サイバーセキュリティレポート

2023.09

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

【1 ページサマリー】

当レポートでは 2023 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『「AKIRA」による Cisco ASA への攻撃と、ランサムウェア攻撃マニュアル』

- 9 月 6 日、米 Cisco 社は、Cisco ASA 及び FTD に脆弱性「CVE-2023-20269」があることを発表した。本脆弱性はこの発表時点で既に AKIRA ランサムウェアグループによって攻撃に利用されていた。
- AKIRA ランサムウェアグループは、ウクライナのランサムウェアオペレーターが作成したマニュアルに沿った攻撃を行っている可能性がある。
- マニュアルを分析した結果、攻撃手順の多くは防御可能な既知のものであったが、一方でゼロデイ脆弱性を悪用するものもあった。システムを最新の状態に保つといった基本的なセキュリティ対策の実施に加え、攻撃者の情報を積極的に収集することも重要である。

第 2 章『米国防総省が 2023 年のサイバー戦略を公表』

- 9 月、米国防総省は今年 5 月に議会に提出したサイバー戦略の要約版を公表した。
- 以前の米軍はサイバー攻撃に対して防御・抑止を中心とした姿勢であったが、2020 年や 2021 年に民間部門を起点とした大規模インシデントやウクライナ戦争での Hunt Forward が、国防総省の意識を大きく変えた。
- 新たな戦略では、米国の同盟国やパートナーのサイバー能力構築の支援を行い、協力してサイバー空間における対応能力を向上させることに、新たに重点を置いている。

第 3 章『企業公式サイトに破産の告知、改ざん被害が相次ぐ』

- 9 月初め、改ざんにより企業公式サイトに破産等の虚偽の告知が掲載される被害が、日本全国で相次いだ。
- 企業公式サイトの改ざんだけでなく、メール配信システムへの不正アクセスにより同様の告知のメールが送信されたケースもあり、被害企業は対応に追われた。
- 企業経営に影響を及ぼしかねない改ざんであり、経営を守るためには、公式サイト等の企業情報を公開するシステムのセキュリティ対策が欠かせないことを再認識させられる事件であった。

1.「AKIRA」による Cisco ASA への攻撃と、ランサムウェア攻撃マニュアル

1.1. 概要

図 1 Cisco ASA シリーズ

9 月 6 日、米国のネットワーク大手 Cisco Systems は、同社のファイアウォール機能付き VPN デバイス「Cisco Adaptive Security Appliance（ASA）」及び、ソフトウェア VPN「Cisco Firepower Threat Defense（FTD）」に、脆弱性「CVE-2023-20269」があることを発表した[1]。

Cisco ASA や FTD で多要素認証が使用されていない場合、攻撃者が本脆弱性を悪用すると、ブルートフォース攻撃等で認証を突破し、SSL VPN セッションを確立できる。春頃から「AKIRA」ランサムウェアグループによって悪用されているが、10 月 11 日に修正版の提供が行われるまで、ゼロデイ脆弱性の状態が続いていた。

1.2. AKIRA ランサムウェアグループ

AKIRA ランサムウェアグループ（以下、AKIRA）は、今年 3 月から活動が確認されている。Cisco ASA の他、仮想環境構築ソフトウェア「VMware ESXi」を利用している企業も AKIRA の被害に遭っている[2]。特定の産業をターゲットにすることはなく、医療、製造、石油・ガス等、様々な分野の企業への攻撃が確認されている。日系企業では、7 月にヤマハ・カナダ・ミュージック（Yamaha Canada Music Ltd.）も被害を受けている[3]。

図 2 AKIRA の暴露サイト

[1] 出典：Cisco Systems『Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Access VPN Unauthorized Access Vulnerability』
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

[2] 出典：Bleeping Computer『Linux version of Akira ransomware targets VMware ESXi servers』
https://www.bleepingcomputer.com/news/security/linux-version-of-akira-ransomware-targets-vmware-esxi-servers/

