Vol.2011-CSEC-54 No.10
Vol.2011-SPT-1 No.10
2011/7/12

耐災害本人認証基盤の構築
- 不死鳥パスワード構想 -

縄田　好寿[†]　國米　仁[††]

大地震大津波の脅威にさらされている日本では，出張先や旅行先で「着の身着のまま」で実行できる本人認証手段を考慮しておくことが望ましい．身体の負傷も視野にいれると記憶照合が最も頼れる本人認証手段であるが，文字パスワードでは可用性と機密性の両立が困難なのに対し，自伝的記憶であるエピソード記憶を活用する画像記憶方式によるならばパニック状態を想定しても可用性と機密性を容易に両立できる．人間が主人公として安心して暮らせる情報社会を実現する観点から，こうした耐災害本人認証基盤の構築を急ぐことを提唱する．

Cyber Platform for Disaster-Tolerant Identity Authentication

YOSHIHISA NAWATA[†]　HITOSHI KOKUMAI[††]

Living in a country threatened by earthquakes and tsunamis that may hit at any time, we should be prepared against the disasters in which we become refugees naked with nothing to certify our identity for coming back to the social life which is now intertwined by real and cyber spaces. We propose to build a cyber platform for disaster-tolerant identity authentication in the belief that graphical passwords made of autobiographical episodic memories can satisfy confidentiality as well as availability at the same time even in a disaster-triggered severe panic.

1.　はじめに

１６年前の阪神大震災も今回の東日本大震災も被害は甚大とはいえ国全体でみれば中枢機能はほぼ無傷であったが，やがては太平洋沿岸を襲うであろう東海・南海大地震大津波では事情はまったく異なるだろう．通信網の多重耐震化やデータの遠隔地分割保管については関係各位の奮闘に期待するとして，本稿では本人認証事業では何ができるかを考察してみたい．

大災害に遭遇しパニックの中で財布も免許証も手帳も携帯電話も失い，周囲に身元を証明してくれる人が誰もいないという状況での本人認証を考慮しておくことが望ましい．一切の所持物を失ったところから出発して身体の負傷も視野にいれると記憶照合が最も頼りになる本人認証手段となる．記憶照合のなかでも懐かしく愛着のある画像を利用する方式ならばパニック状態を想定しても可用性を維持して所期の目的を果たすことができる可能性が高いと考えられる．

２．本人認証の変遷と記憶照合の意義

先ずは大災害などの異常事態を視野にいれつつ本人認証の変遷について考えてみたい．

①　特定の本人認証手段を意識する必要のなかった有史以前

狭い共同体の中や周辺のみで社会生活が行われた時代があったと想定してみると，そこでは特定の本人認証手段を意識する必要などなかっただろうと推測される．

当人が誰であるかは当人が母親のお腹の中にいるときから周囲の全員が知っており，もし大怪我をして顔や身体の特徴や声からは特定ができなくても当人と他の共同体メンバーとが共通の継続した記憶を共有していることが判れば共同体メンバーは確信をもって当人を本人であると認めることができただろう．

②　所持物ないし署名を手段とする本人認証を必要とした歴史時代

遠隔地にある共同体との交流や帰属の関係が始まると初対面の人物の前で自らの身元を証明する何らかの手段が必要となる．

[†] 然株式会社
Zen Co. Ltd.
[††] 株式会社ニーモニックセキュリティ
Mnemonic Security, Inc.

Vol.2011-CSEC-54 No.10
Vol.2011-SPT-1 No.10
2011/7/12

模倣や複製の困難な手形・拇印・花押・署名や印鑑・印籠が登場する．時に破られることもあったろうが，こうした本人認証手段は採集狩猟社会・農耕社会から近代工業社会を通じて最近まで有効な手段として頼られてきた．目立たない存在ではあるが，それなしでは社会生活が根本から成り立たないという意味でインフラの中のインフラと言えるだろう．

さて，災害などの異常事態の時にはどうしていたかを考えてみるに，結局は当人と関係者の間で共通の記憶を確認する以外には決着を付けようがなかったと思われる．また，災害時でなくとも提示された所持物に贋造や盗用の可能性が疑われるときには，やはり当人と関係者の間での共通の記憶の確認が望まれたと考えられる．

