サイバーセキュリティレポート

2023.05

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　OSINT モニタリングチーム

目次

1. 米 Ubiquiti 社の内部不正犯に実刑判決下る 3
1.1. 概要 3
1.2. 内部不正事件の経緯 3
1.3. 内部不正とサイバー攻撃の狭間 4
1.4. まとめ 4
2. 日本でも被害が広がり始めた SIM スワップ詐欺とその対策 6
2.1. 日本でも広がり始めた SIM スワップ詐欺 6
2.2. SIM スワップとは 6
2.3. SIM スワップの防御方法 8
2.4. まとめ 9
3. 警察庁、簡単なウェブサイト改ざん被害点検を呼びかけ 10
3.1. 警察庁の呼びかけ 10
3.2. ウェブサイト改ざん被害の自己点検 11
3.3. Google Dorks による調査の活用 13
3.4. まとめ 13

【当レポートについて】

当レポートでは 2023 年 5 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『米 Ubiquiti 社の内部不正犯に実刑判決下る』

- 2023 年 5 月、米 Ubiquiti（ユビキティ）社の元社員に、禁錮 6 年の判決の他、約 160 万ドルの賠償金の支払い等の命令が言い渡された。この人物は、Ubiquiti 社に在職中の 2020 年末に、同社から機密データを窃取し、外部のハッカーを装って同社を脅迫し、逮捕されていた。
- 英国では、企業の社員が外部から実行されたサイバー攻撃に乗じて、その攻撃者になりすまし、自社に対して身代金を要求したことにより、有罪判決を受けた事例が報じられている。また、Telegram では外部協力者を探す不正な活動と考えられる投稿がみられる。
- 今後、内部不正と外部からのサイバー攻撃の境界を跨ぐような事案が増加する可能性があり、それらに対しては組織間の連携を密にする必要があると考えられる。

第 2 章『日本でも被害が広がり始めた SIM スワップ詐欺とその対策』

- 5 月 11 日、警察庁は他人のスマートフォンの SIM カードを再発行して電話番号を乗っ取る「SIM スワップ」により、ネットバンキングで電話番号を悪用して不正に送金したとして、栃木県の女を逮捕した。
- 攻撃者は被害者になりすまし SIM カードを再発行する等して、被害者の電話番号を乗っ取る。乗っ取り完了後は、電話番号を利用した SMS 認証等も突破できるようになり、銀行や暗号資産のアプリを利用し、被害者名義の口座から攻撃者の口座に送金させるといったことが可能になる。
- SIM スワップに備え、重要なサービスで SMS を使った認証を使っている場合は、FIDO や認証アプリや物理キーを使った多要素認証に切り替えることを推奨する。

第 3 章『警察庁、簡単なウェブサイト改ざん被害点検を呼びかけ』

- 警察庁は 5 月、ウェブサイト改ざんの点検を呼び掛ける注意喚起において、インターネット検索を応用した調査手法を紹介した。
- この手法を使うと、改ざんされたページが検索結果に表示されるため、簡単に確認することができる。
- 上記のような Google Dorks（グーグル・ドークス）と呼ばれるインターネット検索を応用した手法は、広い範囲を効率的に調査し、自社のセキュリティ上の問題等の発見に役立つ。

1. 米 Ubiquiti 社の内部不正犯に実刑判決下る

1.1. 概要

2023 年 5 月、米 Ubiquiti（ユビキティ）社の元社員 Nickolas Sharp（ニコラス シャープ [以下、Sharp]）に、禁固 6 年と多額の賠償金支払いを命じる判決が下された。Sharp は Ubiquiti 社に在職中の 2020 年末に、ハッカーを装って同社を脅迫する事件を起こし、逮捕されていた[1] [2]。

1.2. 内部不正事件の経緯 [3]

Ubiquiti 社はワイヤレスネットワーク製品等を提供する、ニューヨーク市を拠点とする企業である。オレゴン州在住の Sharp は、2018 年 8 月から Ubiquiti 社に勤務し、ソフトウェア開発やクラウドインフラのセキュリティ等の業務を担当していた。

Ubiquiti 社では、開発環境で AWS と Github を使用しており、Sharp は上級開発者として、いずれの認証情報にもアクセスすることが可能であった。

【攻撃の概要】

Sharp は上記のアクセス権を悪用し、2020 年 12 月中旬から下旬にかけて Ubiquiti 社内の AWS や GitHub に関連する多量の機密情報を窃取した。また、攻撃の痕跡を隠すだけに留まらず、他の 5 名の Ubiquiti 社従業員がこの漏えいに関与しているように見せかけた。

年明けの 2021 年 1 月になると、Sharp は外部の攻撃者を偽装し、Ubiquiti 社の上層部社員らに、合計 50 ビットコイン（約 190 万ドル相当）の身代金を要求するメールを送信した。そしてこのメールの中で、金銭と引き換えに、窃取したデータを公開せず返還する等の取引を持ち掛けた。

