

ニフクラ

# セキュリティホワイトペーパー

富士通クラウドテクノロジーズ株式会社

2021 年 12 月 8 日（第 30 版）

## 1. 目次

|                                   |    |
|-----------------------------------|----|
| 1. 目次 .....                       | 2  |
| 2. はじめに .....                     | 5  |
| 3. クラウドサービスとは .....               | 6  |
| 3.1. クラウドサービスの仕組み .....           | 6  |
| 4. クラウドにおけるセキュリティの考え方 .....       | 7  |
| 4.1. クラウドセキュリティの基本的な考え方 .....     | 7  |
| 4.2. ニフクラにおけるセキュリティの基本的な考え方 ..... | 8  |
| 5. ニフクラサービスにおけるセキュリティ対策 .....     | 9  |
| 5.1. 概要 .....                     | 9  |
| 5.2. 物理的設備・装置 .....               | 10 |
| 5.2.1. データセンター・オフィス環境 .....       | 10 |
| 5.2.2. 物理的装置 .....                | 11 |
| 5.3. サービス構成 .....                 | 11 |
| 5.3.1. 概要 .....                   | 11 |
| 5.3.2. 機密性 .....                  | 11 |
| 5.3.3. 完全性 .....                  | 11 |
| 5.3.4. 可用性 .....                  | 12 |
| 5.4. サービス管理 .....                 | 12 |
| 5.4.1. サービスの運用体制 .....            | 12 |
| 5.4.2. サービスの継続的な開発及び提供 .....      | 13 |
| 5.4.3. システムライフサイクル .....          | 14 |
| 5.4.4. ネットワーク管理 .....             | 14 |
| 5.4.5. 監視の実施 .....                | 14 |
| 5.4.6. キャパシティ管理 .....             | 15 |
| 5.4.7. インシデント管理 .....             | 15 |
| 5.4.8. 端末管理 .....                 | 15 |
| 5.4.9. 供給者関係 .....                | 16 |
| 5.4.10. 顧客データの取扱記録の保管 .....       | 16 |
| 5.5. その他 .....                    | 16 |

|        |                                 |    |
|--------|---------------------------------|----|
| 5.5.1. | 規約・SLA/SLO .....                | 16 |
| 5.5.2. | 法制度 .....                       | 17 |
| 5.5.3. | コンプライアンス.....                   | 17 |
| 5.5.4. | 利用契約終了後の措置.....                 | 18 |
| 5.5.5. | EU 一般データ保護規則への対応 .....          | 18 |
| 6.     | ニフクラユーザーのためのセキュリティ関連機能.....     | 18 |
| 6.1.   | ニフクラへのアクセス・運用管理.....            | 19 |
| 6.1.1. | ログイン画面 .....                    | 19 |
| 6.1.2. | IP 許可制限 .....                   | 19 |
| 6.1.3. | マルチアカウント.....                   | 19 |
| 6.1.4. | アクティビティログ .....                 | 19 |
| 6.1.5. | ファイアウォールのログ .....               | 19 |
| 6.1.6. | 時刻の管理 .....                     | 19 |
| 6.2.   | サーバー.....                       | 20 |
| 6.2.1. | SSH キー接続 .....                  | 20 |
| 6.2.2. | 自動フェイルオーバー(HA 機能) .....         | 20 |
| 6.2.3. | SSL 証明書 .....                   | 20 |
| 6.2.4. | IDS.....                        | 20 |
| 6.3.   | バックアップ .....                    | 20 |
| 6.3.1. | バックアップ .....                    | 20 |
| 6.3.2. | カスタマイズイメージ.....                 | 20 |
| 6.3.3. | ワンデイスナップショット.....               | 21 |
| 6.4.   | ネットワーク.....                     | 21 |
| 6.4.1. | ファイアウォール.....                   | 21 |
| 6.4.2. | ロードバランサー .....                  | 21 |
| 6.4.3. | プライベート LAN .....                | 21 |
| 6.4.4. | ダイレクトポート（専用線・閉域網 接続サービス） .....  | 21 |
| 6.4.5. | プライベートアクセス（閉域網 集線型接続サービス） ..... | 22 |
| 6.4.6. | プライベートブリッジ.....                 | 22 |
| 6.4.7. | VPN ゲートウェイ .....                | 22 |
| 6.4.8. | リモートアクセス VPN ゲートウェイ .....       | 22 |

|   |    |
|---|----|
| 6.4.9. インターネット VPN (H/W) .....  | 22 |
| 6.5. 監視.....  | 22 |
| 6.5.1. 基本監視.....  | 22 |
| 6.5.2. パフォーマンスチャート .....  | 22 |
| 6.5.3. 有人監視.....  | 23 |
| 6.6. サードパーティのセキュリティ関連サービス .....   | 23 |
| 6.6.1. WAF (Scutum) .....   | 23 |
| 6.6.2. WAF (攻撃遮断くん).....  | 23 |
| 6.6.3. サーバー向けクラウド型セキュリティ (Trend Micro Cloud One –<br>Workload Security) ..... | 23 |
| 6.6.4. ウイルス・スパイウェア対策 (ESET File Security for ニフクラ) .....                      | 24 |
| 6.6.5. Web 改ざん検知 (GRED セキュリティサービス) .....                                      | 24 |
| 6.6.6. クラウド型バックアップサービス (Acronis Backup Cloud for ニフクラ)<br>ラ) 24               |    |
| 6.6.7. 脆弱性診断サービス Powered by イエラエセキュリティ .....                                  | 24 |
| 6.6.8. 統合ネットワークサービス (IPCOM VE2 シリーズ) .....                                    | 25 |
| 6.7. メンテナンス及び各種通知 .....   | 25 |
| 6.7.1. 通知について .....   | 25 |
| 6.7.2. メンテナンスについて .....   | 25 |
| 6.7.3. 障害・お知らせ通知 .....  | 25 |
| 7. 附属 A : ISO/IEC 27001 Annex A との関連について .....                                | 26 |
| 8. 附属 B : E U 一般データ保護規則との関連について .....   | 27 |
| 9. 参考文献 .....   | 28 |
| 10. 更新履歴 .....  | 30 |

## 2. はじめに

ニフクラは、柔軟なコンピューティング資源をオンデマンドで利用できるクラウドサービスです。クラウドサービスでは、必要な時に必要なだけコンピューティング資源を利用することにより、ビジネスにおけるIT活用のスピード効率を向上することができます。一方で、従来のオンプレミスのフルカスタマイズが前提な利用形態と異なり、クラウドサービスのように定型化されたサービスを利用する際には、個々のクラウドサービスの特徴を踏まえたセキュリティ対策の実践が必要になります。

「ニフクラセキュリティホワイトペーパー」（以下「本ドキュメント」といいます）、ユーザーのクラウドサービス選定及び、利用時のセキュリティ対策実装のための補助的な情報として、ニフクラにおいて実施されているセキュリティ対策について紹介します。さらに、ニフクラのユーザーが利用できるセキュリティ関連機能についても紹介します。ニフクラを利用した安全なシステムの構築運用時の参考として活用ください、なお、個別の機能の仕様についてはニフクラのHP(<https://pfs.nifcloud.com/>)を参照してください。

