Computer Security Symposium 2020
26 - 29 October 2020

暗号化SMB通信に対するネットワークフォレンジック手法の有効性の検証

海野 由紀[1,a)]　江田 智尊[1]　小久保 博崇[1]　森川 郁也[1]　村上 雅彦[1]

概要：標的型攻撃では組織内に侵入した攻撃者は Windows コマンドでリモート管理操作やファイル操作を行う．Windows コマンドの内部では，Server Message Block（SMB）と呼ばれるプロトコルが利用されている．SMB はバージョン 3.0 以降でエンドツーエンドのデータ転送を暗号化することが可能になった．著者らが開発した「高速フォレンジック手法」はネットワークフォレンジック手法の一つである．この手法は通信データを読み込んでフローを再構築し，SMB プロトコルを解析して，リモート管理操作やリモートファイル操作の証跡を抽出する．本論文では Windows OS がサポートする SMB のバージョン，SMB のプロセス間通信の挙動，SMB の暗号化設定と暗号化通信の挙動を明らかにする．暗号化設定に応じて高速フォレンジック手法がどの程度証跡を抽出できるかについて検証し，手法の有効性について述べる．また SMB 通信が暗号化されている場合のフォレンジック手法について考察する．

キーワード：フォレンジック，インシデントレスポンス，暗号化通信, SMB

Verification of Effectiveness of Network Forensics Method for Encrypted SMB Communications

Yuki Unno[1,a)]　KodaSatoru[1]　Hirotaka Kokubo[1]　Ikuya Morikawa[1]　Masahiko Murakami[1]

Abstract: In targeted attacks, an attacker who invades the organization uses Windows commands to perform remote management operations and file operations. Inside the Windows command, a protocol called Server Message Block (SMB) is used. With SMB version 3.0 or later, it is possible to encrypt end-to-end data transfer. The high-speed forensic method developed by the authors is one of the network forensic methods. This method captures the communication data, reconstructs the flow, analyzes the SMB protocol, and extracts the trail of remote management operations and remote file operations. In this paper, we clarify the version of SMB supported by Windows OS, the behavior of SMB interprocess communication, the encryption setting of SMB, and the behavior of encrypted communication. We verify to what extent our method can extract trails according to the encryption settings, and describe the effectiveness of the method. We also consider the forensic method when SMB communication is encrypted.

Keywords: Forensics, Incident Response, Encrypted Communications, SMB

1. はじめに

標的型攻撃では，攻撃者はソーシャルエンジニアリング手法を利用した標的型攻撃メールを送るなどして，組織内に設置されている Windows OS ベースの PC を RAT（Remote Access Trojan/Remote Administration Tool）と呼ばれるマルウェアに感染させる．RAT はリモートからコマンド・シェルを実行する機能，攻撃サーバである C2 サーバへ接続する機能を持っている．攻撃者は C2 サーバから RAT に要求メッセージを送信し，感染した PC の周辺の業務サーバを探索し，さらに別の PC をマルウェアに感染させるなどして，機密情報の窃取を試みる．その際，

[1] 株式会社富士通研究所
FUJITSU LABORATORIES LTD.
[a)] yuki_m@fujitsu.com

攻撃者は自身が開発した攻撃用のツールを送りこむだけでなく，Windows OS に標準で搭載されているコマンドを利用することが実際のインシデントで観測されている．文献 [1][2][3][4] において攻撃者が悪用する Windows コマンドが報告されている．攻撃者が悪用する Windows コマンドの内，リモートの Windows OS ベースの PC やサーバに操作を行うリモートコマンドには内部で SMB を使うものがある．SMB にはバージョン 1 から 3 が存在しているが，バージョン 3.0 以降でエンドツーエンドのデータ転送を暗号化することが可能になった．

著者らが提案した高速フォレンジック手法はネットワークフォレンジック手法の一つである．リアルタイムに通信データをキャプチャしながら通信フローを再構築して，コマンドベースで Windows OS のリモート管理操作・リモートファイル操作の証跡を抽出する方式，アカウントとリモート管理操作・リモートファイル操作のコマンドを自動的にひも付けする方式，および攻撃の特徴を示す属性値で攻撃シナリオを抽出・連結して, 攻撃の進行状況を追跡する方式から構成される．SMB の暗号化機能が有効にされ，通信データからリモート管理操作・リモートファイル操作のコマンドを特定するための情報が得られない場合はコマンドベースの証跡を取得できない．

