RICOH Unified Communication System

Security White Paper (Ver. 4.0)

- UCS terminals P3500
- Apps
  - (for Windows)
  - (for iPad/iPhone)
  - (for Android)
  - (for 360 VR Live)
  - (for Rooms)

RICOH Co., Ltd.

Apr 2023

* This white paper does not target RICOH Unified Communication System Advanced (UCS Advanced).

Provided status on RICOH Unified Communication System

RICOH imagine. change.

✓ Available　　x Unavailable

		Available or Unavailable
Terminals	P3500	✓
	P1000	×
	P3000	×
	S7000	×
Apps	for Windows	✓
	for iPad/iPhone	✓
	for Mac	×
	for Android	✓
	for 360 VR Live	✓
	for Rooms	✓

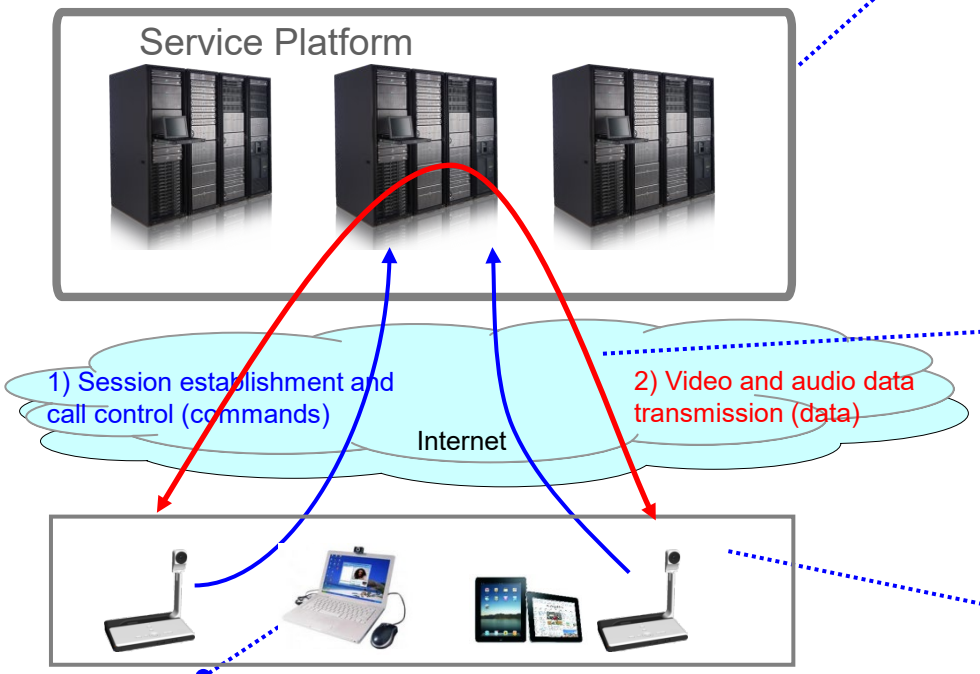
Revision History

Date	Version	Modification from the previous version
August, 2013	3.2	Information about Apps for Mac and iPhone has been added.
April, 2014	3.3	Information about P1000 has been added.
August, 2014	3.4	Information about P3500 and Android app has been added.
January, 2017	3.5	Information about the Service platform which became to be high availability by distributed DC configuration has been changed. Information about UCS for IWB has been added.
July, 2019	3.6	Information about 360 VR Live and Android app has been added.
September, 2020	3.7	Information about Apps for Rooms has been added.
Jan, 2021	3.8	Information about P3000 has been added.
Nov, 2021	3.9	Information about Apps for Mac has been added.
Apr, 2023	4.0	Information about P3000, S7000, P1000, Apps for Mac has been deleted.

Overview

The Ricoh Unified Communication System performs communication through a service platform built on the cloud.

The service platform controls the connections between terminals and relays video and audio data.



Service Platform (Cloud)

Ensure availability with redundancy
All service platform components, including firewalls, network equipment and servers, are redundant.

Access restrictions
The firewalls prevent unauthorized access.

Vulnerability measures
A tool-based vulnerability assessment is conducted every three months. If any vulnerability is detected, countermeasures will be taken within five business days.

System monitoring
In addition to monitoring within the service platform, normal conference operation is checked from the outside.

