HULFT-WebConnect
Security White Paper

Version 7~~6~~

April ~~December~~ 1, 2024~~2~~

Saison Technology ~~Information Systems~~ Co., Ltd.

History of Revisions

The history of revision of this document is as follows:

Version	Date of Issue	Description of Revision
1	April 2015	Establishment
2	August 2016	Added “Authorization and Approval of API” Added block functions due to the types of clients within the “Confidentiality” section
3	December 11, 2017	Added access restriction functions due to IP filters to the “Access Control” section
4	August 16, 2018	Amended the contents of the “Availability” section
5	August 17, 2020	Amended how the types of clients are described
6	December 1, 2022	Added "Handling of Data" Amended the contents of the "Notice" section
7	April 1, 2024	Changed the company name Changed “~~"~~http”~~"~~ to “~~"~~https”~~"~~ in URLs Changed URL of “Announced Items pursuant the Act on the Protection of Personal Information”

This HULFT-WebConnect Security White Paper (this "Document") introduces the security measures implemented for the infrastructure and application of HULFT-WebConnect provided by Saison Technology ~~Information Systems~~ Co., Ltd. (the "Company").

Cloud Computing Environment

HULFT-WebConnect adopts Amazon Web Services ("AWS") as its cloud computing environment. For security measures of such cloud computing environment, please see the following link:

AWS Security Center
https://aws.amazon.com/security/

Monitoring

Instance monitoring (live-monitoring of hardware and operation systems, and live-monitoring of CPU usage) and application monitoring (live-monitoring of web server processes and live-monitoring of AP server processes) is performed for HULFT-WebConnect using automatic monitoring systems. When an irregularity is detected or a threshold is crossed, push notifications are sent to operators and developers of the Company along with alert information.

Availability

HULFT-WebConnect provides multiple access points. Client of HULFT-WebConnect automatically selects the closest access point depending on the usage environment of the customer. If for some reason the closest access point does not respond, Client will automatically select the most appropriate access point from among access points that it can connect to.
With HULFT-WebConnect, a redundant configuration is taken with respect to the web server, AP server and DB server to ensure service availability.

Confidentiality

In order to ensure the confidentiality of the transmissions of HULFT-WebConnect, routing encryption by TLS is applied at all times to transmissions between HULFT-WebConnect and Client.

For the purpose of preventing unauthorized use of registered accounts and connection information, HULFT-WebConnect maintains hashed account passwords and connection passwords.

HULFT-WebConnect does not write the data being relay-transferred on discs, but the data is relayed on-memory.

Furthermore, in order to prevent receiving files being transferred from any unexpected counterpart, relay permission may be configured (which is a configuration to filter whether to allow relay transfers or not in a white list format) by ways such as limiting the types of client (HULFT, API/CLI) which can connect to such connection ID by the connection configuration. For the configuration of relay permission, it must be configured on both the sending and receiving sides of the file transfer. Therefore, compared to a configuration only for either the sending side or the receiving side, it offers stronger security.

Authorization and Approval of API

Web API and CLI made public on HULFT-WebConnect provide a structure for authorization and approval using API keys. It is possible to configure the effective period as well as the scope of access using the API keys. By configuring the API keys in accordance with the applicable work, it is expected that fraudulent manipulation in ways such as the access of unauthorized information will be prevented.

Access Control

In order to prevent attacks by malicious users in and outside of the Company, HULFT-WebConnect adopts a system in which only preapproved users may access the administration server of HULFT-WebConnect. Also, by limiting the access to the administration server only to the Company, it deters unauthorized access, whether intentional or negligent.

In addition, connections to HULFT-WebConnect may be restricted by connection source IP addresses due to IP filters.

Security Measures in the Development Process

In order to detect vulnerabilities in the source code of HULFT-WebConnect during an early stage, inspections using static source analysis tools and pseudo attack diagnosis tools are performed during the development process.

Furthermore, the Company adopts a structure where the development environment, staging environment and production environment (which is the environment that the customer will use) are made available so that unverified applications are not deployed in the production environment.

Personal Information

In providing the Services, the Company handles personal information (which refers to information defined in Article 2 (2) of the Act on the Protection of Personal Information), confidentiality of transmission and privacy appropriately pursuant to the Act on the Protection of Personal Information, the

Telecommunications Business Act, other relevant laws and regulations, and “Announced Items pursuant the Act on the Protection of Personal Information” (https://www.saison-technology.com/en~~home.saison.co.jp~~/privacy~~/~~) of the Company.

Handling of Data

The Company handles the data listed below (1) for provision of the HULFT-WebConnect Services and (2) for research and analysis in order to improve the HULFT-WebConnect Services.
This data does not include the contents of the texts, images, programs, and any other information transferred using the Services (the "Data"; the same data as defined in HULFT-WebConnect Terms of Use Article 9.3).
"Information registered by the customer such as transfer settings" and "history of service functions used by the customer" are encrypted, stored, and managed in the HULFT-WebConnect Service infrastructure.

- Information registered by the customer such as transfer settings
- History of service functions used by the customer
- Various server logs output while the Services are running

The Company does not access the Data without either (1) the Customer's written consent in advance to do so, or (2) the order to do so by a court, by an administrative agency, or according to other laws or regulations.
Additionally, HULFT-WebConnect does not store the Data in the functions of the Services.
When the customer uses the functions of HULFT-WebConnect to relay the Data on-memory, HULFT-WebConnect takes measures to prevent data leakage within the scope of the Services.
However, the customer is responsible for preventing data leakage outside the scope of the HULFT-WebConnect Services, in communications networks on the internet.
Additionally, the customer is responsible for deciding on and implementing security requirements (level of strength of security and such) suitable to the nature of the Data, the customer's business, and the service utilization purposes.
Therefore, the customer must control the configuration of the HULFT-WebConnect Services and the handling of "customer transferred data" under the customer's own judgment and responsibility.

Notice

This Document is provided only for the purpose of providing information. This Document provides information as of the date of its effective date. The Information contained herein may be changed without advance notice. Please see (https://www.hulft.com) for the most updated information.

The customer is responsible for making its own evaluation of the information in this Document as well as the use of HULFT-WebConnect. The information is provided to you “as is” without warranty of any kind, whether express or implied.

- END -