会誌「情報処理」Vol.63 No.5（May 2022）「デジタルプラクティスコーナー」

JISA招待論文

ID秘匿化ワンタイム多要素認証 ―SECUREMATRIXの研究開発―

下平哲也[1]

[1]（株）シー・エス・イー

昨今のテレワーク増加に伴い，社外での働き方が以前よりも一般的になりつつある．しかし，多くの企業ではテレワーク導入においてセキュリティを担保できるのかという懸念を抱えている．既存のシステムの多くが，ファイアウォール等でネットワークの境界を区切る，境界型認証モデルで構築されてきた．しかし，テレワークの増加による社外から社内への接続，クラウドサービスの利用普及による社内から社外への接続等が広がっており，境界型認証モデルの前提が崩れつつある．このような時代の変遷に合わせ，ゼロトラスト型認証モデルが注目されている．ゼロトラスト型認証モデルとは，すべてのネットワークには常に危険が潜んでいると考え，IDによってあらかじめ認証・認可されたユーザやデバイスのみが，ITリソースにアクセスできる新しい認証モデルである．ゼロトラスト型認証モデルのIDベースという考えにおいては，IDの保護という観点が今後のセキュリティ課題となることから，この問題を解決すべくID秘匿化ワンタイム多要素認証をコンセプトとする認証製品SECUREMATRIX V12を開発した．

1. ID秘匿化ワンタイム多要素認証の概要

1.1 背景

以前まで，多くの企業では業務システムやサービスはオンプレミス，または，セルフホスティングの形をとり，信頼されたネットワーク内に構築してきた．社員は社内環境から該当システムに接続し，社外からシステムを使うことは想定されていなかった．

時代が変わり，クラウドサービスの台頭，テレワークの増加により，従来の境界型の考え方でのセキュリティ担保が難しい時代が到来している．昨今のサプライチェーン攻撃による被害拡大等は境界型の考え方の限界を示す，典型的な例である．

そこで注目されているのがゼロトラストという考え方である．ゼロトラストとは，すべてのネットワークには常に危険が潜んでいると考え，ネットワークの境界ではなくIDベースの認証を，セキュリティの担保とする考え方である．

多要素認証も，近年重要視されているセキュリティ上のキーワードである．総務省公表のテレワークセキュリティガイドライン[1]では多要素認証の重要性がうたわれており（**表1**），主要なクラウドベンダにおいても，多要素認証の積極的な導入が進んでいる．

表1　システム・セキュリティ管理者が実施すべき対策
（テレワークセキュリティガイドライン第5版[1]より抜粋）

管理者 H-1 基本対策	テレワーク時にアクセスする社内システムやクラウドサービスへのアクセスで必要となる利用者認証機能について、技術的な基準（**多要素認証**方式の利用、パスワードポリシーの規定等）を明確に定める。
管理者 H-2 基本対策	社内システムやクラウドサービスへのアクセス時の利用者認証機能として、可能な限り**多要素認証**を強制する。
管理者 H-3 基本対策	テレワーク端末がオフィスネットワークやクラウドサービスに接続する際は、接続先のサーバの正当性（サーバ証明書等）と、接続元のテレワーク端末の正当性（パスワードやクライアント証明書）を相互に認証する仕組みを備えたものとする。
管理者 H-4 基本対策	テレワーク端末へのログインパスワードや、オフィスネットワークやクラウドサービスにアクセスする際のパスワードは、強力なパスワードポリシーの適用を強制する。
管理者 H-5 基本対策	テレワーク端末やアプリケーションの初期パスワードが強制的に変更されるか、十分な強度のある個別のパスワードが個々に設定されるようにする。
管理者 H-6 基本対策	利用者認証に一定回数失敗した場合、テレワーク端末の一定時間ロックや、テレワーク端末上のデータ消去を行うよう設定する。
管理者 H-7 基本対策	異動や担当変更等を適切に把握し、不要なアカウントの削除やアカウント権限の更新等を実施する。

