学校現場を変えていくゼロトラストセキュリティ
――高校教師から転職したIT企業社員から――

栗原太郎　Taro Kurihara　日本マイクロソフト株式会社

1 ゼロトラストへのいざない

GIGAスクール構想が前倒しになり，ICT環境の整備が進められてきた．一人1台端末によって個別最適化された創造性を育む教育を目指す夢のような政策であるが，徐々に既存の環境とのひずみが見えてくるようになった．平成29年に策定された文部科学省の「教育情報セキュリティポリシーに関するガイドライン」[(1)]は，従来のパソコン教室からクラウド基盤の一人1台活用といった，いわゆる令和時代のスタンダードなICT環境に対応するために大幅に改訂が進んでいる．令和4年3月における第3回目の改訂では，新しいICT環境の目玉として位置付けられているゼロトラストセキュリティの対策をより具体的に記すこととなった．最近ではゼロトラスト基盤を採用する学校が増えており，自治体規模でも導入が進んでいる．更に文部科学省自身もこの仕組みを採用し，中央省庁として初めてフルクラウド基盤のシステムをマイクロソフトのクラウドサービスで構築した．教育現場では一人1台端末の整備が終わったが，今までのICT環境が根本から変わっていく，まさに過渡期の状況にある．

ゼロトラストという言葉は本マガジンのテレワーク小特集で登場しており[(2)]，以前よりも多くの人に知られるようになっている．今回は可能な限り技術の詳細は省き，学校というものを題材に，テクノロジーがどのように人々の生活を変えていくかを言語化することに終始したい．技術に関心がある読者にとっては，時に技術そのもの以上に重要度が高いものだと感じている．これは私のようなIT企業の人間が得意としていない領域であり，自戒の念も込めて進めていきたい．

現在私は，日本マイクロソフトにおいて全国の教育機関向けのカスタマーサクセスを担当している．余りなじみのない役職だが，IT企業では広く取り入れられており，年々需要が高まっている領域である．簡単に言うと買って頂いて終わりではなく，購入後いかに使って頂くかに注力する仕事だ．この説明をするとICTの基本的な使い方研修を行う人のイメージを持たれることが多いが，使う際に障壁となる技術的な課題を解決することを主な仕事としているため，当社での役割は技術者である．一方で，新しいものの導入に消極的な組織文化をどう変えていくかといった，技術が一切関係ない領域も担当する．もちろん前述の使い方の講義もする，言わば「何でも屋」である．

そんな技術職として働いている私は，2020年3月まで高校倫理の教員をしており，古代ギリシア哲学好きでICTとは無縁の世界に生きていた．働いていた頃はまさに大学入試制度の変わり目であり，従来の学びを先生の働き方とともに改革していく必要があった．そこでICTの可能性に気づき，全国に先駆けてゼロトラストの仕組みを先生たちと構築して学校を変えていった．聞こえはいいが，学校が抱える課題を解決するような理想的なICT環境を求めて奮闘する中で，「Microsoft 365 A5」（図1,2）と呼ばれる「全部入り製品」の機能に目を通して，一つ一つ有効化していったら，たまたまゼロトラストに基づく仕組みになっていたというだけである．新しい環境では今までとは比べられないほど利便性と安全性を高めることができ，効率化と質の向上につながった．この後ICTによって学校現場を変えたいと思い転職を決意したが，基盤としてのゼロトラストは学校を変えていく大きな希望であると思っている．

2 ゼロトラストの広がりと理由

詳しい話はほかに譲るとしてここでは概略について書いていく．ゼロトラストとはセキュリティに関する考え方であり，信じること（トラスト）をしない（ゼロ）ことを前提として作られたモデルである．これに対して従来の境界型セキュリティと呼ばれる対策は，信頼でき

