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（その 2）

野崎 真之介[1]　芹澤 歩弥[1]　吉平 瑞穂[1]
藤田 真浩[2]　吉村 礼子[2]　大木 哲史[1]　西垣 正勝[1,*]

概要：今や PC のマルウェア感染は日常茶飯事であり，パスワード等の正規クレデンシャルの提示のみをもって正規ユーザであると断定し切れないという状況にある．この問題に対する典型的な解決策が多要素認証であるが，認証の度に複数のクレデンシャルを提示する必要が生じ，ユーザビリティが低下してしまう．多要素認証が必要となる原因が PC へのマルウェア感染にあるならば，正規ユーザの証明のために複数のクレデンシャルを確認せずとも，「人間が正規クレデンシャルを提示した」という事実を確認すれば十分ではないだろうか．そこで我々は，「クレデンシャルの正当性に加え，人間による物理的な認証行為の発生を確認する」というコンセプトに基づいた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．提案方式においては，ユーザの提示した単一の正規クレデンシャルが多点で同時に観測されることが，「正規ユーザが実際に認証行為を行った」という事象発生の証左となり，これにより多要素認証と同等の効果が達成される．本稿では，提案方式の実装を行い，6 名の実験協力者による基礎実験を通じて利便性，プライバシ，認証時間の観点から提案方式を評価した．

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

Multi-Observed Multi-Factor Authentication:　A Multi-Factor Authentication Using Single Credential (part 2)

Shinnosuke Nozaki[1]　Ayumi Serizawa[1]　Mizuho Yoshihira[1]
Masahiro Fujita[2]　Ayako Yosimura[2]　Tetsushi Ohki[1]　Masakatsu Nishigaki[1,*]

Abstract: Nowadays, it is no longer uncommon for a PC to be infected with malware. User authentication based on only one legitimate credential (such as a password) may be insufficient for judging whether a user is legitimate. A typical solution to this problem is two-factor authentication, which is a method of authentication based on the presentation of two factors by the user. However, this reduces usability by forcing the user to present multiple factors at each authentication. Therefore, we proposed a method called multi-observed multi-factor authentication, whereby multi-factor authentication is performed to confirm that a human has input a legitimate credential by observing the user's input of a single legitimate credential at multiple points. In this method, a single legitimate credential is observed at multiple points simultaneously. Thereby, it provides proof of the occurrence of the event that " a legitimate user has actually performed the authentication action," and thus has the same effect as multi-factor authentication. In this study, we implemented the proposed method and evaluated usability, privacy, and authentication time through the results of basic experiments with six research participants.

Keywords: User Authentication, Multi-Factor Authentication, Usable Security

1. はじめに

近年，急速な 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，社員固有の認証情報（以降，社員をユーザ，社員固有の認証情報をクレデンシャルとする）を窃取するマルウェアの被害が拡大している[1]．DX 環境では，ユーザは PC からクラウド業務システムにログインして業務を行う．ここで，クレデンシャルを窃取したマルウェアが PC に常駐していることを想定すると，認証サーバは 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を判別することは困難となる．このことから，クレデンシャル単体のみを用いた単要素認証では，正規クレデンシャルの提示自体を以って正規ユーザであると断定し切れない．

この問題に対する典型的な解決策が多要素認証である．多要素認証は次の 3 つの要素のうち 2 つ以上のクレデンシャルを提示することで正規ユーザであることを証明する[2].

1. 知識情報：パスワードなどの，正規ユーザのみが知っている情報

1 静岡大学
Shizuoka University
2 三菱電機株式会社
Mitsubishi Electric Corporation
* nisigaki@inf.shizuoka.ac.jp

2. 所持情報：ID カードやスマートフォンなどの，正規ユーザのみが所持するものに付随する情報
3. 生体情報：顔情報や指紋情報など，正規ユーザ特有の身体的な情報

一般的には，1 要素目のクレデンシャルを PC に，2 要素目のクレデンシャルをスマートフォンに提示することで認証が行われている[3][4]．すなわち多要素認証とは，「認証の多重化」によって安全性を強化する方法だといえる．しかし，認証の度に複数のクレデンシャルの提示を強いることを意味し，利便性の低下を引き起こしている．ここで，利便性の向上のみを考えた場合，所持情報（スマートフォンの所持）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 との近接を自動的に検出することによって 2 要素認証を完了させる方法が考えられる[5]．しかしこの方法では，マルウェアが事前に窃取した 1 要素目のクレデンシャルを正規ユーザの PC 業務中に送信することで，2 要素目の認証が通過されてしまう．すなわち，単要素認証と同義となってしまう．

多要素認証が必要となる原因が PC へのマルウェア感染にあるならば，正規ユーザの証明のために複数のクレデンシャルを確認せずとも，「人間が正規クレデンシャルを提示した」という事実を確認すれば十分ではないだろうか．そこで我々は，「クレデンシャルの正当性に加え，人間による物理的な認証行為の発生を確認する」というコンセプトに基づいた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[6]．ユーザの提示した単一の正規クレデンシャルが多点で同時に観測されることが，「正規ユーザが実際に認証行為を行った」という事象発生の証左となり，これにより多要素認証と同等の効果が達成される．

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応用可能である．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 2 要素認証のコンセプトを説明し，4 章では提案方式の実装を行い，6 名の実験協力者による基礎実験を通じて利便性，プライバシ，認証時間の観点から提案方式を評価する．5 章では提案方式のリスクに関して考察を行う．6 章にてまとめを述べる．

2. 2 要素認証

COVID-19 の感染拡大に伴い，在宅での勤務が浸透してきている．社員は自宅での PC 業務を行うにあたり，必要に応じて社内クラウド内の情報資産に認証を経た上でアクセスを行う．この業務形態の変化を狙い目として，社員の PC に感染し，認証用のクレデンシャルを窃取するマルウェアが急増している[1]．そんなマルウェアへの不正対策として，認証方式の強化が求められており，現在，多くの企業で 2 要素認証の利用が広がっている．

2.1 単要素認証と多要素認証

単要素認証は，正規ユーザのみが所有するクレデンシャル（知識/所持/生体）が提示されたことを根拠に，認証サーバがユーザの正当性を判断する．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ている反面，利便性（認証トークンを携帯する負担）やプライバシ（認証サーバに生体情報を登録することへの抵抗）の観点から，知識情報を用いた単要素認証が一般的となっている．

PC で業務を行うユーザが知識情報，例えばパスワードを用いて社内クラウド内の情報資産にアクセスを行う場合，単要素認証の流れは次のようになる．（図 1）

【単要素認証】
1. ユーザは PC にパスワード（PW）を入力
2. PC は入力された PW を認証サーバに送信
3. 認証サーバは PC から受信した PW をもとに，ユーザが正当か否かを判断

なお，図 1 では，ユーザが提示したクレデンシャルと認証サーバに送信されるクレデンシャルをそれぞれ PW，PW_{PC} と書き分けているが，実際には PW=PW_{PC} である．

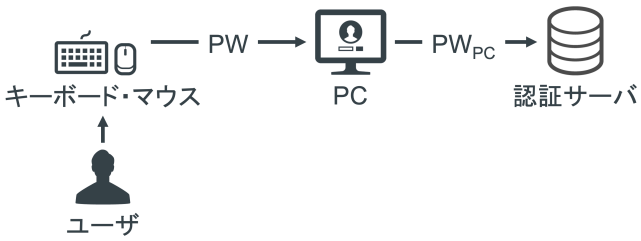

図 1 単要素認証

Fig. 1 Single-factor Authentication

ここで，PC がマルウェアに感染していると想定した場合，マルウェアも PW を持ち得ることとなり，”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．そのため，認証サーバは PW_{PC} の確認をもってユーザの正当性を判断することができなくなってしまう．この問題に対する典型的な解決策が，2 つの正規クレデンシャルを用いる 2 要素認証である．

PC がマルウェアに感染すると，PC はマルウェア（あるいは，マルウェアを遠隔操作する不正者）によって操作される可能性がある．そのため，ユーザの PC 自体を 2 要素目のクレデンシャルとして登録し，PW（知識情報）と PC の登録情報（所持情報）を用いて 2 要素認証を行うことは悪手と言える．また，マルウェアは感染した PC に入力される任意の情報を窃取する可能性もある．そのため，PC を経由して 2 要素目のクレデンシャルを送信することも得策

ではない[b]．従って，現在スマートフォンを 2 要素目のクレデンシャルの送信手段として用いた 2 要素認証が一般的である．PC とは異なる認証経路を確保することによって，PC がマルウェアに感染し，1 要素目のクレデンシャル（PW）が窃取されたとしても，不正者がスマートフォンでの認証を突破しない限り，なりすますことができない．

本稿では以降，PC とスマートフォンの構成による一般的な 2 要素認証（図 2）を具体例として議論を進める．図 2 では，1 要素目のクレデンシャルを PW，2 要素目のクレデンシャルを PIN と示しているが，知識情報以外のクレデンシャルを用いても良い．実際の認証手順では，認証サーバが PW_{PC} を受信した場合にのみ，認証サーバからスマートフォンに PIN の提示を要求する形となるが，図 2 ではその記載を省略する．図 1 同様，図 2 でもクレデンシャルを区別するため，PW，PW_{PC}，PIN，PIN_{SP} と書き分けているが，実際には $PW=PW_{PC}$，$PIN=PIN_{SP}$ である．

