8/24 更新　Microsoft 社より 2021 年 7 月のセキュリティ更新プログラムが公開

中国地域サイバーセキュリティ連絡会会員様
中国地域のサイバーセキュリティ担当者様

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。

米国サイバーセキュリティ庁より Microsoft Exchange Server の問題を悪用されていると注意喚起があり、
Microsoft 社からの 2021 年 7 月のセキュリティ更新プログラムの公開情報が更新されましたので、
以下のとおり情報展開させていただきます。
－－
米国サイバーセキュリティ庁より Microsoft Exchange Server の問題を悪用されていると注意喚起あり。
業務に影響を及ぼさない時間や復旧可能な準備等を整えつつ、早めの対応を推奨。
－－

Ⅰ. 概要
　Microsoft 社より 2021 年 3 月度の定例セキュリティアップデートが公開されました。
　対象製品は OS 等の業務利用製品の他、複数のサーバソフトウェア等が対象に含まれます。
　一部の問題は海外で悪用された事例が確認されているため、早めのアップデートを推奨します。

8/24 更新：
　米国サイバーセキュリティ庁（CISA）より、Microsoft Exchange Server の問題を悪用する
攻撃が確認されているとの注意喚起が公表されました。

■対象製品一覧
[OS]

Windows 7 SP1
Windows 8.1、RT 8.1
Windows 10
Windows 10 Version 1607、1809、1909、2004、20H2、21H1
Windows Server 2008 SP2、2008 R2 SP1、2012、2012 R2、2016、2019
Windows Server, version 1909、2004、20H2

[サーバソフトウェア]
Microsoft Exchange Server 2013、2016、2019
Microsoft SharePoint Enterprise Server 2013 SP1、2016
Microsoft SharePoint Server 2019

[アプリケーション]
.NET Education Bundle SDK Install Tool
.NET Install Tool for Extension Authors
HEVC Video Extensions
Microsoft 365 Apps
Microsoft Bing Search for Android
Microsoft Dynamics 365 Business Central 2020、2021
Microsoft Excel 2013 SP1、2013 RT SP1
Microsoft Excel 2016
Microsoft Malware Protection Engine
Microsoft Office 2013 SP1、2013 RT SP1、2016、2019、Online Server、Web Apps Server 2013 SP1
Microsoft SharePoint Foundation 2013 SP1
Microsoft Word 2016
Open Enclave SDK
Power BI Report Server
Visual Studio Code

Ⅱ. 対策・回避策
影響を受ける製品を利用している場合や、利用しているか不明な場合は、下記の関連トピックの内容を
システムを運用されている担当者や委託先事業者の窓口の方に共有していただき、対策等のご検討をお願いいたします。

大会前ということを踏まえ、セキュリティ更新プログラムの適用の際には、業務に影響を及ぼさない時間や
復旧可能な準備等を整えたうえで実施することを推奨します。

－－

【関連トピック】
米国 CISA より Exchange Server の 3 つの脆弱性（CVE-2021-34473、34523、31207）の悪用について注意喚起。
修正プログラムが適用されていない場合は、業務に影響を及ぼさない時間や復旧可能な準備等を整えつつ対応を推奨。

Ⅰ. 概要
Microsoft 社より 2021 年 7 月のセキュリティ更新プログラムが公開されました。
ベンダー評価 Critical の脆弱性が 12 件、Important の脆弱性が 103 件となります。
このうち、次の脆弱性は既に攻撃として悪用されていることが確認されています。

・CVE-2021-33771(7.8)　Windows カーネルの特権の昇格の脆弱性
・CVE-2021-34448(6.8)　スクリプト エンジンのメモリ破損の脆弱性
・CVE-2021-31979(7.8)　Windows カーネルの特権の昇格の脆弱性

