1. Collect 採取情報

本コマンドでは、以下の障害解析情報を収集する。

－ESMPRO/ServerAgent－
- レジストリ情報
- イベントログ情報
- ファイルデータ情報
- ログファイル情報
- システム情報(msinfo32)
- Dr.Watson のログ情報
- 問題のレポートと解決策の情報
- ネットワーク情報
- WMI 情報
- MIB 情報
- SMBIOS 情報
- FT サーバ情報
- slmgr 情報
- アレイ関連情報
- DianaScope Agent 情報
- EXPRESSBUILDER 情報
- 装置情報収集ユーティリティ
- ESMPRO/ServerAgent 情報
- 更新プログラム適用情報
- グループポリシー適用情報
- ボリュームマウント情報
- ドメインコントローラ正常性情報
- ドメインコントローラ複製情報
- 時刻同期情報
- ボリューム一覧情報
- ボリューム破損状態情報
- Windows Update 情報
- 監査ログの出力設定
- DNS ゾーンの情報
- kerberos チケットの情報
- 所属サイトの情報、セキュアチャネル確立先 DC の情報
- SYSVOL フォルダ配下の情報
- フィルタードライバーおよびボリュームのインスタンス情報
- 電源プランの設定
- シャドウコピー関連の設定情報

－ESMPRO/ServerAgentService－
- レジストリ情報
- イベントログ情報
- ファイルデータ情報
- ログファイル情報
- システム情報(msinfo32)
- Dr.Watson 情報
- 問題のレポートと解決策の情報
- ネットワーク情報
- WMI 情報
- SMBIOS 情報
- slmgr 情報
- アレイ関連情報
- DianaScope Agent 情報
- EXPRESSBUILDER 情報
- 装置情報収集ユーティリティ
- WinRM 設定情報
- NeoFace Edge Server 固有ログ
- ESMPRO/ServerAgentService 情報
- 更新プログラム適用情報
- グループポリシー適用情報
- ボリュームマウント情報
- ドメインコントローラ正常性情報
- ドメインコントローラ複製情報
- 時刻同期情報
- ボリューム一覧情報
- ボリューム破損状態情報
- Windows Update 情報
- 監査ログの出力設定
- DNS ゾーンの情報
- kerberos チケットの情報
- 所属サイトの情報、セキュアチャネル確立先 DC の情報
- SYSVOL フォルダ配下の情報
- フィルタードライバーおよびボリュームのインスタンス情報
- 電源プランの設定
- シャドウコピー関連の設定情報
- NAS サーバー性能情報
- NEC ICT 機器可視化基盤 Agent のログファイル

1.1. レジストリ情報

レジストリ情報を収集する。
詳細については別紙 collect(ファイルレジストリ)参照。

1.2. イベントログ情報

イベントログ情報は、以下の情報を採取する。

イベントタイプ
システム
セキュリティ
アプリケーション
Directory Service
DNS Server
ファイル複製サービス
セットアップ

DFS レプリケーション
Internet Explorer
Key Management Service
ハードウェアイベント
Windows Powershell
Media Center
VHDMP
Microsoft-Windows-WMI-Activity/Operational
Microsoft-Windows-WMI-Activity/Trace
Microsoft-Windows-Backup
Microsoft-Windows-GroupPolicy/Operational
Active Directory Web Services

1.3. ファイルデータ情報

ファイルの日付(作成日付・更新日付・アクセス日付)とサイズ情報、ファイルバージョン、内部名を採取する。
詳細については別紙 collect(ファイルレジストリ) 参照。

1.4. ログファイル情報

ログファイルを収集する。
詳細については別紙 collect(ファイルレジストリ)参照。

1.5. システム情報(msinfo32)

msinfo32 コマンドを利用してシステム情報を採取する。

1.6. Dr.Watson のログ情報

Dr.Watson のログ情報を採取する。

1.7. 問題のレポートと解決策の情報

問題のレポートと解決策の情報を採取する。

1.8. ネットワーク情報

以下のコマンドを実行した結果を採取する。

コマンド:

```
% ipconfig /all
% route -p print
% net use
% net share
% net config WORKSTATION
```

