ＮＩＳＣ重要インフラニュースレター第２８７号

中国地域サイバーセキュリティ連絡会へ入会頂いた皆様へ

中国地域サイバーセキュリティ連絡会　事務局の木坂です。

NISCより、重要インフラニュースレター第２８７号（6/8）が
下記のとおり発行されましたので、お送りいたします。
（必要に応じて幅広く展開していただいて結構です）

既にご購読の方で、配信不要の場合は事務局までお知らせください。

■━━━━━━━━━━━━━━━━━━━━━━━━━━━━□
┃　◆◆　NISC重要インフラニュースレター　◆◆
┃　（２０２１年６月８日発行 第２８７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２８７号の目次　◆──────────────┐

├──────────────────────────────┤

○今号は、５月２５日～６月７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）ランサムウエアに関する注意喚起

・Neuberger 米大統領副補佐官は民間企業経営層に宛て、ランサムウエアに対する注意喚起を趣旨とするレターを発し、ランサムウエアから保護する 5 つの対策(①定期的なバックアップの取得及びテスト、②迅速なパッチ適用、③業務継続計画の準備、④セキュリティチーム強化、⑤ネットワークのセグメント化)を紹介
https://www.spencerfane.com/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf

・ランサムウエア「Conti」の攻撃が医療機関と救急医療のネットワークに影響を与える(FBI)(05/20)
https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf

（２）プロジェクト情報共有ツールに関する注意喚起

・プロジェクト情報共有ツールに対する不正アクセス対策の確認に関する政府機関等及び事業者等への注意喚起の発出について(NISC)(05/25)
https://www.nisc.go.jp/press/pdf/projectist20210525.pdf

（３）Google 製品(Chrome)に関する脆弱性

・Google は Chrome のセキュリティアップデートをリリース(米国 DHS)(05/26)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/26/google-releases-security-updates-chrome

（４）VMware 製品に関する脆弱性

・VMware vCenter Server の複数の脆弱性（CVE-2021-21985、CVE-2021-21986）に関する注意喚起(JPCERT/CC、米国 DHS)(05/26、06/04)
https://www.jpcert.or.jp/at/2021/at210025.html
https://us-cert.cisa.gov/ncas/current-activity/2021/06/04/unpatched-vmware-vcenter-software

（５）その他

・CyberNewsFlash「複数の Apple 製品のアップデートについて」(JPCERT/CC)(05/25)
https://www.jpcert.or.jp/newsflash/2021052501.html

・Bluetooth コア仕様およびメッシュ仕様に複数の脆弱性(JVN)(05/26)
https://jvn.jp/vu/JVNVU99594334/

・Pulse Secure 製 Pulse Connect Secure にバッファオーバーフローの脆弱性(JVN)(05/26)
https://jvn.jp/vu/JVNVU98263390/
※CVSSv3 では基本値「8.5」となっています。

・Zettlr におけるクロスサイトスクリプティングの脆弱性(JVN)(05/26)
https://jvn.jp/jp/JVN98239374/

・Luxion 製 KeyShot における複数の脆弱性(JVN)(05/27)
https://jvn.jp/vu/JVNVU98395603/
※CVSSv3 では基本値「7.8」となっています。

・複数の Rockwell Automation 製品に中間者攻撃が可能な脆弱性(JVN)(05/27)
https://jvn.jp/vu/JVNVU99402132/

・Checkbox Survey に安全でないデシリアライゼーションの脆弱性(JVN)(05/27)
https://jvn.jp/vu/JVNVU99816551/

・三菱電機製 MELSEC iQ-R シリーズの MELSOFT 交信ポートにおけるリソース枯渇の脆弱性(JVN)(05/27)
https://jvn.jp/vu/JVNVU98060539/

・GENIVI Alliance 製 dlt-daemon にヒープベースのバッファオーバーフローの脆弱性(JVN)(05/28)
https://jvn.jp/vu/JVNVU94613356/
※CVSSv3 では基本値「9.8」となっています。

・Sensormatic Electronics 製 VideoEdge に境界条件の判定に関する脆弱性(JVN)(05/28)
https://jvn.jp/vu/JVNVU91343607/
※CVSSv3 では基本値「7.8」となっています。

・MesaLabs 製 AmegaView における複数の脆弱性(JVN)(05/28)
https://jvn.jp/vu/JVNVU98845656/
※CVSSv3 では基本値「10.0」となっています。

・ISC DHCP におけるバッファオーバーフローの脆弱性(JVN)(05/28)
https://jvn.jp/vu/JVNVU95111565/

・バッファロー製ルータ WSR-1166DHP3 および WSR-1166DHP4 における複数の脆弱性(JVN)(05/31)
https://jvn.jp/vu/JVNVU92862829/

・複数のトレンドマイクロ株式会社製品の脆弱性に対するアップデート（2021 年 5 月)(JVN)(05/31)
https://jvn.jp/vu/JVNVU93332929/

・Hillrom 製 Welch Allyn medical device management tools に複数の脆弱性(JVN)(06/02)
https://jvn.jp/vu/JVNVU94926489/

・スマートフォンアプリ「goo blog（goo ブログ)」におけるアクセス制限不備の脆弱性(JVN)(06/02)
https://jvn.jp/jp/JVN91691168/