しかし Ubiquiti 社はこれに応じなかったため、支払期限の数分前、Sharp は同社に SNS「Keybase」でメッセージを送信し、「ビットコインは無し。話（交渉）も無し。ここで完了だ」と伝えた。そのメッセージには、あらゆる Keybase ユーザーがアクセス可能なフォルダへのリンクが含まれており、Sharp はそのフォルダに Ubiquiti 社から窃取したデータの一部をアップロードしていた。

【逮捕】

攻撃から 1 年後の 2021 年 12 月、Sharp は電信詐欺や FBI に対する偽証等の容疑により逮捕された[4]。そして 2023

---

[1] 出典：SecurityWeek『Former Ubiquiti Employee Who Posed as Hacker Sentenced to Prison』
https://www.securityweek.com/former-ubiquiti-employee-who-posed-as-hacker-sentenced-to-prison/

[2] 出典：U.S. Department of Justice『Former Employee Of Technology Company Sentenced To Six Years In Prison For Stealing Confidential Data And Extorting Company For Ransom』
https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-sentenced-six-years-prison-stealing-confidential

[3] 出典：Condé Nast『UNITED STATES DISTRICT COURT, SOUTHERN DISTRICT OF NEW YORK「GOVERNMENT'S SENTENCING MEMORANDUM REGARDING DEFENDANT NICKOLAS SHARP」』
https://cdn.arstechnica.net/wp-content/uploads/2023/05/US-v-Sharp-Sentencing-5-11-2023.pdf

[4] 出典：U.S. Department of Justice『Former Employee Of Technology Company Charged With Stealing Confidential Data And Extorting Company For Ransom While Posing As Anonymous Attacker』
https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-charged-stealing-confidential-data-and-extorting

年 5 月 10 日、Sharp に対して禁錮 6 年の判決の他、約 160 万ドルの賠償金の支払い等の命令が言い渡された[5]。

1.3. 内部不正とサイバー攻撃の狭間

従業員が素性を隠して自組織に金銭を要求する事件は、Sharp のケースだけではない。

2018 年 2 月、英国にある企業が身代金要求を伴うサイバー攻撃を受けた。同社の Ashley Liles は IT セキュリティアナリストとして本件を調査していたが、攻撃者の代わりに自身が身代金を受け取ることを思いついた。そして自社の役員の私的なメールに繰り返し不正アクセスを行い、実際の攻撃者が送信していた脅迫メールを改ざんし、当初指定されていた身代金の送付先を自身の暗号通貨ウォレットに変更した。また、メールアドレスを偽装して攻撃者になりすまし、自社に対して身代金の支払いを強く迫ったが、企業が応じることはなかった。Liles はこの直後に逮捕された。

そして 5 年以上が経過した 2023 年 5 月、彼はついに有罪を認めた[6] [7]。

上記の Sharp や Liles のケースは外部のハッカーを装った内部不正者の犯行であったが、Telegram にて、真偽は不明ながら、日本の銀行員を名乗る者が外部の協力者を募る投稿を発見した（図 1）。

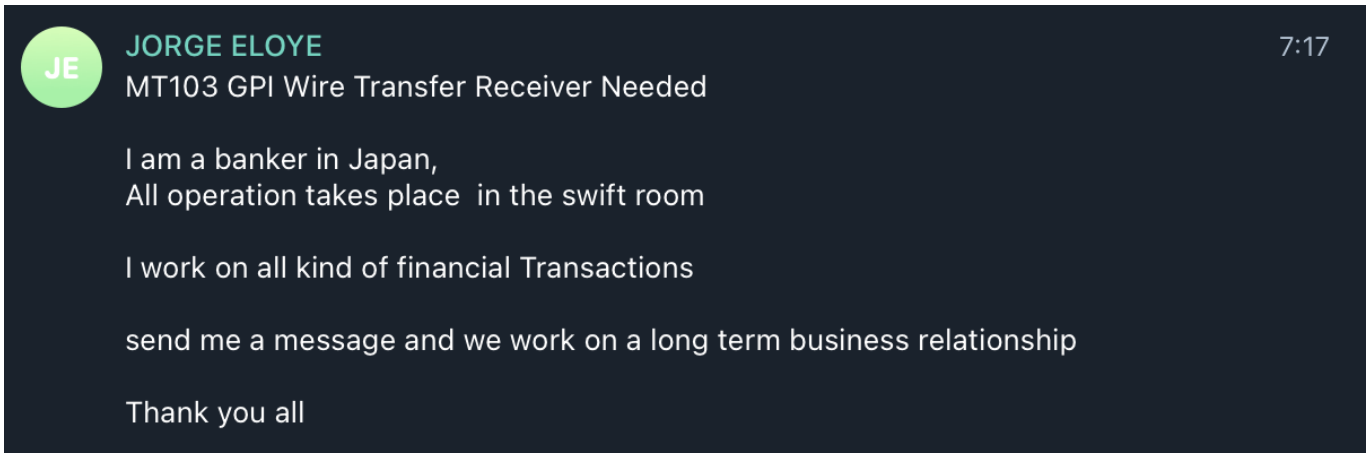

図 1 日本の銀行員と称する人物が投稿した、電信送金の受取人を募る投稿

和訳：私は日本の銀行員だ。全ての業務は SWIFT※ルームで行われており、私はあらゆる金融取引に従事している。
メッセージを送ってくれ。長期にわたって取引しよう。
※ 銀行間の国際金融取引に関するネットワークシステム

