働き方改革時代のセキュリティ対策セミナー

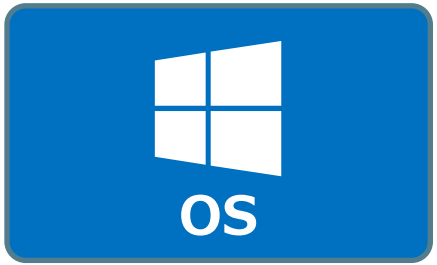
～ひとり情シスの業務が変わる 編～

Windows 10 運用とセキュリティ対策の勘所

アルファテック・ソリューションズ株式会社
ビジネスアライアンス部 技術グループ
山添 光洋

本日のテーマ

エンドポイントに関する
セキュリティインシデントの運用



Windows 10 に関する運用

BIOS攻撃に対する
ハードウェアのセキュリティ対策

Agenda

- Windows 10 のおさらい
- Windows 10 の具体的なお困りごと
- Windows 10 運用を少し楽に
- まとめ

山添 光洋（ヤマゾエ ミツヒロ）

直近10年の経歴

2009年～16年 ：**エンドポイントセキュリティの運用管理**
※ ウイルス対策、セキュリティパッチ、デバイス暗号化・制御、資産管理

2009年 ：**シンクライアント環境の企画・構築**

2009年～10年 ：**Windows XP → Windows 7 更新**

