デジタル社会推進実践ガイドブック　DS-221

政府情報システムにおける

脆弱性診断導入ガイドライン（案）

2024（令和6）年1月DD日

デジタル庁

〔~~標準ガイドライン群ＩＤ~~ドキュメントの位置付け〕

~~DS-221~~Informative

参考とするドキュメント

〔キーワード〕

セキュリティ、脆弱性、脆弱性診断

〔概要〕

政府情報システムの関係者が脆弱性診断を効果的に導入するための基準及びガイダンスを提供する。

改定履歴

改定年月日	改定箇所	改定内容
2022年6月30日	-	初版決定
2024年1月N日	1.1	・政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）の改定に伴い記載を変更
	1.2	・Webアプリケーションプログラミングインターフェイス（Web API）の診断に関する記載を追加
	2.2	・OWASP Mobile Application Security Verification Standard (MASVS)の改定に伴い記載を変更
	2.3	・診断を実施するセキュリティベンダーの脆弱性検出能力を測る手段として、国内外の脆弱性届出制度や開発者等への報告及び調整実績を記載 ・脆弱性の深刻度評価におけるCVSS（Common Vulnerability Scoring System）のバージョン指定を廃止
	3	・政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）の改定に伴い記載を変更
	3.2	・政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）の改定に伴い記載を変更 ・各機関が保有するインベントリの見直し方法にASM（Attack Surface Management）を追加
	3.3	・OWASP Mobile Application Security Verification Standard (MASVS)の改定に伴い記載を変更 ・セキュリティベンダーの脆弱性検出能力を測る手段として、国内外の脆弱性届出制度や開発者等への報告及び調整実績を記載 ・脆弱性の深刻度評価におけるCVSS（Common Vulnerability Scoring System）のバージョン指定を廃止 ・定期診断を実施する際の留意点を追加 ・検出した脆弱性の深刻度評価に際し、CVSSの評価根拠の明記を求める旨を追加
	付録A	・政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）の改定に伴い記載を変更 ・OWASP Mobile Application Security Verification Standard (MASVS)の改定に伴い記載を変更 ・各脆弱性を診断する際の諸条件を記載
	付録B	・政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）の改定に伴い記載を変更 ・参考資料を更新

目次

１　はじめに

社会全体のデジタルトランスフォーメーションが加速し、我々を取り巻く様々な分野において ICT の利活用が進んでいる。他方、サイバー攻撃はその発生頻度の増加と高度化が続く状況下にあり、サイバーセキュリティ対策のさらなる強化が不可欠となってきている。こうした中で、政府情報システムに対しても、今後、サイバー攻撃の脅威は高まっていくことが予想される。

政府情報システムは国民生活や行政の活動の根幹を支える基盤であり、これらのシステムにおけるインシデントは社会基盤の機能停止に直結するリスクがある。このため、令和 3 年度に閣議決定されたサイバーセキュリティ戦略[1]に基づき、任務及び機能の自律性の毀損に繋がるおそれのあるサイバー空間の脆弱性を把握し、その信頼性確保に向けた取り組みが必要となる。

多くの政府情報システムでは、これまでにも脆弱性やセキュリティリスクの特定を目的として脆弱性診断を導入してきているが、その診断対象や診断サービスの選定に明確な基準や指針があるとは言えない状況にある。

脆弱性診断の実施においては、診断に対する正しい理解を持ち、高度な専門性に加え、安全性確保のための体制を有する適切なセキュリティベンダーから診断サービスを調達する必要がある。また、診断の手法は多岐に渡り、一つの手法でシステムのセキュリティリスクの全体像を把握することは困難であることから、適切な診断手法を組み合わせて行う必要がある。さらに、脆弱性診断は実施するだけでなく、検出されたセキュリティリスクを基点としてシステムや組織の弱点を見直し、セキュリティの実施計画の改善や強化につなげることが重要となる。このような観点を踏まえ、本書では、政府情報システムの関係者が脆弱性診断を円滑かつ効果的に進めるための基準及びガイダンスを提供する。

１．１　目的とスコープ

本書は、政府情報システムに対する脆弱性診断を効果的に実施することを目的として、政府情報システムの管理責任や各機関のセキュリティ管理を担う職員に対して、脆弱性診断を実施する際の基準及びガイダンスを提供するものである。各機関では、本書を参考に脆弱性診断の実施計画の立案、調達を行うことが望ましい。また、既に脆弱性診断を実施している機関では、実施してきた診断内容を見直す際の参考にすることが望ましい。

本書で述べる基準は令和 ~~3~~5 年度版の「政府機関等のサイバーセキュリティ対策のための統一基準群[2]」（以下、「統一基準群」という。）の「政府機関等の対策

[1] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf

[2] https://www.nisc.go.jp/policy/group/general/kijun.html

基準策定のためのガイドライン（令和５年度版）[3]」における「脆弱性検査を含む情報セキュリティの観点での試験を実施」（基本対策事項 5.2.2(1)-1 f)）やウェブアプリケーションを運用段階へ移行する前に実施する「脆弱性診断」（基本対策事項 6.6.1(3)-2)、アプリケーション・コンテンツの運用時における「定期的に脆弱性対策の状況を確認」（遵守事項 6.6.1(4)(b)）、ソフトウェアに関する脆弱性対策を目的とした「脆弱性診断~~を実施~~」（基本対策事項 7.2.1(1)-1）並びに「定期的な脆弱性診断」（基本対策事項 7.2.1(1)-6）における実施基準としての活用を想定する。また、「自己点検の実施」（遵守事項 2.3.1(2)(a)）を背景に点検の手段として脆弱性診断を行う際や、情報セキュリティ監査における「実際の運用が情報セキュリティ関連規定に準拠していること」（~~遵守事項~~基本対策事項 2.3.2(2)-2 c)）の確認手段として脆弱性診断を取り入れる際の実施基準としての活用も想定に含む。

１．２　適用対象

本書は、政府情報システムにおいて広く導入されている以下の 3 種類の脆弱性診断を適用対象とする。

- プラットフォーム脆弱性診断（以下、「プラットフォーム診断」という。）
  サーバやネットワーク機器等に対して行う脆弱性診断を示す。
- Web アプリケーション脆弱性診断（以下、「Web アプリ診断」という。）
  Web アプリケーション（以下、「Web アプリ」という。）や Web アプリケーションプログラミングインターフェイス（以下、「Web API」という。）に対して行う脆弱性診断を示す。後者の Web API に対する診断は API 診断等のサービス名称で提供されることがあるが、本書では同義のものとして扱う。
- スマートフォンアプリケーション脆弱性診断（以下、「スマートフォンアプリ診断」という。）
  Google Android や Apple iOS/iPadOS 端末上で動作するスマートフォンアプリケーション（以下、「スマートフォンアプリ」または「アプリ」という。）に対して行う脆弱性診断を示す。

なお、本書は脆弱性診断の導入に対する理解を深めるための参考文書であり、適用の遵守を求めるものではない。

[3] https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

１．３　位置づけ

~~本書は、標準ガイドライン群の一つとして位置づけられる。~~本文書は、標準ガイドライン群の Informative（情報提供）のレベルの参考文書である。

１．４　本書の構成

２章では、脆弱性診断を推進する上で必要となる基本的な事項を概説する。はじめにシステムの脆弱性対策における脆弱性診断の位置付けを示し、次に脆弱性診断の手法の違いや診断サービスを選定し実施する上での留意事項を示す。

３章では、２章を踏まえ、政府情報システムにおける脆弱性診断の実施基準を示す。この中では、システム開発段階で実施する診断に加え、自己点検や情報セキュリティ監査を目的として定期的に脆弱性診断を行う際の実施要件も示す。

