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

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

# 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 Nishigaki*

**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． 2 要素認証とは，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，一般的には 1 つ目を PC に，2 つ目をスマートフォンに入力することによって被認証者を認証する．しかし，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ため，利便性が低下してしまっている．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，正規ユーザであることの証明にわざわざもう 1 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．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，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多点観測型多要素認証を提案する．

**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

## 1. はじめに

近年，DX（デジタルトランスフォーメーション）に伴う業務体系の変化に対応しきれていない個人や企業を対象に，Emotet 等のクレデンシャルを窃取するマルウェアによって被害が拡大している現状にある[1]．クレデンシャルを窃取したマルウェアが PC に常駐している以上，認証サーバが PC から受け取ったクレデンシャルが正規ユーザからなのかマルウェアからなのか判別をすることは困難となる．そのため，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．

この問題に対する典型的な解決策が 2 要素認証である．2 要素認証とは，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，一般的には 1 要素目のクレデンシャルを被認証者の PC に，2 要素目の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[2][3]．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ことは，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 2 要素目のクレデンシャルとして採用し，スマートフォンが PC 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，正規ユーザが PC を用いて業務を行っている際にマルウェアが第 1 クレデンシャルを不正入力すると，2 要素目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

* 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.
† 三菱電機株式会社，〒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.

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 1 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，PC とスマートフォンで同時に観測することによって，「人間による正規クレデンシャルの入力」を確認する．提案方式によって利便性と安全性を両立した 2 要素認証が達成される．

なお，PC の利用形態や攻撃者の脅威モデルによっては，スマートフォンで確認すべき内容が，「人間が正規クレデンシャルらしき情報を入力した」こと，あるいは，「正規ユーザが正規クレデンシャルを入力した」ことに変更される．本稿では，これらの場合に対する提案方式の改良についても提案する．

本稿では，説明を簡素にするために 2 要素認証に焦点を当てて議論を進めるが，提案方式は 3 要素以上の多要素認証にも拡張可能である．以降，2 章で既存の 2 要素認証について整理し，2 要素認証の要件を示す．3 章では 2 点観測型多要素認証のコンセプトと具体的な実現方式を説明し，提案方式の利便性と安全性を評価する．4 章では提案方式の変更とリスクに関して考察する．5 章はまとめである．

## 2. 2 要素認証

COVID-19 が DX を後押しする形で在宅ワークが浸透した．社員は自宅の PC で業務を行うにあたり，必要に応じて社内クラウドの情報資産にアクセスする．社内データへのアクセスの都度，社員にはユーザ認証が求められる．これに伴い，社員の PC に感染してユーザ認証用のクレデンシャルを盗取するマルウェアが急増している [1].

### 2.1 単要素認証と 2 要素認証

単要素認証では，正規ユーザのみが所有するクレデンシャル (記憶情報／所持情報／生体情報)) が提示されたことを根拠に，認証サーバが被認証者を正規ユーザであると判断する．なりすまし耐性の観点からは所持情報や生体情報の使用が推奨されるが，利便性 (複数デバイスを跨っての情報アクセスができない) やプライバシ (生体情報の登録・管理が必要となる) の観点から記憶情報を用いた単要素認証が一般的となっている．

PC で業務を行っている社員が記憶情報 (パスワード) を用いて社内データにアクセスする場合，単要素認証の流れは次のようになる (図 1)．

1. 被認証者が PC にパスワード PW を提示する．
2. PC は提示された PW を認証サーバに送信する．
3. 認証サーバは PC から受信した PW をもとに被認証者が正規ユーザであるか否かを判断する．

なお，図 1 においては，手順 1 と手順 2 の PW を区別するために，それぞれを PW，$PW_{PC}$ と書き分けている．実際には PW＝$PW_{PC}$ である．

