BLACKDUCK®

ソフトウェア脆弱性スナップショット

web およびソフトウェア・アプリケーションによく見られる 10 の脆弱性に関する 3 年間の分析

CyRC

ブラック・ダック セキュリティ・テスト・サービスと
ブラック・ダック サイバーセキュリティ・リサーチセンターによる分析

目次

概要

本「ソフトウェア脆弱性スナップショット」レポートを作成するにあたり、ブラック・ダック サイバーセキュリティ・リサーチ・センターとブラック・ダック セキュリティ・テスト・サービスのコンサルタントは、商用ソフトウェア・システムおよびアプリケーションに対して 3 年間にわたって実施したテストで得た匿名化データを使用しました。

ブラック・ダックのテストにより、web およびソフトウェア・アプリケーションのセキュリティ上で重大な課題である、常習的に発生している脆弱性が明らかになりました。特に、最も多い脆弱性は以下に関連するものでした。

- 情報流出 / 漏えいとプライバシー
- 設定のミス
- 不十分なトランスポート層の保護

このテストは、脆弱なサードパーティ・ライブラリによってもたらされる目下の危険性を強調するとともに、ソフトウェアの 90% 以上にオープンソースが使用されるというソフトウェア開発環境において、堅牢なソフトウェア・サプライチェーンのセキュリティの必要性を明らかにします。以下のデータから、基本的な静的解析のみに頼ることなくアプリケーション・セキュリティ・テストを拡張することの重要性も分かります。

ソフトウェア・セキュリティ・プログラムの責任者は、ソフトウェアのリスクについての理解を深めることにより、セキュリティ対策の戦略的な改善計画を立てることができます。戦術的観点からセキュリティ・プログラムに関与している方は、本レポートの情報を使用することにより、サードパーティの支援の下でセキュリティ・テスト拡張の必要性を主張するための論拠を得ることができます。

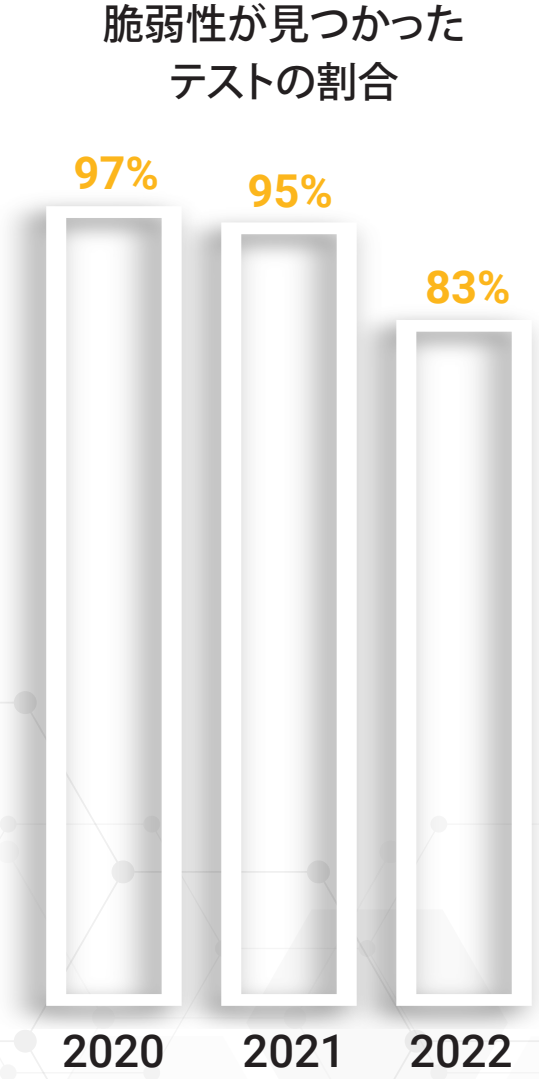
テストで見つかったセキュリティの問題

2020 年には、テストの 97% で脆弱性が見つかりました。2021 年には 95% に下がり、2022 年にはさらに 83% まで低下しました。収集された 3 年分のデータを通して、テストの 92% でターゲット・アプリケーションに脆弱性が見つかりました。

開発チームがエラーのないコードを書く能力が高まっており、コード・レビュー、自動テスト、継続的インテグレーションなどのプラクティスがプログラミングで発生しがちなミスの削減に役立っているため、全体の脆弱性が一貫して減少を続けていることが分かります。

プログラミング言語や統合開発環境（IDE）の進歩により、重大な問題になる前にミスを発見できるビルトインのチェックやツールを利用できるようになりました。一般的なオープンソース・プロジェクトの場合、多くのコミュニティでコードの精査が強化され、品質基準が高まっています。

残念ながら、これはあまり一般的ではない、あるいは古いオープンソース・プロジェクトには当てはまりません。中には、2022 年に保守管理されていた Java および JavaScript のオープンソース・プロジェクトのうち、現在保守されておらず、脆弱性やエクスプロイトに晒されているものが 20% 近くあるという報告もあります。



重大度が高および緊急の脆弱性

3 年間全体で、テストの 27% に重大度が高の脆弱性が見つかり、6.2% に重大度が緊急の脆弱性が見つかりました。クロスサイト・スクリプティング（XSS）を許してしまう脆弱性は、一貫して、ブラック・ダックのテストで見つかる重大度が高の脆弱性の上位にランクインしています。同様に、重大度が緊急の脆弱性の上位にランクインしている SQL インジェクションは、2020 年～ 2022 年にかけて常にトップでした。

年別に見ると、重大度が高の脆弱性は 2021 年と 2022 年を比べるとわずかに増加（20% → 25%）していますが、2020 年と 2022 年を比べれば減少（30% → 25%）しています。重大度が緊急の脆弱性は 2022 年（6.7%）が、2021 年（4.5%）と 2020 年（6.1%）よりも高くなりました。