・スマートフォンアプリ「ATOM - スマートライフ」におけるサーバ証明書の検証不備の脆弱性(JVN)(06/03)
https://jvn.jp/jp/JVN64064138/

・Advantech 製 iView における複数の脆弱性(JVN)(06/04)
https://jvn.jp/vu/JVNVU92160646/
※CVSSv3 では基本値「9.1」となっています。

・urllib3 における、正規表現を用いたサービス運用妨害（ReDoS）の脆弱性(JVN)(06/07)
https://jvn.jp/vu/JVNVU92413403/

□━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━■

┃２．政府機関の動き

┼───────────────────────────────┼

（１）ＮＩＳＣ

・重要インフラ専門調査会第 25 回会合を開催(05/31)
https://www.nisc.go.jp/conference/cs/ciip/index.html#ciip25

・普及啓発・人材育成専門調査会第 15 回会合を開催(06/02)
https://www.nisc.go.jp/conference/cs/jinzai/index.html

（２）総務省

・「テレワークセキュリティガイドライン（第 5 版）」（案）に対する意見募集の結果及び当該ガイドラインの公表(05/31)
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00111.html

■━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━□

┃３．関係機関の動き

┼───────────────────────────────┼

●　ＪＰＣＥＲＴ　コーディネーションセンター

・Weekly Report 2021-05-26 号(05/26)
https://www.jpcert.or.jp/wr/2021/wr212001.html

・JPCERT/CC Eyes「ラッキービジター詐欺で使用される PHP マルウェア」(06/01)
https://blogs.jpcert.or.jp/ja/2021/06/php_malware.html

・Weekly Report 2021-06-02 号(06/02)
https://www.jpcert.or.jp/wr/2021/wr212101.html

□━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━■

┃４．海外の動き

● 米国 DHS

・政府機関、政府間組織及び非政府組織を対象とする高度なスピアフィッシングキャンペーン(05/29)
https://us-cert.cisa.gov/ncas/alerts/aa21-148a

・高度なスピアフィッシングキャンペーンに関する CISA と FBI の共同サイバーセキュリティ・アドバイザリ(05/28)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/28/joint-cisa-fbi-cybersecurity-advisory-sophisticated-spearphishing

・Drupal はセキュリティアップデートをリリース(05/27)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/27/drupal-releases-security-updates

・Pulse Connect Secure のアラートを更新(05/27)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/27/updates-alert-pulse-connect-secure

・ Microsoft は NOBELIUM の新しい活動を公表(05/27)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/27/microsoft-announces-new-campaign-nobelium

・FBI は Fortinet FortiOS の脆弱性悪用について更新(05/28)
https://us-cert.cisa.gov/ncas/current-activity/2021/05/28/fbi-update-exploitation-fortinet-fortios-vulnerabilities

・Cisco は複数製品のセキュリティアップデートをリリース(06/02)
https://us-cert.cisa.gov/ncas/current-activity/2021/06/02/cisco-releases-security-updates-multiple-products

・Cisco は複数製品のセキュリティアップデートをリリース(06/03)
https://us-cert.cisa.gov/ncas/current-activity/2021/06/03/cisco-releases-security-updates-multiple-products

・Mozilla は Firefox のセキュリティアップデートをリリース(06/02)
https://us-cert.cisa.gov/ncas/current-activity/2021/06/02/mozilla-releases-security-updates-firefox

・2021 年 5 月 24 日の週の脆弱性概報(05/31)
https://us-cert.cisa.gov/ncas/bulletins/sb21-151

・2021 年 5 月 31 日の週の脆弱性概報(06/07)
https://us-cert.cisa.gov/ncas/bulletins/sb21-158

・三菱電機の FA エンジニアリング製品に引用符で囲まれていないプログラムパスの脆弱性(更新)(05/28)
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-04
※CVSSv3 では基本値「8.3」となっています。

・三菱電機の FA 製品にパストラバーサルの脆弱性(更新)(05/27)
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-03
※CVSSv3 では基本値「8.3」となっています。

・三菱電機の FA エンジニアリング用ソフトウェア製品にヒープベースのバッファ オーバーフローの脆弱性(更新)(05/27)
https://us-cert.cisa.gov/ics/advisories/icsa-21-049-02
※CVSSv3 では基本値「7.5」となっています。

・Siemens の JT2Go 及び Teamcenter Visualization に範囲外の読み取りの脆弱性(更新)(05/27)
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-03
※CVSSv3 では基本値「7.8」となっています。

・Siemens の JT2Go 及び Teamcenter Visualization に範囲外の読み取りの脆弱性(更新)(05/27)
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-06
※CVSSv3 では基本値「7.8」となっています。

・Siemens の JT2Go 及び Teamcenter Visualization に範囲外の読み取りの脆弱性

(05/27)
https://us-cert.cisa.gov/ics/advisories/icsa-21-147-04
※CVSSv3 では基本値「7.8」となっています。

・Siemens の SIMATIC S7-1200 及び S7-1500 CPU Families にメモリバッファの境界内での操作の不適切な制限の脆弱性(06/01)
https://us-cert.cisa.gov/ics/advisories/icsa-21-152-01
※CVSSv3 では基本値「8.1」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、２０２１年６月２２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。