ローカルブレイクアウトやゼロトラストセキュリティで解消がされた課題と実践事例

教育DX戦略アドバイザー
柏市教育委員会　教育研究専門アドバイザー
西田　光昭
nishida@derek.jp

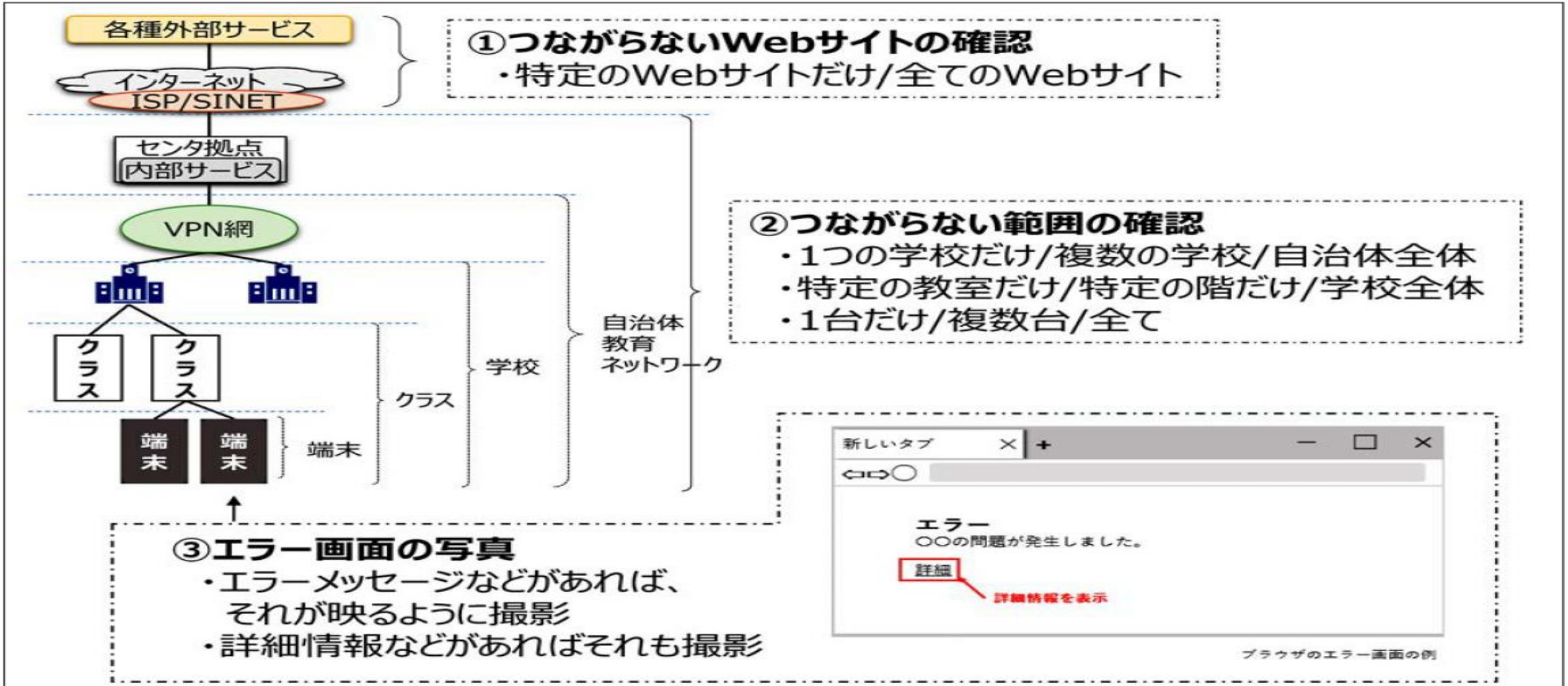
ネットワーク利用に支障がある。

- 全くつながらない
- 表示されない　:接続中
- 同時利用をすると、思うように動かない
- 子どもによって、安定しない

- 働き方改革事例をしてみたいけど・・

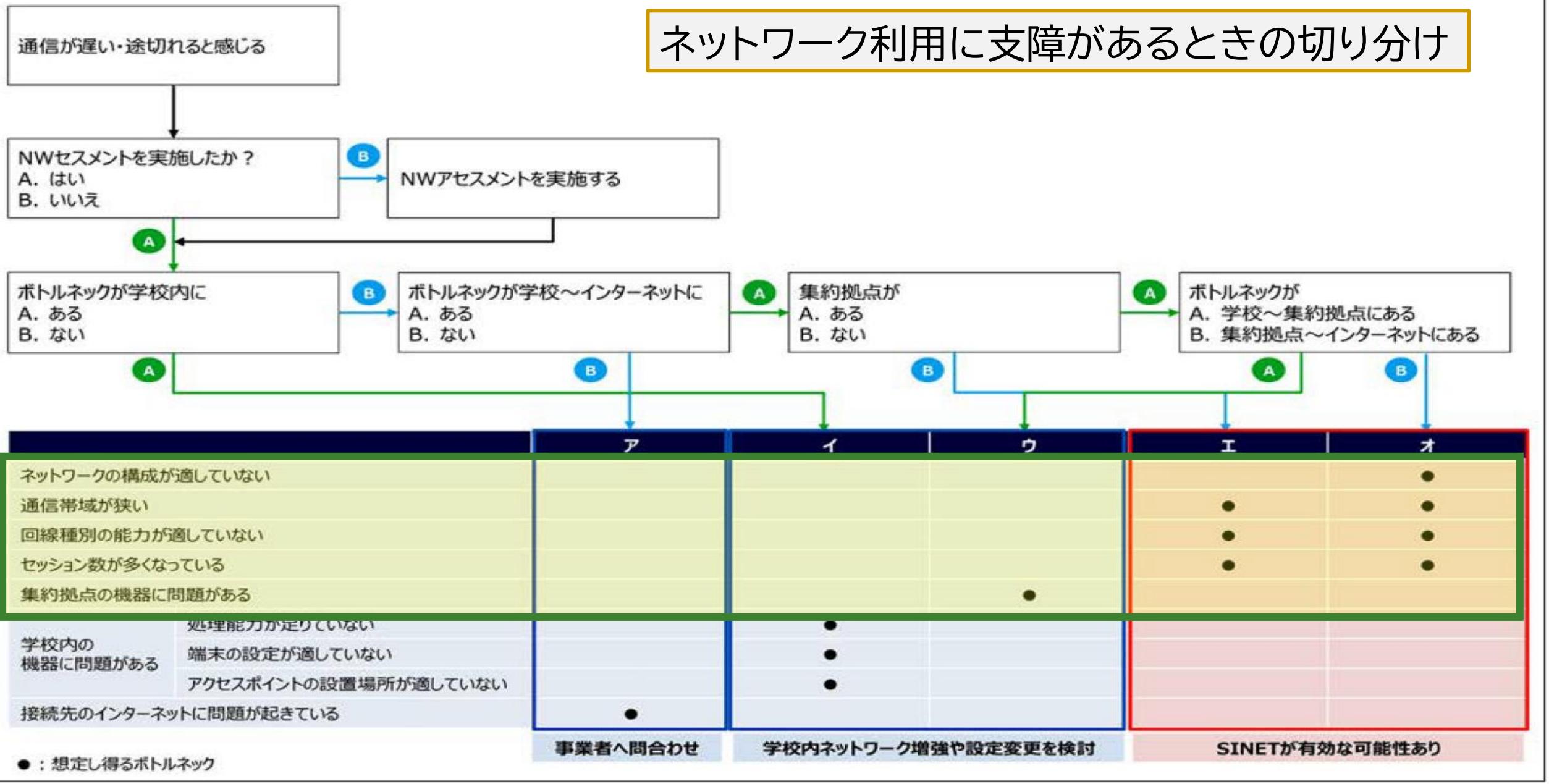
ネットワークがつながらなくなった時の確認事項（令和2年度事業における整理）

図 10　ネットワークがつながらなくなった時の確認事項



参照：「学習系ネットワークにおける通信環境最適化ガイドブック」より引用
https://www.mext.go.jp/content/20210405-mxt_jogai01-000010127_005.pdf

