講 座

《新連載》

映像情報メディア関連のセキュリティ［全12回］
開講にあたって

前論文部門委員長 小川一人

「*情報のセキュリティって必要だよね．でも，どうなっているのかわからないから，業者やお店で薦められたものを使っておこう．*」

そんな経験ありませんでしょうか．そして，

「*自分で判断できれば，どんな対策をすればよいか自分で選ぶけど・・・*(;-_-)」

というのが，みなさんの願いであり，本音ではないでしょうか．

皆様のこのような願望にお応えして，全12回にわたるセキュリティの講座を組むことにいたしました．映像情報に関わるセキュリティだけでなく，みなさんがお持ちの情報，どこかに預けてある情報，さらには，世の中に出回っている情報，もっと進めて，使用している機器，これから使用するであろう機器に対し，どんな危険があり，どんなセキュリティ対策技術があるのか．事例あり，対策技術あり，対策技術を培う基盤技術あり，どれをとってもおろそかにできないことばかりを第一線で活躍されている方々に講師になっていただき教えていただこうと思います．

「セキュリティって難しい」という先入観を払拭できるように，講師の方々にはできるだけ平易に教えていただくようにしております．ぜひ，この講座を継続して読んでいただき，セキュリティ技術を自分で選べるようになる，その第一歩にしていただければありがたく思います．また，適切なセキュリティ技術を導入することで，情報提供者も安心して情報を提供できるようになり，より多くの，リッチな情報が流通することになります．そして，ICT社会における皆様の生活を潤すことにもつながることを実感していただきたいと思います．

なお，本講座は，清水直樹編集理事，大久保英彦編集幹事と私小川が担当いたします．

12回にわたる長丁場ですが，お付き合いの程，よろしくお願い申し上げます．

予定目次（全12回）

（第1回）	著作権保護	山村千草（NHK）
（第2回）	ビッグデータの利活用とプライバシー保護の難しさ	山口利恵（東京大学）
（第3回）	SSL/TLSの仕組みを知っていますか？	神田雅透（NTT）
（第4回）	マルウェア対策	井上大介（情報通信研究機構）
（第5回）	パスワード	金岡　晃（東邦大学）
（第6回）	暗号技術（共通鍵暗号）	渡辺　大（日立製作所）
（第7回）	暗号技術（公開鍵暗号）	満保雅浩（金沢大学）
（第8回）	暗号技術（量子暗号）	鶴丸豊広（三菱電機）
（第9回）	電子透かし	栗林　稔（神戸大学）
（第10回）	バイオメトリクス	青木隆浩（富士通研究所）
（第11回）	モバイルセキュリティ	竹森敬祐（KDDI）
（第12回）	アプリケーションセキュリティ	渡辺　創（産業技術総合研究所）

講 座

映像情報メディア関連のセキュリティ〔第1回〕

著作権保護

正会員 山村千草†

1．まえがき

皆さんは普段の生活のなかで，どれだけの量のコンテンツに接しているでしょうか？「朝起きたらテレビをつけながら新聞を読む」，「音楽を聴きながら通勤・通学する」，「スマートフォンでオンラインゲームをしながら帰宅する」，「家に帰ったらパソコンでインターネット動画を楽しむ」－このように身の周りは数多くのコンテンツで溢れています．通常，これらのコンテンツには，著作権という権利が発生します．今や，さまざまなコンテンツをいつでも手軽に入手できる時代となり，日々の生活のなかで著作権を意識する機会は少ないかもしれません．一方で，ディジタル化によって，誰もが高品質なコンテンツを簡単に複製・頒布できるようになったことで，著作権侵害は身近に起こりうる社会問題となっています．

現在，身の周りに流通しているコンテンツのなかには，何かしらの技術的手段によって著作権が保護されているものが数多くあります．その保護形態は，映像や音楽といったコンテンツの種別やその品質，流通形態などによってさまざまです．実際には，ビジネス的価値や社会環境などを総合的に判断したうえでコンテンツの保護要件が決定され，コストや利便性にもあった技術が選択されます．

本稿では，著作権保護について，技術的な内容を中心にお話します．その他，法律やビジネスについて詳細に知りたい方は，他の文献などを参照していただきたいと思います．皆さんが普段見聴きしているコンテンツがどのように保護されているのか，本稿を通じて実感していただければ幸いです．

2．コンテンツを取り巻く環境の変化

音楽，映像，書籍，ゲームといったさまざまなジャンルでコンテンツのディジタル化が進み，その流通形態や利用形態は時代とともに変化してきました．私たちのコンテンツ利用行動は，10数年前と比べて大きく変容したと言えるでしょう．21世紀に入ってからの経緯を簡単に振り返りながら，コンテンツを取り巻く環境の現状（図1）について示します．

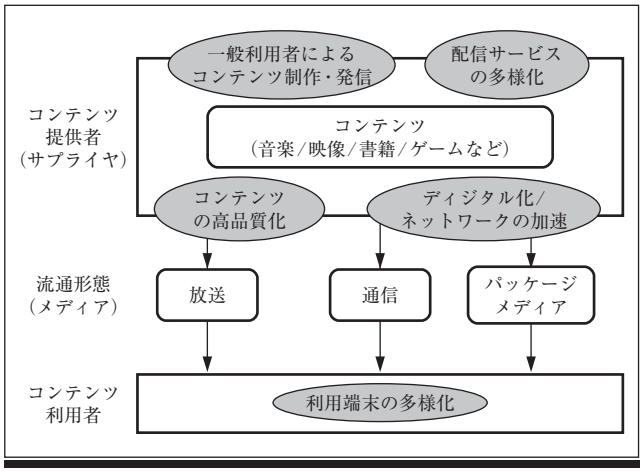


図1　コンテンツを取り巻く環境の現状

これまでのコンテンツ産業で，革新的な取組みを先導してきたのは音楽の分野でした．米国では1999年にP2P音楽共有ソフトNapsterが登場し，楽曲をネットワーク上で自由に交換できることが話題を集めました．しかし，著作権を無視した違法な流通が蔓延したことで，大手レコード協会が訴訟を起こし，Napsterは窮地に追い込まれる結果となりました．そうしたなか2001年に登場したのが，AppleのiPodおよびその楽曲管理・購入ソフトであるiTunes[1]です．Napsterとは対照的に，権利者へ適切な対価を還元する合法的なサービスとして広く受け入れられ，オンライン上で購入した楽曲を携帯して楽しむスタイルは，瞬く間に利用者の間に拡がりました．この影響は，その後のパッケージメディアの売り上げ低迷を招き，ネットワーク化を加速させる要因にもなりました．

映像の分野では，2000年に国内でBSデジタル放送が開始し，放送を介して高品質な映像を伝送することが可能になりました．また，ネットワーク環境のブロードバンド化により，数多くの動画配信サービスが誕生したのもこの頃です．通信

† NHK放送技術研究所
"Security Technologies on Image Information (1); Digital Rights Management" by Chigusa Yamamura (NHK Science & Technology Research Laboratories, Tokyo)

映像情報メディア学会誌 Vol. 69, No. 1, pp. 64～71（2015）

事業者のIP網を介してSTB（Set Top Box）に動画を配信するIPTVサービスや，インターネット網を介してPCや携帯端末にコンテンツを配信するOTT（Over The Top）サービスなど，さまざまな形態の動画配信ビジネスが登場しました．なかでも，2005年に登場したYouTube[2]は現在もなお，圧倒的な存在感を示しています．現在，月間10億人の利用者数を誇る一大サービスへと成長したYouTubeですが，その訴求力の背景には，動画を無料で楽しめる手軽さと，自ら作ったコンテンツを発信できる革新的スタイルがあったと言えるでしょう．誰もがクリエータになり得る環境の変化は，自分の著作物に対する権利，すなわち著作権への意識を高めるきっかけにもなりました．

このほか，米国では，高品質で価値のある作品ラインナップを武器にNetflix[3]やHulu[4]といった動画配信サービスが盛り上がりをみせ，日本でも放送局によるオンデマンドサービスが本格化しています．近年では，コンテンツ単位で対価を支払うPPV（Pay Per View）より，定額料金での無制限・見放題をうたった定額制サービスが優勢であり，得られた収益をいかに権利者に適正に分配できるかが，動画配信サービスの行く末を見通す重要な鍵となっています．

このように放送・通信インフラ技術の進展は，これまで映像配信プラットフォームを拡大させ，多様なサービスを生み出してきました．しかし，より高品質な映像体験への追求は止むことがなく，現在もなお，4K·8Kといった高精細な映像表現の実現に向けた歩みが続いています[5]．

音楽や映像の分野と同様，書籍やゲームの分野においても，ディジタル化に伴うネットワーク化の流れは進んでいます．特に，近年のスマートフォンやタブレット端末の急速な普及が後押しとなり，その流れは一層加速しています．書籍の分野では，印刷媒体の売り上げが低迷するなか，電子書籍の市場規模は年々拡大傾向にあります．また，ゲームの分野では，各種オンラインゲームが活況であり，特にスマートフォン向けのゲームは顕著な伸びを示しています．

現在，コンテンツ市場のうち，ディジタルコンテンツが占める割合は64%程度であり，その市場規模は国内だけでも8兆円弱と試算されています[6]．特に，日本のコンテンツはクールジャパンとして海外からの高い評価を得ており，海外展開による市場規模の拡大は，国家の経済成長戦略としても位置付けられています[7]．

良質なコンテンツは，人々に喜びや感動を与えるだけではなく，豊かな文化の形成や新たな価値の創造に必要不可欠です．そのため，良質なコンテンツの制作・流通機会は，守られなければなりません．仮にコンテンツ制作者に不利益が生じることがあれば，コンテンツ制作者の創作意欲は低下し，結果的には経済的または文化的な損失を生むことになります．そのため，コンテンツ制作者に対する適切な対価還元は非常に重要です．一方で，その対策を過度に行うと，コンテンツの利用障壁を高めることになり，本来の目的であるコンテンツ利用を停滞させてしまう恐れがあります．「コンテンツ制作者への適切な対価還元」と「コンテンツ利用者にとっての利便性の確保」は，良質なコンテンツの流通を促す健全な市場を形成するうえで，いずれも欠かせない要素です（図2）．

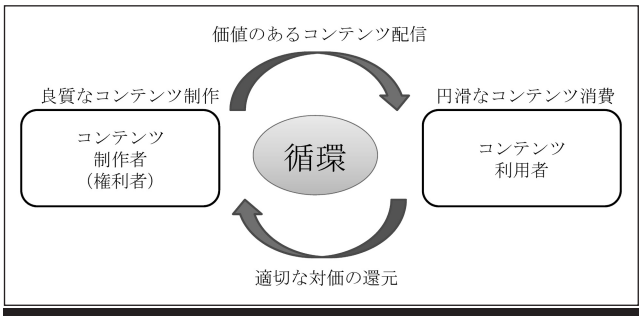


図2　良質なコンテンツ流通を促す健全な市場の形成

3．著作権保護の基礎

著作権法によれば，著作権の保護対象である著作物は，「思想または感情を創作的に表現したものであって，文芸，学術，美術または音楽の範囲に属するもの」と定められています[8]．著作物の創作者である著作者には，創作の時点で自動的に著作権が付与されます．

著作権は具体的に，複製権，上演権および演奏権，上映権，公衆送信権および公衆伝達権，口述権，展示権，頒布権，譲渡権，貸与権，翻訳権および翻案権，2次的著作物の利用に関する原著作者の権利といった複数の権利（支分権という）から構成されています．これらすべての権利は，著作者が専有できる権利となっており，他人が著作者の許諾を得ることなく，勝手に権利を行使することはできません．例えば，他人の著作物を勝手に複製する行為は，私的な複製を行う場合を除いて，複製権の侵害に当たります．また，他人の著作物を無断でインターネット上へアップロードする行為は，公衆送信権の侵害に当たります．

元来，著作権法は，文学作品や絵画といった典型的な著作物を対象にしてきました．アナログ時代には，そうした著作物を複製するのは容易なことではなく，その脅威は限定的なものと考えられてきました．しかし，ディジタル時代に入り，誰もが高品質なコンテンツを劣化なく，複製・改変・発信できるようになると，著作権侵害は誰もが侵し得る大きな脅威となりました．それ以降，幾度にわたって，技術の進歩やサービスの進展に応じた法制度の見直しが行われてきました．例えば，違法にアップロードされたコンテンツと知りながらコンテンツをダウンロードする行為や，技術的な保護手段を回避するような行為は違法とみなされるようになりました．また，これまで紙媒体による出版のみを対象としてきた現行の出版権を電子書籍にまで拡大するなど，新たなサービスに対応した法改正も行われて

います．

著作権保護の根底にある考え方は，著作者の許諾の範囲を超えた著作物の複製や頒布を防ぐことにあります．しかし，利用者の行動すべてを人海戦術で監視するには限界があります．そこで，その対策を技術的な手段で行うのが，著作権管理技術DRM（Digital Rights Management）です．

ただし，DRMの目的は，コンテンツの違法な複製や流通を防止することだけに限られていません．広義には，権利者へ不利益が生じることがないようにコンテンツの利用を制御・管理する技術を，総称してDRMと呼んでいます．つまり，不正をさせない，不正を発見する，不正をやめさせる，不正を蔓延させないなど，その技術的手段は多岐にわたります．

次章以降では，各メディアで用いられている代表的な著作権管理技術について説明します．

4．日本のデジタル放送における著作権管理技術

日本のデジタル放送では，有料放送の要件を考慮して，コンテンツの受信を契約者のみに制限する限定受信方式CAS（Conditional Access System）が採用されています[9]．図3に示すとおり，CASでは，視聴権限のある契約者のみが，視聴ライセンス，すなわちコンテンツを視聴するための鍵を取得できます．これにより，片方向の特性を有する放送メディアでも，契約者単位でコンテンツの視聴可否を

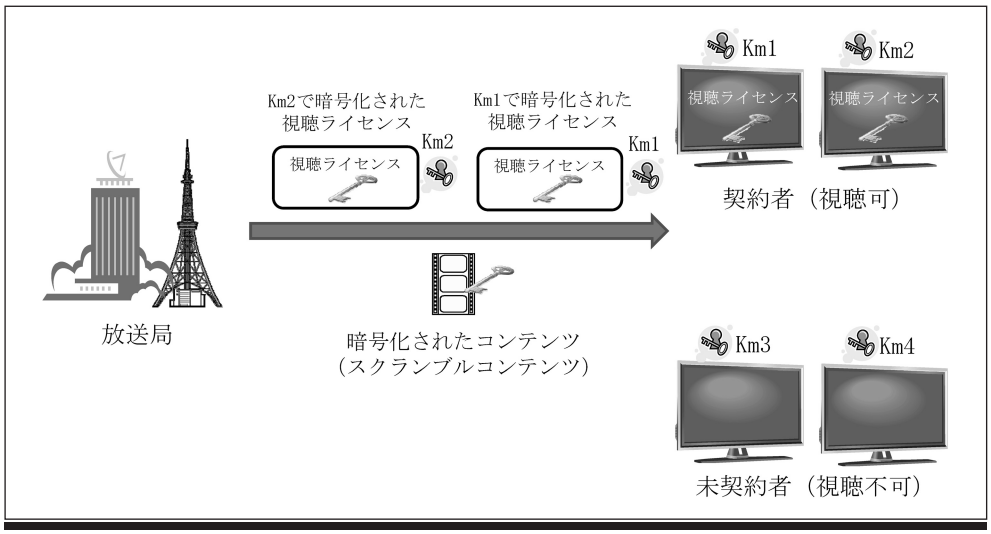


図3　CASにおけるアクセス制御の概要

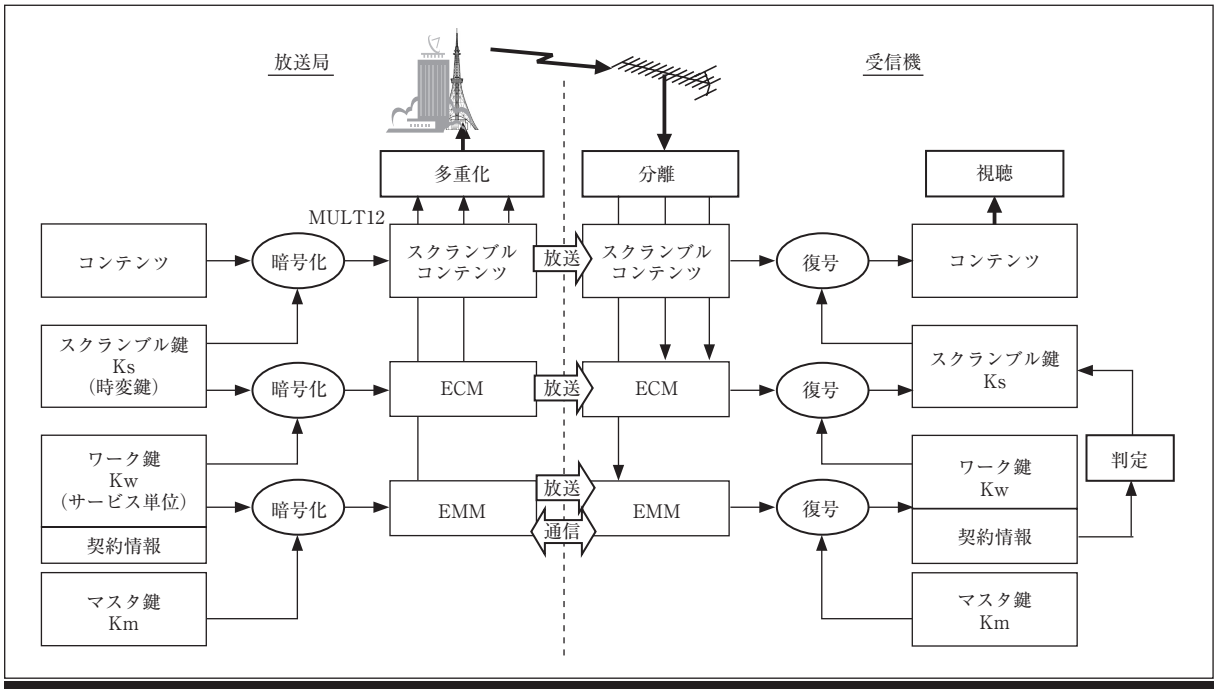


図4　3重鍵構造によるCASの仕組み

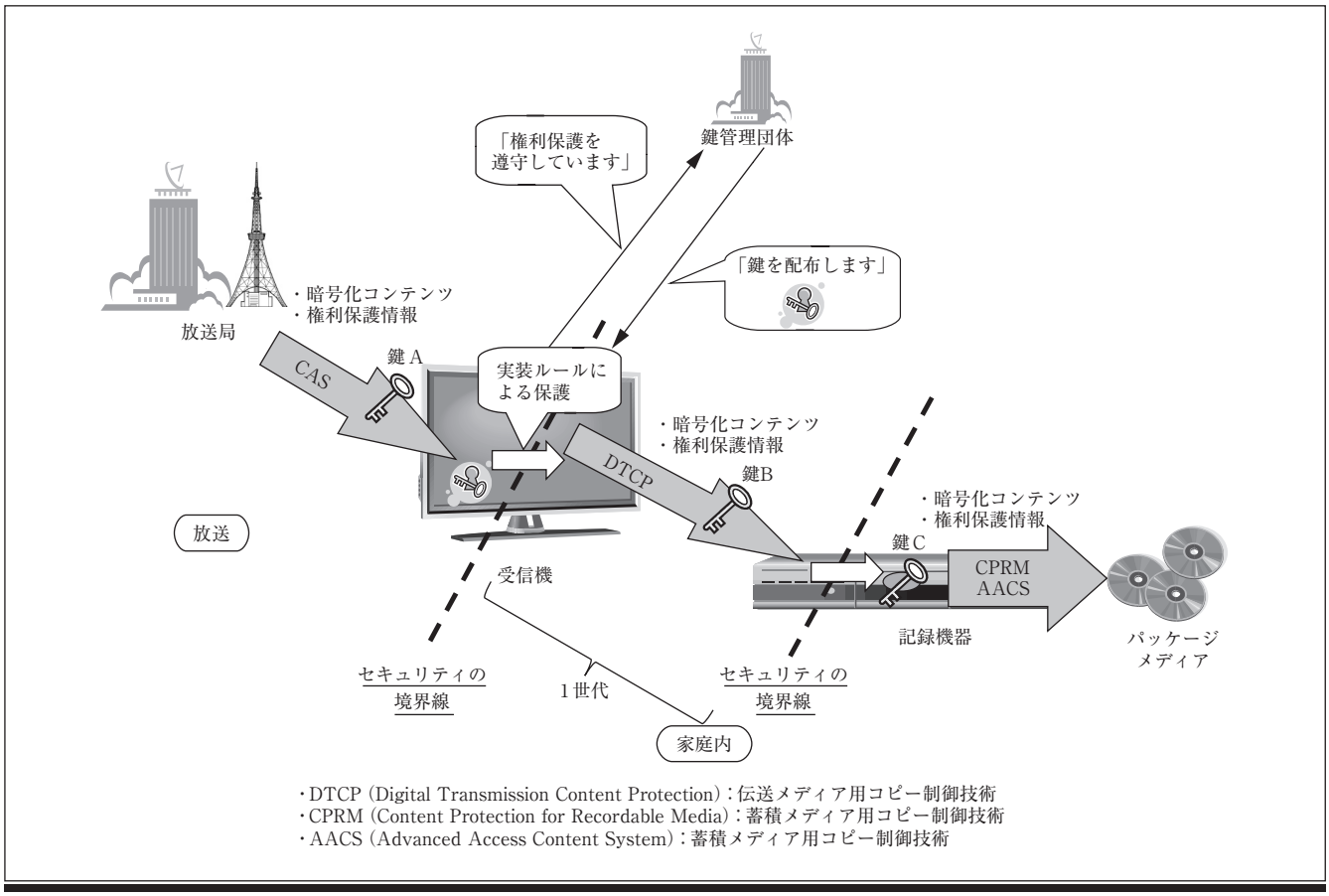


図5　セキュリティチェーン形成による著作権保護

制御（アクセス制御）することが可能になっています．

視聴ライセンスを正規の契約者に対して正しく配送する仕組みには，図4に示すような3重鍵構造が用いられます．その仕組みについて以下に示します．

放送コンテンツは時々刻々と変化するスクランブル鍵Ksで暗号化され，放送波でスクランブルコンテンツが伝送されます．そのため，このKs（＝視聴ライセンス）が得られない限り，放送コンテンツを視聴できないようになっています．Ksは，ワーク鍵Kwと呼ばれる鍵で暗号化され，ECM（Entitlement Common Message）という契約者共通の情報として伝送されます．また，Kwは，契約者個別のマスタ鍵Kmと呼ばれる鍵で暗号化され，EMM（Entitlement Management Message）という契約者個別の情報として伝送されます．契約者は受信したEMMを，あらかじめ保有するKmを用いて復号してKwを抽出した後，さらにKwを用いてECMを復号し，最終的にKsを抽出します．このようにして得られたKsでスクランブルコンテンツを復号することで，契約者のみが暗号化された放送コンテンツを視聴できるようになっています．

現在，Kmは，テレビ購入時に同梱されるICカード（B-CASカード）内に事前に埋め込まれて配布されます．B-CASカードには契約者ごとにそれぞれ異なるKmが割り振られており，EMMの情報は該当の契約者以外は正しく処理できないようになっています．

デジタル放送では，このような契約者単位のアクセス制御の仕組みに加え，一度復号されたコンテンツの複製や外部機器への出力を制御するコピー制御の仕組みが設けられています．放送波には，「制約条件なしにコピー可」や「1世代のみコピー可」といったコピー制御情報や，外部機器への信号出力時の暗号化を指示する情報が重畳され，受信機はこれらの権利保護情報に正しく反応して動作することが求められます．市販されるすべての受信機に，この要件を確実に遵守させるための方策（エンフォースメント）として，権利保護情報に正しく反応する受信機に対してのみ，視聴ライセンスの取得に必要なKmを埋め込んだICカードを与えます．権利保護情報を無視して動作する不正な受信機にはカードが与えられないため，実質的に放送コンテンツの視聴ができなくなります．このエンフォースメントによって，すべての受信機が強制的に権利保護機能を搭載することになり，権利者の意図に応じた著作権保護を実現しています．

一方で，エンフォースメントの効果が及ぶのは受信機までに限られ，受信機から出力される信号については，他の記録/再生機器や機器間インタフェースにおける保護方式に委ねられています．受信機だけではなく，外部機器も含めてトータルで著作権保護を実現するには，受信機が受信

した権利保護情報を，DTCP（Digital Transmission Content Protection）など他の保護方式に確実に引き渡し，セキュリティチェーンを形成する必要があります．セキュリティチェーン形成による著作権保護のイメージを図5に示します．

現在，「1世代のみコピー可」と設定されたコピー制御情報は，“ダビング10”の運用がなされており，対応機器に録画されたコンテンツについては，10回のダビング行為が許可されています（9回コピー＋1回移動）[10) 11)]．

地上波では2012年から，有料放送の要件を考慮した限定受信方式CASに加え，コンテンツ保護のみを目的としたRMP（Rights Management and Protection）の運用を開始しています．限定受信方式であるCASとコンテンツ保護方式であるRMPの違いは，前者は契約者ごとに視聴可否を制御するのに対し，後者は契約者単位の視聴制御を必要としません．つまり，RMPでは，権利保護情報に対して正しく動作することさえ保証されれば，すべての受信機に対して視聴ライセンスが配信されます．また，CASはICカードでの実装となっているのに対し，RMPでは専用ソフトウェアでの実装を可能としており，スマートフォンやタブレット端末にも適用することが可能です．CASとRMPの比較を，表1に示します．

これまでCASは長年にわたって運用されてきましたが，現在ではさまざまな攻撃が仕掛けられているのも事実です．そこで，より安全性に考慮したアクセス制御方式として，「デジタル放送におけるアクセス制御方式（第2世代）およびCASプログラムのダウンロード方式」が新たに規格化されました[12)]．このなかでは，スクランブル方式の暗号化アルゴリズムなどが見直されたほか，CASプログラムの安全性を維持するためのCASプログラムダウンロード方式が規定されており，安全なCASプログラムへの切替えが可能になっています．CASプログラムのダウンロードは放送または通信で行うことが可能ですが，放送経由のダウンロードを行う場合には，図6に示すような3重鍵構造で通信路が保護されます．これによって，CASプログラムの安全なダウンロードを実現しています．

表1　CASとRMPの比較

	CAS	RMP
方　式	限定受信方式	コンテンツ保護方式
実装手段	ICカード（B-CASカード）	受信機の専用ソフトウェア
制御単位	契約者単位（カードごと）	端末単位
用　途	有料放送/無料放送	無料放送のみ

5．インターネットにおける著作権管理技術

インターネットで用いられるDRMは数多く存在し，その形態は多岐にわたります．ここでは図7を用いて，DRM

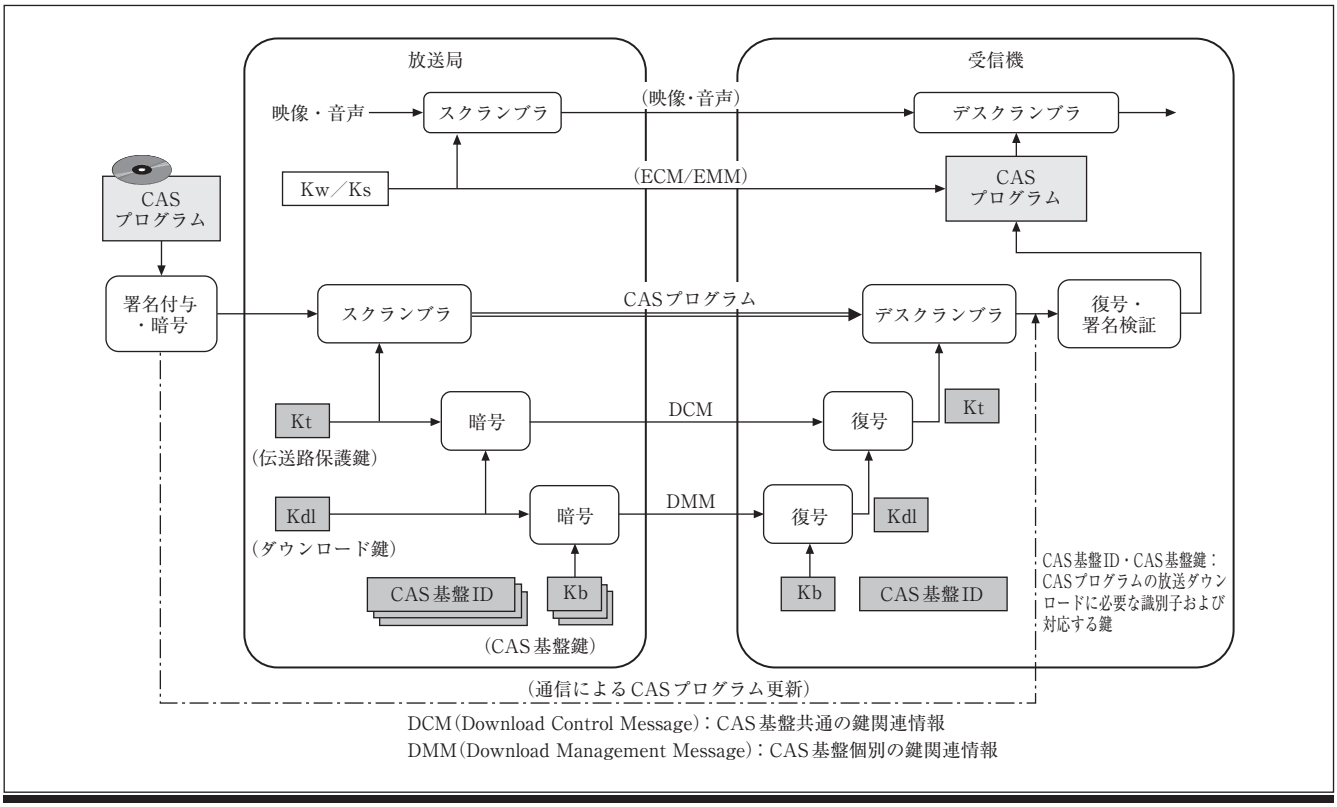


図6　アクセス制御プログラムのダウンロード方式概要[12)]

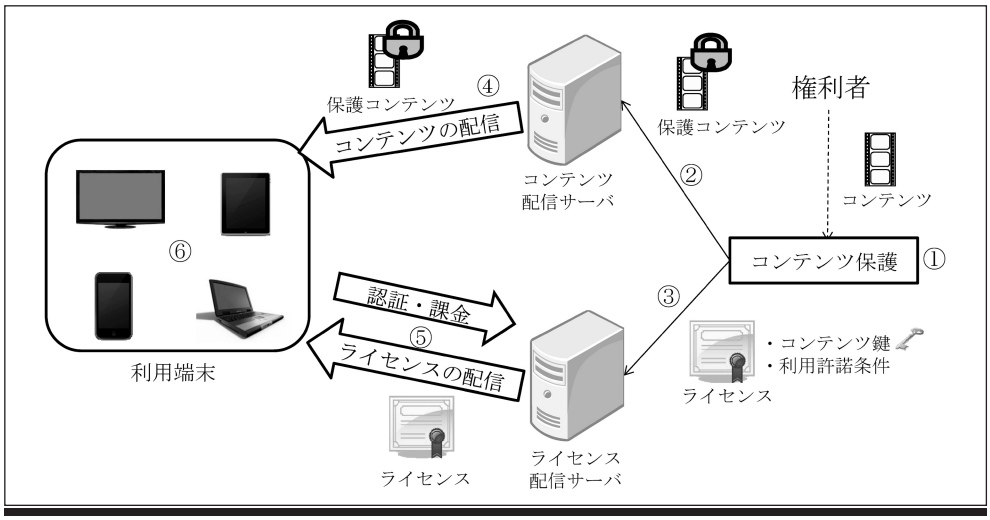


図7　DRMシステムの基本モデル

システムの基本モデルについて説明します．典型的な処理の流れは，以下のとおりです．

① 権利者はコンテンツに対して，暗号化などのコンテンツ保護を施す．コンテンツの利用許諾条件（利用端末や利用期間，利用料金など），および，暗号化に使用したコンテンツ鍵を含むライセンスを生成する．

② ①で暗号化し，配信用にエンコード/パッケージ化したコンテンツ（保護コンテンツ）を，コンテンツ配信サーバに格納する．

③ ①で生成したライセンスを，ライセンス配信サーバに格納する．

④ 利用者は，コンテンツ配信サーバから保護コンテンツを取得し，必要となるライセンス情報を特定する．

⑤ 利用者は，ライセンス配信サーバにライセンスを要求し，必要に応じて契約に基づくユーザ認証や課金決済を行ったうえで，ライセンスを取得する．

⑥ 利用者は特定のハードウェアまたはソフトウェア上で，ライセンスに含まれる利用許諾条件の範囲内で保護コンテンツを利用する．

コンテンツの利用許諾条件の記述方法には，条件を表す特定のフラグを規定する方法のほか，MPEG REL（Rights Expression Language）[13]のように標準化された権利記述言語を用いることも可能です．

これまでのDRMは，囲い込みを目的として，端末やOSの環境に依存したものが多く，利用者にとっては利便性が高いものとは言えませんでした．しかし，最近では多くのDRMが複数の端末環境に対応し，さまざまな端末にまたがってコンテンツを利用できる環境を実現しています．シェアを伸ばしているDRMには，AppleのFairPlay[14]やMicrosoftのPlayReady[15]，GoogleのWidevine[16]などがあります．AppleのFairPlayはiTunesなどで使用されていますが，ネットワークを介したApple IDのアカウント認証に基づいて利用者の端末を管理し，一人あたり最大5台の制約のもとで，購入した楽曲コンテンツの再生を許可しています．また，MicrosoftのPlayReadyは，さまざまなジャンルのコンテンツに対応できるように複数のファイルフォーマットをサポートしているほか，複数の端末をグループ化したドメインという概念を導入し，ドメイン内でのコンテンツ利用を可能にしています．また，GoogleのWidevineは，ライセンスフリーを売りに，モバイルアプリやテレビでの利用を狙っています．このように，個々のDRMは，利用端末環境の変化などに応じて，柔軟性や拡張性の高いものになってきています．その一方で，DRMごとに対応フォーマットや使用される暗号化方式がまちまちであり，異なる方式を持つ多数のDRMが乱立している状況は変わっていません．こうした環境のなか，米国の大手映画スタジオを含む業界団体DECE（Digital Entertainment Content Ecosystem）は，個人が購入したコンテンツの視聴権利をクラウドで一括管理し，複数の端末のそれぞれのDRM環境下で，正規の購入者が自由にコンテンツを視聴できる環境を実現するUltraViolet[17]を推進しています．このように，複数のコンテンツフォーマットやDRMの相互運用を図る取組みも進んでいます．

また，近年主流となっているWeb動画配信では，これまでAdobe Flash[18]やMicrosoft Silverlight[19]といったプラグインに入っているコンテンツ保護機能が使われてきました．しかし最近では，W3CでEME（Encrypted Media Extensions）[20]が新たに標準化され，プラグイン非対応でもWeb動画コンテンツの保護を行うことが可能になりました．このEMEはJavaScript API仕様群であり，HTML内のビデオオブジェクトを複数のDRMから選択して保護することが可能です．

有料サービスで用いられるDRMの多くは，「不正を防止すること」を目的としており，主には暗号化技術が用いら

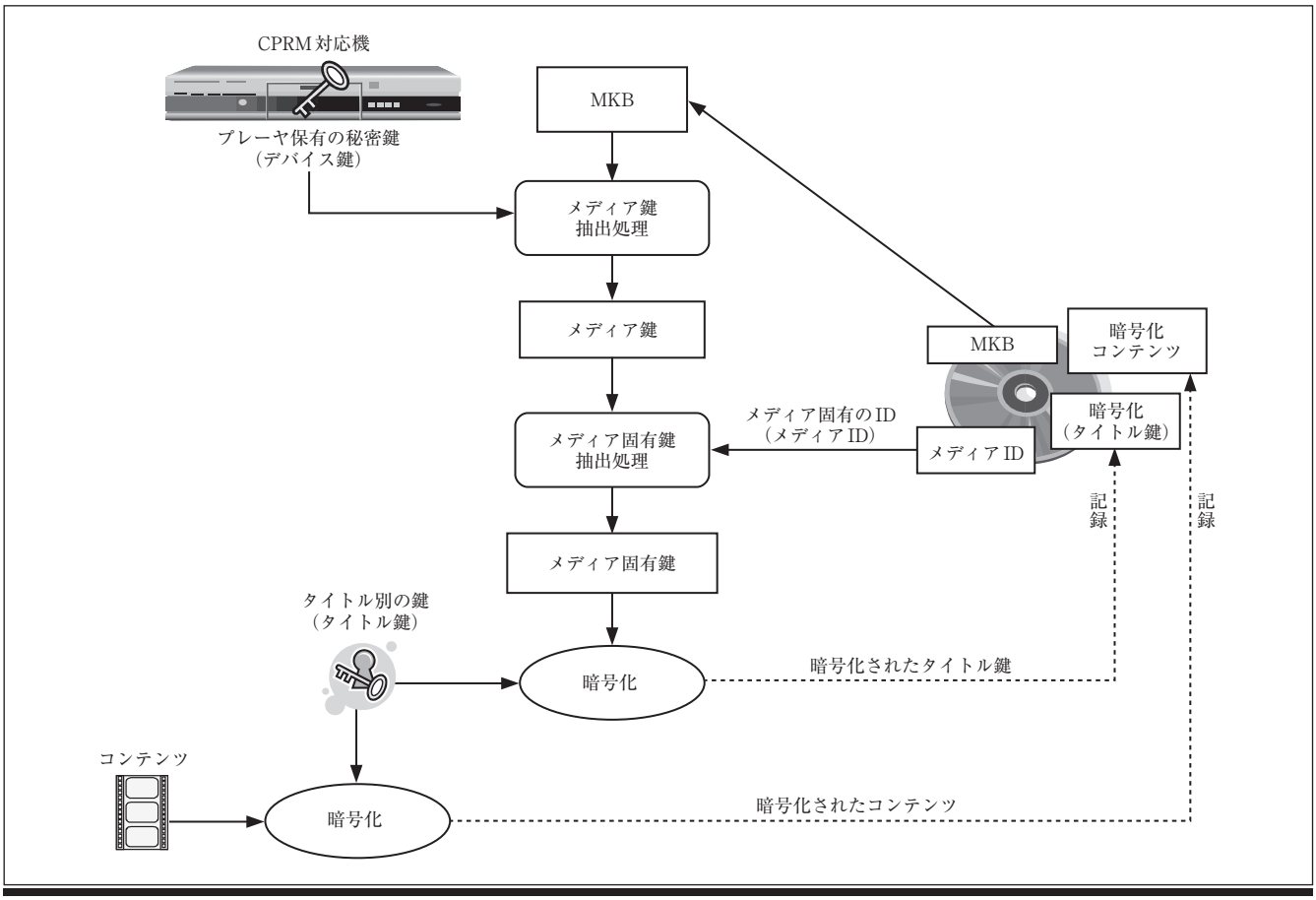


図8　CPRMにおける鍵管理方法

れます．しかし，3章でも述べたように，DRMの目的はさまざまであり，広告ベースの無料動画配信サービスYouTubeでは，「違法流通を食い止める」ことに注力しています．具体的には，アップロードされた画像のスキャンから一意に生成されるIDを管理し，違法動画が出回った際に，管理されているIDとの比較を行うことで，違法流通に迅速に対応できるようにしています．また，著作権侵害を繰り返す利用者に対しては，そのアカウントを停止するなどの措置を講じ，悪質な利用形態が蔓延しないようにしています．

このほか，コンテンツを大幅に劣化させないよう，画像や音声の知覚されにくい部分に情報を埋め込む，電子透かしと呼ばれる技術もDRMの一つとして知られています．電子透かしを用いて，コンテンツを識別するためのIDや著作権情報をコンテンツに埋め込む対策も，コンテンツが不正に流出した際の追跡を可能とする点で有効と言えます．

このように実現するサービスやコンテンツの価値に応じて，さまざまな形態のDRMが採用されています．

6．その他メディアにおける著作権管理技術

DVDパッケージメディアにおいては，DVD-Video用の保護技術であるCSS（Content Scramble System）やDVD-Audio用の保護技術であるCPPM（Conent Protection for Pre-recorded Media）が古くから知られています[14]．CSSは，ディスク上のコンテンツを3階層で暗号化し，メーカ単位に用意される秘密鍵セットで復号する方式です．しかし，CSSは1999年に解読されて以降，その実効性は失われています．

その後，CSSの改良版として登場したのが，DVDやその他記録メディアでも用いられているCPRM（Content Protection for Recordable Media）[21]です．CPRMにおける鍵管理方法を図8に示します．CPRM対応メディアには，事前にメディア固有のメディアIDと，MKB（Media Key Block）と呼ばれる鍵管理情報が記録されています．CPRM対応プレーヤでは，あらかじめ機器単位に個別に割り振られている秘密の鍵（デバイス鍵）を用いてMKBを処理し，さらにメディアIDを用いることでメディア固有鍵を生成します．このメディア固有鍵を用いて，タイトル別のタイトル鍵を暗号化します．このため，あるメディアに記録したデータを別のメディアに単純にコピーしても，メディアIDが異なるため，記録されたデータを正しく復号することができません．これによって，記録したメディアでしか再生できない仕組み，すなわち“コピーワンス”を実現しています．また，MKBとデバイス鍵はともにライセンス管理

団体によって管理されており，デバイス鍵が異なっていても同一のメディア鍵が生成できるようになっています．仮に，デバイス鍵が漏洩した場合には，それ以降に発行されるパッケージメディアでMKBを書換えることによって，正規のメディア鍵を生成できないようにし，鍵が漏洩したプレーヤでの再生機能を無効化することができます．

Blu-rayパッケージにおいては，AACS（Advanced Access Content System）[22]と呼ばれる保護技術が用いられています．AACSは，光メディアやプレーヤにとどまらず，ホームネットワークやポータブルデバイスにまでターゲットを広げている点が特徴です．誌面の都合上，説明は割愛しますが，詳細は参考文献を参照していただきたいと思います．

7．むすび

本稿では，メディアごとに用いられている代表的な著作権管理技術を取り上げ，身の周りにあるコンテンツがどのように保護されているのか，動向を交えながら紹介しました．保護という言葉は守りの印象の強い言葉ですが，著作権保護の本来の目的は，権利者に不利益が生じないようにコンテンツ流通を図ることにあります．利用者の利便性を損なうことなく，安全なコンテンツ流通を促進させるには，多種多様なDRMの互換性を図っていくことが今後ますます重要となってくるでしょう．

（2015年10月1日受付）

〔文　献〕

1）iTunes, http://www.apple.com/jp/itunes/
2）YouTube, https://www.youtube.com/
3）Netflix, https://www.netflix.com/global
4）Hulu, http://www.hulu.com/
5）総務省：“4K・8Kロードマップに関するフォローアップ会合中間報告”，http://www.soumu.go.jp/main_content/000312825.pdf（Sep. 2014）
6）ディジタルコンテンツ協会編：“ディジタルコンテンツ白書2014”，ディジタルコンテンツ協会（2014）
7）経済産業省:“クールジャパン政策について”，http://www.meti.go.jp/policy/mono_info_service/mono/creative/CJseisakunituiteSeptember.pdf（Sep. 2014）
8）中山信弘著：“著作権法”，有斐閣（2008）
9）ARIB STD-B25：“デジタル放送におけるアクセス制御方式”，6.4版
10）ARIB TR-B14：“地上デジタルテレビジョン放送運用規定”，5.6版
11）ARIB TR-B15：“BS/広帯域CSデジタル放送運用規定”，6.5版
12）ARIB STD-B61：“デジタル放送におけるアクセス制御方式（第2世代）およびCASプログラムのダウンロード方式”，1.0版
13）ISO/IEC 21000-5:2004: "Information technology", Multimedia framework（MPEG-21），Rights Expression Language”（2004）
14）今井秀樹編著：“ユビキタス時代の著作権管理技術”，東京電機大学出版局（2006）
15）PlayReady, https://www.microsoft.com/playready/
16）Widevine, http://www.widevine.com/
17）UltraViolet, https://www.uvvu.com/
18）Adobe Flash, http://get.adobe.com/jp/flashplayer/
19）Silverlight, http://www.microsoft.com/ja-jp/silverlight/
20）EME, https://dvcs.w3.org/hg/html-media/raw-file/tip/encrypted-media/encrypted-media.html
21）CPRM, http://www.4centity.com/specification.aspx#cppmcprm
22）AACS, http://wwww.aacsla.com/specifications

山村　千草（やまむら　ちぐさ）　2005年，京都大学大学院情報学研究科修士課程修了．同年，NHK入局．名古屋放送局を経て，現在，放送技術研究所に勤務．著作権保護，アイデンティティ管理，放送通信連携サービスに関する研究開発に従事．正会員．

講 座

映像情報メディア関連のセキュリティ〔第2回〕

ビッグデータの利活用とプライバシー保護の難しさ

山口利恵†

1．まえがき

「ユーザの嗜好により適したサービスの提供を行ったり，適切なサービス設計を行うことでシステム全体の効率化を行うためには，ビッグデータを利活用するべきである」と言われています．その一方，「データ活用が進めば進むほどユーザのプライバシーに触れる情報が，ユーザの意図に反し，容易に外部に出ていくことがあり，ユーザのプライバシーが侵される危険性がある」とも言われています．このデータの利活用とセキュリティ（プライバシー）の問題はトレードオフの関係であり解決が困難です．

本稿ではこの問題について，以下の構成で説明します．2章では，ユーザに関わる情報の多くを紐づけるために役立つIDについて考えます．現状でなぜIDが必要か，IDを利用することによって社会がどのように効率化されるか，その半面，IDをつけることによって名寄せのようにプライバシーにおいて問題が生じてしまうことを述べます．次に，名前と履歴がついていない仮IDであったとしてもプライバシーに問題が生じる事例について3章で紹介します．この事例に限らず，「そもそもデータを利活用するためには，『匿名データ』がよい」とよく言われていますが，データの所有者を完全に匿名化することはとても困難です．どのような点が困難かについて4章で述べ，完全に匿名化されたデータ生成を実現するためには実データ解析が必要であることについて述べます．5章では，プライバシー保護のために有効とされている技術に対し議論します．そして，6章では，ユーザのとるべき対応と，データ解析について述べ，7章でまとめさせていただきます．

本稿を通じて，皆さんのプライバシーが使用され，保護されていかなければならないかを実感していただければ幸いです．

† 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
"Security Technologies on Image Information (2); Privacy Inconsistency with Big Data" by Rie Shigetomi Yamaguchi (Social ICT Research Center Graduate School of Information Science and Technology, the University of Tokyo, Tokyo)

2．電子情報化社会とID

みなさん，多くのポイントカードを持ち「ポイント」を集めていませんでしょうか．一昔前は，商店街等の各店舗で購入を行った際に，切手のようなシールをもらい，各自が自分で台紙にのりで貼り付けていました（図1，図2）．近年では，ポイントカードを活用し，機械的に情報を収集している商店街が増えてきました．このポイントカードにはIDがつけられていて，システムの中でポイントを収集しています．

この変化により，従来の各家庭で行っていたのり付けが不要となります．また，ポイントをチェックする人も，台

図1　切手型ポイントの事例（1）
千歳烏山商店街で現在でも利用しているダイヤスタンプ[1)]

図2　切手型ポイントの事例（2）
ダイヤスタンプの台紙[2)]

紙の1枚1枚のチェックが不要となり，人の手がかからなくなってきました．つまり，ポイントカードの電子化は顧客満足度の増加につながりますし，各商店街のチェック等の事務的な負担の減少にもつながります．このように情報を電子化するメリットは多くあります．

2.1 IDについて

一方，情報の電子化をより効率的に活用するためにはIDが不可欠です．例えば，国民の住民情報がすべて保存されている住基ネットを例に取ります．現状住基ネットにおいては，基本四情報のみがあり，特に番号はなく情報が入れられています[3]．基本四情報とは，

住所，氏名，生年月日，性別

のことです．

日本語の住所や名前のバリエーションは，欧米のアルファベットで記述できるものとは違い，大変多くの種類があります．住所表記で考えると：

・中央区1－2－3
・中央区一丁目二番地三号
・中央区1丁目2ー3

のようにさまざまな表記が可能です．また，名前についても，「さいとう」を例にとると：

斉藤，斎藤，齋藤，齊藤，齊籐，齋籐，濟藤…

のようになかなか一つには決まりません．手続きを簡潔にするために，齋籐さんは，普段は斉藤さんとして名乗っているであろうことが予想されますが，日によっては，斎籐とすることもあるかもしれません．

100年前，情報が電子化されていなかった時代，情報は紙媒体によって保管され，手作業で管理されていました．そのときは，上記のような場合であっても，住所や生年月日などの別の情報を活用することにより，人の目で見て「これは同一人物に違いない」と簡単に発見することができました．電子情報が機械によって登録がなされるような場合，「齋籐」と「斉藤」は違う人物となってしまいます．つまり，同じ人にもかかわらず，名前の表記が違うために，データベースに保存する場合は他人として登録され，同一人物が複数のエントリーとして登録されてしまいます．

このようなことが起こると多くの不都合が生じてきます．典型的な例が，いわゆる「年金問題」です．同じ人にもかかわらず，違う名前や住所で登録されている危険性があります．例えば，支払いにおいて別のIDを利用してしまうようなケースが生じ，支払ったはずなのに支払ってないと判断される危険性があります．そこで，年金機構はDB化の際に名寄せを行いましたが，完全にはできなかったと言われています．年金問題は，一概にこれだけが問題ではありませんが，紙媒体の情報を唯一無二のIDなしに電子化する場合にはこのような問題が起こってしまいます．

2.2 IDの重要性とプライバシー

電子化された情報（以下，電子情報）において，IDは非常に便利なものです．先ほどの事例のように，一人の「斉藤」さんが複数の書き方を使い分けている場合についても，もし，各個人にIDがついていたら上記の問題は起きません．なぜなら，各個人が番号で管理されているため，名前や住所の表記が違ったとしても，同一人物であることが簡単にわかるためです．これにより，税金の年末調整や児童手当手続きの簡素化，バックオフィスと言われる企業内の事務処理でも複数のIDの複雑な管理がなくなり，国民全体が利用するシステムも効率化が進むでしょう．一方で，国が国民一人一人の監視に繋がるという声もあります．そのため，国民に唯一無二の番号を付番することの是非については，内閣官房おいて検討が進められています[4]．

2.3 商店街のポイントカード電子化とプライバシー

さて，商店街のポイントカードの話を思い出してみましょう．従来の切手型のポイントカードの場合，商店街は各顧客が収集したポイントから，どの店で何を購入したのかについて追跡をすることができません．それに対し，電子化されたポイントカードでは，あるユーザがどの店で何を購入したか(買い物履歴)を追跡できるようになりました．商店街は顧客の巨大な買い物履歴を持つことが可能となります．あるユーザがいつどの店舗で何を買っているのかの履歴を完全に持つことになります．それらの履歴は，電子データであるため，検索等も簡単で詳細な解析が可能です．商店街はいろいろな解析により，より顧客満足度を上げるサービスを行うとともに，売り上げの増加をねらうことが可能となります．

また，最近では，SuicaやPASMOを使ったポイント収集が可能な商店街（図3）も存在します．このような広く利用されているIDを活用したサービスが普及すると，この共通IDを起点としたデータの突き合わせが可能となり，他の履歴情報との統合ができます．特に国民番号のような唯一無二の番号があれば，なおさら統合が容易に実現できます．

図3　SuicaやPASMOでのポイント収集の事例[5]

電子情報においてIDは非常に重要ですが，一方で，あるIDを起点として，各個人が受けているサービスの追跡が容易であるため，各個人の趣味趣向や価値観までもが簡単にわかってしまいます．つまり，電子情報にとってIDは大変重要であるし，必要不可欠ではあるものの，プライバシーに関しては多々問題をおこす原因ともなります．

3．プライバシー保護データ作成の難しさ

次に，プライバシー保護のための匿名化処理として，名前を隠したとしても，プライバシーに問題が起きている事例について紹介します．

3.1　Netflix社のDVDレンタル履歴

2006年，米国の大手DVDレンタル会社であるNetflix社は，匿名化されたDVDレンタル履歴を公開し，リコメンデーションのためのアルゴリズムを競わせるコンテスト（Netflix Prize）を行いました（図4）．約50万ユーザ，1億件分のデータから個人を識別できる情報を削除し，各個人がどのような趣味趣向があるのかについてのコンテストでした．そして，Netflix社は，自ら持っていたIDではなく，IDを付番しなおし，仮IDに対して，映画名とその映画に対する評価（レーティング），登録日を公開しました．

