ＮＩＳＣ重要インフラニュースレター第２８４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２８４号（4/27）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４月２７日発行 第２８４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２８４号の目次　◆―――――――――――――――――――――――――――┐

├―――┤
○今号は、４月１３日～４月２６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）大型連休等に向けた注意喚起

・大型連休等に伴うセキュリティ上の留意点について(NISC)(04/26)
https://www.nisc.go.jp/active/infra/pdf/renkyu20210426.pdf

・ゴールデンウィークにおける情報セキュリティに関する注意喚起(IPA)(04/21)
https://www.ipa.go.jp/security/topics/alert20210421.html

（２）Pulse Connect Secure に関する脆弱性(注意喚起)

・Pulse Connect Secure の脆弱性対策について(CVE-2021-22893)(IPA、JPCERT/CC、JVN、米国 DHS、米国 CERT/CC)(04/21)
https://www.ipa.go.jp/security/ciadr/vul/alert20210421.html
https://www.jpcert.or.jp/at/2021/at210019.html
https://jvn.jp/vu/JVNVU94842247/
https://us-cert.cisa.gov/ncas/alerts/aa21-110a
https://us-cert.cisa.gov/ncas/current-activity/2021/04/20/cisa-releases-alert-exploitation-pulse-connect-secure
https://us-cert.cisa.gov/ncas/current-activity/2021/04/20/cisa-issues-emergency-directive-pulse-connect-secure
https://kb.cert.org/vuls/id/213092
※CVSSv3 では基本値「10.0」となっています。

（３）Microsoft 製品に関する脆弱性

・2021 年 4 月マイクロソフトセキュリティ更新プログラムに関する注意喚起(JPCERT/CC)(04/14)
https://www.jpcert.or.jp/at/2021/at210017.html

・Microsoft 製品の脆弱性対策について(2021 年 4 月)(IPA)(04/14)
https://www.ipa.go.jp/security/ciadr/vul/20210414-ms.html

・Windows 版 MySQL に権限昇格の脆弱性(JVN)(04/22)
https://jvn.jp/vu/JVNVU92599577/

（４）Adobe 製品に関する脆弱性

・複数の Adobe 製品のアップデートについて(JPCERT/CC、米国 DHS)(04/13、

04/14)
https://www.jpcert.or.jp/newsflash/2021041401.html
https://us-cert.cisa.gov/ncas/current-activity/2021/04/13/adobe-releases-security-updates

（５）Oracle 製品に関する脆弱性
・2021 年 4 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起(JPCERT/CC、IPA、米国 DHS)(04/20、04/21)
https://www.jpcert.or.jp/at/2021/at210018.html
https://www.ipa.go.jp/security/ciadr/vul/20210421-jre.html
https://us-cert.cisa.gov/ncas/current-activity/2021/04/20/oracle-releases-april-2021-critical-patch-update

（６）Google 製品(Chrome)の脆弱性
・Google は Chrome のセキュリティアップデートをリリース(米国 DHS、Google)(04/13、04/15、04/21、04/26)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/13/google-releases-security-updates-chrome
https://us-cert.cisa.gov/ncas/current-activity/2021/04/15/google-releases-security-updates-chrome
https://us-cert.cisa.gov/ncas/current-activity/2021/04/21/google-releases-security-updates-chromehttps://us-cert.cisa.gov/ncas/current-activity/2021/04/20/cisa-releases-alert-exploitation-pulse-connect-secure
https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html

（６）その他
・スマートフォンアプリ「ぐるなび」におけるアクセス制限不備の脆弱性(JVN)(04/14)
https://jvn.jp/jp/JVN54025691/index.html

・Advantech 製 WebAccess/SCADA に重要な情報に対するアクセス権の不適切な割り当ての脆弱性(JVN)(04/14)
https://jvn.jp/vu/JVNVU99008843/index.html
※CVSSv3 では基本値「8.8」となっています。

・Schneider Electric 製 SoMachine Basic に XML 外部実体参照（XXE）に関する脆弱性(JVN)(04/14)
https://jvn.jp/vu/JVNVU92527693/index.html
※CVSSv3 では基本値「8.6」となっています。

・Schneider Electric 製 C-Bus Toolkit における複数の脆弱性(JVN)(04/16)
https://jvn.jp/vu/JVNVU94098767/
※CVSSv3 では基本値「8.8」となっています。

・ジェイテクト製 TOYOPUC シリーズにおけるサービス運用妨害（DoS）の脆弱性(JVN)(04/15)
https://jvn.jp/vu/JVNVU92524237/
※CVSSv3 では基本値「7.5」となっています。

