インシデント調査のための攻撃ツール等の実行痕跡調査に関する

報告書

一般社団法人 JPCERT コーディネーションセンター

2016 年 6 月 28 日

目次

1. はじめに

近年のサイバー攻撃では、マルウエアに感染したマシンを侵入の起点として、他のマシンへの感染拡大や、内部サーバへの侵入など、組織内の至るところを侵害する事例が多く確認されている。こうした事案においては調査対象ポイントが多数になるので、それらを重大な事象を見落とすことなく迅速に調査して、できる限り正確に被害の全体像を掌握し、善後策の立案に必要な事実を収集するための手立てが求められている。

一方、攻撃対象であるネットワークの構成は組織によって様々だが、攻撃の手口にはよく見られる共通したパターンが存在する。ネットワーク内部に侵入した攻撃者は、まず侵入した端末の情報を、ipconfig や systeminfo などの Windows で標準的に準備されているツールを使用して収集し、次に、net 等のツールを利用してネットワークに接続されている他の端末の情報や、ドメイン情報、アカウント情報などを調査する。調査した情報を基に次に侵入する端末を選んだら、ユーザのパスワード情報を盗み出すためにパスワードダンプツール mimikatz や PwDump 等のツールを使用し、パスワード情報を入手する。そして、net や at 等のツールを駆使して他の端末に侵入し、機密情報を収集するのである。

このような常套的な攻撃手口の中で使用されるツールも同じものが使用されることが多い。このような攻撃者によって使われることが多い代表的なツールがどのようなものか、さらに、それらが使用されると、どこにどのような痕跡が残るのかを把握していれば、多数の調査対象ポイントを体系的かつ迅速に調査できるようになると考えられる。

このような利用を想定した上で、JPCERT コーディネーションセンター (以下「JPCERT/CC」という。) では、近年確認されている組織内ネットワークでのインシデント調査を通じて、多くの攻撃者が使用するツールを抽出し、それらツールの実行でサーバやクライアントにどのようなログが残るのか、またどのような設定をすれば十分な情報を含むログを取得できるようになるのかを調査した。本報告書は、その調査結果をまとめたものである。

本書の構成は次のとおりである。まず、第 2 章では、本調査を行った環境や実際に調査したツールについて説明する。続いて第 3 章では、本調査の結果について説明する。第 4 章には、第 3 章で記載した調査結果を基にインシデント調査をする方法について説明する。

2. 調査方法

本章では、本調査の方法について記載する。

2.1. 調査実施内容

本調査の目的は、インシデント調査のためのログ分析において、多くの攻撃者が使用するツールの実行痕跡を読み解くことによって、攻撃の実像に迫ろうとする分析者のために参考となる、基礎的な情報を整理して提供することにある。すなわち、ログに記録された情報から、どのツールが実行されたのかを割り出し、また逆に、あるツールが実行された場合に、どのような情報がどのログに記録されるのかを提示することにより、効果的なログ調査をガイドできるような辞書づくりを目指した。

本調査では、多くの攻撃者によって使用されていると我々が考えたツールについて調査している。どのようなツールを多くの攻撃者が使用していると我々が考えたかに関しては次節で述べる。調査するログなどの対象は、インシデント調査の専門家ではない人でも比較的容易に調べることができる次の項目を対象とした。

- イベントログ
- 実行履歴
- レジストリエントリ

なお、Windows の標準設定では調査のために十分なイベントログを取得できない。本調査では、次の設定をした場合とデフォルト設定のままの場合について記録されるログを調査した。

- 監査ポリシーの有効化
- Sysmon のインストール

監査ポリシーとは、Windows に標準で搭載されているログオン・ログオフやファイルアクセスなどの詳細なログを取得するための設定である。監査ポリシーは、ローカル グループ ポリシーから確認、設定変更することができる。

また、Sysmon はマイクロソフトが提供するツールで、プロセスの起動、ネットワーク通信、ファイルの変更などをイベントログに記録することができる。Sysmon をインストールすると以下のようにイベントビューアーから記録されたログを確認することができるようになる。

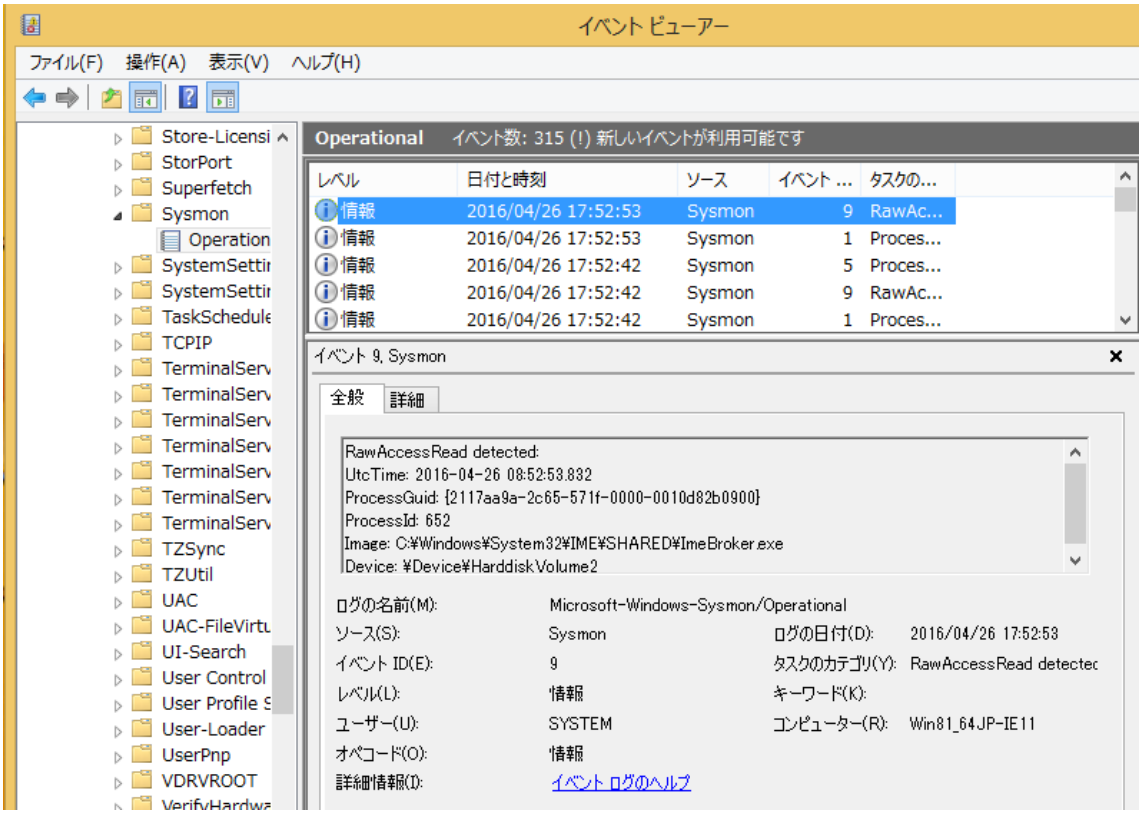


図 2-1: イベント ビューアーから Sysmon のログを確認

本調査では、2.2 節で記載したツールを Windows のドメインコントローラおよびクライアントからなる仮想環境ネットワーク上で実際に実行し、実行の前後でのシステムの変化を調べる方法により、実行履歴とイベントログ、レジストリエントリの記録を調査して、3 章にまとめた。調査に利用したネットワーク環境の詳細は 2.3 節で述べる。

2.2. 調査したツール

JPCERT/CC が対応したインシデント調査で、複数の事案で攻撃者による使用が確認されたものの中から、コマンド実行やパスワードハッシュの入手、リモートログインなどの攻撃動作に直接つながるものを中心に 44 種類を、インシデント調査において鍵となる、多くの攻撃者が使用するツールとして選定した。それらをツールの攻撃者による使用目的ごとに分類して表 2-1 に示す。

表 2-1: 調査したツール一覧

攻撃者がツールを使用する目的	ツール	章番号
コマンド実行	PsExec	3.2.1
	wmic	3.2.2
	PowerShell	3.2.3
	wmiexec.vbs	3.2.4
	BeginX	3.2.5
	winrm	3.2.6

攻撃者がツールを使用する目的	ツール	章番号
	at	3.2.7
	winrs	3.2.8
	BITS	3.2.9
パスワード、ハッシュの入手	PWDump7	3.3.1
	PWDumpX	3.3.2
	Quarks PwDump	3.3.3
	Mimikatz(パスワードハッシュ入手)	3.3.4
	Mimikatz(チケット入手)	3.3.5
	WCE	3.3.6
	gsecdump	3.3.7
	lslsass	3.3.8
	Find-GPOPasswords.ps1	3.3.9
	Mail PassView	3.3.10
	WebBrowserPassView	3.3.11
	Remote Desktop PassView	3.3.12
通信の不正中継 （パケットトンネリング）	Htran	3.4.1
	Fake wpad	3.4.2
リモートログイン	RDP	3.5.1
Pass-the-hash **Pass-the-ticket**	WCE (リモートログイン)	3.6.1
	Mimikatz (リモートログイン)	3.6.2
SYSTEM 権限に昇格	MS14-058 Exploit	3.7.1
	MS15-078 Exploit	3.7.2
権限昇格	SDB UAC Bypass	3.8.1
ドメイン管理者権限 アカウントの奪取	MS14-068 Exploit	3.9.1
	Golden Ticket (Mimikatz)	3.9.2
	Silver Ticket (Mimikatz)	3.9.3
Active Directory データベースの奪取 （ドメイン管理者ユーザの作成、もしくは管理者グループに追加）	ntdsutil	3.10.1
	vssadmin	3.10.2
ローカルユーザー・グループの追加・削除	net user	3.11.1
ファイル共有	net use	3.12.1
	net share	3.12.2
	icacls	3.12.3
痕跡の削除	sdelete	3.13.1
	timestomp	3.13.2
イベントログの削除	wevtutil	3.14.1

攻撃者がツールを使用する目的	ツール	章番号
アカウント情報の取得	csvde	3.15.1
	ldifde	3.15.2
	dsquery	3.15.3

2.3. 調査の実施環境

本調査では、攻撃の対象となるシステムを単純化した一対のクライアントとサーバからなるシステムを仮想環境ネットワーク上に構築し、この上でツールを実行して、実行に伴うファイルやレジストリ等の変化を観測した。クライアントとサーバには、それぞれの次のバージョンの Windows OS を搭載した、合計 4 通りのシステム構成について調査した。また、サーバ上には Active Directory を稼働させてクライアントを管理する構成をとった。

- クライアントの搭載 OS
  - Windows 7 Professional Service Pack 1
  - Windows 8.1 Pro
- サーバの搭載 OS
  - Windows Server 2008 R2 Service Pack 1
  - Windows Server 2012 R2

3. 調査結果

本章では、本調査で検証したツールの機能等の基本情報と、当該ツールを実行した時に記録されるログ情報をまとめている。基本情報については、攻撃者の視点を交えて一連の攻撃の中でのツールの意味合いを理解しやすいように努めた。また、本章では、2.1 節で記載した設定を行った上で取得可能なログの詳細について記載している。(なお、監査ポリシーの設定および Sysmon のインストール方法については、7 章に記載している。)

3.1. 本章の構成

以降では、44 種類の各ツールについて、以下のような表形式で解説している。

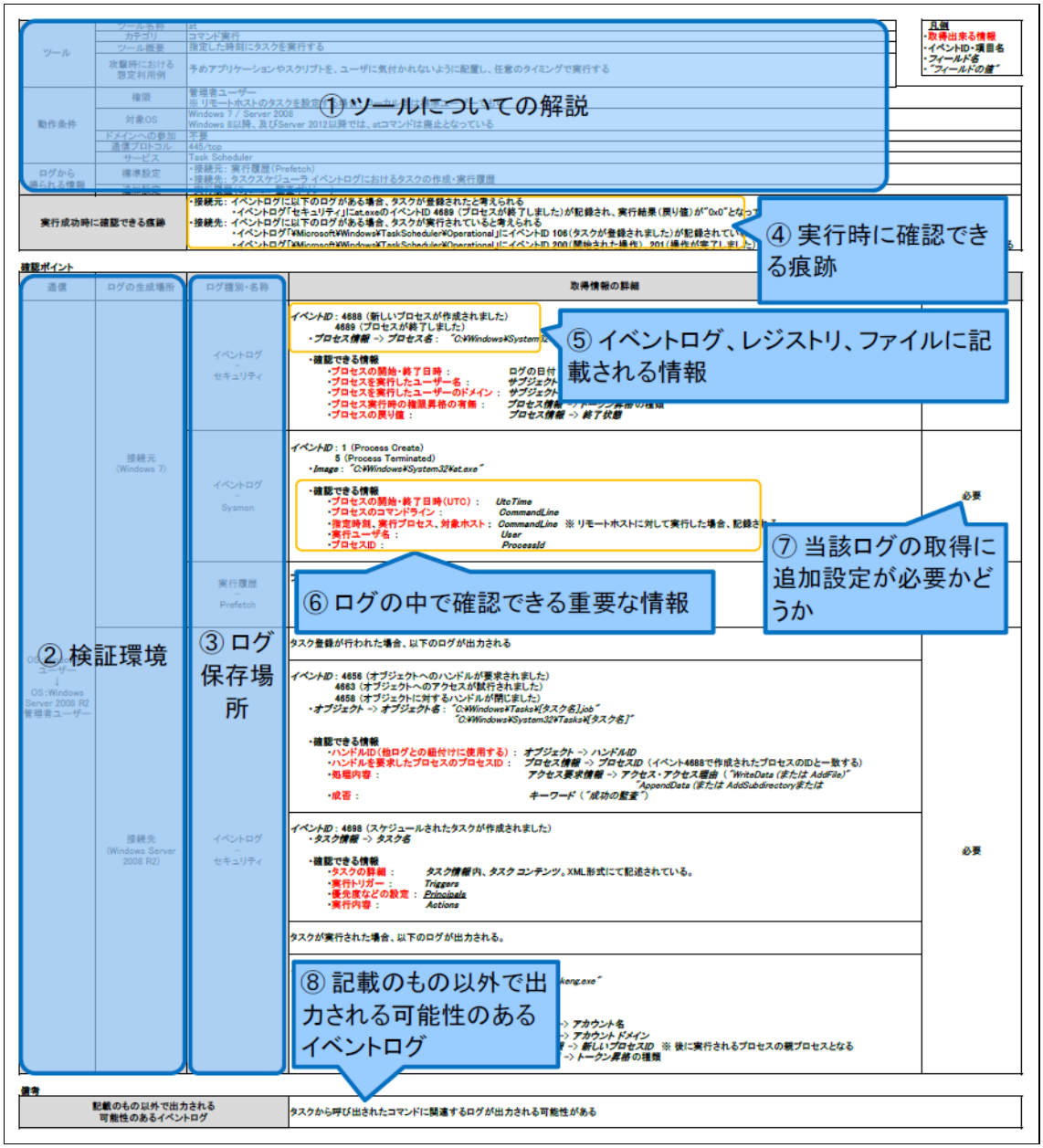


図 3-1: 次節以降の記載内容

各項目で記載している内容について以下で説明する。

① ツールについての解説

- ツールを使用された場合の影響やツールを使用する際の権限、通信方式、関連するサービスについて記載

② 検証環境

- 接続元および接続先の OS 情報

③ ログ保存場所

- レジストリ、イベントログの保存場所

④ 実行成功時に確認できる痕跡

- ツールの実行が、成功したことを確認する方法を記載

⑤ イベントログ、レジストリ、ファイルに記載される情報

- この項目の記載内容に一致しているものがある場合は、当該ツールの実行によって記録された可能性があるため、調査する必要がある

⑥ ログの中で確認できる重要な情報

- 対象のログで記録される調査に活用できる重要な情報を記載（すべての記録される情報を記載しているわけではない）

⑦ 当該ログの取得に追加設定が必要かどうか

- 標準設定で取得可能な場合「-」、追加設定が必要な場合「必要」

⑧ 記載のもの以外で出力される可能性のあるイベントログ

- その他に記録される可能性があるログがある際のみ記載

3.2.1. PsExec

<基本情報>

ツール	ツール名称	PsExec
	カテゴリ	コマンド実行
	ツール概要	リモートシステム上でプロセスを実行する
	攻撃時における想定利用例	ドメイン内の端末やサーバーに対して、リモートでコマンドを実行する ・接続元： PsExecコマンド実行元 ・接続先： PsExecコマンドによってログインされた先
動作条件	権限	・接続元： 標準ユーザー ・接続先： 管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	135/tcp、445/tcp、ランダムなHigh Port ※ ドメイン環境下で実行する場合は、ドメインコントローラとのKerberos認証通信が発生する
	サービス	–
ログから得られる情報	標準設定	・接続元： PsExecの使用許諾契約に同意した旨のレジストリが記録される ・接続先： "PSEXESVC"サービスがインストールされ、開始・終了したことが記録される
	追加設定	・実行履歴（Sysmon・監査ポリシー） ・接続元： PsExecプロセスを実行したこと、接続先にネットワーク接続したこと、リモート実行されたコマンド名及び引数が記録される ・接続先： PSEXESVCのバイナリが作成・アクセスされたこと、接続元からネットワーク接続されたこと、リモート実行されたコマンド名及び引数が記録される
実行成功時に確認できる痕跡		以下が確認できた場合、PsExecが実行された可能性がある ・接続元： イベントログに以下のログがある場合 ・イベントログ「セキュリティ」にpsexec.exeのイベントID **4689**（プロセスが終了しました）が記録され、実行結果（戻り値）が"0x0"となっている ・接続先： PSEXESVC.exeがインストールされている

凡例
・**取得出来る情報**
・**イベントID・項目名**
・***フィールド名***
・*"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows 管理者ユーザー	接続元	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[実行ファイル（psexec.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[実行ファイル（psexec.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ※ コマンドライン内の引数に、**リモート実行されたコマンド**が記録される ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		実行履歴 – レジストリ	**レジストリエントリ**： HKEY_USERS¥[SID]¥Software¥Sysinternals¥PsExec ・***EulaAccepted*** ※ 過去にPsExecを実行したことが無い場合、使用許諾契約に同意した旨のレジストリが出力される （過去に実行している場合、レジストリの内容は変化しない）	–
	接続先	イベントログ – システム	***イベントID*** : **7045**（サービスがシステムにインストールされました） ・**確認できる情報** ・**プロセス名**： *"PSEXESVC"* ・**パス**： *"%SystemRoot%¥PSEXESVC.exe"*	–
			イベントID : **7036**（サービスの状態が移行しました） ※ サービス *"PSEXESVC"* が、リモートプロセス実行前に *"実行中"* となり、実行後に *"停止"* となる	
		イベントログ – セキュリティ	***イベントID*** : **5156**（フィルタリング プラットフォームによる接続の許可） ※ 接続元から接続先に対して、宛先ポートを135及び445とした通信が発生する （例： *192.168.0.10:49210から192.168.0.2:**445** への通信がWindows フィルタリング プラットフォームにより、接続が許可されました*） ※ 接続元から接続先に対して、ランダムなHigh Port（1024以上のポート）を宛先ポートとした通信が発生する	必要
			イベントID : **5140**（ネットワーク共有オブジェクトにアクセスしました） ・**確認できる情報** ・**接続された日時**： ログの日付 ※ PSEXESVC.exeの開始より前の日時となる ・**接続に使用されたアカウント**： ***サブジェクト*** -> ***セキュリティID*** 及び ***アカウント名*** ・**接続元端末**： ***ネットワーク情報*** -> ***接続元IPアドレス*** 及び ***接続元ポート*** ・**接続された共有**： *"¥??¥C:¥Windows"*（管理共有）	
			イベントID : **4672**（新しいログオンに特権を割り当てました） ※ このイベントが発生する前に、イベント 4624が発生する イベント**4624**でログオンしたアカウントに対して、特権が割り当てられる ・**確認できる情報** ・**接続に使用されたアカウント**： ***サブジェクト*** -> ***セキュリティID*** 及び ***アカウント名*** ・**割り当てられた特権**： ***特権***	
			イベントID : **4656**（オブジェクトに対するハンドルが要求されました）、**4663**（オブジェクトへのアクセスが試行されました） ・***オブジェクト*** -> ***オブジェクト名***： *"C:¥Windows¥PSEXESVC.exe"*	
			イベントID : **5140**（ネットワーク共有オブジェクトにアクセスしました） ・**確認できる情報** ・**接続に使用されたアカウント**： ***サブジェクト*** -> ***セキュリティID*** 及び ***アカウント名*** ・**接続元端末**： ***ネットワーク情報*** -> ***接続元IPアドレス*** 及び ***接続元ポート*** ・**接続された共有**： *"¥¥*¥IPC$"*（管理共有）	
			イベントID : **5145**（ネットワーク共有オブジェクトに対する、クライアントのアクセス権をチェックしました）※ 同イベントIDは数度記録される ・**確認できる情報** ・**接続に使用されたアカウント**： ***サブジェクト*** -> ***セキュリティID*** 及び ***アカウント名*** ・**接続元端末**： ***ネットワーク情報*** -> ***接続元IPアドレス*** 及び ***接続元ポート*** ・**対象となる共有**： ***共有情報*** -> ***対象パス*** ※ 対象パスに含まれるものには、*"PSEXESVC"* 及び *"¥¥??¥C:¥Windows"* がある	
			イベントID : **4656**（オブジェクトに対するハンドルが要求されました） **4660**（オブジェクトが削除されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセスID*** : *"0x4"*（SYSTEM） ・**確認できる情報** ・**対象ファイル**： ***オブジェクト*** -> ***オブジェクト名***（*"C:¥Windows¥PSEXESVC.exe"*） ・**ハンドルID**： ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容**： ***アクセス要求情報*** -> ***アクセス***（*"DELETE"*、*"ReadAttributes"*） ・**成否**： ***キーワード***（*"成功の監査"*）	

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows 管理者ユーザー （続）	接続先 （続）	イベントログ － Sysmon	***イベントID***：**1**（Process Create） **5**（Process Terminated） ・***Image***：*"C:¥Windows¥PSEXESVC.exe"* ・***User***：*"SYSTEM"* **・確認できる情報** **・PSEXESVC.exeが実行された日時**：ログの日付	必要
			イベントID：**1**（Process Create） **5**（Process Terminated） **・確認できる情報** **・リモート実行されたプロセス**：***Image*** **・引数**：***CommandLine*** **・プロセスの開始・終了日時（UTC）**：***UtcTime*** ※ PSEXESVC.exeの開始より後、終了より前の日時となる **・リモート実行に使用されたアカウント**：***実行ユーザー***	

<備考>

記載のもの以外で出力される可能性のあるイベントログ	PsExecを用いて実行されたプロセスに関連する情報が、「接続先」に記録される可能性がある

3.2.2. WMIC (Windows Management Instrumentation Command Line)

<基本情報>

ツール	ツール名称	WMIC (Windows Management Instrumentation Command Line)
	カテゴリ	コマンド実行
	ツール概要	Windowsのシステム管理に使用するツール
	攻撃時における想定利用例	WMIを用いて、リモートシステムの情報を取得することや、コマンドを実行することが考えられる ・接続元： wmicコマンド実行元 ・接続先： wmicコマンドによってアクセスされた端末
動作条件	権限	標準ユーザー　※ リモート側で実行するコマンドによっては、管理者権限が必要な場合もある
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	135/tcp, 445/tcp, 1024以上のランダムに選択されるTCPポート
	サービス	Windows Management Instrumentation、Remote Procedure Call (RPC)
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・プロセスの実行内容（wmicへの引数）、及び実行成否（戻り値）（Sysmon・監査ポリシー）
実行成功時に確認できる痕跡		「接続元」「接続先」において、同時刻に以下のログが確認できる場合、リモート接続が行われた可能性がある ・接続元： イベントログに以下のログがある場合 ・イベントログ「セキュリティ」にWMIC.exeのイベントID **4689**（プロセスが終了しました）が記録され、実行結果（戻り値）が"0x0"となっている ・接続先： Sysmonに以下のログがある場合 ・イベントログ「Sysmon」でイベントID **1**、**5**でWmiPrvSE.exeが実行されたことが記録されている

凡例
・**取得出来る情報**
・**イベントID・項目名**
・***フィールド名***
・*"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows 管理者ユーザー	接続元	イベントログ － セキュリティ	***イベントID*** ： **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** ： *"C:¥Windows¥System32¥wbem¥WMIC.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** ： ログの日付 ・**プロセスを実行したユーザー名** ： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** ： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** ： ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値** ： ***プロセス情報*** -> ***終了状態***	必要
		イベントログ － Sysmon	***イベントID*** ： **1**（Process Create） **5**（Process Terminated） ・***Image*** ： *"C:¥Windows¥System32¥wbem¥WMIC.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** ： ***UtcTime*** ・**プロセスのコマンドライン** ： ***CommandLine***　※ wmic.exeの引数より、**リモートホスト**と**実行コマンド**が確認可能 ・**実行ユーザ名** ： ***User*** ・**プロセスID** ： ***ProcessId***	必要
		実行履歴 － Prefetch	**ファイル名： C:¥Windows¥Prefetch¥WMIC.EXE-98223A30.pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** ： ***Last Run Time***	－
	接続先	イベントログ － Sysmon	***イベントID*** ： **1**（Process Create） **5**（Process Terminated） ・***Image*** ： *"C:¥Windows¥System32¥wbem¥WmiPrvSE.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** ： ***UtcTime*** ・**プロセスのコマンドライン** ： ***CommandLine***　*（"C:¥Windows¥System32¥wmiprvse.exe -secured -Embedding"）* ・**実行ユーザ名** ： ***User***　*（"NT AUTHORITY¥NETWORK SERVICE"）* ・**プロセスID** ： ***ProcessId***	必要
		実行履歴 － Prefetch	**ファイル名： C:¥Windows¥Prefetch¥WMIPRVSE.EXE-1628051C.pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** ： ***Last Run Time***	－

<備考>

記載のもの以外で出力される可能性のあるイベントログ	・wmicで呼び出された処理によっては、処理特有のログが記録される可能性がある ・ユーザがActive Directory上に存在する場合、認証要求がドメインコントローラに記録される可能性がある しかし、wmicにより発生した認証要求であるか、それ以外のものであるかを断定することは出来ない

3.2.3. PowerShell (リモートコマンド実行)

<基本情報>

ツール	ツール名称	PowerShell (リモートコマンド実行)
	カテゴリ	コマンド実行
	ツール概要	Windowsの管理や設定に利用可能なコマンドラインツール (Windows 7以降では標準で利用が可能) PowerShellを実行したホストのみでなく、ネットワークを介して他のホストに対してコマンドを実行することも可能
	攻撃時における想定利用例	ネットワーク内の、ドメインコントローラや他ホストに対して、管理者権限が必要な動作を可能とするよう設定を変更する ・接続元: PowerShellコマンド実行元 ・接続先: PowerShellコマンドによってログインされた先
	実行例 (検証時に使用したコマンド)	以下のコマンドを実行 ※ 接続先で、Windows Remote Management (WS-Management)サービスを起動しておく必要がある > Enable-PSRemoting -force > Set-Item WSMan:¥localhost¥Client¥TrustedHosts -Value * > Enter-PSSession "[接続先]" -Credential Administrator
動作条件	権限	PowerShellは一般ユーザーでも利用可能 ※ 設定を変更するスクリプトを実行する場合、設定変更対象となるホストにおいて適切な権限が必要
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	ローカル端末内を管理する場合は不要 ※ 他端末を管理する場合、HTTPでは80/tcp又は5985/tcp、HTTPSでは443/tcp又は5986/tcpを使用する
	サービス	接続先: Windows Remote Management (WS-Management)
ログから得られる情報	標準設定	実行履歴(Prefetch)
	追加設定	実行履歴(Sysmon・監査ポリシー) ※ PowerShellの終了イベントより、実行結果を確認可能 監査ポリシーにより、接続元から、接続先の5985/tcp(HTTP)又は5986/tcp(HTTPS)への通信が発生していることを確認可能
実行成功時に確認できる痕跡		以下のログが同じ時刻に確認できた場合、リモートコマンド実行が行われた可能性がある ※ Prefetchの場合も同様 ・接続元: イベントログに以下のログがある場合 ・イベントログ「セキュリティ」にPowerShellのイベントID **4689** (プロセスが終了しました)が記録され、実行結果(戻り値)が"0x0"となっている ・接続先: イベントログに以下のログがある場合 ・イベントログ「セキュリティ」にwsmprovhost.exeのイベントID **4689** (プロセスが終了しました)が記録され、実行結果(戻り値)が"0x0"となっている

