漏洩に強いセキュリティ理論

東京理科大学 創域理工学部 情報計算科学科 教授 入山（いりやま） 聖史（さとし）

「クレジットカードを紛失！　すぐに以下の電話番号へお知らせください.」暮らしの中でどうしても起こってしまうトラブルです．何かをなくしたとき，慌てずにサービス停止ができるような仕組みが情報セキュリティにもあると便利ですね．本稿では，どうしても起きてしまうデジタル災害（内部漏洩など大規模な情報漏洩）に備えた，情報漏洩に強いセキュリティをどうやって実現するかについてお話しようと思います．

皆さんは他人に見られたくない，盗られたくないものはどうやってしまっておきますか．机の引き出しの奥や本棚の裏，鍵のかかる箱の中など，とにかくすぐには見つからないようにするでしょう．このとき，しまう物を平文，しまう方法を暗号化と呼びます【図1】．なるべく他の人にわからない方法で，実際に箱に入れて鍵をかけるのもいいですね．厳重に守る，鍵を誰にも渡さない，これらは情報セキュリティでも同じ考えで，実際には複雑なコンピュータプログラムや長い鍵で情報は守られています（この特集のほかのお話を参照）．

次に，他の人に隠したい物が渡ってしまったとき，例えば日記を友達に見られてしまった！　というような場面を考えます．友達の手に渡ってしまった日記には，私たちの分かる言葉で書かれていて，友達はすべてを読めてしまいます．このとき，クレジットカードをなくした時と同じように，「ここに電話すれば日記のサービスが終了して，もう友達は読めなくなります」ということになれば少し安心です．その仕組みを作るにはどうすればよいでしょうか【図2】．

ここでの前提は，友達はいつでもあなたの暗号化を破ることができて日記を読めてしまう，ということにします．もはや友達とは呼べない気もしますが，世の中にはいろんな友達がいてもいいのです．さて，どうやって日記を隠してもダメそうなので，日記の中身を工夫することにしましょう．

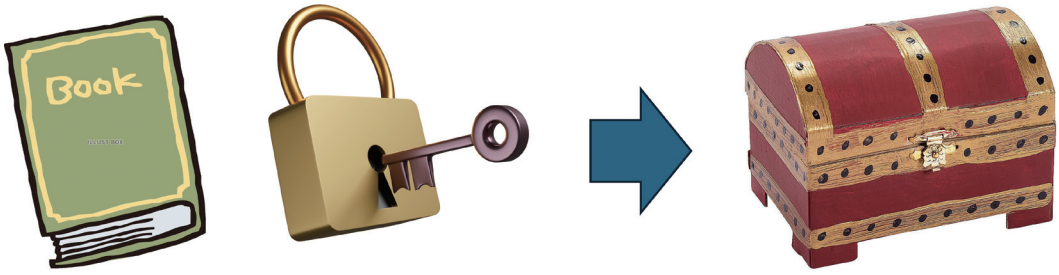
情報を隠すコツは今から100年以上前の1919年，バーナムにより発明され，特許をとられました[1]．いまでもワンタイム暗号として応用され，アカウント情報の設定や高額な売買の際に使われています．これはコイントスを使う方法で，平文は簡単のため0か1の2種類で作られる文字列とします．暗号化では平文の1文字ずつにコイントスを行って，

表が出た　→　なにもしない

裏が出た　→　平文が0なら1，1なら0にする

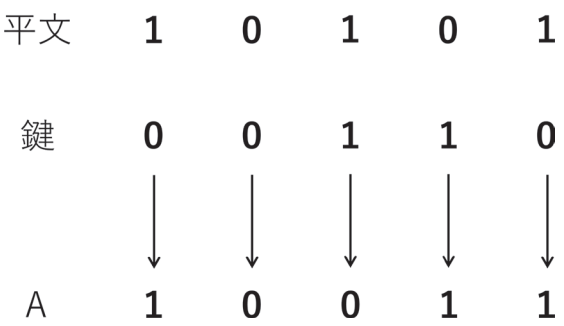
という作業をします．コイントスの結果は保存して，これを鍵とよびます．例えば平文が「10101」として，コイントスの結果が鍵「表表裏裏表」とします．表，裏だと見にくいので表を0，裏を1とします．つまり鍵「表表裏裏表」は鍵「00110」と表します．平文をさっきのルールで作業すると，裏の時だけ平文の0，1をひっくり返すので，平文「10101」は鍵「00110」で「10011」となります（左から1文字ずつ作業します）．出来上がったものをAとします【図3】．

さて，この作業で状況はどう変わったでしょうか．平文は鍵とAに分解されました．次に，ここが重要な点です．鍵とAの管理のため，新たに犬を2匹飼うことにしました[2]．それぞれ犬Dと犬Sとします．

