

レジリエンシー・オーケストレーションによる サイバー・インシデント・リカバリー

ハイブリッド・マルチクラウド環境において、迅速で
信頼性が高く、拡張が容易な、サイバー・レジリエンス
実現の復旧ソリューション



目次

- 2 変更は待ったなし
- 4 サイバー・レジリエンスへのアジャイルなアプローチを実現するアーキテクチャー
- 5 プラットフォーム構成用のサイバー・インシデント・リカバリー
- 6 データ用のサイバー・インシデント・リカバリー
- 7 管理をシンプルにするダッシュボードとレポート作成機能
- 8 Kyndrylをお勧めする理由

変更は待ったなし

オンプレミス、パブリッククラウド、マルチクラウドの環境を相互接続したインフラストラクチャー全体でのデータやアプリケーションの使用が増えるにつれ、サイバー攻撃者は企業の事業継続性を妨げる手口を増やしています。ハイブリッド・マルチクラウド環境の複雑な性質により、重要なデータやシステム構成がかつてないほど高いレベルのリスクにさらされ、そのためサイバー攻撃が成功する可能性が間違いなく高まっています。ITセキュリティ・チームがどれほど用心深くても、サイバー攻撃はやがては障害、データ盗難あるいはデータ破壊という形でビジネスの中断につながり、その結果評判が損なわれたり財政に悪影響が及ぶこととなります。

それほど遠くない過去には、最も一般的なサイバー攻撃による被害を軽減するのに、従来型の災害復旧ソリューションを頼りにすることができました。しかしそれはハイブリッド・マルチクラウド環境が実現するよりもずっと前のことでした。ITインフラストラクチャーが複雑に成長すると同時に、サイバー攻撃者もますます巧妙になってきています。今ではデータ暗号化とマルウェア攻撃は、かつては想像できなかったような方法でデータのバックアップをターゲットにするよう設計されています。その結果、これらの攻撃がバックアップや災害復旧のロケーションにアクセスできるようになり、本番データとバックアップ・データの両方が使用できなくなり、本来の業務の復旧が大幅に遅れてしまいます。

Kyndryl レジリエンシー・オーケストレーションによるサイバー・インシデント・リカバリーは、ハイブリッド・マルチクラウド環境全体にわたる迅速で信頼性が高く拡張が容易な復旧によって、サイバー攻撃によるビジネスへの影響を最小化します。

ハイブリッド・マルチクラウド専用のサイバー・リカバリー

Kyndryl™ レジリエンシー・オーケストレーションによるサイバー・インシデント・リカバリーでは、サイバー攻撃によりシステムが停止した際に、データやプラットフォーム構成を迅速に復旧することができます。データ保護と災害復旧ワークフローのインテリジェントな自動化を提供して、ハイブリッド・マルチクラウド環境全体で復旧テスト、データ不変性、異常検知、モニタリング、管理およびレポート作成を実現します。このソリューションは、サイバー攻撃を受けたビジネス・プロセス、アプリケーション、システムおよびデータベースを含む物理および仮想のワークロードに、自動化された信頼性の高い迅速な復旧を実現します。

サイバー・インシデント・リカバリーで以下が可能になります。

- 本番環境に影響を及ぼさない、簡単なテスト機能
- ダウンタイムの最小化につながる、データ破損の迅速な検知と迅速な対応
- リカバリー・ポイント目標 (RPO) を最適化する、効率的なポイント・イン・タイム・リカバリー
- 大規模なサイト・レベルでの検知とリカバリーを数分で行える、拡張の容易性
- シンプルな可視化機能と、レポート機能により、各種法規制への対応をサポート

Kyndryl レジリエンシー・オーケストレーションによるサイバー・インシデント・リカバリーは、サイバー攻撃を受けた物理およびデジタルのワークロードに、自動化された信頼性の高い迅速な復旧を実現します。



サイバー・レジリエンスへのアジャイルなアプローチを実現するアーキテクチャー

サイバー・インシデント・リカバリー機能を構成する技術要素は、コンピュータ・レイヤーとデータ・レイヤー双方のプラットフォームにわたり、本番環境と災害復旧環境の両方になります。これにより、仮想ワークロードと物理ワークロード全体でのリカバリーへのアジャイルなアプローチが実現されます。

イミュータブル・ストレージ(不変ストレージ)

