エンドポイントセキュリティ自動化のための IT基盤の作り方

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

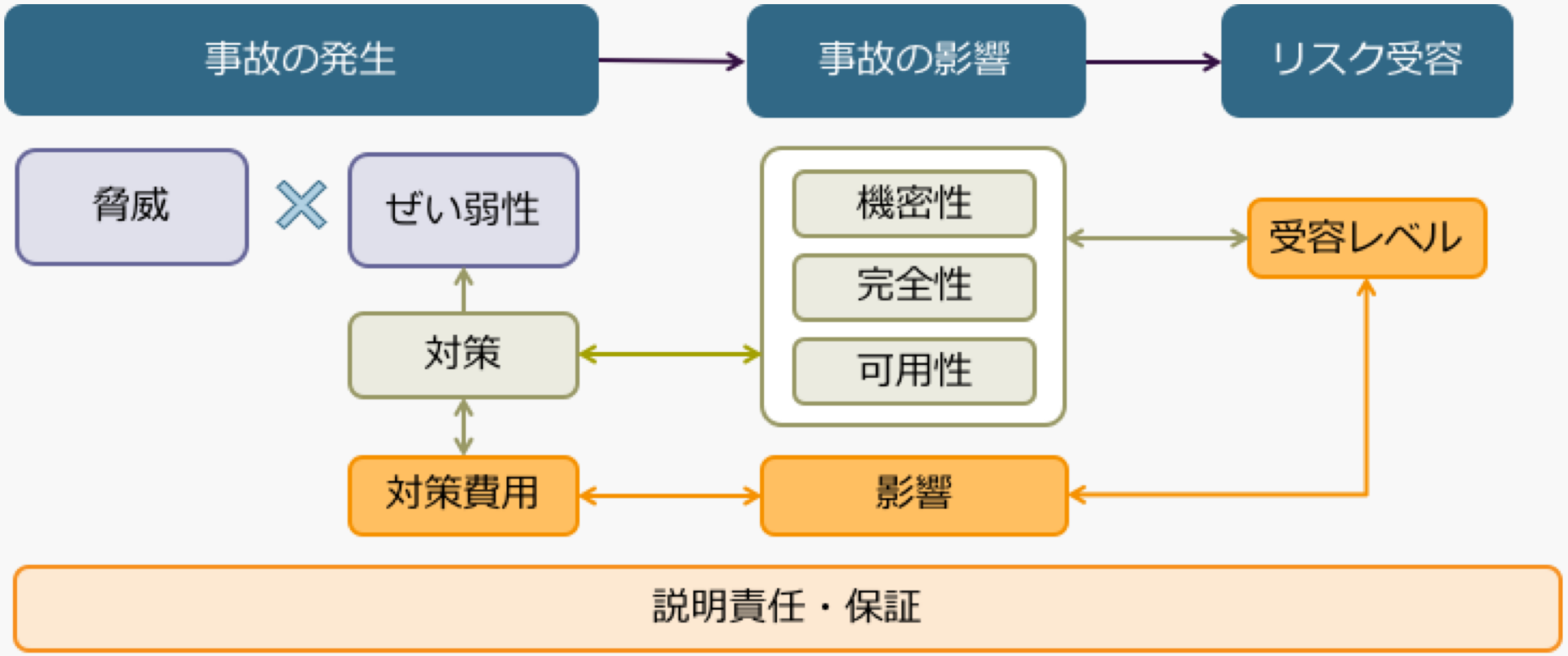
Microsoft

セキュリティに求められているもの

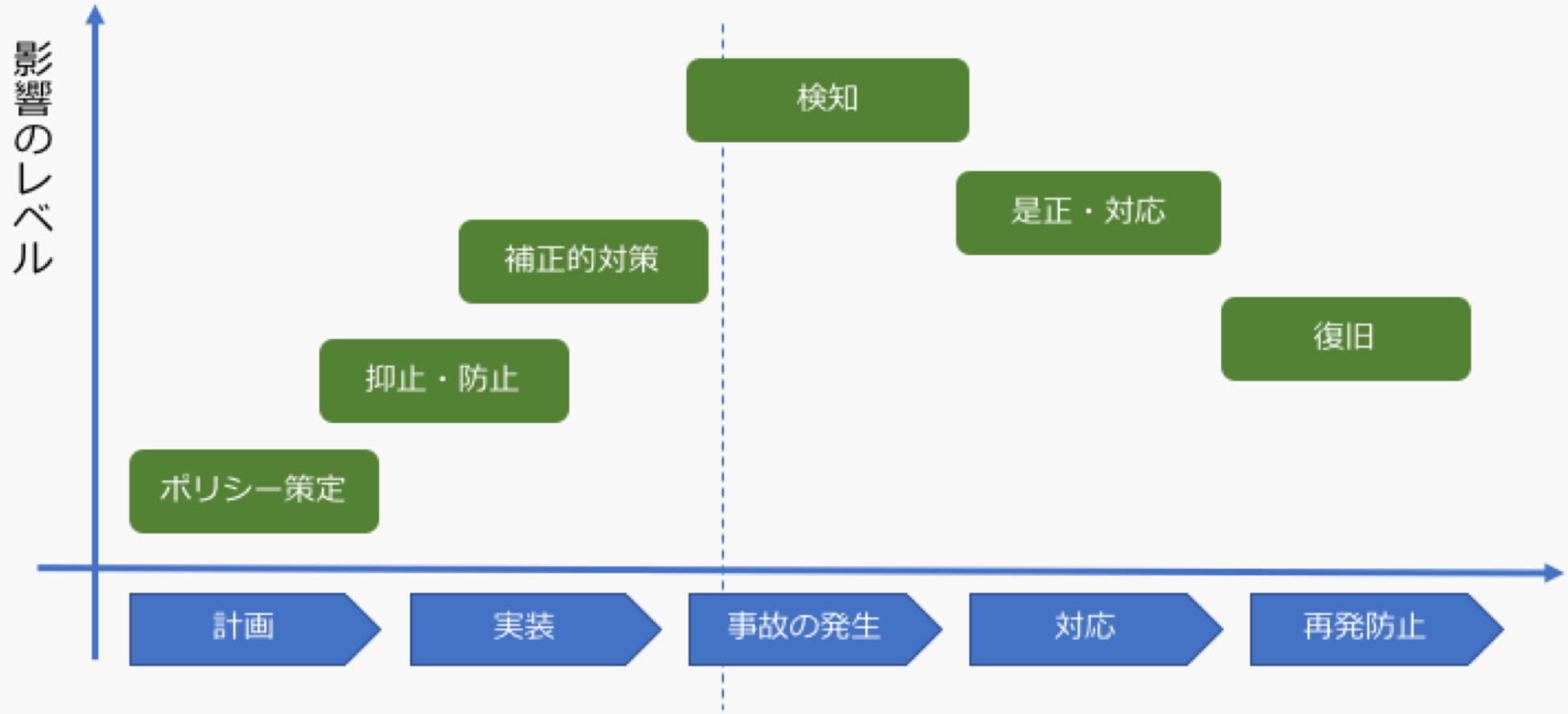
Keep Productivity with Sec

生産性を損なわないセキュリティ

リスクマネジメントフレームワーク



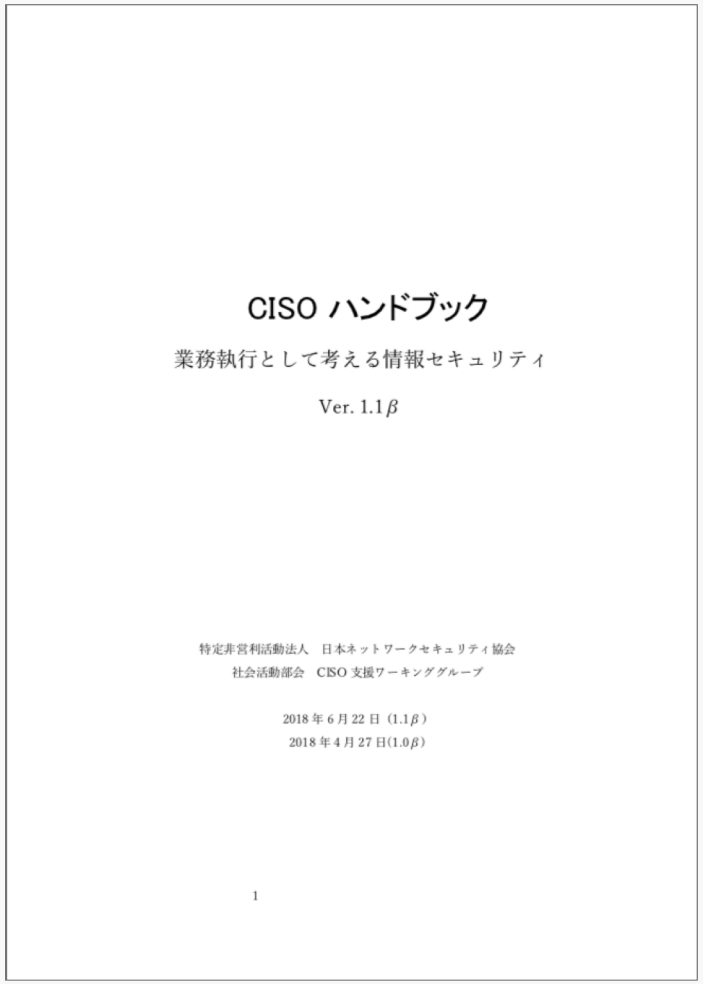
迅速な検知、対応では間に合わない



事故を検知した時の対応

- 事故に気が付いたら影響を低減するためにPCをシャットダウンするという勘違い
  - PCをシャットダウンしたら、ビジネスは続かない
  - PCを止めている間は損失が拡大しているということをセキュリティ専門家は気が付いていない（ので、ネットワークの分離やVDIをセキュリティだと勘違いしている）
- リスク受容レベルを決めて、その中で改善のサイクルをまわす
  - 自動補正を行うための要件をシステムに組み込んでいく必要がある
  - テストを簡略化できなければ、レジリエントシステムは作れない

CISOハンドブックとダッシュボード



CISO ハンドブック

業務執行として考える情報セキュリティ

Ver. 1.1β

特定非営利活動法人　日本ネットワークセキュリティ協会
社会活動部会　CISO 支援ワーキンググループ

2018 年 6 月 22 日（1.1β）
2018 年 4 月 27 日(1.0β)

