# SQAT®
# 情報セキュリティ瓦版

2020年1月号

株式会社ブロードバンドセキュリティ
セキュリティサービス本部
東京都新宿区西新宿 8-5-1 野村不動産西新宿共同ビル 4F
TEL：03-5338-7417 FAX：03-5338-7435
https://www.bbsec.co.jp/

# 高まる APT 攻撃の脅威
## ー あらためて、「侵入前提」の備えを ー

**「攻撃のターゲットに定めた組織に対し、高度かつ複雑な手法を用いて長期間にわたり執拗な攻撃を行う」―「APT」と呼ばれるタイプの攻撃の矛先が、今、日本にも向けられるようになっています。従来、APTには侵入を前提とした多層防御が有効とされてきましたが、国際的に注目度の高いイベントであるオリンピック・パラリンピックが目前に迫り、日本を対象とした攻撃がこれまでになく増えると予想される中、あらためて自組織の状況を点検し、セキュリティの強化を図る必要があります。**

### APT28 とは

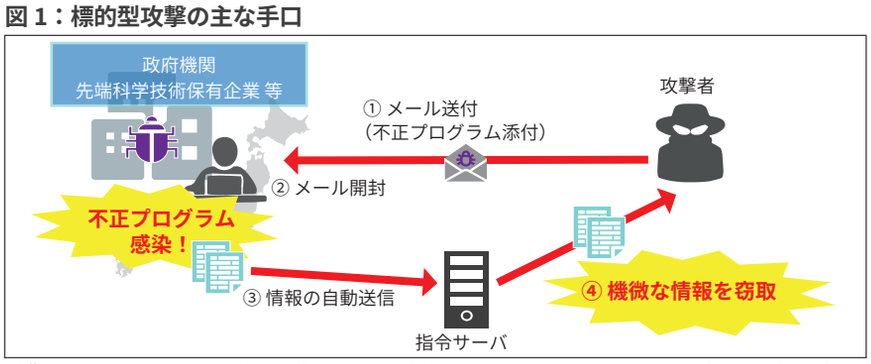
「APT」と は「Advanced Persistent Threat」（直訳すると「高度で持続的な脅威」）の略語で、日本では主に「高度標的型攻撃」という呼称が使われています。「標的型攻撃」は、文字どおり、特定の組織をターゲットにした攻撃を指します（図１参照）。この中でも高度な手法を用いた長期にわたるものが「APT」とみなされます。狙いを定めた相手に適合した方法・手段を用いて侵入・潜伏を図り、攻撃に必要な情報を入手するための予備調査も含め、執拗に活動を継続するのが特徴です。なお、セキュリティ機関や調査会社では、こうした攻撃が確認されると、攻撃の実行主体（APTグループ）を特定し、活動の分析に取り組みます。グループを追跡する際は、組織が自ら名乗る名称に加え、多くの場合、「APT＋数字の連番」（例:「APT 1」「APT 2」）がグループ名として使用されています。

### 広範かつ大規模な攻撃活動

これまでに特定された APT グループの数は、上記連番方式により同定されているグループだけでも約 40 に上ります。国家レベルの組織による支持や支援を受けているとみられるものも多く存在し、その攻撃は高度であるだけでなく、広範かつ大規模です。直近では 2019 年 10 月に、ロシアの支援を受けているとみられる「APT28」（自称「Fancy Bear」）による脅迫メールが世界的な注目を集めました。

脅迫の手口は、「攻撃対象の組織の Web サイト、外部から接続可能なサーバ・インフラに対する DDoS 攻撃を予告し、それを回避するための費用として仮想通貨を期日内に支払うよう要求する」というも

**図１：標的型攻撃の主な手口**




出典：https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_kami_cyber_jousei.pdf

ので、危機感を煽るため実際にDDoS 攻撃を行ったケースもありました。ペイメント、エンターテインメント、小売といった業種の複数組織を対象に同グループによる脅迫メールが送付されていることを、ドイツのセキュリティベンダが特定し、その後、JPCERT/CC により日本国内においても複数の組織が同様のメールを受け取っていることが確認され、注意喚起が出されています。なお､同グループは､2016 年の米大統領選挙のほか、政治団体やスポーツ団体などをターゲットにした攻撃への関与も疑われています。

