Microsoft

ポスト境界領域防御：最新 IT 環境のリスクマネジメント

マイクロソフトが取り組む

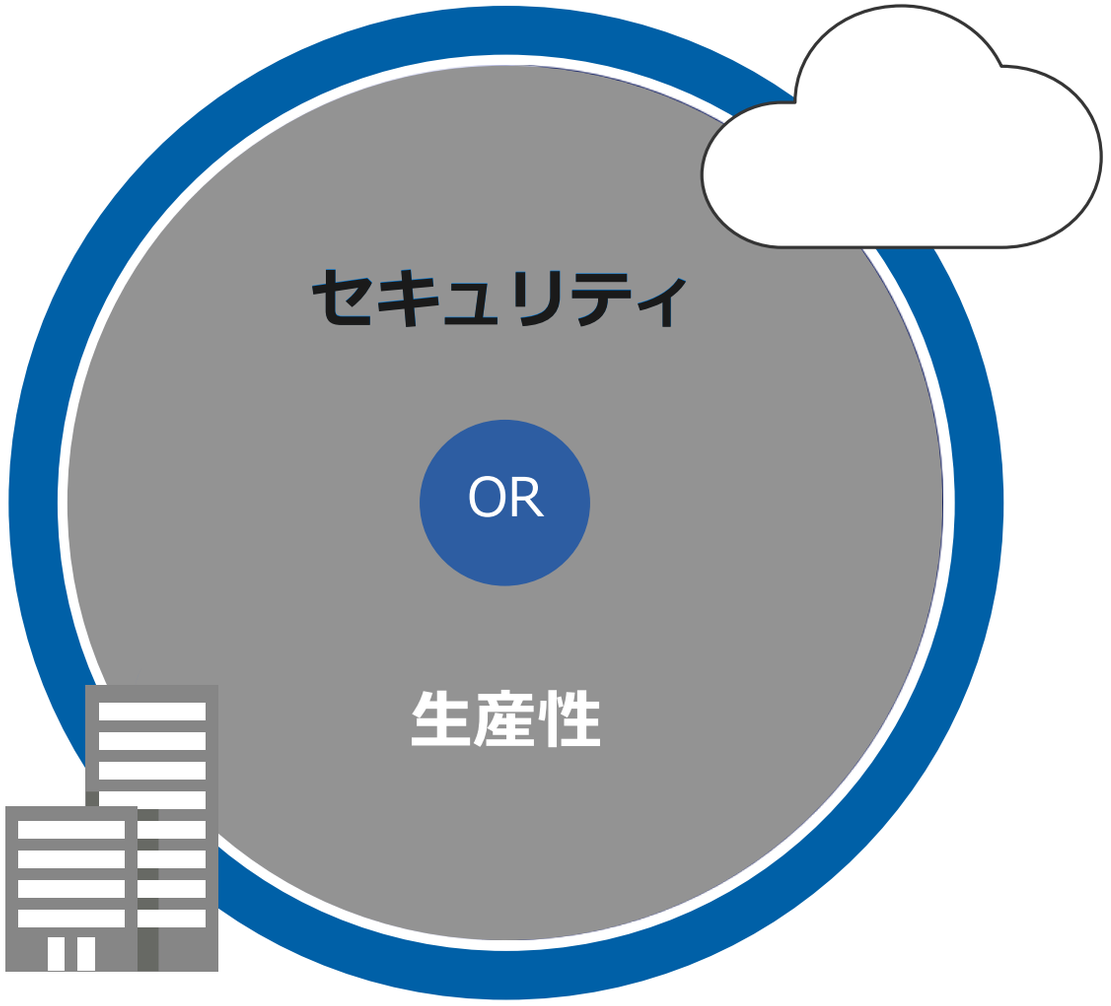
Identity-based Security

安納 順一 Junichi Anno

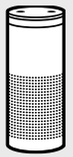
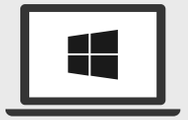
Microsoft Japan
Commercial Software Engineering
Technical Evangelism Manager

