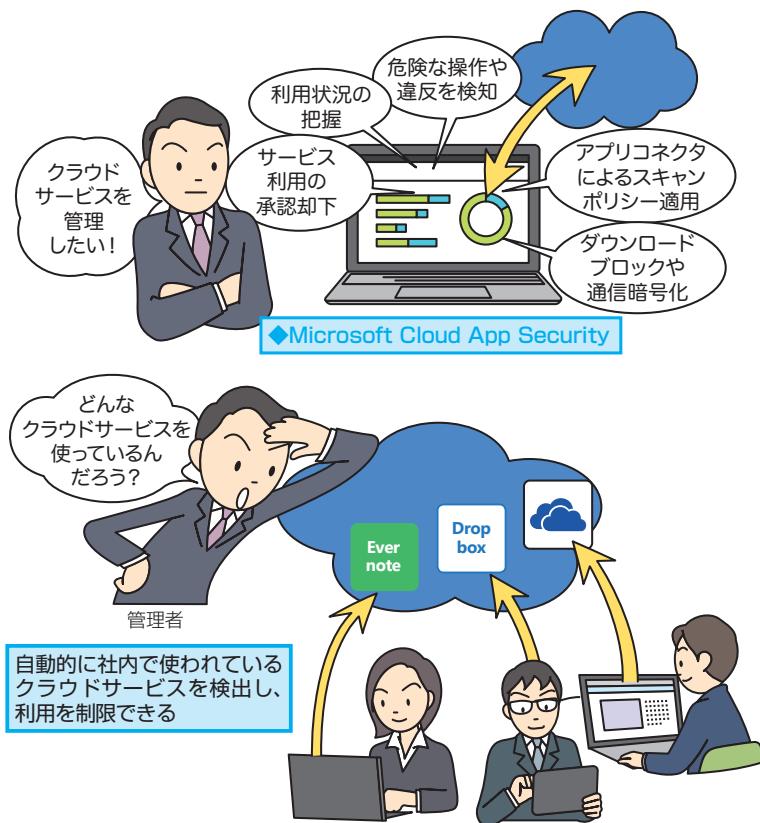
デバイスの構成管理に利用することもできます。パスワードの最小文字数を設定したり、画面のキャプチャを禁止することができます。また、スマートフォンが組織のWi-Fiに接続するための設定情報や、外出先から組織のネットワークに接続するためのVPNの設定情報をプロファイルとして配信することもできます。

次のページに続く

Microsoft Cloud App Securityによるクラウドサービスの管理

●クラウドサービスを可視化して制御

クラウドサービスは、組織の生産性を向上させるのに役立つものですが、組織のルールを外れて個人が勝手にサービスを利用すると、それが情報漏えいなどのリスクにつながる可能性もあります。これまで、組織の誰がどのサービスを使っているのかを把握するのは困難でしたが、Microsoft 365のMicrosoft Cloud App Securityを利用することで、誰がどのサービスをいつ使っているのかを可視化し、そのリスクまでも評価できます。もちろん、その利用の承認や却下もできるため、組織が無法地帯になってしまふことを防止できます。



●Microsoft Cloud App Securityでクラウドサービスの管理がこう変わる

- ・組織で利用しているクラウドサービスを可視化できる
- ・クラウドサービスの利用を承認、却下できる
- ・ポリシーで自動的に利用を制御できる

▼もっと詳しく知りたいときはこちらへ！

<https://docs.microsoft.com/ja-jp/cloud-app-security/what-is-cloud-app-security>

HINT! どうやってサービスを特定するの？

Microsoft Cloud App Securityでは、Cloud Discoveryと呼ばれる機能によって、クラウドサービスを特定します。組織に設置されているファイアウォールやプロキシのログをCloud Discoveryにアップロードすることで、組織で利用されているクラウドサービスを分析します。