1. 本ドキュメントは、富士通クラウドテクノロジーズ株式会社（以下「富士通クラウドテクノロジーズ」といいます）が情報提供のみを目的として作成したものです。
2. 本ドキュメントは、本ドキュメントを作成した時点における富士通クラウドテクノロジーズの見解を反映したものです。本ドキュメントの内容は事前の予告なく変更されることがあります。
3. 本ドキュメントのいかなる内容も、富士通クラウドテクノロジーズの保証、表明、義務、確約等を意味するものではなく、本ドキュメントの内容の正確性、特定の目的への適合性を含め、富士通クラウドテクノロジーズは、本ドキュメントに関するいかなる保証も行いません。また、富士通クラウドテクノロジーズは、本ドキュメントの利用により生じたいかなる状況についても、その理由の如何を問わず、一切の責任を負いません。
4. 富士通クラウドテクノロジーズとニフクラのユーザーとの間の契約条件は、「ニフクラサービス利用規約<sup>1</sup>」等に定めるとおりであり、本ドキュメントはその一部とはなりません。また、本ドキュメントによって当該契約条件が変更されることもありません。
5. 本ドキュメントの内容の全部又は一部を無断転載することを禁じます。
6. 本ドキュメントに掲載されている会社名、製品名などは、それぞれ各社の商標、登録商標、製品名です。

<sup>1</sup> <https://pfs.nifcloud.com/term/>

## 対象範囲について

本ドキュメントでは、仮想サーバー、ストレージ、ファイアウォールなどのインフラ（IaaS）、また RDB、DNS などのエンジニアリングパーツ（PaaS）について、富士通クラウドテクノロジーズ自らが仕組みを提供するサービスの範囲を対象にしています。

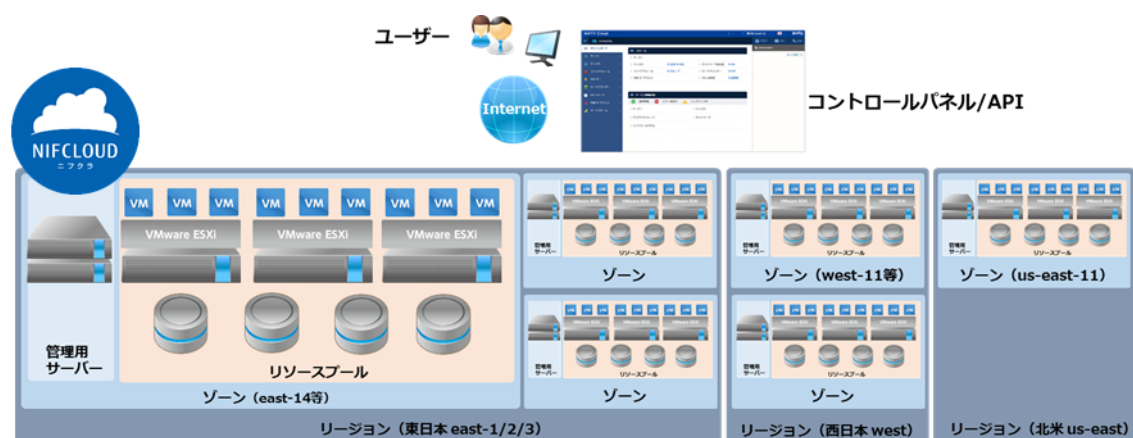
## 3. クラウドサービスとは

### 3.1. クラウドサービスの仕組み

パブリック型クラウドコンピューティングには一般的に以下のような特徴があります。

- ネットワークを経由したアクセス
- 利用量に応じた課金
- マルチテナントでリソース共有
- オンデマンド・セルフサービス
- 弾力性と伸縮性

これら特徴の実現のためには、仮想化に代表される数多くの技術・パラダイムが活用されています。また、継続的なクラウドサービスの提供のために、先進的な技術・パラダイムを積極的に取り入れ、頻繁にサービス内容の追加・変更・終了が行われていることも注目するべき点と言えます。



ユーザーは、ニフクラのコントロールパネルや API などのインターフェースを通じてクラウドサービスの利用を行います。作成したサーバーや増設ディスクなどのストレージにどのようなデータを保管するかは、ユーザーが選択して実行することができます。

## 4. クラウドにおけるセキュリティの考え方

### 4.1. クラウドセキュリティの基本的な考え方

クラウドセキュリティには2つの側面があります。1つはサービスの提供者がクラウドサービスの提供のためにどのようなセキュリティ対策を実施しているか、もう1つはユーザーがクラウドサービス上でどのようなセキュリティ対策を実施するか、ということです。これらはクラウドサービスの提供者、ユーザーそれぞれで完結しているかのように見えますが、実際は相互に影響しています。まず、クラウドサービスのユーザーにとって必要なセキュリティ対策は、サービスの提供者がどのようなセキュリティを実行しているかに大きく影響されます。例えば、ユーザーがどれほどユーザーリソースに対して堅固なセキュリティを実装したとしても、サービスの提供者が管理するデータセンターのセキュリティが不全でインシデントが頻発するような状況では、ユーザーのシステムがセキュアに運用されているとは言えません。逆もまた同様に、サービスの提供者のセキュリティが厳しく管理されていたとしても、ユーザーが適切な対策を実施しなければ、ユーザーのセキュリティを担保することは難しいでしょう。

さらに、特にクラウドサービス提供者がマルチテナントのクラウドサービスを提供する場合、サービスレベルを全てのユーザーに対して維持するためには、ユーザー環境が相互に深刻な影響を与えないような仕組み作りが必要です。それには技術的な環境の隔離だけではなく、規約等による制限も含まれます。ユーザーはクラウドサービスの利用に際して、どのようなことができるのかを利用規約などから把握する必要があります。

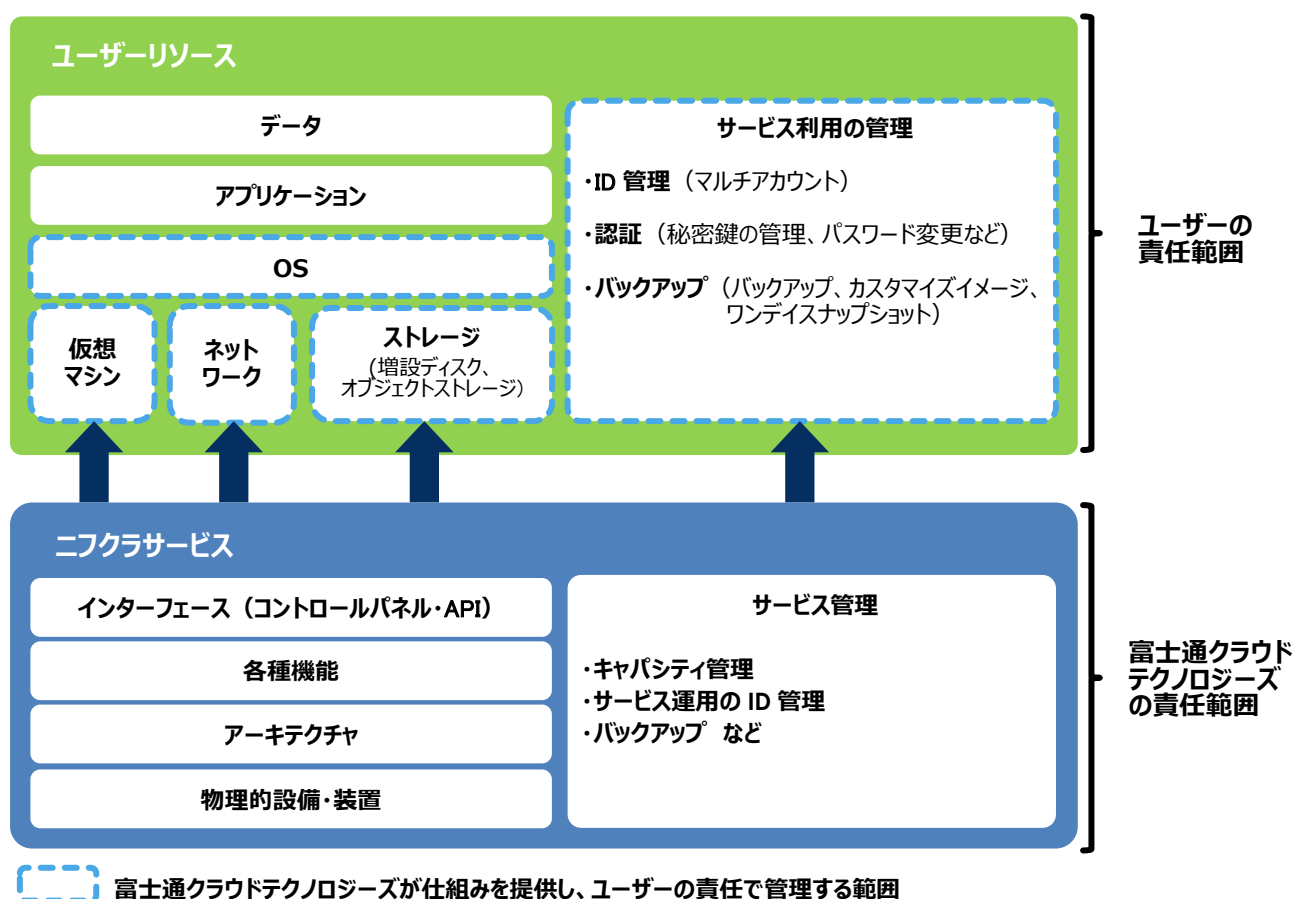
このような互いのセキュリティ対策の適切な実施のために、相互で役割と責任の理解の上、セキュリティ対策の実践が必要であるという考え方は「共同責任モデル (Shared Responsible Model)」と呼ばれます。詳しくは経済産業省の「クラウドサー

