サイバーセキュリティレポート

2023.12

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

© NTT Security Holdings

目次

© NTT Security Holdings

【1 ページサマリー】

当レポートでは 2023 年 12 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『暴露型ランサムウェア攻撃 2023 年活動まとめ』

- 2023 年、年間を通してランサムウェアグループによる被害組織に関する暴露サイトへの投稿は増加した。参入が容易になったことで、ランサムウェアグループも増加している。
- ランサムウェアグループが運用する RaaS において、アフィリエイト（実行役）の身代金における取り分も上昇した。
- ランサムウェアグループ間の競争は激化しており、アフィリエイトに対するサポート体制の強化や、ランサムウェアブランド力の強化などに力を入れると考えられる。

第 2 章『遺伝子検査サービス「23andMe」、サイバー攻撃により約 690 万人の情報が漏洩』

- 2023 年 12 月 5 日、遺伝子検査サービスを提供している米国の企業「23andMe」は、10 月に受けたサイバー攻撃により約 690 万人分の遺伝子情報が盗まれことを公表した。
- クレデンシャルスタッフィング攻撃で、一部のユーザーの認証が突破され情報を窃取されただけでなく、23andMe の特有のサービスにより、突破されたユーザーと近い遺伝子を持つユーザーの情報も漏洩した。
- 「究極の個人情報」と呼ばれる遺伝子情報の今後の利用拡大において、慎重なプライバシー保護と利便性の両方を確保した環境作りが進むことを期待したい。

第 3 章『ウクライナで大規模サイバー攻撃、ロシア関連のハッカーが犯行声明』

- ウクライナ最大の通信事業会社「キーウスター」が、ロシアによる大規模なサイバー攻撃を受け、 数百万人の携帯電話やインターネットのサービス、警報システムが停止するなど、重要インフラに多大な影響があった。
- 攻撃の実行者として複数のロシアのハクティビストグループが犯行声明を出しているが、実際は、ロシアの軍傘下の Sandworm による攻撃とみられている。
- 今回の事件は物理的な攻撃と同様の効果をサイバー攻撃で狙ったものと考えられる。使用不能になると他の社会的な機能にも影響が波及する重要インフラにおける、有事に備えたサイバー防御の重要性を本件は示している。

© NTT Security Holdings

1. 暴露型ランサムウェア攻撃 2023 年活動まとめ

1.1. はじめに

弊社の OSINT モニタリングチームでは、暴露型ランサムウェアグループが運営する暴露サイトの投稿を日々モニタリングしている。そのモニタリング結果に基づいて、2023 年の暴露型ランサムウェアグループの活動・動向をまとめた。

1.2. ランサムウェア攻撃の増加

暴露型ランサムウェアグループとは、ランサムウェアを用いてターゲット組織のネットワークにあるファイルを暗号化／窃取したうえで、復号キーとの引き換えに身代金を要求し、さらに期限までに身代金が支払われなければ、グループが運営するサイトで窃取したファイルを公開（暴露）する、と被害組織を二重に脅迫する犯罪グループである。

暴露サイトの多くはダークウェブに存在しているが、誰でもアクセスできるサイトや SNS を利用するランサムウェアグループもある。

2023 年に全てのランサムウェアグループが行った、被害組織に関する投稿の総数の推移を月ごとにまとめた（図 1）。

前年の 2022 年は、平均して月に 200 件程度の投稿であったが、2023 年は年間を通して増加傾向が見られ、3 月以降は月に 300 件以上の投稿が常態化した。

