

報告書 (第2版)

一般社団法人 JPCERT コーディネーションセンター2017 年 11 月 9 日

# 目次

1.	はじ	めに	.2
2.	調査	五方法	.3
2	.1.	調查実施内容	3
2	.2.	調査したツール	4
2	.3.	調査の実施環境	6
3.	調査	£結果	.7
3	5.1.	ツール分析結果シートの構成	7
4.	追加	ロログ取得について	.9
4	.1.	追加ログ取得の重要性	9
4	.2.	追加ログ取得設定の影響	9
5.	イン	シデント調査におけるツール分析結果シートの活用方法1	0
5	5.1.	本報告書を使用したインシデント調査	10
6.	おわ	つりに1	11
7.	付錡	₽ A1	2
7	<b>.</b> 1.	Sysmon のインストール方法	12
7	.2.	監査ポリシーの有効化方法	12

# 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、ユーザーのパスワー 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、本調査の結果をもとに作成した「ツール分析結果シート」 について説明する。第4章では、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 るイベントログや実行履歴を含め、以下を対象とした。なお、下記項目の中で最もツールの実行痕 跡が残るのはイベントログであることを確認している。そのため、本報告書ではイベントログの調 査手法を中心に記載している。

- イベントログ
- 実行履歴
- Prefetch
- USN ジャーナル
- MFT
- UserAssist
- パケットキャプチャ

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に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。

8		イベントビ	ューアー					
ファイル(F) 操作(A) 表示(V) ヘルプ(H)								
Store-Licensi	Operational 1	イベント数: 315 (!) 新しいイイ	いたが利用可能	<u> </u>				
StorPort		日付と時刻	ソース	1/521	<u>タスクの</u>		^	
Superfetch		2016/04/26 17:52:52	Evenon	1. 0.1	Dawle		-	
A Sysmon		2016/04/26 17:52:53	Sysmon	9	Dracos			
		2010/04/20 17:52:33	Sysmon	1	Proces			
SystemSetti		2010/04/20 17.52.42	Sysmon	J	Proces			
		2010/04/20 17.52.42	Sysmon	9	Dracas			
		2010/04/20 17:52:42	Systition	1	Proces		*	
	イベント 9, Sysmon						×	
TerminalServ	全般 ≣¥細							
TerminalServ								
Filler TerminalServ	BawAccessBear	detected:				<u>^</u>		
D I TerminalServ	UtcTime: 2016-1	04-26 08:52:53.832						
D I TerminalServ	ProcessGuid: {2	117aa9a-2c65-571f-0000-0	010d82b0900}					
⊳ 🧮 TerminalServ	ProcessId: 652							
▷ I TZSync	Image: C:¥Windo	ws¥System32¥IME¥SHARE	D¥ImeBroker.e	xe				
TZUtil	IDevice: #Device	¥Harddisk Volume2				Ŧ		
DAC	ログの名前(M):	Microsoft-Wind	ows-Sysmon/	Operational				
D UAC-FileVirtu	ソース(S):	Sysmon		ログの日付(ロ	): 2016/	04/26 17:52:53		
UI-Search	イベント ID(E):	9		タスクのカテゴ	U(Y): RawA	ccessRead detected		
Diser Control		小主五品						
Diser Profile S					/D) UF 04	04 ID 1511		
Diser-Loader	1-9-(U):	STOLEM		1761-8-	(FV: WIN81	_040P-IE11		
DiserPhp	オペコード(0):	이주 특기						
▷ VDRVROOT	■====================================	<u>イベント ログのへ</u>	ルプ					
🕟 🦳 VerifvHardwa								

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ことで、OS 上に記録されているログを調査した。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 49 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。

攻撃者がツールを使用する目的	ツール
コマンド実行	PsExec
	wmic
	schtasks

表 2-1: 調査したツール一覧

	wmiexec.vbs
	BeginX
	WinRM
	WinRS
	BITS
パスワード、ハッシュの入手	PWDump7
	PWDumpX
	Quarks PwDump
	Mimikatz
	(パスワードハッシュ入手 Isadump::sam)
	Mimikatz
	(パスワードハッシュ入手
	sekurlsa::logonpasswords)
	Mimikatz (チケット入手 sekurlsa::tickets)
	WCE
	gsecdump
	Islsass
	AceHash
	Find-GPOPasswords.ps1
	Get-GPPPassword (PowerSploit)
	Invoke-Mimikatz (PowerSploit)
	Out-Minidump (PowerSploit)
	PowerMemory (RWMC Tool)
	WebBrowserPassView
通信の不正中継	Htran
(パケットトンネリング)	Fake wpad
リモートログイン	RDP
Pass-the-hash	WCE (リモートログイン)
Pass-the-ticket	Mimikatz (リモートログイン)
権限昇格	MS14-058 Exploit
	MS15-078 Exploit
	SDB UAC Bypass
ドメイン管理者権限	MS14-068 Exploit
アカウントの奪取	Golden Ticket (Mimikatz)
	Silver Ticket (Mimikatz)
ローカルユーザー・グループの 追加・削除	net user