1.4. まとめ

多くの企業では、内部不正と外部からのサイバー攻撃をそれぞれ、カテゴリーの異なる事象として捉えており、管轄する部

[5] 出典：U.S. Department of Justice『Former Employee Of Technology Company Sentenced To Six Years In Prison For Stealing Confidential Data And Extorting Company For Ransom』
https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-sentenced-six-years-prison-stealing-confidential

[6] 出典：South East Regional Organised Crime Unit『Man convicted of blackmail and other offences』
https://serocu.police.uk/man-convicted-of-blackmail-and-other-offences/

[7] 出典：Bleeping Computer『IT employee impersonates ransomware gang to extort employer』
https://www.bleepingcomputer.com/news/security/it-employee-impersonates-ransomware-gang-to-extort-employer/

署も別である。しかし、今回紹介したように内部不正者がサイバー攻撃や外部の協力者を犯行に組み込む様々な事例が既に存在し、今後増える可能性も考えられる。それらに対応するために、組織間の連携を密にし、カテゴリーを跨ぐような事案に備えることが必要と考えられる。

2. 日本でも被害が広がり始めた SIM スワップ詐欺とその対策

2.1. 日本でも広がり始めた SIM スワップ詐欺

5 月 11 日、他人のスマートフォンの SIM カードを再発行して電話番号を乗っ取り、その電話番号を利用してネットバンキングで不正に送金したとして、警察庁は栃木県の女を逮捕した[8]。「SIM スワップ」と呼ばれる手法による詐欺で、今年 1 月に神奈川県の男が検挙されて以降[9]、日本でも被害事例が確認されてきている。


An official website of the United States government. Here's how you know

MORE ≡ > CONTACT US > FIELD OFFICES > SAN FRANCISCO > NEWS > PRESS RELEASES FBI Search FBI

SAN FRANCISCO

About News Wanted And Missing Persons Community Outreach Recruitment

FBI San Francisco
San Francisco Media Office
media.sf@fbi.gov

Twitter Facebook Email

March 6, 2019

FBI San Francisco Warns the Public of the Dangers of SIM Swapping

Criminals Are Targeting Victims with Cryptocurrency and Other Digital Currency Accounts

SAN FRANCISCO—The San Francisco Division of the Federal Bureau of Investigation (FBI) is seeking to warn potential victims of SIM swapping. Criminal actors engage in SIM swapping for the purpose of gaining access to the victim's digital currency accounts. Most of the individuals targeted are heavy investors in or early adopters of cryptocurrency.

図 2　FBI による SIM スワップへの注意喚起

米国ではおよそ 5 年前から被害が報告されており、最初の逮捕事例は 2018 年 7 月のことで[10,11]、その後も欧米を中心に被害が広がり続けてきた。FBI のサンフランシスコ支局は 2019 年 3 月[12]（**図 2**）以来、そしてユーロポールは 2020 年 3 月[13]以来、ユーザーや携帯電話キャリアに対して繰り返し注意を呼び掛けている。

このように海外では既に確認されていた手口だったが、日本ではこれまで公的機関からの注意喚起は行われていなかった。

2.2. SIM スワップとは

SIM（Subscriber Identity Module）カードは、契約者と電話番号とを紐づけ、4G や 5G といった電話回線を使った通信の処理を行う小型の IC チップである[14]。スマートフォンに装着することで、電話や SMS、インターネット通信等が利用できるようになる。一般的に電話番号を管理しているのはスマートフォン本体ではなくこの SIM カードであるため、例えば、同じスマートフォンでも、別会社の SIM カードに差し替えることで、別の電話番号で利用できるようになる。

しかし悪意を持つ者がこの仕組みを利用した場合、被害者になりすまし、携帯電話キャリアに SIM カードを再発行させる等

---

[8] 出典：産経新聞『スマホ乗っ取る「ＳＩＭスワップ」詐欺か　他人装い出金容疑で女逮捕　警視庁』
https://www.sankei.com/article/20230511-75NGJHDMMBJGZL2QFQMFUC3QLE/

[9] 出典：読売新聞『他人のＳＩＭカードを不正取得、偽造された運転免許証で…スマホ乗っ取り送金か』
https://www.yomiuri.co.jp/national/20230127-OYT1T50032/

[10] 出典：Bleeping Computer『Third SIM Swapper Arrested in the US』
https://www.bleepingcomputer.com/news/security/third-sim-swapper-arrested-in-the-us/

[11] 出典：VICE『'TELL YOUR DAD TO GIVE US BITCOIN:' How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers』
https://www.vice.com/en/article/a3q7mz/hacker-allegedly-stole-millions-bitcoin-sim-swapping

[12] 出典：FBI『FBI San Francisco Warns the Public of the Dangers of SIM Swapping』
https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/fbi-san-francisco-warns-the-public-of-the-dangers-of-sim-swapping

