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

有村汐里† 小林真也† 可児潤也†† 司波章††† 西垣正勝††

†静岡大学情報学部情報科学科，〒432-8011，浜松市中区城北 3-5-1
††静岡大学大学院情報学研究科，〒432-8011，浜松市中区城北 3-5-1
†††株式会社富士通研究所，〒211-8588，川崎市中原区上小田中 4-1-1

あらまし 近年ビックデータの活用が注目され始め，それに伴い文脈情報（コンテキスト）のセキュリティ応用に関する研究が再び活発になってきている．本稿では，被認証者と周囲のユーザとの間に成立する「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．隣席者どうし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強度を動的に変更するユーザ認証の仕組みを k-Contact と名付ける．提案方式においては，隣席者どうしの物理的な信頼関係がユーザ認証の礎となっているため，フィジカルなコミュニケーションを促進する効果も期待できる．

i/k-Contact: a context-aware user authentication using physical social trust

Shiori Arimura† Shinya Kobayashi† Junya Kani†† Akira Shiba†††

Masakatsu Nishigaki††

†Faculty of Informatics, Shizuoka University,
3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan
††Graduate school of Informatics, Shizuoka University,
3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan
†††Fujitsu Laboratories Ltd., 4-1-1 Kamiodanaka, Nakahara, Kawasaki, 211-8588 Japan

Abstract In recent years, with the growing demands towards Big Data application, various research on context-aware security has once again become active. This paper proposes a new kind of context-aware user authentication that can control the authentication level using the context of “trust relationship” between users. “i-Contact” is the mechanism that confirms visually the owner of mobile device using the surrounding users’ eyes, and “k-Contact” is the mechanism that changes dynamically the authentication level of each user using the context information collected through i-Contact. By leveraging our proposal, it could expect promotion of physical communication of users because the proposed authentication scheme is based on physical trust relationship of users.

1　はじめに

2012 年 12 月時点で毎日生成されるデータ量は全世界で 2.5 エクサバイト（2.5×10^{18} バイト）に達し，今もなおデータ量の増加の勢いはますます加速している[1]．近年では，このようなビッグデータが注目を集め，膨大なデータを社会に役立てるために，ビッグデータの活用についての研究が盛んに行われている．ユーザのスマート端末から収集される位置情報や時間情報など，様々な文脈情報もビッグデータの一種であり，文脈情報を活用したコンテキストアウェアネスについての研究が数多くなされている．スマート端末に関するコンテキストアウェアネスは「モバイルデバイス管理」（mobile device management: MDM）と呼ばれており，文脈情報に応じてサービスや情報を自動的に配信・実行・消去する情報端末技術基盤（コンテキストデスクトップ）[2][3]などの研究開発が進んでいる．

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[4]に関する研究も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[5][6]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[7]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「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，ユーザどうしのフィジカルコミュニケーションを促進することも可能となる．

本論文の構成は以下のとおりである．2 章では既存の関連研究について述べ，3 章で我々の提案手法の詳細について述べる，4 章で提案方式を実装するにあたっての要素技術，実装したアプリケーションの動作について述べ，5 章で提案方式の可用性について考察する．最後に 6 章で本論文をまとめ，今後の課題を述べる．

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[4]．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[5]．例えば文献[6]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[7]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し，確認をするといった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）そのものを正しく推測することが難しい．センサ情報を利用したユーザの行動推定や，ライフログを活用したユーザ認証[8]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[9][10]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の可能性を探る.

3 提案手法

3.1 コンセプト

本稿では,「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「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, お互いに面識のある 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, 各ユーザの携帯デバイスにお互いの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という確度が高い. 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である.

本稿では, 隣席者どうし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強度を動的に変更するユーザ認証の仕組みを「k-Contact」と名付ける. 提案方式においては, 知人どうし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, ユーザ間のフィジカルなコミュニケーションを促進する効果も期待できる.

本稿では, 以降, 企業等の組織内での利用を想定して議論を進める. 社員は携帯デバイスを所持し, 携帯デバイスのアドレス帳には同僚の携帯デバイスに関する情報(端末 ID と社員名の対応情報)が登録されていることを前提とする. 社員の携帯デバイスは, 社内インフラにアクセス可能である.

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「信頼関係」という文脈情報を用いて, 端末の不正所持(なりすまし)を検知する仕組みである.

正規社員 A の携帯デバイスが, 正規社員 B の携帯デバイスと隣席した際に, お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, 画面には携帯デバイスの端末 ID から特定した社員情報を表示する(社員 A の携帯デバイスの画面には「社員 B と隣席している」という情報が, 社員 B の携帯デバイスの画面には「社員 A と隣席している」という情報が表示される). 社員 A および B は, お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社員であるかを確認する(図 1).

