ＮＩＳＣ重要インフラニュースレター第２９６号

中国地域サイバーセキュリティ連絡会の皆様へ

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２９６号（１０／２６）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１０月２６日発行 第２９６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２９６号の目次　◆―――――――――――――――――――――――――――┐

１．チェックが必要な情報
２．政府機関の動き
３．関係機関の動き
４．海外の動き
５．読者へのお願い
６．次回予告

├―――┤

○今号は、１０月１２日～１０月２５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）米国の上下水道システムへの脅威に関する注意喚起

・米国の上下水道システムに対する進行中のサイバー脅威(米国 DHS)(10/14)

https://us-cert.cisa.gov/ncas/alerts/aa21-287a

https://us-cert.cisa.gov/ncas/current-activity/2021/10/14/ongoing-cyber-threats-us-water-and-wastewater-systems-sector

（２）GPSD に存在する不具合に関する注意喚起

・GPS デーモン(GPSD)のロールバックバグ(米国 DHS)(10/21)

https://us-cert.cisa.gov/ncas/current-activity/2021/10/21/gps-daemon-gpsd-rollover-bug

（３）Adobe 製品に関する脆弱性

・Adobe Acrobat および Reader の脆弱性対策について(APSB21-104)(CVE-2021-40728 等)(米国 DHS、IPA、JPCERT/CC)(10/12、10/13)

https://us-cert.cisa.gov/ncas/current-activity/2021/10/12/adobe-releases-security-updates-multiple-products

https://www.ipa.go.jp/security/ciadr/vul/20211013-adobereader.html

https://www.jpcert.or.jp/at/2021/at210044.html

（４）Microsoft 製品に関する脆弱性

・Microsoft 製品の脆弱性対策について(2021 年 10 月)(米国 DHS、IPA、JPCERT/CC)(10/12、10/13)

https://us-cert.cisa.gov/ncas/current-activity/2021/10/12/microsoft-releases-october-2021-security-updates

https://www.ipa.go.jp/security/ciadr/vul/20211013-ms.html

https://www.jpcert.or.jp/at/2021/at210045.html

（５）Oracle 製品に関する脆弱性

・Oracle Java の脆弱性対策について(CVE-2021-3517 等)(米国 DHS、IPA、JPCERT/CC)(10/19、10/20)

https://us-cert.cisa.gov/ncas/current-activity/2021/10/19/oracle-releases-

october-2021-critical-patch-update
https://www.ipa.go.jp/security/ciadr/vul/20211020-jre.html
https://www.jpcert.or.jp/at/2021/at210046.html

（６）Google 製品に関する脆弱性
・Google が Chrome のセキュリティアップデートをリリース(10/20)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/20/google-releases-security-updates-chrome

（７）その他
・Intel 製品に関する複数の脆弱性について(JPCERT/CC、JVN)(10/13)
https://www.jpcert.or.jp/newsflash/2021101301.html
https://jvn.jp/vu/JVNVU92532697/

・Schneider Electric 製 IGSS における複数の脆弱性(JVN)(10/13)
https://jvn.jp/vu/JVNVU99126536/
※CVSSv3 では基本値「9.8」となっています。

・Schneider Electric 製 ConneXium Network Manager における不適切な権限管理の脆弱性(JVN)(10/15)
https://jvn.jp/vu/JVNVU93150395/
※CVSSv3 では基本値「7.8」となっています。

・複数の Advantech 製品における複数の脆弱性(JVN)(10/13)
https://jvn.jp/vu/JVNVU97189148/
※CVSSv3 では基本値「9.8」となっています。

・CyberNewsFlash「複数のアドビ製品のアップデートについて」(JPCERT/CC)(10/15)
https://www.jpcert.or.jp/newsflash/2021101501.html

・Siemens 製品に対するアップデート(2021 年 10 月)(JVN)(10/13)
https://jvn.jp/vu/JVNVU95938083/

・Siemens 製品に対するアップデート(2021 年 9 月)(JVN)(10/15)

https://jvn.jp/vu/JVNVU96712416/

・Apache Tomcat におけるサービス運用妨害(DoS)の脆弱性(JVN)(10/15)
https://jvn.jp/vu/JVNVU92237586/

・オムロン製 CX-Supervisor における領域外のメモリ参照の脆弱性(JVN)(10/15)
https://jvn.jp/vu/JVNVU90041391/