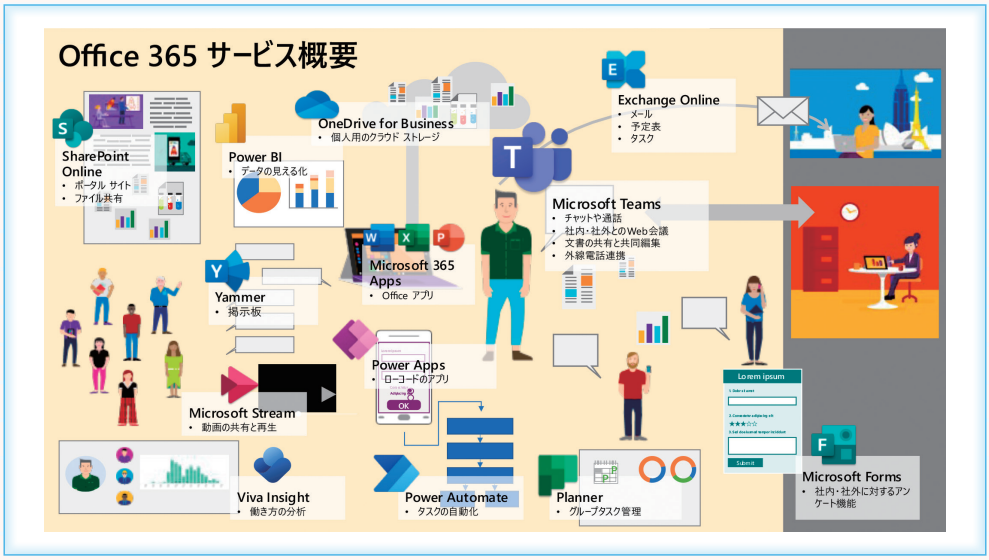

図 1　Microsoft 365 A5 サービス概要 Office 365 編

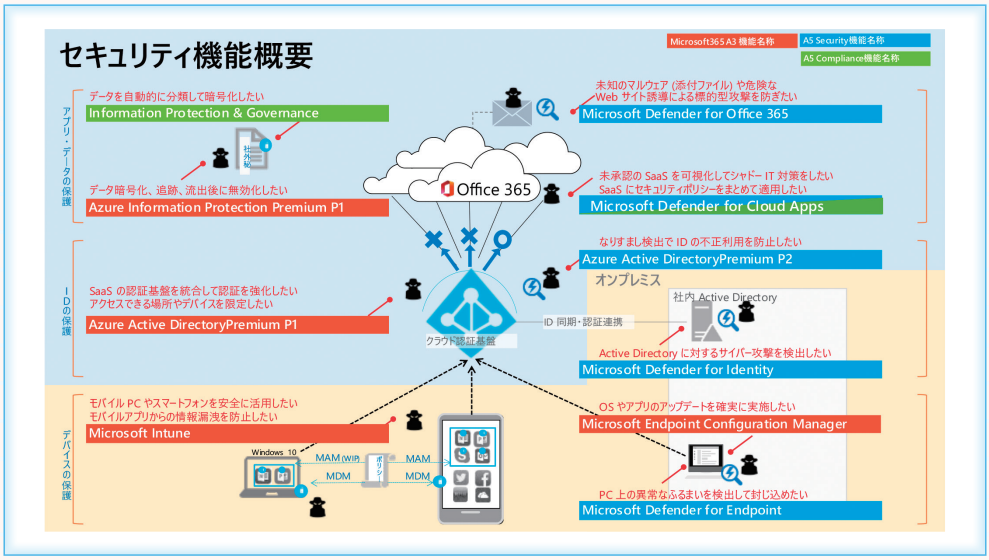

図 2　Microsoft 365 A5 サービス概要 セキュリティ機能編

る領域（トラストゾーン）を作り，出入り口の対策を行うことで，内的，外的脅威から組織の資産を守っていく仕組みである．極端な企業を例にすると，顧客情報は社内に閉じたオンプレミス（自社運用）サーバにあり，社内のデスクトップ PC からしか閲覧できない．USB を挿入するとアラートが鳴り，クラウドサービスへのアクセスもネットワークから制限されている．少し前まではなじみのあるシステムであったが，なぜ新しいものに転換する必要があったのだろうか．幾つか理由はあるが代表的なものを見ていこう．

第 1 の理由はより高度なセキュリティ対策が必要になったということである．境界型セキュリティはトラストゾーンを突破されないことを前提としているが，近年の巧妙な手口によるサイバー攻撃では，トラストゾーンをすり抜ける事例が出ており，不正侵入，情報流出に関して名だたる企業のセキュリティ事故がニュースになるのも日常的になってきた．最大の原因となるのは従来のトラストゾーンの相対的な縮小である．今まではメール・ファイルサーバ，デスクトップ PC 等々，会社内部の限られた領域だけでシステムが完結していた．近年のクラウドサービスや持ち運び端末の普及によって，本来守るべき領域が拡大し，出入り口となり得る点も増えることで今までの仕組みでは対応できなくなってしまった（図 3）．ゼロトラストの仕組みでは ID を軸に，データ，端末，アプリそれぞれを守っていくことでトラストゾーンに依存せずにセキュリティを担保できる．また，境界型セキュリティの弱点である，突破された後の対策が充実していることも忘れてはいけない．たとえ侵入された後でも検知，ブロック，対処の一連の作業を自動で行うことに強みがある．更にはクラウドに蓄積された脅威に関するデータと AI の分析技術の発展によって，今までの対策の基本となっていた既知の脅威だけでなく，未知

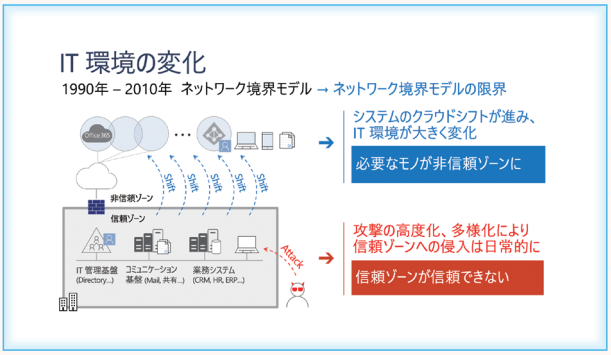

図３　IT 環境の変化

の脅威に対策を施すことも可能となった．

ゼロトラストへの転換が進んだ第２の理由として，外部からでも仕事ができる環境が必要になったということだ．テレワークは働き方改革の一環として少しずつ進んでいたが，コロナ禍では出社せずに仕事ができる環境が求められ，整備が急速に進んだ．事前にテレワークができる環境を整備している企業もあったが，大人数の外部からの一斉アクセスといった想定外の事態には対応できなかった．ネットワークがパンクし，「遅い・重たい・つながらない」といった VPN（仮想プライベートネットワーク）渋滞と呼ばれる問題が起きた（図 4）．緊急事態宣言下においては渋滞を避けるため，部署ごとに働く時間を決めて働くことを行う企業が少なくはなかった．一方でネットワークに依存しないゼロトラストの仕組みはテレワークとの相性も良く，コロナ禍では脱 VPN の対策としてその知名度を上げることになった（図 5）．

