情報処理学会論文誌 Vol.57 No.12 2654–2663 (Dec. 2016)

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,a)]

受付日 2016年3月10日, 採録日 2016年9月6日

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，本論文では，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” を提案する．隣席者同士が目視によって携帯デバイスの所有者を確認する仕組みが “i-Contact”，i-Contact を通じて集約される情報を利用して認証強度を動的に変更するユーザ認証の仕組みが “k-Contact” である．さらに，i/k-Contact の具体的な適用先として，適応型 2 段階認証システムの実装および評価を行う．被認証者が「不正が発生しにくい状況 = 衆人環視の下にある状況」にあることを i/k-Contact により検出し，そのような状況下では 2 段階目の認証を免除することで，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：コンテキストアウェアユーザ認証，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,a)]

Received: March 10, 2016, Accepted: September 6, 2016

Abstract: While CPS (Cyber Physical Systems) and IoT (Internet of Things) are receiving a lot of attention, it is becoming important that humans, who can be defined as “high-function and high-generic processing modules”, interact with ICT (Information and Communication Technology) modules to empower the smart environment. In this paper, we propose one such application “i/k-Contact” that inputs visual contact by humans to cyber-world and to function as user authentication. i-Contact is the mechanism that visually confirms a user (owner of a mobile device) by the eyes of humans nearby in environment. k-Contact is the mechanism that dynamically changes the authentication level of each user using the context information collected through i-Contact. In addition, we implement and evaluate an adaptive two-factor authentication system using i/k-Contact as a concrete application. Our system detects that an authenticated user is entering a “situations in public” (i.e., situations where it is apparent that some dishonest acts may not occur) by i/k-Contact. In that case, by exempting the second factor of authentication, our system can adjust dynamically the balance of safety and usability for two-factor authentication.

Keywords: context-aware user authentication, 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ともなって，文脈情報のセキュリティ応用 [1] に関する

[1] 静岡大学大学院情報学研究科
Graduate School of Informatics, Shizuoka University, Hamamatsu, Shizuoka 432–8011, Japan
[2] 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University, Hamamatsu, Shizuoka 432–8011, Japan
[3] 静岡大学情報学部情報科学科
Faculty of Informatics, Shizuoka University, Hamamatsu, Shizuoka 432–8011, Japan
[4] 株式会社富士通研究所
Fujitsu Laboratories Ltd, Kawasaki, Kanagawa 211–8588, Japan
[a)] nisigaki@inf.shizuoka.ac.jp

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，個々の被認証者自身から提供され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．

そこで本論文では，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 “i/k-Contact” を提案する．i/k-Contact は，周囲のユーザの助けを借りて被認証者の正当性を検証する認証方式といえる．これによって，ユーザ同士の対面コミュニケーションが促進されるという副次的効果も期待される．さらに，i/k-Contact の具体的な適用先として，適応型 2 段階認証システムの実装および評価を行う．現状のセキュリティ対策では，安全性に対する要求の向上にともない，OS 起動時のパスワード認証などの基本対策に加え，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 = 衆人環視の下にある状況」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．

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うえで，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 章および 6 章では，4 章の 2 段階認証システムを用いての評価実験とその実験結果を示す．7 章で提案方式に対して考察し，8 章でまとめと今後の課題を述べる．

2. 関連研究

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あげられる．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]．たとえば文献 [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．たとえば文献 [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．

しかし，人間の行動は多岐にわたるため，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基本的には困難である．センサ情報を利用したユーザの行動推定 [5] や，ライフログを活用したユーザ認証 [6] においても，この点が大きな課題となっている．また，1 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 [7], [8] においても，認証精度の確保が課題となっている．

このように，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，個々の被認証者自身から提供される文脈情報のみをユーザ認証に利用するという文献 [1], [2], [3], [4] のアプローチでは，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．そこで本論文では，被認証者からの文脈情報だけではなく，周りのユーザから提供される「被認証者に関する情報」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について探る．

周りのユーザから提供される「被認証者に関する情報」を利用する関連研究としては，文献 [9] がある．文献 [9] は，ユーザ同士の物理的信頼関係を用いて，正規ユーザと正規携帯デバイス（未登録のデバイス）を紐づける方法を提案している．ユーザ認証は，通常，登録フェーズと認証フェーズから構成されるが，文献 [9] は，登録フェーズにおける「ユーザ同士の物理的信頼関係」の利用を目的としたものであることに注意されたい．これに対し，本論文は，認証フェーズにおける「ユーザ同士の物理的信頼関係」の利用を目的としており，周りのユーザから提供される「被認証者に関する情報」を利用して「正規ユーザが正規携帯デバイス（登録済のデバイス）を所持している」ことを確認する方式を提案するものである．

