視聴覚メディアによる即時認証機能を付加した鍵交換方式

磯部光平[†1]　毛利公美[†2]　白石善明[†3]　岩田彰[†1]

ネットワーク上で内容を秘匿してデータをやりとりするにはデータを暗号化する．暗号化には，通信を行う二者間で相手を確認した上で暗号化に用いるセッション鍵を共有する．第三者が発行する電子証明書を用いたセッション鍵の共有は，相手の面識の有無を問わず行えるが，電子証明書の発行に不正や過失があった場合には有効に機能しない．面識がある相手との対面では，相手の顔や声などの特徴を認識して，相手を確認している．本稿では，面識のある相手とネットワーク上で第三者の仲介なしに相手の顔や声などの特徴を直接確認し，セッション鍵を共有する方式を提案する．提案方式では，人の顔や声などの特徴を取り込むためにカメラやマイクなどが搭載されたデバイスを用い，両者が互いに相手の特徴を確認することで相手を認識し，それと同時に DH 鍵共有を行う．提案方式を用いた暗号化ファイル送受信システムの構成例についても述べている．

Key Exchange Scheme with Instant Authentication Function by Audiovisual

KOHEI ISOBE[†1]　MASAMI MOHRI[†2]　YOSHIAKI SHIRAISHI[†3]
AKIRA IWATA[†1]

1. はじめに

ネットワーク上で内容を秘匿した状態でファイルをやりとりする場合，ファイルを暗号化する．暗号化をするには，通信を行う二者間で暗号化に用いるセッション鍵（共通鍵）を共有する必要がある．セッション鍵が通信主体と紐づいていれば，暗号化によりファイルは送受信者の双方で正しく共有できる．ネットワークを介したセッション鍵の共有は，(1)鍵を共有しようとする相手が確かに意図した相手であるかを認証し，(2)セッション鍵を配送あるいは交換することによって行われる．

(1)の相手の認証は，信頼できる第三者の発行する電子証明書により行われる．電子証明書による認証では，面識がない相手であっても第三者の証明によって確認ができる．一方で，証明書を発行する第三者に過失や不正があると，認証が正しく機能しなくなってしまう．例えば，証明書を発行する認証局に対する攻撃[1]や認証局での誤った処理[2]により，不適切な証明書の発行が行われたことがある．面識がない相手ではなく，面識がある相手に対しては，対面であれば第三者を介さずに本人確認を行っている．ネットワーク上においても同様に本人確認を行うことができれば，第三者の証明を介さずに直接的に認証ができる．最近のパソコンやスマートフォン，タブレットなどのデバイスには，カメラやマイクなどの装置があらかじめ搭載されるようになってきており，これらのデバイスは相手を確認することに利用可能である．そして，(2)のセッション鍵の共有が，(1)の認証と同時にできれば，第三者の仲介なしに暗号化ファイル送受信が正しくできることになる．

本稿では，通信相手を直接確認しながら鍵共有する方式を提案し，それを用いた暗号化ファイル送受信システムの実装例を示す．以降，2 章ではネットワーク上での暗号通信とセッション鍵の共有について，3 章では提案方式，4 章では 3 章で提案した提案方式の実装例を示し，5 章でまとめる．

†1 名古屋工業大学
Nagoya Institute of Technology
†2 岐阜大学
Gifu University
†3 神戸大学
Kobe University