重大度が中～緊急の多くの脆弱性を発見するには、多層的なテストが必要

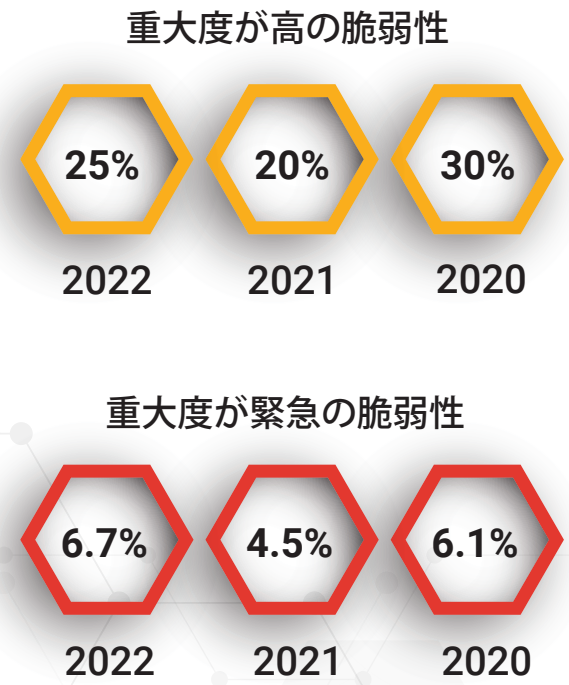
この数字から、重大度が高および緊急の脆弱性がここ数年増加し続けていること、2022 年に最高を記録したことが分かります。2022 年に報告された CVE の 80% が重大度中または高のいずれかで、16% が緊急と判定されました。開発チームが全体的な脆弱性の数を減らしてはいるものの、重大度が中～緊急の多くの脆弱性を発見するためにペネトレーション・テストなどの、より堅牢なテストが必要であることがこのデータから読み取れます。

	2022	2021	2020
緊急	28%	54%	77%
高	38%	46%	63%
中	60%	64%	72%

図 1：再テストで見つかった脆弱性を元のテストで見つかった脆弱性と比較したときの減少率

図 1 は、動的テスト（何らかの種類のペネトレーション・テスト、動的アプリケーション・セキュリティ・テスト（DAST）など）が静的アプリケーション・セキュリティ・テスト（SAST）を補完するのに効果的であることを示しています。再テスト（特定の修正が適用されたことを簡単に確認すること）のサンプリングによると、脆弱性が発見された後、各年とも、重大度が緊急、高、中の脆弱性が減少していることが分かります。例えば、2022 年には、重大度が中の脆弱性は 60% 減少し、高は 38%、緊急は 28% 減少したことが分かりました。

2020 年～ 2022 年の重大度が高および緊急の脆弱性



重大度の定義

重大度のレベルは、脆弱性がネットワーク・セキュリティにもたらすリスクを CVSS v3 の尺度で評価したものです。重大度が緊急の脆弱性は、CVSS スコアが 9.0 ～ 10.0 で、エクスプロイトまたは概念実証コードが公開されているか、積極的に悪用されているものです。これには、コマンド、コード、SQL インジェクション・エクスプロイトなどが含まれます。

重大度が高の脆弱性は、CVSS スコアが 7.0 ～ 8.9 のもの、通常、重大度が緊急の脆弱性よりも悪用が困難なものです。それでもなお、リスクに晒されているアプリケーション / システムのビジネス上の重要性や脅威の現状などの要因を考慮して脆弱性をレビューし、迅速に対処する必要があります。

ほんの数秒で数千ものシステムを攻撃できる自動エクスプロイト・ツールを使用する攻撃者が増えているため、高リスクおよび緊急リスクの脆弱性が検出された場合は、一刻も早い修正が必要です。報告された脆弱性の半数以上が、公開から 1 週間以内に悪用されているからです。

デプロイされたアプリケーションのセキュリティや脆弱性の問題は、組織（またはその顧客）の業務を中断させる可能性があるだけでなく、SDLC（ソフトウェア開発ライフサイクル）全体、ひいてはソフトウェア・サプライチェーンに影響を与えることによって、連鎖的に深刻化する傾向があります。

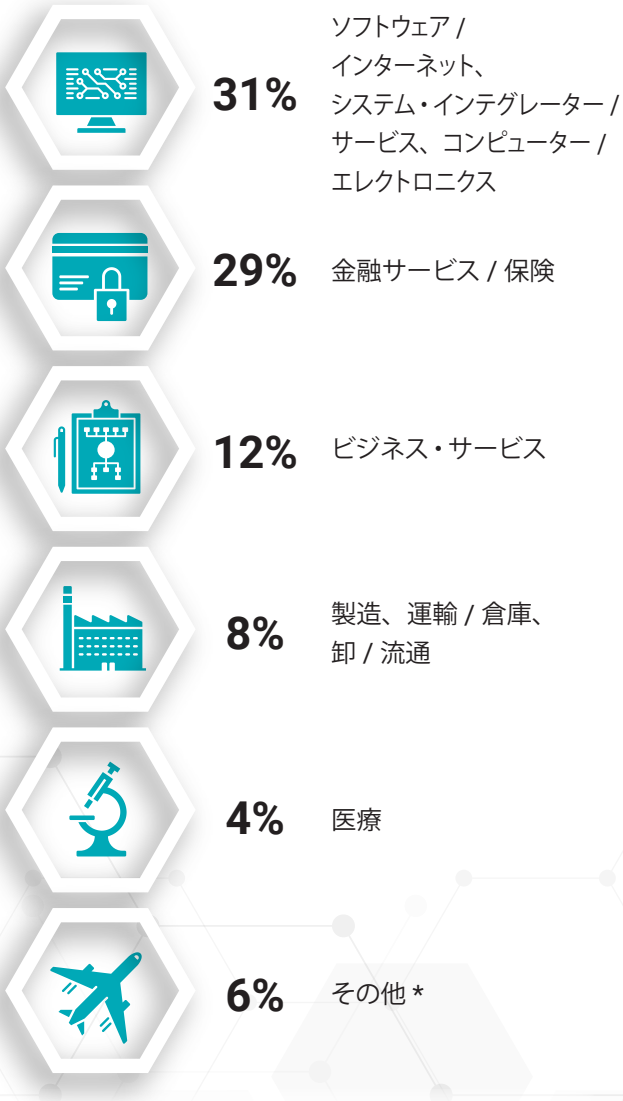
実際、ブラック・ダックのレポート「世界の DevSecOps の現状 2023」では、回答者の 80% 以上が、2022 ～ 2023 年の間に重要なセキュリティ / 脆弱性の問題に対処する必要性があったため組織のソフトウェアの納期に影響が出たと回答しています。

