Panasonic

教職員の在宅勤務を進めたいが
セキュリティは担保したい！

小・中学校テレワーク実現ガイドブック

パナソニック インフォメーションシステムズ株式会社

本資料でお伝えすること

先生の校務に関する負担は年々増えています。英語の必修化、プログラミング教育の推進…さらにコロナ禍での授業対応…。働き方改革推進と業務効率化にはテレワークが有効ですが、セキュリティを担保しながらどのようにテレワーク環境を実現していけばよいのでしょうか？

本資料では、文部科学省のセキュリティポリシーに則ったテレワークの実現方法を詳しくご説明します。

内 容

1．テレワークに適している業務とは

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

3．テレワークの実現手法（VPN？VDI？）

4．　VPNとVDIの違い

1．テレワークに適している業務とは

まずは「テレワークでできること」「できないこと」を考えましょう。

テレワークしやすい

一人でできる業務

- 授業コンテンツ（教材）の作成
- 日報、成績評価 出欠管理

一人で実施可能な成果物のある業務

⇒ テレワークしやすい
校務システムはセキュリティを考慮する必要あり

複数人で行う業務

- Web会議
- オンライン授業
- 共有事項の連絡

連絡事項等の個別連絡、情報共有、申請手続きの承認行為といった複数人で行うことを必要とする業務

⇒ テレワークしやすい
コミュニケーションツールや電子決裁、ワークフローを活用する

対面で行う業務

- 職員会議
- 部活動
- 対面授業
- 子供たちへの指導

対面での授業や子供たちへの機微な指導等

⇒ テレワークしにくい
生徒とのコミュニケーションは優先的に対面で行う

テレワークしにくい

１．テレワークに適している業務とは

教職員のテレワークを行う際は、セキュリティに考慮しましょう。

一人でできる業務

- 授業コンテンツ（教材）の作成
- 日報、成績評価 出欠管理

一人で作成など成果物がある業務

⇒ テレワークしやすい
校務システムはセキュリティを考慮する必要あり

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」に沿った形での実現が重要です！

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

以下、6つの指針が「教育情報セキュリティポリシー」で示されています。

セキュリティガイドラインでの6つの指針	対応方法
①組織体制を確立すること	教育委員会が主管となりセキュリティ順守の運用/教育を行うことが求められており、セキュリティに関して学校間で共通した対策、ソリューションの導入が求められる。
②児童生徒による機微情報へのアクセスリスクへの対応を行うこと	児童生徒と機微な個人情報等を扱う校務系ネットワークは物理的もしくは論理的にネットワークを別々にして、児童生徒（学習系ネットワーク）からアクセスができないようなシステム構成にすることが求められる。
③インターネット経由による標的型攻撃などのリスクへの対応を行うこと	学習活動やメール等インターネットの活用が増えていることから、標的型攻撃、インターネット上の脅威に対する対策を講ずることが求められる。
④教育現場の実態を踏まえた情報セキュリティ対策を確立させること	個人情報等については暗号化でのアクセスが必須！ そのうえでリモートでの成績処理を行う場合、**VPNやVDIでのセキュリティ対策**を講じることが推奨される。
⑤教職員の情報セキュリティに関する意識の醸成を図ること	研修等を通じて教職員へ情報セキュリティへの意識の醸成を図ることやセキュリティ対策が講じてあるシステムを使うことで日常でのセキュリティ意識が高まってくる。
⑥教職員の業務的負担軽減及びICTを活用した多様な学習の実現を図ること。	情報セキュリティ対策を実施しながら、利便性を損ねず、効率化を図る。 センター型校務システム、リモート環境、ICTをフル活用して効率化を図り、生徒との時間を創出する。

3．テレワークの実現手法（VPN？VDI？）

「教育情報セキュリティポリシーに関するガイドライン」に沿った形で
どの手法で実現させるのが正解でしょうか？

テレワークの手法としてはVPN方式またはVDI方式が代表されますが、
セキュリティの観点からガイドラインに沿った形でメリット、デメリットのバランスを対比しながら
学校の業務にあった手法を選択することが必要です。