1.2　新しい働き方における認証の課題

1.2.1　境界型認証モデルの課題

既存のシステムの多くが，ファイアウォール等の境界で区切られた，信頼できるネットワークの内側であれば安全であるという考え方を前提とする，境界型認証モデルで構築されてきた．

境界型認証モデルは，社外からのアクセスやクラウドサービスの利用等を想定しない，境界の内部に閉じたネットワークを基本とするモデルであり，ひとたび脅威の侵入を許せば，侵入個所からの横移動攻撃による被害拡大の恐れがある．

テレワークに対応するため，VPN接続等の技術を用いて社外からのアクセスを利用可能とした際には，そのVPN接続されたたった1カ所の脆弱な部分から，ネットワーク全体に被害が拡がる（**図1**）．

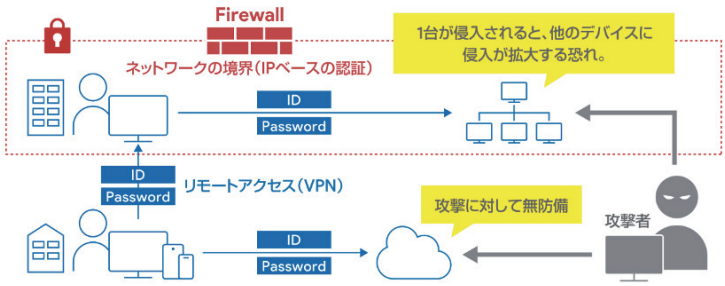

図1　境界型認証モデル

1.2.2　ゼロトラスト型認証モデルの課題

境界型認証モデルの課題を解決するモデルとして注目されているのが，ゼロトラスト型認証モデルである．

ゼロトラスト型認証モデルとは，すべてのネットワークには常に危険が潜んでいると考え，IPアドレスやネットワーク境界ではなく，IDベースすなわち信頼できる本人であることの証明を担保として，どこからのアクセスなのか，どこにいるのかといったネットワーク上のロケーションによらず，IDによってあらかじめ認証・認可されたユーザやデバイスのみが，ITリソースにアクセスできる新しい認証モデルである．ネットワークに依存せず，IDベースの認証を基本とするため，クラウドサービスの利用や外部公開した社内システム等の利用等，いつでもどこでも安全にITリソースにアクセスすることが可能となる．

ゼロトラスト型認証モデルではIDがセキュリティの要となるため，IDの保護がセキュリティ上の課題となる（**図2**）．

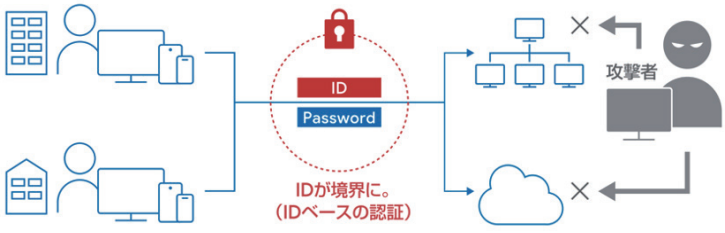

図2　ゼロトラスト型認証モデル

1.3　ID秘匿化ワンタイム多要素認証の提案

新しい働き方における認証の課題を解決すべく，認証に用いるIDを秘匿化し，記憶要素と所持要素の多要素認証をワンタイムで実現するID秘匿化ワンタイム多要素認証（**図3**）を提案する．

図3　ID秘匿化ワンタイム多要素認証

認証経路にID情報を流さず，ユーザによるID入力も不要となるため，ゼロトラスト型認証モデルの課題であるID情報漏洩のリスクを解消し，安心・安全なセキュリティを提供する．認証時のID入力操作が不要となることで，日々の業務で頻繁に行う認証作業の負担を減らし，利便性の向上も期待できる．

1.3.1　マトリクス認証（ワンタイムパスワード）

マトリクス認証とは，認証の際にマトリクス表に乱数を並べ，ユーザが記憶した形からワンタイムパスワードを導出する認証方式である．ユーザはパスワードを文字や数字として覚えるのではなく形で記憶し，認証時には記憶した形の位置と順番からマトリクス表の各マスの数字を入力する（**図4**）．

