ランサムウェアの人質にならないために（VPN、RDP 他）

目次

ランサムウェアの人質にならないために（VPN、RDP 他）

はじめに

2024 年の 6 月に動画配信も行っている日本の大手出版会社がサイバー攻撃を受け、一か月経っても動画配信の復旧ができないという状況が発生しました。詳細な手口は公表されていませんが、被害は ①「サイト内の情報を暗号化し、復号鍵の対価」、②「盗み出した個人情報等のファイルを公開しない対価」の 2 段階で受けたようです。この攻撃は暗号化で拘束されたデータの身代金（ransom）を要求するのでランサムウェア攻撃と呼ばれます。世界で最初のランサムウェア攻撃は 1989 年の、「AIDS Trojan」というマルウェア[1]とこれを起動する AUTOEXEC.BAT をフロッピーに書き込んで配布したもので、挿入と同時にマルウェアが起動してハードディスクを暗号化するというものでした。今回の事件では恐らくインターネット経由による侵入で、暗号化だけでなく 1.5T バイトのデータが犯人の手元にコピーされてこれも人質に使われています。

現代（VisualBasic 世代以降）のシステム開発はインターネットに接続して情報取得することが前提になりましたが、在宅勤務が一般化してからは逆にインターネット側から企業の内部ネットワークに接続して作業をするようになりました。外部から接続することの危険性については、具体的にどのような攻撃が行われ、何から身を守らなければいけないのかという情報はあまり知らされてきませんでした（方法を知って試されるのも怖いですが）。システム管理者以外の開発担当者／利用者の身の回りにどんな危険があるのか Windows を使った場合で考えます。

1. 侵入の道具は VPN、RDP？

警視庁のサイト https://www.npa.go.jp/publications/statistics/cybersecurity/ に「サイバー空間をめぐる脅威の情勢等」という情報が掲載されています。この中の 令和 5 年におけるサイバー空間をめぐる脅威の情勢等について(4.12MB) によれば、ランサムウェアの被害にあった企業・団体等が回答した（有効数 115 件）感染経路は、VPN 機器からの侵入が 73 件で 63%、リモートデ スクトップからの侵入が 21 件で 18% …テレワーク等に利用される機器等のぜい弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが約 82%と大半を占めた…そうです。

この情報からは、「機器（ファームウェアやミドルウェア含む）を常に最新化し、パスワード等を定期的に変更する」という対策が出てきそうですが、これに関して以下のような疑問があります。

① 63%+18%=82%という計算式は正しい？ 社外からアクセスできる RDP ポートなんてある？[2]
… VPN 上の RDP 等、実際の攻撃パターンが把握できていないとしたら対策の正しさも疑わしい

② VPN 機器や RDP の認証情報の脆弱性を直接狙ったのであれば、システム管理者の対策で十分？
… もっと簡単な攻撃方法（弱点）がありそうだけど

---

[1] 警視庁 マルウェア「ランサムウェア」の脅威と対策（脅威編）
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_threat.html

[2] 念の為調べたところ、RDP ポート（3389）に対する侵入の試みは行われていて、更にファイル共有ポート（445）まで試されているので、ノーガード戦法を採っている組織もあるのかもしれません
〔情報通信研究機構〕NICTER 観測レポート 2023 https://www.nict.go.jp/press/2024/02/13-1.html