凡例
・**取得出来る情報**
・**イベントID・項目名**
・***フィールド名***
・*"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS:Windows ユーザー ↓ OS:Windows 管理者ユーザー	接続元	イベントログ - セキュリティ	***イベントID*** : **4688** (新しいプロセスが作成されました) **4689** (プロセスが終了しました) ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥Windows PowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **5156** (フィルタリング プラットフォームによる接続の許可) ・***プロセス名*** : *"¥device¥harddiskvolume2¥windows¥system32¥windowspowershell¥v1.0¥powershell.exe"* ・***ネットワーク情報*** -> ***方向*** : *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** : *"::1"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** : *"47001"・"6"(TCP)*	
			イベントID : **5156** (フィルタリング プラットフォームによる接続の許可) ・***プロセス名*** : *"¥device¥harddiskvolume2¥windows¥system32¥windowspowershell¥v1.0¥powershell.exe"* ・***ネットワーク情報*** -> ***方向*** : *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** : *"[接続先ホスト]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** : *"5985"(HTTP)又は"5986"(HTTPS)・"6"(TCP)* ※ポート番号は、接続先側で指定することで変更が可能	
		イベントログ - Sysmon	***イベントID*** : **1** (Process Create) **5** (Process Terminated) ・***Image*** : *"C:¥Windows¥System32¥Windows PowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** : *"C:¥Windows¥System32¥Windows PowerShell¥v1.0¥powershell.exe"* ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		実行履歴 - Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥POWERSHELL.EXE-920BBA2A.pf** ・**確認できる情報** (ツールを利用して下記を確認できる ツール:WinPrefetchView) ・**最終実行日時** : ***Last Run Time***	-
	接続先	イベントログ - セキュリティ	***イベントID*** : **5156** (フィルタリング プラットフォームによる接続の許可) ・***プロセスID*** : *"4"* ・***アプリケーション名*** : *"System"* ・***ネットワーク情報*** -> ***方向*** : *"着信"* ・**確認できる情報** ・**接続元ホスト**: ***ネットワーク情報*** -> ***送信元アドレス*** ・**着信ポート**: ***ネットワーク情報*** -> ***ソース ポート*** (HTTPの場合 *"5985"*、HTTPSの場合 *"5986"*) ・**プロトコル**: ***ネットワーク情報*** -> ***プロトコル*** (*"6"*)	必要
			イベントID : **4624** (アカウントが正常にログオンしました) ・***ログオン タイプ*** : *"3"* ・**確認できる情報** ・**ログオンが成功した日時**: ***ログの日付*** ※ 接続元における、wsmprovhost.exeプロセス作成(イベントID **4688**)直後、終了(イベントID **4689**)より前となる ・**接続先端末においてプロセスを実行したアカウント名** : ***新しいログオン*** -> ***セキュリティID・アカウント名***	-
			イベントID : **4634** (アカウントが正常にログオフしました) ・**確認できる情報** ・**ログオフした日時**: ***ログの日付*** ※ 接続元における、wsmprovhost.exeプロセス終了(イベントID **4689**)後となる	
		イベントログ - Sysmon	***イベントID*** : **1** (Process Create) **5** (Process Terminated) ・***Image*** : *"C:¥Windows¥System32¥at.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** : *"C:¥Windows¥System32¥wsmprovhost.exe -Embedding"* ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		実行履歴 - Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥WSMPROVHOST.EXE-EF06207C.pf** ・**確認できる情報** (ツールを利用して下記を確認できる ツール:WinPrefetchView) ・**最終実行日時** : ***Last Run Time***	-

<備考>

記載のもの以外で出力される可能性のあるイベントログ	実行されたコマンドによっては、そのコマンドが出力するログが接続先に記録される可能性がある

3.2.4. wmiexec.vbs

<基本情報>

ツール	ツール名称	wmiexec.vbs
	カテゴリ	コマンド実行
	ツール概要	Windowsのシステム管理に使用するツール
	攻撃時における想定利用例	他端末に対して、スクリプト処理を実行する ・接続元： wmiexec.vbs実行元 ・接続先： wmiexec.vbsによってアクセスされた端末
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	135/tcp, 445/tcp
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・ファイルの作成・削除履歴（監査ポリシー） ・実行履歴（Sysmon）
実行成功時に確認できる痕跡		接続先： "WMI_SHARE"共有が作成され、削除されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows ユーザー	接続元	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥cscript.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***プロセス名*** : *"¥device¥harddiskvolume2¥windows¥system32¥cscript.exe"* ・**確認できる情報** ・**送信元ポート**: ***ネットワーク情報*** -> ***宛先ポート*** ※ ポート番号は、接続先側で指定することで変更が可能	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"C:¥Windows¥System32¥cscript.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名：C:¥Windows¥Prefetch¥CSCRIPT.EXE-D1EF4768.pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** : ***Last Run Time***	–
	接続先	イベントログ – セキュリティ	***イベントID*** : **4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***オブジェクト*** -> ***オブジェクト名*** : *"(C:¥Windows¥Temp¥wmi.dll)"* ・***アクセス要求情報*** -> ***アクセス・アクセス理由*** : (*"WriteData (または AddFile)"*、*"AppendData (または AddSubdirectory または CreatePipeInstance)"*) ・**確認できる情報** ・**プロセス名**: *"C:¥Windows¥System32¥cmd.exe"* ・**ハンドルID**: ***オブジェクト*** -> ***ハンドルID*** ※ 他のログとの紐付けに使用する	必要
			イベントID : **5142**（ネットワーク共有オブジェクトが追加されました） ・**確認できる情報** ・**プロセスの開始日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**共有名**: ***共有情報*** -> ***共有名***：（*"¥¥*¥WMI_SHARE"*） ・**共有パス**: ***共有情報*** -> ***共有パス:***（*"C:¥Windows¥Temp"*）	
			イベントID : **5145**（クライアントに必要なアクセスを付与できるかどうかについて、ネットワーク共有オブジェクトがチェックされました） ・**確認できる情報** ・**プロセスの開始日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**共有名**: ***共有情報*** -> ***共有名***（*"¥¥*¥WMI_SHARE"*） ・**共有パス**: ***共有情報*** -> ***共有パス***（*"¥??¥C:¥windows¥temp"*） ・**共有パス**: ***共有情報*** -> ***相対ターゲット名:***（*"wmi.dll"*）	必要
			イベントID : **4656**（オブジェクトに対するハンドルが要求されました） **4660**（オブジェクトが削除されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***オブジェクト*** -> ***オブジェクト名*** : *"(C:¥Windows¥Temp¥wmi.dll)"* ・***アクセス要求情報*** -> ***アクセス・アクセス理由*** : *"DELETE"* ・**確認できる情報** ・**プロセス名**: *"(C:¥Windows¥System32¥cmd.exe)"*	
			イベントID : **5144**（ネットワーク共有オブジェクトが削除されました。） ・**確認できる情報** ・**共有名**: ***共有情報*** -> ***共有名***（*"¥¥*¥WMI_SHARE"*） ・**共有パス**: ***共有情報*** -> ***共有パス:***（*"C:¥Windows¥Temp"*）	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"C:¥Windows¥System32¥wbem¥WmiPrvSE.exe"* *"C:¥Windows¥System32¥cmd.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加 設定
OS：Windows ユーザー ↓ OS：Windows ユーザー （続）	接続先 （続）	実行履歴 － Prefetch	**ファイル名：** C:¥Windows¥Prefetch¥CSCRIPT.EXE-D1EF4768.pf C:¥Windows¥Prefetch¥WMIPRVSE.EXE-1628051C.pf **・確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） **・最終実行日時**：　*Last Run Time*	－

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	－

3.2.5. BeginX

<基本情報>

ツール	ツール名称	BeginX
	カテゴリ	コマンド実行
	ツール概要	クライアントからサーバに対してリモートコマンド実行をする
	攻撃時における想定利用例	リモートホストの設定を変更したり、情報を取得したりする ・接続元： BeginXクライアント実行元 ・接続先： BeginXサーバ実行元
	参考情報	https://www.jpcert.or.jp/present/2015/20151028_codeblue_ja.pdf
動作条件	権限	一般ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	tcpまたはudpでポート番号は検体毎に異なる
	サービス	–
ログから得られる情報	標準設定	・両ホスト： 実行履歴（Prefetch） ・接続先： Windowsファイアウォールの設定変更が実施される
	追加設定	・両ホスト： 実行履歴（Sysmon・監査ポリシー） 所定のポートを経由して通信したことが記録されている
実行成功時に確認できる痕跡		・接続元： 接続先で意図せず許可されているポートと通信をしたことが記録されている ・接続先： 意図しない通信がWindows Firewallで許可されており、該当のポートでリッスンしている検体が存在する

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー → OS：Windows ユーザー	接続元	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体]"* ・**確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	–
			イベントID : **5156**（Windowsフィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション名*** : *"[検体]"* ・**確認できる情報** ・**通信の方向**: ***ネットワーク情報*** -> ***方向***（*"送信"*） ・**ソースポート**: ***ネットワーク情報*** -> ***ソース ポート*** ・**宛先ホスト**: ***ネットワーク情報*** -> ***宛先アドレス***（検体名を実行時に指定したホスト） ・**宛先ポート**: ***ネットワーク情報*** -> ***宛先ポート ・プロトコル***	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ イベントID 1に記録される ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名： C:¥Windows¥Prefetch¥[検体]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**: ***Last Run Time***	–
	接続先	イベントログ – セキュリティ	検体が実行された直後に、以下が記録される	–
			イベントID : **5154**（Windows フィルターリング プラットフォームで、アプリケーションまたはサービスによるポートでの着信接続のリッスンが許可されました） ・***アプリケーション名*** : *"[検体]"* ・**確認できる情報** ・**ソースポート**: ***ネットワーク情報*** -> ***ソース ポート*** ・**利用プロトコル**: ***ネットワーク情報*** -> ***プロトコル***	
			イベントID : **5447**（Windows フィルターリング プラットフォームのフィルターが変更されました） ※ ファイアウォールへの設定変更反映 **4946**（Windows ファイアウォールの例外の一覧が変更されました） ※ ファイアウォールへの設定変更反映	
			接続元がコマンドを実行する際に、以下が記録される	
			イベントID : **5156**（Windowsフィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション名*** : *"[検体]"* ・**確認できる情報** ・**通信の方向**: ***ネットワーク情報*** -> ***方向***（*"着信"*） ・**ソースポート**: ***ネットワーク情報*** -> ***ソース ポート*** ・**宛先ホスト**: ***ネットワーク情報*** -> ***宛先アドレス***（リモート接続元のホスト） ・**宛先ポート**: ***ネットワーク情報*** -> ***宛先ポート ・プロトコル***	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体]"*, *"netsh.exe"*, *"rundll32.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 各***Image***ごとに実行した内容が記載されている ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名： C:¥Windows¥Prefetch¥CMD.EXE-4A81B364.pf** **C:¥Windows¥Prefetch¥[検体]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**: ***Last Run Time***	–
		実行履歴 – レジストリ	**レジストリエントリ： HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥services¥SharedAccess¥Parameters¥FirewallPolicy¥FirewallRules** ※ 検体実行時にWindowsファイアウォールの設定が変更されるため、レジストリの値が変更される ルール内に、検体の実行ファイル名が含まれる	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.2.6. WinRM

<基本情報>

ツール	ツール名称	WinRM
	カテゴリ	コマンド実行
	ツール概要	リモートの端末から情報を搾取する
	攻撃時における想定利用例	リモートコマンドを実行する前に調査のため実施する ・接続元： WinRMマンド実行元 ・接続先： WinRMコマンドによってアクセスされた端末
動作条件	権限	管理ユーザー
	対象OS	Windows
	ドメインへの参加	–
	通信プロトコル	5985/tcp (HTTP) 又は 5986/tcp (HTTPS)
	サービス	接続先： Windows Remote Management (WS-Management)
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・接続元： 実行履歴（Sysmon・監査ポリシー） ・接続先： 接続元からの着信接続
実行成功時に確認できる痕跡		・接続元： 以下のログがある場合、WinRMが実行された可能性がある ・イベントログ「Sysmon」の**イベントID:1、5**でcscript.exeが接続先にアクセスしたログが記録されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows 管理者ユーザー ↓ OS：Windows 管理者ユーザー	接続元	イベントログ – セキュリティ	***イベントID***： **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名***： *"C:¥Windows¥System32¥cscript.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時**： ログの日付 ・**プロセスを実行したユーザー名**： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**： ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**： ***プロセス情報*** -> ***終了状態***	必要
			イベントID： **5156**（Windowsフィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション名***： *"¥device¥harddiskvolume2¥windows¥system32¥cscript.exe"* ・**確認できる情報** ・**通信の方向**： ***方向***（*"送信"*） ・**送信先ホスト**： ***ネットワーク情報*** -> ***宛先アドレス*** ・**送信先ポート**： ***宛先ポート***（*"5958"（HTTP）又は "5986"（HTTPS）*）、***プロトコル***（*"6"* = TCP）	
		イベントログ – Sysmon	***イベントID***： **1**（Process Create） **5**（Process Terminated） ・***Image***： *"C:¥Windows¥System32¥cscript.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**： ***UtcTime*** ・**指定時刻、実行プロセス、対象ホスト**： ***CommandLine*** ・**実行ユーザ名**： ***User*** ・**プロセスID**： ***ProcessId***	必要
		イベント ログ – アプリケーションとサービス Microsoft¥Windows¥Windows Remote Management	***イベントID***： **166**（選択された認証機構） ・**確認できる情報** ・**認証方式**： ***認証機構***（*選択された認証機構は Kerberos です*）	–
			イベントID： **80**（操作 Get の要求を送信しています） ・**確認できる情報** ・**送信先コンピューターおよびポート**： *"[ホスト名]:[ポート]"*	
			イベントID： **143**（ネットワーク レイヤーから応答を受信しました） ・**確認できる情報** ・**ステータス**： ***状態***（*200 (HTTP_STATUS_OK)*）	
			イベントID： **132**（WSMan の操作 Get が正常に完了しました） ・**確認できる情報** ・**完了日時（UTC）**： ***UtcTime***	
		実行履歴 – Prefetch	**ファイル名： C:¥Windows¥Prefetch¥CSCRIPT.EXE-D1EF4768.pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**： ***Last Run Time***	–
	接続先	イベントログ – セキュリティ	***イベントID***： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名***： *"SYSTEM"* ・***ネットワーク情報*** -> ***方向***： *"着信"* ・***ネットワーク情報*** -> ***ソースポート***： *"5985"*（HTTP）又は *"5986"*（HTTPS） ・***ネットワーク情報*** -> ***プロトコル***： *"6"*（TCP） ・**確認できる情報** ・**接続元ホスト**： ***ネットワーク情報*** -> ***宛先アドレス*** ・**接続元ポート**： ***ネットワーク情報*** -> ***宛先ポート***	必要
			イベントID： **4624**（アカウントが正常にログオンしました） ・***ログオン タイプ***： *"3"* ・**確認できる情報** ・**使用されたセキュリティID**： ***新しいログオン*** -> ***セキュリティID*** ・**ログオンID**： ***サブジェクト*** -> ***ログオンID*** ・**アカウント**： ***アカウント名・アカウント ドメイン***	
			イベントID： **4656**（オブジェクトに対するハンドルが要求されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名***： *"C:¥Windows¥System32¥svchost.exe"* ・***オブジェクト*** -> ***オブジェクト名***：*"¥REGISTRY¥MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥WSMAN¥Client"* ・***オブジェクト*** -> ***オブジェクト名***：*"¥REGISTRY¥MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥WSMAN¥Service"* ・**確認できる情報** ・**ハンドルID**： ***オブジェクト*** -> ***ハンドルID*** ・**アクセス要求内容**： ***アクセス要求情報*** -> ***アクセス*** （"READ_CONTROL"、"キー値の照会"、"サブキーの列挙"、"キー変更に関する通知"） ※ 複数回この処理を実施する。	

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows 管理者ユーザー ↓ OS：Windows 管理者ユーザー （続）	Active Directory ドメイン コントローラー	イベントログ － セキュリティ	***イベントID*** ： **5156**（Windowsフィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** ： *"¥device¥harddiskvolume2¥windows¥system32¥lsass.exe"* ・***ネットワーク情報*** -> ***方向*** ： *"着信"* ・***ネットワーク情報*** -> ***ソース ポート*** ： *"88"* ・**確認できる情報** ・**接続元ホスト**： ***ネットワーク情報*** -> ***宛先アドレス***	必要
			イベントID ： **4769**（Kerberosサービス チケットが要求されました） ・***ネットワーク情報*** -> ***クライアント アドレス*** ： *"[接続元ホスト]"* ・**確認できる情報** ・**利用されたユーザー**： ***アカウント情報*** -> ***アカウント名***	

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	－

3.2.7. WinRS

<基本情報>

ツール	ツール名称	WinRS
	カテゴリ	コマンド実行
	ツール概要	リモートホスト上でコマンドを実行する
	攻撃時における想定利用例	BITSなどによりツールを送り込み、winrsを用いてツールをリモートから実行する ・接続元： WinRSコマンド実行元 ・接続先： WinRSコマンドによってアクセスされた端末
動作条件	権限	・接続元： 標準ユーザー ・接続先： 管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	5985/tcp (HTTP) 又は 5986/tcp (HTTPS)
	サービス	接続先： Windows Remote Management (WS-Management)
ログから得られる情報	標準設定	・WinRMの実行ログ ・実行履歴（Prefetch）
	追加設定	・実行履歴（Sysmon・監査ポリシー） ・Windowsフィルターリングプラットフォームを経由した、通信の記録
実行成功時に確認できる痕跡		・イベントログ「アプリケーションとサービス¥Microsoft¥Windows¥Windows Remote Management¥Operational」に、WinRSの実行が記録されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows 標準ユーザー ↓ OS：Windows 管理者ユーザー	接続元	イベントログ － セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥winrs.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4648**（明示的な資格情報を使用してログオンが試行されました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥winrs.exe"* ・**確認できる情報** ・**使用されたアカウント**: ***資格情報が使用されたアカウント*** -> ***アカウント名・アカウント ドメイン*** ・**接続先ホスト**: ***ターゲット サーバー*** -> ***ターゲット サーバー名*** ・**使用されたプロトコル**: ***ターゲット サーバー*** -> ***追加情報***（*"[プロトコル]/[ターゲット サーバー名]"*）	
			・***イベントID*** : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** : *"¥device¥harddiskvolume2¥windoows¥system32¥winrs.exe"* ・***ネットワーク情報*** -> ***方向*** : *"送信"* ・***ネットワーク情報*** -> ***宛先ポート*** : *"5985"*（HTTP）又は *"5986"*（HTTPS） ・***ネットワーク情報*** -> ***プロトコル*** : *"6"*（TCP） ・**確認できる情報** ・**接続先ホスト**: ***ネットワーク情報*** -> ***宛先アドレス***	
		イベントログ － Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"C:¥Windows¥System32¥winrs.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ※ **接続先ホスト**、**使用されたアカウント**、**実行されたコマンド**などが記録される ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		イベントログ － アプリケーションとサービス¥Microsoft¥Windows¥Windows Remote Management¥Operational	WinRSが実行されたことが記録されている	－
			イベントID : **80**（要求の処理） ・**確認できる情報** ・**接続先ホスト**: ***詳細***タブ -> ***EventData¥url*** ・**接続先ポート**: ***詳細***タブ -> ***EventData¥port***	
		実行履歴 － Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥WINRS.EXE-483CEB0F.pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** : ***Last Run Time***	－
	接続先	イベントログ － セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥winrshost.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[接続元から指定されたコマンド]"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	
			イベントID : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** : *"System"* ・***ネットワーク情報*** -> ***方向*** : *"着信"* ・***ネットワーク情報*** -> ***ソースポート*** : *"5985"*（HTTP）又は *"5986"*（HTTPS） ・***ネットワーク情報*** -> ***プロトコル*** : *"6"*（TCP） ・**確認できる情報** ・**接続元ホスト**: ***ネットワーク情報*** -> ***宛先アドレス***	

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows 標準ユーザー ↓ OS：Windows 管理者ユーザー （続）	接続先 （続）	イベントログ － Sysmon	***イベントID*** ： **1**（Process Create） **5**（Process Terminated） ・***Image*** ： *"C:¥Windows¥System32¥winrshost.exe"* **・確認できる情報** **・プロセスの開始・終了日時（UTC）** ： ***UtcTime*** **・プロセスのコマンドライン** ： ***CommandLine*** **・実行ユーザ名** ： ***User*** **・プロセスID** ： ***ProcessId***	必要
			イベントID ： **1**（Process Create） **5**（Process Terminated） ・***Image*** ： *"[接続元から指定されたコマンド]"* **・確認できる情報** **・プロセスの開始・終了日時（UTC）** ： ***UtcTime*** **・プロセスのコマンドライン** ： ***CommandLine*** **・実行ユーザ名** ： ***User*** **・プロセスID** ： ***ProcessId***	
		イベントログ － アプリケーションとサービス¥Microsoft¥Windows¥Windows Remote Management¥Operational	接続元のログに対応する、WinRSの処理が実行されたことが記録されている	－
			イベントID ： **81**（要求の処理）	
		実行履歴 － Prefetch	**ファイル名： C:¥Windows¥Prefetch¥WINRSHOST.EXE-ECE7169D.pf** **・確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） **・最終実行日時** ： ***Last Run Time***	－

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	WinRS経由で実行されたコマンドによる、ログが出力される可能性がある

3.2.8. atコマンド

<基本情報>

ツール	ツール名称	at
	カテゴリ	コマンド実行
	ツール概要	指定した時刻にタスクを実行する
	攻撃時における想定利用例	予めアプリケーションやスクリプトを、ユーザに気付かれないように配置し、任意のタイミングで実行する ・接続元： atコマンド実行元 ・接続先： atコマンドによってタスクが登録された端末
動作条件	権限	管理者ユーザー ※ リモートホストのタスクを設定する場合、ローカル側は標準ユーザーでも可
	対象OS	Windows 7 / Server 2008 Windows 8以降、及びServer 2012以降では、atコマンドは廃止となっている
	ドメインへの参加	不要
	通信プロトコル	445/tcp
	サービス	Task Scheduler
ログから得られる情報	標準設定	・接続元： 実行履歴（Prefetch） ・接続先： タスクスケジューラ イベントログにおけるタスクの作成・実行履歴
	追加設定	・実行履歴（Sysmon・監査ポリシー）
実行成功時に確認できる痕跡		・接続元： イベントログに以下のログがある場合、タスクが登録されたと考えられる ・イベントログ「セキュリティ」にat.exeのイベントID **4689**（プロセスが終了しました）が記録され、実行結果（戻り値）が"0x0"となっている ・接続先： イベントログに以下のログがある場合、タスクが実行されていると考えられる ・イベントログ「¥Microsoft¥Windows¥TaskScheduler¥Operational」にイベントID **106**（タスクが登録されました）が記録されている ・イベントログ「¥Microsoft¥Windows¥TaskScheduler¥Operational」にイベントID **200**（開始された操作）、**201**（操作が完了しました）が記録され、イベントID **201**における戻り値が成功となっている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows 7 ユーザー ↓ OS：Windows Server 2008 R2 管理者ユーザー	接続元 （Windows 7）	イベントログ － セキュリティ	***イベントID*** ： **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** ： *"C:¥Windows¥System32¥at.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** ： ログの日付 ・**プロセスを実行したユーザー名** ： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** ： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** ： ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値** ： ***プロセス情報*** -> ***終了状態***	必要
		イベントログ － Sysmon	***イベントID*** ： **1**（Process Create） **5**（Process Terminated） ・***Image*** ： *"C:¥Windows¥System32¥at.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** ： ***UtcTime*** ・**プロセスのコマンドライン** ： ***CommandLine*** ・**指定時刻、実行プロセス、対象ホスト** ： ***CommandLine*** ※ リモートホストに対して実行した場合、記録される ・**実行ユーザ名** ： ***User*** ・**プロセスID** ： ***ProcessId***	必要
		実行履歴 － Prefetch	**ファイル名： C:¥Windows¥Prefetch¥AT.EXE-BB02E639.pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** ： ***Last Run Time***	－
	接続先 （Windows Server 2008 R2）	イベントログ － セキュリティ	タスク登録が行われた場合、以下のログが出力される	必要
			イベントID ： **4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***オブジェクト*** -> ***オブジェクト名*** ： *"C:¥Windows¥Tasks¥[タスク名].job"* *"C:¥Windows¥System32¥Tasks¥[タスク名]"* ・**確認できる情報** ・**ハンドルID（他ログとの紐付けに使用する）** ： ***オブジェクト*** -> ***ハンドルID*** ・**ハンドルを要求したプロセスのプロセスID** ： ***プロセス情報*** -> ***プロセスID***（イベント**4688**で作成されたプロセスのIDと一致する） ・**処理内容** ： ***アクセス要求情報*** -> ***アクセス・アクセス理由***（*"WriteData (または AddFile)"* *"AppendData (または AddSubdirectoryまたは CreatePipeInstance)"*） ・**成否** ： ***キーワード***（*"成功の監査"*）	
			イベントID ： **4698**（スケジュールされたタスクが作成されました） ・***タスク情報*** -> ***タスク名*** ・**確認できる情報** ・**タスクの詳細** ： ***タスク情報*** 内、***タスク コンテンツ***。XML形式にて記述されている。 ・**実行トリガー** ： ***Triggers*** ・**優先度などの設定** ： ***Principals*** ・**実行内容** ： ***Actions***	
			タスクが実行された場合、以下のログが出力される。	
			イベントID ： **4688**（新しいプロセスが作成されました） ・***プロセス情報*** -> ***プロセス名*** ： *"C:¥Windows¥System32¥taskeng.exe"* ・**確認できる情報** ・**プロセスの開始日時** ： ログの日付 ・**プロセスを実行したユーザー名** ： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** ： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセスID** ： ***プロセス情報*** -> ***新しいプロセスID*** ※ 後に実行されるプロセスの親プロセスとなる ・**プロセス実行時の権限昇格の有無** ： ***プロセス情報*** -> ***トークン昇格*** の種類	必要
			イベントID ： **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** ： タスクで実行されるプロセス ・**確認できる情報** ・**プロセスの開始・終了日時** ： ログの日付 ・**プロセスを実行したユーザー名** ： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** ： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセスID** ： ***プロセス情報*** -> ***新しいプロセスID*** ※ タスク中で別の子プロセスが実行される場合、このプロセスが親プロセスとなる ・**プロセス実行時の権限昇格の有無**： ***プロセス情報*** -> ***トークン昇格*** の種類 ・**親プロセスID** ： ***プロセス情報*** -> ***クリエーター プロセスID*** ※ 親プロセスが、先に実行されているtaskeng.exeとなる ・**プロセスの戻り値** ： ***プロセス情報*** -> ***終了状態***	
			イベントID ： **4656**（オブジェクトに対するハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） ・***オブジェクト*** -> ***オブジェクト名*** ： *"C:¥Windows¥Tasks¥[タスク名].job"* ・***アクセス要求情報*** -> ***アクセス・アクセス理由*** ： *"WriteData (または AddFile)"*・*"AppendData (または AddSubdirectory または CreatePipeInstance)"* ・**確認できる情報** ・**ハンドルID** ： ***オブジェクト*** -> ***ハンドルID*** ※ 他のログとの紐付けに使用する	

