SECURITY REPORT

2021 DEC

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

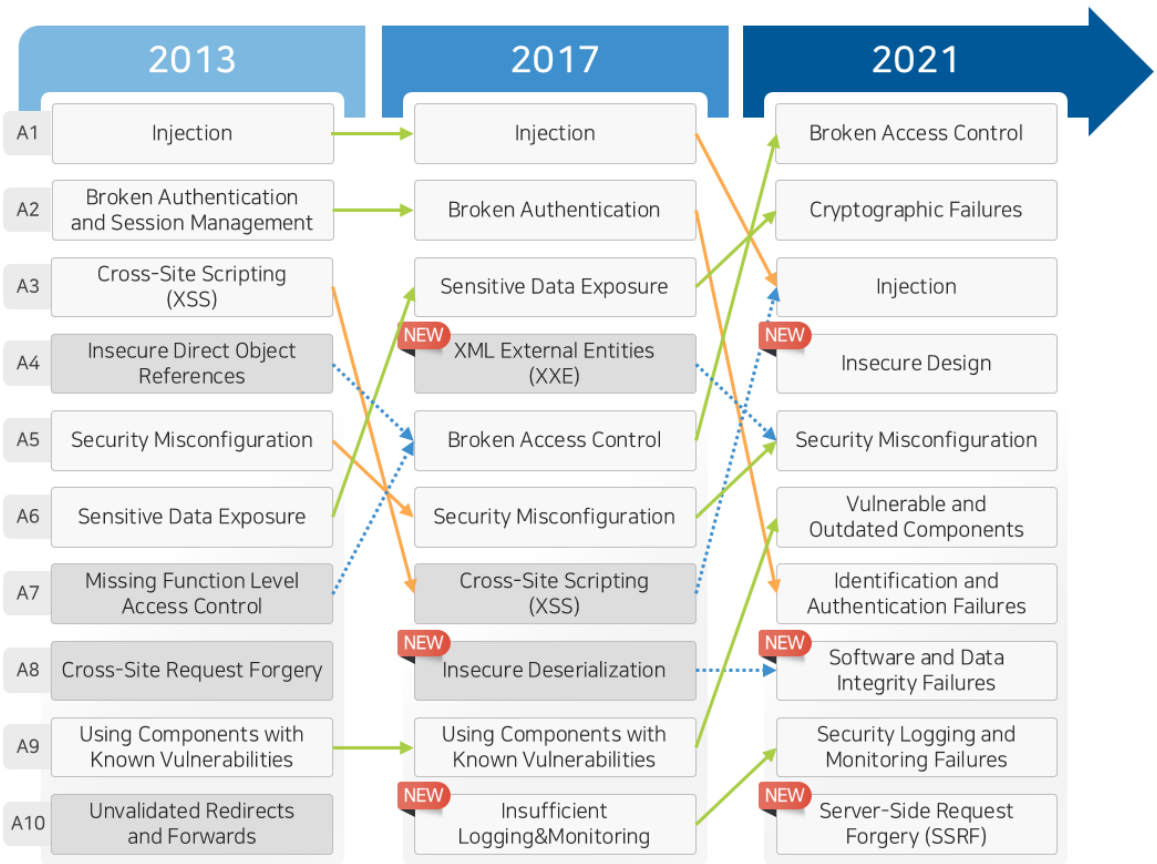
前もって確認するOWASP Top 10 2021（ドラフト）

01. 概要

OWASP(The Open Web Application Security Project)は2021年新たなアプリケーションセキュリティ脅威10個を発表した。

OWASPの場合、主にウェブ環境にて発生しうる脆弱性(情報漏洩、マルウェア及びスクリプト、セキュリティ脆弱性など)を研究し、様々な脆弱性の中で、上位10個の脅威に対して3~4年周期で発表している。今回発表したOWASP Top 10は2017年に発表して以来の4年ぶりで、2004年を始めに今年2021年まで6回の発表があった。

