


SECURITY SOLUTION



サーバーバックアップシステム

ランサムウェアから 企業データを守る

ITソリューションプロバイダー

 株式会社さくらコミュニケーション



 商号	株式会社 さくらコミュニケーション Sakura Communication Co., Ltd.	
 資本金	3,000万円	
 取引銀行	西武信用金庫 / みずほ銀行 / 三井住友銀行 / りそな銀行	
 役員	取締役社長 鈴木 祐一 取締役 桑村 時生	代表取締役 松尾 浩 執行役員 荒木 泰孝
 主要業務	<ul style="list-style-type: none"> ● ソフトウェアの開発・維持・管理 ● ITインフラ基盤設計・構築・運用 ● 海外事業者向けビジネス構築サービス ● 海外オフショア開発サービス ● WEBサイト制作・運営・管理 ● エンジニアの派遣 ● 国内事業者向けICTコンサルティング 	
 認許可	Pマークプライバシーマーク (10825146) 派遣労働者派遣事業 (派13-309616) テレワーク東京ルール実践企業宣言 地方創生テレワーク推進運動Action宣言	
	85名	
 加入団体	NPO法人 JASIPA (Japan System Integration Partners Association)	
 主要取引先	国土交通省（MLIT） / 情報通信研究機構（NICT） / 一般財団法人 調布市市民サービス公社 / 日本電気 株式会社 / NECソリューションイノベータ 株式会社 / 株式会社 アグレックス / 株式会社 ウォールナット / 株式会社 エヌアイデイ / 株式会社 東邦システムサイエンス / 日本自動化開発 株式会社 / 日本デイベレイク 株式会社	

