Vol.2015-SPT-16 No.15
Vol.2015-EIP-70 No.15
2015/11/20

i/k-Contact:
物理的ソーシャルトラストを利用した適応型 2 段階認証

有村汐里[†1]　藤田真浩[†2]　松野宏昭[†3]　可児潤也[†4]　司波章[†4]　西垣正勝[†2]

概要：サイバーフィジカルや IoT が注目されている中で，人間という高機能かつ汎用的なプロセシングモジュールを ICT モジュールと共生させることが重要な時代となってきた．その一方式として，著者らは，現実世界の「人間による目視」をサイバーワールドにインプットし，ユーザ認証に利用する“i/k-Contact”を提案している．本稿では，i/k-Contact を利用した適応型 2 段階認証システムの提案，実装，評価を行った．現状のセキュリティ対策では，安全性の向上に伴い，OS 起動時のパスワード認証などの基礎対策に加え，何らかの追加対策を併用する場合が大半である．これに対し，本システムでは，被認証者が「不正が発生しにくい状況＝衆人監視の下にある状況」にあることを i/k-Contact により検出する．このような状況下では追加対策の実施を免除することで，2 段階認証の安全性と利便性のバランスを動的に調整することができる．

キーワード：サイバーフィジカルシステム，物理的ソーシャルトラスト，2 段階ユーザ認証

i/k-Contact:
an adaptive two-factor authentication using physical social trust

SHIORI ARIMURA[†1]　MASAHIRO FUJITA[†2]
HIROAKI MATSUNO[†3]　JUNYA KANI[†4]
AKIRA SHIBA[†4]　MASAKATSU NISHIGAKI[†2]

Abstract: While CPS (Cyber Physical Systems) and IoT (Internet of Things) are receiving a lot of attention, it is becoming important that humans which are high-function and high-generic processing modules live associated with ICT (Information and Communication Technology) modules. One of those, we proposed “i/k-Contact” that inputs visual contact by humans to cyber-world and use to user authentication. In this paper, we propose, implement, and assess adaptive two-factor authentication system using i/k-Contact. Under present security measure system, people usually take the additional measure in addition to the basic measure like the password authentication at activate the OS. In contrast, our system detects that an authenticated user is putted in “situations where are forecasted that some dishonest acts don’t occur = situations in public” by i/k-Contact. In that case, by exempting additional measure, it can adjust the two-factor authentication’s safety and convenience balance dynamically.

Keywords: Cyber-physical systems, Physical social trust, 2-factor user authentication

1. はじめに

近年，ビッグデータとコンテキストアウェアネスの注目に伴って，文脈情報のセキュリティ応用[1]に関する研究が再び活発になってきている．場所や時間などの文脈情報をパスワードの代わりに（またはパスワードに追加して）利用する拡張型ユーザ認証[2][3] や，文脈情報から正規ユーザらしさを計算して，その値によって認証方法を変化させるリスクベース認証[4] などがその典型例である．しかし，これらは，個々の被認証者に関する情報のみを利用しているという点で，既存のユーザ認証の枠を超えていない．

そこで本稿では，被認証者と周囲のユーザとの間に成立する「物理的な信頼関係」という文脈を用いて被認証者の認証可否をコントロールする，新たなタイプのコンテキストアウェア認証を提案する．これによって，ユーザ同士の対面コミュニケーションを促進することも可能となる．

本論文の構成は次のとおりである．2 章では関連研究を概説する．3 章で提案方式を説明した上で，4 章で提案方式による 2 段階認証システムについて述べる．5 章で実験環境の構築について，6 章で実験の概要について述べ，7 章で提案システムに対して考察する．8 章はまとめと今後の課題である．なお，本論文は文献[5][6]の内容に，i/k-Contact を利用した 2 段階認証システムに関する考察を付け加えたものである．

†1 静岡大学大学院情報学研究科
Graduate School of Informatics, Shizuoka University.
†2 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University
†3 静岡大学情報学部情報科学科
Faculty of Informatics, Shizuoka University
†4 株式会社富士通研究所
Fujitsu Laboratories Ltd.