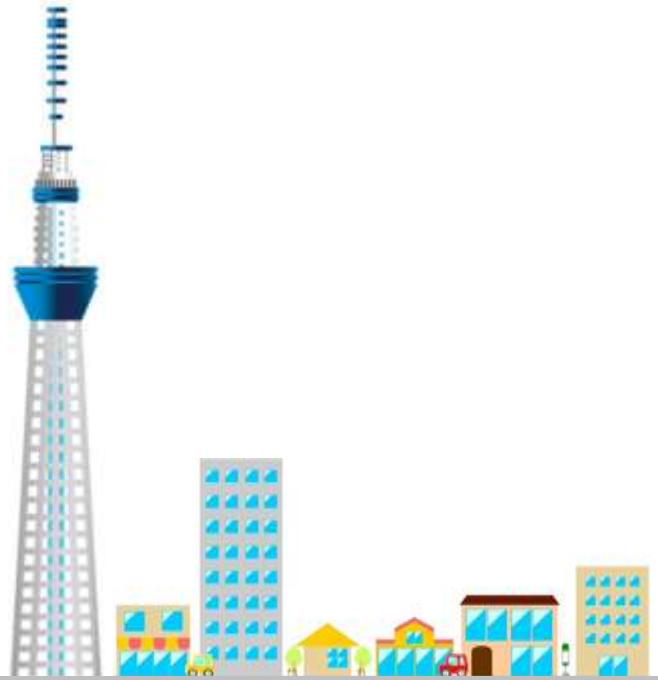
2010年 ：**サーバ用セキュリティパッチ運用改善**

2011年 ：**エンドポイント資産管理の企画・構築**

2014年～16年 ：**セキュリティ推進室兼務**
※ セキュリティポリシー見直し、情報漏洩対策の検討・構築、
セキュリティインシデント対応、CSIRT検討

2015年～16年 ：**Windows 10 の仕様検討、構築**

2017年～ ：**Windows 10 外販へのセールス支援**

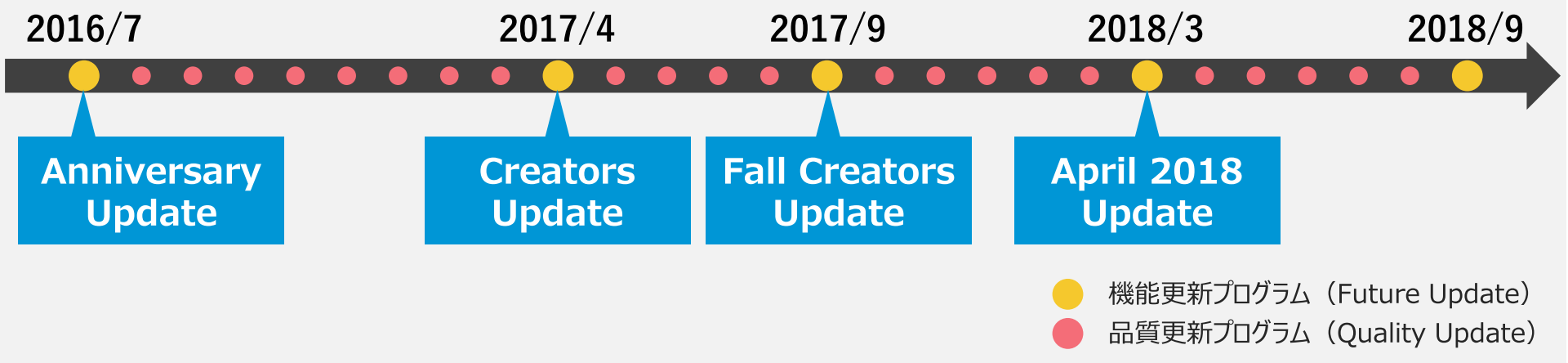


Windows 10 のおさらい

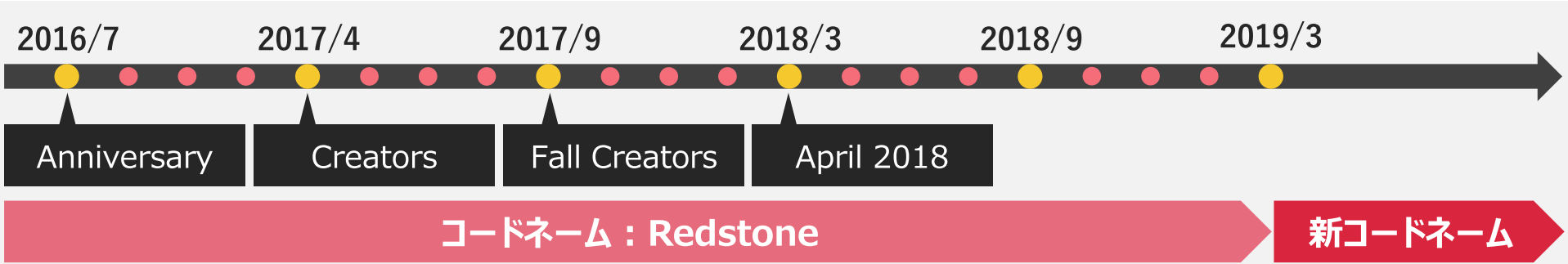
Microsoft社はWindows 10 からコンセプトを変更

Windows as a Service

機能更新プログラム(FU) と 品質更新プログラム(QU) が継続的に提供され
常に最新のWindows 10 環境が維持される