・三菱電機製 MELSEC iQ-R シリーズ CPU ユニットにおける複数の脆弱性(JVN)(10/15)
https://jvn.jp/vu/JVNVU98578731/
※CVSSv3 では基本値「9.1」となっています。

・三菱電機製 GENESIS64 および MC Works64 の AutoCAD(DWG)ファイルのインポート機能における境界外書き込みの脆弱性(JVN)(10/22)
https://jvn.jp/vu/JVNVU94862669/
※CVSSv3 では基本値「7.8」となっています。

・128 Technology Session Smart Router における認証不備の脆弱性(JVN)(10/18)
https://jvn.jp/jp/JVN85073657/
※CVSSv3 では基本値「9.8」となっています。

・Uffizio 製 GPS Tracker における複数の脆弱性(JVN)(10/19)
https://jvn.jp/vu/JVNVU97257022/
※CVSSv3 では基本値「9.8」となっています。

・「Movable Type」の XMLRPC API における OS コマンド・インジェクションの脆弱性について(JVN#41119755)(IPA、JPCERT/CC、JVN)(10/20)
https://www.ipa.go.jp/security/ciadr/vul/20211020-jvn.html
https://www.jpcert.or.jp/at/2021/at210047.html
https://jvn.jp/jp/JVN41119755/
※CVSSv3 では基本値「9.8」となっています。

・Trane 製 Tracer SC にクロスサイトスクリプティングの脆弱性(JVN)(10/20)
https://jvn.jp/vu/JVNVU90596716/

・AUVESY 製 Versiondog における複数の脆弱性(JVN)(10/21)
https://jvn.jp/vu/JVNVU91590103/
※CVSSv3 では基本値「9.8」となっています。

・トレンドマイクロ製企業向けエンドポイントセキュリティ製品における権限昇格の脆弱性(JVN)(10/25)
https://jvn.jp/vu/ JVNVU92842857/

２．政府機関の動き

（１）ＮＩＳＣ・総務省・経済産業省
・第 14 回「日・ASEAN サイバーセキュリティ政策会議」の結果(10/22)
https://www.nisc.go.jp/press/pdf/AMSJ_CPM_20211021_r2.pdf
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00123.html
https://www.meti.go.jp/press/2021/10/20211022006/20211022006.html

（２）ＮＩＳＣ
・ランサムウェア特設ページを公開(10/13)
https://security-portal.nisc.go.jp/stopransomware/

・重要インフラ専門調査会第 26 回会合を開催(10/25)
https://www.nisc.go.jp/conference/cs/ciip/index.html#ciip26

（３）金融庁
・「金融業界横断的なサイバーセキュリティ演習(Delta Wall Ⅵ)」について(10/19)
https://www.fsa.go.jp/news/r3/20211019/deltawall.html

（４）総務省
・サイバーセキュリティタスクフォース(第 34 回)(10/14 開催)(10/22)

https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00200.html

３．関係機関の動き

（１）ＩＰＡ及びＪＰＣＥＲＴ コーディネーションセンター

・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 3 四半期(7 月～9 月)](10/21)

https://www.ipa.go.jp/security/vuln/report/vuln2021q3.html

https://www.jpcert.or.jp/report/press.html

（２）ＩＰＡ

・「制御システム関連のサイバーインシデント事例」シリーズの第 8 集、第 9 集を公開しました。(10/18)

https://www.ipa.go.jp/security/controlsystem/incident.html

・脆弱性対策情報データベース JVN iPedia の登録状況［2021 年第 3 四半期(7 月～9 月)］(10/20)

https://www.ipa.go.jp/security/vuln/report/JVNiPedia2021q3.html

（３）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2021-10-13 号(10/13)

https://www.jpcert.or.jp/wr/2021/wr214001.html

・JPCERT/CC 活動四半期レポート［2021 年 7 月 1 日～2021 年 9 月 30 日](10/14)

https://www.jpcert.or.jp/pr/index.html

・JPCERT/CC インシデント報告対応レポート［2021 年 7 月 1 日～2021 年 9 月 30 日](10/14)

https://www.jpcert.or.jp/ir/report.html

・CyberNewsFlash「2021 年 7 月から 9 月を振り返って」(10/18)

https://www.jpcert.or.jp/newsflash/2021101801.html

・JPCERT/CC Eyes「TSUBAME レポート Overflow（2021 年 7～9 月)」(10/19)

https://blogs.jpcert.or.jp/ja/2021/10/tsubame_overflow_2021-07-09.html

・JPCERT/CC インターネット定点観測レポート[2021 年 7 月 1 日～2021 年 9 月 30 日](10/19)
https://www.jpcert.or.jp/tsubame/report/report202107-09.html

