

Windows 10 と最新 Office で実現する

マイナンバー時代の セキュリティ対策読本

本書の内容

マイナンバー時代に必要なセキュリティ対策を知る

- マイナンバー制度への備えはできていますか？ P. 3
- マイナンバーのセキュリティ対策についてチェックしましょう P. 3
- マイナンバーのセキュリティ対策に対するチェック結果 P. 4
- マイナンバーの情報漏えいは中堅・中小企業にとって
大きなダメージを与えます P. 4
- マイナンバーはすべての情報への入口です。今すぐ対策を！ P. 5
- 多層防御によってマイナンバーを含む個人情報の漏えいをブロック P. 5
- クラウドか？または社内設置の IT システムか？ P. 5

Office 365 によるセキュリティ対策を知る

- マイナンバーの管理に最適な Office 365 P. 6
- Office 365 × Windows10 による多層防御の実現 P. 7
- Office 365 / Windows 10 によるデータの保護 P. 8
- Office 365 と Windows 10 によるアプリケーション アクセスの制御 P. 10
- Office 365 と Windows 10 によるデバイスの保護 P. 11
- Office 365 によるネットワークの保護 P. 12
- マイナンバーのセキュリティ対策は Office 365 × Windows10 で実現 P. 13

購入方法について知る

- Office 365 のラインナップ P. 14
- Windows 10 のラインナップ P. 15

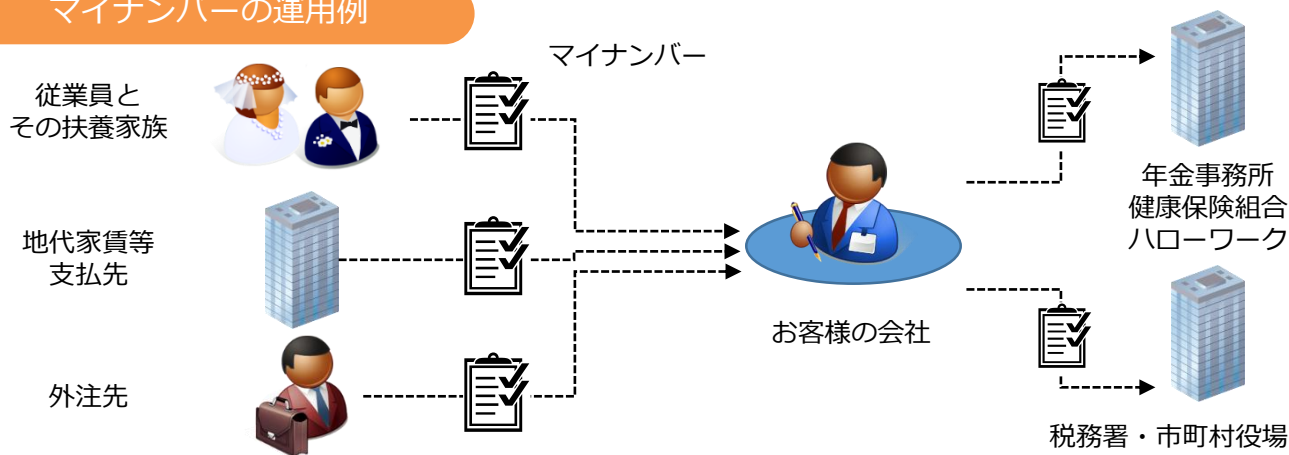
マイナンバー制度への備えはできていますか？

2016 年 1 月から運用が開始されるマイナンバー制度。
マイナンバー時代に合わせたセキュリティ対策として何をすべきか悩んでいませんか？

マイナンバーで私たちに求められること

マイナンバーの運用が開始されると、すべての企業で従業員等や商取引先企業からマイナンバーを収集し、マイナンバーを利用して税務署・年金事務所・健康保険組合等への報告を行います。
そのため、マイナンバーは企業で扱う情報の中でも、とても重要な位置づけとなります。

マイナンバーの運用例



マイナンバーのセキュリティ対策についてチェックしましょう

		チェック
①	マイナンバーを含むファイルを扱っている人が特定できる仕組みを用意している	
②	マルウェア対策ソフトウェアを導入し、最新のパターンファイルで定期的にチェックを行うように構成されている	
③	マイナンバーを含むデータは使用しない時には暗号化されている	
④	法的な保存期間が終了したデータについて、決まった廃棄方法を定めている	
⑤	マイナンバーを扱うアプリケーションを決めている	
⑥	社内のみ/クラウドのみなど、マイナンバーを扱える場所を定めている	
⑦	マイナンバーを含むメールの誤送信の対策を施している	
⑧	マイナンバーが含まれるファイルやメールを扱うときはそのことを意識させている	
⑨	マイナンバーを含むコンピューターを限定している、または紛失した時の対応方法を定めている	
⑩	マイナンバーが保存されている領域へのユーザー認証を設定している	
⑪	マイナンバーを保存する領域に対する不正アクセスを検出するような仕組みを定めている	
⑫	マイナンバーをメールなど、ネットワーク経由で送受信する場合、その内容は暗号化されている	
⑬	マイナンバーの利用方法に関するルールを定めている	