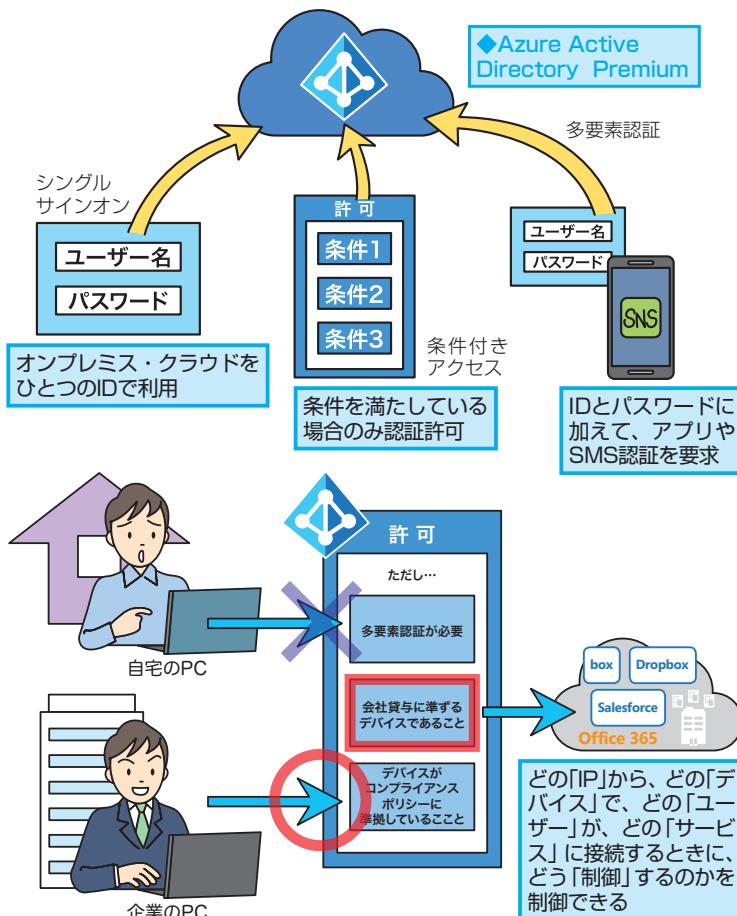
HINT! APIを使ってクラウドサービスを安全に使うこともできる

Microsoft Cloud App Securityでは、クラウドサービスが提供するAPI経由でのアクセスもサポートします。これにより、より詳細なクラウドサービスの利用状況を把握したり、やりとりされるデータをスキャンして問題を発見することができます。

Azure AD Premiumによる条件アクセス

●リソースへのアクセス方法の制御

クラウドのメリットは、場所やデバイスを問わず、組織のデータにアクセスできることです。しかし、利用するアプリや扱うデータによっては、こうした自由をすべて認めてしまうのはリスクにつながる可能性があります。そこで、活用したいのが、Azure AD Premiumで提供される「条件付きアクセス」です。条件付きアクセスは、Azure ADによるユーザー認証に、文字通り、条件を付け加えることができる機能です。例えば、特定のアプリを使うときを条件に多要素認証を義務付けたり、社内の別のフロアなど場所を条件に業務アプリへのアクセスを禁止することなどができます。



●条件付きアクセスでID保護がこう変わる

- ・特定のサービスや特定の場所での認証を強化できる
- ・特定のデバイス（OS）やアプリからのアクセスを制限できる

▼もっと詳しく知りたいときはこちらへ！

<https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/overview>

HINT! アカウントは Azure ADで管理される

Microsoft 365では、アカウントがクラウド上のAzure ADで管理されます。Azure ADを利用するとWindows 10へのサインインやOffice 365の利用など、複数のサービスをシングルサインオンで使えるうえ、多要素認証や条件付きアクセスを使ってアカウントのセキュリティを高めることができます。

HINT! どんな条件が使えるの？

条件付きアクセスでは、「ユーザーとグループ」「クラウドアプリ」「サインインリスク（サインインに失敗したアカウントなど）」「デバイスプラットフォーム」「デバイスの状態（Azure ADに参加しているかどうかなど）」「場所」「クライアントアプリ」などを条件として、認証をコントロールすることができます。

HINT! サインインリスクの高いユーザーを検出できる

Azure ADでは、サインインに失敗したユーザーなど、リスクが高いと思われるアカウントの一覧を「リスクのフラグ付きユーザー」として表示できます。この情報を元に、条件付きアクセスで、リスクの高いユーザーに多要素認証を要求するなどの設定ができます。

