クラウド時代の
セキュリティ基盤の考え方と作り方

日本マイクロソフト株式会社
Chief Security Officer
技術統括室
河野 省二, CISSP

Microsoft

クラウドは安全か？

- という議論はもうやめましょう
  - 各社ともそれなりに安全です
  - ハードウェア環境についても整備され、正しい運用ができるようになりました
- 今の課題は・・・サイバーセキュリティ経営
  - サプライチェーン
  - ガバナンス
  - 平時の情報開示　など
- 情報の保護
  - 機密性だけではなく、完全性も可用性も保護しなくちゃいけないのに、相変わらず暗号強度の話ばかりしている人がいる

サプライチェーン管理の課題

委託時に監査、その後は1年に1度のオンサイト監査

それで本当に安心できますか？

事故の影響を軽減するためには、どのような対策が必要でしょうか

監査チェックリストの有効性

- 自分たちのやっているセキュリティ対策を押し付けていませんか？
  - 自分たちが勝手に作ったチェック項目を相手に求めても、結果としてセキュリティを確保することはできません
  - 対策の目的を共有するのならば良いのですが、対策そのものを共有しても負担になって「抜け道」を探すだけになってしまいます
- 共通プラットフォームの利用が最適
  - マイクロソフトではセキュリティポリシー文書を読んで、それを個人が実践することはありません。すべてITプラットフォームの中に組み込まれていて、その範囲で自由に仕事をすることができます

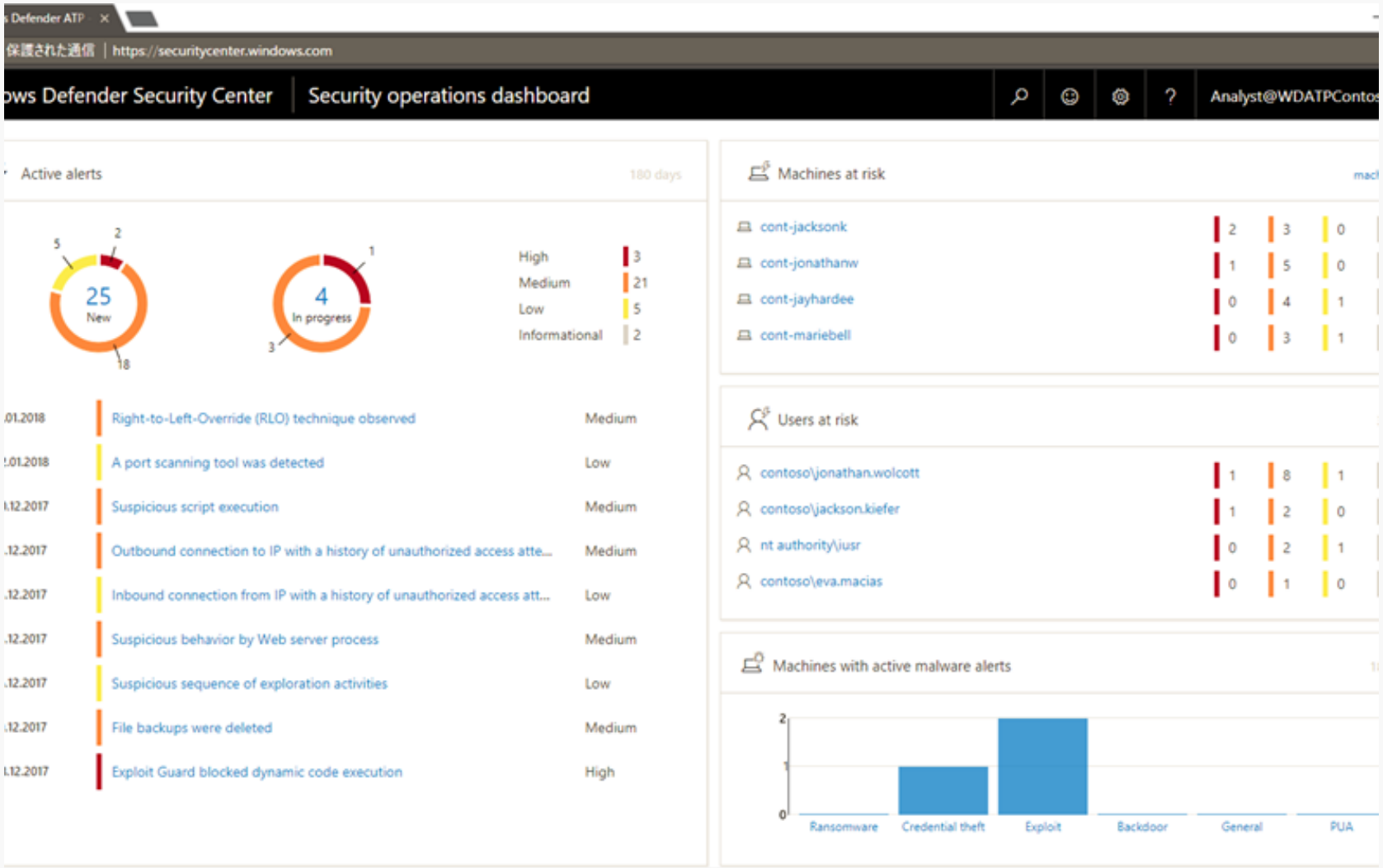
共通基盤としてのクラウドサービス

- プラットフォームとしてクラウドサービスを利用
  - とはいうものの、IaaSを使ってもあまり意味がない
  - PaaSやSaaSで基本的なセキュリティを組み込んだ形で利用する
- レポートも共通
  - PaaSやSaaSで得られるレポートは共通かつ客観性が高いので、信頼性をもってそれを活用することができる
  - 必要なレポートを必要な時に取り出すことができる
- 継続的監視の実践
  - 監査は4半期に1回程度が望ましいが、リアルタイムに実施できるのが最も良い