マイクロソフトが取り組んでいる長年の課題

生産性と**セキュリティ**を
どう両立させるのか？

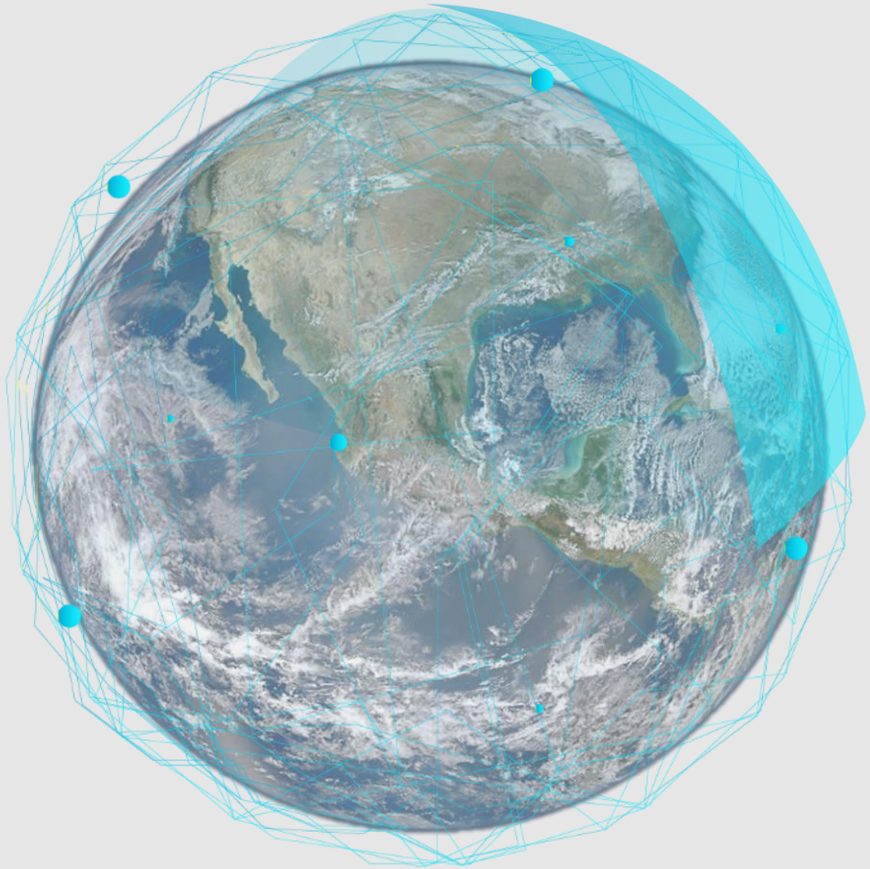





モバイル/個人デバイス
クラウドアプリケーション

On-premises /
Private cloud



直面している脅威

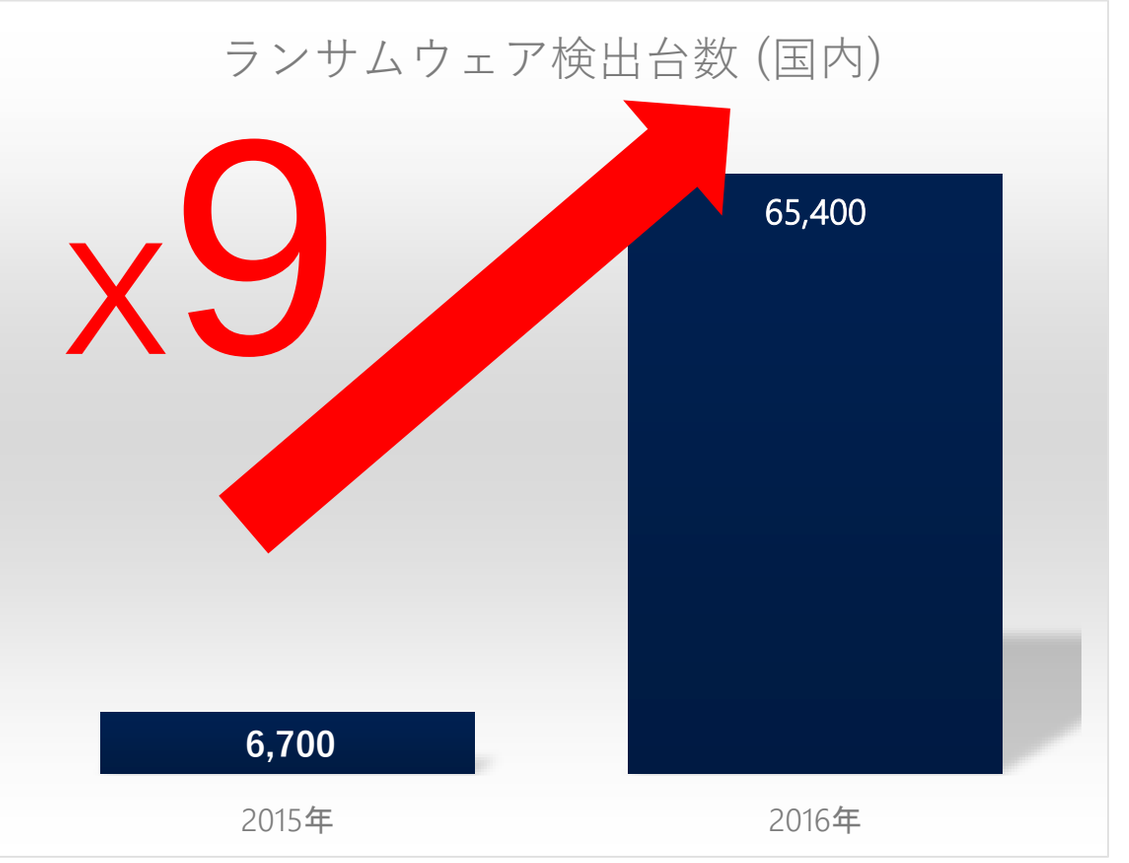
年間のユーザーアカウント攻撃が **300%** 増加

96% のマルウェアがポリモーフィック

1回のデータ漏洩で **$15,000,000** のインパクト

Ransomware 被害状況

Ransomware: last 22 months

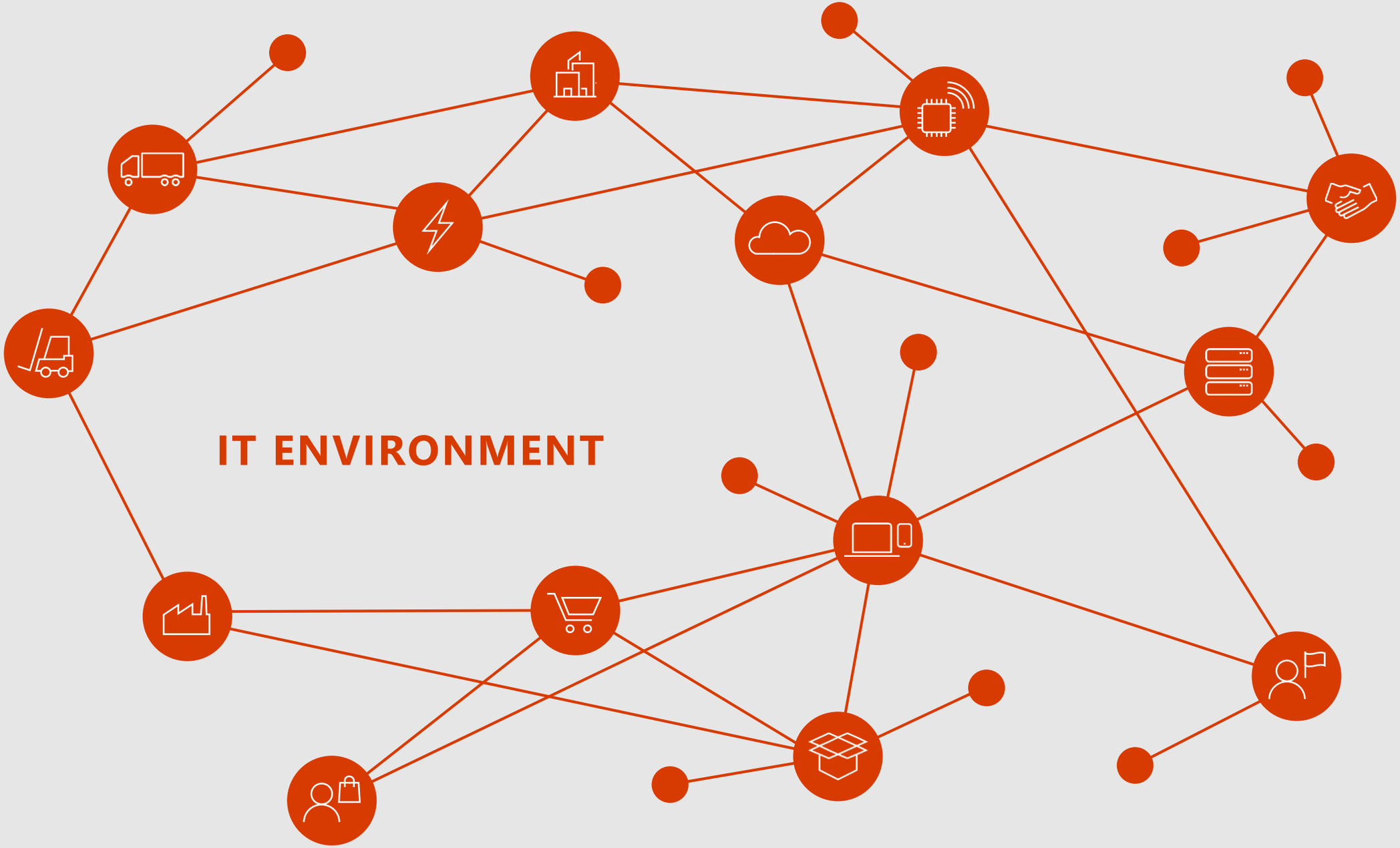


出典：[トレンドマイクロ 2016年 年間セキュリティラウンドアップ]

脆弱性はどこにあるのか?

アイデンティティとエンドポイント


IT ENVIRONMENT


IT ENVIRONMENT

マイクロソフトのアプローチ

- **ユーザー Id を中心としたセキュリティ設計**
  - “認証/認可の分離”とシングルサインオン
  - 認証/認可の4層構造（User Id, Device, Application, Data)
- **AI を使用した迅速な脅威検出とリスク算出、対策の自動化**
  - OS, その他のプロダクトにアイデンティティ連携を組み込み
  - IoT を含む Windows OS 自身のセキュリティ強化
- **各種プラットフォーム共通の製品、アプリケーション開発環境**
  - Windows, MAC OS, Linux, iOS, Android
- **チップセットメーカーとの連携によるハードウェアの開発**
  - Surface **シリーズ、**Project Sopris

先端技術の
取り込み

Windows の
DevOps 的
開発サイクル

Microsoft acquires .....

https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Microsoft

163	May 1, 2014	GreenButton	Cloud computing	New Zealand	—	[185]
164	May 1, 2014	Capptain	(Mobile) application development	France	—	[186]
165	July 2, 2014	SyntaxTree	Developer tools	France	—	[187]
166	July 11, 2014	InMage	Disaster recovery solutions	United States	—	[188]
167	August 1, 2014	Inception Mobile Inc.	Software	Canada	—	[189]
168	November 6, 2014	Mojang	Video games	Sweden	2,500,000,000	[190]
169	November 13, 2014	Aorato	Enterprise Security & machine learning	Israel	—	[191]
170	December 2, 2014	Acompli	Mobile Email Apps	United States	—	[192]
171	December 11, 2014	HockeyApp	Mobile Beta Distribution Analytics	Germany	—	[193]
172	January 20, 2015	Equivio	Text Analytics Service	Israel	—	[194]
173	January 23, 2015	Revolution Analytics	Statistical computing and predictive analytics	United States	—	[195]
174	February 4, 2015	Sunrise Atelier, Inc.	Sunrise Calendar applications	United States	100,000,000	[196]
175	February 12, 2015	N-trig	Styli and pen input hardware and software	Israel	200,000,000	[197]
176	March 26, 2015	LiveLoop	PowerPoint collaboration	United States	—	[198]
177	April 14, 2015	Datazen Software, Inc.	Mobile business intelligence & Data visualization	Canada	—	[199]
178	June 2, 2015	6Wunderkinder GmbH	Wunderlist to-do list applications	Germany	—	[200]
179	June 10, 2015	BlueStripe Software	Application management	United States	—	[201]
180	July 16, 2015	FieldOne Systems LLC	Enterprise Field Service	United States	—	[202]

Microsoft Advanced Threat Analytics

Outlook Mobile

Microsoft acquires .....

https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Microsoft

185	September 28, 2015	Adxstudio Inc.	Web portal and application lifecycle management solutions	Canada	—	[208]
186	October 2, 2015	Telekinesys Research Ltd.	Game technology	eland	—	[209]
187	November 5, 2015	Mobile Data Labs, Inc.	MileIQ, a mileage tracki	United States	—	[210]
188	November 9, 2015	Secure Islands Technologies Ltd.	Data protection	Israel	—	[211]
189	December 18, 2015	Metanautix	Big Data Analytics	United States	—	[212]
190	December 21, 2015	Talko, Inc.	Mobile communications	United States	—	[213]
191	January 19, 2016	Teacher Gaming LLC	Education software	Finland	—	[214]
192	February 3, 2016	TouchType, Ltd.	SwiftKey, a keyboard productivit		250,000,000	[215][216][217]
193	February 9, 2016	Groove	Music Discovery		—	[218]
194	February 24, 2016	Xamarin	Mobile application development	United States	—	[219][220][221][222]
195	May 3, 2016	Solair	Internet of Things platform	Italy	—	[223]
196	August 8, 2016	Beam (now known as Mixer)	Video game streaming	United States	—	[224][225]
197	August 20, 2016	Genee	AI-powered scheduling assistant service	United States	—	
198	December 8, 2016	LinkedIn	Professional Networking Service	United States	26,200,000,000	[226]
199	January 13, 2017	Maluuba	Artificial Intelligence	Canada	—	[227]
200	January 17, 2017	Simplygon	3D Gaming	Sweden	—	[228]
201	April 10, 2017	Deis	Container Ma			29][230]
202	April 18, 2017	Intentional Software	Collaborative Productivity Pl	United States	—	[231]
203	June 8, 2017	Hexadite	Cybersecurity	Israel	100,000,000	[232]
204	June 28, 2017	Cloudyn	Cloud Business Management	Israel	50,000,000	[233]
205	August 15, 2017	Cycle Computing	Cloud HPC	United States		[234]
206	October 3, 2017	AltspaceVR	Virtual reality	United States		[235]
207	November 7, 2017	SWNG	Cinemagraphic photo app	United States		[236][237]

