ふくしまPITネットワーク
令和６年
第 11 号

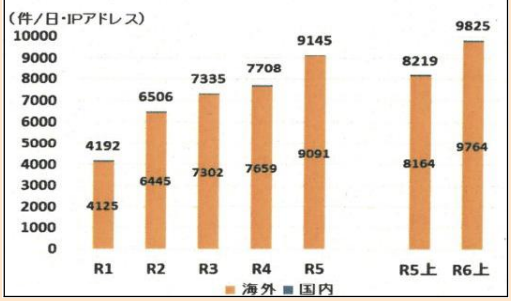
ふくしま技術情報不正流出防止ネットワーク
Fukushima Prevention Network for Illegal Leakage of Technological Information

サイバー空間をめぐる脅威

◆　近年、世界各地で重要インフラの機能停止や機密情報の窃取を企図したサイバー攻撃が相次いで発生しており、日本でも被害が発生しています。

◆　サイバー攻撃の前兆ともなるぜい弱性探索行為等の不審なアクセス件数は、増加の一途をたどっており、その大部分が海外を送信元とするアクセスとなっています。（右図）

【ぜい弱性探索行為等の不審なアクセス件数の推移】



ぜい弱性とは？

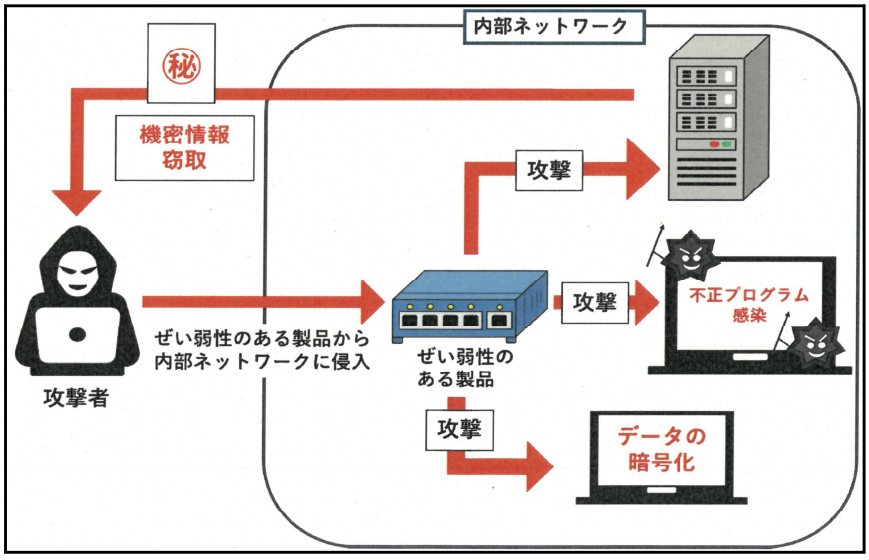
「ぜい弱性」とは、コンピュータのＯＳやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因で発生するサイバーセキュリティ上の欠陥のことです。

ぜい弱性は、セキュリティホールとも呼ばれ、ぜい弱性が残された状態でコンピュータを利用していると、不正にアクセスされたり、ウィルスに感染する危険性があります。

（総務省「国民のためのサイバーセキュリティサイト」より抜粋）

悪用の危険性

攻撃者は、ぜい弱性があるネットワーク機器を攻撃の足掛かりとして、内部ネットワークに侵入し、不正プログラムへの感染や機密情報の窃取、ランサムウェアによるデータの暗号化等の攻撃を行います。その結果、攻撃を受けた事業者は、被害拡大を防止するためにシステムの運用を停止せざるを得なくなる場合や、業務に必要なファイルが暗号化されることによって業務継続に影響が及ぶ場合があります。



左図で、ぜい弱性を放置することの危険性を確認してください。

対策について

◎　自組織で使用している機器のぜい弱性を放置することなく、各製品の販売業者が公表している助言等を基にファームウェア(※1)のアップデート、侵害の有無の確認等の対策を確実に実施してください。
　平素からぜい弱性情報やアップデートに関する情報を確認し、対処することが必要です。
◎　管理外のネットワーク機器が存在しないか確認することも必要です。
◎　システム保守を外部委託している場合は、ぜい弱性の対処が保守契約に含まれているかを確認し、対処が適切に実施されていることを確認することも重要です。

