Newton IT
脆弱性診断サービスのご紹介

第一版

Newton Information Technology Ltd.

IT脅威の現状

サイバー攻撃関連の通信数は全世界的に増加の傾向にあります。2015年と2023年の状況と比較すると、その数は**9.8倍**となっており、今後ますますセキュリティの強化が必要となる状況です。

情報処理推進機構(IPA)が発表した、2025年の情報セキュリティ10大脅威においては、システム脆弱性を突いた攻撃が3位となっております。また、1位のランサム攻撃による被害、２位のサプライチェーンや委託先を狙った攻撃についても、IT環境の脆弱性を悪用する手法が用いられることを鑑みると、**脆弱性への対処**が、セキュリティ強化対策の重要なポイントとなることが分かります。

(出典)総務省 NICTERにおけるサイバー攻撃関連の通信数の推移

組織編

順位	脅威
1	ランサム攻撃による被害
2	サプライチェーンや委託先を狙った攻撃
3	システムの脆弱性を突いた攻撃
4	内部不正による情報漏えい
5	機密情報等を狙った標的型攻撃
6	リモートワーク等の環境や仕組みを狙った攻撃
7	地政学的リスクに起因するサイバー攻撃
8	分散型サービス妨害攻撃（DDoS攻撃）
9	ビジネスメール詐欺による金銭被害
10	不注意による情報漏えい等の被害

