BLACKDUCK®

2024
ソフトウェア脆弱性スナップショット

ブラック・ダックによる 20 万件以上のアプリケーション・セキュリティ・スキャンに基づく重大な脆弱性に関する知見

目次

エグゼクティブ・サマリー

本レポートは、19 業種にまたがる約 1,300 のアプリケーションに対し、2023 年 6 月から 2024 年 6 月にかけてブラック・ダックが実施した 20 万余りの動的アプリケーション・セキュリティ・テスト (DAST) のスキャンデータを分析したものです。

この調査結果では、web ベースのアプリケーションおよびシステムでのセキュリティの現状と、金融、保険、ヘルスケアなどのリスクの高い分野で脆弱性が事業運営に及ぼす潜在的な影響に関する知見を提供します。

また、DAST が静的アプリケーション・セキュリティ・テスト (SAST) やソフトウェア・コンポジション解析 (SCA) を含むその他のセキュリティ・テスト手法に、どのように補完する重要な役割を果たすかの考察と、実際の攻撃シナリオを模倣することでアプリケーション・セキュリティに関する独自の観点を提供します。

ブラック・ダックについて

シノプシスのソフトウェア・インテグリティ・グループを前身とするブラック・ダックは、業界で最も包括的かつ強力で、信頼されるアプリケーション・セキュリティ・ソリューションのポートフォリオを提供しています。私たちには、お客様がソフトウェアを迅速に保護し、効率的にセキュリティを開発環境に統合し、革新的な新技術を安全に採り入れられるように支援してきた他にはない実績があります。

主な調査結果

脆弱性の状況

2023 ～ 2024 年に実施されたスキャンでは、合計 96,917 件の脆弱性が特定されました。非常に多く特定された重大なリスクのある脆弱性には、次のようなものがあります。

暗号化の失敗 (機密データの曝露)
これらは、アプリケーションが機密情報を保護する仕組みにおける脆弱性です。このカテゴリには、重要なデータのインターネット経由での送信時に、暗号化していない。古い、もしくは脆弱な暗号化方式を使用している。パスワードやその他の秘密情報を適切に保護していない。といった問題が含まれます。このような暗号化の失敗はデータ侵害を引き起こす可能性があり、個人情報、財務データ、ログイン資格情報などの機密情報が攻撃者によって盗まれ、不正に改ざんされる恐れがあります。

ブラック・ダックの DAST 解析では、この脆弱性カテゴリが広範囲に渡って確認されており、顧客の 86% に影響が及び、確認された脆弱性は 30,726 件に上っており、4,882 件の重大なリスクの事例が含まれています。このため、業種を越えて最もよく見られる深刻なセキュリティ上の問題の 1 つとなっています。組織がこのような脆弱性に対処するために必要なのは、強力な暗号化プラクティスの実施、最新セキュリティ・プロトコルの使用、送信中/保管時の両方での機密データの適切な保護です。

インジェクション脆弱性
このタイプの脆弱性があると、攻撃者が悪意のあるコードやコマンドをアプリケーションに挿入することで、アプリケーションの意図しないアクションの実行や適切な権限なしでのデータ・アクセスを実行させることができます。今回の解析で発見されたインジェクション脆弱性は 4,814 件で、顧客毎の蔓延率は 59% という高い値となりました。このカテゴリの重大な脆弱性は 2 番目に多く (2,491 件)、深刻なセキュリティ侵害を引き起こす可能性が示されています。

インジェクション脆弱性は多くの場合、ユーザー入力が、データベース・クエリー、オペレーティング・システム・コマンド、web ページ・コンテンツで使用される前に、適切に検証またはサニタイズされていない場合に発生します。一般的なインジェクション攻撃には、SQL インジェクション、コマンド・インジェクション、クロスサイト・スクリプティング (XSS) が含まれ、攻撃が成功すると、データ窃取や不正なデータ操作に加え、システム全体の侵害にさえもつながります。

組織がインジェクション脆弱性を防止するには、適切な入力検証を実装し、パラメータ化したクエリーを使用し、安全なコーディング・プラクティスに従う必要があります。SAST および DAST のどちらでもインジェクション脆弱性を検出できますが、DAST では特に実行時に依存する複雑な問題を効果的に特定できます。定期的なセキュリティ・テストを、特に DAST を使用して実施すると、これらの脆弱性の特定と対処に役立ちます。

業種別の知見

ハイリスク・セクターには、金融および保険 (1,299 件の重大な脆弱性)、ヘルスケアおよび社会扶助 (992 件の重大な脆弱性)、情報サービス (446 件の重大な脆弱性) が含まれます。金融および保険業種 (FSI) で確認された重大な脆弱性が最も多く、サイトの複雑さにかかわらず、小規模 FSI サイトでは 565 件、中規模サイトでは 580 件、大規模サイトでは 154 件の重大な脆弱性が特定されました。次に多かったのはヘルスケアおよび社会扶助業種で、小規模サイトで 367 件、中規模サイトで 486 件、大規模サイトで 139 件の重大な脆弱性が確認されました。

データでは、大規模サイトよりも中小規模サイトで発見される重大な脆弱性の方が多い傾向が見られ、FSI セクターでは特にそれが顕著でした。

対応完了までの期間の分析

脆弱性の対応を完了するまでの期間に関しては、業種によって大きなばらつきが見られました。重大な脆弱性の対応を完了するまでの期間がすべてのサイト間で最長であったのは、公益事業です。公益事業で、大規模サイト (1 日) よりも、小規模サイト (107 日) と中規模サイト (876 日) でのクローズに長い時間がかかっている原因には、サイバーセキュリティ・リソースが限られていることと予算が制約されていることが考えられます。公益事業では、パッチ適用と更新が難しいレガシー・システムで運用していることも少なくありません。大規模サイトの場合は、より堅牢なプロセスと専属のセキュリティ・チームを導入しており、より迅速に脆弱性に対処できる可能性があります。

