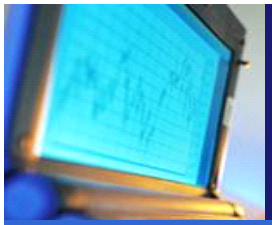
遠隔（リモート）バックアップサービス
CryptoRemoteBackup

BCPソリューション

glovix 株式会社グロービクス

目次

glovix
株式会社グロービクス



現状のバックアップの主な問題点と弊社の着眼点

現状のバックアップの主な問題点：

- 生データをそのままクラウドに保存していること！
- 事業部等のファイルサーバーの多くは、物理的な、別環境への自動バックアップ化は出来ていないこと！
- ほとんどは、社内のHDDの二重化までであること！
- 情報管理や、復帰作業は、システム管理者にあること！

弊社の着目点：

- 暗号化して保存することで、IDやパスワードが万が一漏れても安全であること！
- 専用線やVPNを使わなくても、暗号化したファイルをSSLを使用して、通常の安価なインターネット網を使用して送受信でき安全であること！
- 暗号化は世界標準のRSA方式であること！
- システム管理者はシステム管理のみであり、情報管理のイニチアシブは経営層であること。しかし、実作業は一般社員であること！

これらを解決するソリューションをご提供します！

glovix
株式会社グロービクス

従来のバックアップとの違い

❖ 通常バックアップ と
遠隔（リモート）バックアップサービスとの違い

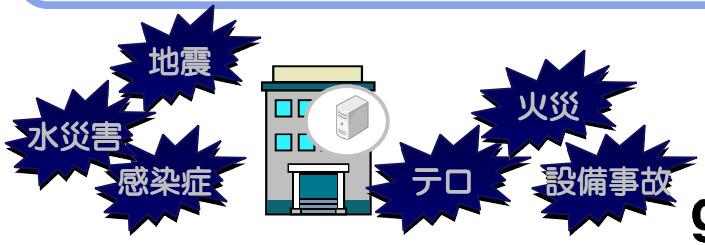
- 通常：　ディスク全体、ディレクトリ全体
- BCP：　日常の業務で、重要性の高いファイルやフォルダーを
暗号化して保管、非常時は決済権限者の指示により、鍵により**ファイル複合**、
速やかな業務再開をセキュリティ機能付きで実現します。
- 保管先：　データセンター等の会社とは遠隔地に保管します。
データセンター等の安全・安心を更に強固にします。

