

BP
business partner

大塚商会の販売最前線からお届けするセールスノウハウマガジン

Navigator

vol. **82**
2015

特集

実施が目前に迫るマイナンバー制度
**マトリックスで
対応課題を解決!**

Windows 10の注目すべき新しい概念
**お客様先で話したい
「Windows 10」のトピックス**

巻頭特別企画

レノボ・ジャパン×大塚商会 座談会
設立10周年の節目を迎えたレノボ・ジャパン
新たな取り組みをビジネスパートナー様と推進

CAD情報

Autodesk
オートデスクからのお知らせ

Navi Value

セミナーレポート
Windows 10から広がるビジネス開拓セミナー

メーカーズボイス

キヤノン株式会社
東芝情報機器株式会社

CONTENTS

巻頭特別企画

- 8 レノボ・ジャパン×大塚商会 座談会
設立10周年の節目を迎えた
レノボ・ジャパン
新たな取り組みを
ビジネスパートナー様と推進

ITソリューション

- 20 特集
実施が目前に迫るマイナンバー制度
**マトリックスで
対応課題を解決!**
- 62 Windows 10の注目すべき新しい概念
**お客様先で話したい
「Windows 10」の
トピックス**
- 58 法人向けSIMフリースマホビジネス Starter Book(スターターブック)
第1回 ~SIMフリースマホの市場動向編~
- 74 CAD情報
Autodesk
リニューアルされたサポートページなど
オートデスクからのお知らせ
メーカーズボイス
- 85 キヤノン株式会社
- 87 東芝情報機器株式会社

製品情報

- 14 New Products
- 69 ソフトウェアカタログ



BP Navi Value

- 42 セミナーレポート
Windows 10から広がるビジネス開拓セミナー
- 44 PC修理
PC販売の付加価値として有効なPC修理サービス
確かな技術力を確認できる工場見学会
- 46 動画で紹介!
One Stop & Value Added
- 48 BP PLATINUM
「BPプラチナ」で売上げアップ!!
周辺機器サイト「Peripheral Portal Site」(PPS) 編
- 50 Web回線提供サービス
スマートで迅速なビジネスを実現できる
「どこでもコネクトiPadレンタル」特別プラン
- 52 MRO調達ビジネス
独自の物流網に支えられた「TPS-SHOP」を活用し
継続的な利益確保と信頼関係の構築にお役立てください

コラム

- 89 最新ITキーワード
- 91 進化するIT基礎技術の可能性
- 93 BP Navigator Back Number / AD Index

特集 実施が目前に迫るマイナンバー制度

マトリックスで 対応課題を解決!

信用失墜

損害賠償

株価低下

情報漏えい

「特定個人情報」として、個人情報以上に注意深い取扱いが必要とされるマイナンバー。いよいよナンバーの通知が始まろうとしているこのタイミングでも、多くのエンドユーザー様は、「なにを?」「どのレベルまで?」行すべきか苦心しているという話は絶えない。今回の特集では、マイナンバーの取り扱いに関する業務フローをマトリックス法を活用して解説。そこで見てきたマイナンバー対応の課題と解決策を紹介する。

アクセスログ

持ち出し制御

暗号化

データ消去

アクセス管理

外部からの
不正アクセス防止

ウイルス対策

マイナンバー

41267

458746

786451267685

9355474684

18541

435246812676

164378962157

605274310352

04541267

079453412784

3×3のグリッドから見えてくる マイナンバー対応の課題と解決策

マイナンバー通知がスタート 企業の対応も本格的に始まる

10月から、いよいよマイナンバーの通知が開始される。通知は、住民票に基づき、10月から11月にかけて行われる。通知カードは紙製で、券面に氏名、住所、生年月日、性別、マイナンバーが記載されたものになる見通しだ。なお、通知カードと2016年1月以降に本人の求めに応じて市区町村が発行する「マイナンバーカード」の混同は避けたい。顔写真入りのマイナンバーカードは身分証明書として機能するが、通知カードはその名の通り、マイナンバーを通知する役割しか持たない。

通知をきっかけに、マイナンバー対応への取り組みを開始するエンドユーザー様は多いだろう。後に詳しく説明するが、スムーズな収集には通知から時間を置かないことが大切になると考えられるからだ。10月からの数カ月は、民間企業を対象としたマイナンバービジネスの天王山になるに違いない。

「特定個人情報」と「個人情報」の違い

個人情報

個人情報保護法適用範囲
対象：過去6カ月以内に5,000件以上の個人情報を個人情報データベース等として所持し事業に用いている事業者

特定個人情報（マイナンバーを含む個人情報）

マイナンバー法適用範囲
対象：全民間事業者
過去6カ月以内に保有する個人事業者が5,000件以下の事業者も対象
直罰規定あり、両罰規定あり
検査権あり（特定個人情報保護委員会）

マイナンバー

特定個人情報ファイル
（保有個人情報を容易に検索可能ように体系的に構成したもの：紙ファイル・電子ファイル等）

マイナンバーへの対応は 企業ごとに異なる

よく知られる通り、マイナンバーは「特定個人情報」として、いわゆる個人情報以上に注意深い取扱いが求められる。これまで個人情報保護法の対象にならなかった中小企業も対策が必要になるため、マイナンバー対応に苦慮するエンドユーザー様は多いと予想される。実際、一人でも従業員を雇用している事業者であれば、規模を問わず、個人情報事務実施者としての対応が求められることになる。

内閣府外局が公開している事業者向け「特定個人情報の適正な取扱いに関するガイドライン」では、4つの安全管理措置（組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置）の内容を具体的に例示している。だがそこで示される措置は、あくまでも対応の一例に過ぎない。エンドユーザー様の最大の戸惑いは、各措置をどこまで自社に取り入れるべきか、という問題に帰結するのではないだろうか。

