特集論文

情報セキュリティソリューション“Mistyシリーズ”のラインアップと基盤技術

見市宏敏* Atsutoshi Miichi
大江哲浩* Akihiro Ooe
高丸祐典* Yuusuke Takamaru
吉田裕美* Hiromi Yoshida

Lineup of Information Security Solutions "Misty Series" and Base Technologies

要　旨

2020年からの新型コロナウイルス感染症(COVID-19)の拡大で社会は大きな変革を余儀なくされた。政府からの要請で広範囲にテレワークが実施され，法制度の改正とともに行政や企業の手続やサービスのデジタル化も進んでいるが，短期間に整備されたため多くの課題を残している。

課題の一つとして，運用やサービスの電子的なフローを早期に確立するための積極的なクラウドサービスの活用でのセキュリティ対策が挙げられる。

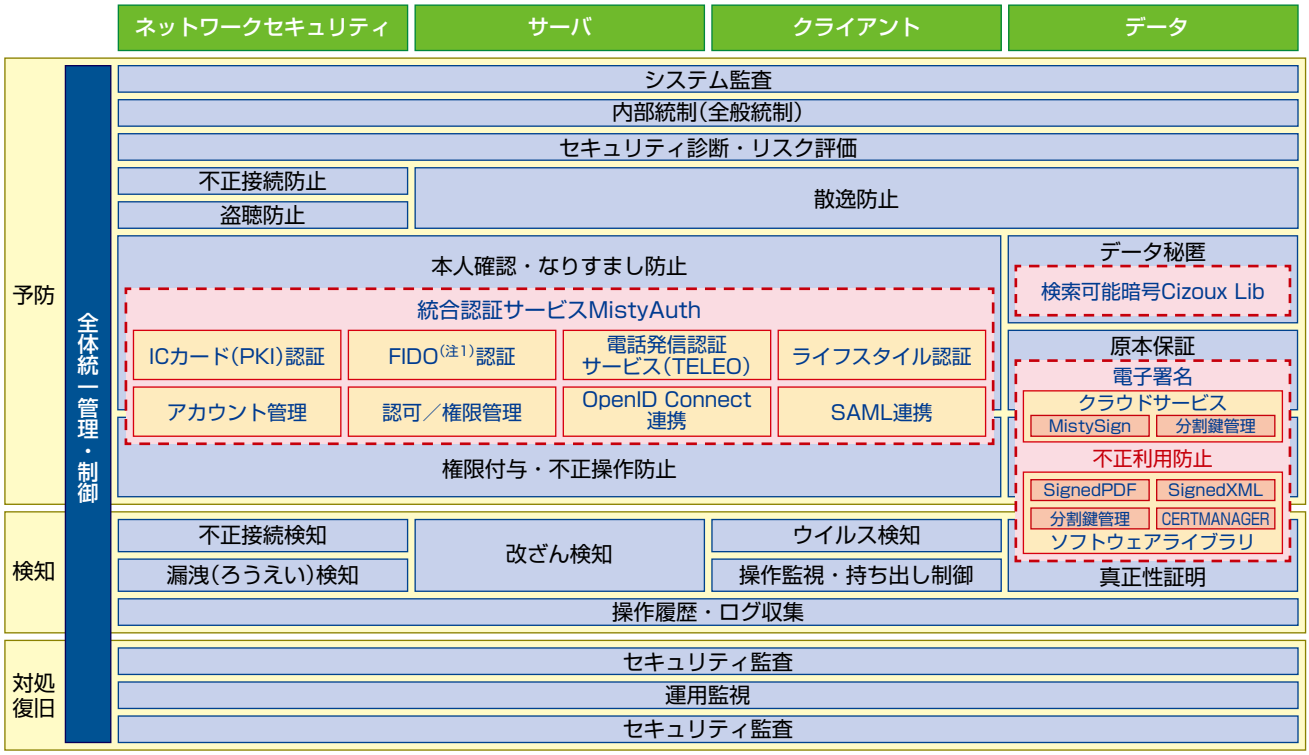
三菱電機インフォメーションシステムズ㈱(MDIS)は，1995年に三菱電機が開発した暗号アルゴリズム“MISTY”で培った技術を発展させた情報セキュリティソリューション“Mistyシリーズ”で，電子署名，統合認証サービス“MistyAuth”，検索可能暗号“Cizoux Lib”等のソリューションを提供する。