次に対応完了までの期間が長かったのは教育サービス・セクターで、小規模サイトで 342 日、中規模サイトで 111 日、大規模サイトで 1 日かかっています。小規模な教育機関では予算が制限されていることが多く、専属のサイバーセキュリティ要員が足りない可能性もあるため、脆弱性の対処までの期間が長くなっていると見られます。一方で、主要大学などの大規模教育機関は、迅速に重大な脆弱性を軽減できるように、比較的資金のある IT 部門と多くのリソースを備えているようです。

対照的に、金融および保険セクターで重大な脆弱性の対応を完了するまでの期間は、小規模サイトでわずか 28 日であるのに対し、中規模サイトでは 53 日、大規模サイトでは 78 日でした。このセクターは規制が厳しく、機密性が非常に高いデータを扱っているため、速やかに脆弱性に対応する必要があります。これらの組織は、通常、Payment Card Industry Data Security Standard (PCI DSS) などの規制を確実に遵守し、金融データを保護するために、かなりのサイバーセキュリティ予算と専属チームを備えています。

ヘルスケアおよび社会扶助セクターの組織が重大な脆弱性の対応を完了するまでの平均期間は、小規模サイトで 87 日、中規模サイトで 30 日、大規模サイトで 20 日でした。ヘルスケア・セクターも規制が厳しく (例 : 医療保険の携行性と責任に関する法律 [HIPAA])、取り扱いに慎重を要する患者データを処理しているため、迅速な脆弱性の修正が求められます。ヘルスケア組織の規模が大きければ大きいほど、リソースと専属セキュリティ・チームを増やし、対応完了までの期間も短くすることができると言えます。

対応完了までの期間という指標のセクター間での違いにより、リソース配分の重要性とレガシー・システムがセキュリティ・イニシアティブにもたらし得る課題が明らかになります。規制圧力が強く機密データを扱うセクターは、脆弱性の軽減に向けて速やかに行動する傾向があり、先を見越した姿勢が表れています。一方で、リソースが限られ予算が制約されているセクターでは、脆弱性にさらされる期間が長くなっています。リソースが不足している業種には個別に調整したサイバーセキュリティ戦略と、投資を増やす必要性があることがわかります。

ブラック・ダックのアナリストは、Black Duck® Continuous Dynamic スキャンにより評価されるアプリケーションの相対的な「サイトの複雑さ」をランク付けするために、独自の指標を使用しています。この指標は、スキャン・プロセスで実行される相互作用がいくつあるかと、どれだけ高度であるかによって決まります。複雑さの低いアプリケーションは、双方向性が最小限でクロール・ツリーが単純、つまり URL 構造がわかりやすいアプリケーションである可能性があります。複雑さの高いアプリケーションであればあるほど、相互作用要素と動的生成コンテンツが増える可能性があります。

ブラック・ダックのスペシャリストは、この指標によりスキャンの挙動をカスタマイズし、アプリケーションの複雑さによってスキャンの深さと攻撃を調整できます。また、比較と基準設定のため、業種間で複雑さの指標に重み付けをすることができます。

データが示す潜在的なビジネスへの影響

これらの脆弱性によるリスクには、次のようなものがあります。

データ漏えい：機微な情報の露出およびインジェクション脆弱性は、あらゆる業種で機密データに重大な脅威をもたらし、データ・リーク、罰金、財務損失、評判の失墜につながるおそれがあります。リスクにさらされる機密データには個人識別情報が含まれ、例としては、社会保障番号、口座情報、ログイン資格情報、クレジットカード番号、医療記録、企業秘密などがあります。

規制不遵守：ハイリスク・セクターでは、データ保護規制に違反するリスクが高まっており、厳しい罰則を受けるおそれがあります。たとえば、2022 年重要インフラ向けサイバーインシデント報告法 (CIRCIA) は、重要インフラ・セクター (とりわけ FSI、ヘルスケア、廃棄物管理など) に適用され、対象事業体に対し、対象となるサイバー・インシデントとランサムウェアの出費を米国サイバーセキュリティ・インフラセキュリティ庁 (CISA) に報告することを義務付けています。PCI DSS はクレジットカード情報を取り扱うすべての組織に適用され、カード会員データを保護するためのセキュリティ標準を義務付けています。HIPAA は患者の健康情報の保護を求めるもので、データ漏えいの報告を義務付けています。一般データ保護規則 (GDPR) は、EU 市民のデータを扱う組織に対して厳格なデータ保護対策と漏えい時の報告を要求しています。

オペレーションの混乱：業種セクター間で蔓延しているセキュリティ設定のミスおよび DoS 脆弱性により、事業継続とサービス可用性が脅かされています。脆弱性と設定ミスによって引き起こされるオペレーションの混乱は、さまざまなセクターに重大な影響を及ぼしかねません。たとえばヘルスケア・セクターで考えられる重大な混乱には、次のようなものがあります。

- **救命設備の停止：**病院のネットワークを狙うサイバー攻撃は、人工呼吸器、注入ポンプ、心臓モニタなど極めて重要な医療機器の停止をもたらすおそれがあります。患者の生命維持がこれらの機器に依存している場合、即座に命に関わる状況に陥りかねません。たとえば人工呼吸器が停止した場合、自ら呼吸できない患者の健康状態には重大な影響が及び、死にさえ至る可能性もあります。
- **電子カルテの侵害：**ランサムウェア攻撃によって患者の記録が暗号化されると、医療提供者はこれらの情報にアクセスできなくなります。患者の病歴、投薬記録、治療計画にアクセスできない場合、ケアの遅れ、誤った治療、投薬ミスが発生する可能性があります。これは患者の治療結果に重大な影響を及ぼすおそれがあり、特に、正確な情報へのタイムリーなアクセスが不可欠な緊急事態ではなおさらです。
- **調剤システムの中断による投薬ミス：**調剤システムに含まれる脆弱性の悪用により、システムがオフラインになる可能性があります。調剤システムの中断は、投薬の遅れ、正しくない投薬量、治療の見逃しを招くおそれがあり、正確な投薬管理が必要とされる危機的状況にある患者にとって特に危険になり得ます。