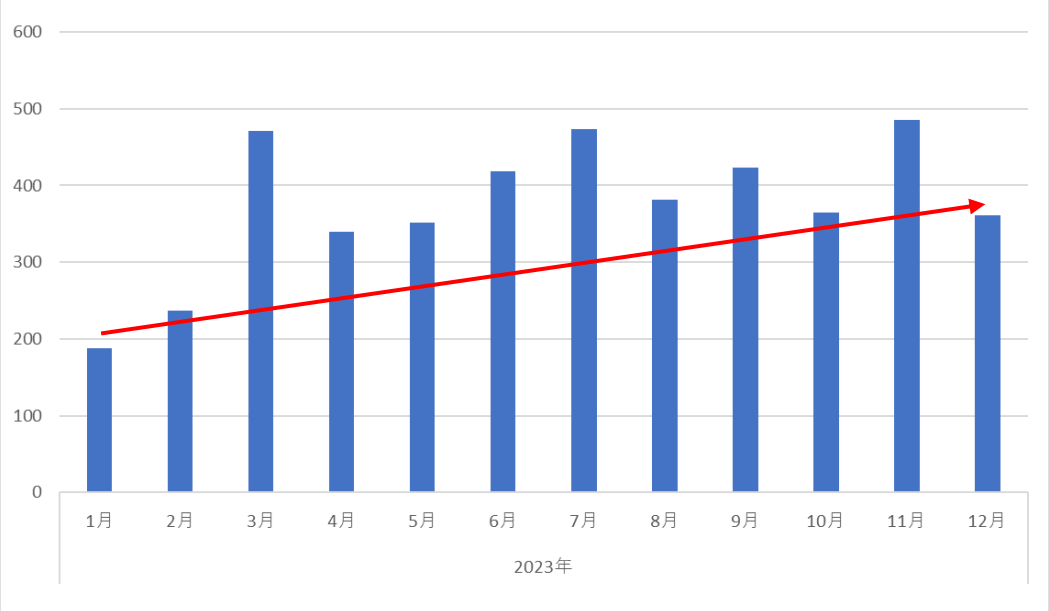


図 1 暴露サイトでの被害組織に関する投稿の総数の推移

1.3. ランサムウェアグループの増加

【ランサムウェアグループの増加】

2023 年に暴露サイトへの投稿が確認されたランサムウェアグループの総数の推移を月ごとにまとめた（図 2）。

1 月と 2 月は、暴露サイトに投稿を行ったのは 20 グループ程度であったが、3 月から増加が明確になり 6 月以降は 30 グ

© NTT Security Holdings

ループを超えることが常態化した。

過去に Conti や Lockbit3.0 などのグループからランサムウェアのソースコードやビルダー、攻撃マニュアルなどが流出している[1, 2, 3]。それらの情報を流用することで、新たなグループを立ち上げることが容易になっており、ランサムウェアグループの増加に繋がっていると考えられる。

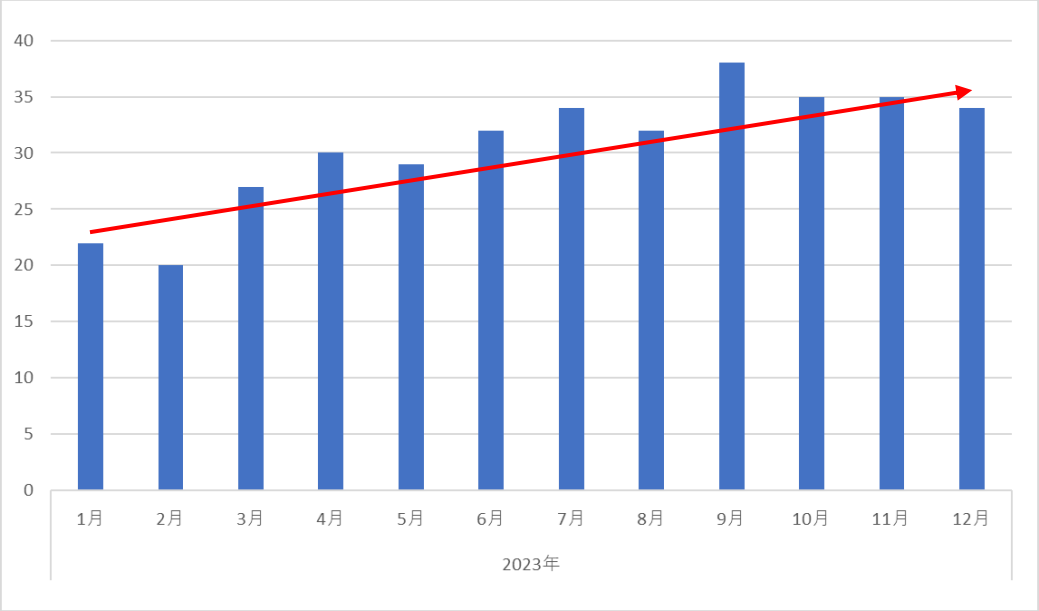


図 2 暴露サイトへの投稿が確認されたグループの総数の推移

【RaaS におけるアフィリエイトの取り分増加】

ランサムウェアグループの多くが、RaaS（Ransomware as a Service）と呼ばれる運用形態を取っている。これは、グループのオペレーターがランサムウェアを用意し、それを利用して実行役であるアフィリエイトがランサムウェア攻撃を行うサービスである。被害組織から得た身代金はオペレーターとアフィリエイトで分配され、その割合の決定権はオペレーターにある。

RaaS は、2015 年にランサムウェアグループ Tox が開始し、他グループにも広がっていった[4]。最初期に RaaS を導入したランサムウェアグループの一つである Chimera は、身代金に占めるアフィリエイトの取り分を 50%としていた [4]。

他のランサムウェアグループが設定していたアフィリエイトの取り分をみると、2019～2022 年に活動していた REvil は

[1] 出典：FORTINET『アフィリエイト向けマニュアル：Conti が直接教えるその攻撃の手法』
https://www.fortinet.com/jp/blog/threat-research/affiliates-cookbook-firsthand-peek-into-operations-and-tradecraft-of-conti

[2] 出典：BleepingComputer『Conti Ransomware source code leaked by Ukrainian researcher』
https://www.bleepingcomputer.com/news/security/conti-ransomware-source-code-leaked-by-ukrainian-researcher/

[3] 出典：BleepingComputer『LockBit ransomware builder leaked online by "angry developer"』
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-builder-leaked-online-by-angry-developer/

[4] 出典：Graham Cluley『Come to the dark side. Chimera ransomware asks victims to become affiliates』
https://grahamcluley.com/chimera-ransomware-asks-victims-affiliates/