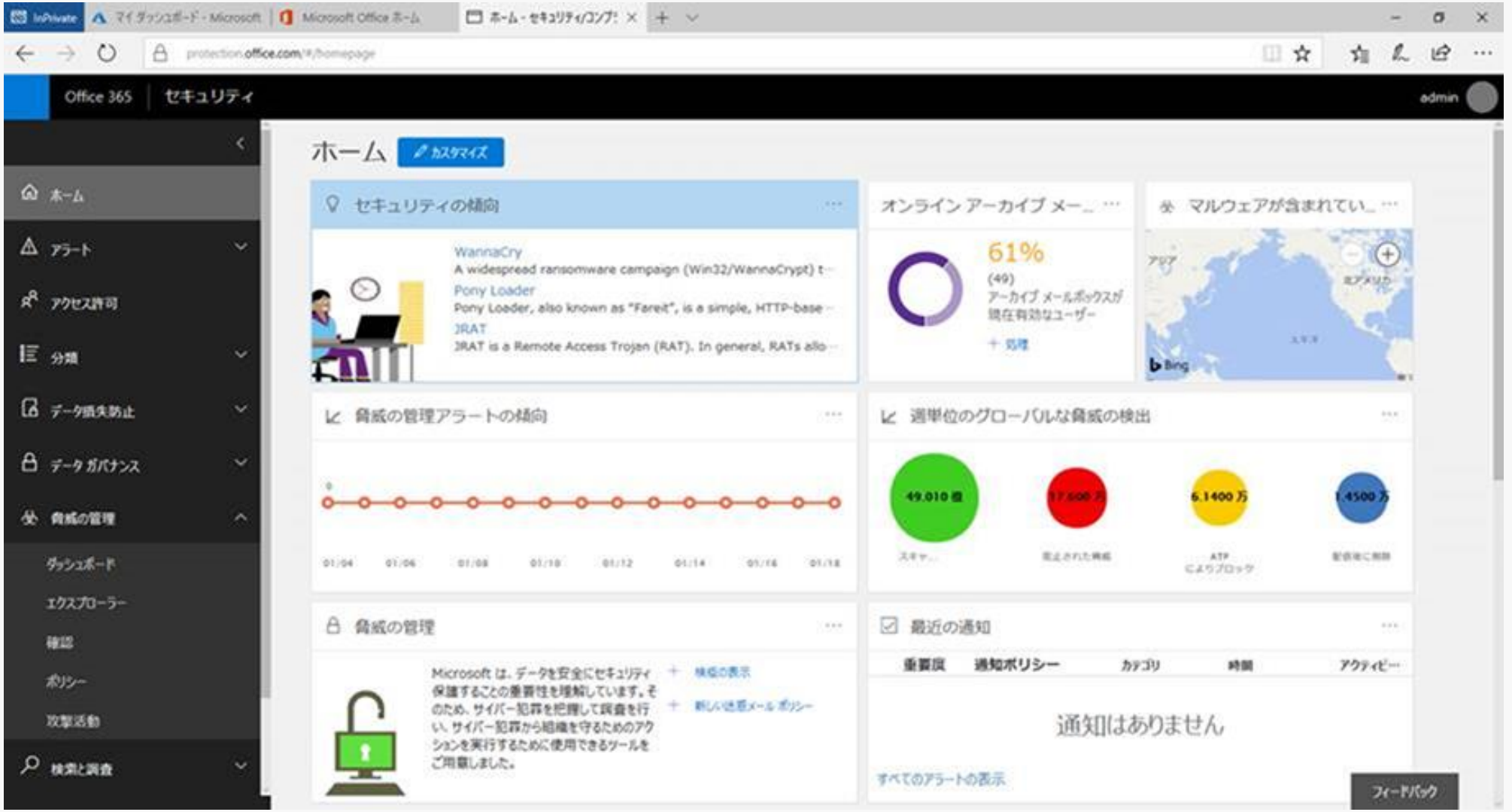
オンサイト監査に代わるもの

- オンサイト監査ではなくダッシュボードを活用
  - SaaSやPaaSにはダッシュボードが用意されています
  - これらのダッシュボードを見ることで、オンサイト監査の代わりをすることが可能です
  - ダッシュボードの閲覧権限が与えられていれば、委託先の監査は日常的に行うことができます
- 継続的な監査の実践
  - 通常時を理解することができるので、異常検知もたやすい
  - セキュリティだけではなく、事業継続やビジネス影響度も同時に判断できるので、コストパフォーマンスの高い見える化が可能

