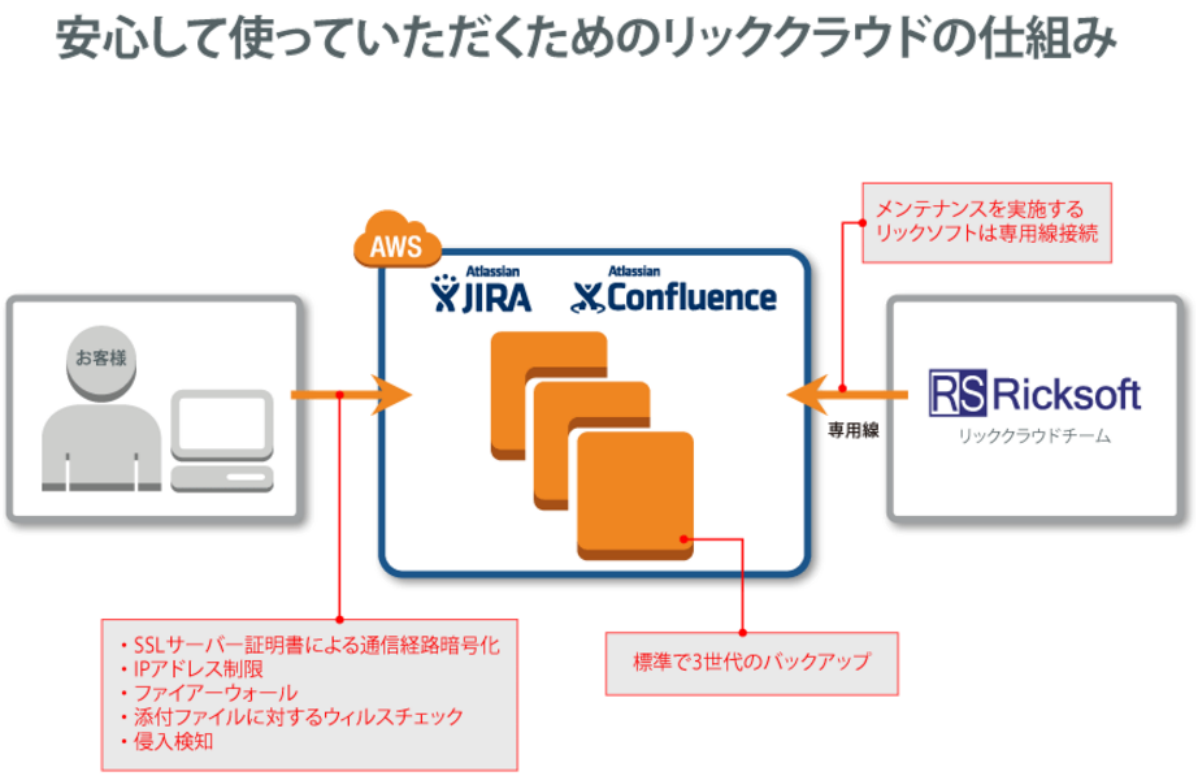
ISO27017：RickCloud利用規約（補足事項）

本RickCloud利用規約（補足事項）は、RickCloudサービスの利用規約で不足する、利用者へ向けたサービス内容の説明資料となっています。
また本説明資料は、ISMSクラウドセキュリティ認証が、利用者への開示を義務付けた要求事項の説明資料の役割も兼ねています。
リックソフトは、第三者認証機関の情報セキュリティ認証を取得することで、お客様へより安全で安心なクラウドサービスの提供を行います。

※（カッコ）内の記号は、情報セキュリティ認証（ISO/IEC27001）の要求事項の項目番号を表します。

【RickCloud環境のイメージ図】



関係当局との連絡（A.6.1.3）

- RickCloudでは、AWS(Amazon Web Services) 東京リージョン(ap-northeast-1)
  を利用してサービスに係る全てのデータを保存しています。

情報セキュリティの意識向上、教育及び訓練（A.7.2.2）

- RickCloud運用担当者は、クラウドサービスにおいて、お客様のデータを適切に扱うための教育及び訓練を定期的に受けています。

情報のラベル付け（A.8.2.2）

- RickCloudでは、お客様の運用環境を識別するためのラベル付け機能を提供しています。
- 運用環境（アプリケーション）ごとに一意のラベルが付与され、お客様は運用環境を識別することが可能です。
- 運用環境に付与されたラベルは、「コントロールパネル」で確認することができます。
- ラベル付けはRickCloud運用担当者が行います。お客様自身でラベルの追加や変更・削除を行うことはできません。
- 原則として、一度設定されたラベルを変更することはできません。

利用者の秘密認証情報の管理（A.9.2.4）

- RickCloudでは、アプリケーション管理者の認証情報を安全な方法でお客様へお知らせいたします。
- アプリケーション管理者は、管理者アカウントの管理および利用者アカウントの作成・削除・参照権限を管理する責任があります。