Information Protection

Xamarin

Windows Defender Advanced Threat Protection

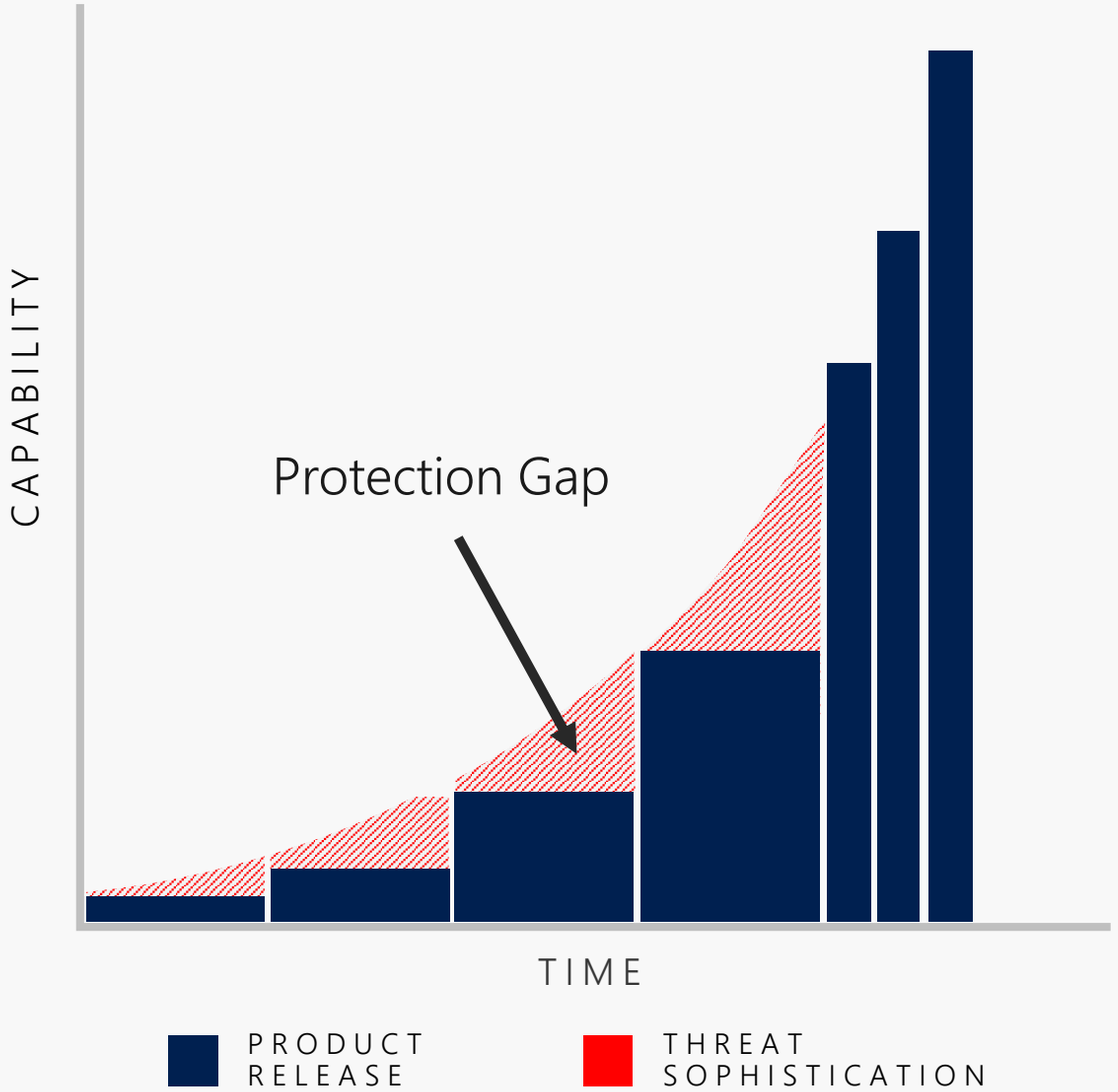
Windows as a Service

従来の Windows OS :

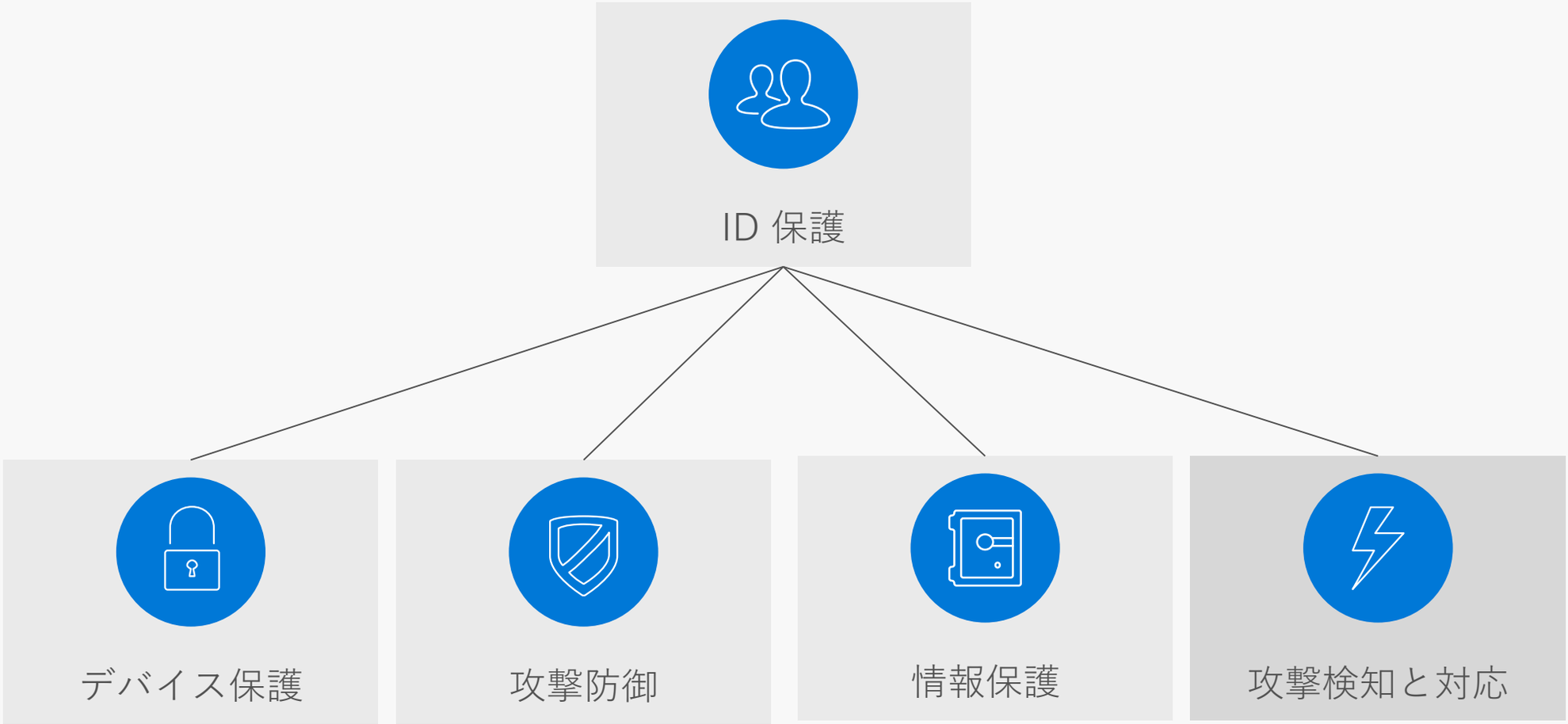
OS の進化のスピードがサイバー攻撃の
進化のスピードに追い付かない

Windows 10 :

WaaS により、迅速なセキュリティ対策が
実装可能に



保護の種類



Windows 10 のセキュリティ機能

デバイス保護
- Virtualization Based Security
- UEFI Secure Boot
- Windows Trusted Boot
- Windows Update
- Trusted Platform Module

攻撃防御
- Application Guard
- Device Guard
- Exploit Guard
- Windows Defender
- Windows Firewall
- SmartScreen

ID 保護
- Remote Credential Guard
- Credential Guard
- Windows Hello Companion Devices
- Windows Hello

情報保護
- Device Encryption
- Windows Information Protection
- BitLocker Admin and Monitoring
- BitLocker
- BitLocker to Go

攻撃検知と対応
- Security Management
- Conditional Access
- Windows Defender Advanced Threat Protection

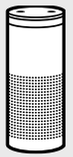
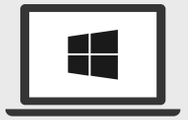
PRE-BREACH → POST-BREACH

