Enterprise Cloud
セキュリティホワイトペーパー
Ver 1.7

2021 年 3 月 19 日

NTT コミュニケーションズ株式会社

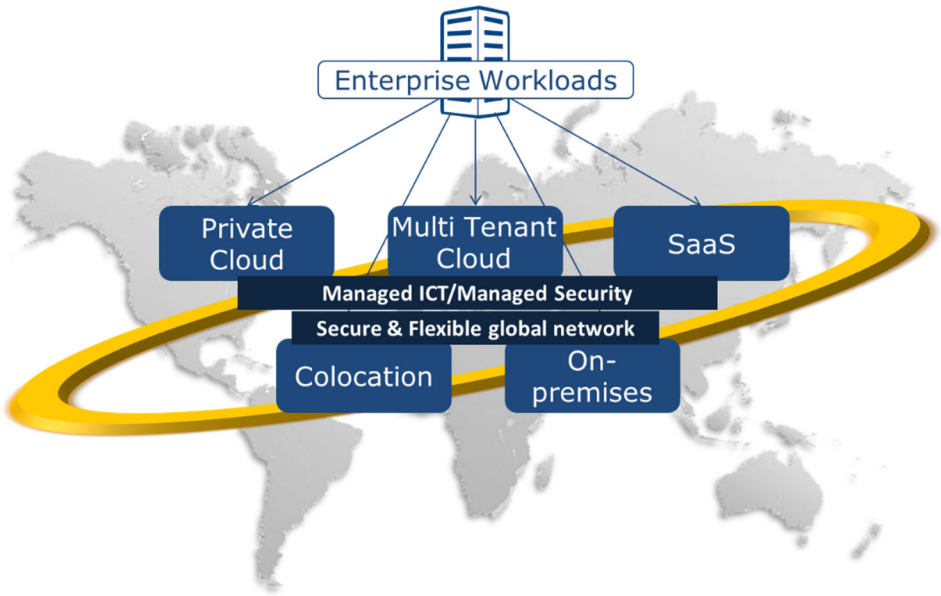
目次

1.Enterprise Cloud とは

エヌ・ティ・ティ・コミュニケーションズ株式会社（以下、「当社」といいます。）が提供する、Enterprise Cloud サービス（以下、「本サービス」「ECL」または「ECL サービス」といいます。）は、基幹システムに求められる「堅牢性」「安全性」にも、デジタルビジネスの展開に必要な「俊敏性」「柔軟性」にも対応可能なハイブリッドクラウドです。

特に、当社は、世界トップクラスの高速で安全なグローバルネットワークと、グローバルで高い評価を受けるデータセンターサービス（Nexcenter）を全世界で提供しており、データセンターとネットワークと一体化された本サービスを利用することで、災害にも強く、セキュアで高信頼な ICT 基盤をグローバルに構築することが可能です。

また、お客さまの複雑化した ICT 環境のガバナンス強化や、リソースやコストを統一的に可視化することにより、お客さまの運用業務の負担軽減を実現します。



2.本資料の目的

Enterprise Cloud セキュリティホワイトペーパー（以下、「本書」といいます。）は、本サービス基盤において、当社が取り組んでいる情報セキュリティ対策等について記載したものです。

クラウドサービスは多くのお客さまがご利用されるシステムであるため、当社がセキュリティについてどのような対策を行っているかをご紹介し、本サービスの導入にあたりお客さまに安心してご利用いただけることを目的としています。

ただし、本書は Enterprise Cloud 2.0(以下、「ECL2.0」といいます。) について記述するものであり、Enterprise Cloud 1.0 (以下、「ECL1.0」といいます。) は対象ではありません。

