

テレワーク向け 操作監視ソリューション

ITガバナンスの維持

情報漏えいのリスク低減

テレワーク環境下では、周りの目による抑止力がなくなるため、システムの不正変更や情報持ち出しなどの内部不正のリスクが高まります。

テレワークのリスク



リスク1 セキュリティルール違反



リスク2 情報漏えい



リスク3 生産性の低下

対策1

対策2

テレワーク時の不正を検知後、
管理者へ通知



未許可アプリ検知



USB利用検知

テレワーク向け 操作監視 ソリューション

操作監視機能

対策3

「監視されている」という
意識付けによる抑止力



操作画面の録画

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、「操作監視機能」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

セキュリティ状況の見える化は、 管理者・従業員双方にメリットがあります。

テレワーク作業の見える化

インシデント時の潔白を証明

機微な作業のエビデンス

マルウェアの感染経緯を説明

テレワーク向け操作監視ソリューションの活用方法

セキュアなリモート接続



リモート端末

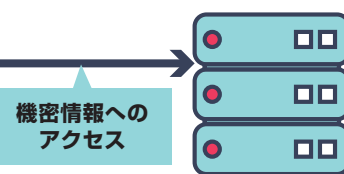
- 社内の端末の画面だけをリモート端末に表示
- リモート端末がウイルスに感染しても、社内
の端末へは持ち込ませない

社内の端末を 監視



管理者へ
リスク発生の
通知

セキュリティルール の統制



- テレワーク端末上でのリスク
となる操作を検知すると、
管理者へ通知

不正操作を抑止

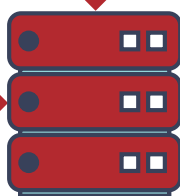
個人所有 端末を監視



個人所有端末

- 録画していることをテレワーク利用者に通知
- 情報持ち出しやシステム不正操作を抑止

セキュリティ事故 発生時の迅速な調査



操作監視サーバー

管理者

- アプリケーションの起動や設定変更などの各種操作ログを
サーバーに蓄積
- 見たい操作画面を検索してピンポイントで再生

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。

HSC202101

*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、2021年1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/