SEA/Jテキストで解説するセキュリティ知識は実社会でどう役立つのか？

～ソフトウェアの脆弱性における脅威を事例から学ぶ～

日本ネットワークセキュリティ協会 (JNSA)

概要・自己紹介

はじめに

①講演タイトル

SEA/Jテキストで解説するセキュリティ知識は実社会でどう役立つのか？
～ソフトウェアの脆弱性における脅威を事例から学ぶ～

・ソフトウェアの脆弱性における脅威
　～Living off the Land攻撃について～
・ソフトウェアの脆弱性における脅威事例
　～Living off the Land攻撃のリスク～
・ソフトウェアの脆弱性を知る
　～CVEを読み解く～

---

②講演概要

この講演では、8章（ソフトウェア脆弱性）にて解説する知識について、「近年におけるソフトウェアの脆弱性と対応しなかった時のリスク」を解説します。
実際の被害事例や不十分な対策事例を知ることで、SEA/J改訂版テキストの内容をより深く理解いただき、より実社会に即した知識定着を図ります。

③講演者情報

日立ソリューションズ・クリエイト（和田明利）

自己紹介

和田 明利

株式会社 日立ソリューションズ・クリエイト
デジタルトランスフォーメーション事業部
セキュリティビジネス本部
主管技師長(本部長)

経歴

・20年間、金融関連のシステムエンジニア、PMに従事
アクセス履歴管理システム、　内部統制システム、
PCIDSSシステム、統合運用基盤システム　他

・15年間、セキュリティサービス事業立上げ、運営に従事
サイバーセキュリティトレーニング(人材育成)
サイバーセキュリティコンサルティング　他

現在

・セキュリティサービス事業に従事
(新規事業計画、セキュリティコンサルティング案件など)

・日立サイバーセキュリティセンター創設(センター長)

・セキュリティ講師の育成、日立CTF支援

・NPO日本ネットワークセキュリティ協会(JNSA)
情報セキュリティ教育実証WG(岡山理科大学講師他)

・サイバー安全保障人材基盤協会(CSTIA)
WG1リーダー(防衛省・自衛隊・サイバー学校支援)

・国立研究開発法人情報通信研究機構(NICT)
サイバーセキュリティ研究所(CYNEX) Co-Nexus C

ソフトウェアの脆弱性における脅威
～Living off the Land攻撃について～

Living off the Land攻撃について

「Living off the Land攻撃」とは？
河野前デジタル相が危険性を指摘

河野大臣記者会見（令和6年8月27日）　4’48″ ～7’12″

引用元：デジタル庁「河野大臣記者会見（令和6年8月27日）」
https://www.digital.go.jp/speech/minister-240827-01

Living off the Land攻撃について

「Living off the Land攻撃」とは？
河野前デジタル相が危険性を指摘（2024.8.27）

河野デジタル大臣記者会見要旨

システム内寄生戦術、Living Off The Landといわれているものに対する技術的な対策文書がオーストラリア政府から発出され、この文書に各国で共同署名、公表を行いました。

システム内寄生戦術への技術的対策に関する文書を22日（木）に公表しております。この**システム内寄生戦術という、検知するのが困難なサイバー攻撃手法が、今国際的に広がりつつあります**。この手法は、システムに侵入した後に、マルウェアを使う従来の攻撃とは異なって、システム内にある正規の管理ツールや機能を使って活動を行うため、検知することが難しいという特徴があります。

このシステム内寄生戦術への対策としては、システムのログを確認することが重要で、この技術的対策に関する文書を22日に公表しました。これはオーストラリア政府が作成し、我が国のNISCを含む9か国の機関が共同署名し公表したもので、仮訳も公開しています。

中規模から大規模な組織を対象としたもので、ITに関する経営幹部のほかネットワーク事業者あるいは重要インフラ事業者の方々に向けて作成したものであります。関係の皆様には是非確認をお願いしたいと思っております。

検知が困難とされるシステム内寄生戦術への技術的な対策について、国際的に文書を発出することは、我が国のサイバーセキュリティの強化、及びサイバーセキュリティ分野での国際連携の強化にもつながるものでありますので、引き続きこうした取組を進めていきたいと思っております。

引用元：デジタル庁「河野大臣記者会見（令和6年8月27日）」
https://www.digital.go.jp/speech/minister-240827-01