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（本論文では，これらの状態を「隣席」と呼ぶ）に，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本来の所有者（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，正規ユーザであると認識

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（信用度）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．

本論文では，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が促進されるという副次的効果も期待される．

以降，提案方式の適用場面の具体例として企業など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，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あげるとともに，携帯デバイスの端末 ID から特定した隣席者情報を画面に表示する（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）[*1]．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）．

たとえば，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かかわらず，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，携帯デバイスの使用者に能動的なユーザ認証を要求することなく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．

[*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，一方のユーザの携帯デバイスにのみ，他方の情報を表示する（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」という情報が表示されるが，ユーザ B の携帯デバイスの画面には何も表示されない）という運用も可能である．このような運用は「すでに部屋に在室しているユーザ A が，新しく部屋に入ってきたユーザ B 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．

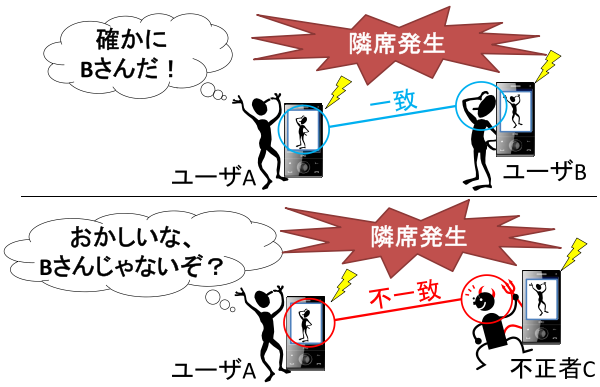


図 1 i-Contact コンセプト図
Fig. 1 Concept of i-Contact.

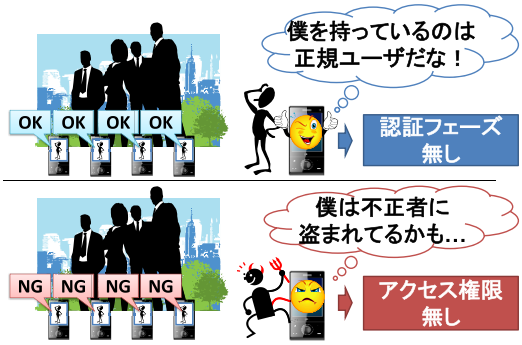


図 2 k-Contact コンセプト図
Fig. 2 Concept of k-Contact.

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（図 2）．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．社内サーバには，すべての携帯デバイスからの OK/NG の報告回数が「信用度」として格納される．

正規ユーザであれば，組織内で他ユーザと隣席するたびに，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わせることなく（ユーザに能動的なユーザ認証を要求することなく）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（信用度）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．単に「携帯デバイスが，他の複数の正規ユーザの携帯デバイスの集団の中に存在しているか否か」を基準とする認証方式と比較して，提案方式は「携帯デバイスが正規ユーザに所持されているかどうかを，隣席者の目視によって判断できる」という点で優れているといえる．さらに，「他人の目」を利用した認証であるため，不正行為に対する抑止効果 [10], [11] も期待される．

k-Contact の利用例としては，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．また，その際，利用シーンに応じて，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（「No Reply=NG」の運用）や，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（「No Reply=OK」の運用）をとることができる．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，1 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 をいちいち返答することは手間になるため，利便性に鑑み後者の方法を選択するという判断がなされることもあるだろう．

4. i/k-Contact を利用した 2 段階認証システム

4.1 適応型 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の強化を余儀なくされる傾向にある．ここで，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，さら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．本論文では，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，基本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，基本対策だけでも十分だといえよう．人間は，周囲に人の目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 [10], [11]．そこで本論文では，i/k-Contact を利用して「ユーザが衆人環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．

ユーザが衆人環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，当該ユーザには基本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．

ユーザが衆人環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本対策のみとなり，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．

なお，3.3 節にて「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 と判定する方法をとることができる」と述べたが，「No Reply=OK」の運用は，ユーザが隣席者を見逃してしまった際に不正者の侵入を許してしまうというリスクをはらむ．その点，2 段階認証システムにおいては，基本対策の実施によって不正者の侵入のリスクを低く保ちつつ，追加対策に対しては i/k-Contact を適用することによって利便性の向上を図るという運用が可能である．

