File Server Cloud Ver.3

ファイルサーバーサービス
重要事項説明書

株式会社ビジネス・アーキテクツ
Version 2.0
2025/1/6

目次

1 はじめに

本書に関する前提事項を以下に記載いたします。

1.1 本書の目的

本書は、株式会社ビジネス・アーキテクツ（以下「当社」といいます。）が提供するファイルサーバークラウド Ver.3 とオプション機能について、導入前に確認を要する重要事項を記載したものです。ご契約の前に一読して頂き、本サービスに対して十分理解したうえでご発注ください。

1.2 本書にて包括されるサービス

本書に記載している内容は、ファイルサーバークラウド Ver.3 に対応します。当社提供のその他のサービスには対応しておりません。

表記において、ファイルサーバークラウド Ver.3 のことを「FSCv3」や「ファイルサーバーサービス」と表記する場合があります。また、ファイルサーバーサービスが稼働しているシステムを「ファイルサーバー」と記載します。

1.3 FSCv3で適用されるサービス

- ファイルサーバー環境の提供（AWS クラウド基盤を利用）
- ファイルサーバー環境の運用/保守
- クライアント用 VPN 接続ツールの提供
- 利用マニュアルの提供
- 運用サービス/サポートデスク
- 障害対応

2 サポート業務仕様

2.1 運用サービス業務内容

当社サポートチームがご提供する運用サービス業務内容は以下になります。「2.2 運用サービス範囲」記載内容以外のサポートに関しては、個別対応となり有償対応となる場合があります。

運用サービス業務はメールベースでの対応を基本としております。これは対応エビデンスを残すためや、重大障害などで業務が停止しているなどのお客様を優先して対応するためとなります。なお、緊急連絡の場合には電話でもサポートを受け付けております。また、よくある問合せをまとめた FAQ 集を公開しておりますのでご活用ください。

2.1.1 運用サービス業務時間

運用サービス業務時間は以下になります。受け付けは 24 時間メールで実施しておりますが、回答は以下の時間内とさせていただきます。

- 営業時間： 平日 10：00～18：00
- 定休日： 土・日・祝日

2.1.2 障害対応時間

当社管理下のファイルサーバーやネットワーク機器などのインフラに関連する障害に関しては 24 時間体制で対応いたします。（土日、祝日、夜間帯はベストエフォート対応となります）

障害の定義につきましては「6 障害」をご参照ください。

2.1.3 お客様側の窓口

本サポートサービスを提供するにあたり、お客様技術担当者（以下、「技術担当者」といいます。）を設けて頂いております。当社への問い合わせは、基本的に技術担当者を介して頂きます。これは当社側では、お問い合わせ頂いているお客様が、適切な権限（管理者権限等）を持っているのか判断出来ません。万が一悪意ある問い合わせに対して回答を行いますと情報漏洩事故につながる危険がありますので、当社では技術担当者以外への情報の提供は基本お断りさせて頂いております。

また、このような問い合わせが万が一行われた場合の対策として、ご質問事項に対しての回答は技術担当者へご連絡差し上げております。

上記事故防止の観点からも、技術担当者以外のご利用者からの問い合わせはご遠慮いただきますよう周知をお願いいたします。

2.2 運用サービス範囲

2.2.1 基本運用サービス範囲

- ファイルサーバーの利用に関するお問い合わせ
  - ✧ VPN 接続ツールのインストール方法
  - ✧ ファイルサーバーへの接続方法
  - ✧ ファイルサーバーの標準機能の設定方法、利用方法
- オプションサービスの利用に関するお問い合わせ
  - ✧ ご契約オプションサービスの利用方法
- 当社よりご提供している情報（マニュアル等）に関するお問い合わせ
- 後

2.2.2 有償サポート対象

- お客様要望によるファイルサーバーの定期アップデート対応
  （Windows アップデートやソフトウェアアップデート含む）
- ユーザーアカウント/グループ作成や、共有設定/アクセス権設定
  アカウント管理やアクセス権設定などはお客様にて行っていただく事項となります。設定方法などご不明な点はサポート対応させていただきますが、実際の設定作業はお客様にて対応をお願いしております。簡易的な操作マニュアルもご用意しておりますのでご要望の際にはご依頼ください。また、オンサイト教育も承っておりますのでご相談ください。
- クライアント PC 環境個別の問題対応（1 台のみが接続できない場合など）
  ただし、当社提供のインストーラーで発生するエラーなどはサポート範囲内となります。

2.2.3 サポート対象外

- 自宅や社外からの接続問題対応 ※社内から正常に接続できる場合
- モバイルルーター（WiMAX EMobile など）からの接続対応
- お客様環境に設置されている当社管轄外のネットワーク機器やプリンターなどの問題
- クライアント端末、オペレーティングシステム個別の問題
- Linux や Unix、android、iOS など、後述の 3.2 接続クライアントに記載されているオペレーティングシステム以外。
- データ領域内のファイルリストの取得
  データ領域「E:」ドライブ内に保存されているフォルダやファイルの一覧取得は提供しておりません。

3 ファイルサーバーサービス前提事項

ファイルサーバーサービスは、Windows Server 2019 オペレーティングシステムをベースとしたサーバーを 1 契約あたり 1 台ご提供します。このファイルサーバーの「E:」ドライブをお客様専用として契約容量に応じたデータ領域としてご提供いたします。クライアントは各種 VPN でファイルサーバーへ接続し、Windows エクスプローラーでファイル操作をしていただくサービスです。

ユーザーアカウントやアクセス権の管理には、ファイルサーバーにリモートデスクトップ接続していただき、Windows OS 標準操作にて管理を行っていただけます。

3.1 アカウント管理

- ファイルサーバーは出荷時に技術担当者専用の Administrators グループに所属したユーザーアカウントを作成しております。こちらにてユーザー管理やアクセス権管理を行ってください。
- ファイルサーバーの運用管理（ユーザー作成・フォルダ権限付与等）は Windows の標準機能である「リモートデスクトップ」をご利用頂きます。専用の管理画面や GUI ツールなどはございません。

3.2 接続クライアントとVPN接続方式

3.2.1 接続クライアント

- ファイルサーバーサービスは Microsoft 社製 Windows OS を前提としたサービスとなっております。なお、ファイルサーバーサービスはビジネスユースを前提としているため、VPN 接続するクライアント PC については Home エディションのサポートは致しておりません。Home エディションのクライアントは VPN 接続ができないケースがあります。
- 日本語版 Windows OS のみが接続サポート対象となります。海外版 Windows OS および、海外版 Windows OS を日本語化した OS はサポート対象外となります。
- Mac OS については VPN 接続のみのサポートとなります。Mac OS のオペレーティング操作はサポート範囲外となりますので、Apple サポートなどへお問い合わせください。
- Mac OS X v10.10 以降のバージョンにて、ファイルサーバーサービスへの接続確認が取れております。ただし、メーカー側の仕様変更などにより今後接続できなくなることも考えられますのでご了承ください。OpenVPN 接続または、IPSec 環境からファイルサーバーサービスへのアクセスが可能となります。SSTP 接続は Microsoft 社独自の接続方式となります。

