nulab



セキュリティ担当者向け

導入前
確認項目
サンプル
付き

社内稟議に役立つ

Backlog
導入推進ガイド

backlog by nulab　nulabpass

目次

プロジェクト・タスク管理ツール「Backlog」の概要 3

ヌーラボ製品のセキュリティ＆ガバナンスを強化する「Nulab Pass」の概要 5

導入前に確認しておきたいセキュリティ要件 7

①安全性と利便性を両立する「アカウント・権限管理」 7

②セキュリティ対策 9

③ データを安全に守り抜く「データ保護・インフラ」 11

ヌーラボが提供しているセキュリティチェック 12

導入前のセキュリティ確認シート（サンプル） 13

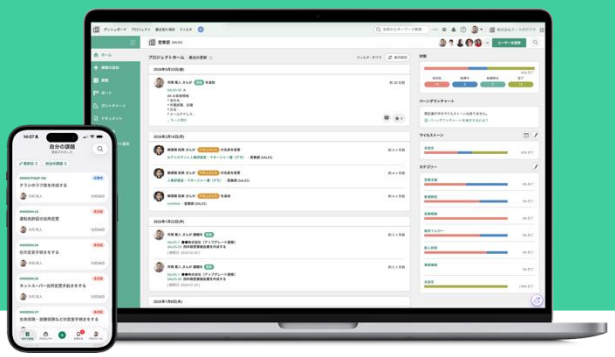
参考リンク 14



© 2026 Nulab Inc. All rights reserved.

プロジェクト・タスク管理ツール

Backlog



チームのタスクを可視化し、コミュニケーションを促進

Backlogでは、タスクを「課題」として登録し、同一プロジェクトのメンバー間で共有します。
課題やコメント、ドキュメントの情報は保持され、更新時には変更履歴が記録されます。

① 課題（タスク）の登録

課題名・内容・担当者・期限・添付ファイルなどの情報を登録します。
プロジェクトに参加しているメンバーが登録・閲覧可能です。
（権限設定で登録のみ／閲覧のみなどの制御も可能です）



② 課題の更新・コメントによる情報共有

作業の進捗に応じて、課題ごとにコメントのやり取りや更新を行います。プロジェクトに参加しているメンバーであれば、権限設定されていない限りコメント・更新が可能です。



③ 課題完了後もデータ保持

課題完了後も、課題データは削除されず保持されます。
更新履歴やコメントも保存されるため、過去の対応内容や判断経緯を追跡できます。



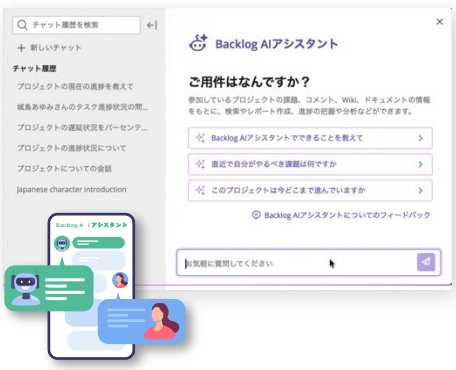
ドキュメント

社内マニュアルや議事録などをまとめ、リアルタイムで同時編集できる機能です。自動保存、変更履歴の確認が可能です。



Backlog AIアシスタント

Backlogに入力された情報をもとに、課題登録や要約、レポート作成をサポートするAI機能です。
・入力されたデータは、AIモデルの学習に利用されません。
・データの参照範囲は、ユーザー自身が参加しているプロジェクトに限られます。



© 2026 Nulab Inc. All rights reserved.

