

見落としてませんか？

セキュリティ対策 6つの 落とし穴



インターネットだけじゃない 見落としがちなセキュリティリスク… 実は「Windows」が守っています。

セキュリティリスクと言われて、まず思い浮かべるのはインターネットの脅威ではないでしょうか。

しかし、実際に企業を脅かしているセキュリティリスクはそれだけではありません。

不注意による紛失・置き忘れ、盗難被害、誤操作、モラル・認識不足、デバイスなどの未管理……

サイバー攻撃もますます高度化、巧妙化し、従来のセキュリティ対策では対抗しきれなくなっています。

こうしたセキュリティリスクから企業を守るために、Windows はさまざまな技術革新を行っています。

社内でも、社外でも、安心して利用できる環境を実現するために。セキュリティを気にすることなく

もっと自由にビジネスができる未来を目指して。Windows はこの先も進化し続けていきます。



見落としてませんか？ 6つの落とし穴

高度化、巧妙化

P4へ ➡

紛失・置き忘れ

P5へ ➡

盗難被害

P6へ ➡

誤操作

P7へ ➡

モラル・認識不足

P8へ ➡

未管理

P9へ ➡





「高度化、巧妙化」 という落とし穴



うちは狙われるような
大きな会社じゃないから…
実はそういう会社こそ
攻撃者から狙われています。

サイバー攻撃は大企業が狙われるもの、そう思い込んでいませんか？ しかし近年では、セキュリティ対策に予算をかけられない中小企業が狙われるケースが増え、その手口もますます高度化、巧妙化しています。例えば、ウイルスに感染させて機密情報を抜き取る手口では、顧客や取引先の情報までもが狙われ、大きな問題に発展してしまうこともあるのです。

そこで Windows 10 のセキュリティ対策

新たな脅威に対抗し、最新機能をスピーディに提供

Windows 10 にはウイルス対策機能「Windows Defender」をはじめ、データの暗号化や生体認証など進化したセキュリティ機能が組み込まれています。さらに、次々と現れるセキュリティの脅威に対抗すべく新たなアップデートの仕組みを採用。これまでの数年ごとにリリースする方式ではなく、新たに開発した最新機能をスピーディに提供し追加していくことで、高度化するセキュリティの脅威に対抗します。





「紛失・置き忘れ」 という落とし穴



ない、ない、ない…

パソコンの紛失・置き忘れは
意外と多いセキュリティ事故。
もしも誰かに使われたら…

セキュリティというとウイルスばかりに注目しがちですが、実は情報漏えいの 14.3%* は「紛失・置き忘れ」が原因です。情報漏えいを恐れるあまり、“社外へのパソコンの持ち出し禁止”をルール化する企業もあります。しかし、訪問先でのプレゼンや打ち合わせ、空き時間を使った資料作成など、社外でパソコンを使いたい社員は多いのではないのでしょうか。

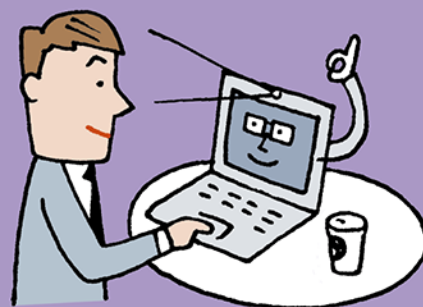
※ 出典：NPO 日本ネットワークセキュリティ協会
(2013 年 情報セキュリティインシデントに関する調査結果)

そこで Windows 10 のセキュリティ対策

本人にしか開けない、パスワードに代わる新しい鍵

Windows 10 ではパソコンを開くための鍵となる認証機能が強化。パスワードに代わる新たな認証機能として、虹彩や顔で生体認証※が行える「Windows Hello」を採用しています。パソコンなどのデバイスだけでなく、「Microsoft Passport」と組み合わせればアプリやWeb サイトの認証にも利用できます。その他にもデータの暗号化を実現する「BitLocker」などがあり、安心して社外に持ち出すことが可能です。

※対応のデバイスが必要です。





「盗難被害」 という落とし穴



まさか、まさかの盗難被害。
当たり前の話ですが、
セキュリティ対策ソフトでは
防げませんし、守れません。

どんなにセキュリティを強化し、ウイルス対策を行っていても、盗まれてしまっただけでは意味がありません。考えられる対策としては、不審者が侵入できないようにビルの警備を強化する。パソコンを鍵付きのストレージに保管する。もちろんそれらも大切ですが、パソコンそのもののセキュリティ対策についてもしっかりと考える必要があります。

そこで Windows 10 のセキュリティ対策

データを暗号化して、中にある“情報”は盗ませない

Windows 10 にはパソコンやタブレット端末などのデバイスに保存したデータを暗号化する「BitLocker」という機能があります。「BitLocker」で暗号化さえしていれば、万が一デバイスが盗まれても、中にあるデータが読み取られることはありません。また、紛失しやすい情報漏えいの原因になりやすいUSBメモリを暗号化できる「BitLocker To Go」も提供しています。





