

生体情報を表出させずに 秘密情報の再生を実現する 筋電位EMSシステム

静岡大学 情報学部 情報科学科
教授 西垣 正勝

2024年11月28日

従来技術とその問題点

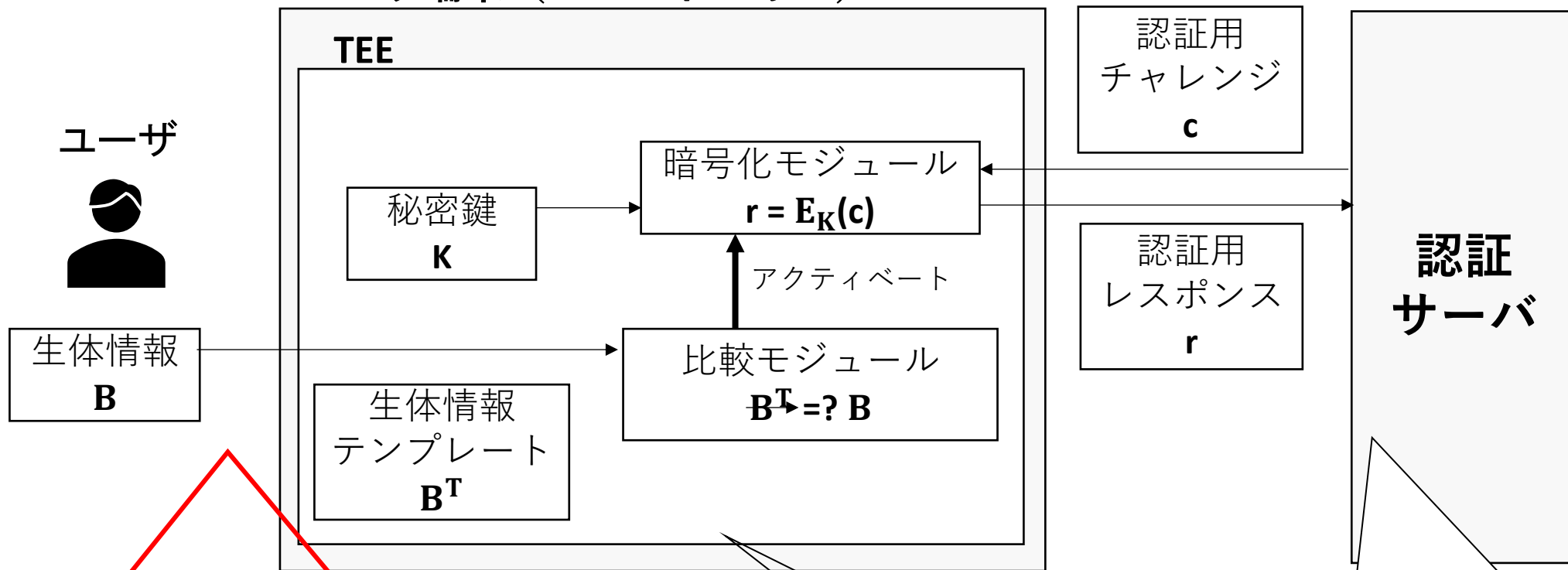
生体認証には「生体情報は生涯不変である」ことに起因する問題点が存在する。

FIDO生体認証（FIDO [1]+生体認証）を使用することで、ユーザ端末（スマートフォン）外に生体情報を登録する必要はなくなるが、認証時には生体情報を端末に提示する形になるため、生体情報の漏洩リスクが残る。

[1] FIDO Alliance: FIDOとは, (オンライン), <https://fidoalliance.org/fido%E3%81%A8%E3%81%AF/?lang=ja>
(参照2023-06-06).

FIDO生体認証

ユーザ端末 (スマートフォン)



生体情報を端末に提示する際に、生体情報の漏洩リスクが残る (例: マルウェアがセンサに感染した場合、マルウェアはセンサが読み取った生体情報を取得可能)