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows 7 ユーザー ↓ OS：Windows Server 2008 R2 管理者ユーザー （続）	接続先 （Windows Server 2008 R2） （続）	イベントログ － Sysmon	タスク登録に関しては、有益な情報は出力されない。タスクが実行された際には、以下のログが登録される。	必要
			イベントID ： **1**（Process Create） **5**（Process Terminated） ・***ParentImage*** 名： *"C:¥Windows¥System32¥taskeng.exe"* **・確認できる情報** **・プロセスの開始・終了日時（UTC）**： ***UtcTime*** **・プロセスのコマンドライン** ： ***CommandLine*** ※ 実行プロセスや引数が記録される **・プロセスID** ： ***ProcessId*** ※ タスクにより実行されたプロセスに対する、実行・アクセス履歴の調査に使用できる	
		イベントログ － アプリケーションとサービスログ ¥Microsoft¥Windows ¥TaskScheduler ¥Operational	タスク登録が行われた場合、以下のログが出力される	－
			イベントID ： **106**（タスクが登録されました） **・確認できる情報** **・タスクを登録したユーザー** ： ***詳細***タブ -> *EventData¥UserContext* **・タスク名** ： ***詳細***タブ -> *EventData¥TaskName*	
			タスクが実行された場合、以下のログが出力される	
			イベントID ： **200**（開始された操作） **・確認できる情報** **・タスク名** ： ***詳細***タブ -> *EventData¥TaskName* **・実行されたコマンド** ： ***詳細***タブ -> *EventData¥ActionName* **・タスクのインスタンスID** ： ***詳細***タブ -> *EventData¥TaskInstanceId*	
			イベントID ： **129**（タスクのプロセスが作成されました） ・***詳細***タブ -> *EventData¥TaskName* が、開始イベント（イベントID **200**）に出力されている*TaskName*と一致する **・確認できる情報** **・実行されたプロセス** ： ***詳細***タブ -> *EventData¥Path* **・プロセスID** ： ***詳細***タブ -> *EventData¥ProcessID*※タスクにより実行されたプロセスに対する実行・アクセス履歴の調査に使用できる	
			イベントID ： **201**（操作が完了しました） ・***詳細***タブ -> *EventData¥InstanceId* が、開始イベント（イベントID **200**）に出力されている*TaskInstanceId*と一致する **・確認できる情報** **・タスク名** ： ***詳細***タブ -> *EventData¥TaskName* **・実行されたコマンド** ： ***詳細***タブ -> *EventData¥TaskActionName* **・実行結果（戻り値）** ： ***詳細***タブ -> *EventData¥ResultCode* ※ 戻り値の意味は、実行された処理により異なる	

<備考>

記載のもの以外で出力される可能性のあるイベントログ	タスクから呼び出されたコマンドに関連するログが出力される可能性がある

3.2.9. BITS

<基本情報>

ツール	ツール名称	BITS
	カテゴリ	コマンド実行
	ツール概要	バックグラウンドでファイルを送受信する（送受信の際、優先度などを設定することが可能）
	攻撃時における想定利用例	他の通信と比較して目立たない程度の帯域で、ファイルを送受信する ・接続元： BITSによってファイルを送信、受信しようとする端末 ・接続先： ファイルの送受信先
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	445/tcp
	サービス	Background Intelligent Transfer Service
ログから得られる情報	標準設定	・接続元： Background Intelligent Transfer Service の実行状態が変わることで、BITSの使用を判断出来る可能性がある ※ 但し、BITSが既に動作している場合は判断できない ・接続先： 有益な情報は記録されない
	追加設定	・接続元： BITSにより作成される一時ファイル *"BITF[ランダム数字].tmp"* に対する書き込みが記録される ・接続先： 有益な情報は記録されない
実行成功時に確認できる痕跡		イベントログに以下のログがある場合、ファイルの転送が行われたと考えられる ・イベントログ「アプリケーションとサービスログ¥Microsoft¥Windows¥Bits-Client」にイベントID: **60**が記録されており、状態コードが"0x0"となっている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows ユーザー	接続元	イベントログ − セキュリティ	***イベントID*** : **4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***オブジェクト*** -> ***オブジェクト名*** : *"[ファイルが作成されたパス]¥BITF[ランダム数字].tmp"* ※ "BITF"で名前が始まる一時ファイルが作成されることから、BITSによるファイル転送が発生したことが分かる **・確認できる情報** ・**ハンドルID（他ログとの紐付けに使用する）**： ***オブジェクト*** -> ***ハンドルID*** ・**ハンドルを要求したプロセスのプロセスID**： ***プロセス情報*** -> ***プロセスID***（イベント**4688**で作成されたプロセスのIDと一致する） ・**処理内容**： ***アクセス要求情報*** -> ***アクセス・アクセス理由***（*"WriteData (または AddFile)"*・*"AppendData (または AddSubdirectoryまたは CreatePipeInstance)"*・*"DELETE"*） ・**成否**： ***キーワード***（*"成功の監査"*）	必要
		イベントログ − Sysmon	***イベントID*** : **2**（File creation time changed） ・***Image*** 名： *"C:¥Windows¥system32¥svchost.exe"* **・確認できる情報** ・**タイムスタンプが変更された一時ファイル**： *"[ファイルが作成されたパス]¥BITF[ランダム数字].tmp"*	必要
		イベントログ − システム	***イベントID*** : **7036**（サービスの状態が移行しました） ・***詳細***タブ -> ***System¥Provider¥Name*** が *"Service Control Manager"* となっている ・***詳細***タブ -> ***EventData¥param1*** が *"Background Intelligent Transfer Service"* となっている **・確認できる情報** ・**サービスの実行**： ***詳細***タブ -> ***EventData¥param2***（*"実行中"*）	−
			・備考 ・端末を最後に起動してから、BITSを利用する処理を実行したことがある場合、ログが出力されない可能性がある （例えば、Windows Updateで使用されているため、Windows Updateでファイルをダウンロードした場合は出力されない可能性がある）	
		イベントログ − アプリケーションとサービスログ ¥Microsoft¥Windows ¥Bits-Client	***イベントID*** : **60** **・確認できる情報** ・**対象ファイル**： ***詳細***タブ -> ***ventData¥url*** ・**成否**： ***全般***タブ -> ***状態コード***	−
		実行履歴 − レジストリ	**レジストリエントリ：** HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥BITS **・確認できる情報** ・**サービスの状態**： ***StateIndex***	−
			・備考 ・BITSの状態が「実行中」となることで変動する ・コマンド実行時にBITSが既に実行状態であった場合、値が変動しない	
	接続先	イベントログ − セキュリティ	***イベントID*** : **5145**（クライアントに必要なアクセスを付与できるかどうかについて、ネットワーク共有オブジェクトがチェックされました） ・***ネットワーク情報*** -> ***送信元アドレス*** : *"[接続元ホスト]"* ・***ネットワーク情報*** -> ***ソースアドレス*** : *"[接続元ポート]"* **・確認できる情報** ・**共有名**： ***共有情報*** -> ***共有名*** ・**共有パス**： ***共有情報*** -> ***共有パス*** ・**配置されたファイル名**： ***共有情報*** -> ***相対ターゲット名***	必要

<備考>

記載のもの以外で出力される可能性のあるイベントログ	・オブジェクトの読み取りに対する監査を実施した場合、転送されたファイルに対する読み取りが記録される

3.3.1. PwDump7

<基本情報>

ツール	ツール名称	PwDump7
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	システム内のパスワードハッシュー覧を表示する
	攻撃時における想定利用例	取得したハッシュ情報を用い、他の端末に対するログオン認証をおこなう
動作条件	権限	管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・実行履歴（Sysmon・監査ポリシー）
実行成功時に確認できる痕跡		イベントログ、実行履歴等では判断できない

凡例
・**取得出来る情報**
・**イベントID・項目名**
・***フィールド名***
・*"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末（Windows）	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(PwDump7.exe)]"* **・確認ポイント** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体(PwDump7.exe)]"* **・確認できる情報** ・**プロセスの開始・終了日時（UTC）**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 使用されたオプションが引数として記録される ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名：C:¥Windows¥Prefetch¥[実行ファイル（PWDUMP7.EXE）]-[文字列].pf** **・確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**: ***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.3.2. PWDumpX

<基本情報>

ツール	ツール名称	PWDumpX
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	リモートホストからパスワードハッシュを取得する
	攻撃時における想定利用例	取得したハッシュを用いて、pass-the-hashなどの攻撃をおこなう ・接続元： PWDumpX実行元 ・接続先： PWDumpXによってログインされた先
動作条件	権限	・接続元： 標準ユーザー ・接続先： 管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	135/tcp, 445/tcp
	サービス	–
ログから得られる情報	標準設定	・両ホスト： 実行履歴（Prefetch） ・接続先： PWDumpXサービスがインストールされ、実行されたことが記録される
	追加設定	・接続元から接続先へ、PWDumpXサービスが送信され、実行されたことが記録される ・ハッシュ情報の作成・受領に、テキストファイルが利用されていることが記録される
実行成功時に確認できる痕跡		・接続元： "[検体のパス]¥[宛先アドレス]-PWHashes.txt"が作成されている場合、実行が成功したものと考えられる

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows 管理者ユーザー	接続元	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（PWDumpX.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			一時ファイルが作成される	
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（PWDumpX.exe）]"* ・***オブジェクト*** -> ***オブジェクト名*** : *"[検体のパス]¥[宛先アドレス]-PWHashes.txt"* ※ 複数回上記ファイルに対して書き込みを実施する	
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（PWDumpX.exe）]"* ・***オブジェクト*** -> ***オブジェクト名*** : *"[検体のパス]¥[宛先アドレス]-PWHashes.txt.Obfuscated"* ・**確認できる情報** ・**ハンドルID** : ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ※ 複数回上記ファイルに対して書き込みを実施する	
			一時ファイルが削除される	
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（PWDumpX.exe）]"* ・***オブジェクト*** -> ***オブジェクト名*** : *"[検体のパス]¥[宛先アドレス]-PWHashes.txt.Obfuscated"* ・**確認できる情報** ・**ハンドルID**： ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容**： ***アクセス要求情報*** -> ***アクセス***（*"DELETE"*）	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体（PWDumpX.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ※ 接続先ホストや使用されたアカウントが引数に入る ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名： C:¥Windows¥Prefetch¥[検体（PWDUMPX.EXE）]-[検体].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** : ***Last Run Time***	–
	接続先	イベントログ セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（DumpSvc.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **5145**（クライアントに必要なアクセスを付与できるかどうかについて、ネットワーク共有オブジェクトがチェックされました） ・***ネットワーク情報*** -> ***送信元アドレス*** : *"[接続元]"* ・***共有情報*** -> ***共有名*** : *"¥¥*¥ADMIN$"* ・***共有情報*** -> ***相対ターゲット名*** : *"system32¥DumpSvc.exe"・"system32¥DumpExt.dll"*	
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥lsass.exe"* ・***オブジェクト*** -> ***オブジェクト名*** : *"C:¥Windows¥System32¥PWHashes.txt"* *"C:¥Windows¥System32¥PWHashes.txt.Obfuscated"* ・**確認できる情報** ・**ハンドルID（他ログとの紐付けに使用する）**： ***オブジェクト*** -> ***ハンドル ID*** ※ 複数回上記ファイルに対して書き込みを実施する	
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥lsass.exe"* ・***オブジェクト*** -> ***オブジェクト名*** : *"C:¥Windows¥System32¥PWHashes.txt.Obfuscated"・"C:¥Windows¥System32¥PWHashes.txt"* *"C:¥Windows¥System32¥DumpExt.dll"・"C:¥Windows¥System32¥DumpSvc.exe"* ・**確認できる情報** ・**ハンドルID**： ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容**： ***アクセス要求情報*** -> ***アクセス***（*"DELETE"*）	

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加 設定
OS：Windows ユーザー ↓ OS：Windows 管理者ユーザー （続）	接続先 （続）	イベントログ － Sysmon	***イベントID*** ： **1**（Process Create） **5**（Process Terminated） ・***Image*** ： *"C:¥Windows¥System32¥DumpSvc.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** ： ***UtcTime*** ・**プロセスのコマンドライン** ： ***CommandLine*** ・**実行ユーザ名** ： ***User*** ・**プロセスID** ： ***ProcessId***	必要
			イベントID ： **8**（CreateRemoteThread detected:） ・***Image*** ： *"C:¥Windows¥System32¥DumpSvc.exe"* ・***TargetImage*** ： *"C:¥Windows¥System32¥lsass.exe"*	
		イベントログ － システム	***イベントID*** ： **7045**（サービスがシステムにインストールされました） ・***サービス名*** ： （*"PWDumpX Service"*） ・***サービス ファイル名*** ：（*"%windir%¥system32¥DumpSvc.exe"*）	－
			イベントID ： **7036**（サービスの状態が移行しました） ・***サービス名*** ： （*"PWDumpX Service"*） ※ サービス *"PWDumpX Service"* が、リモートプロセス実行前に *"実行中"* となり、実行後に *"停止"* となる	
		実行履歴 Prefetch	**ファイル名 ： C:¥Windows¥Prefetch¥DUMPSVC.EXE-DB3A90FA.pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** ： ***Last Run Time***	－

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	－

3.3.3. Quarks PwDump

<基本情報>

ツール	ツール名称	Quarks PwDump
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	ローカル・ドメインアカウントのNTLMハッシュや、キャッシュされたドメインパスワードを取得する 端末内の情報に加え、NTDS.DITファイルを指定して解析することも可能
	攻撃時における想定利用例	取得したハッシュ情報を用い、他の端末に対するログオン認証をおこなう
動作条件	権限	管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・実行履歴（Sysmon・監査ポリシー） ・一時ファイル（*"SAM-[ランダム数字].dmp"*）が作成されたことの記録
実行成功時に確認できる痕跡		・一時ファイル（*"SAM-[ランダム数字].dmp"*）が作成され、削除されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 (Windows)	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（QuarksPwDump.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態*** ※ 成功の場合は"0x0"、失敗の場合はそれ以外の値となる	必要
			イベントID : **4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（QuarksPwDump.exe）]"* ・**確認できる情報** ・**対象ファイル**: ***オブジェクト*** -> ***オブジェクト名***（*"C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥SAM-[ランダム数字].dmp"*） ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス***（*"WriteData（または AddFile）"*）	
			イベントID : **4656**（オブジェクトへのハンドルが要求されました） **4660**（ファイルが削除されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（QuarksPwDump.exe）]"* ・***プロセス情報*** -> ***プロセスID*** : *"[検体のプロセスID]"* ・***オブジェクト*** -> ***オブジェクト名*** : *"C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥SAM-[ランダム数字].dmp"* ・**確認できる情報** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**要求された処理**: ***アクセス要求情報*** -> ***アクセス・アクセス理由***（*"DELETE"*） ・**成否**: ***キーワード***（*"成功の監査"*）	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体（QuarksPwDump.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 指定されたオプション（**取得されたパスワードの種類**）が引数に記録される ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥[検体（QUARKSPWDUMP.EXE）]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** : ***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.3.4. Mimikatz（パスワードハッシュ入手）

<基本情報>

ツール	ツール名称	mimikatz ＞ sekurlsa::logonpasswords mimikatz ＞ lsadump::sam
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	記憶された認証情報を搾取
	攻撃時における想定利用例	パスワードを取得したり、ドメインAdministrator権限に昇格する際に実行する
動作条件	権限	管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・実行履歴（Sysmon・監査ポリシー）
実行成功時に確認できる痕跡		イベントログ、実行履歴等では判断できない

凡例
・**取得出来る情報**
・**イベントID・項目名**
・***フィールド名***
・*"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 （Windows）	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（mimikatz.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体（mimikatz.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 使用されたオプションが引数として記録される ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名：C:¥Windows¥Prefetch¥[実行ファイル（MIMIKATZ.EXE）]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**: ***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.3.5. Mimikatz (チケット入手)

<基本情報>

ツール	ツール名称	mimikatz > sekurlsa::tickets
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	端末が全てのセッションのチケットを取得する
	攻撃時における想定利用例	リモートでコマンドを実行するためにチケットを取得する
動作条件	権限	管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴(Prefetch)
	追加設定	・実行履歴(Sysmon・監査ポリシー) ※ チケットを出力したファイルが生成されたことが記録される
実行成功時に確認できる痕跡		・チケットを出力したファイルが生成された場合、処理が成功したものと考えられる

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 (Windows)	イベントログ – セキュリティ	***イベントID*** : **4688**(新しいプロセスが作成されました) **4689**(プロセスが終了しました) ・***プロセス情報*** -> ***プロセス名*** : *"[検体(mimikatz.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
			全チケットを処理するまで以下**イベントID:4656、4663、4658**の処理を繰り返す	
			イベントID : **4656**(オブジェクトに対するハンドルが要求されました) ・***プロセス情報*** -> ***プロセス名*** : *"[検体(mimikatz.exe)]"* ・**確認できる情報** ・**対象ファイル**: ***オブジェクト*** -> ***オブジェクト名*** (*"[チケットファイル名]"*) ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス*** (*"READ_CONTROL"、"SYNCHRONIZE"、"WriteData (または AddFile)"、"AppendData (または AddSubdirectory または CreatePipeInstance)"、"WriteEA"、"ReadAttributes"、"WriteAttributes"*)	
			イベントID : **4663**(オブジェクトへのアクセスが試行されました) ・**確認できる情報** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス*** (*"WriteData (または AddFile)"、"AppendData (または AddSubdirectory または CreatePipeInstance)"*)	
			イベントID : **4658**(オブジェクトに対するハンドルが閉じました) ・**確認できる情報** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID***	
		イベントログ – Sysmon	***イベントID*** : **1** (Process Create) **5** (Process Terminated) ・***Image*** : *"[検体(mimikatz.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 使用されたオプションが引数として記録される (イベントID 1に記録される) ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥[実行ファイル(MIMIKATZ.EXE)]–[文字列].pf** ・**確認できる情報** (ツールを利用して下記を確認できる ツール:WinPrefetchView) ・**最終実行日時**: ***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.3.6. WCE (Windows Credentials Editor)

<基本情報>

ツール	ツール名称	WCE (Windows Credentials Editor)
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	ログイン端末のメモリ内に存在する、パスワードハッシュ情報を取得する
	攻撃時における想定利用例	取得したハッシュ情報を用いて、pass-the-hashなどの攻撃を実施する
動作条件	権限	管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴(Prefetch)
	追加設定	・検体が実行されたこと、及び検体実行時に使用されたオプション(Sysmon) ・検体による、lsass.exeの参照(Sysmon) ・ファイルの作成・削除(監査ポリシー)
実行成功時に確認できる痕跡		・*"C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥wceaux.dll"*ファイルが作成、削除されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 (Windows)	イベントログ – セキュリティ	***イベントID*** : **4688**(新しいプロセスが作成されました) **4689**(プロセスが終了しました) ・***プロセス情報*** -> ***プロセス名*** : *"[検体(wce.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4656**(オブジェクトへのハンドルが要求されました) **4663**(オブジェクトへのアクセスが試行されました) **4658**(オブジェクトに対するハンドルが閉じました) ・***プロセス情報*** -> ***プロセス名*** : *"[検体(wce.exe)]"* ・**確認できる情報** ・**対象ファイル**: ***オブジェクト*** -> ***オブジェクト名*** : *("C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥wceaux.dll")* ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス*** (*"READ_CONTROL"、"SYNCHRONIZE"、"ReadData (または ListDirectory)"、"WriteData (またはAddFile)"、"AppendData (または AddSubdirectory または CreatePipeInstance)"、"ReadEA"、"WriteEA"、"ReadAttributes"、"WriteAttributes"*) ・**成否**: ***キーワード*** (*"成功の監査"*)	
			イベントID : **4656**(オブジェクトに対するハンドルが要求されました) **4660**(オブジェクトが削除されました) **4658**(オブジェクトに対するハンドルが閉じました) ・***プロセス情報*** -> ***プロセス名*** : *"[検体(wce.exe)]"* ・**確認できる情報** ・**対象ファイル**: ***オブジェクト*** -> ***オブジェクト名*** : *("C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥wceaux.dll")* ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス*** (*"DELETE"*) ・**成否**: ***キーワード*** (*"成功の監査"*)	
		イベントログ – Sysmon	***イベントID*** : **1** (Process Create) **5** (Process Terminated) ・***Image*** : *"[検体(wce.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
			イベントID : **8** (CreateRemoteThread detected) ・***Image*** : *"[検体(wce.exe)]"* ・***TargetImage*** : *"C:¥Windows¥System32¥lsass.exe"* ・**確認できる情報** ・**プロセスの開始日時(UTC)** : ***UtcTime***	
		実行履歴 – Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥[検体(WCE.EXE)]-[文字列].pf** ・**確認できる情報** (ツールを利用して下記を確認できる ツール:WinPrefetchView) ・**最終実行日時** : ***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.3.7. gsecdump

<基本情報>

ツール	ツール名称	gsecdump
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	SAM/ADやログオンセッションから、ハッシュを抽出するツール
	攻撃時における想定利用例	取得したハッシュ情報を用い、他の端末に対してログオンする
動作条件	権限	管理者ユーザー
	対象OS	Windows 32ビット (64ビット環境で動作する検体は未確認)
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴(Prefetch)
	追加設定	・実行履歴(Sysmon・監査ポリシー)
実行成功時に確認できる痕跡		イベントログ、実行履歴等では判断できない

凡例
・**取得出来る情報**
・**イベントID・項目名**
・***フィールド名***
・*"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 (Windows)	イベントログ – セキュリティ	***イベントID*** : **4688** (新しいプロセスが作成されました) **4689** (プロセスが終了しました) ・***プロセス情報*** -> ***プロセス名*** : *"[検体]"* ・**確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
		イベントログ – Sysmon	***イベントID*** : **1** (Process Create) **5** (Process Terminated) ・***Image*** : *"[検体]"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 使用されたオプションが引数として記録される ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥[検体(GSECDUMP.EXE)]-[文字列].pf** ・**確認できる情報** (ツールを利用して下記を確認できる ツール:WinPrefetchView) ・**最終実行日時**: ***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.3.8. lslsass

<基本情報>

ツール	ツール名称	lslsass
	カテゴリ	パスワード、ハッシュ入手
	ツール概要	lsassプロセスから、有効なログオンセッションのパスワードハッシュを取得する
	攻撃時における想定利用例	取得したハッシュ情報を用い、他の端末に対するログオン認証をおこなう
動作条件	権限	管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・実行履歴（Sysmon・アクセス履歴）
実行成功時に確認できる痕跡		イベントログ、実行履歴等では判断できない

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末（Windows）	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(lslsass[ビット数].exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウントドメイン*** ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体(lslsass[ビット数].exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 使用されたオプションが引数として記録される ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 Prefetch	**ファイル名：C:¥Windows¥Prefetch¥[実行ファイル（LSLSASS[ビット数].EXE）]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**: ***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	

3.3.9. Find-GPOPasswords.ps1

<基本情報>

ツール	ツール名称	Find-GPOPasswords.ps1
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	グループポリシーのファイルにパスワードの記載がある場合、それを取得する
	攻撃時における想定利用例	取得したパスワードを用いて、他ホストへの侵入などを試みる（Active Directory上で実行する）
動作条件	権限	管理者ユーザー
	対象OS	Windows Server 本調査はドメインコントローラー上で実施
	ドメインへの参加	要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch） ※ 通常時からPowerShellを使用している場合は参考にならない
	追加設定	・PowerShellを起動したことが記録される ・パスワードをダンプしたファイル（GPPDataReport-[ドメイン名]-[日時].csv）を出力したことが記録される
実行成功時に確認できる痕跡		・パスワードをダンプした結果のファイル（GPPDataReport-[ドメイン名]-[日時].csv）が出力されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	Active Directory ドメインコントローラー (Windows Server)	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4656**（オブジェクトに対するハンドルが要求されました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**対象ファイル** : ***オブジェクト*** -> ***オブジェクト名*** : *("C:¥Users¥[ユーザー名]¥AppData¥Local¥Microsoft¥Windows¥SchCache¥[ドメインコントローラーFQDN].sch")* ・**ハンドルID** : ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容** : ***アクセス要求情報*** -> ***アクセス*** (*"READ_CONTROL","SYNCHRONIZE","WriteData (または AddFile)","AppendData (またはAddSubdirectory または CreatePipeInstance)","WriteEA","ReadAttributes","WriteAttributes"*)	
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**ハンドルID** : ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容** : ***アクセス要求情報*** -> ***アクセス*** (*"WriteData (または AddFile)"、"AppendData (または AddSubdirectory または CreatePipeInstance)"*)	
			イベントID : **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**ハンドルID** : ***オブジェクト*** 内、***ハンドル ID*** ※ 先に出力される、イベント**4663**で記録される***ハンドルID***と同じ	
			イベントID : **4656**（オブジェクトに対するハンドルが要求されました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**対象ファイル** : ***オブジェクト*** -> ***オブジェクト名*** : *("GPPDataReport-[ドメイン名]-[日時].csv")* ・**ハンドルID** : ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容** : ***アクセス要求情報*** -> ***アクセス*** (*"READ_CONTROL","SYNCHRONIZE","WriteData (または AddFile)","AppendData (またはAddSubdirectory または CreatePipeInstance)","WriteEA","ReadAttributes","WriteAttributes"*)	
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**対象ファイル** : ***オブジェクト*** -> ***オブジェクト名*** : *("GPPDataReport-[ドメイン名]-[日時].csv")* ・**ハンドルID** : ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容** : ***アクセス要求情報*** -> ***アクセス*** (*"WriteData (または AddFile)"、"AppendData (または AddSubdirectory または CreatePipeInstance)"*)	
			イベントID : **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**ハンドルID** : ***オブジェクト*** -> ***ハンドル ID*** ※ 先に出力される、イベント**4663**で記録される***ハンドルID***と同じ	
			イベントID : **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**プロセスの終了日時** : ログの日付 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"C:¥Windows¥System32¥Windows PowerShell¥v1.0¥powershell.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** : ***UtcTime*** ・**実行ユーザー名** : ***User*** ・**プロセスID** : ***ProcessId***	必要

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.3.10. Mail PassView

<基本情報>

ツール	ツール名称	Mail PassView
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	端末上のメールクライアントの設定に保存されているアカウント情報を抽出する
	攻撃時における 想定利用例	本ツールを使用して取得した情報を用いて、メールを送受信する 同じユーザ名・パスワードが他所でも使用されている場合、利用される可能性がある
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから 得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・実行履歴（Sysmon・監査ポリシー）
実行成功時に確認できる痕跡		イベントログ、実行履歴等では判断できない　※ 抽出したパスワードが保存されている場合は、成功したと判断できる 保存されている情報に対するパスワード保護がある場合などは本検体で解読できないため、実行の成功と情報収集の成功は必ずしも一致しない

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	**ログの生成場所**	**ログ種別・名称**	**取得情報の詳細**	**追加 設定**
–	端末 （Windows）	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***新しいプロセス名*** : *"[検体(mailpv.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時** :　ログの日付 ・**プロセスを実行したユーザー名** :　***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザのドメイン** :　***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**:　***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** :　***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） **4656**（オブジェクトへのハンドルが要求されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(mailpv.exe)]"* ・**確認できる情報** ・**対象ファイル**: ***オブジェクト*** -> ***オブジェクト名*** : *"[引数で指定したファイル]"* ・**ハンドルID**:　***オブジェクト*** -> ***ハンドル ID***　※ 他ログとの紐付けに使用する ・**処理内容**:　***アクセス要求情報*** -> ***アクセス***（*"WriteData (または AddFile)"*）	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体(mailpv.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**:　***UtcTime*** ・**プロセスのコマンドライン**:　***CommandLine***　※ 出力先となるテキストファイル名を、引数で指定する ・**実行ユーザー名**:　***User*** ・**プロセスID**:　***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥[検体(MAILPV.EXE)]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**:　***Last Run Time***	–

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	Mail PassViewが対応しているメールクライアントのプロファイルに、読み取りアクセスが発生する可能性がある

3.3.11. WebBrowserPassView

<基本情報>

ツール	ツール名称	WebBrowserPassView
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	端末のWebブラウザに保存されているユーザー名・パスワードを抽出する
	攻撃時における想定利用例	イントラネットや外部サービスを利用する際に入力するアカウント情報を抽出し、利用する
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・実行履歴（Sysmon・監査ポリシー）
実行成功時に確認できる痕跡		イベントログ、実行履歴等では判断できない　※ 抽出したパスワードが保存されている場合は、成功したと判断できる 保存されている情報に対するパスワード保護がある場合などは本検体で解読できないため、実行の成功と情報収集の成功は必ずしも一致しない

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 （Windows）	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(WebBrowserPassView.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時** :　ログの日付 ・**プロセスを実行したユーザー名** :　***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザのドメイン** :　***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**:　***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** :　***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） **4656**（オブジェクトへのハンドルが要求されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(WebBrowserPassView.exe)]"* ・**確認できる情報** ・**対象ファイル**: ***オブジェクト*** -> ***オブジェクト名*** : *"[引数で指定したファイル]"* ・**ハンドルID**:　***オブジェクト*** -> ***ハンドル ID***　※ 他ログとの紐付けに使用する ・**処理内容**:　***アクセス要求情報*** -> ***アクセス***（*"WriteData (または AddFile)"*）	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体(WebBrowserPassView.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**:　***UtcTime*** ・**プロセスのコマンドライン**:　***CommandLine***　※ 出力先となるテキストファイル名を、引数で指定する ・**実行ユーザー名**:　***User*** ・**プロセスID**:　***ProcessId***	必要
		実行履歴 Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥[検体(WEBBROWSERPASSVIEW.EXE)]–[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**:　***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	・WebBrowserPassViewが対応しているブラウザがシステム上にインストールされている場合、各ブラウザのプロファイルに対する読み取りが発生する ・最新のWebBrowserPassViewはGUI用であり、実行後に設定を"[検体名].cfg"に保存する特徴がある