[13] 出典：Twitter『Europol』
https://twitter.com/europol/status/1238378996179574787

[14] 出典：NTT 西日本『SIM（Subscriber identity Module）カード』
https://www.ntt-west.co.jp/business/glossary/words-00067.html

して、被害者の電話番号を乗っ取る[15]。これが SIM スワップと呼ばれる攻撃手法であり、具体的な情報はハッカーフォーラム等で容易に見つけることができる。

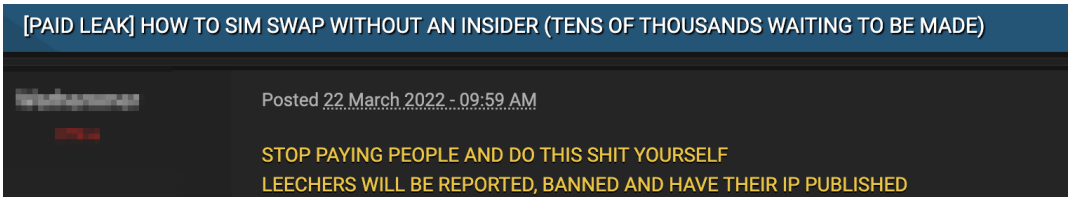

図 3　SIM スワップの実行方法に関するハッカーフォーラムの投稿(画像の一部を修正)
「内部関係者の手を借りずに SIM スワップをする方法」

例えば、攻撃者はまずフィッシング等でターゲットの個人情報を盗み、身分証明書を偽造する[16]。次に、携帯電話のキャリアのサポートに連絡して被害者になりすまし、SIM カード紛失・再発行の手続きを取ったり、他のキャリアに乗り換える MNP の手続きを行ったりすることで、同じ電話番号の新しい SIM カードを発行させる。これにより、攻撃者が持つ新しい SIM カードが有効となり、被害者の手元の SIM カードは無効となるため、電話番号への電話や SMS 等は被害者ではなく攻撃者のスマートフォンで受信されるようになってしまう。

こうして乗っ取りが完了した後は、電話番号を利用した SMS 認証等も突破できるようになり、銀行や暗号資産のアプリを利用し、被害者名義の口座から攻撃者の口座に送金させるといったことが可能になる。

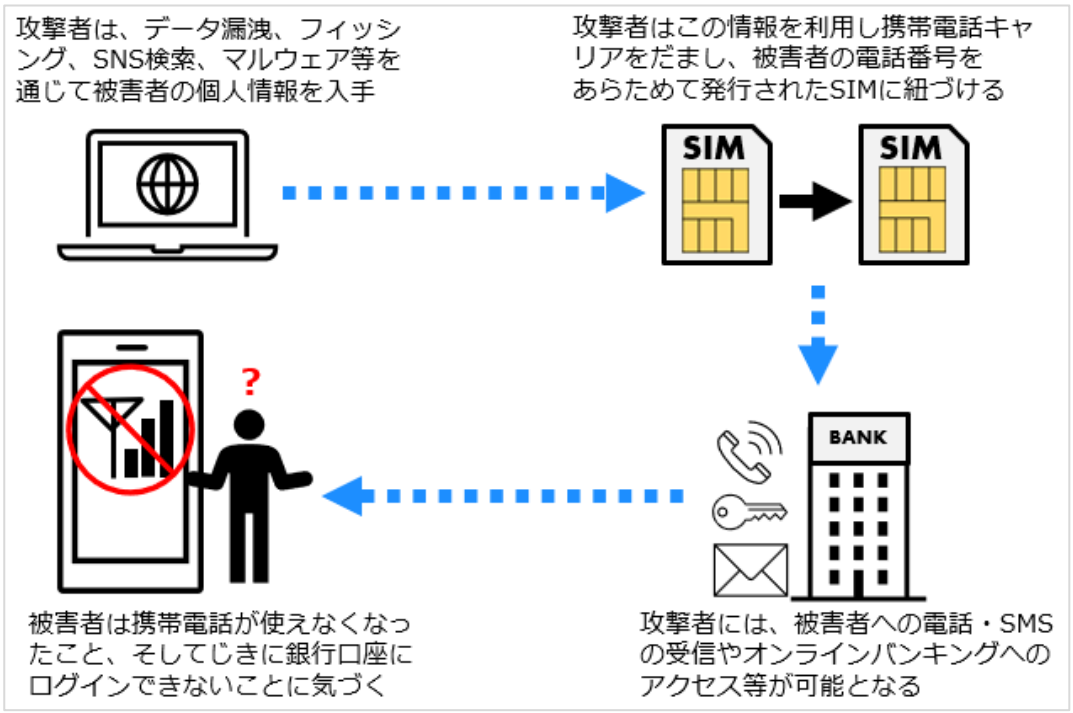

図 4　SIM スワップの模式図(ユーロポールの注意喚起を参考に日本語化・簡略化したもの)