それに対し，NarayananとShmatikovは，これらの公開データとthe Internet Movie Database（映画のレビューサイト）のデータを突き合わせることで，二人の個人が識別できたと発表しました[6]．彼らは，Netflixより貸し出したDVDによって，観た映画の順番に注目し，映画レビューサイトに投稿した順番が等しいものを探しだしました．順番を利用し，データの突き合わせを実現したのです．つまり，IDを振り直したとしても，他の情報を突き合わせることにより，データを記載した個人を推測することが可能だったのです．

このような動きを受け，Netflixは米国連邦取引委員会の調査や法律家による訴訟を受けることになり，計画されていたNetflix Prizeの続編は中止に追い込まれました．

3.2　マサチューセッツ医療データ

2002年，マサチューセッツ州は，医療データの一部を公開しました（図5）．このデータは，マサチューセッツ州が独自に匿名化処理した医療データによって，何か新たな医療に関する研究を行うことができないかという意図をもって行われたものです．ここで匿名化処理とは「医療データから氏名を削除したデータ」のことです．このデータに対して，性別，生年月日と郵便番号，および診療結果や投薬の情報なども含めて公開しました．

その年Sweeneyは，すでに公開・販売されている投票者の名簿と医療データとのデータマッチングを行いました．特に彼女は州知事のデータに注目し，知事と同じ地域に住む54,000人の住民が載る投票人名簿の中から，知事と同じ生年月日のレコードが6人，うち3人が男性であることがわかりました．そして，郵便番号から1人に特定し，州知事の医療情報を特定することに成功しました[7][8]．

図4　Netflix Prizeにおける項目

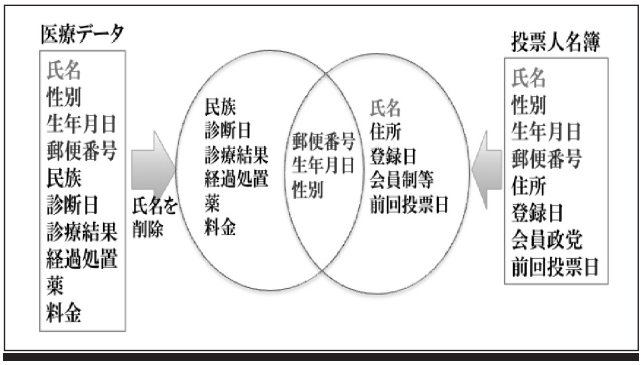


図5　マサチューセッツ州の医療データにおける項目

この問題は，医療データの公開先を研究機関等に限定していたため大きな問題にはなりませんでしたが，簡単な氏名の削除によって匿名化しただけでは，個人の追跡が可能であった例です．

4．匿名化データとは

ここまで，データに名前がなかったとしても個人が特定されてしまう危険性について述べました．では，個人が特定されないような情報，つまり，匿名情報とはどういう情報でしょうか？ これについてはいろいろな議論があります．この章では，あるデータベース内のデータを匿名化するにはどうしたらよいのかについてその概要を簡単に説明します．なお，その詳細は文献9）で述べていますのでそちらを参照していただきたいと思います．

4.1　匿名化における諸概念と用語

まず，以降で使う用語を定義します．前提として，各個人に関してその人を記述する複数の属性の情報が記述された個人情報のデータベースが存在したとします．そして，このデータベースは，実在しないような人が存在しないデータであり，実世界のうち誰であるかを示す個人とその個人の属性を示すようなデータを対象にしています．実世界の個人を以下では個人と記します．

個人の属性データは従来，以下の三つに分類されてきました．

- 個体識別属性：個人を直接的かつ一意に識別する属性であり，氏名や個人番号が相当します．
- 擬似識別属性：個人を間接的に識別する属性であり，必ずしも一意に識別するものではありません．例えば，性別，生年月日，出生地，国籍，住所などが相当しま

す．これらは，単独では個人を一意に識別できませんが，複数の属性を併せると，個人を一意に識別することができます．

・その他の属性：個体識別属性，擬似識別属性以外の個人データを記述する属性です．例えば，病歴，収入，債務など他人に知られることが個人にとって不利益をもたらしかねない属性とします．

個人情報のデータベースに対して，一般的に言われる名前の削除や仮名化による匿名化は，個体識別属性を削除する，もしくは，無意味な文字列や番号に置き換える，つまり，仮名化されていることを意味しています．

また，擬似識別属性を利用したとしても，特定個人が一意に識別できるとは限りません．ここでは，擬似識別属性を利用して，記述された個人が識別される場合を表す概念を整理します．

・識別：ある個人を他者とは違う属性を持つ存在として一意に定めることを意味します．ただし，同一の個人であることが一意に定まっただけであり，実世界の誰を指し示すかまでは分からなくてもよいとします．

・特定：ある個人がその人の属性データから一意に定まり（識別され），かつ実世界の誰であるかを差し示す（特定する）ことができることを意味します．

この二つの概念を用いると，個人の属性データからの識別や特定を行える情報を次の3種類に分類できます．

・識別特定情報：個人が識別され，かつ特定される状態となるための擬似識別属性データの集合．生年月日や名前等も含まれますが，同じ誕生日や同姓同名の人も存在しますので，一つだけでは個人への識別に至るとは限りません．これは，一般的に「個人情報」と見なされている情報です．

・識別非特定情報：データベースに記載された個人の一人ひとりは識別されますが，実世界の個人の誰であるかは特定されない状態の擬似識別属性データの集合．当然，個人を特定するためには，他のデータベースと突き合わせる処理が必要です．

・非識別非特定情報：データベースに記載された一人ひとりが特定されず，かつ識別もされない状態の擬似識別属性データの集合．

この分類は，一つのデータベースを念頭においた定義に見えますが，個人情報のデータベースを複数個使って，突き合わせる処理を行った場合にも通用します．その場合の属性は，複数のデータベースの属性の和集合を使うことになります．

4.2　完全な匿名化に関する考察

個人情報から，個人を認識したり，特定したりすることができないようにする「匿名化」をここでは，「完全な匿名化」と呼ぶことにします．この完全な匿名化が行われた場合，その後，いかなる他のデータと照合を行ったり，加工や変換を行ったとしても，個人を識別・特定するための情報は一切増えることがありません．以下ではこのような完全な匿名化を実現する汎用的な変換法が存在するかどうかを検討します．

4.2.1　匿名化技術とその問題

非識別非特定なデータになるように匿名化をする方法として一般的な“k-匿名性”について考えます．k-匿名性とは，2002年にSweeneyが最初に提案した匿名化技術です[7]．k-匿名性は，擬似識別属性に注目し，一つ一つの擬似属性情報をより抽象的に表現し，あるデータから特定できる個人がk人未満にはできないように工夫された技術です．すなわち，ある属性データをもつ個人はk人以上となるようにデータを加工することで匿名性を確保する技術です．ここで擬似識別属性を抽象化するとは，例えば，ある「渋谷3丁目3番地」と「渋谷2丁目5番地」にいる人が1人ずつ存在し，$k \geq 2$としてデータを公開する場合には，渋谷だけが共通点なので，「渋谷」に2人いるとして加工データを公開することです．

このk-匿名性は，どの属性に注目するのかによって，できあがる加工データが変わります．これは，上記の例のように，データ加工の方法が個体識別属性の削除ないしは仮名化を行って擬似識別属性の抽象度を上げる場合，加工対象以外の属性についてはそのまま情報が残されますので，注目する属性に応じて，抽象化する属性とそのまま残される情報が異なるためです．

k-匿名性を単純に用いた場合であっても，設計者がありとあらゆる想定ができるわけではないため，ケースによってはk=1のデータが存在する可能性があります．また，一つのデータベースではk-匿名性があったとしても，3章に示したように別の情報と組合せることにより，本人と特定されてしまう可能性もあります．データセットが「本人を完全に特定できないデータである」というためには，その他の属性のデータでさえ抽象度を上げk人以上のデータとしなければなりません．この場合，その他の属性データも，擬似識別属性と同じ種類のデータとなります．すなわち，完全な匿名化を満たすデータを作成する必要条件の一つとして，擬似識別属性はもちろんのこと，その他の属性も含めた全項目においてk-匿名性が満たされなければならなくなります．

4.2.2　属性情報推定のリスク

その他の属性も擬似識別属性と見なす，すなわち個体識別属性以外の属性をすべて擬似識別属性として扱い，その上ですべての擬似識別属性を合わせた情報が非識別非特定情報である場合を考えなければなりません．この場合，データベース内のすべてのデータから個人を特定することも識別することもできません．しかし，このような状態でもなお，以下のようにデータから個人が推定されてしまう場合が存在します．

例えば，k-匿名化の結果，k人を含むグループyができたとします．そして，グループy内の全員が就職活動中の学

生であり，最寄り駅がz駅であって，かつ消費者金融に出入りしていることが彼らの擬似識別属性からわかったとします．

ここで，他のなんらかの方法である個人xがこのデータベースに存在し，しかもグループyに含まれることが判明したとします．グループyにはk人が含まれており，個人xがk個のどのデータに相当するかはわかりません．しかし，グループyのメンバは全員就職活動中の学生で，なおかつ最寄り駅がz駅で，さらに消費者金融に出入りしていたのですから，グループyに含まれる個人xもこの擬似識別属性をもつことになります．結果として個人xは消費者金融に出入りしていることがわかります．つまり個人xが「消費者金融に出入りしていた」という事実は個人xが秘匿していたとしても，個人xがグループyに所属しているという事実が判明することで確定します．

このことはk-匿名化が完全に満たされていたとしても個人の属性情報が暴露されてしまう可能性があり，個人のプライバシーにおける問題が生じる可能性があることを示しています．例えば，個人xが「消費者金融に出入りしていた」という事実が明らかになれば，就職活動において会社から採用内定がもらえないなどという不利益を被る可能性もあります．

上記の例のような非識別非特定情報からも属性情報が推定されるという状況が個人の病歴などの属性で起きた場合には，ある地域ではAという病気が流行っているという噂によって，その地域の人全員がAという病気にかかっているような印象を与えるというような風評被害といった重大な問題が発生すると想定されます．このような被害については，すでに文献10)において指摘されています．

このような問題の一つの解決策として，l-多様性の概念が提案されました[11]．l-多様性とはk人のグループ全員のその他の属性が1種類以上の多様性を持つことです．複数種類の属性値のうちのどれか一つに当てはまっていれば，属性を満たしていると判断されるようにk-匿名化を行うことで，属性の推定を困難にします．簡単に説明すると，先ほどの病気の例だと，Aという病気だけでなく，Bという病気を属性として増やすことが対策ということです[8]．

このように汎用の技術による完全な匿名化は非識別非特定情報を生成すればよいというものではなく，機械的に生成することが極めて困難ないし種々の問題点を内包していると言えます．

4.3　匿名性を高めることの困難性

上述しましたように，汎用的な匿名化を施すのは容易ではありません．その理由は主に次のことが挙げられます．

(1) データの種類が多様で複雑です：ビッグデータの特徴であるデータの多様化と複雑さが秘匿を難しくしています．道路交通データのような連続値の数列とオンライン商取引のような独立した離散値とで，対処方法は変えなくてはなりません．またデータセットのデータ量と個人の数も匿名性に関係します．例えば，10人からなる1 GBのデータと100万人が生成した1 GBのデータでは，後者の方の匿名性が高くなります．それゆえ，データの利用方法や統計的な解析なしには，匿名化の度合いを正しく評価することはできません．

(2) プライバシーの度合いは個人の主観で判断されています：個人情報の定義は明確でも，プライバシー情報の重要度には個人の主観によるあいまいさがあります．位置情報を深刻なプライバシー侵害と感じる人もいる一方で，各種ポイントカードによるプライバシーを抵抗なく提供する人も多くいます．したがって，一律な匿名化度合いは定められません．

(3) 匿名化の方法は多様で一意に決められません：すでに説明しているように，匿名化にはさまざまな種類があり，目的とする匿名度を満足する方法は一意に決められません．k-匿名化一つをとっても，加工する属性情報の組合せが多数存在するため，計算機での計算がとても難しいことが証明されています[12]．

(4) 攻撃者のレベルを特定できません：ここでの攻撃とは，匿名化措置されたデータから個人を再識別することを指します．この攻撃者の持つ知識や技術レベルを予め想定することは不可能です[7]．ゆえに，有用性を保ったまま匿名性を高めるためには，データ提供先への再識別禁止措置により，攻撃者のレベルを一定以下に抑えることが必須となります．

4.4　データベース保護に関する議論

以上のようにデータベースを匿名化するためには，k-匿名性のような技術を完全に適用し，世論調査のような統計データのように，そのデータだけでは個人を特定できないようにする必要性があることを説明しました．しかしながら，個別のデータではなく，複数のデータを解析した結果である統計データであっても属性推定のリスクがあるだけでなく，統計データとなるためにデータを削りすぎたため，利活用しづらいような情報となってしまう可能性がすでに報告されています[13) 14)]．

5．そのほかのプライバシー保護手法

プライバシーを保護することを目的とした技術は多数提案されています．特に暗号技術を基盤とした技術は，数学的な計算テクニックを活用してプライバシー保護を目指した技術です．ここでは二つの技術を紹介するとともに，それらの問題点についても議論します．

(1) 匿名認証・グループ署名技術

匿名認証，グループ署名技術について紹介します[15) 16)]．この技術はユーザをサービス提供者がわからないにも関わらず，認証を行ったり署名をしたりする技術です．

サービス提供者は，ユーザの名前を確認したり利用料を受け取るなどして，ユーザに対して権利を発行したにも関

わらず，ユーザが権利を行使した際には，サービス提供者は誰であるかどうかがわからないままに，権利の確認をすることができます．また，匿名であるためユーザが不正に権利を行使する可能性もありますが，不正に対しては，後から登録した際の名前に対して追跡することもできます．この技術を利用すると，選挙などにおいて，選挙権があるかどうかの確認ができるにもかかわらず，誰が誰に投票したのかわかりません．

一方で，上記の技術は，グループで一人しか登録していないような場合には，その人を特定することになります．

(2) 準同型暗号

準同型暗号とは，データベース管理者は誰がどのようなキーワードで検索をしていたかわからないし，逆にどのようなデータがあるのかもユーザにはわからないようにすることができる，という暗号技術です[17]．

しかし，ユーザが何度も検索した場合には，データベース全体がわかってしまう危険性があります．何回権利を行使して良いかについて，適切な設定が求められます．

6．プライバシー保護に関する議論

この章では，ここまでに説明してきた匿名化や暗号の技術だけではプライバシーの問題を解決できないという点について説明します．たとえ画期的な技術が発明されたとしても，ユーザに対してどのように説明していくのか，技術をどのように使うのかについての検討が不可欠です．ここでは，現状の問題点と今後の検討すべき内容，同意とデータ解析について説明します．

6.1　ユーザ同意における問題点

プライバシーは各個人で考え方が違うため，ユーザ毎にデータの扱い方を変更する必要があります．ユーザは常に自分の意思を確認するようにしなければならなりません．意思を示す方法として現在利用されている方法は，サービスを受けるたびにサービス提供者に示す「同意」です．この同意をとったとしても，専門知識のないユーザのプライバシーが危険にさらされる例も存在しています．このような事例を以下に述べます．

・スマートフォンアプリの同意

現在行われているサービスにおいて，ユーザが頻繁に「同意」している例として，スマートフォンアプリにおける同意が上げられます（図6）．ユーザがあまり考えずにこの同意をクリックするような事例も存在します．例えば，「LIME POP」[18]というような人気ゲームととても類似したような名前がつけられたアプリや，「電波改善」[19]といった利便性をあげるようなアプリが存在しています（図7）．

これらのゲームは，ゲームや電波改善のようなことは起こらずに，ユーザ端末の持つ住所録情報やGPS情報等，ユーザのプライバシーに大きく関連するような情報を集めています．ユーザは，「同意」しているものの，ユーザ自身が意図しない形でプライバシーに関わる情報がとられています．このようにプライバシーに問題があるようなアプリであっても，現状ユーザはどの情報をサービスに提供してよい，悪いの適切な選択ができているといえません．

図6　アンドロイドアプリのダウンロード画面の一部[20]

図7　電波測定アプリと称したアプリ画面
（IPAホームページより引用[19]）

6.2　データ解析の必要性に関する議論

ここまでプライバシー上のさまざまな問題について述べてきましたが，今後，これらをどのように解決したら良いのでしょうか．最新のプライバシー保護技術を単純に適用すればいいのでしょうか．

5章に示したプライバシー保護技術は，ユーザのどのデータを守るべきであるのかをセキュリティパラメータにしなければなりません．つまり，どのデータがどの程度集まった場合にプライバシーとして問題となるのかについて定めなければなりません．また，アンケートの○×のようにデータを単純化し，さらに，集計して収集することで匿名性を高くして情報を集めることができる一方で，一部の集め方については，濡れ衣などの問題があるので，その配慮も不可欠です．濡れ衣とは，自分があるデータに含まれるとして，自分はやっていないにもかかわらず，そこに所属する大多数の人が行っている行為がある場合，自分もやっていると勘違いをされてしまうことです．

次に，たとえ一意（k=1）に決まったとしても識別特定不能情報とすることも可能です．例えば，属性値の推定を防ぐ手法としては，そもそも個人xがグループyに存在するかどうかをわからなくする方法，すなわち，あるデータセットから個人xとグループyが1対1対応しないようにした上でk-匿名化をかける方法や，異なる擬似識別属性値の関係をデータの意味を変えないように工夫した上でランダムにつなぎかえるなどの手法がかんがえられます[8]．

どの形態でも，膨大な要求の中から有用な情報を定義し，本人を特定できないようなデータであることを保証した上で扱われる必要があります．

さて，どのようにしたらデータを有用とできるのでしょうか．

有用な情報収集の例として，世論調査や統計局調査等があります．世論調査における自由記述欄は，k=1であったとしても識別非特定情報であり，他のデータベースとの突き合わせはされませんでした．このような過去の成功事例を参考にしながら，それぞれの利用領域に特化し，活用するデータ・利用シーンごとに丁寧な解析を行い適切に利用する必要があります．

次に，データを誰が利用し，解析したとおりにデータが利用されているのかについての検討も必要です．この「誰が」について，ユーザに対して説明しなければなりません．同時に利用の目的も提示する必要があります．このような提示も，「同意」と同様の問題が起こりえます．したがって，プライバシーを保護していることを簡単にユーザに提示する方法も求められています．

7．むすび

匿名性と有用性はそれぞれ評価が可能で，定性的に互いにトレードオフの関係にあります．有用な情報であればあるほど，匿名性が犯されている危険性が高いと一般的に言われています．一方で，プライバシーを保つ情報を作成する方法として，「匿名化」手法が存在します．安易な匿名化手法では使えないデータしかでてこないことや，匿名化しきれていないデータが生成されるなど，複数の問題が残ってしまいます．また，データを何にどう利用したいのかについての議論がないままにさまざまな手法の提案が行われ，プライバシーに関するデータの使用基準がないままに適用されてきています．

今後は，データを利用する領域に特化された利用シーンや活用データの解析を行い，必要となる技術を開発したり選択することで，高いプライバシーと有用性を両立するデータ利活用が求められています．

（2014年11月3日受付）

〔文　献〕

1）えるもーる烏山：“ダイヤスタンプ”， http://www.elmall.or.jp/point/（2014/11/27アクセス）
2）キッズスペースぶりっじ：“2013年4月3日Blog記事”， http://plaza.rakuten.co.jp/bridgeroka/diary/201304030000/（2014/11/27アクセス）
3）総務省：“『住基ネット』って何？”， http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/daityo/juuki01.html（2014/11/27アクセス）
4）内閣官房：“社会保障・税番号制度”， http://www.cas.go.jp/jp/seisaku/bangoseido/（2014/11/27アクセス）
5）すがもネット：“すがもさくらポイント加盟店”， http://www.sugamo-net.com/store/point.asp（2014/11/27アクセス）
6）A. Narayanan and V. Shmatikov: "Robust De-anonymization of Large Sparse Datasets", Proc. of IEEE S&P'08, pp.111-125（2008）
7）L. Sweeney: "k-anonymity: a model for protecting privacy", International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10, 5, pp.557-570（2002）
8）Ars Technica, Net news, http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/（2014/11/27アクセス）
9）板倉陽一郎，伊藤孝一，菊池浩明，高木浩光，高橋克巳，中川裕志，疋田敏朗，廣田啓一，山口利恵，渡辺創：“『完全な匿名化』幻想を超えて”，情報とセキュリティシンポジウム2014（SCIS 2014），3D1-4（2014）
10）中川裕志，角野為耶：“滞在場所のk-匿名化と濡れ衣”，情報処理学会，第62電子化知的財産・社会基盤研究発表会（EIP研究会），2013-EIP-62，12，pp.1-6（2013）
11）A. Machanavajjhala, D. Kifer, J. Gehrke and M. Venkitasubramaniam: "L-diversity: Privacy beyond k-anonymity", ACM Transactions on Knowledge Discovery from Data（TKDD）TKDD Homepage archive, 1, 1, Article No.3（Mar. 2007）
12）A. Meyerson and R. Williams: "On the complexity of optimal k-anonymity", Proc. of ACM PODS'04, pp.223-228（2004）
13）菊池浩明，高橋克己：“乗降履歴データの安全な匿名化は可能か？”，情報とセキュリティシンポジウム2014（SCIS 2014）3D3-4（2014）
14）R.S. Yamaguchi, K. Hirota, K. Hamada, K. Takahashi, K. Matsuzaki, J. Sakuma and Y. Shirai: "Applicability of existing anonymization methods to large location history data in urban travel", ACM SMC'12, pp.997-1004（2012）
15）J. Camenisch and M. Stadler: "Efficient Group Signature Schemes for Large Groups（Extended Abstract）”, Proc. of CRYPTO'97, pp.410-424（1997）
16）J. Camenisch and A. Lysyanskaya: "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation", Proc. of EUROCRYPT'01, pp.93-118（2001）
17）M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan: "Fully homomorphic encryption over the integers", Proc. of EUROCRYPT'10, pp.24-43（2010）
18）シマンテック：“Lime Pop: Android.Enesolutyの新しい不正アプリ”，http://www.symantec.com/connect/ja/blogs/lime-pop-androidenesoluty（2014/11/27アクセス）
19）IPA：“2012年9月の呼びかけ：『情報を抜き取るスマートフォンアプリに注意！』～スマートフォンの中の個人情報が狙われています～”，http://www.ipa.go.jp/security/txt/2012/09outline.html（2014/11/27アクセス）
20）Google，Android同意画面：“Twitterアプリ”，https://play.google.com/store/apps/details?id=com.twitter.android&hl=ja（2014/11/27アクセス）

山口　利恵（やまぐち　りえ）　2003年，津田塾大学理学研究科数学専攻修士課程修了．2006年，東京大学大学院情報理工学系研究科博士後期課程修了・2006年，（独）産業技術総合研究所研究員．2007年～2011年，内閣官房情報セキュリティセンター員兼務．2013年より，同センター次世代個人認証技術講座特任准教授．博士（情報理工学）．

SSL/TLSの仕組みを知っていますか？

神田雅透†

1．まえがき ～SSL/TLSを使ったことありますか～

まず皆さんに質問です．

「あなたは，Amazonで買い物したり，オンラインでチケットや楽曲を買ったりしたことがありますか？ あるいは，ネットバンキングやネットトレードなどをしたことがありますか？」

この質問の答えが「YES」だった人は，例えSSL/TLS＊1のことを知らなかったとしても普通にSSL/TLSを使っているということになります．

SSL/TLSは，クレジットカード番号やパスワードなどの重要な情報をインターネット上で安全にやり取りするために使うセキュリティプロトコルの一つです．ブラウザに標準搭載されており，ブラウザのURLが表示されているあたりに「鍵（南京錠）マーク」が表示されていたら，その通信はSSL/TLSで通信している状態になっていることを表しています．

本稿では，SSL/TLSはどのような仕組みで動いているのかを解説します．

2．SSL/TLSは何をするものですか？ ～役割と仕組み～

SSL/TLSには，以下の2つの大きな役割があります．

(1) 通信相手を確認する：ネットワークを介した通信相手が本当に自分の意図した相手であるかを確認します．例えば，アクセスした先のサイトが，本物に似せたフィッシングサイトなどの危険なサイトではないことを確認することです．

(2) 通信内容を保護する：通信内容を第三者に盗聴されないように，暗号通信を行います．オンラインショッピングなどで「情報は暗号化されています」といった説明があるとき，この機能が使われていることを意味しています．

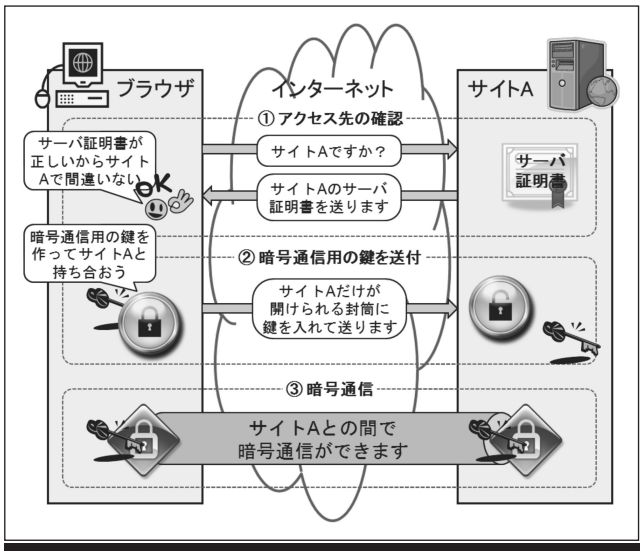


図1　SSL/TLSの動作

次に，実際のSSL/TLSの動作を見てみましょう．

SSL/TLSでは暗号通信が始まるまでに，大きく三つのステップが実行されます（図1）．

最初に行われるのが，SSL/TLSを使ってあるサイト（サイトA）にアクセスしたときに，アクセスした先のサイトAが本物であるかどうかの確認です．

その確認のために使われるのがSSL/TLSサーバ証明書（単にサーバ証明書ともいいます）です．具体的に何を行っているかは4章を参照してもらうとして，概念としては，「サイトAの正しいサーバ証明書を持っているのはサイトAだけである」ということを踏まえ，ブラウザが受け取ったサイトAと称したサーバ証明書が正しければ，そのサーバ証明書を送ってきたサイトは正しいサイトAである，と判断し，次の暗号通信のための準備に移ります．

もしサーバ証明書が正しいものと確認できなかった場合には，図2のように何らかの警告表示がブラウザに出るようになっています．

サーバ証明書によって自分の意図したサイトAにアクセスしていると確認できると，次のステップとして，暗号通信を行うための秘密鍵をブラウザが自動的に作成し，後述

＊1　SSL/TLS: Secure Socket Layer/Transport Layer Security.

† NTTセキュアプラットフォーム研究所
"Security Technologies on Image Information (3); How SSL/TLS Works?; Role and mechanism" by Masayuki Kanda (NTT Secure Platform Laboratories, Tokyo)

映像情報メディア学会誌 Vol. 69, No. 3, pp. 228～233 (2015)

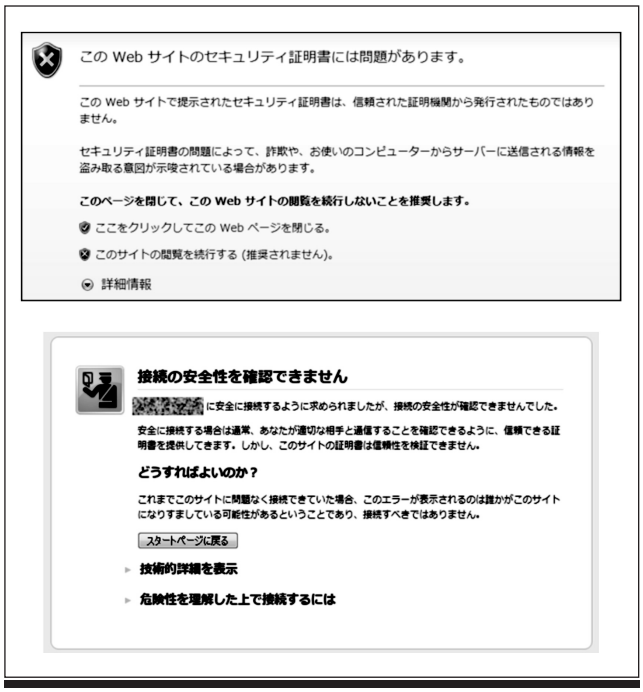


図2　警告表示の例（IE 8（上），Firefox 33（下））

する公開鍵暗号を使ってサイトAにその秘密鍵を送ります．そして，サイトAがその秘密鍵を取出した時点で，ブラウザとサイトAとの間で安全に秘密鍵の共有ができたことになります．

これで，SSL/TLSのもう1つの役割である，暗号通信のための準備が終了したことになります．その後，ブラウザとサイトAとで共有した秘密鍵を用いて実際の暗号通信が始まります．この暗号通信では共通鍵暗号が使われます．

3．どんな暗号を使いますか？
～共通鍵暗号・公開鍵暗号～

SSL/TLSでは，共通鍵暗号（図3）と公開鍵暗号（図4）と呼ばれる二つの方式を使います．

共通鍵暗号は，暗号化と復号で同じ鍵（秘密鍵と言います）を使う方式で，はるか昔，古代ローマ時代から使われてきました．暗号化処理が高速であるという特長を持つため，主に大きなサイズのコンテンツやメッセージの暗号化に使われています．

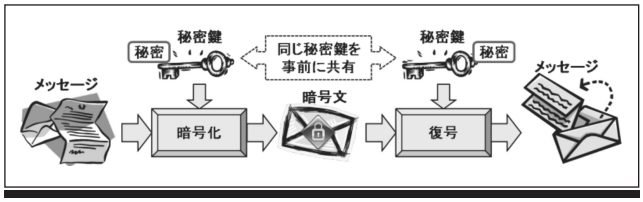


図3　共通鍵暗号

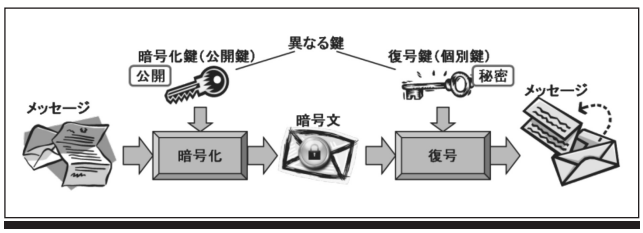


図4　公開鍵暗号

共通鍵暗号で使う秘密鍵は通信相手同士が互いに秘密に持たなければなりません．そのため，通信相手同士が何らかの手段で事前に秘密鍵を安全に共有する必要があります．この欠点を解決したのが公開鍵暗号です．

公開鍵暗号は，暗号化鍵と復号鍵が異なる方式で，その暗号化鍵で作った暗号文は対応する復号鍵でしか元に戻せません．しかも，暗号化鍵は公開することができる一方，復号鍵は一人が秘密にして持てるという特長があります．そこで，前者を公開鍵，後者を個別鍵とも言います．

この特長は，事前に鍵共有を行う必要がない，不特定多数の相手と暗号通信を行う場合に適しています．例えば，不特定多数の利用者を相手にするサイトAでは，サイトAの公開鍵で暗号化してもらうようにすることで，どのブラウザからもサイトAへの暗号通信を事前準備なく始めることができます．

ただし，共通鍵暗号と比較すると，はるかに複雑な計算を必要とするため，暗号化処理が遅く，大きなサイズのコンテンツやメッセージなどの暗号化には向きません．そのため，共通鍵暗号で使う秘密鍵の配送手段として公開鍵暗号を使い，実際のコンテンツやメッセージは共通鍵暗号で行うハイブリッド型（図5）がよく使われます．SSL/TLSはハイブリッド型の典型的な利用例です．

ところで，公開鍵暗号では復号鍵を一人しか持たないことから，その鍵を逆に利用して暗号文を作るとすると，その鍵（この場合は，復号鍵が暗号化鍵になりますが）による暗号文は一人しか作れないともいえます．この概念を応用したものがディジタル署名（図6）です．メッセージに対し，秘密に持つ鍵（署名鍵）で署名を行い，公開されている鍵（署名検証鍵）で署名検証することによって，そのメッセージの正当性と署名者を検証できます．

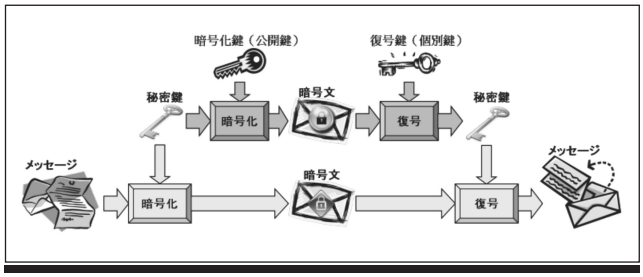


図6　ディジタル署名

4．どうやって相手を信じますか？
～トラストモデル～

4.1　公開鍵暗号基盤

サーバ証明書は，①ブラウザに対して，アクセスした先のサイトAが意図する相手（運営組織等）によって管理されるサーバであることを確認する手段を提供することと，②SSL/TLSによる暗号通信を行うために必要なサーバの公開鍵をブラウザに正しく伝えること，の2つの役割を担っています．前者がアクセスした先のサイトが本物であることの確認のために使われ，後者がブラウザの作った秘密鍵を暗号化してサイトAに安全に送るために使う公開鍵として使われます．

ところで，アクセスした先のサイトAが意図した相手であると確信できるためには“サイトAのサーバ証明書が本物”でなければなりません．そこで，サーバ証明書が本物であると確認できる仕組みが必要となります（図7）．

具体的には，信頼できる第三者としての認証局（CA＊2）が，サイトA自体の存在とサイトAの公開鍵が確かにAのものであるということの両方を確認した後，サイトAの公開鍵に認証局自らのディジタル署名を付与します．これがサイトAのサーバ証明書となります．

ブラウザでは，サイトAのサーバ証明書に認証局の正当なディジタル署名が付いていることを根拠に，認証局によってサイトAの存在が確認されており，かつサイトAの公開鍵が正しいものと判断します．

サーバ証明書の中でも，サーバの運営組織の法的実在性をCA/Browser Forumが規定した国際的な認定基準に基づいて認証局が確認して発行されるサーバ証明書はEV＊3証明書と呼ばれています．ブラウザの「グリーンバー」機能により，有効なEV証明書で運用されているサイトにアクセスするとアドレス表示部分等が緑色になるため（図8の黒枠内），利用者にとって有効なサーバ証明書の視認性が高いものとなっています．

ところで，どうして認証局が信頼できるといえるのかと疑問に思った方もいるかもしれません．勝手に認証局になることはないのでしょうか．

答えから言えば，サーバ証明書の発行プログラムさえあれば誰もがサーバ証明書を自由に作ることができ，認証局の役割を担うことができます．つまり，どの認証局が発行したサーバ証明書かによって信頼性はまったく異なります．

そこで，今度は認証局をどうやって信頼するのかという課題が出てきます．この課題を解決する仕組みが公開鍵認証基盤（PKI＊4）です（図9）．PKIを簡単に言えば，下位の認証局の信頼性を上位の認証局が保証し，その上位の認証局の信頼性をさらに上位の認証局が保証する，といった階層型の信頼スキームのことです．そして，最上位に位置する認証局のことをルート認証局といいます．

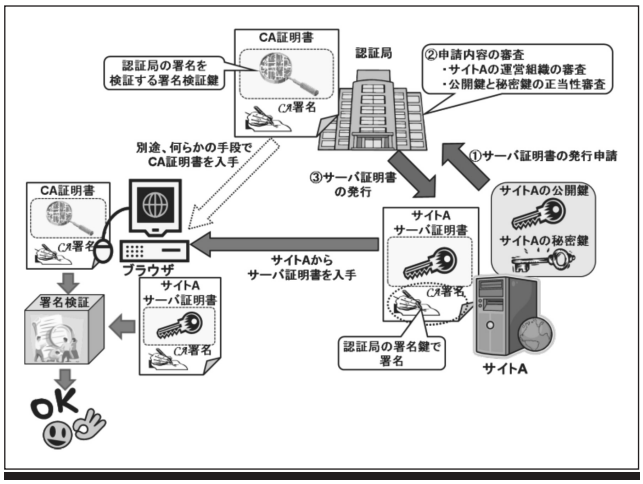


図7　サーバ証明書の使い方

図8　EV証明書を使うサイトでのアドレス表示

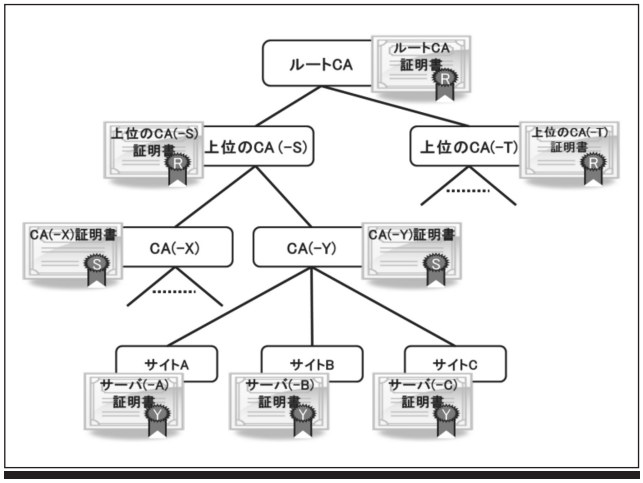


図9　公開鍵認証基盤

Web Trust for CAなどの一定の基準を満たしていることを第三者の監査機関によって審査された代表的なルート認証局は，「信頼されたルート証明機関」や「認証局証明書」として予めブラウザに登録されています．これにより，そのルート認証局が発行するルートCA証明書を信頼起点（トラストアンカ）として，順次検証を行い，最終的にサーバ証明書の正当性を自動的に検証する仕組みになっています（図10）．

4.2　公開鍵暗号基盤の信頼性が揺らいだ事件

とは言え，PKIの信頼性が大きく揺らいだ事件が2009年～2012年に相次いで発覚しています．特に衝撃的だったのは，2008年末に発表されたRapidSSL事件[1]，2011年に起きたDigiNotar事件[2]，2012年に発覚したFlame事件[3]です．

いずれの場合も，ブラウザベンダがルートCA証明書を

＊2　Certification Authority.
＊3　Extended Validation.
＊4　Public Key Infrastructure.

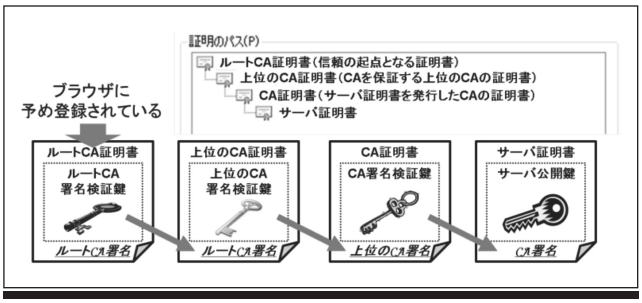


図10　ブラウザでの証明書の自動検証の様子

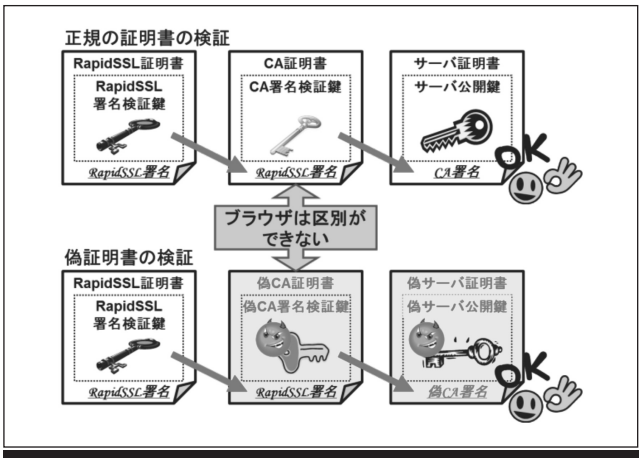


図11　RapidSSLでの偽証明書の検証

失効させるなどのセキュリティパッチを緊急リリースするなどの対策に追われました．

(1) RapidSSL事件

安全性が低下したハッシュ関数MD5の脆弱性を悪用して，偽認証局のCA証明書が偽造された事件で，2008年末のChaos Communication Congressで発表されました[1)]．

この偽認証局のCA証明書は，ルート認証局（RapidSSL）が発行した正規のCA証明書であるとブラウザが判断するように作られていたため，偽認証局が発行した偽サーバ証明書でも，ブラウザは最終的に正しいサーバ証明書であると誤認証してしまうことを実際に示しました（図11）．

この事件は，PKIの中で有効に機能してしまう偽CA証明書が実際に偽造できることを証明するために行われた実験であったため，実害が生じることはありませんでした．ただし，当時はCA証明書やサーバ証明書にMD5を使っているものが少なくありませんでしたが，この事件を契機に多くの認証局がMD5を使うCA証明書やサーバ証明書の発行を取りやめました．

(2) DigiNotar事件

2011年夏に，オランダに本拠を置くルート認証局DigiNotarがComodo hackerと名乗る人物に不正侵入され，少なくとも531枚ものサーバ証明書が不正発行されたことが判明した事件です．そのうち，少なくとも344枚にはGoogle，マイクロソフト，Mozilla，Skypeなど有名なドメイン名が使われ，またイスラエル諜報特務局，英国MI6，米国CIAといった諜報機関のドメインも含まれていました．

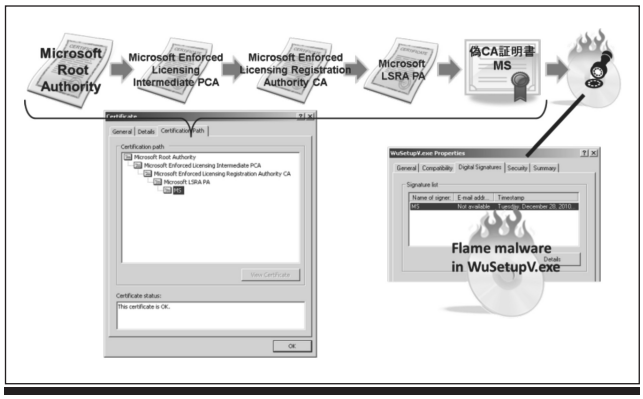


図12　Flameでの検証

この事件は単なる不正侵入事件にとどまらず，①Comodo hackerは約半年前に別の認証局Comodoでも偽サーバ証明書を不正発行させる攻撃に成功していたこと（この事件が発端でComodo hackerとの名がついた），②Comodo hackerはイラン在住の人物であることを名乗っており，実際にDigiNotarから不正発行されたサーバ証明書がイラン政府機関（体制側）等による盗聴行為に利用された可能性があったこと，③マイクロソフト，Mozilla，Google，Appleなどの主要ブラウザベンダがDigiNotarのルート証明書を失効させるセキュリティパッチを緊急発行したこと，④DigiNotarが信用を失って破産したこと，といった実害が発生しました．

(3) Flame事件

サーバ証明書での不正事件とは違いますが，PKIの信頼性を失わせた事件という意味で2012年に発覚したFlame事件も紹介しておきます．

サーバ証明書の代わりにドキュメントやソースコードに認証局の署名をつけるとそのドキュメントやソースコードを認証局が保証したことになります．

Flame事件では，Windowsが上位の認証局が保証したCA証明書と区別できないような偽認証局のCA証明書（図12の偽CA証明書MS）が偽造され，その偽認証局がマルウェアであるFlameを保証していました．しかも，そのときのルートCA証明書がMicrosoft Root Authorityであったため，マルウェアであるFlameがWindows updateの正規対象とWindowsが誤認することとなりました．

この事件が衝撃的なのは，①イランを中心にFlameの感染が拡大しており，発覚する5年以上前から存在していた可能性があること，②米国政府機関がFlameに関与していたと報道されたこと，③イランの核開発を中断させたstuxnetと兄弟的な関係にあるマルウェアであったこと，など，Flameがサイバー兵器としての様相も見せていたことです．しかも，Windows updateの正規対象と見えていたことから，利用者がWindowsのセキュリティパッチを適用したら気付かないうちにFlameに感染した可能性さえあります．

なおFlame事件を受けて，マイクロソフトはWindows updateで使うルートCA証明書とそれ以外の目的で使う

ルートCA証明書を分離しました．この対策により，現在では，非正規な更新プログラムをWindows updateの対象とWindowsが誤認するような事態はなくなりました．

5．どうやって情報を守りますか？
～暗号との関係～

5.1　プロトコルバージョンと暗号スイート

SSL/TLSは鍵交換アルゴリズム，署名アルゴリズム，暗号化アルゴリズム，ハッシュ関数等のアルゴリズム（広い意味での暗号アルゴリズム）が複数組合されたプロトコルです．20年以上使われているため，その間に何度か仕様の見直しが行われ，現在までに5つのバージョンが作られています．また，2000年以前は米国の暗号輸出規制のためにあえて弱い（＝解読しやすい）暗号アルゴリズムしか使えなかったこともあり，仕様上は強い（＝解読が事実上できない）暗号アルゴリズムから弱い暗号アルゴリズムまでさまざまな暗号アルゴリズムが使えるようになっています．

基本的に，プロトコルのバージョンが後になるほど，以前の攻撃に対する対策が盛り込まれ，また強力な暗号アルゴリズムも利用できるようになるなど，より安全性が高くなっています（表1）．

実際にどのプロトコルバージョンと暗号アルゴリズムを暗号通信で使うかは，サイトの確認や秘密鍵の交換をするときに，サーバとブラウザの両方が実装しているプロトコルバージョンと暗号アルゴリズムのなかから決めています．なお，利用する暗号アルゴリズムは「鍵交換__署名__暗号化__ハッシュ関数」の組で構成された暗号スイートの形で決まっています．選択された暗号スイートに記載された鍵交換，署名，暗号化，ハッシュ関数の各暗号アルゴリズムによりSSL/TLSにおける各種処理が行われますので，どの暗号スイートが選ばれるかによって使われる暗号アルゴリズムが異なり，SSL/TLSにおける安全性が変わります．

ちなみに，SSL/TLSの仕様上，どのような優先順位でプロトコルバージョンや暗号スイートを選択するかは明確には決められておらず，サーバやブラウザの設定によって異なります．このため，同じサイトにアクセスしても使うブラウザによって異なるプロトコルバージョンや暗号アルゴリズムが使われることがあります．

5.2　最近のSSL/TLSへの攻撃

ここ数年，SSL/TLSへの攻撃が相次いでいます．ここでは，有名な攻撃の概要を紹介します．

（1）BEAST攻撃やPOODLE攻撃など

ID/パスワードの入力を要求するサイトにおいて，ブラウザを閉じた直後にもう一度そのサイトにアクセスするとIDやパスワードを入力していないのにブラウザを閉じる前のページがそのまま表示された経験がないでしょうか．

これは，Cookieと呼ばれるデータにログイン状態などを記録してサイトとブラウザとの間で一定時間共有することにより，そのCookieを使ってアクセスしてきたブラウザに対してサイトが自動的に元のログイン状態に戻しているために起きている現象です．多くの場合，セッションIDと呼ばれる情報でログイン状態を管理しており，暗号化された状態でサイトとブラウザに記録されます．

ここ数年，相次いで公表されたBEAST攻撃[4]やPOODLE攻撃[5]などは，暗号化されたCookie（セッションID）の中身を攻撃者が知ろうとする攻撃方法です．上記のCookieの仕組みから，これらの攻撃に成功すると，ユーザUのCookie（セッションID）を攻撃者が自由に使うことができるようになり，ユーザUのID/パスワードを知らなくてもそのサイトAにユーザUに成りすまして不正アクセスできることになるからです．

これらの攻撃方法の詳細な説明は省略しますが，技術的には共通鍵暗号のなかのブロック暗号で長いメッセージの暗号化を行うモードであるCBCモードで利用したときの脆弱性を利用した攻撃とされています．攻撃方法の原理は，以下の攻撃条件がそろった時に，暗号化されたCookieについて1バイトずつ攻撃者が中身を知ることができるような攻撃方法を構築でき，それを繰り返すことでCookie全体の情報がわかるようになるというものです．ここでのポイントは，攻撃者が秘密鍵を知らなくても暗号化されたCookieの中身を知ることはできるということです．

- 攻撃対象のブラウザUにマルウェアを感染させる等により，攻撃者がブラウザUからサイトAに任意のメッセージを同じ秘密鍵で暗号化させたうえで大量に送信できる状態にできる
- 攻撃者は，ブラウザUからサイトAに送るメッセー

表1　プロトコルバージョンの違い

		TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
	開発年数	2008	2006	1999	1995	1994
SSL/TLSへの攻撃方法に対する耐性	ダウングレード攻撃（最弱の暗号アルゴリズムを強制的に使わせることができる）	安全	安全	安全	安全	脆弱
	バージョンロールバック攻撃（SSL2.0を強制的に使わせることができる）	安全	安全	安全	安全	脆弱
	ブロック暗号のCBCモード利用時の脆弱性を利用した攻撃（BEAST/POODLE攻撃など）	安全	安全	パッチ適用要	脆弱	脆弱
利用できるより安全な暗号アルゴリズム	128ビットブロック暗号（AES，Camellia）	可	可	可	不可	不可
	認証付暗号利用モード（GCM，CCM）	可	不可	不可	不可	不可
	楕円曲線暗号	可	可	可	不可	不可
	SHA-2ハッシュ関数（SHA-256，SHA-384）	可	不可	不可	不可	不可

ジの中身を自由に加工できる
・攻撃者は，ブラウザUからサイトAに送る暗号化されたパケットをすべて傍受できる

これらの攻撃を防ぐために，CBCモードを利用したときの脆弱性が使われないようにする対策*5が考案されており，これらの対策はセキュリティパッチ等の形ですでに広く配布されています．したがって，セキュリティパッチを適用することが対策となります．

また，これらの攻撃方法が成功するためには，攻撃者がブラウザUを自由にコントロールできることが必要ですので，マルウェアの感染を防止するなどの対策も有効です．

(2) RC4の脆弱性を利用した攻撃

RC4は1987年に開発された共通鍵暗号の1つです．RC4ではキーストリームという秘密の情報を生成して暗号化していきますが，そのキーストリームの出力分布に微妙な偏りがあり，大量の異なる秘密鍵で統計解析をするとある程度キーストリームの出力分布を識別できるという脆弱性があります．

この脆弱性を使った攻撃方法[6]が提案されており，詳細な説明は省略しますが，攻撃原理は，異なる秘密鍵で同じ内容のメッセージを大量に送信した時に得られる暗号文を集めて統計解析すると，RC4のキーストリームの出力分布に依存する形になることを用います．そこから，キーストリームの影響を取り除くと，もともとのメッセージに復元できます．例えば，2^{32}個の暗号文があれば最初の257バイト分のメッセージを高確率で求めることができます．

この攻撃は大量の暗号文を必要とする点で直ちに現実的な脅威になるというわけではありませんが，防御策がないという点で，現在ではRC4を使わないようになってきています．

(3) Heartbleed：実装の脆弱性を利用した攻撃

2014年4月に発覚したHeartbleedは，TLS1.2の拡張機能として組込まれた，サーバの動静を簡易に確認するHeartbeatの実装上の脆弱性を利用した攻撃[7]です(図13)．

SSL/TLSそのものに対する攻撃ではありませんが，SSL/TLSの機能をサーバに実装するためのオープンソースライブラリーであるOpenSSL(もしくは暗号化ソフト)の致命的な脆弱性としてニュースでも大きく取り上げられたため，ご存知の方も多いかと思います．

具体的にはOpenSSLでのHeartbeatの実装において，メモリーサイズのチェックを充分にしない脆弱性があったために，OpenSSLを使って構築したSSL/TLSサーバでは返信すべきデータに隣接するメモリー領域のデータまでも返信してしまいました．その中にパスワードやクレジット番号などがたまたま含まれていると，それらが漏えいしたことになります．

問題は，①OpenSSLを使っているサーバが多数あること，②この脆弱性が2年以上も対策されずにいたこと，③意図せず偶然持っていかれたデータなので漏えいした内容の特定が困難であること，④サーバ側に攻撃の痕跡が残らないため攻撃されているかどうかの判断さえも困難であること，といった点にあります．そのため，被害の全容を把握することができず，重要なデータが漏えいしたとの前提で対策することが必要となりました．現在では，この脆弱性を修正したバージョンのOpenSSLがあり，対策されています．