ネットワーク利用に支障があるときの切り分け



インターネット接続やアプリケーションの動作が遅くなる原因（例）　（文部科学省による整理）

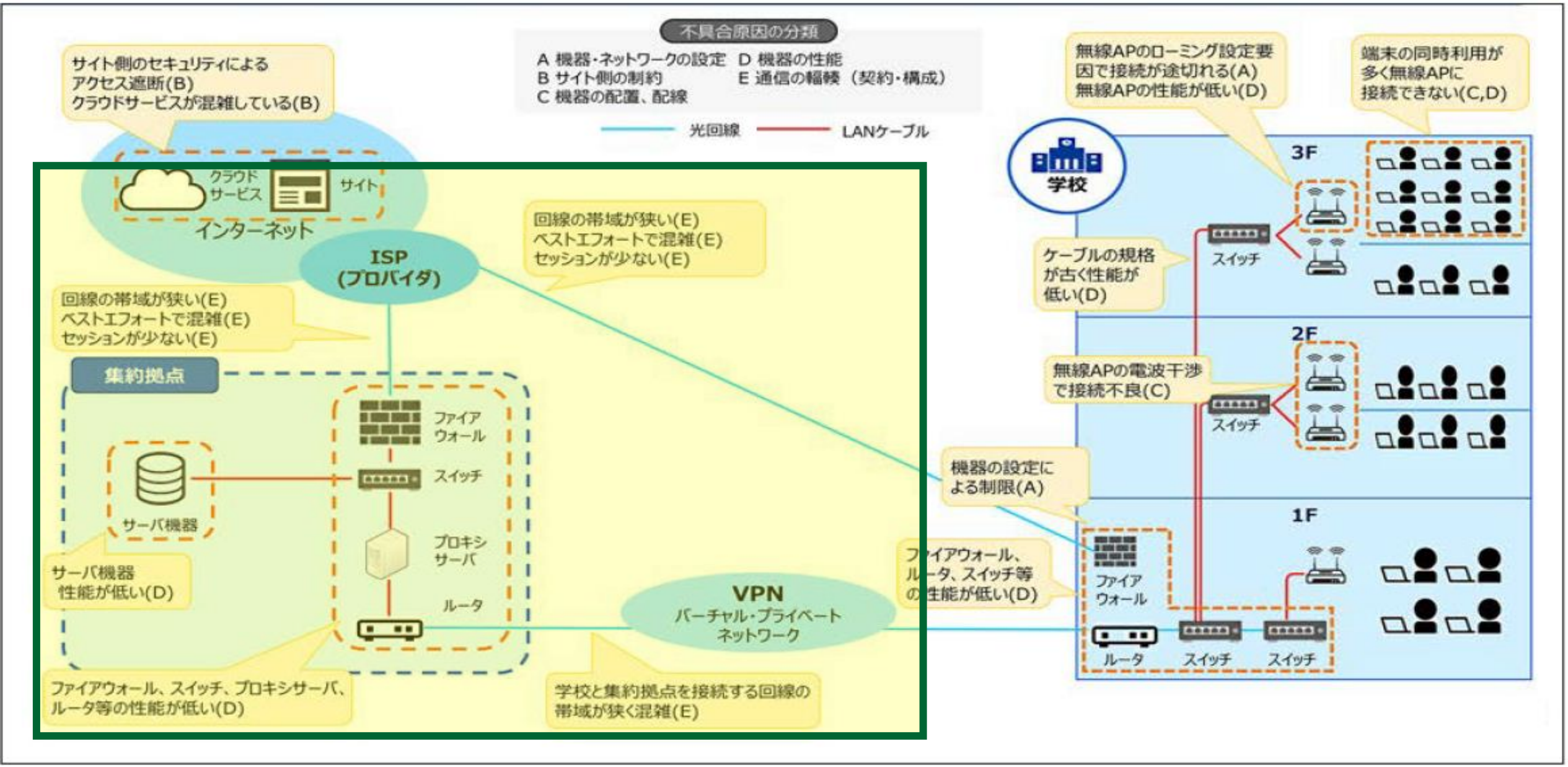


図 29　通信の流し方の考え方

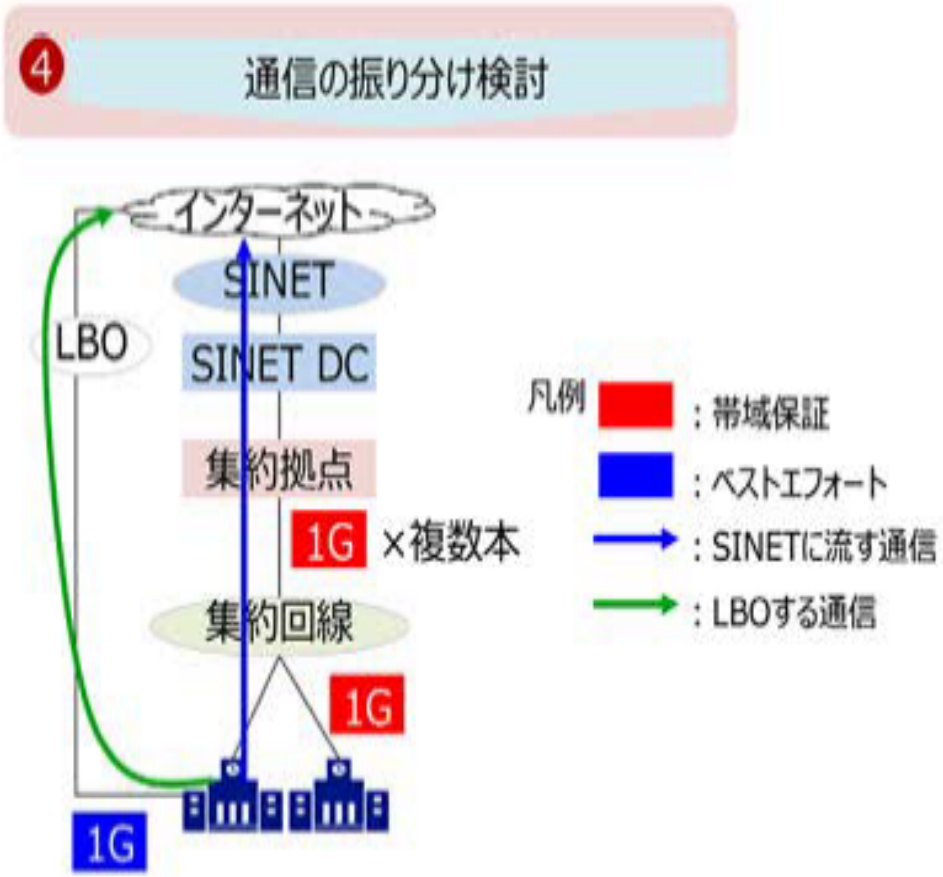


表 3　何を振り分けるか

何を振り分けするか、の観点

例	SINET	LBO
1	ユーザーが意図して発生する通信	ユーザーが意図せずに発生する通信
2	使用帯域/セッション数の多い学校の全通信	使用帯域/セッション数の少ない学校の全通信
3	スパイクする可能性がある通信	スパイクする可能性がない通信

表 4　どうやって振り分けるか

どうやって振り分けするか、の観点

設計案(一部)	設計内容
1	宛先グローバルIPアドレス or ポート番号による制御
2	アプリごとのドメインによる制御
3	アプリケーション制御 (ネットワーク機器が保持するアプリケーションデータベースをもとに通信振り分け)
4	プロキシ制御(例.プロキシ宛ての通信は集約拠点経由、グローバルIPアドレス宛はLBO)

