

スカイディブ デスクトップ クライアント







# シンクライアントシステムで 重要データの取り扱いをより安全に

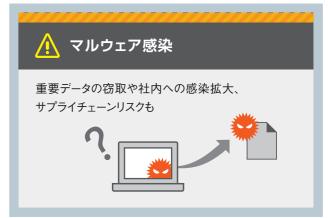
働き方改革の推進やコロナ禍の影響により、テレワークを導入されている企業が増えています。しかし、セキュリティが行き届いた社内に比べて、自宅などのテレワーク環境には情報漏洩リスクが多く存在します。そこで、安全なテレワークを実現する方法としてご活用いただけるのが、シンクライアントシステムです。シンクライアントシステムが組織のテレワークにどのようなメリットをもたらすのかをご紹介します。



# テレワークにはさまざまな情報漏洩リスクが!

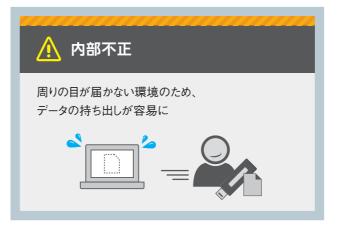
そもそも、テレワークにはどのような情報漏洩リスクがあるのでしょうか。例えば、PCの紛失・盗難によるデータ流出やマルウェアによるデータ窃取、内部不正によるデータ持ち出しなど、さまざまなケースが考えられます。安全なテレワークを実施するには、これらリスクへの対策が必須となります。

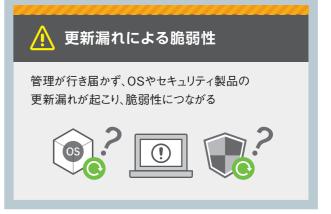












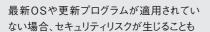
# リスク対策を踏まえ、働き方に応じたテレワーク方法の選定を

テレワークを実施する際は、組織の大切なデータを社外で扱う以上、あらゆる情報漏洩リスクへの対策を徹底しなければいけません。また、安定して運用できるように考慮することも大切です。セキュリティ面、運用面を踏まえると、私物PCよりも各種対策が施された

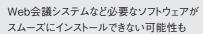
1 会社貸与PCを持ち帰って利用するのがよいでしょう。しかし、会社の規模や状況によってノートPCを従業員に手配することが難しい場合は、
2 リモートデスクトップを利用したり、
3 シンクライアントシステムを利用して仮想環境で作業する方法もあります。

#### 私物PCをそのまま利用すると …







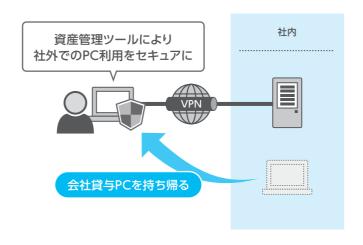




プライベートでの利用も含めた操作ログなど の情報が、社内サーバーに保存されることに

## 会社貸与PCを持ち帰って利用する

セキュリティソフトウェアや資産管理ツールの導入、OSの更新やハードディスクの暗号化など各種セキュリティ対策を施したPCを組織で用意し、持ち帰って利用する方法です。普段から業務でノートPCを利用している場合はそのPCを活用することで、導入コストを抑えることができます。ハードディスクなどを暗号化しておけば情報漏洩リスクを軽減できますが、PCの紛失・盗難が発生すれば企業の信用問題につながる恐れもあるため、持ち帰りには細心の注意が必要です。



#### ○ メリット "

- 組織のポリシーに沿ってセキュリティ対策を施したPCを利用できる
- 普段から利用しているノートPCを活用すれば導入コストを抑えられる

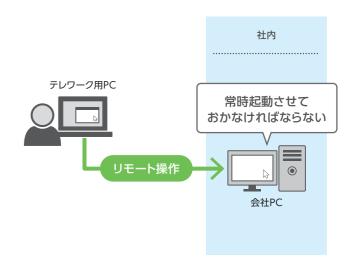
#### メ デメリット

• 持ち帰りに伴うPCの紛失・盗難リスクが発生

## 2

#### リモートデスクトップを利用する

業務でデスクトップPCを利用していて持ち帰りが困難な場合などに、別のPCから社内のPCをリモート操作する方法です。操作する側のPCにデータが残らず情報漏洩リスクを軽減できるほか、私物PCを利用すれば導入コストを抑えることができます。デメリットとして、リモート接続する会社PCを常時起動しておく必要があること、不具合発生時に会社PCを再起動するなどの人員が必要になり、会社全体で一斉にテレワークを実施する場合には運用が難しいことなどがあります。また、私物PCを利用する場合には、セキュリティ面での管理が別途必要となり、手間が発生します。



