SiSOC TOKYO

WannaCry ランサムウエアに関するレポート

2017 年 5 月 18 日（第 2 版）

東京大学大学院情報学環

セキュア情報化社会研究寄付講座

変更履歴

2017 年 5 月 18 日　第 2 版 検証内容および結果について追記

2017 年 5 月 16 日　初版

1. 概要

2017 年 5 月 12 日 頃から、WannaCry と呼ばれるランサムウエアの被害が相次いで報告されています[1][2][3]。本ランサムウエアは E メールに添付されたマルウエアなどを通じてインターネットに接続した端末が感染します。その後、組織内ネットワークの他の Windows 端末に対して、SMBv1 の脆弱性(CVE-2017-0145)や RDP(リモートデスクトップサービス)などのリモートアクセスサービスを悪用し、感染を広げます。

直接インターネットに接続していない端末であっても、感染端末からリモートアクセスが可能な場合は、感染端末を起点として、感染の被害を受ける可能性があります。インターネットに接続していない端末やサーバはセキュリティ更新プログラムの適用が遅れるケースも多いため、本マルウエアによる攻撃の影響の有無を確認し、適切な対処を取る必要があります。

2. 本マルウエアによる攻撃の影響を受ける可能性がある端末

以下いずれかの条件に該当する端末は影響を受ける可能性があります。

E メールの受信や Web サイトの閲覧を行なっている端末

現時点で、感染経路に関する情報は確認できていませんが、典型的なランサムウエアは E メールの添付ファイルを開く、あるいは不正なサイトに誘導されることによって感染するケースが多いです。