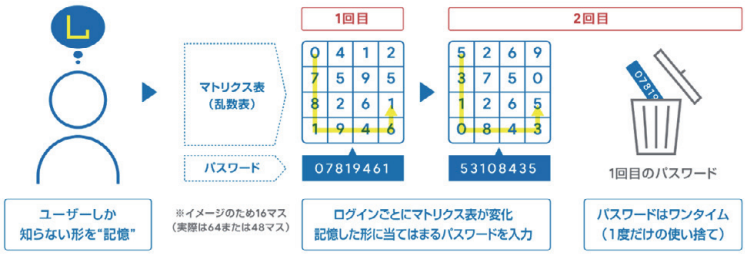

図4　マトリクス認証

マトリクス表の各マスの数字は毎回異なる値となるため，認証を行うたびにパスワードは異なる．仮に悪意ある第三者が通信を傍受してパスワードを窃取したとしても，次回認証時はパスワードが異なるため，悪用することができない．

マトリクス認証は，認証の3つの要素のうち，記憶要素に該当する．

1.3.2　デバイス認証（ワンタイムデジタル身分証）

ID秘匿化ワンタイム多要素認証では，デバイス認証のための電子証明書を各デバイスに付与し，これを保持するデバイスのみ認証を許可している．電子証明書は，ID情報にデバイス情報を初めとするさまざまな属性情報を紐づけて一元管理しており，現実世界の身分証のようにふるまうため，デジタル身分証と名付けた．

このデジタル身分証は認証を行うたびに更新されるため，電子証明書とID情報，双方のワンタイム性を実現しており（ワンタイムデジタル身分証，**図5**），仮に悪意のある第三者が不正に入手したとしても悪用することは困難である．

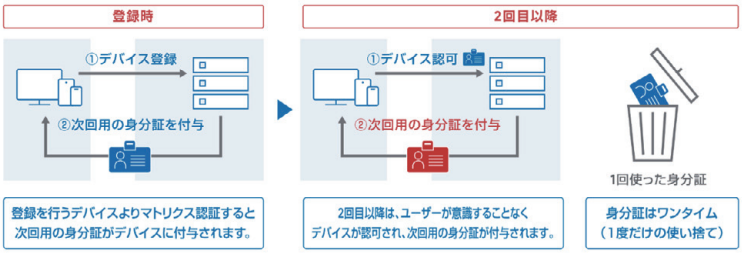

図5　デバイス認証

デバイス認証は，認証の3つの要素のうち，所持要素に該当する．

コラム：認証の3つの要素
認証の3つの要素とは，記憶の認証，所持の認証，生体の認証の3つのことである．それぞれ長所と短所があり，2要素以上を組み合わせて多要素認証を行うことが，テレワークセキュリティガイドラインなどでも推奨されている[1]．

記憶の認証とは，本人だけが知っている情報による認証であり，具体例としては固定パスワードやPINが挙げられる．

所持の認証とは，本人だけが持っている情報による認証であり，具体例としてはICカードやハードウェアトークンが挙げられる．

生体の認証とは，本人の身体的特徴による認証であり，具体例としては指紋認証や顔認証が挙げられる．

1.3.3　ID秘匿化

一般的な認証手順では，ID情報を入力して送信し，サーバに対象のユーザを特定させた上でパスワードの照合を行うが，このような手順において，ID情報は通信傍受やショルダーハッキング等による漏洩の危険にさらされている．

ID秘匿化ワンタイム多要素認証では，ステルスID方式と名付けたパスワードからIDを特定する特許技術により，ユーザによるID入力を不要とし，通信経路上にID情報を直接流さないようにすることで，ID情報漏洩のリスクを解消した（**図6**）．

図6　ID秘匿化

2. ID秘匿化ワンタイム多要素認証の実現

2.1　ステルスID方式

ID秘匿化を実現するにあたり，認証手順に関する新たな技術を発明[2]し，これをステルスID方式と名付けた．

ステルスID方式では，ユーザが入力したパスワード文字列へID情報や属性情報を自動挿入することで，IDの秘匿化を行いながら，パスワードからIDを特定することを可能としている（**図7**）．通常の認証手順では，IDの特定を先行した後にパスワードの照合を行うが，これを逆転し，パスワードからIDを特定するようにした点が，本特許の独創的な部分である．

