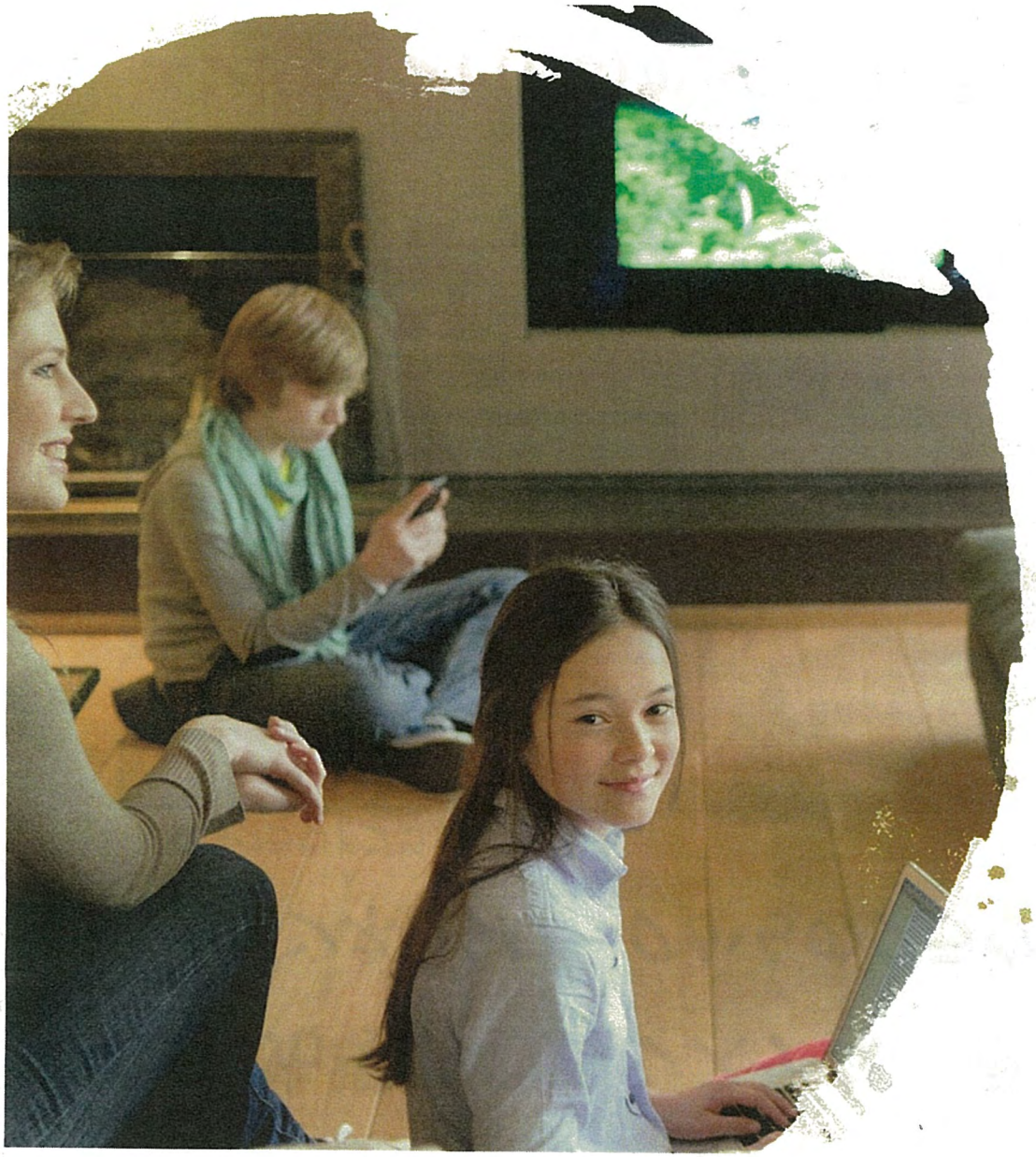
資料２－３



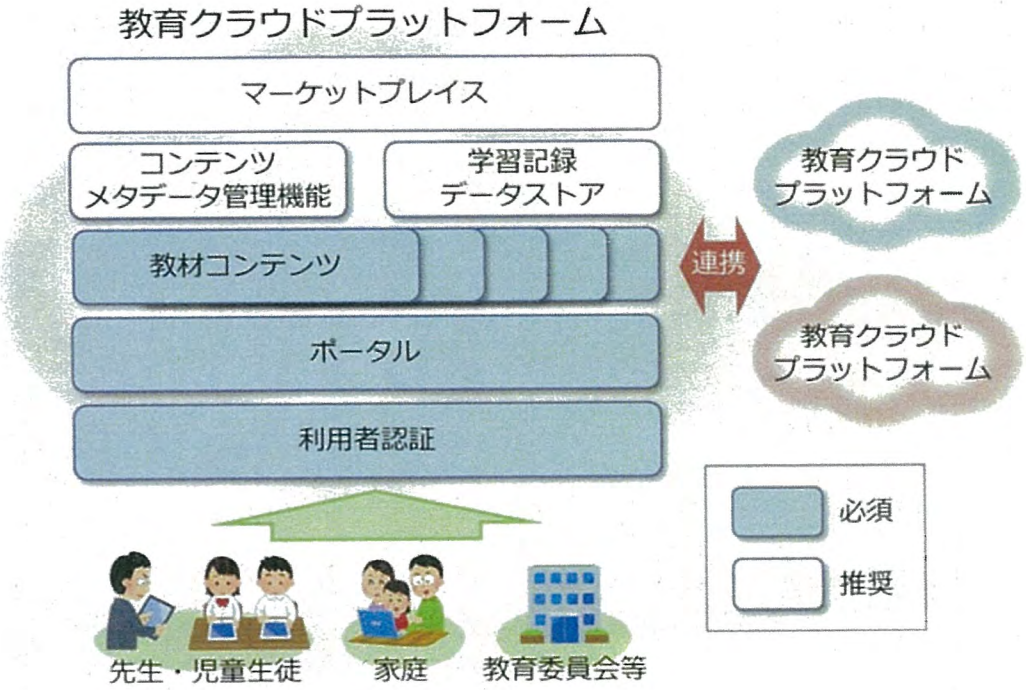
Microsoft

オープンネットワークからのパブリッククラウド利用は安全なのか

2019年1月8日
日本マイクロソフト株式会社
パブリックセクター事業本部
文教営業統括本部

総務省先導的教育システム「高コストパフォーマンス実証事業」

オープンネットワークからのクラウド利用 ＋ 低価格端末の活用



エンドポイント(PC)からクラウドまで、トータルなセキュリティ対策が必要

総務省先導的教育システムのポイント

新しいICT環境

- ✓SaaS (Software as a Service)の利用
- ✓共同調達

セキュリティ対策

- ✓ 利用するクラウドはコンシューマクラウドと区別されていることが重要
- ✓ エンドポイント(PC)からクラウドまで、トータルなセキュリティ対策が必要

教育クラウドプラットフォーム

- ✓「教育の情報化」という次元を超え、EduTech が作り出す「学習中心」の未来を作りだすためのプラットフォームの形成

教育機関へのサイバー攻撃

1. コンテンツを狙った攻撃

相対的に国・公立学校では、お金をたくさん持っていることではないですが、クラッカーは、教育機関を攻撃ターゲットとします。

2017年4月、NUS(National University of Singapore)とNanyang Technological University(NTU)は、政府研究データを収集する攻撃を受けました。

このようなクラッキングは、大学が政治的な軍事戦略や技術に関する研究を政府と協力して実行するために、このような情報を得るため、競争国から攻撃するものと推測されます。しかし、思ったより多くの大学がサイバー脅威に対応する準備ができていないという問題点があります。2016年3月には、英国大学の30%以上が毎時間サイバー攻撃を経験していることが明らかになりました。