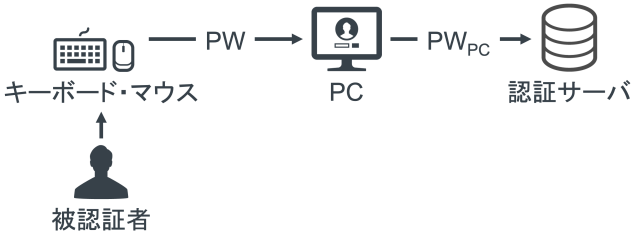


図 1　単要素認証

ここで，社員 (正規ユーザ) の PC がマルウェアに感染していると想定した場合，”正規ユーザのみが所有する”というクレデンシャルの前提が崩れるため，認証サーバは，PW が提示されたことのみをもって被認証者の本人性を判別することはできなくなる．この問題に対する典型的な解決策が，2 つのクレデンシャルを用いる 2 要素認証である．

社員の PC に感染しているマルウェアは，自律的あるいは不正者の遠隔操作によって，感染 PC から認証サーバに PW を送信することができる．このため，社員 (正規ユーザ) の PC を登録し，登録 PC (所持情報) と PW (記憶情報) による 2 要素認証とする方法は悪手である．また，マルウェアは，感染 PC に入力される任意の情報を盗取することも可能である．このため，2 つ目のクレデンシャルを社員の PC を経由して認証サーバに送信する形の 2 要素認証も得策ではない[1]. 以上より，現在では，スマートフォンを 2 つめのクレデンシャルとして関与させた 2 要素認証が一般的となっている．PC とは異なる認証経路が確保されることによって，PC がマルウェアに感染し第 1 クレデンシャル (PW) が窃取された場合でも，スマートフォンの認証が突破されない限り，なりすましは防がれる．

本稿では以降， PC とスマートフォンの構成による 2 要素認証 (図 2) を具体例として議論を進めていく．図 2 では，第 1 クレデンシャルを PW，第 2 クレデンシャルを PIN と示しているが，記憶情報以外のクレデンシャルを用いてもよい．なお，実際の認証手順としては，PC からの PW が認証サーバに届いた時点で，認証サーバからスマートフォンに PIN の入力を要求する形となるが，

[1] ワンタイムパスワード (OTP) を第 2 クレデンシャルとして採用できる場合には，この限りではない．例えば方式[3]では，認証サーバからスマートフォンに届いた OTP を，ユーザが PC 経由で認証サーバに提示するという 2 要素認証を構成している．

図 2 ではその記載を省略している．図 2 においても，被認証者が入力するクレデンシャルと認証サーバに送られるクレデンシャルを区別するために，それぞれを PW，$PW_{PC}$，PIN，$PIN_{SP}$ と書き分けている．実際には PW＝$PW_{PC}$，PIN＝$PIN_{SP}$ である．

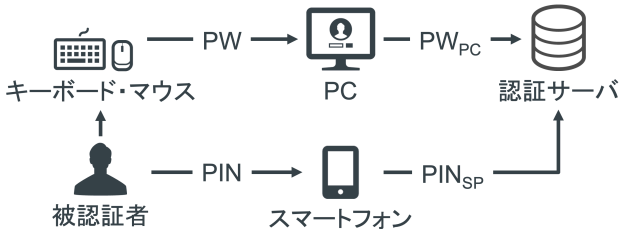


図 2　2 要素認証

## 2.2　2 要素認証の課題

図 2 では 2 つのクレデンシャルを PW，PIN として示したが，被認証者の実際の操作としては，PC にログインした上で PW を入力し，かつ，スマートフォンをアクティベートした上で PIN を入力することになる．これを正確に記すと，図 2 は図 3 となる．ここで，

- $AC_{PC}$ : 被認証者が PC にログインする際に，被認証者が PC に対して入力する PC アクティベート用のクレデンシャル．
- PW : 被認証者が情報資産にアクセスする際に，被認証者が PC に対して入力する第 1 クレデンシャル．PC から認証サーバに送られる．
- $AC_{SP}$ : 被認証者がスマートフォンを使用する際に，被認証者がスマートフォンに対して入力するスマートフォンアクティベート用のクレデンシャル．
- PIN : 被認証者が情報資産にアクセスする際に，被認証者がスマートフォンに対して入力する第 2 クレデンシャル．スマートフォンから認証サーバに送られる．

