

Microsoft Teams プライバシー・セキュリティ への取り組み ～プライバシー～

日本マイクロソフト株式会社
2020年4月16日



「企業や個人のユーザーがテクノロジーを心から受け入れるとすれば、それはそのテクノロジーを信頼することができた場合だけです。」

Satya Nadella
Chief Executive Officer
Microsoft Corporation



Microsoft におけるプライバシー



プライバシーは基本的人権の一つであると Microsoft は考えます。データがどのように収集され使用されるかをお客様が選択できるように、製品、情報、コントロールを提供していくことをお約束します。

[お客様のデータを守る](#)[GDPR](#)[プライバシーの原則](#)[データ管理](#)[その他のリソース](#)

お客様のデータを守ることは Microsoft の最優先事項

プライバシーを守るための設計

- データはお客様のもの
- データの使用目的は契約に明記。目的外使用は禁止。
- データへのアクセスは厳しく制限
- 契約終了後はデータを削除
- 各種法令、規制に対応
- データの運用に関する情報公開

顧客データの使用

- ❑ お客様が顧客データのすべての権利を持ちます。
 - ❑ M S による使用目的を契約に明記し、目的外使用は禁止です。
 - お客様へのオンラインサービス（＝クラウドサービス）提供のため
 - クラウドサービス機能の提供
 - トラブルシューティング
 - 生産性、ライセンス、有効性、セキュリティ面での製品改良
 - オンラインサービス提供に伴うM S の正当な事業運営のため
 - サイバー犯罪への対応
 - 課金やアカウント管理
 - インセンティブ計算
 - 内部報告（業績予測、キャパシティ計画など）
 - アクセシビリティ、プライバシー、エネルギー効率面での製品改良
 - 財務報告その他M S の法令遵守
- ※ユーザープロファイリング、広告その他商用目的では使用しません。

顧客データへのアクセス

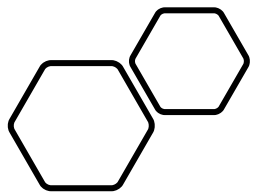
- お客様は契約期間中**自由**にアクセスできます
- **MS**の顧客データへのアクセスは**厳しく制限**されています
- **MS**は**第三者**に顧客データを**開示しません**

<例外>

- ✓ お客様の指示がある場合
- ✓ 契約に明記されている場合
- ✓ 法令上の要求

法執行機関からの要請への対応プロセス

1. MSではなくお客様に請求するよう回答
2. （再要請を受けたときは）強制力のある要請が法務部門にて詳しく検討
3. 強制力のある要請の場合のみ、必要最低限の情報を提供
4. （法令上認められれば）お客様に要請があったことを通知



契約終了後のデータ削除

契約期間中

お客様は自由にデータを保存、
抽出、削除可能

契約終了後90日

機能限定アカウントにデータ
が保持される

お客様によるデータ抽出可能

契約終了後91日から 180日

お客様はアクセスできない
期間内にアカウント無効とな
り、データ削除

下請業者の利用

- 下請業者を利用します。
- 下請業者は、MSとの書面契約に基づき、の責任を負います。
- 顧客データの処理にかかわる下請業者リストを公開。
 - 新規の業者を追加する場合、アクセスするデータの種類に応じて、60日または14日前までに通知
 - その業者の使用を認めない場合、ペナルティなしで解約可能



Microsoft Online Services Subprocessors List

This list identifies the subprocessors authorized to access customer data and personal data in Microsoft's Online Services. Any such subprocessors will be permitted to process customer data or personal data only to deliver the services Microsoft has retained them to provide, and they are prohibited from using such data for any other purpose. These subprocessors (including their subsidiaries) may provide services to one or more of the online services. The list below may not apply to previews or other services not yet in general release.

Subprocessors who provide technologies to power certain Microsoft Online Services

The following subprocessors provide technologies used to deliver specific Microsoft Online Services. If you deploy one of the services below, the subprocessor(s) identified for that service may process, store, or otherwise access customer data or personal data in the course of helping to provide that service.