・Siemens 製品に対するアップデート（2021 年 4 月)(JVN)(04/15)
https://jvn.jp/vu/JVNVU96269392/

・CyberNewsFlash「GarageBand に関するアップデートについて」(JPCERT/CC)(04/15)
https://www.jpcert.or.jp/newsflash/2021041502.html

・EIPStackGroup 製 OpENer Ethernet/IP における複数の脆弱性(JVN)(04/16)
https://jvn.jp/vu/JVNVU93310734/
※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パスワードマネージャーにおける DLL 読み込みに関する脆弱性(JVN)(04/19)
https://jvn.jp/vu/JVNVU98074915/
※CVSSv3 では基本値「7.8」となっています。

・トレンドマイクロ製品に搭載された検索エンジンにおけるサービス運用妨害（DoS）の脆弱性(JVN)(04/20)
https://jvn.jp/vu/JVNVU93009588/

・ウイルスバスター ビジネスセキュリティおよび Trend Micro Security (for Mac) における複数の脆弱性(JVN)(04/20)
https://jvn.jp/vu/JVNVU92208501/
※CVSSv3 では基本値「7.8」となっています。

・ウイルスバスター ビジネスセキュリティサービスにおける複数の脆弱性(JVN)(04/20)
https://jvn.jp/vu/JVNVU97680506/
※CVSSv3 では基本値「7.8」となっています。

・Trend Micro Apex One, Apex One SaaS およびウイルスバスター コーポレートエディションの脆弱性(CVE-2020-24557)に関する注意喚起(JPCERT/CC)(04/21)
https://www.jpcert.or.jp/at/2021/at210020.html

・Apex One、Apex One SaaS およびウイルスバスター コーポレートエディションにおける複数の脆弱性(JVN)(04/21)
https://jvn.jp/vu/JVNVU93491927/
※CVSSv3 では基本値「7.8」となっています。

・Hitachi ABB Power Grids 製 Ellipse APM におけるクロスサイトスクリプティングの脆弱性(JVN)(04/22)
https://jvn.jp/vu/JVNVU97456009/

・Rockwell Automation 製 Stratix Switches に複数の脆弱性(JVN)(04/22)
https://jvn.jp/vu/JVNVU99743643/
※CVSSv3 では基本値「7.8」となっています。

・複数の Delta Electronics 製品に複数の脆弱性(JVN)(04/22)
https://jvn.jp/vu/JVNVU93609621/
※CVSSv3 では基本値「9.8」となっています。

・Eaton 製 Intelligent Power Manager における複数の脆弱性(JVN)(04/22)
https://jvn.jp/vu/JVNVU98754213/
※CVSSv3 では基本値「8.7」となっています。

・三菱電機製 GOT の VNC サーバ機能におけるパスワード認証回避の脆弱性(JVN)(04/22)
https://jvn.jp/vu/JVNVU97615777/index.html

・yappa-ng におけるクロスサイトスクリプティングの脆弱性(JVN)(04/22)
https://jvn.jp/jp/JVN55833077/index.html

・Qlocker によるランサムウェア攻撃に対するご案内（QNAP)(04/22)
https://www.qnap.com/ja-jp/news/2021/qlocker-%E3%81%AB%E3%82%88%E3%82%8B%E3%83%A9%E3%83%B3%E3%82%B5%E3%83%A0%E3%82%A6%E3%82%A7%E3%82%A2%E6%94%BB%E6%92%83%E3%81%AB%E5%AF%BE%E3%81%99%E3%82%8B%E3%81%94%E6%A1%88%E5%86%85qnap-nas-%E3%82%92%E5%AE%89%E5%85%A8%E3%81%AB%E3%81%8A%E4%BD%BF%E3%81%84%E3%81%84%E3%81%9F%E3%81%A0%E3%81%8F%E3%81%9F%E3%82%81%E3%81%AB

・Horner Automation 製 Cscape に複数の脆弱性(JVN)(04/23)
https://jvn.jp/vu/JVNVU96064711/index.html
※CVSSv3 では基本値「8.4」となっています。

・FileZen の脆弱性(CVE-2021-20655)に関する注意喚起(JPCERT/CC)(04/23)
https://www.jpcert.or.jp/at/2021/at210009.html
・Horner Automation 製 Cscape に複数の脆弱性(JVN)(04/23)
https://jvn.jp/vu/JVNVU96064711/
※CVSSv3 では基本値「8.4」となっています。