3.取り組み内容

■　外部認証等の取得について

ECL2.0 は、ISO27001、ISO27017、ISO20000 の認証の取得、および、SOC1、PCI DSS に準拠しています。

最新情報につきましては、Knowledge Center をご覧ください。

https://ecl.ntt.com/certificate/

取得している認証等についての概要は以下の通りです。

認証名	説明
ISO27001 (ISMS)	情報セキュリティマネジメントシステムの国際規格。 情報資産の保護、利害関係者からの信頼を獲得するための ”セキュリティ体制の確保”を目的に、基準となるべき手順を体系的に整理するもの。
ISO27017 (ISMS クラウドセキュリティ)	ISO27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範。 お客さまと ECL2.0 を提供する当社が協調的に連携しながら、それぞれの情報セキュリティマネジメントの目的を達成するための管理策を整理するもの。
ISO20000 (ITSMS)	IT サービスマネジメントの国際規格。 IT サービスの品質の維持/効率性の向上のための管理体制の整備を目的に、基準となるべき手順を体系的に整理するもの。
SOC1	アウトソーシングサービスなどの受託業務にかかわる内部統制が基準に準拠していることを、受託側が委託側に保証する報告書。 各国/地域の監査法人団体が基準を策定。 本サービスは、以下の基準に準拠。 • 「SSAE18」米国保証業務基準 • 「ISAE3402」国際会計士連盟基準
PCI DSS (Payment Card Industry Data Security Standard)	カード会員のクレジットカード情報/取引情報を安全に守るため、 JCB/AMEX/Discover/MasterCard/VISA の 5 社が共同で策定した、クレジット業界におけるグローバルセキュリティ基準。

■　脆弱性の管理について

ECL2.0 サービス基盤の脆弱性管理は、PCI DSS の評価基準を満たした当社の規程に基づくソフトウェア更新の随時実施、脆弱性検査の適宜実施により行っています。また、これらの規程を遵守していることについて、独立した第三者の審査機関による評価を受けています。

■　セキュリティ対策について

ECL2.0 のサービス基盤における主なセキュリティ概要は以下のとおりです。

項目	説明
仮想サーバー	仮想化ソフトウェアによって論理的に分離されています。 情報管理ポリシーなどの理由で、物理サーバーを他のユーザーと共有することを許容できないお客さまには、物理的に分離された専有型のベアメタルサーバーメニューをご用意しています。
ストレージ	管理するソフトウェアの制御により、論理的に分離されています。 なお、他のユーザーの利用による性能への影響を懸念するお客さまには、IOPS 性能確保型のブロックストレージメニューをご用意しています。
ネットワーク	SDN, VLAN 技術などを活用した仮想ネットワークによって論理的に分離されています。 クラウド環境と外部環境を接続するネットワークとして、VPN 接続とインターネット接続のメニューをご用意しています。

■　セキュリティメニューについて

ECL2.0 では、不正アクセスやマルウェア対策など、豊富なセキュリティメニューを提供しています。これらのメニューは、WideAngle※セキュリティメニューの一部を ECL2.0 向けに仕様化したもので、非常に高レベルなマネージドセキュリティサービスです。

※　「WideAngle」とは、当社が提供しているグローバル統一の統合セキュリティサービスブランドです。WideAngle では、グローバルセキュリティオペレーションセンター（GROC）をワールドワイドに展開しており、効率的かつグローバル均一の品質を実現し、リスク分析官の集中配置による高度で最先端の分析を可能としています。また、日本国内最大の ISP であり、国内外のネットワークオペレーションを行う当社ならではのノウハウと、世界トップレベルのセキュリティ研究機関と連携を活かし、お客さまの ICT 環境を防御します。

■　情報セキュリティインシデント発生時のお客さまへの情報提供について

情報セキュリティインシデント発生時のお客さまへの情報提供について、以下のように定めております。なお、データの取り扱いに関する責任については Smart Data Platform サービス利用規約をご参照ください。

当社がお客さまに報告する情報セキュリティインシデントの範囲を以下のように定めます。

・当社責任区間を起因としてお客さまデータの滅失、棄損若しくは漏洩した場合

当社では情報セキュリティインシデントを認定してから 72 時間以内を目標にお客さまに通知することに努めます。お客さまへの通知はメールやポータル掲載など当社が選択した方法で送信されます。ただし、次の場合を除きます。

・通知することにより、他のお客さまへのリスクの増大が考えられる場合

・当社情報セキュリティチーム等によって判断される特殊な場合

情報セキュリティインシデントが発生した場合には、その内容に応じて当社において回復策を実施いたします。またご利用のお客さまに実施いただく必要のある回復策について当社から情報提供をいたします。