## 地域・文化を超えるサイバー攻撃

従来、APT 攻撃は主に欧米の組織を標的にしており、日本語という言語の特殊性などがハードルとなり日本企業は狙われにくいとの認識がありました。しかし、近年は、巧みな日本語を使用した、明らかに日本企業を標的とする攻撃が増加傾向にあります。

たとえば、独立行政法人情報処理推進機構（IPA）に報告されたサイバー攻撃に関する情報（不審メール、不正通信、インシデント等）の 2019 年の集計結果では、9 月末時点で寄せられた攻撃情報、計 897 件のうち 235 件が標的型とみなされており、直近の 7 月～ 9 月でその比率が顕著に上昇しています（表 1 参照）。当該データ 113 件のほぼ 9 割がプラント関連事業に対する攻撃で、実在すると思われる開発プロジェクト名や事業者名を詐称し、プラントに使用する資機材の提案や見積もり等を依頼する内容の偽メールが送信されています。IPA は、「現時点では、攻撃者の目的が知財の窃取にある（産業スパイ活動）のか、あるいはビジネスメール詐欺（BEC）のような詐欺行為の準備段階のものかは不明」としつつも、特定の組織へ執拗に攻撃が繰り返されていることから、これらをAPT 攻撃の可能性がある標的型メールの一種に位置づけたと説明しています。

**表 1：標的型の攻撃が増加**

| | 1 月 ~3 月 | 4 月 ~6 月 | 7 月 ~9 月 | 合計 |
|---|---|---|---|---|
| IPA への情報提供件数合計 | 238 | 424 | 235 | 897 |
| うち、標的型と見られる情報の件数 | 47 | 75 | 113 | 235 |

出典：サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2019 年 1 月～ 3 月 ]、[2019 年 4 月～ 6 月 ]、[2019 年 7 月～ 9 月 ] より当社作成

同様の傾向は、他国のセキュリティ機関の分析からも伺えます。タイの CSIRT 組織 ThaiCERT によるレポート『THREAT GROUP CARDS: A THREAT ACTOR ENCYCLOPEDIA』（2019 年 6 月公開）*1 を見ると、日本をターゲットに含めた攻撃は、もはや少ないとは言えません。たとえば、「Blackgear」と呼ばれる攻撃グループは日本を明白なターゲットにしており、C&C の拠点を日本に置き、日本語の文書を使って攻撃を仕掛けます。また、2018 年に確認された東南アジアの自動車関連企業をターゲットとした攻撃では、タイミングを同じくして特定の日本企業への攻撃が複数回観測されています。さらに、ターゲットとされる業種や狙われる情報の種類が多様であることも目を引きます。かつては、銀行のデータや個人情報がまず標的になりましたが、ここ数年、ターゲットの業界が航空宇宙・自動車・医療・製薬へとシフトし、ブラックマーケットでの高額取引が期待できる、各業界に固有の技術情報や特許出願前情報の奪取へと、攻撃目標が変化しています（次ページ、表 2 参照）。

個人情報が流出した場合の損害賠償や事態収拾のための費用などを含めた事後対策費は平均 6 億 3,760 万円[1)] と言われていますが、技術情報が流出した場合の想定被害額はその数十倍、数百倍に及ぶ可能性があります。技術情報のみならず、いわゆる「営業秘密」とされる知的財産の流出は、事業活動の根幹を揺るがす事態に発展しかねない規模の損失を招く恐れがあります。近年各社により提供されるように

なっているサイバーセキュリティ保険等で損害補償対策を検討するのも一案ですが、国家の関与が疑われる APT グループの攻撃被害については保険金が支払われない可能性もあります。より甚大な被害をもたらす攻撃を行うグループが、今、日本企業を新たな標的に定めつつあるという事実は、国内のあらゆる事業者が共有すべき攻撃の傾向となっています。