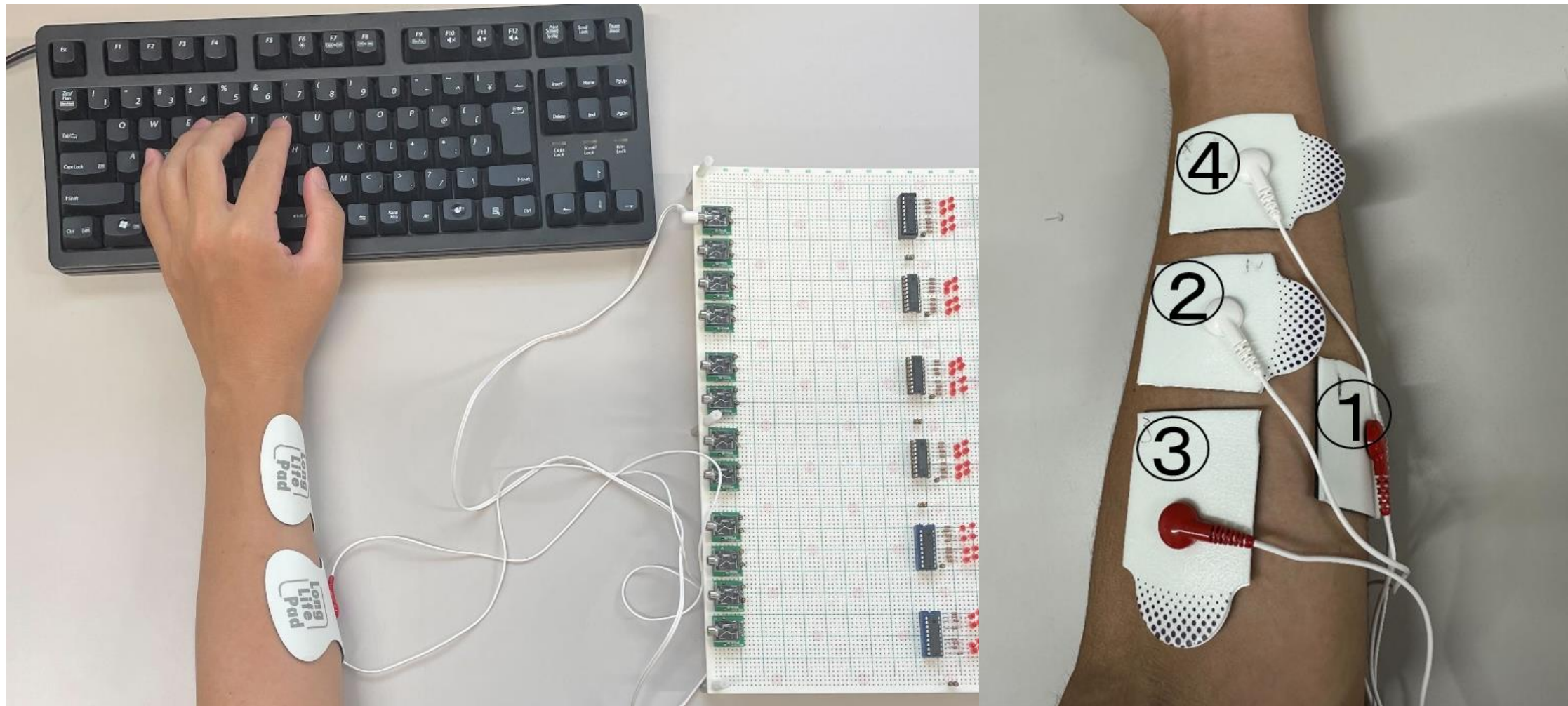
生体情報はユーザ端末 (のセキュア領域) 内に格納され、認証の際にも通信経路上には表れない

新技術の特徴・従来技術との比較

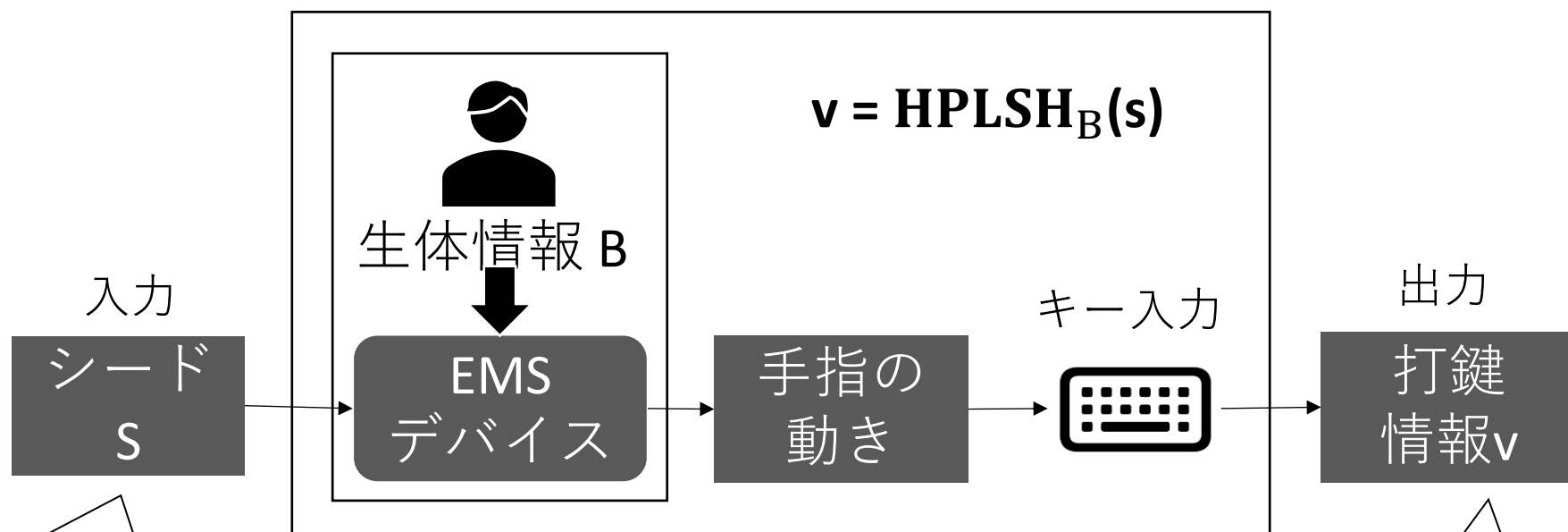
- 生体情報を「データを変質させる媒体として利用する」というアプローチによる、新たな生体認証技術の提案。
 - 記憶認証 = パスワード、持ち物認証 = スマートフォン、生体認証 = 生体情報という区分を壊して、「生体情報に基づくパスワード認証」を新たに実現。
- ユーザの前腕に装着した電氣的筋肉刺激（EMS）デバイスから電気刺激を流し、ユーザの手指が不随意的に動くことで生じるキーボードの打鍵情報によって認証情報を生成（P5-P6）。
 - ElectricAuth [2]は、生体情報（電気刺激を加えた際の筋肉の反応）そのものの個人差を本人認証に用いている。
 - 新技術は、生体情報を打鍵情報に変換し、打鍵情報を用いて本人認証を行っている。（打鍵情報の漏洩 ≠ 生体情報の漏洩）
- 3つのメリット（P7-P14）を有する生体認証の実現。