電子署名は公開鍵暗号基盤の技術でデータ・記録の真正性を担保し，クラウド上の電子署名での秘密鍵の取り扱いの安全性を分割鍵管理で確保している。

統合認証サービスは複数の多要素認証方式と認証基盤を組み合わせることで，様々なユースケースに対して厳格な本人認証の早期導入を可能にし，シングルサインオンで利便性も確保している。

検索可能暗号は暗号化した状態でのデータ利活用を実現することで，クラウド時代の情報の取り扱いの安全性と利便性を確保している。

MDISは，Mistyシリーズの拡充を通して安心・安全なデジタル化社会の実現に貢献していく。



(注1) FIDOは，Fido Alliance, Inc.の登録商標である。
SAML：Security Assertion Markup Language

情報セキュリティ対策マップでの“Mistyシリーズ”の適用領域

情報セキュリティ対策マップでの情報セキュリティソリューションMistyシリーズの適用領域(図の鎖線枠内)を示す。Mistyシリーズは統合認証サービスMistyAuth，検索可能暗号Cizoux Lib，電子署名等のソリューションを提供し，ネットワークセキュリティからデータの各層で予防・検知のプロセスのセキュリティ対策を広くカバーする。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

新型コロナウイルス感染症の拡大に伴う出社抑制の方策として大都市圏を中心に広範囲にテレワークが実施され，行政や企業の各種手続やサービスのデジタル化も進んでいるが，短期間での急速な整備となったため多くの課題を残している。

課題は，①タスクの進捗管理，労務管理，コミュニケーション希薄化等の業務上の課題，②積極的なクラウドサービスの活用でのセキュリティ上の課題，③インフラ整備のコストと運用等が挙げられる。

MDISは，今後も加速する各種手続やサービスのデジタル化とテレワークで鍵となるセキュリティ上の課題に対するソリューションをMistyシリーズで提供する。Mistyシリーズは，真正性証明，原本保証及び不正利用防止に対応する電子署名，本人認証・なりすまし防止と権限付与・不正操作防止に対応する統合認証サービスMistyAuth，データ秘匿に対応する検索可能暗号Cizoux Lib等から構成される。

本稿では，Mistyシリーズの電子署名，MistyAuth，Cizoux Libとそれらの基盤技術について述べる。

2. 電子署名

MDISは，電子文書の真正性を担保することを目的として，公開鍵と秘密鍵を利用する公開鍵暗号基盤(Public Key Infrastructure：PKI)の技術を用いて電子文書へ電子署名の付与と電子署名が付与された電子文書の検証を行うソフトウェアライブラリ製品と，同じ機能をクラウド上で行うサービスの，二つのソリューションを提供している。

2.1 ソフトウェアライブラリ“SignedPDF”／“SignedXML”

SignedPDFやSignedXMLは，PDF(Portable Document Format)やXML(eXtensible Markup Language)文書に対して電子署名，タイムスタンプ，長期署名の付与と検証を実施するソフトウェアライブラリである。PDF署名は国際標準規格PAdES(PDF Advanced Electronic Signatures)に準拠し，XML署名は国際標準規格XAdES(XML Advanced Electronic Signatures)に準拠している。どの規格も使用されている暗号アルゴリズムが破られたとしても電子的に署名された文書を長期間有効とする長期著名のプロファイルを規定しており，文書の真正性の担保が可能である。

ライブラリは様々な電子証明に対応しており，ICカード(マイナンバーカード(注2)，HPKI(ヘルスケアPKI)カード等)内に保管された電子証明書やクライアントのWindows(注3)証明書ストア内に保管された電子証明書を用いて電子署名を付与するクライアント署名，サーバ側に保管された電子証明書を用いて電子署名を付与するサーバ署名に加えて，ネットワーク経由でHSM(Hardware Security Module)も利用可能である。

ライブラリのインタフェースはWeb開発で幅広く使用されているJava(注4)で提供され，同一のサーバ上で複数の電子証明書を取り扱うことが可能なため，Webサービスや業務アプリケーションごとに電子証明書を使い分けるシステムの構築が容易になる(**図1**)。

MDISのPDF署名は，印影イメージやロゴを利用した可視署名にも対応している。

(注2) マイナンバーは，デジタル庁会計担当参事官の登録商標である。
(注3) Windowsは，Microsoft Corp.の登録商標である。
(注4) Javaは，Oracle America, Inc.の登録商標である。

2.2 クラウド電子署名“MistySign”

