サイバー攻撃の現状

2020

公安調査庁

はじめに

公安調査庁は、我が国の情報コミュニティのコアメンバーとして、国際テロや周辺国情勢、国内諸団体の動向など、我が国の公共の安全に影響を及ぼし得る国内外の諸動向について情報を収集・分析し、それらを関係機関に適時・適切に提供することで、政府の危機管理や安全保障等の重要施策の推進に貢献しています。

このたび、国内外で深刻さを増すサイバー攻撃の現状について、広く国民の皆様に知っていただくため、本冊子を作成いたしました。サイバー攻撃に関する理解の一助となりましたら幸いです。

●表紙で使用している写真について

①（写真：アフロ）
②（写真：アフロ）

サイバー攻撃

東京オリンピック・パラリンピック競技大会を直前に控える中、業務の妨害、機密情報の窃取、金銭の獲得等を狙ったサイバー攻撃が国内外で常態化しています。サイバー攻撃の手口は巧妙化しており、被害者となった組織や個人がマルウェア感染やネットワーク侵入に長期間気付かない例も存在するため、実際には、被害が表面化した攻撃だけでなく、更に多くの攻撃が実行されていると考えられます。

加えて、技術の進展によるサイバー空間の社会への拡大・浸透に伴い、サイバー空間における悪意ある主体の活動によって、社会・経済の持続的な発展や国民生活の安全・安心が脅かされる懸念は、一層高まっています。

近年の主なサイバー攻撃事案

2017年

ランサムウェアによる大規模サイバー攻撃により、世界規模で大きな混乱が生じました。

- 我が国を含む世界約150か国において、ランサムウェア「WannaCry」によるサイバー攻撃事案が発生（5月）。
- ウクライナを始めとする欧米各国で、ランサムウェア「NotPetya」によるサイバー攻撃事案が発生（6月）。

2018年

巧妙な標的型攻撃が継続的に把握されたほか、暗号資産（仮想通貨）を狙ったサイバー攻撃などが発生しました。

- 我が国の政府機関職員を装った標的型メールの大学関係者への送付（1月）。
- 我が国の政府機関職員を装った標的型メールの海洋政策関係者への送付（3月）。
- 我が国企業が運営する暗号資産交換所において、外部からの不正アクセスにより、暗号資産が外部に不正送金される事案が発生（1月及び9月）。

2019年

業務の妨害、機密情報の窃取、金銭の獲得等を狙ったサイバー攻撃が発生しました。

- 我が国の自動車販売会社の保有する顧客情報が不正アクセスを受ける事案が発生（3月）。
- 我が国企業のスマートフォン決済サービスの一部アカウントが第三者に不正アクセスされ不正利用される事案が発生（7月）。
- 我が国企業が運営する暗号資産交換所において、外部からの不正アクセスにより、暗号資産が外部に不正送金される事案が発生（7月）。

攻撃主体

サイバー攻撃の目的は様々で、攻撃に関与する主体も様々です。かつては、ハクティビスト（※）集団、金銭目的の犯罪者、愉快犯等、非国家主体によるとみられる攻撃が目立ちましたが、近年では、国家の関与が疑われる高度なサイバー攻撃も見られ、国家の安全保障に重大な影響を及ぼしかねない深刻な脅威として懸念されています。

（※）社会的・政治的主張を目的として、サイバー攻撃を行う個人・組織等

国家主体

サイバー攻撃には、国家が関与しているものもあるとみられ、米国等は、サイバー攻撃等への国家の関与を指摘・非難しています。

サイバー攻撃等への国家の関与の指摘事例

発表年月	概要
2018年9月	米国司法省が、北朝鮮による複数のサイバー攻撃に関与したとして北朝鮮籍の人物を訴追
2018年10月	米国、オランダ等6か国が、ロシア軍参謀本部情報総局（GRU）による国際機関等へのサイバー攻撃について非難する声明等を一斉に発表
2018年12月	米国司法省が、中国国家安全部と関連を有し、セキュリティ業界で「APT10」と呼ばれるサイバー攻撃グループの中国人ハッカー2人を起訴したと発表
2019年2月	米国司法省が、イランによるサイバー攻撃に関与したとして、米国空軍の元情報将校及びイランの革命防衛隊の関係者4人の起訴を発表
2019年9月	米国財務省が、「Lazarus」等として知られる、北朝鮮が国家的に主導する3グループを制裁対象に指定