マイナンバーのセキュリティ対策に対するチェック結果はこちら



チェックシートでチェックをつけた番号から
必要なセキュリティ対策の分野を確認しましょう。
あなたの会社は合格点まで到達しましたか？

2 アプリ

3

デバイス

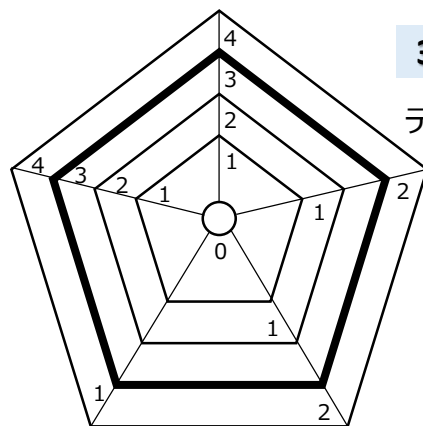
1

データ

5 組織のルール

4 ネットワーク

セキュリティ分野	チェックシートの番号	チェック数
データ	①, ②, ③, ④	
アプリ	⑤, ⑥, ⑦, ⑧	
デバイス	⑨, ⑩	
ネットワーク	⑪, ⑫	
組織のルール	⑬	



マイナンバーの情報漏えいは中堅・中小企業にとって大きなダメージを与えます。

情報漏えいはデータ、アプリ、デバイス、ネットワーク、組織のルール、どこに不備があっても発生します。5000 件以上の個人情報を扱う事業者だけを対象とした個人情報保護法とは異なり、マイナンバーの法律は中堅・中小企業を含む、すべての事業者を対象としています。そのため、マイナンバーの情報漏えいは事業規模を問わず、様々なペナルティを受ける可能性があるのです。

チェック結果で合格点まで達しなかった場合、
マイナンバーの管理責任や漏えいによるペナルティの可能性があります。



刑事罰

番号法※による 4 年以下の懲役または 200万円以下の罰金



民事訴訟

漏えいされたマイナンバー保有者からの訴訟



信用低下

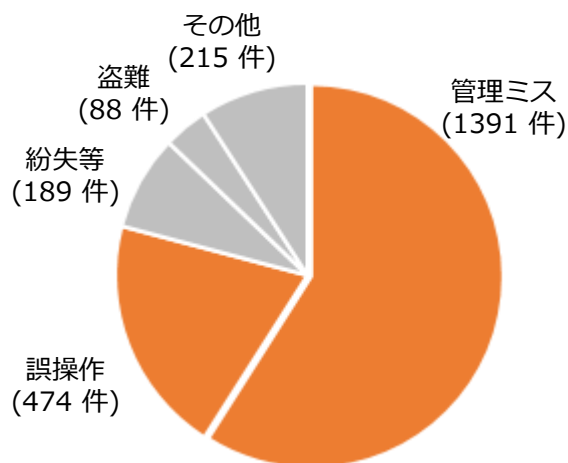
信用低下による新規案件受注減や取引停止

※ 行政手続における特定の個人を識別するための番号の利用等に関する法律

マイナンバーはすべての情報への入口です。今すぐ対策を！

マイナンバーひとつで税務、雇用、保険の情報に関連しているため、狙われやすい情報といえます。実際、日本のマイナンバーに当たる、米国の SSN (Social Security Number) では 2015 年 9 月には約 8000 万件の情報漏えいが発生するなど、情報漏えいの問題が後を絶ちません。また、SSN はクレジットカード作成など民間企業の業務にも活用されるため、SSN を悪用した還付金詐欺が毎年のように発生しています。こうした事件は今後、用途の拡大が予想される日本でも同様の事件が発生する可能性が考えられるでしょう。

NPO 日本ネットワークセキュリティ協会が 2012年に調査した結果によると、日本で発生した情報漏えいの約 8 割が管理ミスまたは誤操作によって発生したものでした。マイナンバーを含む個人情報を社内のサーバーに保存し、管理する方法ではマイナンバーの収集から廃棄までのフェーズに合わせた管理工数が増え、ミスを誘発する要因になることが考えられます。専属のサーバー管理者がいない企業ではその確率はさらに上がることが考えられます。