1 FUはサービスパックじゃなくバージョンアップ

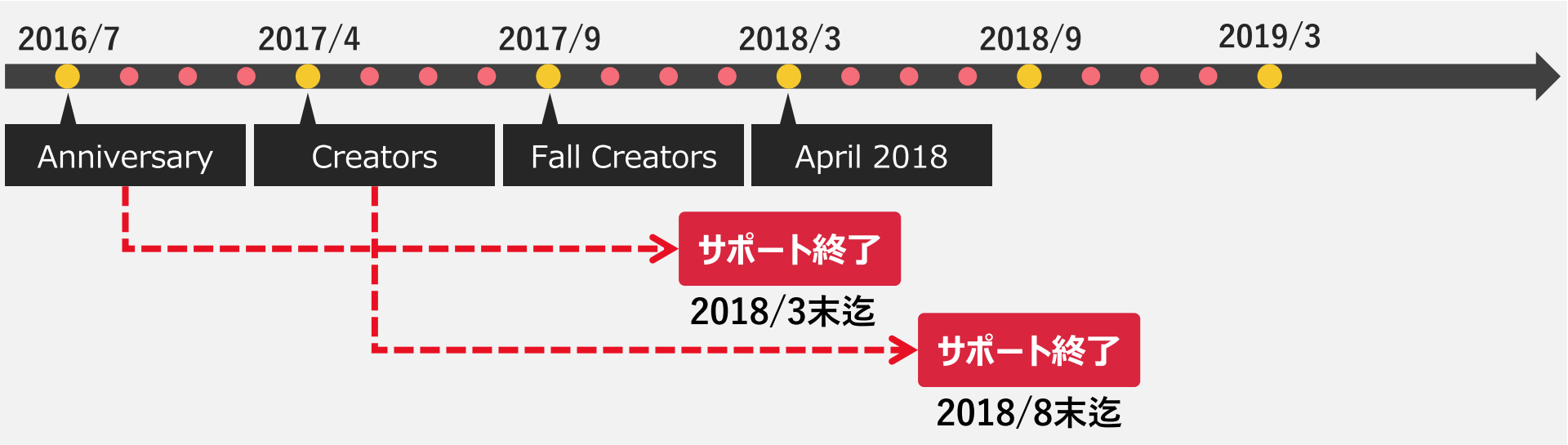


2019年4月からガラッと変わる可能性も秘めている…

Windows 10 のおさらい

1 FUはサービスパックじゃなくバージョンアップ

2 サポートはリリースから2世代（約18ヶ月サイクル）



これまでの 4～5年 から 半年～1年半 の運用サイクルに

Windows 10 のおさらい

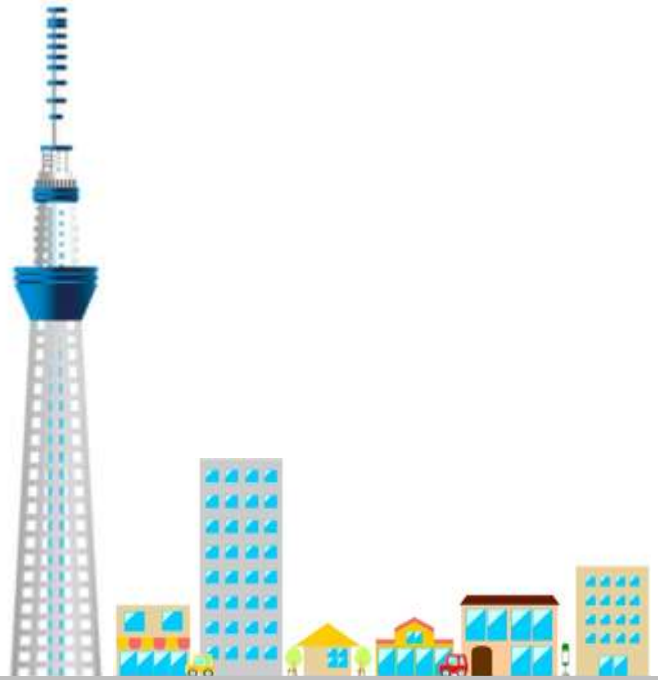
Windows 10 は Windows 8.1 までのOSとは ”まったく別物”

これまで以上に
運用をしっかり検討していく必要がある

Windows 10 運用の大前提

提供モデル	アプリケーションの開発サイクル
Windows XP Windows 7 Windows 8.1	大投資 → 何年もかけて予算取りや企画立案 → 大投資
Windows 10	大投資 → 時代の変化とニーズに応じて常にアップデート → 中投資