米国政府による北朝鮮籍の人物の訴追発表（写真：AP/アフロ）

米国政府による「APT10」メンバーの起訴発表（写真：アフロ）

非国家主体

「アノニマス」等ハクティビストは、政治的主張の一環として、ウェブサイト改ざん、DoS（サービス拒否）攻撃だけでなく、窃取した情報を公開することもあります。

「アノニマス」支持者による抗議集会（写真：AP/アフロ）

「イラク・レバントのイスラム国」（ISIL）との関連は不明ですが、イスラム過激派の支持者とみられるハッカーによる政府機関等へのサイバー攻撃も見られます。

金銭目的の犯罪者、愉快犯等は、インターネットを悪用し、金銭の窃取、自己の能力誇示や欲求充足などのために、サイバー攻撃を実行します。

オリンピックにおけるサイバー攻撃

来年（2021年）7月から9月にかけて東京オリンピック・パラリンピック競技大会が開催されます。

近年、オリンピック・パラリンピック競技大会は、サイバー攻撃の脅威にさらされており、特に、ロンドンオリンピック競技大会（2012年7～8月、英国）以降、その脅威は顕著となっています。

ロンドン大会では、大会の運営に支障はなかったものの、電力供給システムを狙ったサイバー攻撃等が実行されました。ソチ冬季オリンピック競技大会（2014年2月、ロシア）では、大会に関連するウェブサイトがDDoS攻撃等を受けて一時的に利用できなくなるなどの被害が生じたほか、リオデジャネイロオリンピック競技大会（2016年8月、ブラジル）では、オリンピック関係機関からの情報窃取等が発生しました。さらに、平昌冬季オリンピック競技大会（2018年2月、韓国）では、開会式当日、サイバー攻撃に起因するシステムの不具合によってチケットが印刷できなくなるなど、大会の円滑な運営に不可欠なシステムが被害に遭いました。

また、サイバー攻撃による大規模停電（2015年、ウクライナ）等、重要インフラへのサイバー攻撃の脅威が現実のものとなっているところ、こうした攻撃が東京オリンピック・パラリンピック競技大会の妨害に用いられた場合、その影響は同大会にとどまらず、国民生活に深刻な影響が及びかねないことから、特に注意を要します。

過去のオリンピックにおけるサイバー攻撃事案

大会名	主な事案
ロンドンオリンピック競技大会 （2012年7～8月、英国）	・　公式サイトに対して2億件以上のサイバー攻撃が発生 ・　電力供給システムを狙ったサイバー攻撃が発生（被害なし）
ソチ冬季オリンピック競技大会 （2014年2月、ロシア）	・　組織委員会に対して約10万回のサイバー攻撃が発生
リオデジャネイロオリンピック競技大会 （2016年8月、ブラジル）	・　公式サイトに対して約2,000万件のサイバー攻撃が発生 ・　WADAのデータベースから選手の医療情報が窃取
平昌冬季オリンピック競技大会 （2018年2月、韓国）	・　開会式でサイバー攻撃に起因するネットワークの不具合が発生 ・　期間中約550万件のサイバー攻撃が発生

攻撃の目的①

情報窃取・スパイ活動

政府機関や民間企業の情報システム、個人のPCやスマートフォン等に侵入し、重要な内部情報を窃取したり、相手の動向を秘密裏に監視したりすることを目的とします。標的組織の職員等に対して、同組織の関係者、著名なウェブサービス事業者等になりすました「標的型メール」を送り付け、端末を遠隔操作するマルウェアに感染させたり、パスワード等を盗み出す偽画面に誘導したりする手口などが使われます。

日本年金機構における個人情報125万件流出事案（2015年5月発覚）

日本年金機構の職員がメールに添付されたマルウェア付きファイルを開封した結果、PC端末が外部から遠隔操作され、加入者の個人情報約125万件が外部に流出。

中国を拠点とする「APT10」によるサイバー諜報活動

米国司法省は2018年12月、中国の情報機関である国家安全部と関連を有し、セキュリティ業界で「APT10」と呼ばれるサイバー攻撃集団のメンバーである中国人ハッカー2人を起訴したと発表。2人は10年以上の間、知的財産、商業秘密及び技術情報を標的に、米国内外の数十に及ぶ企業及び政府機関のコンピュータに侵入した模様。

情報システムの破壊・機能妨害

情報システムの停止、誤作動等を引き起こすことを目的とします。DoS攻撃や、事前に感染させたマルウェア等が用いられ、ウェブサイトの書き換えや閲覧障害といった比較的軽微な被害のほか、重要インフラのまひや物理的な損傷といった深刻な被害を引き起こす可能性もあります。

ウクライナにおける大規模停電 (2015年12月)

ウクライナの電力会社がサイバー攻撃を受け、制御システムが不正に操作された結果、同国西部で数時間に及ぶ停電が発生し、約22万5,000人が影響。

韓国・平昌冬季オリンピック大会妨害事案（2018年2月)