Point

高度な情報漏えい対策が手軽にできる

内部からの情報漏えい対策は、まだあまり進んでいない組織が多いかもしれません。しかし、Microsoft 365を利用すれば、まとめて対策することができます。Azure Information Protectionを使った文書のアクセス制御、Microsoft Intuneによるデバイス制御、Microsoft Cloud App Securityによるクラウドサービス制御、Azure ADの条件付きアクセスによるID制御を組み合わせて、情報を守るためにの対策をしておきましょう。

安全性を維持するために必要な更新の管理

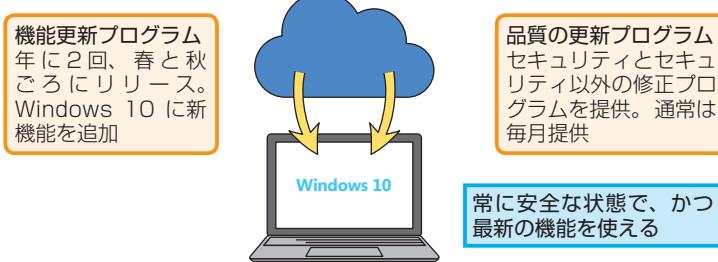
WindowsとOffice 365 ProPlusの更新

組織のデバイスを安全に使うには、Windows 10やOffice 365 ProPlusを常に最新の状態に保つことが重要です。更新の展開方法を見てみましょう。

WaaS

● Windowsの更新

Windows 10は、「Windows as a Service (WaaS)」という新しい考え方が採用されたOSです。WaaSは、アップデートによって進化し続けるクラウドサービスのように、デバイスにインストールされたWindowsも継続的なアップデートによって常に進化していくというサービスモデルです。年に2回の機能更新プログラムで新機能を追加しつつ、毎月のセキュリティ更新プログラムによって安全性が確保され、常に快適かつ安全な状態でWindows 10を使えるようになっています。ただし、用途によっては頻繁な機能更新が適さないデバイスもあるため、それぞれの更新を導入するタイミングやインストール方法をカスタマイズすることができます。



● 新機能を導入するタイミングが選択可能

	半期チャネル	長期チャネル
メリット	Semi-Annual Channel オフィスワーカー向け	Long-Term Servicing Channel 特殊用途向け
考慮事項	年2回の機能更新 ■ 新しい機能を活かした生産性の向上 ■ 最新のセキュリティの利用 ■ 新しいデバイスやサービスのサポート ■ 働き方やインフラの変化に伴う柔軟な対応	2~3年ごとの機能更新 ■ 環境の固定による安定性・安全性の向上 ■ 最低限の機能・セキュリティのみ ■ 10年間のサポート

● WaaSで更新管理がこう変わる

- 機能更新と品質更新の2種類で継続的に進化する
- 更新を適用するタイミングや方法を選択できる

▼もっと詳しく知りたいときはこちらへ！

<https://docs.microsoft.com/ja-jp/windows/deployment/update/waas-overview>



Long-Term Servicing Channelはどんなデバイスに

向いているの？

Long-Term Servicing Channel（長期サービス チャネル）は、特殊用途のデバイスにのみに使用してください。組織内の一般的なPCへの展開は想定していません。ガイドラインとして、Microsoft OfficeがインストールされているPCは汎用デバイスであり、通常はインフォメーションワーカーが使用します。このため、インフォメーションワーカー向けには半期サービスチャネルの方が適しています。



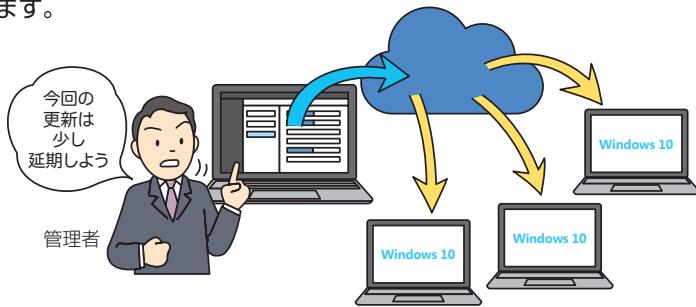
どうやって管理するの？

Windows 10の更新管理は、「Windows Update」「Windows Update for Business (Intune)」「Windows Server Update Services」「System Center Configuration Manager」で管理できます。それぞれの管理の違いは以下の表の通りです。

