人権保護や民主主義の推進に関与する組織や個人のためのガイダンス：限られたリソースでサイバー脅威を緩和

公表　2024年5月14日

要約

米国サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA)及び次の組織(今後は「執筆機関」と言う)は、主要な政府、非政府、産業界、人権保護や民主主義の推進に関与する組織やパートナーと調整して、このガイダンスを作成し、共同執筆した。執筆機関は、人権保護や民主主義の推進に関与する組織や個人など、民主主義の価値を損なうためのサイバー攻撃の被害にあう危険が高いコミュニティに対しサイバーセキュリティガイダンスを提供するために、この合同ガイダンスを公表している。

- 国土安全保障省インテリジェンス・分析室(DHS I&A)
- 連邦捜査局(FBI)
- カナダサイバーセキュリティセンター(CCCS)
- エストニア国家サイバーセキュリティセンター(NCSC-EE)
- JPCERTコーディネーションセンター(JPCERT/CC)
- 日本内閣サイバーセキュリティセンター(NISC)
- フィンランド国家サイバーセキュリティセンター(NCSC-FI)
- 日本警察庁(NPA)
- 英国国家サイバーセキュリティセンター(NCSC-UK)

「シビル・ソサエティ」とは、例えば、非営利、権利擁護、文化、信仰に基づく団体、学術界、シンクタンク、ジャーナリスト、非抑圧派、ディアスポラ組織など、人権保護や民主主義の推進に関与するコミュニティや個人を指し、これらの組織やその構成員は、民主主義の価値や利益を損なおうとする「国家」を背景とする脅威アクターの攻撃対象となるリスクが高いと考えられている。「国家」を背景とするアクターは、人権保護や民主主義の推進に関与する組織や個人を威圧し、沈黙させ、強制させ、ハラスメントを行い、危害を加えるため、その組織や個人の機器やネットワークを侵害する。こうした侵害は、定期的に、国境を越えた抑圧(国境を越えたデジタル抑圧とも呼ばれる)の一形態として行われる。

産業界の報告によると、サイバー攻撃の被害にあう危険が高いコミュニティを標的とする「国家」の背景は、主にロシア、中国、イラン、北朝鮮の「政府」からのものである。こうしたアクターは、通常、潜在的な被害者について徹底的な事前調査や、ソーシャルエンジニアリングを支える情報の収集、ログイン認証情報の取得などを行う。アクターは、組織のネットワーク、電子メール等の個人アカウント、個人機器・ネットワークを標的とし偵察や監視を行う。その際、スパイウェアアプリケーション、すなわち、標的の機器からデータを収集するマルウェアを経由することもある。

このガイダンスは、人権保護や民主主義の推進に関与する組織や個人に対し、検知した悪意のある振る舞いに基づき、「国家」を背景とするサイバーオペレーションの脅威を緩和するための提言を行う。このガイダンスは、さらに、ソフトウェア作成業者に対し、顧客のセキュリティ態勢を改善するための提言も行う。

目次

導入

産業界の報告においては、人権保護や民主主義の推進に関与する組織や個人に対するサイバー脅威が深刻かつグローバルである点が強調されており、政治やイデオロギー上の理由から攻撃を行う多様な脅威アクターに対し備えを行う必要がある。人権保護や民主主義の推進に関与する組織は、脅威レベルが高く、かつ防衛能力は低いため、リスクの高いコミュニティとみなされる。

- 人権保護や民主主義の推進に関与する組織やそのスタッフは、悪意あるサイバーアクターの標的となる脅威が高い。産業界の報告に基づくと、こうした組織とそのスタッフは、民主主義の価値を損なおうとする「国家」アクターの標的であることが知られている。
- 人権保護や民主主義の推進に関与する組織は防衛能力が低いことがある。こうした組織はITサポート部局やサイバーハイジーンが不十分で、悪意ある活動の可能性を防げないためである。例えば、ライフサイクル管理、パッチ管理、多要素認証、パスワード管理が十分でない。さらに、人権保護や民主主義の推進に関与する組織の下にある個人は通信する際に安全でない経路に依存したり、業務推進のため公開プロファイルの管理を必要とする場合がある。防御能力が低い組織は、ソーシャルエンジニアリングの試みといった平凡なサイバー脅威にも備えができず脆弱である。

こうした防衛能力の低さが悪化するのは、殆どの場合、製品やサービスがサイバー脅威を減らす負担を顧客やエンドユーザーに負わせるように設計されているためである。例えば、顧客やエンドユーザーが、サイバーセキュリティを改善するため、一定の、特に煩雑な行動をとることが求められる場合がある。

この合同ガイダンスは、CISAの「High-Risk Community Protection(HRCP)イニシアティブ*」及びNCSC-UKの「Defending Democracyキャンペーン†」の一部として作成され、人権保護や民主主義の推進に関与する組織や個人に対し、共通するサイバー脅威に基づくリスク軽減のための対策を示すものである。執筆機関としては、人権保護や民主主義の推進に関与する組織や関連する個人に対し、このガイダンスに示す対策をとるよう強く求める。また、執筆機関は、ソフトウェア作成業者に対しても、このガイダンスにある対策を講じ、悪意あるアクターによる最も共通した攻撃の種類を防ぐよう製品を設計することにより、顧客のセキュリティ結果に責任を負うことを求める。‡