暗号化、鍵をかけて保管

24時間、常時ログ監視

権限者のみ復号

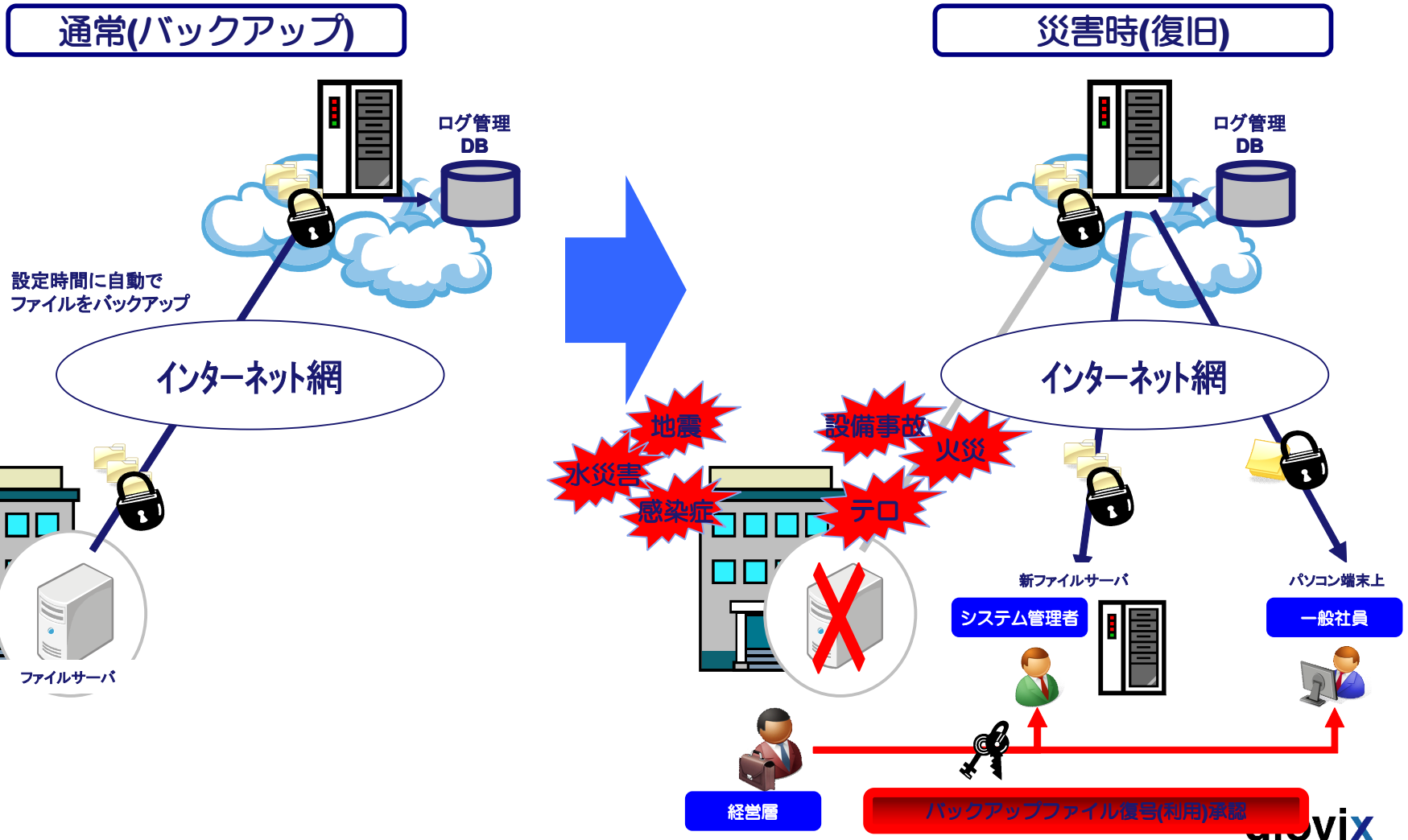
暗号化（**RSA**方式）機能付きで
バックアップを更に強固に！



glovix
株式会社グロービクス

遠隔(リモート)ﾊﾞｯｸｱｯﾌﾟｻｰﾋﾞｽの概要

自動化により、ファイルサーバーにある重要データを暗号化した後に、クラウド環境にデータバックアップを行うサービスです。



株式会社グロービクス

サービスの特徴

1.暗号化により安全にクラウド環境に保管します

タスクスケジュールに基づいて、対象ファイルを**ファイルサーバー側で暗号化(RSA方式)**してバックアップ処理を行います。万が一データが盗まれても、暗号化されているため安全です。

2.煩雑なバックアップ業務を自動化します

煩雑なバックアップ業務を、タスクスケジュール設定より自動化することで、**人為的ミスのリスク軽減及び業務コストの削減**を可能にします。

3.安全に通常回線でアップロードできます

暗号化後に転送する為、**原則として専用線やVPN、SSL等を使わなくても、**通常の安価なインターネット網を使用しての安全な送受信を可能にします。

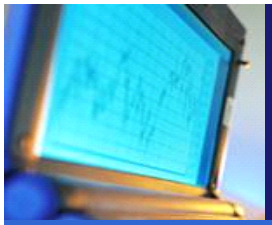
4.データの最終決裁権限は経営層にあります

システム管理者はシステム管理のみを基本とします。**情報管理のイニチアシブは経営層**であり、**実作業は一般社員である**という**明確な権限(ユーザー)管理を行っています。**

5.安否確認機能連携で緊急対応を強化します

安否確認機能と連携する事により、一斉指示による**緊急時の迅速なリカバリーを可能**にすると共に、従業員の安否状況の把握により、**的確な復旧作業を実現**します。

glovix
株式会社グロービクス



強固なセキュリティ

RSA暗号による公開鍵方式

パスワードに基づくセキュリティではなく、AES/RSA暗号により、強固なセキュリティを実現。環境設定時に公開鍵と秘密鍵を生成、公開鍵をお客様の ファイルサーバ、秘密鍵をバックアップサーバに厳重に保管し暗号バックアップを行います。

ファイル暗号化×SSH通信

バックアップ元のファイルサーバとリモートバックアップサーバをグローバルIPでの認証によるSSH通信採用、ネットワーク上を流れるデータは暗号化され るため、通常インターネット回線経由でも、更に安全なデータアップロードを実現します。

厳重な鍵管理

生成された鍵は、万が一の鍵破損に備えて、何重にもバックアップをとるなど、万全な保管体制でお客様のデータを守ります。

ファイル復号は経営層権限

復旧(リストア)の際には、システム管理者及び社員はファイルのダウンロードは出来ても、経営層 (BCP責任者)のパスワードがなければ復号できない仕組みになっております。