[3] 出典：Malwarebytes『Ransomware groups claim responsibility for double-attack on Yamaha』
https://www.malwarebytes.com/blog/news/2023/07/ransomware-groups-claim-responsibility-for-double-attack-on-yamaha

1.3.「ネットワーキングマニュアル」

AKIRA は Cisco ASA へのログイン時にブルートフォース攻撃を行っている。これは、「Мануал по работе с сетями（ネットワーキングマニュアル）」に記載されている手法であると専門家は指摘している[4]。このマニュアルの著者は、ウクライナのランサムウェアオペレーターであり、REvil 等のランサムウェアグループで活動していた[5]。マニュアルは、2021 年に無料配布された初期バージョンと、その後 2022 年 12 月に発表され有償で配布されたバージョン 2.0 があり[6]、いずれもランサムウェアグループ等の攻撃者の間で流通している。

図 3 マニュアルの表紙（バージョン 2.0 より）

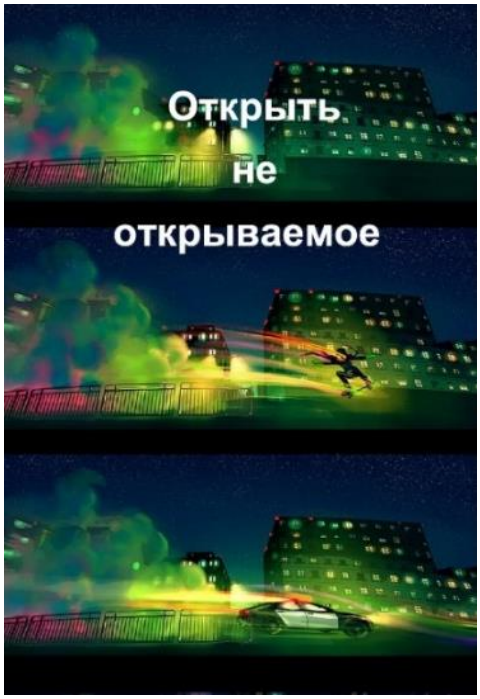

図 4 ネットワークへの侵入に関する章の扉絵「開かないものを開ける」（バージョン 2.0 より）

インターネットに流出した両方のマニュアルを入手し、分析を行った。初期バージョンが 63 ページ、バージョン 2.0 が 24 ページあり、バージョン 2.0 は初期バージョンの改訂版ではなく、補完的な位置付けにある。

初期バージョンの序文に記載されているように、このマニュアルには「特定のエクスプロイトがどう機能するかという意味のない説明や理解できないコードの山はなく、すぐに実際に適用可能な」手順が記載されている。攻撃に必要な環境の構築にはじまり、VPN 装置への攻撃、企業ネットワークに侵入後のドメインコントローラーの攻略、権限昇格、アンチウイルスの攻略、といったように実際の攻撃の流れに沿って章立てされている。特に、Cisco の VPN に関しては、AKIRA が行っているとみられるブルートフォース攻撃を実施する手順が、バージョン 2.0 で具体的に説明されている（**図 5**）。

---

[4] 出典：Rapid7『Under Siege: Rapid7-Observed Exploitation of Cisco ASA SSL VPNs』
https://www.rapid7.com/blog/post/2023/08/29/under-siege-rapid7-observed-exploitation-of-cisco-asa-ssl-vpns/

[5] 出典：The Record『The hacker ******** in his own words: Portrait of an access broker as a young man』
https://therecord.media/bassterlord-interview-hacker-initial-access-broker

[6] 出典：Analyst1『Ransomware Diaries: Volume 2 – A Ransomware Hacker Origin Story』
https://analyst1.com/ransomware-diaries-volume-2/

