サイバーセキュリティレポート

2022.09

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 9 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『Uber 社のハッキング被害』

- Uber 社がハッキンググループである LAPSUS$に社内ネットワークへと侵入され、多数の社内システムの権限を奪われた事件が明らかになった。
- LAPSUS$は、MFA 疲労攻撃等のソーシャルハッキングを駆使して多要素認証を突破する手法を特徴とし、Uber 社以外にもこれまで Microsoft、NVIDIA、Samsung といった多数の有名な大企業への侵入に関与してきた。
- LAPSUS$が得意とするソーシャルハッキングはランサムウェアグループ等にも広まる恐れがあり、最新のソーシャルハッキングを意識してユーザー教育や多要素認証の強化といった対策を継続して実施することが重要である。

第 2 章『アルバニアがサイバー攻撃を理由に、イランとの国交断絶を表明』

- 2022 年 7 月、政府ポータル e-Albania.al がサイバー攻撃によって一時停止した。同年 9 月、アルバニア政府は、この攻撃にイランが関与したとして国交断絶を発表した。
- Microsoft 社の分析によると、攻撃を実行したのは、イランの情報安全保障省（MOIS）傘下にある 4 つのグループであった。
- 国家的なサイバー攻撃が軍事的な攻撃と同等に捉えられる恐れが強まる中、サイバー攻撃を理由に国交が断絶する世界初の事態が起きた。攻撃の事実確認の難しい国家間のサイバー攻撃について、国際的な仲裁等の仕組みが必要になってくると考えられる。

第 3 章『米政府、政府機関が調達するソフトウェアに新たなセキュリティ対策を義務付け』

- 9 月 14 日、米国行政管理予算局は、米国政府機関が新たに調達するソフトウェアについてセキュリティ要件を強化するガイダンスを発表した。
- 新しいソフトウェアの導入前に、開発者に「安全なソフトウェア開発フレームワーク」と「ソフトウェアサプライチェーンセキュリティガイダンス」を遵守していることを証明させることが必要になり、また、公募時に、ソフトウェア部品表(SBOM)の提示を求めることもできるようになった。
- このガイダンスは政府機関だけでなく、一般企業のソフトウェア調達や利用におけるセキュリティ改善にも役立てられる可能性がある。

1. Uber 社のハッキング被害

1.1. 概要 [1]

2022 年 9 月 15 日、配車サービス等を手掛ける Uber 社がハッキンググループである LAPSUS$のサイバー攻撃を受けて社内ネットワークに侵入され、多くの社内システムの権限を奪われたことが明らかになった（図 1）。Uber 社のような多要素認証(MFA)で守られた大企業のシステムであっても、ソーシャルハッキングを駆使されると社内システムの奥まで侵入されて被害に遭うということを、今回の事件は証明した。

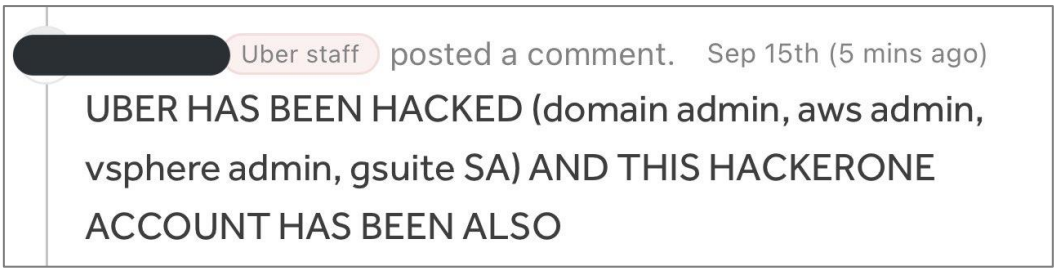

図 1 ハッカーが Uber 社内の Slack に書き込んだ犯行声明 [2]

1.2. Uber 社へのソーシャルハッキングによる侵入 [3] [4] [5]

攻撃者は Uber 社のシステムのサプライチェーンにおいて末端にいる、システム開発の請負業者（以下、A 氏）を狙った。

攻撃者はまず、A 氏が Uber 社のシステム内にアクセスするための認証情報（アカウントとパスワード）を入手した。具体的な入手方法は明らかではないが、ダークウェブのマーケットで購入した等が考えられている。

Uber 社のシステムは MFA を導入しているため、認証情報だけではログインできない。しかし、攻撃者はパスワード入力によるログイン試行を繰り返して MFA の通知を A 氏の端末に何度も表示させてクリックを誘う、ソーシャルハッキングの一種である**MFA 疲労攻撃**を仕掛け、ログインしようとした。

さらに攻撃者は Uber 社のサポートチームに偽装して SNS の WhatsApp を通じて A 氏に、承認ボタンをクリックすることでこの認証のトラブルは解消するというアドバイスのメッセージを送った[6]。A 氏はこれに騙されて MFA を承認し、MFA 疲労攻撃は成功した。

