■―――――――――――――――――――――――――――――――――□

┃　　◆◆　NISC 重要インフラニュースレター　◆◆

┃　　（２０２０年２月１２日発行 第２５５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２５５号の目次　◆―――――――――――――――――――――――――┐

├―――┤

○今号は、１月２８日～２月１１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）Intel 社製品に関する脆弱性

・Intel 製 CPU の投機的実行機能に対するサイドチャネル攻撃（Vector Register Sampling、L1D Eviction Sampling)(JVN)(01/28)

https://jvn.jp/vu/JVNVU97139173/index.html

（２）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)(01/29)

https://jvn.jp/vu/JVNVU95678717/index.html

（３）Cisco 社製品に関する脆弱性

・Cisco Discovery Protocol (CDP) を使用する製品に複数の脆弱性(JVN)(02/06)

https://jvn.jp/vu/JVNVU95679983/index.html

※CVSSv3 では基本値「8.8」となっています。

（４）その他

・Android アプリ「MyPallete」におけるサーバ証明書検証不備の脆弱性(JVN)(01/28)

https://jvn.jp/jp/JVN28845872/index.html

・スマートフォンアプリ「AWMS Mobile」におけるサーバ証明書の検証不備の脆弱性(JVN)(01/31)
https://jvn.jp/jp/JVN00014057/index.html

・OpenSMTPD に権限昇格と任意コード実行の脆弱性(JVN)(02/03)
https://jvn.jp/vu/JVNVU90495537/index.html
※CVSSv3 では基本値「9.8」となっています。

・Ghostscript におけるアクセス制限回避の脆弱性(JVN)(02/05)
https://jvn.jp/jp/JVN52486659/index.html
※CVSSv3 では基本値「7.8」となっています。

・Movable Type におけるクロスサイトスクリプティングの脆弱性(JVN)(02/05)
https://jvn.jp/jp/JVN94435544/index.html

・HtmlUnit において任意のコードが実行可能な脆弱性(JVN)(02/10)
https://jvn.jp/jp/JVN34535327/index.html

２．政府機関の動き

（１）ＮＩＳＣ

・サイバーセキュリティ戦略本部第 23 回会合を開催（01/30）
https://www.nisc.go.jp/conference/cs/index.html#cs23

・「サイバーセキュリティ戦略」に基づき、2020 年度に実施すべき施策に関する意見の募集について（01/30）
https://www.nisc.go.jp/active/kihon/cyber-security2020.html

・重要インフラ専門調査会第 21 回会合を開催　（1/29 開催）(02/06)
https://www.nisc.go.jp/conference/cs/ciip/index.html#ciip21

（２）警察庁

・複数の IoT 機器等の脆弱性を標的としたアクセスの増加等について(01/31)
https://www.npa.go.jp/cyberpolice/important/2020/202001301.html

・令和元年 12 月期観測資料(01/31)
https://www.npa.go.jp/cyberpolice/important/2020/202001302.html

（３）総務省・経済産業省

・「クラウドサービスの安全性評価に関する検討会　とりまとめ」の公表(01/30)
https://www.soumu.go.jp/menu_news/s-news/2001m.html

・クラウドサービスの安全性評価に関する検討会の検討結果を取りまとめました(01/30)
https://www.meti.go.jp/press/2019/01/20200130002/20200130002.html

３．関係機関の動き

（1）ＩＰＡ

・「情報セキュリティ 10 大脅威 2020」を決定(01/29)
https://www.ipa.go.jp/security/vuln/10threats2020.html

・更新：「Emotet」と呼ばれるウイルスへの感染を狙うメールについて(01/30)
https://www.ipa.go.jp/security/announce/20191202.html

・ニューヨークだより 2020 年 1 月号「ダークウェブに関する現状」(01/31)
https://www.ipa.go.jp/files/000080167.pdf