・Weekly Report 2021-10-20 号(10/20)
https://www.jpcert.or.jp/wr/2021/wr214101.html

４．海外の動き

● 米国 DHS

・Apple が CVE-2021-30883 に対応するセキュリティアップデートをリリース(10/12)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/12/apple-releases-security-update-address-cve-2021-30883

・Juniper Networks が複数製品のセキュリティアップデートをリリース(10/14)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/14/juniper-networks-releases-security-updates-multiple-products

・Siemens の Solid Edge に解放後の使用等の脆弱性(10/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-06
※CVSSv3 では基本値「7.8」となっています。

・Siemens の RUGGEDCOM ROX に不適切な特権管理等の脆弱性(更新)(10/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-259-01
※CVSSv3 では基本値「8.8」となっています。

・Siemens の PROFINET Devices に制限や調整なしのリソースの割り当ての脆弱性(更新)(10/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-03
※CVSSv3 では基本値「7.5」となっています。

・Siemens の Linux ベース製品に不十分な乱数値使用の脆弱性(更新)(10/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-03

※CVSSv3 では基本値「7.4」となっています。

・Siemens の SIMATIC SmartVNC HMI WinCC にバッファ終了後のメモリ位置へのアクセス等の脆弱性(更新)(10/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-12
※CVSSv3 では基本値「9.8」となっています。

・Siemens の SCALANCE W1750D に入力のサイズをチェックしないバッファコピー等の脆弱性(更新)(10/14)
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-14
※CVSSv3 では基本値「9.8」となっています。

・Siemens の PROFINET-IO Stack に制御されていないリソース枯渇の脆弱性(更新)(10/14)
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-04
※CVSSv3 では基本値「7.5」となっています。

・Siemens の産業用リアルタイム機器に不適切な入力検証の脆弱性(更新)(10/14)
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-01
※CVSSv3 では基本値「7.5」となっています。

・Siemens の PROFINET Devices に適切でないリソース消費制限の脆弱性(更新)(10/14)
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-02
※CVSSv3 では基本値「7.5」となっています。

・Siemens の SCALANCE X に予想される行動違反の脆弱性(更新)(10/14)
https://us-cert.cisa.gov/ics/advisories/ICSA-19-085-01

・Siemens の産業オートメーション機器に不適切な入力検証の脆弱性(更新)(10/14)
https://us-cert.cisa.gov/ics/advisories/ICSA-17-339-01
※CVSSv3 では基本値「7.5」となっています。

・Siemens の PROFINET DCP を実装した機器に不適切な入力検証の脆弱性(更新)(10/14)

https://us-cert.cisa.gov/ics/advisories/ICSA-17-129-02

・ランサムウェア「BlackMatter」(10/18)
https://us-cert.cisa.gov/ncas/alerts/aa21-291a

・CISA、FBI 及び NSA が共同でランサムウェア「BlackMatter」に関するサイバーセキュリティアドバイザリをリリース(10/18)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/18/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-blackmatter

・2021 年 10 月 11 日の週の脆弱性概報(10/18)
https://us-cert.cisa.gov/ncas/bulletins/sb21-291

・2021 年 10 月 18 日の週の脆弱性概報(10/25)
https://us-cert.cisa.gov/ncas/bulletins/sb21-298

・Cisco が IOS XE SD-WAN ソフトウエアのセキュリティアップデートをリリース(10/21)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/21/cisco-releases-security-updates-ios-xe-sd-wan-software

・NPM パッケージ ua-parser-js でマルウェアの発見(10/22)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js

・Discourse における重大な RCE の脆弱性(10/24)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/24/critical-rce-vulnerability-discourse

・クラウドサービスやその他のテクノロジーに対する NOBELIUM 攻撃(10/25)
https://us-cert.cisa.gov/ncas/current-activity/2021/10/25/nobelium-attacks-cloud-services-and-other-technologies

■――□

┃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１１月９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。