例えば・・・

① **端末**：デスクトップ型？ノート型？

② **個人情報**：個人情報データの取り扱いをどうする？

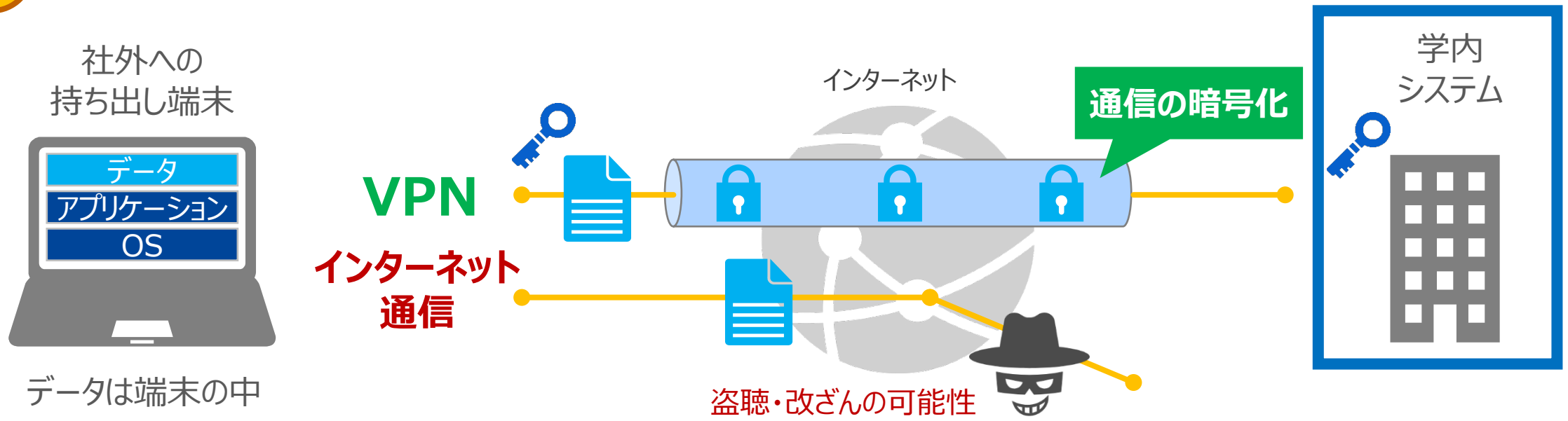
③ **コスト**：コストはどちらが高い？

④ **ネットワーク**：ネットワーク環境はどうなっている？

3．テレワークの実現手法（VPN？VDI？）

VPN（Virtual Private Network）とは、名前の通り、インターネット環境での通信において、仮想的に自分たち専用のネットワーク環境を実現する方法です。データの盗聴や改ざんなどを防ぐために、通信は暗号化されます。

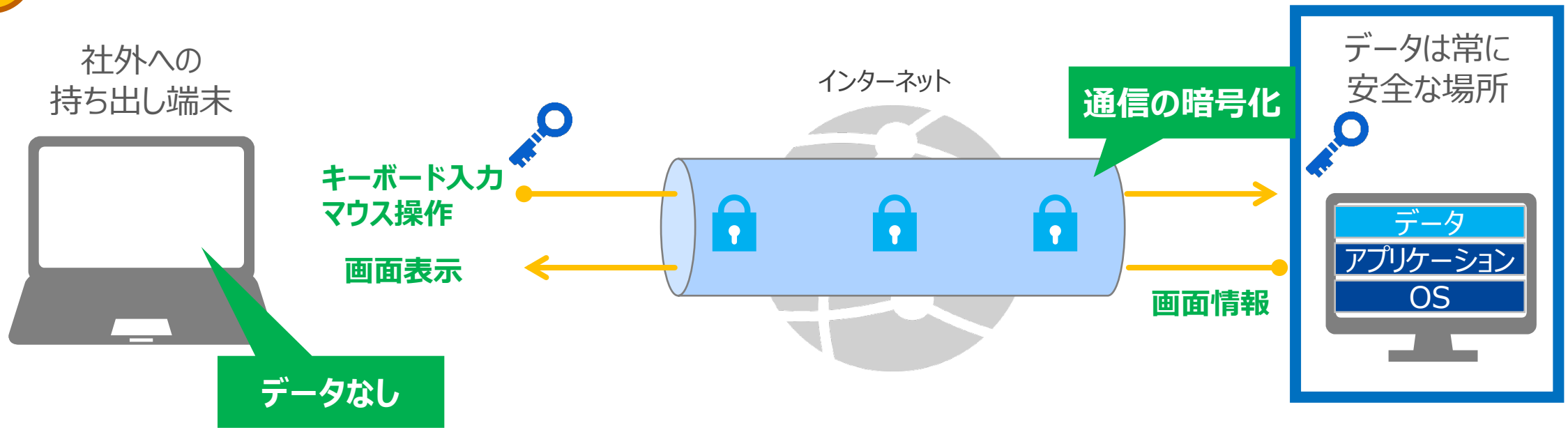
VPNは、安全に “通信する” しくみ



3．テレワークの実現手法（VPN？VDI？）

VDI（Virtual Desktop Infrastructure）とは、遠隔地で実行されているOSやアプリケーションを、手元で操作する物理端末でリモート操作する方法です。ネットワーク上は、実データではなく、画面やキーボード操作などの入出力情報を暗号化して通信します。

