SQAT®
SECURITY REPORT

2021-2022年 秋冬号

株式会社ブロードバンドセキュリティ
セキュリティサービス本部
東京都新宿区西新宿8-5-1 野村不動産西新宿共同ビル4F
TEL：03-5338-7417　FAX：03-5338-7435
https://www.bbsec.co.jp/

知る・守る
続ける

BBSecは内閣サイバーセキュリティセンターの
「サイバーセキュリティ普及啓発」に賛同しています

はじめに

株式会社ブロードバンドセキュリティ
セキュリティサービス本部 本部長
齊藤 義人

本レポートは、株式会社ブロードバンドセキュリティ（以下、BBSec）の脆弱性診断サービス「SQAT®」における2021年上半期（1月～6月）の膨大な診断結果からデータを抽出し、集約したものを、当社のエンジニアらの感性も交えてアウトプットしたレポートです。主にサイバーセキュリティのトレンドや展望についてお楽しみいただくことができる内容となっております。

2021年上半期もさまざまなニュースが散見されました。前期から引き続き、テレワーク絡みのセキュリティの盲点をついた攻撃や、セキュリティ対策が不十分な中小企業への攻撃とそれに起因する大企業等への攻撃が目を引きました。テクノロジーの発展と攻撃手法の高度化は比例していますが、今期におけるランサムウェア攻撃件数の圧倒的な増加を鑑みると、攻撃の糸口の基本は大きく変わっていないともいえるでしょう。

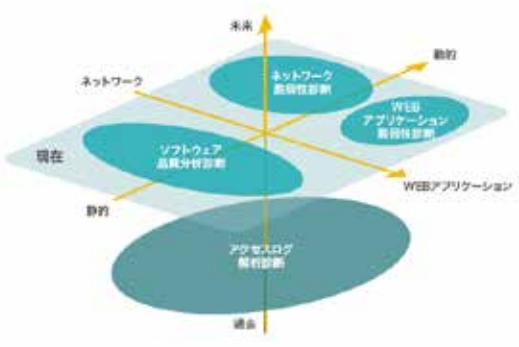
日常生活、事業活動のいずれにおいても、Webサービスやスマホアプリの利用にあたってログイン認証を行う機会は少なくないでしょう。パスワード認証をはじめとする認証機構は、サイバー攻撃者たちに狙われやすいポイントの1つです。認証情報を奪われてしまうと、不正アクセスを受けて個人情報が盗まれたり、不正利用による直接的な金銭被害が発生したりといった、深刻な被害を招きかねません。認証機構の不備をついた攻撃に対する対策は必須といえます。巻頭企画では、サイバーセキュリティ対策を実装する上で重要な認証技術に焦点を当て、システムの安全性を高めるための方策を考えます。

仮にセキュリティにあまり詳しくない方でも、脅威に対してどのようなセキュリティ対策をすべきか検討する機会に、「コンピュータウイルス」や「Webサイト改竄」といった単語を脳裏に思い浮かべることは多いでしょう。今号の注目テーマは、不正なソフトウェア「マルウェア」の解説をすると同時に、その歴史をたどり、セキュリティとの関わりに着目して昨今の社会に与えた影響を紐解きます。

本レポートが、読者の皆様のセキュリティ対策における有益な情報としてご活用いただけることを願ってやみません。それこそが「便利で安全なネットワーク社会を創造する」をモットーに掲げるBBSecの使命であると考えております。

SQAT®（Software Quality Analysis Team）とは
～スペシャリスト集団が組織の脆弱性対策をトータルに支援～

「SQAT®」は、BBSecがご提供する脆弱性診断サービスです。エンジニア、コンサルタント、ホワイトハッカー等から編成された精鋭チームが、あらゆる側面から網羅的な診断を実施。スペシャリストのノウハウを結集して組織の情報システム強化をお手伝いします。お客様は金融機関・インターネット事業者などの民間企業から、官公庁をはじめとする公共機関まで幅広く、これまでに延べ6,420組織、38,200を超えるシステムで利用されています。



CONTENTS

※本レポートは、当社セキュリティサービス本部のホームページ
「SQAT®.jp（URL：https://www.sqat.jp/）」
https://www.sqat.jp/sqat-securityreport/からダウンロード可能です。