Communication

1) Session establishment and call control
After establishing a session, the information needed for call control is encrypted by TLS.

2) Video and audio transmission
Video, audio, and PC screen-sharing data are all encrypted.
The SRTP data transfer method is used.

Terminals

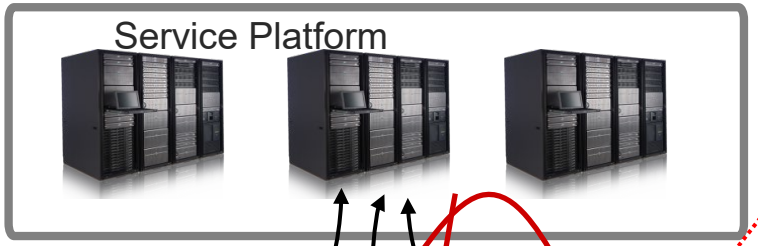
Vulnerability measures
When a vulnerability is found in the software, a software update will be distributed via the Internet.

Preventing unauthorized use
If a terminal is lost or stolen, it will be rendered inoperable by the data center to prevent unauthorized use. Each terminal is specified by its CID (contact ID).
A UCS terminal contains a mechanism for identifying itself as a genuine client terminal. In the case of Apps, terminal authentication is performed using both a CID and password.

Mutual Authentication

Limiting communication partners
The system can make connections when the devices have been mutually authenticated in advance by using the web-based management utility or the application on each device.
However, it is also possible to accept calls with contact IDs from unregistered users if the user sets up the terminal to permit such calls. (Supported exclusively by P3500/for Windows/ for Rooms.)

System Security



Video and audio (data)
Video encoding method: H.264 SVC (H.264/AVC Annex G)
Streaming data transfer method: SRTP

Session establishment and call control (command)
The transferred data is encrypted by TLS.
M2M communication data, contact list, and other data are protected by encrypted communication.

Terminals

Session establishment and call control

When a Ricoh UCS terminal starts, it connects to the service platform and displays the contact list.
After start-up, all data transfer is encrypted by TLS.
Both video and audio data is encrypted by a communication protocol called SRTP (Secure RTP). If the video and audio data should somehow be secretly monitored or saved by a third party, it cannot be decrypted.

Restricting access to the service platform from the Internet

The firewall accepts only HTTPS access using a browser from the management utility and access through a designated port from a successfully authenticated Ricoh UCS terminal. A tool-based vulnerability assessment is conducted every three months.

System monitoring

The resources, including the CPUs, memory and network band, as well as the logs are checked using monitoring software.
Dedicated software deployed at several locations outside the system checks whether the conference session can start and is executing normally.

Security of the Service Platform

RICOH
imagine. change.

Service platform as a whole

The service platform consists of several data centers. Even if a single data center becomes unavailable due to a natural disaster or a large-scale problem, its functions are automatically transferred to the other servers, and the service can be continued. Each data center has acquired ISO27001 certification.