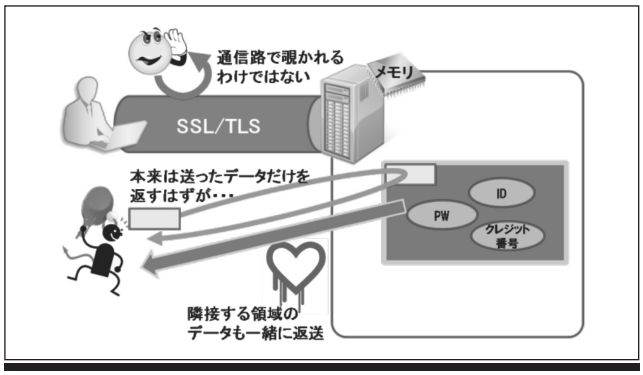


図13　Heartbleed

*5　POODLE攻撃については，強制的にSSL3.0にダウングレードさせたうえで攻撃する方法があり，SSL3.0の仕組み上，対策が困難とされています．

6．むすび

SSL/TLSは，電子商取引での利用をはじめとして，インターネット社会においてなくてはならないセキュリティプロトコルです．ただ，20年以上も前に開発されたプロトコルであるうえ，相互接続性を優先させてきた背景から，さまざまな点で脆弱性があることも事実です．

今回，SSL/TLSがどのような仕組みで動いているのかを知ることで，皆さんがより安全にSSL/TLSを使えるようになっていただければ幸いです．

(2014年11月27日受付)

〔文　献〕

1) MD5 considered harmful today, http://www.win.tue.nl/hashclash/rogue-ca/
2) Black Tulip Update, http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update.html
3) Microsoft releases Security Advisory 2718704, http://blogs.technet.com/b/msrc/archive/2012/06/03/microsoft-releases-security-advisory-2718704.aspx?Redirected=true
4) BEAST, http://vnhacker.blogspot.jp/2011/09/beast.html
5) B. Möller, T. Duong, and K. Kotowicz: "This POODLE Bites: Exploiting the SSL 3.0 Fallback", https://www.openssl.org/~bodo/ssl-poodle.pdf
6) T. Isobe, T. Ohigashi, Y. Watanabe, and M. Morii,: "Full Plaintext Recovery Attack on Broadcast RC4", Proc. of FSE '13, pp.179-202 (2013)
7) The Heartbleed Bug, http://heartbleed.com/

神田　雅透(かんだ　まさゆき)　1993年，東京工業大学大学院修了．同年，NTT入社．NTT研究所にて，共通鍵暗号の研究に従事し，Camelliaの設計に関わる．現在，NTTセキュアプラットフォーム研究所主任研究員．2009年より，IPA非常勤研究員として暗号政策の調査等にも関与する．平成26年度文部科学大臣表彰，第53回前島賞等受賞．

マルウェア対策

井上大介†

1．マルウェアとは？

サイバー攻撃は日々高度化を続け，その攻撃対象は一般ユーザから企業，政府官公庁まで多岐にわたっています．サイバー攻撃は1990年代の前半までは愉快犯的なものや自己顕示を目的としたものが多かったのですが，1990年代後半以降は金銭詐取を目的としたものが大半を占めるようになってきました．さらに2000年代に入ると，示威活動（ハクティビズム）や諜報活動（サイバーエスピオナージ）のために行われるサイバー攻撃が出現し，攻撃の目的自体も多様化が進んでいます．このようなサイバー攻撃において，頻繁に利用されるプログラムを「マルウェア」と呼びます．

マルウェアは英語のMalicious（悪意のある）とSoftwareを組合せた混成語であり，ユーザの望まない不正な動作を行うプログラムの総称として，2001年頃から広く使われるようになった用語です[1]．それ以前は，このような不正なプログラムを（広義の）ウイルスと呼ぶことが多かったのですが，ウイルスの多様化が爆発的に進み，その感染形態や機能，目的などによって数多の用語（2章参照）が乱立することとなりました．そこで，多様化・高度化・悪質化する不正なプログラムを統一的に表現する新たな用語が，社会的に，また学術的にも必要とされた結果，マルウェアという言葉が世界規模で認知され定着することとなったと考えられます．

図1はワームと呼ばれるタイプのマルウェアが，日本に向けて大量の攻撃を送信している様子をリアルタイムに可視化したものです．このように，インターネット上ではマルウェアによる攻撃が常態化しており，マルウェア対策は社会的な課題となっています．

2．マルウェア関連用語

マルウェアに関する用語は，その感染形態や目的，機能など，異なる切り口による分類から生み出されたものが混在しており，さらにそれらの用語について厳密なコンセンサスが形成されているわけではありません[2]．本章では，いくつかの分類に絞ってマルウェア関連用語を紹介します．

2.1　マルウェアの感染形態に着目した分類

・ウイルス（Virus）

ウイルス（狭義のウイルス）とは，それ単体では動作せず，自分自身を他のファイルやプログラムに寄生させる感染形態のマルウェアを指し，感染対象によって，ブートセクタ感染型とファイル感染型に大別できます．前者は，フロッピーディスクやハードディスクなどのシステム領域を感染対象とし，後者は実行可能ファイルを主な感染対象とします．ウイルスの中には，他のウイルスを感染対象とするものも存在します．

・ワーム（Worm）

ワームとは，狭義のウイルスのように宿主となるファイルやプログラムを必要とせず，単体で動作し自己増殖を行う感染形態のマルウェアを指します．一般に狭義のウイルスに比べ高い感染力を有し，大規模感染を引き起こす傾向にあります．ワームの感染手法には，電子メールやリムーバブルメディア(USBメモリーなど)を移動媒体とするもの，Windowsのファイル共有やメッセージング機能を利用するもの，そしてOSやアプリケーションの脆弱性に対する攻撃コードを用いるもの，などが存在します．

・トロイの木馬（Trojan Horse）

トロイの木馬とは，ギリシャ神話のトロイア戦争で計略に用いられた木馬に倣い，有用なプログラムやファイルを装ってユーザ自身によるシステムへの導入・起動を誘い，実際にはユーザの意図しない不正な動作を行うマルウェアを指します．トロイの木馬の多くはユーザの不注意を利用してシステムへの侵入を果たすため，感染機能を持っていません．

上記以外にも，フィルタドライバとして実装され，OSのカーネルの深部に潜伏する巧妙な感染形態を持つマルウェアも少なからず存在しています．例えば，マルウェアのファイルやプロセスをアンチウイルスソフトやタスクマネージャに対して隠蔽するルートキット（Rootkit）や，

† 独立行政法人情報通信研究機構 ネットワークセキュリティ研究所 サイバーセキュリティ研究室
"Security Technologies on Image Information (4); Countermeasures against Malware" by Daisuke Inoue (Cybersecurity Laboratory, Network Security Research Institute, National Institute of Information and Communications Technology, Tokyo)

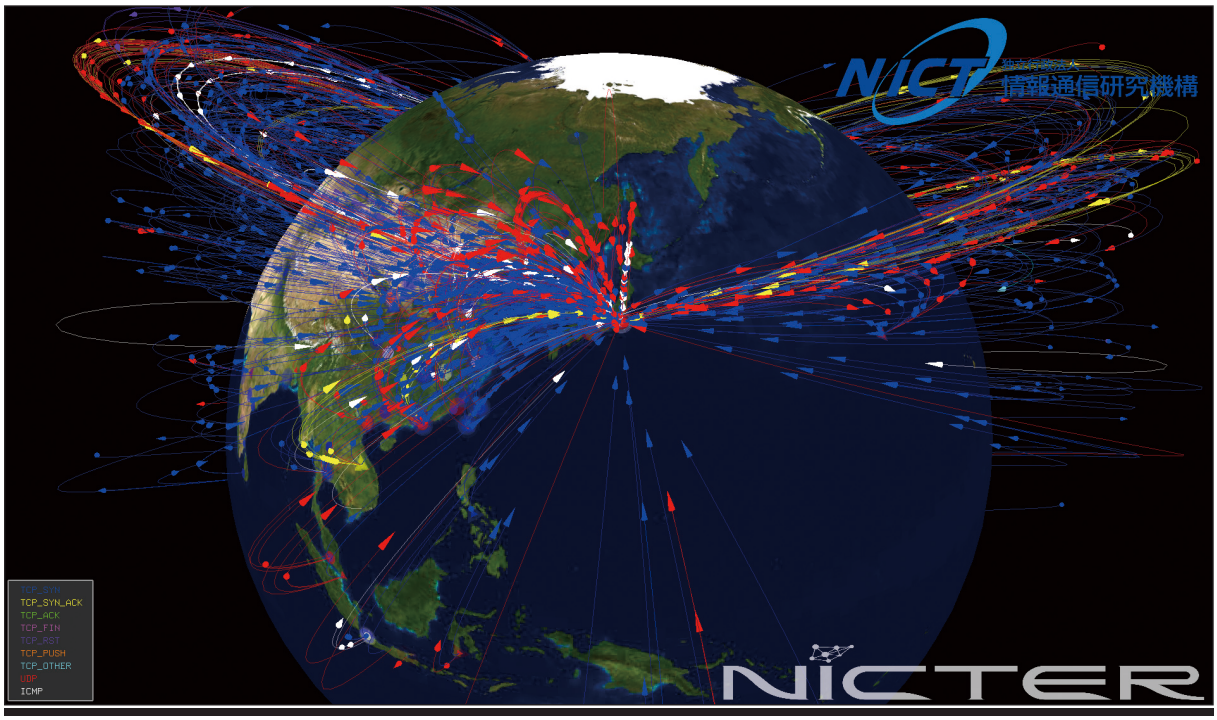


図1　マルウェアによるサイバー攻撃の可視化

ユーザのキーボード操作を記録・収集するキーロガー（Keylogger）などの多くは，この感染形態を取っています．

2.2　マルウェアの目的に着目した分類

・スパイウェア（Spyware）

スパイウェアとは，ユーザのPC上で個人情報や行動履歴を収集し，特定のサーバなどに送信することを目的としたマルウェアを指します．キーロガーも目的という点ではスパイウェアの一種と考えられます．

・アドウェア（Adware）

アドウェアとは，ユーザに企業広告などを提示することを目的にしたプログラムであり，無害なアドウェアも存在する一方，ユーザの同意なしに広告を頻繁にポップアップしたり，ユーザの意図しないWebサイトに強制誘導したりするものはマルウェアと見なされます．

・ランサムウェア（Ransomware）

ランサムウェアとは，ユーザのPC上のディレクトリやファイルに対して強制的に暗号化やパスワード付きZIP圧縮を行うことで，ユーザのデータを「人質」にし，そのデータの復号や解凍の見返りとして，ユーザから身代金（ransom）を詐取することを目的としたマルウェアです．

・スケアウェア（Scareware）

スケアウェアとは，ユーザに虚偽の情報を提示し不安（scare）を煽ることで，無意味なソフトウェアを販売することを目的としたマルウェアです．典型的な例として，偽のマルウェア感染情報をユーザに提示してWebサイトに誘導し，実際には何の機能も有さないプログラムをアンチウイルスソフトと称して販売しようとするものがあります．

2.3　マルウェアの機能に着目した分類

・ダウンローダ（Downloader）

ダウンローダとは，それ自身とは別のマルウェアを特定のサイトからダウンロードし，感染PCにインストールする機能を持ったマルウェアです．最近のマルウェアの多くは，感染後にダウンローダを多段に用いることで解析を困難にしたり，定期的にダウンロードを繰り返したりすることで，新しい機能を持ったマルウェアを容易に拡散させることが可能になっています．

・ドロッパ（Dropper）

ドロッパとは，マルウェアを内包した状態で流通し，ユーザのPC上で実行されると，暗黙のうちにマルウェアをインストール（ドロップ）する機能を持ったマルウェアです．ドロッパの中にはMicrosoft Wordなどの文書ファイルになりすまし，実行されると実際の文書を表示すると同時にマルウェアをインストールするという巧妙なものも存在します．

2.4　その他の分類

・ボット（Bot）

ボットとはロボットの短縮語であり，指令者からの遠隔操作によって，多岐にわたる活動，目的，機能を実現するマルウェアです．ボットに感染したPCはボットネットと呼ばれる一種のオーバレイネットワークを形成します．ボットネットは小規模なものでは数百，大規模なものでは数十万もの感染PC群によって成り立っています．指令者は，指令サーバ（IRCサーバやHTTPサーバ）経由でボットネットに制御命令を同報し，その結果，多数のボットが命令にしたがって一斉動作を行います．今日，ボットネット

はスパムメールの大量送信や，DDoS攻撃，大規模な感染活動などさまざまなセキュリティインシデントの源泉となっています．

3．マルウェア観測・収集技術

マルウェア対策を行うためにはまず，インターネット上でマルウェアの活動を観測し，マルウェアの検体（マルウェアの実行ファイル）を収集する必要があります．マルウェア観測・収集技術は受動的手法と能動的手法に大別できます．

3.1　受動的観測・収集技術

マルウェアを受動的に観測・収集するために，ダークネットと呼ばれるインターネット上の未使用のIPアドレスブロックに各種のセンサを設置する手法が多く用いられています．

未使用のIPアドレスに対しパケットが送信されることは，通常のインターネット利用の範囲においては発生する可能性が低いですが，実際にダークネットを観測してみると相当数のパケットが到着していることがわかります（図1はダークネットに届くパケットを観測・可視化したもの）．これらのパケットの多くは，ワーム型のマルウェアが次の感染先を探索するために送信する，スキャンと呼ばれる通信です．そのため，ダークネットに到着するパケットを大規模に観測することで，インターネット上で発生しているワーム型マルウェアの不正な活動の傾向把握が可能になります．また，スキャンに対して適切な応答を行うことで，マルウェア検体を取得することも可能です．

ダークネット観測を行う場合，センサと呼ばれるパケット収集・応答用のサーバマシンを設置します．センサは，パケットの送信元に対する応答の程度によって次のように分類されます．

(1) ブラックホールセンサ：パケットの送信元に対し，まったく応答を行わないセンサ．メンテナンスが容易であり大規模なダークネット観測に向きます．無応答であるため，外部からセンサの存在を検知することが困難であるという利点もあります．マルウェアの感染活動の初期段階であるスキャンは観測可能ですが，それ以降の挙動を観測することはできません．

(2) 低インタラクションセンサ：パケットの送信元に対し，一定レベルの応答を返すセンサ．TCP SYNパケットに対してSYN-ACKパケットを返すセンサや，OSの既知の脆弱性をエミュレートするセンサなどがここに含まれます．観測しているポートの傾向などからセンサの存在を検知され易く，アドレスが連続した大規模なダークネットでの運用には不向きです．

(3) 高インタラクションセンサ：実ホスト，もしくはそれに準じた応答を返すセンサ．マルウェア感染時の挙動や攻撃者のキーストロークまで多様な情報が取得可能ですが，実際にマルウェアがシステムに感染するため，安全な運用を行うためのコストは高く，大規模運用には不向きです．

低インタラクションセンサと高インタラクションセンサは，マルウェアを招き寄せることからハニーポットとも呼ばれ，マルウェア検体を捕獲する機能を有します．特に高インタラクションセンサは，OSの機能を忠実に再現することで（あるいは実際のOSを用いてハニーポットを構築することで），未知のマルウェアを捕獲できるポテンシャルを有します．

3.2　能動的観測・収集技術

ダークネット観測は受動的な（待ち受け型の）観測手法であり，インターネット上で無作為に行われる大規模な攻撃の観測に適しています．その一方，マルウェア側から能動的に攻撃を仕掛けないような攻撃活動を観測することは困難です．例えば，ユーザがWebサイトを閲覧した際に，ユーザのWebブラウザもしくはWebブラウザが利用するプラグインやアプリケーションの脆弱性が悪用され，ユーザが気付かないうちにマルウェアのダウンロードと実行が行われるドライブバイダウンロード[3]と呼ばれる攻撃は，ダークネット観測では捉えられない事象です．

このような攻撃活動を観測するために，能動的にWebサイトを巡回して，不正なサイトを検知・収集するクローリング技術が使われます．この技術はクライアントハニーポット[4]とも呼ばれ，スクリプトなどを使ってクライアントを模擬してWebコンテンツを取得する低インタラクション型と，実際のOS環境やWebブラウザを使う高インタラクション型に大別されます．前者は自動化や並列化が容易でありコンテンツの取得も高速ですが，未知の脆弱性を模擬することは困難です．後者は実環境を用いるため，未知の脆弱性を突くマルウェアを取得できる可能性がありますが，クロール速度が遅く，実際にシステムへの感染を行わせるため運用コストも高くなります．

4．マルウェア解析技術

前章のような観測・収集手法でマルウェア検体を取得した後，マルウェアの解析が行われます．マルウェア解析の手法は大別すると，動的解析と静的解析の二つのアプローチに分けられます．

4.1　動的解析

動的解析はブラックボックス解析とも呼ばれ，マルウェアの検体を犠牲となるマシンの上で実際に実行して，マルウェアの挙動をAPIフックなどの技術を用いてトレースし，またマルウェアのネットワークアクセスなどを解析するものです[5]．動的解析は解析の自動化が比較的行いやすく，大量のマルウェアを高速に解析することが可能ですが，実行時に呼び出される機能以外は解析できないため，マルウェアが持つ機能全体を自動的に解析することは困難です．

4.2　静的解析

静的解析はホワイトボックス解析とも呼ばれ，マルウェ

アの実行コードを逆アセンブルして，アセンブリレベルでマルウェアの持つ機能や特徴を詳細に解析するものです．最近のマルウェアには逆アセンブルを阻害する難読化やアンチデバッグ機能が備わっているものが多いため，静的解析を完全に自動化することは難しく，高度な技術を持つ解析者による手動解析が主流です．

マルウェア解析は，マルウェアが持つ耐解析機能との戦いであり，さまざまな解析ノウハウが存在します．マルウェア解析の具体的な詳細については文献6）を参考にしてください．

5．マルウェア検知技術

マルウェア解析によって得られた知見をベースにして，マルウェア検知が行われます．マルウェア検知は，アンチウイルスソフトに代表されるホストベースと，侵入検知システムなどのネットワークベースに大別できます．

5.1　ホストベースの検知技術

・シグネチャマッチング

アンチウイルスソフトの多くは，マルウェアに含まれる特徴的なコードなどを事前にシグネチャ（定義ファイルやパターンファイルとも呼ばれる）として定義しておき，ホスト上でそのシグネチャと合致したものをマルウェアとして検出します．この手法は，シグネチャマッチング方式と呼ばれ，既知のマルウェアには高い検出率を示しますが，シグネチャの存在しない未知の（あるいは亜種の）マルウェアを検出することは困難です．今日のマルウェアの多くは，シグネチャによる検出を逃れるための難読化（パッキング）が施されており，機能は同等でも異なるコードを持つマルウェアが大量に発生しています．そのため，アンチウイルスソフトのシグネチャの更新が間に合わず，多くのマルウェアが見過ごされているのが現状です[7]．

・ヒューリスティック検知

未知や亜種のマルウェアを検知できないというシグネチャマッチング方式の問題点を補うため，ヒューリスティック検知方式では，マルウェアが行う特徴的な「挙動」を定義しておきます．そして，ホスト上のプロセスを監視し，マルウェアに類似した挙動を行うプロセスを検知するため，未知や亜種のマルウェアであっても検知できる可能性があります．その一方で，正常なプログラムをマルウェアとして誤検知することもあり，一長一短があります．

5.2　ネットワークベースの検知技術

・侵入検知システム/侵入防止システム

侵入検知システム（IDS: Intrusion Detection System）と侵入防止システム（IPS: Intrusion Prevention System）は，インターネットと組織のローカルネットワークの境界で，組織外からの攻撃を検知（アラート発報）あるいは防止（遮断）するシステムです．両システムとも多くの場合，ホストベースのシグネチャマッチングと同様に，攻撃に用いられるトラフィックのパターンをシグネチャ化しておき，シグネチャに合致した通信を検知・遮断します．侵入検知システムは組織のコアスイッチなどからミラーされたトラフィックを監視することが多いですが，侵入防止システムは不正な通信を遮断するためにインラインでの監視が必要となります．

・URLブラックリスト

マルウェア配布サイトやボットの指令サーバなど，不正なURLをブラックリスト化しておき，組織内のホストがブラックリストに合致した宛先と通信を試みた場合に，アラート発報あるいは通信を遮断する方式です．URLブラックリストは3.2節で述べたクローリング技術などで検知された不正サイトの情報を基に更新されていきますが，その網羅性や迅速さが課題となっています．

・サンドボックス

サンドボックスはマルウェアの動的解析で用いられる箱庭環境ですが，組織のローカルネットワークを流れる通信の中からファイルなどを抜き出し，サンドボックス内で実行させてマルウェアを検知する方式です．最近のマルウェアにはサンドボックスによる解析を回避する機能を持っているもの（Evasive Malware）もあり[8]，解析機能と解析回避機能のいたちごっこがここでも起こっています．

6．新たな対策技術

侵入検知システムや侵入防止システムなどの従来のマルウェア対策技術の多くは，組織のローカルネットワークがインターネットと接続しているネットワーク境界において，組織外からのサイバー攻撃を検知・防御する「境界防御」が主流となっています．しかしながら，USBメモリーやメールの添付ファイル，持ち込みPCなど組織内を始点としたマルウェア感染によって境界防御を突破されるセキュリティインシデントが多発しており，従来の境界防御の仕組みを補完するセキュリティ対策の重要性が増しています．

そこで，情報通信研究機構で研究開発を進めている対サイバー攻撃アラートシステムDAEDALUS（ダイダロス）*は，マルウェア感染を完全に防止することは困難であるという事故前提の考え方に基づき，感染後の対策として，組織内のマルウェア感染端末（特にワーム型マルウェア）を早期検知し，その組織に向けたアラートの発報を可能にする，新たな対策技術です．

DAEDALUSが攻撃を検知し，アラートを発報する仕組みは非常にシンプルであり「特定の組織からダークネットにパケットが届くとその組織に向けてアラート発報する」というものです．3.1節で述べた通り，ダークネットに届くパケットの大部分はマルウェアに起因した不正な通信であり，その送信元はマルウェアに感染している疑いが強いと考えられます．そこで，その送信元IPアドレスを使用して

＊　Direct Alert Environment for Darknet and Livenet Unified Security.

図2　DAEDALUS-VIZの可視化画面

いる組織にアラートを発報することで，迅速なインシデント対応のトリガとなります．

図2はDAEDALUSのアラート発報状況を俯瞰的に把握するための可視化エンジンDAEDALUS-VIZ[9]の表示画面です．中央の球体がインターネット，その周りを周回している各リングが，ブラックホールセンサを設置している組織のネットワークを表しています．球体とリングの間を飛び交う流星状のオブジェクトはダークネットへの通信を表しています．リングの水色部分がライブネット（使用中のIPアドレスブロック），濃紺部分がダークネットであり，リングの外周の「警」のマークは組織内でアラートの原因となった送信元IPアドレスを指し示しています．DAEDALUS-VIZ上でアラートが表示されるとほぼ同時に，該当組織には電子メールでアラートが自動送信されています．

この攻撃検知，可視化，アラートシステムにより，より早く組織内のマルウェア感染に対応することが可能となります．

7．むすび

マルウェアは日々高度化を続けており，マルウェア対策技術も持続的な進化を遂げてきています．マルウェアによる攻撃は元来視認できないものですが，その脅威に迅速かつ適切に対応するため，本稿で述べた対策技術に加えて，可視化技術も重要な研究テーマとなっています．映像情報メディアの力を借りつつ，マルウェア対策技術を向上させ，安心・安全な社会の構築を進める必要があります．

（2015年1月16日受付）

〔文　献〕

1）瀬戸洋一ほか：“情報セキュリティ概論”，日本工業出版（2007）
2）NIST: "Guide to Malware Incident Prevention and Handling", NIST Special Publication 800-83（2005），http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
3）N. Provos, D. McNamee, P. Mavrommatis, K. Wang and N. Modadugu: "The Ghost in the Browser: Analysis of Web-based Malware", HotBots'07（2007）
4）M. Akiyama: "Study on High Interaction Client Honeypot for Infiltrative Intrusion Detection", NAIST Academic Repository（2013）
5）D. Inoue, K. Yoshioka, M. Eto, Y. Hoshizawa and K. Nakao: "Automated Malware Analysis System and its Sandbox for Revealing Malware's Internal and External Activities", IEICE Trans. On Information and Systems, E92-D, 5, pp.945-954（2009）
6）新井悠，岩村誠，川古谷裕平，青木一史，星澤裕二：“アナライジング・マルウェア”，オライリージャパン（2010）
7）S. Gibbs: "Antivirus software is dead, says security expert at Symantec", the Guardian（2014），http://www.theguardian.com/technology/2014/May/06/antivirus-software-fails-catch-attacks-security-expert-symantec
8）C. Kruegel: "Full System Emulation: Achieving Successful Automated Dynamic Analysis of Evasive Malware", Black Hat USA（2014）
9）D. Inoue, K. Suzuki, M. Suzuki, M. Eto and K. Nakao: "DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System", 9th International Symposium on Visualization for Cyber Security（VizSec 2012），pp.72-79（2012）

井上　大介（いのうえ　だいすけ）　2003年，横浜国立大学大学院工学研究科博士課程後期修了後，通信総合研究所（現（独）情報通信研究機構）に入所．2006年より，インシデント分析センターNICTERの研究開発に従事．現在，情報通信研究機構ネットワークセキュリティ研究所サイバーセキュリティ研究室室長，同機構サイバー攻撃対策総合研究センター（CYREC）サイバー防御戦術研究室室長（兼務）．2002年，暗号と情報セキュリティシンポジウム論文賞，2009年，科学技術分野の文部科学大臣表彰（科学技術賞），2013年，グッドデザイン賞，2014年，Asia-Pacific Information Security Leadership Achievements等を受賞．博士（工学）．

パスワードの安全性

金岡　晃†

1．パスワードとは

情報通信が社会的基盤として広まった今，通信の先にいる相手が誰なのかを保証する認証（Authentication）は必須の技術です．米国標準技術研究所（NIST: National Institute of Standards and Technology）が定めた文書SP 800-63-2「電子的認証に関するガイドライン」[1]では，認証システムは以下の三つの要素から認証を行うとされています．

(1) Something you know（記憶による認証）
(2) Something you have（所持による認証）
(3) Something you are（生体情報による認証）

パスワードはこのうち記憶による認証にあたります．

本稿ではパスワードに使われる技術の概要とパスワードに関するセキュリティについて解説します．

2．パスワードによる認証の流れ

パスワードによる認証の流れを図1に示します．利用者は自分自身のIDと記憶してあるパスワードを入力します．認証サーバはまず利用者のIDを使い，サーバが持つデータベース（DB）より同じIDを持つ情報を調べ，登録されているパスワードを取り出します．そして入力されたパスワードと一致するかを確認し，認証の成功あるいは失敗を通知します．

大まかな方式は図1の通りですが，いくつかの観点からそのままでは利用者の保証がなされません．

まず送信時の第3者による覗き見（盗聴）の危険性があります．もしIDとパスワードがそのままの情報（平文）で送信され，その情報が通信路の途中で第3者により覗き見られる可能性がある場合，第3者がIDとパスワードを知ることになり「本人以外が知らない」ことで担保される記憶による利用者認証の保証が崩れます．その対策として，通信路の暗号化があげられます．Web上のサービスでパスワード認証を行う場合は，このセキュリティ講座第3回[2]で説明しましたTLS（Transport Layer Security）を用いた通信路の暗号化が一般的です．

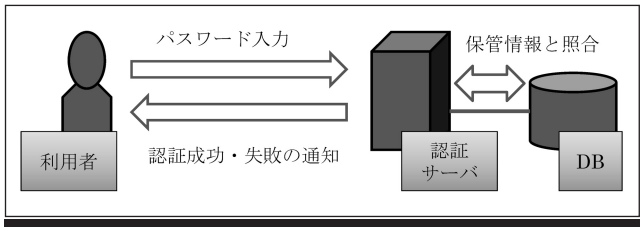


図1　パスワード認証の流れ

続いて，サーバDBでのパスワードの保管方法に気を配らなければなりません．サーバDBにパスワードが平文で保管されている場合，サーバの管理者は各利用者のパスワードを知ることができます．そのため，覗き見の場合と同じく本人以外が知ることとなり利用者認証の保証が崩れます．その対策として，データをランダムな値に圧縮する暗号学的ハッシュ関数（以下単にハッシュ関数と呼ぶ）を用いた方式が導入されます．利用者が入力したパスワードはハッシュ関数に通されてハッシュ値が生成され，DBに保管されます．ハッシュ関数の特性により，ハッシュ値からハッシュ関数に入力されたデータ（パスワード）を求めることは困難です．認証時は，入力されたパスワードから同様にしてハッシュ値を生成し，そのハッシュ値と保管されているハッシュ値が一致するかを確認します．図2にその流れを示します．DBの情報が漏えいしたとしても，漏えい情報を取得した者はハッシュ値のままでは認証に利用できないため，情報漏えいの対策にもなっています．

これらにより通信路上の第3者，そして認証を行うサーバ管理者が利用者のパスワードを知ることへの対策がなされます．

3．パスワード認証に対する攻撃

パスワードで認証を行うシステムに対し，悪意のある第3者が行う行為（攻撃）は，なりすましが主なものです．この攻撃の成功にはIDとパスワードのペアを知らなければなりません．第3者がIDとパスワードを得る攻撃は，主に以下のものに分類されます．

† 東邦大学
"Security Technologies on Image Information (5): The Security of Passwords" by Akira Kanaoka (Toho University, Chiba)

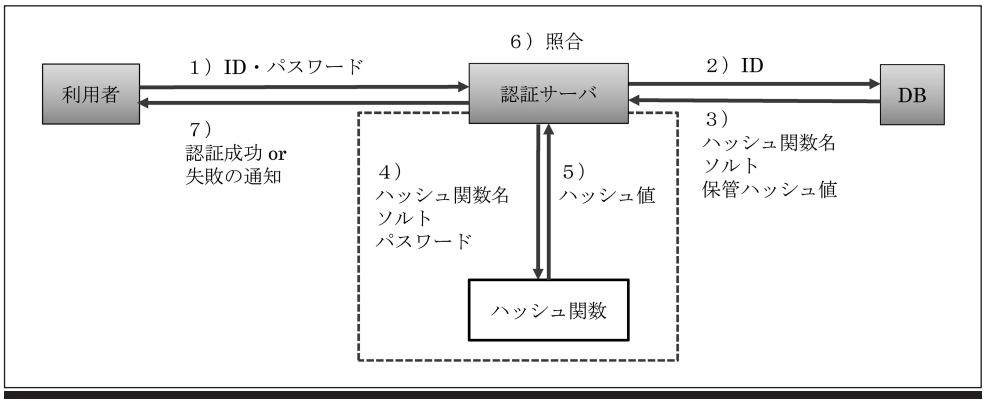


図2　ハッシュ関数を用いたパスワード認証

(1) オンライン攻撃
(2) オフライン攻撃
(3) ソーシャルエンジニアリング

オンライン攻撃とオフライン攻撃は，ともに考えうるパスワードの種類（またはIDとパスワードの組合せ）を試行するもので，総当たり攻撃と呼ばれます．

オンライン攻撃は，実際のサービスに対して（オンラインで）パスワードを総当たりで入力するものです．オンライン攻撃に対しては，一定時間内で認証を失敗する数に応じて，サービスを中断したりアカウントを凍結するなどの対処により脅威を回避できます．総当たり攻撃では通常は攻撃対象となるIDを固定して総当たりを仕掛けます．アカウント凍結によりその攻撃は回避することができますが，アカウント凍結を避ける方法として，パスワードを固定してIDを総当たりにするリバースブルートフォース攻撃もあります．IDに何らかの規則性や制限がある場合や，パスワード自体も制限があり複雑なパスワードが利用できない場合では，このリバースブルートフォース攻撃の脅威が増加します．国内で発生したある航空会社サイトへの不正アクセスでは，このリバースブルートフォース攻撃が行われたのではないかと言われています．

オフライン攻撃は，何らかの方法で取得したIDとパスワードのハッシュ値に対して，実際のサービスを使うことなく（オフラインで）一致するパスワードを探すもので，攻撃者のコンピュータで実行可能です．

とは言うものの，オフライン攻撃は簡単には行えません．ハッシュ値がとりうる値は，例えば，SHA-256の場合はハッシュ値のデータが256ビットになるため，2^{256}通りになります．これらに対して総当たりを行うことは多大な時間と多くのCPU等のリソースが必要です．

ハッシュ値のオフライン攻撃を強力に行う方法としてレインボーテーブルがあります．レインボーテーブルはあらかじめ計算しておいたハッシュ値とその入力データのペアを保存してあるDBであり，ハッシュ値を毎回計算するのではなく，一致するものを探すだけで総当たりと比べて圧倒的に早くキーワード(パスワード)を探すことかできます．ハッシュ値の探索の効率は，テーブルの構成方法や実装に依存しますが，探索自体は通常のデータ探索方法でも用いられる効率の良い探索方法が利用可能なため高速に探索が可能です．当然，レインボーテーブルを作成することは総当たり攻撃を行うことと同じ労力を要しますが，レインボーテーブルは1度作成すれば再利用が可能です．レインボーテーブルは販売されているものもあることから，金銭コストを負担すれば容易にオフライン攻撃ができるようになります．

レインボーテーブルを用いたオフライン攻撃への対策には，ソルトの導入があります．パスワードのハッシュ値生成の際，ハッシュ関数への入力にパスワードだけではなく乱数のSalt（塩）を入れるものです．これによって，同じパスワードでも乱数ごとに異なるハッシュ値が現れることになります．サーバ側ではハッシュとともにソルトを保管しておき，認証時は利用者から入力されたパスワードと保管されたソルトでハッシュ値を計算し，保管されたハッシュ値と比較します．ハッシュ値とソルトが漏えいした場合には，総当たりによるオフライン攻撃は変わらず可能ですが，レインボーテーブルを用いた攻撃は難しくなります．

Linuxではパスワードの保管にソルトを用いることが一般的です．パスワードは利用されたハッシュ関数とソルト，ハッシュ値の組で保管されます（図3）．このときハッシュ

```
$6$oEvgDECg$9YAGJc7ttuXe7bG（中略）XBY3uCt9F7KEmvhr/
①    ②                    ③
```

①：ハッシュ関数の種類（6はSHA-512を示す）
②：ソルト
③：ハッシュ値
※一般的には/etc/shadow として格納されている

図3　Linuxにおけるパスワードの保管情報

関数を繰り返し用いて計算するストレッチングも用いられます．Windowsでは，LMハッシュとNTハッシュの二つの方式が用いられています．LMハッシュは共通鍵暗号であるDESを用いたハッシュ値生成方法で，NTハッシュではパスワードをハッシュ関数MD4でハッシュ化します．どちらもソルトは使われていません．Windows Vista以降ではNTハッシュだけが利用されています．

パスワード認証への攻撃耐性を持たせるために認証回数制限や，ソルトの追加，ストレッチング処理を用いたハッシュ値生成を行うことで，攻撃者に残された方法はオフライン攻撃において総当たりすることのみとなります．つまり，サーバ側が検討すべきパスワードの安全性はこのオフライン攻撃だけを考えれば良い，ということもできます．

4．パスワードの情報量

このような総当たり攻撃への耐性を情報量（エントロピー）として表すこともあります．NISTのSP 800-63-2[1]では，Appendix Aにおいてパスワードの情報量が議論されています．パスワードを利用者が選択した場合とランダムに選択した場合では，その情報量に差があることを数値で示しています．ASCIIのPrintable Characters 94文字を用いた場合，利用者選択（制限なし）の場合18ビット，ランダム選択の場合52.7ビットの情報量がある，としています．この情報量が大きいほどパスワードは安全となります．以下では，パスワードの安全性，その強度を判断する指標として情報量を用います．

利用者による選択では偏りが生じることから，パスワードがランダムに選択される場合と利用者が選択する場合では情報量に差が出ています．パスワードは記憶による認証であるため，利用者の振る舞いにその強度が大きく依存します．

利用者が選択するパスワードの強度については，面白い調査結果も存在します．2010年にWeirらは大規模な漏えい事件により得られた3,200万の利用者のパスワードを解析し，その特徴をさまざまな角度から示しました[3]．そこでは現実に利用者に選択されたパスワードが持つ情報量が，NISTの予想している情報量よりも低いことが示されています．また，パスワードをすべて数値で設定している利用者が全体の20.51%であることや，パスワード内に数値を設定する場合には，パスワードの最後に数値を付け足す形に設定する利用者が全体の64.28%であることなどが示されています．その他，いくつかの興味深い結果も得られていますので以下に列挙します．

(1) 大文字小文字混在の7文字パスワードの場合
- すべて大文字のパスワードが全体の53.56%
- 頭文字だけ大文字のパスワードが全体の35.69%

(2) 記号利用パスワードの場合
- 最後の1文字だけ記号を利用するパスワードが全体の28.50%

(3) 記号利用のパスワードの各記号の利用率
- “.”の利用が17.81%
- “_”の利用が14.72%
- “！”の利用が11.34%
- “－”の利用が10.25%

5．ソーシャルエンジニアリング

パスワードの情報量は利用者の振る舞いにその強度が大きく依存したことは先ほど述べました．この「利用者の振る舞い」のように，人間の行動や心理を逆手に取った攻撃手法があります．オンライン攻撃，オフライン攻撃とは別に，効果的であるといわれるソーシャルエンジニアリングです．上司や関係者などを騙り利用者から聞き出すことや，ログイン画面の覗き見など社会的な手段でIDとパスワードを取得する方法です．

米国のあるブログメディアのライターが，ソーシャルエンジニアリングによりTwitterのアカウントやGmailアカウント，Apple IDアカウント情報を不正に操作されたという事例があります．そこでは，攻撃者によるアカウント名の推定や，サービス提供会社への電話連絡による新しいクレジットカード情報の登録やパスワードの変更依頼などが行われていました．

6．パスワードの強化方法

利用者の振る舞いがパスワードの強度に大きく影響する点に注目し，利用者の振る舞いを制限するなどしてパスワード強化を狙う方法がいくつかあります．本稿では，そのうちパスワードの構成ポリシとパスワードメータ，パスワードマネージャについて紹介します．

パスワード構成ポリシは，パスワード構成時に一定のルールを設け，ルールに沿ったパスワード構成を利用者に強制するものです．代表的なものとして，最少の文字数を設定するものや，IDと同じパスワードを禁止するもの，辞書に載っている言葉をそのままパスワードに設定することを禁止するもの，などがあります．2012年にKelleyらはパスワード構成ポリシの効果について大規模な調査を行い，どのような構成ポリシがパスワード強化に効果があるかを示しました[4]．そこでは複雑な構成ポリシ（最低8文字＋辞書に含まれる用語排除＋大文字・小文字を含む＋記号含む＋数値含む）よりも，単純に最低文字長を16文字に拡大したポリシのほうがより強いパスワードが生成される傾向があることが示されました．前述したNIST文書[1]でも同様にパスワード構成ポリシの違いによる情報量を予想していますが，ここでもその数値との乖離が指摘されました．しかしこの指摘は，NISTが予想する情報量が大きすぎるというものではなく，実際の情報量のほうが大きい，つまりパスワード構成ポリシは，NISTの予想以上に効果が高

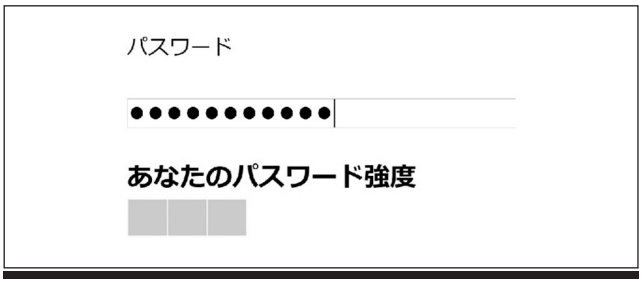


図4　パスワードメータの例

いとの指摘でした．

パスワード構成ポリシとともに近年よく採用されるのがパスワードメータです．利用者がパスワード設定をする際，入力されたパスワードの強度を自動的に計算し，その強度をリアルタイムで表示するものです．段階的に棒や線のような絵柄を伸ばしていくものや，数値を示すもの，あるいは“Good”，“Fair”のように評価の文だけを示すものがあります．またそれぞれの表示に赤・黄・緑で色付けをしてその安全性を強調するものも多くあります（図4）．パスワードメータの効果については，2012年にUrらが網羅的な調査を行いました[5]．Urらの実験では，「メータなし」と14種類のメータを用意し，それぞれで被験者を用いたパスワード生成実験を行い，メータによるパスワード強度の効果を測定しました．その結果，もっとも弱いパスワード構成がされる場合は「メータなし」であり，他のいずれのメータもメータなしと比較して高い強度を持つことが示されました．もっとも高い強度を示したものには，実際のスコアの半分のスコアしか表示しないメータと，実際のスコアの1/3のスコアしか表示しないメータの二つが挙げられました．メータ表示の種類ではなく，スコアの計算方法の違いによる強度向上が見られたことは興味深い点です．

パスワードの保管方法や高強度のパスワード構成の促進方法は，いわばサービス提供者側の対応であると言えます．しかしネットワークにつながるサービスが一般化するにつれ，提供者側だけではなくサービス利用者側の対応も必要になってきました．1人の利用者がさまざまなサービスを利用することが普通になり，サービスごとに複数のIDやパスワードを持つことが求められるようになりました．人間の記憶には限界があり，また利用するサービスの頻度はサービス毎にまちまちであるため，すべてのIDとパスワードを別々に設定し正確に記憶することは困難です．そのため，利用者は同じあるいは類似したIDとパスワードを利用する傾向がでてしまいます．これを悪用した攻撃がリスト型攻撃と呼ばれるものです．あるサービスから漏えいしたIDとパスワードのペアを，他のサービスの認証で試行する攻撃です．リスト型攻撃はパスワードの記憶管理の問題点を突いたものと言えます．

利用者による複数サービスのIDとパスワードの管理問題の対策として，ここではID連携とパスワードマネージャを紹介します．

ID連携は，サービスごとにIDとパスワードを設定し，サービス提供者がその認証機構と認証情報を持つのではなく，IdP（Identity Provider）と呼ばれるIDの提供者が認証機構と認証情報を持ち，各サービス提供者はIdPに認証の委託とIDに関する情報の交換を行うことにより，提供者自身で認証情報を持たずとも適切にサービス提供が可能になるものです．

パスワードマネージャは，利用者が使うクライアント環境で動くソフトウェアであり，さまざまなサービスのIDとパスワードを利用者に代わり管理・保存するものです．利用者は個別のIDとパスワードを設定・記憶する必要がなくなるため，利用者の負荷を下げるメリットがあります．しかし，認証に関する多くの情報をそのマネージャが持つこととなり，信頼性の点で非常に重要な役割を背負うことになります．そのために高いリスクを持つことも指摘されています[6)7)]．例えば，パスワードマネージャ自身のセキュリティが低いものであれば，利用者のパスワードがさまざまなサービスにおいて悪用をされてしまう可能性が高くなります．

7．多要素，多段階での認証

パスワードの管理の難しさやリスト型攻撃への対策には，パスワード強化以外のアプローチもあります．記憶による認証であるパスワードとそれ以外の要素（例えば，所持による認証）を併せて二つの要素で認証するケースもあります．例えば，Web上でのログインの際に，あらかじめ登録しておいた携帯電話のメールアドレスにサービス提供者よりメールが送られ，メール上に記載された情報をログイン時に入力させる手法などがあります．メール自体は所持による認証にはあたりませんが，携帯電話のメールアドレスは，利用者個人が持つ携帯電話に紐づいていることから所持による認証として扱っています．また銀行などのWebサービスでは，利用者に時刻により数値が変動するワンタイムパスワードトークンを配付し，ログイン時にはID・パスワードとともにトークンに表示されている数値を入力させています．トークンの時計とサーバ側の時計がある程度同期がとれており，なおかつそのトークン以外には次の数値を計算することが困難になるように設計されています．

またパスワードだけではなく，他の秘匿情報と合わせて認証するケースもあります．これはいずれも記憶による認証であることから単一の要素ではありますが，段階を複数回経ていることから多段階認証とも呼ばれます．多段階認証では，生年月日や秘密の質問などが多くみられますが，それらはいずれもパスワードの強化にはなりえないことに注意が必要です．それらの情報は，その利用者の周辺を調

査することができれば比較的容易に得られる情報です．SNS（ソーシャルネットワーキングサービス）上は意図せず利用者が開示した情報で溢れていると言えます．例えば，生年月日の場合，利用者は自身の生年月日を公開こそしていませんが，友人たちによるサプライズを込めたプレゼントに対して，その光景を感想とともに掲載してしまうことは良くある風景であり，そのことから生年月日は類推可能となります．またSNSには生年月日を登録そして公開可能にしているものもあります．

8．パスワードを超えて

パスワードは長い歴史を持っており，情報通信技術の発展に従い，その管理の難しさが指摘されてきています．本稿で述べたように，さまざまな面で対策がなされてきていますが，いずれも本質的な解決にはなっていないことは否定できません．そういった点に対し，これまでさまざまな認証方式がパスワードに代わるべく提案されてきましたが，残念ながら，いまだパスワードを代替する技術とはなりえていません．Bonneauらは2012年にこれまで提案されてきた多くの認証方式とパスワードについて，25の評価項目を用意し，35の方式に対して評価を行いました[8]．評価項目は大きく利便性を示す“Usability”，容易に適用可能かを示す“Deployability”，安全性を示す“Security”の三つの軸に分けられ評価がされましたが，パスワード以外のさまざまな手法は，Security項目においてパスワードを超える評価を得ているものの，Usabilityが低いものが多くありました．なにより特徴的なことは，すべての認証方式がいずれもDeployabilityにおいてパスワードと同等あるいはそれ未満であると評価されたことです．パスワードのDeployabilityの高さが示された結果となりました．

そして最近では，論文で現れるような先端研究だけではなく，実用面でもパスワードによる認証に代わる手段の提供を推進する動きが出てきています．アップル社が提供する決済機能「Apple Pay」では，iPhoneの指紋認証センサ「Touch ID」とNFC（Near Field Communication）と呼ばれる近距離無線通信技術を使い，パスワードを使わない認証で決済を行っています．またマイクロソフトやグーグルを含む複数の企業から構成されるFIDO（First Identity Online）アライアンスから2014年12月に発表された仕様では，まずクライアント側で認証を行い，認証がクライアントで成功した後に，公開鍵暗号技術を用いてクライアントとサーバ間でのチャレンジ－レスポンスの認証を行います．クライアント側での認証は，指紋認証やPIN（Personal Identification Numberの略であり，パスワードと同様に利用者の記憶する情報により認証されます．4桁の数字が代表的です）などが利用可能ですが，どの認証を利用するかはサービスを提供する側が指定可能になっていますが，身近になった指紋認証がパスワード入力に代わるものとして期待されていることが伺えます．マイクロソフト社は次期のWindowsであるWindows 10にFIDOを採用すると発表しており，今後の広まりに注目です．

Bonneauらの論文で指摘されたDeployabilityの問題解決は，二つの方法があると考えられます．一つはよりDeployabilityの高い方式の検討です．そしてもう一つはDeployabilityが低いとされている方式をなんとか普及させることでDeployabilityを高める方法です．世界中で大きなシェアを持つ企業が導入することや，複数企業が協力をすることで導入を推進する，といった手段がありますがいずれも簡単ではありません．ようやく最近になりアップル社のApple Payの仕組みやFIDO仕様が出てきました．今まさにパスワードを超えた認証方式が広まる大きな転機を迎えているのかもしれません．

今後の研究や実用化において，Deployabilityの高さを併せ持つ認証方式の登場と世の中への展開を期待したいと思います．そして一般利用者がより安心して情報通信のサービスを広範に受けられるようになることを願います．

（2015年2月4日受付）

〔文　献〕

1）NIST Special Publication 800-63-2: "Electronic Authentication Guideline", Aug. 2013）
2）神田：“SSL/TLSの仕組みを知っていますか？”，映情学誌，69，3，pp.228-233（2015）
3）M. Weir, S. Aggarwal, M. Collins and H. Stern: "Testing metrics for password creation policies by attacking large sets of revealed passwords", Proc. of ACM CCS'10, pp.162-175（2010）
4）P.G. Kelley, S. Komanduri, M.L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L.F. Cranor and J. Lopez: "Guess again（and again and again）: Measuring password strength by simulating password-cracking algorithms", Proc. of IEEE S&P'12, pp.523-537（2012）
5）B. Ur, P.G. Kelley, S. Komanduri, J. Lee, M. Maass, M.L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin and L.F. Cranor: "How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation", Proc. of USENIX Security Symposium'12, pp.65-80（2012）
6）D. Silver, S. Jana, D. Boneh, E. Chen and C. Jackson: "Password Managers: Attacks and Defenses", Proc. of USENIX Security Symposium'14, pp.449-464（2014）
7）Z. Li, W. He, D. Akhawe and D. Song: "The Emperor's New Password Manager: Security Analysis of Web-based Password Managers", Proc. of USENIX Security Symposium'14, pp.465-479（2014）
8）J. Bonneau, C. Herley, P.C. Oorschot, F. Stajano: "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", Proc. of IEEE S&P'12, pp.553-567（2012）

金岡（かなおか）　晃（あきら）　2004年，筑波大学大学院博士課程システム情報工学研究科修了．同年，セコム（株）入社．筑波大学システム情報工学研究科研究員，同助教を経て，2013年より，東邦大学理学部講師．2010年より，情報通信研究機構招聘専門員兼務．セキュリティとプライバシのユーザビリティ，暗号技術の応用，リスクの定量化に関する研究に従事．

講座

映像情報メディア関連のセキュリティ〔第6回〕

共通鍵暗号

渡辺　大†

1．まえがき

暗号技術の起源は紀元前にまで遡り，主に軍事目的で，秘密裏に情報をやりとりする技術として発達してきました．しかし，昨今では，インターネットを中核とするIT技術の普及に伴い，私たちの日常を支える技術として発展を続けています．

本講座でも，これまで暗号技術にまつわるトピックが何度か取り上げられていますが，これから数回に分けて暗号技術とはどのようなものなのか，もう少し掘り下げて見ていきたいと思います．今回はその第一歩としまして，昔からある共通鍵暗号の現在について紹介します．

共通鍵暗号の用途は，ざっくり言うと「データの保護」です．では，データの保護とはどういうことでしょうか？もちろん，「データがなくならないように保管する」という観点もありますが，セキュリティ的な観点からすれば

(1) データを共有すべき人以外にはデータが見えないようにしたい（情報の秘匿）

(2) データが勝手に書換えられては困る（情報の完全性保証）

という2点が主な課題になります．これらの課題をどのように解決するか，ここから議論したいと思います．

2．共通鍵暗号と公開鍵暗号

暗号技術は，共通鍵暗号と公開鍵暗号の2つに分けられます．共通鍵暗号とは，通信する二者間で同じ秘密鍵を共有することで，秘密通信を実現します．一方の公開鍵暗号は，暗号化で使う鍵と復号に使う鍵が異なるのが特徴です．

共通鍵暗号は古来より使われてきた暗号化方式ですが，「どうやって秘密鍵を共有するか？」という課題があります．軍事目的で使われていた頃は，通信相手が特定できていたため，出発前にあらかじめ秘密鍵を渡しておく，という方法でこの問題を解決していました．しかし，インターネットのように不特定多数との通信を前提とする社会では，この方法は使えません．この課題を解決するのが公開鍵暗号です．

公開鍵暗号では，データを暗号化するときに使う鍵（公開鍵と呼びます）と暗号化されたデータを復号するときに使う鍵（秘密鍵と呼びます）は，2つで対となる，異なる値です．また，公開鍵から秘密鍵を推定することが難しいという特徴があります．ある人（アリスさんとします）が対となる公開鍵と秘密鍵を生成したとします．そして，暗号化に使う公開鍵だけ公開します（これが名前の由来です）．この公開により「誰でも暗号化できる」ようになります．ただし，「復号できるのは秘密鍵を持っているアリスだけ」というシステムができます．