2. メールアドレス取得を狙った攻撃

よくクラッカーたちが狙うデータと言えば、クレジットカード番号のようなことを思い出すが、実はダークウェブで最も人気のあるアイテムは学生のメールアドレスです。

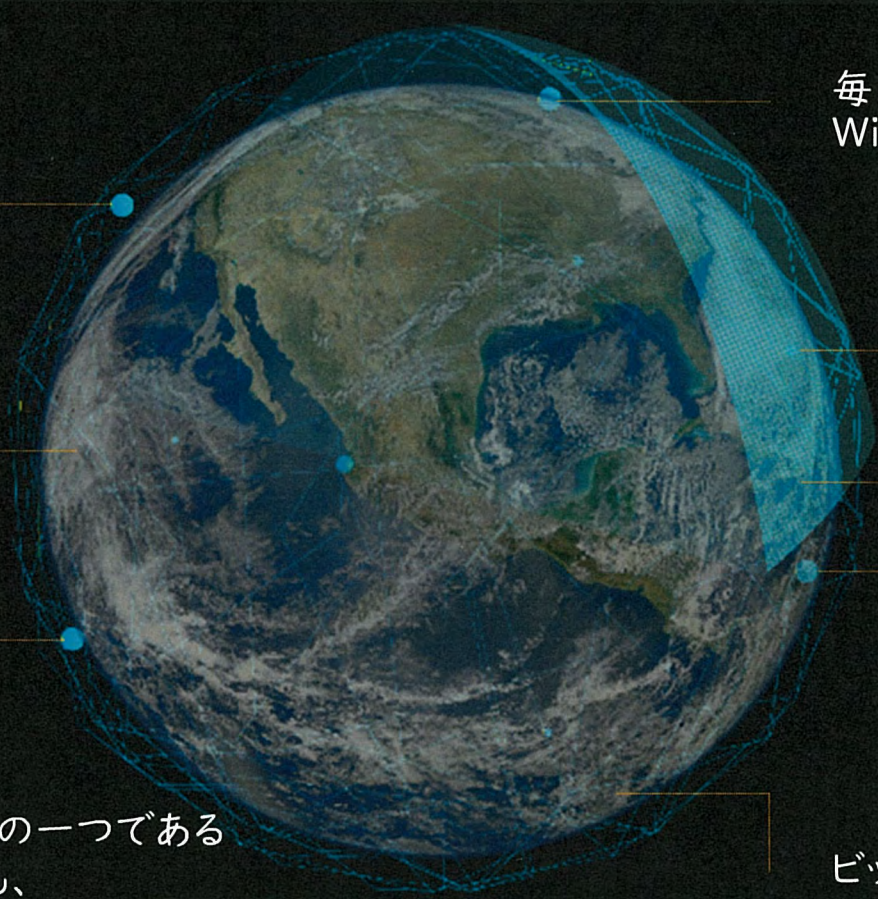
2017年3月、デジタル市民連合(Digital Citizens Alliance、DCA)は、犯罪者が大学の資格証を盗んで、これを活用することに対する調査結果を発表しました。2017年現在、ダークウェブには約1千4百万個のメールアカウントがあり、これは、3.50ドルから10ドルに販売されています。なぜよりによって学生たちのメールアドレスが人気でしょうか。普通、高価のソフトウェアやその他の製品は学界の人々に大幅に割引された価格で提供されたりするからです。

さらにクラッカーは、教育機関が保有したさらに敏感なデータへのアクセス権限を得るためにこのアドレスを使用することもできるかもしれません。例えば、クラッカーはIDを盗用し、学校寄付金のリストまたは使用可能な金額に対する情報にアクセスしようとすることもできるからです。

3. ネットワーク活用に向けた攻撃

クラッカーたちは、クラッカー活用のためのハッキング攻撃も頻繁に行います。規模が大きかったり、権威のある大学の場合、膨大なコンピューティングシステム・ネットワークを保有しているために、このようなインフラはフィッシングを通じてさらなる攻撃をために、または教授や学生がよく利用するウェブサイトに悪性コードを挿入するのに使われることができます。もちろん、すべての学校のセキュリティアーキテクチャが不足したものではありません。多くの流出事故は大学のシステム上で行われるより、教職員や学生たちが定期的に訪問するウェブサイトやプラットフォームから発生するためです。