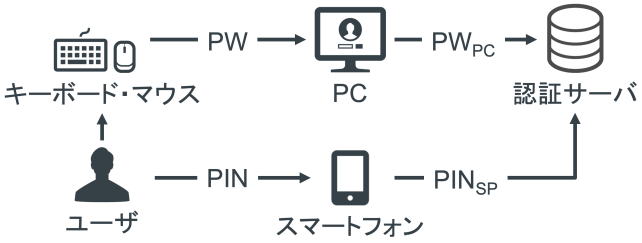

図 2　2 要素認証

Fig.　2　　Two-factor Authentication

2.2　2 要素認証の課題

図 2 では，単純に 2 つのクレデンシャル（PW，PIN）のみを示したが，実際のユーザの操作は，PW 入力の前に PC のログイン，PIN 入力の前にスマートフォンのアクティベートが必要になる．図 3 は，図 2 に実際の動作を含めたものである．なお，図 2 と同様に，$PW=PW_{PC}$，$PIN=PIN_{PC}$ である．

- AC_{PC} : ユーザが PC にログインする際に，PC に提示する PC アクティベート用のクレデンシャル
- PW : ユーザが情報資産にアクセスする際に，PC を経由して認証サーバに提示する 1 要素目のクレデンシャル
- AC_{SP} : ユーザがスマートフォンを使用する際に，スマートフォンに提示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 : ユーザが情報資産にアクセスする際に，スマートフォンを経由して認証サーバに提示する 2 要素目のクレデンシャル

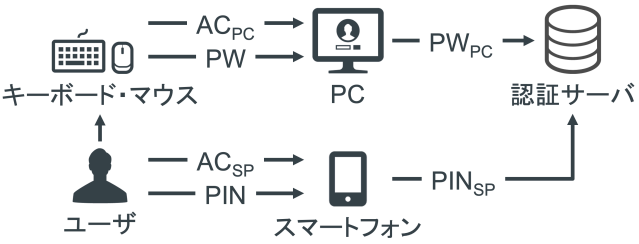

図 3　2 要素認証の詳細

Fig.　3　　Details of Two-factor Authentication

2 要素認証の利便性を低下させているクレデンシャルがどれなのかを確認する．まず，AC_{PC} を考える．正規ユーザ（社員）が情報資産（社内クラウド）にアクセスする時点で，正規ユーザは PC に対峙している．すなわち，PC は既にアクティベートされている状態にある．このため，この時点における AC_{PC} の入力は不要である．次に，PW を考える．ゼロトラスト環境下においては，社内の情報資産へのアクセスにあたっては，正規ユーザであろうと PW の提示を求められることが一般的である．また，前述の通り，正規ユーザが情報資産にアクセスする時点で，正規ユーザは PC に対峙している．このため，PC への PW の入力は，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と言える．続いて，PIN を考える．スマートフォンの端末番号（所持情報）を PIN として採用すれば，正規ユーザがその都度，PIN を手入力する必要はなくなる．第 2 パスワード（記憶情報）を PIN として用いる場合も，PIN をスマートフォンに記憶させておけば，正規ユーザは PIN の手入力から解放される．最後に，AC_{SP} を考える．マルウェアに感染した PC からの依頼を受けて，スマートフォンが自動的に PIN を認証サーバに送信してしまっては，2 要素認証が突破されてしまう．すなわち，スマートフォンが PIN を発出する前には，正規ユーザの意思の確認が必須となる．この役目を果たすのが，スマートフォンへの AC_{SP} の入力である．ここで，基本的には PC 業務中に正規ユーザがスマートフォンを操作し続けていることはないため，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．このため，正規ユーザに，PC 業務中に自分の意識をスマートフォンに向け，スマートフォンを手に取って AC_{SP} を入力するという手間が課されることになる．

以上より，図 3 の 2 要素認証の利便性に悪影響を与えているのは，AC_{SP} の入力である．正規ユーザ（社員）は，認証の度に，業務とは関係のないスマートフォンに意識を向けてスマートフォンを操作する必要が生じる．特に，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．認証操作 1 回当たりの利便性低下は些少であったとしても，それ

b ワンタイムパスワード（OTP）を 2 要素目のクレデンシャルとして採用可能な場合には，この限りではなくなる．例えば[4]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．