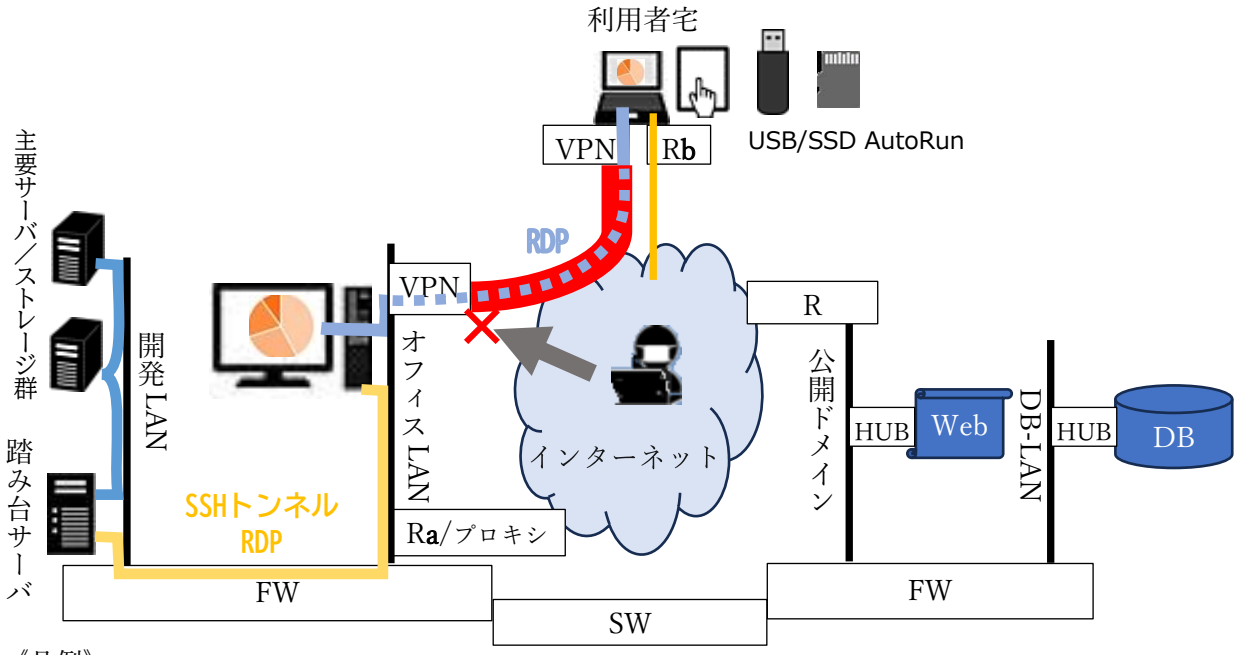
ランサムウェアの人質にならないために（VPN、RDP 他）

2. VPN

VPN（Virtual Private Network）は許可された利用者だけがアクセスできる仮想のネットワークで、拠点（VPN 機器）間の接続は暗号化によりトンネル化されて利用者からは透過的に LAN に参加しているように見えます。

2.1. VPN とネットワークの構成例

ネットワーク下層では通信会社の専用回線／サービスを使う使わない等 VPN の実現方式はいくつかありますが、物理的な中継機器を抽象化して赤いトンネルで表現すると下図のようになります。



《凡例》

VPN …VPN 機器

R、Ra、Rb …ルーター

SW …スイッチングハブ

FW …ファイアウォール

※ 上記通信機器は複数の機能をもっている（VPN 機能付きルータ、L3 スイッチ等）場合がありますが、当該箇所で主に必要な機能を記載しています

《利用事例》

・自宅 PC から日常業務を行うオフィス LAN に VPN で接続し、会社 PC にリモートデスクトップ（RDP）でログインする。自宅 PC は VPN を通さずにインターネットに接続できる経路がある

・オフィス LAN から開発 LAN へは開発 LAN の踏み台サーバを使って接続する。接続の方法は ssh、scp または ssh のポートフォワーディングでリモートデスクトップを使う

・公開ドメインの Web サイトや DB-LAN にも保守担当者が VPN 接続をする環境を作った場合その IP／ポートを公開することでリスクが上がりますが、ここでは一般利用に話を絞ります

ランサムウェアの人質にならないために（VPN、RDP 他）

2.2. 脅威が生じる場所

ネットワークのセキュリティ強度はネットワーク上の一番脆弱な場所と同一の水準まで低下します。

自宅 PC は VPN を通してネットワークの一部になるため自宅 PC に侵入されると利用者の権限が使われてオフィス LAN と接続している全ての LAN が侵入可能になります。自宅 PC のインターネットへの経路や媒体の挿入口がネットワークの弱点となり、侵入を受ける可能性があります。

3. RDP 他

RDP は通信パケットの暗号化を選択することができます[3]が、利用者の認証は ID とパスワードを基にして行います。パスワードが送られることはありません（平文でもハッシュ値でも）が、攻撃者は辞書攻撃や総当たり攻撃等の古典的な攻撃手法を使うことができます。また、過去に利用者名簿が漏れていると、同一の ID とパスワードの組合せで侵入が試されます。(VPN の認証方式は製品により幾つか選択肢がありますが、証明書等による強度の高いクライアント[端末]認証が行われます)

