



Webセキュリティの対策マトリクス

社団法人日本ネットワークインフォメーションセンター
セキュリティ事業担当
木村泰司

Webセキュリティの対策マトリクス (全体)

	一般ユーザ	エンドユーザ のシステム管 理者	Webアプリの開 発者	ネットワークオ ペレータ
Phishing Pharming	利用上の対策 端末での対策 届出 / 連絡	端末での対策 連絡体制	セキュアな開発 連絡受付	セキュアな提供 連絡体制
XSS CSRF	端末での対策 届出 / 連絡	管理下PC・ Webブラウザ の脆弱性除去 連絡体制	セキュアな開発 連絡受付	セキュアな提供 連絡体制
DoS	利用上の対策 端末での対策	端末での対策 連絡体制	セキュア (負荷 も考慮)な開発 連絡受付	セキュアな提供 監視 連絡体制

対策マトリクス (ユーザサイド)

	一般ユーザ	エンドユーザのシステム管理者
Phishing Pharming	利用PCの脆弱性除去 メール内容の確認 「フィッシング110番」の利用 フィッシングに対する知識	管理下PC・機器の脆弱性除去 フィルタリングソフトの導入 「フィッシング110番」の利用 フィッシングに対する知識
XSS CSRF	利用PC・Webブラウザの脆弱性除去 脆弱性発見の際の届出	管理下PC・Webブラウザの脆弱性除去
DoS	利用PCのソフトウェア管理 アンチウイルスソフトの導入 DoSに関する啓発	利用者PCのソフトウェア管理 ログ・状態監視 DoSに関する啓発

対策マトリクス (xSPサイド)

	Webアプリの開発者	ネットワークオペレータ
Phishing Pharming	管理サーバ/機器/Webアプリの脆弱性除去 適切なWebサイト表示 適切なサーバ証明書導入/利用 組織内での対応窓口/手順確立	管理サーバ/機器 提供サービスの脆弱性除去 迷惑メール対策 報告窓口設置 連絡体制確立 Bot化顧客対応
XSS CSRF	セキュアな開発の推進 脆弱性と対策の正確な知識	(ASP) 管理下Webアプリのセキュリティ検査 管理下Webアプリの脆弱性対策
DoS	負荷に対する設計 (テスト) 資源の利用状況の監視	トラフィック制御 ネットワーク監視 問い合わせ窓口の準備