サイバーセキュリティレポート

2023.06

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 2023 年 6 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『CISA がインターネットに公開された管理インターフェイスについて拘束力のある運用指令を発行』

- 米国政府のセキュリティ対策を統括する CISA は、多発するネットワーク内への侵入を背景として、全ての行政機関に対し管理インターフェイスをインターネットに公開しないよう指示する「拘束力のある運用指令」（BOD23-02）を発行した。
- 当指令は、管理インターフェイスをインターネットからアクセスできないよう内部ネットワークからのみのアクセスに限定することを求めている。
- 指令の対象は米国政府機関に限られるが、民間企業でも同様の対策を進めることを推奨する。

第 2 章『社労士事務所向け SaaS「社労夢」のランサムウェア被害』

- 社会保険等の手続きを支援する SaaS「社労夢」等を提供しているエムケイシステムがランサムウェア攻撃の被害に遭い、社労夢を利用している社労士事務所等で業務が滞る影響が出た。
- 個人情報を扱うシステムでサイバー攻撃による被害が発生し漏えいの恐れがある場合、個人情報保護委員会へ報告しなければならない。今回のケースではエムケイシステムだけでなく、社労夢を利用する社労士事務所（委託先）とその顧客企業（委託元）にも報告義務が発生した。
- 個人情報が SaaS から漏えいした場合でも報告義務に迅速に対応できるよう、顧客や社員の個人情報の委託先を洗い出し連携できるようにしておくことが、企業には求められる。

第 3 章『オーナーの逮捕で停止していたハッカーフォーラム「BreachForums」が復活』

- 6 月 13 日、世界最大規模のハッカーフォーラム「BreachForums」が 3 か月ぶりに活動を再開した。閉鎖以前と同様、様々な漏洩情報の投稿やハッキングに関する議論が盛んに行われている。
- 復活後すぐにライバルフォーラムから DDoS 攻撃やハッキングを受けたが特に大きな影響は見られず、現在まで順調にユーザー数を伸ばしている。
- BreachForums は、ハッカー達の間で今後も主導的な位置付けを担うコミュニティとして存在する可能性が高く、投稿される内容や参加しているハッカーの動向には警戒が必要である。

1. CISA が公開された管理インターフェイスについて拘束力のある運用指令を発行

1.1. 概要

2023 年 6 月 13 日、米国土安全保障省サイバーセキュリティインフラセキュリティ庁（CISA：Cybersecurity & Infrastructure Security Agency）は、拘束力のある運用指令 BOD23-02 を発行した[1]。

対象となるのは米国連邦民間行政機関（FCEB: Federal Civilian Executive Branch（以下、「米国政府機関」）のデバイスであり、当指令はネットワーク経由で設定や管理を行うための「管理インターフェイス」がインターネットに公開されている場合に、サイバー攻撃に利用されるリスクを軽減するための措置を強制する。

また、対応が必要となるケースとして想定されているのは、例えば、本来は組織のユーザーのみが利用するはずの Web 管理ポータルのログイン画面がインターネットから誰でもアクセスできる状態となっていること等である。

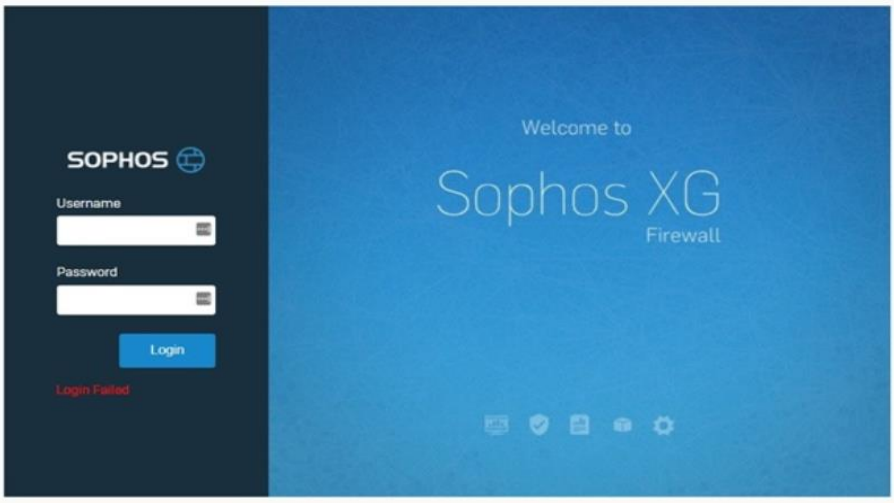

図 1 WEB 管理ポータルのログイン画面（サンプル）[2]

1.2. 背景

米国政府機関は膨大な量の機密データを保持しており、サイバー攻撃で最も標的とされるセクターのひとつであるため[3]、厳重なセキュリティ対策が求められている。しかし、多くの米国政府機関がメンテナンス等のため、外部のインターネットから組織のネットワーク内部にあるデバイスの管理インターフェイスへと直接アクセスできるようにしているのが実情である。管理インターフェイスがインターネット上に公開されている場合、世界中のどこからでも簡単に発見できるため、近年ハッカーに組織のネットワークへの侵入口として悪用されるケースが発生している[4]。CISA はこのような状況を鑑みて、米国政府機関のネットワーク内への侵

[1] 出典：CISA『Binding Operational Directive 23-02』
https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02

[2] 出典：Sophos Community『Web Interface Login Failed 17.03』
https://community.sophos.com/sophos-xg-firewall/f/discussions/100119/web-interface-login-failed-17-03