---

[1] 出典：日本経済新聞『Uber へのサイバー攻撃、ハッカー集団「ラプサス」関与か』
https://www.nikkei.com/article/DGXZQOGN201D60Q2A920C2000000

[2] 出典：Twitter『@vxunderground』
https://twitter.com/vxunderground/status/1570597582417821703

[3] 出典：Uber『Security update | Uber Newsroom』
https://www.uber.com/newsroom/security-update

[4] 出典：Bleeping Computer『Uber hacked, internal systems breached and vulnerability reports stolen』
https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/

[5] 出典：Twitter『@hacker_』
https://twitter.com/hacker_/status/1570582547415068672

[6] 出典：Malwarebytes『Welcome to high tech hacking in 2022: Annoying users until they say yes』
https://www.malwarebytes.com/blog/news/2022/09/taking-up-the-slack-on-fatigue-attacks

攻撃者は Uber 社のネットワークに侵入した後、さらに他の従業員アカウントに対してハッキングを展開し、最終的にスクリプトに含まれたユーザー名とパスワードを探し出し、G-Suite や Slack を含む多くの社内ツールの管理者権限を手に入れることに成功した。

9 月 15 日、Uber 社がハッキング被害に遭い、社内システムが使えなくなったことが従業員の SNS 等から明らかになった。翌 16 日に Uber 社は、侵入被害に対応中であること、また、Uber のユーザーのアカウントやクレジットカード情報等の漏洩はみられないことを発表[7]した。

1.3. Uber を攻撃した LAPSUS$について

【LAPSUS$の特徴】[8] [9] [10]

Uber 社へのハッキングは、ハッキンググループである LAPSUS$が関連していると考えられており、Uber 社も被害についての発表で攻撃者を LAPSUS$に関連付けている。

LAPSUS$は、主に英国の 10 代の少年らがいたずら目的で活動しているグループとみられている。2021 年末から活動し、これまで Microsoft、NVIDIA、Samsung、Okta といった多数の有名な大企業のシステムへの侵入に関与し、盗み出した情報を暴露する等して、企業に被害をもたらしている。暴露した情報を売りに出す行為が確認されているが、恐喝や金銭的利益自体には興味が向いていないように見えると Palo Alto Networks 社は分析している。侵入の成果を Twitter 等の SNS で誇る行為も確認されていることから、実利よりも顕示欲が強いと考えられている。

LAPSUS$の侵入には、多要素認証をソーシャルハッキングで突破する手法が多いことが目に付く。認証基盤システムの Okta に侵入した際に「我々は（Okta 本体ではなく）Okta の顧客にしか興味がない」と述べており、これは Okta の提供する多要素認証を利用している顧客を狙っていることをほのめかしたと理解されている。

このグループが LAPSUS$として大企業への侵入活動をする前は、有名人等からフィッシングで詐取した Twitter アカウントをダークウェブ等のマーケットに売る活動をしていたことから、フィッシングを成功させるための多要素認証の突破を試みるうちに、ソーシャルハッキングの技術を磨いたと考えられている。

【Uber 社侵入の主犯】

2022 年 3 月、英国のロンドン市警察は LAPSUS$のハッキングに関係したとして 10 代の少年達 7 人を逮捕したが、すぐに全員を保釈した[11]。それから約半年後の 9 月 22 日、ロンドン市警察はハッキング容疑で 17 歳の少年を逮捕したと発表した（図 2）。ロンドン市警察が発表した起訴内容には 2 件の保釈条件違反があることから、この少年は 3 月に逮捕された少年の一人の可能性があり、さらに、Uber 社への侵入の主犯ではないかと推測されている。

---

[7] 出典： Uber『Security update | Uber Newsroom』
https://www.uber.com/newsroom/security-update

[8] 出典： Palo Alto Networks『脅威に関する情報: Lapsus$グループ』
https://unit42.paloaltonetworks.jp/lapsus-group/

[9] 出典： Krebs on Security『A Closer Look at the LAPSUS$ Data Extortion Group』
https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/

[10] 出典： Krebs on Security『The Original APT: Advanced Persistent Teenagers』
https://krebsonsecurity.com/2022/04/the-original-apt-advanced-persistent-teenagers/

[11] 出典： BBC News『Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal』
https://www.bbc.com/news/technology-60864283

Uber 社を攻撃したと主張する人物は New York times に対し、ハッキングの証拠のファイルを添えて自分は 18 歳のハッカーであると述べており[12]、逮捕された少年と年齢が近い。また同時期に、Twitter 等で「Teapot」と名乗るハッカーが人気ゲームシリーズ「Grand Theft Auto」の開発元である Rockstar Games 社へ侵入し開発情報を暴露しているが、Teapot も Uber への犯行について語っており[13]同一人物と考えられている。TeaPot は 9 月 22 日のツイート[14]を最後に約 2 週間沈黙しており、これはロンドン市警察による逮捕の時期と符合する。なお、10 月 5 日に TeaPot は保釈されたことを発表（図 3）しており、これは上記のロンドン市警察による逮捕・保釈を指すとみられる。