サービスツール	更新プログラムを延期できるか	更新プログラムを承認する機能	ピアツーピアオプション
Windows Update	○(手動)	×	配信の最適化
Windows Update for Business	はい	×	配信の最適化
WSUS	はい	はい	Branch Cacheまたは配信の最適化
SCCM	はい	はい	Branch Cache、クライアントピアキャッシュ

IntuneによるWindowsの更新管理

Intuneを利用すると、組織のデバイスに対して、どのチャネルを利用して、いつ、どの更新を適用するかを詳細にカスタマイズできます。ユーザーやグループごとに更新ポリシーを割り当てることもできるので、組織内の部門ごとに方法やタイミングを調整することもできます。



- ・ Windows 10 サービス チャネル選択
 - 半期チャネル
 - 半期チャネル (対象指定)
 - Windows Insider - 高速
 - Windows Insider - 低速
 - Windows Insider のリリース
- ・ 遅延設定
 - デバイスグループに対して更新プログラムのインストールを遅らせる
- ・ 一時停止
 - 問題を検出した場合に、更新プログラムのインストールを延期できる
- ・ メンテナンス期間
 - 更新プログラムをインストールできる時間を構成できる
- ・ 更新プログラムの種類
 - インストールされる更新プログラムの種類を選択できる（品質更新プログラム、機能更新プログラム、ドライバーなど）。
- ・ インストールの動作
 - インストール後にデバイスを自動的に再起動するなどを設定できる
- ・ ピアのダウンロード
 - ピアのダウンロードを構成するように選択できる

● IntuneでWindowsの更新がこう変わる

- ・ 更新チャネルや更新タイミングを調整できる
- ・ グループごとに個別の設定で更新を適用できる

▼もっと詳しく知りたいときはこちらへ！

<https://docs.microsoft.com/ja-jp/intune/windows-update-for-business-configure>

HINT! Windows 10のサポート期限

Windows 10 の Semi-Annual Channelでは、機能更新プログラムのリリース日から18ヶ月間*、品質更新プログラムが提供されます。このため、年2回の機能更新を適用し続けることで、サポート期限が継続的に延長されることになります。

* ただしEnterprise/Education Editionは次のリリースに限り30カ月サポートします。

HINT! デバイス管理もできる

Intuneは、組織のデバイスを統合的に管理できるサービスです。レッスン⑥で解説したMicrosoft Intuneでも利用されています。デバイスの構成情報を取得したり、ポリシーを使ってデバイスやアプリの利用を制限したり、遠隔操作によるデータ消去をしたり、ここで紹介したソフトウェアの更新を管理することなどができます。