[2] Chen, Y., et al.: User Authentication via Electrical Muscle Stimulation, Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Vol.6, pp.1-15 (2021).

特徴：生体情報を「データを変質させる媒体」として利用する



特徴：生体情報を「データを変質させる媒体」として利用する



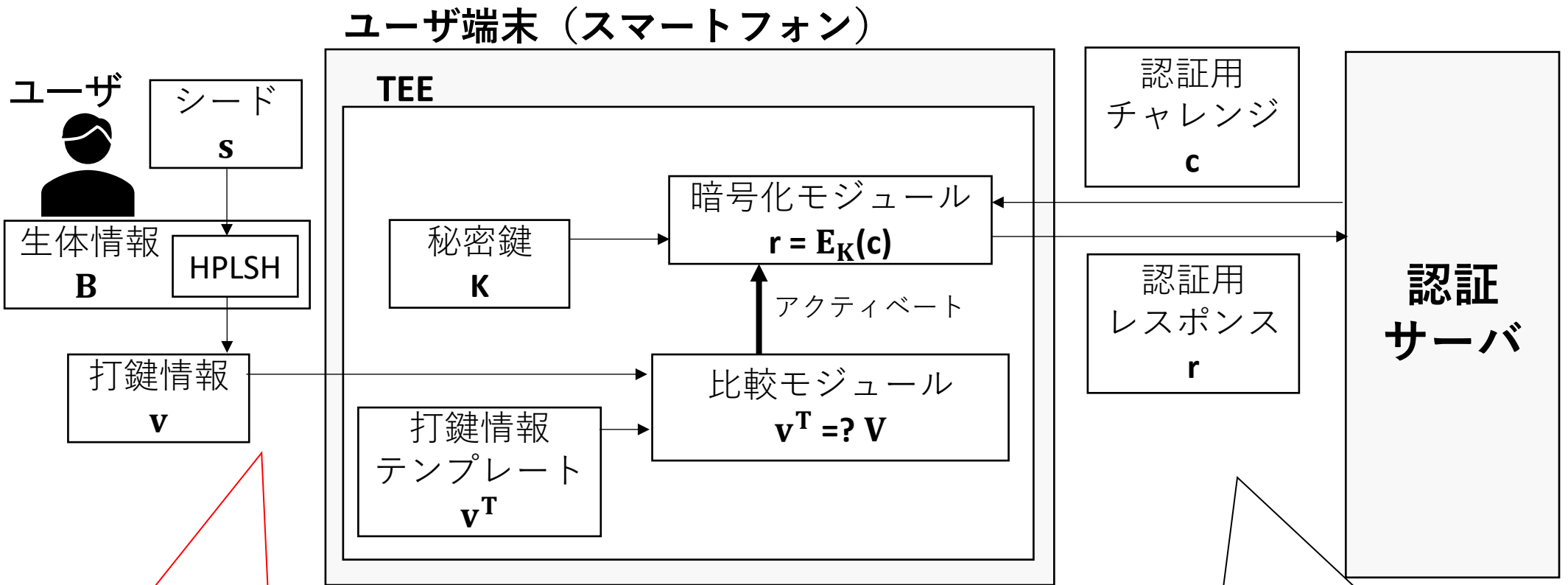
入力される情報は「乱数」
(EMS電気パルス)

