広　報　資　料
平成29年２月２日
警　　察　　庁

ウイルス感染を目的としたウェブサイト改ざんの対策について

１　背景

一般財団法人日本サイバー犯罪対策センター(JC3)と連携した分析により、平成28年９月頃から、「RIG-EK」と呼ばれる攻撃ツールが組み込まれたサイトに誘導するよう改ざんされたウェブサイトが急増していることが確認された。

２　改ざんウェブサイトアクセスによるウイルス感染の仕組み

(1)　正規のウェブサイトに設置されたファイルを改ざんして不正な文字列を挿入し、これにより、当該ウェブサイトにアクセスした者を「RIG-EK」の組み込まれた別のサイトに誘導する。

(2)　当該サイト閲覧者の端末に脆弱性を悪用する指令をダウンロードさせる。

(3)　当該指令により閲覧者の端末を不正に操作し、ランサムウェアや不正送金ウイルスをダウンロードさせて、端末に感染させる。

３　警察による対応

国内の改ざんされたサイトの管理者が判明した298サイトについて、38都道府県警察において、当該サイト管理者等に対して、改ざん状況の確認、サイトの修復の依頼等の対策を実施。

４　対策

管理者及び一般ユーザによる未然防止対策として、以下の対策を推奨。

(1)　サイト管理者及びサーバ管理者によるウェブサイト改ざん対策

- 　OSを含む各種ソフトウェアの最新の状態へのアップデート
- 　コンテンツ管理システムの最新版の導入
- 　ログインパスワードについて、推測が容易なものを避けるほか、定期的な変更

(2)　一般ユーザによるウイルス感染対策

- 　OSを含む各種ソフトウェアの最新の状態へのアップデート
- 　ウイルス対策ソフトの導入及び最新の状態へのアップデート

５　その他

JC3においても、改ざんサイトによるウイルス感染について、注意喚起を実施。