Datachemical LAB
ホワイトペーパー

データケミカル株式会社

目次

I. 目的

セキュリティホワイトペーパー（以下本書）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、当社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 の取り組みを強化します。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

当社の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。

・Datachemical LAB

なお、Datachemical LABについては以下サイトをご参照下さい。

https://www.datachemicallab.com/

お問い合わせの窓口

Datachemical LABお問い合わせサポート

- 電話：03-6778-2045
- メール：inquiry@datachemicallab.app
- 営業時間：平日 9:00 ～ 18:00

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、そのまま使用しています。Datachemical LABで利用している用語については、Datachemical LAB利用規約で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

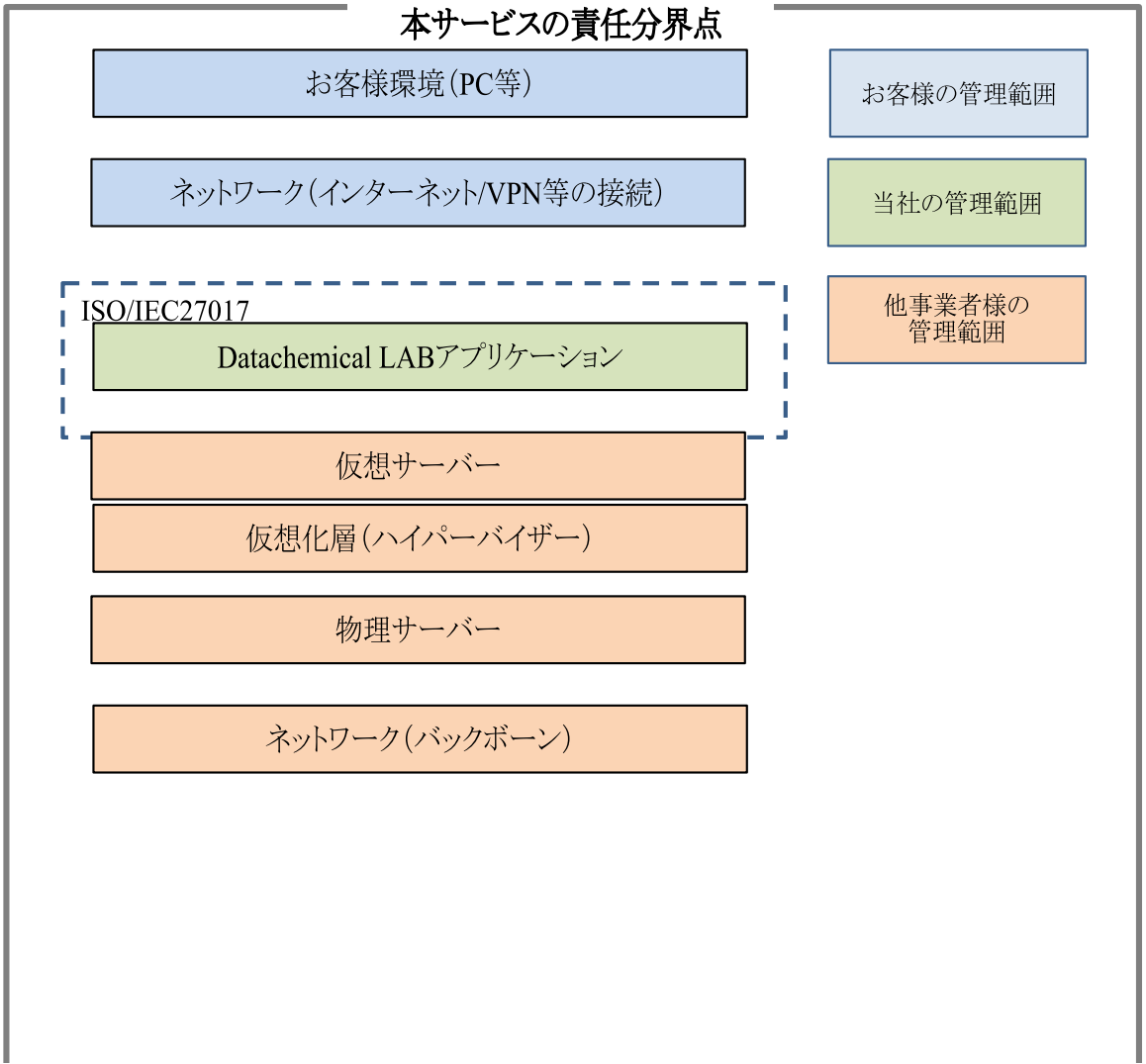
クラウドサービスプロバイダ(CSP)は、 クラウドサービスの提供および利用に取り組むため、情報セキュリティ方針を拡充することが求められています。Datachemical LABでは、当社の情報セキュリティ方針並びにクラウドサービス情報セキュリティ方針に従いサービスを運用しています。

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および責任

情報セキュリティの役割および責任について利用規約に定め、サービスを提供しています。Datachemical LAB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

当社所在地は、東京都渋谷区神宮前6丁目23-4　桑野ビル2階となります。また、クラウドサービスで保存いただく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および責任の共有および分担

情報セキュリティの役割および責任について利用規約に定め、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および責任」をご参照下さい。

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、教育および訓練

情報セキュリティ要件の周知徹底とクラウドサービスの運営ルール徹底を目的として、サービスに従事する要員を対象とした教育・訓練およ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明確に分離し、情報資産台帳に登録しています。

なお、Datachemical LAB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 クラウドサービス利用者の資産の除去