また、リモートデスクトップの接続は個人単位なので、VPN を経由しないで離れた拠点に接続するためには利用者の数だけポートを解放することになり脅威が飛躍的に増大します。

ファイル共有の Windows SMB1.0（SMBv1）は 2017 年に現れたランサムウェア「WannaCry」でとても有名になりました。WannaCry は某国家機関が脆弱性を発見して開発した EternalBlue というソフトウェアが流出して使われたそうですが、このツールは今でもネットに公開されています[4]。

EternalBlue は SMBv1 のドライバのバグを利用し、リモートでコードを実行するマルウェアです。

※ Windows10 以降は最新化さえしていれば SMBv1 は無効になっているはずです

RDP の危険性は、現在でも新しい脆弱性が見つかっている点にもあります。

＜Microsoft セキュリティ レスポンス センター＞

https://msrc.microsoft.com/update-guide/vulnerability

remote desktop でフィルタリング

リリース日	最終更新日	CVE番号 ↓	CVE のタイトル	影響	最大度	タグ
2024年7月9日	-	CVE-2024-38099	Windows リモート デスクトッ	サービス拒否	重要	Windows リモート デスクトッ
2024年7月9日	-	CVE-2024-38077	Windows リモート デスクトッ	リモートでコードが実行される	緊急	Windows リモート デスクトッ
2024年7月9日	-	CVE-2024-38076	Windows リモート デスクトッ	リモートでコードが実行される	緊急	Windows リモート デスクトッ
2024年7月9日	-	CVE-2024-38074	Windows リモート デスクトッ	リモートでコードが実行される	緊急	Windows リモート デスクトッ
2024年7月9日	-	CVE-2024-38073	Windows リモート デスクトッ	サービス拒否	重要	Windows リモート デスクトッ
2024年7月9日	-	CVE-2024-38072	Windows リモート デスクトッ	サービス拒否	重要	Windows リモート デスクトッ

[3] リモート デスクトップ プロトコル
https://learn.microsoft.com/ja-jp/windows/win32/termserv/remote-desktop-protocol

[4] Eternalblue-2.2.0.exe
https://github.com/x0rz/EQGRP_Lost_in_Translation/tree/master/windows/specials

ランサムウェアの人質にならないために（VPN、RDP 他）

4. 侵入の手順と対処

ネットワークへの侵入を防ぐためにはネットワークに接続している全ての装置や通信機器を安全に保つ必要がありますが、攻撃する側は穴を一つ見つければ十分です。

4.1. 準備段階

具体的な侵入の手順として以下のようなことが考えられます。

① 標的になる企業の社員名簿／メール連絡先等を手に入れる
ランサムウェアの標的になった大手出版社の海外子会社が過去に侵入されていたようです

② 社員のパスワードや個人情報を収集する
名簿やサイトに公開されている社員や企業の取引先にメールや SMS を送り（フィッシング）、偽装サイトに誘導するか直接マルウェアをメールに添付する

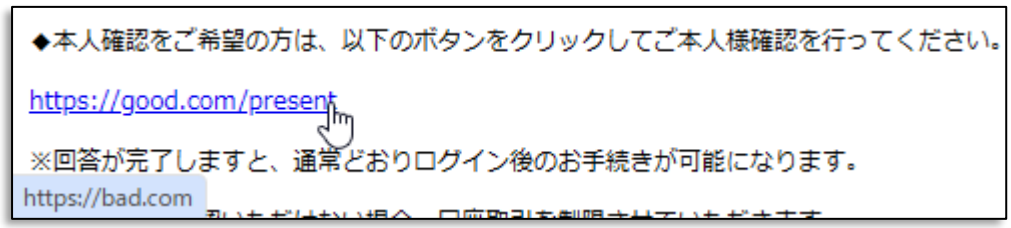
③ 誘導先の偽装サイトでパスワードを入力させたり、マルウェアをダウンロードさせる