---

*CISA の HRCP イニシアティブは 2023 年に開始され、サイバー攻撃を受けるリスクの高いコミュニティを特定し協力するための CISA の活動の拠点となるもの。これにより、直面する脅威を理解し、防御を強化するためのできるリソースを明確にし、支援のギャップを埋めることが可能となる。CISA の HRCP に関する情報は国土安全保障省（DHS）プレスリリース「Secretary Mayorkas Discussions New U.S. Efforts to Counter Spread of Digital Authoritarianism at Summit for Democracy」を参照願いたい。

†NCSC-UK は、サイバー防衛に対して Whole of Society アプローチを採用し、人権保護や民主主義の推進に関与する組織や個人を 3 つの重要セクターの 1 つと見ている。NCSC は、「Defending Democracy」を通じ、サイバー攻撃を受ける可能性の高い市民や議員と協力して、個人用及び企業用機器双方を標的とした高度な脅威に対する理解の促進を追求している。更なる情報は、NCSC-UK の Web ページ「Defending Democracy」を参照願いたい。

‡セキュリティと安全性を念頭に設計された製品を「セキュアバイデザイン」と呼ぶ。セキュアバイデザインの要点は、ソフトウェア作成業者がサイバーセキュリティを設計と開発に組み込むことによって、顧客のセキュリティ結果に責任を負うこと。更なる情報は、「cisa.gov/securebydesign」及び合同ガイダンス「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design and Default」を参照願いたい。

人権保護や民主主義の推進に関与する組織や個人に対するサイバー脅威

脅威テレメトリー情報の報告や脅威インテリジェンスの提供が不足し、さらに、サイバー攻撃を受けるリスクが高い組織や個人が企業と同水準の解決策を講じられないことも加わり、民間・政府組織双方にとって、こうした組織や個人が直面する脅威を正確に評価することは困難となっている。産業界の報告は、「国家」を背景とするサイバーアクターが人権保護や民主主義の推進に関与する組織や個人の一部を標的としているという一貫したパターンを示す。特に、「国家」を背景とするアクターによって、頻繁に、非政府組織(NGO)、シンクタンク、人権活動家、ジャーナリストが標的となっている。

- マイクロソフト社によると、2023年において、NGO及びシンクタンクは、「国家」を背景とするアクターの攻撃対象として情報技術セクターに次いで第二位であった。
- CrowdStrike社の報告では、2023年11月の時点で、5つの「国家」を背景とするグループがシンクタンクを標的にしていることが知られており、11グループがNGOに対する潜在的な脅威であること、2グループが被抑圧派を標的としていること、1グループが非営利団体(NPO)を標的にしていることを明らかにしている。
- Cloudflare社は、人権保護や民主主義の推進に関与する組織に対する悪意あるサイバー活動が、総じて増加していることを観測した。2023年の第2四半期において、総トラフィックの割合としてNPOのウェブサイトへの悪意のあるトラフィックを見ると、NPOは他のどの業界よりも標的となった。2023年の第3四半期において、NPO及び独立メディア組織は金属・鉱業業界に次いで第二位になり、NPOへの全トラフィックの17.14%がDDoS攻撃であった。欧州連合サイバーセキュリティ機関(ENISA)は、2022年7月から2023年6月までに、人権保護や民主主義の推進に関与する組織に所属する個人が、グローバルに標的とされたセクターの中で第二位であった。

「国家」を背景とするアクターは、民主主義の価値を損なうためのツールキットの一部として、人権保護や民主主義の推進に関与する組織や個人を標的とする。具体的には、威圧、強制、監視、ハラスメント[§]を主な手段として、オンライン上で組織や個人を標的とする。これらはデジタル越境抑圧と呼ぶ国境を越えた抑圧の一種である。

脅威アクターは、デジタル越境抑圧に先立ち、企業のウェブサイトやソーシャルメディア、地政学に関する出版物、プレスリリースなどの徹底的なオンライン調査を行い、標的とする組織や個人に関する情報を収集する。「国家」を背景とするアクターは、こうした調査の後、組織ネットワークや個人機器にアクセスを確保することが多い。こうしたアクセス確保の方法は、第一にソーシャルエンジニアリングによって被害者にアカウント認証情報を漏えいさせたり、又はマルウェアをダウンロードさせるか、第二にユーザーにマルウェアを忍ばせた一見正規のアプリをダウンロードさせるかである。脅威アクターは、機器へのアクセス確保後、スパイウェアをインストールすることもある。スパイウェアは、広範囲に及ぶ偵察能力(位置追跡、画像・音声キャプチャ、個人ファイルや通信へのアクセスを含む)を提供する商用ツールである。

人権保護や民主主義の推進に関与する組織を標的とすることが知られている「国家」を背景とするグループについての情報は「付録A:「国家」を背景とするアクター」を、また、脅威アクターがネットワークや機器にアクセスし、個人を偵察、監視できるようにするサイバー攻撃に関する技術情報については「付録B:「国家」を背景とするグループの戦術と技術」を参照願いたい。

[§] ハラスメントとは、独立したツールとして、被抑圧派を沈黙させ、コントロールし、弾圧するために「国家」によって実施されるものであり、デジタルハラスメントとは、例えば、ソーシャルメディアアカウントを動員し個人に対して行われる等、それがオンライン上で行われる場合を言う。

緩和策

組織

執筆機関は、人権保護や民主主義の推進に関与する組織に対して、CISAのサイバーセキュリティパフォーマンス目標 (CPG) によって定義されたベストプラクティスを実践するよう強く促す。これらのサイバーセキュリティ管理措置は、最も一般的かつインパクトのある脅威や行動の情報に基づく最低限のプラクティス・防護策を提供する。「国家」を背景とするアクターは偵察を行い、また、フィッシングや流出したパスワードを介し企業ネットワークへの初期アクセスを行うが、こうしたアクターの脅威を軽減するため次の措置を優先する。