２　脆弱性診断の概要

本章では、脆弱性診断を効果的に推進する上で必要となる基本的な事項を解説する。脆弱性診断はシステムにおけるセキュリティ上の弱点を特定するものであるが、診断のみでシステムのセキュリティリスクを防ぐことはできない。また、脆弱性診断は既に作り込まれた脆弱性を検出するものであるが、それ以前に脆弱性の発生を未然に防ぐことが肝要である。こうした背景から、脆弱性診断は他のセキュリティプロセス（パッチマネジメントやセキュアコーディング、セキュリティレビュー等）と組み合わせて実施することが望ましい。さらに、脆弱性診断の検出結果をセキュリティプロセスそのものの改善に役立てていくことが望ましい。

２．１　脆弱性対策における脆弱性診断の位置付け

本節では、はじめにシステムの脆弱性対策全体を俯瞰し、その中における脆弱性診断の位置付けを明らかにする。図　２－１は、システムにおける脆弱性を集合として表したものである。

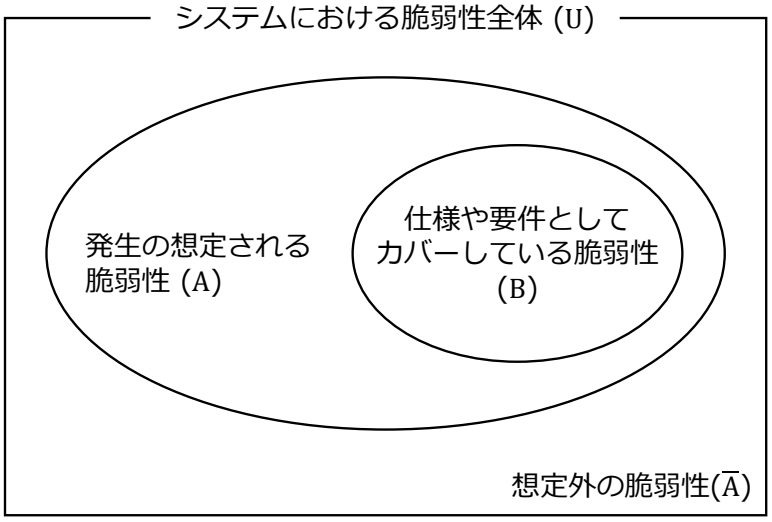

図　２－１　システムにおける脆弱性の分類

図　２－１では、次の集合を定義している。

・システムにおける脆弱性全体（U）
当該のシステムにおいて本来対処すべき脆弱性の母集団と定義する。サイバー攻撃の高度化や新しい攻撃手法の発見、システム構成の複雑化等の複合的な要因により、(U)は時間とともに増えていく構造にある。

・発生の想定される脆弱性（A）
脆弱性の母集団(U)のうち、システム開発に関わるステークホルダーが発生を予期できる脆弱性の集合を(A)と定義する。(A)には、過去に検出されたことのある脆弱性や一般的によく知られている脆弱性等が含まれる。往々にして、(A)の集合の大きさはシステムに携わる者の知見に左右される。政府機関においては、外部有識者の知見を活用し、組織や開発プロセスを通じて(A)を補強していく必要がある。また、母集団(U)が拡大を続けていく中、最新の脅威情報に基づき、常に(A)を最新化していくことが必要である。
・仕様や要件としてカバーしている脆弱性（B）
集合(B)は発生の想定される脆弱性(A)の部分集合にあたり、各機関の情報セキュリティポリシーや開発の要件定義等において発生を防ぐための対策が求められるものである。対策内容が明示的であることから、仕様や実装に適切に反映されていること（トレーサビリティ）の確認や、対策状況について第三者による確認や検証が可能である。理想的には(B)を(A)に近づけていくことが望ましいが、(A)には有識者ならではの暗黙的な知見や、汎化や明文化の難しい各システム固有の脅威も含まれることから、部分的とならざるを得ない状況にある。
・想定外の脆弱性($\overline{A}$)
集合($\overline{A}$)は、システム開発に関わるステークホルダーでは発生の予期できない脆弱性である。システムを運用していく中では、予期しない脆弱性が常に発生しうることを認識しておくことが重要である。サイバー攻撃に悪用される脆弱性は母集団(U)であることから、攻撃を防ぐためには、発生を予期できる脆弱性(A)を(U)に近づけて行くための取り組みや、攻撃者の目線から($\overline{A}$)の存在をテストするといった取り組みが必要となる。

上記の構造を踏まえた上で、脆弱性診断は発生の想定される脆弱性(A)の確認を目的として実施することが望ましい。これには、仕様や要件としてカバーすべき脆弱性(B)として本来対処すべきであったものの漏れを検出することや、発生が想定される脆弱性(A)のうち政府機関内の知見ではカバーできていなかったものを検出することが含まれる。

脆弱性診断そのものは既に発生してしまった脆弱性を検出するものであることから、セキュリティ・バイ・デザイン等の取り組みを強化し、脆弱性が作り込まれない状態を目指していくことが重要である。また、脆弱性診断は対象システムにおける将来の脆弱性の発生を防ぐものではないことから、診断で検出され

た脆弱性はシステム開発の要件定義や組織のセキュリティプロセスに反映し、(B)の対策の強化につなげていくことが望ましい。

想定外の脆弱性(Ā)の対策には脆弱性報奨金制度により未知の脆弱性の検出を試みること等が挙げられるが、本書のスコープからは除外するものとする。(Ā)の対策は際限なく実施できるため、システムが侵害された際のリスクや費用対効果を鑑み、対策の実施内容を決めることが望ましい。

２.２　一般的な脆弱性診断の種別

図　２−２は、システムに脆弱性が混入しうる箇所を部位ごとにまとめたものである。

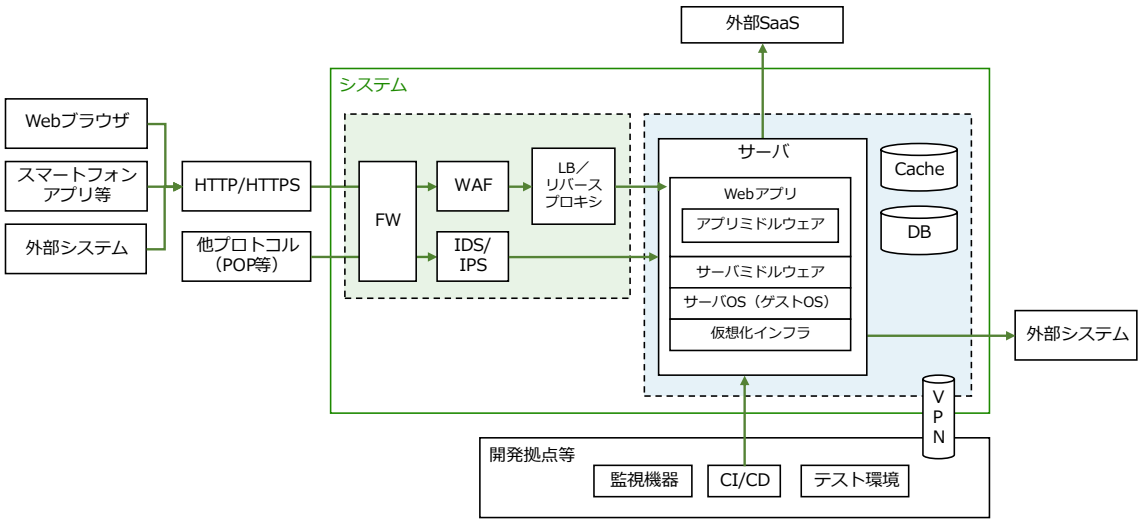

図　２−２　情報システムにおける脆弱性の発生部位

図　２−２が示すとおり、脆弱性の発生箇所はシステムの広範に渡る。攻撃のアクターはこれら全体の中から脆弱性を見つけ出し悪用しうることから、その対策もまたシステム全体を網羅的に行う必要がある。セキュリティベンダーが提供する診断サービスもまた、診断対象の部位に応じてサービスが分かれている。