システムへの組み込みを想定したソフトウェアライブラリであるSignedPDF／SignedXMLに対し，電子署名の機能を様々な用途へ早期に導入できるようにするため，クラウド上に電子署名を行う環境を構築してサービスとして機能を提供している。

電子署名サービスは以下二つの提供形態を持つ。

(1) 簡易に利用を開始可能なGUI(Graphical User Interface)での提供

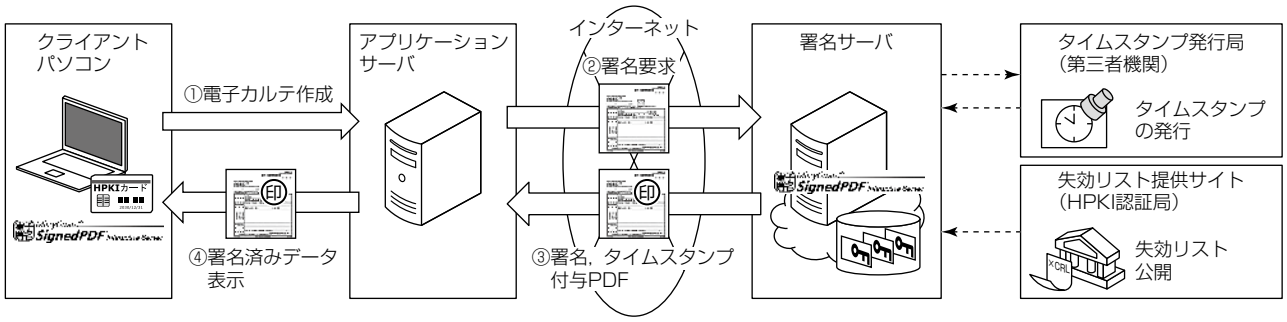


図1．電子署名サーバの構築例

⑵ 既存のシステムとの連携が容易なWeb API(Web Application Programming Interface)での提供

電子署名をクラウドで行うサービスでは，ユーザーの秘密鍵をサービス側で管理することになるため，セキュリティの高い鍵管理が必要である。このサービスでは次項で述べる分割鍵管理方式を採用している。

2.3 分割鍵管理[1]

MDISは，しきい値暗号の技術を用いて一つの秘密鍵を分割してクライアントとサーバの各々へ保管する方式を開発した。

秘密鍵として用いるには分割して保管された全ての情報が必要になる。MDISの分割鍵管理では，秘密鍵を必要とする演算をクライアントとサーバの各々で実施する。秘密鍵の情報が1か所に集約されることがなく，分割して保管された情報が同時に漏洩しない限り秘密鍵の安全性は保たれる。

秘密鍵を分割する際には任意の文字列をクライアントの秘密鍵として指定してサーバの秘密鍵を生成できるため，利用者が指定するパスワードを使用して分割鍵を運用することが可能になる。運用や利便性は従来の鍵管理と同等になり，HSM等を利用することなく，利便性を損なわずに低コストで安全性の高い鍵管理を実現する(**図2**)。

欧州のクラウド署名規格では，鍵生成や鍵利用のセキュリティ要件としてISO/IEC15408やFIPS 140-2を参照している。分割鍵管理の方式がこれらの要件に適用しているか評価した結果，鍵保管のハードウェアに関する要件以外は適応しており安全性も高い。

分割鍵管理の方式は，管理者の誤操作や不正操作による秘密鍵の漏洩への耐性も高く，サーバが攻撃を受けたことによる秘密鍵の漏洩への耐性はHSMを用いる鍵管理と同等である(**表1**)。

