サイバーセキュリティレポート

2022.10

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

【当レポートについて】

当レポートでは 2022 年 10 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『退職した社員による元・勤務先への不正アクセス事件』

- 2022 年 10 月、静岡県警は、元勤務先の会社に不正アクセス等を行った容疑で、男性を逮捕した。
- 男性は在職中に私物のスマートフォンで元勤務先のネットワークに VPN 接続できるようにしており、退職後に不正アクセスを行い、システム内の重要なファイルを削除したとみられている。
- 内部不正は一般に、機会・動機・正当化の「不正のトライアングル」が揃うことで発生すると考えられている。今回の事件も「不正のトライアングル」を防ぐ対策を適切に実施していれば、発生を防げた可能性が高い。

第 2 章『日本政府、暗号資産を狙う攻撃の実行犯として北朝鮮の関与を指摘』

- 日本の金融庁、警察庁、内閣サイバーセキュリティ―センター（NISC）は合同で、北朝鮮のサイバー攻撃グループ「ラザルス(Lazarus)」が日本の暗号資産関連企業への攻撃を行ったとする文書を公開した。
- ラザルスはソーシャルエンジニアリングを主体とした攻撃手法を得意としており、主に金融機関を対象としている。セキュリティ企業のカスペルスキー社は「金融業界に対する大規模攻撃で最も成功したグループの 1 つ」であると評している。
- 日本政府は、実行犯を名指しすることや攻撃手法を公開する「パブリック・アトリビューション」を行うことで、国民への周知や将来の攻撃を抑止することを狙っていると考えられる。

第 3 章『トヨタ自動車が個人情報漏洩の可能性』

- トヨタ自動車は、個人情報を保管するサーバーへのアクセスキーを含んだソースコードが、GitHub で 5 年間にわたり第三者からアクセスできる状態となっていたことを発表した。
- 攻撃者の中には、認証情報を利用して組織への侵入を試みるために、GitHub で公開されている認証情報の漏洩を探す者がいることが知られている。
- 公開を目的としていないソースコードは、非公開リポジトリを使用することを徹底する等、セキュリティに配慮した環境を整備することが開発において重要である。

1. 退職した社員による元・勤務先への不正アクセス事件

1.1. 概要 [1]

2022 年 10 月 3 日、静岡県警は不正アクセス禁止法違反で浜松市の男性を逮捕した。2021 年 12 月下旬、元勤務先の OA 機器販売会社のサーバーに不正アクセスしたとされ、男性は容疑を認めている。犯行動機等は捜査中で、他にも新たなアカウントを追加設定して重要なファイルへアクセスできるようにし、さらに、ファイルの消去等も行ったとみられている[2]。

静岡県警によれば、このような不正アクセス事件は全国的にも珍しいという[3]。

1.2. 元勤務先への不正アクセス

【不正アクセスの準備】[4]

容疑の男性は、2021 年 1 月まで、OA 機器販売会社の浜松市にある営業所に勤務し、サーバー管理などを行うメンテナンス部に所属していた。在職中に規則に反し、社内ネットワークに接続できる VPN に私物のスマートフォンを登録・設定しており、そのまま退職していた。（図 1 左）

【不正アクセスとデータ消去を実行】[5]

退職から約 1 年後の 2021 年 12 月 31 日、年末年始の会社の休業期間を狙い、男性は社内ネットワークに不正アクセスを行った。（図 1 右）

予め登録してあったスマートフォンで VPN に接続して社内ネットワークに侵入した後、人事や経理についての情報が入っている重要なシステムである管理システムへ、在職時に記憶していたパスワードを使用してアクセス[6]した。さらに、管理システムで認証するための証明書を発行して自身の PC に導入し、スマートフォンよりも処理能力の高い PC で外部から直接管理システムにアクセスできるようにした。そして、管理システムにある重要なフォルダーにアクセスできるよう新たなアカウントを追加設定した。

