

テレワーク向け

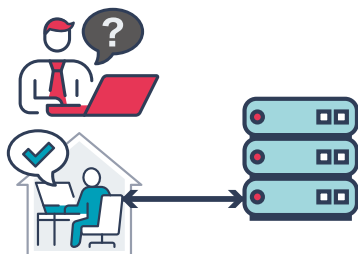
テレワーク環境整備

コンプライアンス対策

システム運用支援ソリューション

新しい働き方へ急速にシフトする中、
システム運用作業もニューノーマル時代を見据えた取り組みが求められています。

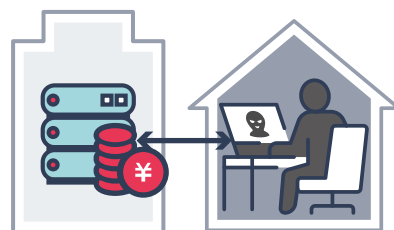
システム運用作業をテレワーク化するときの課題



課題1 作業者と管理者での
クロスチェックが困難



課題2 作業結果の提出が困難



課題3 不正操作の監視が困難

管理者
A



対策1

リアルタイムの
クロスチェックを実現

作業者
B



対策2

ユーザーごとに
作業結果取得、
作業内容を「見える化」

アクセス制御機能

対策3

権限の限定付与による
不正行為の抑止

システム変更
するサーバー



保守日9-17時
AとBにアクセス許可



アクセス不可

機密情報

テレワーク向け システム運用支援 ソリューション

リモートアクセス機能

既存のネットワーク環境はそのまま、セキュアにリモートアクセスを実現
※既設のテレワーク環境を活用して「アクセス制御機能」のみご利用いただくことも可能です。

当社は豊富な導入実績とノウハウを基に、効果的な対策をご提案します

新しい働き方に向けて、 ぜひ、テレワークできる業務の拡大をご検討ください

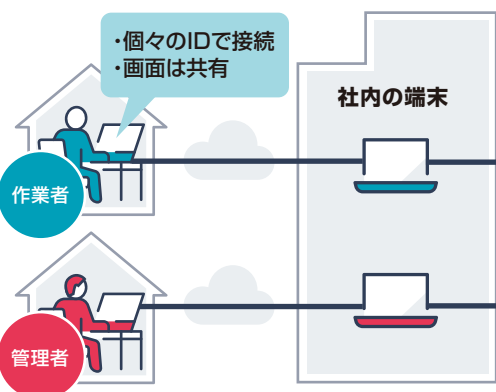
導入効果

●テレワーク環境で従来の運用レベルを維持 ●テレワーク作業の見える化

テレワーク向けシステム運用支援ソリューションの 活用方法

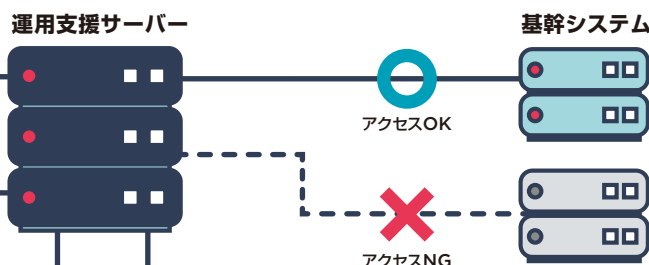
セキュアなリモート接続

- 画面だけをリモート端末に表示
- リモート端末がウイルスに感染していても、社内に持ち込まない

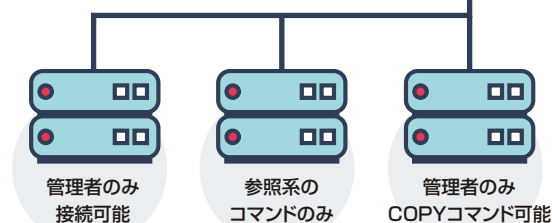


特権アカウントの不正利用を防止

- 作業員は特権ID/パスワードを知る必要なし
- 作業員と管理者で画面を共有して、クロスチェック、インシデント発生時管理者からの割り込み操作も可能
- アクセスできるサーバー、時間帯、抑止するコマンドの定義・制限
- 実行コマンドを事前登録し、定常業務の自動化や人的ミスを排除



情報漏えい対策



- 接続させる資産の重要度やユーザーの権限に応じて使用可能なコマンドを制御
- 必要最低限の権限を付与し
アクセスコントロールをすることで、システムへの直接的な不正を抑止

証拠保全・フォレンジック



管理者操作画面よりログの一括管理
・動画ログ ・テキストログ
・電子ファイルの持ち出しログ など

- LinuxとWindowsのログを一元管理、作業内容を「見える化」、証拠保全
- ユーザーごとにIDと適切な権限を付与、「いつ」「誰が」「どんな操作」を行ったか特定が可能
- 管理者操作画面より、ログの閲覧や、CSV形式での外部出力が可能
- ミスの追跡や、不正がなかったことの証明など、ステークホルダーと資産を守る

Linuxは、米国、その他の国におけるLinux Torvaldsの登録商標です。Windowsは、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。

商品・サービスに関するお問い合わせ・ご相談受付

Webによる受付

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールによる受付

hsc-contact@mlc.hitachi-solutions.com

*ご相談・ご依頼いただいた内容は回答などのため、当社の関連会社（日立ソリューションズグループ会社）および株式会社日立製作所に提供（共同利用含む）することがあります。
取り扱いには十分注意し、お客様の許可なく他の目的に使用することはありません。

HSC202010

*商品仕様は、改良のため予告なく変更する場合がございます。最新情報は、当社Webページをご確認ください。
*本カタログに記載されている会社名、商品名は各社の商標または登録商標です。
*本カタログの内容は、2020年10月現在のものです。

株式会社 日立ソリューションズ・クリエイト
www.hitachi-solutions-create.co.jp/