例えば, 不正者 C が社員 B の携帯デバイスを盗んで社内に侵入した場合には, 社員 A の携帯デバイスには「社員 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, 社員 A の周囲に社員 B が居ないという状況となる. これによって, 社員 A は「不審者が社員 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居る」という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」を判断する方

式となっている.

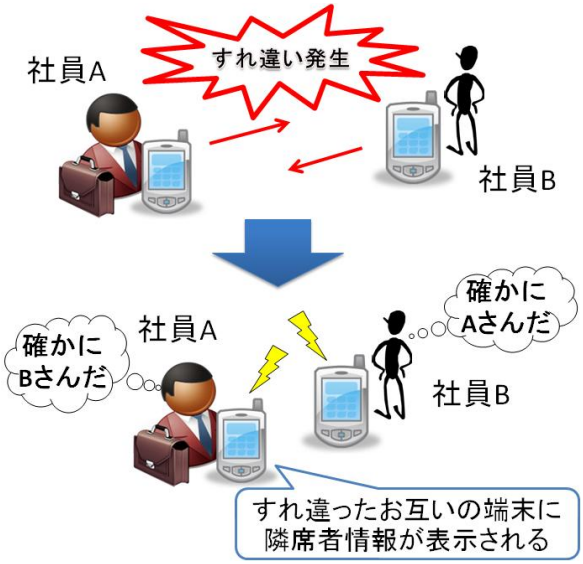

図 1　i-Contact のコンセプト

3.3　k-Contact

k-Contact は，前節で述べた i-Contact の情報を利用し，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強度を動的に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「目視によるお互いの確認」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」または「NG ボタン」が表示され，ユーザがそのボタンを押すことによって，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.

正規社員であれば，社内で他の社員と隣席する度に，隣席者から OK の報告を受けることになる．すなわち，OK の報告数が多く，かつ，NG の報告の少ないユーザほど，正規社員が正しく携帯デバイスを所持している確度が高い．このため，そのような社員に対しては，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，言わば，衆人環視型のユーザ認証システムである．たとえば，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ったり，複数の社員が同席しての会議の際にはユーザ認証なしで会議資料へのオンラインアクセスを許すような利用例が考えられる.

4　実装

本稿では，文献[2][3]で開発されている情報端末技術基盤（コンテキストデスクトップ）の上で，i/k-Contact のプロトタイプ実装を試みる.

4.1　コンテキストデスクトップ

コンテキストデスクトップにおいては，文脈情報に応じてユーザの携帯デバイスにアプリケーションを自動的に配信・表示・実行させる Push&Play [11]という技術が利用可能である．また，GPS による測位が不可能である屋内における場所情報の利用を実現するために，プレイスサーバ 2 が開発されている．プレイスサーバはロケーションごとに設置されており，ユーザの所持している携帯デバイス D がプレイスサーバ P の通信可能範囲に入る（チェックイン）ことによって，「携帯デバイス D がロケーション P に存在している」という文脈情報を得ることができる．プレイスサーバは携帯デバイス内の場所検知アプリ（プレイスサーバを検知してロケーションを取得するアプリ）とプレイスサーバ内の場所検知サーバ（ロケーションやアプリを提供するサーバ）でこの機能を提供している.

今回は，Push&Play とプレイスサーバを利用することによって，i/k-Contact の仕組みをスマートフォンのアプリとして実装する．端末側のアプリの実装は HTML5 をベースに行った．プレイスサーバは Tomcat 上の Java サーブレットとして動作する．スマートフォンの OS は Android 4.2.2 であり，プレイスサーバの OS は

Debian 6.0.7 である.

4.2 i-Contact の実装

社員の隣席状況は社員の位置情報のみを用いて判定可能であるため, i-Contact はそれぞれのプレイスサーバごとに実装する. i-Contact のアーキテクチャを図 2 に示す.