Subprocessor	Service Provided	Corporate Location
Accenture LLC	SAP HANA on Azure (Large Instances)	Ireland
Akamai CDN	Content Delivery Network (CDN)	United States
AT&T Inc [Merged from previous personal data list]	Multi-factor Authentication	United States
CenturyLink, Inc [Merged from previous personal data list]	Multi-factor Authentication	United States
CLX Communications (f/k/a Sinch) [Merged from previous personal data list]	Multi-factor Authentication	Sweden
Databricks, Inc	Azure Databricks	United States
Infobip Ltd [Merged from previous personal data list]	Multi-factor Authentication	United Kingdom
NetApp, Inc (Added to the list May 13, 2019)	Azure NetApp Files	United States
Nexmo, Inc [Merged from previous personal data list]	Multi-factor Authentication	United States
Red Hat, Inc (Added to the list May 13, 2019)	Azure Red Hat OpenShift	United States
TeleSign	Multi-factor Authentication	United States
Twilio Inc	Multi-factor Authentication	United States
Verizon Communications Inc. (f/k/a Edgecast Networks, MCI)	Content Delivery Network (CDN) Multi-factor Authentication	United States

Subprocessors who provide ancillary services to support Microsoft Online Services

The following subprocessors provide ancillary services to help support, operate, and maintain the Online

コンプライアンス-世界各国の基準や法律に対応

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

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

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

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



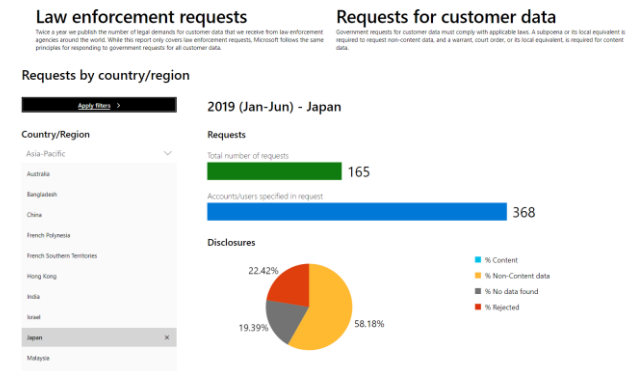
IRS 1075

積極的な情報公開

- クラウドサービスのセキュリティ、プライバシーに関するweb上での**情報提供**
- クラウドサービスの運用に関する**契約をwebで公開**
 - 誰でも、サービス利用前でも内容確認可能
 - 過去の契約も確認
- 法執行機関からの**開示要請への対応状況をwebで公開**



クラウドでデータ整合性を維持するための原則



トラストセンター

<https://www.microsoft.com/ja-jp/trust-center>



トラスト センター

セキュリティ

プライバシー

コンプライアンス

製品とサービス

業種

ツールとドキュメント

すべて Microsoft 製品

検索

カート

サインイン



"人を守ることができなければ、その人の信頼を得ることはできません。"

- Brad Smith (プレジデント兼最高法務責任者)

セキュリティ、プライバシー、コンプライアンスは、組織がその顧客のために活動できるよう Microsoft が支援するときの中心の原則です。

ビデオを見る



クラウドでデータ整合性を維持するための原則



セキュリティ

デジタル トランスフォーメーションのための安全な世界をどのように作るかをご紹介します。

[詳細情報 >](#)



プライバシー

Microsoft はプライバシーの不变的な価値を信じており、お客様のデータをお客様が制御できるようにしています。

[詳細情報 >](#)



コンプライアンス

Microsoft は地域の法律と規制を尊重し、幅広いコンプライアンス認証に対応しています。

[詳細情報 >](#)

オンラインサービスデータ保護追加条件

Data Protection Addendum

 Microsoft

Cloud ▾

Mobility ▾

Productivity ▾

Licensing

Product Licensing ▾

Licensing Programs ▾

Existing Customer ▾

Learn More ▾

How to Buy ▾

Support ▾

Licensing Terms and Documentation

Quickly access licensing terms, conditions, and supplemental information relevant to the use of products and services licensed through Microsoft Volume Licensing programs.

Licensing Terms Search

Licensing Documents Search

[Return to Document Search](#)

SLAs, terms and other agreement-related documents
Find licensing documents by selecting any of the filters below (document type, language, region or sector). Once you start making selections, results will appear in the table below.

Search for Documents:

Note: This page does not include any signed Volume Licensing agreements, enrollments or Microsoft Business and Services Agreement, and is intended solely for reference purposes.

