多点観測認証：単一クレデンシャルによる多要素認証の達成（その3）

SCIS 2023 2023 Symposium on
Cryptography and Information Security
Fukuoka, Japan, Jan. 24 – 27, 2023
The Institute of Electronics,
Information and Communication Engineers

多点観測認証：単一クレデンシャルによる多要素認証の達成（その 3）
Multi-Observed Authentication: A Multi-Factor Authentication Using Single Credential (part 3)

野崎真之介* 芹澤歩弥* 吉平瑞穂*
藤田真浩† 吉村礼子† 大木哲史* 西垣正勝*
Shinnosuke Nozaki* Ayumi Serizawa* Mizuho Yoshihira*
Masahiro Fujita† Ayako Yoshimura† 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手間が生じる．現在，認証チケットを用いた利便性向上策はあるが，ユーザの PC 内にマルウェアが感染している場合，認証チケットを自在に扱われてしまう．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，複数のクレデンシャルを確認せずとも，「人間が認証を行なった」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，「認証の際のユーザの意思表示」を物理事象として捉え，「パスワード入力という物理イベントを多点で同時に観測する」というコンセプトに基づいた新たなユーザ認証方式（多点観測認証）を提案した．提案方式においては，物理的な認証動作が多点同時観測されることが，「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，基本方式および認証チケット使用方式の 2 つの多点観測認証の提案と評価，考察を行った．

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，物理事象の同時多点観測

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（知識情報／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ユーザの PC に，2 要素目のクレデンシャルをユーザのスマートフォンに入力することでユーザを認証する[2][3][4]．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，認証の度にユーザ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自体）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[5]．しかしその場合は，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，ユーザの認証の意思を確認するため

* 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.

に，わざわざもう 1 つ別のクレデンシャルを提示せずとも，「(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ある．そこで我々は，「認証の際のユーザの意思表示」を物理事象として捉え，「クレデンシャルの入力という物理イベントを多点同時観測する」というコンセプトに立脚する新たなユーザ認証方式（多点観測認証）を提案した[6]．提案方式は，「ユーザによる単一の正規クレデンシャルの入力」という物理イベントを，PC とスマートフォンの 2 点で同時に観測することによって，利便性と安全性を両立した 2 要素認証を達成する．

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 章では利用環境に則した提案方式の派生系やリスクに関して考察し，5 章で認証チケットを利用する場合の方式を提案し，6 章にて本稿のまとめを行う．

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た．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]．そのよう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 要素認証の普及が進んでいる．

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[2]．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が，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】

0. ユーザはアクセス要求を行う
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．

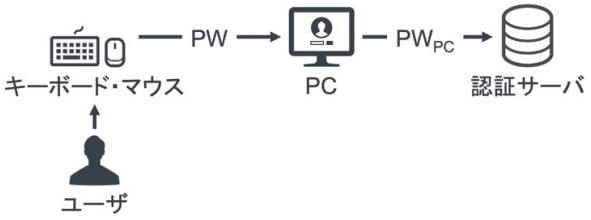

図 1 単要素認証

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認証サーバに送信することも得策ではない[1]．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[3][4]．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，不正者はスマートフォンを操作することはできないため，なりすますことが不可能となる．

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} を受信した時点で，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．

[1] 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．

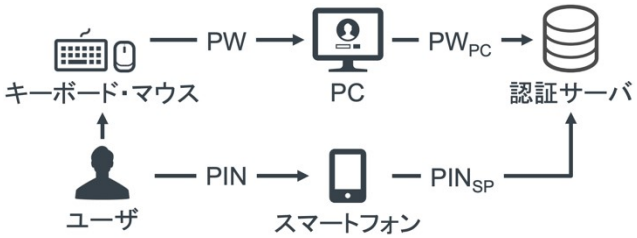

図 2 2 要素認証

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

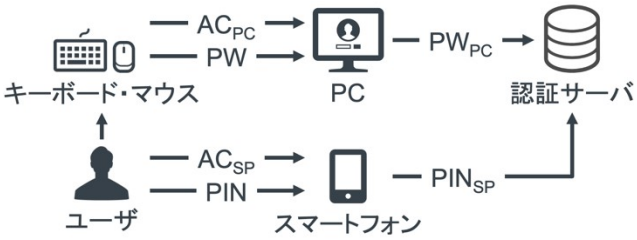

図 3 2 要素認証の詳細

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．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（知識情報）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，正規ユーザの認証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．このアイデアを 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，スマートフォンに 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，認証サーバからの 2 要素目の認証要求に対して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．