平昌冬季オリンピックの開会式に際して、会場内でのWi-Fi接続、公式ウェブサイト、チケット発券等の機能が一時停止するシステム障害が発生。その後、同障害は、大会運営システムを破壊するマルウェア攻撃によって引き起こされたことが判明。

攻撃の目的②

不正な金銭獲得

銀行預金、暗号資産等の金銭を不正に獲得することを目的とします。銀行や暗号資産交換所等のシステムへの侵入による外部への不正送金、ランサムウェア、クリプトジャッキング（※）等の手段が用いられます。

（※）仮想通貨の「マイニング」（取引データの検証作業に必要なコンピュータの処理能力を提供して対価を得ること）を行うプログラムを他人のPC等で勝手に実行させ、第三者が不正な金銭的利益を得る行為。

ランサムウェア「WannaCry」の世界規模での感染事案 (2017年5月)

ネットワーク経由で急速に自己伝染する機能を持つランサムウェア「WannaCry」が世界中に拡散し、我が国を含む約150か国の政府機関、医療機関、企業等が感染被害。2017年12月、我が国、米国等6か国は、同事案には北朝鮮が関与したと発表。

暗号資産交換所における不正送金事案 (2018年1月)

我が国企業が運営する暗号資産交換所のシステムが、外部からの不正アクセスを受けた結果、約580億円相当（当時のレート）の暗号資産が不正に送金。

心理戦・影響力工作

情報の意図的な利用等により、人々の認知、意思決定、行動等に影響を及ぼすことを目的とします。欧米諸国等では特に、外国政府がハッキングで窃取した情報や偽情報をインターネット上で流布するなどして、世論形成や選挙に干渉することで、民主主義の基盤が脅かされる事態への懸念が強まっています。

2016年米国大統領選挙へのロシアの干渉

米国政府の発表によると、ロシアは、2016年米国大統領選挙に影響を与える取組として、①ロシア軍当局者が民主党及びクリントン候補陣営のメール等をハッキングにより窃取し、ネット上で公開・拡散する活動、②ロシア政府に近い企業が偽情報の流布やソーシャルメディア上での工作を行う活動を展開。

手法と対策①

攻撃の手法は、攻撃の対象や目的によって異なり、日々進化・高度化しています。最新の脅威や攻撃の手口をよく知り、対策を取ることが重要です。

標的型攻撃

手法

特定の組織・個人に狙いを定め、悪意のある添付ファイル・URLを送り付けて当該組織等で使用されている端末等をマルウェアに感染させるなどして、遠隔操作や情報窃取等を行います。

例：日本年金機構における個人情報流出事案（2015年）は、同機構に対し、100通以上もの標的型メールが送信され、「Emdivi」（エムディヴィ）と呼ばれるマルウェアが一部の端末に感染したことによって引き起こされたものとされます。

対策

不審なメールの添付ファイルを開封しない、リンクをクリックしないなどして攻撃を防ぐことが重要です。また、標的型メールは、不信感を抱かれないよう、普段からやり取りしている組織・人物を装うなど、標的ごとに巧妙に作り込まれている例も確認されていることから、マルウェアの感染等を想定し、ログを日常的に取得して異常な通信の早期発見に備えるなど、被害を最小限に抑えるための対策を行うことも重要です。

DDoS攻撃

手法

複数のコンピュータから、標的のサービスに悪意を持って大量の処理要求を送り付けるなどして、サービス提供を妨害したり停止させたりします。

例：DNSサーバを管理する米国Dyn社のDNSインフラストラクチャーが、DDoS攻撃を受け、同社顧客のウェブサイトがアクセスできない状態となりました（2016年）。この攻撃では、「Mirai」と呼ばれるマルウェアに感染した多数のIoT機器が利用されたと指摘されています。

対策

インターネット向けサービスでは、DDoS攻撃の影響を完全に排除することは困難ですが、オーバースペックなサーバや回線を備えたり、攻撃を行うおそれのある国やドメインからの通信を拒否したりすることで攻撃の影響を緩和することができます。また、攻撃者にDoS攻撃ツールを仕込まれ、気付かずにDDoS攻撃に加担してしまうことがないよう、コンピュータの脆弱性を修正しておくなど注意が必要です。

手法と対策②

ランサムウェア攻撃

手法

コンピュータをランサムウェアに感染させてその内部のファイルを暗号化・利用不能にした上で、被害者に対し、元に戻す見返りに「身代金」を要求します。

例：ランサムウェア「WannaCry」によるサイバー攻撃（2017年）では、ランサムウェアに感染した端末のデータを回復する条件として犯人側は金銭を要求していましたが、米国政府の発表（同年5月）によると、支払によってデータが回復した例は把握していないとのことでした。