ブラック・ダックのセキュリティ・テスト・サービスについて

開発チームはますます複雑になるソフトウェアを
かつてないスピードで開発することを求められていますが、
スキルのある熟練した人材は不足しています。

ブラック・ダックのセキュリティ・テスト・サービスを利用するお客様は、業界や組織は違ってもテストのカバレッジを補完したい、という共通のニーズをお持ちです。開発チームはますます複雑になるソフトウェアをかつてないスピードで開発することを求められていますが、特にソフトウェア・セキュリティに関しては、スキルのある熟練した人材が不足しています。

調査した業種の内訳



* 旅行 / 娯楽、教育、エネルギー / 公益事業、公共部門を含みます。

本レポートでは、各業界の 3 年間（2020 年～ 2022 年）の平均を示します。

ソフトウェア・セキュリティに影響を与える戦略、ツール、プラクティスに関するブラック・ダックのレポートによれば、回答者 1,000 人のうち 33% 以上が、主な障害としてセキュリティ・トレーニングが不足していることを挙げており、これにセキュリティ担当者の不足（31%）が僅差で続いています。また、同レポートの回答者の 33% が、外部のコンサルタントが組織のセキュリティ・テストに役立っていると回答しています。

サードパーティのセキュリティ・テスターと契約して、組織のセキュリティ体制について先入観にとらわれない見解を得ることは、非常に重要です。実際、「セキュア開発成熟度モデル（BSIMM）」レポートによれば、BSIMM プロジェクトに参加した組織の 88% が外部のペネトレーション・テスターを活用し自社のセキュリティ・アクティビティを補完しています。これらのテストによって、組織内部のテストでは見つけることのできなかった問題を検出でき、場合によっては組織のセキュリティ・プラクティスの弱点が浮き彫りになる可能性もあります。

自社のセキュリティ・テストのカバレッジが十分だと思えたとしても、テストを検証し、社内のセキュリティ管理が正常に機能しているかどうかを確認したい場合もあります。あるいは、第三者評価を義務付けている規制基準や顧客などの要件を満たすべき場合もあります。例えば、PCI DSS 4.0 の要件 11 は、定期的なペネトレーション・テストの実施を特に義務付けています。この要件は、正式な監査が必要な加盟店に適用され、すべてのサービス・プロバイダーにも適用されます。

米国の医療保険の携行性と責任に関する法律（HIPAA）は、医療従事者に対し、情報の機密性とセキュリティを確保する技術的保護手段を使用して、電子的に保存された医療情報を保護することを義務付けています。HIPAA は、特にペネトレーション・テストや脆弱性スキャンを求めてはいませんが、リスク分析は義務付けています。そのため、対象事業体は事実上、セキュリティ対策をテストする必要があります。

HIPAA の「評価」を規定するセクションでは、特に「定期的な技術的評価と非技術的評価」の方法について言及しています。また、米国国立標準技術研究所（NIST）は、HIPAA に関するガイダンスにおいて、それが合理的かつ適切な場合に、技術的評価要件を満たす上で推奨される方法として外部および内部、あるいはその両方のペネトレーション・テストを挙げています。

金融サービスの分野では、米国の金融業規制機構（FINRA）が金融機関のサイバーセキュリティ・ルールを策定し、定期的または主要な事象（企業のインフラストラクチャやアクセス制御に大きな変更があった場合など）の後に、ペネトレーション・テストを実施することを推奨しています。2022 年より、2023 年 6 月に施行期限を迎えるグラムリーチブライリー法（GLBA）は、金融機関に対し、セキュリティ・アクティビティの一環として毎年ペネトレーション・テストと脆弱性スキャンを実施することを明示的に求めています。

ブラック・ダックのレポートでは（回答者：1,000 人）

33% 以上

主な障害として
セキュリティ・トレーニングの不足を
挙げている割合

31% 以上

セキュリティ担当者の不足を
問題として挙げている割合

ブラック・ダックのセキュリティ・テストの詳細

ブラック・ダックのテストは、ブラックボックス・テストとグレーボックス・テストの両方を取り入れ、実際の攻撃者と同じような方法で動作中のアプリケーションを探索して脆弱性を特定し、トリアージを実施して必要に応じて修正できるようにすることを目的としています。ブラックボックス・テストとは、外部の視点からターゲットのセキュリティ状態にアプローチする手法です。一方のグレーボックス・テストとは、資格情報を持つ認証されたユーザーをシミュレートする手法で、本質的には、より深い内部情報を使用したブラックボックス・テストと言えます。テスト対象は、ほとんどが web システム / アプリケーション（82%）とモバイル・システム / アプリケーション（13%）で、残りの少数はネットワーク（3.0%）とソースコード（2.0%）でした。

ペネトレーション・テスト

テスト全体の 66% を占めていたのはペネトレーション・テスト（ペンテスト）でした。ペネトレーション・テストとは、コンピュータ・システムのセキュリティを評価するために実行される公認の模擬攻撃です。ペネトレーション・テスターは、攻撃者と同じツール、技術、プロセスを使用してシステムの弱点を発見し、それがビジネスに与える影響を実証します。ペネトレーション・テストでは、認証済みと未認証の立場からの攻撃、およびさまざまなシステムの役割からの攻撃に耐えられる堅牢性があるかどうかを検査します。

多くの場合、業界の規制や標準に準拠するには外部ペンテストが必要とされます。外部ペンテストには、自社のセキュリティ態勢について先入観のない視点が得られるだけでなく、外部の攻撃者に悪用される可能性のある潜在的な脅威や脆弱性を正確にシミュレーションできるなどの利点もあります。

最適なリスク管理には、ペネトレーション・テストに対する包括的なアプローチが不可欠です。ブラック・ダックのペネトレーション・テストには以下のようなターゲットを含めることができます。