Windows Defender ダッシュボードの一例



Office 365 ダッシュボードの一例



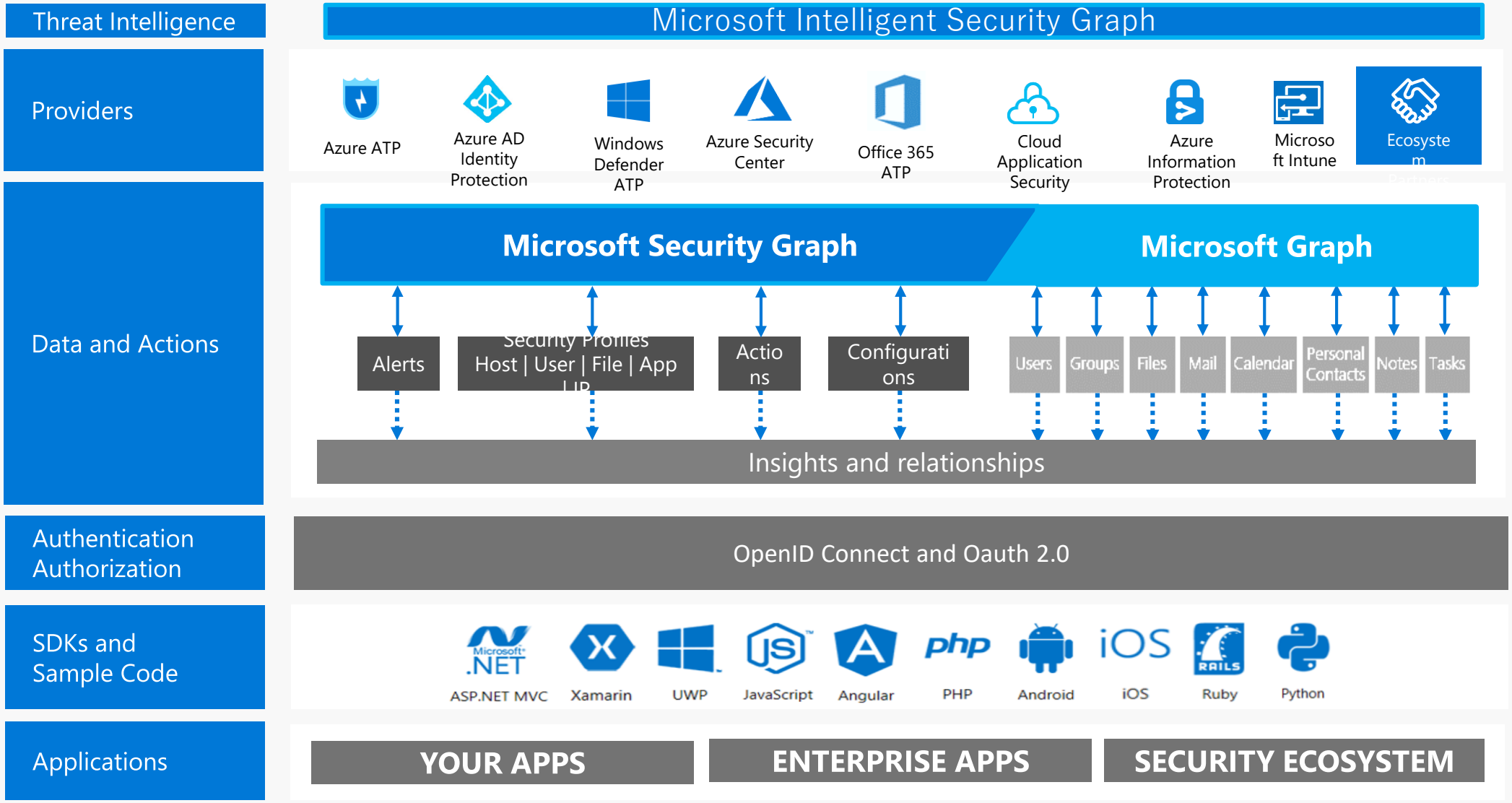
クラウド導入時の判断

- クラウドサービスのセキュリティ認証
  - ISO/IEC 27017 (ISO/IEC 27001が必要)
  - ISMSクラウドセキュリティ認証
  - CSゴールドマーク・シルバーマーク
  - Cloud Security Alliance STAR認証
- 認証を取得していることで最低限のセキュリティ管理ができていることを証明
  - ISO/IEC 27017はプロバイダーとカスタマーの情報連携が正しくできることを保証している（CSマークも同様）

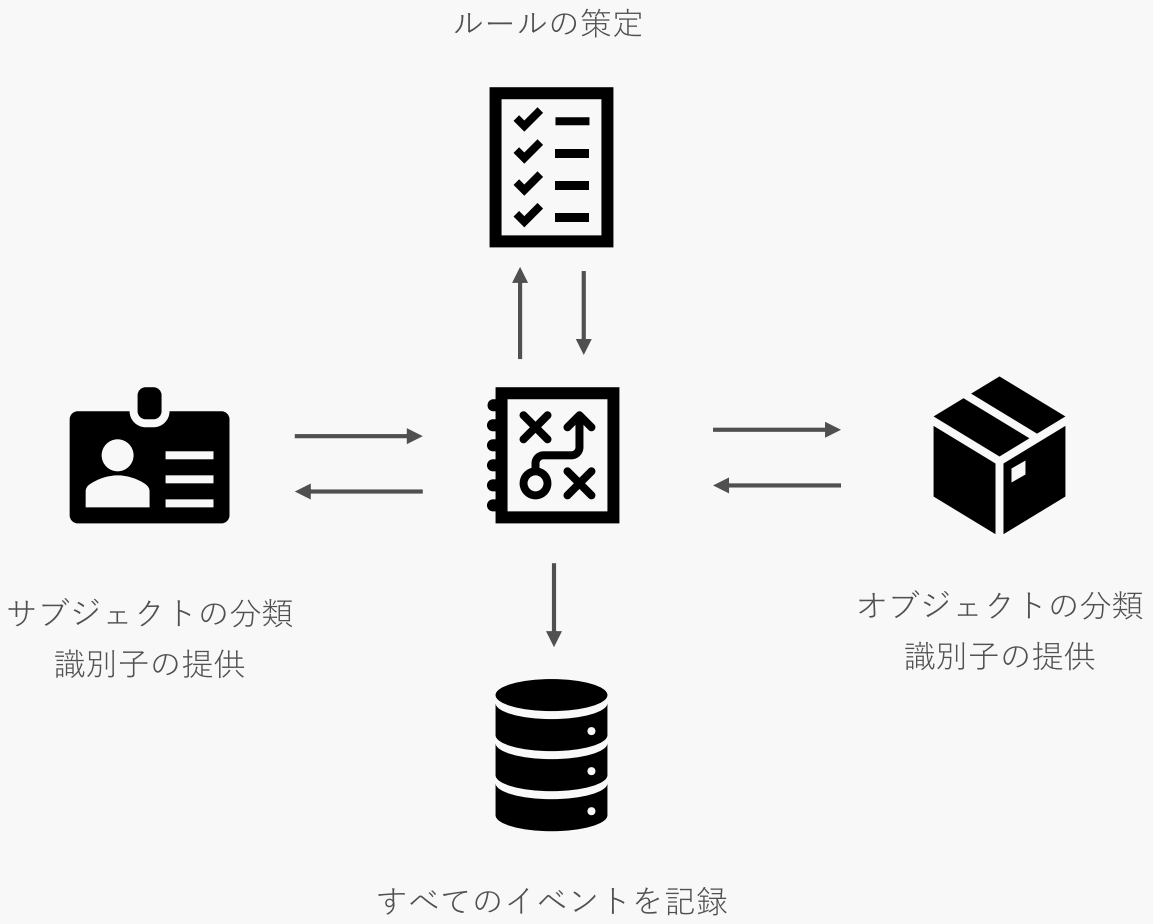
認証取得済みクラウドサービスの評価

- 三菱総合研究所様による調査
  - CSゴールドマークをベースにしながら、オンプレミス、データセンター、認証取得済みのクラウドサービスについて比較している
  - 監査の観点に利用しやすい内容になっている
  - 結果として、（CSゴールドマーク）認証取得済みのクラウドサービスの安全性が高いことがわかった