このように，公開鍵暗号は共通鍵暗号に比べていろいろな使い方ができるのですが，残念ながら，処理が複雑なために暗号化/復号処理に時間がかかってしまうというデメ

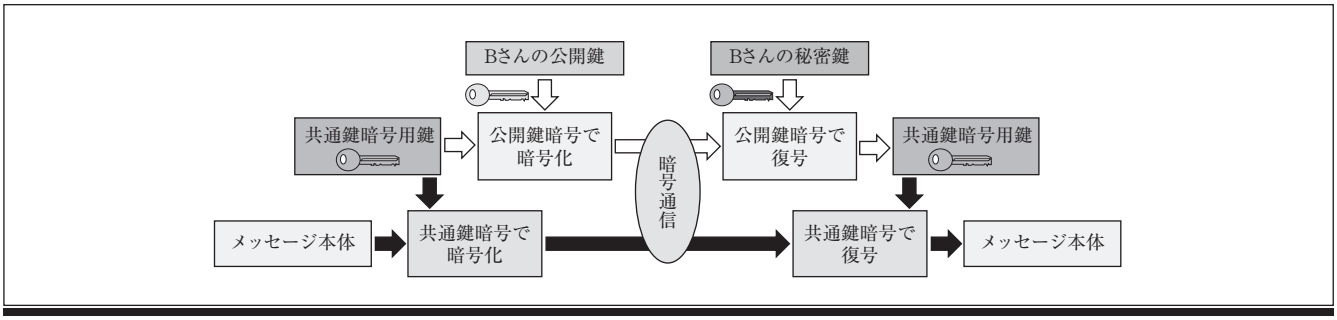


図1　ハイブリッド暗号

† 株式会社日立製作所横浜研究所

"Security Technologies on Image Information (6); Symmetric Key Encryption" by Dai Watanabe (Yokohama Laboratory, Hitachi, Ltd., Yokohama)

リットがあります．そこで，鍵共有には公開鍵暗号を，データが大きいコンテンツの暗号化には共通鍵暗号を，という感じで用途に応じて暗号の種類を使い分けるのが一般的な利用法です．図1に共通鍵暗号と公開鍵暗号をハイブリッドに使用した，メッセージの伝送方法を示します．

3．データの暗号化と情報の秘匿

前者の課題を解決する基本的な手段はデータを暗号化して，秘密鍵を持っている人だけが読めるようにすることです．歴史上でも，紀元前から暗号が使われていたことが知られており，スパルタのスキュタレー暗号や，ローマのシーザー暗号が有名です．ちなみに，スキュタレー暗号は，文章を共有したい人が同じ太さの棒(スキュタレー)を持ち，棒にでたらめに見える文字列が書かれた革ひもを巻きつけると，棒の長さ方向に文章となる方式です．図2にその例を示します．ひもには「いちよらろりたむちはぬ…」という訳のわからない文字列が書かれています．この紐を棒に巻くと「いろはにほへと…」と読めるわけです．少し専門的に言うと，一種の転置処理であり，文字の順番を入れ替えて読むことで元の平文がわかるわけです．棒の太さが鍵になっています．シーザー暗号は，文章を共有したい人がある数値を共有し，アルファベットをその数値分だけずらした(一種の換字処理をした)文章を送受する方式です．送り手がアルファベットを3つずらせば，受け手は反対方向に3つずらせば平文を読むことができます．このずらす幅が鍵となっています．図3にひらがなを利用したシーザー暗号の例を示します．ここでは3文字ずらすことが鍵となっており，「はなのいろはうつりにけりな…」という文章が「へうやにほへおらをとえをう…」という暗号文になっています．

現在では，データの暗号化を行う技術はより高度化しています．暗号化方式を大きく分けるとストリーム暗号とブロック暗号の二つになります．ストリーム暗号はデータを乱数でマスクする方法です．ブロック暗号は，データをブロック単位に区切り，秘密の置換テーブルを使って別の値に置換する方法です．1ブロックの大きさ(ブロック長)は，通常8バイトか16バイトです．ここで「置換テーブルを使って変換する」と書きましたが，ブロック長が8バイトの場合

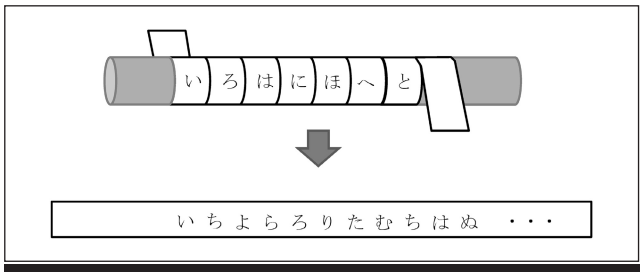


図2　スキュタレー暗号

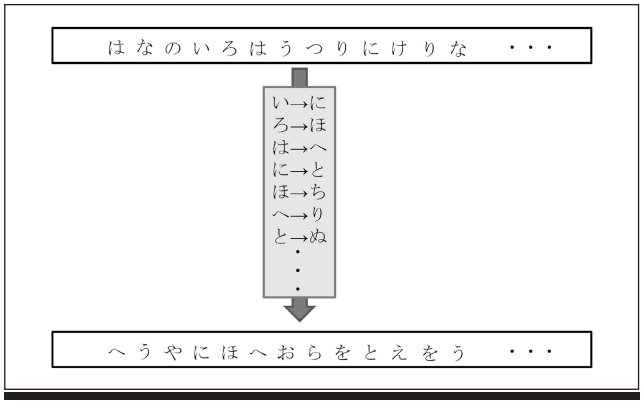


図3　シーザー暗号

でも，置換テーブルの大きさは($2^{64}\times8\times2=$)256 EB(エクサバイト：1 EB=10^{18}バイト)になってしまいます．現実には変換テーブルをメモリー上に持っておくかわりに，特定のアルゴリズムにしたがって，テーブルの値を毎回計算しています．

はじめての商用暗号(アルゴリズム公開型暗号)であるDES(Data Encryption Standard)[1]のインタフェースは，ブロック長64ビット，鍵長56ビットです．開発当時から，DESの鍵長は安全性の観点から短すぎるのではないか，という懸念がありました．計算機の処理能力が大きくなるにつれ，この懸念が大きな問題になってきます．そこで，RSA社は，1997年からDESの解読コンテストを開催し，鍵の総当りがどれくらい現実的であるかを明らかにしようとしました．表1に解読コンテストの結果を示します．初回のチャレンジでは，7万台のPCを使って鍵の総当り探索を行い，96日で解読に成功しました．また，2年後の1999年に開催された第3回のチャレンジでは，10万台のPCに加え，

表1　ブロック暗号の解読コンテスト

対象暗号	鍵　長	コンテスト名	解読日	解読時間	計算量
DES	56ビット	DES Challenge	1997/1	96日	PC約7万台
		DES Challenge II-1	1998/1	39日	PC約5万CPU
		DES Chal	1998/7	56時間	専用ハードウェアDES Cracker(制作費25万ドル)
		DES Challenge III	1999/1	22時間15分	DES Cracker+ PC 10万台
RC5-64	64ビット	RC5-64 Secret-Key Challenge	2002/9	約4年	PC約7万台
SHA-256＊	—	ビットコインの採掘	2015/3時点	2^{58}回/秒	—

＊現在の計算リソースを過去のコンテスト時と現在の計算リソースとを比較するために表に掲載しました．
SHA-256の安全性が損なわれているわけではありません．

専用の解読用ハードウェアを使って，解読時間を22時間まで短縮しています．かなりの計算コストではありますが，DESチャレンジは，DESを安全に使える時代の終わりを告げるものでした．

余談になりますが，最近では，ネットとコンピュータを用いて一儲けを考えている人たちの間で，ある膨大な計算を行い，解答を出すことで，ネット上でやり取りされている仮想通貨であるビットコインを大量に入手できる（“金脈を掘り当てる”と言われています），いわゆる“採掘”を目的として暗号処理（ハッシュ関数SHA-256）の計算が大量に行われています．ビットコインに関する最新の統計情報を提供しているBlockchain.info[2]を見れば，現時点でどれくらいの暗号計算ができるのか，簡単に調べることができます．試しに，採掘状況を調べてみると，なんと1秒にハッシュ関数の計算を2^{58}回以上実行していました（2015年3月19日時点）．これは，DESの鍵を1秒に4個解読できてしまう，ということを意味しています．金の採掘を目的とする欲望の前では，56ビットというDESの鍵が提供する安全性がいかに脆弱なものなのか，おわかりいただけるのではないでしょうか．

DESの延命を図る技術として，Triple-DESという方式が導入されました[1]．これは，DESの暗号化処理を3回繰り返す，というもので，2つの鍵を使うものと，3つの鍵を使うものがあります．処理速度を犠牲にして，安全性を改善するというわけです．

しかし，より根本的な解決を目指すべく，DESチャレンジと時を同じくして，米国標準技術研究所（NIST: National Institute for Standards and Technology）は，DESの後継を担う暗号の選定プロジェクトを開始しました[3]．次世代標準暗号（Advanced Encryption Standard: AES）の選定は，プロセスの透明性を重視し，オープンなコンペティション方式で行われました．コンペティションには，世界中から21のアルゴリズムが応募され，3年をかけて審査が行われました．審査の内容は，安全性の観点での評価に加えて，ICカードやPC，ハードウェアを含むさまざまなプラットフォームにおける実装性能評価が行われました．安全性評価についても，当初想定されていた以上に厳しい審査が行われ，評価技術の向上にも繋がりました．このように，多大なコストをかけて行われたプロジェクトの結果，当時ベルギーの学生であったRijmen氏とDaemen氏が提案したRijndaelがAESに選ばれました．余談ですが，Rijndaelという名称は，提案者の名前を繋げたものなのだそうです．AESの標準仕様は2001年に文書化され[4]，現在に到るまでインターネットで使われている暗号の主流となっています．

4．ブロック暗号（AES）のアルゴリズム

それでは，共通鍵暗号の代表格であるAESの暗号化アルゴリズムを簡単に紹介しましょう．AESはブロック長が128ビットで，DESのブロック長の2倍あります．また，鍵長は128ビット，192ビット，256ビットの3種類が用意されています．

次に処理構造を見ていきましょう．図4にブロック暗号の

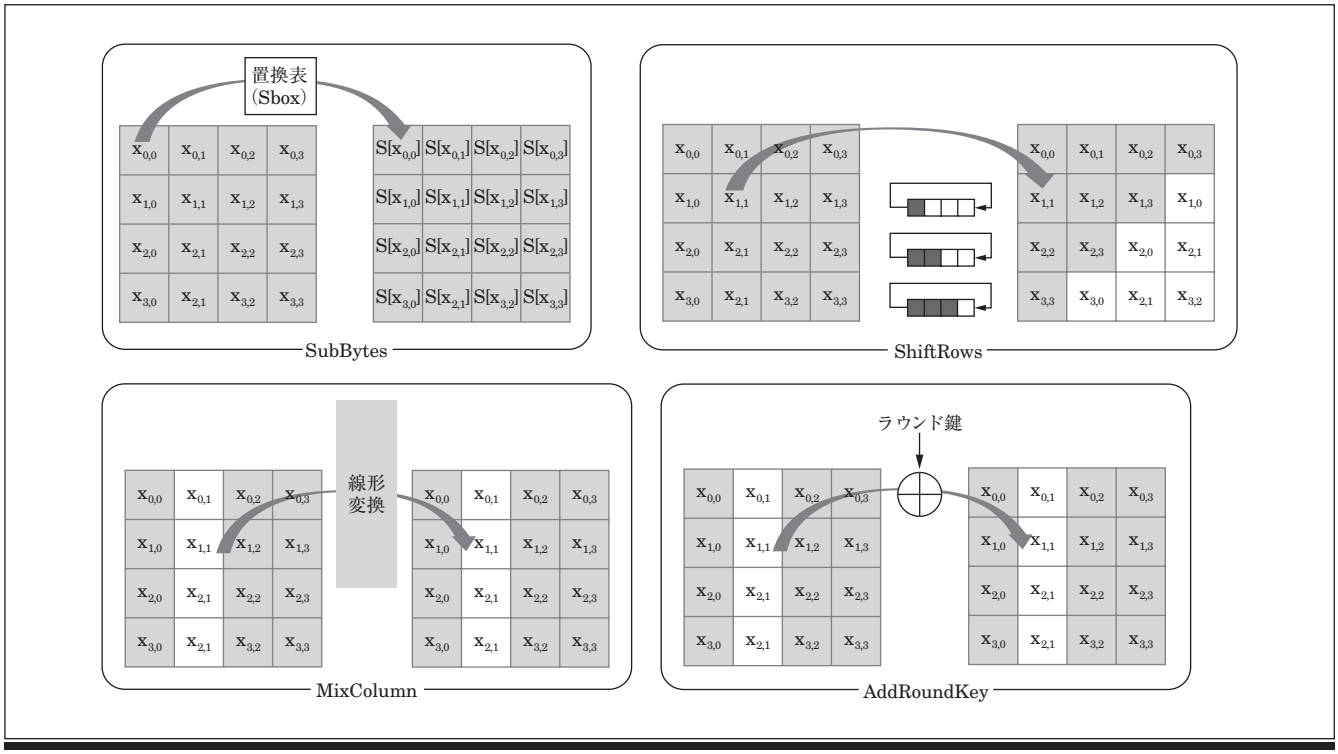


図4　ブロック暗号の基本構造

基本構造を示します．ブロック暗号の暗号化関数は，一般的にデータランダム化部と鍵スケジュール部とに分けられます．データランダム化部は，ラウンド関数と呼ばれる処理の繰り返しになっています．ラウンド関数は，毎回異なるラウンド鍵を使いますが，秘密鍵からラウンド鍵を生成するのが鍵スケジュール部です．一般には，ラウンド処理の回数が多いほど，より安全になると考えられており，AESは鍵長が128ビットの場合は10ラウンド，鍵長が256ビットの場合は14ラウンドの処理を行います．

ブロック暗号の設計でキモとなるのが，ラウンド関数です．AESのラウンド関数は，128ビットの入力に対し，SubBytes, ShiftRows, MixColumns, AddRoundKeyという4つの処理が順番に行われ，128ビットのデータを出力する関数です．それぞれの処理を図5に示します．

いずれもバイト単位の処理になっていることが，AESの特徴の1つになっています．SubBytesは，1バイトデータの置換表(S)を使って，128ビット(16バイト)の値を1バイトずつ置き換えます($x_{i,j} \leftarrow S[x_{i,j}]$)．ShiftRowsは，バイトの位置を入れ替えます($x_{i,j} \leftarrow x_{i,j+i \bmod 4}$)．つまり，SubBytesはシーザー暗号に代表される換字処理，ShiftRowsはスキュタレー暗号に代表される転置処理を行っているわけです．しかし，これだけではバイト単位の出現頻度分布が変わりませんので，次のMixColumnsで，4バイトを一括で線形変換($f_i()$)する多文字変換処理を行います($x_{i,j} \leftarrow f_i(x_{0,j}, x_{1,j}, x_{2,j}, x_{3,j})$)．ShiftRowsとMixColumnsの組合せは，2ラウンドの処理を行うと，1バイトの入力値が16バイト全体に影響するように設計されています．また，これら3つの処理は公知のものなので，誰でも逆変換を構成できてしまいます(つまり，解読できます)．そこで，最後にAddRoundKeyでラウンド鍵を排他的論理和し，秘密情報を混ぜ込みます($x_{i,j} \leftarrow x_{i,j} \oplus r_{i,j}$: ただし，$r_{i,j}$はラウンド鍵，⊕は排他的論理和演算を示します)．このラウンド鍵は鍵スケジュール部に入力された秘密鍵を用いて生成されます．

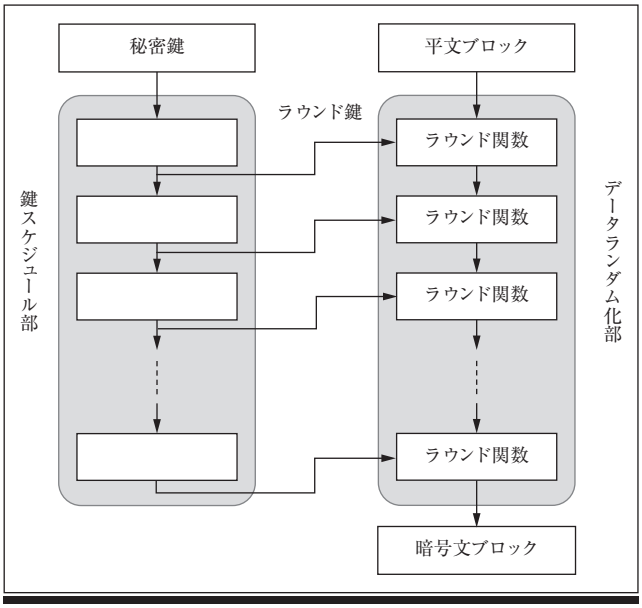


図5　AESのラウンド関数を構成する4つの処理

このように，AESを構成する処理をひとつひとつ見ていくと，昔の暗号と大きく変わっているというわけではありません．しかし，置換表の作り方や線形変換の選び方に関する知識は大幅に増え，良い要素を選ぶ理論も確立されています．

5．モード：ブロック暗号の使い方

さて，ブロック暗号を実際に使うことを考えましょう．AESを使うならば，まずデータを16バイトごとに区切ります．データ長は16バイトの倍数とは限りませんから，何らかの数値を追加して，16バイトの倍数にします．

次に，AESを使って順に暗号化すれば良いように思えます．この暗号化方式はECB(Electric Code Book)[5]モードと呼ばれています．図6にECBモードのブロック図を示します．E_Kが共通鍵暗号のブロックで，鍵Kが使用されることを示します．Pnが入力の平文，Cnが出力となる暗号文を示します．

ECBは，任意長のデータを暗号化できますが，同じデータが連続するような場合には，平文の情報が漏えいしてしまうかもしれません．1ブロック＝16バイトもあるので，なかなか同じ入力が続くことは考えにくいかもしれませんが，例えば，図7は，冗長性が高い画像ファイルをECBモードで暗号化してみた結果です．暗号化されていても，

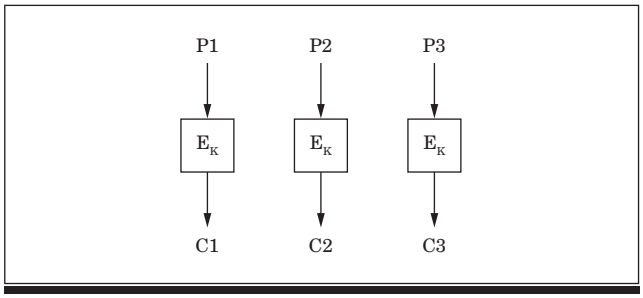


図6　ブロック暗号のECBモード

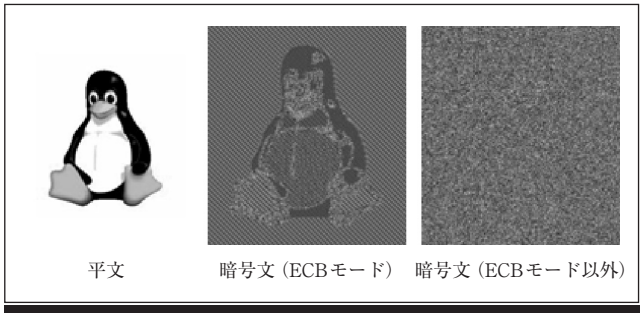


図7　暗号化処理の結果
(Wikipedia「暗号利用モード」より転載)

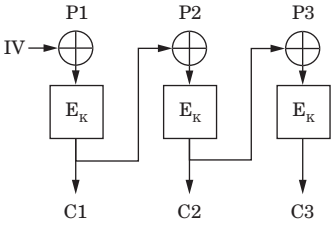


図8　ブロック暗号のCBCモード

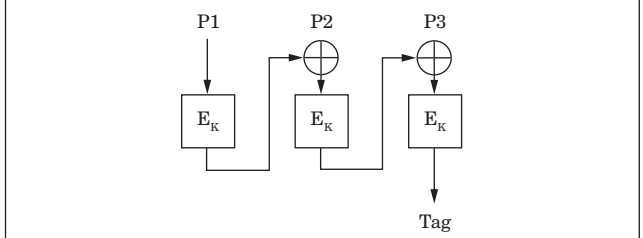


図9　CBC-MACモード

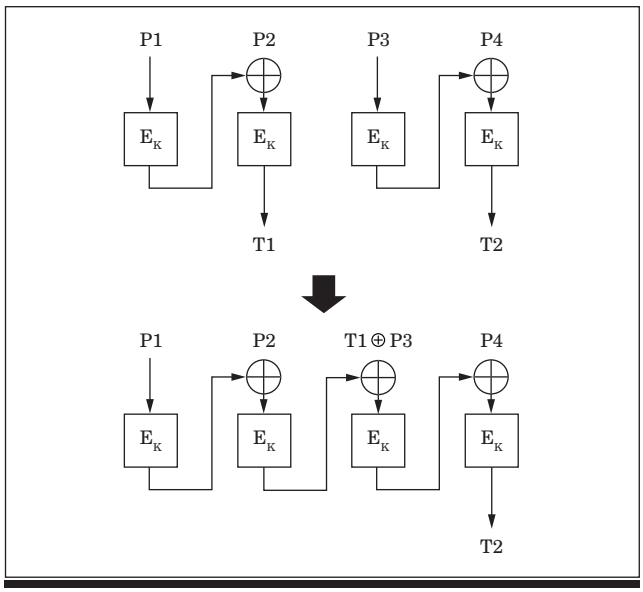


図10　CBC-MACの脆弱性

ペンギンの輪郭が確認できるのではないでしょうか．

ECBの問題点を解決するために考案されたのがCBC（Cipher Block Chaining）[5]モードと呼ばれる暗号化方式です．図8にCBCモードのブロック図を示します．IVは初期ベクトル（Initial Vector）であり，Pnと同じサイズの乱数です．

CBCモードでは，暗号文ブロック（ほとんど乱数です！）を次の平文ブロックと排他的論理和（⊕）することで，ブロック暗号への入力が常に変化し続けるようになっており，ECBモードのような問題は起こりません．CBCモードは単純な仕掛けながら安全性が高いということで，DESやAESとセットで広く使われてきた暗号化方式のモードです．しかしながら，本講座の第3回[6]でも触れられていましたが，「パディングオラクル攻撃」という攻撃を使うと，CBCモードで暗号化されたデータを復号できる可能性があることが2002年にわかりました[7]．これは，CBCモードが弱い，というよりはCBCモードの使い方が間違っていることに起因する脆弱性なのですが，昨今では，TLSなど標準暗号プロトコルの安全性を脅かすようになり，CBCモードの継続使用には黄信号が灯っている状態です．

6．メッセージ認証コード

ところで，パディングオラクル攻撃では，暗号文を改ざんしてサーバの応答を観測することで，暗号文を復号していきます．したがって，改ざんを検出するメッセージ認証技術を（正しく）使うことで，パディングオラクル攻撃を防ぐことができます．メッセージ認証技術の基本は誤り検出に用いる巡回冗長検査（CRC: Cyclic Redundancy Check）と同じです．まず，事前にデータの特徴値を抽出し，データに付加しておきます．データが改ざんされているかチェックするときは，データの特徴値を改めて計算し，事前に計算しておいた値と一致するかを確認します．もちろん，CRCがデータの破損チェックに使えるのは「データが壊れているのに，『たまたま』CRCは一致するなんてことはないだろう」という前提があります．ところが暗号解読者の視点からすれば，「意図的に」CRCの値が一致するようにデータを改ざんするのは簡単です．そこで，特定の人しか計算できないような特徴値の計算方法として，メッセージ認証コード（MAC: Message Authentication Code）が必要になります．MACの簡単な構成例として，ブロック暗号を使うCBC-MACがあります．図9にCBC-MACのブロック図を示します．Tagが最終的に出力される認証用のコードとなります．名前からもわかるように，CBC-MACは暗号化に用いるCBCモードをMACに流用しています．

CBC-MACは，固定長のデータを取り扱う分には安全であることが理論的に証明されていますが，いろいろな長さのデータを取り扱う場合には，安全性が損なわれる可能性があります．例えば，2つのデータをつなぎ合わせて新しいデータを偽造する攻撃に弱いことが知られています．図10で攻撃方法を説明してみましょう．具体的には，MACを生成するための鍵を持たない攻撃者が，未知のメッセージとTagのペアを生成できます．まず，何らかの方法で，攻撃者が事前に2つのメッセージM1=（P1, P2）とM2=（P3, P4）に対する認証コードT1とT2を入手したとします．（M1, T1）と（M2, T2）のメッセージとタグのペアを出力しても，これはすでに知っているので，攻撃とはなりません．次に，M=（P1, P2, T1⊕P3, P4）というタグの値を知らない未知のメッセージを考えてみましょう．3ブロック目の「T1⊕P3」が攻撃のキモになっています．（P1, P2）に対す

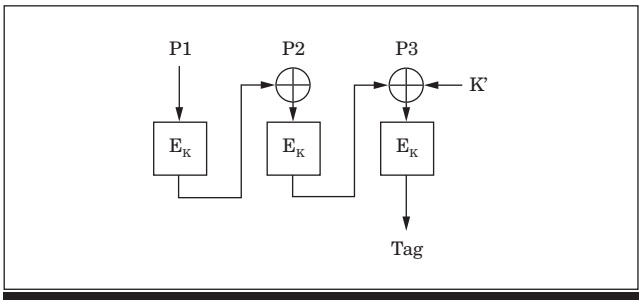


図11　CMACモード

る認証コードがT1であることがわかっていますので，3ブロック目の暗号化処理の入力はT1⊕（T1⊕ P3）=P3になります（同じ値T1の排他的論理和T1⊕ T1はゼロになります）．したがって，（P1, P2, T1⊕ P3, P4）に対する認証コードはT2になり，攻撃者は未知のメッセージMとタグT2のペア（M, T2）を偽造できたことになります．

このような脆弱性を避けるため，現在では，CBC-MACを改良したCMAC[8]が標準技術になっています．図11にCMACのブロック図を示します．K'は副鍵と呼ばれ暗号化E_Kに使われる鍵とは別の鍵です．

K'が攻撃者に知られない限り，CBC-MACと同じ攻撃はできなくなっています．

この他によく使われるMACとしては，ハッシュ関数を利用するHMAC[9]があります．

7．ストリーム暗号，ハッシュ関数

本稿では，ブロック暗号を中心に解説を進めてきました．この他に，共通鍵暗号に分類される技術として，ストリーム暗号とハッシュ関数があります．ストリーム暗号は，データと（擬似）乱数を排他的論理和する，という単純な処理で暗号化を実現しています．ブロック暗号のように「なんにでも使える」という便利さはありませんが，暗号化処理がビット単位で実行できるので，①半端な長さのデータを暗号化するのに向いている，②エラーが他のビットに伝播しない，という特徴があり，昔から無線通信の暗号化に使われてきました．AESが普及した現在でも，携帯電話の標準3GPP（Third Generation Partnership Project）ではストリーム暗号を多く利用しています．ちなみに，昨今，WEPやSSL/TLSの脆弱性の一因を担っているRC4もストリーム暗号の一種です．

ハッシュ関数は，MACと同じくデータの特徴値を取出す技術で，一方向性を持っていることが特徴です．一方向性とは「出力から入力を特定できない」ことを意味しています．通常の暗号技術でも「鍵を知らない限り」暗号文から平文の情報を得ることはできませんが，ハッシュ関数は，鍵なしで一方向性を実現しているという点で，暗号技術の中でも異色の存在です．ハッシュ関数は前述のメッセージ認証にも使えます．CMACでは，安全性を確保するために，最後のブロックでもう1つ別の鍵を使いましたが，ハッシュ関数を使ってメッセージ認証を行うHMACモードでも同じようなテクニックで「2つのデータをつなぎ合わせる攻撃」を防いでいます．この他にも，ハッシュ関数は，公開鍵暗号の基本技術である電子署名や公開鍵証明書でも使われており，複雑な暗号方式の構成では必須の要素技術になっています．

標準のハッシュ関数として，Rivestが開発したMD5[10]とNSA（National Security Agency）が開発したSHA-1[11]が長らく使われてきましたが，2004年頃にこの2つのアルゴリズムに対する攻撃が発表されました[12)13)]．特に，MD5に対する攻撃は深刻で，2009年には認証局のルート証明書が偽造されるという事件に発展しました[14)]．幸いにも，NISTは，これに先立ってDES, SHA-1といった旧来のアルゴリズムをAES, SHA-2[11]に置き換えていく暗号移行プログラムを推進していました．置き換えるアルゴリズムがないまま立ち往生する最悪の可能性は避けることができたのです．また，NISTは，SHA-2が安全ではなかった場合を想定して，SHA-3を準備することにしました[15)]．この選考は，AESコンペティションを踏襲したスタイルで2008年から約5年をかけて行われました．筆者もLuffaというアルゴリズムを応募し，1次選考は通ったのですが，残念ながら，最終選考に進むことができませんでした．SHA-3には，AESの開発者でもあるDaemen氏が率いるチームが提案したKeccakが選ばれました．

8．共通鍵暗号技術に関する標準

最後に，標準化されている共通鍵暗号を少し紹介しておきましょう．表2を参照してください．もっとも包括的に暗号技術をまとめているのはISO（International Organization for Standardization）で，ブロック暗号ではTriple DESやAESの他にもMISTY1やCamelliaが，ストリーム暗号ではSNOW 2.0やMUGIが収録されています[16)17)]．その一方で，おそらくもっとも参照されて，実際に利用されているのは米国のNIST標準暗号でしょう．NISTはブロック暗号として3-key Triple DESとAES，ハッシュ関数としてSHA-1とSHA-2だけを標準化しています．そして，擬似乱数生成やTLSなどの暗号プロトコルで利用される鍵の伸長など，共通鍵暗号技術に分類される機能はブロック暗号とハッシュ関数のモードを利用するように規定されています．日本や欧州でも，同様に安全な暗号アルゴリズムを選定するプロジェクト（CRYPTREC[18)]，NESSIE[19)]）がAESコンペティション後に始まり，独自のラインナップを揃えています．

9．むすび

本稿では，広く使われているAESとその周辺に話題を絞って，共通鍵暗号技術を紹介してきました．暗号というと，とかく「難しい」，「わからない」と敬遠されがちですが，

表2　標準暗号

	64ビットブロック暗号	128ビットブロック暗号	ストリーム暗号	ハッシュ関数	メッセージ認証コード
ISO	TDEA (triple DES) MISTY1 CAST-128 HIGHT	AES Camellia SEED	MUGI SNOW 2.0 Rabbit Decim v2 KCipher-2	RIPEMD-128 RIPEMD-160 SHA-1 SHA-256 SHA-284 SHA-512 WHIRLPOOL	
NIST	3-key triple DES	AES	—	SHA-1 SHA-256 SHA-384 SHA-512	CMAC HMAC
CRYPTREC （推奨暗号）	3-key triple DES	AES Camellia	KCipher-2	SHA-256 SHA-384 SHA-512	CMAC HMAC
CRYPTREC （推奨候補暗号）	CIPHERUNICORN-E Hierocrypt-L1 MISTY1	CIPHERUNICORN-A CLEFIA Hierocrypt-3 SC2000	Enocoro-128v2 MUGI MULTI-S01	—	PC-MAC-AES
NESSIE	MISTY1	AES Camellia SHACAL-2*	—	Whirlpool SHA-256 SHA-384 SHA-512	UMAC TTMAC EMAC HMAC

＊SHACAL-2は256ビットブロック暗号に分類される．

スマート化が進む社会では，日常的に暗号を利用したサービスが提供されています．本稿を通して，暗号が少しでも皆さんの身近になれば，これに勝る喜びはありません．

（2015年4月1日受付）

〔文　献〕

1) National Institute of Standards and Technology: "Data Encryption Standard (DES) ; specifies the use of Triple DES", Federal Information Processing Standards Publication 46-3, Oct. 25, 1999 (Withdrawn: May 19, 2005)
2) https://blockchain.info/
3) National Institute of Standards and Technology: "Advanced Encryption Standard (AES) Development Effort", http://csrc.nist.gov/archive/aes/
4) National Institute of Standards and Technology: "Advanced Encryption Standard", Federal Information Processing Standards Publication 197 (Nov. 2001)
5) National Institute of Standards and Technology: "Recommendation for Block Cipher Modes of Operation - Methods and Techniques", NIST Special Publication 800-38 A (Dec. 2001)
6) 神田雅透：“SSL/TLSの仕組みを知っていますか？”，映情学誌，69，3，pp.228-233 (2015)
7) S. Vaudenay: "Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS ...", Advances in Cryptology - EUROCRYPT 2002, Lecture Notes in Computer Science, 2332, pp.534-546, Springer (2002)
8) National Institute of Standards and Technology: "Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication", NIST Special Publication 800-38B (May 2005)
9) National Institute of Standards and Technology: "The Keyed-Hash Message Authentication Code (HMAC) ", Federal Information Processing Standards Publication 198-1 (July 2008)
10) R. Rivest: "The MD5 Message-Digest Algorithm", IETF RFC 1321 (1992)
11) National Institute of Standards and Technology: "Secure Hash Standard (SHS) ", Federal Information Processing Standards Publication 180-4 (May 2012)
12) X. Wang and H. Yu: "How to break MD5 and other hash functions", Advances in Cryptology, Eurocrypt2005, Lecture Notes in Computer Science, 3494, pp.19-36, Springer (2005)
13) X. Wang, L. Yin and H. Yu: "Finding collision in the full SHA-1", Advances in Cryptology, CRYPTO2005, Lecture Notes in Computer Science, 3621, pp.17-37, Springer (2005)
14) A.K. Lenstra, D. Molnar, D.A. Osvik, B. de Weger, M. Stevens, A. Sotirov and J. Appelbaum: "Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate", Advances in Cryptology-CRYPTO 2009, Lecture Notes in Computer Science, 5677, pp.55-69 (2009)
15) National Institute of Standards and Technology: "Cryptographic Hash and SHA-3 Standard Development", http://csrc.nist.gov/sgroups/ST/hash/
16) ISO/IEC 18033-3:2010, Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers
17) ISO/IEC 18033-4:2011, Information technology - Security techniques - Encryption algorithms - Part 4: Stream ciphers
18) CRYPTREC: Cryptography Research and Evaluation Committee, http://cryptrec.go.jp/
19) NESSIE: New European Schemes for Signatures, Integrity and Encryption, https://www.cosic.esat.kuleuven.be/nessie/

渡辺（わたなべ）　大（だい）　1996年，東北大学理学研究科数学専攻博士前期課程修了．1999年，(株)日立製作所に入社．システム開発研究所に配属．現在は同横浜研究所に勤務．共通鍵暗号の設計および安全性評価業務に従事．

公開鍵暗号

満保雅浩†

1．まえがき

本講座の第6回「共通鍵暗号」[1]でも紹介しましたように，暗号技術の起源は紀元前にまで遡り，主に軍事目的で，秘密裏に情報をやりとりする技術として発達してきました．しかし，昨今では，インターネットを中核とするIT技術の普及に伴い，私たちの日常を支える技術として発展を続けています．

本講座では，暗号技術とはどのようなものなのか，少し掘り下げて見ていただくための第2弾としまして，公開鍵暗号（Public-Key Encryption）の現在について紹介します．

みなさんは，クレジットカードを使ったインターネット決済において，送信する前にhttps://で始まるURLになっているかを確認しているでしょうか？ https://で始まるURLになっていれば暗号通信が実行されて安全に送信できると知っている方もいらっしゃるかもしれません．

一口に暗号化されると言っても，SSL/TLSは幾つかの異なる機能を実現する暗号技術が組合されて，最終的に，データが暗号化されています．正しいサイトと接続したことを確認したブラウザは，暗号通信を行うための秘密の鍵を生成して，その鍵を公開鍵暗号により暗号化してサイトに送ります．このようにしてブラウザとサイトが共有した鍵を用いて共通鍵暗号によりデータが暗号化されます．

鍵をサイトに送るための暗号とデータの暗号化のための暗号は同じではいけないのでしょうか？単に他の人に読まれなければいいのでは？という素朴な疑問を持たれた方もいらっしゃるでしょう．もしくは，そもそも，公開鍵暗号と共通鍵暗号は何が違う？と思った方もいらっしゃるかもしれません．

今回紹介する公開鍵暗号の用途は大雑把に言うと「データの保護」ですが，鍵共有，署名なども公開鍵暗号の仲間として考えられています．これら三つについてより細かく見ていきたいと思います．

2．公開鍵暗号の出現は必然であったか？

公開鍵暗号は，暗号化で使う鍵（公開鍵）と復号に使う鍵（秘密鍵または復号鍵）が異なることが特徴です．図1に公開鍵暗号を用いてデータを暗号化し，復号する手順を図示します．

なぜ，このような暗号ができてきたのでしょうか．秘密の情報，つまり，秘密の鍵を持ち合えば，その鍵を用いて暗号通信が実現できそうであることは想像しやすいのでは

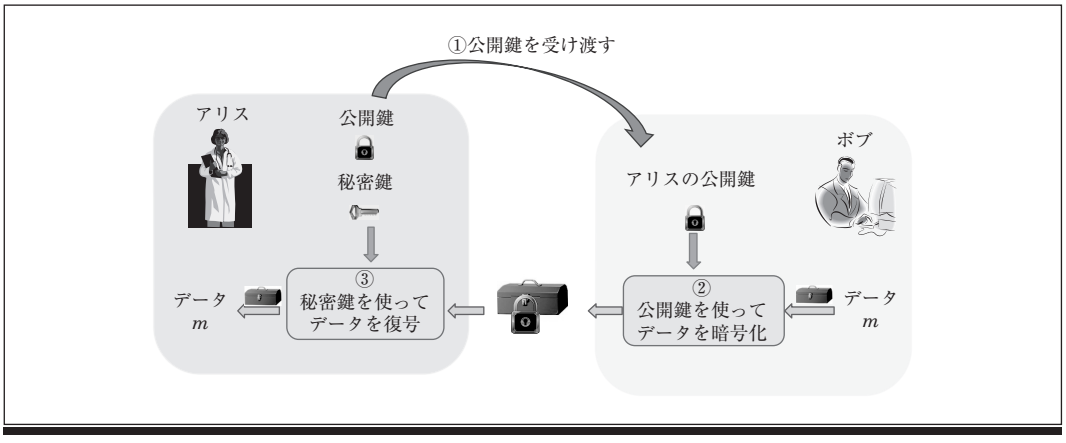


図1　公開鍵暗号を用いた暗号化

† 金沢大学
"Security Technologies on Image Information (7); Public-Key Encryption"
by Masahiro Mambo (Kanazawa University , Kanazawa)

映像情報メディア学会誌 Vol. 69, No. 7 pp. 714～720（2015）

ないかと思います．これには，第6回『共通鍵暗号』で取り上げられた，送信者と受信者が共通の鍵を利用する共通鍵暗号を利用すればよいことになります．暗号通信を利用する人が沢山いるわけではなく，例えば，外交官や軍隊といった限られた人達が，外交文書の送信や軍事機密情報の送信などの特殊な場合にのみ暗号通信を利用しているときは，相手も限られており，やり取りするデータも，ある程度限られた量となります．このようなときに必要な量の鍵を事前に安全に共有し合うことは，簡単ではないにせよ，実行しようと思えばできます．

一方，1990年代から急速に広まったインターネットでの通信において，インターネット上の誰と通信するかわからないならば，通信相手との鍵を事前に共有しておくことは容易ではありません．もし，インターネット上のすべての人と事前に鍵を共有することができれば，どの相手とも暗号通信をすぐに開始できます．しかし，インターネット上に誰がいるのかをすべて把握することは容易ではありませんし，実際に通信することになるのはインターネット上の一部の相手でしょうから，インターネット上に存在する非常に沢山の相手のすべてと鍵を共有するのはとても効率が悪く，非現実的です．

この打開策として，以下の二つの方法が考えられます．

(1) 暗号通信を行いたい相手が決まった段階で，鍵を共有し，その鍵を用いて暗号通信を行う．

(2) 通信相手の公開鍵を入手して，その公開鍵を用いた公開鍵暗号により暗号通信を行う．

(1) は，鍵が共有されていれば共通鍵暗号を用いて暗号通信を行えますから，いつ誰と暗号通信を行いたいかが決まった後に鍵を共有するための手続きを実行しようという素直な発想です．この方法はまさに，SSL/TLSでの秘密の鍵を生成して公開鍵暗号によりサイトに送る手順と，それに続く，共有した鍵を用いた共通鍵暗号によるデータの暗号化が対応します．

ここで，“鍵を管理する信頼のおけるセンターを導入して，鍵の安全な保管や配送を担ってもらえば，そのセンターに聞くだけで鍵の共有が実現するのでは？”と疑問に思った方がいるかもしれません．暗号通信を行いたい相手が決まった段階で，センターに聞いて鍵をもらい，共通鍵暗号で暗号通信を行うのです．これならば，公開鍵暗号というものを使う必要はなくなります．

残念ながら，この方法では，鍵を管理する信頼のおけるセンターから鍵が漏洩してしまえば安全ではなくなります．また，例え信頼できるセンターがあったとしても，インターネットのような非常に沢山の人が関係するネットワークにおいて，それらすべての人を網羅するセンターによる鍵の保管・配送を効率的に動作させることは容易ではありません．これに対して，先に述べた公開鍵暗号を用いた鍵の共有は，相手（例えば，サイト）の公開鍵さえ入手できれば，いつでも鍵を送ることができるようになり，大規模なネットワークにおいても機能するのではないかと期待されます．

(2) は，まず，公開できる鍵を各自が準備して，他の人が入手できる状態にします．例えば，公開の掲示板に，誰がどの公開鍵を使用するのかを掲示します．暗号通信を行う人は，通信を行う時に相手の公開鍵を入手して，公開鍵暗号によりデータを暗号化して暗号通信を行います．

この方式ならば，事前に鍵を共有しておく必要もなく，公開されている公開鍵を必要なときに取ってきて処理すればよいことになります．ネットワーク上に存在するn人のすべてと事前に鍵を共有した場合にネットワーク全体で$n(n-1)/2$個の鍵を準備する必要があるのに対して，公開鍵暗号ならばn個でよいことになり，効率的になることもわかります．

以上のように，ネットワーク社会に適した暗号として，公開鍵暗号の出現は必然ともいえます．

3．公開鍵暗号と共通鍵暗号の機能と役割

公開鍵暗号を構成するためにいろいろな工夫が行われましたが[2)]，共通の鍵を使う共通鍵暗号と比べると，多大な計算量が必要な暗号となっています．これらの特徴を踏まえて，この両者の役割は大きく異なっています．

通常，大容量のデータ（メッセージ）を暗号化するためには共通鍵暗号を使用します．公開鍵暗号でも暗号化ができないわけではないですが，多大な時間が必要となってしまいます．ただし，共通鍵暗号を利用する際には，暗号化する人と，復号する人が同じ鍵を共有しなければなりません．そこで，大容量のデータを暗号化するためには，図2に示すように，公開鍵暗号と共通鍵暗号がハイブリッドに使われるのが一般的です．まず，この鍵を共有するために公開鍵暗号を使用します．共通鍵暗号で使用する鍵は，数十から数百ビット（64ビットや128ビットが多く使われる）ですので，公開鍵暗号を利用したとしてもそれほど時間を要しないわけです．

また，公開鍵暗号で使用する暗号化の鍵（暗号鍵）は公開し，誰でも暗号化することができます（このため，公開鍵暗号と呼ばれています）．ただし，この暗号鍵とペアとなる復号鍵を持っている人しか，その暗号化されたデータを復号することはできません．共通鍵暗号は暗号化する鍵と復号する鍵が同じであることから対称鍵暗号（Symmetric Encryption），公開鍵暗号は別々の鍵を使用することから非対称鍵暗号（Asymmetric Encryption）と呼ばれることもあります．

この公開鍵暗号の仕組み，および，公開鍵暗号の仲間である鍵共有，ディジタル署名方式について，代表例を交えて，以下の章ですこしずつ掘り下げて説明いたします．

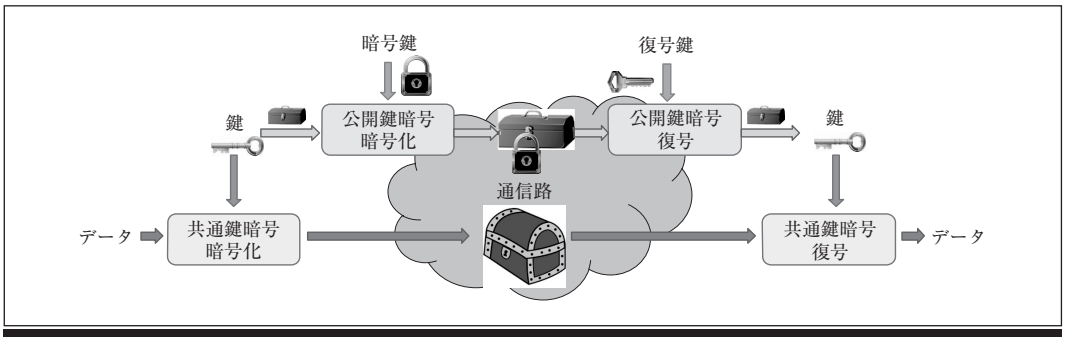


図2　共通鍵暗号と公開鍵暗号を使用したデータ（メッセージ）の伝送

4．公開鍵暗号 RSA[3)]

1976年にDiffieとHellmanが公開鍵暗号の概念を提唱しました．ただし，この時は実際の公開鍵暗号は示されませんでした．この後1年たって，Rivest，Shamir，Adlemanが初めてのRSA暗号を発表しました．RSAとはその開発者3名，Rivest，Shamir，Adlemanの頭文字をとってつけられています．

現在最も使用されている公開鍵暗号はこのRSA暗号をベースにしたものです．そこで，図1の公開鍵暗号を用いた暗号化の手順も思い出しながら，RSA暗号のアルゴリズムを見てみようと思います．

RSA暗号は三つの部分からできています．暗号化の準備を行う初期設定，データを暗号化する部分，そして，暗号化の逆変換である復号となります．それぞれ，以下のようになります．

(1) 初期設定（図2の公開鍵と秘密鍵を作る部分）
- 大きな二つの素数p, qを準備する．
- p, qの積$n = pq$を求める．
- 公開鍵eを$(p-1)(q-1)$と互いに素となる$(p-1)(q-1)$より小さな正の整数として選ぶ（二つの数に共通の約数が1しかないとそれらは互いに素といいます）．
- 秘密鍵dを$ed = 1 \bmod (p-1)(q-1)$となるように選ぶ（ただし，mod xはxで割った余りを出力する演算）．
- (e, n)を公開する（図1では公開手順を省略．公開することにより受信者（アリス）へ受け渡します（①））．

(2) メッセージmの暗号化（図1の公開鍵を使ってデータを暗号化する部分（②））
- 暗号文$c = m^e \bmod n$

(3) 暗号文cのメッセージmへの復号（図1の秘密鍵を使ってデータへ復号する部分（③））
- メッセージ$m = c^d \bmod n$

数式を見ることに拒否反応さえ示さなければ，それほど難しい計算をしていないことがわかると思います．

メッセージの暗号化はmをe乗しているだけです．復号はcをd乗しているだけです．初期設定にある$ed = 1 \bmod (p-1)(q-1)$となるdを求めることも，実際はそれほど難しい演算ではありません．

この暗号のからくりはmを$e \times d$乗すればmが得られるというところにあります．ただし，ただ単に$e \times d$乗するのではなく，$e \times d$乗した後でmod nを行っています．少し小さい数字で例を示します．

まず，素数pとqを3と7としましょう．そうすると$n = pq = 21$です．この$n = 21$を考える前に，例えば，仮に$n = p = 7$とおいて，$m = 2$に対して，$2^1 \bmod 7, 2^2 \bmod 7, 2^3 \bmod 7$と順に求めてみましょう．すると，順に，2, 4, 1となることがわかります．一旦，1になってしまえば，$2^4 \bmod 7 = 2 \times 2^3 \bmod 7 = 2$となり，2に戻ることがわかります．このように，べき乗をしていってnで割った余りが1になれば，その次の順番のべき乗のときに元のメッセージに戻ります．それでは，$n = pq = 21$ではどうでしょうか？そこで，nより小さな正の整数について，$(p-1)(q-1)+1 = 13$までのすべてのべき乗を表1に記載します．

表1をご覧になっていただくとわかりますように，どのデータも7乗と13乗すれば元に戻っています．この何乗すれば元のデータに戻るかは，pとqの値によって決まるわけですが，必ず，$(p-1)(q-1)+1$乗すれば元に戻ることが知られています．つまり，$n = p = 7$の例で見たように，一つ前の$(p-1)(q-1)$乗したときに1になります．このことは，$e \times d$乗した後でmod nを求める計算において，$e \times d$乗する代わりに，実は，$e \times d \bmod (p-1)(q-1)$乗してもよいことを意味します．$e, d$を選ぶときに$ed = 1 \bmod (p-1)(q-1)$を満たすように求めていますから，最終的に，$e \times d \bmod (p-1)(q-1)$乗は1乗と等しくなり，元のメッセージが復号できることになります．

なお，$(p-1)$と$(q-1)$の最小公倍数がより小さいときは，その数+1でも元に戻るため，$p = 3, q = 7$では7乗でも元に戻ります．

表1をもとに，公開鍵と秘密鍵の決め方を説明します．まず，eを$(p-1)(q-1)$と互いに素となる$(p-1)(q-1)$より小さな正の整数から任意に選びます．$e = 5$と決めま

表1　mod nにおけるべき乗計算($n=21$)

		べき乗数												
		1	2	3	4	5	6	7	8	9	10	11	12	13
データ	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	2	2	4	8	16	11	1	2	4	8	16	11	1	2
	3	3	9	6	18	12	15	3	9	6	18	12	15	3
	4	4	16	1	4	16	1	4	16	1	4	16	1	4
	5	5	4	20	16	17	1	5	4	20	16	17	1	5
	6	6	15	6	15	6	15	6	15	6	15	6	15	6
	7	7	7	7	7	7	7	7	7	7	7	7	7	7
	8	8	1	8	1	8	1	8	1	8	1	8	1	8
	9	9	18	15	9	18	15	9	18	15	9	18	15	9
	10	10	16	13	4	19	1	10	16	13	4	19	1	10
	11	11	16	8	4	2	1	11	16	8	4	2	1	11
	12	12	18	6	9	3	15	12	18	6	9	3	15	12
	13	13	1	13	1	13	1	13	1	13	1	13	1	13
	14	14	7	14	7	14	7	14	7	14	7	14	7	14
	15	15	15	15	15	15	15	15	15	15	15	15	15	15
	16	16	4	1	16	4	1	16	4	1	16	4	1	16
	17	17	16	20	4	5	1	17	16	20	4	5	1	17
	18	18	9	15	18	9	15	18	9	15	18	9	15	18
	19	19	4	13	16	10	1	19	4	13	16	10	1	19
	20	20	1	20	1	20	1	20	1	20	1	20	1	20

しょう．次に，dを作るわけですが，

$$e \times d = k \times (p-1)(q-1)+1 = k \times 12+1$$

となればよいわけです．すなわち，

$$d = (k \times (p-1)(q-1)+1)/e$$
$$= (k \times 12+1)/5$$

です．この右辺の式が5で割り切れる一番小さいkは2ですから，そのときの$d=5$となります．実際に，このようなdを簡単に求める方法が知られています．

この$e=5$，$d=5$を用いて表1を見ながらデータの暗号化と復号をしてみましょう．例えばデータ$m=17$とします．この時の暗号文cは

$$c = m^e \bmod n = 17^5 \bmod 21 = 5$$

これを復号した結果は

$$m = c^d \bmod n = 5^5 \bmod 21 = 17$$

と正しく復号されることがわかります．他の値でも是非お試しください．RSA暗号のからくりが実感できると思います．

この暗号は「大きな数の素因数分解をすることが難しい」，ということに基づいて，安全であることが知られています．素因数分解とはnのように複数の数の掛け算で生成された数から，pとqのような，掛け算の元になった数を求めることを言います．もし，素因数分解が簡単であるとすると，nは公開されるわけですから，そこからpとqがわかってしまいます．dはeとpとqを用いて生成されますから，公開されているeと素因数分解されたpとqより，秘密鍵を生成した方法でdを求めることができます．結果として，暗号が解読されてしまいます．もう少し安全性について話すと，コンピュータの進歩に伴い，計算が早くなり，素因数分解の速度も速くなってきます．ということは，コンピュータの進歩とともに，より大きな数をpやqやnに使わなければいけない，ということになります．

現在では，素因数分解を解くことによる攻撃だけでなく，種々の攻撃法がRSA暗号に対し見つけられてきたため，そのままのRSA暗号が使われることはあまりありません．

5．鍵共有 DH[4)]

公開鍵暗号を使わずとも，鍵共有ができる方法があります．公開鍵暗号の概念を提唱したDiffieとHellmanがその最初の方法（DH鍵共有）を示しました．この方法は公開鍵暗号を使っているわけではありませんが，ある情報xを秘密にしておいてgとg^xを公開する．この公開された情報からxを求めることが困難であるということを利用し，安全に鍵共有ができる方法となっています．