4.2 ケーススタディ

適応型 2 段階認証システムの典型的なケーススタディとして，10 名程度の社員（ユーザ）が 1 つの部屋で仕事をするという環境を想定し，

- 基本対策（第 1 段階の認証）：
  ユーザが PC を利用する際に OS 起動時のパスワード認証が要求される．
- 追加対策（第 2 段階の認証）：
  ユーザがブラウザを利用する際に，ブラウザ起動時およびブラウザ使用中の一定の時間ごとにパスワード認証が要求される．i/k-Contact の適用により，一定数以上のユーザから OK を受けたユーザは，追加対策の実施が免除される（**図 3**）．

によって構成される適応型 2 段階認証システムを実装する．

4.2.1 適用シーン

筆者らの研究室に在籍する学生に社員の役を演じてもらうことによって，筆者らの研究室に「互いに面識のある社員（ユーザ）が 1 つの部屋に同席する」シーンを再現し，

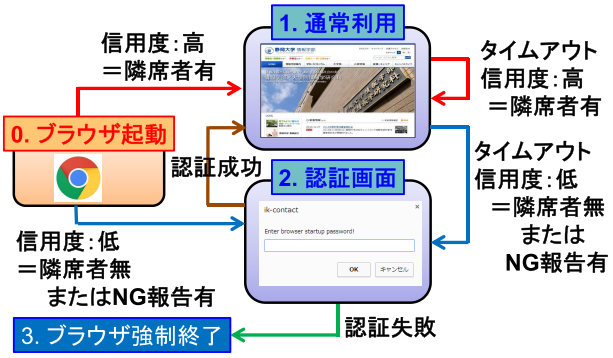


図 3 ブラウザの画面遷移図
Fig. 3 Screen transition diagram of browser.

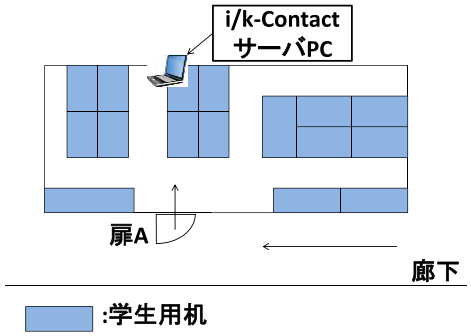


図 4 間取り図
Fig. 4 Floor plan.

i/k-Contact を利用した適応型 2 段階認証システムを運用する．

研究室の間取りは図 4 のとおりである．扉 A はユーザの入退室時以外は閉じられている．研究室の学生同士はお互いの顔と名前を認識している．研究室の広さは 4.6×11.2 m であり，室内のユーザはお互いに目視での本人確認が可能である．在室者（隣席者）が不審者の入室に十分気付き得る広さであるため，今回は，1 人以上の隣席者から OK を受けたユーザについては追加対策の実施を免除するというルールとした．

各ユーザは研究室内で自身の席が決まっている．席上には各ユーザのデスクトップ PC が設置されており，各ユーザは在席中，自身のデスクトップ PC を使ってインターネットをブラウジングする．また，ユーザは i/k-Contact を実施するための携帯デバイスを各自所持している．隣席者およびその信頼度を管理するための i/k-Contact サーバが 1 台設置されている．隣席者からの OK/NG の報告は i/k-Contact サーバに集約される．各ユーザのデスクトップ PC は，利用者の信頼度を i/k-Contact サーバに問合せ，その値に応じてユーザに追加対策を要求するか免除するかを決定する．

以下，4.2.2 項および 4.2.3 項で，本実験システムにおける被認証者の入退室と隣席者の見逃し防止に関する条件設定について説明する．

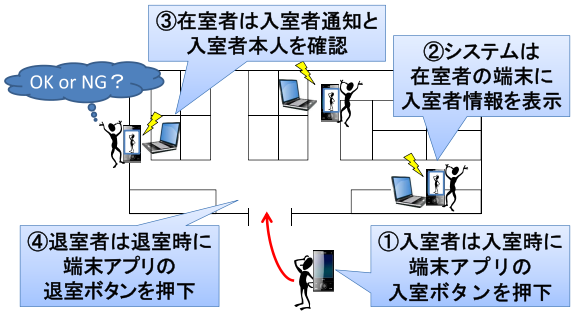


図 5 ユーザの入退室
Fig. 5 Entry and exit of users.

図 6 入室者情報の表示
Fig. 6 Information of entry.

