ダメなセキュリティ対策とその悪影響

名古屋大学 情報基盤センター
情報基盤ネットワーク研究部門
嶋田 創

概要

- 一般的な視点からのダメなセキュリティ対策とその悪影響
- ダメなセキュリティ対策とその悪影響の事例
- 良いセキュリティ対策の事例
- 個人的に「理解不足でダメなセキュリティ対策」になりそうで気になる案件

  注: この項目は特に主観が強く入るとともに、技術動向で変化する可能性が高いです

ダメなセキュリティ対策による悪影響の基本

- 英語ではsecurity theater(セキュリティ劇場)なる用語があるらしい[1]
  - 「セキュリティ対策やっています」をアピールするために、意味がほぼ無いセキュリティ対策もどきを実施すること
  - 個人的には「セキュリティ茶番」と呼んでいる
- 弊害
  - 効果が無く安全ではないのに、関係者に安心感を与えてしまう
    - 根拠の無い安心感は事故のもと
  - 本来なら効果的なセキュリティ向上にお金が使われるべきなのに、効果がないものにお金が注ぎ込まれてしまう
  - 人の手間は増える(作業時間コストがかかる)のに、セキュリティ的には意味は無い

[1] https://en.wikipedia.org/wiki/Security_theater

ダメなセキュリティ対策はサイバーセキュリティに限らない

- そもそも、security theaterという言葉が、9・11事件後の航空業界で、実効性のほぼ無い対策を揶揄するために作られた感じ
  - 一部の対策が効果が無いことが統計的に示されている(by 通過したテロリスト数 vs 発見できたテロリスト数)
  - 顔認証とかで無関係の人間を引っ掛けてしまう話も
- 最近の日本だと、ハンコがやり玉に上げられている感じ
  - 3Dプリンタの進歩によって、捺印をもとに、同じ印章となるハンコなんぞいくらでも作れる
  - 実印も、そもそも役所に(偽の身分証明書で標的のフリをして)別の印鑑を実印として(再)登録される(&印鑑証明書を発行する)という穴も

概要

- 一般的な視点からのダメなセキュリティ対策とその悪影響
- ダメなセキュリティ対策とその悪影響の事例
- 良いセキュリティ対策の事例
- 個人的に「理解不足でダメなセキュリティ対策」になりそうで気になる案件

  注: この項目は特に主観が強く入るとともに、技術動向で変化する可能性が高いです

パスワード認証や多要素認証の前提

- 計算機性能の向上により、安全なパスワードの長さは10文字ぐらいまで伸びた
  - 安全なパスワードの定義: ハッシュ化後のパスワードを入手後、総当たりで破られるまでの時間が現実的でない
- 当然ながら、パスワードは他サービスと共用してはいけない
  - …が、現実には、100以上のサービスでパスワードを作ったりすると、似通った所は出てきたりする

→パスワードマネージャの使用が望ましい。安全に管理したメモもあり

- 多要素認証の「パスワード(固定値)」以外の要素は、「パスワード(固定値)」にならない物でなければいけない
  - 例: 事前にダウンロードしたシードを基に30秒ごとに更新される値(OATH-TOTP), 事前登録メールアドレスへのワンタイムパスワード

パスワードに関するダメなセキュリティ対策

- 定期変更の強制
- 特定の文字列の強制
- 秘密の質問
- コピー&ペーストの禁止
- エセ多要素認証
- その他のセキュリティを阻害する仕様など

パスワードの定期更新について

- 一部のサイトではパスワードの定期更新を要求されますが、もうかなり前に「意味がないどころか有害」となった
  - 悪人が破った(盗んだ)パスワードをしばらくこっそりと使うことが前提
  - 余裕が無い時に定期更新を要求して安易な物にされる害の方が大
  - 言ってくるサイトはセキュリティの意識が低いと考えて良い
  - NISTは約10年前から言っているが、まだやる所多いので改めて[1]
- 一応、盗聴などを目的として、悪人が破った(盗んだ)パスワードをしばらくこっそりと使うことの事例は0ではないが…
  - 検出には利用履歴やログイン履歴を時々チェックする方が確実
- 基本「パスワード漏洩のニュースがあったらすぐ変更」でOK
- なお、「パスワードを変更して下さい」の偽メールには注意
  - メール中のURLは触らず、サービスのトップページから確認と対応