が積算された結果，ユーザの操作コストの激増，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

Bardram らは，ユーザの状況に応じて動的に認証方式を変更するコンテキストアウェア認証を提案した[7]．この方式は，ユーザが所持する IC カードと認証要求を行う PC が近接しているかどうかを確認する．両者が近接していることが確認できる場合には，自動的にユーザ認証を行い，確認できない場合には，ユーザにパスワードの入力を要求する．

Karapanos らも PC とスマートフォンの近接性に基づく 2 要素認証の利便性向上手法を提案している[5]．具体的には，PC の周囲の環境音とスマートフォンの周囲の環境音の類似性を利用して，PC とスマートフォンの近接を判定する．

コンテキストアウェア認証や，周囲の環境音を 2 要素認証に利用することで，スマートフォン側の 2 要素目の認証を自動化することができる．具体的には，認証サーバに PW_{PC} が届いた段階で，認証サーバはスマートフォンに 2 要素目の認証要求を送信するようにする．スマートフォンには PIN を記憶させておき，スマートフォンが PC と近接していることを確認できた場合にのみ，スマートフォンから認証サーバに PIN_{SP}（＝PIN）を自動送信する．

Fathy らは，スマートフォンのフロントカメラで撮影した動画を用いて，全自動顔認証システムの有用性の検討を行った[8]．全自動顔認証システムを 2 要素認証に利用することで，スマートフォン側の 2 要素目の認証を自動化することができる．具体的には，認証サーバに PW_{PC} が届いた段階で，認証サーバはスマートフォンに 2 要素目の認証要求を送信する．スマートフォンには PIN を記憶させておき，スマートフォンが全自動顔認証システムによってユーザの存在を確認できた場合にのみ，スマートフォンから認証サーバに PIN_{SP}（＝PIN）を自動送信する．

これらの既存研究のように，スマートフォンが PC との近接やユーザの正当性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制することはできる．しかし，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．正規ユーザの PC 業務中に，マルウェアがバックグラウンドで PW_{PC} を認証サーバに送信した場合，スマートフォン側で PC との近接あるいはユーザの正当性が確認できてしまうため，スマートフォンは認証サーバに PIN_{SP} を送信してしまう．すなわち，2 要素目を自動化すると，マルウェアに 2 要素認証が突破されてしまう．2 要素目の認証を自動化する場合であっても，ユーザ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，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，認証を多重化する副作用として，認証の度にユーザに複数のクレデンシャルの提示を強いることとなる．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．しかし，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，安全性を確保しつつも利便性を向上させる新しい形式の 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，多要素認証が必要となる原因が PC へのマルウェア感染にあるならば，正規ユーザの証明のためにわざわざ複数のクレデンシャルを確認せずとも，「人間が正規クレデンシャルを提示した」という事実を確認することで 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，「クレデンシャルの正当性に加え，人間による物理的な認証行為の発生を確認する」というコンセプトに基づいた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．ユーザの提示した単一の正規クレデンシャルが多点で同時に観測されることが，「正規ユーザが実際に認証行為を行った」という事象発生の証左となり，これにより多要素認証と同等の効果が達成される．

3.2 認証手順

提案方式で用いるクレデンシャルはパスワードである．本方式では，PC へのキーボード，マウスの入力が，スマートフォンにも同時に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，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する）の Bluetooth ユニットを改造し，ワイヤレス入力デバイスからの入力を PC とスマートフォンの両方で受信可能にする．

多点観測型多要素認証の認証手順は以下の通りである（図 4）．図 4 においては，PC 側の PW とスマートフォン側の PW を区別するために，PW_{PC}，PW_{SP} と書き分けているが，実際には $PW=PW_{PC}=PW_{SP}$ である．

【多点観測型 2 要素認証】

1. PC 業務の中で，ユーザが認証サーバに情報資産へのアクセスを要求
2. 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
3. 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
4. 認証サーバは，PC に認証画面の表示を要求

5. PC は認証画面を表示
6. ユーザがワイヤレス入力デバイスを用いて PC に PW を入力
7. ユーザが PC へ入力した PW を，スマートフォンも受信
8. PC，スマートフォンは受信した PW をそれぞれ認証サーバに送信
9. 認証サーバは PC から受信した PW（PW_{PC}）とスマートフォンから受信した PW（PW_{SP}）の両者の正当性を確認し，ユーザが正当か否かを判断
10. 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
11. 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

なお，手順 8 にて PW_{PC} は正当であったが PW_{SP} が不正であると判断された場合には，従来の 2 要素認証にシームレスに移行して，ユーザに改めてスマートフォンへの第 2 クレデンシャルの入力を促すという運用も可能である．