3.3.12. Remote Desktop PassView

<基本情報>

ツール	ツール名称	Remote Desktop PassView
	カテゴリ	パスワード、ハッシュの入手
	ツール概要	端末上のRDPの設定に保存されているアカウント情報を抽出する
	攻撃時における想定利用例	リモートデスクトップの設定ファイル内に保存されているパスワードを抽出し、そのパスワードを用いて他のホストへログインする
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・実行履歴（Sysmon・監査ポリシー）
実行成功時に確認できる痕跡		イベントログ、実行履歴等では判断できない　※ 抽出したパスワードが保存されている場合は、成功したと判断できる

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 (Windows)	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(rdpv.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4656**（オブジェクトに対するハンドルが要求されました） ・***プロセス情報*** 内、***プロセス名*** : *"[検体(rdpv.exe)]"* ・**確認できる情報** ・**対象ファイル**: ***オブジェクト*** -> ***オブジェクト名*** :*("対象検体のファイル名は検体に引数で指定")* ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス*** (*"READ_CONTROL","SYNCHRONIZE","WriteData (または AddFile)","AppendData (または AddSubdirectory または CreatePipeInstance)","WriteEA","ReadAttributes","WriteAttributes"*)	
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） ・**確認できる情報** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス*** (*"WriteData (または AddFile)"、"AppendData (または AddSubdirectory または CreatePipeInstance)"*)	
			イベントID : **4658**（オブジェクトに対するハンドルが閉じました） ・**確認できる情報** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID***	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体(rdpv.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 使用されたオプションが引数として記録される（イベントID 1に記録される） ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名： C:¥Windows¥Prefetch¥[実行ファイル（RDPV.EXE）]-[文字列].pf** ・**確認できる情報** （ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**: ***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.4.1. Htran

<基本情報>

ツール	ツール名称	Htran
	カテゴリ	通信の不正中継
	ツール概要	TCPセッションを作成し、他ポートの通信をトンネリングさせる
	攻撃時における想定利用例	ファイアウォールなどで許可されているポートを経由して、許可されていないポートの通信を通過させる ・接続元： Htran実行元 ・接続先： Htranによって接続した端末
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	任意のTCPポート
	サービス	–
ログから得られる情報	標準設定	・接続元： 実行履歴（Prefetch） ・接続先： トンネル経由で実行された通信を使用するアプリケーションに依存する
	追加設定	・接続元： 検体の実行 （プロセス追跡の監査） トンネルホスト（攻撃者）・トンネル先ホスト（接続先）との通信有無 （オブジェクトアクセスの監査） ・接続先： トンネル経由で実行された通信を使用するアプリケーションに依存する
実行成功時に確認できる痕跡		・接続元： イベントログに以下のログがある場合、通信した可能性がある ・イベントログ「セキュリティ」にイベントID 5156でトンネルホスト・トンネル先ホストとそれぞれ通信したことが記録されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

※ 本資料では「Htranが実行された端末」を「接続元」、「Htranを経由して接続された端末」を「接続先」とする。

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows ユーザー	接続元	イベントログ – セキュリティ	***イベントID*** ： **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** ： *"[検体]"* **・確認できる情報** ・**プロセスの開始・終了日時** ： ログの日付 ・**プロセスを実行したユーザー名** ： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** ： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** ： ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** ： ***プロセス情報*** -> ***終了状態***	必要
			「接続元」ホストから、2箇所に対する通信が発生する	
			イベントID ： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** ： *"[検体]"* ・***ネットワーク情報*** -> ***方向*** ： *"送信"* ・***ネットワーク情報*** -> ***送信元 アドレス*** ： *"[接続元ホストのIPアドレス]"* ・***ネットワーク情報*** -> ***プロトコル*** ： *"6"*（TCP） **・確認できる情報** ・**トンネルホスト**： ***宛先アドレス*** ・**トンネルに利用されたポート**： ***宛先ポート***	
			イベントID ： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** ： *"[検体]"* ・***ネットワーク情報*** -> ***方向*** ： *"送信"* ・***ネットワーク情報*** -> ***送信元 アドレス*** ： *"[接続元ホストのIPアドレス]"* ・***ネットワーク情報*** -> ***プロトコル*** ： *"6"*（TCP） **・確認できる情報** ・**トンネルホスト**： ***宛先アドレス*** ・**トンネルに利用されたポート**： ***宛先ポート***	
		イベントログ – Sysmon	***イベントID*** ： **1**（Process Create） **5**（Process Terminated） ・***Image*** ： *"[検体]"* **・確認できる情報** ・**プロセスの開始・終了日時（UTC）** ： ***UtcTime*** ・**プロセスのコマンドライン** ： ***CommandLine*** ・**指定時刻、実行プロセス、対象ホスト** ： ***CommandLine*** ※ 引数に、**トンネルホスト（攻撃者）のIPアドレス及びポート番号** **トンネル先となるホスト（接続先）のIPアドレス及びポート番号**が記録される ・**実行ユーザ名** ： ***User*** ・**プロセスID** ： ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名： C:¥Windows¥Prefetch¥[検体]-[文字列].pf** **・確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** ： ***Last Run Time***	–
	接続先	各種ログ	トンネル経由で実行された通信を使用するアプリケーションによって複数のログが記録される可能性がある Htran経由で多く使用されるものとして、リモートデスクトップ（RDP）がある。この場合はトンネル先である「接続先」に、Htranが実行された「接続元」を接続元IPアドレスとする、宛先ポート 3389/tcp の通信が記録される ※ RDPのログ詳細については、別途RDPの資料を参照	必要

<備考>

記載のもの以外で出力される可能性のあるイベントログ	HTTPプロキシ対応版が使用された場合、プロキシにHTTPS通信が記録される HTTPSのため、SSLをデコード出来ない場合、CONNECTメソッドのみが記録される

3.4.2. Fake wpad

<基本情報>

ツール	ツール名称	Fake wpad
	カテゴリ	通信の不正中継
	ツール概要	wpadサーバとして動作し、通信内容を取得・変更する
	攻撃時における想定利用例	ユーザーに気付かれないように、攻撃者のサイトを埋め込むよう、レスポンスを改変する ・接続元： 偽装されたwpadファイルを受信する ・接続先： 偽装されたwpadファイルを接続元に送信することで、接続元のプロキシとなる
	参考情報	https://www.jpcert.or.jp/present/2015/20151028_codeblue_ja.pdf
動作条件	権限	・接続先（wpadサーバ）： 80/tcp及び8888/tcpをlistenする。Windowsファイアウォールで受信を許可するなどの変更が必要なため、管理者権限が必要 ・接続元： 標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	80/tcp、8888/tcp
	サービス	–
ログから得られる情報	標準設定	・接続元： 最後に取得されたプロキシ設定（レジストリ）が記録される ※ 通常時からwpadを使用している場合は区別出来ない ・接続先： 実行履歴（Prefetch）
	追加設定	・接続元： 検体を実行しているホストに対して、80/tcp及び8888/tcpで通信していることが記録される（オブジェクトアクセスの監査） wpad.datのキャッシュが作成されたことが記録される（オブジェクトアクセスの監査） ・接続先： 80/tcp及び8888/tcpをリッスンしたことが記録される（オブジェクトアクセスの監査） wpad.datや、プロキシのログであるproxy.logに対するハンドルの要求が記録される（オブジェクトアクセスの監査）
実行成功時に確認できる痕跡		・接続元： 本来プロキシやHTTPサーバーで無いはずのホストと、80/tcp及び8888/tcpによる通信をおこなっている ・接続先： 本来プロキシやHTTPサーバーで無いはずのホストが、80/tcp及び8888/tcpをリッスンしている wpad.dat、proxy.logが作成されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー → OS：Windows ユーザー	接続元	イベントログ – セキュリティ	wpadを取得する際に、以下が記録される（以下はInternet Explorerの例であるため、他のブラウザでは保存場所や挙動が異なる） なお、イベントID **4656・4663・4658** は、wpadを使用している場合に記録されるため、wpadを利用している場合は不正なものと区別がつかない	必要
			イベントID： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名***： *"¥device¥harddiskvolume2¥program files¥internet explorer¥iexplore.exe"* ・***ネットワーク情報*** -> ***方向***： *"送信"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル***： *"80"・"6"*（TCP） **・確認できる情報** ・**接続したホスト**： ***ネットワーク情報*** -> ***宛先アドレス***	
			イベントID： **4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） **・確認できる情報** ・**対象のファイル**： ***オブジェクト*** -> ***オブジェクト名***（*"C:¥Users¥[ユーザー名]¥AppData¥Local¥Microsoft¥Windows¥Temporary Internet Files¥Content.IE5¥[文字列]¥wpad[1].htm"*） ・**ハンドルID**： ***オブジェクト*** -> ***ハンドルID*** ※ 他ログとの紐付けに使用する ・**処理内容**： ***アクセス要求情報*** -> ***アクセス***（*"WriteAttributes"・"WriteData (またはAddFile)"・"AppendData (または AddSubdirectory または CreatePipeInstance"*） ・**成否**： ***キーワード***（*"成功の監査"*）	
			プロキシが利用されると、以下が記録される wpad.dat 内で当該ホストをプロキシとして使用しない条件が書かれている場合、***宛先アドレス*** は実際に接続する先のホストとなる	
			イベントID： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名***： *"¥device¥harddiskvolume2¥program files¥internet explorer¥iexplore.exe"* ・***ネットワーク情報*** -> ***方向***： *"送信"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル***： *"8888"・"6"*（TCP） **・確認できる情報** ・**プロキシとして利用されたホスト**： ***ネットワーク情報*** -> ***宛先アドレス***	
		アクセス履歴 – レジストリ	**レジストリエントリ**： HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Internet Settings¥Connections¥SavedLegacySettings HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Internet Settings¥Connections¥DefaultConnectionSettings **・確認できる情報** ・**最後に取得されたプロキシ設定** ※ 通常時からwpadを使用している場合、区別出来ない	–
	接続先	イベントログ – セキュリティ	***イベントID***： **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***新しいプロセス名***： *"[検体（wpad.exe）]"* **・確認できる情報** ・**プロセスの開始・終了日時**： ログの日付 ・**プロセスを実行したユーザー名**： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**： ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**： ***プロセス情報*** -> ***終了状態***	必要
			検体が実行された直後に、以下が記録される	
			イベントID： **5154**（Windowsフィルターリング プラットフォームで、アプリケーションまたはサービスによるポートでの着信接続のリッスンが許可されました） ・***アプリケーション情報*** -> ***プロセスID***： イベントID **4688**で記録された***プロセスID*** ・***アプリケーション情報*** -> ***アプリケーション名***： *"¥device¥harddiskvolume2¥[検体（wpad.exe）]"* **・確認できる情報** ・**リッスンされたポート**： ***ネットワーク情報*** -> ***ソース ポート***（*"80"・"8888"*） ・**プロトコル**： ***ネットワーク情報*** -> ***プロトコル***（*"6"* = TCP）	
			イベントID： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***プロセスID***： *"4"* ・***アプリケーション情報*** -> ***アプリケーション名***： *"System"* ・***ネットワーク情報*** -> ***方向***： *"送信"* ・***ネットワーク情報*** -> ***送信元アドレス***： *"[検体を実行したホスト]"* ・***ネットワーク情報*** -> ***宛先ポート・ソース ポート・プロトコル***： *"137"*（宛先・ソース共）・*"17"*	
			接続元がwpadを取得する際に、以下が記録される	
			イベントID： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***プロセスID***： イベント**4688**で記録された***プロセスID*** ・***アプリケーション情報*** -> ***アプリケーション名***： *"¥device¥harddiskvolume2¥[検体（wpad.exe）]"* ・***ネットワーク情報*** -> ***方向***： *"着信"* ・***ネットワーク情報*** -> ***ソース ポート・プロトコル***： *"80"・"6"*（TCP） **・確認できる情報** ・**接続したホスト**： ***ネットワーク情報*** -> ***宛先アドレス***	

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows ユーザー （続）	接続元 （続）	イベントログ － セキュリティ	***イベントID*** : **4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(wpad.exe)]"* **・確認できる情報** ・**対象のファイル** : ***オブジェクト*** -> ***オブジェクト名*** (*"[検体のパス]¥wpad.dat"*) ・**ハンドルID** : ***オブジェクト*** -> ***ハンドルID*** ※ 他ログとの紐付けに使用する ・**処理内容** : ***アクセス要求情報*** -> ***アクセス*** (*"SYNCHRONIZE"・"ReadData (またはListDirectory)"・"WriteData (またはAddFile)"・"AppendData (またはAddSubdirectoryまたはCreatePipeInstance)"・"ReadEA"・"WriteEA"・"ReadAttributes"・"WriteAttributes"*) ・**成否** : ***キーワード*** (*"成功の監査"*)	必要
			接続元がホストをプロキシとして利用する際に、以下が記録される ログファイル(proxy.log)が、実行ファイルと同じパスに作成される(ログに対するハンドルは、都度要求され、閉じられる)	
			イベントID : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***プロセスID*** : イベント**4688**で記録された***プロセスID*** ・***アプリケーション情報*** -> ***アプリケーション名*** : *"¥device¥harddiskvolume2¥[検体(wpad.exe)]"* ・***ネットワーク情報*** -> ***方向*** : *"着信"* ・***ネットワーク情報*** -> ***ソース ポート・プロトコル*** : *"8888"・"6"*(TCP) **・確認できる情報** ・**接続したホスト** : ***ネットワーク情報*** -> ***宛先アドレス***	
			イベントID : **4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(wpad.exe)]"* **・確認できる情報** ・**対象のファイル** : ***オブジェクト*** -> ***オブジェクト名*** (*"[検体のパス]¥proxy.log"*) ・**ハンドルID** : ***オブジェクト*** -> ***ハンドルID*** ※ 他ログとの紐付けに使用する ・**処理内容** : ***アクセス要求情報*** -> ***アクセス*** (*"WriteData (またはAddFile)"*) ・**成否** : ***キーワード*** (*"成功の監査"*)	
			イベントID : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***プロセスID*** : イベント**4688**で記録された***プロセスID*** ・***アプリケーション情報*** -> ***アプリケーション名*** : *"¥device¥harddiskvolume2¥[検体(wpad.exe)]"* ・***ネットワーク情報*** -> ***方向*** : *"送信"* ・***ネットワーク情報*** -> ***送信元アドレス*** : *"[検体を実行しているホスト]"* ・***ネットワーク情報*** -> ***ソース ポート・プロトコル*** : *"[宛先サーバのポート](指定が無い場合は80)"・"6"*(TCP) **・確認できる情報** ・**接続先** : ***ネットワーク情報*** -> ***宛先アドレス***	
		イベントログ － Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体(wpad.exe)]"* **・確認できる情報** ・**プロセスの開始・終了日時(UTC)** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ※ iframeなどが使用された場合、引数から読み取ることが可能 ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		実行履歴 Prefetch	**ファイル名： C:¥Windows¥Prefetch¥WPAD.EXE-[文字列].pf** **・確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** ： ***Last Run Time***	－

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	－

3.5.1. RDP (Remote Desktop Protocol)

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<基本情報>

ツール	ツール名称	RDP (Remote Desktop Protocol)
	カテゴリ	リモートログイン
	ツール概要	リモートデスクトップサービスが稼働しているサーバーに接続するためのプロトコル
	攻撃時における想定利用例	・ログインされた端末上でファイルを閲覧 ・他のサーバ・端末に接続するための情報を収集 ・他の機器に接続する踏み台として利用
動作条件	権限	標準ユーザー
	対象OS	・接続元：Windows ・接続先：リモートデスクトップを有効化したWindows
	ドメインへの参加	不要
	通信プロトコル	3389/tcp
	サービス	・接続先：Remote Desktop Services
ログから得られる情報	標準設定	・接続先：RDPセッションの接続開始・終了日時 接続元IPアドレス ログインされたユーザー名及びアカウントドメイン 接続の成否
	追加設定	・接続元：mstsc.exeの実行履歴、ファイルのアクセス履歴
実行成功時に確認できる痕跡		・接続先：イベントログに以下のログがある場合、接続が成功していると考えられる ・イベントログ「セキュリティ」にイベントID: **4624**が記録されている ・イベントログ「Microsoft¥Windows¥TerminalServices-LocalSessionManager¥Operational」にイベントID：**21**、**24**が記録されている

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows ユーザー	接続元	イベントログ – セキュリティ	***イベントID***：**4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***新しいプロセス名***： *"C:¥Windows¥System32¥mstsc.exe* ・**確認できる情報** ・**プロセスの開始・終了日時**： ログの日付 ・**プロセスを実行したユーザー名**： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザのドメイン**： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**： ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**： ***プロセス情報*** -> ***終了状態***	必要
			イベントID：**4663**（オブジェクトへのアクセスが試行されました） **4656**（オブジェクトへのハンドルが要求されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名***：*"C:¥Windows¥System32¥mstsc.exe"* ・**確認できる情報** ・**対象のファイル**： ***オブジェクト*** -> ***オブジェクト名***（例：*"C:¥Users¥[ユーザー名]¥Documents¥Default.rdp"*） ・**ハンドルID（他ログとの紐付けに使用する）**： ***オブジェクト*** -> ***ハンドルID*** ・**処理内容**： ***アクセス要求情報*** -> ***アクセス***（*"WriteData (またはAddFile)"* *"AppendData (またはAddSubdirectoryまたは* ・**成否**： ***キーワード***（*"成功の監査"*）	
		実行履歴 – Sysmon	***イベントID***：**1**（Process Create） **5**（Process Terminated） ・***Image***：*"C:¥Windows¥System32¥mstsc.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**： ***UtcTime*** ・**プロセスのコマンドライン**： ***CommandLine*** ・**実行ユーザー名**： ***User*** ・**プロセスID**： ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名**：**C:¥Windows¥Prefetch¥MSTSC.EXE-76A46E8A.pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**： ***Last Run Time***	–
		アクセス履歴 – レジストリ	**レジストリエントリ**：**HKEY_USERS¥[SID]¥Software¥Microsoft¥Terminal Server Client¥Default¥** ・**確認できる情報** ・**リモートデスクトップの接続履歴**： ***値の名前*** = *"MRU0"～"MRU9"* ※ 上記の***値のデータ***として、**過去に接続したIPアドレス**が記録される MRU0が最後に接続した履歴 キーの***最終書き込み時刻***は、*"MRU0"*の***値のデータ***が**更新された日時**(接続履歴にない接続先に対して初めて接続した時間)が記録される	–
			レジストリエントリ：**HKEY_USERS¥[SID]¥Software¥Microsoft¥Terminal Server Client¥Servers¥[接続先IPアドレス]¥** ・**確認できる情報** ・**最後にアクセスしたアカウントドメイン及びユーザー名**： ***値の名前*** = *"UsernameHint"* ※ 値のデータとして、過去に接続したIPアドレスごとに最後にアクセスした アカウントドメイン及びユーザー名が記録される	
	接続先	アクセス履歴 – 監査ポリシー	***イベントID***：**4624**（アカウントが正常にログオンしました） ・***ログオン タイプ***：*"10"* ・***ネットワーク情報*** -> ***ソース ネットワーク アドレス***：イベント**5156**における、***宛先アドレス*** ・***ネットワーク情報*** -> ***ソース ポート***：イベント**5156**に記録された、***宛先ポート*** ・***詳細な認証情報*** -> ***ログオン プロセス***：*"Kerberos"* ・**確認できる情報** ・**接続元ホスト**： ***ネットワーク情報*** -> ***ソース ネットワークアドレス*** ・**使用されたユーザー**： ***新しいログオン*** -> ***アカウント名・アカウント ドメイン*** ・**新しいログオンID（他ログとの紐付けに使用）**： ***新しいログオン*** -> ***ログオンID***	必要
		イベントログ – アプリケーションとサービス ログ ¥Microsoft¥Windows ¥TerminalServices-LocalSessionManager ¥Operational	**イベントID:21**（リモートデスクトップ セッション ログオン成功） ・**確認できる情報** ・**セッションの接続開始日時**： ***ログの日付*** ・**ログインされたアカウントドメイン及びユーザー名**： ***ユーザー*** ・**接続元IPアドレス**： ***ソースネットワークアドレス***	–
			イベントID:24（リモートデスクトップ セッション 切断） ・**確認できる情報** ・**セッションの接続開始日時**： **イベントID:21**の***セッションID***が同じイベントログの***ログの日付*** ・**ログインされたアカウントドメイン及びユーザー名**： ***ユーザー*** ・**接続元IPアドレス**： ***ソースネットワークアドレス***	

<備考>

記載のもの以外で出力される可能性のあるイベントログ	接続先のイベントログ「セキュリティ」には環境によって下記のログが出力される可能性がある ***イベントID***：**4624**（アカウントが正常にログオンしました） ・***ログオン タイプ***：*"12"*

3.6.1. WCE (リモートログイン)

<基本情報>

ツール	ツール名称	WCE (リモートログイン)
	カテゴリ	pass-the-hash, pass-the-ticket
	ツール概要	取得したパスワードのハッシュを利用し、上位権限でコマンドを実行する
	攻撃時における想定利用例	ADに所属する管理者ユーザ権限のハッシュを利用し、他端末にリモートでコマンド実行を行う ・接続元: WCE実行元 ・接続先: WCEによってログインされた先
動作条件	権限	ローカルの管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	ランダムな5桁のポート(WMIC)
	サービス	–
ログから得られる情報	標準設定	・接続元: 実行履歴(Prefetch) WCESERVICEがインストールされ、実行されていることの記録
	追加設定	・両側: WMIの実行履歴、及びWindowsフィルターリングプラットフォームのログ ・接続先: リモートからログインが発生していること
実行成功時に確認できる痕跡		・接続元: WCESERVICEがインストール・実行されたことが記録されている ・接続先: リモートホストからログオンしたことが記録されている ・両側: WMIを用いて通信したことが記録されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS:Windows 管理者ユーザー ↓ OS:Windows 管理者ユーザー	接続元 (Windows)	イベントログ – セキュリティ	***イベントID*** : **4656**(オブジェクトへのハンドルが要求されました) **4663**(オブジェクトへのアクセスが試行されました) **4658**(オブジェクトに対するハンドルが閉じました) ・***オブジェクト*** -> ***オブジェクト名*** : *"(C:¥Windows¥Temp¥wceaux.dll)"* ・***アクセス要求情報*** -> ***アクセス・アクセス理由*** : (*"WriteData (またはAddFile)"*) ・**確認できる情報** ・**プロセス名**: *"[検体 (wce.exe)]"* ・**ハンドルID**: ***オブジェクト*** -> ***ハンドルID***	必要
			イベントID : **4656**(オブジェクトへのハンドルが要求されました) **4660**(オブジェクトが削除されました) **4658**(オブジェクトに対するハンドルが閉じました) ・***オブジェクト*** -> ***オブジェクト名*** : *"(C:¥Windows¥Temp¥wceaux.dll)"* ・***アクセス要求情報*** -> ***アクセス・アクセス理由*** : (*"DELETE"*) ・**確認できる情報** ・**プロセス名**: *"[検体 (wce.exe)]"* ・**ハンドルID**: ***オブジェクト*** -> ***ハンドルID***	
			イベント**4656・4663・4658**の処理を、複数ファイルに対しておこなう	
			イベントID : **4656**(オブジェクトへのハンドルが要求されました) **4663**(オブジェクトへのアクセスが試行されました) **4658**(オブジェクトに対するハンドルが閉じました) ・***オブジェクト*** -> ***オブジェクト名*** : *"(C:¥Users¥[ユーザー名]¥AppData¥Local¥Microsoft¥Windows¥Temporary Internet Files¥Content.IE5)"* ・***アクセス要求情報*** -> ***アクセス・アクセス理由*** : (*"SYNCHRONIZE"*、*"WriteAttributes"*、*"WriteData (またはAddFile)"*) ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥wbem¥WMIC.exe"* ・**確認できる情報** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドルID*** ※ 他のログとの紐付けに使用する	
			イベントID : **5156**(Windows フィルターリング プラットフォームで、接続が許可されました) ・***アプリケーション情報*** -> ***アプリケーション名*** : (*"C:¥Windows¥System32¥wbem¥WMIC.exe"*) ・***ネットワーク情報*** -> ***方向*** : *"送信"* ・**確認できる情報** ・**接続先ホスト**: ***宛先アドレス*** ・**接続先ポート**: ***宛先ポート***	
		イベントログ – システム	***イベントID*** : **7045**(サービスがシステムにインストールされました) ・***サービス名*** : *"WCESERVICE"* ・**確認できる情報** ・**プロセスの開始日時**: ログの日付 ・**サービス ファイル名**: *"[検体 (wce.exe)] -S"*	–
			イベントID : **7036** ・***詳細タブ*** -> ***System¥Provider¥Name*** : *"Service Control Manager"* ・***詳細タブ*** -> ***EventData¥param1*** : *"WCESERVICE"* ・**確認できる情報** ・**サービスの実行**: ***詳細タブ*** -> ***EventData¥param2*** (*"実行中"*)・(*"停止"*)	
		イベントログ – Sysmon	***イベントID*** : **1** (Process Create) **5** (Process Terminated) ・***Image*** : *"[検体 (wce.exe)]"* ・***Image*** : *"C:¥Windows¥System32¥wbem¥WMIC.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
			イベントID : **8** (CreateRemoteThread detected) ・***SourceImage*** : *"[検体 (wce.exe)]"* ・***TargetImage*** : (*"C:¥Windows¥System32¥lsass.exe"*) ・**確認できる情報** ・**プロセスの開始日時(UTC)**: ***UtcTime***	
			イベントID : **9** (RawAccessRead detected) ・***Image*** : *"C:¥Windows¥System32¥cmd.exe"* ・**確認できる情報** ・**プロセスの開始日時(UTC)**: ***UtcTime*** ・**アクセス先**: ***Device***	
		実行履歴 – レジストリ	**ファイル名 : C:¥Windows¥Prefetch¥[検体(WCE.EXE)]-[文字列].pf** **C:¥Windows¥Prefetch¥WMIC.EXE-A7D06383.pf** ・**確認できる情報** (ツールを利用して下記を確認できる ツール:WinPrefetchView) ・**最終実行日時** : ***Last Run Time***	–

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows 管理者ユーザー ↓ OS：Windows 管理者ユーザー （続）	接続先 （Windows）	イベントログ － セキュリティ	***イベントID*** : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** : （*"¥device¥harddiskvolume2¥windows¥system32¥svchost.exe"*） ・***ネットワーク情報*** -> ***方向*** : *"受信"* ・**確認できる情報** ・**接続元ホスト**: ***宛先アドレス*** ・**接続元ポート**: ***宛先ポート***	必要
			イベントID : **4624**（アカウントが正常にログオンしました） **4634**（アカウントがログオフしました） ・**確認できる情報** ・**プロセスの開始日時**: ログの日付 ・**接続元アカウント名**: ***新しいログオン*** -> ***アカウント名・ドメイン名*** ・**接続元**: ***ネットワーク情報*** -> ***ソース ネットワーク アドレス***	
			イベントID : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥wbem¥WmiPrvSE.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態*** ・**親プロセス ID**: ***プロセス情報*** -> ***クリエーター プロセス ID***	
		イベントログ － Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"C:¥Windows¥System32¥wbem¥WmiPrvSE.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
			イベントID : **9**（RawAccessRead detected） ・***Image*** : *"C:¥Windows¥System32¥wbem¥WmiPrvSE.exe"* ・**確認できる情報** ・**プロセスの開始日時（UTC）**: ***UtcTime*** ・**アクセス先**: ***Device***	
		実行履歴 － Prefetch	**ファイル名：C:¥Windows¥Prefetch¥WMIPRVSE.EXE-1628051C.pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** : ***Last Run Time***	－