バックアップシステムの重要性

データ喪失のリスクは常に存在します。予期せぬトラブルから企業資産を守るために。

システム障害



OSのクラッシュ、パッチ適用の失敗、ソフトウェアの不具合などにより、突然データにアクセスできなくなるリスク。

ウイルス感染



ランサムウェアによるデータの暗号化や、標的型攻撃によるデータの破壊・改ざんの脅威。

SOLUTION



バックアップにより、復旧可能

誤操作・削除



重要なファイルの誤削除、上書き保存、設定ミスなど、人為的なミスによるデータ消失。

ハードウェア故障



HDD/SSDの破損、サーバー機器の老朽化、自然災害（雷・水害）による物理的な故障。



これらのリスクは予測が難しく、発生時のビジネスインパクトは甚大です。
適切なバックアップ運用は、ビジネス継続計画（BCP）の中核となります。

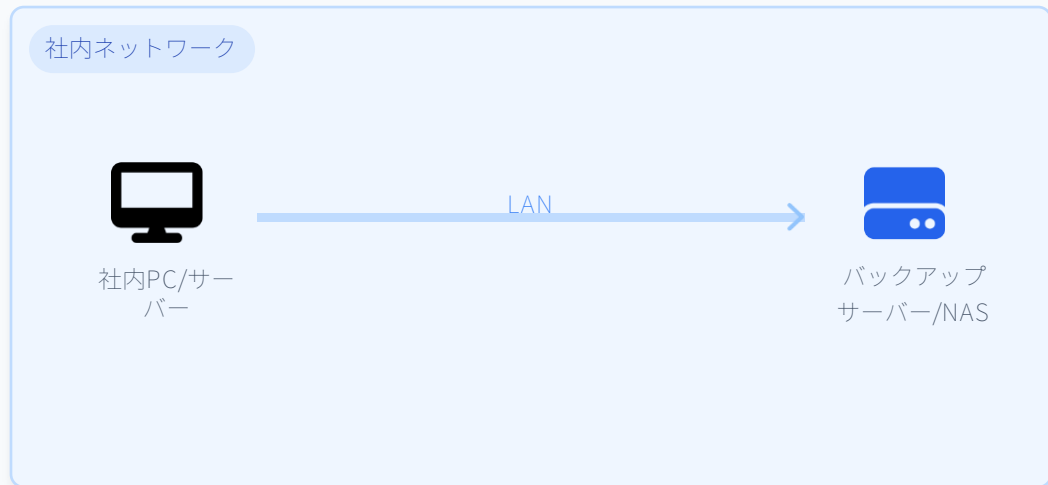
バックアップシステムの各種方法

企業のニーズに合わせて選択可能な2つの主要なアプローチ



オンプレミス

On-Premises Backup



社内に物理的なストレージやハードウェアを用意し、管理する従来型の方式です。

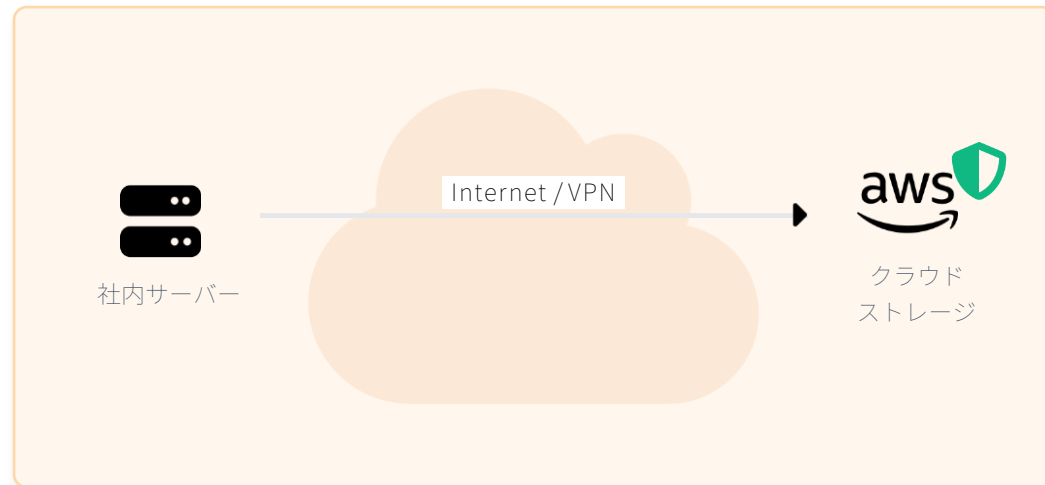
社内ネットワークを経由して、高速にバックアップデータを保管

インターネット切断時もバックアップ・復旧が可能



クラウド

Cloud Backup (AWS)



インターネットを経由して、AWS（アマゾンウェブサービス）などの高信頼クラウドにデータを保管します。

物理的なハードウェア管理が不要

地理的に離れた場所へ保管するため、災害対策（DR）として有効



※バックアップ頻度は、毎日・毎週・毎月など、お客様の要件に合わせて自由に設定できます。

各バックアップ方式のメリット比較

自社の運用ポリシーやセキュリティ要件に合わせて最適な方式を選定するための比較



オンプレミス

On-Premises



物理的に自社管理ができる

サーバーやストレージを物理的に管理できるため、アクセス権限やセキュリティ設定を自社の厳格なポリシーに合わせて自由に制御可能です。



復旧作業が早い

社内ネットワーク（LAN）内でのデータ転送となるため、インターネット回線の帯域に依存せず、大容量データでも即座に高速復旧が可能です。

VS



クラウド

Cloud (AWS)



災害に強い（BCP対策）

データセンターが地理的に分散しているため、本社が被災した場合でもバックアップデータは安全に保全され、事業継続性を確保できます。



高度なセキュリティ

クラウドベンダーによる多層的なセキュリティ対策、暗号化、アクセス制御により、データを強固に保護します。常に最新のセキュリティが適用されます。

オンプレミス・バックアップの特徴

自社環境でデータを管理・保護する従来型アプローチの強み

01



社内データ保管

自社内でデータを安全に保管し、外部からのアクセスを完全に遮断します。物理的なセキュリティ対策と組み合わせることで、最高レベルの機密性を確保することが可能です。

02



迅速なデータ復旧

オンプレミス環境でのバックアップにより、ネットワーク遅延なしで迅速にデータを復旧できます。大容量データであっても、業務停止時間（ダウンタイム）を最小限に抑えることが可能です。

03



世代管理

毎晩のバックアップなどで複数世代にわたるデータ管理を行います。「昨日のデータに戻したい」「1週間前の状態が必要」といった、過去のバージョンへの柔軟なロールバックが可能です。

オンプレミス構成図

堅牢なセキュリティと高速なバックアップを実現するシステムアーキテクチャ



データフロー設定

日次：変更部分のみの「増分/差分」バックアップで時間を短縮。週次/月次：システム全体の「フルバックアップ」を取得し、完全な復旧ポイントを確保。

セキュリティ対策

ネットワーク分離：バックアップ専用VLANを構築し、通常業務LANからのマルウェア拡散を防止。
WORM機能：「書き込み一度、読み取り何度でも」の設定で、データの改ざん・削除を物理的に防止。