ビス利用のための情報セキュリティマネジメントガイドライン」及び「クラウドセキュリティガイドライン活用ガイドブック」にて解説されています。

本章では、共同責任モデルに基づいたニフクラでの富士通クラウドテクノロジーズとユーザーの役割と責任について解説し、富士通クラウドテクノロジーズにおけるセキュリティ対策の概要を紹介します。

## 4.2. ニフクラにおけるセキュリティの基本的な考え方

ニフクラは、仮想化されたコンピューティングリソース及び、コンポーネントをサービスとして「コントロールパネル及び API」(以下、「**インターフェース**」と表記)を通じて提供し、「ニフクラをサービスとして構成するための物理的設備からインターフェースまでのコンポーネント及び関連するサービス運用プロセス」(以下「**ニフクラサービス**」と表記)の提供について責任を有しています。



ユーザーがインターフェースを通じて作成したサーバーやその中にインストールしたアプリケーション、保管したデータなどの「リソース及びコンポーネント」(以下、



「**ユーザーリソース**」と表記)は、ユーザーが任意に変更・削除できます。ニフクラの利用についてはユーザーの責任となります。ユーザーリソースは、ユーザーの責任によって管理することができます。富士通クラウドテクノロジーズは、ユーザーリソースを等しく情報として扱い、その内容、特性等については関知していません。なお、ユーザーリソースと外部の間の通信（以下、「**外部通信**」と表記）につきましても、同様に富士通クラウドテクノロジーズでは内容、特性等について関知いたしません。が、ニフクラサービス及び、ユーザーリソースのセキュリティ確保の観点から、ニフクラサービス及び、ユーザーリソースに対して攻撃的通信が行われているか否かを推測するために、外部通信の内容を確認することがあります。ニフクラの利用にあたっては、ユーザーによるリスクアセスメントを踏まえ、本ドキュメントを参考に必要な対策を検討し、実施してください。

## 5. ニフクラサービスにおけるセキュリティ対策

### 5.1. 概要

本項では、富士通クラウドテクノロジーズがニフクラの継続的なサービス提供にあたり、実施しているセキュリティに関する情報を述べています。富士通クラウドテクノロジーズは、ウイルスからサイバーテロまで様々な脅威を考慮したデータセンター設備を構築するとともに、サービス提供機器のセキュリティ対策や監視強化について継続的な投資を行っております。また、情報セキュリティマネジメントシステム (ISMS) の規格である、「ISO/IEC 27001:2013,JIS Q 27001:2014」<sup>2</sup>や

「ISO/IEC27017 に基づく ISMS クラウドセキュリティ認証」<sup>3</sup>の第三者評価認証制度による認証の取得等、外部の客観的なチェック機構も積極的に活用しております。富士通グループとして、情報セキュリティマネジメントを適切に行うために必要なセキュリティポリシーを公開しています。<sup>4</sup>

ニフクラでは多層的にニフクラサービス及び、ユーザーリソースの保護を行っております。本ドキュメントで述べている内容は、ニフクラで実施しているセキュリティ対策の一部を紹介しています。参考として**「附属 A : ISO/IEC 27001 Annex A との関連**

---

<sup>2</sup> <https://fjct.fujitsu.com/about/safety/isms/index.html>

<sup>3</sup> <https://fjct.fujitsu.com/about/safety/isms-cloud/index.html>

<sup>4</sup> <https://www.fujitsu.com/jp/about/csr/security/>

について"において ISMS における箇条に対する本ドキュメントの対応内容のポイントを示しています。詳細な情報をご希望の場合にはニフクラの導入相談窓口<sup>5</sup>へお問い合わせください。ただし、お問い合わせの内容によっては、開示をお断りする場合があります。あらかじめご了承ください。

## 5.2. 物理的設備・装置

### 5.2.1. データセンター・オフィス環境

ニフクラのデータセンターは、火災、落雷、水害、地震、その他災害の影響を極力避けた立地のデータセンター専用建物を利用しており、それらの災害及び、障害に対しては発生時の被害最小化のための対策を実施しています。また、データセンターは建築基準法に準拠した建物であり、耐震性、耐火性を備えています。

敷地内への不法侵入、破壊行為などの人為的災害については、柵、フェンス、監視カメラなど複数の手段によって侵入防止と監視を実施しています。サーバールームは独立した無窓の部屋であり、外部からの容易な侵入ができません。回線設備は専用の設備にあり、専用の錠によって施錠されています。

電源は2回線以上から引き込み、停電時でも継続して稼働できるよう、自家発電設備及び、UPSを冗長構成で備えています。また、機器への引き込みは専用分電盤から供給し、その他のデータセンターの設備系からは独立しています。

サーバールームの空調は専用となり、温度、湿度は自動制御の上、24時間365日の監視を実施しています。その他、電源・空調・防災・防犯など設備類は24時間365日集中監視を行っています。

障害や事故、災害時に備えて責任者や役割、対応手順等をまとめたマニュアル類を策定しています。また、障害、事故、災害の事象や原因を記録し、根本原因を分析した結果を再発防止策に役立てています。定期的に事業継続訓練や防災訓練を実施しています。データセンター及び、本社では、入退館、指定エリアへの入退室が可能な従業員を限定しており、厳格な本人認証の上、持ち込み品の制限、記録の取得などの入退室管理を行っています。

---

<sup>5</sup> <https://pfs.nifcloud.com/inquiry/>

### 5.2.2. 物理的装置

ニフクラは、システムを構成するサーバー、ストレージ、ネットワーク等の機器を適切に管理しています。ニフクラを構成する機器は、障害や事故、災害時に備えて、迅速に事業継続ができるよう必要な予備、冗長化構成を整備しています。ストレージ機器については RAID6 相当の冗長化を行っています。また、構成管理を定められた方法にて適切に実施しています。機器に対して予防の計画を策定し、定期的実施しています。必要に応じて適切な保守を実施しています。

