SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

IP アドレスをサブジェクトに含んだ Web サーバ証明書の調査と分析
Study of Web Server Certificates Containing IP Addresses As Subjects

金岡 晃 * 小山 裕輝 * 岡田 雅之 †
Akira Kanaoka Yuki Koyama Masayuki Okada

キーワード PKI, Web サーバ証明書, IP アドレス

あらまし

Web サーバ証明書の設定項目の CN (Common Name) や SAN (Subject Altanative Name) に FQDN (Fully Qualified Domain Name) の代わりにサーバの IP アドレスが設定された証明書 (以後 WebIP 証明書と呼ぶ) が存在する。WebIP 証明書であれば、クライアントが IP アドレスでそのサーバに SSL/TLS 接続しても正しい通信相手として検証される。認証局（Certificate Authority, CA) が WebIP 証明書の発行をする場合、そのルールの中に IP アドレスの利用権や所有権をサーバやサーバ管理者が保持しているかの確認がされていない可能性がある。その結果、本来であればその IP アドレスの所有権を持たない第 3 者がその IP アドレスに対する証明書発行を受けられてしまう可能性がある。

こういったリスクがある中で、どの程度の発行が行われているかの調査についてはこれまでされてこなかった。そこで本研究では全 IPv4 アドレスに対して TLS 接続をし証明書を取得し、WebIP 証明書の存在状況や利用される IPv4 アドレスの特徴を調査した。

主要な Web サーバ証明書発行サービスの規定調査の結果、IP アドレスの確認方法を明記した上で WebIP 証明書の発行を行っていることがわかった。また、2020 年 11 月と 2021 年 8 月に行った WebIP 証明書の実在調査の結果ではそれぞれ 908,071 枚、882,735 枚の証明書を取得した中で WebIP 証明書が 44,628 枚（取得証明書の 4.91%)、45935 枚（取得証明書の 5.20%) が発見された。

* 東邦大学, 千葉県船橋市三山 2-2-1, Toho University, Miyama 2-2-1, Funabachi, Chiba
† 長崎県立大学, 長崎県西彼杵郡長与町まなび野 1-1-1, University of Nagasaki, 1-1-1 Manabino, Nagayo-cho, Nishi-Sonogi-gun, Nagasaki