White Paper

# ナラティブブック

第 1.2 版

2025 年 12 月 8 日

クロスケアフィールド株式会社

# はじめに

### White Paper の目的

ナラティブブックは利用者と利用者を見守る専門家の書き込みを集約・保管することにより、利用者本人へのより適切なサポート提供の環境づくりを実現する、当社のクラウドサービスです。

本ドキュメントは、ナラティブブックの提供において基盤として利用するクラウドサービスにおけるセキュリティに関する方針、並びにプロセスの概要をご理解いただくとともに、ISMS クラウドセキュリティ認証である ISO/IEC 27017 の要求に従う公表を行うことを目的とします。

なお、本書では下記の様に用語を定義します。

・ユーザ　ナラティブブックシステムの利用アカウントを持つすべての方
・利用者　ナラティブブックシステムを利用して、自身の情報を管理する本人

### White Paper の対象

ナラティブブックの導入を検討中の方
ナラティブブックを利用中の方

### クラウドコンピューティングのための情報セキュリティ方針

当社では、クラウドコンピューティングに関する情報セキュリティの方針を定め、ユーザ様に満足いただける機能的でセキュアなサービスの提供を目指しています。

> **クラウドコンピューティングに関する情報セキュリティ方針**
> 当社は、クラウドコンピューティング環境におけるユーザ様の情報資産を情報セキュリティ上の脅威から保護するための措置を講じ、ユーザ様が安心してご利用いただけるセキュアなサービスを提供します。

当社の「情報セキュリティ方針」は以下の URL からご確認頂けます。

https://xcf.co.jp/isms/

### 情報セキュリティ組織

当社では、情報セキュリティに関する統括責任者を任命し、情報セキュリティに関する統括責任と権限を与えています。また、情報セキュリティ委員会を設置し、情報セキュリティのマネジメントシステムの運用と継続的改善に取り組んでいます。

**地理的所在地**

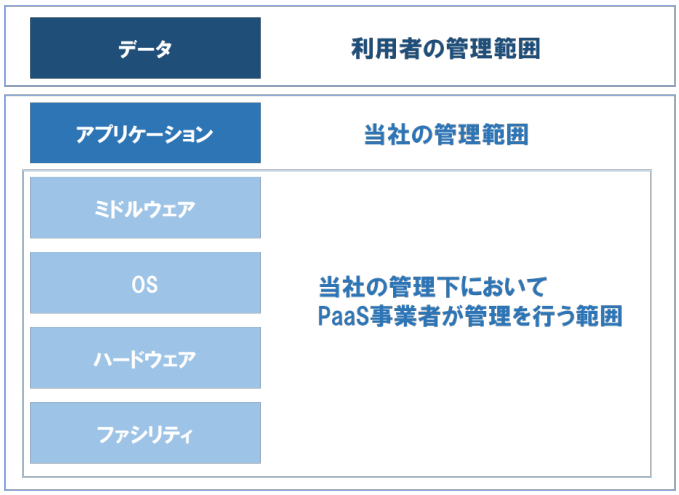
当社の所在地、並びに当社がお客さまのデータを保存する国は日本国となります。当社が基盤として利用するクラウドサービスにおいて、日本国以外のリージョンにユーザ様のデータを保存する必要性が生じた場合、ユーザ様に事前に通知したうえで行います。

**責任範囲（共有 Model）**

仮想レイヤーや施設におけるコンポーネントは、当社が基盤として利用するクラウドサービス事業者によって管理されます。当社は、当社のサプライヤーに対するセキュリティポリシーに従い、調達時のセキュリティ審査、及びパフォーマンスのモニタリングによりクラウドサービス事業者を管理します。