☐ Show Archived

Search:

Title	Language	Sectors	Regions
MicrosoftOnlineServicesDPA(Hungarian) (January2020)	Hungarian	Commercial, Public Sector, Third Party, Common Document, Academic, Government, Nonprofit	EU-EFTA (European Union and EFTA), EMEA (Europe, Middle East and Africa)
MicrosoftOnlineServicesDPA(Italian) (January2020)	Italian	Commercial, Public Sector, Third Party, Common Document, Academic, Government, Nonprofit	EU-EFTA (European Union and EFTA), EMEA (Europe, Middle East and Africa)
MicrosoftOnlineServicesDPA(Japanese) (January2020)	Japanese	Commercial, Public Sector, Third Party, Common Document, Academic, Government, Nonprofit	Japan

ボリューム ライセンス

マイクロソフト オンライン サービス データ保護追加契約 2020 年 1月

顧客データ取扱い、セキュリティなど詳細。法的拘束力のある契約。ダウンロード可。日本語、外国語にも対応。

<https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67>

オンラインサービス条件 Online Services Terms (OST)



製品条項 (PT)

製品条項には、マイクロソフト ボリューム ライセンス プログラムを通じてソフトウェアやオンライン サービスのライセンスを購入する方法のあらゆる条件が含まれています。製品条項は毎月更新され、最新のバージョンもアーカイブもダウンロードすることができます。製品条項についての詳細は、製品ライセンスについてよく知っておくべきこと (PDF, 1.47 MB) をご覧ください。

ご注意: 製品条項は、製品使用権説明書と製品表の代わりに、2015 年 7 月 1 日から提供開始となったドキュメントです。2015 年 7 月以前の製品使用権説明書と製品表のご確認は、以下の日本語版のアーカイブ (英語サイト) よりご確認ください。

Arabic	English	Korean	Serbian
Bulgarian	Estonian	Latvian	Slovak
Catalan	Finnish	Lithuanian	Slovenian
Chinese Simplified	French	Norwegian	Spanish
Chinese Traditional	German	Polish	Swedish
Croatian	Greek	Portuguese Brazil	Thai
Czech	Hungarian	Portuguese EMEA	Turkish
Danish	Italian	Romanian	Ukrainian
Dutch	Japanese	Russian	

日本語版のアーカイブ (英語サイト)

※ 日本語の過去のドキュメントのご確認は、英語サイトへアクセス後、表示されたテーブルの右上部の [Show Archived] のチェック ボックスをクリックしてください。「レ」が入り、アーカイブのテーブルが先の表示されたテーブルの直下に表示されますので、新たに表示されたテーブルの左上の [All Languages] で [Japanese] をご確認ください。

オンライン サービス条件 (OST)

マイクロソフト ボリューム ライセンス プログラムを通じてオンライン サービスのサブスクリプションを使用する場合、使用方法に関するサービス条件は、ボリューム ライセンス オンライン サービス条件 (OST) およびプログラム契約にて定義されます。OST は毎月更新され、最新のバージョンもアーカイブもダウンロードすることができます。

ご注意: 2014 年 7 月 1 日より、マイクロソフト オンライン サービス使用権説明書 (OLSUR) はマイクロソフト オンライン サービス条件 (OST) に置き換わりました。OLSUR については、下記の日本語版アーカイブ (英語サイト) よりダウンロードいただけます。

Arabic	English	Korean	Serbian
Bulgarian	Estonian	Latvian	Slovak
Catalan	Finnish	Lithuanian	Slovenian
Chinese Simplified	French	Norwegian	Spanish
Chinese Traditional	German	Polish	Swedish
Croatian	Greek	Portuguese Brazil	Thai
Czech	Hungarian	Portuguese EMEA	Turkish
Danish	Italian	Romanian	Ukrainian
Dutch	Japanese	Russian	

日本語版のアーカイブ (英語サイト)

日本語の過去のドキュメントの確認方法は、上記の「※」をご参照ください。

サービス プロバイダー製品使用権説明書 (SPUR)

サービス プロバイダー製品使用権説明書 (SPUR) は、Microsoft Services Provider License Agreement (SPLA) を通じて取得した製品の使用方法に関する詳細情報を提供します。SPUR は四半期ごとに更新されます。SPUR については最新版とアーカイブ版をダウンロードすることができます。