Vol.2015-SPT-16 No.15
Vol.2015-EIP-70 No.15
2015/11/20

2. 関連研究

2.1 既存研究

文脈情報のセキュリティ応用に関する研究が行われてきている[1]．コンテキストアウェア認証は文脈情報をユーザ認証に利用する技術であり，文脈情報を利用した拡張型ユーザ認証やリスクベース認証がその代表例として挙げられる．拡張型ユーザ認証は，場所や時間などの文脈情報をパスワードの代わりに（またはパスワードに追加して）利用する[2]．例えば文献[3]では，位置情報を利用した認証が提案されている．

リスクベース認証は，文脈情報から正規ユーザらしさを計算して，その値によって認証方法を変化させる．例えば文献[4]では，通常と異なる利用環境からのアクセスにおいてはユーザに対して追加認証を要求するシステムが実際に運用されている．

2.2 問題点

人間の行動は多岐に渡るため，各種センサから得られた情報から文脈（ユーザの状態や意図など）を正しく推測することは困難である．センサ情報を利用したユーザの行動推定[13]や，ライフログを活用したユーザ認証[7]においても，この点が大きな課題となっている．また，一つの行動を行う場合においても，人間は完全に同じ動作を行うことはない．人間の動作に基づく動的生体認証[8][9]においても，認証精度の確保が課題となっている．

ユーザ（人間）の行動・動作には多分に曖昧性が含まれている．このため，個々の被認証者に関する文脈情報のみをユーザ認証に利用するというアプローチでは，コンテキストアウェア認証システムの正確性の確保に限界がある．そこで本稿では，被認証者に関する情報だけではなく，周りのユーザも巻き込んだ文脈情報を利用するというアプローチによる新たなコンテキストアウェア認証を探る．

3. i/k-Contact

3.1 コンセプト

「人間が人間を目視する」ことによって被認証ユーザと周囲のユーザとの間に成立する「物理的な信頼関係」という文脈情報を用いて，被認証者の認証可否をコントロールする新たなタイプのコンテキストアウェア認証を提案する．

具体的には，互いに面識のある 2 名のユーザが 1 つの部屋に同席したり，廊下ですれ違ったりした際に（本稿では，これらの状態を「隣席」と呼ぶ），各ユーザの携帯デバイスに隣席者情報を表示する．それぞれのユーザは，隣席者を目視で確認し，その隣席者が確かに自分の携帯デバイスに表示された人物であるか否か（OK／NG）をサーバに報告する．

正規ユーザであれば，知人と隣席する度に，隣席者から OK の報告を受ける．すなわち，OK の報告数が多く，かつ，NG の報告が少ないほど，当該携帯デバイスが正規ユーザに所持されている確度が高い．このため，そのようなユーザに対しては，ユーザ本人にパスワードの入力を要求するまでもなく，本人であると認識してしまっても構わないであろう．このように，OK／NG の報告数に応じて認証の要求強度を動的に変更するようなユーザ認証システムを運用することが可能となる．

本稿では，隣席者同士の目視による人物確認の仕組みを「i-Contact」，i-Contact を通じて集約される OK／NG 情報を利用して認証閾値を動的変更するユーザ認証の仕組みを「k-Contact」と名付ける．提案方式では，知人同士の物理的な信頼関係がユーザ認証の礎となっている．このため，ユーザ間の対面コミュニケーション促進効果も期待される．

以降，提案方式の適用場面の具体例として企業等の組織内での利用を想定して議論を進める．各ユーザは携帯デバイスを有し，携帯デバイスのアドレス帳には同僚およびその携帯デバイスに関する情報（端末 ID，ユーザ名，顔写真）が登録されていることを前提とする．

3.2 i-Contact

i-Contact は「人間が人間を目視する」ことによって，被認証者・周囲のユーザ間に成立する「物理的な信頼関係」という文脈情報を用いて，携帯デバイスの不正所持（なりすまし）を検知する仕組みである．

