

サイバーセキュリティ対策セミナー

令和4年度 第1期

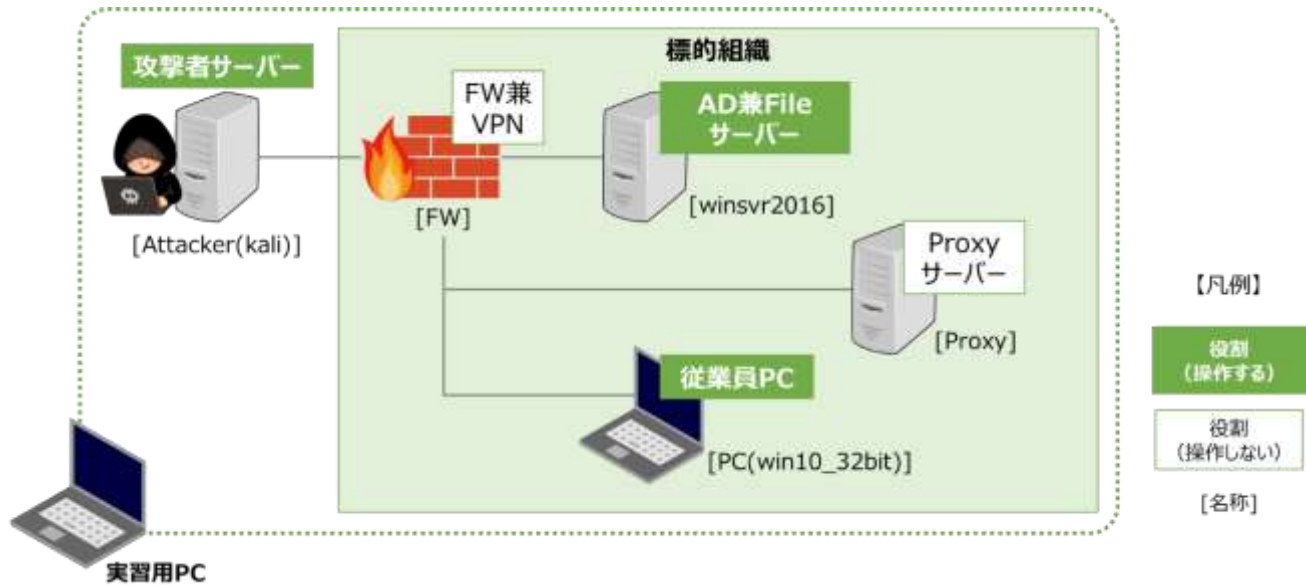
実習手順書

目次

1. 実習環境の構成	3
2. Emotet 感染・対応の体験.....	4
2.1 攻撃 & 被害体験	5
2.2 感染が疑われる場合の対応	8
2.3 感染を防ぐための事前対策	17
3. ランサムウェア感染・対応の体験	20
3.1 攻撃 & 被害体験	21
3.2 感染時の対応	27
3.3 感染に備える事前対策	45

1. 実習環境の構成

実習環境の構成は、次の通りです。



実習用 PC 上（仮想環境）で、5 台のサーバーや PC が、それぞれ独立して動作しています。

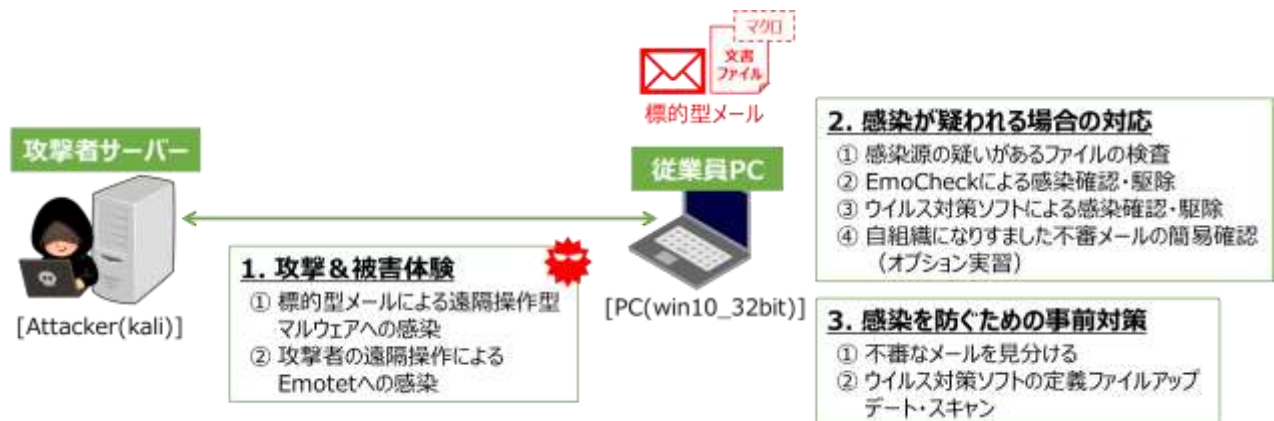
「2. Emotet 感染・対応の体験」では、「攻撃者サーバー」と「従業員 PC」、

「3. ランサムウェア感染・対応の体験」では、「攻撃者サーバー」と「AD 兼 File サーバー」

をそれぞれ操作しながら、実習を進めます。

2. Emotet 感染・対応の体験

標的型メール攻撃の理解を深めるために、Emotet を例に「**攻撃&被害体験**」、「**感染が疑われる場合の対応**」、「**感染を防ぐための事前対策**」を実習で確認します。



2.1 攻撃&被害体験

従業員 PC で、「**標的型メールによる遠隔操作型マルウェアへの感染**」を体験します。

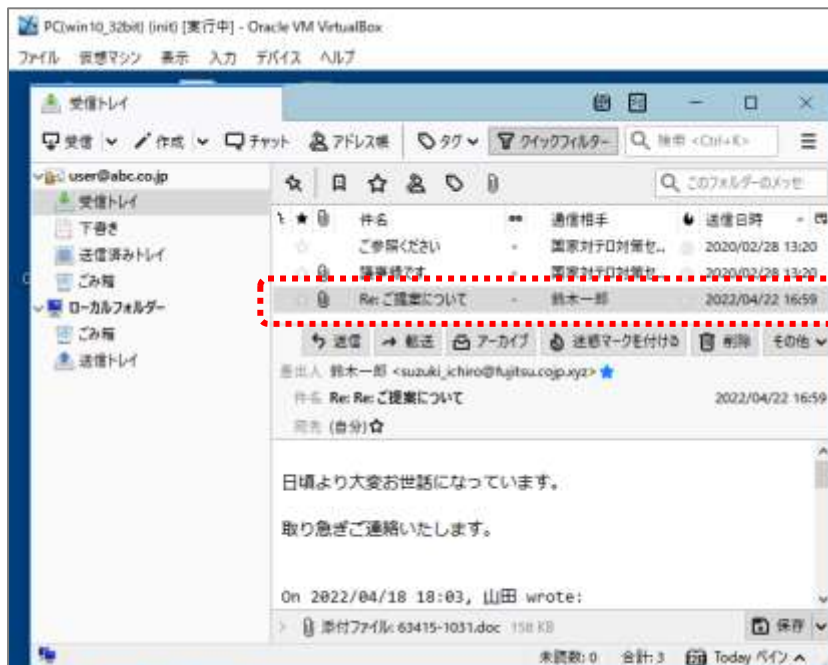
その後、攻撃者サーバーで「**攻撃者による遠隔操作**」を体験し、「**従業員 PC を Emotet に感染**」させます。



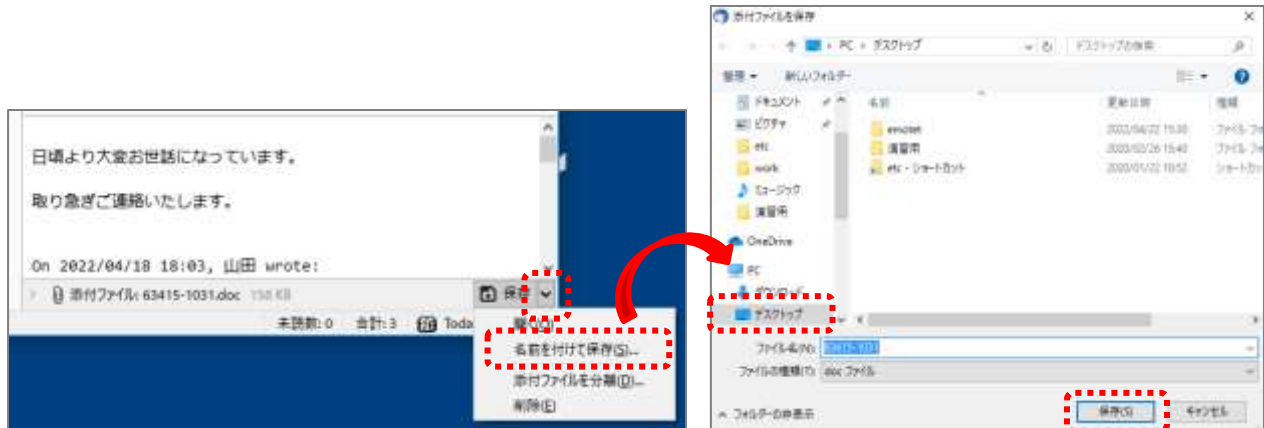
① 標的型メールによる遠隔操作型マルウェアへの感染 [PC(win10_32bit)]

従業員 PC で標的型メールを確認し、添付ファイルのマクロを有効化することで、遠隔操作型マルウェアに感染することを体験します。

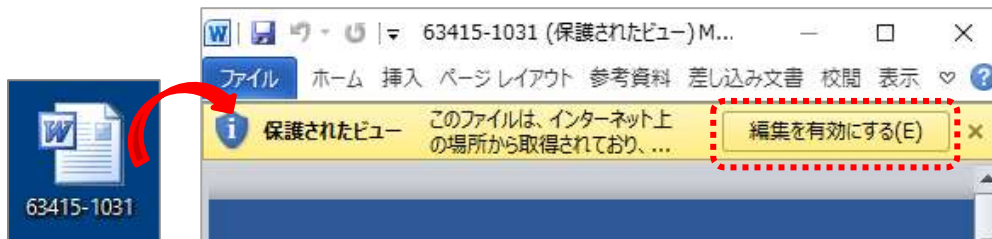
メールソフト（Thunderbird）で、「**鈴木一郎**」さんから届いているメール「**Re: ご提案について**」を選択します。