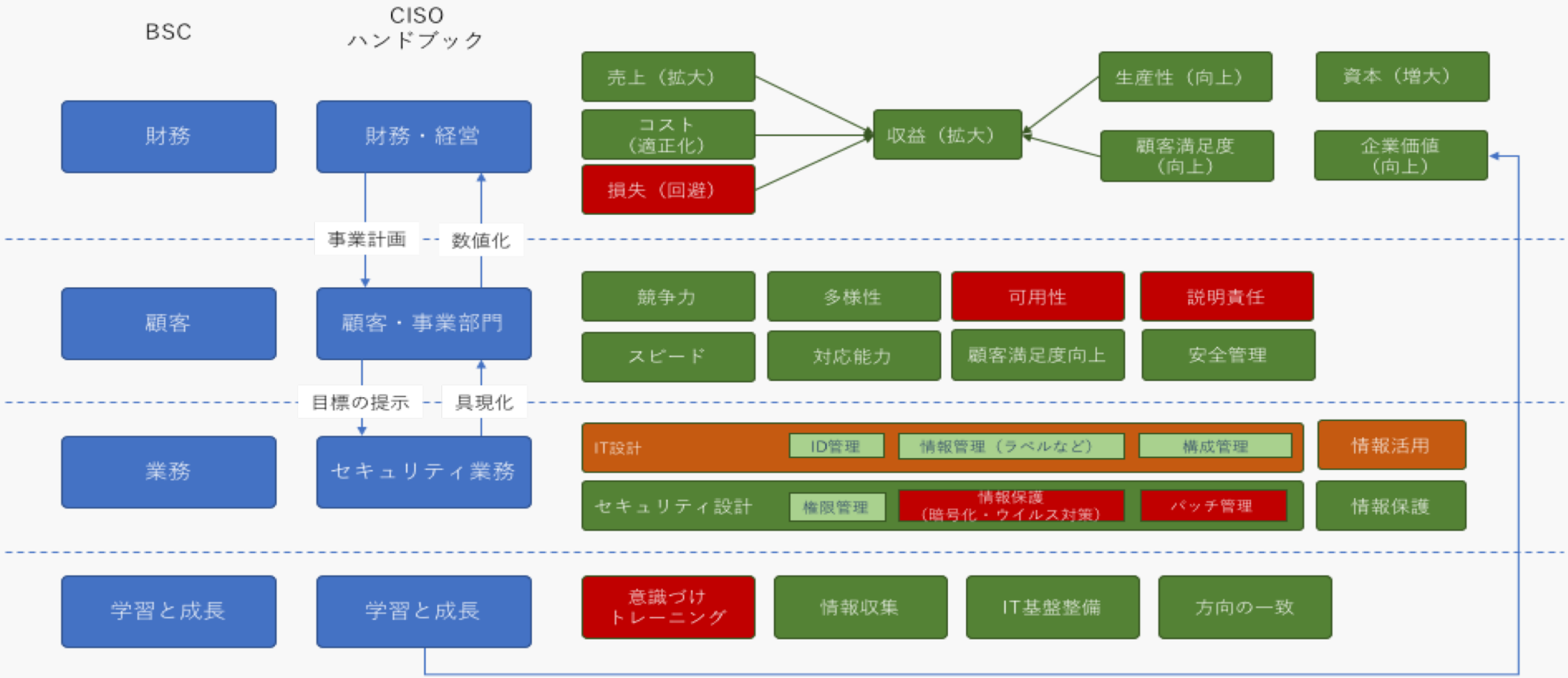
1

日本ネットワークセキュリティ協会（JNSA）が作成したCISOのためのハンドブックとセキュリティ指標のガイド

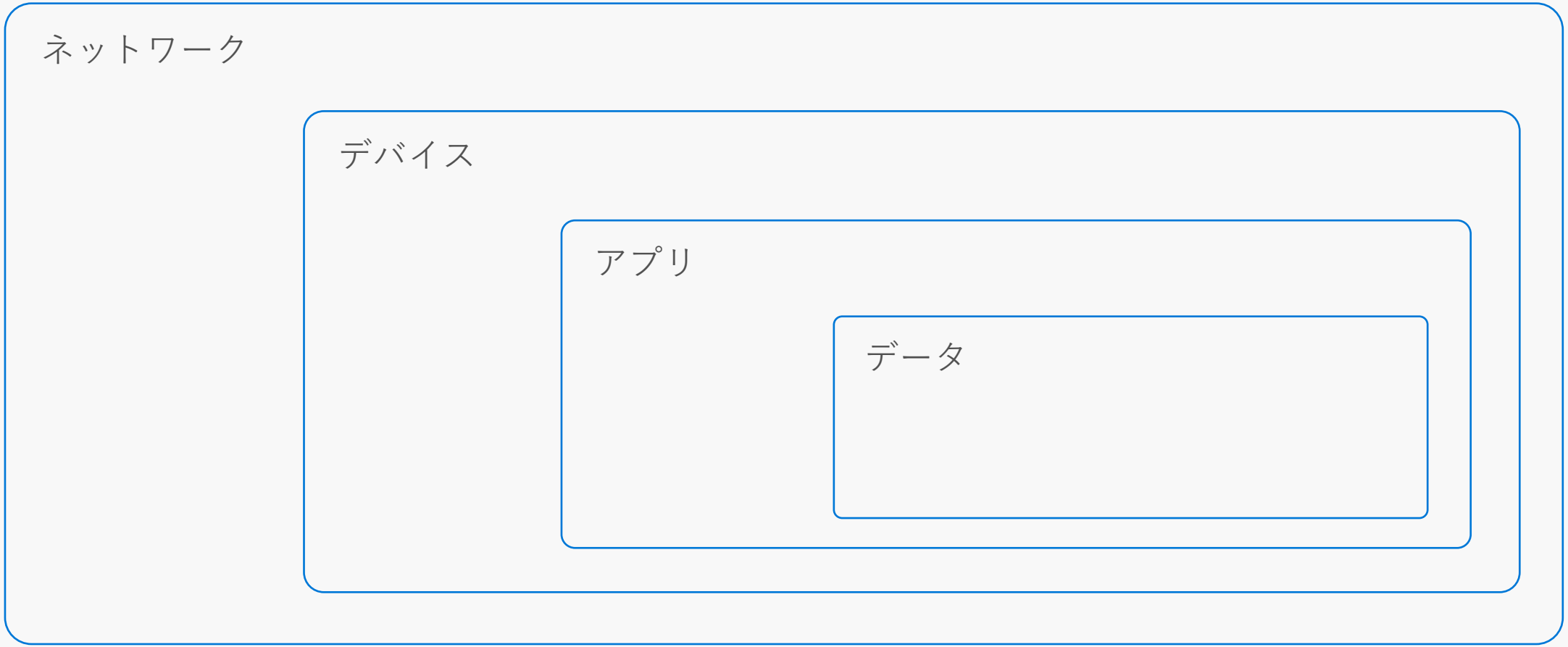
- 経営会議で資料を作る際のひな型として
- 技術担当から CISO になった人がビジネスを理解するための参考として
- セキュリティ経験の少ない CISO がセキュリティ業務を理解するための参考として
- 経営会議で話される業務執行（CISO の役割と責任、業務）の概要を理解する参考として
- ビジネスに関連付けた計測項目と判断基準の例として
- ビジネスに沿ったセキュリティ計画や、事業継続計画の策定の資料として

https://www.jnsa.org/result/2018/act_ciso/

バランストスコアカードによる指標作り



管理の粒度を変更する



管理のレベルでしか制御できない。データレベルで制御するためには・・・

Information Protection

情報保護のための基盤づくり

脅威の定番は「なりすまし」

標的型メール攻撃

差出人　ファイル　URLリンク

ビッグデータ改ざん

IoT機器　連携システム

ウイルス感染

ファイル　プログラム

フィッシング

URLリンク　ホームページ

巧妙になりすまされたら、防御できない
どうすれば、ホンモノであることを確認できるのか

中国で電子決済が普及している理由

WEDGE Infinity
日本を もっと、考える

お知らせ
- Wedge6月号『明治に学ぶ　日本のリノベーション』
- ひととき6月号『苔 緑色の小宇宙』
- 新刊書籍『職場のイライラをすっきりなくす本』

TOP　政治・経済　国際　ビジネス　社会　ライフ　特集　BBC

サイバー空間の権力論　2017年6月6日

電子決済の普及で中国人が「道徳的」に？

透明化する個人情報が孕む諸問題

塚越健司 （拓殖大学非常勤講師）

»著者プロフィール　ツイート　シェア 80　印刷画面

前回はコンピュータと人間の脳を接続することで新たな展望を図る、Facebookをはじめとした様々な試みを取り上げた。そこでは、病気などの対処として期待が持てる一方、SF小説が描いてきた未来のコミュニケーションにおける盲点について考察した。我々は不完全であるが故に向上心を持つ存在なのだろう。

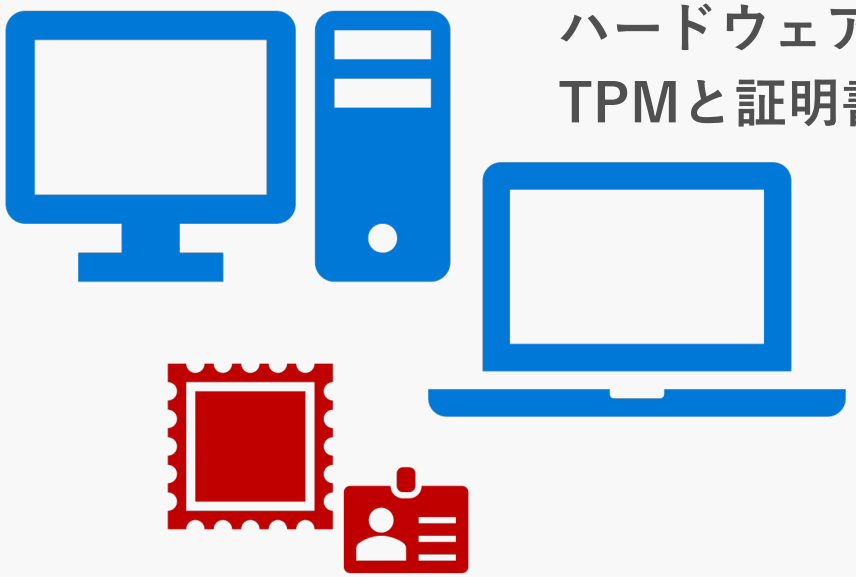
技術は我々の生活に大きな影響を与えるが、今回は中国で生じている興味深い事例について検討したい。それは驚くべき現象であり、疑問を抱く点も多い一方、単純に否定できない複雑な問題を我々に提示している。

- 現金をホンモノだと判断できない
  - 紙幣が本物であるという確証を持てない
- 毎回オーソリをしたい
  - 紙幣を確認する機械を使っているが、それが本物かどうかもわからない
  - オンラインでリアルタイムに確認をしたい
- 実はケニアなどでも
  - 中国よりも先にアフリカなどではデポジットベースのSNS電子決済が普及しており、コーヒーショップなどの少額決済に使われている

資産管理もホンモノかどうかが重要

- ガバナンスの前にインベントリ管理
  - 企業の資産すべてを把握し、構成を管理する
  - そしてサプライチェーンを通じた影響管理
- 効果的な資産管理とは？
  - 入手（作成）した時から、固有のIDをつけて管理したい
  - 資産を廃棄した後でも、廃棄前の状態を把握しておきたい
  - これらを自動的に行うことで、人的コストを削減したい
- 法的監査以外は縮小傾向にある
  - 年に一度の棚卸や、システム監査は縮小傾向
  - 継続的監視によるコスト削減