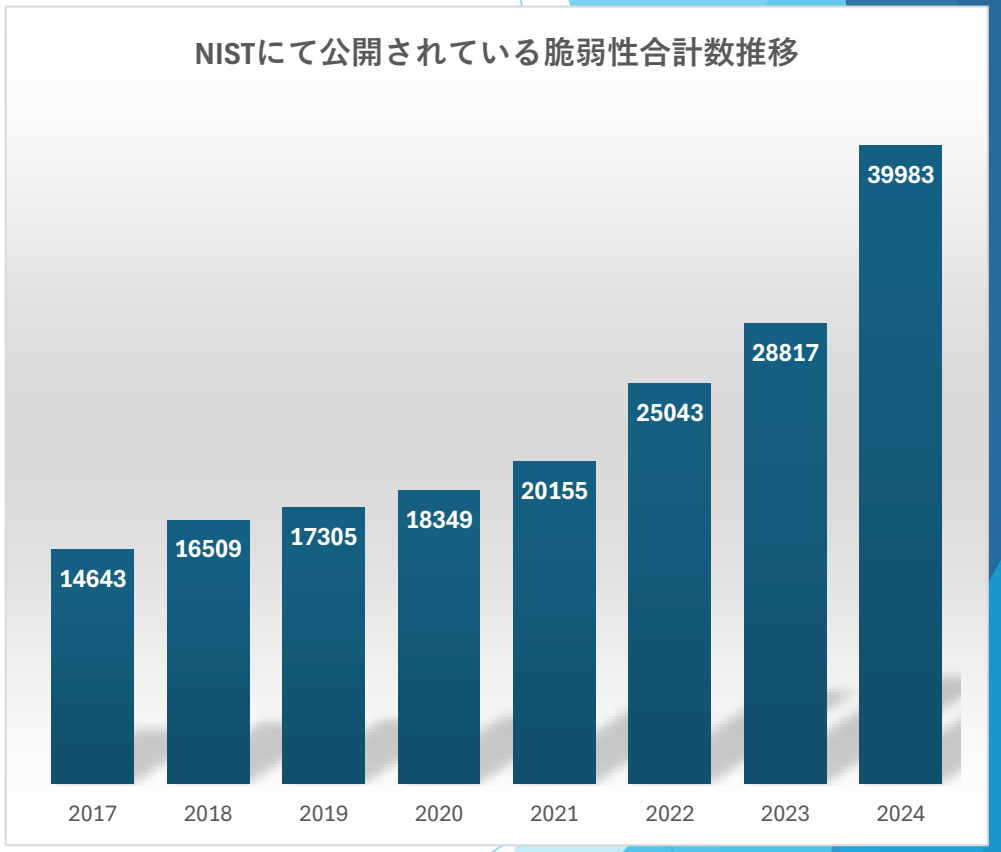
(出典)IPA 情報セキュリティ10台脅威2025

脆弱性とその傾向

脆弱性とは、コンピュータのオペレーティングシステムや、ソフトウェアにおいて、プログラムの不具合等が原因となって発生するサイバーセキュリティ上の欠陥を指します。

脆弱性が放置されていると、外部から攻撃を受けたり、ウイルスの感染に利用されたりする危険性があるため、インターネットに接続しているコンピュータにおけるサイバーセキュリティ上の大きな問題の一つとなっています。このような脆弱性が発見されると、多くの場合、ソフトウェアを開発したメーカーが更新プログラムを作成して提供します。しかしながら、**脆弱性は完全に対策を施すことが困難であり、次々と新たな脆弱性が発見されている**のが現状です。
(参考)総務省国民のためのサイバーセキュリティサイト

米国国立標準技術研究所(NIST)が運営する脆弱性データベース (右グラフ)によると、2024年に全世界で発見された脆弱性は39,983件となっております。IT専任部署がある、もしくは、IT環境管理を専門企業にアウトソースしている場合であっても、**人の手のみですべての脆弱性をタイムリーに把握し、迅速に対処するのは難しい**のが現状です。



海外拠点からグループ全体への被害拡大

海外拠点における脆弱性対策が十分でない場合、サイバー攻撃を受けた際にその**被害がグループ全体まで拡大する可能性は非常に高い**状況です。以下は実際にそのような事象が発生した日系企業の例となります。

業種	発生年	攻撃内容	被害概要
自動車メーカー	2024年	米国支社への不正アクセスが発生。	財務情報や健康保険情報顧客や従業員の個人情報を含む、約240GBの機密情報が流出。
眼鏡・レンズメーカー	2024年	海外の事業所に対するサイバー攻撃が発生。	内視鏡検査を受診した患者の氏名、性別及び年齢を含む個人情報が流出。
光ケーブルメーカー	2024年	タイ子会社への不正アクセスが発生。国際ネットワーク経由で日本のサーバー等にもアクセスあり。	製造及び出荷に影響が発生。銀行口座情報を含む従業員の個人情報も流出した可能性あり。
情報処理サービス	2024年	業務委託先の海外拠点へのランサムウェア攻撃が発生。	管理を受託していた自治体や企業の住民・顧客リストより、約150万件の個人情報が漏洩。
電子部品メーカー	2024年	中国現地法人への不正アクセスが発生。	生産・出荷に影響が発生。社員の個人情報や業務ファイルが外部へ流出。
ゲームソフトウェアメーカー	2020年	北米の現地法人に設置していた旧型VPN装置へのサイバー攻撃が発生。	1万件以上の個人情報が外部へ流出。

Newton IT 脆弱性診断サービス概要

お客様のICT環境の脆弱性を可視化し、改善提案を行います。

- ICTインフラストラクチャー/Webアプリケーション(Webサイト)に対する脆弱性診断を実施
- 以下2種類の診断後レポートを作成の上、脆弱性を可視化
  1. サマリーレポート
  2. 詳細レポート
- 可視化された脆弱性に対する改善案を、対応費用も含めてご提案
- 質疑応答等のアフターフォローまで実施
- 必要に応じて、日本本社ITご担当者様へのご説明も実施可能

診断レポートサンプル

サマリーレポート

Newton Information Technology Limited
166 College Road, Harrow, HA1 1BH, United Kingdom
Tel: +44 (0)20 8782 1920
www.newtonit.com