例えば，見知らぬ軍服姿の男が現れて軍司令官の指示書を出し「諸君は今から私の指揮下に入る．」と言ったとしよう．「司令官殿は次の誕生日には髭を剃ると言っておられました．一週間前に誕生日を迎えられたはずですが約束どおり髭は剃っておられましたでしょうか？」といった種類の引っ掛け質問に対しては偽者なら「剃っておられた」か「剃っておられなかった」と答えてしまうだろう．「そんな約束をしたとは聞いたことがない．もともと髭など生やしておられなかっただろう．」と答えられない限り，提示した指示書が本物であれ偽者であれ，この人物は成りすましを試みた偽者であると判る．こうしたやり取りを幾つも繰り返し全て通過して初めて部下達は指揮下に入ることに納得するだろう．

有史以前でも歴史時代でも，当人と周囲の人々との間で記憶の共有を確認する方法はいつでも最後の砦として頼られてきたものと思われる．

③　電子的本人認証が必須となるサイバー時代

対面での質疑応答が例外となるネットワーク環境を前提とするサイバー時代ではこれまでは考える必要もなかった電子的本人認証手段が必要になってきた．サイバー空間では印鑑・手形・拇印・署名といったものの提示によって本人認証を行うのははや現実的とは言えないからである．

印鑑はＩＣカード，チップ入りトークン，携帯電話など電子的に真正性を証明し得る所持物に姿を変え，手形や拇印に代わって指紋・静脈紋・顔貌など肉体の特徴点を計測照合する静的バイオメトリクス，署名に代わって暗証番号・パスワードやサイン照合・行動パターン照合などの動的バイオメトリクスが登場してきた．パスワードは当初は文字しか使えなかったが最近になってデジタル画像処理技術の高機能化・低価格化とともに画像パスワードという選択肢も現れてきた．

それぞれの特徴について概観してみると，

所持物：　災害やトラブルに遭遇した利用者を想定すると，利用者はいつでも必ず保持しているものと前提するのは非現実的と思われる．

バイオメトリクス（生体認証）：　利用者の負傷やパニックを想定しなければならない災害場面でいつでも可用であると考えるのは難しい．

文字パスワード：　原理上は当人が意識喪失状態では実行しえないので機密性の基本要件は満たしている．メモに記載して持ち歩かない限りは，つまり，所持物に化けていない限りは，災害時に着の身着のままとなっても理屈のうえでは実行可能のはずである．

しかしながら，「覚え易いパスワードは破られ易い」→「長大なパスワードを何とか覚えて公私混同使い回し」→「使いまわしを禁止されると覚えやすいパスワードを登録」と繰り返される閉鎖サイクルからなかなか抜け出せない．この問題は平常時でも大きな頭痛の種だが，災害に巻き込まれてパニックになったような状況ではひときわ際立つ．極度のパニック状態でも長大で無機質なパスワードを難なく思い出せる人は極く少数派だろう．少なくとも筆者には無理である．

画像パスワード：　認知心理学では「文字記憶に対する画像記憶の優位性」，「再生（穴埋問題の解答）に対する再認（選択問題の解答）の優位性」，「加齢における文字エピソード記憶に対する画像エピソード記憶の優位性」が既知となっている．

Vol.2011-CSEC-54 No.10
Vol.2011-SPT-1 No.10
2011/7/12

なお，有史以前からの「当人と周囲の人たちとの継続した記憶の共有確認」はサイバー空間では「当人の記憶と認証ソフト登録情報の共有確認」で代行されていると考えられる．

注１：　記憶の主観性

サイバー空間の性格を考えると，電子的本人認証手段は時と場所を選ばない無制限の脅威に曝され続けるものと想定しておかねばならない．最先端の IT 知識と悪知恵に長けた頭脳集団の執拗な組織的攻撃にも耐える強靭さが必要である．