Living off the Land攻撃について

「Living off the Land攻撃」は、なぜ 検知が困難 なのか？

Living off the Land :「その土地に生きる」という意味

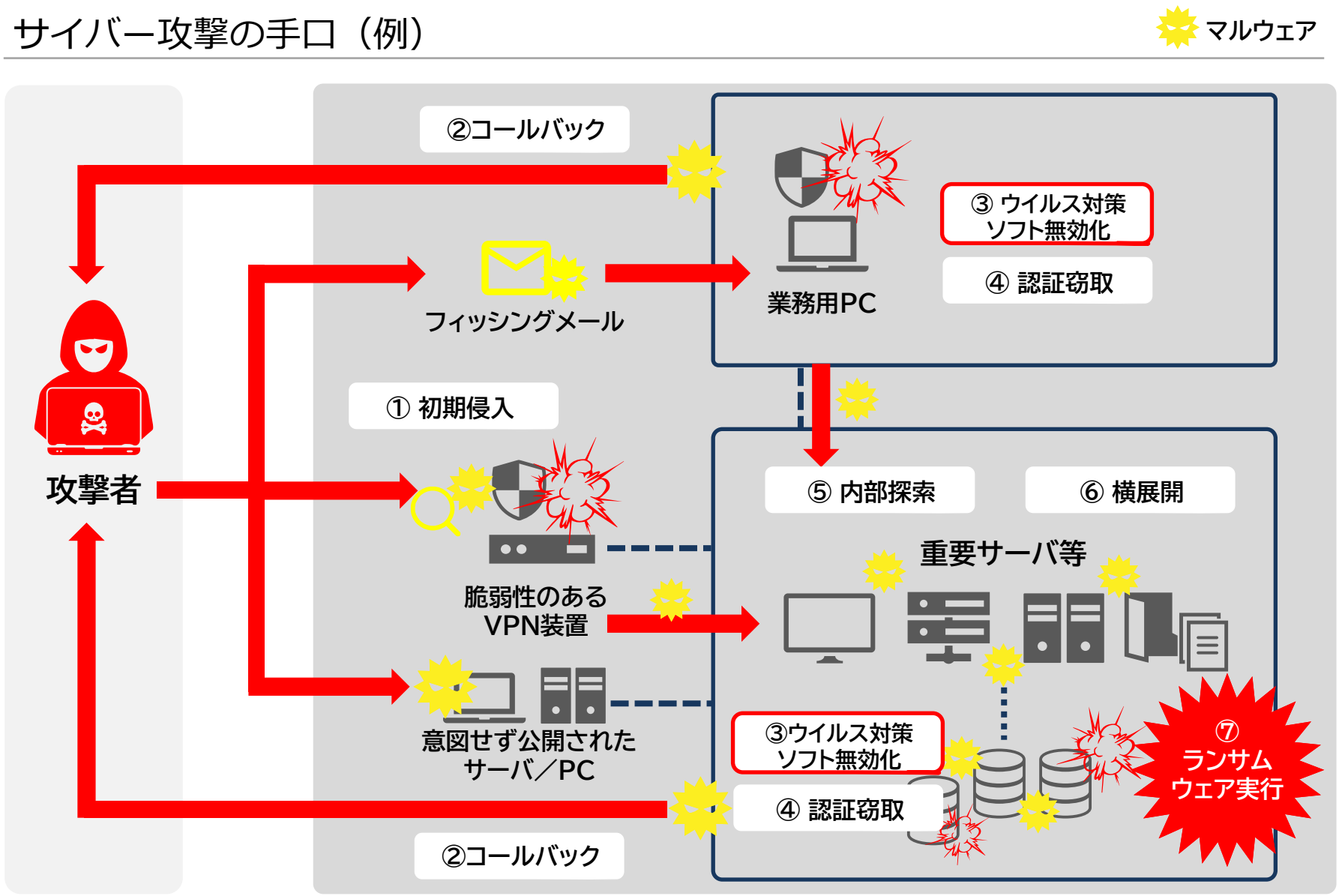
Living Off The Landの攻撃（以下、LotL攻撃と略す）とは、**対策側の監視や調査を回避することを目的**とし、持ち込んだ正規ツールの悪用や被害者の環境にあるシステムを悪用する、**痕跡を残さない手法を用いる攻撃手法**です。

従来のマルウェア攻撃とは異なり、LotL攻撃では、**外部から不正なプログラムファイルを持ち込みません**。代わりに、標的のシステム内にすでに存在する正規のツール※や機能を巧妙に悪用します。侵入後も、痕跡を巧みに隠蔽しながら潜伏し、機密情報の窃取や次の攻撃に向けたバックドア（システムに不正侵入するための裏口）の作成などの不正行為を働き続けます。