#### ○ メリット …

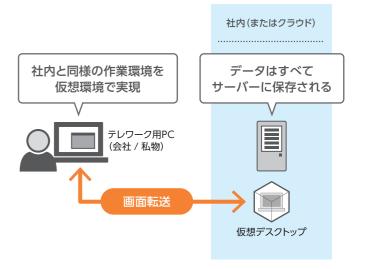
- PCにデータが残らないため情報漏洩リスクを軽減できる
- 私物PCを利用すれば導入コストを低減できる

#### メ デメリット …

- リモート先の社内PCを常時電源ONにしておく必要がある
- 不具合発生時などに社内PCを再起動するための人員が必要
- 私物PCの利用時に管理の手間が発生

# シンクライアントシステムを利用する

サーバー上に構築した仮想環境を、テレワーク用のPCから利用する方法です。PCへは仮想環境のデスクトップ画面が転送されるだけで、扱ったデータはPCに保存されないため、セキュリティ面のメリットが大きいのが特長です。また、複数の仮想環境をサーバー上で集中して管理できるため、個々のPCを管理するよりも負担を軽減できるほか、私物PC・タブレット端末、会社貸与PCなどのさまざまな機器から仮想環境を利用できます。ただし新規でシステムを導入する場合は、サーバー構築などの導入コストが発生します。



#### ○ メリット

- PCにデータが残らないため情報漏洩リスクを軽減できる
- サーバー側で複数の仮想環境を集中管理でき、管理者の負担を軽減
- 私物PC・タブレット端末、会社貸与PCなどさまざまな機器から仮想環境が利用可能

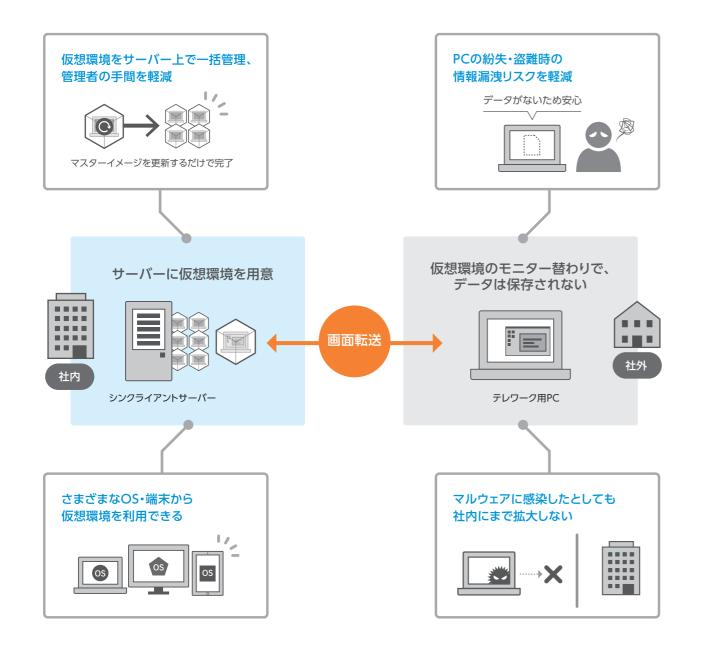
#### メ デメリット

サーバー構築などの導入コストがかかる

# さまざまなメリットがあるシンクライアントシステム

シンクライアントシステムでは、テレワーク中の物理PCから仮 サーバーに感染が拡大することもありません。OSやソフトウェ できます。操作した内容はすべて仮想環境で処理され、PCに データが保存されることもありません。そのため、PCの紛失・盗 ることができます。またPCがマルウェアに感染しても、社内のです。