4.Q&A

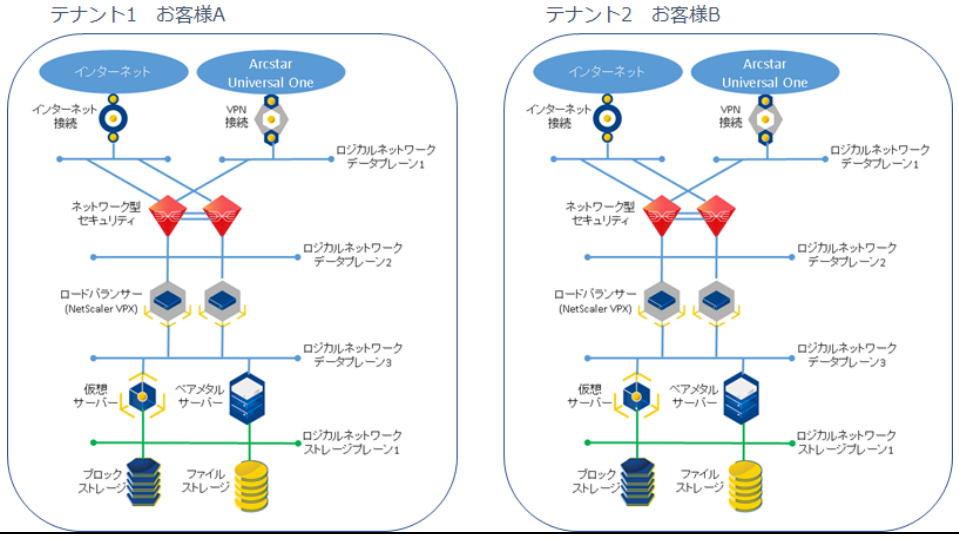
Q&A は下記を参考にしております。

- ENISA(European Network and Information Security Agency：欧州ネットワーク情報セキュリティ庁
- 「クラウドコンピューティング：情報セキュリティ確保のためのフレームワーク(2009 年 11 月版)」
- 総務省「クラウドサービスの安全・信頼性に係る情報開示指針(平成 29 年 3 月版)」
- 経済産業省「クラウドセキュリティガイドライン改訂版(2013 年度版)」

項番	設問	回答
1	IT 監査はどのように実施すればよいですか？	ISO27001、ISO27017、ISO20000 の証書、及び SOC1、PCI DSS の監査レポートを、当社規定の条件に基づき開示可能です。 IT 監査は、お客さまのコンプライアンス担当と監査担当により実施頂く必要がありますが、本サービスの外部認証取得証書及び監査レポートを、お客さま監査担当とのレビューにご利用できます。 最新情報につきましては、Knowledge Center をご覧ください。 https://ecl.ntt.com/certificate/

2	ユーザーデータの保存場所はどこにありますか？	お客さまは、ECL 保管データ（お客さまが ECL 上にアップロード・保管されるデータをいいます）をアップロード・保管するリージョンを自由に選択できます。当社は、お客さまとの契約に基づくお客さまからの明確な指示又は、法令上効力と拘束力のある要請がない限り、ECL 保管データを他のリージョンに移動することは致しません。 本書執筆の時点では、7 か国で提供しています。 （日本、アメリカ、イギリス、ドイツ、シンガポール、香港、オーストラリア） 最新情報につきましては、Knowledge Center をご覧ください。 https://ecl.ntt.com/documents/service-descriptions/region_zone_group/region_zone_group.html#id22

3	データセンター訪問は可能ですか？	ECL2.0 は複数のお客さまにてご利用いただいているため、また、データセンター内のクラウド設備へのアクセスを厳しく制限しているため、お客さまの訪問は受け入れておりません。 このようなお客さまのニーズを満たすために、独立した第三者の審査機関が統制の有無と運用を検証し、SOC1 レポートを発行しています。 ECL2.0 の契約を結んでいる当社のお客さまは、SOC1 レポートのコピーを要求できます。データセンターの物理的なセキュリティについても、 ISO27001、SOC1、PCI DSS の評価基準を満たしていることについて、独立した第三者の審査機関による評価を受けています。
4	第三者がデータセンターに訪問することは可能ですか？	当社は、当社の従業員であっても、データセンターへのアクセスを厳しく統制しています。 また、データセンターにアクセスするには、アクセスポリシーに従って、データセンター管理者による許可が必要です。 データセンターにおけるアクセスの統制については、SOC1 の評価基準を満たしていることについて、独立した第三者の審査機関による評価を受けています。
5	データセンター管理者等の内部者による不適切なアクセスに対処していますか？	当社は内部者による不適切なアクセスの脅威に対処するため、SOC1 の統制基準を遵守しています。また、PCIDSS、ISO27017 の評価基準に従い、内部者によるアクセスに対処しています。 これらが遵守されていることについて、独立した第三者の審査機関による評価を受けています。 統制ルールについては、当社内部でリスク評価を行い、定期的に見直す仕組みがあります。

