Vol.2014-GN-90 No.21
Vol.2014-CDS-9 No.21
Vol.2014-DCC-6 No.21
2014/1/24

ステガノグラフィを用いた 第三者の仲介不要なセッション鍵共有方式

宮嵜仁志[†1]　福本真輝[†1]　奥村香保里[†1]
福田洋治[†2]　廣友雅徳[†3]　毛利公美[†4]　白石善明[†5]

サービスの窓口で身分証明書を確認し，直接利用者の本人確認をされることがある．また，他者に見られないよう，間仕切りなどで他者の視線を遮ってやりとりをすることがある．これらはネットワーク上では，伝送するデータを通信セッションごとに異なるセッション鍵で暗号化することに対応する．利用者の直接的な本人確認をしたうえでセッション鍵を共有できればオンライン窓口を実現できる．本稿では，オブジェクトベース AKE という概念に基づいて，利用者を示す連続静止画により直接的に本人確認できる，ステガノグラフィを用いた第三者の仲介不要なセッション鍵共有方式を提案する．評価用のプログラムによりユーザ実験を行った結果，20 人中 19 人が正しく本人確認できた上でセッション鍵を共有できた．

Session Key Sharing Scheme Using Steganography without Third Party

Hitoshi MIYAZAKI[†1]　Masaki FUKUMOTO[†1]　Kaori OKUMURA[†1]
Youji FUKUTA[†2]　Masanori HIROTOMO[†3]
Masami MOHRI[†4]　Yoshiaki SHIRAISHI[†5]

At a service window, we are sometimes identified directly by identification papers, and users and a teller communicate in a partitioned place to avoid other's eye. These correspond to encryption with session keys which vary according to sessions. The session key exchange with direct user identification enables to realize online windows. In this paper, we propose an object-based session key exchange scheme using steganography. The scheme enables direct identification with continuous still image of users, and does not require agency. We conducted a user experiment, and made sure that 19 out of 20 users could exchange a session key with accurate identification.

1. はじめに

インターネットオークションなどネットワーク上で金品の取引をするサービスでは，詐欺などのトラブルを防ぐために会員登録の際に利用者の本人確認を行う．金品などを取り扱うような本人確認が必要な手続きは，銀行口座の開設の手続きのときのように基本的には本人が窓口に出向いて行うことで本人確認の有効性を担保している．場所を選ばないネットワーク上のサービスと一般の窓口は性質が異なることから，ネットワーク上のサービスの会員登録の際に，本人が直接出向いて利用者の確認をされることは通常なされない．代替手段として本人確認書類を郵送する簡易的な手順が認められている場合がある．しかし，インターネットオークションにおいて，相手方の連絡先が実在しない[1]といったトラブルが起きており，本人確認の代替手段は窓口と同様の本人確認の有効性を担保できていない．

†1 名古屋工業大学
Nagoya Institute of Technology
†2 愛知教育大学
Aichi University of Education
†3 佐賀大学
Saga University
†4 岐阜大学
Gifu University
†5 神戸大学
Kobe University

見知らぬ個人間の取引において，相手の保証を求める声が大きく[2]，サービスの窓口業務をネットワーク上で実現できれば，安心して金品などの個人取引を行える付加価値がサービスに与えられるようになる．

オンライン窓口を実現するために，一般に窓口業務で行われている手順を，オンライン窓口で再現することを考える．まず，窓口業務では身分証明書を確認して，直接利用者の本人確認をする．他人に見られたくない情報を扱うこともあるため，やり取りを他人に見られないように間仕切りや個室を設けるなどで他者からの視線を遮った上で，サービス利用者と窓口業務者がやり取りをする．ネットワーク上で他者からの視線を遮ることは，通信セッションごとに異なるセッション鍵を用いて伝送するデータを暗号化して機密性を確保する方法が対応する．したがって，窓口業務をネットワーク上で実現するには，直接利用者の本人確認をした上でセッション鍵の共有をするということになる．

従来，ネットワーク上で直接本人確認をする方法がなかったため，ネットワーク上で通信相手が意図した相手であることを確認するときには，意図した相手しか持ち得ない秘密情報を持っていることを確認して通信相手を認証，すなわち，間接的な本人確認をしてきた．

ネットワーク上で認証とセッション鍵を共有すること

Vol.2014-GN-90 No.21
Vol.2014-CDS-9 No.21
Vol.2014-DCC-6 No.21
2014/1/24

を合わせた認証鍵交換(AKE: Authenticated Key Exchange)プロトコルがある．代表的な AKE プロトコルは，パスワードベース AKE と PKI(PKI: Public Key Infrastructure)ベース AKE である．

パスワードベース AKE は，第三者に知られないように事前共有した共通鍵を所有していることを証明することで，認証が実現される．送受信者でパスワードを共有する際に，事前に対面で本人確認をしなければならない．このことはオンライン窓口を実現する手順と矛盾するものである．

PKI ベース AKE は，電子署名技術を用いたもので，秘密情報である秘密鍵を所有していることを証明することで認証が実現される．電子署名は公開鍵暗号を応用した技術であり，公開鍵と秘密鍵のペアを生成し，公開鍵のみを公開する．この方法では，通信相手が持っている秘密鍵が意図した相手のものであることを確認するために，認証局が発行した公開鍵証明書が必要となる．信頼できる第三者である認証局がオフラインで本人確認を行ってから発行する公開鍵証明書を所有している個人はほとんどいない．