正規ユーザ A の携帯デバイスが，正規ユーザ B の携帯デバイスと隣席した際に，互いの携帯デバイスは，音声や振動などによって自身の所有者にアラートを挙げるとともに，画面に携帯デバイスの端末 ID から特定した隣席者情報を表示する[1]（ユーザ A の携帯デバイスの画面には「ユーザ B と隣席している」という情報が，ユーザ B の携帯デバイスの画面には「ユーザ A と隣席している」という情報が表示される）．ユーザ A および B は，互いに隣席者を目視で確認し，その隣席者が確かに自分の携帯デバイスに表示されたユーザであるかを確認する（図 1）．

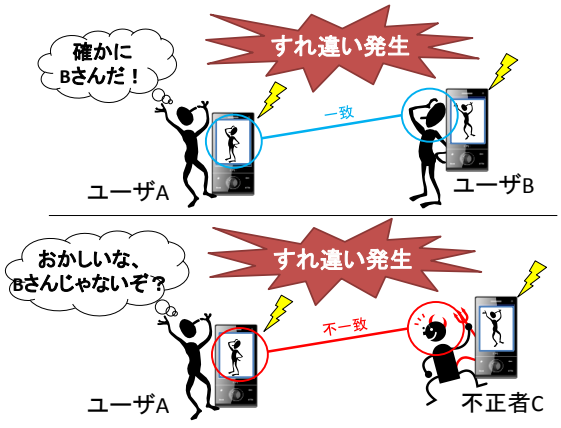

図 1 i-Contact コンセプト図

[1] 互いの携帯デバイスに互いの情報を表示するのではなく，一方のユーザ（ユーザ A）の携帯デバイスにのみ，他方（ユーザ B）の情報を表示するという運用も可能である．本運用は「既に部屋に在室しているユーザが，新しく部屋に入ってきたユーザを目視で確認する」といった場面で有効である．実際，4 章で実装した今回のシステムはこの運用を想定している．

Vol.2015-SPT-16 No.15
Vol.2015-EIP-70 No.15
2015/11/20

例えば，不正者 C がユーザ B の携帯デバイスを盗んで社内に侵入した場合には，ユーザ A の携帯デバイスには「ユーザ B が隣席している」という情報が表示されているにも関わらず，ユーザ A の周囲にユーザ B が居ないという状況となる．これによって，ユーザ A は「ユーザ B の携帯デバイスが不審者に盗まれ，かつ，その不審者が自分の周囲にいる」ことに気付くことができる．現在の技術では，携帯デバイス自身が「自分が正しい所有者に所持されているか」を自律的に判断することは難しい．i-Contact は，携帯デバイスが，周りのユーザの眼を借りて「自分が正しい所有者に所持されているか」を確認してもらう（互いに確認しあう）方式となっている[2].

3.3 k-Contact

k-Contact は，前節で述べた i-Contact を利用し，ユーザが携帯デバイスや社内リソースにログインする際の認証の要求強度を動的変更する仕組みである．この実現のために，i-Contact においてユーザに求められる「目視による互いの確認」の結果を，OK／NG の形で集約する．各ユーザの携帯デバイスには「OK ボタン」と「NG ボタン」が表示され，ユーザがそのボタンを押すことで，OK／NG の情報が社内サーバに送られる[3]．社内サーバには，全ての携帯デバイスからの OK／NG の報告回数が格納される．正規ユーザであれば，組織内で他ユーザと隣席する度に，隣席者から OK 報告を受ける．すなわち，OK の報告が多く，かつ，NG の報告の少ないユーザほど，正規ユーザが正しく携帯デバイスを所持している確度が高い．そのようなユーザに対しては，個別のユーザ認証を行うことなく携帯デバイス内のリソースや社内サーバ内のリソースへのアクセスを許可してしまっても構わないであろう．このように，OK／NG の報告数に応じて認証の要求強度を動的に変更するユーザ認証システムが k-Contact である．

k-Contact は，いわば，「衆人環視型」のユーザ認証システムである．利用例としては，出社の際に自分のデスクにつく間に多くの同僚とすれ違うことで業務用 PC に対するユーザ認証が不要になる場合や複数のユーザが同席しての会議の際にユーザ認証なしで会議資料へのアクセスを許す場合が考えられる．さらに，当人以外のユーザによる目視を利用した認証であるため，不正行為に対する抑止効果[15][16]も期待される．

