サイバーセキュリティレポート

2024.03

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 ページサマリー】

当レポートでは 2024 年 3 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『サイバー保険、国家関与の攻撃は「戦争免責」として保険金支払いを見送りへ』

- 複数の国内の大手損保会社が、サイバー攻撃や事故に関連する損害を補償する保険商品で戦争免責の適用基準を導入した。
- 戦争免責の対象となるのは、国家関与型サイバー攻撃で、重要インフラや、安全保障、防衛に重大な影響を及ぼすもの等が挙げられている。
- 特に重要インフラを担う企業においては、今後、国家関与型サイバー攻撃を受けた際に保証を受けられない可能性があるため、保険以外のサイバーセキュリティ対策を強化していくことが、ますます重要になる。

第 2 章『ドイツ軍幹部によるウクライナ支援についての会議内容をロシアメディアが暴露』

- 3 月 2 日、ドイツ公共放送 ARD は空軍幹部のオンライン会議の内容がロシアに漏洩し暴露されていることを明らかにした。
- この会議ではウクライナへの軍事支援に関する協議を行っており、漏洩の原因は、参加者の 1 人がホテルの部屋でセキュリティ対策の施されていない回線から会議に接続したためとみられる。
- ドイツは重要会議が傍受されたことを深刻な問題と受け止め、本件を調査している。一方ロシアは、傍受した内容に自国への攻撃に関する軍事計画が含まれていたとして、ドイツを非難している。

第 3 章『商用スパイウェア悪用に対する規制の動き』

- 商用スパイウェアの悪用がここ数年問題となっており、米国を中心として規制の動きが広がっている。
- 米国連邦地裁は商用スパイウェアを提供するイスラエルの NSO グループに対し、開発／販売するスパイウェアに関する情報を、コンピューター不正行為防止法違反等の理由で同社を訴えていた Meta 社とその子会社 WhatsApp 社に引き渡すよう命令を下した。
- 3 月 18 日には、日本を含めた 17 か国から、商用スパイウェアの悪用に反対する共同声明が発表された。このような取り組みの広がりは、野放しになってきたスパイウェアの悪用への歯止めとして、歓迎したい。

1. サイバー保険、国家関与の攻撃は「戦争免責」として保険金支払いを見送りへ

1.1. 概要

複数の国内の大手損保会社が、サイバー攻撃・事故に関連する損害を補償する保険商品において戦争免責の適用基準を導入した（開始時期は 4 月）[1]。外国政府が関与する重大なサイバー攻撃の被害に遭った場合、保険金の支払いが行われないことになる。

1.2. サイバー保険と戦争免責

【サイバー保険】

サイバー保険は、インターネットや情報技術を利用した活動によって生じる損害を補償するための保険商品である。近年、コンピューターやネットワーク技術は日常生活に広く浸透しており、企業を取り巻くサイバーリスクも多様化している。サイバー保険は、そのようなリスクに備える手段の一つとして、企業に利用されている。例えば、データ漏洩事故が発生したり、サイバー攻撃を受けたりした場合に、調査や復旧等のための費用が企業に補償される。

【戦争免責】

保険契約では一般的な条項である戦争免責は、戦争や軍事行動に起因する損害を補償の**対象外**とする。これは、戦争による損害は広範囲かつ重大になるため、保険会社が補償に耐え切れないためである[2]。

【サイバー戦争免責】

ロシアによるウクライナ侵攻では、直接的な武力衝突のみならず、国家が関与するとみられるサイバー攻撃が多発した。これを踏まえて保険会社の間で、サイバー保険の補償が増大する懸念が広がり、見直しが議論されるようになった[3]。英国のロイズ保険協会は、サイバー戦争免責条項を含む新しい保険契約の基準を定め、2023 年 3 月 31 日以降の契約ではこれを適用するよう保険会社に要請した[4]。

【サイバー戦争免責の対象となる攻撃】

例えば、三井住友海上のサイバー保険「サイバープロテクター」の 4 月 1 日以降契約用のパンフレットによると、サイバー戦争免責の対象となるのは、国家関与型サイバー攻撃で、戦争および外国の武力行使等の過程において、または直接的な準