機器の移動、廃棄の場合には、円滑、確実かつ安全に実施するため、不正防止、機密保護対策を含めた計画、手順を策定しています。

## 5.3. サービス構成

### 5.3.1. 概要

ニフクラはユーザーリソースの機密性、完全性、可用性を意識した設計及び、サービス提供を行っています。

### 5.3.2. 機密性

ユーザーとの契約に関する情報など特に重要なデータについては、ニフクラを構成するシステム内に保持していません。ユーザーリソースへの機密性については、ユーザーにより適切な対策を行ってください。

ユーザーの、サービス利用中のユーザーリソースの削除、もしくはサービス利用解除の際には、ニフクラサービス及び、それを構成する機器等からデータの漏洩が生じないように防止策が講じられています。

サービスインターフェースに対しては不正アクセス等の対策を実施しています。

### 5.3.3. 完全性

ニフクラは、ユーザーリソースについてデータ保護を実施し、厳重な管理を行っています。ニフクラは、コンピュータウイルス等の不正プログラムによる被害を防ぐため、開発及び、運用で使用する機器について、ウイルスチェック・脆弱性チェックなどのセキュリティ対策を実施しています。インシデントが発生した場合は、定められた手順に従い、報告、調査、駆除、再発防止を実施しています。

ユーザーリソースへの完全性については、ユーザーにより適切な対策を行ってください。

#### 5.3.4. 可用性

ニフクラではユーザーリソースとサービス管理のための領域を、ネットワークを含め分離しています。リージョン内では、リソースプールを完全に独立したいくつかのまとまりに分割し、ゾーンとして提供することで障害時の影響範囲を限定しています。また、それぞれのユーザーリソースも、ネットワークを含め分離する機能を提供しています。

ニフクラは、障害が発生した場合に、ユーザーリソースを自動的に復旧する機能を有しています。また、その他障害発生時の回復についても手順を定めています。ユーザーリソースの OS、アプリケーション、データについてはユーザーにより適切な監視及び、インシデント管理を行ってください。

データセンター及び、本社では事故・災害時に備えて責任者や役割、対応手順等をまとめたマニュアル類を策定しています。また、大規模な事故・災害を想定した訓練も実施しています。

ユーザーリソースへの可用性については、ユーザーにより適切な対策を行ってください。また、ユーザーリソースへアクセスするためのネットワークもシステムのセキュリティ要件に合わせて選択及び、利用してください。

### 5.4. サービス管理

#### 5.4.1. サービスの運用体制

ニフクラでは、サービス提供に携わる要員に対して、スキルの把握を実施し、能力と責任に応じた育成を実施しています。その中には、順守すべきセキュリティルールや最新のセキュリティ動向／対策等を反映した教育等も含まれます。

また、ニフクラサービスを始めとした情報システムを利用する従業者を限定し、権限の設定を行っています。アカウント管理（発行、削除、棚卸し等）、パスワード管理及び、これに関連するルールの策定を実施しています。さらに、情報システムにアクセスした各種ログを一定期間保存し、不正防止やインシデント発生を防止しています。社内ルールに基づいた情報システムの操作、運用管理等をまとめた文書類の策定、保管、見直しを行っています。また、マニュアル類のバックアップを取得しています。

富士通クラウドテクノロジーズでは、ファイルのコピーや盗難等を防ぐために、保存先のアクセス制限やパスワードによる認証を実装しています。認可されていないデータのコピーや盗難等を防ぐために、情報資産を重要度に応じて分類し、ストレージや通信の暗号化も含めて適切に管理しています。また、本社内で使用している LAN 及び本社と DC と結ぶ回線は暗号化することで盗聴による漏洩防止策が実装されています。情報または情報通信の保護に暗号化を用いる場合は、CRYPTREC 暗号リストに準じた強度の暗号技術を用いています。

ニフクラの運用管理時には、緊急対応で社外・在宅で対応を行う場合も含め専用線接続もしくは VPN 接続による機密性を保持した通信を行っています。

ニフクラは、ユーザーが個別にクラウド上に保存している情報資産の分類、ラベル付け等の管理機能は提供していません。ユーザーは、自身の責任で情報資産を分類、ラベル付け等を実施して、後述の「6. ニフクラユーザーのためのセキュリティ関連機能」を活用して適切な情報管理・漏洩対策を実施してください。

#### **5.4.2. サービスの継続的な開発及び提供**

ニフクラは、中長期のロードマップに基づいたシステム開発を行っています。立案したシステム開発計画は、責任者による確認と承認を行っています。

ニフクラでは、本番システムのセキュリティを維持するため、複数段階の環境を整備しています。セキュリティ管理の方針、及び、実装や運用で考慮すべき要件を定め、設計段階から品質を確保するためのプロセスを実施しています。システム開発に際しては、仕様書に基づいた開発とテストを行い、標準化や自動化にも取り組んでいます。テスト工程では検証環境と稼働環境との整合性やウイルスチェック、脆弱性チェックなどの結果を検証し、問題がないことを確認しています。

ニフクラサービスなどの情報システムへの変更については、変更管理プロセスに則って変更作業を実施しています。また、定型的变化作業については、作業手順書を整備しています。機能変更時の品質を確保するために、変更機能に加えて既存機能のリグレッションテストを実施し、影響度の検証、障害の有無を検証しています。

ニフクラは、定常運用におけるオペレーションや監視、チェック機能について、実施者は必ず複数名で多面的にチェックを行うのはもちろん、プログラムによる自動化を含めて品質確保に取り組んでいます。

サービスのリリース及び、エンハンスに関わる情報は、関連部門に事前共有した上で適切な手順で実施しています。

#### 5.4.3. システムライフサイクル

ニフクラではシステムの導入に際しては、機能もしくは性能に関する評価を経た上で実施する体制を取っています。また、サポート契約、ベンダーとのリレーションシップ、バージョン管理を含むシステムの運用管理を実施しています。

システムの廃棄の際には、円滑、確実かつ安全に実施するため、運用及び、責任者の承認を得て不正防止、機密保護対策を含めた計画、手順を策定しています。

#### 5.4.4. ネットワーク管理

ニフクラでは目的ごとにネットワーク領域を分離し、運用しています。ネットワークセキュリティ方針に従い、ネットワークの設定は物理と仮想において整合性を保っています。ニフクラのサービス管理のためのネットワークはユーザーのサービス利用のものとは分離しています。また、必要な通信のみを許可し、ウイルス対策ソフトや不正アクセス検知装置、迷惑メールフィルタ等の技術的な対策を実装しています。

また、ニフクラにおいてはサーバー間のプライベート通信はユーザー共用のネットワークを利用しています。ユーザーは「6.3. ネットワーク」を参考に、ユーザーリソースへのネットワークについて適切な手段を選択し、ファイアウォールなどを利用してグローバル及びプライベートのネットワークに対して適切な保護を実施してください。

#### 5.4.5. 監視の実施

ニフクラは、ニフクラサービスにおける各機器（物理サーバー、ネットワーク、ストレージ）、システムの性能・リソース・API などについて、監視を実施しています。ニフクラは、異常を迅速に検知・通知する監視機能を実装しています。また、データセンターの死活監視を行い、複数のリージョン及び、ゾーンを運用することなどにより、サービスの継続性を維持する取り組みを行っています。

ニフクラは、ニフクラサービス全体に対する監視を実施しており、ユーザー個別のユーザーリソースの監視は実施していません。ユーザーは「6.4. 監視」を参考に、ユーザーリソースに対する適切な監視及び、対応を実施してください。