プロジェクト・タスク管理ツール Backlog



機能一覧

チームのプロジェクト・タスク管理に必要な機能を オールインワンで提供

親子課題・孫課題

大きな課題にある複数の課題も管理可能

課題ごとのコメント

タスクごとのコミュニケーションが可能

ガントチャート

全体の進行状況を一目で確認可能

ボード

ステータスごとのタスク量が、カード形式で一目瞭然

Backlog AIアシスタント

タスクの起票や要約、レポート作成をAIが支援

ファイル共有

資料の共有もBacklog上で完結

ドキュメント

情報を一括蓄積し、チームで共同編集・更新

バーンダウンチャート

PJ進捗をマイルストーンごとにグラフで表示

Git / Subversion

レビュー等が課題に自動でコメントされる

お知らせ機能

担当者割り当てや課題更新時に通知

モバイルアプリ

モバイルからもタスク内容の確認が可能

IPアドレス制限

外部ネットワークからの侵入を防止

2段階認証

高いセキュリティ性

活用ポイント

情報の一元管理

散在する情報を集約し、
必要な情報にすぐアクセス

- プロジェクト全体やタスクの状況を一元管理
- 検索機能による素早い情報アクセス

活用例
プロジェクト関連のドキュメント、会議議事録、成果物をすべてBacklog内で管理し、情報の分散を防止

業務の可視化

誰が何をしているか、
進捗状況をリアルタイムに把握

- 担当者と期限の明確化
- ステータスによる進捗の透明化

活用例
ガントチャートやボードで全体の進捗を把握し、遅延リスクを早期に特定してプロジェクト管理を効率化

AIによるタスク起票や要約

「Backlog AIアシスタント」がタスク起票や要約、レポート作成などを支援
（プレミアム・プラチナプランが対象）

- 情報把握の時間を短縮し、業務を効率化

活用例
タスク起票、会議資料の作成・要約、月報などのレポート作成、膨大なコメントの要約、メンバーのタスク量の整理

アクセスログの取得

ユーザーが、いつ、Backlog内のURLにアクセスしたかを記録可能
（プラチナプランが対象）

- 月に1回、前月のアクセスログのダウンロードリンクをメールでお届け

活用例
不審なアクセスの有無をチェック、インシデント発生時のアクセス履歴追跡

柔軟なカスタマイズ

チームや用途に合わせたカスタム設定や機能のON/OFF調整が可能

- 必要に応じて入力項目をカスタマイズ
- 通知や表示させる機能を設定できる

活用例
開発チームではGit/Subversion機能をON、営業チームでは「確度」の入力項目を追加するなど、部門別に最適化

外部サービス連携

SlackやTeamsなど外部ツールとシームレスに連携

- チャットツールへの通知連携
- API連携による自動化

活用例
SlackやTeams上で課題の更新通知を受け取り、Backlogのタスクを直接参照するなど、ワークフローを効率化

© 2026 Nulab Inc. All rights reserved.

ヌーラボ製品のセキュリティ＆ガバナンスを強化する

Nulab Pass



ヌーラボ製品のセキュリティとガバナンスを強化
脅威を未然に防ぐ強力なセキュリティ基盤を構築

主な用途

- ユーザー管理
- セキュリティ強化
- IT管理者業務効率化
- アクセス制御
- 監査対応

特長

SAML認証
企業の認証基盤と連携したシングルサインオン

- Microsoft/OKTA/HENNGE Oneほか主要IDプロバイダと連携
- ワンクリックでBacklog/Cacooにアクセス
- 社内認証ポリシーの一元適用

監査ログ
ユーザーの操作履歴を記録し、監査やセキュリティ対策に活用

- ユーザーの活動をCSVでダウンロード
- 不審なアクティビティの追跡
- 監査やセキュリティインシデント対応支援

アカウント管理
ヌーラボサービスのアカウントを一元管理

- ユーザープロビジョニングでユーザーの追加・変更・削除を一括管理
- ユーザー退職時の一括アクセス停止

活用ポイント

セキュリティ強化
SAML認証による不正アクセス防止

- 社内IDシステムと連携した強固な認証
- アドレス制限による不正アクセス防止

活用例
ご利用中のIDプロバイダーと連携することで、退職者のアカウント無効化を自動化し、情報漏洩リスクを大幅に低減

管理工数の削減
複数サービスのアカウント管理を一元化

- 一括アカウント作成・変更・削除
- パスワードリセット対応の負荷を軽減

活用例
アカウント管理工数が大幅に削減され、担当部門は本来の業務に集中可能に

コンプライアンス対応
監査ログで、内部監査や第三者監査に対応

- ユーザーの操作履歴を詳細に記録
- セキュリティ監査や調査の効率化

活用例
定期的な監査対応の準備時間を短縮。アクセス記録の提出要求にも迅速に対応可能に

ユーザー体験の向上
シングルサインオンによるアクセス簡略化

- 複数パスワードの管理負担軽減
- ログイン操作の簡略化と時間短縮

活用例
複数ツール間の行き来がスムーズになり、ユーザーからのパスワードリセット依頼が減少

運用コストの最適化
アカウント管理の効率化と人的コストの削減

- IT部門の運用工数削減
- セキュリティインシデント対応コスト低減

活用例
アカウント管理に関わる年間コストを削減し、IT担当者のリソースを戦略的業務へ再配分

ガバナンスの強化
組織全体でアクセス管理ポリシーを統一

- 統一されたセキュリティポリシーの適用
- 権限管理の透明性と一貫性の確保

活用例
複数部門にまたがるプロジェクトでも、統一されたアクセスルールを適用し、情報共有と適切なアクセス制限を両立

© 2026 Nulab Inc. All rights reserved.