④ 過去に PC の OS やブラウザの脆弱性を狙いアクセスしただけでマルウェアのインストールを行う（Drive-by Download 攻撃）JavaScript を、スマートホン向けサイトに広告に隠して仕込む

＜送られてきたフィッシングの例（一部抜粋：Base64 だったものをデコードし URL は変更）＞

```
----------------------
<P>◆本人確認をご希望の方は、以下のボタンをクリックしてご本人様確認を行ってください。
</P>
<P><A href="https://bad.com">https://good.com/present</A></P>
<P>※回答が完了しますと、通常どおりログイン後のお手続きが可能になります。</P>
----------------------
```

＜メールに表示される該当部分＞



※近年は日本語に違和感がなく、ビジネスルールを心得た文面になっています
また、トップレベルドメインは.cn、.xyz から.com 等のそれらしいものに変わっています

4.2. 常駐環境をつくる

侵入した PC を足場にするためにマルウェアが常時起動した状態をつくります。利用者が管理者権限を持っていればそれも利用できます。最初に攻撃者がダウンロードさせるのは exe 形式とは限らずスクリプトの場合もあります。特に Windows であれば[5]Powershell から.net API を利用できるので、面倒なプログラミング無しにその場で侵入するための武器を作ることができます。

---

[5] Linux と macOS 向け開発物と異なり、Windows 向けは OS 周りの環境変更が可能です
https://learn.microsoft.com/ja-jp/powershell/scripting/whats-new/unix-support?view=powershell-7.4

ランサムウェアの人質にならないために（VPN、RDP 他）

常駐に使える Windows の主要な機能と、状態確認の方法は以下があります。

① スタートアップフォルダ

利用者個人用または全利用者用のスタートアップフォルダに格納します。
スタートアップフォルダの内容はエクスプローラから以下を参照することで確認できます。
利用者…shell:startup、全利用者…shell:common startup

② レジストリキー

レジストリに登録されたコマンドが実行されます。
具体的なキー値はマイクロソフト社のサイト「Run および RunOnce レジストリ キー」参照
https://learn.microsoft.com/ja-jp/windows/win32/setupapi/run-and-runonce-registry-keys

＜以下、レジストリ内容を表示する Powershell のコマンド例＞

```
Get-Item 'HKLM:¥Software¥Microsoft¥Windows¥CurrentVersion¥Run'
Get-Item 'HKLM:¥Software¥Microsoft¥Windows¥CurrentVersion¥RunOnce'
Get-Item 'HKCU:¥Software¥Microsoft¥Windows¥CurrentVersion¥Run'
Get-Item 'HKCU:¥Software¥Microsoft¥Windows¥CurrentVersion¥RunOnce'
```

③ タスクスケジューラ―

● タスクスケジューラ―に登録されているタスクは Get-ScheduledTask で確認できます。

```
PS C:\Users\remoteuser> Get-ScheduledTask

TaskPath                                    TaskName                          State
--------                                    --------                          -----
\                                           OneDrive Per-Machine Standalon... Ready
\                                           OneDrive Reporting Task-S-1-5-... Ready
\Microsoft\Office\                          IMESharePointDictionary           Ready
\Microsoft\Office\                          Office Automatic Updates 2.0      Ready
（以下略）
```

● 実行中のタスクの詳細は、以下のコマンドラインで確認できます。

```
Get-ScheduledTask | ? State -eq running | Get-ScheduledTaskInfo
```

```
PS C:\Users\remoteuser> Get-ScheduledTask | ? State -eq running |Get-ScheduledTaskInfo


LastRunTime        : 2024/07/24 9:28:28
LastTaskResult     : 267009
NextRunTime        :
NumberOfMissedRuns : 0
TaskName           : SystemSoundsService
TaskPath           : \Microsoft\Windows\Multimedia\
PSComputerName     :

LastRunTime        : 2024/07/24 12:29:29
LastTaskResult     : 267009
NextRunTime        :
NumberOfMissedRuns : 0
TaskName           : CacheTask
TaskPath           : \Microsoft\Windows\Wininet\
PSComputerName     :
```


● 次の起動予定が登録されているスケジュールは、以下のコマンドラインで確認できます。

```
Get-ScheduledTask | Get-ScheduledTaskInfo | ? {$_.NextRunTIme.count -ne 0} `
| sort Nextruntime | select TaskPath, LastRunTime, NextRunTime
```