**表 2：日本を標的に含めている主な攻撃グループ**

| グループ名 [2] | ターゲットの業種 |
|---|---|
| APT 12/ Numbered Panda | 防衛、電子・ハイテク産業、通信およびメディア |
| APT 17/ Deputy Dog | 防衛、政府、IT、鉱業、NGO および法執行機関 |
| APT 29/ Cozy Bear/The Dukes | 防衛、エネルギー、政府、法執行機関、メディア、NGO、製薬、通信、シンクタンク、運輸 |
| APT 32/ OceanLotus/SeaLotus | 政府、ホスピタリティ、製造、小売、反体制派、ジャーナリスト |
| APT 16/ SVCMONDR | 金融、政府、ハイテク、メディア、航空、自動車、化学技術 |
| Axiom/Group 72 | 航空宇宙、防衛、製造およびメディア |
| Blackgear | (省略)※本文を参照 |
| BlackTech | 金融、政府、ヘルスケア、テクノロジー |
| Blue Termite/ Cloudy Omega | 自動車、化学、建設、教育、エネルギー、金融、食品と農業、政府、ヘルスケア、ハイテク、産業、IT、メディア、不動産、通信、輸送 |
| Bronze Butler/ Tick | 重要インフラ、防衛、政府、製造業の技術情報 |
| Sofacy/APT 28/ Fancy Bear/Sednit | 化学、防衛、外交機関、エンジニアリング、政府、製造、諜報機関、メディア、NGO およびシンクタンク |
| Lazarus Group/Hidden Cobra/ Labyrinth Chollima | エンジニアリング、金融、政府、テクノロジー |
| Mabna Institutem/ Silent Librarian | 大学 |
| Samurai Panda/APT 4 | 防衛、政府 |
| Snake Wine | 政府、小売り、教育 |
| Stone Panda/APT 10/ menuPass | 航空宇宙、防衛、政府、医療、製薬 |
| DragonOK | ハイテク企業、製造業 |
| Winnti Group/Blackfly/ Wicked Panda | オンラインビデオゲーム会社、製薬、通信 |

出典：『THREAT GROUP CARDS: A THREAT ACTOR ENCYCLOPEDIA』より当社作成

## より強靭な「多層防御」で APT 攻撃の影響を最小限に抑える

APT 攻撃への対策としては、従来、侵入を前提とした多層防御が有効とされてきましたが、足元で APT グループによる日本への攻撃が増加傾向にある中、あらためて、多層防御の状況を点検し、攻撃耐性を高めていくことが求められています。防御策としてまず思い浮かぶのは、出入口を守るファイアウォールや UTM（統合脅威管理）、既知の脆弱性への対応などですが、それだけでは十分とは言えません。

APT 攻撃での代表的な手口は、ターゲットにした組織への侵入を試みる目的で使用される標的型メールです。この入口対策を考えると、疑似的な攻撃メールを用いて開封率などを可視化して「ヒト」に対する教育訓練を施す「標的型メール訓練」は検討に値する対策の 1 つです。留意したいのは、開封率の低減を最重要視するのではなく、「開封されても仕方なし」というスタンスで取り組むことです。訓練の目標を「開封された後の対応策の見直しと初動訓練」に設定し、定められた対応フロー通りに報告が行われるか、報告を受けて対策に着手するまでにどれくらいの時間を要するかを可視化して、インシデント時の対応フローおよびポリシーやガイドラインの有効性を評価することをお勧めします。また、従業員のセキュリティ意識を向上させるために、教育および訓練と演習を実施するのが望ましいでしょう。

また、「多層防御」対策を立てる前提として、情報資産の棚卸しも重要です。日本企業は、他国に比較して、知的財産の重要性に対する認識が低く、情報の所在や管理が徹底されていないという指摘があります [3]。組織内に存在する情報に関し、機密とするもの、公知であってよいものを分類し、それらがどこに格納されて、どのように利用されているかを可視化した上で、防御の対応をする機器・人・組織といったリソースを適切に振り分けて防御する仕組みを構築することが求められます。こうした仕組みは、侵入の早期発見にも繋がり、事業活動の継続を左右する重要情報へのアクセスを遮断することで、万一侵入を許しても被害を最小限に抑えられます。さらに感染経路・奪取可能な情報を洗い出し、感染範囲・重要情報へのアクセス状況・流出経路などを可視化できれば、システム内部へ拡散するリスクを把握することもできます。この「標的型攻撃のリスク可視化」により、「出口」対策へ効果的にリソースを有効活用することで、実効性をさらに効果的にリスク評価することが可能になります。