※正規ツールとは、Windows OSであればcmd.exeやcertutil.exeといったマイクロソフトによって署名されている正規のファイルのことです。

Living off the Land攻撃について

サイバー攻撃の手口（例）



Living off the Land攻撃について

Living off the Landの攻撃に良く悪用されるツールの例（トレンドマイクロによる調査）

ツール（開発元）	正規の想定用途	LotLでの主な悪用方法
Cobalt Strike（Fortra）	ペネトレーションツール（脅威エミュレーション）	横展開（ラテラルムーブメント）、バックドア、遠隔操作ツール（RAT）としての多数の機能
AnyDesk（AnyDesk Software）	遠隔でのデスクトップ操作	ネットワーク上のPCの遠隔操作など
PsExec（Microsoft）	遠隔でのプロセス実行	任意のコマンドシェルの実行、横展開
Mimikatz（オープンソース）	PoCツール（脆弱性の実証）	認証情報の窃取
Process Hacker（オープンソース）	システムリソースの監視、ソフトウェアのデバッグ、不正プログラムの検出	セキュリティ製品などの正規プロセス／サービスの探索と停止
AdFind（オープンソース）	Active Directory（AD）検索	AD探索、横展開時の情報収集
MegaSync（Mega Limited）	クラウドストレージとの同期	窃取データの外部送出
Rclone（オープンソース）	クラウドストレージとの同期	窃取データの外部送出

サイバー攻撃で悪用されやすいWindows標準コマンドの例（トレンドマイクロによる調査）

コマンドに使用されるプログラム名	正規の想定用途	LotLでの主な悪用方法
powershell.exe	Windows PowerShellの実行	Base64の文字列からコマンド複合など
rundll32.exe	DLL内の関数の実行	外部Webサーバからjavascriptを取得
reg.exe	Windowsレジストリの操作	レジストリからクレデンシャル取得
mshta.exe	HTMLアプリケーションの実行	外部Webサーバからスクリプト取得
findstr.exe	ファイル内の文字列を検索	端末の定義ファイル内パスワード取得
certutil.exe	証明書のインストールなどセキュリティ証明書の管理	外部サーバからファイルを取得

引用元：トレンドマイクロ「Living Off The Land(LotL:環境寄生型)のサイバー攻撃～正規ログの中に埋没する侵入者をあぶりだすには？」
https://www.trendmicro.com/ja_jp/jp-security/23/h/securitytrend-20230825-01.html

ソフトウェアの脆弱性における脅威事例
～Living off the Land攻撃のリスク～

Living off the Land攻撃の事例①

中国のハッキンググループ『Volt Typhoon』、米国小規模電力会社を攻撃

マサチューセッツ州の小さな公的電力供給会社が、中国のハッキンググループ「Volt Typhoon」によってネットワークが侵害された。

2025年3月12日、ICS／OTセキュリティ企業のDragos社は中国の脅威アクターVolt Typhoonが米国の電力網に侵入した事例を報告するケーススタディによると、標的にされたのは小規模公営企業Littleton Electric Light and Water Departments（LELWD）で、同社への侵害は2023年11月下旬に判明した。さらに調査を行った結果、2023年2月から300日以上にわたって「Volt Typhoon」の侵入を許し、OTシステムからデータを盗まれていたことが確認されたという。