この不正な設定変更の容疑により私電磁的記録不正作出・同供用の容疑で再逮捕されている[7]。報道によれば、さらに、フ

---

[1] 出典：静岡県警察『県内事件・事故速報』
https://www.pref.shizuoka.jp/police/about/koho/10/1003.html
https://www.pref.shizuoka.jp/police/about/koho/10/1020.html

[2] 出典：静岡新聞『不正アクセス事件　業務上データ消去か　静岡県警、業務妨害視野に捜査』
https://www.at-s.com/news/article/shizuoka/1132055.html

[3] 出典：静岡新聞『元勤務先に不正アクセスか　特殊データ悪用　静岡県警など男を逮捕』
https://www.at-s.com/news/article/shizuoka/1131776.html

[4] 出典：静岡朝日テレビ『元勤務先の管理システムに不正にアクセスか　49 歳の男を逮捕　静岡県警』
https://look.satv.co.jp/_ct/17574771

[5] 出典：静岡新聞『元勤務先に不正アクセスか　特殊データ悪用　静岡県警など男を逮捕』
https://www.at-s.com/news/article/shizuoka/1131776.html

[6] 出典：静岡新聞『会社のＰＣ窃盗疑い　不正アクセスの元社員再逮捕　静岡南署など』
https://www.at-s.com/news/article/shizuoka/1148521.html

[7] 出典：静岡新聞『不正アクセス事件　追加設定しデータ閲覧か　静岡南署など元社員を再逮捕』
https://www.at-s.com/news/article/shizuoka/1139190.html

ォルダー内に有った数万件の受発注等に関する記録を消去したという[8]。

【余罪】[9]

逮捕後の取り調べで、不正アクセス実行前の 2021 年 12 月 4 日には、元勤務先の営業所に侵入して PC 1 台を盗んだ疑いがあることも判明し、静岡県警は窃盗と建造物侵入で男性を再逮捕した。このことから、盗んだ PC についての受発注記録を消すために不正アクセスをした可能性が考えられている。