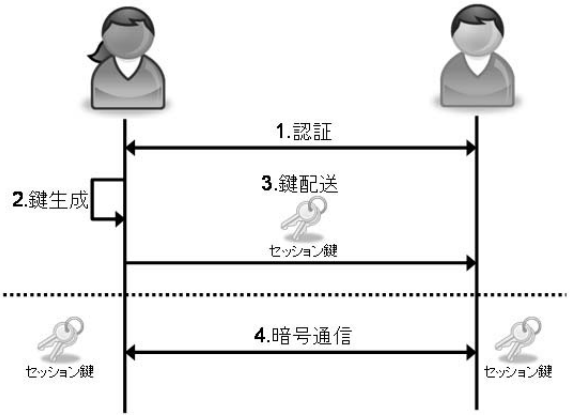

図 1 ネットワークを介したセッション鍵共有

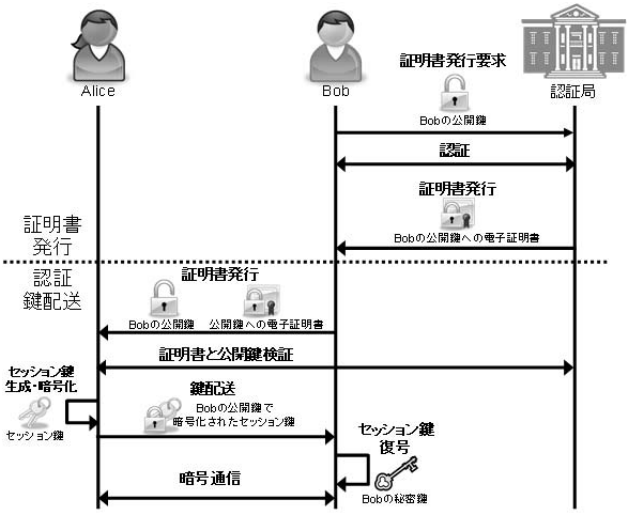

図 2 電子証明書を用いた認証鍵交換

2. ネットワーク上の暗号通信とセッション鍵共有

2.1 暗号通信

ネットワーク上で内容を秘匿して通信を行うには，通信内容を暗号化して送受信を行う．暗号化をするには，送信者と受信者間で暗号化に用いるセッション鍵を事前に共有する．送信者と受信者が暗号化に用いるセッション鍵を，鍵が両者それぞれに紐づく方法で共有することにより，送信者が自身に紐づくセッション鍵を用いて暗号化したデータを，受信者は自身に紐づいたセッション鍵を用いて復号することができる．ネットワークを介したセッション鍵の共有は，図 1 に示すようにセッション鍵を共有する相手が確かに意図した相手であるかを確認した上で，セッション鍵を配送または交換することで行われる．ネットワークを介して相手を認証した上で鍵共有を行うことを AKE(認証鍵交換)と呼ぶ.

認証鍵交換を実現する方式として第三者の発行する電子証明書を用いる方式がある．これを PKI ベース AKE[3]と呼ぶ．PKI ベース AKE を利用するにあたり，利用者は自身の公開鍵と秘密鍵を生成する．このとき，認証局は利用者を認証し，本人であると確認した上で電子証明書を発行する．認証鍵交換の流れを図 2 に示す．認証鍵交換を行う際に，利用者は自身の公開鍵と認証局から発行された電子証明書を相手へ送信する．公開鍵と電子証明書を受け取った相手は, 電子証明書が公開鍵に紐づいているものであり，かつ電子証明書が証明する人物を認証局に確認することで，公開鍵を検証する．検証の結果，意図する相手であった場合，認証に成功したことになり，鍵交換へと移る．暗号通信に用いるセッション鍵を生成し，検証に成功した公開鍵で暗号化して返送する．利用者は暗号化されたセッション鍵を自身の秘密鍵で復号し, セッション鍵を得る. 以上で，電子証明書を用いた認証鍵交換が行われる．セッション鍵は，利用者と紐づいた電子証明書が証明する公開鍵による暗号化を介して共有されるので，セッション鍵は両者に紐づいて共有されているといえる.

PKI ベース AKE では, 認証局が発行する電子証明書を基に相手を認証する．利用者は第三者である認証局の証明を信用して認証を行うため，第三者の仲介を経てセッション鍵の共有を行っているといえる．認証局が不正や過失などの理由から不適切な電子証明書の発行を行うと，電子証明書による証明が信用できなくなるため, PKI ベース AKE では認証が行えなくなってしまう．第三者の仲介なしに相手を認証し鍵交換が行えれば，第三者の不正や過失の影響を受けずに，いつでも当事者間でセッション鍵を共有し，暗号通信を行うことができるようになる.

2.2 第三者の仲介なしにセッション鍵を共有するアイデア

面識がある相手と対面する場合, 第三者の仲介を受けずに直接相手を本人と確認している. ネットワーク上でも同様に本人確認を行うことができれば, 第三者の仲介なしに認証を行うことができる. 面識がある相手と対面する場合, 相手の顔や声などの特徴を認識することで, 相手を本人だと確認している．ネットワークを介する場合でも，送信者と受信者の双方が互いの特徴を認識できれば, 直接本人確認が行える.

本人を確認しながら同時に鍵交換を行えば，第三者の仲介なしに認証鍵交換を行うことができることになる．鍵交換方式の一つに DH 鍵共有[4]がある． DH 鍵共有では，セッション鍵共有を行う二者がそれぞれ秘密鍵となる数をランダムに選択して自身の DH 公開鍵を生成し，その DH 公開鍵を相手に提示する．提示された相手の DH 公開鍵と自身の秘密鍵を用いて二者間で同じセッション鍵を共有することができる. 本人を確認しながら, その人が生成した DH 公開鍵を同時に提示することで，セッション鍵と人が紐づいた状態すなわち認証鍵交換を同時に行うことができる.

