ＮＩＳＣ重要インフラニュースレター第２９０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290号（7/27）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7月２７日発行 第２９０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２９０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、７月１３日～７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）夏季休暇等に伴うセキュリティ上の留意点について(NISC)(07/21)

https://www.nisc.go.jp/active/infra/pdf/summer20210721.pdf

（２）中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について(注意喚起)(米国 DHS、NISC、警察庁)(07/19)

https://www.nisc.go.jp/press/pdf/20210719NISC_press.pdf

https://www.npa.go.jp/cybersecurity/pdf/20210719pr.pdf

https://us-cert.cisa.gov/ncas/current-activity/2021/07/19/us-government-releases-indictment-and-several-advisories-detailing

https://us-cert.cisa.gov/ncas/alerts/aa21-200a

https://us-cert.cisa.gov/ncas/alerts/aa21-200b

（３）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 7 月)(米国 DHS、IPA、JPCERT/CC)(07/13、07/14)

https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/microsoft-releases-july-2021-security-updates

https://www.ipa.go.jp/security/ciadr/vul/20210714-ms.html

https://www.jpcert.or.jp/at/2021/at210031.html

・CISA が MicrosoftWindows の PrintSpooler で緊急指令を発行(米国 DHS)(07/13)

https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/cisa-issues-emergency-directive-microsoft-windows-print-spooler

（４）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(APSB21-51)(CVE-2021-35980 等)(IPA、JPCERT/CC)(07/14)

https://www.ipa.go.jp/security/ciadr/vul/20210714-adobereader.html

https://www.jpcert.or.jp/at/2021/at210030.html

・複数のアドビ製品のアップデートについて(米国 DHS、JPCERT/CC)(07/14、07/21、07/26)
https://www.jpcert.or.jp/newsflash/2021071401.html
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/adobe-releases-security-updates-multiple-products
https://www.jpcert.or.jp/newsflash/2021072601.html
https://us-cert.cisa.gov/ncas/current-activity/2021/07/21/adobe-releases-security-updates-multiple-products

（５）Mozilla 製品に関する脆弱性
・Mozilla は Firefox 及び Thunderbird のセキュリィティアップデートをリリース(米国 DHS)(07/13)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/mozilla-releases-security-updates-firefox-thunderbird

（６）VMware 製品に関する脆弱性
・VMware がセキュリティアップデートをリリース(米国 DHS)(07/13)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/vmware-releases-security-update

（７）SolarWinds 製品に関する脆弱性
・SolarWinds が Serv-U の脆弱性に関するアドバイザリをリリース(米国 DHS)(07/13)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/solarwinds-releases-advisory-serv-u-vulnerability

（８）Oracle 製品に関する脆弱性
・Oracle Java の脆弱性対策について(CVE-2021-2388 等)(IPA、JPCERT/CC)(07/21)
https://www.ipa.go.jp/security/ciadr/vul/20210721-jre.html
https://www.jpcert.or.jp/at/2021/at210032.html

（９）その他
・Apache Tomcat における複数の脆弱性(JVN)(07/13)
https://jvn.jp/vu/JVNVU91880022/

・スマートフォンアプリ「Retty」における複数の脆弱性(JVN)(07/13)
https://jvn.jp/jp/JVN26891339/

・複数の Schneider Electric 製品に複数の脆弱性(JVN)(07/14)
https://jvn.jp/vu/JVNVU97215148/
※CVSSv3 では基本値「8.6」となっています。

・Siemens 製品に対するアップデート(2021 年 7 月)(JVN)(07/14)
https://jvn.jp/vu/JVNVU99475598/

・光 BB ユニット E-WMTA2.3 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)(07/14)
https://jvn.jp/jp/JVN34364599/

・トレンドマイクロ製 InterScan Web Security シリーズにおけるクロスサイトスクリプティングの脆弱性(JVN)(07/16)
https://jvn.jp/vu/JVNVU94115268/

・Ypsomed 製 mylife に複数の脆弱性(JVN)(07/16)
https://jvn.jp/vu/JVNVU92529180/

・Intel 製 BIOS のテスト設計機能に権限昇格の脆弱性(JVN)(07/16)
https://jvn.jp/vu/JVNVU96708815/
※CVSSv3 では基本値「7.5」となっています。

・GroupSession における複数の脆弱性(JVN)(07/19)
https://jvn.jp/jp/JVN86026700/

・三菱電機製 MELSEC F シリーズ Ethernet インタフェースブロックにおける NULL ポインタ参照の脆弱性(JVN)(07/20)
https://jvn.jp/vu/JVNVU94348759/
※CVSSv3 では基本値「7.5」となっています。

・Minecraft Java Edition におけるディレクトリトラバーサルの脆弱性(JVN)(07/21)
https://jvn.jp/jp/JVN53278122/

・CyberNewsFlash「複数の Apple 製品のアップデートについて(2021 年 7 月)」(JPCERT/CC)(07/26)
https://www.jpcert.or.jp/newsflash/2021072602.html

・Arcadyan 製ソフトウェアを使用するルーターにディレクトリトラバーサルの脆弱性(JVN)(07/26)
https://jvn.jp/vu/JVNVU92877673/index.html
※CVSSv3 では基本値「8.1」となっています。

２．政府機関の動き

● 総務省
・サイバーセキュリティタスクフォース(第 33 回)(07/26)

https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00191.html

３．関係機関の動き

（１）ＩＰＡ
・NIST 文書 SP800-53 rev.5「組織と情報システムのためのセキュリティおよびプライバシー管理策」及び SP800-53B「組織と情報システムのための管理策ベースライン」の翻訳版を公開しました。(07/19)
https://www.ipa.go.jp/security/publications/nist/index.html

