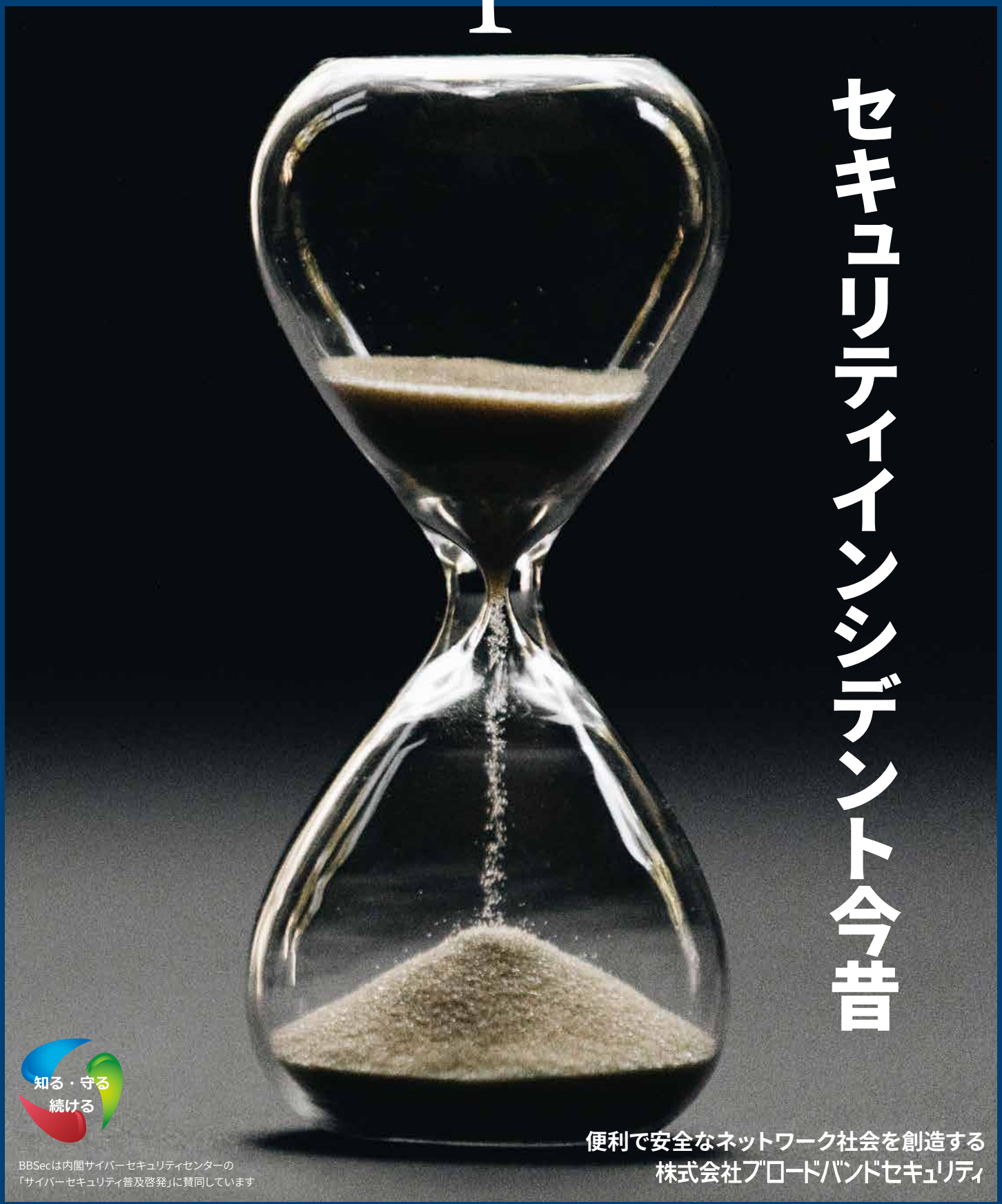
SQAT® Security Report

2023年 春夏号



セキュリティインシデント今昔

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

便利で安全なネットワーク社会を創造する
株式会社ブロードバンドセキュリティ

ごあいさつ

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

日本国内の 2022 年のサイバー攻撃は、前年度比でおよそ 3 割も増加したとみられています。増加からくるものなのか、世界各国の大半が、「2022 年にもっとも脅威に感じたこと」を「気候変動」としている中、日本は「サイバー攻撃」としているとのデータもあります。

下半期に影響範囲が広かったサイバー攻撃の中に、医療機関へのランサムウェア攻撃があります。この攻撃は、サプライチェーン攻撃の側面も持っており、サイバー攻撃の複雑化を象徴していたかのようにも思えます。また、ロシア系ハクティビストグループ「KILLNET（キルネット）」による日本を標的としたサイバー攻撃が発生し、重要インフラ事業者を含む、複数の組織が攻撃を受けました。