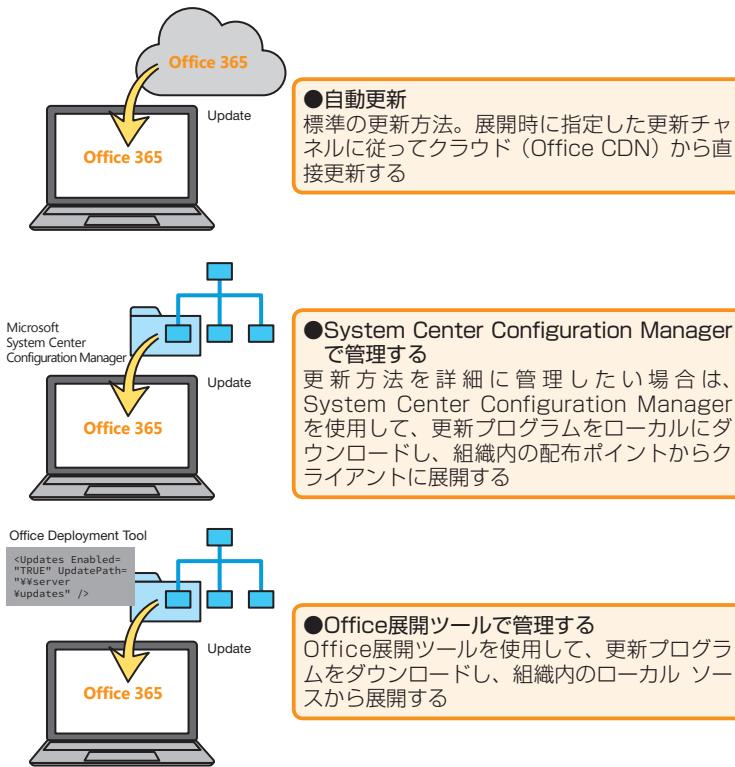
HINT! ピアのダウンロードって何？

ピアのダウンロードは、更新プログラムをダウンロードするための帯域を節約するための機能です。組織内に大量のデバイスが存在する場合、一斉にクラウドから更新をダウンロードすると、インターネット接続のための帯域が不足する可能性があります。一方、ピアのダウンロードを構成すると、デバイスで更新プログラムのダウンロードが完了すると、ほかのデバイスがそのデバイスからの更新プログラムをダウンロードできるようになるため、WAN回線のトラフィックを軽減できます。

次のページに続く

Office 365 ProPlusの更新

組織内のデバイスに展開したOffice 365 ProPlusを最新の状態に保つ方法は、大きく分けて3つあります。標準の方法は自動更新です。クラウド（Office CDN）から自動的に更新が適用されます。更新タイミングなどを詳細に制御したい場合はSystem Center Configuration Managerを利用する必要があります。更新をローカルにダウンロードし、配布ポイントから組織内のデバイスに展開しましょう。もちろん、Office展開ツールを使って構成することもできます。同様に組織内の配布ポイントから更新を展開できます。



●展開ツールの活用でOffice 365 ProPlusの展開がこう変わる

- ・ローカルからの配信でネットワーク負荷を軽減できる
- ・更新タイミングや展開グループを指定できる

HINT! Office展開ツールを活用しよう

Office展開ツールは、定義ファイルに記載した内容によって、Office 365 ProPlusの展開や更新を制御できるコマンドラインツールです。更新で利用する場合は、更新ファイルのソースや更新チャネルを指定できます。ダウンロード方法や使い方は次の文書を参照してください。

▼Office展開ツール

<https://aka.ms/2016odt>

▼Office 365 ProPlus展開ガイド

<http://aka.ms/odtman>

HINT! Office展開ツールの定義ファイル

Office展開ツールで必要となる「configuration.xml」を、GUIで簡単に作成できるエディターもぜひ活用してください。

▼Office Customization Tool

<https://config.office.com/>

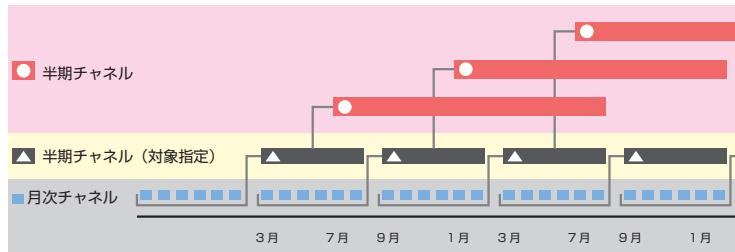
▼もっと詳しく知りたいときはこちらへ！

<https://aka.ms/plano365pp>

Office 365 ProPlusの更新チャネル

Office 365 ProPlusを更新するタイミングは、デバイスの用途などによって選択可能となっています。新機能をいち早く試したい場合は、毎月公開される機能の更新プログラムとセキュリティの更新プログラムの両方がすぐに適用される「月次チャネル」を利用するのが最適ですが、マクロやアドインを含め、組織内で使用するアプリケーションとの互換性を評価する必要がある場合は、機能更新プログラムを6ヶ月ごとに適用する「半期チャネル」が適しています。「半期チャネル（対象指定）」は、半期チャネルのテストのための選択肢です。次の半期チャネルで提供予定の機能更新を4ヶ月前に提供することで、マクロなどのテストや修正を事前に準備できます。

●Office 365 ProPlusの更新モデル



更新プログラム チャネル	主な目的	新機能の更新頻度	次の製品の既定の更新プログラムチャネル
月次チャネル	公開されたらすぐに Office の最新機能をユーザーに提供	月次	Visio Online プラン2、Project Online デスクトップ クライアント、Office 365 Business、Business Premium などの一部の Office 365 プランに付属する Office のバージョン
半期チャネル	年に数回のみ Office の新機能をユーザーに提供	6ヶ月ごとに、1月と 7月	Office 365 ProPlus
半期チャネル（対象指定）	パイロット ユーザーとアプリケーション互換性テスト担当者に次の 半期チャネル をテストする機会を提供	6ヶ月ごとに、3月と 9月	なし