接続サポート対象のクライアントと接続方式を以下に記載します。

	サポートOS	SSTP 接続	OpenVPN 接続	IPSec 接続
Windows 32bit 版	Windows 10 Pro	○	○	○
Windows 64bit 版	Windows 10 Pro	○	○	○
	Windows 11 Pro	○ *3	○	○
macOS	OS X v10.10 以降 *1	X	○ *2	○

*1 VPN 接続のみのサポート

*2 ソフトウェアの更新により、将来的にサポート対象外となるケースあり

*3 2018 年 1 月以降に提供のクラウドファイルサーバーが対象

- Windows11 サポートは、2018 年 1 月以降に提供されたクラウドファイルサーバーが対象となります。2017 年 12 月以前に提供されたクラウドファイルサーバーは Windows11 端末から SSTP 接続することができません。クライアント端末へ証明書を追加インストールすることで Windows11 対応とすることが可能となります（詳細は当社までお問い合わせください)。
- モバイル端末からの接続には、スマホ＆タブレットオプションをご契約ください。WebDAV アプリケーション経由で接続していただけます。なお、WebDAV 対応のアプリケーションはお客様にてご準備していただきます。アプリケーションのインストール方法や接続設定方法および、利用方方法についてはアプリケーションメーカーへお問い合わせください。
- スキャナーや複合機からファイルサーバーへの接続やデータ転送については、当社ではサポートしておりません。機器メーカーへお問い合わせください。

3.2.2 VPN接続方式

- ファイルサーバーへの VPN 接続方式は Windows 標準搭載である SSTP を利用します。SSTP は Windows OS のみで利用できます。そのため、MacOS を利用されるお客様へは OpenVPN による接続もサポートしております(有償)。また、お客様環境とファイルサーバー環境とを VPN 装置で常時接続する IPSec 接続もご提供可能です。IPSec 接続ではクライアント OS の種類による接続制限はございません。

  ※ お客様環境のプロキシサーバーにて BASIC 認証を使用している場合には SSTP 接続はサポート対象外になります。

  ※ VPN クライアントのインストールには、原則として管理者権限が必要となります。管理者権限が付与されていないユーザーアカウントでインストールを実行する場合には、管理者権限のユーザーID/パスワードの入力が必要となります。

VPN 接続方式を以下に記載します。

	実現方式	導入単位	認証	最大接続ユーザー数	接続 OS
SSTP	OS 標準ソフトウェアの設定	クライアント PC	証明書 ユーザーID/パスワード	240 名	Windows
OpenVPN (SSL-VPN)	オープンソースソフトウェアのインストール	クライアント PC	証明書 ユーザーID/パスワード	60 名	Windows Mac
IPSec	VPN 機器の設置	拠点	ユーザーID/パスワード	無制限	制限なし

※ ユーザーIP/パスワード認証は、ファイルサーバー側の OS ユーザーアカウント認証をさします。

3.3 アクセスポートの解放

お客様拠点から外部への通信を制限している場合は、接続方法に応じて、お客様拠点側 Firewallに以下のポートの通信許可を設定してください。なお、接続先であるファイルサーバー側のIPアドレスについてはお客様ごとに異なりますので別途ご連絡します。

接続方法	プロトコル・ポート	通信速度	接続先
SSTP	TCP：443（HTTPS）	平均20Mbps	ファイルサーバーIPアドレス
OpenVPN	UDP：1194	最大10Mbps	
IPSec	UDP: 500	平均190Mbps	

※ お客様環境のプロキシサーバーで BASIC 認証を使用している場合には SSTP 接続はサポート対象外になります。

※ 通信速度の記載は無負荷時の論理値であり、実際の速度は回線や電波状況等の環境要因により大きく低下する場合があります。

※ SSTP・OpenVPN 接続のお客様環境の Firewall 設定変更作業はお客様にて実施していただきます。

3.4 ネットワークの制限

- お客様環境のネットワーク（論理、物理）に関しては当社サポート範囲外となります。当社サポートで回答可能な情報については開示いたしますが、基本的には機器固有のパラメーターのご質問、設定に関するご質問については回答を控えさせて頂いております。当社パートナーのネットワークについては当社パートナーが提供および開示する範囲でのサポートとなります。

- 海外拠点からの接続については、各国のネットワーク回線に問題がある場合がほとんどです。VPN 通信の制限がされている場合や、ポートが閉じられている場合もありますので、不明な場合は当社試使用環境でご確認ください。本サービスを締結した後に万が一接続できない場合でも解約される場合は違約金が発生します。

- お客様専用回線の敷設、お客様機器（ルーター等）の設置についてはカスタマイズ扱いとなりますので、納期、サービス内容（監視、運用）が通常のサービスとは異なります。事前に当社にご確認ください。

- お客様環境にて PROXY サーバーが導入さている場合で Basic 認証を利用している場合には SSTP 接続はサポートされません（Windows 仕様）。無料お試し環境にて接続性をご確認ください。

3.5 ファイルサーバー仕様

- 原則として、ファイルサーバーに他のアプリケーションをインストールすることは出来ません。アプリケーションのインストールが必要な場合は、別途 PaaS インスタンス（サーバーを丸ごとお貸しするサービス）をご契約していただきます。またお客様にて当社に無断でアプリケーションのインストールを実施した場合は、上記 PaaS インスタンスとして再計算を行い、差額を請求させて頂く場合がございますのでご注意ください。

- サーバーオペレーティングシステム標準の機能については使用可能としております（VSS 機能やクォータ機能など）。ただし、その機能の仕様やバグなどによるトラブルについては当社では対応できない場合がございます。

- 当社がご提供するファイルサーバーには Microsoft Office®製品はインストールされておりません。よって Microsoft Office®製品がインストールされていないクライアント PC からファイルサーバー上にある Word 形式（.docs）や Excel 形式（.xlsx）等の Office 製品で作成されたファイルを開くことはできません。また同様の理由で PDF 形式（.pdf）のファイルも開くことは出来ません。

- ファイルサーバーのデータ領域は「E:」ドライブとして認識されます。システム領域「C:」ドライブは当社管理となりますので、データ保存は禁止となります。

- お客様システム環境が Active Directory 環境の場合、AD レプリケーションオプションをご契約いただく前提となっております。Active Directory のクライアント環境から、ワークグループ上のファイルサーバーへ接続する場合、クライアント環境にて名前解決ができなくなる場合がございます。Active Directory 環境の場合には、事前にご相談ください。

3.6 パフォーマンス関連

- パフォーマンスの低下に対して、原則として当社は障害もしくはトラブルとしての取り扱いは致しません。これは時間と共に使用状況が変化し、出荷段階のパフォーマンスを維持、修復する事が困難となりますので経年劣化として対応させて頂きます。対応内容としてファイルサーバーの一時停止を伴うメンテナンスや再起動を実施させていただく場合がございます。

- 長期間の利用で Widows オペレーティングシステムのメモリリソースが枯渇する場合、オペレーティングシステムの再起動（メモリリフレッシュ）を実施させていただきます。原則としてお客様と再起動タイミングを調整のうえで実施しますが、緊急時や休日夜間の場合には、お客様への連絡なく再起動を実施する場合がございますのでご了承ください。