マイナンバー制度への対応において「具体的に何をすべきか」「どのレベルまで整備を行うべきか」は、企業規模や業務の実情に応じてそれぞれ異なる。

そこで「収集」「管理」「利用」という業務フローを「関係者への教育」「業務プロセス見直し」「システム導入・改修」という3つの視点から再確認していくことは、適正な対応を図る上で大きなヒントになるだろう。

そこで「収集」「管理」「利用」という業務フローを「関係者への教育」「業務プロセス見直し」「システム導入・改修」という3つの視点から再確認していくことは、適正な対応を図る上で大きなヒントになるだろう。

マトリックスで対応方法を理解

	関係者への教育	業務プロセス見直し	システム導入・改修
収集	1-1	1-2	1-3
管理	2-1	2-2	2-3
利用	3-1	3-2	3-3

「収集」「管理」「利用」という業務フローを「関係者への教育」「業務プロセス見直し」「システム導入・改修」という視点から再確認して、適正な対応を提案したい。

1 収集

	関係者への教育	業務プロセス見直し	システム導入・改修
収集	1-1	1-2	1-3

マイナンバーをスムーズに収集するために

マイナンバー収集は、「誰から」「どのような方法で」「誰が」提供を受けるかを決めることが大切だ。特に、従業員以外でも個人への支払いが発生する際はマイナンバー収集が必要になる点に注意したい。講演を依頼した講師や社外の協力スタッフなど、従業員以外のマイナンバー収集は、業務をスムーズに進める上での一つの鍵になる。

1-1

収集における関係者への教育

扶養親族のマイナンバー手配など
従業員への啓発活動が不可欠

10月から、いよいよマイナンバーの通知が開始される。通知は、住民票に基づき、10月から11月にかけて行われる。通知カードは紙製で、券面に氏名、住所、生年月日、性別、マイナンバーが記載されたものになる見通しだ。なお、通知カードと2016年1月以降に本人の求めに応じて市区町村が発行する「マイナンバーカード」の混同は避けたい。顔写真入りのマイナンバーカードは身分証明書としての機能するが、通知カードはその名の通り、マイナンバーを通知する役割しか持たない。

通知をきっかけに、マイナンバー対応への取り組みを開始するエンドユー

ザー様は多いだろう。後に詳しく説明するが、スムーズな収集には通知から時間を置かないことが大切になると考えられるからだ。10月からの数ヶ月は、民間企業を対象としたマイナンバービジネスの天王山になるに違いない。

1-2

収集における業務プロセス見直し

マイナンバー収集は
10月から12月中の実施が理想

では、マイナンバー収集はいつ行うべきか。新規雇用や退職に伴う業務を除けば、マイナンバー利用が生じるのは、2016(平成28)年分の給与関連の法定調書からになる。あわてて全社的な収集を行う必要がないとも言えるが、マイナンバー通知から時間が経てば経つほど、通知カード紛失などのトラブルも発

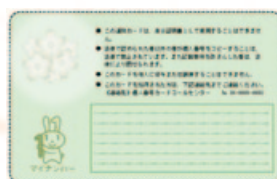


政府インターネットテレビ
マイナンバー・社会保障・税番号制度が始まります(個人向け編)
<http://nettv.gov-online.go.jp/prg/prg11626.html>

生するだろう。収集は、通知直後の10月から12月に一気に行うことが理想だ。

講演を依頼した講師や販促ツールに寄稿してもらった著者、月極で利用している駐車場オーナーなど、支払先が個人である場合もマイナンバー収集が必要になる。こうした場合、誰がどのような手段で収集するか、あらかじめルール化しておく必要があるだろう。具体的には、「担当者が書類の写しを預かる」「事務取扱担当者が直接受け取る」「郵送やメール添付ファイルを利用する」などの方法が考えられる。

マイナンバー通知カードのイメージ(おもて/うら)



通知カードは、身分証明書としての機能はなく、その名の通り、マイナンバーを通知する役割しか持たない。

1-3

収集におけるシステム導入・改修

拠点展開する場合、電子署名や
クラウド利用も視野に入れたい

マイナンバー収集では、原則として対象者が番号を所有する本人であることの確認が求められる。マイナンバー

カードがあれば番号と本人の確認を同時に行えるが、それ以外の場合は、「通知カード+運転免許証」の組み合わせなどによる本人確認が必要だ。

ただし、雇用契約時に身元確認を行った従業員などは、事務取扱担当者・責任者が人違いでないことを認め

ることで身元確認が不要になる。実際に身元確認が必要になるのは、従業員以外に限られる。

マイナンバー収集は、対面か郵送が基本になるが、「電磁的方法による提供」も認められている。この場合、書類をスキャンした上で、電子署名付きメー

ルに添付して提供するなどの対策が求められる。複数拠点を持つエンドユーザー様がマイナンバー収集の窓口を本社に一元化しようとする場合、電子署名の利用やクラウドサービスを介した受け渡しの仕組みを検討する必要があるだろう。

2 管理

マイナンバーを安全に保管するために

マイナンバーは、特定個人情報として適正に保管することが求められる。大部分のエンドユーザー様は電子化して保管するはずだが、その場合、システムへの不正アクセス防止、ログ収集、個人認証・アクセス制御などの取り組みが不可欠になる。それはマイナンバー提案の重要なポイントになるだろう。