アイデンティティの保護

脅威モデルと STRIDE

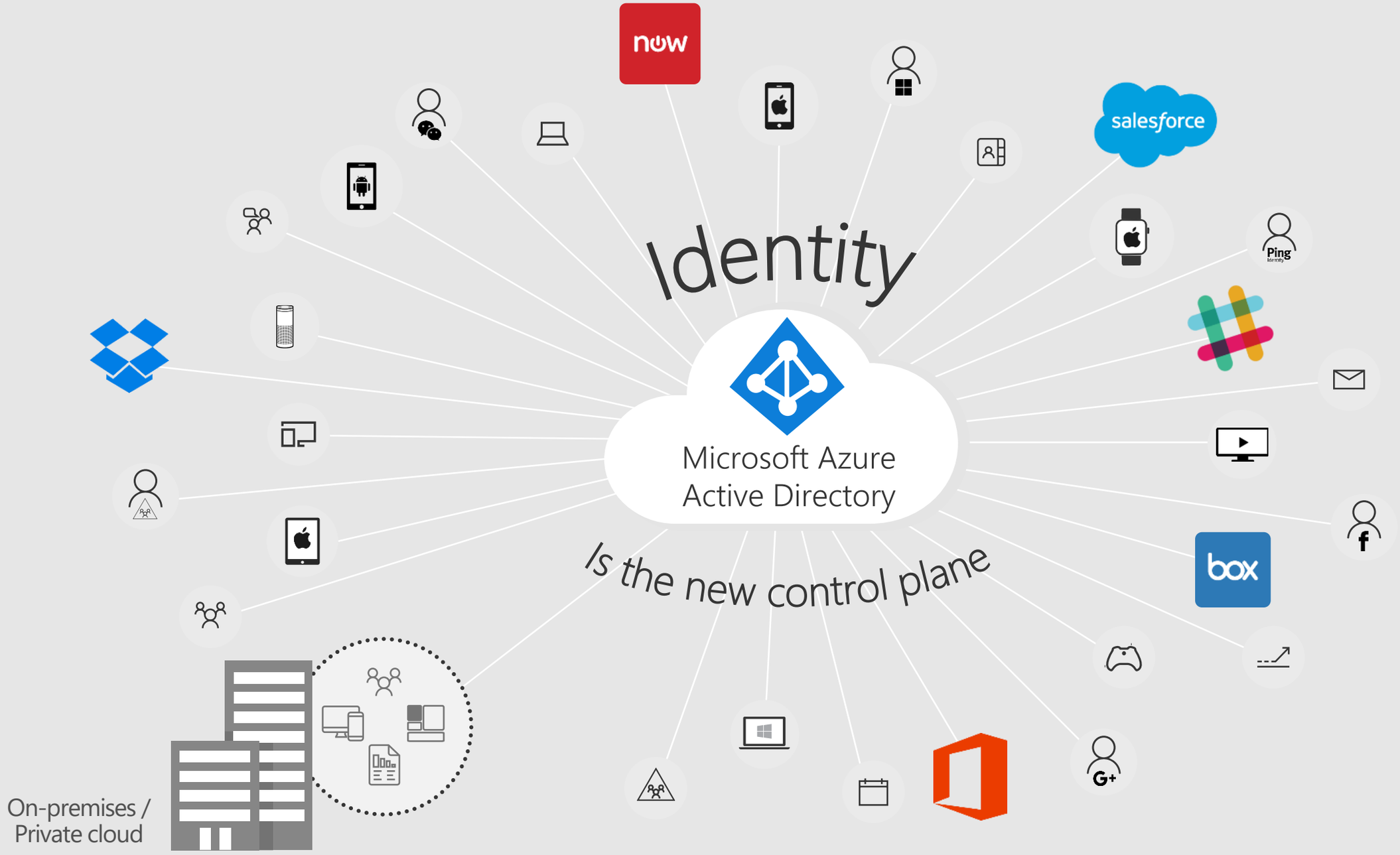
- なりすまし (Spoofing identity) ➡ 認証(Authentication)
- 改ざん (Tampering with data) ➡ 完全性(Integrity)
- 否認（Repudiation） ➡ 非否認(Non-Repudiation)
- 情報漏えい (Information disclosure) ➡ 秘匿性(Confidentially)
- サービス拒否 (Denial of service) ➡ 可用性(Availability)
- 特権の昇格 (Elevation of privilege) ➡ 認可(Authorization)