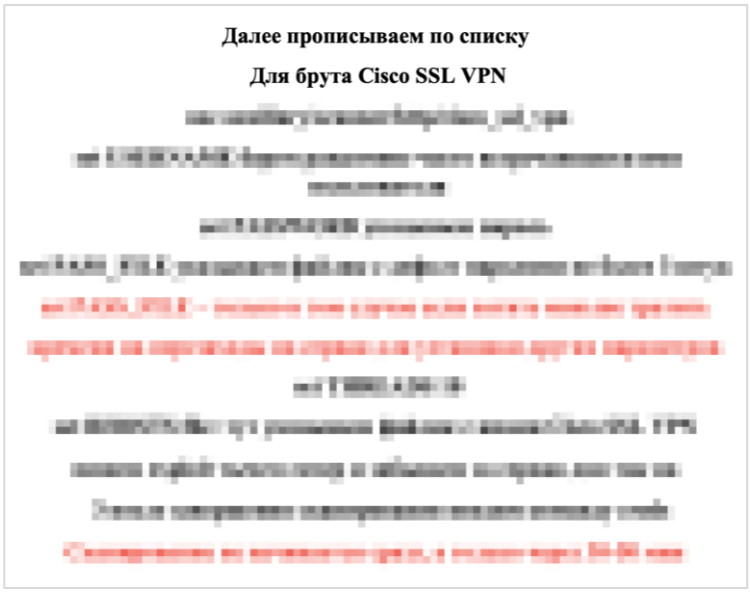

図 5 マニュアルより①

ページ上部の和訳「次にリストを作成する。Cisco SSL VPN をブルートフォース攻撃する場合…」

また、前述の「VMware ESXi」を対象にした攻撃に関する記述も確認できる（**図 6**）。

図 6 マニュアルより②

ページ下部の抄訳「…その結果、ESXi からのパスワード窃取を可能にするコンピューターの情報が手に入る」

なお、マニュアルの著者はインタビューで、コードの書き方をほとんど知らない者がそのマニュアルを持っていればランサムウェア攻撃が可能か、という質問に対し、**両方のバージョンのマニュアルを持っていれば可能である**[7]、と回答している。

[7] 出典：The Record『The hacker ******** in his own words: Portrait of an access broker as a young man』 https://therecord.media/bassterlord-interview-hacker-initial-access-broker

1.4. まとめ

マニュアルの分析から、記載されている多くの作業手順は既知のものであり、最新のセキュリティ対策や適切な設定の実施によって、防御は十分に可能であることが分かった。一方で、ベンダーが発見できていなかった脆弱性を悪用する手法が、攻撃者の間では、既に昨年 12 月から知られていた可能性があることも判明した。

システムを最新の状態に保つといった基本的なセキュリティ対策の実施に加え、攻撃者の情報を積極的に収集し、攻撃を未然に防ぐことも重要である。

2. 米国防総省が 2023 年のサイバー戦略を公表

2.1. 概要

2023 年 9 月 12 日、米国国防総省（United States Department of Defense [DoD]）が、サイバー戦略の要約（2023 DoD Cyber Strategy Summary[8] [以下、DoD サイバー戦略]）を公表した。これは今年 5 月に連邦議会に提出されていたサイバー戦略から機密部分を除いたもので、約 5 年ぶりの改訂となる[9]。

米国ではサイバー空間における様々な脅威の増大に直面しており、DoD サイバー戦略ではそのリスクを抑止する方法や、国内防衛を推進するための活動方針などについて説明している[10]。