#### 5.4.6. キャパシティ管理

ニフクラは、システムの性能及び、キャパシティ管理のプロセスを定め、文書を策定し、それに基づいて実施しております。その中には監視対象、監視内容、監視方法が含まれ、管理表等のドキュメントを策定し、運用しています。また、監視から得られた情報や過去の動向などを基にして、コンピューティング資源の増強のためのプロセスを定め、監視により得られた情報などを基に随時増強を実施することで、ユーザーリソースのためのコンピューティング資源の枯渇を未然に防ぎ、ユーザーがオンデマンドでユーザーリソースを作成・管理できるように継続的に取り組んでいます。

#### 5.4.7. インシデント管理

ニフクラでは、ニフクラサービスに対する監視や、JPCERT 等の外部機関からの情報提供に基づき、イベント管理を行っています。インシデントの発生時には、手順に基づき関係者への情報伝達を行い、対処にあたっています。また、ユーザーリソースに影響がある可能性があるインシデント、あるいはデータ侵害の可能性のあるインシデントの発生時には、メール等の手段により通知を行っています。通知はニフクラサービスにおけるサービス障害のほか、ユーザーが禁止事項に抵触した際の、ニフクラ側での対応結果も含まれます。

お客様がご利用中のサーバー、ディスク、ネットワークにおいてニフクラの SLA 判定基準に該当する障害発生を富士通クラウドテクノロジーズが確認してから 60 分以内の通知を目標とします。

障害の告知方法は、「障害・お知らせ通知」<sup>6</sup>にてお知らせしています。

また、ニフクラでは過去の障害情報を蓄積、分析することにより、障害の再発防止に継続的に努めています。

#### 5.4.8. 端末管理

ニフクラは、コンピュータウイルス等の不正プログラムによる被害を防ぐため、開発／運用で使用する機器について、ウイルス対策、脆弱性チェックを含んだセキュリティ対策を実施しています。特に、悪意のあるコードを検知した場合の対応手順は明確化及び、ルール化しているため、これに従って報告、調査、駆除、再発防止を実施

---

<sup>6</sup> <https://pfs.nifcloud.com/service/notice.htm>

しています。さらに、本社の PC（社外持ち出し PC を含む）はハードディスクを暗号化しています。

#### 5.4.9. 供給者関係

システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲等を明確にしています。また、外部委託先の選定に際しては手続きを明確にし、委託業者を客観的に評価しています。委託業者の決定にあたっては、責任者の承認を得て行うのはもちろん、安全性確保のため、機密保護、安全運行等に関する項目を盛り込んだ委託契約を締結しています。

ニフクラは、機能、性能、サポート等に関する評価をした上でシステムを導入する体制を構築しています。他システムとの整合性など結合テストを含めて確認しています。

システムの開発や運用等で外部委託先を選定する場合、目的や要求事項、業務範囲等をまとめたプロセスを明確にしています。取り扱う情報や委託業務等を考慮し、外部委託先の選定を行っています。また、作業拠点の情報セキュリティ監査を実施しています。選定した外部委託先には、情報漏洩等を防ぐための安全管理処置の内容を義務づけた契約を締結しています。

#### 5.4.10. 顧客データの取扱記録の保管

ニフクラは処理者として GDPR に準拠するため、管理者または処理者に代わり行った顧客データの取扱い記録を保管します。

### 5.5. その他

#### 5.5.1. 規約・SLA/SLO

ニフクラを利用するためには、ニフクラ基本利用規約<sup>7</sup>ならびにニフクラサービス利用規約<sup>8</sup>への同意が必要となります。

また、ニフクラは品質保証制度（SLA）<sup>9</sup>を提供しています。SLA 対象サービスの月間稼働率が、規定の稼働率に満たなかった場合、当社は当該ユーザーの有償オプションサービス料金を除く当月分の利用料金の 10%に相当する金額を翌々月以降、ニフクラ

---

<sup>7</sup> <https://customer.nifcloud.com/terms/>

<sup>8</sup> <https://pfs.nifcloud.com/term/>

<sup>9</sup> <https://pfs.nifcloud.com/sla/>



ご利用料金から減額いたします。減額対応にあたりましては、当社 SLA 窓口への申請が必要となります。なお、定義した SLA を達成するためにサービスレベル目標（SLO）<sup>10</sup>を設定しています。制度及び手続きにつきましては、以下をご確認ください。

### 5.5.2. 法制度

ニフクラはニフクラ基本利用規約において、準拠法を日本法とし、専属的合意管轄裁判所を東京地方裁判所としています。

外国為替及び外国貿易法、米国輸出管理規則等の安全保障輸出管理に関する法令、個人情報保護法、GDPR、不正アクセス禁止法等の情報セキュリティに関する法令、暗号及び暗号化機能を含めた技術に関する外国為替及び外国貿易法ならびに米国輸出管理規則（Export Administration Regulations）などの安全保障に関する法令、規範及びガイドラインを順守し運営しています。当社はクラウドサービスに係る法規制について特定し「当社が順守するクラウド関連法規一覧」として順守しております。

また、ニフクラは各リージョンが置かれた各種法令を順守し運営しています。お客様がニフクラに保管したデータについても同様に各リージョンが置かれた地域の法令等の順守が求められ、ユーザー自身での管理が必要となります。ニフクラにおいては、ユーザーのデータは等しく情報として扱い、内容については検知していません。捜査当局や裁判所などの機関からの開示要求については、富士通クラウドテクノロジーズにおいて定められた手順により判断を行っております。また、ニフクラでは、ユーザー自身の操作によるものを除き、ユーザーのデータを他のリージョンへ移転していません。

### 5.5.3. コンプライアンス

当社は富士通グループの社員一人一人の行動規範として定められた「The FUJITSU Way」に沿ってコンプライアンス遵守の取り組みを継続して推進しています。また、内部監査を実施するためのルールを策定しており、年に1回、ニフクラを含めた情報システムを対象に、内部監査を実施して予防・是正に取り組んでいます。ニフクラが取得又は受領している第三者認証は以下の通りです。

- ISO/IEC 27001:2013 (ISMS)
- ISO/IEC27017 (ISMS クラウドセキュリティ認証)

---

<sup>10</sup> <https://pfs.nifcloud.com/slo/>

ニフクラでは、直接の監査要求は受け入れていません。また、ユーザーによる個別の監査要求は受け入れていませんが、インシデント発生時には内部監査を実施し、その結果を開示できるようにしています。ユーザーが監査を受ける際に、ニフクラからの情報提供が必要な場合は、あらかじめ個別にご相談ください。その他、ニフクラでは、公益財団法人「金融情報システムセンター（FISC）」によりまとめられた「金融機関等コンピュータシステムの安全対策基準・解説書（通称：FISC 安全対策基準）」に対して、クラウドサービス事業者として実施済みの対応やお客様自身で必要な対応をまとめたチェックリストを公開しています。

#### 5.5.4. 利用契約終了後の措置

解約その他の事由により利用契約が終了した後、富士通クラウドテクノロジーズは、本サービスの利用により当該ユーザーによってサーバーに格納されたデータの全てを消去します。

#### 5.5.5. EU 一般データ保護規則への対応

EU 一般データ保護規則（以下「GDPR」といいます）とは EU の個人情報保護に関する法律です。お客様が GDPR における管理者または処理者として EU 個人データを取り扱うとき、ニフクラは、処理者として GDPR に準拠したサービスを提供します。本ドキュメントで述べている内容は、ニフクラで実施している GDPR 対応の一部を紹介しています。参考として“附属 B：EU 一般データ保護規則との関連について”において GDPR における条文に対する本ドキュメントの対応内容のポイントを示しています。

