

NISC重要インフラニュースレター第292号

中国地域サイバーセキュリティ連絡会の皆様へ

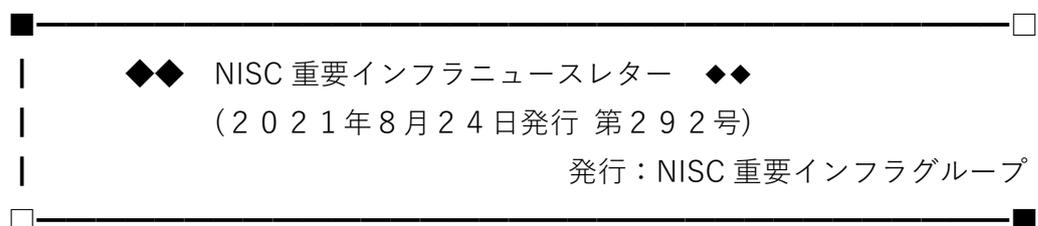
中国地域サイバーセキュリティ連絡会 事務局の末原です。

NISC より、重要インフラニュースレター第292号（8/24）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で結構です）

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。



―◎ 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292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、8月11日～8月23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) 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8月)(IPA、JPCERT/CC)(08/11)
<https://www.ipa.go.jp/security/ciadr/vul/20210811-ms.html>
<https://www.jpccert.or.jp/at/2021/at210034.html>

(2) Google 製品(Chrome)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(米国 DHS)(08/18)
<https://us-cert.cisa.gov/ncas/current-activity/2021/08/18/google-releases-security-updates-chrome>

(3) その他

- ・ 複数のアドビ製品のアップデートについて(JPCERT/CC)(08/11、08/18)
<https://www.jpccert.or.jp/newsflash/2021081101.html>
<https://www.jpccert.or.jp/newsflash/2021081801.html>
- ・ Intel 製品に関する複数の脆弱性について(JPCERT/CC、JVN)(08/11)
<https://www.jpccert.or.jp/newsflash/2021081102.html>
<https://jvn.jp/vu/JVNVU91826524/>
- ・ Siemens 製品に対するアップデート (2021年8月) (JVN)(08/11)
<https://jvn.jp/vu/JVNVU99791395/>
- ・ HTTP Web プロキシや Web アクセラレータの HTTP/2 実装不備による HTTP リクエストスマグリングの脆弱性(JVN)(08/12)
<https://jvn.jp/vu/JVNVU99039870/>
- ・ Plone におけるオープンリダイレクトの脆弱性(JVN)(08/12)
<https://jvn.jp/jp/JVN50804280/>
- ・ NicheStack TCP/IP スタックに複数の脆弱性(JVN)(08/12)
<https://jvn.jp/vu/JVNVU98488549/>

※CVSSv3 では基本値「9.8」となっています。

- ・ Cognex 製 In-Sight OPC Server に信頼できないデータのデシリアライゼーションの脆弱性(JVN)(08/13)

<https://jvn.jp/vu/JVNVU97245059/>

※CVSSv3 では基本値「8.8」となっています。

- ・ Horner Automation 製 Cscape に複数の脆弱性(JVN)(08/13)

<https://jvn.jp/vu/JVNVU96261114/>

※CVSSv3 では基本値「7.8」となっています。

- ・ D-LINK ルータ DSL-2750U に複数の脆弱性(JVN)(08/16)

<https://jvn.jp/vu/JVNVU92088210/>

※CVSSv3 では基本値「8.8」となっています。

- ・ Microsoft Windows の印刷スプーラーにリモートコード実行の脆弱性(JVN)(08/17)

<https://jvn.jp/vu/JVNVU96414899/>

※CVSSv3 では基本値「7.3」となっています。

- ・ Huawei 製 EchoLife HG8045Q における OS コマンドインジェクションの脆弱性(JVN)(08/17)

<https://jvn.jp/jp/JVN41646618/>

- ・ CyberNewsFlash 「Apple 製品のアップデートについて (2021 年 8 月)」(JPCERT/CC)(08/17)

<https://www.jpcert.or.jp/newsflash/2021081103.html>

- ・ 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不適切なパーミッションの割り当ての脆弱性(JVN)(08/18)

<https://jvn.jp/vu/JVNVU90091573/>

- ・ ThroughTek 製 Kalay P2P SDK におけるアクセス制限不備の脆弱性(JVN)(08/18)

