

Enterprise Cloud Security White Paper Ver 2.0

03/04/2023

NTT Limited

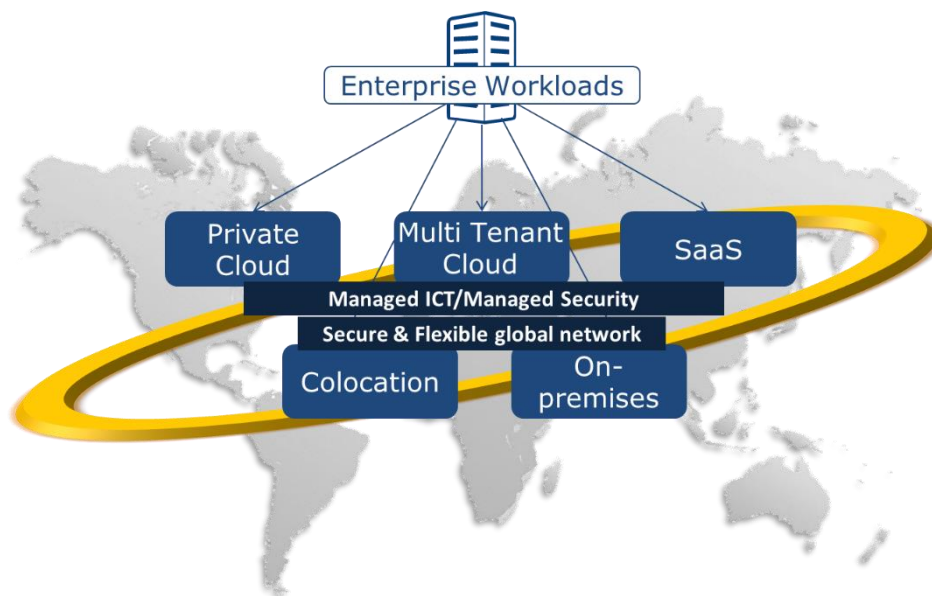
Table of contents

- 1. What is Enterprise Cloud? 2
- 2. Purpose of this document..... 3
- 3. Measures by NTT Limited 4
- 4. Q&A..... 8

1.What is Enterprise Cloud?

The Enterprise Cloud service (hereafter referred to as this “service”, “ECL” or “Enterprise Cloud Service”) is a cloud service of globally common specifications and high performance that can meet with a single cloud platform both the needs of “robustness” and “safety” required of a core system, as well as “agility” and “flexibility” necessity for expansion of digital business.

In particular, NTT provides world's highest-class network and datacenters globally. Our capability realizes that client's standardized ICT platform in one-stop. Because of its globally standardized specification, this service can unify security and compliance levels and can optimize an increasingly complicated ICT environment by strengthening the governance of the ICT environment and centrally visualizing its resources and costs.



2. Purpose of this document

Enterprise Cloud Security White Paper (hereafter referred to as “this document”) describes information security measures, etc. Referring this service that NTT Limited is taking measures. Note, that this document covers Enterprise Cloud 2.0 (hereafter referred to as “ECL2.0”) and not Enterprise Cloud 1.0 (“ECL1.0”).

This document is intended to introduce the security measures NTT Limited takes and have users introduce and use this service without worry, as cloud computing is a system that is used by many clients.

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

THIS ENTERPRISE CLOUD SECURITY WHITE PAPER (“DOCUMENT”) IS FOR REFERENCE PURPOSE ONLY AND THE USE OF THIS DOCUMENT IS AT THE CUSTOMER’S SOLE RISK.

THIS DOCUMENT REFERS TO ENTERPRISE CLOUD SERVICE 2.0. THE INFORMATION ON THIS DOCUMENT DOES NOT APPLY TO ENTERPRISE CLOUD 1.0.

THIS DOCUMENT AND ALL INFORMATION INCLUDED ON OR OTHERWISE MADE AVAILABLE TO THE CUSTOMER THROUGH THIS DOCUMENT ARE PROVIDED BY NTT LIMITED ON AN “AS IS” AND “AS AVAILABLE” BASIS. UNLESS OTHERWISE DESCRIBED IN A WRITTEN AGREEMENT, NTT LIMITED MAKES NO EXPRESS OR IMPLIED WARRANTIES AND DISCLAIMS ANY WARRANTIES, AS TO THE INFORMATION INCLUDED IN OR OTHERWISE MADE AVAILABLE TO THE CUSTOMER.