いずれの理由もそれ以外に選択肢のない消極的な理由であり，「うちは会社に出社するから関係ないよ」と断言している人を説得するのは難しい．もう少し積極的

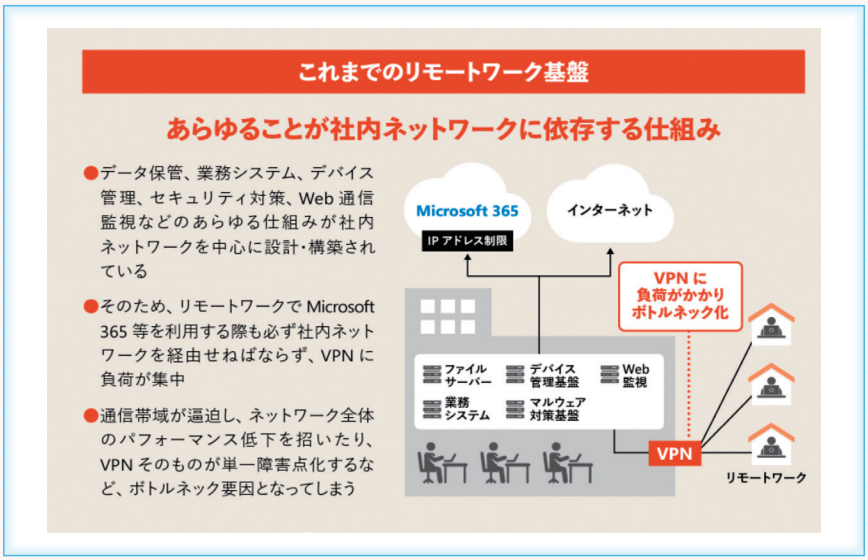

図４　これまでのリモートワーク基盤

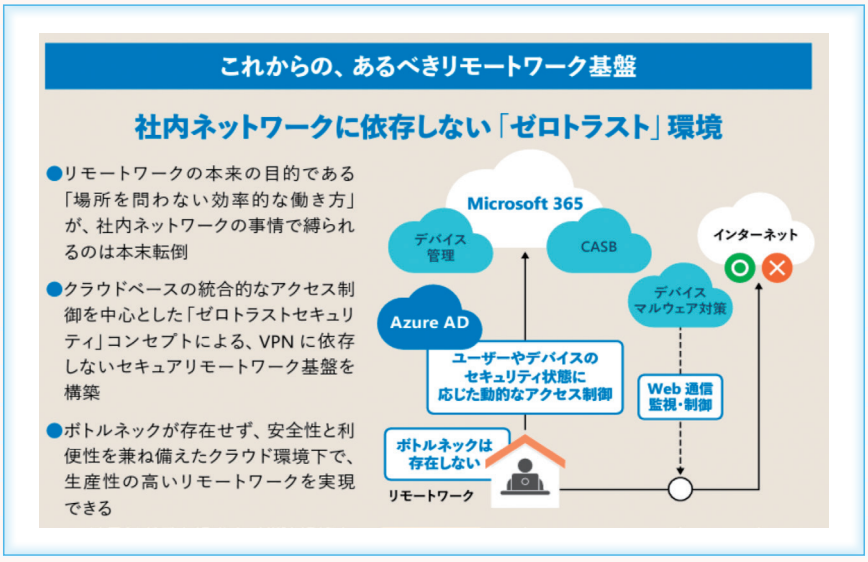

図５　これからの，あるべきリモートワーク基盤

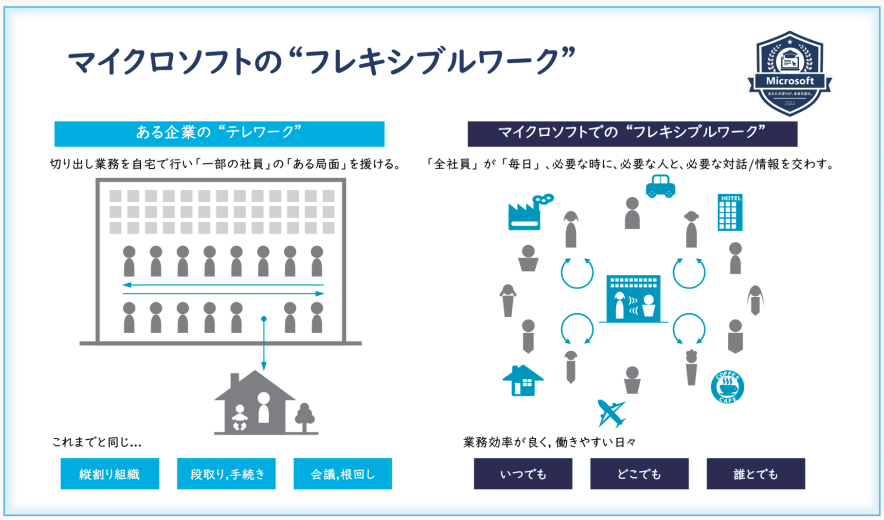

図６　テレワークとフレキシブルワークの違いについて

な意味を考えていきたい．マイクロソフトではコロナ以前から，出社してもしなくても仕事ができる環境になっていた．ただし，テレワークとは呼ばず（誰が見てもテレワークである），フレキシブルワークといった，大層な名前を付けている（図 6）．マイクロソフトの言い分はこうだ．テレワークはある一部の社員がある局面において，一部の仕事を切り出して行うものであり，フレキシブルワークは全社員がいつでも，どこでも，誰とでも仕事ができる仕組みである．マイクロソフトはフレキシブルワークによって，効率良く仕事をするだけでなく，組織や時間，場所を超えてコミュニケーションが起こり，創造性のある仕事ができている．そしてそれを支えているものがゼロトラストセキュリティというストーリーだ．理想的な「いかにも」な話ではあるが，実際に学校と企業で身をもってゼロトラスト環境を体験している私にはしっくりきている．ただし，体感するまでこのメリットを感じにくいものである．実際に学校で導入時に説明しても納得してもらえなかったが，変化した後では先生たちに「前の環境には絶対戻れない」とまで言われた．今回は諦めずに可能な限り言語化していきたいと思う．その上でまずは学校の現状の問題点について見ていく．

3　学校における ICT 環境と課題

境界型セキュリティを採用している学校を見ていく．大きく分けると学習系と校務系の２系統のシステムがある．正確には３系統であるが，少しややこしくなるので今回は２系統にさせて頂く．学習系は授業で使用するものであり，従来のパソコン教室はここに該当する．GIGA スクール構想は学習系の端末を子供たちが一人１台使えるようにした政策である．対する校務系は先生が機密情報を扱うシステムであり，具体的には子供