対策

OSやソフトウェアをアップデートせずに古いまま放置していると、セキュリティ上の問題点が修正されず、それを悪用したマルウェアに感染してしまうおそれがあります。OSやソフトウェアは、最新版を使用したり、修正プログラムを適用したりすることが、ランサムウェアの感染の防止に有効です。また、感染してしまった場合にいち早く復旧させるためには、定期的にシステムやデータのバックアップを行っておくことが不可欠です。

不正ログイン

手法

IDやパスワードを解明し、相手の機器を乗っ取るため、ウェブサービスなどから流出したパスワードのリストなどを使う「リスト型攻撃」、文字の組み合わせを全て試す「総当たり攻撃」、パスワードによく使われる文字列を試す「辞書攻撃」などの手法が使われます。

対策

パスワードの安全性を高めるため、複雑なパスワードを設定し、複数のウェブサービスでパスワードの使い回しをしないほか、パスワードを適切に管理することが重要です。また、サービスへのログインの安全性を高めるためには、複数の要素を使って認証する二段階認証や多要素認証が効果的です。

公安調査庁とサイバー関連調査

政府機関としての公安調査庁の役割

公安調査庁は、破壊的団体の調査を行い、規制の必要があると認められる場合には、公安審査委員会に対し、その団体の活動制限や解散指定の請求を行います。

公安調査庁は、我が国の情報関係機関によって構成される情報コミュニティのコアメンバーとして、官邸や内閣官房を始めとする関係機関に対し、政府の施策決定に資する情報を日々提供しています。

団体規制

- 暴力主義的破壊活動を行う危険性のある団体を調査
- 公安審査委員会に対し、活動の制限や解散指定を請求
- 観察処分に付された団体に対する規制措置を実施

情報貢献

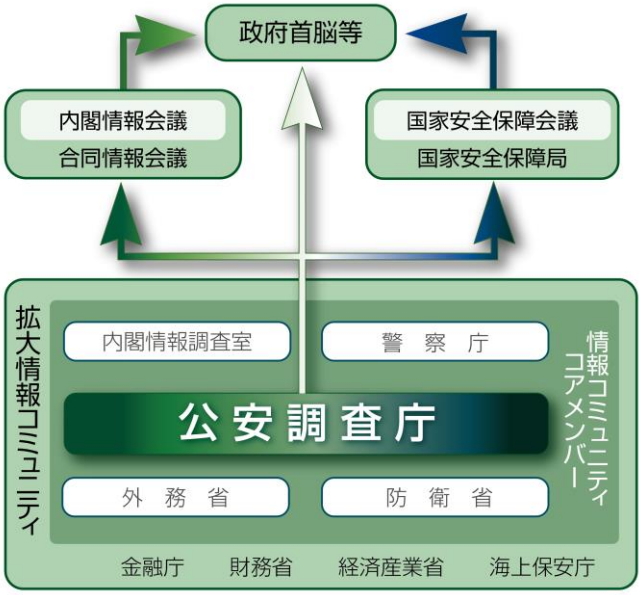
- 我が国の情報コミュニティのコアメンバー
- 関係機関に対し、政府の施策決定に資する情報を提供

サイバー関連調査の推進

公安調査庁は、サイバー空間の状況についても、情報の収集と分析を行った上、関係機関への適時適切な情報提供を行っています。

【参考】

我が国政府の「サイバーセキュリティ戦略」（2018年7月閣議決定）に基づく最新の年次計画「サイバーセキュリティ2019」では、公安調査庁の役割として、「サイバー関連調査の推進に向け、人的情報収集・分析体制の強化及び関係機関への適時適切な情報提供等、サイバーインテリジェンス対策に資する取組を実施する」などとされています。



公安調査庁からの情報発信・公表資料

公安調査庁WEBサイト

お知らせしたい情報はこちらで発信しております。
是非ご覧ください。

http://www.moj.go.jp/psia/

公安調査庁ソーシャルメディア公式アカウント

以下のソーシャルメディアにおいて、施策や取組、お知らせしたい情報等について、写真や動画等を活用しつつ情報発信を行っています。

Twitter

「公安調査庁@MOJ_PSIA」

YouTube

「PSIAchannel」

国際テロリズム要覧

世界のテロリズムの動きについて取りまとめた「国際テロリズム要覧」を公表しています。
公安調査庁WEBサイト上において、「国際テロリズム要覧」WEB版を公開しています。

内外情勢の回顧と展望

毎年、国内外の情勢についてまとめた「内外情勢の回顧と展望」を公表しています。
公安調査庁WEBサイトでもご覧いただけます。

情報の力で、国民を守る

PSIA 公安調査庁
PUBLIC SECURITY INTELLIGENCE AGENCY