[2] 関連研究として文献[14]があるが，文献[14]はユーザどうしの物理的信頼関係を用いて，相手が正規ユーザであることを確認している．これに対し提案方式は，ユーザどうしの物理的信頼関係を用いて，正規ユーザが正規端末（登録済の端末）を所持していることを確認していることに注意されたい．

[3] 隣席者に関する OK／NG の報告については，目視にて相手が確認できた場合のみ OK ボタンを押し，所定時間内にボタンが押されなければ自動的に NG と判定する方法と，目視にて相手が確認できなかった場合のみ NG ボタンを押し，所定時間内にボタンが押されなければ自動的に OK と判定する方法が考えられる．セキュリティを第一に考えた場合は，確実に OK である場合のみを信頼する前者の方法が適切であろう．一方で，一つの場所に比較的多数の社員が集まる場合には，すべての隣席者に対する OK を返答するという手間のない後者の方法のほうが便利であると思われる．

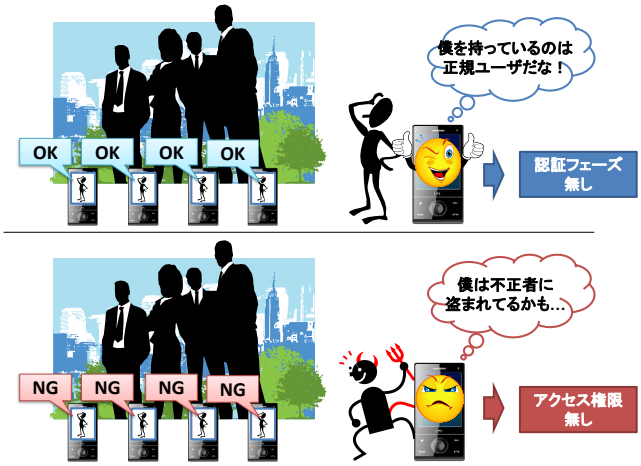

図 2 （上）信用度の高いユーザと（下）信用度の低いユーザの認証要求強度の変化の例

4. i/k-Contact における 2 段階認証システム

近年の情報セキュリティ事故の頻発を受け，組織の情報セキュリティ対策はユーザの利便性を犠牲にする形で強化を余儀なくされる傾向にある．そして，組織の情報セキュリティ対策の強化は，往々にして，現時点までの情報セキュリティ対策（以下，基本対策）を残しながら，更にもう一段階の情報セキュリティ対策（以下，追加対策）が追加されるという形で実施されることが一般的である．本稿では，現時点までの基本対策のみの認証システムを「1 段階認証システム」，基本対策と追加対策が併用された後の認証システムを「2 段階認証システム」と呼び分けることにする．

2 段階認証システムにおける追加対策は，基礎対策のみでは防ぐことのできない「万が一の事故」への備えである．これを逆に考えれば，「万が一の事故」が起きないことが保障されている状況であれば，基礎対策だけでも十分だといえよう．人間は，周囲に人の眼がある環境においては，不正行為に対する抑止効果が顕著に現れることが知られている[15][16]．そこで本稿では，i/k-Contact を利用して「ユーザが衆人監視の眼がある状況に置かれている」ことを検出し，2 段階認証システムにおける追加対策の適用の要否を動的に制御する方式を提案する．

ユーザが衆人監視環境下におかれていない場合は，「万が一の事故」が発生し得る状況であると判断し，当該ユーザには基礎対策と追加対策の両方が課される．これによって，1 段階認証システムよりも高い安全性が達成される．追加対策が適用されることによって，ユーザの利便性は低下することになるが，組織が追加対策を導入するという判断を下すにあたっては相応の理由が存在しており，利便性よりも安全性が優先されることとなる．

ユーザが衆人監視環境下におかれていれば，「万が一の事故」が発生し得ない状況であると判断し，当該ユーザには追加対策の適用を免除する．この場合，ユーザに課されるのは

基礎対策のみとなり，1 段階認証システムと同等の利便性が維持される．安全性の強化に対する組織の要求（組織が 2 段階認証システムを採用するに至った理由）を認識しつつ，ユーザの利便性に配慮した運用が達成される．