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]．文献[5]では，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．

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]．文献[8]のような継続認証のアイデアを 2 要素認証に利用することによっても，同様に，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，スマートフォンにはPINを記憶させておき，スマートフォンが継続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，認証サーバからの2要素目の認証要求に対して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. 多点観測認証

2要素認証は，「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，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．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要素認証が必要である．

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，「認証の際のユーザの意思表示」を物理事象として捉え，「クレデンシャルの入力という物理イベントを多点同時観測する」というコンセプトに基づいた新たなユーザ認証方式（多点観測認証）を提案した[6]．

「ユーザがPCの前に存在しており，かつ，キーボードにパスワードを入力する」というイベントは，物理世界の中で発生する事象である．物理事象であれば，そのイベントが発生した際には，その結果が複数のセンサにおいて同時に観測されるはずである（例 1：福島県沖の地震が宮城と福島で同時に観測される，例 2：新幹線の走行によって風圧と騒音が同時に観測される）．この常識に基づけば，「1種類のクレデンシャルの入力」というイベントが「2箇所（以上）で同時に観測された」という事実をもって，クレデンシャルの入力が実際に発生した物理事象であると確認できる．これが「認証に対するユーザの意思（正規ユーザが実際に認証行為を行った）」を示す証左となり，多要素認証と同等の効果が達成される．

従来の2要素認証では「2要素目のクレデンシャル」としてスマートフォンを利用していたが，多点観測認証ではユーザの入力する「1要素目のクレデンシャルの入力」を確認するための2つ目の観測器としてスマートフォンを利用していることに留意されたい．

3.2 基本方式

本節では，提案方式の具体的な認証手順を説明する．なお，本節で説明する方式を基本方式と呼称することとする．

本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のBluetoothユニットを改造し，ワイヤレスキーボードからの入力をPCとスマホの両方で受信可能にする．

基本方式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．

【基本方式】

1. PC業務の中で，ユーザが認証サーバにファイルアクセスを要求
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，ワイヤレスキーボード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キーボードを用いてPCにPWを入力
7. スマートフォンも，ユーザがPCへ入力したPWを受信
8. PCならびにスマートフォンは，個々が受信した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，ユーザ認証が正規ユーザの意思によるものであるか否かを判断
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，ワイヤレスキーボードからの信

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．

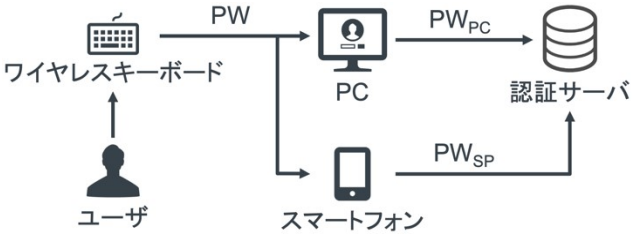

図 4 基本方式

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を評価する．

基本方式においては，ユーザに求められるのは PC への PW の入力のみである．よって，基本方式はスマートフォンへ意識を向けずとも認証が行えるため，利便性に関する要件 1 を満たす．また，ユーザからは慣れ親しんだパスワード認証に見えるため，ユーザの心的観点からは，基本方式の導入障壁はほとんどないと言える．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，PW の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を操作することは不可能である．従って，スマートフォンが受信した PW は，ユーザ自身が入力した PW であると同定できる．すなわち，スマートフォン側での PW の受信が，ユーザが自らの意思によるものである証左となる．よって，基本方式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，ユーザ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 によってユーザの意思確認が行われるので，手順 9（スマートフォンからの PW_{SP} の受信）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）．