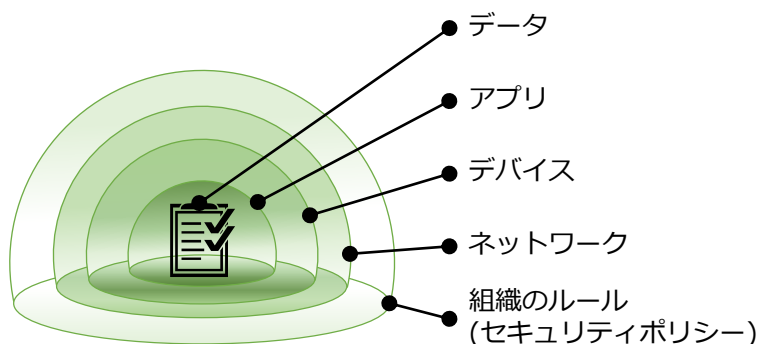


多層防御によってマイナンバーを含む個人情報の漏えいをブロック

マイナンバーを取り扱いを安全・確実に行うには、データ・アプリ・デバイス等、マイナンバーの取り扱いに関わる全ての分野に対するセキュリティ対策を抜け・漏れなく実施することが欠かせません。

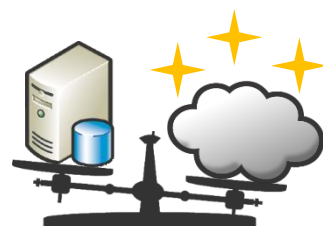
ひとつの製品や機能によって、セキュリティ対策を完了させるのではなく多層防御による全方位的なセキュリティ対策によって、様々な情報漏えいから身を守ることができるのです。

多層防御によるセキュリティ対策



クラウドか？または社内設置の IT システムか？

多層防御によるセキュリティ対策を実装するシステムとして、クラウドを利用する方法と、社内設置の IT システムを利用する方法があります。これまでは「重要情報は社内のサーバーに残しておく」との考え方が主流でしたが、近年の大規模な情報漏えい事件の多くは社内設置の IT システムがきっかけとなったものです。特に専任の管理者を配置することが難しい中堅・中小企業では、片手間でセキュリティ対策を行ってリスクを高めるよりも、セキュリティに対する多大な投資を行い、運用されているクラウドを利用して多層防御を実装し、マイナンバーの管理を行うことがふさわしいといえるでしょう。



マイナンバー管理のセキュリティは、マイナンバーの取得・利用・提供・廃棄の処理に必要な機能と生産性を低下させない仕組みがあって初めて成り立つものです。

Office 365 は、Word、Excel、PowerPoint などの Office アプリケーションとクラウド グループウェアをセットにした、サービス型の Office です。Office アプリケーションを従来通り PC にインストールして使えることはもちろん、Exchange Online によるメール・スケジュール・連絡先管理、SharePoint Online による情報・ドキュメント共有、Skype for Business Online によるオンライン会議も可能です。また大容量 1 TB のオンライン ストレージも標準提供するため、契約してすぐにマイナンバーの管理を簡単に始められます。



■ 電子メール

電子メールのサービスをクラウドから提供することで、Outlook アプリケーションはもちろんのこと、ブラウザやモバイルデバイスからいつでも、どこでもメールの送受信ができます。

■ 社内社外の人と共同作業

スピーディーで円滑な情報共有を行うためには場所や時間を問わずアクセスできるインフラが欠かせません。Office 365 ではポータルサイト機能を通じて社内または社外の人との共同作業をサポートします。

■ 社内 SNS

Office 365 に含まれる Yammer では、社内 SNS としての機能を通じて、円滑なコミュニケーション手段を提供します。

■ バックアップ

Office 365 に保存されたデータはマイクロソフトのデータセンターによって自動的にバックアップされるため、安心してデータを保存し、活用することができます。

■ 個人用クラウドストレージ

クラウドにファイルの保存領域を用意し、いつでも、どこでも必要なデータにアクセスできます。また、共有設定によって他の従業員と共有することも可能です。

■ オンライン会議

Office 365 ではリアルタイムのコミュニケーション手段として、Skype for Business によるオンライン会議機能を提供します。ビデオや音声による会議で理解を促進し、生産性を向上します。