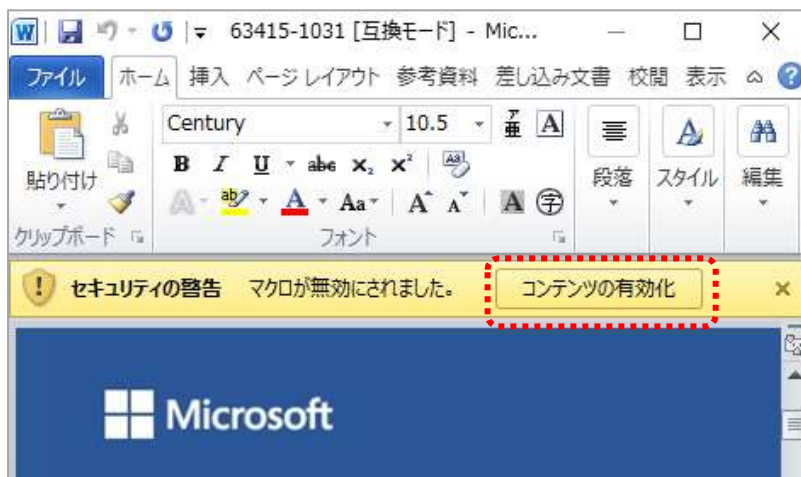
画面右下の「v」-「名前を付けて保存」をクリックし、表示された画面で「デスクトップ」を選択して「保存」をクリックします。



保存した文書「63415-1031」をダブルクリックして開き、「編集を有効にする」をクリックします。



続いて、「コンテンツの有効化」をクリックして、マクロを有効化します。



マクロを有効化したことで、遠隔操作型マルウェアに感染し、攻撃者から遠隔操作可能な状態になってしまいました。しかし、従業員 PC の見た目には、特に変化がないことを確認します。

② 攻撃者の遠隔操作による Emotet への感染 [Attacker(kali)]

攻撃者サーバーで従業員 PC を遠隔操作し、従業員 PC を Emotet に感染させます。

攻撃者サーバーで、「[*] Meterpreter session ○ opened・・・」の「○」の数字を確認します。

```
Attacker(kali) (init) [実行中] - Oracle VM VirtualBox
ファイル 仮想マシン 表示 入力 デバイス ヘルプ

[*] https://92.168.100.10:443 handling request from 192.168.100.250; (UUID: gs6d5lgr) Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 1 opened: (92.168.100.10:443 -> 192.168.100.250:37620) at 2022-04-26 10:31:35 +0900
msf exploit(multi/handler) >
```

「msf exploit(multi/handler) >」に続けて、以下のコマンドを入力し、「Enter」キーを押します。

```
sessions_ -i_ 1
```

※「_」は半角スペースです。

※「1」の部分は先ほど確認した数字です。「1」ではなかった場合は、確認した数字を入力します。

※入力内容は、攻撃者サーバーのデスクトップに保存されているメモ（memo）に記載されています。

メモからコピー＆ペーストして入力することもできます。

```
Attacker(kali) (init) [実行中] - Oracle VM VirtualBox
ファイル 仮想マシン 表示 入力 デバイス ヘルプ

msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
```

「meterpreter >」と表示されたら、従業員 PC の遠隔操作が可能な状態です。

本実習では講師の指示に従い、従業員 PC を Emotet に感染させます。

2.2 感染が疑われる場合の対応

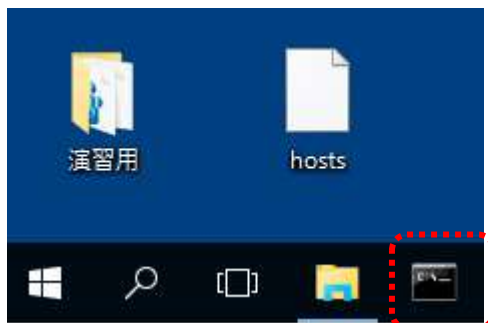
従業員 PC で、マルウェアへの感染が疑われる場合の対応を体験します。



① 感染源の疑いがあるファイルの検査 [PC(win10_32bit)、実習用 PC]

感染源の疑いがあるファイルを特定できている場合は、「VirusTotal」サービスを活用して、ファイルの安全性を確認できます。 <VirusTotal の操作は難易度が高いため、操作が難しい場合は講師のデモを確認してください。>

従業員 PC で、タスクバーから「コマンドプロンプト」をクリックして起動します。

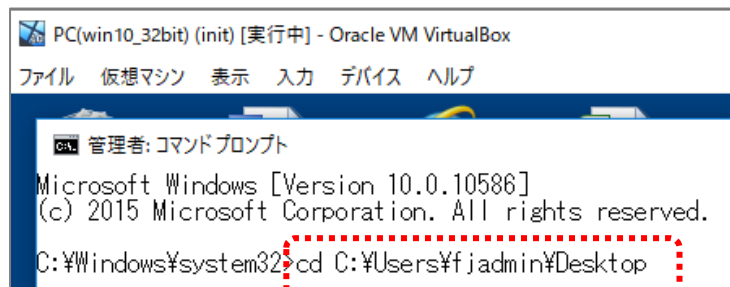


コマンドプロンプトで以下のコマンドを入力し、「**Enter**」キーを押します。(デスクトップトップに移動するコマンド)

```
cd C:\Users\%fjadmin\Desktop
```

※入力内容は、従業員 PC のデスクトップに保存されているメモ (**memo**) に記載されています。

メモからコピー & ペーストして入力することもできます。



続けて以下のコマンドを入力し、「**Enter**」キーを押します。さらに、表示されたハッシュ値を「**コピー**」します。
(メールから保存した文書「63415-1031.doc」のハッシュ値を表示するコマンド)

```
certutil -hashfile 63415-1031.doc sha256
```



```

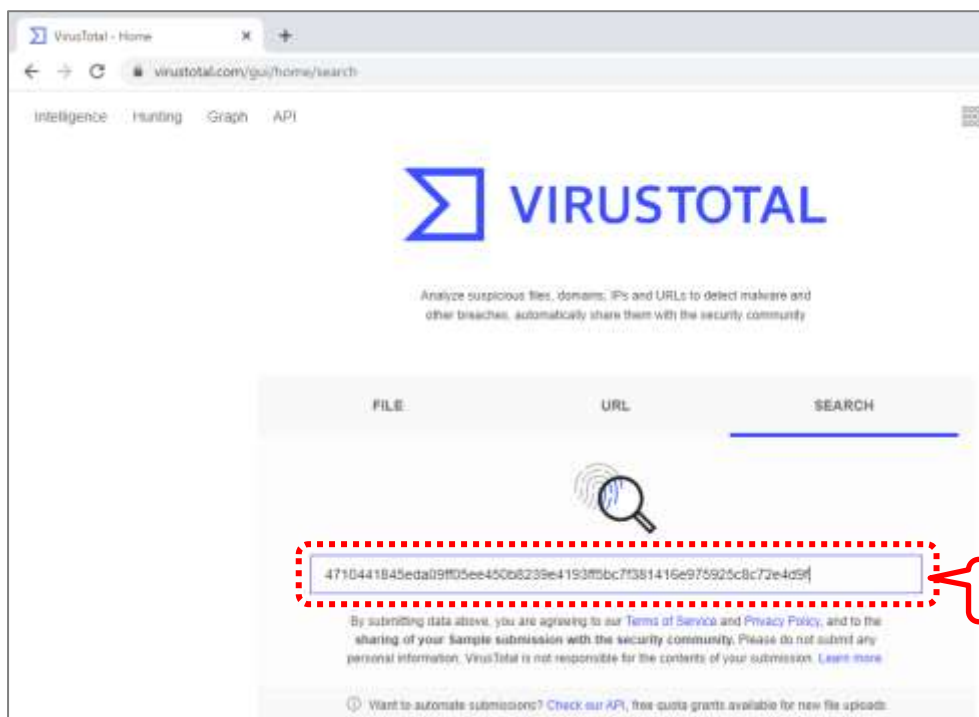
管理: コマンド プロンプト
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\ffjadmin\Desktop
C:\Users\ffjadmin\Desktop>certutil -hashfile 63415-1031.doc sha256
63415-1031.doc (certutil) 63415-1031.doc
4710441845eda09f05ee450b6239e4193f5bc7f381416e975925c8c72e4d9f
CertUtil: -hashfile コマンドは正常に完了しました。
C:\Users\ffjadmin\Desktop>
  
```

以降の VirusTotal の操作は、インターネット接続が可能な「実習用 PC のローカルホスト上」で実施します。

実習用 PC でのデスクトップから、「**VirusTotal**」をダブルクリックして開きます。

先ほどコピーしたハッシュ値を貼り付けて、空白を全て削除し、「**Enter**」キーを押します。

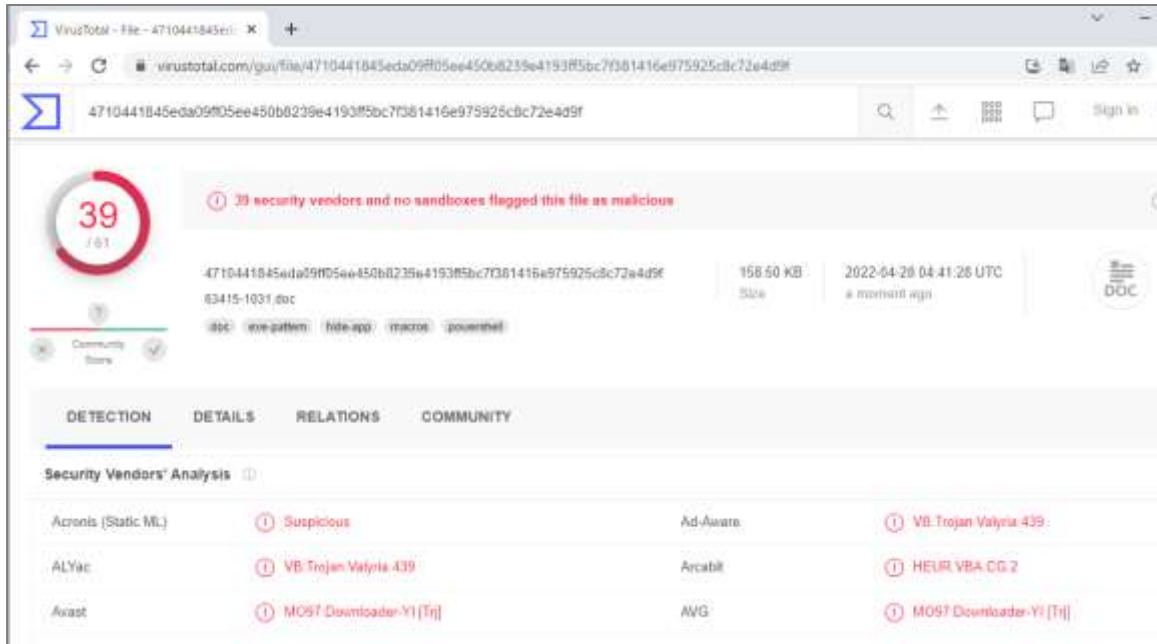


※VirusTotal は、Google 社が提供する「ファイルや Web サイトがマルウェアを含むかどうか」を確認できるサイトです。

※「**FILE**」タブを選択すると、ファイルを直接アップロードして検査することもできます。

しかし、意図せず情報が漏えいする恐れがあるため、推奨されません。

メールから保存した文書「63415-1031.doc」が、悪意のあるファイルであったことが分かります。



The screenshot shows the VirusTotal web interface for a file analysis. The file name is 63415-1031.doc, with a size of 158.50 KB and a date of 2022-04-28 04:41:26 UTC. A red circular badge indicates a score of 39/61. A red banner states: "29 security vendors and no sandboxes flagged this file as malicious". The file is categorized as a doc. The 'DETECTION' tab is active, showing a table of security vendor analyses.