MS17-010 のセキュリティアップデートを未適用で、かつ SMBv1 を有効化してる端末

組織ネットワーク内での感染拡大の手法の 1 つとして、SMBv1 の脆弱性(CVE-2017-0145)を悪用することが報告されています[4]。

RDP を有効にしている端末

上記の脆弱性の悪用以外にも、RDP サービスを通じて感染を拡大させるとの情報があります[5]。

3. 攻撃シナリオ

図 1 は、E メールを通じてマルウエアに感染し、組織内の端末やサーバに感染を拡大させるシナリオの例です。

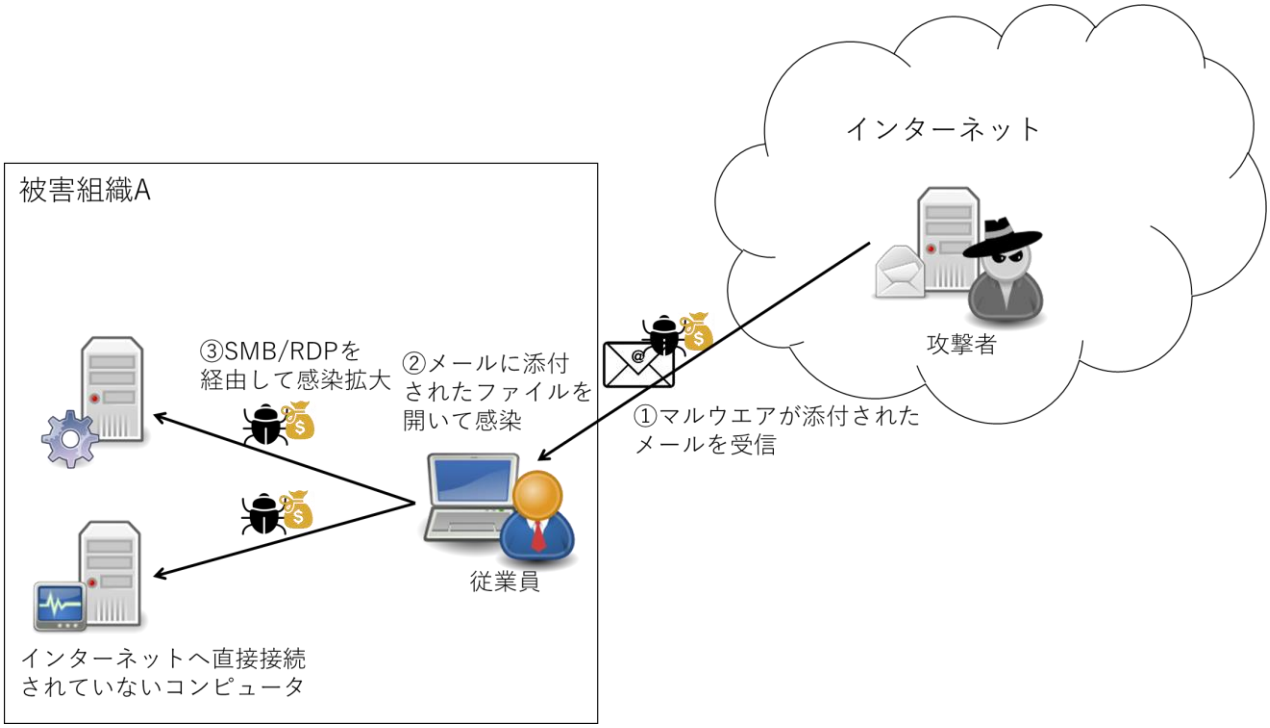


図 1. 攻撃シナリオの例

1. 攻撃者は、ターゲットにマルウエアが添付されたメールを送信する
2. 被害者が外部（インターネット）からメールを受信する端末にて、マルウエアの実行ファイルが添付されているメールを受信し、添付ファイルを開いたことによって当該端末が初期感染する
3. 感染した端末を起点として、IP リーチャビリティのある他の端末やサーバに感染が拡大する。このように、最初に感染した端末を起点として組織内での感染拡大を活動することを、以下「横展開」と呼びます。

4. 被害事例

英国国民保健サービス(NHS)

NHS を提供する一部の団体で被害が発生し、サービスが停止する事態になりました。これにより、レントゲン撮影や患者のファイルの閲覧などを行うことができなくなる、予定されていた手術が中止となるなどの業務影響が生じました[6]。

ドイツ鉄道

フランクフルトの駅などで　図 2 のように列車の発着時刻を表示する電光掲示板で障害が発生しました。

図 2．ドイツ東部にある Chemnitz 駅の電光掲示板[7]

国営中国石油天然気集団公司

直営のガソリンスタンドで、電子決済が利用できなくなる障害が発生し、現金支払いにて対応しました。

図 3. 中国のガソリンスタントにあるセルフサービス電子決済端末[6]

自動車製造会社

英国日産自動車製造会社やルノー子会社においても被害が発生し、一部製造ラインが停止する事態となりました[8]。

5. 検証

SiSOC にて、WannaCry の感染および感染後の挙動としてどのように横展開を行うのかについて検証しました。検証結果より、一部の環境で端末が WannaCry に感染し、端末のファイルが暗号化され、金銭を要求する画面が表示されることを確認しました。さらに、横展開によって他の端末やサーバに感染を拡大する動きが見られましたが、環境によって挙動が異なることがわかりました。

5.1. 検証環境

以下の仮想化された OS を使用しました。

- Windows Server 2008 R2 64bit
- Windows 7 Professional 64bit
- Windows XP Professional 32bit

表 1．検証環境

OS	Windows ファイアウォール	SMBv1
Windows Server 2008 R2 64bit	有効（デフォルト）	有効（デフォルト）
Windows 7 Professional 64bit	無効	有効（デフォルト）
Windows XP Professional 32bit	無効	有効（デフォルト）

5.2. 検証したマルウエア（検体）

WannaCry の初期（5 月 12 日ごろ）の検体を使用しました。セキュリティベンダにより検体名が異なるため、代表的なものをいくつか列挙します（カッコ内はセキュリティベンダ名）。

- Ransom.Wannacry（Symantec）
- Ransom-O（McAfee）
- Trojan-Ransom.Win32.Wanna.m（Kaspersky）
- WORM_WCRY.A（TrendMicro-HouseCall）

ハッシュ値は以下です。

MD5 db349b97c37d22f5ea1d1841e3c89eb4

SHA1 e889544aff85ffaf8b0d0da705105dee7c97fe26

SHA256 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

5.3. 検証結果の概要

初期感染を想定し、マルウエアを手動で動作させた端末の挙動は表 2 のようになりました。

表 2. マルウエアを手動で動作させた端末の挙動

OS	端末の挙動
Windows Server 2008 R2 64bit	マルウエアに感染し、ファイルが暗号化される
Windows 7 Professional 64bit	マルウエアに感染し、ファイルが暗号化される
Windows XP Professional 32bit	ブルースクリーンになる（マルウエアには感染しない）

初期感染端末（Windows Server 2008 R2 64bit）から、同一ネットワーク上に存在する端末への横展開の結果は表 3 のようになりました。初期感染から 10 分程度経過した時の挙動を記載しています。