※１行目末尾の[`]はコマンドラインを２行に分けるために改行をエスケープしたものです

```
PS C:\Users\remoteuser> Get-ScheduledTask | Get-ScheduledTaskInfo | ? {$_.NextRunTIme.count -ne 0} `
>> | sort Nextruntime | select TaskPath, LastRunTime, NextRunTime

TaskPath                                                LastRunTime         NextRunTime
--------                                                -----------         -----------
\Microsoft\Windows\Flighting\FeatureConfig\             2024/07/09 12:35:35 2024/07/24 13:35:35
\Microsoft\Windows\Offline Files\                       1999/11/30 0:00:00  2024/07/24 14:06:06
\Microsoft\Windows\Application Experience\              2024/07/24 9:33:33  2024/07/24 15:38:38
\Microsoft\Windows\Application Experience\              2024/07/24 9:33:33  2024/07/24 15:54:54
\Microsoft\Windows\Storage Tiers Management\            1999/11/30 0:00:00  2024/07/24 17:00:00
\Microsoft\Windows\Windows Error Reporting\             2024/07/24 9:33:33  2024/07/24 17:12:12
\Microsoft\Office\                                      2024/07/24 11:04:04 2024/07/24 17:53:53
\Microsoft\Windows\Customer Experience Improvement Program\ 2024/07/24 12:00:00 2024/07/24 18:00:00
\Microsoft\Windows\Flighting\OneSettings\               2024/07/24 10:30:30 2024/07/24 19:09:09
\Microsoft\Windows\Data Integrity Scan\                 1999/11/30 0:00:00  2024/07/24 23:03:03
\Microsoft\Windows\Maps\                                1999/11/30 0:00:00  2024/07/25 0:10:10
\Microsoft\Windows\Security\Pwdless\                    2024/07/24 9:42:42  2024/07/25 3:00:00
```

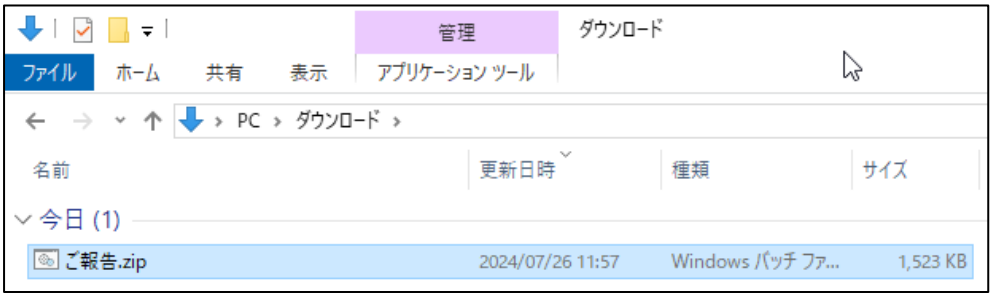
④ Windows PowerShell でスケジュールされたジョブ

PowerShell のバックグラウンド ジョブとタスクスケジューラ タスクの便利なハイブリッド[6]で、登録されていれば Get-Scheduledjob で表示できます。

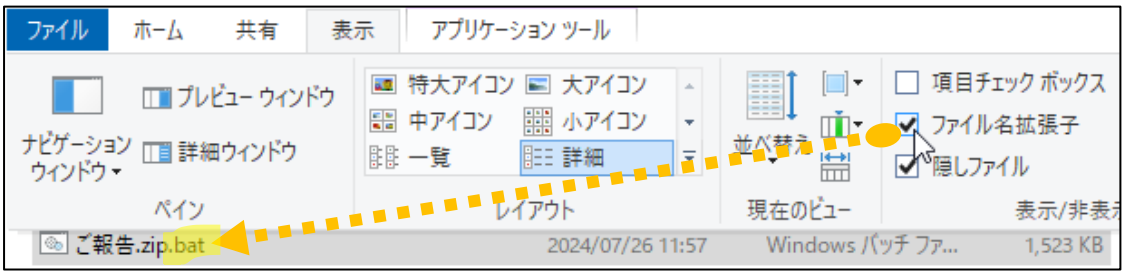
4.3. 侵入者による環境操作例

PowerShell の場合、情報収集の Get に対応する更新系の Create、Add、Registry.SetValue があります。前項で紹介した機能の更新系を書いたテキストファイルを実行に導けば侵入が成功します。