導入前に確認しておきたいセキュリティ要件

①安全性と利便性を両立する「アカウント・権限管理」

ユーザー権限の管理

Backlogには3つのユーザー権限があります。また、ユーザーごとに追加の権限を付与したり、制限を設定できます。情報の閲覧や操作を統制することで、不要な操作や情報へのアクセスを抑止できます。

ユーザーの種類

管理者	Backlogの契約関連以外のすべての設定を閲覧、編集できます。 チームの追加、削除、編集ができます。ユーザーの追加、編集、組織からの除外ができます。
一般ユーザー	課題、ドキュメント、ファイル、リポジトリなどの機能を利用できます。 組織のメンバーと自分が所属しているチームを参照できます。新しいチームを作成できます。
ゲスト	課題、ドキュメント、ファイル、リポジトリなどの機能を一般ユーザーと同じように利用できます。 自分が所属しているチームのみを参照できます。プロジェクト管理者になることはできません。

追加権限

管理者や一般ユーザーに対して、追加で組織に関する権限を与えられます。

契約管理者	組織のスペースのプランや契約に関する事項を閲覧、編集できる権限です。 他の契約管理者から付与できます。
プロジェクト管理者	プロジェクト管理者の権限があるプロジェクトで、管理者と同等のプロジェクトの編集ができる権限です。他のプロジェクト管理者や管理者から付与できます。（権限が付与されていないプロジェクトの管理は行えません）
メンバー招待	組織に新しい一般ユーザー・ゲストを追加できる権限です。管理者から一般ユーザーに対して付与できます。設定方法は、メンバー招待権限を参照してください。 プロジェクト管理者に対して付与すると、Backlogの画面上から、組織に参加していないメンバーもプロジェクトに追加できます。 メンバーを招待する際は、権限の内容をよく確認してください。
チーム管理者	新規にチームを作成すると、まずは作成者がチーム管理者になります。他のメンバーをチーム管理者にしたい場合、チーム管理者または管理者から付与できます。（権限が付与されていないチームの管理は行えません）

制限

管理者は、ユーザーの編集画面で、一般ユーザーとゲストに対して機能制限（制限なし・課題の登録のみ・課題の閲覧のみ）を設定できます。

© 2026 Nulab Inc. All rights reserved.

導入前に確認しておきたいセキュリティ要件

①安全性と利便性を両立する「アカウント・権限管理」

▶ SSO、ユーザープロビジョニングによるアカウント管理

Backlogのアカウントを適切に管理するために、Nulab Passを併用したSSOやユーザープロビジョニングの活用が有効です。

SAML認証によるシングルサインオン（SSO）機能【Nulab Pass併用】

SAMLにより、ユーザーのログイン時の手間を省き、お客様のセキュリティ基準を満たしたIDプロバイダーを介してアカウントを認証できます。

お使いのIDプロバイダーにより認証が行われるため、端末単位でのアクセス制限や、資格情報の流出、不正アクセスなどのリスクマネジメントが可能となります。



SCIMによるユーザープロビジョニング機能【Nulab Pass併用】



お客様がご利用のIDプロバイダーで、Nulab Passの管理対象アカウントを一元管理できます。IDプロバイダーで行ったユーザー追加・変更・削除を検出し、ユーザー名やユーザー権限を管理対象アカウントに反映します。

入社や退社などに伴う社員のアカウント管理をより効率的に行なうことができます。

※ ユーザープロビジョニング機能は、SCIM2.0に対応しているIDプロバイダーでご利用いただけます。動作確認済みのIDプロバイダーについては、対応しているIDプロバイダー を参照してください。

© 2026 Nulab Inc. All rights reserved.

