ABSTRACT

A communication apparatus includes: a memory (418) that holds CA information A(301a) including (i) a CA certificate A(106a) indicating that an AP server certificate A(402a) that indicates the validity of an application server (401) is valid and (ii) a URL B(302b) indicating the URL of a download server B(406b) where CA information B(301b) including the next valid CA certificate B(106b) is stored; a server authentication unit (416) that verifies the AP server certificate A(402a) using the CA certificate A(106a); and a CA information update unit (417) that obtains the CA information B(301b) from the download server B(406b) indicated by the URL B(302b), wherein when the CA certificate A(106a) becomes revoked, the server authentication unit (416) thereafter authenticates the application server (401) using the CA certificate B(106b) included in the CA information B(301b) obtained by the CA information update unit (417).