Enterprise Cloud

セキュリティホワイトペーパー

Ver 1.2

NTT コミュニケーションズ株式会社

Transform your business, transcend expectations with our technologically advanced solutions.

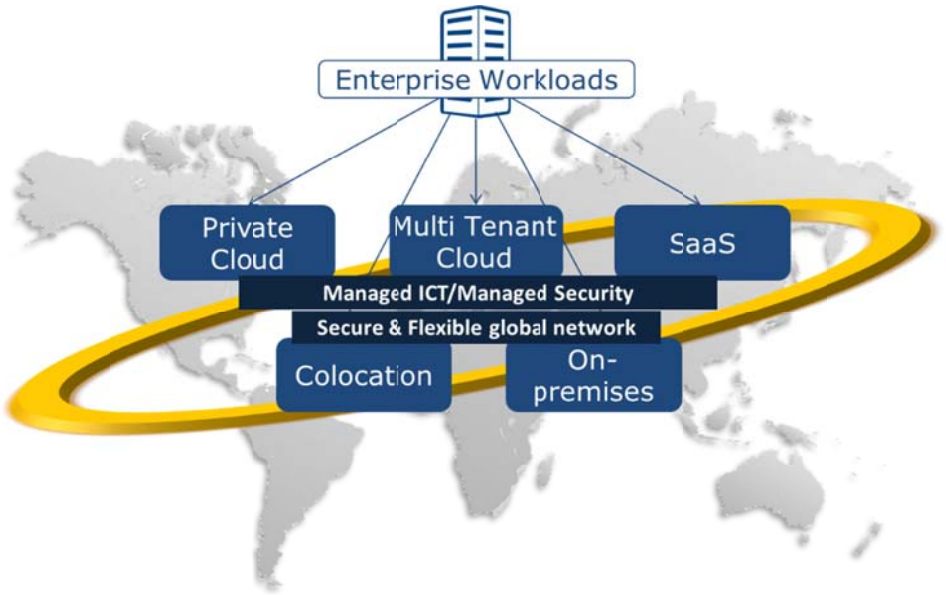
目次

1. Enterprise Cloud とは

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、基幹系システムに求められる「堅牢性」「安全性」と、デジタルビジネスの展開に必要な「俊敏性」「柔軟性」双方のニーズを1つのクラウド基盤で実現可能な、グローバル共通仕様/高品質のクラウドサービスです。

特に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、ネットワーク、データセンター、クラウドコンピューティングをワンストップで契約、保守運用ができ、グローバルに共通な ICT 基盤をスピーディーに構築・運用が可能です。

グローバル共通仕様であるため、セキュリティ・コンプライアンスレベルを統一でき、複雑化する ICT 環境のガバナンス強化や、リソース/コストを一元的に可視化することで ICT 環境の最適化が可能となります。



2. 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、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。）が取り組んでいる、本サービスに関わる情報セキュリティ対策等について記載したものです。ただし、本書は Enterprise Cloud 2.0(以下、「ECL2.0」といいます。)についての記述であり、Enterprise Cloud 1.0 (以下、「ECL1.0」といいます。)は対象としていません。

クラウドコンピューティングは多くのお客様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、本サービス導入にあたりお客様に安心してご利用いただけることを目的としています。

3. 取り組み内容

本サービスは、ISO27001、ISO27017、ISO20000 の認証取得および、SOC1、PCI DSS に準拠しています。

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。お客様と 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。 NTT Com 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。

本サービスの脆弱性管理は、PCI DSS の評価基準を満たした弊社規定に基づき、随時ソフトウェアの更新を実施し、かつ脆弱性検査を適宜実施しています。また、遵守していることを、資格を持つ第三者評価機関により評価頂いています。

クラウド基盤であれば、自社でインフラを持たず、基盤の運用やセキュリティ対策をサービス提供側に任せることが可能です。仮想サーバー、ストレージ、ネットワークのクラウド基盤について、それぞれセキュリティ概要は下記になります。

