■―――――――――――――――――――――――――――――――――□

┃　　◆◆　NISC 重要インフラニュースレター　◆◆

┃　　（２０１９年６月１１日発行 第２３９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２３９号の目次　◆―――――――――――――――――――――┐

├―――――――――――――――――――――――――――――――――――┤

○今号は、５月２８日～６月１０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）Apple 社製品に関する脆弱性

・複数の Apple 製品における脆弱性に対するアップデート(JVN)(05/29)

https://jvn.jp/vu/JVNVU98453159/index.html

（２）Microsoft 社製品に関する脆弱性

・Microsoft Windows リモートデスクトップのネットワークレベル認証に Windows ロックスクリーンをバイパスされる問題(JVN)(06/05)

https://jvn.jp/vu/JVNVU94741708/index.html

（３）WordPress に関連する脆弱性

・WordPress 用プラグイン Zoho SalesIQ における複数の脆弱性(JVN)(05/31)

https://jvn.jp/jp/JVN88962935/index.html

・WordPress 用プラグイン Attendance Manager における複数の脆弱性(JVN)(06/10)

https://jvn.jp/jp/JVN95685939/index.html

・WordPress 用プラグイン Online Lesson Booking における複数の脆弱性(JVN)(06/10)

https://jvn.jp/jp/JVN96988995/index.html

（４）その他

・Quest 製 Kace システム管理アプライアンス（K1000）における複数の脆弱性(JVN)(06/03)
https://jvn.jp/vu/JVNVU91210160/index.html

・Joruri Mail における複数の脆弱性(JVN)(06/07)
https://jvn.jp/jp/JVN58052567/index.html

・Joruri CMS 2017 におけるクロスサイトスクリプティングの脆弱性(JVN)(06/07)
https://jvn.jp/jp/JVN29188908/index.html

・GROWI における複数の脆弱性(JVN)(06/07)
https://jvn.jp/jp/JVN84876282/index.html

２．政府機関の動き

● 総務省

・「IoT セキュリティ総合対策 プログレスレポート 2019」の公表(05/31)
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00026.html

３．関係機関の動き

（１）ＩＰＡ

・「情報セキュリティ早期警戒パートナーシップガイドライン」の 2019 年版を公開(05/30)
https://www.ipa.go.jp/security/ciadr/partnership_guide.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2019-05-29 号(05/29)
https://www.jpcert.or.jp/wr/2019/wr192001.html

・マルウエアが含まれたショートカットファイルをダウンロードさせる攻撃(05/29)
https://blogs.jpcert.or.jp/ja/2019/05/darkhotel_lnk.html

・情報セキュリティ早期警戒パートナーシップガイドライン 2019 年版(05/30)
https://www.jpcert.or.jp/vh/index.html#link_japan

・Weekly Report 2019-06-05 号(06/05)
https://www.jpcert.or.jp/wr/2019/wr192101.html

４．海外の動き

● 米国 DHS

・米国全州情報共有・分析センター（MS-ISAC)が Verizon 社のデータ漏洩報告を紹介。(05/29)

https://www.us-cert.gov/ncas/current-activity/2019/05/29/MS-ISAC-Highlights-Verizon-Data-Breach-Report-Release

・Google が Chrome についてのセキュリティアップデートをリリース。(06/04)
https://www.us-cert.gov/ncas/current-activity/2019/06/04/Google-Releases-Security-Update-Chrome

・米国国家安全保障局(NSA)が、以前のバージョンの Windows における RDP プロトコルに関する脆弱性「BlueKeep」（CVE-2019-0708）について、パッチを適用するよう注意喚起を実施。(06/05)
https://www.us-cert.gov/ncas/current-activity/2019/06/04/NSA-Releases-Advisory-BlueKeep-Vulnerability

・Cisco 社が複数の製品についてのセキュリティアップデートをリリース。(06/05)
https://www.us-cert.gov/ncas/current-activity/2019/06/05/Cisco-Releases-Security-Updates-Multiple-Products

・Vmware 社が Tools 10 及び Workstation 15 についてのセキュリティアップデートをリリース。(06/06)
https://www.us-cert.gov/ncas/current-activity/2019/06/06/VMware-Releases-Security-Updates-Tools-and-Workstation

・米国国内歳入庁（ＩＲＳ）が新たな２種類の税金詐欺について注意喚起を実施。(06/07)
https://www.us-cert.gov/ncas/current-activity/2019/06/07/IRS-Warns-New-Tax-Scams

・米国インターネット犯罪苦情センター（ＩＣ３）が HTTPS フィッシングに関する注意喚起を実施。(06/10)
https://www.us-cert.gov/ncas/current-activity/2019/06/07/IRS-Warns-New-Tax-Scams

・５月２７日の週の脆弱性概報(06/03)
https://www.us-cert.gov/ncas/bulletins/SB19-154

・６月３日の週の脆弱性概報(06/10)
https://www.us-cert.gov/ncas/bulletins/SB19-161

・Emerson 社の制御システムコントローラーにスタックベースのバッファオーバーフロー等の脆弱性。(05/28)
https://ics-cert.us-cert.gov/advisories/ICSA-19-148-01

・AVEVA 社の SCADA ソフトに十分でない資格情報保護の脆弱性。(05/30)
https://ics-cert.us-cert.gov/advisories/ICSA-19-150-01

・Geutebrück 社の監視カメラシステムにクロスサイトスクリプティング等の脆弱性。(06/04)
https://ics-cert.us-cert.gov/advisories/ICSA-19-155-03
※CVSSv3 では基本値「7.2」となっています。

・Phoenix Contact 社のＮＡＴスイッチに不適切なアクセス制御の脆弱性。(06/04)
https://ics-cert.us-cert.gov/advisories/ICSA-19-155-02
※CVSSv3 では基本値「8.8」となっています。

・Phoenix Contact 社の I/O 機器用コントローラーに不適切なアクセス制御等の脆弱性。(06/04)
https://ics-cert.us-cert.gov/advisories/ICSA-19-155-01

※CVSSv3 では基本値「7.6」となっています。

・パナソニック株式会社のＰＬＣ用ソフトウェアにヒープベースのバッファオーバーフロー等の脆弱性。(06/06)
https://ics-cert.us-cert.gov/advisories/ICSA-19-157-02
※CVSSv3 では基本値「7.3」となっています。

・Optergy 社のビル管理システムに情報漏洩等の脆弱性。(06/06)
https://ics-cert.us-cert.gov/advisories/ICSA-19-157-01
※CVSSv3 では基本値「10.0」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、６月２５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。

- ni(　^s^)c