である．図 3 においても，被認証者が入力するクレデンシャルと認証サーバに送られるクレデンシャルを区別するために，それぞれを PW，$PW_{PC}$，PIN，$PIN_{SP}$ と書き分けている．実際には PW＝$PW_{PC}$, PIN＝$PIN_{SP}$ である．

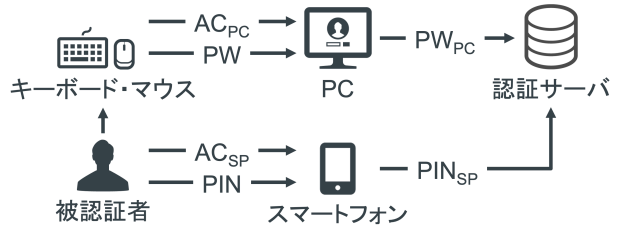


図 3　2 要素認証の詳細

社員の PC 業務中は，社員の PC は常にアクティベートされている状態にある．すなわち，PC への $AC_{PC}$ の入力は不要である．また，社員が社内データにアクセスする時点で，社員は PC に対峙している．このため，PC への PW の入力は，社員（正規ユーザ）にとってそれほど大きな負担となるものではない．これに対し，基本的には PC 業務中に社員がスマートフォンを操作し続けることはないため，スマートフォンはアクティベートされていない状況にある．よって，スマートフォンへの $AC_{SP}$ の入力は必ず必要となる．その一方で， PIN に関しては，PIN をスマートフォンに格納しておき，（被認証者からの $AC_{SP}$ の入力が確認できたという条件の下に）スマートフォンが自動的に PIN（$PIN_{SP}$）を認証サーバに送信するという方法を採用することが可能である．

以上より，図 3 において大儀となるのは，$AC_{SP}$ の入力である．社員（被認証者）には認証のたびに業務とは関係ないスマートフォンに意識を向ける必要が生じる．情報資産の大部分が社内クラウドに格納されている現在においては，社内データへのアクセスが頻繁に発生する．その度にスマートフォンのアクティベートが要求される 2 要素認証は，被認証者の操作コストを激増させてしまい，社員の業務効率の低下を招いてしまう．よって，利便性の観点からは，正規ユーザにスマートフォンを意識させない 2 要素認証が求められる（要件 1）．

## 2.3　2 要素認証の利便性改善に関する既存研究

既存研究[4]では，被認証者の状況に応じて動的に認証方法を変更するコンテキストアウェア認証のアイデアが提案されている．認証サーバが被認証者の所持するスマートカードを検知し，認証サーバとスマートカードが近接している場合は，自動でユーザ認証が実施される．認証サーバとスマートカードの近接が確認できない場合には，被認証者にパスワードの入力が求められる．コンテキストアウェア認証を利用することで，2 要素目の認証を自動化できる．認証サーバに PW（$PW_{PC}$）が届いた時点で，認証サーバからスマートフォンに 2 要素目の認証要求が送られ，スマートフォンが PC との近接を確認できたならば，スマートフォンから認証サーバに PIN（$PIN_{SP}$）が送信される．

また，既存研究[5]では，被認証者にユーザ認証の存在を意識させない認証を「非積極的認証」と呼び，その例として動画顔認証を紹介している．非積極的認証を利用することで，2 要素目の認証を自動化できる．認証サーバに $PW_{PC}$ が届いた時点で，認証サーバからスマートフォンに 2 要素目の認証要求が送られ，スマートフォンが動画顔認証によって被認証者の存在を確認できたならば，スマートフォンから認証サーバに PIN（$PIN_{SP}$）が送信される．

両既存研究のようにスマートフォンが被認証者を自動で認証することで，スマートフォンのアクティベートに起因する 2 要素認証の利便性低下を抑えることはできる．しかし，社員が使用している PC にマルウェアが感染している状況においては，このような自動化による対処では不十分となる．PC 内に潜むマルウェアが，社員が PC を用いて業務を行っている最中に，バックグラウ

