Advanced Malware Protection サービスおよび Threat Grid サービスのファイル基準ガイド（Cisco Content Security 製品用）

発行日：2014 年 3 月 12 日

改訂日：2019 年 3 月 22 日

Advanced Malware Protection 機能は、AsyncOS 8.0.5 for Cisco Web Security Appliances および AsyncOS 8.5.5 for Cisco Email Security Appliances から導入されました。

Cisco Web セキュリティ アプライアンス および Cisco Email Security または Cloud Email Security アプライアンスのファイル レピュテーションおよびファイル分析サービスは、このドキュメントで説明される基準を満たすファイルのレピュテーション情報と挙動分析を提供します。

このドキュメントへのアクセスについて

このドキュメントにアクセスするには、シスコの顧客プロファイルとサポート契約が必要です。

アカウントを登録するには、https://tools.cisco.com/RPF/register/register.do にアクセスしてください。

この情報は予告なしに変更されることがあります

ファイル基準は随時変更される可能性があり、このドキュメントは頻繁に更新される場合があります。

Cisco Systems, Inc.
www.cisco.com

ファイル レピュテーション クエリ

ファイル レピュテーション サービスは、大半のファイルを評価できます。ただし、以下の点に注意してください。

- (E メール セキュリティ アプライアンス のみ)アプライアンスは、ワークキュー内の Advanced Malware Protection サービスに到達する前に、メッセージから除去された添付ファイルについては、ファイル レピュテーション サービスをクエリしません。
- (E メール セキュリティ アプライアンス のみ)ファイル レピュテーションは、暗号化されたメッセージについてはクエリされません。これは、暗号化されたメッセージからは添付ファイルを抽出できないためです。
- (E メール セキュリティ アプライアンス のみ)暗号化されていないメッセージの暗号化された添付ファイルが、評価のために送信されます。ただし、これらの添付ファイルの種類は、スキャンできないものとして扱われます。
- (AsyncOS 8.5 for Web Security および AsyncOS 9.0 for Email Security 以降)圧縮されたアーカイブ ファイル(RAR、7z、Gzip、ZIP、TAR、LZH、TGZ)内のコンテンツが抽出され(最大 5 段階のネスト レベル)、すべての抽出されたファイルのレピュテーションが評価されます。抽出されたファイルのいくつかの判定が「不明(unknown)」である場合、それらの抽出ファイルは、状況に応じて、分析のために送信されます(そのように設定されており、ファイル タイプがファイル分析でサポートされている場合)。
- (Web セキュリティ アプライアンス のみ)[セキュリティサービス(Security Services)] > [マルウェア対策およびレピュテーション(Anti-Malware and Reputation)] ページの [DVSエンジンオブジェクトスキャンの制限(DVS Engine Object Scanning Limits)] の設定も、レピュテーションを評価するために最大ファイル サイズを決定します。

ファイル分析

分析用にファイルをアップロードするための基準は次のとおりです。

- Cisco E メール セキュリティ アプライアンス(AsyncOS 11.0 以前のバージョン)および Cisco Web セキュリティ アプライアンスの場合、現在次のファイル タイプを分析用に送信することができます。
  - (ファイル分析をサポートしているすべてのリリース)Windows 実行可能ファイル(例: .exe、.dll、.sys、および .scr ファイル)。
  - Adobe Portable Document Format(PDF)、Microsoft Office 2007 +(オープン XML)、Microsoft Office 97-2004(OLE)、Microsoft Windows/DOS 実行可能ファイル、その他の悪意がある可能性のあるファイル タイプ。
  - マルウェア対策およびレピュテーション設定ページ(Web セキュリティの場合)またはファイル レピュテーションと分析の設定ページ(E メール セキュリティの場合)でアップロード用に選択したファイル タイプ。初期のサポートには、PDF と Microsoft Office ファイルが含まれます。
  - (E メール セキュリティの場合 AsyncOS 9.7.1 から開始)[その他の悪意の可能性があるファイルタイプ(Other potentially malicious file types)] オプションを選択している場合、次の拡張子が付いた Microsoft Office ファイルが XML または MHTML 形式で保存されています。ade、adp、adn、accdb、accdr、accdt、accda、mdb、cdb、mda、mdn、mdt、mdw、mdf、mde、accde、mam、maq、mar、mat、maf、ldb、laccdb、doc、dot、docx、docm、dotx、dotm、docb、xls、xlt、xlm、xlsx、xlsm、xltx、xltm、xlsb、xla、xlam、xll、xlw、ppt、pot、pps、pptx、pptm、potx、potm、ppam、ppsx、ppsm、sldx、sldm、mht、mhtm、mhtml、および xml。