すなわち，既存の AKE プロトコルでは，オンライン窓口の利用者にあたる個人のための本人確認をした上でセッション鍵共有をすることは難しく，一般に窓口業務で行われている手順を再現できない．また，既存の AKE プロトコルでは，通信相手が意図した相手のみが所持しているはずの秘密情報を持っていることを確認して認証，すなわち間接的な本人確認を行うものばかりであるが，一般に窓口業務では，利用者を対面で直接本人確認している．第三者を介さない直接的な本人確認をした上でセッション鍵共有ができれば，オンライン窓口を実現できる．

本稿では，まずオブジェクトベース AKE と呼ぶ対象物を利用した認証の概念を示し，次にその一構成法としてステガノグラフィを用いた第三者仲介不要のセッション鍵共有方式を提案する．ステガノグラフィは埋め込みデータをカバーデータに埋め込んでステゴデータを作成し，埋め込みデータの存在を他者から隠す技術である．ステガノグラフィ技術は情報を伝送していること自体を隠すことを目的としているが，カバーデータに情報が埋め込まれていることを前提に応用した研究が数多く行われており[3]，それらの研究ではステガノグラフィ技術を，埋め込みデータとカバーデータの二つのデータを結びつける目的で用いている．カバーメディアをカメラによって撮影された証明者を示す連続静止画とし，それにセッション鍵を埋め込むことで二つのデータを紐づけすれば，ネットワーク上で利用者の直接的な本人確認をしながら，セッション鍵を共有することが実現できる．

以下，2 章では一般に窓口業務で行われている手順をオンライン窓口で再現することを考え，オンライン窓口を実現するための課題について述べる．3 章では既存の秘密情報を利用した認証鍵交換プロトコルの認証方法と，それらがオンライン窓口業務での本人確認に適さないことを述べる．4 章ではネットワーク上で直接本人確認をするためのアイデアとそれを実現する技術について述べる．5 章では提案方式について述べ，6 章では提案方式の安全性についての考察を述べる．7 章では試作した提案方式の評価用プログラムとその基本性能，ユーザ実験について述べ，8 章でまとめる．

2. オンライン窓口を実現するための課題

オンライン窓口を実現するために一般に窓口業務で行われている本人確認の手順を，オンライン窓口で再現することを考える．窓口を利用する人を「利用者」，窓口で業務を行う人を「窓口業務者」とする．まず，一般の窓口業務での直接的な本人確認の手順を図 1 に示す．

1. 利用者が身分証明書を窓口業務者に渡す
2. 窓口業務者が身分証明書の写真と利用者の顔が一致しているか確認する

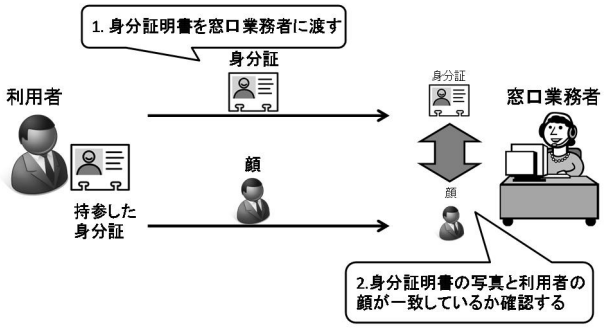

図 1 窓口における身分証明書による本人確認の手順
Fig. 1 Step of identity verification at offline teller window.

次に，これらの手順をオンライン窓口で再現する手順を考える．1. の手順をオンラインで行うには，スキャンやカメラで撮影しデータ化した身分証明書の写しを，窓口業務者の公開鍵で暗号化して送り，サーバーにアップロードする方法が考えられる．アップロードされた身分証明書の写しに受付番号を発行しておけば，同じ受付番号を持った利用者がオンライン窓口にアクセスしたときに身分証明書の写しと利用者の顔が一致していることを確認できる．

以上をまとめると，図 2 に示した一般の窓口業務の手順に対応するオンライン窓口での手順は以下のようになる．

1-1. 利用者が身分証明書の写しを窓口側の管理するサーバーに登録する
1-2. 身分証明書の写しに受付番号が発行される
1-3. 利用者が窓口業務者に受付番号を送る
1-4. 窓口業務者が身分証明書の写しの受付番号と送られてきた受付番号が一致するか確認する
2. 窓口業務者が身分証明書の写しと利用者が本人であることを示す情報が一致しているか確認する

Vol.2014-GN-90 No.21
Vol.2014-CDS-9 No.21
Vol.2014-DCC-6 No.21
2014/1/24

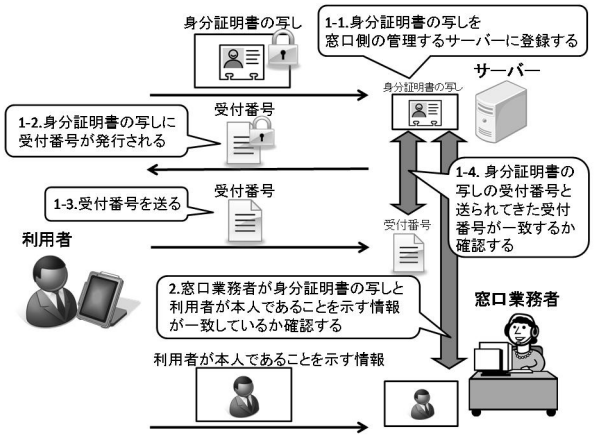

図 2 一般の窓口業務の手順に対応するオンライン窓口での手順

Fig. 2 Step of identity verification at online teller window.