2020 年、オリンピック・パラリンピックがいよいよ目前に迫り、日本への攻撃がさらに激しさを増していくと予想されます。同イベントには膨大な数の事業者が関与するため、セキュリティ的に脆弱な組織が APT 攻撃を受け、サプライチェーンや IoT を通じて被害が歯止めなく広がるリスクが大いに懸念されています。既存のセキュリティ体制をあらためて点検し、強靭化を図ることで被害を最小限に食い止めましょう。

注：

[1] JNSA：2018 年情報セキュリティインシデントに関する調査結果より

[2] 同一のグループに対し、セキュリティ機関による命名、攻撃グループによる自称などを列挙

[3] コンサルティング会社 PwC が 2017 年に実施した調査より（https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2018/assets/pdf/economic-crime-survey.pdf) 日本における「組織がサイバー攻撃の狙いとなった不正行為」の種類を問う質問で「知的財産の盗難」と回答した比率は 25% で、世界平均の 12% と比べて顕著に多い数字となった。

参考情報：

[*1] https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf

# Web アプリケーションに求められる「二極のスコープ」による診断

**Web アプリケーションの脆弱性は時として深刻な被害にもつながる、看過できない脅威です。「攻撃者の視点」でセキュリティホールを特定する脆弱性診断に加え、「開発者の視点」から問題を特定するソースコード診断も重要です。前者はアプリケーションの「外」から脆弱性を検出するのに対し、後者はアプリケーションの「内」から問題部位をピンポイントで検出します。両者を連携させることが、Web アプリケーションのセキュリティを効果的に高めるカギになります。**

## 脆弱性はどこから生まれるか

そもそも、Web アプリケーションでセキュリティの脅威となる脆弱性が生まれるのは、「プログラムの処理において、開発者が意図していない動作が行われないようにする」という点で適切な制御ができていないことに原因があります。

Web アプリケーション開発において広く利用されている PHP で検出された脆弱性の例を挙げましょう。2019 年 10 月、nginx と PHP-FPM を組み合わせた一部の環境で、PHP プログラムの内部処理の不具合により不正なリモートコードが実行され得る脆弱性 (CVE-2019-11043) が発見されました。この脆弱性は、具体的には、「使用される値（URL）に対して、入力値としての妥当性が確認されないことを想定しておらず、適切に制御されない」という不備に起因するもので、サポートが終了しているバージョンおよび対策済みバージョン未満のすべての現行版が影響を受けました。

PHP は、WordPress をはじめとする多くの Web アプリケーションで利用されており、当該脆弱性の影響は、PHP ベースのアプリケーションを開発する多くの組織に及んでいます。警察庁の最近の調査によれば、同庁のインターネット定点観測においても、当該脆弱性を狙った攻撃を目的とする探索行為が観測されています [*1]。

Web アプリケーションを開発する組織は、こうした脆弱性の影響により、さまざまな対応に追われることになります。開発言語の脆弱性に加えて、アプリケーションのプログラミングで発生する脆弱性も、発覚がライフサイクルの後工程になればなるほど、対応のための負荷が増大します。なお、後者の脆弱性については、開発サイクルの可能な限り手前の工程で問題を特定・解消できていれば、修正にかかるコスト、影響範囲ははるかに小さく済みます。その意味で、Web アプリケーションのソースコードを点検することには、大きな意義があります。

## Web アプリケーションの構造

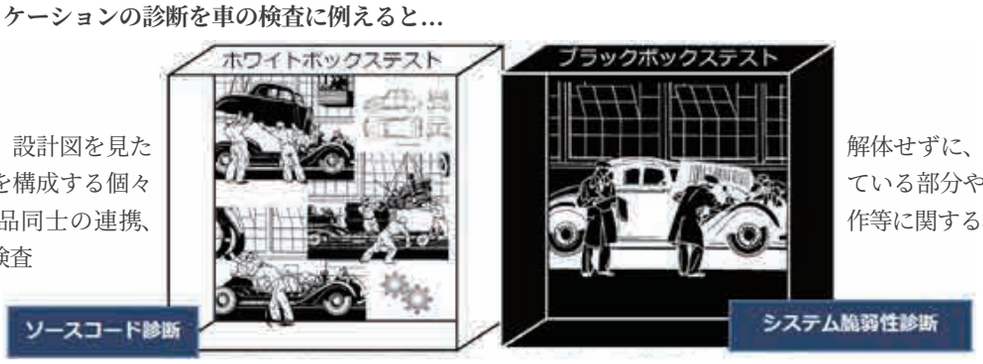
プログラムは、「入力」→「ロジック」→「出力」の 3 つの処理で構成されています。脆弱性を作り込まないためには、これらすべての処理を制御し、意図しない動作が起きないようにすることが重要であり、「入力」「ロジック」「出力」の各処