2022 年は AI 技術の発展が目覚ましい年でもありました。特にチャットボット「ChatGPT」の登場は、大きなインパクトを持って迎えられました。多くの人々の関心が高まっていますが、同時にサイバー攻撃者からの関心も高まることも忘れてはならないでしょう。フィッシングメールの生成や、マルウェアの組み立てなど、様々な面で攻撃に活用してくることが予想されます。

高度化と増加を続けるサイバー攻撃に備えるためにも、セキュリティの強化は急務です。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株式会社ブロードバンドセキュリティ（以下、BBSec）の使命であると考えております。

本レポートは、BBSec の脆弱性診断サービス「SQAT®」における 2022 年下半期（7 月～ 12 月）の診断結果からデータを抽出し、集約したものを当社エンジニアらの知見も交えてアウトプットしたものです。今号は、過去に起こったセキュリティインシデントのうち、現代まで系譜があるものの変遷から有効な対策を紐解く企画や、PCI DSS v4.0 について、求められる要件のうち脆弱性診断に係る事項に焦点を当て、対応や概要をつづった企画を掲載しております。

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

セキュリティインシデント今昔

SQAT® Security Report 編集部

時代を意識したセキュリティ対策ができているだろうか？
企業としてセキュリティ対策を行うのはいまや当たり前の現代。ここでは過去から現代に至るまでのセキュリティインシデントの変遷をみることで、現代において、どのように注意を払っていくべきなのかを対策とともに取り上げる。

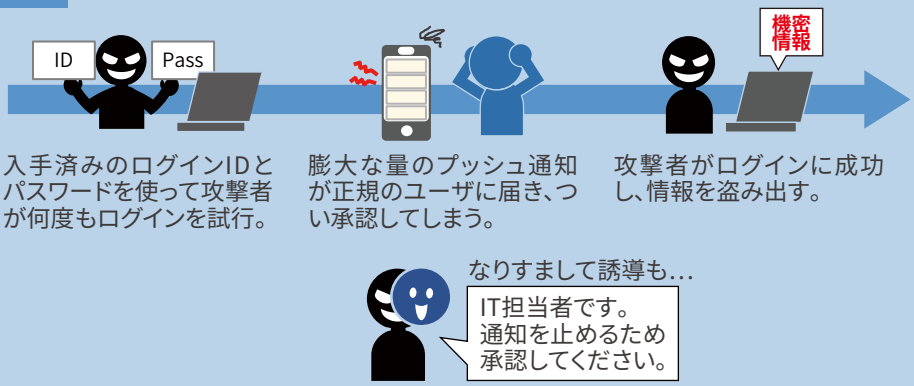
認証バイパス

本題に入る前にまず、現代の攻撃例として、認証バイパスについて紹介する。認証バイパスとは認証の迂回、つまり攻撃者が認証機能を回避してシステムにアクセスすることを指す。認証の資格情報がない攻撃者もシステムにアクセス可能となるため、危険度の高い攻撃となる。

パスワードのみといったように、単一要素による認証が主流であったが、近年では、認証強度を高めるため、多要素認証が用いられるようになってきた。多要素認証とは右記の三要素のうち、パスワードとICカード、暗証番号と指紋認証、といった具合に複数の要素を用いる認証方式である。

では、この認証をバイパスする攻撃パターンの例を以下に紹介する。

1 MFA Fatigue（多要素認証疲れ）攻撃



入手済みのログインIDとパスワードを使って攻撃者が何度もログインを試行。

膨大な量のプッシュ通知が正規のユーザに届き、つい承認してしまう。

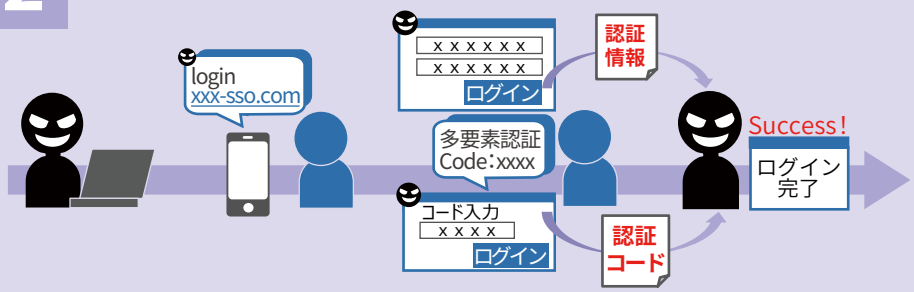
攻撃者がログインに成功し、情報を盗み出す。

※ MFA：Multi-Factor Authentication（多要素認証）

Point

多要素認証を用いていても、「通知を止めたくてつい承認してしまう」、「怪しい通知と気づいていても、誤った操作で承認してしまう」というヒューマンエラーを誘う攻撃が存在する