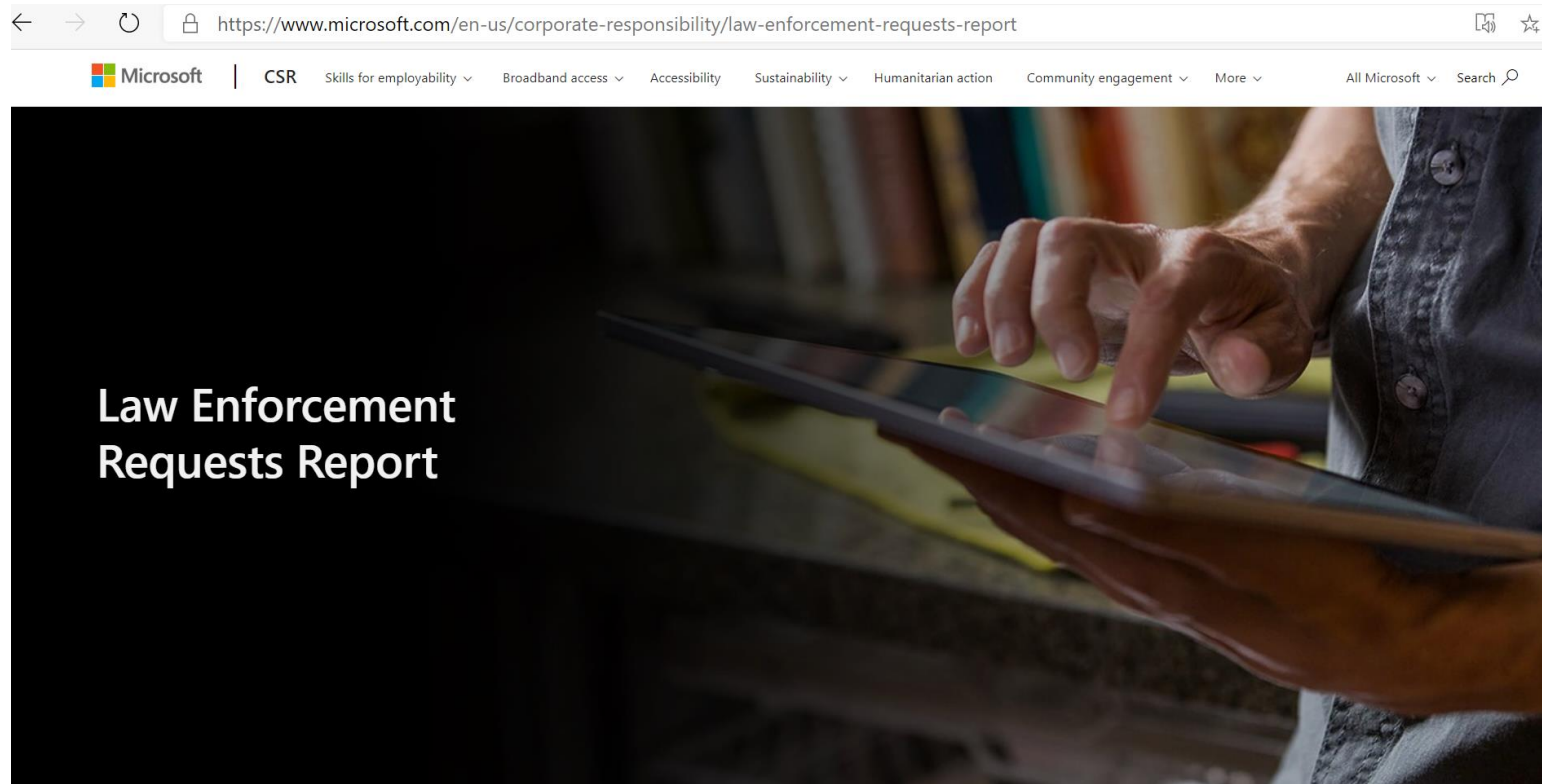
Volume
Licensing

オンライン サービス条件
2020 年 4 月

オンラインサービス毎の条件。顧客データの保存場所。
法的拘束力のある契約。ダウンロード可。
毎月更新。日本語、外国語にも対応。

<https://www.microsoft.com/ja-jp/licensing/product-licensing/products>

法執行機関からの開示要請情報の公開



情報開示要請の状況
（要請件数、国、対応等）について6か月毎に公開

2019年上半期
法人向けクラウドに関する要請件数合計：74
（内訳）

拒絶、非開示：32
非コンテンツ開示：20
コンテンツ開示：22

お客様のデータを守ることは Microsoft の最優先事項

Microsoft Teams プライバシー・セキュリティ への取り組み

日本マイクロソフト株式会社
2020年4月16日



セキュリティ

情報セキュリティの3大要素 - CIA



【情報セキュリティの3大要素 CIA】

完全性 Integrity

情報が保存した時点のまま維持されていること
(改ざんや破壊がされていない)

機密性 Confidentiality

情報が漏れないこと
(正当な権限を持つものだけが情報を利用可能)

可用性 Availability

情報が利用したいときに利用できること
(業務継続性の確保)