CPGの主な特徴:
- サイバーセキュリティプラクティスのうち優先すべき措置
- リスク軽減のため優先すべきもの
- CISAやその政府・産業パートナーが確認した脅威に基づく情報
- 重要インフラ運用と市民双方のリスクの十分な低減を意図

1) **ユーザーの機器及びITインフラストラクチャーのソフトウェアを常にアップデートする。**ソフトウェアのアップデートは、既知の欠陥を修正する。速やかにソフトウェアのアップデートをインストールすることは、アクターがこうした欠陥を利用してシステムにアクセスすることができないことを意味する。
2) **耐フィッシング多要素認証(MFA)[CPG 2.H]を実装する。**耐フィッシングMFAを設定することにより、アクターがユーザーアカウントを侵害することが一層困難になり、同時に、正当なユーザーのサインインが一層容易になることがある。追加情報は、CISAの「Phishing-Resistant Multifactor Authentication」ガイドを参照願いたい。
3) **アカウントを監査し、未使用や不要のアカウントを無効にする。**不要なアカウントを削除し、アクターがシステムへの侵入に利用できるアクセス経路を減らす。
4) **退職するスタッフのユーザーアカウントと組織リソースへのアクセス権を無効にする**[CPG 2.D]。アカウントを無効にすることにより、システムの露出を最小にし、アクターがシステムへの侵入に利用できるオプションを無くすことができる。
5) **最小特権の原則を適用する。**アクターが侵害したアカウントを介して与える被害を減らすため、管理者アクセスといった広い、又は影響の強い許可権限を持つアカウントを監査する。管理者のユーザーアカウントを定期的な日常業務に使用することは避ける[CPG 2.E]。不正で悪意ある活動を検知するため、管理者のユーザーアカウントの使用は定期的に監視されることが望ましい。
6) **クラウドサービスプロバイダー(CSP)やマネージドサービスプロバイダー(MSP)を含むベンダーの選択時には、デューディリジェンスを実施する。**これはサプライチェーンリスクを軽減する。セキュアバイデザインプラクティスを如何に受け入れるかを明確に説明する、評判の良いベンダーのみを使用する。CISAの「Secure by Design Pledge and recommended practice」のソフトウェア作成業者の節を参照願いたい。
7) **全てのサービスプロバイダーとの契約関係をレビューし、**重要なサービスのプロバイダーをまずは優先する。契約には次の点を確実に含める。
   - 顧客の特定のニーズに合わせたセキュリティコントロール
   - プロバイダーが管理する顧客システムの適切な監視とログ記録
   - サービスプロバイダーのプレゼンス・活動や、顧客のネットワークへの接続に対する継続的に監視し、サイバーセキュリティパフォーマンス目標やセキュアバイデザイン原則の遵守を確保
   - プロバイダーのインフラ・管理ネットワークで発生した、確認された、又は疑わしいセキュリティイベントやインシデントのアップデートした受け手への通知

8) **次の手段によりアーキテクチャリスクを管理する。**
   - 顧客システム、サービスプロバイダーシステム、特にクラウド・サービス、電子メールサーバー、仮想プライベートネットワーク（VPN）サーバーなどインターネットに公開されている、その他の顧客保護領域（エンクレイヴ）間の接続の監査・検証。
   - 専用VPNを使用してMSPインフラに接続する。MSPからの全てのネットワークトラフィックはこの専用の安全な接続のみを通過する。
9) **アカウントフィッシング、電子メール・ブラウザセキュリティ及びパスワードセキュリティ[CPG 2.I]などの概念をカバーする、サイバーセキュリティの基礎研修を実施する。**研修には、「国家」を背景とするアクターが個人の電子メールや機器を標的としていることや、スタッフが次ページ以降の個人に関する提言を守り、個人電子メールアカウントやモバイル機器を侵害から保護すべきことを含める。
10) **インシデント対応・復旧計画を作成し訓練する**[CPG 2.S]。こ計画では、少なくとも組織にとって決定的に重要なシステムをカバーし、支援を求めるために誰にインシデントについて連絡や報告を行うかを確実に含める。執筆機関に報告する情報についてはこのガイダンスの「連絡先情報」の項を参照願いたい。また、インシデント対応・復旧計画の作成に関する指針については「参考資料」の項を参照願いたい。

個人

執筆機関は、人権保護や民主主義の推進に関与する個人に対し、企業ネットワーク及びモバイル機器にアクセスし偵察・監視する「国家」を背景とするアクターの影響を軽減するため、次の提言を実施することを強く促す。これらの緩和策はCISAの「Project Upskill」に沿ったものである。この「Project Upskill」は、CISAのJoint Cyber Defense Collaborative(JCDC)の「2023 High-Risk Communities Protection」計画の一部として作成されたものであり、技術専門家ではないユーザーがデジタルセキュリティを強化するのを支援する指針を纏めたものである。次の提言を実施する方法に関する詳細とガイダンスの詳細及び指針については「Project Upskill 」を参照願いたい。

