Microsoft

「教育情報セキュリティポリシーに関するガイドライン (令和元年 12 月版) 」ハンドブック

第 1.2 版

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
文教営業本部

1 はじめに

政府の成長戦略※1には、「**Society 5.0 時代に向けた人材育成**」がメインテーマの 1 つとして掲げられています。この中には『a) 大学等における人材育成』として「**大学等における AI・データサイエンス人材育成**」が、また『b) 初等中等教育段階における人材育成』として「**初等中等教育段階における ICT 環境整備**」が掲げられ、「小学校、中学校、高等学校等における必要な ICT 環境について、児童生徒人一人がそれぞれ端末を持ち、十分に活用できる環境を実現する」ことと、その実現環境として「学校の ICT 環境のクラウド化を推進し、授業・学習系システムと校務系システムの安全な連携手法を確立する」ことが掲げられています。この成長戦略方針に沿った施策が「**GIGA スクール構想**※2」です。本構想の実現に向けて、文部科学省は 5 つの取り組みを掲げました。

少子高齢化を含めた Society 5.0 時代には、社会構造や雇用環境が大きく変化すると考えられています。そのような社会で求められる能力や子供たち自身の多様化を踏まえ、ICT を活用した自宅学習、個別最適化された学びなど児童・生徒の学習の多様化や、その実現に向けたテレワークなど教員の働き方改革、地域ボランティアの活用など、教育現場の改善をクラウド化された ICT 環境の下で安全、安心に構築することが求められています。本書では文部科学省の「**GIGA スクール構想の実現パッケージ**」の 1 つである「**クラウド活用前提のセキュリティガイドライン**※3」について解説します。

※1: 成長戦略ポータルサイト https://www.kantei.go.jp/jp/singi/keizaisaisei/portal/
※2: GIGA スクール構想の実現について https://www.mext.go.jp/a_menu/other/index_00001.htm
※3: 教育情報セキュリティポリシーに関するガイドライン (令和元年 12 月版)
https://www.mext.go.jp/content/20191223-mxt_jogai02-000003329_006.pdf

GIGA スクール構想の実現パッケージ ～令和の時代のスタンダードな学校へ～

1 環境整備の標準仕様例示と調達改革

- 「新時代の学びを支える先端技術活用推進方策」の考え方に基づく、**学習者用端末の標準**仕様を例示
- 「GIGA スクール構想」に基づく、高速回線に向けた**校内 LAN 整備の標準仕様**を例示
- 容易に大規模な調達が行えるよう、標準仕様書を基に**都道府県レベルでの共同調達**を推進

学校 ICT 環境の整備調達をより容易に

2 クラウド活用前提のセキュリティガイドライン公表

各教育委員会・学校が情報セキュリティポリシーの作成や見直しを行う際の参考とする、**『教育情報セキュリティポリシーに関するガイドライン』(平成 29 年策定)**を、**クラウド・バイ・デフォルト**の原則を踏まえて改訂

- 整備の硬直化を避けるための位置づけや構成の見直し
- クラウド・バイ・デフォルトの原則追記
- クラウドサービス事業者が留意すべき事項の追加

クラウド活用により使いやすい環境へ

3 学校 ICT 利活用ノウハウ集公表

教師や学校、教育委員会等が、情報教育や ICT を活用した指導、ICT 環境整備等を行う際に参考となる様々な情報をまとめた「**教育の情報化に関する手引**」を公表。特に「第 4 章教科等の指導における ICT の活用」においては、ICT を効果的に活用した学習場面の 10 の分類例を示すとともに、

- 小学校、中学校、高等学校については各学校段階における各教科等ごとに
- 特別支援教育については学習上の困難・障害種別ごとに **ICT を活用した効果的な学習活動の例を提示**

全ての教職員がすぐに使えるように

4 関係省庁の施策との連携

- 総務省：教育現場の課題解決に向けた**ローカル 5G の活用モデル構築**
- 経済産業省：**EdTech 導入実証**事業、学びと社会の連携促進事業、**学びと社会の連携促進**事業

ローカル 5G や教育コンテンツも活用して未来の学びを実現

5 民間企業等からの支援協力募集

将来の ICT 社会を創造し、生きていく子供達に向けた社会貢献として、**民間企業等から学校 ICT 導入・利活用に対するあらゆる協力を募る。**

- 校内 LAN など通信環境の無償提供
- 新品、中古問わず十分なスペックの端末の学習者への提供
- ICT 支援員として学校の利活用の人的サポート等

公表し、文部科学省から教育委員会へ随時繋いでいく

民間等の外部支援により導入・利活用加速

2 教育情報セキュリティポリシーに関するガイドライン (令和元年 12 月版) の改訂内容

「教育情報セキュリティポリシーに関するガイドライン (令和元年 12 月版) の改訂では、以下の 2 点に対して追記が行われました。

平成 29 年度版ガイドライン	令和元年 12 月版ガイドライン
オンプレミス環境による構築を想定した内容であり、クラウド利用を前提とした記載がなく、教育現場におけるクラウドサービス利用に関する方向性が不明確であった。	「政府情報システムにおけるクラウドサービス利用に係る基本方針」(2018 年 6 月 7 日　各府省情報化統一責任者 (CIO) 連絡会議決定) の内容を参考に、**教育現場におけるクラウドサービス利用に関する考え方**を追記。
クラウドサービス利用時の、クラウドサービス提供事業者における情報の取り扱い方法が必ずしも明確でない。(同意のない目的外利用、第三者提供が行われていないかなど)	クラウドサービス提供事業者が**留意すべきプライバシーに関する事項**を追加。

