i/k-Contact：ユーザ間の信頼関係を利用したコンテキストアウェア認証

藤田 真浩 * 有村 汐里 * 可児 潤也 † 司波 章 † 西垣 正勝 *

概要. 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・実装する．提案方式は，i-Contact と k-Contact という二つのメカニズムから構成される．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を i-Contact，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．提案方式は，物理的な信頼関係を利用した認証方式であるため，ユーザ同士の対面コミュニケーションを促進する効果も期待される．

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 章では関連研究について述べ，3 章では提案方式の詳細について述べる．4 章で提案方式の適用シーンを述べた上で，その実装を示す．5 章で提案方式について考察する．最後に 6 章でまとめと今後の課題を述べる．なお，本論文は文献 [5][6] の内容に，実験システムの実装と更なる考察を付け加えたものである．

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アクセスした場合に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

* 静岡大学
† 富士通研究所

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）．

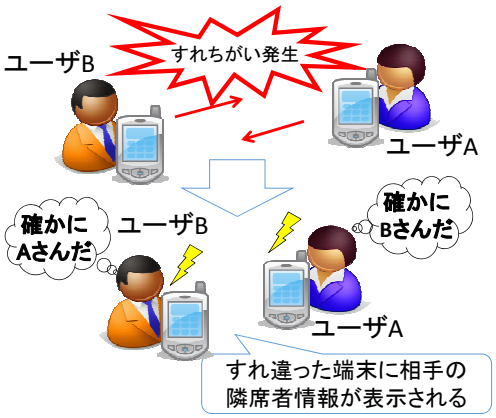

図 1. i-Contact コンセプト図

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．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

[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（ユーザ A）のデバイスにのみ，他方（ユーザ B）の情報を表示する運用も可能である．後者は「既に部屋に在室しているユーザが，新たな入室者を目視で確認する」等の場面で有効である．4 章で実装するシステムはこの運用を想定している．

[2] 関連研究として文献 [14] があるが，文献 [14] はユーザ同士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，ユーザ同士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．

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．

4　実装

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」や「押し間違い」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，筆者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．

4.1　概要

「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 2 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．

すべてのユーザ（学生）は自身の携帯デバイスを有する．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「OK/NG」ボタンを表示する．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 OK ボタンを押す．そうでなければ，NG ボタンを押す．

研究室内には，機密情報を取り扱う（機密情報が入っていると想定した）システムが設置されている．機密情報システム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，単一の認証または認証なしでアクセス可能である [3]．

4.2　機器

実験環境構築のために以下に示す機器を用意した（図 2）．

- 携帯デバイス（Android 端末）複数台：i/k-Contact のクライアントアプリが常時端末上で動作している．NFC リーダ機能を有する．
- 無線ルータ 1 台
- 入室検知モジュール：扉 A に設置されている．加速度センサによって扉の開閉を検知し，その結果を i/k-Contact サーバへ通信する機能を有する．
- i/k-Contact サーバ
- 機密情報を取り扱う PC：機密情報が中にあると想定して，通常（単なるパスワード認証）よりも強い認証がかけられている．今回は [4]，通常時，図 3 に示すとおりパスワード認証と画像認証の 2 段階認証を要するものとしてある．PC には，NFC タグが設置されている．