4.2.2 ユーザの入退室

ユーザの携帯デバイスどうしが互いの接近を感知し，隣席のアラートを表示するようなシステムが実現できることが理想であるが，携帯デバイスの位置推定の精度が不十分であったため，今回は，携帯デバイスに入室通知機能，退室機能を持つ Android アプリを実装することによって代用した．ユーザには，入退室の際に図 4 中の扉 A を開ける前に，アプリの入室ボタン/退室ボタンをタップするよう指示した．これによって，ユーザの入退室が i/k-Contact サーバに通知される．

ユーザの入退室の流れを図 5 に示す．扉 A からユーザ X が入室すると，i/k-Contact サーバからその時点で室内に在席しているユーザ（隣席者）の携帯デバイスに通知が発せられる．これによって，隣席者の携帯デバイスにアラート（振動）とともに，画面上にユーザ X の顔写真と NG ボタンが表示される（図 6）．隣席者は，入室者を目視で確認

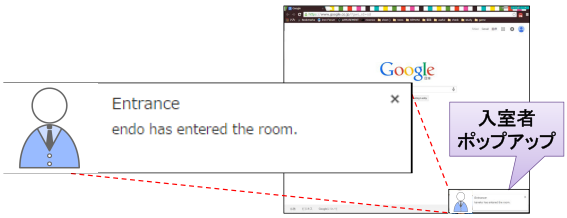


図 7 入室者情報のポップアップ
Fig. 7 Pop-up of entry information.

し，確かにユーザ X（正規ユーザ）であれば何もせず，そうでなければ NG ボタンをタップする．

入室後 15 秒[*2]以内に NG ボタンが押されなければ，携帯デバイスは自動的に OK 報告を i/k-Contact サーバに送信する（No Reply=OK の運用）ように設定した．1 人以上の隣席者から OK 報告を受けたユーザに対しては，当該ユーザ本人が退室する，または，当該ユーザ以外の隣席者が全員退室するまで追加対策の実施が免除される．隣席者が NG ボタンをタップした場合は，その時点で NG 報告が i/k-Contact サーバに送信される．1 人以上の隣席者から NG 報告を受けたユーザに対しては，追加対策の実施は免除されない．今回の実験システムでは，NG 報告を受けたユーザ本人が退室した時点で，過去の NG 報告はリセットされる設定とした．

4.2.3 見逃しの発生の防止

今回のケーススタディでは，基本対策によるユーザ認証が必ず実施されるため，追加対策における i/k-Contact の見逃しのリスクがある程度補償される形になってはいるものの，入室者に対する在席者（隣席者）の目視による確認が確実に行われる（在席者が入室者を見逃すことはない）ような状況を構築しておくことは重要である．このため，今回は，以下の条件を設定した．

まず，入室者に対しては「入室にあたっては，1 人ずつ 5 秒程度の間隔をあけて扉 A を通過すること」といった社内ルールが設けられているという前提をおくこととした．これによって，複数のユーザが同時に入室する（誰がどの携帯デバイスを所持して入室してきたのかが分からない）という状況が発生することを防止している．実験に際しては，扉 A をつねに施錠する状態にしておき，入退室する際には必ず 1 人ずつ開錠してから入室するようにユーザに指示した．

次に，在席者に対しては「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が設けられているという前提をおくこととした．また，ユーザの入室の際には，在席者の携帯デバイスへの表示に加え，在席者の PC のブラウザの画面にも入室者情報（入室者の顔写真と名前）を表示するポップアップ機能を搭載した（**図 7**）．さらに，著者らの研究室内には実際には衝立が設置されていたが，図 5 の環境を構築するにあたっては衝立を取り外し，在室者はどの席からも扉付近の入室者を目視できるようにした．

[*2] 15 秒という時間は，予備実験を通じて経験的に定めた．

5. 実験

4.2 節の環境を使って，i/k-Contact を用いた 2 段階認証システムの利便性と安全性を評価する．

5.1 機器

ユーザの携帯デバイスは，Android スマートフォン（富士通 ARROWS NX F-01F）を利用した．被験者となるすべてのユーザ（学生）に実験期間中，1 台ずつ貸与した．i/k-Contact サーバは，CPU：Intel(R) Core(TM) i5，メモリ：4 GB，OS：Windows7 の PC によって実装した．携帯デバイスにおける i/k-Contact の機能（図 6）は，Android アプリの形で実装した．ブラウザにおける追加対策（図 3）と入室者情報ポップアップ（図 7）の機能は，Google Chrome のアドオンによって実装した．実験実施前に被験者に「何分に 1 回パスワードの入力を要求されたら面倒であると感じると思うか」という事前アンケートを行ったところ，平均 22.5 分という結果が得られたため，本実験では追加対策の頻度を 22.5 分に 1 回に設定した．