NTT LIMITED DISCLAIMS LIABILITY OF ANY KIND ARISING FROM THE USE OF THIS DOCUMENT OR FROM ANY INFORMATION, INCLUDED IN OR OTHERWISE MADE AVAILABLE TO THE CUSTOMER, INCLUDING, BUT NOT LIMITED TO DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES OF ANY KIND OR NATURE, UNLESS OTHERWISE DESCRIBED IN AN WRITTEN AGREEMENT.

THIS DOCUMENT IS NOT A PART OF OR WILL NOT AMEND ANY AGREEMENT BETWEEN CUSTOMER AND NTT COMMUNICATIONS OR ANY AFFILIATED COMPANIES.

3.Measures by NTT Limited

This service is certified by ISO27001, ISO27017, ISO20000, MTCS (Singapore), and conforms to SOC1, SOC2 (Japan) and PCI DSS.

Please refer to the following URL for details.

<https://ecl.ntt.com/en/certificate/>

Certification	Description
ISO27001 (ISMS)	International standard of information security management system. This standard systematically puts in order procedures that should serve as criteria for the purpose of “ensuring a security system” to protect information assets and win trust from stakeholders.
ISO27017 (information security controls for cloud services))	Code of practice for information security controls based on ISO27002 for cloud services. ISO27017 also organizes control measures to achieve objectives of information security management that both the clients and NTT Limited as provider of ECL2.0 have.
ISO20000 (ITSMS)	International standard of IT service management. This standard systematically puts in order procedures that should serve as criteria for the purpose of preparing a management system to maintain the quality of an IT service and improve its efficiency.
MTCS	Multi-Tiered Cloud Security Management System (MTCS) is a cloud security certification operating in Singapore. ECL2.0 is certified to be IaaS (Multi-Tiered Cloud Security – Level 1) compliant.
SOC1	A report that evaluates the risks of the internal control of the commissioned party providing ECL2.0 for use by the commissioning party and their auditors in auditing their financial statements. Audit corporations in each country or region formulate the standards. NTT Limited conforms the following standards: <ul style="list-style-type: none">• 「SSAE18」 U.S. security affair standard• 「ISAE3402」 International Federation of Accountants standard

SOC2	<p>A report for clients that assesses the risks of the internal control of the commissioned party providing ECL2.0 related to Security, Availability, Processing Integrity, Confidentiality, and Privacy under the Trust Service Standards. The Japan regions have been evaluated for Security Type 1 (base date valuation).</p> <ul style="list-style-type: none"> 「Trust Service Standards」 Standards set by the American Institute of Certified Public Accountants (AICPA) <p>Security is mandatory, and other scope can be added as needed at the commissioned party.</p>
PCI DSS (Payment Card Industry Data Security Standard)	<p>Global security standards in the credit industry, which is jointly established by five companies – JCB, AMEX, Discover, MasterCard, and VISA – to safely protect the credit card information and transaction information of card members.</p>
ISMAP (Information system Security Management and Assessment Program)	<p>ISMAP aims to ensure the security level of the government's cloud service procurement and the smooth introduction of cloud services by evaluating and registering cloud services that meet the government's security requirements in advance.</p> <p>Please refer to the following website of Information-technology Promotion Agency, Japan (IPA) for ISMAP target menus.</p> <p>https://www.ismap.go.jp/csm?id=csm_ismap_index</p>

As vulnerability management of this service, the software is updated as necessary and vulnerability check is appropriately conducted based on NTT Limited's regulations that meet the evaluation criteria of PCI DSS. The compliance of the service is audited by a qualified third-party evaluation organization.

A cloud platform allows you to entrust a service supplier to operate the platform and take security measures without the need to have your own infrastructure. The security of the virtual server, storage, and network are outlined below.

Item	Description
Virtual server	Logically separated by virtualization software. Clients who don't want to share a physical server because of their information management policies require a physically separated, exclusive server environment using a Baremetal server.
Storage	Logically separated under management of controlling software. Clients who are concerned about influences on the performance as a result of use by other users can use block storage of IOPS performance provisioned.
Network	Logically separated by a virtual network using SDN and VLAN technologies. Both a band-securing type and band-sharing best-effort type external connection menus or VPN service are supplied.