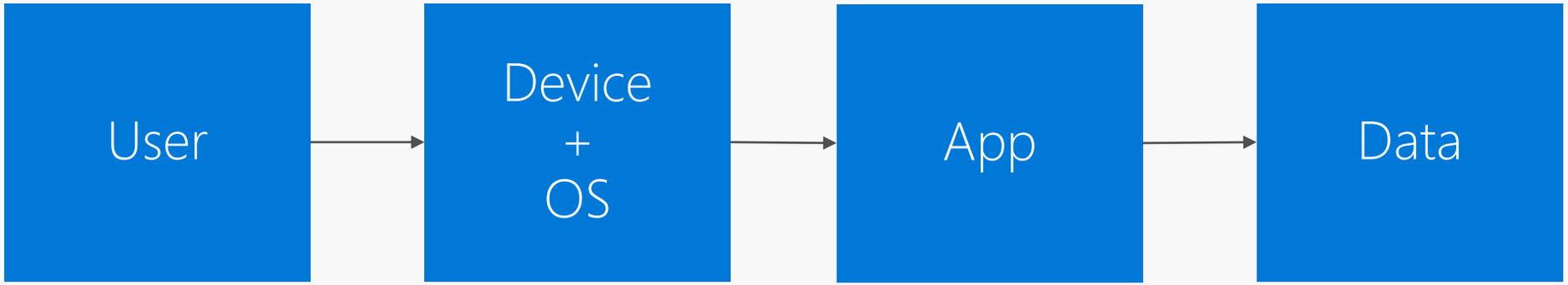



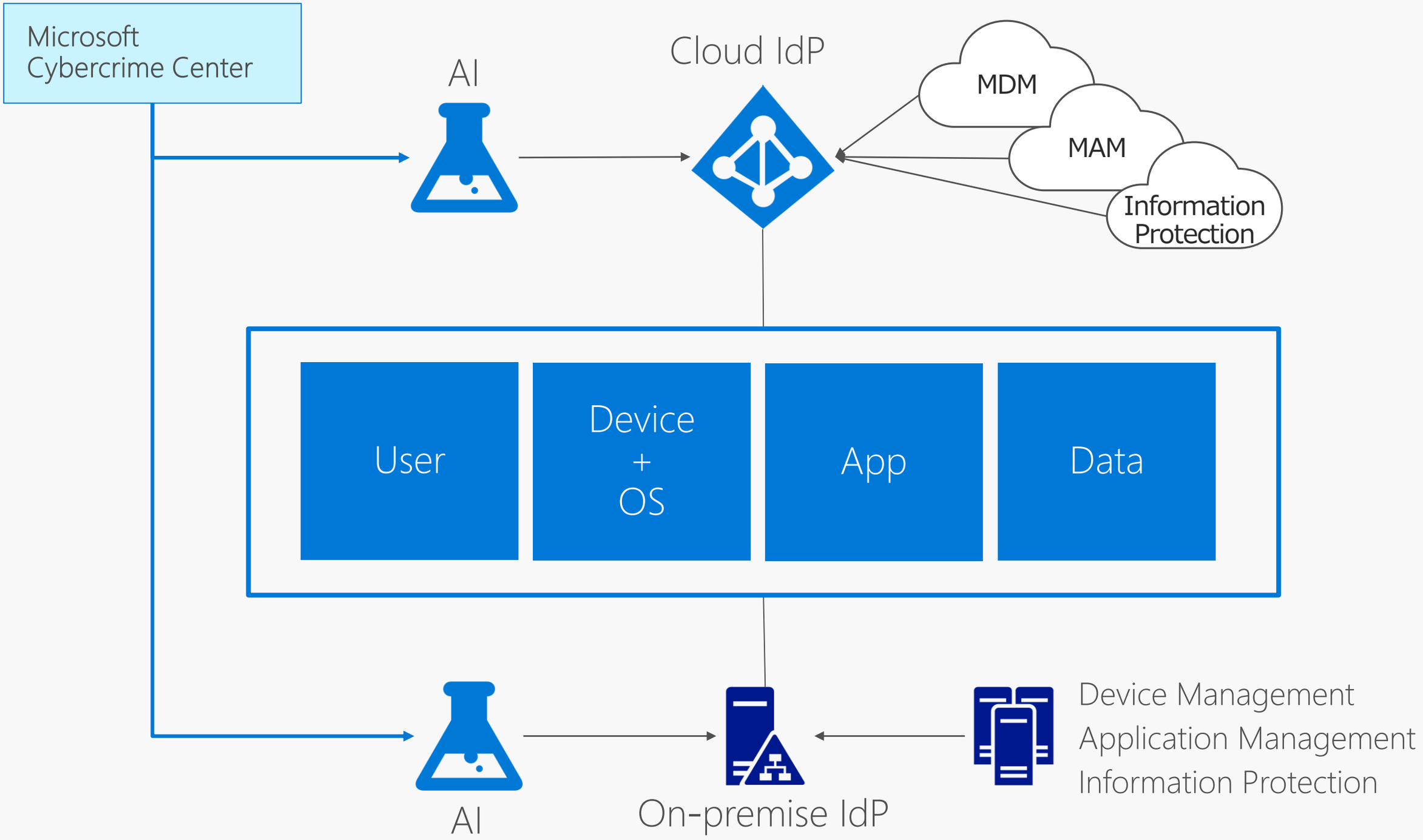

モバイル/個人デバイス
クラウドアプリケーション

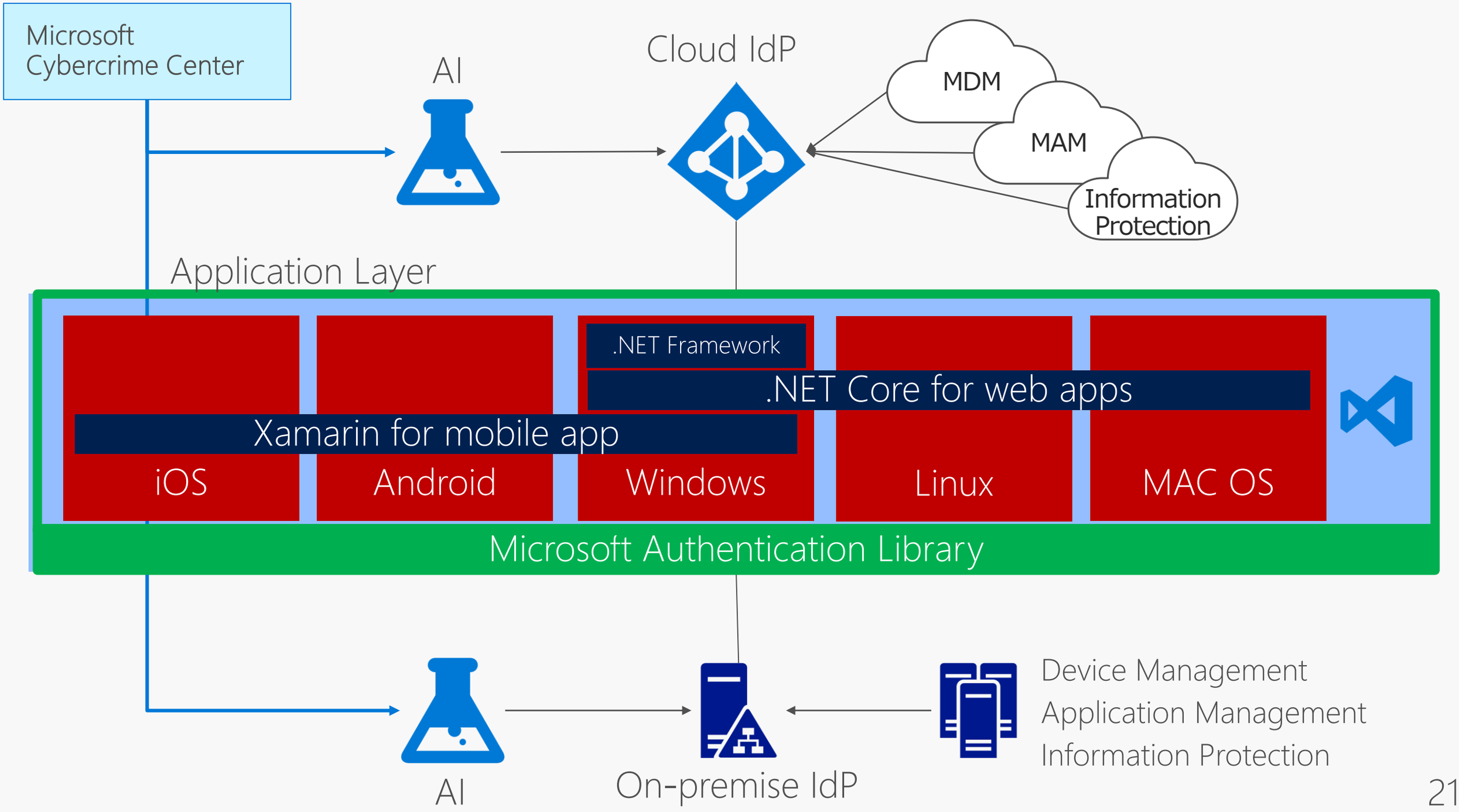
On-premises /
Private cloud


Identity
Microsoft Azure
Active Directory
Is the new control plane
On-premises /
Private cloud

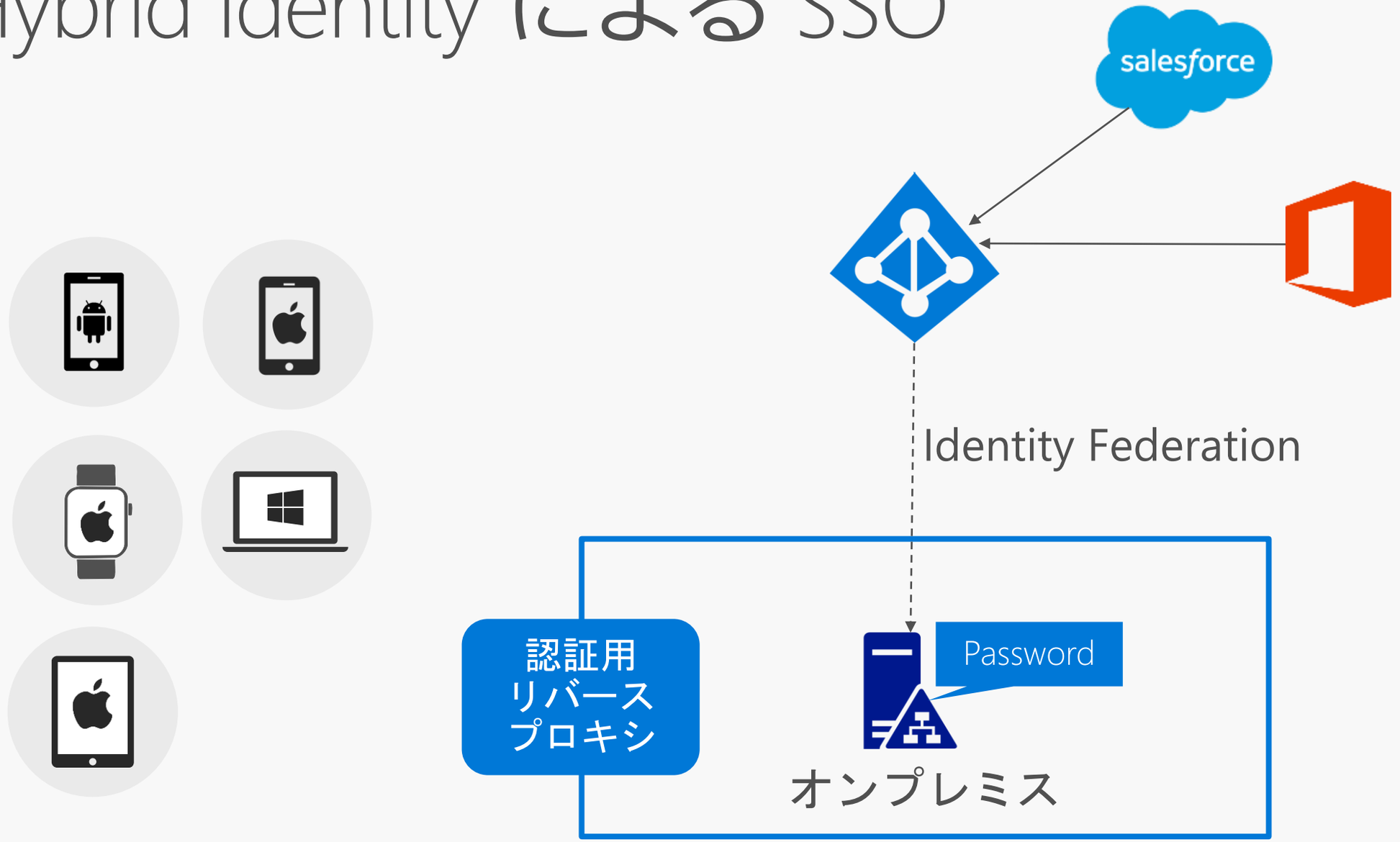
防御対象となる4レイヤ




Microsoft
Cybercrime Center
AI
Cloud IdP
MDM
MAM
Information
Protection
User
Device
+
OS
App
Data
AI
On-premise IdP
Device Management
Application Management
Information Protection


Microsoft
Cybercrime Center
AI
Cloud IdP
MDM
MAM
Information
Protection
Application Layer
.NET Framework
.NET Core for web apps
Xamarin for mobile app
iOS
Android
Windows
Linux
MAC OS
Microsoft Authentication Library
AI
On-premise IdP
Device Management
Application Management
Information Protection