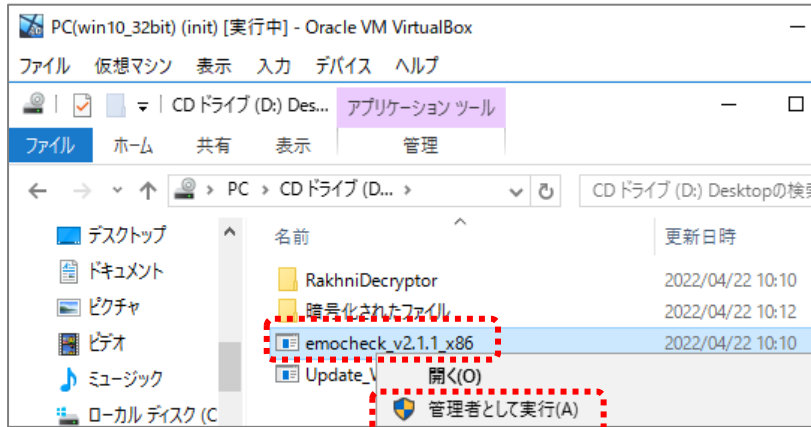
Security Vendors' Analysis			
Acronis (Static ML)	ⓘ Suspicious	Ad-Aware	ⓘ VB-Trojan Vainia.439
ALYac	ⓘ VB-Trojan Vainia.439	Arcabit	ⓘ HEUR VBA.CG.2
Avast	ⓘ MO57 Downloader-YI [Trj]	AVG	ⓘ MO57 Downloader-YI [Trj]

② EmoCheck による感染確認・駆除 [PC(win10_32bit)]

不審なメールを開いてしまった従業員 PC で、EmoCheck を活用して Emotet に感染していないか確認します。

従業員 PC でエクスプローラー（フォルダー）を開き、「PC」の中から「CD ドライブ」を開きます。

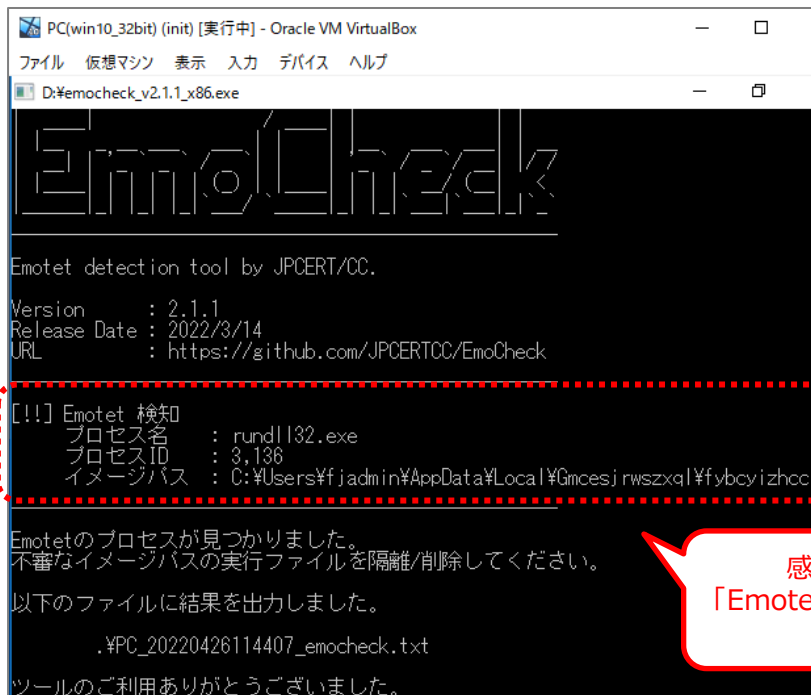
「emocheck_v2.1.1_x86」を右クリックし、「管理者として実行」をクリックします。



※安全が確認されている PC で、インターネットから最新の EmoCheck をダウンロードし、CD 等に焼いて準備します。
本実習では、既に準備されている実行ファイル（emocheck_v2.1.1_x86）を利用します。

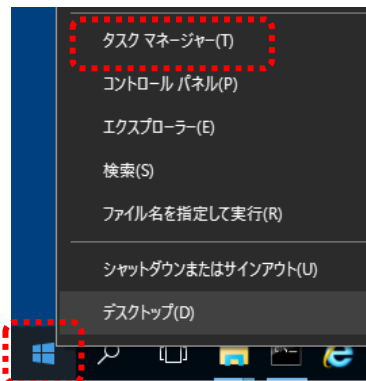
EmoCheck が実行され、「[!!] Emotet 検知」と表示されます。

Emotet のプロセス名、イメージパス（プログラムの格納場所・ファイル名）を確認します。



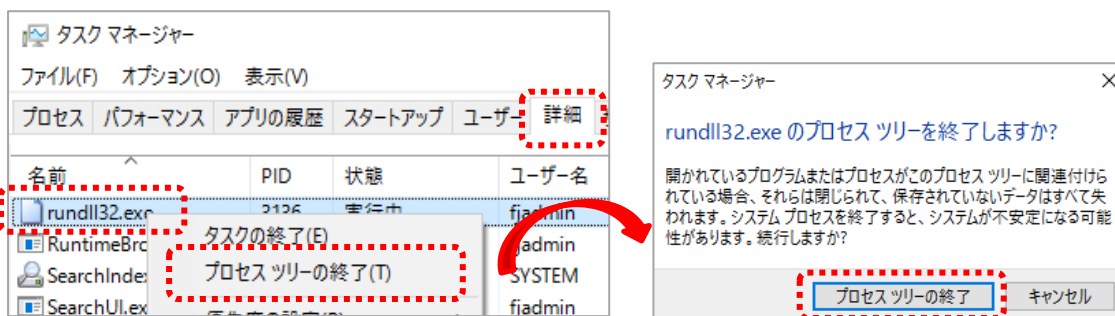
感染していない場合、
「Emotet は検知されませんでした」
と表示されます

Emotet の感染が確認された場合は、Emotet のプロセスを終了させ、プログラムを削除します。
従業員 PC の左下「ウィンドウズマーク」を右クリックして、「タスクマネージャー」をクリックします。



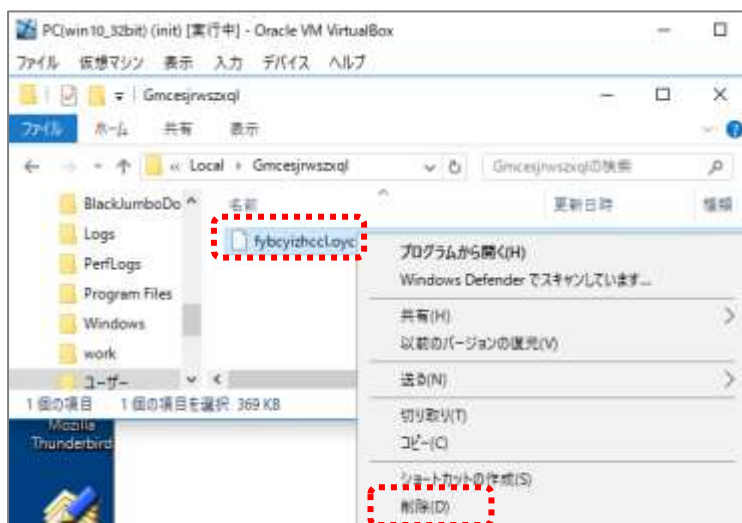
EmoCheck で確認した、Emotet のプロセスを停止します。

タスクマネージャーで「詳細」タブを選択します。該当のプロセスを探して右クリックし、「プロセスツリーの終了」をクリックします。確認画面で、「プロセスツリーの終了」をクリックします。



EmoCheck で確認した、Emotet のプログラムを削除します。

エクスプローラーで該当のパスを開き、ファイルを右クリックして、「削除」をクリックします。



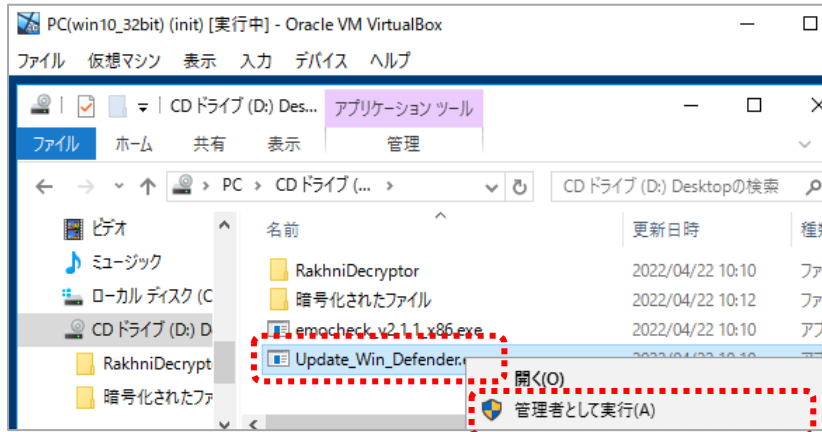
③ ウイルス対策ソフトによる感染確認・駆除 [PC(win10_32bit)]

不審なメールを開いてしまった従業員 PC で、ウイルス対策ソフトの定義ファイル更新・スキャンを実施して、マルウェアに感染していないか確認します。

本実習では、ウイルス対策ソフトとして「**Windows Defender**」を活用して、感染確認・駆除を体験します。

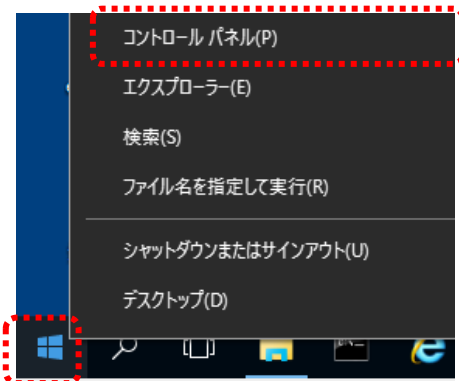
従業員 PC でエクスプローラー（フォルダー）を開き、「PC」の中から「**CD ドライブ**」を開きます。