5. 実験環境の構築

提案方式の安全性と利便性（ユーザにどの程度の負荷となり得るか，「見逃し」はどの程度発生するのか，k-contact によって要求強度が下がることをユーザはどの程度有用と思うか，等）を調査するため，著者らの所属する研究室にて実験環境を整えた．今後，実際に評価実験を実施していく．

5.1 実験環境

「互いに面識のあるユーザが一つの部屋に同席する」シーンを対象にして，i/k-Contact の実装を行う．筆者らの研究室の間取りは図 3 のとおりである．扉 A はユーザの入室時以外は閉じられている．

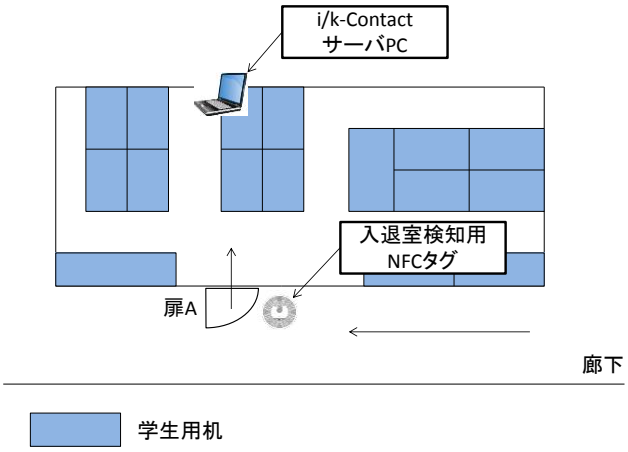

図 3 間取り図

5.2 機器

本システムは 4 章における利用シーンを想定し，すべてのユーザ（学生）の所持する NFC リーダ機能を有した Android 端末，ユーザ同士のすれ違いや各ユーザの信用度を管理する i/k-Contact サーバ，部屋への入退室検知用 NFC タグ，またユーザの信用度の変化に応じて認証の要求強度を変化させる Google Chrome のアドオンによって設計されている．

全機器は同一のネットワーク（研究室 LAN）に接続されている．ただし，携帯デバイスは無線ルータを介して研究室 LAN と接続される（無線ルータの通信可能範囲に入った場合，自動的に接続される）．

5.2.1 ユーザの入退室

部屋の入退室の検知は扉 A に設置された入退室検知用の NFC タグに NFC リーダ機能を有した携帯デバイスをかざすことにより行う．扉 A からユーザ X が入室した際に，その時点で室内に在席しているユーザの携帯デバイスにアラート（振動）を通知するとともに，画面上にユーザ X の顔写真と NG ボタンを表示する（図 4）．在席するユーザは，入室したユーザを目視で確認し，確かにユーザ X（正規ユーザ）であれば何もせず（OK=NoReply とする），そうでなければ，NG ボタンを押す[4]．退室時も入室時と同様に，入退室検知用の NFC タグに再度携帯デバイスをかざすことで検知する．

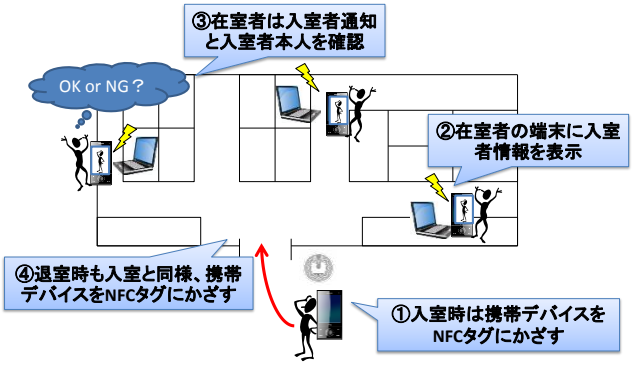

図 4 ユーザの入退室

図 5 入室者情報

5.2.2 認証フェーズ

ユーザは研究室内で自身の PC を利用する際，基本対策である OS 起動時のパスワード認証に加え，セキュリティ強化のためブラウザの起動時とブラウザ使用中の一定の時間毎に追加対策としてパスワード認証が要求される．ブラウザの使用は多段階認証によって守られてるが，一定数以上のユーザから OK を受けたユーザは，基本対策のみの実施でブラウザの利用を許可される．