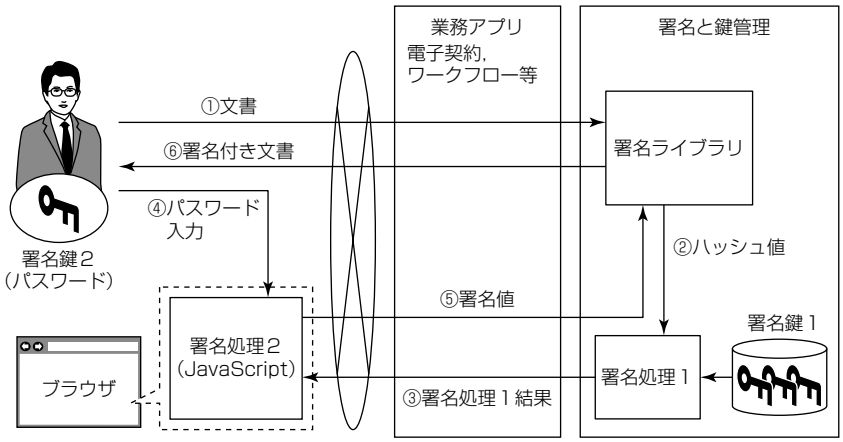


図2．分割鍵管理での署名方法

表1．分割鍵管理方式とHSM方式の比較

	分割鍵管理方式	HSM方式
漏洩リスク	○ 分割された情報全てそろわなければ漏洩しない	◎ 物理的に切り離されている
サーバへの攻撃に対するリスク	○ サーバに保管された情報だけでは利用できない	○ 物理的に切り離されている
管理者の誤操作・不正	○ サーバに保管された情報だけでは利用できない	× 管理者権限での操作には耐性はない
コスト	○ 1鍵　1,000円程度	△ 1鍵　2,000円程度

3．統合認証サービスMistyAuth[2]

B2B(Business to Business)，B2C(Business to Customer)を問わずWebサービスの広範囲な普及に伴い，個人認証での課題が顕在化している。例えば，認証用パスワードへのサイバー攻撃が増加しており，現実に被害が多数発生している。その対策として多要素認証の必要性が高まっているが，ユースケースやユーザー環境によって適切な認証方式が異なる。

また，認証の課題の一つとしてユーザーのアクセス権限管理も挙げられることが多いが，アクセス権限管理には複雑なシステム開発が必要になる。

このような認証での課題を解決するため，統合認証サービスMistyAuthでは複数の多要素認証方式とアクセス権限管理等の導入を容易にする認証基盤をサービスとして提供している(**図3**)。

3.1 多要素認証方式

MistyAuthでは次に示す複数の認証方式を提供する。これらの認証方式は任意に組み合わせて利用することが可能であり，様々なユースケースやユーザー環境に即した多要素認証を実現している(**表2**)。また，新技術を採用した特長ある認証技術を継続的に追加する予定である。

3.2 認証基盤

ID管理，アクセス権限管理等の認証基盤の機能がクラウド上で提供されるため，導入に多大な期間とコストを要する認証基盤を早期に利用可能になり，管理運用の負荷も軽減する。最近主流となりつつあるセキュリティ方針であるゼロトラストの重要な要素であるIAM(Identity and Access Management)を実現している(**表3**)。

表２．MistyAuthの提供する多要素認証(3) (4)

BASIC認証	ID，パスワードによる認証
FIDO認証	端末内での本人確認とPKIによるオンライン認証を組み合わせた認証 端末内での本人確認に生体認証が用いられることが多い
ICカード(PKI)認証	ICカード内に保存された電子証明書による認証
電話発信認証サービス TELEO	登録済み電話番号からの発信による認証
ライフスタイル認証(注5)	スマートフォンの位置情報等の行動履歴を蓄積し，現在の行動との一致度をAIが分析する認証(今後実装予定)

（注５） 東京大学とMDISなど民間企業４社が共同研究を行っているライフスタイル認証は，東京大学の登録商標である。

表３．MistyAuthの提供する認証基盤の機能

IAM	特定のリソースへ適切なユーザーがアクセス可能にする(アクセス権限管理)ためのポリシーとテクノロジーのフレームワーク
認可	特定のリソースへのアクセス権限を付与すること
SAML	ユーザーの認証情報，属性，権限の認可等の情報を連携することでシングルサインオンを実現する規格
OpenID Connect	権限認可の規格であるOAuth2.0を拡張した規格で，外部のOpenID Providerの提供するIDとの認証連携に利用されることもある

また，OpenID ConnectやSAMLの仕様への準拠によって，一度のログインで複数のサービスを利用できるシングルサインオンの機能も提供している。

3.3 適　用　例

MistyAuthは多要素認証と認証基盤をサービスとして提供するが個別に導入することも可能である。それぞれの事例を次に示す。

⑴ ライフスタイル認証で普段の行動と一致している場合は自動で認証し，普段と異なる行動が検出された場合は電話発信認証サービス“TELEO”で追加認証させる(多要素認証の組合せ利用)。

⑵ 自社やグループ会社が複数の顧客向けWebサービスを展開していて，同一ユーザーでもIDがサービスごとに異なる場合，MistyAuthの認証基盤内で各サービスのIDを統一IDに紐(ひも)づけてユーザーを管理し，ユーザーには統一IDの下にある一つのIDでの認証で全てのサービスへのシングルサインオンを提供する。