ンドで PW（$PW_{PC}$）を認証サーバに送信した場合，スマートフォン側で社員（正規ユーザ）の存在が確認できてしまい，認証サーバに PIN（$PIN_{SP}$）が自動的に送信されてしまう．すなわち，社員の PC 業務中においては，マルウェアは造作もなく 2 要素認証を突破することができてしまう．2 要素目の認証を自動化する場合であっても，被認証者に認証の意思を確認する必要が残る．よって，安全性の観点からは，正規ユーザの認証の意思が確認できる 2 要素認証が求められる（要件 2）．

## 3. 多点観測型多要素認証

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，認証の多重化は，認証の度に被認証者に複数のクレデンシャル提示を強いることになる．特に認証操作が頻発するゼロトラスト環境下では，2 要素認証の導入による利便性低下は著しい．単純に 2 要素目の認証を自動化するだけでは，安全性が担保されない．本章では，利便性と安全性を兼ね備えた新しい形式の 2 要素認証を提案する．

### 3.1 コンセプト

前章にて説明した 2 要素認証に求められる要件を以下にまとめる．

(要件1) 正規ユーザにスマートフォンを意識させない．

(要件2) 正規ユーザの認証の意思を確認できる．

ここで，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，わざわざもう 1 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」ことを確認することができれば，2 要素認証の目的が達成されることに気付く．

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．PC とは異なる認証経路を設けることが 2 要素認証の本質である．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，2 経路（PC とスマートフォン）で同時に観測することによって，「確かに人間が正規クレデンシャルを入力した」ことを確認する認証方式となっている．

### 3.2 基本方式（方式 A）の認証手順

本節では，多点観測型多要素認証の具体的な認証手順を説明する（図 4）．なお，本稿では 4 章にて本節の認証手順の変更版についても説明する．このため本稿では，本節の認証手順を「基本方式（方式 A)」と呼称し，4 章の「変更方式（方式 B，方式 C)」と呼び分ける．

提案方式が用いるクレデンシャルは，パスワード PW である．提案方式の実現にあたり，PC へのキーボード入力，マウス入力が，スマートフォンにも複製されて入力されることを前提とする．典型的には，ワイヤレスキーボードおよびワイヤレスマウス（本稿では以降，「ワイヤレス入力デバイス」と呼ぶ）が PC と接続されており，かつ，キーボードとマウスの操作が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想定を置く．

多点観測型多要素認証の基本方式（方式 A）の流れは次の通りである（図 4）．

1. 被認証者は PC を用いて業務を行っている（PC はアクティベートされている）．
2. 被認証者が，認証サーバに情報資産へのアクセスを要求する．
3. 認証サーバは，スマートフォンに PC 入力の受信開始を指示する．
4. スマートフォンは，ワイヤレス入力デバイスからの信号の受信を開始する．
5. 認証サーバは，PC に認証画面の表示を指示する．
6. PC は認証画面を表示する．
7. 被認証者が，ワイヤレス入力デバイスを用いて PC に PW を入力する．
8. PC は PW を認証サーバに送信する．
9. 被認証者が手順 7 で入力した PW は，スマートフォン側でも受信できている．スマートフォンも PW を認証サーバに送信する．
10. 認証サーバは，PC から受信した PW とスマートフォンから受信した PW の正当性を確認する．確認できた場合には，被認証者を正規ユーザと判定する．
11. 認証サーバは，スマートフォンに PC 入力の受信終了を指示する．
12. スマートフォンは，ワイヤレス入力デバイスからの信号の受信を停止する．