[15] 出典：EUROPOL『SIM SWAPPING – A mobile phone scam』
https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/sim-swapping-%E2%80%93-mobile-phone-scam

[16] 出典：Norton Blog『What is SIM swapping? SIM swap fraud explained and how to help protect yourself』
https://us.norton.com/blog/mobile/sim-swap-fraud

2.3. SIM スワップの防御方法

SIM スワップ攻撃には、携帯電話キャリアのスタッフを加担させたり SIM カードを直接盗んだりする方法もあるが、多くの場合、攻撃者は被害者になりすます必要がある。なりすましによる攻撃およびその被害を最小化する方法として、FBI やユーロポール、セキュリティ企業等の注意喚起では、下記のような措置を推奨している[17,18]。

【なりすましからの防御】

なりすましを防ぐために、攻撃者のターゲットにされないよう、個人情報は非公開とすることが重要である。

例えば、資産（特に暗号資産）を有していること等を SNS 等で発信しないようにして、不用意に攻撃者の興味をひかないようにする。SNS やショッピングサイト等のインターネット上のサービスには、できるだけ個人情報を登録しないようにする。

また、なりすましを狙ったフィッシング攻撃を想定し、メールや SMS で届いた怪しいリンクやファイルを開かないようにする。

【攻撃された場合の被害の最小化】

SMS で受信した数字やキーワードを入力する SMS 認証は、SIM スワップ攻撃をされた場合に突破される恐れがあるため危険である。認証では SMS の利用を避け、FIDO（生体認証と公開鍵認証を利用し、サーバー側にパスワードを送信・保存しない方式）や、認証アプリや物理キーを使った多要素認証を実施することで、SIM スワップによる被害を最小化することができる。

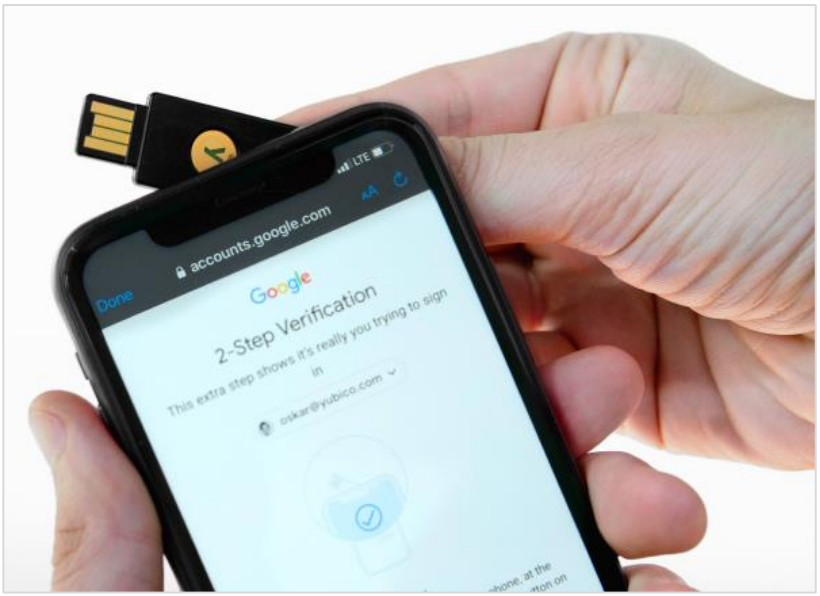

図 5 物理的なセキュリティキーを用いた認証の例[19]

[17] 出典：FBI『Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public』 https://www.ic3.gov/Media/Y2022/PSA220208

[18] 出典：EUROPOL『SIM SWAPPING – A MOBILE PHONE SCAM』 https://www.europol.europa.eu/cms/sites/default/files/documents/sim_swapping.pdf

[19] 出典：Yubico『Yubico Authenticator』 https://www.yubico.com/products/yubico-authenticator/

2.4. まとめ

日本でも SIM スワップによる被害事例が確認された。SMS 認証に過度に依存している場合、攻撃を受けると資産の損失を含む甚大な被害を受ける恐れがある。SIM スワップに備え、重要なサービスでは FIDO や認証アプリや物理キーを使った多要素認証を利用し、SMS を使った認証を避けることが重要である。

3. 警察庁、簡単なウェブサイト改ざん被害点検を呼びかけ

3.1. 警察庁の呼びかけ

警察庁は 5 月 8 日、ウェブサイトを設置している企業に対し、自社サイトに見覚えのないページが作成されていないかの確認を呼びかけ、Google 等のインターネット検索エンジンを応用した手法を紹介した（図 6）[20]。

ウェブサイト改ざんにより、身に覚えのない偽サイトが設置される被害は後を絶たないが、自社のウェブページが被害に遭わなければ気づきにくいため、長期間、犯罪者のビジネスに利用されるケースが少なくない。