そこで Windows OS に搭載されているリモート管理操作，リモートファイル操作のコマンドを実行した際の通信データを解析して，Windows OS がサポートする SMB のバージョン，SMB のプロセス間通信の挙動，SMB の暗号化設定と暗号化通信の挙動を明らかにした．また，SMB3 をサポートしている Windows OS を用いて暗号化の範囲をサーバ全体に設定した評価環境と共有フォルダのみに設定した評価環境を構築し，リモート管理操作コマンド 19 種類，リモートファイル操作コマンド 3 種類に対して高速フォレンジック手法がどの程度証跡を抽出できるか有効性を検証した．サーバ全体で SMB の暗号化機能を有効にした場合，通信データを入力にしたネットワークフォレンジック技術では，標的型攻撃で組織内に侵入した攻撃者の操作証跡を解析することは難しい．従来から行われている PC やサーバ，ネットワーク機器のログを監視・分析する手法の応用や新しい手法の検討が考えられる．

本稿では，第 2 章で攻撃者が悪用するリモートコマンドとその内部で使われている SMB の実際の挙動について述べる．第 3 章では通信データから SMB ベースのリモート操作コマンドが実行された証跡を抽出する高速フォレンジック手法について，第 4 章では SMB の暗号化設定を行った環境を用いて高速フォレンジック手法の証跡抽出機能を動作させた結果と考察を，第 5 章でまとめについて述べる．

2. 攻撃者が悪用するリモートコマンドと SMB

2.1 標的型攻撃のフェーズと攻撃者が悪用するリモートコマンド

2009 年にロッキードマーチンは標的型攻撃における攻撃者の一連の行為をモデル化した [5]．このモデルは Cyber Kill Chain と呼ばれ，Reconnaissance（偵察），Weaponization（武器化），Delivery（配送），Exploitation（攻撃），Installation（インストール），Command and Control（遠隔制御），Actions on Objectives（目的の達成）という 7 つのフェーズから構成される．組織内に設置されている Windows OS ベースの PC が RAT に感染するという事象は Installation（インストール）のフェーズに相当する．RAT と C2 サーバが通信可能となり，攻撃者が RAT に感染した PC を操作できる状態は Command and Control（遠隔制御）のフェーズに相当する．Command and Control のフェーズで攻撃者に悪用されるコマンドにはローカル内に閉じて動作するローカルコマンドとリモートの PC やサーバに対して操作を行うリモートコマンドがある．悪用されるリモートコマンドには net コマンド，at コマンド，schtasks コマンド，sc コマンド，reg コマンド，wmic，winrm/winrs コマンドがある [1][2][3][4]．リモートコマンドにはプロセス間通信の機能が実装されており, net コマンド，at コマンド，schtasks コマンド，sc コマンド，reg コマンドの内部では SMB が使われている．wmic コマンドの内部では Distributed Component Object Model（DCOM）が，winrm/winrs コマンドの内部では http/https が使われている．次節以降は SMB について述べる．

2.2 SMB

SMB はファイルやプリンタ，シリアルポートの共有でよく知られているプロトコルであるが，ネットワーク上のプロセス間通信にも利用されるプトロコルで，TCP/IP プロトコルもしくは別のネットワークプロトコルの上で使用できる．SMB サーバはクライアントがファイルシステムとリソースを利用できるようにする．SMB クライアントはリソースに対して SMB リクエストを送信し，SMB サーバは SMB クライアントへ SMB 応答を送信する．SMB のバージョンには 1.0, 2.0/2.02, 2.1, 3.0, 3.0, 3.02, 3.1.1 がある．Windows OS の種類に応じて，サポートするバージョンが異なっている（**表 1**）．Windows XP と Windows Server 2003 R2 以前は SMB 1.0 を，Windows Vista と Windows Server 2008 は SMB2.0/2.02 を，Windows 7 と Windows Server 2008 R2 は SMB 2.1 をサポートしている．また，Windows 8 と Windows Server 2012 は SMB3.0 を，Windows 8.1 と Windows Server 2012 R2 は SMB3.02 を，Windows 10 と Windows Server 2016, Windows Server 2019 は SMB3.1.1 をサポートしている．また，Microsoft は SMB1.0 を一般