表 3. 横展開の対象となった端末の挙動

OS	横展開に対する挙動
Windows Server 2008 R2 64bit	マルウエアに感染し、ファイルが暗号化される
Windows 7 Professional 64bit	以下 2 パターンの挙動を確認している。 ・マルウエアに感染し、ファイルが暗号化される ・ブルースクリーンになる（マルウエアには感染しない）
Windows XP Professional 32bit	ブルースクリーンになる（マルウエアには感染しない）

※上記はあくまで SiSOC にて検証で確認した結果であり、挙動は環境や検体によって異なる可能性があります。

5.4. 検証結果の詳細

マルウエアの実行ファイルを端末で実行したところ、図 4 のようにファイルが暗号化され、開くことができない状態になりました。

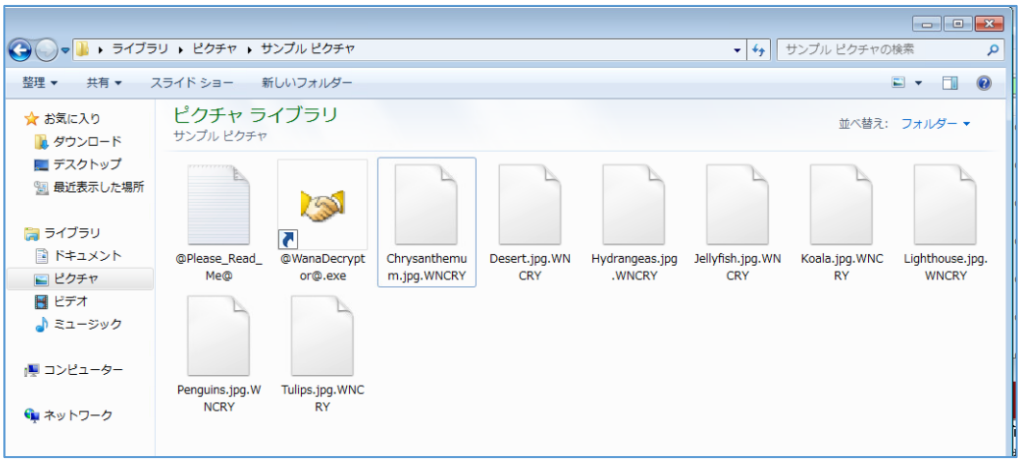


図 4. 暗号化されたファイルの例

なお、Windows Server では、シャドウコピーの機能（デフォルトでは無効）を使用して、共有フォルダのデータについて特定時点のコピーを保存し、復元することができます。検証では、Windows Server 2008 R2 でシャドウコピーを有効化し、マルウエアによって暗号化された共有フォルダのデータをシャドウコピーから復元できることを確認しました。詳細は以下を参照してください。

共有フォルダーのシャドウ コピーを有効にして構成する
https://technet.microsoft.com/ja-jp/library/cc771893(v=ws.11).aspx

さらに図 5 のような、金銭を要求する画面が表示されることを確認しました。日本語で 300 ドル分（2017 年 5 月 16 日時点で 3.4 万円）のビットコインを要求しています。

図 5. 金銭を要求する画面

マルウエア感染後の通信から、以下のような挙動を確認できます。

1. 特定のドメインへ接続を試みる

   感染した端末は、まず図 6 のように特定のドメインの名前解決を試みます。その後、そのドメインと疎通が取れない場合、「2 横展開を試みる」を行います。疎通が取れた場合、ここでマルウエアの活動は停止し、端末は感染せず、ファイルは暗号化されません。