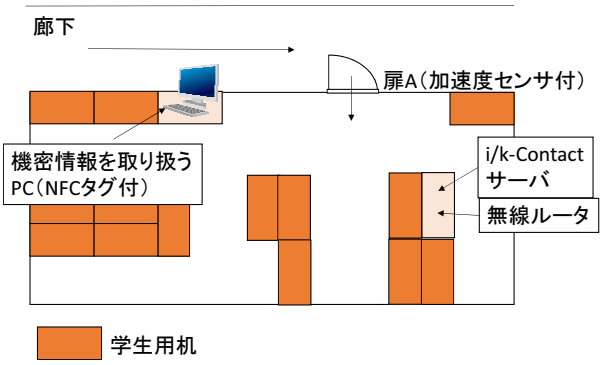

図 2．間取り図

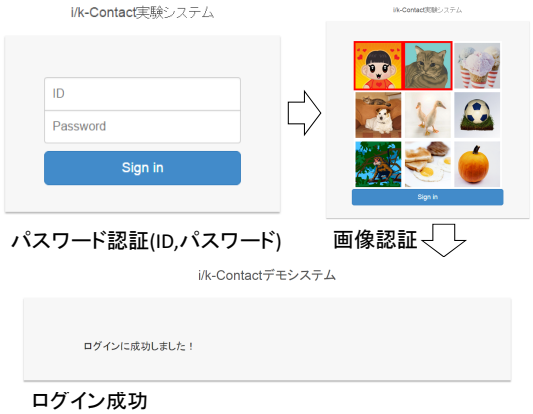

図 3．認証システム（通常時）

すべての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）．

4.3　プロシージャ

実装した i/k-Contact システムのプロシージャを入室時，認証時，退室時の 3 つの場合に分けて次に示す．

[3] 評価実験では，たとえば，各ユーザに毎日決まった時間にシステムへログインすることを求める．

[4] パスワード認証＋生体認証，パスワード認証＋画像認証＋生体認証…のように，他の認証方式の組み合わせへ変更することも容易な実装形態を採っている．今後，評価実験を通じて，様々な認証要素の組合せやそれぞれの認証閾値について精査を行うことを予定している．

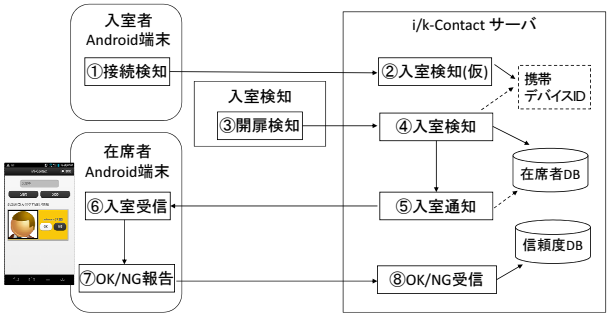

図 4. 入室時プロシージャ

4.3.1 入室時

入室時のプロシージャは以下の通りである（図 4）.

(1) 入室者の携帯デバイス上の i/k-Contact アプリは，無線ルータの通信可能範囲に入ったことを検知した時点で，自身の携帯デバイスの端末 ID を i/k-Contact サーバへ送信する.

(2) i/k-Contact サーバは，入室者から送られてきた携帯デバイス ID を一時的に記録しておく.

(3) 入室者が扉を開いた時，扉 A に設置された入室検知モジュールがこれを検知し，扉が開かれたことを i/k-Contact サーバへ伝える.

(4) i/k-Contact サーバは，(3) の通知を受け，部屋に在室するユーザ一覧を記したリスト（在席者 DB）に，(2) で記録した端末 ID を追加する.

(5) i/k-Contact サーバは，在席者 DB より在室者一覧を取得し，在室ユーザ全員の携帯デバイスに隣席者情報表示のリクエストを送信する.

(6) (5) を受け，在室者の携帯デバイスの i/k-Contact アプリは，振動によって入室者の存在を自身の持ち主へ伝える．同時に，画面に入室者の情報（顔写真と名前）と OK/NG ボタンを表示する.

(7) 在室者は，自身の携帯デバイスの画面に表示された情報（顔写真と名前）が実際の入室者と一致しているかを目視によって確認し，OK/NG ボタンを押す．i/k-Contact アプリは，在室者の入力をサーバへ伝える.

(8) i/k-Contact サーバは，各携帯デバイスから OK/NG を受け取り，その結果 {端末 ID，OK の総数，NG の総数} をデータベース（信頼度 DB）へ記録しておく.