2 フィッシングによる認証バイパス



攻撃者がユーザが普段使っているサイトに似せた偽サイトを作成し、そこへのアクセス・ログインを促す。

ユーザが偽サイトでログインし、その認証情報が攻撃者へ送られる。攻撃者はその情報ですぐにログイン試行。正規の認証コードがユーザに届き、それを偽サイトに入力してしまうことで、攻撃者が認証コードも入手し、ログインが成功。

Point

よく用いられている認証コードによる多要素認証だが、すべて文字情報による認証のため、人の判断ミスにより攻撃者に情報が漏洩すると、ログインが可能となってしまう

3 VPNの脆弱性を突く攻撃

ソフトウェアに脆弱性があるVPN機器に対して、攻撃者がその認証方法に合わせて、メモリやログなどの情報を取得し、認証が成功している状態の情報を獲得する。

認証が成功した状態を偽装することで、認証を行っていないのに、VPN接続が成功してしまう。

Point

VPN接続後にその他のアプリに対してSSOを適用していてかつVPNの脆弱性を放置していた場合、VPN認証が回避されると各種アプリの不正利用が行われる可能性がある

※ SSO：Single Sign-On
一度の認証で連携している複数のシステムにサインオンできる

4 脆弱性などによりCookieを悪用する攻撃

攻撃者がブラウザなどの脆弱性を突いたり、ダークウェブ経由あるいはマルウェアなどを用いたりして、ユーザのセッションCookieを入手する。

攻撃者が入手したセッションCookieをブラウザに投入し、ログイン完了の状態に遷移する。

Point

Pass-the-cookie攻撃と呼ばれる手法で、「ログイン済み」という情報を盗まれるので、多要素認証を導入していてもバイパスが成功してしまう

最近話題となった攻撃が**「MFA　Fatigue（多要素認証疲れ）攻撃」**だ。これは何度も承認要求されると、通知を止めるために、つい承認を行ってしまう人の心理を突いた攻撃である。また、同様に**「フィッシングによる認証バイパス」**も、偽サイトに気づかずに情報を送ってしまう人の隙を突いた攻撃と言える。それに対し、**「VPNの脆弱性を突く攻撃」**は、VPN機器の中で動くソフトウェアの脆弱性を突いた攻撃であり、そして**「脆弱性などによりCookieを悪用する攻撃」**はブラウザなどの脆弱性を突いた攻撃である。

このように、認証バイパス一つをとっても、人の心理やシステムの脆弱性など、様々な要因によって被害が発生する可能性があることがわかる。

では、次のページから、サイバー攻撃の種類のうち、いくつかのテーマを取り上げて、それぞれにまつわる事例と共に説明していく。攻撃者が狙うセキュリティの穴はどういったところに存在するのか、ご確認いただきたい。