「誤操作」 という落とし穴



あっ、うわっ

しまった、機密情報が…

最も身近な“漏えいリスク”、
それは社員の不注意です。

誤った操作をしていることに気づいて思わずヒヤリとした…そんな経験はありませんか？ タブレット端末などのデバイスには、SNS などの個人用アプリもインストールされているため、ちょっとした誤操作で情報漏えいにつながる危険性も…。情報漏えいを起こした企業は、多額の賠償金の支払いや企業イメージの低下など、大きな痛手を負いかねません。

そこで Windows 10 のセキュリティ対策

企業と個人の領域に分け、領域間の“コピペ”を制限

Windows 10 では不注意による情報漏えいを防止するために、「Enterprise Data Protection (EDP)」というデータ保護機能を提供しています。EDP はデバイス上にあるアプリやデータを企業と個人の領域に分離し、企業領域だけを自動的に暗号化。さらに、個人領域との間でのコピー＆ペーストに制限がかけられるので、誤操作などによる情報漏えい事故を未然に防ぐことができます。





「モラル・認識不足」 という落とし穴



仕事に役立ちそうだからと
無料アプリをダウンロード。
その“何気ない行為”、
セキュリティ的にはアウトです。

インターネット上ではさまざまなアプリが公開されています。仕事に役立つアプリも多く、誰でも簡単にダウンロードできます。しかし、中には悪意を持った人物がウイルスを仕込んだアプリを用意して待ち構えていることも…。仕事に役立ちそうだからと安易な気持ちでダウンロードすると、取り返しのつかない事態を招いてしまうかもしれません。

そこで Windows 10 のセキュリティ対策

危険なアプリから、デバイスをしっかりガード

1 日に 30 万件も発生すると言われるウイルスなどのマルウェア。Windows 10 ではこうした未知のマルウェアの侵入を防ぐために、「Device Guard」という保護機能を提供しています。「Device Guard」が有効になっているデバイスでは、信頼された証明機関によって署名されたアプリしか実行できません。社員が安易な気持ちでダウンロードしようとしても、署名がない場合はセキュリティ上問題ありと判断し、即座にブロックします。





「未管理」 という落とし穴



うちはパソコンもサーバーも
しっかり管理してるから…
でも、忘れていませんか、
“タブレット端末”のこと。

いまや業務でも当たり前のように利用されているタブレット端末。当然、パソコンと同じように企業システムの一部としてしっかり管理する必要があります。しかし、企業の管理下から外れているケースも多く、管理者の目の届かないところで利用者が勝手にアプリをインストールしていたり、アップデートを行ってなかったり…思わぬリスクを生んでいます。

そこで Windows 10 のセキュリティ対策

PCも、タブレットも、Active Directoryで管理

Windows 10 を搭載したタブレット端末なら、従来の Windows PC と同様に「Active Directory」に対応しているため、企業システムにも簡単に追加することができます。デバイス管理面でも、すでにある企業のポリシーを継続して利用することができ、さらに、クラウド型のデバイス管理サービス「Microsoft Intune」を活用すれば、より詳細なセキュリティ ポリシーの設定やアプリの配布なども行えるようになります。



あなたの職場にさらなる安心と安全を！

Office 365 の便利なセキュリティ機能

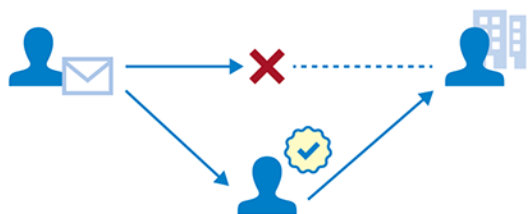
「Office 365」は先進的なセキュリティ機能を備えたマイクロソフトのクラウドサービスです。ここでは、メールフローの制御から、機密情報の保護、アクセス権の管理まで、企業のセキュリティ対策をさらに進化させる Office 365 のセキュリティ機能をご紹介します。



ミスが多い新人のメール、
お客様に送信する前にチェックしたい

特定の条件でメールフローを制御 『トランスポート ルール』

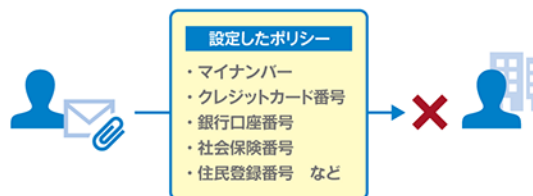
Office 365 が提供するメール機能には、特定の条件に応じてメールフローを制御できる「トランスポート ルール」という仕組みがあります。例えば、“組織外にメールを送信する際には上司の承認を得る”というルールを設定し、ミスの多い新人のメールを上司が必ずチェックするフローに変えることも可能です。