仮想コンピューティング環境における分類（A.9.5.1）

- RickCloudでは、お客様へ提供する環境（データ、アプリケーション、OS、ストレージ、ネットワークなど）と他社様の動作環境の論理的分離を保証しています。
- 論理的分離は、AWSのEC2(Elastic Compute Cloud), EBS(Elastic Block Store), VPC(Virtual Private Cloud)により実現されます。

仮想マシンの要塞化（A.9.5.2）

1. お客様の運用環境（インスタンス）は、AWS環境下の仮想化されたマルチテナント環境(EC2)で運用しています。
2. お客様の運用環境が、他の利用者と共有されることはありません。
3. お客様の運用環境は、ファイアウォール（AWSのセキュリティグループ、および
   ネットワークACL）とIPS（侵入防止システム）により、外部（インターネット側）からの脅威を低減する仕組みを備えています。
4. お客様の運用環境は、クライアント証明書およびIPアドレス制限など、セキュリティを強化するためのオプションによって接続元の制限を行っていただけます。
5. お客様の運用環境で行われた操作は、ログに記録され、管理されます。このログは、アプリケーションより提供されるログダウンロード機能により取得することができます。
6. お客様の運用環境は、日次でのデータバックアップ（ログ含む）、ウィルスチェックなどがスケジュールされ実行されています。
7. お客様の運用環境のOS（オペレーティングシステム）およびミドルウェアに脆弱性が生じた場合は、修正プログラム（セキュリティパッチ）の適用が行われます。
8. お客様の運用環境と、お客様の運用環境へ接続を行う端末間のデータ通信は、HTTPS(SSL/TLS)により保護され、通信経路は暗号化され、安全に接続されます。
9. リックソフトは、プライベート接続(Direct Connect,
   VPN等)およびSSH接続を用いてAWSへ安全に接続し、お客様の運用環境等のメンテナンスを実施しています。
10. お客様の運用可能等のメンテナンスを実施可能な端末は、特定の端末に限定されています。
11. リックソフトのRickCloud運用担当者により行われた操作は、特権的な操作を含め、全てログに記録・管理されます。

暗号による管理策の利用方針（A.10.1.1）

- RickCloudで利用される暗号は「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」に準拠します。

装置のセキュリティを保った処分又は再利用（A.11.2.7）

- RickCloudでは、物理的装置の廃棄についてはAWSの仕様に準拠します。利用したインスタンスの再利用などは一切行いません。

実務管理者の運用のセキュリティ（A.12.1.5）

- アプリケーション管理者であってもクラウドサービス環境に影響を及ぼすような操作は実行できません。

情報のバックアップ（A.12.3.1）

1. バックアップ範囲及びスケジュール
   - データのバックアップはお客様のインスタンス単位に毎日0時30分より一斉に実施されます。
2. 該当する場合は暗号を含む、バックアップ手法とデータ形式
   バックアップデータは、お客様の運用環境とは別の領域へ安全に保管されます。
   a. ファイル・フォルダ単位のバックアップ（アプリケーションに関するディレクトリ配下）
   b. データベースのバックアップ
   c. スナップショットのバックアップ（アプリケーションインスタンスのボリューム全体）
3. 完全性検証手順
   a. ファイル・フォルダ単位のバックアップ（アプリケーションに関するディレクトリ配下）
      - バックアップ後にエラーが発生しないことを確認します。
      - 後述の「試験手順」の実施を行い、不定期に方法・結果の検証を行います。
   b. データベースのバックアップ
      - バックアップ後にエラーが発生しないことを確認します。
      - 後述の「試験手順」の実施を行い、不定期に方法・結果の検証を行います。
   c. スナップショットのバックアップ（アプリケーションインスタンスのボリューム全体）
      - スナップショット取得後にエラーが発生しないことを確認します。
      - 後述の「試験手順」の実施を行い、不定期に方法・結果の検証を行います。
4. データ復旧（リストア）手順と所用時間
   - データボリュームのサイズおよび復旧方法（ボリューム単位／ファイル・データベース単位）により異なります。
   - バックアップからの復旧には、通常24時間程度を想定しておりますが、お客様のデータボリュームにより差異が生じる場合がございます。
5. 試験手順
   - お客様の運用環境を模した環境を用意し不定期に復元（リストア）試験を行い、バックアップ機能の正常性を検証しています。
   - また、お客様の運用環境は、復元後にログイン可能な状態であることを確認したうえで引き渡しています。
6. 保存期間（保持期間）

- バックアップデータは過去３日間分の保存が保証されています。

クロックの同期（A.12.4.4）

- NTPを用いて、時刻合わせを行っています。
- 時刻合わせに用いるNTPサーバは、Amazon Time Sync Service および ntp.orgを使用しています。