本書が対象とする３種類の脆弱性診断は、図　２−２の次の部位を対象とする。上記の脆弱性診断は、脆弱性の発生部位に応じて組み合わせて行う必要がある。

- プラットフォーム診断
  FW（ファイアウォール）、LB（ロードバランサ）、リバースプロキシ、仮想化インフラ、サーバ OS（ゲスト OS）、サーバミドルウェア、VPN
- Web アプリ診断
  Web アプリ、アプリミドルウェア
- スマートフォンアプリ診断
  スマートフォンアプリ

昨今は VPN 機器や外部ネットワークに接続されている複合機等が攻撃の起点として狙われていることから、これらも診断対象とする必要がある。また、連携する外部システムも侵入の糸口となるおそれがあることから、脆弱性診断の実施状況等を確認することが望ましい。

1)プラットフォーム診断

プラットフォーム診断は、対象のサーバやネットワーク機器等に対して疑似的な攻撃の通信を行うことにより、脆弱性やセキュリティリスクの有無を確認するものである。一般的には自動化されたツールを用いて診断を行い、誤検出（偽陽性）の精査やツールでは検出できない脆弱性の診断を人手で補う。

プラットフォーム診断では、主に表 2-1のようなセキュリティ上の問題が検出される。

表 2-1　プラットフォーム診断で検出される脆弱性

脆弱性の種別	概要
不要ポートの開放	ポートスキャンにより通信可能なポートを確認する。結果として、外部からの接続を意図していないオープンポートや、第三者に仕掛けられたバックドア等の不審なサービスが検出される。
脆弱なソフトウェアの利用	上記で検知したオープンポートに接続を試み、サーバから取得したバナー情報に基づき、ポートを待ち受けている OS やミドルウェアの情報を推定する。結果として、既知の脆弱性を含むバージョンのソフトウェアの利用等が検出される。
設定の不備	主にツールに搭載されたシグネチャに基づき、サーバの設定不備を確認する。結果として、推測可能なパスワード（システムの初期パスワード等）や意図しない情報の公開等の問題が検出される。
プロトコル固有の脆弱性	主にツールに搭載されたシグネチャに基づき、プロトコル固有の脆弱性を確認する。結果として、DNS、FTP、SSH、POP、SMTP、TELNET、SSL/TLS 等のプロトコルを扱うソフトウェアの脆弱性や、脆弱なアルゴリズムの利用等が検出される。

プラットフォーム診断には、外部診断（リモート診断）と内部診断（オンサイト診断）が存在する。外部診断は、グローバル IP アドレスを通じてインターネットからアクセス可能な装置を対象とし、セキュリティ境界の外側より攻撃者

が悪用可能な脆弱性を明らかにすることを目的とする。一方の内部診断は、システム内のネットワークや拠点のLAN内等における主にプライベートIPアドレスを有する装置を対象とし、セキュリティ境界の内側で、内部犯や境界防御を超えて侵入した外部の攻撃者により悪用されうる脆弱性を明らかにする。

過去に診断を実施していない場合、優先して実施すべきは外部診断である。外部診断の場合、診断対象はグローバルIPアドレス単位となり、診断の費用はIPアドレス数に応じて変動する。内部診断もまた、診断対象のIPアドレス数に応じて費用が変動する。また、現地に出向いて診断を行うことに対する追加費用が生じることがある。

新しい脆弱性や攻撃手法は日々公表されるため、診断サービスの選定においては、最新の脆弱性情報を収集し診断項目に反映させていることの確認が必要である。また、ツールの検出結果には誤検出や実際には攻撃の困難な指摘事項が含まれうるため、診断対象のシステムに対する現実的な攻撃の発生可能性に基づいて対応要否を判断する必要がある。

2)Webアプリ診断

Webアプリ診断は、対象のWebアプリ（Web APIを含む）に対して疑似的な攻撃のリクエストを行うことにより、情報漏えいやサイト改ざん等につながる脆弱性の有無を確認するものである。診断手法には、ツールによる自動診断、専門家による手動診断、両者を併用するものの3種類が存在する。情報処理推進機構（IPA）の「安全なウェブサイトの作り方[4]」等のセキュリティ標準への準拠を謳う診断サービスも存在する。

Webアプリ診断では、主に表 2-2のような脆弱性が検出される。

表 2-2 Webアプリ診断で検出される脆弱性

大分類	分類	脆弱性の例
(A)Webアプリの仕様に起因する脆弱性	(A-1)固有のビジネスロジックに依存するもの	ID連携の不備により他のユーザになりすましができる等
	(A-2)一般的な仕様上の不具合	他人のデータを読み書きできる、管理者権限の機能を誰でも利用できる、パスワードリセット機能の悪用、認証の回避等
(B)Webアプリの実装に起因	(B-1)実装のメカニズムに対する高度な理解が要求され	レースコンディションによるデータの不整合、Officeファイルの投稿機能における XML 外部エンティティ参照（XXE）、電

[4] https://www.ipa.go.jp/security/vuln/websecurity.html

大分類	分類	脆弱性の例
する脆弱性	るもの	子署名の迂回等
	(B-2)一般的な実装の不備	SQL インジェクション、ディレクトリトラバーサル、クロスサイトスクリプティング等
(C)利用する Web アプリミドルウェア固有の脆弱性		ログ出力や画像変換ライブラリ等における既知の脆弱性の悪用、CMS（Content Management System）や Web アプリケーションフレームワークの誤用に起因する脆弱性等

ツールによる自動診断は効率の観点では有用であるが、仕様に起因する脆弱性(A)全般の検出が難しい。また、実装上の問題(B)の中でも、対象の Web アプリの内部実装に対する深い洞察を要する脆弱性(B-1)や、一般的な実装の不備による脆弱性(B-2)においても一定の制限を迂回しなければ攻撃できないものが見落とされやすいため、専門家の人手による診断で補強する必要がある。

セキュリティ標準に基づく診断サービスも、テストのカバレッジを確認する用途では有用であるが、これらの標準がカバーするのは多くの Web サイトに見られる一般的な脆弱性(A-2)(B-2)に留まることから、専門家の知見に基づき、対象の Web アプリに固有の脆弱性(A-1)(B-1)を診断する必要がある。

情報システムの開発では、Web アプリケーションフレームワークや CMS 等の様々なサードパーティのミドルウェアが利用されるため、これらに固有の脆弱性(C)が検出できることも重要である。この中には、個々のミドルウェアが提供する機能の誤用や設定の誤りにより発現するものが含まれるため、システムの利用するミドルウェアの内部構造に精通した専門家による診断が必要となる。

過去に診断を実施していない場合、優先して実施すべきはインターネットからアクセス可能な箇所である。この場合の診断は、対象の外部公開機能に対してインターネットを通じて行われる。診断対象は主に画面数や API 等のリクエスト数単位となり、診断の費用もこれらの数によって変動する。