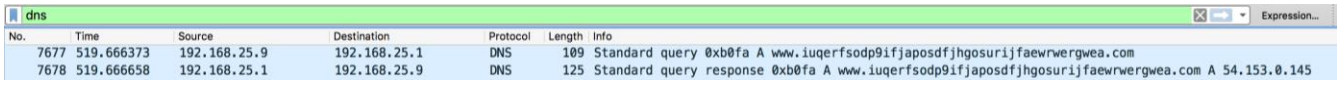
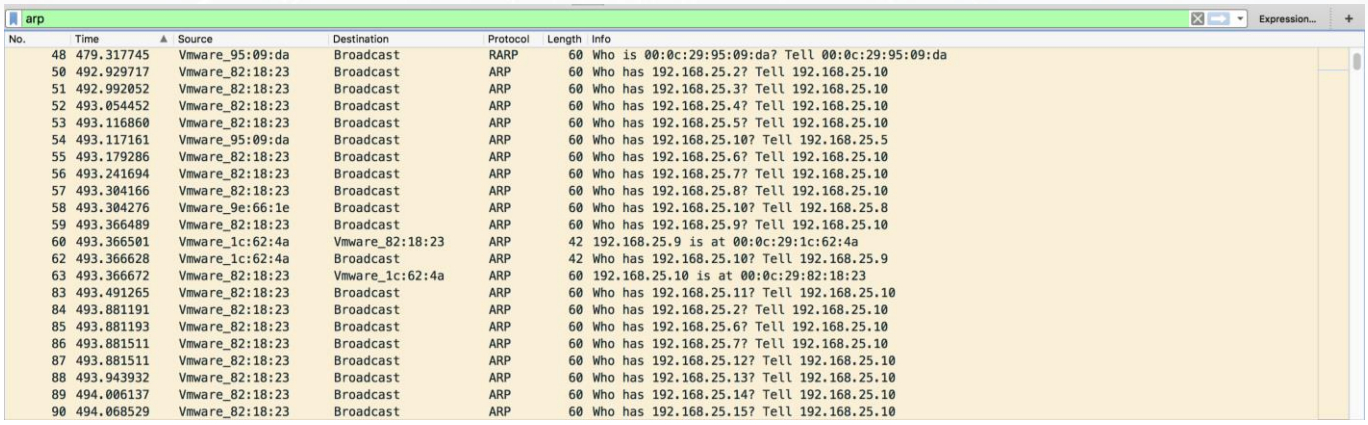