どんなに頭の良い攻撃者が如何に手の込んだ攻撃方法を考え出しても，個々人それぞれが長い人生の中で蓄積してきたその人固有の自伝的な記憶をその人の主観的な文脈通りに取り出すことはできない．本人であれば簡単に主観的な文脈通りに取り出せる秘密情報，それは過去の懐かしい自伝的な記憶．こうした過去の懐かしい記憶をイメージとして活用することで，人格の尊厳を損なうことなくストレスのない安心で確実な本人認証を実現できる．

こうした自伝的イメージ記憶を活用できる電子的本人認証技術は，文字パスワードが果たすものと期待されていながら果たしきれなかった秘密情報の確実な照合を最新のデジタル画像技術の活用によって果たすものと位置づけられる．

この中に私自身が登録した愉しく懐かしい画像が幾つか.何時でも何処でも私には難なく見つけられる.全て正しく見つけられるのは世界中で私だけ.

自伝的記憶につながる画像を登録し無感動な画像を囮としていれば災害時のパニック状態でも速やかに識別して選択できる可能性が高い.

注２：　想い出写真の効用

文字を入力する「再生」から画像を選ぶ「再認」に移行するだけでも記憶の負担がはるかに軽くなるが，更に自分の気に入った写真を選ぶのは楽しいという歓迎すべき副次的効果も出てこよう．

また，想い出写真には一般的効用として認知症の進行抑制や孤独感の軽減などの効果があることが判って来ている．懐かしく愉しい想い出写真をネットワーク上に保管しておき，一方ではこうした一般的な効用の期待できる用途で活用しつつ，他方では「着のみ着のまま」になる災害時でも不自由なく実行できる本人認証に利用するといった連携システムの構想も進んでいる．

④　電子的本人認証技術の寿命

電子的本人認証手段としての「所持物の保持」,「生体の特徴点」,「文字パスワード」,「画像パスワード，特に自伝的画像記憶活用型」の差異は原理的なものであり，サイバー空間がサイバー空間である限りその相対関係は将来も変わらないと思われる．

やがては脳と直接交信して本人を認証できるようになるのではないかと考えることは可能だろう．ただし，こうした方法が簡便に実行可能になったとすると第三者による情報窃取も容易になるのだから，脳内情報が固定したものであれば無断で情報を窃取した攻撃者によるリプレーを考えなければならない．対策としては利用者に提示される一時的にユニークな情報に対する一時的でありながらも本人固有の反応をモニターすることが必要になるが，可用性も同時に満たそうとするとやはり自伝的なイメージ記憶の利用が望ましいと考えられる．

実装技術や運用技術は止まることなく進化を続けなければならないが，自伝的な記憶を活用できる画像活用型本人認証という技術範疇そのものの寿命はサイバー時代の続く限り続くと考えてもよいのではないかと思われる．

３．機密性の考察

可用性における画像利用パスワードの優位性は上述のように顕著であるが，本人認証手段としては併せて機密性の検討が欠かせない．主に問題となるのは「覗き見」，「数学的強度」，「推測攻撃」の３つであろう．

①覗き見：　覗き見（ショルダーハッキング）に対しては文字パスワードのタイプ入力に比べて画像選択型は脆弱であるとの見解もあるが，文字であれ画像であれ利用者が無防備であれば共に覗き見され得るし，注意して画面や指の動きを遮蔽すれば肉眼によるものであれビデオ盗撮であれ共に覗き見を防げる．画像だから文字より脆弱ということはない．

Vol.2011-CSEC-54 No.10
Vol.2011-SPT-1 No.10
2011/7/12

②数学的強度：　任意の文字パスワードと同じ数学的強度になるように画像を登録することができれば手動の総当り攻撃に対して画像方式は文字方式に対して優位でも劣位でもない．利用者は守るべき情報資産の価値と利用時の手間隙のバランスを図って適切なマトリックスサイズと登録画像数を選べばよい．