本サービスでは、利用者データに対する情報漏洩リスクを低減するため、サービス上にデータを保存しない仕様としており、データ保存領域を設けないことを以てリスク対策としております。

8.2 情報の分類

8.2.2 情報のラベル付け

Datachemical LABは、登録情報に対してIDや各種番号によるラベル付け機能を搭載しており、円滑なサービス提供を実現しています。詳細は、操作マニュアルにてご確認頂けます。

9 アクセス制御
9.2 利用者アクセスの管理
9.2.1 利用者登録および登録削除
ローカルアカウントの利用者登録及び削除は、スタンダードアカウントの利用者がユーザー管理画面にて行うことができます。

9.2.2 利用者アクセスの提供(provisioning)
お客様は、Datachemical LABの各種機能を当社が設定した必要な範囲でご利用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
お客様は、メールアドレスとパスワードによりDatachemical LABをご利用いただくことができます。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
Datachemical LABのログインパスワードは当社のパスワードポリシーが適用されます。利用開始時にパスワードポリシーに沿ってパスワードを設定してください。

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
Datachemical LABのご利用にあたっては、当社が設定した権限の範囲で情報にアクセスすることができます。

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。
当社にて運用保守のために保持するGoogle adminについては、利用者を限定し、定期的にログをレビューしております。

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
マルチテナント環境で動作します。テナント毎のIDによるアクセス資源の分離を実施し、別テナントへのアクセス制御を実施しています。

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ポート・プロトコルへの制限を実施し、不正アクセスを遮断して適切にログを保存しています。

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
Datachemical LABのデータはクラウド上の保存されない仕様とすることでデータ保護をはかっています。また、通信は　https を用いて暗号化しています。

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、当社では直接装置の処分を行うことはありません。Google の施設、建物、および物理上のセキュリティに基づきます。

【ハードウェアの追跡および廃棄】
https://cloud.google.com/docs/security/overview/whitepaper?hl=ja#hardware_tracking_and_disposal

12 運用のセキュリテイ
12.1 運用の手順及び責任
12.1.2 変更管理
提供するサービスに影響を与えるメンテナンス等を実施する場合、事前にメールにて通知いたします。

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、各サーバー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
Datachemical LAB操作方法は、ご契約いただきましたお客様に対して専用のサポートサイトにてご案内しております。

12.3 バックアップ
12.3.1 情報のバックアップ
本サービスはデータの保管を目的とするものではないため、バックアップ機能は提供しておりません。データのバックアップ作業についてはお客様責任で実施いただくものとします。

12.4 ログ取得及び監視
12.4.1 イベントログ取得
Datachemical LABをご利用いただくにあたり、お客様の必要に応じて過去半年間分のアクセスログをご提供することができます。Datachemical LABお問い合わせサポートまでお問い合わせください。

12.4.4 クロックの同期

Datachemical LABではGCPが基準とするNTP サーバーを参照することで時刻を同期（日本標準時）しています。

CLD.12.4.5 クラウドサービスの監視

Datachemical LAB ではGoogleのCloud Monitoringを用いてリソース、エラーログを監視し、必要な措置を取っています。

12.6 技術的脆弱性管理

12.6.1 技術的脆弱性の管理

Datachemical LABに関する脆弱性については、情報収集を実施しており、当社の責任の範囲で対応が必要となった場合には、定期または緊急メンテナンスにて対応を実施します。メンテナンス情報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

インターネット回線を利用してDatachemical LABへ接続し、テナント毎にIDにより論理的にセキュリティを確保しています。

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および仕様化

当社では、情報セキュリティ方針の下で、お客様が要求される情報セキュリティを維持、提供しています。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、当ホワイトペーパーは以下の項目を記載しています。

- アクセス制限機能（9.4.1 情報へのアクセス制限、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

当社では、セキュリティに配慮した開発方針として、開発時点からセキュリティに関するリスク対応、脆弱性対応を行っています。

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

Datachemical LABにおける役割及び責任については、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および責任」をご参照下さい。

15.1.3 ICT サプライチェーン

当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、Datachemical LAB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。

Datachemical LABは、GCPをクラウドサービスプロバイダとして運用しています。GCPのセキュリティ対策につきましては、以下のGoogle Cloud Security Whitepaperをご参照下さい。

https://services.google.com/fh/files/misc/security_whitepapers_4_booklet_jp.pdf

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 責任および手順

利用者に大きな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 24時間以内を目標にメールで通知いたします。

セキュリティインシデントに関する問合せは、Datachemical LAB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

Datachemical LABにおいて発生した情報セキュリティインシデントの予兆と思われる事象については、メールにて通知いたします。

また、お客様にて事象を検知した場合は、Datachemical LABお問い合わせサポートより受付けています。

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、利用者の同意なく、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、Datachemical LAB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Datachemical LAB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 適用法令および契約上の要求事項の特定

Datachemical LABの利用に関して、適用される「準拠法」は「日本法」と

なります。

Datachemical LAB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、法的準拠するように努めています。

18.1.2 知的財産権

Datachemical LAB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、Datachemical LABお問い合わせサポートまでお問い合わせ下さい。

18.1.3 記録の保護

利用者のDatachemical LAB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

Datachemical LABでは　httpsによる通信の暗号化を使用しています。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

当社では、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り組みを行うことで、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2023年5月を予定）

V. 変更履歴

版	日付	改訂内容
第1.0版	2023/1/31	初版作成
第1.1版	2024/2/1	情報漏洩対策強化に伴ってデータ登録機能を廃止した変更をCLD8.1.5の記載に反映した。

以上