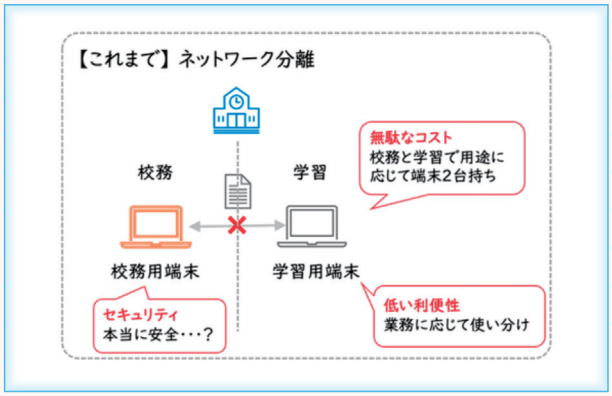

図７　これまでの学校の ICT 環境

たちの成績情報を含んだ様々な個人情報を取り扱う．学習と校務は両者行き来できないようになっている（図 7）．校務系を第 1，学習系と校務系を含んだ学校内と外とを分ける境界を第２のトラストゾーンとした二重構造になっている．先生たちの間では，学習系と校務系の分離である第 1 の境界の意識の方が強い傾向にあると感じている．決して外部に情報が流出することを軽視しているわけではなく，絶対に機密情報を見せてはいけない子供という存在がすぐそばにいるからである．そんな中，職員室と教室を絶えず行き来し，子供たちと接している．境界と外的脅威が学校内にあるという極めて不思議な構造になっている．

GIGA スクール構想で子供たちに一人 1 台の端末が行き届いた．では，先生たちの端末はどうなっているのか．例外はあるが，成績処理等で使う校務端末は GIGA 以前に先生に一人 1 台整備されていた．通常は職員室にあり，持出しができない状況になっている．学習系端末は GIGA スクール構想のタイミングで先生一人 1 台整備が行われたが，必ずしも全ての先生に行き届いているわけではなく，特に教員に助言を与え指導する立場の

指導主事や，授業を行う講師の先生といった関係者に渡っていないことが少なくはない．つまり自治体によって差があるものの，環境が良いとされているのは学習系と校務系端末を２台持っているところである．ここからはこの良いと言われている環境の問題点を見ていく．

２台持ちであることの最大のデメリットは単純に不便であるということである．セキュリティレベルや用途の異なる２台の端末を各々が管理し，使い分けることは我々のようなICTにたけている企業であっても難しく，学校現場ではどちらかが活用されない状況になっている．では，授業で使う学習端末と成績処理等の機密情報が入った校務端末のどちらを使うか．実は授業時間が多くを占める先生たちが使うのは校務系端末である．学習系端末を使わないことの最大の理由は，ICTを使わざるを得ない必須業務が入っていないことであろう．成績処理や通知表はパソコンなしでは仕事にならないが，授業は黒板とチョークがあれば成り立つし，今までも成り立っていた．どちらか一方を選ぶとなると校務系を使うことになる．