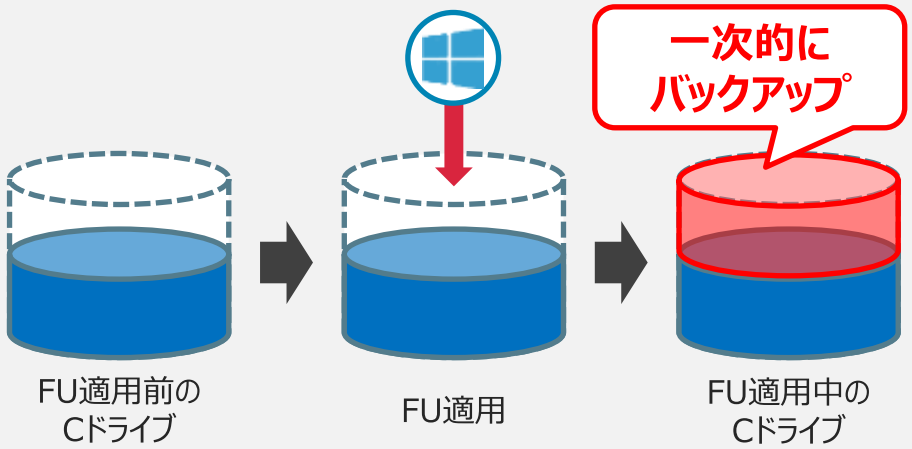
プロジェクトのあり方そのものの変化
（解散しないプロジェクト）



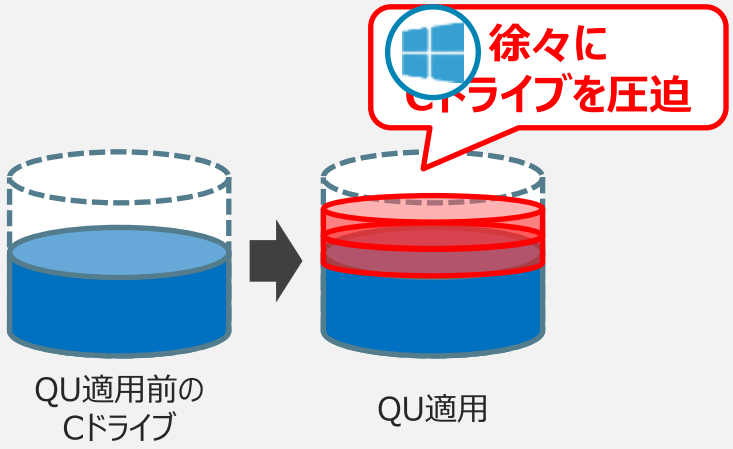
Windows 10 の具体的なお困りごと

Cドライブの空き容量確保

FU適用時は20GB程度の空きが必要



QU累積パッチで毎月1GB利用



全端末の空き容量の管理が必要・・・

Windows10 の具体的なお困りごと ②

クライアントアプリケーションのサポート確認