4.3.2 認証時

ユーザは機密情報を取り扱う PC にログインする際に，図 3 の認証システムを通過する必要がある．ユーザが，入室の際に周囲のユーザの多くから OK を得ていた場合，認証の要求強度が引下げられる．今回は，「パスワード認証＋画像認証」から「画像認証のみ」または「認証要求なし」に下げることが可能である.

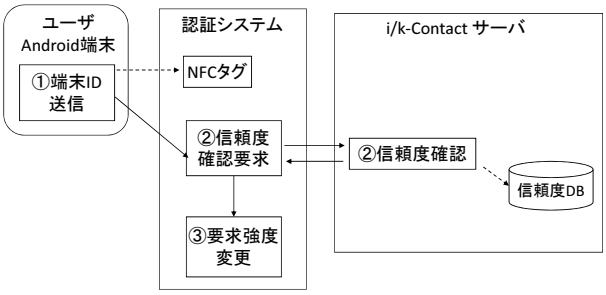

図 5. 認証時プロシージャ

認証時のプロシージャは以下の通りである（図 5）.

(1) 機密情報 PC へのログインを試みるユーザは，認証画面（パスワード認証）が表示された状態で，PC の NFC タグに触れる．これがトリガとなり，携帯デバイス上の i/k-Contatct アプリは認証システムへ端末 ID を送信する.

(2) 認証システムは受け取った端末 ID の信頼度を i/k-Contact サーバへ問い合わせる．i/k-Contact サーバは信頼度 DB の中から端末 ID と一致するエントリを取り出し，OK と NG の総数に基づいて「信頼度」を計算し，認証システムへ返す．信頼度の計算方法は，組織のセキュリティポリシに依存するため種々の方法が考えられるが [5]，今回は単に「OK の総数－ NG の総数」とした.

(3) 認証システムは，受け取った信頼度によって認証の要求強度を変更する．今回は，図 6 のとおりに設定した．信頼度が 0 のユーザは，通常どおり，パスワード認証＋画像認証でログインしなければならない．信頼度が 1 のユーザは，パスワード認証は不要とし，画像認証だけが必要となる．信頼度が 2 以上のユーザは，パスワード認証，画像認証が不要となり，システムへ即座にログインが可能となる.

4.4 退室時

退室時のプロシージャは以下の通りである（図 7）.

(1) 退室者の携帯デバイスが，無線ルータの通信範囲外に移動する.

(2) i/k-Contact サーバは，退室者の携帯デバイスが通信不可能になったことを検出する [6]．在席者 DB から，通信不可能になったデバイスの端末 ID を削除する.

[5] たとえば，セキュリティを第一に考える場合には，1 度でも NG が報告されている端末 ID は，信頼度をゼロにする計算方法が考えられる.

[6] 入室時 (1) から，i/k-Contact サーバが定期的に携帯デバイスへ生存確認を行うことで，生存確認に失敗したデバイスを退室と扱う.