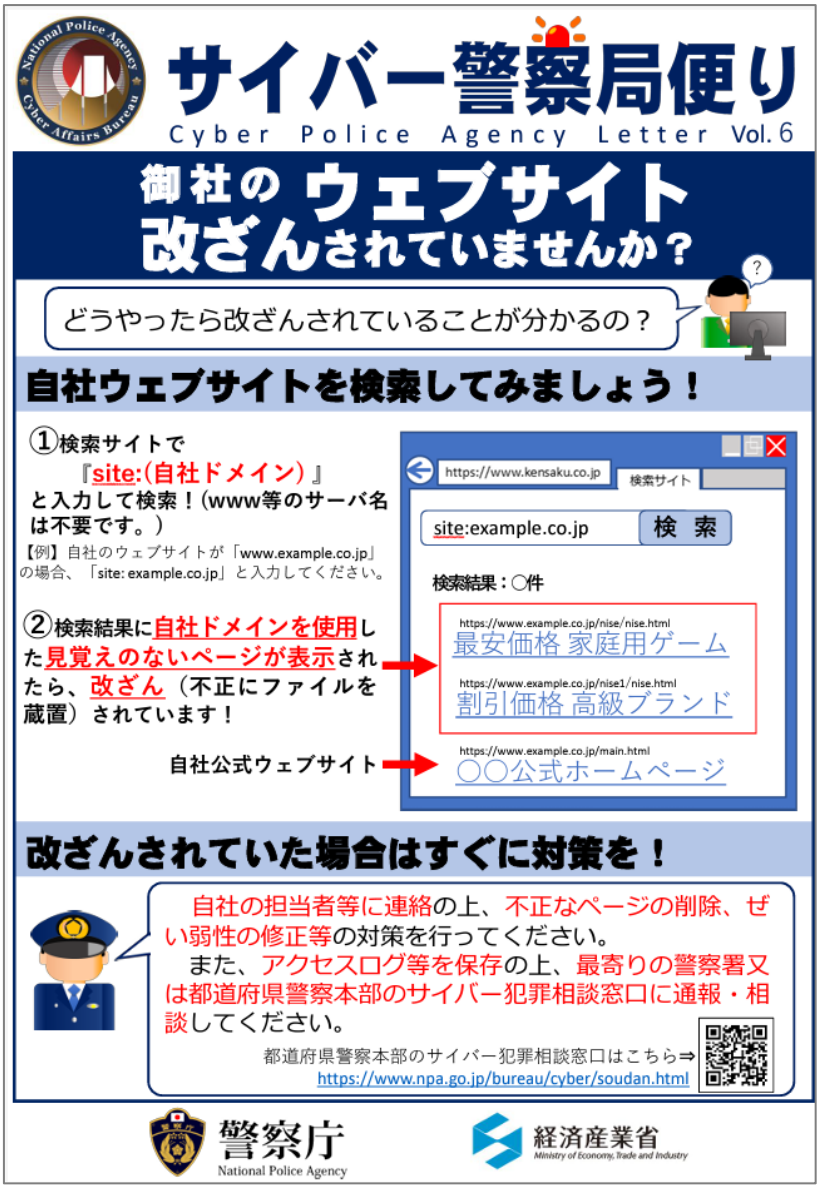

図 6 警察庁の「サイバー警察局便り」

[20] 出典：警察庁『サイバー警察局便り Vol.6「御社のウェブサイト改ざんされていませんか？」（注意喚起）』
https://www.npa.go.jp/bureau/cyber/pdf/Vol.6cpal.pdf

3.2. ウェブサイト改ざん被害の自己点検

【簡単な調査手法】

警察庁が紹介した方法は簡単で、Google 検索等の**検索サイトで『 site:○△□.jp 』など、『 site: 』の後に自社のウェブサイトのドメイン名を入力するだけ**[20]である(図 7)。

検索結果が出たら、作成した覚えのないページへのリンクが表示されていないか確認する。下の例のように事業に全く関係ないページが現れた場合、自社のウェブサイトが改ざんされている可能性が高い。

