セキュリティホワイトペーパー
Ver.1.1

Copyright © 2022 Ricoh Company, Ltd. All rights reserved.

株式会社リコー
2022 年 11 月

変更履歴

バージョン	日付	前バージョンからの変更
1.0(初版)	2022 年 4 月	
1.1	2022 年 11 月	3.2.8 多要素認証を追加（挿入）しました。

Copyright © 2022 Ricoh Company, Ltd. All rights reserved.

目次

Copyright © 2022 Ricoh Company, Ltd. All rights reserved.

1 はじめに

1.1 本書は、toruno をお客様に安心して使って頂くために、セキュリティ対策とその仕組みを対象として説明します。

2 toruno について

2.1 「toruno」は、オンライン会議をまるごと”とる”サービスです。

2.2 お使いのオンライン会議ソフトと toruno を一緒に立ち上げ、「記録開始」ボタンをクリックするだけで、自動で文字起こしをしながら、会議音声、PC に映った画面を記録します。面倒な連携は不要で、かんたんに会議を記録できます。

2.3 会議後は、会議の振り返りや共有、議事録作成にお使いいただいたり、ファイル化された動画や音声を文字起こしするのにお使いいただけます。

Copyright © 2022 Ricoh Company, Ltd. All rights reserved.

3　セキュリティ対策と仕組み

3.1 脆弱性対策

3.1.1　セキュリティ専門部門が最新の脆弱性情報を収集しています。脆弱性が発見された場合は、本サービスに与える影響を確認し、定められたルールに従い対応を実施しています。

3.1.2　定期的、さらに必要に応じて適宜に専門の脆弱性診断ツールを用いて、OS やミドルウェア等のパッチ未適用の検出、不適切なセキュリティ設定の検出、不要な通信サービスの検出等の検査を実施しています。 脆弱性が発見された場合は、本サービスに対する影響を確認し、定められたルールに従い対応を実施しています。

3.1.3　不正なアクティビティを阻止するための IDS の仕組みを導入しております。

3.1.4　利用者、および弊社運用担当者が外部から使用するネットワークポート以外は、ネットワーク層、トランスポート層でのファイアウォールにより接続を不許可にし、不正な攻撃から防御することで、脆弱性を利用したサービス妨害から保護しています。アプリケーション層でのファイアウォールについては未導入です。

3.2 情報漏洩対策

3.2.1　インターネット上の通信は、https 通信（TLS1.2 以上）を許可することでセキュリティ保護しています。

3.2.2　利用者、および弊社運用者が外部から使用するネットワークポート以外はファイアウォールにより接続を不許可にすることで、外部からの情報不正入手に対してセキュリティ保護しています。

Copyright © 2022 Ricoh Company, Ltd. All rights reserved.

3.2.3 データを保存している外部のデータセンターは、ISO27001/ISO9001 などのセキュリティ認証を取得されていることを確認し、充分なセキュリティ体制の運用を確認しています。

3.2.4 toruno で記録されたデータやご登録いただいた情報は、サーバー上ですべて暗号化した状態で保存することでセキュリティ保護しています。

- 暗号化方式：公開鍵暗号
- 暗号アルゴリズム：AES
- 鍵長：256

3.2.5 定期的にバックアップされるバックアップデータは、すべて暗号化しています。

3.2.6 ユーザーは、ID とパスワードで認証することで、情報にアクセスすることができます。認証されないとデータへアクセスできません。なお、ID フェデレーション機能は提供しておりません。

3.2.7 パスワード規則は現状では 8 文字以上としており、英数混合などの制限はありません。

3.2.8 ユーザーのパスワード漏洩対策として、スマートフォンアプリの認証アプリを利用した多要素認証（MFA）を提供しております。

3.2.9 toruno サービススタッフが利用する端末には OS やアプリケーションを最新にアップデートすることや、セキュリティツールを導入し、検出データベースを最新に維持すること、クリアデスク・クリアスクリーンの徹底をする等、セキュリティ対策を施しております。

3.2.10 toruno サービスを運用する上で、リソースの変更やシステムに対するアクセスログを取得し、監視するようにしております。

Copyright © 2022 Ricoh Company, Ltd. All rights reserved.

3.2.11 toruno はクラウドサービス上に構築されているため、toruno サービススタッフは、データセンターおよびサーバーに対し物理的にアクセスすることはできません。

3.2.12 ユーザーの操作ログ・アクセスログに関しては、障害解析用のためのログを取得しております。お客様提供用としての取得・保管は現在行っておりません。

3.2.13 IP 制限、SSO（シングルサインオン）機能は提供しておりません。

3.3 サービス妨害対策

3.3.1 外部から直接アクセスされる部分と、処理を実行する部分をネットワーク上分割し、耐久性の高い仕組みとなっています。

3.3.2 利用者、および弊社運用者が外部から使用するネットワークポート以外はファイアウォールにより接続を不許可にし、不正な攻撃から防御することでサービスを継続可能にしています。

3.3.3 システム構成の変更管理については、規定された手順に基づいて実施しております。

3.4 機器障害対策

3.4.1 各機能を構成するインフラストラクチャーを冗長化することで、機器障害に強い構成を実現しています。

3.4.2 データセンターの所在する地域は日本および一部アメリカとなっております。お客様のデータ（会議情報、ユーザー情報等）は日本に保管しております。アメリカには、お客様のデータは保管しておらず、システム稼働のために必要な情報を保管しております。

Copyright © 2022 Ricoh Company, Ltd. All rights reserved.

3.4.3 災害または重大な障害発生時に備えて、バックアップシステムを構築しております。構築にあたっては、日本国内全体規模の障害が発生しない限りサーバー等が単一障害点にならないような設計をしております。災害または重大な障害発生時は、事業継続および災害復旧のためにベストエフォートで対応致します。

3.5 パフォーマンス対策

3.5.1 利用者のアクセスが増大してもパフォーマンスが悪化しないよう、ロードバランサーでのアクセスに関する負荷分散や SSL オフロード機能を利用することでの処理側の負荷軽減、オートスケールに対応した音声認識エンジンの選定などを行っております。

3.6 障害対策

3.6.1 常時、システム監視を実施しています。 サービス提供環境内でのリソース監視やログ監視の他に、サービス提供環境外からの監視も実施しています。

3.6.2 障害発生時には、予め定めている障害レベルと対応手順に従い対応を実施します。

3.6.3 障害発生時には、メールや Web サイト twitter などでお知らせいたします。

- Web サイト： https://toruno.biz
- twitter: https://twitter.com/toruno_biz

Copyright © 2022 Ricoh Company, Ltd. All rights reserved.

4 リコーグループの情報セキュリティ

4.1 情報化社会の中で、常に信頼されるグローバルブランドを目指し、情報セキュリティへの取り組みに励んでいます。

4.2 離任したスタッフのアカウントは規定に基づき、適切に削除しております。

4.3 toruno 情報セキュリティに関する窓口

- 問い合わせフォーム：https://bit.ly/3pKePYg
- 対応時間： 平日 9:00 – 17:00
  ※ただし、土日祝日、夏期・年末年始・その他大型連休期間を除く
- サポート手段： メール

4.4 本サービスの開発・提供元であるリコーは全社レベルでの公的認証を取得しておりません。但し、認証取得可能なレベルでの内部監査は定期的に実施しております。詳しくは下記「リコーグループの情報セキュリティ」をご参照ください。
https://jp.ricoh.com/security/management

なお、本サービスの販売元となるリコージャパンにおいては以下の認証を取得しております。

ISO27001（JQA-IM1520）

Copyright © 2022 Ricoh Company, Ltd. All rights reserved.