OWASPが変化するIT情報で選定したウェブアプリケーションのセキュリティ脅威は何があるのか確認し、2013年から今までどのようにセキュリティ脅威が変化したか確認してみよう。



【▲ OWASP Top 10カテゴリーの変化(参考：OWASP)】

前もって確認するOWASP Top 10 2021（ドラフト）

分類	2013年	2017年	2021年
基盤	アプリケーションセキュリティ専門7企業、8個のデータセットを基盤	アプリケーションセキュリティ専門企業が提出した40個以上のデータと業界順位調査(500名)を基盤	8個のカテゴリー：データから選択 2個のカテゴリー：業界問い合わせから選択
データ	数百個の企業、数千個のアプリケーションの500,000個以上の脆弱性	・数百個の組織と10万個が超える実際アプリケーションおよびAPIから収集された脆弱性 ・CWEデータを規定された配下集合から収集	・500,000個以上のアプリケーションに対するデータ ・CWEに対する制限なしデータを収集
優先順位	悪用の可能性、検知可能性、影響の拡散及び推定値を基盤としてリストを作成し、優先順位を決める	攻撃利用の可能性、検知可能性及び影響度を推定した値のデータによって選別し、優先順位を指定	・悪用の可能性と影響に対するデータを使用 ・発生率で優先順位指定
データセットの数	-	約30CWE	約400CWE

【▲ OWASP変化(参考：OWASP)】

2013年から2017年のバージョンアップデートでAPI脆弱性が話題になった。
2017年のOWASPデータにAPIを含める理由は、最新アプリケーションにはAPIを繋ぐ多くのクライアントアプリケーションが含まれている場合が多いが、APIは大体脆弱で組織はこのような問題に対して気を付ける必要があるからである。

2017年から2021年のバージョンアップデートでCWEデータを30から400に増やした。
CWEデータ収取方法の変化により、カテゴリーの構成方法も変更した。
2017年OWAPからは発生率別にカテゴリーを決めて可能性を判断した後、数十年間の利用可能性、検知可能性及び技術的影響による経験を基にして順位を付けた。

2021年からは悪用の可能性と影響に対するデータを使用する。

前もって確認するOWASP Top 10 2021（ドラフト）

02. OWASP TOP 10 2021

OWASP TOP 10 2021年からは三つの項目が新たに追加され、4つの項目からカテゴリーが新たに割り当てられた。また、OWASPからは2021年のOWASP TOP 10はデータを基に作成(Data-driven)しているが単純にデータ中心にしたものではないと明らかにした。

OWASPから発表した脆弱性は、下記の表のようなデータ要素で分けられる。それぞれの値と内容は次になる。

Data Factors	説明
CWEs Mapped	それぞれの脆弱性項目にマッピングされたCWE数
Incidence Rate	インシデント件数からCWEに脆弱なアプリケーションの比率
(Testing) Coverage	特定CWEに対する全ての組織がテストしたアプリケーションの比率
Weighted Exploit	CWEにマッピングされたCVEからCVSSv2及びCVSSv3点数を10点に換算したExploit点数
Weighted Impact	CWEにマッピングされたCVEからCVSSv2及びCVSSv3点数の影響度を10点に換算した点数
Total Occurrences	CWEがカテゴリーにマッピングされたもので発見された総アプリケーションの数
Total CVEs	カテゴリーにマッピングされたCWEにマッピングされたNVD DBの総CVE数

【▲ OWASP Top 10 Data Factors(参考：OWASP)】

前もって確認するOWASP Top 10 2021（ドラフト）

1) A01- Broken Access Control(アクセス制御の不備)

CWEs Mapped	Max Incidence	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences	Total CVEs
34	55.97%	3.81%	94.55%	47.22%	6.92	5.93	318,487	19,103

OWASP Top 10 - 2017にA05に位置したBroken Access Control(アクセス制御の不備)が4段階あがり1位(A01)に移動した。
過去には一つのサービスもしくは、システムで構成されたアプリケーション開発であったが、現在は相互独立的な構成で分割され開発される場合が多くなっている。
従って、これまでアクセス統制として一つのサービスからのアクセスとしていたが、機能が分割されることでアクセス統制が複雑化したため、1位に移動したとみられる。
また、34個のマッピングされたCWEは、他の項目に比べ多くのアプリケーションから脆弱性が発見されたことで順位が変更した思われる。