乱数はいつでも変更
(して再登録) 可能

生体情報をセンサに提示しない

生体情報 (EMS信号に対する
筋反応の個人差) に応じた
打鍵情報が得られる

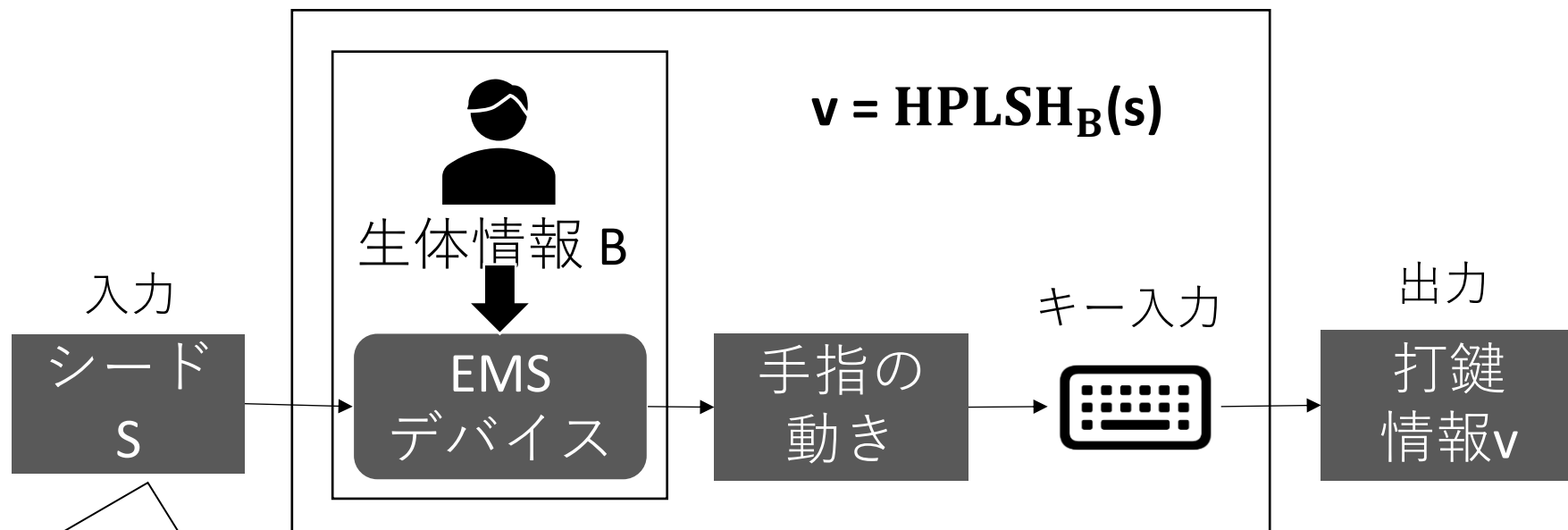
メリット1: 生体情報が表出しない 生体認証を実現可能



生体情報自体をセンサに提示することはない

生体情報はどこにも格納されておらず、通信経路上にも表れない

メリット2: 記憶負担のない形で非常に長いパスワードを用いたユーザ認証が可能



シードを長くすればするほど
生成される打鍵情報も長くなる
(超長いパスワードを脳外に
記憶していることに相当)

メリット3: 近未来の「EMSを用いた自動人体操作環境」との親和性

- 従来, 人間の体はブラックボックス (それ以上分解できないもの) として考えられてきた
- 技術の進化に伴い, 人間を臓器単位に分解して捉えることが可能になってきた
 - 眼球や腕などを人工的なものにする[3,etc]
 - 「記憶」をマイクロチップなどで代替する[4,etc]
 - BMI (Brain Machine Interface) を用いて意思疎通を行う[5, etc]

[3] Gu, L., et al.: A biomimetic eye with a hemispherical perovskite nanowire array retina, Nature, Vol.581, No.7808, pp.278-282 (2020).

[4] 未来コトハジメ: 脳をデジタル化することで永遠の命の実現は可能になるのか, https://project.nikkeibp.co.jp/mirakoto/atcl/robotics/h_vol38/?P=2 .

[5] 産業技術総合研究所: 脳を読み取る新型コミュニケーション, https://www.aist.go.jp/aist_j/magazine/s0004.html .

Internet of Functions (IoF)

- 人間を臓器単位で捉えることが可能になると、自身の身体機能をパーツ単位で制御可能になる
- そのような世界（ここでは「IoF」世界と呼称）では、個々のパーツは機能ごとにAPI化され、各機能を自由に呼び出して自在に利用することができるようになる

IoF世界の人体

- 身体の欠損・機能低下に対し、パーツを取り替えることにより能力を回復させることが可能
 - 視力が低下した際に、眼球ごと取り替える
- 機能拡張用の人工パーツを使用することにより、身体機能の増強が可能
 - 筋力が高いパーツ（腕）に取り替えることで、重い荷物の持ち運びが可能に
- 高い能力を有する他者の能力を借用することが可能
 - スポーツ選手の能力をデータとして保存し、電気刺激を介して自分の体を駆動
- 他者と五感を共有することが可能
 - 手パーツが物を持った際の「振動」をコピーして他者に送信することで、触覚の共有が可能に

IoF世界のセキュリティ

- これまで人間を「ブラックボックス」として捉えることで成り立っていた従来のセキュリティ技術を、「パーツ（機能）」単位で捉える必要がある
- 人体がパーツごとに分解された結果、アタックサーフェスが増加し、不正者による攻撃が複雑化・激甚化することが考えられる
- 現在の「ユーザ認証」を身体機能（パーツ）ごとに分解した場合について考えることから始める
 - IoF世界でも、ICTを利用するためには必ず「サイバー空間にログインする」必要がある
 - ユーザ認証は必要不可欠で本質的なセキュリティ要素の1つ