© NTT Security Holdings

70%[5]、2021 年には Lockbit2.0 が 80%としていた[6]。

Lockbit3.0、CL0P に続き、2023 年に 3 番目に多い被害組織数を記録したランサムウェアグループ ALPHV は、従来アフィリエイトの取り分を身代金の金額によって 80%、85%、90%のように変動させていた[7]（※被害組織数は弊社調べ）。しかし、2023 年 12 月に ALPHV はこれまでのルールを変更し、アフィリエイトの取り分を一律 90%とする、また VIP アフィリエイト向けの専用プログラムを開始すると発表した。

この背景には、既存アフィリエイトの囲い込みと新規アフィリエイトの参加増を狙った ALPHV の戦略があると考えられる。12 月に FBI（米国連邦捜査局）が行った作戦により、ALPHV は使用していた暴露サイトを含む一部 IT インフラの差し押さえを受けた[8]。差し押さえは一部に留まったが、その中に暴露サイトも含まれており、ALPHV は暴露投稿ができなくなった。ALPHV は一時的に暴露サイトを取り戻した際に、FBI の作戦に対する反発として攻撃を強めることを表明し、その一環としてアフィリエイトの取り分の上昇などルール変更を行う旨を発表した（図 3）。ALPHV は現在、新たに立ち上げた暴露サイトで被害組織に関する投稿を行うなど、活動を継続している。

以上のように、RaaS におけるアフィリエイトの身代金取り分の割合は年々上昇しており、働きが良ければ特別待遇が受けられる状況にまでなっている。

[5] 出典：White Hat IT Security『THE REVIL IS IN THE DETAILS』
https://whitehat.eu/the-revil-is-in-the-details/

[6] 出典：KELA『LockBit 2.0 Interview with Russian OSINT』
https://www.kelacyber.com/lockbit-2-0-interview-with-russian-osint/

[7] 出典：SOCRadar『Dark Web Profile: BlackCat (ALPHV)』
https://socradar.io/dark-web-profile-blackcat-alphv/

[8] 出典：Krebs on Security『BlackCat Ransomware Raises Ante After FBI Disruption』
https://krebsonsecurity.com/2023/12/blackcat-ransomware-raises-ante-after-fbi-disruption/