窓口業務者は，利用者が身分証明書の写しをアップロードした人物であることは確認できるが，確かに身分証明書の人物であるかはわからない．そこで，オンライン窓口を実現するには，利用者が本人であることを示す情報を窓口業務者に送る方法を考えればよいことになる．また，ネットワークを介して機密性のあるデータを伝送するときは，通信セッションごとに異なるセッション鍵を用いて伝送するデータを暗号化する．そこで，窓口業務をネットワーク上で再現するには，直接利用者の本人確認をした上でセッション鍵の共有をすることになる．

3. 秘密情報を利用した認証鍵交換

従来，ネットワーク上で直接本人確認を行う方法はなく，ネットワーク上で通信相手が意図した相手であることを確認したいときには，本人しか知らないはずの秘密情報を所持していることを確認して認証し，これを間接的な本人確認としてきた．何らかの手段で通信相手を認証し，鍵を交換する方式は認証鍵交換と呼ばれている．AKE の代表的な方式として，認証にパスワードを用いる認証鍵交換(パスワードベース AKE)と，公開鍵基盤を用いる認証鍵交換(PKI ベース AKE)がある．

3.1 パスワードベース AKE

パスワードベース AKE として ISO-9798-2 で標準化されている共通鍵暗号技術を用いたエンティティ認証技術[4]を利用したものがある．この認証方式では，第三者に知られないように事前共有した共通鍵を所有していることを証明することにより認証が実現される．パスワードによる認証により示すことができるのは，証明者がパスワード(秘密情報)を持っていることのみである．そのためパスワードによる通信相手の本人確認を行うためには，送受信者でパスワードを共有する際に，事前に対面で本人確認をしなければならない．このことはオンライン窓口を実現する手順と矛盾するものである．よって，パスワードベース AKE はオンライン窓口業務での本人確認には適さない．

3.2 PKI ベース AKE

PKI ベース AKE として ISO-9798-3 で標準化されている電子署名技術を用いたエンティティ認証技術[5]を利用したものがある．この認証方式では，秘密情報である秘密鍵を所有していることを証明することにより認証が実現される．電子署名は公開鍵暗号を応用した技術である．公開鍵暗号を用いるときには，公開鍵と秘密鍵のペアを生成し，公開鍵のみを公開する．公開鍵の所有者がわからないとなりすましによる不正ができてしまうため，公開鍵暗号を安全に利用するには，第三者が発行した公開鍵が所有者本人のものであることを証明する公開鍵証明書が必要となる．PKI ベース AKE では，認証局(CA: Certificate Authority)により発行される公開鍵証明書を利用する．センシティブな情報を扱う場合の公開鍵証明書は一般にオフラインで本人確認をして発行される．信頼できる第三者である認証局がオフラインで本人確認を行ってから発行する公開鍵証明書を所有している個人はほとんどいない．公開鍵証明書の発行には，費用，手間などのコストが大きいからである．以上の状況や理由から，PKI ベース AKE もオンライン窓口業務での本人確認には適さない．

4. 認証者に紐付けられた対象物を利用した認証鍵交換

4.1 オブジェクトベース AKE

3 章で述べたパスワードベース AKE と PKI ベース AKE は，共に証明者しか持ち得ない秘密情報である認証のための鍵を所有していることを証明することにより認証を実現している．具体的には，秘密情報を知る者以外に生成できない本人証明のためのデータを生成し，通信相手である検証者がそれを確認している．証明者以外に生成できないデータを検証者に示し，検証者がそれを確認する，ということができれば認証を実現できる．

ここで，証明者以外に生成できない証明のためのデータとして，証明者に紐付けられた対象物の画像データを用いることを考える．例えば，対象物として証明者の顔や，証明者であることを特定できる所有物があげられる．検証者が，証明者に紐付けられた対象物を確認することで，直接的な本人確認をできるようになる．このことは，公開鍵暗号技術を用いた認証を行う際に必要である公開鍵証明書を発行する機関を始めとした第三者が仲介を行うことなく，直接的な本人確認を実現できるようになるということである．このような直接的な対象物による認証をしながらセッション鍵を共有する方式を**オブジェクトベース AKE** と呼ぶこととする．

なお，単に証明者に紐付けられた対象物の画像データと

Vol.2014-GN-90 No.21
Vol.2014-CDS-9 No.21
Vol.2014-DCC-6 No.21
2014/1/24

セッション鍵を同時に送るだけでは，セッション鍵と対象物の紐付けがないため，セッション鍵が証明者本人から送られてきたことを確認できない．そこで，画像データとセッション鍵の紐付けは 4.2 節で述べるステガノグラフィに着目し，5 章ではオブジェクトベース AKE の一構成法を与える．

4.2 ステガノグラフィとその利用

ステガノグラフィは埋め込みデータを密かに相手に伝えるために，第三者が一見して不自然に見えない冗長性のあるデータに対して他のデータを埋め込む技術である．図 3 にステガノグラフィのモデルを示す．

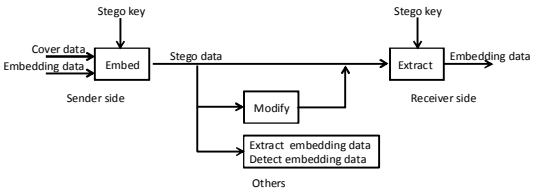

図 3 ステガノグラフィの秘匿通信モデル
Fig. 3 Model of steganography.