に非推奨とし，Windows 10 バージョン 1709、Windows Server バージョン 1709 以降ではデフォルトでは SMB1.0 はインストールされない．プロセス間通信をする際は SMB クライアントと SMB サーバが通信の最初に行うネゴシエーションプロトコルにて SMB のどのバージョンを利用してセッションを確立するかを決める（**図 1**）．Windows OS の組合せ毎に実際にどの SMB のバージョンでセッションを確立しているかを調査した結果について**表 2** に記す．表 2 には Samba が実装している SMB バージョンについて調査した結果を加える．Samba は Windows 以外の OS で SMB など Windows ネットワークの機能を利用できるようにするフリーソフトウェアである．

2.3 SMB 通信の暗号化

SMB1.0，2.0/2.02，2.1 は暗号化をサポートしていないが，SMB3.0 以降ではオプションで暗号化機能を利用できる [6][7]．機密情報などセキュリティが必要なデータを取り扱う場合，SMB 通信の暗号化が推奨されている．暗号化機能を有効にする手順は 2 通りある．1 つは Windows Server のサーバーマネージャーを利用する方法，もう 1 つは Powershell のコマンドレットを利用する方法である．サーバーマネージャを利用する場合は，暗号化したい共有フォルダを指定して暗号化機能を有効にする．Windows OS が標準で用意している管理共有 IPC$に対しては暗号化機能を有効にすることはできない．PowerShell を利用する場合は，次のように共有フォルダを指定して暗号化機能を有効にする方法と，サーバ全体で暗号化を有効にする方法がある．

```
個々のファイル共有の暗号化を有効にする
    Set-SmbShare -Name <sharename>-EncryptData $true
暗号化を有効にし新しいファイル共有を作成する
    New-SmbShare -Name <sharename>-Path <pathname>-EncryptData $true
ファイルサーバ全体で暗号化を有効にする
    Set-SmbServerConfiguration ?EncryptData $true
```

共有フォルダまたはサーバ全体に対して暗号化を有効にすると，SMB1 や SMB2 などのクライアントはアクセスを拒否される．しかし Windows 7，Windows 2008，Windows 2008 R2 のサポートが 2020 年 1 月 14 日で終了しており，今後は SMB3 をサポートしていないクライアント自体が減少していくため，SMB の暗号化を有効にした利用が増加することが予想できる．

表 1　デフォルトの SMB バージョン
Table 1　Default SMB versions

	Windows OS	Samba
SMB 1.0	Windows XP	Samba 1.x
	Windows Server 2003 R2 以前	
SMB 2.0/2.02	Windows Vista	Samba 3.6
	Windows Server 2008	
SMB 2.1	Windows 7	Samba 4.0
	Windows Server 2008 R2	
SMB 3.0	Windows 8	Samba 4.2
	Windows Server 2012	
SMB 3.02	Windows 8.1	Samba4.3
	Windows Server 2012 R2	
SMB 3.1.1	Windows 10	Samba4.3
	Windows Server 2016	
	Windows Server 2019	

