■―――――――――――――――――――――――――――――――――――――□

┃　　◆◆　NISC 重要インフラニュースレター　◆◆

┃　　（２０１９年１１月１２日発行 第２４９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２４９号の目次　◆―――――――――――――――――――――――┐

├―――――――――――――――――――――――――――――――――――――┤

○今号は、１０月２３日～１１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）マイクロソフト社製品に関する脆弱性

・Microsoft Office for Mac において XLM マクロに対する挙動が不適切な問題(JVN)(11/06)

https://jvn.jp/vu/JVNVU98504876/index.html

※CVSSv3 では基本値「7.8」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)(10/31)

https://jvn.jp/vu/JVNVU96749516/index.html

（３）トレンドマイクロ社製品に関する脆弱性

・トレンドマイクロ株式会社製の複数の製品における XML 外部実体参照（XXE）に関する脆弱性(JVN)(10/25)

https://jvn.jp/vu/JVNVU99059651/index.html

・ウイルスバスターコーポレートエディションの脆弱性（CVE-2019-18187）に関する注意喚起(JPCERT/CC、JVN)(10/28)

https://www.jpcert.or.jp/at/2019/at190041.html

https://jvn.jp/vu/JVNVU96213168/index.html

※CVSSv3 では基本値「8.2」となっています。

・トレンドマイクロ株式会社製の複数の製品におけるディレクトリトラバーサルの脆弱性(JVN)(11/08)
https://jvn.jp/vu/JVNVU91743132/index.html
※CVSSv3 では基本値「8.8」となっています。

・Trend Micro Anti-Threat Toolkit (ATTK) における任意のコード実行が可能な脆弱性(JVN)(11/11)
https://jvn.jp/vu/JVNVU91935870/index.html
※CVSSv3 では基本値「7.5」となっています。

（４）その他
・PowerCMS におけるオープンリダイレクトの脆弱性(JVN)(10/23)
https://jvn.jp/jp/JVN34634458/index.html

・複数の D-Link 製ルータにおけるコマンドインジェクションの脆弱性(JVN)(10/24)
https://jvn.jp/vu/JVNVU95198984/index.html
※CVSSv3 では基本値「9.8」となっています。

・図書館情報管理システム LIMEDIO におけるオープンリダイレクトの脆弱性(JVN)(10/28)
https://jvn.jp/jp/JVN45633549/index.html

・Apex One におけるコマンドインジェクションの脆弱性(JVN)(11/05)
https://jvn.jp/vu/JVNVU90577675/index.html
※CVSSv3 では基本値「8.2」となっています。

・オムロン製 Network Configurator for DeviceNet における DLL 読み込みに関する脆弱性(JVN)(11/06)
https://jvn.jp/vu/JVNVU94145643/index.html
※CVSSv3 では基本値「7.3」となっています。

・スマートフォンアプリ「ラクマ」における認証情報漏えいの脆弱性(JVN)(11/07)
https://jvn.jp/jp/JVN41566067/index.html

２．政府機関の動き

（１）ＮＩＳＣ
・重要インフラ専門調査会第 20 回会合を開催 （2019.10.28 開催）(11/06)
https://www.nisc.go.jp/conference/cs/ciip/index.html#ciip20

・2019 年度「分野横断的演習」を実施しました（2019.11.8 実施）(11/11)
https://www.nisc.go.jp/active/infra/pdf/bunya_enshu20191111.pdf

（２）警察庁
・フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）(10/24)
https://www.npa.go.jp/cyber/policy/caution1910.html

・vBulletin の脆弱性（CVE-2019-16759）を標的としたアクセスの観測等について(10/29)
https://www.npa.go.jp/cyberpolice/important/2019/201910291.html

・令和元年９月期観測資料(10/29)
https://www.npa.go.jp/cyberpolice/important/2019/201910292.html

・令和元年８月期観測資料(10/29)
https://www.npa.go.jp/cyberpolice/important/2019/201910023.html

（３）総務省
・脆弱な IoT 機器及びマルウェアに感染している IoT 機器の利用者への注意喚起の実施状況（2019 年度第 2 四半期）(10/25)
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00043.html

・日米 ISAC 間の協力に係る覚書への署名(11/11)
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00046.html

３．関係機関の動き

（１）ＩＰＡ
・脆弱性対策情報データベース JVN iPedia の登録状況［2019 年第 3 四半期（7 月～9 月）］(10/23)
https://www.ipa.go.jp/security/vuln/report/JVNiPedia2019q3.html

・ソフトウェア等の脆弱性関連情報に関する届出状況[2019 年第 3 四半期（7 月～9 月）](10/23)
https://www.ipa.go.jp/security/vuln/report/vuln2019q3.html

・「情報セキュリティ安心相談窓口の相談状況［2019 年第 3 四半期（7 月～9 月）］」を公開しました。(10/25)
https://www.ipa.go.jp/security/txt/2019/q3outline.html