ステガノグラフィでは，隠したいデータのことを‘埋め込みデータ’, 埋め込みデータを隠すメディア(データ)のことを‘カバーデータ’, 埋め込みデータをカバーデータに隠して一体化したものを‘ステゴデータ’と呼ぶ．埋め込みデータとカバーデータからステゴデータを作成する操作を‘埋め込み’, ステゴデータとカバーデータから埋め込みデータを復元する操作を‘抽出’と呼ぶ．ステガノグラフィの埋め込み操作は，埋め込みデータをカバーデータと結合しており，抽出操作は結びついたデータを分離するものである．

ステガノグラフィの方式を非公開にしておき，方式を知っている者だけが埋め込みと抽出を行えるとする考え方がある[6]．しかし，採用している方式が知られてしまうと．もうその方式は使えなくなってしまうため，通常は埋め込み鍵と抽出鍵を用意する．埋め込み鍵が使える場合には埋め込みができ，抽出鍵が使える場合には抽出ができる，という方式を導入することが多い[6]．埋め込み鍵と抽出鍵を総称して，‘ステゴ鍵’という．

このように，一般的なステガノグラフィは情報が伝送されていること自体を隠すことを主目的にした情報ハイディング技術であるが，カバーデータに情報が埋め込まれていることを前提に応用した研究が数多く行われている[3]．画像[7]や，文字認識[8]，音声[9]への応用が試みられており，これらは埋め込みデータとカバーデータの 2 つを組み合わせることを目的にステガノグラフィ技術を用いている．

これらの研究と同様に本稿でも，ステガノグラフィ技術を，画像データと共有データを紐付ける目的で応用する．カバーデータを受信者が送信者を確認できるデータとし，埋め込みデータをセッション鍵とすることで，送信側でセッション鍵と送信者を結びつけることができる．そして受信側でセッション鍵と送信者を確認できるデータを分離し，送信者の確認ができる．以上のようなステガノグラフィを用いたセッション鍵共有が実現できれば，相手の顔を見ながら通信し，第三者を介することなくセッション鍵を共有できる．

5. オブジェクトベース AKE の一構成法：ステガノグラフィを用いた第三者の仲介不要なセッション鍵共有方式

受信者が送信者に紐付けられた対象物を直接確認し，第三者を仲介せず送信者の本人確認ができるセッション鍵共有方式を提案する．提案方式を図 4 に示す．送信者が操作する送り元デバイス，受信者が操作するあて先デバイスには，小型カメラ・マイクと通信インターフェースが搭載されているものとする．本方式は，ステゴ鍵共有フェーズ，連続静止画取得フェーズ, セッション鍵埋め込みフェーズ, セッション鍵抽出フェーズの 4 つのフェーズから成り，これらを順に実行することにより認証鍵交換を実現する．

(1) ステゴ鍵共有フェーズ … 送り元デバイスとあて先デバイスの間で，Diffie-Hellman(DH)鍵共有法[10]に従い，ステゴデータの作成，埋め込みデータの抽出の際に使用するステゴ鍵を共有する．

(2) 連続静止画取得フェーズ … 送り元デバイスでステゴ鍵から何らかの計算をして動作指示を作成し，送信者にそれを提示する．送信者は指示に応じたアクションをカメラ前で行い，その様子を連続静止画として記録する．

(3) セッション鍵埋め込みフェーズ … 連続静止画をカバーデータとみなして，連続する画像 1 枚 1 枚に，静止画向け空間領域ステガノグラフィに従い，ステゴ鍵を用いて送りたいセッション鍵を埋め込み，ステゴデータを作成し，これをあて先デバイスに送る．

(4) セッション鍵抽出フェーズ … 送信者が映った連続静止画を見て，ステゴ鍵から生成した動作指示と送信者のアクションが一致するか，送信者が誰かを受

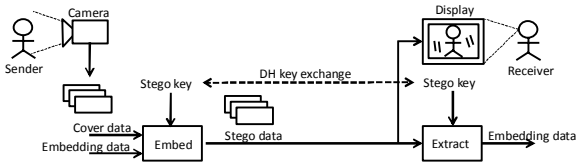

図 4 提案する第三者の仲介不要な認証付き
セッション鍵共有のモデル
Fig. 4 Model of the authenticated key exchange without third party.

Vol.2014-GN-90 No.21
Vol.2014-CDS-9 No.21
Vol.2014-DCC-6 No.21
2014/1/24

信者が確認する．これと平行して，ステゴデータである連続静止画とステゴ鍵から静止画向け空間領域ステガノグラフィに従い埋め込みデータを抽出する．最終的に送信者が送りたかったセッション鍵が埋め込みデータとして受信者側に全て届き，その間に送信者が本人であると受信者が判断したら受信したセッション鍵を受理する．

(3)と(4)では，連続静止画に対するセッション鍵の埋め込みを高速に実行できるようにするために，静止画のピクセルを直接変更する空間領域ステガノグラフィを使用するものとする．オリジナルの静止画(カバーデータ)に比べて，ステゴデータの品質が劣化したことが人間に知覚されないように，セッション鍵を埋め込む強度を調整する．

データ伝送の観点では，通信経路上のノイズによるステゴデータの変化，欠落や，第三者によるステゴデータの偽造や改ざんを検出することが求められる．これについては埋め込みデータに送信したいセッション鍵のダイジェスト，フラグメント情報を含めることで検出する．