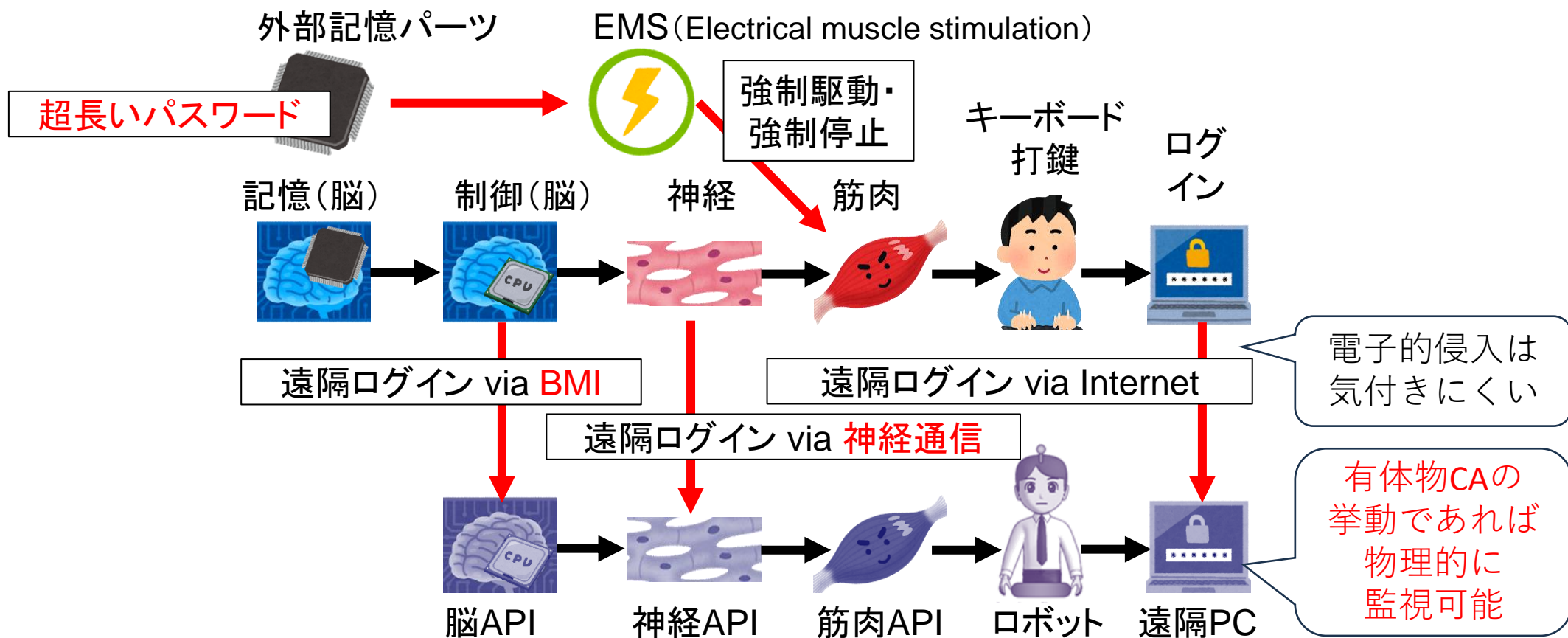
IoF世界のセキュリティ

- ユーザ認証とは：
 - 物理空間の住人である人間が有する何らかの「クレデンシャル」を、何らかの「入力手段」によってサイバー空間（コンピュータ）に入力する行為
- IoF世界のクレデンシャル：
 - 記憶：記憶補助パーツによってサポートされる形に変化
 - 持ち物：身体パーツを自分の持ち物として使用する形に変化
 - 生体情報：身体パーツを自分の生体として使用する形に変化
- IoF世界の入力手段：
 - 新技術とともに新しい入力手段は増えていく（例：ゲームやVRに対するにコントローラ型デバイス）が、
 - ペン/キーワード/マウス（約8000/150/60年前からその形は変わっていない）も使用され続ける

IoFパスワード認証における

新たな3つのセキュリティメカニズム

- 外部記憶パーツを用いたパスワード長の増大
- ロボットを利用したの遠隔ログイン **本発明**
- 認証失敗時の筋肉機能の停止



想定される用途

- 生体認証の表出が許容されないシーンにおけるユーザ認証
- EMSを用いた自動人体操作環境における近未来型ユーザ認証

実用化に向けた課題

- EMSを用いた自動人体操作技術は、まだまだ道半ばであり、4指の制御しかできていない。
- 再現性もまだ十分とは言えず、それ故に認証精度も低い。
- 実用化に向けて、多くのハードルを乗り越える必要がある。