2-1

管理における関係者への教育

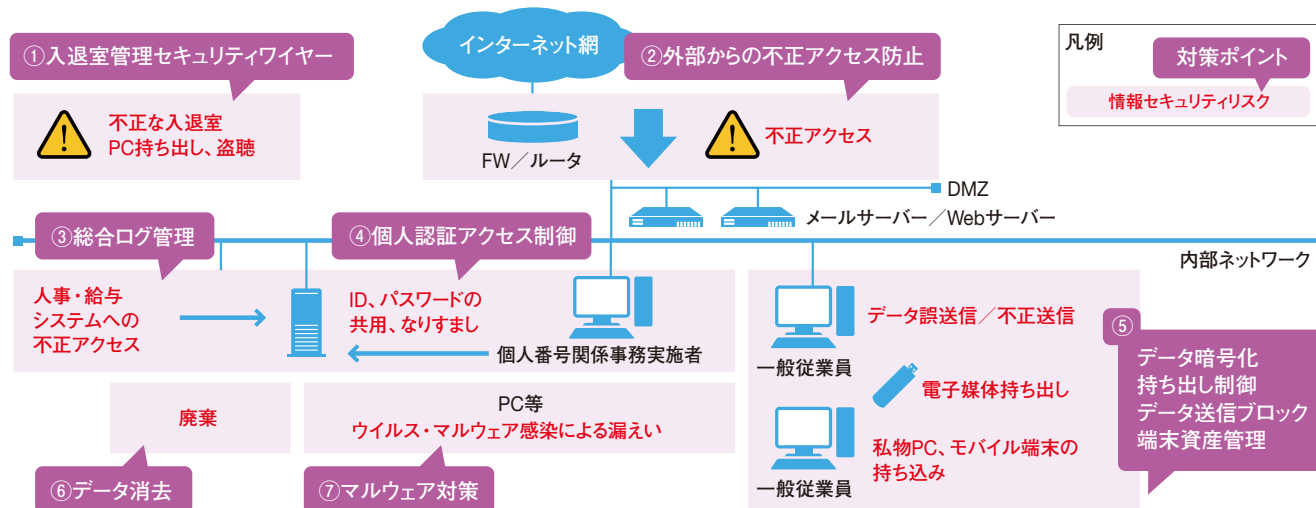
最終的な廃棄まで含めた 管理規程の策定が必要に

特定個人情報の取扱いでは、「不要になったマイナンバーの廃棄」まで含めた取扱規程を定めることが求められている。従業員から収集したマイナンバーは、雇用が続く限り継続的な利用が予定されるため、保管し続けることができる。一方、講演者や原稿執筆者のマイナンバーはそれが単発の依頼である場合、利用後は速やかに廃棄する必要がある。また従業員が退職した場合、マイナンバーだけでなく、それが記載された文書も所管法令で定められた保存期間が過ぎた時点で随時廃棄していく必要がある。具体的には、「電子データとして保存しているマイナンバーの削除」「マイナンバーが記載された

ガイドラインが示す安全管理措置



マイナンバー管理におけるシステム導入イメージ



文書の廃棄またはマイナンバー部分の「マスキング」などを行うことになる。また番号を廃棄した際には、廃棄に関する記録を残すことが求められる。

2-2

管理における業務プロセス見直し

ガイドラインに準じた
保管体制の構築が重要に

特定個人情報であるマイナンバー流出を避ける上で、ガイドラインが示す措置は、その参考になるだろう。なお、マイナンバーに関する業務の全部または一部を税理士事務所などに委託することも可能だ。その際には、事業者自らが果たすべき安全管理措置と同等の措置が講じられていることを確認することが求められる。

2-3

管理におけるシステム導入・改修

マイナンバーに伴う
システム改修ニーズは大きい

システムの観点から安全管理措置を

見た場合、具体的対策は大きく7つに分けて考えることができる。

①入退室管理

FeliCaなどの非接触ICカードを利用した入退室管理システムのほか、監視カメラの活用も効果的だ。

②外部からの不正アクセス防止

ファイアウォール、不正侵入検知/防御などの機能を備える統合脅威管理(UTM)の導入が望まれる。

③総合ログ管理

操作ログは、情報漏えい事故が発生した際の原因究明や改善策立案に不可欠であるだけでなく、故意の漏えいに対する有効な抑止力として機能する。ログ管理機能を備える各種ソフトの導入は不可欠と言えるだろう。

④個人認証・アクセス制御

事務取扱担当者及び責任者だけがマイナンバーが含まれるデータにアクセスできる環境の構築はもっとも重要なことのひとつだ。

具体的には、Active Directoryによるアクセス制御、生体認証等によるアクセス時の認証の厳密化などの手法が考えられるだろう。

⑤データ暗号化・持ち出し制限

電子媒体持ち出しによる漏えいを防止する上では、データ暗号化とActive Directory、IT資産管理ソフト等を使ったUSBメモリなどの電子媒体の利用制限が効果的だ。また、マイナンバーの12桁の番号を検知し、持ち出しや漏えいを制御する機能を備えるセキュリティ管理ソフトの利用も有意だ。

⑥データ消去

マイナンバーが記載された機器を廃棄したり、リサイクルする場合、ハードディスクをフォーマット(初期化)するだけでは、データが復元されるリスクがある。データを完全に消去するには、データ消去ソフトの利用が望ましい。

⑦マルウェア対策

情報漏えいを防止する上で、マルウェア対策は必須だ。だが近年その脅威が取り沙汰される標的型攻撃の場合、従来のウイルス対策ソフトだけでは対応が難しいのが実情だ。

Windows 10が実装した、管理者が承認したアプリ以外の実行をガードする新機能「Device Guard」の利用も効果的だろう。

利用	3-1	3-2	3-3
----	-----	-----	-----

マイナンバー利用は、税や社会保障などの目的に限られる。それ以外の目的への利用は、たとえ本人の合意を得ていたとしてもNG。業務において実際にマイナンバーを扱う業務取扱担当者には、取扱上の注意の周知徹底が必要になる。

利用における関係者の教育

現時点でのマイナンバー利用は、社会保障、税、災害対策の3分野に限られる。仮に本人の合意があったとしても、マイナンバーを社員IDに流用することなどはできない。現実問題として、企業においてマイナンバー利用が許されるのは社会保障と税の2分野に限られると考えていいだろう。マイナンバー運用の適正化を図る上では、業務取扱担当者・責任者を対象とした教育は重要だ。「管理規程の策定にコンサルティングサービスを利用する」「従業員教育にeラーニングを利用する」など、社外リソースの活用も有効だろう。