図 4 においては，手順 7，手順 8，手順 9 の PW を区別するために，それぞれを PW，$PW_{PC}$，$PW_{SP}$ と書き分けている．実際には $PW=PW_{PC}=PW_{SP}$ である．$AC_{PC}$ は PC アクティベート用のクレデンシャルである．被認証者が PC を用いて業務を開始する時点（手順 1 よりも前）で，被認証者は $AC_{PC}$ を入力することによって PC へのログインを済ませている．次節で説明するが，基本方式 A においては，スマートフォンアクティベート用のクレデンシャル $AC_{SP}$ は不要である．

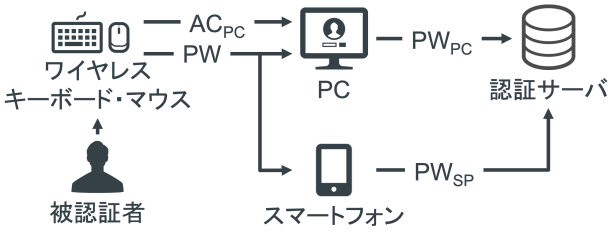


図 4　2 点観測型 2 要素認証（方式 A）

### 3.3 評価

利便性（要件 1）と安全性（要件 2）の観点から基本方式（方式 A）を評価する．

基本方式 A においては，被認証者に求められるのは PC への PW の入力（手順 7）のみである．よって，基本方式 A は利便性に関する要件 1 を満たす．また，基本方式 A は，被認証者からはパスワードを用いた単要素認証に見える．被認証者にとって慣れ親しんだパスワード認証であるため，ユーザの心的面の観点からは，基本方式 A の導入障壁は皆無である．PC への入力がスマートフォンにも転送されることは，プライバシの観点からの懸念を孕み得る．しかし，基本方式 A においては，PC 入力のスマートフォンへの同報が働くのは手順 7 の間のみであるため，ユーザの心的負担は限定的であると期待される．

PC 内に潜むにマルウェアは，手順 8 の PW 送信を不正に実行することはできるが，物理的にキーボードやマウスを操作することは不可能であるため，手順 7 を行うことができない．従って，手順 9 でスマートフォンが受信した PW は，手順 7 で被認証者自身が入力した PW であると同定できる．すなわち，手順 9 のスマートフォン側の PW の受信が，被認証者が自らの意思によってクレデンシャルを入力したことの証左となる．よって，基本方式 A は安全性に関する要件 2 を満たす．

既存の 2 要素認証（図 3）において，スマートフォンアクティベート用のクレデンシャル $AC_{SP}$ が要求される理由は，被認証者の認証の意思をスマートフォン側で確認する必要があるためである．基本方式 A においては，手順 9 によって被認証者の意思確認が行われるので，手順 9（スマートフォンの PW 受信）をもって，スマートフォンをアクティベートしても支障はない．すなわち基本方式 A では，スマートフォンアクティベート用のクレデンシャル $AC_{SP}$ の確認については省略可能である（このため図 4 には $AC_{SP}$ が記載されていない）．これにより，要件 1（正規ユーザにスマートフォンを意識させない）を満たしながら，要件 2（正規ユーザの認証の意思を確認できる）が達成されている．

## 4. 考察

### 4.1 PW 検査を緩和した変更方式（方式 B）

2 章冒頭で示したように，本稿は社員の在宅ワークを想定して議論を進めてきた．このため 3 章で提案した基本方式 A は，正規ユーザの周囲（物理的近傍）に不正者が存在していないという環境での 2 要素認証となっている．物理的近傍に不正者が居ない以上，不正者にキーボードやマウスが物理的に操作されることはない．すなわち，キーボードやマウスを用いて物理的に PW が入力されたならば，それは被認証者（正規ユーザ）本人によって入力された正規クレデンシャルであると判断して良い．

ここで，「物理的近傍に不正者が居ない以上，不正者にキーボードやマウスが物理的に操作されることはない」という道理からは，キーボードあるいはマウスが物理的に操作されさえすれば「被認証者の意思の介在」を認めてしまってよいようにも思える．しかし，次に説明する通り，その考えは早計である．2.3 節で述べたように，PC 内に潜むマルウェアは，社員が PC を用いて業務を行っている最中に，バックグラウンドで PW を認証サーバに送信することができる．この結果，基本方式 A の手順（3.2 節）が実行されるが，このとき社員は他の業務のために PC（キーボードやマウス）を操作しているので，手順 9 でキーボードやマウスの操作が観測されてしまう．よって，被認証者の認識の意思を確認するためには，キーボードあるいはマウスから正規クレデンシャル PW が入力されたことを検査する必要がある．基本方式 A では，この検査を手順 10 で行っている．