想環境を通じて、社内のファイルサーバーなどのデータを操作 アの更新管理についても、マスターイメージを更新するだけで 済むため、PCを個別に管理するよりも手間を軽減できます。加 えて、Windows以外でも、対応しているOSであれば仮想環境 難や不正アクセスなどが起きたとしても、被害を最小限に抑え が利用可能なため、さまざまな端末から操作できるのもメリット



# シンクライアントシステムとほかの方法を併用しコストを最適化

テレワークの運用面で有利な点が多いシンクライアントシステ 末をシンクライアントシステムで利用するより、まずは部署ごと ムですが、利用するにはサーバーなどのハードウェアの購入や、の業務内容や作業形態によって、会社貸与PCの持ち帰りや 各種ライセンス費用など導入コストがかかります。すべての端 リモートデスクトップと併用するのも一つの手段です。

#### 特に機微なデータを扱う場合などにシンクライアントシステムを利用

例えば、セキュリティ対策の行き届いた会社貸与のノートPCを普段から利用している方は、そのPCを持ち帰ってテレワークで も利用することができます。またCADやデザインツール、映像編集ツールなどが必要で、高性能なデスクトップPCでしか業務 ができないという方は、リモートデスクトップを利用すればいいでしょう。普段ノートPCを利用しているけれど、個人情報など特に 機微な重要データを扱う方は、持ち帰りによる情報漏洩リスクが高いため、私物PCや別途会社で用意したノートPCからシン クライアントシステムを利用するという方法もあります。



#### オンプレミス?クラウド? コストや運用面の違いとは

シンクライアントシステムなど、組織のさまざまなシステムを運用していく手段に、オンプレミスとクラウドがあります。オンプレミスは組織内ですべての環境を構築するため、サーバーなどの調達にかかる費用や時間、構築後の保守運用の負担が発生します。クラウドは物理的な環境構築が不要なため、それらにかかる費用や時間を節約できるほか、サーバーなどの保守運用はサービスの提供者側が行うため、その分の負担も軽減できます。一方で、保守運用コストなどを含むサービスの利用料金が継続して発生します。

#### クラウドは用途によってサービスが分類される

laaS	サーバーやストレージなどのリソースを利用できるサービスです。主にシステムの構築環境として利用されます。CPUやメモリなど
	サーバーやストレージなどのリソースを利用できるサービスです。主にシステムの構築環境として利用されます。CPUやメモリなどのスペックを自由に選択できますが、それらを含む全体の設計やシステムの保守運用が必要です。

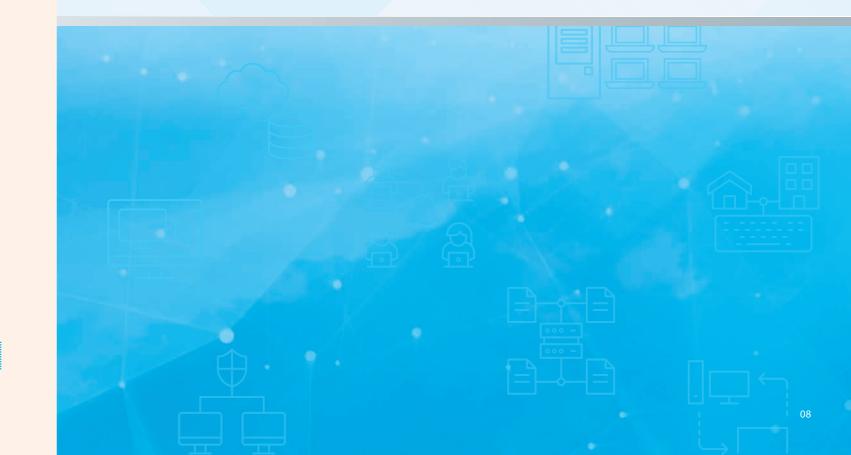
SaaS アプリケーションをインターネット上で利用できるサービスです。PCにアプリケーションをインストールすることなくインターネット経由で手軽に使えるほか、アプリケーションの更新管理などの負担が発生しません。