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	－

3.6.2. Mimikatz (リモートログイン)

<基本情報>

ツール	ツール名称	Mimikatz (リモートログイン)
	カテゴリ	pass-the-hash, pass-the-ticket
	ツール概要	取得したパスワードのハッシュを利用し、他ユーザーの権限でコマンドを実行する
	攻撃時における想定利用例	管理者ユーザー権限のハッシュを利用し、他端末にリモートでコマンド実行を行う ・接続元: Mimikatz実行元 ・接続先: Mimikatzによってログインされた先
動作条件	権限	接続元: 管理者ユーザー 接続先: ハッシュを利用されたユーザーの権限
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	ランダムな5桁のポート(WMIC)
	サービス	Windows Management Instrumentation
ログから得られる情報	標準設定	・実行履歴(Prefetch)
	追加設定	・リモート接続時の通信の発生ログ ・接続が発生した過程のログ
実行成功時に確認できる痕跡		・接続先: イベントログに以下のログがある場合、リモートからログインされていると考えられる ・イベントログ「セキュリティ」にイベントID **4624**が記録され、意図しない接続元からアクセスされている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS:Windows 管理者ユーザー ↓ OS:Windows ユーザー	接続元	イベントログ - セキュリティ	***イベントID***: **4688**(新しいプロセスが作成されました) **4689**(プロセスが終了しました) ・***プロセス情報*** -> ***プロセス名***: *"[検体(mimikatz.exe)]"* *"C:¥Windows¥System32¥cmd.exe"* *"C:¥Windows¥System32¥wbem¥WMIC.exe"* **・確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
			イベントID: **5156**(Windows フィルターリング プラットフォームで、接続が許可されました) ・***アプリケーション情報*** -> ***アプリケーション名***: *"C:¥Windows¥System32¥wbem¥WMIC.exe"* ・***ネットワーク情報*** -> ***方向***: *"送信"* **・確認できる情報** ・**接続元ポート**: ***ソース ポート*** ・**接続先ホスト**: ***宛先アドレス*** ・**接続先ポート**: ***宛先ポート***(5桁のポートとなる)	
			イベントID: **4648**(明示的な資格情報を使用してログオンが試行されました) ・***プロセス情報*** -> ***プロセス名***: *"C:¥Windows¥System32¥wbem¥WMIC.exe"* **・確認できる情報** ・**プロセスの開始日時**: ログの日付 ・**接続先端末においてプロセスを実行したアカウント名**: ***資格情報が使用されたアカウント*** -> ***アカウント名・ドメイン名*** ・**接続先**: ***ターゲット サーバー*** -> ***ターゲット サーバー名***	
		イベントログ - Sysmon	***イベントID***: **1**(Process Create) **5**(Process Terminated) ・***Image***: *"C:¥Windows¥System32¥at.exe"* *"C:¥Windows¥System32¥cmd.exe"* *"C:¥Windows¥System32¥wbem¥WMIC.exe"* **・確認できる情報** ・**プロセスの開始・終了日時(UTC)**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ・**実行ユーザ名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 - レジストリ	**ファイル名: C:¥Windows¥Prefetch¥CMD.EXE-4A81B364.pf** **C:¥Windows¥Prefetch¥[検体(MIMIKATZ.EXE)]-[文字列].pf** **C:¥Windows¥Prefetch¥WMIC.EXE-A7D06383.pf** **・確認できる情報**(ツールを利用して下記を確認できる ツール:WinPrefetchView) ・**最終実行日時**: ***Last Run Time***	-
	接続先	イベントログ - セキュリティ	***イベントID***: **4624**(アカウントが正常にログオンしました) ・***ログオン タイプ***: *"3"* **・確認できる情報** ・**プロセスの開始日時**: ログの日付 ・**接続元アカウント名**: ***新しいログオン*** -> ***アカウント名・ドメイン名*** ・**接続元**: ***ネットワーク情報*** -> ***ソース ネットワーク アドレス***	必要
			イベントID: **5156**(Windows フィルターリング プラットフォームで、接続が許可されました) ・***アプリケーション情報*** -> ***アプリケーション名***: *"¥device¥harddiskvolume2¥windows¥system32¥svchost.exe"* ・***ネットワーク情報*** -> ***方向***: *"受信"* **・確認できる情報** ・**接続元ホスト**: ***宛先アドレス*** ・**接続元ポート**: ***宛先ポート*** ※ 接続元ホストにおける***ソース ポート***と一致する ・**接続先ポート**: ***ソース ポート*** ※ 接続元ホストにおける**宛先ポート**と一致する	
		イベントログ - Sysmon	***イベントID***: **1**(Process Create) ・***Image***: *"C:¥Windows¥System32¥wbem¥WmiPrvSE.exe"* **・確認できる情報** ・**プロセスの開始日時(UTC)**: ***UtcTime*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 - レジストリ	**ファイル名: C:¥Windows¥Prefetch¥WMIPRVSE.EXE-1628051C.pf** **・確認できる情報**(ツールを利用して下記を確認できる ツール:WinPrefetchView) ・**最終実行日時**: ***Last Run Time***	-

<備考>

記載のもの以外で出力される可能性のあるイベントログ	-

3.7.1. MS14-058 Exploit

<基本情報>

ツール	ツール名称	MS14-058 Exploit
	カテゴリ	SYSTEM権限に昇格
	ツール概要	指定したコマンドを、SYSTEM権限で実行する
	攻撃時における想定利用例	本来管理者権限が必要なコマンドを、標準権限しか持たないユーザーで実行する
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・検体、及び検体によりSYSTEM権限で実行されたプロセスのプロセス名・引数（Sysmon・プロセス追跡の監査）
実行成功時に確認できる痕跡		イベントログに以下のログがある場合、権限昇格が成功していると考えられる ・イベント: **4688**においてSYSTEM権限で実行されているプロセスにおいて、親プロセスが検体やそのプロセスの親となり得ないものとなっている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 (Windows)	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体]"* **・確認できる情報** **・プロセスの開始・終了日時** : ログの日付 **・プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** **・プロセスを実行したユーザのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** **・プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 **・プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***新しいプロセス名*** : *"[SYSTEM権限で実行されたプロセス]"* **・確認できる情報** **・プロセスの開始・終了日時** : ログの日付 **・プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名***（*"[コンピュータ名]$"*） **・プロセスを実行したユーザのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** **・プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 **・プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体]"* **・確認できる情報** **・プロセスの開始・終了日時（UTC）** : ***UtcTime*** **・プロセスのコマンドライン** : ***CommandLine*** ※ **SYSTEM権限で実行されたコマンド**が、引数に記録される **・実行ユーザー名** : ***User*** **・プロセスID** : ***ProcessId***	必要
			イベントID : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[SYSTEM権限で実行されたプロセス]"* **・確認できる情報** **・プロセスの開始日時（UTC）** : ***UtcTime*** **・プロセスのコマンドライン** : ***CommandLine*** ※ **コマンドに対する引数**が記録される **・実行ユーザー名** : ***User***（*"NT AUTHORITY¥SYSTEM"*） **・プロセスID** : ***ProcessId*** **・親プロセス名** : ***ParentImage***（*"[検体]"*） **・親プロセスに指定されたコマンドライン** : ***ParentCommandLine***	
		実行履歴 – Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥[検体]-[文字列].pf** **・確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） **・最終実行日時** : ***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	SYSTEM権限で実行されたプロセスに関連する、他のログが出力される可能性がある

3.7.2. MS15-078 Exploit

<基本情報>

ツール	ツール名称	MS15-078 Exploit
	カテゴリ	SYSTEM権限に昇格
	ツール概要	指定したコマンドを、SYSTEM権限で実行する
	攻撃時における想定利用例	本来管理者権限が必要なコマンドを、標準権限しか持たないユーザーで実行する
動作条件	権限	標準ユーザー
	対象OS	Windows 7・8・2008 本検証環境では、Windows Server 2012では実行不可
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・検体、及び検体によりSYSTEM権限で実行されたプロセスのプロセス名・引数（Sysmon・プロセス追跡の監査）
実行成功時に確認できる痕跡		イベントログに以下のログがある場合、権限昇格が成功していると考えられる ・イベント: **4688**においてSYSTEM権限で実行されているプロセスにおいて、親プロセスが検体やそのプロセスの親となり得ないものとなっている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 (Windows)	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***新しいプロセス名*** : *"[検体]"* **・確認できる情報** **・プロセスの開始・終了日時** : ログの日付 **・プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** **・プロセスを実行したユーザのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** **・プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 **・プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***新しいプロセス名*** : *"[SYSTEM権限で実行されたプロセス]"* **・確認できる情報** **・プロセスの開始・終了日時** : ログの日付 **・プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名***（*"[コンピュータ名]$"*） **・プロセスを実行したユーザのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** **・プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 **・プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体]"* **・確認できる情報** **・プロセスの開始・終了日時（UTC）** : ***UtcTime*** **・プロセスのコマンドライン** : ***CommandLine*** ※ **SYSTEM権限で実行されたコマンド**が、引数に記録される **・実行ユーザー名** : ***User*** **・プロセスID** : ***ProcessId***	必要
			イベントID : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[SYSTEM権限で実行されたプロセス]"* **・確認できる情報** **・プロセスの開始日時（UTC）** : ***UtcTime*** **・プロセスのコマンドライン** : ***CommandLine*** ※ **コマンドに対する引数**が記録される **・実行ユーザー名** : ***User***（*"NT AUTHORITY¥SYSTEM"*） **・プロセスID** : ***ProcessId*** **・親プロセス名** : ***ParentImage***（*"[検体]"*） **・親プロセスに指定されたコマンドライン** : ***ParentCommandLine***	
		実行履歴 – Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥[検体]-[文字列].pf** **・確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） **・最終実行日時** : ***Last Run Time***	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	SYSTEM権限で実行されたプロセスに関連する、他のログが出力される可能性がある

3.8.1. SDB UAC Bypass

<基本情報>

ツール	ツール名称	SDB UAC Bypass
	カテゴリ	権限昇格
	ツール概要	アプリケーション互換データベース（SDB）を用いて、本来UACにより制御されるアプリケーションを管理者権限で実行する
	攻撃時における想定利用例	通常のアプリケーションを実行するように見せかけて、他のアプリケーションを実行させる この際、本来は管理者権限が必要なアプリケーションを、ユーザーによる承諾を経ることなく実行できる
	参考情報	https://www.jpcert.or.jp/magazine/acreport-uac-bypass.html
動作条件	権限	管理者パスワードを入力することなく、UACにより管理者権限を利用することが可能な権限を持つユーザー （クライアント端末における、Administratorsグループに所属するユーザー）
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・実行履歴（Sysmon・監査ポリシー） ・親プロセス名に、本来は親プロセスとならないことが想定されるアプリケーションを含む、プロセスが開始される ・「回避に使用するアプリケーション」及び「回避実行されたアプリケーション」が記録される
実行成功時に確認できる痕跡		・親プロセス名に、本来は親プロセスとならないことが想定されるアプリケーションを含む、プロセスが実行されたことが記録されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 （Windows）	イベントログ – セキュリティ	SDBファイルがインストールされる際、以下が記録される	必要
			イベントID：**4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名***： *"C:¥Windows¥System32¥sdbinst.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時**： ログの日付 ・**プロセスを実行したユーザー名**： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**： ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**： ***プロセス情報*** -> ***終了状態***	
			イベントID：**4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名***： *"C:¥Windows¥System32¥sdbinst.exe"* ・**確認できる情報** ・**SDBファイル**： ***オブジェクト*** -> ***オブジェクト名***（*"C:¥Windows¥AppPatch¥Custom¥[[GUID]].sdb"*） ・**ハンドルID**： ***オブジェクト*** -> ***ハンドルID*** ※ 他ログとの紐付けに使用する ・**ハンドルを要求したプロセスのプロセスID**： ***プロセス情報*** -> ***プロセスID***（イベント**4688**で作成されたプロセスのIDと一致する） ・**処理内容**： ***アクセス要求情報*** -> ***アクセス・アクセス理由***（*"WriteData（または AddFile）"*・*"AppendData（または AddSubdirectoryまたは CreatePipeInstance"*） ・**成否**： ***キーワード***（*"成功の監査"*）	
			回避実行がされた場合、以下が記録される	
			イベントID：**4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名***： *"[回避実行されたコマンド]"* ・**確認できる情報** ・**プロセスの開始・終了日時**： ログの日付 ・**プロセスを実行したユーザー名**： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**： ***プロセス情報*** -> ***トークン昇格***の種類 ・**このアプリケーションを実行した、回避用に使用されたアプリケーションのプロセスID**： ***プロセス情報*** -> ***クリエーター プロセスID*** 「回避に使用されるアプリケーション」のプロセスIDと一致する。 ・**プロセスの戻り値**： ***プロセス情報*** -> ***終了状態*** 成功の場合は *"0x0"* となる。失敗の場合、エラーに応じて異なる値が入る。コマンドプロンプト上で実行するものなど、回避に使用されるアプリケーションによっては、通常通りに実行しただけでは戻り値が *"0x0"* とならない可能性があるため、場合によっては判断材料とすることが可能。 ※「回避実行されたアプリケーション」は必ず「回避に使用されるアプリケーション」より後に開始されるが、終了については呼び出し方に応じて、前後関係が入れ替わる可能性がある。	
		イベントログ – Sysmon	SDBファイルがインストールされる際、以下が記録される	必要
			イベントID：**1**（Process Create） **5**（Process Terminated） ・***Image***： *"C:¥Windows¥System32¥sdbinst.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**： ***UtcTime*** ・**プロセスのコマンドライン**： ***CommandLine*** ・**利用されたSDBファイル**： ***CommandLine*** ・**実行ユーザ名**： ***User*** ・**プロセスID**： ***ProcessId***	
			回避実行がされた場合、以下が記録される	
			イベントID：**1**（Process Create） **5**（Process Terminated） ・***Image***： *"[回避実行されたコマンド]"* ・**確認できる情報** ・**プロセスの開始日時（UTC）**： ***UtcTime*** ・**プロセスのコマンドライン**： ***CommandLine*** ・**実行ユーザ名**： ***User*** ・**プロセスID**： ***ProcessId*** ・**親プロセス名**： ***ParentImage*** ※ SDB内で指定されているアプリケーション 本来は**本プロセスの親とならないことが想定されるアプリケーション**が、本プロセスの親となる ・**親プロセスID**： ***ParentProcessId*** ※ 先に実行された、「SDB内で指定されているアプリケーション」のプロセスIDと一致する ※ このプロセスがバッチなどのスクリプト系ファイルであった場合、このプロセスが親プロセスとなって更に子プロセスが実行される 順番にプロセスIDを追跡することで、実行されたアプリケーションのプロセスツリーを確認することが可能	
		アプリケーションとサービス ログ ¥Microsoft¥Windows ¥Application-Experience ¥Program-Telemetry	***イベントID***：**500**（互換性修正プログラムが適用されています）	–
			・**確認できる情報** ・**適用されたプログラム**： ***詳細***タブ -> ***UserData¥CompatibilityFixEvent¥ExePath*** ・**修正プログラム**： ***詳細***タブ -> ***UserData¥CompatibilityFixEvent¥FixName***	

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加 設定
– （続）	端末 （Windows） （続）	実行履歴 – Prefetch	**ファイル名： C:¥Windows¥Prefetch¥SDBINST.EXE-5CC2F88B.pf** **・確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） **・最終実行日時** ： ***Last Run Time***	–
			・備考 ・上記の他に、回避に使用されたアプリケーション、及び実行されたアプリケーションにおける最終実行日時が変化する	
		実行履歴 – レジストリ	**レジストリエントリ: HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥{[GUID]}.sdb** **・確認できる情報** **・SDBの内容**： ***DisplayName***（回避に使用されるアプリケーション名が入る） **・削除コマンド**： ***UninstallString***（*"%windir%¥system32¥sdbinst.exe -u "C:¥Windows¥AppPatch¥Custom¥[[GUID]].sdb"*）	–
			レジストリエントリ: HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥AppCompatFlags¥Custom¥{[UAC回避に使用されるアプリケーション名]} **・確認できる情報** **・SDBをインストールしたタイムスタンプ**： ***DatabaseInstallTimeStamp***（16進数の値となる）	
			レジストリエントリ: HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥AppCompatFlags¥InstalledSDB¥{[GUID]} **・確認できる情報** **・SDBファイルのパス**： ***DatabasePath***（*"C:¥Windows¥AppPatch¥Custom¥[[GUID]].sdb"*） **・SDBの種類**： ***DatabaseType*** **・SDBの内容**： ***DatabaseDescription***（回避に使用されるアプリケーション名が入る） **・SDBをインストールしたタイムスタンプ**： ***DatabaseInstallTimeStamp***（16進数の値。上記 "Custom"配下の値と同じ）	
			・備考 ・上記レジストリの値は、SDBファイルをアンインストールすると削除されるため、必ずしも残存するとは限らない ・痕跡削除として、SDBファイルをアンインストールする検体が確認されている	

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	・上記以外に、「回避に使用されるアプリケーション」及び「回避実行されたアプリケーション」によるログが記録される可能性がある

3.9.1. MS14-068 Exploit

<基本情報>

ツール	ツール名称	MS14-068 Exploit
	カテゴリ	ドメイン管理者権限、アカウントの奪取
	ツール概要	ドメインユーザーの権限を、他のユーザーに変更する
	攻撃時における想定利用例	入手したドメインユーザのアカウントを用いて、管理者になりすまし、権限が必要な操作をおこなう (検証では、Exploitを使用してアカウントのTGTチケットを入手し、mimikatzを利用してリモートログインしている) ・接続元： Exploit実行元 ・接続先： 取得されたチケットによってリモートログインされた端末
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	要
	通信プロトコル	88/tcp, 445/tcp
	サービス	Active Directory Domain Services
ログから得られる情報	標準設定	・接続元： 実行履歴(Prefetch)
	追加設定	・接続元： 実行履歴(Sysmon・監査ポリシー) ・接続先： 本来の権限以上の特権が、他のアカウントに対して認可されていること(監査ポリシー)
実行成功時に確認できる痕跡		・接続先： イベントログ「セキュリティ」のイベントID **4672**において、標準ユーザーに対して上位の特権が認可されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows Server 管理者ユーザー	接続元	イベントログ － セキュリティ	チケットの生成に際し、以下のプロセスが実行される	必要
			イベントID : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(ms14-068.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	
			イベントID : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** : *"¥¥device¥harddiskvolume2¥[検体(ms14-068.exe)]"* ・***アプリケーション情報*** -> ***プロセスID*** : *"[イベント **4688** で記録されたプロセスID]"* ・***ネットワーク情報*** -> ***方向*** : *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** : *"[ドメインコントローラのIPアドレス]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** : *"88"・"6"*(TCP) ・**確認できる情報** ・**接続元ポート**: ***ソース ポート*** ※ドメインコントローラ側ログとの紐付けに使用する	
			取得したチケットを使用する際に、以下のプロセスが実行される	
			イベントID : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(mimikatz.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	
			イベントID : **4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(ms14-068.exe)]"* ・**確認できる情報** ・**対象のファイル**: ***オブジェクト*** -> ***オブジェクト名*** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドルID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス*** (*"WriteData (またはAddFile)"*・*"AppendData (またはAddSubdirectoryまたは*	
			イベントID : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** : *"System"* ・***ネットワーク情報*** -> ***方向*** : *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** : *"[ドメインコントローラのIPアドレス]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** : *"445"・"6"*(TCP) ・**確認できる情報** ・**接続元ポート**: ***ソース ポート*** ※ドメインコントローラ側ログとの紐付けに使用する	
			イベントID : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** : *"[¥device¥harddiskvolume2¥windows¥system32¥lsass.exe"* ・***ネットワーク情報*** -> ***方向*** : *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** : *"[ドメインコントローラのIPアドレス]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** : *"88"・"6"*(TCP) ・**確認できる情報** ・**接続元ポート**: ***ソース ポート*** ※ドメインコントローラ側ログとの紐付けに使用する	
			mimikatz.exeの場合、取得したチケットを使用する際に特権利用(失敗)が発生する(管理者権限で実行している場合は発生しない)	
			イベントID : **4673**（特権のあるサービスが呼び出されました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(mimikatz.exe)]"* ・***プロセス情報*** -> ***プロセスID*** : *"[検体のプロセスID]"* ・***サービス要求情報*** -> ***特権*** : *"SeTcbPrivilege"* ・***キーワード*** : *"失敗の監査"* ・**確認できる情報** ・**上記の動作を試みたアカウント**: **アカウント名**	

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows Server 管理者ユーザー （続）	接続元 （続）	イベントログ － Sysmon	***イベントID*** ： **1**（Process Create） **5**（Process Terminated） ・***Image*** ： *"[検体(ms14-068.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** ： ***UtcTime*** ・**プロセスのコマンドライン** ： ***CommandLine*** ・**実行ユーザ名** ： ***User*** ・**プロセスID** ： ***ProcessId***	必要
			イベントID ： **1**（Process Create） **5**（Process Terminated） ・***Image*** ： *"[検体(mimikatz.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** ： ***UtcTime*** ・**プロセスのコマンドライン** ： ***CommandLine*** ・**実行ユーザ名** ： ***User*** ・**プロセスID** ： ***ProcessId***	
		実行履歴 － Prefetch	**ファイル名：** **C:¥Windows¥Prefetch¥[検体（MS14-068.EXE）]-[文字列].pf** **C:¥Windows¥Prefetch¥[検体（MIMIKATZ.EXE）]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** ： ***Last Run Time***	－
	接続先	イベントログ － セキュリティ	チケットの生成に際し、以下の通信・認証が発生する	必要
			イベントID ： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** ： *"[¥device¥harddiskvolume2¥windows¥system32¥lsass.exe"* ・***アプリケーション情報*** -> ***プロセスID*** ： *"[イベント **4688** で記録されたプロセスID]"* ・***ネットワーク情報*** -> ***方向*** ： *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** ： *"[ドメインコントローラのIPアドレス]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** ： *"88"・"6"*（TCP） ・**確認できる情報** ・**接続元ポート**：***ソース ポート*** ※ドメインコントローラ側ログとの紐付けに使用する	
			イベントID ： **4768**（Kerberos認証チケット(TGT)が要求されました） ・***サービス情報*** -> ***サービス名*** ： *"krbtgt"* ・***追加情報*** -> ***チケット オプション*** ： *"0x50800000"* ・**確認できる情報** ・**実行アカウント**：***アカウント情報*** -> ***アカウント名*** ・**接続元ホスト**：***ネットワーク情報*** -> ***クライアント アドレス*** ・**接続元ポート**：***ネットワーク情報*** -> ***クライアント ポート***	
			イベントID ： **4769**（Kerberosサービス チケットが要求されました） ・***サービス情報*** -> ***サービス名*** ： *"krbtgt"* ・***追加情報*** -> ***チケット オプション*** ： *"0x50800000"* ・**確認できる情報** ・**実行アカウント**：***アカウント情報*** -> ***アカウント名・アカウント ドメイン*** ・**接続元ホスト**：***ネットワーク情報*** -> ***クライアント アドレス*** ・**接続元ポート**：***ネットワーク情報*** -> ***クライアント ポート***	
			取得したチケットを使用する際に、以下の通信が発生する	
		イベントログ － セキュリティ	***イベントID*** ： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** ： *"System"* ・***アプリケーション情報*** -> ***プロセスID*** ： *"[イベント **4688** で記録されたプロセスID]"* ・***ネットワーク情報*** -> ***方向*** ： *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** ： *"[ドメインコントローラのIPアドレス]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** ： *"445"・"6"*（TCP） ・**確認できる情報** ・**接続元ポート**：***ソース ポート*** ※ドメインコントローラ側ログとの紐付けに使用する	必要
			イベントID ： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** ： *"[¥device¥harddiskvolume2¥windows¥system32¥lsass.exe"* ・***アプリケーション情報*** -> ***プロセスID*** ： *"[イベント **4688** で記録されたプロセスID]"* ・***ネットワーク情報*** -> ***方向*** ： *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** ： *"[ドメインコントローラのIPアドレス]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** ： *"88"・"6"*（TCP） ・**確認できる情報** ・**接続元ポート**：***ソース ポート*** ※ドメインコントローラ側ログとの紐付けに使用する	
			イベントID ： **4769**（Kerberos サービス チケットが要求されました） ・**確認できる情報** ・**クライアントIPアドレス**：***ネットワーク情報*** -> ***クライアント アドレス*** ・**チケット要求の種類**（異なる組のものが2つ出力される） ・ ***サービス情報*** ： *"[ホスト名]$"*、***チケット オプション*** ： *"0x40810000"* ・ ***サービス情報*** ： *"krbtgt"*、***チケット オプション*** ： *"0x60810010"*	
			イベントID ： **4672**（新しいログオンに特権が割り当てられました） ・**確認できる情報** ・**権限が昇格したアカウント**：***サブジェクト*** -> ***アカウント名・アカウント ドメイン*** ・**利用可能な特権**：***特権***（*"SeSecurityPrivilege"・"SeRestorePrivilege"・"SeTakeOwnershipPrivilege"・"SeDebugPrivilege"・"SeSystemEnvironmentPrivilege"・"SeLoadDriverPrivilege"・"SeImpersonatePrivilege"・"SeEnableDelegationPrivilege"*）	
			イベントID ： **4624**（アカウントが正常にログオンしました） ・***ログオン タイプ***： *"3"* ・**確認できる情報** ・**使用されたセキュリティID**：***新しいログオン*** -> ***セキュリティID*** ※ 使用されたセキュリティIDとアカウントが異なる場合、この値は奪取されたアカウントのセキュリティIDとなる ・**アカウント**：***アカウント名・アカウント ドメイン*** ・**ログオンを要求したホスト**：***ネットワーク情報*** -> ***ソース ネットワーク アドレス***	

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	昇格した権限を用いて実行されたコマンドのログが、接続先に記録される可能性がある

3.9.2. Mimikatz (Golden Ticket)

<基本情報>

ツール	ツール名称	Mimikatz (Golden Ticket)
	カテゴリ	ドメイン管理者権限、アカウントの奪取
	ツール概要	不正な、任意の期間で有効なKerberosチケットを発行し、再度の認証経ることなく接続を認可させる
	攻撃時における想定利用例	認証要求の記録を隠蔽するホストに対して、Golden Ticketを用いて接続を認可させる ・接続元： Mimikatz実行元 ・接続先： Mimikatzによってログインされた先
動作条件	権限	標準ユーザー ※ドメイン上のkrbtgtアカウントの、NTLMパスワードハッシュを取得済みであること
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	Active Directory Domain Service
ログから得られる情報	標準設定	・接続元： 実行履歴(Prefetch)
	追加設定	・接続元： 実行履歴(Sysmon・監査ポリシー) アクセス履歴(Sysmon – RawAccessRead、監査ポリシー – 重要な特権の使用) ・接続先： 不正なドメインを持つアカウントによるログオン
実行成功時に確認できる痕跡		・接続先： イベントログに以下のログがある場合、不正ログオンが実行されていると考えられる ・イベントログ「セキュリティ」のイベントID **4672**、**4624**、**4634**で、不正なドメインを持つアカウントによるログオンが記録されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows Server 管理者ユーザー	接続元	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(mimikatz.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4673**（特権のあるサービスが呼び出されました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(mimikatz.exe)]"* ・***プロセス情報*** -> ***プロセスID*** : *"[検体のプロセスID]"* ・***サービス要求情報*** -> ***特権*** : *"SeTcbPrivilege"* ・***キーワード*** : *"失敗の監査"* ・**確認できる情報** ・**上記の動作を試みたアカウント**: ***アカウント名***（標準ユーザー）	
			・***イベントID*** : **4663**（オブジェクトへのアクセスが試行されました） **4656**（オブジェクトへのハンドルが要求されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(mimikatz.exe)]"* ・**確認できる情報** ・**対象のファイル**: ***オブジェクト*** -> ***オブジェクト名*** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドルID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス***（*"WriteData (またはAddFile)"*・*"AppendData (またはAddSubdirectory またはCreatePipeInstance)"*） ・**成否**: ***キーワード***（*"成功の監査"*）	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体(mimikatz.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
			イベントID : **9**（RawAccessRead detected） ・***Process*** : イベント1で記録された、***ProcessId*** ・***Image*** : *"[検体(mimikatz.exe)]"* ・***Device*** : *"¥Device¥HarddiskVolume2"*	
		実行履歴 – Prefetch	**ファイル名： C:¥Windows¥Prefetch¥[実行ファイル(MIMIKATZ.EXE)]-[文字列].pf** ・**確認できる情報** (ツールを利用して下記を確認できる ツール：WinPrefetchView) ・**最終実行日時**: ***Last Run Time***	–
	接続先	イベントログ – セキュリティ	***イベントID*** : **4769**（Kerberos サービス チケットの操作） ・**確認できる情報** ・**クライアントIPアドレス**: ***ネットワーク情報*** -> ***クライアント アドレス*** ・**チケット要求の種類**(異なる組のものが2つ出力される) ・ ***サービス情報***: *"[ホスト名]$"*、***チケット オプション***: *"0x40810000"* ・ ***サービス情報***: *"krbtgt"*、***チケット オプション***: *"0x60810010"*	必要
			イベントID : **4672**（新しいログオンに特権が割り当てられました） ・**確認できる情報** ・**Golden Ticketを取得されたアカウント**: ***アカウント***（実在するアカウント名） ・**ドメイン**: ***アカウント ドメイン***（不正な値となる） ・**ログオンID**: **ログオンID** ※ 他ログとの紐付けに使用 ・**利用可能な特権**: ***特権***	
			イベントID : **4624**（アカウントが正常にログオンしました） ・***ログオン タイプ*** : *"3"* ・***新しいログオン*** -> ***アカウント名・アカウント ドメイン*** : *"[イベント **4672** で記録された **アカウント名・アカウント ドメイン**]"* ・***新しいログオン*** -> ***ログオンID*** : *"[イベント **4672** で記録された **ログオンID**]"* ・**確認できる情報** ・**使用されたセキュリティID**: ***新しいログオン*** -> ***セキュリティID*** ・**認証情報を使用した端末**: ***ネットワーク情報*** -> ***ソース ネットワーク アドレス***	
			イベントID : **4634**（ログオフ） ・***ログオン タイプ*** : *"3"* ・***新しいログオン*** -> ***アカウント名・アカウント ドメイン*** : *"[イベント **4672** で記録された **アカウント名・アカウント ドメイン**]"* ・***新しいログオン*** -> ***ログオンID*** : *"[イベント **4672** で記録された **ログオンID**]"*	