そのサーバはホンモノですか？



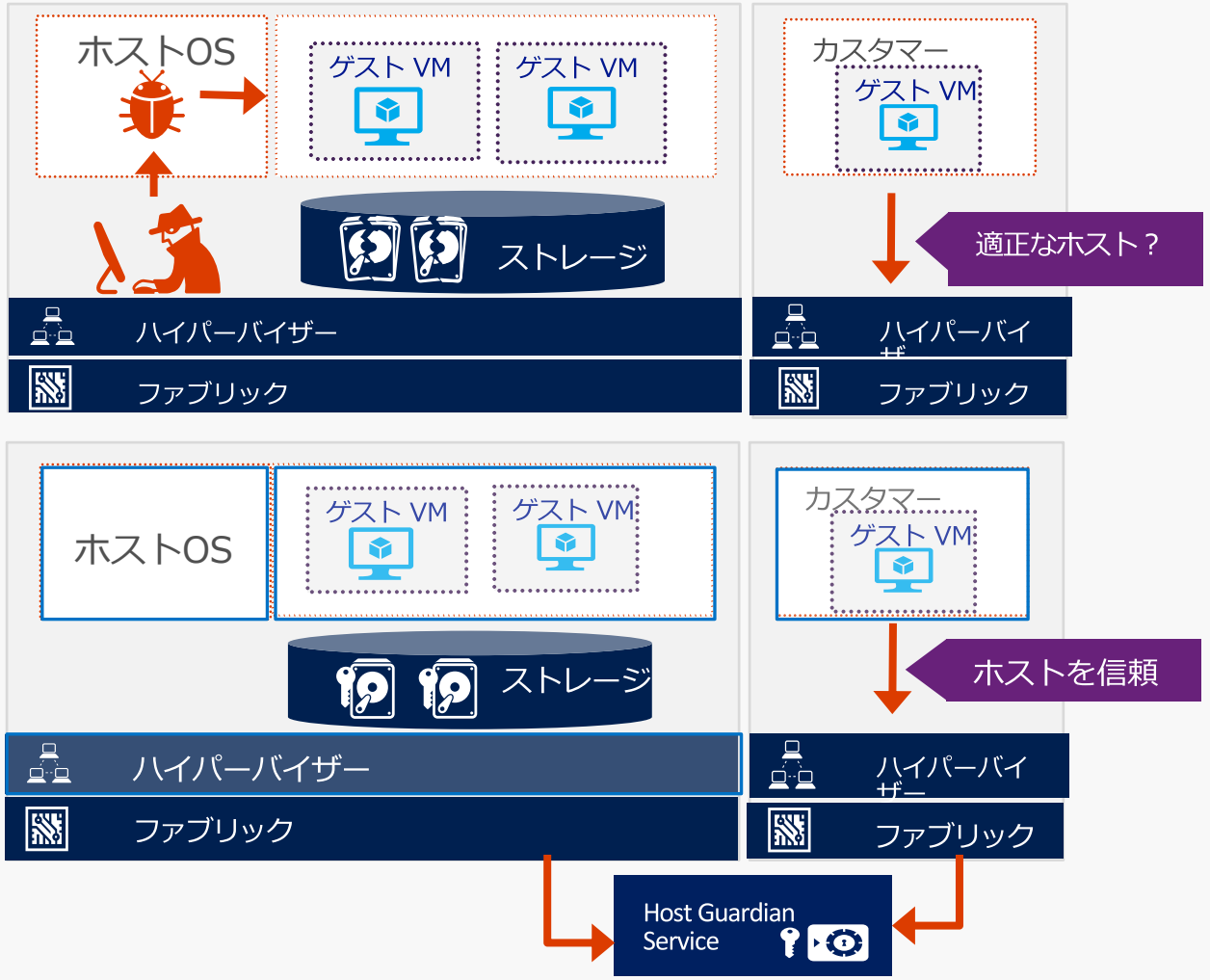
ハードウェアには
TPMと証明書

ソフトウェアには
デジタル署名

その証明書やデジタル署名は信用できますか？
仮想化されたハードウェア（シンクライアントやVM）のTPMは使えない？

仮想マシンの信頼性 – Server 2016の新機能

- Virtual Secure Mode
- ハードウェアのテクノロジーに基づき、ゲストOS をホストOSのアドミニストレーターから分離
- Host Guardian Service
- テナントの Shielded VM を動かすことのできる適正なホストであることを保証する防護されたファブリック
- Shielded VM
- 仮想マシンを暗号化する仮想トラステッド プラットフォーム モジュール (vTPM)



