◆◆ NISC 重要インフラニュースレター ◆◆
（２０２０年１月２９日発行 第２５４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２５４号の目次 ◆

○今号は、１月１５日～１月２７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 社製品に関する脆弱性

・Microsoft 製品の脆弱性対策について(2020 年 1 月)(IPA)(01/15)
https://www.ipa.go.jp/security/ciadr/vul/20200115-ms.html

・2020 年 1 月マイクロソフトセキュリティ更新プログラムに関する注意喚起(JPCERT/CC) (01/15)
https://www.jpcert.or.jp/at/2020/at200001.html

・Microsoft Windows CryptoAPI における Elliptic Curve Cryptography (ECC) 証明書の検証不備の脆弱性(JVN)(01/15)
https://jvn.jp/vu/JVNVU91499458/index.html

・Microsoft Windows リモートデスクトップゲートウェイにおける任意のコード実行が可能な脆弱性(JVN)(01/15)
https://jvn.jp/vu/JVNVU98033252/index.html
※CVSSv3 では基本値「9.8」となっています。

・Microsoft Internet Explorer の未修正の脆弱性（CVE-2020-0674）に関する注意喚起（公開）(JPCERT/CC)(01/19)

https://www.jpcert.or.jp/at/2020/at200004.html

・Microsoft Internet Explorer の脆弱性対策について(CVE-2020-0674)(IPA)(01/20)
https://www.ipa.go.jp/security/announce/alert.html

・Microsoft Internet Explorer の JScript スクリプトエンジンにおけるメモリ破損の脆弱性(JVN)(01/20)
https://jvn.jp/vu/JVNVU90794960/index.html

（２）Oracle 社製品に関する脆弱性
・Oracle Java の脆弱性対策について(CVE-2020-2604 等)(IPA)(01/15)
https://www.ipa.go.jp/security/ciadr/vul/20200115-jre.html

・2020 年 1 月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起(JPCERT/CC) (01/15)
https://www.jpcert.or.jp/at/2020/at200002.html

・CyberNewsFlash「複数の Adobe 製品のアップデートについて」(JPCERT/CC) (01/15)
https://www.jpcert.or.jp/newsflash/2020011501.html

（３）Citrix 社製品に関する脆弱性
・Citrix ADC および Citrix Gateway における任意のコード実行の脆弱性（CVE-2019-19781）について(IPA)(01/17)
https://www.ipa.go.jp/security/ciadr/vul/alert20200117.html

・複数の Citrix 製品の脆弱性(CVE-2019-19781)に関する注意喚起(公開)(JPCERT/CC)(01/17)
https://www.jpcert.or.jp/at/2020/at200003.html

（４）Intel 社製品に関する脆弱性
・CyberNewsFlash「Intel 製品に関する複数の脆弱性について」(JPCERT/CC)(01/15)
https://www.jpcert.or.jp/newsflash/2020011502.html

・Intel 製品に複数の脆弱性(JVN)(01/15)
https://jvn.jp/vu/JVNVU98694410/index.html

（５）トレンドマイクロ社製品に関する脆弱性
・トレンドマイクロ製パスワードマネージャーにおける情報漏えいの脆弱性(JVN)(01/17)
https://jvn.jp/jp/JVN49593434/index.html
https://jvn.jp/jp/JVN37183636/index.html

（６）その他
・複数の CDN サービスプロバイダが HTTP キャッシュポイズニングの影響を受ける問題(JVN)(01/15)
https://jvn.jp/vu/JVNVU98141012/index.html
※CVSSv3 では基本値「7.2」となっています。

・富士ゼロックス製の複数のスマートフォンアプリにおける SSL サーバ証明書の検証不備の脆弱性(JVN)(01/21)
https://jvn.jp/jp/JVN66435380/index.html

・Firefox の脆弱性（CVE-2019-17026）に関する注意喚起(JPCERT/CC)(01/27)
https://www.jpcert.or.jp/at/2020/at200005.html

□―――■

┃２．政府機関の動き

┼―――┼

（１）ＮＩＳＣ

・『ソードアート・オンライン アリシゼーション War of Underworld』と内閣サイバーセキュリティセンターがタイアップ！(01/23)
https://www.nisc.go.jp/security-site/files/tieup_2020.pdf

（２）総務省

・公衆無線 LAN のセキュリティ対策に係るオンライン講座の開講(01/27)
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00053.html

・脆弱な IoT 機器及びマルウェアに感染している IoT 機器の利用者への注意喚起の実施状況（2019 年度第 3 四半期）(01/28)
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00058.html

・「我が国のサイバーセキュリティ強化に向け速やかに 取り組むべき事項[緊急提言]」の公表(01/28)
https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00093.html

■―――□

┃３．関係機関の動き

┼―――┼

（１）ＩＰＡ

・Windows7 のサポート終了について(01/15)
https://www.ipa.go.jp/security/announce/win7_eos.html

・【国家資格「情報処理安全確保支援士」がわかる！説明会（2020 年 1 月開催）】講演映像を公開しました。(01/21)
https://www.ipa.go.jp/siensi/toberiss/wakaru.html

・脆弱性対策情報データベース JVN iPedia の登録状況［2019 年第 4 四半期（10 月～12 月）］(01/22)
https://www.ipa.go.jp/security/vuln/report/JVNiPedia2019q4.html

・ソフトウェア等の脆弱性関連情報に関する届出状況[2019 年第 4 四半期（10 月～12 月）］(01/23)
https://www.ipa.go.jp/security/vuln/report/vuln2019q4.html