■ データ分析

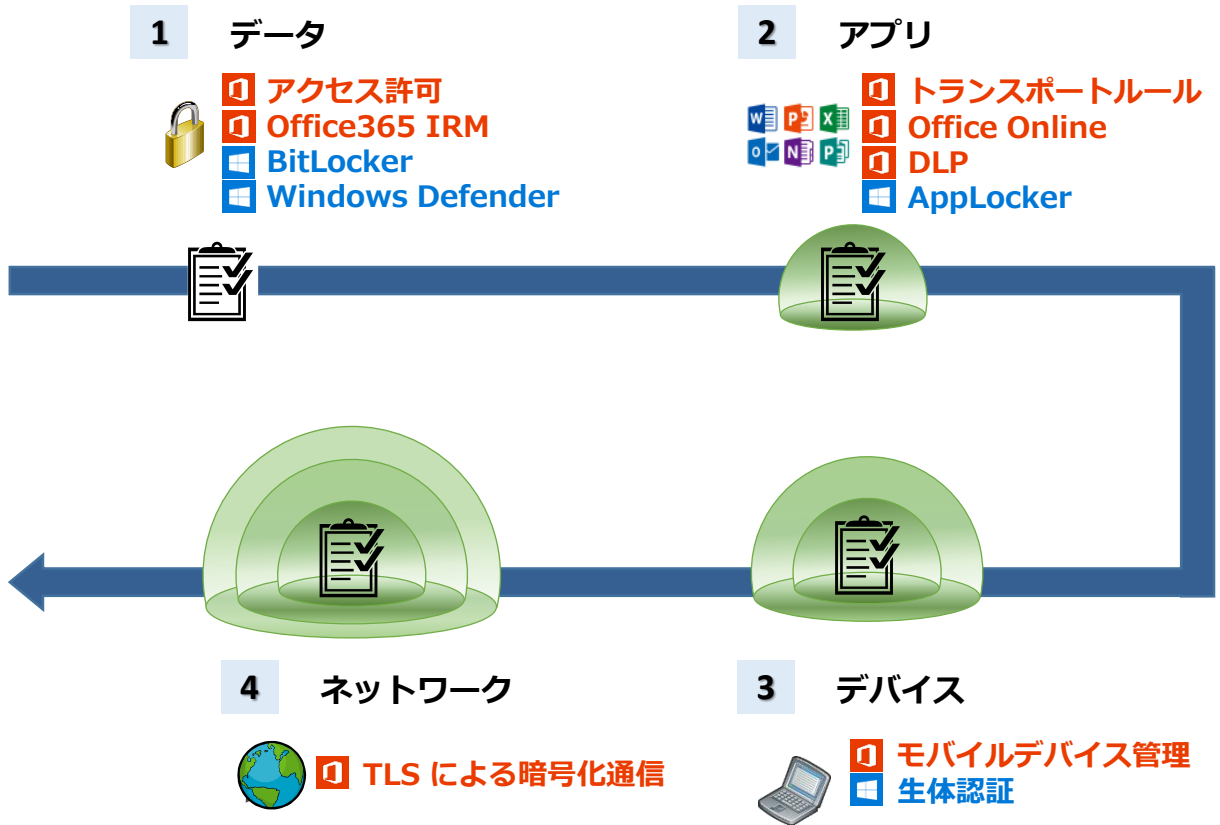
クラウドに蓄積されたデータは単純にそのデータを参照するだけでなく、分析を行い、組織の意思決定に必要な情報を提供します。

■ Office 365 ProPlus

Office 365 に含まれる Word や Excel などの Office アプリケーションを利用して、Office365 に保存されたデータへの簡単なアクセスを実現します。

Office 365 × Windows10 による多層防御の実現

セキュリティ対策で大事なことは一点豪華主義ではなく、多層防御のような全方位的な対策を行うことです。Office 365 と Windows 10 では、安全にマイナンバーを利用するために必要なセキュリティ機能を全方位的に網羅。Office 365 を使い始めたその日から、簡単に、データ、アプリ、デバイス、ネットワーク、組織のルールと、すべての分野に渡るセキュリティ対策が実現します。



組織での利用に最適な Windows 10

マイナンバーの保存場所に Office 365 を利用しても、マイナンバーを扱うときはクラウドを離れて、コンピューターで扱われます。Windows 10 はマイナンバーを扱うための様々なセキュリティ機能を備えているため、先進的なデバイスや機能を活用しながら安全に業務を遂行できます。



🔒 Office 365 と 🖥️ Windows 10 を活用したデータからネットワークまでのセキュリティ対策は次のページから

マイナンバーを含むデータはどこにあっても安全に保存されている必要があります。Office 365 ではアクセス許可によるアクセス可能ユーザーの限定に加え、Office 365 IRM での暗号化や可能な操作の限定が可能です。このようなアクセス制御により、うっかりミスや意図的に行われる情報漏えいに効果を発揮します。



