■―――――――――――――――――――――――――――――――――――――□
┃　　◆◆　NISC 重要インフラニュースレター　◆◆
┃　　（２０１９年２月１３日発行 第２３１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２３１号の目次　◆―――――――――――――――――――――――――┐

├―――――――――――――――――――――――――――――――――――――┤
○今号は、１月２９日～２月１２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
・Microsoft Exchange 2013 およびそれ以降における NTLM 中継攻撃が可能な脆弱性(JVN)(01/29)
　https://jvn.jp/vu/JVNVU97449410/index.html
※CVSSv3 では基本値「8.8」となっています。

（２）Apple 社製品に関する脆弱性
・複数の Apple 製品における脆弱性に対するアップデート(JVN)(02/08)
　https://jvn.jp/vu/JVNVU98819755/index.html

（３）その他
・UNLHA32.DLL、UNARJ32.DLL、LHMelting および LMLzh32.DLL における DLL 読み込みに関する脆弱性(JVN)(01/31)
　https://jvn.jp/jp/JVN52168232/index.html
※CVSSv3 では基本値「7.8」となっています。

・UNLHA32.DLL、UNARJ32.DLL および LHMelting のインストーラにおける DLL 読み込みに関する脆弱性(JVN)(01/31)
　https://jvn.jp/jp/JVN83826673/index.html
※CVSSv3 では基本値「7.8」となっています。

・POWER EGG において任意の EL 式を実行される脆弱性(JVN)(02/05)
　https://jvn.jp/jp/JVN63860183/index.html
※CVSSv3 では基本値「7.3」となっています。

・OpenAM（オープンソース版）におけるオープンリダイレクトの脆弱性(JVN)(02/06)
https://jvn.jp/jp/JVN43193964/index.html
※CVSSv3 では基本値「3.4」となっています。

・Marvell 製 Avastar ワイヤレス SoC における複数の脆弱性(JVN)(02/06)
https://jvn.jp/vu/JVNVU92674930/index.html
※CVSSv3 では基本値「8.8」となっています。

・V20 PRO L-01J においてクラッシュが引き起こされる脆弱性(JVN)(02/12)
https://jvn.jp/jp/JVN40439414/index.html

## ２．政府機関の動き

（１）NISC
・約束のネバーランド×サイバーセキュリティ月間　特設サイトオープン！(02/01)
https://neverland.nisc.go.jp/

（２）総務省
・IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施(02/01)
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html

・「サイバーセキュリティ国際シンポジウム」の開催(02/08)
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00016.html

（３）警察庁
・32764/TCP 及び 37215/TCP に対する Mirai ボットの特徴を有するアクセスの増加等について(02/01)
https://www.npa.go.jp/cyberpolice/important/2019/201902011.html

・平成 30 年 11 月期観測資料(02/01)
https://www.npa.go.jp/cyberpolice/important/2019/201902012.html

・平成 30 年 12 月期観測資料(02/01)
https://www.npa.go.jp/cyberpolice/important/2019/201902013.html

## ３．関係機関の動き

（１）ＩＰＡ
・「情報セキュリティ 10 大脅威 2019」を決定(IPA)(01/30)
https://www.ipa.go.jp/security/vuln/10threats2019.html

・「サイバー情報共有イニシアティブ（J-CSIP） 運用状況［2018 年 10 月～12 月］」を公開しました。(IPA)(01/31)
https://www.ipa.go.jp/security/J-CSIP/index.html

・「情報セキュリティ安心相談窓口の相談状況［2018 年第 4 四半期（10 月～12 月）］」を公開しました。(IPA)(01/31)

https://www.ipa.go.jp/security/txt/2018/q4outline.html

・「コンピュータウイルス・不正アクセスの届出状況［2018 年第 4 四半期（10～12 月）］」を公開しました。(IPA)(01/31)
https://www.ipa.go.jp/security/outline/todokede-j.html

・NIST 文書「重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版」翻訳版を公開しました。(IPA)(01/31)
https://www.ipa.go.jp/security/publications/nist/index.html

・【講演映像公開】国家資格「情報処理安全確保支援士」がわかる！制度説明会（2019 年 1 月開催）(IPA)(02/05)
https://www.ipa.go.jp/siensi/toberiss/wakaru.html

（２）ＪＰＣＥＲＴ コーディネーションセンター
・Weekly Report 2019-01-30 号(JPCERT/CC)(01/30)
https://www.jpcert.or.jp/wr/2019/wr190401.html

・JPCERT/CC Eyes「Japan Security Analyst Conference 2019 開催レポート～前編～」(JPCERT/CC)(01/31)
https://blogs.jpcert.or.jp/ja/2019/01/jsac2019report1.html

・Weekly Report 2019-02-06 号(JPCERT/CC)(02/06)
https://www.jpcert.or.jp/wr/2019/wr190501.html

