街中での自律的情報交換における端末間認証と相互評価方式の提案

中川 文博 † 玉井 祐輔 ‡ 高田 秀志 §
立命館大学情報理工学部 † 立命館大学大学院理工学研究科 ‡ 立命館大学情報理工学部 §

1. はじめに

我々は，Bluetoothなどを用いて端末内の情報を自律的に端末間で交換し，ユーザの偶発的な情報発見を促す協調的情報共有環境「街角メモリ」[1]の構築を行っている．この街角メモリの端末は，他の端末とすれ違ったときに，互いに通信し情報を交換する．これにより，自分から情報にアクセスする場合とは違う，口コミや漏れ聞きのような受動的で偶発的な情報発見の機会が生まれる．

このとき，利用が許可された端末のみが情報交換を行えるようにするには，端末同士で利用権の確認を行えるようにする必要がある．また同時に，端末間で情報を交換する中で，社会的に不適切な情報が氾濫しないようにする必要がある．そこで，各端末が自律的に情報交換を行うとき，端末で以下の確認を行うことにする．

- 通信相手の端末が第三者機関から利用権を与えられているか
- 受信した情報の作成者が，公序良俗に反する迷惑情報を作成したり，発信したりするユーザでないか

前者は，公開鍵認証系を利用した端末同士の相互認証により確認する．また，後者についてはまず，各ユーザが作成する情報が，どの程度公序良俗に則するかを示す，ユーザの評価値を各自の端末に持たせる．また，それを指標として，受信側の端末で閾値によるフィルタリングを行い，評価値の低いユーザに作成された情報を，受信側の端末のユーザに見せないようにする．

本稿では，このような端末間での相互認証と相互評価を行うための手法を提案する．また，この手法を実現したプロトタイプシステムの実装について述べる．

2. 街中での自律的情報交換

近年，携帯型情報端末の普及により，個人に宛てた電子メールを送信したり，公衆向けのweb情報を閲覧する機会が増えた．これらの携帯型情報端末で扱われる情報は，誰かから意図的に送信されたり，自らアクセスしない限り，ユーザの目に触れることはない．つまり端末のユーザは，井戸端会議や他人の会話を漏れ聞くなどのように，他人の携帯端末内の情報を受動的で偶発的に発見することはできない．

そこで本手法では，携帯型情報端末に含まれる情報を端末が自律的に交換することで，ユーザの偶発的な情報発見を促進する．これにより，例えば従来ならばユーザが自ら調べないと存在すら知らなかったイベントの情報を，偶発的に入手できるといったことが起こりえる．

我々が構築を目指す協調的情報共有環境「街角メモリ」では，端末同士がそばにいるときにBluetoothで通信し，互いの端末内の情報を交換することを想定している．ユーザが無秩序に情報を流すことができると，違法性のある情報や公序良俗に反する情報の氾濫が予想される．本稿では，このような問題への対策として，自律的情報交換における端末間認証と相互評価方式を提案する．

3. 端末間認証と相互評価のモデル

本手法では，先に述べた問題を解決するために，サーバがユーザの登録を管理し，サーバに登録されたユーザの端末同士のみが通信できるようにする．また，ユーザの端末には，ユーザ自身が変更できない識別子と評価値を持たせ，この識別子と評価値をサーバで管理する．

3.1 認証による相手端末の利用権の判定

端末同士が通信するとき，通信相手がサーバに登録された端末であるかを確認する必要がある．本手法では，サーバから端末に電子会員証を発行し，端末間でその会員証を互いに確認しあうことでこれを実現する．この手順を図1に示す．

3.1.1 電子会員証の取得

各端末がサーバから電子会員証を取得する．手順は以下のとおりである．

1. 各端末は定期的に，サーバに自端末の識別子を通知する．(a)
2. サーバは通知を受けると，その識別子が登録された端末のものかを確認し，登録されていればその端末用の電子会員証を端末に送る．(b) 電子会員証は，自端末の識別子と評価値，有効期限，電子署名を含む．この電子署名は，識別子と評価値，有効期限が改ざんできないように発行されたものである．また有効期限は，その電子会員証の有効期限である．
3. 同時に，サーバは端末に，電子会員証の署名検証用として公開鍵を送る．(c)