今回の実験では「衆人環視の下にある状況＝1 人以上のユーザと同席している状況」とし，同席者がいる且つ，NG 報告を受けていないユーザは追加対策が免除されるよう実装されている．同席者がいない，もしくは NG 報告を一度でもされている場合には追加対策であるパスワード認証が要求され，認証が成功すると一定時間はブラウザを通常利用できる．一定時間が経過（タイムアウト）すると，再度

[4] 今回の実験システムでは，ユーザビリティに考慮し，在室者が目視にて入室者の本人性を確認できなかった場合のみ NG ボタンを押す方法を採用した．入室者の入室後 5 秒以内に NG ボタンが押されなければ，在室者からの OK が自動的に i/k-Contact サーバへ送信される．

信用度の問い合わせが行われ，その値によって認証を再度要求するか否かが決定される．

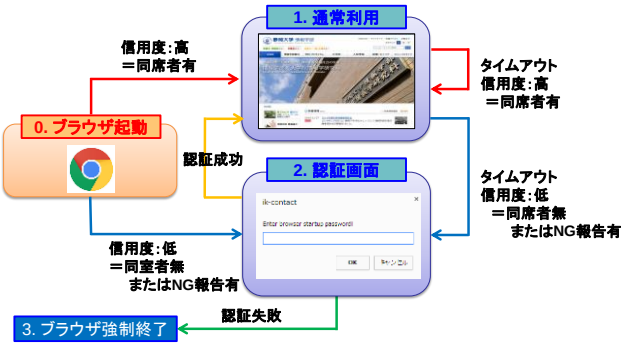

図 6 ブラウザの画面遷移図

5.2.3 不正者実験

また，実験期間中は「OK=NoReply」の妥当性の検証の為，被験者の所持する端末のすり替えを行い，正しく NG が押されるかどうかを調査する．端末のすり替えは内部犯を想定し，不正者が他の被験者の端末を盗んだ（端末を不正に 2 台所持している）場面，不正者が他の被験者になりすました（他の被験者の端末を不正に所持している）場面に加え，外部犯を想定した被験者以外の学生が被験者の端末を不正に所持している場面でのすり替えを実施する．

5.3 制約

5.1 節の環境下で i/k-Contact が適切に機能するにあたっては，下記の制約条件を満たす必要がある．

(i) 入室者に対する在室者の目視による確認は必ず行われる（在室者が入室者を見逃すことはない）

(ii) ユーザの入室時は，既に在室しているユーザに「今，誰が入室したか」が明確である状況になっている

(ア) 入り口付近に在室者の目視を妨げる障害物が存在しない

(イ) 2 人以上のユーザの同時入室が発生しない

制約条件(i)は，各ユーザに平素からの目視による確認を促すための条件であり，これを満たす為，今回は「誰かが入室した際には一度目を向けること」といった社内ルールを設けることを前提とする．また，制約条件(i)の在室者が入室者を見逃す可能性があるという問題に対し，ブラウザアドオンにはユーザの入室と同時に入室者情報（入室者の顔写真と名前）を表示する入室者ポップアップ機能を搭載した（図 7）．これにより，在室者の耳が塞がってしまっている場合や，端末への入室者通知に気が付けなかった場合にも，PC の画面上に表示されるポップアップを見ることによって入室者の存在に気が付くことができる．