- **アカウント上で強いパスワードを使用し、MFAを実装する**[Project Upskill, Module 2, Topic 2.0及びTopic 2.2]
  - デジタル・トークンやハードウェア・トークンなどの堅牢なMFAソリューションを使用して、アカウントを保護する。
- **公に入手可能な情報の公開を制限する。**
  - ソーシャルメディアやオンラインでは注意する。公開されたプラットフォームに入力する情報に気を付ける。
  - 友人や家族の間で共有されるデータを制限することを提唱し、悪用の可能性に対するセキュリティを全般的に高める。
- **連絡先を検証し、ソーシャルエンジニアリングに注意する。**個人や組織のサイバーセキュリティを高めるためには、業界や自身に関する特定の脅威や行動を理解することが重要である。自分の任務、関心、組織に関連した独特のリスク情報を考慮した、潜在的な脅威の概略を記述した参照リストを作成する。これには、業界固有のサイバー脅威、規制上の考慮、伝統的な攻撃パターンを含む。
  - ソーシャルメディア上での連絡元の身元を確認し、偽のプロファイルやソーシャルエンジニアリング戦術のリスクを軽減する。
  - ジャーナリスト等と主張する個人からのなりすましの試みに警戒し続ける。
  - 電子メール、テキストメッセージ、他の通信プラットフォームでリンクやメールの添付ファイルをクリックするときは気を付ける。

- 知らない発信元からのリンクや添付ファイルをクリックするときは気を付ける。

- **オンラインサービスに接続する際には暗号化対策を使用し全ての通信を保護する**[Project Upskill、Module 4、Topic 4.0]。暗号化は、オンラインサービスを利用する際に全ての通信を保護するために不可欠である。暗号化を行わない場合には、脅威アクターは、暗号化されていない又は認証されていないチャネルを利用して、ユーザーの機器をマルウェアに感染させる可能性があり、プライバシーとセキュリティに重大なリスクをもたらす。これらのリスクを軽減するため、ユーザーは、ユーザーの機器とWebサイトのサーバーの間でやり取りされるデータを暗号化することで盗聴や悪意のあるアクターによる改ざんから保護するHTTPSを介したWebサイトやサービスへのアクセスを優先すべきである。また、暗号化されたメッセージアプリの利用は、メッセージや通話が改ざんされず、秘密であり、許可されていない者にアクセスできないことを確実にすることで、セキュリティを一層高める。
- **アプリを慎重に選択する**。
  - 信頼できるアプリストアを使用し、悪意ある第三者アプリの潜在的脅威を回避する。
  - ダウンロード前にアプリの詳細と開発者情報を入念にチェックし、潜在的リスクを元から軽減する。
  - 第三者アプリをテストし、サイバーセキュリティ基準を満たすことを確認する[Project Upskill, Module 1, Topic 1.4]。
- **アプリの許可設定を定期的に見直し、制限し、データ公開を最小にし、セキュリティを全般的に高める**[Project Upskill, Module 1, Topic 1.3]。
- **アプリケーションとOSを常にアップデートする**[Project Upskill, Module 1, Topic 1.1]
  - 脅威アクターによる脆弱性の悪用を防止するため、迅速にアップデート版をインストールする。
  - 能動的にセキュリティを維持するため、OSとアプリケーションの自動更新を有効にする。
- **インストールされたスパイウェアを削除できるようにするため、毎週、モバイル機器の再起動を行うことを検討する**。一部のモバイル機器には、再起動をスケジュールする機能がある。この機能を使用すると、指定した時間に再起動を設定でき、スケジュールオプションは間隔を毎日から毎週まで設定可能である。
- **安全なウェブ閲覧習慣とデジタルフットプリント管理**。
  - iPhone/iPadについては、iOSのプライベートWi-Fiアドレスを有効にする。リスクの高いターゲット環境では、iOSロックダウンモードを有効にすることを検討する。iOSロックダウンモードについては、Appleサポート-ロックダウンモードについ てのWebページを参照願いたい。
  - 機密性の高い調査を行う際には、ウェブ閲覧のセキュリティを高めるため、リモートブラウザ隔離ソリューションの採用を検討する。
  - ウェブ閲覧やその他の通常のタスクでは標準のユーザーアカウントを使用する[Project Upskill, Module 1, Topic 1.0]。

ソフトウェア作成業者

執筆機関は、ソフトウェア作成業者に対し、セキュアバイデザインのプレッジを公にコミットし、積極的に実施するよう強く促す。このコミットメントには、(1)顧客のセキュリティ結果に責任を持ち、(2)徹底的な透明性と揺らぎのないアカウンタビリティを受け入れ、(3)ソフトウェアの開発と展開のあらゆる段階でセキュリティを優先するための根本的な変化を実行するため、トップから主導し、トップダウンのリーダーシップを実践する。顧客のセキュリティを改善するための緩和策には次のものが含まれる。

- **脆弱性管理。侵害の機会を減らすために、自社製品における脆弱性の種類全体を無くすことに取り組む**。悪意のあるサイバーアクターは、良く知られたソフトウェアの弱点を悪用し、マルウェアを経由してペイロードを送ることが多い。作成業者は、侵害を予防するために自らの製品の脆弱性の種類を無くす作業をすることが望ましい。
- **全ての製品でMFAをデフォルトで有効にする**。
- **顧客に対し追加料金なしでログ記録を提供し、ネットワーク上の疑わしい又は異常な振る舞いを注意喚起する**。
- **顧客に目立つ形で注意喚起を行い、安全でないコンフィグレーション、疑わしい振る舞い、マルウェアのダウンロードを認知させる**。
- **企業の財務報告にセキュアバイデザインのプログラムの内容を記載する**。

連絡先情報

米国の組織：このガイダンスにある情報に関連する不審な、又は犯罪活動を報告するため、次に連絡願いたい。

- CISAのオペレーションセンター(Report@cisa.gov又は(888)282-0870)、又はFBI現地事務所。可能な限り、インシデントに関する次の情報を含めて頂きたい。すなわち、インシデントの日時や場所、活動の種類、被害を受けた人数、活動に使用された機器の種類、情報を提出する会社や組織の名前、担当と指定された者の連絡先。