[1] 出典：日本経済新聞『サイバー保険、国家関与は「戦争免責」』
https://www.nikkei.com/article/DGKKZO79306140W4A310C2MM8000/

[2] 出典：WTW『ロシアのウクライナ侵攻に見る戦争損害への備え』
https://www.wtwco.com/ja-jp/insights/2022/03/crb-nl-march-otani

[3] 出典：損保総研レポート『国家の関与するサイバー攻撃とサイバー保険の戦争免責条項について ― 主席研究員 濵田 和博』
https://www.sonposoken.or.jp/reports/wp-content/uploads/2022/12/sonposokenreport141_1.pdf

[4] 出典：Clifford Chance『Lloyd's cyber war exclusion』
https://www.cliffordchance.com/insights/resources/blogs/insurance-insights/2023/09/lloyds-cyber-war-exclusion.html

備として行われるものと、重要インフラや、安全保障、防衛に重大な影響を及ぼすものである[5]。（他損保大手も似た基準を導入している）

国家関与型かどうかの判定は、攻撃に使用されたツールや手法、政治的背景の調査・分析を必要とする複雑なプロセスを伴い[6]、公的機関等の第三者の見解を根拠に行われる[7]。

1.3. まとめ

保険大手各社は今回実施したサイバー戦争免責の導入によって、台湾有事への備えを進めていると考えられる。特に、重要インフラを担う企業は、今後サイバー攻撃を受けた際、そしてそれが国家関与型であった場合に、保険によるリスク転嫁ができなくなる可能性がある。保険以外のサイバーセキュリティ対策を強化していくことが、今後ますます重要になる。

[5] 出典：三井住友海上『サイバープロテクター』
https://www.ms-ins.com/pdf/business/indemnity/pd-protector.pdf

[6] 防衛研究所『NIDS コメンタリー第 179 号 国家のサイバー攻撃とパブリック・アトリビューション ― 瀬戸 崇志 政策研究部グローバル安全保障研究室』
http://www.nids.mod.go.jp/publication/commentary/pdf/commentary179.pdf

[7] 出典：日本経済新聞『サイバー保険、国家関与は「戦争免責」』
https://www.nikkei.com/article/DGKKZO79306140W4A310C2MM8000/

2. ドイツ軍幹部によるウクライナ支援についての会議内容をロシアメディアが暴露

2.1. 概要

3 月 2 日、ドイツ公共放送 ARD は、空軍幹部のオンライン会議の内容がロシア側に漏洩したことを明らかにした。この会議ではウクライナへの軍事支援に関する協議が行われており、1 日にロシアの国営メディア「Russia Today（RT）」の編集長がその会議の内容を複数の SNS に投稿していた。漏洩の原因は、ドイツ軍幹部の 1 人がホテルの部屋でセキュリティ対策の施されていない回線から会議に接続していたためとみられる。 ドイツのショルツ首相は本件を重く受け止め、調査を進めていると述べた[8, 9]。