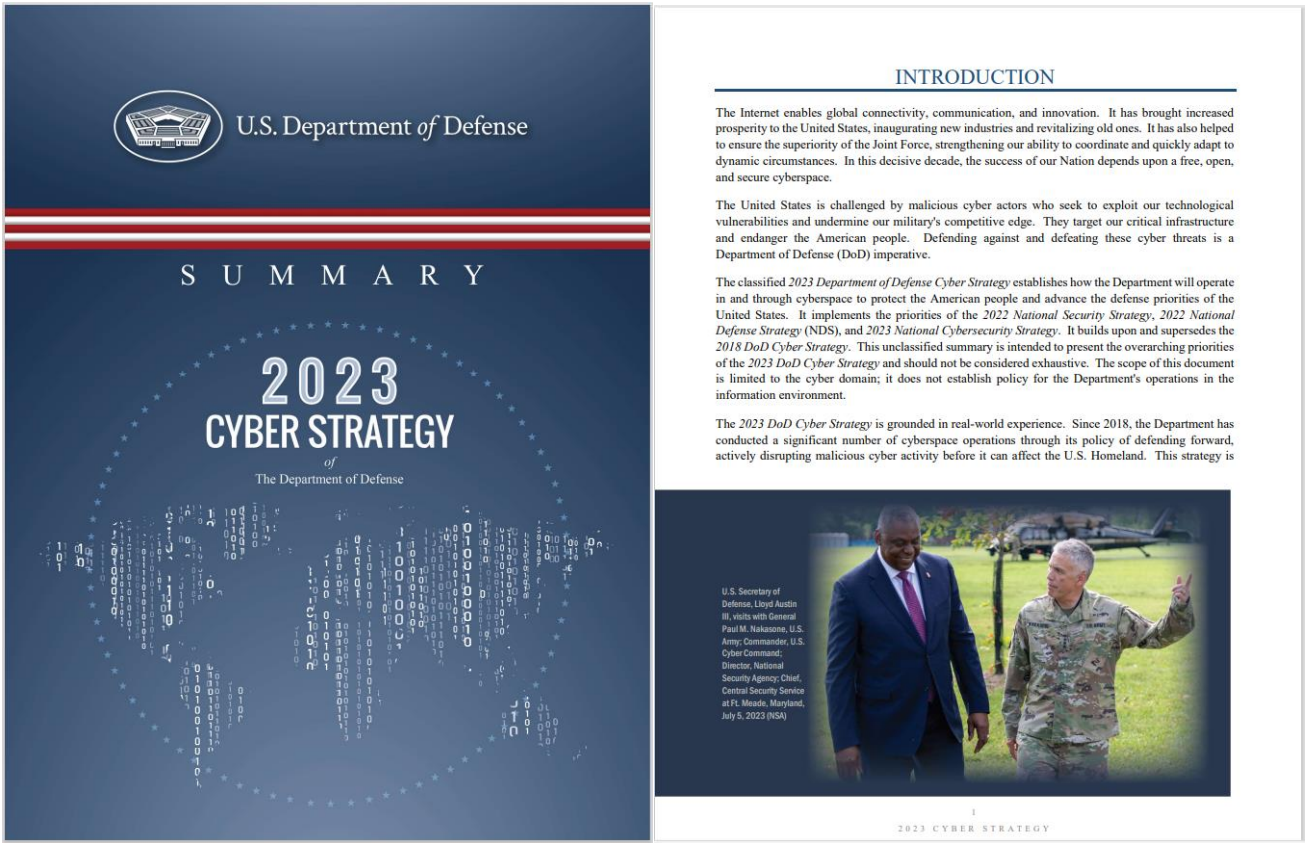

図 7 2023 DoD Cyber Strategy Summary の表紙と INTRODUCTION[11]

[8] 出典：U.S. Department of Defense『2023 DOD Cyber Strategy Summary』
https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

[9] 出典：毎日新聞『中国の「デジタル権威主義」台頭に警鐘 アメリカ国防総省の新戦略』
https://mainichi.jp/articles/20230913/k00/00m/030/043000c

[10] 出典：Cyber Daily『US DOD releases 2023 cyber strategy to combat emerging threats』
https://www.cybersecurityconnect.com.au/defence/9585-us-dod-releases-2023-cyber-strategy-to-combat-emerging-threats

[11] 出典：U.S. Department of Defense『2023 DOD Cyber Strategy Summary』
https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

2.2. 変化する DoD サイバー戦略

DoD サイバー戦略はこれまで、2011 年、2015 年、2018 年と改訂されてきた。

オバマ政権下の 2011 年 7 月に公表された最初の DoD サイバー戦略は、あくまでも防衛体制の強化のためであり、サイバー空間を「軍用化」する意図はないことが強調されていた[12]。