長期にわたる脆弱性の露出：公益事業や教育サービスなどのセクターでは、脆弱性のクローズまでに長い時間がかかることで、悪用と、ビジネスへの潜在的な影響のリスクが増大しています。たとえば、送電網制御システムの脆弱性にパッチを適用しないままにしていると、長時間の停電が引き起こされ、膨大な数の家庭と企業に影響するおそれがあります。極端なケースでは相互接続された電力系統間で障害が連鎖し、地域全体の大規模停電に至る可能性もあります。水処理施設の制御システムに含まれる脆弱性が未処理のままの場合、化学処理プロセスが改ざんされ、水質汚染が引き起こされかねません。その結果、疾病が蔓延し、広範囲にわたる装置の洗浄が必要になり、水の安全に対する国民の信頼が失われないとも限りません。

教育サービス・セクターで学生情報システムに未対応の脆弱性があると、個人情報、成績、財務情報を含む生徒の機密データの曝露につながり得ます。このようなデータ漏えいは、なりすまし、学歴詐称、家族の教育の権利とプライバシー法 (FERPA) などのプライバシー法の違反を引き起こし、教育機関に法的な影響と信頼の失墜をもたらすおそれがあります。

推奨事項

ブラック・ダックが実施した 20 万件以上のスキャンから得られた調査結果データに基づき、特にハイリスク・セクターで、機密データの曝露 (OWASP 2021 の分類では暗号化の失敗と呼ばれる) とインジェクション脆弱性 (SQL インジェクション、クロスサイト・スクリプティングを含む) への対処を優先することを推奨します。

すべてのセクターの組織で、重大な脆弱性をクローズするまでの期間の短縮を重視することを推奨しますが、修正に長い期間がかかっているセクターには特にこれが当てはまります。また、すべての業種で、情報が漏えいして評判が失墜する可能性を最小化するため、セキュリティの設定ミスに対処することを推奨します。

総合的に、開発およびセキュリティ・チームが、ソフトウェア開発ライフサイクル全体を通じて最も包括的なカバレッジを達成するために、DAST、SAST、SCA を統合した多面的なセキュリティ・アプローチを実行することを推奨します。調査結果によると、このような全面的アプローチをアプリケーション・セキュリティ・テストに適用すると、重大な脆弱性への潜在的な曝露が大幅に小さくなります。

このレポートの対象業種セクター

農業、林業、漁業、
狩猟

鉱業/採石、
石油/ガス採掘

建設

卸売

不動産および賃貸

会社企業経営

製造

行政支援および
廃棄物管理

宿泊および
食品サービス

芸術、エンターテインメント、
レクリエーション

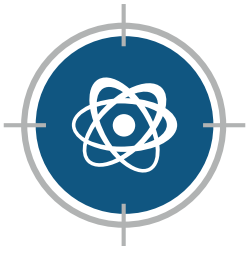
教育サービス

金融および保険

ヘルスケアおよび
社会扶助

情報サービス

その他サービス



専門、科学、
技術サービス

行政

小売

輸送および倉庫

公益事業

動的アプリケーション・セキュリティ・テストの基礎

DAST はアプリケーション・セキュリティ環境に不可欠なコンポーネントですが、web アプリケーションがますます複雑で脆弱になるにつれ、その重要性が特に高くなっています。このセクションでは、DAST の包括的な概要とその意義、堅牢なアプリケーション・セキュリティ戦略で DAST が果たす役割について解説します。

DAST の主な特徴

DAST はブラックボックス・セキュリティ・テスト手法で、実行状態にあるアプリケーションを分析します。アプリケーションの設計、アーキテクチャ、内部への特権アクセスは必要ありません。ソース・コードを調査する SAST とは異なり、DAST はライブ・アプリケーションに対する実際の攻撃をシミュレートして、実行時のみ、または複数のサブシステム間の相互作用においてのみ現れる脆弱性を特定します。このアプローチにより、DAST では、認証の問題、サーバー設定ミス、クロスサイト・スクリプティングの脆弱性など、その他のテスト手法では見つからないであろう問題を検出できます。

最近のセキュリティ状況における DAST

DAST の重要性が著しく高くなっている要因には次のようなものがあります。

- **web アプリケーションの複雑化 :** マイクロサービス・アーキテクチャ、API 主導開発、クラウドネイティブ・アプリケーションの増大により、アタック・サーフェスが大幅に拡大しています。
- **進化するサイバー脅威 :** 攻撃者がますます巧妙になっていることで、実際の攻撃をシミュレートする DAST の能力が極めて貴重になっています。
- **規制の遵守 :** GDPR や PCI DSS などの規制フレームワークでは、堅牢な継続的セキュリティ・テストが要求されているため、これを遵守するために DAST は欠かせないツールとなっています。
- **DevSecOps への統合 :** DAST は継続的インテグレーション/継続的デプロイ (CI/CD) パイプラインに統合できるため、最近の DevSecOps プラクティスに準拠しています。
- **コストへの影響 :** 脆弱性を早期に検出することで、デプロイ後にセキュリティ問題を修正する場合のコストを大幅に削減できます。

DAST とその他のテスト手法

DAST は強力ですが、最も効果が高くなるのはその他のセキュリティ・テスト手法と併用する場合です。たとえば、SAST の強みにはコーディングの欠陥の早期検出などがありますが、実行時の脆弱性やコンポーネント間の意図しない相互作用は見逃される場合があります。これらを発見できるのが DAST です。同様に、SCA はサードパーティ・コンポーネント内の脆弱性を特定しますが、DAST では、これらの脆弱性が実行中のアプリケーションで悪用されるかどうかを検証できます。