・「サイバー情報共有イニシアティブ（J-CSIP） 運用状況［2019 年 7 月～9 月]」を公開しました。(10/31)
https://www.ipa.go.jp/security/J-CSIP/index.html

（２）ＪＰＣＥＲＴ コーディネーションセンター
・JPCERT/CC Eyes「攻撃グループ BlackTech が使うダウンローダ IconDown」(10/23)
https://blogs.jpcert.or.jp/ja/2019/10/IconDown.html

・Weekly Report 2019-10-24 号(10/24)
https://www.jpcert.or.jp/wr/2019/wr194101.html

・ソフトウェア等の脆弱性関連情報に関する届出状況［2019 年第 3 四半期（7 月～9 月)](10/24)
https://www.jpcert.or.jp/report/press.html

・JPCERT/CC インターネット定点観測レポート［2019 年 7 月 1 日～2019 年 9 月 30 日](10/29)
https://www.jpcert.or.jp/tsubame/report/report201907-09.html

・CyberNewsFlash「DDoS 攻撃を示唆して、仮想通貨を要求する脅迫メールについて」(10/30)
https://www.jpcert.or.jp/newsflash/2019103001.html

・Weekly Report 2019-10-30 号(10/30)
https://www.jpcert.or.jp/wr/2019/wr194201.html

・Weekly Report 2019-11-07 号(11/07)
https://www.jpcert.or.jp/wr/2019/wr194301.html

・PSIRT Services Framework Version 1.0 日本語版(11/07)
https://www.jpcert.or.jp/research/psirtSF.html

４．海外の動き

● 米国 DHS

・Juniper Networks 社が Junos OS についてのセキュリティアップデートをリリース。(10/23)
https://www.us-cert.gov/ncas/current-activity/2019/10/23/juniper-networks-releases-junos-os-security-advisory

・Mozilla が Firefox 及び Firefox ESR についてのセキュリティアップデートをリリース。(10/23)
https://www.us-cert.gov/ncas/current-activity/2019/10/23/mozilla-releases-security-updates-firefox-and-firefox-esr

・米国連邦取引委員会（ＦＴＣ）が「ストーカーアプリ」に関して警告する記事をリリース。(10/23)
https://www.us-cert.gov/ncas/current-activity/2019/10/23/beware-stalking-apps

・米国連邦捜査局（ＦＢＩ）が e-skimming への関心を高めるための記事をリリース。(10/23)
https://www.us-cert.gov/ncas/current-activity/2019/10/23/fbi-releases-article-defending-against-e-skimming

・英国サイバーセキュリティセンター（ＮＣＳＣ）が２０１８年９月１日から２０１９年８月３１日までの年間レビューをリリース。(10/24)
https://www.us-cert.gov/ncas/current-activity/2019/10/24/ncsc-releases-2019-annual-review

・米国連邦捜査局（ＦＢＩ）が選挙のセキュリティに係る追加の情報をリリース。(10/24)
https://www.us-cert.gov/ncas/current-activity/2019/10/24/fbi-expands-election-security-resources

・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。(10/24)
https://www.us-cert.gov/ncas/current-activity/2019/10/24/mozilla-releases-security-update-thunderbird

・オーストラリアサイバーセキュリティセンター（ＡＣＳＣ）が拡大する Emotet キャンペーンに関する注意喚起をリリース。(10/25)
https://www.us-cert.gov/ncas/current-activity/2019/10/25/acsc-releases-advisory-emotet-malware-campaign

・米国連邦取引委員会（ＦＴＣ）がハッカーによる個人情報窃取から守るための助言をリリース。(10/29)
https://www.us-cert.gov/ncas/current-activity/2019/10/29/ftc-provides-tips-warding-hackers

・Samba チームが複数のバージョンの Samba についてのセキュリティアップデートをリリース。(10/29)
https://www.us-cert.gov/ncas/current-activity/2019/10/29/samba-releases-security-updates

・Microsoft 社が反ドーピング組織及びスポーツ機関を標的としたサイバー攻撃に関する情報をリリース。(10/29)
https://www.us-cert.gov/ncas/current-activity/2019/10/29/microsoft-reports-global-cyberattacks-sporting-and-anti-doping

・米国全州情報共有・分析センター（MS-ISAC)がハイパーテキストプリプロセッサー(PHP)における脆弱性に関する注意喚起をリリース。(10/30)
https://www.us-cert.gov/ncas/current-activity/2019/10/30/ms-isac-releases-advisory-php-vulnerabilities

・米国全州情報共有・分析センター（MS-ISAC)がサービス提供が終了するソフトウェアのリストをリリース。(10/30)
https://www.us-cert.gov/ncas/current-activity/2019/10/30/ms-isac-releases-eos-software-report-list

