ヌーラボセキュリティホワイトペーパー

2.3版

2025年6月26日

株式会社ヌーラボ

目次

目次
1. 方針と体制
    株式会社ヌーラボ (以下『当社』と表記) の方針
    セキュリティ体制
2. 利用者との責任分界点
    当社の責任
        当社におけるユーザーデータの取り扱い
    利用者の責任
3. データの処理と保管場所
4. データの削除
5. ラベル付け機構
    当社が提供するサービス共通
        チーム機能 (Backlogクラシックプラン除く)
    Backlog
        プロジェクト機能
        チーム機能 (Backlogクラシックプランのみ)
    Cacoo
        フォルダ機能
    Typetalk
        トピック機能
6. 利用者登録及び削除
    全サービス共通 (Backlogクラシックプラン除く)
        利用者登録
        利用者削除
        組織への招待
        組織からの除外
    Backlog (クラシックプラン)
    Nulab Pass
7. アクセス権の管理
    全サービス共通 (Backlogクラシックプラン除く)
    Backlog
    Backlog (クラシックプラン)
    Cacoo
    Typetalk
    Nulab Pass
8. パスワードの配布方法

ヌーラボアカウント
初期パスワード配布方法
パスワード変更方法
Backlog (クラシックプラン)
初期パスワード配布方法
パスワード変更方法
Nulab Pass
9. 暗号化の状況
利用者情報
サービスとの通信
データベースの暗号化
10. 変更管理
11. 手順書の提供
12. バックアップの状況
当社が提供するサービス共通
Nulab Apps / Nulab Pass
Backlog
Cacoo
Typetalk
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. 人的セキュリティに関する取り組み
17. インシデント発生時の対応
18. ユーザーデータの保護および第三者提供について
19. 適用法令
20. 認証制度
【ISMSクラウドセキュリティ認証登録範囲】
21. 外部クラウドサービスの利用
改定履歴

1. 方針と体制

株式会社ヌーラボ (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、可用性といった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 (Backlog、Cacoo、Typetalk、Nulab Apps(※1)、Nulab Pass) 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）

※1
Nulab Appsは、当社が提供するサービスで共有するアカウント (以下、『ヌーラボアカウント』と表記) などの機能を提供します。

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。
    1. 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。
    2. 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。

- アカウント (※2) の適切な管理 (登録、削除、管理権限の付与など)
- 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)
- 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

※2
以後、アカウントをユーザーと表記する箇所がありますが、全てアカウントと同義です。

3. データの処理と保管場所

データを処理し保管する場所

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でサービス提供に必要な処理を行い保管します。

サービス名	データを処理し保管する場所
Nulab Apps	AWS (米国 オレゴン州)
Backlog	日本語サイトからのお申込みの場合 AWS (日本 東京) 英語サイトからのお申込みの場合 AWS (米国 オレゴン州)
Cacoo	AWS (米国 カリフォルニア州)
Typetalk	AWS (米国 オレゴン州)
Nulab Pass	AWS (米国 オレゴン州) ※監査ログ以外のデータを保管 AWS (日本 東京) ※監査ログのデータのみを保管

データを処理する場所

特定の機能を通じて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でサービス提供に必要な処理を行います。データの保管は行いません。

サービス名	機能名	データを処理する場所
Backlog	AI アシスタント	日本語サイトから利用した場合 AWS (日本 東京) AWS (日本 大阪) AWS (韓国 ソウル) AWS (インド ハイデラバード) AWS (インド ムンバイ) AWS (シンガポール) AWS (オーストラリア シドニー) AWS (オーストラリア メルボルン)

		英語サイトから利用した場合 AWS (米国 オレゴン) AWS (米国 バージニア) AWS (米国 オハイオ)

4. データの削除

当社が提供するサービスの契約管理者がサービス利用終了手続(※1)を行った場合に、お客様からお預かりしたデータ(以下、『ユーザーデータ』と表記)を削除します。
また、正式なプラン申込みなくトライアルの期間が満了した場合や、当社が提供するサービスの利用料金の支払いを遅滞するなどして利用停止となった場合には、ユーザーデータを削除します。
この場合において、削除されたユーザーデータは、ヌーラボであっても復旧することができません。
削除する条件、削除タイミングおよび削除対象となるユーザーデータは、下記の”削除する条件と削除タイミング”のとおりとします。

※1
次のいずれかの操作を指します。(以下”サービス利用終了手続”について同じ)

- ヌーラボアカウントの”組織の削除”
- Backlogクラシックプランの”解約手続”