3.1.2 相手端末の利用権の判定

端末間で互いの電子会員証を確認し合う手順は，以下のとおりである．

1. 端末間で互いに識別子と電子会員証を交換する．両端末で，受信した電子会員証に含まれる識別子と有効期限，これらの電子署名を公開鍵で検証し，電子会員証が改ざんされていないかを確認する．また，相手の識別子が電子会員証の識別子と一致し，有効期限が現在日時と比較して有効かを確認する．(d)
2. これらの確認が取れれば，端末間で相手の会員証は正しいものであると判定でき，会員証に含まれる識別子の端末はサーバに登録された端末であると確認できるため，端末間で情報交換を開始する．(e)

3.2 発信者評価値による情報の健全性の判定

前節の手法では，自端末が他端末と通信するとき，通信相手の端末が第三者機関から利用権を与えられているかのみを確認できる．しかしこれは，端末が受信する情報が，公序良俗に反する迷惑情報でないことを保障するものではない．そこで，各ユーザが作成する情報が，どの程度公序良俗に則するかを示す評価値を，各端末で持つようにする．また，情報を受信した端末で，その情報の発信者の評価値を指標としてフィルタリングする．フィルタリングを通過しなかった情報を，受信した端末でユーザに見られないようにすることで，ユーザが迷惑情報を閲覧する可能性を低減させる．この手法を，図2を用いて以下に説明する．

An Authentication and Mutual Evaluation Method for Autonomous Information Exchange.

† Fumihiro Nakagawa・Ritsumeikan University
‡ Yusuke Tamai・Ritsumeikan University
§ Hideyuki Takada・Ritsumeikan University

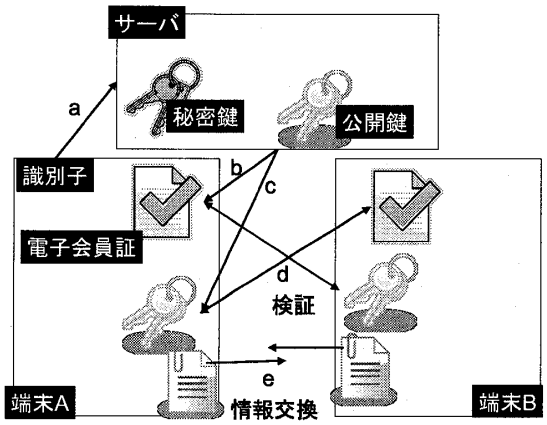

図 1: 通信相手の認証

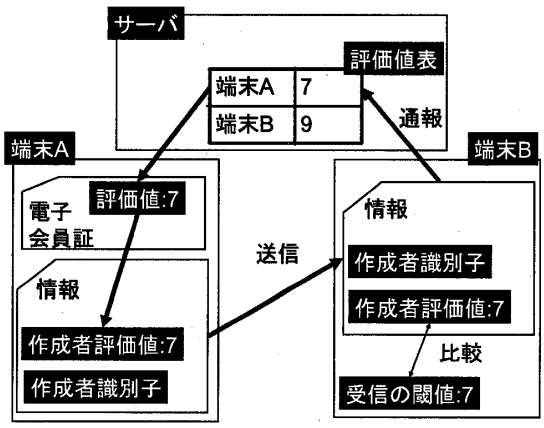

図 2: 情報発信者の評価値に基づく迷惑情報の判定

3.2.1 評価値の管理

サーバでは，全端末のユーザの評価値が一元管理される．3.1 節で述べたように，本手法では，各端末で自端末のユーザの評価値が含まれた電子会員証を定期的に取得する．取得した評価値は，ユーザ自身で改ざんできないよう，識別子や有効期限と共に暗号化して，端末内に保存される．

3.2.2 受信閾値によるフィルタリング

本手法では，端末が情報を受け取ったとき，情報の作成者の評価値を用いて，端末で情報がユーザに見られるか見られないかを判定できるようにする．そのために，各ユーザは最初に，この一定基準を受信閾値として自分の端末に設定する．この閾値未満の評価値を持つユーザが作成した情報は，自端末が受信しても自動的に削除されるものとする．ユーザは，自分の端末が受信する迷惑情報が多いと感じたとき，この閾値を引き上げることで，評価値の低いユーザが作成した情報を，受信しないようにすることができる．