以上より，提案方式においては，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）が達成される．

4. 考察

4.1 利便性と安全性のバランス

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は，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認証方式となっている．物理的近傍に不正者が居ない以上，不正者にキーボードが物理的に操作されることはない．すなわち，キーボードを用いて物理的に PW が入力されたならば，それはユーザ本人によって入力された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，キーボードが物理的に操作されさえすれば「ユーザの意思の介在」を認めてしまってよいようにも思える．しかし，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可能である．その場合は，社員は他の業務のために PC を操作しているので，キーボードの操作が観測されてしまい，スマートフォンから認証サーバに PW_{SP} が送信されてしまう．すなわち，ユーザの認証の意思を確認するためには，キーボードからクレデンシャル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」と「PW 入力の際のキーボード操作」が大きく異なる場合には，PW_{SP} の正当性を確認せずとも，「PW（＝PW_{SP}）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しても良いだろう．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．

ユーザによっては，キーボードに入力した PW がスマートフォンにも送られることに対して，プライバシの懸念を感じる場合がある．「PW らしき情報」の入力を確認する方法であれば，スマートフォンで PW（＝PW_{SP}）自体を観測する必要がないため，(安全性は少々低下するものの）ユーザの利便性（プライバシに対する配慮）の向上につながる．

一方で，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．従って，この場合には，単に「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．ここで，PC へのマルウェア感染が疑われている以上，PC から認証サーバに届く PW は改竄されている可能性が否定できない．このため，「正規ユーザによって PW が入力されたのか否か」の確認は，スマートフォンから認証サーバに届く PW_{SP} に対して検査がなされることになる．

これを実現する一つの方法が，キーストローク認証の採用である[9]．スマートフォン側で，PW 入力時のキーストローク情報を併せて取得し，これを認証サーバに送信する．認証サーバ側で PW（PW_{SP}）の正当性をキーストローク認証の観点からも確認することで，不正者（マルウェアと結託した人間）による正規クレデンシャル（PW）の入力を排除することが可能となる．

4.2 提案方式特有のリスク

これまで挙げた 3 つの提案方式は，PC，スマートフォンの両者と接続されるキーボード，マウスの使用を前提とした認証方式となっている．Bluetooth では同一プロファイルでの通信では 1 対 1 接続であるため，提案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の脆弱性は，提案方式のリスクとなる．キーボード，マウ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[10]が，その典型例である．正常であれば，キーボード，マウスから 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キーボード，マウスを操作することが可能となってしまう．これは基本方式，認証チケット使用方式にとっては致命的なセキュリティホールとなる．キーストローク認証方式にとっても，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キーボード，マウ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. 認証チケット使用型多点観測認証

認証そのものの利便性を向上させる方法として，現在，Kerberos 認証などのような，認証を一度行った後に得られる認証チケットを用いることでユーザに再認証の手間を生じさせない方法がある[11]．しかし，今回の想定であるユーザの PC 内にマルウェアが常駐していた場合，ユーザの意思に関係なくマルウェアに認証チケットを利用されてしまう．

本稿で提案したコンセプトは，「1 要素目のクレデンシャルの入力」という「認証の際のユーザの意思表示」を，物理イベントとして多点同時観測することある．しかし，認証チケットを利用した場合には，（再認証の際には）PW の入力が生じないため，「1 要素目のクレデンシャルの入力」を観測することができない．そこで本章では，「ユーザのアクセス要求動作」によって生じる物理事象を多点同時観測することで，ユーザの情報資源へのアクセスの意思を捉え，多点観測認証のアイデアを利用して認証チケットの使用を許可する方式を提案する．基本方式と同様に，PC へのマウスのクリック操作がスマートフォンでも同時に受信できることを前提としている．本章で説明する方式を認証チケット使用方式と呼称することとする．