	オンプレミス	クラウド(laaS)
導入コスト	サーバーなどのハードウェアや各種ソフトウェ アの調達、インフラ環境の整備にかかる費 用と時間が必要	サービスの契約費用などが必要。物理的な 環境構築が不要なので、それらにかかる費 用や時間は発生しない
導入の手軽さ	システムの設計やハードウェア・ソフトウェア の調達、構築作業などにより、数か月単位の 時間と手間が必要。「HCI」などの機器を利 用することで、導入が容易になることも	Web上から必要なリソースの規模を申し込み、すぐに利用可能
運用コスト	保守運用にかかるコストが発生	保守運用コストなどを含むサービスの利用料 金が発生。中長期的に見た場合、コストが 高くなることも
管理者の負担	ハードウェアのメンテナンス、ソフトウェアの 更新など、保守運用の負担が継続的に発 生。また、管理者の専門的な知識も必要	ハードウェアに関する保守運用はサービス 提供者側が行うため、その分の負担を軽減 できる



# シンクライアントシステムでのテレワークを「SKYDIV Desktop Client」がサポート

「SKYDIV Desktop Client」は、国産のシンクライアントシステムです。開発から販売、サポートまでをすべて国内で行っており、長く安心してご利用いただけるのが特長です。クライアント運用管理ソフトウェア「SKYSEA Client View」と組み合わせて利用することで、組織にとって最適なテレワークの実施をご支援いたします。



# 「SKYDIV Desktop Client」と 「SKYSEA Client View」を組み合わせて、 組織のテレワークを全面的にサポート!

テレワークの各方法に応じてソフトウェアを利用することで、より安全で快適なテレワーク運用が実現します。例えば、会社貸与PCを持ち帰る場合やリモートデスクトップ方式でテレワークを行う場合は、「SKYSEA Client View」の利用をお薦めします。PCの操作ログを収集してテレワーク中の状況把握に活用できるほか、情報漏洩を防ぐための各種セキュリティ対策をPCに施すことができます。

特に機微なデータをテレワークで扱う場合は、シンクライアントシステム「SKYDIV Desktop Client」の利用を推奨します。テレワーク用PCから仮想環境を通じて社内の重要データを扱うことで、データ自体はPCに保存されないため情報漏洩リスクを軽減することが可能です。

会社PCを持ち帰る

#### テレワークで利用するPCは 「SKYSEA Client View」でセキュリティ強化

情報漏洩リスクを伴う操作を制限したり、OSやセキュリティ製品の更新管理を徹底するなど、各種セキュリティ対策を「SKYSEA Client View」で施すことができます。収集した操作ログからテレワーク中の状況を把握することも可能です。

営業職など、普段から持ち運び可能なノートPCを利用 している場合は、持ち帰ってテレワークでも利用

#### リモートデスクトップ方式は 「SKYSEA Client View」で操作状況を把握

社内にあるリモート操作対象のPCに「SKYSEA Client View」を導入することで、PCの各種セキュリティ対策を強化できるほか、自宅からリモート操作した内容を操作ログで記録・確認することができます。

開発・設計や映像編集など、社内の高性能なデスクトップ PCでしか業務ができない場合は自宅からリモート操作

#### 特に機微なデータを扱う場合は 「SKYDIV Desktop Client」を

個人情報など特に機微なデータを扱う場合は、シンクライアントシステムの「SKYDIV Desktop Client」を利用。転送された仮想環境の画面からいつもと同じように社内のデータを扱うことができますが、データ自体はテレワーク用のPCに保存されないため、PCの紛失・盗難などによる情報漏洩の心配もありません。