マイクロソフトの地球規模でのセキュリティデータを用いたセキュリティー対策



2,000 万社以上の企業、
10 億人以上のユーザー、
などビジネス・
コンシューマ双方に
クラウド サービスを提供

検索エンジンを通じて
毎月 18 億以上の
Web ページをスキャン

世界で最も攻撃を受けている組織の一つである
マイクロソフト社としても、
世界 15万 ものユーザーを攻撃から保護

毎月 10 億台以上の
Windows デバイスが更新を適用

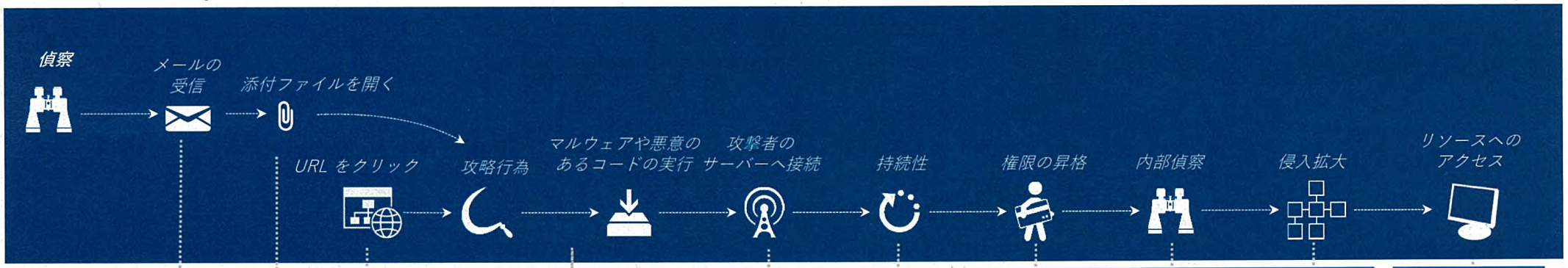
毎月 4,500億件の
ユーザー認証を処理

年間 1,100 億円以上の
セキュリティ研究・開発

毎月 4,000 億通
のメールを分析

ビッグデータ・AI を活用した
セキュリティ運用の自動化にも投資を継続

Cyber Kill Chain: 攻撃者の主戦場は学内・社内ネットワーク

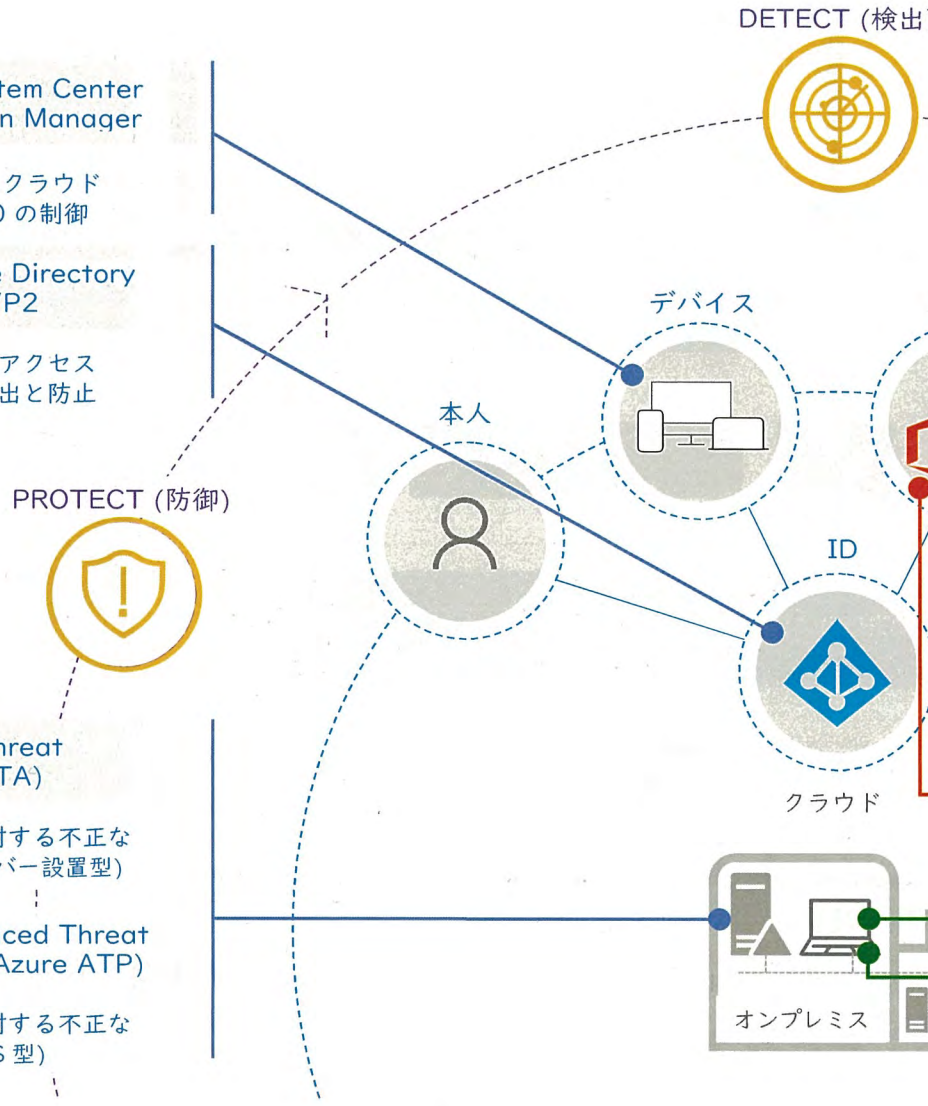


偵察 Reconnaissance	配送 Delivery	攻撃 Exploitation	インストール Install	遠隔操作 Command & Control	侵入拡大 Lateral Movement	目的達成 Objectives
Protect	**なしすまし メール着弾** 悪意のある添付ファイルや悪意のあるサイトに誘導するための URL が記載されたメールが着弾	**悪意のあるサイトへの誘導** 悪意のあるサイトへ誘導してバックドアを仕込む **悪意のある Office マクロやスクリプトの利用** 攻撃者のサーバーに接続するためのツールとして悪用 **拡張子を偽装した添付ファイルの利用 (RLO 攻撃)** Exe を実行させるために拡張子を右から左に変更し、アイコンを Office や PDFに偽装する	**既知のマルウェア** ウイルス、ワーム、トロイの木馬、スパイウェアなど既知のマルウェア攻撃 **ランサムウェア** データを暗号化し暗号化解除に仮想通貨での支払いを要求する **ファイルレス攻撃** 実行ファイルを利用せず、Power Shell やコマンドなど正規のプログラムを攻撃に活用 **正規のプロセスになりすまして攻撃** プロセスホロウィングなど正規のプロセスに偽装して攻撃を行う	**不審な IP アドレスとの通信** ハッカーのサーバへの通信を確立させ攻撃を継続化させる **攻撃の持続性確保** タスクスケジューラやレジストリの変更により攻撃の持続性を確保	**OS の脆弱性を利用した権限の昇格** MS14-068やMS11-013 の悪用など **ドメインを乗っ取るためのネットワークの内部調査** 同じネットワークにいる端末に横展開するための偵察行為 **他の端末に不正アクセス** Mimikaz や psexec などのツールを使用し、Pass the Hash や Pass the Ticket を利用した不正アクセスを実施	**ドメイン侵害** ドメイン Admin の資格情報を保有する端末に不正アクセスし資格情報を不正に取得
Detect						
Respond						

一連の攻撃プロセス全てが学内・社内 LAN 内で行われる

Microsoft 365 によるセキュリティの徹底

Office365 EMS Windows10



EMS : Intune, System Center Configuration Manager

デバイスの設定管理、クラウドベースの Windows 10 の制御

EMS : Azure Active Directory Premium P1/P2

クラウドの認証基盤とアクセス制御、なりすましの検出と防止

EMS : Microsoft Cloud App Security (MCAS)

アプリを監視し機密・個人情報を検出、保護 (CASB)

EMS : Azure Information Protection P1/P2 (AIP)

機密情報を検出、分類、暗号化、追跡/権限はく奪

EMS : Advanced Threat Analytics (ATA)

Active Directory に対する不正なふるまいを検出 (サーバー設置型)

EMS : Azure Advanced Threat Protection (Azure ATP)

Active Directory に対する不正なふるまいを検出 (SaaS 型)