図 2 ロンドン市警察による少年逮捕の発表 [15]

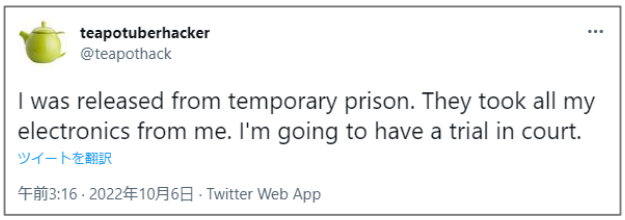

図 3 保釈を報告する「TeaPot」と名乗るハッカーの Twitter [16]

（訳：一時的な刑務所から釈放された。彼らは俺の電子機器を全て取り上げた。俺は裁判を受けることになっている）

1.4. ソーシャルハッキングへの対策

LAPSUS$のような攻撃に対抗するには、最新のソーシャルハッキングを意識した対策が必要である。

まず、人的対策としてユーザーに対し、MFA 疲労攻撃や、連絡を取ってくる攻撃者の存在といった最新の攻撃について社員に教育を実施し、攻撃者に意表を突かれることが無いようにする。

人的対策だけでなく多要素認証の強化も必要である。MFA 疲労攻撃対策として、Microsoft 社は自社の AzureAD の

[12] 出典： The New York Times『Uber Investigating Breach of Its Computer Systems』
https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html

[13] 出典： Twitter『@hacker_』
https://twitter.com/hacker_/status/1570582547415068672

[14] 出典： Twitter『@teapothack』
https://twitter.com/teapothack/status/1573057296166436865

[15] 出典： Twitter『@CityPolice』
https://twitter.com/CityPolice/status/1573281533665972225
https://twitter.com/CityPolice/status/1573553836802936833

[16] 出典： Twitter『@teapothack』
https://twitter.com/teapothack/status/1577724339616899072

「リスクベースの条件付きアクセスポリシー構成」機能を紹介している（図 4）[17]。この機能は、MFA の通知が何度も表示される挙動を検知後、正規のユーザーがログインした際、自動的にパスワード変更を求める機能である。MFA 疲労攻撃を受けているユーザーは攻撃者にパスワードを窃取されている。パスワード変更により攻撃者が使っているパスワードを無効化することで、攻撃者による MFA の要求の通知が止まり、MFA 疲労攻撃を阻止できる。

認証自体についてもプッシュ通知から、MFA 疲労攻撃のみならずフィッシング等のさまざまなソーシャルハッキング攻撃への耐久性を高めるために、端末の証明書と生体認証を組み合わせた認証（FIDO2）への切り替えを検討していくべきである。

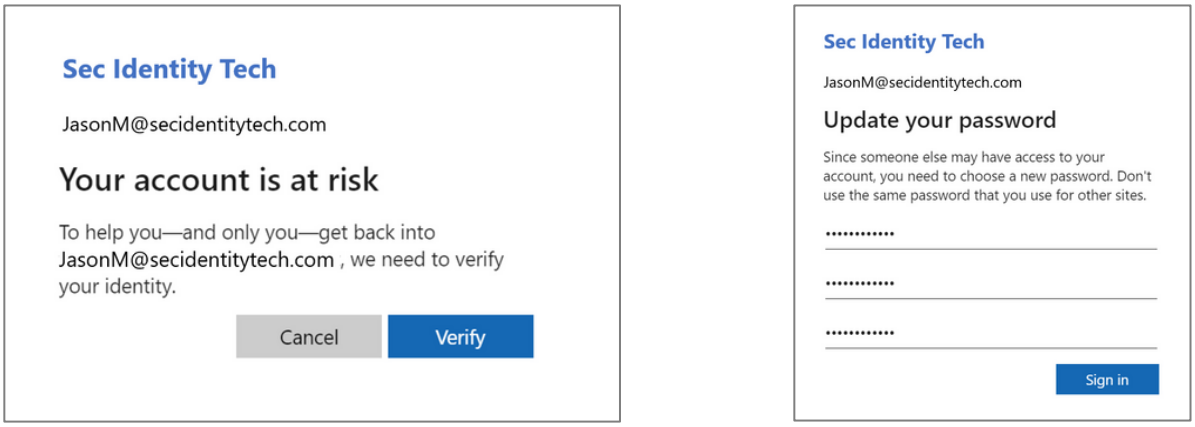

図 4 攻撃の可能性の通知画面と、パスワード変更画面

1.5. まとめ [18]

ユーザーを狙って騙すソーシャルハッキングの発想自体は新しいものではない。だが、その発想に基づき新たに編み出された MFA 疲労攻撃は、どのような組織に対しても応用が可能であり、一旦成功すると企業の奥底にまで侵入されてしまうことを LAPSUS$の攻撃は証明した。