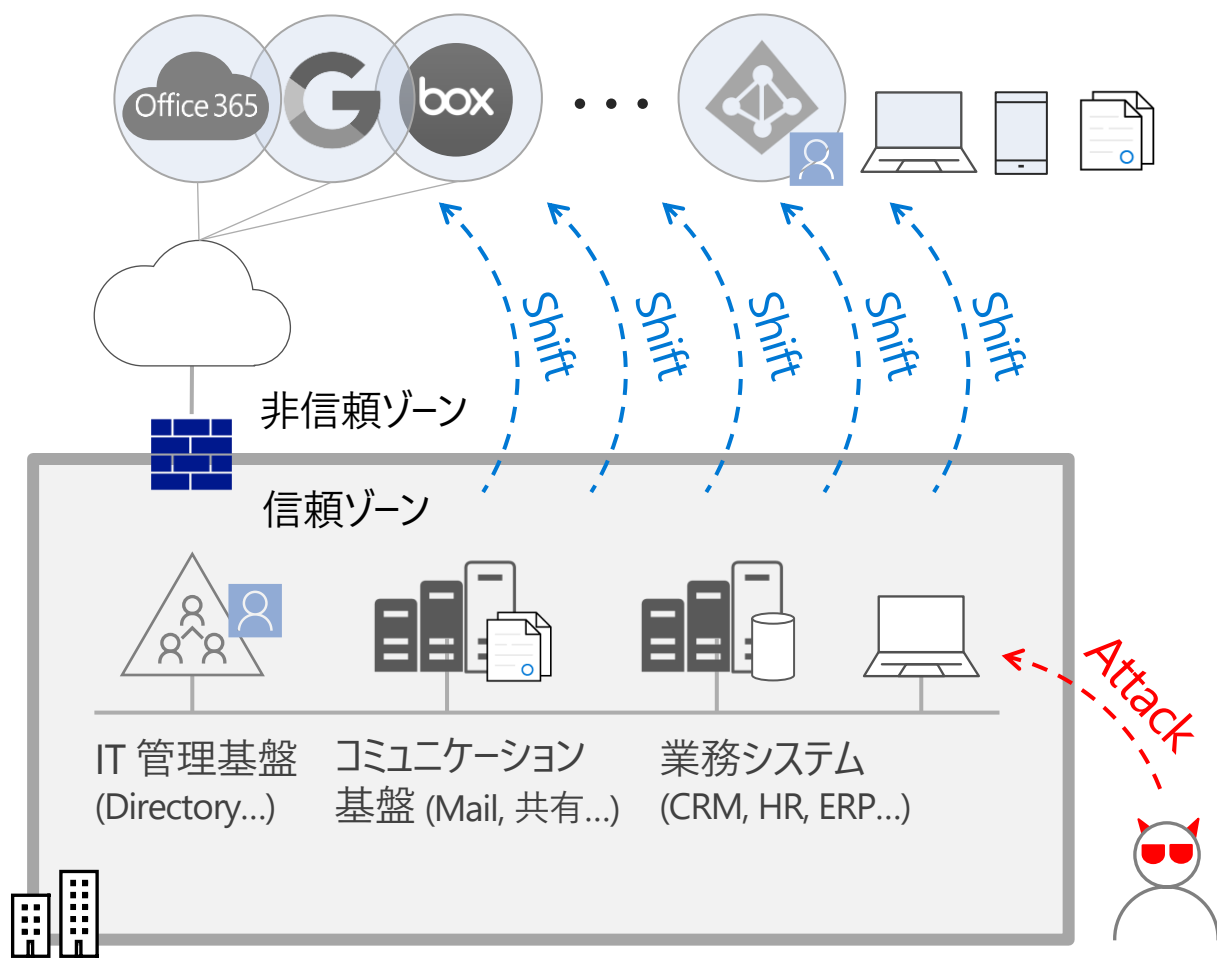
IT 環境の変化

1990年 – 2010年 ネットワーク境界モデル



IT 環境の変化

1990年 – 2010年 ネットワーク境界モデル → ネットワーク境界モデルの限界



システムのクラウドシフトが進み、
IT 環境が大きく変化

必要なモノが非信頼ゾーンに



攻撃の高度化、多様化により
信頼ゾーンへの侵入は日常的に

信頼ゾーンが信頼できない

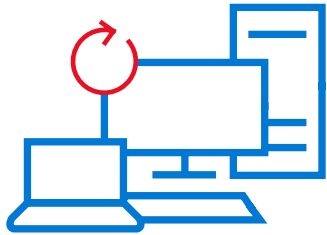
新しい考え方



失敗を前提に – The Mindshift

THEN

高い信頼性:
Designed not to fail