[3] 出典：InvGate『The 5 Industries Most Vulnerable to Cyber Attacks in 2023』
https://blog.invgate.com/industries-most-vulnerable-to-cyber-attacks

[4] 出典：The Record『CISA orders US civilian agencies to remove tools from public-facing internet』
https://therecord.media/cisa-binding-operational-directive-remove-tools-from-public-internet

入発生を軽減するため、今回の発令に至った[5]。

1.3. 対策

当指令での対象となる管理インターフェイスを有するデバイスには、ルーターやファイアウォール、プロキシー、ロードバランサ等のネットワークデバイスのほか、サーバーも含まれる。

CISA は米国政府機関に対し、管理インターフェイスについて、インターネットからアクセスできないよう内部ネットワークからのみのアクセスに限定することを求めている。もしくは理想的な解決策として、ユーザー管理やポリシーの適用等により内部ネットワークでのアクセスを最小限に制御するゼロトラストアーキテクチャの組み込みを提示している。そして、その設定が出来ていないインターフェイスをインターネット上で発見した日（または CISA が実施するスキャンの結果により通知された日）から 14 日以内に、当該インターフェイスを削除するよう義務付けている。また、新たに追加するデバイスも含めて、その管理インターフェイスが上記のように保護されるよう対策/管理策の実装を要求している。

下記は CISA が提示した管理者（Remote /On-Site Administrator）が組織のネットワーク内にある管理インターフェイスを使用する際の、禁止される構成と許容される構成の例である[6]。

【禁止される構成】

図 2 は、外部（External Entities [同図左上]）からネットワーク内部へのアクセス制御がされておらず、インターネットから管理インターフェイスに接続可能な状態になっているため、禁止とされている。

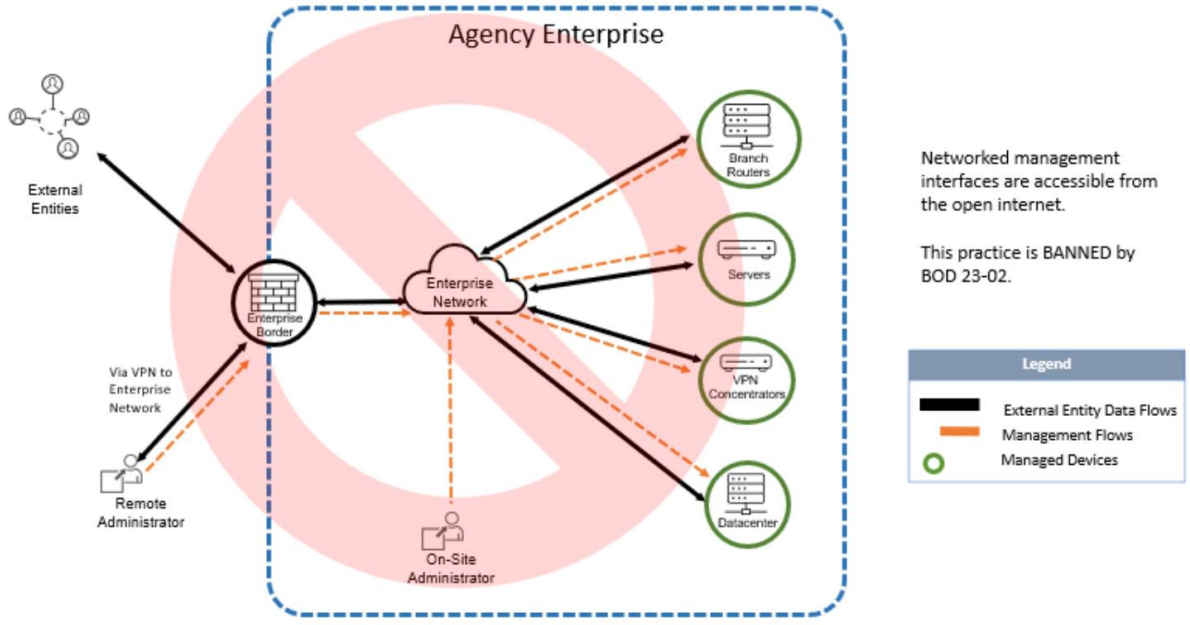

図 2 インターネットからアクセス可能な管理インターフェイス

[5] 出典：CISA『CISA Directs Federal Agencies to Secure Internet-Exposed Management Interfaces』
https://www.cisa.gov/news-events/news/cisa-directs-federal-agencies-secure-internet-exposed-management-interfaces

[6] 出典：CISA『Binding Operational Directive 23-02 Implementation Guidance』
https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02-implementation-guidance