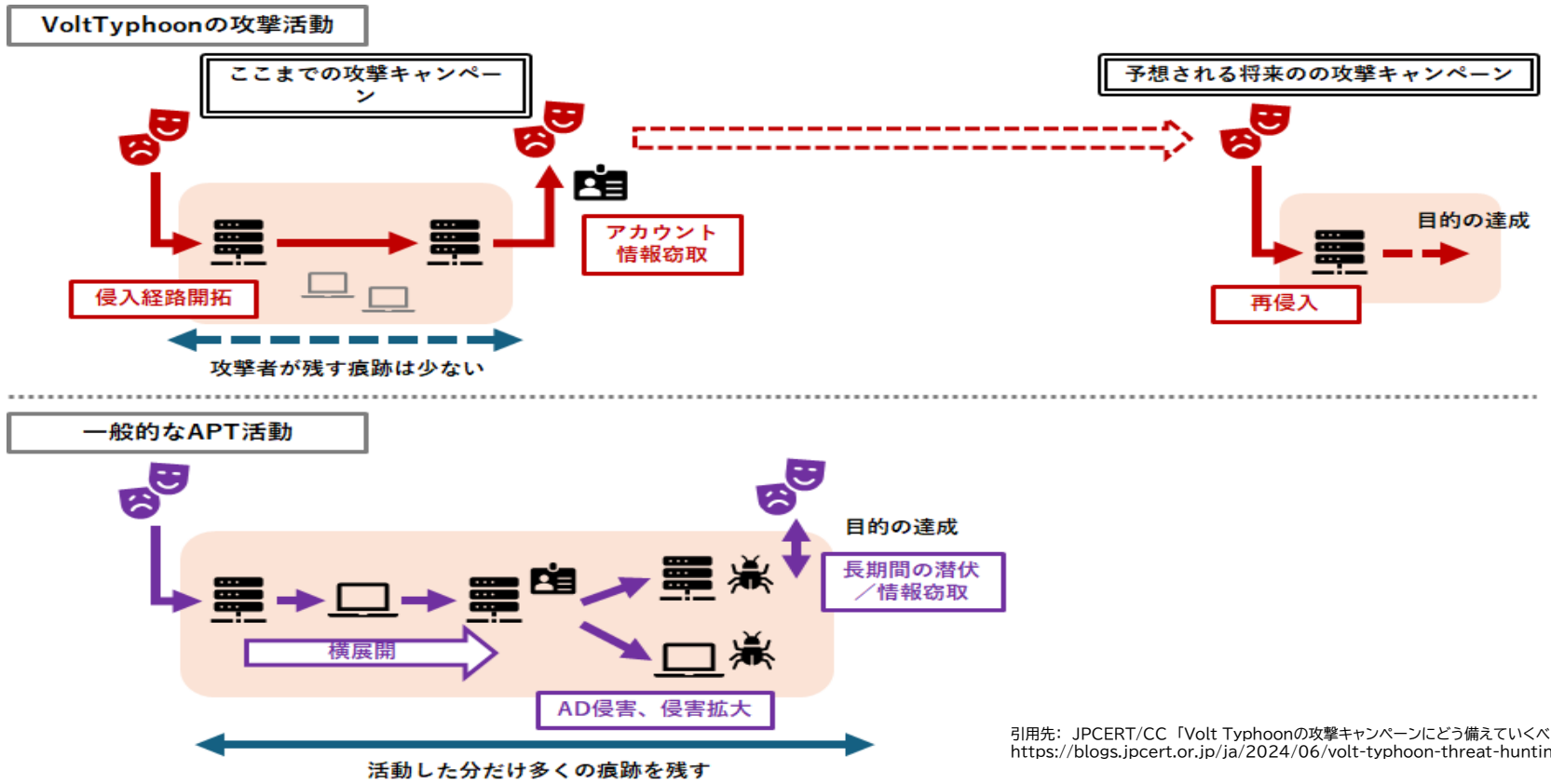
「Volt Typhoon」は、システム内寄生戦術（Living off the Land（LotL）攻撃）を使用することでステルス性が高まり、サプライチェーンをほとんど目に見えない形で操っているのです。
スパイ活動そのものが目的ではなく、アクセスそのものが目的で、そのアクセスはブルートフォース※ではなく、サプライチェーンの間隙を縫って行われています。

※ブルートフォース攻撃とは、パスワードなどの認証情報を突破するために、考えられるすべての組み合わせを試す攻撃手法のことです。総当たり攻撃とも呼ばれ、力任せに試行を繰り返すことから、ブルートフォース（Brute Force）という名前が付けられています。