また、当社は、基盤上に構築したアプリケーションに対して責任を負います。

アプリケーション上のデータについては、ユーザ様の責任において保護していただく必要があります。




当社の責任

・ナラティブブックのセキュリティ対策

・ナラティブブックに保管されたユーザ様情報の保護

ユーザ様の責任

・利用者アカウントの管理（登録、削除、権限設定、管理者設定、アクセス権の設定など）

・パスワード等の利用者の秘密認証情報の管理

・ユーザ様が取扱うデータに対してのバックアップ

**情報セキュリティの意識向上，教育及び訓練**

当社は、全従業員に対する定期的な情報セキュリティ教育を実施し、情報セキュリティに対する意識向上に努めています。また、クラウドコンピューティングに関する契約相手に対しても、同等レベルの教育を求めています。

### 情報セキュリティのパフォーマンス評価

当社では、定期的（最低でも年に一回）に情報セキュリティに関する内部監査を実施しています。定期的な内部監査以外に、組織、施設、技術、プロセス等の重大な変化にあわせて、独立した内部監査を行っています。

### インシデント対応プロセス

当社では、ISO/IEC27001 に準拠した標準化された情報セキュリティインシデント対応プロセスを整備しています。情報セキュリティインシデントに関する報告、エスカレーションに関する全ての手順が文書化され、情報セキュリティ委員会により一元的に管理されています、報告されたインシデントはインパクトや緊急性に応じてハンドリングされています。

## 開発/調達

### 開発プロセス

当社のクラウドサービスの開発は、機能性とユーザビリティの確保はもちろんのこと、情報セキュリティについても配慮することを方針として行われます。開発は非機能要件としてのセキュリティ要件を定義し、厳格な承認プロセスを得たうえで実施されます。セキュリティ機能に関するソースコードはレビューされ、テストプロセスを経たうえでビルドされます。

### サプライチェーン

当社のクラウドサービスの提供に関連するサプライヤー、及びサプライチェーンは以下の手段により管理することを方針としています。

・情報セキュリティ水準を当社と同等又はそれ以上に保つことを事前の審査により確実にする
・契約により秘密保持の確保を担保する
・サプライヤーがサプライチェーンを形成しサービス提供している場合、サプライヤーのサプライチェーンメンバーに対するセキュリティ管理の能力について審査する

# アプリケーションのセキュリティ機能

### 情報セキュリティ機能

主にユーザ様が検討される情報セキュリティ機能として、本ホワイトペーパーは以下を記述しています。

| 機能（ISO/IEC27017 の管理策） | 本ホワイトペーパーの記述 |
|---|---|
| A.9.2.1 利用者登録及び登録削除 | 利用者アクセスの管理 |
| A.9.2.2 利用者アクセスの提供 | 利用者アクセスの管理 |
| A.9.2.3 特権的アクセス権の管理 | 認証情報の管理 |
| A.9.2.4 利用者の秘密認証情報の管理 | 認証情報の管理 |
| A.9.4.1 情報へのアクセス制限 | 利用者アクセスの管理 |
| A.10.1.1 暗号による管理策の利用方針 | 暗号化 |
| A.12.3.1 情報のバックアップ | バックアップ |
| A.12.4.1 イベントログ取得 | ログ |
| CLD.12.4.5 クラウドサービスの監視 | クラウドサービスの監視 |

### 利用者アクセスの管理

ナラティブブックは、ユーザ様がストレスなく、安全に利用者アクセスの管理を行うためのユーザインターフェイスと機能を提供します。
お客さまは管理者画面から簡単な操作によりアカウント登録・削除を行い、またユーザに対する権限の割り当てを行うことが出来ます。使用方法の詳細は「ユーザマニュアル」をご参照ください。

### 認証情報の管理

初期のアカウント登録手順は「ユーザマニュアル」をご参照ください。
アカウント作成に先立って登録メールの疎通確認があります。登録したメール本文のリンクからアカウントを作成ください。
パスワードの設定はユーザ様のセキュリティポリシーにもとづいて実施してください。