・JPCERT/CC Eyes「Japan Security Analyst Conference 2019 開催レポート～後編～」(JPCERT/CC)(02/07)
https://blogs.jpcert.or.jp/ja/2019/02/jsac2019report2.html

・Docker 等で使用する runc の権限昇格に関する脆弱性（CVE-2019-5736）について(JPCERT/CC)(02/12)
https://www.jpcert.or.jp/newsflash/2019021201.html

## ４．海外の動き

●US-CERT
・Mozilla が Firefox についてのセキュリティアップデートをリリース。(01/30)
https://www.us-cert.gov/ncas/current-activity/2019/01/29/Mozilla-Releases-Security-Updates-Firefox

・Google が Chrome についてのセキュリティアップデートをリリース。(01/29)
https://www.us-cert.gov/ncas/current-activity/2019/01/29/Google-Releases-Security-Updates-Chrome

・Mozilla が Thunderbird についてのセキュリティアップデートをリリース。(01/30)
https://www.us-cert.gov/ncas/current-activity/2019/01/30/Mozilla-Releases-Security-Update-Thunderbird

・米国国家安全保障局（ＮＳＡ）がサイドチャンネルの脆弱性に関するガイドライン改定版をリリース。(02/01)
https://www.us-cert.gov/ncas/current-activity/2019/02/01/NSA-Releases-Updated-Guidance-Side-Channel-Vulnerabilities

・Microsoft 社が Microsoft Exchange Server の権限の昇格の脆弱性への対処に関する忠告をリリース。(02/05)
https://www.us-cert.gov/ncas/current-activity/2019/02/05/Microsoft-Releases-Security-Advisory-Exchange-Server

・２月４日の週の脆弱性概報(02/11)
https://www.us-cert.gov/ncas/bulletins/SB19-042

●米 ICS-CERT
・AVEVA 社の産業オートメーション用システムに不十分な資格情報保護の脆弱性(01/29)
https://ics-cert.us-cert.gov/advisories/ICSA-19-029-03
※CVSSv3 では基本値「8.8」となっています。

・三菱電機株式会社のシーケンサにリソース枯渇の脆弱性(01/29)
https://ics-cert.us-cert.gov/advisories/ICSA-19-029-02
※CVSSv3 では基本値「7.5」となっています。

・Becton, Dickinson and Company 社のフローサイトメーターに不適切なアクセス制御の脆弱性(02/05)
https://ics-cert.us-cert.gov/advisories/ICSMA-19-029-02
※CVSSv3 では基本値「6.8」となっています。

・Stryker 社の医療用ベッドにノンスの再利用の脆弱性(01/29)
https://ics-cert.us-cert.gov/advisories/ICSMA-19-029-01
※CVSSv3 では基本値「6.8」となっています。

・Schneider Electric 社の電気自動車充電システムにコードインジェクション等の脆弱性(01/31)
https://ics-cert.us-cert.gov/advisories/ICSA-19-031-01
※CVSSv3 では基本値「9.8」となっています。

・Identicard 社のアクセス管理システムにハードコーディングされた資格情報等の脆弱性(01/31)
https://ics-cert.us-cert.gov/advisories/ICSA-19-031-02
※CVSSv3 では基本値「8.8」となっています。

・Kunbus 社の通信ゲートウェイに不適切な認証等の脆弱性(02/05)
https://ics-cert.us-cert.gov/advisories/ICSA-19-036-05
※CVSSv3 では基本値「10.0」となっています。

・Siemens 社のオートメーションシステムに不適切な入力検証の脆弱性(02/05)
https://ics-cert.us-cert.gov/advisories/ICSA-19-036-04
※CVSSv3 では基本値「7.5」となっています。

・WECON Technology 社の HMI プログラミングソフトウェアにスタックベースのバッファオーバーフロー等の脆弱性(02/05)
https://ics-cert.us-cert.gov/advisories/ICSA-19-036-03

※CVSSv3 では基本値「7.8」となっています。

・Rockwell Automation 社のサーバーに不適切な入力検証の脆弱性(02/05)
https://ics-cert.us-cert.gov/advisories/ICSA-19-036-02
※CVSSv3 では基本値「5.3」となっています。

・AVEVA Software 社の HMI システムにリソースインジェクション等の脆弱性(02/05)
https://ics-cert.us-cert.gov/advisories/ICSA-19-036-01
※CVSSv3 では基本値「9.8」となっています。

・Siemens 社のイーサネットシステムに不適切な入力検証の脆弱性(02/07)
https://ics-cert.us-cert.gov/advisories/ICSA-19-038-02
※CVSSv3 では基本値「7.5」となっています。

・Siemens 社の測定変換器に捕捉されない例外の脆弱性(02/07)
https://ics-cert.us-cert.gov/advisories/ICSA-19-038-01
※CVSSv3 では基本値「5.3」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、２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