The security menu (security option) for this service uses Wide Angle[※] security menu for the cloud service and supplies managed security services including extremely high-level host-based security and network type security.

The globally standardized common ICT platform and security measures allow clients to avoid worldwide duplicated investment. Moreover, governance reinforcement can be efficiently supported through preparation of global security criteria and standardization of processes with users in each country having to be aware of securing swiftness and reliability, unifying security levels, and strengthening compliance.

Provision of Information at the Event of an Information Security Incident

The provision of information to clients in the event of an information security incident is stipulated as follows. NTT Limited is not responsible for any damage caused in case the client data is lost, damaged or leaked.

We define the scope of information security incident to be reported to client as follows.

- In the event of loss, destruction, or leakage of client data caused by scope of work which NTT Limited is responsible for.

We strive to notify clients of information security incidents within 72 hours after they are certified. Notification is sent via email, portal or other means that NTT Limited has chosen, except in the following cases.

- Cases in which notice may increase the risk to other clients.
- Decisions made by the our company Information Security Team.

In case that an Information Security Incident has occurred, NTT Limited shall implement recovery measures in accordance with the details thereof. NTT Limited will also provide information on recovery measures that clients need to take.

※ "Wide Angle" is the brand of a globally unified integrated security service supplied by NTT Com. Wide Angle sets up a global security operation center (GROC) and realizes efficient, globally uniform quality, making high-level, advanced analysis possible through concentrated stationing of risk analyzers. NTT Com is also the largest ISP in Japan who has know-how by providing provides network operations at domestic and outside of Japan, also utilize the collaboration effort with a world's top security research institution to protect ICT environments of customers.

4.Q&A

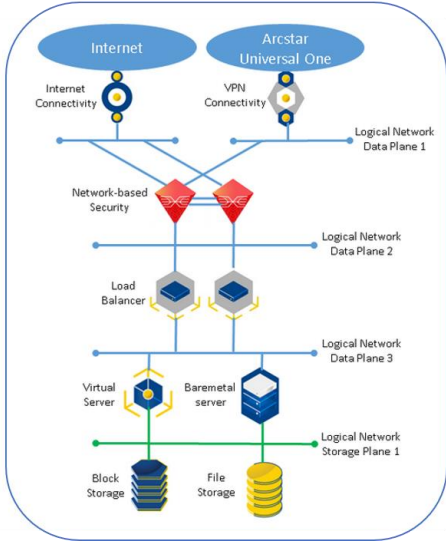
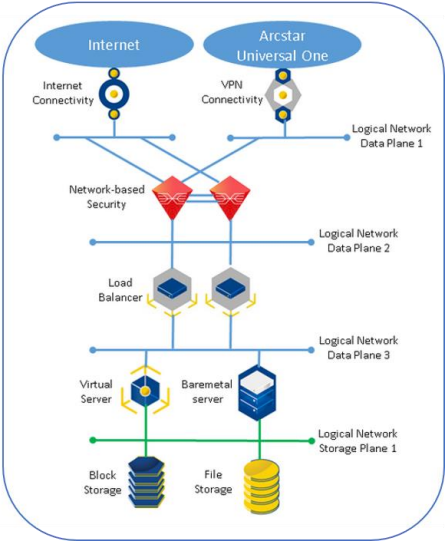
For Q&A, the following is used as a reference:

- ENISA “Cloud Computing: Framework for Securing Information Security (11/2009)”
- Ministry of Internal Affairs and Communications “Information Disclosure Guidance concerning Safety and Reliability of Cloud Service (03/2017)”
- Ministry of Economy, Trade and Industry “Cloud Security Guideline, revised version (2013)”

No.	Question	Answer
1	How should we conduct an IT audit?	<p>We can disclose, based on the terms of the company regulation, the certificates of ISO 27001, ISO27017, ISO 20000, MTCS, and the audit reports of SOC1, SOC2, PCI DSS.</p> <p>IT audits need to be conducted by the persons in charge of compliance and audit at the client. The third party’s certifications acquired by ECL and the audit reports are available for review by the auditors at the clients.</p> <p>For the latest information, please refer to Knowledge Center. https://ecl.ntt.com/en/certificate/</p>
2	Where is the data stored?	<p>You are free to select the region you upload and store the data (“ECL Stored Data”). We will not move ECL Stored Data to any other regions which client has not selected unless we have specific instructions from the client under the contract, or to comply with a legally valid and binding order.</p> <p>For the latest information, please see the service description. https://ecl.ntt.com/en/documents/service-descriptions/rsts/common/region_zone_group.html#id24</p>