構成データにイミュータブル・ストレージ(不変ストレージ)技術を使用し、アプリケーション・データに WORM(*)ストレージを使用することにより、一度保存されたバックアップの破損を防止し、確実なリカバリーを行うことができます。WORM(*):Write Once Read Many アプリケーション・データについては、この方法でポイント・イン・タイムの増分変更の新規コピーのみを書き込むことにより、ストレージ・コストの削減にもつながります。

エア・ギャップ保護

ネットワークを隔離することで、本番環境をリモートまたは災害復旧(DR)サイトで保護されている WORM ストレージのバックアップ・データと分離できます。また、WORM ストレージへのアクセスも、データのバックアップ時のみに制限されます。この方法をイミュータブル・ストレージ(不変ストレージ)と組み合わせることで、ネットワークをトラバースしたり、バックアップ・データを狙うマルウェアによる保護データの破壊を防止します。

異常検出

Kyndryl レジリエンシー・オーケストレーションには、人工知能(AI)により強化された、ルール・ベースのヒューリスティック ID を使用する異常検知機能が含まれます。これは既知のマルウェアのさまざまな変更パターンでトレーニングされており、バックアップ・データの変更パターンを収集して比較し、データの異常を高い精度で予測します。

この DR サイトでの異常検知機能は、バックアップされた異常なスナップショットを特定して、クリーン・コピーから復元するのに役立ちます。

構成データの検証

このコンポーネントは、組み込みの AI ベースの異常検知機能を使用して、保護対象の構成やデータがクリーンで復旧可能なものになるよう、サポートします。レジリエンシー・オーケストレーションに組み込まれたこのプロセスは、システム構成が変更されると、自動的に検出します。レジリエンシー・オーケストレーションをお客様のアプリケーション妥当性検証スクリプトと統合して、アプリケーション・レベルとデータ・レベルでのテストを行うこともできます。

オートメーションとオーケストレーション

レジリエンシー・オーケストレーションでは、データおよびアプリケーションの復旧プロセスをエンドツーエンドで自動化し、IT 環境の迅速な回復を実現します。レジリエンシー・オーケストレーションは、従来の手動のプロセスを、テスト・検証済みの事前定義されたワークフローに置き換えます。これにより、ボタンをクリックするだけで、ビジネス・プロセス全体、アプリケーション、データベース、または個別のシステムを復旧できます。これらのワークフローは、相互接続されたシステムやデータの復旧に必要な複数の手順を統合したもので、人的ミスを防ぎます。レジリエンシー・オーケストレーションは、ワークフロー定義に使える部品(事前に定義されたパターン)を 800 種を超えるライブラリーとして用意することによって、ソリューション実装までの時間の短縮を実現します。

プラットフォーム構成用のサイバー・インシデント・リカバリー

マルチウェアはデータ自体を破壊する前に構成を変更することがよくあります。そのため実際のデータが感染する前に、どんな構成変更でも検出することが重要です。サイバー・インシデント・リカバリーのプラットフォーム構成機能は、オンプレミス、パブリッククラウド、ハイブリッドクラウド、およびマルチクラウドの環境にわたり、仮想および物理のワークロード、アプリケーション、ストレージ・システム、ネットワーク・デバイスの構成データを保護します。