人の手で業務を分類することが困難であることも，学習系が使われない理由の一つである．実際に先生の業務において，個人情報が含まれないものを探す方が難しく，学習系端末で使用できるように情報を適切に分類する前に，使うことを諦める流れの方が自然である．例えば，保護者向けに学級便りを作成した場合，連絡事項だけであれば個人情報を含まないが，子供が何かの大会で表彰されたことを報告するものであれば個人情報が含まれる．つまり状況や使う人によって，同じ学級便りでも分類する必要があり，使うことのハードルを上げている．

学習系本来の役割である授業での利用だけに限定しても，個人情報が障壁になっている．子供たちの名前と学習の成果物のセットを個人情報とみなすため，個人を特定できないようにしている自治体も多い．アカウントの表示名を数字にし，誰が誰かをあえて判別できなくしている．そんな中，先生は表示名と名前がセットになった名簿を印刷し，アカウントと照らし合わせながら授業で使っている．このような状況では日常活用する方がかえって負担になるため，活用は進まない．教員のスキル不足によって授業でのICT活用が進まないとされているが，使われない裏にはこういったこともあることを是非知って頂きたい．

この状況下では先生たちのセキュリティに対する不安は高まるばかりである．セキュリティに対する不安は二つの点で更にICT活用を停滞させる．一つ目は使う人の心理的なハードルを上げることだ．「安全じゃないかもしれない」といった考えが学校現場に与える影響は計り知れない．活用の停滞だけでなく，そんな中でも使おうとICTを推進しようとする先生とそのほかの先生の分断を加速させ，意図しない対立を生み現場を更に疲弊させている．二つ目は利便性を下げることだ．従来のセキュリティでは様々な制限を行うことが有効な対策だと考えられていたため，ルールで縛り，多くの機能を制限していた．情報が流出しないよう端末を職員室から持ち出せないようにしよう．危険なアプリは勝手に入れられないようにしよう．端末において，検索アプリだけしか許可していないケースもいまだに多い．活用停滞だけならまだしも，逆に危険性を高めている場合もある．セキュリティを高めようと設定したルールや機能面での制限によって，幾つもの抜け穴が使われるようになった(図８)．