組織は DAST をその他のテスト手法を組み合わせて実施することで、複雑なオンライン・アプリケーション環境でのセキュリティ態勢を大幅に強化できます。

DAST の主な特徴

- 攻撃者の考えを模倣した外部観点のテスト
- トレンドになっている動作の可視化
- アプリケーションの実行時解析
- 継続的テスト
- ソース・コードへのアクセスなしでのテスト機能

本番前と本番での DAST

DAST ソリューションは CI/CD パイプラインに統合できるため、脆弱性を早期に特定することで、改善を加速して修正コストを削減することができます。このアプローチは、特に、特定の種類のインジェクション脆弱性など、実行中アプリケーションのみで顕在化する可能性がある問題や、サービスおよびコンポーネント間での予期しない相互作用を検出する上で役立ちます。

DAST ソリューションを本番で使用するとさらに別の利点があり、特に、複雑で動的なアプリケーションを使用する組織や、規制の厳しい業種の組織にとって有効です。また、継続的監視も提供されるため、構成変更、新たに検出されたエクスプロイト、アプリケーションの実行時環境の変更によって生じる可能性のある脆弱性を検出できます。これは特に、時間の経過とともに脆弱になる可能性のあるサードパーティ・コンポーネントの問題を特定したり、パッチの有効性を検証したりする際に役立ちます。

一部の組織では、本番前と本番での DAST テストを組み合わせることで、最も包括的なセキュリティ・カバレッジを達成できます。こういったケースでの最適なシナリオは、本番前の DAST テストを広範囲で実施し、本番テストは主要なセキュリティ戦略ではなく補助的手段として使用する方法です。このような組み合わせによるメリットには、次のようなものがあります。

- **リスクの軽減：** 本番前テストにより、ライブ環境での計画外ダウンタイムやデータ破損のリスクが解消されます。
- **コスト効果：** 開発サイクルの早期に脆弱性を修正すると、通常、本番での対応よりも大幅に低コストで済みます。
- **開発者フレンドリー：** IDE および CI/CD パイプラインへの統合により、セキュリティ・テストが自然に開発プロセスの一部になります。
- **コンプライアンス：** 多くの規制標準で、本番デプロイ前のテストが推奨または義務付けられています。
- **包括的テスト：** 本番前環境では、ユーザーやデータへの影響を心配することなく、より徹底的かつ積極的なテストを実施できます。

本番での DAST テストは次のようなシナリオで有益になります。

- **継続的なセキュリティ検証：** さらに別のセキュリティ・レイヤーの役割を果たして、本番前テストで見逃された問題を捕捉します。
- **新たな脅威の検出：** DAST は新たな脅威を自動的に検出します。
- **クラウドネイティブ・アプリケーション：** 本番環境の構成が独特でテスト環境での再現が難しい場合、本番環境でのテストが役立ちます。
- **レガシー・システム：** 包括的な本番前環境を持たない旧式のアプリケーションは、本番で DAST を実施すれば効果が高くなる場合があります。

本番前環境と本番環境の両方で戦略的に DAST を実施することで、バランスの取れたアプローチが実現し、システム・インテグリティやユーザー・エクスペリエンスを損なうことなく徹底的なテストを実行できます。この多面的な戦略により、アプリケーション・ライフサイクルのさまざまな段階で脆弱性の検出が強化されるだけでなく、レガシー・システムからクラウドネイティブ・アプリケーションまでの多様なアプリケーション・アーキテクチャに起因する固有の課題に対処できます。最終的に、このアプローチは、進化する脅威の状況に適応できる、回復力の高いセキュリティ態勢の構築を可能にします。

脆弱性の状況の分析

約 1,300 のアプリケーションでの 20 万件を超える DAST スキャンの分析から、懸念の多い脆弱性の状況が明らかになっています。このセクションでは、広がりと重要度が最も大きい脆弱性とその業種別分布、さらに事業運営への潜在的な影響について詳しく解説します。

特定された脆弱性クラス Top 10

	脆弱性クラス	説明	特定された脆弱性の件数
1	不十分なトランスポート層の保護	送信中のデータが適切に暗号化されていないため、傍受と改ざんが可能。	30,712
2	セキュアヘッダーの欠落	各種の web ベース攻撃を防止する重要な HTTP セキュリティ・ヘッダー (X-XSS-Protection、X-Frame-Options、Content-Security-Policy など) が欠如している。	22,321
3	情報漏えい	攻撃者がシステムのアーキテクチャまたは脆弱性を見抜くために利用できる、アプリケーション応答 (エラー・メッセージやコメントなど) を介した、意図せず機密情報が曝露する。	8,097
4	予測可能なリソースの位置	攻撃者により容易に推測または予測できる場所にリソースやファイルが保管されているため、潜在的に機密情報/機能への不正アクセスが可能。	5,468
5	フレーム化可能なリソース	iframe や別のサイト内への web ページの埋め込みを可能にする脆弱性で、潜在的にクリックジャッキング攻撃をもたらす。X-Frame-Options ヘッダーの欠如や不適切な設定によって生じる。	4,481
6	脆弱なライブラリ	既知のセキュリティ脆弱性を含むサードパーティ・ライブラリ/コンポーネントの使用が、それを使用するアプリケーションに脆弱性をもたらす場合がある。	4,215
7	フィンガープリンティング	攻撃者がテクノロジー・スタック、バージョン、システム構成に関する情報を取得すると、潜在的な脆弱性の特定やより絞り込んだ標的型攻撃の計画に使用される可能性がある。	3,700
8	クロスサイト・スクリプティング	この脆弱性により、別のユーザーが見る web ページに攻撃者が悪意のあるスクリプトを注入できる。機密情報の盗用またはセッション・ハイジャッキングにつながる可能性がある。	2,415
9	認可の不備	不完全なアクセス制御により、ユーザーに想定された権限を超えるアクション実行やリソース・アクセスが可能になる。権限チェックの不適切な実装に起因することが多い。	2,396
10	ブルートフォース (総当たり) に対する脆弱性	いつか当たることを期待して、攻撃者が組織的に多数のパスワードやパスフレーズを試行する攻撃手法。弱いパスワード・ポリシーやアカウント・ロックアウト・メカニズムの欠如を悪用されることが多い。	2,235