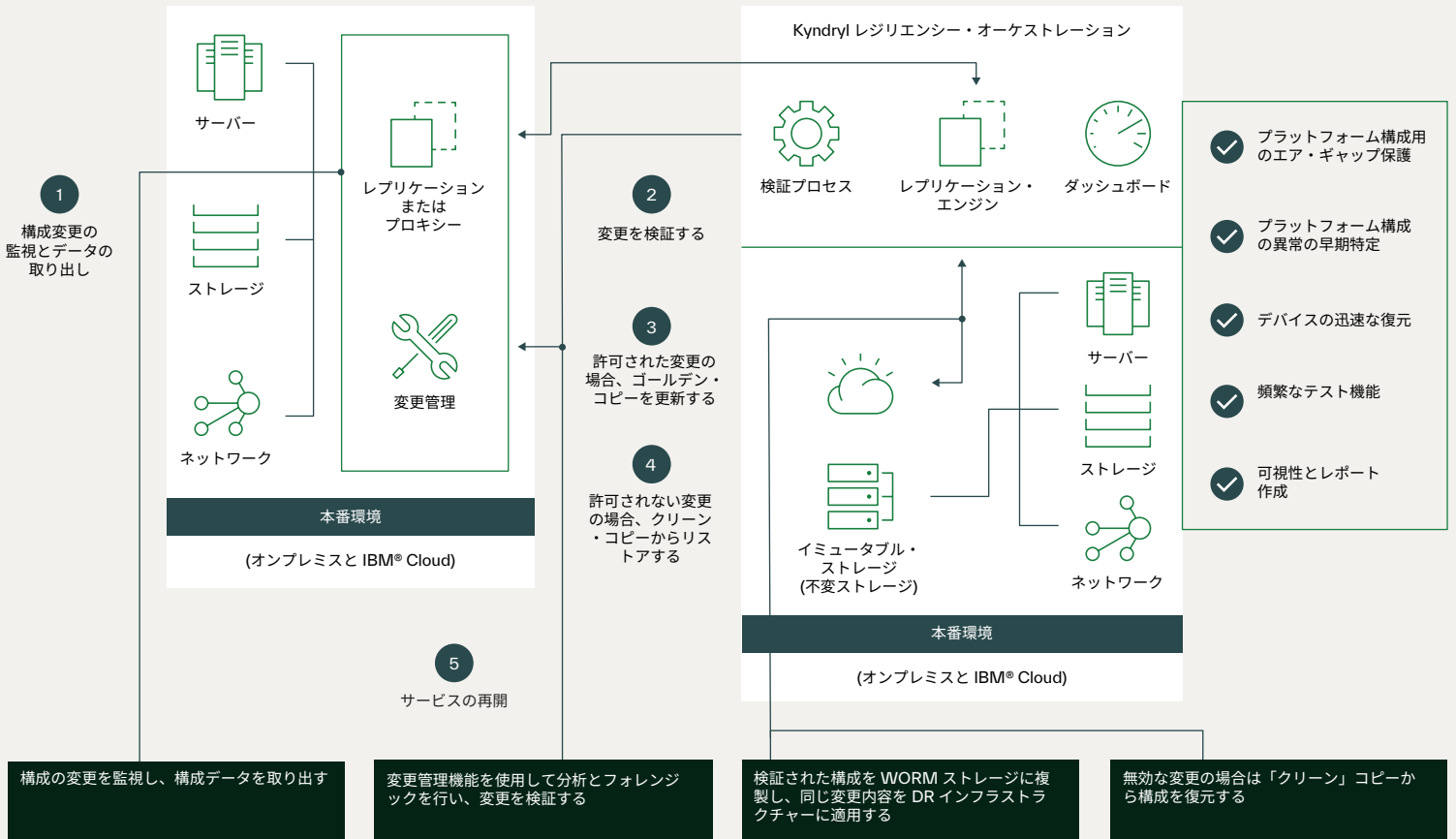
「ゴールデン・コピー」でビジネスを継続する

このコンポーネントは組み込みのテクノロジーを使用して、本番環境のエンドポイント構成のどんな変更も特定し、許可および無許可の変更をユーザーにアラートします。また、このアラートによって、変更制御管理ソフトウェアから関連するチケットが発行されます。短時間でサービス回復を実現するために、サイバー・インシデント・リカバリーは、サーバーやデバイス構成データの「ゴールデン・コピー」を、エア・ギャップで保護されたイミュータブル・ストレージ (不変ストレージ) に複製します。

無効および有効な構成変更への対応

有効な変更であった場合、構成データは新しい「ゴールデン・コピー」をイミュータブル・ストレージ (不変ストレージ) に複製することで保護されます。無効な変更が検知された場合、レジリエンシー・オーケストレーションが事前準備されたポリシーと適切な承認に基づいて、デバイス構成の最新のクリーン・コピーを本番環境に即時に復旧します。専用の仮想マシン構成は、クリーンな本番環境に復旧されます。有効な変更の場合には、イミュータブル・ストレージ (不変ストレージ) 内に新しい「ゴールデン・コピー」が作成されます。

Kyndryl Cyber Recovery as a Service
プラットフォーム構成用のサイバー・インシデント・リカバリー



*エア・ギャップはクラウドでホストされるイミュータブル・ストレージ (不変ストレージ) ではサポートされない

データ用のサイバー・インシデント・リカバリー

サイバー・インシデント・リカバリーのデータ機能は、データそのものを破壊するサイバー攻撃に対して、信頼性の高い、短時間での復旧を実現します。この機能は、エア・ギャップによる保護およびイミュータブル・ストレージ (不変ストレージ) を使用することでデータを保護しながら、災害復旧サイトで迅速に復旧を行います。

