01 情報セキュリティ

コンピュータが扱うデータや情報を他者から守ることを情報セキュリティといいます。ただ一口にデータを守るといっても具体的にどんなデータをどうやって守るのでしょうか。そのためのセオリーとその中での暗号や認証の立ち位置を理解しましょう。

情報セキュリティの三要素

情報セキュリティ（単にセキュリティとも）がどのようなものか、ネットショッピングを例に取ります。

お客はショップのサイトにアクセスして名前や住所を登録し、商品の購入手続きをします。ショップはお客の情報に基づいて商品の手配をします。次回の購入時に便利なようにお客の情報をサーバに保存することもあります。

■ ネットショッピング

まず自分がどこでどんな商品を買ったかという情報は他人に知られたくありません。またショップで働く人なら誰でも購買情報を見られるというのも不安です。ショップ内でも一部の限定された人しか情報にアクセスできないようになっていてほしいです。この性質を**機密性**（confidentiality）といいます。

次に機密性があったとしても、購入した品物の値段が勝手に書き換えられて過大な請求が来たり、届け先を書き換えられて商品が来なかったりするのも困ります。情報が改竄（かいざん）されたり、消えたりしないことが求められます。この性質を**完全性**（integrity）といいます。

最後に自分の好きなときに買い物ができたり、購入履歴を見られたりできるよう、システムは常に正常に動作していてほしいです。万一システムが破損し

一番単純な攻撃は全パターンのパスワードを順次試すブルートフォース（Brute-force）攻撃です。ただこの攻撃は時間がかかるため、「12345678」とか「password」といったよく使われるパスワードの一覧（リスト）を入手しておき、そのリストを順次試すと成功率が上がります。**辞書攻撃**といいます。

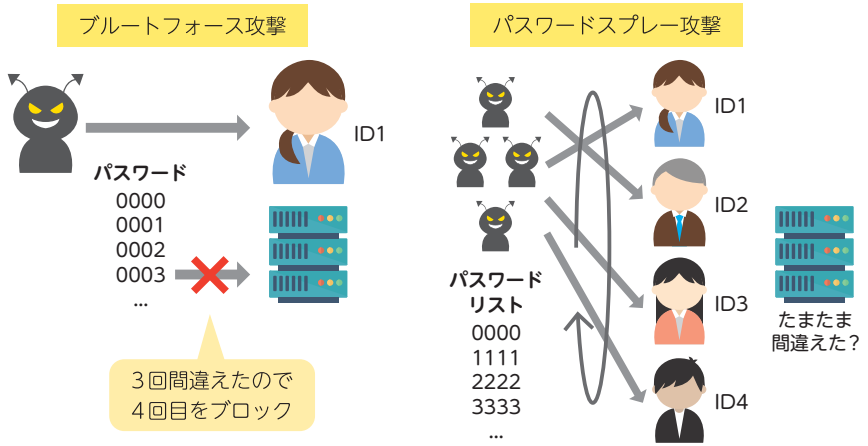
これらの攻撃に対する対策は、ATMと同じく、あるユーザが複数回連続してパスワードを間違えたら、そのユーザを一時的にロックすることです。ユーザが弱いパスワードを登録しようとすると警告を出すのも有用です。

あるユーザ（のID）を固定してパスワードを順に試すのが**ブルートフォース攻撃**ですが、逆にパスワードを固定してIDを順に試す攻撃があります。**リバースブルートフォース攻撃**といいます。

2019年にオーストラリアのサイバーセキュリティセンターACSC（Australian Cyber Security Centre）が大規模な**パスワードスプレー攻撃**がなされているとの警告を出しました[12]。パスワードスプレー（password spray）とは、攻撃者が多数のユーザIDのリストを持ち、各IDに対して同じパスワードを順次試す方法です。IDが一巡したらパスワードリストの次のパスワードを試します。リバースブルートフォース攻撃の一種です。攻撃者は攻撃を気づかれにくくするために、時間を空けたり、複数の場所からログインを試みたりします。

この方法は、あるユーザに対して連続的に攻撃するわけではないので攻撃検知やロック対策がとりづらいです。後述する多要素認証を導入するとよいです。

■ ブルートフォース攻撃とパスワードスプレー攻撃



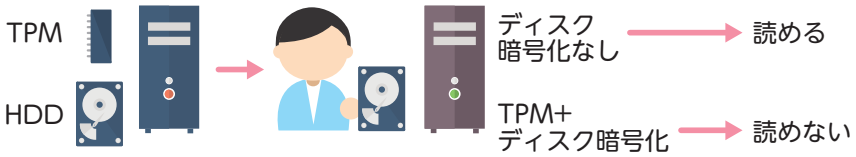
16 ディスクの暗号化

パソコンやスマートフォンに内蔵されているHDDやSSDは暗号化されていないと抜き出して容易に中身が見えます。そのため近年のパソコンやスマートフォンは紛失や盗難に備えてディスク全体を暗号化する仕組みを導入しています。