Office 365 : Threat Intelligence, Attack Simulator

自社のテナントへの攻撃情報を可視化、攻撃シミュレーション

Office 365 : Office 365 Advanced Threat Protection

不正な添付ファイルやリンクへの誘導を防御

Win10 : Windows Defender System / App / Exploit Guard

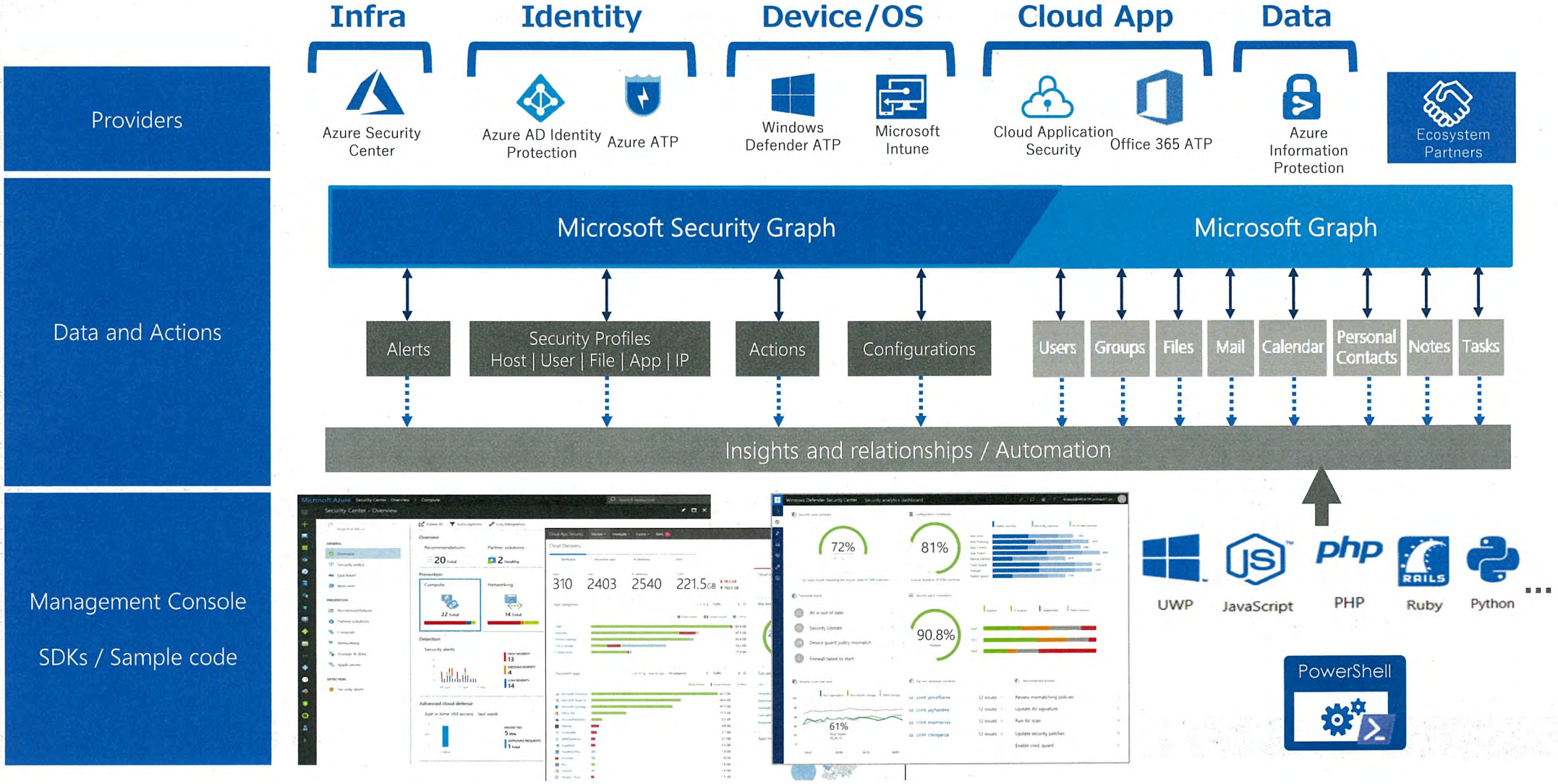
エンドポイントセキュリティ

Win10 : Windows Defender Advanced Threat Protection

エンドポイントのふるまい検知、フォレンジック機能 (EDR)

インフラ (IaaS/PaaS) から認証、デバイス、データまで一気通貫のインサイトと管理

セキュリティの自動化を実現するビジョンのもとに各セキュリティ ソリューションを設計



オープンネットワークからのクラウド利用のまとめ

- ✓ 攻撃の着弾点となるパソコンの保護
  - エンドポイントセキュリティ
  - エンドポイントのふるまい検知
- ✓ 被害拡大の要因となるIDの保護
  - 多要素認証、リスクベース認証
- ✓ 第三者がデータを読めないようにデータを保護
  - ユーザー認証ベースのデータの暗号化
- ✓ クラウドサービスを安全に利用するために
  - なりすましの検出と防止
  - アプリの監視し、個人・機密情報の漏洩の検知、保護
  - ML, AI を利用した高度なセキュリティ検知

クラウドを利用する上での検討事項

- ✓ SaaS (Software as a Service) を積極的に利用することが重要

  ⇒ 既存の予算と SaaS 採用によるコスト削減により更なるICT環境整備が可能となる

- ✓ 採用するクラウドは新のエンタープライズクラウドである必要があり、コンシューマクラウドベースのサービスは採用すべきでない

  ⇒ セキュリティーの観点から

- ✓ 世界の潮流は「個別最適化学習スタイル&eポートフォリオ時代にむかっての教育サービス提供」であり、これらを実現できるコンポーネントをもつクラウドを採用すべきである

  ⇒ ML, AI の活用