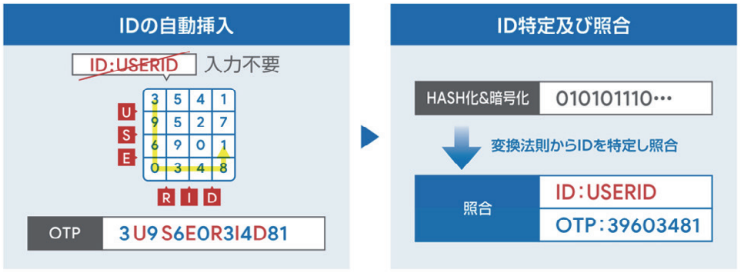

図7　ステルスID方式

パスワードからIDを特定するためには，パスワードがユーザユニークである必要があるが，通常，パスワードは各ユーザが任意に設定するものであり，ユーザユニークとはならない．パスワードをユーザユニークにするため，システムからパスワードを押し付けるようでは，ユーザの利便性が損なわれる．そこでステルスID方式では，ワンタイムパスワードを用いることを前提に，ワンタイムパスワードの生成を制御することで，利便性を保ちながらパスワードをユーザユニークとし，パスワードからユーザを特定することを可能とした．

2.2　ID秘匿化ワンタイム多要素認証の実装

2.2.1　ステルスID方式の実装

ステルスID方式の特許取得に際し，製品実装も同時並行して検討を進めた．

ID秘匿化ワンタイム多要素認証では，ワンタイムパスワードとしてマトリクス認証を採用している．マトリクス認証とは，前述したとおり，システムが提示するマトリクス表にユーザが記憶している位置と順番を適用して，ワンタイムパスワードを導出するものである．これはすなわち，マトリクス認証においては，パスワードの実体である位置と順番はユーザが任意に設定するものだが，ワンタイムパスワードを導出するためのマトリクス表は，システムの制御下にある（つまり利便性を損なわずに押し付けることができる）という状況である．そのため，マトリクス表の生成を適切に制御できれば，導出されるワンタイムパスワードをユーザユニークにすることができ，パスワードからユーザを特定することが可能となる（**図8**）．

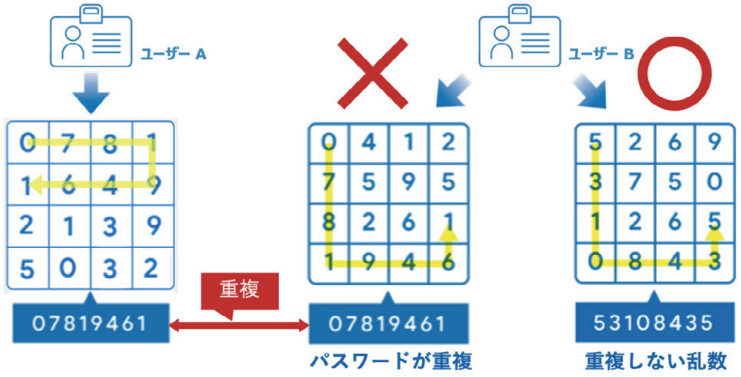

図8　マトリクス表の制御によるユーザ特定

2.2.2　ワンタイムパスワードの生成，入力

ID秘匿化ワンタイム多要素認証の実装では，マトリクス表の生成にワンタイムデジタル身分証を用いることとした．認証時は，事前にデバイスに付与しているワンタイムデジタル身分証の情報より，マトリクス表を生成する．ユーザは，記憶している位置と順番からパスワードを導出し入力する．

2.2.3　認証要求

ステルスID方式では，パスワード文字列にID情報を自動挿入してサーバに送信するが（説明の便宜上，この送信データを認証要求データと呼ぶ），ID秘匿化ワンタイム多要素認証の実装では，IDを直接用いるのではなく，ワンタイムデジタル身分証を利用した．これによりID情報もワンタイム化される．