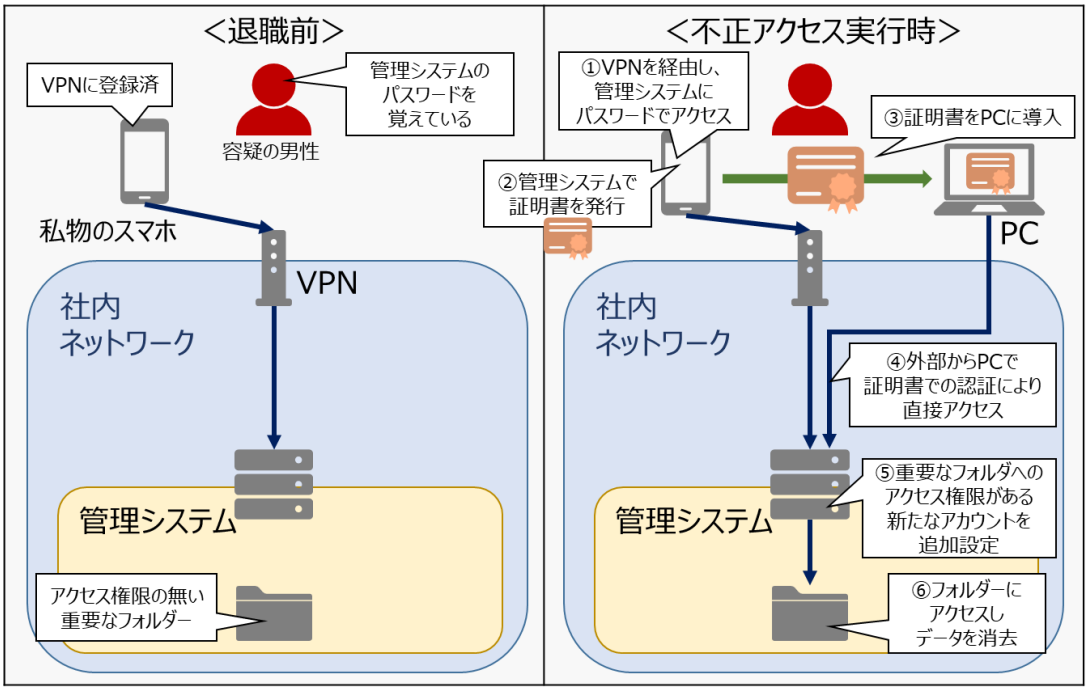


図 1 不正アクセスの模式図（報道を元に作成）

1.3. まとめ

システム内部への侵入によるデータ破壊はランサムウェアで注目されているが、アクセス権限を有する従業員や元従業員の内部不正でも起こり得る。

一般に、内部不正の発生は、米国の組織犯罪研究者ドナルド・R・クレッシーが提唱する「不正のトライアングル」モデルで考えられている。従業員はシステム内部でのアクセス権限を有し、重要情報にアクセスする「機会」がある。加えて、現在の処遇への不満、金銭問題を抱えているといった「動機」、不当に感じる待遇に復讐したいといった「正当化」する条件が揃うと不正が発生する（図 2）[10]。

組織が能動的に実施可能な「やりにくくする」「割に合わない」「やると見つかる」「言い訳させない」「その気にさせない」対策に

[8] 出典：静岡新聞『不正アクセス事件　業務上データ消去か　静岡県警、業務妨害視野に捜査』
https://www.at-s.com/news/article/shizuoka/1132055.html

[9] 出典：静岡新聞『会社のＰＣ窃盗疑い　不正アクセスの元社員再逮捕　静岡南署など』
https://www.at-s.com/news/article/shizuoka/1148521.html

[10] 出典：独立行政法人 情報処理推進機構『組織の内部関係者の不正行為による情報漏えいを防止するため、セキュリティ対策の見直しを！』
https://www.ipa.go.jp/security/announce/20140710-insider.html

より、不正のトライアングルのうち「機会」「正当化」に対抗することが有効である[11]。

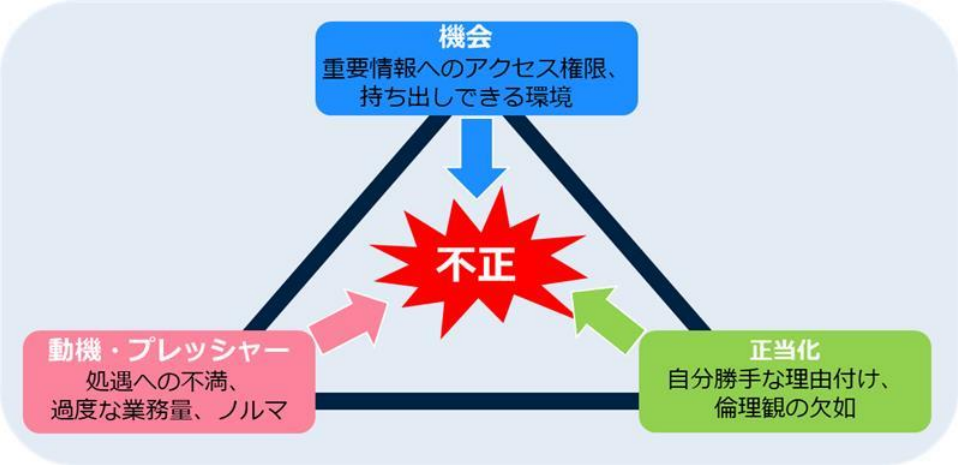


図 2 セキュリティ対策における内部不正のトライアングル
（IPA 記事を元に作成）

今回の不正アクセス事件も、適切な内部不正対策を講じていれば防げた可能性が高い。例えば、退職後にアクセスしないよう誓約書を提出させ「言い訳させない」ためのけん制をする。社員証や貸与機器等を返却（BYOD の場合は登録されているハードーウェアキーの削除）させ、退職直後には元従業員の ID/パスワードを確実に削除し、アクセスの機会自体を無くす。