削除する条件と削除タイミング

	ユーザーデータが削除される条件	削除時期 (原則)
Backlog クラシックプラン	解約手続を実施済みであること	有料プランのスペースでは現在の契約期間終了から180日経過後、有料プランのトライアル中のスペースや無料プランのスペースでは解約手続の実施日から180日経過後にユーザーデータの削除作業を開始し、開始から10日以内に削除を完了します。(※)
	左記のプランについて正式な申込みなくトライアルの期間が	トライアル期間満了日から30日経過後にスペースの解約手

	満了したこと	続を実施します。解約手続の実施日から180日経過後にユーザーデータの削除を開始し、開始から10日以内に削除を完了します。（※）
	当社が提供するサービスの利用料金の支払いを遅滞するなどしてヌーラボ利用規約第9条第1項の定めにより利用停止になったこと	契約期間満了日から90日経過後にスペースの解約手続を実施します。解約手続の実施日から180日経過後にユーザーデータの削除作業を開始し、開始から10日以内に削除を完了します。（※）
Cacoo プラスプランおよび2019年11月26日以前申込のフリープラン	ヌーラボアカウントの削除が実施されること	ヌーラボアカウントの削除を実施したときにユーザーデータの削除作業を開始し、開始から10日以内に削除を完了します。（※）
上記以外のBacklog、Cacoo、Typetalk、Nulab Passのプラン	組織の削除が実施されること	組織の削除を実施して組織が削除されてから180日経過後にユーザーデータの削除作業を開始し、開始から10日以内に削除を完了します。（※）
	左記のプランについて正式な申込みなくトライアルの期間が満了したこと	トライアル期間満了日から30日経過後に、システムで自動的に組織を削除します。組織が削除されてから180日経過後にユーザーデータの削除作業を開始し、開始から10日以内に削除を完了します。（※）
	当社が提供するサービスの利用料金の支払いを遅滞するなどしてヌーラボ利用規約第9条第1項の定めにより利用停止になったこと	契約期間満了日から90日経過後に、システムで自動的に組織を削除します。組織が削除されてから180日経過後にユーザーデータの削除作業を開始し、開始から10日以内に削除を完了します。（※）
ヌーラボアカウント	ヌーラボアカウントの削除が実施されること	ヌーラボアカウントの削除を実施したときにユーザーデータの削除作業を開始し、開始から10日以内に削除を完了します。（※）

管理対象アカウント	組織の削除または管理対象アカウントの削除が実施されること	組織の削除を実施した場合は組織が削除されてから180日経過後にユーザーデータの削除作業を開始し、管理対象アカウントの削除を実施した場合はその実施のときにユーザーデータの削除作業を開始します。そして、削除開始から10日以内に削除を完了します。（※）
	Nulab Passについて正式な申込みなくトライアルの期間が満了したこと	トライアル期間満了日から30日経過後に、システムで自動的に組織を削除します。組織が削除されてから180日経過後にユーザーデータの削除作業を開始し、開始から10日以内に削除を完了します。（※）
	Nulab Passの利用料金の支払いを遅滞するなどしてヌーラボ利用規約第9条第1項の定めにより利用停止になったこと	契約期間満了日から90日経過後に、システムで自動的に組織を削除します。組織が削除されてから180日経過後にユーザーデータの削除作業を開始し、開始から10日以内に削除を完了します。（※）
監査ログ	組織の削除が実施されること	組織の削除を実施して組織が削除されてから180日経過後に監査ログの削除作業を開始し、開始から10日以内に削除を完了します。（※）
	Nulab Passについて契約期間が満了したこと	契約期間満了日から30日経過後に監査ログの削除を開始し、開始から10日以内に削除を完了します。（※）
	Nulab Passについて正式な申込みなくトライアルの期間が満了したこと	トライアル期間満了日から30日経過後に監査ログの削除を開始し、開始から10日以内に削除を完了します。（※）
	Nulab Passの利用料金の支払いを遅滞するなどしてヌーラボ利用規約第9条第1項の定めにより利用停止になったこと	契約期間満了日から30日経過後に監査ログの削除を開始し、開始から10日以内に削除を完了します。（※）

