

多点観測型多要素認証:単一クレデンシャルによる多要素認証の達成

Multi-Observed Multi-Factor Authentication:A Multi Factor Authentication Using Single Credential

野崎真之介* 芹澤歩弥* 吉平瑞穂* 藤田真浩† 柴田陽一†
山中忠和† 松田規† 大木哲史* 西垣正勝*
Shinnosuke Nozaki* Ayumi Serizawa* Mizuho Yoshihira*
Masahiro Fujita† Yoichi Shibata† Tadakazu Yamanaka† Nori Matsuda†
Tetsushi Ohki* Masakatsu Nisigaki*

キーワード ユーザ認証, 多要素認証, ユーザブルセキュリティ

あらまし

今やPCのマルウェア感染は日常茶飯事であり、パスワード等のクレデンシャル単体のみを用いたユーザ認証においては、正規クレデンシャルの入力自体を以って正規ユーザであると断定することができないという現状にある。この問題に対する典型的な解決策が2要素認証である。一般的な2要素認証は、正規クレデンシャル(記憶情報/所持情報/生体情報)を2つ用意し、第1クレデンシャルを被認証者のPCに、第2クレデンシャルを被認証者のスマートフォンに入力することで被認証者を認証する。すなわち2要素認証とは、「認証の多重化」によって安全性を強化する方法だと言える。しかし、認証が多重化するという事は、認証の度に被認証者に複数のクレデンシャル提示が強いられることを意味し、利便性の低下を引き起こしてしまっている。利便性の向上のみを考えた場合には、所持情報(スマートフォンを所持していること)を第2要素のクレデンシャルとして採用し、PCがスマートフォンの近接を自動的に確認することによって2要素目の認証を完了させるという方法も考えられる。しかしこの方法では、PCに感染したマルウェアが正規ユーザのPCでの業務中に第1クレデンシャルを不正入力すると、第2要素の認証も通過してしまう。すなわち、1要素のみの認証と同義となってしまう。

2要素認証が必要となる理由が、PCへのマルウェア感染にあるのならば、被認証者が正規ユーザであることを

証明するために、わざわざもう一つ別のクレデンシャルを用いずとも、「(マルウェアではなく)人間が正規クレデンシャルを入力した」ことを確認すれば十分ではないだろうか。この結果、被認証者はこれまで通り自身のPCに1つのクレデンシャルを入力するだけで済むため、利便性を維持しつつ、安全性を向上させることができる。

そこで我々は、「人間による正規クレデンシャルの入力」を確認するというコンセプトに立脚する新たなユーザ認証方式として、多点観測型多要素認証を提案する。提案方式は、被認証者による単一の正規クレデンシャルの入力を、多点で観測することによって多要素認証を達成する認証方式である。

本稿では、多点観測型多要素認証の典型的な具体例についても提案する。提案方式は、被認証者がPCとスマートフォンを所持しており、ワイヤレスキーボードとワイヤレスマウスを用いてPCを操作するような利用シーンを想定している。そして、提案方式が使用するワイヤレスキーボードとワイヤレスマウスにおいては、キーボードならびにマウスの操作が被認証者のスマートフォンにおいても受信できるように改造されているということが提案方式の前提となる。ユーザ認証の実施にあたり、被認証者は自身のPCに正規クレデンシャルを入力する。その入力はPCとスマートフォンの双方に同時に届き、PCとスマートフォンがそれぞれ個別に入力されたクレデンシャルの正当性を確認する。人間によってキーボードやマウスが物理的に操作された場合にのみワイヤレス信号が発信されるため、PCにマルウェアが感染していたとしても、当該マルウェアがワイヤレス信号をスマートフォンに送ることはできない。スマートフォンにマルウェアが感染していた場合も同様である。

* 静岡大学, 〒432-8011 静岡県浜松市中区城北 3-5-1, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011, Japan.

† 三菱電機, 〒247-8501 神奈川県鎌倉市大船 5-1-1, Mitsubishi Electric Corporation, 5-1-1 Ofuna, Kamakura, Kanagawa, 247-8501, Japan.