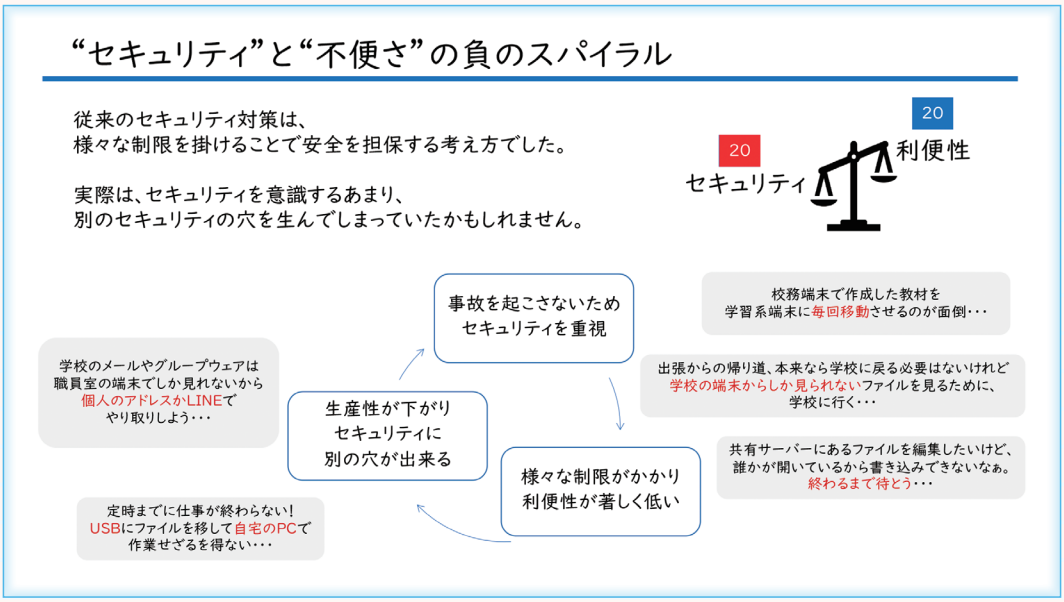

図８　セキュリティと不便さの負のスパイラル

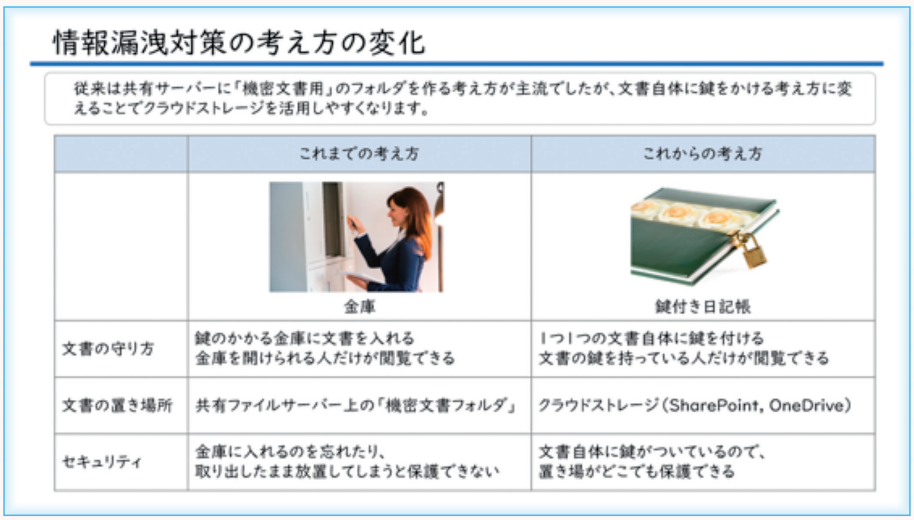

図９　情報漏えい対策の考え方の変化

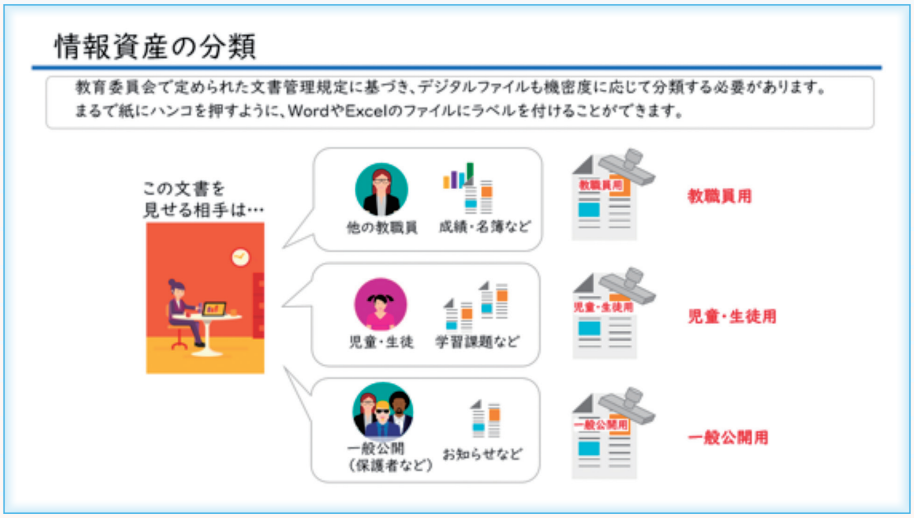

図 10　情報資産の分類

4　ゼロトラストで守られる学校

学校が境界型セキュリティで分離している理由の一つは，校務の情報が子供に渡ってしまう情報流出を避けるためである．そして分離の環境は先生たちに理解されやすい．基本的には紙と同じだからである．例えば成績情報が書かれた紙があったとする．安全のため教員は職員室でしかその紙を取り扱ってはいけない．成績処理期間中は教員以外を職員室には入れてはいけない．処理後は管理職しか開けられない金庫に入れ，施錠する．紙での重要情報を職員室という特定の領域の中で守っており，「職員室」と「その他」という教員の方々が持っている物理的なセキュリティ意識と親和性が高いため広く浸透し，逆に新しいセキュリティの考え方が浸透しにくい要因になっている．

ゼロトラストでこの課題をどう解決されるか．成績情報の書かれた「紙」を例に考えてみる．今回はこの「紙」を使用できる場所は限定しない．校内・校外問わずいつでもどこでも取り扱って構わない．うっかり教室に置き忘れてしまった場合はどうなるのか．生徒が「紙」を読もうとしたら，読めないように「黒塗り」になる．先生が「紙」を回収しに来るとまた読めるようになる．まるで魔法のような世界だが，現在の技術ならこのようなことが容易にできる．本物の紙は金庫に入れて守るしかないが，最新の技術を使った「紙」は，誰に見られているかを自分で理解し，見てはならない人に対しては情報を隠すのだ．金庫の外に出しても，自分で自分を守る「紙」だと言える（図 9,10）．これはマイクロソフトの製品で言えば Azure Information Protection と呼ばれる機能であり，ファイルをスキャンし，自動で分類，暗号化し，適切な権限を持つ人しか開けないようにするものである．情報流出対策のコンプライアンス製品に該当するものであり，人が行うこと全てを疑った性悪説を基に作られているため，今まで防げなかったものへの対策がで

きる．元々は悪意のある内部ユーザ対策であり，故意の情報流出を防ぐために作られていた．内部情報を高額で売ることや，転職のための「お土産」にしようとする悪意のある内部犯をいかに防ぐかに焦点を合わせている．学校のように先生が気をつければ防げるだろうといった，性善説を基に作られた仕組みとは対策のレベルが根本から異なる．

前述したアカウントの表示名を分からなくし，個人を特定できないように対策しているケースはどのように解決されるのか．状況に応じて自動で身分確認のレベルを変えていくことが有効だとされている．ガイドラインにも書かれているリスクベース認証と呼ばれるこの仕組みは，膨大なデータと機械学習によって（図 11），本人が普段しないような怪しい振舞いを検知して対処する．例えば，学校でログインした 5 分後に，遠く離れた海外から不正アクセスが起きたときはどうなるのか．この場合はシステムが本人ではないと判断し，ブロックや本人確認のための多要素認証を要求する．これは利用者の普段の振舞い，場所，端末や時間，様々な要素を分析することで，いつもとは違う動きを検知して，たとえ ID とパスワードが一致していたとしても本人かどうかを確認する仕組みである．しかも，怪しい振舞いがあったときのみ，詳細に確認されるため，利用者の利便性を下げない（図 12）．怪しい振舞いを検知する仕組みはマイクロソフトの様々な領域で共通して実装されている機能である．例えば，端末がマルウェア等に感染したときには通常と違う動きを検知し，ネットワークから分断し，自動で対処する EDR 機能がある（図 13）．これは普段から端末の利用状況を取得し分析することで，今まで対処ができなかった未知の脅威に対しての対策にもなる．