- web アプリ：テスターは、セキュリティ対策の有効性を検証し、隠れた脆弱性、攻撃パターン、web アプリの侵害につながりそうなその他の潜在的なセキュリティ・ギャップを探します。
  - モバイル・アプリ / デバイス：テスターは、自動テストと拡張マニュアル・テストの両方を使用して、モバイル・デバイス上で実行されるアプリケーションのバイナリと対応するサーバーサイドの機能、これらの脆弱性を探します。サーバーサイドの脆弱性には、セッション管理、暗号の問題、認証と認可の問題、その他の一般的な web サービスの脆弱性が含まれます。アプリケーション・バイナリの脆弱性には、認証と認可の問題、クライアント側のトラストの問題、セキュリティ対策の設定ミス、クロスプラットフォーム開発フレームワークの問題などが含まれます。
  - ネットワーク：このテストでは、外部ネットワークおよびシステムに存在するクリティカルな脆弱性を特定します。専門家は、暗号化されたトランスポート・プロトコル、SSL 証明書のスコープの問題、管理サービスの使用などのテスト・ケースを含むチェックリストを採用しています。この 3 年間に実施したペネトレーション・テストのうち、ネットワーク・セキュリティに関するペネトレーション・テストは約 3%（2.7%）でした。

3 年間に実施したテストの種類

66%
ペネトレーション・テスト

15%
DAST

13%
MAST

- API：「OWASP API Security Top 10」のリストを網羅するため、自動テストとマニュアル・テストの両方が使用されます。テスターが探すセキュリティ・リスクと脆弱性には、オブジェクト・レベルの認可の不備、ユーザー認証、過度なデータの曝露、リソース / レート制限の欠如などがあります。

攻撃者のように考えて行動する専門家のペンテスターは、スクリプト化されたルーチンに従った自動化されたテスト・ソリューションでは不可能な方法でデータを分析して攻撃対象を絞り、システムや web サイトをテストすることで、必要とする人間的な要素を取り入れます。また、脆弱性の種類によっては自動テスト・ツールでは検出が難しいものもあり、これらは人間の手で検出するしかありません。例えば、安全でないオブジェクト直接参照（IDOR）の脆弱性が存在すると、攻撃者は権限のないデータにアクセスできますが、この脆弱性を効果的に検出するには人間によるマニュアル・テストが不可欠です。

DAST

この 3 年間に実施したテスト中、DAST（動的アプリケーション・セキュリティ・テスト）が占める割合は 15% でした。DAST は、実行中のアプリケーションを調査するアプリケーション・セキュリティ（AppSec）テストの手法の 1 つですが、テスターはアプリケーション内部のやりとりやシステムレベルの設計について何の事前知識も持たず、ソース・プログラムへのアクセス権や可視性なしにテストを実行します。この種のブラックボックス・テストでは、外部からアプリケーションを見て、その実行状態を調べ、テスト・ツールによるシミュレートされた攻撃への反応を観察します。このような攻撃に対するアプリケーションの反応は、アプリケーションが脆弱かどうか、悪意のある攻撃を実際に受けた際に影響を受けやすいかどうかを判断するのに役立ちます。

その目的は、想定外（であることにより、攻撃者がアプリケーションを危殆化させるために利用する可能性がある）の結果を発見することです。DAST ツールは、アプリケーションやソースコードに関する内部情報を持たないため、外部のハッカーとまったく同じように、アプリケーションについて限られた知識と情報を元に攻撃します。

DAST ソリューションでは、他のセキュリティ・テストでは発見しづらい実行時の脆弱性を発見できます。これらの脆弱性には、認証およびサーバー設定エラー、コード・インジェクション、SQL インジェクション、クロスサイト・スクリプティング・エラーなどがあります。

前述したように、ソフトウェア・セキュリティの全体像を把握するには、人間の介在が必要になることがあります。ブラック・ダックの DAST 評価には手動テストが含まれ、これによって認証とセッション管理、アクセス制御、情報漏えいに関係する一部の脆弱性など、既製のツールでは通常見つけることのできない脆弱性を検出します。

MAST

この 3 年間に実施したテスト中、13% を占めていたのがモバイル・アプリケーション・セキュリティ・テスト（MAST）でした。ブラック・ダックのモバイル・アプリケーション・セキュリティ・テストは、モバイルのクライアント側コード、サーバー側コード、サードパーティ・ライブラリの解析に重点を置いており、ソースコード不要でモバイル・アプリケーションのセキュリティ脆弱性を体系的に発見し修正します。ブラック・ダックは、独自の静的解析と動的

ソフトウェア・セキュリティの
全体像を把握するには、
人間の介在が必要になることが
あります。

解析のツールを組み合わせて脆弱性を発見し、各テスト対象アプリケーションのリスク・プロファイルに基づいてテスト・レベルを調整することでさまざまな深さの解析を提供します。

モバイル・アプリの普及にもかかわらず、ほとんどの開発チームとセキュリティ・チームはモバイル・セキュリティへの取り組みが遅れています。NowSecure の MobileRiskTracker の統計によれば、アプリストアで公開されているモバイル・アプリの 85% に高リスク脆弱性が 1 つ以上あるか、OWASP アプリケーション・セキュリティ検証標準の 1 つ以上の要件に違反しています。さらに、70% が個人情報を漏えいしており、GDPR/CCPA やその他のプライバシー規制に違反している可能性があります。

脆弱性の概要

「OWASP（Open Web Application Security Project）Top 10」と「CWE（共通脆弱性タイプ一覧）Top 25」は、最も一般的なセキュリティ脆弱性のリストと最も危険性の高いセキュリティ脆弱性のリストです。いずれも、セキュリティ研究者、脆弱性データベース、インシデント報告などを含むさまざまな情報源から得られたデータを元にしています。

OWASP Top 10 は、web アプリケーションに対する最も深刻なセキュリティ・リスクについて、多数の開発者および web アプリケーション・セキュリティ・チームによるコンセンサスを反映したリストです。CWE Top 25 は、MITRE が SANS Institute と共同で作成した、25 の最も危険な脆弱性のリストです。OWASP では注意喚起文書と位置付けていますが、多くの組織がこれらのリストをセキュリティ対策の有効性を測る上で、セキュリティのデファクト・スタンダードとして使用しています。

OWASP Top 10 が web アプリケーション特有のセキュリティ・リスクに注目しているのに対し、CWE Top 25 はソフトウェアの脆弱性とそれに関連する共通脆弱性タイプの一覧に重点を置いています。

図 2 に示す通り、2 つのリストには、用語が異なるとはいえ、重複があります。例えば、OWASP のカテゴリ「A05:2021—セキュリティの設定ミス」は、CWE Top 25 の CWE-798（ハードコードされた認証情報の使用）や CWE-276（不適切なデフォルトパーミッション）など、さまざまな弱点に関連しています。