ただし，社員の「正規業務内のキーボード操作，マウス操作」と「PW 入力の際のキーボード操作，マウス操作」が大きく異なる場合には，PW の完全一致を確認せずとも，「PW らしき情報が入力された」ことを確認するだけでも十分とみなすことも可能である．例えば，マウス操作のみで完了する正規業務を担当している社員の場合，キーボードの使用が認証操作時に限られるのであれば，キーボード操作の発生をもって「PW らしき情報が入力された」と判断できる．本稿では，基本方式 A に対し，PW 入力の検査を緩和した変更方式を方式 B と呼ぶ．

### 4.2 キーストローク認証を併用した変更方式（方式 C）

不正者（マルウェアと結託した人間）が社員（正規ユーザ）の PC に物理的に接近することが可能な場合には，社員が PC を置いて離席している隙を狙って，マルウェアが窃取した PW を不正者が PC に直接入力することが可能である．このような環境においては，「PC に正規クレデンシャル PW が入力された」ことを確認するだけでは不十分であり，「PW を入力したのは（マルウェアでもなく不正者でもなく）正規ユーザである」ことを確認する必要が生じる．その場合には，PW の正当性を確認すること以外に，被認証者（PW を入力した社員）が正規ユーザであることを確認するためのクレデンシャルがもう 1 つ必要となってくる．

これを効率良く実現するために，本稿では，基本方式 A（3.2 節）の手順 9 において，スマートフォンに届いた PW 入力に対してキーストローク認証を追加するという変更を提案する．これにより，被認証者にはこれまで通り手順 8 の操作（PC への PW 入力）を行ってもらうだけで，PW の正当性（PW が正規クレデンシャルと一致するか）の確認と被認証者の本人性（PW を入力したユーザが正規ユーザであるか）の確認を同時に達成する．本稿では，基本方式 A に対し，キーストローク認証を追

加した変更方式を方式 C と呼ぶ.

キーストローク認証の実装については，既存のテキスト指定型キーストローク認証をそのまま採用可能である. 例えば既存研究[6]では，ユーザのパスワード入力時のキー入力のダイナミクス（タイミング，スピード，リズムなど）の相違を，XGBoost を用いて識別することによって，認証精度 93.59%のキーストローク認証を実現している．なお，パスワード入力時のキー入力音の相違を用いたキーストローク認証[7]もあるが，著者らが調査した範囲ではダイナミクスを用いる方式のほうが認証精度は高かったため，変更方式 C ではキーダイナミクスを用いたキーストローク認証の採用を想定している.

キーストローク認証の利用にあたっては，事前にユーザ登録が必要となる. 具体的には, 被認証者が PC に PW を入力する際のキーストローク情報を（必要であれば複数回）登録する．「事前に登録したキーストローク情報」と「手順 8 で入力された PW のキーストローク情報」を比較することによって, 正規ユーザか否かが判定される.

3.3 節で説明した通り，基本方式 A においては，被認証者の PC への入力がスマートフォンに同報されるのは手順 7 の間のみである．変更方式 C においても，手順 7 にて被認証者が PC に PW を入力する際のキーストローク情報のみを用いて被認証者の本人性が確認される．このように, 変更方式 C もユーザのプライバシに配慮した方式となっている.

### 4.3 提案方式特有のリスク

提案方式 (基本方式 A, 変更方式 B, 変更方式 C) は, PC とスマートフォンの両者と接続されるワイヤレス入力デバイスの使用を前提とした認証方式となっている. Bluetooth のペアリングは 1 対 1 の接続が基本となるため，提案方式を実装するにあたっては，無線通信プロトコルの改造が必要となる．よって，フィージビリティの観点からは，提案方式の導入障壁は無視できない.