3 教育情報セキュリティポリシーに関するガイドライン (令和元年 12 月版) の改訂ポイント

「教育情報セキュリティポリシーに関するガイドライン (令和元年 12 月版) 改訂のポイントを以下に示します。

クラウドサービス選定の推奨項目

1. 守秘義務、目的外利用及び第三者への提供の禁止

個人情報を取り扱うクラウドサービスを利用する場合は、クラウドサービスにおける
個人情報の規定 (ISO27018, ISO2770 など) などの認証を取得しているサービスが望ましい。 P8

参照 : クラウドサービスにおける個人情報の取り扱い (改訂個人情報法との関連) P9

2. 準拠する法令、情報セキュリティポリシー等の確認

自らの情報資産の管理に**日本の法律が適用**されること、係争時における**管轄裁判所が日本国内**になることに留意する必要がある。 P12

3. 監査

クラウドサービスが安全に運用されているかの確認には、**日本のクラウド情報セキュリティ監査 (CS ゴールドマーク)** で
認定を受けているクラウドサービスを選定することで、クラウド利用者による直接監査を行う必要なく、
CS ゴールドマークを導入時や年次の**利用者自身の監査結果として利用できる**。 P5 P7

クラウドサービス利用時におけるセキュリティ対策

4. セキュリティ モデル

最新の**セキュリティ モデル (ゼロトラスト)** を採用することで、クラウドを安全に利用することが可能。 P13

5. 標的型攻撃対策

校務に携わる者のセキュリティには、**標的型攻撃への対策**が施されていることが望ましい。 P15

4 クラウドサービスの選定にあたって

4.1 政府情報システムにおけるクラウドサービス調達基準※4

クラウドサービスの情報セキュリティ機能の実態を利用者が個別、かつ詳細に調査することは困難です。そのためパブリッククラウドの利用選定に際しては、第三者による認定や各クラウドサービスの提供する**監査報告書を利用することが重要**です。パブリッククラウドの利用選定に際しては、以下のいずれかの認定制度の認証を取得し、または監査フレームに対応していることが推奨されます。

【認証制度】

① ISO/IEC 27017 による認証の取得
https://isms.jp/isms-cls/lst/ind/index.html

② JASA クラウドセキュリティ推進協議会 CS ゴールドマーク
https://jcispa.jasa.jp/cs_mark_co/cs_gold_mark_co/

③ 米国 FedRAMP
https://marketplace.fedramp.gov/#/products?stuatus=Compliant&sort=productName

※4: 政府情報システムにおけるクラウドサービスの利用に係る基本方針　2018 年 (平成 30 年 6 月 7 日各府省情報化統括責任者 (CIO) 連絡会議決定)
https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

4 クラウドサービスの選定にあたって

4.2 クラウドサービスの安全性評価制度※5 とは

教育情報セキュリティ対策を考えるにあたり、

① 政府機関等の情報セキュリティ対策のための統一基準※2

② 政府情報システムにおけるクラウドサービスの利用に係る基本方針※1

を考慮する必要があります。

この 2 つの「基準」および「方針」の適合性を監査・評価するのが、現在制度設計が行われている「**クラウドサービスの安全性評価制度**※3」です。

運用が開始された際には、本制度の認証を取得したクラウドを採用することが推奨されています。

※5: 経済産業省 | クラウドサービスの安全評価に関する検討会　https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/index.html

4 クラウドサービスの選定にあたって

4.3 クラウド情報セキュリティ監査制度※6

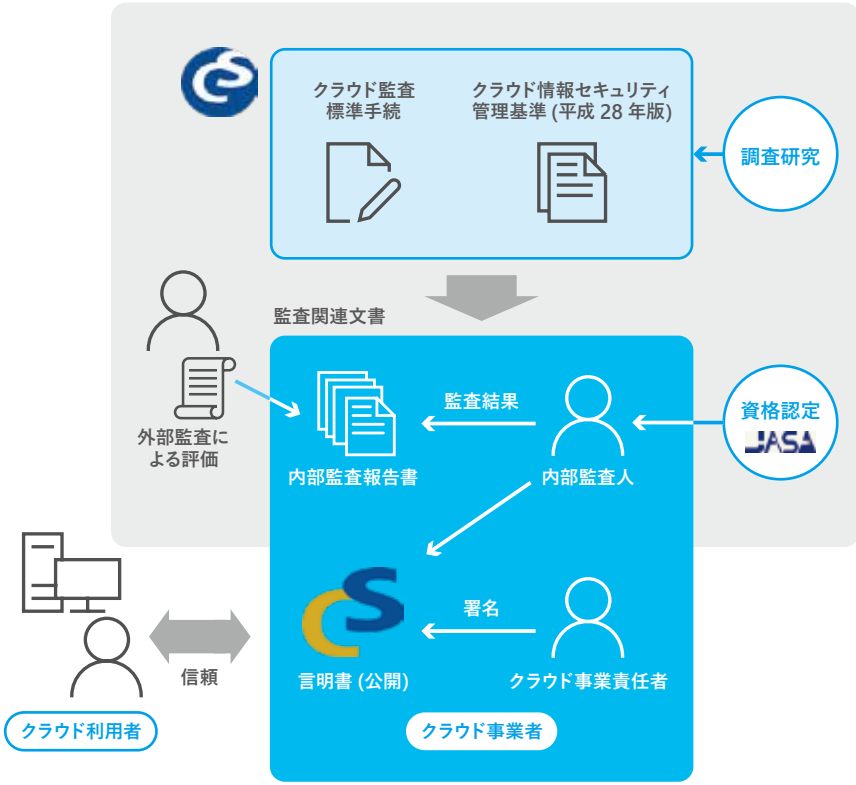
2020 年に政府のクラウド安全性評価制度が開始されます。そのベースになっているのが、経済産業省が公開している「**クラウド情報セキュリティ監査制度**」です。クラウド情報セキュリティ監査とは、標準的なサービスを多数の顧客に提供するクラウドサービスの特性を踏まえて、事業者が行うべき情報セキュリティマネジメントの基本的な要件 (基本言明要件) を定め、事業者がこれに沿って実施しているかを基準に基づき評価し、安全性が確保されていることを顧客に対して明確にする仕組みです。