・情報セキュリティ白書 2021 の概要および販売開始日について(07/20)
https://www.ipa.go.jp/security/publications/hakusyo/2021.html

・脆弱性対策情報データベース JVN iPedia の登録状況［2021 年第 2 四半期(4 月～6 月)](IPA)(07/21)
https://www.ipa.go.jp/security/vuln/report/JVNiPedia2021q2.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2021-07-14 号(07/14)
https://www.jpcert.or.jp/wr/2021/wr212701.html

・Weekly Report 2021-07-21 号(07/21)
https://www.jpcert.or.jp/wr/2021/wr212801.html

・JPCERT/CC インシデント報告対応レポート［2021 年 4 月 1 日～2021 年 6 月 30 日］(07/15)
https://www.jpcert.or.jp/ir/report.html

・JPCERT/CC 活動四半期レポート［2021 年 4 月 1 日～2021 年 6 月 30 日］(07/15)
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 4 月 1 日～2021 年 6 月 30 日］(07/26)
https://www.jpcert.or.jp/tsubame/report/report202104-06.html

・JPCERT/CC Eyes「TSUBAME レポート Overflow(2021 年 4～6 月)」(07/26)
https://blogs.jpcert.or.jp/ja/2021/07/tsubame_overflow_2021-04-06.html

４．海外の動き

（１）米国 DHS

・Kaseya ランサムウェア攻撃：ガイダンスとリソース(07/13)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/kaseya-ransomware-attack-guidance-and-resources

・SAP が 2021 年 7 月にセキュリティアップデートをリリース(07/13)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/sap-releases-july-2021-security-updates

・Citrix が仮想アプリとデスクトップのセキュリティアップデートをリリース(07/13)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/citrix-releases-

security-updates-virtual-apps-and-desktops

・Citrix がセキュリティアップデートをリリース?(07/20)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/20/citrix-releases-security-updates

・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)(07/13)
https://us-cert.cisa.gov/ics/advisories/icsa-19-253-03
※CVSSv3 では基本値「7.5」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)(07/13)
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05

・Siemens の SIPROTEC 4、SIPROTEC Compact、DIGSI 4、および EN100 イーサネットモジュールに重要な機能に対する認証の欠如等の脆弱性(更新)(07/13)
https://us-cert.cisa.gov/ics/advisories/ICSA-18-067-01
※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) (07/13)
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。

・CISA インサイト：MSP および中小企業向けのガイダンス(07/14)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/14/cisa-insights-guidance-msps-and-small-and-mid-sized-businesses

・新しい Web サイト StopRansomware.gov -ランサムウェアを停止するための米国政府のワンストップロケーション(07/15)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/15/new-stopransomwaregov-website-us-governments-one-stop-location

・Juniper Networks が複数の製品のセキュリティアップデートをリリース(07/15)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/15/juniper-networks-

releases-security-updates-multiple-products

・EOLSonicWallSRA および SMA8.x 製品のパッチが適用されていないランサムウェアリスク(07/15)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/15/ransomware-risk-unpatched-eol-sonicwall-sra-and-sma-8x-products

・Cisco はセキュリティアップデートをリリース(07/16、07/22)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/16/cisco-releases-security-updates
https://us-cert.cisa.gov/ncas/current-activity/2021/07/22/cisco-releases-security-updates

・Fortinet が FortiManager と FortiAnalyzer のセキュリティアップデートをリリース(07/19)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/19/fortinet-releases-security-updates-fortimanager-and-fortianalyzer

・中国のガスパイプライン侵入キャンペーン、2011 年から 2013 年(07/20)
https://us-cert.cisa.gov/ncas/alerts/aa21-201a

・2021 年 7 月 12 日の週の脆弱性概報(07/19)
https://us-cert.cisa.gov/ncas/bulletins/sb21-200

・2021 年 7 月 19 日の週の脆弱性概報(07/26)
https://us-cert.cisa.gov/ncas/bulletins/sb21-207

・ICS を標的とした歴史的に重要なサイバー侵入キャンペーン(07/20)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/20/significant-historical-cyber-intrusion-campaigns-targeting-ics

・Google は Chrome のセキュリティアップデートをリリース(07/21)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/21/google-releases-security-updates-chrome

・MITRE が 2021 年最も危険なソフトウェアエラー25 選を公開(07/21)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/21/2021-cwe-top-25-most-dangerous-software-weaknesses

・Pulse Secure Devices を標的としたマルウェア(07/21)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/21/malware-targeting-pulse-secure-devices

・マルウェア分析レポート(AR21-202A-AR21-202K)(07/21)
MAR-10333209-1.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202a
MAR-10333243-1.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202b
MAR-10334057-1.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202c
MAR-10334057-2.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202d
MAR-10334587-1.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202e
MAR-10334587-2.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202f
MAR-10335467-1.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202g
MAR-10336161-1.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202h
MAR-10336935-1.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202i
MAR-10337580-1.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202j
MAR-10337580-2.v1: パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202k
MAR-10338401-1.v1:: パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202l
MAR-10338868-1.v1：パルスコネクトセキュア
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-202m

・Drupal がセキュリティアップデートをリリース(07/22)
https://us-cert.cisa.gov/ncas/current-activity/2021/07/22/drupal-releases-security-updates

（２）その他
・Microsoft Windows の 印刷スープラ–で Point and Print を使用すると、任意のキュー固有のファイルをインストール(米国 CERT/CC)(07/18)
https://kb.cert.org/vuls/id/131152

・Microsoft Windows の system32 ￥ config ファイルへの非特権ユーザーアクセスの脆弱性(米国 CERT/CC)(07/20)
https://kb.cert.org/vuls/id/506989

■――――――――――――――――――――――――――――――――――□

┃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８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。