また、VPN や社内ネットワーク、管理システムのログを監視し、定期的に情報資産の棚卸をして不正な機器の登録や ID の削除漏れ等が無いか確認することで、在職中・退職後を問わず不正アクセスを「やりにくくする」「やると見つかる」ようにする。

加えて、懲戒処分を規定した就業規則等を整備して、在職中から内部不正防止のルール化と周知徹底を行い従業員に対する教育を定期的に実施して、退職後の不正を予防することも重要である。

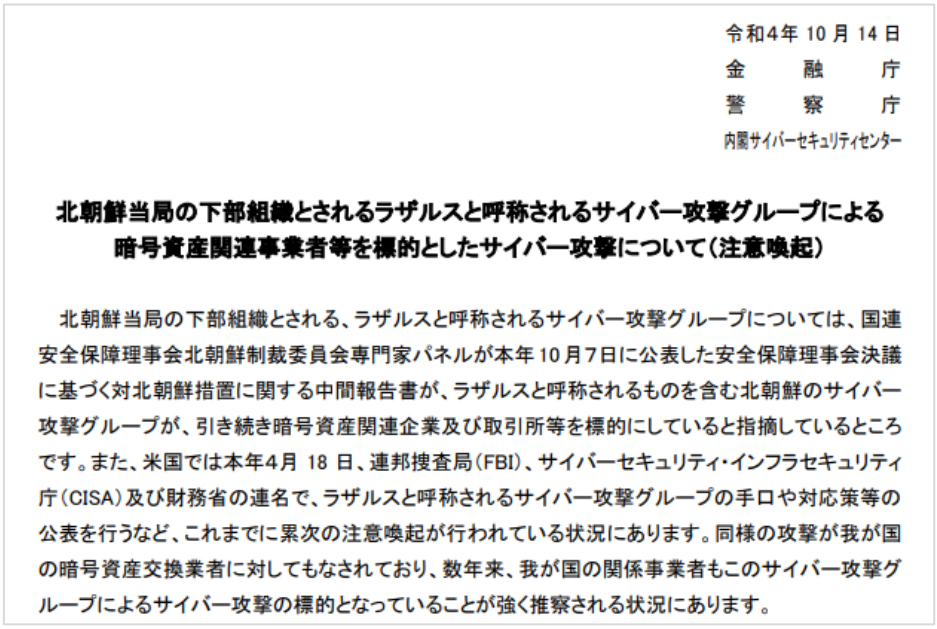
[11] 出典：独立行政法人 情報処理推進機構『組織における内部不正防止ガイドライン』
https://www.ipa.go.jp/security/fy24/reports/insider/

2. 日本政府、暗号資産を狙う攻撃の実行犯として北朝鮮の関与を指摘

2.1. 概要

10 月 14 日、金融庁、警察庁、内閣サイバーセキュリティ―センター（NISC）は合同で国民への注意喚起文書を発表した[12]。この文書では、北朝鮮政府の関与する「ラザルス（Lazarus）」というグループが日本の暗号資産関連業者等に対して攻撃を行ったと指摘すると共に、同グループがこれまで世界中で実行してきた攻撃の特徴や、リスク低減のための推奨対策が説明されている。

また、警察庁の露木長官は 10 月 20 日の定例記者会見で、同様の指摘を行うとともに、北朝鮮当局が関与していることから、今後も攻撃を継続する可能性が高いと注意を呼び掛けた[13]。



令和4年 10 月 14 日
金　　融　　庁
警　　察　　庁
内閣サイバーセキュリティセンター

北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）

北朝鮮当局の下部組織とされる、ラザルスと呼称されるサイバー攻撃グループについては、国連安全保障理事会北朝鮮制裁委員会専門家パネルが本年 10 月7日に公表した安全保障理事会決議に基づく対北朝鮮措置に関する中間報告書が、ラザルスと呼称されるものを含む北朝鮮のサイバー攻撃グループが、引き続き暗号資産関連企業及び取引所等を標的にしていると指摘しているところです。また、米国では本年4月 18 日、連邦捜査局（FBI）、サイバーセキュリティ・インフラセキュリティ庁（CISA）及び財務省の連名で、ラザルスと呼称されるサイバー攻撃グループの手口や対応策等の公表を行うなど、これまでに累次の注意喚起が行われている状況にあります。同様の攻撃が我が国の暗号資産交換業者に対してもなされており、数年来、我が国の関係事業者もこのサイバー攻撃グループによるサイバー攻撃の標的となっていることが強く推察される状況にあります。