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共有することを許容できないお客さまにおいては、ベアメタルサーバーをご利用いただくことで物理的に分離された専有型のサーバー環境をご利用いただけます。
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おいては、IOPS 性能確保型のブロックストレージをご利用いただけます。
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。外部接続メニューは帯域確保型と、帯域を共有するベストエフォート型の双方、また VPN サービスを提供しています。

また、本サービスのセキュリティメニュー (セキュリティオプション) は、WideAngle セキュリティメニューをクラウドサービス向けに仕様化し、非常に高レベルなホスト型セキュリティ、ネットワーク型セキュリティなどのマネージドセキュリティサービスを提供しています。

※「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) を設置しており、世界 14 カ国 1,400 名以上(本書執筆時点)のセキュリティ提供体制で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、お客様の ICT 環境を防御します。

グローバルに標準化された共通 ICT 基盤及びセキュリティ対策により、ワールドワイドでの重複投資が避けられるようになります。また、迅速性、柔軟性の確保やセキュリティレベルの統一、コンプライアンス強化を各国の利用者が意識せず、グローバルなセキュリティ基準の整備やプロセス標準化によるガバナンス強化にも効率的に対応できます。

4. 免責及び責任の制限

本書はお客様への情報提供を目的とし、本書の利用は、お客さまの責任において行われるものとします。

本書を通じてお客さまが利用できる情報は、NTT コミュニケーションズが「現状有姿」および「提供可能な限度」で提供し、明示的であるか黙示的であるかにかかわらず、いかなる種類の表明も保証もいたしません。また、別途書面による合意がない限り、本書から取得された情報によって生じたあらゆる損害に関して、弊社は一切の責任を負いません。

本書は、お客さまと弊社間の契約の一部を構成するものではなく、また、お客さまと弊社間の契約が本書により変更されることはありません。

5. 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（日本）
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 の監査レポートは 弊社規定の条件に基づき開示可能です。 IT 監査は、お客様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、 ECL の外部認証取得証書及び監査レポートを、お客様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？	お客様は、ECL 保管データ（お客様が 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。弊社は、お客様との契約に基づくお客様 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） なお、最新情報については、サービス説明書をご覧下さい。 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？	弊社クラウドサービスは複数のお客様にてご利用いただいており、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、お客様の訪問は実施しておりません。 このようなお客様のニーズを満たすために、独立し資格を持つ監査人が統制の有無と運用を 検証し SOC 1 レポートを発行しています。 契約を結んでいる　弊社のお客様は、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の個別の確認も、ISO27001 評価、PCI DSS 評価により 第三者検証評価を行っています。
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？	弊社は、弊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、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。 弊社データセンターへのアクセスの統制については、SOC1 レポートを参照してください。

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？	弊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 統制を遵守し、 PCIDSS,　ISO27017 の基準に従い、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を、独立した資格を持つ監査人が定期的に評価しています。 統制ルールについては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？	各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 の基準が準拠されていることを、独立した資格を持つ監査人が定期的に評価しています。 以下が各サービスコンポーネントにおける分離方法の例です。 ■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共有することを許容できないお客さまにおいては、ベアメタルサーバーをご利用いただくことで物理的に分離された専有型のサーバー環境をご利用いただけます。 ■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おいては、IOPS 性能確保型のブロックストレージをご利用いただけます。 ■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。 外部接続メニューは帯域確保型と、帯域を共有するベストエフォート型の双方を提供しています。
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？	クラウド基盤の脆弱性管理については、ISO, SOC, PCIDSS の評価基準を満たした弊社規定にもとづき、随時ソフトウェアの更新を実施し、かつ脆弱性検査を定期的に実施しています。 また、遵守していることを、資格を持つ第三者評価機関により評価頂いています。ISO27001 ISO27001,ISO27017,SOC1,PCI DSS の評価レポートは弊社規定の条件に基づき開示可能です。 脆弱性対策など、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、お客様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。 また、ロードバランサーや Managed WAF などのサービスをご利用頂き適切に設定いただくことなどにより、通信を暗号化し、盗聴・改ざん・なりすましなどを防止することが可能です。 バックアップサービスをご契約のお客様については、弊社にて暗号化しデータ保存を行っています。