Hybrid Identity による SSO



認証の課題

- パスワード漏洩
- 認証の精度
- 利便性と生産性

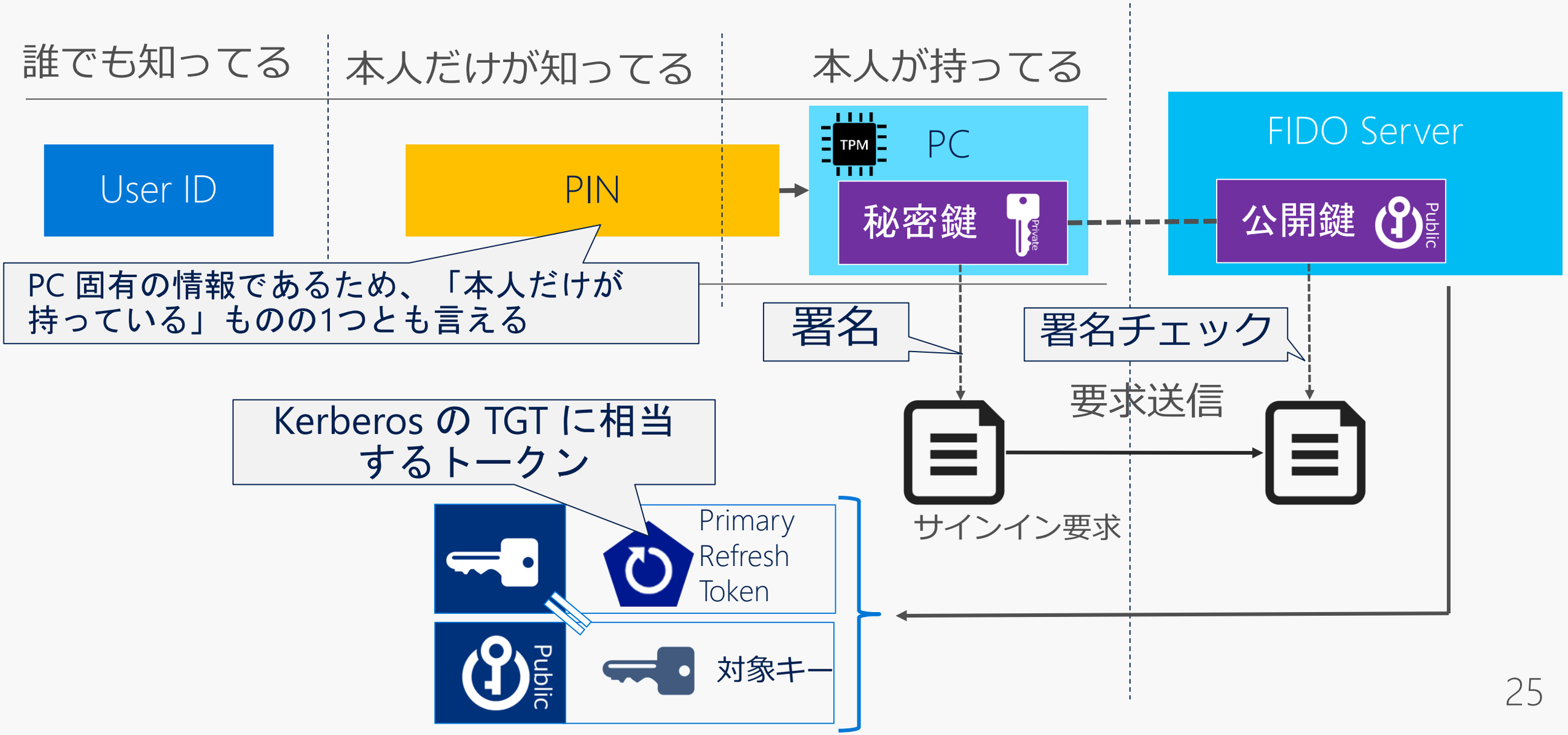
IC カード
（証明書）

スマフォ
・電話
・OTPアプリ

生体情報
・顔
・指紋
・虹彩

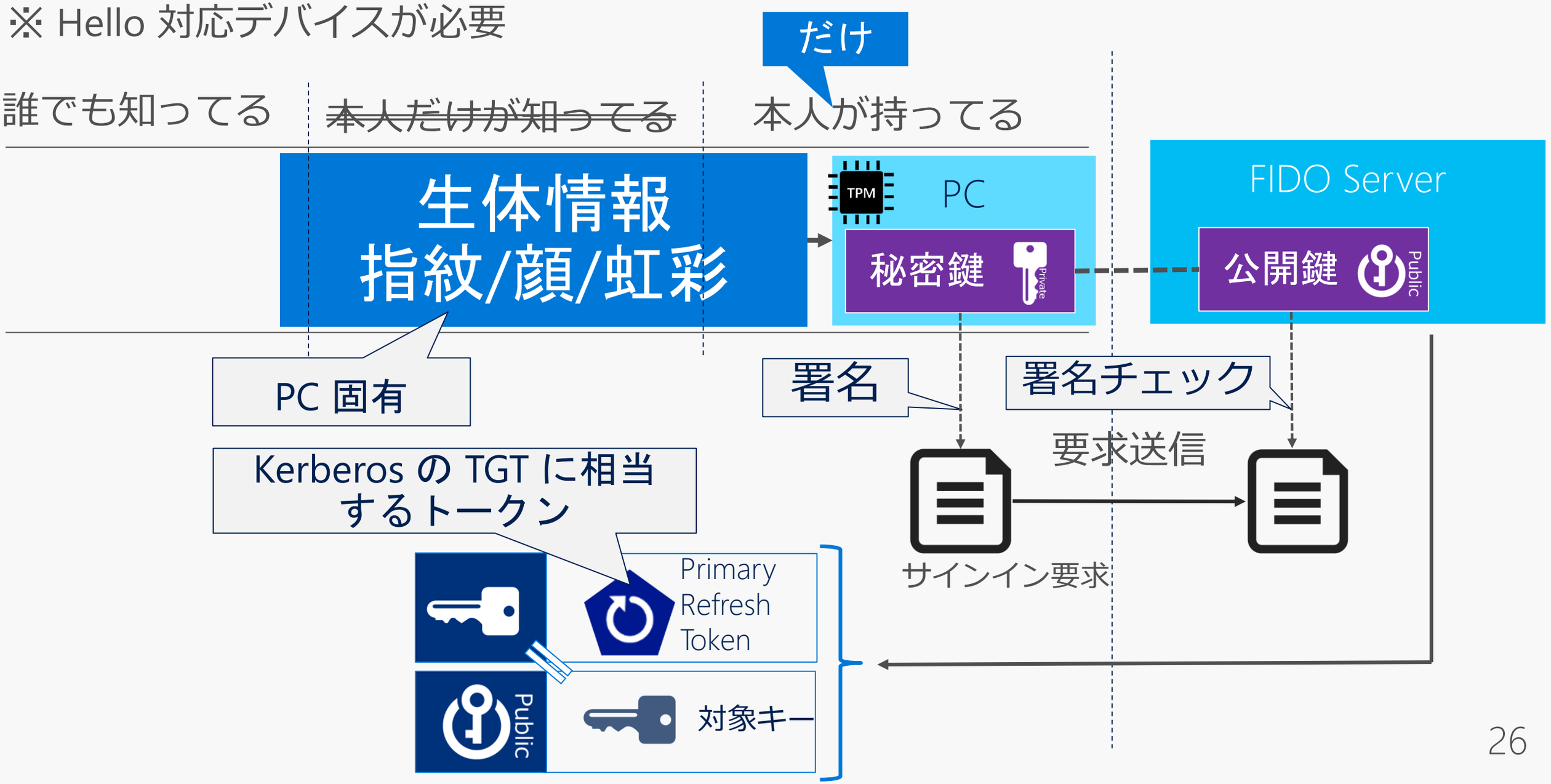
FIDO – The Fast Identity Online Alliance

FIDO によるユーザー認証



FIDO + Biometrics

※ Hello 対応デバイスが必要



FIDO 2.0

https://w3c.github.io/webauthn/

堅牢にユーザー認証を行うために、強度が高く、暗号化されたScoped（特定のWEBアプリに対する）Credential を作成するための API に関する仕様

Web Authentication: An API for accessing Public Key Credentials Level 1

Editor's Draft, 22 November 2017

This version:
https://w3c.github.io/webauthn/

Latest published version:
https://www.w3.org/TR/webauthn/

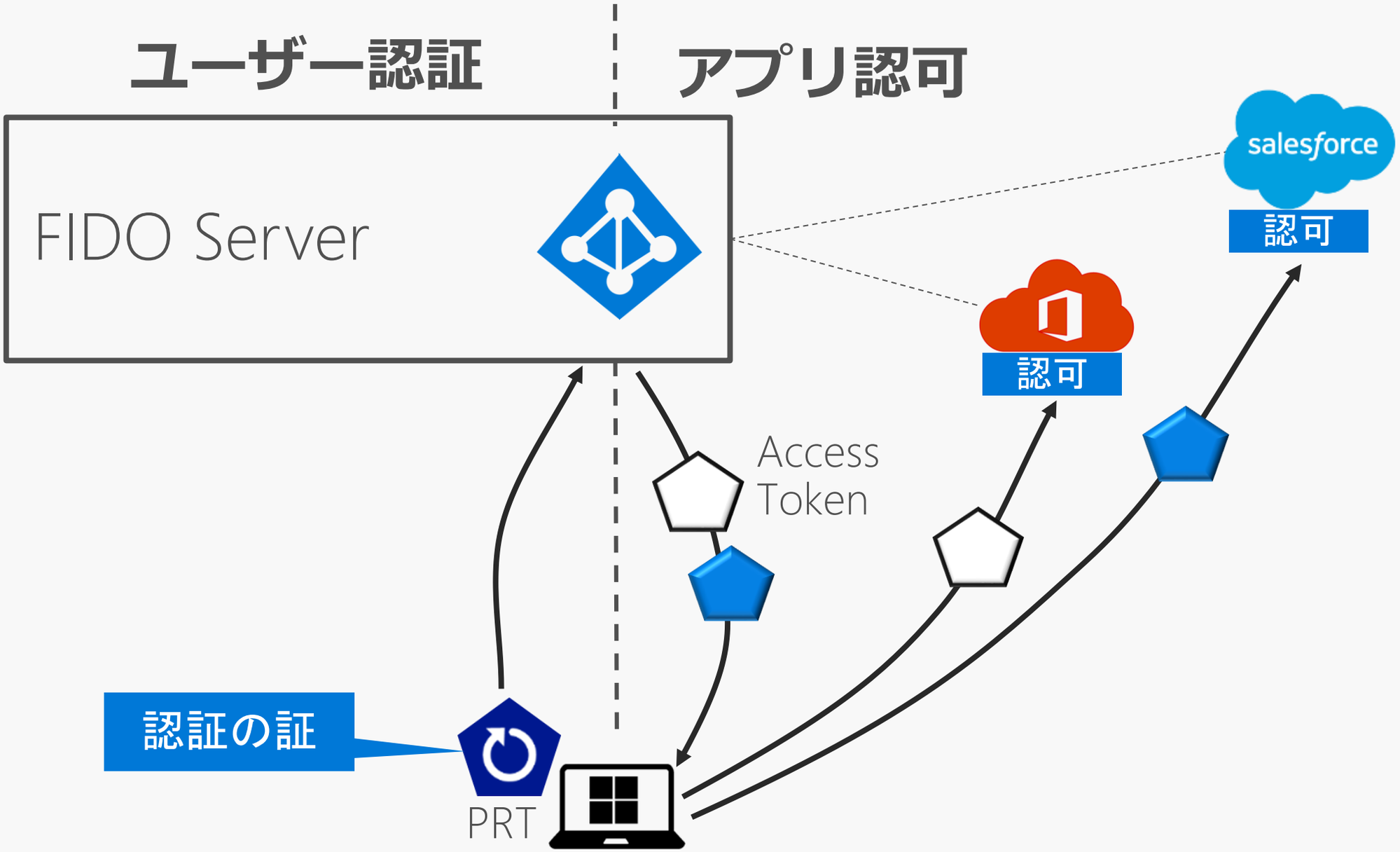
Previous Versions:
https://www.w3.org/TR/2017/WD-webauthn-20170811/
https://www.w3.org/TR/2017/WD-webauthn-20170505/
https://www.w3.org/TR/2017/WD-webauthn-20170216/
https://www.w3.org/TR/2016/WD-webauthn-20161207/
https://www.w3.org/TR/2016/WD-webauthn-20160928/
https://www.w3.org/TR/2016/WD-webauthn-20160902/
https://www.w3.org/TR/2016/WD-webauthn-20160531/