カナダの組織：CCCS(contact@cyber.gc.ca)にメールしインシデントを報告する。

エストニアの組織：cert@cert.eeにメールするか、+372 663 0299に電話しサイバーセキュリティインシデントを報告する。

フィンランドの組織：NCSC-FI(ncsc@ncsc.fi)にメールする又は、
https://www.kyberturvallisuuskeskus.fi/en/reportにインシデントを報告する。

日本の組織：このガイダンスに関連したインシデントについては、
https://www.kantei.go.jp/jp/forms/nisc_opinion.html（NISC）にアクセスするか、
info@jpcert.or.jp(JPCERT/CC)にメールを頂きたい。また、犯罪活動に関する報告は、
https://www.npa.go.jp/bureau/cyber/soudan.html(警察庁)にアクセスする。

英国の組織：重大なサイバーセキュリティインシデントを報告するため、ncsc.gov.uk/report-an-incidentにメールするか、緊急の支援が必要な場合は03000 200 973に電話する。

参考資料

CISAの「Project Upskill」を参照願いたい。これは、サイバーセキュリティ態勢を改善し、時間やリソースの観点から脅威アクターにとって攻撃のコストを上げる方法に関する詳細なガイダンスである。

市民の方々が利用できるサイバーセキュリティ研修については、CISAのCybersecurity Training & Exerciseのウェブページを参照願いたい。

インシデント対応・復旧計画に関する情報については次を参照願いたい。

- CISA：「Incident Response Basics」, 「Federal Government Cybersecurity Incident and Vulnerability Response Playbook」（このプレイブックは、米国連邦文民部門（FCEB）機関用に作成されたが、サイバーセキュリティインシデントと脆弱性対応の活動を計画・実行するための運用手続と、それらの詳細な手順を提供する。）
- NCSC-EE: サイバーセキュリティに対する気づきと防止については、以下のサイトを参照願いたい https://www.itvaatlik.ee/

もしデジタルの緊急状況になった場合には、Access Nowの「Digital Security Helpline」とAmnesty Internationalの「Security Lab」は、攻撃の標的となったと考える人権保護や民主主義の推進に関与する組織のメンバーに実践的なサポートを提供する。

スパイウェアの標的になったと考える場合には、調査の支援を求めるため、Cisco社に対しno-spyware@external.cisco.com宛にメールを送付することができる。

免責

この報告にある情報は、情報提供のみを目的として「無保証」で提供される。執筆機関は、この文書内で関係する団体、製品、サービスを含む、いかなる商用団体、製品、会社、サービスを推奨するものではない。サービスマーク、商標、製造業者などによる特定の商業団体、製品、プロセス、サービスへのいかなる言及も、執筆機関による推奨、推薦、優遇を意味したり、示唆するものではない。

謝辞

このガイドには、Atlantic Council、Authentic8、Cisco Talos、Cloudflare及びMetaが貢献した。

付録 A:「国家」を背景とするアクター

産業界の報告によると、「国家」を背景とするリスクの高い組織を標的とした攻撃は、主に、ロシア、中国、イラン、北朝鮮の「政府」によるものである**。しかしシンクタンクの研究は、他の多くの国も、被抑圧派を処罰し、沈黙させることに重点を置いて、デジタル越境抑圧の戦術を利用していることを示している。

人権保護や民主主義の推進に関与する組織を標的とすることで知られるグループには次が含まれる。

- **Velvet Chollima**:北朝鮮に関係し、サイバースパイ活動を行う。Velvet Chollimaは、朝鮮半島問題を報道するジャーナリストや、NGO・シンクタンク・学術機関の東アジア政策を専門とする研究者を主な攻撃対象としている。
    - 別名:Kimsuky, THALLIUM, Black Banshee, Emerald Street
- **Mustang Panda**:中国に関係するグループであり、重点は政治スパイ活動。このグループは、米国、欧州、台湾、香港、チベット、ミャンマー、モンゴル、ベトナム、アフガニスタン、パキスタン、インド他、様々な地域に所在するNGO、宗教機関、シンクタンク、活動家グループなどを幅広く攻撃対象にしている。主な目的は被害者の活動を綿密に監視することであり、被害者の評判を損なう周到な努力を伴う。Mustang Pandaの戦術は、標的を絞った長期にわたる政治スパイ活動の有効性を示している。
    - 別名:BRONZE PRESIDENT, TA416, RedDelta
- **Charming Kitten**:イラン政府に関係するグループであり、被抑圧派、人権組織、メディア放送局、イラン研究者を攻撃対象とし、サイバースパイ活動により情報を窃取することを専門とする。イランのサイバー脅威アクター追跡を専門とするCERTFAによると、Charming Kittenは、2014年以降、米国・欧州・中東の個人、学術関係者ジャーナリスト、活動家、シンクタンク、軍・政府部門を攻撃対象としたことが確認されている。IBM X-Forceは、Charming Kittenが2020年8月から2021年5月にかけてイランの改革派運動の中の複数の被害者の侵害に成功したことを文書化した。このキャンペーンは、2021年6月のイラン大統領選挙に向けた監視対象に一致させる形で、個人のWebメールやソーシャルメディアアカウントに入り込むことに戦略的な重点を置いている。
    - 別名:TA453, COBALT ILLUSION, Magic Hound, ITG18, Phosphorus, Newscaster, APT35, Mint Sandstorm,
- **Earth Empusa**:中国を背景とするグループであると特定され、重点は、活動家、ジャーナリスト、被抑圧派のうち、特にトルコ、カザフスタン、米国、シリア、豪州など海外在住のウイグル人を監視することである。
    - 別名:POISON CARP, Evil Eye