図 1. 脆弱性の特定件数

ブラック・ダックの分析では合計 96,917 件の脆弱性が特定されました。図 1 は、最も多く特定された脆弱性を示し、図 2 は、それぞれの脆弱性が確認された顧客の割合を示しています。

最も一般的な問題である不十分なトランスポート層の保護によって、組織はデータの傍受および改ざんのリスクにさらされており、データ侵害やコンプライアンス違反につながる可能性があります。2 番目によくある脆弱性、セキュアヘッダーの欠落では、アプリケーションが各種の web ベース攻撃を受けやすい状態のままになるため、全般的なセキュリティ態勢が揺るぎます。

情報漏えいと予測可能なリソースの位置は重大な脆弱性に相当し、攻撃者がシステムに侵入経路として選びがちです。8,097 件の脆弱性が特定され、3 番目に位置づけられた情報漏えいでは、エラー・メッセージ、コメント、アプリケーション応答を介して、意図せず機密情報が曝露します。これにより、システムのアーキテクチャや脆弱性を知るために有益な情報が、攻撃者の手に渡りかねません。

5,468 件の脆弱性が特定された 4 番目の予測可能なリソースの位置では、簡単に推測できる場所にリソースやファイルが保管されている場合に発生し、機密情報や機能への不正アクセスを可能にしかねません。

これらの脆弱性クラスが明らかにする共通の問題は、不注意による情報開示が攻撃者に悪用される可能性があるという事実です。これらの脆弱性は、複雑な技術的な問題ではなく、見過ごしや不適切なセキュリティ慣行に起因することが多いため、特に懸念されるものの、どちらも一般的であり、適切なセキュリティに対する認識とプロトコルがあれば、少なくとも理論上は対応しやすいと言えます。

脆弱性クラス	脆弱性が特定された顧客の割合
セキュアヘッダーの欠落	97%
不十分なトランスポート層の保護	87%
情報漏えい	66%
フレーム化可能なリソース	60%
脆弱なライブラリ	57%
不適切な認可	50%
フィンガープリンティング	46%
クロスサイト・スクリプティング	41%
不適切な入力確認	40%
予測可能なリソースの位置	35%

図 2. 特定の脆弱性クラスに含まれる脆弱性が確認された顧客の割合

重大なリスクのある、あるいは緊急の対処が必要な脆弱性

脆弱性クラス	重大なリスクのある脆弱性	緊急対処の必要性
不十分なトランスポート層の保護	4,882	2
クロスサイト・スクリプティング	2,256	1
情報漏えい	510	-
クロスサイト・リクエスト・フォージェリ (CSRF)	434	-
機能の悪用	248	36
HTTP レスポンス分割	203	-
コンテンツ・スプーフィング	76	-
パス・トラバーサル	73	-
パスワード・ポリシーの実装の不備	67	-
プロセス検証の不備	61	-

図 3. 重大なリスクのある脆弱性と緊急の脆弱性

特定された脆弱性のうち、重大なリスクのある脆弱性や緊急の対処が必要な脆弱性として際立ったものがありました。これらには、不十分なトランスポート層の保護 (4,882 件の重大な事例)、クロスサイト・スクリプティング (2,256 件のクリティカル事例)、情報漏えい (510 件の重大な事例) が含まれます。

不十分なトランスポート層の保護の重大な脆弱性が非常に多いことは、潜在的なデータ漏えいリスクの広がりを表しており、特に憂慮すべきです。クロスサイト・スクリプティングの脆弱性は、件数は少ないものの、セッション・ハイジャッキングやデータ盗用をもたらす可能性があるため、重大な脅威となります。

機能の悪用の注目すべき点は、緊急の対処が求められる重大な脆弱性の件数が多いことです。このタイプの脆弱性はしばしば、正当なアプリケーション機能の誤用に関係します。つまり、複雑な手段でセキュリティ対策をバイパスすることなく、即座に脆弱性が悪用される可能性があります。アプリケーションの中核に影響を与え得る脆弱性であるため、潜在的に広範なユーザーやクリティカルなビジネス・プロセスに影響が及びます。また、時として権限の昇格や機密データへのアクセスの原因となるため、迅速な対処が極めて重要です。

OWASP Top 10 カテゴリの分析

OWASP カテゴリ	特定された脆弱性の件数	対応する CWE
A01:2021 – アクセス制御の不備	9,954	CWE-35、CWE-548、CWE-287、CWE-352、CWE-425、CWE-601、CWE-424
A02:2021 – 暗号化の失敗	30,726	CWE-319、CWE-330、CWE-311
A03:2021 – インジェクション	4,814	CWE-943、CWE-91、CWE-20、CWE-643、CWE-113、CWE-77、CWE-89、CWE-610、CWE-652、CWE-94、CWE-79、CWE-78、CWE-97、CWE-90
A04:2021 – 安全が確認されない不安な設計	7,581	CWE-799、CWE-840、CWE-525、CWE-1021
A05:2021 – セキュリティの設定ミス	36,321	CWE-497、CWE-550、CWE-209、CWE-611、CWE-525、CWE-200、CWE-703、CWE-202、CWE-693、CWE-16、CWE-1004、CWE-614、CWE-544
A06:2021 – 脆弱で古くなったコンポーネント	4,215	CWE-1104
A07:2021 – 識別と認証の失敗	1,057	CWE-521、CWE-640、CWE-613、CWE-285、CWE-384
A08:2021 – ソフトウェアとデータの整合性の不具合	1,929	CWE-345、CWE-451、CWE-148、CWE-829
A10:2021 – サーバーサイドリクエストフォージェリ (SSRF)	1	CWE-918
A11:2021 – サービス拒否攻撃 (DoS)	319	CWE-400