具体的に，アリスとボブが秘密鍵を共有する例を示します．図3にそのやりとりを図示します．

① 共通パラメータの準備（と共有）
　素数 p
　生成元 g
②－A アリスの秘密情報と公開情報の設定
　秘密情報 a
　公開情報 $g^a \bmod p$
②－B ボブの秘密情報と公開情報の設定
　秘密情報 b
　公開情報 $g^b \bmod p$
③ アリスとボブの公開情報を交換
　アリス g^a → ボブ
　ボブ g^b → アリス
④ 共有する秘密鍵の生成
　アリス $g^{ab} = (g^b)^a \bmod p$
　ボブ $g^{ab} = (g^a)^b \bmod p$

こちらも，数式を見ることに拒否反応さえ示さなければ，それほど難しい計算をしていないことがわかると思います．ちょっと難しい言葉で生成元という言葉が入っています．ある特定の値ではありますが，ここでは，べき乗計算に使われる大元の数値と思っていただければいいと思います．

秘密鍵の共有において，アリスはボブの公開情報に自分の秘密情報をべき乗する，ボブはアリスの公開情報に自分の秘密情報をべき乗することで同じ値になっていることがわかると思います．

実際のインターネットを流れる情報は，アリスとボブが公開情報の交換を行う際のg^aとg^bになります．これらの値はインターネット上で盗聴されれば，取得されてしまう値です．このため，誰に見られてもよいように生成しておかなければなりません．見方を変えれば，これが公開情報となります．これに対して，共有された秘密鍵はg^{ab}です．

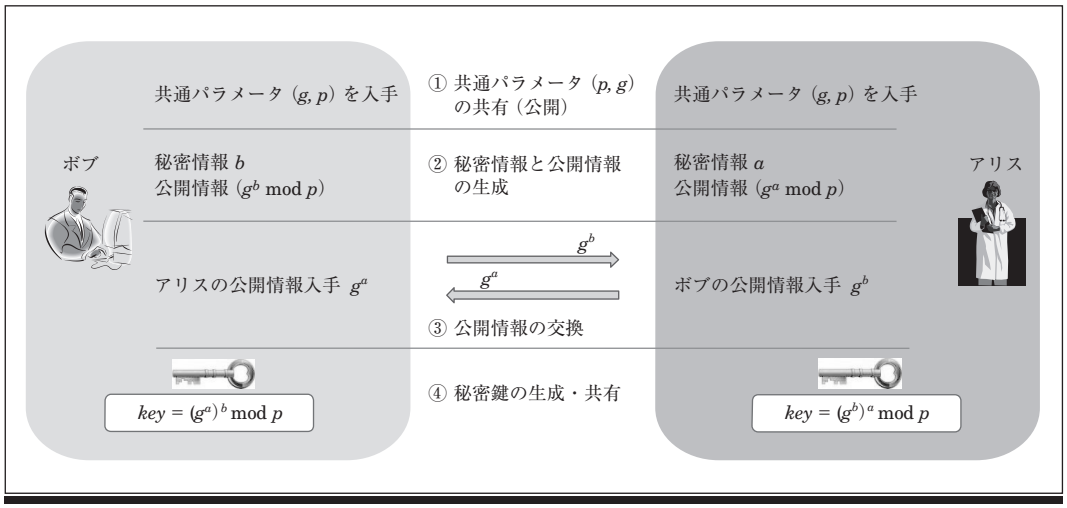


図3　鍵共有

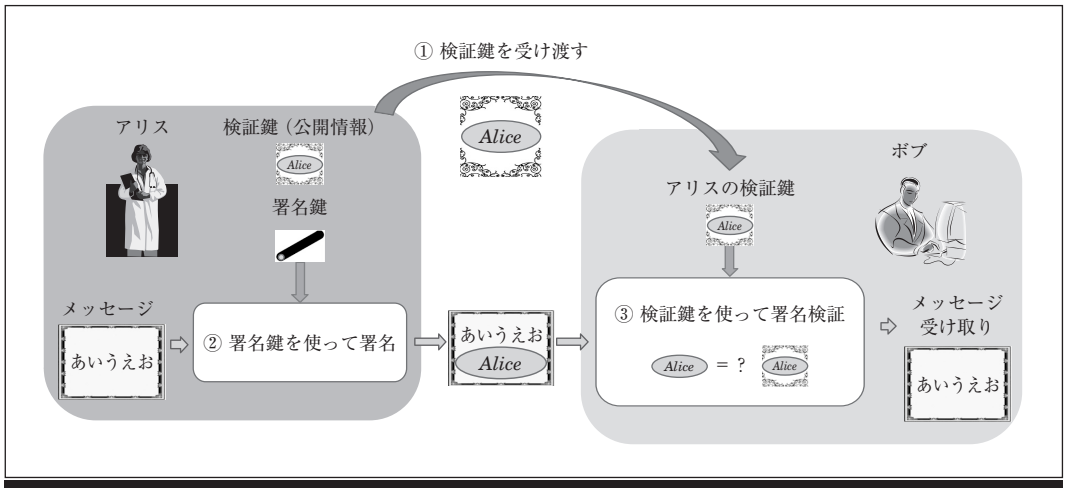


図4　ディジタル署名

さて，公開情報から秘密鍵を作成することができるでしょうか．公開情報からaやbを求めることができれば，g^aやg^bから秘密鍵を計算することができます．しかし，g^aからaを求めたり，g^bからbを求める問題は，古くから一生懸命チャレンジされている離散対数問題という問題であり，容易に解く方法が見つけられていません．

すなわち，インターネット上でいくら盗聴していたとしても，その情報だけでは秘密鍵が生成できないため，安全に秘密鍵を共有できるようになります．

6．ディジタル署名 DSA[5)]

公開鍵暗号関係にもう一つの大きな仲間がいます．それがディジタル署名です．公開鍵暗号の目的が守秘，鍵共有の目的が秘密鍵の共有であるのに対して，ディジタル署名があれば，メッセージの作成者が誰であるかを検証することができます．

具体的な方法として，アリスは自分が作った文章に署名を付与するには，アリスの秘密の署名鍵を使用します．この署名鍵は実社会の印鑑と同じように，他人に渡すことはなく，アリスが秘密裏に保管するものです．この付与された署名に対して，公開の検証鍵があり，署名が正しいものであるかどうか，メッセージを受け取った人が判定することができます．これは，実社会において印鑑証明があり，印鑑証明と実際の押印を見て正しいかどうかを判断することと同様です．この印鑑証明は公的機関が発行しますが，検証鍵をどうやって公的機関が発行するのか，という疑問があるかもしれません．この点については第7章公開鍵基盤においてご説明いたします．話を戻して，ディジタル署名の使用方法を図4に示します．

ここでは，DSA（Digital Signature Algorithm）と呼ばれるディジタル署名を例としてより細かく紹介します．DSAは以下のようになっています．

(1) 鍵生成（図4の検証鍵と署名鍵を生成する部分）
- 素数 p, q　　q は $p-1$ を割り切る．
- 元 g．
- 署名者は秘密鍵 x を選択し，$y=g^x$ を計算する．
- 検証鍵 (p, q, g, y)．
- 署名鍵 x（検証鍵を公開する（図4では公開手順を省略．公開することにより受信者（ボブ）へ受け渡します（①））．

(2) 署名（図4の署名鍵を使って署名する部分（②））
- ランダムな値 k を選択
- $r=(g^k \bmod p) \bmod q$ を計算．
- メッセージ m に対して $s=k^{-1}(H(m)+xr) \bmod q$ を計算（ただし $H(\ )$ はハッシュ関数）．
- (r, s) がメッセージ m に対する署名として (r, s) を出力．

(3) 検証（図4の検証鍵を使って署名を検証する部分（③））
- 署名から $w=s^{-1} \bmod q$ を計算．
- $u1=H(m)\,w \bmod q$ を計算．
- $u2=rw \bmod q$ を計算．
- $r=((g^{u1}y^{u2}) \bmod p) \bmod q$ であるかどうかを確認．等しければ（＝であれば），正しい署名と判断する．

これまでのRSA暗号やDH鍵共有に比較すると若干複雑かもしれません．

署名・検証を細かく見てみると，$s=k^{-1}(H(m)+xr) \bmod q$ や $u1=H(m)\,w \bmod q$ と書かれた計算があります．$H(\ )$ はハッシュ関数ですが，このハッシュ関数を使用せず，メッセージそのものを $s=k^{-1}(m+xr) \bmod q$ のように扱うと，実は長いメッセージにおいてメッセージの一部にのみ署名を付与していることになってしまいます．このため，メッセージが長い場合は，メッセージを分割して，分割された部分メッセージのそれぞれに署名するという方法も取れますが，計算時間が多大になるなどの問題があります．そこでハッシュ関数の登場となります．ハッシュ関数は入力値に対し，ある特定の短い長さのダイジェストを作ってくれます．このダイジェストはランダムな値となっています．原理的には，同じ出力となってしまう異なる入力が存在するのですが，これを発見するのは非常に困難という性質がある関数です．このような関数を使用することで，メッセージをメッセージ全体に依存した小さなダイジェストにして，計算量を減らすことができます．加えて，同じ署名に相当する異なるメッセージを見つけることが困難であるため，署名が付与されたメッセージをすり替えて，あたかも著名が付与されたように偽造することを困難としています．

また，この署名も離散対数問題を解くことが困難である，ということを根拠として，安全とされています．

7．公開鍵基盤（PKI）

これまでに述べてきた公開鍵暗号やディジタル署名はそのままでは使うことができません．なぜでしょう．

公開鍵暗号においては公開鍵，ディジタル署名おいては検証鍵と言われる公開情報があります．公開鍵暗号の公開鍵を利用してデータを暗号化する場合や，ディジタル署名の検証鍵を用いて署名を検証する場合，その公開鍵が受信者の公開鍵であることや，メッセージの署名者の検証鍵であることを確認しなければなりません．逆に考えると，今使おうとしている公開鍵や検証鍵が誰のものであるかわからなければ，誰宛の暗号文を作成したのか，誰が署名を作成したのかが判定できなくなります．

この問題を解決しようとしたのが公開鍵基盤，いわゆるPKI（Public Key Infrastructure）です．

PKIでは公開鍵・検証鍵に対して証明書を付けます．この証明書は信頼できる第3者機関が発行したものとなります．証明書の中には，例えば，公開鍵とその所有者の情報が記載されており，それに対して第3者機関のディジタル署名が付与されています．この様子を図5に示します．

図5では，ボブがアリスに公開鍵暗号を用いて暗号化されたデータを送る場合を示しています．まず，アリスさんは，公開鍵と秘密鍵のペアを作成し，公開鍵を信頼できる第3者機関に渡します（①）．第3者機関は，受け取った公開鍵に対する証明書を作成し（②），アリスに送ります（③）．アリスは，データを送ろうとしているボブに公開鍵と証明書を送ります（④）．ボブは，証明書を確認（検証）し，公開鍵がアリスのものであると確証を持たなくてはいけません．この例では，第3者機関に証明書の検証を依頼し（⑤），第3者機関での検証（⑥）の後に，その結果の知らせを受ける（⑦）という，面倒ですが，正確な方法を示しています．証明書の確認は中に付与されているディジタル署名の検証ですので，ボブが第3者機関の検証鍵をすでに持っているような場合は，ボブの手元で証明書の検証を行うことも可能です．さて，証明書の検証結果が正しかった場合，すなわち，証明書に付与されているディジタル署名が正しい署名であった場合，ボブは，アリスから送られた公開鍵がアリスのものであると判断できますので，安心してその公開鍵でデータを暗号化して（⑧）アリスに送ることができます．後は，アリスが自分の秘密鍵を使ってデータを復号するだけです（⑨）．

署名の場合も同様で，検証鍵に証明書が付けられています．この証明書を検証した後に，検証鍵を用いてメッセージの署名を検証することになります．

公開鍵の正しさを保障することは思いのほか手間が掛かりますが，インターネット上のすべてのユーザの公開鍵とまでいかないまでも，サーバの公開鍵ぐらいならば，充分に機能します．

8．公開鍵暗号技術に関する標準化

標準化されている公開鍵暗号関連の方式を少し紹介します．

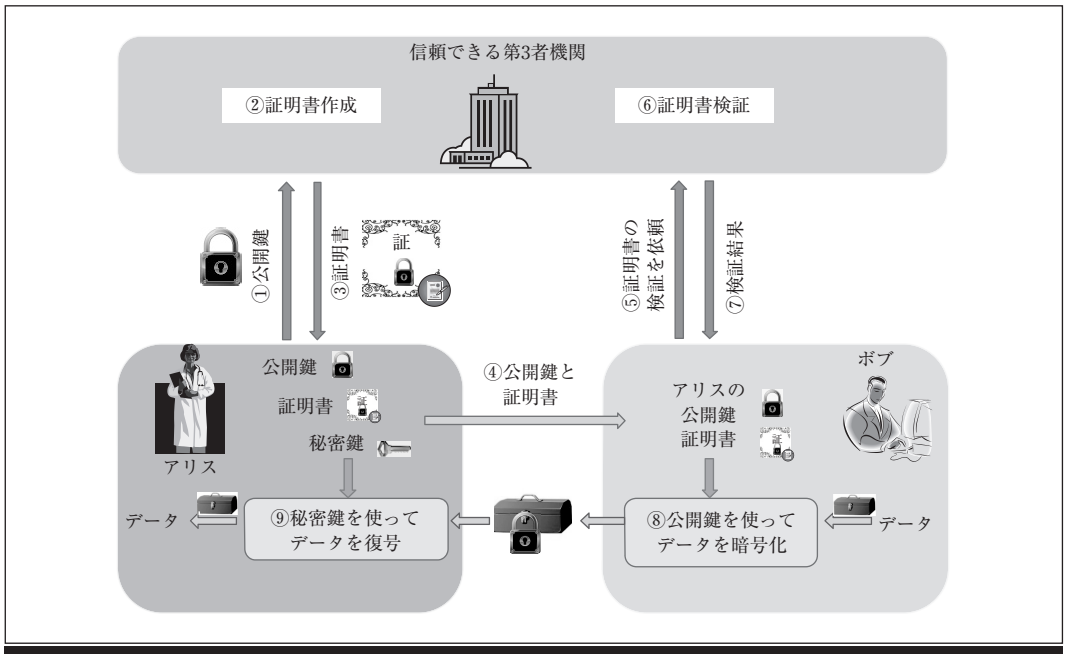


図5　公開鍵暗号基盤

ISO/IEC（国際標準化機構/国際電気標準会議）では長らく登録制度を採用していましたが，標準化に移行し，公開鍵暗号としてPSEC-KEM, HIME®，RSA-OAEP（RSAをベースにした公開鍵暗号方式）などを選定しています[6]．日本ではCRYPTREC[7]が電子政府における調達のために参照すべき暗号リストとして，DSA，ECDSAなどの署名方式，守秘のためのRSA-OAEP，鍵共有のためのDHとECDHを推奨しています．また，世界中でもっとも参照されているRSAはPKCS（Public-Key Cryptography Standards）の中に収録されています[8]．さらに，鍵共有については，米国のNIST（National Institute of Standards and Technology）でDHやECDHなどが収録されています[9]．欧州連合ではNESSIE（New European Schemes for Signature, Integrity and Encryption）プロジェクト[10]が，PSEC-KEM，RSA-KEMなどの公開鍵暗号，ECDSA，RSA-PSSなどのディジタル署名を選定し推奨しています．

9．むすび

本稿では，広く使われているRSA，DH，DSAとその周辺に話題を絞って，公開鍵暗号関連の技術を紹介してきました．暗号というと，とかく「難しい」，「わからない」と敬遠されがちですが，スマート化が進む社会では，日常的に暗号を利用したサービスが提供されています．本稿でも数式を書かせていただきましたが，できるだけシンプルな表現とし，簡易な説明を心がけました．本稿を通して，セキュリティの基盤技術を少しでも理解していただき，皆さんに納得して，安心して使っていただけるようになればと願っています．

（2015年6月28日受付）

〔文　献〕

1）渡辺大：“講座：共通鍵暗号”，映情学誌，69，6，pp.553-559（2015）
2）太田和夫，國廣昇：“本当に安全？現代の暗号”，岩波科学ライブラリー102（2005）
3）R.L. Rivest, A. Shamir and L.M. Adleman: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of ACM, 21, 2, pp.120-126（1978）
4）W. Diffie and M.E. Hellman: "New directions in Cryptography", IEEE Tran. on Information Theory, IT-22, 6, pp.644-654（1976）
5）National Institute of Standards and Technology: "Digital Signature Standard（DSS）", Federal Information Processing Standards Publication 186-4（July 2013）
6）ISO/IEC 18033-2:2010, Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers
7）CRYPTREC: Cryptography Research and Evaluation Committee, http://cryptrec.go.jp/
8）RSA, http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf
9）National Institute of Standards and Technology: "Digital Signature Standard（DSS）", Federal Information Processing Standards Publication 800-56 Ar2（May 2013）
10）NESSIE: New European Schemes for Signatures, Integrity and Encryption, https://www.cosic.esat.kuleuven.be/nessie/

満保（まんぽ）　雅浩（まさひろ）　1988年，金沢大学工学部電気・情報工学科卒業．1993年，東京工業大学大学院理工学研究科博士後期課程修了．2011年より，金沢大学教授．情報セキュリティの教育・研究に従事．博士（工学）．

講座

映像情報メディア関連のセキュリティ〔第8回〕

量子暗号

鶴丸豊広†

1．まえがき

量子暗号は，通信を盗聴しようとするどんな盗聴者に対しても盗聴を防止できる安全な暗号方式です．なおこの暗号方式は，これまでこのシリーズで対象としてきた暗号とは違って，まだ一般には普及していない，次世代の暗号方式です．

RSA方式をはじめとする，現在普及している暗号方式（これを以下，現代暗号と呼ぶことにします）は，既存の方式のコンピュータで，既知のアルゴリズムを使ったとしても，人間が想定しうるまともな時間内（例えば，100億年以内）では解読ができないという「予想」（計算量的な仮定）に基づいて安全性が保証されています．例えば，広くつかわれているRSA方式は，素因数分解が効率的に短い時間で実行できないという予想が正しい限りにおいて安全となっています．逆にいうとこれらの方式は，新アルゴリズムや，（量子コンピュータのような）新原理のコンピュータの出現により，ある日突然破られる可能性があります．

量子暗号の場合はこれより一歩進んでいて，安全性の根拠となっているのは予想ではなく物理法則です．そしてその物理法則は量子力学です．もしこの方式が破れたとすると，それは量子力学に反する現象が起こったことを意味します．量子力学がみつかってから100年近くたちますが，いまだにそれに反する現象は報告されていません．例えば，半導体の物性や素粒子の挙動といった具体的な物理現象でも，すべて量子力学と合致した測定結果が得られています．すなわち，仮に新原理のコンピュータが出現したとしても量子力学が変わることはありませんので，量子力学のもとで安全性が保証されている量子暗号は依然として盗聴不可能です．そのためそこで共有した乱数は未来永劫漏えいすることはないと考えられています．

本稿では，量子暗号の概要，現状の課題，および今後の方向性について紹介していきます．とくに既存の暗号方式を比較対照にして，暗号装置として実際に使う場合のメリットとデメリットについて整理するとともに，その現状のデメリットの解消にむけた取組みについても紹介します．デメリットについて述べる箇所では，量子暗号を否定しているように感じられる内容も含んでいますが，著者の真意は決して量子暗号を否定することではありません．むしろ，このような課題を正面から分析して楽しむことによって，量子暗号研究のさらなる発展に寄与していきたいと考えています．なお量子暗号に関するこれまでの文献では，個々の課題については指摘されているものの，それらをまとめて分析したものは著者の知る限り存在しないようでした．それらをまとめて議論することも，本稿の目的の一つです．

2．量子暗号の機能と安全性

比較として，現代暗号の機能について思い起こしてみましょう．RSA方式をはじめとする現代暗号方式では，メッセージから暗号文を作ることを目的としています．そして暗号文を自由に複製し，電子メールに添付したり，印刷して封書で送ったりすることができます．また，インターネットで送ることもできます．一方で量子暗号は，このような素朴な暗号方式と二つの意味で異なります．

一つ目の違いとして，量子暗号の役割はメッセージを直接送ることではなく，それを暗号化するために必要な鍵，つまり乱数を安全に送ることにあります．一旦そのような乱数が安全に共有できたら，あとはそれをメッセージと排他的論理和をとる（ワンタイムパッド）ための値や，ブロック暗号の秘密鍵として使えば秘密通信ができるので，「暗号」の名がついています．ただし量子暗号装置自身の機能は，あくまで秘密鍵を共有するところまでです．現代暗号の用語でいうなら，量子暗号の機能は鍵共有のみであり，メッセージの暗号化は別の方式に任せるということです．ただし現代暗号でも，Diffie-Hellmann（DH）方式のような鍵共有方式があり，この一つ目の意味だけですと量子暗号特有というほどの特徴ではありません．

二つ目の違いがむしろ量子暗号ならではの特徴です．上述のとおり，量子暗号の目的は乱数を安全に送る/共有す

† 三菱電機株式会社 情報技術総合研究所
"Security Technologies on Image Information (8): Quantum Cryptography" by Toyohiro Tsurumaru (Information Technology R&D Center, Mitsubishi Electric Corporation, Kanagawa)

ることですが，その際，乱数を運ぶための媒体は，インターネットや紙ではだめで，ある物理的性質を持つものでなければなりません．そしてその物理的性質を規定しているのが量子力学です．

またその性質をもつものを量子と呼ぶことがありますが，この先の説明においては，量子とは要するに極端に弱めた光のことだと思っても支障はありません．量子暗号では，極端に弱めた光をランダムに変調して（スクランブルをかけて）光ファイバのような光が通る通信路を用いて送受信します．その光が途中で盗聴された場合，量子としての性質により，必ず何らかの変化が起こります．そしてその変化を見ることにより盗聴を検出する，というのが基本的な考え方です．

以下では，この点についてできるだけ詳しく述べていきます．本稿の理解する上で必要になると思い，量子力学についても一部触れています．この部分に興味のない方は3章まで飛んでいただいても，ひととおり意味はわかるようになっています．なお，以下はかなりデフォルメした説明になっていますので，意味不明な箇所もあると思いますが，そのような場所でも立ち止まらずに雰囲気を味わっていただきたいと考えています．より正確なところを知りたい方は，文献1）等を参照していただきたいと願います．

2.1　量子力学について

どのような物質でも，分子のサイズ以下の微小な精密測定をすると，高校で習うようなニュートン力学や電磁気学とはつじつまが合わない性質を示すということに，100年ほど前のヨーロッパの物理学者が気付きました．そこで，そのつじつまを再度合わせるために登場したのが量子力学です．つまり量子力学は，ニュートン力学や電磁気学といった理論の後継バージョンです．そして，ニュートン力学や電磁気学では説明がつかないが，量子力学では説明のつくような性質のことを量子的な性質と呼びます．量子暗号ではこの量子的な性質を使って，絶対に破れない暗号を実現します．

とくに量子暗号に限っていえば，量子として使うのは原子核でも電子でもなく，もっぱら光だけです．以下に述べるとおり，光の強度を極端に弱めて，さらに2種類の変調方式を使い分けて送受信すると，量子的な性質が表れてきます．とくに量子暗号では，不確定性原理という性質が本質的になります．

2.2　光を弱める

物質を細かく測定する場合は分子レベルの精密測定をすると書きましたが，光の場合はそれが光を弱めることに相当します．これが量子暗号ですべきことの一つ目です．具体的にどれくらい光を弱めればいいかについても明確な基準があって，それがエネルギー量子（$=h\nu$ジュール．ただしνは光の振動数（毎秒），hはプランク定数$h=6.63\times10^{-34}$ジュール秒です）と呼ばれる量です．量子力学ではこのエネルギー量子を単位にして光を1個2個…と数えて，その1個ずつを光子と呼びます．量子暗号ではパルスレーザの光を減衰器で弱めて，1つのパルスあたり1個程度の光子しかない状況を作ります（図1）．これは通常の光通信の1/100万分くらいのエネルギーしかない弱い光です．

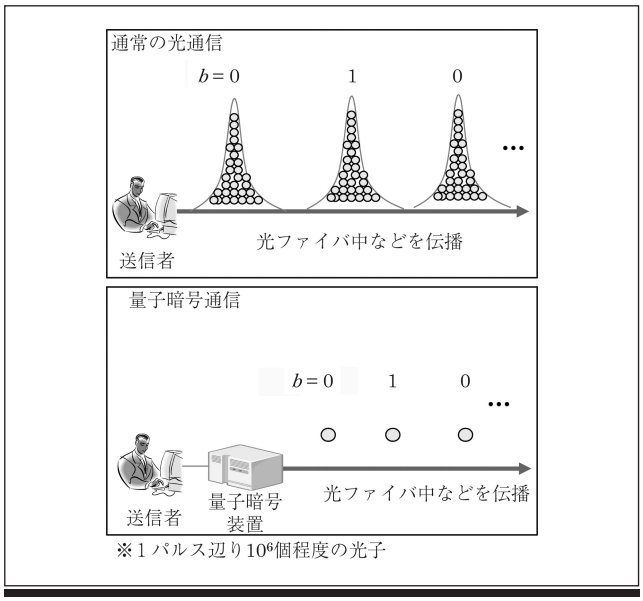


図1　量子暗号における光強度

2.3　2つの変調方式をランダムに使う（スクランブル）

こうして弱めた光パルス1つずつに，乱数ビット値0,1をのせて送受信します．その際に，後で説明する2つの異なる変調方式，X基底とZ基底をランダムに切替えます．これは，盗聴行為を検出しやすくするために，スクランブルをかけることに相当します．量子暗号の用語では，変調方式のことを「基底」と呼びます．そして2種類ある変調方式をそれぞれX基底，Z基底と呼ぶことが多いです．

X基底，Z基底の実装法にはさまざまなやり方がありますが，イメージしやすいのは，光の偏光（振動方向のこと）を使うやり方です．この方法では，進行方向を軸として0°，90°方向（45°，135°方向）に振動する光パルスに，ビット値0,1をそれぞれあてはめるのがZ基底（X基底）です．要するに量子暗号では，光を弱めたうえで，1ビット分の情報（0,1）を，4つの状態（振動方向0°，45°，90°，135°）に水増しして送っていることになります．

2.4　不確定性原理

もし通常の通信のように光が充分強ければ，測定によって，これら4つの振動方向を特定できてしまいます．すなわち，充分強い光を弱い光に分離して，4つの測定を行うことで，どの基底が使われ，どのビット値があてはめられているかがわかります．また1種類の変調方式（基底）しか使わなければ，光の強弱に関わらず，やはり乱数ビットを測定で特定できてしまいます．つまり例えば，X基底で0,1に符号化された光子を，同じくX基底で測定した場合を考

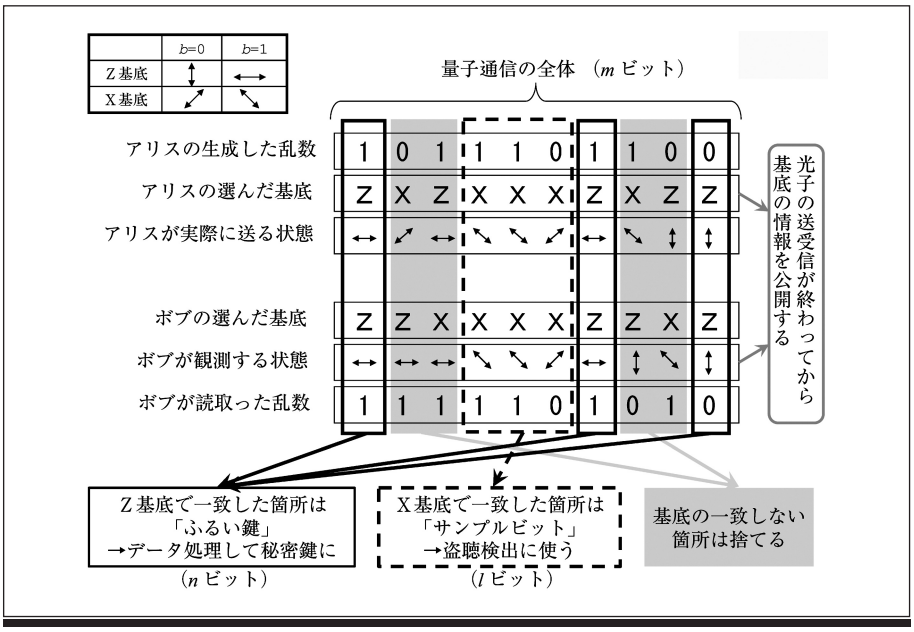


図2　盗聴者がいない場合の処理の流れ

えると，常に正しいビット値0,1が測定されます．これらにより盗聴が可能となります．しかし光を弱めて，なおかつスクランブルを行うとすると，乱数ビット0,1の値を確実に測定することは不可能になります．これが通常の電磁気学とは違う，量子論的な性質の一例であり，不確定性原理と呼ばれています．例えば，単一光子にX基底でビット値0,1に符号化したのち，それをZ基底で測定するとします．このときの測定結果は，もとの値0,1に関係ないランダム値0,1になります．なおかつ測定が終了した時点で光子の状態は変化しているので，基底を変えて再度測定し直したとしても，元の値は再現できません．

ここで重要なことは，このような現象が起こるのは，測定装置の性能が足りないからとか，測定の方法に不備があるからという理由によるのではないということです．そうではなく，単一光子を一度測定したら，同じ状態が保持されず，測定をやり直すことができないという状況が，物理法則（量子力学）のために生じています．したがってこの状況は，測定装置の性能がいくら向上しても改善しません．これがニュートン力学とは違う，量子的な性質の一例です．

2.5　BB84プロトコル

量子暗号ではこの不確定性原理を使って盗聴を検出します．正規の送受信者は，X, Z基底をランダムに振って送受信します．一方で盗聴者は，どの基底が選択されているかを知らずに乱数値を測定せねばなりません．ここで光子を一旦測定してしまうとその状態が変化してしまいます．従いまして，誤った基底で測定をするとその状態を正確に知ることができず，測定しなおすこともできないため，元に戻すことができません．正しい基底で測定していれば，正しい状態がわかるので，同じ状態を持つ光を再送信することで，同じ状態を作ることが可能です．正規の送受信者は，少なくとも，誤った基底を用いて盗聴された場合の痕跡を検出すれば，盗聴を検出できます．

ここから先は具体的なプロトコルをみた方が速いので，Bennett-Brassard 1984（BB84）方式を例にとって話を進めます．この方式は1984年に提案された最古の量子暗号方式であり，これまで最も深く研究されてきた方式でもあり，安全性も厳密に証明されています．

● 使用する通信路

このプロトコルでは，2つの通信路を使います．

・量子通信路：乱数を光子にのせて送るためのもので，通常は光ファイバが使われます．盗聴者は，ここを流れる光子を自由に盗聴できるものとします．

・認証つき公開通信路：乱数本体ではなく，補助的な情報（選択された基底，サンプルビットの値）を送るためのものです．これらはディジタル信号なので，例えば，インターネットや携帯電話が使えます．盗聴者は通信内容を自由に盗聴できますが，改変はできないとします．改変を防ぐために，通常はWegman-Carter方式と呼ばれる情報理論的なメッセージ認証方式を使います．

● プロトコルの手順

図2もあわせてご覧ください．またこの節では通信における送信者をアリス（Alice），受信者をボブ（Bob），盗聴者をイブ（Eve）と呼ぶことにします．

(1) 量子通信：

1-1 アリスは，m ビットの乱数ビットを，それぞれ個別の光子パルスに，X, Z基底をパルスごとにランダムに選んで変調し，量子通信路を通じてボブに送信します．

1-2 ボブは，X，Z基底をパルスごとにランダムに選び，受け取ったパルスを測定します．
1-3 アリスとボブはお互いに選択した基底を，公開通信路を使って公開します．お互いの基底が一致したパルスの乱数ビットのみを残し，それらをまとめて生鍵（raw key）とします．それ以外のビット値は破棄し，以後の処理には使いません．
1-4 生鍵ビットのうちZ基底のもの（長さnビットとする）をまとめて，ふるい鍵（sifted key）と呼び，X基底のもの（長さlビットとする）をまとめてサンプルビットと呼びます．

(2) サンプルビットの誤り率p_{smp}の算出：アリスとボブはお互いがX基底で測定した分（つまりサンプルビット）を公開し，その誤り率を算出してp_{smp}とします．

(3) 誤り訂正：アリスはkビットのシンドローム（パリティ情報）を公開します．ボブはそのシンドロームと誤り訂正符号を用いて，自分のふるい鍵の誤りを訂正します．なお訂正されたふるい鍵を，訂正鍵と呼びます．

(4) 秘匿性増強処理：
4-1 秘密鍵長算出：ステップ(2)で算出したp_{smp}をもとに，パラメタ$s=\max[n(1-h_2(\hat{p}_x))-k-t,0]$の値を算出します．これが以下で最終的に生成される秘密鍵の長さです．なおここで$h_2(x)=-x\log_2 x-(1-x)\log_2(1-x)$は2値エントロピー，$t$はある定数です（4.1節(1)参照）．また$\hat{p}_x$は，ここではひとまず簡単のため，ステップ(2)で算出したp_{smp}と等しい，つまり$\hat{p}_x=p_{\mathrm{smp}}$だと思ってかまいません（正確にいうと$\hat{p}_x$は$p_{\mathrm{smp}}$を変数にもつ関数であり，ふるい鍵長が充分大きい（$n\to\infty$）とき，$\hat{p}_x\to p_{\mathrm{smp}}$に漸近します）．
4-2 ランダム行列乗算：ランダムなビット値をもつ$s\times n$行列Mを生成し，それに(3)で出力した訂正鍵を乗算します．そして，その乗算の結果得られた長さsのビット列を秘密鍵とします．

こうして得られた秘密鍵を，ワンタイムパッドの鍵として使えば，絶対安全な秘密通信ができます．またそれ以外にもメッセージ認証等の秘密鍵として使うこともできます．

● プロトコルの解説

上記の各ステップのこころは以下の通りです．

まずステップ(1)の量子通信では，①イブからみるとX, Z基底がランダムに選ばれていて，なおかつ，②アリスとボブの基底選択は一致している，という状況が作りたいわけです．これを安直に実現するには，アリスとボブが予め乱数を共有しておいて，それで基底を選ぶという方法も考えられるのですが，それだと生成する乱数よりも消費する乱数が大きくなって意味がありません．そこで代わりにステップ(1) 1-1で送りだす光パルス数に無駄を許して，余分に送りだすという戦略をとります．つまりアリス，ボブが基底を各自勝手にランダムに選び，たまたま基底が一致したパルスの測定結果だけを採用して生鍵とします．また基底が一致しなかったパルスは無視して捨てて（つまり忘れて）いますが，この行為は以下のとおり正当化できます．まず，そもそも送っているのがメッセージではなく乱数なので，捨ててそれ以降決して使わないという運用が可能です．決して使わない情報が盗聴者に漏れたところで実害はありませんので，暗号の安全性としても問題ないのです．

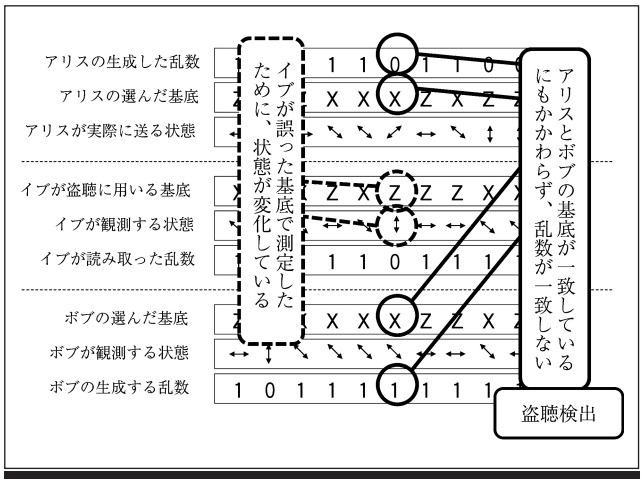


図3　盗聴検出のイメージ

したがって安全性を考える分には，基底が一致しなかった部分は忘れて，生鍵だけを考慮すればよく，そこでは上記の状況①，②が実現できています．そしてその状況が，アリスとボブがZ基底でふるい鍵を測定している最中に，たまにランダムなタイミングでX基底測定を繰り出しているとも解釈できます．イブにしてみれば，このX基底測定はいわば抜き打ちチェックです．つまり，ふるい鍵の内容を探ろうとZ基底で盗聴をしている最中に，アリスとボブが突如X基底に切替えるわけで，イブはある確率で誤った基底（Z基底）の測定を仕掛けることになり，それによりサンプルビット列の誤り率p_{smp}が増えます（図3）．つまりp_{smp}はイブの盗聴行為の強さに相当しますが，これを検出するのがステップ(2)の役割です．

より定量的には，サンプルビットの誤り率がp_{smp}であれば，盗聴によってイブに$nh_2(p_{\mathrm{smp}})$ビット程度（正確には$nh_2(\hat{p}_x)$ビット）分の情報が漏洩していると結論できます（安全性証明の理論による）．さらにステップ(3)の誤り訂正でkビットのシンドロームを公開しているので，ステップ(3)で生成された訂正鍵nビットのうち，合計$nh_2(p_{\mathrm{smp}})+k$ビット程度（正確には$nh_2(\hat{p}_x)+k$ビット）分がイブに漏洩していると結論できます．非常に大雑把ないい方をするなら訂正鍵には，盗聴者の知っている$nh_2(p_{\mathrm{smp}})+k$ビットと，知らない残りの$n-(nh_2(p_{\mathrm{smp}}\hat{p}_x)+k)$ビットが混在している状況にあります（図4）．

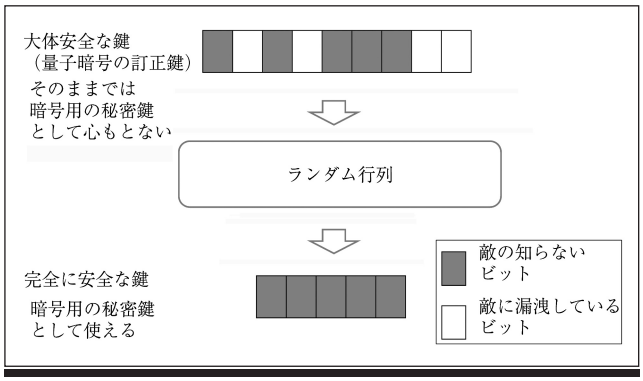


図4　秘匿性増強の大まかなイメージ
秘匿性増強とは，「大体安全」な暗号鍵を「完全に安全」にする統計処理です（＊この図はあくまでイメージです）．

この訂正鍵を暗号通信用の秘密鍵として使うのは明らかに危険です．そこでステップ（4）の秘匿性増強処理では，訂正鍵にランダム行列をかけて撹拌，圧縮することにより，盗聴者が知らない$n-(nh_2(p_{\mathrm{smp}}\hat{p}_x)+k)$ビット分だけを取出しています（図4）．これによって最終的に，厳密な意味で安全な秘密鍵が生成されます．

秘匿性増強のイメージをつかむには，以下の例がわかりやすいと思います．訂正鍵が2ビットあり，どちらかわからないがそのうち1ビットの値が盗聴者に漏れていて，もう1ビットは漏れていないとします．このとき明らかに，その2ビットをXORして1ビットに圧縮してしまえば，その値は盗聴者にもまったくわからなくなります．より一般のビット数の場合には，XORではなくランダム行列を使えばいいことが知られていて，それがいわゆる秘匿性増強です．

なおここでは簡単のため，イブが常にX，Z基底のどちらかで盗聴を行うとして話を進めました．実際の量子暗号の理論ではこのような制約は存在せず，イブが物理法則で許される限りのあらゆる攻撃をしたとしても，安全性が成り立つということが証明できています．

3．実装の現状

量子暗号の研究は1984年に提案されたBB84方式に始まりました．現在でも，この方式の改良版であるデコイBB84方式が事実上の標準方式になっています．1992年には提案者自らが実証実験に成功し，2000年代には世界中で実験報告が爆発的に増えました．2010年頃には通信距離50 km，通信速度1 Mbpsといった性能を，NECや東芝欧州研など複数の研究機関が安定して叩き出すようになり今日に至ります．

またこのようなトップスピードとは乖離があるものの，量子暗号の製品を売る企業も複数存在しています．すでに2000年代前半にはベンチャー企業が複数存在していて，そのなかでもスイスのid Quantique社，および中国のQuantumCTek社は現在も活発に活動しています．とくにid Quantique社のある社員によれば，同社にはこれまで100台程度の販売事例があるといいます（具体的な顧客名は公表されていませんが）．

2008年に欧州の複数の大学とベンチャー企業が，各々の量子暗号装置を持ちより，ウィーンでネットワーク通信実験を行いました（SECOQCプロジェクト）．つづいて類似のプロジェクトが2010年に東京（Tokyo QKD Network），2012年に中国の合肥市，2013年に同じく中国の済南市でも実施されました．さらに2013年には米国Battelle社が，id Quantique社の量子暗号装置を複数つなぎ合わせて，全長400 kmの商用量子暗号通信ネットワークをオハイオ州に構築しました．さらに同社は2016年までに，オハイオ州・ワシントンDC間650 kmを結ぶ量子暗号線を構築するとしています．また中国も同じく2016年までに国家プロジェクトとして，上海・合肥・済南・北京の4都市を結ぶ全長2,000 kmの量子暗号ネットワークを構築するとしています．

4．既存の暗号方式との比較

1990年代以降「量子コンピュータが実現すると公開鍵暗号が破れるのに対し，量子暗号は破れない．そこで量子暗号が必要になる」という宣伝文句が盛んに使われ，実際にそれが量子暗号の研究の推進に大きく役立ちました．そして2000年代には，量子暗号はすでに実験室の外に飛び出せており，2010年前後からは世界各国で，国家プロジェクトによる大規模ネットワーク実験も進んでいます．しかしながら現在でも，商用で運用された例は明らかになっておらず，普及しているとはいい難い状況にあります．

量子暗号の研究者はそれに対して「まだ量子コンピュータが普及していないから」とか「量子暗号のコストが高いから」といった理由を挙げることが多いですが，以下ではこの点を深く掘り下げてみます．とくに量子暗号を既存の暗号方式と比較することにより，暗号としてのメリットとデメリットを整理してみます．

4.1　現代暗号との強度比較

まずは量子暗号の安全性，つまり暗号強度について整理します．

（1）情報理論的安全性

量子暗号のメリットは，何といってもその安全性です．冒頭でも述べたとおり，現代暗号は結局のところ，ある種の予想（仮定）にもとづいて安全とされているだけです．何らかの都合のよい予想（例：素因数分解が効率的に解けない）を設定し，さらに盗聴者の計算能力を制限（チューリングマシン上で多項式時間）したうえで，盗聴成功確率を評価しています．そしてその確率が無視できるほど小さい場合のみ，その暗号方式は安全だとされます．逆にいうと現代暗号は，設定した予想や制限の根拠が失われた場合には破れる可能性があります．例えば，量子コンピュータが実現したら，RSA方式やDH方式といったメジャーな公開鍵暗号方式は破れてしまうことが知られています．

これに対し量子暗号には，そのような予想や制限は一切ありません．盗聴者が通信路上の光子をどう盗聴しても，その盗聴成功確率はある確率以下であると厳密に証明できます．なおかつ送受信者は，その確率を（秘匿性増強におけるパラメータt（現代暗号における鍵の長さに類似するパラメータ）を大きくすることにより）いくらでも小さく抑えることができます．このように，盗聴者の計算量の制約なしに，盗聴成功確率を抑えることのできる暗号方式を，情報理論的に安全な暗号方式と呼ぶことがあり，量子暗号もその一種です．もちろん量子コンピュータが実現しても，量子暗号は安全なままです．

このように量子暗号には，現代暗号とは次元の違う高いレベルの安全性（情報理論的な安全性）が実現できるというメリットがあります．もし現代暗号の安全性を，量子暗号と同じ設定で考えるなら，つまり予想や制限を一切撤廃したら，現代暗号はたちどころに破れてしまいます．すなわち量子暗号の基準でいうと，現代暗号は暗号ですらないということになります．現代暗号と量子暗号の安全性を直接比較することは，そもそも不可能なのです．

(2) 量子コンピュータへの耐性

繰り返しになりますが，量子コンピュータが実現した場合，RSA方式やDH方式といった主な公開鍵暗号方式は破れてしまいますが，量子暗号は安全なままです．ただし現代暗号側にも公平を期していうなら，これは決して，現代暗号がすべて破れるという意味ではありません．

そもそもRSA方式やDH方式が公開鍵暗号のすべてというわけではなく，それ以外にも昔からさまざまな方式が知られています．とりわけ多変数多項式暗号や格子暗号といった方式については，量子コンピュータによる解読法は見つかっていませんし，恐らく解けないだろうと予想されています．むしろこれらの方式は最近，その性質から「ポスト量子暗号」（Post-quantum Cryptography）と呼ばれ，盛んに研究されるようになっています（例えば文献2））．またAESやMISTYといった共通鍵暗号も同様に，量子コンピュータによる解読法は見つかっていません（Groverのアルゴリズムと言われる演算方法を使っても，解読時間が従来の1/2乗に削減されるだけです．したがって指数関数時間の指数部分が半分になるだけで，依然として指数関数時間であることには変わりがありません）．

したがって量子コンピュータが実現したとしても，解けないという予想で満足できるならば，ひきつづき現代暗号を使い続けることができます．量子暗号が必要なのはそのような予想では満足できず，情報理論的な安全性が欲しいというユーザに限られます．

4.2 公開鍵暗号との機能比較

つぎは公開鍵暗号との機能比較をします．

そもそも公開鍵暗号が広く利用されている最大の理由は，暗号通信を始めるまでに必要な鍵のセットアップが簡便になることにあります．もし公開鍵暗号が使えなくなったとして，そのとき量子暗号が，公開鍵暗号と同様のメリットをもたらすことはできるのでしょうか（これは要するに現代暗号でいうところの鍵配送の問題ですが，量子鍵配送やDH鍵共有といった用語との混乱を避けるため，ここでは「鍵のセットアップ」という言葉を用いることにします）．

太古の昔から1970年代前半に至るまで，すべての暗号は共通鍵暗号でした．これはユーザAとBがそれぞれ同じ秘密鍵k_{AB}を共有しておいて，メッセージの暗号化に使うものです．AがBだけと秘密通信を行いたい場合にはこれで終わりですが，そこにさらにCさん，Dさん，…が加わっていくと，それに応じて秘密鍵k_{AC}，k_{AD}，…を共有する必要があります．一般にN人のユーザがお互いに自由に秘密通信をしたい場合，各ユーザは自分以外の$N-1$人と異なる鍵を共有したうえで，安全に保管しなければなりません．したがってN人全体では，合計$\binom{N}{2}=N(N-1)/2$種類の異なる鍵を共有，保管する必要があります．

しかし1990年代以降インターネットが普及して，世界中と自由に通信できるようになると，すべての相手と秘密鍵をいちいち共有しておくのは不便だということになり，RSA方式に代表される公開鍵暗号，およびディジタル署名が使われるようになりました．具体的にはまず，各ユーザが自らの公開鍵を一つ公開します．つぎに，公開鍵のすり替えを防ぐために，信用できる認証局を最低1ヵ所設置し，公開鍵をディジタル署名してもらいます．つまり公開鍵基盤（PKI）を構築します．結果として，各ユーザは公開鍵を生成したのち，認証局と一度だけ安全なやりとりをすればよいだけであり，セットアップの手間は大幅に削減されます．全体としては最初に$O(N)$個の公開鍵を，認証局に安全に送ればよいだけです．

それでは量子暗号の場合はどうかというと，少なくとも現状の方法そのままでは，共通鍵暗号の場合と同様に，セットアップに際して$O(N^2)$個の秘密鍵共有が必要になります．量子暗号は，DH方式と同様に，鍵共有の機能を実現できる方式なのになぜ？と思われるかもしれませんが，問題は古典通信路のメッセージ認証にあります．

量子暗号の存在意義は，情報理論的な安全性にあるので，メッセージ認証にも情報理論的な方式を使わなければなりません．このため公開鍵的なメッセージ認証方式，つまりディジタル署名は使えません．実際の量子暗号装置ではそのかわりに，Wegman-Carter方式と呼ばれる情報理論的な方式を使っています．この方式では，共通鍵暗号の場合と同様に，N人のユーザがいたら，各ユーザは$N-1$種類の異なる秘密鍵を事前に共有しなければなりません．そして全体としてはやはり，合計$N(N-1)/2$種類の異なる鍵を共有して保管する必要となります．

以上をまとめると，N人のユーザがいたとして，公開鍵暗号では鍵のセットアップの手間は$O(N)$で済みます．こ

れに対し量子暗号は1対1の秘密通信に適した方式であり，セットアップに$O(N^2)$の手間がかかってしまいます．つまりこの比較においては，公開鍵暗号と同様のメリットを果たせないようにみえます．

4.3 秘密鍵を手で運ぶ場合とのコスト比較

最後にコストを比較します．4.1節(1)でみたとおり，量子暗号と現代暗号の安全性はそもそも直接比較できないので，コストの直接比較も意味をなしません．そもそも量子暗号の目的は，秘密鍵を安全に配布することでありましたが，そのためのもっとも簡単な方法は他ならぬ，人間が手で運ぶことです．実際に戦前から，軍事用の暗号の乱数表は手で運ばれていたという記録がありますし，現在でも簡単に実行できる方法です．そこでこの方法と量子暗号を，コスト面から比較してみます．

現状の量子暗号装置の例を図5に示します．このような装置は，材料費だけでも1セットあたり数百万円はかかります．そして性能としては，通信距離50 km，通信速度1 Mbpsが敷設ファイバ上で達成できています[3]．そこでかなり楽観的な見積りではありますが，以下では通信距離50 km，通信速度1 Mbpsの量子暗号装置が1,000万円で実装できて，1年間継続して使えるという仮定をおいてみます．そうすると1,000万円で，4 TB程度（＝1 Mbps × 60秒 × 60分 × 24時間 × 365日/8bit）の乱数が運べるという計算になります．これはいまどきのハードディスクドライブ（HDD）1, 2台程度に収まる量ですし，そのようなHDDは1台あたり1万円程度で買えます．であれば，自組織内の信用できる人に毎年1回，HDDを50 km先まで運んでもらえばよいことになります．これだと1日程度の人件費が余計にかかるだけなので10万円程度ですみます．一方で量子暗号は1,000万円ですから，現状ではコストとして100倍程度の開きがあることになります．

ただしこの100倍という数字の精度は高くなく，上下10倍くらいの誤差は平気でありえるので，あくまで一つの目安として考えていただきます．誤差の原因としてまず，量子暗号装置のコストを押し下げる要素があります．いまのところ量子暗号装置の材料には特注品が多いうえに，それを研究者が1台ずつ手作りで組み上げているような状況なので，量産効果はまったく効いていません．したがって，例えば，3節でふれた中国や米国の国家プロジェクトにおいて装置が大量生産されれば価格が下がる可能性はあります．さらに上の比較では距離を50 kmに固定しましたが，これが例えば，10 kmでよければ通信速度は10倍の10 Mbps程度に増やせます．量子暗号では，距離を縮めると，通信速度が指数関数的に増えるという性質があるためです．その一方でもちろん，コスト差を逆に拡げる要素もあります．そもそも上の比較では量子暗号装置の開発費，製造コスト，維持費等は含まれていませんし，その一方で比較対象であるHDDの価格は今後も下落していくと予想されます．

図5 量子暗号装置の例（NEC提供）

5．デメリットの解消にむけた方向性

5.1 運用方法の改良

4章でも述べましたが「量子コンピュータが実現すると公開鍵暗号が破れるのに対し，量子暗号は破れない．そこで量子暗号が必要になる」という宣伝文句がよく使われてきました．しかし4.2節でみた通り，量子暗号は実は1対1の秘密通信に適した方式です．したがって，仮に公開鍵暗号がすべて破れてしまったとしても，量子暗号にその代役は務まらないようにみえます．公開鍵暗号では鍵のセットアップの手間は$O(N)$ですむのに対し，現状のままの量子暗号方式では，セットアップに$O(N^2)$の手間がかかってしまうからです．このデメリットの解消が今後もひき続き重要です．

方向性の一つは，量子暗号の運用方法を工夫して，セットアップの手間を$O(N)$に削減することです．例えば，非常に単純なやり方として，信用できるセンターを1ヵ所設置するものがあります（公開鍵暗号の場合でも，信用できる認証局を最低1ヵ所設置する必要があったことを思い出してください）．そしてセットアップ時にN人のユーザすべてが，センターとの間に，メッセージ認証用の秘密鍵を共有しておきます．あとはすべての暗号通信をセンター経由で行うことにすれば，N人のユーザが自由に暗号通信できます．もちろんこのような単純な方式では，センター1ヵ所に負荷が集中するので必ずしも効率的ではありません．また仮にセンターが悪意を持った場合の被害パターンが，公開鍵暗号のそれと同じとは限りません．これらの問題の解消にむけて，今後さらなる研究が必要と思われます．