マイナンバーなど、
個人情報が含まれるメールを検知したい

メールに含まれる機密情報を検出 『Data Loss Prevention機能※』

「Data Loss Prevention (データ損失防止)」はメールや添付ファイルに含まれている個人情報等の機密情報を検出する機能です。マイナンバーや口座番号、社会保険番号など、事前に設定したポリシーに違反した内容が含まれる場合には、警告を通知し、送信できないようにブロックします。

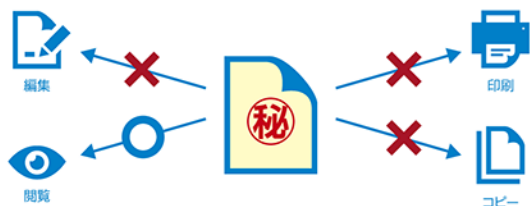


※Office 365 のE3、E4、E5 プラン以外ではオプションです。

社外秘のファイルだから
コピーやプリントアウトを禁止したい

編集・印刷などの権限設定が可能に 『IRM によるアクセス権管理※』

「IRM (Information Rights Management)」は、組織内でOffice ファイルをやり取りする際に、特定の使用制限をかけることができる仕組みです。IRM がかけられたOffice ファイルは暗号化され、権限のあるユーザーのみが利用できます。編集/閲覧/印刷/コピーなどの権限を設定することが可能です。

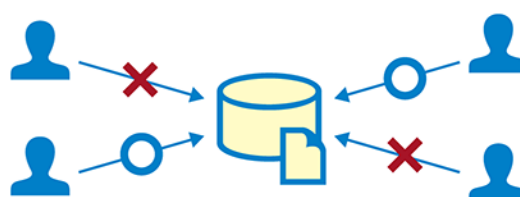


※Office 365 のE3、E4、E5 プラン以外ではオプションです。

プロジェクトに関する
メンバーだけでデータを共有したい

特定の相手とのデータ共有を実現 『OneDrive のアクセス許可』

企業向けのクラウドストレージ「OneDrive for Business」では、各データに対して“アクセス許可”を設定し、共有する相手を自分で指定することができます。プロジェクトのメンバーだけでやり取りしたい情報など、機密度の高いデータの保存や共有に適した安心の機能です。



Office 365 が日本初のクラウドセキュリティゴールドマーク取得!

Office 365 と Microsoft Azure が、日本で初めて「クラウドセキュリティゴールドマーク」を取得。ISMS (ISO/IEC 27001)、HIPAA、FedRAMP、SOC 1、SOC 2 など数多くの認証に続き、国際的な基準で、安全性・信頼性が確認されたサービスであることが証明されました。



今すぐ使える! 仕事に役立つ!

Office 関連コンテンツ特集

日々の業務に役立つ“おすすめコンテンツ”を紹介。

WordやExcelでの作業をもっと快適なものにするために、ぜひご利用ください。

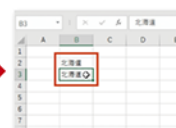
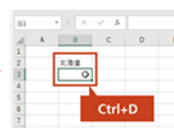
作業効率を高める新機能 & 裏技をまとめて紹介!

Microsoft Office Tips 集

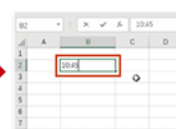
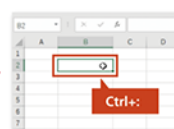


例えば、Excel 編ではこんな“裏技”を紹介

上のセルと
同じデータを
一発入力する
裏技



その日の
日付を
一発入力する
裏技



そのまま使える便利な業務用テンプレートを提供!

ビジネスに役立つ Office テンプレート

経理系
テンプレート



- 交通費精算書
- 給与支払明細書
- 見積書
- 現金出納帳
- 納品書
- 収支計算書 など

営業系
テンプレート



- 提案書
- PDCA サイクル
- 組織図
- 会社案内
- 業務フロー
- 会議議事録 など

管理系
テンプレート



- 業務報告書
- 顧客管理シート
- 社員台帳
- ストレスチェック質問票
- 稟議書
- 在庫管理表 など

Office Tips 集 &
テンプレートはこちら

お役立ちコンテンツが満載! マイクロソフトのビジネス情報サイト
<http://aka.ms/tsukaeru>

Windows 10 情報はこちら

http://aka.ms/ms_win10

ビジネスに役立つコンテンツはこちら

<http://aka.ms/businesslibrary>

製品に関するお問い合わせは、次のインフォメーションをご利用ください。

インターネットホームページ <http://www.microsoft.com/ja-jp/>

カスタマー インフォメーション センター 0120-41-6755 (受付時間 9:00-17:30 ※土日祝、弊社指定休業日を除く)

© 2017 Microsoft Corporation. All rights reserved.

※ Microsoft、Microsoft ロゴは、米国 Microsoft Corporation およびその他の国における登録商標または商標です。

※ その他、記載されている会社名および製品名は、各社の登録商標または商標です。

※ 記載の内容は 2017 年 3 月現在のものです。内容については予告なく変更される場合があります。予めご了承ください。



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

<http://www.microsoft.com/ja-jp/>