■―――――――――――――――――――――――――――――――――□

┃　　◆◆　NISC 重要インフラニュースレター　◆◆

┃　　（２０１９年１２月１０日発行 第２５１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２５１号の目次　◆―――――――――――――――――――――――┐

├―――┤

○今号は、１１月２６日～１２月９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）マルウェア Emotet に関する注意喚起

・マルウエア Emotet の感染に関する注意喚起(公開)(JPCERT/CC)(11/27)
https://www.jpcert.or.jp/at/2019/at190044.html

・CyberNewsFlash「マルウエア Emotet の感染活動について」(JPCERT/CC)(11/27)
https://www.jpcert.or.jp/newsflash/2019112701.html

・JPCERT/CC Eyes「マルウエア Emotet への対応 FAQ」(JPCERT/CC)(12/02)
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

・「Emotet」と呼ばれるウイルスへの感染を狙うメールについて(IPA)(12/02)
https://www.ipa.go.jp/security/announce/20191202.html

（２）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複数の脆弱性(JVN)(11/26)
https://jvn.jp/vu/JVNVU94282488/index.html

（３）その他

・CyberNewsFlash「長期休暇に備えて 2019/12」(JPCERT/CC)(12/05)
https://www.jpcert.or.jp/newsflash/2019120501.html

・WordPress 用プラグイン WP Spell Check 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)(11/26)
https://jvn.jp/jp/JVN26838191/index.html

・STAMP Workbench インストーラーにおける DLL 読込みに関する脆弱性について(IPA、JVN)(11/26)
https://www.ipa.go.jp/ikc/info/20191126.html
https://jvn.jp/jp/JVN19386781/index.html
※CVSSv3 では基本値「7.8」となっています。

・エムオーテックス株式会社製の複数の製品における権限昇格の脆弱性(JVN)(12/02)
https://jvn.jp/jp/JVN49068796/index.html
※CVSSv3 では基本値「7.8」となっています。

・OpenSSL におけるバッファオーバーフローの脆弱性(JVN)(12/09)
https://jvn.jp/vu/JVNVU90419651/index.html

２．政府機関の動き

● 警察庁

・PHP-FPM の脆弱性（CVE-2019-11043）を標的としたアクセスの観測等について(11/28)
https://www.npa.go.jp/cyberpolice/important/2019/201911281.html

・令和元年 10 月期観測資料(11/28)
https://www.npa.go.jp/cyberpolice/important/2019/201911282.html

３．関係機関の動き

（１）ＩＰＡ

・インターネット安全教室の指導用教材（試行版）を公開しました。(11/28)
https://www.ipa.go.jp/security/keihatsu/material.html

・「サイバーレスキュー隊（J-CRAT）活動状況 2019 年度上半期」を公開しました(11/29)
https://www.ipa.go.jp/security/J-CRAT/index.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2019-11-27 号(11/27)
https://www.jpcert.or.jp/wr/2019/wr194601.html

・JPCERT/CC Eyes「PSIRT Services Framework v1.0 日本語版」(12/03)
https://blogs.jpcert.or.jp/ja/2019/12/psirt-services-framework-v10.html

・Weekly Report 2019-12-04 号(12/04)
https://www.jpcert.or.jp/wr/2019/wr194701.html

４．海外の動き

● 米国 DHS

・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。(12/04)
https://www.us-cert.gov/ncas/current-activity/2019/12/04/mozilla-releases-security-updates-firefox-and-firefox-esr

・ニュージーランドサイバーセキュリティセンター（NCSC-NZ）が、経営層向けのサイバー・ガバナンスに関する記事をリリース。(12/05)
https://www.us-cert.gov/ncas/current-activity/2019/12/05/ncsc-nz-releases-cyber-governance-resource-leaders
https://www.ncsc.govt.nz/newsroom/gcsb-encourages-leaders-to-connect-with-cyber-security-governance/
https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Security-Resilience-Assessment.pdf

・Microsoft 社が Windows Hello for Business (WHfB)に関するセキュリティアドバイザリーをリリース。(12/05)
https://www.us-cert.gov/ncas/current-activity/2019/12/05/microsoft-releases-security-advisory-windows-hello-business

・豪州サイバーセキュリティセンター（ＡＣＳＣ）が、cross domain solution（CDS）技術に関するガイドをリリース。(12/05)
https://www.us-cert.gov/ncas/current-activity/2019/12/05/acsc-releases-fundamentals-cross-domain-solutions
https://www.cyber.gov.au/publications/fundamentals-of-cross-domain-solutions
https://www.cyber.gov.au/sites/default/files/2019-12/PROTECT%20-%20Fundamentals%20of%20Cross%20Domain%20Solutions%20%28December%202019%29.pdf

・Vmware 社が ESXi 及び Horizon DaaS についてのセキュリティアップデートをリリース。(12/06)
https://www.us-cert.gov/ncas/current-activity/2019/12/06/vmware-releases-security-updates-esxi-and-horizon-daas

・２０１９年１１月２５日の週の脆弱性概報。(12/02)
https://www.us-cert.gov/ncas/bulletins/sb19-336

・２０１９年１２月２日の週の脆弱性概報。(12/09)
https://www.us-cert.gov/ncas/bulletins/sb19-343

・ABB 社の保護リレーに不適切な入力検証等の脆弱性。(11/26)
https://www.us-cert.gov/ics/advisories/icsa-19-330-02
https://www.us-cert.gov/ics/advisories/icsa-19-330-01
※CVSSv3 では基本値「10.0」となっています。

・Moxa 社の産業用無線機器に不適切な入力検証等の脆弱性。(12/03)
https://www.us-cert.gov/ics/advisories/icsa-19-337-02

※CVSSv3 では基本値「9.8」となっています。

・Reliable Controls 社のライセンス管理機器に引用符で囲まれていないプログラムパスの脆弱性。(12/03)
https://www.us-cert.gov/ics/advisories/icsa-19-337-01
※CVSSv3 では基本値「7.8」となっています。

・Weidmueller 社の産業用イーサネットスイッチにブルートフォース攻撃により認証機能の迂回を許してしまう問題等の脆弱性。(12/05)
https://www.us-cert.gov/ics/advisories/icsa-19-339-02
※CVSSv3 では基本値「9.8」となっています。

・Thales 社のセキュリティ製品にリンクフォローイングの脆弱性。(12/05)
https://www.us-cert.gov/ics/advisories/icsa-19-339-01
※CVSSv3 では基本値「7.3」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、１２月２４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―――┤

■―――――――――――――――――――――――――――――――――□