3	Can we visit the data center?	<p>As our cloud service is used by multiple clients, we strictly restrict access to cloud facility in the data center. Therefore, we do not allow clients to visit our data center.</p> <p>In order to meet the needs of the clients, independent and qualified auditors verify the presence and operation of the control, and issue SOC1 and SOC2 reports.</p> <p>Clients who have a contract with us can request a copy of the SOC1 and SOC2 report.</p> <p>Confirmation of individual physical securities of the data centers is also verified and assessed by third parties in ISO27001, MTCS※, SOC1※, SOC2※ and PCI DSS assessments.</p> <p>※Physical securities in the data centers have been evaluated as follows.</p> <ul style="list-style-type: none"> • MTCS in Singapore • SOC1 in Japan and Singapore • SOC2 in Japan
4	Is it possible for a third party to visit the data center?	<p>We apply strict control on the access to our data centers, even to our own employees.</p> <p>Authorization by the data center administrator is required in accordance with the access policy.</p> <p>For information on the control of access to our data center, please see the SOC1 and SOC2 report.</p>
5	Do you have a prevention system in place to address inappropriate access by insiders, such as data center administrators?	<p>In order to address threats resulting from inappropriate access by insiders, we comply with SOC1 and SOC2 control and follow PCI DSS, ISO27017 and MTCS standards.</p> <p>Third-party auditors regularly make assessment to verify that we are in compliance.</p> <p>With regard to the rules for internal control, we have a system in place to internally conduct risk assessment and to review them periodically.</p>

6	Is the system properly isolated among the users?	<p>Each user's system environment is properly isolated.</p> <p>Third-party auditors regularly make assessment to verify that we are compliant with ISO 27017 and MTCS.</p> <p>See the following examples for the method of isolation in each service component.</p> <p>■ Server</p> <p>The virtual servers are logically isolated by virtualization software. If a client does not allow itself to share a physical server owing to its information management policy or for other reasons, we offer a dedicated server environment physically isolated by use of a Baremetal server.</p> <p>■ Storage</p> <p>They are logically isolated by control of software managing the storage.</p> <p>For clients with concerns about the impact on performance from operations of other users, IOPS performance provisioned block storage is available.</p> <p>■ Network</p> <p>They are logically isolated by a virtual network utilizing SDN, VLAN and other technologies.</p> <p>We offer two choices in the menu for external connections: bandwidth guaranteed type and best-effort type, in which bandwidth are shared.</p> <p><Image of logical isolation></p>
---	--	--

		<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 10px; width: 45%;"> <p style="text-align: center;">Tenant 1 : Customer A</p>  </div> <div style="border: 1px solid black; padding: 10px; width: 45%;"> <p style="text-align: center;">Tenant 2 : Customer B</p>  </div> </div>
7	Do you have measures in place for known vulnerabilities in each system, i.e. hypervisor or virtual OS? Is there any occasion in which the service stops for various maintenance tasks, such as in response to vulnerabilities?	<p>To control the vulnerability of the cloud structure, we update the software as necessary and regularly inspect for vulnerability. It is based on the company's regulations, which meet the assessment criteria of ISO, MTCS, SOC2 and PCI DSS.</p> <p>We also have a qualified third-party assessment agency to assess the status of our compliance. Based on the terms of the company regulations, we can disclose the assessment reports of ISO 27001, ISO27017, MTCS, SOC2 and PCI DSS.</p> <p>We may stop a service if it is necessary in order to protect the service and client environment; in such occasions, for instance, as applying measures against vulnerabilities.</p> <p>With regard to OS and middleware on the virtual servers, it is necessary for the clients to implement measures against vulnerabilities (such as updating software or applying patches).</p>
8	Do you support encryption in each service?	<p>With regard to OS and middleware on virtual servers, clients are free to apply their own encryption technology.</p>