各パターンの対策例

MFA Fatigue（多要素認証疲れ）攻撃
- パスワード認証に依存しない認証方式を検討する
- 身に覚えのないプッシュ通知などの認証リクエストを承認しない

フィッシングによる認証バイパス
- 不審なメールの URL リンクをクリックしない
- 認証情報を入力する際にはアクセスしている URL が正規のものか確認する

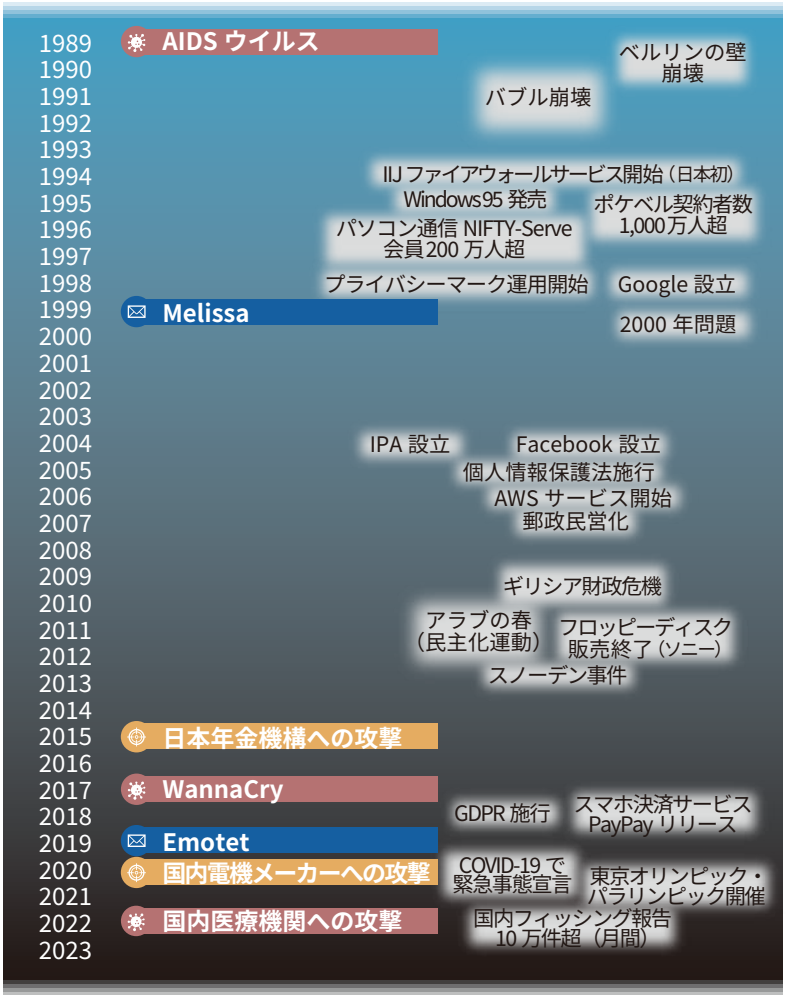
VPN の脆弱性を突く攻撃
- セキュリティアップデートが公開された際には迅速にアップデートを行う

脆弱性などにより Cookie を悪用する攻撃
- ログインが必要なサービスは、利用が終わる都度ログアウトしてから閉じる
- Cookie を定期的に削除するようブラウザを設定する

セキュリティインシデント今昔

組織・企業の事業運営に欠かせないシステムやネットワークが侵害されれば、事業継続に影響する深刻な被害に陥る恐れがあり、セキュリティ対策はいつの時代も重要であることに変わりはない。しかしながら、サイバー攻撃は巧妙化しており、セキュリティ対策にかかるパワーやコストは上がるばかりである。そのことに頭を悩ませる経営者やセキュリティ担当者は多いかもしれない。

ここからは、セキュリティ対策のヒントとして、これまでのセキュリティインシデント事例を振り返りながら、サイバー攻撃の変遷を見ていく。



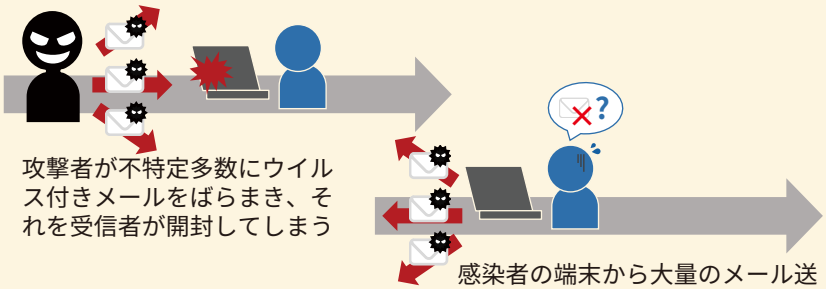
メールによる大規模感染

メールにより感染を広げる攻撃の中でも、特に大規模な感染を引き起こした例を取り上げ、今昔それぞれの特徴を見てみたい。

メールによる初の大規模な感染を発生させたウイルスとも言われる「Melissa」は、ジョーク目的だったと言われており、攻撃者本人がメール遅延やサーバ停止のような大きな被害については想定外だったと語っている。

Melissa

意図せず大規模感染を引き起こしたウイルス「Melissa」



1999 年、大規模感染を引き起こしたマルウェア「Melissa」は、Word のマクロ機能を悪用したマクロウイルス。
感染者の Outlook のアドレス帳に存在するメールアドレス宛にマクロウイルス付のメールを自動送信するウイルスであったため、大規模感染となった。
感染端末では大量のメール送信が行われてトラフィックを圧迫し、メールサーバに負荷がかかったため、送信遅延やサーバ停止などの被害も発生した。

特徴

- 感染端末のアドレス帳の宛先に対して自動送信を行う機能を有していた
- メールの件名や本文は、受信者に開封を促すような内容だった

対策

- 「Office 製品のマクロ機能を不用意に有効にしない」等の教育
- アンチウイルス製品のを導入
- マクロの自動実行を無効化

注目ポイント

この大規模感染によって引き起こされたサーバ停止等は攻撃者も想定しておらず、**意図せず大きな被害**を招いた。
メールの内容は特定の組織に特化したものではなく、**不特定多数にばらまく**形で感染を広げた。