MFA 疲労攻撃は LAPSUS$以外でも、6 月のランサムウェア攻撃グループによるとみられる Cisco 社のシステムへの侵入において使用がみられる等被害が増加しており、今後、同様の手法が他のランサムウェア攻撃、さらには国家を背景にした攻撃に採用されていく可能性は否定できない。

MFA 疲労攻撃が克服されたとしても、また別のソーシャルハッキングが編み出されて侵入されるイタチごっこが予想される。最新のソーシャルハッキングを常に意識し、ユーザーに攻撃手法についての教育を継続して実施し、また多要素認証自体も耐久性を高め続けていく対策が必要である。

[17] 出典： Microsoft『Defend your users from MFA fatigue attacks - Microsoft Tech Community』 https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677

[18] 出典： WIRED『The Dire Warnings in the Lapsus$ Hacker Joyride』 https://www.wired.com/story/lapsusdollar-uber-rockstar-breach-multifactor-authentication-weaknesses

2. アルバニアがサイバー攻撃を理由に、イランとの国交断絶を表明

2.1. 概要

2022 年 9 月 7 日、東ヨーロッパのバルカン半島に位置するアルバニアが、同年 7 月に受けたサイバー攻撃はイランによる支援を受けたものだとして、イランとの国交断絶を発表した。今回の一件は、サイバー攻撃を理由として国交を断絶した初の事例と考えられている。アルバニアは北大西洋条約機構(NATO)の加盟国であるため、NATO や米国がイランへの非難やアルバニアへの支援を表明した。

図 5 アルバニアとイランの位置関係

2.2. イランによるアルバニアへのサイバー攻撃

2021 年 5 月、アルバニアの行政プラットフォーム administrata.al のサーバーがイラン系とみられるグループからサイバー攻撃を受けた[19]。それから 1 年後の 2022 年 7 月 17 日、今度は政府ポータル e-Albania がサイバー攻撃によって一時停止した[20]。この政府ポータルは、住民登録や、税金の支払い、社会保険、各種証明書の発行など、公共サービスの大半をアルバニア国民に提供していた[21]。

米国とアルバニア政府は調査を行い、この攻撃の背後にもイランが存在すると結論付けた。9 月 7 日、アルバニアのラマ首相

[19] 出典: Security Boulevard『Albania Breaks Ties With Iran After 2022 Microsoft Investigation of CVE-2019-0604』 https://securityboulevard.com/2022/09/albania-breaks-ties-with-iran-after-2022-microsoft-investigation-of-cve-2019-0604/

[20] 出典: EURACTIV『Albania has two countries in crosshairs following cyberattack』 https://www.euractiv.com/section/politics/short_news/albania-has-two-countries-in-crosshairs-following-cyberattack/

[21] 出典: Exit News『On May 1st, Public Services in Albania Go All-Digital』 https://exit.al/en/2022/04/30/on-may-1st-public-service-counters-in-albania-go-all-digital/

はビデオ声明でイランとの断交を発表[22]。「我々は同盟関係にある NATO に通知し、反論の余地のない結果を共有した。閣僚理事会は、イランとの外交関係の終了を直ちに決定した」と述べ[23]、イランにいる外交官と大使館職員に 24 時間以内の国外退去を命じた[24]。これに対しイラン外務省は、イランがサイバー攻撃を行ったというアルバニアの主張を否定した。またアルバニアの断交措置を非難し、賛同する米国を牽制した。

断交発表後の 9 月 9 日、アルバニア警察の総合情報管理システム(TIMS)がサイバー攻撃によって、24 時間停止した。アルバニアのラマ首相は本件について、「7 月のハッキングを実行した者と同じ攻撃者による仕業だった」とツイートした[25]。

アルバニアは国民の半数以上がイスラム教徒という背景もあり、アルバニア政府はイスラム主義を唱えるイランの反主流組織「人民ムジャヒディーン」(MEK)の亡命者を米国の依頼に基づき受け入れており、以前からイランとは緊張関係にあった。アルバニア国民の多くは、この攻撃をイランによる報復であったと考えている[26]。

2.3. イランのハッカーグループ[27] [28] [29]

アルバニア政府は、イランとの断交の声明で、7 月の政府ポータルへの攻撃にはイランの国家的支援を受けた 4 つのハッカーグループが関与していたと発表した。被害調査に協力した Microsoft 社の分析によると、いずれのグループもイランの情報安全保障省（MOIS）傘下にあり、連携してアルバニア政府のシステムへ侵入し、ランサムウェア攻撃・データ窃取を実行した。ランサムウェアの感染画面に表示された画像(図 6)には、アルバニア政府による MEK 支援を揶揄するメッセージが書かれていた。イランによる攻撃を示唆するものと考えられている。

[22] 出典：ロイター 『アルバニアがイランと断交、7 月のサイバー攻撃巡り』
https://jp.reuters.com/article/albania-iran-idJPKBN2Q903G