SQAT.jp

巻頭企画

認証技術は今

SQAT® Security Report 編集部

認証とは、主に、特定の場所への入場や特定のシステムの利用などにあたって、「その人物が確かに入場や利用を許可された当人であるか」確認することを指す。認証技術は、様々なシステムにおいてユーザの真正性を確認するためのものであり、セキュリティの要といえる。本稿では、Webサービスおよびスマートフォン（以下、スマホ）アプリにおけるユーザ認証技術について、昨今の実情を今一度整理し、セキュアなシステム構築のためにどのような認証機構が求められているのかを探る。

認証をとりまくリスク

サイバー攻撃のうち、認証の仕組みに不備があることにより発生するのが、アカウントの乗っ取りである。最近報告された国内のインシデントには以下のような例がある。

報告時期	インシデント	影響
2021年6月	大学研究員のメールアカウントの不正利用*1	海外の不特定多数の宛先に迷惑メールが送信された。
2021年2月	メッセージングアプリアカウントへの不正アクセス*2	3,000を超える認証情報が流出した恐れ。
2020年9月	電子決済サービス不正口座利用*3	多数の銀行口座から不正引き出し。金融庁が対応要請を出した。

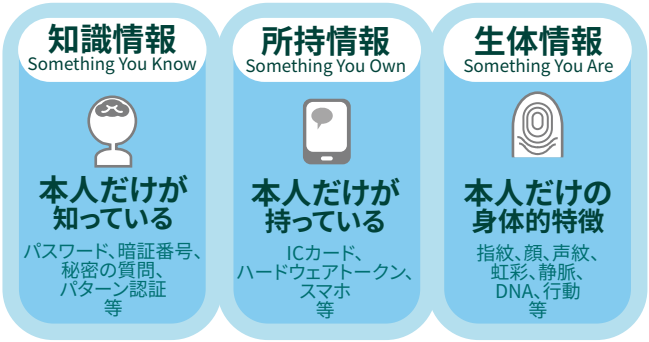
参考情報

*1 https://www.tohtech.ac.jp/topics/wp-content/uploads/2021/06/b2bf7149426b908ee02bf708390706db-1.pdf
*2 https://linecorp.com/ja/security/article/364
*3 https://www.fsa.go.jp/news/r2/sonota/20200915/20200915.html

認証の3要素

ここで、そもそも認証にはどのような要素があるか、おさらいしたい。認証の要素になり得るのは、その本人だけに属するモノ・コトだ。次のとおり、「知識」「所持」「生体」の3種類の要素が挙げられる。

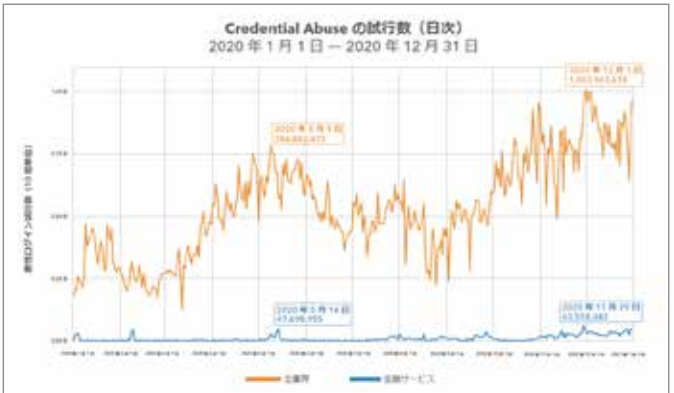
いずれの要素も、「本人だけ」という点が重要だ。他人が知っていたり、所持していたりしては、その本人を認証したことにはならないからだ。



パスワード認証の限界

ID・パスワードによるログインを試行する攻撃手法は複数あるが、パスワードリスト攻撃の一種で、ボットにより大量の不正ログインを試みるCredential　Abuseは、1日に億単位で実行されている。このうち特に金銭被害に直結しがちな情報を保持する金融サービス業では、1日あたり数千万件との報告もある（右・折れ線グラフ）。

しかしながら、どれほどサービス提供側が警告を発したとしても、ユーザは複数のサービスで同じパスワードを使いがちだ。実際、複雑なパスワードを設定するのも、複数の異なるパスワードを管理するのも面倒である。ヒトの記憶に頼るパスワード認証という方法の宿命と言えるだろう。



出典：Akamai Technologies, Inc.「SOTI インターネットの現状/セキュリティ」レポート第2号『金融業界に対するフィッシング攻撃』
https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/soti-security-phishing-for-finance-report-2021.pdf