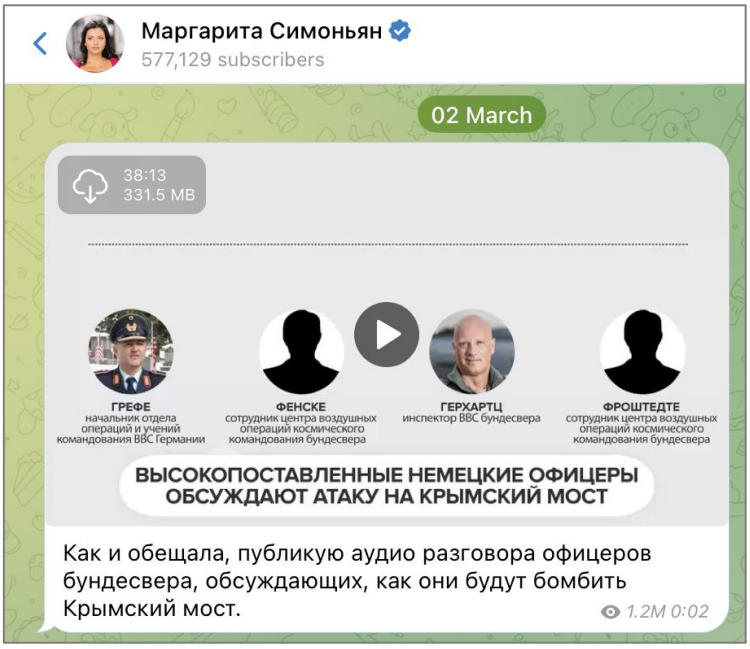

図 1 RT 編集長による Telegram への投稿画面

「お約束した通り、クリミア橋を爆撃する方法について話し合っているドイツ連邦軍の将校たちの会話音声を公開します」

2.2. オンライン会議の漏洩について

今回 RT が公開したのは、2024 年 2 月 19 日に実施されたドイツ空軍のオンライン会議。38 分間にわたる録音や文字起こしにより、会議内容が暴露された。これらのデータによると、会議にはゲアハルツ総監を含むドイツ空軍幹部 4 人が参加しており、ドイツ製の巡航ミサイル「タウルス」をウクライナが使用する場合の、標的や影響、引き渡し方法などを議論していた。ドイツメディアによると、ウクライナ兵の訓練やロシア本土とクリミア半島を結ぶクリミア橋の攻撃について、また同盟国の作戦（別の

[8] 出典：読売新聞オンライン『ドイツ軍の機密会議、ロシアが傍受し国営放送が暴露…イギリス軍要員のウクライナでの活動にも言及』 https://www.yomiuri.co.jp/world/20240303-OYT1T50041/

[9] 出典：POLITICO『Berlin blames Taurus call leak on officer logging in via insecure Singapore hotel line』 https://www.politico.eu/article/german-defense-minister-blames-taurus-call-leak-officer-logging-via-insecure-hotel-line/

巡航ミサイルを供与したイギリス軍のウクライナでの活動等）にも言及していた[10]。

ウクライナは、フランスとイギリスが共同開発したミサイルの提供を既に受けているが、射程距離がその倍である「タウルス」の供与をドイツに求めている。ショルツ首相は戦闘の激化を恐れ、これまで通り、ミサイル引き渡しの可能性を断固として否定している[11]。

そのような中で RT の編集長は、クリミア橋の攻撃について協議されていたこと等を根拠に、漏洩した会議の内容はドイツがクリミア攻撃を計画している証拠だと、SNS で主張。RT はこれを基にニュースを発信した[12]。

図 2 ロシア本土とクリミア半島を結ぶクリミア橋[13]

【漏洩の原因】[14, 15, 16, 17]

会議中の音声を RT がどのように入手したのかについて、ロシア側は詳細を明らかにしていない。ドイツの国防相は、漏洩の

[10] 出典：読売新聞オンライン『ドイツ軍の機密会議、ロシアが傍受し国営放送が暴露…イギリス軍要員のウクライナでの活動にも言及』
https://www.yomiuri.co.jp/world/20240303-OYT1T50041/

[11] 出典：REUTERS『Why a leaked German military recording on Ukraine aid is causing an outcry』
https://www.reuters.com/world/europe/why-leaked-german-military-recording-is-causing-outcry-2024-03-04/

[12] 出典：RT『German discussion of attacks on Russia: What has emerged so far』
https://www.rt.com/news/593561-german-audio-crimea-bridge/

[13] 出典：EU Today『WebEx: German Officials Authenticate Recordings, Confirming Leakage of Highly Sensitive Military Discussions』
https://eutoday.net/webex-cisco-leakage/

[14] 出典：POLITICO『Berlin blames Taurus call leak on officer logging in via insecure Singapore hotel line』
https://www.politico.eu/article/german-defense-minister-blames-taurus-call-leak-officer-logging-via-insecure-hotel-line/

[15] 出典：朝日新聞 DIGITAL『独空軍の情報漏洩、接続操作の誤りが原因か 会議参加者、手順従わず』
https://www.asahi.com/articles/ASS357RLFS35UHBI041.html

[16] 出典：Global Village Space『German Defense Ministry uses '1234' as password』
https://www.globalvillagespace.com/german-defense-ministry-uses-1234-as-password/

