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

IoT 機器における効率的な真贋判定方式
Efficient authenticity and integrity monitoring technology for IoT devices

千葉伸浩 * 瀧口浩義 * 中嶋良彰 *
Nobuhiro Chiba Hiroyoshi Takiguchi Yoshiaki Nakajima

キーワード IoT セキュリティ

あらまし

IoT(Internet of Things)機器は、工場、ビル、医療現場、家庭等で幅広く使用されている．しかし、これらの機器は、限られたリソースしかなく、十分なセキュリティ対策が行えない場合が多い．このため万一機器内ファイルの改ざんといったサイバー攻撃が行われても、これに早期に気付くことが困難である．

このような攻撃を早期に検知するため、機器内のファイルの整合性等を常時監視することにより、ファイルの改ざんを検知する方式（ソフトウェア真贋判定）が有効である．

ソフトウェア真贋判定は、事前に機器の正常状態のファイルの内容をダイジェスト化したものや、ファイルの属性情報（タイムスタンプ、アクセス権、所有者、サイズ等）を保存しておき，判定時は、この値と、機器で算出したそれぞれの値とを比較することで、ファイルが改ざんされていないかを判定する仕組みである[1],[2],[3].

しかし、ファイル内容をダイジェスト化して比較する検知方法では、ファイル内容の変化を確実に検出することができるものの、ファイル内容を読み込み、ダイジェスト値を生成する部分において、IoT 機器への負荷が大きく、さらに機器本来の動作を妨げないよう使用リソースを制限して判定しようとすると、判定処理に時間がかかることになり、効率的に判定する仕組みが必要である．

また、ファイルの属性情報の比較による検知では、ファイル内容を読み込まない分、負荷が小さいものの、ファイル内容が改ざんされても属性情報が変わらない場合が存在するため、漏れなく検知する仕組みが必要である．

本稿では、リソースの少ない IoT 機器であっても、機器内ファイルの改ざんに早期に気付くことができるよう、ファイルの格納領域の位置情報と、ファイルの属性情報を組み合わせて用いることで、効率的に、漏れなく改ざんを検知可能な、新たな方式を提案する．

ファイルの格納領域の位置情報とは、機器のファイルシステム上で、ファイルが保存されている場所を示す情報であり、例えば Linux のファイルシステムである ext2 では、データブロック番号が該当する．ファイルシステムの特性上、ファイルが更新された際、ファイルシステム上の別の位置にファイルが保存しなおされる場合がある．

本方式ではこれを応用し、ファイルの位置と属性情報の組み合わせが正常状態から変化した場合、ファイルが改ざんされたと判断する．

最後に、本方式について、試験環境で効率性や検知漏れがないかについて、想定される改ざんパターンをもとに動作検証を行い、本方式の有効性について、評価を行った．

参考文献

[1] Kim, G.H. and Spafford, E.H., “The design and implementation of tripwire: a file system integrity checker”, Proc. 2nd ACM Conference on Computer and Communications
[2] トリップワイヤ・ジャパン,
https://blog.tripwire.co.jp/blog/check-point-for-website-security
[3] 大貫 大輔,
https://atmarkit.itmedia.co.jp/ait/articles/0203/19/news002_2.html

* NTT 社会情報研究所, 〒180-8585 東京都武蔵野市緑町 3-9-11,
NTT Social Informatics Laboratories ,3-9-11 Midori-cho,
Musashino-shi, Tokyo 180-8585,Japan.