【許容される構成】

以降の構成では内部ネットワークをインターネットから切り離しており、外部からの攻撃が困難であるため、許容される。

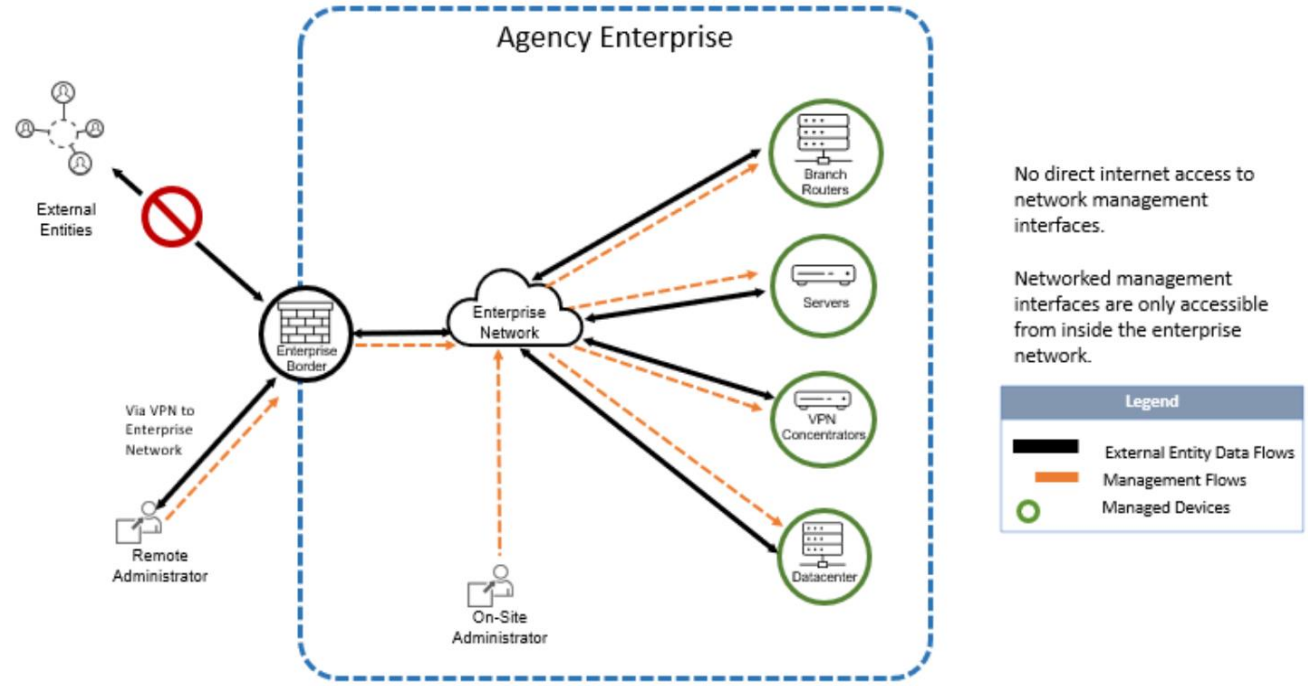

図 3 組織内からのみアクセス可能

（接続を許可した管理者（ネットワーク内部/VPN を経由）のみアクセス可能とする）

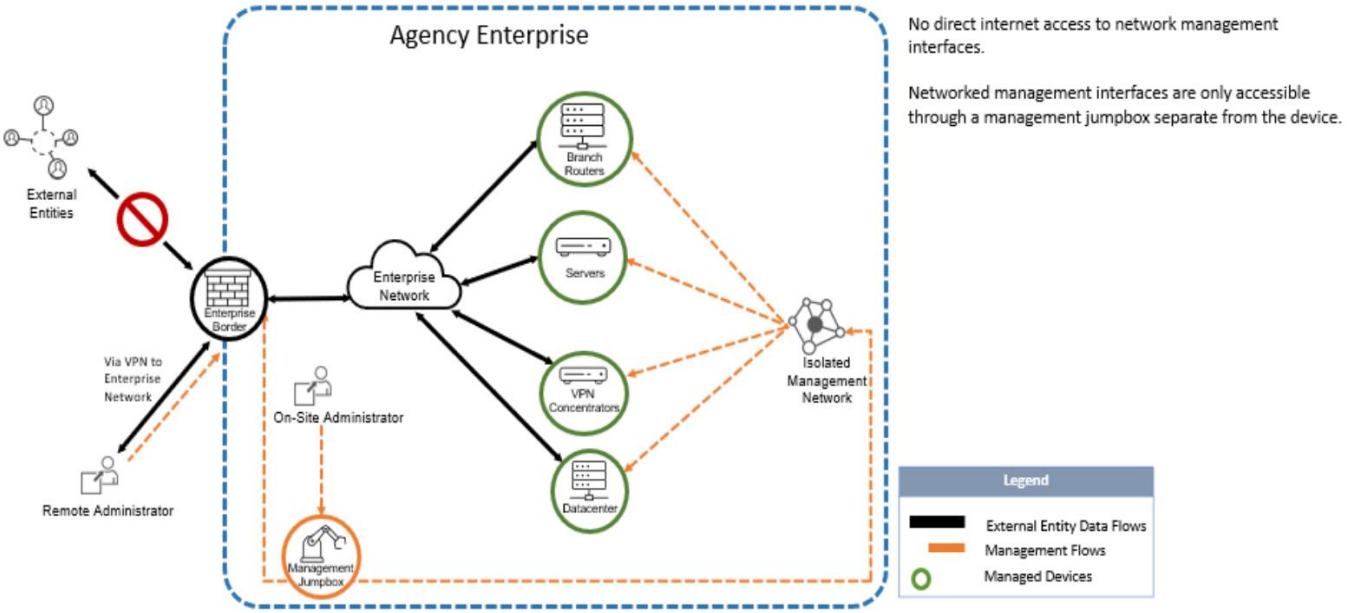

図 4 踏み台サーバーを介してのみアクセス可能

（管理用踏み台サーバー（Management Jumpbox）を介してのみアクセス可能とする ）

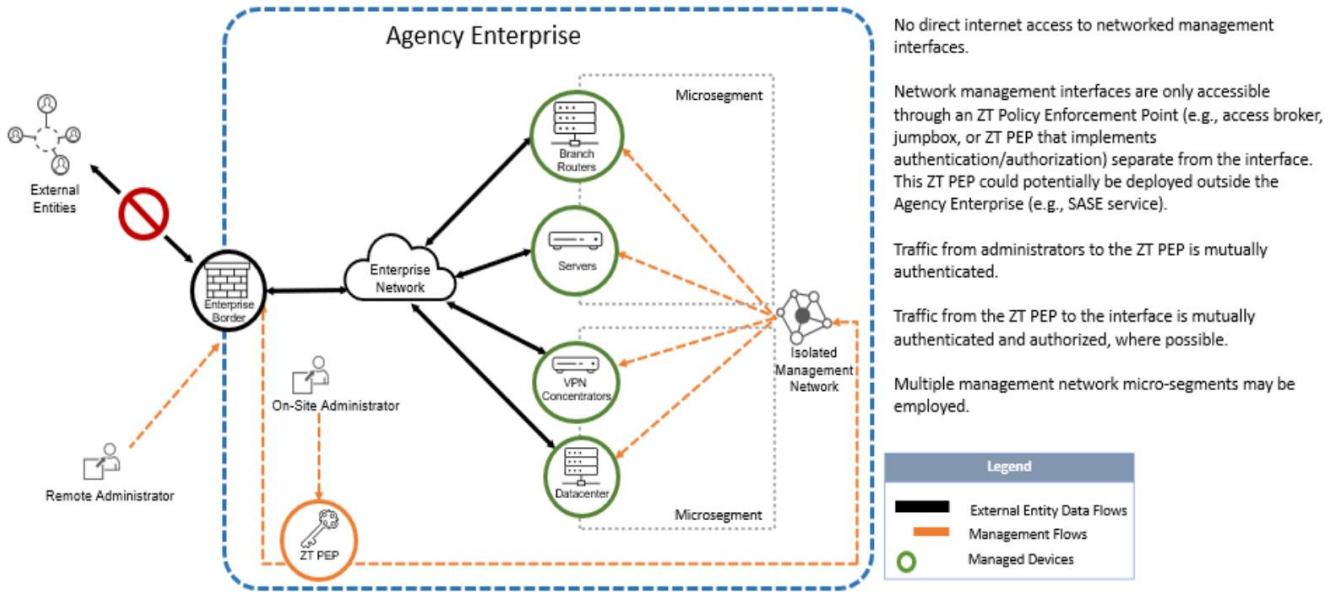

図 5 ZT PEP を介して管理ネットワークのマイクロセグメントからのみアクセス可能

（ZT PEP（ゼロトラストのポリシー実施ポイント）にて認証した
管理者およびその端末に限定しアクセス可能とする）

1.4. まとめ

今回の CISA の運用指令は、管理インターフェイスがシステム管理者のみで利用するものであるため、誰でもアクセスできるインターネットには公開しないという最小権限の原則に従ったものである。これと類似するアドバイザリーや注意喚起は今までにも様々な公的機関が発行しているが、拘束力のある指令として今回 CISA が対応したことは特筆に値し、公開されている管理インターフェイスのリスクが米国政府にとって許容できない状態であることを示している。

指令の対象は米国政府機関に限られるが、攻撃のリスクは官民関わらず存在すると考えられるため、民間企業でも同様の対策を進めることを推奨する。

2. 社労士事務所向け SaaS「社労夢」のランサムウェア被害

2.1. 概要

6 月 5 日、社会保険労務士（以下「社労士」）事務所や企業の人事労務部門向けに SaaS（ソフトウェア・アズ・ア・サービス）の「社労夢」（しゃろうむ）等を提供しているエムケイシステムがランサムウェア攻撃の被害に遭った。これにより、サービスを利用できなくなった社労士事務所の多くで業務に影響が出た[7]。

