■―――□
┃　　◆◆　NISC 重要インフラニュースレター　◆◆
┃　　（２０１９年３月１２日発行 第２３３号）
┃　　発行：NISC 重要インフラグループ
□―――■

┼―◎ はじめに ―――――――――――――――――――――――――――――┼

　重要インフラニュースレターは、重要インフラの関係者を中心に情報セキュリティに関する情報を幅広く紹介するものです。
　情報システム部門の担当者から管理職や経営層の方まで必要に応じて幅広く共有いただければ幸いです。

┼―――┼

┌◆　第２３３号の目次　◆―――――――――――――――――――――――――┐

├―――┤
○今号は、２月２６日～３月１１日頃の記事を集めて編集しています。
└―――┘

■―――□
┃１．チェックが必要な情報
┼―――┼

（１）Microsoft 社製品に関する脆弱性
・Windows 7 における DLL 読み込みに関する脆弱性(JVN)(02/28)
　https://jvn.jp/jp/JVN69181574/index.html
　※CVSSv3 では基本値「7.8」となっています。

・Microsoft Teams のインストーラにおける DLL 読み込みに関する脆弱性(JVN)(02/28)
　https://jvn.jp/jp/JVN79543573/index.html
　※CVSSv3 では基本値「7.8」となっています。

（２）トレンドマイクロ社製品に関する脆弱性
・ウイルスバスター コーポレートエディションにおける複数の脆弱性(JVN)(03/01)
　https://jvn.jp/vu/JVNVU91054129/index.html

・Smart Protection Server における OS コマンドインジェクションの脆弱性(JVN)(03/01)
　https://jvn.jp/vu/JVNVU99357827/index.html

・Trend Micro Mobile Security における複数の脆弱性(JVN)(03/01)
　https://jvn.jp/vu/JVNVU97891221/index.html

・InterScan for Microsoft Exchange における複数の脆弱性(JVN)(03/01)
　https://jvn.jp/vu/JVNVU95147316/index.html

（３）その他
・Drupal の脆弱性対策について(CVE-2019-6340)(IPA、JPCERT/CC)(02/26)
https://www.ipa.go.jp/security/ciadr/vul/20190226-drupal.html
https://www.jpcert.or.jp/at/2019/at190010.html

・ISC BIND 9 に対する複数の脆弱性（CVE-2018-5744, CVE-2018-5745, CVE-2019-6465）に関する注意喚起(JPCERT/CC)(02/26)
https://www.jpcert.or.jp/at/2019/at190009.html

・WordPress 用プラグイン FormCraft におけるクロスサイトリクエストフォージェリの脆弱性(JVN)(02/26)
https://jvn.jp/jp/JVN83501605/index.html

・CyberNewsFlash「OpenSSL の脆弱性（CVE-2019-1559）について」を公開(JPCERT/CC)(02/27)
https://www.jpcert.or.jp/newsflash/2019022701.html

・ナブラークにおける複数の脆弱性(IPA、JVN)(02/27)
https://www.ipa.go.jp/security/ciadr/vul/20190227-jvn.html
https://jvn.jp/jp/JVN56542712/index.html
※CVSSv3 では基本値「8.2」となっています。

・WordPress 用プラグイン Smart Forms におけるクロスサイトリクエストフォージェリの脆弱性(JVN)(02/28)
https://jvn.jp/jp/JVN97656108/index.html

・Adobe ColdFusion の脆弱性（APSB19-14）に関する注意喚起(JPCERT/CC)(03/04)
https://www.jpcert.or.jp/at/2019/at190011.html

・Dradis Community Edition および Dradis Professional Edition におけるクロスサイトスクリプティングの脆弱性(JVN)(03/05)
https://jvn.jp/jp/JVN40288903/index.html

２．政府機関の動き

（１）警察庁
・平成３０年におけるサイバー空間をめぐる脅威の情勢等について(03/07)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf

（２）経済産業省
・クレジットカード取引におけるセキュリティ対策の強化に向けた「実行計画 2019」を取りまとめました(03/04)
http://www.meti.go.jp/press/2018/03/20190304004/20190304004.html

・「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第１版（案）」の意見公募手続（パブリックコメント）を開始しました(03/11)
http://www.meti.go.jp/press/2018/03/20190311001/20190311001.html

３．関係機関の動き

（１）ＩＰＡ

・「情報セキュリティ 10 大脅威 2019」の解説資料を公開しました。(02/28)
https://www.ipa.go.jp/security/vuln/10threats2019.html

・「安全なウェブサイトの運用管理に向けての 20 ヶ条」の参考資料として「ウェブサイト運営のファーストステップ～ウェブサイト運営者がまず知っておくべき脅威と責任～」を公開しました。(03/06)
https://www.ipa.go.jp/security/vuln/websitecheck.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2019-02-27 号(02/27)
https://www.jpcert.or.jp/wr/2019/wr190801.html

・Weekly Report 2019-03-06 号(03/06)
https://www.jpcert.or.jp/wr/2019/wr190901.html

・ 2018 年度 中南米 CSIRT 動向調査 (03/07)
https://www.jpcert.or.jp/research/LACSIRT-survey.html

４．海外の動き

（１）US-CERT

・Cisco 社が複数の製品についてのセキュリティアップデートをリリース。(02/27)
https://www.us-cert.gov/ncas/current-activity/2019/02/27/Cisco-Releases-Security-Updates

・Cisco 社が複数の製品についてのセキュリティアップデートをリリース。(03/06)
https://www.us-cert.gov/ncas/current-activity/2019/03/06/Cisco-Releases-Security-Updates

・Google が Chrome の version 72.0.3626.121 をリリース。(03/07)
https://www.us-cert.gov/ncas/current-activity/2019/03/07/Google-Releases-Security-Updates-Chrome

・３月４日の週の脆弱性概報(03/11)
https://www.us-cert.gov/ncas/bulletins/SB19-070

（２）米 ICS-CERT

・Moxa 社のイーサネットスイッチに不適切なアクセス制御等の脆弱性。(02/26)
https://ics-cert.us-cert.gov/advisories/ICSA-19-057-01
※CVSSv3 では基本値「9.8」となっています。

・PSI GridConnect 社の通信機器にクロスサイトスクリプティングの脆弱性。(02/28)
https://ics-cert.us-cert.gov/advisories/ICSA-19-059-01
※CVSSv3 では基本値「8.5」となっています。

・Rockwell Automation 社のデータ伝送機器にスタックベースのバッファオーバーフローの脆弱性。(03/05)
https://ics-cert.us-cert.gov/advisories/ICSA-19-064-01
※CVSSv3 では基本値「10.0」となっています。

５．読者へのお願い

ニュースレターについてのご意見、ご感想、掲載を希望する記事等ございましたら以下の連絡先にご連絡下さい。
mailto:nisc-infra-letter@cyber.go.jp

６．次回予告

次回は、３月２６日配信の予定です。
※本ニュースレターは、原則として、毎月第２・第４火曜日頃に発行しますが、都合により変則的な配信日となることがあります。

◎官民で連携した重要インフラ防護に係る取組をご紹介しています。
https://www.nisc.go.jp/active/infra/index.html

◎NISC や関係機関が作成した情報セキュリティに係る意識啓発動画を掲載しています。
https://www.youtube.com/user/NISCchannel/videos

◎本ニュースレターは、主にセプターや重要インフラ事業者等に対して、情報セキュリティに関する取組等を幅広く紹介することを目的としています。このため、掲載内容の利活用の方法や本ニュースレターの転送等について、特に制限はしておりませんが、利活用や転送等に際しては、リンク先の情報を参照の上、ご自身の責任でお願いいたします。
また、掲載情報が一部重複する場合もございますが、ご容赦願います。

ni(　^s^)c