「**Update_Win_Defender.exe**」を右クリックし、「**管理者として実行**」をクリックします。（何も表示されません）



※安全が確認されている PC で、インターネットから最新の定義ファイルをダウンロードし、CD 等に焼いて準備します。
本実習では、既に準備されている定義ファイルを利用します。

従業員 PC の左下「**ウインドウズマーク**」を右クリックして、「**コントロールパネル**」をクリックします。

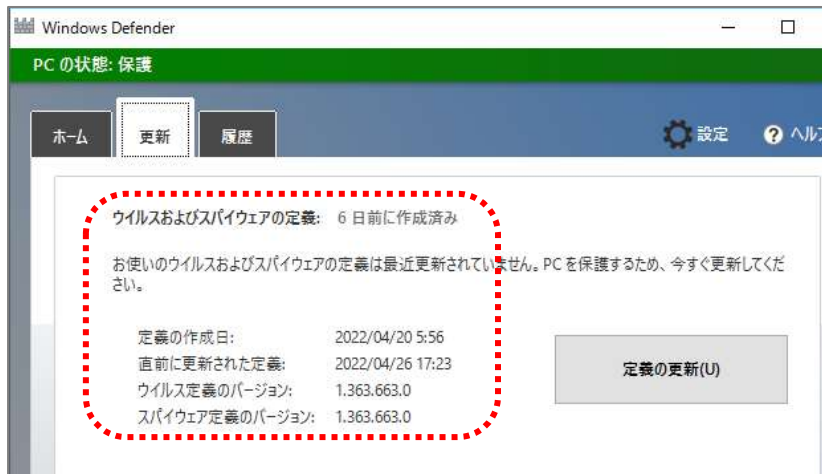


コントロールパネルで、「**Windows Defender**」をクリックして起動します。



定義ファイルの更新日時を確認します。

(「直前に更新された定義」が本日の日付になっていれば、更新に成功しています。)

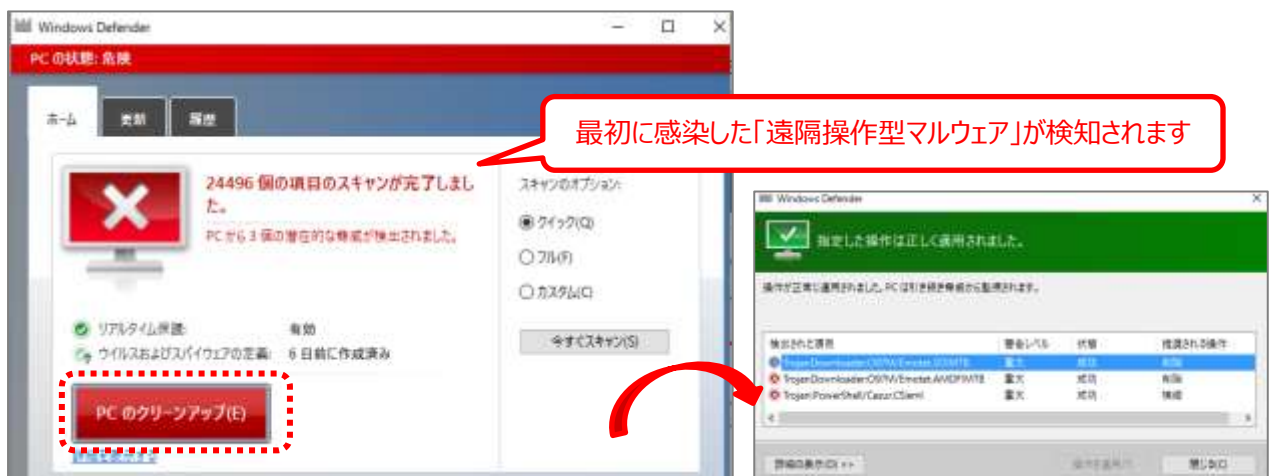


「クイック」を選択して、「今すぐスキャン」をクリックします。

(実習時間短縮のためにクイックスキャンを実施しますが、本来はフルスキャンの方が効果的です。)



悪意のあるファイルが検知された場合は、「PC のクリーンアップ」をクリックして駆除します。



④ 自組織のメールアドレス（ドメイン）が Emotet のメール送信に悪用されていないか（オプション実習） [実習用 PC]

自組織のメールアドレス（ドメイン）が Emotet のメール送信に悪用されていないか確認します。

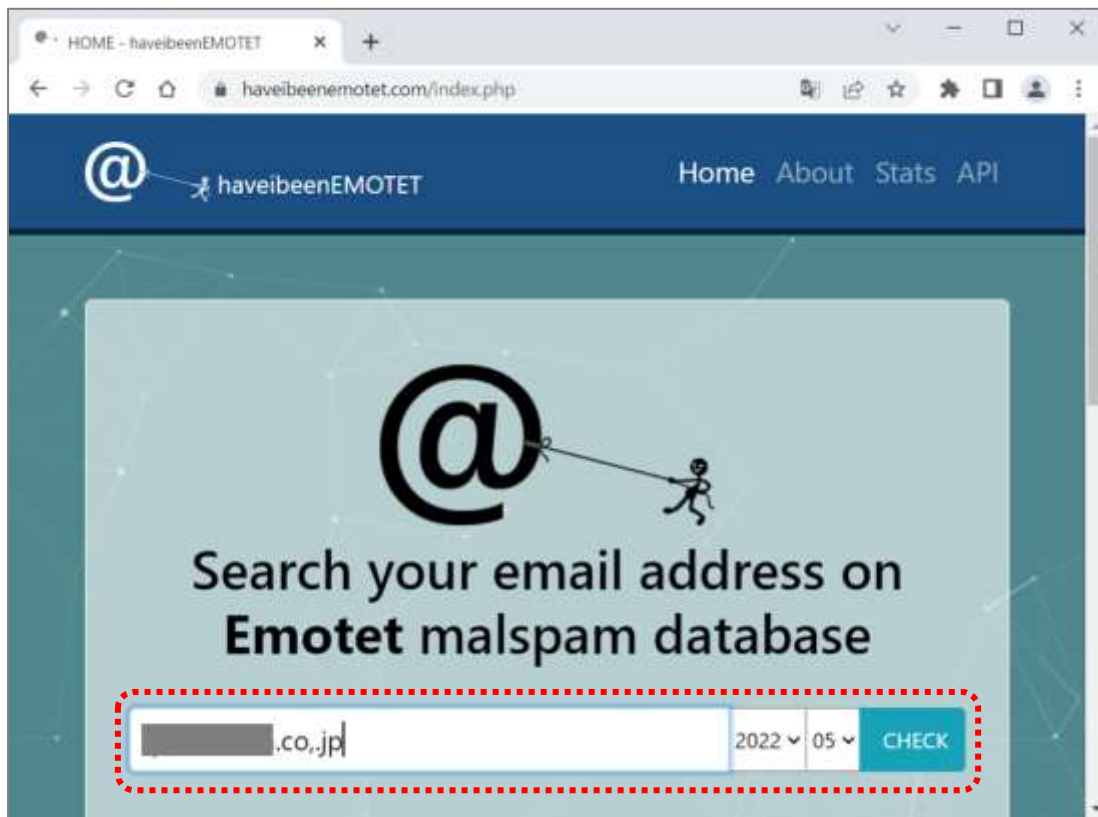
本実習では、「haveibeenEMOTET」で自組織のメールアドレスを確認します。

以降の haveibeenEMOTET の操作は、インターネット接続が可能な「実習用 PC のローカルホスト上」で実施します。

実習用 PC のデスクトップから、「haveibeenEMOTET」をダブルクリックして開きます。

自組織のメールアドレスのドメイン（@以降）を貼り付けて、年・月を選択し、「CHECK」ボタンをクリックします。

※年、月を変更すると確認できる場合もあるため、適宜変更してください。（1 日 20 回まで確認できます。）



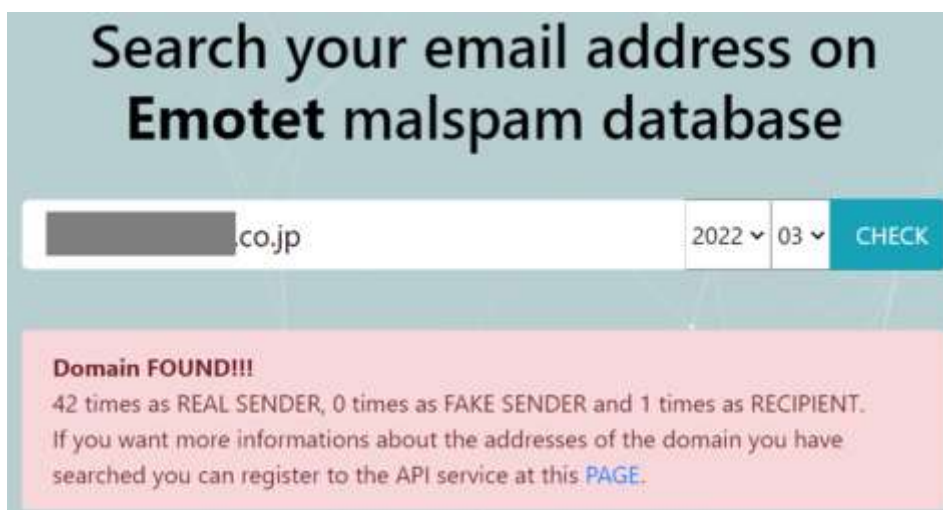
※haveibeenEMOTET は、イタリアのセキュリティ企業「TG Soft」社が提供している Emotet に感染して自組織になりすましたメールが送信されていないかを確認できるサイトです。

Emotet に感染して自組織になりすましたメールが**送信されていない**場合、「**Great! Domain NOT found.**」と表示されます。



The screenshot shows a web interface titled "Search your email address on Emotet malspam database". It features a search bar with a domain ".co.jp" entered, a date selector set to "2022" and "04", and a "CHECK" button. Below the search bar, a green message box displays "Great! Domain NOT found."

Emotet に感染して自組織になりすましたメールが**送信されている**場合、「**Domain found!!!**」と表示されます。社外や関係者に対して、自組織になりすましたメールが届く可能性がある旨を注意喚起することを推奨します。



The screenshot shows the same search interface as above, but with the date selector set to "2022" and "03". Below the search bar, a pink message box displays "Domain FOUND!!!". It also includes statistics: "42 times as REAL SENDER, 0 times as FAKE SENDER and 1 times as RECIPIENT." and a link to "this PAGE" for more information.