③推測攻撃：　ある特定の利用者の好悪・人脈・趣味などの情報を入手しての推測攻撃に対しては以下のようなガイドラインの提示で対抗することが考えられる．

- 日頃から好きだと公言している人物やブランド品ばかりで正解データを作るのは不可．
- いつも自宅外で持ち歩いているものを正解データにすることは不可．
- 家族から情報を守るのが主目的の人が家族や親族の画像ばかりを正解データに使うのは不可．
- 雛型の上に追加したものを全て正解画像として登録することは不可．
- 正解データは全て古い写真ばかりで，囮は全て新しい写真ばかりは不可．
- 位置・パターンを記憶の場合，四隅・直線・斜線・単純なアルファベットやカナを使うのは不可．

上述のように画像活用方式は運用方法を間違えない限り一定の可用性を維持しつつ文字方式よりも高い機密性を実現し，或いは，一定の機密性を維持しつつ文字方式よりも高い可用性を実現出来るものであると考えられる．

４．顛倒夢想

今のサイバー世界を作ることになった情報通信技術は当初は軍事目的で開発された．ENIAC は大砲の弾道計算が目的であったし，インターネットは核攻撃を念頭に遠距離のコンピュータを繋いでその危険を回避するのがもともとの目的だったと言われている．

コンピュータは一文字の違いで誤作動する代物である．人間のようには曖昧なデータや情報を柔軟に解釈してくれない．こうした技術がそうした原理的特徴を変えないままに軍事用から民生用に開放されるのだが，当初の軍事的な要素を引きずった故か人間に奉仕するというより人間の奉仕を要求し，人間に管理されるのではなく人間を管理支配する視点が色濃く残存しているように思われる．民生用途では人間の福祉が目的であるが，その目的実現のための手段である情報通信技術が自己目的化してしまっているとも言えるのではないか．

サイバー空間において個人情報を集積するのは最終的には当人の福祉のための筈であり本人に関わる情報の管理権は当人に属するべきものであるであるのに，それがいつしか本人の判断を介在させないでコンピュータ計算能力に管理を委ねるようになってしまったように思われる．自分の情報を自らが管理できない状況では『安心』など存在できるわけはないが、本稿のテーマに即して述べるならば『当人が意識不明であっても実行できてしまえる本人認証』などというものが存在し得るように語られている状況とは何かということである．

自己の情報の管理権は自己にあるという原則に立脚するならば，本人認証は意識不明では実行できないような手段手法によって実行されるべきであるということは明らかと考えられる．

５．『着の身着のまま』本人認証

一切の所持物を失ったところから出発して身体の負傷も視野にいれると記憶照合以外に頼れる本人認証手段はない．同じ記憶照合でも，文字パスワードでは可用性と機密性の両立は困難，エピソード記憶を活用する画像記憶方式ならば可用性と機密性を容易に両立でき所期の目的を果たせる．

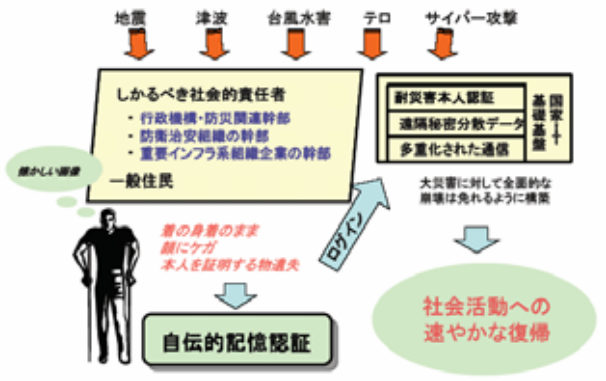
着の身着のままとなる状況を想定してみよう．いずれ必ず起こると予想されていた大地震がついに起り大津波が広く東京湾から大阪湾までの太平世沿岸を襲った．出張中に津波に遭遇したＡ氏はパニックの中で財布も免許証も手帳も携帯電話も失った．周囲に氏の身元を証明してくれる人はいない．もし面識のあった人がいたとしても負傷で顔が変わっていれば判らない．

Ａ氏は

- 行政機構の防災関連幹部
- 防衛治安組織の幹部
- 重要インフラ系組織企業の幹部

のような位置の人で，一刻も早い業務復帰が国と社会のために望ましく，他方もし悪意の第三者による成りすましを許してしまうと国と社会が大きなダメージをこうむる，そうした人物と考える．例えば火を噴き出した原発の迅速な鎮火に貢献できる知見を持つ関係者なども．