5　ゼロトラストで変容する学校

いずれの対策も高度に自動化されており，利用者側はセキュリティを意識することなく利用できる．この意識しないセキュリティによって先生や子供たちは様々な制

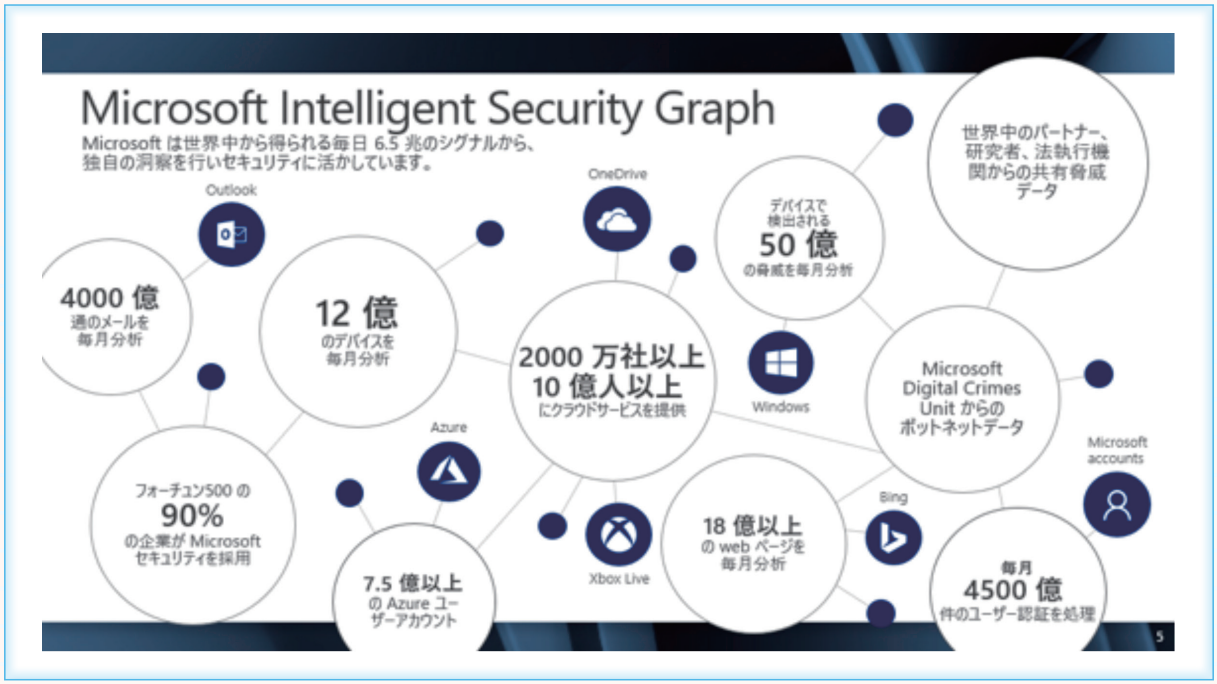

図 11　Microsoft Intelligent Security Graph

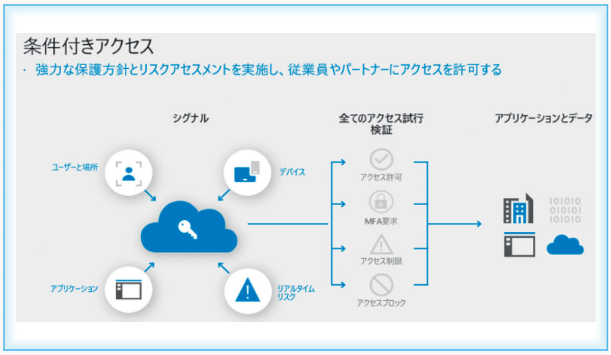

図 12　ID を保護するための機能

図 13　Microsoft Defender for Endpoint（EDR）

図 14　事例：聖徳大学附属取手聖徳女子中学校・高等学校事例

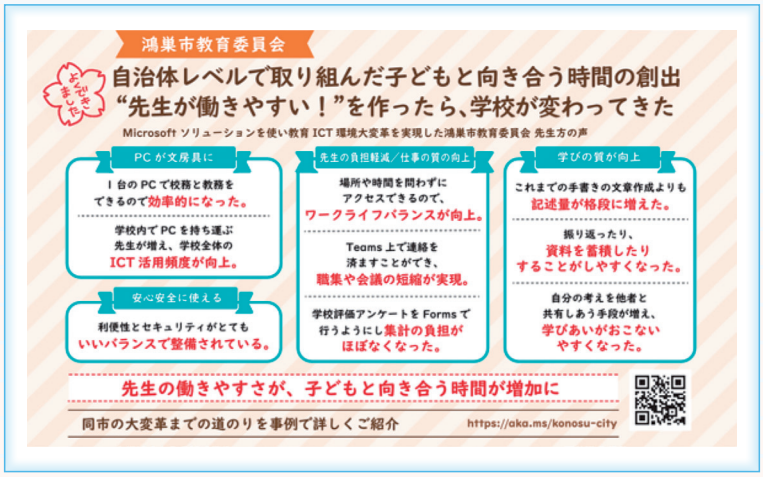

図 15　事例：埼玉県鴻巣市教育委員会

約から解放され，学校現場は大きく変化する．「アプリが使えない」「端末が動かない」「ネットが遅い」といった機能的な制約から生じる声は，機器に制限や負荷を掛けずに安全性を高めることができるこの仕組みでなくなる．また，先生が使う端末を学習用・校務用に分け，費用の面から低品質の端末を導入せざるを得ない金銭的な制約から生じる問題も解決できる．端末を 1 台にすることで，低コストでより性能の高い端末を購入することが可能になり，同様に今まで必要だった機能制約を掛けるための様々なハードやソフトウェアの導入・保守・更新費用が不要になるので，その分も含めて経済的であると言える．

何よりも大きいのは先生の働き方に対する制約がなくなることである．「いつでも・どこでも・どんな端末でも」仕事ができることの効果は，何も今回のコロナ禍のような自宅からの遠隔授業のみに限定されない．自分の生産性が上がる環境を選択できることは学校現場にこそ必要なものである．そもそも教員は授業，部活，出張など 1 か所にとどまらない上，職員室外での仕事が勤務時間の大半を占めている．そんな中，職員室の校務 PC といった限定的な場所・時間・端末でしか ICT が利用できない状況では，当然生産性も低くなる．この環境ではどこかで無理が生じ，情報事故等のミスが起きてしまう．そのことで更に制約が増え，生産性が低くなるという悪循環に陥っている．

私自身が以前勤めていた学校では，この意識しないセキュリティによって様々な制約を撤廃し，多様な働き方を選択できる仕組みを整えていった（図 14，15）．先生たちの生産性が上がり，ワークライフバランスが良くなるだけでなく，全体の労働時間も減った．端末ごとに情報を分類する必要がなくなったことで，子供たちの情報を円滑に共有できるようになった．授業と校務のデータにおける分断がなくなることで，子供たちの学習と評価が連携でき，子供たちの成長につながるような ICT 活用へと発展していった．プログラミング知識のない先生たちがローコードツールを活用し，保護者からの欠席