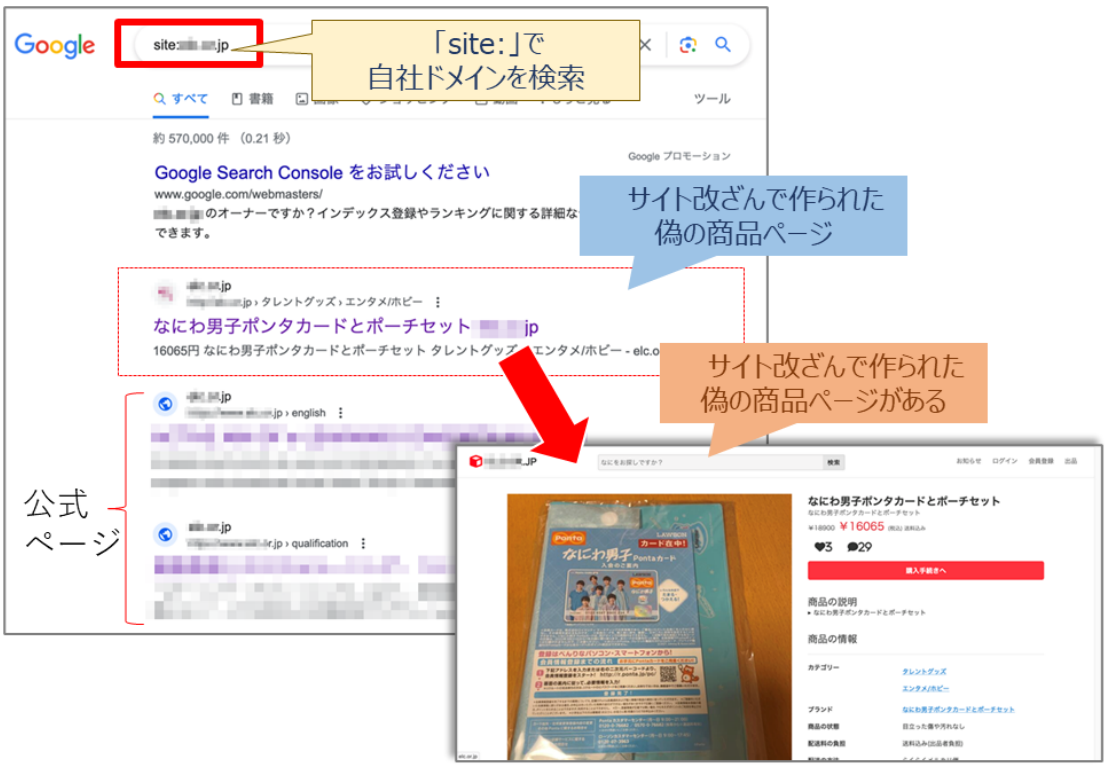

図 7 検索により実際に改ざんを発見した例

【インターネット検索とウェブサイト改ざん】

インターネット検索結果には上のような偽の商品ページへのリンクがしばしば表示される。これらの多くは攻撃者が企業サイト等を改ざんし設置したページで、偽ショッピングサイトへの誘導を狙ったものである（図 8）。偽ショッピングサイトでは、正規のショッピングサイトを模倣する等して、利用者から購入代金を騙し取ったり、粗悪品を販売したりする詐欺が行われている[21]。

攻撃者はウェブサイト改ざんの成功率を上げるため、インターネット上にあるサイトへ無差別に攻撃を行っており、脆弱なサイトが被害に遭うことが多い[22]。ウェブサイトが改ざんを受けても企業が作成した公式ページは変わりなく表示されるため、異常に気づくことは難しい。

---

[21] 出典：一般財団法人日本サイバー犯罪対策センター（JC3）『偽ショッピングサイトに注意』
https://www.jc3.or.jp/threats/topics/article-462.html

[22] 出典：警察庁『ウェブサイト改ざん対策』
https://www.npa.go.jp/bureau/cyber/countermeasures/hacked-website.html

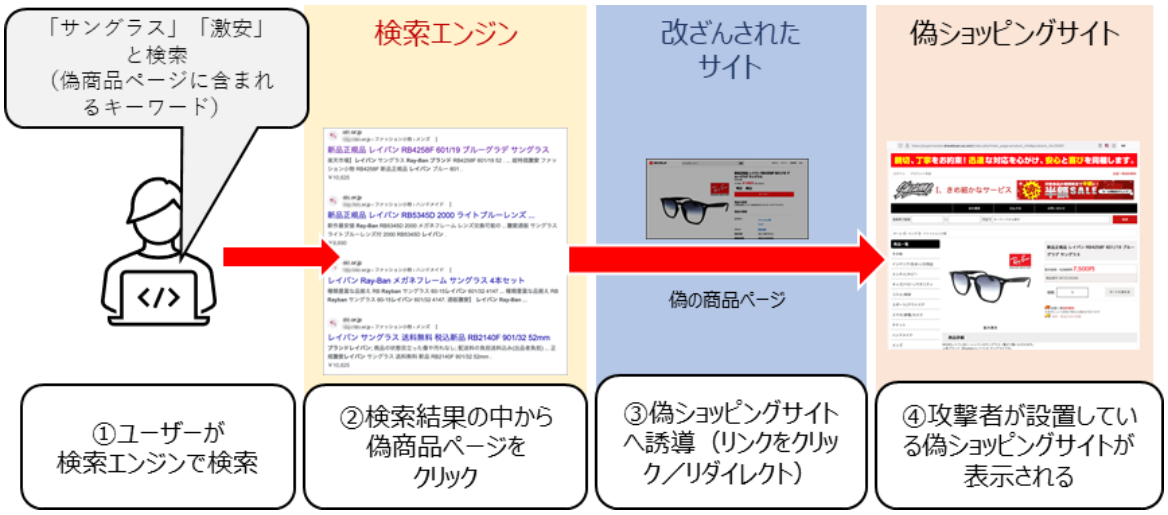

図 8 改ざんされたウェブサイトを利用した、偽ショッピングサイトへの誘導

【攻撃者の狙い】

企業サイト等の一般のサイトは検索エンジンから高評価を受け、検索結果の上位に表示されやすいが、偽ショッピングサイトは上位に表示されにくい。そこで攻撃者は企業サイトに寄生することで、検索結果の上位に効率的に表示させることを狙っていると考えられる(図 9)。