新たなFU → Windows10

ウイルス対策　デバイス制御　ドライブ暗号化　・・・

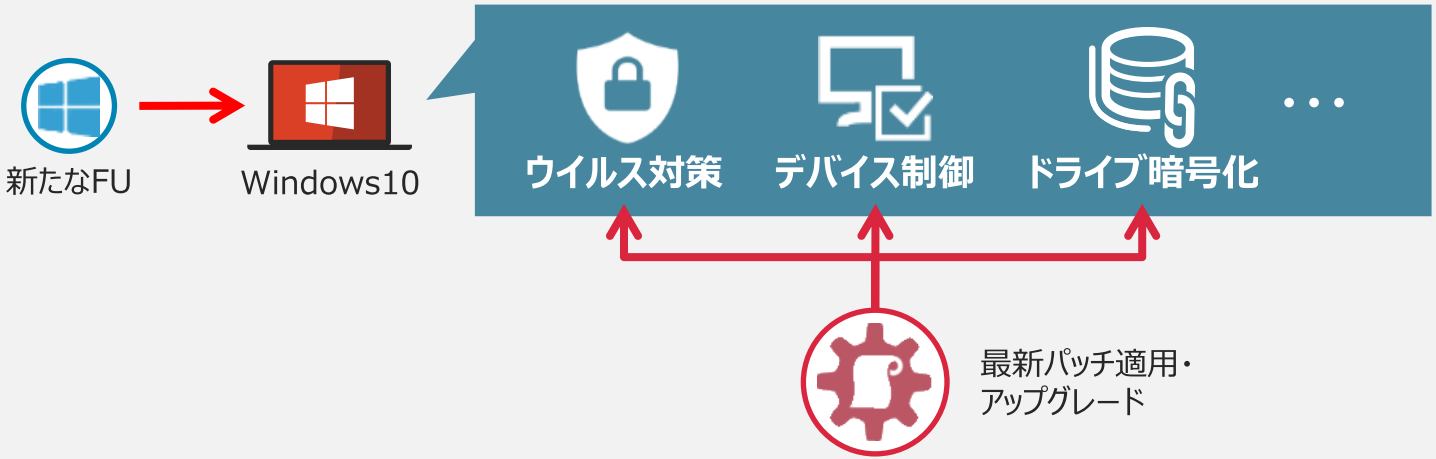
FUが途中でストップ

FUが適用できてない

2018年9月5日時点
https://www.lanscope.jp/an/news/5305/

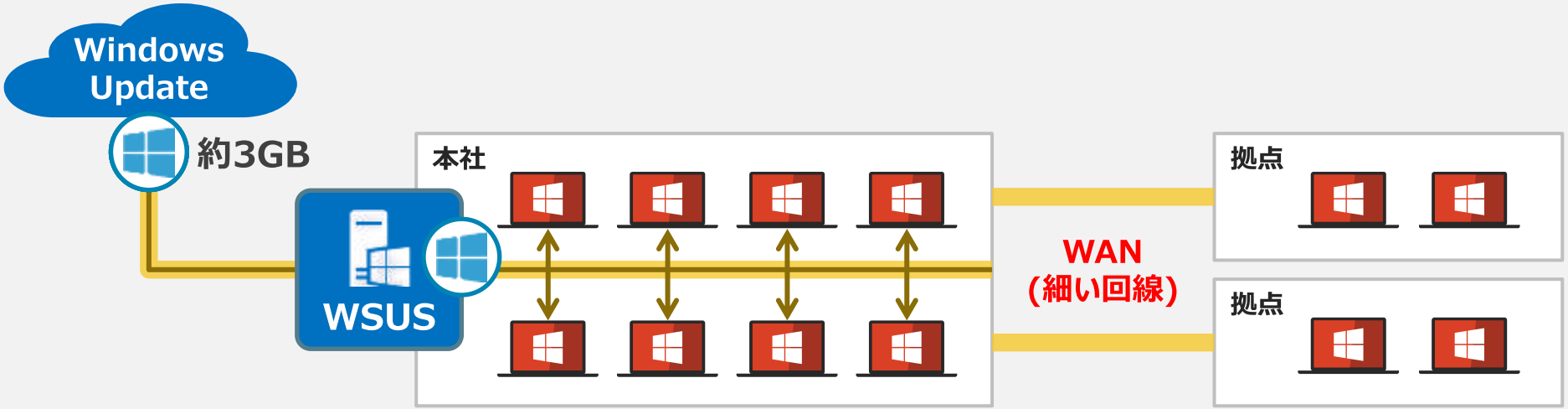
2018年9月5日時点
https://support.symantec.com/ja_JP/article.TECH235458.html