①ユーザーが意図して発生する通信と、アップデート等のユーザーが意図せず発生するシステム通信とで、通信の振り分けを検討します。

②使用帯域 / セッション数の多い学校と少ない学校について、活用率を確認しながら通信の振り分けを検討します。

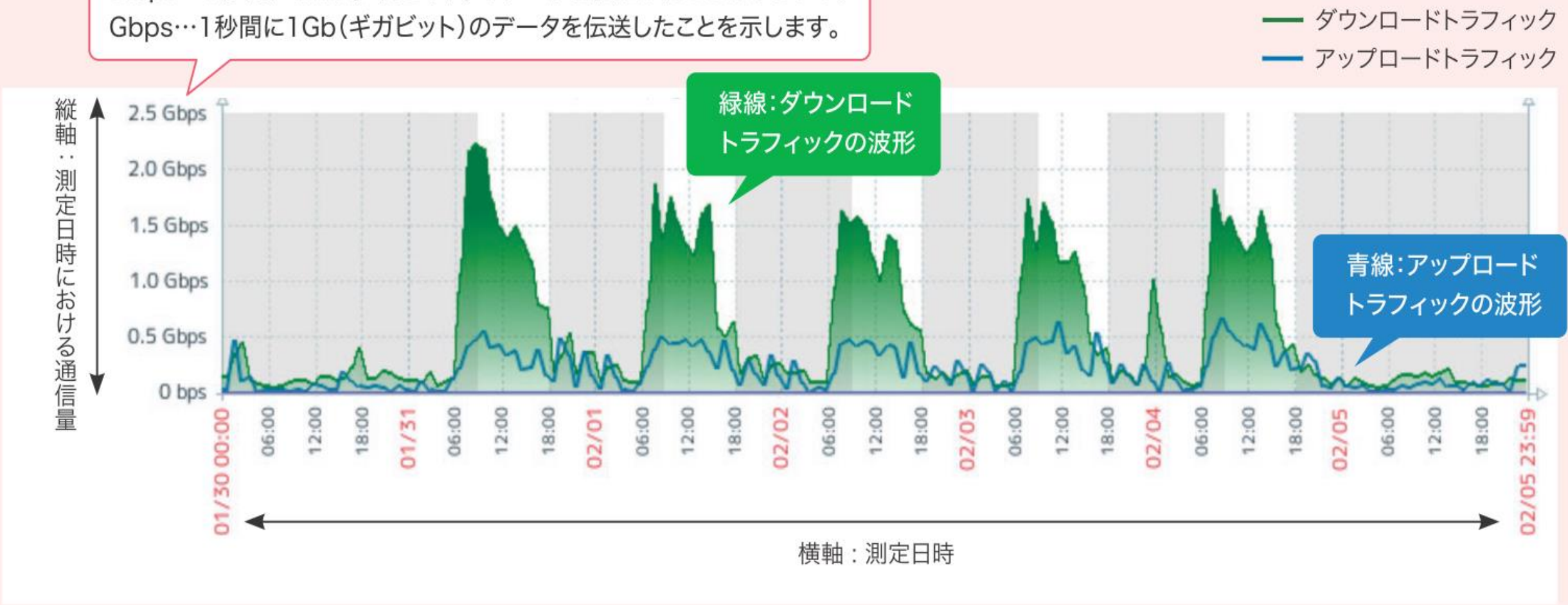
③スパイク※ 24 する可能性で通信の振り分けを検討します。VR や AR のような先進技術を用いる通信や大人数で顔を出しながら画面共有を行う Web 会議等の通信をスパイク性があると想定し対象の通信を個別に振り分ける検討が有効です。

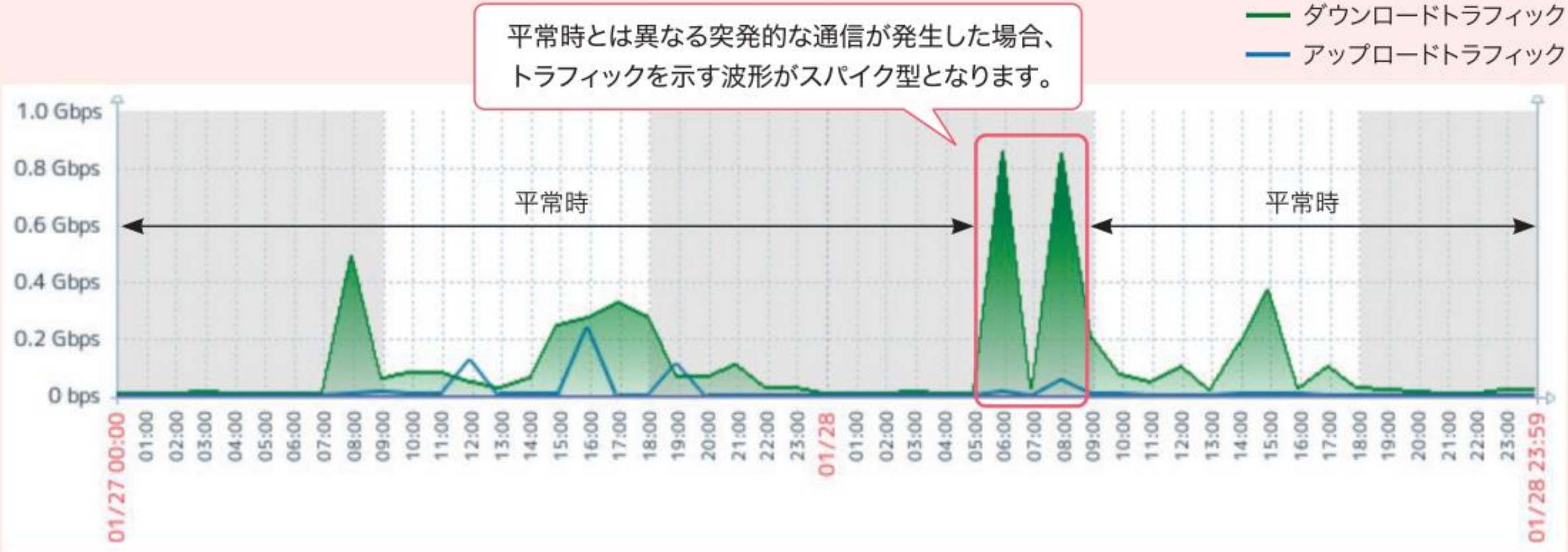
※24 スパイク：トラフィックが急激に上昇する現象のこと。

●トラフィックグラフは主に以下の情報にて構成されます。

※通信量を測定するツールによってトラフィックグラフの表記は異なります。　例示したトラフィックグラフはあくまで一例です。

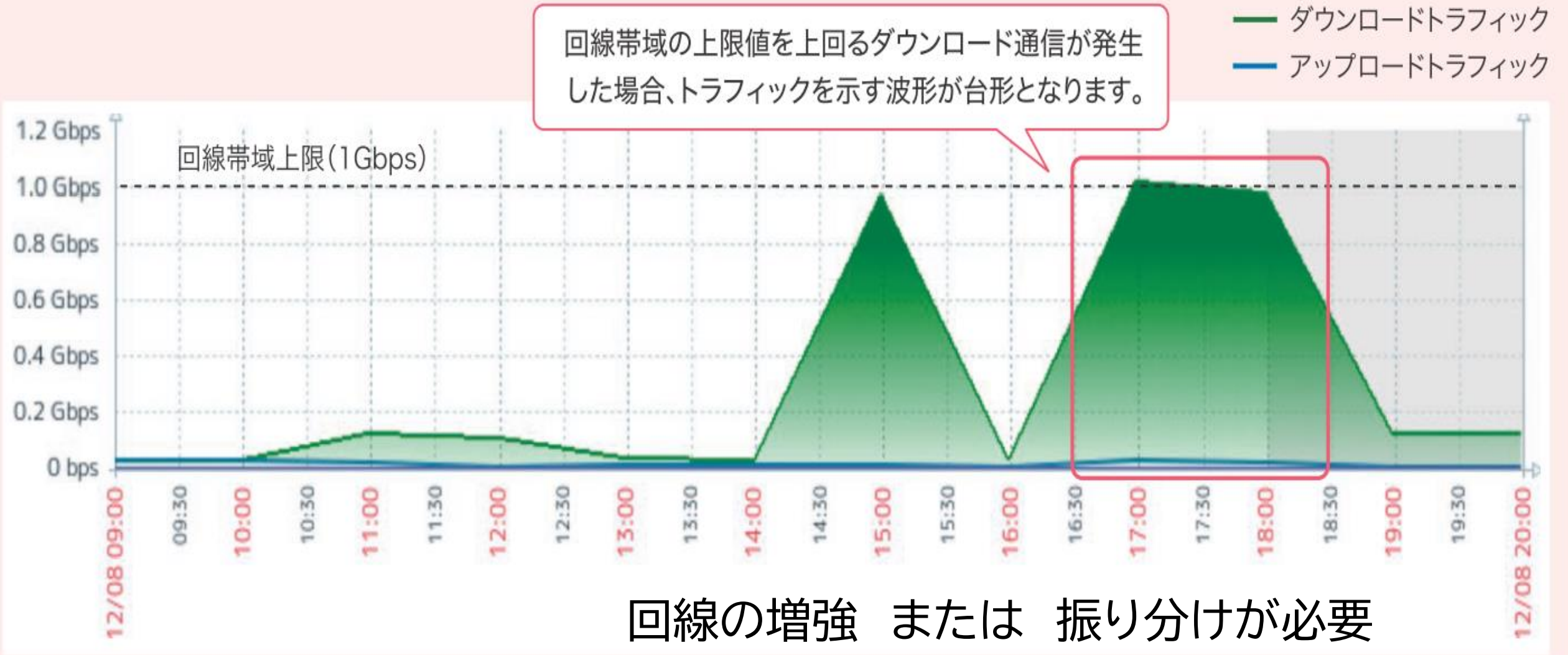
通信量の単位として、Mbps（Mega bit per second）や
Gbps（Giga bit per second）を用いることが多いです。
Mbps…1秒間に1Mb（メガビット）のデータを伝送したことを示します。
Gbps…1秒間に1Gb（ギガビット）のデータを伝送したことを示します。