Microsoft 365 Graph API



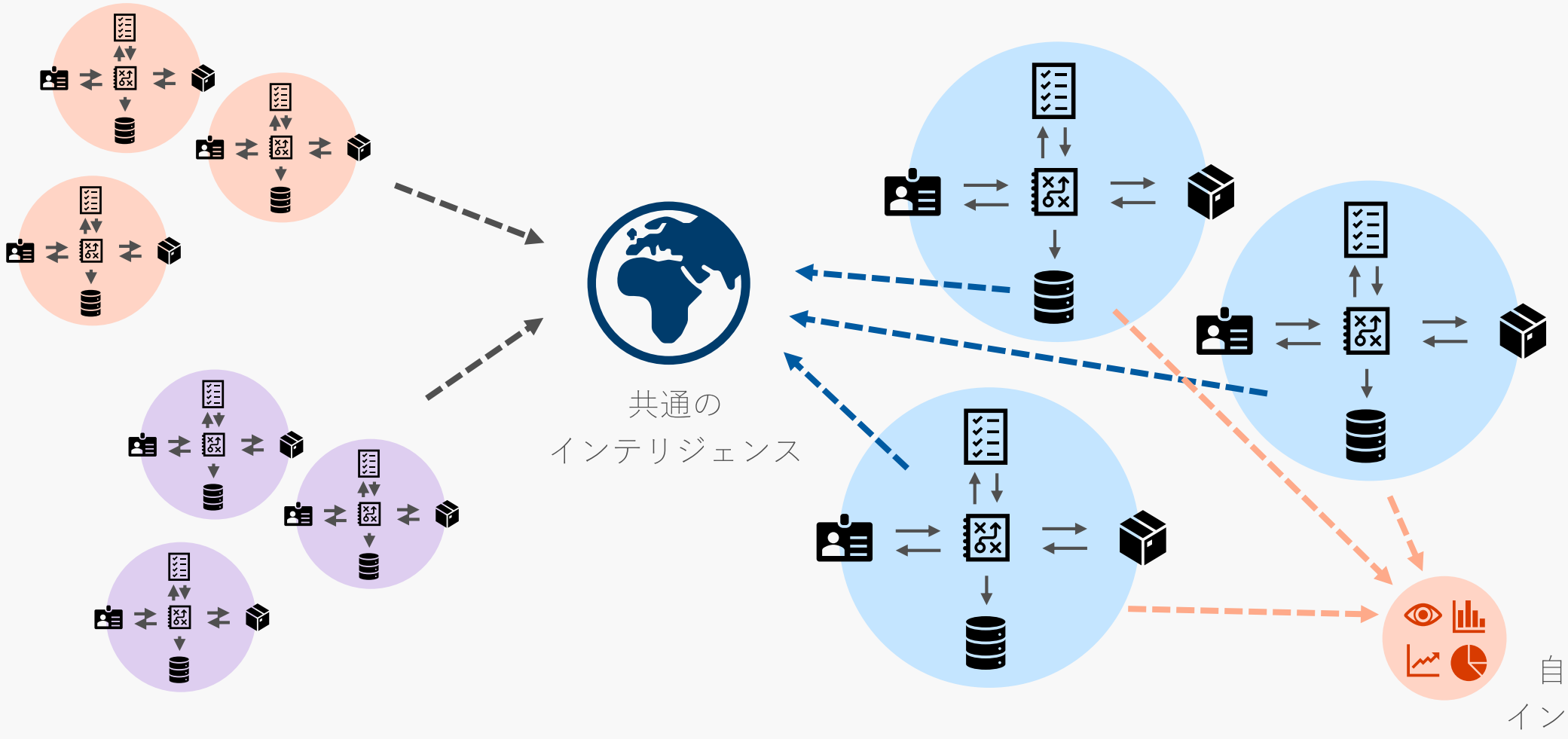
すべてのデータを取るための仕組み



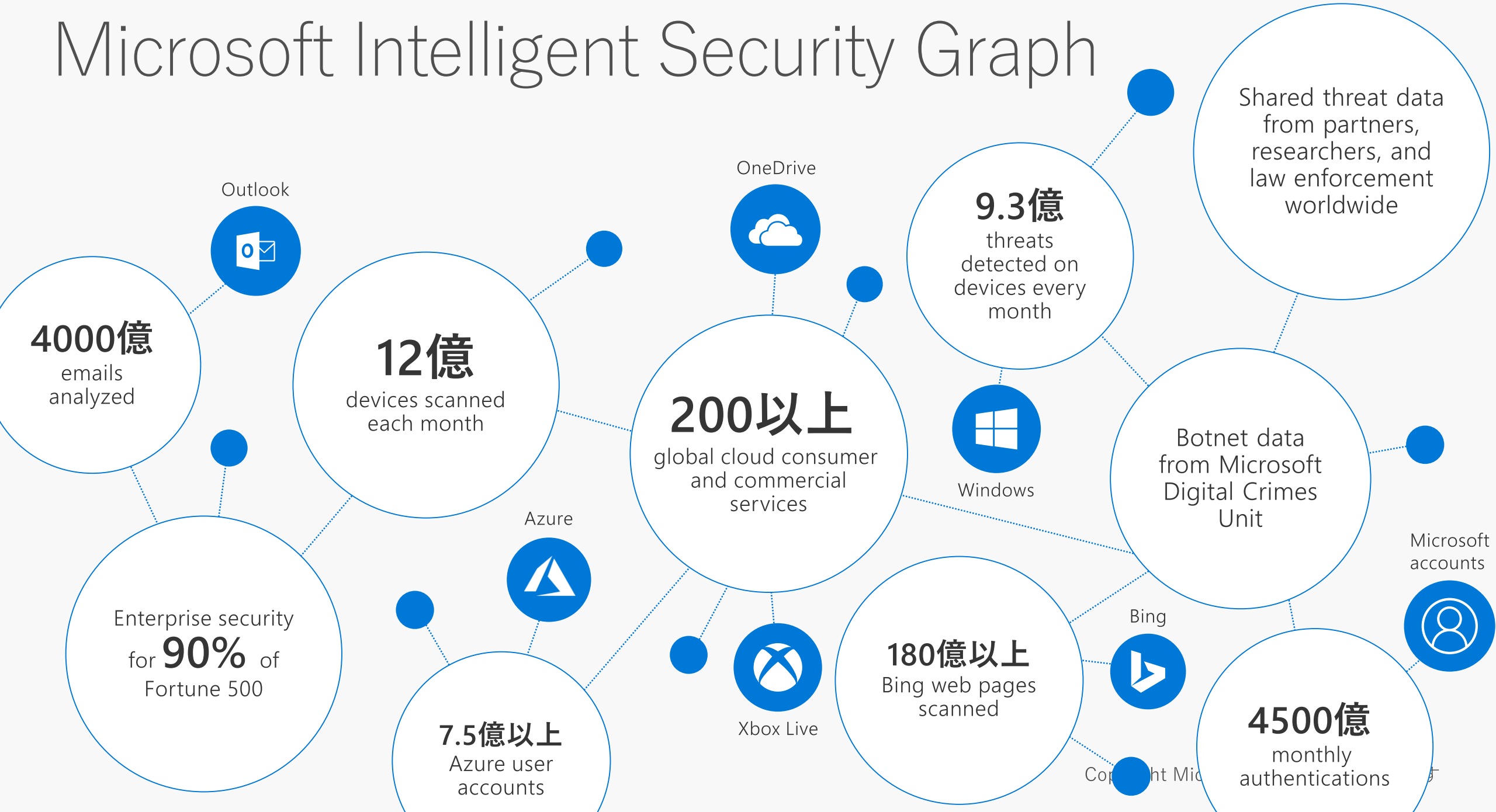