[23] 出典：EURACTIV 『Albania cuts diplomatic ties with Iran over cyberattacks』
https://www.euractiv.com/section/politics/news/albania-cuts-diplomatic-ties-with-iran-over-cyberattacks/

[24] 出典：REUTERS 『Albania cuts Iran ties over cyberattack, U.S. vows further action』
https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/

[25] 出典：CNN politics 『Albania blames Iran for second cyberattack since July』
https://edition.cnn.com/2022/09/10/politics/albania-cyberattack-iran/index.html

[26] 出典：DW 『Albania once again the target of cyberattacks after cutting diplomatic ties with Iran and expelling diplomats』
https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285

[27] 出典：アルバニア政府 『VIDEOMESSAGE OF PRIME MINSTER EDI RAMA』
https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/

[28] 出典：Microsoft 『Microsoft investigates Iranian attacks against the Albanian government』
https://www.microsoft.com/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

[29] 出典：Mandiant 『New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit』
https://www.mandiant.com/resources/blog/targeted-attack-in-middle-east-by-apt34

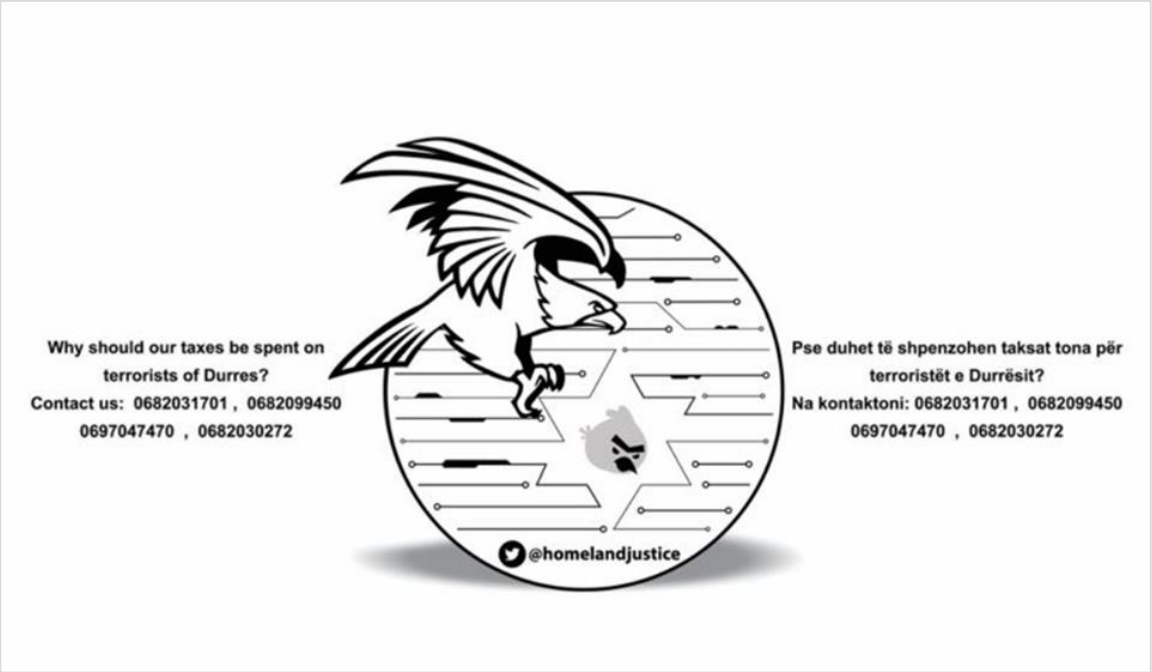

図 6 ランサムウェアの感染画面の画像

（訳：なぜ私たちの税金がドゥレスのテロリスト（※MEK の事を指すと考えられる）に費やされるべきなのか）

これらグループは、過去にイスラエル、サウジアラビアなどの中東の政府関連組織に対して、電子メール窃取等の攻撃を行っている。

2.4. 米国と NATO の対応

バイデン米政権は 9 月 9 日、NATO 加盟国で米国の同盟国であるアルバニアへのサイバー攻撃に関与したとして、イランの情報安全保障省とその諜報大臣に対する制裁を発表した[30]。

NATO のストルテンベルグ事務総長は、Twitter で、イランによるアルバニアへのサイバー攻撃を強く非難し、NATO はサイバー脅威を抑止し防御するために、セキュリティを強化し続けると述べた（図 7）[31]。また、NATO も同様の公式声明を発表している[32]。

[30] 出典：Bleeping Computer『US sanctions Iran's Ministry of Intelligence over Albania cyberattack』
https://www.bleepingcomputer.com/news/security/us-sanctions-iran-s-ministry-of-intelligence-over-albania-cyberattack/

[31] 出典：Twitter『@jensstoltenberg』
https://twitter.com/jensstoltenberg/status/1570098153881206790