- Cisco E メール セキュリティ アプライアンス（AsyncOS 11.1 以降のバージョン）および Web セキュリティ アプライアンス（AsyncOS 11.7 以降のバージョン）の場合、現在次のファイル タイプを分析用に送信することができます。

ファイル グループ名	ファイルの説明	ファイル拡張子
アーカイブおよび圧縮	GLOX ファイル	.glox
	GrooveToolArchive	.gta
	Jarfile	.jar
	Microsoft.System.Update.1	.msu
	Pbkfile	.pbk
	VisualStudio.ContentInstaller.vsi	.vsi
設定	AcroExch.SecStore	.secstore
	Aspfile	.cdx
	BrmFile	.printerExport
	CABFolder	.cab
	CLSID\{9E56BE60-C50F-11CF-9A2C-00A0C90A90CE}	mapimail
	CRLFile	.crl
	CRTXFile	.crtx
	CSSFile	.css
	Campfile	.camp
	Cdmpfile	.cdmp
	Contact_wab_auto_file	.contact
	Cplfile	.cpl
	Diagnostic.Config	.diagcfg
	Diagnostic.Perfmon.Config	.perfmoncfg
	Diagnostic.Resmon.Config	.resmoncfg
	Emffile	.emf
	GCSXFile	.gcsx
	GQSXFile	.gqsx
	GrooveLinkFile	.glk
	GrooveStub	.gfs
	Group_wab_auto_file	.group
	H1cfile	.H1C
	H1dfile	.H1D
	H1ffile	.H1F
	H1hfile	.H1H
	H1kfile	.H1K
	H1sfile	.H1S
	H1tfile	.H1T
	H1vfile	.H1V

ファイル グループ名	ファイルの説明	ファイル拡張子
	H1wfile	.H1W
	Hlpfile	.hlp
	Icmfile	.icm
	InfoPath.SolutionManifest.3	.xsf
	Inifile	.ini
	InternetShortcut	.URL
	JNLPFILE	.jnlp
	Jtpfile	.jtp
	LibraryFolder	.library-ms
	LpkSetup.1	.mlc
	MSGraph.Chart.8	.gra
	MSProgramGroup	.grp
	MSSppPackageFile	.slupkg-ms
	MediaCatalogMGC	.mgc
	MediaCatalogMML	.mml
	MediaCenter.C2R	.c2r
	MediaCenter.MCL	.mcl
	MediaPackageFile	.mpf
	Microsoft.PowerShellXMLData.1	.ps1xml
	Microsoft.WindowsCardSpaceBackup	.crds
	Migfile	.mig
	Ocxfile	.ocx
	OfficeListShortcut	.ols
	OneNote.TableOfContents	.onetoc
	OneNote.TableOfContents.12	.onetoc2
	Outlook.File.hol.14	.hol
	Outlook.File.ics.14	.ics
	Outlook.File.nk2.14	.nk2
	PCBFILE	.pcb
	PDXFileType	.pdx
	Prffile	.prf
	RDBFileProperties.1	.sfcache
	RDP.File	.rdp
	Ratfile	.rat
	RemoteAssistance.1	.msrcincident

ファイル グループ名	ファイルの説明	ファイル拡張子
	SHCmdFile	.scf
	SavedDsQuery	.qds
	Scrfile	.scr
	Sysfile	.sys
	VisualStudio.Launcher._sln	._sln
	VisualStudio.Launcher._sln60	._sln60
	VisualStudio.Launcher._sln70	._sln70
	VisualStudio.Launcher._sln71	._sln71
	VisualStudio.Launcher._sln80	._sln80
	VisualStudio.Launcher._vbxsln80	._vbxsln80
	VisualStudio.Launcher._vcppxsln80	._vcppxsln80
	VisualStudio.Launcher._vcsxsln80	._vcsxsln80
	VisualStudio.Launcher._vjsxsln80	._vjsxsln80
	VisualStudio.Launcher._vstasln80	._vstasln80
	VisualStudio.Launcher.sln	.sln
	Vxdfile	.vxd
	Wab_auto_file	.wab
	Wbcatfile	.wbcat
	Wcxfile	.wcx
	Windows.gadget	.gadget
	Wmffile	.wmf
	XEV.GenericApp	.xevgenxml
	XTP2FILE	.xtp2
	XTPFILE	.xtp