図 3　金融庁、警察庁、NISC 合同の注意喚起 [12]

2.2. 北朝鮮の「ラザルス」とは

ラザルスは、北朝鮮政府が関与するサイバー犯罪集団であり、「HIDDEN COBRA」等の様々な別名でも知られている[14]。

グループの正確な起源は明らかになっていないが、最初に確認された攻撃は、2009 年に米国と韓国の政府系 Web サイトに対して行われた DDoS 攻撃であった[15]。

---

[12] 出典：警察庁『北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）』
https://www.npa.go.jp/news/release/2022/20221014001.html

[13] 出典：朝日新聞デジタル『北朝鮮、暗号資産狙ったサイバー攻撃か　警察庁の新設部隊が分析』
https://www.asahi.com/articles/ASQBN4F2YQBNUTIL007.html

[14] 出典：MITRE ATT&CK『Lazarus Group, Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Group G0032』
https://attack.mitre.org/groups/G0032/

[15] 出典：Harvard International Review『The Cybercrime Syndicate Financing the North Korean State』
https://hir.harvard.edu/the-cybercrime-syndicate-financing-the-north-korean-state/

主に銀行や金融機関への攻撃を行っており、セキュリティ企業のカスペルスキー社はラザルスを「金融業界に対する大規模攻撃で最も成功したグループの 1 つ」であると評している[16]。米国の諜報機関は、北朝鮮は長年の国際的な制裁により経済難にあり、ラザルスのサイバー攻撃は**同国政府の集金手段の一つになっている**と指摘する [15]。また、同グループが窃取した資金は核開発やミサイル開発での利用が疑われている [15]。

ラザルスは金融機関以外の企業を標的とすることもあり、2014 年には、ソニーピクチャーズ社が、金正恩の暗殺をテーマにしたコメディ映画『THE INTERVIEW』を公開しようとしていたことに関連し、同社に対して攻撃を行っている。これは従業員の個人情報や機密情報を漏えいさせ、さらに内部サーバーの 75%を破壊し、結果として映画は一旦公開中止になった[17]。

図 4「THE INTERVIEW - Official Teaser Trailer」より [18]

2018 年 9 月、米司法省はこのソニーピクチャーズに対する攻撃や 2017 年の「WannaCry」ランサムウェア攻撃に関与したとして、ラザルスのメンバーである北朝鮮国民パク・ジニョク容疑者を訴追[19]。現在も指名手配中である[20]。

[16] 出典：Kaspersky『LAZARUS UNDER THE HOOD』
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf

[17] 出典：日経 XTECH『ソニーピクチャーズ、問題の映画「The Interview」を公開中止』
https://xtech.nikkei.com/it/atcl/news/14/121802308/

[18] 出典：YouTube『THE INTERVIEW - Official Teaser Trailer』
https://www.youtube.com/watch?v=Mj3uHftd5FQ

[19] 出典：ZDNet JAPAN『米司法省、北朝鮮人ハッカーを訴追--「WannaCry」やソニー攻撃に関与』
https://japan.zdnet.com/article/35125225/

[20] 出典：FBI『PARK JIN HYOK』
https://www.fbi.gov/wanted/cyber/park-jin-hyok

図 5 パク容疑者の指名手配書 [20]

2.3. パブリック・アトリビューション

今回の日本政府が発表した文書や、その後の記者会見での表明のように、攻撃者の摘発に至らなくともサイバー攻撃の実行者や背後にいる政府組織を指摘する行為は「**パブリック・アトリビューション**」と呼ばれる。