クラウドサービスの監視（A.12.4.5）

- お客様向け監視機能として、お客様運用環境のリソース状況および’転送量をお客様自身でご確認いただける機能（コントロールパネル）を提供しております。
- RickCloudでは、お客様運用環境の稼働状況の監視を随時行っており、正常運用に影響が予想される場合、お客様へ通知いたします。
- OSやアプリケーションの不具合等により正常運用が困難と判断された場合、アプリケーション再起動が自動または手動で行われます。
- お客様の利用状況によりアプリケーションの性能不足が継続的に生じ、正常な運用を行うことが難しい場合は、お客様へプラン変更等の提案を行います。
- RickCloudでは、アプリケーションの脆弱性を確認した場合、お客様へその影響範囲を通知します。

情報セキュリティ要求事項の分析及び仕様化（A.14.1.1）

アプリケーション環境に関する安全性

- アプリケーションの運用管理と権限設定はお客様自身で管理することができます。
- IPアドレス制限、クライアント証明書オプションを利用いただくことで、接続元の制限が可能です。
- HTTPS(SSL/TLS)接続により、アプリケーションとお客様の端末間の通信経路は暗号化されます。え

仮想マシン（インスタンス）に関する安全性

- 第三者機関によるクラウドサービス認証を取得したプロバイダー（AWS）を利用しています。
- ファイアウォール、IPSにより外部（インターネット側）からの脅威を低減しています。
- OS・ミドルウェアに脆弱性が確認された場合は、お客様へ通知の上で更新プログラム（セキュリティパッチ）の適用を行います。

運用・管理に関する安全性

- 接続可能な端末を限定し、かつプライベート接続(Direct Connect,
  VPN等)およびSSH接続を用いて、安全に運用保守作業を行っています。
- 認証サーバによるアカウント管理およびユーザー認証、暗号鍵（公開鍵・秘密鍵）によるユーザー認証を行っています。
- RickCloud運用作業者は、必要時のみ作業用のアカウントが付与され、また作業に必要なインスタンス以外に接続できないようになっています。

アプリケーションに関する例外事項

- RickCloudでは、アプリケーションのバージョンアップは自動的に行われません。
- RickCloudでは、お客様へアプリケーションの脆弱性の影響範囲を通知いたします。お客様は、影響範囲よりバージョンアップ実施の有無を検討いただけます。
- アプリケーションのバージョンアップが必要となる場合、お客様はRickCloudへバージョンアップの依頼を行います。バージョンアップに係る作業はリックソフトが行います。
- アプリケーションの脆弱性により、RickCloudサービス全体や他のお客様へ影響を及ぼす可能性がある場合、お客様のインスタンスを停止させていただく場合がございます。

セキュリティに配慮した開発のための方針（A.14.2.1）

- RickCloudの検証環境は、お客様運用環境とは異なるインスタンスとして用意します。
- RickCloudの検証環境は、リッククラウド管理者が環境準備を行い、作業担当者へ検証用インスタンスを割り当てます。

責任及び手順（A.16.1.1）

インシデント管理に関する責任の割当てと手順は以下のとおりです。

1. お客様へ報告する情報セキュリティインシデントの範囲：お客様の運用環境に何らかの異常な影響を及ぼす状況
2. 情報セキュリティインシデントの検出及び対応の開示レベル：当社によるお客様運用環境の監視結果から影響範囲と対策を開示する
3. 情報セキュリティインシデントの通知目標時間：24時間以内
4. 情報セキュリティインシデントの通知手順：ヘルプデスクまたはお客様担当窓口への電話連絡
5. 情報セキュリティインシデントに関する窓口情報：ヘルプデスクまたは当社問い合わせ窓口
6. 特定の情報セキュリティインシデントが発生した場合に適用可能な全ての対処
    a. お客様運用環境の緊急停止の必要性有無の判断
    b. お客様運用環境の復旧方法についての検討
    c. お客様運用環境の復旧後の検証方法の検討
    d. お客様運用環境における再発防止策と適用方法の検討

証拠の収集（A.16.1.7）

- お客様は、基本的なディジタル証拠（ログファイル等）をアプリケーション上で取得することができます。
- アプリケーション上で取得できないディジタル証拠（ログファイル等）は、有償で取得することが可能です。

記録の保護（A.18.1.3）

- お客様の運用環境内にあるディジタル証拠（ログファイル等）は、アプリケーションデータと同様に安全に保護されます。

暗号化機能に対する規制（A.18.1.5）

- RickCloudでは、データ送受信をHTTPS(SSL/TLS)を用い保護します。対応する暗号リストは、CRYPTREC暗号リストに準拠します。
- RickCloudでは、お客様の接続元の国およびその国の法域について一切関知しません。日本国外からの利用については、お客様の責任のもとで行っていただきます。
- RickCloudでは、IPアドレス制限オプション提供しております。本オプションを利用いただくことで、接続元を制限し、暗号化規制のある国からの接続を制限することが可能です。

情報セキュリティの独立したレビュー（A.18.2.1）

- RickCloudは、弊社が取得するISO/IEC 27001のセキュリティ運用ルールに基づき安全に管理されています。

2017年04月01日 制定
2017年06月25日 改訂
2018年05月18日 改訂

リックソフト株式会社

情報セキュリティ管理責任者 佐藤 聖吾