8/24 更新：
米国 CISA より、次の 3 つの Microsoft Exchange の脆弱性が攻撃に悪用されているとの注意喚起が公表されました。

・CVE-2021-34473(9.1)　Microsoft Exchange Server のリモートでコードが実行される脆弱性
・CVE-2021-34523(9.0)　Microsoft Exchange Server の特権の昇格の脆弱性
・CVE-2021-31207(6.6) Microsoft Exchange Server のセキュリティ機能のバイパスの脆弱性(*1)
*1:CVE-2021-31207 は 2021 年 5 月に修正プログラムがリリースされた脆弱性となります。(参考情報④)

■対象製品一覧

[OS]

Windows 7 SP1
Windows 8.1、RT 8.1
Windows 10
Windows 10 Version 1607、1809、1909、2004、20H2、21H1
Windows Server 2008 SP2、2008 R2 SP1、2012、2012 R2、2016、2019
Windows Server, version 1909、2004、20H2

[サーバソフトウェア]

Microsoft Exchange Server 2013、2016、2019
Microsoft SharePoint Enterprise Server 2013 SP1、2016
Microsoft SharePoint Server 2019

[アプリケーション]

.NET Education Bundle SDK Install Tool
.NET Install Tool for Extension Authors
HEVC Video Extensions
Microsoft 365 Apps
Microsoft Bing Search for Android
Microsoft Dynamics 365 Business Central 2020、2021
Microsoft Excel 2013 SP1、2013 RT SP1
Microsoft Excel 2016
Microsoft Malware Protection Engine
Microsoft Office 2013 SP1、2013 RT SP1、2016、2019、Online Server、Web Apps Server 2013 SP1
Microsoft SharePoint Foundation 2013 SP1
Microsoft Word 2016
Open Enclave SDK
Power BI Report Server
Visual Studio Code

■CVE 番号（CVSS v3.0 基本値）及び概要

※リリースノート（参考情報①）に掲載された CVE 番号のうち、重要度の高い CVSS 7.0 以上を記載しています。

詳細については、Microsoft 社のリリースノート（参考情報①②）を参照ください。

・CVE-2021-34458(9.9)　Windows カーネルのリモートでコードが実行される脆弱性
・CVE-2021-34473(9.1)　Microsoft Exchange Server のリモートでコードが実行される脆弱性
・CVE-2021-34523(9.0)　Microsoft Exchange Server の特権の昇格の脆弱性
・CVE-2021-33749(8.8)　Windows DNS スナップインのリモートでコードが実行される脆弱性
・CVE-2021-33750(8.8)　Windows DNS スナップインのリモートでコードが実行される脆弱性
・CVE-2021-33752(8.8)　Windows DNS スナップインのリモートでコードが実行される脆弱性
・CVE-2021-33756(8.8)　Windows DNS スナップインのリモートでコードが実行される脆弱性
・CVE-2021-33780(8.8)　Windows DNS サーバーのリモートでコードが実行される脆弱性
・CVE-2021-34494(8.8)　Windows DNS サーバーのリモートでコードが実行される脆弱性
・CVE-2021-34508(8.8)　Windows カーネルのリモートでコードが実行される脆弱性
・CVE-2021-34525(8.8)　Windows DNS サーバーのリモートでコードが実行される脆弱性
・CVE-2021-34450(8.5)　Windows Hyper-V のリモートでコードが実行される脆弱性
・CVE-2021-33767(8.2)　Open Enclave SDK の特権の昇格の脆弱性
・CVE-2021-34469(8.2)　Microsoft Office のセキュリティ機能のバイパスの脆弱性
・CVE-2021-33779(8.1)　Windows ADFS のセキュリティ機能のバイパスの脆弱性
・CVE-2021-33781(8.1)　Active Directory のセキュリティ機能のバイパスの脆弱性
・CVE-2021-33786(8.1)　Windows LSA のセキュリティ機能のバイパスの脆弱性
・CVE-2021-34492(8.1)　Windows 証明書のなりすましの脆弱性