パブリック・アトリビューションは、いわゆる「ファイブアイズ（Five Eyes）」諸国によって行われることが多い。例えば、2020 年 12 月に発覚した SolarWinds 社への攻撃について、ファイブアイズ構成国は 2021 年の 4 月に非難を表明した。アメリカ、イギリスの両政府は、ロシア対外諜報庁（SVR）を、それにつづいてカナダ、オーストラリア、ニュージーランド政府もロシア政府を非難した。

【効果】

日本の防衛研究所（NIDS）研究員の瀬戸崇志氏は、パブリック・アトリビューションには主に「**抑止**」、「**対処・防御**」、「**規範設定**」という 3 つの効果があると述べている[21]。

「抑止」は、相手を名指しすること、攻撃手法を公開すること、さらに刑事訴追や制裁、サイバー攻撃による反撃等を示唆することで将来の攻撃を思いとどまらせる効果がある。

「対処・防御」は、抑止の効果が上がらない場合でも、攻撃能力の無力化や被害の軽減が期待できるというものである。例えば、攻撃手法を公開することによって、政府機関や民間企業へ周知が進み、攻撃の検知を早くする、被害を局所化するといった効果がある。

[21] 出典：防衛研究所 NIDS コメンタリー『瀬戸崇志　国家のサイバー攻撃とパブリック・アトリビューション』
http://www.nids.mod.go.jp/publication/commentary/pdf/commentary179.pdf

「規範設定」は、発生したサイバー攻撃が既存の国際法に照らして違法、または合法であっても許容しがたいという評価を示すことで、新たな規範設定の布石となり、将来の慣習国際法の形成にも影響する、という効果である。

日本の過去のパブリック・アトリビューションの事例としては、2017 年に「WannaCry」のサイバー攻撃で北朝鮮を非難する外務省の談話や、2021 年に中国系のハッカーグループが行った宇宙航空研究開発機構（JAXA）への攻撃に関する警察庁長官の発表等が挙げられる [13]。

2.4. 発表された文書について

今回、日本の政府機関により発表された文書は、「**北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）**」と銘打たれている。

【事件について】

文書では、特定の事件を明示していない。大手メディアによると、関係者への取材や公開されている過去の事例から、今回指摘されているのは 2018 年の暗号資産交換所「Zaif（ザイフ）」からビットコイン約 67 億円相当分が盗まれた事件や、2019 年に「ビットポイントジャパン」から 35 億円相当のリップル（暗号資産）が消失した事件のことと推定されている[22]。

【推奨対策】

ラザルスは、近年、暗号資産関連業者を対象とした攻撃を行っており、「標的企業の幹部を装ったフィッシング・メールを同組織の従業員に送る」、「虚偽のアカウントを用いた SNS を通じて、取引を装って標的企業の従業員に接近する」等の方法により「マルウェアをダウンロードさせ、そのマルウェアを足がかりにして標的のネットワークへアクセスする」といった、いわゆるソーシャルエンジニアリングを用いることが確認されている。

ただ、ラザルスはソーシャルエンジニアリング以外にも多様な手口を駆使しているため、今回発表された文書では様々なリスク低減対策が紹介されている。例を挙げると、「端末の保護（いわゆるエンドポイント・プロテクション等）の実施」、「秘密鍵のオフラインでの保存」、「自社を装ったフィッシングサイトへの注意」がある。

2.5. まとめ

日本政府は今回の文書や警察庁長官による記者会見で、ラザルスによる犯行の手口を公開し、北朝鮮政府が関与していると名指しで指摘した。前述のように、政府によるパブリック・アトリビューションは、発表を見た自国民がセキュリティ対策を実施することを期待している。ラザルスによる攻撃は今後も継続することが推測されている状況であり、金融機関は特に注意を要する。また、ソーシャルエンジニアリングを主体とした攻撃手法は近年拡がりを見せており、他の業界においても最新のソーシャルエンジニアリング手法について常にアップデートを行い、対策を進めることを推奨する。