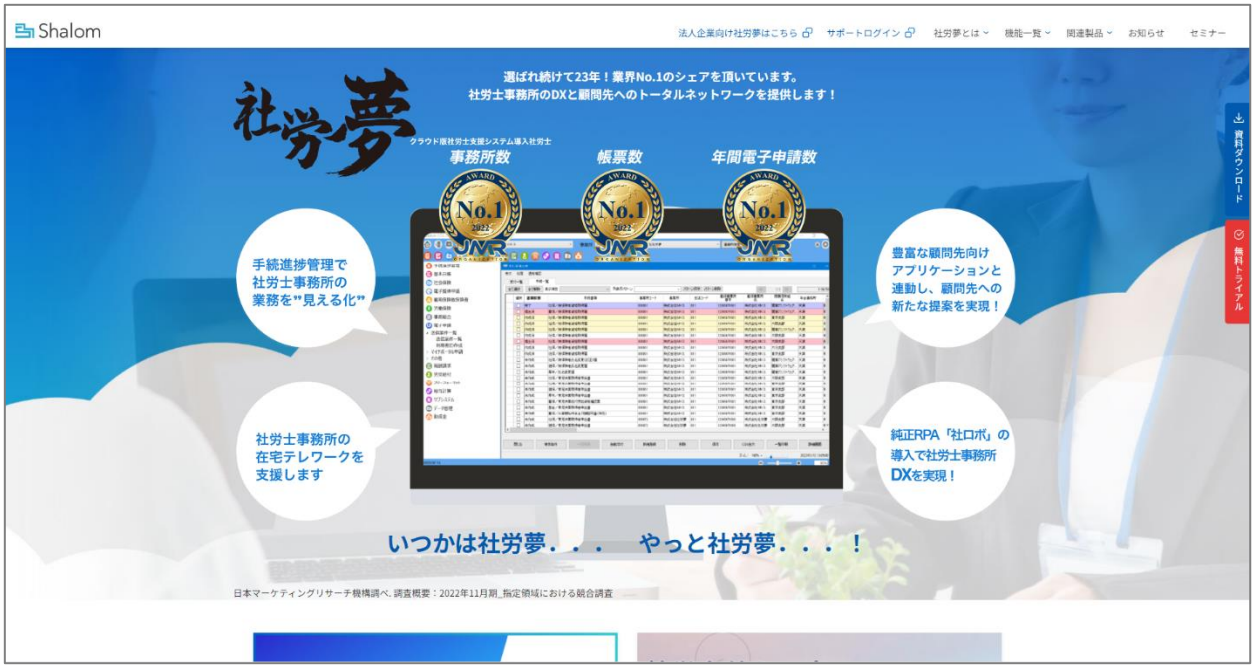

図 6 エムケイシステムの SaaS「社労夢」Web サイト

2.2. エムケイシステムの「社労夢」サービス停止

エムケイシステムは、社会保険等の手続きを支援する Web システム「社労夢」や給与計算システム「ネット de 賃金 WEB 版」といった SaaS を、社労士事務所等に提供している。エムケイシステムは社労夢について、国内社労士事務所の 50.4%が使用する「業界 No.1 のシェア」（図 6）と謳っている[8]。また、これらの社労士事務所により約 57 万事業所、約 826 万人の在職者が社労夢で管理されている[9]。

【ランサムウェア感染被害】

6 月 5 日早朝、サービス提供用のサーバーが全てランサムウェアの暗号化で動作不能になり、「社労夢」等のサービスが提

[7] 出典：ITmedia NEWS『ユーザーの大半にサービス提供できない」 社労士向けシステムのランサムウェア被害、発生から 2 週間たつも完全復旧せず』 https://www.itmedia.co.jp/news/articles/2306/22/news163.html

[8] 出典：株式会社エムケイシステム『社労夢 ｜ シェア No.1 のクラウド社労士業務システム』 https://www.mks.jp/shalom/

[9] 出典：株式会社エムケイシステム『一目でわかるエムケイシステム』 https://www.mks.jp/company/ir-information/ataglance/

供できなくなった。エムケイシステムは、この攻撃により約 3,400 社あるサービス利用事業者の大半が影響を受けたと発表している[10]。

【個人情報の漏えいの可能性について】

エムケイシステムはログ等の調査から、個人情報の漏えいや外部へのデータ送信等の被害の形跡はみられないと発表している。また社労夢等で扱っているマイナンバーは、サービス用の環境とは切り離した環境にあり暗号化もしていることから、悪用等はできない仕組みであると説明している[11]。

【復旧と社労士事務所への影響】

システムのバックアップデータは被害に遭わなかったため[12]バックアップを戻すことで復旧を進めるほか、開発中のシステムの提供時期を前倒しする等により、エムケイシステムは順次サービスを再開している[13]。

一方で社労士事務所にとって、住民税の変更やボーナス支給処理等様々な事務手続きが重なり、1 年の中でも多忙な 6 月に社労夢が使えないことは、まさに悪夢であった。システムで自動化していた処理の多くが手作業になり、社労士事務所の従業員の業務は増大した。前倒しして提供された開発中のシステムもアクセスの集中により不安定であったため、アクセスの減る夜中に起きて毎晩処理をすることで業務の期限に間に合わせた社労士もいた[14]。

2.3. SaaS 利用者と報告義務

個人情報を扱うシステムでサイバー攻撃による被害が発生し漏えいの恐れがある場合は、個人情報保護法に基づき、個人情報保護委員会へ速やかに報告する義務がある。速報として発覚日から 3～5 日以内、その後に確報として発覚日から 30 日以内（サイバー攻撃等の不正な目的による漏えいは、発覚日から 60 日以内）と、期限内の報告が求められている[15]。

報告は、システム提供会社だけでなくシステムを利用する側にも義務付けられている。個人情報保護委員会はガイドラインで[16]、報告義務の主体を「漏えい等が発生し、又は発生したおそれがある個人データを取り扱う個人情報取扱事業者である」と示している。今回のケースでは、エムケイシステムだけでなく、**社労士事務所（委託先）とその顧客企業（委託元）にも報告義務が発生する。**

当初、エムケイシステムはユーザーである各社労士事務所からの報告が免除されるよう、個人情報保護委員会への働きか

---

[10] 出典：日経会社情報 DIGITAL『エムケイシステム[3910]：第三者によるランサムウェア感染被害への対応状況のお知らせ（第 2 報） 2023 年 6 月 21 日(適時開示)』
https://www.nikkei.com/nkd/disclosure/tdnr/20230620507046/

[11] 出典：株式会社エムケイシステム『東京新聞に掲載された記事について』
https://www.mks.jp/company/topics/20230616

[12] 出典：Security NEXT『人事労務システム障害、給与システムを順次提供 - MK システム』
https://www.security-next.com/146843

[13] 出典：株式会社エムケイシステム『一部サービス再開のご報告』
https://www.mks.jp/company/topics/20220703a

[14] 出典：日経クロステック（xTECH）『職場のトラブル相談室 番外編：ランサムウエア攻撃が憎い、顧客の給与支給が間に合うか窮地に立たされる』
https://xtech.nikkei.com/atcl/nxt/column/18/00084/00270/

[15] 出典：個人情報保護委員会『漏えい等の対応とお役立ち資料』
https://www.ppc.go.jp/personalinfo/legal/leakAction/

