



NILTO セキュリティホワイトペーパー

2025年03月19日

フェンリル株式会社

# 目次

## 目次

1. 方針と体制
  2. 利用者との責任分界点
  3. データ保管場所
  4. データの削除
  5. ラベル付け機構
  6. 利用者登録及び削除
  7. アクセス権の管理
  8. パスワードの配布方法
  9. 暗号化の状況
  10. 変更管理
  11. 手順書の提供
  12. バックアップの状況
  13. ログのクロックに関する情報
  14. 脆弱性管理に関する情報
  15. 開発におけるセキュリティ情報
  16. インシデント発生時の対応
  17. ユーザーデータの保護および第三者提供
  18. 適用法令
  19. 認証
  20. 外部クラウドサービスの利用
- 改定履歴

## 1. 方針と体制

### フェンリル株式会社(以下『当社』と表記)の方針

当社は情報セキュリティ基本方針 (<https://www.fenrir-inc.com/jp/about/security/>) を掲げ、基本方針を遵守し、情報資産の機密性、完全性、可用性の情報セキュリティを維持するための活動を実践します。

### セキュリティ体制

当社は不可抗力による損失、破損、改変、不正アクセスもしくは漏えい、または不法行為による破壊といったセキュリティインシデントからユーザーデータを保護するために、セキュリティ体制を確立します。組織的・人的・技術的・物理的など様々な観点から適切な対策を実施し、それらを維持管理します。

## 2. 利用者との責任分界点

### 当社の責任

当社は、以下のセキュリティ対策を実施します。

- 当社が提供するサービス（NILTO）のセキュリティ対策
- 上記サービスに保管されたユーザーデータの保護
- 上記サービスの提供に利用するミドルウェア、OS、その他インフラのセキュリティ対策
- 上記サービスの運用にかかわるアカウントの適切な管理(登録、削除、管理権限の付与など)

### 当社におけるユーザーデータの取り扱い

- 当社の従業員が利用者の承諾なくユーザーデータを処理することはありません。当社の従業員は、ユーザーデータに関して秘密保持義務を負っており、かかる義務は、職責を離れた後も継続します。
- 利用規約や関連する規約、プライバシーポリシーにおいて規定されている場合を除き、当社が本サービスの使用を通して受領するユーザーデータを業務委託先を含む第三者に転送することはありません。
- 当社は、以下の目的でユーザーデータを使用します。
  - 利用者に本サービスを提供すること  
これには、本サービスの運用に影響する問題の防止、検出、および修復を目的とするトラブルシューティング、ならびに発生し拡散する脅威（マルウェアやスパム）を検出し、ユーザーデータを保護する機能の改善が含まれます。
  - 法令等に基づく開示要請に対応するため当社は、法令により要求される場合を除いて、ユーザーデータを法執行機関に開示しません。法執行機関が当社に対してユーザーデータの開示を要求した場合、当社は、法執行機関に対して、ユーザーに直接要求するように要請します。この手順の一環として、当社はユーザーの基本的な連絡先情報を法執行機関に提供することがあります。法執行機関によりユーザーデータの開示を強制された場合、当社はかか

る開示を行う前に、ユーザーに通知するための商業上合理的な努力をします。

## 利用者の責任

利用者は、以下のセキュリティ対策を実施する必要があります。

- パスワードの適切な管理(二段階認証で利用するデバイスの適切な管理も含む)
- アカウントの適切な管理(登録、削除、管理権限の付与など)
- 登録したユーザーデータの適切な管理
- 当社から通知可能なメールアドレス等の正確な連絡先の登録

### 3. データ保管場所

お客様からお預かりしたデータは、下記に示すクラウドベンダーのデータセンターに保管されます。

データ種別	データ保管場所
登録事項	Google Cloud (日本 東京都)
コンテンツデータ	Google Cloud (日本 東京都)
メディアデータ	Google Cloud (日本 東京都)
コンテンツデータおよびメディアデータのキャッシュ	Fastly エッジサーバ ※Fastlyのエッジサーバは世界の各地に広く配置されており、利用環境により保管場所が異なります。全ての保管場所については、Fastly Network Map ( <a href="https://www.fastly.com/network-map">https://www.fastly.com/network-map</a> ) を参照してください。
監査ログ ( <a href="https://www.nilto.com/ja/docs/topics/audit_log">https://www.nilto.com/ja/docs/topics/audit_log</a> )	Google Cloud (日本 東京都)