初期実験の結果

1. 電極の組特定実験

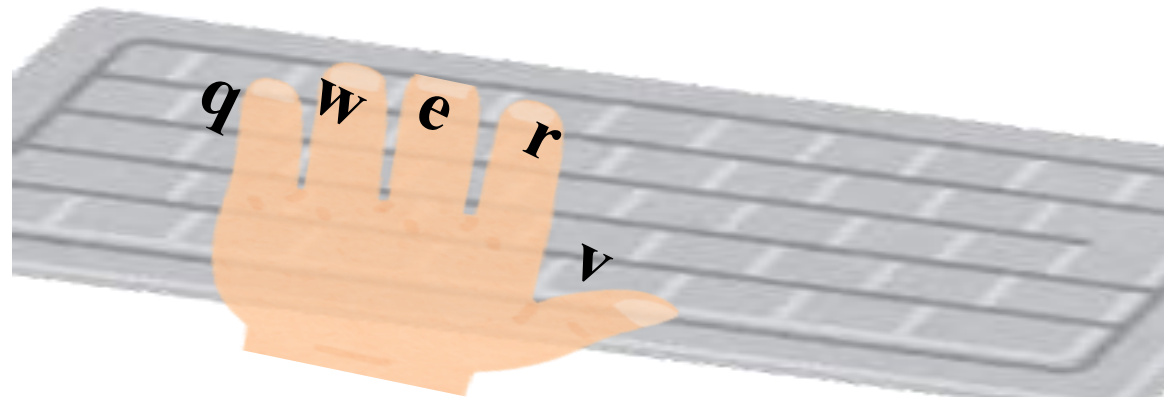
- ユーザの手指を動かすための電気刺激s（電極の組）を特定

2. 疑似的ユーザ認証

- 1で特定した電気刺激sを使用し、自分の指をどの程度制御可能か検証（本人一致率の評価）
- 1で特定した電気刺激sを他人に使用することで、他人の打鍵がどの程度自分の打鍵と類似するのか検証（エフォートなしの他人受入率の評価）

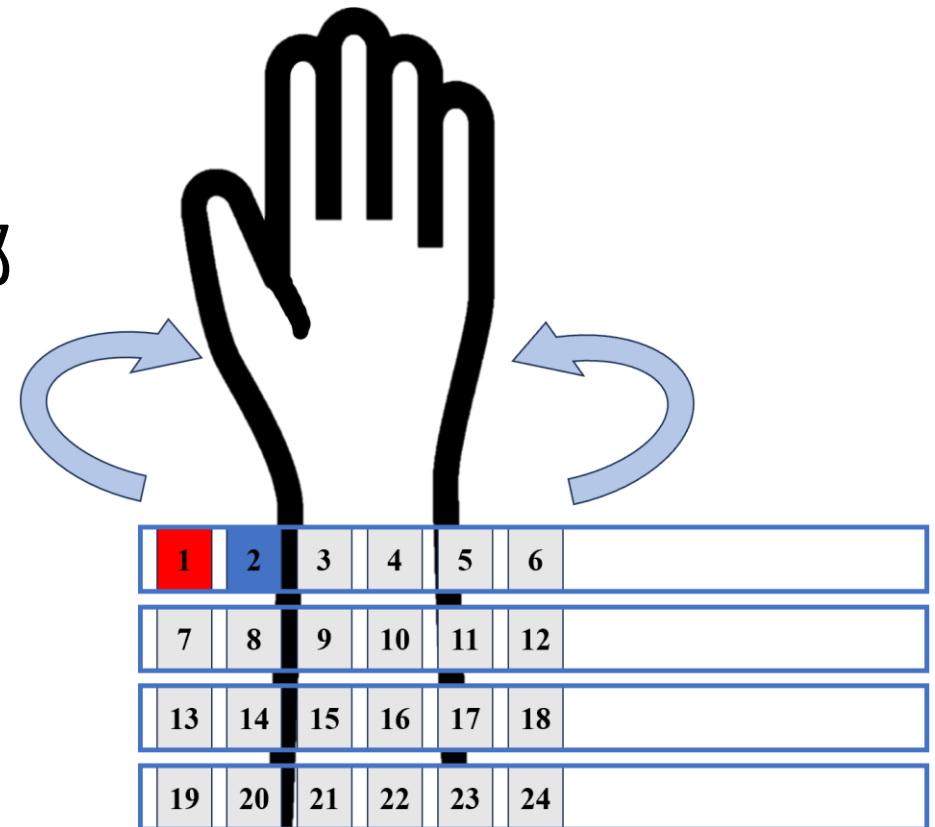
実験諸元

- 静岡大学の研究倫理委員会の審査を経て実施
- 20代の男子大学生5名
- 各指の曲げ伸ばしのみをEMSで制御
 - 肩や上腕, 肘などは動かない
 - 各指は常に同じキーを押下
 - 小指/薬指/中指/人差し指/親指がそれぞれ
キーボードのq/w/e/r/v を押すように手を置く