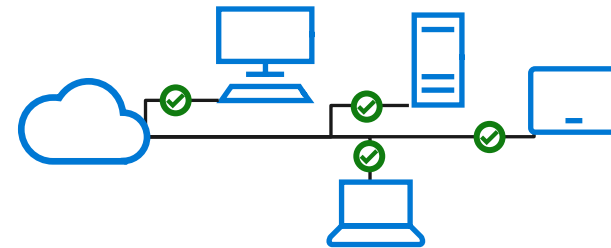


鉄壁の防御:
Every possible attack

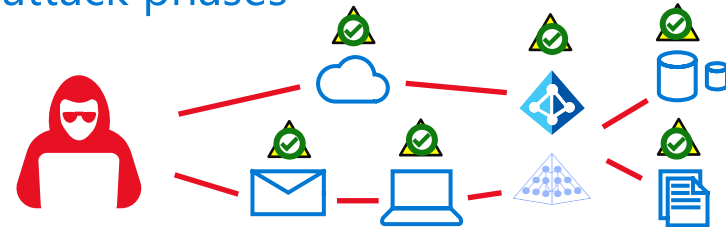


NOW

レジリエンス:
Designed to recover quickly

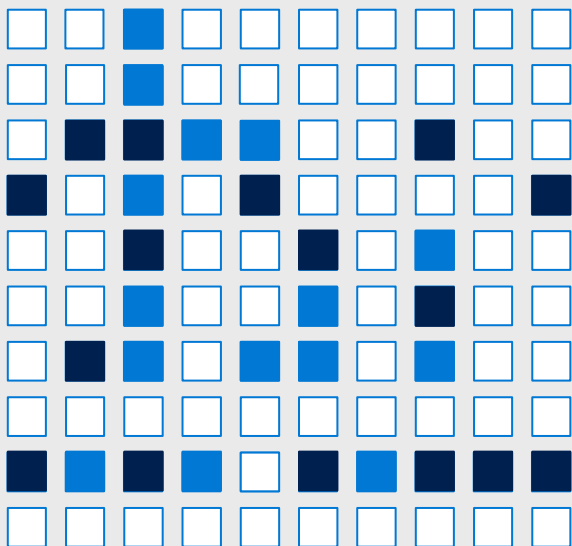


Assume Compromise:
Protect, detect, and respond along
attack phases

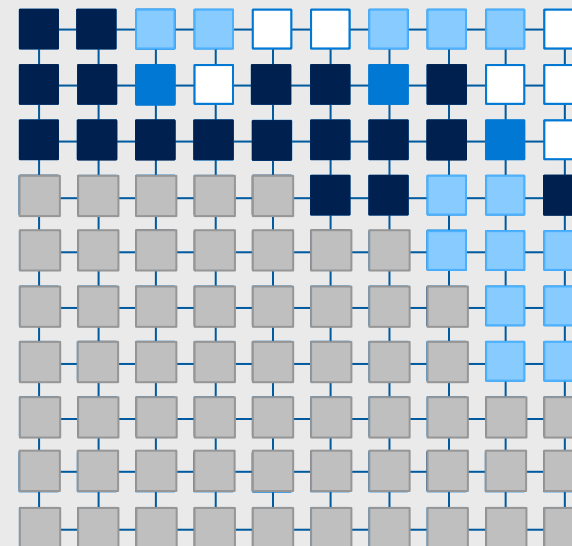
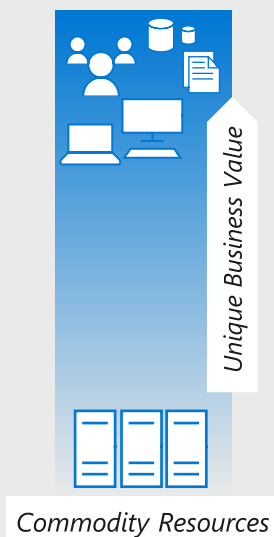