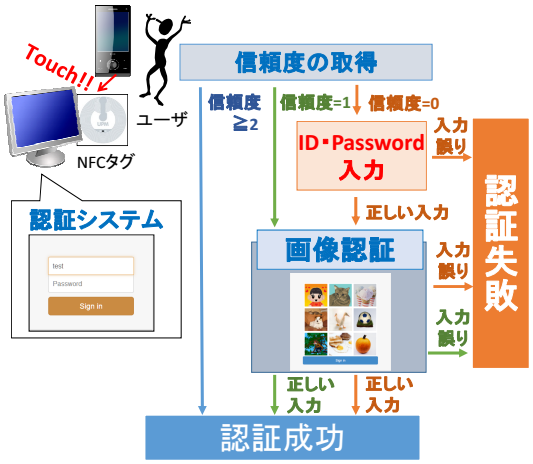

図 6. 認証の要求強度の変更

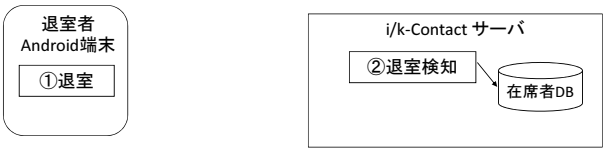

図 7. 退室時プロシージャ

5 考察

5.1 安全性に関する考察

提案方式に関する脅威としては，携帯デバイスの盗難が考えられる．不正者は，隣席者との i-Contact を済ませた正規ユーザが所持している携帯デバイスを盗むことができれば，当該デバイスの所有者になりすますことが可能である．また，内部犯は，組織内の権限者の携帯デバイスを盗むことができれば，盗んだデバイスと自身の携帯デバイスとの間で不正な i/k-Contact を実行することにより，盗んだデバイスの信頼度を高めてその権限者になりすますことが可能である．

この時，不正者は，盗んだデバイスを衆人環視の環境（隣席者が居る環境）の外で使用する必要がある（さもないと隣席者に発見されてしまう）．そこで，信頼度を有するデバイスが衆人環視環境外に移動した時点でデバイスの信頼度をクリアするという対策が効果的である．後者に関しては，認証閾値 k を高く設定することでリスクの更なる軽減が可能である．しかし，閾値の引上げは正規ユーザの利便性低下に直結する．今後，安全性と利便性のバランスを考慮した認証閾値の決定方法も検討していく．

5.2 隣接者情報の表示

i/k-Contact は，現時点の実装では，ユーザ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「前方からユーザ 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ユーザ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．

5.3 OK/NG の報告方法

隣席者に関する OK／NG の報告については，(1) 目視で確認できたか否かを OK/NG 共にユーザがボタンを押して報告する方法，(2) 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，(3) 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．

今回はシンプルな方法 (1) を実装したが，方法 (2) をとることで提案方式の利便性向上が可能である．一方で，一つの場所に比較的多数のユーザが集まる場合には，すべての隣席者へ OK を返答する手間のない方法 (3) をとることも有効であろう．

5.4 適用範囲

i/k-Contact は「人が人を確認する」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ユーザ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．

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．

5.5 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．

6 まとめと今後の課題

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，実際に実験環境を整えた．今後は，実装した実験環境を利用することで，提案方式の可用性，利便性，安全性を評価する予定である．提案方式が本当に対面コミュニケーションを促進する効果を有するのか否かについても確認していきたい．

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.comsocial-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

未来ビジョン

機械（コンピュータ）の能力の発達は著しい．2045 年問題が知られるように，機械の能力は今後より一層発展し，人間の能力を凌駕していくであろう．しかし，機械が得意な能力と人間が得意な能力は根本的にベクトルが異なるものである．人間と機械の両方の能力の活用が，機械を人間と競わせることでは到達できない別次元の可能性を開く鍵になる．

この実現のためには，機械と人間が互いに能力を利用しあえる環境が必須である．近年では，HCI 技術の発達によって機械側の計算処理結果を人間側へ入力することは比較的容易になってきた．一方で，人間側の認知処理結果を機械側へ入力する方法についてはまだまだ検討がなされていない．

本稿で提案した i/k-Contact は，人間の認知能力の一つである「目視」に着目し，人間の目視の結果を機械へ入力することを実現するための具体的な一方式として具現化したものである．人間の目視を利用することによって，機械が曖昧でアノマリの多い人間の行動を正確にセンシングすることが可能となる．

ただし，i/k-Contact は，人間の目視の結果を機械に入力する一手法に過ぎない．著者らは i/k-Contact が「人間の目視の結果をサイバーワールドにインプットする」ための唯一の方法であるとは考えてはおらず，それ以外の可能性についても模索を続けている．また，目視以外の認知処理にも焦点を当て，新たなサービスを創り出していく予定である．