利用における業務プロセス見直し

2016年度以降、源泉徴収票、給与支払報告書、健康保険被保険者資格取得・喪失届、雇用保険被保険者資格取得・喪失届などへのマイナンバーの記載が必要になる。中小規模のエンドユーザー様の場合、これらの業務を税理士や社会保険労務士に委託しているケースが少なくない。すでに触れた通り、これらの業務はマイナンバーの取扱も含め、外部委託が可能だ。業務を分担する場合、「収集」「保管」「利用」の各段階における役割分担の取り決めや、委託先とのセキュアなデータ連携手段の確保が大切だ。

年金
労働
医療
福祉

税

災害対策

利用におけるシステム導入・改修

マイナンバーを直接的に取り扱うのは、人事・給与系のシステムに限られる。パッケージ製品の場合、その大部分はバージョンアップによる対応が可能だ。一方、システムを自社構築している場合は、一刻も早く具体的な対応を進めることが求められる。その場合は自社開発の人事・給与システムを対象としてマイナンバー登録、管理、申告業務をアドオンで提供するソリューション等の利用を提案することも効果的だろう。

平成 28年 給与所得の源泉徴収票

給与支払者 株式会社 〇〇〇〇

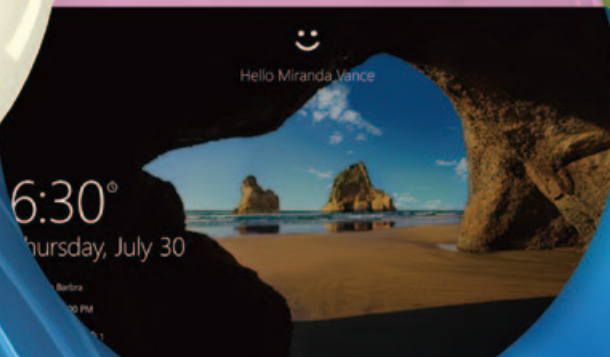
支払を受ける者の個人番号欄が追加されます

控除対象配偶者及び扶養親族の「個人番号」欄等が追加されます

支払者の「個人番号又は法人番号」欄が追加されます(税務署提出用のみ)

特集 Windows 10の注目すべき新しい概念
お客様先で話したい**「Windows 10」の
トピックス**

Windows 10がリリースされて、2カ月が過ぎ、そろそろエンドユーザー様からの問い合わせも増えている頃だろう。本格的な導入はまだ先の話。しかし将来を見据えた情報収集と、エンドユーザー様への情報提供は、パートナー様のビジネスには必要不可欠といえる。そこで今回は、Windows 10に関する新しい概念についてご紹介する。ぜひ、パートナー様の営業にお役立ていただきたい。

**Windows
as a Service****HoloLens****Universal
Windows Platform****Windows Hello &
Microsoft Passport**

注目ポイント

1 サービスとしてのWindowsとは？

Windows 10はバージョンアップの最終形 新機能の提供は今後、クラウドで行われる

変化への柔軟な対応と 信頼性強化の両立を実現

Windows 10を理解する上でまず押さえてほしいポイントは、新機能の追加は、今後すべてWindows Update(クラウド)経由で行われる点だ。Windows OSはこれまで2、3年に一度のメジャーバージョンアップを通して機能強化を図ってきた。今後、機能追加は従来のセキュリティパッチのインストールのように、クラウド経由で行われることになる。Windows 10が「Windowsの最終形」と呼ばれる理由もここにある。

Windows as a Serviceと名付けられたこの全面的な方針転換の背後に、変化への柔軟かつ迅速な対応と一層のセキュリティ向上という、今日のシステム管理部門が直面する二律背反する課題があることは間違いない。日々刻々と変わるニーズに対応する上では、必

要に応じて随時、クラウドを経由して迅速に機能強化できる形への移行は必然とも言えるからだ。

今後、マイクロソフトは、デバイスが製品寿命を終えるまで無償でWindows 10の更新サービスを提供し続けることを発表している。それに伴い、エンドユーザー様は、OSではなくハードウェアのサポート寿命に基づいたリプレースを行うようになる点も、重要なポイントになるだろう。

段階的リリースによって スムーズな更新を実現

一般報道で触れられることは少ないが、プログラム更新に対するマイクロソフトの考え方が大きく変わることも注目すべき点の一つだ。Windows 10では新機能の追加は随時行われるが、それをリスクと考えるエンドユーザー様は決

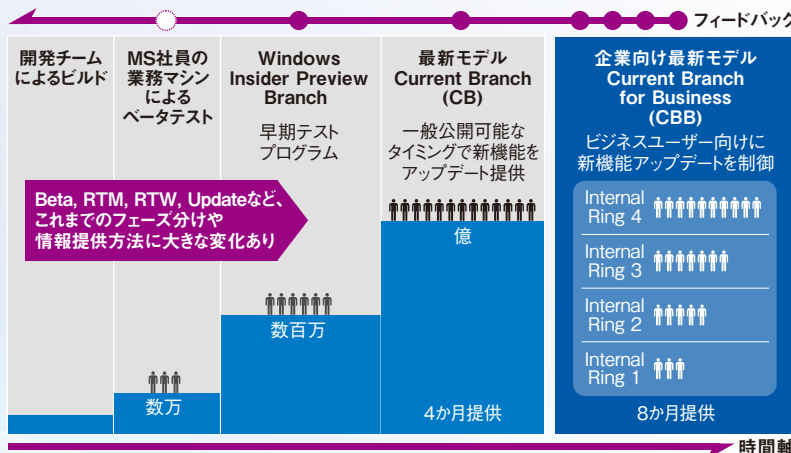
して少なくないだろう。更新に伴い、既存システムに思わぬ障害が生じかねないことがその理由だ。この課題にマイクロソフトは、マイクロソフト社員から数百万人が登録するWindows Insiderへ、そして一般ユーザーから企業ユーザーを経て、企業ユーザーの特別なニーズへと、段階的にリリースし、バグ出しや検証のフィードバックも段階的に進めることで対応を図る考えだ。