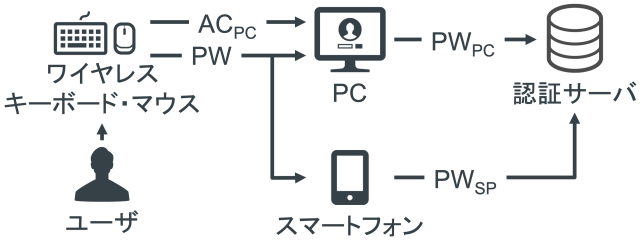

図 4　2 点観測型 2 要素認証

Fig.　4　　Two-observed Two-factor Authentication (Method A)

4. 基礎実験

今回の基礎実験では，一般に用いられている従来の 2 要素認証と提案方式との比較実験を通じて，利便性，プライバシ，認証時間の観点から提案方式の評価を行った．

4.1 実験用システム

従来の 2 要素認証にはいくつかの方式があるが，今回はユーザの手間が最少となる下記の手順（以降，実験用従来方式と呼ぶ）を採用した（図 5）．ここで，手順 7 におけるスマートフォンへの「OK」ボタンのタップが，2.2 節の図 3 で説明した従来の 2 要素認証方式における AC_{SP} の入力に該当していることに留意されたい．

【実験用従来方式】

1. ユーザは PC にパスワード（PW）を入力
2. PC は入力された PW を認証サーバに送信
3. 認証サーバは PC から受信した PW をもとに，ユーザの正当性を確認
4. 正当であった場合には，認証サーバは PC にワンタイムパスワード（OTP）用トークンを通知
5. PC はスマートフォンにトークンを転送
6. スマートフォンはユーザの意思を確認するために，「OK」ボタンを画面に表示
7. ユーザがスマートフォンの「OK」ボタンをタップ
8. スマートフォンはトークンを認証サーバに送信
9. 認証サーバはスマートフォンから受信したトークンの正当性を確認
10. 正当であった場合には，認証サーバはスマートフォンに OTP を通知
11. スマートフォンは PC に OTP を転送
12. PC は OTP を認証サーバに送信
13. 認証サーバは PC から受信した OTP の正当性を確認
14. 正当であった場合には，認証サーバはユーザを正規ユーザと判断

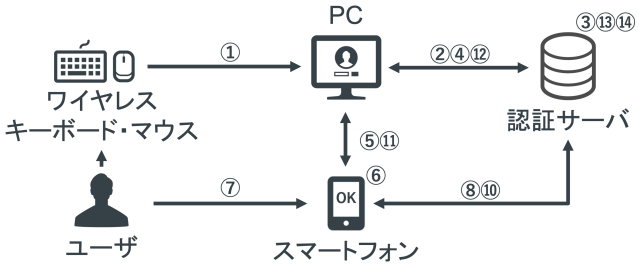

図 5　実験用従来方式

Fig.　5　Existing Method (Experimental Use)

提案方式の手順は 3.2 節で説明した通りであるが，認証サーバにおける 2 要素認証の実装上の制約から，今回は従来方式をベースとした下記の手順（以降，実験用提案方式と呼ぶ）へと提案方式を改訂した（図 6）．具体的には，実験用従来方式の認証サーバにおいて稼働している OTP 方式の 2 要素認証モジュールを，実験用提案方式を構成するパーツとして再利用することによって，提案方式と等価な認証システムを再現している．ユーザが実行する操作自体は，提案方式と実験用提案方式は完全に同一である．

【実験用提案方式】

1. ユーザは PC にパスワード（PW）を入力
2. PC は入力された PW を認証サーバに送信
3. 認証サーバは PC から受信した PW をもとに，ユーザの正当性を確認
4. 正当であった場合には，認証サーバは PC に OTP 用トークンを通知
5. PC はスマートフォンにトークンを転送
6. スマートフォンも手順 1 の PW を受信
7. スマートフォン内で PW の正当性を確認
8. 正当であった場合には，スマートフォンは手順 4 の OTP 用トークンを認証サーバに送信
9. 認証サーバはスマートフォンから受信したトークンの正当性を確認
10. 正当であった場合には，認証サーバはスマートフォンに OTP を通知

11. スマートフォンは PC に OTP を転送
12. PC は OTP を認証サーバに送信
13. 認証サーバは PC から受信した OTP の正当性を確認
14. 正当であった場合には，認証サーバはユーザを正規ユーザと判断