ファイル共有	net use
痕跡の削除	sdelete
	timestomp
	klist purge
	wevtutil
情報収集	ntdsutil
	vssadmin
	csvde
	ldifde
	dsquery
	dcdiag
	nltest
	nmap

# 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 したシステムについて調査した。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
  - Ø Windows 7 Professional Service Pack 1
  - Ø Windows 10
- サーバの搭載 OS
  - Ø Windows Server 2012 R2

## 3. 調査結果

本調査では、2.2 節で記載したツールを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、ファイルシス テムの記録を調査した。また、特徴的な通信を行うツールに関してはパケットキャプチャも調査し た。調査結果は「ツール分析結果シート」として以下で公開している。

ツール分析結果シート: https://jpcertcc.github.io/ToolAnalysisResultSheet\_jp/

上記サイトでは、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。また、調査結果では、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. ツール分析結果シートの構成

「ツール分析結果シート」では、49種類のツールについて分析した結果を掲載している。各ツール の分析結果は表形式で解説しており、各項目で記載している内容について以下の通りである。

ツール概要

Ø ツールについての説明およびツールの攻撃時における想定利用例について記載

ツール動作概要

Ø 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

ログから得られる情報

ダ デフォルト設定(標準設定)および監査ポリシーの設定および Sysmon がインストール された状態(追加設定)でツール実行時に得られるログの概要を記載

実行成功時に確認できる痕跡

Ø ツールの実行が、成功したことを確認する方法を記載

実行時に記録される主要な情報

Ø 対象のイベントログやレジストリ、USN ジャーナル、MFT など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)

詳細

Ø には含まれていない記録されるすべてのログについて記載

備考

Ø その他に記録される可能性があるログや検証時に確認した事項について記載

# 4. 追加ログ取得について

本章では、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ツール分析結果シートの活用方法

本章では、インシデント調査の事例をもとにツール分析結果シートの利用イメージについて述べる。

#### 5.1. 本報告書を使用したインシデント調査

ツール分析結果シートは、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」に何か不審なログがないか確認することが 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「ツール分析結果シート」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、「ツール分析結果シート」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。

#### 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。本報告書およびツール分析結果シートでは、 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。

+40	- H- H.	8-84+7	2.2	
セキュリティ	11	前のバージョン	21-9	
オブジェクト名: グループ名またはユー	C:¥ ザー名(G):			
Authenticate	ed Users			-
SYSTEM				
Administrato	xrs (WIN10-64)	P¥Administrators)		
KUSers (WIN1)	0-64JP¥Users)			
アクセス許可を変更 フリークンナオ	(するには(編集)	8	<b>愛編集(E)</b>	
Pクセス許可(P): A Jsers	uthenticated	許可	拒否	
ע-םאעב עול			9000	9
T.F.				
読み取りと実行				
フォルダーの内容	の一覧表示			
御み歌り				1
050.74				
の神なマクセス時間	107-1012-0010-7	remera D	Bill for BA starts of the	-
ALL ADDRESS OF ALL ADDRESS OF	01-01.03	e warry is w	ITHERCE (V)	
[[]]][]]][]]][]]]][]]]]]]]]]]]]]]]]]]]				

4. [監査]タブから監査対象のオブジェクトを追加する。

6年: 作件书:	Tusted	hstaller XE(C)					
ウセス許可	LW	有効なアクセス					
増についての	5. <b>511</b> 5.279	キャノルクリックしていこさ	OVERTOPOLE P	DIVER TALAGORDATIV (MORT)	(10円できる場合) セクリックしま	F.	
推动	プリンシッパル		アクセス	輕量元	這些快		

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

0-nil 7	6(3.7 (6) の監察エントリ		- ¤ ×
Jussit	Ar best (WINTO-648Proced) 792757/Grid BR		
12:05	¥42 ~		
建用心	2017×114-1977×114-86071416 ~		
A#97	2012年日) □ 20132トロール □ 2013年の人キャンプアイルの実行 □ 2013年の一覧データの読み取り □ 間信の読み取り □ 間信の読み取り □ 間信の読み取り ○ 2014の代表のデーの書を込み ○ 2014年の代表が手のの書を込み	ご 雪性の巻き込み 必能感染性の着き込み のサブフォルダーとフィルの制除 の予約 コアウセス肝可の読み取り のアウセス肝可の読み取り のどかなた可の変更 のなたたのの意味	64079EXH488A90
<u>⊡</u> 2602	ビノスのノール・ハルレックスの起この テナー内のオブジェクトオたヨコンテナーのみにこれらの転還取また。	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	\$<79JP
			0K #+256

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 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。

ツノルノリッツリ いんさい。 監査エノドツで変更 9 るには、エノドツで選択し、[補集](沢田 できる

	W	/indows 한	F_JJ77 X	
64		セキュリティ	の適用エラー	×
			セキュリティ情報を適用中にエラーが発生しました: C:¥Documents and Settings	
			コンテナー内のオブジェクトを列挙できませんでした。アクセスが拒否され す。	いていま
			続行(C) キャンセ	JL

本文書内に記載されている情報により生じるいかなる損失または損害に対して、JPCERT/CC は 責任を負うものではありません。