	監査ログの保存期間である13ヶ月を経過したこと	監査ログが保存されてから400日経過後に監査ログの削除を開始し、開始から10日以内に削除を完了します。（※）

※ ただし、当社が提供するサービスで取得しているバックアップデータには、上掲の削除タイミングによりユーザーデータが削除された後も、ユーザーデータが一定期間残ります。
例えば、1日1回取得しているバックアップの保持回数が30回の場合は、削除が完了してから30日はデータが残り、31日目に削除されます。
※ Typetalk については、上掲の「削除する条件と削除タイミング」の定めによらず、サービス提供終了後の2025年12月31日をもってバックアップも含めてすべて削除します。

削除対象となるユーザーデータ

次のデータを除き、利用者が各サービスに登録した全てのユーザーデータが削除されます。

- 当社が提供するサービスの契約/請求/入金に関するデータ
- 各サービスの契約管理者の氏名および連絡先
- Backlog（クラシックプラン）のスペースオーナーの氏名および連絡先
- BacklogのスペースID
- Nulab Passの[ヌーラボ組織ID]
- Cacooにアップロードした挿入画像
- 削除時点でアカウントに設定しているアイコン画像

ただし、ヌーラボアカウント、管理対象アカウント、またはBacklog(クラシックプラン)のアカウントの削除を実施した場合には、該当アカウントで作成されたBacklog/Typetalk/Cacoo(2019年11月26日以前のフリープランおよびプラスプランを除く。)のユーザーデータは削除されません。
これらのユーザーデータが削除されるためには、上記表に記載の”ヌーラボアカウント”または”管理対象アカウント”を除くいずれかのパターンに当てはまる必要があります。

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 Amazon Web Services、及び、Datadog 上に出力し保存します。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。
ログの保存期間は最大545日とします。その保存期間の経過後にログの削除作業を開始し、開始から10日以内に削除を完了します。

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。
ラベル付け機構に関する機能全般については、各サービスの手順書（11. 手順書の提供）を参照してください。

当社が提供するサービス共通

チーム機能 (Backlogクラシックプラン除く)

ヌーラボアカウントを利用者自ら追加したチームにグルーピングすることが可能です。

- チームの一覧と新規作成 (マニュアルページ)

Backlog

プロジェクト機能

アカウントを利用者自ら追加したプロジェクトにグルーピング (プロジェクト参加) することが可能です。

- プロジェクトの追加 (マニュアルページ)
- ユーザーの追加 (マニュアルページ)
- プロジェクトの設定 (マニュアルページ)

チーム機能 (Backlogクラシックプランのみ)

アカウントを利用者自ら追加したチームにグルーピングすることが可能です。

- チームの設定 (マニュアルページ)

Cacoo

フォルダ機能

作成した図を利用者自らが追加したフォルダーにグルーピングすることが可能です。

- フォルダーでの図、ステンシル、テンプレートの共有 (マニュアルページ)

Typetalk

トピック機能

利用者自ら特定のテーマについてチャットするためのトピックを利用することが可能です。

- トピックの作成 (マニュアルページ)
- トピックの編集 (マニュアルページ)
- トピックのアーカイブと削除 (マニュアルページ)

6. 利用者登録及び削除

全サービス共通 (Backlogクラシックプラン除く)

利用者登録

お客様は、サインアップ (※1) または、組織への招待を受けて組織に参加する際に、ヌーラボアカウントを作成できます。サインアップ時に作成されたヌーラボアカウントは、組織の管理者となり、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。

- ヌーラボアカウントの作成 (マニュアルページ)
- Backlog無料トライアル申し込み (プラン選択ページ)
- Cacoo無料トライアル申し込み (プラン選択ページ)
- Nulab Pass無料トライアル申込み (申込みページ)

※1
サインアップとは、当社が提供するサービスを無料トライアル等で利用開始すること、またはヌーラボアカウントの作成画面よりアカウントを作成することを指します。

利用者削除

利用者は、いつでも自由にヌーラボアカウントを削除することができます。
ヌーラボ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。

- ヌーラボアカウントの削除 (マニュアルページ)

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。

- ユーザーの招待 (マニュアルページ)

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、組織で利用しているサービスを利用できなくなります。

Backlog (クラシックプラン)

Backlog (クラシックプラン) では、ヌーラボアカウントでの利用以外に、Backlog内でのみ利用可能なユーザーを作成して、そのユーザーで利用することができます。
招待権限を持つ利用者は、契約されているプランの範囲内において、ユーザーの登録・削除を行うことが可能です。

- ユーザーの追加、編集、削除 (マニュアルページ)

Nulab Pass

Nulab Passは、IdP (Identity Provider)を利用したシングルサインオン(SSO)可能な管理対象アカウントを作成して、利用することができます。
管理者は、管理対象アカウントの登録・削除を行うことが可能です。
また、契約プランにより監査ログの記録・保存を行うことが可能です。