Living off the Land攻撃の事例①

『Volt Typhoon』の攻撃手口

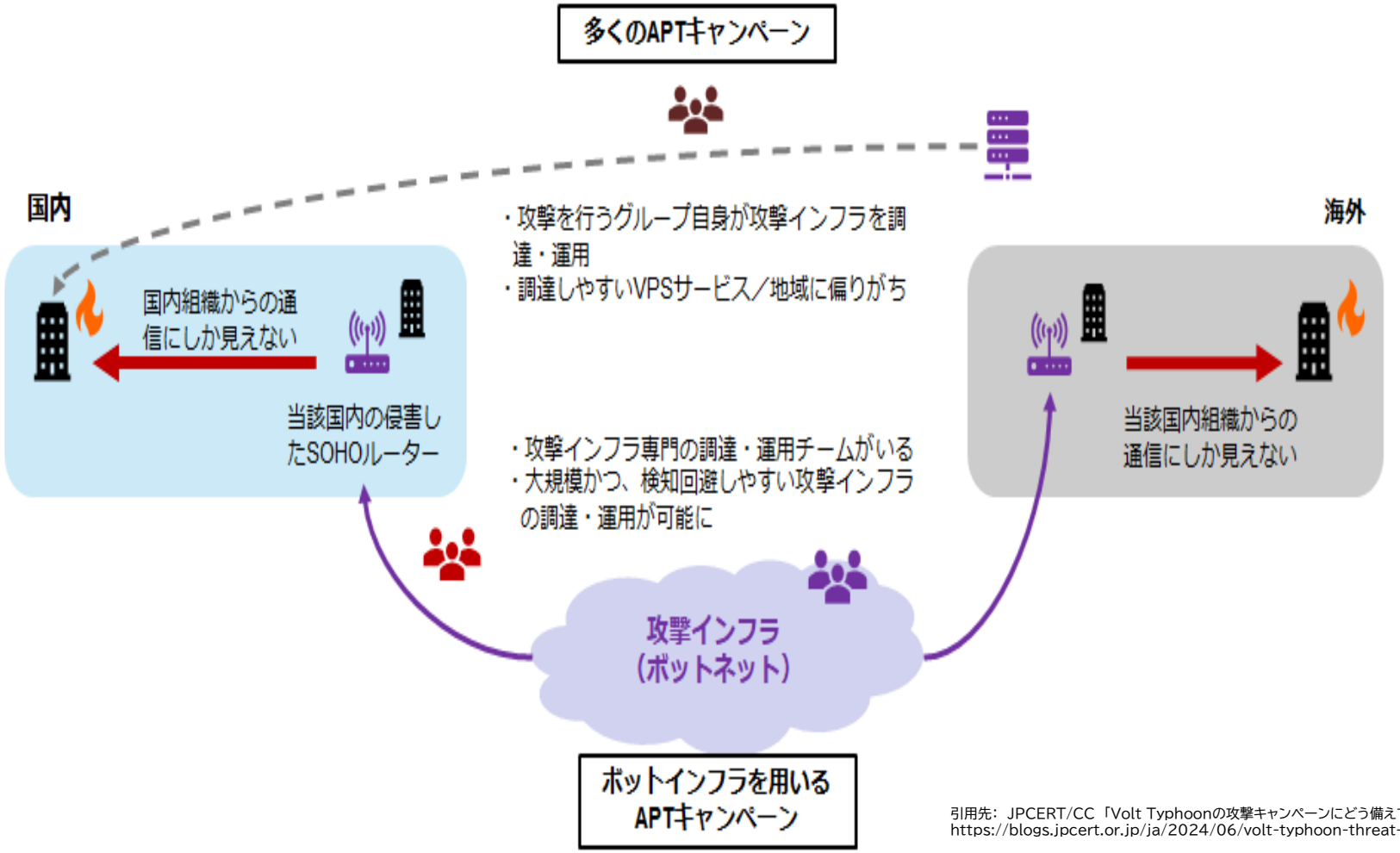
一般的なAPTでは攻撃キャンペーン期間内においてC2サーバーやマルウェアを使いまわすため、これらの情報を共有することで、未認知の被害をあぶり出すことや被害拡大防止を行うことができます。Volt Typhoonは、グループ固有のマルウェアをほとんど使わないなどのシステム内寄生戦術（Living off the Land（LotL）攻撃）の徹底により、被害現場にはIoC※となる情報をほとんど残しません。



引用先：JPCERT/CC「Volt Typhoonの攻撃キャンペーンにどう備えていくべきなのか」
https://blogs.jpcert.or.jp/ja/2024/06/volt-typhoon-threat-hunting.html

Living off the Land攻撃の事例①

『Volt Typhoon』の攻撃手口



多くのAPTアクターは攻撃インフラを自前で調達・運用していると考えられるため、限られたリソースの中で効率的にオペレーションを行うためにC2サーバーやマルウェアの使いまわしを合理的に選択している。
他方で大規模なボットネットを使う場合、ボットネットの構築、運用・維持に膨大なリソースが必要であるため、基本的に単独の攻撃グループが攻撃自体の実施とボットネットの運用と並行して行うことは困難と思われます。
いわゆるサイバークライム系の攻撃活動ではボットネットの構築・運用グループと、これを利用した複数のクライム系グループとの分担・連携が度々観測されています。