[32] 出典：NATO『Statement by the North Atlantic Council concerning the malicious cyber activities against Albania』
https://www.nato.int/cps/en/natohq/official_texts_207156.htm

図 7　NATO のストルテンベルグ事務総長の Twitter 投稿

2.5. まとめ

アルバニアのサイバー空間をイランが侵害したことにより、現実世界では国交断絶にまで至る事態となった。国家が関与したサイバー攻撃によって社会インフラが破壊され、現実世界に大きな影響を与えた場合、軍事的な攻撃と同一視される可能性がある。サイバー攻撃は国際的な紛争の手段として、拡大・過激化している一方で、被害の実態や影響が他国には分かりにくく、攻撃者の特定も、過去の事例や地政学的な状況を踏まえた類推に留まることが多い。

今回の事件ではイランと敵対している米国が NATO 加盟国であるアルバニアに協力して調査を行っているが、このような第三国による協力が不適切なケースや、更なる紛争を引き起こすケースも考えられる。将来的には紛争当事国以外の中立な国際機関による仲介や、当事国以外の国々が調査を実施するためのルール策定等が必要になってくると考えられる。

3. 米政府、政府機関が調達するソフトウェアに新たなセキュリティ対策を義務付け

3.1. 概要

2022 年 9 月 14 日、米国行政管理予算局（Office of Management and Budget, OMB）は、米国政府機関が新たに調達するソフトウェアについて、セキュリティ要件を強化するガイダンスを発表した[33]。

今後、連邦政府機関が新たにソフトウェアを調達し、政府のネットワークに接続する場合、事前に当該ソフトウェアの開発者に NIST の 2 つの文書、「安全なソフトウェア開発フレームワーク（SP 800-218, Secure Software Development Framework, SSDF）」及び「ソフトウェアサプライチェーンセキュリティガイダンス（Software Supply Chain Security Guidance）」の遵守を証明させることが必要となった。

また、政府機関は調達するソフトウェアの重要性に応じて、公募時に、第三者による評価やソフトウェア部品表の提出を要求できることが明記された。このガイダンスは単体のソフトウェアだけでなく、クラウド上のサービスや、ソフトウェアを組み込んだ製品、OS 等も対象となる。

BRIEFING ROOM

Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience

SEPTEMBER 14, 2022 • BLOGS

By Chris DeRusha, Federal Chief Information Security Officer and Deputy National Cyber Director

The Biden-Harris Administration is committed to delivering a Government that works for all Americans – and technology powers our ability to do so. In order for Federal agencies to provide critical services, information, and products to the American people, they need access to secure and reliable software that manages everything from tax returns to veteran's health records.

図 8 調達するソフトウェアのセキュリティ要件を強化する OMB のガイダンス[34]

3.2. 経緯

9 月 14 日に発表されたガイダンスは、2021 年 5 月 12 日にバイデン大統領が署名した「国家のサイバーセキュリティの改善に関する大統領令（Executive Order 14028[35]）」に基づいている。この大統領令は、連邦政府機関のソフトウェアサ

[33] 出典：JETRO『バイデン米政権、政府機関が調達するソフトウエアにセキュリティー対策を義務化』
https://www.jetro.go.jp/biznews/2022/09/e43da89f71ddf4b3.html

[34] 出典：THE WHITE HOUSE『Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience』
https://www.whitehouse.gov/omb/briefing-room/2022/09/14/enhancing-the-security-of-the-software-supply-chain-to-deliver-a-secure-government-experience/

[35] 出典：THE WHITE HOUSE『Executive Order on Improving the Nation's Cybersecurity』
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

プライチェーンのサイバーセキュリティ強化を主な目的としている。2020 年末から相次いだ、中露のハッカーグループが米国の組織に対して行った 3 つの大きなサイバー攻撃（下記）への対策として、「サイバーセキュリティについて、現在のように自由放任主義で”次の事件を待つ”という状況をそのままにはできない[36]」として発せられた。

【① SolarWinds 社「Orion」を狙った攻撃】

2020 年 12 月、SolarWinds 社の更新用サーバーが攻撃され、同社のネットワーク監視ツール「Orion」にバックドア型マルウェアが混入されたことが発覚した。約 18,000 の顧客がこの更新プログラムをダウンロードし、内部システムへの侵入や電子メールの窃取等の攻撃を受けた[37]。顧客の中には、財務省、国防総省等の米国政府組織が含まれていた他、本件を最初に発見したセキュリティ企業 FireEye 社（現 Mandiant 社）も攻撃の被害に遭った。

米政府は英政府と共に、この攻撃はロシアの諜報機関を後ろ盾にしたハッカーによるものだと非難する声明を出した[38]。

【② Microsoft Exchange Server の脆弱性を狙った攻撃】

2021 年 3 月、Microsoft 社は「Exchange Server」に重大な脆弱性があるとして、緊急セキュリティ更新プログラムをリリースした[39]。米国で少なくとも 3 万の組織が攻撃を受け、電子メールの窃取などの被害を受けた。CISA は Microsoft 社の発表を受け、連邦政府機関に直ちに脆弱性に対処することを要求する緊急指令を発令した[40]。