「フィンガープリンティング」（情報を得るために web アプリケーションに探りを入れること）は、OWASP Top 10 のいずれのカテゴリにも直接言及されてはいないものの「セキュリティ・ログとモニタリングの失敗」か「アクセス制御の不備」のどちらかに分類できるでしょう（ここでは前者に分類しました）。同様に、フィンガープリンティングに関連する最も近い CWE は恐らく「情報漏えい（CWE-200）」でしょう。図 2 の 1 行目、4 行目、6 行目、9 行目から分かるように、ブラック・ダックのテストで多く見つかった問題は情報流出 / 漏えいのさまざまな側面に絡むものでした。

アプリストアで公開されている
モバイル・アプリの 85% が
1 つ以上の高リスク脆弱性を
抱えています。

ブラック・ダックの 2022 年脆弱性カテゴリトップ 10	2021 年の順位	2020 年の順位	関連する OWASP Top 10/ Mobile Top 10 カテゴリ	関連する CWE
1. 情報流出：情報漏えい	1	1	A01:2021—アクセス制御の不備	情報漏えい（CWE-200）。その他のアクセス制御管理に関する問題には、不正な認証（CWE-863）とサーバサイドのリクエストフォージェリ（CWE-918）が含まれる。
2. サーバー設定のミス	2	2	A05:2021—セキュリティの設定ミス	CWE-798、CWE-276 などのセキュリティの設定ミス。
3. 不十分なトランスポート層の保護	3	3	A05:2021—セキュリティの設定ミス M3：安全でない通信	CWE-798、CWE-276 などのセキュリティの設定ミス。
4. 不十分な認可	4	4	A01:2021—アクセス制御の不備 M6：安全でない認可制御	情報漏えい（CWE-200）。その他のアクセス制御管理に関する問題には、不正な認証（CWE-863）とサーバサイドのリクエストフォージェリ（CWE-918）のが含まれる。
5. アプリケーション設定のミス	9	9	A05:2021—セキュリティの設定ミス	CWE-798、CWE-276 などのセキュリティの設定ミス。
6. アプリケーション・プライバシーの失敗	5	5	A02:2021—暗号化の失敗	情報漏えい（CWE-200）。信頼できないデータのデシリアライゼーション（CWE-502）。
7. 認証：不十分な認証	8	8	A07:2021—識別と認証の失敗	CWE-287、CWE-306 などの不適切な / 欠落した認証
8. コンテンツ・スプーフィング / コンテンツ・インジェクション	6	6	A03:2021—インジェクション	SQL インジェクション（CWE-89）、コマンド・インジェクション（CWE-78、CWE-77）、コード・インジェクション（CWE-94）、クロスサイト・スクリプティング（CWE-79）。
9. フィンガープリンティングの影響の受けやすさ	7	7	A09:2021—セキュリティ・ログとモニタリングの失敗	情報漏えい（CWE-200）。
10. クライアント側 / クロスサイト・スクリプティング攻撃への曝露	トップ 10 入りしていない	10	A03:2021—インジェクション	クロスサイト・スクリプティング（CWE-79）、クロスサイト・リクエスト・フォージェリ（CWE-352）。

図 2：ブラック・ダックの脆弱性カテゴリトップ 10

セキュリティの問題の詳細

図 2 に示すように、脆弱性カテゴリの順位はここ数年大きく変わっていません。興味深い例外は、「アプリケーションの設定ミス」で、前の 2 年間は 9 位だったにもかかわらず 2022 年に 5 位になりました。

設定ミスは、アプリケーション、ブラウザ、ネットワーク、オペレーティング・システム、サーバーで発生する可能性があります。例えば、2022 年、オーストラリアの大手通信会社である Optus では 970 万人の顧客の個人情報が流出するという深刻な情報漏えいを経験しました。ファイアウォールの設定ミスによってサードパーティの請負業者が顧客の機密データにアクセスできる状態になっていたことが漏えいにつながりました。

一般に、設定ミスの問題の最も一般的な原因はヒューマン・エラーです。組織はアプリケーションやデプロイメント・スクリプトを十分に検証できず、攻撃に対して脆弱なままになっています。テスト手順中に設定を変更したまま、安全な設定に戻していないこともあります。新しいハードウェアやソフトウェアが組織のセキュリティ要件を満たすかどうかを適切にテストしていない場合もあります。

「アプリケーションの設定ミス」の順位が急に上がったことは、1 つのセキュリティ・テスト・ツールに頼るのではなく、複数のセキュリティ・テスト・ツールが必要であることを示しています。いくら組織がコーディングの脆弱性の全体的な数を減らすことに成功していたとしても、特に実行時環境に関しては単一のテスト・ツールに頼るべきではありません。実行中のアプリケーションの設定ミスなどの問題を発見するには、広範なテスト・ツールが必要なのです。

2022 年のテストで見つかった脆弱性カテゴリのトップ 10 について以下に述べます。

1. **情報流出（情報漏えいとも呼ぶ）。**このセキュリティ問題は、機密情報が権限を持たない者に漏えいした場合に発生します。例えば、何らかのセキュリティの設定ミスによって web サイトからユーザー名、財務情報などのユーザーに関する情報が漏えいするような場合です。この 3 年間のテストで見つかった全脆弱性のうち平均 19% が情報漏えいの問題に直接関連していました。

   OWASP チームでは、情報流出を「A01:2021—アクセス制御の不備」カテゴリに分類し、このカテゴリに該当する脆弱性は他のどのカテゴリよりも多いと指摘しています。「アクセス制御の不備」に属する代表的な脆弱性としては、「認可を受けていない者への機密情報の露出」、「送信データへの重要な情報の挿入」、「クロスサイト・リクエスト・フォージェリ」などがあります。

この 3 年間のテストで見つかった
全脆弱性のうち平均 19% が
情報漏えいの問題に
直接関連していました。

2. **サーバー（セキュリティ）の設定ミス。**OWASP の「A05:2021—セキュリティの設定ミス」カテゴリに属する「サーバーの設定ミス」は、この 3 年間のテストで見つかった脆弱性のうち平均 18% を占めていました。当社の結果はサーバーの設定ミスに焦点を当てているものの、セキュリティの設定ミスは、ネットワーク・サービス、プラットフォーム、web サーバー、アプリケーション・サーバー、データベース、フレームワーク、カスタム・コード、およびプリインストール済みの仮想マシン、コンテナ、ストレージなど、アプリケーション・スタックのあらゆるレベルで発生する可能性があります（カテゴリ 5. を参照）。このような欠陥があると、多くの場合、攻撃者は権限なしにシステムのデータや機能にアクセスでき、場合によってはシステムが完全に乗っ取られることもあります。