3)スマートフォンアプリ診断

スマートフォンアプリ診断は、Android や iOS/iPadOS 端末上で動作するアプリの脆弱性の有無を確認するものである。診断対象にはアプリ本体に加え、アプリとサーバとの間の通信等も含まれる。診断手法にはアプリ本体をツールで自動解析するものや、リバースエンジニアリングを用いるもの、アプリとサーバ間の通信内容に着目し脆弱性を探索するもの等がある。

スマートフォンアプリ診断で検出される脆弱性の発生箇所を図 2-3に示す。

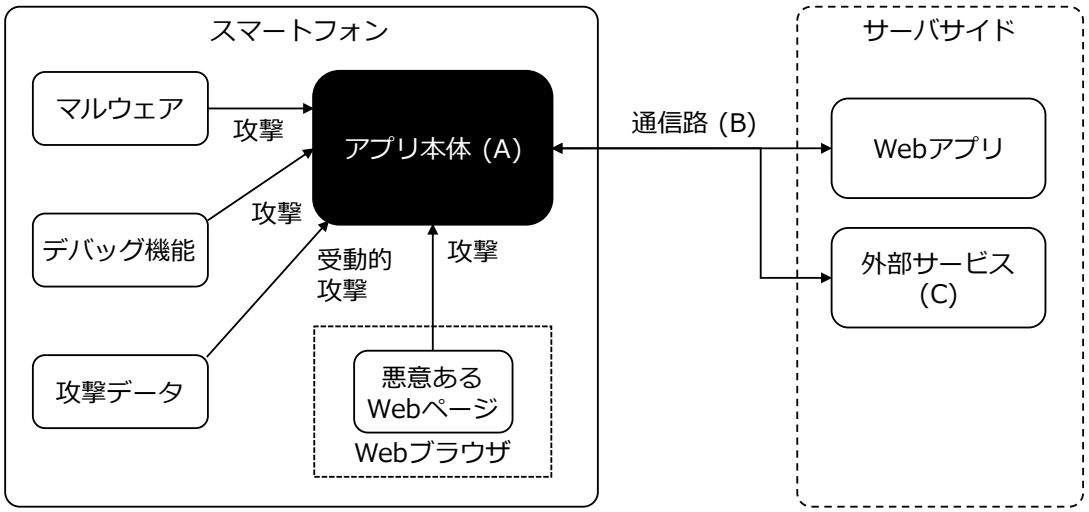

図 2-3 スマートフォンアプリにおける脆弱性の発生箇所[5]

図 2-3の(A)～(C)において検出される脆弱性の代表例は以下の通りである。

表 2-3 スマートフォンアプリ診断で検出される脆弱性

脆弱性の発生部位	脆弱性の例
アプリ本体(A)	・他のアプリから機密情報を参照される ・カスタムURLスキーム等のアプリ間連携機能により意図しない機能が実行される ・WebView（アプリ上にWebページを表示する機能）上で悪意のあるWebページを開かされる
通信路(B)	・サーバ証明書の検証不備 ・平文による機密情報の送受信
外部サービス(C)	・アプリにハードコードされた認証情報を用いて外部サービスに不正アクセスされる ・アプリにハードコードされたURLを通じて、脆弱な設定のクラウドストレージやMBaaS（Mobile Backend as a Service）の存在が特定される

診断サービスを選定する際は、上記の(A)～(C)に述べた発生部位の脆弱性が

[5] 一般社団法人日本スマートフォンセキュリティ協会「Androidアプリのセキュア設計・セキュアコーディングガイド」（https://www.jssec.org/dl/android_securecoding/）を基に筆者作成

網羅されることを確認する必要がある。また、ツールによる自動解析では実際には悪用できないものが脆弱性として指摘される場合があるため、攻撃の実証までを行う診断サービスを選定することが重要である。さらに、昨今 JVN[6]等で公表されている脆弱性にはアプリに認証情報がハードコードされている等のリバースエンジニアリングにより発見されるものが見られることから、脆弱性を未然に防ぐためには、ソースコードレビューやリバースエンジニアリング等の手法が含まれる診断サービスを選定する必要がある。

スマートフォンアプリは各利用者の端末上で実行されることや、アプリ本体を容易に解析可能であることから、セキュリティを確保することが難しい。様々な脅威を全て対策することは不可能であり、また対策にかかる費用も高額となることから、費用対効果に応じて対策を行うことが望ましい。~~こうした背景から、OWASP の「モバイルアプリケーションセキュリティ検証標準（MASVS: Mobile Application Security Verification Standard）[7]」では、以下の 3 段階の対策レベルを定め、各々のレベルの対策内容を定義している。~~

~~・MASVS-L1~~
~~標準セキュリティレベルであり、スマートフォンアプリにおけるセキュリティのベストプラクティスに準拠する。全てのスマートフォンアプリに適している。~~

~~・MASVS-L2~~
~~多層防御に位置付けられ、標準的な要件を超える高度なセキュリティコントロールを導入する。モバイルバンキングアプリ等の機密性の高いデータを処理するアプリに適している。~~

~~・MASVS-R~~
~~リバースエンジニアリングと改ざんへの耐性を有するレベルであり、アプリに対する様々な攻撃に対して耐性を有する。モバイルゲーム等のように知的財産の保護やアプリの改ざんを防止する必要のあるアプリに適している。~~

~~MASVS では、MASVS-L1 は全てのアプリにおいて準拠を求める一方で、MASVS-L2 以上のプラクティスは費用対効果に応じて取捨選択することを推奨している。脆弱性診断においても、多くの情報システムにおいては、MASVS-L1 相当の水準で診断を行うことが望ましい。~~

---

[6] https://jvn.jp/

~~[7] https://owasp.org/www-project-mobile-security-testing-guide/~~

4) その他の脆弱性診断

これまでに述べた脆弱性診断の他にも、様々な種類の診断サービスが存在する。情報システムではなく制御システムや IoT 機器を対象とするもの、システムではなく物理環境、組織とその従業員を対象とするもの等が登場してきている。これらの診断については、政府情報システムにおける導入の必要性が高まってきた際に、適宜、本書のスコープに加えるものとする。

２．３　脆弱性診断を行うにあたっての留意事項

1) 脆弱性診断サービスの選定

高度化するサイバー攻撃の脅威を未然に防ぐためには、十分な経験と能力を有したセキュリティベンダーの選定を要することから、選定に際しては経済産業省の定義する「情報セキュリティサービスに関する審査登録機関基準[8]」を満たすことの確認に加えて、脆弱性を検出する能力を測るため、ペネトレーションテストの国際資格の保有状況や CTF（Capture The Flag）等のセキュリティコンテストにおける上位入賞実績、国内外の脆弱性届出制度[9]や開発者等への報告及び調整実績 ~~CVE（Common Vulnerabilities and Exposures）の付与された脆弱性の発見数等~~を問い合わせること等が有効である。また、診断サービスの調達においては、上記の基準に沿った有識者や有資格者が、診断の実施の中で、どのような役割として、何名、どの期間に関わる予定であるかを確認することが望ましい。

診断サービスの選定においては、ツールによる自動的な診断のみでは不十分であり、専門家による手動による診断との併用が不可欠である。また、手動の診断においても、事前に定義された脆弱性を網羅的に検出することに加え、専門家の知見に基づきリスクベースで追加の脆弱性検出を試みるサービスを併用することが必要である。

脆弱性診断の推進においては、システムの非公開情報や検出した脆弱性をはじめとする機密性の高い情報を取り扱うこととなるため、統一基準群に基づき、情報管理体制を有することの確認が必要となる。また、診断におけるシステムへの影響を最小化するための仕組みやルールの有無に加え、診断を行う要員にルールを遵守させるための取り組みを備えていることを確認することが望ましい。

