# クラウドサービス
# セキュリティガイドライン

初版 2022 年 12 月 5 日

更新 2023 年 2 月 1 日

株式会社網屋

# 改訂履歴

| 版数 | 改訂内容 | 改訂日 |
|---|---|---|
| **1.0** | 新規作成 | 2022 年 12 月 5 日 |
| **1.1** | Verona 関連サービスの名称変更に伴う改訂 | 2023 年 2 月 1 日 |
| | | |
| | | |
| | | |
| | | |

# 目次

# はじめに

本クラウドサービスセキュリティガイドライン（以下、「本ガイドライン」といいます）は、

**株式会社網屋**（以下、「弊社」といいます）がお客様に提供するクラウドサービス「Verona」及び「Hypersonix」におけるセキュリティに関する取り組みを記述した文書であり、JIS Q 27017 (ISO/IEC27017)の規格（以下「ISO27017」といいます）に依拠して作成されたものです。

なお、本ガイドラインの内容は冒頭記載の時点での取り組みに基づくものです。内容は予告なく変更される場合があります。

# 1. お客様との責任分界点

「責任分界点」とはお客様と弊社のそれぞれがクラウド基盤のどこからどこまでを担当するかを定めた境界をいいます。「クラウドサービスの管理範囲」と捉えていただければと存じ上げます。

Verona 及び Hypersonix は、SaaS 型のクラウドサービスです。

本ガイドラインの対象となるサービス（以下「本サービス」といいます）は、その機能によってクラウド管理センターと配下の VPN 装置、無線アクセスポイント等について、弊社へのご依頼に応じお客様側で制御する仕組みを取ることができるようになっています。この点、一般的な SaaS 型クラウドサービス（お客様側で管理・制御できるところがほとんどないもの）とは異なっています。