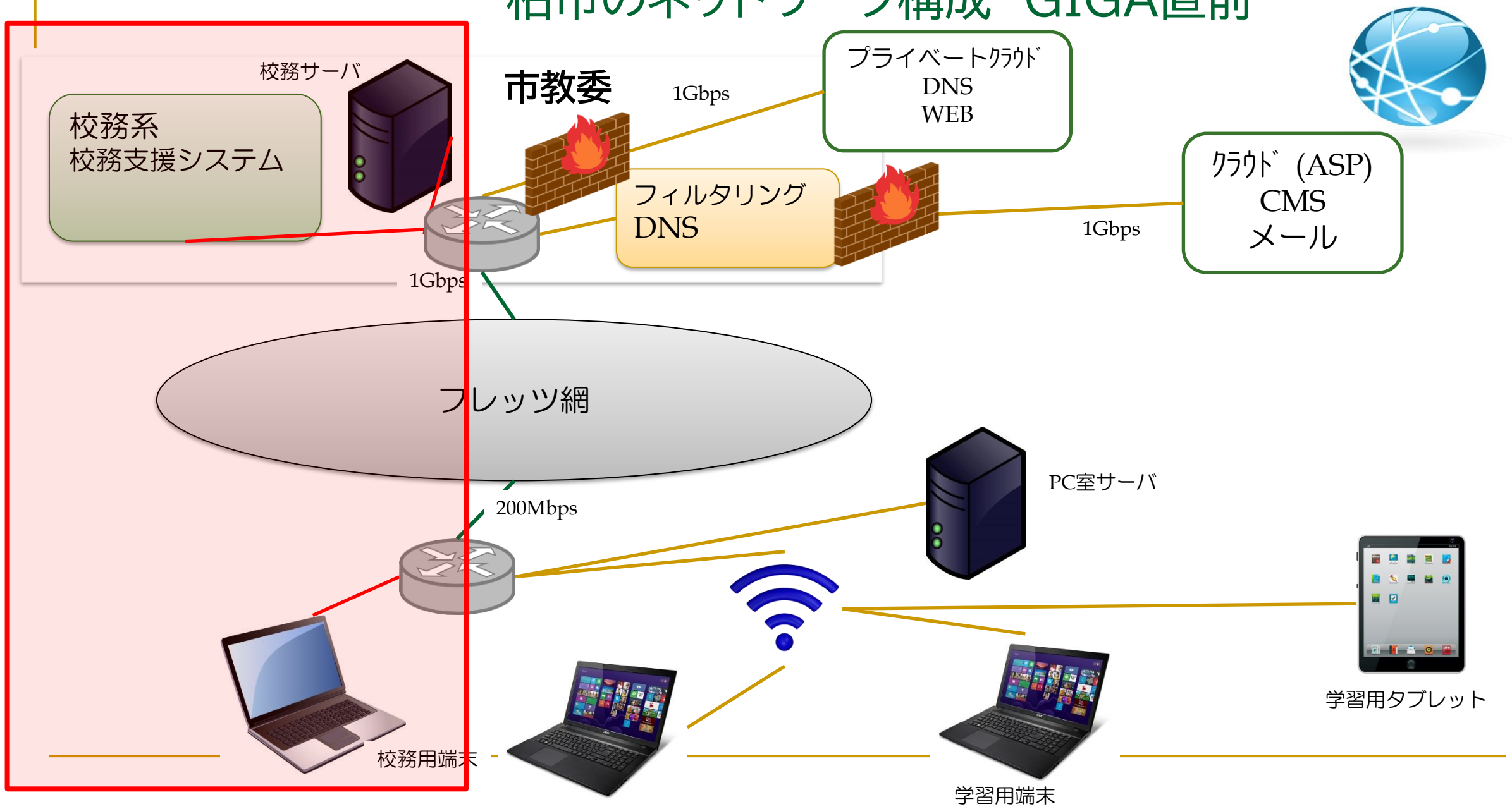
- スパイク型のトラフィックが発生した場合、該当時間帯において発生した通信をファイアウォール等のログから調査することが望まれます。スパイク型のトラフィックがその他通信に影響を与えている場合、対策案の検討が必要です。
- 本実証事業において発生したスパイク型の通信の大半は、学習端末のソフトウェア更新に係るダウンロード通信によるものでした。