完全仲介システムの提供

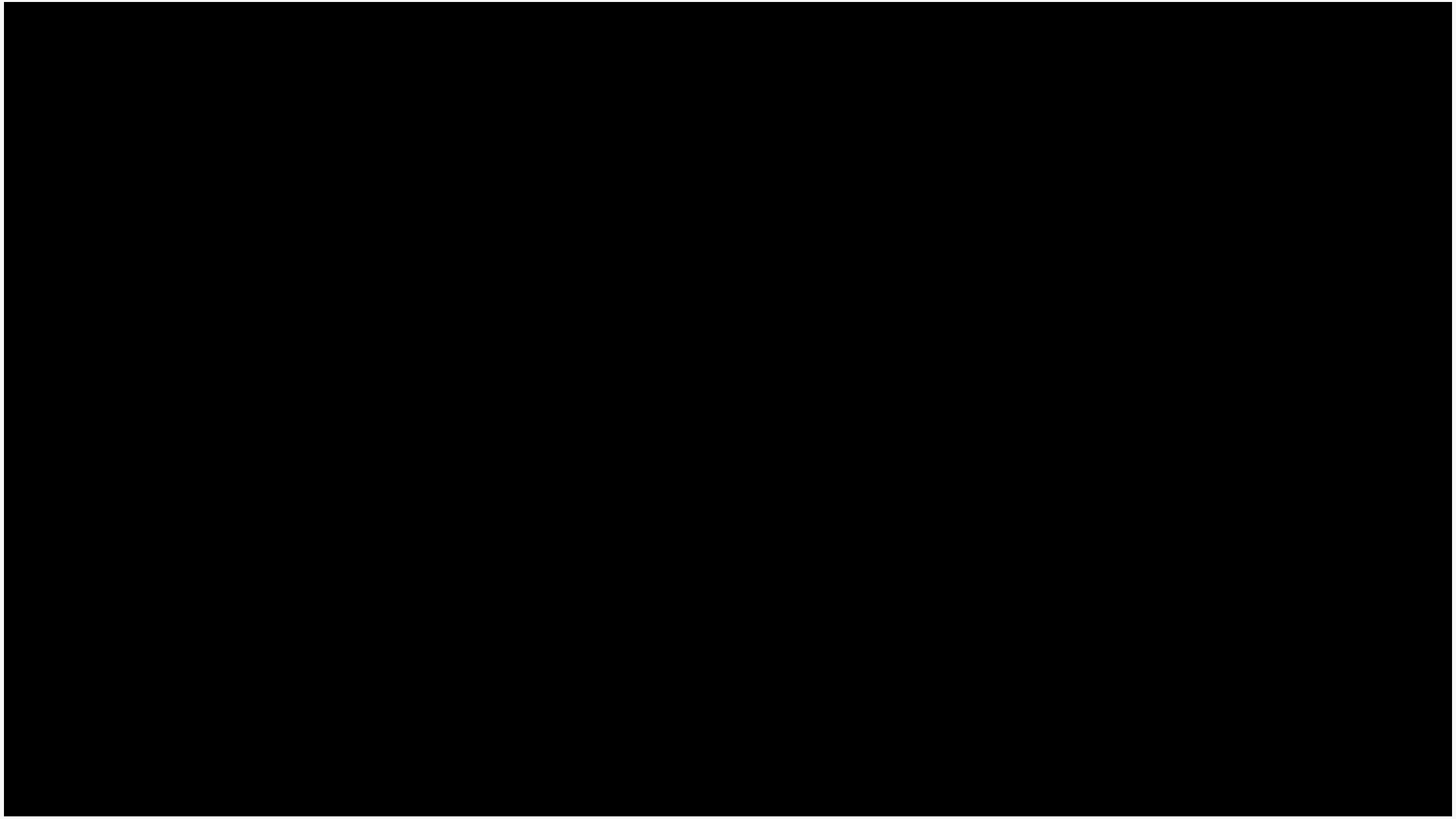
- 組織内に存在するすべてのものにID（識別子）を付与する
- すべてのアクセスがルールの上で判断される
- すべてのイベントを記録する
- 例外を許さない