Vol.2011-CSEC-54 No.10
Vol.2011-SPT-1 No.10
2011/7/12



たどり着いた支援拠点で誰かが通信機能の生き残っている情報端末を持っていたら，そこで住所氏名などのパニック状態でも何とか思い出せるであろう基本情報を指か音声か視線追跡で入力するとＡ氏として登録していた認証画面が表示される．Ａ氏が本人ならばパニック状態でも再認できる正解画像を過不足なく選択し，指か音声か視線追跡かで正しく入力できる．

そこで救護所の責任者に自称Ａ氏が真正のＡ氏であることの証明書を発行してもらって，最寄の銀行でキャッシュを借り，健康保険で持病の治療を継続して受け，もし備えがあれば携帯電話の臨時貸与も受けられ，ようやくパニックを脱し落ち着いて業務を再開する．証明書には初期登録時のＡ氏の写真に加えて救護所で撮影した被災時のＡ氏の写真も併せて印刷しておくことも考えられる．

支援拠点発行の証明書記載内容に加えて時刻・位置情報その他の付加情報も含む電子版コピーを同僚がネット上で確認することができるようにすれば，悪意ある攻撃者が遠隔地のＡ氏に成りすまして重要な権限を乗っ取る可能性は極小化される．

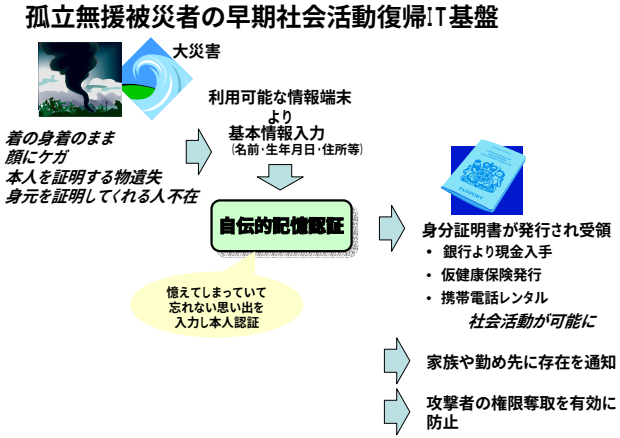
地元で被災した場合には事前の登録のない場合には被災者救護所において急ぎ登録してもらうことも考えておきたい．利用状況の一例を想定してみる．

１．避難所には陸海空からネット接続ＰＣ及びスキャナー，デジカメ又はデジカメ搭載モバイル端末が配られる．

２．公的機関で本提言の本人認証サイトが立ち上がる．

３．被災者は避難所で町長や自治会長などの立会いのもとで名前・住所をＩＤとして自伝的記憶による画像パスワードの登録をする．避難所での隣人・知人やそこの事物・風景の写真を撮って使うのも一案．

４．被災地から遠隔地に転出したＢさんは転入先にある通信端末で名前・住所を入力して自分の画像認証画面を呼び出すと「着の身着のまま」であっても本人であれば認証を通過でき，転入先で身元の確かな市民としての生活を始める．犯罪者による安否不明被災者の身元詐取も排除できる．