例えば、メールの誘導で偽取引先のサイトから～.zip という名前のファイルをダウンロードします。



ファイル拡張子が隠されていて（Win10,11 のデフォルト）、中身を確認するためにダブルクリック



[6] about_Scheduled_Jobs https://learn.microsoft.com/ja-jp/powershell/module/psscheduledjob/about/about_scheduled_jobs?view=powershell-5.1&viewFallbackFrom=powershell-7.4

「ご報告.zip.bat」の中身が以下のようになっていたら

```
----------------------
powershell -c "Start-Process powershell -Verb runAs -ArgumentList '$global:p=Join-Path $env:TEMP ''¥poweshell-admin.output'';echo 侵入中 >>$p;echo $p;sleep 100'"
----------------------
```

このスクリプトが起動すると、

① 管理者の PoweShell ターミナルが起動し

② 環境変数 TEMP のディレクトリにファイル poweshell-admin.output を作って“侵入中”という文字列を書き込み

③ 100 秒停止後、ターミナルが閉じます（sleep が無ければ①、②実行後すぐに閉じます）

※ このスクリプトは temp ディレクトリにファイルを 1 つ作る以外の害はありせんが、echo の部分が攻撃用のコマンドであれば管理者の権限で PC を操作、環境変更することができてしまいます。但し、幸いなことに Windows10､11 のデフォルト設定ではダウンロード後に起動する際や管理者の権限で実行する際には許可するか否かの確認のダイアログが表示されます。

【注意】・ファイルの拡張子は常時 表示させておいてください。

・身に覚えがない実行の許可確認が表示された場合はキャンセルか esc キーを押下し、どのアクションで何がされようとしたのかを確認してください

5. Windows への接続ツールと注意点

Windows から Windows への接続のために RDP（Remote Desktop Protocol：アプリは mstsc.exe）がデフォルトでインストールされていますが、それ以外にも Windows10 以降の PC には Linux で培われてきたオープンソースのソフトウェアがインストールされています。過去には TeraTerm や Putty 等のアプリを使ってネットワークの作業を行っていた場面が ssh コマンドで代替えできます。これは侵入者にとってもとても便利なツールです。他にも自由に使える接続ツールがあり、それらの注意点は以下のとおりです。

5.1. Windows RDP（リモートデスクトップ）

認証情報を保存して ID/パスワードを省略する環境にしていると侵入者にとっても好都合です。更に、通常は 1 セッションの開通だけが許されており、他から接続要求があると開設済のセッションに切断してよいかという問い合わの後に新たなセッションが開設されますが、これは簡単なパッチをあてることで並列した複数セッションを実行可能にできます（これはライセンス違反状態です）。

5.2. FreeRDP

公開されている RDP の技術情報を使ったオープンソースの実装で、Linux や Mac、タブレットやスマートホンに対応したソフトウェア（サーバ、クライアント）が開発されています。Windows を含め相互接続ができ、認証方法の拡張がされ、オープンソースのため脆弱性に素早く対処できることを有利な点としてうたっています。攻撃者にとってはマイクロソフト社製 RDP サーバへの攻撃道具に使ったり、サーバ機能を送り込んでバックドアにすることができます。

https://github.com/FreeRDP/FreeRDP

ランサムウェアの人質にならないために（VPN、RDP 他）

5.3. Chrome リモート デスクトップ

Google アカウントと Google Chrome 等の WebRTC を実装した Web ブラウザを使って家や職場のパソコンへのリモート アクセスや他のユーザーとの画面の共有を簡単に行うことができます。

主な用途は、外出先から自宅の PC を操作したり第三者と画面を通して情報共有することですが、VPN 環境内の PC に Chrome リモート デスクトップのホスト機能をインストールすると Google 社のサイトを経由してオフィス LAN のファイアウォールに穴を開けたのと同じ状態になります。