## 6. ニフクラユーザーのためのセキュリティ関連機能

本章では、ユーザーがニフクラを活用する際に役立つセキュリティ関連機能・サービスを紹介します。個々の機能・サービスの仕様についてはニフクラの HP<sup>11</sup> を参照してください。

---

<sup>11</sup> <https://pfs.nifcloud.com/service/>

## 6.1. ニフクラへのアクセス・運用管理

### 6.1.1. ログイン画面

ニフクラのコントロールパネルへログインする際には、ニフクラ ID 及び、パスワードが必要です。ニフクラ ID 及び、パスワードはユーザー自身で適切に管理してください。パスワードの変更は契約管理メニューから行うことができます<sup>12</sup>。なお、ニフクラ ID では、第三者による不正なログインを防ぐために、ID/パスワードの認証に加えてソフトウェアトークンによるワンタイム PW 認証を追加して多要素認証にすることが可能です<sup>13</sup>。パスワード入力時にはパスワードが表示されないようにしています。

### 6.1.2. IP 許可制限

IP 許可制限は、コントロールパネルや API へのアクセスについて、特定のホストや IP アドレスからのアクセスのみを許可する機能です。許可した IP アドレス以外からのアクセスを制限します。

### 6.1.3. マルチアカウント

ニフクラをご利用中のお客様が、操作範囲に制限を持たせたアカウントを作成できる機能です。

### 6.1.4. アクティビティログ

過去 6 カ月分のコントロールパネル操作ログをご確認いただけます。  
また、毎月のログファイルを全件、CSV 形式でダウンロードできます。

### 6.1.5. ファイアウォールのログ

ファイアウォールごとに直近 1,000 件、又は 2 週間まで拒否された通信のログを確認いただけます。  
2 週間経過すると、1 日分ごとにログを削除します。ログの保存件数は、100,000 件に変更することができます。

### 6.1.6. 時刻の管理

ネットワーク上で時間同期（NTP）をお客様で実施いただけます。

---

<sup>12</sup> <https://agreement.nifcloud.com/>

<sup>13</sup> <https://customer.nifcloud.com/agreement/password.html>

詳しくは、ニフクラ FAQ「ニフクラ上のサーバーを NTP で管理したい。」<sup>14</sup>を参照ください。

## 6.2. サーバー

### 6.2.1. SSH キー接続

サーバーの作成やログインに必要な SSH キーの管理を、コントロールパネル上で行うことができます。

### 6.2.2. 自動フェイルオーバー(HA 機能)

ニフクラを提供する富士通クラウドテクノロジーズのシステムにおいて、物理サーバーに障害が発生した場合、当該物理サーバー上に展開されていたお客様のサーバーは、自動で別の物理サーバー上に移動します（お客様のサーバーは自動で再起動します）。

### 6.2.3. SSL 証明書

SSL 証明書を作成・管理できる機能です。ニフクラでは、サイバートラスト株式会社、日本ジオトラスト株式会社の SSL 証明書をオプションとしてご用意しています。

### 6.2.4. IDS

ニフクラ上のお客様のサーバーへのさまざまな不正アクセスやサーバーに仕掛けられた悪意のあるプログラム（トロイの木馬、バックドアなど）の発する情報を常時監視し、ファイアウォールで防ぐことのできない攻撃も検知します。

## 6.3. バックアップ

### 6.3.1. バックアップ

ニフクラのサーバーを対象に定期的な自動バックアップや任意のタイミングでバックアップを取得する機能です。トラブル発生時には、取得したバックアップデータから、別サーバーとして新規作成し、バックアップ時の状態で復元させることが可能です。

### 6.3.2. カスタマイズイメージ

カスタマイズイメージは、サーバーを作成する際のテンプレートをイメージ化して保存しておく機能です。

---

<sup>14</sup> [https://pfs.nifcloud.com/cs/catalog/cloud\\_faq/catalog\\_131128001606\\_1.htm](https://pfs.nifcloud.com/cs/catalog/cloud_faq/catalog_131128001606_1.htm)

起動中のサーバーや、ディスクを増設しているサーバーで実行できますので、バックアップ用途として利用できます。

### 6.3.3. ワンデイスナップショット

ワンデイスナップショットは、現時点のサーバー状態を保存する機能です。起動中のサーバー、増設ディスク付きのサーバーでも保存することができ、万一の場合はワンデイスナップショット作成時点への早急な復旧が可能になります。

## 6.4. ネットワーク

### 6.4.1. ファイアウォール

ユーザーのサーバーへの通信を、あらかじめ定義されたルールに従って L3 レベルでフィルタリングする機能です。

サーバーの外でフィルタリングを行うため、複数のサーバーに一括で同じ設定のファイアウォールを適用することができます。

### 6.4.2. ロードバランサー

サーバーの冗長化やトラフィックの負荷分散を実施するための機能です。L4（レイヤー4）に対応した「ロードバランサー（L4）」、プライベートネットワークにも対応した「マルチロードバランサー」、アプリケーション情報をベースに負荷分散を行う「L7 ロードバランサー（Ivanti Virtual Traffic Manager）」、L7 ロードバランサー機能とセキュリティ機能を搭載した「統合ネットワークサービス（IPCOM VE2 シリーズ）」を提供しています。

### 6.4.3. プライベート LAN

共用ネットワークから L2 レベルで隔離されたプライベートネットワークセグメントを利用することができます。

### 6.4.4. ダイレクトポート（専用線・閉域網 接続サービス）

従来インターネットを通して二フクラに転送していたデータを、ユーザーの専用線・閉域網から可能にするためのサービスです。二フクラへダイレクトに接続するためのポートを提供します。

二フクラのプライベート LAN とあわせて利用することで、二フクラをユーザーのプライベート環境と変わらないセキュリティレベルでご利用いただくことが可能になります。

#### 6.4.5. プライベートアクセス（閉域網 集線型接続サービス）

プライベートアクセスは、ニフクラから回線事業者の閉域網へのプライベートな接続を提供するサービスです。ニフクラと回線事業者の閉域網の物理接続を事前に行っているため、論理接続を構築するだけで接続が可能です。

#### 6.4.6. プライベートブリッジ

プライベート LAN 同士を L2 接続するネットワークサービスです。対応リージョン内のプライベート LAN 同士を接続することで、複数のゾーン・リージョンを利用したシステムを簡単に構築できます。

#### 6.4.7. VPN ゲートウェイ

ニフクラ上の自社環境にセキュアに接続可能な、インターネット VPN サービスです。L2/L3 レベルそれぞれでニフクラをユーザーの社内ネットワークの延長線上にあるシステムとしてご利用いただけます。

#### 6.4.8. リモートアクセス VPN ゲートウェイ

ニフクラ上のプライベート LAN に、お客様オフィスネットワークなどからセキュアに接続できるリモートアクセス型の VPN サービスです。お客様の端末に専用アプリケーションをインストールし、SSL による暗号化で安全に接続することができます。

#### 6.4.9. インターネット VPN（H/W）

インターネット VPN（H/W）は、機器設置型（ハードウェアタイプ）の VPN サービスです。ユーザーの社内環境とニフクラをインターネット VPN とプライベート LAN によりセキュアに接続します。本サービスにより、ニフクラをユーザーの社内ネットワークの延長線上にあるシステムとしてご利用いただけます。