- オペレーティングシステムの再起動後にもパフォーマンス低下が回復しない場合があります。この場合はパフォーマンス低下の要因と思われる事象について出来るだけ調査を行いますが、完全に初期状態に復旧する保証は出来かねます。これは Windows オペレーティングシステムのリソース状況、パッチ等による影響、ユーザー数の増加、御社ネットワークおよび機器の影響など、原因切り分けが困難であるためです。この場合はサーバーのスペックアップなどのご提案をさせていただく場合がございます。

- ウィルスチェックオプションではリアルタイムスキャンを提供するサービスです。ディスクフルスキャン機能も備わっていますが実行によりパフォーマンスに大きな影響を及ぼします。環境によっては、その他の機能が正常動作しなくなる可能性がございます（バックアップ処理が 24 時間以上継続するなど)。ディスクフルスキャンを定期実行する場合には当社サポートへご相談ください。サーバータイプのスペックアップなどの対応が必要となる場合がございます。

- イベントログアーカイブや ALog SMASH などのログ管理オプションを利用している場合、ログ分析処理中にパフォーマンスに影響を及ぼす可能性があります。ミラーオプションや、ウィルスチェックオプションを併用する場合、アクセスログが欠落する場合があります。データ容量やユーザーアクセス量などにより異なりますため、アクセスログの欠落頻度が高い場合にはサーバータイプのスペックアップなどの対応が必要となる場合がございます。

- オプションの中には、CPU リソース消費が大きくなるものがあります。ウィルスチェックオプション、ミラーオプション、ログ管理オプションについては CPU リソース消費が大きくなるため、サーバータイプ「ゴールド」以上が推奨環境です。サーバータイプ「スタンダード」では、レスポンスの低下や、他のオプション動作に影響を与える場合があります。

- バックアップオプションの VSS 機能にて、過去の VSS データが消えるなどの問題が発生する場合があります。これは、Windows オペレーティングシステムの問題であり、現時点での解決策はありませんのでご了承ください。データ保管の要件にあわせてミラーオプションやスナップショットオプションの併用もご検討ください。

3.7 データ移行

- お客様環境からファイルサーバーへのデータ移行をご要望は事前にご相談ください。アクセス権限（ACL）の移行可否なども併せて確認させていただきます。

- お客様データの移行に際して、事前にデータバックアップの取得をお願いします。バックアップ処理によってお客様のデータに欠損および不整合が発生する場合がございます。この場合、当社にてデータの修正及び保障は致しかねます。

- データ移行後、ファイルやアクセス権の正常性をご確認ください。お客様の確認後にデータ移行完了とします。正常性完了まではお客様側データは保持していただく

3.8 障害対応

- 障害発生における当社の免責事項については約款をご参照ください。
- 障害の定義は「6.1 障害定義」をご参照ください。

3.9 データ領域

3.9.1 領域の監視

ご契約いただいているデータ領域の使用量についてはお客様にてご確認ください。データ領域が 100%になりますとファイルを保存できなくなり、編集中ファイルの変更が反映されない等の問題が発生いたします。このような場合、当社はデータの保全は実施しておりませんので復旧することは出来ません。データ領域が逼迫する前に、データ領域の整理を行うか、データ領域の拡張をご依頼ください。（領域の拡張作業はサービスを一時停止した状態で実施させて頂いております）

なお、データ領域が 80%を超えた場合、当社サポートからお客様に対してご連絡を差し上げておりますが、サポート時間外の場合はご連絡ができない場合がございますのでご了承ください。

3.9.2 データ保護

当社ではご契約頂いているデータ領域に保存されているデータの保護（バックアップ等による退避）は

実施しておりません。データ保護が必要な場合はバックアップオプション（ミラーオプションまたは、定期スナップオプション）をご用命ください。なお、VSS 機能はデータ保護のための"バックアップ機能"ではございませんのでご注意ください。VSS で取得したバックアップデータは同じシステム内に保管されるため、HDD 物理故障や、システム論理障害などが発生した場合、データと同時に VSS で取得したバックアップデータも消失します。

3.9.3 データ領域拡張

ご契約いただいたデータ領域「E:」ドライブの容量は拡張することが可能です。拡張にはサービス停止が伴いますので事前にお客様と相談のうえで実施します。なお、システムの仕組み上、データ領域の縮小はできません。縮小をご要望の場合には当社サポートまでご相談ください。

3.9.4 データ消失

当社では、ファイルサーバー上のデータが消失した場合でも当社では一切の責任を負いません。ハードウェア障害や、Windows OS の障害、ファイルシステムの論理障害などが発生した場合には、システムが起動できなくなることや、データ領域に保存したファイルが消失する可能性があります。データ保全のために「ミラーオプション」または、「定期スナップオプション」をご利用ください。

※ ボリュームシャドーコピーサービス（VSS）は、「ファイル削除」に対する有効策となります。Windows オペレーティングシステムが起動しない場合や、データ領域が参照できないような場合には、VSS ではデータの復元はできません。

※ ファイルサーバー上のデータを、お客様管轄のデータ領域（クライアント PC など）に転送/保存することは可能ですが、バックアップによる大量データの転送によるサーバーレスポンスへの影響などが発生する可能性がございます。

3.10 各オプションの注意事項

ファイルサーバーサービスの各オプションをご注文頂く際の注意点について記載いたします。

3.10.1 スマホ&タブレット

WebDAV 通信を利用してのファイルサーバー接続が可能となります。これにより、スマートフォンやタブレット経由でファイルサーバーにアクセスすることが可能となります。

ドメイン利用について、当社ドメイン”fileserver-cloud.jp”や、お客様ドメインを利用することも可能です。お客様ドメインを利用される場合には、事前にお客様環境の DNS サーバー設定変更（A レコード追加）が可能であることをご確認ください。証明書発行までの手続きは当社にて代行いたします。（別途 SSL 証明書発行代行費用がかかります）。

SSTP 接続を併せて利用する場合には、こちらの証明書を SSTP 接続でも利用します。

クライアントアプリケーションは当社からは提供および、ご案内をしておりません。お客様にてご用意し、クライアント PC へインストールしていただきます。アプリケーションにより特性がありますので、利用シーンやセキュリティポリシーに合わせて最適なものをご選択ください。なお、クライアントアプリケーションプログラム自体の導入や設定および、トラブル対応については当社サポート対象外となりますのでご了承ください。

スマホ&タブレット、SSTP で利用可能な公的証明書は 1 年更新（各契約証明書の更新期間）となります。更新が近づいた場合は当社よりご連絡します（当社が提供している場合のみ）。更新しない場合は接続方法に影響があり、再セットアップが必要な場合があります。

3.10.2 ADレプリケーションサービス（ADパック、ADPaaS連携）

お客様環境の現行 Active Directory サービスが正しく構成され、エラーが発生していない状態であることが導入前提となります。なお、サポート可能な Windows Server の Edition は「Datacenter」と「Standard」となります。その他の Edition である「Essentials」や「Foundation」などについてはサポート外となる場合がございますので事前にご相談ください。

現行 Active Directory 機能レベルが Windows Server 2008R2 以上である必要があります。現行環境への操作は原則としてお客様へお願いをしております。

お客様へは以下についてもお願いをしております。

- ファイルサーバー保守用として、Domain Admin の権限をもつユーザーをお借りします。
- 通信に必要な FW のポートを解放して頂きます。
- クライアントに設定する DNS サーバーアドレスが必要となります。お申込書にご記載ください。