導入前に確認しておきたいセキュリティ要件

①安全性と利便性を両立する「アカウント・権限管理」

▶ 管理対象アカウントによる統合的なアカウント管理【Nulab Pass併用】

「管理対象アカウント」を利用すると、ユーザーの追加・削除などのアカウント管理を自動化できるため、大規模な組織でも効率的に運用できます。また、認証を組織の管理者によるIDプロバイダー（IdP）に委任することで、お客様の認証ポリシーに沿ったログイン管理が可能となります。

	管理対象アカウント	管理対象ではないアカウント
アカウント管理	組織の管理者が作成・変更・削除可能（IdP連動）※1	ユーザー自身のみが作成・変更・削除可能
ログイン時の認証	SAML認証による シングルサインオン	パスワード認証または パスワードレス認証 （SAML認証は非対応）
ユーザープロビジョニング	SCIM APIによってIdPから ユーザー情報を同期できる※1	ユーザー情報を同期できない
アカウントの停止と アクティブの切り替え	切り替えできる（IdP連動）※2	切り替えできない
組織への参加	複数の招待された組織に参加できる （IdPと連携された組織からは抜けられない）	複数の招待された組織に参加できる （全ての組織から抜けられる）
2段階認証の設定	IdPの2段階認証※3	ヌーラボアカウントの2段階認証
アカウント種別の切り替え	管理元の組織の管理者によって、 管理対象ではないアカウントに 変更できる	アカウントのメールアドレスのドメインを 認証している組織の管理者によって、 管理対象アカウントに変更できる

※1 同期されるのは、プロビジョニングされた管理対象アカウントのみです。

※2 プロビジョニングされた管理対象アカウントのみ、停止とアクティブの切り替えが可能です。
また、切り替えはIdPの設定画面かSCIM APIの使用にて変更できます。組織設定からは変更できません。

※3 管理対象アカウントはヌーラボの2段階認証は利用できません。
また、Backlogの2段階認証を必須にする設定の影響を受けません。



© 2026 Nulab Inc. All rights reserved.

導入前に確認しておきたいセキュリティ要件

②不正アクセスを未然に防ぐ「アクセス制限」

▶ Backlogのセキュリティ対策

「管理対象アカウント」は管理対象ではないヌーラボアカウントよりも管理者の操作権限が強く、不正利用や不正アクセスなどを対策しながら大規模利用を可能にします。

	フリー	スターター	スタンダード	プレミアム	プラチナ
2段階認証	✔	✔	✔	✔	✔
2段階認証の必須化				✔	✔
アクセス制限（IP制限）			✔（50個まで）	✔（100個まで）	✔（無制限）
アクセスログの提供					✔
セキュリティシートの提供				✔（有料オプション）	✔（年一回まで無償）
SAML認証（オプション）	nulabpass の併用でSAML認証でのシングルサインオンや メンバーの操作ログも取得可能				
監査ログ（オプション）					
ユーザープロビジョニング（オプション）					

※Backlogのプランについて、最新情報はサービスサイトをご確認ください。

▶ Backlogのアクセスログ

ユーザーが、いつ、Backlog内のURLにアクセスしたかを記録したログです。（プラチナプランが対象）
操作履歴は記録されません。URLやHTTPリクエストメソッド、ステータスコードなどの情報からある程度の操作は特定できますが、操作されたファイル名など具体的な情報は把握できません。
出力される情報の詳細は、こちらのヘルプページをご覧ください。

・保存期間
スペースを契約している期間はログが保管されます。スペース解約後、一定期間が経過すると削除されます。

・アクセスログのダウンロード
毎月10日頃、ダウンロードリンクがメールで届きます。過去に提供したアクセスログも、Backlogを解約するまでダウンロードできます。ダウンロードは、正式登録時のスペースオーナーまたは契約管理者のみ行えます。

こちらから、アクセスログのサンプルをダウンロードいただけます
https://backlog.com/download/demo/backlog_access_log.201509.zip

© 2026 Nulab Inc. All rights reserved.

導入前に確認しておきたいセキュリティ要件

②不正アクセスを未然に防ぐ「アクセス制限」

▶ 監査ログ【Nulab Pass併用】

監査ログとアクセスログの違い

監査ログは、「いつ」「だれが」「何をしたか」が記録された、監査証跡となるログとなります。組織の管理やプロジェクトの運用などに影響を及ぼすような構成の変更を記録するものです。そのため、「課題を閲覧した」などのアクセスしただけのログは記録されません。

	監査ログ	Backlogのアクセスログ※
目的	BacklogやNulabPassに対する参照以外の操作を記録するログ。データの変更・持ちだしなどのログを確認可能	ユーザーが、いつ、Backlog内のURLにアクセスしたかを記録するログ
記録される内容	操作内容が詳細に記録される 課題などを閲覧しただけでは記録されない （下記「監査ログに出力する情報」をご参照ください）	操作内容は詳細に記録されない 課題などを閲覧しただけでも記録される
ダウンロードできるタイミング	いつでもダウンロード可能	翌月にならないと閲覧できない