※本サイトは簡易的な確認のため、自組織になりすましたメールが送信されていることを「**必ず確認できるものではない**」ことにご注意ください。

2.3 感染を防ぐための事前対策

従業員 PC で、そもそも不審なメールからマルウェアに感染しないために、有効な対策を確認します。



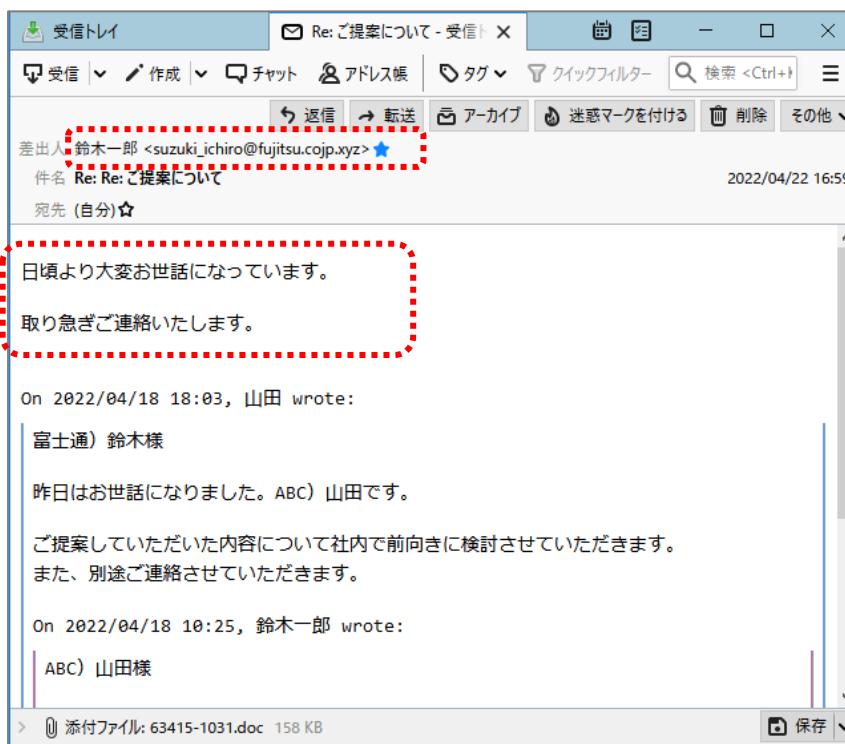
① 不審なメールを見分ける [PC(win10_32bit)]

従業員 PC で感染源となったメールを再度表示し、不審な点がないか確認してみましょう。

少しでも不審な点がある場合は、差出人にメール以外の方法で確認するのが確実です。

<確認観点の例>

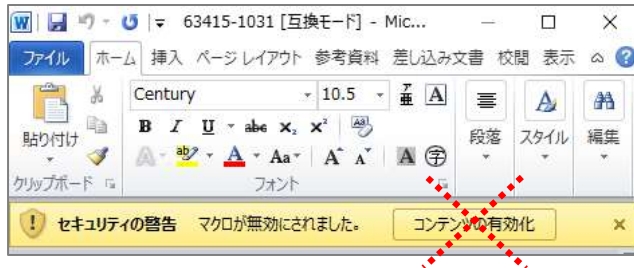
- ✓ メールアドレスは正しいか？（特に@以降のドメイン名が正しいか）
- ✓ メール本文に不審な点がないか、心当たりがあるか 等



<添付ファイルの取り扱い>

今回は添付ファイルのマクロを有効化したことで、攻撃者と不正な通信が開始されてしまいました。

マクロの有効化（「コンテンツの有効化」ボタンをクリック）は、確実に安全なファイルの場合のみ実施してください。



② ウイルス対策ソフトの定義ファイルアップデート・スキャン [PC(win10_32bit)]

ウイルス対策ソフトの**定義ファイル**を**最新の状態**に保ち、**定期的にスキャン**することが有効です。

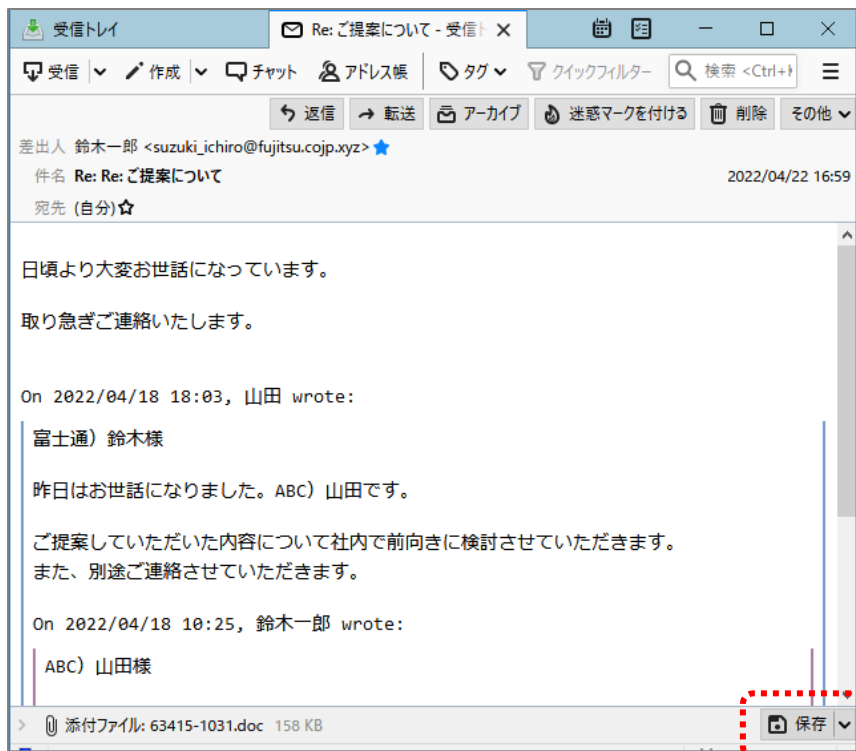
特に、「**リアルタイム保護**」（リアルタイムスキャン）を有効にしておくと、ダウンロードしたファイル等が常時スキャンされ、不正なプログラムを含むファイルが自動で隔離されます。

本実習で使用している「Windows Defender」は、標準で「**リアルタイム保護**」が有効になっています。

ウイルス定義ファイルが更新されている状態で、再度、不審なメールから添付ファイルをダウンロードするとどうなるか、確認してみます。

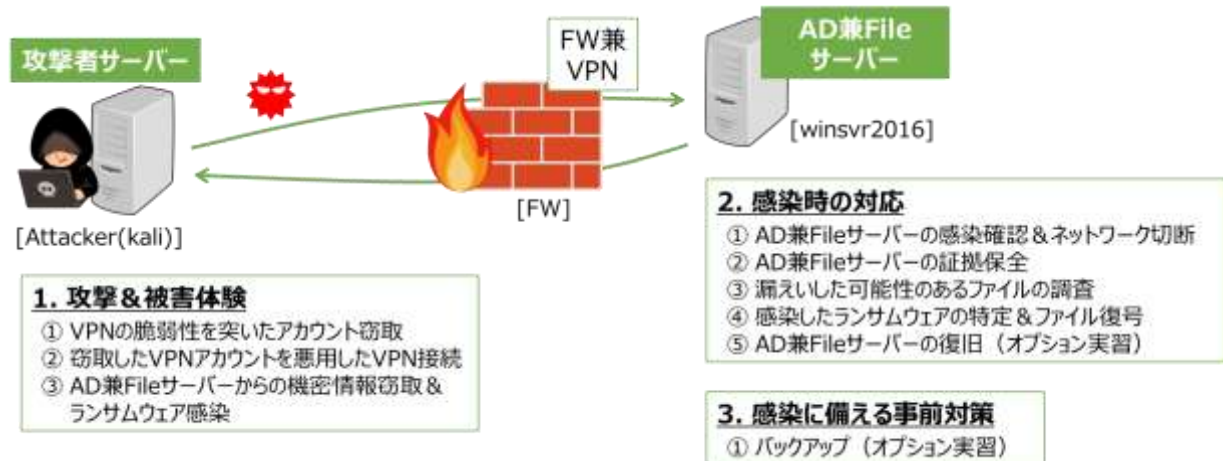


再度、メールソフト（Thunderbird）で「**鈴木一郎**」さんから届いているメール「**Re: ご提案について**」を選択します。添付ファイルを保存し、Windows Defender によって自動で隔離されることを確認します。



3. ランサムウェア感染・対応の体験

ランサムウェアの理解を深めるために、「攻撃&被害体験」、「感染時の対応」、「感染に備える事前対策」を実習で確認します。

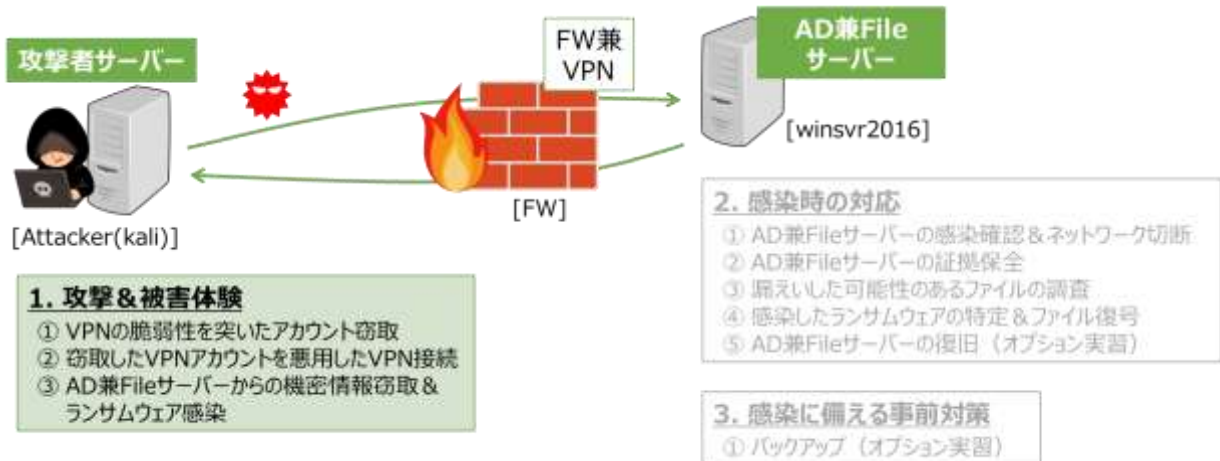


3.1 攻撃&被害体験

攻撃者が VPN の脆弱性を突いてアカウントを窃取します。（講師デモ）

攻撃者サーバーで、窃取した VPN アカウントを悪用した VPN 接続を行います。

VPN 接続（組織内に侵入）できたら、AD 兼 File サーバーから機密情報を窃取し、AD 兼 File サーバーをランサムウェアに感染させます。



① VPN の脆弱性を突いたアカウント窃取

講師がデモを行います。講師の操作画面を確認してください。

② 窃取した VPN アカウントを悪用した VPN 接続 [Attacker(kali)]