% net config server
% netstat –ano
% tasklist /svc
% netsh interface tcp show global
% netsh advfirewall show currentprofile

1.9. WMI 情報

以下の WMI クラスから WMI 情報を採取する。

ESMPRO/ServerAgent

名前空間	WMI クラス
root¥cimv2	IBMPSG_TemperatureSensor
root¥cimv2	IBMPSG_Tachometer
root¥cimv2	IBMPSG_Fan
root¥cimv2	IBMPSG_PowerSupply
root¥cimv2	IBMPSG_UMSComponentHealth
root¥cimv2	SSD_CPUBoard
root¥cimv2	SSD_IOAdapter
root¥cimv2	SSD_DIMM
root¥cimv2	SSD_Ethernet
root¥cimv2	SSD_PCISlotInfo
root¥cimv2	SSD_Processor
root¥cimv2	SSD_SCSIAdapter
root¥cimv2	SSD_SCSIBus
root¥cimv2	SSD_SCSIDisk
root¥cimv2	SSD_SCSIEnclosure
root¥cimv2	SSD_SCSISlot
root¥cimv2	SSD_SCSIEnclosureElectronics
root¥cimv2	SSD_Driver
root¥cimv2	SSD_GigabitEthernet
root¥cimv2	SSD_SMM
root¥cimv2	SSD_BigBoardDriver
root¥cimv2	SRA_BoardInstanceDriver
root¥cimv2	SRA_CPUBoard
root¥cimv2	SRA_IOBoard
root¥cimv2	SRA_DIMM
root¥cimv2	SRA_Processor
root¥cimv2	SRA_PCIAdapter
root¥cimv2	SRA_PCIEmbeddedDevice
root¥cimv2	SRA_PCISlotInfo
root¥cimv2	SRA_StorageEnclosure
root¥cimv2	SRA_EnclosurePowerSupply
root¥cimv2	SRA_EnclosureSlot
root¥cimv2	SSD_FCAdapter
root¥cimv2	SSD_IPMIDriver
root¥cimv2	SSD_SCSILun
root¥cimv2	SRA_NetworkPort
root¥cimv2	SSD_BMC
root¥cimv2	SRA_Tachometer
root¥cimv2	SRA_TemperatureSensor
root¥cimv2	SRA_VoltageSensor
root¥cimv2	Win32_NetworkAdapter

ESMRPO/ServerAgentService

名前空間	WMI クラス
root¥ESMPRO¥AS	_Provider
root¥ESMPRO¥AS	ESM_Processor
root¥ESMPRO¥AS	ESM_GeneralInformation
root¥ESMPRO¥AS	ESM_ReportSetting
root¥ESMPRO¥AS	ESM_StorageThread
root¥ESMPRO¥AS	ESM_StorageConfig
root¥ESMPRO¥AS	ESM_StorageTotalNumber
root¥ESMPRO¥AS	ESM_StorageController
root¥ESMPRO¥AS	ESM_StorageSCSIDevice
root¥ESMPRO¥AS	ESM_StorageIDEDevice
root¥ESMPRO¥AS	ESM_StorageHardDisk
root¥ESMPRO¥AS	ESM_StorageCDROM
root¥ESMPRO¥AS	ESM_StorageTape
root¥ESMPRO¥AS	ESM_StorageOpticalMemory
root¥ESMPRO¥AS	ESM_StorageMisc
root¥ESMPRO¥AS	ESM_StorageLifeSpan
root¥ESMPRO¥AS	ESM_FileSystemThread
root¥ESMPRO¥AS	ESM_FileSystemConfig
root¥ESMPRO¥AS	ESM_FileSystemTotalNumber
root¥ESMPRO¥AS	ESM_FileSystem
root¥ESMPRO¥AS	ESM_SensorConfig
root¥ESMPRO¥AS	ESM_TemperatureSensor
root¥ESMPRO¥AS	ESM_VoltageSensor
root¥ESMPRO¥AS	ESM_FanSensor
root¥ESMPRO¥AS	ESM_LiquidLeakageSensor
root¥ESMPRO¥AS	ESM_PhysicalMemory
root¥ESMPRO¥AS	ESM_VirtualMemory
root¥ESMPRO¥AS	ESM_PageFile
root¥ESMPRO¥AS	ESM_Alive
root¥ESMPRO¥AS	ESM_GWASetting
root	_CacheControl
root¥cimv2	Win32_NetworkAdapter
root¥cimv2	Win32_ComputerSystemProduct
root¥cimv2	Win32_PerfRawData_PerfOS_Processor
root¥cimv2	Win32_PerfformattedData_PerfOS_Processor
root¥cimv2	Win32_Processor
root¥cimv2	Win32_DiskDrive
root¥cimv2	Win32_LogicalDisk
root¥cimv2	Win32_OperatingSystem