オフサイト保管（オプション）

テープメディア等を定期的に遠隔地へ搬送することで、火災や地震などの物理的災害リスクに対応します（3-2-1ルールの実践）。

クラウド・バックアップの特徴

AWS基盤を活用した堅牢かつ柔軟なデータ保護ソリューション

01



高度なセキュリティ

クラウド環境での多層的なセキュリティ対策により、データを強固に保護します。最新の暗号化技術や厳格な認証システムを駆使し、不正アクセスや情報漏洩を未然に防ぎます。

02



AWSストレージの信頼性

世界的に信頼されるAWSのインフラを使用し、データの安全性と可用性を確保します。極めて高い耐久性を持つ冗長設計により、データロスのリスクを実質的にゼロに近づけます。

03

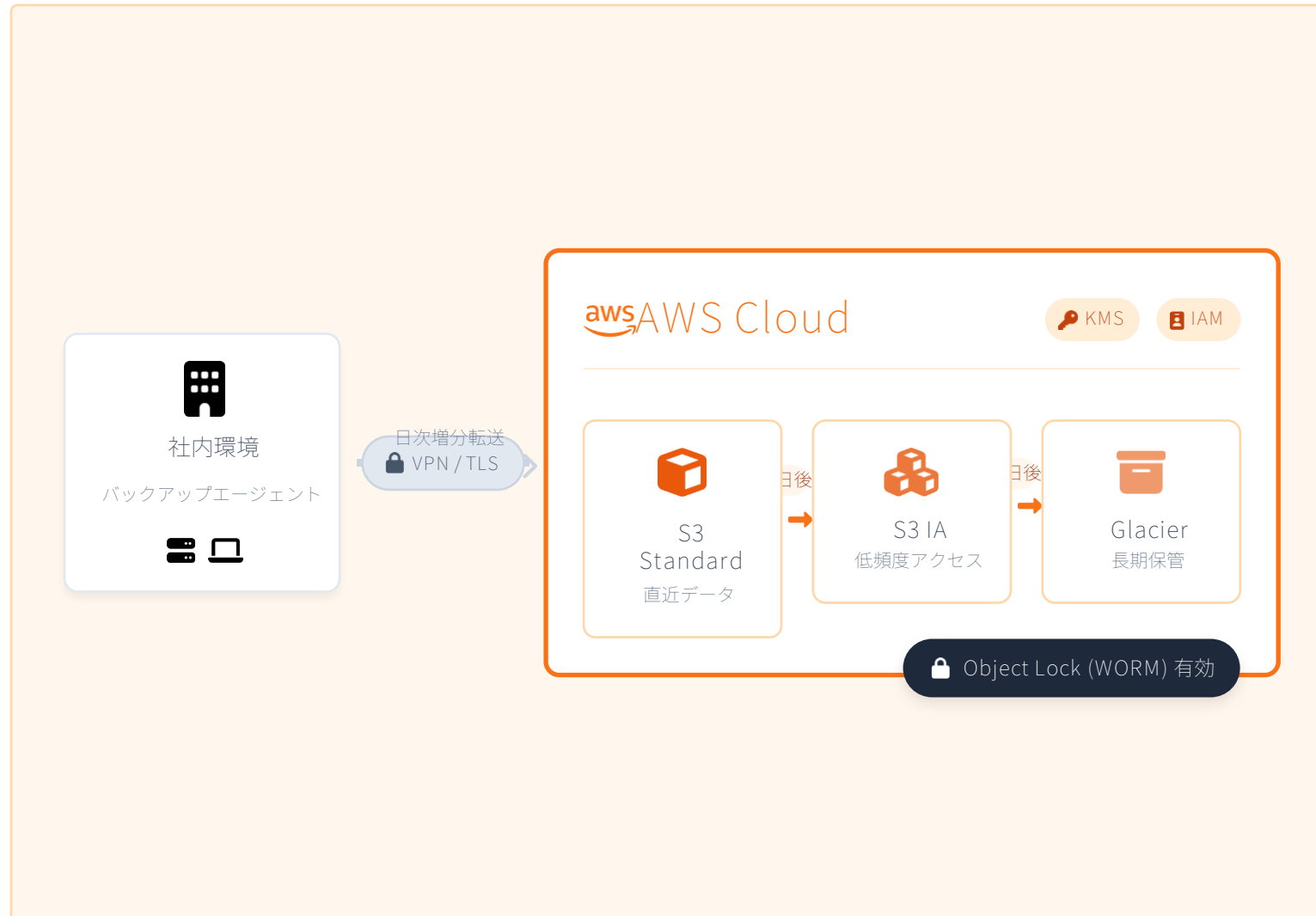


冗長性・スケーラビリティ

クラウドならではの柔軟性を活かし、データ量の増加にも即座に対応可能です。必要な分だけリソースを利用するため、コスト効率の高い最適なストレージ運用を実現します。

クラウド構成図

AWS基盤を活用した堅牢なバックアップアーキテクチャ



ライフサイクル管理

データの鮮度に応じて、S3 Standard（高頻度）からGlacier（長期アーカイブ）へ自動的にデータを移動。コストを最適化しながら長期保存を実現します。

暗号化とアクセス制御

転送経路はSSL/TLSで暗号化し、保管データはAWS KMSで暗号化。IAMによる厳格なアクセス権限管理で、許可された管理者のみが操作可能です。

改ざん防止（WORM）

S3 Object Lock機能により、設定期間内は管理者であってもデータの削除や変更が不可能になります。ランサムウェア対策として極めて有効です。

ハイブリッド・バックアップの特徴

オンプレミスの即時性とクラウドの冗長性を組み合わせた最適解

01



オンプレミスの即時性

ローカルでのバックアップ運用により、迅速なデータアクセスと復旧を実現します。日常的な運用において、業務への影響を最小限に抑え、スムーズなリストアが可能です。

02



クラウドの冗長性

クラウドへの遠隔バックアップで、災害時のデータ保護を強化します。地理的に分散したデータ保管を実現し、BCP（事業継続計画）対策としても極めて有効です。

03



柔軟な運用

オンプレミスとクラウドを組み合わせることで、データの重要度に応じた最適な保護戦略を立てられます。コストとパフォーマンスのバランスを考慮し、効率的な運用設計が可能です。