図 6. 特定のドメインへの通信

2. 横展開を試みる

横展開を行うため、図 7 のように IP アドレスを変更しながら、同一ネットワークで感染拡大できそうな端末を探索します。



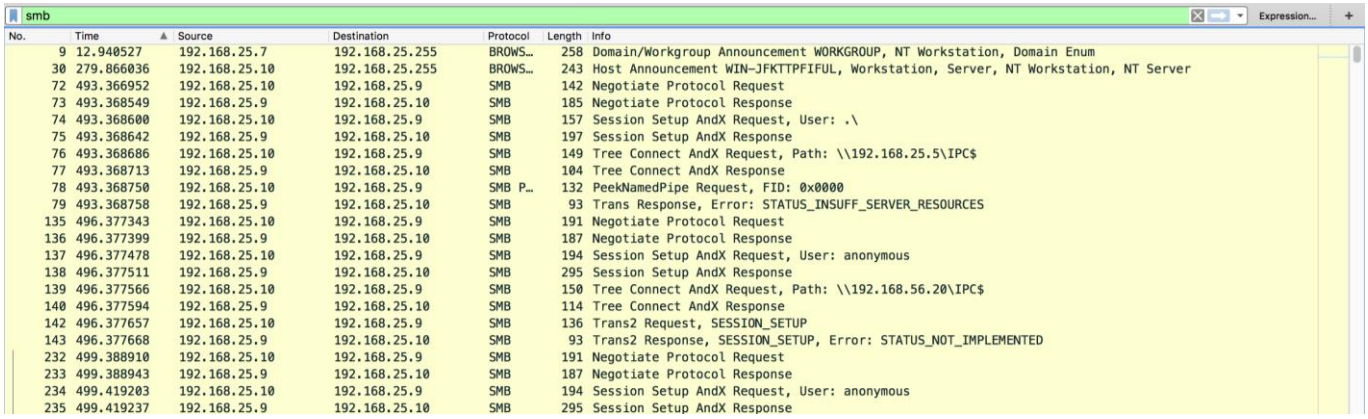
arp

No.	Time	Source	Destination	Protocol	Length	Info
48	479.317745	Vmware_95:09:da	Broadcast	RARP	60	Who is 00:0c:29:95:09:da? Tell 00:0c:29:95:09:da
50	492.929717	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.2? Tell 192.168.25.10
51	492.992052	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.3? Tell 192.168.25.10
52	493.054452	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.4? Tell 192.168.25.10
53	493.116860	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.5? Tell 192.168.25.10
54	493.117161	Vmware_95:09:da	Broadcast	ARP	60	Who has 192.168.25.10? Tell 192.168.25.5
55	493.179286	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.6? Tell 192.168.25.10
56	493.241694	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.7? Tell 192.168.25.10
57	493.304166	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.8? Tell 192.168.25.10
58	493.304276	Vmware_9e:66:1e	Broadcast	ARP	60	Who has 192.168.25.10? Tell 192.168.25.8
59	493.366489	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.9? Tell 192.168.25.10
60	493.366501	Vmware_1c:62:4a	Vmware_82:18:23	ARP	42	192.168.25.9 is at 00:0c:29:1c:62:4a
62	493.366628	Vmware_1c:62:4a	Broadcast	ARP	42	Who has 192.168.25.10? Tell 192.168.25.9
63	493.366672	Vmware_82:18:23	Vmware_1c:62:4a	ARP	60	192.168.25.10 is at 00:0c:29:82:18:23
83	493.491265	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.11? Tell 192.168.25.10
84	493.881191	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.2? Tell 192.168.25.10
85	493.881193	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.6? Tell 192.168.25.10
86	493.881511	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.7? Tell 192.168.25.10
87	493.881511	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.12? Tell 192.168.25.10
88	493.943932	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.13? Tell 192.168.25.10
89	494.006137	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.14? Tell 192.168.25.10
90	494.068529	Vmware_82:18:23	Broadcast	ARP	60	Who has 192.168.25.15? Tell 192.168.25.10

図 7. 感染拡大活動

3. SMBv1 の脆弱性の悪用によって感染を拡大する

図 8 のように、「2 横展開を試みる」で応答があった端末やインターネット上のグローバル IP アドレスを持った端末に対して、TCP445 番に対して SMBv1 の脆弱性を狙う攻撃を開始します。



smb

No.	Time	Source	Destination	Protocol	Length	Info
9	12.940527	192.168.25.7	192.168.25.255	BROWS…	258	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
30	279.866036	192.168.25.10	192.168.25.255	BROWS…	243	Host Announcement WIN-JFKTTPFIFUL, Workstation, Server, NT Workstation, NT Server
72	493.366952	192.168.25.10	192.168.25.9	SMB	142	Negotiate Protocol Request
73	493.368549	192.168.25.9	192.168.25.10	SMB	185	Negotiate Protocol Response
74	493.368600	192.168.25.10	192.168.25.9	SMB	157	Session Setup AndX Request, User: .\
75	493.368642	192.168.25.9	192.168.25.10	SMB	197	Session Setup AndX Response
76	493.368686	192.168.25.10	192.168.25.9	SMB	149	Tree Connect AndX Request, Path: \\192.168.25.5\IPC$
77	493.368713	192.168.25.9	192.168.25.10	SMB	104	Tree Connect AndX Response
78	493.368750	192.168.25.10	192.168.25.9	SMB P…	132	PeekNamedPipe Request, FID: 0x0000
79	493.368758	192.168.25.9	192.168.25.10	SMB	93	Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
135	496.377343	192.168.25.10	192.168.25.9	SMB	191	Negotiate Protocol Request
136	496.377399	192.168.25.9	192.168.25.10	SMB	187	Negotiate Protocol Response
137	496.377478	192.168.25.10	192.168.25.9	SMB	194	Session Setup AndX Request, User: anonymous
138	496.377511	192.168.25.9	192.168.25.10	SMB	295	Session Setup AndX Response
139	496.377566	192.168.25.10	192.168.25.9	SMB	150	Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
140	496.377594	192.168.25.9	192.168.25.10	SMB	114	Tree Connect AndX Response
142	496.377657	192.168.25.10	192.168.25.9	SMB	136	Trans2 Request, SESSION_SETUP
143	496.377668	192.168.25.9	192.168.25.10	SMB	93	Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
232	499.388910	192.168.25.10	192.168.25.9	SMB	191	Negotiate Protocol Request
233	499.388943	192.168.25.9	192.168.25.10	SMB	187	Negotiate Protocol Response
234	499.419203	192.168.25.10	192.168.25.9	SMB	194	Session Setup AndX Request, User: anonymous
235	499.419237	192.168.25.9	192.168.25.10	SMB	295	Session Setup AndX Response

図 8 . SMBv1 の脆弱性を悪用した感染活動

SMBv1 の脆弱性は任意のコード実行に繋がる脆弱性です。本脆弱性の悪用によって不正なコードを実行することに成功した場合は、横展開を行った端末に新たにマルウエアを設置します。結果として、その端末上でさらなる感染活動を開始し、ファイルを暗号化します。