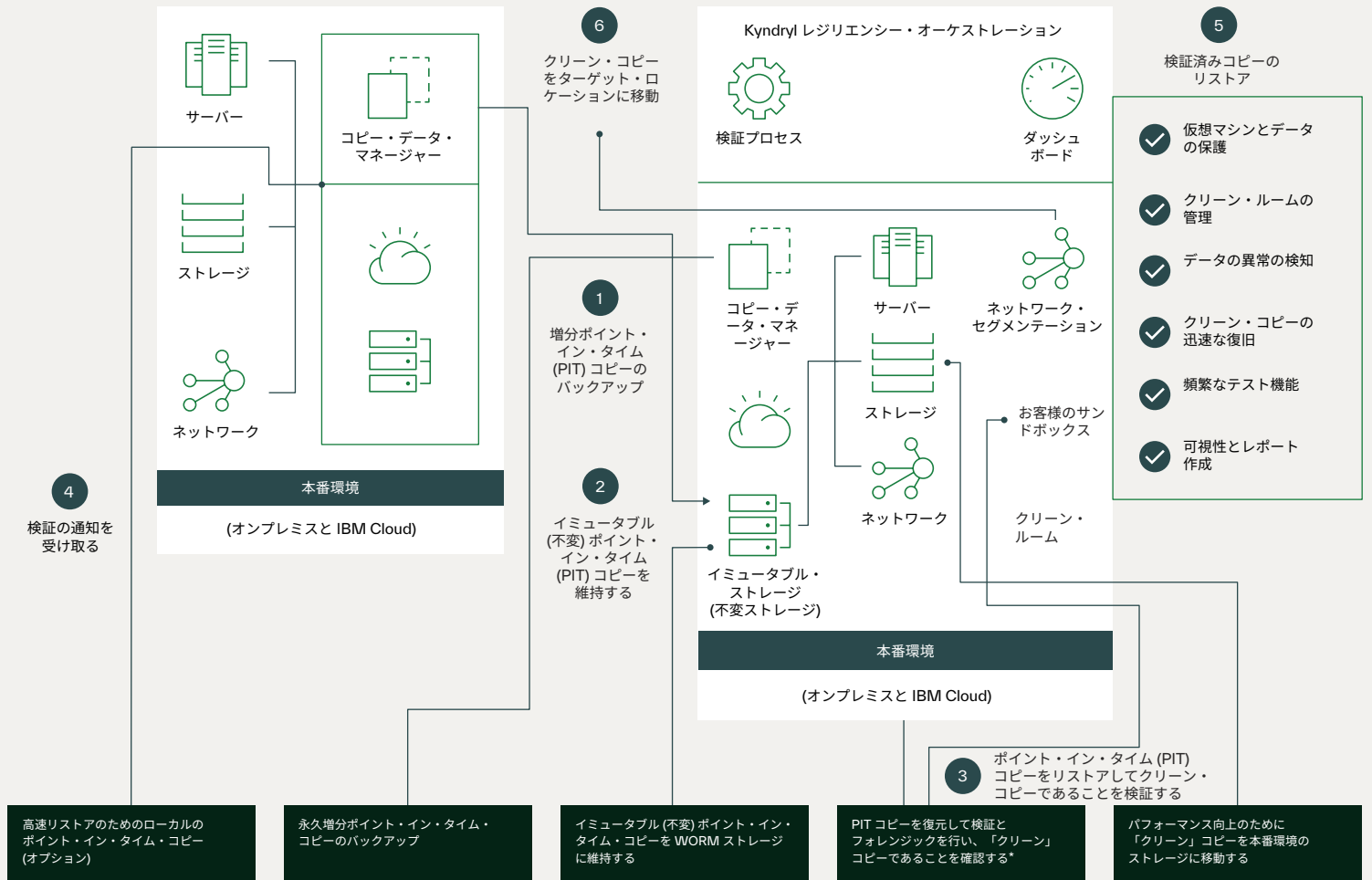
あらゆる環境にわたる大量のデータの保護

サイバー・インシデント・リカバリーは、大規模なアプリケーション・データがどこにあっても、それを扱うことを想定して設計されています。コピー・データ管理テクノロジーを採用し、データの増分ポイント・イン・タイム (PIT) コピーを作成して保持します。クラウド・オブジェクト・ストレージまたは WORM ストレージなどのイミュータブル・ストレージ (不変ストレージ) に保持されるこれらのコピーは、変更ができない「永久」コピーです。コピー・データ管理ソフトウェアは、データを災害復旧サイト (代替サイト) に複製し、ポイント・イン・タイム (PIT) コピーを作成します。ポイント・イン・タイム (PIT) コピーを本番サイトに保管することで、迅速な復旧を実現することもできます。