Issue Tracking:
Github

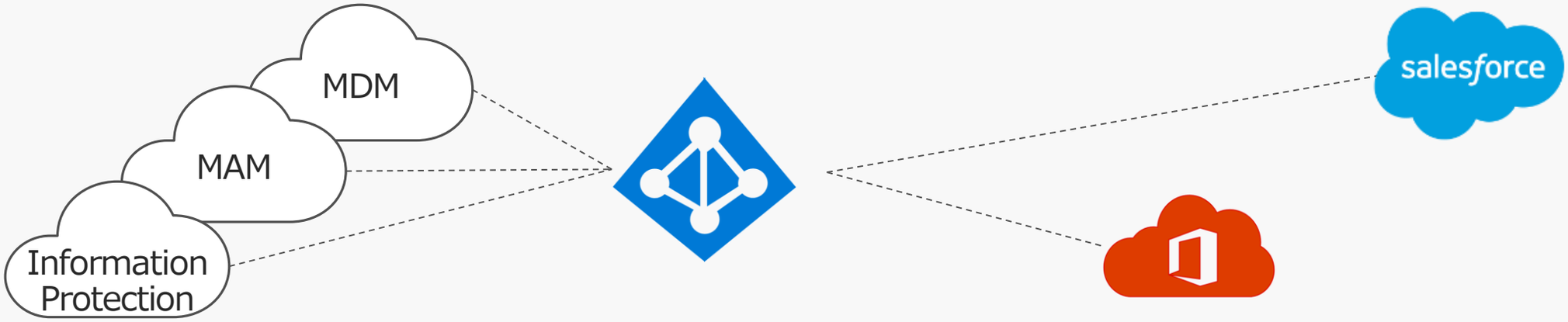
Editors:
Vijay Bharadwaj (Microsoft)
Hubert Le Van Gong (PayPal)
Dirk Balfanz (Google)
Alexei Czeskis (Google)
Arnar Birgisson (Google)
Jeff Hodges (PayPal)
Michael B. Jones (Microsoft)
Rolf Lindemann (Nok Nok Labs)
J.C. Jones (Mozilla)

Tests:
web-platform-tests webauthn/ (ongoing work)

FIDO 2.0

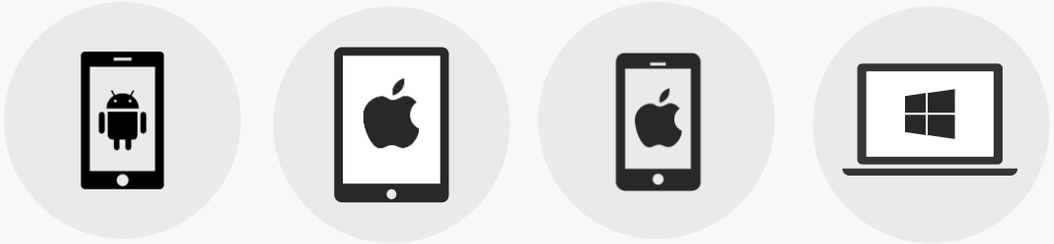

ユーザー認証
アプリ認可
FIDO Server
salesforce
認可
認可
Access
Token
認証の証
PRT

Conditional Access

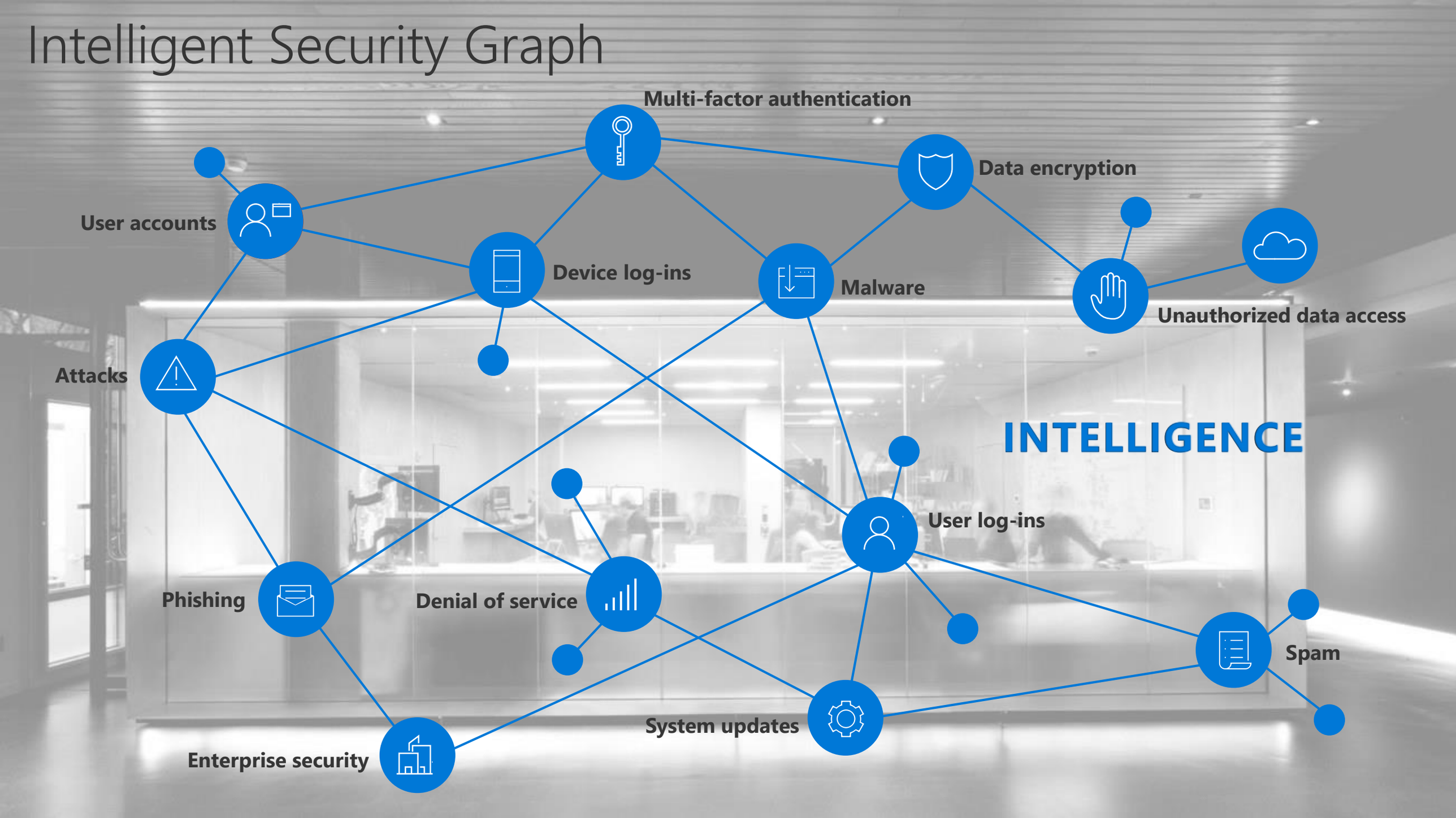


条件判定

- 利用者のロール、属性
- 場所
- 利用しているクライアントアプリ
- デバイスやOSの種類
- デバイスの安全性
- リスク
- アクセス先
- 認証方法



Intelligent Security Graph



Endpoint Detection Response (EDR)

- 現在進行する攻撃(未知も含む)に対する早期の検知
- 検知された攻撃への迅速な対処
- これらサービスの継続的な提供

Indicator of Compromise (IOC)