2) 検出された脆弱性の深刻度評価

診断により検出された脆弱性は、保有するシステムに対するリスク評価に基

---

[8] https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun.pdf

[9] 国内では情報セキュリティ早期警戒パートナーシップ等が該当

づき、優先度を定め対応する必要がある。こうした脆弱性の評価において世界的に活用されているのはFIRST(Forum of Incident Response and Security Teams)が公開するCVSS（Common Vulnerability Scoring System）~~v3.1~~[10]である。CVSS~~v3.1~~では、脆弱性そのものの技術的な深刻度を評価する基本評価基準（Base Metrics）~~と~~に加え、攻撃コードの出現状況や~~等の現状のリスクを算定する現状評価基準（Temporal Metrics）、そして~~対象のシステム環境において想定される脅威~~に応じて最終的なリスクを算定する環境評価基準(Environmental Metrics)の3軸~~に基づき、0.0～10.0までのスコアで脆弱性の深刻度を評価する。また、このスコアに応じて、深刻度を以下の5段階で表現している。

表 2-4 CVSS~~v3.1~~のスコアと深刻度

CVSS~~v3.1~~スコア	深刻度
9.0～10.0	緊急（Critical）
7.0～8.9	重要（High）
4.0～6.9	警告（Medium）
0.1～3.9	注意（Low）
0.0	なし（None）

脆弱性診断では、検出された脆弱性の深刻度をCVSS~~v3.1~~の基本評価基準で評価することが多い。しかし、基本評価基準はあくまでもその脆弱性の技術的特性を示すものであり、それ単体で対応の優先度を決めるべきものではない。基本評価基準を参考に自身のシステム環境において想定される具体的なリスクに基づいて対応の優先度を定めることが望ましい。セキュリティベンダーによっては、独自基準で脆弱性の深刻度を評価する場合がある。こうした場合も、CVSS~~v3.1~~の基本評価基準と同等のものとして扱い、自身のシステムにおけるリスク評価を行う必要がある。

3)脆弱性診断に伴うリスク

脆弱性診断は対象のシステムに対して疑似的な攻撃を仕掛けるため、システムに影響を与えるおそれがある。診断の実施においては、システムに発生しうるリスクを認識し、事前に関係者との間でリスクの低減に向けた取り組みを行う必要がある。生じうるリスクには以下のようなものが挙げられるが、他にも予期しない問題が生じる可能性がある。

・診断の通信によるネットワーク通信帯域の圧迫

[10] https://www.first.org/cvss/

・システムのクラッシュ等に伴うサービス停止
・疑似攻撃のペイロードを含むダミーデータのデータベースへの残存
・大量のメール送信の発生
・データの破損や損失
・脆弱性の検証に伴う個人情報や機密情報の意図せぬ閲覧
・攻撃の検知やエラーの大量発生等に伴う監視アラートの発生

これらのリスクを低減するため、本番環境ではなく検証環境で診断することや、本番環境で行う場合は事前のデータバックアップ等を検討する。また、業務への影響を避けるため、休日や夜間、メンテナンス時間帯等に診断を行うことも考慮し、その旨を発注時にも明記する。診断の開始前には、異常発生時のエスカレーションルールや事業継続計画（BCP: Business Continuity Plan）を確認しておくことで、万が一障害が発生した際、迅速な対応が可能となる。

テストを行う際は、影響を受けるおそれのある全ての関係者に対して、事前に周知と診断可否の確認を行う。この際の関係者には主に以下を含むが、対象のシステムによって異なる。

・対象システムの責任者（システムオーナー）
・対象システムの開発や運用者
・対象システムの負荷や異常監視を行う者
・インフラ提供者（クラウドサービスプロバイダー等）

特にインフラ提供者によって禁止されている診断項目や、関係者がリスクを許容できない診断内容は実施を避ける必要がある。プラットフォーム診断等においてサービス妨害（DoS: Denial of Service）の脆弱性を診断する必要がある場合は、明示的に確認を行い、関係者の許可を得る必要がある。診断を行うセキュリティベンダーにも、安全管理の指針を組織として有することの確認や、安全対策に関する項目を盛り込んだ契約を締結する。

３　政府情報システムにおける脆弱性診断の実施基準

本章では、政府情報システムに対して脆弱性診断を行う際の実施基準を示す。ここでは診断を実施する目的の違いに着目し、以下 2 種類の診断施策を定義する。これらの診断は目的に応じて組み合わせて実施することを想定しており、一方の診断を代替するものではない。

・構築時診断
各システムの構築時に行う診断で、脆弱性対策の実施内容の確認やセキュリティ品質の確保を目的として実施するものを示す。各システムの情報セキュリティ責任者や PJMO 等が、統一基準群に従い~~の求める~~自身の Web アプリを運用段階へ移行する前に脆弱性診断を実施する場合や、ソフトウェアに関する脆弱性対策の一環として~~に従い~~、自身の管理するシステム、あるいは新たに設置したサーバ装置、端末及び通信回線装置に対して~~における~~脆弱性診断を~~対策の一環として~~実施する場合~~こと~~を想定する。各システムの開発にあたる者は、システムの構築や更改時に適切な診断が行われるようにするため、本章の基準に従い、調達仕様書等に脆弱性診断要件を明記するものとする。

・定期診断
各機関で定期的に実施する診断で、各システムの脆弱性対策が適切に実施されていることの点検や監査を目的として実施するものを示す。統一基準群の求める情報セキュリティ対策における自己点検や情報セキュリティ監査の一環として自組織のシステム全体を視野に実施する場合、自身の管理するシステムの運用時の対策として行う場合等を想定する。各機関で定期点検や監査にあたる者は、適切な脆弱性診断が行われるようにするため、本章の基準を参考に、脆弱性診断の実施方針を定義するものとする。

３．１　脆弱性診断の対象システム

1)構築時診断

新規構築または機能追加等の改修を行ったシステムを対象とする。ただし、Web アプリとスマートフォンアプリに対する脆弱性診断は、変更が軽微である場合の実施を任意とする。実施要否の判断の目安として、以下の変更が行われた場合には診断を行うことが望ましい。

ア　Web アプリ診断

・外部から入力されたデータの処理（フォームや API 等）に追加や変更がある場合
・動的な画面生成処理に追加や変更がある場合
・認証、暗号化、ファイルアップロード等、実装に注意を要する処理に追加や変更がある場合
・開発を担当するベンダーに変更がある場合

イ　スマートフォンアプリ診断

・ネットワーク通信に関する処理に追加や変更がある場合
・認証、暗号化等のセキュリティ機能に追加や変更がある場合
・アプリ間連携機能（カスタム URL スキーム等）に追加や変更がある場合
・開発を担当するベンダーに変更がある場合

2)定期診断

定期診断の対象システムは各機関の自己点検や監査計画に準ずるものとし、本書では選定の基準を設けないものとする。保有するシステムが多く、全てのシステムの診断を行うことが難しい場合は、最高情報セキュリティアドバイザー等の有識者に相談の上、各システムのセキュリティリスクの大きさや過去の脆弱性診断の実施状況等を踏まえた総合的な判断を行うことが望ましい。

３．２　脆弱性診断の実施範囲

1)構築時診断

当該のシステムに対する外部攻撃のリスク低減を行う目的から、外部から攻撃を受ける可能性のある箇所（アタックサーフェス）の全てを診断の対象とする。外部との接続点を持たない箇所に対する診断は、システムの脅威環境に応じて任意で実施とする。また、実際の脅威への耐性の確認を目的として、診断対象は本番環境を前提とする。システムに対する影響を許容できない場合は検証環境等での実施も可能とするが、この場合、当該環境のシステム構成が本番環境と同等であることとする。ただし、侵入防止システム（IPS: Intrusion Prevention System）や WAF（Web Application Firewall）については、脆弱性の存在を隠蔽してしまうおそれがあることから、診断時は無効化しておくことが望ましい。これらの前提を踏まえ、各診断の対象を以下に定義する。実際の診断範囲は、以下の基準に基づき、対象システムの内部構成を把握する開発担当者を交えて検討