上記の関係性、及びお客様と弊社の管理範囲については、サービスごとに以下へ図示します。

## 1-1. Verona の責任範囲

1-1-1A Verona Edge（ハードウェア及びソフトウェアで構成されるもの）

・Verona Edge (VPN 装置)の物理的なハードウェアの保管・維持を含む管理責任は、

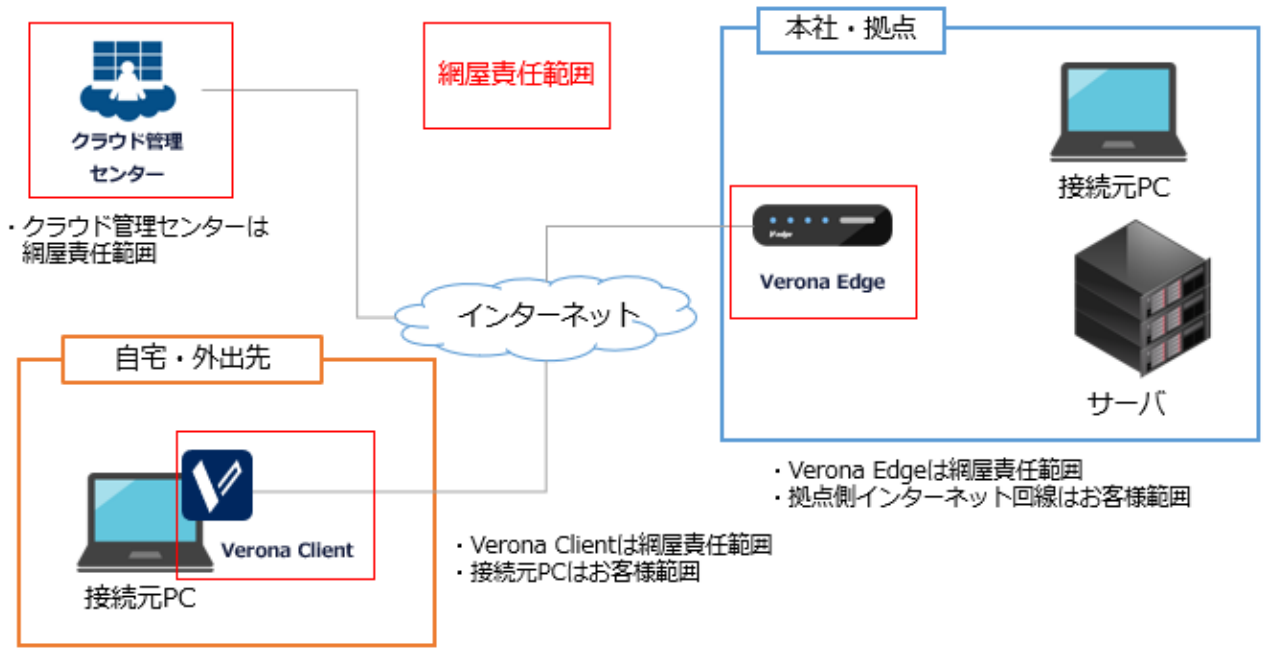
買取品・レンタル品に限らず、お客様にあるものとします。

・Verona Edge 内のソフトウェアの管理責任は、弊社にあるものとします。

1-1-1B Verona Client（ソフトウェア）

Verona Client の管理責任は、弊社にあるものとしますが、これをインストールした接続元 PC の管理責任は、お客様にあるものとします。

1-1-1C 拠点側インターネット回線の管理責任は、お客様にあるものとします。



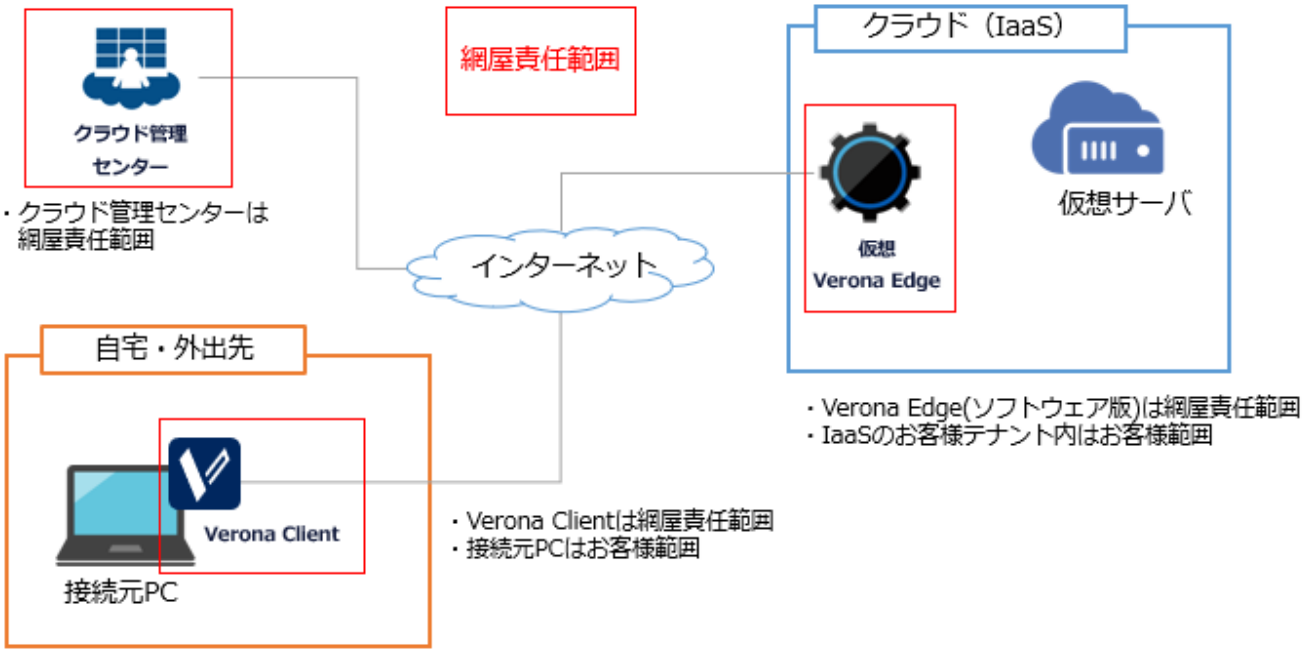
1-1-2 Verona Edge (ソフトウェア版)