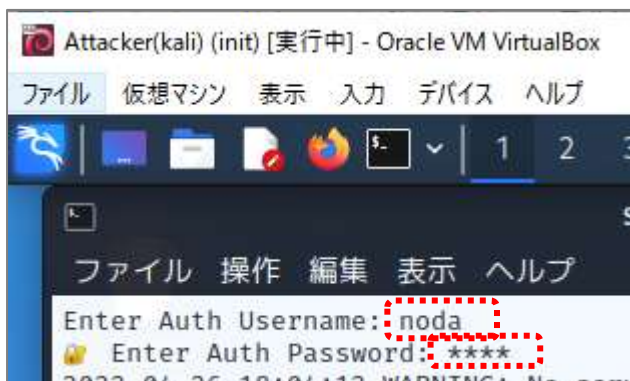
攻撃者サーバーで、窃取した VPN アカウントを悪用して VPN 接続します。

攻撃者サーバーのターミナルで、「root@kali:~#」に続けて以下のコマンドを入力し、「**Enter**」キーを押します。

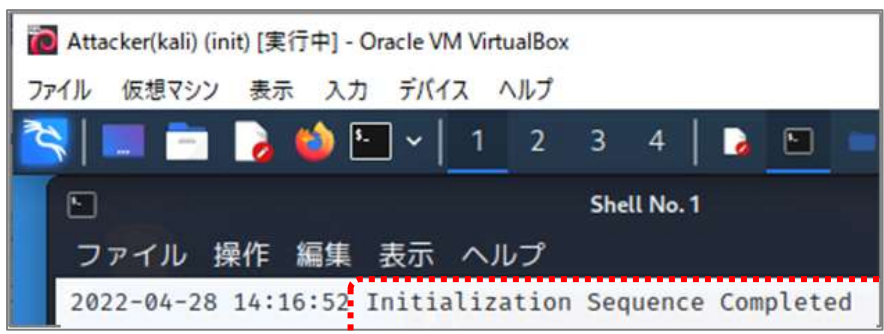
```
./vpn_connect.sh
```



「Username:」に続けて、窃取した VPN アカウントのユーザー名「**noda**」を入力し、「**Enter**」キーを押します。
また、「Password:」に続けて、窃取した VPN アカウントのパスワード「**noda**」を入力し、「**Enter**」キーを押します。



VPN 接続が成功すると、「Initialization Sequence Completed」と表示されます。
(接続状態を保ったまま、おいておきます。)



③ AD 兼 File サーバーからの機密情報窃取&ランサムウェア感染 [Attacker(kali)]

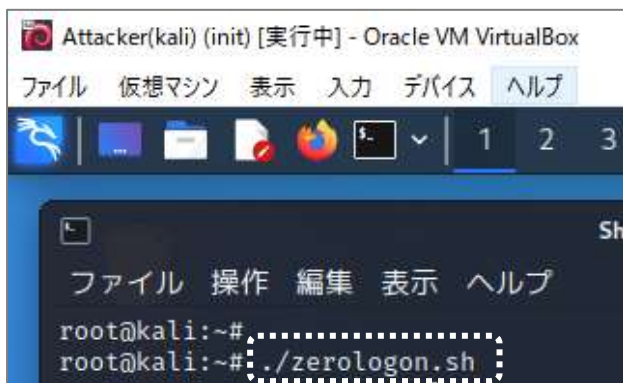
攻撃者サーバーから AD 兼 File サーバーに不正アクセスし、機密情報を窃取した上でランサムウェアに感染させます。

攻撃者サーバーで、新しくターミナルを起動します。



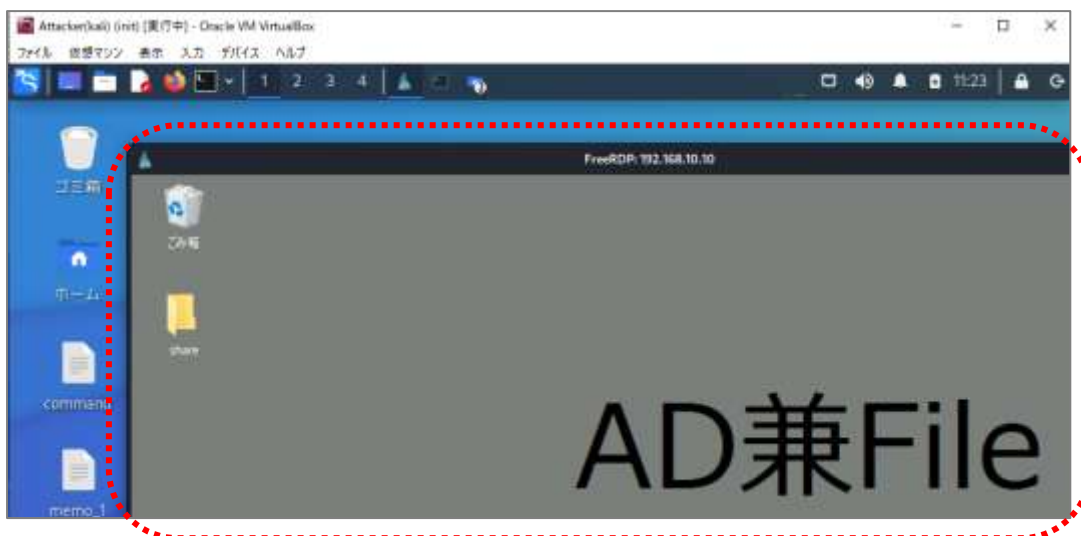
「root@kali:~#」に続けて以下のコマンドを入力し、「Enter」キーを押します。

```
./zerologon.sh
```



※AD の脆弱性を悪用して特権アカウントを窃取し、AD 兼 File サーバーにリモートデスクトップ接続するプログラム。
ファイルを送受信しやすいように、AD 兼 File サーバー上に、攻撃者サーバーのネットワークドライブ「kali の home」も作成。

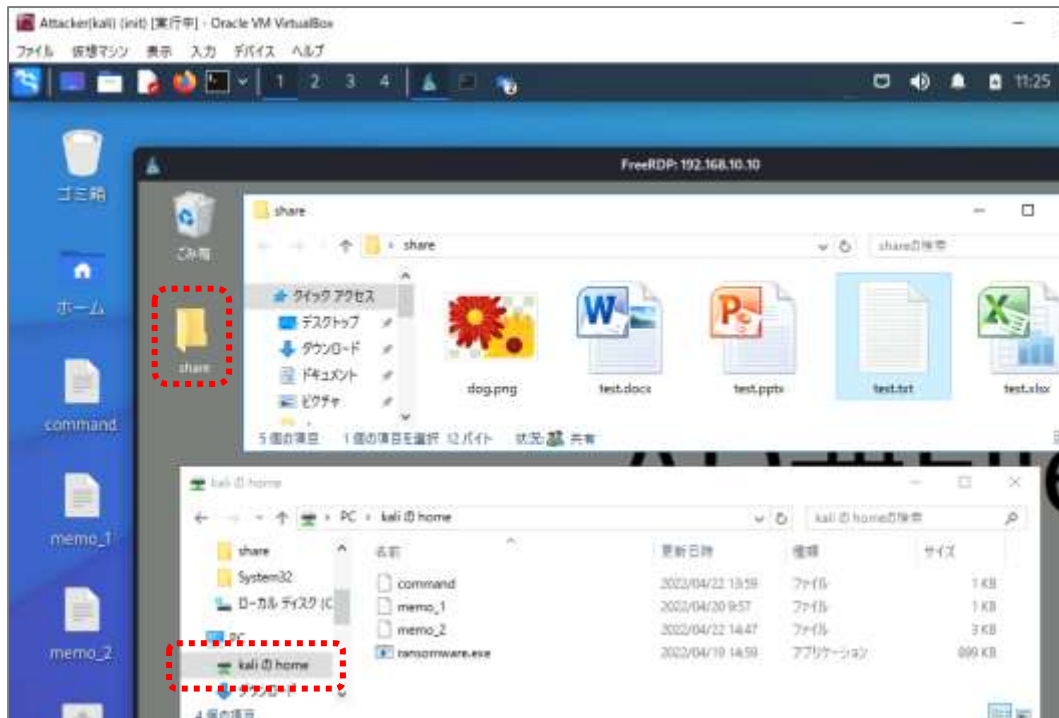
AD 兼 File サーバーへの不正アクセスが成功すると、AD 兼 File サーバーのデスクトップ画面が表示されます。



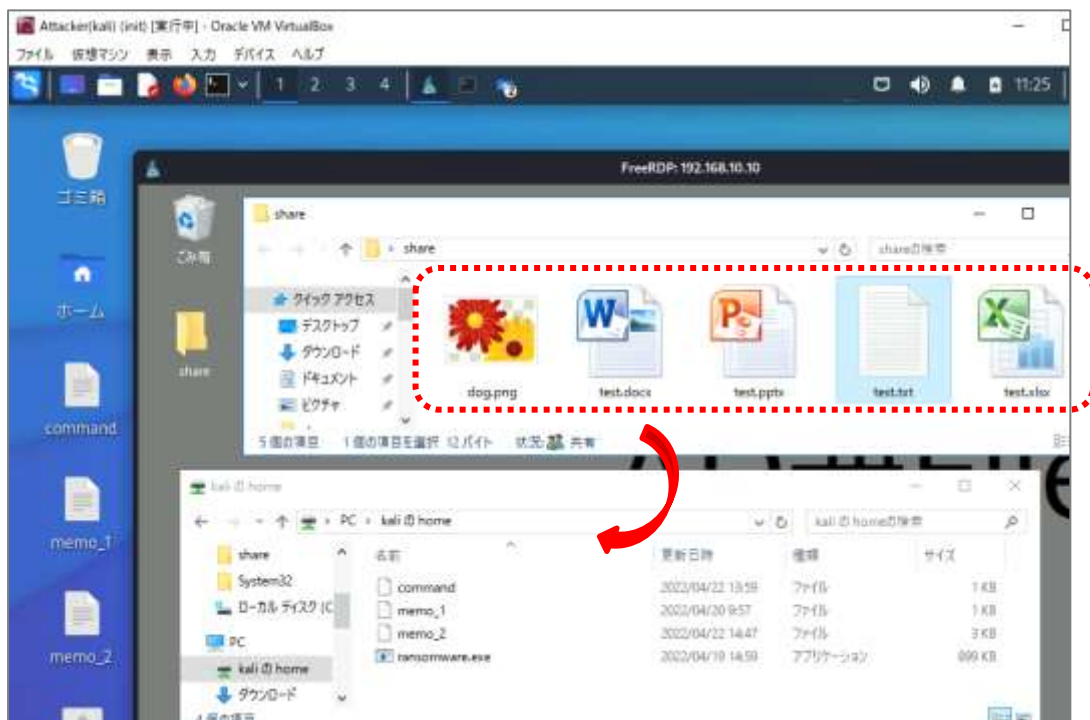
<機密情報の窃取>

AD 兼 File サーバーのタスクバーで「エクスプローラー」(フォルダー) をクリックし、「PC」の中の「kali の home」を開きます。(情報送信先となる攻撃者サーバーのデスクトップフォルダー)

