令和６年４月　教育委員提案

教職員用端末の一元化について

戸田市教育委員会
教　育　総　務　課

ネットワーク一元化実施前（令和５年度夏まで）

○ネットワーク一元化実施前

校務系端末（870台＋デスクトップ18台、出退勤用18台）　＋　学習系タブレット（680台）　＝　合計1,586台



令和5年度の夏までは教育ネットワーク（Edu-net）は業務の性質に応じ、「校務系※1」と「学習系※2」の二つのネットワークに分離して運用。この仕組は平成27年の日本年金機構に対する不正アクセスに端を発した政府全体のセキュリティ対策を踏まえたもので、ネットワーク間のデータの閲覧や受け渡しを制限することで、データの流出・漏洩を防ぐもの。

しかしながら、ネットワークを分離することで、校務系、学習系、それぞれ別で端末を調達する必要があり、教職員数より多い台数の端末を整備していたが、実際には数が不足している状況で端末の追加要望の声が現場サイドから多くあった。

また、GIGAスクール構想による児童生徒の１人１台端末の整備により、膨大な学習ログ（データ）が生成されているが、ネットワークが分離されていることで、校務系での円滑なデータ利用が困難な状況。また、感染症対策や働き方や活用の柔軟性に対応するため、自宅への持ち帰りや課外授業等、利用場所を選ばない環境構築も必要な状況。

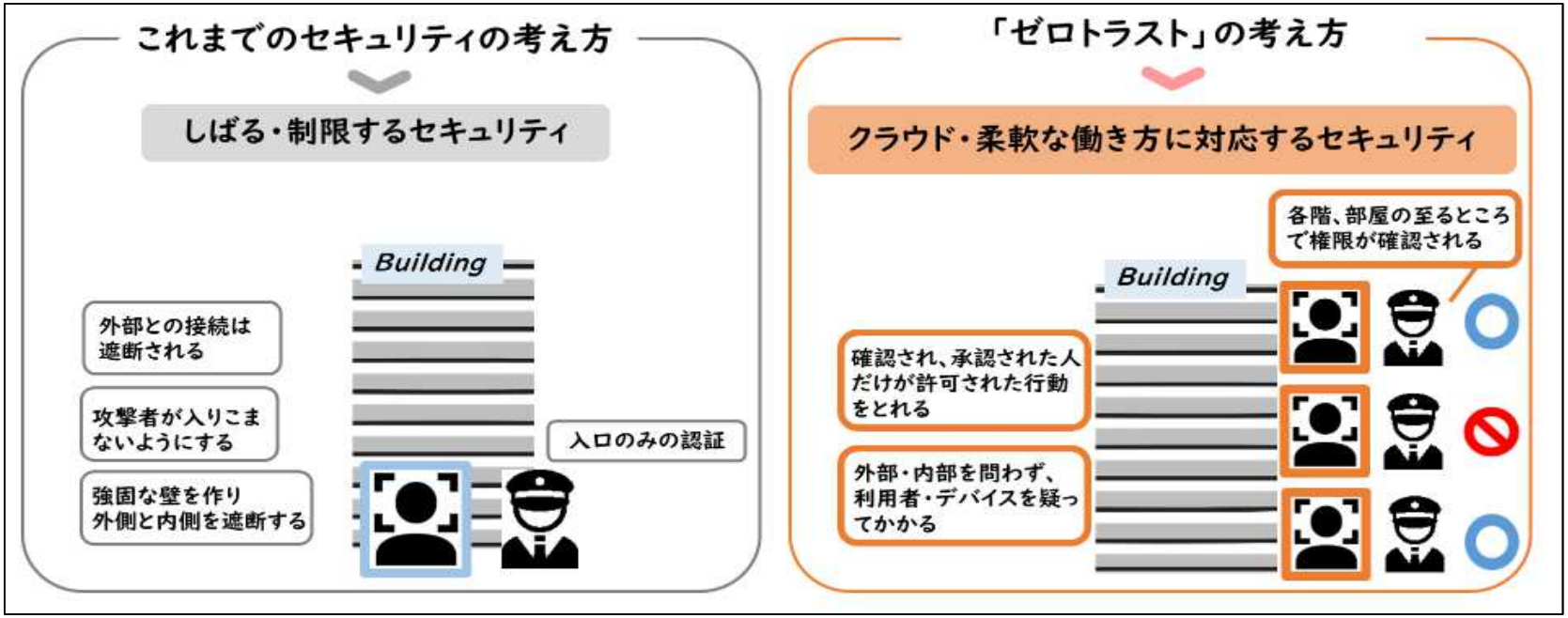
これらを解決し、システムの効率化、柔軟な働き方等を実現するためには、新たなセキュリティ対策が必要