VDIは、安全に “デスクトップを利用する” しくみ



４．VPNとVDIの違い（ユーザ利用面）

VPNは、学内で利用しているノートPCを持ち出して使うという運用が一般的です。従来学内でデスクトップ型PCを利用している人が急にリモートワークが必要になった場合、準備に時間が掛かり、直ぐに利用できない可能性があります。

VDIは、物理端末とは関係なく利用できるしくみですので、端末手配の苦労は少なくなります。

	ＶＰＮ方式	ＶＤＩ方式
急な対応	 • 基本的にノート型端末が前提 • 常に持ち歩かないと急なテレワークへの対応はできない。	 • Windows、MacなどOS問わず。 • 学内はデスクトップ型、学外はノート型という使い分けも可能
ネットワーク環境	 • 学内共有データにアクセスするときは、実サイズのデータが流れるため、ネットワーク通信に負荷がかかる。	 • 画面情報だけで、実サイズのファイルは流れないため、ネットワーク負荷は少ない。
オフラインでの利用	 • 端末に保存しているデータを操作するだけのときは、オフラインで利用が可能	 • 常にネットワーク通信しながら遠隔操作するしくみのため、常時ネットワーク通信ができないと使えない。

４．VPNとVDIの違い（情報セキュリティ面）

VPNは、学内とのネットワーク通信を保護するしくみです。端末に保存されているデータの保護については、ディスクの暗号化や盗難時への対処としてのリモート消去など、別の対策を組合せて実施する必要があります。

VDIは、データを持ち出さないしくみです。USBメモリの使用可否についても制御可能です。

	ＶＰＮ方式	ＶＤＩ方式
ネットワーク 通信内容の保護	 • 暗号化により通信内容の保護が行われます。	 • 暗号化により通信内容の保護が行われます。通信内容は実データではなく、画像情報が中心です。
端末データの保護	 • 端末内にデータが存在するため、紛失に備えたディスクの暗号化や、USBメモリの使用制御などそれを保護する対策が必要です。 • VPN未接続状態のインターネットへのデータ流出への考慮も必要	 • 端末内にはデータは存在しません。 • USBメモリなどへのデータ書き出しも、管理者が設定するポリシーで制御可能 • 画面キャプチャによる漏洩を防ぐ機能が備わった製品もあります。

４．VPNとVDIの違い（システム構成･コスト面）

VPNは、実データが流れますので、学内ネットワークに設置するゲートウェイ装置の性能と、インターネット回線の速度に留意する必要があります。

VDIは、OSやアプリケーションの稼働は、学内サーバとなるため利用者が使う端末は低スペックでも稼働するというメリットがありますが、学内サーバ環境には大きな投資が伴います。

	ＶＰＮ方式	ＶＤＩ方式
システム構成	 • VPN環境自体は、シンプルなシステム構成で実現できます。 • その他の情報セキュリティ対策も組み合わせる必要があります。	 • 複数の実現方式があります。 • それぞれの実現方法については、別紙『失敗しないVDI導入 5つのポイント』を参照ください。
コスト	 • しくみがシンプルですので、比較的低コストで構築ができます。 • 充分なネットワーク通信速度を確保するためのコストや、その他の情報セキュリティ対策も含めたコスト試算が必要です。	 • 実現するためのコストは、実現方式によって異なりますが、VPN方式と比べると、コストが高くなる傾向があります。

まとめ

学校での業務は生徒への指導、生徒と向き合う時間、
どうしても現場で、対面でなければ対応を行うことができない業務が
様々にあります。

ただ、現場に縛られることなくリモートで効率化可能な業務もあり、
ハイブリッドで運用して負担を減らしていくことがお奨めです。

そのためにもVPNやVDIの手法を使って、
学校の実態にあったセキュリティ対策をし、
環境の整備を実現していくことが求められます。

オンライン無料個別相談のご紹介

学校PC管理に関するあらゆる疑問にお答えする
「オンライン無料個別相談」を実施しています。
「とにかく聞いてみたい」という方も、経験豊富な
担当者が承りますので、お気軽にご相談ください。

お問い合わせフォームはこちら

お問い合わせ先

パナソニック インフォメーションシステムズ株式会社

E-mail : sales-pisc@ml.jp.panasonic.com