**産業界や政府は、様々な分析方法を使用して活動クラスターを追跡する。すなわち、グループに名前を付けることで、同じアクターのグループを起源とすると考えられる活動を特定する。また、複数の組織が独立に活動を追跡するため、複数の名前を有するグループや、重複するグループが存在する。APT(Advanced Persistent Threat)という用語は、一般に、長期にわたるネットワークやシステムへの侵入を狙った高度な活動に従事する、十分なリソースのある、「国家」を背景とするグループに対して使用される。これ以上の情報については、CISA の「国家」サイバーアクターに関する Web ページ及び attack.mitre.org/groups を参照願いたい。

- **Syrian Electronic Army(SEA)又はAPT-C-27**：人道組織、ジャーナリスト、被抑圧派、特に現政権に反対する自由シリア軍と関係する者を対象に標的を絞った攻撃を行うことに重点を置くグループである。

付録 B:「国家」を背景とするアクターの戦術と技術

執筆機関にとって、悪意あるサイバーアクターの行動を理解することは、ネットワークとデータを保護するための最初のステップであることが多い。十分なリソースを備えた組織にとって、ネットワークの防御者が悪意あるサイバー攻撃の検知や緩和に成功するか否かは、この理解にかかっている。人権保護や民主主義の推進に関与する組織は内部のネットワーク防護スタッフが不足している可能性があるが、悪意ある行動を理解することで、「国家」を背景とする活動を緩和するための基本的なサイバーセキュリティ管理に関し、十分な情報に基づくリソースに関する意思決定が可能となる。

この付録は、次のようなサイバー攻撃を概観する。すなわち、アクターが将来の標的設定を支援する情報を収集し、そして企業ネットワークやモバイル機器にアクセスし、偵察や監視を支援し、攻撃対象の使命、関心、連絡先を知ることを可能とする攻撃である。活動は、グローバルにアクセス可能な、悪意あるサイバー行動に関する知識基盤であるMITRE ATT&CKフレームワークにマッピングされる。こうしたサイバー行動は、定義された戦術と手法に分類される[††]。

- 戦術は「なぜ」、つまり、悪意あるサイバーアクターが行動する上での技術的な目的、最終目標、動機を表す。
- 技術は、敵がある行動をとることにより「どのように」戦術的な目標を達成するのかを表す。

[‡‡]MITRE ATT&CKは、3つの「技術領域」の枠組みで構成される。すなわち、アクターが攻撃するエコシステムとして、企業(エンタープライズ)、移動機器(モバイル)、産業制御システムで構成される。この付録は人権保護や民主主義の推進に関与する組織の中でも企業及びモバイルに対する戦術と技術を概観する。

企業(エンタープライズ)

戦術:偵察[TA0043]

定義:サイバーアクターは、将来の攻撃に利用できる情報を収集する。

既知の偵察技術の説明:「国家」を背景とするアクターは、情報収集のためにオープンソースの調査を利用する。多くの人権保護や民主主義の推進に関与する組織やスタッフは本質的に公的な性格を帯びるため、高いリスクに晒されることとなる。具体的には、人権保護や民主主義の推進に関与する組織や個人は、組織のウェブサイトやソーシャルメディアでの啓発、地政学的な出版物、プレスリリースを介して、オンライン上での存在感を強く示すため、「国家」を背景とするアクターはこうした情報を次のために利用する。

- 侵害後の目標の範囲と優先順位付けを行う。
- フィッシング攻撃の可能性のため、個人を含め攻撃対象を特定する。
- IPアドレスやOS等、デバイスやネットワークに関する情報を収集する。

脅威アクターはソーシャルエンジニアリングの一形態であるフィッシングも利用し、ネットワークの初期アクセスのためにログイン認証情報を窃取する。こうした例では、脅威アクターは、同僚、知人、組織など信頼できる発信元を装い、被害者がログイン認証情報を提供させようと仕向ける。例えば、攻撃アクターが管理するサイトに認証情報を入力させて、取得することもある。

「国家」を背景とするアクターは、相当の時間とリソースを費やし、フィッシングの試みのためアイデンティティーを作成するが、それは特に「スピアフィッシング」と呼ばれる、周到にカスタマイズされた試み

[††]サイバーコミュニティでは、悪意のある行動は、一般に、戦術、技術、手順(TTP)と定義される。
[‡‡]詳細について attack.mitre.org 及び共同ガイド「Best Practices for MITRE ATT&CK Mapping」を参照願いたい。

に繋がることがある。概ね電子メールを介して実行されることが多いが、攻撃アクターは、サイバー攻撃を受けるリスクの高いコミュニティのコミュニケーションの好みに応じ、テキストメッセージ、ソーシャルメディアプラットフォーム、調査や啓発に利用される様々なデジタルチャネルも利用する。

Velvet Chollimaの例：Velvet Chollimaは、標的の使命、関心、業務連絡先に関する情報を収集するため偵察を行う。Velvet Chollimaは、偵察の一環として、ユーザーを騙しGoogleログインページに似た不正なウェブページに認証情報を入力させ、被害者のログインの詳細を取得し、フォロー活動のためのアクセスを可能とする