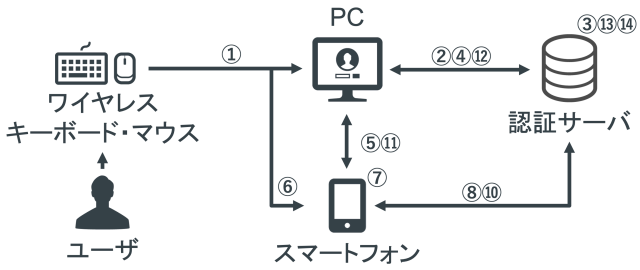

図 6　実験用提案方式

Fig.　6　Proposed Method (Experimental Use)

4.2 実験用システムの実装

4.1 節で詳説した実験用従来方式,実験用提案方式を実装した．実験システムの諸元を表 1 に，実験システムの構成を図 7 に示す．認証サーバの実装には，AWS マネージドサービスを用いた.なお,実験用提案方式の手順 8 において，スマートフォン側で PW の正当性が確認できなかった場合は，実験用従来方式の手順 6 に移行するようにしてある．これは，Bluetooth 通信の不具合などの理由で提案方式による正規ユーザの認証が失敗してしまった場合には，シームレスに従来方式の 2 要素認証に移行することによって，正規ユーザを救済するための措置である．

3.2 節でも説明した通り，提案方式においては，ワイヤレス入力デバイスからの入力が PC とスマートフォンの両方に接続されることが前提となっている．本実装では，USB 分配器と Bluetooth 変換アダプタを用いることによって,キーボード入力が PC とスマートフォンに同時にワイヤレス接続されるようにした．なお，今回の実験用従来方式，実験用提案方式においては，スマートフォンが受信するのは PW 入力のみである．このため，マウス接続の分配は実装しておらず，マウス入力は PC のみに届くようになっている．

表 1　実験システムの諸元

Table 1　Experimental System Specification

PC	型番	DELL，P117G002
	CPU	11th Gen Intel(R) Core(TM) i7-1195G7 @ 2.90GHz
	メモリ	32GB
	OS	Windows 11 Home
	Web ブラウザ	Google Chrome 104.0.5112.101
スマートフォン	型番	Google，GR1YH
	サイズ	158.6mm×74.8mm
	CPU	Google Tensor
	メモリ	8GB
	OS	Android 12
	Web ブラウザ	Google Chrome 104.0.5112.101
キーボード	型番	PFU，PD-KB800
マウス	型番	Logicool，M650LGR
モニタ	型番	DELL，U2720QM
	サイズ	61.13cm×39.52cm
USB 分配器	型番	Bewinner，Bewinners5xprhct2q
Bluetooth 変換アダプタ	型番	BitTradeOne，ADU2B02P

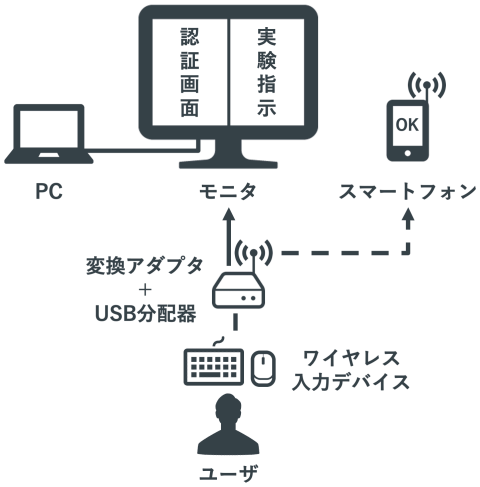

図 7　実験システムの構成

Fig.　7　Experimental System Configuration

4.3 実験手順

実験協力者は,情報系学部に所属する大学生 6 名である．今回の実験協力者は男性のみであった．実験の手順は次の通りである．

1. 実験の流れを説明
2. 2 要素認証の説明
3. 本実験で使用する ID/PW を作成
4. 2 種類の 2 要素認証を 5 回ずつ試行（各認証試行において，認証の成否と認証に要した時間を記録）
5. 事後アンケートに回答

手順 2 については，2 章の図 3 と 3 章の図 4 を実験協力者に提示し，2 要素認証と提案方式の仕組みを概説した．ただし，方式の名称が確証バイアスを生み得るため，実験の中では従来方式を「方式 A」，提案方式を「方式 B」と呼称している．手順 3 については，各実験協力者が普段利用している ID/PW を再利用せず,今回の実験でのみ使用する