引用先：JPCERT/CC「Volt Typhoonの攻撃キャンペーンにどう備えていくべきなのか」
https://blogs.jpcert.or.jp/ja/2024/06/volt-typhoon-threat-hunting.html

Living off the Land攻撃の事例②

IIJ社が受けた「Living off the Land攻撃」

インターネットイニシアティブ(IIJ)社が2025年4月15日に同社のメールセキュリティーサービス「IIJセキュアMXサービス」から400万件超のアカウント情報が漏洩した可能性があると発表しました。同社の谷脇康彦社長は2025年5月13日、決算会見の冒頭で漏洩事故について謝罪し、サービスが受けた攻撃は**「Living off the Land(LotL)攻撃」**だったことを明らかにしました。

総務省は7月18日、サービス利用者の情報が漏洩した問題を受け、インターネットイニシアティブ(IIJ)社を行政指導したと発表した。

漏えい事実が確認されたお客様契約数

当該サービスで作成された電子メールのアカウント・パスワードの漏えい
対象のお客様契約数：132契約

(※)このうちの一部のお客様契約については電子メールアカウントのみ漏えい事実が確認されています。
(※)第一報で漏えいの可能性があるとした電子メールアカウント4,072,650件のうち、311,288件が該当します。

当該サービスを利用して送受信された電子メールの本文・ヘッダ情報の漏えい
対象のお客様契約数：6契約

当該サービスと連携して動作するように設定されていた他社クラウドサービスの認証情報の漏えい
対象のお客様契約数：488契約

引用元：IIJ「IIJセキュアMXサービスにおけるお客様情報の漏えいについてのお詫びとご報告」
https://www.iij.ad.jp/news/pressrelease/2025/0422-2.html

(攻撃手法)
　攻撃者はこの脆弱性を利用して、任意コードを実行し、不正アクセスを行いました。
(IIJ社の対応)
　IIJ社は2025年2月時点でActive! mailをサービスから除外し、現在は当該ソフトウェアを使用していません。
(クオリティアの対応)
　「Active! mail」の開発元であるクオリティアは、脆弱性を修正した新バージョンをリリースし、適用を呼びかけています。

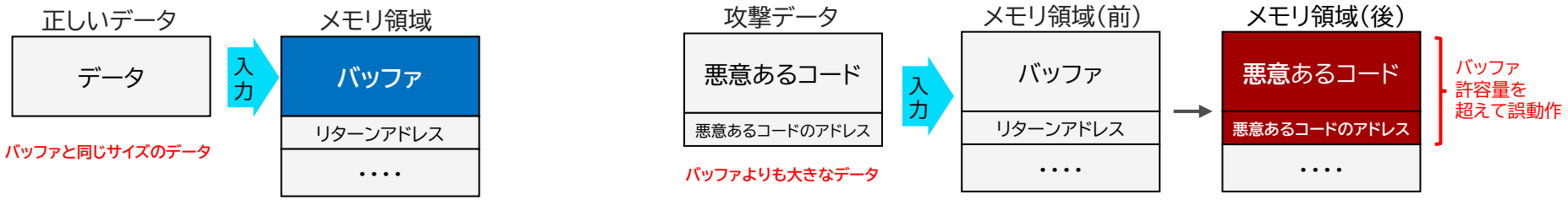
Living off the Land攻撃の事例②

IIJ社が受けた「Living off the Land攻撃」

IIJ(インターネットイニシアティブ)社のサイバー攻撃の原因は、同社が提供する「IIJセキュアMXサービス」で使用されていた第三者製ソフトウェア「Active! mail」の脆弱性を悪用されたことによるものです。この脆弱性は、不正アクセスが発生するまで発見されていなかった「ゼロデイ脆弱性」でした。

(原因)

IIJセキュアMXサービスで使用されていた「Active! mail」に、スタックベースのバッファオーバーフローを引き起こす未発見の脆弱性(CVE-2025-42599)が存在しました。



プログラムは、指示された処理を行うためにメモリ上に「バッファ」と呼ばれる使用領域を確保しています。この「バッファ」の中でもローカル変数や関数の引数、リターンアドレスなどを格納するメモリの領域はスタック領域と呼ばれています。スタックベースのバッファオーバーフロー攻撃では、主にスタック領域のリターンアドレスが書き換えられ、意図しないコードが実行される可能性があります。

脆弱性(CVE-2025-42599)