## 4. データの削除

ユーザーデータ（3. データ保管場所 データ種別に記載）については、ユーザーアカウントが削除されてから最大で60日以内に完全に削除されます。削除されたユーザーデータは、弊社でも復旧できません。

ただし、一部のユーザーデータについては、サービスの改良等を目的として、個人が特定されないよう配慮したうえで、ユーザーのサービス利用状況等の情報を解析・加工して活用できるものとしています。

### ログの保護と削除

当社のサービスはアクセスログおよびアプリケーションログをGoogle Cloud 上に保存します。このログは、特定業務従事者のみアクセス可能としています。ログの保存期間は30日とします。その保存期間の経過後に削除されます。

### 装置のセキュリティを保った処分又は再利用

当社が契約するクラウドサービスプロバイダが構築する仮想環境上で提供しており、当社が直接処分または再利用を行う資源（装置、データストレージ、メモリ、ファイル）は、保有しておりません。当社が契約するクラウドサービスプロバイダが、契約に基づき資源の処分または再利用を適切に実施していることを確認します。

## 5. ラベル付け機構

当社のサービスでは情報を分類するための様々な設定や機能（ラベル付け機構）を提供します。こちらの章では主にアカウントのアクセスを制御する機能を紹介します。

- スペースメンバー ([https://www.nilto.com/ja/docs/topics/space\\_member](https://www.nilto.com/ja/docs/topics/space_member))
- スペースロール ([https://www.nilto.com/ja/docs/topics/space\\_role](https://www.nilto.com/ja/docs/topics/space_role))
- タグ設定 (<https://www.nilto.com/ja/docs/topics/tag>)

## 6. 利用者登録及び削除

### 利用者登録

お客様は、アカウント登録または組織への招待を受けて、ユーザーアカウントを作成できます。アカウント登録時に作成されたユーザーアカウントは、組織オーナーとなり、下記”組織への招待”などの組織の管理を行うことができます。

- アカウント登録 ([https://www.nilto.com/ja/docs/topics/add\\_account](https://www.nilto.com/ja/docs/topics/add_account))

### 利用者削除

利用者は、いつでも自由にユーザーアカウントを削除することができます。ただし、利用者が組織オーナーである場合は、他の利用者にオーナー権限を譲渡しなければ、削除することができません。

ユーザーアカウントの削除は、利用者自身のみが行うことができます。

- アカウント削除 ([https://www.nilto.com/ja/docs/topics/account\\_setting#6f3b24e5b8d8d232393e5047779e99a27a6116f4](https://www.nilto.com/ja/docs/topics/account_setting#6f3b24e5b8d8d232393e5047779e99a27a6116f4))

### 組織への招待

招待権限を持つ利用者は、いつでも自由に新たな利用者を組織へ招待することができます。

- メンバーの追加 ([https://www.nilto.com/ja/docs/topics/org\\_member#2aafb83a8115e9e9537338f40543f80ebdf12588](https://www.nilto.com/ja/docs/topics/org_member#2aafb83a8115e9e9537338f40543f80ebdf12588))



## 組織からの除外

管理者は、いつでも自由に組織内の利用者を組織のメンバーから除外することができます。除外することで、組織内のスペースを利用できなくなります。

- メンバーの削除 ([https://www.nilto.com/ja/docs/topics/org\\_member#088364fbb24660736b806234849e613e06509e86](https://www.nilto.com/ja/docs/topics/org_member#088364fbb24660736b806234849e613e06509e86))

## 7. アクセス権の管理

ユーザーは組織のメンバーのアクセス権を個別に設定することが可能です。

- スペースロール ([https://www.nilto.com/ja/docs/topics/space\\_role](https://www.nilto.com/ja/docs/topics/space_role))

## 8. パスワードの配布方法

- アカウント登録時、およびパスワードの再設定時に、利用者自らパスワードを設定します。本システムが作成するパスワードの配布はありません。
- パスワードの再設定方法 ([https://www.nilto.com/ja/docs/topics/reset\\_password](https://www.nilto.com/ja/docs/topics/reset_password))