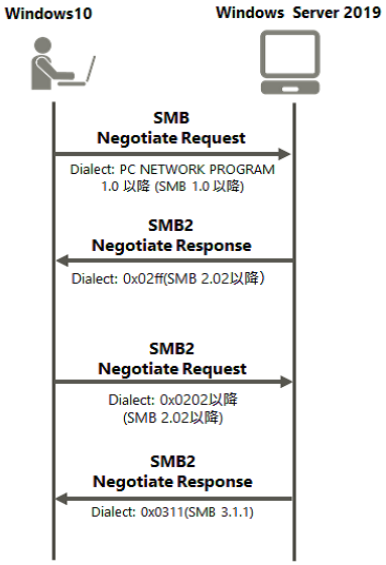

図 1　SMB のネゴシエーションプロトコル
Fig. 1　SMB negotiation protocol

3. 高速フォレンジック手法と SMB

3.1 高速フォレンジック手法

高速フォレンジック手法は，標的型攻撃における従来デジタルフォレンジック技術の 2 つの課題「セキュリティに関する高度な知識と技術を保持する専門家が必要であること」「調査対象の通信データ・HDD イメージが膨大で攻撃の証跡分析に時間がかかること」を解決するために著者らが提案したネットワークフォレンジック手法である [8][9][10][11][12]．本手法は，3 つの方式で構成される．リアルタイムに通信データをキャプチャしながら通信フローを再構築して，コマンドベースで Windows OS のリモート管理操作・リモートファイル操作の証跡を抽出する方式，アカウントとリモート管理操作・リモートファイル操作のコマンドを自動的にひも付けする方式，および攻撃

表 2　Windows OS の組合せごとの SMB のバージョン
Table 2　SMB versions used in OS combinations

Dest → / Src ↓	XP 2003 R2 以前	Vista 2008	7 2008 R2	8 2012	8.1 2012 R2	10 2016 2019
XP 2012 R2 以前	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0
Vista 2008	SMB 1.0	SMB2.0/2.02	SMB 2.0/2.02	SMB 2.0/2.02	SMB 2.0/2.02	SMB 2.0/2.02
7 2008 R2	SMB 1.0	SMB2.0/2.02	SMB 2.1	SMB 2.1	SMB 2.1	SMB 2.1
8 2012	SMB 1.0	SMB2.0/2.02	SMB 2.1	SMB 3.0	SMB 3.0	SMB 3.0
8.1 2012 R2	SMB 1.0	SMB2.0/2.02	SMB 2.1	SMB 3.0	SMB 3.02	SMB 3.02
10 2016 2019	SMB 1.0	SMB2.0/2.02	SMB 2.1	SMB 3.0	SMB 3.02	SMB 3.1.1

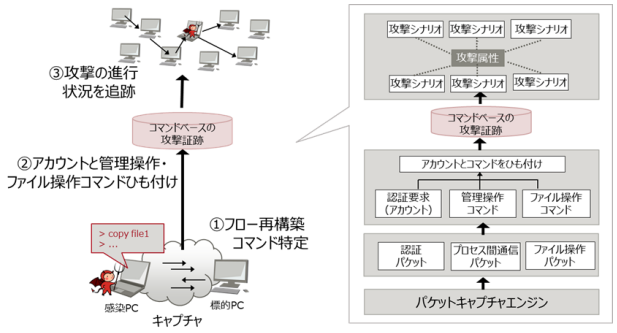

図 2　高速フォレンジック手法
Fig. 2　High-Speed Forensic Method

の特徴を示す属性値で攻撃シナリオを抽出・連結して, 攻撃の進行状況を追跡する方式である（**図 2**）.