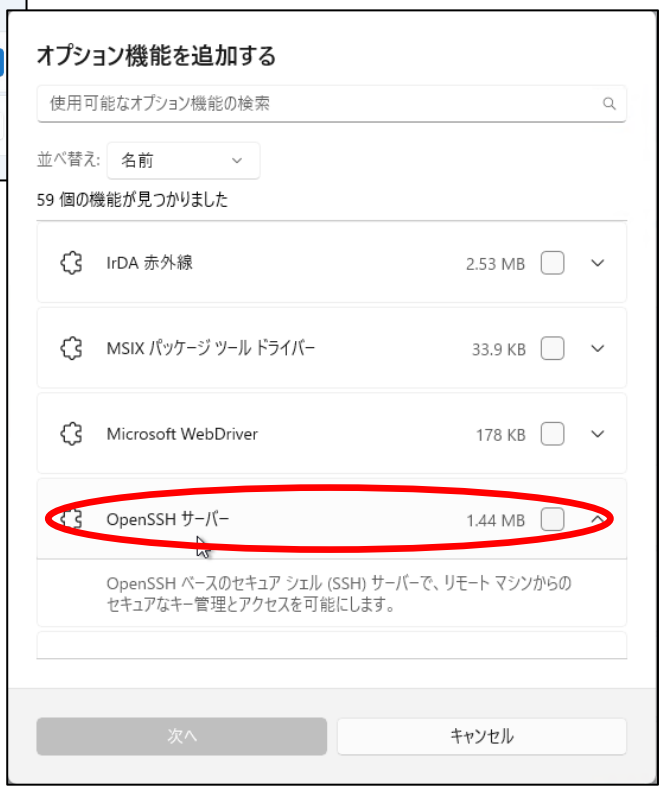
VPN 利用者宅で個人的に使う場合でも、2 段階認証を使えば一般的にはセキュリティ強度は上りますがウィルス等によるスマートホン乗っ取りや SIM スワップ等の被害がニュースになっている昨今では完全とはいえません（まぁ、スマホを盗られたら PC を気にするどころではないかもですが...）。

5.4. OpenSSH サーバとファイルウォール

OpenSSH サーバが有効になっていると ssh コマンドで接続したり scp でファイルコピー（入出共）が可能になります。設定は以下の手順で確認できます。

スタートボタンを右クリックしてシステムを選び、「オプション機能」をクリックします。

（画面が少し異なりますが、Windows 10 と 11 のメニュー構成は同じ）



侵入者は画面を表示すること無く、
Add-WindowsCapability で設定を変えられます

＜ファイアウォールの確認＞

ポートは Get-NetFirewallPortFilter で設定を確認します。ssh のデフォルトの 22 ポートの設定を見たい場合は、管理者として開いたターミナルから以下を実行します。更に詳細なファイアウォールの設定値は Get-NetFirewallRule をパイプで連結して確認します。

```
Get-NetFirewallPortFilter | ?{$_.LocalPort -eq 22}
Get-NetFirewallPortFilter | ?{$_.LocalPort -eq 22} | Get-NetFirewallRule
```


5.5. その他（WSL、Git Bash）

Windows10 以降、WSL (Windows Subsystem for Linux)が入っていて Linux 環境のインストールが簡単にできます。また、近年の開発で定番の Git を Windows にインストールすると bash ターミナルと Linux の基本的なコマンドがインストールされ、その中にも ssh サーバや証明書を作ったり公開鍵をサーバに登録するためのコマンド等が入っています。

攻撃者がこれらを使って、以下のことができます。

① 利用者の公開鍵や暗号鍵を自分のもので置き換える

② Windows にプレインストールの OpenSSH サーバとは別のポートで起動してバックドアを作る

```
$ where ssh*
C:\Tools\Git\usr\bin\ssh-add.exe
C:\Tools\Git\usr\bin\ssh-agent.exe
C:\Tools\Git\usr\bin\ssh-copy-id
C:\Tools\Git\usr\bin\ssh-keygen.exe
C:\Tools\Git\usr\bin\ssh-keyscan.exe
C:\Tools\Git\usr\bin\ssh-pageant.exe
C:\Tools\Git\usr\bin\ssh.exe
C:\Tools\Git\usr\bin\sshd.exe
C:\Windows\System32\OpenSSH\ssh-add.exe
C:\Windows\System32\OpenSSH\ssh-agent.exe
C:\Windows\System32\OpenSSH\ssh-keygen.exe
C:\Windows\System32\OpenSSH\ssh-keyscan.exe
C:\Windows\System32\OpenSSH\ssh.exe
C:\Tools\TortoiseGit\bin\sshaskpass.exe
C:\Users\User\AppData\Local\UniGetUI\Chocolatey\bin\ssh-copy-id.exe
```