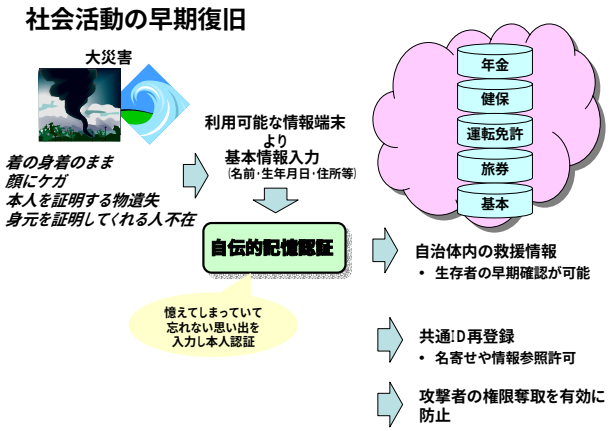


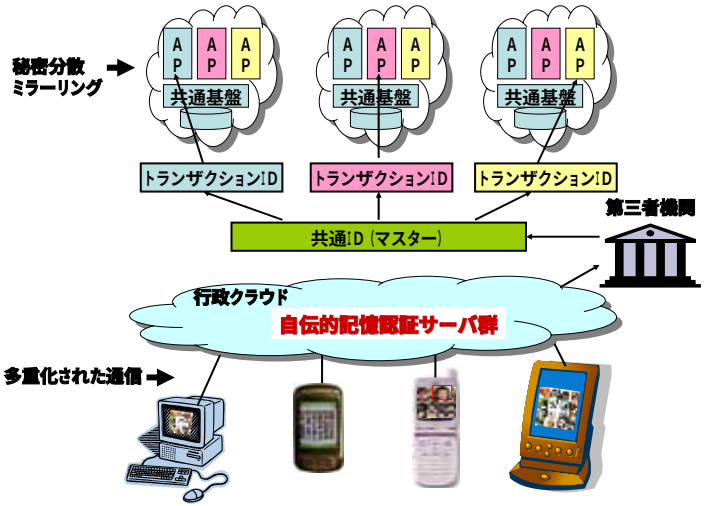
視点を事業主体側に移してみる．事業所内のシステムは破壊され紙台帳も喪失したとしても利用者の本人認証に関わるデータやアプリケーションは秘密分散技術を利用して遠隔地に分散保管されていれば認証サービス機能はクラウド上に機能を維持できている．

身元を証明するものを失いパニック状態になっている被災者であっても，本提言方式による本人認証システムが作動すれば避難場所の無線等で動くＰＣやＧＰＳ付携帯端末，或いはその場に居合わせた人がスマートフォン等を保持していれば即座に本人

Vol.2011-CSEC-54 No.10
Vol.2011-SPT-1 No.10
2011/7/12

認証を始めることができる．それによりアクセスできた被災者と，アクセスできない被災者（死者の可能性も）が短時間のうちに仕分けが可能となり，被災者対策の初期情報として大いに役立つことになる．





6．災害時にも停止しない情報通信基盤

平常時に屋内で運用可能だからといって災害時に屋外でも運用可能とは限らないが，災害時に屋外で運用可能なシステムは平常時には余裕をもってどこでも運用可能である．つまり異常事態専用のシステムを作ることにはならず，システムは汎用的に全国民的規模に拡張できる。本提言の本人認証基盤は災害時にも運用を止めることのない平時運用の基本的な情報通信基盤の一部として利用される．

こうした災害時にも運用を止めない情報通信基盤構築は (i) 自伝的画像記憶認証による本人認証基盤の耐災害化，及び(ii) 有線・無線・衛星などに通信の多重化による耐災害化，(iii) 遠隔秘密分散保管によるデータ保管の多重化による耐災害化を基本要件とした基盤層の上で重層的な ID 連携やデータ連携が機能するものとなることが望まれる．

関連領域

クラウドコンピューティング
電子的割符
電子証明書発行
オンデマンド印刷
携帯無線･衛星通信
音声認識･視線追跡･脳波計測
画像収集･加工･編集
＋
写真預託 (情報銀行)
＋
認知心理学･法学･経済学

Vol.2011-CSEC-54 No.10
Vol.2011-SPT-1 No.10
2011/7/12

７．終わりに

米国では大統領府が「アイデンティティ・エコシステム」を提唱しているが，本提言のテーマはそうした問題意識の方向性を先取りするものでもある．我々の提言がこうした世界大での動きのパイオニア的事業として早期に実現されることを願うものである．

参考文献

1) 北神慎司，原田悦子，桝野隆平，鵜野幸一郎：人の視点から考えるパスワード問題：認知心理学の観点からの提言（2011)
2) National Strategy for Trusted Identities in Cyberspace: http://www.dhs.gov/xlibrary/assets/ns.tic.pdf