基本言明要件は、経済産業省が公開している「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」に基づくクラウド情報セキュリティ管理基準で定められたものです。クラウド事業者はこの管理策を実装・運用することで、クラウドの情報セキュリティを確保します。

監査は事業者が行う内部監査と、その結果を独立した第三者が評価する外部監査に分かれます。クラウドサービスは規模が大きく、技術的に新しくかつ変化の激しいテーマであることから、クラウドの知識をもつ監査人が限られています。そこでクラウド技術者が監査の知識を習得し、内部監査を適切に行い、その監査手続について独立した外部監査人が監査して、監査結果の妥当性を評価する制度が必要となります。外部監査人が監査結果を客観的に監査することにより、内部監査の透明性を高めることで、セキュリティ対策の実効性を確保しようとするのが目的です。

クラウド情報セキュリティ監査基準による監査、認定を行い、認定を受けた事業者には「CS ゴールドマーク※7」の使用が許諾されます。

CS ゴールドマーク※7 は国際的な基準とされる Service Organization Controls (SOC) 2 と並ぶ日本初の第三者認定制度であり、**クラウドサービスの利用者は CS ゴールドマーク※4 を、導入時や年次の監査結果として利用することができます**。



※6:「クラウド情報セキュリティ監査制度」について　https://jcispa.jasa.jp/cloud_security/
※7:「CS ゴールドマーク」について　http://aka.ms/csmark

4 クラウドサービスの選定にあたって

4.4 情報セキュリティ マネジメント システムの国際規格

ISO/IEC 27001 は、情報セキュリティ マネジメント システム (ISMS) に関する国際規格です。
情報の機密性・完全性・可用性をバランスよくマネジメントし、情報を有効活用するための組織の枠組みを示しています。

4 クラウドサービスの選定にあたって

4.5 クラウドサービスにおける個人情報保護 (改正個人情報保護法との関連)

個人情報保護法ガイドライン・Q & A では、第三者提供・委託の部分でクラウドに関する言及がなされています。

① クラウドサービスの利用が、第三者提供にも委託にもあたらない場合

- クラウドサービス提供事業者において個人データを取り扱わないこととなっている場合、個人データの第三者提供や委託には該当しない。(個情法 Q & A 5-33)
- 「クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合」とは、契約条項に当該事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合など。(個情法 Q & A 5-33)
- ただし、クラウド利用事業者は、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある。(個情法 Q & A 5-34)

② クラウドサービスの利用が、委託にあたる場合

- クラウドサービス提供事業者が (顧客企業の利用目的の達成に必要な範囲内で) 個人データを取り扱う場合。
- 委託元企業には「委託先監督義務」が発生。
- 適切な委託先の選定・委託契約の締結・委託先における個人データ取扱状況の把握。
- なお、委託にあたり「第三者提供時の確認義務」は適用されない。

③ (委託ではない) 第三者提供にあたる場合

- クラウドサービス提供事業者が (顧客企業の利用目的の達成に必要な範囲を超えて) 独自の目的で利用する場合。
- 「本人の同意」「第三者提供時の確認」などの義務が発生。

※ 個人情報を取り扱うクラウドサービスを利用する場合には、ISO27018, ISO27701 などの認証を取得したサービスを採用することが望ましい。

4 クラウドサービスの選定にあたって

4.6 家族の教育の権利とプライバシー法※8 FERPA (米国) とマイクロソフトのクラウド

FERPA とは

「家族の教育の権利とプライバシー法 (FERPA)※8」は、米国教育省の基金を受けている**教育機関での学生の記録のプライバシーを保護するための法律**です。FERPA は監査やその他の認定を必要としないため、FERPA の対象となる学術機関は、クラウドサービスの使用が FERPA 要件を遵守する能力に持っているかどうか、またどのように影響するかを評価する必要があります。

マイクロソフトのコミットメント※9

マイクロソフトは FERPA のコンプライアンスを証明するため、以下の契約上のコミットメントを行っています。

- マイクロソフトは、オンラインサービス条項※10 に基づき、FERPA に基づくお客様データに「**正当な教育上の権利**」を「**学校職員**」に指定することに同意します。(顧客データには、学校による Microsoft クラウド サービスの使用を通じて提供される学生レコードが含まれます。学生教育記録を取り扱う場合、マイクロソフトは、学校関係者と同様に、34 CFR 99.33(a) によって課される制限事項と要件を遵守することに同意します。)
- さらに、マイクロソフトは、クラウド サービスと互換性のある目的 (マルウェア検出の向上など) を組織に提供するためにのみ顧客データを使用することを約束し、**広告用に顧客データを利用しません**。
- マイクロソフトは、契約に記載されているように、または法律で義務付けられている教育機関の指示を除き、**お客様のデータを開示しないこと**を契約上義務付けています。したがって、Microsoft クラウド サービスの使用を通じてマイクロソフトに教育記録を提供する学校は、これらのレコードの使用と開示に関する厳しい契約上の制限を受けることを保証できます。

これらの契約上のコミットメントの結果として、FERPA の対象となるお客様 (教育機関と機密性の高い学生データへのアクセスを提供するサード パーティの両方) は、スコープ内の Microsoft ビジネス クラウド サービスを安心して利用することができます。

※8: Family Education Rights and Privacy Act (FERPA)　https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.htm
※9: マイクロソフトの FERPA に対するコミットメント　https://docs.microsoft.com/ja-jp/microsoft-365/compliance/offering-ferpa
※10: オンラインサービス条項　http://go.microsoft.com/?linkid=9840733