[16] 出典：個人情報保護委員会『個人情報の保護に関する法律についてのガイドライン（通則編）- 3-5 個人データの漏えい等の報告等（法第 26 条関係）』
https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-5

けをしていたという。しかし、個人情報保護委員会は報告義務に免除の仕組みは無いという見解を崩さなかった。そのためエムケイシステムは社労士事務所に対し、誤って免除の可能性を伝えたことを謝罪した[17]。

なお、報告は委託先と委託元が連名で行うことが認められている。本件では全国社会保険労務士会連合会が連名による報告書のフォーマットを提供[18]し、社労士事務所がそのフォーマットを利用して委託元である顧客企業を取りまとめて、連名で報告する対応が行われた[19]。

2.4. まとめ

ここ数年でランサムウェア攻撃による SaaS での被害が増えている[20]。そのような中で、SaaS に預けた自社の個人情報について、漏えい等の事故を想定しておく必要性が高まっている[21]。

本件では、個人情報を扱う SaaS で事故が発生した場合、サービスを利用している企業、さらにその企業に個人情報を委託している企業にも、個人情報保護法に基づき報告義務が求められることが再確認された。各企業は委託元として、社労士事務所といった個人情報の委託先を洗い出してインシデント対応フローを整理し、漏えい事故発生時に報告等で連携できるよう備えることが重要である。また、国外の居住者の個人情報を扱う場合は、GDPR（EU）等の現地の法規制[22]へ抵触する可能性についての注意や確認が必要である。

---

[17] 出典：朝日新聞 ツギノジダイ『「社労夢」のエムケイシステム、ランサムウェア被害で個人情報漏洩の恐れ』
https://smbiz.asahi.com/article/14930843

[18] 出典：Twitter『東京都社会保険労務士会（公式）』
https://twitter.com/tokyosr_/status/1669609709719130113

[19] 出典：社会保険労務士法人 さくらマネジメントオフィス『過去に弊社と顧問契約及びスポット契約を締結いただいた会社様及び左記の従業員又は従業員であった皆様へのお知らせ』
https://www.sr-sakuram.jp/news/20230703/259/

[20] 出典：Odaseva『New Research: Ransomware Attacks Targeting SaaS Data』
https://www.odaseva.com/blog/new-research-ransomware-attacks-targeting-saas-data/

[21] 出典：日経クロステック（xTECH）『相次ぐ SaaS への攻撃で浮かぶ「嫌な仮説」、事業者は有事に備え再点検を』
https://xtech.nikkei.com/atcl/nxt/column/18/00138/061901311/

[22] 出典：経済産業省九州産業局『令和 3 年度 地域 SECUNITY サイバーセキュリティセミナー 講演「サイバーセキュリティの各国法規制～海外ビジネスにおける頻出論点の解説～」 TMI 総合法律事務所 パートナー （弁護士） 寺門峻佑氏』
https://www.kyushu.meti.go.jp/seisaku/jyoho/pamph/pdf/cs21_2_3.pdf

3. オーナーの逮捕で停止していたハッカーフォーラム「BreachForums」が復活

3.1. BreachForums 復活

サイトのオーナーが逮捕された影響で 3 月に閉鎖された世界最大のハッカーフォーラム「BreachForums」が、新たなオーナーを迎え 6 月 13 日に活動を再開した[23]。

この復活はハッカー達の間で話題となっており、7 月 13 日の時点で 1 万人以上が登録している。閉鎖以前と同様、様々な漏洩情報の投稿やハッキングに関する議論が盛んに行われている。

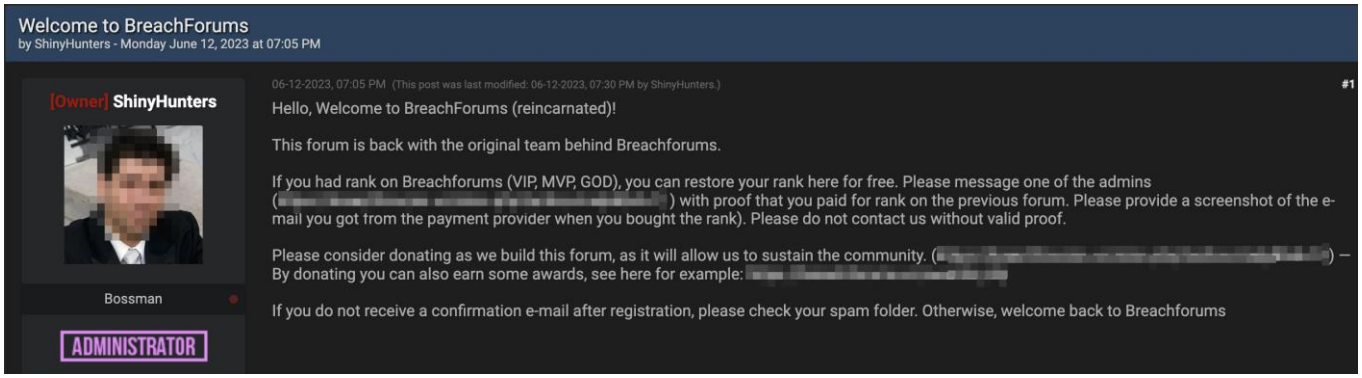

図 7 新たなオーナーとなった ShinyHunters による BreachForums のウェルカムメッセージ（画像を一部加工）
『生まれ変わった BreachForums へようこそ！このフォーラムは元のチームと共に帰ってきました』