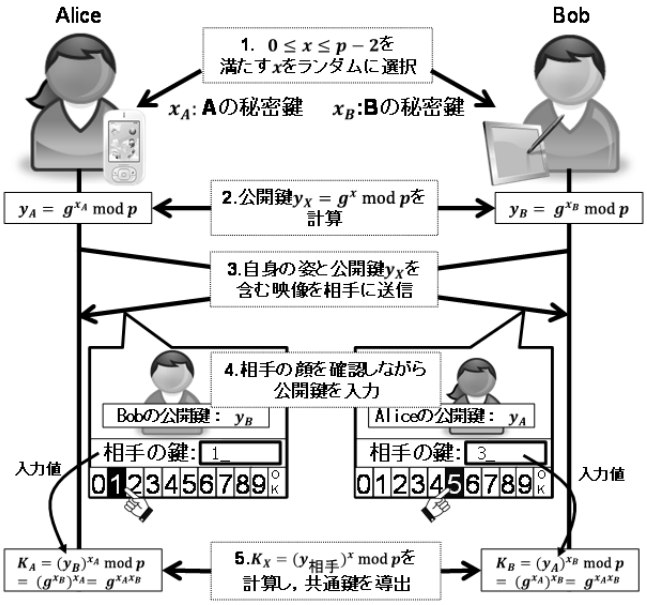

図 3 提案方式の概要

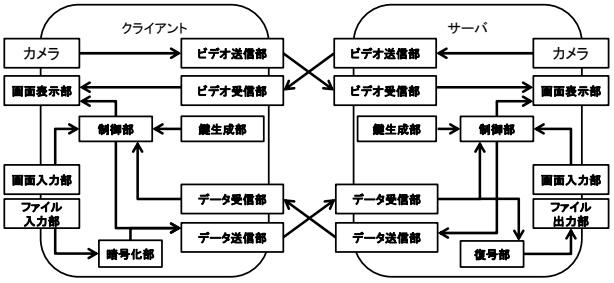

図 4 システムの構成

3. 提案方式 : 第三者の仲介不要なセッション鍵共有方式

通信相手を直接確認しながら DH 鍵共有を用いる認証鍵交換方式を提案する．提案方式の概要を図 3 に示す．提案方式においては，相手の特徴を認識することで本人確認を行うため，人物の特徴である顔や声などを取り込むことができるカメラやマイクが搭載されたデバイスを用いる．利用者は，自身と自身の鍵を同時にカメラに映し，相手へ提示する．一方，映像を提示された利用者は，映像から相手が意図した人物であることを確認し，相手が示す鍵を自身のデバイスに入力する．提案方式の手順を次に記す．

1. 送信者と受信者は，DH 鍵共有のパラメータである素数pに基づきそれぞれ乱数xを選択し，秘密鍵とする
2. 秘密鍵から DH 公開鍵y_Xを計算する．
   また，送信者と受信者はいずれも自身の DH 公開鍵y_xを紙などに書き，相手に提示できる状態にする
3. デバイスに搭載されたカメラに対し，自身の姿と公開鍵y_Xを同時に映して提示する
4. デバイスに表示される相手からの映像に意図した相手が映っていることを確認し，映像に同時に提示された DH 公開鍵をデバイスに入力する
5. デバイスは自身の秘密鍵xと，入力された相手の DH 公開鍵$y_{相手}$からセッション鍵である共通鍵Kを導出する

以上により認証鍵交換が行われる．提案方式では，相手のデバイスから送信された映像に映っている人物が，利用者が通信を行いたいと意図した人物であるかを利用者自身が確認するため，第三者の仲介なしに本人確認を行うことができる．また，DH 鍵共有を用いたセッション鍵の共有に必要となる相手方の DH 公開鍵は，相手の姿と共に映像に映っているため，人物と DH 公開鍵が紐付いていることを直感的に確認できる．したがって，セッション鍵の共有は人物に紐づいて行われており，本方式で共有したセッション鍵を用いて適切に暗号通信を行うことができる．

4. 実装

本章では，3 章の提案方式を用いて暗号通信路を確立し，ファイルを暗号化して送受信するシステムの構成例について述べる．実装したシステムの構成図を図 4 に示す．なお，このシステムではファイルの送信者が使うシステムをクライアントシステム，受信者が使うシステムをサーバシステムと呼ぶ．図 5 に示したシステムの動作の流れは次の通りである．

1. クライアント，サーバの両システムで秘密鍵となる乱数を選択し，公開鍵を生成する
2. 生成した DH 公開鍵をデバイスに表示し，利用者が自身の DH 公開鍵を確認できるようにする
3. クライアントシステム利用者は自身の顔などの姿をカメラに示したり，発言することで声をマイクに収録したりする．この際に，2.で表示されている DH 公開鍵を利用者のアクションによって同時に相手に示す．
4. クライアントシステムから送信された，姿や音声と，アクションによる公開鍵の提示を含む映像を受信したサーバシステム利用者は，姿や音声から通信を行いたい相手であることを確認した上で，アクションによって示される DH 公開鍵を自身のデバイスへ入力する
5. 手順 3 と 4 をクライアントとサーバを逆にした上で同様に行い，両者のデバイスで相手の DH 公開鍵の入力を終えた状態にする
6. 両者のデバイスは入力された DH 公開鍵と 1.で選択した秘密鍵からセッション鍵を求める
7. クライアントシステムでは，求めたセッション鍵を用いてファイルを暗号化し，サーバシステムへ送信する
8. クライアントシステムから送信された暗号化ファイ