その後、米国に重大な影響のあるサイバーインシデントが増加したことにより、方針が変化した。2015 年に発行された戦略では、前回のような楽観的にも見える印象は薄れ、最大限に警戒すべき敵対者として、ロシア、中国、イラン、北朝鮮、非国家主体を名指しした。しかし、この時点でもサイバー脅威の対処において軍に頼ることは避け、抑止のアプローチを維持するとしていた[13]。

2016 年の米大統領選挙でのロシアのサイバー情報工作を経て 2018 年に発行された戦略は、「我々の利益を断固として守る」とし、抑止中心の体制から「一歩踏み込んだ防衛」を行うことにした。つまり、悪意あるサイバー活動の発生源に米国が積極的に関わって敵を混乱させ、攻撃を妨害・阻止するという「Defend Forward（ディフェンド・フォーワード：前方防衛）」という新しい概念の追加である[14, 15]。

また、「Persistent Engagement（パーシステント・エンゲージメント：継続的従事）」も積極的な姿勢への変化を意図したものである。これは、サイバー空間で発生するインシデントに積極的に関わり、対処・対応を行うことで、有事の際の対応能力を継続的に上げ、国家の安全を脅かされるような破壊的な被害を未然に防ぐことを狙ったものである[16]。

このような Defend Forward や Persistent Engagement などの概念を取り入れることで、米軍は防御や抑止中心の体制から抜け出すことを狙っていた。

2.3. 2023 年の DoD サイバー戦略について

今回公表されたサイバー戦略の概要では、米国に対する根強い脅威として、中国、ロシア、北朝鮮、イラン、暴力的過激派組織、国外の犯罪組織を挙げ、米軍の対応能力向上を目指すと述べている[17, 18]。名指しされた国／組織の中では、特に中国からの脅威について踏み込んだ印象が強い。また、新たに同盟国やパートナーとの協力を強めることについて、項目が追加されている[19]。

---

[12] 出典：日本経済新聞『米、サイバー空間の防衛力増強　国防総省が戦略発表』
https://www.nikkei.com/article/DGXDZO32274060V10C11A7EB2000/

[13] 出典：OXFORD ACADEMIC『The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation』
https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988

[14] 出典：OXFORD ACADEMIC『The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation』
https://academic.oup.com/cybersecurity/article/9/1/tyad006/7097988

[15] 出典：U.S. Department of Defense『CYBER STRATEGY SUMMARY FINAL』
https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[16] 出典：U.S. Department of Defense『CYBER STRATEGY SUMMARY FINAL』
https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[17] 出典：Cyber Daily『US DOD releases 2023 cyber strategy to combat emerging threats』
https://www.cybersecurityconnect.com.au/defence/9585-us-dod-releases-2023-cyber-strategy-to-combat-emerging-threats

[18] 出典：U.S. Department of Defense『2023 DOD Cyber Strategy Summary』
https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

[19] 出典：U.S. Department of Defense『DOD's Cyber Strategy Emphasizes Building Partner Capacity』
https://www.defense.gov/News/News-Stories/Article/Article/3523840/dods-cyber-strategy-emphasizes-building-partner-capacity/

【米国のサイバー被害と方針の転換】[20], [21], [22], [23], [24]

2018 年のサイバー戦略立案後も国防総省は米軍のネットワークをサイバー攻撃から守ることに多くのリソースを集中させていた。しかし、米軍のネットワークではないところで大規模なサイバー攻撃が相次いだ。

2020 年 12 月、ロシア対外情報庁（SVR）による SolarWinds 製品の大量ハッキング事件が発生。同社の顧客には米フォーチュン誌が発行する「Fortune 500」に名を連ねる多くの企業や米政府の機関が含まれていた。これにより、米軍を含む政府関連の機密情報が窃取されたのではないかと考えられている。

また、2021 年 5 月には、米東海岸のコロニアル・パイプライン社がロシア拠点のハッカー集団「DarkSide」によるランサムウェア攻撃を受け、東海岸のガス供給の約半分が停止する事件が発生した。これは米国の市民生活に大きな混乱をもたらした。同じ頃、ブラジルでは世界最大の食肉加工会社 JBS が、ランサムウェアグループ「REvil」による攻撃を受けて事業が停止し、米国でも食肉の供給に影響が出る可能性があった。

