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

ゼロトラストアーキテクチャにおけるブラウザフィンガープリントを利用したアクセス制御

Access Control Using Browser Fingerprints in Zero Trust Architecture

高木 祥一 *　　大久保隆夫 *
Shoichi TAKAGI　　Takao OKUBO

キーワード ゼロトラストアーキテクチャ，ブラウザフィンガープリント，アクセス制御

あらまし

近年クラウドサービスの急増やモバイルの活用，テレワークの増加等に伴い，社内／社外という境界にフォーカスした境界型セキュリティだけでは脅威の侵入を防ぎきれなくなっていると言われている．ゼロトラストモデルは，2010 年に Forrester Research 社の John Kindervag が [1] において提唱したモデルであり，特定の信頼を想定せず「全てのリソースを検証して安全を確保し，アクセス制御を制限して厳格に実施し，全てのトラフィックを検査して記録しなければならない」という考え方があることから注目を集めている．ゼロトラストアーキテクチャを公的に定義したものとして，2020 年 8 月 11 日に NIST SP 800-207[2] が出版されたが，本文書はゼロトラストアーキテクチャの概念の定義が主であり，実装方法においては具体性が乏しいという問題がある．

[2] ではゼロトラストの基本的な考え方が 7 つ紹介されている．1 つ 1 つの内容としてはセキュリティを確保する上での理想が述べられているが，その実現方式については特に触れられていない．その 7 つのゼロトラストの考え方のうちの 1 つ,「企業リソースへのアクセスは，セッション単位で付与する.」を本稿の焦点とする．セッション開始の度に認証を実施することが最も実現方式として簡易な方法であるが，認証は基本的にユーザの操作が求められるため，ユーザビリティが損なわれることが考えられる．そこでユーザ操作を必要とせずアクセス元の検証ができるものとして，ブラウザフィンガープリントに着目した．ブラウザフィンガープリントとは，JavaScript などを用いてブラウザから UserAgent やブラウザの使用言語等の特徴量を取得する技術であり，ブラウザ識別に関する研究に利用されている．このことから，ユーザ操作を必要とせず取得できるものであり，またブラウザフィンガープリントの値 (BFP 値) が継続して同じであることは，ユーザが継続して同じ環境を利用し続けている確度が高いとも言える．

本稿ではブラウザからアクセスする Web リソースを対象とし，ブラウザフィンガープリントを利用してアクセス制御を行う手法を提案する．具体的には，アクセス元から取得した BFP 値を継続的に検証する機能をリクエスト元と Web リソース間に設けることで，検証済リクエストのみを Web リソースに届ける．手法の提案にあたって，攻撃者による BFP 値の偽装が行われることも想定し，その対策も盛り込んだ．提案手法の評価にあたり提案手法を実装した Web サイトを構築し，クレデンシャル情報の漏えいを仮定した不正アクセスと，セッション (Cookie) ハイジャックによる不正アクセスに対して有効であることを示す．また，ユーザビリティの観点で提案手法適用時に適切な BFP 値の要素についても考察を行う．

参考文献

[1] John Kindervag. Build Security Into Your Network's DNA: The Zero Trust Network Architecture. *Forrester Research.*, Nov 2010.

[2] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. Zero Trust Architecture, NIST Special Publication 800-207. Aug 2020.

* 情報セキュリティ大学院大学, 神奈川県横浜市神奈川区鶴屋町 2-14-1, Institute of Information Security, 2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-city, Kanagawa 221-0835, JAPAN