管理者権限はユーザ様のセキュリティポリシーに従い厳重に管理することをお願いします。

### 暗号化

データベースに保管されるユーザ様データは、AES-256 暗号化アルゴリズムを使用して暗号化しています。
ユーザ様のパスワードは、ハッシュ化をしています。

ナラティブブックとユーザ様との間での通信は、SSL/TLS で暗号化し、情報の盗聴等のリスクに対処しています。

# 運用

### 変更
ユーザ様に影響を与えるナラティブブックの重要な変更は、ご登録頂いたメールアドレス宛への事前通知、ログイン直後の通達画面、ナラティブブックランディングページのお知らせの項目にて告知します。

### 管理者用手順
「ユーザマニュアル」等の各種マニュアルの提供に加え、お問い合わせ画面よりサポートを提供しています。また、サーポートセンターでは電話によるサポートにも対応しています。

### バックアップ
システム及びユーザ様データのバックアップは、日次で 35 世代分のデータを保持します。ただし、ユーザ様からのバックアップデータの復元等に関するご要望には対応してせん。

### ログ
ナラティブブックの維持管理に必要となる適切なログを取得しています。
ユーザ様が必要となる場合は、当社のナラティブブックサポートセンターまでご相談ください。

ナラティブブックは、基盤として利用するクラウドサービス事業者が提供する時刻同期サービスを利用し時刻同期を行っています。
ログは GMT で提供されます。

### クラウドサービスの監視
当社は、ナラティブブックが正常に提供され、他社を攻撃する基盤として使用される等に不正に使用されていないこと、データの漏洩が発生していなか等の監視を行っています。
監視結果をユーザ様に公開できるサービス機能は有しておいません。監視結果が必要な場合は、当社のナラティブブックサポートセンターまでご相談ください。

### 技術的脆弱性の管理
アプリケーションを構築する上で使用するソフトウェアに脆弱性が検知された場合、ナラティブブックのトップ画面およびランディングページのお知らせで通知し、速やかに影響調査を行います。
脆弱性情報の収集は以下の手段により行います。

・JPCERT コーディネーションセンターから公開される脆弱性情報
・当社関係者による検知
・ユーザ様、基盤を提供するクラウドサービス事業者等の外部からの情報提供

検出した脆弱性については、速やかに影響調査を行い、必要な対策を講じます。対策の状況は随時、ナラティブブックのトップ画面およびランディングページのお知らせにて公表します。

**容量・能力の管理**

当社は、サーバリソース、及びネットワークリソースを監視しています。またリソースの増減は GUI から瞬時に実行することができます。サーバリソースはインスタンスの構成を変更せずにスケールアップによることを原則としていますが、将来的なニーズに照らして、必要があればスケールアウトによる対応も行います。

**負荷分散/冗長化**

ナラティブブックは基盤を提供するクラウドサービス事業者のマネジメントサービスを使用し、複数の仮想サーバに処理を振り分ける、ロードバランシングを採用しています。

また、アプリケーションの構成はコンテナイメージとして保存し、即時に複製が可能な状態を整えています。

**インシデント対応**

ナラティブブックに関連した情報セキュリティインシデントを検出した場合、以下の内容で速やかに通知します。

ギリシャ語のアルファベット

| 項目 | 内容 |
|---|---|
| **報告する範囲** | データの消失、長時間のシステム停止等のユーザ様に大きな影響を及ぼす可能性のある情報セキィリティインシデント |
| **対応の開示レベル** | 当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、すべて同等のレベルで対処します。 |
| **通知を行う目標時間** | 検知から 72 時間以内を目標に通知します。 |
| **通知手順** | ご登録頂いたメールアドレス宛、管理者画面<br>（必用に応じて電話等の手段を使用する場合もあります。） |
| **問合せ窓口** | ナラティブブックサポートセンター |
| **適用可能な対処** | 当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、あらゆる手段を講じて対処します。 |

また、ユーザ様において情報セキュリティインシデントを検出された場合、またはその疑いをもたれた場合は、ナラティブブック内のお問合せページ、又は当社ナラティブブックサポートセンターからご連絡ください。