米国の組織や社会に甚大な被害を与えたこれらの事件は米国政府に衝撃を与え、大統領は事件直後の 2021 年 5 月に「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 1402835）」を発出した。本来守るべき国土・国家が守られていないということから、国防総省がサイバーセキュリティは国家安全保障であると認識するきっかけとなった。この流れを受け、2023 年のサイバー戦略では、米軍のネットワークのみならず米国の政府機関や重要インフラを担う民間企業等との連携によるサイバー能力向上が重視されている。

【Hunt Forward】[25], [26], [27]

今回の DoD サイバー戦略は、2018 年からの「Persistent Engagement（継続的従事）」の一環として、「Hunt Forward（ハントフォーワード）」を推進している。これは米サイバー軍が、同盟国やパートナーからの要請を受けた上で防衛要員を派遣し、システム内を調査することにより、脆弱性のあぶり出しやマルウェアの検出を行い、対処方法をアドバイスすることである。

Hunt Forward チームは 2022 年のロシアによるウクライナ侵攻の際にも派遣されており、ロシアのサイバー攻撃からウクライナを守ることに寄与しただけでなく、サイバー戦争におけるロシアの戦略・戦術などの貴重な情報を持ち帰ることに成功していた。

---

[20] 出典：GIZMODE『SolarWinds ハッキング事件について現在までわかっていること』
https://www.gizmodo.jp/2020/12/what-we-know-so-far-about-the-solarwinds-hacking-scandal.html

[21] 出典：REUTERS『'Flattered' Russian spy chief denies SolarWinds attack - BBC』
https://www.reuters.com/technology/russian-spy-chief-denies-svr-was-behind-solarwinds-cyber-attack-bbc-2021-05-18/

[22] 出典：BBC NEWS JAPAN『米 FBI、食肉加工最大手へのサイバー攻撃はロシア系ハッカーと』
https://www.bbc.com/japanese/57339918

[23] 出典：Tokio Cyber Port『コロニアル・パイプライン事件他で米国サイバーセキュリティは激変予感』
https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/column-detail93

[24] 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/

[25] 出典：U.S. CYBER COMMAND『U.S. Cyber Command 2022 Year in Review』
https://www.cybercom.mil/Media/News/Article/3256645/us-cyber-command-2022-year-in-review/

[26] 出典：日本経済新聞『米軍のサイバー戦略、中国の本土攻撃警戒 同盟国と連携』
https://www.nikkei.com/article/DGXZQOGN131AW0T10C23A9000000/

[27] 出典：Wedge ONLINE『法的制約で米軍からの訓練断る 自国を守れないニッポン』
https://wedge.ismedia.jp/articles/-/29268?page=3

【同盟国やパートナーとのサイバー領域における連携強化】[28], [29]

前述のような重大なセキュリティインシデントが多発したことや、Hunt Forward で実績を積んだことにより、国防総省は同盟国やパートナーとのコミュニケーションや防衛支援の必要性を実感し、2023 年のサイバー戦略では、ともにサイバー空間を守るという方針に発展させることとなった。

サイバー政策担当の Mieke Eoyang 国防副次官補は、次のように述べている。

「これまでとは異なり、今回の DoD サイバー戦略は同盟国やパートナーとサイバー能力を構築することにより、サイバー攻撃に対する我々の集団的なレジリエンスを高めることを約束するものである。同盟国やパートナーは、競争相手が太刀打ちできない戦略的優位性を持っている。」

図 8 9月 12 日、ワシントン D.C.のペンタゴンで記者会見をする Mieke Eoyang 国防副次官補 [30]