※Backlogのアクセスログはプラチナプランをご利用のスペースで、毎月10日に前月のアクセスログを提供します

監査ログで記録できる操作

監査ログでは次のような操作を記録します。

プロジェクト管理・タスク管理ツール backlog by nulab

課題	追加、更新、削除
コメント	追加、更新、削除
ファイル	追加、ダウンロード、削除
Gitリポジトリ	追加、クローン、プッシュ
ドキュメント	追加、更新、削除

ヌーラボ製品のセキュリティ・ガバナンス強化 nulabpass

メンバー	招待・削除・権限変更・メンバー一覧のダウンロード
管理対象アカウント	作成、更新、削除
チーム	作成、削除
チームメンバー	追加、削除
支払情報の変更	
契約者情報の変更	



※ 更新した内容の詳細や投稿したメッセージなどは記録しません。

監査ログに出力する情報

監査ログのCSVファイルには以下の情報を出力します。

項目	説明	項目	説明
product	プロダクト名 （Backlog, Cacoo, Apps）	operation_user_id	操作したメンバーを識別するシステム内部のID
date	操作を行った日時　UTC（日本時間 -9時間）	operation_user_name	操作したメンバーのユーザー名
category	操作のカテゴリ（Issue, Document, Project など）	operation_user_email	操作したメンバーのメールアドレス
event	操作のイベント （Add an issue, Update a documentなど）	ip_address	操作したメンバーのIPアドレス
action	イベントがどの課題に対するものなのか、などが判別できる情報が記録されます	user_agent	操作したメンバーのブラウザー情報

© 2026 Nulab Inc. All rights reserved.

導入前に確認しておきたいセキュリティ要件

③ データを安全に守り抜く「データ保護・インフラ」

Backlogのセキュリティ

信頼性の高いデータセンターを使用	サービスを提供するデータセンターとしてAmazon Web Services（AWS）を利用しています。
細心の注意を払ったデータ管理（ISO/IEC 27001、ISO/IEC 27017:2015、ISO/IEC 27018に準拠した運用体制）	AWS上の環境へのアクセスは、AWS SSOによる厳格なシングルサインオン認証とセッション管理を行い、認証も許可されたデバイスのみに制限しています。アクセス可能な運用担当者や権限は必要最低限に限定。サーバ上のデータへは、お客様から調査等の依頼があった場合のみアクセスし、個人情報はプライバシーポリシーに従い扱っております。
不正なアクセスはしっかりブロック	Backlogではお客様毎に独自のURLを提供します。URLを知らない限り、第三者はアクセスできません。スペースごとの、IPアドレスによるアクセス制限も可能です。（スタンダードプラン以上）
通信はすべてTLS暗号化	Backlogとの通信は、PC版、モバイル版、バージョン管理システム、共有ファイルと機能を問わず全てTLSにより暗号化されています。第三者が盗聴をしても、その内容を知ることはできません。
サーバの監視・障害対応	サーバの監視は24時間365日体制で行っており、異常検知時には運用スタッフに即座に通知され、対応します。平時より障害にあわせたマニュアルを整備し、迅速に復旧できる体制を整えています。
障害やメンテナンス情報は最新情報をお知らせ	メンテナンスによる計画停止の原則5営業日前に、BacklogサイトやXアカウント、ダッシュボードで告知します。極力、早朝や深夜の作業時間帯を選んでいます。障害発生時には、速報としてXで対応状況を公開し、収束後にBacklogサイトで状況報告します。→現在の稼働状況を確認する
データのバックアップと障害対策方法	以下のバックアップ対策を実施し、万一データ領域で障害が発生した場合に迅速に復旧します。 **データベース** 常時、別のデータセンターへ複製。毎日1回バックアップを取り、30回分を保管 **共有ファイルとGit、Subversion** 毎日2回バックアップを取り、60回分を保管 **バックアップデータの保管** AWS内の高可用性・高耐久性ストレージに保管

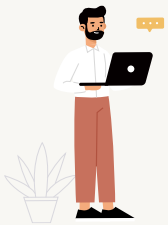


© 2026 Nulab Inc. All rights reserved.