送信者を写した連続静止画と，伝送データを結びつけるという観点では，連続静止画とステゴ鍵すなわち当該のセッション鍵共有のための一連の通信の関連付けが重要である．そこで(2)では，ステゴ鍵を共有した後で，送り元デバイスで送信者にステゴ鍵のダイジェストから何らかの計算をして生成した指示を提示し，送信者がカメラ前でこれに応じたアクションをとることとしている．

ステゴ鍵のダイジェストに対する送信者のアクションとしては，例えば，送信者にダイジェストの値を 1 桁ずつ提示して送信者に空中に指先で数字を描かせる，送信者にダイジェストの値から上下左右前後の指示を生成し，それに応じて身体の一部を動かしてもらうといったことが考えられる．受信者は，送信者が映った連続静止画を見て，ステゴ鍵のダイジェストに送信者のアクションが応じているかを確認し，そして送信者が誰かを確認した後で，送信されたデータを受理する．他にも送信者の本人確認の精度を高めるために，連続静止画と併せて，本人の音声も記録して，受信者に確認させることがオプションとして考えられる．

本方式は送受信者間において，受信者が送信者を示す連続静止画を確認し，直接本人確認を行うことで，第三者の仲介不要なセッション鍵共有を実現している．

6. 考察

6.1 DH 鍵共有法の中間者攻撃について

提案方式では，セッション鍵の送信者を識別できる情報としてカバーデータを作成し，それと紐付けするかたちで送信したいセッション鍵を埋め込み，ステゴデータを作成している．ここで，正規の送信者の映像を持った第三者がステゴ鍵を不正に入手し，正規の送信者になりすましてセッション鍵を送る行為について考える．DH 鍵共有法[10]には正規の送信者と受信者の間に介在して両者になりすますことにより，正規の送信者,受信者に対して，それぞれ異なる偽の鍵を共有させる中間者攻撃が可能であり，これに対処しなければ,送信者とセッション鍵の紐付けの関係が崩れて，上記のようなことができてしまう．

提案方式では，連続静止画取得フェーズにおいて，DH 鍵共有法[10]により共有されたステゴ鍵のダイジェストが,送信者のアクションというかたちで連続静止画に含まれることから，受信者によって当該セッション鍵を伝送する一連の通信のステゴ鍵が正しく使われているかどうかを確認できるようになっている．これは，中間者攻撃の攻撃者はランダムに変化するステゴ鍵に合った送信者のアクションが記録された映像を作り出すことが困難であることを前提とした攻撃の検出方法である．

6.2 ステゴデータの盗聴について

提案方式では，ステゴデータそのものは秘匿されていない．ここで，通信を盗聴するなどして，送信者に連続静止画を作らせ，送信者のアクション映像を複数パターン収集する行為について考える．送信者のアクションの映像を多数蓄積すると，映像を繋ぎ変えて任意のアクションを含んだ連続静止画像を作ることで，先に考察したような，なりすまし行為の検出をすり抜けることが懸念される．この対処として，セッション鍵埋め込みフェーズにおけるステゴデータの暗号化が挙げられる．ステゴデータの暗号化には AES などの共通鍵暗号を用い，その鍵は受信者の公開鍵で暗号化して,事前に送信者から受信者に渡しておけばよい．

7. 評価

提案方式において，受信者は送られてきた送信者を示す連続静止画を確認することによって，直接送信者の本人確認をする．連続静止画の表示品質が悪いと，通信相手本人であるのか，なりすましであるのかを正しく識別できない恐れがある．本人確認を正しく行うには，安定して受信側で表示を続けなければならない．

本章では，連続静止画による本人確認が正しく行われるかを評価するために，提案方式のプログラムを試作した．試作したプログラムの基本性能としてステゴ画像の平均 PSNR(dB)，ステゴ画像の受信速度を測定する．さらに，本人確認が正しく行われるかをユーザ実験により評価する．

7.1 試作した評価用プログラム

連続静止画による本人確認の観点では，安定して受信側で表示を続けなければならない．ここでは提案方式の初期段階の評価として，提案するセッション鍵共有方式の基本性能について，遅延とそのゆらぎに対応する機能を省いたシンプルな評価用プログラムを試作して確認する．

Vol.2014-GN-90 No.21
Vol.2014-CDS-9 No.21
Vol.2014-DCC-6 No.21
2014/1/24

評価用プログラムは，利用する場面にオンライン窓口を想定し，送り元デバイスは利用者としてスマートデバイスの上で，宛先デバイスは窓口業務者として PC の上で動作するよう作成した．それぞれの利用デバイスはマイクと Web カメラを備えたものを想定している．また，初期段階の評価用プログラムであるため，通信インターフェースには遅延と揺らぎが小さい LAN インターフェースを介してネットワーク接続している．データの送り元のスマートデバイスには，ステゴ鍵共有，連続静止画取得，セッション鍵埋め込み，セッション鍵生成の機能を実装したクライアントプログラム(C)を動作させる．データのあて先の PC には，ステゴ鍵共有，連続静止画取得，埋め込みデータ抽出の機能を実装したサーバプログラム(S)を動作させる．なお，提案方式において送信者の本人確認をするためには，受信者を示す連続静止画は不要だが，窓口業務での利用を考え，C にも S がカメラで取得した連続静止画が単に表示だけされるようにしている．簡単のため評価用プログラムの動作説明からは省いている．