（※1）ハードウェアを動かすためのソフトウェアのこと。

悪用の危険性の高い重大なぜい弱性の例

○　悪用されるとネットワーク機器に侵入されるおそれのある重大なぜい弱性に関する情報が令和６年上半期、複数公表（下記に例示のとおり）されており、国内又は海外でこれらのぜい弱性を悪用する攻撃が発生したことが公表されています。
○　該当製品を使用している場合、サイバー攻撃の被害を防止するため確実な対処が必要になります。

● **Ivanti社：VPN製品及びネットワークアクセス制御製品**
　令和６年１月、Ivanti社は、同社のVPN製品であるIvanti Connect Secure 及びネットワークアクセス制御製品であるIvanti Policy Secure ゲートウェイについてそれらのぜい弱性(CVE-2023-46805 及び CVE-2024-21887)に関する情報を公開
※　https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

● **Fortinet社：次世代ファイアウォール製品及びWebプロキシ製品**
　令和６年２月、Fortinet社は、同社の次世代ファイアウォール製品に搭載されている FortiＯＳ及びWebプロキシ製品である FortiProxy におけるぜい弱性(CVE-2024-21762)に関する情報を公開
※　https://www.fortiguard.com/psirt/FG-IR-24-015

● **Palo Alto Networks社：次世代ファイアウォール製品**
　令和６年４月、Palo Alto Networks社は、同社の次世代ファイアウォール製品に搭載されている PAN-ＯＳ ソフトウェアにおけるぜい弱性(CVE-2024-3400)に関する情報を公開
※　https://security.paloaltonetworks.com/CVE-2024-3400

● **Check Point Software Technologies社：次世代ファイアウォール製品**
　令和６年５月、Check Point Software Technologies社は、同社の次世代ファイアウォール製品のVPN機能におけるぜい弱性(CVE-2024-24919)に関する情報を公開
※　https://support.checkpoint.com/results/sk/sk182336

（警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」より引用）

ふくしまPITネットワーク

令和６年
第 12 号

ふくしま技術情報不正流出防止ネットワーク
Fukushima Prevention Network for Illegal Leakage of Technological Information

技術流出の防止に向けて

令和６年中も、「ふくしまPITネットワーク」を毎月発出し、大切な技術情報を守るために役立つ情報をお届けしてきました。
本号では、「ふくしまPITネットワーク」と同じく技術情報等の流出防止に向けた警察の取組の一つである「アウトリーチ活動」について紹介します。

警察の取組（アウトリーチ活動）

○　警察では、技術情報等を扱う企業等に対し、警察が捜査を通じて把握した技術情報等の獲得に向けた
- ◆　外国からの働きかけの手口に関する情報
- ◆　その対策に資する情報

を提供する「アウトリーチ活動」を強化し、企業等の対策を支援しています。

※　アウトリーチ活動は、外事課及び県内各警察署の警察官が、対象となる企業等を直接訪問する形で行っています。
皆様のご理解とご協力をお願いいたします。

○　技術情報等の流出防止対策を呼びかけるためのパンフレットや動画を公開しています。
パンフレット「技術流出の防止に向けて」では、技術流出がどのようにして起きるのか、事例を交えて説明し、流出を防ぐために、

「企業やアカデミアに守ってほしい３つのＳ」
- ◇　Ｓｅｅ　（相手・書類をよく見る）
- ◇　Ｓｔｏｐ　（立ち止まってリスクを把握する）
- ◇　Ｓｈａｒｅ（共有する・相談する）

を始めとする対策等を紹介するとともに、

「技術流出のリスクパターン」
- ◇　サイバー攻撃による技術流出
- ◇　スパイ工作による技術流出
- ◇　経済・学術活動を通じた技術流出

等について紹介しています。
動画については、福島県警察本部や警察庁のホームページのほか、下の「ＱＲコード」から閲覧できますので、是非、社内会議や社員教養にご活用ください。

パンフレット

「技術流出の防止に向けて」

「技術流出の防止」

「リスク＆ケーススタディ編」

「対策編」

ふくしまPITネットワーク
令和７年
第　１　号

ふくしま技術情報不正流出防止ネットワーク
Fukushima　Prevention Network for　Illegal Leakage of　Technological Information

サイバー攻撃に注意

警察庁及び内閣サイバーセキュリティセンターは、
「ＭｉｒｒｏｒＦａｃｅ」（ミラーフェイス、別名：Ｅａｒｔｈ Ｋａｓｈａ（アース カシャ））と呼ばれるサイバー攻撃グループ
によって、日本国内の組織、事業者、個人に対するサイバー攻撃キャンペーンが実行されたとして、注意喚起を発出しています（本年１月８日付け）。