クラウドの活用

TRADITIONAL APPROACH



CLOUD-ENABLED SECURITY



セキュリティ対策の充実度

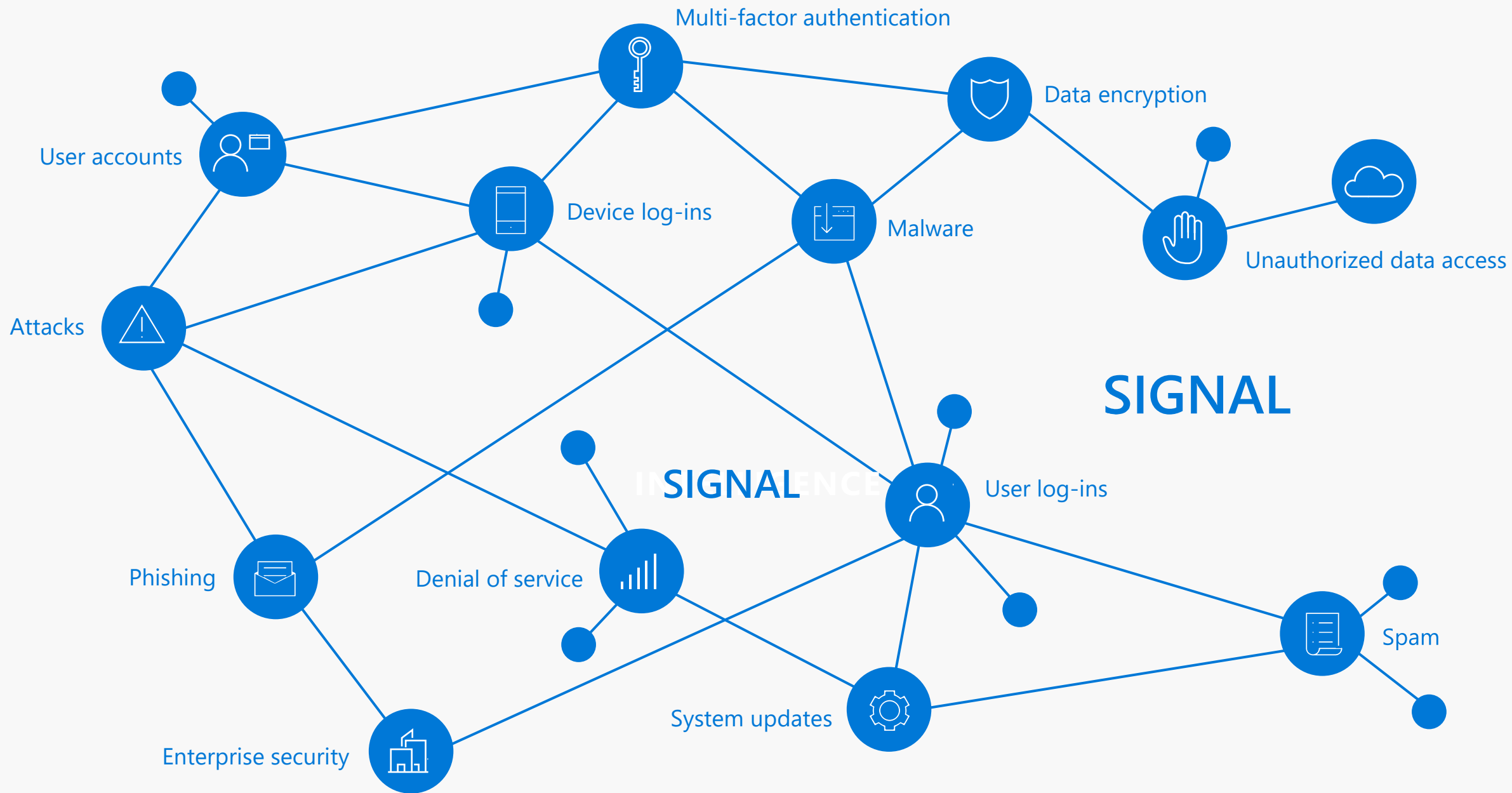
- | | |
|-----------|------------------------------|
| ■ 責任範囲の達成 | □ 未達成 |
| ■ 部分的に達成 | ■ クラウドの責任 (Trust but verify) |

クラウドテクノロジーのメリット:

- 一般的な責任範囲をクラウドにアウトソース、重要なところに集中
- クラウドのセキュリティ機能を有効活用
- 検知・レスポンス時間の短縮のためのインテリジェンス