**サービス利用停止後のデータの扱い**

ナラティブブックで利用者様が作成・保存した利用者様のデータの削除に関しては削除要請の手続きを受理してから 60 日以内に削除を実施します。ただし、利用者様のデータを含まないサービス共通のログデータは対象外になります。

**利用者様の登録データの削除要請の手順**

ナラティブブックのお問い合わせフォームのお問い合わせ内容に「退会ユーザーのデータ削除要請」と記載し、お名前、フリガナ、メールアドレスを記入して送信ください。
担当者がお問い合わせを受理後、メールにて「保有個人データ開示等請求書」を送付いたしますので、「保有個人データ開示等請求書」に削除に関わる必要事項を記入の上、返信ください。
担当者が「保有個人データ開示等請求書」の内容を確認後、登録データの削除を実施します。

**装置のセキュリティを保った処分又は再利用**

当社は、情報システム管理者に装置の処分又は再利用に関する役割を集中し、従業員による個別対応を排除することで、セキュア且つ確実な装置の処分又は再利用を実現しています。

# その他

### 証拠の収集
法令また権限のある官公庁からの要求によりナラティブブック上にあるデータ等の情報を、当該官公庁またはその指定先に開示もしくは提出することがあります。合意について別途、「利用規約」をご参照ください。

### 適用法令及び契約上の要求事項
利用契約に関する準拠法は、日本法とします。

### 知的財産権
本サービスを構成する有形または無形の構成物（プログラム、データベース、画像、マニュアル等の関連ドキュメントを含むがこれらに限られない）に関する著作権を含む一切の知的財産権その他の権利は当社に帰属します。

### 記録の保護
アプリケーションにおけるデータ操作等のログはユーザ様にて保護して頂く必要があります。当社は、仮想ネットワークへのアクセスに関するログ、及びサービスのバージョンアップに関する内部要員による作業ログを一定期間保存します。

### 暗号化機能に対する規制
ナラティブブックにおいて暗号化の規制対象になる地域にはサービスを提供していません。

# 第3者認証

### ISO/IEC27001

当社は、全社を認証範囲として 2016 年 5 月 9 日に ISMS（Information Security Management System）の国際規格である ISO/IEC27001 を取得しています。

### ISO/IEC27017

当社は、ナラティブブックサービスを認証範囲として 2025 年 4 月 20 日に ISMS（Information Security Management System）のアドオン規格である ISO/IEC27017 を取得しています。

# ナラティブブックに関するお問い合わせ

ナラティブブックサポートセンター

TEL：　050-3188-3610

メール：support@narrativebook.jp

# 更新履歴

| 版数 | 日付 | 更新内容 |
|---|---|---|
| 第 1.0 版 | 2025 年 2 月 28 日 | 初版 |
| 第 1.1 版 | 2025 年 4 月 10 日 | 情報セキュリティのパフォーマンス評価に「ISO/IEC27017 認証の取り組み」を追加 |
| | | 「適用法令及び契約上の要求事項」を変更<br>「知的財産権」を変更 |
| | | 暗号化の誤記修正 |
| 第 1.2 版 | 2025 年 12 月 8 日 | 情報セキュリティのパフォーマンス評価から ISO/IEC27017 認証の取り組みにおける内部監査の結果を、お客様の要求に応じ開示致しますので、以下のお問い合わせフォームよりご連絡ください。<br>お問い合わせフォーム：<br>https://narrativebook.jp/contact を削除 |
| | | 第三者認証に ISO/IEC27017<br>当社は、ナラティブブックサービスを認証範囲として 2025 年 4 月 20 日に ISMS（Information Security Management System）のアドオン規格である ISO/IEC27017 を取得しています。を追加 |
| | | 「保有個人データ削除依頼書」を「保有個人データ開示等請求書」に変更<br>「保有個人データ開示等請求書」に削除に関わる必要事項を記入の上、返信ください。に変更 |
| | | ログの日本標準時（UTC＋９）を GMT に変更 |
| | | ページ番号を追加 |