警察庁が紹介した調査方法は、上記の攻撃者の狙いを逆手にとったものである。

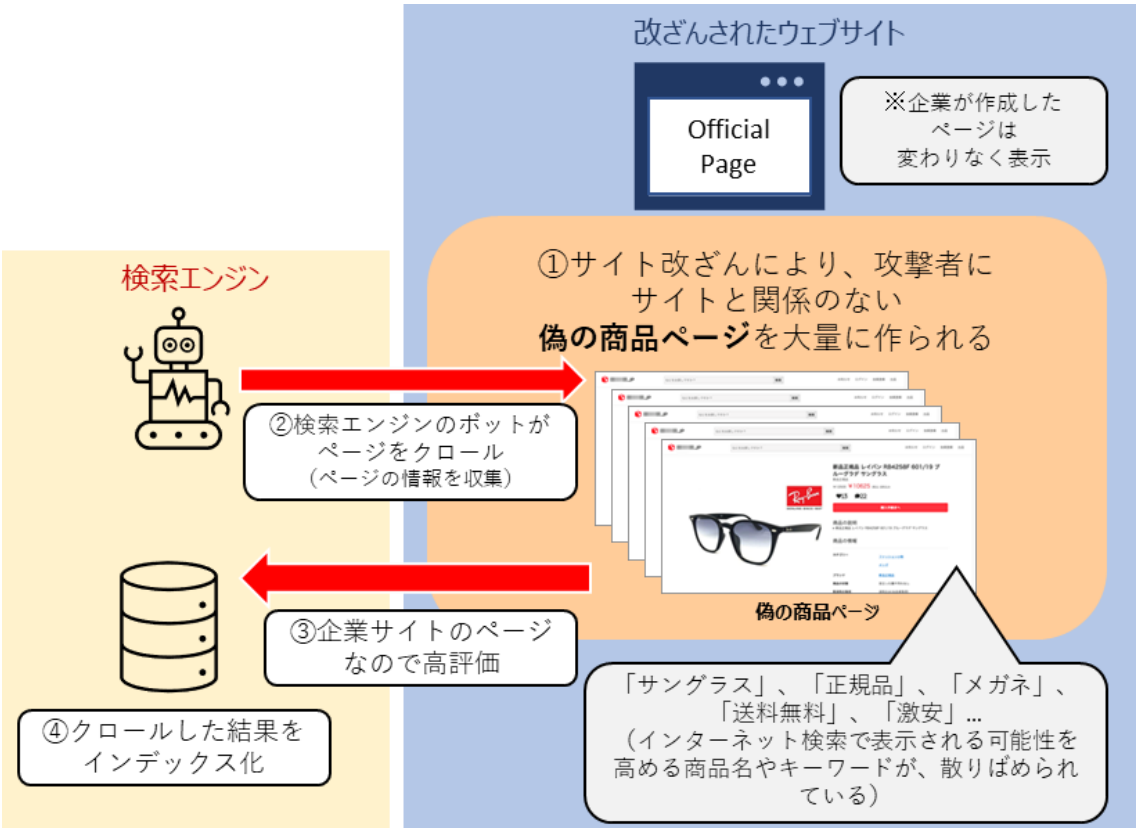

図 9 ウェブサイト改ざんによる偽の商品ページが、検索エンジンに登録される仕組み

3.3. Google Dorks による調査の活用

Google 検索を活用した調査手法は Google Dorks（グーグル・ドークス）と呼ばれている。Google Dorks で自社サイトを調査する事で、ウェブサイト改ざん等の攻撃被害を発見するだけでなく、管理上の不備を見つけることができる。

例えば、Google 検索で『 **intitle:"index of" site:○△□.jp** 』と自社ウェブサイトを検索すると、ディレクトリ画面を見つけることができる（図 10）。このようなディレクトリ画面を意図せず公開している場合、攻撃者に攻撃のヒントを与えたり、機密情報等の、外部から見えてはいけないファイルにアクセスできたりする可能性がある。そのため、発見したらディレクトリの設定を非公開に修正することが望ましい。

図 10 Google 検索で発見したディレクトリ画面

その他にもセキュリティ上有益な Google Dorks は多数存在する。以下はその一例である（表 1）。

検索キーワード （※ ○△□.jp は自社ウェブサイト）	調査目的	備考
inurl:backup site:○△□.jp	「backup」の文字列を含む URL で、バックアップデータを公開していないか確認	バックアップデータに機密情報が含まれている場合がある
ext:log site:○△□.jp	拡張子が「.log」のログデータを公開していないか確認	ログに ID/パスワードが含まれている場合がある

表 1 Google Dorks の検索キーワードの例

3.4. まとめ

Google Dorks は、一つ一つウェブページを調べていたのでは時間がかかるような広い範囲を効率的に調査し、セキュリティ上の問題や管理上のミスを発見することができる便利な手法である。自社に合わせた活用方法を探してみてはいかがだろうか。

以上

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　OSINT モニタリングチーム
メールアドレス： WA_Advisorysupport@ntt.com