Office 365 に保存されたデータへのアクセス許可

Office 365 (OneDrive for Business) に保存したデータは勝手に共有されることはありません。

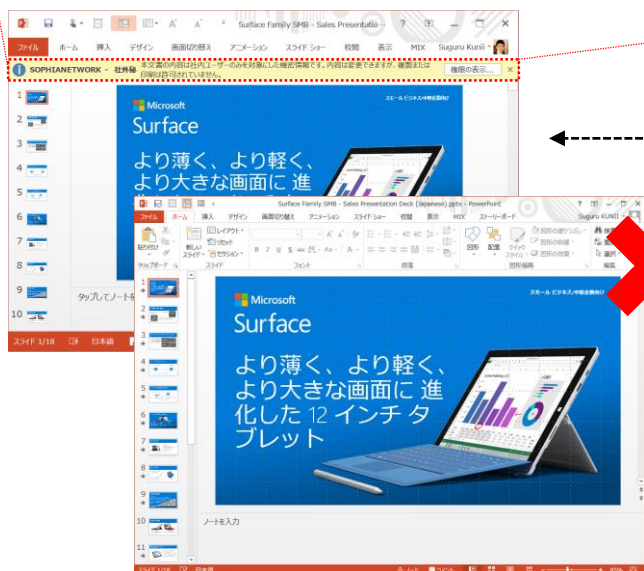
共有する相手は自分で指定するので、情報漏えいのリスクを抑えることができます。また、共有する相手は簡単に設定でき、ファイルの一覧から現在の共有状況も簡単に確認できます。



Office 365 IRM によるデータの暗号化とアクセス権限管理

Office 365 のライセンスに含まれる IRM では、ファイルやメールに対して暗号化を施し、適切な権限を持つユーザーだけがアクセスできます。また、IRM で暗号化されたメールやファイルには、アクセス権限が設定できるので、ファイルに対しては印刷や名前を付けて保存の操作の制限、メールに対してはファイルに対する操作の制限に加えてメールの転送を制限することで情報漏えいを防ぎます。

i SOPHIANETWORK - 社外秘 本文書の内容は社内ユーザーのみを対象にした機密情報です。内容は変更できますが、複製または印刷は許可されていません。 権限の表示... ×



閲覧権限のあるユーザー



権限のないユーザー



作成者
すべての操作が可能

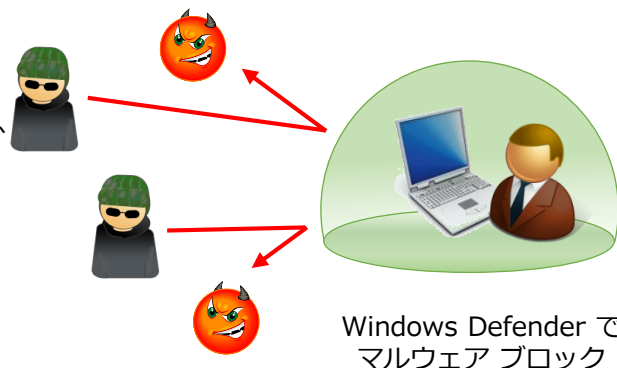
マイナンバーを含むデータは Office 365 から Windows 10 に保存され、扱われることがあります。Windows 10 に保存されたデータに対しては、BitLocker によるデータの暗号化と Windows Defender によるマルウェア対策でデータを保護します。



Windows Defender によるマルウェア ブロック

近年のサイバー攻撃に多用されるマルウェア(ウイルス)は凶悪化の一途を辿っており、甚大な被害に繋がる可能性があります。このような攻撃に対抗するため、Windows 10 ではマルウェア対策ソフトを標準装備しています

マルウェア対策ソフトの Windows Defender は定期的に提供されるウイルス定義と共に最新のマルウェアを常に監視・除去します。



BitLocker でデータを暗号化

データセンターに保存されたデータもクライアント PC にダウンロードし、保存すれば、クライアント PC 上にリスクが残ります。Windows 10 では、BitLocker 機能によるディスク暗号化機能によって、簡単な操作で万が一のデバイス紛失時にもデータの漏えいを防ぎます。

オペレーティング システム ドライブ

Windows (C:) BitLocker が有効です



- 保護の中断
- 回復キーのバックアップ
- BitLocker を無効にする



USB メモリも暗号化で安全に利用

USB メモリのような持ち運びしやすいハードウェアは情報漏えいを起こしやすく、多くの組織で敬遠されてきました。しかし、本当に危険なのは中に保存されているデータの漏えいであって、USB メモリそのものではありません。USB メモリの利用を禁止するのではなく、USB メモリ内のデータを BitLocker To Go を利用して暗号化すれば、漏えいのリスクを抑えて、もっと自由に、円滑に、仕事が進められるでしょう。