Configuration of the infrastructure in each data center

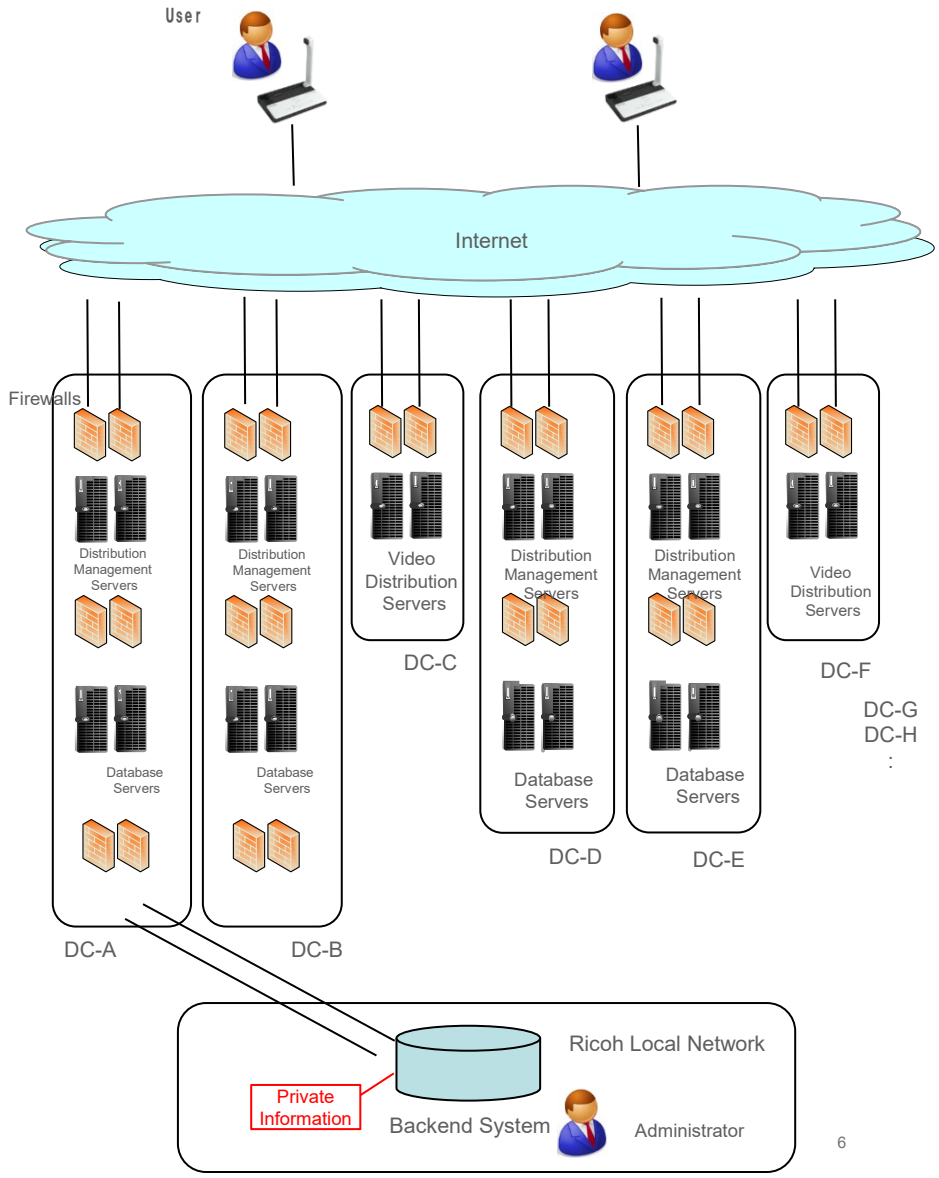
The firewalls, network equipment, database, and application servers are all redundant. The video distribution servers are also redundant, and can be scaled out according to an increase in the number of users to ensure sufficient resources.
The database that stores important data is always located behind a double firewall to prevent data leakage.
The connection to the Internet is also redundant.

Customers' Private Information

Private information provided during the contract process is not recorded in this service platform. It is managed only by the backend system within the Ricoh Network.

Vulnerability measures

A tool-based vulnerability assessment is conducted every three months.
If any vulnerability is detected, countermeasures will be taken within five business days.



Terminal Security (Common)

Restricting connections with other terminals

A Ricoh UCS terminal exchanges video and audio with other terminals around the world through the Internet.
To prevent unexpected connections, a UCS terminal only accept calls (for establishing the connections for conferences) from the terminals registered in the Contact List.
To register a user in the Contact List of another user, a contact registration request needs to be sent to the other party's terminal using the management utility on the Web or in an application.
When the other party approves the request, the terminals are registered in the Contact Lists of both parties.

However, it is also possible to accept calls with contact IDs from unregistered users if the user sets up the client to permit such calls (contact ID connections). (Supported exclusively by P3500/for Windows /for 360 VR Live/ for Rooms for both calling and receiving calls.)

Vulnerability measures

When any software vulnerability is found, a software update will be distributed through the Internet.

Reporting from a terminal

To diagnose problems occurring in the service, the terminal sends (reports) its status.

The information collected from the terminals is used by Ricoh only to analyze the problems in the software and hardware, never for other purposes.

Terminal Security (P3500)

RICOH
imagine. change.

Preventing information leakage

The information stored in the internal storage media, including programs and application logs, is password protected.
(Even if the storage media is connected to a PC, the content cannot be read.)
The user information required for terminal authentication is encrypted.

Preventing program tampering

The firmware is signed with a digital signature. If it is tampered with, verification of the digital signature fails and the terminal will not start.
When the PC Screen Share feature is used, intrusion (writing) of computer viruses and other malware from the PC is prevented by making the storage area of the terminal read-only before it is connected to the PC through a USB port.