の上、決定するものとする。

ア　プラットフォーム診断

(1) 追加や構成の変更が生じた全ての外部公開 IP アドレス（グローバル IP アドレス）を診断の対象とする（必須）
(2) 診断対象は本番環境とする。システム構成が本番環境と同等である場合に限り、検証環境等での診断を可能とする（必須）
(3) IPS や WAF は脆弱性の存在を隠蔽するおそれがあるため、無効化した上で診断を行う（推奨）
(4) グローバル IP アドレスを持たない装置に対する診断は、システム内部のネットワークの脅威環境に基づき、必要に応じて実施とする。実施を推奨する例としては、複数の異なるサブシステムが相乗りして利用するマルチテナント型のシステムが挙げられる。この場合は、システムを利用する一つのテナントが侵害を受けた際、他のテナントに対して侵害が及ぶ可能性を確認することを目的として、内部診断を行うこととなる（任意）

イ　Web アプリ診断

(1) 新規追加や変更の生じた全ての外部公開インタフェース（動的画面や API 等）を診断の対象とする。外部公開とは、ネットワーク層での送信元 IP アドレス制限やクライアント証明書等によるアクセス制限等が施されておらず、インターネットから HTTP（WebSocket を含む）による何らかの通信が可能であるものを示す（必須）
(2) 他のシステムと連携する場合は、その外接箇所も診断の対象とする（推奨）
(3) IPS や WAF は脆弱性の存在を隠蔽するおそれがあるため、無効化した上で診断を行う（推奨）
(4) ネットワーク層での十分なアクセス制限等が施された内部機能（管理者向け画面等）の診断は必要に応じて実施とする（任意）
(5) 診断対象は本番環境を前提とする。検証環境等での診断を行う場合は、全ての外部公開インタフェースが本番と同等に診断できるように、診断用のアカウント設定やデータの投入、外部システム連携等の準備を行うものとする（必須）

ウ　スマートフォンアプリ診断

(1) アプリストアに公開する全ての Android と iOS/iPadOS 向けのアプリを診断の対象とする（必須）
(2) 診断対象のアプリは本番用を前提とする。検証用のアプリを対象とする場

合は、サーバとの接続等を含めた全ての機能が本番用と同等に診断できるように準備を行うものとする（必須）

2)定期診断

各機関が保有するシステムのインベントリ情報（構成情報）に基づき、構築時診断と同様に外部から攻撃を受ける可能性のある箇所（アタックサーフェス）を対象に診断を行う。

ア　インベントリ情報の管理

診断に際して、各機関が保有するインベントリは常に最新化されていることが重要である。インベントリの把握が難しい場合や、把握の抜け漏れが生じうる場合には、各システム担当者へのヒアリング等に加えて、セキュリティベンダーの提供する OSINT（Open Source Intelligence）[11]や ASM（Attack Surface Management）等のサービスを活用し、定期的なインベントリの見直しを行うことが望ましい。

インベントリ情報の管理対象としては、利用しているグローバル IP アドレスとドメイン名、OS とミドルウェア、サーバや PC 端末、セキュリティ製品(ファイアウォール、WAF、IPS/IDS)、ネットワーク機器(VPN、ネットワーク複合機等のインターネットに接続されるもの)等が例として挙げられる。

イ　脆弱性診断の実施規模

診断の実施範囲はシステムごとに異なり、事前の把握が難しい。このため、定期診断の調達に際しては、上限となる IP アドレス数や画面数を定めた上で調達を行うことが望ましい。この場合、実際の診断時には上限の実施数までの範囲で、優先度を付けて診断対象を選定する形となる。実施規模の目安として、プラットフォーム診断は 10～30IP アドレス程度、Web アプリ診断は 50～100 リクエスト程度、スマートフォンアプリ診断は 10～20 画面程度の間で定めると良い。また、実際に各システムの診断対象を決める際は、サイトのトップページから辿れる範囲で行うことや、同様の作りの画面が複数ある場合は代表する 1 画面のみを診断対象とすること等の選定方針を決めておくと良い。また、同じシステムを再度診断する場合は、過去に行った診断とは異なる画面や API を対象とすることが望ましい。いずれにせよ、最終的な診断対象は、対象システムの内部構成を把握する運用担当者を交えて決定するものとする。

[11] インターネット等に一般公開されている情報を収集及び分析し、サイバーセキュリティ上の目的に役立てること

３．３　脆弱性診断の実施要件

それぞれの診断の実施要件を以下に述べる。要件には、全ての診断に共通するものと、診断の種別ごとに異なるものがある。実際に要件を策定する際は、これらの要件を組み合わせるものとする。

1)全ての脆弱性診断に共通する要件

全ての診断に共通する要件は、診断の品質に関わる実務要件、診断を円滑に進めるための管理要件、そして診断の成果物に関する要件に大別される。特記すべき点として、実務者のスキルに関する要件（以下(5)）は必須ではなく推奨に留めている。これは、国内では高度な専門性を有する人材が限られており調達が困難であるという現状に鑑みたものである。しかしながら、脆弱性診断の品質は実務者の知見や経験に大きく左右されるため、リスクの高いシステム等においては、(5)を必須とすることが望ましい。

脆弱性診断では検出した脆弱性等の機微な情報を扱うことから、以下の要件に加え、各機関の定める情報管理や秘密保持等に関する要件を併せて求める必要がある。

(1) 経済産業省の「情報セキュリティサービスに関する審査登録機関基準[12]」における「脆弱性診断サービス」の認定を取得したセキュリティベンダーであること（必須）
(2) 上記(1)の認定基準における「技術要件」と「品質管理要件」を満たす人員が 1 名以上診断に参画すること（必須）
(3) 作業従事者のうち少なくとも 1 名は、当該の種別の診断において 2 年以上の経験を有すること（必須）
(4) 業務に関連する外部ステークホルダーとのコミュニケーションや調整業務について、2 年以上の実務経験を有する者が診断に参画すること(必須)
(5) 以下を満たす者が 1 名以上診断に参画すること。条件を満たさない場合は、経験を満たすことと同等以上の技術を保持していることを政府機関の職員が判断できる理由が具体的に提示されること（推奨）

[12] https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun2.pdf

(5-1) OSCP[13]、OSWA[14]、GWAPT[15]、GPEN[16]、GMOB[17]またはその上位資格の保有
(5-2) CTF 等のセキュリティコンテストにおける上位入賞実績
(5-3) 国内外の脆弱性届出制度[18]や開発者等への報告及び調整実績（付与された CVE 識別番号[19]等）

(6) ツールを用いる場合は、診断対象の見落とし、診断のエラーや誤検出が含まれないように手動で精査すること（必須）
(7) 要請に応じて、休日夜間における診断業務が実施可能であること（任意）
(8) 要請に応じて、使用するネットワーク通信帯域を制限可能であること（任意）
(9) 診断の実施前に実施計画書を提出すること。実施計画書には以下を含むものとする（必須）
(9-1) 診断の実施方針及び実施内容
(9-2) スケジュール
(9-3) 実施体制
(9-4) 情報セキュリティ管理体制
(9-5) 実施上の留意事項や準備事項
(10) 診断の実施前に、対象システムの責任者及び担当者に対して説明会を実施すること。説明会の内容は上記(9)で作成した実施計画書に準ずるものとし、診断を円滑に進められるよう、双方の役割やコミュニケーション体制を確認するものとする（推奨）
(11) 診断結果の報告書には、以下の項目を記載すること。フォーマットは機関からの指定の無い限り、PDF（Portable Document Format）形式で作成するものとする。これ以外の形式を使用する場合は、事前に機関へ相談すること（必須）
(11-1) 検出された脆弱性の概要
(11-2) 検出された脆弱性の深刻度
(11-3) 検出された脆弱性による影響
(11-4) 検出された脆弱性の対策方法