Automated Security

自動化による責任の軽減

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

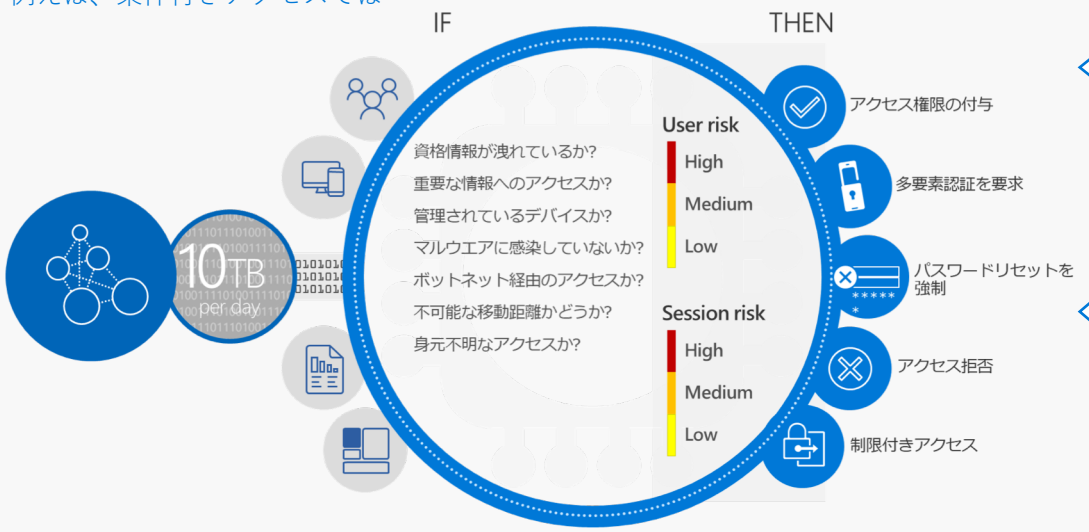
増え続ける資産

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

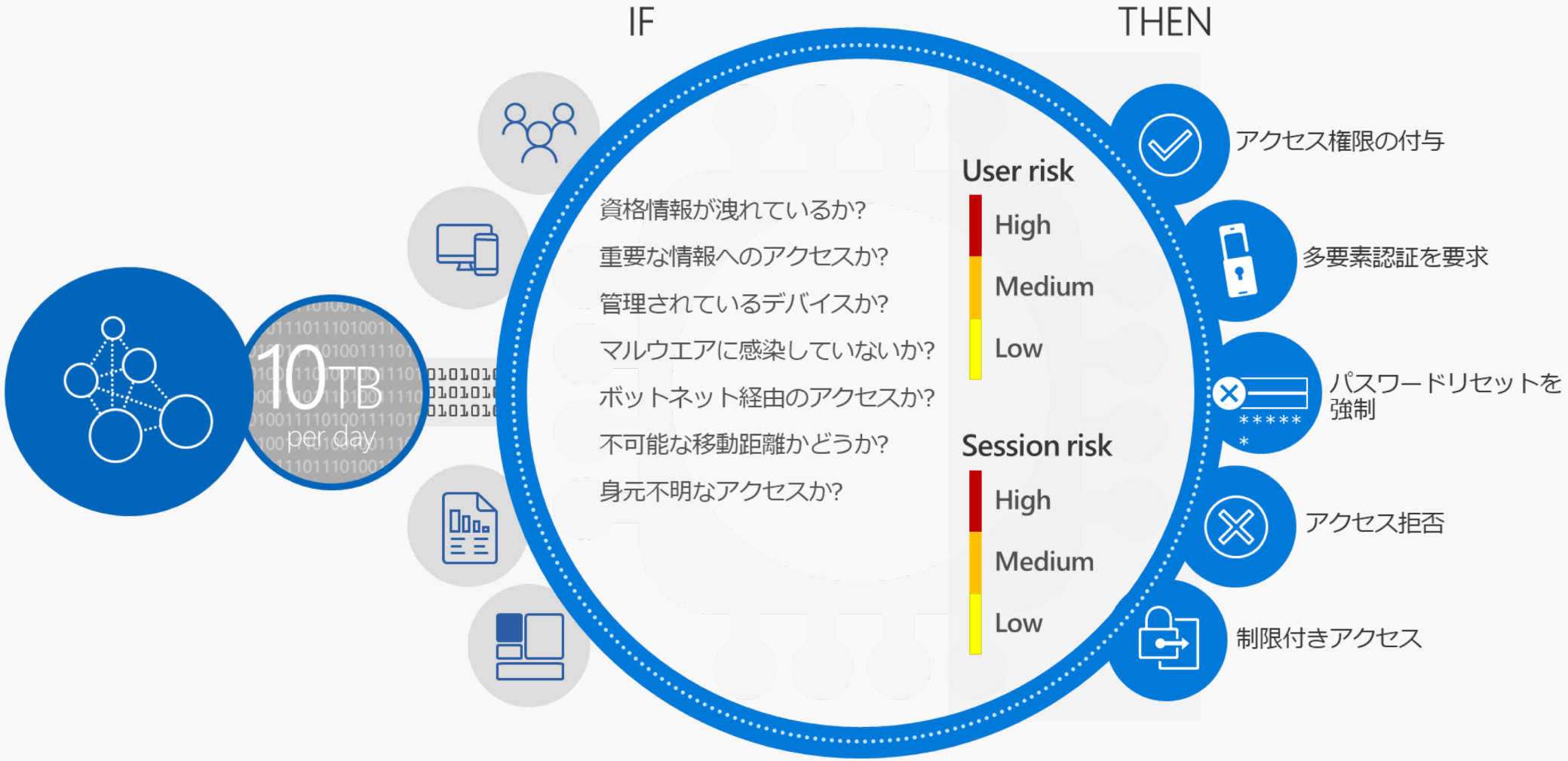
アンチマルウェアだけではなく、様々な攻撃や脅威の検知と自動対策を実現しました。事故が発生した際のセキュリティ専門家とのコミュニケーションを円滑にするためのダッシュボードで少人数のCSIRTづくりも可能です。