Preventing unauthorized use of a Ricoh UCS terminal

・A UCS terminal has a mechanism for identifying itself as a genuine client terminal.
・If a terminal is lost or stolen, it will be rendered inoperable by the data center to prevent unauthorized use.
(In addition, the CID of a lost or stolen terminal can be reassigned to a different terminal. Therefore, it is possible to use the same CID and Contact List on the new terminal.)

Authentication and encryption for wireless LAN

The following protocols are supported.
Authentication protocols (wireless LAN):
Open key system authentication, shared key authentication, WPA-PSK, WPA2-PSK, WPA-EAP(*), and WPA2-EAP(*)
Encryption protocols (wireless LAN):
WEP 128bit/64bit, TKIP: WPA-PSK/WPA2-PSK/WPA-EAP/WPA2-EAP
AES: WPA-PSK/WPA2-PSK/WPA-EAP/WPA2-EAP

* For WPA-EAP and WPA2-EAP, only the PEAP method is supported.

Terminal Security (for Windows and 360 VR Live)

RICOH
imagine. change.

Preventing information leakage

1) User information

Information on the user and environment used by the application is encrypted in the client terminal and saved in the profile folder of Windows.

2) Application logs

Application logs are saved in the profile folder of Windows, which cannot be accessed by other users.

3) Information embedded in the program

Important information in the application is encrypted in order to mitigate the risks of information leakage.

Preventing program tampering

Ricoh distributes an installer with code signing signature, which ensures that it cannot be tampered with or changed.

Preventing unauthorized use of the application

- This application has a mechanism for performing authentication using both a CID and password.
- If the CID or password, or both are lost or leaked, the CID can be disabled by the data center.
- The service can not be used unless the user registers an email address and changes the initial password.

Terminal Security (for Rooms)

RICOH
imagine. change.

Preventing information leakage

1) User information

Information on the user and environment used by the application is encrypted in the client terminal and saved in the profile folder of Windows.

2) Application logs

Application logs are saved in the profile folder of Windows, which cannot be accessed by other users.

3) Information embedded in the program

Important information in the application is encrypted in order to mitigate the risks of information leakage.

Preventing program tampering

Ricoh distributes an installer with code signing signature, which ensures that it cannot be tampered with or changed.

Preventing unauthorized use of the application

- This application has a mechanism for performing authentication using both a CID and password.
- If the CID or password, or both are lost or leaked, the CID can be disabled by the data center.
- The service can not be used unless the user registers an email address and changes the initial password.
- Partial setting changes and function execution within the application can be protected with a password. Therefore, it is designed so that it cannot be used by outsider.

Terminal Security (for iPad/iPhone)

RICOH
imagine. change.

Preventing information leakage

1) User information

Information on the user and environment used by the application is encrypted and saved using the Keychain Service provided by the iOS, which cannot be accessed by other applications.

2) Application logs

Application logs are saved in an area dedicated for the application using the Sandbox function provided by the iOS, which cannot be accessed by other applications.

Preventing program tampering

The application is saved in a dedicated area using the sandbox function provided by the iOS. An iOS application needs to be signed, which ensures that it cannot be tampered with or changed.

Preventing unauthorized use of the application

- This application has a mechanism for performing authentication using both a CID and password.
- If the CID or password, or both are lost or leaked, the CID can be disabled by the data center.
- The service can not be used unless the user registers an email address and changes the initial password.

Terminal Security (for Android)

RICOH
imagine. change.

Preventing information leakage

1) User information

Information on the user ID and password used by the application is encrypted inside the application and saved in the internal storage specific to the application, which cannot be accessed by other applications due to the application footprint.

2) Application logs

The log files are stored in the internal storage specific to the application, which cannot be accessed by other applications.

3) Information embedded in the program

Important information in the application is encrypted in order to mitigate the risks of information leakage.

Preventing program tampering

Distribution of the Android application needs to be signed, which ensures that the application distributed by Ricoh cannot be tampered with or changed.

Preventing unauthorized use of the application

- This application has a mechanism for performing authentication using both a CID and password.
- If the CID or password, or both are lost or leaked, the CID can be disabled by the data center.
- The service can not be used unless the user registers an email address and changes the initial password.