2) A02 - Cryptographic Failures(暗号化の失敗)

CWEs Mapped	Max Incidence	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences	Total CVEs
29	46.44%	4.49%	79.33%	34.85%	7.29	6.81	233,788	3,075

OWASP Top 10 - 2017にはA03に位置していたSensitive Data Exposure(機密データの露出)項目がCryptographic Failures(暗号化の失敗)の名前に変わり、当該項目は1段階あがり2位(A02)に移動した。
2017年に存在した機密データの露出は根本的な原因が存在するわけではなく、色々な分野から広範囲に発生する事象だと判断していた。
2017年以降、データ暗号化に関する問題が多く、掲載順位が変更されたとみられる。

前もって確認するOWASP Top 10 2021（ドラフト）

3) A03 - Injection (インジェクション)

CWEs Mapped	Max Incidence	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences	Total CVEs
33	19.09%	3.37%	94.04%	47.90%	7.25	7.15	274,228	32,078

OWASP Top 10 – 2017にはA01に位置していたInjection(インジェクション)が2段階下落して3位(A03)に移動した。
2017年に存在していたA1 – InjectionとA7 – Cross Site Scripting(XSS)が統合され、計33個のCWEがマッピングされていて、アプリケーションからはBroken Access Controの2番目に多い脆弱性として確認された。
Injectionは過去からSQL、NoSQL、OSコマンド、ORM(Object Relation Mapping)、LDAP、ELE(Expression Languages)、OGNL(Object Graph, Navigation Libarary)インジェクションなど、様々な脆弱性が存在していて、Cross Site Scripting脆弱性が統合されることによって未だに危険性を持っている脆弱性だと判断されるため、3位に位置したと思われる。

4) A04 - Insecure Design (安全が確認されない不安な設計)

CWEs Mapped	Max Incidence	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences	Total CVEs
40	24.19%	3.00%	77.25%	42.51%	6.46	6.78	262,407	2,691

Insecure DesignはOWASP Top 10 – 2017には存在していなかった新しい項目である。
企画段階からアプリケーション設計のセキュリティ事項を守ることを意味し、設計過程から発生するセキュリティ欠陥を指す。
設計が間違っているアプリケーションはセキュリティテストで発見された問題は簡単に処置することが難しく、危険性を持ったまま運用する場合が多いため、当該の項目が新しく登場したと思われる。

前もって確認するOWASP Top 10 2021（ドラフト）

5) A05 - Security Misconfiguration (セキュリティ設定のミス)

CWEs Mapped	Max Incidence	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences	Total CVEs
20	19.84%	4.51%	89.58%	44.84%	8.12	6.56	208,387	789

OWASP Top 10 – 2017にはA06に位置していたSecurity Misconfiguration(セキュリティ設定のミス)項目がA04のXML External Entities(XXE)項目と統合され、段階上昇して5位(A05)に移動した。
90%が間違った構成でテストが行われリリースされたもの、間違って構成されたHTTPヘッダーおよび敏感な情報が含まれているエラーメッセージでセキュリティホールが知られる可能性があるものを指している。
安全に設計されたアプリケーションを開発していてもテスト及びデバッグのために設定するオプションを間違う場合が多数ある。
このような理由で脆弱性の順位が一段階上昇したとみられる。

6) A06 - Vulnerable and Outdated Components (脆弱で古くなったコンポーネント)

CWEs Mapped	Max Incidence	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences	Total CVEs
3	27.96%	8.77%	51.78%	22.47%	5.00	5.00	30,457	0