２．政府機関の動き

（１）ＮＩＳＣ

・「政府機関等のサイバーセキュリティ対策のための統一基準群」の改定(案)に関する意見の募集について(04/26)
https://www.nisc.go.jp/active/general/kijun2021.html

（２）警察庁

・犯罪インフラ化するＳＭＳ認証代行への対策について(04/22)
https://www.npa.go.jp/cyber/policy/pdf/R030422_SMStaisaku.pdf

（３）総務省
・「スマートシティセキュリティガイドライン（第 2.0 版）」(案)に対する意見募集(04/23)
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00109.html

（４）経済産業省
・機器のサイバーセキュリティ確保のためのセキュリティ検証の手引きを取りまとめました(04/19)
https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

・「サイバーセキュリティ体制構築・人材確保の手引き」（第 1.1 版）を取りまとめました(04/26)
https://www.meti.go.jp/press/2021/04/20210426002/20210426002.html

３．関係機関の動き

（１）ＩＰＡ
・STAMP Workbench の不具合を修正した Ver.1.0.2 を公開(04/13)
https://www.ipa.go.jp/sec/tools/stamp_workbench.html

・「各国政府のセキュリティ政策に関する実施体制、法制度及び認証制度調査」報告書を公開しました。(04/14)
https://www.ipa.go.jp/security/fy2021/reports/crypto_survey/index.html

・「情報セキュリティ安心相談窓口の相談状況［2021 年第 1 四半期（1 月～3 月)]」を公開しました。(04/20)
https://www.ipa.go.jp/security/txt/2021/q1outline.html

・脆弱性対策情報データベース JVN iPedia の登録状況［2021 年第 1 四半期（1 月～3 月）] (04/21)
https://www.ipa.go.jp/security/vuln/report/JVNiPedia2021q1.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2021-04-14 号(04/14)
https://www.jpcert.or.jp/wr/2021/wr211501.html

・CyberNewsFlash「2021 年 1 月から 3 月を振り返って」(04/15)
https://www.jpcert.or.jp/newsflash/2021041501.html

・JPCERT/CC インシデント報告対応レポート［2021 年 1 月 1 日～2021 年 3 月 31 日］(04/15)
https://www.jpcert.or.jp/ir/report.html

・JPCERT/CC 活動四半期レポート［2021 年 1 月 1 日～2021 年 3 月 31 日］(04/15)
https://www.jpcert.or.jp/pr/index.html

・JPCERT/CC インターネット定点観測レポート［2021 年 1 月 1 日～2021 年 3 月 31 日］(04/20)
https://www.jpcert.or.jp/tsubame/report/report202101-03.html

・Weekly Report 2021-04-21 号(04/21)
https://www.jpcert.or.jp/wr/2021/wr211601.html

・ソフトウェア等の脆弱性関連情報に関する届出状況[2021 年第 1 四半期（1 月～3 月）](IPA、JPCERT/CC)(04/22)
https://www.ipa.go.jp/security/vuln/report/vuln2021q1.html
https://www.jpcert.or.jp/report/press.html

４．海外の動き

（１）米国 DHS

・CHIRP IOC 検出ツールを使用した侵害後の脅威アクティビティの検出(04/15)
https://us-cert.cisa.gov/ncas/alerts/aa21-077a

・米国と同盟国を標的としたロシアの SVR に関する NSA-CISA-FBI 共同勧告(04/16)

https://us-cert.cisa.gov/ncas/current-activity/2021/04/15/nsa-cisa-fbi-joint-advisory-russian-svr-targeting-us-and-allied

・ソーラーウィンズに関連したマルウエアの CISA 及び CNMF(国防総省 サイバー国家ミッションフォース)による分析(04/15)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/15/cisa-and-cnmf-analysis-solarwinds-related-malware

・CISA はインシデント対応中の SUPERNOVA マルウエアの分析レポートをリリース(04/22)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/22/cisa-incident-response-supernova-malware

・ロシア対外情報庁(SVR)のサイバー作戦：ネットワークディフェンダーの動向とベストプラクティス(04/26)
https://us-cert.cisa.gov/ncas/alerts/aa21-116a

・ロシア対外情報庁(SVR)のサイバー作戦に関する FBI-DHS-CISA の共同勧告(04/26)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/26/fbi-dhs-cisa-joint-advisory-russian-foreign-intelligence-service

・ソフトウェアサプライチェーン攻撃に対する防御について、CISA と NIST が新しい機関間リソースをリリース(04/26)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/26/cisa-and-nist-release-new-interagency-resource-defending-against