この 3 年間で見つかった脆弱性のうち平均 11% が
不十分なトランスポート層の保護に関連していました。

3. **不十分なトランスポート層の保護。**これは、アプリケーションがネットワーク・トラフィックを保護する手段を取っていないために生じるセキュリティ上の弱点です。認証中は SSL/TLS を使用していても、アプリケーションの別の機能を実行中は使用していないことがよくあり、それによってデータとセッション ID が曝露されます。

   不十分なトランスポート・レイヤー・セキュリティに関する問題は非常に多くのモバイル・アプリケーションに見られるため、OWASP Mobile Top 10 では「安全でない通信」が 1 つの独立したカテゴリとされています。「モバイル・アプリケーションの多くがネットワーク・トラフィックを保護できていません。認証時には SSL/TLS を使用していても、それ以外では使用していません。この一貫性のなさにより、データとセッション ID が曝露し、傍受されるリスクを招いています」と OWASP は指摘しています。この 3 年間で見つかった脆弱性のうち平均 11% が不十分なトランスポート層の保護に関連していました。

4. **不十分な認可。**これらの脆弱性は、ユーザーが本来アクセスできないはずのデータ、コンテンツ、機能へのアクセスを許してしまう可能性があります。これは、アプリケーションやシステムがユーザーの身元を適切に検証していない場合や、適切なアクセス制御を適用できていない場合に発生する可能性があります。

   モバイル・アプリがリクエストの一部としてユーザーの役割や権限を暗号化せずにバックエンド・システムに送信することは、安全でない認可の一例です。多くの場合、IDOR の脆弱性が存在するのはコードが有効な認可チェックを実行していないためであると OWASP は指摘しています。この 3 年間で見つかった脆弱性のうち平均 9% が不十分な認可に関連していました。

5. **アプリケーションの設定ミス。**セキュリティの設定ミスが蔓延するもう 1 つの例であり、OWASP Top 10:2021 の脆弱性のうち 5 番目に危険なリスクでもあります。

   デバッグ機能や QA 機能など、多くのアプリケーションには、デプロイ時に無効化しないと非常に危険な開発者向け機能が備わっています。設定ファイルを適切にロックダウンしないと、クリアテキスト（誰でも読むこと

サーバーの設定ミスは、
この 3 年間のテストで
見つかった脆弱性のうち
平均 18% を占めていました。

ができる暗号化されていないテキスト）が公開される可能性があります。また、設定ファイルのデフォルト設定がセキュリティを考慮して設定されていないこともあります。この 3 年間で見つかった脆弱性のうち平均 5% がアプリケーション設定のミスに関連していました。

6. **アプリケーション・プライバシー不全。**アプリケーション・プライバシー不全は、情報漏えい / 流出に関連しており、アプリケーションが適切に設計または実装されていない、またはパッチが適用されていないために、潜在的なプライバシー侵害が生じて権限のないユーザーがデータやコンテンツにアクセスできるようになっているときに発生します。開発するアプリケーションのプライバシーについて企業が問うべき質問には次のようなものがあります。
   - 開発者は web アプリケーションのプライバシーに関するトレーニングを受けているか？
   - 安全なコーディング・ガイドラインが適用されているか？
   - ソフトウェア（サーバー、データベース、ライブラリ・コードを含む）は最新に保たれているか？
   - パッチは定期的に適用されているか？
   - ソフトウェアに含まれるサードパーティおよびオープンソースのコードを安全かつ最新に保つためにどのような対策を取っているか？
   - 特定の目的に使用した後、個人情報は削除されているか？

   この 3 年間で見つかった脆弱性のうち平均 5% がプライバシーの問題に関連していました。

7. **不十分な認証。**OWASP の「A07:2021—識別と認証の失敗」は、以前は「認証の不備」と呼ばれていたもので、現在は識別の失敗に関する脆弱性もこのカテゴリに含めるようになっており、これにはブラック・ダックのリストの 4. と 7. が含まれます。この 3 年間で見つかった脆弱性のうち平均 5% が不十分な認証に関連していました。

   不十分な認証と認可とは、アプリケーションやシステムがユーザーの身元を適切に検証していない場合や、適切なアクセス制御を適用できていない場合に発生するセキュリティ脆弱性を指します。権限のないユーザーが機密情報にアクセスしたり、本来は実行できないはずのアクションを実行したりする可能性が生じ、データ漏えいやデータ損失などのセキュリティ問題につながります。

8. **コンテンツ・スプーフィング / コンテンツ・インジェクション。**コンテンツ・スプーフィング（コンテンツ・インジェクションとも呼ぶ）は、ユーザーから提供されたデータを適切に扱っていない web アプリケーションの脆弱性によって可能となる、ユーザーを標的にした攻撃です。

   攻撃者が web アプリケーションにコンテンツを提供し、web アプリケーションが信頼済みドメインというコンテキストの下でそのコンテンツ（通常は改変されたページ）を無防備なユーザーに提示した場合に発生します。OWASP では、この種の攻撃は、ほとんどまたはまったく影響のないよくある web 脆弱性として広く誤解されていると指摘しています。実際には、コンテンツ・スプーフィング攻撃は、攻撃者が正規の組織になりすましてユーザーをだまし、ログイン資格情報を提供させるような様々な詐欺で使用されています。

デバッグ機能や QA 機能など、多くのアプリケーションには、デプロイ時に無効化しないと非常に危険な開発者向け機能が備わっています。

それ以上に懸念されるのは、コンテンツ・スプーフィングにより、コード・インジェクションやクロスサイト・スクリプティングなどの危険な攻撃を仕掛けられる可能性があるということです。この 3 年間で見つかった脆弱性のうち平均 4% がコンテンツ・スプーフィングまたはコンテンツ・インジェクションに関連していました。