**＜ホワイトボックステスト＞**
システムの内部構造に着目して機能や動作を検証。
開発工程で例えると、プログラム・詳細設計書レベルで評価を行う、「単体テスト」。

**＜ブラックボックステスト＞**
システムの内部構造とは無関係に外部から見た機能や動作を検証。開発工程で例えると、仕様・機能設計書レベルで評価を行う、「総合テスト」。

**Web アプリケーションの診断を車の検査に例えると…**

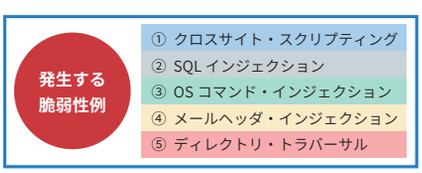
解体したり、設計図を見たりして、車を構成する個々の部品や部品同士の連携、仕組み等を検査




解体せずに、車内外の見えている部分や想定される動作等に関する検査

理が適切に制御しているかを、「内部」すなわちソースコード診断により検証し、あわせて、「外部」から確認できる挙動（リクエスト・レスポンス）を検証することで、問題の検出精度を高めることができます。

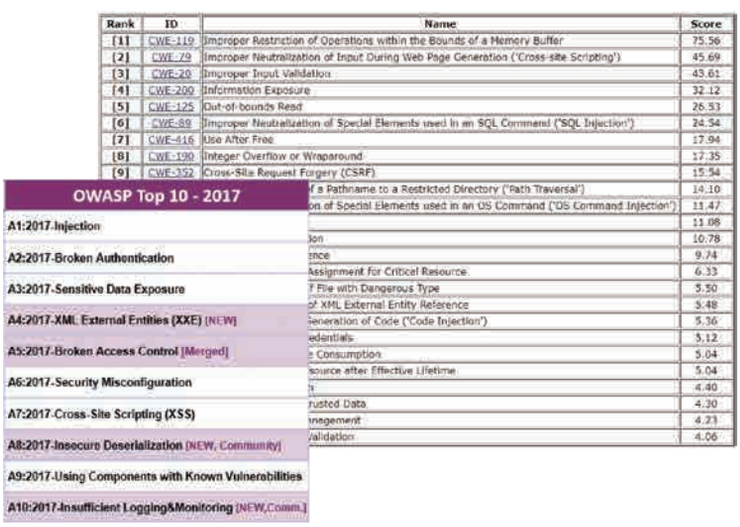
なお、こうした二極からの検証は、「ホワイトボックステスト」、「ブラックボックステスト」とも呼ばれます。前ページで示したように、車の検査に例えるとわかりやすいかもしれません。両者にはそれぞれ異なる役割があり、両者を組み合わせることで、より信頼度の高い検査をすることが可能になります。


## 脆弱性に関する業界ガイドライン

業界標準のガイドラインも Web アプリケーションの脆弱性を評価する際に役立ちます。代表的なものとして、本稿では「OWASP Top 10」と「CWE Top 25」をご紹介します。

OWASP Top 10 は、Web アプリケーションの脆弱性を、「悪用のしやすさ」、「蔓延度」、「検出しやすさ」、「技術面への影響」、「ビジネスへの影響」といった観点からランク付けし、最も重大な Web アプリケーションセキュリティリスク（「Most Critical Web Application Security Risks」）Top 10 を選出しています。一方、CWE Top 25 は、ソフトウェア開発で起こり得るプログラミングエラーを体系的に分類した項目リストである CWE（共通脆弱性タイプ一覧）をベースにしたものです。リストの各項目に対し、米国の脆弱性情報データベース NVD の評価を加味して危険度のスコアを算出し、最も危険性が高いと評価されるソフトウェアエラー（「Most Dangerous Software Errors」）Top 25 を選出しています。Web アプリケーションの観点でいうならば OWASP Top 10 が「ブラックボックステスト」であり、CWE Top 25 は「ホワイトボックステスト」と考えることができます。