4．検索可能暗号Cizoux Lib

自治体や企業での業務システムのクラウド化が進む一方で，サイバー攻撃の巧妙化やクラウドサービス運用者からの情報流出対策の重要性が指摘されている。クラウドサービス上に機密情報を保管する際の情報漏洩対策の一つとしてデータの暗号化が挙げられるが，一度暗号化してしまうと利用する度に復号する必要がある等，安全性や利便性に欠ける点が課題である。

MDISは，データを暗号化した状態で検索が可能な技術“検索可能暗号”をWebシステムやクラウドサービス等に組み込めるソフトウェアライブラリ検索可能暗号Cizoux Libを提供している。これは，三菱電機 情報技術総合研究所が開発した“秘匿検索基盤ソフトウェア”の技術を基にMDISが製品化したものである。

4.1 特　　長

Cizoux Libの特長は，次のとおりである。**図４**にCizoux Libの検索処理イメージと特長を示す。

⑴ 暗号化したまま検索ができる“検索可能暗号”

Cizoux Libの検索処理は，データベース内の秘匿したい情報と検索キーワードを独自の“検索可能暗号”の技術で暗号化し，どちらも一切復号されず暗号化された状態で検索を行う。同一の文字列でも“検索可能暗号”で暗号化されたデータは異なるものとなるため，類推防止の効果も期待できる。

⑵ データベース上に鍵の保管が不要

一般的にデータベースの暗号化機能では，検索に際してデータベースの復号が行われる。この場合，復号に用いる鍵をデータベースからアクセス可能な環境に配置しておく必要があるため，データベースへのサイバー攻撃が発生した際には鍵も併せて漏洩する危険がある。