コマンドベースで Windows OS のリモート管理操作・リモートファイル操作の証跡を抽出する方式では，SMB のプロセス間通信の要求メッセージの特徴から，端末で実行されたコマンドの種類を特定している．SMB のプロセス間通信は Distributed Computing Environment/Remote Procedure Calls（DCE/RPC）で実装されており，マイクロソフトの DCE/RPC は MSRPC[13] とも呼ばれている．MSRPC のメッセージの Transport は複数の方式がある．TCP/IP（NCACN_IP_TCP），SMB（NCACN_NP）,SPX（NCACN_SPX），NetBIOS over IPX（NCACN_NB_IPX），NetBIOS over TCP（NCACN_NB_TCP），NetBIOS over NetBEUI（NCACN_NB_NB），AppleTalk（NCACN_AT_DSP），RPC over HTTP（ncacn_http）などである．これらの Transport 方式のうち，どの方式を使うのかは SMB クライントに依存する．そこで著者らは攻撃者に悪用されるコマンドを実際に実行した際の通信データから Transport 方式を調査して，TCP/IP（NCACN_IP_TCP）方式，SMB（NCACN_NP）方式の二種類が利用されていることを明らかにした．sc コマンド，schtasks コマンドは TCP/IP（NCACN_IP_TCP）方式と SMB（NCACN_NP）方式の両方を実装している．at コマンド，net コマンド，reg コマンドは TCP/IP（NCACN_IP_TCP）方式を実装しておらず，SMB（NCACN_NP）方式のみを実装している．TCP/IP（NCACN_IP_TCP）方式では MSRPC は直接 TCP/IP の上で，SMB（NCACN_NP）方式では TCP/IP の上位の SMB の上で動作する．TCP/IP（NCACN_IP_TCP）方式，SMB（NCACN_NP）方式の両方を実装している SMB クライアントでは TCP/IP（NCACN_IP_TCP）方式の利用が優先となる．TCP/IP（NCACN_IP_TCP）方式ではリモートの PC，サーバへ接続する際には，まず End Point Mapper（EPM）に目的のリモートサービスの情報を問合せる．この情報にはリモートサービスに接続するための TCP のポート番号が含まれる．SMB クライアントは EPM から返却されたリモートサービスのポート番号に接続して目的のサービスを利用する．もし，EPM が停止している，または Firewall が EPM への通信（135/TCP）を遮断している状況である場合は，SMB クライアントは TCP/IP（NCACN_IP_TCP）方式の利用を中断して SMB（NCACN_NP）方式の利用に移行し目的のサービスを利用する．高速フォレンジック手法は Windows OS のリモート管理操作・リモートファイル操作の証跡を抽出するために MSRPC の Transport 方式を考慮する必要がある．**図 3** のように，TCP/IP（NCACN_IP_TCP）方式，SMB（NCACN_NP）方式の通信データのふるまいを解析する．

図 4 は認証サーバに Active Directory が導入された環境において，感染 PC と標的 PC の SMB ネゴシエーション

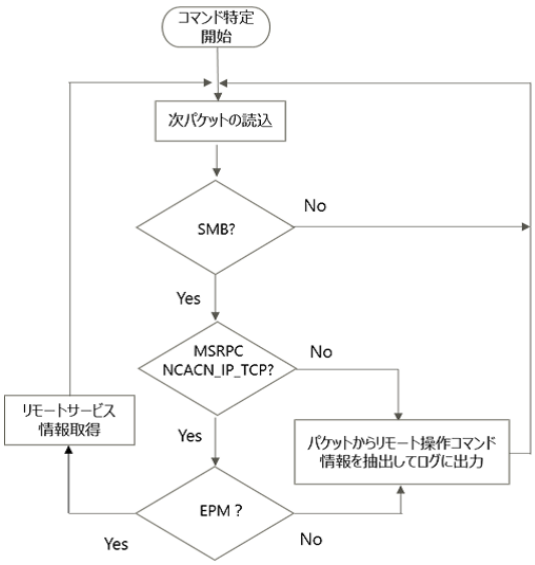

図 3　リモート操作コマンドの特定
Fig. 3　Remote Command Identification

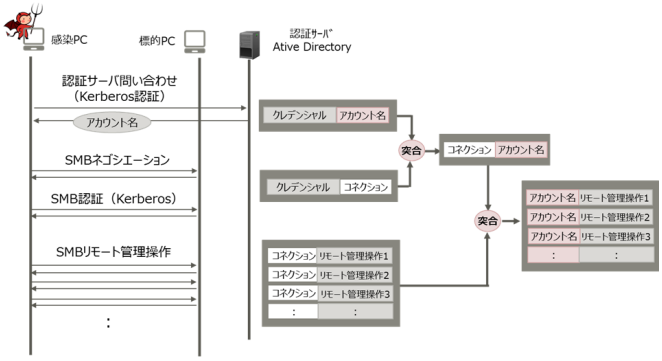

図 4　アカウントとコマンドのひも付け
Fig. 4　Automatically correlating accounts with operations

によって認証プロコトルが Kerberos に決められた場合のアカウントとリモート管理操作コマンドのひも付けを示したものである．最初に，Active Directory のアカウントでログインする際の認証メッセージを解析してクレデンシャルとアカウント名の情報を取得する．次に SMB 認証に該当するセッション・セットアップのメッセージを解析して，クレデンシャルとコネクションの対応情報を取得する．それらをクレデンシャルで突合してコネクションとアカウント名の対応情報を得る．SMB のリモート操作のメッセージを解析してコネクションとリモート管理操作の対応情報を得る．この情報と先の突合結果をコネクションで突合し，アカウントとリモート管理操作コマンドをひも付ける．

