プレスリリース
2018 年 5 月 30 日
独立行政法人情報処理推進機構

「ウェブサイト開設等における運営形態の選定方法に関する手引き」を公開
～ウェブサイトの発注者、受注者間でセキュリティ対策に必要な確認項目の合意が容易に～

IPA（独立行政法人情報処理推進機構、理事長：富田達夫）は、主に小規模事業者を対象に、ウェブサイトの新規開設、および刷新において、クラウドサービスなどの運用形態別にメリット･デメリット、およびセキュリティ対策に必要な確認項目を整理した、「ウェブサイト開設等における運営形態の選定方法に関する手引き」を公開しました。
URL：https://www.ipa.go.jp/security/technicalwatch/20180530.html

企業・組織において、ウェブサイトは、事業案内、販売促進などを目的としたコミュニケーションツールとして事業活動に不可欠なツールです。
一方、企業等のウェブサイトが不正アクセスにより、個人情報が流出したといったトラブルが報道されることは、今や珍しいことでは無くなりました。

IPA では、2004 年 7 月からソフトウェアの脆弱性関連情報の届出を受け付けています(*1)。これまでに受付けたウェブサイトの脆弱性のうち､修正等が完了していないのは 329 件で､全体の約 5%(*2)です。
こうしたウェブサイトは、主にセキュリティ対策への認識が不十分な小規模組織による運営です。そして、対策のための体制やコスト等の準備がなく、開設後に問題が指摘されても、修正も、廃棄もできません。これが“攻撃を受けてしまうウェブサイトの放置”に繋がっています。

そこで、問題のあるウェブサイトが不用意に制作されない様、発注事業者、および制作を請負う受注者の利用を想定した手引きを作成・公開しました。ウェブサイト開設・刷新における、クラウドサービス利用などの運営形態別のメリット・デメリット、および必要なセキュリティ対策などが整理されています。これにより、安全なウェブサイトの開設に必要な確認項目などの合意が、発注者、受注者間で容易になります。

表 1「運営形態ごとの選定項目の比較」（手引き P9）

項目番号	ウェブサイト開設・運営に関わる項目 ＼ 運営形態		モール	ASP	SaaS型クラウドサービス	PaaS型クラウドサービス	レンタルサーバ	IaaS型クラウドサービス	ハウジング	オンプレミス		補足事項
①	ウェブサイトの機能の自由度	低									高	(注1) ECサイトの場合、月々の売上の一部が維持費用に課金される場合がる。
②	ウェブサイト開設までの日数	短									長	
③	ウェブサイト開設のため調達が必要な物品数	少									多	
④	ウェブサイト開設・運営に必要な人的資源	少									多	
⑤	ウェブサイト開設に必要な費用	少									多	
	ウェブサイトの維持・運営に必要な費用	少	(注1)	(注1)	(注1)						多	
⑥	検討が必要なセキュリティ対策項目	少									多	

優 劣
左側の色の項目程、優れていることを示す。
※上記の表は各運営形態の典型的な例をもとに比較しているため、
サービスや導入機材によっては実際の優劣が変わる場合が存在する。

(*1) 経済産業省の告示に基づき策定された“情報セキュリティ早期警戒パートナーシップガイドライン”に則り運用。

(*2) 2018 年 4 月 25 日公表「ソフトウェアなどの脆弱性関連情報に関する届出状況 2018 年第 1 四半期」脆弱性の累計受付件数は 9,715 件で、うち取り扱いが終了したのは 9,287 件と約 95%。https://www.ipa.go.jp/security/vuln/report/vuln2018q1.html

表 2「運営形態ごとに必要となる費用」（手引き P19）

運営形態 / 費用項目	モール ASP SaaS型クラウドサービス	PaaS型クラウドサービス レンタルサーバ IaaS型クラウドサービス	ハウジング オンプレミス
サーバ室の整備費用			○
ネットワーク回線の敷設費用			○
ネットワーク機器の購入費用			○
サーバの購入費用			○
ウェブアプリケーションの開発費用・購入費用		○	○
ウェブサーバの構築費用	○	○	○
ウェブサイトの運用管理費用	○	○	○
サービス利用費用、課金	○	○	△ (ハウジングのみ)

表 3「運営形態ごとに検討すべきセキュリティ対策」（手引き P22）

セキュリティ対策項目				運用形態			
区分	分類		代表的対策例	モール ASP SaaS	PaaS レンタルサーバ IaaS	データセンタ	オンプレミス
システムセキュリティ対策	技術的対策	物理	・サーバ室 ・入退管理				○
		ネットワーク	・FW　・IDS/IPS ・WAF・VPN ・ウイルス対策製品 ・サンドボックス型製品 ・DDoS対策		△	△	○
		アプリケーション	・改ざん検知 ・認証　・アクセス制御 ・データ保護		○	○	○
	運用管理的対策	セキュリティパッチ	・パッチ適用 ・仮想パッチ適用		△（アプリ）	○	○
		監視	・ログ収集、分析		△	○	○
		ｲﾝｼﾃﾞﾝﾄ対応	・バックアップ ・切り分け　・抜線		△	○	○
	人的対策	要員教育	・ポリシー教育 ・技術教育		△	○	○
業務セキュリティ対策	社員教育		・リテラシー教育	○	○	○	○
	ユーザ・顧客管理		・ポリシー教育 ・情報取扱い規則	○	○	○	○
	コンテンツ管理		・コンテンツ更新ルール	○	○	○	○

サイト運営者対応　○：対応の検討が必要
△：一部対応の検討が必要

これらにより、ウェブサイト構築・運用における、“理想と現実”が整理でき、企業・組織の実情に即したウェブサイト構築と運用を可能にします。

IPA では、この手引きを通じて、企画から廃棄までのライフサイクル全体を念頭にした、ウェブサイトの運用・管理がすすみ、安全なインターネット環境が整備されることを期待しています。

■ 本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター　熊谷／板橋
Tel: 03-5978-7527　Fax: 03-5978-7552　E-mail: vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部 広報グループ　白石
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp