Ｓ．Ｔ．Ｅ．Ｐ
プライベートクラウドサービス
セキュリティホワイトペーパー

２０２４年4月

第1.0版

北海道総合通信網株式会社

変更履歴

版	変更年月	変更内容	備考
第 1.0 版	2024/4	初版	

目次

Ⅰ．目的

セキュリティホワイトペーパー（以下、本書という）は、ISMS（情報セキュリティマネジメントシステム）のクラウドセキュリティ認証である「ISO/IEC 27017：2015」で求められている要求事項の中で、北海道総合通信網株式会社（以下、弊社という）がお客様に対し提供しているセキュリティの取組みについて明確にし、ご確認いただくことを目的としています。

・ISO/IEC 27017 について・・・ISO/IEC 27017 は、クラウドサービスの提供及び利用に適用できる情報セキュリティ管理策のための指針を示した国際規格です。クラウドサービスに関する情報セキュリティ管理策の実践の規範として、ISO/IEC 27017 で、情報セキュリティ全般に関するマネジメントシステム規格 ISO/IEC 27001 の取組みを強化します。これにより、クラウドサービスにも対応した情報セキュリティ管理体制を構築し、その実践を支援します。

Ⅱ．適用範囲について

弊社の ISO/IEC 27017 の適用範囲は、以下のサービス内容に対するものです。
・S.T.E.P プライベートクラウドサービス （https://www.hotnet.co.jp/service/pvc/）

Ⅲ．用語について

本書では ISO/IEC 27017:2015（JIS Q 27017:2016)で記されている用語については、改変せずに使用しています。本サービスで利用している用語については、「S.T.E.P プライベートクラウド サービス利用規約」及び「S.T.E.P プライベートクラウドサービス仕様書」にてご確認いただけます。

Ⅳ．ISO/IEC 27017:2015（JIS Q 27017:2016）への対応

以下に ISO/IEC 27017:2015（JIS Q27017:2016)が求める要求事項に対する管理策を記載します。番号・タイトルは、ISO/IEC 27017 が求める「情報セキュリティ管理策の実践の規範」 5～18（17 を除く）の小項目番号・要求事項原文を示しています。

5. 情報セキュリティ方針のための方針群

5.1 情報セキュリティのための経営陣の方向性

5.1.1 情報セキュリティのための方針群

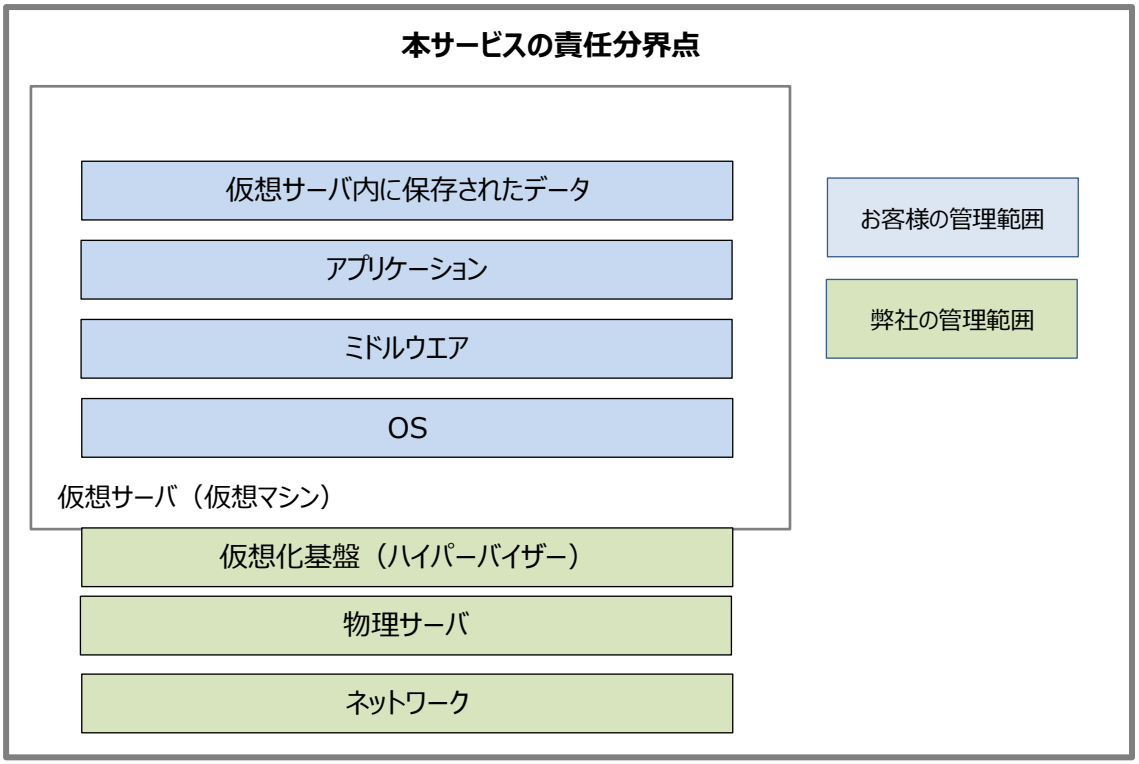
クラウドサービスプロバイダ(CSP)は、クラウドサービスの提供及び利用に取り組むため、情報セキュリティ方針を拡充することが求められています。 本サービスでは、弊社の情報セキュリティ方針並びにクラウドセキュリティ方針に従いサービスを運用しています。

6. 情報セキュリティのための組織

6.1　内部組織

6.1.1　情報セキュリティの役割及び責任

情報セキュリティの役割及び責任について、「S.T.E.P プライベートクラウドサービス利用規約」に定め、サービスを提供しています。本サービスにおける責任分界点は、下図のとおりです。



6.1.3　関係当局との連絡

弊社所在地は、北海道札幌市中央区北1条東2丁目5番3 塚本ビル北1館となります。また、本サービス上に保存されるデータの所在は日本国内になります。

CLD.6.3　クラウドサービスカスタマとクラウドサービスプロバイダとの関係

CLD.6.3.1　クラウドコンピューティング環境における役割及び責任の共有及び分担

情報セキュリティの役割及び責任について、「S.T.E.P プライベートクラウドサービス利用規約」に定め、サービスを提供しています。本サービスの責任分界点に関しては、「6.1.1 情報セキュリティの役割及び責任」をご参照ください。

7.　人的資源のセキュリティ

7.2　雇用期間中

7.2.2　情報セキュリティの意識向上、教育及び訓練

本サービスのセキュリティ要件及び運営ルールの順守を目的として、サービスに従事する要員を対象とした教育・訓練及び意識向上の策を実施しています。

8.　資産の管理

8.1　資産に対する責任

8.1.1　資産目録

利用者の情報資産(保存データ)とサービス提供者が運営するための情報資産は、情報資産台帳上で明確に識別の上分離しています。

なお、本サービスに利用者が作成・保存する情報資産は、利用者の管理範囲となります。

CLD.8.1.5　クラウドサービスカスタマの資産の除去

お客様が本サービスの利用を停止または終了した場合、お客様が本サービス上に保存したデータは、お客様の責任において削除いただくことを原則としております。その上で、弊社において「S.T.E.P プライベートクラウドサービス利用規約」に基づき、解約申し込み日から翌々月末日までに削除いたします。

8.2　情報の分類

8.2.2　情報のラベル付け

本サービスをご利用いただくにあたり、お客様はインスタンス名称をラベル付け機能として利用し、対象となる仮想サーバを識別することができます。

9.　アクセス制御

9.2　利用者アクセスの管理

9.2.1　利用者登録及び登録削除

お客様のサービス利用開始時に、弊社より初期IDをご案内いたします。お客様は当該IDを利用し、仮想マシン上のユーザー管理及びアクセス権管理を実施いただくことができます。

9.2.2　利用者アクセスの提供(provisioning)

お客様は、弊社より払い出した初期IDを利用し、仮想マシン上のユーザーのアクセス権管理を実施いただくことができます。

9.2.3　特権的アクセス権の管理

特権的アクセス権は管理者アカウントが該当いたします。当該権限の利用においては、仮想マシンにログインする際に、ログインID、パスワードによる認証によって情報セキュリティを確保しています。アカウントは、自己の責任で適切に管理をお願いします。

9.2.4　利用者の秘密認証情報の管理

お申し込み後の初回利用時の初期パスワードは、担当よりご案内いたします。初期パスワードでログイン後は、お客様のパスワードポリシーに従って設定いただくことが可能です。

9.4　システム及び業務用ソフトウェアのアクセス制御

9.4.1　情報へのアクセス制限

本サービスのご利用にあたっては、お客様側のアクセスポリシーを適用し、お客様の設定

にて情報へのアクセス制限を行うことができます。

9.4.4　特権的なユーティリティプログラムの使用

利用者に対し、セキュリティ手順を回避し各種サービス機能の利用を可能とするAPI等のユーティリティプログラムの提供は、行っておりません。

また、弊社にて運用保守のために保持する特権的ユーティリティプログラムについては、利用者を厳しく限定し、ログによるレビューを実施しております。

CLD.9.5　共有する仮想環境におけるクラウドサービスカスタマデータのアクセス制御

CLD.9.5.1　仮想コンピューティング環境における分離

本サービスでは、お客様毎にリソース及びネットワーク領域を分離しており、マルチテナント環境でご利用いただけます。

CLD.9.5.2　仮想マシンの要塞化

構築するすべての仮想化環境は、お客様からサービス申込の際にご指定いただいた設定でご提供いたします。また、弊社標準の仮想マシン構築手順を整備し、ポート・プロトコルへの制限を実施した上で仮想マシンを要塞化してご提供します。

10.　暗号

10.1　暗号による管理策

10.1.1　暗号による管理策の利用方針

本サービスでは、以下の暗号化を実施しております。

ストレージ：ストレージの暗号化機能を搭載

なお、仮想マシン内で扱うデータの暗号化については、お客様にて任意の暗号化を設定いただけます。

通信：SSL通信を利用（弊社の保守端末から仮想基盤間）

なお、お客様環境から仮想マシンまでの通信及びサービス上のデータについては、お客様にて任意の暗号化を実施いただけます。

11.　物理的及び環境的セキュリティ

11.2　装置

11.2.7　装置のセキュリティを保った処分又は再利用

機器の老朽化、故障等により交換した機器媒体の処理については、弊社内のルールに従って廃棄・再利用しており、廃棄に際しては記録を保持しております。

12.　運用のセキュリティ

12.1　運用の手順及び責任

12.1.2　変更管理

提供するサービスの更新や定期メンテナンスを実施する場合、その影響がお客様に限定される場合は、サービスお申込み時に取り決めた期日までにお知らせいたします。すべてのお

客様に影響がある作業については、原則30日前までに通知させていただきます。なお、通知方法はメールとなります。

12.1.3　容量・能力の管理

安定的なサービス提供を行うため、仮想基盤のリソースを監視し、必要に応じてキャパシティの増強を行っています。

CLD.12.1.5　実務管理者の運用のセキュリティ

本サービスにおけるDashboardの操作方法は、Dashboard上に必要な操作説明のページを準備しております。

12.3　バックアップ

12.3.1　情報のバックアップ

本サービスでは、ストレージのデータバックアップについては、お客様が指定したタイミングで契約単位に取得します。データバックアップからのリストアについては、仮想サーバリストアオプションを利用することで、仮想サーバ単位でリストアすることが可能です。

12.4　ログ取得及び監視

12.4.1　イベントログ取得

本サービスでは、お客様に仮想化基盤へのログイン/ログアウト及び操作ログの取得機能を過去30日分までご提供可能です。ログについては、アクセス制御されたログ管理サーバで保存しております。弊社側でアクセスログの追跡はできかねますので、お客様ご自身で管理をお願い致します。

12.4.4　クロックの同期

本サービスは、日本時間を基準としており、お客様に時刻同期の基準となるNTPサーバを参照できるよう設定いただくことができます。

CLD.12.4.5　クラウドサービスの監視

本サービスでは、開発・構築時に監視要件を決定し、実装しております。お客様はDashboardの機能を利用してリソース監視を実施することができます。

12.6　技術的脆弱性管理

12.6.1　技術的脆弱性の管理

本サービスでは、脆弱性情報を常時収集しております。収集した情報を元に、サービス設備への影響を評価し、弊社の責任範囲において影響がある場合は、速やかに対応しております。お客様への影響があり、メンテナンスを必要とする場合は、Dashboard 上でのお知らせ、またはメールで通知いたします。

13. 通信のセキュリティ

13.1 ネットワークセキュリティ管理

13.1.3 ネットワークの分離

本サービスでは、開発・構築時にNWセキュリティ要件を決定し、用途別にネットワークを分離しております。

CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合

本サービスにおける物理ネットワーク及び仮想ネットワークは、それぞれ管理表に基づいて弊社内部ネットワーク領域とお客様ネットワークの割り当てを管理することで整合性を確保しています。

14. システムの取得、開発及び保守

14.1 情報システムのセキュリティ要求事項

14.1.1 情報セキュリティ要求事項の分析及び仕様化

弊社では、弊社内の規程に従い、サービスの設計・開発・構築時にセキュリティ要件を決定し、実装しております。

主にお客様が検討される情報セキュリティの機能の仕様として、本書は以下の項目を記載しています。

・アクセス制限機能（CLD.9.5.2 仮想マシンの要塞化）
・通信暗号化機能（10.1.1 暗号による管理策の利用方針）
・ログ取得機能（12.4.1 イベントログ取得）

14.2 開発及びサポートプロセスにおけるセキュリティ

14.2.1 セキュリティに配慮した開発のための方針

弊社では、セキュリティに配慮した開発方針として「セキュリティ・バイ・デザイン」の原則に則り、社内の規程に従って開発時点からセキュリティに関するリスク対応、脆弱性対応を実装し、試験を実施した上でリリースしております。

15. 供給者関係

15.1 供給者関係における情報セキュリティ

15.1.2 供給者との合意におけるセキュリティの取扱い

本サービスにおける役割及び責任については、「S.T.E.P プライベートクラウド サービス利用規約」に定め、サービスを提供します。本サービスの責任分界点に関しては、「6.1.1 情報セキュリティの役割及び責任」をご参照ください。

15.1.3 ICT サプライチェーン

弊社が、利用するクラウドサービスプロバイダの情報セキュリティ水準を把握し、本サービスの情報セキュリティとの整合性が取れていることを確認しています。

16.　情報セキュリティインシデント管理

16.1　情報セキュリティインシデントの管理及びその改善

16.1.1　責任及び手順

利用者が本サービス上で取り扱う情報の機密性、完全性、可用性に影響を与えるセキュリティインシデント(データの消失、長時間のシステム停止等) が発生した場合は、インシデントの発生を確認してから3営業日を目標に、メール、電話、弊社Webサイトへの掲載により通知いたします。セキュリティインシデントに関する問合せは、本サービスお問い合わせサポートより受け付けています。

16.1.2　情報セキュリティ事象の報告

Dashboard上でのお知らせ、またはメールで通知いたします。

また個別のお問い合わせは、本サービスお問い合わせサポートより受け付けています。

16.1.7　証拠の収集

裁判所からの開示請求など、法律に基づいた正当な開示請求が行われた場合、お客様の同意なく、利用者のデータを当該機関に開示することがあります。詳細は、「S.T.E.P プライベートクラウド サービス利用規約」をご確認ください。なお、お客様に重要なインシデントが発生し、実態調査を目的としたログ情報等が必要な場合には本サービスお問い合わせサポートまでお問い合わせください。

18.　順守

18.1　法的及び契約上の要求事項の順守目的

18.1.1　適用法令及び契約上の要求事項の特定

本サービスの利用に関して適用される「準拠法」は、「日本法」となります。本サービス運用に関連する各種法令に関しては法規制管理台帳を作成し、準拠するように努めています。

18.1.2　知的財産権

本サービスをご利用いただく上で知的財産権に関わるお問い合わせは、本サービスお問い合わせサポートまでお問い合わせください。

18.1.3　記録の保護

利用者の本サービスご利用に関して蓄積された記録に対しては、不正アクセス・改ざんなどを防ぐためアクセス制限を実施しています。

18.1.5　暗号化機能に対する規制

本サービスでは、各種暗号化機能を利用しています。　(10.1.1　暗号による管理策の利用方針　参照) なお、輸出規制の対象となる暗号化の利用はありません。

18.2　情報セキュリティのレビュー

18.2.1　情報セキュリティの独立したレビュー

弊社では、社内内部監査、マネジメントレビュー、年度リスクアセスメントの実施に加え、ISO/IEC 27001、ISO/IEC27017に基づく第三者による認証審査を受け、情報セキュリティに対する取組みを行うことで、安全なセキュリティレベルを確保します。（初回認証審査は2024年11月を予定）

以上