4 クラウドサービスの選定にあたって

4.6 マイクロソフトが提供するクラウドサービスが取得しているコンプライアンス

マイクロソフトが提供するクラウドサービス「Microsoft Azure」、「Office 365」は **90 を超えるコンプライアンス認定資格**※10 をご利用いただけます。その中には、グローバル リージョンに加え、米国、欧州連合、ドイツ、日本、英国、インド、中国など各国に固有な 50 以上のコンプライアンス認定資格があります。さらに、医療、政府、会計、**教育**、製造、メディアなど、主要産業の必要に固有な、35 以上のコンプライアンス認証も入手できます。新たに生じるコンプライアンス要件もカバーされます。マイクロソフトは、政府、規制当局、標準化団体、非政府組織とグローバルに連携しています。

グローバル	米国の政府機関	地域 / 国に固有		業界に固有	
CIS ベンチマーク	CJIS	BIR 2012 (オランダ)	IT-Grundschutz (ドイツ)	23 NYCRR 500 (米国)	GLBA (米国)
CSA STAR 証明	CNSSI	C5 (ドイツ)	LOPD (スペイン)	AFM/DNB (オランダ)	GxP (米国)
CSA STAR 認証	DFARS	CS ゴールド マーク (日本)	MeitY (インド)	AMF/ACPR (フランス)	HIPAA (米国)
CSA STAR の自己評価	DoD L 2、4、5	Cyber Essentials Plus (米国)	MTCS Level 3 (シンガポール)	APRA (オーストラリア)	HITRUST (米国)
ISO 20000	DoE 10	DJCP (中国)	マイ ナンバー法 (日本)	CDSA	KNF (ポーランド)
ISO 22301	EAR	EN 301 549 (EU)	ニュージーランド CC Framework	CFTC 131 (米国)	MARS-E (米国)
ISO 27001	FDA CFR Title 21	ENISA IAF (EU)	PASF (UK)	DPP (UK)	MAS/ABS (シンガポール)
ISO 27017	FedRAMP	ENS (スペイン)	PIPEDA (カナダ)	EBA (EU)	MPAA (米国)
ISO 27018	FIPS 140-2	EU モデル契約条項	PDPA (アルゼンチン)	FACT (UK)	NBB/FSMA (ベルギー)
ISO 9001	IRS 1075	EU-US プライバシー シールド	TISAX (ドイツ)	FCA/PRA (UK)	NEN 7510 (オランダ)
SOC 1、2、3	ITAR	GB 18030 (中国)	TRUCS (中国)	FERPA (米国)	NHS IG (UK)
WCAG 2.0	NIST CSF	G-Cloud OFFICIAL (UK)	TruSight	FFIEC (米国)	OSFI (カナダ)
	NIST 800-171	GDPR		FINMA (スイス)	PCI DSS

※10: 取得済み認証制度について　https://azure.microsoft.com/ja-jp/overview/trusted-cloud/

4 クラウドサービスの選定にあたって

4.7 クラウドサービスの法令 (準拠法と管轄裁判所)

教育情報セキュリティポリシーに関するガイドライン (令和元年 12 月版) には、「クラウドサービスによっては、管理する情報資産やシステムについて、日本の法令が適用されないケースや、係争時における管轄裁判所が日本国外となるケースが存在し、情報資産の保全に影響することがある。クラウドサービス選択の際には、自らの情報資産の管理に日本の法令が適用されること、**係争時における管轄裁判所が日本国内となることを留意する**必要がある。」と記載されています。

クラウドサービスによっては、管理する情報資産やシステムについて、日本の法令が適用されないケースや、係争時における管轄裁判所が日本国外となるケースが存在し、情報資産の保全に影響することがあります。クラウドサービスの選択の際には、自らの情報資産管理に**日本の法令が適用される**ことに加え、係争時における**管轄裁判所が日本国内**となることが望ましいと言えます。

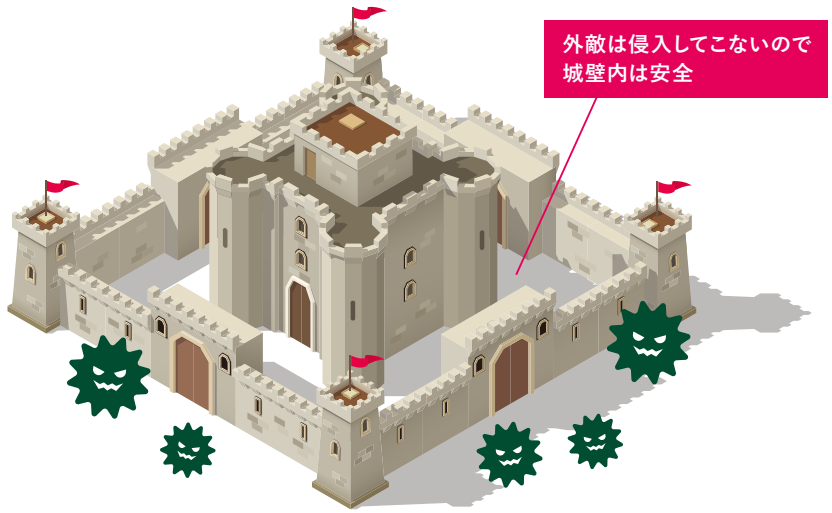
また、**外貨で決済する場合には、その時点で明示されなくても当該通貨発行国の法令が適用されます**。準拠法、管轄裁判所以外にも、支払通貨に関して留意する必要があります。

マイクロソフトが提供するクラウドサービス (Azure, Office 365, Dynamics 365 など) は、**日本円での決済**が可能です。また利用契約は**日本の法令に準拠**し、**管轄裁判所は東京地方裁判所**となります。