●チャネルの選択で更新の展開がこう変わる

- ・デバイスごとに更新のタイミングを選べる
- ・マクロやアドインの互換性を確認しながら新機能を利用できる



チャネルの名称が変更された

チャネルの名称は、2017年から現在の名称に変更されました。変更前の名称は、「月次チャネル」が「現在のチャネル」、「半期チャネル」が「段階的提供チャネル」、「半期チャネル（対象指定）」が「段階的提供チャネル向けの最初のリリース」です。従来の名称になじみがある場合は、それぞれがどれに相当するのかを確認しておきましょう。



新機能を確認したいときは

Office 365 ProPlusの機能更新プログラムで、どのような機能が追加されるのかを確認したいときは、次のWebページを参照してください。ページをスクロールして表示される「以前のリリース」で、過去の機能更新プログラムで追加された機能を参照することもできます。

▼Office 365の新機能

<https://aka.ms/officewhatsnewjp>

▼もっと詳しく知りたいときはこちらへ！

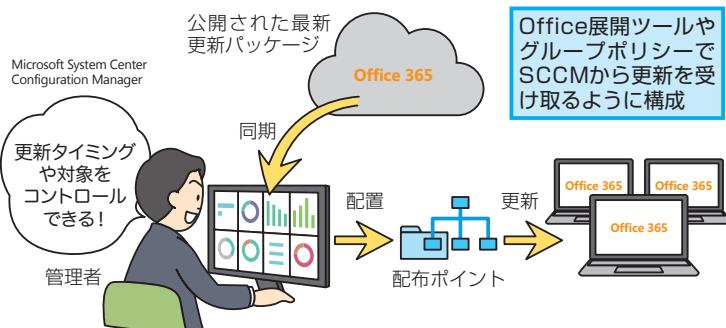
<https://aka.ms/o365ppchan>

次のページに続く

System Center Configuration Manager

●Office 365 ProPlusの更新

System Center Configuration Managerを利用すると、Office 365 ProPlusの更新を組織内の配布ポイントから展開できます。System Center Configuration Managerは、クラウドに公開されたOffice 365 ProPlus用の更新パッケージを取得して、配布ポイント（共有フォルダーなど）に配置し、そこからデバイスへと更新プログラムを展開します。



●System Center Configuration Managerで更新がこう変わる

- 構成管理、展開、更新を一元管理できる
- 組織内の配布ポイントを使って更新を細かく制御できる

▼もっと詳しく知りたいときはこちらへ！

<https://aka.ms/usesccm>

HINT! System Center Configuration Managerって何？

System Center Configuration Managerは、組織内のPCやサーバー、スマートフォンなど、各種デバイスを構成管理するための包括的なソリューションです。デバイスの構成情報を取得したり、OSやソフトウェアを展開したり、更新プログラムを配信したりすることができます。この利用には、オンラインプレミスの環境が必要です。次からダウンロードできる評価ガイドなどを参考に環境を整えるといいでしょう。

▼評価ガイド

<https://aka.ms/emsguidejp>

HINT! 環境を用意するには

System Center Configuration Managerで、Office 365 ProPlusの更新を管理するには、次が必要です。

- System Center Configuration Manager、更新プログラム 1602以降
- Office 365 ProPlusクライアント
- Office 365 クライアントでサポートされるチャネルバージョン
- Windows Server Update Services (WSUS) 4.0
- インターネット接続環境
- 管理対象PCでOffice COM オブジェクトが有効になっていること

HINT! デバイスでの設定も必要

System Center Configuration Managerで更新を管理するには、組織内のデバイスで更新にSystem Center Configuration Managerを使うための設定が必要です。Office展開ツールか、グループポリシー（Office 2016管理用テンプレートが必要）を使って、System Center Configuration Managerから更新を取得するように設定する必要があります。