ファイルサーバーをお客様 DC のメンバーサーバーとして登録する構成は推奨しておりません。お客様環境の DC に対して都度ユーザー認証を実施するためパフォーマンスの低下がみられます。メンバーサーバーとして構成する場合には、別途 Windows CAL（クライアントアクセスライセンス）が必要になりますのでお客様でご用意ください。

3.10.3 OpenVPN接続

OpenVPN アプリケーションは、オープンソースのアプリケーションとなります。インターネット上からセットアップファイルをダウンロードし、クライアントごとにインストールして頂きます。インストールマニュアルは当社にてご用意しております。

Windows 標準機能の SSTP 接続と比べ、OpenVPN 接続では通信断が発生する頻度が高くなります。原因

によっては監視システムで検知ができないケースがございますので、その場合には当社サポートにご連絡ください。

Windows 標準の SSTP では Windows アップデートにより SSTP のセキュリティパッチも適用されますが、OpenVPN ではクライアントごとにセキュリティパッチを手作業で適用するなどの運用が必要となります。クライアント側のパッチ適用はお客様にて対応して頂きます。ファイルサーバー側のセキュリティパッチ適用は当社サポートにて対応します。サービス停止を伴うメンテナンス作業が必要な場合には事前にご連絡した上で実施します。

クライアントの OpenVPN プログラムバージョンと、ファイルサーバーの OpenVPN プログラムバージョンの差異によっては接続に問題が発生する可能性も考えられます。バージョンアップの際には、事前に接続検証を行うことをお勧めします。

3.10.4 SSTP接続と公的証明書

SSTP 接続でご用命頂いた場合、通常は私的証明書を作成して出荷いたします。別途ご用命を頂ければ SSTP 接続を公的証明書に切り替える事も可能です。この場合は証明書の取得代行サービスをご利用ください。スマホ＆タブレットオプションを利用する場合は、標準で公的証明書のご利用となり、SSTP も公的証明書での提供となります。

3.10.5 ログ管理オプション

アクセス権の無いファイルについては操作ログを取得することができません。データ領域「E:」ドライブに対して”LogManagementTarget”グループを監査設定しています。アクセスログの出力をさせたいユーザーアカウントは当該グループに所属していただく必要があります。当該グループに所属していないユーザーアカウントのアクセスログは記録されませんのでご注意ください。

設定には Administrator もしくは同等の権限をもつユーザーが必要になります。AD を導入中のお客様はこれらの情報をご開示頂く場合がございます。また導入後は必ずお客様にてアクセスログが取得できている事を確認してください。ファイルへの実アクセスがないとログ記録がされないためです。

ログ管理の方法として、以下の 2 種類のオプションをご用意しております。お客様の情報セキュリティ要件などを踏まえご検討ください。

- イベントログアーカイブ（無償オプション）

Windows OS 標準のイベントログから、セキュリティログ部分を「.evtx(イベントビューアー形式)」ファイルでデータ領域「E：」ドライブへ保存する機能となります。Windows OS が出力する生データのまま、データ成形などは行っておりません。取得可能な操作ログは当社からは公表しておりません。クラ

イアントの Windows OS バージョン（更新プログラム）などにより異なることがあるため、Microsoft 社の情報をご参照ください。

取得されたログデータの内容確認や、ユーザー操作の証跡を確認する場合には、お客様にてご対応をお願いしております。「.evtx」ファイルはバイナリファイルとなります。内容を確認するにはイベントビューアーをご利用ください。

圧縮されたログデータはお客様のデータ領域「E:」ドライブへ保存されます。保存期間の制限はございませんが、データ領域の空き容量が無くなるとログデータも保存できなくなります。不要になったファイルを整理するか、データ領域の拡張（有償）などご検討ください。

ログ出力量につきましては、ご利用人数やアクセス頻度および、オプションによって大きく変動します。ミラーオプションやウィルスチェックオプション、全文検索オプションの動作ではファイルに対するアクセスが発生することから、その操作も記録されます。そのためログ出力量が大きくなります。データ領域「E：」ドライブの容量にご注意ください。当社監視によるディスク容量アラート連絡は行いますが、当社でログ出力を停止するような操作は行いません。（重要なセキュリティ情報となる場合があるため）

イベントログアーカイブオプションの処理は、セキュリティログ出力を漏れなく取得することを保証するものではございません。ご了承ください。

バックアップオプションご契約の環境では、圧縮されたログデータも一緒にバックアップされます。

➢ ALog SMASH on FSC

アクセスログ管理製品を利用して、アクセスログを見やすく変換します。ブラウザを使用した Web コンソール画面を利用することで大量のログの中から必要な情報を抽出することや、レポート機能やアラート通知機能を設定できます。

※ 詳細な機能や利用方法につきましては別紙「ALog SMASH ユーザーズガイド」をご参照ください。

※ 操作マニュアルは、ALog SMASH メーカーマニュアルをご提供します。ご不明な点は当社サポートまでお問い合わせください。

Web コンソール画面で参照可能なアクセスログの期間は直近 3 か月間となります。3 か月を超えたデータは「.csv（カンマ区切りファイル）」に変換され、zip 圧縮された後にデータ領域「E:」ドライブへ保管されます。この仕組みにより、4 か月以上前のアクセスログデータを参照するには、別途.csv ファイルからの逆変換が必要となります。Web コンソールから GUI 操作が可能ですが、データ量が多い場合には処理に時間を要する場合があります。

.csv に変換されたファイルの保存期間の制限はございませんが、データ領域の空き容量が無くなると

ログデータも保存できなくなります。不要になったファイルを整理するか、データ領域の拡張（有償）などご検討ください。

ALog SMASH on FSC オプションは 300 ユーザー以下の環境でご利用いただけます。300 ユーザーを超える環境の場合には別途ご相談ください。

ログ出力量の例として、ユーザー数 100 名でファイルサーバーを利用した場合には、年間 1.2GB が目安となります。ウィルスチェックオプションなどによるファイルへのアクセスが発生すると、その操作も記録されるためログ出力量が大きくなることがあります。

ALog SMASH で取得可能な操作ログを以下に記載します。以下のログ出力例では、Suzuki ユーザーが file.txt を開いた後に、file.txt を削除したことがわかります。

アクセスログの出力例

日時	ユーザー	操作対象	出力データ（操作）	詳細
2020/4/1 15:30:00.508	Domain¥Suzuki	E:¥public¥file.txt	READ	ClientIP:192.168.0.1 Count:3
2020/4/1 15:30:30.590	Domain¥Suzuki	E:¥public¥file.txt	DELETE	ClientIP:192.168.0.1 Count:1

アクセスログに記録されるユーザー操作

ユーザーの操作	出力データ
ファイルを開く	READ
フォルダを開く	出力なし
ファイルを新規作成	WRITE
フォルダを新規作成	WRITE
ファイルを更新	WRITE
ファイルを削除	DELETE
フォルダを削除	DELETE *1