・「サイバー情報共有イニシアティブ（J-CSIP） 運用状況［2019 年 10 月～12 月］」を公開しました。(01/31)
https://www.ipa.go.jp/security/J-CSIP/index.html

・「コンピュータウイルス・不正アクセスの届出状況［2019 年（1 月～12 月）］」を公開しました。(02/07)
https://www.ipa.go.jp/files/000080224.pdf

・「コンピュータウイルス・不正アクセスの届出事例［2019 年下半期（7 月～12 月）］」を公開しました。(02/07)
https://www.ipa.go.jp/files/000080223.pdf

（2）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2020-01-29 号(01/29)
https://www.jpcert.or.jp/wr/2020/wr200401.html

・JPCERT/CC インターネット定点観測レポート［2019 年 10 月 1 日～2019 年 12 月 31 日](01/29)
https://www.jpcert.or.jp/tsubame/report/report201910-12.html

・Weekly Report 2020-02-05 号(02/05)
https://www.jpcert.or.jp/wr/2020/wr200501.html

４．海外の動き

● 米国 DHS

・Cisco 社が Cisco Small Business Switches についてのセキュリティアップデートをリリース。(01/30)
https://www.us-cert.gov/ncas/current-activity/2020/01/30/cisco-releases-security-updates-cisco-small-business-switches

・Adobe 社が Magento Commerce 及び Open Source editions についてのセキュリティアップデートをリリース。(01/31)
https://www.us-cert.gov/ncas/current-activity/2020/01/31/adobe-releases-security-updates-magento

・米国国内歳入庁（ＩＲＳ）が「個人情報窃取センター」サイトを公開。(02/04)
https://www.us-cert.gov/ncas/current-activity/2020/02/04/irs-launches-identity-theft-central-webpage

・Google が Chrome 80 をリリース。(02/05)
https://www.us-cert.gov/ncas/current-activity/2020/02/05/google-releases-security-updates-chrome

・豪州サイバーセキュリティセンター（ＡＣＳＣ）が、ランサムウェア「Mailto」事案に関するアドバイザリーをリリース。(02/06)
https://www.us-cert.gov/ncas/current-activity/2020/02/06/acsc-releases-advisory-mailto-ransomware-incidents

・Mozilla が Firefox、Firefox ESR 及び Thunderbird についてのセキュリティアップデートをリリース。(02/11)
https://www.us-cert.gov/ncas/current-activity/2020/02/11/mozilla-releases-security-updates-multiple-products

・Adobe 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。(02/11)
https://www.us-cert.gov/ncas/current-activity/2020/02/11/adobe-releases-security-updates-multiple-products

・Intel 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。(02/11)
https://www.us-cert.gov/ncas/current-activity/2020/02/11/intel-releases-security-updates

・Microsoft 社が２０２０年２月期のセキュリティアップデートをリリース。(02/11)
https://www.us-cert.gov/ncas/current-activity/2020/02/11/microsoft-releases-february-2020-security-updates

・２０２０年１月２７日の週の脆弱性概報。(02/04)
https://www.us-cert.gov/ncas/bulletins/sb20-034

・２０２０年２月３日の週の脆弱性概報。(02/10)
https://www.us-cert.gov/ncas/bulletins/sb20-041

・Medtronic 社の埋め込み型心臓デバイス用のプログラマーにエンドポイントに対する適切でない通信チャネルの制限等の脆弱性。(01/30)
https://www.us-cert.gov/ics/advisories/ICSMA-18-058-01
※CVSSv3 では基本値「7.1」となっています。

・Medtronic 社の医療用モニターに不適切なアクセスコントロール等の脆弱性。(01/30)
https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01
※CVSSv3 では基本値「9.3」となっています。

・AutomationDirect 社のＨＭＩタッチパネルに十分でない資格情報保護の脆弱性。(02/04)
https://www.us-cert.gov/ics/advisories/icsa-20-035-01
※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、２月２６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