連絡や日程調整，申請業務といったあらゆる業務を自動化していった．セキュリティの意識という制約がないだけで，ICT を様々なことに応用していく先生たちの姿には驚くばかりであった．こういった学校の変化を見ていくと，「何のためのセキュリティ？」といった，そもそものセキュリティの意義を改めて問い直す必要性を感じる．「制限することこそセキュリティだ」という従来の方針から，「人々の力を最大限解放するためのセキュリティ」へと考え方の転換が求められているのではないか．今まで生じていた安全性か利便性かといった二項対立を乗り越える技術は十分にある．ゼロトラストには学校現場を大きく変えていく力があると信じている．

6 終わりに

ゼロトラストの良さは「いつでも，どこでも，誰とでも」どんな端末やアプリであっても自由に働くことができ，従業員の選択肢を潰さないことにある．知らず知らずに生じていた，見えない制約から解放され，ICT の可能性は今まで以上に広がっていく．ただし，私自身としてはあくまでゼロトラストを体験した後に，振り返ってみてようやく分かることが多かった．当時はフレキシブルワークといったことは余り考えてはおらず，子育て世代の先生たちをテレワークによって救いたいと必死にもがいていた程度であった．本稿では学校現場が最低限のスタートラインに立っていないような書き方をしてしまったかもしれないが，これはあくまで外部から状況を見たから分かることである．当事者にはそういった意識はない上，私自身にも今ほどはなかった．今回は教育以外の業界の人にも何か参考になればという思いで書いた．教育業界が少し特殊な状況に写ったかもしれないが，どこの業界でも多かれ少なかれ要素は含んでいると考えている．これを読んだ人が少しでも何かの参考になり，より良い状況で仕事や学びができることを願っている．

■文献

(1) 文部科学省，“「教育情報セキュリティポリシーに関するガイドライン」公表について，” March 2022. https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm
(2) 市瀬幸雄，高橋静香，大谷佳裕，“テレワーク時代のセキュリティ――ペリメタモデルからゼロトラストモデルへ――，” 信学通誌 , vol. 14, no. 4, pp. 315-322, March 2021.

栗原太郎

日本マイクロソフト株式会社文教営業統括本部カスタマーサクセスマネージャー／元高校教員．活用促進のスペシャリストとして学校現場の ICT 化に従事．先生と児童・生徒目線を大切にしながら，全国の様々な教育委員会と学校現場に ICT を使った教育改革の実現を目指した活動をサポート．慶大・法・政治卒．聖徳大学附属取手聖徳女子中学校・高等学校教諭（倫理），日本ヒューレット・パッカード株式会社 IT コンサルタント（製造業）を経て 2020 から現職．