© NTT Security Holdings

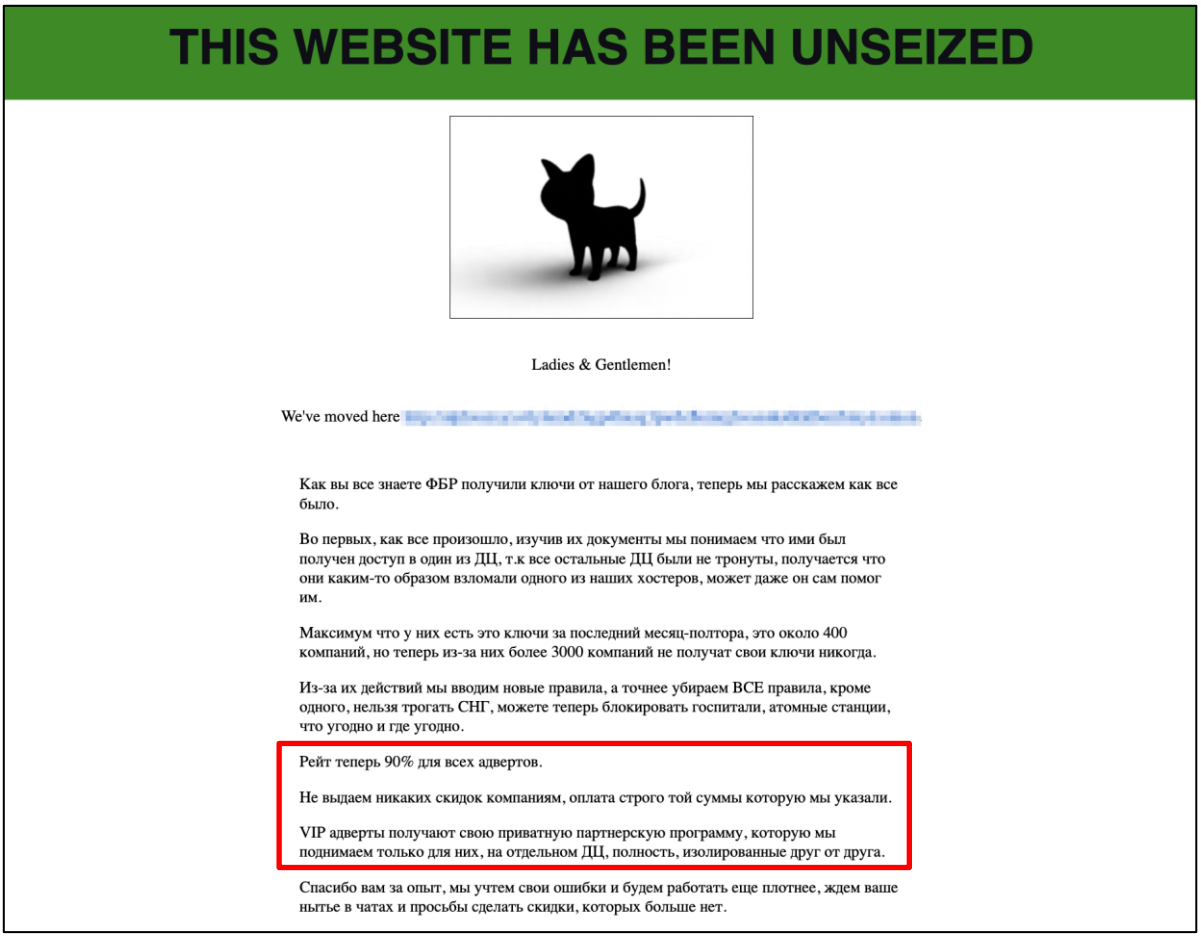


図 3 IT インフラ差し押さえ後の ALPHV の発表

※赤枠部分：アフィリエイトの取り分を 90%とすること、VIP プログラムを始めることが記載されている

1.4. まとめ

2023 年はランサムウェアの脅威が増大していたことが確認できた。また、RaaS への参入が容易になったことで、RaaS を導入するランサムウェアグループ間の競争は激化しており、優秀なアフィリエイトを確保するためにアフィリエイトの取り分は上昇を続けている。今後もアフィリエイト優位な状況は続くと考えられ、グループのオペレーターはアフィリエイトに対するサポート体制の強化を実施すると予想される。また、被害組織が身代金を払う確率を上げるため、このグループなら身代金を払えばファイルを復旧してくれると思わせるような、いわばブランド力の強化のため、被害組織に対し復旧のサポート等を強化すると考えられる。

© NTT Security Holdings

2. 遺伝子検査サービス「23andMe」、サイバー攻撃により約 690 万人の情報が漏洩

2.1. 概要

2023 年 12 月 5 日、遺伝子検査サービスを提供している米国の企業「23andMe」は、10 月に受けたサイバー攻撃によるデータ漏洩の被害者数が約 690 万人にのぼると発表した[9]。この攻撃により窃取されたデータは、ハッカーフォーラムに投稿されていた。

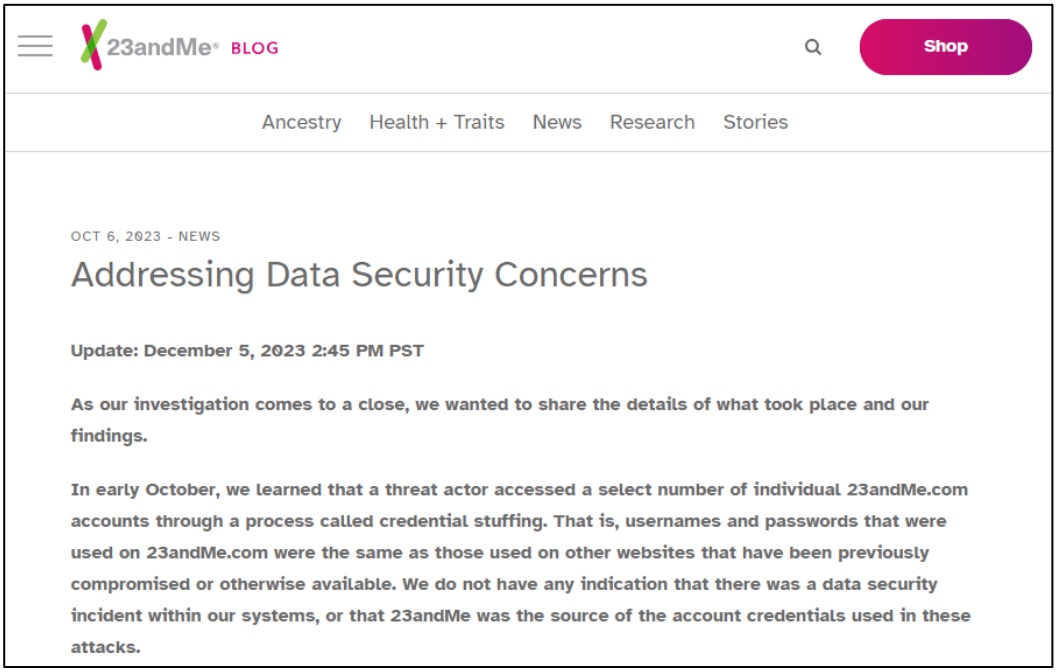


図 4 データ漏洩について報告する 23andMe のブログ投稿

2.2. 23andMe

「23andMe」は、唾液を用いた遺伝子情報検査サービスを提供している企業である。2006 年にサンフランシスコで創立され、社名は人間が持つ 23 対の染色体に由来している[10]。ユーザーは、検査する内容に応じて約 100 ドルから 300 ドルの検査キットを購入し、採取した自分の唾液を同社に送ることで、糖尿病や喘息といった病気の遺伝的なリスクの保有率や、自分の祖先の出身地の構成割合といったことを調べられる。これまでに 1,400 万人がサービスを利用している。

同社の特徴的な会員サービスとして、「DNA Relatives」（“relatives”は「親戚、親族」の意）がある。このサービスでは、DNA が近い会員同士で相互の情報を開示することができる。基本的な開示情報は名前および DNA の一致割合で、さらに希望した場合には住所やプロフィール写真、家系図データといった情報も開示される[11]。