1-1-2A Verona Edge (ソフトウェア版) の管理責任は、弊社にあるものとします。

1-1-2B Verona Edge (ソフトウェア版)が搭載される IaaS のお客様テナント内の管理責任は、お客様にあるものとします。

1-1-2C Verona Client の管理責任は、弊社にあるものとします。
これをインストールした接続元 PC の管理責任は、お客様にあるものとします。

1-1-2D お客様テナント側インターネット回線の管理責任は、お客様にあるものとします。



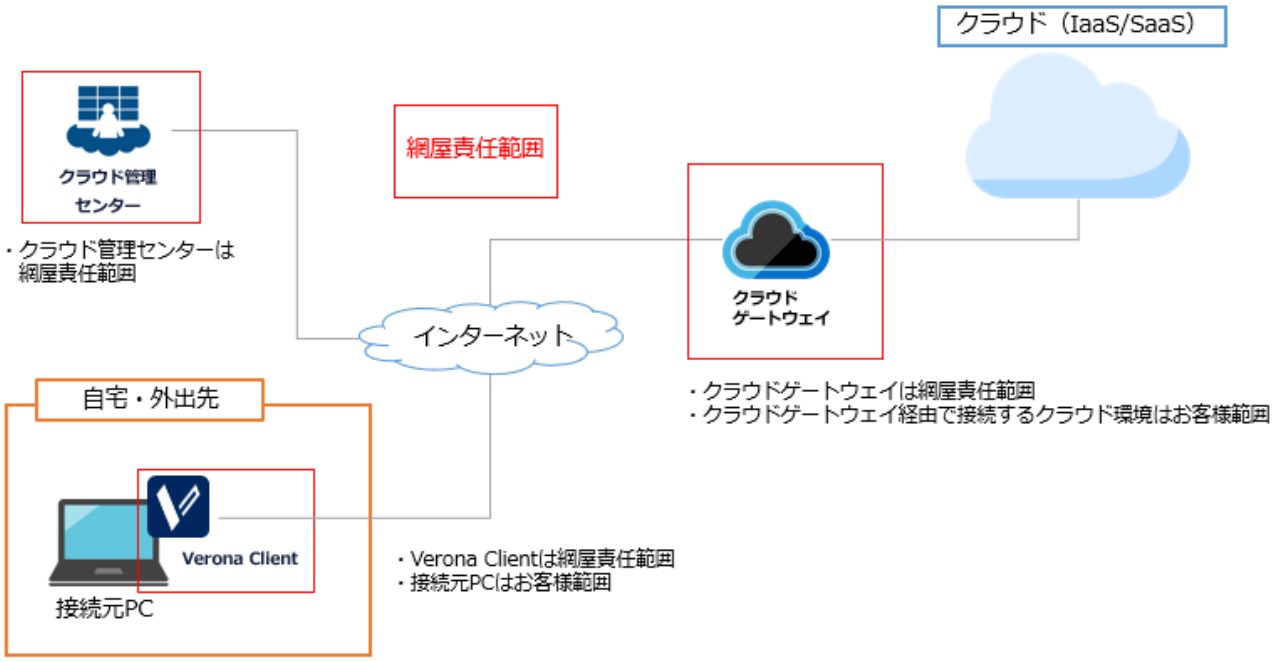
1-1-3 クラウドゲートウェイ

1-1-3A クラウドゲートウェイの管理責任は、弊社にあるものとします。

1-1-3B クラウドゲートウェイ経由で接続するクラウド環境の管理責任は、