[17] 出典：BBC『Ukraine war: German call leak due to individual error, minister says』
https://www.bbc.com/news/world-europe-68467333

原因は参加者の一人がシンガポールのホテルの部屋からオンライン会議に出席する際、求められていた安全な接続手順に従わず、セキュリティ保護のない回線を使用したことにあると説明している。

今回の会議には軍の内部システムではなく、Cisco の Web 会議アプリ「Webex」が使われていた。国防相は、軍の用意したサーバーにインストールする等、安全対策が強化された政府機関向けの Webex を利用しており、ある程度の機密レベルの協議においても利用を認めていると説明している。また、捜査の結果から、ドイツの通信システムへの侵害や、会議にスパイが密かに参加していた可能性は否定している。

なお、Webex の会議には、PC やスマートフォンにインストールされた Webex アプリを使用する他に、Webex のサーバーが払い出した電話番号に電話をかけることで参加することもできる。そのため、今回の盗聴は Webex の暗号化対策の外にある脆弱な、電話接続の部分が狙われた可能性が指摘されている。

当時、シンガポールでは国際航空ショーのために各国から軍事関係者が集まっていた。ロシアの諜報機関は国際会議をターゲットにすることで知られており、狙われやすい状況にあった中でたまたま盗聴できた会話が、ロシアにとって好都合なものであったと考えられている。

【ドイツや同盟国の反応】[18, 19, 20]

3 月 2 日、ドイツのショルツ首相は、会議内容がロシアに漏洩したことについて「非常に深刻な問題」と訪問先のバチカンで述べ、迅速に調査することを表明した。また、政府報道官は、この情報漏洩はドイツと同盟国との間に不和の種をまくことを目的とした、ロシアの「ハイブリッド偽情報攻撃」であると述べた。

ドイツの野党の保守派であるキーゼヴェッター氏はテレビ局の取材に答え、ドイツの機密情報が恒常的にロシアに流れており、今後さらなる情報が漏洩する可能性があると警告した。

なお、NATO 諸国は今回の漏洩について、公にドイツを批判していない。例えばイギリスは引き続きドイツと協力してウクライナを支援すると述べている。

【ロシアの反応】[21, 22]

国営メディアである RT が盗聴を暴露した直後から、ロシア政府はドイツを強く非難している。背景として、ウクライナ侵攻は NATO からロシアを防衛する代理戦争と主張する上で、NATO の主要国であるドイツにロシア攻撃の意志があるという話は、都合が良いということが挙げられている。

ロシアのラヴロフ外相は、ドイツ軍の「あからさまな自己暴露」によって「ずる賢い計画」が明らかになったと述べた。ロシア安全保障会議のメドヴェージェフ副議長は「古くからのライバルであるドイツ人が、再び私たちの宿敵となった」とテレグラムに投稿した。

---

[18] 出典：REUTERS『Why a leaked German military recording on Ukraine aid is causing an outcry』
https://www.reuters.com/world/europe/why-leaked-german-military-recording-is-causing-outcry-2024-03-04/

[19] 出典：BBC『Russia publishes German army meeting on Ukraine』
https://www.bbc.com/news/world-europe-68457087

[20] 出典：REUTERS『Germany accuses Russia of seeking to divide Europe with leaked call』
https://www.reuters.com/world/europe/kremlin-says-german-army-discussing-strikes-russia-asks-if-scholz-is-control-2024-03-04/

[21] 出典：REUTERS『Why a leaked German military recording on Ukraine aid is causing an outcry』
https://www.reuters.com/world/europe/why-leaked-german-military-recording-is-causing-outcry-2024-03-04/

[22] 出典：Deutsche Welle (DW)『Germany braces for Russian influence operations』
https://www.dw.com/en/hybrid-warfare-germany-braces-for-russian-influence-operations/a-68670972