これに関連して、常に最新の機能が提供される「最新化モデル(CB)」、「いつ、どの種類の更新プログラムをどのデバイスに展開するか」が選択できる「企業向け最新化モデル(CBB)」、機能強化は行われず、セキュリティ更新とバグフィックスのみが提供されるミッションクリティカルシステム向けの「固定化モデル(LTSB)」という3種類のサービシングモデルが提供される点も注目点の一つになるだろう。

Windows 10のリリースの考え方

ミッションクリティカルシステム向けには別の仕組みを提供

フィードバック



アップデート提供のモデル

最新化モデル (CB)	・コンシューマー向け ・常に最新の機能をいち早く提供
企業向け最新化モデル (CBB)	・ビジネスユーザー向け ・最新機能&こなれたビルドを提供 ・アップデートを一定期間遅らせることができる
固定化モデル (LTSB)	・特定システム向け ・セキュリティ更新とバグフィックスのみ提供 ・機能アップデートはなし ・最長10年間同じイメージを利用可能 ・Windows SA または Windows 10 Enterprise Upgrade で利用可能

注目ポイント 2 すべてのデバイスにWindowsが搭載される!

同じUIや操作感で、ストレスなく
多様なデバイス进行操作できる4インチから84インチまで
あらゆるデバイスに対応

WindowsはPC用のOSというのがこれまでの常識だった。PCやタブレット、スマートフォン、さらにはゲーム専用機やIoT(モノのインターネット)など、多様なデバイスに一元的に対応する開発プラットフォームでもあるWindows 10の登場は、この常識を大きく変えることになるだろう。

エンドユーザー様の視点からUniversal Windows Platformと名付けられたこの特徴を見た場合、第

一のメリットと言えるのは、デバイスを問わず、統一的なユーザーインターフェースや操作感が実現することにある。Windows 10には、デバイスの画面サイズに応じて表示を自動的に最適化する機能を実装している。それにより4インチのスマートフォンから、マイクロソフトが発売を予定する84インチのSurface Hubに至るデバイス上で、一つのアプリをスムーズに動かすことが可能だ。

さらにUniversal Windows Platformには、「さまざまな開発言語への対応」という意味も含まれている。

マイクロソフトが提供する開発キットを利用することで、iOSやAndroid環境で開発された既存アプリは、今後、最小限の変更を加えるだけでWindows 10に移植できるようになるのだ。

日本でもWindows 10のスマートフォンの発売が予定されているが、AndroidやiOSに比べ、アプリ充実度が見劣りすることを指摘する声は多い。一方アプリ開発者にとっては、市場規模の関係で開発コスト回収が難しいという問題があった。開発キットの存在は、この「鶏が先か、卵が先か」というジレンマを一気に乗り越える起爆剤になる可能性もある。

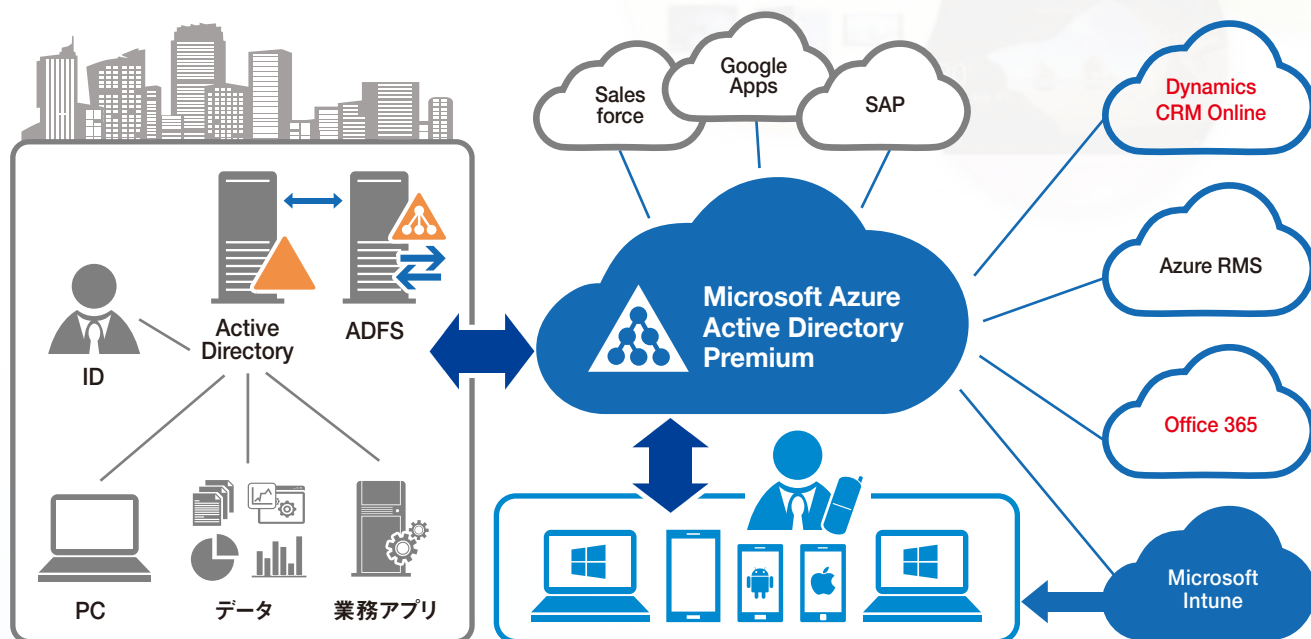
Universal Windows Platform

Windowsならモバイル端末への
既存管理ツール活用が可能

Windowsベースの持ち出しデバイスを選択することのメリットは、操作性だけではない。既存の業務アプリケーション、Active Directoryなどの管理ツール、プリンターをはじめとする周辺機器がスムーズに流用できる点は、ほかのOSにはない大きなアドバンテージだ。