・Google が Chrome version 78.0.3904.87 をリリース。(10/31)
https://www.us-cert.gov/ncas/current-activity/2019/10/31/google-releases-security-updates-chrome

・１１月は米国重要インフラセキュリティ・レジリエンス月間。(11/1)
https://www.us-cert.gov/ncas/current-activity/2019/11/01/national-critical-infrastructure-security-and-resilience-month

・米国国土安全保障省（ＤＨＳ）サイバーセキュリティ・インフラセキュリティ庁（ＣＩＳＡ）がサイバーセキュリティ評価ツール（ＣＳＥＴ）version 9.2 をリリース。(11/04)
https://www.us-cert.gov/ncas/current-activity/2019/11/04/cset-version-92-now-available

・米国サイバー軍が７つのマルウエアサンプルを公開。(11/06)
https://www.us-cert.gov/ncas/current-activity/2019/11/06/us-cyber-command-shares-seven-new-malware-samples

・Cisco 社が同社製品についてのセキュリティアップデートをリリース。(11/07)
https://www.us-cert.gov/ncas/current-activity/2019/11/07/cisco-releases-security-updates

・マルウエア解析レポート：北朝鮮政府が使用するトロイの木馬型マルウエア「HOPLIGHT」(10/31)
https://www.us-cert.gov/ncas/analysis-reports/ar19-304a

・１０月２１日の週の脆弱性概報(10/28)
https://www.us-cert.gov/ncas/bulletins/SB19301

・１０月２８日の週の脆弱性概報(11/04)
https://www.us-cert.gov/ncas/bulletins/sb19-308

・Honeywell 社の入退出管理システムに重要な機能に対する認証の欠如の脆弱性。(10/24)
https://www.us-cert.gov/ics/advisories/icsa-19-297-02

・Rittal 社の冷却器に重要な機能に対する認証の欠如等の脆弱性。(10/24)
https://www.us-cert.gov/ics/advisories/icsa-19-297-01
※CVSSv3 では基本値「9.1」となっています。

・Philips 社の周産期情報システムに他の領域へのリソースの漏洩の脆弱性。(10/24)
https://www.us-cert.gov/ics/advisories/icsma-19-297-01

・Moxa 社のイーサネット機器にバッファオーバーフロー等の脆弱性。(10/24)
https://www.us-cert.gov/ics/advisories/ICSA-19-057-01
※CVSSv3 では基本値「9.8」となっています。

・Phoenix Contact 社のオートメーション用ソフトウェアに不適切な入力検証の脆弱性。(10/29)
https://www.us-cert.gov/ics/advisories/icsa-19-302-01
※CVSSv3 では基本値「7.8」となっています。

・Honeywell 社の監視カメラシステムにキャプチャリプレイ攻撃による認証機構の迂回等の脆弱性。(10/31)
https://www.us-cert.gov/ics/advisories/icsa-19-304-04
https://www.us-cert.gov/ics/advisories/icsa-19-304-03
https://www.us-cert.gov/ics/advisories/icsa-19-304-02
※CVSSv3 では基本値「7.5」となっています。

・Advantech 社のＩｏＴ用ソフトウェアにパストラバーサル等の脆弱性。(10/31)
https://www.us-cert.gov/ics/advisories/icsa-19-304-01
※CVSSv3 では基本値「9.8」となっています。

・VxWorks のリアルタイムＯＳ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（更新）。(11/05)
https://www.us-cert.gov/ics/advisories/icsma-19-274-01
※CVSSv3 では基本値「9.8」となっています。

・オムロン社の HMI ソフトウェアに廃止された機能の使用の脆弱性。(11/06)
https://www.us-cert.gov/ics/advisories/icsa-19-309-01
※CVSSv3 では基本値「9.8」となっています。

・富士電機の遠隔監視ソフトウェアにヒープベースのバッファオーバーフローの脆弱性。(11/07)
https://www.us-cert.gov/ics/advisories/icsa-19-311-02
※CVSSv3 では基本値「7.8」となっています。

・三菱電機のＦＡ用シーケンサに適切でないリソース消費制限の脆弱性。(11/07)
https://www.us-cert.gov/ics/advisories/icsa-19-311-01
※CVSSv3 では基本値「7.5」となっています。

・Medtronic 社の電気手術器用機器に資格情報がハードコーディングされている問題等の脆弱性。(11/07)
https://www.us-cert.gov/ics/advisories/icsma-19-311-02
https://www.us-cert.gov/ics/advisories/icsma-19-311-01

※CVSSv3 では基本値「9.8」となっています。

・Philips 社の電子カルテシステムにクロスサイトスクリプティング等の脆弱性。(11/07)
https://www.us-cert.gov/ics/advisories/ICSMA-19-120-01

■―――――――――――――――――――――――――――――――――□

┃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、１１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――――┤

■―――――――――――――――――――――――――――――――――□