5.2 量子鍵配送としての性能向上

4.3節でみたとおり，量子暗号と現代暗号のコストを直接比較することは意味がなく，むしろ，秘密鍵を人間が自ら手で運ぶ状況とのコストを比較すべきです．そしてその差

は現状で100倍程度です．この100倍という数字の精度はあまり高くないし，これを大きいと考えるか小さいと考えるかは個人の感覚や信条の問題です．しかし仮にこのギャップを埋めることができて，秘密鍵を手で運ぶよりも，量子暗号を使った方が安いとか簡単だということになれば，ユーザのメリットははっきりしますし，普及する可能性がでてきます．例えば，コストが1,000倍下がって，毎年1,000台のHDDを自分で運ぶ手間を，100万円の量子暗号装置が代行できるということになれば，その方が便利だと考える人はいるかもしれません．

なおこの種の話では性能指標として，距離，速度，コストの3種類がありますが，どれが改善しても本質的には同じだと考えてかまいません．量子暗号では，距離を縮めると通信速度が指数関数的に増えるという性質がありますので（光ファイバにして50 km縮まるごとに10倍以上）．したがって限界距離が改善したということは，同時に短距離での速度が向上したことも意味します．そして速度が向上すればもちろん，秘密鍵を共有するのにかかるコストも削減できるのです．

いずれにせよ，今ある方式を変えずに，実装技術の工夫だけでコストを1/1,000まで下げるのは難しいことです．したがって今後さらに何段階かのブレイクスルーが必要なわけですが，以下ではそれを狙った取組みについて紹介します．

(1) これまでのブレイクスルー

まず過去を振り返っても，理論の進展やプロトコルの改良によって，量子暗号の性能が向上してきた経緯があります．2000年代前半までは，プロトコルや安全性証明に対する理解が未熟だったために，量子暗号装置には単一光子源，単一光子検出器が必須だと考えられていました．つまり光子1つ1つを厳密に制御する技術が必要だと考えられていました．しかしながら（当時も今も）単一光子源や単一光子検出器の実装は困難なので，量子暗号の実験では安価な代替手段として，光源にはレーザと減衰器が，光検出器にはアバランシェフォトダイオード（APD）が広く使われていました．これらは代替手段であるから，それらを用いた量子暗号装置は，厳密には安全ではないと考えられていました．

しかし2004年になって新たなプロトコルとして，デコイBB84方式が提案され，それにより，レーザを用いたとしても厳密な安全性が保証できるようになりました．また2000年代後半には安全性証明の理論が改良されたことにより，APDを用いても安全性が保証できることが新たに判明しました．この結果，現在ではレーザやAPDはもはや代替手段ではなく，量子暗号の正当な部品とみなされています．そして量子暗号装置の実装コストは劇的に下がり，上述の50 km，1 Mbpsが達成されるに至りました．

(2) プロトコルの改良の方向性

現在でもそのようなブレイクスルー狙いは続いています．1つ目の方向性はプロトコルの改良です．最近の主流は，デコイBB84方式を一旦忘れて，プロトコルを根本から設計し直すものです．有名なものとして，連続変数量子暗号（CVQKD）やRR-DPSQKD方式がありますが，ここでは日本発の技術としてRR-DPSQKD方式について述べます．時系列で説明すると以下のとおりです．

まず発端となったのは，2002年に提案されたDPSQKD（Differential Phase Shift Quantum Key Distribution）方式です[4]．この方式は実は，すでに光通信の世界で知られていたDPSK（Differential Phase Shift Keying）という方式の光強度を落としただけのものでした．DPSKの送信側に減衰器を挿入して出力を単一光子レベルまで落とし，受信側の検出器を高感度なものにおき換えれば，それがDPSQKD方式の量子暗号装置となります．このように既存の光通信用の部品を流用して，比較的簡単に実装できるので安定性が高く，（盗聴者由来ではない）装置由来のノイズが少ないという長所があります．そしてこの長所により，200 kmを超える長距離通信が可能になることが最大の売りです．またヨーロッパではその変形版であるCOW（Coherent One Way）プロトコルが研究されていまして，最近では300 kmを超える通信が可能になったという報告もあります．

ただしこれらのプロトコルでは，デコイBB84方式よりも装置を簡単化した反動として，安全性証明は格段に難しくなってしいました．このため現在でも，盗聴者の能力にある制約を課した場合（コレクティブ攻撃）の安全性しか証明できておらず，制約なし（コヒーレント攻撃という）での安全性は証明できていません．

この状況を打開するため，2014年にRR-DPSQKD（Round Robin DPSQKD）方式が提案されました[5]．これはDPSQKD方式に，ある種のスクランブル処理を付加したものです．それによって安全性証明で扱う数式が簡単化され，コヒーレント攻撃に対する安全性が証明できるようになりました．なおかつこの方式が，通信路の擾乱に対して非常に優れた耐性を持つということが判明しました．この性質を利用すれば，量子暗号の性能を飛躍的に向上できる可能性があるため，現在研究が盛んになりつつあります．

(3) 安全性証明理論の改良の方向性

ブレイクスルー狙いのもう1つの方向性は，安全性証明理論の改良です．中でも最近は，装置無依存量子暗号（Device Independent QKD，以下DIQKD）に関する研究が活発になっています（文献6）およびその参考文献参照）．これは一言でいうと，光の送受信機（装置）をどう実装したかには関係なく（無依存），ある手順（プロトコル）にしたがって通信している限りは，必ず盗聴が検出できるというアイディアです．そしてその手続き（プロトコル）のことを，装置無依存な量子暗号方式と呼びます．

DIQKDの目的は，サイドチャネル攻撃の問題を一気にすべて解決することにあります．現代暗号と同様に，量子

暗号でもサイドチャネル攻撃の問題があります．つまり暗号装置が壊れたり，調整を間違えたりした場合，それによって盗聴が容易になり，乱数が漏えいするという問題があるわけです．例えば，BB84方式のレーザの強度の調整を誤って，単一光子レベルよりずっと強い光が出ていれば，盗聴者は4種類の状態（振動方向0°，45°，90°，135°）を測定によって識別でき，乱数の値を確実に読取れてしまいます．ただしこれも一例にすぎず，これ以外にもサイドチャネル攻撃は無数にありえます．そしてそれを人がすべて1つずつチェックして塞ぐことは事実上不可能です．

DIQKDとは，安全性証明理論の改良により，そのようなサイドチャネル攻撃を一網打尽にする考え方です．まずBB84方式では誤り率をチェックすることによって，盗聴を検出していました．その一方で1991年に提案されたEkert 1991（E91）方式では，誤り率に加えて，ベル（J.S. Bell，人名)不等式と呼ばれる関係式をチェックしています．そして2000年以降の理論研究の進展により，実はこのベル不等式チェックが，あらゆるサイドチャネル攻撃を検出する能力を秘めていた，ということが判明しました．例えば，前段落のレーザ強度の例でいえば，光強度が強ければそれは必ずベル不等式チェックで検出されます．なおかつそれ以外のあらゆるサイドチャネルについても，同様にベル不等式チェックで検出されるということです．したがってE91プロトコルでは，ベル不等式チェックさえ通過できている限り，サイドチャネル攻撃の心配をする必要がないのです．

このようにDIQKDはもともと，量子暗号の安全性向上のために導入された証明テクニックです．しかし著者はこれが量子暗号のコスト削減にも役立つと期待しています．まず量子暗号全般にいえることとして，コストダウンを狙って部品を安価なものに置き換えると，安全性証明は難しくなります．部品が安価であればあるほど，その挙動を記述するための数式は複雑になる傾向があって，その結果，安全性証明で扱う数式も難しくなるからです．DPSQKD方式やCOW方式の安全性証明が困難を極めているのも，このような事情によります．しかし「装置無依存」の名が示す通り，DIQKDの理論では，部品に対応する数式の複雑さに関係なく，安全性証明をつけることができます．これによりDPSQKD方式やCOW方式の安全性証明が成功すれば，量子暗号の通信距離は飛躍的に向上すると期待されます．

6．むすび

本稿では，既存の暗号方式を比較対象にして，量子暗号の暗号装置としてのメリットとデメリットを整理するとともに，デメリットの解消にむけた取組みについて議論しました．これをきっかけにして，現代暗号の研究者が量子暗号について興味を持っていただき，ざっくばらんな議論ができるようになれば幸いです．

なお本文中では量子暗号をつかった秘密通信のみについて紹介しましたが，決してこれが量子暗号研究のすべてというわけではありません．これ以外にも量子的な性質を使った電子現金，ディジタル署名，暗号プロトコル等に関する研究も引き続き続けられています．これらの分野の今後の発展についても期待したいと思います．

（2015年8月7日受付）

〔文　献〕

1）M.A. Nielsen and I.L. Chuang: "Quantum Computation and Quantum Information", Cambridge University Press (2000)，日本語版：木村達也訳：“量子コンピュータと量子通信”，オーム社（2005）
2）高木剛：“ポスト量子暗号”，数学セミナー，7，日本評論社（2015）
3）A.R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe and A.J. Shields: "Continuous operation of high bit rate quantum key distribution", Appl. Phys. Lett. **96**, 161102（2010）
4）K. Inoue, E. Waks and Y. Yamamoto: "Differential Phase Shift Quantum Key Distribution", Phys.Rev.Lett., **89**, 037902（2002）
5）T. Sasaki, Y. Yamamoto and M. Koashi: "Practical quantumkey distribution protocol without monitoring signal disturbance", Nature **509**, 475-478（2014）
6）U. Vazirani and T. Vidick: "Fully device independent quantum key distribution", Phys. Rev. Lett. **113**, 140501（2014）

鶴丸（つるまる）　豊広（とよひろ）　2001年，東京大学大学院理学系研究科物理学専攻博士後期課程修了．同年，三菱電機（株）入社．情報技術総合研究所勤務．以来，現代暗号と量子暗号に関する研究開発を続けている．博士（理学）．

講 座

映像情報メディア関連のセキュリティ〔第9回〕

電子透かし

栗林　稔†

1．まえがき

情報ハイディング（Information Hiding）技術は，秘密の情報をどこかに密かに忍ばせることや，通信自体を隠すことを実現させるための技術の総称として扱われています．特にディジタルコンテンツを取り扱った情報ハイディング技術では，コンテンツの品質をあまり損ねることなく情報を埋め込むことが可能であり，その埋め込まれた情報を正しく抽出することが可能です．より皆様の身近なところでは，Adobe社のPhotoshopに搭載されている画像に情報を埋め込む機能のplug-inが有名です．

情報ハイディング技術は，その目的や用途に応じて二種類に分類されます．埋め込む情報が重要であり，かつその存在が知られないことが求められる場合には，ステガノグラフィ（Steganography）と呼ばれます．一方，秘密の情報が埋め込まれたコンテンツ自体が重要な場合には，電子透かし（Digital Watermark）と呼ばれます．文献によってはこれらの用語の定義が異なることもありますが，本稿ではこのように分類するように致します．

本稿で紹介する電子透かしは，次に示すように目的に応じて二つに分類することができます．コンテンツを歪ませる攻撃に対して高い耐性を有する，いわゆるロバスト電子透かし（Robust Watermark）と，反対にコンテンツのわずかな歪みに対して脆弱なフラジール電子透かし（Fragile Watermark）です．ロバスト電子透かしは，各種攻撃に対して高い耐性を有することから，著作権保護や不正者特定などの用途が想定されます．一方，フラジール電子透かしはコンテンツの改ざん検知が主な用途として考えられています．

電子透かしでは，透かし情報の入っていない元のコンテンツを検出時に必要としない場合はコンテンツ非参照型方式（ブラインド方式）と呼ばれます．ある透かし入りコンテンツが与えられた際に，元のコンテンツを特定すること自体が難しい場合や，保存されている元のコンテンツまでのアクセスができない場合が一般的であるため，元のコンテンツを必要とする非ブラインド方式は実用性に欠けると考えられます．厳密には，ブラインド方式では，元のコンテンツそのものだけでなく，元のコンテンツに関する情報すべてが不要であることが求められます．例えば，画像のある周波数成分にのみ透かし信号を埋め込む方式において，その周波数成分の値を保存して検出時にその値のみを参照する場合はブラインド方式とは言えません．ブラインド方式の電子透かしはこれまでに多数提案されていますが，本稿ではその中でも代表的なスペクトル拡散法や量子化法を紹介します．

2．コンテンツと透かし情報

電子透かし技術が対象としているコンテンツとしては，主に画像（静止画），映像（動画），音響（音楽），音声，テキスト（文書）などが挙げられます．他にも3Dのポリゴンデータや，pdfファイル，XMLファイルなどのデータもありますが，ここではディジタル信号処理されることを想定したコンテンツについて考えます．

電子透かし技術は，ディジタルコンテンツを雑音のある通信路とみなして，透かし情報を何らかの通信用信号に変調した上で送受信するシステム（図1）であると考えることができます．この通信路の特性はコンテンツに大きく依存することになります．また，状況によってはもう一つの雑音のある通信路の存在も考えなければなりません．最初の通信路で想定される雑音はコンテンツに起因する雑音成分ですが，もう一つの通信路は攻撃に起因する雑音を想定したものです．透かし情報をコンテンツに埋め込む際には，

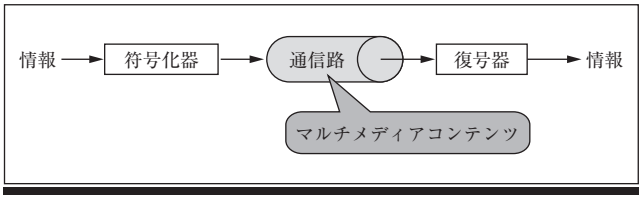


図1　通信システムでのモデル化

† 岡山大学 大学院自然科学研究科
"Security Technologies on Image Information (9); Digital Watermark" by Minoru Kuribayashi (Graduate School of Natural Science and Technology, Okayama University, Okayama)

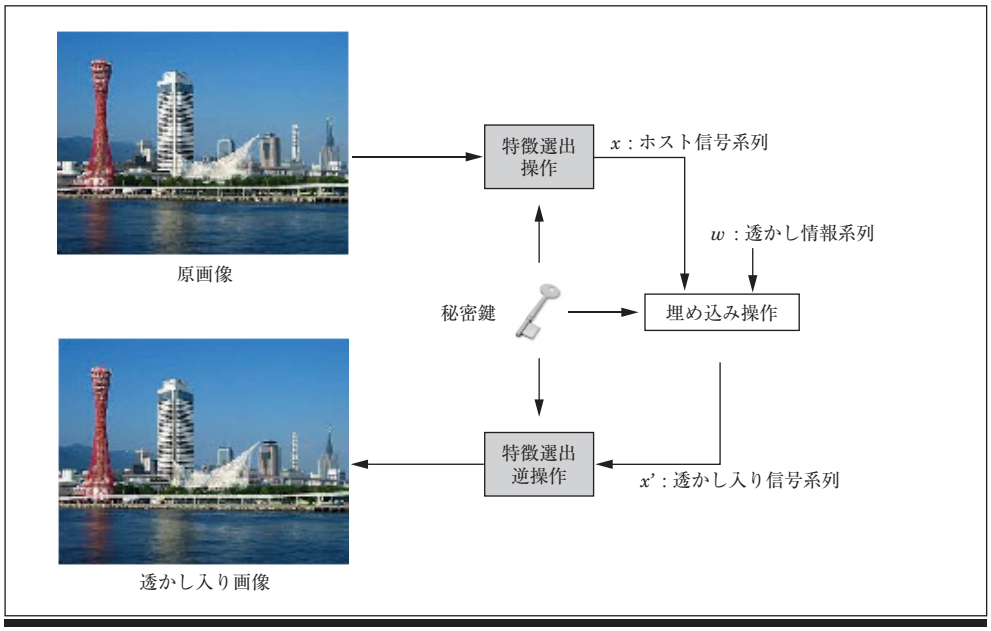


図2　コンテンツとホスト信号

これら通信路の雑音の影響を抑えるための処理が必要であり，そのために透かし情報をどのような信号に変調するかが重要となります．

電子透かしを埋め込む際には，図2に示すように秘密の鍵情報に基づいてディジタルコンテンツよりサンプリングされた系列が一般的に扱われます．例えば，ディジタル画像であれば，複数の画素や，離散コサイン変換などによって得られる周波数成分などがこの系列となります．ロバスト電子透かしでは，各種攻撃に対して耐性を考慮してこの系列を適切に選出する必要があり，なるべく攻撃の影響を受けにくい系列であることが望まれます．以後，このサンプリングした系列を特徴ベクトルと呼ぶこととします．この特徴ベクトルの選び方によって雑音による影響も大きく変化します．特にロバスト電子透かしでは，攻撃による影響を受けにくい特徴ベクトルを選出することが重要となるわけです．一般的に，この特徴ベクトルはホスト信号と呼ばれ，透かし信号を埋め込む対象として扱われます．

電子透かし方式において，埋め込む透かし情報の情報量の扱いには注意が必要です．例えば，ロバスト性を考慮して透かし情報を誤り訂正符号で符号化することを考えましょう．この場合，符号長は埋め込むビット系列の長さとなりますが，実際の情報量は元の符号化する前の透かし情報を表現するためのビット数であります．透かし情報から実際に埋め込む透かし信号においても同様な議論が言えます．

ロゴマークを埋め込むタイプの電子透かし方式ではさらに注意が必要です．白黒二値の画像で表現されるロゴマークをコンテンツに埋め込む場合，そのロゴマークの画素数が，例えば1024画素だとします．この場合，透かし情報の情報量をどのように考えれば良いでしょうか．ロゴマークを表現するには1024ビット必要ですが，実際には透かし情報はそれほど多くの情報量を有しません．なぜならば，わずか1画素でも異なる画像が検出された場合には，異なるロゴマークであると判断しなければなりませんが，一般的には検出されたロゴマークにわずかな違いしか生じていないのであれば，ロバスト性を考慮してむしろ同一視する方針であるためです．つまり，実際に埋め込むロゴマークは1024ビットだとしても，実際の透かし情報ははるかに少ないビット数であることが理解できます．もし，識別するための候補となるロゴマークが16パターンであれば，透かし情報は4ビットと考えるべきです．

上述のように透かし情報と透かし信号の違いをはっきりと理解した上で，電子透かし方式の優劣を評価する必要があります．時々この点を誤って認識されている論文がありますが，情報理論的に正しく透かし情報の情報量を定量的に示すことに注意して頂きたいと思います．

電子透かしでは，埋め込む透かし情報の種類によっていくつかのアプリケーションが提案されています．最も良く知られているものは，コンテンツの著作権が誰に帰属するかを示す著作権情報を埋め込むものです．もし，コンテンツを購入したユーザを特定することができる情報を埋め込んだ場合，不正コピーから不正者を追跡できる電子指紋技術として応用することも可能です．他には，ディジタル署名を透かし情報として埋め込むことで，改ざん検知機能を考慮した応用システムなどがあります．

3．可逆な電子透かし

マルチメディアコンテンツは，一般的に冗長成分を多く含んでいるため，情報源符号化によって圧縮した後に保存

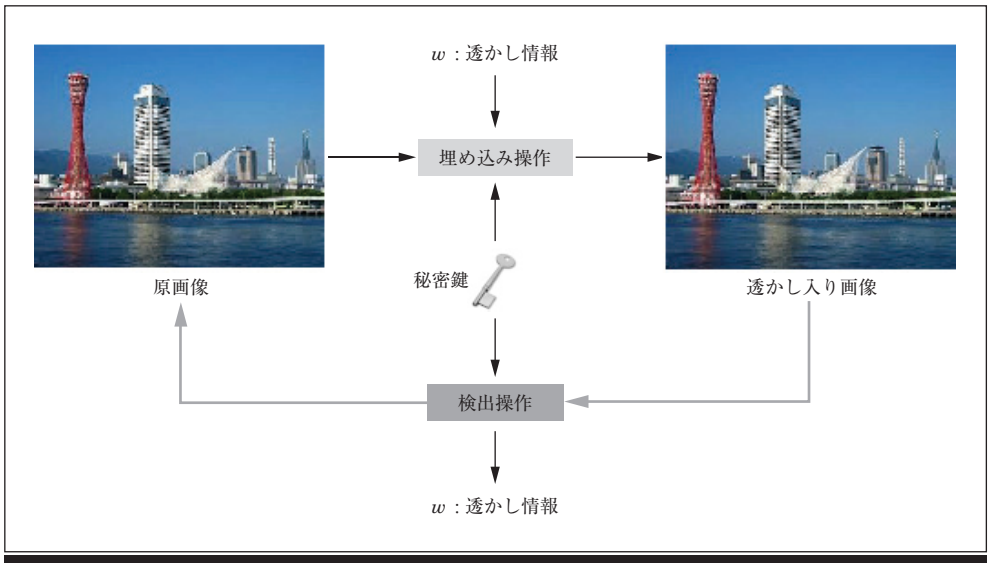


図3　可逆電子透かしの処理

されます．圧縮アルゴリズムの中には，元の情報を完全に復元できる可逆圧縮と多少の歪みが生じる非可逆圧縮があります．電子透かしにおいても，通常は非可逆な処理によって透かし信号をコンテンツに埋め込みますが，可逆の埋め込み方法も存在します．透かし信号はコンテンツより選出された特徴ベクトルに埋め込まれますが，可逆電子透かしでは透かし信号を検出する際に，元の特徴ベクトルを完全に復元できます．つまり，透かし情報の埋め込まれたコンテンツは歪みが生じていますが，検出の際に透かし情報だけでなく，元のコンテンツを復元できる方式です．以後，ディジタル画像に注目して議論を進めます．図3に可逆電子透かしの埋め込み・検出処理の概略を示します．

画像圧縮アルゴリズムでは画像の持つ冗長成分を解析し，うまく符号化することによって情報量の削減を図っています．可逆電子透かしでは，冗長性を削減する過程および情報を埋め込む過程を可逆に設定することによって透かし入り画像の可逆性を実現します．つまり，透かし入り画像は原画像からわずかに劣化していますが，透かし情報を検出する過程において透かし情報だけでなく，原画像を完全に復元することが可能となるわけです．

埋め込み容量を増やすために，冗長性を多く削減して自由空間を広く取ることは埋め込み後の画質を大きく落とすことにつながります．埋め込み容量を増やしながら，画質を綺麗に保つことは矛盾した要求です．それゆえ，埋め込み容量対画質劣化特性が最も重視されています．つまり，同じ埋め込み容量において画質劣化のより低い方式が優れた方式となります．

文献1）では，周辺画素と画像の上位ビットプレーンを効果的に利用することで下位ビットプレーンを圧縮し，自由空間を作り出し情報を埋め込む方式が提案されています．文献2）では，画素値のヒストグラムに可逆な処理を施して透かし情報を埋め込む方式が提案されています．一方，文献3）では，隣接する2個の画素間の差分値を拡大することにより自由空間を作り出し，可逆の埋め込みを行う方式を提案しています．この手法は差分拡大法と呼ばれ，上記二つの手法に比べて，大容量の埋め込みができる点で注目されています．その後，近隣にある複数の画素をまとめて処理をする一般形[4]に拡張され，さらに可逆圧縮で用いられる予測器を用いて予測誤差を利用する方式[5]が提案されています．

差分拡大法では，差分値を2倍することでうまく透かし情報ビットを埋め込む空間（すなわち最下位ビット）を作り出していますが，もし差分値が大きい場合には逆変換後の画素値が大きく変更される恐れがあります．場合によっては，画素値の値域である0～255の値を超えてしまう可能性もあります．これらはオーバフローやアンダーフローと呼ばれ，画質を著しく損なうだけでなく可逆性も失われてしまいます．それゆえ，埋め込みによってそのような状況に陥らないために，埋め込みに用いたベクトルとそうでないものを区別するためのロケーションマップと呼ばれる付加情報が必要となってきます．本稿では，ページ数の制限の関係上，ロケーションマップの具体的な構成方法や扱い方に関しては言及しませんが，このロケーションマップを圧縮する方法や不要となるように埋め込み操作に制限を設けるなどの研究がなされています．興味がある読者は，関連する文献を参照されることをお勧めします．

4．ロバストな電子透かし

ロバスト性を考慮した方式として，主に2種類のアプローチがあります．一つは攻撃に対して影響を受けにくい特徴ベクトルをコンテンツより選出するアプローチであり，もう一つは透かし情報を特徴ベクトルに埋め込む際に

冗長を加えて変調するアプローチです．これらのアプローチは混合して認識される場合もありますが，正しく区別しておけば電子透かし方式の利点・欠点を把握しやすくなります．ここでは，後者のアプローチとして代表的なスペクトル拡散法と量子化法を紹介します．

4.1　スペクトル拡散法

スペクトル拡散型の電子透かし方式は，コンテンツを通信路とみなして，透かし信号を広帯域に拡散させて埋め込む方式[6]です．例えば，1ビットの透かし情報を拡散系列で変調し，振幅をうまく調整して特徴ベクトルに加える操作が考えられます．この例は，加算によって透かし情報を埋め込むことから，加法性の埋め込みと呼ばれています．加法性の埋め込みの場合，変調された透かし信号は特徴ベクトルと完全に独立して生成されるため，コンテンツによっては透かし信号の埋め込みにより生じる劣化が知覚されやすくなる問題が指摘されています．別の観点から考えますと，劣化を抑えるためにはあまり強い信号エネルギーを埋め込むことは避けなければなりません．

特徴ベクトルに応じて透かし信号をさらに変調することができれば，強い信号エネルギーを埋め込んだとしても，その劣化は知覚されにくくなります．特徴ベクトルの各要素の大きさに応じて，透かし信号の振幅を適切に調整して埋め込みを行えば良いわけです．画像や映像などのコンテンツにおいては，人間の視覚特性を考慮した振幅の調整方法が提案されており，音響や音声などのコンテンツであれば，人間の聴覚特性を考慮した方法が提案されています．

埋め込んだ透かし信号を検出するためには，変調に用いた拡散系列との相関値を調べなければなりません．1ビットの透かし情報ならば，相関値の符号の正負により判定します．対象となるコンテンツより埋め込み時に選出した特徴ベクトルを抽出し，その特徴ベクトルより透かし情報を検出することになります．

電子透かし方式が非ブラインド型である場合は，抽出された特徴ベクトルから元の特徴ベクトルの成分を除去すれば，埋め込んだ透かし信号系列に攻撃等によって生じた雑音系列が加わった系列が得られます．この場合，雑音の影響が少なければ元の透かし情報を正しく検出できます．一方，ブラインド型の場合は，元の特徴ベクトルの成分が干渉成分として相関値に影響を与えてしまいます．ゆえに，埋め込む透かし信号の強度が低い場合は，攻撃を受けていなくても透かし情報を正しく検出できないこともあります．

このブラインド型スペクトル拡散法における問題点を解決する手法として補正処理[7]が提案されています．基本的な考え方は以下の通りです．元の特徴ベクトルに起因する干渉成分は，特徴ベクトルと拡散系列との相関値であり，埋め込み時に求めることができます．したがって，埋め込み処理を行う際に干渉成分を積極的に抑制すれば良いわけです．ただし，この補正処理によって生じるコンテンツの劣化の程度と検出性能とのトレードオフを考慮する必要があることは留意しなければなりません．

4.2　量子化法

前述通りスペクトル拡散法では，ブラインド型の検出器を使う場合に，コンテンツに起因する干渉成分の扱いに注意が必要であり，補正操作を行うことでその検出性能を高めています．しかしながら，その補正操作により生じるコンテンツの歪みは，透かし情報のビット数が増えれば増えるほど無視できなくなります．電子透かしの埋め込みにおいて，透かし信号の容量と攻撃耐性，コンテンツの品質は互いにトレードオフの関係があり，これらをうまく調整したバランスの良い方式が望ましいと言えます．その中でも，量子化法（QIM: Quantization Index Modulation）[8]と呼ばれる方法は，攻撃耐性対品質の性能が優れていることが証明されています．

量子化法では，特徴ベクトルの各要素に対してあるステップサイズで量子化を行います．通常は，量子化する場合に最も近い量子化点に丸め込まれますが，透かし情報ビットに応じて最も近い偶数もしくは奇数値となる量子化点に丸め込む方法が量子化法です．とても単純ですが，透かし情報ビットの検出時において元の特徴ベクトルがなくても，原画像に起因する干渉成分がまったく発生しないことが長所であり，スペクトル拡散法に比べて優位な点です．

コンテンツの周波数成分を特徴ベクトルとして扱う場合，量子化法を直接用いると埋め込み後の周波数成分の値が特定の量子化ステップの整数倍となります．この場合，特徴ベクトルが秘密鍵によって周波数成分よりランダムに選出されたとしても，攻撃者にその位置を特定される恐れがあります．また，周波数成分全体の振幅を変更させる攻撃に対しては脆弱です．これらの問題を解決する手法として，ディザ変調（Dither Modulation）を利用する方法も提案されています．量子化誤差に起因する劣化を抑えたディザ変調方式としては，DC-QIM（Distortion Compensated QIM）があり，さらに攻撃に対する耐性を考慮して，RDM（Rational Dither Modulation）や STDM（Spread-Transform Dither Modulation）などが提案されています．

5．電子透かしの評価

情報ハイディング技術では，埋め込み品質，攻撃耐性，埋め込み容量の評価があります．基本的に，これら三つの指標は互いにトレードオフの関係がありますので，バランスを考慮して評価しなければなりません．ここで，品質評価は埋め込まれるコンテンツ毎に基準が異なるため，静止画像や動画像などに対する画像処理技術や，音声や音響などに対する音響処理技術などの技術分野を含む必要があります．埋め込み容量評価に対しては，2章で述べた通り正しく情報量を測ることが必要です．

ロバスト電子透かし方式の研究において注目される評価

図４　IHC評価基準のバージョン４の画像部門において最も性能の高い方式[11]で作成された画像

指標は攻撃耐性ですが，上述の通り埋め込み品質と埋め込み容量との関係が正しく示されていなければ正確な評価をすることは困難となります．これまでに各種多様な方式が提案されてきましたが，それぞれ個々の指標の下で攻撃パラメータを設定して評価しており，論文中に示された数値だけでは客観的に評価することは困難な状況です．ベンチマークツールとして，StirMark[9]がありますが，公正な評価のためには埋め込み容量と画質も考慮しなければなりません．さらに6章で言及する安全性に対する理論的な枠組みがないために，標準化やアルゴリズム公開は困難と考えられています．

上述の背景を鑑みて，情報ハイディング技術に関する評価基準の確立を目指して，IHC（Information Hiding and its Criteria for evaluation）委員会[10]が2011年に設立されています．このIHC委員会では，統一化された評価基準を策定し，IHC評価基準をクリアする優れた方式をコンテストという形式で広く募集しています．2012年には，第11回情報科学技術フォーラム（FIT 2012）のイベント企画にて第1回電子透かしコンテストの結果発表と表彰が行われました．翌2013年にも，第12回情報科学技術フォーラム（FIT 2013）のイベント企画にて第2回電子透かしコンテストが報告されました．2014年には国際化され，国際会議IWIHC 2014（1st International Workshop on Information Hiding and its Criteria for evaluation）のWatermark Competitionのセッションにて，第3回電子透かしコンテストにて認定された方式が発表されました．2015年には，国際会議IWDW 2015（14th International Workshop on Information Forensics and Watermarking）のSpecial Sessionにて，第4回電子透かしコンテストが企画されています．

IHC評価基準のバージョン4の画像部門では，4608×3456画素のカラー画像6枚を使用し，200ビットの透かし情報を埋め込み，次のような条件において耐性評価を科しています．

(1) 透かし入り画像をJPEG圧縮で1/15以下のファイルサイズに圧縮
(2) 微小な拡大・縮小，回転，もしくはこれらの複合処理を実施
(3) (2) の逆処理を実施
(4) 2回目のJPEG圧縮で1/25以下まで圧縮
(5) 特定の位置（10箇所）よりHDTVサイズ（1920×1080画素）で切り取り
(6) 各切り取り画像において，200ビットの透かし情報を特定の誤り確率以下で検出

上述の条件を満足する方式において，最も性能の高い方式[11]で作成された画像の一例を図4に示します．

同じ評価基準の下で，最も優れた方式を評価するIHC委員会の試みは，電子透かし技術に興味を持つ研究者を刺激することも期待されます．今後の電子透かし技術の発展において，そのIHC評価基準だけでなくIHC委員会によって認定された方式が重要な役割を担っていくものと考えられます．

6．電子透かしのセキュリティ

電子透かし技術において安全性を議論する場合，一般的には信号処理によって透かし情報の入ったコンテンツを歪ませる攻撃が考えられています．例えば，非可逆圧縮，各種フィルタ処理，一部の切り抜き，拡大縮小回転等のコンテンツ全体に対して処理されるものが想定されています．これらの攻撃に対する耐性を考慮してロバスト電子透かし方式が研究され，多くの優れた方式が学術的に発表されています．

電子透かし技術において，そのアルゴリズムを公開した場合には安全性を評価する観点が異なります．透かし情報は，何ビットなのか，どのような特徴ベクトルに埋め込まれているのか，どのような埋め込み処理がなされているのか，どのような検出を行うのかなどの知識を攻撃者が得た場合，上述のような信号処理による攻撃は非効率的であると考えられます．攻撃者としては，透かし情報の入ったコンテンツをなるべく劣化させずに入っている透かし情報を検出できなくすれば良いため，コンテンツ全体を歪めるような信号処理を行うよりも，特定の領域に対象を絞って攻撃する方が効果的だと言えます．ゆえに電子透かしの安全性を語る上で，ロバスト性とセキュリティは異なることを理解しておく必要があります．セキュリティシステムの安全性を評価する場合，システムに関する知識に基づいて弱い箇所への攻撃が考慮されます．システムを完全にブラックボックス化するのであれば，直接攻撃だけで良いかもしれませんが，システムの仕様が公開された場合には，弱い箇所を徹底的に調査して攻撃耐性を調べなければなりません．電子透かし技術においては，図5に示すようにロバスト性評価とセキュリティ評価が異なることを理解して頂ければ良いでしょう．

以上の観点から，電子透かし方式の評価において，ケルクホフスの原理[12]に基づいて安全性を議論すべきとの意見が10年以上前から挙がっています[13]．ケルクホフスの原理

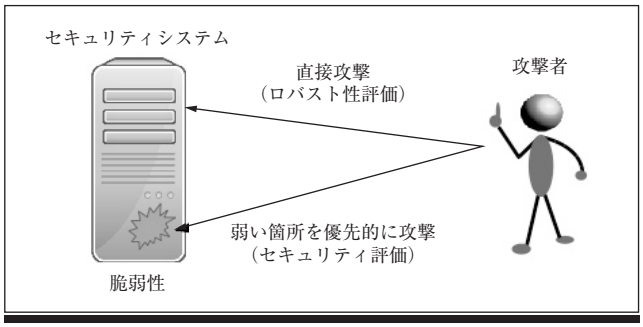


図5　セキュリティシステムの安全性の評価

では，秘密鍵を除いてシステムのすべての情報が公開されたとしても，システムの安全性が守られる必要があることを述べています．主には暗号システムを指していますが，電子透かしのシステムでも同様な議論がなされています．つまり，秘密のパラメータ（秘密鍵）を除いて，埋め込みアルゴリズムおよび検出アルゴリズムがすべて公開されたとしても，攻撃者は透かし入りコンテンツから透かし情報を除去・改変することは困難であることが求められます．

電子透かし方式の安全性評価において，KMA（Known Message Attack）フレームワークは透かし入りコンテンツと透かし信号が与えられた条件において攻撃するモデルであり，WOA（Watermarked Only Attack）フレームワークは透かし入りコンテンツのみから攻撃するモデルです．一般的には透かし信号は未知である場合が多いため，WOAフレームワークについての議論が主になされています[14) 15)]．

WOAフレームワークにおいて，攻撃者は電子透かし方式のアルゴリズムを知っていますので，コンテンツ全体への攻撃ではなく，対象を絞って透かし入りコンテンツに処理を加えることが考えられます．例として，画像の特徴ベクトルが秘密鍵に基づいて周波数成分より選出されている場合を考えます．電子透かし方式の中には，画像をブロック分割して周波数成分を求めるものや，画像全体を処理して周波数成分を求めるものがありますが，これらの情報は既知となります．また，JPEG圧縮などの非可逆圧縮では主に高周波成分が除去されやすいため，透かし信号を低・中周波成分に絞って埋め込む場合にその情報も既知となります．これらの情報から，特徴ベクトルとして選出される成分までは限定されることが想定されます．賢い攻撃者であれば，透かし情報を埋め込む候補となる画像の成分のみを対象に効果的な攻撃を加えますので，この条件においてもロバスト性を担保できるかを本来は議論すべきです．

電子透かしシステムでは，暗号システムとは求められる安全性の程度は異なりますが，少なくとも『秘密鍵を使っているから安心』のような誤った認識は改めるべきであると筆者は考えます．少しでもシステムの仕様に関する情報が漏れれば，電子透かし技術の安全性が直ちに毀損されるようでは実用的であるとは言えないのではないでしょうか．最近では，WOAフレームワークにおいて安全性を確保する方法の研究[16)]も進んでいます．今後も更なる技術的な向上が期待されています．

7．むすび

電子透かし技術の研究が始まって20年以上の年月が経過してきました．当初は著作権保護への応用に注目が集まっておりましたが，技術的な課題や問題点が指摘される中で，次第にさまざまな応用研究へ広がりつつあります．本稿では主に信号処理の観点から説明をしてきましたが，電子透かし技術に適用される他分野の技術も多種多様となっており，その裾野も広がっています．情報ハイディング技術の分野として，マルチメディアコンテンツの価値を高める新たな技術への可能性も最近では注目を集める話題となっています．複数の研究分野の方々が電子透かし技術に興味を持って頂き，今後更なる発展がなされることを期待したいと思います．

（2015年9月16日受付）

〔文　献〕

1) M.U. Celik, G. Sharma, A.M. Tekalp and E. Saber: "Lossless generalized-LSB data embedding", IEEE Trans. Image Processing, **14**, 2, pp.253-266（2005）
2) Z. Ni, Y.-Q. Shi, N. Ansari and W. Su: "Reversible data hiding", IEEE Trans. Circuits and Systems for Video Technology, **16**, 3, pp.354-361（2006）
3) J. Tian: "Reversible data embedding using a difference expansion", IEEE Trans. Circuits Syst. Video Technol., **13**, 9, pp.890-896（2003）
4) M. Alattar: "Reversible watermark using the difference expansion of a generalized integer transform", IEEE Trans. Image Processing, **13**, 8, pp.1147-1156（2004）
5) D.M. Thodi and J.J. Rodriguez: "Expansion embedding techniques for reversible watermarking", IEEE Trans. Image Processing, **16**, 3, pp.723-730（2007）
6) I.J. Cox, J. Kilian, F.T. Leighton and T. Shamson: "Secure spread spectrum watermarking for multimedia", IEEE Trans. Image Processing, **6**, 12, pp.1673-1687（1997）
7) H.S. Malvar and D.A.F. Florêncio: "Improved spread spectrum: A new modulation technique for robust watermarking", IEEE Trans. Signal Processing, **51**, 4, pp.898-905（2003）
8) A. Chen and G.W. Wornell: "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding", IEEE Trans. Inform. Theory, **47**, 4, pp.1423-1443（2001）
9) Stirmark Benchmark, http://www.petitcolas.net/watermarking/stirmark/
10) 情報ハイディングおよびその評価基準（IHC）委員会, http://www.ieice.org/emm/ihc/
11) H. Ogawa, M. Kuribayashi, M. Iwata and K. Kise: "DCT-OFDM based watermarking scheme robust against clipping, rotation and scaling attacks", Proc. IWDW2015, LNCS, Springer（2015）（to appear）
12) A. Kerckhoffs: "La cryptographie militaire", Journal des sciences militaires, 9, pp.5-83（1883）
13) M. Barni, F. Bartolini and T. Furon: "A general framework for robust watermarking security", Signal Processing, **83**, 10, pp.2069-2084（2003）
14) F. Cayre and P. Bas: "Kerckhoffs-based embedding security classes for WOA data hiding", IEEE Trans. Information Forensics and Security, **3**, 1, pp.1-15（2008）
15) J. Cao and J. Huang: "Controllable secure watermarking technique for tradeoff between robustness and security", IEEE Trans. Information Forensics and Security, **7**, 2, pp.821-826（2012）
16) B. Mathon, F. Cayre, P. Bas and B. Macq: "Optimal transport for secure spread-spectrum watermarking of still images", IEEE Trans. Image Processing, **23**, 4, pp.1694-1705（2014）

栗林　稔（くりばやし　みのる）　2002年，神戸大学大学院自然科学研究科博士課程中退．同年，神戸大学工学部助手就任．神戸大学大学院助教を経て，2015年より，岡山大学大学院准教授．情報ハイディングと情報セキュリティ，符号理論等の研究に従事．2015年，IEEE関西支部Young Professionals Award受賞．IEEE，IEICEシニア会員．博士（工学）．

講 座

映像情報メディア関連のセキュリティ〔第10回〕

バイオメトリクス

青木隆浩†

1．まえがき

本稿では，映像情報メディアをセキュリティのための根幹に据えた技術として，バイオメトリクスを紹介します．システムを攻撃者から守るためには，あらゆる面からの攻撃に備える必要があります．その中の重要な要素として，確実な本人認証が挙げられます．いくら安全性の高いシステムを構築しても，攻撃者が正当な利用者になりすましてしまえば，簡単に侵入を許してしまうことになります．身近な例で言えば，最高のセキュリティ設備を導入していても，入り口を守っているパスワードをポストイットで貼り付けていては安全とは言えません（図1）．

このようなケースに対し，バイオメトリクスは威力を発揮します．

本稿の構成は以下の通りです．まず，第2章でバイオメトリクスの概要について説明します．第3章ではバイオメトリクスで用いられる代表的な認証特徴（モダリティ）について説明します．第4章，第5章ではバイオメトリクスの精度評価および国際標準化について説明します．第6章では生体情報保護技術について，第7章ではバイオメトリクスの実社会運用について簡単に紹介します．

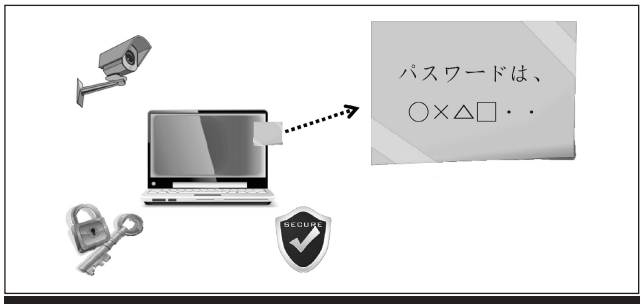


図1　システムの安全性は…？

† 株式会社富士通研究所 知識情報処理研究所 次世代認証・認可プロジェクト
"Security Technologies on Image Information (10); Biometrics" by Takahiro Aoki (Next Generation Authentication and Authorization Project, Knowledge Information Processing Laboratories, Fujitsu Laboratories Ltd., Kawasaki)

2．バイオメトリクスとは

本章では，バイオメトリクスの概要について説明します．まず，バイオメトリクスとは，人体固有の身体的特徴あるいは行動的特徴を用いて個々を識別する技術で，一般的に自動的に認識処理を行う技術を言います[1]．代表的なバイオメトリクスとしては，指紋認証技術や顔認証技術などが挙げられます．

バイオメトリクスは上記のように個人を識別する技術ですが，同様のことはパスワードやIDカードを使っても実現することができます．バイオメトリクスが，これらと異なる点として，漏えいや他人へ譲渡が難しい点が挙げられます．パスワードやIDカードの場合，認証に必要な情報や物が簡単に他人の手にわたってしまう可能性があります．もう少し具体的な例を挙げると，最近は，複数システムで異なったパスワードを覚える必要が出てきています．こちらのシステムはパスワード12文字以上，あちらでは10文字と記号のパスワードを覚える必要がある，といった具合です．すると先ほどの例のように，パスワードをポストイットでメモするようなことが起こってしまいます．また，出退勤をIDカードで管理している場合，他人にカードを渡して通してもらうことも簡単にできてしまいます．

一方，バイオメトリクスは個人に属する情報を使って認証するため，盗難や漏洩，譲渡といった脅威に対する耐性は非常に高いと言えます．一方で，バイオメトリクスでは，特徴情報が万一漏洩してしまった場合，パスワードと違って変更することが難しい点が懸念として指摘されています．この点に関しては，いろいろな方式が提案されています（6章参照）．

以下，バイオメトリクスの歴史を簡単に見てみます．バイオメトリクスという言葉が生まれる以前から，身体的特徴をもとに個人を認証することは行われてきました．例えば，フランスでは1882年にBertillon Systemというものが存在しました[2]．これは，身長や座高などの情報から個人を絞込むシステムで，バイオメトリクスの原型とも言えるものです．また，日本でも古くから拇印を本人確認に使う習慣がありました．科学的な指紋研究としては，1685年に

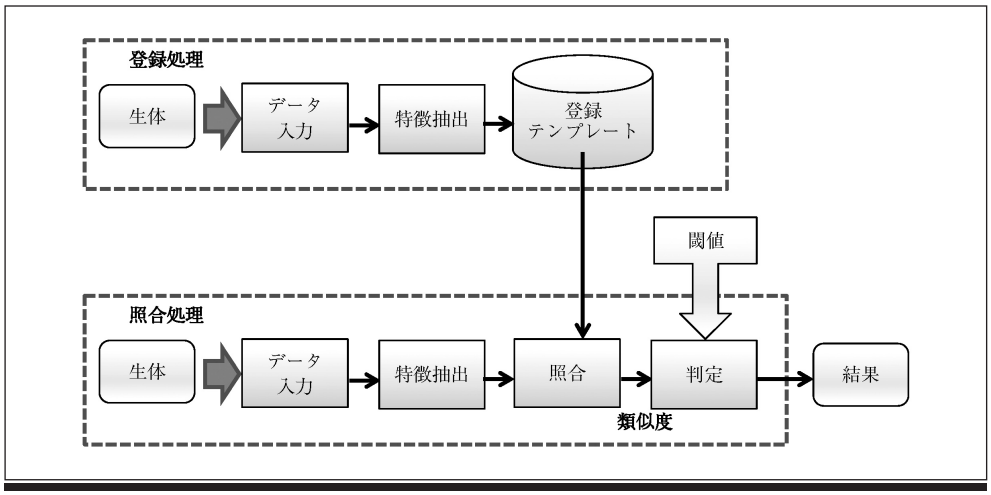


図2　本人認証動作の流れ

イギリスで皮膚の模様に関する論文があり，その後，年金支給などに利用されたと言われています[3]．1960年代に入るとコンピュータの発展に伴い，自動で認識するバイオメトリクスの研究が始まりました．指紋や音声，顔認識などの研究は1960年代には始まっており，50年以上の歴史があります[4]．

以下では，バイオメトリクスを使った本人認証動作の流れを見てみます（図2）．

まず，事前に本人の生体特徴データを「登録テンプレート」として登録します．ここで，生体特徴データとは，指紋や顔などから認証に必要となる特徴データのみを取出したものです．バイオメトリクスでは，登録テンプレートを認証の基礎として用いるため，登録テンプレートは非常に重要な情報になります．また，セキュリティの観点から，登録テンプレートは安全に保管することが必要です．

照合処理の際には，認証処理を行う利用者から特徴データを取得して登録テンプレートと比較します．具体的には，登録テンプレートと取得した特徴データがどの程度似ているかを表す“類似度”を算出します．類似度が所定の閾値を上回っている場合は“本人”と判断し，下回っている場合は“他人”と判断します．

バイオメトリクスを使った認証方式の大きな区分として，1：1認証と1：N認証があります．1：1認証は，認証の始めに自分のIDを入力してから照合処理を行う方式です．IDで個人を一意に特定した上で，バイオメトリクスは本当に本人かどうかの確認として用います．一方，ID情報を入力せず，生体情報から直接個人を一意に識別する1：N認証方式もあります．1：N認証では，生体情報のみを入力し，登録済の全テンプレートと比較を行います．一般的には，すべての登録テンプレートと比較した中で，最も高い類似度を示した利用者として識別します．入退室管理などでは，ID入力が不要な1：N認証の方が利便性は高くなります．一方，1：N認証では，データベースに登録されているすべての登録テンプレートと照合を行う必要があるため，処理負担が非常に重くなります．また，登録されている人数が増えるにしたがって，誤った識別を行う確率が統計的に高くなっていきます．そのため，1：N認証は1：1認証よりも技術的，システム的に難易度が高いといえます．

3．バイオメトリクスの種類

バイオメトリクスで認証に用いる特徴データにはさまざまな種類が存在します．バイオメトリクスで認証に用いる特徴の大分類を“モダリティ”と言います[5]．先に述べたように，バイオメトリクスは身体的または行動的特徴を用いて個人を識別します．身体的特徴として用いられる代表的なモダリティには以下のようなものがあります．

◇指紋認証

指先の紋様を使って認証するもので，代表的なバイオメトリクスの一つです．認証精度が高く，装置を小型/安価に製造できるため，近年ではスマートフォンなどにも搭載されています．一方，認証特徴が皮膚の表面に存在しているため，肌荒れなどの影響を受け，誤認証することがあります．

◇顔認証

人の顔を画像処理技術によって認識する方式です．認証精度はあまり高いと言えませんが，利用者が特定の認証動作をする必要がなく，自然な形で認証できるため，利便性が高い方式です．例えば，利用者が歩いている間に認証を行う，ウォークスルー認証などの研究が行われています．最近では，Deep Learningと呼ばれる機械学習の応用によって認証精度が高まり，注目を集めています[6]．

◇虹彩（アイリス）認証

虹彩（アイリス）とは，瞳の周辺にあり，瞳に入る光の量を調節する領域のことです．虹彩認証はこの領域にある模様によって認証を行う方式です．虹彩認証も古くから研究されているバイオメトリクスの一つです[7]．虹彩認証と良く間違えられるものに“網膜認証”があります．網膜認証は，目の奥にある血管パターンを用いて認証するもので，虹彩認証とは別の特徴を用います．虹彩認証は，正しく認証特

徴が取得されれば高い精度が得られる一方，メガネやカラーコンタクトなどの影響を受け，精度が低くなることがあります．

◇静脈認証

比較的最近登場したバイオメトリクスです．近赤外線などを用いて体内に存在する静脈のパターンを読取り，そのパターンを比較して認証します．認証特徴が体内に存在するため，特徴漏洩の危険性が低く，認証精度が高い点が特徴です．指や手のひら，手の甲などさまざまな部位の静脈パターンを用いる方式が研究されています[8]．

また，行動特徴のモダリティとしては以下のようなものがあります．

◇音声認証

人の話す声によって認証する方式です．決まった言葉を用いて認証するテキスト依存型や，自由な会話から認証するテキスト独立型，システムが認証に用いる言葉を指定するテキスト指定型などがあります．

◇サイン認証

人が書くサインを使って認証するものです．従来の紙ベースのサインと異なり，バイオメトリクスのサイン認証では，ペンタブレットなどを使ってサインを書くスピードや筆圧なども利用します．また，スマートフォンやタブレットPCのタッチパネルを用いたサイン認証技術も研究されています．

◇歩容認証

人が歩く際の歩き方を特徴として認証します．個人認証以外にも人の流れの分析などの応用があります．

上記以外にもDNA認証，耳介（じかい：耳の形）認証，キー入力の時間的な特徴を用いるキーストローク認証，手のジェスチャによるジェスチャ認証など数多くのバイオメトリクスが提案されています[8]．

また，単一のモダリティではなく，複数のモダリティを用いた“マルチモーダルバイオメトリクス”も提案されています．マルチモーダルは，一般に価格や装置サイズの面では不利となりますが，適切なバイオメトリクス特徴を組合せて利用することで，単一バイオメトリクスでは実現不可能な高い精度や認証の安定性を実現することができるようになります．

これだけバイオメトリクスのモダリティに種類があると，「どのバイオメトリクスが良いの？」という疑問が出てくると思います．現時点では，すべての利用目的を満足できるような万能のバイオメトリクスは存在しないため，利用目的に応じて使い分けることが望ましいと言えます．具体的には，認証精度や価格，センサのサイズ，利用者の使い勝手などをトータルに検討することになります．例えば，高い安全性が求められるシステムの場合，認証精度が高く，認証特徴が漏洩しにくい静脈認証が向いているケースがあります．一方，あまり高い認証精度は必要ではなく，手軽に認証したい場合は顔認証が向いているケースもあります．このようにバイオメトリクス導入検討の際には，認証精度を外して考えることはできません．次の章ではバイオメトリクスの精度評価について説明します．