認証チケット使用方式の使用手順は以下の通りである（図 5）．

【認証チケット使用方式】

1. 事前に一度，従来の 2 要素認証を行い，PC が認証サーバから認証チケットを取得
2. PC 業務の中で，ユーザが認証サーバに情報資源へのアクセス（典型的にはファイルアクセス）を要求
3. 同時に，PC から認証サーバに認証チケットを送信
4. 認証サーバは，スマートフォンにワイヤレスマウスの操作の受信開始を指示
5. スマートフォンは，ワイヤレスマウスからの信号の受信を開始
6. 認証サーバは，PC に情報資源アクセスの確認画面の表示を要求
7. PC はファイルアクセスの確認画面（例：「本当にこのファイルを閲覧する場合には，OK をクリックして下さい」）を表示
8. ユーザが，ワイヤレスマウスを用いて確認画面内の「OK」をクリック
9. ユーザによるワイヤレスマウスの操作（クリック＋マウスの座標）を，スマートフォンも受信
10. PC は，確認画面の「OK」がクリックされたことを認証サーバに送信
11. スマートフォンは，ワイヤレスマウス操作の情報を認証サーバに送信
12. 認証サーバは，手順 3 で PC から届いた認証チケット，手順 10 で PC から届いた「OK」クリック，手順 11 でスマートフォンから届いたワイヤレスマウスの正当性を確認し，情報資源アクセスが正規ユーザの意思によるものであるか否かを判断
13. 認証サーバは，スマートフォンにワイヤレスマウスの操作の受信終了を指示
14. スマートフォンは，ワイヤレスマウスからの信号の受信を停止

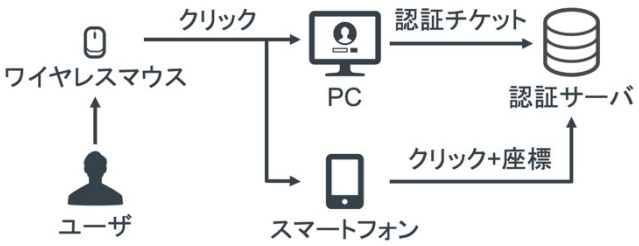

図 5 認証チケット使用方式

本方式では，認証チケットを使用した場合に比べ，確認画面に表示される「OK」のクリック操作が増加する．しかし，PC に重要なアクションを実行させる場合に再確認のための「OK」のクリックが求められることは一般的であるため，利便性の低下は些細であるのではないかと推測される．基本方式同様，ユーザの PC 内に潜むマルウェアにはマウスを操作することは不可能であるため，基本方式と同等の安全性を保つことが可能である．

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,「ユーザ認証の際に発生する物理事象を多点同時観測する」というコンセプトに基づいた多点観測認証を議論した．提案方式の具体例を示し，利便性と安全性の観点から提案方式を評価した．認証チケットを使用する場合の多点観測認証に関する提案，評価，考察が文献[6]に加えての貢献である．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．

参考文献

[1] “Emotet modules and recent attacks”, SECURELIST, Kaspersky, https://securelist.com/emotet-modules-and-recent-attacks/106290/, （参照 2022-12-08).

[2] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., Koucheryavy, Y.: Multi-Factor Authentication: A Survey, Cryptography, vol. 2, no. 1, 2018. https://doi.org/10.3390/cryptography2010001.

[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 2022-12-08).

[4] ”Adding MFA to a user pool”, Amazon, https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-settings-mfa.html （参照 2022-12-08).

[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，吉村礼子，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（その 2），コンピュータセキュリティシンポジウム (CSS2022) 論文集，pp.675-682 (2022.10).

[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, doi: 10.1109/ICASSP.2015.7178258.

[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, doi: 10.1109/ICCSP48568.2020.9182115.

[10] 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, Dec. 2016.

[11] “Kerberos Authentication Overview”. Microsoft, https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview, (参照 2022-12-08).