5.2 実験方法

研究室の学生 7 人に 4 日間 × 2 回の計 8 日間，本システムを使用してもらった．追加対策（ブラウザ利用時のパスワード認証）の不便さを平等に体験してもらうために，1 回目の 4 日間の実験と 2 回目の 4 日間の実験の間に，22.5 分ごとにパスワードの入力を要求されるブラウザを全被験者に 2 時間利用してもらった．

「No Reply=OK」の運用の妥当性を検証するため，実験期間中に 1 日 2 回，被験者の所持する携帯デバイスのすり替えを行い，在室者（隣席者）が正しく NG を報告するかどうかの調査を行った．ここで，携帯デバイスのすり替えは，内部犯によるデバイス窃盗（ある不正者役の被験者が，他の被験者の携帯デバイスを盗み，携帯デバイスを不正に 2 台所持して入室），内部犯によるなりすまし（ある不正者役の被験者が，他の被験者の携帯デバイス 1 台のみを不正に所持して入室），外部犯の侵入（被験者以外の学生 1 名が，ある被験者の携帯デバイス 1 台を不正に所持して入室）のケースを，実験実施者がランダムに選んで実施した．

5.3 評価方法

本実験システムの評価は，実験システムのログ解析と実験終了後の被験者へのアンケート調査によって行う．

ログ解析では，被験者/不正者の入室と OK（No Reply）/NG の報告数から，被験者間の目視による互いの確認が正しく機能したかどうかを調査した．

実験アンケートでは，提案方式の利便性に関して，「質

問①：入室者に対して一度は目視をしていたか」，「質問②：入室者を目視するという行為は自然か」，「質問③：パスワード入力を何分に 1 回ごとに要求されるのであれば提案システムを使いたいと思うか」，安全性に関して，「質問④：入室通知に気が付くことができたか」，「質問⑤：入室通知に気付いたにもかかわらず入室者を見つけられないことがあったか」をそれぞれ 5 段階評価（1：いいえ～5：はい）で評価してもらい，その理由とともに調査した．

また，3.1 節にて述べた，提案方式の対面コミュニケーション促進の可能性に関し，「質問⑥：提案方式で対面コミュニケーションは生まれると思うか」，「質問⑦：実験中に実際にコミュニケーションが生まれた場面はあったか」についても調査した．提案方式の対面コミュニケーションの促進効果についての考察は，7.4 節にて後述する．

6. 実験結果

5 章の実験で得られた結果から，利便性と安全性の 2 つの観点で提案方式の評価を行う．

6.1 利便性

6.1.1 目視によるユーザへの負荷

アンケートの質問①（実験中は入室者に対して一度は目視を行っていたか）に対する評価は，5 と回答した被験者が 6 名，4 と回答した被験者が 1 名であった．今回の実験では「誰かが入室した際には一度目を向けること」という社内ルールを設けたが，質問①の回答より，実験期間中は被験者は目視に対する意識が実際に高かったことが伺える．

質問②（入室者を目視する行為は自然な行為か）に対しは，5 または 4 と回答した被験者が 6 名，2 と回答した被験者が 1 名であることから，多くの被験者が目視をするという行為に対してさほど負担に感じていないという結果となった．評価が 2 であった被験者からは，「実験を行った部屋の扉に背を向ける形で席が配置されているため，頻繁に行われる入退室に対して首を横に向けたり，後ろを振り向かなければならなかったため，面倒であった」という意見が得られた．

提案方式は，いわば，ユーザ本人の認証行為を周囲のユーザに肩代わりさせる方式である．しかし，以上の実験結果をふまえると，十分な視界を確保できる環境であれば，ユーザは入室者に対する目視確認を大きな負担には感じないということが確認できた．

6.1.2 目視による追加対策の免除

表 1 に，実験期間中の各被験者のブラウザに対するパスワードの入力回数，認証の成功/失敗回数，i/k-Contact によってブラウザへのパスワード入力が免除された回数を示す[*3]．被験者がパスワードを入力した回数の平均は 8 日間で 16.0 回（標準偏差 10.7 回），認証が免除された回数が平均 70.1 回（標準偏差 31.2 回）となっており，提案方式によって，被験者は 22.5 分おきのパスワード入力の約 8 割が免除されたことが分かった．

表 1 各被験者のブラウザにおける認証回数
Table 1 Number of Authentications performing at browser.