ヌーラボが提供しているセキュリティチェック

ASSURED
クラウドリスク評価「アシュアード」

Backlogのセキュリティ情報は、セキュリティ評価プラットフォーム
「Assured（アシュアード）」からリクエストいただけます。
Backlog導入検討時のセキュリティチェック業務をスピーディーに実施されたい方は、
こちらをご利用ください。



セキュリティ評価をリクエストする

セキュリティチェックシート



経済産業省による「クラウドサービスレベルのチェックリスト」や、IPA（独立行政法人情報処理推進機構）による「安全なウェブサイトの作り方改訂第7版」に準拠したセキュリティチェックシートをダウンロードいただけます。

セキュリティチェックシートをダウンロードする

セキュリティチェックシートへの回答（有料オプション）

弊社側でセキュリティチェックシートの内容確認やお客様独自フォーマットへの記入が必要な場合は、別途有料オプションを提供しております。
詳しくはBacklogヘルプページ をご覧ください。

© 2026 Nulab Inc. All rights reserved.

導入前のセキュリティ確認シート（サンプル）

ツール導入前の、セキュリティ要件の確認書サンプルです。
導入担当者へ記入をご依頼いただき、ご活用ください。

確認日		所属部署		氏名	

件名	プロジェクト・タスク管理ツールBacklog　および ヌーラボ製品のセキュリティ＆ガバナンスを強化するNulab Pass導入に関するセキュリティ確認
利用目的	＜記入例＞ ・開発部、営業部、カスタマーサポート部、総務部における日常のタスク管理 ・部門横断プロジェクトの進行管理 ・外部委託パートナーを交えたプロジェクト・タスク管理
機能	タスク管理、コメント機能、ファイル管理、ドキュメント共有、通知機能、AIアシスタント機能、ガントチャート、カンバンボード、バーンダウンチャート、Git によるバージョン管理、モバイルアプリ提供
想定利用者	＜記入例＞ ・開発部・営業部・カスタマーサポート部・総務部 計150名程度 ・外部委託パートナー30名（特定プロジェクトのみ参加）
取り扱う情報	＜記入例＞ ・業務内容（プロジェクト内容、議事録、進捗状況 等） ・個人情報（顧客担当者名、メールアドレス等） ・社外秘情報（企画書、予算情報等の社内資料）
アクセス経路	＜記入例＞ ・社内PCおよびスマートフォン端末からブラウザ利用 ・社内ネットワークまたは会社が管理するリモートアクセス環境から接続
契約プラン	＜記入例＞ ・Backlog プレミアムプラン：税抜 307,800円／年（年間契約／ユーザー課金なし） ・Nulab Pass：税抜 288,000円／年（年間契約／100ユーザー以下）
セキュリティ対策	・Backlog：2段階認証、IP制限、アクセスログ、プロジェクト単位の権限設定 ・Nulab Pass：SAML認証、監査ログ、ユーザープロビジョニング 信頼性の高いデータセンター（AWS）の使用および通信のTLS暗号化、サーバーの監視・障害対応とその状況報告、データのバックアップなどを実施。 「ISO27001:2013」「ISO27017」「ISO27018」といった複数のセキュリティ認証を取得。
導入前のセキュリティチェック方法	・セキュリティ評価プラットフォーム「Assured（アシュアード）」によるセキュリティ評価 ・経済産業省による「クラウドサービスレベルのチェックリスト」や、IPA（独立行政法人情報処理推進機構）による「安全なウェブサイトの作り方改訂第7版」に準拠したセキュリティチェックシート ・顧客独自のセキュリティチェックシートへ回答（有料オプション）

Word形式でダウンロードする

© 2026 Nulab Inc. All rights reserved.

参考リンク



セキュリティホワイトペーパー

ヌーラボのプライバシーとセキュリティにおける
取り組みを示した「セキュリティホワイトペーパー」
を公開しています。

セキュリティホワイトペーパーを見る



お問い合わせ

BacklogやNulab Passのご不明点はお気軽に
お問い合わせください

問い合わせる



個別相談会開催中

BacklogやNulab Passの個別相談会を
随時開催しています

個別相談会を申し込む

© 2026 Nulab Inc. All rights reserved.



会社概要

社名	株式会社ヌーラボ
設立	2004年3月
事業内容	チームのコラボレーションを促進するサービスの開発・提供 ● プロジェクト・タスク管理ツール『Backlog』 ● オンラインホワイトボードツール『Cacoo』 ● ヌーラボ製品のセキュリティ＆ガバナンスを強化する『Nulab Pass』 ● ワークフロー自動化ツール『Nulab Flowbase』
本社	福岡県福岡市中央区天神一丁目11番1号

nulab