既知の侵入痕跡のデータベース

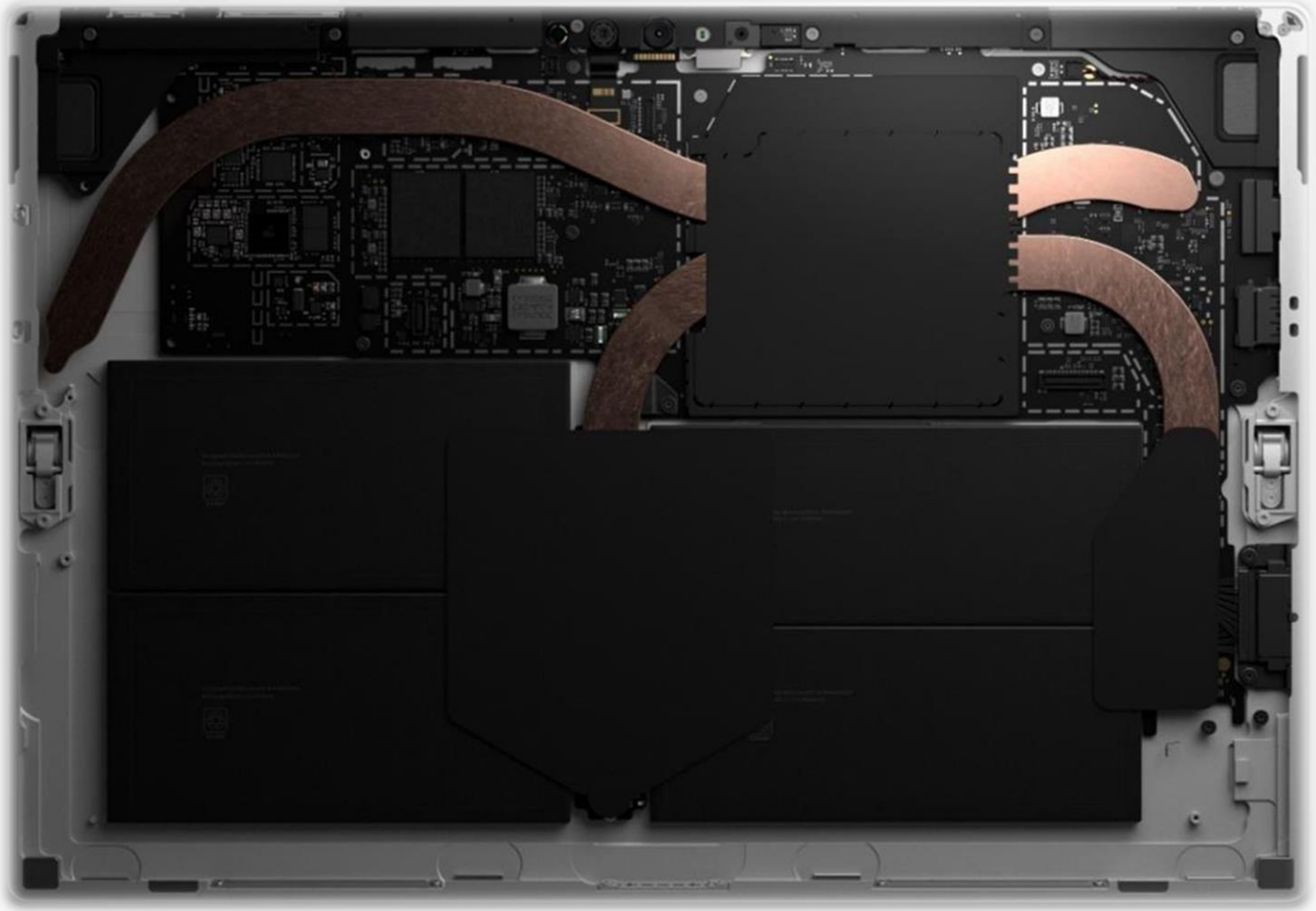
- マルウェアのシグネチャ
- ファイル名
- IP アドレス
- レジストリ

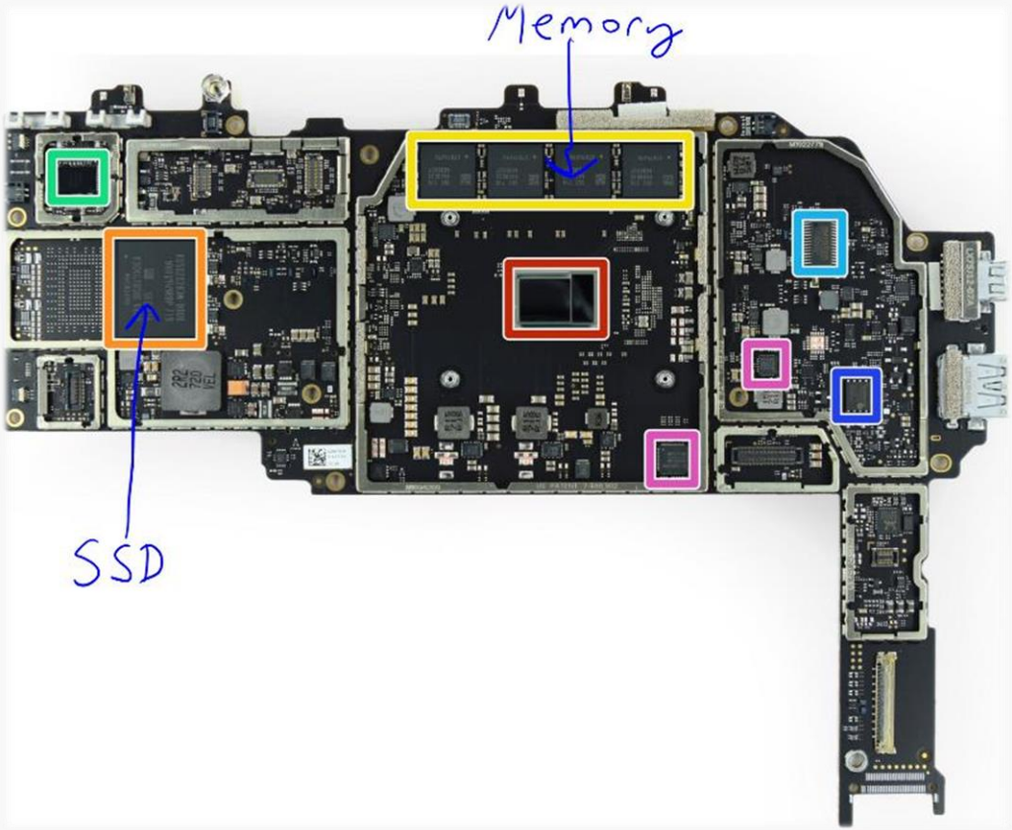
Indicator of Attack (IOA)

- 攻撃手段のデータベース
- 侵入のステップにマッピング
- 攻撃者の行動の関連性を分析

Surface Memory and Disk Components

- No DMA port
- Non removable SSD

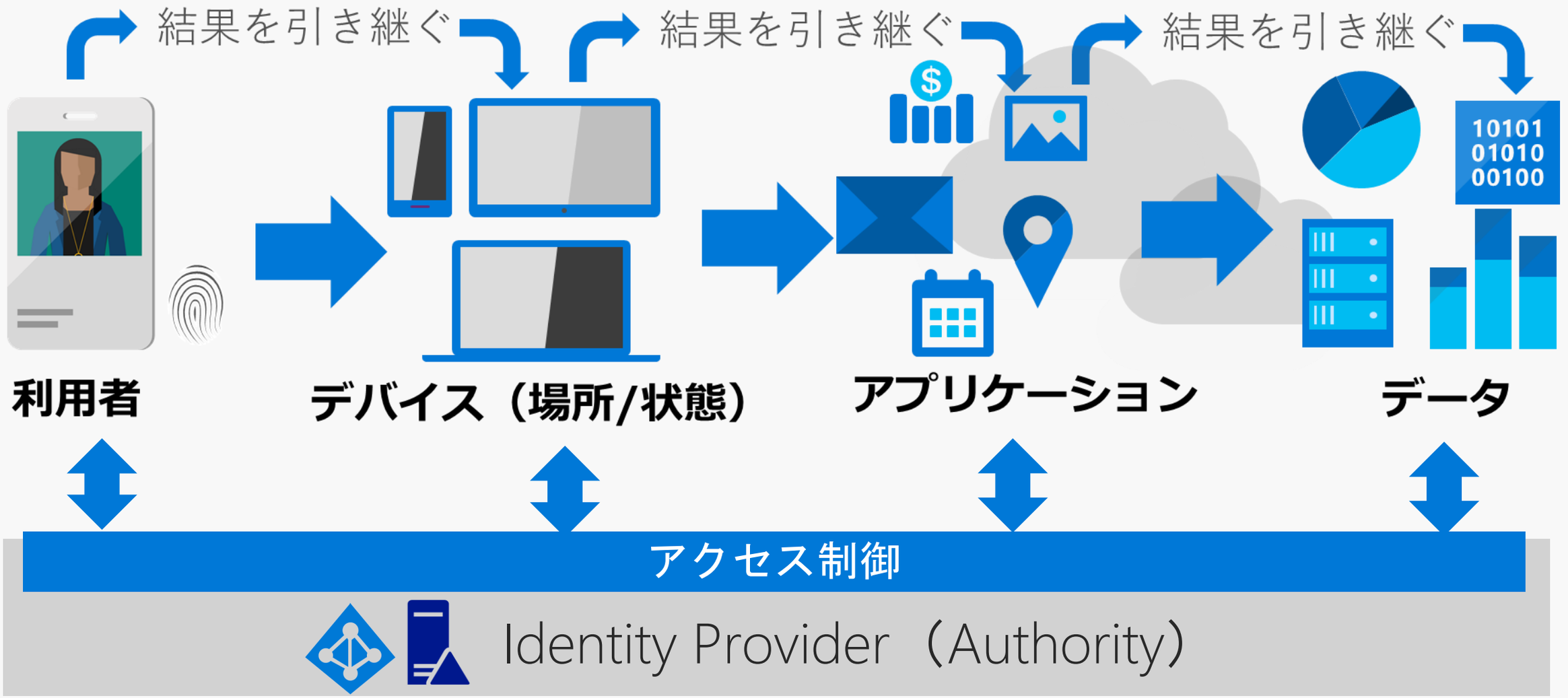




まとめ

人を中心としたセキュリティ設計

People-Centric IT



Azure: The Trusted Cloud

GLOBAL

ISO 27001

ISO 27018

ISO 27017

ISO 22301

SOC 1 Type 2

SOC 2 Type 2

SOC 3

CSA STAR
Self-Assessment

CSA STAR
Certification

CSA STAR
Attestation

US GOV

Moderate
JAB P-ATO

High
JAB P-ATO


DoD DISA
SRG Level 2


DoD DISA
SRG Level 4


DoD DISA
SRG Level 5

SP 800-171

FIPS 140-2


Section 508
VPAT


ITAR

CJIS

IRS 1075

INDUSTRY

PCI DSS
Level 1

CDSA


MPAA

FACT UK

Shared
Assessments

FISC Japan

HIPAA /
HITECH Act

HITRUST

GxP
21 CFR Part 11

MARS-E

IG Toolkit UK


FERPA


GLBA

FFIEC

REGIONAL


Argentina
PDPA


EU
Model Clauses

UK
G-Cloud

China
DJCP


China
GB 18030

China
TRUCS

Singapore
MTCS

Australia
IRAP/CCSL

New Zealand
GCIO

Japan My
Number Act

ENISA
IAF

Japan CS
Mark Gold

Spain
ENS

Spain
DPA

India
MeitY

Canada
Privacy Laws

Privacy
Shield

Germany IT
Grundschutz
workbook