MITRE ATT&CKマッピング：企業のためのMITRE ATT&CKフレームワークにマッピングされた既知の偵察技術については、表1を参照。

表1　MITRE ATT&CK 偵察技術

技術の名称	ID	説明
被害組織の情報収集	T1591	悪意あるアクターは、将来の攻撃に利用可能な標的組織、又は標的個人に関する情報を収集する。
公開のウェブサイト/ドメインの検索	T1593	悪意あるアクターは、将来の攻撃に利用可能な標的に関する情報を収集するためウェブサイトやドメインを検索する。
公開のウェブサイト/ドメインの検索：ソーシャルメディア	T1593.001	悪意あるアクターは、将来の攻撃に利用可能な標的に関する情報を収集するためソーシャルメディアを検索する。
被害者の身元情報の収集	T1589	悪意あるアクターは、将来の攻撃に利用可能な標的個人又は標的組織のスタッフに関する情報を収集する。身元に関する情報は、氏名や電子メールアドレスなど個人データから認証情報など機微なものまで、様々な詳細が含まれる。
被害者のホスト情報の収集	T1592	悪意あるアクターは、標的を決める時に利用できる被害者のホスト（機器、コンピューター、サーバー）から情報を収集する。ホストに関する情報には、割り当てられた IP アドレスなど管理データや、OS などコンフィグレーション仕様まで、様々な詳細が含まれる。
被害者のネットワーク情報の収集	T1590	悪意あるアクターは、標的を決める時に利用できる被害者のネットワークに関する情報を収集する。ネットワークに関する情報には、IP アドレスやドメインネームなどの管理データ、トポロジーやオペレーションに関する仕様まで、様々な詳細が含まれる。
情報のためのフィッシング	T1598	悪意あるアクターは、フィッシングメッセージを送信して、ログイン認証情報など、将来の攻撃に利用できる機密情報を引き出す。

戦術:初期アクセス [TA0001]

定義:初期アクセスは、悪意あるサイバーアクターが標的ネットワークへのアクセス獲得を試みる時である。

既知の初期アクセス技術の説明:APTアクターは、ネットワークにアクセスするため、フィッシングの試み(「偵察」の項を参照)によって取得した認証情報を利用する。

また、APTアクターは、標的への初期アクセスを得るため、マルウェアベースのフィッシングも利用する。マルウェアベースのフィッシング攻撃では、悪意あるアクターは信頼できる発信元であるふりをして、被害者に悪意あるハイパーリンクに反応させたり、電子メールの添付を開かせたりして、ホストシステム上でマルウェアを実行する。展開されたマルウェアは、データの窃取、偵察、高度なサイバー侵入を可能にする。悪意あるアクターがマルウェアのペイロードを展開するために悪用する良く知られたソフトウェア脆弱性が広がっていることから、フィッシングは容易になることもある。

例:イラン、中国、北朝鮮、ロシアに関係するAPTグループは、サイバー攻撃を受けるリスクが高い組織や個人を狙った広範な攻撃にスピアフィッシングメールを組み込んでいる。これらのグループは、カスタマイズされた、極めて説得力のあるメッセージを送付し、ユーザーにリンクや添付を実行させる。

Velvet Chollima: Velvet Chollimaは、インタビューを求めるジャーナリストや調査参加に誘う学者を装うことが確認されている。Velvet Chollimaは、当初、電子メールのやりとりを通じて信頼を確立し、通常は偽のリンクや添付を介して、その後のコミュニケーションに悪意ある要素を巧みに導入する。特に、これらのリンクにはマルウェアが隠されることが多く、Velvet Chollimaが被害者のパソコンに不正アクセスしたり、被害者の通信を監視したりすることを可能にする。

さらに、Velvet Chollimaは、被害者のメールアカウント内に自動転送ルールを確立し、アカウントへの直接のアクセスが失われた後も、通信を継続的に監視できるようにする。

Velvet Chollimaのスピアフィッシング攻撃は、価値の高い標的の通信に侵入し監視するためソーシャルエンジニアリングと悪意のあるペイロードを利用する。これは繊細で、標的を絞ったサイバー諜報戦略を体現している。

Mustang Panda: このグループが好む初期侵入の方法は、主に、遠隔アクセスのトロイの木馬(RAT)を展開するためのスピアフィッシングメールである。これにより、標的のコンピュータの遠隔管理が容易となり、ユーザーの活動を完全に監視することが可能となる。Mustang Pandaは、標的がリンクや添付をクリックするように仕向ける戦術をとり、時事問題に言及したり、正規文書や盗んだ文書から悪意のあるバージョンを仕込むこともある。例えば、2022年1月、欧州の標的に送信されたメールには、おとり文書の欧州委員会報告書の添付や人権の重点分野に関するEUプレスリリースへのリンクが含まれていた。

Mustang Pandaは、初期アクセスを得た後、長く、かつ密かに監視を行うため、高度な技術を活用する。幾つかの事例では、このグループは、長期にわたり監視しデータ窃取する能力があることが明らかとなった。これは組織のネットワーク内に検知されずに潜むことができることを示している。

Charming Kitten: Charming Kittenは、多様なオンライン通信プラットフォームを使用して、高度なソーシャルエンジニアリング攻撃を実行する。このAPTグループは、ジャーナリストやNGOのスタッフに成りすまし、信頼を得るため標的と偽の会話を行い、その後、悪意のあるファイルやリンクを展開する。IBM X-Forceは、2020年5月、Charming Kittenの40ギガバイトの研修動画を発見し、良く知られた電子メールプラットフォームからデータを流出させる手法を知る手がかりとなった。