9. **フィンガープリンティングの影響の受けやすさ。**フィンガープリンティング（情報を得るために web アプリケーションに探りを入れること）では、OS の種類やバージョン、SNMP 情報、ドメイン名、ネットワーク・ブロック、VPN ポイントなど、多くの重要な情報を攻撃者に知られてしまう可能性があります。この 3 年間で見つかった脆弱性のうち平均 3% がフィンガープリンティング関係の脆弱性に関連していました。

テストで見つかった特定のフィンガープリンティング・セキュリティ問題の多くは、リスク・レベルが最小〜低、中程度でした。つまり、これらの問題を攻撃者が悪用しても、それだけでシステムや機微なデータへのアクセスを許してしまうことはありません。とはいえ、これらの脆弱性を可視化することは決して無駄なことではありません。なぜなら、低リスクの脆弱性であっても、悪用されると攻撃の一助となることがあるためです。

例えば、フィンガープリンティングに関連するセキュリティ問題の 1 つである抑制されていないサーバー・バナー（図 5）は、常にペネトレーション・テストの 1/3、DAST スキャンの 1/2 近くで常に発見されています。中リスクの脆弱性ではありますが、抑制されていないサーバー・バナーは、サーバー名、種類、バージョン番号など、攻撃を開始するのに十分な情報を攻撃者に与えてしまう可能性があります。

	見つかった高リスク脆弱性が全体に占める割合	2021 年の順位	2020 年の順位
1. クロスサイト・スクリプティング	19%	2	1
2. 不十分な認可	16%	1	2
3. 不十分な認証	6%	3	3
4. アプリケーションの設定ミス	4%	6	9
5. 不十分なトランスポート層の保護	4%	4	5
6. 情報流出 / 情報漏えい	3%	7	6
7. サーバーの設定ミス	2%	9	8
8. SQL インジェクション	2%	8	10
9. 意図しないデータ漏えい	1%	*	*
10. 不十分なプロセス検証	1%	*	*

* トップ 10 入りしていない

図 3：2022 年に見つかった高リスク脆弱性トップ 10（再テストを除く）

2022 年のテストで発見された高リスク脆弱性全体のうち 19% がクロスサイト・スクリプティング攻撃に関連していました。

	見つかった緊急リスク脆弱性が全体に占める割合	2021 年の順位	2020 年の順位
1. SQL インジェクション	30%	1	1
2. 不十分な認可	9%	2	2
3. クロスサイト・スクリプティング	7%	9	9
4. 不十分な認証	7%	3	3
5. 情報流出 / 情報漏えい	6%	4	4
6. 不十分なプロセス検証	5%	8	5
7. OS コマンド実行	3%	7	7
8. サーバーの設定ミス	2%	*	*
9. アプリケーションの設定ミス	2%	6	9
10. SQL インジェクション	1%	*	*

* トップ 10 入りしていない

図 4：2022 年に見つかった緊急リスク脆弱性トップ 10（再テストを除く）

10. クライアント側 / クロスサイト・スクリプティング攻撃への曝露。ブラック・ダックが 3 年間にわたって実施したテストで見つかった高リスク脆弱性の中で 1 番目または 2 番目に多かったクロスサイト・スクリプティング（XSS）は、クライアント側のコード・インジェクション攻撃です。攻撃者は、正規の web ページや web アプリケーションに悪意のあるコードを仕掛けることで、被害者の web ブラウザで悪意のあるスクリプトを実行しようとします。2022 年のテストで発見された高リスク脆弱性全体のうち 19% がクロスサイト・スクリプティング攻撃に関連していました（図 3 参照）。

コンテンツ・セキュリティ・ポリシー（CSP）などの保護機能を安全な形で実装してセキュリティの層を増やすことで、クロスサイト・スクリプティングやデータ・インジェクション攻撃（テストで見つかった緊急リスク脆弱性攻撃の中で最多。図 4 参照）など、特定の種類の攻撃を検出および軽減しやすくなります。攻撃者はクッキーやフォームなどのユーザー・データの安全でない送信を利用することで、web サーバー上のシステム・シェルにコマンドを埋め込み、特権を利用してサーバーを乗っ取ることができる可能性があります。

多くの組織にとって、安全でない CSP や、CSP の欠落は、低リスクの問題だと考えることでしょう。しかし、クロスサイト・スクリプティングやクリックジャッキング、クロスサイト・リークの悪用が多発している現状を考えると、CSP（単なる CSP ではなく、悪意のあるスクリプトがクライアント側で実行されないようにする CSP）を使用することは、さまざまな種類の攻撃（クロスサイト・スクリプティング、データ・インジェクション攻撃など）に対する保護の層を増やすという点で大いに意義があります。

SQL コマンド・インジェクションは、テストで見つかった緊急リスク脆弱性の中で最多でした。

脆弱なサードパーティ・ライブラリの危険性

図 6 に示すように、ブラック・ダックが 2022 年に実施したテストの 25% で、「脆弱なサードパーティ・ライブラリの使用」が見つかりました。これは、OWASP Top 10 カテゴリの「A06:2021—脆弱で古くなったコンポーネント」に該当します。OWASP では、サードパーティおよびオープンソースのコンポーネントを含め、ソフトウェアが使用しているすべてのコンポーネント（クライアントサイドとサーバーサイドの両方）のバージョンを把握していない場合、ソフトウェアが脆弱である可能性が高いと指摘しています。

	2022 年の全テスト・ターゲットに占める割合	2021 年の順位	2020 年の順位
1. 弱い SSL/TLS 設定	70%	1	4
2. コンテンツ・セキュリティ・ポリシー（CSP）ヘッダーの欠落	43%	2	1
3. 抑制されていないサーバー・バナー	37%	3	2
4. キャッシュ可能な HTTPS コンテンツ	34%	5	5
5. HSTS（HTTP Strict Transport Security）未実装	34%	4	3
6. 安全でないコンテンツ・セキュリティ・ポリシー（CSP）ヘッダー	31%	6	8
7. 弱いパスワード・ポリシー	28%	7	7
8. マスクされていない非公開情報データ	25%	*	*
9. 脆弱なサードパーティ・ライブラリの使用	25%	*	*
10. 過剰なセッション・タイムアウト時間	24%	*	*