ファイル グループ名	ファイルの説明	ファイル拡張子
データベース	ACLFile	.acl
	Access.ACCDAExtension.14	.accda
	Access.ACCDCFile.14	.accdc
	Access.ACCDEFile.14	.accde
	Access.ACCDRFile.14	.accdr
	Access.ACCDTFile.14	.accdt
	Access.ACCFTFile.14	.accft
	Access.ADEFile.14	.ade
	Access.Application.14	.accdb
	Access.BlankDatabaseTemplate.14	.mdn
	Access.BlankProjectTemplate.14	.adn
	Access.Extension.14	.mda
	Access.MDBFile	.mdb
	Access.MDEFile.14	.mde
	Access.Project.14	.adp
	Access.Shortcut.DataAccessPage.1	.maw
	Access.Shortcut.Diagram.1	.mag
	Access.Shortcut.Form.1	.maf
	Access.Shortcut.Function.1	.mau
	Access.Shortcut.Macro.1	.mam
	Access.Shortcut.Module.1	.mad
	Access.Shortcut.Query.1	.maq
	Access.Shortcut.Report.1	.mar
	Access.Shortcut.StoredProcedure.1	.mas
	Access.Shortcut.Table.1	.mdt
	Access.Shortcut.Table.1	.mat
	Access.Shortcut.View.1	.mav
	Access.WebApplicationReference.14	.accdw
	Access.WizardUserDataFile.14	.accdu
	Access.Workgroup.14	.mdw
	Accesshtmlfile	.mdbhtml
	Accesshtmlfile	.mfp
	Accessthmltemplate	.wizhtml
	Bootstrap.vsto.1	.vsto
	CATFile	.cat
	Dbfile	.db
	MSDASC	.UDL

ファイル グループ名	ファイルの説明	ファイル拡張子
	MSHelp.hxt.2.5	.hxt
	Microsoft.Jet.OLEDB.4.0	.jod
	Microsoft SQL Server Compact Edition データベース ファイル	.sdf
	Odcdatabasefile	.odcdatabasefile
	Odcnewfile	.odcnewfile
	Odctablefile	.odctablefile
	Rqyfile	.rqy

ファイル グループ名	ファイルの説明	ファイル拡張子
マニュアル	AcroExch.Document	.pdf
	AcroExch.FDFDoc	.fdf
	AcroExch.Plugin	.api
	AcroExch.XDPDoc	.xdp
	AcroExch.XFDFDocAcroExch.XFDFDoc	.xfdf
	AcroExch.pdfxml	.pdfxml
	Chm.file	.chm
	GrooveSpaceArchive	.gsa
	GrooveVCard	.vcg
	Htmlfile	.html
	InfoPath.Document.3	.infopathxml
	Jntfile	.jnt
	MSHelp.hxc.2.5	.hxc
	MSHelp.hxd.2.5	.hxd
	MSHelp.hxe.2.5	.hxe
	MSHelp.hxf.2.5	.hxf
	MSHelp.hxh.2.5	.hxh
	MSHelp.hxi.2.5	.hxi
	MSHelp.hxk.2.5	.hxk
	MSHelp.hxq.2.5	.hxq
	MSHelp.hxr.2.5	.hxr
	MSHelp.hxs.2.5	.hxs
	MSHelp.hxv.2.5	.hxv
	MSHelp.hxw.2.5	.hxw
	Mhtmlfile	.mhtml
	Odccubefile	.odccubefile
	Otffile	.otf
	Outlook.File.fdm.14	.fdm
	PowerPoint.OpenDocumentPresentation.12	.odp
	Shtmlfile	.shtml
	Windows.DVD.Maker	.msdvd
	Windows.XPSReachViewer	.xps
	Word.OpenDocumentText.12	.odt
	Word.RTF.8	.rtf
	Xhtmlfile	.xhtml
	Xmlfile	.xml

ファイル グループ名	ファイルの説明	ファイル拡張子
Email	Microsoft.PowerShellConsole.1	.psc1
	Outlook.File.eml.14	.eml
	Outlook.File.msg.14	.msg
	Outlook.File.ofs.14	.ofs
	Outlook.File.pab.14	.pab
	Outlook.File.vcf.14	.vcf
	Outlook.File.vcs.14	.vcs
エンコードおよび暗号化	CERFile	.der
	CertificateStoreFile	.sst
	Certificate_wab_auto_file	.p7c
	MSSppLicenseFile	.xrm-ms
	P10File	.p10
	P7MFile	.p7m
	P7RFile	.p7r
	P7SFile	.p7s
	PFXFile	.pfx
	SPCFile	.spc