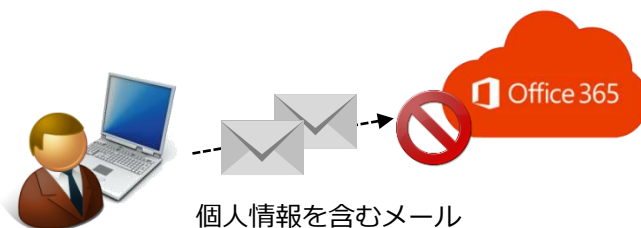


BitLocker To Go による
USB メモリ暗号化

データを保護するためには、データを扱うアプリケーションも安全なものである必要があります。Office 365 と Windows 10 では誤操作による漏えいや、不適切なアプリによるマイナンバーの利用を防ぐことで、アプリケーションレベルでのセキュリティ対策を実現します。

トランスポールルールで誤送信をブロック

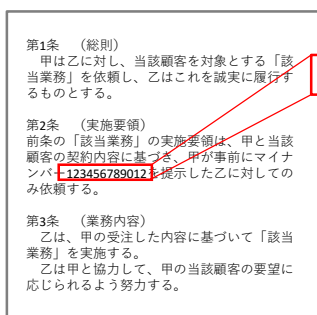
Office 365 のトランスポールルールでは、メールを送信する際にメールの内容をチェックし、個人情報が含まれる場合にはメールの送信をブロックします。個人情報の送信が必要であれば、上司がチェックしてからメールを送信するように構成することも可能です。



データ損失防止で個人情報の漏えいをブロック

誤操作による情報漏えいはよくある原因のひとつです。Office 365 では、データ損失防止 (DLP) によって、メールや Office 365 に保存されたファイルの中から個人情報に該当するデータが含まれていないか確認し、自動的に報告または送信のブロック等を行います。

また、Office 365 ProPlus として提供される Office 2016 アプリケーションにも DLP は搭載されているので、Word によるファイル保存時や Outlook でのメール送信時にも DLP チェック機能が働いて、誤操作による情報漏えいを未然に防ぎます。



- ・ 個人情報が含まれることを自動検出
- ・ メールによる漏えいを防止
- ・ 個人情報が含まれることに気がつかない状態でのファイル保存を防止

Office Onlineによるデータを残さない運用

Office Online はブラウザ画面から利用可能な Office アプリケーションです。Office Online を利用することで、Office 365 に保存されたデータを直接操作するため、マイナンバーを含むファイルをデバイスに保存することなく作業ができます。これにより万が一のデバイス紛失・盗難にも情報漏えいという最悪の事態を回避できます。



AppLocker によるアプリ実行をブロック

Windows 10 に付属する AppLockerではコンピュータで実行可能なアプリケーションを限定することができます。マイナンバーを取り扱うコンピュータではマイナンバーを取り扱うアプリケーションのみを実行可能にすることで、マルウェアに代表される不適切なアプリケーションからマイナンバーが扱われることのないように構成できます。



Office 365 に保存したデータはデータセンター内で他のお客様のデータと分離され、安全に保管されます。一方、私たちは Office 365 に保存されたデータを扱うクライアント コンピューターに保存されたデータのセキュリティも検討しなければなりません。Office 365 と Windows オペレーティング システムでは、クライアントコンピューターの場所を問わず、デバイスを保護し、漏えいの原因を防ぎます。

Office 365 モバイルデバイス管理でアクセス制御

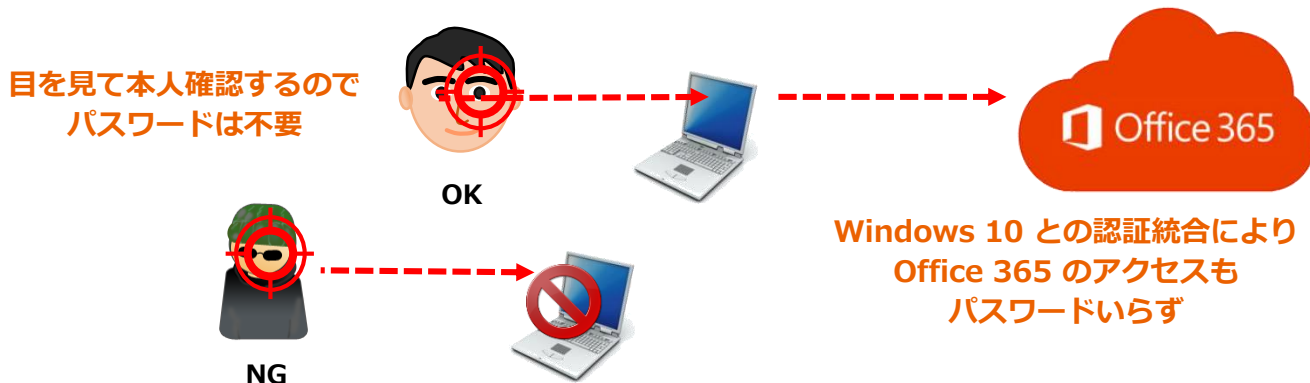
通常、メールボックスやポータルサイトへのアクセスは正しいユーザー名とパスワードを入力できれば、だれでもアクセスできてしまいます。Office 365 ではユーザー名とパスワードだけでなく、適切なデバイスからのアクセスであることを確認し、Office 365 のメールボックス (Exchange Online) やポータルサイト (SharePoint Online/OneDrive for Business) へのアクセスを許可します。