*1 サブフォルダに対しても「DELETE」が出力されます

ユーザーの操作	出力データ（元ファイル）	出力データ（新ファイル）
ファイルをコピー	COPY/READ	WRITE
フォルダをコピー	COPY/出力なし	WRITE *1
ファイルを名前変更	RENAME	WRITE/READ/出力なし
フォルダを名前変更	RENAME	WRITE/READ/出力なし
ファイルを移動（同ドライブへの移動）	MOVE	WRITE
フォルダを移動（同ドライブへの移動）	MOVE/RENAME	WRITE/READ/出力なし *2
ファイルを移動（別ドライブへの移動）	DELETE	WRITE
フォルダを移動（別ドライブへの移動）	DELETE	WRITE

*1 フォルダを上書きコピーする場合は、新ファイル「出力なし」となります。

*2 フォルダを上書き移動する場合は、元ファイル「DELTETE」/新ファイル「出力なし」となります。

コピーや移動の操作は、元ファイルと新ファイルの双方が監査対象である場合に上記のように出力されます。監査対象外のマシンやドライブへのコピーや移動は、出力されているイベントログからわかる情報の範囲で変換されます。

ALog SMASH は、以下のアプリケーションによるファイル操作が正しく反映されるように作成されています。その他アプリケーションによる操作は期待する結果がえられないことがありますのでご了承ください。

・エクスプローラー
・メモ帳
・ペイント
・Microsoft Office（Word, Excel, Power Point）
・Adobe Acrobat Reader

機能の詳細につきましては、別紙「ALog SMASH ユーザーズガイド」をご参照ください。ご不明な点がございましたら当社までお問い合わせください。

3.10.6 ウィルスチェックオプション

リアルタイムスキャンを提供するオプションです。データ領域全体に対する定期フルスキャンも実行可能ですが、CPU リソースを大量消費するために、パフォーマンスに大きな影響があります。フルスキャン処理の動作についてはサポート範囲外となります。当社サポートへお問い合わせいただくことは可能ですが、一部回答できない場合もございますのでご了承下さい。

3.10.7 データ領域・暗号化オプション

データ領域ボリューム内の保存データが暗号化されます。また、作成されたスナップショットも暗号化されます。（スナップショットの取得は有償オプションとなります）

ボリューム単位（データ領域のディスクごと）の暗号化となります。

3.10.8 データ重複除去オプション

Windows OS 標準機能で、複数のファイル間で重複するデータ領域を取り除いて 1 カ所にまとめ、全体的なディスク使用量を抑制する機能です。本処理を行う場合、データ容量によりますが、ディスク I/O および、CPU 使用率が増加します。パフォーマンス低下が著しい場合はワンランク上のサーバータイプをご検討ください

3.10.9 バックアップオプション

3種類のバックアップ方式をご用意しております。またバックアップデータ保管先についても、東京リージョンや大阪リージョンまたは、海外のリージョンなど、お客様のデータ保管要件に合わせてご選択いただけます。

種別	データ保管先	使用用途の例
定期スナップショット	東京リージョン	定常バックアップ用
	大阪リージョン	大規模災害対策用 (※)
	海外リージョン	大規模災害対策用 (※)
ミラー	東京リージョン	定常バックアップ用
	大阪リージョン	定常バックアップ用、大規模災害対策用
	海外リージョン	定常バックアップ用、大規模災害対策用
VSS	ファイルサーバー内	ユーザー操作ミスによるファイル削除など

※ 定期スナップショットの大阪リージョンおよび、海外リージョンを利用した場合、東京リージョンからの復旧時間と比較して1営業日～2営業日ほど多くの時間がかかるため、お客様のシステム復旧時間要件などとも合わせてご検討ください。

➢ 定期スナップショット

システム領域および、データ領域をディスク単位でバックアップします。復元もディスク単位となりますので、ファイル単位での復元はできません。仕組み上、メモリやキャッシュ上にあるデータは取得ができません。完全な状態でのバックアップが必要な場合には当社サポートまでご相談ください。

スナップショット取得スケジュールは毎日午前 0 時です。保管世代は日次 7 世代となります。スケジュールの変更や保管世代のご要望がある場合にはご要請ください。

バックアップデータ保管先が大阪リージョンまたは、海外のリージョンを場合には、東京リージョンからの復元と比較して、復元までの時間が 1 営業日～2 営業日ほど長くなります。

データ保管先	復元時間の目安（※）	備考
東京リージョン	1 営業日～（最短 1 時間）	データ容量に影響しません
大阪リージョン	2 営業日～	データ容量によって異なります
海外リージョン	2 営業日～	データ容量によって異なります

※ 復元時間の目安は、その時間を保証するものではございませんのでご了承ください。障害や被害の規模によって復元時間は大きく異なる場合があります。

※ 復元時間の目安は、管理者様がデータにアクセスできるようになるまでを想定しております。別途アクセス権設定などの作業が必要になるケースもございます。

➢ ミラー

データ領域をファイル単位でバックアップします。システム領域はバックアップ対象外です。ファイルアクセス権（ACL）はバックアップされません。ファイル復旧後はお客様にてアクセス権の再設定作業が必要となります。システム障害によりシステム全体の復元を行う場合には、システム領域の再構築後にバックアップデータを復元します。お客様作業にてユーザー/グループ作成および、アクセス権の再設定が必要となります。このため、サービス完全復旧までに時間を要するケースがございます。

ミラー処理の開始スケジュールは毎日午前 0 時です。保管世代は 1 世代となります。スケジュールの変更や複数世代のバックアップ取得をご希望の場合にはご要請ください。

バックアップデータ量が 1TB を超える場合には、定期スナップショットオプションをご利用ください。ミラー処理では、データ量に比例してバックアップ時間も長くなるため、1TB を超えると 24 時間でバックアップ処理が終了しない可能性があります。

バックアップデータ保管先が大阪リージョンや海外リージョンであっても、東京リージョンと比較して、バックアップ取得時間および、復元時間ともに大きな差異はございません。復元はファイル単位でのデータ転送が発生するため、データ容量によっては、すべてのデータ復元が完了するまでに 1 営業日～3 営業日ほどかかるケースがございます。

➢ Volume Shadowcopy Service (VSS)（無償オプション）

Microsoft が提供する「Volume Shadowcopy Service（以下 VSS）」をご利用いただけます。VSS 機能ではデータ領域のスナップショットを取得します。設定したバックアップ容量を上限に最大 64 世代までのスナップショットを取得することができ、ファイル単位での復元が可能です。

VSS で取得したスナップショットは、標準でファイルサーバーのデータ領域「E:」ドライブ内へ保存されます。任意設定した上限値としてデータ領域を使用します。

VSS 機能の動作については当社サポート対象外となります。VSS 機能で発生した問題について当社では責任を負えませんのでご了承の上でご利用ください。利用方法については、当社ではベストエフォートにてサポートいたします。

Microsoft 社より、保管した VSS データが消失する事象が確認されています。事象が頻発する場合など、Microsoft が事象回避対策として推奨する「VSS 専用ディスク領域（F ドライブ）」を準備することも可能となります。当社サポートへご相談ください。

3.10.10 外部共有（FSC Collabo Powered by DocPlug）

「FSC Collabo Powered by DocPlug」は外部共有機能をご提供します。Web ブラウザを利用したファイルデータの閲覧やダウンロード/アップロードが可能です。ファイルサーバー上のファイルを直接編集することはできません。