6. 侵入者によるネットワーク内部の探索

侵入者は足場を作ったら次の侵入可能なネットワーク上の資材（サーバやストレージ）を探します。

Windows 固有のネットワーク関係の情報収集コマンドがあり、Windows 7 以前からデフォルトでインストールされています。侵入者はすぐに以下の情報を使って侵入を試みることができます。

（1）コンピューター上で共有されているリソースの一覧

```
net view
```

オプションなしで使用した場合は、現在のドメインまたはネットワークのコンピューターの一覧が表示されます。

（2）Windows の NBT（NetBIOS over TCP/IP）を使った接続先

```
nbtstat -c
```

-c（cache） NBT のキャッシュにあるリモート [コンピューター] 名と IP アドレスを一覧表示

（3）DNS キャッシュ

```
ipconfig /displaydns
```

/displaydns DNS リゾルバー キャッシュの内容を表示します。

ランサムウェアの人質にならないために（VPN、RDP 他）

7. ネットワークの確認方法

侵入に気づいたら LAN ケーブルを抜き無線ルータの電源を切ってセーフモードで再起動をするべきでしょうが、PowerShell や前項で紹介したツールはアンチウィルスソフトの処理対象になりません。検知されるのは恐らく、別のサーバ等に侵入して管理者の権限を奪おうとしたときです。

もし、システム管理者から権限外のファイルにアクセスしてアラートがあがったという注意を受けたり、自分が実行している処理と関係なく突発的にネットワークのトラフィックが上昇したという場合は、以下のコマンドで他ほホストと接続しているポートと使用しているファイルを確認できます。

netstat -an

-a　すべての接続とリッスン ポートを表示します。

-b　それぞれの接続またはリッスン ポートの作成に使われた実行可能ファイルを表示します。(管理者として実行している必要あり…以下詳細略)

-n　アドレスとポート番号を数値形式で表示します。(n でサービス名検索の時間を節約可能)

8. パスワードやパスフレーズの強度

認証は多くの場合、ID とパスワードを使って行います。証明書や公開鍵方式を使った場合でも暗号鍵はコピー可能なファイルなのでパスフレーズで暗号化して保護するか、外部媒体に保存します。スマホやタブレットが一般化してからは生体認証やワンタイムパスワード、2 段階認証が組み合わせられるようになりましたが、企業内の LAN でサーバを利用する場合はパスワードを知っているか否かで本人確認を行うのがまだ一般的です。

パスワードの攻撃方法は辞書攻撃 Dictionary、ブルートフォース brute-force、レインボーテーブル rainbow tables、ルールベース Rule-based 他 がありクラッキングツールや辞書集が出回っています。

攻撃に共通しているのは人間の思考を模倣することで、以下が試されます。

・辞書に載ってる単語

・オーo をゼロ 0、q を 9、a を@ 等の置き換えを行う

・Password という単語と 0 ～ 9999 を組み合わせる

・キーボードの配置を使い、1234567890-^¥

・過去に流出したことがある ID とパスワードの組合せ

※ これらは簡単に解読されます

高性能な CPU を使って時間無制限でブルートフォース攻撃を実行されたら破れないパスワードはありませんが、3 回失敗で 10 秒間受け付けを停止する等の運用と辞書に載っていない（人間が発想しない）文字列をパスワードに設定することで実用に耐えるようになります。

例えば以下のように、文字列そのものではなく文字列導出ルールを**自分だけで**決めておきます。

① 社員番号にパスワードの変更日と変更時間（厳密である必要はない）を足してブレを加味する

② 先頭の数字をアルファベットの小文字に（9⇒i)、3 文字目を大文字（2⇒B）

※ 変更日等はメモっておいても不自然ではないでしょう...たぶん

以上