1.10. MIB 情報(ESMPRO/ServerAgent のみ)

以下の OID の示す MIB 情報を採取する。(青字は ESM MIB)

OID	備考
.1.3.6.1.4.1.119.2.2.4.4.1	General Information Group
.1.3.6.1.4.1.119.2.2.4.4.2	CPU Group
.1.3.6.1.4.1.119.2.2.4.4.4	Memory Group
.1.3.6.1.4.1.119.2.2.4.4.9	Security Group
.1.3.6.1.4.1.119.2.2.4.4.10	Environment Group
.1.3.6.1.4.1.119.2.2.4.4.11	Power Supply Group
.1.3.6.1.4.1.119.2.2.4.4.12	Storage Group
.1.3.6.1.4.1.119.2.2.4.4.15	Server Recovery and Maintenance Group

.1.3.6.1.4.1.119.2.2.4.4.19	User Defined Polling and Option Trap Group
.1.3.6.1.4.1.119.2.2.4.4.20	Operational Status Group
.1.3.6.1.4.1.119.2.2.4.4.21	Partner Extension Group
.1.3.6.1.4.1.119.2.2.4.4.22	Agent Configuration Group
.1.3.6.1.4.1.119.2.2.4.4.25	FRU Group
.1.3.6.1.4.1.119.2.2.4.4.26	LCD Group
.1.3.6.1.4.1.119.2.2.4.4.27	FTC Group
.1.3.6.1.4.1.119.2.2.4.4.29	Volume Group
.1.3.6.1.4.1.119.2.2.4.4.30	Alert based Control Group
.1.3.6.1.4.1.119.2.2.4.4.31	ESMDiskArray
.1.3.6.1.4.1.119.2.2.4.4.32	LiquidLeak Group
.1.3.6.1.4.1.119.2.2.4.4.33	NIC Information Group
.1.3.6.1.4.1.1608	MYLEXRAID-MIB (Mylex Global Array Manager 用)
.1.3.6.1.4.1.3582	MEGARAID-MIB (LSI Logic Power Console Plus 用)
.1.3.6.1.4.1.7933	Promise
.1.3.6.1.2.1.1	MIBII System
.1.3.6.1.2.1.2	MIBII Interfaces
.1.3.6.1.2.1.7	MIBII Transmission (ether)
.1.3.6.1.2.1.9	MIBII Transmission (token)
.1.3.6.1.2.1.10	MIBII Transmission (fddi)

1.11. SMBIOS 情報

SMBIOS サポート機種において、SMBIOS 情報を採取する。
(BIOS で管理している CPU やメモリ等の物理情報)

1.12. FT サーバ情報(ESMPRO/ServerAgent のみ)

FT サーバにおいて、FT サーバに関するログや情報を採取する。

1.13. slmgr 情報

Windows OS ライセンス認証情報のログを採取する。

1.14. アレイ関連情報

アレイの管理ユーティリティに関連するログや情報を採取する。

1.15. ARCServe 情報(ESMPRO/ServerAgent のみ)

ARCServe に関連するログや情報を採取する。

1.16. DianaScope Agent 情報

DianaScope Agent に関連するログや情報を採取する。

1.17. EXPRESSBUILDER 情報

EXPRESSBUILDER に関連するログや情報を採取する。

1.18. WindowsOS 情報

WindowsOS のインストールに関連するログ、WindowsUpdate、
ネットワーク、イベントログ、サービスやドライバなどの情報を採取する。

1.19. 装置情報収集ユーティリティ(Ezclct)