ユーザーパスワード管理

ログイン時に、パスワードを規定数間違えるとユーザーアカウントを規定時間ロック、更にそれらの操作を規定数回行った場合は、ユーザーアカウントがロック され管理者のみが解除できるようにするなど、厳しいパスワード管理により更に安全性を高めます。

glovix
株式会社グロービクス

運用フロー概要

ユーザー	事前準備	復旧作業
システム管理者 (運用責任者)	1.BCPサービス初期導入 2.保管運用ケジュール設定 3.一般ユーザー登録	1.復号パスワード申請 2.一括復号処理(全データ)
経営層ユーザー (最終決裁者)	1.経営層ユーザー登録 2.復号パスワード設定	1.復号パスワード通知の承認
一般ユーザー (実務担当者)	1.ユーザーパスワード変更	1.復号パスワード申請 2.復号処理(ファイル単位)

暗号化（RSA方式）機能付きバックアップ処理

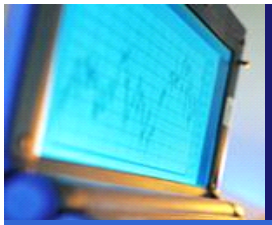
申請

許可

許可

申請

glovix



厚生労働省
医療情報システムの安全管理に関するガイドライン対応

危険性と対策方法	セキュリティ対応策
盗聴 医療機関等においてネットワークを通じて情報を伝送する場合には、万が一、伝送途中で情報が盗み取られたり、意図しない情報漏えいや誤送信等が発生した場合でも、医療情報を保護するために暗号化など適切な処置を取る必要がある。少なくとも情報を伝送し、医療機関等の設備から情報が送出される段階においては暗号化されていることが望ましい。	**世界標準AES/RSA暗号化** バックアップ元のファイルサーバで暗号化した後にリモートバックアップサーバにアップロードするので、通信上及びバックアップサーバ上では**データは全て暗号化されています。**何らかの事象により万が一情報漏洩した場合でも安心です。
	ファイル復号は経営層権限 暗号化されたデータを復号する際は、**経営層の承認が無ければ復号が出来ない**仕様になっている為、大切なデータを勝手に見られる心配はありません。
なりすまし 情報を送ろうとする医療機関等は、送信元及び送信先は双方で意図した相手であるかを確認しなくてはならない。例えば通信の起点と終点の機関を適切に識別するために、公開鍵方式や共有鍵方式等の確立された認証の仕組みを用いてネットワークに入る前と出た後で相互に認証する等の対応を取ることが考えられる。	**SSH通信(グローバルIP認証)** バックアップ元のファイルサーバとリモートバックアップサーバはそれぞれの**グローバルIPの認証により、秘密鍵及び暗号鍵を用いた暗号通信を行う**ので、なりすましをされる心配はありません。
	ユーザーパスワード管理 登録後一定期間パスワード変更を行わなかったり、指定時間内に規定回数ログインエラーが発生した場合にはアカウントがロックされる等、**厳重なログイン管理**を行っています。
改ざん 情報を暗号化して伝送する場合には改ざんへの危険性は軽減するが、通信経路上の障害等により意図的・非意図的要因に係わらず、データが改変されてしまう可能性があることは認識しておく必要がある。又、ネットワーク自体に情報の秘匿化機能が不十分な場合もあり、検地する為の仕組みなど改ざんに対する対処は確実に実施しておく必要がある。	**ハッシュによる改ざん検知** バックアップ元で暗号化された全てのデータに対して、1方向関数により求めたハッシュ値と、ダウンロード後、復号処理の前段階で同様に求めたハッシュ値を比較し、**通信上及びサーバ上で改ざんされたかどうかを検知**します。

※ 改ざん防止機能はオプションサービスとなります。

glovix
株式会社グロービクス

サービス内容一覧

サービス名		無料サービス	有料サービス(通常)		有料サービス(改ざん防止機能付き)	
		共用サーバ	共用サーバ	専用サーバ	共用サーバ	専用サーバ
バックアップ容量		2GB	5GB～※1			
バックアップスケジュール		1回のみ / 毎日 / 曜日指定 / 週次 / 月次				
暗号方式		AES(128bit) / RSA(2048bit)暗号				
バックアップ対象ファイル容量確認		○				
アップロード通信回線		SSH(グローバルIP認証)				
登録ユーザー数	BCP責任者	20				
	システム管理者	5				
	復号業務担当者	100				
ユーザー一括登録※2		○				
仮ユーザー本登録制限時間設定		24h				
ユーザーパスワードロック		○				
アプリケーションによる一括ファイルダウンロード&復号		×	○			
個別ファイルダウンロード&復号※3		○				
復号ソフトウェア使用制限時間設定		24h				
復号ソフトウェアダウンロードパスワード一斉通知		○				
改ざん防止機能		×			○	
安否確認機能		○				
サーバ		共用	共用	専用	共用	専用
独自ドメイン運用		×	×	○	×	○

※1 詳細は次ページの料金表を御参照下さい。
※2 一括登録は復号業務担当者(100名まで)の仮登録となります。
※3 ブラウザからの個別ファイルダウンロードと、アプリケーションによる復号処理となります。

glovix 株式会社グロービクス

料金プラン

月額料金(税抜き)
(初期費用かかりません)