6	ユーザー間のシステムは適切に分離されていますか？	ユーザーごとのシステム環境については、適切に分離されています。 ISO27017 の評価基準が遵守されていることについて、独立した第三者の審査機関による評価を受けています。 以下は、サービス基盤における主な分離方法の例です。 ■サーバー 仮想サーバーについては、仮想化ソフトウェアによって論理的に分離されています。 情報管理ポリシーなどの理由で、物理サーバーを他のユーザーと共有することを許容できないお客さまには、物理的に分離された専有型のベアメタルサーバーメニューをご用意しています。 ■ストレージ ストレージを管理するソフトウェアの制御により、論理的に分離しています。 なお、他のユーザーの利用による性能への影響を懸念するお客さまには、IOPS 性能確保型のブロックストレージメニューをご用意しています。 ■ネットワーク SDN、VLAN 技術などを活用した仮想ネットワークによって論理的に分離されています。 ECL2.0 上のお客さま環境と外部環境を接続するネットワークとして、VPN 接続とインターネット接続のメニューをご用意しています。 <分離構成イメージ> 

7	各システム（ハイパーバイザー、仮想OS）において既知の脆弱性に対処していますか？また、脆弱性対応など保守のためにサービス停止することがありますか？	ECL2.0 サービス基盤の脆弱性管理については、ISO、SOC、PCI DSS の評価基準を満たした当社の規程に基づくソフトウェア更新の随時実施、脆弱性検査の適宜実施により行っています。 また、これらの規程を遵守していることについて、独立した第三者の審査機関による評価を受けています。ISO27001、ISO27017 の認証取得証書、及び、SOC1、PCI DSS の評価レポートは当社規定の条件に基づき開示が可能です。 なお、脆弱性対策の実施などにより、ECL2.0 サービスおよびお客さま環境の保護のためにサービス停止が必要な場合、サービスを停止することがあります。 仮想サーバー上の OS、ミドルウェアについてはお客さまにて脆弱性対策（ソフトウェアアップデート、パッチ）を実施いただく必要があります。
8	各サービスにおいて暗号化をサポートしていますか？	仮想サーバー上の OS、ミドルウェアについては、お客さま独自の暗号化技術を自由にご利用いただくことが可能です。 バックアップメニューをご契約されたお客さまについては、当社にて暗号化しデータ保存を行っています。暗号化アルゴリズムは電子政府推奨暗号リストに対応したものを用いています。
9	DDoS 攻撃、EDoS 攻撃に対して適切に対処していますか？	ECL2.0 のサービス基盤に DDoS 攻撃対策の仕組みを実装しています。この仕組みは、NTT によるキャリアならではの独自技術を用いたものであり、プロアクティブな DDoS 対策を実施しています。 また、ECL2.0 のネットワークメニューに係る課金体系は、利用時間に応じた月額上限付課金のため、妨害攻撃等により大量のトラフィックが発生したとしても、月額上限以上の料金は発生しません。 お客さま環境への大規模な DDoS 攻撃、EDoS 攻撃などへの対策として、別途有償にて CDN サービスをご提供しています。
10	保存したデータのエクスポートは可能ですか？	お客さまが管理されているデータのエクスポートは可能です。 専用ハイパーバイザーメニューにおいて、他基盤（他クラウドサービスやオンプレミス）に移行する際は、ハイパーバイザー固有のツールや API を利用した移行が可能です。 仮想サーバーイメージのエクスポートは、イメージ化して持ち出す方法や、各種バックアップツールをご利用いただくことが可能です。