- 管理対象アカウントの作成・編集・削除 (マニュアルページ)
- SAML認証 (SSO) の設定 (マニュアルページ)
- 組織のメンバーのアカウント管理を変更する (マニュアルページ)
- 監査ログの記録・保存 (マニュアルページ)
- ユーザープロビジョニング (マニュアルページ)

7. アクセス権の管理

全サービス共通 (Backlogクラシックプラン除く)

利用者自ら、組織内のヌーラボアカウント及びチームのアクセス権を設定することができます。
設定できる権限は、"管理者"、"一般ユーザー"、"ゲスト"の3つです。
また、"一般ユーザー"には、"メンバー招待権限"を追加で付与することができます。

- メンバーの権限 (マニュアルページ)
- 組織へのメンバーの招待 (マニュアルページ)
- 一般ユーザーへのメンバー招待権限の設定 (マニュアルページ)

Backlog

利用者自ら、プロジェクトやプロジェクト内の情報に対するアクセス権を設定することができます。

- ユーザーの権限 (マニュアルページ)
- ユーザーの追加、編集、削除 (マニュアルページ)
- プロジェクト管理者の設定 (マニュアルページ)
- プロジェクト参加ユーザーの編集 (マニュアルページ)
- チームの追加、変更、削除 (マニュアルページ)

Backlog (クラシックプラン)

Backlog (クラシックプラン) は、アカウント及びチーム管理機能を提供します。

- ユーザーの権限 (マニュアルページ)
- ユーザーの追加、編集、削除 (マニュアルページ)
- チームの追加、編集、削除 (マニュアルページ)

Cacoo

利用者自ら、組織の中にフォルダーに対するアクセス権を設定することができます。
設定できる権限は、"閲覧のみ"、"編集者"、"オーナー"の3つです。
また、組織の管理者は、組織内のメンバーの中から、Cacooを利用できるメンバーを選択することができます。

- フォルダーアクセスの管理 (マニュアルページ)
- 有効なメンバーの管理 (マニュアルページ)

Typetalk

利用者により設定された組織の権限に応じて、Typetalk内のトピックに対する権限が設定されます。
また、組織の管理者は、組織内のメンバーの中から、Typetalkを利用できるメンバーおよびトピックに参加するメンバーを選択することができます。

- メンバーの権限 (マニュアルページ)
- トピック参加メンバーの管理 (マニュアルページ)
- 組織メンバーの管理 (マニュアルページ)

Nulab Pass

利用者自ら、記録・保存された監査ログに対するアクセス権を設定することができます。
- 監査ログの権限 (マニュアルページ)

8. パスワードの配布方法

ヌーラボアカウント

初期パスワード配布方法

ヌーラボアカウントは、利用者がアカウントを登録する際に自身のパスワードを設定できます。

パスワード変更方法

- パスワードの管理 (マニュアルページ)

Backlog (クラシックプラン)

Backlog (クラシックプラン) は、スペースの管理者がユーザーを作成するときに初期パスワードが発行されます。

初期パスワード配布方法

管理者が、新規アカウントを追加したと同時に、初期パスワードが生成され、新規アカウントのメールアドレスに送付されます。

- ユーザーの追加、編集、削除 (マニュアルページ)

パスワード変更方法

- パスワードの変更 (マニュアルページ)

Nulab Pass

Nulab Passの管理対象アカウントにログインするためのログインID・パスワードは、Nulab Passと連携するお客様のIdP (Identity Provider)のID・パスワードを利用します。
Nulab Pass内にはパスワード情報は保存されません。

- SAML認証 (SSO) を使ってログインする (マニュアルページ)

9. 暗号化の状況

利用者情報

- データベースに保管される、利用者の各種情報 (氏名、メールアドレス等) など個別のデータは暗号化されませんが、適切なアクセス権のもとで保管されます。
- パスワードは、不可逆暗号化 (ハッシュ化) された状態で保管されます。

サービスとの通信

- 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。

データベースの暗号化

- 一部のサービスでは、データベースファイル自体を暗号化しています。
  - 対象サービス：Cacoo、Typetalk

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。また、大きな影響がある場合は、各サービスのダッシュボード、ニュースレターでもお知らせします。