ファイル グループ名	ファイルの説明	ファイル拡張子
実行可能ファイル	AWFile	.aw
	Access.LockFile.14	.ldb
	Application.Manifest	.application
	Application.Reference	.appref-ms
	Batfile	.bat
	Cmdfile	.cmd
	Comfile	.com
	Diagnostic.Perfmon.Document	.blg
	Drvfile	.drv
	Evtfile	.evt
	Exefile	.exe
	FlashPlayer.AudioForFlashPlayer	.f4a
	FlashPlayer.FlashVideo	.flv
	Gmmpfile	.gmmp
	Htafile	.hta
	Inffile	.inf
	JobObject	.job
	JSEFile	.JSE
	JSFile	.js
	LEXFile	.lex
	LnkFile	.lnk

ファイル グループ名	ファイルの説明	ファイル拡張子
	MSCFile	.msc
	MSInfoFile	.nfo
	Microsoft.PowerShellData.1	.psd1
	Microsoft.PowerShellModule.1	.psm
	Microsoft.PowerShellScript.1	.ps1
	Microsoft.PowerShellScript.1	.psm1
	Msi.Package	.msi
	OPCFile	.opc
	Odcfile	.odc
	Oqyfile	.oqy
	Piffile	.pif
	PowerPoint.Wizard.8	.pwz
	Regfile	.reg
	Scriptletfile	.wsc
	ShockwaveFlash.ShockwaveFlash	.swf
	Textfile	.wtx
	VBEFile	.VBE
	VBSFile	.vbs
	VisualStudio.ContentInstaller.vscontent	.vscontent
	VisualStudio.Launcher.suo	.suo
	WSHFile	.WSH
	WebpnpFile	.webpnp
	Windows.IsoFile	.iso
	Word.Wizard.8	.wiz
	WSFFile	.wsf

ファイル グループ名	ファイルの説明	ファイル拡張子
Microsoft ドキュメント	Dqyfile	.dqy
	Excel.AddInMacroEnabled	.xlam
	Excel.Addin	.xla
	Excel.Backup	.xlk
	Excel.CSV	.csv
	Excel.Dialog	.xld
	Excel.Macrosheet	.xlm
	Excel.OpenDocumentSpreadsheet.12	.ods
	Excel.Sheet.12	.xlsx
	Excel.Sheet.8	.xls
	Excel.SheetBinaryMacroEnabled.12	.xlsb
	Excel.SheetMacroEnabled.12	.xlsm
	Excel.SLK	.slk
	Excel.Template	.xlst
	Excel.Template.8	.xlt
	Excel.TemplateMacroEnabled	.xltm
	Excel.Workspace	.xlw
	Excel.XLL	.xll
	Excelhtmlfile	.xlshtml
	Excelmhtmlfile	.xlsmhtml
	Excelhtmltemplate	.xlthtml
	Excelxmlss	.xlxml
	GrooveFile	.grv
	H1qfile	.H1Q
	Iqyfile	.iqy
	OfficeTheme.12	.thmx
	OneNote.Package	.onepkg
	OneNote.Section.1	.one
	Outlook.File.det.14	.det
	Outlook.File.oft.14	.oft
	Outlook.File.ost.14	.ost
	Outlook.File.otm.14	.otm
	Outlook.File.pst.14	.pst
	PowerPoint.Addin.12	.ppam
	PowerPoint.Addin.8	.ppa
	PowerPoint.Show.12	.pptx

ファイル グループ名	ファイルの説明	ファイル拡張子
	PowerPoint.Show.8	.ppt
	PowerPoint.ShowMacroEnabled.12	.pptm
	PowerPoint.Slide.12	.sldx
	PowerPoint.SlideMacroEnabled.12	.sldm
	PowerPoint.SlideShow.12	.ppsx
	PowerPoint.SlideShow.8	.pps
	PowerPoint.SlideShowMacroEnabled.12	.ppsm
	PowerPoint.Template.12	.potx
	PowerPoint.Template.8	.pot
	PowerPoint.TemplateMacroEnabled.12	.potm
	Powerpointhtmlfile	.ppthtml
	Powerpointhtmltemplate	.pothtml
	Powerpointmhtmlfile	.pptmhtml
	Powerpointxmlfile	.pptxml
	Publisher.Document.14	.pub
	Publisherhtmlfile	.pubhtml
	Publishermhtmlfile	.pubmhtml
	VisioViewer.Viewer	.vtx
	VisualStudio.Launcher._vwdxsln80	._vwdxsln80
	Windows.XamlDocument	.xaml
	Windows.Xbap	.xbap
	Word.Addin.8	.wll
	Word.Backup.8	.wbk
	Word.Document.12	.docx
	Word.Document.8	.doc
	Word.Template.12	.dotx
	Word.Template.8	.dot
	Word.TemplateMacroEnabled.12	.dotm
	Wordhtmlfile	.dochtml
	Wordhtmlfile	.docm
	Wordhtmltemplate	.dothtml
	Wordxml	.docxml
	UXDCFILE	.uxdc
	Xslfile	.xsl