2.4. まとめ

米国のサイバー戦略は 2011 年から 3 回の改訂を行っているが、公表当時の情勢に合わせ、サイバースペースの脅威と軍の関わり方が大きく変化してきた。

新たなセキュリティ戦略により、今まで民間部門や同盟国で野放しになっていた敵対勢力の活動に牽制／封じ込めを行う方向性が示された。この戦略の進展により、米軍や同盟各国でのサイバー対応能力が高まることが期待される。

---

[28] 出典：毎日新聞『中国の「デジタル権威主義」台頭に警鐘 アメリカ国防総省の新戦略』
https://mainichi.jp/articles/20230913/k00/00m/030/043000c

[29] 出典：U.S. Department of Defense『DOD's Cyber Strategy Emphasizes Building Partner Capacity』
https://www.defense.gov/News/News-Stories/Article/Article/3523840/dods-cyber-strategy-emphasizes-building-partner-capacity/

[30] 出典：DEFENSE DAILY『DoD's New Cyber Strategy Includes Developing Tech To 'Confound' Malicious Actors』
https://www.defensedaily.com/dods-new-cyber-strategy-includes-developing-tech-to-confound-malicious-actors/cyber/

3. 企業公式サイトに破産の告知、改ざん被害が相次ぐ

3.1. 概要

企業公式サイトのトップページに破産等の虚偽の告知が掲載される事件が、9 月初めに日本全国で相次いだ。不正アクセスによる改ざんとみられている [31]。

3.2. 不正アクセスによる、虚偽情報の告知

【サイト改ざん】

8 月 31 日から 9 月 4 日にかけ、複数の企業公式サイトで、業績悪化等を理由として「2023 年●月●日付で破産手続きを開始いたしました。」といった告知文が掲載されているのが確認された。被害企業は実際には破産しておらず、これらの告知文は事実無根の虚偽であった。何者かが Web サーバーへ不正アクセスを行い、被害企業が気付かないうちにコンテンツを書き換えたとみられている [32]。

このような改ざんが同時期に、全国で少なくとも 7 件 [33]あったことが確認されている。業種や地域等に規則性は無いが、いずれも告知の内容等が類似していることから、一連の事件と考えられている。

【なりすましメール】

不正アクセスが行われたのは Web サーバーだけではなかった。メール配信システムを利用している複数の被害企業においては、同システムへの不正アクセスもみられた。メールマガジン登録者等に対し、破産を告知する虚偽の成りすましメールが送信された。被害に遭った精肉店のケースでは、保健所から食中毒発生の連絡があり、債務不履行に陥ったとの破産の理由まで、でっち上げられていた [33]。

脆弱性のあるメール配信システム「acmailer」を狙って不正アクセスし、虚偽の内容のメールを送信する事件が今回の事件前から度々あったため、本件でも同様の手口が使われたと考えられている。実際に事件に前後して、京都府警 [34]やホスティング事業者 [35]がサーバー管理者に対し acmailer の脆弱性悪用についての注意喚起を行っている。

【被害対応】

被害企業は、これらの告知が虚偽であることの発表や連絡に追われた。各企業は警察に被害届を出しており、偽計業務妨害の可能性で捜査が進められている。また、メール配信システムに侵入された企業は、システムに保存していたメール配信先の

---

[31] 出典：ITmedia NEWS『公式サイトに「破産した」の偽情報 改ざんの被害続々 研修施設、コンサルなどで』
https://www.itmedia.co.jp/news/articles/2309/04/news118.html

[32] 出典：ねとらぼ『「破産手続きを開始しました」 企業サイトの改ざん被害、全国で相次ぐ 「餃子の王将」運営会社も』
https://nlab.itmedia.co.jp/nl/articles/2309/04/news117.html

[33] 出典：FNN プライムオンライン『「破産手続き開始」企業サイトの"改ざん被害"各地で相次ぐ』
https://www.fnn.jp/articles/-/581910

[34] 出典：X『京都府警察サイバーセンター』
https://x.com/KPP_cyber/status/1677210845170810880

[35] 出典：さくらインターネット『acmailer の脆弱性にご注意ください | さくらのサポート情報』
https://help.sakura.ad.jp/notification/n-2621/