また、Office 365 に一度登録したデバイスを紛失した時は遠隔からデータを消去することも可能です。



Windows Hello によるパスワードを使わない認証

Windows のサインイン パスワードに、クラウドのサインイン パスワード... 私たちの生活ではあらゆる場所でパスワードの入力を求められます。Windows 10 では顔や虹彩、指紋などの「生体認証」を使うことでパスワードを使わずにサインインできます。さらに、Windows 10 の認証は Office 365 の認証と統合できるため、パスワードを一度も入力することなく、Windows と Office 365 の両方にアクセスできます。



Windows 10 コンピューターから Office 365 へのアクセスにはネットワークを経由します。そのネットワークとネットワークの先にある Office 365 の保存領域（データセンター）を安心して利用できるよう、業界最高水準の次のような保護方法を用意しています。



暗号化通信



すべての通信に暗号化通信を採用し、漏えいをブロック

Office 365 にアクセスするための通信には業界標準の暗号化通信プロトコルである TLS を利用しています。



データのプライバシー保護



データセンター内でお客様のマイナンバーを含むデータを完全分離

Office 365 のお客様のデータが宣伝用の製品およびコンテンツの開発に使用されることはありません。また、お客様の顧客データとコンシューマーサービスで使用するデータを混同することはありません。



予防措置としてのモニタリング



通信を監視し、不正アクセス（と見られる）通信を特定

予防措置として Office 365 サービスを監視し、悪意のある動作を予測して未知および既知の潜在的な脅威を特定します。また、脅威の可能性のある不規則なイベントも監視します。



Data Portability



マイナンバーの廃棄を確実に実施

Office 365 の顧客データはお客様に帰属します。お客様はいつでもデータを削除できます



多層防御



私たちの求める多層防御をデータセンターレベルで実現

お客様のデータは、データ層、アプリケーション層、ホスト層、ネットワーク層、物理層等、複数の層においてしっかりと多層防御されます。また、Office 365 は常に最新の状態で保護されているため、安心してデータを預けて頂けます。



ISO 27001 認定取得



ISMS 適合性評価制度に沿ったデータの運用

ISO27001 は、世界で最も利用されているセキュリティ ベンチマークの 1 つです。Office 365 は、ISO 27001 によって定義される物理的および論理的なプロセスおよび経営管理プロセスをすべて実装したサービスです。



深い経験



15 年以上のクラウド運用の経験に基づくセキュリティの実装

Microsoft は、オンラインのデータに対するセキュリティ保護における 15 年以上の経験により、独自の対応策およびポリシーを確立しています。



データの保存場所



データの保存場所を把握し、企業のポリシーに沿ったデータ保存を実現

お客様は、主要なデータセンターの場所と Office 365 で扱うデータが保存される場所を知ることができます。

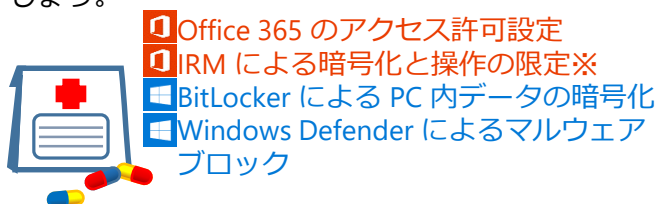


マイナンバーのセキュリティ対策のための処方箋

マイクロソフトがお届けするグループウェアのクラウド「Microsoft Office 365」とオペレーティングシステム Windows 10 を組み合わせて利用することで、どの分野でもマイナンバーのセキュリティ対策が施されるので、今日から安心してマイナンバーの運用を始められます。

1 データのセキュリティ対策

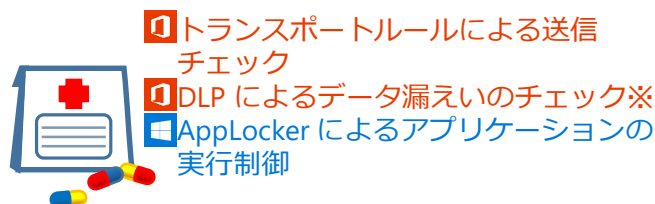
データの保存場所がどこであっても同じセキュリティレベルを維持できるよう、次の対策を行いましょう。