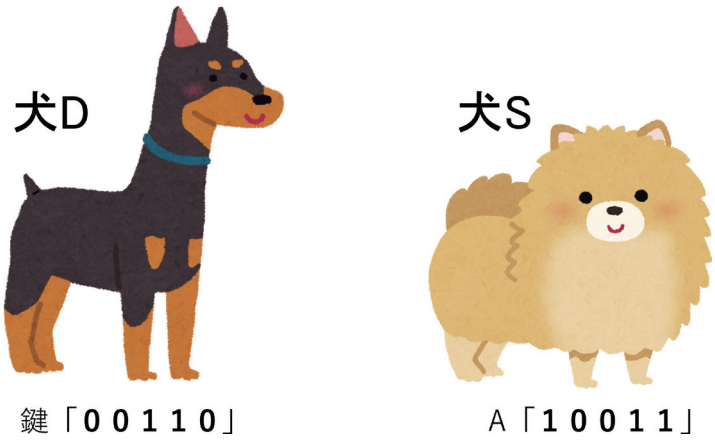


【図1】平文と暗号化

【図 2】情報漏洩の対策



【図 3】平文と鍵から A ができる



【図 4】吠える犬 D と賢い犬 S

犬 D は鍵を持ち，外から来るデータに鍵を使って計算して，答えが全部 0 になったら OK の意味で明るく吠えて（ワン！），答えに 1 ヵ所でも 1 が含まれていたら NG の意味で唸ります（ウー）．怖いですね．犬 S はデータ A を持ち，外から来るデータと A との違いを計算，すなわち 1 文字ずつ同じかどうかをチェックし，同じなら 0，違うなら 1 を返してきます．例えば「00011」と「10110」の違いは，「10101」となります．左から 1 文字ずつ確かめるとわかります．このとき結果には 1 が含まれているので NG で唸られることになります．ウー．

さて，いまの状況を整理すると，あなたの平文すなわち日記は鍵と A に分けられて，鍵は犬 D に，A は犬 S に預けられました【図 4】．さあ，もとの日記は燃やしてしまいましょう．するとあなたにできることは，

(1) 日記の内容を思い出して犬 S に聞かせ，答えを持っておく．これを B とします．
(2) B を犬 D に聞かせて，それが鍵と同じかどうか確かめる．同じなら犬 D は明るく吠えて，違うなら唸られます．

あなたは日記の内容を覚えているので，平文「10101」を犬 S に聞かせます．犬 S は，A「10011」と平文「10101」を比較して B「00110」を答えます．次に犬 D に B「00110」を聞かせると，それは犬 D の持つ鍵「00110」と同じなので，犬 D は明るく吠えてくれます．ワン．おめでとうございます．ここでのポイントは犬 S には必ず平文と同じ「10101」を聞かせる必要があることです．ここで間違ってしまうと必ず犬 D に唸られます．