6. 横展開に対する対策

SMBv1 の脆弱性を悪用した攻撃の対策を以下に記載します。

6.1. MS17-010 のセキュリティ更新プログラムを適用する

一連の攻撃は SMBv1 の脆弱性を悪用して感染拡大を試みます。セキュリティ更新プログラムを適用することで、本脆弱性悪用による横展開を防止することができるため、早期の適用をお勧めします[4]。表 4 に検証した OS と、それぞれの結果(初期感染から 10 分程度経過した時の挙動)を記載します。

表 4. MS17-010 のセキュリティ更新プログラムを適用後の挙動

OS	セキュリティ更新プログラム	横展開に対する挙動
Windows Server 2008 R2 64bit	KB4012212	影響を受けない(感染しない)
Windows 7 Professional 64bit	KB4012212	影響を受けない(感染しない)
Windows XP Professional 32bit	KB4012598	影響を受けない(感染しない)

7. 横展開に対する回避策

SMBv1 の脆弱性を悪用した横展開を回避するための手法を以下に記載します。

7.1. SMBv1 の無効化や SMBv1 が使うポートの閉鎖

SMBv1 の脆弱性を悪用する横展開を抑止するために、業務への影響を十分に検討の上、以下いずれかの回避策を適用することを検討してください。

各端末の設定で SMBv1 を無効化

各端末の設定で SMBv1 を無効化することを検討してください。詳細については以下を参考にしてください。

※「SMB サーバーで SMB プロトコルを有効/無効にする方法」と「SMB クライアントで SMB プロトコルを有効/無効にする方法」がありますが、本脆弱性の悪用による横展開を防止するためには

「SMB サーバーで SMB プロトコルを有効/無効にする方法」を実施してください。

How to enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server
https://support.microsoft.com/ja-jp/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012

表 5 に、SMBv1 の無効化についての検証結果を記載します。

表 5. SMBv1 を無効にした場合の挙動

OS	横展開に対する挙動
Windows Server 2008 R2 64bit	影響を受けない(感染しない)
Windows 7 Professional 64bit	影響を受けない(感染しない)
Windows XP Professional 32bit	Windows XP で SMBv1 を無効化する方法については未確認。Windows 7 と同様の方法を適用した場合「表 3 マルウエアの横展開の挙動」と同じ結果となり、脆弱性を悪用する攻撃を抑止することができなかった。

ファイアウォールなどを用いたポートの遮断

SMBv1 が使うポート（TCP 139 番や TCP 445 番など）に対する通信を遮断することも有効です。
表 6 は、Windows のパーソナルファイアウォールの機能を用いて、SMB 通信を遮断する設定にして検証を行った結果です。
なお、SMBv1 が使うポートは、ファイル共有やプリンターのアクセスなどで使われている可能性がありますので、業務への影響を十分に検討してから実施してください。

表 6. SMBv1 を無効にした後の挙動

OS	パーソナルファイアウォールのルール	横展開に対する挙動
Windows Server 2008 R2 64bit	ファイルとプリンターの共有（SMB 受信） ※デフォルトで遮断する	影響を受ける(感染する) ※遮断する設定になっていても、実際には横展開は防止できなかった
Windows 7 Professional 64bit	ファイルとプリンターの共有（SMB 受信） ※デフォルトで遮断する	影響を受けない(感染しない)
Windows XP Professional 32bit	ファイルとプリンターの共有 ※デフォルトで遮断する	影響を受けない(感染しない)

7.2. RDP の無効化

リモートデスクトップを運用で使用していない場合は、RDP を無効化することを検討してください。詳細については以下を参考にしてください。

リモート デスクトップ サービス接続を無効にする
https://technet.microsoft.com/ja-jp/library/cc731588(v=ws.11).aspx

またファイアウォールなどを用いて、RDP が使うポート（TCP 3389 番 など）に対する通信を遮断することも検討してください。業務に影響を及ぼす可能性があるため、十分なテストを実施のうえ適用することをお勧めします。