被験者No.	1	2	3	4	5	6	7
パスワード入力回数(回)	17	7	8	13	24	8	35
認証成功回数(回)	17	5	6	13	23	8	32
認証失敗回数(回)	0	2	2	0	1	0	3
認証免除回数(回)	105	28	66	40	69	69	114

アンケート項目の質問③（何分に 1 回パスワード入力を要求されるのであれば，提案方式を使いたいと思うか）に対しては，20 分，29 分，1 時間，2 時間，12 時間，24 時間と回答した被験者がそれぞれ 1 名，1 名，2 名，1 名，1 名，1 名という結果であった．すなわち，今回の実験（22.5 分ごとにパスワードを入力）を負担に感じない被験者は 1 名のみという結果であった．個人差はあるものの，パスワード入力が頻繁に要求されるとユーザは負担に感じるという結果が得られたことから，提案方式（追加対策の免除）が利便性の向上に寄与することが確かめられたといえる．

6.2 安全性

6.2.1 目視による確認の妥当性

アンケート項目の質問④（入室通知に気が付くことができたか）に対しては，被験者全員から「気付けた」という回答が得られた．質問⑤（入室通知受信後に正しい入室者を見つけられないことがあったか）に対しては，ほとんどの被験者が「なかった」という回答であったものの，1 名から「立て続けの入室により，目視が遅れると入室者を正しく特定できない」という回答があった．

提案方式の安全性を担保するためには，隣席者同士の目視による確認が確実に行われることが肝要である．今回の実験では，被験者からは，おおむね入室者通知に気付くことができ，入室者を正しく特定できたという回答が得られたが，（扉 A の鍵を 1 人ずつ開錠して入室するようにルールを定めてはいたものの）複数のユーザが連続して入室するようなシーンにおいては目視による確認が正しく機能しない場合が発生しうることが明白となった．この問題に対しては，ユーザの入室時に目視確認をする代わりに，ユーザが自分の席に着席する時点で周囲の席に座っているユーザが目視確認をするという運用を採用することができると考えている．

[*3] 被験者のうち，1 名に関しては，ブラウザのログファイルを誤って削除してしまったため，i/k-Contact サーバ側のログ（当該被験者と他の被験者の在室履歴）から当該被験者のパスワード入力回数とパスワード入力が免除された回数を算出した．当該被験者へのヒアリングから，パスワード入力の失敗はなかったという証言が得られたため，認証失敗回数については 0 回とした．

表 2 不正者実験の結果
Table 2 Experimental resultsforillegal users.

不正者の入退室回数(回)	16
発生したすれちがい回数(回)	51
NGが報告された回数(回)	36
NoReplyであった回数(回)	15
NGを報告した在室者の割合	0.71
NoReplyの在室者の割合	0.29

6.2.2 不正者の特定と見逃し

今回の実験期間中に計 16 回行われた不正者実験において得られた結果を**表 2** に示す．まず，提案システム（i/k-Contact）の運用にあたって，「ユーザはどれくらい NG 報告をしてくれるのか」という点を評価するために，不正者実験において発生したすれ違いの総数における NG 報告の総数を計算した．この結果，16 回の不正者の入室に対し，約 7 割の NG 報告がなされていることが分かった．つまり，確率的には，隣席者が 1 人でも存在すれば 7 割の確率で，隣席者が 2 人になれば 9 割以上の確率で不正者の入室に対して NG が押されることになる．

しかしながら，NG 報告がなされるか否かの期待値は単純な確率計算では評価できず，そのつどの状況に大きく左右される．実際，今回の実験の中でも「不正者が入室したにもかかわらず，在席者（隣席者）が誰も NG をタップしなかった」という事例が 3 回発生した．このような事例が起こった際の状況としては，不正者の入室の前後に他の被験者の入退室が頻繁に発生していた．今後の課題として，不正が発生する状況ごとに個別に分析を行う必要があると考えるが，6.2.1 項で述べた「ユーザの入室時に目視確認をする代わりに，ユーザが自分の席に着席する時点で周囲の席に座っているユーザが目視確認をする」という運用は，この問題に対しても効果的に働くと期待される．

なお，「不正者が入室した際に在席者が 1 人も存在しない」という場合も当然生じるが，このような際には i/k-Contact によって追加対策が免除されるという状況が起こり得ず，不正者に対して基本対策と追加対策の両方が適用されるため，2 段階認証システムの本来の安全性が維持される．

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，内部犯か外部犯か，シンプルな犯行か複合的な犯行かの観点での分析を行う．