*トップ 10 入りしていない

図 5：2022 年のセキュリティ問題トップ 10

オープンソース・コードの人気が爆発的に高まり、ソフトウェア開発のスピードと効率を劇的に向上させることができることから、現代のソフトウェアには不可欠な構成要素となっています。実績のあるコードに簡単にアクセスできる利便性により、ソフトウェア開発者は時間と限られたリソースを費やして「車輪の再発明」をする必要がなくなります。

しかしながら、ブラック・ダックの年次レポート「オープンソース・セキュリティ＆リスク分析レポート」によれば、オープンソース・コードにはリスクがつきものです。実際、2023 年のレポートでは、オープンソースのセキュリティ・リスクがかつてないほど高まっており、ほとんどの企業が自社のコードの中身を十分に把握していないことが分かっています。

ほとんどの企業は、
自社のコードの中身を
十分に把握していません。

同レポートによれば、高リスクのオープンソース脆弱性は、過去 5 年間で恐るべき割合で増加しています（小売業と e コマース分野のみで 557%）。さらに、プロジェクトの依存ファイルに対してセキュリティ・パッチの適用や保守がなされていないことも懸念されます（91% に古くなったオープンソース・コンポーネントが含まれていました）。

大規模なサプライチェーン攻撃が注目を集める中、サードパーティ・ソフトウェアを使用している組織（つまり、現代のほぼすべての組織）にとってソフトウェア・サプライチェーンのセキュリティが大きな関心事となっています。サプライチェーンのリスクをより適切に管理するため、自動ツールを使用してソフトウェア部品表（SBOM）を生成する組織が増えています。これにより、使用しているサードパーティ・ソフトウェアとオープンソース・ソフトウェアを特定できます。

SBOM への機運が高まっていることは、BSIMM のレポートでアクティビティ「デプロイ済みソフトウェアの BOM を作成する」を実施している組織の数が増加していることからも見て取れます。BSIMM データからは、脆弱なオープンソース・プロジェクトを標的とした攻撃の増加を受けて「オープンソースを特定する」と「オープンソースのリスクを管理する」アクティビティを実施している組織が大幅に増加していることも分かります。

多くの企業が数百ものアプリケーションやソフトウェア・システムを使用しており、さらにその 1 つ 1 つが数百から数千ものサードパーティ / オープンソース・コンポーネントに依存している可能性が高いため、これらコンポーネントを効果的に追跡するには正確な SBOM を常に最新の状態に維持することが急務となっています。

考察と提言

- **多層的なセキュリティ・アプローチを導入する：**静的アプリケーション・セキュリティ・テスト（SAST）などの単一のセキュリティ・テスト・ソリューションに頼るだけではもはや十分ではありません。組織は、コーディングの欠陥を特定する SAST、実行中のアプリケーションを検査する DAST、サードパーティのコンポーネントによってもたらされる脆弱性を特定するソフトウェア・コンポジション解析（SCA）、他のテストでは見落とされがちな設定ミスや脆弱性などの問題を特定するペネトレーション・テストから成る、複合的なセキュリティ・アプローチを導入する必要があります。

  ブラック・ダックのレポート「世界の DevSecOps の現状 2023」では、回答者の 44% が外部ペンテストをセキュリティ・テストの重要な要素でありその他のテストを補完するものとして挙げています。外部ペンテストには、自社のセキュリティ態勢について先入観のない第三者的視点が得られる、他のテストで見逃され攻撃者に悪用される可能性のある潜在的な脅威や脆弱性を正確にシミュレーションできるなどの利点があります。

- **自動セキュリティ・テストとマニュアル・セキュリティ・テストを併用する：**テストの自動化は一貫性、拡張性、時間とコストを節約する上で重要ですが、人的要因によって複雑かつ微妙なセキュリティ問題を特定するのに不可欠な洞察力と適応性が加わります。例えば、DAST は、ブラックボックス・テスト（アプリケーションの内部構造についての知識なしに実施する）の性質上、開発者とセキュリティの専門家が検出結果を検証し、トリアージする必要があります。

ソフトウェアの脆弱性で
最も危険なものは、
開発者が気づいていない
脆弱性です。

- **パッチ管理を優先的に行う：**特にサードパーティおよびオープンソースのコンポーネントについて、脆弱性に対して迅速にパッチを適用できるよう、常に注意を払うようにします。潜在的なエクスプロイトを軽減するため、パッチの迅速な特定、評価、適用を可能にする明確なプロセスを確立します。
- **強力なアクセス制御を採用する：**アプリケーションおよびネットワーク全体に厳格なアクセス制御のポリシーを適用します。最小特権の原則を導入し、ユーザーがタスクを実行するのに必要な最小レベルのアクセス権を付与します。不正アクセス防止のため、アプリケーションのアクセス権限を定期的に見直し、更新します。
- **ソフトウェア開発ライフサイクルに SBOM の生成を組み込む：**ソフトウェアの脆弱性で最も危険なものは、開発者が気づいていない脆弱性です。総合的なインベントリを使用してコンポーネントを特定することで、セキュリティの状態を適切に評価し、脆弱性の問題が発生したときにも効果的に対応できるようになります。
- **セキュリティ・テストを補完する必要があるかどうか判断する：**チームに、セキュリティ上の不具合をテストするのに十分なアプリケーション・セキュリティ・スキルとリソースはありますか?また、規制当局や顧客に求められているレベルでソフトウェアをテストする時間はありますか?
- **専門家によるオンデマンドのセキュリティ・テストでチームを強化できるベンダーを選択する：**ブラック・ダックのセキュリティ・テスト・サービスを利用すれば、あらゆるアプリケーションを、あらゆる深さで、いつでも、高い費用対効果で解析するために必要なスキル、ツール、規律を備えたエキスパートを継続的に利用できます。

ブラック・ダックでは、ペネトレーション・テスト、動的アプリケーション・セキュリティ・テスト、静的アプリケーション・セキュリティ・テスト、モバイル・アプリケーション・セキュリティ・テスト、ネットワーク・ペネトレーション・テスト、レッド・チーム、IoT および組み込みソフトウェア・テスト、シック・クライアント・テストなど、あらゆる種類のテスト・サービスを提供しています。

あなたのチームを強化するブラック・ダックのオンデマンド・リソース

無料相談のご予約はこちらまで。

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。
詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社
www.blackduck.com/jp

©2024 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2024 年 10 月