### 6.5. 監視

#### 6.5.1. 基本監視

サーバー及び、ロードバランサーの稼働状況・負荷状況の監視を自動で行い、異常が発生した場合には、メールにて通知します。

#### 6.5.2. パフォーマンスチャート

対象項目のパフォーマンスをコントロールパネル上のグラフで確認することができます。

### 6.5.3. 有人監視

ユーザーのニーズに応じたレベルでサーバーの稼働状況を 24 時間 365 日監視します。

異常が発生した場合には、メール又は電話で通知し、必要に応じてニフクラに精通したエンジニアが 1 次対応を行います。

## 6.6. サードパーティのセキュリティ関連サービス

### 6.6.1. WAF (Scutum)

WAF (Web アプリケーションファイアウォール/Scutum) とは、HP 上のアプリケーションに特化したファイアウォール機能を SaaS 型で提供するサービスです。

ユーザーからの入力を受け付けたり、リクエストに応じて動的なページを生成したりするタイプの HP を不正な攻撃から守る役割を果たします。一般的なファイアウォールとは異なり、データの中身をアプリケーションレベルで解析できるのが特徴です。

提供：株式会社セキュアスカイ・テクノロジー

### 6.6.2. WAF (攻撃遮断くん)

WAF (攻撃遮断くん) は、WEB サイト/WEB サーバーへのサイバー攻撃を可視化・遮断するセキュリティサービスです。シグネチャ自動更新により、最新の攻撃へ迅速に対応し、簡単に WEB サイトのセキュリティ対策を実現します。

攻撃遮断くんは、3 つのセキュリティタイプをご用意しており、お客様の用途に応じたタイプをお選びいただけます。

提供：株式会社サイバーセキュリティクラウド

### 6.6.3. サーバー向けクラウド型セキュリティ (Trend Micro Cloud One – Workload Security)

ニフクラ上のサーバーを、トレンドマイクロ社がクラウド上で提供する管理サーバーから集中管理することにより、管理サーバー構築の工数を削減し、迅速に安全性の高いシステムを構築・運用することが可能になります。

提供：トレンドマイクロ株式会社

#### 6.6.4. ウイルス・スパイウェア対策（ESET File Security for ニフクラ）

マルチプラットフォーム対応のウイルス・スパイウェア対策製品です。

Windows サーバー用プログラムと Linux サーバー用プログラムから選択して利用可能です。利用環境に合わせてご導入いただけます。

提供：ESET（国内総販売代理店：キヤノン IT ソリューションズ株式会社）

#### 6.6.5. Web 改ざん検知（GRED セキュリティサービス）

HP の改ざんの有無を定期的にチェックすることで、HP の安全性を確保します。改ざんをいち早く見つけることで、ユーザー保護と再発防止に貢献します。

本サービスは、一般の HP 閲覧と同じように、インターネット側からコンテンツをチェックするため、サーバー側の監視では見つけることができない改ざんも検知が可能です。

また、自社開発したヒューリスティック検知エンジンが、コンテンツの様々な要素を解析するので、多様なパターンの改ざんを検知します。

提供：株式会社セキュアブレイン

#### 6.6.6. クラウド型バックアップサービス（Acronis Backup Cloud for ニフクラ）

クラウド型バックアップサービス（Acronis Backup Cloud for ニフクラ）は、ニフクラでご利用いただいているサーバーやお客様のオンプレミス環境にある物理/仮想サーバー、クライアント PC/MacOS を含めたシステム（ディスク）をまるごとバックアップ・復元します

提供：アクロニス・ジャパン株式会社

#### 6.6.7. 脆弱性診断サービス Powered by イエラエセキュリティ

脆弱性診断サービス Powered by イエラエセキュリティは、セキュリティ診断のプロフェッショナルカンパニーである株式会社イエラエセキュリティのセキュリティエンジニアが、お客様のアプリケーションやシステムの脆弱性診断を実施するサービスです。

ニフクラ上に構築されたお客様のアプリケーションやシステム、ネットワークの脆弱性診断が可能です。

提供：株式会社イエラエセキュリティ



#### 6.6.8. 統合ネットワークサービス（IPCOM VE2 シリーズ）

統合ネットワークサービス（IPCOM VE2 シリーズ）は、富士通が提供する仮想アプライアンスソフトウェア「FUJITSU Network IPCOM VE2 シリーズ」を利用したサービスです。長年に渡り企業のネットワーク基盤を支えてきた同製品がニフクラ基盤に対応し、ニフクラ上の仮想マシンに対して高度なネットワーク機能を提供します。これによりお客様は、クラウドシステムへ求められる多くの機能を一元的に管理し活用することにより、セキュリティ対策や可用性向上の課題を解決することが可能です。

提供：富士通株式会社

### 6.7. メンテナンス及び各種通知

#### 6.7.1. 通知について

ニフクラでは、ユーザー向けの情報として、メンテナンス・障害情報などのお知らせをお送りしています。その他、新サービスの提供、仕様変更などについては、ニフクラの HP やメールなどを通じて連絡しています。

#### 6.7.2. メンテナンスについて

メンテナンスの情報は、コントロールパネル内のお知らせ欄に掲載します。掲載時期は、メンテナンス実施の約 2 週間前を目安としています。定期メンテナンスは、毎月第 3 木曜日 午前 8 時～10 時に行います。なお、定期メンテナンスについては、お客様への事前告知を行いません。定期メンテナンス中は、コントロールパネルと API をご利用いただけない場合があります。お客様のサーバーは通常通りご利用いただけます。緊急メンテナンスの場合は、上記の限りではありません。

#### 6.7.3. 障害・お知らせ通知

障害・お知らせ通知は、ニフクラで障害が発生した際、経過や復旧情報などをメールにてご連絡するサービスとなります。また、メンテナンスなどのお知らせが発生した際も、同様にメールにてご連絡します。

## 7. 附属 A : ISO/IEC 27001 Annex A との関連について

それぞれの管理策を網羅しているものではありません。ニフクラでは ISMS に基づいた情報セキュリティマネジメントの実施にあたり、リスクアセスメントの結果を考慮し必要な対策を実践しています。

| ISO/IEC 27001 管理策 |                 | 本ドキュメントにおける箇所   |
|-------------------|-----------------|---|
| A.5               | 情報セキュリティのための方針群 | 5.1   |
| A.6               | 情報セキュリティのための組織  | 5.4.2<br>5.4.7  |
| A.7               | 人的資源のセキュリティ     | 5.4.1   |
| A.8               | 資産の管理           | 5.4.1<br>5.4.3  |
| A.9               | アクセス制御          | 5.3.1<br>5.3.2<br>5.3.3<br>5.3.4<br>5.4.1<br>5.4.5<br>5.5.2 |
| A.10              | 暗号による管理策        | 5.4.1<br>5.4.8  |
| A.11              | 装置              | 5.2.1<br>5.2.2<br>5.3.2<br>5.3.3<br>5.3.4<br>5.4.3          |
| A.12              | 運用のセキュリティ       | 5.3.2<br>5.3.3<br>5.3.4<br>5.4.1<br>5.4.2<br>5.4.3          |

|      |                           |   |
|------|---------------------------|---|
|      |                           | 5.4.4<br>5.4.5<br>5.4.6<br>5.4.8<br>5.5.3                   |
| A.13 | 通信のセキュリティ                 | 5.3.4<br>5.4.4<br>5.4.9                                     |
| A.14 | システムの取得、開発及び保守            | 5.4.2<br>5.4.3<br>5.4.4<br>5.4.9                            |
| A.15 | 供給者関係                     | 5.4.9   |
| A.16 | 情報セキュリティインシデント管理          | 5.2.1<br>5.2.2<br>5.3.3<br>5.3.4<br>5.4.7<br>5.4.8          |
| A.17 | 事業継続マネジメントにおける情報セキュリティの側面 | 5.2.1<br>5.2.2<br>5.3.4<br>5.4.2<br>5.4.7                   |
| A.18 | 順守                        | 5.2.1<br>5.4.3<br>5.4.9<br>5.5.1<br>5.5.2<br>5.5.3<br>5.5.4 |