Microsoft 社はこの攻撃を分析した記事の中で、本件の実行者は中国政府が支援するハッカーグループ「Hafnium」であると発表した[41]。

【③ コロニアルパイプライン社へのランサムウェア攻撃】

2021 年 5 月、コロニアルパイプライン社がランサムウェア攻撃によってデータを窃取されていることが発覚した。脅威の拡大を防ぐため、同社はネットワーク全体をシャットダウンさせた。このことにより、石油パイプラインが一時的に操業停止に陥った[42]。更に、同社はデータの身代金として 500 万ドル相当の仮想通貨を支払った（後に FBI が大部分を奪還した[43]）。

---

[36] 出典：THE WHITE HOUSE『Background Press Call by Senior Administration Officials on Executive Order Charting a New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks』
https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/12/background-press-call-by-senior-administration-officials-on-executive-order-charting-a-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

[37] 出典：INSIDER『The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal』
https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

[38] 出典：ZDNet Japan『SolarWinds 製品に対する攻撃、ロシアの諜報機関が背後に--米英が公に非難』
https://japan.zdnet.com/article/35169463/

[39] 出典：ZDNet Japan『「Microsoft Exchange Server」の脆弱性を悪用したハッキング、3 万の米組織に影響の恐れ』
https://japan.zdnet.com/article/35167461/

[40] 出典：CISA『EMERGENCY DIRECTIVE 21-02 - MITIGATE MICROSOFT EXCHANGE ON-PREMISES PRODUCT VULNERABILITIES』
https://www.cisa.gov/emergency-directive-21-02

[41] 出典：Microsoft『新たな国家支援型サイバー攻撃について』
https://news.microsoft.com/ja-jp/2021/03/05/210305-new-nation-state-cyberattacks/

[42] 出典：BleepingComputer『Largest U.S. pipeline shuts down operations after ransomware attack』
https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/

[43] 出典：npr『How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom Back』
https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac

FBI はロシアに拠点を置くと見られるランサムウェアグループ「DarkSide」がこの件に関与していると発表した[44]。

3.3. NIST のセキュリティ文書とソフトウェア部品表（SBOM）

今回のガイダンスでは、米政府機関が調達するソフトウェアの開発者は、NIST（米国国立標準技術研究所）の 2 つの文書である、「安全なソフトウェア開発フレームワーク」と「ソフトウェアサプライチェーンセキュリティガイダンス」を遵守するよう求めている。NIST は、米国政府機関が準拠すべきセキュリティレベルを定めている、商務省傘下の機関である。また、各政府機関に対して、ソフトウェアを使い始める際には、納入者からガイダンスに沿って安全に開発したという証明書を提出させるよう義務付けている。

【安全なソフトウェア開発フレームワーク】

NIST の定めるセキュリティの基準文書群である SP-800 シリーズのひとつ（SP 800-218）では、ソフトウェア開発の際の枠組みを定めている。前述の大統領令（Executive Order 14028）を受け、2022 年 2 月 3 日にリリースされた[45]。開発対象のソフトウェアの安全性だけに注目するのではなく、その開発やテスト、配布を行う環境の安全性を確保することや、ソースコードやデータにデジタル署名を行うことで、改ざん防止を行うこと等、ソフトウェア開発全般をカバーしている。

このフレームワークの目的は、形骸化しがちなチェックリストを作成することではない。安全なソフトウェア開発手法を採用することにより、ソフトウェア開発を継続的に改善するためのリスクベースのアプローチを計画・実施するための基礎を提供することである。

このフレームワークでは安全なソフトウェア開発について、「組織の準備」「ソフトウェアの保護」「安全性の高いソフトウェアの作成」「脆弱性への対応」と 4 つのグループに分けて説明している。例えば、「組織の準備」では、開発するソフトウェアに組み込まれる別のソフトウェアの開発元も含め、関連する組織の全ての人がセキュリティ要件を理解していることや、開発支援ツールを導入することで人的労力の削減と問題発生の抑止を両立させること等が推奨されている。

【ソフトウェアサプライチェーンセキュリティガイダンス】

ソフトウェアサプライチェーンのセキュリティ対策強化について解説した文書である。大統領令の後、2 度のドラフト版を経て 2022 年 5 月 5 日に正式にリリースされた[46]。NIST は、「サプライチェーンは世界規模の商業活動の弱点であるため、組織が安全な製品やサービスを購入し使用できるように、組織を保護する」ことが本文書の目的であると説明している[47]。

例えば、使用を検討しているソフトウェア製品は、別のコンポーネント（単一の機能を果たす小さなプログラム）を含む場合があり、それはそのソフトウェア製品の開発会社とは別の組織によって作られた可能性がある。NIST は、ユーザー組織が、ソフトウェア製品の脆弱性だけでなく、コンポーネントの脆弱性についても意識し、それらのコンポーネントがどのように製品に組み込まれたのかまでも考慮することを推奨している。また、時間や人員といったリソースは有限であるため、リスクに優先順位を付け、