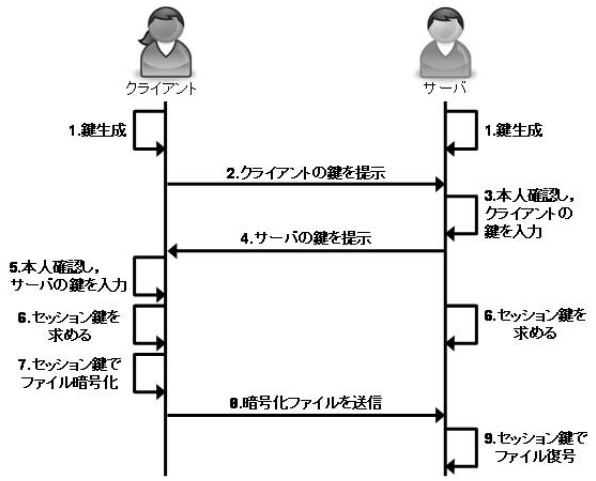

図 5 システムの動作の流れ

ルを受信したサーバシステムは，6.で得たセッション鍵を用いて復号する

以上により，第三者の仲介なしに相手を直接確認した上で，暗号化ファイルの送受信ができる．

鍵を示すアクションとして，3 章では DH 公開鍵を紙に書いて，その紙を映すという方法を例示した．これ以外にも鍵を示すアクションとして次のような方法が考えられる．なお，ここでは鍵を示すアクションを行うものを提示者，提示者のアクションを受け，自身のデバイスに鍵を入力するものを受理者と呼ぶことにする．

- 提示者は自身の公開鍵を声で一文字ずつ読み上げ，受理者は発声している人物が意図した相手であることを確認しながら自身のデバイスへ読み上げられた鍵を入力する
- 提示者は自身の鍵をポインティングデバイスやタッチパネルを用いてデバイスへ一文字ずつ書き，書いた文字を提示者が映る映像と合成し，受理者のデバイスへ送信する．受理者は，書き込みを行っている人物が意図した相手であることを確認しながら自身のデバイスへ映像に合成された鍵を入力する

いずれの方法も提示者が自らの動作により鍵を示す方法であり，かつ動作を行っている姿を確認することによって意図した人物と通信を行っていることを確認できる．アクションを通じて伝える鍵長が大きい場合，鍵の提示や入力に多くの時間がかかる．Biometric Word List[5]などを用いて鍵を別の英単語に置換して伝える方法や，音声認識や画像からの文字認識技術を利用し，受理者の鍵入力を支援することが考えられるが今後検討していく．

5. おわりに

本稿では，第三者の仲介なしに通信相手を直接確認しながら同時に鍵共有する方式と提案方式を用いた暗号化ファイル送受信の実装例について述べた．提案方式においては，認証に顔見知り間での顔や声などの特徴を確認する方法を用い，利用者の顔や声などの特徴と利用者の公開鍵を同時に提示することで，認証と鍵交換を同時に行えるようにした．

本稿では提案方式を用いた暗号化ファイル送受信システムの構成例を示したが，ユーザビリティという側面については評価できていない．相手を確認するという認証プロセスは直感的に行えるものの，鍵を確認し入力するという操作は 4 章で述べたとおり，いろいろな方法で実現可能である．これらを比較し，ユーザビリティに優れた暗号化ファイル伝送方式の提案については今後の課題としたい．

参考文献

[1]Adam Langley, Google Online Security Blog: Enhancing digital certificate security, Google Online Security Blog (online), available from<http://googleonlinesecurity.blogspot.jp/2013/01/enhancing-digital-certificate-security.html >(accessed 2014-05-16)

[2]独立行政法人情報処理推進機構，不正な電子証明書発行に関する問題について，情報処理推進機構（オンライン），入手先<http://www.ipa.go.jp/security/ciadr/vul/20110915-sslcert.html>(accessed 2014-05-16)

[3]ISO/IEC 9798-3, Information technology – Security techniques – Entity authentication-Part2: Mechanisms using digital signature techniques.

[4]W. Diffie and M. E. Hellman: “New Directions in Cryptography”, IEEE Transactions on Information Theory, vol.IT-22, No.6, pp.644-654, (1976).

[5]Juola, P.: Whole-word phonetic distances and the PGPfone alphabet, *Proc. of Fourth International Conference on Spoken Language Processing. ICSLP ’96*, pp.98-101 (1996)