攻撃進行状況の追跡方式では，Cyber Kill Chain の Command and Control（遠隔制御）に特徴的なリモート管理操作コマンドの動作や操作の不審度，攻撃に悪用されたアカウント名などの攻撃属性によって，コマンドベースの証跡ログをフィルタリングしながら攻撃シナリオを抽出する．最後に攻撃シナリオを操作の方向で連結して攻撃進行状況

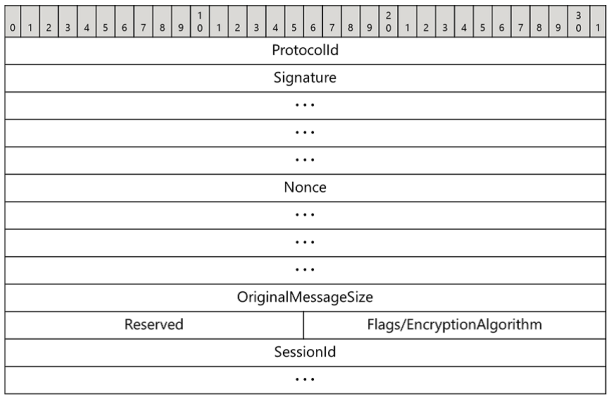

図 5　SMB2 TRANSFORM_HEADER
Fig. 5　SMB2 TRANSFORM_HEADER

を示すタイムラインを作成する．

3.2　SMB 通信の暗号化によるコマンドベースの操作証跡抽出への影響

SMB の暗号化機能を有効にすると，SMB クライアントとサーバがネゴシエーションを行い，SMB クライアントがセッション確立のリクエストを送信した後は，データは全て暗号化される．SMB クライアントとサーバは SMB2 TRANSFORM_HEADER を使って暗号化したデータを送信する．**図 5** で SMB2 TRANSFORM_HEADER の構造を示す．SMB2 TRANSFORM_HEADER からはオリジナルのメッセージサイズや暗号化アルゴリズムの情報は得られるが，リモート管理操作・リモートファイル操作のコマンドを特定するための情報が全く得られない．仮に Windows OS において暗号化機能を有効にした際にリモート管理操作・リモートファイル操作の通信が常に暗号化されるとした場合，高速フォレンジック手法ではコマンドベースの証跡を全く取得することができないことになる．

4.　評価

4.1　実験

実際に SMB の暗号化機能を有効にした環境で高速フォレンジック手法でコマンドベースの証跡が収集できるのか評価した．SMB3 をサポートしている Windows OS を用いて暗号化の範囲をサーバ全体に設定した評価環境と共有フォルダのみに設定した評価環境を構築した．両環境で，標的 PC の EPM を有効にし TCP/IP（NCACN_IP_TCP）方式でプロセス間通信を行うようにした場合と，EPM を無効にして SMB（NCACN_NP）方式でプロセス間通信を行うようにした場合に，リモート管理操作コマンド 19 種類，リモートファイル操作コマンド 3 種類をオプションと引数を変更しながら複数回実行して通信データを収集した．収集したデータを高速フォレンジック手法のプログラムで解析させ，SMB メッセージからコマンド，オプション，引数を抽出して証跡を取得できたかを確認した．その

表 3　実験結果 #1
Table 3　Result of Experimentation #1

操作コマンド	暗号化の範囲	MSRPC	証跡取得結果
net view %s	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
net user	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
net group	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
net localgroup	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
net use	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
sc	サーバ全体	NCACN_IP_TCP	可
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	可
		NCACN_NP	可
schtasks	サーバ全体	NCACN_IP_TCP	可
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	可
		NCACN_NP	可
reg	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
psfile	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
psgetsid	サーバ全体	NCACN_IP_TCP	可
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	可
		NCACN_NP	可
psinfo	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可