3.2. 閉鎖から復活まで

【閉鎖前後の動き】

BreachForums は、2022 年 4 月に当時世界最大のハッカーフォーラムであった「RaidForums」が閉鎖されたことを受け、そのユーザーを勧誘し取り込む形で始まった。その後、更に多くのハッカーを集め、取り扱う漏洩情報のレコード数は 150 億件に達し、RaidForums を凌ぐ規模を誇っていた。

しかし今年 3 月、FBI が BreachForums のオーナーであったコナー・ブライアン・フィッツパトリック（Conor Brian Fitzpatrick [別名：pompompurin]）というハッカーを逮捕。この時、フォーラムのシステムは共同管理者たちによって運用されていたが、彼らは捜査当局がフィッツパトリックから押収した管理者権限を使用してアクセスしている可能性等を危惧し、BreachForums を閉鎖した。

これらの管理者たちのうち、フォーラム閉鎖の決定や、今後の方針の検討などを主導していたのは「Baphomet」と名乗る人物であった。Baphomet は、フォーラムが閉鎖されている間も BreachForums のユーザー達が会話できるように、Telegram 上にチャットグループを開設した。これには 4,000 人以上が参加し、新しいフォーラムの在り方に関する議論や、後釜狙いの新興フォーラムへの悪態等、ごく日常的なチャットが行われていた。

Baphomet はフォーラムの閉鎖を決めた時点ですでに複数の競合するフォーラムの管理者等から連絡を受けていたようで、将来的にそのうちの何人かと協力して BreachForums の機能を備えた新たなコミュニティを構築したいと語っていた。

[23] 出典：Cybernews『BreachForums is back – for real this time』
https://cybernews.com/security/breachforums-back-online/

【新たなオーナー：ShinyHunters】

BreachForums の閉鎖から約 3 か月後、新たにオーナーとなった「ShinyHunters」が、「フォーラムが帰ってきた」という宣言と共に BreachForums の新しい URL を、前述の Baphomet のチャットグループに投稿した。

ShinyHunters は、Microsoft の GitHub アカウントに対するハッキング[24]や、PDF ソフト「Nitro PDF」のユーザーデータおよそ 770 万件の窃取[25]といった、様々な組織への攻撃を行っている悪名高いハッカーグループである。

新しくなった BreachForums は、ShinyHunters、そして Baphomet を含む以前の管理者たちが協力しながら運営している。

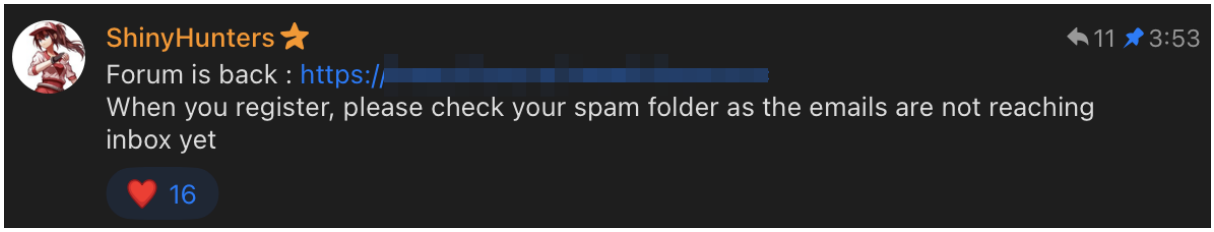

図 8 BreachForums の再開を告げる ShinyHunters の投稿（画像を一部加工）

3.3. 閉鎖に対する他のハッカーフォーラムの反応

3 か月前の BreachForums は世界最大のハッカーフォーラムであった。このため、同フォーラムの閉鎖後に行き場を失ったユーザーを囲い込もうと、多くの同様のフォーラムが新設され、既存のフォーラムも交えてユーザーの争奪戦となった。

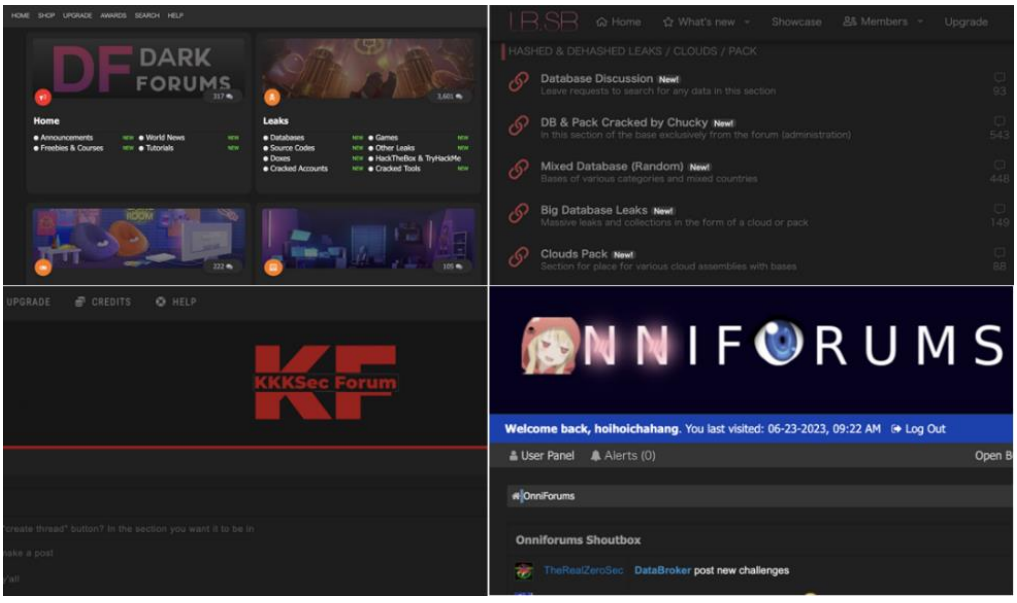

図 9 BreachForums の閉鎖後に活発になったフォーラムの例

[24] 出典：HACKREAD『Hackers claim to breach Microsoft's GitHub account; steal 500GB of data』 https://www.hackread.com/hackers-breach-microsoft-github-account-steal-500gb-data/