2.3. まとめ

2022 年のロシアによるウクライナ侵攻以降、ドイツはウクライナに対し、アメリカに次ぐ規模の軍事支援を提供している。このため、ロシアのスパイ活動において、ドイツは主要な標的とされている[23]。このような状況下においてドイツ軍幹部がセキュリティ保護のない回線を使用して重要な会議に接続したことにより、議論の中心であったロシアにその内容を暴露されるという重大インシデントが発生してしまった。ドイツ側の機密情報の取り扱いの甘さが露呈した事件であり、このような一見単純と思われる操作にも大きな事故につながる可能性が潜んでいること、またインターネットに適切に接続するための手順を周知徹底することの重要性を認識させられる事件であった。

[23] 出典：REUTERS『Why a leaked German military recording on Ukraine aid is causing an outcry』
https://www.reuters.com/world/europe/why-leaked-german-military-recording-is-causing-outcry-2024-03-04/

3. 商用スパイウェア悪用に対する規制の動き

3.1. 概要

3 月 18 日に開催された第 3 回民主主義サミットにおいて、日本や米国を含む計 17 か国から、商用スパイウェアの悪用によって引き起こされる脅威の他、商用スパイウェアの研究、開発に関係する技術の拡散及び規制の必要性について共同声明が発表された[24]。

スマートフォンの OS やメッセージアプリ等を密かに狙う商用スパイウェアの脅威は、これまで様々に問題視されてきた。例えば 2 月 23 日には、米国連邦地裁が、スパイウェアメーカー大手であるイスラエルの NSO グループに対し、同社が開発／販売するスパイウェアに関する情報を、Meta 社とその子会社 WhatsApp 社に開示するよう命令を下している[25]。

国家安全保障や外交政策上の利益にリスクをもたらすとして、米国を中心にスパイウェアの悪用を規制する動きが広がっている。

3.2. NSO グループとスパイウェア

【NSO グループと Pegasus】

NSO グループは、2010 年に設立されたイスラエルのサイバーインテリジェンス企業で、特にスパイウェア **Pegasus** を開発／販売していることで有名である。社名の NSO は、創設者の 3 名 **N**iv、**S**halev、**O**mri の頭文字から取られた。同社の社員には、イスラエルの諜報機関である 8200 部隊の出身者が多いとされる[26]。

Pegasus は iOS と Android 向けのスパイウェアである。インストール先デバイスのカメラ、マイク、位置情報、画像、動画等にアクセスできるため[27]、Pegasus を監視対象者のスマートフォンにインストールすれば、その人物がどこにいるか、誰とどのような通話を行っているか、どのようなメッセージを交換しているか等を長時間、検知されずに監視することが可能となる。

攻撃者は、ゼロデイ脆弱性を悪用することにより、ターゲットに気付かれずに、遠隔から Pegasus をインストールすることができる。このような攻撃は、フィッシング攻撃等と異なりユーザーの操作を必要としないことから「ゼロクリック攻撃」と呼ばれている。

NSO グループは、国内外の政府機関に対して Pegasus を販売している。同社製品は、イスラエルの国家機密として扱われており、他国の政府機関に販売する場合はイスラエル国防相の許可が必要となっている[28]。→

---

[24] 出典：The White House『Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware』
https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/

[25] 出典：Casetext『WhatsApp Inc. v. NSO Grp. Techs.』
https://casetext.com/case/whatsapp-inc-v-nso-grp-techs-9

[26] 出典：The New York Times『The Battle for the World's Most Powerful Cyberweapon』
https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

[27] 出典：アムネスティ・インターナショナル日本『ペガサスプロジェクト：記者らの携帯情報を盗むスパイウェア』
https://www.amnesty.or.jp/news/2021/0805_9278.html

[28] 出典：The Guardian『Court orders maker of Pegasus spyware to hand over code to WhatsApp』
https://www.theguardian.com/technology/2024/feb/29/pegasus-surveillance-code-whatsapp-meta-lawsuit-nso-group