<https://jvn.jp/vu/JVNVU92334702/>

※CVSSv3 では基本値「9.6」となっています。

- ・ Advantech 製 WebAccess/NMS における認証不備の脆弱性(JVN)(08/18)
<https://jvn.jp/vu/JVNVU97362937/>
- ・ xArrow Software 製 xArrow における複数の脆弱性(JVN)(08/18)
<https://jvn.jp/vu/JVNVU96999992/>
- ・ ISC BIND 9 の脆弱性 (CVE-2021-25218) に関する注意喚起(JPCERT/CC、JVN)(08/19)
<https://www.jpccert.or.jp/at/2021/at210035.html>
<https://jvn.jp/vu/JVNVU95033866/index.html>
- ・ Navigate CMS における複数の脆弱性(JVN)(08/19)
<https://jvn.jp/vu/JVNVU95261759/index.html>
※CVSSv3 では基本値「8.8」となっています。
- ・ AVEVA 製 SuiteLink Server における複数の脆弱性(JVN)(08/20)
<https://jvn.jp/vu/JVNVU92695780/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



●警察庁

- ・ 令和3年度 不正アクセス行為対策等の実態調査及びアクセス制御機能に関する技術の研究開発の状況等に関する調査の実施について【令和3年8月23日】(08/23)
https://www.npa.go.jp/cyber/pdf/R030823_access.pdf



| 3. 関係機関の動き



(1) IPA

- ・ 「サイバーセキュリティ経営可視化ツール」を公開しました。(08/17)
<https://www.ipa.go.jp/security/economics/checktool/index.html>
- ・ Microsoft 社 Internet Explorer のサポート終了について(08/18)

https://www.ipa.go.jp/security/announce/ie_eos.html

・ NIST 文書 SP800-172 「管理対象非機密情報を保護するための拡張セキュリティ要件: NIST SP 800-171 の補足」 の翻訳版を公開しました。(08/20)

<https://www.ipa.go.jp/security/publications/nist/index.html>

・ 「コンピュータウイルス・不正アクセスの届出事例 [2021 年上半期 (1 月～6 月)]」 を公開しました。(08/23)

<https://www.ipa.go.jp/security/outline/todokede-j.html>

・ 「情報セキュリティ 10 大脅威 2021 簡易説明資料[個人編] (一般利用者向け)」 を公開しました。(08/23)

<https://www.ipa.go.jp/security/vuln/10threats2021.html>

(2) J P C E R T コーディネーションセンター

・ Weekly Report 2021-08-12 号(08/12)

<https://www.jpccert.or.jp/wr/2021/wr213101.html>

・ Weekly Report 2021-08-18 号(08/18)

<https://www.jpccert.or.jp/wr/2021/wr213201.html>

□ _____ ■

| 4. 海外の動き

+

● 米国 DHS

・ Drupal がセキュリティアップデートをリリース(08/13)

<https://us-cert.cisa.gov/ncas/current-activity/2021/08/12/drupal-releases-security-updates>

・ 2021 年 8 月 9 日の週の脆弱性概報(08/16)

<https://us-cert.cisa.gov/ncas/bulletins/sb21-228>

・ 2021 年 8 月 16 日の週の脆弱性概報(08/23)

<https://us-cert.cisa.gov/ncas/bulletins/sb21-235>

- ・ BlackBerry の QNXRTOS に影響を与える BadAlloc の脆弱性(08/17)
<https://us-cert.cisa.gov/ncas/alerts/aa21-229a>
<https://us-cert.cisa.gov/ncas/current-activity/2021/08/17/badalloc-vulnerability-affecting-devices-incorporating-older>
- ・ 複数の RTOS に整数オーバーフローまたはラップアラウンドの脆弱性(更新)(08/17)
<https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04>
※CVSSv3 では基本値「9.8」となっています。
- ・ CISA がランサムウェアに起因するデータ侵害から情報を保護するための推奨事項を提供(08/18)
<https://us-cert.cisa.gov/ncas/current-activity/2021/08/18/cisa-provides-recommendations-protecting-information-ransomware>
- ・ Mozilla が Firefox 及び Thunderbird のセキュリティアップデートをリリース(08/18)
<https://us-cert.cisa.gov/ncas/current-activity/2021/08/18/mozilla-releases-security-updates>
- ・ Cisco が複数製品のセキュリティアップデートをリリース(08/19)
<https://us-cert.cisa.gov/ncas/current-activity/2021/08/19/cisco-releases-security-updates-multiple-products>
- ・ 緊急：ProxyShell の脆弱性の積極的な悪用から保護する(08/21)
<https://us-cert.cisa.gov/ncas/current-activity/2021/08/21/urgent-protect-against-active-exploitation-proxyshell>
- ・ ハリケーン関連の詐欺(08/21)
<https://us-cert.cisa.gov/ncas/current-activity/2021/08/21/hurricane-related-scams>



| 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9月14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、特に制限はしていませんが、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。