※１校務系：児童生徒の成績、出欠席等の学校が保有する情報資産うち、それらの情報を学校・学級の管理運営、学習指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報を扱うネットワーク（本市では有線ネットワークとして整備）

※２学習系：児童生徒のワークシート、作品等の学校が保有する情報資産のうち、それらの情報を学校における教育活動において活用することを想定しており、かつ、当該情報に教員及び児童生徒がアクセスすることが想定されている情報を扱うネットワーク（本市では無線ネットワークとして整備）

新たなセキュリティ対策（ゼロトラスト対策）

○セキュリティ対策の考え方○



ゼロトラストとは

「全てのアクセスを信頼せず、必ず確認せよ」という考え方
外部は当然のこと、内部のアクセスであっても信頼しないという前提に立ってセキュリティを施すもの。

ゼロトラストの考え方が必要となった背景には、

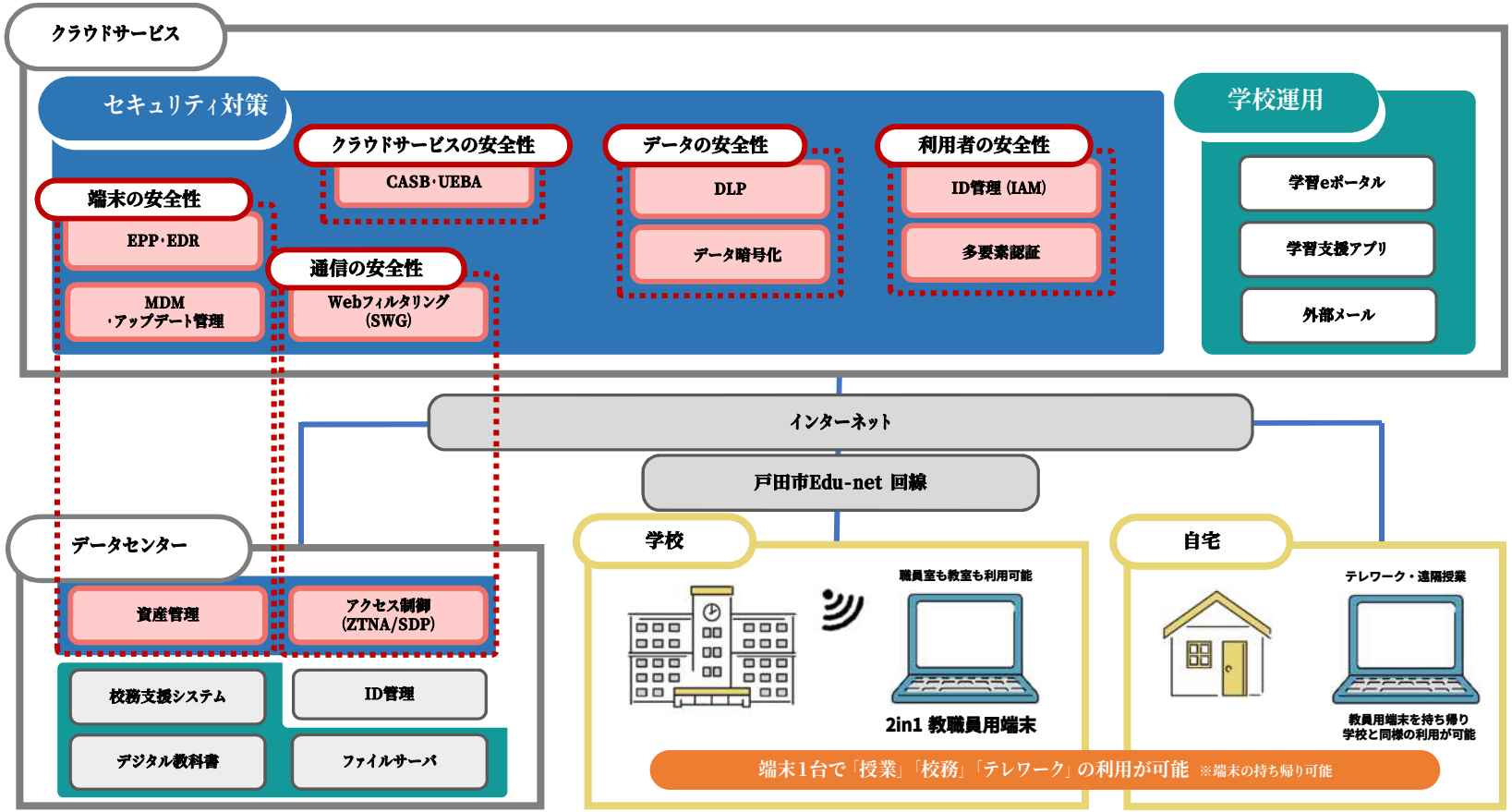
- **サイバー攻撃の高度化や内部不正などのセキュリティ脅威の増加**
- **新型コロナウィルス感染症の流行により加速したリモートワークの普及**
- **サーバやソフトウェア等を自社の管理施設内で管理・運用する状態から外部管理・運用型のクラウドサービスへの利用拡大により、どこまでが内部のネットワークかという境界があいまいになってきたこと**