5 クラウドサービス利用時における情報セキュリティ対策

5.1 境界防御型 (Perimeter) セキュリティ モデルとゼロトラスト (Zero Trust) セキュリティ モデル

教育情報セキュリティポリシーに関するガイドラインに記載されている「データセンターなどを利用し、ネットワーク分離を基礎としたリスク対応イメージ (P.13)」は**境界防護型**セキュリティ モデルに基づき設計されたものでした。境界防護型セキュリティ モデルとは、守るべき情報資産は境界内部にあり、アクセスは境界内部 (と認識した範囲) からのみとして、脅威は境界外部にとどめておく (攻撃者を境界の内部に侵入させない) という考え方です。クラウドの活用が進み、デバイスを学外へ持ち出すようになると、学内のネットワークにおける学内、学外の境目はあいまいになります。ネットワークの境界線が変われば、セキュリティの境界線も変わります。学外からの侵入だけではなく、社内にも脅威は存在する ― **そう考えると、脅威を防ぐのはネットワークではなく、ID 管理を利用した論理的防御になりつつあります。**



「ゼロトラスト セキュリティ」とは、もともと Forrester Research が 2010 年に提唱した考え方で、" 社内 (ネットワーク内) は安全である " という前提に立って境界を守るやり方では守れなくなった現状を踏まえ、「信頼しないことを前提に、すべてのトラフィックを検査、ログ取得を行う」という " 性悪説 " のアプローチです。

ゼロトラスト セキュリティが提案された背景には、2010 年前後に重大なセキュリティ侵害や情報漏えいが多発したという事実があります。これは従来のセキュリティ対策では不十分である証拠として、今後のセキュリティ対策の方向性を抜本的に変える必要があったのです。

具体的には、アクセスの認証を行う際に、毎回セキュリティレベルに達しているかを検査することでセキュリティを担保します。たとえば、

- ✓ **アクセスしてくる端末は、組織でデバイス登録された端末か**
- ✓ **アンチウイルスソフトの定義ファイルは最新か**
- ✓ **端末がマルウェアに感染していないか**
- ✓ **漏えいした ID からのアクセスではないか**

といった項目を毎回自動で確認し、必要に応じてアクセス制御を行います。この仕組みは「ユーザ、パケット、インタフェース、ネットワークに対し、常に疑いを持って接する」というイメージとなっています。複雑なシステムに思えるかもしれませんが、**Microsoft 365 と Windows 10 で実現**することができます。

5 クラウドサービス利用時における情報セキュリティ対策

5.2 ゼロトラスト セキュリティ モデルで、セキュリティ防御技術はどう変わるか

下表は境界防御型セキュリティとゼロトラスト セキュリティでの違いを示しています。

境界防御型セキュリティ モデルでは、学外からの侵入を阻止するためにファイアウォール (Firewall) を設置し、学外から学内のシステムを利用する際は VPN (Virtual Private Network) を使用していました。

ゼロトラスト セキュリティ モデルでは、厳密なアクセス管理を実現するために IAM、EDR、UEGA などの対策を行う必要があります。

大項目	小項目	境界防御型	ゼロトラスト
資産	守るべき情報資産	境界内部に	境界内外部に
	利用者アクセス	境界内部から	境界内外部から
脅威	脅威・攻撃者	境界の外に留める	どこにでも
	攻撃者の初期目的	境界内に入る	なりすまし
対策	安全性のよりどころ	境界防御	厳密なアクセス管理
	安全性の確認	基本、出入り	常に
	防御のコア技術	FW・VPN	IAM・EDR・UEBA
利便性	働く環境	境界内のみ	世界中どこでも
	勤務時間	営業時間	いつでも
	企業間コラボ	考慮なし	考慮あり

ゼロトラスト セキュリティ モデルに基づくマイクロソフト製品

Azure Active Directory

IAM (Identity and Access Management)
アイデンティティ / アクセス管理

IT 環境にアクセスする際にはユーザ ID を使用します。誰がどのような役割を持ち、役割を遂行するため何にアクセスできるようにするか (あるいは、できないようにするか)、そして実際に何にアクセスしたのか――このような内容はすべて「ユーザ ID」をベースに制御・管理が行われます。

ユーザ ID は実在の人物とマッチしている必要があり、実在しない人物の ID が存在し、それが使用されている、あるいは実際の職務では扱う必要のない他部門のデータにアクセスできるといった状況では、IT 統制が取れた環境であるとは言えません。この管理を的確と行うためインフラ・基盤としてまず IAM を整備することで、IT 統制に効果が発揮されます。

Windows Defender ATP

EDR (Endpoint Detection and Response)
エンドポイントでの検出と対応

EDR とは「Endpoint Detection and Response (エンドポイントでの検出と対応)」のことです。EDR プラットフォームはエンドポイントの監視を強化するために構築され、標的型攻撃やランサムウェアなどによるサイバー攻撃を検出して対応するために使用するエンドポイント・セキュリティ・ソリューションです。

Windows Defender ATP

UEBA (User and Entity Behavior Analytics)

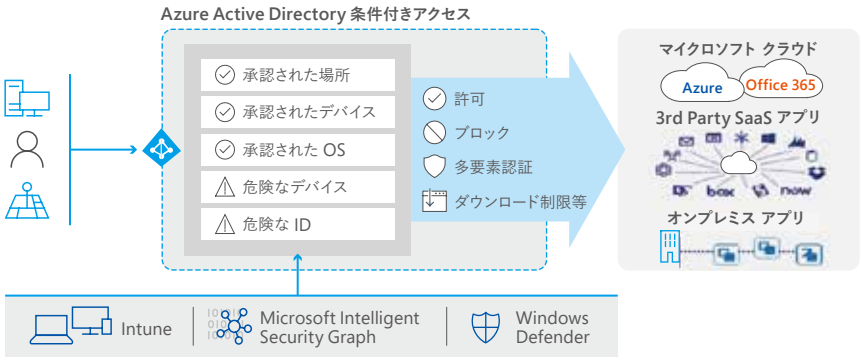
UEBA とは「User and Entity Behavior Analytics」のことで、ユーザ及びエンティティの行動分析を行い、不正な行動、リスクを早期に検知するための技術です。