回線の帯域が不足している時

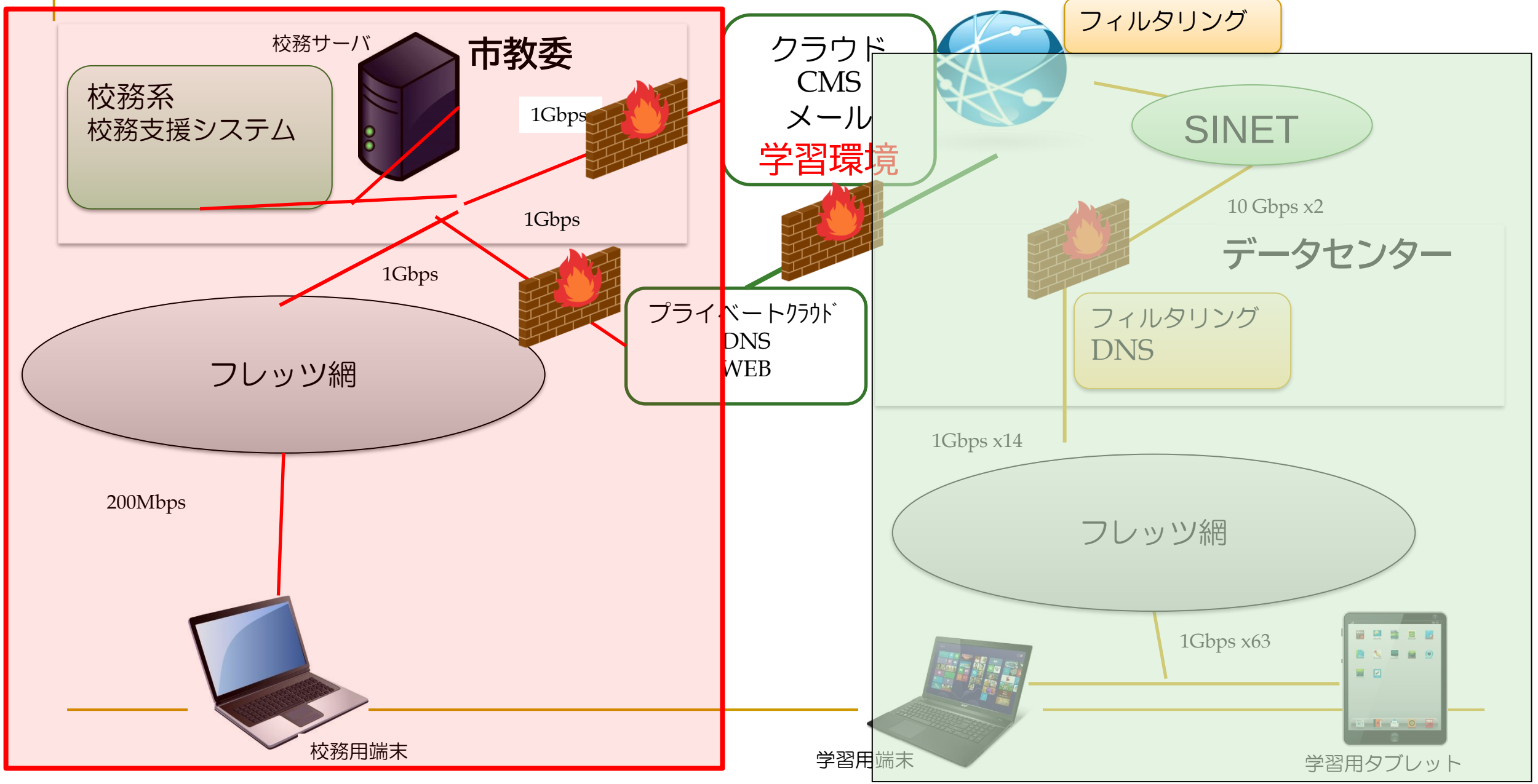


回線の増強　または　振り分けが必要

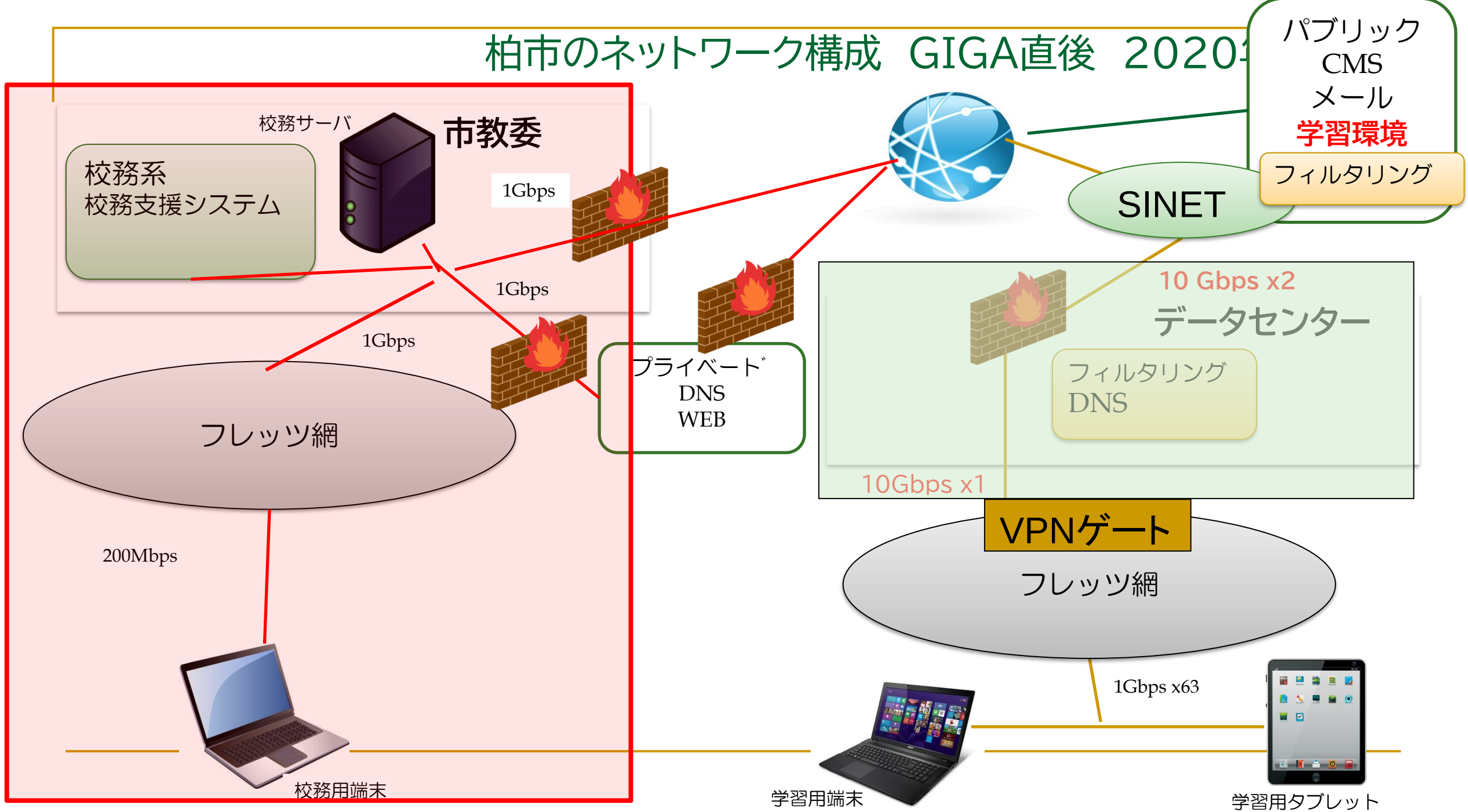
柏市のネットワーク構成　GIGA直前



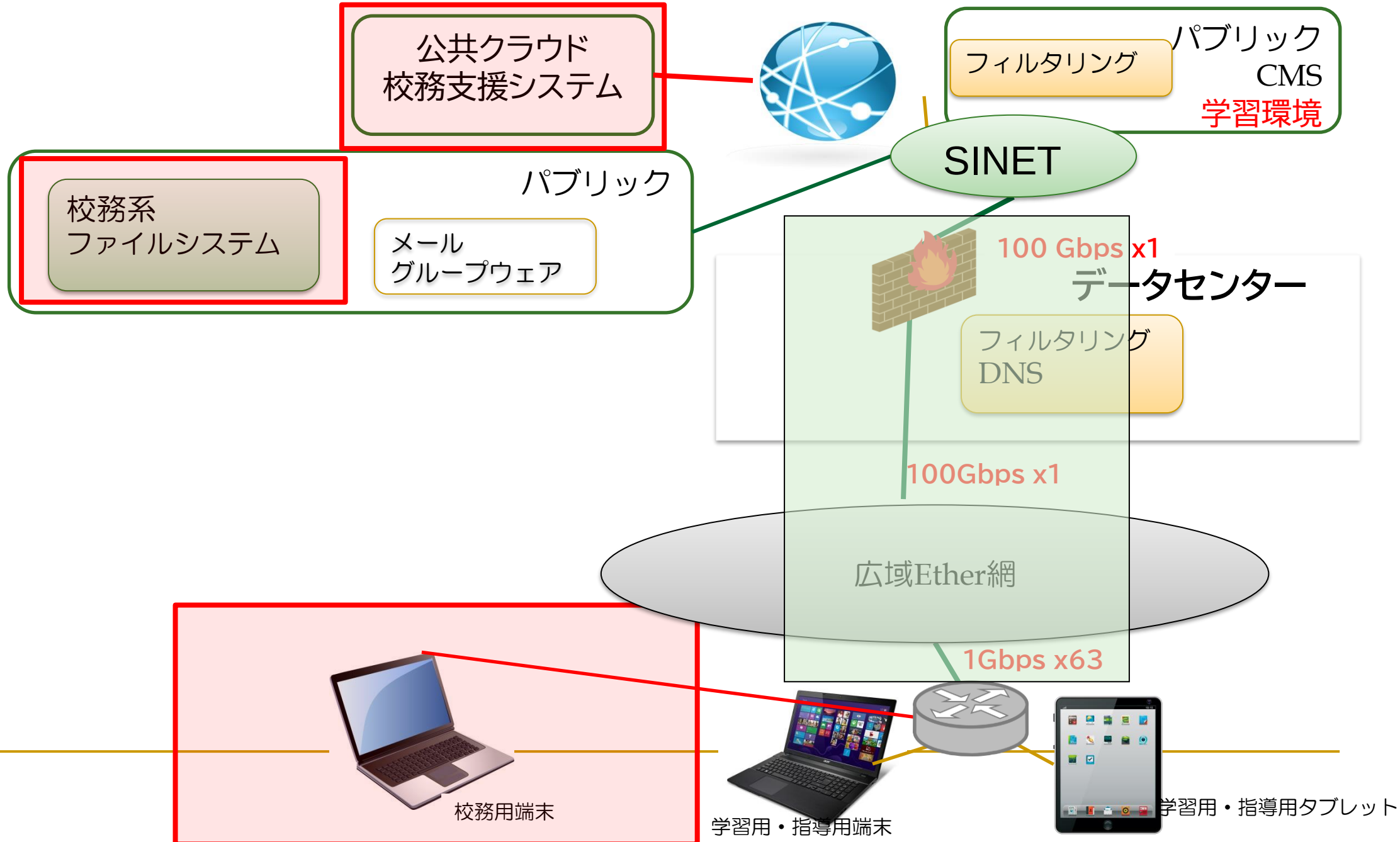
柏市のネットワーク構成　GIGA直後　2020年4月



柏市のネットワーク構成　GIGA直後　2020年



柏市のネットワーク構成　GIGA現在　2023年4月

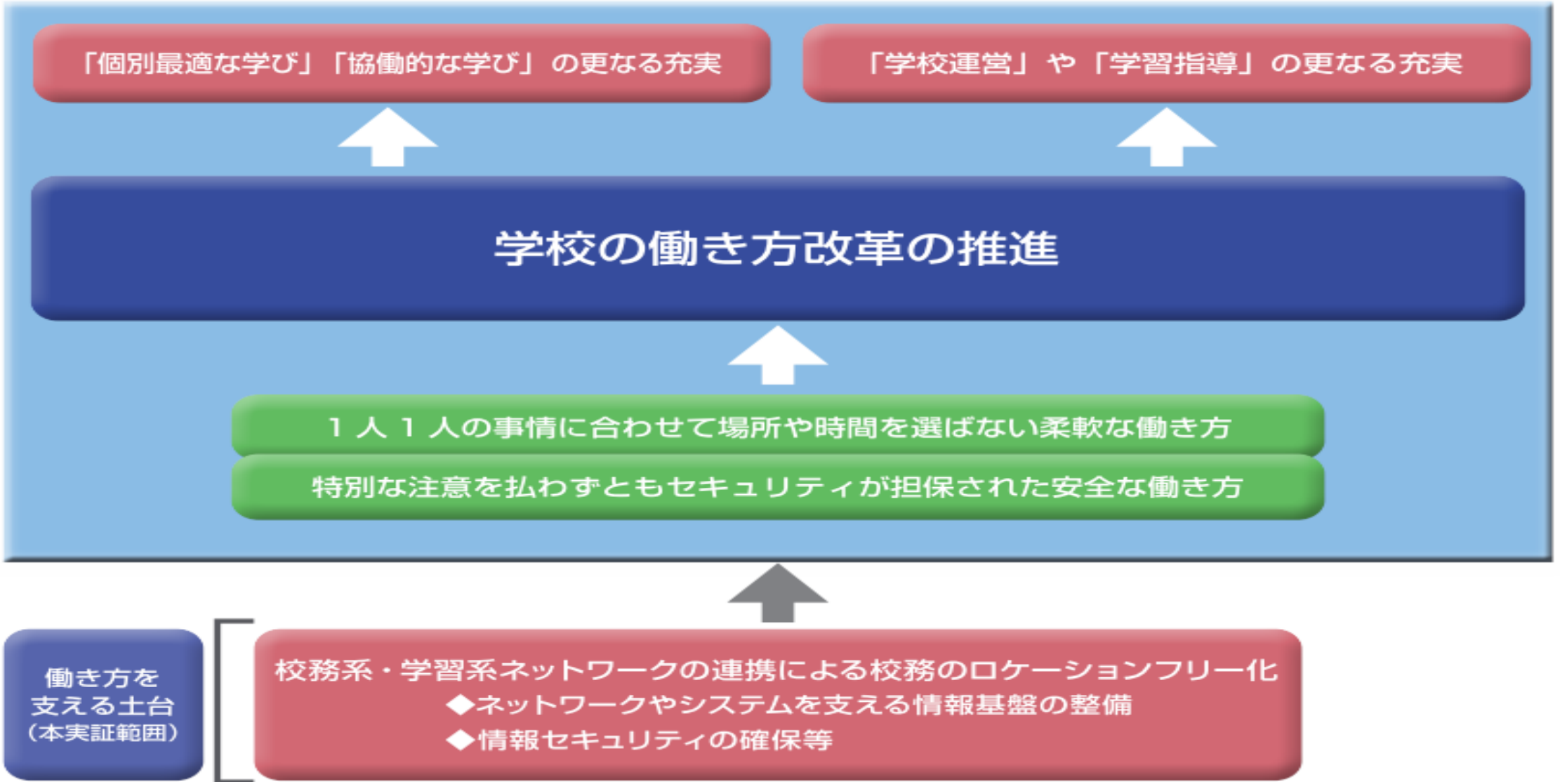


ゼロトラストセキュリティ

校務情報化の課題を解決するための手段

- ◆ 校務系・学習系ネットワークの連携
- ◆ 校務支援システムのクラウド化
- ◆ データ連携基盤の創出
- ◆ 安全安心な形で実装するためのセキュリティの確保

校務系・学習系ネットワークの連携により目指す方向性（イメージ）



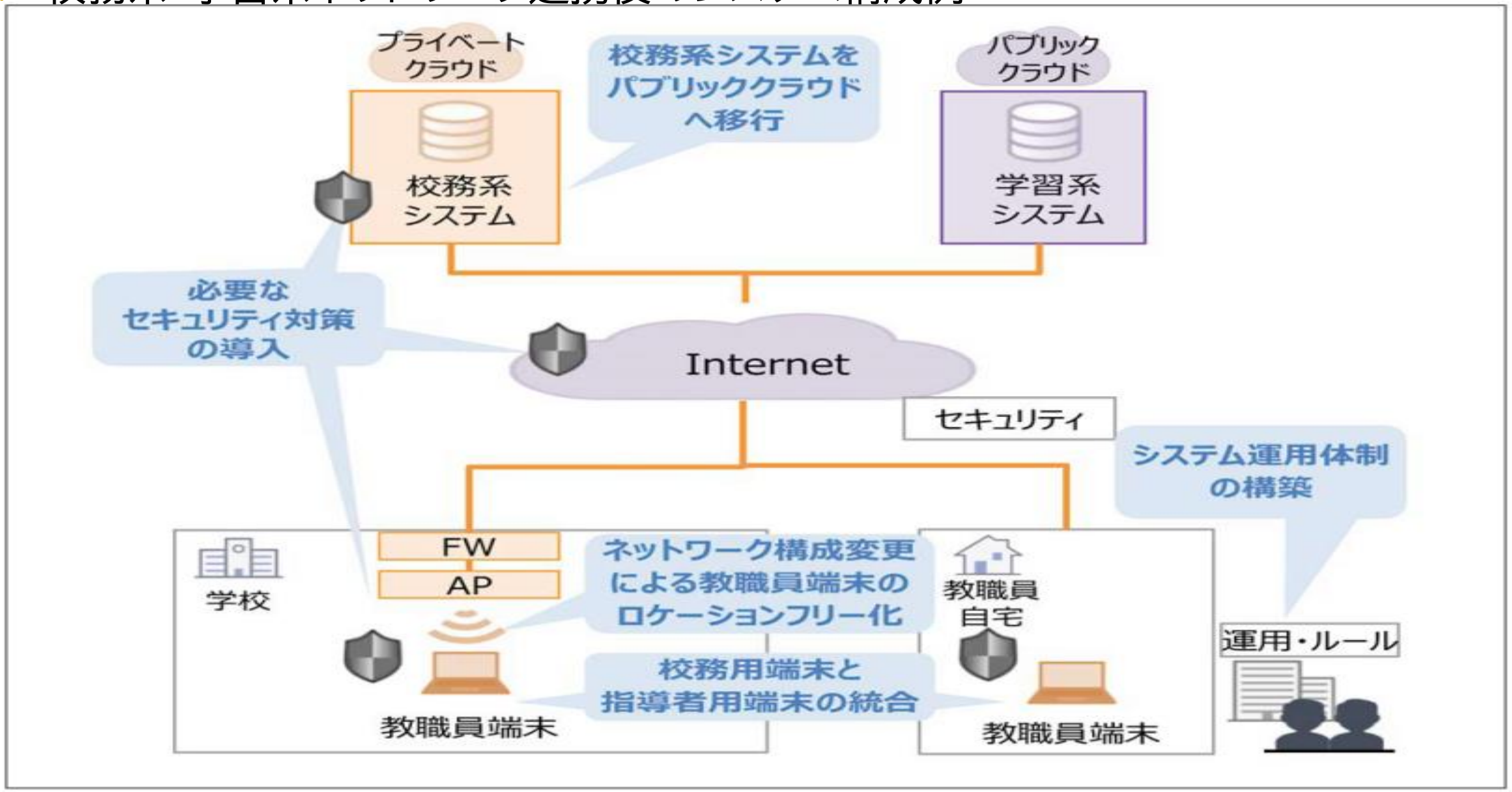
令和4年度 校務系・学習系ネットワークの連携における導入・運用・活用に関するガイドブック

移行先環境ごとの特徴

環境の特徴		パブリッククラウド (SaaS ※ 16)	パブリッククラウド (IaaS ※ 17)	プライベートクラウド (ホスティング型※ 18)	オンプレミス / プライベートクラウド (ハウジング型) ※ 19
①データの重要性	≒ セキュリティ	提供サービスによる	提供サービスを利用 ※ 20	環境整備が必要	
②データ量	≒ イニシャルコスト	低			高 ※ 21
	≒ ランニングコスト	高※ 22			低 / 中 ※ 25
		定額 ※ 23	変動 ※ 24	定額 ※ 23	
③利用場所	≒ ネットワーク	オープン ※ 26 （インターネット接続）		閉域 ※ 27（インターネット非接続）	
④利用者数 増加見込み	≒ 拡張性	プラン変更 ※ 28	自動拡張	プラン変更 ※ 28	機器増強が必要
⑤バックアップ	≒ データの保全性	提供サービスに含まれる ※ 29	提供サービスを利用	環境整備が必要	