また、この攻撃キャンペーンについては、**「主に我が国の安全保障や先端技術に係る情報窃取を目的とした、中国の関与が疑われる組織的なサイバー攻撃活動である」**と評価されています。
その注意喚起の中から、概要や検知策・緩和策の一部を抜粋して紹介しますので、被害に遭わないよう適切なセキュリティ対策を講じましょう。

概要・手口等

2019年から2023年にかけて、主に日本のシンクタンク、政府（退職者を含む）、政治家、マスコミに関係する個人・組織に対し、マルウェアを添付したメールを送信してマルウェアに感染させ、情報窃取を試みるサイバー攻撃が確認されました。

＜具体的手口例＞

◆　送信元アドレス
- ✓　フリーメールアドレスの使用
- ✓　第三者の正規アドレスの悪用（認証情報を窃取しなりすまして送付）

◆　送信者名
- ✓　受信者が所属する（していた）組織の元幹部
- ✓　受信者が関心のある専門分野の有識者を詐称

◆　件名
- ✓　安全保障情勢や国際情勢に関連したもの（「日米同盟」や「台湾海峡」等のキーワードが含まれるものなど）
- ✓　「勉強会案内」「会合資料」といった受信者の関心を引くもの
- ✓　受信者と交流のある人物を詐称して「●●●●です」といったもの

◆　メール開披への誘導等
- ・　最初はファイルを添付せず、メールのやりとりの中でファイルを添付
- ・　セミナー等の申込不備を指摘して、添付ファイルを開くように誘導

2023年頃から、インターネットに接続されたネットワーク機器に対し、ソフトウェアのぜい弱性を悪用して標的ネットワーク内に侵入するサイバー攻撃が確認されました。主な標的は、日本の半導体、製造、情報通信、学術、航空宇宙の各分野です。

◆　ぜい弱性の悪用等
- ✓　ＶＰＮ機器（クラウド向け仮想アプライアンスを含む）のぜい弱性の悪用
- ✓　何らかの手段で得た認証情報（クライアント証明書を含む）の悪用
- ✓　外部公開サーバのSQLインジェクションのぜい弱性の悪用　　など

（次頁へ）

2024年６月頃から、主に日本の学術、シンクタンク、政治家、マスコミに関係する個人・組織に対し、マルウェアをダウンロードするリンクを記載したメールを送信してマルウェアに感染させ、情報窃取を試みるサイバー攻撃が確認されました。

＜具体的手口例＞

◆　マルウェアに感染させる手口
- ✓　ダウンロードしたZipファイルを展開後、Microsoft Office文書を開いてマクロを有効化することで感染
- ✓　Microsoft Office文書に偽装されたリンクファイル（拡張子がlnk）を開くことで感染

◆　送信元アドレス
- ✓　フリーメールアドレスの使用
- ✓　第三者の正規アドレスの悪用（認証情報を窃取しなりすまして送付）

◆　送信者名
- ✓　マスコミ関係者や受信者が関心のある専門分野の有識者を詐称
- ✓　悪用した正規アドレスの使用者名

◆　件名
- ✓　「取材のご依頼」「所蔵資料のおすすめ」「国際情勢と日本外交」といったキーワードを含むもの

◆　本文
- ・　送信者が過去に第三者とやりとりしていたメールを何らかの手段で窃取し、一部だけ改変しているとみられるため、違和感がない。

検知・緩和策

◎　普段からの交流相手でもメールアドレスに注意

普段と少しでも異なる状況や違和感があれば、添付ファイルを開いたり、リンクをクリックしたりせず、送信者に確認してください。

（例）
- ・　普段はファイルをそのまま添付するのが多いのに、パスワード付きZipファイルが届いた
- ・　拡張子が「VHD」や「ISO」といった日頃見かけない形式のファイルが届いた

◎　安易に「コンテンツの有効化」をクリックしない
- ・　ファイルを開いた際に、ファイルのマクロ「コンテンツを有効化」ボタンをクリックさせるよう誘導される場合がありますが、安易にクリックしないでください。
- ・　マクロとは、自動的に様々な処理を行うことが可能な便利な機能ですが、受信したファイル内容（論文、申込書、案内など）の表示・閲覧にマクロのような高度な機能が真に必要か検討し、不審に感じたらファイル提供元に確認してください。

このような受信者向けの対策のほか、システム管理者向けの対策等も紹介されています。詳しくは、
「MirrorFaceによるサイバー攻撃について（注意喚起）」をご確認ください。

（出典：「MirrorFaceによるサイバー攻撃について」R7.1.8付 警察庁・内閣ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰ連名）