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

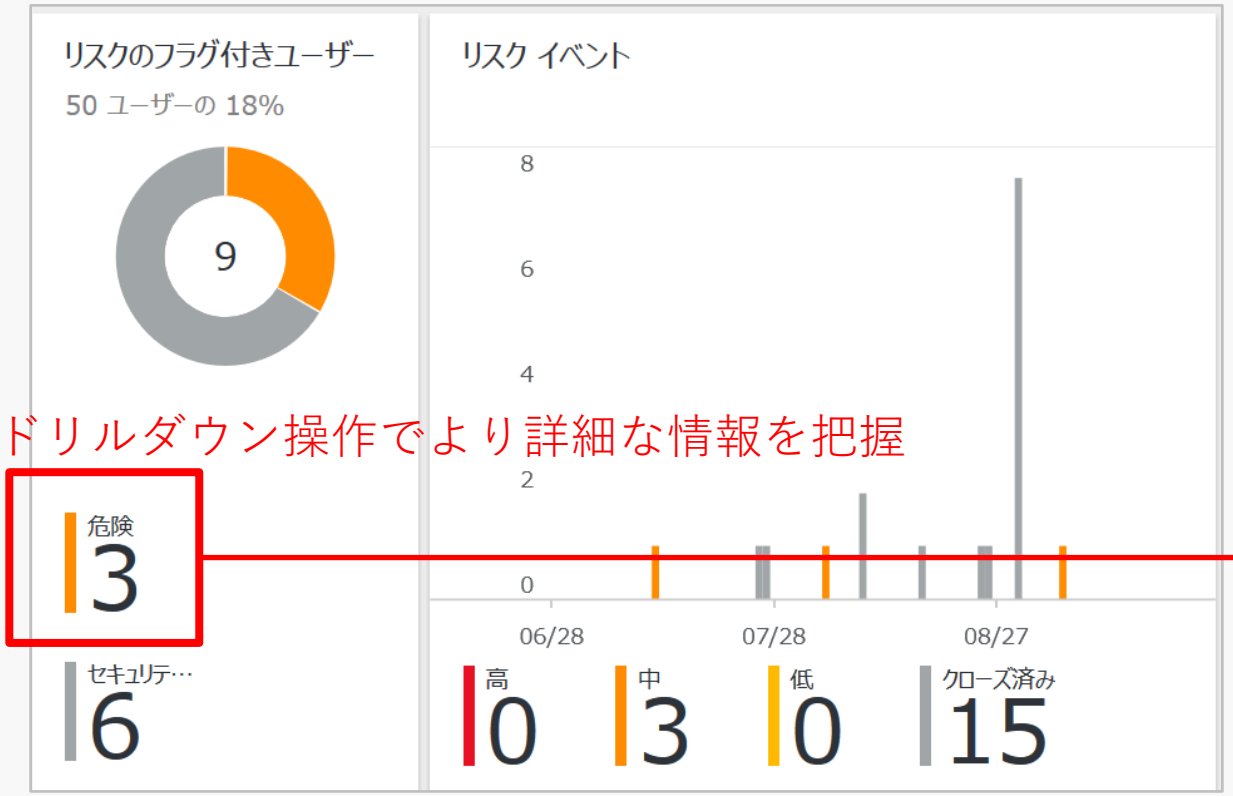
条件付きアクセス



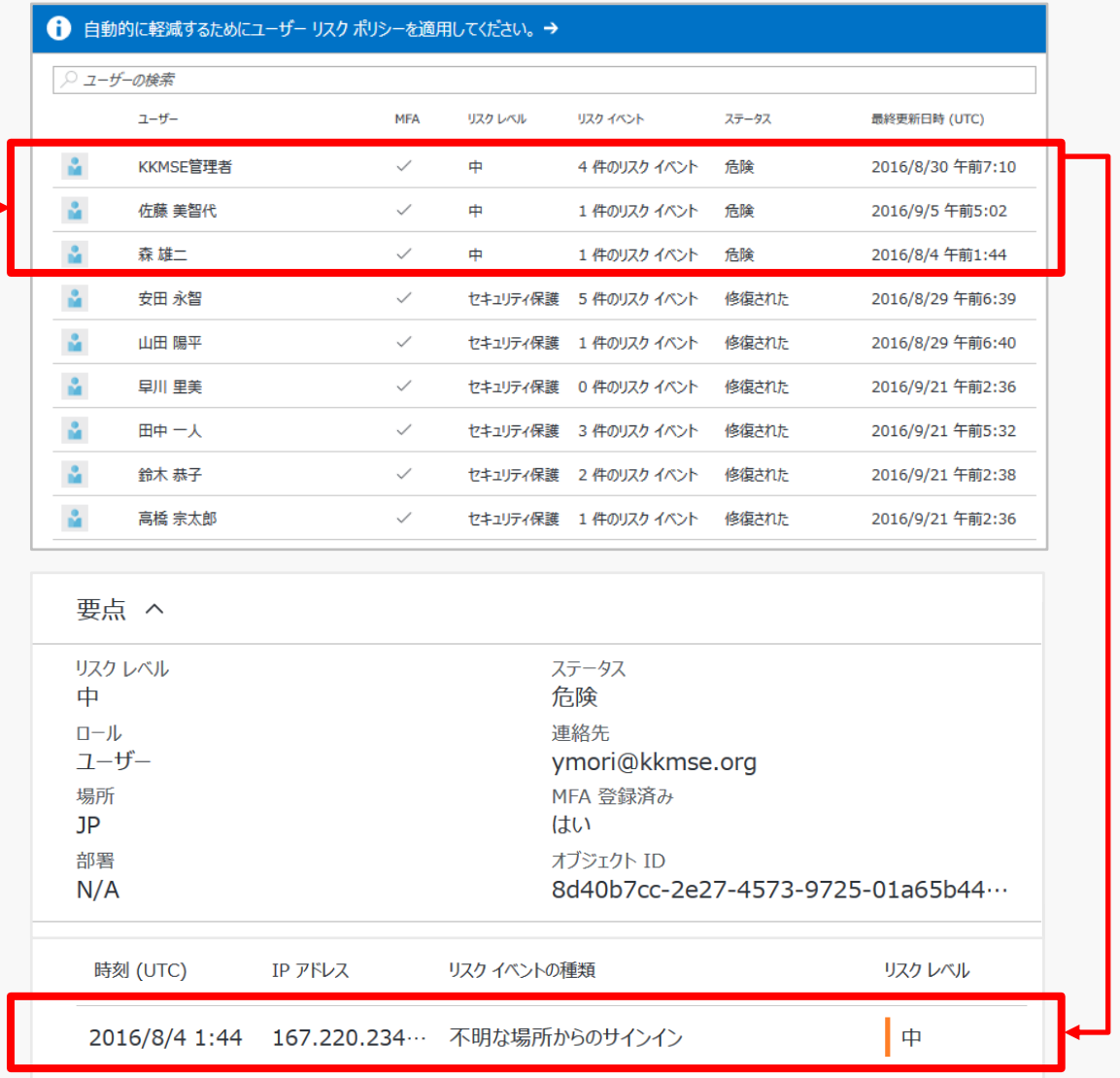
コンプライアンス主義からデータ主義

- コンプライアンス主義 - 人が頑張る
  - 情報セキュリティポリシーを策定
  - 遵守のためのリテラシー教育
  - 遵守していることを1年に1回もしくは数回監査
  - 遵守できていない部門　人に再度教育
- データ主義 - システムで実装する
  - セキュリティの基準（KPI）を設定
  - KPIを判断するためのデータを収集
  - 適切なパフォーマンスが出ていない部分について付随情報を収集して判断
  - KPIの修正もしくはシステムの修正
  - オフラインの資産があると調査に時間がかかる

ログインの自動ブロック

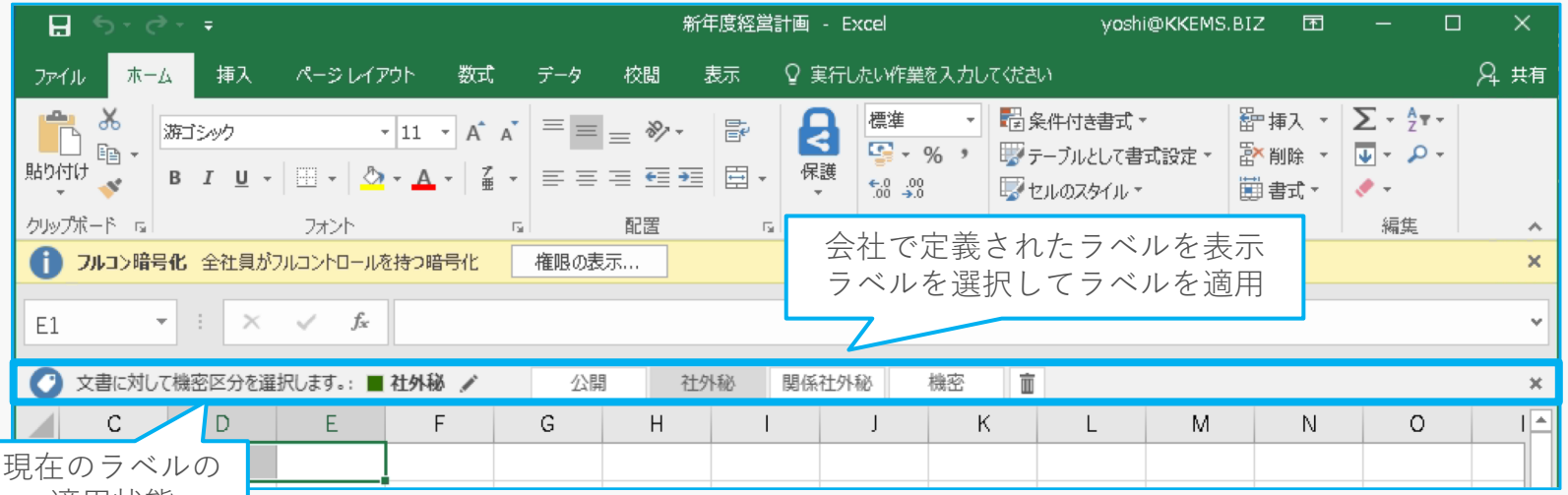


ドリルダウン操作でより詳細な情報を把握

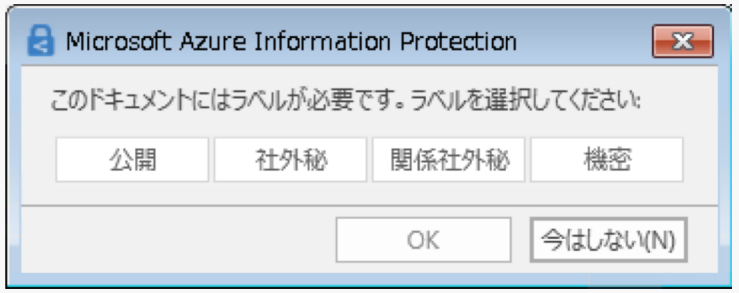


情報の自動分類と保護

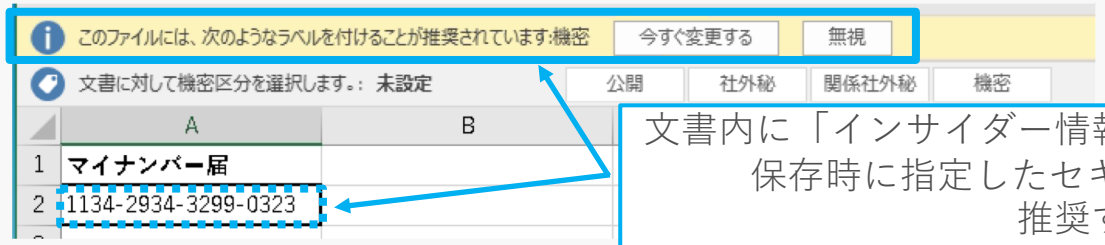
定義された分類ラベルを Office アプリケーションの画面上部のバーに表示
ユーザーが適した分類ラベルを選択



分類ラベルが未選択の場合は、保存時に、
ポップアップで選択を要求可能
(既定の分類を指定しておくことも可能)



ドキュメント内のキーワードに応じて分類ラベルを
推奨したり強制することが可能（管理者側で設定）



文書内に「インサイダー情報」など指定した語句を含む場合に、
保存時に指定したセキュリティ ラベルを強制したり
推奨することが可能
正規表現でマイナンバー 12 桁なども定義可能
(¥d{4}-¥d{4}-¥d{4})

分類ラベルに応じて社員しか開けない暗号化、
ヘッダー/フッター/透かし文字の挿入などの
保護が可能（管理者側で設定）

を禁じます

Total Security with Partners

パートナーと作るトータルセキュリティ

Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- SIEM + Analytics
- Cybersecurity Operations Service (COS)
- Incident Response and Recovery Services
- Azure Security Center
- Windows Defender
- Office 365 Security & Compliance
- Azure
- Cloud App Security
- Advanced Threat Protection (ATP)
- Graph Security API *(Public Preview)*
- Alert & Log Integration