なお、タブレットであってもWindowsならマウスでの操作が快適だ。そのため軽量のタブレットは、用途によってはPCと持ち出しデバイスの1台2役を担うこともできる。機能面で一定の制約があることは確かだが、Surface Pro 3などのWindows搭載タブレットの提案

Azure Active Directory + クラウド活用の概念図



は、導入コストを抑えたいと考えるエンドユーザー様にとって魅力的な提案になりえるだろう。

さらにマイクロソフトが提供するクラウドサービス、Azure Active Directory (Azure AD) を認証基盤として活用できる点もメリットの一つだ。Azure AD を認証基盤として設定することで、Office 365、Google Apps、Sales force など、サービス提供者の垣根を越えたクラウドサービスにシングルサインオンできる点は、特に注目したいポイントになる。また、オンプレミスの Active Directory と Azure AD を連携させることで、一度 Azure AD で認証を行えばクラウドとオンプレミスのリソースの双方にシングルサインオンすることが今後は可能になる見通しだ。

これに関連して、持ち出しデバイスの管理機能の強化もぜひ抑えておきたいポイントの一つだ。持ち出しデバイスが業務に欠かせないものになる中、その管理機能の必須要件として、紛失・

盗難の際の「リモートによるフルワイプ」を挙げるエンドユーザー様は多い。それを受け、マイクロソフトでは Windows 10 リリースに伴い、クラウド型デバイス管理ツール Microsoft Intune を機能強化し、リモートによるフルワイプを実現している。さらに次ページで紹介するように、必要に応じて、デバイス内の企業データのみ消去することも可能になっている。

専用ポータルを活用で アプリ購入の一元管理を実現

Windows 10 のリリースと共に、マイクロソフトは法人専用の Web ベースポータル「ビジネスストア」の提供をスタートしている。持ち出しデバイスの運用に関連することなので、ここで Azure AD 利用を前提とした同ポータルの特長について簡単に紹介しておこう。

ビジネスストアの最大のメリットは、同ポータルを経由することで、Windows ス

トアのアプリ購入やその設定、ライセンス管理などが一元化できる点にある。Windows ストアはこれまで Microsoft アカウントでログインする必要があった。だがビジネスストアを経由することで、企業が管理する Azure AD アカウントでログインできるようになることがその理由だ。IT 管理者がここで入手したアプリを利用者に割り当てれば、利用者はリンクをクリックするだけでアプリをインストールできる。

中堅・中小規模のエンドユーザー様の場合、独自の企業ポータルを持っていないことが多い。ビジネスストアを利用することで、エンドユーザー様は、自社開発アプリを含め、必要なアプリのみを利用者に提供することが可能になる。

また Windows ストアは、これまでクレジットカード決済が前提だった。だがビジネスストアを利用することで、発注書・請求書による取引が可能になることも訴求ポイントになる。

注目ポイント 3

セキュリティ強化と仮想現実への取り組み

「さよならパスワード!」という言葉の意味は?

生体認証とデバイス認証で
セキュアなアクセスを実現

従来のID・パスワードによる認証方式の限界を指摘する声は多い。覚えやすい単純なパスワードでは侵入者に容易に破られてしまう可能性がある一方、あまりに複雑なパスワードを設定した場合、今度は運用面で課題が生じてしまう。また、マルウェアによる標的型攻撃でまず狙われるのは、ローカルのID・パスワードであることが多い。ID・パスワードによる認証の場合、万が一それが盗まれた際、ローカルを踏み台にした大規模な情報漏えいを防ぐことは困難だ。

Windows 10が提案する、生体とデバイスを鍵にした2段階の認証機構は、こうした課題への一つの回答と言える。

Windows Helloと名付けられた生体認証によるWindows 10へのロ

グオンは、「顔認証」「虹彩認証」「指紋認証」をサポートする。この中で特に注目したいのは顔認証で、Intel RealSense 3Dカメラなどの対応デバイスによって、変装によるなりすましや写真と本人を識別することができる。この機能を使えば、利用者が自席に座ると、自動的にログオンを行うこともできる。

Microsoft Passportは、一口で言うなら、Active DirectoryやAzure ADと組み合わせることでシステムやサービスへのアクセスの際、Windows 10搭載デバイス自体が「鍵」として機能する認証機構。Windows Helloと併用することで、スムーズかつセキュアなアクセスが実現する。万が一、デバイスが盗難にあった場合でも、生体認証を突破することは困難であることがその理由だ。なお、Windows Helloによる生体認証を利用しない場合、PIN(暗証番号)の

入力によってシステムやサービスにアクセスすることが可能だ。

よりセキュアなBOYDが
容易に実現可能に

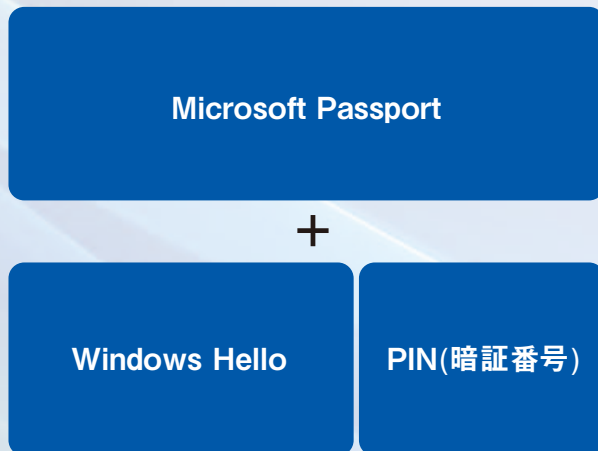
Device Guardと名付けられた、アプリケーション管理機能も注目点の一つになるだろう。これは特定のソフトウェアベンダーのアプリ、所属組織の署名を持ったアプリ、Microsoftの審査を通過したWindows ストア上のアプリ以外の実行をすべてブロックする機能。マルウェアの感染は、メール添付ファイルのクリックやWebサイト上のリンクのクリックなど、利用者の不注意が原因ということが多い。同機能によって、こうした不注意によるマルウェア感染を回避することが可能になる。