ID/PW を作成するように依頼した．その際，PW の作成にあたっては，「実験が終了するまで覚えていられること」，「半角英数 8 桁以上であること」を満たすよう指示した．なお，今回の実験で使用した ID/PW は実験終了後に削除した．手順 4 においては，順序効果に配慮し，6 名の実験協力者のうち 3 名は従来方式→提案方式の順に，残り 3 名は提案方式→従来方式の順に実験を行ってもらった．手順 5 の事後アンケートについては，次節で説明する．

図 8(a)に PC の認証画面，図 8(b)にスマートフォンに表示される確認画面を示す．PC の認証画面は，実験用提案方式と実験用従来方式で同じである．実験用提案方式ではユーザがスマートフォンを操作しないので，実験協力者がスマートフォンの確認画面を目にするのは，実験用従来方式の実験時のみとなる．今回の実験では，モニタの右半分に実験説明書を表示し，実験説明書に記されている説明，指示に従いながら，モニタの左半分に表示した認証画面（図 5(a)）を用いて実験を進めてもらった．実験中，スマートフォンは常に（実験用従来方式の手順 7 で実験協力者が「OK」ボタンをタップする時以外は）画面を伏せた状態で机上に置く形式に統一した．

(a)　(b)

図 8　(a) PC の認証画面，(b) スマートフォンの確認画面
Fig. 8　(a) Authentication Screen of PC, (b) Confirm Screen of Smartphone

4.4 事後アンケート

事後アンケートでは次の 6 つの質問に回答してもらった．

1. 年齢
2. PC とスマートフォンを用いた 2 要素認証の経験の有無
3. ユーザビリティの観点でどちらの方式を使いたいか（7 段階＋理由）
4. 提案方式におけるプライバシの懸念（5 段階＋理由）
5. 質問 3，4 を踏まえた上でどちらを使いたいか（7 段階＋理由）
6. 認証頻度が増加した環境を想定した上で，どちらを使いたいか（7 段階＋理由）

質問 1 は，年齢によって記憶力などの認知能力に差があることが知られており，アンケート結果に影響を及ぼし得る実験協力者の属性を把握するために確認している．質問 2 も，実験協力者のこれまでの経験がアンケート結果に影響を及ぼし得るためである．質問 3 は，両認証方式の利便性を聴取している．質問 4 は，提案方式においては PW がスマートフォンにも送信されることになるため，これに伴うプライバシ懸念の大きさを聴取している．質問 5 は，利便性（質問 3）とプライバシ（質問 4）のトレードオフを考慮した上で，提案方式と従来方式のどちらに対する許容度が高いのか確認している．質問 6 は，質問 5 に対する回答が，認証頻度が増加によって如何に変化するのか確認している．

事後アンケートは，Google Forms を用いて作成，実施，集計を行った．なお，実験協力者の個人情報とは紐付かないように管理してある．

4.5 アンケート結果

今回は基礎実験ということで，実験協力者全員が大学生であった．このため，質問 1 の回答は 6 名とも「20 代」であった．また，質問 2 の回答も，実験協力者全員が「2 要素認証の利用経験あり」という結果であった．

質問 3 は，「提案方式のほうが非常に使いやすかった（3 名）」，「提案方式のほうがかなり使いやすかった（3 名）」という結果が得られた．理由は，概ね「スマートフォンを確認せずとも PC 上で認証を完結することができる（6 名）」といったものであった．以上から，提案方式が 2 要素認証の利便性向上に寄与することが確かめられた．また，実験協力者 1 名からは，「スマートフォンを必ずしも手の届く範囲においてなくてもいい」というコメントが寄せられた．在宅時にはスマートフォンを充電スポットに置くようなユーザも少なくない．提案方式であれば，スマートフォンを充電スポットに収めたままでも 2 要素認証が機能するため，ユーザの多様な利用形態にマッチするといえる．

質問 4 は，提案方式において PC に入力した PW がスマートフォンにも受信されることに対し，抵抗を「全く感じなかった（2 名）」，「あまり感じなかった（1 名）」，「少し感じた（3 名）」という結果であった．理由からは，「本当に PW 入力時しかスマートフォンに送信されていないか」，「スマートフォンの外に PW が漏洩していないか」といった信用の問題が原因であることが伺い知れた．このため，提案方式の信用を如何に高めるかが今後の課題となるだろう．

質問 5 は，「非常に提案方式を使いたい（3 名）」，「かなり提案方式を使いたい（2 名）」，「どちらかといえば従来方式を使いたい（1 名）」という結果が得られた．理由は，「提案方式のほうが利便性が高いから（5 名）」，「自分でスマートフォンを確認した方が安心できる（1 名）」であった．この結果から，提案方式は大半のユーザに許容される認証方式であると結論付けて良いだろう．