---

[9] 出典：23andMe『Addressing Data Security Concerns』
https://blog.23andme.com/articles/addressing-data-security-concerns

[10] 出典 NBC NEWS『DNA test company 23andMe now fueling medical research』
https://www.nbcnews.com/health/health-news/dna-test-company-23andme-now-fueling-medical-research-n958651

[11] 出典：23andMe『DNA Relatives Privacy & Display Settings』
https://customercare.23andme.com/hc/en-us/articles/212170838

© NTT Security Holdings

2.3. ハッカーフォーラムへの投稿と 23andMe の対応

【ハッカーフォーラムへの投稿】

2023 年 10 月 1 日、ある大手ハッカーフォーラムに遺伝子情報を含むデータを販売（一部を無料配布）する投稿が行われた。その後、この投稿は削除されたが、当該データをダウンロードしていた者が、データを改めて配布する投稿を行った。この再配布の投稿はフォーラムの参加者の注目を集め、多くの返信が寄せられている。

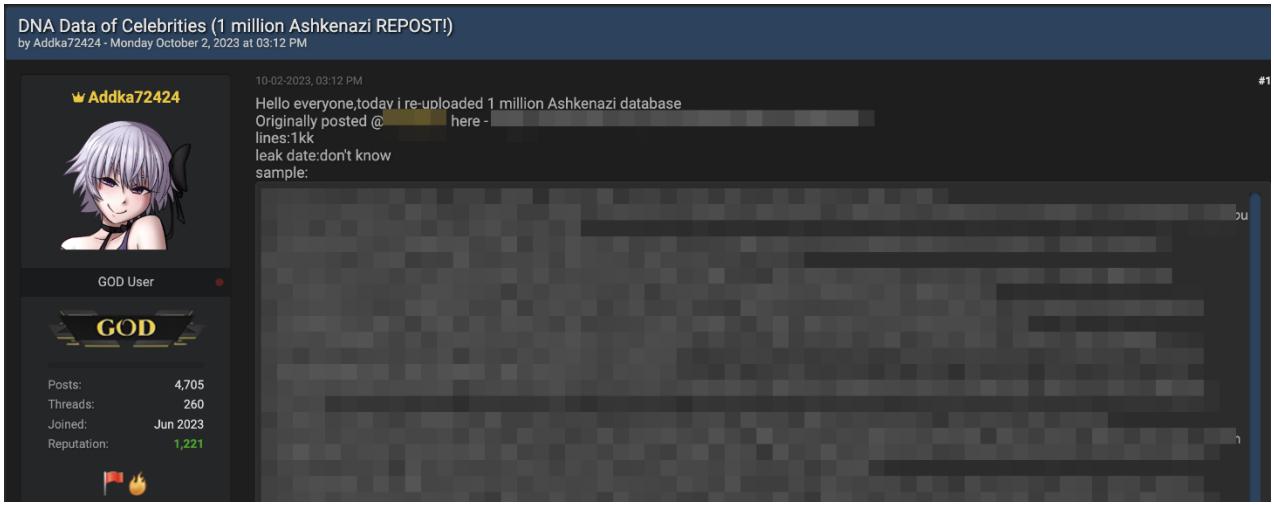


図 5 遺伝子情報を配布する投稿
「有名人の DNA データ（東欧系ユダヤ人 100 万人分 再投稿！）」

【23andMe の対応】

10 月 6 日、23andMe は公式ブログで、クレデンシャルスタッフィング攻撃（別名「パスワードリスト型攻撃」）を受けたユーザーのアカウントから情報を窃取されたと発表した[12]。この攻撃に用いられたパスワードは、他のサービスから流出したものであり、これと同じパスワードを 23andMe においても使用していた人々が被害に遭った。同社はすべてのユーザーに対し、パスワードをリセットし、他のサイトで利用していない固有のパスワードを設定するよう求めた。

同社は 12 月 1 日に米証券取引委員会へ提出したセキュリティ事故を報告する文書の中で、漏洩したのは全ユーザー1,400 万人の 0.1 パーセント、つまり 1 万 4,000 人分の遺伝子情報であると記載した[13]。しかし、この数字は過少であった。攻撃者は前述の「DNA Relatives」機能等を利用し、他のユーザーの情報にもアクセス可能であった。すなわち、攻撃者は侵入したアカウントで「DNA Relatives」機能を使うことで、遺伝的に近いユーザーのデータも芋づる式に窃取することができた。12 月 5 日、同社は公式ブログを更新し、実際には約 640 万人分のデータが盗まれていたことを認める投稿を行った。なお、23andMe がデータを保護するのに必要な措置を怠たり遺伝子情報が流出したことに対して、補償を求める裁判が複数

[12] 出典：23andMe『Addressing Data Security Concerns』
https://blog.23andme.com/articles/addressing-data-security-concerns

[13] 出典：TechCrunch『23andMe says hackers accessed 'significant number' of files about users' ancestry』
https://techcrunch.com/2023/12/01/23andme-says-hackers-accessed-significant-number-of-files-about-users-ancestry/