Software as a Service

- Office 365
  - Secure Score
  - Customer Lockbox
- Dynamics 365

Identity & Access

- Azure Active Directory
- Conditional Access – Identity Perimeter Management
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM
- Azure ATP
- Active Directory
- ESAE Admin Forest

Information Protection

- Cloud App Security
- Azure Information Protection (AIP)
  - Discover
  - Classify
  - Protect
  - Monitor
  - *Hold Your Own Key (HYOK)*
  - AIP Scanner
- Classification Labels
- Office 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
- Azure SQL Threat Detection
- SQL Encryption & Data Masking
- Azure SQL Info Protection *(Preview)*
- Endpoint DLP

Clients

- Unmanaged & Mobile Devices
- Intune MDM/MAM
- Managed Clients
- System Center Configuration Manager
- Windows Defender ATP
  - Secure Score
  - Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet

- NGFW
- Edge DLP
- SSL Proxy
- IPS

Security Appliances

Express Route

Intranet Servers

- Windows Server 2016 Security
  - Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...
- Shielded VMs
- Azure Stack
- VMs

Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

Windows 10 Enterprise Security

- Network protection
- Credential protection
- Exploit protection
- Reputation analysis
- Full Disk Encryption
- Attack surface reduction
- App control
- Isolation
- Antivirus
- Behavior monitoring
- S Mode

IoT and Operational Technology

- Windows 10 IoT
- Azure IoT Security
- Azure Sphere
- IoT Security Maturity Model
- IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

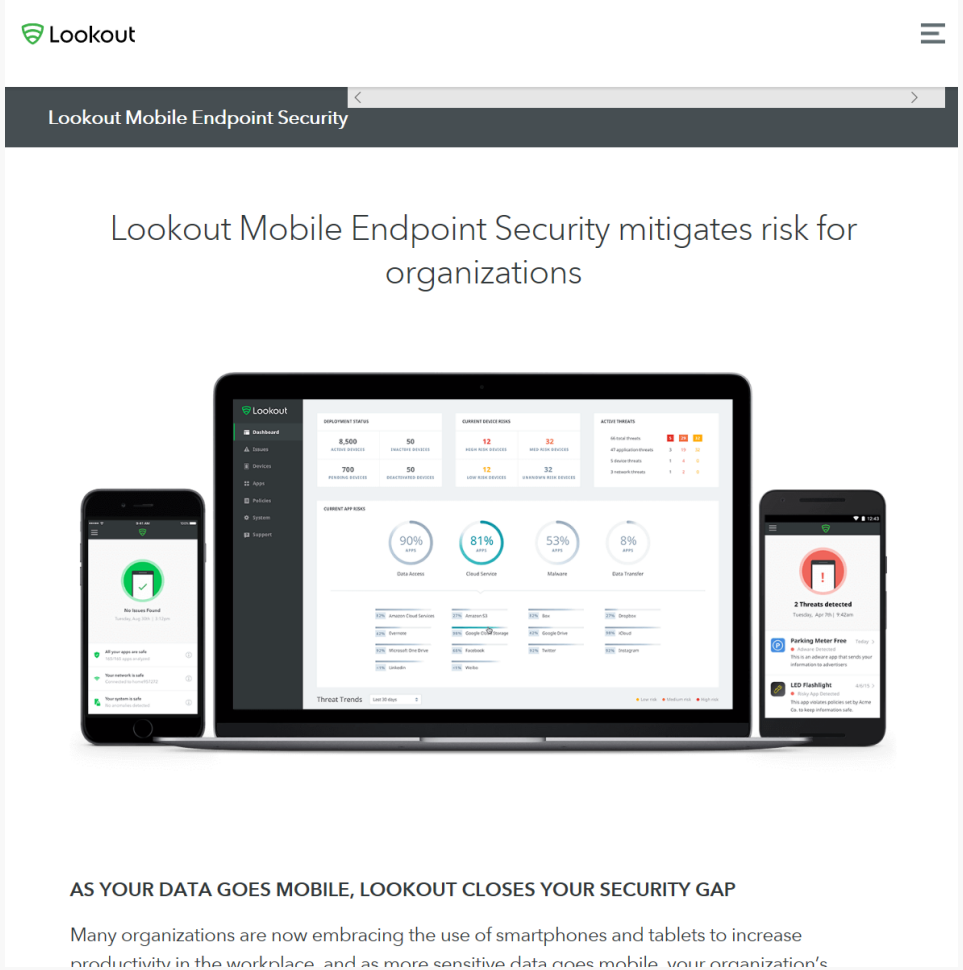
Security Development Lifecycle (SDL)

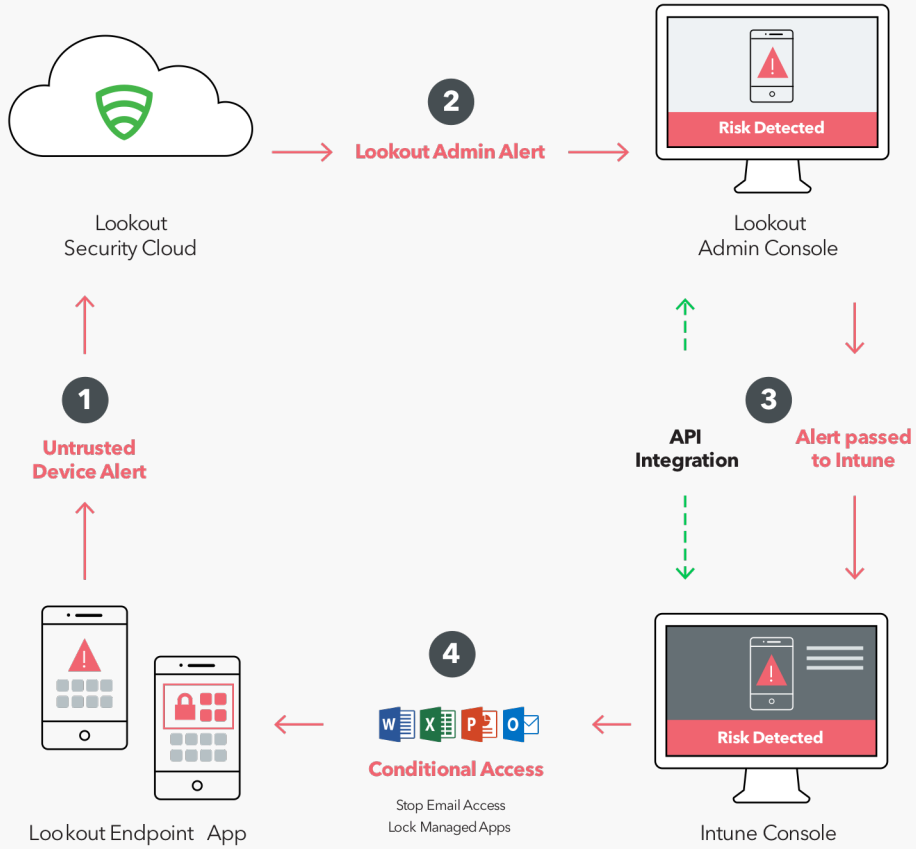
Trust Center | Intelligent Security Graph