お客様にあるものとします。

1-1-3C Verona Client の管理責任は、弊社にあるものとします。
これをインストールした接続元 PC の管理責任は、お客様にあるものとします。

1-1-3D クラウドゲートウェイに接続するインターネット回線の管理責任は、お客様にあるものとします。



## 1-2. Hypersonix の責任範囲

1-2A V-sonic(無線 AP)及び V-Switch(スイッチ) （ハードウェア及びソフトウェアで構成されるもの）

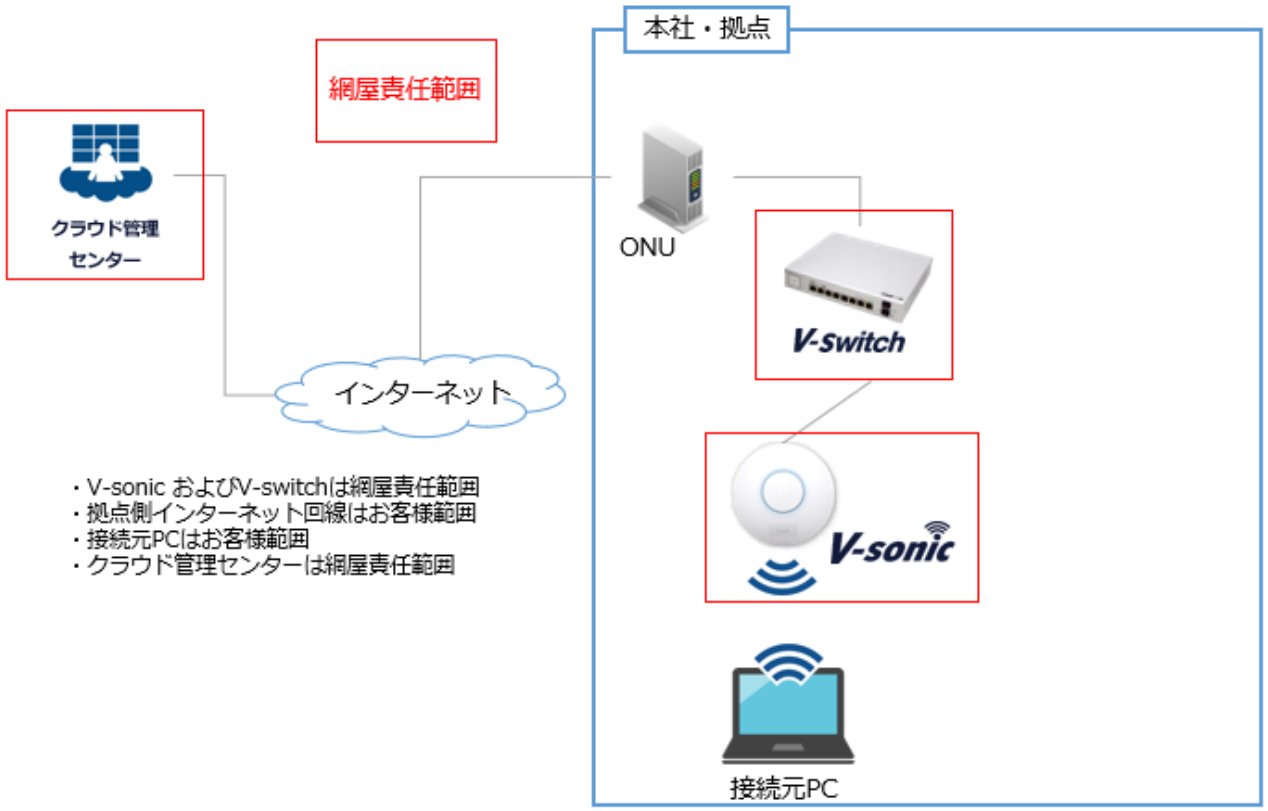
・V-sonic(無線 AP)及び V-Switch(スイッチ)の 物理的なハードウェアの保管・維持を含む管理責任は、買取品・レンタル品に限らず、お客様にあるものとします。