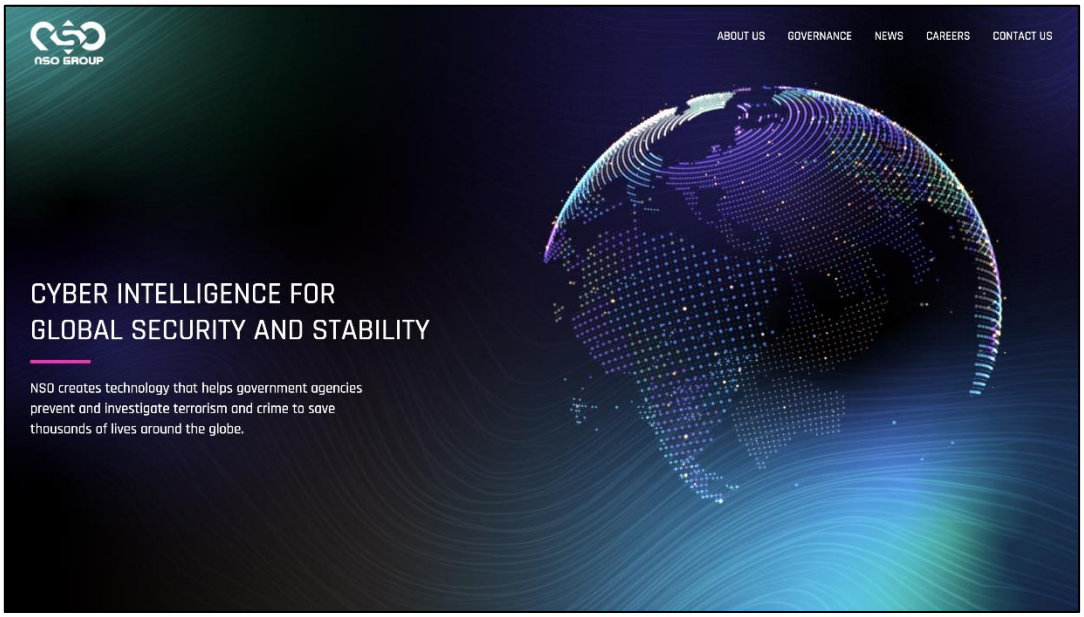

図 3 NSO グループの Web サイト

【Pegasus の悪用に関する問題】

NSO グループが、「私たちの使命は、政府機関にテロや犯罪との戦いに役立つテクノロジーを提供し、世界がより安全となるよう貢献すること[29]。」と語っているように実際、テロ対策や犯罪対策を目的として Pegasus を購入し使用している機関も存在する。しかし一方で、著名な人物、人権活動家、他国の外交官、ジャーナリスト、反体制派等を監視するために Pegasus を使用している機関もあり、こういった行為は人権侵害や違法であるとして問題になっている。

カナダの The Citizen Lab は、2018 年 9 月に、36 の機関が Pegasus を利用し、計 45 か国に監視対象となる人物が存在するとの調査結果を公表した[30]。このうち少なくとも 6 か国で、政治家、弁護士、ジャーナリスト、人権活動家、反体制派を監視する目的で Pegasus が使用されていた。

2018 年 10 月、サウジアラビア人のジャーナリストで反体制派であるジャマル・カショギ氏が、トルコのイスタンブールにあるサウジアラビア総領事館で政府職員により殺害された[31]。この事件では、カショギ氏の協力者であるカナダ在住のサウジアラビア人、オマル・アブドルアジズ氏のスマートフォンが、サウジアラビア政府が用いた Pegasus に感染しており[32]、両名がやりとりしていた政府への批判が筒抜けであったとされる[33]。また、カショギ氏の死後も、同氏の家族や協力者に対し、サウジアラビア政府やその

[29] 出典：USA TODAY『Spyware firm tied to iPhone hack has U.S. ties』
https://www.usatoday.com/story/tech/news/2016/08/26/shadowy-israeli-firm-behind-apple-hack-tool/89408936/

[30] 出典：The Citizen Lab『HIDE AND SEEK - Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries』
https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[31] 出典：BBC『Jamal Khashoggi: Turkey says journalist was murdered in Saudi consulate』
https://www.bbc.com/news/world-europe-45775819

[32] 出典：The Citizen Lab『The Kingdom Came to Canada - How Saudi-Linked Digital Espionage Reached Canadian Soil』
https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/