運用中のファイルサーバーのフォルダ構成を維持したまま導入する場合、フォルダ構成やアクセス権

の変更が必要になります。事前に当社サポートへご連絡ください。設定が適切でないと、意図しないユーザーからフォルダ構成が閲覧できてしまう場合があります。

「8443 ポート」を利用します。お客様拠点から外部への通信を制限している場合は、お客様拠点側 Firewall にポートの通信許可を設定してください。

Web ブラウザ経由でアクセスした際の操作がログファイルに記録されます。ログ管理オプションでのログ取得対象外となりますのでご注意ください。取得できるログについてはサポートまでお問い合わせください。

動作対象ブラウザは以下となります。
お客様への予告なしに変更となる場合がございますので詳細はお問い合わせください。

対象ブラウザ（PC）	対象ブラウザ（モバイル）
InternetExplorer 11 Microsoft Edge Safari Firefox Chrome	iOS/Safari iPadOS/Safari Android/Chrome

※ InternetExplorer 6, 7, 8, 9, 10 はサポート対象外です
※ InternetExplorer 11 はサポート 2022 年 6 月でサポート終了します
※ 64bit 版の”ブラウザ”では、直接ファイルオープン機能は動作しません。
※ Firefox・Chrome は最新バージョンを推奨します
※ Firefox は、Windows 版のみ対応しています。Mac 版では一部の機能が動作しない可能性があります
※ Safari では、一部の機能が制限されます（ファイルのアップロード時に同時に選択できるファイル数に制限があるなど）

3.10.11 全文検索（FSC Search Powered by DocPlug）

「FSC Search Powered by DocPlug」は全文検索機能をご提供します。「FSC Collabo Powered by DocPlug」の外部共有機能も利用可能です。

運用中のファイルサーバーのフォルダ構成を維持したまま導入する場合、フォルダ構成やアクセス権の変更が必要になります。事前に当社サポートへご連絡ください。設定が適切でないと、意図しないユーザーからフォルダ構成が閲覧できてしまう場合があります。

「8443 ポート」を利用します。お客様拠点から外部への通信を制限している場合は、お客様拠点側 Firewall にポートの通信許可を設定してください。

Web ブラウザ経由でアクセスした際の操作がログファイルに記録されます。ログ管理オプションでのロ

グ取得対象外となりますのでご注意ください。取得できるログについてはサポートまでお問い合わせください。

動作対象ブラウザについては、3.10.11 FSC Collabo Powered by Docplug をご参照ください。

ライセンス料金は利用ユーザー数ライセンスと文書数ライセンスで構成されます。ご契約時のライセンス料金を超えて利用される場合には、当社サポートまでご連絡ください。利用ユーザーは「専用グループ」に所属させていただく必要がございます。

検索エンジンは Unicode に対応しています。Microsoft Office など Unicode 対応ドキュメントについては世界中の言語・文字コードの文書を検索可能です。ただし、正しく検索されない場合や、全文検索できないファイルが存在する可能性があります。

4 ファイルサーバーオプションの変更

ファイルサーバーサービス提供後にオプションの変更をする場合の注意事項を以下に記載します。サービス提供後にオプションを追加する場合は、サービスを維持した状態での作業となりますので、作業時間が限定され稼働までに時間を有する場合があります。これらのオプションについてはサービス開始前に導入検討いただくことをお勧めいたします。なお、サービス開始後のオプションに追加につきましては、無償オプションの場合にも、一部有償対応（初期費用の発生）となる場合がございます。

4.1 サービス開始後のVPN接続方法の変更

- VPN 接続方法に応じてインストーラーが異なります。よってファイルサーバーへの接続方法が変わる場合は、クライアント側にて再インストール作業が必要になります。
  - ✧ OpenVPN
  - ✧ SSTP（スマホ＆タブレットオプション無し）
  - ✧ SSTP（スマホ＆タブレットオプション有り）
  - ✧ スマホ&タブレット（ご利用のアプリケーションの設定変更をお願いします）

※ 接続方法を変更する場合は、サーバー側のサービスを切り替えます。複数同時には VPN 接続ができないため、一時的にファイルサーバーへ接続ができない期間が発生します。接続クライアント側の切り替えタイミングにご注意ください。

※ IPSec 接続への変更はクライアント側に対して作業は不要です。

※ IPsec から SSTP や OPENVPN への切り替えは上記インストーラーを使ったクライアント設定が必要となります。

4.2 スマホ&タブレット

- スマホ&タブレットは公的証明書を利用します。SSTP 接続をご利用の場合には、クライアントのインストーラーが変更となることで SSTP 接続の再インストールが必要となりますのでご注意ください。また、お客様側にて DNS への A レコード登録作業と証明書作成時の承認メールの処理が必要となります。
- 公的証明書の取りやめ（スマホ＆タブレットの解約、公的証明書の契約終了）を行った場合、SSTP 接続方法が私的証明書を利用する方法に変更になります。この場合にもクライアントのインストーラーが変更になることで、SSTP 接続の再インストールが必要となります。

5 サービスの保守

ファイルサーバーサービスの保守に関して以下に記載いたします。

5.1 保守区分

ファイルサーバーサービスは、Amazon Web Services（以下、AWS）より提供されているクラウドコンピューティングサービスと呼ばれるインフラストラクチャーサービスを利用します。

クラウド上のインフラ基盤の運用・保守は AWS サポートにより実施されます。当社は AWS が提供するインフラ基盤上に、Windows OS および、ファイルサーバーサービスを提供するために必要なプログラムやサービスおよび、クライアント用の接続ツールなどを提供し、運用管理をします。

以下の機器およびソフトウェアは当社が運用・保守致します。

- ファイルサーバーのオペレーティングシステム部分とファイルサーバーサービスとして提供する為に必要なツール一式（ファイルサーバーサービスのみ）

※ クライアント端末および、それに付随する機材、またクライアントオペレーティングシステムに関してはお客様にて保守をお願いします。

※ AWSクラウド環境の構成機材についての保守、障害対応はAWSサポートでの対応となます。メンテナンス連絡等は、AWSサポートから当社サポートが連絡を受けたうえで、必要に応じてお客様へ情報展開いたします。

5.1.1 定期メンテナンス

ファイルサーバーサービスにおいて、正常に動作し続けるために行われる保守・点検作業を示します。

具体的にはクラウド環境構成部材におけるオペレーティングシステムのバージョンアップ、セキュリティパッチの適用などにより、四半期または、半年毎を目安にメンテナンスを実施いたします。サービス停止を伴うメンテナンスが発生する場合には、事前にお客様とまた、AWS クラウド環境構成機材（サーバー機器、ストレージ機器等）のメンテナンスは、AWS サポートからのメンテナンス連絡を当社が受けたうえで、メンテンナンス実施についてお客様へご報告、実施調整をさせていただきます。

5.1.2 緊急メンテナンス

サーバー・ネットワーク・各種ケーブルを含むハードウェアの故障によるサービス停止や、オペレーティングシステムの論理障害等、予め予期出来ない事象に対して、即日復旧作業を実施する場合に、事前の連絡を行わずに、一時的にサービスを停止させる場合がございます。また被害を拡大させないための予防

的サービス停止もございます。

具体的にはクラウドプラットフォームの障害による物理サーバー・ネットワーク機器の停止、上位回線の障害によるサービスへのアクセス障害等になります。他のお客様で発覚したセキュリティホールが他環境にも共通する場合は、当該環境の停止等を行います。