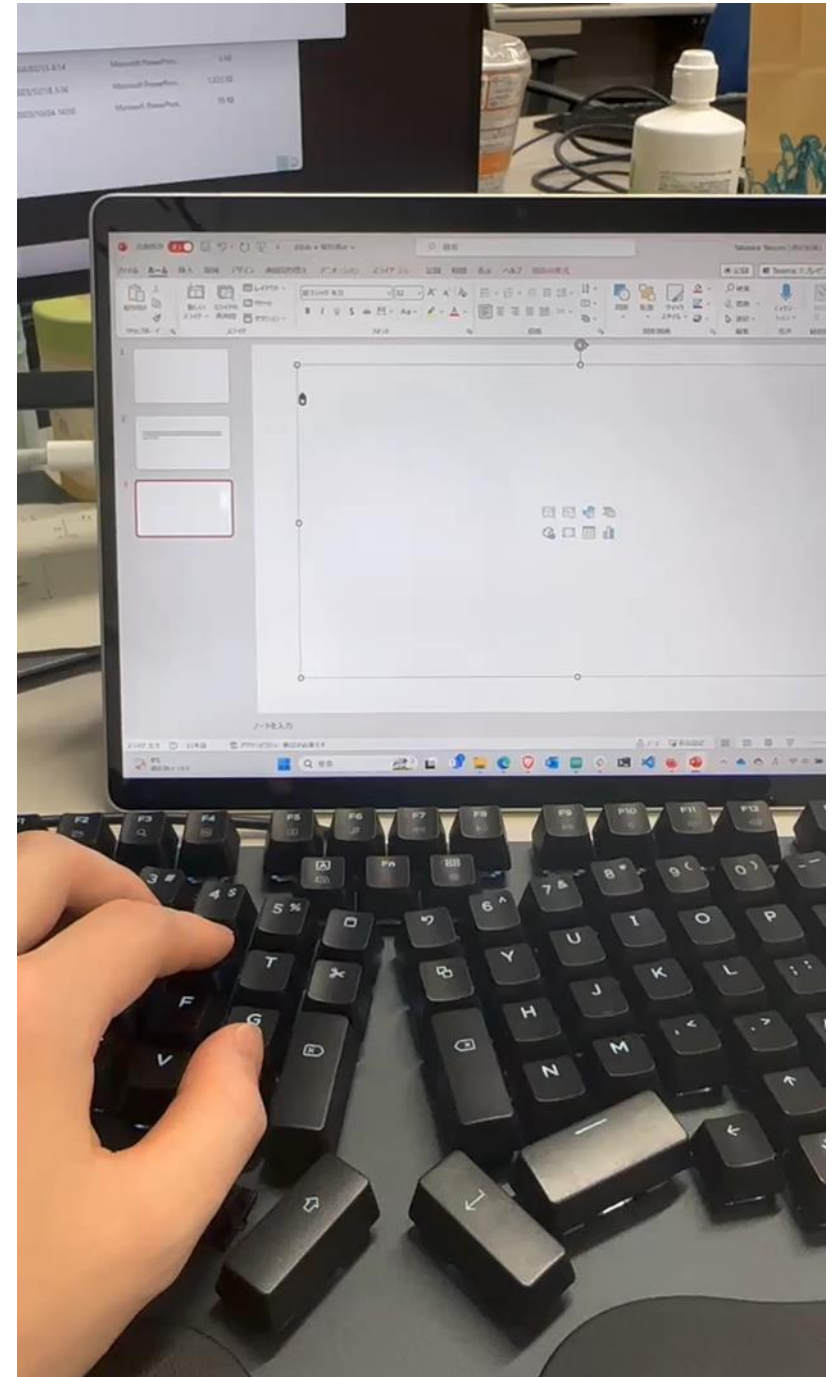


実験諸元

- EMS
 - パルス幅：200 μ sec, 周期：30msecの二相パルス
 - 18V
- マルチパッド電極
 - 計24個の電極を左前腕部に装着
 - 各電極の大きさ
 - 幅：20mm, 長さ：30mm,
 - 間隔：24mm
 - 6個ずつベルトに固定

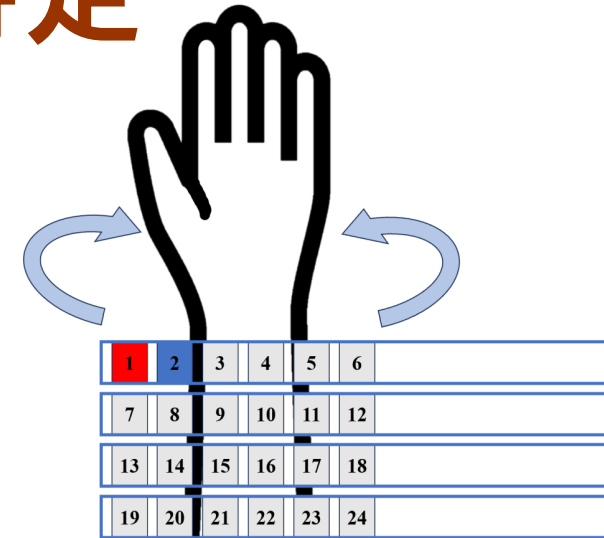


実験風景



実験1: 電極の組の特定

- ユーザの手指を動かすための電気刺激s（電極の組）の特定
- マルチパッド電極を前腕に装着
- それらのうち1つを刺激電極（赤）、もう1つを戻り電極（青）として使用
- 刺激電極と戻り電極の全ての組でEMSを印加し、キーボードを打鍵
- キーボードを打鍵することが出来るほど指が動いた際の電極の組を記録