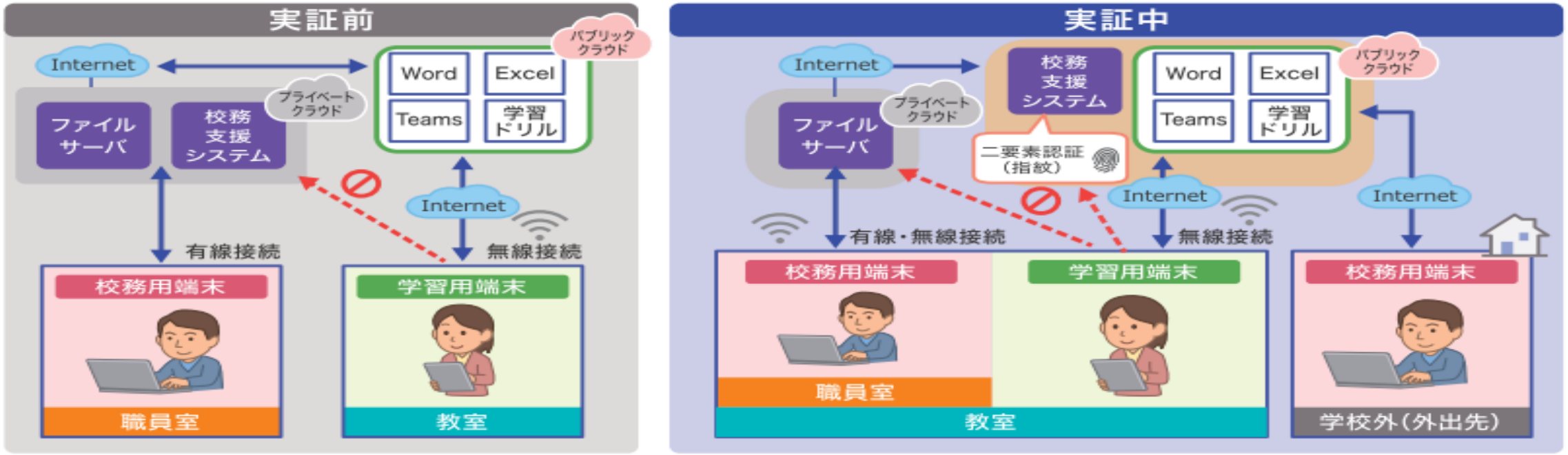
「何から」守るか	「どのように」守るか	
発生し得るセキュリティ脅威例	セキュリティ対策例	対応する要素技術例※36
組織管理外の端末を利用した校務支援システムへの不正アクセス	・組織内の全ての端末を一元的に管理し、組織管理下の端末のみ校務支援システムにアクセスできるよう制限する	・MDM
不正なソフトウェアのダウンロードによるマルウェア感染	・不要なアプリケーションのダウンロードを制限する	・MDM
端末 OS やソフトウェアの脆弱性を突いた攻撃	・端末 OS や各種ソフトウェアのバージョンを最新版にする	・MDM
校務用端末の紛失	・リモートワイプ機能を利用する ・デバイス上のデータを暗号化する	・MDM ・データ暗号化
重要性の高い情報をやり取りする通信への不正アクセス	・通信を暗号化し、第三者から閲覧されないようにする	・通信の暗号化
不適切な Web サイトへのアクセス履歴の消去	・Web サイトのアクセスに関するログを収集する	・Web フィルタリング
不正な Web サイトへのアクセスによる校務用端末のマルウェア感染	・不正な Web サイトへのアクセスを制限する ・端末にマルウェア対策ソフトウェアを導入する ・不審な挙動が見られた際に自動でネットワークから隔離する	・Web フィルタリング ・アンチウイルス※37 ・EDR/SOC
第三者による重要性の高い情報の窃取	・端末の IP アドレスや位置情報を基にデータへのアクセス制御を行う	・リスクベース認証
ID/PW の漏洩による校務支援システムへの不正アクセス	・二要素以上の認証手段を導入する	・多要素認証
複数のサービスで共通かつ安易に推測できるパスワードを設定する	・複数のクラウドサービスを一回の認証でアクセス可能とする	・SSO
校務支援システムや校務ファイルサーバに対する、不正アクセスや OS の脆弱性を利用した攻撃	・クラウド上に保存するデータを暗号化する ・各種サーバやシステムの保護を行う	・データ暗号化 ・IDS/IPS
校務支援システムに対する、Web アプリケーションの脆弱性を利用した攻撃	・Web アプリケーションの保護を行う	・WAF

校務系・学習系ネットワーク連携後のシステム構成例



令和4年度 校務系・学習系ネットワークの連携における導入・運用・活用に関するガイドブック

実証実験での校務系・学習系ネットワークの連携イメージ



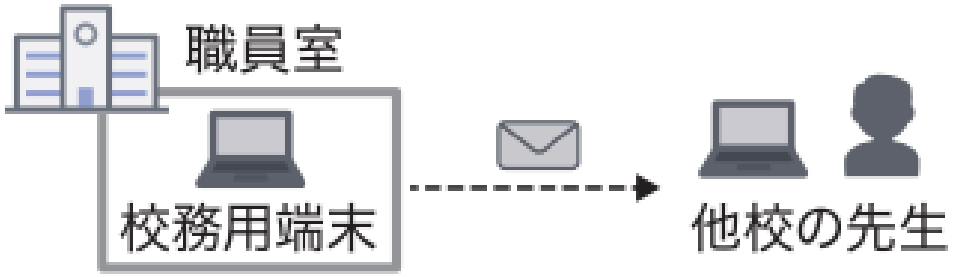
	実証前	実証中
ネットワーク構成	二層分離型	アクセス認証型
校務支援システム構成場所	プライベートクラウド	パブリッククラウド
校務支援システムへのアクセス方法	校務用端末／有線／職員室からのみ	校務用端末／ロケーションフリー