Microsoft

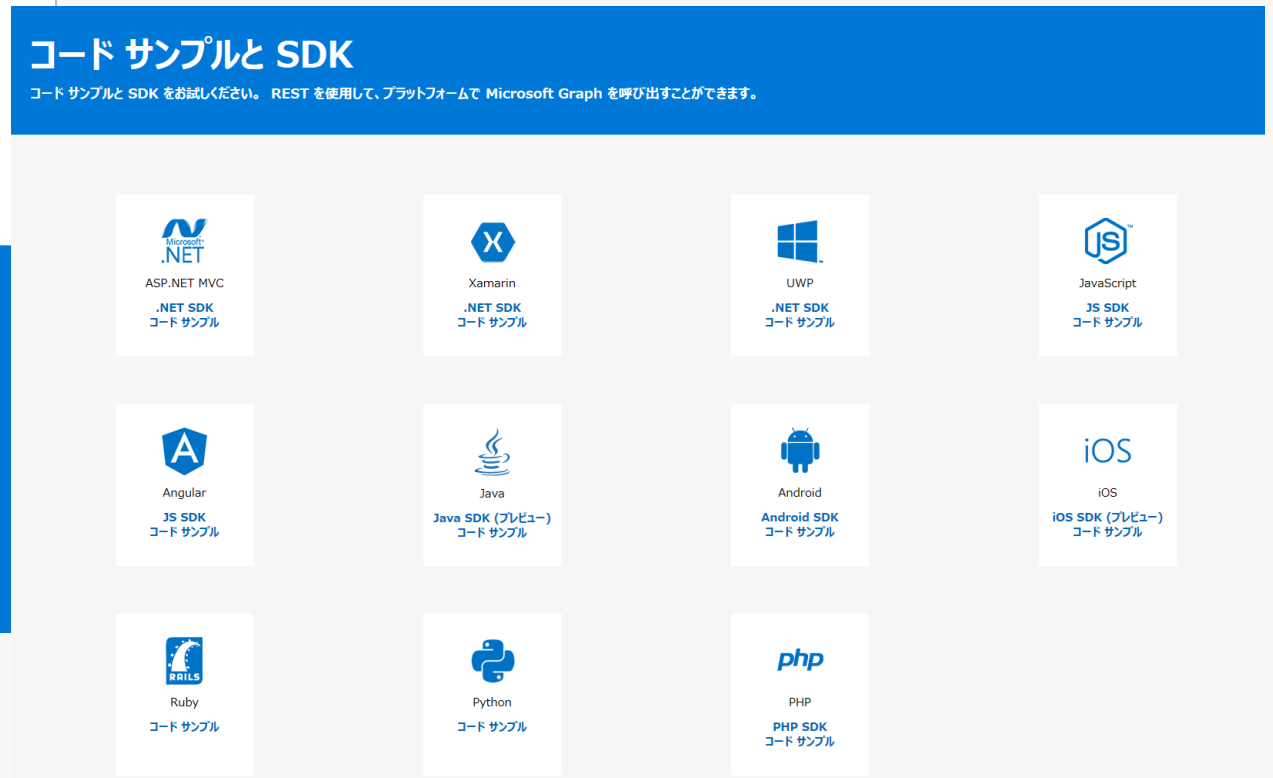
APIを使ったパートナー連携

Lookout社によるiOS/Androidのエンドポイントセキュリティの連携





実は自社アプリもGraph APIで作れます



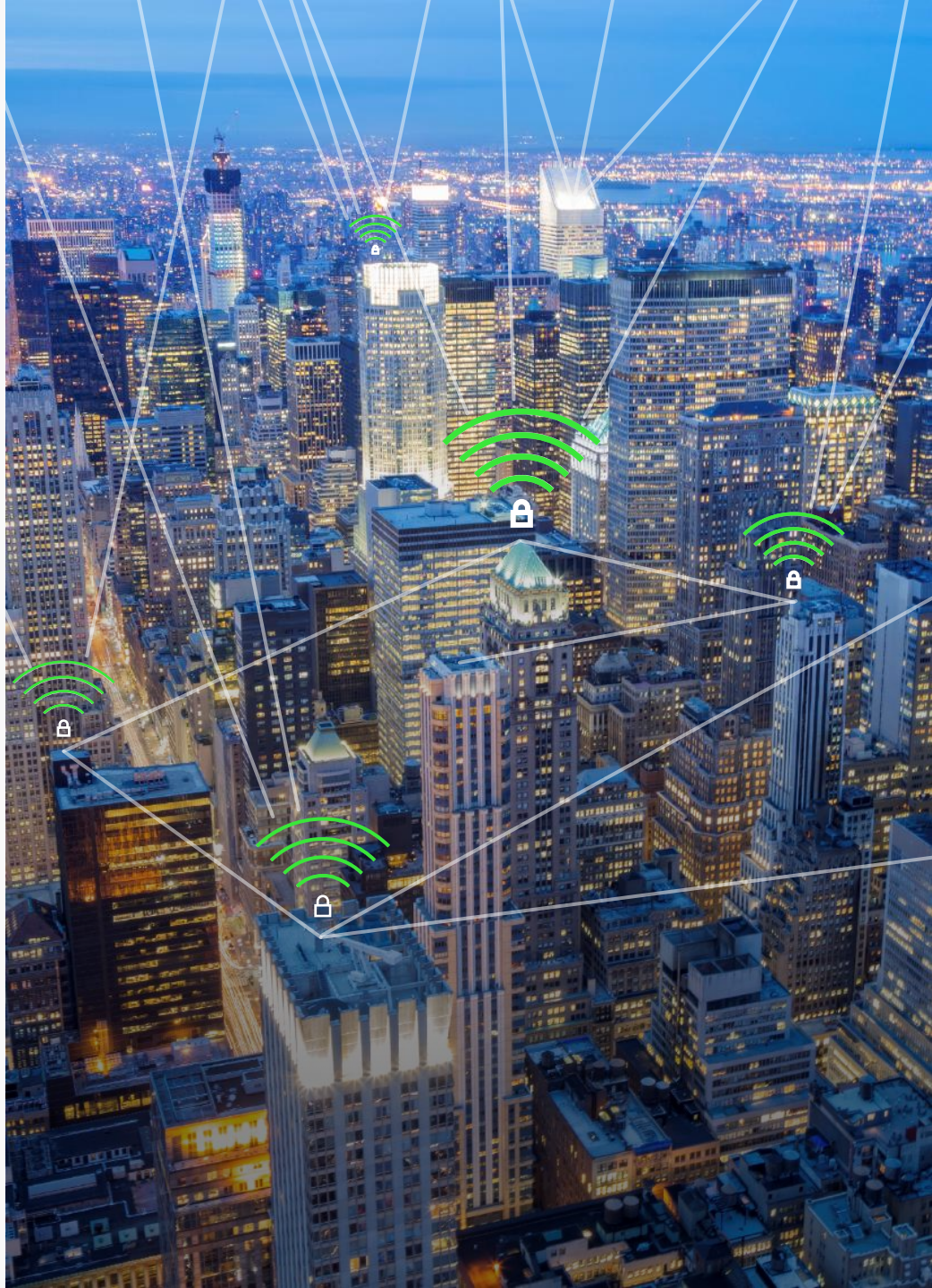
https://developer.microsoft.com/ja-jp/graph/code-samples-and-sdks

デジタルトランスフォーメーション

- デジタル化とは
  - 0か1かを明確にする
  - 数字になるので計算できる
  - 基準やルールさえ決めれば自動化できる
- すべてのことを評価できる
  - ルールを守る（コンプライアンス）から、ルールの調整（ガバナンス）へと変化している
  - ガバナンスは統制ではなく、モニタリングと経営判断である
- 性悪説、性善説はない
  - 仕事をすべてIT基盤に乗せる
  - 社内不正の監視ではなく、社員の評価のためのIT基盤を作ることから始める

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