また，無線通信プロトコルに脆弱性が存在していた場合には，提案方式に対するリスクが生じる．例えば，ワイヤレス入力デバイス内のデバイスドライバがマルウェアによって自在に改竄可能であった場合[8]が，その典型例である．正常であれば，キーボードやマウスの通信は一方向（ワイヤレス入力デバイス→PC）であるが，マルウェアによって双方向通信型のデバイスドライバにすり替えられてしまうと，PC に感染しているマルウェアがワイヤレス入力デバイスを操作することが可能になってしまう.

基本方式 A および変更方式 B においては, これは致命的なセキュリティホールとなる. 変更方式 C についても, マルウェアによって正規ユーザのキーダイナミクスまで偽装された場合には認証が突破されてしまう．この問題に対しては，マルウェアがワイヤレス入力デバイスを双方向通信型に変更していることを逆手に取り，スマートフォン側からワイヤレス入力デバイスのデバイスドライバの真贋性を，コード署名を用いて検証するという対策が可能ではないかと考えている．具体的な解決方法については今後の課題とする.

## 5. まとめ

本稿では，2 要素認証が抱える利便性の問題点をもとに,「マルウェアではなく人間による正規クレデンシャルの入力」を PC とスマートフォンでそれぞれ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した. 提案方式の具体例（基本方式 A，変更方式 B，変更方式 C）を示し，利便性と安全性の観点から提案方式を評価した．引き続き，提案方式の実装を進め，実機を用いての利便性，安全性評価を行う予定である.

## 参考文献


[1] 独立行政法人情報処理推進機構セキュリティセンター: コンピュータウイルス・不正アクセスの届出状況 [2020 年（1 月~12 月）], （オンライン）, 入手先< https://www.ipa.go.jp/files/000088692.pdf >（参照 2021-12-23）.

[2] Microsoft: 動作のしくみ: Azure AD Multi-Factor Authentication, Microsoft（オンライン）, 入手先< https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/concept-mfa-howitworks >（参照 2021-12-23）.

[3] Amazon: ユーザープールへの多要素認証 (MFA) の追加，Amazon（オンライン），入手先< https://docs.aws.amazon.com/ja_jp/cognito/latest/developerguide/user-pool-settings-mfa.html >（参照 2021-12-23）.

[4] Bardram, Jakob E., Rasmus E. Kjær, and Michael Ø. Pedersen. "Context-aware user authentication-supporting proximity-based login in pervasive computing." Internationa Conference on Ubiquitous Computing. Springer, Berlin, Heidelberg, 2003.

[5] 鈴木 武志, 動画顔認証を中心とした生体認証技術：現状と，安全・安心な社会の実現に向けて，情報管理, 2017-2018, 60 巻，8 号，p. 564-573, 公開日 2017/11/01,https://www.jstage.jst.go.jp/article/johokanri/60/8/60_564/_article/-char/ja,

[6] S. Singh, A. Inamdar, A. Kore and A. Pawar, "Analysis of Algorithms for User Authentication using Keystroke Dynamics," 2020 International Conference on Communication and Signal Processing (ICCSP), 2020, pp. 0337-0341, doi:

10.1109/ICCSP48568.2020.9182115.

[7] C. Tietz, E. Klieme, L. Behrendt, P. Böning, L. Marschke and C. Meinel, "Verification of Keyboard Acoustics Authentication on Laptops and Smartphones Using WebRTC," 2019 3rd Cybersecurity in Networking Conference (CSNet), 2019, pp. 130-137, doi: 10.1109/CSNet47905.2019.9108962.

[8] Choi, Byung-jun and Suh, Taeweon, “A Security Program To Protect against Keyboard-Emulating BadUSB,” Journal of the Korea Institute of Information Security & Cryptology, vol. 26, no. 6, pp. 1483–1492, Dec. 2016.