9	DDoS 攻撃、EDoS 攻撃に対して適切に対処していますか？	サービス基盤として DDoS 攻撃対策の仕組みを実装済みです。NTT によるキャリアならではの独自技術を用いた DDoS 対策により、プロアクティブな DDoS 対策を標準実装しています。 また、当社のネットワークに係る課金体系は、利用時間に応じた月額上限付課金です。 妨害攻撃により大量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。 尚、DDoS 攻撃、EDoS 攻撃などの大量アクセス発生時にも処理可能な CDN サービスを別途有償にて提供可能です。
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（クラウドやオンプレミス）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、ECL 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、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など、お客さまにて適切にデータ消失対策を実施頂く必要がございます。 一方、サービス基盤については冗長化されています。ただし、ベアメタルサーバーについては 1 台からのご提供となっておりますので、お客様にて冗長化構成など自由に設計することが可能です。
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？	弊社は、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。 また弊社では、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。破壊手続きは PCIDSS、ISO27017 を遵守しており PCIDSS の基準を満たしていることは審査資格を持つ第三者評価機関により、年次で評価を頂いています。PCI DSS の評価レポートは弊社規定の条件に基づき開示可能です。 個別の廃棄証明書については、ECL サービスとしてお客さまの要望に応じた無償での発行は原則致しかねますが、有償でのメニュー提供について検討中です。（2017.12 現在）

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、お客様への通知、Knowledge Center への公開を実施します。 ただし、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ございます。
15	各サービスの提供終了時期は決まっていますか？	サービスの全体廃止においては、廃止の 180 日前までに弊社の規定する通知方法により通知を行います。 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？	ECL 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、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 下記ページをご覧ください。 https://ecl.ntt.com/documents/service-descriptions/support/support.html
17	最低利用期間はありますか？	Enterprise Cloud サービスにおいては、最低利用期間はございません。(2017.12 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 下記ページをご覧ください。 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、弊社規定に基づく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し、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、および本サービス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、ネットワーク帯域保障型プランがございます。
20	NTT コミュニケーションズは ECL 保管データに対する権利はありますか？	ECL 保管データは、お客さまが所有・管理されるものであり、弊社は、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）。 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？	各サービス毎の提供範囲は、サービス説明書に記載しております。 https://ecl.ntt.com/documents/service-descriptions/
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、弊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）、管轄裁判所は東京地方裁判所になります（同 41 条）。
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 下記ページをご覧ください。 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、どのように対策されていますか？	サービスにおいて行う通信については、通信の暗号化により データ漏えい対策が実施されています。 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では、NTT Com が保有する閉域ネットワークにて接続しています。
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？	脆弱性診断サービスは、別途有償のマネージドセキュリティサービスとして提供されています。 ペネトレーションテストについては、基本的には制限はございませんが、本サービスに著しい支障を及ぼし、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 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？）	Enterprise Cloud サービスとして、解約違約金が存在するオプションはございません。（2017.12 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？	基盤についてウイルス対策が適切に実施されており、PCIDSS, ISO27017 により認定されています。 お客さま環境においては、ISO27017 に準拠しサービス説明書で案内している、セキュリティオプション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、以下のサービス説明書をご参照ください。 ■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 の基準に準拠のバックアップサービスを提供しております。当該基準が準拠されていることを、独立した資格を持つ監査人が定期的に評価しています。 お客様にて対象 OS へバックアップエージェントを導入いただくことで、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。詳細はサービス説明書を参照ください。 https://ecl.ntt.com/documents/service-descriptions/backup/backup.html#id16 本メニュー以外にも、ユーザー個別のバックアップ要件や要望を実現するために、 サードパーティバックアップソフトウェアのライセンス販売もしております。
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以下をご覧ください。 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。 詳細は以下をご覧ください。 https://ecl.ntt.com/documents/tutorials/rsts/ECLC/index.html