シンプルな犯行については，5.2 節で想定したとおり，内部犯か外部犯かを基準に，(i) 内部犯によるデバイス窃盗（内部犯が，他の正規ユーザ α の携帯デバイスを盗み，自身の携帯デバイスと一緒に 2 台所持して入室），(ii) 内部犯によるなりすまし（内部犯が，正規ユーザの携帯デバイスを盗み，正規ユーザ α の携帯デバイス 1 台のみを所持して入室），(iii) 外部犯の侵入（外部犯が，正規ユーザ α の携帯デバイスを盗み，正規ユーザの携帯デバイス 1 台のみを所持して入室）の 3 種類に大別することができる．(ii) と (iii) の場合は，不正者が正規ユーザ α の追加対策を不正に免除させるためには，正規ユーザ α 以外の正規ユーザとの i-Contact が必要となり，その時点で隣席者から NG 報告が届くことになるだろう．一方で，(i) の場合は，不正者は 2 台の携帯デバイスを使って，正規ユーザ α の追加対策を不正に免除させることが可能である．しかし，4.1 節で述べたように，「No Reply=OK」の運用による 2 段階認証システムは，基本対策の実施によって不正者の侵入のリスクを低く保ちつつ，追加対策に対しては i/k-Contact を適用することによって利便性の向上を図ることが主眼である．(i) の場合であっても，不正者が正規ユーザ α になりすますためには，正規ユーザ α の基本対策については何らかの方法で突破する必要があるため，基本対策による安全性のレベルは維持され続ける．

複合的な犯行については，(iv) 複数の不正者による結託，(v) 信頼度がたまった携帯デバイスを盗難しての犯行，(vi) 不正者が正規ユーザ α の携帯デバイスを盗んだ上で正規ユーザ α の近くに潜んで（あるいは，正規ユーザ α を脅し，不正者の近くに隣席することを強要して）犯行に及ぶ場合などが考えられる．(iv) については，認証要求強度の閾値（何人以上のユーザからの OK 報告があったら信頼するか）を十分に大きくすることでリスクを軽減可能である．しかし，この閾値を高く設定することは，利便性を下げてしまうことに直結するため，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る．(v) については，信頼度がたまった携帯デバイスが盗難された場合であっても，基本的には，不正者が他の正規ユーザと隣席する状況に陥った時点で，周囲のユーザの目視によって携帯デバイスの盗難が発覚することが期待できる．しかし，携帯デバイスを盗んだ不正ユーザが，他の正規ユーザと一度もすれ違わないようにして不正を行う状況も十分考えられるだろう．(vi) についても，（不正者と一緒に）正規ユーザ α がその場に隣席している以上，周囲のユーザの目視によって携帯デバイスの盗難を察知することは不可能である．これらの状況を想定したうえで，提案方式の運用方法を検討していかなければならない．

7.2 隣席者情報の表示

i/k-Contact は，現時点の実装では，同僚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 [12], [13]．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「前方から同僚の A さん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同僚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．これらの適用シーンにおいては「No Reply=OK」の運用が適していると考えられる．

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，互いの顔を知らない者同士の間では本方式を運用することができない．本論文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，互いに面識のない社員も会社内に多数存在する．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，6.2.1 項の結果から，複数のユーザが連続して入室するようなシーンにおいては目視による確認が正しく機能しない場合が発生し得ることが確認されている．さらにいえば，人混みの中では「同僚が数 m 以内に隣席している」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ともない，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，空間を超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 [14]．

i/k-Contact では，知人同士の隣席が発生した際に，相手の存在をユーザに通知し，相手の顔を見て確認をとることを求めている．我々は提案方式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を促進すると考えている．

5 章で行った実験のアンケートの質問⑥（提案方式で対面コミュニケーションは生まれると思うか）については，5 または 4 と回答した被験者が 3 名，3 または 2 と回答した被験者が 4 名という結果であった．質問⑦（実験中に実際にコミュニケーションが生まれた場面はあったか）に関しては，質問⑥の回答が 5 または 4 であった被験者からは，「人と目が合う回数が増えたため，自然と挨拶が行える」，「会話のきっかけが増えた」という回答が得られた．質問⑥の回答が 2 であった被験者からは，「今回の実験期間中の目視はあくまで認証の手段であるため，コミュニケーションにはつながらない」という意見が示された．このように，今回の実験では，おおむね半数の被験者は提案方式に対し，対面コミュニケーション促進の効果を実感しているようであった．よって，本方式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を向上させうる可能性が確認された．

著者らは，提案方式が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を期待している．ただし，その一方で，提案方式が運用されることによって新たに引き起こされる社会的問題（たとえば，相手を困らせようとして意図的に NG 報告を送るというような新種の「ネットいじめ」）についても十分検討をしておく必要があることは忘れてはならない．

