Campus Wireless LAN Connection Reference Material

July 2021

Saitama University Information Technology Center

※ The information described in this document is open only to Saitama University-related persons (students, faculty, etc.).

※ Unauthorized reprinting is strictly prohibited.

■ Eligibility to use the campus wireless LAN

Currently, there are about 300 wireless LAN access points set up within Saitama University's Okubo Campus, and those who have the university-wide authentication account can freely connect and use them.

In using it, it is necessary to comply with the "Saitama University Information Security Policy". Please ensure you adhere to information ethics, and avoid criminal or nuisance behaviors, or situations leading to undesirable situations such as information leaks.

■ Campus Wireless LAN Connection Specifications

The connection and user authentication to the campus wireless LAN are carried out under the following specifications. You can connect with devices that meet the following specifications, including personal computers, smartphones, PDAs, etc.

For the settings to use the wireless LAN on your computer, please refer to the separately published manual. It explains the setup procedure to meet the above.

[Wireless LAN compliance standards] 802.11 ac/a/g/n

[Connection authentication specifications]

- SSID (Access Point Identifier): su-wireless
- SSID stealth: Enabled*
- Security: WPA2-Enterprise (Note: not WPA2-PSK)
- Encryption method: AES
- User authentication standard: IEEE 802.1X
- Authentication method: PEAP / EAP-MSCHAP v2
- Authentication server (or domain name): su-ap.saitama-u.ac.jp

  (Root CA: Security Communication RootCA2)
  - Server certificate thumbprint (SHA-1 fingerprint): Please check here.

■ Settings for Connecting Smartphones, Tablets, etc.

Currently, the leading OSs for mobile devices include iOS (iPhone, iPad, etc.), Android, Windows Mobile, etc., and the method of setting varies greatly for each OS and its version. Furthermore, implementations are different between each manufacturer and model, making it difficult to fully support connections.

For the time being, we will limit our description to examples of configurations that have allowed connections.

Although we have confirmed that the examples below follow the connection specifications, we cannot guarantee that it will be possible to connect by setting it as in this example, or that malfunctions and side effects will not occur, so please refer to it after understanding this point.

<<Example: iPhone (iOS 14.4)>>
To set it up, go to "Settings" → "Wi-Fi" → "Other...", and set like this:

- Name: su-wireless* Security: WPA2 Enterprise
- Username: [User ID of the university-wide unified authentication account]
- Password: [Password of the university-wide unified authentication account]
- Certificate: su-ap.saitama-u.ac.jp

<<Example: Android 10 (Verified on SHARP AQUOS SH-M07)>>
Set up as follows via "Settings" → "Wi-Fi" → "Add Network":
Items marked with (*) are displayed by tapping on "Advanced Settings"

- SSID: su-wireless
- Security: WAP/WPA2/WPA3-Enterprise* EAP Method: PEAP
- Phase 2 authentication: MSCHAPV2
- CA certificate: "Use system certificate"
- Domain name: su-ap.saitama-u.ac.jp
- ID: [User ID of the university-wide unified authentication account]
- Anonymous ID: (blank)
- Password: [Password of the university-wide unified authentication account]
- Privacy: "Use random MAC"(*)
- Metered: "Detect automatically"(*)
- Proxy settings: "None"(*)* IP Setting: "DHCP" (*)
- Private Network: "Yes" (*)

≪Example: IDEOS (Former Android)≫

- SSID: su-wireless
- Security: 802.1x EAP
- EAP Method: PEAP
- Phase 2 Authentication: MSCHAPV2
- CA Certificate: (Not specified)
- User Certificate: (Not specified)* ID: [User ID of the university-wide unified authentication account]
- Anonymous ID： (Blank)
- Password: [Password of the university-wide unified authentication account]

■ Information about device dependence

In some models, there may be a case where the CA certificate ("Security Communication Root CA2") required for the su-wireless access point validation is not incorporated. For inquiries about the installation method of the certificate, please contact the manufacturer.

■ Revision history

Issued in June 2012
Revised in June 2015Revised in March 2016
Revised in May 2017
Revised in November 2018
Revised in November 2019
Revised in April 2021
Revised in July 2021