図 4. OWASP Top 10 カテゴリと対応する CWE

今回の調査結果を OWASP Top 10 カテゴリに当てはめることで、いくつかの知見が得られます。

A02:2021 – 暗号化の失敗/機微な情報の露出 : 4,882 件の重大なリスクのある事例を含む、30,726 件の脆弱性。このカテゴリは、顧客での蔓延率が 2 番目に高く (86%)、機密データの適切な保護に関する問題の広がりを示しています。このカテゴリに含まれる CWE には次が含まれます。

- CWE-319: この CWE は、アプリケーションが平文で機密情報を送信しており、攻撃者による傍受と読み取りが可能な状態を表します。
- CWE-330: この CWE は、ランダム・パスワードや暗号化キーなどの予測不可能性が求められるコンテキストで、予測可能な値を使用しているアプリケーションを指します。
- CWE-311: この CWE は、保管または送信の前に機密データを暗号化しておらず、傍受や不正アクセスの対象になりやすいアプリケーションを指します。

A03:2021 – インジェクション : 2,491 件のクリティカル事例を含む 4,814 件の脆弱性、顧客での高い蔓延率 (59%)。これは、各種アプリケーション間でインジェクション攻撃の脅威が続いていることを強く示しています。

このカテゴリの CWE には、CWE-943、CWE-91、CWE-20、CWE-643、CWE-113、CWE-77、CWE-89、CWE-610、CWE-652、CWE-94、CWE-79、CWE-78、CWE-97、CWE-90 が含まれます。これらのうちの多くは、アプリケーションにコード、コマンド、データを注入する攻撃に関連しており、アプリケーションでの意図しないコマンドの実行や適切な権限のないデータ・アクセスが引き起こされるおそれがあります。

SQL インジェクションやコマンド・インジェクションなどのインジェクション攻撃は、CWE の最も危険な脆弱性リストの上位に位置づけられています。該当する CWE には、CWE-91、CWE-77、CWE-89、CWE-94、CWE-79、CWE-78、CWE-97、CWE-90 が含まれます。

インジェクション・カテゴリのその他の CWE には、CWE-610、CWE-652、CWE-643、CWE-943 が含まれ、そのすべてが、意図せぬ動作を招く可能性のある、データまたは特殊要素の不適切な中和に関連しています。

A05:2021 – セキュリティ設定のミス： 36,321 件の脆弱性が特定されており、顧客での蔓延率が最も高くなっています (98%)。

セキュリティ設定のミスに関して特定された脆弱性の大部分 (84%) は、ブラック・ダックのエキスパートによって「情報に関する」脆弱性という名称を付けられました。つまり、この設定により機密情報が開示される可能性はありますが、環境、ホスト、アプリケーションに特定のセキュリティ・リスクがもたらされることはありません。

ただし、この情報には、インストール済みソフトウェア、オープン・ポート、システムとその動作に関する一般的な情報などが含まれる場合があり、悪用の足がかりとなり得ます。組織がセキュリティの強化に向けて、設定変更が必要かどうかを十分な情報に基づいて判断するためには、少なくとも、このような最初の脆弱性の存在を認識しておく必要があります。

業種別に見た脆弱性のトレンド

脆弱性の状況は業種によって大きく異なります。金融および保険では重大な脆弱性の件数が最も多くなっており (1,299 件)、規制の厳しいセクターでの本質的なリスクが明らかになっています。ヘルスケアおよび社会扶助の重大な脆弱性は 2 番目に多く (992 件)、患者データの保護と規制遵守に関する懸念が生じています。情報サービスでは合計 446 件の重大な脆弱性が特定されており、データ中心業界での堅牢なセキュリティの必要性が示されています。

とりわけ、複雑さが小～中程度のサイトは、複雑さがより大きいサイトよりも重大な脆弱性が多い傾向にあり、これは特に金融および保険セクターで顕著でした。このトレンドから、組織が小規模サイトやそれほど複雑でないアプリケーションのセキュリティ要件を軽視している可能性がうかがえます。

これらの調査結果による影響は重大です。金融および保険セクターで確認された多数の重大な脆弱性は、財務損失、規制による罰則、評判の失墜をもたらすおそれがあります。ヘルスケア・セクターの脆弱性は、患者データの侵害により HIPAA などの規制の違反を引き起こす可能性があります。情報サービス企業が直面するデータ漏えいリスクは、顧客の信頼と事業運営を根底から揺るがしかねません。

不十分なトランスポート層の保護のような基本的セキュリティの問題が業種間で広がっていることは、セキュリティ・プラクティスを根本から改善する必要性を示しています。組織は機密データを保護し、規制遵守を維持し、事業運営と評判を守るために、これらの脆弱性の対応を優先する必要があります。

図 5 から、小規模サイトでは重大な脆弱性が最多になることが多く、対応完了までの期間には大きなばらつきがあることがわかります。中規模サイトでは中程度～多数の脆弱性が検出されていることが多く、対応完了までの期間は大きく異なります。大規模サイトでは一般に重大な脆弱性の数は少なく、多くの場合でより速やかにこれらへの対応が完了しています。

業種	サイトの複雑さ	重大な脆弱性	重大な脆弱性の対応完了までの期間 (日数)
農業、林業、漁業、狩猟	小	2	-
	中	0	
	大	0	
鉱業/採石、石油/ガス採掘	小	0	
	中	0	
	大	0	
建設	小	3	234
	中	2	150
	大	1	-
卸売	小	11	20
	中	1	1
	大	0	
不動産および賃貸	小	27	413
	中	4	158
	大	7	1
会社企業経営	小	2	397
	中	2	9
	大	0	-
製造	小	66	14
	中	22	248
	大	2	-
行政支援および廃棄物管理	小	3	5
	中	0	-
	大	1	-
宿泊および食品サービス	小	30	1
	中	33	1
	大	5	1
芸術、エンターテインメント、レクリエーション	小	62	34
	中	87	30
	大	15	63