さらに、AD 兼 File サーバーのデスクトップから「share」フォルダーをダブルクリックして開きます。(AD 兼 File サーバーに保存されている機密情報の想定)

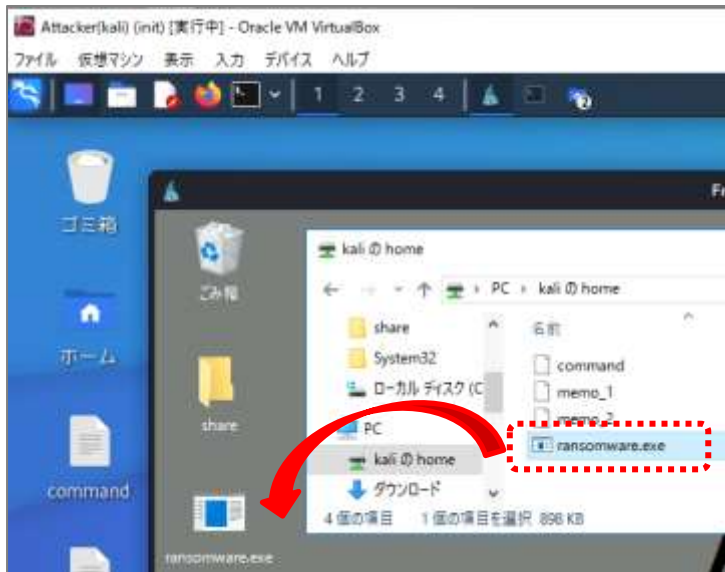


「share」フォルダーから、「kali の home」フォルダーにファイルをコピー & ペーストして、機密情報を窃取します。



<ランサムウェア感染>

「kali の home」フォルダーから、AD 兼 File サーバーのデスクトップに「ransomware.exe」をコピー & ペーストします。



このままランサムウェアに感染させると、「kali の home」フォルダーも被害を受ける可能性があるため、一旦、AD 兼 File サーバーへのリモートデスクトップ接続を終了します。

「FreeRDP」と表示されている右側の青色×ボタンをクリックします。



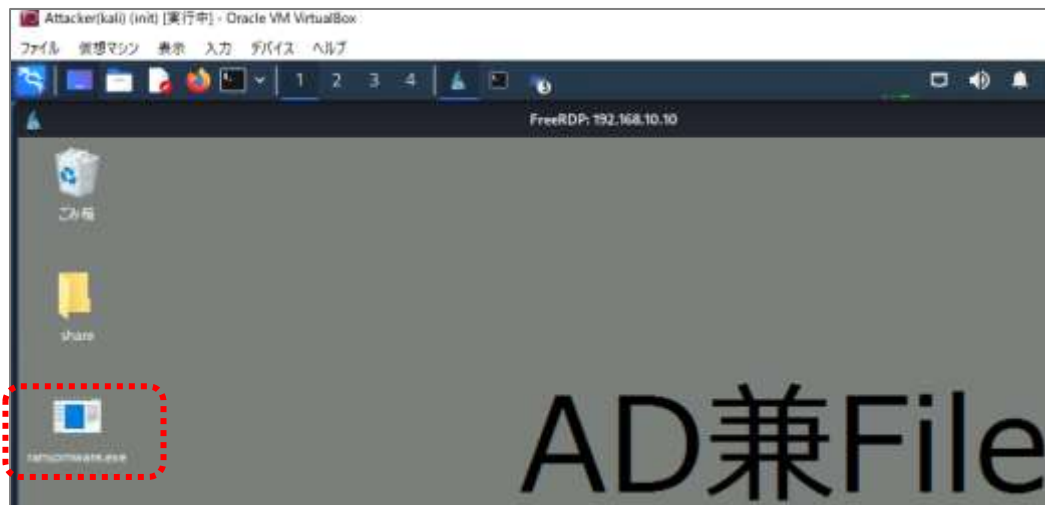
「root@kali:~#」に続けて以下のコマンドを入力し、「Enter」キーを押します。

```
./rdp.sh
```



※AD 兼 File サーバーにリモートデスクトップ接続するプログラム。ネットワークドライブ「kali の home」は作成しない。

AD 兼 File サーバーのデスクトップ上で、「**ransomware.exe**」をダブルクリックして実行します。

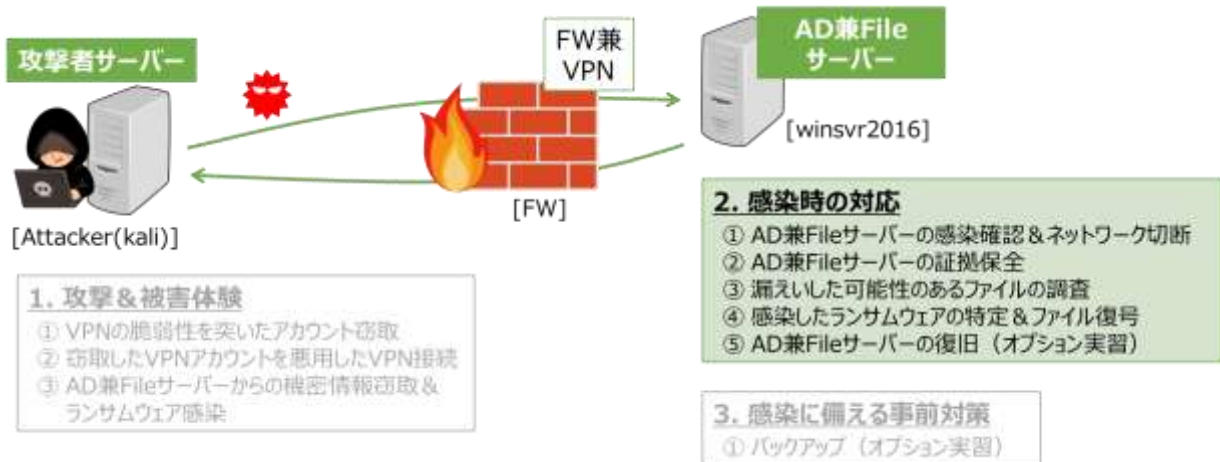


AD 兼 File サーバーがランサムウェアに感染します。
ファイルが暗号化され、デスクトップの壁紙も変更されます。



3.2 感染時の対応

AD 兼 File サーバーの管理者等が、ランサムウェア感染時に行う対応（一部）を体験します。

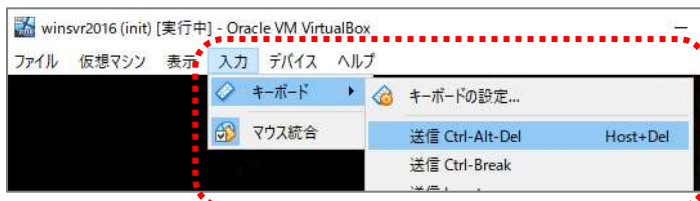


① AD 兼 File サーバーの感染確認 & ネットワーク切断 [winsvr2016]

標的組織では、AD 兼 File サーバーのファイルを参照できない等の事象が発生します。

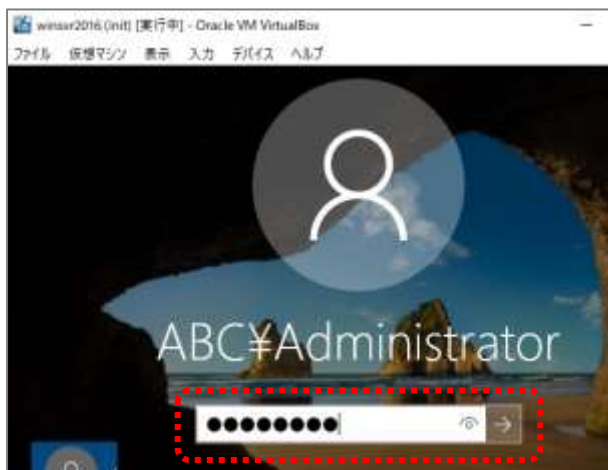
AD 兼 File サーバーにログインして状況を確認し、ネットワークから切断します。

AD 兼 File サーバーで、「入力」-「キーボード」-「送信 Ctrl-Alt-Del」をクリックします。



Administrator のパスワード「P@ssw0rd」を入力し、「Enter」キーを押します。

（大文字ピー、アットマーク、小文字エス、小文字エス、小文字ダブルユー、ゼロ、小文字アール、小文字ディー）

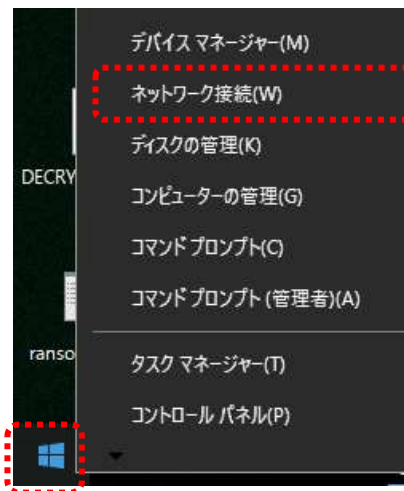


ファイルが暗号化され、デスクトップの壁紙が変更されており、ランサムウェア感染が疑われることを確認します。

感染拡大を防ぐために、AD 兼 File サーバーをネットワークから切断します。

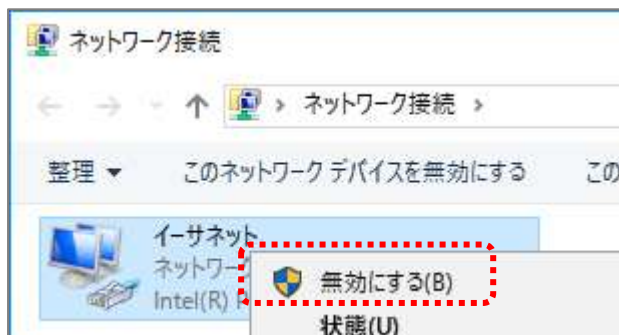
通常は LAN ケーブルを抜染しますが、本実習環境では LAN ケーブルを抜染できないため、ネットワークアダプターを無効化することで、ネットワークから切断します。（無線 LAN に接続している場合、無線 LAN も切断します。）