図 5 に示した作成した評価用プログラムは以下のように動作する．

(1) ステゴ鍵共有フェーズ

Step1-1 C と S は，DH 鍵共有法に従い，ステゴ鍵 k を共有する．

Step1-2 S は，k を一方向性ハッシュ関数 h()に入力し，ダイジェスト d_k =h(k) を計算，そして時刻 t_k を取得して，k, d_k, t_k を保管する．

Step1-3 C は，同様に k から d_k を計算して，k, d_k を保管する．

送信者は，C を操作して，伝送したいセッション鍵 m を与える．C と S は，m を分割した $m_{(i)}$, i=1, 2,…, N に対して以下の(2)～(4)の手順を繰り返す．

(2) 連続静止画取得フェーズ

Step2-1 C は，送信者に対して，d_k の値を提示する．

Step2-2 送信者は，d_k の値に従い，カメラ前でアクションをとる．

Step2-3 C は，送信者をカメラで撮影し，連続静止画（カバーデータ）$cov_{(i)}$を保管する．

(3) セッション鍵埋め込みフェーズ

Step3-1 C は，分割されたセッション鍵のダイジェスト $d_{m(i)}$=h($i \parallel N \parallel m_{(i)}$)を計算，埋め込みデータ $emb_{(i)}$={i, N, $m_{(i)}$, $d_{m(i)}$}を構成する．

Step3-2 C は，k を用いてステゴデータ $ste_{(i)}$= A_{emb}($cov_{(i)}$, $emb_{(i)}$, k, p)を作成して，これを S へ送る．ここで，A_{emb}() は埋め込みアルゴリズムで，p は埋め込み処理の固有パラメータとする．

Step3-3 S は，時刻 $t_{s(i)}$を取得して，$t_{s(i)}$ - t_k < ε の場合，受け取った $ste_{(i)}$と $t_{s(i)}$を保管する．これ以外の場合，S は処理を中断する．

(4) セッション鍵抽出フェーズ

Step4-1 S は，k を用いて埋め込みデータ $emb_{(i)}$=A_{ext}($ste_{(i)}$, k, p)を抽出し，その中の i, N, $m_{(i)}$が完全かどうか h($i \parallel N \parallel m_{(i)}$)==$d_{m(i)}$により確認する．$A_{ext}$() は抽出アルゴリズムである．$i$, N, $m_{(i)}$が完全である場合，分割されたセッション鍵 $m_{(i)}$を保管する．それ以外の場合，S は手続きを中断する．

Step4-2 受信者は，S を操作して，$ste_{(i)}$, i=1, 2,…を再生し，d_k と送信者のアクションが一致していることを確認するとともに，送信者の本人確認を行う．d_k と送信者のアクションが一致し，かつ送信者の本人確認ができたと判断すれば，保管されているセッション鍵 $m_{(i)}$, i=1, 2,…を受理する．それ以外の場合，処理を中断する．

C は Java 言語，Android API レベル 14(Android OS 4.0 以上で動作)，UDP ソケット通信により実装している．使用するスマートデバイスは ASUS 社製 Nexus7(2012), Android OS 4.4 としている．S は Java 言語，JDK7.0，Java MediaFramework2.1.1e，UDP ソケット通信により実装している．Web カメラは，HP HD Webcam を使用している．使用する PC は，OS を Windows7 Pro 64bit，メモリを 8GB, CPU を Intel Core i5 3210M 2.5GHz, NIC を Realtek PCIe GBE Family Controller としている．

ステゴ鍵のダイジェストに対する送信者のアクションは，ダイジェストの値から上下左右の指示を生成し，それに応じて体の一部を動かしてもらう，という方法を想定して実装した．

全ての埋め込みデータをカバーデータに埋め込むため，埋め込みデータ $emb_{(i)}$, i=1,2,…, N, カバーデータの総ピクセル数 pixs に関して，R_{emb}・pixs >> | $emb_{(i)}$|, i=1,2,…,N を満たすように N, |$emb_{(i)}$|, p を設定する．R_{emb} は空間領域ステガノグラフィの手法に依存する埋め込みレートである．ステゴデータを作成する機能 A_{emb}()，埋め込みデータを抽出する機能 A_{ext}()は，静止画向け空間領域ステガノグラフィの一例として MBNS 法[11]を用いて，カバーデータであるカラー静止画を ppm 形式で取得し，その R 成分（256 階調）のピクセル値にデータを埋め込んでいる．なお，MBNS 法は，

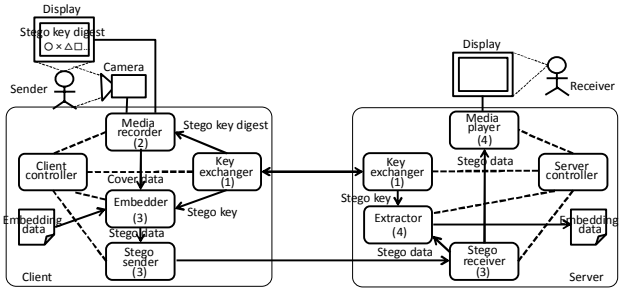

図 5 評価用プログラムの構成

Fig. 5 Construction of the evaluation software program.