クライアントアプリケーションのサポート確認



対象のクライアントアプリケーションが多いと大変…

FUのデータが大きすぎる



WSUSがあっても社内ネットワークは圧迫
さらにPushしかできないため勝手にアップデートがかかる

FU配信により業務に影響が出てしまう…

ローカルポリシー/ストアアプリがリセット

Fall Creators Update

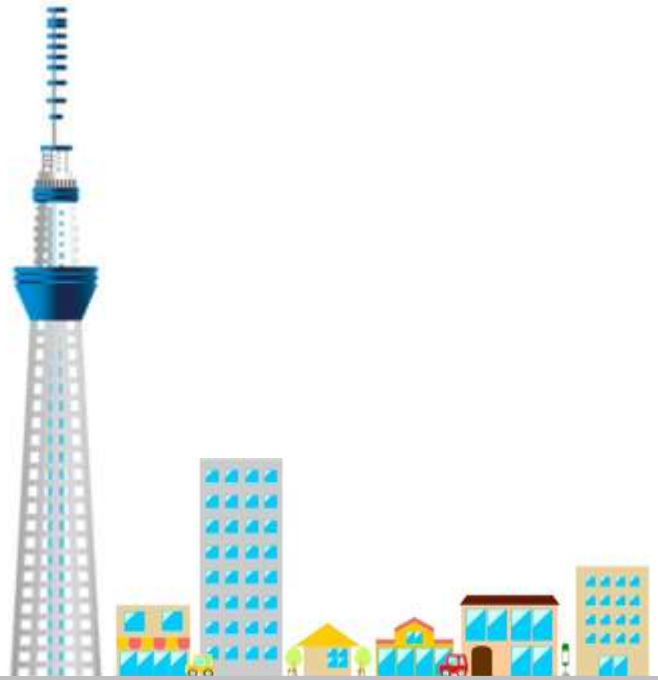
設定が逆転
「いいえ」が「はい」に変わる

ポリシー自体がなくなる
ポリシーの場所が変わる

プロビジョニングされたアプリは
すべてデフォルトに

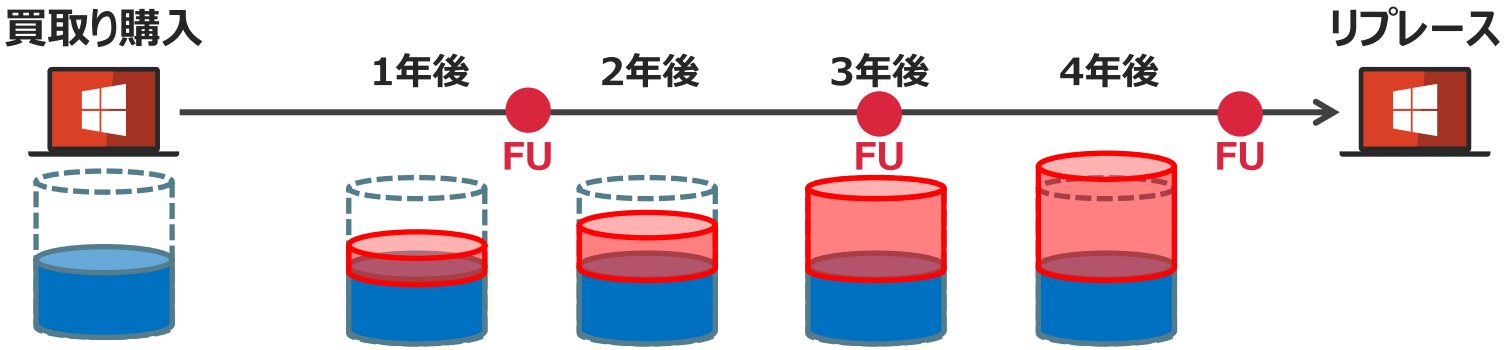
ストアアプリのアップデートは
全部アプリが対象

端末個々への設定変更・管理は無理…