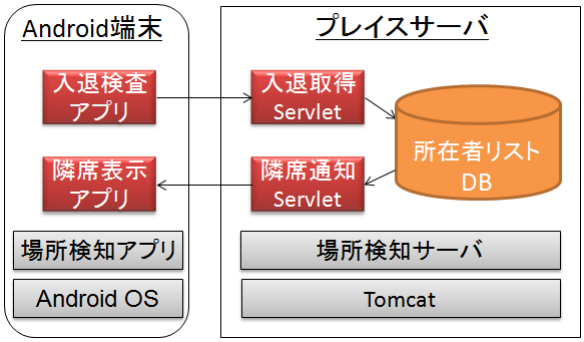

図 2 i-Contact アーキテクチャ

1. 社員の携帯デバイスがプレイスサーバとの通信可能範囲内にチェックインした時点で,「入退検査アプリ」によって携帯デバイスの端末 ID がプレイスサーバに送られる.
2. プレイスサーバは,「入退取得サーブレット」によって端末 ID を受信し,「所在者リスト」に端末 ID(および, その携帯デバイスの所有者)を登録する.
3. プレイスサーバ内の所在者リストに 1 つ以上のエントリが登録されている状況において, 新たな携帯デバイスが当該プレイスサーバにチェックインした場合には,「隣席通知サーブレット」はリスト内のすべて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.
4. これを受け, それぞれの携帯デバイス内の「隣席表示アプリ」が画面に隣席者の情報を表示する.
5. 社員の携帯デバイスがプレイスサーバとの通信可能範囲外に退出すると, 入退検査アプリと入退取得サーブレットの働きによって, 当該携帯デバイスの端末 ID がプレイスサーバ内の所在者リストから削除される.

4.3 k-Contact の実装

i-Contact の運用によって, 社内すべてのプレイスサーバにて社員どうしの隣席者チェックが実行されることになる. k-Contact では, その際の OK／NG 情報を全プレイスサーバから集約し, この情報を利用して社員の社内リソースへのアクセスをコントロールする. このため, k-Contact は, 社内の集中管理サーバにて実装する. k-Contact のアーキテクチャを図 3 に示す. ただし, 今回はプロトタイプのため, 集中管理サーバの機能はプレイスサーバ内に実装するという形態とした. また携帯デバイス内のリソースへのアクセスを認証するという利用シーンを想定したシステム実装となっている.

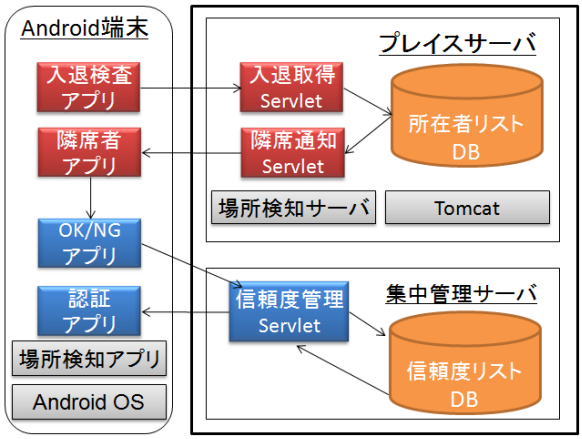

図 3 k-Contact アーキテクチャ

1. i-Contact の運用によって, 社員が社内で他の社員と隣席した際に, 隣席者から OK／NG の評価が戻される. この評価結果は, 携帯デバイスの「OK／NG アプリ」によって, 集中管理サーバに直接送信される.
2. 集中管理サーバは,「信頼度管理サーブレット」によって, 携帯デバイスから届く情報を集約し, 管理している. 具体的には, 社員ごとに「隣席者から OK の報告がなされた回数」,「NG の報告がなされた回数」を集計し, この情報を各社員の信頼度として「信頼度情報リスト」の中に記録する.
3. 社員が自身携帯デバイスにアクセスする際には,「認証アプリ」が集中管理サーバに携

帯デバイス所有者の信頼度を問い合わせる.

4. 信頼度管理サーブレットは，当該社員の信頼度を認証アプリに返答する.
5. 携帯デバイスは，当該社員の信頼度が高い場合は，ユーザ認証なしで携帯デバイス内のリソースへのアクセスを許可する. 信頼度が低い場合は，所有者に所定のユーザ認証の実施を促し，認証に通過した場合のみリソースへのアクセスを許可する.

手順 5 においては，社員の信頼度に応じて，ユーザ認証の要求強度を多段階に設定してもよい. 例えば図 4 の例では，信頼度の高い社員はパス画像を選択するだけで認証成功となるが，信頼度の低い社員はパス画像を選択した上でパスワード入力も求められる方式となっている.

図 4 k-Contact 認証画面例

5 考察

5.1 信頼度の評価

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.

また，OK／NG の報告数から信頼度を算出する方法についても，幾つかのアルゴリズムが考えられる. 例えば，セキュリティを第一に考える場合には，NG の報告数に比例して当該社員の信頼度を下げていく方法よりも，1 度でも NG と報告された時点で信頼度をゼロにする方法のほうが適切だと思われる.

5.2 認証強度の変更

k-Contact においては，社員が携帯デバイスや社内リソースにアクセスする際に要求される認証強度が，隣席者からの OK／NG の報告数に応じて変化する. 基本的には，OK の報告数が多くなるほど，または，NG の報告が少ないほど要求される認証強度は下がっていくことになるが，具体的にどのように認証強度を変化させるのかに関しては，社内のセキュリポリシに応じて設定されることになる. 具体例を表 1 に示す.