日記を更新したいときは，同じように鍵と A に分けてから 2 匹の犬の情報を新しいものに更新します．

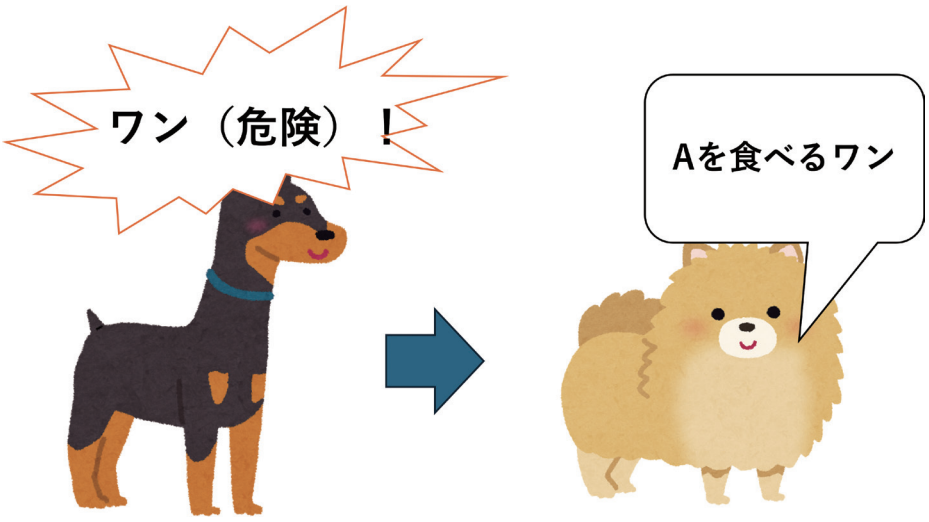
さてこのとき，日記を読みたい友達はどうするでしょう．

(1) 日記の内容を想像して犬 S に聞かせ，答えを持っておく．これを C とします．
(2) C を犬 D に聞かせて，もとの内容と同じかどうか確かめる．

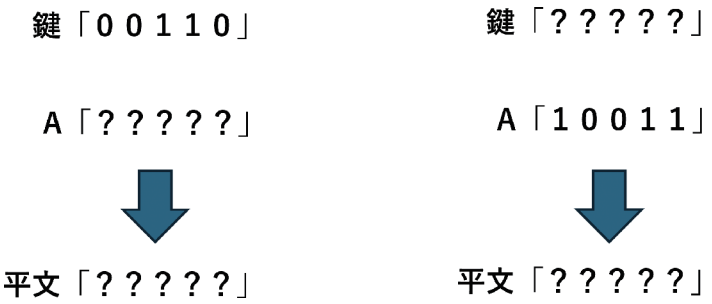
友達は勝手に想像した内容で犬 D に聞くので，日記がある程度長いものであれば全く正解することはありません．友達は正解にたどり着くため何回も作業をくり返します．するとあなたは犬の恐ろしい唸り声を何回も聞くことになり（ウーウーウー），友達が日記を読みたがっていることを知ります．そこで，鍵と A を新しいものに変えて，犬たちにも今度友達がきても無視してねと注意して一安心です．あなたの秘密は守られました．

友達はこれに懲りて，今度は犬 S と犬 D から直接情報を盗もうとします．鍵と A があればその違いを計算することで，もとの平文に戻すことができるのでこれは名案です．早速友達は犬小屋へ向かい，情報を取ろうとします．

ここで犬たちに「盗まれたら吠える！　片方の吠え声が聞こえたら自分の情報を食べちゃう！」という芸を仕込んでおきます．これは，だれかが盗もうとやっ



【図 5】危険なときは情報を破棄



【図 6】鍵と A，どちらか片方では役に立たない

てきたときに相手に知らせ，またどちらかが盗難にあったら情報は破棄する，という仕組みです．重要なポイントです．そうすることで鍵と A は同じタイミングで持ち去られることはなくなるというわけです【図 5】．また，友達は片方だけ盗むことができたとします．このとき何ができるでしょうか．

(1) 犬 D のもつ鍵「00110」が盗まれたとき，犬 S は A を破棄しているので，平文の手掛かりはなくなる．

(2) 犬 S の持つ A「10011」が盗まれたとき，犬 D は鍵を破棄しているので，平文の手掛かりはなくなる．

つまり，鍵や A が単体で盗まれたなら友達は何もできなくなり，あなたには鍵と A を新しいものに更新する十分な時間があります【図 6】．

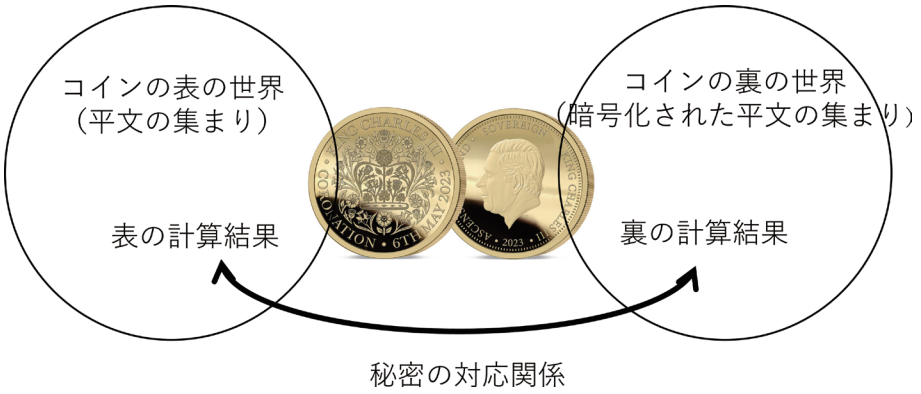
まとめると，もとの平文を鍵と A に分け，2 匹の犬たちに分けて持たせる．犬たちには盗難されたときにそれを知らせ，自分の情報を破棄する芸を仕込む．鍵と A が同時に揃わないようにする．以上のことで，盗まれた情報に意味をなくすことができるというわけです．

一番初めに考えた，日記をそのまま隠す方法と何が違うでしょうか．日記を隠す方法では，友達が探し当てるまでの時間が十分長くなるように工夫します．もちろん友達も最新テクノロジーを駆使して探し当ててくるので，イタチごっこになってしまいます．たとえ盗まれたときに鳴る警報をつけていても，一旦盗まれた場合は日記を読み放題になります．また，いくら日記を鍵と A に分けても，犬たちに芸を仕込んでおかなくては，ただの時間稼ぎにしかなりません．