Enterprise版に実装される

Windows Hello & Microsoft Passport



2段階認証のイメージ



Microsoft HoloLens



Enterprise Data Protection (EDP)にも注目したい。EDPはコピー・ペーストによる企業データの流出を制御する機能。企業データと個人データを分離して管理し、企業データについては、クラウド型のデバイス管理サービスMicrosoft Intuneなどと連携し、コピー・ペーストの全面的なブロック、操作時のアラート表示などを行うことができる。デバイス紛失などの際には、個人データに影響を及ぼすことなく企業データののみリモートで消去することも可能だ。

SNSの普及により、今後は企業データのSNSへのアップロードをきっかけにした情報漏えいも十分に考えられる。EDPによるアラート表示は、「ついうっかり情報を漏えいしてしまった」という事態を回避する上でも効果がある。

デバイス導入コスト削減、テレワークの促進などの観点から、BOYDに取り組もうとするエンドユーザー様は多い。その際、企業データの保護は、常に大きな課題であり続けてきた。その解決策としてまず挙げられるのは、デスクトップ仮想化だが、EDPやDevice Guardの

活用はそれを補完するだけでなく、比較的簡易な代替策にもなりえるだろう。

現実世界に仮想現実を投影するHoloLens

最後に注目したいのが、Windows 10と同時に発表された、拡張現実用ヘッドマウントディスプレイHoloLensである。現実空間にホログラムによる仮想現実を投影するHoloLensの実機は、国内未上陸で、その発売は来年以降になる見通しだが、そのポテンシャルは高い。

ビジネス分野でもっとも親和性が高いのは、3次元CADとの連携だろう。2次元のモニター以外に有効な表現手段を持たないことは、これまで3次元CADにとって大きな制約になり続けてきた。現実問題として、試作機を作らず、3次元CADのみでデザインレビューを行うことに限界を感じてきた開発担当者は少なくない。実機と同じ大きさで眼前にホログラムとして投影され、見る位置を変えれば、それに応じて姿を変え

る。解決策になりえる。

製造業やメンテナンス業では、3次元CADを従業員教育に活用するケースも少なくない。現実世界にホログラムを重ね合わせられる特徴を生かすことで、建設業のBIM (Building Information Modeling) との連携も有意になるだろう。例えば、壁の中の配線・配管の状態を視覚的に確認できれば、メンテナンスがより効率的に行えるだろう。

もちろん、教育やエンターテインメント分野での活用も大いに期待されるところだ。特にゲーム業界ではそのいち早い取り込みが予想されている。魅力的なコンテンツの登場次第で、HoloLensは急速に普及する可能性を秘めているのだ。

Windows 10の登場によって、Windows OSは大きな飛躍を遂げた。また一般コンシューマーを対象に、Windows 7、Windows 8.1の無償アップグレードを行うなど、話題は尽きない。これからのIT業界のエコシステムは、Windows 10を一つの軸として動くことは間違いなさだろう。【BP】



IT Keyword 最新ITキーワード

RSA

【Rivest Shamir Adleman】

公開鍵暗号基盤(PKI)の代表的な方式であるRSAは、インターネット上でやりとりされるデータを暗号化したり、そのデータに電子署名を付加したりするために広く使われている。この技術がパスワードに替わる認証方式として、もっと簡単に、高いセキュリティの運用を実現するかもしれない。

RSAは、公開鍵暗号基盤(PKI)の代表的な実現方式の一つである。インターネットを経由する通信は簡単に傍受されてしまうので、それへの対抗策として、データを暗号化したり、電子署名を付したりするために使われることが多い。RSAという名称は、3人の考案者の名字(Ronald L. Rivest, Adi Shamir, Lenard Adleman)にちなむ。

暗号の歴史は、古代ギリシャ時代にまでさかのぼると言われる。

しかし、PKIが実用化される1982年まで使われていたのは、送信者(暗号化する側)と受信者(復号化する側)が同じ「鍵」を使う共通鍵暗号方式だけだった。

もちろん、十分に複雑な鍵を使い、鍵の再使用を避けるための運用手順を関係者全員が順守すれば、共通鍵暗号方式でも通信の安全性は保つことができる。ただ、同じ鍵を送信者と受信者が持っていることが前提となるため、鍵を紛失したり鍵が盗まれたりしたときには、全員の鍵を別のものに交換する必要がある。取り替えておかないと、鍵を不正に入手した人がすべての通信データを読めるようになってしまうからだ。しかし、鍵の再配布には多額の費用と長い期間がかかるため、多数の人が使うシステムに共通鍵暗号方式を適用することは難しかった。

これに対して、PKIなどの公開鍵暗号方式では暗号化用の鍵と復号化用の鍵を別々のものとし、暗号鍵は公開(配布)するが、復号鍵は本人だけが持つという仕組みを採用した。暗号鍵と復号鍵は1:1のペアになっていて、ある人の復号鍵で復号化できるのは、その人が公開した暗号鍵で暗号化された通信データに限られる。したがって、復号鍵さえ盗まなければ、暗号鍵が盗まれても通信データの内容が盗み見されることはない。