ユーザの信頼度	認証強度	再生型認証	生体認証
高い	認証情報の入力不要		
	弱い	軌跡認証	甘い閾値
↕	↕	↕	↕
低い	強い	フルパスワード	厳しい閾値
	アクセスを許可しない		

表 1 OK／NG に対する認証強度変更例

また，表 2 の例のようにアクセスする情報（携帯デバイス内のリソースや社内サーバ内のリソース）の機密度に応じて認証強度を調整することもできる.

リソースの機密度	要求される認証方法	
	α 人以上からの隣席者からのOKが届いているユーザは認証情報の入力なしでアクセス可能	β 以下の隣席者からしかOKが届いていないユーザはフルパスワードの入力ができない限りアクセスが許可されない
高い	α =10	β =9
↕	↕	↕
低い	α =2	β =1

表 2 リソースの機密度に応じた認証強度の設定例

5.3 隣席者情報の表示

i/k-Contact は，現時点では，社員の携帯デバイス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，今後スマートフォンは進化を遂げ，イヤホンタイプやメガネタイプのスマートフォンが現れるだろう．このような次世代スマートフォンにおいては，ユーザに音声で「前方から社員 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社員の頭上に隣席者情報を表示するようなことが可能となると考えている．

5.4 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よる認証方式となっているため，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．本稿では社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社員も社内に多数存在する．部署ごとにを i/k-Contact を運用するなどの方法が必要となる．

また，満員電車や雑踏の中では，同僚が数メートル以内に居るという情報を知ることができたとしても，その同僚を見付けることができない場合があるだろう．i/k-Contact の運用が可能となる要件を精査する必要がある．

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って，ユーザどうし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．これによって，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，知人どうしの隣席が発生した際に，お互いの存在を認識し，目を合わせて確認をとることが要求される．これが，挨拶や会話のきっかけになるなど，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あるのではないかと期待している．

6 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「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である i/k-Contact を提案した．隣席者どうし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 であり，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．

本稿では，i/k-Contact の詳細を示した上で，プロトタイプの実装までを行った．今後は，i/k-Contact を実際に稼働させることによって，本方式の可用性，利便性，安全性を評価していく必要がある．また，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．

今回の実装においては，プレイスサーバを利用して i/k-Contact のプロトタイプを構築したが，すれ違い通信[13]によってお互いの情報をやり取りすれば，携帯デバイス自身が他デバイスとの隣席を判断したり，隣席者からの OK／NG の報告を受け取ることも可能である．今後は，携帯デバイス自身が i/k-Contact の機能を担う分散型方式についても検討していきたい．

参考文献

[1]日経トレンディネット，”今年の IT 業界を席巻したビッグデータとは？”，
http://trendy.nikkeibp.co.jp/article/column/20121214/1046357/（参照 2013/08/26）
[2]松本達郎，二村和明，司波章，藤井彰，”コンテキストデスクトップ技術”，FUJITSU，vol.63,

No.5, pp.531-536,
(2012/09)http://img.jp.fujitsu.com/downloads/jp/jmag/vol63-5/paper06.pdf
[3] 奥山敏, 森信一郎, 小川晃弘, "屋内ロケーション管理技術", FUJITSU, vol.64, No.1, pp.66-73(2013/01)
[4]インプレス SmartGrid フォーラム, "コンテキストアウェアネスと情報セキュリティ", http://wbb.forum.impressrd.jp/feature/20081119/703（参照 2013/08/26）
[5] 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,(2006.01)
[6] 坂本宏, "位置情報を用いた認証システム, 認証サーバおよび位置情報を用いた認証方法", 特願 2006-320768, 2006.11.28 出願
[7]西京銀行, "リスクベース認証", http://www.saikyobank.co.jp/personal/service/chotnet/riskbase_authentication.htm（参照 2013/08/26）
[8]石原雄貴, 小池英樹, "ライフログを用いた認証システム", マルチメディア, 分散, 協調とモバイル(DICOMO 2007)シンポジウム論文集, Vol.2007, No.1, pp.264-268, July.2007
[9]行方エリキ, 石原進, 水野忠則, "携帯端末の動きによる個人認証～コヒーレンスに基づく評価～", 情報処理学会論文誌, Vol.32, No.7, pp.37-44, (1991/07)
[10]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", 処理学会論文誌, Vol.1, No.2, pp.76-85 , July.2008
[11]Ito, H., Nimura, K., Nakamura, Y., Shiba, A. and Fujino, N.: Application Push & Play – Proposal on Dynamic Execution Environment Combined with Personal Devices and Cloud Computing.- , IWIN 2011, pp97-103 (2011).
[12]angels-eyes, "インターネット Addiction, コミュニケーション能力の低下", http://angels-eyes.com/net_a/c-down.html（参照 2013/08/26）
[13] 任天堂, "ニンテンドー3DS 専用ソフトの通信機能について", http://www.nintendo.co.jp/3ds/support/network_icon.html