サイバー攻撃に迅速に対応して事業継続性を維持する

データ・ブリーチや暗号化のマルウェア感染が検知されたという通知を災害復旧管理者が受け取ると、災害復旧サイトでポイント・イン・タイム (PIT) コピーの自動テストが実行され、データの復旧の可能性を検証します。テストや検証のプロセスで最新の「クリーン」コピーとして判別されると、そのコピーはレジリエンシー・オーケストレーション・ソフトウェアにより災害復旧インフラストラクチャー上で復旧されます。災害復旧サイトでテストを頻繁に実施することで、ビジネス・オペレーションに影響を与えることなく、データの復旧の可能性を確認することもできます。レジリエンシー・オーケストレーションは、プラットフォームを短時間で並行して復旧できるようサポートします。

Kyndryl Cyber Recovery as a Service
データ用のサイバー・インシデント・リカバリー



管理をシンプルにするダッシュボードと レポート作成機能

サイバー・インシデント・リカバリーには、サイバー・リカバリー管理や、プラットフォーム構成の変更やデータの変更のモニタリングをシンプルにするダッシュボードがあります。これは RPO や目標復旧時間 (RTO) の偏差や、スナップショット検証状況、重要なサイバー・リカバリー更新情報を、リアルタイムで可視化します。

その間に、上級経営陣または取締役会は重要なサイバー・リカバリー更新情報をリアルタイムで受け取って、情報に基づいて迅速な意思決定を行うことができます。

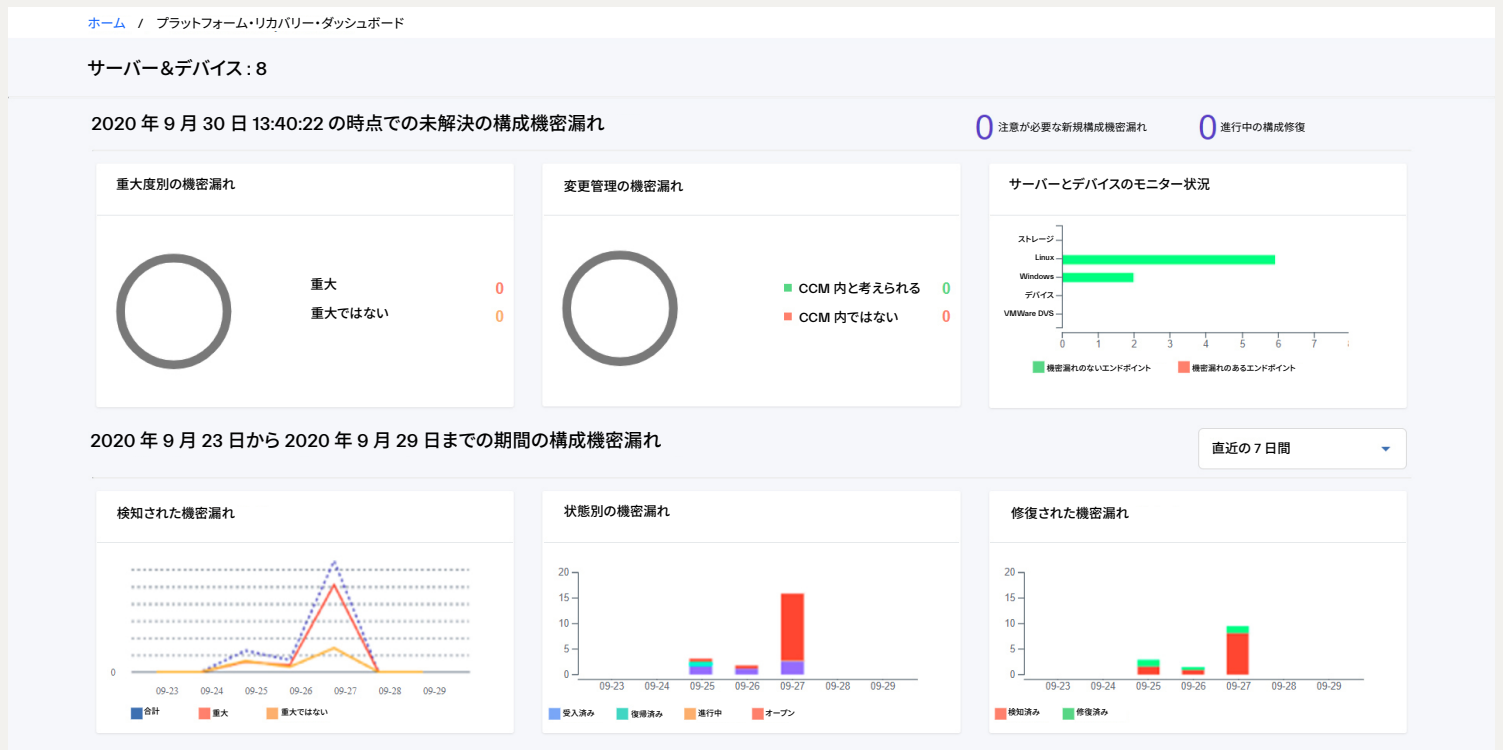
脆弱性の追跡と可視性の向上

サイバー・インシデント・リカバリー・ダッシュボードでは、ご使用の環境全体に存在する脆弱性の数と、各脆弱性の重大度レベルが表示されます。サイバー RPO 偏差、サイバー RTO 偏差、スナップショット検証状況、サイバー攻撃に対する現在の準備状況の可視化により、未解決の脆弱性を追跡して、情報に基づく意思決定を行うことができます。

堅固なレポート作成機能

レポート作成機能を活用すれば、サイバー・レジリエンスや災害復旧体制などの豊富なレポートを活用して、通常のオペレーションで作成したグラフと併せて、規制当局に提出し、コンプライアンス対応を容易に実施することができます。

サイバー・インシデント・リカバリーは、RPO や RTO の偏差や、スナップショット検証状況、重要な更新情報を、リアルタイムで可視化します