ハイブリッド構成図

オンプレミスの即時性とクラウドの冗長性を統合した最適解

✓ 3-2-1 ルール準拠システム

オンプレミス



業務サーバー群
VM / 物理サーバー



ローカルNAS
一次バックアップ

高速リストア

スケジュール複製

重複排除
暗号化転送

aws クラウド (AWS)



S3 バケット
二次バックアップ

WORM保護



S3 Glacier
長期保管アーカイブ

コスト最適化



階層化バックアップ

直近データはローカルNASで即時復旧。古いデータはクラウドへ自動転送し、運用コストを最適化します。



BCP・災害対策

データを物理的に離れたクラウドへ複製。オフィスが被災してもデータは安全に守られます。



ランサムウェア対策

クラウド側で「不可変 (Immutable)」設定を適用。管理者権限でも削除できない最強の保護を実現。

データ復旧作業の流れ

緊急時に確実な業務再開を実現するための3ステップ



復旧フロー図解

障害発生から業務再開までの標準対応プロセス



バックアップ計画の策定

業務継続性を確保するための4つの循環プロセス



バックアップ設定例

対象システム	優先度	設定方針 (頻度 / 期間 / 場所)
基幹システム 会計・人事・販売管理	高	頻度: 毎日 (夜間フル + 日中増分) 期間: 7年 (法令対応) 場所: ハイブリッド (WORM)
ファイルサーバー 共有ドキュメント	中	頻度: 毎日 (夜間増分) 期間: 1年 場所: オンプレミス + クラウド
一般PC端末 カルデータ	低	頻度: 週1回 期間: 1ヶ月 場所: クラウド (個人領域)

システム更新や組織変更のタイミングで、少なくとも年1回は計画の見直し（Step 4）を実施することを推奨します。

Next Step

ランサムウェアから 企業データを守る

最適なバックアップを。

現状のバックアップ体制に不安はありませんか？

ヒアリングから要件定義、PoC（概念実証）まで、

貴社の課題に合わせたソリューションをご提案します。

- ✓ 無料相談・現状診断
- ✓ お見積り・構成案作成



Simple. Secure

株式会社さくらコミュニケーション

Sakura Communication Co., Ltd.



Official Website

<https://www.sakura-communication.co.jp>