8. まとめと今後の課題

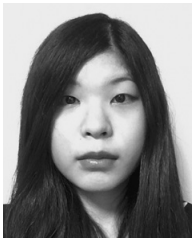
本論文では，現実世界の「人間による目視」を利用した新しいユーザ認証方式である i/k-Contact を提案し，i/k-Contact を用いた適応型 2 段階認証システムの実装・実験・評価を行った．今後は，提案方式の様々な適応シーンを模索していくとともに，多くの被験者による評価実験を行うことによって提案方式の有効性を調査していく．特に，隣席者に積極的に OK 報告あるいは NG 報告を行わせることができる仕組みの有無が，i/k-Contact の実効性に大きく関与する．このため，隣席者に OK/NG 報告に対するインセンティブやモチベーションを与える方法についても模索したいと考えている．また，提案方式を「ユーザ同士の対面的なコミュニケーションを促進」という目的のために利用していく方法についても探っていきたい．

謝辞 本研究は，秋田県立大学飯田一郎教授，静岡産業大学漁田武雄教授より貴重なご助言をいただきました．ここに深く謝意を表します．

参考文献

[1] What is context-aware security, available from ⟨http://searchsecurity.techtarget.com/definition/context-aware-security⟩ (accessed 2015-08-23)
[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] Zhang, F., Kondoro, A. and Muftic, S.: Location-based Authentication and Authorization Using Smart Phone, *Proc. TrustCom2012*, pp.1285–1292 (2012).
[4] Risk-Based Authentication, available from ⟨https://www.schneier.com/blog/archives/2013/11/risk-based_auth.html⟩ (accessed 2015-08-23).
[5] 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).
[6] 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).
[7] 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コンピュータビジョンとイメージメディア（CVIM），Vol.1, No.2, pp.76–85 (2008).
[8] 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).
[9] 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 へリンクする一方式の提案，日本知能情報ファジィ学会，Vol.20, No.4, pp.566–577 (2008).
[10] Gil, M. and Angela, S.: Assessing the impact of CCTV, London: Home Office Research, Development and Statistics Directorate (2005).
[11] コトヴェール：統合警備システム，複数人照合機能，入手先 ⟨http://www.coteau-vert.co.jp/products/TISS/index.html⟩（参照 2015-10-15）．

[12] Telepathy, available from ⟨http://telepathywear.com/product/⟩ (accessed 2015-08-23).
[13] HMZ-T3Z, available from ⟨http://www.sony.jp/hmd/products/HMZ-T3/⟩ (accessed 2015-08-23).
[14] SOCIAL MEDIA: THE DECLINE OF FACE-TO-FACE COMMUNICATION, available from ⟨http://www.brandandmortar.com/social-media/social-media-killer-face-face-communication⟩ (accessed 2015-08-23).



有村 汐里

2014 年 3 月静岡大学情報学部情報科学科卒業．2016 年 3 月同大学院修士課程修了．在学中，情報セキュリティに関する研究に従事．

藤田 真浩 （学生会員）

2013 年 3 月静岡大学情報学部情報科学科卒業．2015 年 3 月同大学院修士課程修了．現在，同創造科学技術大学院博士後期課程．情報セキュリティ，ヒューマンインタフェースに関する研究に従事．2016 年度情報処理学会山下記念研究賞受賞．

松野 宏昭

2016 年 3 月静岡大学情報学部情報科学科卒業．現在，同大学院修士課程．情報セキュリティに関する研究に従事．

可児 潤也

2012 年 3 月静岡大学情報学部情報科学科卒業．2014 年 3 月同大学院修士課程修了．同年株式会社富士通研究所入社．在学中，情報セキュリティに関する研究に従事．

司波 章

1982 年 3 月上智大学理工学部電気電子工学科博士前期課程卒業．同年 4 月株式会社富士通研究所入社．在学中から 1993 年にかけて超音波診断装置の研究開発に従事．その後，モバイルコンピューティングの研究開発を進め，2009 年よりヒューマンセントリックコンピューティングを研究開発中．

西垣 正勝 （正会員）

1990 年静岡大学工学部光電機械工学科卒業．1992 年同大学院修士課程，1995 年同博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．同講師，助教授の後，2006 年より同創造科学技術大学院助教授，2010 年同教授．博士（工学）．情報セキュリティ全般，特にヒューマニクスセキュリティ，メディアセキュリティ，ネットワークセキュリティ等に関する研究に従事．2013～2014 年情報処理学会コンピュータセキュリティ研究会主査．2015 年より電子情報通信学会バイオメトリクス研究専門委員会委員長．