・CVE-2021-34520(8.1)　Microsoft SharePoint Server のリモートでコードが実行される脆弱性
・CVE-2021-33746(8.0)　Windows DNS サーバーのリモートでコードが実行される脆弱性
・CVE-2021-33754(8.0)　Windows DNS サーバーのリモートでコードが実行される脆弱性
・CVE-2021-33768(8.0)　Microsoft Exchange Server の特権の昇格の脆弱性
・CVE-2021-34446(8.0)　Windows HTML プラットフォームのセキュリティ機能のバイパスの脆弱性
・CVE-2021-34470(8.0)　Microsoft Exchange Server の特権の昇格の脆弱性
・CVE-2021-34474(8.0)　Dynamics Business Central のリモートでコードが実行される脆弱性
・CVE-2021-31947(7.8)　HEVC ビデオ拡張機能のリモートでコードが実行される脆弱性
・CVE-2021-31979(7.8)　Windows カーネルの特権の昇格の脆弱性
・CVE-2021-33740(7.8)　Windows Media のリモートでコードが実行される脆弱性
・CVE-2021-33743(7.8)　Windows Projected File System の特権の昇格の脆弱性
・CVE-2021-33759(7.8)　Windows デスクトップ ブリッジの特権の昇格の脆弱性
・CVE-2021-33761(7.8)　Windows Remote Access Connection Manager の特権の昇格の脆弱性
・CVE-2021-33771(7.8)　Windows カーネルの特権の昇格の脆弱性
・CVE-2021-33773(7.8)　Windows Remote Access Connection Manager の特権の昇格の脆弱性
・CVE-2021-33775(7.8)　HEVC ビデオ拡張機能のリモートでコードが実行される脆弱性
・CVE-2021-33776(7.8)　HEVC ビデオ拡張機能のリモートでコードが実行される脆弱性
・CVE-2021-33777(7.8)　HEVC ビデオ拡張機能のリモートでコードが実行される脆弱性
・CVE-2021-33778(7.8)　HEVC ビデオ拡張機能のリモートでコードが実行される脆弱性
・CVE-2021-33784(7.8)　Windows Cloud Files Mini Filter ドライバーの特権

の昇格の脆弱性
・CVE-2021-34438(7.8)　Windows Font Driver Host のリモートでコードが実行される脆弱性
・CVE-2021-34439(7.8)　Microsoft Windows メディア ファンデーションのリモートでコードが実行される脆弱性
・CVE-2021-34441(7.8)　Microsoft Windows メディア ファンデーションのリモートでコードが実行される脆弱性
・CVE-2021-34445(7.8)　Windows Remote Access Connection Manager の特権の昇格の脆弱性
・CVE-2021-34452(7.8)　Microsoft Word のリモートでコードが実行される脆弱性
・CVE-2021-34455(7.8)　Windows File History Service の特権の昇格の脆弱性
・CVE-2021-34456(7.8)　Windows Remote Access Connection Manager の特権の昇格の脆弱性
・CVE-2021-34459(7.8)　Windows AppContainer の特権の昇格の脆弱性
・CVE-2021-34460(7.8)　Storage Spaces Controller の特権の昇格の脆弱性
・CVE-2021-34461(7.8)　Windows Container Isolation FS Filter ドライバーの特権の昇格の脆弱性
・CVE-2021-34464(7.8)　Microsoft Defender のリモートでコードが実行される脆弱性
・CVE-2021-34477(7.8)　Visual Studio Code .NET Runtime の特権の昇格の脆弱性
・CVE-2021-34479(7.8)　Microsoft Visual Studio のなりすましの脆弱性
・CVE-2021-34488(7.8)　Windows Console Driver の特権の昇格の脆弱性
・CVE-2021-34489(7.8)　DirectWrite のリモートでコードが実行される脆弱性
・CVE-2021-34498(7.8)　Windows GDI の特権の昇格の脆弱性
・CVE-2021-34501(7.8)　Microsoft Excel のリモートでコードが実行される脆弱性
・CVE-2021-34503(7.8)　Microsoft Windows メディア ファンデーションのリモートでコードが実行される脆弱性
・CVE-2021-34504(7.8)　Windows アドレス帳のリモートでコードが実行される脆弱性
・CVE-2021-34510(7.8)　Storage Spaces Controller の特権の昇格の脆弱性