個人情報などの機微なデータを取り扱う場合は、シン クライアントシステムでセキュリティを確保







SKYDIV Desktop Client センターサーバー



仮想デスクトップ

シンクライアントサーバー

社内

リモート操作

インターネット

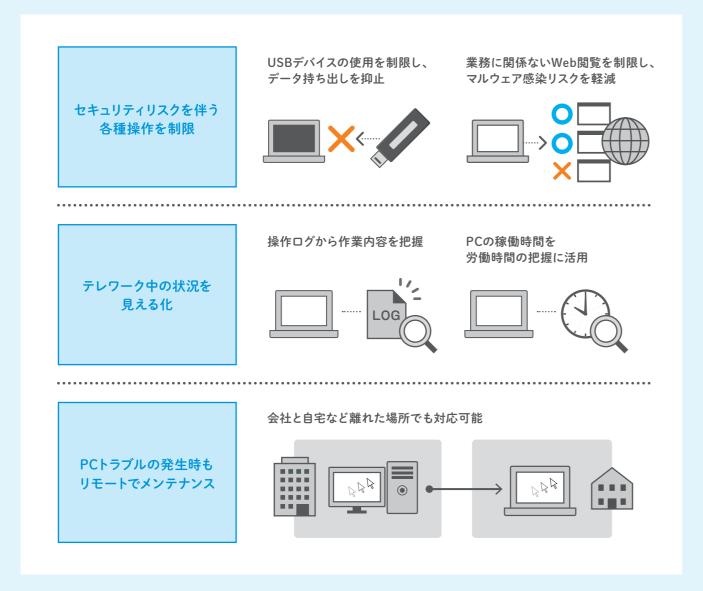


会社貸与PC持ち帰り

リモートデスクトップ

# 「SKYSEA Client View」で、 テレワークPCのセキュリティを万全に!

「SKYSEA Client View」を活用すれば、USBデバイスの使用など情報漏洩リスクを伴う操作を制限したり、脆弱性対策としてOS・セキュリティ製品の更新を徹底するなど、テレワークで利用するPCのセキュリティを強化できます。また、管理の目が届きづらいテレワークにおいて、PCの操作ログからテレワーク中の状況を見える化することも可能です。



#### SKYSEA Client Viewでは「テレワークEdition」をご用意しています

「テレワークEdition」には、上記の機能に加えて、テレワークをより安全に行うための各種セキュリティ対策を支援する「ITセキュリティ対策強化」機能や、情報の持ち出しを防ぐための「画面キャプチャー防止」機能などがご利用いただけます。詳しくは下記URLをご覧ください。

https://www.skyseaclientview.net/telework/edition/

シンクライアントシステム

# 「SKYDIV Desktop Client」で 安全・安心なテレワーク環境を構築!

「SKYDIV Desktop Client」は、国産ならではの強みを持つシンクライアントシステムです。開発から販売、導入後のサポートまでをすべて国内で対応しているほか、お客様のご要望を基に機能追加や改善を行い、定期的にバージョンアップを重ねているので、長く安心してご利用いただくことができます。

特長 **1** 

# わかりやすく使いやすい

#### 利用者の使いやすさ

#### 初めてでもすぐに使えるシンプルな操作性

デスクトップのアイコンをクリックするだけで、すぐに仮想環境でインターネットやアプリケーションを利用することができます。ローカル環境でアプリケーションを操作する場合と同じ感覚でご利用いただけます。

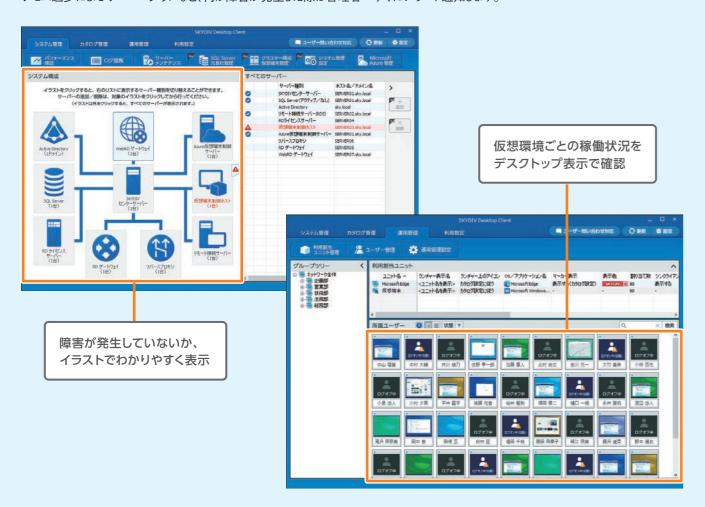


%1~SBC(RDS)方式でアプリケーションを使用している場合のみ、、マーカー表示されます。また、マーカー表示は任意でON / OFFが可能です。

#### 管理者の使いやすさ

#### 日々の管理業務を支援するグラフィカルな画面

仮想環境の利用状況をデスクトップ画面の一覧から確認できたり、サーバーの障害状況をイラストから視覚的に把握することができます。アクセス過多によるサーバーダウンなど、何か障害が発生した際は管理者へすぐにアラート通知します。