企業のためのMITRE ATT&CKマッピング：企業のためのMITRE ATT&CKフレームワークにマッピングされた初期アクセス技術については、表2を参照。

表2：企業のための MITRE ATT&CK：初期アクセス技術

技術の名称	ID	使用
フィッシング	T1566	悪意あるアクターは、フィッシングメッセージを送信し、被害者のシステムにアクセスを得る。このメッセージにより、被害者のシステム上でコードが実行される、又は、マルウェアがダウンロードされることとなる。
フィッシング:スピアフィッシング添付	T1566.001	悪意あるアクターは、被害者のシステムにアクセスを得る試みのため、悪意ある添付のあるスピアフィッシングメールを送信する。
フィッシング:スピアフィッシングリンク	T1566.002	悪意あるアクターは、被害者のシステムにアクセスを得る試みのため、悪意あるリンクのあるスピアフィッシングメールを送信する。このリンクは、通常、受信者が URL を積極的にクリックするか、コピーすることを促すソーシャルエンジニアリング(そのためには関係する技術のユーザー実行[T1204]が必要)を介し、被害者システム上でマルウェアがダウンロードされることに繋がる。

モバイル

戦術：初期アクセス [TA0027]、発見[TA0032]、収集[TA0035]、指揮統制[TA0037]

定義：初期アクセスは、悪意あるサイバーアクターが標的のモバイル機器にアクセスを得ることを試みる時である。発見は、アクターが、攻撃をサポートするため機器について学習する時に起こる。収集は、アクターが機器からデータの収集を試みる時である。指揮統制は、アクターが侵害した機器を支配下に置くために通信を試みる時である。

既知の技術の説明:アクターは、機器へのアクセスを得るためフィッシングを利用する。その際にSMSを介することが多い。また、トロイの木馬化されたアプリケーションも利用することもある。ユーザーは、一見正規なアプリをダウンロードするが、これらにはマルウェアが仕込まれており、アクターが通話ログや位置情報を含む機微なユーザー情報にアクセスしたり、ユーザーの機器を乗っ取ることを可能にしてしまう。

アクターは機器へのアクセスを得た後、PegasusやIntellexaといったスパイウェアを機器にインストールすることがある。スパイウェアは、位置追跡、画像や音声キャプチャ、個人ファイルや通信へのアクセスといった幅広い監視機能を提供するツールである。
例：次の例は、「国家」を背景とするアクターが、トロイ木馬化したアプリやスパイウェアを攻撃でどのように使用するかを示すものである。

Earth Empusa	Meta社は、2021年、Earth EmpusaがサードパーティのAndroidアプリストアに似た偽のウェブサイトを開設したと報告した。このおとりプラットフォームは、キーボードアプリ、礼拝用アプリ、辞書アプリ等ウイグル人(中国中・東部全般地域に起源を有し、かつ文化的に関係するチュルク語族グループ)向けにカスタマイズされたアプリを配信した。 TrendMicro社の分析は、これらのアプリをダウンロードすると、ユーザーの機器がマルウェアに感染することを明らかにした。Earth Empusaによって計画・調整されたマルウェアの目的は、位置情報、通話ログ、SMSメッセージなどの幅広い機微データを収集することである。また、マルウェアは機器のカメラ、マイク、スクリーンショット機能への不正アクセスを許可し、このグループの有する高度かつ干渉的な監視技術の典型例となっている。
APT-C-27	APT-C-27は、個人のセキュリティを侵害するために、巧妙に悪意のあるアプリを作成した。その中には、Telegramなど良く知られた通信プラットフォームのおとりバージョンやシリア語のニュースアプリの他、VPN Secureというアプリがある。APT-C-27は、この一見無害なアプリを戦略的に利用しており、そのことは、標的のセキュリティやプライバシーを損なおうとするAPT-C-27の高度なアプローチを示している。 APT-C-27は、自由シリア軍の関係者や元兵士を標的にした2回目の攻撃を実施した。このグループは、ソーシャルエンジニアリングを用いて、標的個人を騙してリンクをクリックさせ、TelegramやFacebookといった良く知られたサービスを真似した偽のウェブサイトに誘導した。

モバイルのためのMITRE ATT&CKマッピング：モバイルのためのMITRE ATT&CKフレームワークにマッピングされた技術については表3から表6を参照。

表3：モバイルのための MITRE ATT&CK：初期アクセス技術

手法の名称	ID	説明
フィッシング	T1660	悪意あるアクターは、悪意あるコンテンツを送信して、被害者の機器にアクセスを得る。

表4：モバイルのための MITRE ATT&CK：発見技術

手法の名称	ID	説明
位置追跡	T1430	悪意あるアクターは、機器の実際の位置を追跡する。

表5：モバイルのための MITRE ATT&CK：収集技術

手法の名称	ID	説明
保護されたユーザーデータ：通話ログ	T1636.002	悪意あるアクターは、通話ログデータを収集する。
保護されたユーザーデータ：SMS メッセージ	T1636.004	悪意あるアクターは、SMS メッセージを収集する。
ビデオキャプチャ	T1512	悪意あるアクターは、機器のカメラを利用して、ビデオ記録を取得し情報収集する。悪意あるアクターは、ビデオファイルの代わりに一定間隔で画像を取得する場合もある。
オーディオキャプチャ	T1429	悪意あるアクターは、ユーザーの会話、周辺、通話などの音声を取得する。
スクリーンキャプチャ	T1513	悪意あるアクターは、スクリーンキャプチャを利用して、画面で実行されているアプリ、ユーザーデータ、認証情報などの標的機器に関する情報を収集する。

表6：モバイルのための MITRE ATT&CK：指揮統制技術

手法の名称	ID	使用
侵入ツールの伝達	T1544	悪意あるアクターは、外部システムからツール、ファイル、マルウェアを被害者の機器に伝達する。