公開ウェブサーバの調達・運用管理等に係る基本的事項

本事項は、ウェブサイト等を構築する際の公開ウェブサーバの調達・運用管理等に係る基本的な事項を示すものである。

なお、本事項に記載のない事項についても、最適なソリューション、最新技術を利用することにより「費用対効果が高い」、「高度なセキュリティ対策が可能」などと考えられる場合は、県と協議し承認を得た上で、実施することができるものとする。

1　基本方針

(1) 栃木県情報セキュリティポリシーに適合するセキュリティ対策を講じること。

(2) ドメインについて、原則として県のサブドメインを活用すること。

(3) ウェブサイト公開時は常時 SSL 化することとし、http 通信は https 通信にリダイレクトする等の対応を検討すること。

(4) ウェブサイトの要件（利用目的、公開コンテンツ、公開期間等）に応じた可用性やイニシャルコスト・ランニングコストを含めた費用対効果の高い構成を検討すること。

2　サーバ要件

(1) 原則、公開するウェブサイト専用のサーバを利用すること。（ネットワークの庁内・庁外、構築サーバの物理・仮想の別は問わない。）

(2) ウェブサイトの運用に当たり、サーバ OS・ミドルウェア等のサポート対応、アップデート等が適時実施され、脆弱性対応等、セキュリティ対策が実施できるサービス形態であること。

(3) 構築事業者又は運用保守事業者以外の者（レンタルサーバ事業者）が提供するレンタルサーバ等を利用する場合は、県にサービスについて説明を行い、認められた場合のみサービスを利用すること。

(4) 県サブドメインの利用設定、個別の SSL 証明書のインストールができること。

(5) ウェブサイトの構築事業者又は運用保守事業者は、自ら公開ウェブサーバが安全な状態であるか（脆弱性の有無）を確認できる状態でウェブサイトを公開すること。

(6) 公開ウェブサーバについて、常に死活監視を行う仕組みや環境をもつこと。

(7) セキュリティ対策について、公開ウェブサーバが利用する機能（利用者がサイト上で行う情報入力やファイルのアップロードの機能等）や公開する情報の性質等を踏まえ、適切なセキュリティ対策を検討の上、県に提示し承認を得た上で、確実に実装すること。

（セキュリティ対策の機能例）
不要な通信の制御やサーバへの攻撃等を検知する仕組み（ファイアウォール、IDS（Intrusion Detection System）、IPS（Intrusion Prevention System）、WAF（Web Application Firewall））、認証機能、リバースプロキシ　等
なお、庁内にサーバを置く場合（栃木県共同利用型基盤利用を含む。）は、WAF/CDN、NTP、WSUS について、県の環境の提供を受けることができる。

(8) アンチウィルスソフトの導入及びその他ウイルス・不正プログラム等に対するセキュリティ対策を確実に実装すること。

3　構築・運用保守要件

(1) ウェブサイトを公開するためのシステム構成、ネットワーク構成、利用 OS、ミドルウェア、SSL 証明書の取得・確認に必要な情報等を県に提供すること。

(2) サーバ OS・ミドルウェア等の脆弱性情報を都度収集し、適切な脆弱性対応を行うとともに、速やかに県に報告すること。

(3) ウェブサイトの構築や改修を実施した場合には、ウェブサイト公開前に当該サイトについて脆弱性チェックツール等を用いて脆弱性診断を行い、適切な処置を講じるとともに結果を県に報告すること。

(4) ウェブサイトの構築、改修等を実施する際には、（独）情報処理推進機構（IPA）が公開する最新の「安全なウェブサイトの作り方」や別冊「ウェブ健康診断仕様」等を確認し、適切なセキュリティ対策が講じられたウェブサイトとすること。
安全なウェブサイトの作り方 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構（https://www.ipa.go.jp/security/vuln/websecurity/about.html）

(5) ウェブサイトの運用中（公開中）は、定期的にポートスキャン、脆弱性チェックを含むプラットフォーム診断を実施し、脆弱性が検出された場合には、適切な処置を講じるとともに結果を県に報告すること。

(6) 構築サーバ、CMS 等の管理者ユーザ（管理者権限）を適切に管理し、不正アクセスを防止するための対策（複雑性のある類推しづらいパスワードの設定、管理ページへのアクセス制限、多要素認証や二段階認証、業務従事者に対するセキュリティ教育の実施等）を講じること。

(7) レンタルサーバ等の利用やウェブサイトを運用・保守するためにクラウドサービスを利用する場合は、取扱情報やサービスについて明らかにした上で、本県が定める外部サービス利用手順への適合について県に確認すること。

(8) ウェブサイトへのアクセスやアプリケーション認証などの必要なログを取得するとともに各ウェブサイトの状況に応じた必要な期間を設定してログを保存することとし、取得するログの項目及び保存期間については、仕様書に従い、又は県に提案して承認を得ること。

(9) 公開ウェブサーバが悪意のある者からの攻撃を受けた場合等、ウェブサイトを即時閉鎖・復旧できるような対策（定期的なバックアップ等）を講じること。

(10) ウェブサイト上で、利用者情報の管理や個人情報の収集等をする場合には、別記「個人情報取扱特記事項」を遵守し、プライバシーポリシーを利用者が容易に確認できるようにすること。

(11) 県等がウェブサイトに対するセキュリティ監査等を行う場合には、必要な情報の提供、レンタルサーバ事業者等関係者との調整に協力すること。

(12) ウェブサイトの監査等により重大な脆弱性が確認された場合には、具体的な作業日を提示し必要な対策を講じること。

(13) 上記以外の脆弱性についても、県と協議の上、対応を速やかに検討しなければならない。

4　障害対応等

(1) 障害発生時等の連絡先について、事前に県に報告すること。

(2) 当該ウェブサイトについて、セキュリティインシデントを検知した場合には、速やかに県に報告をするとともに、対策を検討し、県の判断を仰ぐこと。

(3) システム障害やセキュリティインシデント等が発生した後の恒久対応について再発防止策を検討し、必要な対策を確実に実施すること。