Kyndryl レジリエンシー・サービスには、世界中のお客様のバックアップや復旧の各種ご要望に何十年も対応してきた豊富な経験があります。

Kyndryl のメリット

- レジリエンシーのライフサイクル全体にわたる専門知識
- 物理、仮想、クラウドのワークロードの自動リカバリー
- 800 を超える定義済みパターンを使用して、迅速かつ効率的な実装と拡張性を実現
- エンタープライズ・レベルの拡張性のためのクラウドの選択肢 (AWS、Azure、IBM Cloud など)

安心

- 9,000 社を超えるお客様が、Kyndryl の災害復旧とデータ管理のサービスで保護されています。
- Kyndryl は年間 3.5 エクサバイト以上をバックアップおよび管理しています。

グローバル展開

- 世界中の 50 カ国以上に 300 を超える IBM レジリエンシー・センターがあります。
- IBM は世界中に 6,000 人以上の専門家を確保し、レジリエンシーへの対応を行っています。

Kyndrylをお勧めする理由

キンドリルには、世界に必要な不可欠なテクノロジー・システムをデザイン、構築、運用する豊富な専門知識があります。私たちは、社会を成長へと導く重要なインフラストラクチャーを発展させることに全力を尽くします。私たちは、新たな方法でシステムを作り出すことで優れた基盤を構築しています。適切なパートナーを選定し、ビジネスに投資し、お客様とともに課題に向き合い、新たな可能性を解き放ちます。

kyndryl

© Copyright Kyndryl Inc. 2021

キンドリルジャパン合同会社
〒103-0015
東京都中央区日本橋箱崎町19-21

Kyndryl は、米国もしくはその他の国における Kyndryl Inc. の商標または登録商標です。他の製品名およびサービス名等は、それぞれ Kyndryl Inc. または他社の商標である場合があります。本資料は発行時点で最新のものであり、キンドリルが随時予告なしに変更する可能性があります。キンドリルが事業展開するすべての国で、全製品もしくはサービスが利用できるわけではありません。キンドリルの製品およびサービスは、提供されている契約書の条件および制約に基づき保証されます。記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。キンドリルの製品およびサービスは、提供されている契約書の条件および制約に基づき保証されます。

詳細はこちらから →