個人情報を窃取された可能性についても、届け出ている [36]。

多くの企業がサーバーを再構築する等して公式サイトを復旧させたが、サイトのデータを全て消去された企業もあった [31]。

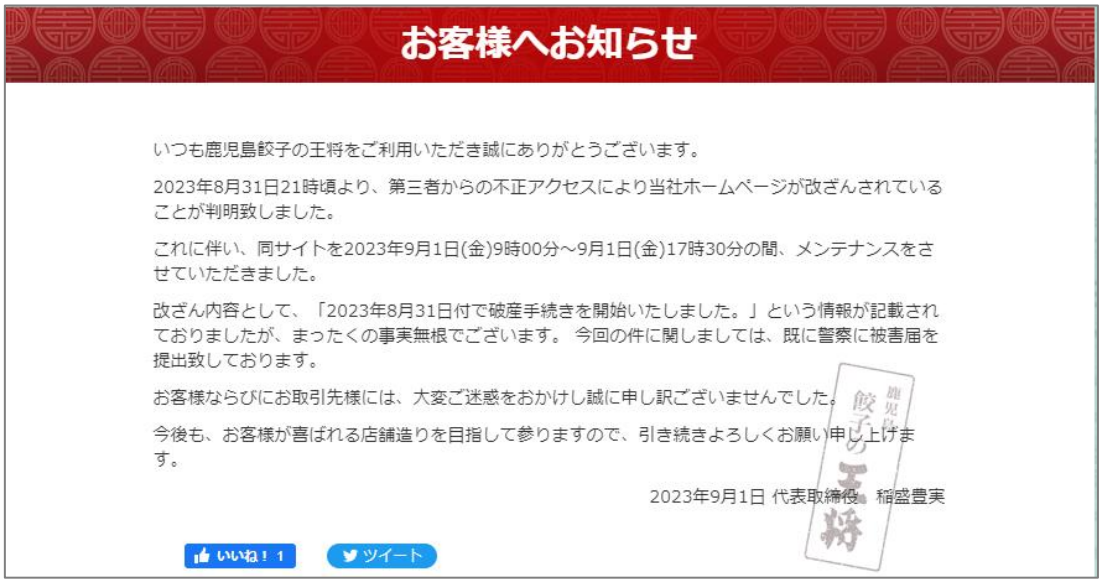

図 9 改ざん被害の発表の例（鹿児島 餃子の王将）[37]

3.3. 企業公式サイトと不正アクセス対策

本件は、攻撃対象の脈絡の無さから、公開しているサーバーに脆弱性がある等で不正アクセスが可能な企業が偶然、被害に遭ったと考えられる。公式サイトを設けている企業は Web サーバーやメール配信システムにおいて不正アクセス対策を行う必要がある。

なお、公式サイトから正常に情報発信できない事態は、改ざんだけでなく DDoS 攻撃やアクセス集中、災害等、他の事由でも起こり得る。緊急事態発生時に公式サイト以外の媒体から情報発信を継続できるようにしておくことも有効な対策である。例えば、公式の SNS アカウントを用意し、事前にアカウントの存在を一般に周知しておくことが挙げられる。

3.4. まとめ

従来、企業公式サイトのトップページに攻撃者がメッセージを書く改ざんでは、ハッキングの成果を誇るいたずら書きや政治的な主張等が主で、企業の経営に影響が出ることは稀であった。今回の事件もいたずら書きの一種と考えられているものの、企業経営に関する虚偽情報という点が従来と異なり、悪質である。もし取引先等が信じた場合、業務への支障や、株価下落等に繋がりかねなかった。

企業の経営を守るためには、インターネットに企業情報を公開するシステムのセキュリティも重要であることを再認識させる事件であったと言える。

以上

---

[36] 出典：株式会社西島畜産『ホームページ復旧のお知らせ』
https://n-meat.co.jp/archives/36088

[37] 出典：鹿児島 餃子の王将『お客様へお知らせ』
https://kagoshima-ohsho.jp/news/4916.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