[1] https://www.infosecurity-magazine.com/news/nist-scraps-passwords-mandatory/

特定の文字列の強制

- 「良いパスワードを作るのではなく、パスワード生成ルールをパスすることを目的として、パスワードの強度を下げる」ことになる人が多数出てくる
- 特に、パスワードの特定の位置の文字列が特定のパターンになる事例が多くなることが考えられる
  - 例: 記号入れるためにパスワードの末尾をスマホで入力しやすい記号に
    - 入力モードの切り替えの手間を考えると、末尾に追加するのが楽
  - 例: 大文字入れるために最初の1文字をアルファベットかつ大文字に

→悪人はこれ前提で解析ツールを組んで来る

- これまた、最近増えてきているので、NISTが新ガイドラインでダメと言った[1]

[1] https://www.infosecurity-magazine.com/news/nist-scraps-passwords-mandatory/

秘密の質問

- 「パスワードを忘れた時のために」とか理由をつけて設定を強要されたりするアレ

- 所感
  - なんでわざわざ攻撃者に対して絶好のクラックルートを追加するんですかね
  - そんなに安全な手順でパスワード再発行するのが面倒ですか？
  - 「セキュリティよりコストを優先する体質」という認識でいいですか？
- 対応
  - 「必ずやれ」と言われたらできるだけ長い乱数(文字や記号入り)を投入しましょう
    - というか、答えの文字数に上限を設定があったりして、さらに破りやすくしてある攻撃者に親切なサービスもちらもら

パスワード欄へのコピー&ペースト禁止

- パスワードマネージャからのパスワードのコピー&ペーストができなくなるアレ

- 所感
  - パスワード欄へのコピー&ペースト禁止は入力しやすさ優先の(脆弱な)パスワードを蔓延させる基盤となり、百害あって一利なし
- 対応
  - 当該ページの特定のJavaScriptをブロックすればコピー&ペーストできるようになる可能性が高い
    - JavaScript ON/OFFのブラウザ用アドオンを使うとか
  - 細かくやるならば、特定サイトのコピー&ペースト禁止の設定をオーバーライドするJavaScriptを特定サイト閲覧時に適用するとか

エセ多要素認証(1/2)

多要素認証に見せかけて実質1要素認証と変わらないアレ

- パズル認証系
  - 「合わせ絵パズルを解いて」「上と同じだけクリックで色を変えて」
  - 認証の答えが同一ページにあるので、認証ですらない
    - 25年前に情報工学科でやった画像処理の演習レベルで自動化可能でボット避けでも役に立たないレベル
    - というか、これを使っていたどこかで盛大に不正アクセスされていたり
  - まともなボット避けフレームワークを使うのがそんなに嫌ですか
- パスワードを2回入力させる
  - 長いパスワードを1回入れさせるのと安全性は変わらない
  - というか、勝手に個人情報を2つ目のパスワードにするのやめろ
    - 「この認証システムクラックされたら、認証情報のついでに自分の誕生日まで流出するな」と思っている所が(総当りでハッシュの現像は容易)

エセ多要素認証(2/2)

- 認証時にOTP送付先メールアドレスを変更できる
  - 攻撃者からすると、自分のメールアドレスに変更すればOKなだけ
  - ひょっとして「古いメールアドレスもう使えない」問い合わせ対策かもしれないが、それはセキュリティよりコストを優先した判断
    - ちゃんと正規のパスワード再発行と同じコストをかけないとダメ

最近増えている傾向にあるため、見つけ次第、積極的に糾弾して欲しい

多要素認証の1要素だけを流用したために脆弱になった事例

- 4桁数字の暗証番号をウェブサービスの認証に利用したためにクラックされた事例
  - あれは、物理鍵(キャッシュカードとか通帳とか)との組み合わせで有効な物
  - そもそも、4桁/6桁の数字の暗証番号の問題は、JAL/ANAのウェブサイトが2014年にやらかしているのに今更という感じ

その他のパスワード認証でセキュリティを阻害する仕様とか

- パスワード長に制限がある
  - パスワード長の制限により、パスワードマネージャが生成する安全な長さのパスワードが使えない
  - 特に明示もなく、最初のn文字までをパスワードとするやっかいなシステムもある
  - (某銀行のオンラインバンキングのパスワード長制限がたった12文字だった時には目が点になった)
- お客様サポート等がパスワードを聞き出そうとする(強要してくる)
  - 他のパスワードの生成ルール推測のヒントになりうる
  - クレジットカードの暗証番号同様、当人に入力させないとダメ