●法令を遵守する体制を整える

近年、組織の活動にはコンプライアンス（法令遵守）が求められるようになってきました。しかし、情報に関する法令は、多岐にわたるうえ、グローバルな活動をする組織では海外の法令にも対応する必要があり、そのための環境を整えるのは容易ではありません。そこで活用したいのが「Compliance Manager」です。マイクロソフトの各種クラウドサービスの利用状況や設定項目を自動的にチェックし、国内のさまざまな基準にどれくらい対応できているかをスコアで表示したり、必要な設定を提案してくれます。法令違反が疑われる行為などがあったときに、法定関連の情報を検索したり、特定の人物のアクティビティを追跡することなどもできます。

●コンプライアンス体制を評価

リスクを評価し、データ保護機能の有効化をガイド

●データの管理/制御でコンプライアンスを維持

暗号化やアクセス制御機能を実装できる

●監査／法的要件に適切に対応

電子情報開示ツールで法定関連情報を検索したり、アクティビティを分析できる



●法的調査を管理するには

場合によっては、組織や従業員に対する訴訟事件に対応しなければならないこともあります。どのように電子的証拠を確保したり、調査すればいいのかは、次の情報を参照してください。

▼Office 365のセキュリティとコンプライアンス

<https://aka.ms/o365securitycomplianceja>

●Compliance Managerでコンプライアンス対策がこう変わる

- ・国内外のさまざまな標準への自組織の対応状況をスコアで表示
- ・必要な対策や具体的な設定を推奨情報として表示
- ・監査や訴訟の際に必要な情報を容易に準備できる

▼もっと詳しく知りたいときはこちらへ！

<https://aka.ms/compliancemgr>



「セキュリティ管理者センター」ポータルを活用しよう

Office 365では、セキュリティやコンプライアンスに関する機能が、「セキュリティ管理者センター」にまとめられています。管理センターから「セキュリティ」を選択するか、次のページにアクセスするといいでしょう。

▼セキュリティ管理者センター

<http://protection.office.com>



手軽にチェックするなら
Microsoft Secure Score
もある

組織のセキュリティ対策状況をチェックしたい場合は、「Microsoft Secure Score」を利用すると便利です。さらにセキュリティを強化するために不足している設定を確認できるので、Microsoft 365に含まれる機能を最大限活用することができます。

▼Microsoft Secure Score

<https://securescore.microsoft.com/>

Point

組織にあった更新方法を選ぼう

Windows 10やOffice 365 ProPlusを最新の状態に保つのは、セキュリティ上、とても重要ですが、環境によっては、機能更新により既存の業務に支障が発生する可能性があるうえ、更新によってネットワークに大きな負荷が発生する可能性があります。このため、更新チャネルや更新ソースを組織に合わせてカスタマイズすることは非常に重要です。さまざまなツールを活用し、最適な更新環境を整えましょう。

「できる Microsoft 365管理編」（以下、本書）は、日本マイクロソフト株式会社から株式会社インプレスが委託を受けて制作した特別版です。本書は無償で提供されるものであり、本書の使用または使用不能により生じたお客様の損害に対して、著者、日本マイクロソフト株式会社ならびに株式会社インプレスは一切の責任を負いかねます。また、本書に関するお問い合わせはお受けしておりません。あらかじめご了承ください。

できる Microsoft 365 管理編

2018年12月 初版発行
2019年4月 第1版第2刷発行

発行 株式会社インプレス
〒101-0051
東京都千代田区神田神保町一丁目105番地

編集 できるシリーズ編集部
執筆 清水理史
本文イメージイラスト 原田 香
シリーズロゴデザイン 山岡デザイン事務所
カバーデザイン 横川信之
DTP制作 株式会社トップスタジオ

Copyright © 2018 Masashi Shimizu and Impress Corporation. All rights reserved.

本書の内容はすべて、著作権法によって保護されています。著者および発行者の許可を得ず、転載、複写、複製等の利用はできません。

「できるサポート」では、本書に関するお問い合わせにはお答えしておりません。
あらかじめご了承ください。

「できるシリーズ」は、画面で見せる入門書の元祖です。

見開き完結のレッスンを基本とし、レッスン1から順を追って

進めていくことで、楽しみながらパソコンの操作を学べます。

また、レッスンを進めるにしたがって、必要な知識が身に付く構成に

なっています。できるシリーズなら、はじめての人でも安心です。

- オールカラーの紙面でわかりやすく解説
- レッスン単位でステップアップ学習できる
- 各レッスンごとに重要ポイントを掲載
- 関連知識をヒント形式で解説