図 7 入室者ポップアップ

制約条件(ii)-アについては，在室者の目視を妨げないよう，扉付近の障害物（ホワイトボード等）を排除することで在室者の視界を確保する．(ii)-イの同時入室の発生の防止は，入室者通知が同時に端末の画面上に表示されることによる入室者の混同を防ぐためである．例えば，ユーザ A がユーザ B の端末を盗んでいたとしても，ユーザ A とユーザ B が同時に入室した場合，在室者には「ユーザ A とユーザ B が入室した」という情報だけが与えられるため，端末の盗難に気づくことができないという問題がある．本システムは入退室を NFC タグで検知しており，2 人以上が同時に NFC タグに携帯端末をかざすという状況はありえないため，同時入室が発生することのない環境を実現している．

6. 実験

6.1 実験目的

本実験は，3 章で述べた実験システムを使用し，同等の安全性が保たれた状況での平素の基礎対策＋追加対策と比較して，i/k-Contact の利便性が高いことを証明することを目的としている．また，i/k-Contact の実運用において，3.2 節で述べた前提条件を満たすことが出来ているか，前提条件によってユーザにどれほどの負荷がかかるのかを調査する．

6.2 実験方法

筆者らが所属する研究室の学生 7 人に 8 日間本システムを使用してもらい，期間中のヒアリングに加えて実験終了後にアンケートへの回答を依頼する．また，実験期間中は「OK=NoReply」の妥当性の検証の為，一日二回程度被験者の所持する端末のすり替えを行い，正しく NG が押されるかどうかを調査する．

6.3 評価方法

今回の実験の評価は，実験期間中のログの解析と，被験者への実験期間中のヒアリング，実験終了後のアンケート調査によって行う．ログ解析により「ユーザ端末すり替え時に正しく NG が押されたかどうか」を調査し，不正者実験時の被験者へのヒアリングと合わせて提案手法の安全性の評価指標とする．被験者へのアンケート調査では，3.2 節で述べた前提条件を満たすことが出来ているか，前提条件によってユーザにどれほどの負荷がかかるのかを調査し，本システムの利便性を評価する．

7. 考察

7.1 安全性に関する考察

提案方式に関する脅威としては，信頼度がたまった端末の盗難や複数ユーザによる結託が考えられる．信頼度がたまった端末の盗難に関しては，基本的に，周囲のユーザの目視によって端末の盗難を検知することで対策可能である．しかし，端末が盗難した不正ユーザが，他ユーザと一度もすれ違わない状況も考えられるだろう．この状況も想定したうえで，信頼度のたまった端末の信頼度をどの程度継続するかについては今後検討していかなければならない．また，複数ユーザによる結託については，閾値 k の値を十分に高めることでリスクを軽減可能である．しかし本対策は，利便性を下げてしまうことに直結するため，今後，安全性と利便性のバランスを考慮した閾値の適切な決定方法についても検討することが必要であろう．

7.2 隣席者情報の表示

i/k-Contact は，現時点の実装では，組織員のスマートフォンの画面に隣席者情報が表示される形態となっている．しかし近年では，ヘッドマウント型の携帯デバイスも普及している（たとえば，[10]，[11]）．このような携帯デバイスを使用することで，ユーザに音声で「前方から組織員 A が歩いてきています」と伝えたり，拡張現実（AR）技術によって現実に隣席している組織員の頭上に隣席者情報を表示したりすることも可能となってくるであろう．

7.3 適用範囲

i/k-Contact は「人が人をチェックする」というコンセプトに基づく認証方式であるため，お互いの顔を知らない者どうしの間では本方式を運用することができない．本稿では組織内での利用を前提として議論を行ったが，大企業の場合は，お互いに面識のない組織員も組織内に多数存在する．部署ごとに i/k-Contact を運用するなどの方法が必要となる．

また，人混みの中では，同僚が数 m 以内に居るという情報を知ったとしても，その同僚を見付けることができない場合があるだろう．今後，i/k-Contact の運用が可能となる要件を調査したうえで，提案方式の適用シーンについて精査していく必要がある．

7.4 対面コミュニケーション

PC やインターネットの普及に伴い，ユーザ同士が顔を合わさずとも相手と対話ができるメールやチャットなどを利用したコミュニケーションが浸透してきている．この結果，空間を越えたコミュニケーションが可能となったが，人間関係の希薄化や対面的コミュニケーション能力の低下という弊害が社会問題になっている[12]
i/k-Contact では，知人同士の隣席が発生した際に，相手の存在を通知し，相手の顔を見て確認をとることを求めている．これが，挨拶や会話のきっかけとなり，対面コミュニケーションの機会向上や，新しい対面コミュニケーション形態の実現へとつながる可能性が十分にある．