[25] 出典：Bleeping Computer『Hacker leaks full database of 77 million Nitro PDF user records』 https://www.bleepingcomputer.com/news/security/hacker-leaks-full-database-of-77-million-nitro-pdf-user-records/

それらのフォーラムは Telegram や Twitter 等の SNS 上で宣伝を行ったり、過去に大企業や政府組織から漏洩したデータを再利用して作成したメッセージを自身のフォーラムに投稿したりすることで、ハッカー達の注目を集めようとしていたが、以前の BreachForums のように突出してユーザー獲得に成功したところはなかった。

【新生 BreachForums への攻撃】

BreachForums の復活後、同フォーラムからのユーザーの奪取を諦めて閉鎖する競合フォーラムもあったが、BreachForums の活動を妨害しようと、攻撃を仕掛けるところもあった。

たとえば、BreachForums は復活後 1 時間も経たないうちに DDoS 攻撃を受け、不安定な状態となった。同フォーラムの管理者の一人は、ライバルフォーラム「Exposed」の管理者が DDoS 攻撃サービスを利用してこの攻撃を行ったと主張した[26]。

また、別のフォーラム「OnniForums」の管理人「dkota」が、ゼロディ脆弱性を利用して BreachForums のシステムを攻撃し、データを窃取した。そして、BreachForums のユーザー約 4,000 人分のメールアドレスや接続元 IP アドレス等のデータを自身のフォーラムに投稿した[27]。ShinyHunters は、ハッキングを受けたことを認め、ユーザーに対する謝罪文を投稿した。

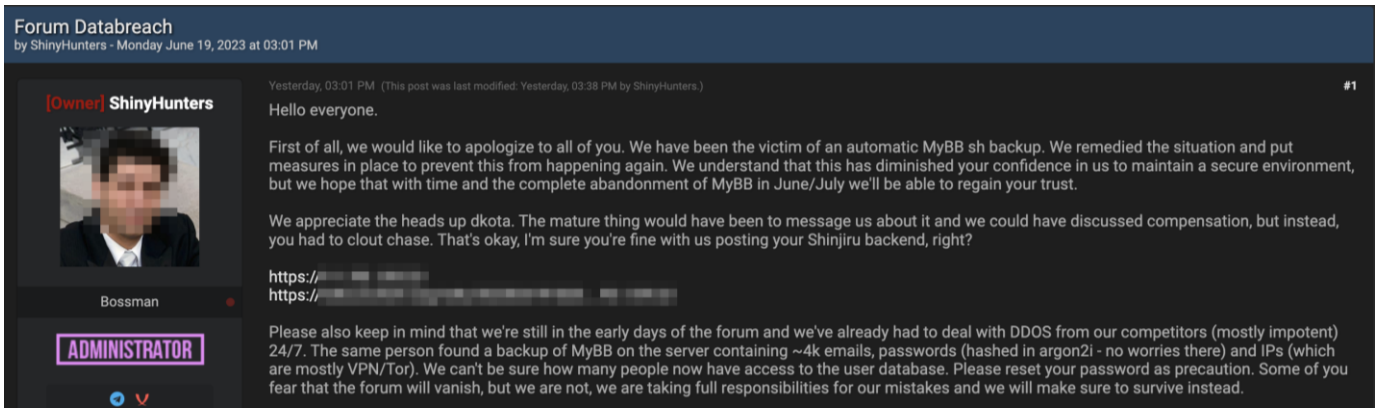

図 10 ハッキングを受けたことを謝罪する ShinyHunters の投稿（画像を一部加工）

ハッカー達の間では VPN や匿名性の高いメールサービスの利用が常識となっていることもあり、この攻撃によって漏洩したデータでは身元の露見等の被害に繋がらず、同フォーラムはその後も順調にユーザー数を増やし続けている。

3.4. まとめ

BreachForums の復活は、多くのハッカーやその予備軍から歓迎されているようである。同フォーラムの前身である RaidForums の時代から、様々な国籍、技量のハッカー達が参加しており、営利目的やハッカーとしての名声を得るために漏洩情報を投稿するだけではなく、雑談したりハッキング技術を教えあったりする場ともなっており、英語圏では最大のハッカーコミュニティを形成している。参加者たちは多くのサイバー攻撃に関与しており、その結果、BreachForums には大量の漏洩デー

[26] 出典：DataBreaches.net『The “reincarnation” of BreachForums: A cyberdrama in three acts』 https://www.databreaches.net/the-reincarnation-of-breachforums-a-cyberdrama-in-three-acts/

[27] 出典：DataBreaches.net『Confused about the drama with the new BreachForums? Reading this will either help you or make your head spin.』 https://www.databreaches.net/confused-about-the-drama-with-the-new-breachforums-reading-this-will-either-help-you-or-make-your-head-spin/

タベースが蓄えられている。今後も同フォーラムは、ハッカーコミュニティとして主導的な位置付けを担う可能性が高く、投稿される内容や参加しているハッカーの動向には警戒が必要である。

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