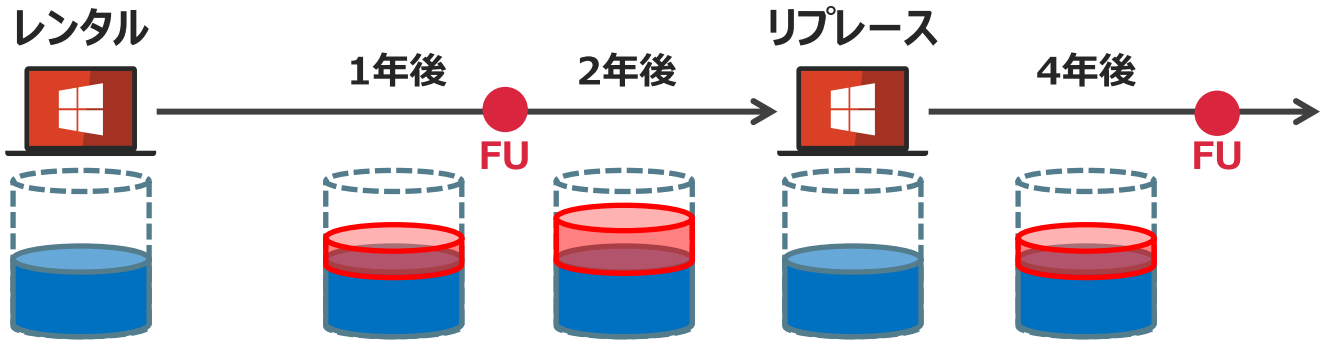
Windows 10
運用を少し楽に

3年程度の短いライフサイクルに変更　レンタルがお勧め



SSD 256GB の端末だと3年が限度
SSD 512GB の端末だと高い

3年程度の短いライフサイクルに変更　レンタルがお勧め



3年周期にすることでCドライブの問題は解決
新たなFUを適用したPCを配布することでネットワークも問題なし

3年程度の短いライフサイクルに変更　レンタルがお勧め

端末のローカルデータはWorkフォルダで同期し、
端末移行の手間を排除

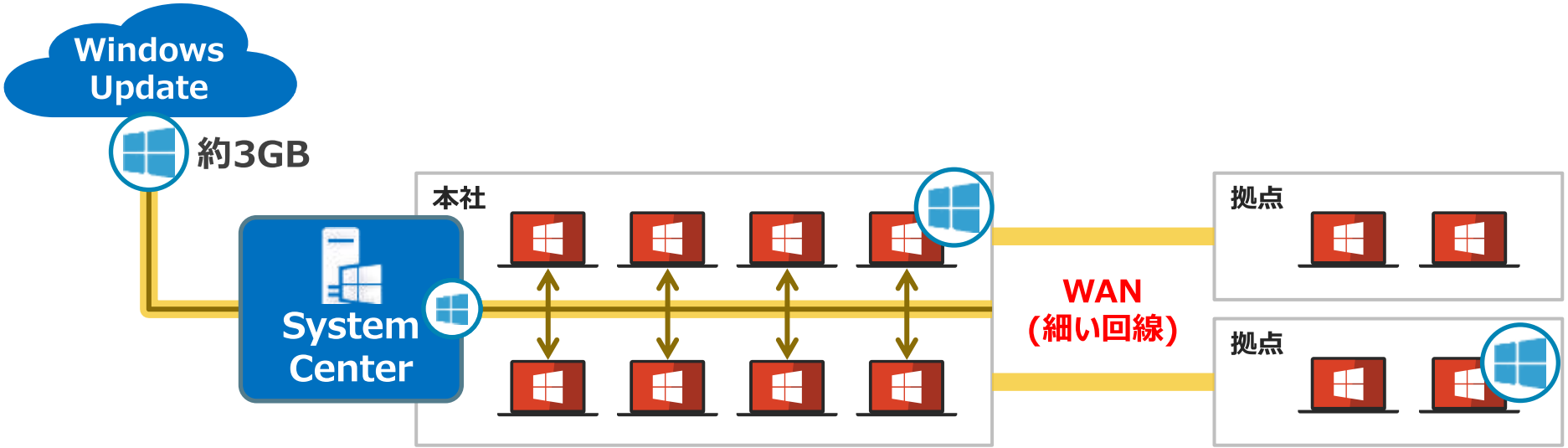
Microsoft 製品を可能な限り利用

FUと同じタイミングで最新版が提供される

ウイルス対策	ディスク暗号化	デバイス制御	二要素認証
			