| Rank | ID | Name | Score |
|---|---|---|---|
| [1] | CWE-119 | Improper Restriction of Operations within the Bounds of a Memory Buffer | 75.56 |
| [2] | CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 45.69 |
| [3] | CWE-20 | Improper Input Validation | 43.61 |
| [4] | CWE-200 | Information Exposure | 32.12 |
| [5] | CWE-125 | Out-of-bounds Read | 26.53 |
| [6] | CWE-89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 24.54 |
| [7] | CWE-416 | Use After Free | 17.94 |
| [8] | CWE-190 | Integer Overflow or Wraparound | 17.35 |
| [9] | CWE-352 | Cross-Site Request Forgery (CSRF) | 15.54 |
| | | of a Pathname to a Restricted Directory ('Path Traversal') | 14.10 |
| | | on of Special Elements used in an OS Command ('OS Command Injection') | 11.47 |
| | | | 11.08 |
| | | ion | 10.78 |
| | | ince | 9.74 |
| | | Assignment for Critical Resource | 6.33 |
| | | F File with Dangerous Type | 5.50 |
| | | of XML External Entity Reference | 5.48 |
| | | Generation of Code ('Code Injection') | 5.36 |
| | | edentials | 5.12 |
| | | e Consumption | 5.04 |
| | | source after Effective Lifetime | 5.04 |
| | | h | 4.40 |
| | | rusted Data | 4.30 |
| | | nagement | 4.23 |
| | | Validation | 4.06 |

OWASP Top 10 - 2017

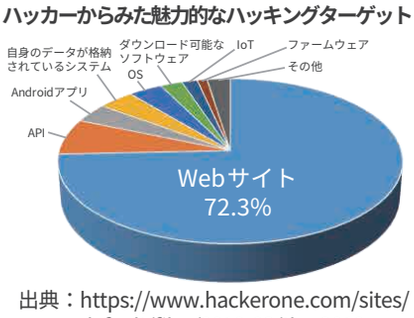
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE) [NEW]
A5:2017-Broken Access Control [Merged]
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization [NEW, Community]
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

出典：https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

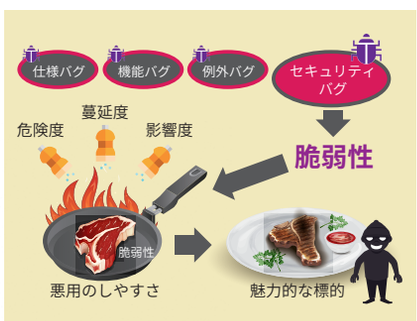
## 攻撃活動を先んじて制する

Web アプリケーションの脆弱性は、攻撃者にとって魅力的な標的です。悪用可能な脆弱性を常に探している彼らは、Web アプリケーションの構造設計やロジックを想定して仮説を立て、解析・検証し、特定の状況・環境・条件下において発現する不具合を見つけ出そうとします。お気づきでしょうか？実は、こうした攻撃者の行動パターンの裏をかくこと、攻撃者の行動に先んじてそれを阻むような手を打つことが、セキュリティ対策になり得るのです。いち早く脆弱性を見つけ、問題を解消することが重要です。この意味でも、リリース前に問題の検出に取り組むことは重要です。ソースコードレビューや単体試験などの段階でのソースコード診断は、効果的なタイミングの一例となります。

**ハッカーからみた魅力的なハッキングターゲット**




出典：https://www.hackerone.com/sites/default/files/2019-03/the-2019-hacker-report_0.pdf



## 上流での対処を促進

脆弱性になるべく上流工程で対処する取り組みを促進することも重要です。たとえば、近年注目を集めているアプローチで、「シフトレフト」というものがあります。これは、ソフトウェア開発で生じる各種課題への対処をできるだけライフサイクルの早期の段階へとシフトさせていこうという考え方で、手戻りを防ぎ、品質を落とすことなく時間やリソースを効果的に節減することを目指すものです。セキュリティ対策においては、プログラムが想定しない動作をしないことを検証するための工程を前倒しすることで、セキュリティ強化・コスト削減・生産性向上といった面からも着実な成果が期待できます。開発ライフサイクルに明示的にセキュリティを組み込む、「DevSecOps」を推進するのも一案です。