## 8. 附属 B : E U 一般データ保護規則との関連について

それぞれの GDPR 要件を網羅しているものではありません。

ニフクラは GDPR の条文のうちクラウドサービスとしての責務を分析し、必要な対策を実践しています。本ドキュメントではそのうちセキュリティ対策に関する部分を記載しています。

| GDPR条文            |                                       | 本ドキュメントにおける箇所   |
|-------------------|---------------------------------------|---|
| 第28条3項(c)         | 技術的および組織的対策                           | 5.3.1<br>5.3.2<br>5.3.3<br>5.3.4<br>5.4.1<br>5.4.8<br>5.5.3 |
| 第28条3項(e),(f),(h) | 管理者の義務を果たすことの支援<br>(管理者の義務を果たすための可用性) | 5.3.4   |
| 第28条3項(g)         | 個人データの消去                              | 5.3.2   |
| 第30条              | 取扱い活動の記録                              | 5.4.10  |
| 第32条              | 技術的および組織的対策                           | 5.3.1<br>5.3.2<br>5.3.3<br>5.3.4<br>5.4.1<br>5.4.8<br>5.5.3 |
| 第33条2項,3項,4項      | インシデント通知                              | 5.4.7<br>6.4.3  |

## 9. 参考文献

1. 経済産業省. クラウドセキュリティガイドライン改訂版. (オンライン) 2013 年.  
<http://warp.da.ndl.go.jp/info:ndljp/pid/8618025/www.meti.go.jp/press/2013/03/20140314004/20140314004.html>

2. 経済産業省. クラウドサービス利用のための情報セキュリティマネジメントガイド  
ライン改訂版. (オンライン) 2013 年.

[http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents\\_000146.html](http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000146.html)

3. International Organization for Standardization(ISO). ISO/IEC 27017:2015. (オンライン) 2015 年.

<https://www.iso.org/standard/43757.html>

4. EU 一般データ保護規則(General Data Protection Regulation).

<https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en>

## 10. 更新履歴

| 版数     | 日付         | 変更内容  |
|--------|------------|---|
| 初版     | 2012/5/8   | 初版作成  |
| 第 2 版  | 2012/6/12  | 更新<br>・ 1.ニフクラのセキュリティ概要のログの記述をマルチアカウントの内容に修正<br>・ VPN の記述を変更                      |
| 第 3 版  | 2012/8/8   | 更新<br>・ 基本監視の記述を変更  |
| 第 4 版  | 2012/9/19  | 更新<br>・ v1.10/11 のエンハンス更新内容を反映  |
| 第 5 版  | 2013/2/7   | 更新<br>・ 不要な記述を削除 (CentOS サポート)  |
| 第 6 版  | 2013/2/19  | 更新<br>・ 1. ニフクラのセキュリティ概要 - データセンターに、西日本データセンターの記述を追記。                             |
| 第 7 版  | 2013/3/19  | 更新<br>・ 機能追加の内容を反映 (L7 ロードバランサー、Web アプリケーションファイアウォール)<br>・ v1.12/13 のエンハンス更新内容を反映 |
| 第 8 版  | 2013/5/30  | 更新<br>・ 不要な記述を削除  |
| 第 9 版  | 2013/8/6   | 更新<br>・ v1.15 のエンハンス更新内容を反映   |
| 第 10 版 | 2013/10/4  | 更新<br>・ SOC2 Type1 の取得内容を追記。  |
| 第 11 版 | 2013/11/19 | 更新  |

|        |            |   |
|--------|------------|---|
|        |            | ・ v1.16 のエンハンス更新内容を反映   |
| 第 12 版 | 2014/01/31 | 更新<br>・ Windows2012 対応を反映   |
| 第 13 版 | 2014/05/08 | 更新<br>・ 誤記を修正（ファイアウォールのプロトコル名）                                    |
| 第 14 版 | 2014/11/19 | 更新<br>・ v1.19 のエンハンス更新内容を反映                                       |
| 第 15 版 | 2015/02/02 | 更新<br>・ データセンターの説明を最新化  |
| 第 16 版 | 2015/05/08 | 更新<br>・ ファイアウォール機能の説明を最新化<br>・ VPN サービスの説明を最新化                    |
| 第 17 版 | 2015/09/16 | 更新<br>・ 北米リージョンを追記  |
| 第 18 版 | 2015/10/28 | 更新<br>・ サーバーログ管理ソフト（VVAULT AUDIT） 追記<br>・ サーバー監視サービス（Mackerel） 追記 |
| 第 19 版 | 2016/2/24  | 更新<br>・ IEC/ISO 27001 に沿った内容にリニューアル                               |
| 第 20 版 | 2016/06/10 | 更新<br>・ 7. 附属 A : ISO/IEC 27001 Annex A との関連について、<br>表中の項番を修正     |
| 第 21 版 | 2017/5/9   | 更新<br>・ 社名変更  |
| 第 22 版 | 2018/3/13  | 更新<br>・ 本ドキュメントの適用範囲に PaaS も含むよう修正<br>・ セキュリティ機能実装に伴う修正           |

|        |            |  |
|--------|------------|--|
|        |            | <ul style="list-style-type: none"> <li>・ 6.1.5 アクティビティログ、 6.1.6 ファイアウォールログに関する事項を追記</li> <li>・ そのほか、表記ゆれや文言の統一を実施</li> </ul>   |
| 第 23 版 | 2018/05/25 | 更新 <ul style="list-style-type: none"> <li>・ EU 一般データ保護規則について追記</li> </ul>  |
| 第 24 版 | 2019/4/10  | 更新 <ul style="list-style-type: none"> <li>・ 5.5.1 規約・SLA に SLO について追記</li> <li>・ 5.5.3 コンプライアンスに富士通グループとしての内部統制体制の整備の取り組みと FISC について追記</li> <li>・ 6.ニフクラユーザーのためのセキュリティ関連機能を最新の内容に更新</li> </ul> |
| 第 25 版 | 2019/7/23  | 更新 <ul style="list-style-type: none"> <li>・ 提供終了サービスの記載を削除</li> </ul>  |
| 第 26 版 | 2019/10/1  | 更新 <ul style="list-style-type: none"> <li>・ 基幹システムの切り替えに伴い、表記を修正</li> </ul>  |
| 第 27 版 | 2020/1/15  | 更新 <ul style="list-style-type: none"> <li>・ 6.4.6. プライベートブリッジを追加</li> </ul>  |
| 第 28 版 | 2020/6/1   | 更新 <ul style="list-style-type: none"> <li>・ サーバー向けクラウド型セキュリティ（Trend Micro Deep Security as a Service）の名称を変更</li> <li>・ 5.4.1. サービスの運用体制を修正</li> <li>・ 6.1.1. ログイン画面に多要素認証についての表記を追記</li> </ul> |
| 第 29 版 | 2021/3/15  | 更新 <ul style="list-style-type: none"> <li>・ 5.4.1.サービスの運用体制に情報または情報通信の保護に用いる暗号化の技術、およびニフクラユーザー自身によるクラウド上の情報資産の分類、ラベル付けについて追記</li> <li>・ 5.5.2.法制度に、準拠法及び各種法令の順守について追</li> </ul>                |



|        |           |   |
|--------|-----------|---|
|        |           | 記<br>・ 5.5.3.コンプライアンスに監査に関する対応について追<br>記                    |
| 第 30 版 | 2021/12/8 | 更新<br>・ ニフクラユーザーのためのセキュリティ関連機能を最<br>新の内容に更新<br>・ 一部文章の表現を修正 |