5 クラウドサービス利用時における情報セキュリティ対策

5.3 Azure AD x Intune x Windows でゼロトラスト ベースを作る

ゼロトラスト ネットワークのカギになるのは **Azure AD (Active Directory)** です。通信の認証を担っており、動的なポリシーでアクセスをブロックしたり、多要素認証を要求することができます。たとえば、位置情報を加味することで「PC を学内で使っている場合はアクセスを許可、学外からのアクセスの場合は多要素認証を要求」といった、複雑な条件を自動で適用できるのです。

さまざまな条件でアプリケーションへのアクセスを制御



ネットワークへのアクセス時に、端末の状態を確認し、さまざまな情報を取得するのはモバイルデバイス管理ツール **Intune** とクラウドベースの EDR **Windows Defender ATP** の役割です。教育機関が期待するデバイスのセキュリティレベルが担保されているかどうかを監視し続けます。

Azure AD における制限付きアクセス (**Identity Protection**) 機能は、従来は IP アドレスのホワイトリストやブラックリストを使って運用する形でしたが、ゼロトラスト ネットワークでは動的なポリシーが重要です。

異常なアクセスを判断する根拠には、さまざまなものがあります。たとえば東京からアクセスした数秒後にシドニーからのアクセスが検知された場合や、Tor ブラウザ (匿名の IP アドレス) からのアクセスがあった場合は異常な通信と判断し、ポリシーが適用され、自動でアクセスコントロールを変更します。

マイクロソフトの製品がこのように高いセキュリティ性能を発揮できる理由は、世界中のあらゆる情報を多くの専門家が分析した知見と、そのデータを活用した AI や機械学習による予測などを掛け合わせ、非常に高度かつ大量のインテリジェンスをリアルタイムにフィードバックしているためです。

架空の URL などを埋め込むことで情報を搾取するビジネスメール詐欺やフィッシングメールなども、これらの取り組みにより大幅な被害軽減を実現しています。

したがって、利用者の方々が専門的な情報収集などを行わなくとも、**最新のセキュリティ対策が自動で施されている環境**を構築できるようになっているのです。

Azure AD はどのようにリスクを検出するか

リスクイベントとリスクの高い ID の検出方法：機械学習とヒューリスティック規則を使用して、6 種類のリスクイベントを検出

リスクイベントの種類	イベントの内容	重要度
漏洩した資格情報	悪質な Web で公開された Azure AD の資格情報を“漏洩した資格情報”として報告	高
特殊な場所へのあり得ない移動	地理的に離れた場所で短時間で発生したサインイン (学習された VPN や場所を除く) を報告	中
感染しているデバイスからのサインイン	Bot サーバーと頻繁に通信しているデバイス (IP アドレス) からのサインインを報告	低
匿名の IP アドレスからのサインイン	匿名プロシキ (Tor など) として識別される IP アドレスからのサインインを報告	中
不審なアクティビティのある IP アドレスからのサインイン	短期間に複数アカウントで多数のサインイン失敗が検出された IP アドレスからのサインインを報告	中
未知の場所からのサインイン	機械学習された過去のサインインの場所から離れた場所からのサインインを報告	中

5 クラウドサービス利用時における情報セキュリティ対策

5.4 多層防御

2016 年 11 月に IPA (情報処理推進機構) は、米国土安全保障省 (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) 発行の "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies" の概訳「**多層防御による制御システムセキュリティの強化概要**」※11 を公開しました。

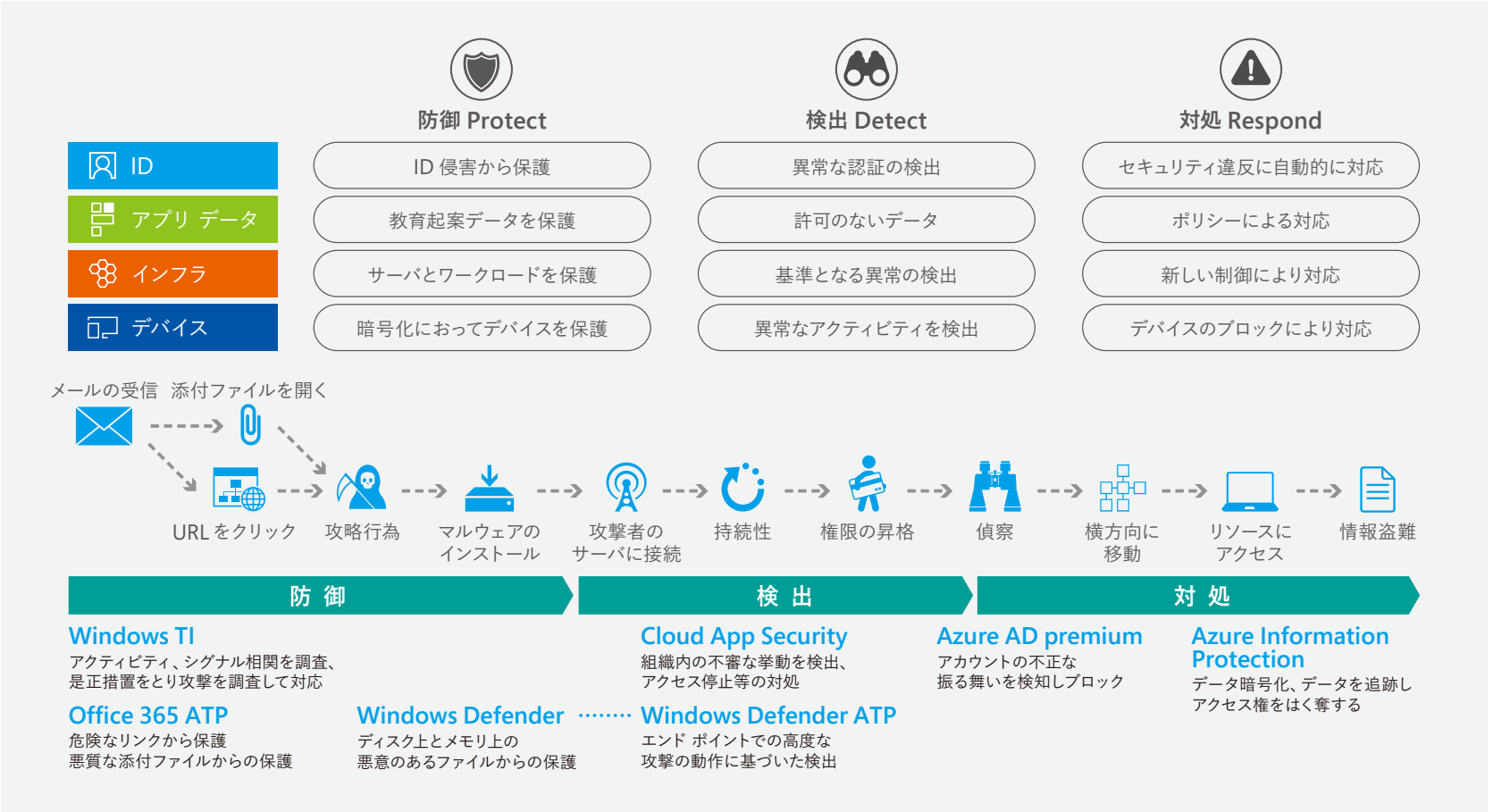
セキュリティ対策における「**多層防御**」とは、セキュリティ対策を組み合わせて階層 (レイヤー) を築くことで、1 つの対策が破られても次の (またその次の) 対策が攻撃を抑止し、重要部への侵入前に攻撃の検知および対応ができるようにする、リスクベースの総合的なセキュリティアプローチです。「**多層防御**」は「**ゼロトラスト セキュリティ**」とともに、今後セキュリティ対策を行っていく上での重要な概念です。