Vulnerability Scan Report

Summary

Date	DD/MM/YYYY
Engineer	Newton IT
Target Host	https://....
Scanner	Qualys vulnerability scanner
Scanner Option	Web Application Scanning and Infrastructure Vulnerability Scan
Confirmed Vulnerabilities	5
Potential Vulnerabilities	1

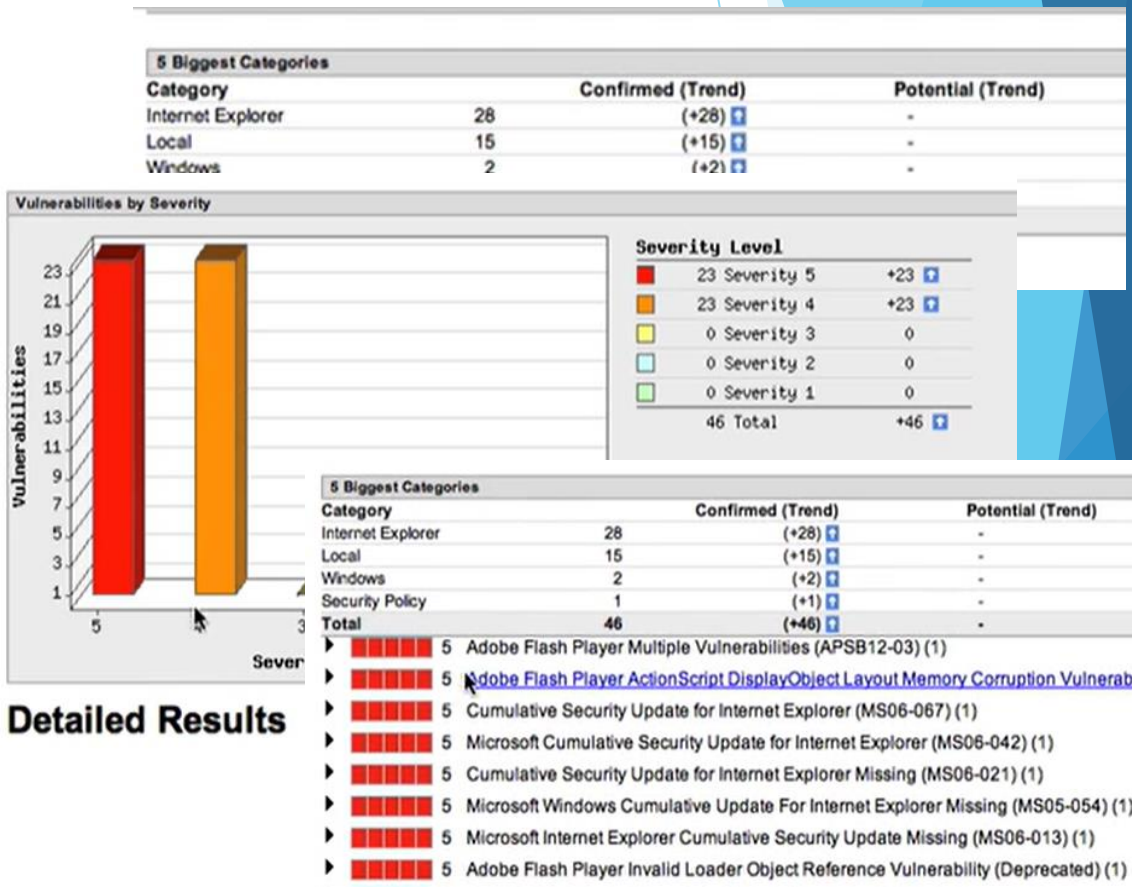
Details

No.	Severity		Category	Vulnerability / Possible Vulnerability	QID	Status	Solution / Remarks
	Confirmed	Potential					
1	5	-	HTML form containing password field(s) is served over HTTP	An HTML form containing a password field (input field with type=password) is served insecurely over HTTP. Serving an HTML form containing a password field (type=password) makes it susceptible to phishing attack. Failure to utilize SSL/TLS for the login landing page could allow an attacker to modify the login form action, causing the user's credentials to be posted to an arbitrary location.	150150	New	Make sure that HTML forms containing password field(s) are always served over HTTPS only.
2	5	-	Sensitive Files Disclosure	A potentially sensitive file was discovered on the Web server. This file may or may not be directly associated with the web application.	150356	New	Verify that access to this file is permitted. If necessary, remove it or apply access controls to it.
3	4	-	Unencoded characters	The web application reflects potentially dangerous characters such as single quotes, double quotes, and angle brackets. These characters are commonly used for HTML injection attacks such as cross-site scripting (XSS)	150084	New	Review the reflected characters to ensure that they are properly handled as defined by the web application's coding practice.
4	4	-	Sensitive form field has not disabled autocomplete	An HTML form that collects sensitive information does not prevent the browser from prompting the user to save the populated values for later reuse. Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.	150112	New	Add the following attribute to the form or input element: autocomplete="off" This attribute prevents the browser from prompting the user to save the populated form values for later reuse. Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment. Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.