埋め込みデータを複数の基底を用いて表現して，カバーデータであるグレイスケール画像のピクセル値に対して，隣接する 3 ピクセルの値の変化量により基底を定め，個々のピクセルに多基底表記されたデータシンボルを強度 p =1/Δで埋め込む手法である．

7.2 評価用プログラムの基本性能

ステガノグラフィを利用する際は，埋め込みデータの存在が人間に知覚されないようにすることが求められ，埋め込みデータサイズとカバーデータに対するステゴデータの品質劣化の割合により一般に性能が評価される．カバーデータに対するステゴデータの品質劣化の割合は，PSNR=10 $\log_{10}(256\text{-}1)^2$/MSE, MSE=1/($h$・$w$) Σ_i Σ_j ($P(i,j)$ - $P'(i,j)$)^2（縦 h ピクセル，横 w ピクセルの 256 階調グレイスケール画像の場合）により評価し，この値が大きいほどステゴデータに含まれるノイズが少ないことを意味している．PSNR が 36dB 以上のとき，人間にはカバーデータとの差が知覚されないと言われている[12].

提案するセッション鍵方式は，連続静止画に対してセッション鍵を埋め込み，これを送信して，あて先で埋め込まれたセッション鍵の抽出を行うことから，その評価においては，N 枚の ppm 形式カラー静止画（縦 h ピクセル，横 w ピクセル）へ，長さ L ビットのセッション鍵を分割して，埋め込み強度 1/Δで埋め込み，あて先へ UDP 送信したときのステゴ画像 R 成分の平均 PSNR(dB)とステゴ画像の受信速度(枚/sec)を求める．

スマートデバイスと PC 間はルータを介して IEEE802.11n(リンク速度 65Mbps)の無線 LAN インターフェースと 1000Base-T の有線 LAN インターフェースで対向接続している．画像一枚に対する埋め込みデータサイズ $|emb_{(i)}|$=19byte($|i|$=1byte,$|N|$=1byte,$|m_{(i)}|$=1byte,$|d_{m(i)}|$=16byte) を設定し，画像サイズは 160x120 と 240x180 の 2 通りとし，共有するセッション鍵のサイズは 256bit とした．画像サイズが 240x180 の場合，画像 1 枚のデータサイズは $240 * 180 * 3 = 1.296 * 10^5$byte であり，画像 1 枚につき 19byte のデータを埋め込んでいる．一般に利用されるセッション鍵の長さは高々256bit であり，最小の 1bit ずつ分割した場合の分割後の数は 256 個であるため，i と N を表現するヘッダサイズはそれぞれ 1byte としている．セッション鍵の分割後のサイズは 1～8bit の範囲で調整できるようになっており，これを変更することでセッション鍵を埋め込む連続静止画の枚数を指定し，セッション鍵の共有に要する時間を調節できるようにしている．本測定ではセッション鍵の分割後のサイズを 2bit としている. なお，Step4-2 の動作と本人性の目視による確認は計測対象に直接は関係がないために操作を省略して計測している．

表 1 ppm 形式 160x120, 240x180 静止画を用いたときの平均 PSNR(dB)，ステゴ画像の受信速度(枚/sec) (N=256, L=256, 1/Δ=2.0 のとき)

Table 1 Average PSNR(dB) and receiving speed of the stego images(frame/sec) for 160x120 and 240x180 ppm images (N=256, L=256, 1/⊿=2.0).

画像サイズ	ステゴ画像の 平均 PSNR (dB)	ステゴ画像の 受信速度(枚/sec)
160x120	59.7	17.1
240x180	63.5	11.1

30 回計測した結果を表 1 に示す. 画像サイズ毎のステゴ画像の平均 PSNR，受信速度の結果から，作成されたステゴデータは，人間が知覚できないレベル 36dB 以上となっておりカバーデータとステゴ画像の差異は小さく，ステゴ画像の受信速度も 10 枚/sec 程度であり，256bit セッション鍵の共有に要した時間は 10 秒程度であった. これは送信者の本人確認に使用できるものと考えている．

また，本方式はステゴ鍵共有フェーズにおいて，ステゴ鍵を共有する際の中間者攻撃を許容している．仮に攻撃されステゴ鍵が漏れたとしても，連続静止画による本人確認により，攻撃者が偽のセッション鍵を共有させることができないようにしている．実装したプログラムにおいて，セッション鍵を埋め込む静止画の枚数が極端に少ないと，受信者が，ステゴ鍵を持つ攻撃者から偽のセッション鍵を埋め込んだ静止画を受け取っても，それに気付かず，後に送られてきた正当な送信者の連続静止画により本人確認をして，偽のセッション鍵を誤って受理してしまうことが懸念される．この対処として，セッション鍵を埋め込む連続静止画の枚数は本人確認ができる程度に長くすることが挙げられる．

7.3 ユーザ実験

試作した評価用プログラムを使い，攻撃者のなりすましに気付くことができるかを以下の手順で評価した．

被験者は 22 歳～25 歳の 20 人であり，オンライン窓口における窓口業務者の立場で参加した. 被験者は 1 人ずつ PC を使ってセッション鍵を共有する利用者の本人確認の際に，なりすましがあったか，なかったかを判断してもらった. 利用者は被験者とは別の男性 1 名, 女性 1 名である. まず，通常の通信相手の連続静止画を見せて，なりすましかどうか判断してもらい，次になりすましの連続静止画を見せ，再び判断してもらった．この手順を利用者それぞれに対して行った. 被験者は上下左右の 4 通りの動作指示を使用し，それに対する利用者側の動作を見て，なりすましかどうかを判断する．被験者が見ている連続静止画が，実際に通信相手とやりとりをしているものなのか，攻撃者のなりすましであるかは事前に伝えていない．この実験におけるなりすましとは，連続静止画が攻撃者によって録画映像にすり

変えられていることである．

実験結果を表 2 に示す．被験者 20 人中 19 人が攻撃者のなりすましがあるときとそうでないときを正しく見分けることができた．被験者の 1 名が男性の利用者の録画映像に対して，なりすましでないと答えた．これは録画映像での男性の動作が，被験者の出した動作指示と一致したからである．なりすましかどうかの判断を誤らない具体的な方法が必要であることが確認できた．

表 2 評価用システムを用いたユーザ実験の結果
Table 2 Result of user experiment using the system for evaluations.