© NTT Security Holdings

提起されている[14]。

2.4. 公的機関によるガイドライン

遺伝子情報を利用したサービスにおいて、情報セキュリティに関するガイドラインとして、日本では、経済産業省が「経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン」を策定している[15]。同ガイドラインでは安全管理措置について、「個人遺伝情報の取扱いについては、情報の漏えい、滅失又は毀損の防止その他の情報の安全管理のため、組織的、人的、物理的及び技術的な措置を講じなければならない。」と、対策を講じることを義務付けている。

米国では、2023 年 12 月 10 日、NIST（米国標準技術研究所）が「遺伝子データのサイバーセキュリティ」（Cybersecurity of Genomic Data.）という報告書を発表した。同報告書は、他のデータと比較して遺伝子情報には特有の懸念点があるが、現在のポリシーや管理方法では十分に対処できない、と遺伝子情報のセキュリティの現状について問題提起している[16]。NIST は、遺伝子情報を取り扱う事業者がセキュリティ対策を取れるようにするためのフレームワークを、近い将来に提供できるように策定を進めている。

2.5. まとめ

遺伝子情報は、今後ますます広く活用される可能性があるが、同時に「究極の個人情報」と呼ばれるほど慎重な取り扱いが求められる。例えば、遺伝的な疾病リスクについての情報が漏洩すると、被害者が保険契約や就職活動に際して、深刻な不利益を被る恐れがある。また、情報が漏洩したユーザー個人だけでなく、近しい遺伝子をもつ人にも被害が及ぶ恐れがあり、家族や親族全体、さらにはこれから生まれる子孫に対するプライバシーの侵害等が懸念される。

政府主導で進んでいるガイドラインやフレームワークの構築は重要だが、実際のサービス提供企業でそれが反映されなければ、その価値は半減してしまう。政府と企業が協力し、プライバシーと利便性の双方を確保しつつ、遺伝子情報の有益な側面を最大限に引き出せるような環境作りが進むことを期待したい。

[14] 出典：BleepingComputer『23andMe hit with lawsuits after hacker leaks stolen genetics data』
https://www.bleepingcomputer.com/news/security/23andme-hit-with-lawsuits-after-hacker-leaks-stolen-genetics-data/

[15] 出典：経済産業省『経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン』』
https://www.meti.go.jp/press/2020/03/20210323003/20210323003-1.pdf

[16] 出典：NIST『Cybersecurity of Genomic Data』
https://csrc.nist.gov/pubs/ir/8432/final

© NTT Security Holdings

3. ウクライナで大規模サイバー攻撃、ロシア関連のハッカーが犯行声明

3.1. 概要

ロシアによるウクライナの軍事侵攻が続いている一方で、サイバー攻撃も激しくなっている。

2023 年 12 月 12 日、ウクライナ最大の通信事業会社「キーウスター（Kyivstar）」が、大規模なサイバー攻撃を受け、数百万人が利用するモバイル通信やインターネットサービスが停止したほか、キーウ周辺の一部地域で空襲警報システムがダウンした。

攻撃には、ロシアの国家支援を受けた攻撃者が関わっていたとみられる。2022 年にロシアの侵攻が始まって以来、警戒態勢も厳しくなっていたが、今回の件はウクライナの重大インフラが受けたサイバー攻撃の中でも特に影響が大きいものとなった[17]。

図 6 キーウスターのロゴ（キーウにある同社の本社）[18]

3.2. キーウスターの大規模障害

キーウスターのネットワーク障害は、12 日の早朝に発生した。同社は加入者からモバイル通信や通話ができなくなった旨の報告を受け、技術的な問題が発生していることを確認した[19]。原因は、キーウスターのシステムに対するハッキングであった。

[17] 出典：REUTERS『Ukraine's top mobile operator hit by biggest cyberattack of war』
https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/

[18] 出典：REUTERS『Hackers linked to Russian spy agency claim cyberattack on Ukrainian cell network』
https://www.reuters.com/technology/cybersecurity/ukraine-says-russian-intelligence-linked-hackers-claim-cyberattack-mobile-2023-12-13/

[19] 出典：Interfax-Ukraine『Large-scale failure in work of Kyivstar mobile operator occurs』
https://en.interfax.com.ua/news/general/953523.html

© NTT Security Holdings

【キーウスターについて】[20]

キーウスターは、1994 年に設立されたウクライナ最大の移動体通信事業者およびブロードバンドインターネットプロバイダーであり、オランダの国際通信グループ Veon の傘下にある。2023 年 3 月時点での携帯電話サービスの契約件数は 2430 万件、インターネットサービスの契約件数は 110 万件以上である。ウクライナ保安局（以下、「SBU」）のサイバーセキュリティ部門の責任者である Illia Vitiuk 氏はインタビューで、キーウスターは資金にも余裕があり、セキュリティにも十分コストをかけて対策しているように見えたと述べている[21]。

【サイバー攻撃の影響】[22]

今回の攻撃では、キーウスターの通信システムの中核が完全に破壊された[23]。攻撃者が、キーウスター内の数千の仮想サーバーや PC を含む、ほぼ全てのシステムのデータを消去したため、キーウスターのインフラの約 40%が使用不能になった[24]。これにより、同社のモバイル通信や空襲警報、銀行のシステム等に障害が発生し、ロシアの侵攻が始まって以来最も大きな影響を受けたサイバー攻撃となった。