今回説明した方法では，盗まれた場合にどうするかを中心に考えています．私たちはスマホなどを通じて様々なサービスに囲まれて過ごしており，あたかも自分がインターネットの中を飛び回って買い物をしているようにも思えます．このとき，その飛び回っているあなたの実体とは何でしょうか．それは，あなたの情報から生成された平文です．これをデジタルアイデンティティ（DI）とよびます．この DI はインターネットの世界のあなたであり，サービスの提供者，すなわちネット上のお店やアトラクションはこの DI とアカウントを結びつけます．つまり，サービスログインのためのログイン id と，あなたの DI である，あなたが自分で設定したパスワードや指紋，顔情報を結びつけて，あなたがサービスを利用していることを認識します．また，メルカリなどのオークションアプリでは，あなたの本人確認のために運転免許証やパスポートなどを DI として考えます．あなたの実体である DI の情報は決して盗まれないようにすることがポイントです．つまり，パスワードを知られないこと，指紋や顔情報，運転免許証などを盗まれないことが重要になります．

ここで，「紛失した！」というときにどうするかという最初の問題に戻ってみましょう．私たちは人間な

ので，うっかりしていたり間違いを起こすことは十分あります．また内部漏洩では企業の内部の情報を持って行ってしまうということも起こります．このとき，今回お話したように，「情報を分けておく」，「情報が盗まれたら破棄する」とすることで，盗まれた情報に意味をなくし，漏洩を発見した場合に速やかに更新することで，もとの平文に戻されるのを防ぐことができると考えます．このような漏洩に強い仕組みづくりは今後ますます必要となってくるでしょう．



【図 7】 平文の計算と暗号化された計算に秘密の対応関係をもたせる

さらに，今回の方法を応用した，いろいろなサービスとの連携を考えてみます．あなたはゲーム 1 とオークション 2，SNS3 を使うとします．それぞれログイン id とパスワードはブラウザやスマホに保存されているので，あなたは意識することなくサービスを利用できます．

さてここで，あなたのログイン id やパスワードが盗まれたとします．ゲーム 1 であなたの大切なキャラクターが勝手に操作されたり，オークションサイト 2 で無断売買されたり，SNS3 では勝手に炎上させられたりするかもしれません．

こういった場合に，今回説明した方法が組み込まれていたらどうでしょうか．つまり，あなたのログインとは別にあなたの本人認証が行われ，もしその認証が通らない場合にはサービスの使用が中止されるものとします．サービス使用時のログインは，あなたの id とパスワードさえ知っていればあなたの友達や全くの他人でも可能です．そこに，あなたが本人であることを示すため，例えば指紋や顔認証をいろいろなタイミングで追加すれば，あなた以外にアプリを使用することができなくなります．

それぞれのサービスに対するログイン id やパスワードは情報漏洩に弱く，一旦漏洩したらそれを悪用される恐れがあります．一般的にデジタル災害の被害はこのような漏洩が大規模におこり，それを使って個人の他の情報にアクセスされ，様々に連鎖して情報が盗まれてしまうことにより引き起こされます．

今回説明した方法では，たとえログイン id とパスワードが盗まれた場合でも，本人の認証は完全に別で行われるため，被害は最小限に抑えられる可能性があります．サービスへのログインと本人認証を完全に独立させた仕組みづくりが情報漏洩の被害を減らす方法の一つです．

日々様々な新しいサービスが発表されています．それぞれ新しいアカウント作成を求められ，その都度，我々の DI を知られてしまったら，情報漏洩のリスクは高まるばかりとなります．こういった状況に対応するためにはログインと本人認証を別にし，どのように情報を守るかと同時に漏洩した場合の対処方法にも考えを巡らせる必要があると思います．

今回のお話では，重要な情報が盗まれたときに被害を最小にするにはどういった仕組みを考えればよいかを説明しました．我々のネット空間における分身であるデジタルアイデンティティ（DI）は，もちろん漏洩してはいけない情報で，厳重に守る必要があると同時に，万が一漏洩した場合に被害を最小限に抑える必要もあります．さらに，情報は守るだけでなく便利に活用して価値が生まれるものでもあります．秘密にすることと活用することは，一見反対のことのように見えて実はコインの表裏のような関係で，ひっくり返されることをコントロールできれば，情報を隠したまま利用することもできると考えます**【図 7】**．

昨日どこに行ったか，今日何を買ったかなどの自分の情報がどのように守られ，または活用されているのか，不正に使われていないかなど，身近なところから調べてみると色々な IT 技術に触れることができると思います．今回のお話で少しでも情報セキュリティの面白さが伝われば幸いです．

[参考文献]

1）Vernam, G. S. “Secret signaling system. 1919.” S. Patent 131071 (1919).

2）M. Kihara, S. Iriyama, Cryptography, 3（3）, 19. https://doi.org/10.3390/cryptography3030019