セキュリティインサイトとインテリジェンス



Microsoft Intelligent Security Graph





90パーセント以上が新しい攻撃

ソーシャルエンジニアリング

専門家不足

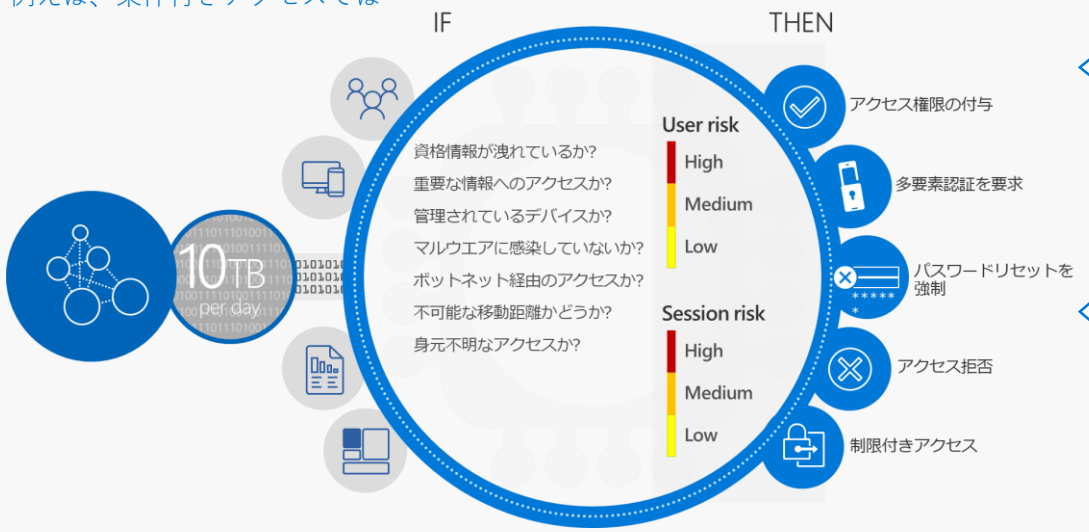
増え続ける資産

働きかた改革

セキュリティの自動化

クラウド利用でさらに広範囲に

例えば、条件付きアクセスでは



インテリジェンスインサイトの活用 → リスクに応じたルールの自動作成 → ルールの自動適用

すべての資産にIDを付与

ユーザだけではなく、デバイス、アプリ、そして場所にまでIDを割り当てることで、きめ細やかなアクセス制御を実現できます。

正常値に基づくふるまい検知

攻撃者のふるまいデータだけでは、異常検知を正確かつ効率的に実施することはできません。ユーザのふるまいを把握することで、迅速かつ適切な対応が可能になります。

ルールの自動作成と自動適応

ユーザのふるまいから生成する正常値を知っているからこそ業務ルールの自動生成が可能です。アプリケーションやドキュメントの権限管理をベースに、必要な作業を止めることなく利用が可能です

Azure Active Directory Premium

クラウド上の資産やサービスを管理し、さらにオンプレミスとの連携を行うためのID管理環境を構築します。サービスを含めた資産の一元管理のための必須条件です。

Windows Defender ATP

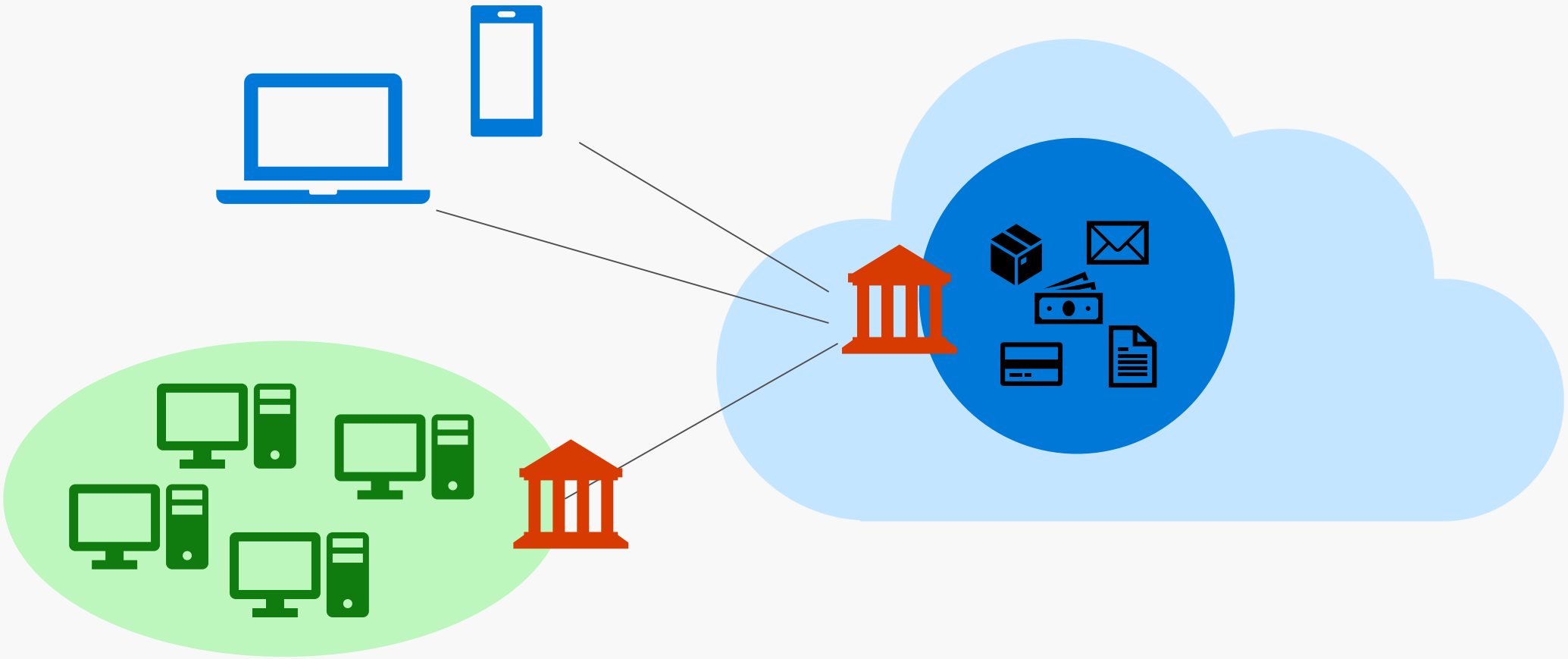
アンチマルウェアだけではなく、様々な攻撃や脅威の検知と自動対策を実現しました。事故が発生した際のセキュリティ専門家とのコミュニケーションを円滑にするためのダッシュボードで少人数のCSIRTづくりも可能です。