		男性の利用者	
		利用者の録画映像	利用者の連続静止画
ユーザの判断	なりすましである	19 人	1 人
	なりすましでない	1 人	19 人
		女性の利用者	
		利用者の録画映像	利用者の連続静止画
	なりすましである	20 人	0 人
	なりすましでない	0 人	20 人

8. おわりに

本人確認が必要な手続きでは，基本的には本人が窓口に出向いて行うことが本人確認の有効性を担保することになる．しかし，ネットワーク上のサービスでは窓口に出向いて手続きできないため，インターネットオークションなど金品を取り扱うサービスであっても，本人確認書類を郵送するなど簡易的な手続きが行われており，取引相手の本人確認の有効性が十分に担保されていないことに懸念する声がある．サービスの窓口業務をネットワーク上で実現できれば，安心して金品などの個人取引を行える付加価値がサービスに与えられるようになる．

本稿では，まず，窓口業務で一般的に行われている手順と同じ手順をネットワーク上で行うには，直接利用者の本人確認をした上で，セッション鍵の共有をしなければならないことを述べた．そして，オブジェクトベース AKE という対象物を利用する認証鍵交換の概念を示し，その具体的な構成法としてステガノグラフィを用いた第三者の仲介不要なセッション鍵共有方式を提案した．カバーデータをカメラで撮影された利用者の連続静止画とし，埋め込みデータをセッション鍵とすることで，利用者の連続静止画とセッション鍵を紐付け，連続静止画による通信相手の直接的な本人確認を実現している．

提案方式を試作し，評価用環境においては画像サイズが 160x120 のときステゴ画像の平均 PSNR は 59.7dB，平均受信速度は 17.1 枚/sec，画像サイズが 240x180 のときステゴ画像の平均 PSNR は 63.5dB，平均受信速度は 11.1 枚/sec であることを確認した．そしてユーザ実験を行った結果，被験者 20 人中 19 人がなりすましかそうでないかを見分けることができた．実験結果から，提案方式がオブジェクトベース AKE として利用できる基本的な性能を備えられることを確認できた．

今後の課題として，提案方式を用いたアプリケーションの開発と，動作指示の種類を増やすなどしてなりすましを検出できるようにすることを挙げる．また，本稿では顔によるオブジェクトベース AKE の方式を提案したが，顔画像以外に有効なオブジェクトデータの検討も行っていく予定である．

参考文献

1) Yahoo!JAPAN : Yahoo!オークション 報告されているトラブルの例(オンライン)，入手先 <http://auctions.yahoo.co.jp/phtml/auc/jp/notice/instances/example.html>(参照 2013-12-19).
2) 山本太郎，植田広樹，関良明，高橋克己，小笠原盛浩，関谷直也，中村功，橋本良明：ネットショッピング・オークション利用に際する不安調査結果に対する一考察，コンピュータセキュリティシンポジウム 2012 論文集，Vol.2012，No.3，pp.547-554(2012).
3) 新見道治：情報ハイディングの現状と展望，電子情報通信学会論文誌 A，Vol.J93-A，No.2，pp.52-61(2010).
4) ISO/IEC 9798-2，Information technology - Security techniques - Entity authentication-Part2:Mechanisms using symmetric encipherment algorithms.
5) ISO/IEC 9798-3，Information technology - Security techniques - Entity authentication-Part3:Mechanisms using digital signature techniques.
6) 松本勉，"インフォメーションハイディングの概要，" 情報処理学会誌，vol.44，no.3，pp.227-235(2003).
7) 杉本修，川田亮一，小池淳，松本修一：不可視マーカ信号埋込による自動客観画質評価方式，電子情報通信学会論文誌 D-II，Vol.J88-D-II，No.6，pp.1012-1023(2005).
8) 大町真一郎，岩村雅一，内田誠一，黄瀬浩一：実環境文字認識のための面積比による付加情報埋込，電子情報通信学会論文誌 D，Vol.J90-D，No.12，pp.3246-3256(2007).
9) 片岡章俊，森岳至，林伸二：補助情報を用いた G.711 の広帯域化，電子情報通信学会論文誌 D，Vol.J91-D，No.4，pp.1069-1081(2008).
10) Diffie, W. and Hellman, M.: New Directions in Cryptography., *IEEE Trans. Information Theory*, Vol.22, No.6, pp.644-654(1976).
11) Zhang, X. and Wang, S.: Steganography Using Multiple-Base Notational System and Human Vision Sensitivity, *IEEE Signal Processing Letters*, Vol.12, No.1, pp.67-70(2005).
12) Wu, N.,I., Wang, C.,M., and Hwang, M.,S.: Data Hiding: Current Status and Key Issues, *International Journal of Network Security*, Vol.4, No.1, pp.1-9(2007).