# 特長 **2**

# 開発からサポートまで すべて国内対応

技術資料 / マニュアルも日本語で提供

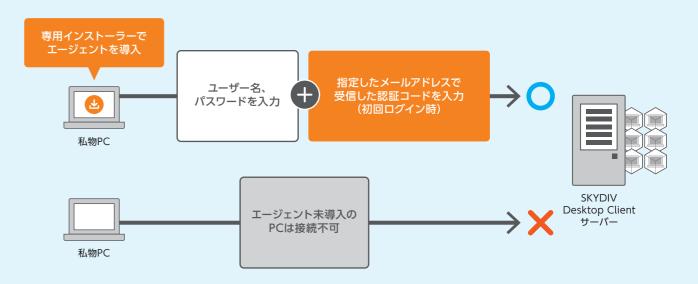
国内で利用されているシンクライアントシステムの多くは海外製のため、日本語環境にまつわるものなど国内特有のトラブルに関しては、問題解決に時間がかかることもあります。「SKYDIV Desktop Client」は、開発・販売からサポートまでをすべて国内で対応。「SKYSEA Client View」など自社開発の製品を通じて多くのお客様をサポートしてきた経験から、素早い対応を可能とします。またソフトウェアの画面上の文字はもちろん、技術資料やマニュアルも日本語を用いて制作しています。



# セキュリティ強化を サポートする各種機能

#### 私物PCからの認証を強化し、不正アクセスを抑止

私物PCから仮想環境を利用する際は、ユーザーごとに作成されたエージェントをあらかじめインストールし、認証時にメールで受信した認証 コードの入力が必要です。認証までのセキュリティを強固にしておくことで、第三者の不正なアクセスを防止します。



#### 仮想環境利用時のセキュリティを強化するポリシー設定

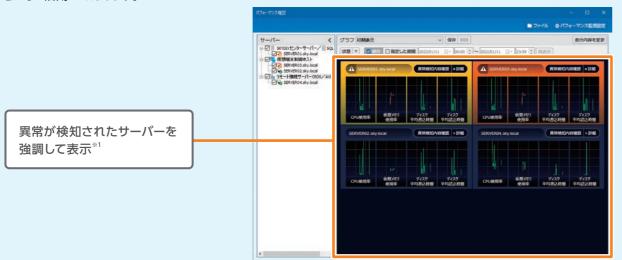
仮想環境でのUSBデバイスやプリンターの使用、ローカル環境とのクリップボード共有など、情報漏洩リスクを伴う操作を制限できます。設定操作もイラストをクリックするだけなので簡単です。



運用支援

# サーバーのパフォーマンスをグラフでわかりやすく表示

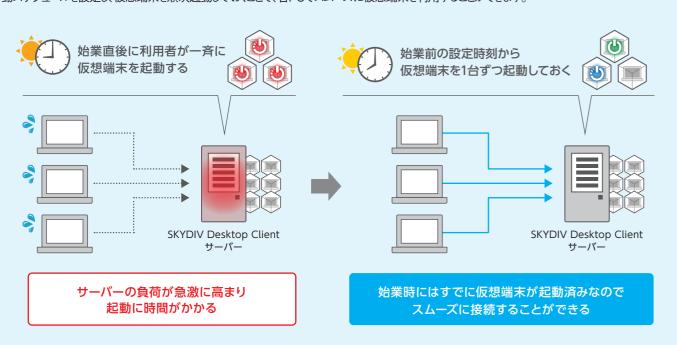
各サーバーのメモリ使用率やネットワークの送信・受信量など、パフォーマンスに関する情報をグラフから視覚的にチェックできます。リソースの使用状況やネットワークの負荷状況などサーバーの稼働状況を定期的に確認したり、トラブル発生時の状況把握や問題の切り分けなどにもご活用いただけます。