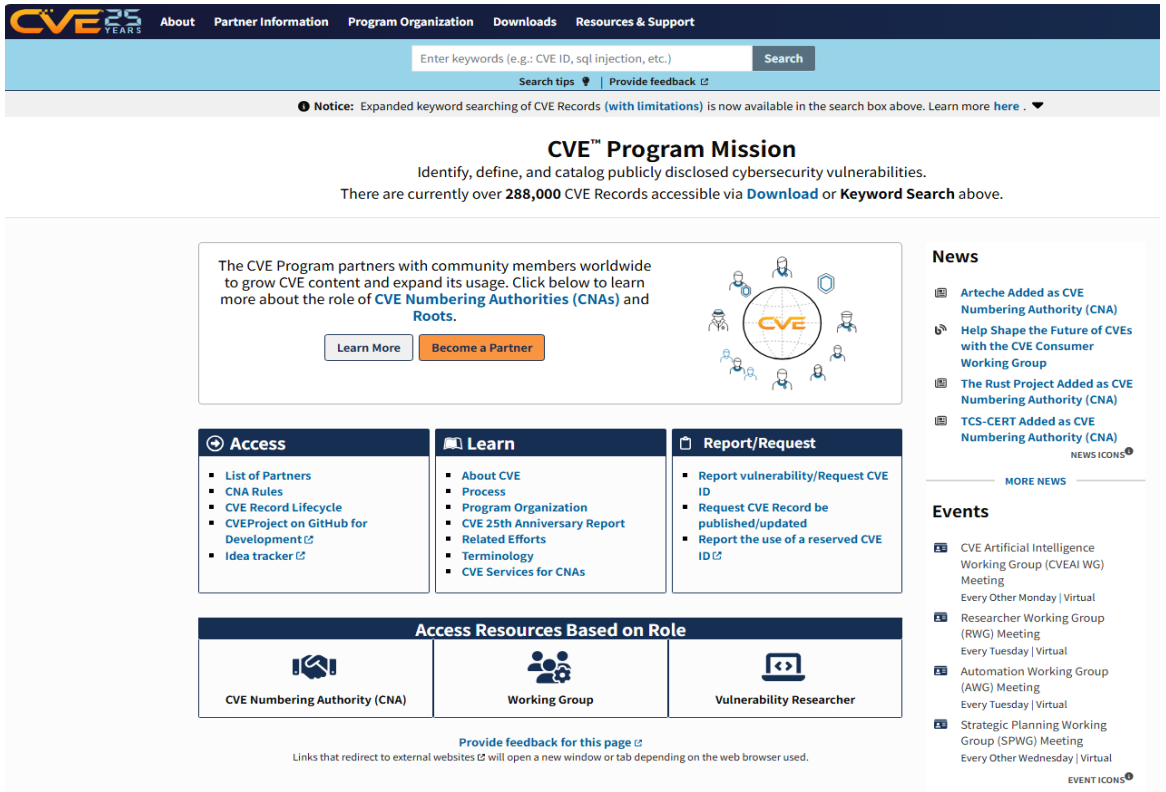
Score	Severity	Version	Vector String
9.8	CRITICAL	3.0	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

ソフトウェアの脆弱性を知る
～CVEを読み解く～

CVEとは

共通脆弱性識別子CVE(Common Vulnerabilities and Exposures)は、**個別製品中の脆弱性を対象**として、米国政府の支援を受けた非営利団体のMITRE社が**採番している識別子**です。
個別製品中の脆弱性に一意の**識別番号「CVE識別番号(CVE-ID)」**を付与している。

脆弱性情報データベース(CVE)プログラムに、世界40カ国以上の400以上のCVE採番機関が協力しており、2024年10月時点で24万件以上のCVEが登録されている。



CVE識別番号
「CVE-YYYY-NNNN」

CVE:
CVE識別子であることを示す固定文字

YYYY:
脆弱性が発見された年を表す西暦4桁の数字

NNNN:
その年で割り当てられた連番を表す4桁以上の数字

出典:https://www.cve.org/

CVEの概要

脆弱性(CVE-2025-42599)を検索すると

Required CVE Record Information

CNA: JPCERT/CC

Published: 2025-04-18 **Updated:** 2025-04-18

Description ← 脆弱性の説明

Active! mail 6 BuildInfo: 6.60.05008561 and earlier contains a stack-based buffer overflow vulnerability. Receiving a specially crafted request created and sent by a remote unauthenticated attacker may lead to arbitrary code execution and/or a denial-of-service (DoS) condition.