9	Do you have appropriate measures in place to address DDoS attacks and EDoS attacks?	We have implemented the service infrastructure with a system to counter DDoS attacks. Proactive counter DDoS measures have been implemented as a standard feature, using NTT's DDoS countermeasures, which use proprietary technology unique to communication carriers. In addition, we set a monthly cap on the amount we charge on our network based on the time of use. Even if a client had a large amount of traffic owing to a jamming attack, we do not charge the client for the amount above the monthly cap. We also offer CDN service at a fee, which is capable of operation even at a time when there is a considerable amount of access, such as in DDoS attack or EDoS attacks.
10	Can we export the saved data?	You can export the data that are controlled by you. When migrating the data to another infrastructure (on cloud or on-premises), you can migrate them using hypervisor-specific tools and APIs in the dedicated hypervisor menu. You can export the virtual server image, by using the method of extracting it as an image, or by using various backup tools.
11	What is the policy on redundancy of the user data saved in each service?	Concerning user data, the ECL service does not offer a service such as, for instance, making their copies on multiple sites. To guarantee the redundancy of user data, it is necessary for the client to properly implement measures against data loss, such as execution of replication to other sites and regular backups. On the other hand, the service infrastructure is redundant. However, as for Baremetal servers, since the Baremetal servers are provided from one unit, client can freely design the system, including configuring them redundant.
12	How do you react if you are required to disclose ECL Stored Data for criminal investigations or under any laws?	We will protect the client data and privacy. We will not disclose ECL Stored Data unless we have to comply with a legally valid and binding order. When we receive an order to disclose ECL Stored Data from the authorities, we will notify the client of it to the extent that it does not cause any breach of laws and regulations.

13	Can you issue the data deletion certificate when deleting certain data? How do you delete the data in deleting operation? Can you issue a data delete certificate?	In principle, ECL Stored Data shall be deleted by the client. At the termination of the service, however, they will be deleted automatically. In addition, for safe discarding of unneeded media, we demagnetize the HDD and destroy the memories physically to prevent the stored data from being reproduced. Our procedure of destruction complies with PCI DSS, ISO27017 and MTCS. Third-party assessment agencies qualified for auditing make assessments annually to confirm that we meet PCI DSS standards. We can disclose the assessment report of PCI DSS, based on the terms of the company regulations.
14	Are you appropriately monitoring the operation status of each service? Are they open to the public?	The operation status of the service infrastructure is centrally monitored. When an abnormality is detected, we will notify the clients and post the information to Knowledge Center as stipulated in the service manual. However, for alive monitoring of individual virtual servers and other services, the clients need to implement them by using a monitoring service or other methods.
15	Is there a fixed date for each service to be discontinued?	When we are to discontinue the entire service, we will issue notifications by a method prescribed by the company up to 180 days before the discontinuation. When we are to terminate some part of a service and if we cannot present alternative means or equivalent functions replacing the function to be terminated, we shall provide notification of the details of the service after the change to the contracted clients in advance, with a notice period of 30 days or more.
16	What is the standard support service? Do you offer different support service with a fee?	ECL offers support functions including ticket support, information posts to Knowledge Center, and the function to indicate the resource status on the portal. https://ecl.ntt.com/en/documents/service-descriptions/rsts/common/support.html
17	Is there a minimum contract period?	There is no minimum use period for Enterprise Cloud service. (As of December 2019)

		However, this may not apply to contractual clauses of individual clients, such as in special contracts.
18	Is SLA defined?	For an option in which its service offering stipulates SLA for monthly availability, we have set the value at 99.99%. For details on the monthly availability and each SLA, please see the following page at Knowledge Center. https://ecl.ntt.com/en/sla/
19	Do you have any measures implemented to address noisy neighbor? (Are impacts to the service caused by other users taken into consideration?)	To address such issues as a noisy neighbor, we implement an upper limit on use based on company regulations. In addition, if there is an act that causes or may cause a serious obstacle to this service, we may notice to the subject user or suspend the user from using this service. We also offer services that are free from impact from other users: option in which the client occupies the whole server, such as in a Baremetal server, and a network bandwidth guarantee plan.
20	Does NTT Limited have any rights against ECL Stored Data?	ECL Stored Data is owned and managed by the client. We are not aware of the contents of ECL Stored Data. We will not access ECL Stored Data unless we have specific instructions from the client under a contract with the client, or to comply with legally valid and binding order (except when the data is deleted upon termination of the contract).
21	What is the demarcation point of responsibility among provided services?	Please see the service manual for the scope of each service. https://ecl.ntt.com/en/documents/service-descriptions/ The network access from client premises to ECL is required to prepare by client separately, such as NTT Limited's secure VPN network service.