※1 異常を検知するための各項目のしきい値を別途指定することができます。

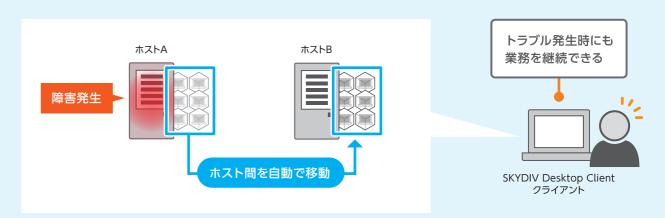
## 始業時の重くなりがちな仮想端末の起動をスムーズに

朝の始業時に多台数のPCが仮想端末を一斉に起動させると、サーバーに負荷が集中して時間がかかってしまうことがあります。管理者が事前に起動スケジュールを設定し、仮想端末を順次起動しておくことで、各PCでスムーズに仮想端末を利用することができます。



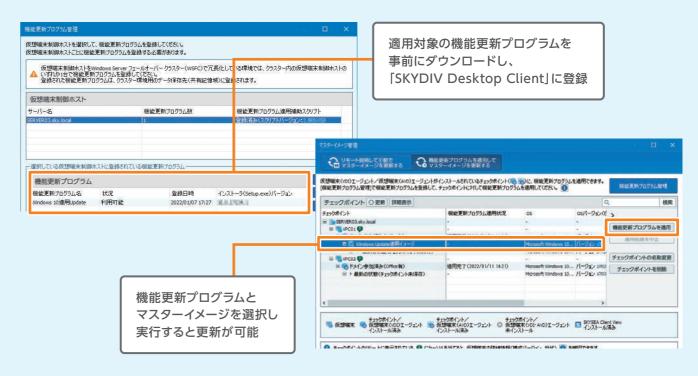
## トラブル発生時も安心して使い続けられる環境を構築

複数の仮想端末制御ホスト間で仮想端末の移動が可能な、クラスター(冗長化)環境に対応。トラブル発生時は別ホストへ仮想端末が移動し継続して利用できるため、業務停止期間を最小限に抑えることができます。管理画面上では、クラスター環境の構築や各ホストに登録された仮想端末の利用状況などが確認できます。



# 仮想環境でのWindows OSの大型アップデート作業を簡略化

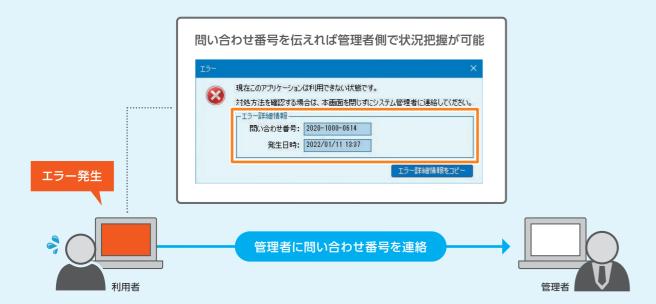
管理画面上でWindowsの機能更新プログラムとマスターイメージを選んで実行するだけで、複数の仮想環境の大型アップデートがまとめて行えます。仮想端末ごとにアップデートを行う必要がないため、作業効率化につなげていただけます。



#### トラブル対応

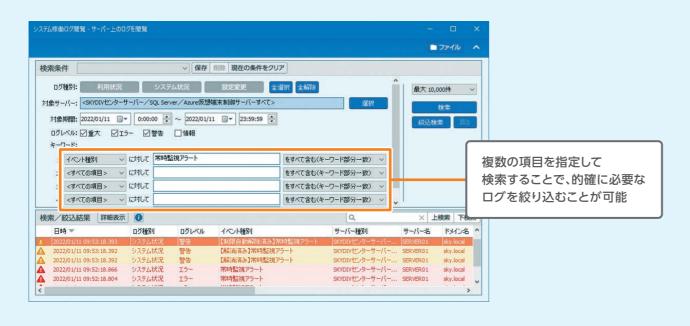
## "問い合わせ番号"からトラブルの状況把握を迅速に

仮想環境が起動しないなどのトラブルが発生した場合は、利用者のPCに問い合わせ番号が記載されたエラーメッセージを表示。利用者から状況を詳しく聞き取れない場合でも、問い合わせ番号からトラブルの詳細が把握でき、その後の対応につなげていただけます。



## 収集したサーバーのログから原因を調査

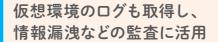
「SKYDIV Desktop Client」が出力するシステム稼働ログや、OSが出力するイベントを収集・管理。サーバーの障害が発生した場合に、該当するサーバーのログを絞り込んで確認することで、原因の調査などに活用いただけます。