5.2 セキュリティパッチ

ご提供のファイルサーバーは構築時点での当社推奨のセキュリティパッチを適用して出荷させて頂いております。追加セキュリティパッチを適用する場合は、システムの再起動が必要となるためお客様の許可がない状態での適用は実施しておりません。適用をご希望の場合は、当社サポートへご連絡ください。毎月 1 回/サポート時間内の対応が基本となります。セキュリティパッチの種類・適用数により再起動後の起動時間にばらつきがございます。30 分～2 時間近くかかる場合もございますので、停止可能な時間に余裕がある時にご依頼ください。なお、サポート時間外でのセキュリティパッチ適用は有償にて対応可能です。

5.3 お客様データへのアクセス

運用中のファイルサーバーにあるお客様データ領域の操作（閲覧・削除・移動・コピー等）を当社で実施することはありません。お客様から要望があった場合でも、当社側ではデータ操作を行うことは出来ませんのでご了承ください。

なお、お客様管轄のファイルサーバーから当社ファイルサーバーへデータ移行する場合は、データ移行作業の終了後にコピー元、コピー先の領域サイズやファイル数等で全ボリュームのデータの整合性を必ずご確認ください。また、お客様管轄のファイルサーバーからデータを削除する必要がある場合は、クライアントの接続先変更を含むファイルサーバーへの運用移管が完了してから実施してください。コピー等に失敗している場合でも、当社ではデータ復元に関する一切の責任を負うことが出来ませんので、移行が完了するまではお客様にてデータを管理して頂きますよう、よろしくお願いいたします。

5.4 バックアップ

ファイルサーバーサービスでは別途バックアップオプション（定期スナップショット/ミラー/VSS）を申込み頂いているお客様のみバックアップを実施しております。

バックアップオプションをお申込みで無い場合、万が一障害が発生した場合にデータを紛失しても当社は責任を負いかねます。ファイルサーバーとは物理的に別のディスクに保管される「定期スナップショット」または、「ミラー」オプションをご利用ください。

6 障害

ファイルサーバーサービスで障害が発生した場合、当社監視サーバーが検知し、サポート対応を開始します。アラート内容を確認後に復旧作業を開始いたします。

6.1 障害定義

障害とは、以下に記載する事象に起因する「当社監視環境とファイルサーバーへの接続が出来なくなった場合」と定義しております。お客様環境の問題、お客様の操作ミス等人的要因に関する事象についてはお客様主導で復旧して頂く形になります。

お客様環境側の定期停電・VPN ルーター停止・再起動等、当社側で障害通知されるメンテナンス業務においては、事前にご連絡ください。

1) ファイルサーバーサービス障害
   - 当社の監視サーバーからの応答要求に反応しない場合（10 分間以上継続）
   - リモートデスクトップで接続時にオペレーティングシステムの応答が無い場合（マウスカーソルが反応しない）
   - ファイルサーバーが起動している物理サーバーの障害
   - Windows オペレーティングシステムのバグ等、ソフトウェアに起因する障害

2) インターネット・拠点間 VPN の通信ができない状態（ファイルサーバーサービスのみ）
   - AWS クラウド環境ネットワークの障害
   - その他、クラウド環境に設置しているネットワーク機器の障害

3) 例外
   - お客様環境において契約している回線の障害に起因する接続断
   - お客様環境でご利用頂いている Firewall 等ネットワーク機器の障害に起因する接続断
   - クライアント PC・クライアント端末へのアプリケーションインストール・設定変更に伴う障害
   - 特定のクライアント端末に限定される接続断（お客様環境の他端末では接続が確認出来ている場合）
   - 前述した、ファイルサーバーに対する設定変更に起因する接続断
   - お客様の操作ミスによるファイル等の損失

※ 障害要因の切り分けを行った結果、お客様環境に限定されるパフォーマンス等の問題に関してはクラウド環境の性質上障害扱いとなりませんのでご了承ください。

※ 永続的なパフォーマンス低下はご利用環境、接続数、用途が原因の場合がございます。つきましては上位サーバータイプへのアップグレードもご検討ください。なお、サーバータイプの切り替えの際には再起動が必要となります。

6.2 対応内容

ファイルサーバーサービスの障害には、主に物理障害（AWSクラウド基盤障害）と、論理障害（サービス障害）があります。ファイルサーバーサービスの利用ができなくなるようなサーバー側の障害では24時間365日で復旧対応を行います。クライアントPC1台からのみ接続ができないなどの問題は平日日中帯でのサポート対応となります。

6.2.1 AWSクラウド基盤障害（ハードウェア故障など）

ファイルサーバーサービスが稼働しているクラウド基盤に障害が発生した場合の対応を記載します。AWSが提供する「Status Check」および、「Auto Recovery」機能を利用しております。ハードウェア故障などにより、Windows OSからのレスポンスがなくなった場合には、自動的に復旧処理が行われます。なお、当社監視システムによる死活監視（ping監視）にても検知し、当社サポートへアラートメールが発報されます。

例として、クラウド基盤の障害によってWindows OSがフリーズした場合には、以下の処理が自動で行われます。

1. AWSシステムによる「Status Check」機能により障害発生を検知。
2. AWSシステムによる「Auto Recovery」機能によりWindows OSを強制停止。
3. AWSシステムによりWindows OSを正常なクラウド基盤上で起動。
4. 当社サポートによる正常性確認（当社環境からの接続確認など）。

※ AWSシステムによる復旧処理が正常に完了しない場合には、当社サポートにて復旧対応を実施します。

6.2.2 ファイルサーバーサービス障害（CIFS接続エラーなど）

Windows OSは稼働しているが、OS上で稼働しているサービスレベルでの不具合などにより、ファイルサーバーサービスが利用できなくなった場合には、当社サポートにて復旧対応を実施します。なお、サービスレベルでの不具合の場合には、監視システムで検知ができないケースがあ

ります。ファイルサーバーサービスへの接続ができない場合には、当社サポートへご連絡ください。

1. 監視システムによる障害検知（または、お客様からの連絡による障害発覚）。
2. 当社サポートによる復旧対応（サービス再起動/Windows OS再起動など）。
3. 当社サポートによる正常性確認（当社環境からの接続確認など）。

ファイルサーバーサービスに障害が発生すると、お客様環境からは接続できない状態（通信断）になります。通信断になった場合でもOffice系アプリケーションの場合は編集中のデータはクライアント側に保管されており、Access等のデータベース形式は直前のトランザクションがファイルサーバーに保管されております。上記より通信が復旧した段階で再度ファイルを保存（場合によっては別名保存）する事でファイルの消失は防げますが、別の要因が重なった場合によりファイルを失う事も想定されますので、「ミラー」「定期スナップショット」の各オプションをご利用ください。

6.3 障害連絡

障害発生時および、復旧時には当社サポートからお客様へご連絡します。なお、障害発生から復旧までの時間が短時間である場合には復旧連絡のみとなる場合があります。

ファイルサーバーサービスに障害が発生した場合のお客様への連絡と連絡方法は、申込書に記載していただいた内容に沿います。

1. 平日10:00～18:00（弊社サポート時間内）

連絡先	連絡方法
申込書記載の技術担当者様	電話および、メール

2. 休日夜間（弊社サポート時間外）

連絡先	連絡方法
申込書記載の技術担当者様	申込書記載の連絡方法 （電話または、メールのみ）

報告書については原則として提出しておりませんのでご了承ください。ご要望があるお客様へは、メールにて障害発生日時と障害内容をご連絡させていただいております。なお、AWSクラウド基盤側の障害では、詳細な障害内容が公表されず、お客様へご連絡できないことがございます。