・V-sonic 及び V-Switch 内のソフトウェアについては、買取品・レンタル品に限らず

弊社責任範囲になります。

1-2B 接続元 PC の管理責任は、お客様にあるものとします。

1-2C 拠点側インターネット回線については、お客様にて管理をお願いいたします。

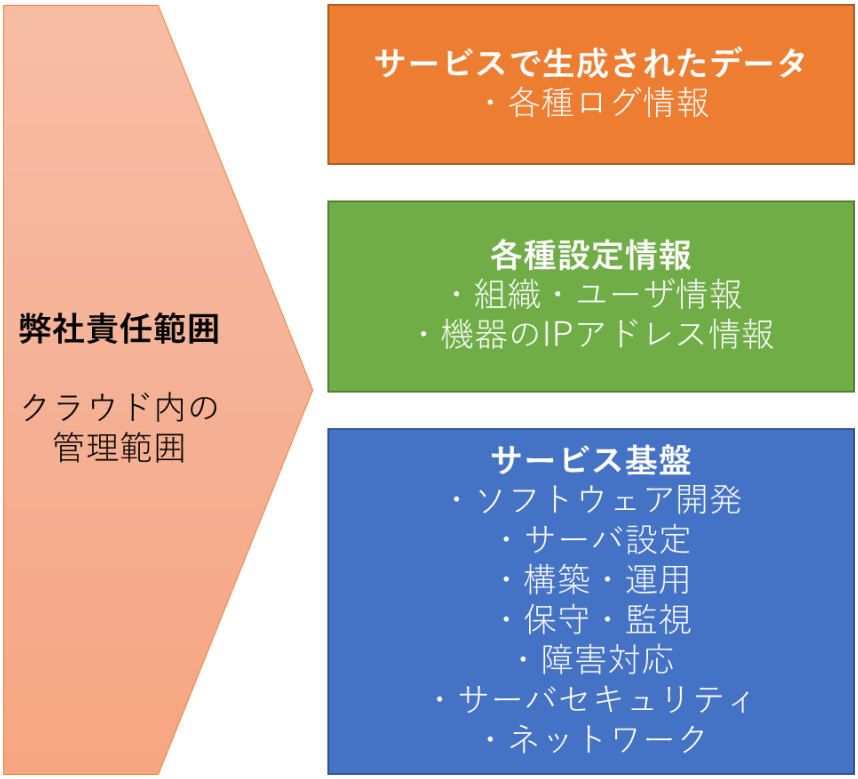


## 1-3. クラウド管理センターの責任範囲

クラウド管理センターにおけるサービス基盤部分・各種設定情報・サービスで生成されたデータの管理責任は弊社にあるものとします。

クラウド管理センター本体に関しては、原則としてお客様で制御できる箇所はなく、その機器等（クラウド管理センター配下の VPN 装置、無線アクセスポイント等）における設定変更及びユーザ情報の変更は、お客様からの依頼を受けて弊社にて実施いたします。ただし、これらの変更の一部をお客様側で実施することも可能です。

※クラウド管理センターにアクセスするためのパスワードの適切な管理(二段階認証で利用するデバイス含む)は、お客様にて責任をもって実施いただけますようお願いいたします。



# 2. 情報セキュリティのための方針群

（以下の「項番」は、本ガイドラインの項目に対応する ISO27017 の規格の項目番号を意味しています。）

## 2-1. 情報セキュリティのための方針群

（項番：5.1.1）

Verona 及び Hypersonix では、弊社の情報セキュリティ基本方針に従い、セキュリティに関する極めて重要な事項として取り扱い、サービス運営を実施します。

詳細は、弊社のセキュリティポリシー(https://www.amiya.co.jp/corporate/security_policy.html)をご確認ください。