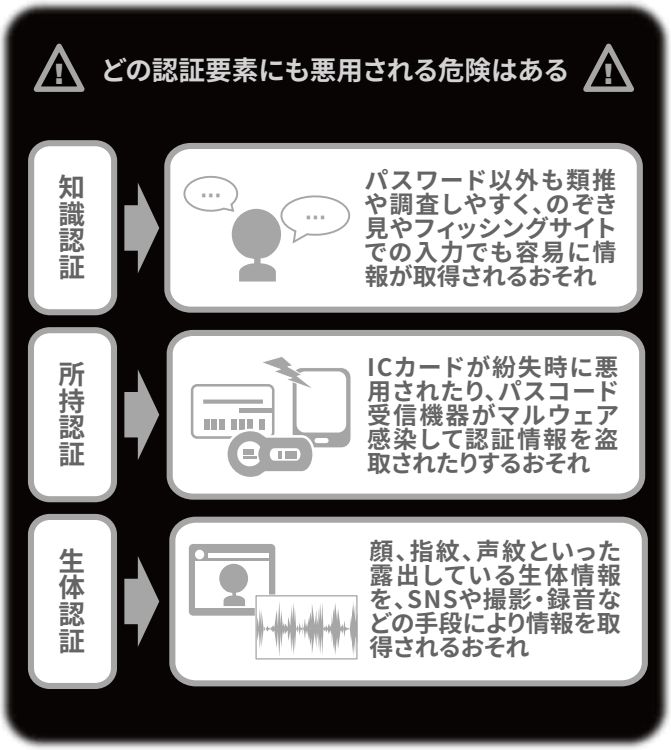
主な認証技術

Webサービスやスマホアプリにおいて使用されている認証方式には、前述した3要素のうち1つのみ用いる**単要素認証**（パスワードのみの認証など）、2つ以上の要素を組み合わせる**多要素認証**（パスワード＋スマホで受信した認証コードなど）、また、認証を二段階で行うが、認証要素自体は同じでもよい**二段階認証**（パスワード＋秘密の質問など）があり、いずれの方式も右のような様々な認証技術を組み合わせて行われる。

Cookie認証	トークン認証	ワンタイムパスワードトークン
Webサーバが発行するCookie（セッションID）を使用した認証	認可サーバが発行するアクセストークンを使用した認証	生成される一回限りの使い捨てパスワードを使用した認証
PKI（公開鍵認証基盤）	**生体認証**	**FIDO認証**
インターネット上で安全に情報をやりとりするためのセキュリティインフラ	指紋、顔、虹彩などの身体的特徴による認証で記憶や所持が不要	生体認証と公開鍵暗号方式を組み合わせたパスワードレス認証

パスワード認証以外なら安全か

では、パスワード認証以外の認証方法なら安全だろうか。各要素による認証について、想定されるリスクには以下のようなものが考えられる。



残念ながらどの認証方法も、完全に安全ということではない。それぞれの特性により、認証が破られて悪用される危険はあるといえる。

リスクをできるだけ回避する多要素認証

そこで、複数の認証要素を組み合わせることで、少しでも破られるリスクを低減させよう、というのが多要素認証の考え方だ。認証を突破するのに手間がかかればかかるほどよい。多要素認証については、右表のような様々なセキュリティ基準やセキュリティガイドラインでも、言及されている。

表　主なセキュリティガイドライン

ドキュメント名	発行元	発行年月
テレワークセキュリティガイドライン 第5版	総務省	2021年5月
地方公共団体における情報セキュリティポリシーに関するガイドライン（令和2年12月版）	総務省	2020年12月
行政手続におけるオンラインによる本人確認の手法に関するガイドライン	内閣官房	2019年2月
医療情報システムの安全管理に関するガイドライン 第5.1版	厚生労働省	2021年1月
教育情報セキュリティポリシーに関するガイドライン（令和3年5月版）	文部科学省	2021年5月
鉄道分野における情報セキュリティ確保に係る安全ガイドライン　第4版	国土交通省	2019年3月
Application Security Verification Standard 4.0.2	OWASP	2020年10月
NIST SP 800-63-3: Digital Identity Guidelines Revision 3	国立標準技術研究所	2020年3月
Payment Card Industry Data Security Standard Version 3.2.1	PCI SSC	2018年5月
CIS Controls Version 8	Center for Internet Security	2021年5月

しかし、たとえFIDO認証などの多要素認証を実装したとしても、認証情報自体が漏洩してしまえば、いかなる認証も破られてしまうことになる。これを防ぐにはどうすればよいか。