TPM

TPM（Trusted Platform Module）とはパソコンやスマートフォンに組み込まれているセキュリティ専用チップです。TPMを使うとチップ内で暗号化や復号、署名の生成や検証ができます。OSの起動時にシステムが改竄されていないかの検証もできます。チップの内部は解析されにくいように設計され、無理に取り出して解析しようとすると保存データを消去する**耐タンパー性**を持ちます。TPMの仕様は**TCG**（Trusted Computing Group）が定めていてTPM 2.0はISO/IEC 11889:2015として標準規格になっています[34]。

■ ディスク暗号化



HDDやSSDなどのディスクに保存されているデータを暗号化する場合、ファイル単位で暗号化するとファイルを開くたびにパスワードを入力することになり利便性が劣ります。そこで近年はHDDやSSDを丸ごと暗号化するディスク暗号化がOSの標準機能として提供されています。ディスク暗号化に使う秘密鍵をTPM内部に保存して管理すると、そのマシンに正しくログインしたときしか秘密鍵を取り出せません。そのため他人が暗号化されたディスクを取り出

20 公開鍵暗号

共通鍵暗号の秘密鍵を共有する方法として、鍵共有の他に公開鍵暗号があります。鍵共有は一度互いにデータを交換して秘密鍵を共有してから共通鍵暗号を使いますが、公開鍵暗号は、公開鍵をもらったらすぐ暗号化できる点が違います。

公開鍵暗号の概念

物理的な錠に対する鍵は、通常開けるときも閉めるときも同じ鍵を使います。共通鍵暗号や古典的な暗号はその類似の概念で、暗号化と復号で同じ秘密鍵を使いました。**公開鍵暗号**では暗号化するときと復号するときに異なる鍵を使うのがポイントです。暗号化用の鍵は誰に知られてもよい**公開鍵**、復号用の鍵は自分しか知らない秘密鍵といいます。

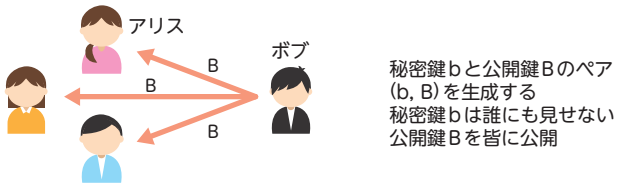
秘密鍵と公開鍵は密接な関係があり、大抵の公開鍵暗号は秘密鍵から公開鍵を作ります。しかし逆に公開鍵から秘密鍵は作れません。そのため公開鍵は他人に知られても問題なく、共通鍵暗号の秘密鍵をこっそり相手に渡すような苦労がありません。この点が共通鍵暗号との一番の違いです。

公開鍵暗号は、**鍵生成**・暗号化・復号の3個のアルゴリズムからなり、アリスがボブに秘密の情報を送りたいときは次のようにします。

鍵生成

ボブは秘密鍵bと公開鍵Bのペア(b, B)を生成して公開鍵を皆に公開します。アリスはその公開鍵Bを受け取ります。この操作は一度だけ行えばよいです。

■ 鍵生成



23 楕円曲線暗号

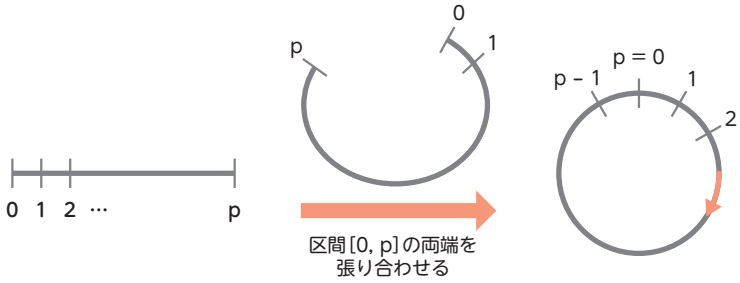
楕円曲線暗号（elliptic curve cryptography）とは楕円曲線と呼ばれる数学的な対象物を利用した暗号技術全般を指します。楕円曲線を用いた公開鍵暗号や鍵共有・署名などがあります。短い鍵長で高い安全性が得られるため普及が進んでいます。

楕円曲線

楕円曲線EC（Elliptic Curve）は、これで一つの専門用語です。楕円の弧の長さを求める研究が端緒なので名前に「楕円」が入っています。しかし楕円曲線は「楕円」でもなければ「曲線」でもなく、後述するようにどちらかというと「曲面」です。

楕円曲線の解説の前に、少しDH鍵共有の有限体をおさらいしましょう。有限体では整数を素数pで割った余りを考えていました。pで割るというのは0以上p以下の線分の両端を貼り合わせたものとみなせます。線分を曲げて貼り合わせると円になります。