図 9 は、対策や回避策の適用イメージです。

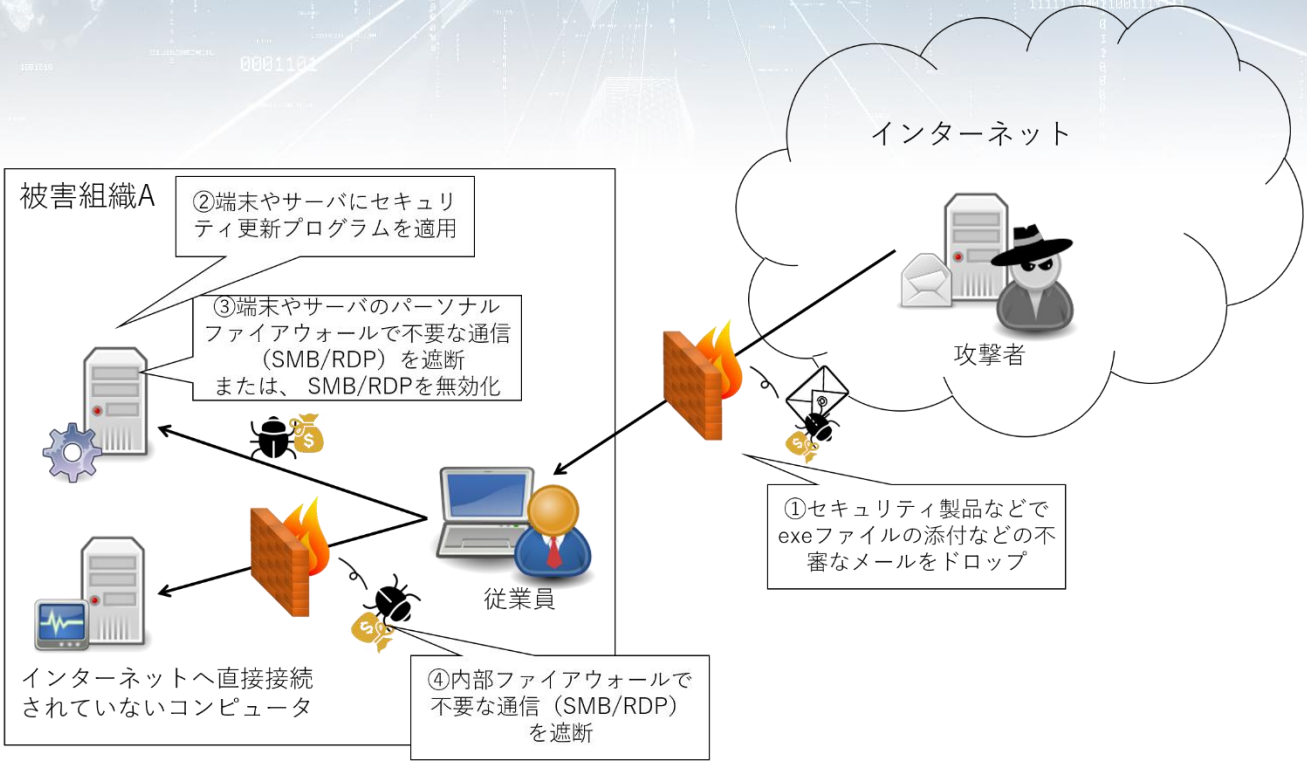


図 9．対策の例

8． マルウエアの検知に関する情報

ファイル名、ハッシュ値などに関する情報については、以下を参考にしてください。

https://www.us-cert.gov/ncas/alerts/TA17-132A

通信先ドメインなどに関する情報については、以下を参考にしてください。

https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/

9. 参考情報

[1] Alert (TA17-132A) Indicators Associated With WannaCry Ransomware
https://www.us-cert.gov/ncas/alerts/TA17-132A

[2] ランサムウエア "WannaCrypt" に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170020.html

[3] An Analysis of the WannaCry Ransomware Outbreak
https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/

[4] マイクロソフト セキュリティ情報 MS17-010 - 緊急
https://technet.microsoft.com/ja-jp/library/security/ms17-010.aspx

[5] Use a Zero Trust Approach to Protect Against WannaCry
https://blogs.vmware.com/networkvirtualization/2017/05/use-zero-trust-protects-against-wannacry.html/

[6] WannaCry Ransomware Outburst
https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

[7] BBC News : WannaCry ransomware cyber-attacks slow but fears remain
http://www.bbc.com/news/technology-39920141

[8] Carmaker Nissan says UK plant hit by cyber attack
http://www.reuters.com/article/us-cyber-attack-nissan-idUSKBN1890EK

東京大学大学院情報学環セキュア情報化社会研究寄付講座

〒113-0033
東京都文京区本郷 7-3-1
TEL: 03-5841-1902
EMAIL: sisoc-sec@iii.u-tokyo.ac.jp