22	Which jurisdiction would be applied to the ECL service agreement? (Would it belong to the country of each region?)	Despite the location of the region you selected, the governing law and the jurisdiction will be the law and court of the country of NTT Communications affiliated company's principal place of business which you have the contract with.
23	How does ECL address to the EU General Data Protection Regulation (GDPR)?	Please see the following URL for ECL's compliance with GDPR. https://ecl.ntt.com/en/faq/2.0/service/gdpr/
24	What measures are you taking for the data leakage in the communication route (at uploading, downloading, or transferring between clouds)?	By using a service menu such as a load balancer or a managed WAF and having it be configured appropriately by client, client can encrypt the communication using an encryption algorithm corresponding to the Japanese government's e-Government Recommended Ciphers List, and prevent eavesdropping, tampering and spoofing. For communications that client makes with external parties, the client needs to implement any encryption method or other measures. As we do not restrict any means or other conditions on encryption which is implemented by the client, you can address requirements in each individual case. Connections to the remote data center [DC Inter-Connectivity menu] are made with the closed area network owned by NTT Limited.
25	Is vulnerability diagnosis service available for the systems constructed by users?	A vulnerability diagnosis service is available for a fee, as a separate managed security service. There is basically no limitation on penetration tests, but for acts that cause or may cause a serious obstacle to this service, we may notice to the subject user or suspend the user from using this service.

	Is there restriction on user's implementation of a penetration test?	
26	Is there any cost to be incurred, other than the service fee for the service actually used by the client such as cancellation fee? (Do you impose penalty or cancellation fee?)	<p>Cancellation fee is not required for any Enterprise Cloud Service (As of December 2019)</p> <p>However, cancellation fee might be required under specific conditions with clients.</p>
27	Is the cloud service infrastructure antivirus-protected? Do you offer any anti-virus service?	<p>The infrastructure is properly implemented with antivirus measures and certified by PCI DSS, ISO27017 and MTCS. Clients can equip their environment with anti-virus measures by our security options. For details, please see the following service manual.</p> <p>■ Managed UTM https://ecl.ntt.com/en/documents/service-descriptions/rsts/security/menu_utm.html</p> <p>■ Managed WAF https://ecl.ntt.com/en/documents/service-descriptions/rsts/security/menu_waf.html</p> <p>■ Managed Anti-Virus https://ecl.ntt.com/en/documents/service-descriptions/rsts/security/host-based/menu_av.html</p>

		<p>■ Managed Host-based Security Package</p> <p>https://ecl.ntt.com/en/documents/service-descriptions/rsts/security/host-based/menu_pk.html</p>
28	Do you offer backup services for files and systems?	<p>We provide third-party backup software licenses as Middleware menus to meet client's individual requirements and requests regarding backup operations.</p> <p>By installing the following menu, you can configure the backup schedule and storage period and execute the file/system restoration from the portal.</p> <p>For details, please see the service manual.</p> <p>https://ecl.ntt.com/en/documents/service-descriptions/rsts/arcserve/arcserve.html</p>
29	What types of operation are available on hypervisor or virtual OS? * Administration screen on a web browser, API, etc.	<p>The following three types of operation are available:</p> <p>■ Client Portal (GUI)</p> <p>You can control the resources by intuitive operation.</p> <p>■ API</p> <p>By specifying the API endpoint for each resource, operations can be executed with API. Please see the following for API reference.</p> <p>https://ecl.ntt.com/en/documents/api-references</p> <p>■ CLI/SDK</p> <p>Each resource can be operated from the command line. You can also use Python SDK for operation. For details, please see the following.</p> <p>https://ecl.ntt.com/en/documents/tutorials/rsts/ECLC/index.html</p>
30	Is data center location are published?	<p>We do not put display boards or signboards outside the data center building to indicate the location of the data center or to identify clients' name of the data center who have racks and so on.</p>

31	How are client's ECL2.0 usage records protected?	In order to prevent unauthorized access and tampering, NTT Limited restricts access to the records of cloud service usage.
----	--	--