# 3. 情報セキュリティのための組織

## 3-1. 情報セキュリティの役割及び責任

（項番：6.1.1）

弊社は、各サービスに関する約款及びサービス仕様書にて契約条件及びサービス内容を定義した上で、各サービスを提供しております。

Verona 及び Hypersonix は SaaS 型のクラウドサービスであり、アプリケーション、設備などサービス基盤の運用は弊社の責任範囲としてサービスの提供範囲に含まれております。

## 3-2.　関係当局との連絡

(項番：6.1.3)

弊社の本社所在地は、東京都中央区日本橋浜町 3-3-2 トルナーレ日本橋浜町 11F です。
なお、クラウドセキュリティサービスに関するお問い合わせ窓口は各サービス仕様書に記載しております。

お客様からお預かりしたデータは、下記に示すクラウドプロバイダーのデータセンターに保管されます。

| サービス名 | 機能名 | データ保管場所 |
|---|---|---|
| Verona | クラウド管理センター | AWS(日本国内) |
| Hypersonix | クラウド管理センター(ハイセキュア) | AWS(日本国内) |
| Hypersonix | クラウド管理センター(スタンダード) | AWS(日本国内) |
| Hypersonix | クラウド管理センター(ベーシック) | GCP(ヨーロッパ) |

## 3-2. 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

(項番：CLD.6.3.1)

約款やサービス仕様書にてサービス内容を定義し、サービス提供を実施しております。
また、責任分界点の詳細は、本ガイドラインの“1. お客様との責任分界点”をご参照ください。

# 4. 資産の管理

## 4-1. クラウドサービスカスタマの資産の除去

(項番：CLD.8.1.5)

サービス解約の際、弊社サービス設備にて保有するデータの除去に関しては、各サービス仕様書をご参照ください。

## 4-2. 情報のラベル付け

(項番：8.2.2)

ご契約いただきましたサービスは、クラウド管理センター内のオーナーコードにて、お客様ごとの識別及び利用サービスを分類しております。（お客様にそのラベル機能は公開しておりません。）

# 5. 利用者アクセスの管理

## 5-1. 利用者登録及び登録削除

(項番：9.2.1)

契約時にご提供いただく申請書を元に、クラウド管理センターへのアカウントを登録します。
アカウントの削除についても、申請書を元にアカウント削除をいたします。

## 5-2. 利用者アクセスの提供

(項番：9.2.2)

クラウド管理センターにてお客様専用管理画面が提供されます。専用管理画面にて確認できる項目は、各サービス仕様書に記載しております。

## 5-3. 特権的アクセス権の管理

(項番：9.2.3)

■Verona

クラウド管理センターの利用にあたって、ID とパスワードの認証に加え、端末証明書による制限を加えております。

■Hypersonix

クラウド管理センターの利用にあたって、多要素認証があるモデルについては、そのための機能を公開しております。

## 5-4. 利用者の秘密認証情報の管理

(項番：9.2.4)

クラウド管理センターを利用される際のアカウントの登録やパスワード変更、再発行方法については弊社が指定する申請書を元に実施します。

### 5-5. 特権的なユーティリティプログラムの使用

(項番：9.4.4)

■Verona

クラウド管理センターにてお客様テナント内の Verona Client 証明書の有効化と無効化が可能です。
これにより、特定のユーザや端末の VPN 接続をお客様が制御できます。

## 6. 暗号

### 6-1. 暗号による管理策の利用方針

(項番：10.1.1)

通信は暗号化プロトコルを使用しています。暗号化していない通信プロトコルは、独自に暗号化し、通信をしています。

## 7. 運用セキュリティ

### 7-1. 変更管理

(項番：12.1.2)

弊社にて本サービスの内容を変更する場合、影響のあるお客様に対し変更内容をクラウド管理センターへ掲載し、かつ、お客様の運用管理担当者様宛にメールにてご連絡しております。

## 7-2. 情報のバックアップ

(項番：12.3.1)

本サービスに何らかの問題が発生した場合の復旧を目的としたバックアップを実施し、遠隔地にて保存しておりますが、お客様にて保存データを直接的にバックアップする機能は付帯していません。