#### 仮想環境の情報漏洩対策を「SKYSEA Client View」でさらに強化

「SKYDIV Desktop Client」の仮想環境に「SKYSEA Client View」を導入することで、ログによる状況把握や、リスクを伴う各種操作の制限、サイバー攻撃対策など、仮想端末上の情報漏洩対策をさらに強化することができます。仮想環境作成時に「SKYSEA Client View」を自動でインストールする設定をご用意していますので、導入も簡単に行っていただくことができます。\*1

※1 「SKYSEA Client View」のライセンスが別途必要です。

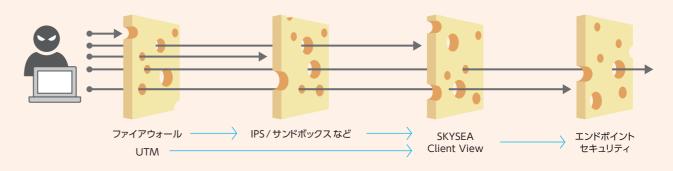


組織内の重要なデータが万が一にも持ち出されないように、仮想端末上で行われた操作もログとして記録し、内部不正の防止を支援します。



#### 連携製品との組み合わせで「多層防御」を支援

UTMやウイルス対策ソフトウェアなどの他社メーカー様の製品と連携することで、多層防御による情報漏洩対策の強化を支援。マルウェア感染などの異常を検知すると、管理者に通知し、端末をネットワークから遮断します。



#### 「SKYSEA Client View」と同期し、 メンテナンス作業を簡略化

「SKYSEA Client View」で管理している部署情報やクライアントPCの利用者情報を、「SKYDIV Desktop Client」のシステムへ定期的に同期できます。双方のソフトウェアを導入している環境において、システムの情報更新作業にかかる手間を軽減できます。





## ト 公式YouTube チャンネル



# 最新機能やテーマ別活用術、導入事例など、 SKYDIV Desktop Clientに関する動画を多数公開!



ご視聴はこちら



Q Sky株式会社 公式チャンネル

SKYDIV Desktop Client は "企業・団体・教育機関・医療機関"のお客様向け商品です

商品に関するお問い合わせや最新情報は …………

**SKYDIV** 

https://www.skydiv.jp/



- 法人名、企業名、学校名、病院名、代表電話番号などをお答えいただけない場合、ご利用できません。
- 教育機関、自治体、法人以外の方からのお問い合わせには対応いたしかねます。
- サービス・品質の向上とお問い合わせ内容などの確認のために、通話を録音させていただいております。

03-5860-2622(東京) 06-4807-6382(大阪)

受付時間 9:30~17:30 (土・日・祝、ならびに弊社の定める休業日を除く平日)

弊社は、Microsoft社の製品やテクノロジーをベースとしたサービスの開発 や販売を行うIT関連企業に対するパートナープログラム制度において、 「マイクロソフトGoldコンピテンシーパートナー」の認定を受けています。

# Microsoft Partner

Microsoft

# Sky株式会社 — https://www.skygroup.jp/—

■東京本社

東京都港区港南二丁目16番1号 品川イーストワンタワー15F

TEL.03-5796-2752 FAX.03-5796-2977

▮大阪本社 **〒532-0003** 

大阪市淀川区宮原3丁目4番30号 ニッセイ新大阪ビル20F

TEL.06-4807-6374 FAX.06-4807-6376

札幌支社 仙台支社 横浜支社 三島支社 名古屋支社 神戸支社

広島支社 松山支社 福岡支社 沖縄支社

<sup>●</sup>SKYDIV、SKYDIV Desktop Client、SKYSEA および SKYSEA Client View は、Sky株式会社の登録商標です。●Microsoft、Windows Server、Hyper-V、SQL Server および Microsoft 365 は、Microsoft Corporationの登録商標または商 標です。

「Inux®は、Linus Torvaldsの登録商標または商標です。

Mac は、Apple Incの登録商標または商標です。

Apple Incの登録商標または商標です。

Apple Incの登録商標または商標です。

Apple Incの登録商標または商標です。 複写、改変、転載することは、いかなる理由、形態を問わず禁じます。●本文中に記載されている事項は予告なく変更することがあります。