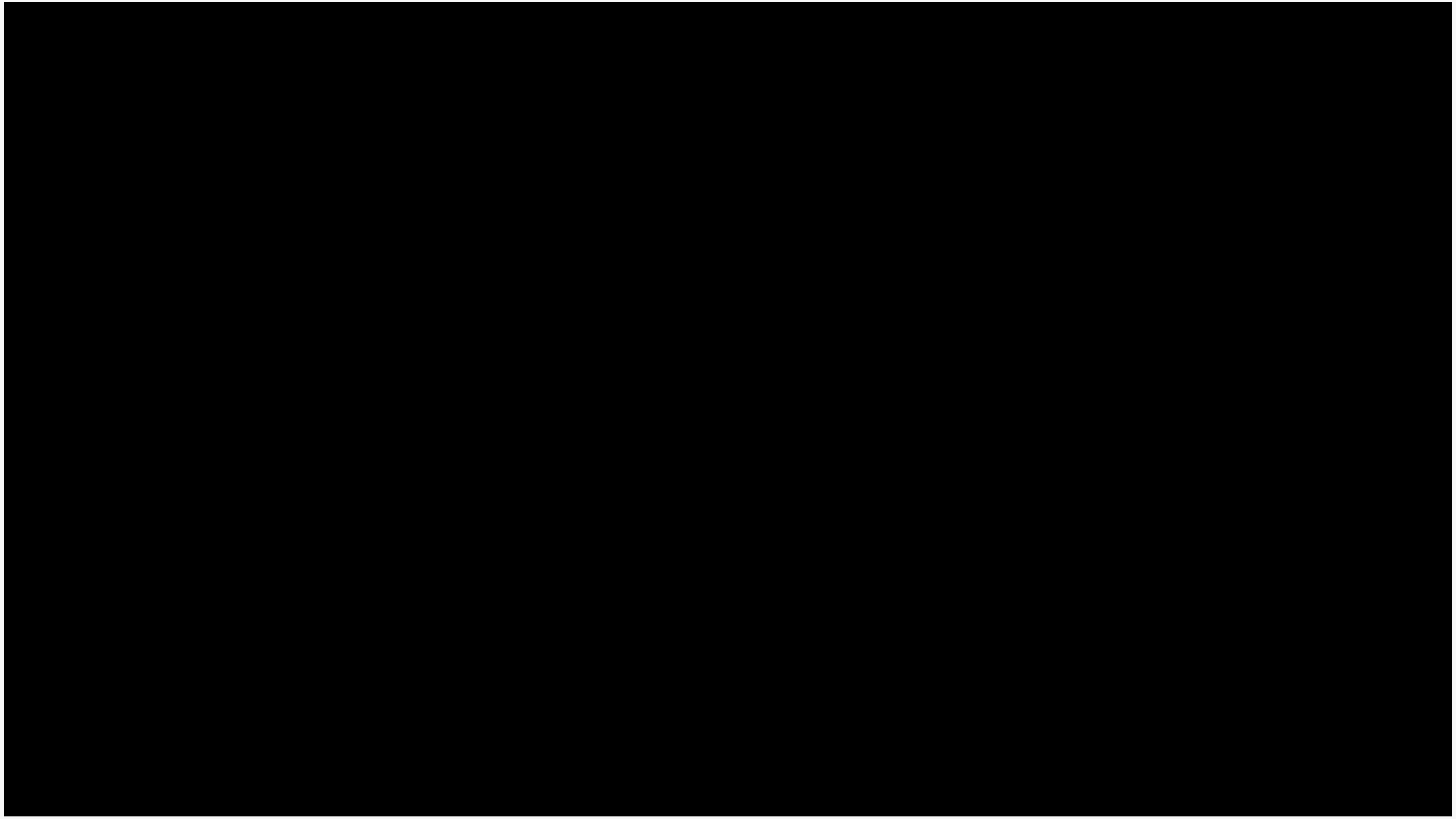
Microsoft Security Graph

週に5000億以上のメール、月に5000億以上のログイン情報から作成したインテリジェンスを活用して自動制御のための情報を提供します。組織のインサイトとAPIベースで連動させて活用していただくことが可能です。

生産性を損なわずに、ITを使い続けられるための基盤づくり – Micrsoft Securityはセキュリティプラットフォームを提供します

「境界」はどこに置くのか





攻撃手法から知る次世代のクラウド

2017/09/13

ニュース解説

ファイルを一切作らない新型ウイルスの脅威

勝村 幸博＝日経NETWORK　　日経NETWORK

トレンドマイクロは2017年8月中旬、感染パソコンに痕跡を残さない新型の「ファイルレス」ウイルスが確認されたとして注意を呼びかけた。ファイルレスウイルスはパソコンにファイルを作成しないウイルス。今回の新型は、従来のファイルレスウイルスよりも痕跡を残さないという。

メモリーに直接読み込まれる

一般的なウイルスは、ファイルの形でパソコンに侵入する。ユーザーがファイルを開くとメモリーに読み込まれて動き出し、悪質な動作をする。

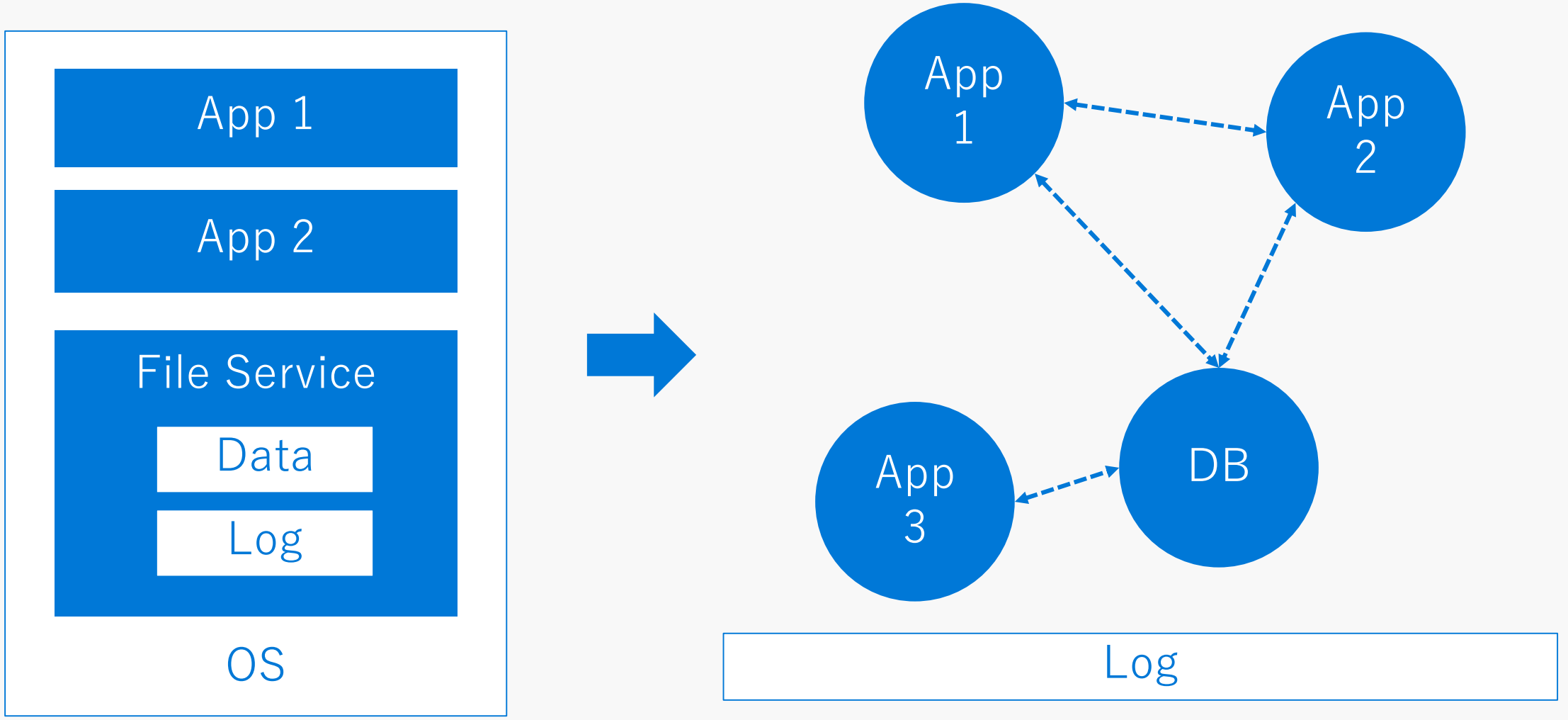
一方、ファイルレスウイルスは、ハードディスクにファイルを作成しない。ウイルスのプログラム（コード）をメモリーに直接読み込ませて動作する。このため、ファイル単位で検索する通常のウイルス対策ソフトでは検知できない。