・「情報セキュリティ安心相談窓口の相談状況［2019 年第 4 四半期（10 月～12 月）］」を公開しました。(01/23)
https://www.ipa.go.jp/security/txt/2019/q4outline.html

（２）ＪＰＣＥＲＴ コーディネーションセンター

・Weekly Report 2020-01-16 号(01/16)
https://www.jpcert.or.jp/wr/2020/wr200201.html

・JPCERT/CC 活動概要［2019 年 10 月 1 日～2019 年 12 月 31 日](01/21)
https://www.jpcert.or.jp/pr/index.html

・JPCERT/CC インシデント報告対応レポート［2019 年 10 月 1 日～2019 年 12 月 31 日](01/21)
https://www.jpcert.or.jp/ir/report.html

・Weekly Report 2020-01-22 号(01/22)
https://www.jpcert.or.jp/wr/2020/wr200301.html

・ソフトウェア等の脆弱性関連情報に関する届出状況［2019 年 10 月 1 日～2019 年 12 月 31 日] (01/23)
https://www.jpcert.or.jp/report/press.html

４．海外の動き

● 米国 DHS

・Google が Chrome version 79.0.3945.130 をリリース。(01/17)
https://www.us-cert.gov/ncas/current-activity/2020/01/17/google-releases-security-updates-chrome

・Samba チームが複数のバージョンの Samba についてのセキュリティアップデートをリリース。(01/21)
https://www.us-cert.gov/ncas/current-activity/2020/01/21/samba-releases-security-updates

・ウェブサイトをサイバー攻撃から守るために(01/21)
https://www.us-cert.gov/ncas/current-activity/2020/01/21/reminder-safeguard-websites-cyberattacks

・米国インターネット犯罪苦情センター（ＩＣ３）が個人情報窃取を目的とした偽求人詐欺に関する注意喚起を実施。(01/22)
https://www.us-cert.gov/ncas/current-activity/2020/01/22/ic3-issues-alert-employment-scams

・増大するマルウェア「Emotet」の活動(01/22)
https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity

・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。(01/23)
https://www.us-cert.gov/ncas/current-activity/2020/01/23/cisco-releases-security-updates

・Citrix 社が Citrix SD-WAN WANOP に影響を及ぼす脆弱性 CVE-2019-19781 に対応したセキュリティアップデートをリリース。(01/23)
https://www.us-cert.gov/ncas/current-activity/2020/01/23/citrix-releases-security-updates-sd-wan-wanop

・米国国家安全保障局(NSA)がクラウドにおける脆弱性の低減に関するガイダンスをリリース。(01/24)
https://www.us-cert.gov/ncas/current-activity/2020/01/24/nsa-releases-guidance-mitigating-cloud-vulnerabilities

・Cisco 社が Cisco Webex Meetings Suite 及び Cisco Webex Meetings Online に影響を及ぼす脆弱性に対応したセキュリティアップデートをリリース。(01/24)
https://www.us-cert.gov/ncas/current-activity/2020/01/24/cisco-releases-security-updates

・複数のキャッシュサービスプロバイダーは HTTP キャッシュポイズニングに対して脆弱。(01/14)
https://kb.cert.org/vuls/id/335217/

・２０２０年１月１３日の週の脆弱性概報。(01/20)
https://www.us-cert.gov/ncas/bulletins/sb20-020

・２０２０年１月２０日の週の脆弱性概報。(01/27)
https://www.us-cert.gov/ncas/bulletins/sb20-027

・OSIsoft 社の可視化ツールに不適切なアクセスコントロール等の脆弱性。(01/14)
https://www.us-cert.gov/ics/advisories/icsa-20-014-06
※CVSSv3 では基本値「7.1」となっています。

・Siemens 社のエンジニアリングフレームワークにパストラバーサルの脆弱性。(01/14)
https://www.us-cert.gov/ics/advisories/icsa-20-014-05
※CVSSv3 では基本値「7.8」となっています。

・Siemens 社のインバーターに保護メカニズムの不具合の脆弱性。(01/14)
https://www.us-cert.gov/ics/advisories/icsa-20-014-04

・Siemens 社の産業用イーサネットスイッチに重要な機能に対する認証の欠如の脆弱性。(01/14)
https://www.us-cert.gov/ics/advisories/icsa-20-014-03
※CVSSv3 では基本値「8.8」となっています。

・Siemens 社のネットワーク管理ソフトウェアに不適切な特権割当ての脆弱性。(01/14)
https://www.us-cert.gov/ics/advisories/icsa-20-014-02
※CVSSv3 では基本値「9.9」となっています。

・GE/Emerson 社のＰＬＣに不適切な入力検証の脆弱性。(01/14)
https://www.us-cert.gov/ics/advisories/icsa-20-014-01
※CVSSv3 では基本値「7.5」となっています。

・Schneider Electric 社のプロセスコントローラーに不適切な異常や例外条件の確認の脆弱性。(01/16)
https://www.us-cert.gov/ics/advisories/icsa-20-016-01
※CVSSv3 では基本値「7.5」となっています。

・Honeywell 社の監視カメラシステムに信頼できないデータのデシリアライゼーション等の脆弱性。(01/21)
https://www.us-cert.gov/ics/advisories/icsa-20-021-01
※CVSSv3 では基本値「9.8」となっています。

・GE 社の医療用機器に不適切な認証等の脆弱性。(01/23)
https://www.us-cert.gov/ics/advisories/icsma-20-023-01
※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１２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