ウクライナ国民は、ロシアの空爆に備えるため、携帯電話の警報に依存している。キーウスターの携帯電話のユーザー数はウクライナの人口の半数以上を占めているが、同社はさらなる攻撃を防ぐために通信網のシャットダウンを強いられ、同社のユーザーは通話やモバイル通信、警報の受信ができなくなった。このような場合は、国内の他の通信事業者の設備を通じて通信できるローミングサービスを使用できるようになっていたが、顧客データの登録システムが部分的に破壊されたため、それもかなわなかった[25]。警報を受信できなくなったキーウスターのユーザーは、他の携帯会社の利用を考え、キーウスターの最大のライバルであるボーダフォンの店舗に行列を作った。また、首都キーウ周辺の 75 以上の集落では空襲警報システム自体が停止した。ほかに、金融システムも影響を受け、銀行取引やクレジットカードのシステムの一部が使えなくなった。

なお、民間人は多大な影響を被ったが、別の通信システムを使用しているウクライナ軍は、今回の影響を受けなかった[26]。

【攻撃の実行者】[27]

今回のキーウスターのインフラに対する攻撃は、ロシアの軍参謀本部情報総局（GRU）傘下のサイバー戦争部隊「Sandworm」による犯行であると、ウクライナの SBU は発表している。Sandworm は 2015 年と 2016 年にもウクライナ

---

[20] 出典：Київстар『Про нас』
https://kyivstar.ua/about

[21] 出典：REUTERS『Exclusive: Russian hackers were inside Ukraine telecoms giant for months』
https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

[22] 出典：REUTERS『Ukraine's top mobile operator hit by biggest cyberattack of war』
https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/

[23] 出典：REUTERS『Exclusive: Russian hackers were inside Ukraine telecoms giant for months』
https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

[24] 出典：Interfax-Ukraine 『Cyber attack destroys about 40% of Kyivstar's infrastructure』
https://en.interfax.com.ua/news/general/955839.html

[25] 出典：Interfax-Ukraine『If situation with Kyivstar outage not changed, company's fixed-line network will be disconnected – Kyivstar president』
https://en.interfax.com.ua/news/general/953719.html

[26] 出典：Interfax-Ukraine『Kyivstar system breakdown doesn't affect Ukrainian military operations – Ground Forces』
https://en.interfax.com.ua/news/general/953645.html

[27] 出典：REUTERS『Exclusive: Russian hackers were inside Ukraine telecoms giant for months』
https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

© NTT Security Holdings

の電力会社にサイバー攻撃を行って停電を発生させたことがあり、その際、システムへの侵入や、データを消去するワイプ攻撃がみられた[28]。今回のキーウスターの攻撃でも同じような手法で、重要インフラを支えるシステムを破壊したと考えられる。

侵入経路は調査中だが、キーウスターによれば、1 人の従業員のアカウントが内部に侵入するための足掛かりにされたとみられている[29]。SBU の調査から、Sandworm のハッカーは遅くとも 2023 年 5 月にはキーウスターへの侵入を試み始め、11 月以降に完全なアクセス権を得たと考えられている。

なお、システムの破壊だけでなく、ハッカーがキーウスターのシステム内に侵入することにより、ウクライナ国民のスマートフォンの情報を窃取していた可能性も懸念されている。例えば、窃取した個人情報から位置情報の把握や SMS メッセージの傍受等を行い、Telegram のアカウントのアクセス権を窃取することまで出来たのではないかとも考えられている。なお、キーウスターは個人データと加入者データの漏洩を否定している。

【段階的な復旧】[30]

同社のサービスは段階的に復旧し、障害発生日である 12 日の 20 時には固定通信サービスが部分的に復旧し[31]、13 日に、家庭向け固定回線インターネット[32]と音声通信[33]が再開した。モバイル通信は、14 日に一部地域で復旧し、15 日の夜に国内全体で使えるようになった。20 日の国際ローミングサービスの復旧をもって同社は国内外の全てのサービスを完全に復旧させたことを発表。ハッキングの発覚から 1 週間が経っていた。

キーウスターは、サプライヤー企業、特にエリクソンとマイクロソフトによる援助が復旧に寄与したと述べている[34]。

3.3. 犯行声明を発表したハクティビストたち

今回の件は、ロシアのハクティビスト集団「Killnet」が、攻撃の発生した 12 日に Telegram 上で犯行声明を出しているが、それを実行した証拠は示していない[35]。翌日には、ロシアのハクティビスト「Solntsepyok」が、キーウスターのサーバーにアクセスしたことを示すスクリーンショットを添えた犯行声明を Telegram に投稿し、1 万台のコンピューター、4000 台以上のサーバー、すべてのクラウドストレージとバックアップシステムを破壊したと主張している[36]。

---

[28] 出典：WIRED『「ウクライナ全土の停電」を目指していたロシアのハッカー集団、その恐るべき攻撃の中身』
https://wired.jp/article/sandworm-russia-ukraine-blackout-gru/

[29] 出典：Interfax-Ukraine『Attackers hacked Kyivstar's cyber defenses through account of one of its employees – company president』
https://en.interfax.com.ua/news/general/954089.html