[33] 出典：Committee to Protect Journalists (CPJ)『How the Saudis may have spied on Jamal Khashoggi』
https://cpj.org/2018/10/how-the-saudis-may-have-spied-on-jamal-khashoggi/

同盟国が Pegasus のインストールを試みており、これに成功し監視していたケースも確認されている[34]。

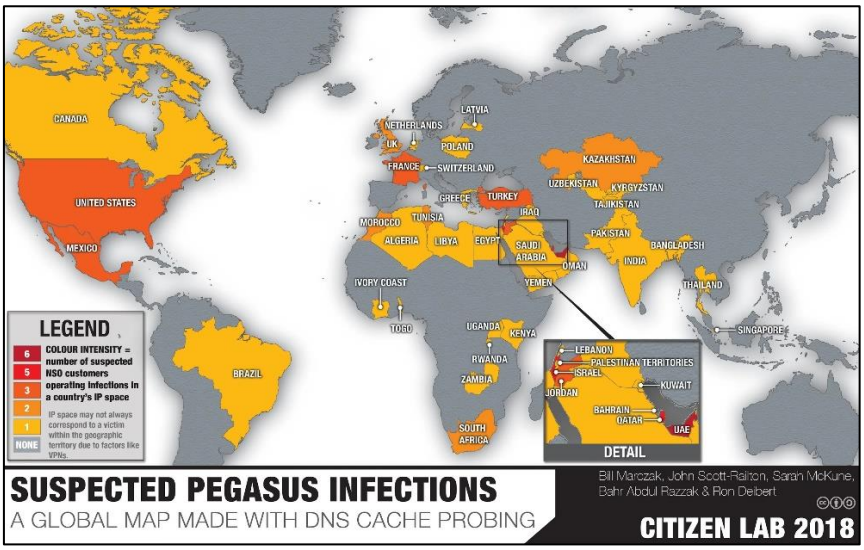

図 4 Pegasus を用いた監視対象の存在が確認された国 [30]
※監視対象者数の多寡を濃淡で表現

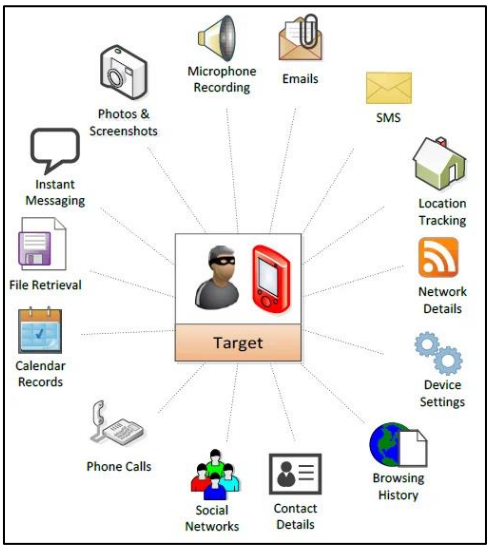

図 5 Pegasus がデバイスから収集できる情報の一覧 [30]

3.3. Meta 社、WhatsApp 社による訴訟

2019 年 4 月下旬から 5 月初旬に掛けて、メッセージアプリ WhatsApp のゼロデイ脆弱性が悪用され、約 1400 台のデバイスにスパイウェアが送信された。Facebook 社（現 Meta 社）とその子会社の WhatsApp 社は、同年 10 月、コンピューター不正行為防止法や WhatsApp の利用規約に違反したとして、スパイウェアの開発元である NSO グループを裁判所に提訴した[35]（なお、裁判記録では具体的な製品名は明らかにされていない）。スパイウェアの送信対象となったのは、弁護士、ジャーナリスト、人権活動家、反体制派、各国の政府高官や外交官であった[36]。送信には WhatsApp アプリの通話機能に存在した、遠隔から実行可能な脆弱性 CVE-2019-3568 が悪用された[37]。

今年の 2 月 23 日、米国連邦地裁は NSO グループに対し、事案の前後 1 年間（2018 年 4 月下旬から 2020 年 5 月初旬）の、Pegasus を含む同社製スパイウェアの全機能に関する情報を Meta 社と WhatsApp 社に開示するよう命じた。ただし、NSO グループの顧客である政府機関の情報は開示する必要はないとした [25]。