11	各サービスで保存されたユーザーデータの冗長性はどのような規定となっていますか？	ユーザーデータについては、ECL2.0 サービス側でマルチサイトにコピーするなどの対応はしておりません。ユーザーデータの冗長性を担保するためには、お客さま側での他サイトへのレプリケーションや定期的なバックアップ実施など、適切なデータ消失対策を実施頂く必要があります。 サービス基盤については可能な限り冗長構成にて構成されています。なお、ベアメタルサーバーメニューなど一部のメニューについては、サービス内容の特性上、冗長構成などはお客さまによる設計を必要とします。
12	犯罪捜査などの法令に従った ECL 保管データの開示要求に対してどのように対処しますか？	当社は、お客さまの情報とプライバシーを保護し、法令上効力と拘束力のある要請がない限り、ECL 保管データを開示いたしません。当局から開示請求があった場合は、法令に違反しない範囲において、開示請求があったことをお客さまに通知致します。
13	データ削除時にデータ削除はどのように実施していますか？ また、データ削除証明書の発行は可能ですか？	ECL 保管データについては、原則お客さまにて削除いただきます。 ただし、サービス解約時においては、自動でデータ削除が行われます。 また当社では、不要になった媒体を安全に破棄するため、保存データを再現できないよう、HDD の消磁やメモリの物理的な破壊を行い、回復不能にしています。この破壊手続きは PCI DSS、ISO27017 を遵守しており、PCI DSS の基準を満たしていることについて、独立した第三者の審査機関による評価を受けています。PCI DSS の評価レポートは当社規定の条件に基づき開示可能です。
14	各サービスの稼働状況は適切に監視されていますか？またそれらは公開されていますか？	サービス基盤の稼働状況は集中監視されています。異常が検知された場合、サービス説明書の記載に従い、お客さまへの通知、Knowledge Center への公開を実施します。 ただし、お客さま環境の個別の仮想サーバーの死活監視などについては、モニタリングサービスのご利用などの方法でお客さまにて実施頂く必要があります。
15	各サービスの提供終了時期	サービスの全体廃止においては、廃止の 180 日前までに当社の規定する通知方法により通知を行います。

	は決まっていますか？	サービスの一部廃止においては、あらかじめ契約者に対してその廃止する機能の代替となる手段または同等の機能を提示できない場合、30 日以上の予告期間をもって、変更後のサービス内容を、通知するものとします。
16	標準のサポートサービスはどのようなものですか？ また、別途有償でのサポートサービスは提供されていますか？	ECL2.0 で提供しているサポート機能は、チケットサポート、Knowledge Center での情報展開、カスタマーポータル上でのリソースステータス表示機能があります。 また有償でのサポートメニューが別途ございます。詳しくは、Knowledge Center のサービス説明書をご覧ください。 https://ecl.ntt.com/documents/service-descriptions/support/support.html
17	最低利用期間はありますか？	ECL2.0 においては、最低利用期間はございません。(2019.11 現在) ただし特約など、お客さま個別の契約条項によるものにおいては、この限りではありません。
18	SLA(品質保証)は定義されていますか？	メニューとして月間利用可能率の SLA を規定しているものについては 99.99%を設定しております。月間利用可能率や各 SLA の詳細については、Knowledge Center をご覧ください。 https://ecl.ntt.com/sla/
19	Noisy neighbor 対策は何かされていますか？（他のユーザー起因によるサービス影響は考慮されていますか？）	Noisy neighbor 対策として、当社の規程に基づき利用上限の設定を実施しております。 また、本サービスに著しい支障を及ぼす、または及ぼす恐れがある行為については、当該ユーザーへの注意喚起、および当該ユーザーの ECL2.0 の利用停止措置を取る場合があります。 なお、他ユーザーの影響を受けないサービスとして、ベアメタルサーバーなどの専有型メニューや、ネットワークメニューの帯域確保型プランがあります。
20	NTT コミュニケーションズは ECL 保管データに対する	ECL 保管データは、お客さまが所有・管理されるものであり、当社は、ECL 保管データのコンテンツを把握することはできず、お客さまとの契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、ECL 保管データにアクセスすることは致しません（契約終了時のデータ消去を除く）。

	権利はありますか？	また、これらのデータが、滅失、毀損、漏洩した場合のお客さまの損害については、エンタープライズクラウドサービス利用規約に記載の通り、いかなる責任も負いかねます。
21	提供サービスの責任分界点はどのようになっていますか？	サービスメニュー毎の提供範囲は、Knowledge Center のサービス説明書に記載しています。 https://ecl.ntt.com/documents/service-descriptions/ 尚、ECL2.0 の各リソースにアクセスするネットワーク等は別途お客さまにて手配いただく必要がございます。お客さま環境など外部環境から ECL2.0 環境へのセキュアな VPN 接続については NTTCom の VPN サービスもご利用が可能です。
22	係争時の管轄裁判所はどこですか？（各リージョンの所属する国が所轄裁判所ですか？）	お客さまが選択したリージョンに関わらず、当社とお客さまとの本サービスに関する係争時の準拠法は日本国法（エンタープライズクラウドサービス利用規約第 42 条に記載。）、管轄裁判所は東京地方裁判所になります（同 41 条に記載。）。
23	ECL は「EU 一般データ保護規則（GDPR）」に対処されていますか？	「EU 一般データ保護規則（GDPR）」への ECL の対応につきましては、Knowledge Center をご覧ください。 https://ecl.ntt.com/security_compliance/gdpr
24	通信経路（アップロード時、ダウンロード時、クラウド間転送）でのデータ漏えいについて、どのよう	ロードバランサーや Managed WAF などのサービスメニューをご利用頂き、お客さまにて適切に設定いただくことなどにより、通信を電子政府推奨暗号リストに対応した暗号化アルゴリズムを用いて暗号化し、盗聴・改ざん・なりすましなどを防止することが可能です。 また、お客さまの行う外部との通信については、お客さまにて暗号化等の対策を実施頂くことが必要です。お客さまにて実施する暗号化の方式等については制限を設けていませんので、個別の要件に対応することが可能です。 なお、遠隔データセンター接続メニューでは、当社が保有する閉域ネットワークを利用しています。