表 4　実験結果 #2
Table 4　Result of Experimentation #2

操作コマンド	暗号化の範囲	MSRPC	証跡取得結果
pskill	サーバ全体	NCACN_IP_TCP	可
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	可
		NCACN_NP	可
pslist	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
psloggedon	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
psloglist	サーバ全体	TCP/IP	N/A
		SMB	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
pspasswd	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	可
psservice	サーバ全体	NCACN_IP_TCP	可
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	可
		NCACN_NP	可
psshutdown	サーバ全体	NCACN_IP_TCP	可
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	可
		NCACN_NP	可
pssuspend	サーバ全体	NCACN_IP_TCP	可
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	可
		NCACN_NP	可
read file	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	不可
write file	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	不可
delete file	サーバ全体	NCACN_IP_TCP	N/A
		NCACN_NP	不可
	共有フォルダ	NCACN_IP_TCP	N/A
		NCACN_NP	不可

結果を**表 3** **表 4** にまとめる．

4.2　考察

本評価では MSRPC の TCP/IP（NCACN_IP_TCP）方式と SMB（NCACN_NP）方式の両方をサポートするリモート管理操作コマンドが 7/19 種類，SMB（NCACN_NP）方式のみをサポートするリモート管理操作コマンドが 12/19 種類存在することが分かった．

リモート管理操作コマンドが MSRPC の TCP/IP（NCACN_IP_TCP）方式でリモートサービスとプロセス間通信を行うとき，SMB の暗号化の範囲によらず，高速フォレンジック手法はコマンドベースの証跡を取得できる．リ

モート監視操作コマンドはリモートの管理共有 IPC$に接続した後，TCP/IP（NCACN_IP_TCP）方式でリモートサービスと通信する．その間は MSRPC が直接 TCP/IP の上で動作するため SMB の暗号化の対象外となる．高速フォレンジック手法は TCP/IP（NCACN_IP_TCP）方式でのプロセス間通信のメッセージからリモート操作コマンドの情報を抽出しているため，コマンドベースの証跡を取得できる．

リモート管理操作コマンドが SMB（NCACN_NP）方式でプロセス間通信を行うとき，高速フォレンジック手法は暗号化の範囲が共有フォルダである場合は証跡を取得できるが，サーバ全体である場合は証跡を全く取得できない．これは，Windows OS ではリモート管理操作コマンドが実行時に利用する Windows の管理共有 IPC$を指定して暗号化機能を有効にできないこと，暗号化の範囲がサーバ全体である場合は IPC$に対しても暗号化機能が有効になることによる．リモートファイル操作コマンドは常に SMB（NCACN_NP）方式でプロセス間通信を行うため，暗号化の範囲がサーバ全体の場合も共有フォルダの場合も高速フォレンジック手法は証跡を取得できない．

以上から，攻撃者の組織内での諜報活動，すなわちインシデントを通信データから検出したい場合は，サーバ全体ではなくファイル共有を指定して暗号化機能を有効にするのがよいことが分かる．機密情報を含むファイルを送受信する際に通信路でファイルの内容を盗聴されるリスクの低減と攻撃者に悪用されるリモート管理操作の追跡を両立することが可能である．しかし，攻撃者にリモート管理操作の内容を通信データから把握させたくないケースや共有フォルダ指定で暗号化機能を有効化する運用の手間を軽減したいケースが考えられ，今後はサーバ全体での暗号化機能の有効化が使われていくであろう．その際のインシデントの検出は PC やサーバ，ネットワーク機器のログを監視・分析する，暗号化された通信の内容を機械学習などの技術でリモート管理操作・リモートファイル操作を予測するなど新しい手法による対応が考えられる．前者については従来から行われている対策であり，近年は Endpoint Detection and Response（EDR）や User and Entity Behaior Analytics（UEBA）などソリューションが提供されているが，監視・分析対象の数が多い場合にスピード，スケーラビリティやコストが課題となっている．後者についてのソリューションは提供されておらず，研究開発のフェーズに位置している．