デバイス登録型2要素認証で認証手続きが容易すぎるもの

- FIDOやMS365など、最初にデバイスとサービスを結びつけての2要素認証で、認証手続きが容易すぎるものがある(あった)
  - 認証時にデバイス側で出たポップアップ上で「OK」を押すだけ
- これ、一般的な人は、「あまり考えずにOKを押す」ことが多々あると考える
  - 日頃から注意している人でも、手が滑ってOKとか、他の作業中のポップアップにOKとかやりそう
- すでに多要素認証疲労攻撃[1]として攻撃が確認されているらしい
- 対策: OKを押す前にPINコードレベルの入力をさせる設定

[1] https://news.mynavi.jp/techplus/article/20220925-2461999/

電子メールに関するダメなセキュリティ対策

- 添付ファイルの意味なく暗号化ZIPにする風潮
  - 実行ファイルにする亜種も存在
- セキュリティのためなのかの謎ルール

添付ファイルを全て暗号化ZIP圧縮ファイルにする風習(1/2)

- メールを窃取される時には、ほぼ例外なく両方のメールを窃取されるために全く意味は無い
- 電子メールを送るときに、自動的にこれをやるソリューションもあるらしい

  →「効果がない物にお金が注ぎ込まれる」という実例
- PPAP(パスワード付きZIPファイル送る、パスワードを送る、暗号化、プロトコル)とか名前をつけてまで馬鹿にされている
  - 余談: PHS(プリントして、判子押して、スキャンする)話も同様にネタにされている
    - 電子データ(PDF)の発注書などに対し、発注をする時にPHSをして送り返すことを要求されることがある
    - 素直に決済システムを構築すれば…

添付ファイルを全て暗号化ZIP圧縮ファイルにする風習(2/2)

- 弊害
  - 暗号化する方も解除する方も手間
  - メールサーバ側のアンチウィルスエンジンでチェックできない
  - というか、「公開されているパンフレット」をわざわざ暗号化して送るのはやめなさい (…が、会社の規則で全添付ファイルはPPAP命令)
- 素直にS/MIMEするのがベスト
  - まあ、認証局を準備するのが面倒くさいのでしょうが…
- 現時点での現実的な解決としては、ファイルサーバに置いてパスワードは一部を双方が分かる匿名化とか
  - ダウンロード状態の追跡もできる
  - ダウンロード試行が異常だったらロックする設定もできる
  - パスワードの一部匿名化は、お互いが知っている物(電話番号の一部)をsuffixに使うとか

暗号化ZIPファイルの亜種

- 添付ファイルをオリジナルの自己解凍形式の圧縮ファイル(実行ファイル)に置き換えるソリューションも
  - 暗号化ZIPの亜種
  - 「電子メールに添付された実行ファイルを実行して下さい」という、情報リテラシ的には気持ち悪いことこの上ない
    - 実行ファイルにDLLインジェクションとかできる脆弱性があったことも
  - 最近では、実行ファイル(拡張子.exeで判断)がアンチウィルスゲートウェイとかではねられるので、ファイル名を変えた上で、「ファイル名を変えて実行して下さい」と悪化している

電子メール関係での謎ルール

- 「電子メールに返信で返してはダメ」というルールを設定されたという話
  - 感染すると、メールボックスのメールに返信するEmotetの話を聞いたから?
- 電子メールなんて、ヘッダを編集すればいろいろ偽装できるので、送信側で謎ルール設定しても意義は非常に薄い
  - From欄の編集(偽装)は当たり前のようにやられてくる
  - In-Reply-ToとかReferencesを編集すれば、全く関係ないメールへの返信に偽装することもできてしまう

悪性サイト啓蒙関係のダメなセキュリティ対策

- 「URLはhttpsで始まるから安全です」という間違い
  - 今時のフィッシングサイトの8割はhttps[1]
  - 攻撃者側も、無料のTLSサーバ証明書サービスや、「必要な投資」として有料のTLSサーバ証明書サービスでサーバ証明書を発行
  - c.f. マルウェアのC&C通信のTLS化もだいぶ前から進んでいる[2]

[1] https://scan.netsecurity.ne.jp/article/2021/04/30/45602.html
[2] P. Calderon, et al. "Malware Detection Based on HTTPS Characteristic via Machine Learning," ICISSP 2018, Jan. 2018.