令和4年度 校務系・学習系ネットワークの連携における導入・運用・活用に関するガイドブック

校務系システムの職員室外利用と校務用端末 / 校務支援システムの学校外利用

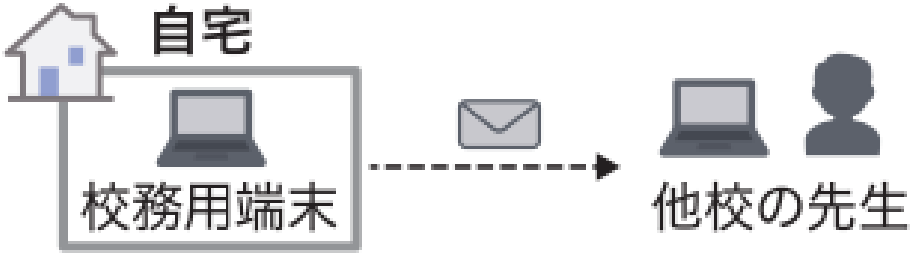
実証前

校務支援システムは職員室でのみ利用



実証中（利活用）

冬休み期間を活用し教員が**リモートワーク**を実施
校務支援システムを利用して、他校の先生へ連絡

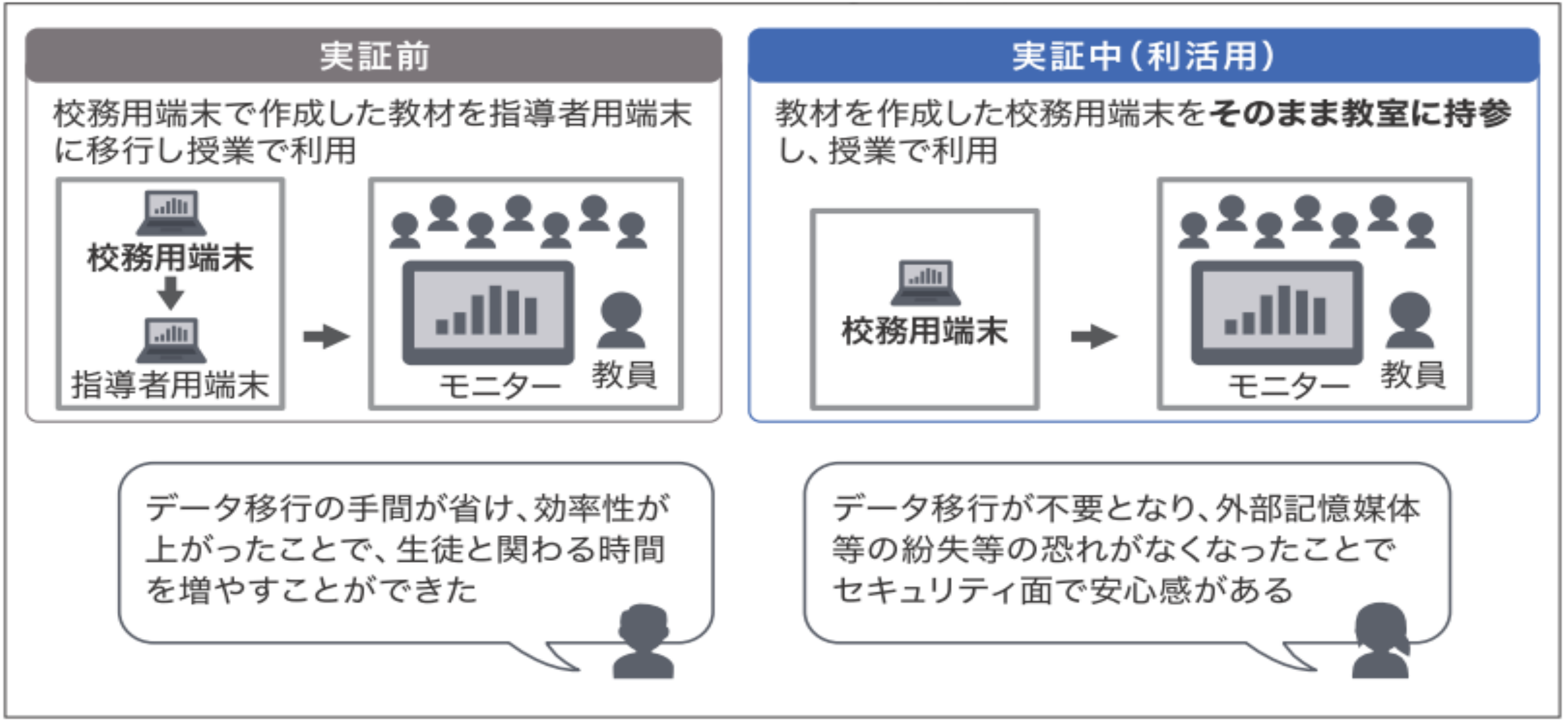


自宅だと仕事に集中でき、かつフレキシブルに業務時間を調整し、作業できたのは良かった

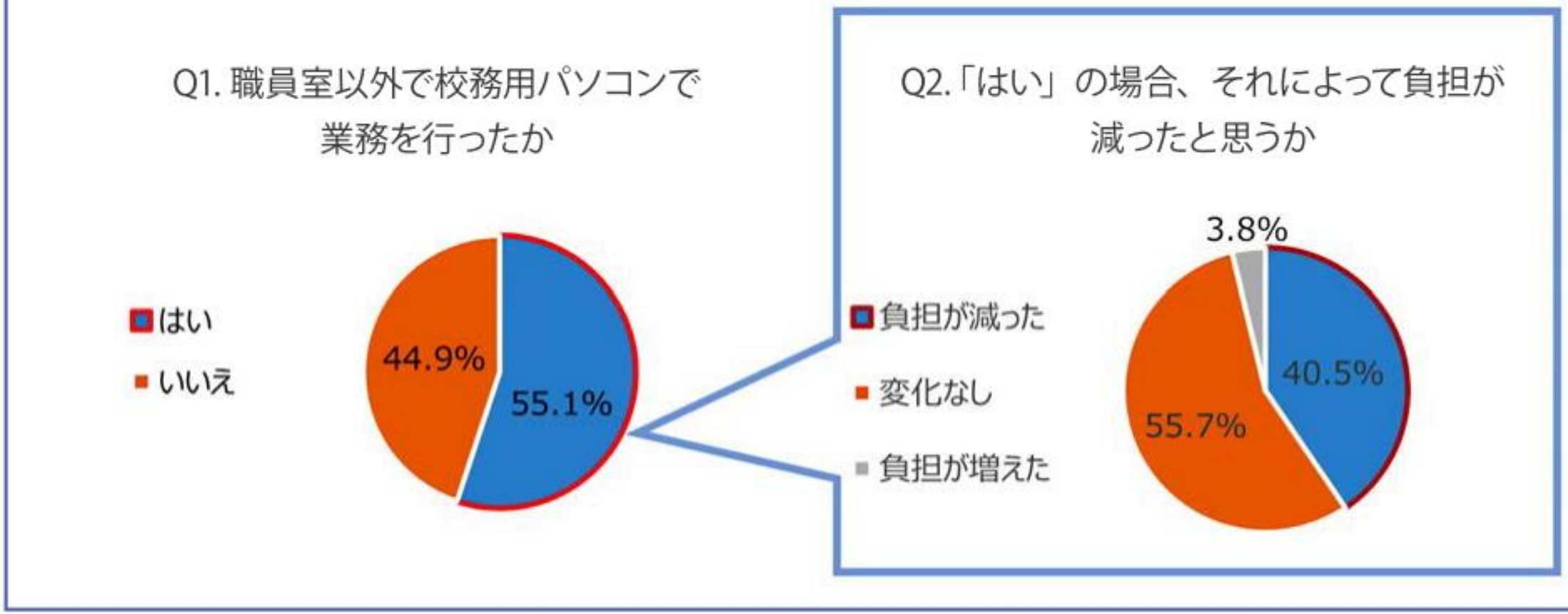
教室と職員室の行き来が減り、無駄が削減された

ペーパーレス化に繋がり、資料を直接編集できるので時間の削減につながった

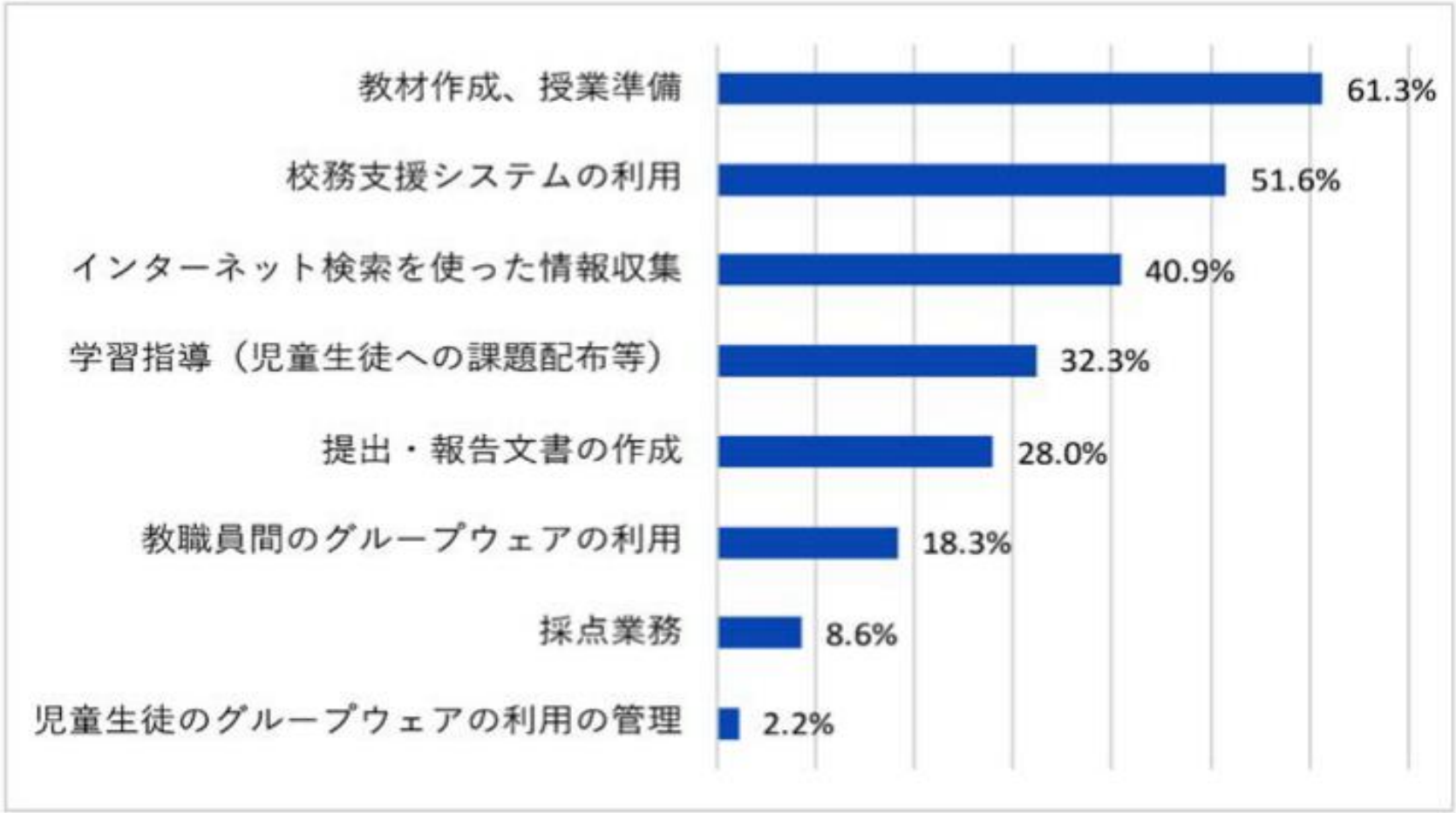
外部記憶媒体の利用が不要



Q1. 職員室以外で校務用パソコンで業務を行ったか
Q2.「はい」と答えた場合、それによって負担は減ったと思うか



Q3. 校務用端末を用いて実際に教室で行うようになった業務は何か



Q1. 通常の勤務日において、リモートワークは実施したか
Q2.「はい」と答えた場合、それによって負担は減ったと思うか