OWASP Top 10 – 2017にはA09に位置していたUsing Components with Known Vulnerabilities(既知の脆弱性を持つコンポーネントの使用)項目がVulnerable and Outdated Components(脆弱で古くなったコンポーネント)に名前が変更されて当該項目は三段階上昇して6位に移動した。
オープンソースを基盤とした多様なライブラリとコンポーネントが繋がっているアプリケーションの場合、提供されるライブラリとコンポーネントに知られている脆弱性が存在する可能性があり、既知の脆弱性が存在するコンポーネントを使用することでソフトウェアに脆弱性が含まれる可能性がある。最近ソフトウェア開発をモジュール化して行うことが多いため、脆弱性順位が変更されたとみられる。

前もって確認するOWASP Top 10 2021（ドラフト）

7) A07 - Identification and Authentication Failures (識別と認証の失敗)

CWEs Mapped	Max Incidence	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences	Total CVEs
22	14.84%	2.55%	79.51%	45.72%	7.40	6.50	132,195	3,897

OWASP Top 10 – 2017にはA02に位置していたBroken Authentication(認証の不備)項目がIdentification and Authentication Failures(識別と認証の失敗)に名前が変わり5段階下落し7位(A07)に移動した。
当該の項目は現在開発されるソフトウェア開発フレームワークの可用性が増えたとによって順位が下落したと思われる。

8) A08 - Software and Data Integrity Failures (ソフトウェアとデータの整合性の不具合)

CWEs Mapped	Max Incidence	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences	Total CVEs
10	16.67%	2.05%	75.04%	45.35%	6.94	7.94	47,972	1,152

OWASP Top 10 – 2017には存在しなかった新しい項目で、2017年に存在したInsecure Deserialization(安全でないデシリアライゼーション)が含まれている。
整合性を証明しないソフトウェアアップデート、重要データ、そしてCI/CDパイプラインに関する内容でCVE/CVSSデータの中で重大な影響を受けた一つではあるが位置の変化はない項目である。

前もって確認するOWASP Top 10 2021（ドラフト）

9) A09 - Security Logging and Monitoring Failures (セキュリティログとモニタリングの失敗)

CWEs Mapped	Max Incidence	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences	Total CVEs
4	19.23%	6.51%	53.67%	39.97%	6.87	4.99	53,615	242

OWASP Top 10 – 2017にはA10に位置していたInsufficient Logging & Monitoring(不十分なロギングとモニタリング)項目が新しい名前に変わった。当該の項目はセキュリティ業界の問い合わせで上位を占めており、OWASPでも一段階上昇して9位(A09)に移動した。
当項目は既存よりも多い種類の問題を含めるように拡張された。ロギングとモニタリングはセキュリティテストが難しいくCVE/CVSSデータにはあまり出ていない。

10) A10 - Server Side Request Forgery (サーバーサイド・リクエスト・フォージェリ)

CWEs Mapped	Max Incidence	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences	Total CVEs
1	2.72%	2.72%	67.22%	67.22%	8.28	6.72	9,503	385

OWASP Top 10 – 2017には存在していなかった項目で、セキュリティ業界の問い合わせで上位を占めており、新たに追加された項目である。
当項目はデータから「脆弱性及び影響潜在性」は均以上の等級を取り、平均的なテスト範囲から較的に低い発生率をみせた。
このことから、現在のデータがきちんと存在しないと思われるが、ウェブアプリケーションファイアウォール(WAF)、ファイアウォール、またはネットワークACLが保護しているシステムをSSRFを利用して攻撃することが可能であり、関連するシナリオが存在して多様な脆弱性が発見される可能性があるため新たに追加されたとみられる。

前もって確認するOWASP Top 10 2021（ドラフト）

03. 結論

今まで2013年から2021年まで変化したOWASP Top 10について調べ、2021年に発表される項目について簡単に確認してみた。
現在OWASPから公開されたセキュリティ脅威Top 10はDRAFT FOR PEER REVIEWバージョンで今後検討をして最終バージョンを公開されると予想される。
従って、今後に発表されるOWASP Top 10 2021最終バージョンを確認する必要がある。

04. 参考資料

[1] OWASP Top 10:2021 (DRAFT FOR PEER REVIEW)
https://owasp.org/Top10/