[22] 出典：読売新聞オンライン『北のハッカー集団、日本の暗号資産狙い攻撃か…警察庁が異例の名指し公表』
https://www.yomiuri.co.jp/national/20221015-OYT1T50014/

3. トヨタ自動車が個人情報漏洩の可能性

3.1. 概要

2022 年 10 月、トヨタ自動車と子会社のトヨタコネクティッド（以下、両社を総称してトヨタ自動車）は、車が通信することでサービスを提供するコネクティッドサービス「T-Connect」の顧客情報（メールアドレスおよび管理番号）29 万 6,019 件が漏洩した可能性があると発表した[23]。開発委託先の企業が誤って GitHub（ソースコードをクラウドに保管し、他者とコラボレーションしながら開発することを容易にする Web サービス[24]）で公開していた T-Connect のソースコードにデータサーバーへのアクセスキーが含まれており、同サーバーに保管されている顧客情報にアクセスできる状態となっていた。

図 6 トヨタ自動車のプレスリリース

3.2. GitHub の誤設定

トヨタ自動車の T-Connect は、リアルタイムの走行情報や、トヨタスマートセンターで収集したビッグデータ等を使って最適なルートをナビに配信[25]したり、24 時間 365 日、オペレーターに口頭で情報の検索や配信を依頼[26]したりすることが可能なサービスである。

図 7 T-Connect のオペレータサービス紹介動画

[23] 出典：TOYOTA『お客様のメールアドレス等の漏洩可能性に関するお詫びとお知らせについて』
https://global.toyota/jp/newsroom/corporate/38095972.html

[24] 出典：TechTarget『GitHub』
https://www.techtarget.com/searchitoperations/definition/GitHub

[25] 出典：TOYOTA『最適な情報を提供してくれるから安心：ハイブリッドナビ』
https://toyota.jp/tconnectservice/service/hybridnavi.html

[26] 出典：トヨタ YouTube ショールーム『【T-Connect】オペレーターサービス（コネクティッドカー用）』
https://www.youtube.com/watch?v=n-ahkfmBo8Q

トヨタ自動車の発表によると、2017 年 12 月、T-Connect の開発委託先企業が、取扱規則に違反しソースコードの一部を誤って公開設定のまま GitHub へアップロードした。それ以来 5 年間にわたり、第三者がソースコードにアクセスできる状態となっていた。

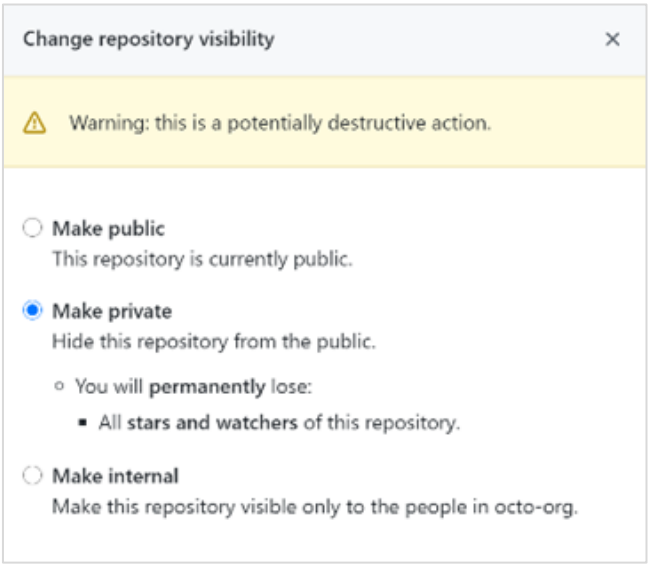


図 8 GitHub のソースコード公開レベルの設定 [27]

インターネットに公開されていたソースコードには、トヨタ自動車のデータサーバーへのアクセスキーが含まれていた。もし何者かがこのソースコードからアクセスキーを見つけ出し、データサーバーにアクセスした場合、顧客情報の窃取等の被害が発生するおそれがあった。トヨタ自動車はソースコードを直ちに非公開化し、データサーバーのアクセスキーを変更する等の対応を行った。また、サーバーのアクセス履歴を検証した結果について、第三者によるアクセスは確認できなかったが、完全に否定することもできないと述べている。