[30] 出典：Interfax-Ukraine『Kyivstar restores 100% of services - company president』
https://en.interfax.com.ua/news/general/955479.html

[31] 出典：Interfax-Ukraine『Kyivstar expects to fully restore services on Dec 13』
https://en.interfax.com.ua/news/general/953727.html

[32] 出典：Interfax-Ukraine 『Resumption of all Kyivstar services in compliance with security protocols takes time – security service』
https://en.interfax.com.ua/news/general/953866.html

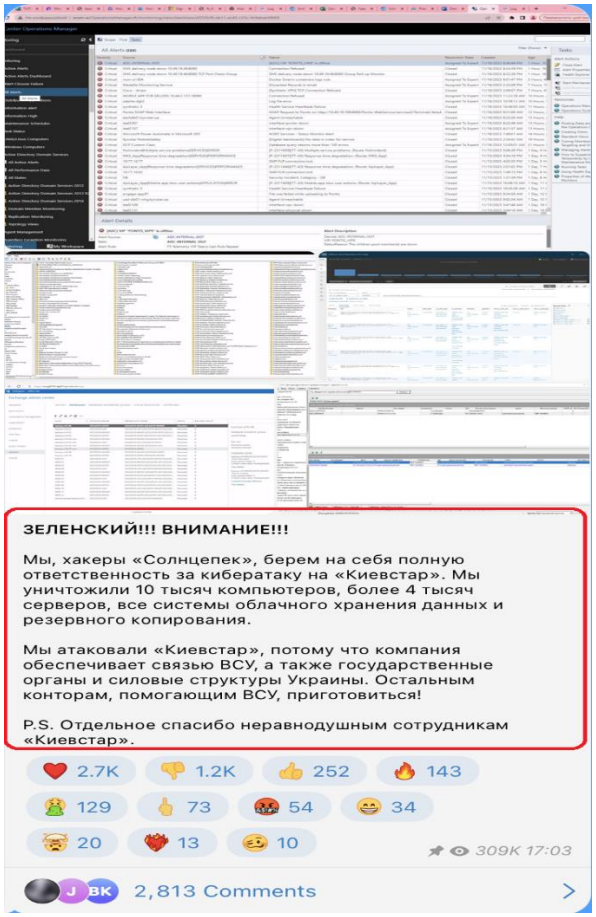
[33] 出典：Interfax-Ukraine 『Kyivstar starts turning on voice communications from 18:00, hopes to restore other services within 24 hours』
https://en.interfax.com.ua/news/general/953965.html

[34] 出典：Interfax-Ukraine『If situation with Kyivstar outage not changed, company's fixed-line network will be disconnected – Kyivstar president』
https://en.interfax.com.ua/news/general/953719.html

[35] 出典：REUTERS『Ukraine's top mobile operator hit by biggest cyberattack of war』
https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/

[36] 出典：REUTERS『Hackers linked to Russian spy agency claim cyberattack on Ukrainian cell network』
https://www.reuters.com/technology/cybersecurity/ukraine-says-russian-intelligence-linked-hackers-claim-cyberattack-mobile-2023-12-13/

© NTT Security Holdings



【赤枠部分の日本語訳】

ゼレンスキー!!!注目!!!

我々、Solntsepyok のハッカーはキーウスターへのサイバー攻撃の全責任を負う。我々は 1 万台のコンピューター、4000 台以上のサーバー、すべてのクラウドストレージとバックアップシステムを破壊した。キーウスターを攻撃したのは、同社がウクライナ軍だけでなく、ウクライナの政府機関や法執行機関に通信を提供しているからである。ウクライナ軍を支援している他のオフィスの皆さん、ご準備を!

追伸:キーウスターの親切な従業員に感謝する。

図 7 Solntsepyok による Telegram での投稿

しかし、サイバーセキュリティの研究者の見解によると、これらのハクティビストたちが今回のような高度なスキルを要する攻撃を画策して実行できたか、実力からみても懐疑的である。投稿されたスクリーンショットも、攻撃の証拠として十分であるか、疑われている。どちらのグループも、犯行声明を出したのは本件についてのメディア報道があった後であり、実行犯であったことが分かる十分な証拠も提示していない。これらの犯行声明については、単に本件への関心を高めようとした、または自らの組織の宣伝であった可能性も考えられる[37]。

3.4. まとめ

ロシア軍はウクライナの重要インフラを破壊するため、ミサイルやドローンで繰り返し攻撃を行っている。今回のキーウスターの事件は物理的な攻撃と同様の効果を、サイバー攻撃で狙ったものと考えられる。重要インフラは使用不能になると他の社会的な機能にも影響が波及する。今回の攻撃ではミサイルの空襲警報システムが機能不全に陥ったが、その最中にミサイル攻撃があった場合に人的被害が拡大する可能性があった。

有事に備えた重要インフラでのサイバー防御の重要性が改めて意識させられる一件であった。

以上

[37] 出典：KELA『Kyivstar 社のインシデントに 関する 5 つの疑問 （とその答え）』
https://www.kelacyber.com/ja/5-questions-and-answers-about-the-kyivstar-attack/

© NTT Security Holdings

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

© NTT Security Holdings