Windows10 を運用して メジャーアップデートされて 出遭った色々なこと

アルバス株式会社

松下　麻紀

自己紹介

- 勤め先

  創業51年、従業員50名前後、独立系ソフトウェア請負開発
  PC・サーバー数　100～120程度（増減あり）

- 管理PCの特徴

  [管理]…グループウェアとOfficeソフトが主用途で、PCは操作簡単が一番
  [担当]…お客様がレガシーならPCもレガシーに、バージョンアップはお願いやめて
  [開発]…割当PCに管理者権限を許可し、固有の開発ツールやDB環境・仮想環境がOSに食い込む

- 講師について

  ひとり情シス　10年目くらい
  「未経験OK、文系歓迎！」の募集に惹かれ、汎用機プログラマで新卒入社
  →　諸々開発系SE、導入系SEを経て　→　専任情シスの必要性を感じるようになり、現職
  予算厳しめ、SIerの入らない環境で、日々できるだけのことをしています

Windows 10の展開状況

2015/ 7
初版
1507

・・・・2台パイロット（CB設定）
↓
予期せずアップデート　→問題対応

2015/11
TH2
1511

いったん、PCをRS1でリフレッシュ

2016/ 7
RS1
1607

・・・・開発、営業10台（CBB設定）
↓
告知あり順次アップデート　→所要3時間超で平謝り

2017/末
RS2
1703

新規展開PCをRS3でリフレッシュ

2018/1
RS3
1709

・・・・40台通常展開
～順次展開

パイロット導入で良かったこと

- 情報統制上、「あきらかに要対策」ということがわかった
  - スタートメニューのライブタイルにがっかり
  - 初回ログオンすると、ポップアップで「OneDriveは無料のストレージです！」って…
  - 様々なテレメトリ送信がデフォルトで有効　→説明責任上の対策が必要
  - Windows Update の配信は「近くのPCからP2P」　→同様に調査、説明、対策が必要

正直、詳しく調べるのも面倒に…。

- Windows Pro エディションが「まずい」ということがわかった
  - ストア機能、特に個人向けアプリの自動展開を抑止したい　→Enterpriseのみ
  - 電源設定の「高速スタートアップ」有効化を抑止したい　→Enterpriseのみ
  - いっそ、メジャーアップデート無し版でいい（LTSC）　→Enterpriseのみ
  - など

Windows 10への移行で起きたこと

- 旧型機種、特に個人向け機種が退出させられる
  - MS Surface 3 …特定の更新プログラムが毎日インストールされ、毎日失敗する不具合
  - メーカーPC…ドライバー提供が遅い型番は「運用を諦めるきっかけ」
  - 移行はOKでも、アップデートを重ねるごとにハードウェアとのミスマッチが蓄積する
- ユーザーが短気になる
  - 待ちきれずに電源を切る、再起動する、「×」を押しすぎることへの対策
- メジャーアップデートそのものに関する変更
  - CB →半期チャネル（ターゲット指定）、CBB →半期チャネル
  - 延期可能日数の最大値がバージョンごとに異なってくる

メジャーアップデートで起きたこと

- 設定が消える
  - ネットワークのリセット　→Radiusの無線登録が無くなり、再登録に奔走
  - 省電力設定のリセット　→夜間帯や会議中に予期せぬスリープ、通信断
  - 標準機能へのリンクがリセット　→ショートカットを作った人の作業フォルダが初期値に
  - AD管理者の「リモートサーバー管理ツール」一式が無くなる　→再ダウンロード
- 抑制した機能が復帰する
  - 消しておいたストアアプリが元通り、OneDriveも元通り　（Proだから…）
  - 電源設定の「高速スタートアップ」有効化が復活　（Proだから…）
- 既存アプリの誤動作　他、なんだかよくわからない障害
  - セキュリティ対策ソフト（シマンテック）　→上書きインストールが必要
  - 機種依存傾向を伴い、予測のつかない・原因調査しかねる現象の発生率が上がった

反省したこと

- 「設定済みPCを渡す」では不十分
- 情報統制とOS価格との関連を根回しすればよかった
- 対応しきれないインフラは固執せずに見直すべき
- アップデートも１つの運用業務として月例時間を取る
  - 「予測できなかった、なんだかわからない不具合」は必ず発生すると諦める
  - ポリシー項目が増える／設定済みのポリシーが影響を受けることがあるため
  - 必ず怒るユーザーがいるので、その対応を「例外時間」にしないため

現在の対応状況（月例アップデート編）

- 再起動抑止スイッチをつけてPUSHインストール
  - 配信ツール　…　QND Advance
  - 更新プログラムをDLするため、ちょっと早めに出勤
  - 業務時間中の再起動要請が出なければ、まあまあ許して戴けています…
- アップデートフォローに月例時間を取る
  - Windows7で有効だった「wuauclt」コマンドは使えません
  - 通信を切られがちなモバイルPCに対しては、場合によりユーザーへ連絡
- 再起動を促す
  - 特に、2-in-1 タイプのPCに対しては、告知のうえ再起動コマンドを配信

現在の対応状況（メジャーアップデート編）

- プッシュアップデート実行の周知
- 設定が消えることに対する対策
  - 個人アプリ　…ログオンスクリプトでPowerShellを実行し、自動修正する
  - ストア　…「ストアへのアクセスを遮断する」だけなら、Pro版でもポリシー可能
    %ProgramFiles%¥WindowsApps¥Microsoft.WindowsStore*　を実行禁止にする
  - 他設定　…グループポリシーが基本、メニューが無くてもレジストリ項目を配信する
    https://getadmx.com/?Category=Windows_10_2016&Language=ja-jp
- 不具合時の突発工数に対する対策
  - 前後2台のPCを準備し、なくなったファイルやレジストリを比較できるようにする
  - 最低本数のLTSC版を常に確保し、深刻な不具合を発した環境に備える

今後対応したいこと

- Radius設定が消えないように、無線環境の更改（…のお金）
- 維持注意な環境に工数を割かないため、Enterprise版（…のお金）
- サクッとキッティングしたいので、MDT配信環境（検証中）
  - BitLocker、個人用アプリ等がからむWindows 10 はSysprepに不向きのため
  - Windows Server + DHCPサーバー + Hyper-V で構成
    → メジャーアップデート時の準備工数が割にあうかも、同時に検証したく