ファイル グループ名	ファイルの説明	ファイル拡張子
その他	AcroExch.acrobatsecuritysettings	.acrobatsecuritysettings
	CLSID\{9E56BE61-C50F-11CF-9A2C-00A0C90A90CE	.desklink
	CLSID\\ {ECF03A32-103D-11d2-854D-006008059367}	.mydocs
	Chkfile	.chk
	Diagnostic.Cabinet	.diagcab
	Diagnostic.Document	.diagpkg
	Dllfile	.rll
	IE.AssocFile.PARTIAL	.partial
	InfoPath.Solution.3	.xsn
	Label	.label
	MSDASQL	.dsn
	MediaCatalogMMW	.mmw
	Microsoft.InformationCard	.crd
	Microsoft.Website	.website
	PKOFile	.pko
	Pfmfile	.pfm
	STLFile	.stl
	Windows.CompositeFont	.compositefont
	WMP11.AssocFile.WMD	.wmd

- Threat Grid には、元のデバイスの API を介して Threat Grid クラウドに送信されたサンプルに関して、24 時間で 30 分のラウンドトリップ サンプル時間目標があります。ラウンドトリップ サンプル時間は、サンプルが Threat Grid のシステムで最初に認識されてから、サンプルを送信した元のデバイスに返送されるまでの時間として定義されています。推奨されるファイル解析隔離値は、1 時間です。
- アップロード用のファイル サイズ基準は、ファイル分析サービスによって、現在の脅威の傾向に基づいて確立されます。この変更は、ユーザに対して透過的に処理され、ユーザによるアクションは不要です。現在の制限は 100 MB で、電子メール クライアントが処理できる平均の上限を上回っています。
- ファイルは、分析用に送信されていない動的コンテンツを含む可能性が低いため、低リスクとみなされます。
- ファイル分析に Cisco Threat Grid パブリック クラウドを使用する場合、ファイルのアップロード制限は、構成されているデバイスに関係なく、デフォルトでは、組織レベルで 1 日あたり 200 ファイルに設定されています。この制限は、組織内の AMP が有効なすべてのデバイスで共有されます。組織がより多くのサンプル キャパ指定を必要とする場合は、シスコのセールス担当者に連絡し、Threat Grid サンプル パックについてお問い合わせください。

コメント ファイル分析サービスの負荷がキャパシティを超えた場合、ファイルの種類が分析用に選択されファイルが分析に適している場合でも、一部のファイルは分析されないことがあります。特定の種類のファイルを処理するために、サービスが一時的に使用できない場合は、アラートを受信します。

特記事項:

- ファイルが最近、送信元からアップロードされた場合、ファイルは再度アップロードされません。このようなファイルのファイル分析結果を得るには、[ファイル分析（File Analysis）] レポート ページから SHA-256 を検索します。
- アプライアンスは、たとえば、接続問題のためにファイルをアップロードできない場合など、アップロードに失敗した場合に、一度だけファイルのアップロードを試みます。失敗の原因がファイル分析サーバの過負荷の場合、アップロードはもう一度試行されます。
- 特定のファイルが分析のために実際に送信されたかどうかを判別するには、[ファイル分析（File Analysis）] レポートまたは AMP のログを参照してください。

判定更新のタイミング（レトロスペクティブ判定）

判定がクラウド内で更新された後、現在は、レトロスペクティブ判定がコンテンツ セキュリティ アプライアンスに反映されるまで、約 1 時間かかります。

詳細情報

このドキュメントの情報は、リリース ノート、およびこれらの機能をサポートする E メールおよび Web セキュリティ リリースのユーザ ガイドを補完します。お使いのリリースを確認するには、ユーザ ガイドまたはオンライン ヘルプのファイル レピュテーション フィルタリングとファイル分析に関する説明を参照してください。

追加の検索キーワード : AMP、VRT、サンドボクシング、レトロスペクティブ、AMP Threat Grid