決済関係の微妙なセキュリティ対策

- 決済処理中にウェブサイト遷移が起きる決済サービス、悪性広告による(決済情報窃取を目的とした)画面操作とまぎらわしい
  - さらに、遷移先のURLが決済サービスと認識しにくい(EV証明書上の実体も含めて)となおさら
    - 参考: DV証明書はドメイン所有のみ確認、OV証明書は所有者実体まで確認、EV証明書は法的実体まで確認して発行
- というか、決済関係で外部の決済サービスを使うなら、最初からその旨を明記した上で、決済の最初から移動してくれた方が遥かにマシ

セキュリティ名目で無茶苦茶な約款を提示する事例

- 「生年月日、電話番号は我々が認証に使うから漏らすな」と無茶苦茶を言ってくる約款を設定したサービスがある
  - ちょっと検索かけると出てきます
- 少なくとも、電話番号は「通信をしたい相手に伝えることを前提」とした識別番号であるため、「本来の目的外のために利用するから、本来の目的(通信)にそぐわないことを強要」する時点で不当条項に値する
- 生年月日も親しい人との間での円滑な人間関係を築くために伝えることは当たり前のように行われているため、それを制限することは、不当な私権の制限(の強要)に値する

セキュリティ対策が甘い会社のソフトウェアを継続的に使う

- 同じような脆弱性を繰り返し(多く)出すソフトウェア
  - 修正した時に他の同様な構造をチェックしたり、開発用チェックリストにノウハウを蓄積できていないのか…
- 複数のバグハンターから評判の悪い企業というのもある
  - 「修正が遅くてやきもきする」「丁寧に説明しても脆弱性について理解してくれない」「対応が悪い」とか
  - セキュリティ対策ソリューションをうたっている企業でもこの手の企業はありうる

→乗り換えコストを考えても、思い切って乗り換えてしまうのも大事

物理セキュリティの微妙なセキュリティ

- ボタンを押す(押したボタンは戻らない)タイプの鍵
  - nCrの組み合わせしか無いので弱い
    - n: ボタン数
    - r: 押すボタンの数
  - よくある10個の数字ボタンを4つ押す製品の場合、10C4=210通り
  - (使ったことないので、「押したボタンが戻らない製品がある(&順番はどうでも良い)」ことを私も知らなかった)
  - 経年使用すると利用ボタンの劣化で容易にバレそう

概要

- 一般的な視点からのダメなセキュリティ対策とその悪影響
- ダメなセキュリティ対策とその悪影響の事例
- 良いセキュリティ対策の事例
- 個人的に「理解不足でダメなセキュリティ対策」になりそうで気になる案件

  注: この項目は特に主観が強く入るとともに、技術動向で変化する可能性が高いです

パスワード関係

- 長さ、文字種(大文字、小文字、記号)の組み合わせからのパスワード強度の判定
  - Dropbox社がzxcvbn[1]なる強度メータをオープンソースで出している
    - 各種言語に移植されている
  - 「大文字x文字、小文字x文字、記号x文字」という制約を提示するよりスマート
  - 最近は単語予測変換も一般的になったし、文章でパスワードを組むのも前よりやりやすくなった

[1] https://dropbox.tech/security/zxcvbn-realistic-password-strength-estimation

認証関係

振る舞いに応じた認証レベル変更

- 毎回毎回2要素認証を要求されるのはユーザ側も面倒
- 通常とは違う環境(IPアドレス、ブラウザフィンガープリント、など)からのアクセス時のみ2要素目を要求
  - 同じ環境でも、ある程度定期的に2要素目を要求する
- 特に怪しければ、3要素目以降も要求したり
  - 電話(音声)による確認は攻撃者にとって嫌そう
  - SMS認証は窃取手段がいろいろ出てきて最近では推奨されていない
- アカウントロックまでやると反感を買う事例あり
  - リモートワーク関連でVPN使って急にsource IPアドレスが変わるとアカウントロックされるサービスの話を聞く

電子メール関係

- 電子メールの添付ファイルをプレビュー機能付きファイルサーバに移動
  - 明らかに内容の無い、悪意のあるファイルをプレビューで避けれる
  - 正規のファイルであるならば、ファイルサーバからダウンロード
  - なお、「遠隔でMS Officeを操作できるサーバ」はMicrosoftのEUAL違反になるので注意
  - まあ、普及したら、プレビュー機能付きファイルサーバ自体を攻撃する話も出てくるかもしれないが、監視点が集約される点で楽
- 電子メール中のURLをアンチウィルス付きウェブプロキシサーバを経由するURLに置き換える
  - ウェブプロキシ側で送り込まれるファイル等を細かくチェックできる