実験1: 電極の組の特定

user 指	User1-1	User1-2	User2-1	User2-2	User3-1	User3-2	User4-1	User4-2	User5-1	User5-2
小指 (q)	5:19, 5:21 5:22, 11:6	5:6, 5:11 6:12, 11:5 11:18	N/A	N/A	1:11, 2:11 4:11, 6:11 7:11, (+13)	3:11, 4:11 6:17, 7:11 8:11, (+4)	N/A	N/A	6:24, 11:10 14:18, 17:5 19:18	18:3, 18:11 24:12
薬指 (w)	1:17, 1:22 1:24, 2:17 2:23, (+17)	1:17, 1:24 2:23, 3:23 4:17, (+21)	2:17, 2:23 3:23, 4:17 4:23, (+36)	1:18, 1:23 2:17, 2:18 2:23, (+51)	2:16, 5:6 9:7, 11:4 11:8, (+30)	3:16, 5:6 6:16, 11:3 11:4, (+6)	N/A	N/A	1:16, 1:17 2:5, 2:11 5:2, (+20)	1:11, 2:1 7:15, 12:17 23:14, (+2)
中指 (e)	7:17, 8:16 9:16, 11:16 12:18, (+10)	8:16, 10:16 12:6, 14:16 16:6, (+5)	2:6, 2:19 3:6, 4:6 6:10, (+6)	13:6	1:15, 2:15 3:9, 3:15 4:9, (+39)	1:5, 1:9 2:9, 2:15 3:15, (+40)	1:16, 2:16 3:22, 4:16 5:11, (+34)	1:16, 2:15 2:16, 2:22 3:24, (+61)	1:15, 1:22 3:15, 5:8 5:14, (+44)	1:9, 1:14 1:20, 2:9 2:15, (+44)
人指 (r)	6:7 10:24	18:4	N/A	N/A	1:10, 2:5 2:10, 3:10 4:10, (+10)	1:10, 2:5 2:10, 3:10 6:10, (+7)	N/A	N/A	1:4, 2:4 2:10, 2:17 4:1, (+23)	1:3, 3:19 4:1, 4:2 4:3, (+17)
親指 (v)	4:17, 6:10 14:22	2:22	N/A	N/A	N/A	N/A	N/A	N/A	N/A	14:6

実験2：疑似的ユーザ認証

- 実験 1 を各実験協力者ごとに2回実施
- 1回目の実験の後，電極は取り外さず、10分後に2回目の実験を実施
- 実験 1 の2回結果を使用し，疑似的にユーザ実験を実施
 - テンプレート：
実験 1 の1回目の結果を登録情報とみなす
 - クエリ：
実験 1 の2回目の結果を認証情報とみなす

実験2: 疑似的ユーザ認証

中指 (e)	User1_Q	User2_Q	User3_Q	User4_Q	User5_Q
User1_T	4/15	0/15	1/15	4/15	3/15
User2_T	0/11	1/11	1/11	0/11	0/11
User3_T	1/44	0/44	13/44	4/44	9/44
User4_T	2/39	0/39	3/39	24/39	5/39
User5_T	4/49	0/49	12/49	6/49	11/49

- 本人認証率：対角要素の数値
- 他人受入率：非対角要素の数値
- まだ道半ば。。。。

企業への期待

- シーズベースの技術であること、近未来型の技術であること、特殊用途向けの技術であることから、適用先の開拓やビジネスモデルの検討に関する知見を有しておられる企業様との協働を希望します。
- 開発力・実装力をお持ちの企業様と、このアイデアを実用的なレベルに高めていくことを希望します。
- 研究志向の強い企業様と、このアイデアを学問的な観点で更に突き詰めることも歓迎です。

企業への貢献、PRポイント

- 情報セキュリティ技術の近未来像について、一緒に議論させて頂くにあたり、20年以上の経験からの発想をご提供できると思います。
- 特にセキュリティのヒューマンファクタに関しては多くの知見を有志いています。

本技術に関する知的財産権

- 発明の名称 : 情報処理装置、方法、プログラム、及びシステム
- 出願番号 : 特願2024-19326
- 出願人 : 静岡大学
- 発明者 : 西垣正勝、大木哲史、高岩拓海
- 本技術の一部は、JSTムーンショット型研究開発事業JPMJMS2215の支援を受けたものです。

産学連携の経歴

- 共同研究実績多数
 - 日立製作所横浜研究所
 - 三菱電機情報技術総合研究所
 - KDDI研究所
 - NTT社会情報研究所
 - 他

お問い合わせ先

国立大学法人静岡大学
イノベーション社会連携推進機構

T E L 053-478-1710

e-mail sangakucd@adb.shizuoka.ac.jp