※ 障害連絡は6.1障害定義の障害であり、ディスク容量閾値アラートなどのサービス停止に至っていないものについては、サポート時間内での対応となります。

6.4 サーバー監視

ファイルサーバーは、当社監視サーバーより一定間隔で監視されており、異常を検知した場合には当社へアラートメールを発報する仕組みとなります。当社ではアラートメール検知後、ファイルサーバーの状態を確認の上で、必要に応じてお客様へご連絡させていただきます。当社にて監視している内容を以下に記載いたします。

- ファイルサーバー自体の死活監視（ping による監視）
- ファイルサーバーとして提供しているデータ領域の使用率監視

データ領域の使用率が監視閾値を超えた時点でお客様へご連絡させていただきます（標準 80%）。その他リソース監視（CPU 監視/メモリ監視）についてのデータ開示は行っておりません。また、監視のカスタマイズは基本的には行っておりませんのでご了承ください。

6.5 データリストア

万が一データが消失した場合でも、データ保護の項でご説明した通りファイルサーバーは別途バックアップオプション（VSS/スナップショット/ミラー）を申込み頂いているお客様のみバックアップを実施しております。データが消失した場合はこちらのデータからリストアを実施いたします。

バックアップオプションをお申込みで無い場合、万が一障害時にデータが消失しても当社は責任を負いかねます。バックアップ方式は前述の方式以外にも様々な方式を用意しておりますので一度ご相談ください（一部コンサルティング費用が別途かかります）。

7 納品業務について

7.1 納品業務分掌

当社サービスは以下の業務分担にて納品致します。

7.1.1 構築準備

当社サービス部門にて本サービスの基本構築を実施するに際し、お客様より情報提供をお願いいたします。必要な情報は当社フォーマットでご提供しております「契約申込書」に記載頂きます。また接続方法（SSTP、OpenVPN、IPSec）等の情報および、カスタマイズが必要な構成の場合は、当社エンジニアがお伺いしてお客様の要望をヒアリングさせて頂く場合がございます。

7.1.2 コンサルティング

当社サービスを導入する際に、お客様ネットワーク環境の最適化や業務の見直し等を実施する場合は、別途コンサルティングを実施させて頂きます（内容により有償）。

コンサルティングを実施する場合の必要な情報に関しては別途ご連絡させて頂きますが、最低限以下の情報が必要となりますので、ご準備のほどよろしくお願いいたします。

- ネットワーク構成図（IP・ネットワークセグメント等が記載されているもの。当社サービスを利用する拠点、セグメント分）
- 回線情報（ルータを新規導入する場合）
- クライアント PC の情報（オペレーティングシステム等）

これら必要な情報を加味し、最適な構成をご提案させて頂きます。

7.1.3 構築

頂いた情報より「注文内容のご確認」メールを送付させて頂いております。またこちらのメールに「スタートアップガイド」を添付しておりますので、サービス開始までの流れをご確認いただけます。なお、sapphire サービス等、他サービスとの組み合わせの場合は別途ご連絡差し上げております。構築・出荷確認が完了しましたら、ご担当者様宛に「開通のご連絡」メールを送付させて頂きます。

7.1.4 セットアップ

お客様にて、当社サービス担当より送付された「開通のご連絡」メールに記載の手順にて、クライアントのセットアップおよび、提供サービスへの接続確認をお願いいたします。セットアップに関するお問い合わせが必要な場合は次節をご覧ください。

7.2 納品ワークフロー

各サービスの「スタートアップガイド」をご覧ください。

7.3 納品物

当社サービスを申込みいただいた場合の納品物を記載致します。ファイルサーバーサービスの場合、接続ガイドはオペレーティングシステム別に用意がございます。ただし基本サービスでご提供させて頂くのは当社が対応しているオペレーティングシステムのみとなります。

- ファイルサーバーサービス

① FSCv3スタートアップガイド.pdf

ファイルサーバーサービス利用までのイメージガイドです。

② FSCV3開通案内（ファイルサーバー名）（貴社名）.pdf

管理者様用の情報です。。ファイルサーバーオペレーティングシステムへログインするためのアカウント情報や、VPNインストーラー/VPN証明書をダウンロードする際のアカウント情報が記載されております。また、ユーザー様に配布して頂きたい情報も記載しております。

③ ファイルサーバーサービス仕様書

本書とは別にサービス仕様について記載した説明書です。

7.4 必要条件

当社サービスを滞りなく納品する為に必要な条件は以下となります。

- 申込書に記載の情報に誤記・漏れがないこと
- 構成情報等に誤りが無い事。また構築途中段階で構成等の変更が無いこと
- お客様管理機材（FW・回線等）の準備および必要な設定が実施されていること
- お客様クライアント環境からインターネットに接続できる環境が用意されていること
- 当社サービスの関連情報はメールベースで提供しているため、メール環境が準備されていること
- お客様クライアントが HTTP で当社 Web サーバーおよび指定サーバーにアクセス出来ること

※ ファイルサーバーサービスの場合、4TB以上の納期をご相談させて頂きます。

※ 注文状況、当社側環境の増強等が必要な場合は別途納期をご相談させて頂きます。

7.5 サービス納期

納期は当社が注文書及び申込書を受領した翌日を起点として 5 営業日後の出荷を基本とさせて頂いております。なお、本項で定義している“納期”とは

「当社サービスをお客様拠点からご利用いただける状態にしてお引渡しまでの日程」

となり、クライアント端末からご利用いただける状態にするには、当社から送付させて頂くアクセス情報を元に、クライアント環境をセットアップする作業がございます。この作業が完了して初めてファイルサーバーをご利用いただけますので、サービス開始日程を検討する際はご注意ください。またデータ移行をご依頼頂いている場合は、接続可能状態にした後でデータ移行を行います。

スマホ&タブレットオプションをご利用いただくお客様については、サーバーに公的証明書の配置が完了した段階での出荷となります。

7.6 作業終了確認・検収

「開通のご連絡」メールの送付を以って当社構築作業の完了と致します。メール受領後に、すみやかに納品された当社サービスをご確認頂き、検収をお願い致します。またファイルサーバーサービスのデータ移行オプションを発注頂いた場合は「開通のご連絡」後にデータコピーを開始致します。課金は「開通のご連絡」メールの送付にて開始とさせていただきます。

8 請求業務について

8.1 請求処理

請求処理は以下の部門が執り行います。

担当部署名	電話	FAX	メール
サービス企画グループ	03-6821-2345	03-4496-5431	es-kanri@b-architects.com

8.2 請求

ご利用の翌月初めに、お客様ご指定の宛先に請求書を送付します。なお、起算日が月半ばであった場合の請求額の算定方法は、契約に依存（日割り処理など）します。

請求の手続き等でご入金が遅れる場合は早急に下記宛先までご連絡ください。ご連絡を頂いてない場合での未入金に関しては約款に基づきサービスの停止、別途延滞金を請求する場合がございます。

以上