裁判の最終的な判決はまだ出ていないものの、NSO グループに対して不利な決定となった。同社は、この決定についてコメントを差し控えている [28]。

---

[34] 出典：The Guardian『Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests』https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus

[35] 出典：REUTERS『WhatsApp sues Israel's NSO for allegedly helping spies hack phones around the world』https://www.reuters.com/article/us-facebook-cyber-whatsapp-nsogroup/whatsapp-sues-israels-nso-for-allegedly-helping-spies-hack-phones-around-the-world-idUSKBN1X82BE/

[36] 出典：Ars Technica『WhatsApp suit says Israeli spyware maker exploited its app to target 1,400 users』https://arstechnica.com/information-technology/2019/10/whatsapp-suit-says-israeli-spyware-maker-exploited-its-app-to-infect-1400-users/

[37] 出典：TechCrunch『WhatsApp exploit let attackers install government-grade spyware on phones』https://techcrunch.com/2019/05/13/whatsapp-exploit-let-attackers-install-government-grade-spyware-on-phones/

3.4. スパイウェア悪用に対する規制の動き

NSO グループを筆頭に、スパイウェア開発企業がここ数年問題となっている。これらの企業は、多額の資金と優れた技術者を投入して WhatsApp のようなメッセージアプリや、Android、iOS、Windows 等のゼロデイ脆弱性を入手している。そしてそのような脆弱性を活用して、ターゲットのセキュリティ対策を突破するためのサービスを提供している。Google 社は、同社製品や Android 環境のデバイスをターゲットとしたゼロデイ脆弱性による攻撃の半数は、スパイウェア開発企業によるものと指摘している[38]。

このような企業が提供するスパイウェアに対し、米国を中心として規制の動きが広がっている。

2021 年 11 月、米国国務省は、 NSO グループを含むスパイウェアメーカー2 社をエンティティリスト（米国製品の輸出禁止企業一覧）に追加したと発表した。政府関係者、ジャーナリスト、活動家などを監視するためのスパイウェアを開発し外国政府に提供したことを規制の理由として挙げている[39]。これにより、NSO グループは、スパイウェア開発等に欠かせないソフトウェア開発ツールなどの米国製品を米国政府の承認なしには購入できなくなり、同社の活動は大きく制限されるようになった[40]。

米国政府は今年 2 月には、国家安全保障や外交政策上の利益にリスクをもたらすとして、開発、販売、利用等、商用スパイウェアの悪用に関わる人物にビザ制限を課すと発表した[41]。また、3 月 18 日に開催された第 3 回民主主義サミットでは、日本や米国を含む計 17 か国から、商用スパイウェアの悪用によって引き起こされる脅威の他、商用スパイウェアの研究、開発に関係する技術の拡散及び規制の必要性について共同声明が発表された [24]。

3.5. まとめ

国防や外交、国際的なビジネスに関わる人物は、スパイウェアを用いた監視対象として他国から狙われる可能性がある。スパイウェアを使った攻撃は居住国に関係なく可能なため、国外だけでなく日本国内にいる場合でも、スパイウェア感染を狙った攻撃を受ける事態を想定して、モバイルデバイスに重要な情報を保存しない等の対策を講じることを推奨する。

高度な機能を有する商用のスパイウェアは、人権を軽視して国家統制を強めたい国々での購入のニーズが根強く、世界全体にとって脅威である。そのような中で、スパイウェアを売らせない・買わせない等の、米国を中心とした取り組みが広がるのは、野放しになってきたスパイウェアの悪用への歯止めとして、歓迎したい。

以上

---

[38] 出典：Google『Buying Spying: How the commercial surveillance industry works and what can be done about it』 https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/

[39] 出典：U.S. Department of State『The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities』 https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/

[40] 出典：MIT Technology Review『世界的スパイウェア企業「NSO」、米制裁で企業存亡の危機』 https://www.technologyreview.jp/s/262066/nso-was-about-to-sell-hacking-tools-to-france-now-its-in-crisis/

[41] 出典：U.S. Department of State『Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware』 https://www.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware/

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