リリースの直前でプログラムの問題が発覚した場合、状況によっては設計を根本から見直す必要が生じるかもしれません。リリース後の診断で重大な脆弱性が明らかになった場合は、サービス停止という事態もありえます。問題の修正にかかるコストや時間は、発覚が後になるほど膨らみ、致命的なビジネス損失を招く恐れがあります。早期の段階で不具合検出のためのリソースを投入することは、結果として最良の費用対効果を得られることにつながります。

## 「二極のスコープからの診断」がカギ

開発工程において常に生み出される可能性がある―これが、Web アプリケーション脆弱性に見られる 1 つの特徴です。リスクを最小化するカギは、できるだけ上流で脆弱性の芽を摘む体制を構築し、かつ、「内と外」の二極から脆弱性評価を行うことです。複眼的な軸を持つことは、評価の客観性を向上させ、対策時の優先度の判断や、サービスの継続・改修といった経営的意思決定におけるスピードと精度を高めることにもつながります。自組織の脆弱性診断では何を見ているのか？―こう自問してみて心もとなく感じた方は、ぜひ、この二極がカバーできているかを、改めて確認してみてください。

参考情報：

[*1]https://www.npa.go.jp/cyberpolice/detect/pdf/20191128.pdf

# OWASP、API Security Top 10（RC 版）を公開

## API 特有のセキュリティリスクの評価指針として要注目

Column
～コラム～

2019 年 9 月 12 日、OWASP は、API セキュリティに関する 10 大リスクを選定、解説した『OWASP API Security Top 10』の RC 版を公開しました。

API は、アプリケーション間の連携を促進する仕組みとして、モバイル、IoT、クラウド等のアプリケーションで幅広く活用されており、今や「つながる世界」を支える上で欠かせません。しかしながら､適切なセキュリティ対策を怠った場合、攻撃による被害は広範囲におよび、深刻なリスクにつながる可能性があります。たとえば、サプライチェーン攻撃がその典型です。

API の場合、エンドポイントが露出するというその特性上、アプリケーションロジックや、個人識別情報（PII）等守秘性の高い情報が露呈するリスクが高くなります。一方で、SQL インジェクション、CSRF、パスマニピュレーション等のリスクは、従来の Web アプリケーションに比べて低いとされています。

対策を最適化する上で、API 固有の脆弱性やセキュリティリスクを把握することはきわめて重要です。OWASP による今回のドキュメントは、その一助になるものと期待されています。

参考情報：
https://www.owasp.org/images/f/ff/API_Security_Top_10_RC_-_Global_AppSec_AMS.pdf

**表 3：OWASP による API セキュリティ 10 大リスク候補**

| | |
|---|---|
| 1 | Broken Object Level Authorization（オブジェクトレベルでの認可の不備） |
| 2 | Broken Authentication（認証の不備） |
| 3 | Excessive Data Exposure（データの過度な露出） |
| 4 | Lack of Resources & Rate Limiting（リソースの制限、頻度の制限の不足） |
| 5 | Broken Function Level Authorization（機能レベルの認可の不備） |
| 6 | Mass Assignment（一括での割り当て） |
| 7 | Security Misconfiguration（不適切なセキュリティ設定） |
| 8 | Injection（インジェクション） |
| 9 | Improper Assets Management（不適切なアセット管理） |
| 10 | Insufficient Logging & Monitoring（不十分なロギングとモニタリング） |

出典：https://www.owasp.org/index.php/OWASP_API_Security_Project より。日本語訳は当社

**SQAT®（Software Quality Analysis Team）とは**
**～スペシャリスト集団が組織の脆弱性対策をトータルに支援～**

「SQAT®」は、BBSec がご提供する脆弱性診断サービスです。エンジニア、コンサルタント、ホワイトハッカー等から編成された精鋭チームが、あらゆる側面から網羅的な診断を実施。スペシャリストのノウハウを結集して組織の情報システム強化をお手伝いします。お客様は金融機関・インターネット事業者などの民間企業から、官公庁をはじめとする公共機関まで幅広く、これまでに延べ 4,300 組織、22,300 を超えるシステムで利用されています。