※11: https://www.ipa.go.jp/files/000055601.pdf

5 クラウドサービス利用時における情報セキュリティ対策

5.5 マイクロソフトのソリューションでどのように多層防護が実現できるのか

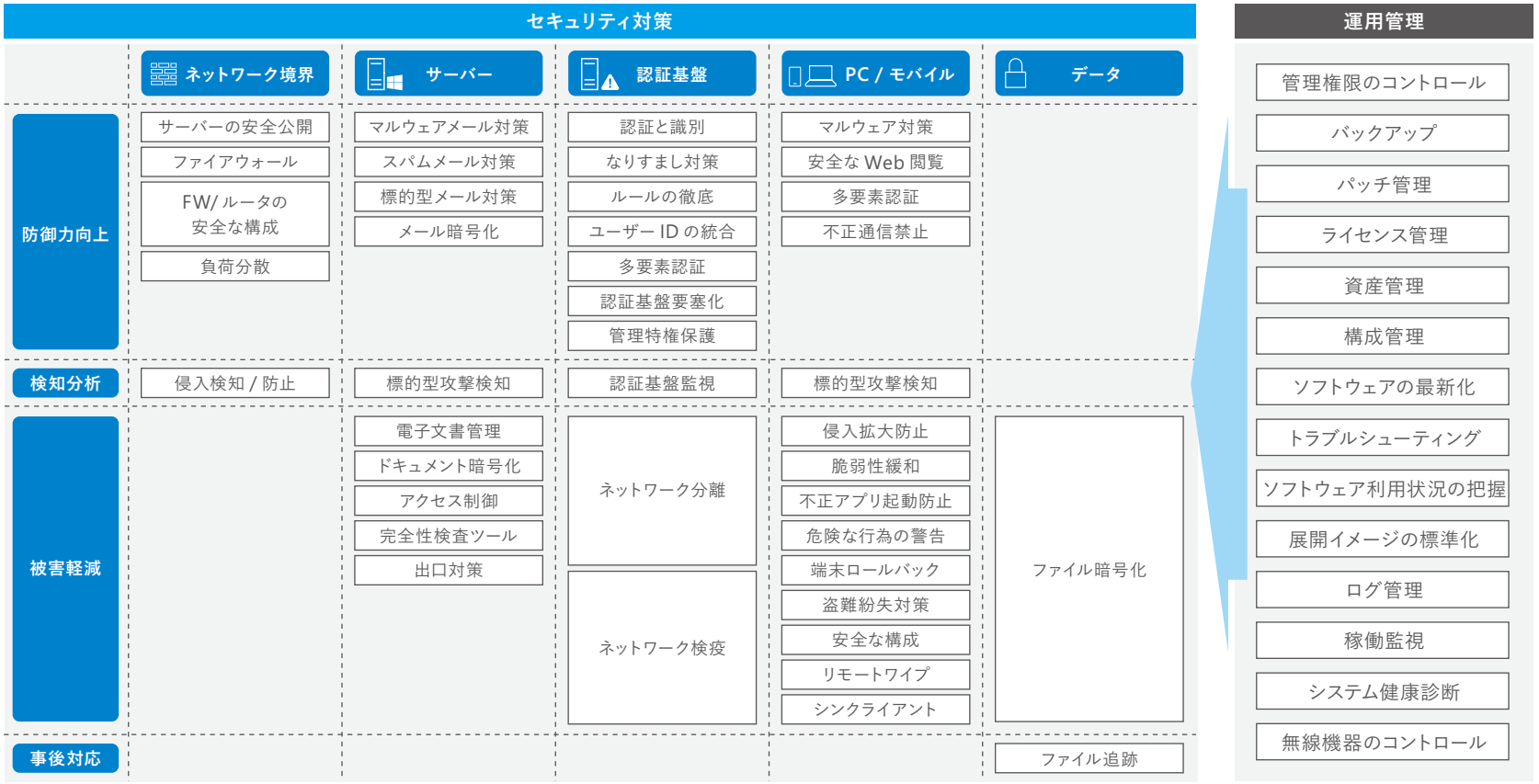
マイクロソフトではそれぞれの階層において対応するソリューションを用意しています。