※ Office 365 Enterprise E3 のみ

2 アプリのセキュリティ対策

アプリケーションでの誤操作による漏えいを起こさないよう、次の対策を行いましょう。



※ Office 365 Enterprise E3 のみ

3 デバイスのセキュリティ対策

万が一のデバイスの紛失や盗難に備えて、次の対策を行いましょう。



4 ネットワークセキュリティ対策

マイナンバーを含むデータはメールなどで扱われる可能性があるため、通信を安全に行えるよう、次の対策を行いましょう。



5 組織のルール

どのようなセキュリティ対策でも、組織で働く従業員の協力なしには安全な運用は実現しません。マイナンバーを誰が、どのように扱うのか？についてのルールを Office 365 の操作マニュアルと共に用意して、セキュリティ対策を万全なものにしましょう。



その対策、 **Office 365 と Windows 10** で
すべて揃います。
これでマイナンバーのセキュリティ対策も安心

 Office 365 +  Windows 10

Web サイトにてご契約いただけます。

ご契約はもちろんのこと、製品の最新情報、無償トライアル、お得なキャンペーン情報をご用意しています。

www.office365.com

■ Office 365 のプラン

Office 365 のプランには家庭向けと法人向けがあります。また、法人向けには、機能を限定して 300 名までで利用可能な Office 365 Business のシリーズと、Office 365 Enterprise のシリーズがあります。ここでは、セキュリティ関連の機能を中心に法人向けプランを確認します。

	Office 365 Business	Office 365 Business Essentials	Office 365 Business Premium	Office 365 Enterprise E1	Office 365 Enterprise E3
1人あたり月額	¥ 900	¥ 540	¥ 1360	¥ 870	¥ 2180
最大ユーザー数	300	300	300	無制限	無制限
Office アプリケーション	Office 365 Business		Office 365 Business		Office 365 ProPlus
	Office Online		Office Online		Office Online
Exchange Online		メール ボックス	メール ボックス	メール ボックス	メール ボックス
		Azure RMS はオプションで別途契約			Azure RMS
					DLP
SharePoint Online		共有 ポータル	共有 ポータル	共有 ポータル	共有 ポータル
	個人用 ストレージ	個人用 ストレージ	個人用 ストレージ	個人用 ストレージ	個人用 ストレージ
モバイル デバイス管理	MDM	MDM	MDM	MDM	MDM

■ ライセンスのしくみ

01 ライセンスの種類： ユーザーサブスクリプションライセンス(USL)

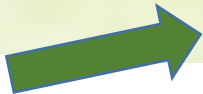
Microsoft Office 365 は、ユーザーサブスクリプションライセンス (USL) という、ご契約期間だけサービスをご利用いただける、非永続ライセンスで提供されます。ご利用になるユーザーごとに USL が必要です。

02 ユーザー利用形態による選択肢 「通常版」と「簡易版」

企業における業務形態によって、日常的にメールやポータルの利用が必要なユーザーもいれば、その必要がないユーザーもいます。そのような場合に、より限定された機能を低価格でご提供するのが、Kiosk Worker (キオスクワーカー) と呼ばれる選択肢です。上記のライセンスとは別のライセンス体系を用意し、安価にご利用いただけます。

■ Windows 10 の入手方法

Windows 10 は Windows 8.1 / 7 からアップグレードする方法、もしくは Windows 10 を新しく購入して利用する方法があります。



Windows 8

Windows 8.1 / 7 がインストールされたデバイスをお持ちの場合、**無償**でアップグレードできます。



Windows 10 を新規にインストールする場合、パッケージまたはライセンスを購入します。

■ Windows 10 のエディション比較

Windows 10 には、個人向けの Home、中堅・中小規模企業様向けの Pro と、より大規模または高度な機能を必要とする企業様向けの Enterprise の 3 つを主なエディションとして提供しています。

特徴	Home	Pro	Enterprise
デバイスの暗号化	✓	✓	✓
ドメイン参加		✓	✓
グループ ポリシー管理		✓	✓
BitLocker		✓	✓
モバイルデバイス管理	✓	✓	✓
Azure Active Directory への参加と、クラウドでホストされているアプリへのシングル サインオン		✓	✓
Pro から Enterprise Edition に簡単にアップグレード		✓	✓
Home から Education Edition に簡単にアップグレード	✓		
Microsoft Passport	✓	✓	✓
Enterprise Data Protection		✓	✓
Credential Guard			✓
Device Guard			✓



● 各種ご相談、お問い合わせは下記まで

マイクロソフト カスタマー インフォメーション センター
0120-41-6755 （営業時間：平日 9:00 - 17:30）



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