ただし、暗号鍵の内容から復号鍵の内容が判明してし

まっては意味がない。つまり、公開鍵暗号方式のための復号鍵には、暗号鍵を使って行われた操作の結果を逆方向に戻せるものでありながら、暗号鍵を分解・加工しても作り出せないものであることという条件が求められるのだ。

そこで、RSAでは「掛け算は容易だが、素因数分解はきわめて難しい」という性質を利用して暗号鍵と復号鍵のペアを生成することにした。おおまかには、桁数が長い二つの素数を基に2種類の演算を行い、それぞれの結果を暗号鍵および復号鍵としているのである。暗号鍵から復号鍵を求めるには桁数が非常に長い数を素因数分解する必要があるため、高性能のコンピューターを使っても常時的な時間内には終わらないだろうと考えたのである。

1978年に発表されたRSAは、電子署名を実現するための仕組みとしても使えることから、おりしも黎明期を迎えていたインターネットのためのPKIとして広く使われることになった。1982年にはこのアイデアを販売するためのRSA Data Security, Inc.(現在はEMC Corporationの一部門)という企業が設立され、1983年に米国特許も取得した(2000年9月に失効)。現在RSAが採用されているおもな製品には、電子メールの暗号化、電子署名、セキュリティトークンなどがある。Windows 10 Enterpriseに採用されたDevice Guard機能(信頼できる人が電子署名したコードのみを実行可能とする制限機能)でも、RSAはPKIの一つとしてサポートされるようだ。

これまで、PCの認証方式は、パスワードを入力する認証方式が採用されてきた。新しいWindowsでは、生体認証と公開鍵暗号方式を加えた複合的な認証方式の運用が可能になる。パスワードを入力しない、セキュリティ的に強固で簡単な認証システムの運用が始まるのだ。新しく仕組みが変わるとき、ビジネスに大きなチャンスが訪れる。セキュリティビジネスに注目したい。BP

Possibility of IT basic technology

進化する

IT 基礎技術の可能性

text by 石井英男

1970年生まれ。ハードウェアや携帯電話などのモバイル系の記事を得意とし、IT系雑誌やWebのコラムなどで活躍するフリーライター。

現実を拡張する「HoloLens」の可能性

最近注目が集まっているデバイスに、HMD(Head Mounted Display)が挙げられる。HMDは、その名の通り、頭部に装着するディスプレイであり、以前から業務用途などで用いられているが、液晶技術などの進化によって高性能化と低価格化が進み、画角や精細感が向上したことで話題を集めている。しかし、今回取り上げる「HoloLens」は、外観はHMDによく似ているが、従来のHMDとは全く異なるデバイスである。

従来のHMDは基本的にディスプレイとしての機能しか持たず、PCやスマートフォンなどを接続して利用するのに対し、マイクロソフトが開発中のヘッドマウント型のデバイスであるHoloLensは、CPUやGPUなどが搭載されており、単体で動作することが最大の特徴だ。

HMDは、装着すると外界が見えなくなる「没入型」(非透過型)と外界が見える「透過型」(シースルータイプ)に大別できるが、HoloLensは透過型であり、装着しても周りの様子が見えるため、そのまま歩き回ることが可能だ。HoloLensは、現実世界に映像(マイクロソフトはホログラムと呼んでいる)を重ねて表示できるデバイスであり、ホログラフィックコンピューティングという新たな概念を実現する。こうした現実世界に映像を重ねる技術を拡張現実(AR)と呼ぶが、これまでは研究室レベルでしか実現されていなかった。一般の人々が気軽に拡張現実を利用できる世界を実現することが、HoloLensのミッションである。HoloLensには、カメラや各種センサー、サラウンドヘッドホンなどが搭載されており、使用者の場所や周囲の状況、ジェスチャー、音声などを認識できる。UI操作は、空中でジェスチャーを行ったり、音声コマンドで行える。天気予報や料理のレシピ、ToDoリストなどを壁や天井に表示させたり、現実の物体に映像を投影してゲームを行うといった利用が可能だ。

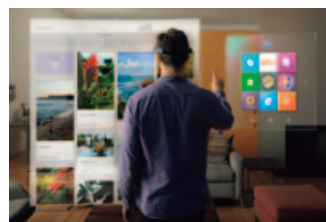
HoloLensは、これまでのコンピューティングの概念を根本的に変える可能性を持つデバイスだ。コンピューターを常に身に付けて利用するウェアラブルコンピューティングは、昔から提唱されているが、これまでは腰に超

小型PCを装着し、PCとケーブルで接続したHMDを装着するというスタイルであった。HoloLensを利用すれば、そうしたケーブルは不要になり、サングラスをかけるような感覚で、ウェアラブルコンピューティングを実現できる。例えば、マイクロソフトはNASAと共同で、HoloLensを国際宇宙ステーションで利用するプロジェクトを進めている。このプロジェクトでは、HoloLensを利用して、宇宙飛行士に地上管制からの指示を出したり、宇宙飛行士が見ているものについて地上管制がリアルタイムでフィードバックを返すといったことを実現する。マイクロソフトの最新OS「Windows 10」にはHoloLens用のAPIが実装されており、Windows 10デバイスと連携することで、さらに可能性は広がる。

HoloLensの価格や発売時期はまだ公表されていないが、最初のモデルの発売は2016年中になると言われている。また、最初のモデルは開発者向けや企業向けとされており、一般ユーザーが入手できるようになるのは、もう少し先になりそうだ。HoloLensは、さまざまな業務の効率を大きく向上させるポテンシャルを秘めたデバイスであり、Slerなどにも新たなチャレンジの機会をもたらすことになるだろう。BP



マイクロソフトが開発中の「HoloLens」。内部にCPUやGPUなどが搭載されており、他のデバイスとの接続が不要で、単体で動作する



HoloLensの利用イメージ。シースルータイプになっており、装着しても周りの様子が見える。現実世界にホログラムのUIが投影されたように見える