5 クラウドサービス利用時における情報セキュリティ対策

5.6 マイクロソフト製品によるセキュリティ対策

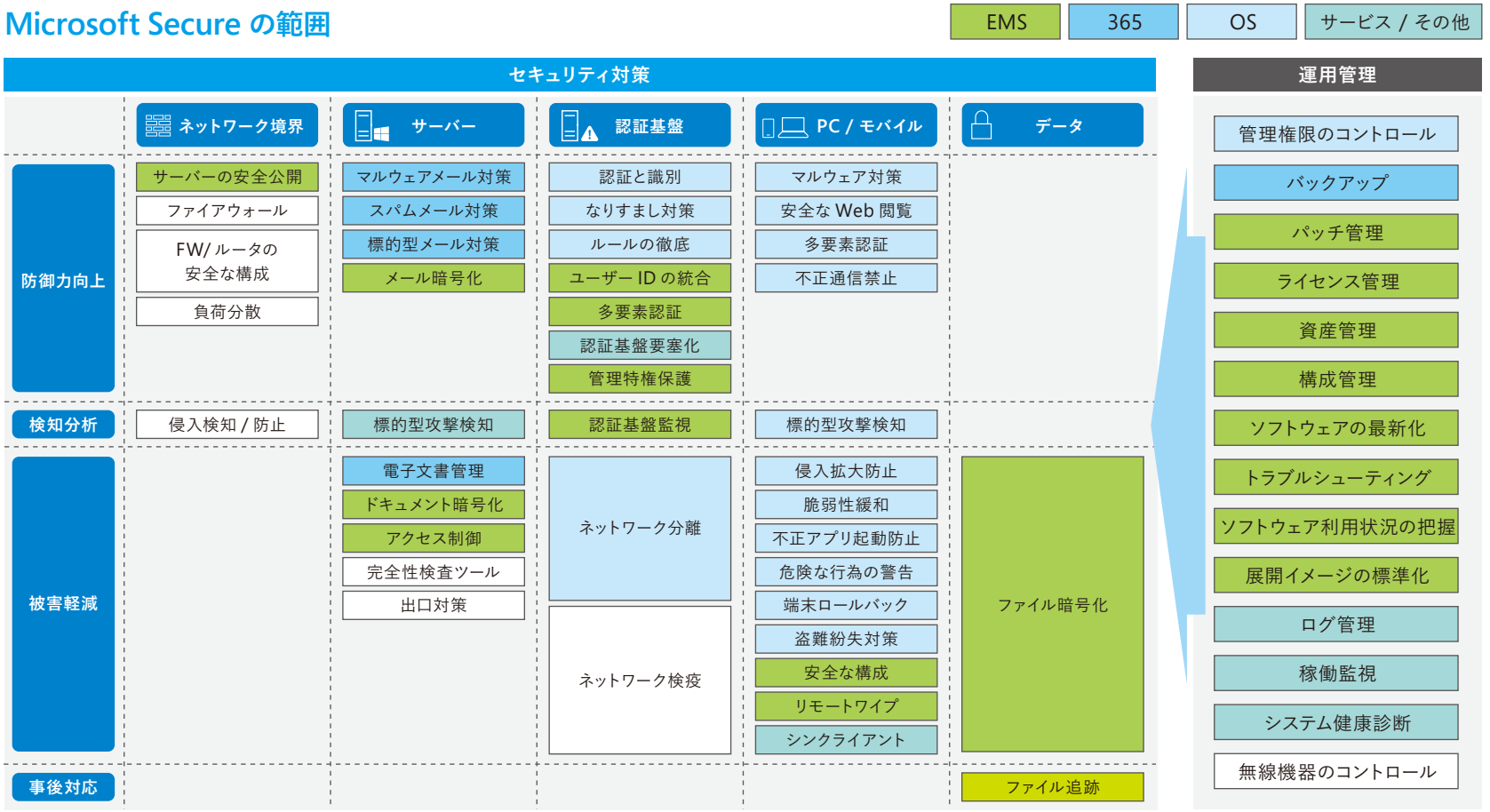
下図は SAMS:20 Critical Security Controls <https://www.sans.org/critical-security-controls/> と
IPA の情報セキュリティ教本 <https://www.ipa.go.jp/security/publications/kyohon2/index.html> を参考に作成した代表的なセキュリティ対策です。



5 クラウドサービス利用時における情報セキュリティ対策

5.6 マイクロソフト製品によるセキュリティ対策

マイクロソフトの製品およびサービスを利用して、以下の範囲の対策を実施することが可能です。



本リーフレットついてのお問い合わせ

本リーフレットに記載された情報は制作当時 (2020 年 1 月) のものであり、閲覧される時点では、変更されている可能性があることをご了承ください。
本リーフレットは情報提供のみを目的としています。Microsoft は、明示的または暗示的を問わず、本書にいかなる保証も与えるものではありません。
製品に関するお問い合わせは次のインフォメーションをご利用ください。
■インターネット ホームページ https://www.microsoft.com/ja-jp/
■マイクロソフト カスタマー インフォメーションセンター 0120-41-6755 (9:00 ～ 17:30 土日祝日、弊社指定休業日を除く)
※電話番号のおかけ間違いにご注意ください。

＊製品の仕様は、予告なく変更することがあります。予めご了承ください。

Microsoft
日本マイクロソフト株式会社
〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー

6300-IP1