## 9. 暗号化の状況

- 本サービスの利用において、お客様の端末と当社が提供するサービス間のインターネット通信は、SSL/TLS通信によって暗号化されます。
- データベースに保存されるユーザー情報やコンテンツデータについては、暗号化されませんが、適切なアクセス権にて管理されます。

## 10. 変更管理

利用者への影響があるサービスの変更や、サービス停止を伴うメンテナンスについての情報は、下記のリンク先から参照できます。

- NILTO公式ブログ (<https://www.nilto.com/ja/blog>)
- NILTO公式X ([https://x.com/nilto\\_jp](https://x.com/nilto_jp))

## 11. 手順書の提供

利用者および管理者が利用できる各種マニュアルは、下記リンク先より閲覧いただけます。

- NILTO公式ドキュメント ([https://www.nilto.com/ja/docs/topics/at\\_first](https://www.nilto.com/ja/docs/topics/at_first))
- NILTO API リファレンス (<https://www.nilto.com/api>)

## 12. バックアップの状況

- サービスのユーザーデータのバックアップを日次で7世代分取得、保持しています。
- バックアップデータの保管場所は、「3. データ保管場所」で指定された場所で保管されます。

## 13. ログのクロックに関する情報

- 当社が提供するサービス内のログ時間は、サーバーの時間であるGMT(UTC+0) またはJST(UTC+9) で取得されます。

## 14. 脆弱性管理に関する情報

- 定期的に脆弱性の情報収集を行い、お客様に影響を及ぼす、またはサービスの影響が発生する場合は、速やかに対応を行います。

## 15. 開発におけるセキュリティ情報

- 本サービスは、当社にて定めた規定に則ったセキュリティに配慮した開発を行っています。また、ソースコードの静的解析などにより脆弱性の確認を開発プロセスに組み込んで実施しています。

## 16. インシデント発生時の対応

- 当社が定めるセキュリティインシデントが発生しユーザーに影響がある場合、もしくは影響が発生する恐れがあると当社が判断した場合は、24時間以内を目安として当社の判断にもとづき、ブログまたは複数の手段により連絡します。
- 情報セキュリティインシデントに関する問い合わせは、下記の当社サイトの問い合わせページより受け付けています。
  - NILTO問い合わせページ (<https://www.nilto.com/ja/contact/others>)

## 17. 知的財産権

- 本サービスをご利用いただく上での知的財産権に関わるご相談は、下記の当社サイトの問い合わせページより受け付けています。
  - NILTO問い合わせページ (<https://www.nilto.com/ja/contact/others>)

## 18. ユーザーデータの保護および第三者提供

- 利用者から預かったデータを適切に保護することは、当社の責任です。
- ログデータを含むユーザーデータは、不正なアクセスや改ざんを防ぐため、各サービス開発チームの一部の人間しかアクセスできないよう設定されたアクセス権のもとで保管されます。
- 但し、裁判所からの証拠提出命令など、法的に認められた形で利用者のデータの提供を要請された場合、当社は、利用者の許可なく、必要最小限の範囲で、ユーザーデータを外部に提供する可能性があります。

## 19. 適用法令

- 利用者と当社との間の契約は、日本法に基づいて解釈されるものとします。

## 20. 認証

- 当社は、情報マネジメントシステム認定センター(ISMS-AC)のISMS適合性評価制度におけるISMS認証を取得しています
  - [https://isms.jp/lst/ind/CR\\_IS\\_x0020\\_633173.html](https://isms.jp/lst/ind/CR_IS_x0020_633173.html)

## 21. 外部クラウドサービスの利用

当社が提供するサービスでは、次に示す機能を運用するために、外部のクラウドサービスを利用しています。当社セキュリティホワイトペーパーに記載されている内容は、以下で示すクラウドサービスにて管理されている範囲には及ばず、また、その内容の遵守を保証するものではありません。

クラウドサービス	用途	運営会社
Google Cloud	インフラ構築、運用	Google LLC
Fastly	CDN	Fastly, Inc.
SendGrid	メール配信	SendGrid, Inc.
Stripe	決済	Stripe, Inc.
Slack	運用、カスタマーサポート	Slack Technologies, LLC
HubSpot	カスタマーサポート	HubSpot, Inc.

## 改定履歴

改定日	改定内容
2025/03/19	初版発行