などが挙げられる。

今後さらに、業務を安全かつ効率的に実施していくためにはこの考え方に基づくセキュリティが必要不可欠。

新たなセキュリティ対策（ゼロトラスト対策）

○戸田市版ゼロトラスト概要図○



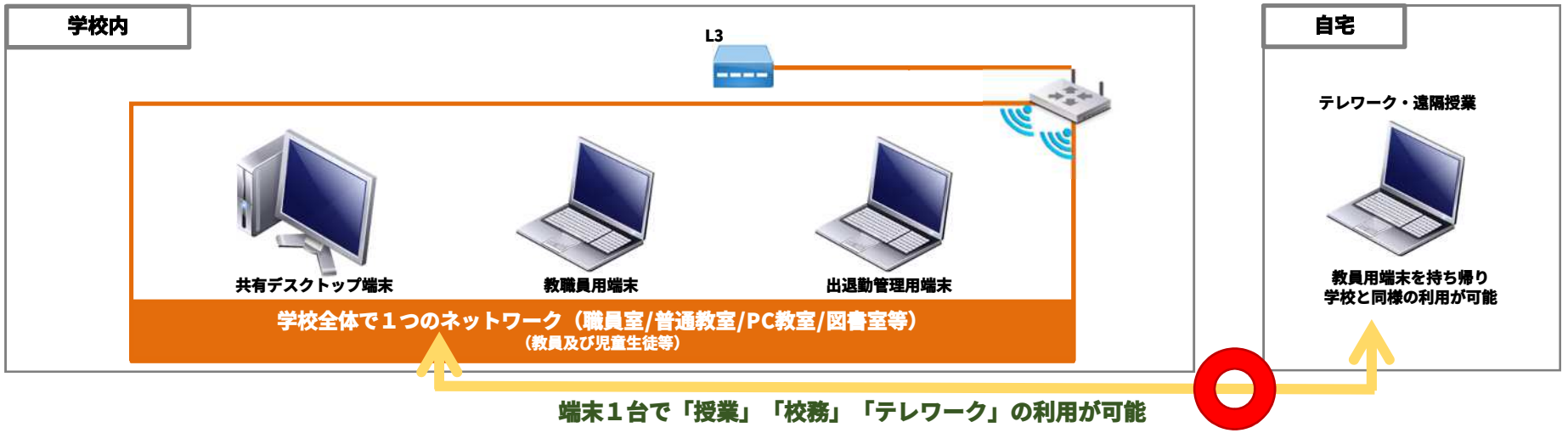
ゼロトラストに基づくセキュリティ対策を以下の５つの観点で実施し、強化

- **端末の安全性･･･**　ウィルス検出や対応、遠隔での統制や監視の実施
- **通信の安全性･･･**　ウィルス等の不正プログラムのブロックや業務に関係のないサイトへの アクセス制限の実施
- **クラウドサービス･･･**クラウドサービス利用におけるアクセス権限の制御、使用の監視の実施
  の安全性
- **データの安全性･･･**　データの監視や保護、暗号化の実施
- **利用者の安全性･･･**　IDやパスワードだけでなく顔認証を施した多要素認証の導入。業務内容 に応じたアクセス制御の実施

指導者用端末の１人１台化・校務系と学習系のネットワーク一元化

○ネットワーク一元化実施後（現在）

教職員用端末（1082台＋デスクトップ18台、出退勤用18台）　＝　1,118台



○セキュリティを担保しながら、効率化や利便性向上を実現した新たな端末構成

今までの教職員用端末



校務用端末



指導用端末

２台利用でそれぞれ利用用途が制限されている

１台化の実現

新しい教職員用端末



【学校現場の声】

校務系、学習系の各データを１台で閲覧、処理できるようになり、業務の効率性が上がった。

1台で校務も授業利用も可能

対策を施すことで、高いセキュリティのもと個人情報を扱う校務系業務を含め端末１台で業務を行うことが可能となり、システムの効率化や柔軟な働き方に寄与。