[44] 出典：REUTERS『FBI confirms DarkSide ransomware used in Colonial Pipeline hack』
https://www.reuters.com/article/us-usa-products-colonial-pipeline-fbi-idCAKBN2CR1RU

[45] 出典：NIST『Secure Software Development Framework SSDF』
https://csrc.nist.gov/Projects/ssdf

[46] 出典：NIST『Software Supply Chain Security Guidance』
https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-supply-chain-security-guidance

[47] 出典：NIST『NIST Updates Cybersecurity Guidance for Supply Chain Risk Management』
https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management

自動化や AI、その他のツールを組み合わせることで現実的に実行可能なサプライチェーン管理を行うこと等を促している[48]。

【ソフトウェア部品表(SBOM)】

9 月 14 日に発表されたガイダンスでは、上記二つのセキュリティ文書に加え、重要なソフトウェアの入札募集時には、ソフトウェアの開発元にソフトウェア部品表（Software Bill Of Materials, 以下、「SBOM」と表記）の提出を求めることができると助言している。

大統領令(Executive Order 14028)では SBOM を「ソフトウェアを構築する際に使用される様々なコンポーネントの明細とサプライチェーン関係を含む正式な記録」と定義している[49]。

米国大統領の電気通信や情報関連政策についての諮問機関である米国商務省電気通信情報局（National Telecommunications and Information Administration, NTIA）の規格では、SBOM の最小構成要素は、「パッケージ名」「サプライヤー名」「SBOM 作成者」「パッケージバージョン」「コンポーネントのハッシュ」「コンポーネントの識別子」「コンポーネント間の関係」から成る。これを満たす SBOM の規格がいくつか承認されており、その中で広く利用されているものが Linux Foundation の「SPDX」という規格（図 9）である[50]。

セクション例	フィールド例
Document creation	SPDX Documentの作成者、作成場所、作成日時
Package	構成パッケージの名前、バージョン、ライセンス、配布元、SPDX識別子
File	構成ファイルのファイル名、ファイルタイプ、チャックサム、SPDX識別子
Snippet	コードスニペットのバイト範囲、SPDX識別子、関連ファイル
Relationships between SPDX elements	SPDX要素間の関係

図 9 SPDX の仕様抜粋[51]

SBOM の作成を容易にする環境も整ってきている。7 月 12 日、Microsoft は「SBOM Tool」をオープンソースで公開した[52]。このツールを利用することで SPDX 形式の SBOM を自動的に生成することができる。

[48] 出典：SecurityIntelligence『NIST Supply Chain Security Guidelines: 10 Key Takeaways』
https://securityintelligence.com/articles/nist-supply-chain-guidelines-ten-takeaways/

[49] 出典：NIST『Software Security in Supply Chains: Software Bill of Materials (SBOM)』
https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

[50] 出典：THE LINUX FOUNDATION『SPDX ： すでに世界共通のソフトウェア部品表（SBOM）およびサプライチェーン セキュリティで使用』
https://www.linuxfoundation.jp/blog/2021/06/spdx-its-already-in-use-for-global-software-bill-of-materials-sbom-and-supply-chain-security/

[51] 出典：NEC セキュリティブログ『ソフトウェアサプライチェーン対策の紹介』
https://jpn.nec.com/cybersecurity/blog/220603/index.html

[52] 出典：Microsoft『Microsoft open sources its software bill of materials (SBOM) generation tool』
https://devblogs.microsoft.com/engineering-at-microsoft/microsoft-open-sources-software-bill-of-materials-sbom-generation-tool/

3.4. まとめ

米国ではサイバー攻撃を受けた経験から、大統領令とそれに基づくガイダンスを通じてソフトウェアサプライチェーンのセキュリティ強化の取り組みが進んでいる。今後、ソフトウェア開発会社が自社の開発環境のセキュリティ文書の遵守状況を明示する、ソフトウェア製品の SBOM を開示するといったケースが増えていくことが予想される。特に SBOM は、今後、入札の要件で求められることが増え、普及が進むと考えられる。こうした情報をうまく活用することで、自社のセキュリティ強化に役立てることができる。例えば、Google のセキュリティチームは、SBOM を「オープンソース脆弱性データベース（Open Source Vulnerabilities[53]）」のような既知の脆弱性データベースと照らし合わせることで、そのソフトウェアに潜む脆弱性を発見する具体的な手順をブログで紹介している[54]。

以上

[53] 出典：Open Source Vulnerabilities『A distributed vulnerability database for Open Source』 https://osv.dev/

[54] 出典：Google Developers『SBOM in Action:「ソフトウェア部品表」で脆弱性を見つける』 https://developers-jp.googleblog.com/2022/08/sbom-in-action.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