項目	CRB料金(通常)	CRB料金 (改ざん検知)
～2GB	無料	–
～5GB	¥4,600	¥6,200
～10GB	¥8,200	¥10,600
～20GB	¥14,200	¥19,000
～50GB	¥19,000	¥25,000
～100GB	¥28,400	¥38,000
～250GB	¥44,600	¥60,000
～500GB	¥57,000	¥78,000
～750GB	¥75,800	¥100,000
～1TB	¥93,800	¥124,000

オリジナル ドメイン運用オプション 仮想専用サーバ+オリジナルドメイン+SSL	¥47,000	¥47,000

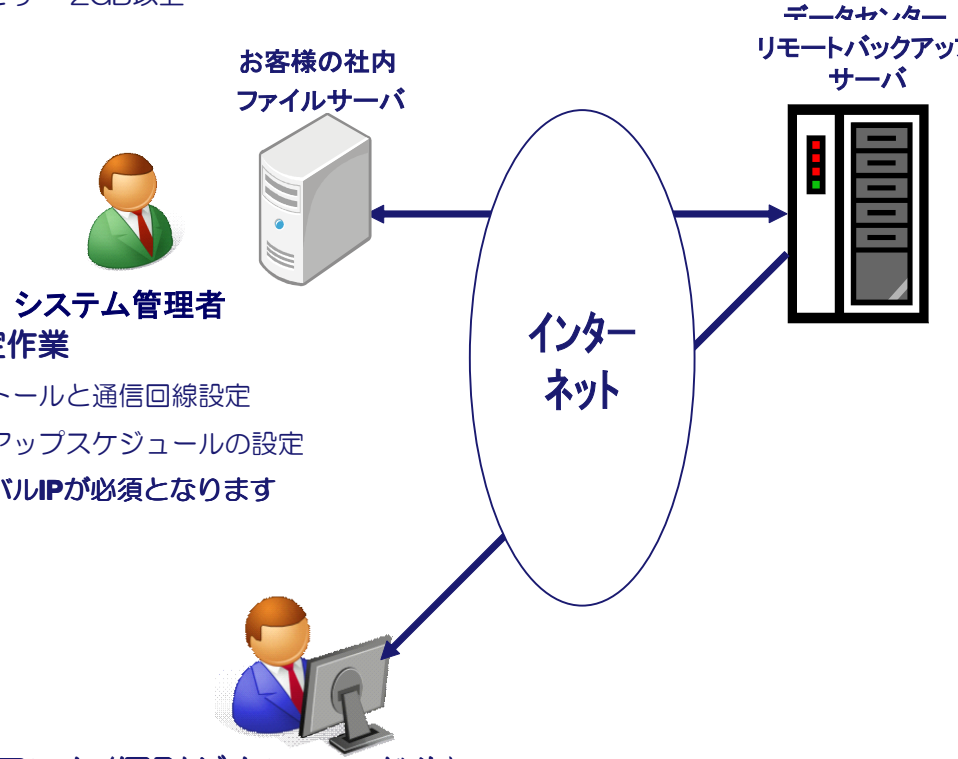
glovix
株式会社グロービクス

バックアップ環境について

【動作推奨環境】

◆ファイルサーバー(バックアップ元)

①OS　Windows 2003以降(VISTA除く)※32bitのみ対応
②CPU　デュアルコア Xeon(R) 2.66GHz 以上
③メモリ　2GB以上



◆クライアント(個別ダウンロード先)

①OS　Windows 2003以降(VISTA除く)※32bitのみ対応
②ブラウザ InternetExproler7.0以上 FireFox3.0以上 GoogleChrome

◆リモートバックアップサーバー

amazon web services

AWS(Amazon Web Services)を利用
(http://aws.amazon.com/jp/)

◆AWSクラウドサービスとは
世界的企業Amazon.comが提供している、Webサービスを通してアクセスできるよう整備されたクラウドサービス群の総称を指しています。

◆AWSクラウドサービスの特徴とメリット
•突発的なアクセスの集中(スパイク現象)発生に関してもクラウドが持つ、トラフィックへの柔軟性を十分に発揮、災害時に強いシステムインフラです。
•AWSが震災後のITリソース不足に対して、無償提供を行い様々な情報発信サイトで導入利用された多くの実績を持っております。

◆セキュリティについて
•第三者認証/認定
•SAS-70 TypeⅡ(2009年取得)
•ISO27001(2010年取得)
•PCI DSS プロバイダー認証(2010年取得)
•FISMA Moderateレベル認定(2011年取得)
•セキュリティホワイトペーパーの提供
AWSセキュリティセンター
(http://aws.amazon.com/jp/security/)

glovix 株式会社グロービクス

ご検討、宜しくお願い致します