端末 A で，ある情報が作成されたとき，その情報は端末 A の識別子，評価値と共に，暗号化して端末 A 内に保存される．この情報は，端末 A が周りに端末を見つけたとき，相手の端末に送信される．

端末 B が端末 A の作成した情報を受信したとき，端末 B では，その情報に含まれる作成者の評価値が確認される．もしその評価値が端末 B の受信閾値以上であった場合は，その情報は端末 B 内に保存される．評価値が受信閾値未満であった場合は，その情報は端末 B 内で削除される．

3.2.3 迷惑情報の通報

端末 B のユーザが，端末 A から受信した情報を閲覧し，迷惑情報であると感じたとき，その情報を迷惑情報として設定できる．迷惑情報として設定された情報は，端末 B で電子会員証が定期的に取得される前に，サーバへ送信される．サーバが迷惑情報の通報を受けると，端末 A のユーザの評価値が下げられる．ただし，評価値は下がるのみだと，時間がたつにつれ評価値の低いユーザばかりになることが予想される．そこで，一定期間ごとに一定値ずつ，全てのユーザの評価値が回復されるようにする．評価値が回復される値の大きさと周期は，別途運用ポリシー等で定めることにする．

4. ソフトウェアの構成

本節では，これまでに述べた手法を実現するためのソフトウェア構成について述べる．実装としては，サーバと端末の通信はインターネットを，端末間の通信は Bluetooth を使用し，端末の識別子は Bluetooth Device Address(BDA) を使用する．

端末は，電子会員証取得ツール，情報作成ツール，情報交換ツール，情報閲覧ツール，通報送信ツールを持つ．

電子会員証取得ツールは，自端末の BDA をサーバに通知し，サーバから公開鍵と電子会員証を取得する機能を持つ．電子会員証に含まれる評価値は，9 点から 0 点の 10 段階で表わされ，ユーザ登録時は 9 点の状態である．情報作成ツールは，ユーザが作成する文章形式の情報を，作成者の評価値，BDA と一緒に暗号化し，他端末に送信する情報として，ファイルに保存する．

情報交換ツールは，周期的に周りの端末を探し，見つかった端末と自端末で電子会員証を交換して，情報を送信する機能を持つ．相手の会員証に不正がなく，相手が送ってきた情報の作成者評価値が自分の受信閾値以上の場合のみ，その情報は端末内に保存され，他は削除される．情報閲覧ツールは，受信した情報を端末で復号し，情報を画面上に表示する機能を持つ．ユーザがその情報を迷惑だと判断すれば，ユーザはそれをボタン操作で，迷惑情報として設定することができる．通報送信ツールは，迷惑情報として設定された情報をサーバに通報し，完了後端末内のその情報を削除する機能を持つ．

サーバは，電子会員証発行ツールと，通報受信ツールを持つ．電子会員証発行ツールは，端末から BDA の通知を受けると，その BDA に対応する端末の電子会員証を生成し，それを端末に送る機能を持つ．通報受信ツールは，端末から送信された迷惑情報の通知に基づき，サーバでユーザの評価値を管理する機能を持つ．

5. おわりに

本稿では，認証によって通信相手の端末の利用権を判定し，さらに，情報発信者の評価値によって情報の健全性を判定する手法を提案した．今後は，悪意ある嘘の通報により，迷惑情報を作成していないユーザの評価値が減少させられる事態を防ぐため，サーバで通報の信憑性を判定する方法を検討する予定である．

謝辞

本研究を進めるにあたり，有益なご助言を頂きました立命館大学情報理工学部島川博光教授，原田史子助教授および研究室の方々に感謝いたします．

参考文献

[1] 高田秀志，伊藤寛修，大西雅宏，玉井祐輔，津田侑，野口尚吾，”個人情報端末間の能動的情報交換による日常的コミュニケーション支援”，インタラクション 2007，2007