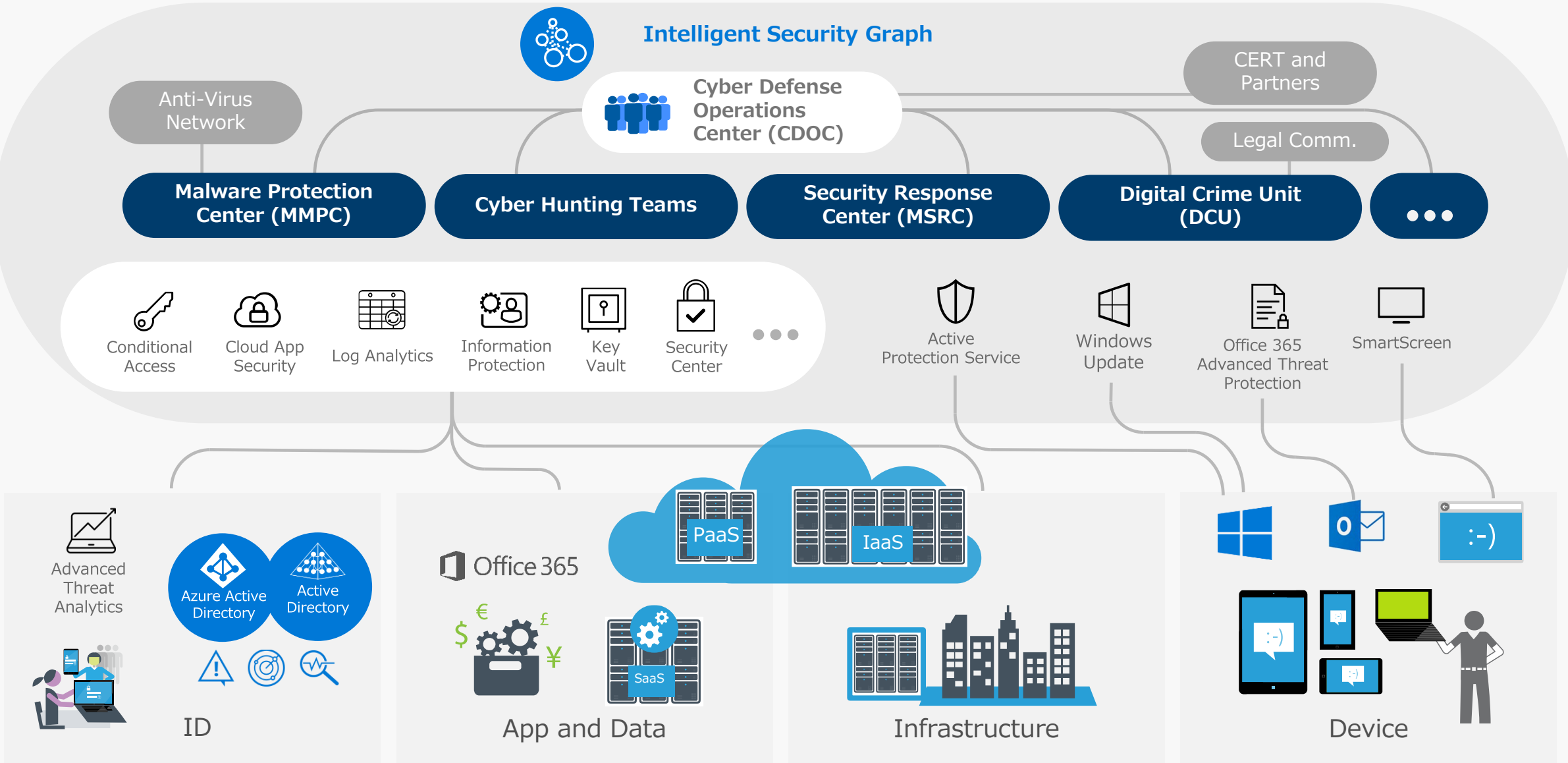
The Microsoft Intelligent Security Graph





The Microsoft **SIGNA**
Intelligent Security Graph

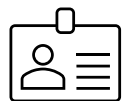
Microsoftのセキュリティ



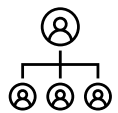
Microsoft Teams

プライバシーとセキュリティへの取り組み

<https://aka.ms/security-teams-blog>



組織外のメンバーが会議に参加するときは、直接参加させるか、**誰かが許可を出すまでロビーで待機**させるかの設定が可能



ゲストアクセス機能で、**自社データを制御したまま**組織外の参加者を追加



AIがチャットを巡回し、いじめやハラスメントなどのネガティブな行動を防ぐ



Teams では**データの転送中も静止状態でも暗号化が施され**、安全なデータセンターネットワーク内に保存



多要素認証 (MFA) による、脆弱なパスワードや盗難パスワードを利用した攻撃からのユーザー保護



HIPAA | GDPR | FedRAMP | SOCなど90以上の**国際的な規制基準や法律**に準拠