■ 円周の世界



この世界で、ある数xのベキ乗x, x^2, x^3, …は円周をぐるぐると移動します。

27 SHA-1の衝突

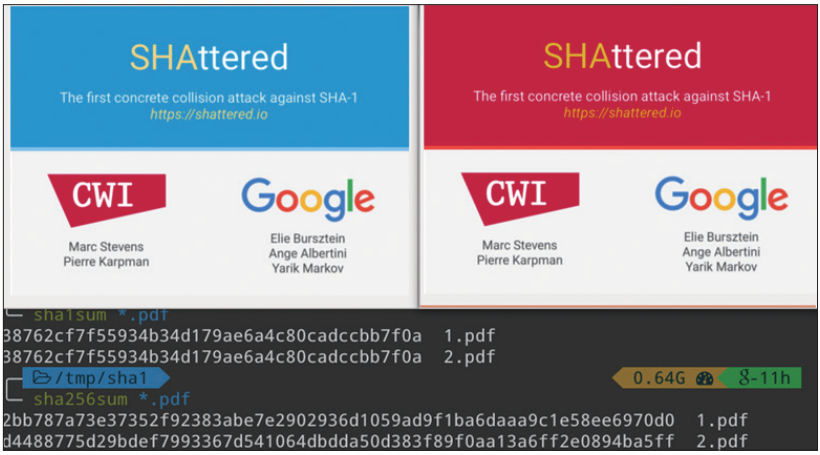
2017年、オランダ国立情報数学研究所CWI（Centrum Wiskunde & Informatica）とGoogleのチームは SHA-1の衝突困難性を破り、ファイルのSHA-1の値は同じなのに、異なる内容を表示する2個のPDFを作成しました。

SHA-1への攻撃の歴史

SHA-1のハッシュ値は160ビットなので理想的には80ビット安全性のはずですが2005年に提案された攻撃法により63ビットまで下がりました。国家レベルの安全性は80ビットでも不十分とされるので、これでは全然安全とはいえません。とはいえ、理論的に分かっていることと実際に破ることは別です。

当初の想定より時間が掛かりましたが、2017年CWIとGoogleのグループが6500年分の単一CPUと110年分の単一GPUの計算リソースを使ってSHA-1の衝突困難性を破りました[62]。なお、その後も攻撃方法の改良は進み、2020年のガイタン（Gaëtan）とトーマス（Thomas）は900個のNVIDIAのGeForce GTX 1060を2カ月動かして4万5千ドルで攻撃しました[63]。

■ https://shattered.io/ の画像を引用



32 ブロックチェーンとビットコイン

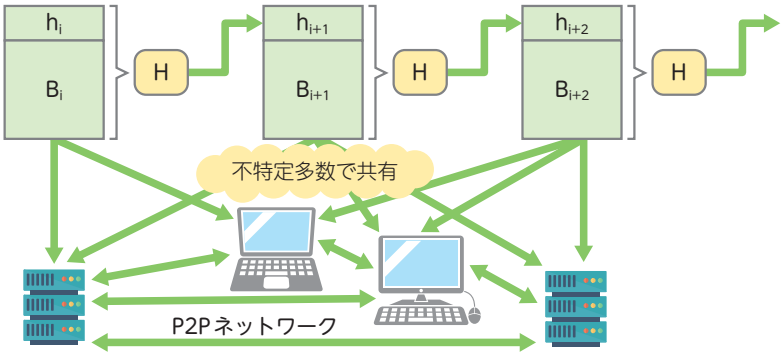
2009年に提案された暗号資産であるビットコインは瞬く間に大きな市場規模となりました。ビットコインの基幹技術であるブロックチェーンは、暗号資産だけでなく様々な応用が考えられています。

ブロックチェーン

タイムスタンプ（sec.31）で紹介したリンクトークン生成型のタイムスタンプは、時刻情報を衝突耐性のあるハッシュ関数Hによるハッシュ値の連鎖（チェーン）を作ることでデータの改竄耐性を得る仕組みでした。この特長は時刻情報だけでなくどんなデータに対しても適用できます。

ブロックチェーンとは、あるデータの固まり（ブロックB_i）と、そのハッシュ値h_{i+1}を次のブロックB_{i+1}につなげることでブロックに含まれるデータの改竄耐性を持たせ、更にそのチェーンを**P2Pネットワーク**で管理する仕組みです。P2P（Peer to Peer）ネットワークとは、ネットワーク全体を管理する特定の管理者が存在せず、不特定多数の主体が所有するコンピュータが互いに通信する形態を指します。管理者がいなく、非中央集権的であることを強調するためにパブリックブロックチェーンということがあります。

■ ブロックチェーン



38 認証付き暗号

認証付き暗号AEAD（Authenticated Encryption with Associated Data）とは暗号化と認証を同時に満たす暗号方式です。認証暗号AEともいいます。