5. まとめ

本論文では Windows OS に搭載されているリモート操作コマンドの通信データを解析して，Windows OS が実装している SMB のバージョン，SMB のプロセス間通信の挙動，SMB の暗号化設定と暗号化通信の挙動を明らかにした．また，暗号化設定に応じて，著者らが開発した高速フォレンジック手法がリモート管理操作やリモートファイル操作の証跡を抽出できる範囲を明確にした．サーバ全体で SMB の暗号化機能を有効にした場合は高速フォレンジック手法を含め，従来のネットワークフォレンジック技術では標的型攻撃で組織内に侵入した攻撃者の操作証跡を解析することは難しい．従来から行われている PC やサーバ，ネットワーク機器のログを監視・分析する手法の課題を解決する手法や暗号化された通信の内容を機械学習などの技術を用いて攻撃者が行った操作を予測するなど新しい手法の検討が必要となる．

参考文献

[1] 朝長 秀誠, “攻撃者が悪用する Windows コマンド (2015-12-02),” 一般社団法人 JPCERT コーディネーションセンター, https://blogs.jpcert.or.jp/ja/2015/12/wincommand.html, 参照 2020 年 8 月 7 日

[2] 朝長 秀誠, “攻撃者の行動によって残る痕跡を調査 (2016-06-28),” 一般社団法人 JPCERT コーディネーションセンター, https://blogs.jpcert.or.jp/ja/2016/06/ir_research.html, 参照 2020 年 8 月 7 日

[3] 一般社団法人 JPCERT コーディネーションセンター, “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 (第 2 版),” https://www.jpcert.or.jp/research/20171109ac-ir_research2.pdf, 2017 年 11 月 9 日, 参照 2020 年 8 月 7 日

[4] MITRE ATT&CK, https://attack.mitre.org/, 参照 2020 年 8 月 7 日

[5] Lockheed Martin, “GAINING THE ADBANTAGE,”https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gainin_the_Advantage_Cyber_Kill_Chain.pdf, 参照 2020 年 8 月 7 日

[6] Microsoft, “Server Message Block (SMB) Protocol,”https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb/f210069c-7086-4dc2-885e-861d837df688, 参照 2020 年 8 月 7 日

[7] Microsoft, “Server Message Block (SMB) Protocol Versions 2 and 3,”https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/5606ad47-5ee0-437a-817e-70c366052962, 参照 2020 年 8 月 7 日

[8] 海野 由紀, 森永 正信, 及川 孝徳, 古川 和快, 金谷 延幸, 津田 侑, 遠峰 隆史, 井上 大介, 鳥居 悟, 伊豆 哲也, 武仲 正彦,“標的型攻撃の被害範囲を迅速に分析するネットワークフォレンジック手法の提案,” 暗号と情報セキュリティシンポジウム (SCIS), 2018

[9] 海野 由紀, 森永 正信, 及川 孝徳, 古川 和快, 金谷 延幸, 津田 侑, 遠峰 隆史, 井上 大介, 鳥居 悟, 伊豆 哲也,“標的型攻撃の被害範囲を迅速に分析するネットワークフォレンジック手法の改良,” コンピュータセキュリティシンポジウム (CSS), p.1170 - 1177, 2018

[10] 海野 由紀, 森永 正信, 及川 孝徳, 古川 和快, 金谷 延幸, 津田 侑, 遠峰 隆史, 井上 大介, 鳥居 悟, 伊豆 哲也,“高速フォレンジック技術を利用した標的型攻撃の挙動分析,” 暗号と情報セキュリティシンポジウム (SCIS), 2020

[11] Yuki Unno, Takanori Oikawa, Kazuyoshi Furukawa, Masanobu Morinaga, Masahiko Takenaka, Tetsuya Izu, “High-Speed Forensic Technology Against Targeted Cyber Attacks (Extended Abstract),” The 20 International Conference on Network-Based Information Sys-

tems (NBiS-2017), 2017
[12] Yuki Unno, Takanori Oikawa, Kazuyoshi Furukawa, Masanobu Morinaga, Masahiko Takenaka, “High-Speed Forensic Technology for Promptly Analyzing Damage After Targeted Attacks,” FUJITSU SCIENTIFIC & TECHNICAL JOURNALVol. 53, No. 5, September 2017
[13] Microsoft, “Remote Procedure Call Protocol Extensions,” https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rpce/290c38b1-92fe-4229-91e6-4fc376610c15, 参照 2020 年 8 月 7 日, 参照 2020 年 8 月 7 日