・Microsoft の 2021 年 4 月のセキュリティ更新プログラムの適用により、新たに公開された Microsoft Exchange の脆弱性を軽減(04/14)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/13/apply-microsoft-april-2021-security-update-mitigate-newly

・SAP は 2021 年 4 月のセキュリティアップデートをリリース(04/13)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/13/sap-releases-april-2021-security-updates

・サイバーセキュリティ研究者をターゲットにした脅威アクター(04/14)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/14/threat-actors-targeting-cybersecurity-researchers

・DNS の実装に影響を与える脆弱性（NAME:WRECK）について(04/15)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/15/namewreck-dns-vulnerabilities

・Juniper Networks はセキュリィティアップデートをリリース(04/15)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/15/juniper-networks-releases-security-updates

・WordPress はセキュリィティとメンテナンスのアップデートをリリース(04/16)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/16/wordpress-releases-security-and-maintenance-update

・Mozilla は Firefox、Firefox ESR 及び Thunderbird のセキュリィティアップデートをリリース(04/20)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/20/mozilla-releases-security-update-firefox-firefox-esr-and

・VMware はセキュリティアップデートをリリース(04/20)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/20/vmware-releases-security-update

・SonicWall は電子メールセキュリティ製品のパッチをリリース(04/21)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/21/sonicwall-releases-patches-email-security-products

・Drupal はセキュリィティアップデートをリリース(04/22)
https://us-cert.cisa.gov/ncas/current-activity/2021/04/22/drupal-releases-security-updates

・2021 年 4 月 12 日の週の脆弱性概報(04/19)
https://us-cert.cisa.gov/ncas/bulletins/sb21-109

・2021 年 4 月 19 日の週の脆弱性概報(04/26)
https://us-cert.cisa.gov/ncas/bulletins/sb21-116

・Siemens の SIMATIC Communication Processor に認証バイパスの脆弱性(更新)(04/13)
https://us-cert.cisa.gov/ics/advisories/ICSA-15-335-03A
※CVSSv3 では基本値「9.8」となっています。

・Siemens 及び PKE の SiNVR、SiVMS Video Server にクリティカル機能認証欠落の脆弱性(更新)(04/14)
https://us-cert.cisa.gov/ics/advisories/icsa-19-344-02
※CVSSv3 では基本値「9.8」となっています。

・Siemens の産業セキュリティ機器に適切でないリソース消費制限等の脆弱性(更新)(04/13)
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-10
※CVSSv3 では基本値「7.5」となっています。

・Siemens のイーサネット機器に不十分なリソース確保の脆弱性(更新)(04/13)
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-07

・Siemens のイーサネットスイッチ等に NULL ポインタ参照等の脆弱性(更新)(04/13)
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-02
※CVSSv3 では基本値「7.5」となっています。

・Siemens の SIMATIC 及び SINAMICS に制御されていない検索パス問題等の脆弱性(更新)(04/13)
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-05
※CVSSv3 では基本値「7.8」となっています。

・Siemens の UMC Stack 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)(04/13)
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05

・Siemens の産業オートメーション機器に整数オーバーフロー等の脆弱性(更新)(04/13)
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-07

・Siemens の組み込み TCP/IP スタックの脆弱性(AMNESIA:33) (更新)(04/13)
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-05

・Siemens の SCALANCE 及び RUGGEDCOM にスタックベースのバッファ オーバーフローの脆弱性（更新）(04/13)
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-03
※CVSSv3 では基本値「8.8」となっています。

・Siemens の SCALANCE 及び RUGGEDCOM に過度の認証試行の不適切な制限の脆弱性(更新)(04/13)
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-02
※CVSSv3 では基本値「8.6」となっています。

・Siemens 及び PKE の SiNVR、SiVMS Video Server にクリティカル機能認証欠落の脆弱性(更新)(04/20)
https://us-cert.cisa.gov/ics/advisories/icsa-20-070-01
※CVSSv3 では基本値「7.5」となっています。

・Siemens の Mendix に不適切な特権管理の脆弱性(04/20)
https://us-cert.cisa.gov/ics/advisories/icsa-21-110-07
※CVSSv3 では基本値「8.1」となっています。

・三菱電機のシーケンサ MELSEC iQ-R series にリソース枯渇の脆弱性(更新)(04/20)
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-02

・日立 ABB パワーグリッドの複数製品に不適切な入力検証の脆弱性(更新)(04/20)
https://us-cert.cisa.gov/ics/advisories/icsa-21-096-01
※CVSSv3 では基本値「7.5」となっています。

■――□

▎6．次回予告

次回は、２０２１年５月１１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。