秘匿性と完全性

共通鍵暗号はデータを隠す秘匿性はありますが、データが正しい（壊れていない、あるいは改竄されていない）ことを示す完全性はありませんでした（p.057, p.100）。逆にMACはデータの完全性を与えますが、秘匿性はありませんでした（p.161）。

そこで従来は共通鍵暗号とMACを組み合わせることでデータの秘匿性と完全性を満たすようにしていました。しかし、組み合わせ方や実装方法によって安全性が損なわれる例が相次いで報告されます。それに対してTLS 1.3で採用された**認証付き暗号 AEAD**は最初から秘匿性と完全性を両立するように注意深く設計されています。

■ 暗号技術の秘匿性と完全性

暗号技術＼性質	秘匿性	完全性
共通鍵暗号	ある	無い
MAC	無い	ある
AEAD	ある	ある

そのためAEADは共通鍵暗号とMACを組み合わせた場合に比べてより安全です。また性能がよいことも多いです。TLS 1.3ではAEADが必須となり、従来使われていた暗号化モード（sec.15）のうちCBCモードなどが削除されました。

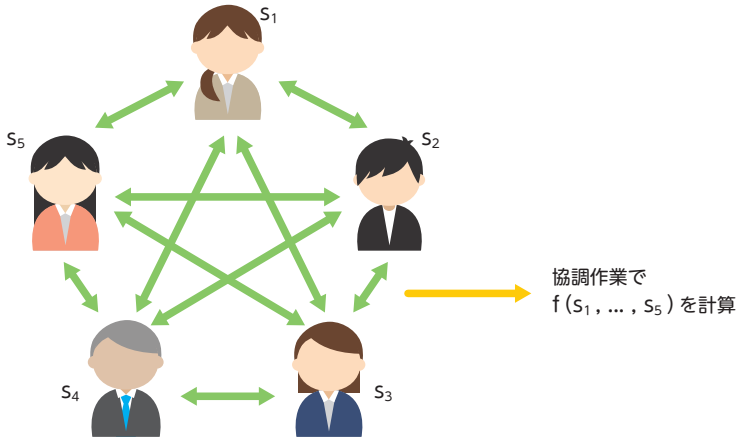
46 秘密計算

秘密計算とはデータを秘匿したまま計算する技術の総称です。近年、複数人で各自の秘密情報を秘匿したまま皆で計算するマルチパーティ計算が注目されています。

MPC

複数人で協調して計算することをマルチパーティ計算**MPC**（Multi-Party Computation）といいます。MPCはn人の参加者が、それぞれ秘密の値s_1, s_2, ..., s_nを持ち寄り、互いに自分の秘密の値を見せることなく、ある関数$f(x_1, ..., x_n)$の値$s=f(s_1, ..., s_n)$を計算するプロトコルです。

■ MPC



たとえば秘密の値が各自の資産で関数fが最大値を求める関数だと、MPCを使って一番お金持ちの資産が分かります。誰が一番お金持ちなのか、2番目以降の人の資産はいくらか、といった情報は誰も得られません。同様に、互いに秘密の値を教えることなく全員の資産の平均値や分散などの計算もできます。

48 量子コンピュータ

現在使われているコンピュータは電流のオン・オフによる2進数の演算を基本としています。それに対して量子コンピュータは量子力学で記述される現象を利用した全く新しいコンピュータで、その発展は暗号技術に対して重大な影響を与えます。

量子ビットと観測

量子とは量子力学で扱われる概念で、粒子と波の両方の性質を持つ物質や状態を指します。量子は粒子のように1個、2個と数えられます。通常の粒子は同じ場所に複数存在することはできませんが、量子は波のように複数の状態が重なり合って存在できます。**量子コンピュータ**は量子の重ね合わせを利用して計算するコンピュータです。

従来の情報の最小単位は、ある状態が0か1のどちらかを示す1ビットでした。それに対して、量子の状態を表す最小単位を量子ビットといいます。量子ビットは0の状態「$|0\rangle$」と1の状態「$|1\rangle$」が重なっていて、式としては$|\psi\rangle = a|0\rangle + b|1\rangle$と表します。ここで$|\psi\rangle$は量子ビットの状態を表し、aとbは$|a|^2 + |b|^2 = 1$となる複素数です。$|\psi\rangle$を$(|0\rangle, |1\rangle)$に従って観測すると確率$|a|^2$で$|0\rangle$に、確率$|b|^2$で$|1\rangle$になります。

aとbが複素数だと分かりにくいので実数に制限し、$|0\rangle$を(1, 0)、$|1\rangle$を(0, 1)という2次元の単位ベクトルとすると$|\psi\rangle$は半径1の円周のどこかを指します。

■ 量子ビットと観測