	に対策されていますか？	
25	ユーザーが構築したシステムに対して、脆弱性診断サービスは提供されていますか？ また、ユーザー側でペネトレーションテストの実施について制限はありますか？	別途有償のマネージドセキュリティサービスにて、脆弱性診断サービスを提供しています。 お客さま側でのペネトレーションテストについては、基本的に制限はございませんが、本サービスに著しい支障を及ぼす、または及ぼす恐れがある行為については、当該お客さまへの注意喚起、および本サービスの利用停止措置を取る場合があります。
26	解約違約金など、利用したサービス以外に費用が発生することはありますか？（解約違約金はありますか？）	ECL2.0 では、解約違約金が存在するメニューはありません。(2019.11 現在) ただし特約など、お客さま個別の契約条項によるものにおいては、この限りではありません。
27	クラウドサービス基盤はウイルス対策されていますか？ また、ウイルス対策サービスの提供はありますか？	サービス基盤については、PCIDSS および ISO27017 の評価基準を満たした当社の規程に従って、ウイルス対策が適切に実施されています。この規定が遵守されていることについて、独立した第三者の審査機関による評価を受けています。 ECL2.0 上のお客さま環境については、ISO27017 に準拠したセキュリティメニューを提供しています。こちらをご利用いただくことでウイルス対策を実施できます。 詳細は、Knowledge Center のサービス説明書をご覧ください。 ■Managed UTM

		https://ecl.ntt.com/documents/service-descriptions/network-based_security/menu_utm.html ■Managed WAF https://ecl.ntt.com/documents/service-descriptions/network-based_security/menu_waf.html ■Managed Anti-Virus https://ecl.ntt.com/documents/service-descriptions/host-based_security/menu_av.html ■Managed Host-based Security Package https://ecl.ntt.com/documents/service-descriptions/host-based_security/menu_pk.html
28	ファイルやシステムのバックアップサービスは提供されていますか？	ISO27017 に準拠したバックアップメニューを提供しています。当該基準に準拠していることについて、独立した第三者の審査機関による評価を受けています。 お客さまにて、本メニューで提供するバックアップエージェントを対象サーバーへ導入いただくことで、カスタマーポータルからバックアップのスケジュールや保管期間の設定、並びにファイル/システムのリストアを実行出来ます。 詳細は Knowledge Center のサービス説明書を参照ください。 https://ecl.ntt.com/documents/service-descriptions/backup/backup.html 本メニュー以外にも、お客さま側の個別のバックアップ要件や要望を実現するために、サードパーティ製のバックアップソフトウェアライセンスをミドルウェアメニューとして提供しています。
29	ハイパーバイザーや仮想 OS の操作は、どのようなものがありますか？ ※ウェブブラウザによる管理画面や API など	以下の 3 パターンの方式で操作が可能です。 ■カスタマーポータル(GUI) 直観的な操作により、リソースの操作が可能です。 ■API リソース毎の API エンドポイントを指定することにより、API での操作が可能です。 API リファレンスについては Knowledge Center をご覧ください。 https://ecl.ntt.com/documents/api-references/ ■CLI/SDK

		各リソースをコマンドラインから操作することが可能です。また、 Python SDK での操作が可能です。詳細は Knowledge Center をご覧ください。 https://ecl.ntt.com/documents/tutorials/rsts/ECLC/index.html
30	データセンターの所在地は公開されていますか。	データセンターの詳細な所在地については、公開しておりません。 また、データセンターの建物外部等にデータセンターの所在を表したり、データセンターのご契約社名がわかったりするような表示板や看板等の設置はしておりません。
31	ユーザーの ECL2.0 利用に関する記録はどのように保護されていますか。	お客さまのクラウド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おります。

以上