Cizoux Libは暗号化したまま検索し，検索結果も暗号

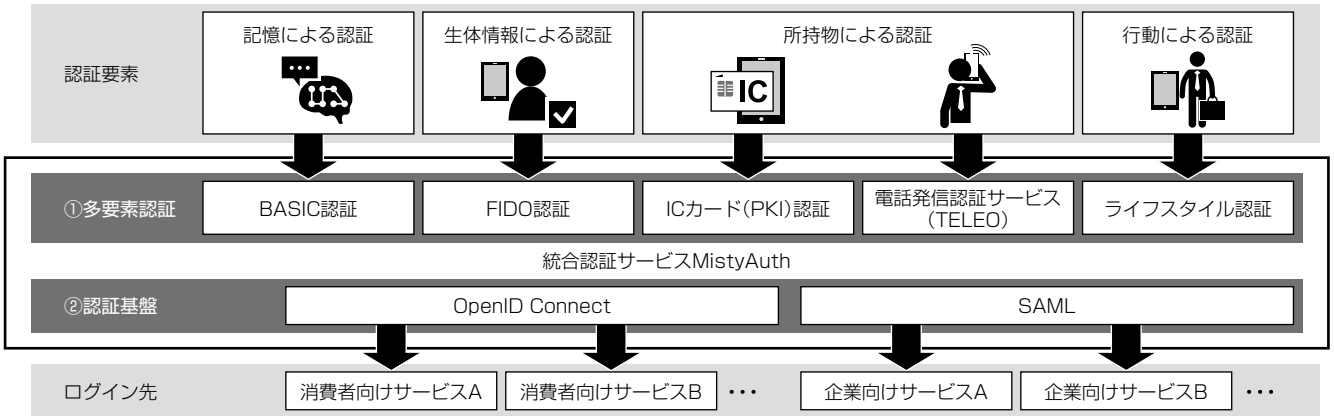


図３．MistyAuthの全体イメージ

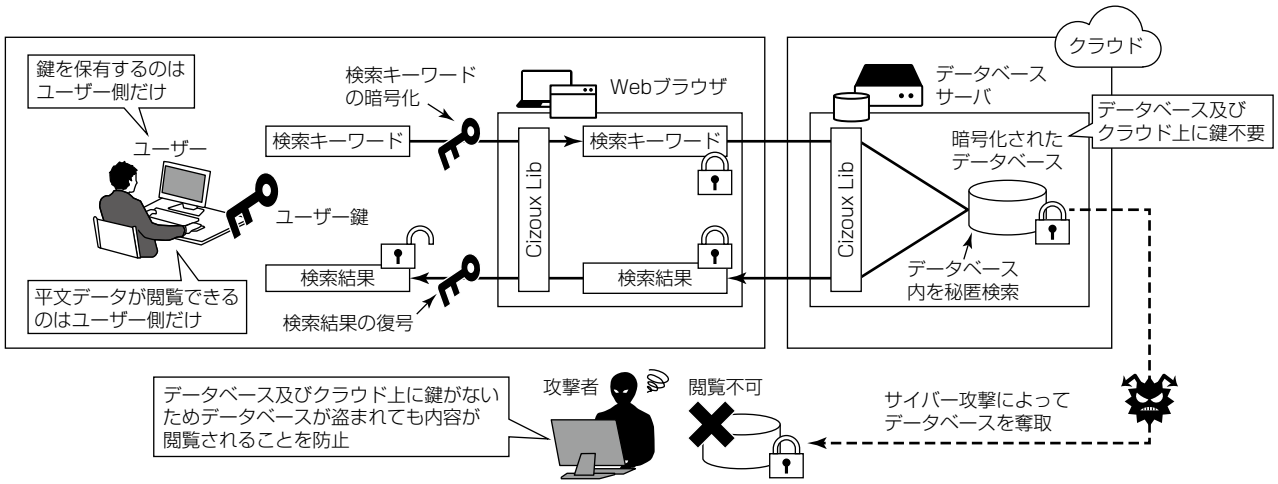


図4．Cizoux Libの検索処理イメージと特長

化された状態でクライアントへ送信されるため，データベース上に鍵を必要としない。

そのためデータベースの管理者でもアクセスが不可能な環境へ鍵を保管でき，データベースへの不正アクセスを受けた場合でも漏洩するデータは暗号化された状態で，復号に用いる鍵はデータベース上にないため，実質的な情報漏洩の防止を期待できる。

⑶　通信経路上のデータを常時暗号化

Cizoux Lib検索処理では，検索者が使用するクライアント上にだけ平文データが存在し，ネットワーク，クラウド上のデータは常時暗号化される。**4. 1. 2項**のデータベースへの不正アクセスに加え，通信データの傍受に対しても情報漏洩の防止の観点で有効である。

⑷　検索機能のバリエーション

Cizoux Libは完全一致検索，部分一致検索のほかに，前方一致検索，数値の範囲検索の機能も提供しており，用途に合わせて検索機能を選択して利用可能である。

4.2　適　用　例

Cizoux Libの特長から，クラウドサービスを利用して個人情報や機密情報，医療での機微な情報や臨床情報等を管理，利活用するシステムへの適用が考えられる。また，クラウドサービス事業者が提供するサービスの付加価値として，検索可能暗号化機能を搭載することも有用な適用例であると考える。

従来の情報漏洩対策は，いかに機密情報の漏洩を防止するかという観点にだけ重点が置かれてきた。サイバー攻撃が巧妙化して情報漏洩事件・事故が後を絶たない昨今では，攻撃によってデータが漏洩してしまうことを前提とした対策も並行して強化していく必要がある。

Cizoux Libは今後も性能の向上と機能の拡充を図りながら様々なユースケースへ対応していく。

5. む　す　び

新型コロナウイルス感染症の拡大を契機としたデジタル化促進，クラウド活用と人々の行動様式の変革は，今後も加速を続けると予想される。

MDISは，データ・記録の真正性の担保，クラウド利用での厳格な本人認証，シングルサインオンによる利便性向上，機密性の高いデータの保護等のセキュリティ技術を基に，Mistyシリーズのラインアップの拡充を図り，安心・安全なデジタル化社会の実現に貢献していく。

参　考　文　献

⑴　山中忠和，ほか：閾値署名を適用したリモート署名システムの安全性評価，コンピュータセキュリティシンポジウム2021論文集，514～521（2021）
https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=214470&item_no=1&page_id=13&block_id=8
⑵　三菱電機：セキュリティとユーザビリティの両立を実現するクラウド提供の統合認証サービス「MistyAuth」，ITソリューション総合サイト
https://www.MitsubishiElectric.co.jp/it/capability/technology_01/
⑶　大江哲浩，ほか：スマートフォン時代の個人認証技術，三菱電機技報，**94**，441～445（2020）
https://www.giho.MitsubishiElectric.co.jp/giho/pdf/2020/2008109.pdf
⑷　東京大学大学院情報理工学系研究科 ソーシャルICT研究センター：ライフスタイル認証による安全快適な社会の実現
http://www.sict.i.u-tokyo.ac.jp/research/lifestyle.html