図 5. 特定された重大な脆弱性の数と対応完了までの期間 (業種およびサイトの複雑さ別)

業種	サイトの複雑さ	重大な脆弱性	重大な脆弱性の対応完了までの期間 (日数)
教育サービス	小	72	342
	中	35	111
	大	69	1
金融および保険	小	565	28
	中	580	53
	大	154	78
ヘルスケアおよび社会扶助	小	367	87
	中	486	30
	大	139	20
情報サービス	小	235	132
	中	140	37
	大	71	111
その他サービス	小	65	38
	中	54	87
	大	4	43
専門、科学、技術サービス	小	124	90
	中	94	36
	大	12	240
行政	小	15	2
	中	40	2
	大	12	9
小売	小	341	63
	中	29	17
	大	6	1
輸送および倉庫	小	21	1
	中	47	13
	大	3	221
公益事業	小	28	107
	中	23	876
	大	4	1

図 5. (続き) 特定された重大な脆弱性の数と対応完了までの期間 (業種およびサイトの複雑さ別)

DAST、SAST、SCA の相互作用

現在の複雑なサイバーセキュリティ環境では、アプリケーション・セキュリティに対する包括的なアプローチが不可欠です。このセクションでは、DAST/SAST/SCA 間の相互作用について考察し、これらの手法が、どのように互いに補完し合って健全なセキュリティ・カバレッジを提供しているかを明らかにします。

特定の脆弱性検出における強みの比較

DAST

- **実行時分析：**DAST が得意とするのは、アプリケーションの実行中のみに顕在化する脆弱性を特定することです。これには、反射型および DOM ベースのクロスサイト・スクリプティング脆弱性など、アプリケーションの実行時の振る舞いに依存する問題が含まれます。
- **実際の攻撃のブラックボックス・シミュレーション：**DAST は外部攻撃者の観点からアプリケーションと相互作用することで、実際の攻撃をシミュレートします。これにより、動的なクエリー構築または複雑なアプリケーションのロジックによって生じる SQL インジェクション脆弱性などの、静的解析では見逃される可能性がある脆弱性を検出します。
- **複雑なインジェクション脆弱性の検出：**SAST はさまざまなインジェクション脆弱性を検出できますが、DAST は特に実行時条件に依存する脆弱性の検出に有効です。たとえば、DAST はアプリケーションと相互作用してその応答を監視することで、LDAP インジェクション脆弱性をより効果的に検出します。
- **悪用可能性の検証：**DAST は、SCA で特定されたサードパーティ・コンポーネント内の脆弱性が、実行中のアプリケーションで曝露され、悪用される可能性があるかどうかを検証できます。
- **継続的監視：**DAST は本番環境で継続的プロセスとして実装できるため、新たにもたらされた脆弱性をリアルタイムで検出できます。この継続的監視は、時間経過により脆弱になる可能性のあるサードパーティ・コンポーネント内の問題を特定し、実行中アプリケーションでのパッチの有効性を検証するために不可欠です。
- **web ベース攻撃の包括的なカバレッジ：**DAST は、不十分なトランスポート層の保護、セキュアヘッダーの欠落、情報漏えいなど、幅広い web ベースの脆弱性を検出します。この包括的なカバレッジは、各種のアタック・ベクターからアプリケーションを確実に保護する上で役立ちます。

SAST

- **早期に検出：**SAST は、アプリケーションが実行状態になる前の開発プロセスの早い段階で潜在的なコーディングの脆弱性を特定します。
- **コード・レベルの解析：**SAST は、クロスサイト・スクリプティングなどの脆弱性をもたらす可能性のある、不適切なエンコードなどの問題を特定します。
- **包括的なコード・カバレッジ：**SAST は、実行時テストでは容易にアクセスできない可能性のある箇所を含めて、コードベース全体を解析できます。
- **特定のインジェクション脆弱性の識別：**実行時に固有のインジェクション問題には DAST の方が効果的な場合が多いものの、SAST は、SQL インジェクション脆弱性の多くの事例に対応しており、特にソース・コード内で明らかな脆弱性を検出できます。
- **コーディング上の欠陥の検出：**SAST は特に、脆弱性につながるおそれのあるコーディング・エラーの特定に長けています。
- **セキュアなコーディング・プラクティス：**SAST は、開発プロセスの早い段階でセキュアなコーディング規約からの逸脱を特定することで、これらの標準とベスト・プラクティスの適用を推進します。
- **費用対効果の高い早期修正：**SAST は開発サイクルの早期に問題を特定することで、より費用対効果の高い、脆弱性の修正を可能にします。

DAST、SAST、SCA を統合するためのベスト・プラクティス

- SAST と SCA を早い段階で (多くの場合、開発プロセス中に) 使用して、潜在的なコーディングの弱点やサードパーティ・ソフトウェアによってもたらされる脆弱性を検出します。
- 本番前の環境でアプリケーションをテストするために DAST を実行し、実行中にのみ現れる可能性のある脆弱性を特定します。
- 実行中のアプリケーションにおける悪用可能性と重大度に基づいて、脆弱性に優先順位を付けます。