・CVE-2021-34511(7.8)　Windows インストーラーの特権の昇格の脆弱性
・CVE-2021-34512(7.8)　Storage Spaces Controller の特権の昇格の脆弱性
・CVE-2021-34513(7.8)　Storage Spaces Controller の特権の昇格の脆弱性
・CVE-2021-34514(7.8)　Windows カーネルの特権の昇格の脆弱性
・CVE-2021-34516(7.8)　Win32k の特権の昇格の脆弱性
・CVE-2021-34518(7.8)　Microsoft Excel のリモートでコードが実行される脆弱性
・CVE-2021-34521(7.8)　Raw Image Extension Remote Code Execution Vulnerability
・CVE-2021-34522(7.8)　Microsoft Defender のリモートでコードが実行される脆弱性
・CVE-2021-34528(7.8)　Visual Studio Code のリモートでコードが実行される脆弱性
・CVE-2021-34529(7.8)　Visual Studio Code のリモートでコードが実行される脆弱性
・CVE-2021-33758(7.7)　Windows Hyper-V のサービス拒否の脆弱性
・CVE-2021-31206(7.6)　Microsoft Exchange Server のリモートでコードが実行される脆弱性
・CVE-2021-31984(7.6)　Power BI のリモート コードが実行される脆弱性
・CVE-2021-31183(7.5)　Windows TCP/IP ドライバーのサービス拒否の脆弱性
・CVE-2021-33772(7.5)　Windows TCP/IP ドライバーのサービス拒否の脆弱性
・CVE-2021-33785(7.5)　Windows AF_UNIX Socket Provider のサービス拒否の脆弱性
・CVE-2021-33788(7.5)　Windows LSA のサービス拒否の脆弱性
・CVE-2021-34442(7.5)　Windows DNS サーバーのサービス拒否の脆弱性
・CVE-2021-34476(7.5)　Bowser.sys のサービス拒否の脆弱性
・CVE-2021-34490(7.5)　Windows TCP/IP ドライバーのサービス拒否の脆弱性
・CVE-2021-33766(7.3)　Microsoft Exchange の情報漏えいの脆弱性
・CVE-2021-31196(7.2)　Microsoft Exchange Server のリモートでコードが実行される脆弱性
・CVE-2021-34467(7.1)　Microsoft SharePoint Server のリモートでコードが実行される脆弱性

・CVE-2021-34468(7.1)　　Microsoft SharePoint Server のリモートでコードが実行される脆弱性
・CVE-2021-33751(7.0)　　Storage Spaces Controller の特権の昇格の脆弱性
・CVE-2021-33774(7.0)　　Windows Event Tracing の特権の昇格の脆弱性
・CVE-2021-34449(7.0)　　Win32k の特権の昇格の脆弱性
・CVE-2021-34462(7.0)　　Windows AppX 展開拡張機能の特権の昇格の脆弱性

Ⅱ. 対策・回避策

以下のベンダ情報（Ⅲ. 参考情報①②）をもとに、更新プログラムの適用を検討ください。

また、すぐに更新プログラムを適用できない場合は回避策の適用も併せてご検討ください。

なお、大会を支えるシステムが該当する場合は、セキュリティ更新プログラムの適用による不具合等に備え
復旧可能な準備を整えたうえで実施することを推奨します。

Ⅲ. 参考情報

①2021 年 7 月のセキュリティ更新プログラム
https://msrc.microsoft.com/update-guide/releaseNote/2021-Jul
②セキュリティ更新プログラムガイド
https://portal.msrc.microsoft.com/ja-jp/security-guidance

8/24 更新：
③CISA：Urgent: Protect Against Active Exploitation of ProxyShell Vulnerabilities
https://us-cert.cisa.gov/ncas/current-activity/2021/08/21/urgent-protect-against-active-exploitation-proxyshell
④Microsoft Exchange Server Security Feature Bypass Vulnerability(CVE-2021-31207)
https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2021-31207