<備考>

記載のもの以外で出力される可能性のあるイベントログ	Golden Ticketを用いてアクセスが認可されたホストにおいて、実行されたコマンドに関連するログが出力される可能性がある

3.9.3. Mimikatz (Silver Ticket)

<基本情報>

ツール	ツール名称	Mimikatz (Silver Ticket)
	カテゴリ	ドメイン管理者権限、アカウントの奪取
	ツール概要	不正な、任意の期間で有効なKerberosチケットを発行し、再度の認証を経ることなく接続を認可させる
	攻撃時における想定利用例	認証要求の記録を隠蔽するホストに対して、Silver Ticketを用いて接続を認可させる ・接続元： Mimikatz実行元 ・接続先： Mimikatzによってログインされた先
動作条件	権限	標準ユーザー ※ドメイン上のサービスアカウントの、NTLMパスワードハッシュを取得済みであること
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	Active Directory Domain Services
ログから得られる情報	標準設定	・接続元： 実行履歴（Prefetch）
	追加設定	・接続元： 実行履歴（Sysmon・監査ポリシー） ・接続先： 不正なドメインを持つアカウントによるログオン
実行成功時に確認できる痕跡		・接続先： イベントログに以下のログがある場合、不正ログオンが実行されていると考えられる ・イベントログ「セキュリティ」のイベントID **4672**、**4624**、**4634**で、不正なドメインを持つアカウントによるログオンが記録されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows Server サービス アカウント	接続元	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(mimikatz.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時**： ログの日付 ・**プロセスを実行したユーザー名**： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**： ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**： ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4673**（特権のあるサービスが呼び出されました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体(mimikatz.exe)]"* ・***プロセス情報*** -> ***プロセスID*** : *"[検体のプロセスID]"* ・***サービス要求情報*** -> ***特権*** : *"SeTcbPrivilege"* ・***キーワード*** : *"失敗の監査"* ・**確認できる情報** ・**上記の動作を試みたアカウント**： ***アカウント名***（標準ユーザー）	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体(mimikatz.exe)]"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)**： ***UtcTime*** ・**プロセスのコマンドライン**： ***CommandLine*** ・**実行ユーザー名**： ***User*** ・**プロセスID**： ***ProcessId***	必要
			イベントID : **9**（RawAccessRead detected） ・***Process*** : イベント1で記録された、***ProcessId*** ・***Image*** : *"[検体(mimikatz.exe)]"* ・***Device*** : *"¥Device¥HarddiskVolume2"*	
		実行履歴 – Prefetch	**ファイル名： C:¥Windows¥Prefetch¥[実行ファイル(MIMIKATZ.EXE)]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**： ***Last Run Time***	–
	接続先	イベントログ – セキュリティ	・Golden Ticketとは異なり、チケット生成時にドメインコントローラへの通信は発生しない ・以下は、チケットを用いて通信が着信した際のログ	必要
			イベントID : **4672**（新しいログオンに特権が割り当てられました） ・***特権*** : *"SeSecurityPrivilege"*・*"SeBackupPrivilege"*・*"SeRestorePrivilege"*・*"SeTakeOwnershipPrivilege"*・*"SeDebugPrivilege"*・*"SeSystemEnvironmentPrivilege"*・*"SeLoadDriverPrivilege"*・*"SeImpersonatePrivilege"*・*"SeEnableDelegationPrivilege"* ・**確認できる情報** ・**奪取されたアカウント名**： ***アカウント***（実在するアカウント名） ・**ドメイン**： ***アカウント ドメイン***（不正な値となる） ・**ログオンID**： **ログオンID** ※ 他ログとの紐付けに使用 ・**利用可能な特権**： ***特権***	
			イベントID : **4624**（アカウントが正常にログオンしました） ・***ログオン タイプ*** : *"3"* ・***新しいログオン*** -> ***アカウント名・アカウント ドメイン*** : *"[イベント**4672**で記録された**アカウント名・アカウント ドメイン**]"* ・***新しいログオン*** -> ***ログオンID*** : *"[イベント**4672**で記録された**ログオンID**]"* ・**確認できる情報** ・**使用されたセキュリティID**： ***新しいログオン*** -> ***セキュリティID*** ・**認証情報を使用した端末**： ***ネットワーク情報*** -> ***ソース ネットワーク アドレス***	
			イベントID : **4634**（ログオフ） ・***ログオン タイプ*** : *"3"* ・***新しいログオン*** -> ***アカウント名・アカウント ドメイン*** : *"[イベント**4672**で記録された**アカウント名・アカウント ドメイン**]"* ・***新しいログオン*** -> ***ログオンID*** : *"[イベント**4672**で記録された**ログオンID**]"*	

<備考>

記載のもの以外で出力される可能性のあるイベントログ	Silver Ticketを用いてアクセスが認可されたホストにおいて、実行されたコマンドに関連するログが出力される可能性がある

3.10.1. ntdsutil

<基本情報>

ツール	ツール名称	ntdsutil
	カテゴリ	Active Directory データベースの取得
	ツール概要	Active Directory データベースを保守するコマンド
	攻撃時における想定利用例	NTDSのデータベースであるNTDS.DITを抽出し、他のツールを用いてパスワードを解析する(Active Directoryで実行)
動作条件	権限	管理者ユーザー
	対象OS	Windows Server
	ドメインへの参加	要
	通信プロトコル	–
	サービス	Active Directory Domain Services
ログから得られる情報	標準設定	・サービスの開始、ストレージデバイスに対するドライバのインストールが発生したこと ・シャドウコピーを作成した履歴
	追加設定	・実行履歴(Sysmon・監査ポリシー)
実行成功時に確認できる痕跡		以下が確認できた場合、情報収集が行われている可能性がある ・ntdsutil.exeが実行され、イベントログに以下のログがある場合 ・イベントログ「セキュリティ」にイベントID: **8222**が記録されている ・オブジェクト *"[システムドライブ]¥SNAP_[日時]_VOLUME[ドライブレター]$"* に対するハンドルの要求が成功している ※ さらに、通常は読み出せない C:¥Windows¥NTDS 配下のファイルをコピーしたログ(イベントID: **4663**)が記録されている場合、シャドウコピーを利用されている可能性がある

凡例
・**取得出来る情報**
・**イベントID・項目名**
・***フィールド名***
・*"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	Active Directory ドメインコントローラ	イベントログ – セキュリティ	***イベントID*** : **4688**(新しいプロセスが作成されました) **4689**(プロセスが終了しました) ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥ntdsutil.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセスID** : ***プロセス情報*** -> ***新しいプロセスID*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4673**(特権のあるサービスが呼び出されました) ・***プロセス*** -> ***プロセス名*** : *"C:¥Windows¥explorer.exe"* ・**確認できる情報** ・**使用されている特権**: ***サービス要求情報*** -> ***特権***(*"SeTcbPrivilege"*)	
			イベントID : **8222**(シャドウ コピーが作成されました) ・**確認できる情報** ・**シャドウコピー名**: ***シャドウ デバイス名*** ※ 本ログは、追加設定せずとも記録される	
			イベントID : **4656**(オブジェクトに対するハンドルが要求されました) ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥VSSVC.exe"* ・**確認できる情報** ・**マウントポイント**: ***オブジェクト*** -> ***オブジェクト名***(*"C¥SNAP_[日時]_VOLUME[C]$"*) ・**成否**: ***キーワード***(*"成功の監査"*)	
			・**備考** ・通常は読み出せない C:¥Windows¥NTDS 配下のファイルをコピーしたログ(イベント**4663**)が成功していた場合、アクセスが成功していたと考えられる なお、イベント**4663**の出力には、オブジェクトアクセスの監査が必要	
		イベントログ – Sysmon	***イベントID*** : **1** (Process Create) **5** (Process Terminated) ・***Image*** : *"C:¥Windows¥System32¥ntdsutil.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		イベントログ – システム	***イベントID*** : **7036** ・***詳細***タブ -> ***EventData¥param1*** が以下のいずれかとなっている、サービスの開始が記録される可能性がある ・*"Volume Shadow Copy"* ・*"Microsoft Software Shadow Copy Provider"* ・*"Windows Modules Installer"* ※ 各サービスが既に実行中の場合、ログは出力されない	–
			イベントID : **20001** ・***詳細***タブ -> ***System¥Provider¥Name*** が *"Microsoft-Windows-UserPnp"* となっている ・**確認できる情報** ・**プロセスID**: ***System¥Execution¥ProcessID*** ※ Sysmonログ中に出力される、drvinst.exeのプロセスIDと一致する ・**スナップショット名**: ***UserData¥InstallDeviceID¥DeviceInstanceID*** ※ 一度同様のスナップショットをマウントしたことがある場合、出力されない可能性がある	
		実行履歴 レジストリ	**レジストリエントリ: HKEY_LOCAL_MACHINE¥CurrentControlSet¥Enum¥STORAGE¥VolumeSnapshot¥HarddiskVolumeSnapshot[Snapshot番号]** ・drvinst.exeが実行された場合、新規にキーが作成される	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	volsnap.inf にドライバのインストールが行われたことが差分として残る可能性がある(一度同様のスナップショットをマウントしたことがある場合、出力されない可能性がある)

3.10.2. vssadmin

<基本情報>

ツール	ツール名称	vssadmin
	カテゴリ	Active Directory データベースの取得
	ツール概要	Volume Shadow Copyを作成し、NTDS.DITを抽出する
	攻撃時における想定利用例	NTDSのデータベースであるNTDS.DITを抽出し、他のツールを用いてパスワードを解析する(Active Directoryで実行)
動作条件	権限	管理者ユーザー
	対象OS	Windows Server
	ドメインへの参加	要
	通信プロトコル	–
	サービス	Active Directory Domain Services
ログから得られる情報	標準設定	・サービスの開始、ストレージデバイスに対するドライバのインストールが発生したこと ・シャドウコピーを作成した履歴
	追加設定	・実行履歴(Sysmon・監査ポリシー)
実行成功時に確認できる痕跡		イベントログに以下のログがある場合、シャドウコピーが作成されたと考えられる ・イベントログ「セキュリティ」にイベントID: **8222**が記録されている ※ さらに、通常は読み出せない C:¥Windows¥NTDS 配下のファイルをコピーしたログ(イベントID: **4663**)が記録されている場合、シャドウコピーを利用されている可能性がある

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	Active Directory ドメインコントローラ	イベントログ – セキュリティ	***イベントID*** : **4688**(新しいプロセスが作成されました) **4689**(プロセスが終了しました) ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥vssadmin.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセスID** : ***プロセス情報*** -> ***新しいプロセスID*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **8222**(シャドウ コピーが作成されました) ・**確認できる情報** ・**シャドウコピー名** : ***シャドウ デバイス名***	–
			・**備考** ・通常は読み出せない C:¥Windows¥NTDS 配下のファイルをコピーしたログ(イベント**4663**)が成功していた場合、アクセスが成功していたと考えられる ログの出力内容は、コピーに使用されたソフトウェアに依存する。なお、イベント**4663**の出力には、オブジェクトアクセスの監査が必要	
		イベントログ – システム	***イベントID*** : **7036** ・***詳細***タブ -> ***System¥Provider¥Name*** : *"Service Control Manager"* ・***詳細***タブ -> ***EventData¥param1*** : *"Volume Shadow Copy"* ・**確認できる情報** ・**サービスの実行** : ***詳細***タブ -> ***EventData¥param2***(*"実行中"*) ※ 既にVolume Shadow Copyサービスが動作している場合、出力されない	–
			イベントID : **20001** ・***詳細***タブ -> ***System¥Provider¥Name*** : *"Microsoft-Windows-UserPnp"* ・**確認できる情報** ・**プロセスID** : ***System¥Execution¥ProcessID*** ※ Sysmonログ中に出力される、drvinst.exeのプロセスIDと一致する ・**スナップショット名** : ***UserData¥InstallDeviceID¥DeviceInstanceID*** ※ 一度同様のスナップショットをマウントしたことがある場合、出力されない可能性がある	
		イベントログ – Sysmon	***イベントID*** : **1**(Process Create) **5**(Process Terminated) ・***Image*** : *"C:¥Windows¥System32¥vssadmin.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ※ シャドウコピー作成対象のドライブなどが記録される ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		実行履歴 – レジストリ	**レジストリエントリ: HKEY_LOCAL_MACHINE¥CurrentControlSet¥Enum¥STORAGE¥VolumeSnapshot¥HarddiskVolumeSnapshot[Snapshot番号]** ・drvinst.exeが実行された場合、新規にキーが作成される	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	volsnap.inf にドライバのインストールが行われたことが差分として残る可能性がある(一度同様のスナップショットをマウントしたことがある場合、出力されない可能性がある)

3.11.1. net user

<基本情報>

ツール	ツール名称	netコマンド (net user)
	カテゴリ	ローカルユーザーの追加・削除、グループの追加・削除
	ツール概要	端末内、又はドメイン上に、ユーザーアカウントを追加する
	攻撃時における想定利用例	侵入した端末にアカウントを作成し、追加のセッションを作成したり、他の端末と通信したりする
動作条件	権限	管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	– ※ ドメインの管理者権限があれば、ドメインコントローラ上にアカウントを作成することも可能
	サービス	–
ログから得られる情報	標準設定	・ユーザーが追加されたことが、ログに記録される
	追加設定	・*"net user"*コマンドで指定されたユーザー名及びパスワードが記録される(Sysmon)
実行成功時に確認できる痕跡		イベントログに以下のログがある場合、ユーザが追加されたと考えられる ・イベントログ「セキュリティ」にイベントID **4720**が記録されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 (Windows)	イベントログ – セキュリティ	***イベントID*** : **4688** (新しいプロセスが作成されました) **4689** (プロセスが終了しました) ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥net.exe"* *"C:¥Windows¥System32¥net1.exe"* ※ net.exeが実行された後、子プロセスとしてnet1.exeが実行される **・確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格*** の種類 ※ 管理者権限が必要なため、1又は2となる ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4656** (SAM - オブジェクトに対するハンドルが要求されました) ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥lsass.exe"* ・***オブジェクト*** -> ***オブジェクトの種類*** : *"SAM_DOMAIN"* **・確認できる情報** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドル ID*** ※ 他ログとの関連付けに使用する ・**要求された処理**: ***アクセス要求情報*** -> ***アクセス*** (*"ReadPasswordParameters"*・*"CreateUser"*・*"LookupIDs"*) ・**成否**: ***キーワード*** (*"成功の監査"*)	
			イベントID : **4720** (ユーザー アカウントが作成されました) ・***新しいアカウント*** -> ***アカウント名*** : "net user"コマンドで指定したユーザー名 **・確認できる情報** ・**ユーザーのグループ**: ***属性*** -> ***プライマリ グループ ID*** ※ 実行した処理内容により、異なるイベント(**4722**, **4724**, **4726**, **4737**, **4738** など)が記録される	
		イベントログ – Sysmon	***イベントID*** : **1** (Process Create) **5** (Process Terminated) ・***Image*** : *"C¥Windows¥System32¥net.exe"* *"C:¥Windows¥System32¥net1.exe"* **・確認できる情報** ・**プロセスの開始・終了日時(UTC)**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 引数内に**ユーザーを追加したこと(user /add)**及び**ユーザー名とパスワード(引数に渡した場合)**が記録される ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要

<備考>

記載のもの以外で出力される可能性のあるイベントログ	グループへの追加などを実施している場合、それに関連するアクセス履歴が記録される

3.12.1. net use

<基本情報>

ツール	ツール名称	netコマンド (net use)
	カテゴリ	ファイル共有
	ツール概要	ネットワーク上で公開されている共有ポイントに接続する
	攻撃時における想定利用例	共有ポイントを経由して攻撃中に使用するツールを送り込んだり、ファイルサーバーから情報を取得したりする ・接続元： netコマンド実行元 ・接続先： netコマンドによってアクセスされた端末
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	445/tcp
	サービス	接続先： Server、接続元： Workstation
ログから得られる情報	標準設定	–
	追加設定	・接続元： 実行履歴（Sysmon・監査ポリシー） ・接続先： Windowsフィルターリング プラットフォームの記録は残るが、具体的に接続されたパスを確認するには読み取りに対する監査が必要 ※共有に対して書き込みがされた場合は、書き込みに対する監査で記録される
実行成功時に確認できる痕跡		・接続元： イベントログに以下のログがある場合、ファイル共有が行われた可能性がある ・イベントログ「セキュリティ」にnet.exeのイベントID **4689** （プロセスが終了しました）が記録され、実行結果（戻り値）が"0x0"となっている

凡例
・**取得出来る情報**
・**イベントID・項目名**
・***フィールド名***
・*"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows ユーザー	接続元	イベントログ – セキュリティ	***イベントID*** : **4688** （新しいプロセスが作成されました） **4689** （プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥net.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **5156** （Windows フィルターリング プラットフォームで、接続が許可されました） ・***ネットワーク情報*** -> ***方向*** : *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** : *"[共有ポイントとして指定したホスト]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** : *"445"・"6"* (TCP) ・**確認できる情報** ・**送信元ポート**: ***ネットワーク情報*** -> ***ソース ポート***	
		実行履歴 – Sysmon	***イベントID*** : **1** (Process Create) **5** (Process Terminated) ・***Image*** : *"C¥Windows¥System32¥net.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時(UTC)**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 引数内に**接続先ホスト**と**共有パス**が記録される ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
	接続先	イベントログ – セキュリティ	***イベントID*** : **5156** （Windows フィルターリング プラットフォームで、接続が許可されました） ・***ネットワーク情報*** -> ***方向*** : *"着信"* ・***ネットワーク情報*** -> ***送信元アドレス*** : *"[ファイルサーバのIPアドレス]"* ・***ネットワーク情報*** -> ***ソース ポート・プロトコル*** : *"445"・"6"* (TCP) ・**確認できる情報** ・**接続元ホスト**: ***ネットワーク情報*** -> ***宛先アドレス*** ・**送信元ポート**: ***ネットワーク情報*** -> ***宛先ポート*** ※ 接続元における、送信元ポートと一致する	必要
	Active Directory ドメイン コントローラ	イベントログ – セキュリティ	***イベントID*** : **4624** （アカウントが正常にログオンしました） ・***ログオン タイプ*** : *"3"* ・***ネットワーク情報*** -> ***ソース ネットワーク アドレス*** : *"[イベント **5156** における、**宛先アドレス**]"* ・***ネットワーク情報*** -> ***ソース ポート*** : *"[イベント **5156** に記録された、**宛先ポート**]"* ・**確認できる情報** ・**使用されたユーザー**: ***新しいログオン*** -> ***アカウント名・アカウント ドメイン***	必要

<備考>

記載のもの以外で出力される可能性のあるイベントログ	・読み取りアクセスを監査対象に含めると、接続された共有パスがイベント**5140**（ファイルの共有）に記録される ・共有に対して書き込みが発生した場合、オブジェクトアクセスの監査に記録される

3.12.2. net share

<基本情報>

ツール	ツール名称	netコマンド (net share)
	カテゴリ	ファイル共有
	ツール概要	特定のフォルダを、ネットワーク経由で利用可能となるよう共有する
	攻撃時における想定利用例	侵入したホスト上で共有パスを作成し、ファイルを読み書きする
動作条件	権限	管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	– ※ 共有されたパスの利用はネットワーク経由でおこなうが、"net share"により共有を追加する際には端末内で完結する
	サービス	Server
ログから得られる情報	標準設定	・レジストリ上に共有パスの情報が残る可能性がある ※ ファイル共有が無効化されると値は消去される
	追加設定	・実行履歴(Sysmon・監査ポリシー) ※ 共有されたパスと、使用された共有名が記録される
実行成功時に確認できる痕跡		イベントログに以下のログがある場合、共有フォルダが作成されたと判断出来る ・イベントログ「セキュリティ」にイベントID **5142** が記録されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 (Windows)	イベントログ – セキュリティ	***イベントID*** : **4688** (新しいプロセスが作成されました) **4689** (プロセスが終了しました) ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥net.exe"* *"C:¥Windows¥System32¥net1.exe"* ※ net.exeが実行された後、子プロセスとしてnet1.exeが実行される **・確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格*** の種類 ※ 管理者権限が必要なため、1又は2となる ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **5142** (ネットワーク共有オブジェクトが追加されました) **・確認できる情報** ・**共有名**: ***共有情報*** -> ***共有名*** ・**共有に使用されたフォルダ**: ***共有パス***	
		イベントログ – Sysmon	***イベントID*** : **1** (Process Create) **5** (Process Terminated) ・***Image*** : *"C¥Windows¥System32¥net.exe"* *"C:¥Windows¥System32¥net1.exe"* **・確認できる情報** ・**プロセスの開始・終了日時(UTC)**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 引数に、**共有名**や**共有に使用されたフォルダ**が記録される ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		アクセス履歴 – レジストリ	**レジストリエントリ: HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥LanmanServer¥Shares¥Security¥[共有名]$** ※ ファイル共有が有効化されると作成される (無効化されると値は消去される) 共有が無効化されると値が消去されるため、常時レジストリを監視するような仕組みが無ければ検知は困難	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.12.3. icacls

<基本情報>

ツール	ツール名称	icacls
	カテゴリ	ファイル共有
	ツール概要	ファイルのアクセス権を変更する
	攻撃時における 想定利用例	・使用されているアカウントで読み取れないファイルを、読み取れるように権限を変更する ・攻撃者が作成したファイルの内容が閲覧できなくなるよう、権限を剥奪する
動作条件	権限	標準ユーザー ※ ACL変更時にはそのファイルに対する適切な権限が必要
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから 得られる情報	標準設定	実行履歴（Prefetch）
	追加設定	実行履歴（Sysmon・監査ポリシー）
実行成功時に確認できる痕跡		イベントログに以下のログがある場合、ファイルのアクセス権変更が行われたと考えられる ・イベントログ「セキュリティ」にicacls.exeに対するイベントID: **4688**及び**4689**が記録されており、イベントID: **4689**中の***終了状態***が *"0x0"*となっている ※ なお、イベントID: **4688・4689**からは対象ファイルが判断出来ないため、対象の絞り込みにはsysmonのイベントID: 1よりicacls.exeのコマンドラインを併せて確認する必要がある

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加 設定
–	端末 （Windows）	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥icacls.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
		実行履歴 – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"C:¥Windows¥System32¥icacls.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**: ***UtcTime*** ・**プロセスのコマンドライン**: ***CommandLine*** ※ 引数内に**対象ファイル**と**設定された権限**が記録される ・**実行ユーザー名**: ***User*** ・**プロセスID**: ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名 : C:¥Windows¥Prefetch¥ICACLS.EXE-CCAC2A58.pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**: ***Last Run Time***	–

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	–

3.13.1. sdelete

<基本情報>

ツール	ツール名称	sdelete
	カテゴリ	痕跡の削除
	ツール概要	ファイルを複数回上書きしてから削除する
	攻撃時における想定利用例	攻撃の過程において作成されたファイルを、復元不可な状態となるように削除する
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch） ・sdeleteを使用した際の使用許諾契約に同意した旨がレジストリに記録される　※ 過去に利用した事がある場合、標準設定で得られるレジストリ情報からは判断できない
	追加設定	・実行履歴（Sysmon・監査ポリシー） ・オブジェクトアクセスの監査による、削除対象ファイルを削除・上書きする動作の記録
実行成功時に確認できる痕跡		・以下のような名前のファイルが繰り返し削除されている ・例：削除対象が sdelete.txt の場合、sdeleAAAAAAAAAAAAAAAAAAA.AAA、sdeleZZZZZZZZZZZZZZZZZZZ.ZZZなど

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 （Windows）	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[実行ファイル（sdelete.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時**: ログの日付 ・**プロセスを実行したユーザー名**: ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン**: ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**: ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**: ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[実行ファイル（sdelete.exe）]"* ・**確認できる情報** ・**削除対象のファイル**: ***オブジェクト*** -> ***オブジェクト名*** ※ 上書き削除の過程で、sdeleteは削除対象ファイルの名前に、アルファベットを付与したファイルを作成し、削除する動作を繰り返す （例：削除対象が sdelete.txt の場合、sdeleAAAAAAAAAAAAAAAAAAA.AAAなど） ・**処理内容**: ***アクセス要求情報*** -> ***アクセス*** ※ 同一のオブジェクトに対して、*"DELETE"*や*"WriteDataまたはAddFile"*などが繰り返される ・**成否**: ***キーワード***（*"成功の監査"*）	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[実行ファイル（sdelete.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine***　※ 実行ファイルの他、上書き回数など、sdelete.exeに渡されたオプションが分かる ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		実行履歴 – Prefetch	**ファイル名： C:¥Windows¥Prefetch¥[実行ファイル（SDELETE.EXE）]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** : ***Last Run Time***	–
		実行履歴 – レジストリ	**レジストリエントリ: HKEY_USERS¥[SID]¥Software¥Sysinternals¥Sdelete** ・初めて利用した場合、**使用許諾契約に同意した旨**が ***EulaAccepted*** に記録される ・過去に端末上でsdeleteを利用した事がある場合、この項目からは区別できない	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.13.2. timestomp

<基本情報>

ツール	ツール名称	timestomp
	カテゴリ	痕跡の削除
	ツール概要	ファイルのタイムスタンプを変更する
	攻撃時における想定利用例	攻撃者が利用したことでタイムスタンプに変更が発生したファイルについて、タイムスタンプを戻すことで、ファイルに対してアクセスしたことを隠蔽する
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	–
	サービス	–
ログから得られる情報	標準設定	・実行履歴（Prefetch）
	追加設定	・実行履歴（Sysmon・監査ポリシー） ・ファイル作成日時に対する変更の監査
実行成功時に確認できる痕跡		イベントログに以下のログがある場合、タイムスタンプが変更されたと考えられる ・イベントログ「セキュリティ」にイベントID **4663**が記録されており、対象ファイルに対する *"WriteAttributes"* の ***キーワード*** が *"成功の監査"* となっている