- サービスアップデート情報 (日本語)
- サービスメンテナンス情報 (日本語 / 英語)
- Backlogアナウンス情報 (日本語 / 英語)
- Backlogリリース情報 (日本語 / 英語)
- Cacooリリース情報 (日本語 / 英語)
- Typetalkリリース情報 (日本語 / 英語)
- Backlog公式X(旧Twitter) (日本語 / 英語)
- Cacoo公式X(旧Twitter) (日本語 / 英語)
- Typetalk公式X(旧Twitter) (日本語 / 英語)

11. 手順書の提供

利用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することが可能です。

- Nulab Appsユーザーガイド (日本語 / 英語)
- Backlogチュートリアル (日本語 / 英語)
- Cacooサポート (日本語 / 英語)
- Typetalkサポート (日本語 / 英語)
- Nulab Passサポート (日本語 / 英語)

12. バックアップの状況

当社が提供するサービス共通

- バックアップは全て、AWSが提供するスナップショット機能を利用します。
- バックアップデータは、AWS内の高可用性・高耐久性ストレージにて保管します
- バックアップデータは、サービス全体の復旧を目的としており、個々のお客様データを個別に復旧することはできません。
- バックアップデータのリージョンは、「2. データ保管場所」で指定されたリージョンと同一になります。

Nulab Apps / Nulab Pass

- 当社が行うバックアップの範囲、頻度、保持期間は下記です。
  - データベース (ユーザー、グループなど) : 1日1回取得し、14回分保持します。

Backlog

- 当社が行うバックアップの範囲、頻度、保持期間は下記です。
  - データベース (課題、wikiなど) ：1日1回取得し、30回分保持します。
  - 共有ファイル、Git、Subversion : 1日2回取得し、60回分保持します。
- 上記内容は、データのバックアップ (障害への対策) にも記載しております。

Cacoo

- 当社が行うバックアップの範囲、頻度、保持期間は下記です。
  - データベース (図、ユーザー定義テンプレートなど) :1日1回取得し、14回分保持します。
  - 図で利用した画像ファイル：高可用性・高耐久性ストレージに保存しており、消失リスクはほぼないと考えられるため、バックアップ対象外とします。
- 上記内容は、セキュリティとプライバシー、障害対応ポリシー にも記載しております。

Typetalk

- 当社が行うバックアップの範囲、頻度、保持期間は下記です。
  - データベース (トピック、メッセージなど) : 1日1回取得し、14回分保持します。
  - 添付ファイル : 高可用性・高耐久性ストレージに保存しており、消失リスクはほぼないと考えられるため、バックアップ対象外とします。
- 上記内容は、データのバックアップ (障害への対策) にも記載しております。
- サービス終了にともない、2025年12月31日をもってバックアップも削除します。

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。
- ログの時間は、AWSが提供するNTPサービスと同期しています。

14. 脆弱性管理に関する情報

- 当社が提供するサービスは、年に1回の頻度で第三者による定期的な脆弱性診断を実施しています。指摘された事項については内容を精査し、必要な対応を行なっています。
- 当社が提供するサービスの開発チームは、利用するOS、ミドルウェア等に関する脆弱性情報を、定期的に収集しています。
- セキュリティ専門家が潜在的な脆弱性を当社に報告しやすくするために、security.txt を公開しています。
- セキュリティ専門家が潜在的な脆弱性を当社に報告するための窓口として、脆弱性開示プログラムを運用しています。
- 当社が提供するサービスで利用しているコンポーネントに対する脆弱性パッチが公開された場合は、予め確立したプロセスに従って速やかに適用します。
- 当社は一般公開されているすべてのソフトウェアの脆弱性について当社での利用有無を含む具体的な情報提供は行いません。
  - 例 : OS、ミドルウェア、ライブラリ、ファームウェア
- 当社が脆弱性の影響を確認した場合は、ご登録いただいている連絡先へ対応の有無も含めて通知します。

15. 開発におけるセキュリティ情報

- 開発担当者による相互コードレビュー実施やソースコードの静的解析などの手段により、基本的な脆弱性への対応ができているかなどの確認を行っています。
- サーバーにインストールされていたり、サービスに組み込まれているライブラリ群について、バージョンが古い、脆弱性が発見されたなどのチェックを定期的に行っています。ソフトウェ

アライフサイクルの終了やサービスが脆弱性の影響を受ける場合、ライブラリ群のアップデートなど適切な対応を行います。

16. 人的セキュリティに関する取り組み

- 従業員のセキュリティ意識を高める取り組みとして、週に1回の頻度でセキュリティテストを配信しています。
- 従業員の役割に応じて、集合研修や e-learning など年間複数のセキュリティに関する研修を実施しています。
- インシデント発生時の対応手順を定め、従業員が迅速に対応できるように訓練を行っています。