5	4	-	Clickjacking - Framable Page	The web page can be framed. This means that clickjacking attacks against users are possible.	150124	New	Clickjacking prevention mechanisms include: - X-Frame-Options: This HTTP response header can be used to prevent framing of web pages. - Content-Security-Policy: The 'frame-ancestors' directive can be used to prevent framing of web pages. - Framekiller JavaScript code designed to prevent a malicious user from framing the page. This method is not recommended due to its unreliability.
6	-	1	Path Disclosure	Suspected Path Manipulation Vulnerability	150622	New	Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Legend

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

詳細レポート



費用体系①

- 初回の診断は、**トライアルとして無償でご提供いたします**(*1)。サービス内容を評価いただいた上で、今後の継続使用有無をご判断いただくことが可能です。
- 無償トライアル実施後のサービス費用は、以下3要素に基づき算出させていただきます。

1. 診断対象が、インターネット経由で到達可能な環境であるか否か

   アクセスにあたってVPN等の使用を必要とする場合、インターネット経由での到達は不可能な環境であると分類

2. 診断対象

   - ICTインフラストラクチャー

     診断対象となるICT資産のグローバルIP数により費用が変化

   - Webアプリケーション

     診断対象となるWebアプリケーションのURL数により費用が変化

3. 実施頻度

   年2回の実施を前提とし、増減のご希望がある場合は別途お見積りとなる

費用体系②

※ 記載の費用はVATを除く

- インターネット経由で到達可能な環境

分類	グローバルIP/URL数	年間費用
ICTインフラストラクチャー	1	£1,800
	2	£2,300
	3	£2,800
	4	£3,300
	5	£3,800
Webアプリケーション	1-10	£4,000
	11-20	£4,500
	21-30	£5,000
	31-40	£5,500
	41-50	£6,000
	51-75	£6,500
	76-100	£7,000

- インターネット経由で到達不可能な環境

分類	グローバルIP/URL数	年間費用
ICTインフラストラクチャー	1	£2,800
	2	£3,300
	3	£3,800
	4	£4,300
	5	£4,800
Webアプリケーション	1-10	£5,000
	11-20	£5,500
	21-30	£6,000
	31-40	£6,500
	41-50	£7,000
	51-75	£7,500
	76-100	£8,000

注意事項

- *1: 無償トライアルは以下の条件にて提供されます。
  - ICTインフラストラクチャー・Webアプリケーションともに、インターネット経由で到達が可能な環境に対する診断に限定
  - ICTインフラストラクチャーに対する診断の場合は、グローバルIP 1点のみが対象となる
  - Webアプリケーションに対する診断の場合は、1アプリケーションが対象となり、対象のURLはお客様と弊社にて検討の上決定させていただく

ご連絡先

Newton Information Technology Ltd.

Sales and Marketing Group

+44(0)20-8782-1920

sales@newtonit.com