凡例
・**取得出来る情報**
・**イベントID・項目名**
・***フィールド名***
・*"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
–	端末 （Windows）	イベントログ – セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（timestomp.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4656**（オブジェクトに対するハンドルが要求されました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（timestomp.exe）]"* ・**確認できる情報** ・**対象ファイル**: ***オブジェクト*** -> ***オブジェクト名*** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドルID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス***（*"SYNCHRONIZE"*、*"ReadAttributes"*、*"WriteAttributes"*） ・**成否**: ***キーワード***（*"成功の監査"*）	
			イベントID : **4663**（オブジェクトへのアクセスが試行されました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（timestomp.exe）]"* ・**確認できる情報** ・**対象ファイル**: ***オブジェクト*** -> ***オブジェクト名*** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドルID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス***（*"WriteAttributes"*） ・**成否**: ***キーワード***（*"成功の監査"*）	
			イベントID : **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[検体（timestomp.exe）]"* ・**確認できる情報** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドルID*** ※ 先に出力される、イベント**4663**及び**4656**で記録される***ハンドルID***と同じ	
		イベントログ – Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[検体（timestomp.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** : *UtcTime* ・**プロセスのコマンドライン** : *CommandLine* ※ コマンドライン内の引数に、**対象ファイル**、**変更対象のプロパティ**、**変更後のタイムスタンプ**が記録される ・**実行ユーザ名** : *User*	必要
			イベントID : **2**（File creation time changed） ・***Image*** : *"[検体（timestomp.exe）]"* ・**確認できる情報** ・**変更が発生した日時（UTC）**: *UtcTime* ・**変更されたファイル名**: *TargetFilename* ・**変更後のタイムスタンプ（UTC）**: *CreationUtcTime* ・**変更前のタイムスタンプ（UTC）**: *PreviousCreationUtcTime* ※ イベント**2** はファイル作成日時の変更を示すが、変更されたタイムスタンプの種類（作成・変更・アクセス）に関わらず出力される 作成日時以外の項目を変更した場合、変更前後のタイムスタンプには同じ時間（元の日時）が記録される ※ 作成日時以外のタイムスタンプは、イベントログには記録されない	
			イベントID : **9**（RawAccessRead detected – ディスクの直接読み取りを検知） ・***Image*** : *"[検体（timestomp.exe）]"* ・**確認できる情報** ・**対象ファイルが存在するデバイス名**: ***Device***（*"¥Device¥HarddiskVolume2"*）	
		実行履歴 – Prefetch	**ファイル名：C:¥Windows¥Prefetch¥[検体（TIMESTOMP.EXE）]–[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** : *Last Run Time*	–

<備考>

記載のもの以外で出力される可能性のあるイベントログ	–

3.14.1. wevtutil

<基本情報>

ツール	ツール名称	wevtutil
	カテゴリ	イベントログの削除
	ツール概要	Windowsのイベントログを削除する
	攻撃時における想定利用例	攻撃の痕跡を削除する ・接続元： wevtutilコマンド実行元 ・接続先： wevtutilコマンドによってアクセスされた端末
動作条件	権限	管理者ユーザー
	対象OS	Windows
	ドメインへの参加	不要
	通信プロトコル	135/tcp
	サービス	Event Log
ログから得られる情報	標準設定	・イベントログが消去されたことが、消去されたホストの各ログに残る
	追加設定	・ログ消去に使用されたアカウントと、消去コマンドが実行されたホストが確認可能
実行成功時に確認できる痕跡		・接続元： イベントログに以下のログがある場合、ログが消去されたこと考えられる ・各対象のイベントログにイベントID: **104** が記録されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows 管理者ユーザー	接続元	イベントログ － セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥wevtutil.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザーのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格*** の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	必要
			イベントID : **4648**（明示的な資格情報を使用してログオンが試行されました） ・***プロセス情報*** -> ***プロセス名*** : *"C:¥Windows¥System32¥wevtutil.exe"* ・***プロセス情報*** -> ***プロセスID*** : イベント**4688**で記録されたプロセスIDと同じ ・**確認できる情報** ・**ローカルアカウント**: ***サブジェクト*** -> ***アカウント名・アカウント ドメイン*** ・**接続先で使用されたアカウント**: ***資格情報が使用されたアカウント*** -> ***アカウント名・アカウント ドメイン*** ・**接続先ホスト**: ***ターゲット サーバー*** -> ***ターゲット サーバー名***	
		イベントログ － Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"C:¥Windows¥System32¥wevtutil.exe"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		イベントログ － 各対象ログ	***イベントID*** : **104**（*[対象]* ログ ファイルが消去されました） ・**確認できる情報** ・**実行したユーザー**: ***詳細*** タブ -> ***UserData¥SubjectUserName・SubjectDomainName*** ・**対象ログ名**: ***詳細*** タブ -> ***UserData¥Channel***	－
	接続先	イベントログ － セキュリティ	***イベントID*** : **4672**（新しいログオンに特権が割り当てられました） ・**確認できる情報** ・**権限が昇格したアカウント**: ***サブジェクト*** -> ***アカウント名・アカウント ドメイン*** ・**利用可能な特権**: ***特権***（*"SeSecurityPrivilege"・"SeRestorePrivilege"・"SeTakeOwnershipPrivilege"・"SeDebugPrivilege"・"SeSystemEnvironmentPrivilege"・"SeLoadDriverPrivilege"・"SeImpersonatePrivilege"・"SeEnableDelegationPrivilege"*）	必要
			イベントID : **4624**（アカウントが正常にログオンしました） ・***ログオン タイプ***: *"3"* ・**確認できる情報** ・**使用されたセキュリティID**: ***新しいログオン*** -> ***セキュリティID*** ・**アカウント**: ***アカウント名・アカウント ドメイン*** ・**ログオンを要求したホスト**: ***ネットワーク情報*** -> ***ソース ネットワーク アドレス***	

<備考>

記載のもの以外で出力される可能性のあるイベントログ	－

3.15.1. csvde

<基本情報>

ツール	ツール名称	csvde
	カテゴリ	アカウント情報の取得
	ツール概要	Active Directory上のアカウント情報をCSV形式で出力する
	攻撃時における想定利用例	存在するアカウントの情報を抽出し、攻撃対象として利用可能なユーザーやクライアントを選択する ・接続元： csvdeコマンド実行元 ・接続先： csvdeコマンドによって情報が収集された端末
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要 ※ 正しい認証情報を入力すれば、ドメインに参加していない端末からリモートで情報を取得することも可能
	通信プロトコル	389/tcp
	サービス	Active Directory Domain Services
ログから得られる情報	標準設定	・接続元： 実行履歴（Prefetch）
	追加設定	・接続元： csvde.exeにより、CSVファイルが作成されたこと CSVファイル作成時の一時ファイルとして、*"C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥csv[ランダム数字].tmp"*が作成されたこと ・接続先： 389/tcpの着信と、Kerberosによるログインが記録される
実行成功時に確認できる痕跡		・接続元： csvde.exeが実行されており、"-f"オプションで指定されたファイルが作成されている ・"C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥csv[ランダム数字].tmp"が作成、削除されている

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows Server ドメインユーザー	接続元	イベントログ － セキュリティ	***イベントID***： **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名***： *"[実行ファイル（csvde.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時**： ログの日付 ・**プロセスを実行したユーザー名**： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザのドメイン**： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無**： ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値**： ***プロセス情報*** -> ***終了状態***	必要
			イベントID： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名***： *"[実行ファイル（csvde.exe）]"* ・***ネットワーク情報*** -> ***方向***： *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス***： *"[ドメインコントローラのIPアドレス]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル***： *"389"・"6"*（TCP） ・**確認できる情報** ・**接続元ポート**： ***ソース ポート*** ※ ドメインコントローラ側ログとの紐付けに使用する	
			イベントID： **4663**（オブジェクトへのアクセスが試行されました） **4656**（オブジェクトへのハンドルが要求されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名***： *"[実行ファイル（csvde.exe）]"* ・**確認できる情報** ・**対象のファイル**： ***オブジェクト*** -> ***オブジェクト名***（*"C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥csv[ランダム数字].tmp"*） ・**ハンドルID（他ログとの紐付けに使用する）**： ***オブジェクト*** -> ***ハンドルID*** ・**処理内容**： ***アクセス要求情報*** -> ***アクセス***（*"SYNCHRONIZE"・"WriteData（またはAddFile）"・"AppendData（またはAddSubdirectoryまたはCreatePipeInstance）"・"WriteEA"・* ・**成否**： ***キーワード***（*"成功の監査"*）	
			イベントID： **4663**（オブジェクトへのアクセスが試行されました） **4656**（オブジェクトへのハンドルが要求されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名***： *"[実行ファイル（csvde.exe）]"* ・***オブジェクト*** -> ***オブジェクト名***： *"[csvde.exe 実行時に "-f" オプションで指定したファイル]"* ・**確認できる情報** ・**ハンドルID（他ログとの紐付けに使用する）**： ***オブジェクト*** -> ***ハンドルID*** ・**処理内容**： ***アクセス要求情報*** -> ***アクセス***（*"WriteDataまたはAddFile"・"AppendDataまたはAddSubdirectoryまたはCreatePipeInstance"*） ・**成否**： ***キーワード***（*"成功の監査"*）	
			イベントID： **4663**（オブジェクトへのアクセスが試行されました） **4656**（オブジェクトへのハンドルが要求されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名***： *"[実行ファイル（csvde.exe）]"* ・***オブジェクト*** -> ***オブジェクト名***（*"C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥csv[ランダム数字].tmp"*） ・**確認できる情報** ・**ハンドルID**： ***オブジェクト*** -> ***ハンドルID*** ※ 他のログとの紐付けに使用する ・**処理内容**： ***アクセス要求情報*** -> ***アクセス***（*"DELETE"*） ・**成否**： ***キーワード***（*"成功の監査"*）	
		イベントログ － Sysmon	***イベントID***： **1**（Process Create） **5**（Process Terminated） ・***Image***： *"[実行ファイル（csvde.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**： ***UtcTime*** ・**プロセスのコマンドライン**： ***CommandLine*** ※ ユーザやファイル名を指定した場合、引数が記録される ・**実行ユーザー名**： ***User*** ・**プロセスID**： ***ProcessId***	必要
		実行履歴 － Prefetch	**ファイル名： C:¥Windows¥Prefetch¥[実行ファイル（CSVDE.EXE）]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**： ***Last Run Time***	－
	接続先	イベントログ － セキュリティ	***イベントID***： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名***： *"¥device¥harddiskvolume2¥windows¥system32¥lsass.exe"* ・***ネットワーク情報*** -> ***方向***： *"着信"* ・***ネットワーク情報*** -> ***ソース ポート・プロトコル***： *"389"・"6"*（TCP） ・***ネットワーク情報*** -> ***宛先ポート***： *"[csvde.exe を実行したクライアントで記録された **ソース ポート**]"* ・**確認できる情報** ・**接続元ホスト**： ***宛先ポート***	必要
			イベントID： **4624**（アカウントが正常にログオンしました） **4634**（アカウントがログオフしました） ・***ログオン タイプ***： *"3"* ・***ネットワーク情報*** -> ***ソース ネットワーク アドレス***： *"[イベント **5156** における、**宛先アドレス**]"* ・***ネットワーク情報*** -> ***ソース ポート***： *"[イベント **5156** に記録された、**宛先ポート**]"* ・**確認できる情報** ・**使用されたユーザー**： ***新しいログオン*** -> ***アカウント名・アカウント ドメイン*** ・**新しいログオンID**： ***新しいログオン*** -> ***ログオンID*** ※ 他のログとの紐付けに使用する	

<備考>

記載のもの以外で出力される 可能性のあるイベントログ	–

3.15.2. ldifde

<基本情報>

ツール	ツール名称	ldifde
	カテゴリ	アカウント情報の取得
	ツール概要	AD上のアカウント情報をLDIF形式で出力する
	攻撃時における想定利用例	存在するアカウントの情報を抽出し、攻撃対象として利用可能なユーザーやクライアントを選択する ・接続元： ldifdeコマンド実行元 ・接続先： ldifdeコマンドによって情報が収集された端末
動作条件	権限	標準ユーザー
	対象OS	Windows
	ドメインへの参加	不要 ※正しい認証情報を入力すれば、ドメインに参加していない端末からリモートで情報を取得することも可能
	通信プロトコル	389/tcp
	サービス	Active Directory Domain Services
ログから得られる情報	標準設定	・接続元： 実行履歴（Prefetch）
	追加設定	・接続元： ldifde.exeにより、LDIFファイルが作成されたことが記録される ・接続先： 389/tcpの着信と、Kerberosによるログインが記録される
実行成功時に確認できる痕跡		・接続元： ldifde.exeが実行されており、"-f"オプションで指定されたファイルが作成されている

凡例
・**取得出来る情報**
・**イベントID・項目名**
・***フィールド名***
・*"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows Server ドメインユーザー	接続元	イベントログ － セキュリティ	***イベントID*** : **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** : *"[実行ファイル（ldifde.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時** : ログの日付 ・**プロセスを実行したユーザー名** : ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザのドメイン** : ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** : ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** : ***プロセス情報*** -> ***終了状態***	－
			イベントID : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** : *"[実行ファイル（ldifde.exe）]"* ・***ネットワーク情報*** -> ***方向*** : *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** : *"[ドメインコントローラのIPアドレス]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** : *"389"・"6"*（TCP） ・**確認できる情報** ・**接続元ポート**: ***ソース ポート*** ※ ドメインコントローラ側ログとの紐付けに使用する	
			イベントID : **4656**（オブジェクトへのハンドルが要求されました） **4663**（オブジェクトへのアクセスが試行されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** : *"[実行ファイル（ldifde.exe）]"* ・***オブジェクト*** -> ***オブジェクト名*** : *"[ldifde.exe 実行時に "-f" オプションで指定したファイル]"* ・**確認できる情報** ・**ハンドルID**: ***オブジェクト*** -> ***ハンドルID*** ※ 他ログとの紐付けに使用する ・**処理内容**: ***アクセス要求情報*** -> ***アクセス***（*"WriteDataまたはAddFile"・"AppendDataまたはAddSubdirectoryまたはCreatePipeInstance"*） ・**成否**: ***キーワード***（*"成功の監査"*）	
		イベントログ － Sysmon	***イベントID*** : **1**（Process Create） **5**（Process Terminated） ・***Image*** : *"[実行ファイル（ldifde.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）** : ***UtcTime*** ・**プロセスのコマンドライン** : ***CommandLine*** ※ ユーザーやファイル名を指定した場合、引数が記録される ・**実行ユーザ名** : ***User*** ・**プロセスID** : ***ProcessId***	必要
		実行履歴 － Prefetch	**ファイル名： C:¥Windows¥Prefetch¥[実行ファイル（LDIFDE.EXE）]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時** : ***Last Run Time***	－
	接続先	イベントログ － セキュリティ	***イベントID*** : **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** : *"¥device¥harddiskvolume2¥windows¥system32¥lsass.exe"* ・***ネットワーク情報*** -> ***方向*** : *"着信"* ・***ネットワーク情報*** -> ***ソース ポート・プロトコル*** : *"389"・"6"*（TCP） ・***ネットワーク情報*** -> ***宛先ポート*** : *"[ldifde.exe を実行したクライアントで記録された **ソース ポート**]"* ・**確認できる情報** ・**接続元ホスト**: ***宛先ポート*** ・**成否**: ***キーワード***	必要
			イベントID : **4624**（アカウントが正常にログオンしました） ・***ログオン タイプ***: *"3"* ・***ネットワーク情報*** -> ***ソース ネットワーク アドレス*** : *"[イベント **5156** における、**宛先アドレス**]"* ・***ネットワーク情報*** -> ***ソース ポート*** : *"[イベント **5156** に記録された、**宛先ポート**]"* ・**確認できる情報** ・**使用されたユーザ**: ***新しいログオン*** -> ***アカウント名・アカウント ドメイン*** ・**新しいログオンID**: ***新しいログオン*** -> ***ログオンID*** ※ 他ログとの紐付けに使用	
			イベントID : **4634**（アカウントがログオフしました） ・***サブジェクト*** -> ***アカウント名・アカウント ドメイン・ログオンID*** : *"[イベント **4624** で記録されたものと同じ]"*	

<備考>

記載のもの以外で出力される可能性のあるイベントログ	－

3.15.3. dsquery

<基本情報>

ツール	ツール名称	dsquery
	カテゴリ	アカウント情報の取得
	ツール概要	ディレクトリサービスより、ユーザーやグループなどの情報を取得する
	攻撃時における想定利用例	存在するアカウントの情報を抽出し、攻撃対象として利用可能なユーザーやクライアントを選択する ・接続元： dsqueryコマンド実行元 ・接続先： dsqueryコマンドによって情報が収集された端末
動作条件	権限	標準ユーザー ※ACLの設定によって、標準ユーザー権限では取得出来ない情報が存在する
	対象OS	Windows
	ドメインへの参加	不要 ※ 本調査はドメインコントローラ上で実施 正しい認証情報を入力すれば、ドメインに参加していない端末からリモートで情報を取得することも可能
	通信プロトコル	389/tcp
	サービス	Active Directory Domain Services
ログから得られる情報	標準設定	・接続元： 実行履歴（Prefetch）
	追加設定	・接続元： 実行履歴（Sysmon・監査ポリシー） ・接続先： 389/tcpの着信と、Kerberosによるログインが記録される
実行成功時に確認できる痕跡		イベントログ、実行履歴等では判断できない　※ 抽出したアカウント情報が保存されている場合は、成功したと判断できる

凡例
- **取得出来る情報**
- **イベントID・項目名**
- ***フィールド名***
- *"フィールドの値"*

<確認ポイント>

通信	ログの生成場所	ログ種別・名称	取得情報の詳細	追加設定
OS：Windows ユーザー ↓ OS：Windows Server ユーザー	接続元	イベントログ － セキュリティ	***イベントID*** ： **4688**（新しいプロセスが作成されました） **4689**（プロセスが終了しました） ・***プロセス情報*** -> ***プロセス名*** ： *"[実行ファイル（dsquery.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時** ： ログの日付 ・**プロセスを実行したユーザー名** ： ***サブジェクト*** -> ***アカウント名*** ・**プロセスを実行したユーザのドメイン** ： ***サブジェクト*** -> ***アカウント ドメイン*** ・**プロセス実行時の権限昇格の有無** ： ***プロセス情報*** -> ***トークン昇格***の種類 ・**プロセスの戻り値** ： ***プロセス情報*** -> ***終了状態***	必要
			イベントID ： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** ： *"[実行ファイル（dsquery.exe）]]"* ・***ネットワーク情報*** -> ***方向*** ： *"送信"* ・***ネットワーク情報*** -> ***宛先アドレス*** ： *"[ドメインコントローラのIPアドレス]"* ・***ネットワーク情報*** -> ***宛先ポート・プロトコル*** ： *"389"・"6"*（TCP） ・**確認できる情報** ・**接続元ポート**： ***ソース ポート***　※ ドメインコントローラ側ログとの紐付けに使用する	
			イベントID ： **4663**（オブジェクトへのアクセスが試行されました） **4656**（オブジェクトへのハンドルが要求されました） **4658**（オブジェクトに対するハンドルが閉じました） ・***プロセス情報*** -> ***プロセス名*** ： *"[実行ファイル（dsquery.exe）]"* ・***オブジェクト*** -> ***オブジェクト名*** ： *"C:¥Users¥[ユーザー名]¥AppData¥Local¥Mirosoft¥Windows¥SchCache¥[ドメイン名].sch"* ・**確認できる情報** ・**ハンドルID**： ***オブジェクト***内、***ハンドルID***　※ 他ログとの紐付けに使用する ・**処理内容**： ***アクセス要求情報***内、***アクセス***（*"WriteDataまたはAddFile"*・*"AppendDataまたはAddSubdirectoryまたはCreatePipeInstance"*） ・**成否**： ***キーワード***（*"成功の監査"*） ※ イベントID **4656**・**4663**・**4658**は、既に有効なschファイルが存在する場合は出力されない可能性がある	
		イベントログ － Sysmon	***イベントID*** ： **1**（Process Create） **5**（Process Terminated） ・***Image*** ： *"[実行ファイル（dsquery.exe）]"* ・**確認できる情報** ・**プロセスの開始・終了日時（UTC）**： ***UtcTime*** ・**プロセスのコマンドライン**： ***CommandLine***　※ ユーザやファイル名を指定した場合、引数が記録される ・**実行ユーザー名**： ***User*** ・**プロセスID**： ***ProcessId***	必要
		実行履歴 － Prefetch	**ファイル名： C:¥Windows¥Prefetch¥[実行ファイル（DSQUERY.EXE）]-[文字列].pf** ・**確認できる情報**（ツールを利用して下記を確認できる ツール：WinPrefetchView） ・**最終実行日時**： ***Last Run Time***	－
	接続先	イベントログ － セキュリティ	***イベントID*** ： **5156**（Windows フィルターリング プラットフォームで、接続が許可されました） ・***アプリケーション情報*** -> ***アプリケーション名*** ： *"¥device¥harddiskvolume2¥windows¥system32¥lsass.exe"* ・***ネットワーク情報*** -> ***方向*** ： *"着信"* ・***ネットワーク情報*** -> ***ソース ポート・プロトコル*** ： *"389"・"6"*（TCP） ・***ネットワーク情報*** -> ***宛先ポート*** ： *"[dsquery.exe を実行したクライアントで記録された **ソース ポート**]"* ・**確認できる情報** ・**接続元ホスト**： ***宛先ポート***	必要
			イベントID ： **4624**（アカウントが正常にログオンしました） **4634**（アカウントがログオフしました） ・***ログオン タイプ***： *"3"* ・***ネットワーク情報*** -> ***ソース ネットワーク アドレス*** ： *"[イベント **5156** における、**宛先アドレス**]"* ・***ネットワーク情報*** -> ***ソース ポート*** ： *"[イベント **5156** に記録された、**宛先ポート**]"* ・**確認できる情報** ・**使用されたユーザー**： ***新しいログオン*** -> ***アカウント名・アカウント ドメイン*** ・**新しいログオンID**： ***新しいログオン*** -> ***ログオンID***　※ 他のログとの紐付けに使用する	

<備考>

記載のもの以外で出力される可能性のあるイベントログ	－

3.16. ツールおよびコマンドの実行成功時に見られる痕跡

下表は、ツールおよびコマンドが実行され、攻撃が成功したことを確認する判断基準を記載する。
なお、ログの詳細に関しては、各シートに記載している。

区分	調査対象	成否の判断
コマンド実行	PsExec	以下が確認できた場合、PsExecが実行された可能性がある ・接続元： イベントログに以下のログがある場合 ・イベントログ「セキュリティ」にpsexec.exeのイベントID **4689**（プロセスが終了しました）が記録され、実行結果（戻り値）が"0x0"となっている ・接続先： PSEXESVC.exeがインストールされている
	wmic	「接続元」「接続先」において、同時刻に以下のログが確認できる場合、リモート接続が行われた可能性がある ・接続元： イベントログに以下のログがある場合 ・イベントログ「セキュリティ」にWMIC.exeのイベントID **4689**（プロセスが終了しました）が記録され、実行結果（戻り値）が"0x0"となっている ・接続先： Sysmonに以下のログがある場合 ・イベントログ「Sysmon」でイベントID **1**、**5**でWmiPrvSE.exeが実行されたことが記録されている
	PowerShell	以下のログが同じ時刻に確認できた場合、リモートコマンド実行が行われた可能性がある ※ Prefetchの場合も同様 ・接続元： イベントログに以下のログがある場合 ・イベントログ「セキュリティ」にPowerShellのイベントID **4689**（プロセスが終了しました）が記録され、実行結果（戻り値）が"0x0"となっている ・接続先： イベントログに以下のログがある場合 ・イベントログ「セキュリティ」にwsmprovhost.exeのイベントID **4689**（プロセスが終了しました）が記録され、実行結果（戻り値）が"0x0"となっている
	wmiexec.vbs	・接続先： "WMI_SHARE"共有が作成され、削除されている
	BeginX	・接続元： 接続先で意図せず許可されているポートと通信をしたことが記録されている ・接続先： 意図しない通信がWindows Firewallで許可されており、該当のポートでリッスンしている検体が存在する
	WinRM	・接続元： 以下のログがある場合、WinRMが実行された可能性がある ・イベントログ「Sysmon」のイベントID:**1**、**5**でcscript.exeが接続先にアクセスしたログが記録されている
	WinRS	・イベントログ「アプリケーションとサービス¥Microsoft¥Windows¥Windows Remote Management¥Operational」に、WinRSの実行が記録されている
	at	・接続元： イベントログに以下のログがある場合、タスクが登録されたと考えられる ・イベントログ「セキュリティ」にat.exeのイベントID **4689**（プロセスが終了しました）が記録され、実行結果（戻り値）が"0x0"となっている ・接続先： イベントログに以下のログがある場合、タスクが実行されていると考えられる ・イベントログ「¥Microsoft¥Windows¥TaskScheduler¥Operational」にイベントID **106**（タスクが登録されました）が記録されている ・イベントログ「¥Microsoft¥Windows¥TaskScheduler¥Operational」にイベントID **200**（開始された操作）、**201**（操作が完了しました）が記録され、イベントID **201**における戻り値が成功となっている
	BITS	イベントログに以下のログがある場合、ファイルの転送が行われたと考えられる ・イベントログ「アプリケーションとサービスログ¥Microsoft¥Windows¥Bits-Client」にイベントID: **60**が記録されており、状態コードが"0x0"となっている
パスワード、ハッシュの入手	PWDump7	–
	PWDumpX	・接続元： "[検体のパス]¥[宛先アドレス]-PWHashes.txt"が作成されている場合、実行が成功したものと考えられる
	Quarks PwDump	・一時ファイル（"SAM-[ランダム数字].dmp"）が作成され、削除されている
	mimikatz （パスワードハッシュ入手）	–
	mimikatz （チケット入手）	・チケットを出力したファイルが生成された場合、処理が成功したものと考えられる
	WCE	・"C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥wceaux.dll"ファイルが作成、削除されている
	gsecdump	–
	lslsass	–
	Find-GPOPasswords.ps1	・パスワードをダンプした結果のファイル（GPPDataReport-[ドメイン名]-[日時].csv）が出力されている
	Mail PassView	※ 抽出したパスワードが保存されている場合は、成功したと判断できる
	WebBrowserPassView	※ 抽出したパスワードが保存されている場合は、成功したと判断できる
	Remote Desktop PassView	※ 抽出したパスワードが保存されている場合は、成功したと判断できる
通信の不正中継 （パケットトンネリング）	Htran	・接続元： イベントログに以下のログがある場合、通信した可能性がある ・イベントログ「セキュリティ」にイベントID **5156**でトンネルホスト・トンネル先ホストとそれぞれ通信したことが記録されている
	Fake wpad	・接続元： 本来プロキシやHTTPサーバーで無いはずのホストと、80/tcp及び8888/tcpによる通信をおこなっている ・接続先： 本来プロキシやHTTPサーバーで無いはずのホストが、80/tcp及び8888/tcpをリッスンしている wpad.dat、proxy.logが作成されている
リモートログイン	RDP	・接続先： イベントログに以下のログがある場合、接続が成功していると考えられる ・イベントログ「セキュリティ」にイベントID: **4624**が記録されている ・イベントログ「Microsoft¥Windows¥TerminalServices-LocalSessionManager¥Operational」にイベントID：**21**、**24**が記録されている
Pass-the-hash, Pass-the-ticket	WCE	・接続元： WCESERVICEがインストール・実行されたことが記録されている ・接続先： リモートホストからログオンしたことが記録されている ・両側： WMIを用いて通信したことが記録されている
	mimikatz	・接続先： イベントログに以下のログがある場合、リモートからログインされていると考えられる ・イベントログ「セキュリティ」にイベントID 4624が記録され、意図しない接続元からアクセスされている
SYSTEM権限に昇格	MS14-058 Exploit	・イベント: **4688**においてSYSTEM権限で実行されているプロセスにおいて、親プロセスが検体やそのプロセスの親となり得ないものとなっている
	MS15-078 Exploit	・イベント: **4688**においてSYSTEM権限で実行されているプロセスにおいて、親プロセスが検体やそのプロセスの親となり得ないものとなっている
権限昇格	SDB UAC Bypass	・親プロセス名に、本来は親プロセスとならないことが想定されるアプリケーションを含む、プロセスが実行されたことが記録されている
ドメイン管理者権限、 アカウントの奪取	MS14-068 Exploit	・接続先： イベントログ「セキュリティ」のイベントID 4672において、標準ユーザーに対して上位の特権が認可されている
	Golden Ticket （mimikatz）	・接続先： イベントログに以下のログがある場合、不正ログオンが実行されていると考えられる ・イベントログ「セキュリティ」のイベントID 4672、4624、4634で、不正なドメインを持つアカウントによるログオンが記録されている
	Silver Ticket （mimikatz）	・接続先： イベントログに以下のログがある場合、不正ログオンが実行されていると考えられる ・イベントログ「セキュリティ」のイベントID 4672、4624、4634で、不正なドメインを持つアカウントによるログオンが記録されている
Active Directory データベースの奪取 （ドメイン管理者ユーザーの作成、もしくは管理者グループに追加）	ntdsutil	以下が確認できた場合、情報収集が行われている可能性がある ・ntdsutil.exeが実行され、イベントログに以下のログがある場合 ・イベントログ「セキュリティ」にイベントID: **8222**が記録されている ・オブジェクト *"[システムドライブ]¥SNAP_[日時]_VOLUME[ドライブレター]$"* に対するハンドルの要求が成功している ※ さらに、通常は読み出せない C:¥Windows¥NTDS 配下のファイルをコピーしたログ（イベントID: **4663**）が記録されている場合、シャドウコピーを利用されている可能性がある
	vssadmin	イベントログに以下のログがある場合、シャドウコピーが作成されたと考えられる ・イベントログ「セキュリティ」にイベントID: **8222**が記録されている ※ さらに、通常は読み出せない C:¥Windows¥NTDS 配下のファイルをコピーしたログ（イベントID: **4663**）が記録されている場合、シャドウコピーを利用されている可能性がある