3.3. GitHub に公開された認証情報を狙う攻撃者

攻撃者の中には、GitHub に公開されたソースコードを、ボットを使用して絶えずスキャンしている者がいる。ソースコードに直接記述された認証情報を探し出し、この情報を利用して組織への侵入を試みるためと考えられる[28]。ある実験で、ハニーポットとして SSH のユーザー名とパスワードを GitHub でわざと漏洩させ、第三者がそれを見つけるかどうかを試したところ、漏洩からわずか 34 分後に最初の不正ログインが行われた[29]。

GitHub には、認証情報を含むソースコードをアップロードした場合に管理者へ通知が送信される「シークレットスキャン」機能がある[30]。しかし、シークレットスキャンが認証情報を見落とす可能性は否定できないため、過信すべきではない。また、管理者

[27] 出典：GitHub Docs『Setting repository visibility』
https://docs.github.com/ja/repositories/managing-your-repositorys-settings-and-features/managing-repository-settings/setting-repository-visibility

[28] 出典：CSO『How corporate data and secrets leak from GitHub repositories』
https://www.csoonline.com/article/3634784/how-corporate-data-and-secrets-leak-from-github-repositories.html

[29] 出典：CRAIG HAYS『What Happened When I Leaked My Server Password on GitHub.com』
https://craighays.com/what-happened-when-leaked-server-password-github/

[30] 出典：Microsoft『シークレット スキャンとは』
https://learn.microsoft.com/ja-jp/training/modules/configure-use-secret-scanning-github-repository/2-what-is-secret-scanning

は GitHub からの通知を見落とさないよう、注意する必要がある。

3.4. 過去の GitHub での漏洩事件[31]

GitHub でソースコードを誤って公開する事件は過去にも発生しており、2021 年 1 月には、三井住友銀行(SMBC)が、事務系システムのソースコードが流出したことを発表した。委託先企業の開発者が、自身で作成したソースコードから年収を診断できる Web サービスを利用するため、所有するコードを公開設定のまま、GitHub にアップロードしたのが原因であった。

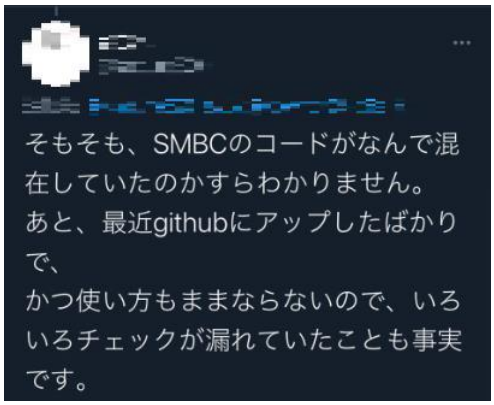


図 9 SMBC 関連のソースコードを GitHub にアップロードしたとみられる人物のツイート

3.5. GitHub を使う場合に注意すべきこと

今回のトヨタ自動車の情報漏洩（可能性）インシデントは、ソースコードを公開状態にしていたこと、さらにそのソースコードにデータサーバーの認証情報が含まれていたことにより引き起こされていた。いずれも GitHub でのソースコード管理がずさんだったことを窺わせるが、これらの問題は、公開を目的としていないソースコードは非公開リポジトリを使用することを徹底する、さらに認証情報は環境変数に記述しソースコードに含まない等、セキュリティに配慮した開発環境を整備することで防ぐことができる。現代的、効率的な開発には、GitHub といったコラボレーションツールは欠かせない。このようなツールのリスクを理解した上で、開発体制の整備の段階からセキュリティを担保し、計画的に導入することが重要である。

以上

[31] 出典：ITmedia NEWS『三井住友銀行などのソースコードが流出 “年収診断”したさに GitHub に公開か【追記あり】』 https://www.itmedia.co.jp/news/articles/2101/29/news107.html

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