悪性URL関係

- DNS側で悪性URLの名前解決をブロックするのは、処理量的にコストパフォーマンス高い
  - IPSなど通信レベルでやると、扱う通信量が多い(= 処理量が多き)ためにコストが高い
- 短縮URLの先を自動展開するアドオンとかもあると良さそう
  - ウェブサービスは知っているが、(残念ながら)アドオンは知らない

穴は残るが、個人的に「まあベターでは」と考えてやっていること

- 相手にファイルサーバに置いたファイルなどのパスワードを伝えたいのだが、どうやって安全に伝えれば良いのか…

  →事前に相手に教えた部分パスワードとメール本文に書いた部分パスワードを連結させてパスワードとする手
  - 勘合貿易をイメージ
  - 最近はメール+Slack系などで分割伝達しやすくなった

その他、嶋田がやっている対策(パラノイア的な物も含む) (1/2)

- データバックアップは定期的にオフラインメディアも含め実施
  - 「すでに破壊されていたファイルをバックアップする」可能性も考えて、数世代の直近バックアップを残す
- 電子メールはUNIX系OS上で送受信
  - 添付ファイルは、必要に応じてプレビュー後にWindowsに送りはする
- メール中のリンクは、ユーザ登録時のメール到達性確認など、自分のアクションに応じて送られて来た物以外は使わない
  - トップページからアクセスする(+ ログインページ等をブックマーク)
  - ブックマーク以外にも自前のURLメモを作成したり

その他、嶋田がやっている対策(パラノイア的な物も含む) (2/2)

- やりとりの無い所からの添付ファイルは、UNIX系OS上でファイル形式変換をかけてからプレビュー
  - 例: PDF文書->PostScript文書、JPEG画像->PNG画像、MS Office系文書をLibreOfficeの--convert-toでPDF変換
- 検索時にアフィリエイトサイトらしい所とか怪しい所が多くまぎれこんだ感じならば、JavaScriptを無効化して閲覧
  - 悪性広告(Malvertizing)とかトラッキングとかの対策
  - 厳密には、JavaScript無効なテキストブラウザ(w3m)で再検索して閲覧
    - 最近はWindows Subsystem for LinuxのおかげでWindows上でも容易

概要

- 一般的な視点からのダメなセキュリティ対策とその悪影響
- ダメなセキュリティ対策とその悪影響の事例
- 良いセキュリティ対策の事例
- 個人的に「理解不足でダメなセキュリティ対策」になりそうで気になる案件

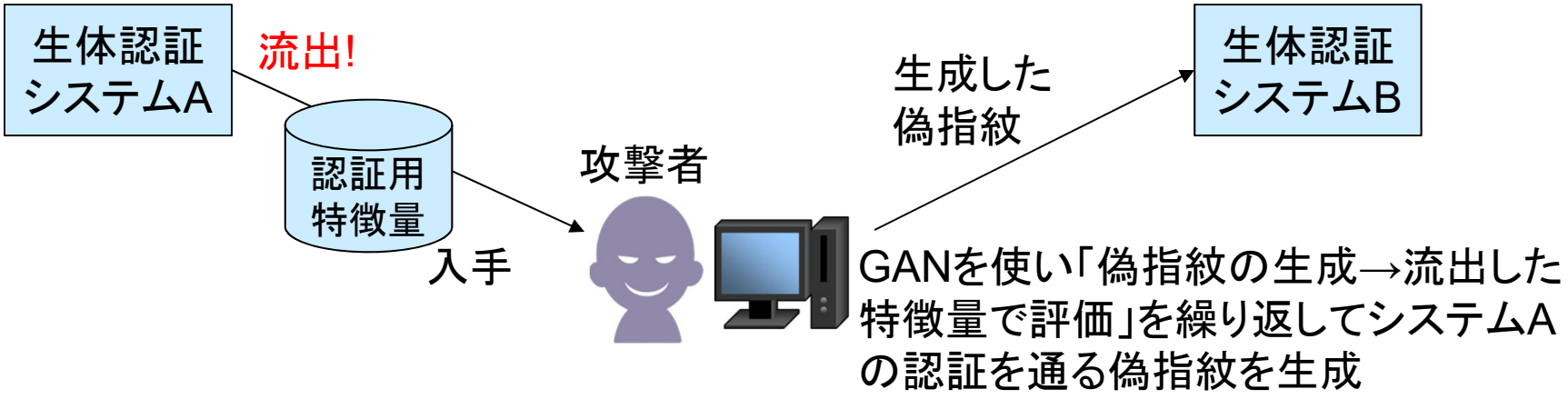
  注: この項目は特に主観が強く入るとともに、技術動向で変化する可能性が高いです