ファイルレスウイルスの多くは、ウイルスプログラムの隠し場所にレジストリを使う。レジストリとは、Windowsの設定情報などを格納しておくデータベース。テキストベースの単なる情報だけではなく、ダイナミックリンクライブラリ（DLL）などのプログラム

どうしてこういう攻撃が研究されているのか・・・

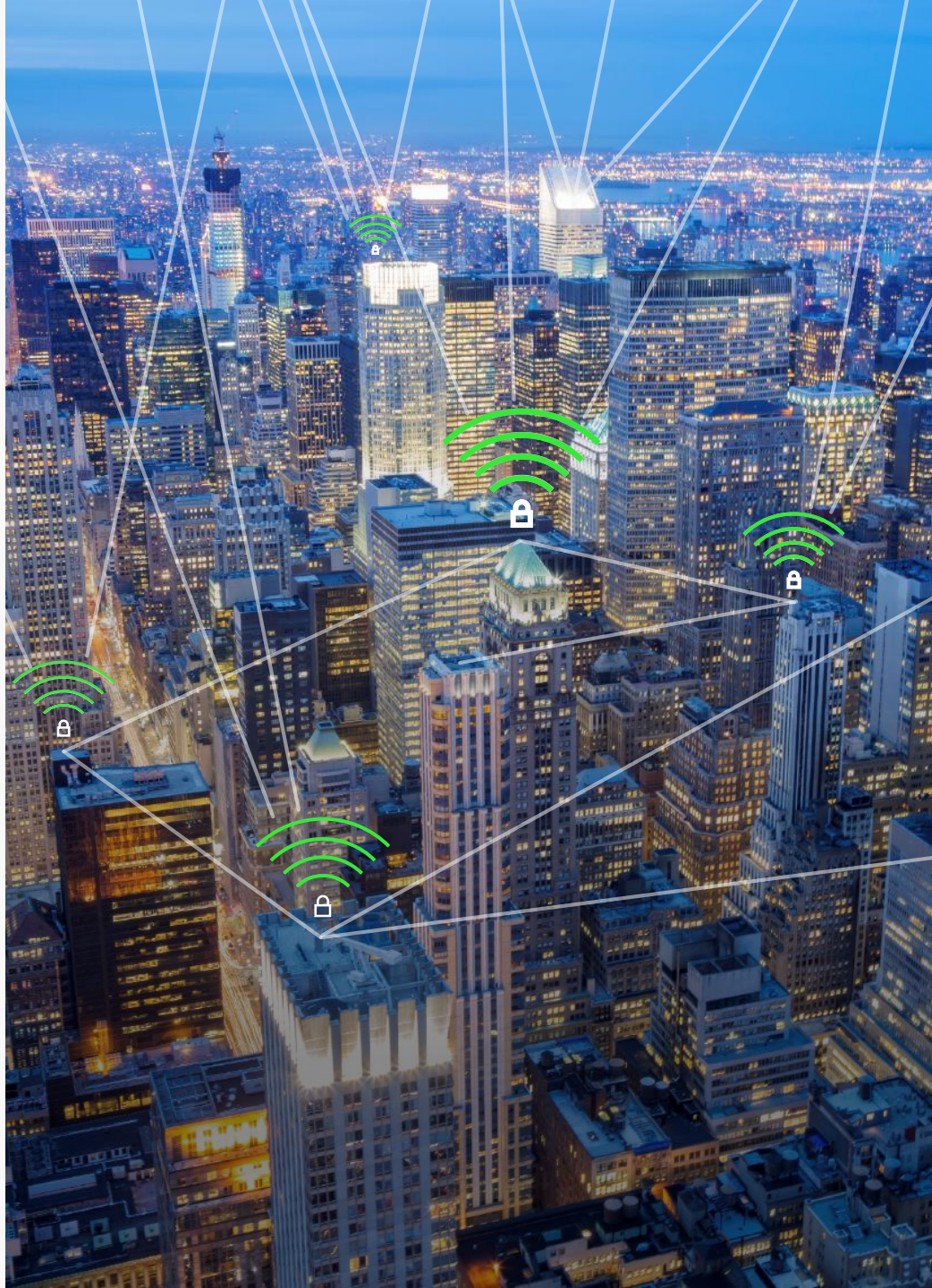
- これまでの攻撃はファイルシステムを使っていた
- ファイルシステムがなくなったら攻撃ができなくなってしまうので、新しい攻撃が試されている
- この攻撃は効率的だろうか？

クラウドサービスにOSは必要ない



Microsoft Secure

包括的なプラットフォーム、独自のインテリジェンス、幅広いパートナーシップを通じて、デジタルトランスフォーメーションによるセキュリティを確保します



Microsoft