CWE 1 Total ← 脆弱性の種類
Learn more

- CWE-121: Stack-based buffer overflow

CVSS 1 Total ← 脆弱性の深刻度
Learn more

Score	Severity	Version	Vector String
9.8	CRITICAL	3.0	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Product Status
Learn more

Vendor ← 製品ベンダー
QUALITIA CO., LTD.

Product ← 製品
Active! mail 6

Versions 1 Total

Default Status: unknown
Affected

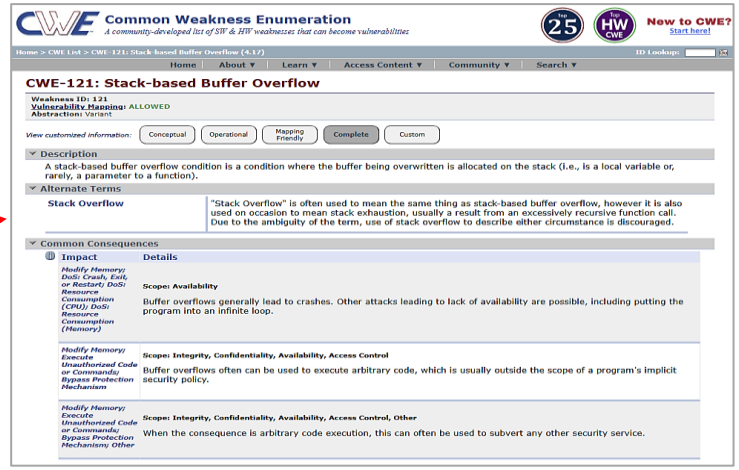
- affected at BuildInfo: 6.60.05008561 and earlier

References 2 Total ← 参考URL

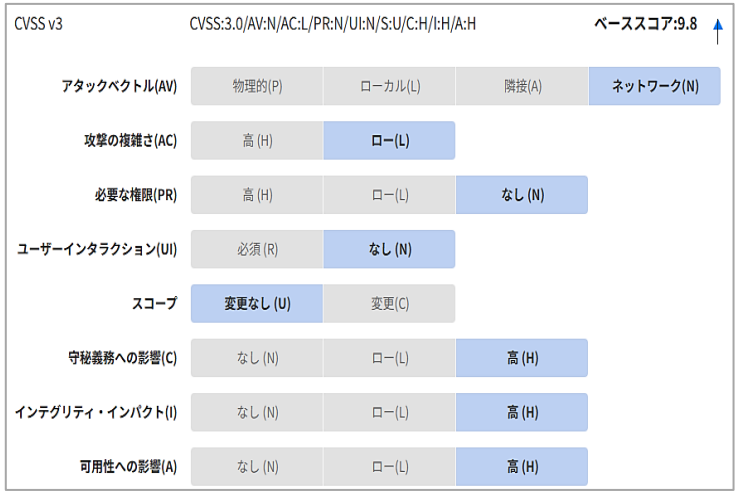
- https://www.qualitia.com/jp/news/2025/04/18_1030.html
- https://jvn.jp/en/jp/JVN22348866/

出典:https://www.cve.org/CVERecord?id=CVE-2025-42599

CWE-121: Stack-based Buffer Overflow



出典:MITRE
https://cwe.mitre.org/data/definitions/121.html



出典:JVN
https://jvn.jp/en/jp/JVN22348866/

今後のCVEは

CVE は今後どうなるのか？

脆弱性情報データベース（CVE）プログラムは、25年間、米国国土安全保障省（DHS）から資金提供を受けた非営利団体のMitre社が中心となって運営を担ってきましたが、2025年4月15日に、米国国土安全保障省（DHS）は**Mitre社への資金提供契約を更新しないことを通知**しました。

2025年4月に、米国政府予算の不透明性によって脆弱性情報データベース（CVE）プログラムの運営継続に支障が出る恐れがあると警告したと報じられ、**CVE Foundation（CVE財団）**※の設立が発表されました。

その一方で、米国サイバーセキュリティ・社会基盤安全保障庁**（CISA）はCVEを管理するMITREとの契約を延長**し、当面の運用資金を確保しましたが継続性にはまだ疑問が残されています。

※CVE Foundationは急遽設立したこともあって、設立時には組織体制や計画などについてなにも発表されていない状態でしたが、2025年6月5日にWebサイトを更新し、取締役会の設立と今後の計画について明らかにしました。


JNSA