2.2.4　パスワード検証，ID特定

サーバでは事前に，ユーザごとの正しい認証要求データを保持しており，デバイスから送信された認証要求データと照合して評価する．認証要求データが一致すればパスワードとIDの両者が一致したことになり，認証が成功したと判断する．

この際，認証要求データの照合のみではIDの誤認が発生し得ることが，検討時の最大の課題であった．ユーザは必ず正しいパスワードを入力するわけではなく，誤ったパスワードを入力することにより，別ユーザの認証要求データと偶然に一致することで，IDを誤認する可能性が考えられた．

そこで，IDの誤認を防ぐため，サーバは認証要求データの一致を確認後，デバイスに対してワンタイムデジタル身分証の送付を要求し，認証要求データとデジタル身分証の組合せが正しいことを確認することで，この課題を解決した．

このように，すべての通信個所においてIDをワンタイムデジタル身分証に置き換えることで，通信経路上でIDが窃取される危険性を回避している．

2.2.5　ワンタイムデジタル身分証の再付与

認証処理後は，デバイスとサーバから認証に用いたワンタイムデジタル身分証を削除し，新たに生成した次回用のワンタイムデジタル身分証を，デバイスとサーバの双方で保持する．

ワンタイムデジタル身分証は，利用時にワンタイムパスワードと一致させる必要があり，認証失敗時に失効してしまう一回使い切りのデータであるため，仮にこれを不正に窃取されたとしても，第三者が悪用することは困難である．

3. SECUREMATRIX V12

ID秘匿化ワンタイム多要素認証の実装として，2020年11月にリリースした製品が，SECUREMATRIX V12である．

SECUREMATRIX V12では，ID秘匿化ワンタイム多要素認証を，Windows PCへのサインインでも利用可能とした．

ワンタイムデジタル身分証の属性情報としてクライアント証明書を紐づけることで，ユーザがPCにサインインするだけで，SECUREMATIRX V12と認証連携を行っているWebシステムやクラウドサービス，ネットワーク機器等の認証が自動で行われることになり，ユーザの利便性が飛躍的に向上した．

ID秘匿化ワンタイム多要素認証を開発するきっかけとなったのは，認証時のセキュリティ強度を上げるために，認証要素を増やし手続きを増やすという一般的な方法論では，利用者の利便性が考慮されていないと考えたことである．セキュリティ強度と利便性を両立する技術を開発することは困難であったが，検討を重ねた結果，認証モデルの課題を解決し，セキュリティ強度と利便性をともに向上するものとなった．

4. 今後の展望

SECUREMATRIX V12は，ID秘匿化ワンタイム多要素認証をコンセプトに，ID秘匿化の特許を取得し，ゼロトラスト型認証モデルを実現するソリューションとして開発した．開発に際しては，時代の流れに合わせて変化してきた認証モデルの弱点に着眼し，改善を行うとともに利便性も追及した．

今後，5G通信・6G通信のようなテクノロジーの発展に伴い，モバイルデバイスやIoTデバイス等で新たなセキュリティ課題が発生することが予想される．このような課題に対し，独創的・革新的な技術で解決を図ると同時に，利便性も追求した研究を進めることで，テクノロジーを利用するすべての人々に安心・安全を提供し，これからの社会を支えていきたいと考えている．

参考文献

1）総務省：テレワークセキュリティガイドライン第5版（令和3年5月）．
2）（株）シー・エス・イー：特許第6721225号，ユーザ認証システム，ユーザ認証サーバ，およびユーザ認証方法（2020年6月22日登録，2020年7月8日発行）．

下平哲也（非会員）tetshimo@cseltd.co.jp
2008年（株）シー・エス・イー入社．通信インフラシステムの制御プログラム開発，Webシステム開発等を経て，2018年セキュリティ戦略部 部長に就任．

受付日：2021年11月20日
採録日：2022年1月18日

編集担当：西山博泰（日立製作所）