---

[13] https://www.offensive-security.com/pwk-oscp/

[14] https://www.offensive-security.com/web200-oswa/

[15] https://www.giac.org/certifications/web-application-penetration-tester-gwapt/

[16] https://www.giac.org/certifications/penetration-tester-gpen/

[17] https://www.giac.org/certifications/mobile-device-security-analyst-gmob/

[18] 国内では情報セキュリティ早期警戒パートナーシップ等が該当

[19] https://www.ipa.go.jp/security/vuln/scap/cve.html

(11-5) 脆弱性を検出した全てのパラメータ
(11-6) 脆弱性を検出した際の入力文字列

(12) 上記(11-2)は、実際の攻撃可能性に基づき、深刻度を評価すること。評価方法はCVSS~~ v3.1~~の基本評価基準に基づく5段階評価(None, Low, Medium, High, Critical) とし、その評価根拠 (CVSS Vector String[20]等) ~~算定方法~~も明記すること (推奨)

(13) 上記(11-3)は、その脆弱性が悪用できることを可能な範囲で実証し、対象システムにおける現実的な攻撃の発生可能性や想定される脅威のシナリオに基づき記述すること。また、可能なものについては、実証した攻撃のスクリーンショット等の証跡を含めること (必須)

(14) 上記(11-1)(11-3)(11-4)は政府職員が読解可能な平易な文章で記述されていること。目安として、サイバーセキュリティに1年程度従事した職員が読解可能であるものとする (推奨)

(15) 診断結果の報告会を実施すること。報告会には診断の作業従事者が同席し、質疑に応じられるようにすること (推奨)

(16) 検出された脆弱性の改修後、改修した脆弱性に対する再診断を行うこと。再診断は報告書の納品から最低1カ月以内の期間、1回以上の実施ができるようにすること (必須)

ア　総合評価の実施

上記の要件は、履行証明書等の提出を通じて入札の参加資格の確認時に利用することを想定するが、総合評価落札方式での調達が可能である場合は、上記の要件を満たすことに加えて、最高情報セキュリティアドバイザー等の有識者を交えた加点評価を行うことが望ましい。この際の主な評価観点を以下に示す。

- 診断に採用する手法やツールについて、診断の品質を高めるための優れた工夫がなされているか
- 報告書は具体的かつ政府職員が読解可能な平易な文章で記述されているか
- 高度な知識や経験を有する人員による体制が組まれているか

イ　定期診断における留意点

同一の条件下で診断を繰り返し実施した場合、初回以降の検査では脆弱性が検出されない可能性がある。このため、定期診断においては、以下のような条件

[20] https://www.first.org/cvss/v4.0/specification-document#Vector-String

を変えて診断を実施することが望ましい。

・診断の実施範囲（対象とする IP アドレスや画面、API 等）
・診断を実施するセキュリティベンダーまたは診断の作業従事者
・診断に採用するツールや手法

2)プラットフォーム診断に関する要件

プラットフォーム診断に固有の要件を以下に示す。

(1) 表 2－1 に示す全ての脆弱性種別（以下、(1-1)～(1-4)）を診断対象とすること（必須）
　(1-1) 不要ポートの開放
　(1-2) 脆弱なソフトウェアの利用
　(1-3) 設定の不備
　(1-4) プロトコル固有の脆弱性
(2) 上記(1-1)では、TCP、UDP に対してオープンポートの確認と稼働しているサービスの推定を行うこと。TCP の確認は 1～65535 番ポートの全てを対象とすること。UDP の確認には多くの時間を要することから、利用するツールが確認を推奨するポート（一般的に利用頻度の高いポート）の上位 100 位相当を確認対象に含めること（必須）
(3) 上記(1-2)(1-3)(1-4)に関する診断は、表 4－1 に示す脆弱性種別を全て網羅すること（必須）
(4) ツールによる診断には、最新の攻撃手法を反映した実績ある商用ツールを活用すること。フリーツールや自社製ツールのみによる診断は行わないこと（必須）

3)Web アプリ診断に関する要件

Web アプリ診断に固有の要件を以下に示す。Web アプリの脆弱性には人手でなければ検出の難しいものが多数存在し、また、その検出能力は実務者の知識や経験に大きく左右される。このため、攻撃されることによる社会的影響の大きいシステムや、実装に注意を要する機能（ファイルアップロード、ID 連携、マイナンバーカードによる署名や認証等）を有するシステムは、上述の共通要件(5)に該当する熟練者による手動の診断を必須とすべきである。

(1) 表 2－2 に示す全ての脆弱性種別（以下、(1-1)～(1-5)）を診断対象とすること（必須）

(1-1) 固有のビジネスロジックに依存するもの
(1-2) 一般的な仕様上の不具合
(1-3) 実装のメカニズムに対する高度な理解が要求されるもの
(1-4) 一般的な実装の不備
(1-5) 利用する Web アプリミドルウェア固有の脆弱性

(2) 上記(1-1)～(1-3)の診断は全て人手で行うこと。ツールの誤検出の除去ではなく、診断そのものを人手で行うものとする（必須）

(3) 上記(1-2)(1-4)の診断は以下の基準に準ずること。具体的には、表 4-2 に示す脆弱性種別を診断対象として網羅すること。他の基準を用いる場合は、表 4-2 に対する充足性を説明すること（必須）
(3-1) NISC「政府機関等の対策基準策定のためのガイドライン（令和~~3~~5 年度版）[21]」
(3-2) IPA「安全なウェブサイトの作り方 改訂第 7 版[22]」
(3-3) 脆弱性診断士スキルマッププロジェクト「Web アプリケーション脆弱性診断ガイドライン 第 1.2 版[23]」

(4) 上記(1-1)～(1-4)の診断は、(3)の基準に加え、熟練者の経験に基づく手動の診断を行うこと（推奨）

(5) 上記(1-4)(1-5)においてツールを用いる場合は、サイトを手動巡回すること（必須）

(6) 機能の確認に十分な権限を有するアカウントを用いて診断を行うこと（必須）

4) スマートフォンアプリ診断に関する要件

スマートフォンアプリ診断に固有の要件を以下に示す。

(1) 表 2-3 に示す全ての脆弱性発生部位（以下、(1-1)～(1-3)）を診断対象とすること（必須）
(1-1) アプリ本体
(1-2) 通信路
(1-3) 外部サービス

(2) 上記(1-1)(1-3)の診断には、対象アプリのソースコードレビューまたはリバースエンジニアリングを用いること（必須）

(3) 上記(1-1)(1-2)の診断は OWASP の「Mobile Application Security

[21] https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

[22] https://www.ipa.go.jp/security/vuln/websecurity.html

[23] https://github.com/WebAppPentestGuidelines/WebAppPentestGuidelines

Checklist（MAS Checklist）[24]」における L1 の実施項目~~（MASVS-L1 相当）~~を網羅するものとする[25]。ただし、MASVS-CODE 及び MASVS-RESILIENCE に属する診断項目は除外して構わない。~~その他の基準を用いる場合は、MAS Checklist の L1 の診断項目に対する充足性を説明すること~~（必須）