質問 6 は，「非常に提案方式を使いたい（5 名）」，「どちらかといえば従来方式を使いたい（1 名）」という結果であ

った．理由からも，認証頻度の増加が利便性に対する要求も高めることが確かめられた．しかし，その一方で，従来方式を好む実験協力者の意見は質問 5 から変化していない．これは，提案方式の信用が高まらなければ，提案方式はユーザに許容されないであろうことを示唆する．提案方式の内部動作の透明性の確保が求められる．

4.6 認証時間に関する実験結果

提案方式の認証に要する時間を評価するために，実験用提案方式と実験用従来方式の両システムの認証時間を測定した．具体的には，ユーザが PC に ID/PW を入力し，入力完了を伝えるための「送信」ボタン押下した時点から，PC 画面に「認証完了」と表示されるまでの時間を測定した．

1 回目の認証試行においては，実験協力者が認証方式に慣れていないことに鑑み，2〜5 回目の計測時間の平均所要時間を算出した．従来方式の平均所要時間は 3.82 秒であったのに対し，提案方式の平均所要時間は 1.27 秒であった．両者の差から，画面を伏せた状態で机上に置かれているスマートフォンを手に取って，スマートフォンに表示される「OK」ボタンをタップする操作が，平均約 2.5 秒であることが分かった．

5. 考察

5.1 提案方式特有のリスク

提案方式は，PC，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 のペアリングは基本的に 1 対 1 接続であるため，提案を実装するにあたっては，4 章で行った実装方法や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の脆弱性は，提案方式のリスクとなる．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な場合[11]が，その典型例である．正常であれば，ワイヤレス入力デバイスから PC への通信は一方向であるが，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書き換えられた場合，PC 内に潜む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となってしまう．この問題に対しては，マルウェアが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．

6. まとめ

本稿では，2 要素認証が抱える利便性低下の問題に対し，「クレデンシャルの正当性に加え，人間による物理的な認証行為の発生を確認する」というコンセプトに基づいた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．提案方式の実装を行い，6 名の実験協力者による基礎実験を通じて利便性，プライバシ，認証時間の観点から提案方式を評価した．本研究の有用性を示すには，より多くの実験協力者による実験を行うことで，統計的分析を行うことが必要である．今後は，より多くの実験協力者数による追加実験，脅威分析モデル STRIDE を用いた安全性の検討を行う予定である．

謝辞　本研究において三菱電機株式会社　柴田陽一様，山中忠和様，松田規様には多くのアドバイスを賜りました．この場を借りて感謝申し上げます．

参考文献

[1] “Emotet modules and recent attacks”.SECURELIST, KaSPersky, https://securelist.com/emotet-modules-and-recent-attacks/106290/, (参照 2022-8-16).
[2] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., Koucheryavy, Y.: Multi-Factor Authentication: A Survey, Cryptography, vol. 2, no. 1, 2018.
[3] “How it works: Azure AD Multi-Factor Authentication”. Microsoft, https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks, (参照 2022-8-16).
[4] ”Adding MFA to a user pool”, Amazon, https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-settings-mfa.html (参照 2022-8-16).
[5] Karapanos, N., Marforio, C., Soriente, C., Capkun, S.: {Sound-Proof}: Usable {Two-Factor} Authentication Based on Ambient Sound. In 24th USENIX security symposium, USENIX security 15, 2015, pp. 483-498.
[6] 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：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，2022 年暗号と情報セキュリティシンポジウム (SCIS2022) 予稿集，4B2-2 (2022.1).
[7] Bardram, J. E., Kjær, R.E., Pedersen, M. Ø.: Context-aware user authentication- supporting proximity-based login in pervasive computing. International Conference on Ubiquitous Computing. SPringer, Berlin, Heidelberg, 2003.
[8] Fathy, M. E., Patel, V. M., Chellappa, R.: Face-based Active Authentication on mobile devices. 2015 IEEE International Conference on Acoustics, SPeech, and Signal Processing (ICASSP), 2015, pp. 1687–1691.
[9] Singh, S., Inamdar, A., Kore, A., Pawar, A.: Analysis of Algorithms for User Authentication using Keystroke Dynamics. 2020 International Conference on Communication and Signal Processing (ICCSP), 2020, pp. 0337–0341.
[10] Tietz, C., Klieme, E., Behrendt, L., Böning, P., Marschke, L., Meinel, C.: Verification of Keyboard Acoustics Authentication on Laptops and Smartphones Using WebRTC. 2019 3rd Cybersecurity in Networking Conference (CSNet), 2019, pp. 130–137.
[11] Choi, B., Suh, T.: 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.