区分	調査対象	成否の判断
ローカルユーザー ・グループの 追加・削除	net user	・イベントログ「セキュリティ」にイベントID 4720が記録されている
ファイル共有	net use	・接続元： イベントログに以下のログがある場合、ファイル共有が行われた可能性がある ・イベントログ「セキュリティ」にnet.exeのイベントID 4689 （プロセスが終了しました）が記録され、実行結果（戻り値）が"0x0"となっている
	net share	・イベントログ「セキュリティ」にイベントID 5142 が記録されている
	icacls	・イベントログ「セキュリティ」にicacls.exeに対するイベントID: **4688**及び**4689**が記録されており、イベントID: **4689**中の終了状態が"0x0"となっている ※ イベントID: **4688**・**4689**からは対象ファイルが判断出来ないため、対象の絞り込みにはsysmonのイベントID: **1**よりicacls.exeのコマンドラインを併せて確認する必要がある
痕跡の削除	sdelete	・以下のような名前のファイルが繰り返し削除されている ・例： 削除対象が sdelete.txt の場合、sdeleAAAAAAAAAAAAAAAAAAAA.AAA、sdeleZZZZZZZZZZZZZZZZZZZZ.ZZZなど
	timestomp	・イベントログ「セキュリティ」にイベントID 4663が記録されており、対象ファイルに対する"WriteAttributes"のキーワードが"成功の監査"となっている
イベントログの削除	wevtutil	・各対象のイベントログにイベントID: **104** が記録されている
アカウント情報の取得	csvde	・接続元： csvde.exeが実行されており、"-f"オプションで指定されたファイルが作成されている ・"C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥csv[ランダム数字].tmp"が作成、削除されている
	ldifde	・接続元： ldifde.exeが実行されており、"-f"オプションで指定されたファイルが作成されている
	dsquery	※ 抽出した情報が保存されている場合は、成功したと判断できる

4. 追加ログ取得について

本章では、3 章に記載した調査結果から分かったデフォルト設定では取得できない詳細ログ取得の重要性および、追加ログ取得を行うことで考慮すべき事項について説明する。

4.1. 追加ログ取得の重要性

今回の調査で、Windows で標準的に搭載されているツールについては、実行された痕跡がイベントログに残るが、Windows に搭載されていないツールのほとんどについては、実行された痕跡がどこにも残らないことが今回の調査で分かった。例えば、リモートログインのためのツール RDP（Remote Desktop Protocol）の場合にはイベントログ「Microsoft¥Windows¥TerminalServices-LocalSessionManager¥Operational」に、タスク登録用のツール at の場合にはイベントログ「Microsoft¥Windows¥TaskScheduler¥Operational」に、それぞれ実行されたことを示す痕跡が残る。

それに対して、追加ログ取得のために監査ポリシーの有効化および Sysmon のインストールをした環境では、大多数のツールの実行痕跡を取得することが可能であった。例えば、監査ポリシーの設定をすることによって、一時的なファイルが作成されたことをイベントログに記録することができる。そうすると、csvde を利用して、アカウント情報を収集しようとした際に作成された一時ファイル「C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp¥csv[ランダム数字].tmp」がイベントログに記録される。ツールが実行されたことを調査する場合は、詳細なログを取得するために、こうした設定を事前に行っておく必要がある。

なお、詳細なログの取得は、監査ポリシーの有効化および Sysmon のインストールによらずとも、監査ソフトウエア（資産管理ソフトなど）でも可能な場合がある。それらのソフトウエアで、次の Windows OS の動作を監視している場合は、監査ポリシーの有効化や Sysmon のインストールをした環境と同様の記録が残る可能性がある。

- プロセスの実行
- ファイルの書込み

4.2. 追加ログ取得設定の影響

追加ログ取得を行う際に事前に考慮しておく必要がある項目として、ログ量の増加が挙げられる。監査ポリシーを有効化するとログの量が増加するため、ログのローテーションが早くなり古いログが残りにくくなる。そのため、監査ポリシーを有効化する場合は、イベントログの最大サイズの変更もあわせて検討していただきたい。イベントログの最大サイズの変更は、イベントビューアーまたは wevtutil コマンドで変更可能である。

なお、イベントログの最大サイズを変更することで、記憶領域を圧迫する恐れがある。イベントログの最大サイズを変更する場合は、検証した上で実施することを推奨する。

5. インシデント調査における本報告書の活用方法

本章では、本調査報告書の第 3 章を活用したインシデント調査の事例を通じて、インシデント調査の現場における本調査報告書の利用イメージを述べる。

5.1. 本報告書を使用したインシデント調査

第 3 章は、インシデント調査時にどのようなツールが実行された可能性があるのかを調査する際に活用されることを想定して作成した。インシデント調査時に確認された特徴的なイベントログのイベント ID やファイル名、レジストリエントリなどをキーに検索することで、実行された可能性があるツールを探し出すことができる。

インシデント調査時にはイベントログ「セキュリティ」に何か不振なログがないか確認するところから着手することが多い。その確認で、例えば「イベント ID: 4663（オブジェクトへのアクセスが試行されました）」が見つかり、「192.168.100.100-PWHashes.txt」というファイルが一時的に作成された痕跡があったとする（監査ポリシーを有効化している場合、記録される）。この特徴的な「PWHashes.txt」という文字列で第 3 章を検索すると、PWDumpX を実行した際に作成されるファイルであることが分かる。

さらに、3.3.2 節を参照しつつ調査を進めることにより、PWDumpX は攻撃者がパスワードハッシュを入手するために実行するコマンドであり、また、「[宛先アドレス]-PWHashes.txt」という名前の一時ファイルが作成されていたことから、IP アドレス 192.168.100.100 のサーバ上のパスワードハッシュを入手すると言う目的を攻撃者が完遂したと推測されることが分かる。

IP アドレス 192.168.100.100 のサーバを、調査すると「C:¥Windows¥System32¥DumpSvc.exe」というファイルが作成および実行されており、さらにサービス「PWDumpX Service」がインストールされていることが「イベント ID: 7045（サービスがシステムにインストールされました）」として記録されていることを確認することができる。このことから、IP アドレス 192.168.100.100 のパスワードハッシュが攻撃者に入手されていると断定することができる。

3.16 節には各ツールが実行されたことを確認するための方法をまとめている。各ツールで記録される情報を一覧できるので、インシデントの調査に着手するのに先立って、調査戦略を立てるための参考にして欲しい。

6. おわりに

近年、標的型攻撃によって多くの組織が被害にあっていたことが明るみになる中、その被害の詳細を調べるインシデント調査は重要度を増しつつある。本報告書では、そのようなインシデント調査において鍵となる、ツールが実行されたことを示す痕跡情報とツールとの対応関係を整理して示した。

Windows のデフォルト設定のままでは、多くのツールについて実行の痕跡が残らず、インシデント調査も迷宮入りしかねない。攻撃者が何をしたのかをより詳細に分析するためには、デフォルト設定で取得できる以上のログを収集できる環境を事前に整備しておくことが必要である。

ネットワーク内部への侵入を阻止するのが難しい現状においては、インシデント発生後の被害状況調査のためにログの取得方法について日頃から検討し、改善しておくことは、被害拡散防止や事後のセキュリティ対策を検討する上でも重要である。本書で示した Windows の標準機能を利用した追加ログ取得方法に限らず、監査アプリケーションを使用する方法など組織に合わせた対応を検討して備えを固めるとともに、インシデントの発生が疑われる場合には、攻撃者によるツール等の実行痕跡を洗い出すために本報告書を活用していただきたい。深刻化する標的型攻撃を早期に発見し的確に対処するために本報告書が一助となれば幸いである。

7. 付録 A

本章では、Sysmon のインストール方法および監査ポリシーの有効化方法について記載する。なお、監査ポリシーの設定および Sysmon のインストールを行うことで、イベントログの量が増大することを確認している。実際に行う場合は、事前に検証することを推奨する。

7.1. Sysmon のインストール方法

1. 以下のサイトから Sysmon をダウンロードする。

   https://technet.microsoft.com/ja-jp/sysinternals/dn798348

2. 管理者権限でコマンド プロンプトを実行し、以下のコマンドを実行する。

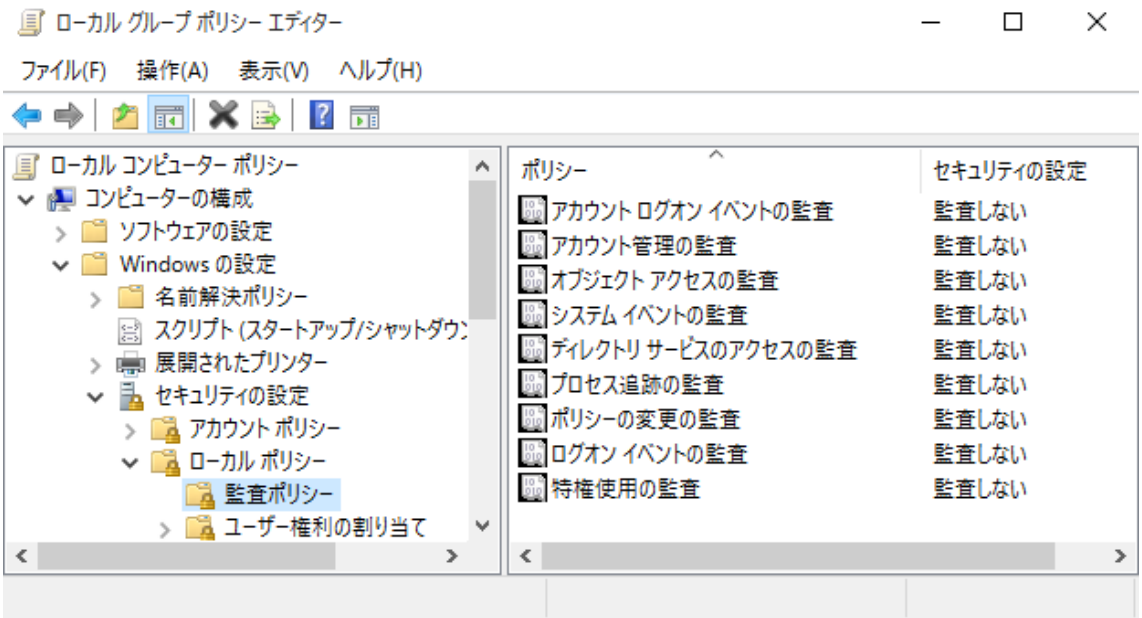
```
> Sysmon.exe -i
```

※ オプション「-n」を追加することで、通信のログを取得できるようになるが、通信に関しては監査ポリシーで対応する。

7.2. 監査ポリシーの有効化方法

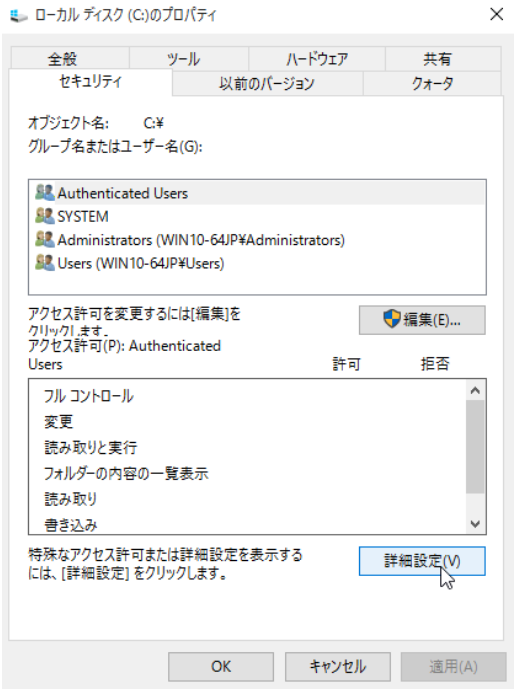
以下では、ローカル コンピュータに対して監査ポリシーを有効にする方法を説明する。なお、以降の設定方法は Windows 10 で設定を行った場合を示す。

1. ローカル グループ ポリシー エディター を開く。([検索] ボックスに「gpedit.msc」と入力し、実行する。)



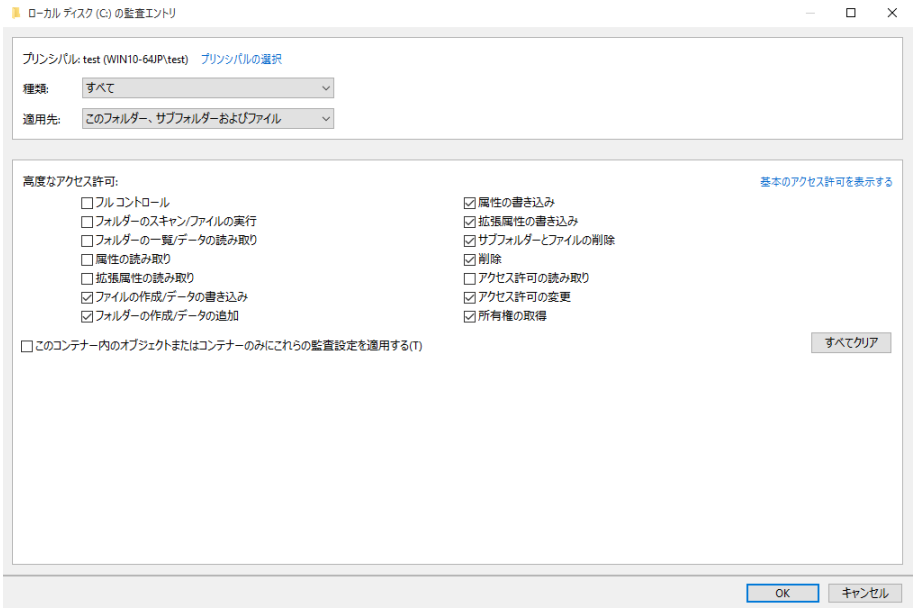
2. [コンピューターの構成]→[Windows の設定]→[セキュリティの設定] →[ローカル ポリシー]→[監査ポリシー]を選択し、各ポリシーの「成功」「失敗」を有効にする。

3. [ローカル ディスク(C:)]→[プロパティ]→[セキュリティ]タブ→[詳細設定]を選択する。



4. [監査]タブから監査対象のオブジェクトを追加する。

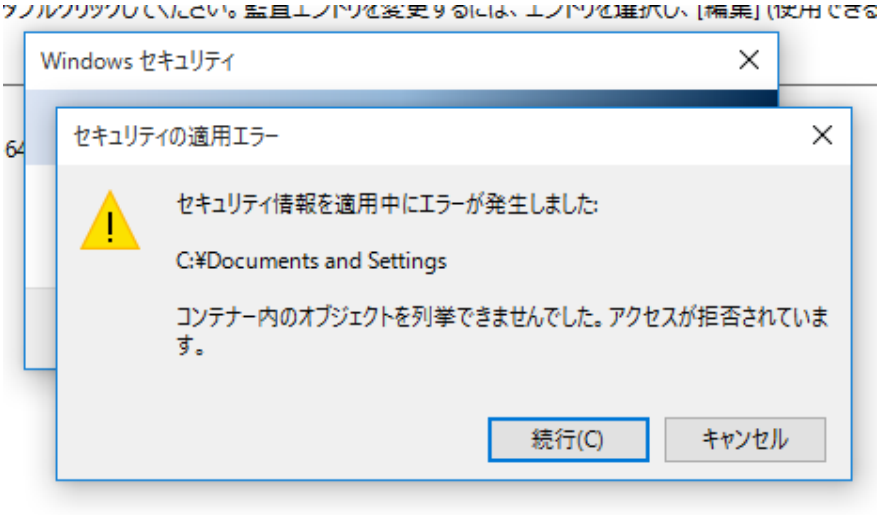
5. 以下のように監査対象のユーザおよび、監査するアクセス方法を選択する。



今回設定した「アクセス許可」は以下の通り。(ファイルの読み取りも記録することで、より詳細な調査が可能になるが、ログの量が増大するため、対象外にしている。)

- ファイルの作成/データ書き込み
- フォルダーの作成/データの追加
- 属性の書き込み
- 拡張属性の書き込み
- サブフォルダーとファイルの削除
- 削除
- アクセス許可の変更
- 所有権の取得

上記設定を行うことで、以下のエラーが多数表示されるが、「続行」する。



8. 付録 B

本一覧には、「初期設定で記録されるログ」および「監査ポリシーの設定およびSysmonのインストールを行うことで追加設定することで記録されるログ」を記載する。
なお、すべての取得可能なログを記載するわけではなく、インシデント調査に活用できるログを抜粋して記載している。

対象	取得可能なログ							
	ログ		入手方法	設定箇所	識別子	イベント名	概要	取得可能な主な情報
全体に共通	Windowsログ	セキュリティ	Windowsの初期設定で記録される		104	ログの消去	ログの消去	・消去されたログのチャンネル
					7036	サービスの状態が移行しました	サービス状態の変動 (実行・停止共に同じイベントID)	・サービス名 ・状態
					7045	サービスがシステムにインストールされました	サービスのインストール	・サービス名 ・実行ファイル名 ・サービスの種類 ・起動タイプ ・サービスアカウント
		システム			20001	デバイスのインストール	デバイスドライバーのインストール	・デバイス インスタンスID ・ドライバー名 ・成否
					8222	シャドウ コピーが作成されました	シャドウコピーの作成	・アカウント名・ドメイン ・シャドウコピーのUUID ・コンピューター名 ・シャドウコピーの作成元 ・作成されたシャドウデバイス名
		セキュリティ （監査ポリシー）	各監査を有効化する。ファイルシステムに対する監査については、SACLの設定も必要。 各ログは、「Windowsログ ＞ セキュリティ」内に保存される。	ログオン/ログオフ ＞ ログオンの監査	4624	アカウントが正常にログオンしました	アカウントのログオン	・セキュリティID ・アカウント名・ドメイン ・ログオンID 他イベントログとの紐付けに使用する ・ログオン タイプ 主要なものでは、2 = ローカル対話型、3 = ネット ワーク、10 = リモート対話型 など ・プロセスID ・プロセス名 ・ログイン元： ワークステーション名・ソース ネット ワーク アドレス・ソース ポート ・認証の手法： 認証パッケージ
					4634	アカウントがログオフしました	アカウントのログオフ	・セキュリティID ・アカウント名・ドメイン ・ログオンID ・ログオン タイプ
					4648	明示的な資格情報を使用してログオンが試行されました	特定のアカウントが指定されたログオン試行	・実行アカウントの情報： サブジェクト内 ・セキュリティID ・アカウント名・ドメイン ・ログオンID ・資格情報が使用されたアカウント ・アカウント名・ドメイン ・ターゲットサーバー ・ターゲットサーバー名 ・プロセス情報 ・プロセスID ・プロセス名 ・ネットワーク情報 ・ネットワーク アドレス ・ポート
				オブジェクト アクセス ＞ ハンドル操作の監査	4656	オブジェクトに対するハンドルが要求されました	オブジェクトの読み書きを目的としたハンドル要求	・アカウント名・ドメイン ・ハンドルの対象： オブジェクト名 ・ハンドルID 他イベントログとの紐付けに使用する ・プロセスID ・プロセス名
					4658	オブジェクトに対するハンドルが閉じました	ハンドルの利用の終了および開放	・アカウント名・ドメイン ・ハンドルID ・プロセスID ・プロセス名
					4690	オブジェクトに対するハンドルの複製が試行されました	既存のハンドルが、他のプロセスで利用可能なように複製された	・アカウント名・ドメイン ・複製元ハンドルID ・複製元プロセスID ・複製先ハンドルID ・複製先プロセスID
				オブジェクト アクセス	4660	オブジェクトが削除されました	オブジェクトの削除	・アカウント名・ドメイン ・ハンドルID ・プロセスID ・プロセス名
					4663	オブジェクトへのアクセスが試行されました	オブジェクトに対するアクセスの発生	・アカウント名・ドメイン ・ログオンID ・オブジェクト名 ・ハンドルID ・プロセス名 ・プロセスID ・要求された処理
				オブジェクト アクセス ＞ SAMの監査	4661	SAM - A handle to an object was requested	SAMに対するハンドル要求 (取得可能な情報はイベント4656と同様)	・アカウント名・ドメイン ・ハンドルの対象： オブジェクト名 ・ハンドルID 他イベントログとの紐付けに使用する ・プロセスID ・プロセス名
				特権の使用	4672	新しいログオンに特権が割り当てられました	特定のログオンインスタンスに対する特権の割り当て	・セキュリティID ・実行アカウント名・ドメイン ・ログオンID ・割り当てられた特権
					4673	特権のあるサービスが呼び出されました	特定の特権が必要な処理の実行	・セキュリティID ・アカウント名・ドメイン ・サービス名 ・プロセスID ・プロセス名 ・使用された特権
				詳細追跡 ＞ プロセス作成の監査	4688	新しいプロセスが作成されました	プロセスの起動	・アカウント名・ドメイン ・プロセスID ・プロセス名 ・権限昇格の有無： トークン昇格の種類 ・親プロセスID： クリエーター プロセスID
				詳細追跡 ＞ プロセス終了の監査	4689	プロセスが終了しました	プロセスの終了	・アカウント名・ドメイン ・プロセスID ・プロセス名 ・戻り値： 終了状態
				アカウントの管理 ＞ ユーザー アカウントの管理の監査	4720	ユーザー アカウントが作成されました	アカウントの作成	・実行アカウントの情報： サブジェクト内 ・セキュリティID ・アカウント名・ドメイン ・ログオンID ・追加対象アカウントの情報： 新しいアカウント内 ・セキュリティID ・アカウント名・ドメイン ・その他の属性情報
					4726	ユーザー アカウントが削除されました	アカウントの削除	・実行アカウントの情報： サブジェクト内 ・セキュリティID ・アカウント名・ドメイン ・ログオンID ・削除対象アカウントの情報： ターゲットアカウント内 ・セキュリティID ・アカウント名・ドメイン
				アカウントの管理 ＞ セキュリティ グループの管理の監査	4728	セキュリティが有効なグローバル グループにメンバーが追加されました	グループへのメンバー追加 (ドメイン上のグループに追加された場合に使用される)	・実行アカウントの情報： サブジェクト内 ・セキュリティID ・アカウント名・ドメイン ・ログオンID ・対象ユーザー： メンバー内 ・セキュリティID ・アカウント名 ・対象グループ： グループ内 ・セキュリティID ・グループ名 ・グループ ドメイン
					4729	セキュリティが有効なグローバル グループにメンバーが削除されました	グループからのメンバー削除 (ドメイン上のグループから削除された場合に使用される)	・実行アカウントの情報： サブジェクト内 ・セキュリティID ・アカウント名・ドメイン ・ログオンID ・対象ユーザー： メンバー内 ・セキュリティID ・アカウント名 ・対象グループ： グループ内 ・セキュリティID ・グループ名 ・グループ ドメイン

対象	取得可能なログ							
	ログ		入手方法	設定箇所	識別子	イベント名	概要	取得可能な主な情報
全体に共通（続）	Windowsログ（続）	セキュリティ（監査ポリシー）（続）	〃	アカウント ログオン > Kerberos 認証サービスの監査	4768	Kerberos認証チケット（TGT）が要求されました	アカウントに関する認証の要求	・アカウント名・ドメイン ・セキュリティID ・送信元アドレス・ソースポート ・チケットオプション ・戻り値
				アカウント ログオン > Kerberos サービス チケット操作の監査	4769	Kerberosサービスチケットが要求されました	アカウントに関するアクセスの認可要求	・アカウント名・ドメイン・ログオンID ・サービス名・サービスID ・クライアントアドレス・ポート ・チケットオプション
				ポリシーの変更 > MPSSVC ルールレベル ポリシーの変更の監査	4946	Windows ファイアウォールの例外の一覧が変更されました	Windowsファイアウォールのルール追加	・プロファイル ・対象のルール名
				オブジェクト アクセス > ファイル共有の監査	5140	ネットワーク共有オブジェクトにアクセスしました	ネットワーク共有へのアクセス	・セキュリティID ・アカウント名・ドメイン ・ログオンID ・送信元アドレス・ソースポート ・共有名 ・共有パス ・要求された処理
					5142	ネットワーク共有オブジェクトが追加されました	ネットワーク共有を新規に作成	・セキュリティID ・アカウント名・ドメイン ・共有名 ・共有パス
					5144	ネットワーク共有オブジェクトが削除されました	ネットワーク共有の削除	・セキュリティID ・アカウント名・ドメイン ・共有名 ・共有パス
				オブジェクト アクセス > 詳細なファイル共有の監査	5145	ネットワーク共有オブジェクトに対する、クライアントのアクセス権をチェックしました	ファイル共有ポイントの利用可否の確認	・セキュリティID ・アカウント名・ドメイン ・ログオンID ・送信元アドレス・ソースポート ・共有名 ・共有パス・相対ターゲット名
				オブジェクト アクセス > フィルタリング プラットフォームの接続の監査	5154	Windows フィルターリング プラットフォームで、アプリケーションまたはサービスによるポートでの着信接続のリッスンが許可されました	アプリケーション又はサービスによるポートリッスン	・プロセスID ・プロセス名 ・アドレス・ポート ・プロトコル番号
					5156	Windowsフィルターリング プラットフォームで、接続が許可されました	Windowsフィルターリング プラットフォーム（Windowsファイアウォール）による接続の許可 （拒否の場合は異なるイベントID（5152）が記録される）	・プロセスID ・プロセス名 ・方向（送信・着信） ・送信元アドレス・ソースポート 送信時は自身、着信時は接続元の情報となる ・宛先アドレス・宛先ポート 送信時は接続先・着信時は自身の情報となる ・プロトコル番号
	アプリケーションとサービス	Sysmon	Microsoft社のサイトからダウンロード https://technet.microsoft.com/ja-jp/sysinternals/bb842062	アプリケーションとサービスログ > Microsoft > Windows > Sysmon > Operational	1	Process Create	プロセスの起動	・プロセスの開始日時： UtcTime ・プロセスのコマンドライン： CommandLine 実行ファイルに渡されたオプションが記録される。 オプション内で他ホストのIPアドレスや
					5	Process Terminated	プロセスの終了	・プロセスの終了日時： UtcTime ・プロセスID： ProcessId
					8	CreateRemoteThread detected	他のプロセスからスレッドを新規に作成	・スレッドの作成日時： UtcTime ・呼出元プロセスID： SourceProcessId ・呼出元プロセス名： SourceImage ・呼出先プロセスID： TargetProcessId ・呼出先プロセス名： TargetImage
at		Microsoft > Windows > TaskScheduler > Operational	Windowsの初期設定で記録される		106	タスクが登録されました	タスクの新規登録	・実行アカウント名・ドメイン ・作成したタスク名
					200	開始された操作	タスクの実行	・タスク名 ・実行した操作
					129	タスクのプロセスが作成されました	タスク内でのプロセス実行	・タスク名 ・プロセスID ・実行されたプロセス
					201	操作が完了しました	タスク内で実行されたプロセスの終了	・タスク名 ・終了したプロセス ・戻り値
					102	タスクが完了しました	タスクの終了	・実行アカウント名・ドメイン ・タスク名
WinRM・WinRS		Microsoft > Windows > Windows Remote Management > Operational			6	WSManセッションを作成しています	新規のセッション作成	・接続先ホスト名
					169	ユーザーの認証： 正常に認証されました	ユーザー認証	・ユーザー名・ドメイン
RDP		Microsoft > Windows > TerminalServices > LocalSessionManager > Operational			21	リモートデスクトップサービスのセッション ログオンに成功しました	RDPで新規にログオン	・セッションの接続開始日時 ・実行アカウント名・ドメイン ・ソースネットワークアドレス
					24	リモートデスクトップサービスのセッションが切断されました	RDPセッションの切断	・セッションの接続開始日時 ・実行アカウント名・ドメイン ・ソースネットワークアドレス

索引