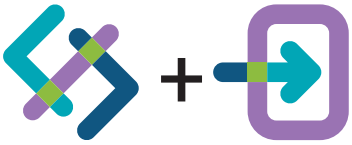
SCA

- **既知の脆弱性の特定：**SCA は、サードパーティ・ライブラリとオープンソース・コンポーネントに含まれる既知の脆弱性を特定するのに長けています。アプリケーションで使用されるコンポーネントを既知の脆弱性のデータベースに対して相互参照することで、潜在的なリスクを迅速に確認します。
- **リスクの優先順位付け：**SCA ツールには多くの場合、脆弱性の重大度と潜在的影響に基づく優先順位付けに役立つリスク評価メカニズムが含まれています。このため、組織は、最初に最も重要な問題の修正に集中できます。
- **依存関係の詳細なインベントリ：**SCA は、すべてのサードパーティ・コンポーネントとアプリケーション内で使用されるバージョンの包括的なインベントリを提供します。この詳細なインベントリは、組織が依存関係の状況を理解し、それを効果的に管理するために役立ちます。
- **脆弱で古くなったコンポーネントの早期検出：**SCA は古くなったコンポーネントやメンテナンスされなくなったコンポーネントを特定するのに特に有効です。
- **ライセンスの遵守：**SCA はセキュリティの脆弱性だけでなく、サードパーティ・コンポーネントのライセンスを識別することで法的リスクの管理にも役立ちます。これにより、組織は使用するオープンソース・ソフトウェアのライセンス条件を確実に遵守できます。
- **開発サイクル内での早期検出：**SCA は開発プロセスの早い段階で組み込めるため、サードパーティ・コンポーネントを本番環境に移行する前に、そこに含まれる脆弱性を特定して対処できます。この早期検出により、ライフサイクルの遅い段階での脆弱性修正に伴うリスクとコストを全般的に削減できます。
- **継続的監視：**SCA ツールは継続的にサードパーティ・コンポーネントを監視して、検出した新しい脆弱性に関する警告を通知します。このため、新たな脅威が出現しても、長期にわたってアプリケーションのセキュリティを確保できます。

それぞれの手法に固有の強みがありますが、真の能力を発揮させるにはこれらを組み合わせて使用することです。今回の分析で示された複雑なセキュリティの問題に対処するには、この包括的なアプローチが不可欠です。

テスト手法の組み合わせによる相乗効果

SAST + DAST



クロスサイト・スクリプティングに関して、SAST は不適切なエンコーディングを特定し、DAST は実行時に固有の事例を捕捉します。SQL インジェクション (例 : CWE- 89) については、SAST は明らかな脆弱性を検出し、DAST が実行時に依存する問題を特定します。

DAST + SCA

SCA がコンポーネントに含まれる潜在的な脆弱性を特定し、DAST は実行中アプリケーションでのその悪用可能性を検証します。DAST は本番環境での継続的監視を提供することで、SCA の静的解析を補完します。また、DAST は、SCA によって特定されたパッチの有効性を実際の実行環境で検証できます。

SCA + SAST

SCA はオープンソースとサードパーティのライブラリに含まれる既知の脆弱性を検出し、SAST はアプリケーションのソース・コード、バイトコード、バイナリ・コードに脆弱性が含まれるかどうかを評価します。この際、アプリケーションを実行する必要はありません。

まとめ

幅広い業種にわたる 1,300 のアプリケーション、システム、サーバーに対して、ブラック・ダックが 2023 ～ 2024 年に実施した DAST 解析の調査結果から、組織のアプリケーション・セキュリティ戦略を強化すべき、差し迫った必要性が明らかになっています。

合計で 96,917 件の脆弱性が特定されましたが、機密データの曝露やインジェクション脆弱性などの重大なカテゴリは、さまざまな業種に著しいリスクをもたらしています。これらの脆弱性は蔓延しており (機密データの曝露の事例が 30,726 件、インジェクション脆弱性の事例が 4,814 件)、組織がセキュリティの取り組みを直ちに優先させる必要があることをはっきり示しています。

DAST はすべての web アプリケーションのセキュリティ問題を解決する「特効薬」ではありませんが、基本的な中心となる要素として SAST および SCA も含む包括的なセキュリティ・プログラムにおいて、決定的な役割を果たします。

SAST は開発プロセスの早い段階でコーディングの欠陥を特定するのに効果的であり、SCA はサードパーティ・コンポーネントに関する有益な情報を提供します。さらに、DAST は実行時の脆弱性を検出し、検出した問題の悪用可能性を検証することを得意としています。これらの手法の相互作用により、組織のセキュリティ態勢をより全体的にとらえ、その他の方法では見逃される可能性のある脆弱性に対処できるようになります。

本番前環境と開発環境に関しては、DAST ソリューションを CI/CD パイプラインに統合できるため、早期に脆弱性を特定することで改善を前倒しして修正コストを削減することができます。このアプローチは、インジェクション脆弱性やサービスおよびコンポーネント間の予期せぬ相互作用など、実行中のアプリケーションでのみ表面化する問題を検出するために特に役立ちます。

本番環境での DAST の使用は、特に複雑で動的なアプリケーションを使用する組織や厳しく規制された業界の組織に追加のメリットをもたらします。本番の DAST は継続的監視を提供することで、構成変更、新たに発見されたエクスプロイト、アプリケーション実行時環境の変更に起因する脆弱性を検出します。これは特に、時間とともに脆弱化する可能性のあるサードパーティ・コンポーネントの問題の特定や、実際の本番環境でのパッチの有効性の検証に有効です。

脅威の状況がますます複雑化する中で、組織がアプリケーション・セキュリティに多面的なアプローチを取り入れることが急務になっています。これには、開発およびデプロイ・プロセスへの DAST、SAST、SCA の統合が含まれます。多面的なアプローチの採用により、組織はより効果的に脆弱性を特定して修正し、顧客の信頼を維持しながら規制要件を遵守することができます。

このレポートの調査結果から極めて明確なように、あらゆる業種の組織は、セキュリティ態勢を強化するために先を見越した措置を講じる必要があります。こういった対策を実施することで、組織がさらされるリスクを大幅に軽減し、機密データと重要なシステムを新たな脅威からさらに効果的に保護できるようになります。

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。