３．４　検出された脆弱性の対応方針

検出された脆弱性は、各機関の対応基準に従い、改修や防御策の適用を行うものとする。構築時診断ではシステムの納品前に、定期診断ではシステムの運用保守において適切に対応が行われるように契約内容等を定める必要がある。この際の対応基準は脆弱性の深刻度に基づいて策定されることが望ましい。また、既に当該の脆弱性を悪用する攻撃が国内外で観測されている場合には、対応基準に関わらず、迅速な対応を行うものとする。

[24] https://mas.owasp.org/checklists/

[25] 網羅の難しい場合は、対象のアプリにおいて生じうるリスクに基づき実施の要否に係る総合的な判断を行うこと

４付録

付録A. 各種診断で検出対象とする脆弱性種別

各種診断において検出対象とすることを求める脆弱性の種別を下表に示す。各表の出典列は、付録Bの文献番号に対応している。

1)プラットフォーム診断

表 ４-１　プラットフォーム診断で対象とする脆弱性種別

No.	脆弱性種別	備考	出典
1	脆弱なソフトウェアの利用	既知脆弱性の有無を確認	(7)(8)(9)
2	不要なポート、サービス、アカウントの存在		(7)(8)
3	公開ディレクトリ、ストレージへの非公開情報の保存	公開不要なファイルの存在等を確認	(8)(9)
4	DNSの設定不備	オープンリゾルバ、ゾーン転送の設定不備等を確認	(7)
5	暗号化されていない、または脆弱な暗号による通信		(8)
6	サーバ証明書の不備		(7)
7	サーバソフトウェアの設定不備	初期パスワードの利用、ディレクトリリスティング等を確認	(9)

2)Webアプリ診断

表 ４-２　Webアプリ診断で対象とする脆弱性種別

No.	脆弱性種別	備考	出典
1	SQLインジェクション		(7)(8)(9)
2	OSコマンドインジェクション		(7)(8)(9)
3	クロスサイトスクリプティング（XSS）	HTMLインジェクション、CSSインジェクション、DOM based XSS等を含む	(7)(8)(9)

No.	脆弱性種別	備考	出典
4	メールヘッダインジェクション		(7)(8)
5	HTTP ヘッダインジェクション（CRLF インジェクション）		(7)(8)(9)
6	eval インジェクション		(7)
7	その他のインジェクション	サーバサイドテンプレートインジェクション（SSTI）、相対パスによる上書き（Relative Path Overwrite）等を含む	(9)
8	ディレクトリトラバーサル（パストラバーサル）	ローカルファイルインクルージョン（LFI）を含む	(7)(8)(9)
9	セッション管理の不備	推測可能なセッション、セッションの盗用、セッションの固定化（セッションフィクセーション）、Cookie の管理不備等を含む	(7)(8)(9)
10	アクセス制御（認証制御）と認可処理の不備	認証回避、ログアウト機能の不備、脆弱なパスワードポリシー、パスワードリセットの不備、復元可能なパスワード保存等を含む	(7)(8)(9)
11	クロスサイトリクエストフォージェリ（CSRF）		(7)(8)(9)
12	クリックジャッキング		(7)(8)(9)
13	レースコンディション（競合状態）	競合状態の発生は確率に依存するため、再現の難しい脆弱性である。実施する診断の程度については、事前に診断の実務者との間で	(7)

No.	脆弱性種別	備考	出典
		認識を合わせおくことが望ましい	
14	バッファオーバーフロー	整数オーバーフローを含む。想定された値域を超えるデータの送信により、主にシステム停止等の異常動作の検出を目的として診断を行う	(7)(8)
15	ファイルアップロードに関する不備	圧縮ファイルの取り扱い（ZIP Bombs 等）を含む	(9)
16	セキュリティの設定ミス		(9)
17	オープンリダイレクト		(9)
18	安全でないデシリアライゼーション		(9)
19	サーバサイドリクエストフォージェリ（SSRF）		(7)(9)
20	クロスサイトウェブソケットハイジャッキング（CSWSH）	WebSocket プロトコルを使用している場合のみ診断対象とする	(9)
21	XML 外部エンティティ参照（XXE）		(9)
22	その他の情報漏えいにつながる脆弱性	エラーメッセージやキャッシュからの情報漏えい等を含む	(9)

3)スマートフォンアプリ診断

スマートフォンアプリ診断で対象とする脆弱性は、OWASP の「Mobile Application Security Checklist（MAS Checklist）[26]」の以下の領域における L1 の実施項目を網羅するものとする。MASVS-CODE 及び MASVS-RESILIENCE に属する診断項目は除外して構わない。

[26] https://mas.owasp.org/checklists/

・MASVS-STORAGE（データストレージとプライバシー）
・MASVS-CRYPTO（暗号化）
・MASVS-AUTH（認証と認可）
・MASVS-NETWORK（ネットワーク通信）
・MASVS-PLATFORM（モバイルプラットフォームとの相互連携）

~~「Mobile Security Testing Guide (MSTG)[27]」における L1 の実施項目を網羅するものとする。具体的には、「OWASP Mobile App Security Checklists v1.4.0[28]」における L1 の診断項目を網羅するものとする。~~

付録B. 参考資料

(1) U.S. General Services Administration - IT Security Procedural Guide: Conducting Penetration Test Exercises CIO-IT Security-11-51 Revision 6
https://www.gsa.gov/system/files/Conducting-Penetration-Test-Exercises-%5BCIO-IT-Security-11-51-Rev-6%5D-11-25-2022.pdf

(2) U.S. General Services Administration - IT Security Procedural Guide: Vulnerability Management Process CIO-IT Security-17-80 Revision 4
https://www.gsa.gov/system/files/Vulnerability-Management-Process-%5BCIO-IT-Security-17-80-Rev-4%5D-03-13-2023.pdf

(3) National Institute of Standards and Technology - SP 800-115 Technical Guide to Information Security Testing and Assessment
https://csrc.nist.gov/publications/detail/sp/800-115/final

~~(4) Carnegie Mellon University - Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization (Version 2.0)~~
~~https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=653459~~

~~(5) 金融情報システムセンター (FISC) - 金融機関等における TLPT 実施にあたっての手引書~~
~~https://www.fisc.or.jp/publication/book/004197.php~~

(6) 経済産業省 - 我が国産業の情報セキュリティ向上に向けた情報セキュリティサービスの高度化方策に関する調査報告書

[27] https://github.com/OWASP/owasp-mstg

[28] https://github.com/OWASP/owasp-mstg/releases/tag/v1.4.0

https://www.meti.go.jp/policy/netsecurity/shinsatouroku/report_2018fy.pdf
(7) NISC - 政府機関等の対策基準策定のためのガイドライン（令和~~3~~５年度版）
https://www.nisc.go.jp/pdf/policy/general/guider5.pdf
(8) IPA - 安全なウェブサイトの作り方 改訂第７版
https://www.ipa.go.jp/security/vuln/websecurity.html
(9) 脆弱性診断士スキルマッププロジェクト - Web アプリケーション脆弱性診断ガイドライン 第1.2版
https://github.com/WebAppPentestGuidelines/WebAppPentestGuidelines
~~(10) OWASP - Mobile Application Security Verification Standard (MASVS)~~
~~https://github.com/OWASP/owasp-masvs~~
~~(11) OWASP - Mobile Security Testing Guide (MSTG)~~
~~https://github.com/OWASP/owasp-mstg~~
(12) OWASP - Mobile Application Security
https://mas.owasp.org/