■Verona

本サービスの復旧を目的としたバックアップについては、一日に複数回、複数世代で取得しております。 また、データ復旧手順の作成と復旧試験の実施を行っております。

■Hypersonix

本サービスの復旧を目的としたバックアップについては、日次で取得しております。 また、データ復旧手順の作成と復旧試験の実施を行っております。

## 7-3. クロックの同期

(項番：12.4.4)

弊社では、NTP による時刻同期の仕組みを有しており、日本時間(JST)で管理しています。

## 7-4. 技術的ぜい弱性の管理

(項番：12.6.1)

弊社では、弊社では本サービスに関連する製品（機器・ソフトウェア）について定期的にぜい弱性情報を収集し、ぜい弱性への対応を行います。また、自社で定期的に当該製品のぜい弱性検査を実施しています。

# 8. システムの取得、開発及び保守

## 8-1. 情報セキュリティ要求事項の分析及び仕様化

(項番：14.1.1)

本ガイドライン及び各サービス仕様書に定めております。

### 8-2. セキュリティに配慮した開発のための方針

(項番：14.2.1)

本ガイドライン及び各サービス仕様書に定めております。

## 9. 供給関係者

### 9-1. 供給関係者のための情報セキュリティ方針

(項番：15.1.1)

お客様から事前にご了承をいただいている場合を除き、弊社運用担当者がお客様の情報にアクセスすることはありません。(障害対応で必要となる場合は、この限りではありませんが、その場合でも情報へのアクセスは最低限とするように努めます。)

### 9-2. 供給者との合意におけるセキュリティの取り扱い

(項番：15.1.2)

Verona 及び Hypersonix は SaaS 型のクラウドサービスです。責任分界点の詳細は、本ガイドラインの“1. お客様との責任分界点”を参照ください。

## 10. 情報セキュリティインシンデントの管理

### 10-1. 責任及び手順

(項番：16.1.1)

弊社の責任範囲である契約者情報やお客様に影響のあるサービス運営上の派生データ等に関する情報セキュリティインシデントが発生した場合には、クラウド管理センターへ掲載、及びお客様の運用管理担当者様宛にメールにてご報告いたします。

### 10-2. 証拠の収集

（項番：16.1.7）

お客様責任範囲における情報セキュリティインシデントに関するログ等の証拠の収集は、お客様にて実施いただく範囲となります。弊社責任範囲でのログ等の証拠が必要な場合は、お客様の要望に応じて個別に対応しております。都度、ご相談ください。

## 11. 法令及び契約上の要求事項の順守

### 11-1. 記録の保護

（項番：18.1.3）

ログデータを含む利用者データは、不正なアクセスや改ざんを防ぐため、弊社の各サービス開発及び運用チームの一部の人間しかアクセスできないよう設定されたアクセス権のもとで保管されます。

■Verona

ログは 3 ヶ月間クラウド管理センター内に保管され、以後アーカイブに保管されます。

■Hypersonix

ログは 1 ヶ月間クラウド管理センター内に保管されます。

### 11-2. 暗号化機能に対する規則

（項番：18.1.5）

クラウド管理センターでは SSL/TLS の暗号化を使用しております。なお、輸出規制の対象となる暗号化の利用はありません。

## 11-3. 情報セキュリティの独立したレビュー

（項番：18.2.1）

弊社では、お客様が大切な情報を安心してお取り扱いいただけるよう、クラウドサービス事業者として情報セキュリティ対策に積極的に取り組み、それらの情報セキュリティ活動については、定期的に内部監査によるレビューを実施しております。なお、レビュー結果情報の開示については、セキュリティ保持の観点から特定の契約条件及び法令順守等の開示要求についてのみ開示されます。

また、弊社では、情報セキュリティマネジメントシステム（ISMS）の国際規格である ISO/IEC27001:2013(JIS Q27001:2014)を取得しております。

以上