8. まとめと今後の課題

本稿では，被認証者と周囲のユーザとの間に成立する「物理的な信頼関係」という文脈を用いて被認証者の認証可否をコントロールするコンテキストアウェア認証システム i/k-Contact を提案した．隣席者同士が目視によって携帯デバイス所有者を確認する仕組みが i-Contact であり，i-Contact を通じて集約される情報を利用して認証閾値を動的に変更するユーザ認証の仕組みが k-Contact である．

本稿では，i/k-Contact の詳細を示した上で，i/k-Contact の実運用に向けた適応型 2 要素認証システムを実装し，実験環境を整えた．今後は，実装した実験環境を用いた提案方式の可用性，利便性，安全性を評価する予定である．また，提案方式は，物理的な信頼関係を利用した認証方式を実現しているため，ユーザ同士の対面的なコミュニケーションを促進する効果を期待している．

参考文献

1) What is context-aware security (2015/08/23 確認)
http://searchsecurity.techtarget.com/definition/context-aware-security
2) 横山重俊，上岡英史，山田茂樹：ユビキタスサービスに適したコンテキストアウェアアクセス制御方式の提案. 電子情報通信学会技術研究報告, Vol. 105, No. 565, MoMuC2005-74, pp. 7-12, 2006.
3) F. Zhang, A. Kondoro and S. Muftic. Location-based Authentication and Authorization Using Smart Phone. *Proc. of TrustCom2012*, pp. 1285-1292, 2012.
4) Risk-Based Authentication (2015/08/23 確認)
https://www.schneier.com/blog/archives/2013/11/risk-based_auth.html
5) 有村汐里，小林真也，可児潤也，司波章，西垣正勝：i/k-Contact: 物理的ソーシャルトラストに基づくコンテキストアウェア認証. CSS2013, pp. 224-231, 2013.
6) S. Arimura, M. Fujita, S. Kobayashi, J. Kani, A. Shiba, M. Nishigaki: i/k-Contact: a context-aware user authentication using physical social trust. *Proc. of PST2014*, pp. 407-413, 2014.
7) 石原雄貴，小池英樹：ライフログを利用した認証システム. DICOMO2007 論文集, pp. 264-268, 2007.
8) 杉浦一成，梶原 靖，八木康史：全方位カメラを 用いた複数方向の観測による歩容認証，情報処理学会論文誌. Vol. 1, No. 2, pp.76-85, 2008.
9) 石原進，行方エリキ，太田雅敏，水野忠則：端末自体の動きを用いた携帯端末向け個人認証, 情報処理学会論文誌. Vol. 46, No. 12, pp. 2997-3006, 2005.
10) Telepathy (2015/08/23 確認)
http://telepathywear.com/product/
11) HMZ-T3Z (2015/08/23 確認)
http://www.sony.jp/hmd/products/HMZ-T3/
12) SOCIAL MEDIA: THE DECLINE OF FACE-TO-FACE COMMUNICATION (2015/08/23 確認)
http://www.brandandmortar.com/social-media/social-media-killer-face-face-communication/
13) 千葉雄樹，宮崎陽司，中尾敏康：センサ装着位置の差異に頑

健な移動行動の推定，情報処理学会研究報告. Vol. 2011-UBI-29, No. 30, pp. 1-7, 2011.
14) 中村嘉志，濱崎雅弘，石田啓介，松尾豊，西村拓一：個人端末を Web 支援システム ID へリンクする一手法の提案．日本知能情報ファジィ学会, Vol.20, No. 4, pp. 566-577, 2008.
15) M. Gil and S. Angela. Assessing the impact of CCTV. London: Home Office Research, Development and Statistics Directorate, 2005.
16) コトヴェール:統合警備システム, 複数人照合機能(2015/10/15 確認)
http://www.coteau-vert.co.jp/products/TISS/index.html