不要な所へのブロックチェーンの利用(濫用)

- 「信頼の大本を担保する所(例: 認証局のサーバ)」を作ればOKな所にもブロックチェーン濫用を口にする人間が…
  - 1取引当たりの処理量が数桁増えて(無駄に増えて)、処理速度や電力消費(グリーンコンピューティング)の点から無駄出まくり
- 2020年の東証のシステムトラブルに関連しても「ブロックチェーン」とか言っている人間が多数でてきたり…
  - この数年で仮想通貨のロールバックは何回起きましたか?
  - 証券取引市場でロールバックなんかやったら市場の信用無くしますよ
    - ジェイコム事件とか見ても「成立した取引はちゃんと遂行させる」がよく分かる(なので、今回も変な取引を成立させるよりは停止としたのだろう)
- もちろん、契約の公的証明の代用とかに有用そうだとは思う
  - 公証人制度はすでにあるが、それを電子化してコスト下げるとか
  - 「信頼の大本を担保するルート認証局を作れない場合の電子署名みたいなデータ保障はどうする?」な場でのみ有用だと思う

生体認証への過度な期待(信用) (1/2)

- 「生体認証で万全」なアピールしている所がそこそこ多い感じ
- 元の指紋の画像無しでも、モデル抽出等から認証を突破する指紋は敵対的生成(GAN)などを使ってできると思う
  - システムAから流出した認証用特徴量を使ってGANでシステムAの認証を通る指紋を作り、同じ設計のシステムBに入れたら?
    - 「元の指紋とは同じではないが、認証は通る指紋」を生成できるのでは?
  - システムAで通るがシステムBで通らない物の方が多いかもしれないが、試行数が多ければ?



生体認証への過度な期待(信用) (2/2)

- すでに画像認識関係ではGANで「人目には物体Aには見えないが、機械学習/深層学習ベースの識別器には物体Bと判断される」画像を作成する話は多数出ている
- 顔認証なども不用意に活用を進めて大丈夫?
  - 「自分の顔をベースに、(ある程度似た)他人と認識されるための化粧方法」をGANで生成することもできそうに思える
  - そもそもprivacy abusing側の問題をろくに考えていない案件が多すぎるように見える
- 利用者側としては、生体認証は破られた時に替えが準備できない所がやっかい
  - さらに、認証を利用しているサービス提供者が「生体認証に過度な信用を置いている」組織だと、実際に生体認証が破られても「そんなこと起きようが無い」と言い張りそうなのも厄介そう

「量子コンピュータ実用化よる暗号の解読」に関して詐欺出てこない?(1/2)

- RSAやEC系は量子コンピュータに弱いと言われている
  - というか「量子コンピュータが実用化すれば…」な槍玉にされるぐらい
- 嶋田の個人的な主観
  - 現状で実用化の量子ビット数(10^3)+αでは、現在公開鍵暗号で標準利用されているビット長の暗号鍵を解くのは無理(10^6～10^9ほど必要)
  - 量子ビット数を増やすほど量子状態の維持が幾何級数的に難しい
  - とりあえず、ビット長を長くすれば当分大丈夫では? (すごいブレイクスルーが無い限り)
- もちろん、対量子コンピュータ暗号(ポスト量子暗号)の研究もだいぶ前から行われている
  - 米国NISTがポスト量子暗号の標準化を開始(2017年)、2024年8月に3アルゴリズムを選定[1]
  - OpenSSHは2022/4から格子暗号系とEC系の組合せが基本に[2]

[1] https://atmarkit.itmedia.co.jp/ait/articles/2408/28/news039.html
[2] https://japan.zdnet.com/article/35186176/

「量子コンピュータ実用化よる暗号の解読」に関して詐欺出てこない?(2/2)

- 懸念:「量子コンピュータの利用が増えたら御社のセキュリティは…」とかの詐欺ソリューションとか出てきそう
- 変なソリューションを使わずに、王道な対応をしましょう
  - とりあえず、実用化されそうな量子コンピュータが対応できない鍵長に伸ばせば良い
  - 無事に、NIST標準のポスト量子暗号コンペティションも終わったので、ポスト量子暗号への移行を粛々と進める

- 量子暗号もひょっとしたら詐欺案件に出てくるかも
  - こちらは秘密鍵の搬送に有用そう
  - 個人的には公開鍵暗号基盤を整備していれば、十分に安全なレベルをコストパフォーマンス良く実現できるかなと
    - もちろん、リモートからの初回の登録をどう運用するかが