Windows Defender	BitLocker	グループポリシー	Windows Hello

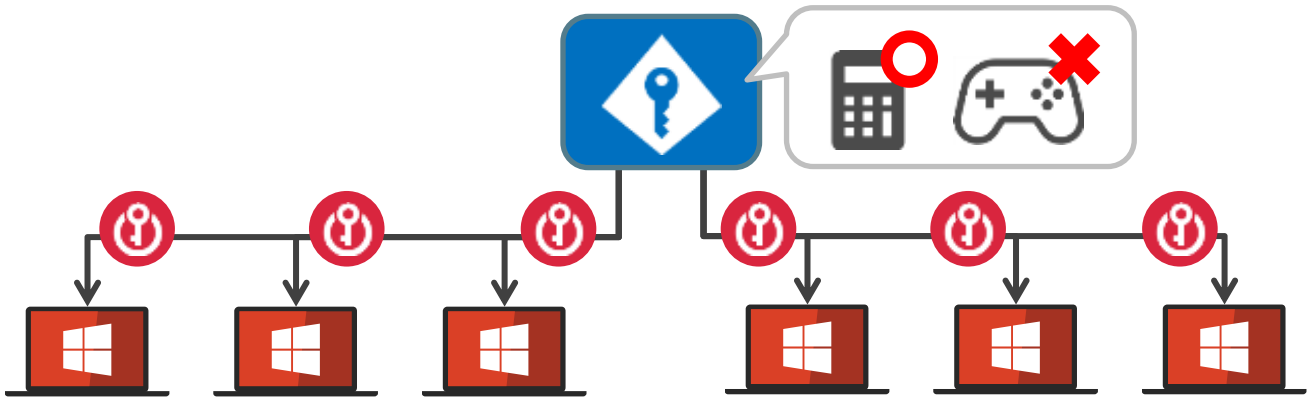
アプリケーションのサポート状況確認や
バージョンアップ作業の手間が省ける

ハイブリッド配信（Push+Pull）

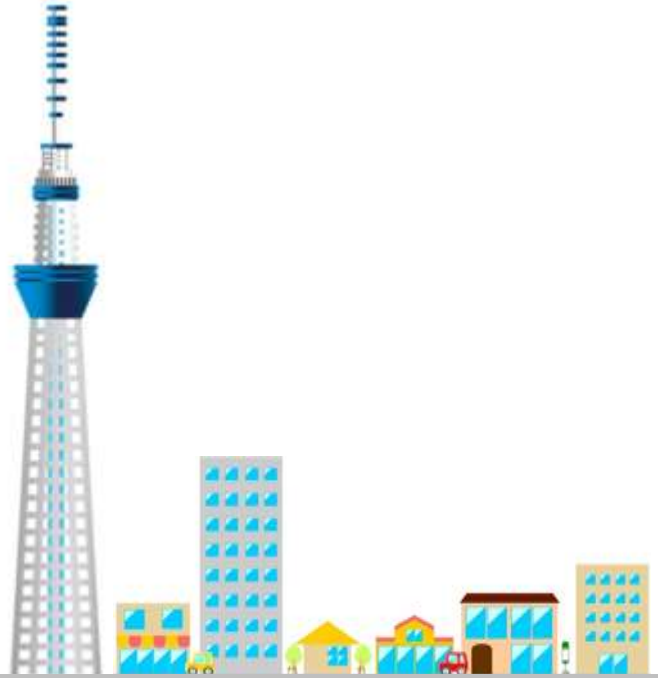


少しずつモジュールを配布しネットワークの負荷を下げる
あとはユーザ任意のタイミングで適用してもらう

ポリシー管理はADを利用　ストアアプリはホワイトリスト運用



ADで管理することでFU後の個別対応がなくなる



まとめ

まとめ

PCのライフサイクルを
短期間に変更

クライアントアプリは
可能な限りMicrosoft

FU配信は
ハイブリッド方式

ポリシーはセンター管理

ご清聴
ありがとうございました