17. 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、72時間以内を目安として、当社の選択に基づき、電子メールその他の1つまたは複数の手段によりユーザーの管理者に連絡します。
- 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お問い合わせページより受け付けています。
    - 当社サイト問い合わせページ : https://nulab.com/ja/contact/

18. ユーザーデータの保護および第三者提供について

- 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. 認証制度

- 当社は、情報マネジメントシステム認定センター (ISMS-AC) が運営する、ISMS適合性評価制度における、ISMS認証を取得しています。(※1)
- 当社は、情報マネジメントシステム認定センター (ISMS-AC) が運営する、ISMS適合性評価制度における、ISMSクラウド・セキュリティ認証を取得しています。(※2)

【ISMSクラウドセキュリティ認証登録範囲】

Backlog, Cacoo, Typetalk, Nulab Appsサービスの提供に係るクラウドサービスプロバイダとしてシステム開発・運用・保守及びアマゾンウェブサービスのクラウドサービスカスタマとしての利用に係るISMSクラウドセキュリティマネジメントシステム

※1 https://isms.jp/lst/ind/CR_IS_x0020_656556.html
※2 https://isms.jp/isms-cls/lst/ind/CR_CLOUD_x0020_681700.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	機能	運営会社
Amazon Web Service	インフラ構築、運用	Amazon Web Services, Inc.
Google Cloud	インフラ構築、運用	Google LLC
PagerDuty	インフラ運用	PagerDuty, Inc.
mackerel	インフラ運用	株式会社はてな
Datadog	インフラ運用	Datadog, Inc.
Intercom	カスタマーサポート	Intercom, Inc.
Google Workspace	カスタマーサポート	Google LLC
Zendesk	カスタマーサポート	Zendesk, Inc.
KARAKURI	カスタマーサポート	カラクリ株式会社

Stripe	決済	Stripe, Inc.
PayPal	決済	PayPal Holdings Inc.
Twilio	SMS送信	Twilio Inc.
Mixpanel	データ分析	Mixpanel, Inc.
Mailchimp	メール送信	Intuit Inc.
SendGrid	メール送信	SendGrid, Inc.
Marketo	メール送信	Adobe Inc.
Salesforce	顧客管理、メール送信	Salesforce, Inc.
Slack	運用、カスタマーサポート	Slack Technologies, LLC
Snowflake	データ分析	Snowflake Inc.

改定履歴

版数	改定日	改定内容
1.0	2019/02/25	初版発行
1.1	2019/06/14	11.バックアップ状況のBacklog部分変更 19.免責の対象サービスの変更
1.2	2019/10/09	3. データの削除の変更
1.3	2019/12/06	19.免責の対象サービスの変更
1.4	2021/07/19	1. 利用者との責任分界点の変更 2. データ保管場所の変更 3. データの削除の変更 4. ラベル付け機構 5. 利用者登録および削除 6. アクセス権の管理 7. パスワードの配布方法 10. 手順書の提供の変更 11.バックアップの状況の変更 15. インシデント発生時の対応の変更 19. 免責の対象サービスの変更
1.5	2021/12/24	Nulab Passの監査ログ機能追加に伴う変更を追加 2. データ保管場所の変更 3. データの削除 5. 利用者登録及び削除 6. アクセス権の管理
1.6	2022/09/26	2. データ保管場所の記載変更 3. データの削除の対象サービス等の記載修正 11.バックアップ状況のCacoo部分変更 19.見出しを適切なものに修正し、対象サービスを棚卸
1.7	2023/05/18	5. 利用者登録及び削除　マニュアルを変更 8. 暗号化の状況　利用者情報を変更 8. 暗号化の状況　データベースの暗号化を追加 11. バックアップの状況　当社が提供するサービス共通に追記
1.8	2023/12/1	13. 脆弱性管理に関する情報の記載変更
2.0	2024/9/18	規約の改訂に伴い内容を刷新
2.1	2024/12/3	20. Salesforceの機能を修正
2.2	2025/3/1	3. データ保管場所　更新

		4. データの削除　更新 10. 変更管理　リンクを更新 11. 手順書の提供　リンクを更新 20. 外部クラウドサービスの利用　追加
2.3	2025/6/26	3. データの処理と保管　更新 14. 脆弱性管理に関する情報　追加 16. 人的セキュリティに関する取り組み　追加 21. 外部クラウドサービスの利用　追加 その他、内容の変更を伴わない軽微な修正