装置情報収集ユーティリティ(Ezclct)がインストールされている場合は実行し、
装置に関連するログや情報を採取する。

1.20. WinRM 設定情報(ESMPRO/ServerAgentService のみ)

WinRM の設定情報及びリスナ情報を採取し、Winrmcgf.txt に出力する。

1.21. NeoFace Edge Server 固有ログ(ESMPRO/ServerAgentService のみ)

NeoFace Edge Server 固有ログを採取する。

1.22. 更新プログラム適用情報

以下のコマンドを実行し、結果を採取します。

```
powershell.exe -command "Get-Hotfix"
dism /Online /Get-Packages /Format:Table
```

1.23. グループポリシー適用情報

以下のコマンドを実行し、結果を採取します。

```
gpresult /h
```

1.24. ボリュームマウント情報

以下のコマンドを実行し、結果を採取します。

```
mountvol
```

1.25.ドメインコントローラ正常性情報

以下のコマンドを実行し、結果を採取します。
dcdiag /v
dcdiag /test:DNS /v

1.26.ドメインコントローラ複製情報

以下のコマンドを実行し、結果を採取します。
repadmin /showrepl

1.27.時刻同期情報

以下のコマンドを実行し、結果を採取します。
w32tm /query /status /verbose
w32tm /query /configuration
w32tm /query /peers /verbose
w32tm /monitor

1.28.ボリューム一覧情報

以下のコマンドを実行し、結果を採取します。
fltmc volumes

1.29.ボリューム破損状態情報

以下のコマンドを実行し、結果を採取します。
fsutil repair state

1.30.Windows Update 情報

以下のコマンドを実行し、結果を採取します。
powershell.exe -command "get-windowsupdatelog -LogPath log¥getwindowsupdatelog.log"

1.31.監査ログの出力設定

以下のコマンドを実行し、結果を採取します。
auditpol /get /category:*

1.32.DNS ゾーンの情報

以下のコマンドを実行し、結果を採取します。
dnscmd /zoneprint %USERDNSDOMAIN%
dnscmd /zoneprint _msdcs.%USERDNSDOMAIN%
dnscmd /EnumZones

dnscmd /Info
dnscmd /ZoneInfo %USERDNSDOMAIN%
dnscmd /ZoneInfo _msdcs.%USERDNSDOMAIN%

1.33. kerberos チケットの情報

以下のコマンドを実行し、結果を採取します。
klist tgt
klist tickets

1.34. 所属サイトの情報、セキュアチャネル確立先 DC の情報

以下のコマンドを実行し、結果を採取します。
nltest /dsgetsite
nltest /sc_query:%USERDNSDOMAIN%

1.35. SYSVOL フォルダ配下の情報

以下のコマンドを実行し、結果を採取します。
dir %systemroot%¥sysvol /s /a
dir %systemroot%¥sysvol_dfsr /s /a

1.36. フィルタードライバーおよびボリュームのインスタンス情報

以下のコマンドを実行し、結果を採取します。
Fltmc.exe Instances

1.37. 電源プランの設定

以下のコマンドを実行し、結果を採取します。
powercfg /L
powercfg /QH

1.38. シャドウコピー関連の設定情報

以下のコマンドを実行し、結果を採取します。
vssadmin list shadowstorage
vssadmin list shadows
vssadmin list writers

1.39. NAS サーバー性能情報(ESMPRO/ServerAgentService のみ)

NAS サーバーの場合は性能に関する情報を採取します。

1.40. NEC ICT 機器可視化基盤 Agent のログファイル(ESMPRO/ServerAgentService のみ)

NEC ICT 機器可視化基盤 Agent のログファイルを採取します。
詳細については別紙 collect(ファイルレジストリ)参照。

2. 更新履歴

更新日	更新内容
2019/01/25	Windows Server 2019 向けの更新。
2019/07/12	NAS サーバーの性能情報を追加。
2020/10/01	NEC ICT 機器可視化基盤 Agent 関連のログを追加。
2024/11/21	Windows Server 2025 向けの更新。 更新プログラム適用情報の取得コマンドを WMIC から PowerShell コマンドに変更。