4．認証精度評価

バイオメトリクスは，画像や音声などの情報を処理して認証を行います．そのため，100%正しい認証を行うことは難しく，一定の割合でエラーが発生します．ここでは，バイオメトリクスにおける精度評価について説明します．なお，バイオメトリクスの認証精度評価方法に関しては，ISO/IEC 19795シリーズとして標準化されています．

まず，バイオメトリクスでは上記の通り，入力された特徴データと登録テンプレート間の類似度を計算します．この時，本人同士を比較した場合と，他人同士を比較した場合の類似度の出現頻度を図示すると図3に示すような形になります．

本人データが入力された場合，相対的に高い類似度が得られる確率が高くなります．一方，他人データが入力された場合，低い類似度が出力される確率が高くなります．そのため，図3には本人の頻度分布と他人の頻度分布の二つの分布が表れています．本人と他人の頻度分布グラフが完全に分離している場合，判定閾値を適切に設定することで，精度100%のバイオメトリクスになります．しかし，一般的には本人と他人の頻度分布に重なる領域が存在します．そのため，判定閾値をどこに設定するかが重要になります．

図3の①に閾値を設けた場合を説明します．先に述べたように閾値以上の類似度の場合には，“本人”と判断されます．そのため，閾値が①に設定された場合，実線で示された本人の頻度分布のほとんどが閾値よりも大きいため，大部分の本人は正しく“本人”と判定されます．一方，点線で表される他人分布を見ると，一定割合の他人が誤って“本人”と判断されてしまうことがわかります．このように誤って他人を“本人”と判断してしまうエラーの割合を他人受入れ率（False Accept Rate=FAR）と言います．一方，

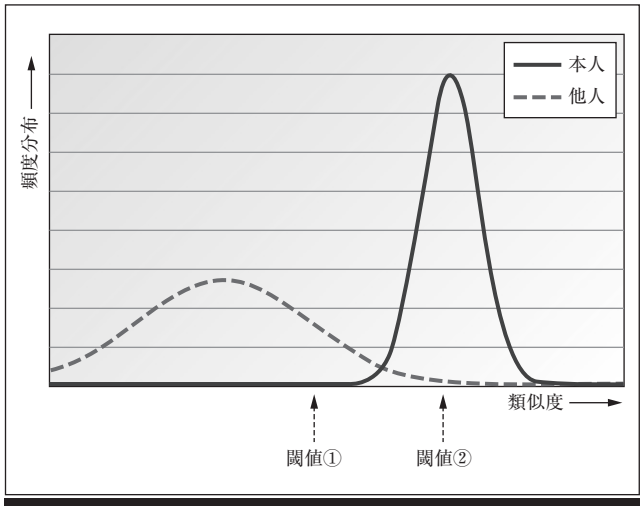


図3　本人と他人の類似度頻度分布

判定閾値を図3の②の位置に設定した場合，他人はほとんど排除できますが，一定割合の本人を誤って“他人”と判断してしまうことになります．このように，誤って本人を“他人”と判断してしまうエラーの割合を，本人拒否率（False Reject Rate=FRR）と言います．

特にFAR=FRRとなる際のエラー率をEER（Equal Error Rate）といいます．これは，図3でFARとFRRが交差している点におけるエラー率に相当します．EERは，異なる生体認証装置間で精度を比較する際の指標として用いられる場合があります．

当然のことながら，FARとFRRは小さければ小さい程望ましいと言えます．しかし，FARとFRRはトレードオフの関係にあります．判定閾値を厳しく設定すれば，他人を誤って受け入れる確率FARは下がりますが，本人を誤って拒否してしまう確率FRRが上がってしまいます．判定閾値を緩めた場合にも同様の問題が起こります．

FARとFRRのトレードオフの関係を表したのがDET（Detection Error Tradeoff）カーブと呼ばれます（図4）．DETカーブは，判定閾値をさまざまな値に設定した時の（FAR, FRR）をプロットしたもので，生体認証の精度評価で良く用いられる代表的な図です．

カーブが図の左下に位置する方が，生体認証装置として高精度であることを意味します．図4の例では，Biometrics-Aの方がBiometrics-Bよりも高精度と言えます．システム構築の際は，利用目的に応じて安全性と使い勝手を考慮して，適切な運用設定を行う必要があります．バイオメトリクスの場合，FARを小さく設定することで，他人を受け入れる確率が低下し，安全性が向上します．一方，利用者の使い勝手はFRRが小さい方が改善します．DETカーブは最適な設定を見つける際に，参考となる便利な図です．

バイオメトリクスの精度評価で留意するべき点として，被験者の選び方によって評価結果が影響を受ける可能性が挙げられます．例えば，装置によっては，その装置を初めて使う人と，その装置に慣れている人で認証精度が大きく違います．このような場合，被験者の選び方によって評価結果が変わってしまいます．そのため，単純なエラー率だけでは，実運用での精度を正しく表していない場合があります．このため，実運用のためにどのような評価軸を設けるべきかということは，バイオメトリクスの基盤技術とともに大きな課題となっています．

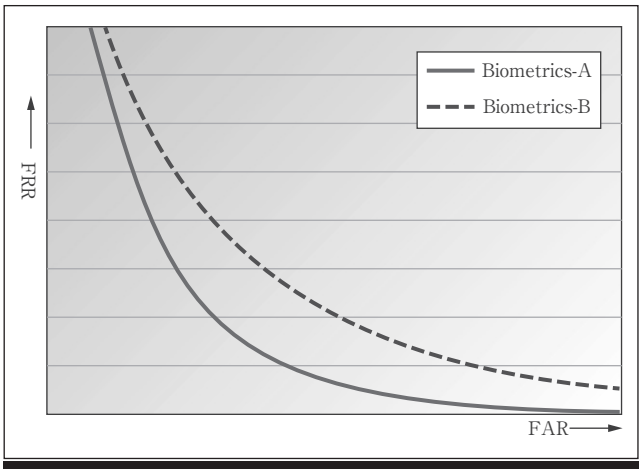


図4　DETカーブの例

5．標準化

本章ではバイオメトリクスの国際標準化について説明します．一般的なバイオメトリクス技術に関しては，ISO/IEC JTC 1/SC 37が中心となって標準化を行っています．SC37には，WG1～WG6までのワーキンググループがあり，標準化を進めています[10]．各ワーキンググループの名称と検討内容を表1に示します．

また，SC37以外にも，ICカード技術をISO/IEC JTC 1/SC 17が，セキュリティ技術をISO/IEC JTC 1/SC 27が検討しています．また，金融関係のISO/TC 68，パスポート関係のICAO（International Civil Aviation Organization，国際民間航空機関）などとも連携しながら，バイオメトリクスの標準化を進めています．

バイオメトリクスに関する標準化は，用語から社会的課題まで多岐に渡ります．ここでは，代表的な国際標準として，API仕様である“BioAPI”とデータ交換フォーマット“CBEFF（Common Biometric Exchange Formats Framework：“シーベフ”と読みます）”について紹介します．

BioAPIは，アプリケーションソフトからバイオメトリクスを利用するための標準的なAPI（Application Programming Interface）です（図5）．BioAPIにしたがって実装することで，ベンダーの枠を超え，インタオペラビリティを高めることができます．BioAPIを使用するアプリケーションプログラムは，“BioAPIフレームワーク”と呼ばれるライブラリーを介して，登録や照合，識別といったバイオメトリクス機能を利用します．これらの機能を実際に提供するのはBSP（Biometrics Service Provider）と呼ばれるプログラムです．BSPは，通常はバイオメトリクスベンダーが提供するものです．つまり，BioAPIフレーム

表1　SC37のワーキンググループ

	名　称	内　容
WG1	Harmonized Biometric Vocabulary	バイオメトリクスの専門用語
WG2	Biometric Technical Interfaces	バイオメトリクスの共通インタフェース
WG3	Biometric Data Interchange Formats	バイオメトリクスのデータ交換形式
WG4	Technical Implementation of Biometric Systems	バイオメトリクスの導入・運用仕様
WG5	Biometric Testing and Reporting	バイオメトリクス技術の試験および報告
WG6	Cross-Jurisdictional and Societal Aspects of Biometrics	バイオメトリクスの社会的課題

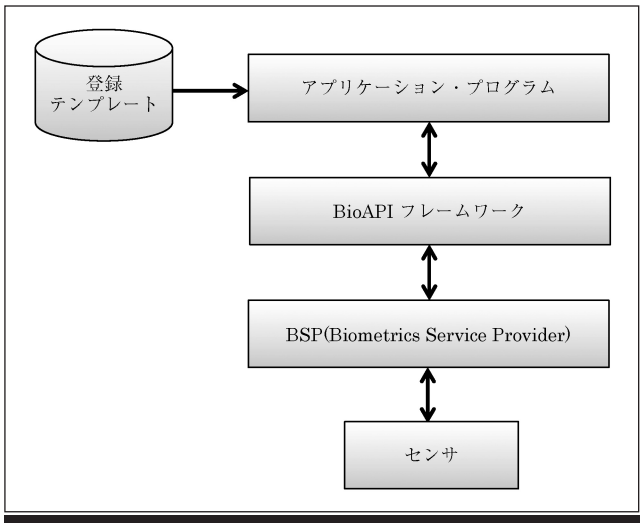


図5　BioAPIを使った生体認証

ワークは，アプリケーションソフトとベンダー提供のBSPの間を取り持つ役割を果たします．BioAPIでバイオメトリクスデータをやり取りする際は，次に述べるCBEFFを用いて行います．

CBEFFは，バイオメトリクスデータ交換を視野にした共通のデータフォーマットフレームワークです．CBEFFを用いることで，ベンダーの壁を越えてバイオメトリクスデータを相互に利用することが可能となります．CBEFF自体は，ヘッダ情報や枠組みを提供しており，具体的な個々の生体データのフォーマットは別の標準化（ISO/IEC 19794シリーズ）で定義されています．

6．生体データ保護技術

バイオメトリクスで用いる指紋や顔といった認証特徴は一般に変えることができません．この点はバイオメトリクスの利点である一方，課題として指摘されています．例えば，パスワードが漏洩してしまった場合，新しいパスワードを再登録すれば良いですが，バイオメトリクスの場合にはそうはいきません．そのため，登録テンプレートなどのデータを安全に運用することが必要となってきます．

この課題を解決するためにさまざまな技術的な取組みがなされています．特に近年のプライバシー意識の高まりとともに活発に研究が進められている分野でもあります．現時点では，安全性や実用性をすべて満たすような方式は開発されておらず，発展途上の分野ですが，代表的な方式を幾つか紹介します．

◇キャンセラブルバイオメトリクス

生体特徴データを取得後に，“変形”してから認証に用いる方式です[11]．仮に登録テンプレートが漏洩しても，変形情報を変えることで，異なった登録テンプレートを生成できます．しかし，変形情報も一緒に漏洩してしまうと，元の生体情報が容易に類推されてしまうリスクがあります．

◇Fuzzy Commitment Scheme

生体認証と暗号技術を融合した方式です[12]．生体情報をビット列に変換した情報bとランダムに生成した秘密鍵sを組合せて利用することで安全な認証を行います．この際にキーとなるのは，誤り訂正符号技術を適用することです．誤り訂正符号は，ネットワークやデバイスからデータを読取る際に発生する誤りを検出し，補正する技術です．Fuzzy Commitment Schemeでは，誤り訂正符号を生体データが持つ変動を吸収するために利用します．

Fuzzy Commitment Schemeを適用するためには生体データをビット列に変換する必要があります．画像など2次元データを1次元のビット列に変換する際には，位置ずれ等の変動があった場合でも不変である必要があり，利用できる情報量が低下するため，結果として一般的には認証精度が低下してしまいます．また，Fuzzy Commitment Schemeに対する攻撃方法や改良方式も幾つか提案されています．例えば，Fuzzy Commitment Schemeでは生体データが一様に分布していることを仮定しています．しかし，一般に生体データの分布には偏りがあるため，それを利用した攻撃が可能となります[13]．

◇Fuzzy Vault Scheme

上記のFuzzy Commitment Schemeは，利用者が正当な利用者かどうかを判断し，出力します．一方，Fuzzy Vault Schemeでは，秘密情報Sを秘匿し，正当な利用者のみがSを取出せるという方式です[14]．Fuzzy Vault SchemeもFuzzy Commitment Schemeと同様に誤り訂正符号を組合せた方式です．Fuzzy Vault Schemeでは，“チャフ”と呼ばれるダミーデータを使って生体情報の秘匿を行います．つまり，生体情報を保存する際に，本物の特徴点の中にダミーデータ（チャフ）を混ぜ込んで保存します．この処理により，保存されたデータを見ただけではどこが本物の生体情報であるか判別できないようになります．これにより，保存データを見た攻撃者であっても，容易に偽の生体情報を生成できなくなります．そして，本物の生体情報を持つ者だけが，正しい特徴点を抽出できるため，最終的に秘密情報Sを取得できるようになります．

Fuzzy Vault Schemeに対する攻撃方法や改良方式も幾つか提案されています．例えば，Fuzzy Vault Schemeでは上記のように“チャフ”を用いて生体データを秘匿します．しかし，人工的に作成したチャフは，本物の生体特徴と比べると出現する位置などが不自然になる場合があり，攻撃に利用されることがあります[15]．

7．実用事例

本章では，実際にバイオメトリクスが社会で使われている事例をいくつか紹介します．

◇スマートフォンなどの携帯端末

以前よりノートPCなどの携帯端末に指紋認証や静脈認証などの生体認証を搭載する例がありました．近年では，スマートフォンや携帯電話など，より小型の携帯端末にバイオメトリクスを搭載する例が増えてきました．これら携帯

端末にはアドレスなどの個人情報が保存されていること，盗難や紛失の可能性が高いことから搭載ニーズが高まっていることが背景としてあります．また，近年のCPUやハードウェアの高性能化に伴い，バイオメトリクスを搭載するハードルが下がってきたことも普及の一因と考えられます．スマートフォン向けとしては，小型化や価格の面で有利な指紋認証の利用が多く見られますが，虹彩認証を搭載する例もあります．また，携帯端末へのバイオメトリクス搭載では，端末のアクセス制御のみでなく，携帯端末を使った決済処理の本人確認手段としても利用されています．

◇銀行ATM

銀行ATMでの本人確認手段としてバイオメトリクスが利用されています．銀行ATMでは体内にあるため，偽造が難しい静脈認証が多く用いられています．また，ICカードと連携した方式も多く利用されています．

◇入退室管理

ビルやサーバルームの入退室管理として生体認証が使われています．入退室管理では，指紋や顔，虹彩などさまざまなモダリティが使われています．また，入退室管理では，利便性を考慮して1：N認証も多く利用されています．

◇出入国審査

空港などで行う出入国審査を迅速に行う目的で生体認証の利用が世界中で検討されています．日本でも出入国審査の効率化として指紋認証を用いた“自動化ゲート”が運用されています．また，より利便性を高める目的で，顔認証を用いた出帰国審査も日本を含めた各国で検討されています[16]．顔認証の場合，パスポートの写真をそのまま登録テンプレートとして利用可能で，登録処理が不要なことが利点として挙げられます．

8．むすび

近年，スマートフォンへの指紋搭載を始めとしてバイオメトリクスが，身近な存在になってきました．一方，まだまだ発展の余地の大きい技術でもあります．例えば，現在のバイオメトリクスでは統計的には精度が高くても，特定の利用者では認証が難しいケースがあります．これは，指紋のように，その利用者の肌荒れなどが原因で生体特徴が不安定なことや，ユーザインタフェースがわかり難いことなどが原因として挙げられます．肌が荒れていても正しく認証できるように，画像補正処理や照合アルゴリズムを改善したり，これまで使われていなかったセンサを用いる方法を考案したり，ユーザインタフェースを容易にするような改善を施すことで，バイオメトリクスは誰でも簡単に使える技術になります．バイオメトリクスは日本が世界の先頭を走っている分野でもあり[17]，今後の研究の発展に期待が持てます．実応用の面で言えば，生体認証などを使ってオンライン決済を安全に行うための“FIDO Alliance”に数多くの企業が参加して活動しており，今後の動きが注目されています．

今後も安全やセキュリティ，プライバシーの重要性はさらに高まり，バイオメトリクスはさまざまな場面や目的で利用されていきます．個人とシステムを安全・確実に結びつける手段として，バイオメトリクスは最も簡易で有効な手段です．安定した認証の実現や，テンプレートの安全性確保など，現状では解決すべき課題はあるものの，生体認証が理想的な本人確認手段の一つであることは間違いありません．職場だけでなく，生活すべてがネットワークに繋がるIoT社会におけるみなさんの安全・安心を，バイオメトリクスによって高めることができます．これらの研究は今後ますます重要であることは間違いありません．

（2015年11月30日受付）

〔文　献〕

1）バイオメトリクスセキュリティコンソーシアム（編集）：“バイオメトリックセキュリティ・ハンドブック”，オーム社
2）橋本一径：“指紋論 心霊主義から生体認証まで”，青土社
3）日本自動認識システム協会（編集）：“これでわかったバイオメトリクス”，オーム社
4）A.J. Jain: "50 Years of Biometric Research: Almost. The Solved, the Unsolved and the Unexplored", Keynote Talk Delivered at the International Conf. On Biometrics, Madrid, Spain（June 5，2013）
5）半谷精一郎，瀬戸洋一，吉田孝博，清水孝一：“バイオメトリクス教科書―原理からプログラミングまで”，コロナ社
6）Y. Taigman, M. Yang, M. Ranzato, L. Wolf. "DeepFace: Closing the Gap to Human-Level Performance in Face Verification", IEEE Conf. Computer Vision and Pattern Recognition（CVPR），p1701-1708（2014）
7）瀬戸洋一：“サイバーセキュリティにおける生体認証技術”，共立出版
8）日本自動認識システム協会（編集）：“よくわかるバイオメトリクスの基礎”，オーム社
9）半谷精一郎：“バイオメトリクス認証技術の動向とセキュリティシステムへの応用”，映情学誌，58，6，pp.750-752（June 2004）
10）瀬戸洋一：“バイオメトリックセキュリティ入門：“ソフトリサーチセンター
11）N.K. Ratha, J.H. Connell and R.M. Bolle: "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, 40, 3, pp.614-634（2001）
12）A. Juels and M. Wattenberg: "A fuzzy commitment scheme", Proc. 6th ACM Conference on Computer and Communications Security, pp.28-36（1999）
13）披田野清良，市野将嗣，大木哲史，高橋健太，小松尚久：“Fuzzy Commitment Schemeを用いたバイオメトリック暗号におけるテンプレートの安全性に関する一考察”，コンピュータセキュリティシンポジウム，pp.89-94（2011）
14）A. Juels and M. Sudan: "A fuzzy vault schem", Proc. IEEE International Symposium on Information Theory（ISIT 2002），p.408（2002）
15）小田雅洋，渡邊幸聖，山本匠，高橋健太，尾形わかは，菊池浩明，西垣正勝：“Fuzzy Vault Schemeにおけるチャフ空間拡大に関する検討”，暗号と情報セキュリティシンポジウムSCIS（2011）
16）法務省報道発表資料：“「日本人出帰国審査における顔認証技術に係る実証実験結果（報告）」について”，http://www.moj.go.jp/nyuukokukanri/kouhou/nyuukokukanri04_00044.html
17）技術経営・イノベーション賞文部科学大臣賞“世界No.1精度の顔認証技術で安心・安全な社会の実現に貢献”，http://www.jates.or.jp/management_study/management_of_technology_meeting/gikei_innovation.html

青木（あおき）　隆浩（たかひろ）　1993年，京都大学理学部学士課程卒業．1995年，京都大学理学部修士課程卒業．同年，（株）富士通研究所に入社．以来，画像処理アルゴリズムや生体認証の研究に従事．

モバイルセキュリティ

竹森敬祐†

1．まえがき

モバイル端末には，通信機能を搭載したパソコン（以後，PC），1990年頃から普及し始めた通話重視の携帯電話（以後，フィーチャーフォン），2010年頃から普及し始めた汎用OSが搭載されたスマートフォンなどさまざまなデバイスがあります．PCについては，ウイルス感染や情報漏洩などのサイバー攻撃の脅威に晒されながら，セキュリティ対策ソフトやファイアウォール等の導入が進んできました．フィーチャーフォンは，端末，OS，アプリケーション（以後，アプリ）を通信事業者が主体となって設計，開発，管理を行う垂直統合モデルで提供されてきており，攻撃の侵入口となるインタフェースがクローズドなものでした．迷惑メールや詐欺行為を除くと，ハッキングの対象になり難い構成となっています．スマートフォンは，利用者が自由にアプリをインストールして機能を向上させることができるオープンな端末です．利便性の高いアプリを実行させるためのアプリインタフェース（以後，API）も揃っていること，利用者に紐付くさまざまな情報が管理されていることから，独特の脅威が潜在しています．本稿では，すでにハッキングの脅威と対策が広く知られているPCと，ほとんど脅威のないフィーチャーフォンを除いた，急速に利活用が進んでいるスマートフォンに注目して，潜在するリスクとセキュリティ対策を解説します．

2．スマートフォンを取り巻くリスク

スマートフォン向けOSには，誰もが安心して利用できるよう，利用者に通知・承諾を経ながらアプリに機能や情報へのアクセス権限を付与する機構や，ウイルスへの自動感染を阻止するインストール制限機構が組込まれており，2000年頃のPCよりも格段に安全性が高まっています．しかし，考慮すべきセキュリティ領域は広く，利用者の不注意やアプリ開発者の設計ミスにより，思わぬ事故に遭遇することもあります．

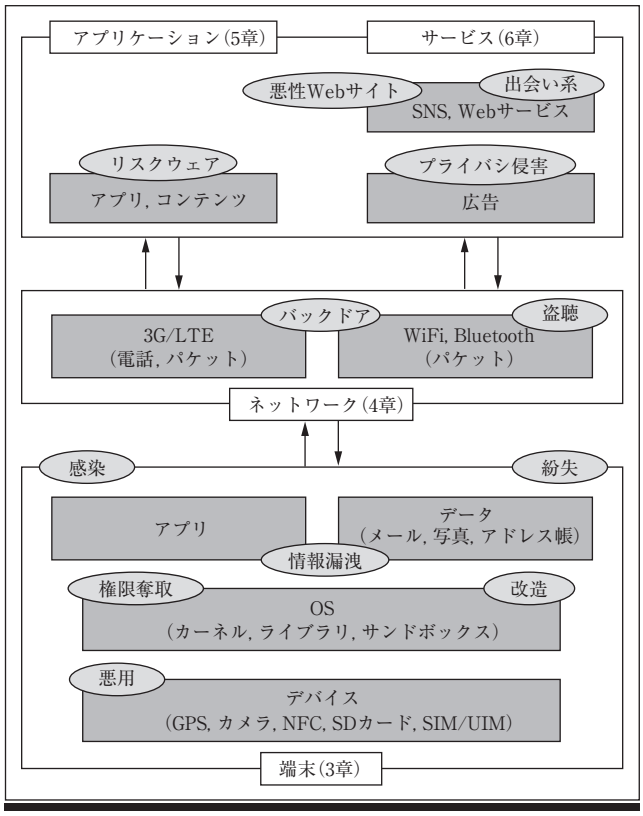


図1　スマートフォンを取り巻くリスクの一例

図1に，スマートフォンを取り巻くリスクの一例を，発生領域ごとに整理しました．端末，ネットワーク，アプリマーケット，サービス提供者の領域があり，それぞれ特有のリスクが潜在します．注意すべきポイントとして，悪意/プライバシー侵害/偽物などのリスクを伴うアプリ（以後，リスクウェア）がセキュリティ審査のないアプリマーケットを通じて出回っていることです．また，常に持ち歩くことで位置を追跡されやすいこと，メールやSocial Network Service（SNS）によるプライベートな情報の発信源となりうること，友達や業務先など第三者のアドレス情報を登録しがちなことなど，利用者の行動や趣向が現れるプライバシー性の高い端末であるということも注目すべき点となります．現在，悪意のあるアプリやプライバシーの漏洩に対する不安のあるアプリの解析技術に関する研究が盛んに行われており，アプリマーケッ

† 株式会社KDDI研究所 ネットワークセキュリティグループ
"Security Technologies on Image Information (11); Mobile Security" by Keisuke Takemori (Network Security Group, KDDI R&D Laboratories Inc., Saitama)

トへの適用が進められています．

以下，3章では端末，4章ではネットワーク，5章ではアプリマーケット，6章ではサービスの各領域に潜むリスクと対策を，利用者や開発者の視点から詳解していきます．

3．端末に潜むリスクと対策

端末に潜むリスクとして，利用者やウイルスによる権限奪取や不正な改造，これに起因して端末が起動しなくなる不具合，遠隔から制御されてしまう踏み台化などが挙げられます．このため端末やOSの堅牢化は重要であり，いくつかの対策が施されています．また，悪意のあるアプリへの感染，情報漏洩，利用者自らの悪用，紛失などに対する端末管理サービス（Mobile Device Management: MDM）もあります．以下，端末やOSの堅牢化とMDMについて，事例を紹介します．

3.1　端末の堅牢化

一般に，スマートフォン向けOSは，端末の改造や踏み台化を阻止する機構を備えています．以下に，その一例を示します．

(1) ウイルスへの自動感染を阻止する手動操作型のインストール機構
(2) セキュリティ運用がなされたアプリマーケット経由のインストール機構（注：OSによっては解除可能）
(3) アプリから端末内の機能や情報へのアクセスを，利用者に通知して承諾を経るパーミッション機構
(4) 個々のアプリを隔離して実行するサンドボックス機構
(5) 不具合への迅速な対応のためのアップデート機構

この他に，端末ベンダの中には，OSやドライバの完全性を検査するセキュアブートの機構を組込み，端末の起動時やOSのアップデート時に実施している事業者もいます．ひとたび端末が出荷されると，さまざまな利用シーンやリスクウェア，悪意のあるWebサイトの閲覧などに晒されるため，所望の状態を保つことが重要です．

なお，(3)については，独自のパーミッション機構を端末にプリセットする通信事業者もあります[1]．アプリの実行時にJust in Timeな通知を行い，アクセス設定（許可/拒否）を選択できます．また，設定画面よりアプリや利用者情報の種別ごとにアクセス設定の変更を行えます（図2）．これにより，利用者情報の送信に関する透明性を確保して，プライバシー情報の漏洩に対する不安の解消に努めています．

3.2　MDM（Mobile Device Management）

端末の紛失やアプリの利用制限のために，リモートロックやワイプ，端末の位置検索，データの暗号化保護，データのクラウド管理などのサービスを提供するMDMがあります．専用のソフト・サービスとして提供されるのが一般的ですが，ウイルス対策のソフトの中には，こうしたMDMの機能を具備するものもあります．MDMは主に法人における業務用端末の管理に利用されることが多く，守りたい対象，管理すべき事項を明確にして導入されています．リスクをゼロにできないスマートフォンをさまざまなシーンに利活用できるよう，環境を整えたいところです．

設定画面より，アプリ，利用者情報種別ごとのアクセス設定（許可・拒否）の確認および変更が可能．

図2　アプリによる利用者情報へのアクセス設定

4．ネットワークに潜むリスクと対策

ネットワーク利用におけるリスクとして，スマートフォンを偽のWiFiアクセスポイントに接続してしまうことでの盗聴などの攻撃リスクがあります．また，社内PCをスマートフォンのWiFiテザリング機能を用いて，インターネットへ直接接続させる社内LANのバックドア化という運用上のリスクがあります．以下，これら二つのリスクと対策について考えます．

4.1　偽のWiFiアクセスポイントへの対策

スマートフォンを偽のWiFiアクセスポイントに接続してしまうことで，通信の盗聴や，通信に割り込む中間者攻撃（Man in the Middle攻撃）の脅威があります．

例えば，図3に，スマートフォン向けアプリで自動車のドアロックを解除するサービスが狙われた事例を紹介します[2]．

① 既存の有名なWiFiアクセスポイントと同じ名前（SSID）の偽のWiFiアクセスポイントを名乗り，パスワード入力を要求することなく，利用者を騙してスマートフォンからの通信を引き込みます．
② 偽のWiFiアクセスポイントから，利用者のスマートフォンにインストールされたドアロック制御アプリに，偽のServer証明書を渡します．
③ 攻撃対象となったドアロック制御アプリは，Server証明書の正しさを検証していませんでした．そして，偽

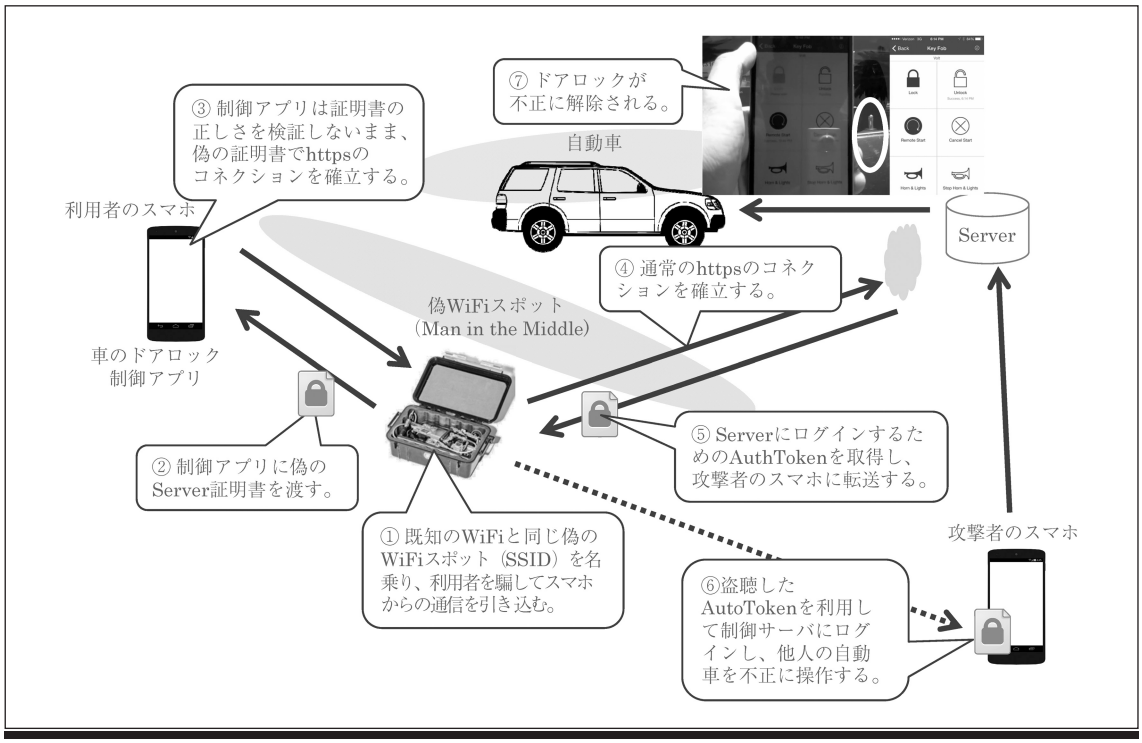


図3　偽のWiFiアクセスポイントにスマートフォン（スマホ）からの通信を引き込む自動車をターゲットとしたMan in the Middle攻撃の事例

の証明書を信じ，偽のWiFiアクセスポイントとの間でhttps通信コネクションを確立します．

④偽のWiFiアクセスポイントは，Serverとの間で通常のhttps通信コネクションを確立します．これにより，ドアロック制御アプリとServerの間の暗号化通信路に，偽のWiFiアクセスポイントが割り込むことに成功します．

⑤偽のWiFiアクセスポイントは，ドアロック制御アプリがServerにログインするための認証情報（AuthToken）を取得（盗聴）し，攻撃者のスマートフォンに転送します．

⑥盗んだAuthTokenを利用して，本人になりすましてサーバにログインし，他人の自動車のコントロールパネルを遠隔操作します．

⑦結果として，ドアロックが不正に解除されます．

このように，昨今ではスマートフォンやアプリの脆弱性が突かれることで，自動車という財産の損失にも繋がり兼ねない問題も出てきています．SSIDを偽装することで，正規のWiFiアクセスポイントになりすますことは容易であり，利用者にとって偽物であることを見抜くことは困難です．利用者ができることとして，パスワード設定のないWiFiアクセスポイントの利用を避けること，WiFiの接続設定において，あらかじめ，パスワードを要求しないアクセスポイントには接続しない設定にすることや，見知らぬSSIDに接続しない心構えが必要です．アプリベンダは，サーバとアプリ間の通信は，httpsなどの暗号化を施すとともに，サイト証明書の正当性を検証する処理を確実に実装する必要があります．

4.2　WiFiテザリングに関する対策

WiFiテザリングは，スマートフォンを経由して周囲のPCをインターネットに直接接続できる便利なツールです．しかし，法人における社内ネットワークの運用においては注意が必要です．例えば，社内PCから外部への通信をゲートウェイで一括監視するような運用を行う法人では，WiFiテザリングによって社内PCからの通信が直接インターネットに繋がってしまいます．これがバックドアとして監視の対象外となり，ウイルスの感染源や情報漏洩の原因となりえます．社内PCから認められていないWiFiアクセスポイントへの接続制限を行う必要があり，WiFiアクセスポイントをPCの管理画面上から見えなくするPC管理ツール[3]などの導入が求められます．

5．アプリマーケットに潜むリスクと対策

現在，アプリマーケットを通じてさまざまなアプリが流通している．アプリの中には，図4に示すリスクを持つリスクウェアも含まれており，アプリマーケット運営者とアプリ利用者に，適切な対処と行動が求められています．以下，リスクウェアの特徴と一般的な対策について考えるとともに，アプリのセキュリティ品質の向上に重要な役割を担うアプリマーケット運営者の対応について考察します．

5.1　リスクウェアと一般的な対策

【悪意のあるアプリ】

OSやアプリの脆弱性を突いて管理者権限を奪うアプリ，端末を不正に改造するアプリ，情報漏洩を狙うスパイウェ

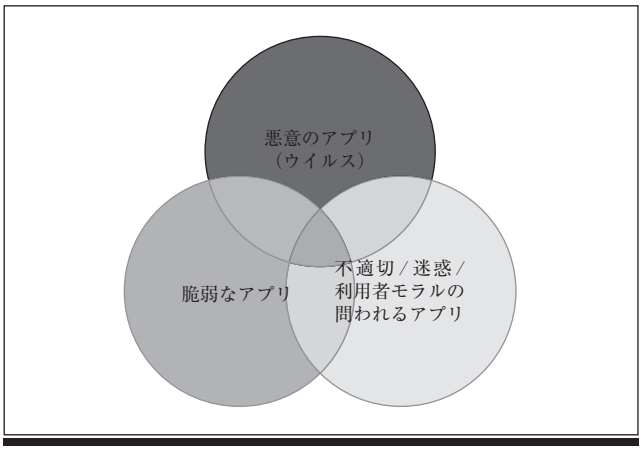


図4　スマートフォンにおけるリスクウェア

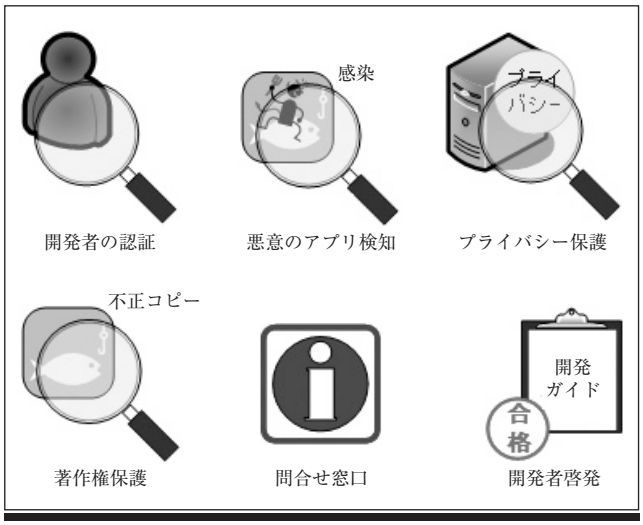


図5　アプリマーケット運営者に期待するセキュリティ運用の一例

アアプリ，遠隔制御を狙う踏み台化アプリなどがあります．これらの中には，本物そっくりの偽者アプリが多く見られます．

悪意のあるアプリに感染しないためには，しっかりしたセキュリティ審査のあるマーケットの利用を心掛けることです．また，不審なアプリを見かけたらインストールを避ける心構えも必要です．

【不適切/迷惑/利用者モラルの問われるアプリ】

悪意はないものの勝手に情報を送信するプライバシー漏洩に対する不安を伴うアプリ，OSを直接制御するコマンドを内包するアプリ，頻繁な通信や電池消費の激しいアプリ，望ましくない出会いなどに悪用されるアプリなどがあります．

PCよりも幅広い年代への普及が進むスマートフォンにおいて，利用者のリテラシ向上は重要な課題です．通信事業者の中には，“ケータイ教室”を通じた注意喚起や啓発を促すプログラムもあります[4]．スマートフォンを通じて巻き込まれやすいトラブルの事例を挙げて，具体的な対応策が解説されています．

【脆弱なアプリ】

アプリ自体に悪意はないものの脆弱性を突かれて，秘匿すべき情報を読取られてしまう場合や，他のアプリから勝手な制御を受けてしまう場合など，踏み台化されてしまうアプリがあります．

アプリ開発者による安全な設計やコーディングの普及が望まれる中，日本スマートフォンセキュリティ協会（JSSEC）から，安全なアプリ開発についてのガイドが公開されています[5]．アプリ開発者は，こうしたガイドを参考に，セキュリティ品質の向上に努めて頂きたいと思います．

5.2　アプリマーケット運営者の対策

図5に，アプリマーケット運営者に望まれるセキュリティ運用を纏めてみました．

【アプリ開発者の認証】

アプリ開発者の所在と事業内容の確認は重要です．アプリの説明欄に，開発者のWebサイトや事業内容，関連アプリについて紹介することが推奨されます．

【悪意のあるアプリの検知】

悪意のあるアプリの検知は，アプリを掲載する前に行われるべきです．アプリの挙動に注目した動的解析や，アプリを構成するファイルやコードに注目した静的解析などの技術を組み合わせて，既知と未知を含めた悪意のあるアプリを検知する体制作りが望まれます．

巧妙化する悪意のあるアプリに対して，解析技術の発展は重要であり，活発な研究開発が進められています．例えば，スマートフォン内の情報を漏洩させるスパイウェアに対しては，テイントと呼ばれる解析技術があります[6]．これは，注目する情報に対してタグ付けしておき，アプリがアクセスした情報が，スマートフォン内で何処から何処へ流れていくかを追跡する技術です．あるアプリがタグ付けされた情報を，暗号化や分割を図りながら複数のファイルに書き出し，別のアプリがこれを外部送信する場合でも，OS側からタグの流れをモニタすることで情報の流れを掴むことができます．この他，アプリがSSLなどの暗号ライブラリーや通信インタフェースを呼びだす処理をフックすることで，アプリの動作をモニタする研究も進められています[7]．図6に，これを応用したアプリ解析専用のOS・仮想端末が開発され，アプリマーケット運営者におけるセキュリティ審査に活用されている様子を示します．

【プライバシー保護】

利用者の趣向や位置を活用した広告モジュールが，アプリの中に組込まれて広く配布されています．便利で透明性が高く，利用者関与の機会が提供される広告モジュールは歓迎されうるものです．しかし，「何の情報」を「何処」へ「なぜ」送信するのか不明確な広告モジュールも少なくなく，勝手な情報送信に対するプライバシー漏洩に対する不安が指摘されています．アプリマーケットでの，アプリ向けプ

図6　アプリの動的解析用OSとSSL処理のフックの様子

図7　悪意のあるWebサイトと連動する振り込め詐欺アプリ

ライバシーポリシ掲載や，アプリをダウンロードする前のプライバシーポリシのポップアップ通知などを通じて，透明性の確保や利用者関与の機会の提供が望まれます．プライバシー保護については，6.2節でサービス提供者視点からも再掲します．

【著作権保護】

アプリマーケット運営者による他者のコードや画像を盗用するアプリについての監査も，開発者のみならず利用者の立場からも望まれます．例えば，日本製のゲームアプリは，開発費を要するものの高品質なアプリが多く，価格もそれなりの額になります．他者のコードを盗用した低品質な無料アプリが普及することで，高額であるが高品質なアプリが埋もれてしまう問題があります．本来受け取るべき対価を得られない高品質なアプリを提供するベンダの運営が脅かされ，品質の低下を招きかねません．この他，有料のゲームアプリを逆コンパイルして，踏み台化コードを埋め込んで再コンパイルし，非公式な配信サイトを通じて無料で公開した事例もあります．ゲームとしての機能はそのままに，密かに踏み台化処理が動作するため，感染しても気づくことは難しくなります．これらのリスクを排除するためにも，著作権保護に関する運営や技術の発展が望まれます．

【問合せ窓口】

リスクウェアに関する問合せ窓口を設けることで，事前審査で漏れたリスクウェアを利用者から通報して貰うことができ，迅速な事後対応が可能になります．

【アプリ開発者向けガイドを通じたサポート・啓発】

安心・安全なアプリの開発を促す開発者向けガイドを通じたサポート・啓発も重要です．

6．サービス提供に潜むリスクと対策

悪意を持ったサービス提供者や，利用者モラルを問われるサイトが数多くみられます．また，利用者の趣向や行動を分析した各種サービスが普及しています．以下，このようなサイトにアクセスする際のリスクに対して，利用者とサービス提供事業者が取組むべき対策について考えます．

6.1　悪意のあるWebサイトや出会い系サイトに潜むリスクと対策

電話番号やメールアドレス，位置情報などスマートフォンが持つ利用者情報を悪用して，利用者を騙す振り込め詐欺が問題となっています．図7に，悪意のあるアプリをインストールさせて，そのアプリを通じてスマートフォンから取得した利用者情報を悪意のあるWebサイトへ転送し，利用者の電話番号などが記載された偽の請求書画面をダウンロード・表示する詐欺の一例を示します．本筆者のスマートフォンを用いて実験した画面ですが，本人を特定するような情報とともに不当な請求がなされており，わかっていても怖さを感じるものでした．

スマートフォン向けセキュリティ対策ソフトの多くは，悪意のあるアプリへの感染や悪意のあるWebサイトの閲覧による被害を抑止する機能が搭載されています．さまざまな悪意のあるアプリや悪意のあるWebサイトが現れる中で，安心・安全な利用のために，こうした対策ソフトの導入が望まれます．

SNSサービスの普及によりネット上での交流が進んでいます．離れた友人との会話やサークルやボランティア活動の支援など，健全な活用が期待されています．しかし見知らぬ人からの友達募集には注意が必要です．善悪の不明な誘いに安易に応えない心構えが求められます．また写真をアップロードする際にも注意が必要です．スマートフォンが持つ位置測位のGPS情報が付与されているケースがあ

り，犯罪被害に繋がるケースがあります．

スマートフォンは個人との結びつきが強く，そこで生じる問題を一人で抱え込んでしまいがちです．不安を感じる際には，勇気をもって周囲に相談してみることが，リスク回避の一歩となります．

6.2　プライバシー侵害のリスクと対策

スマートフォンでは，アプリを通じたサービス提供が進んでいます．主なものとして，利用者の趣向や行動に合わせた広告サービスが挙げられます．以下，アプリを介した情報送信の実態調査と，行政や事業者の取組みについて紹介します．

【実態調査】

多くのアプリは，アプリ本来の機能を提供するコードに加えて，利用者の趣向に合わせた広告を提供する第三者ライブラリーから構成されています．こうしたアプリからの情報送信について，3年にわたる実態調査が公表されています（**表1**）[8]．2013年2月のデータでは，情報送信を伴うアプリが63%ある中で，送信情報について何らかの説明を行うアプリが57%，送信情報が正しく説明されているアプリが11%という状況にありました．2011～2013年の変化をみると，送信情報について何らかの説明を試みるアプリが13%→19%→57%と大幅に改善してきていますが，送信情報を正しく説明できている割合は，9%→3%→11%と，1割程度に留まっているのが実情です．

【行政/業界によるプライバシー保護に向けた取組み】

利用者情報を勝手に送信するアプリがプライバシー保護の観点から懸念される中，総務省から，2012年8月に「スマートフォンプライバシーイニシアティブ（SPI）」が，2013年9月にその続編「SPIⅡ」が公表されました[9]．SPIでは，アプリから送信される情報についての透明性を確保するために，アプリ開発者向けに，**表2**に示す8項目をわかりやすく説明するアプリ向けプライバシーポリシを作成し，利用者へ説明することが提言されています．SPIⅡでは，アプリ向けプライバシーポリシの内容が正しく，端的な説明の普及に向けた取組み事例が紹介されています．

SPI・SPIⅡの提言を受け，複数の業界団体においてプライバシー保護に関わる取組みが進められています．アプリ向けプライバシーポリシの作成面では，2012年11月にモバイルコンテンツフォーラム（MCF）が，2013年4月に日本オンラインゲーム協会（JOGA）が，作成フォームを含めたガイドラインを公表しています[10) 11)]．また，JSSECから，SPI・SPIⅡに則したプライバシーポシリの作成と利用者への開示手順について易しく解説されています[12)]．アプリ開発者は，是非参考にして頂きたいと思います．

海外においても，プライバシー保護については重視されており，例えば，2013年1月に米国カルフォルニア州司法長官とOSベンダとの間で，利用者のプライバシー保護に向けた対策について合意に至っています[13)]．

表1　人気上位アプリからの情報送信に関する実態調査
（KDDI研究所調べ[8)]）

調査期間	2011年8月	2012年4月	2013年2月
対象：人気の無料アプリ	400アプリ	100アプリ	100アプリ
利用者情報の送信アプリ	45%（181/400）	81%（81/100）	63%（63/100）
ポリシを開示	13%（24/181）	19%（15/81）	57%（36/63）
送信情報の正しい記載	9%（17/181）	3%（2/81）	11%（7/63）

表2　SPI提唱のアプリ向けプライバシポリシに記載すべき8項目
（本筆者による要約）

①	アプリ提供者等の氏名または名称
②	取得される情報の項目
③	取得方法（自動送信，手動送信）
④	利用目的の特定・明示
⑤	通知・公表または同意取得の方法
	利用者関与の方法
⑥	外部送信・第三者提供の有無
	情報収集モジュールの有無
⑦	問合せ窓口
⑧	プライバシポリシの変更を行う場合の手続

7．今後の期待

ここまで，スマートフォンに潜むリスクと対策技術について紹介してきました．現在のスマートフォンを安心・安全に利活用するための基礎知識となります．

最後に，セキュリティ技術が支えるスマートフォンの未来の可能性について，筆者なりに予測してみます．ポイントは，耐タンパ性のあるSubscriber Identity Module（SIM）と呼ばれるセキュアエレメントを搭載している点です．**図8**にSIMとスマートフォン向けアプリを連携させたオンラインバンキングサイト向けの認証，電子署名の応用例を示します．一般にオンラインバンキングサイトへのログイン処理は，ID，Passwordによる記憶認証と，乱数表などを用いた所有認証が組み合わされています．これに対して，偽のログイン画面にログインID，Password，そして乱数表の値をすべて入力させることで，騙し取る攻撃が出てきています．そこで図8に，乱数表の代わりとなる2要素目の認証として，SIMの中にクライアント証明書を管理しておき，ID，Passwordの検証後に，サイト側からチャレンジを送付し，スマートフォンのSIMの内部でレスポンスを生成して返送する認証モデルを考えています．このモデルは，通信事業者がSIMに対して行う利用者認証と同レベルの強固な認証方式であり，かつ利用者による特別な操作が不要なことから，次世代の2要素目の認証技術として期待されます．

①ID，Passwordの検証後に，スマートフォンのSIMに発行されたクライアント証明書を，オンラインバンキングサイトへ送付します．なお，ペアとなる秘密鍵は，SIM内で安全に管理されることを想定します．

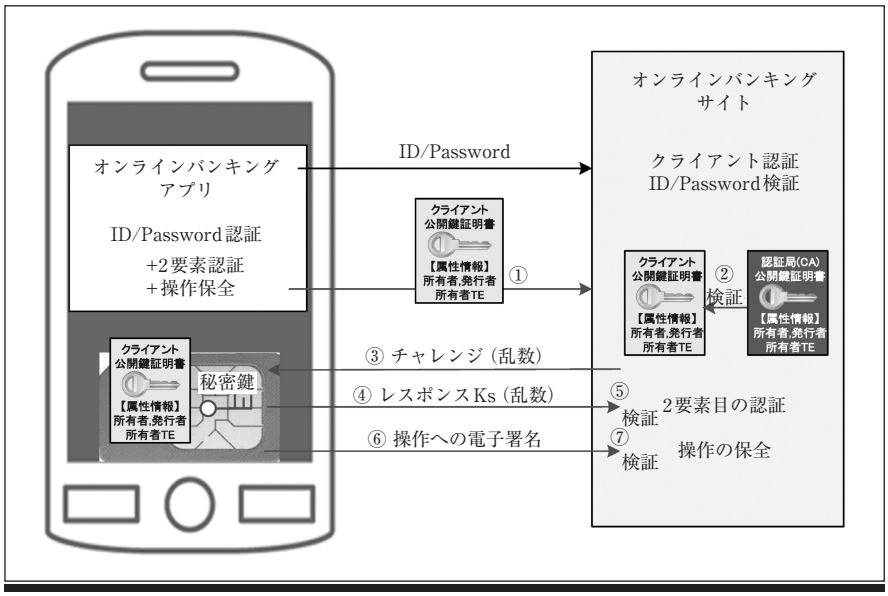


図8　サービスサイトに対する二要素認証・電子署名

②サイト側では，クライアント証明書を発行した認証局の公開鍵証明書でこの正当性を検証します．

③検証に成功すると，サイト側からスマートフォンに向けてチャレンジ（乱数）を送付します．

④スマートフォンのSIMで管理される秘密鍵で，チャレンジを暗号化し，レスポンスとしてサイト側へ返送します．

⑤レスポンスを検証済みのクライアント証明書で検証します．具体的には，クライアント証明書に記載された公開鍵でレスポンスを復号し，チャレンジとして送付した値と同じ値であるか検証します．検証に成功すると，振り込みなどの重要な処理の実行を承認します．

⑥必用に応じて，スマートフォン側のオンラインバンキングアプリが操作ログを出力し，これに対して，SIM内の秘密鍵で電子署名を施し，サイト側へ送付します．なお，電子署名は，操作ログのダイジェストを算出し，これを秘密鍵で暗号化することで作らます．

⑦サイト側は，操作ログに付与された電子署名を，クライアント証明書で検証し，証拠として保全します．この電子署名の検証は，クライアント証明書に記載された公開鍵で電子署名を復号した値と，操作ログのダイジェストとして算出した値が，一致するかを確認します．

ちなみに，通信事業者などがRoot認証局となって発行された中間認証局アプリを，SIMの内部に組込むことで，スマートフォン内のアプリに対して，クライアント証明書を簡単に発行できるようになります．公的証明書を用いて貸与されるSIMがスマートフォン内のアプリと連携することで，人からアプリ，そして外部サイトへの信頼の輪が繋がるようになります．将来，スマートフォンが，身元を堅牢かつ簡易に証明できるパーソナルな認証局を担う時代がくるかもしれないですね．

（2016年2月2日受付）

〔文　献〕

1) KDDI：プライバシーデータ設定，http://news.kddi.com/kddi/corporate/newsrelease/2014/10/20/besshi713.html
2) S. Gallagher: "OwnStar Wi-Fi attack", http://arstechnica.com/security/2015/08/simple-wi-fi-attack-grabs-bmw-mercedes-and-chrysler-cars-virtual-keys/
3) 日立ソリューションズ：PC管理ツール“秘文”，http://www.hitachi-solutions.co.jp/company/press/news/2013/1127.html
4) KDDI：ケータイ教室，http://www.kddi.com/family/
5) JSSEC：Androidアプリのセキュア設計・セキュアコーディングガイド，http://www.jssec.org/dl/android_securecoding.pdf
6) W. Klieber: "Android Taint Flow Analysis for App Sets", The 3rd ACM SIGPLAN International Workshop on the State of the Art in Java Program Analysis（SOAP '14）（June 2014）
7) 川端秀明ほか：“Androidにおける細粒度アクセス制御機構”，情処論，54，8，pp.2090-2102（Aug. 2013）
8) 竹森敬祐ほか：“アプリ/コンテンツ向けプライバシポリシーの第三者検証フレームワーク”，情処，第62回CSEC研究会，62（July 2013）
9) 総務省：スマートフォン・プライバシ・イニシアティブ（SPI），SPIⅡ，http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html，http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000122.html
10) MCF：“スマートフォンのアプリケーションプライバシポリシーに関するガイドライン”，2012年11月，http://www.mcf.or.jp/temp/sppv/mcf_spappp_guidline.pdf
11) JOGA：“スマートフォンゲームアプリケーション運用ガイドライン”，2013年4月，http://www.japanonlinegame.org/pdf/JOGA130405.pdf
12) JSSEC：“スマートフォン・アプリのプライバシーポリシー作成・開示についての考察”，https://www.jssec.org/dl/140206_03-1_app_policy.pdf
13) 米国カルフォルニア州司法長官：“PRIVACY on the GO”，http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf

竹森　敬祐（たけもり　けいすけ）　1996年，慶應義塾大学理工学研究科修士課程修了．同年，現（株）KDDI研究所へ入社．主に，インターネットセキュリティ，スマートフォンセキュリティ，自動車セキュリティの研究に取組む．2006年，Interop Tokyoプロダクト部門グランプリ，2010年，山下記念論文賞，2013年，喜安業績記念賞など受賞．JSSECアプリWGリーダを務め，2013年，総務大臣表彰を受ける．博士（工学）．

講 座

映像情報メディア関連のセキュリティ〔最終回〕

マイナンバー制度とマイナンバーカード

渡邊　創†

1．まえがき

2015年1月より連載されてきた「映像情報メディア関連のセキュリティ」も最終の12回目となりました．今回は，セキュリティ・プライバシー技術を活用した身近な実システムとして，2015年10月より通知カード配布が開始され，2016年1月より運用が開始されたマイナンバー（「個人番号」が正式名称ですが，以降通称であるマイナンバーで記述します）を用いたシステム（社会保障・税番号制度，あるいは個人番号制度）[1]，マイナンバーカード（個人番号カード）[2][3]とそれを用いたシステムについて紹介します．

マイナンバーとマイナンバーカードが何に使われる/使えるのか，どのような不正にどのようなセキュリティ対策が採られているのかなど，多くのメディアでも誤った解説が散見されます．これまでの連載で解説されてきた技術が，システムの表側，裏側でどのように活用され，不正が防がれているのか，本稿が皆様の理解の一助になれば幸いです．

2．マイナンバーとは

マイナンバーは，住民票を有するすべての人（中長期在留者や特別在留者などの外国人を含む）各々に個別の12桁の番号を付け，社会保障，税，災害対策の分野で効率的に情報を管理し，複数の機関に存在する個人のデータが同一人のものであることを確認するために活用されるものです．これにより，例えば，同姓同名の人の区別など，これまで人が判断することで起きていた確認手続の誤り等がなくなり，早く，簡単かつ正確に行えるようになります．マイナンバーは，市町村長が法定受託事務として，住民票コードを変換することで生成されたものです．ちなみに，マイナンバーから住民票コードを復元することはできない変換法を使用しています（一方向性関数の利用）．住民票コードも個人に割当てられた番号なのですが，住民票コードは今回のような利用を想定しておらず，運用の大幅な改変が必要になることや，パブリックコメントの多数意見が「新しい番号の利用」だったこと等が理由になり，新たな番号を各個人に付番することになりました．

マイナンバー導入により期待される効果としては，主に次の三つが挙げられています．

(1) 公平・公正な社会の実現：所得や他の行政サービスの受給状況を把握しやすくなるため，負担を不当に免れることや給付を不正に受けることを防止するとともに，本当に困っている方にきめ細かな支援を行えるようになります．

(2) 国民の利便性の向上：市町村役場内の別の部署で保存されるデータの関連をとることが容易となり，行政手続が簡素化され，国民の負担が軽減されます．また，2017年1月に開設が予定されている「マイナポータル」と呼ばれる個人用のポータルサイトを活用することで，行政機関が持っている自分の情報を確認したり，行政機関から個人向けのさまざまなサービスのお知らせをより簡単に受け取ったりできるようになります．

(3) 行政の効率化：行政機関や地方公共団体などで，さまざまな情報の照合，転記，入力などに要している時間や労力が大幅に削減されます．複数の業務の間での連携が進み，作業の重複などの無駄が削減されるようになります．

(1) については，例えば，2007年に起きた年金の情報が紛失された「年金記録問題」，また「生活保護の不正受給」といった問題を防止することに役立つと考えられています．(2) の行政手続きの簡素化，国民負担の軽減については，例えば，市町村役場内での手続きにその市町村の証明書添付が必要だったものが，手続き窓口でのマイナンバー提示のみで済むようになります．また今後，マイナポータルと呼ばれるサイトが作られ（2017年1月稼働開始を予定），マイナンバーが何の目的で使われているのか（行政サービスが，自分のどのような情報をいつどこから取得したのかなど）を確認できるようになる予定です．(3) は，ある人のデータをマイナンバーで一意に特定できるようになること

†国立研究開発法人産業技術総合研究所

"Security Technologies on Image Information (Final study); Social Security and Tax Number System and Individual Number Card" by Hajime Watanabe (National Institute of Advanced Industrial Science and Technology, Tsukuba)

による，行政側で実現できる効率化のことで，人力に頼っていた確認作業やデータの突合，連携作業の電子化，自動化ができるようになります．

マイナンバー導入による一番の効果は，(3) の行政の電子化による効率化だと言えます．それにより (1) の年金や税金などの公平・公正化や (2) の利便性向上も実現されると理解するぐらいが良いのではないでしょうか．導入時にはコストはかかりますが，将来的には電子化したメリットの方が大きくなると考えられ，効率化やコストダウンでサービスの質の向上や予算の別事業への移し替えも可能となるでしょう．

3．マイナンバーとは何であり何でないか

マイナンバーは，いわゆるIDと呼ばれるものの一種です．ISO/IEC 29100 Information technology - Security techniques - Privacy framework[4] の用語を用いるとPII (Personally Identifiable Information) の一つであると定義できます．すなわち個人を一意に特定できる情報です．一方，マイナンバーは個人を認証する情報としては使えません．氏名もPIIの一つですが，ネットワークで「メッセージの送り主である」と主張する名前が送られてきたからと言って，その名前の人からメッセージが来たとは言えません．名前を知っている人は誰でも，そのような主張が可能であるからです．マイナンバーも同様に，個人認証の用途では用いることはできません．

マイナンバー導入への不安でよく言われるのが，“米国の社会保障番号 (SSN: Social Security Number) や韓国の住民登録番号を用いた成りすましや個人情報の流出[5][6] と同じことが起きるのでは？”ということです．

ではなぜ米国や韓国の番号が成りすまし犯罪の原因となったか，具体的に振り返ってみましょう．米国のSSNは1936年より米国社会保障局 (Social Security Administration) が発行し，社会保障制度で用いる9桁の個人を特定するための番号です．SSNもPIIの一種です．実質的に国民全員に振られている番号であるため，さまざまな分野での連携に用いられる共通番号となっています．税の確定申告など官での活用だけでなく，銀行口座の開設やクレジットカードの発行などでも提示が求められるなど，民でも幅広く用いられています．またしばしば，SSNの下4桁を知っているかどうかで本人確認が行われていました．SSNは信頼度の低い相手にも提示する機会が少なくなく，結果として悪意のある人に番号を知られる可能性が少なくありません．悪意のある人が他人のSSN番号を取得すれば，その4桁の番号を利用してなりすますことは容易でしょう．当然その対策も進められており，SSNの印刷やSSNを認証に用いることを禁止する法律を制定する州も存在します．しかし民間での商用利用を禁止するまでには至っていません．1968年に導入された，韓国の住民登録番号も同様の誤った使い方がされてきました．住民登録証以外に，パスポート，運転免許証，健康保険証，公務員証など政府と公共団体が発行するほとんどの証明証に住民登録番号が記載され，番号が本人確認の用途で使われてきました．韓国の大手通信会社では，無料Wi-Fiの利用で自社ユーザ以外がアクセスしてきた場合に，住民登録番号を要求して本人確認を行っていたりします．韓国政府は住民登録番号に代わるI-PIN (Internet Personal Identification Number) と呼ばれる新たな番号を本人認証に使用できるようにするなど，対策を進めています．

以上述べたように，PIIを認証に使っていることが問題なわけですが，さて日本でのマイナンバーの使われ方はどうなるのでしょう？ 個人番号の目的外利用がマイナンバー法 (行政手続における特定の個人を識別するための番号の利用等に関する法律：第16条) で禁止されており，個人番号利用事務以外の場面でそうした不適切な本人確認が行われるような事態が起こらないよう，当初から対応されています．ただ世間一般での理解が充分でないことから，不適切なマイナンバーの取得や利用がいくつか報告されている[10] ため，引き続き「目的外 (ましてや認証) に使ってはいけない」ことを広く周知する必要があるでしょう．

マイナンバーが漏えいなどで悪意ある人に知られてしまうと何が起きるでしょうか？ 基本的にはPII，例えば，名前が漏えいした時と同じ状況であると考えられます．それだけでは大した問題ではありません．しかし，マイナンバーとそれに紐付けされた情報が漏えい等で複数知られると，それら複数の情報がマイナンバーでまとめられてしまいます．上で述べたように，氏名もPIIの一種ですが，例えば，同姓同名があり得るわけですから，氏名はマイナンバーに比べて個人特定の性能が悪いPIIであると言えます．逆に言えば，マイナンバーの方が性能の良いPIIと言えますので，その人個人の情報がマイナンバーによって確実に収集蓄積 (名寄せ) される可能性が高まります．このようなリスクを避けるために，SNSなどで無闇にマイナンバーを見せることは避けるべきでしょう．

4．マイナンバーを用いたシステムの情報管理とやり取り

図1のように，個人の情報はこれまで通り，各行政機関が保有します．つまり，情報は一つの場所に集められず，分散管理されているままです．別の機関がある情報を必要とした場合は，マイナンバーを用いて照会します．図1の例では，日本年金機構が市町村に対して地方税情報の提供を求めた場合の例が書かれています．行政手続きでは，

(1) 個人が行政機関 (例の場合：日本年金機構) にマイナンバーを提供 (あるいは登録しておく等，あらかじめ提供) する
(2) その人の情報はその都度マイナンバーを利用して情報 (例の場合：地方税情報) を保持する行政機関 (例

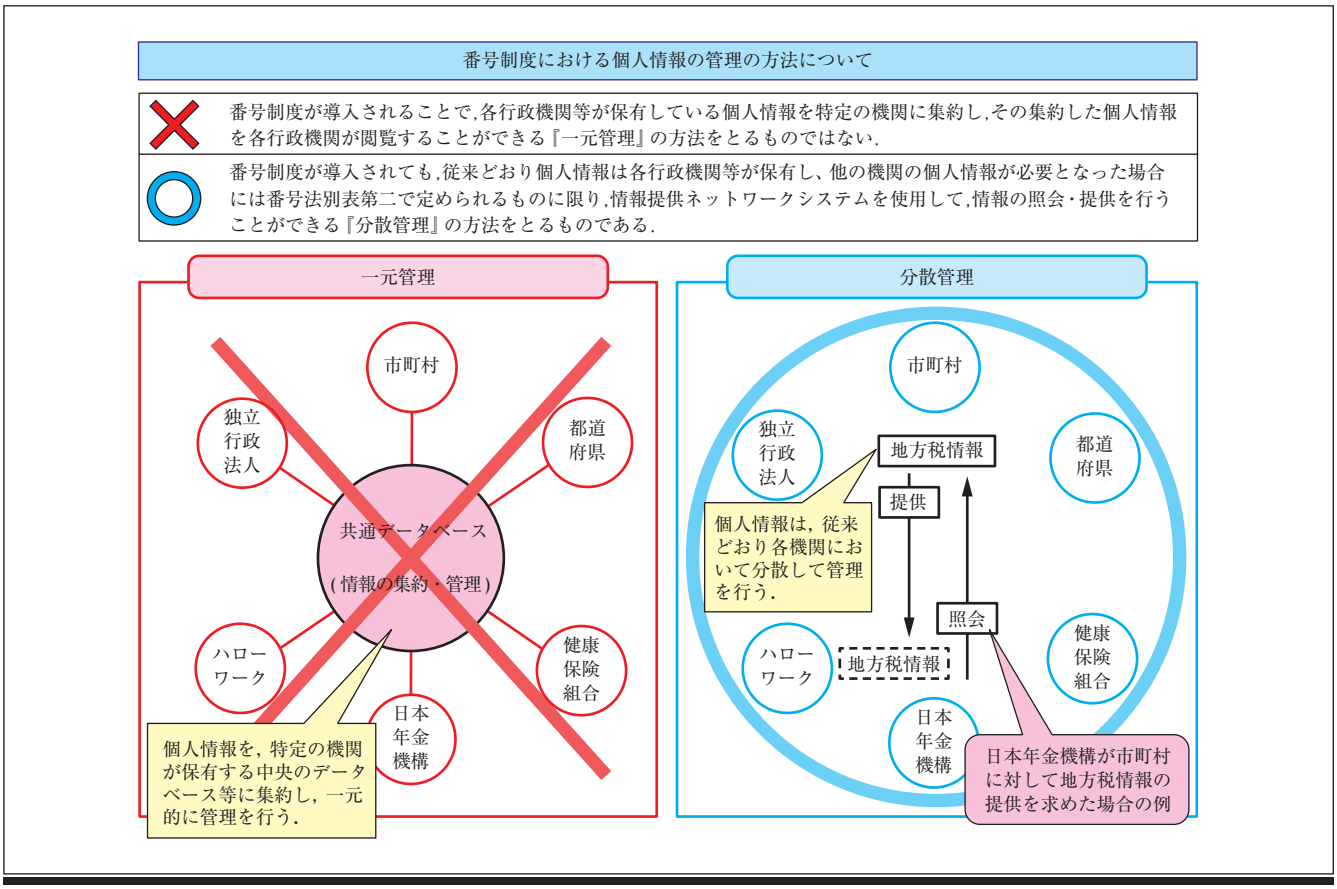


図1　個人情報の分散管理

の場合：市町村）に照会される

(3) その人の情報が照会元（例の場合：日本年金機構）に提供される

といった形で情報のやり取りが行われます．個人が行う手続き (1) では，窓口での本人確認後にマイナンバーの通知カード，またはマイナンバーカードを提示することで，あるいはネットワーク越しに，マイナンバーカードを利用した個人認証（5章を参照）での本人確認後にマイナンバー情報を送信することで，マイナンバーを行政機関に提供することになります．

さて，このような分散管理（これまでと同様の管理）機構で，情報が盗み出されるリスクを考えてみましょう．個々の機関のデータベースから盗み出されるリスクは，これまでと同程度であると考えられます，これまで紙でやり取りしていた部分が電子化された部分（図1右側「分散管理」の矢印で表された情報の流通）で盗み出されるリスクは新たに考える必要が出てきますが，通信路は暗号化されること，情報一つずつの入手となること，行政機関の職員が認証された上で処理が行われるので，どの職員が誰のどの情報を照会したのかすべて記録されること，などから，これまでと比べて大量の情報が一度に盗み出されるリスクはあまり上がらないと考えられます．

5．マイナンバーカードとは

2016年1月より，マイナンバーカードの交付が開始されました．マイナンバーカードは，本人の申請により交付されるICカードで，マイナンバーを証明する書類や本人確認の際の公的な身分証明書として利用できます．また，このカードがあれば，各種行政サービスのオンライン申請やコンビニエンスストアでの証明書取得など，さまざまな行政サービスを受けることができるようになります．当面の間，無料で交付されます．マイナンバーカードは図2のような構成になっています．表面には，氏名，住所，生年月日，性別，顔写真，電子証明書の有効期限の記載欄，セキュリティコード，サインパネル領域（券面の情報に修正が生じた場合，その新しい情報を記載（引越した際の新住所など）），臓器提供意思表示欄が記載されており，顔写真入り身分証明書として使えるようになっています．裏面にはマイナンバー（個人番号）とその番号のQRコードが記載されており，マイナンバーを提示するための機能が実現されています．実はマイナンバーカードでマイナンバーに関係する部分は裏面の記載とネット経由でマイナンバーを送付する際に使われるICチップ内に格納された番号情報のみなのです．対面でのマイナンバーカードの使用に関しては，通知カードに顔写真付きの身分証が付いたものという位置付けで，こ

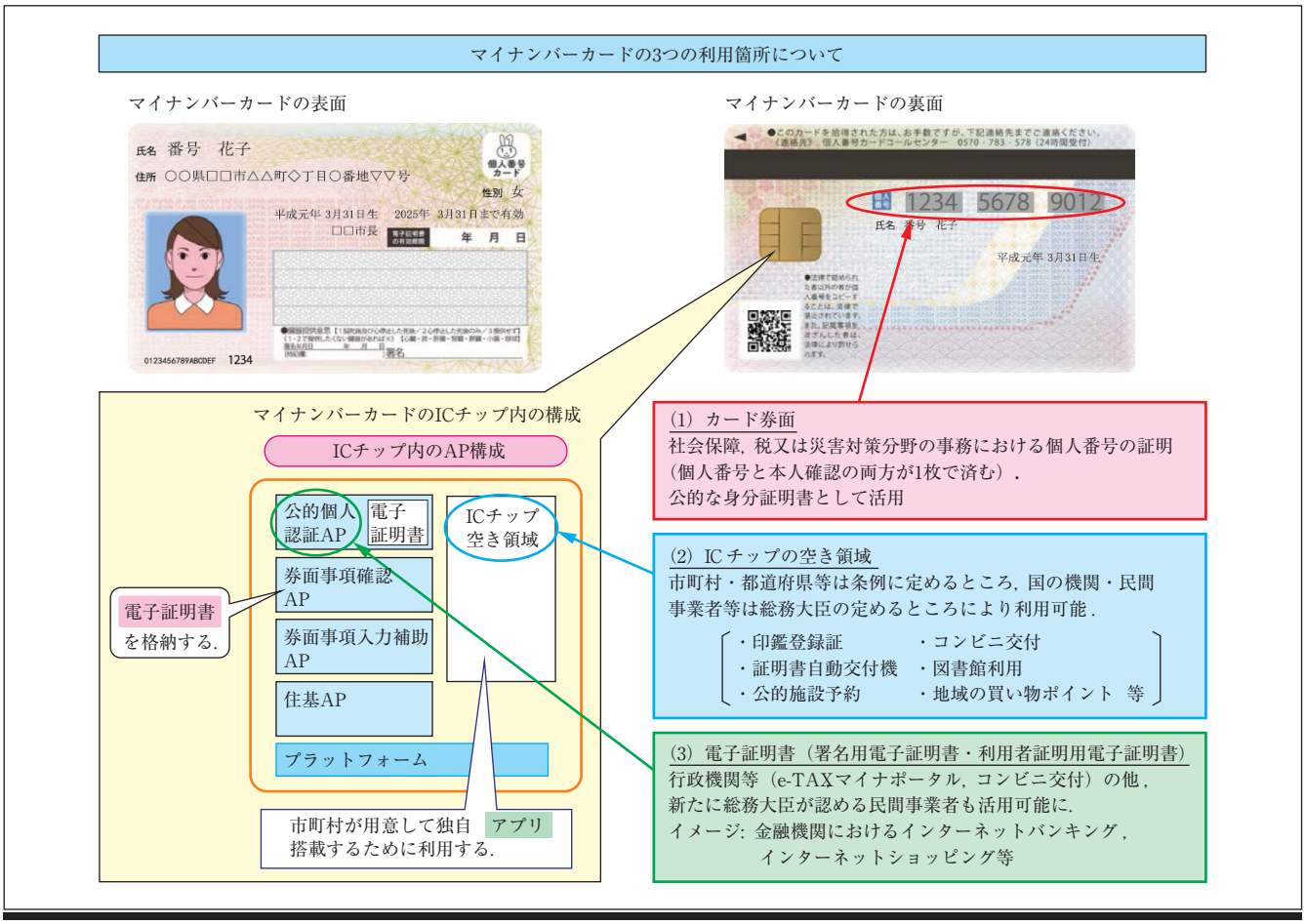


図2 マイナンバーカードの構成

れ1枚持っていけばマイナンバーに関する処理が行える（免許証等の提示は不要になる）というものになっています．

ICカードとしての機能はどうでしょう？ ICチップには，券面記載事項（氏名，住所，生年月日，性別，顔写真，個人番号等），総務省令で定める事項（署名用電子証明書，利用者証明用電子証明書）と，これらの情報や券面情報を利用したサービスを実現するためのアプリケーションソフトウェア（以下ではアプリ）が搭載されています．一番活用が期待されるのが，二つの電子証明書を利用した公的個人認証サービスです（図3）．「署名用電子証明書」は，氏名，住所，生年月日，性別の4情報が記載され，e-Taxの確定申告など電子文書を送信する際に使用できます．住民基本台帳カードですでに実現されていたサービスであり，今回住民基本台帳カードを置き換える機能となっています．この証明書を用いることで，「作成・送信した電子文書が，利用者が作成した真正なものであり，利用者が送信したものであること」を証明することができます．「利用者証明用電子証明書」は，マイナポータルや住民票などのコンビニエンスストアでの交付サービスの利用時等，本人であることを証明する際にその手段として使用できます．これは住民基本台帳カードには搭載されておらず，マイナンバーカードで新たに実現された機能です．この証明書を用いることで，「ログインした者が，利用者本人であること」を証明することができます．これら二つの電子証明書については，2016年1月から，総務大臣が認める民間事業者も使用可能となります．

6．マイナンバーカードのセキュリティ

マイナンバーカードには，マイナンバーの提示，署名用電子証明書，利用者証明用電子証明書等の機能を実現する必要最小限の情報のみが記録されます．図4のように，マイナンバーカードのICチップ内には，「公的個人認証AP」，「券面事項確認AP」，「券面入力補助AP」，「住基ネットAP」の4つのアプリと市町村等の行政機関が独自サービスを行うための空き領域があります．行政機関が保持している「地方税関係情報」や「年金給付関係情報」などプライバシー性の高い個人の情報は記録されません．

アプリごとにアクセス権限に関する情報を設定することにより，各サービス用システムから異なるアプリへのアクセスを制御しています（図5）．例えば，Aサービス用システムがカード内の情報Aにアクセスする場合，Aサービス用システムが情報Aにアクセスしても良いと確認されたときのみ，アクセス可能となるということです．また，ICチップ内の各アプリケーション間は「アプリケーション

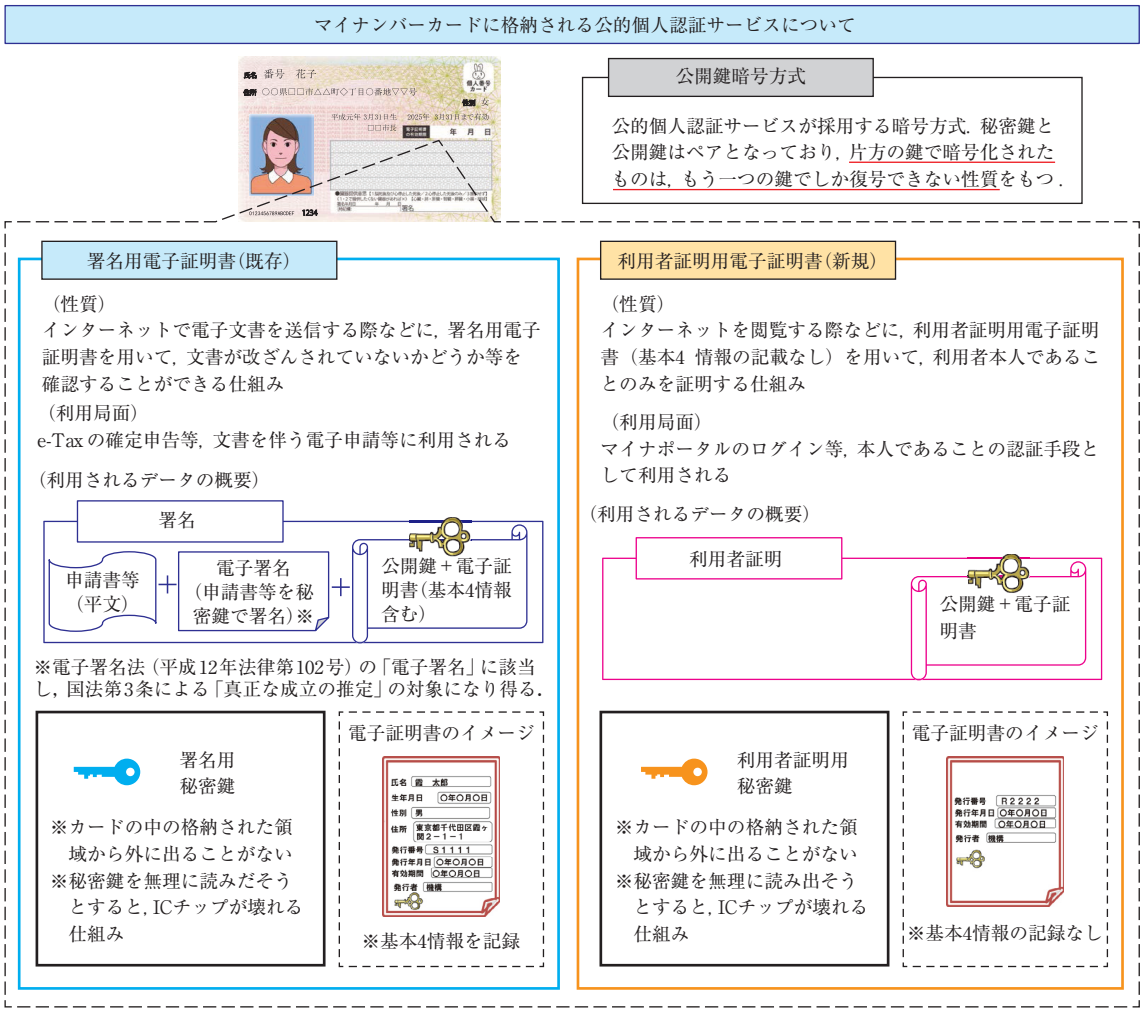


図3　マイナンバーカードを利用した公的個人認証サービス

ファイアウォール」により独立しており，例えば，カードアプリ（B）はカードアプリ（A）やカードアプリ（C）の情報にアクセスできないようになっています．

カードを盗まれたり落としたりしても，もちろん券面に書かれた氏名やその人のマイナンバーは読まれてしまいますが，直ちにICカードの機能が使われることがないよう，以下のようなさまざまな対策がとられています．

(1) 暗証番号：アプリ毎に異なる暗証番号を設定して情報を保護しています．また暗証番号の入力を一定回数以上間違えるとカードがロックされる仕組みが組込まれています．「署名用電子証明書」を使用するには6～16文字の英数字が，「利用者認証用電子証明書」を使用するには4桁の数字，など，アプリごとにその機能の重要性や有効期間を考慮した設定がされています（図6）．

(2) 耐タンパー性：耐タンパー性とは，ICチップ内の情報を不正に読出したり解析したりするのが困難であるという性質のことです．マイナンバーカードのICチップは，ICチップを取出し，電気的または物理的に情報を不正に読出すような行為に対して，

・光が当たるとメモリー内容が消去される
・メモリー回路素子が表面から観察できない
・電圧異常，クロック異常等の検知をした場合は動作を停止する
・メモリー素子をランダムに配置したり，記録内容を暗号化することにより，解読を困難にする

といった対策がとられています．またICチップの電力消費量や処理時間等を測定・解析し，情報を推測するような不正行為に対しても，消費電力，処理時間をかくはんすることで，読取った信号の統計的な解析を困難にする対策が講じられています（図7）．

(3) ISO/IEC15408認証：ISO/IEC15408認証とは，コンピュータシステムや製品のセキュリティ機能の評価を行うための国際標準です．これを取得することにより，IT製品として必要なセキュリティ機能要件が備わっていることが第三者により証明されます．マ

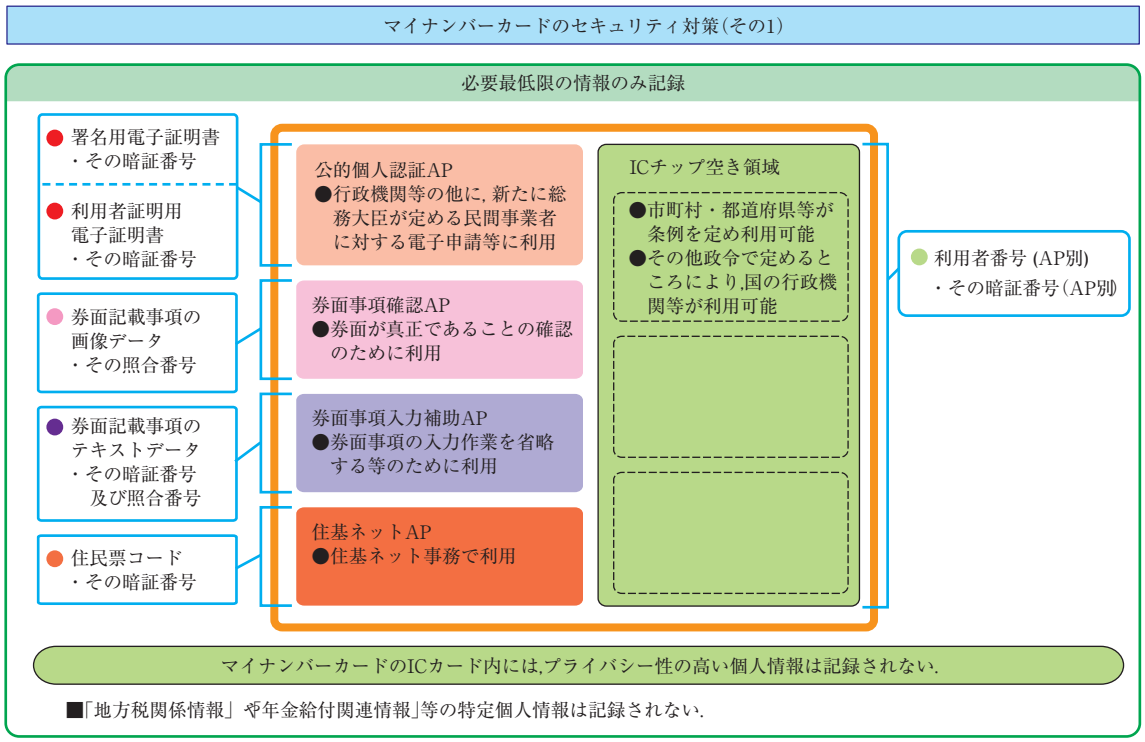


図4　マイナンバーカードに載っている情報・アプリ

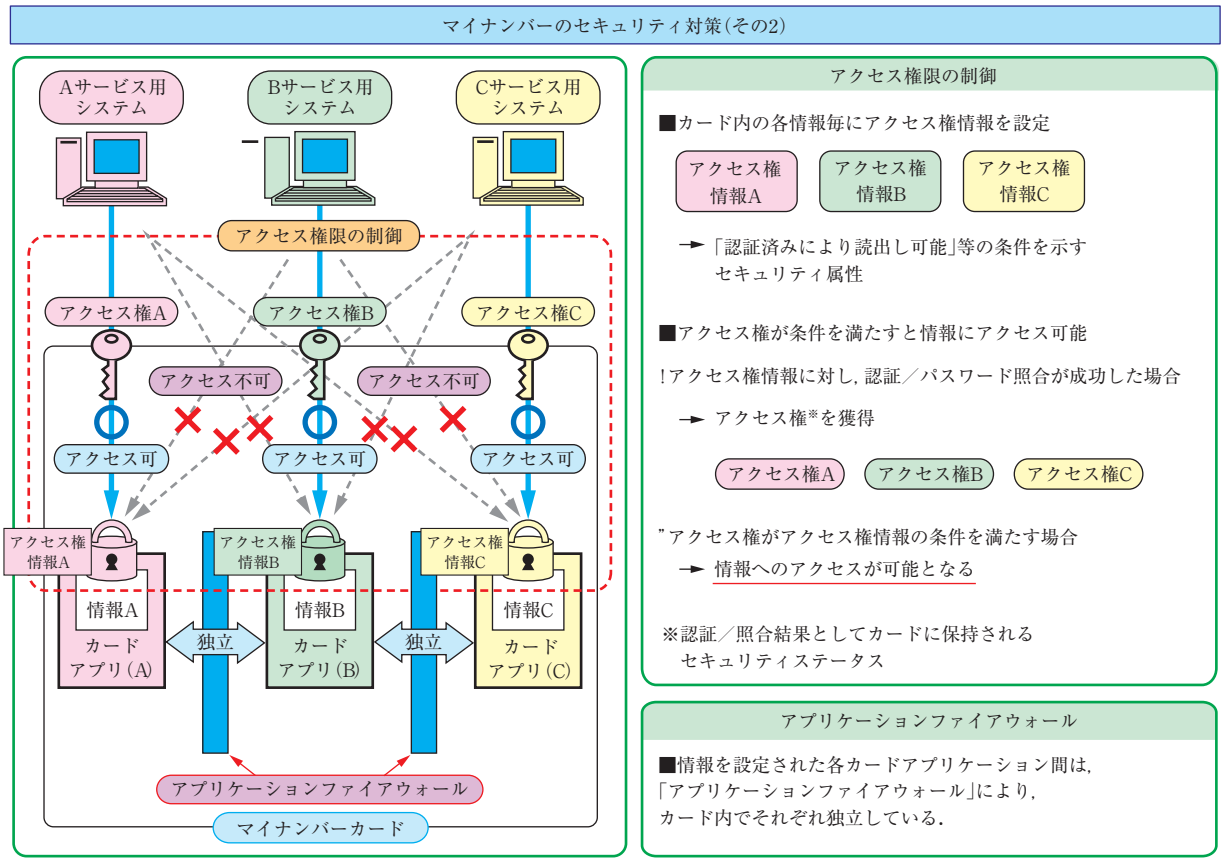


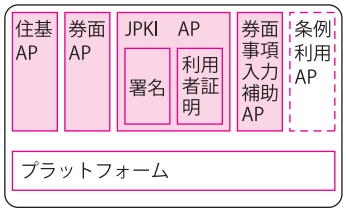
図5　マイナンバーカード内でのアクセス制御

マイナンバーカードのアプリの概要

マイナンバーカードの表面（案）

マイナンバーカードの裏面（案）

マイナンバーカードのAP構成



AP	個人番号取得，本人確認における役割	アクセスコントロール
券面AP	（目的） ・対面における券面記載情報の改ざん検知 ・対面における本人確認の証跡として画像情報の利用 （記録する情報） ・表面情報：4情報+顔写真の画像 ・裏面情報：個人番号の画像	・個人番号を利用できる者 表と裏の券面情報 ：照合番号A(個人番号12桁） ・個人番号を利用できない者 表の券面情報のみ ：照合番号B(14桁：生年月日6桁+有効期限 西暦部分4桁+セキュリティコード4桁)
JPKI-AP	（署名用） ・電子申請に利用	暗証番号（6~16桁の英数字 ）
	（利用者証明用）【新規】 ・マイナポータル等のログインに利用	暗証番号（4桁の数字）
券面事項入力補助AP（新規）	・個人番号や4情報を確認（対面・非対面）し，テキストデータとして利用することが可能 【記録・利用する情報】 ①個人番号及び4情報並びにその電子署名データ ②個人番号及びその電子署名データ ③4情報及びその電子署名データ 注）①,②については，番号法に基づく事務でのみ利用可能．	①については，暗証番号（4桁の数字） ②については，照合番号A（個人番号12桁） ※これにより，券面目視により個人番号を手入力するようなケースで正誤チェックが可能となる． ③については，照合番号B（14桁:生年月日6桁＋有効期限西暦部分4桁＋セキュリティコード4桁）
住基AP	・住民票コードを記録 ・住基ネットの事務のために住民票コードをテキストデータとして利用可能	暗証番号（4桁の数字）

※「暗証番号（4桁の数字）」については，統一の設定も可能．
ただし，生年月日やセキュリティコード等と同一は不適当．

図6　アプリごとのアクセスコントロール

イナンバーカードは，このISO/IEC15408認証を取得したものが採用されています．

その他，レーザエングレーブやマイクロ文字など，券面の偽変造を防止するためのセキュリティ加工も施されています．

マイナンバーカードの交付場所などで，カードケースが無料で配布されています．このカードケースにカードを入れると，表面に記載された性別，臓器提供意思表示欄，裏面のマイナンバーが隠れ，情報の不要な開示を防ぐようになっています（2016年4月現在）．しかし裏面のQRコードは隠れていません．実はこのQRコードはマイナンバーを符号化（画像として表現）したものなので，QRコードの読取りには注意が必要です．うっかりネット上に公開したりしないよう注意しましょう．

7．マイナンバーを用いた複数機関での情報連携の仕組み

4章で情報連携の説明をしましたが，実際のシステムは少し複雑です．図8の情報連携の概要図[8]をご覧下さい．

実は情報連携において，12桁の数字列である「マイナンバー」そのもの（番号）は，行政機関には送られません．情報保有機関の間で個人情報を連携させる際には，マイナンバーの代わりに数十桁の記号文字列である「機関別符号」が用いられます．機関別符号は，ある人の個人番号と紐付けられた，その機関のみが保持している番号です．情報提供ネットワークシステム（コアシステム）が個人番号と機関別符号を変換し，連携する二つの機関の機関別符号同士を紐付けすることで，情報連携を実現しています．番号の変換方法はコアシステム（のみ）が知っており，その対応は他の

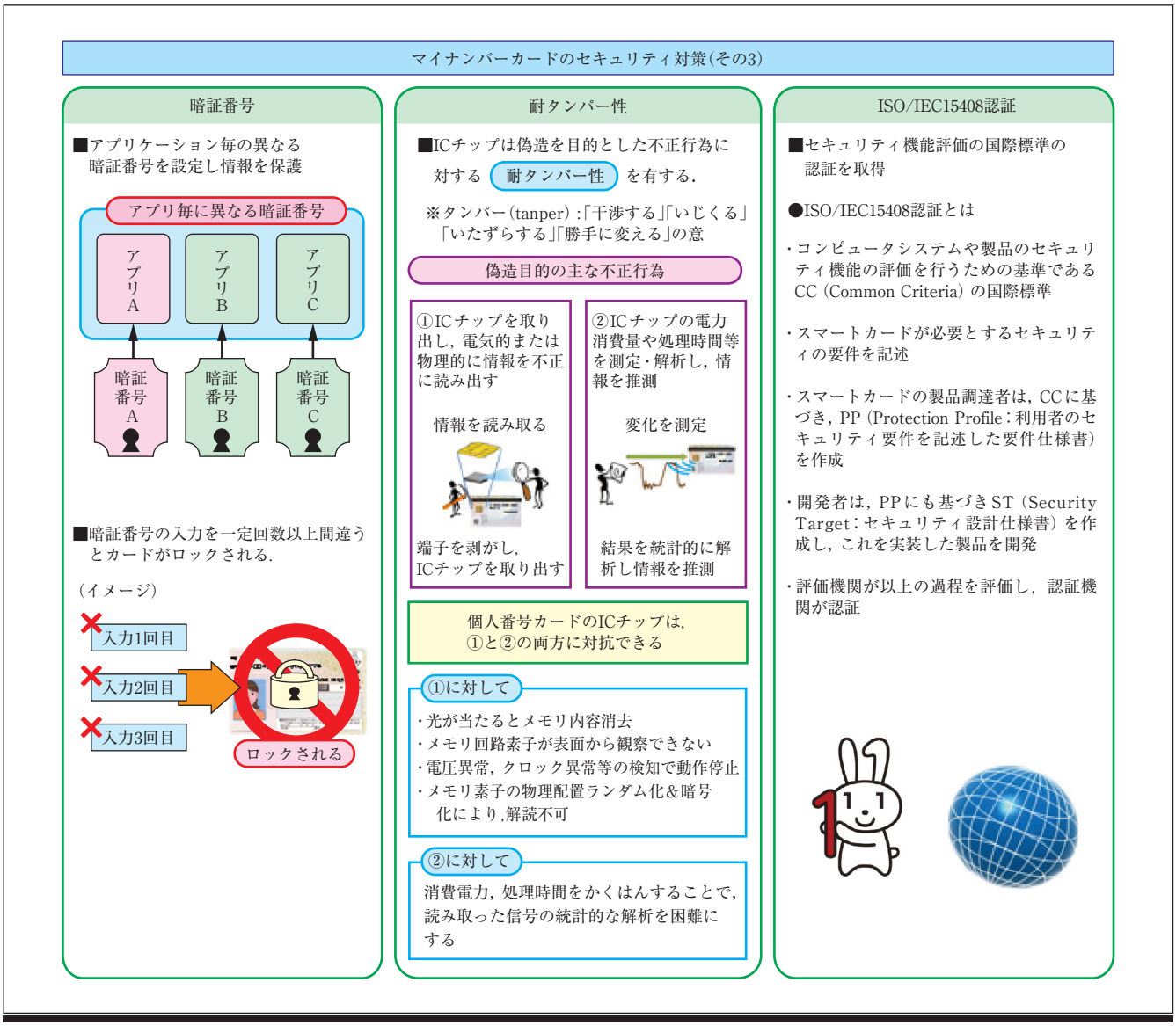


図7　マイナンバーカードの解析対策

システムでは推測できないように構成されています．図8の「地方公共団体以外の機関」(機関A)がある「個人番号」の情報を「地方公共団体」(機関B)から取得する場合，以下のようなやり取りが行われます．

(1) 機関Aは「個人番号」に対応する機関Aに割当てられた番号「機関別符号A」を，情報保持機関名「機関B」と要求する個人情報名とともにコアシステムに送信する．

(2) コアシステムは受け取った情報に基づき，「機関別符号A」を「機関別符号B」に変換し，必要とする個人情報名とともに機関Bへ送信する．

(3) 機関Bは受け取った情報に基づき，機関Aが要求した「個人番号」の個人情報を取出し，機関Aに送信する．

結果として，マイナンバーをネットワーク上に流すことなく，情報連携を実現しています．内閣官房のマイナンバー説明ページでも「マイナンバーを使った情報連携は行いません」と宣伝されています．しかしこの図をよく見ると，各機関のデータベース(既存システム)上には，当然ながらマイナンバー(図の「個人番号」)がその個人の情報と一緒に格納されています．情報提供ネットワークシステムは処理リクエスト時にマイナンバーを取得しています．図のような番号の変換と連携が必要なので中間サーバが必要になるわけですが，中間サーバにも個人の情報が連携時に保持されます．

このような複雑な番号の変換・連携システムを作ってまで，どのような不正を守ろうとしているのでしょう？結局，政府共通ネットワークやLGWAN(総合行政ネットワーク)といったプライベートなネットワークでの，情報提供ネットワークシステムと中間サーバ間の通信を守ろうとしているように見えます．通信は暗号化されており，通信者間では相手の認証も行われているので，さらに言えばこの番号変換は，例え暗号が解読されても(！)「個人番号」は漏れ

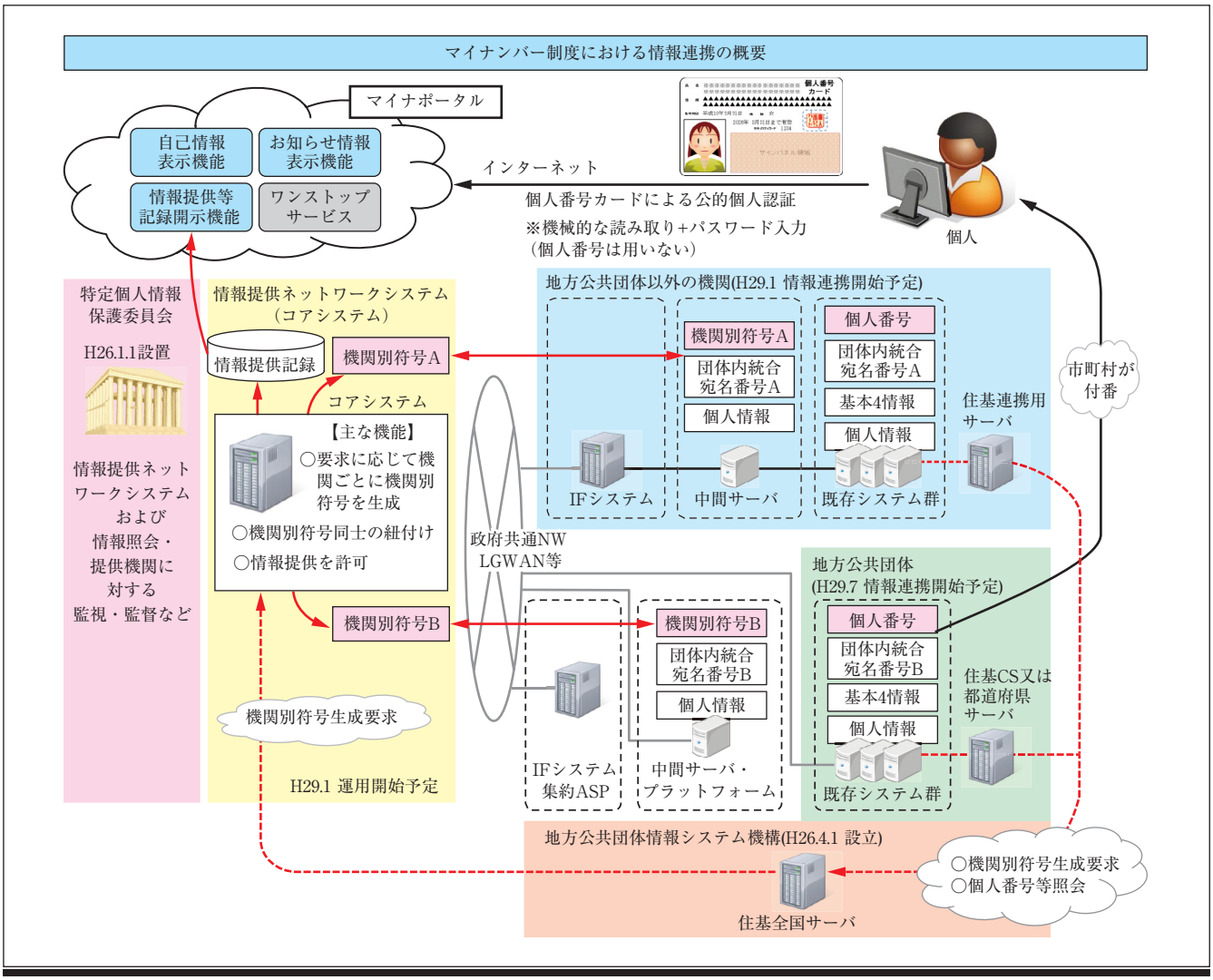


図8　マイナンバーを用いた情報連携（本資料発表後マイ・ポータルはマイナポータルと名称変更）

ないよう対策しているのだと考えられます．ただし，個人番号制度を検討した，情報連携基盤技術ワーキンググループの「中間とりまとめ」[7]では，「個人番号」を用いて行政機関の間での情報連携を行わないのは，「個人情報を一元的に管理することができる機関または主体が存在しないこと」を実現するためであると書かれています．そもそもデータ自体は分散管理されていますので，一元管理する主体は存在しません．また行政機関は上に述べたように「個人番号」を保持しているわけですから，直接「個人番号」をやり取りしても問題はありません．医療用の別の番号や民間の番号との連携する場合にだけ，番号変換機能を情報提供ネットワークとして作るなど，重い処理や重要な情報を一時的に保持する中間サーバを置かない別の形もあり得たかも知れません[9]．

8．むすび

マイナンバーの活用，マイナンバーカードの機能である公的個人認証の活用で，行政サービスの効率化やネットワークサービス化による利便性の向上が期待できます．米国や韓国，欧州での国民番号制度をしっかり分析して構築されたこともあり，情報システムとしての最適性には疑問はあるものの，妥当なレベルのセキュリティ対策がとられていると考えられます．軽減税率の還付でマイナンバーカードを活用する案や，公務員の身分証にマイナンバーカードを活用する案，マイナンバーの他の行政/民間サービスでの活用など，マイナンバーやマイナンバーカードの活用を広げる案が報道されています．マイナンバーカードを利用したテレビでの親子支援情報の表示なども検討されています[11]が，このような案を実際に導入する際には，導入前に充分なリスク分析が行われているか，新たなサービスで，これまで守られてきたセキュリティ要件やプライバシー要件が侵されていないか，しっかりチェックすることが重要であると考えます．また，その要件にあった技術を開発していくことがマイナンバーカードをより有用なものに発展させていくことに繋がると考えます．

（2016年4月12日受付）

〔文　献〕

1）マイナンバー社会保障・税番号制度，内閣官房，http://www.cas.go.jp/jp/seisaku/bangoseido/
2）マイナンバー制度とマイナンバーカード，総務省，http://www.soumu.go.jp/kojinbango_card/index.html
3）マイナンバーカード総合サイト，地方公共団体情報システム機構（J-LIS），https://www.kojinbango-card.go.jp/index.html
4）ISO/IEC 29100:2011, Information technology - Security techniques - Privacy framework，http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123（無償ダウンロード可能）
5）近藤佳大：“日本の番号制度（マイナンバー制度）の概要と国際比較：個人識別子と行政統制の視点から”，科学技術振興機構，情報管理，56，6，pp.344-354（2013），https://www.jstage.jst.go.jp/article/johokanri/56/6/56_344/_pdf
6）第1部第4節（2）諸外国における国民ID制度を活用した事例，平成24年版情報通信白書，総務省（2013），http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc114920.html
7）情報連携基盤技術ワーキンググループ中間とりまとめ，情報連携基盤技術ワーキンググループ，内閣官房（2011），http://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/cyukan/
8）マイナンバー社会保障・税番号制度概要資料，内閣官房，内閣府（2015），http://www.cas.go.jp/jp/seisaku/bangoseido/download/summary_zentai.pdf
9）高木浩光，山口利恵，渡邊創：“国家による個人識別番号とその利用システムのあり方 ～プライバシーの観点から～”，コンピュータセキュリティ研究会（CSEC），情報処理学会（2013）
10）（教えて！続マイナンバー：7）占いに使うと違法？，朝日新聞，2016年1月15日，http://www.asahi.com/articles/DA3S12159699.html
11）マイナンバー制度のマイナンバーカードを利用したテレビでの親子支援情報の表示サービスの開始について，http://www.jdserve.co.jp/news/2016/196/

渡邊（わたなべ）　創（はじめ）　1994年，大阪大学大学院基礎工学研究科博士後期課程中退．同年，奈良先端科学技術大学院大学助手．1999年より，国立研究開発法人産業技術総合研究所（2000年3月まで電子技術総合研究所）．現在，情報技術研究部門上級主任研究員．暗号と情報セキュリティ，プライバシー技術に関する研究に従事．CRYPTREC暗号技術検討会構成員（総務省・経済産業省）等を歴任．博士（工学）．

《講座》

映像情報メディア関連のセキュリティ［全12回］

閉講にあたって

編集幹事一同

『「情報のセキュリティって必要だよね．でも，どうなっているのかわからないから，業者やお店で薦められたものを使っておこう」　そんな経験ありませんでしょうか．そして，「自分で判断できれば，どんな対策をすればよいか自分で選ぶけど・・・(;-_-)」』

というみなさまの思いにこたえるべく2015年1月に始まりました「映像情報メディア関連のセキュリティ［全12回］」が，今回で閉講となります．いかがでしたでしょうか．

編集幹事としても，ネット上での情報のやり取りの際に注意を払い，パスワードマネジメントも気にかけるなど，日々の生活の中でセキュリティを意識している部類の人間だと自負していました．しかし，その仕組みの詳細や安全性を担保できる理由などについては調べることすらしていませんでした．

この全12回のセキュリティ講座では，それぞれの回が難しいテーマを含みながら，しかし実は身近なもので，とっつきにくくなりがちな内容を興味深く読めるように工夫されており，われわれもさまざまな勉強をさせていただいたという感想を抱いております．

われわれ編集サイドとしても，さまざまな専門用語が新出する中，幅広い読者層にできるだけわかり易く，かつ，具体的にどのように役に立つのかということをお伝えしたいという気持ちで携わって参りました．執筆者の先生方には大変お忙しい中，時には海外出張先からもご対応いただき深く感謝しております．おかげさまで先生方の熱い心を込めた原稿に対し，読者の方々からさまざまなコメントをいただき，執筆者と編集者・読者が繋がっていることを強く実感いたしました．

セキュリティの重要性は今後ますます大きくなることと思われます．この講座が読者の皆様のお役に立ち，「どんな対策をすればよいか，自分で選ぶことできるようになったよ（^^;）」と言っていただける一助になれば幸いに思います．