AD 兼 File サーバーの左下「**ウインドウズマーク**」を右クリックして、「**ネットワーク接続**」をクリックします。

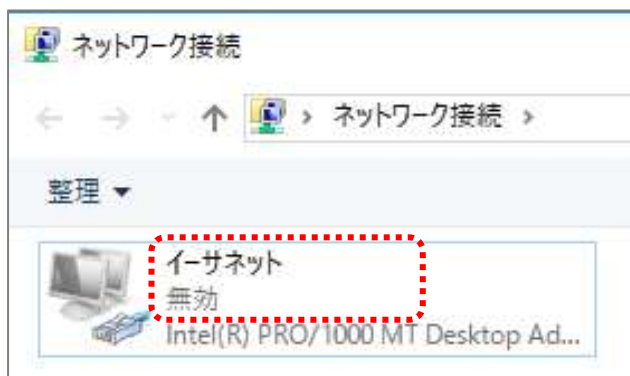


「**イーサネット**」を右クリックして、「**無効にする**」をクリックします。

（ネットワークアダプターが複数ある場合は、すべてのネットワークアダプターを無効にします。）



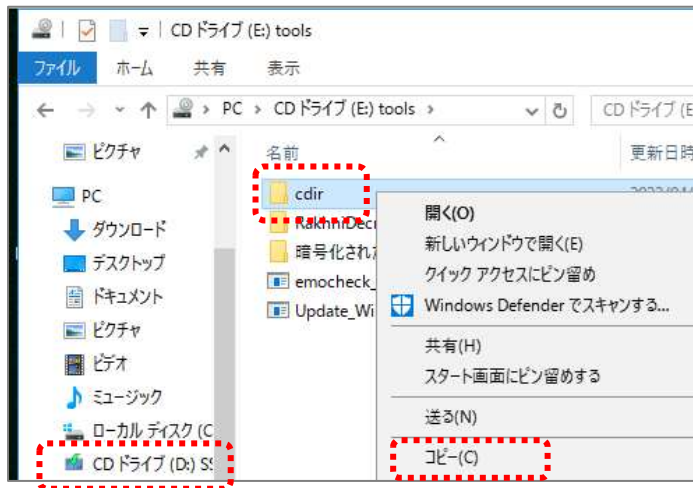
「無効」と表示されたことを確認します。



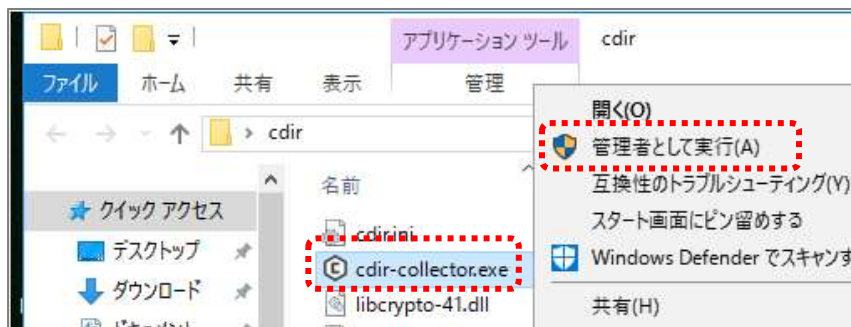
② AD 兼 File サーバーの証拠保全 [winsvr2016]

保全ツールを活用して、AD 兼 File サーバーのメモリ情報やログ等の証拠を保全します。
本実習では、サイバーディフェンス研究所が提供している「CDIR-C」を活用して保全します。
(<https://www.cyberdefense.jp/products/cdir.html>)

AD 兼 File サーバーでエクスプローラー（フォルダー）を開き、「PC」の中から「CD ドライブ」を開きます。
「cdir」フォルダーをコピーして、AD 兼 File サーバーのデスクトップに貼り付けます。



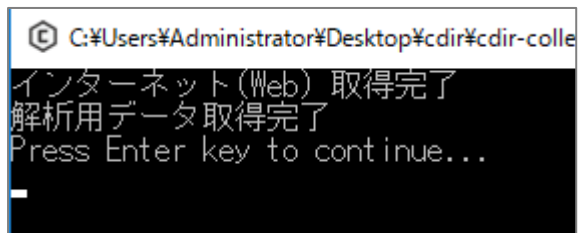
AD 兼 File サーバーのデスクトップで、「cdir」フォルダーをダブルクリックして開きます。
「cdir-collector.exe」を右クリックして、「管理者として実行」をクリックします。



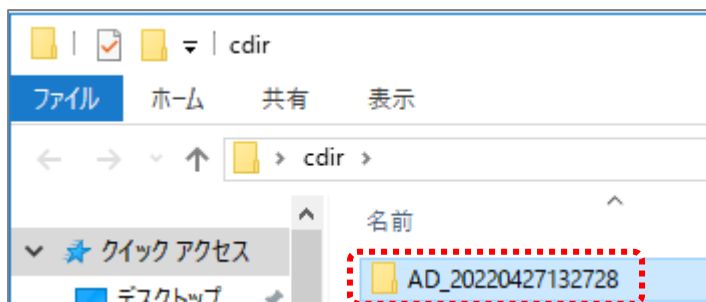
「>」に続けて、「1」と入力し、「Enter」キーを押します。



「Press Enter key to continue...」と表示されたら、「**Enter**」キーを押します。



メモリー情報やログ等の証拠が収集されて、保存されます。



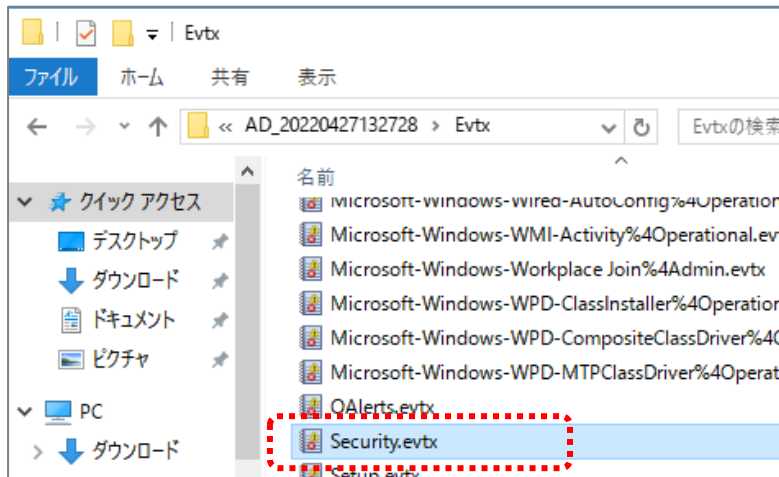
③ 漏えいた可能性のあるファイルの調査 [winsvr2016]

AD 兼 File サーバーで保全したイベントログから、漏えいた可能性のあるファイルを調査します。

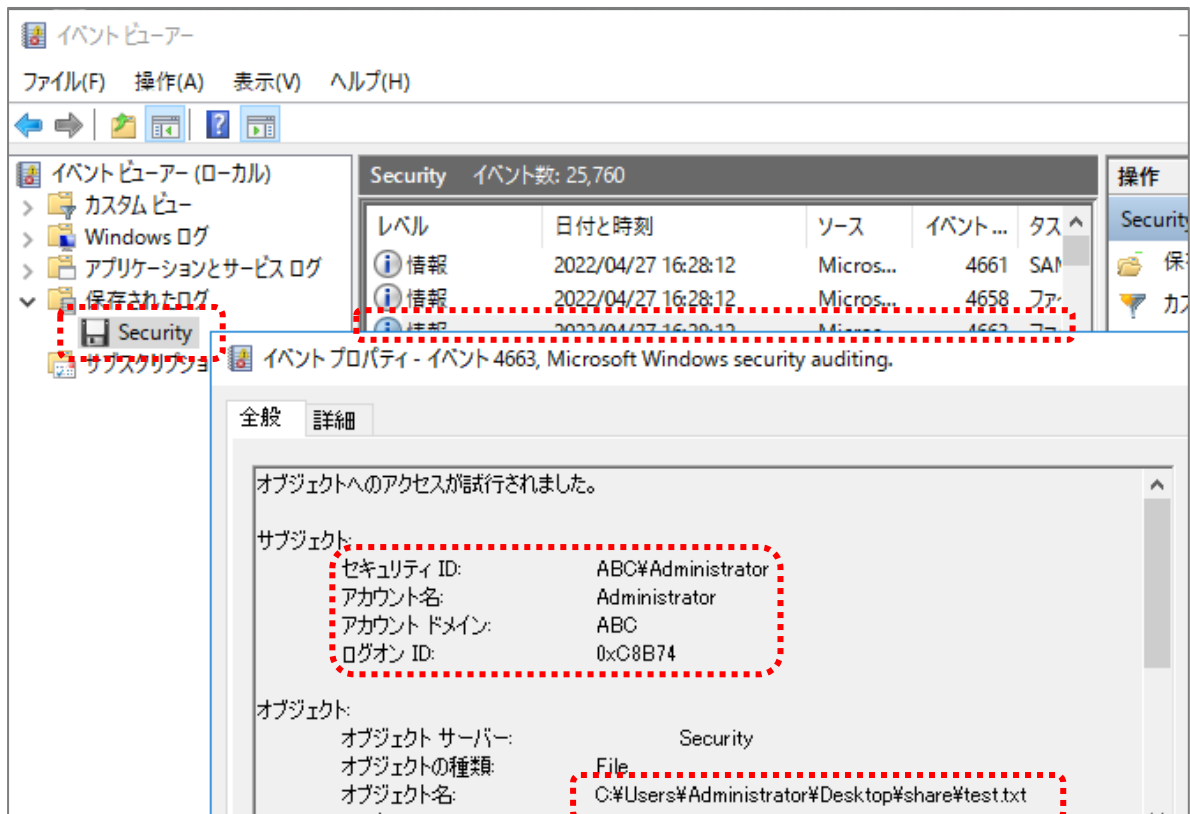
本来は解析用 PC 等を準備して実施しますが、本実習では環境の制約上、AD 兼 File サーバー上で調査します。

AD 兼 File サーバーで、保全したフォルダー「AD_2022XXXX」をダブルクリックして開きます。

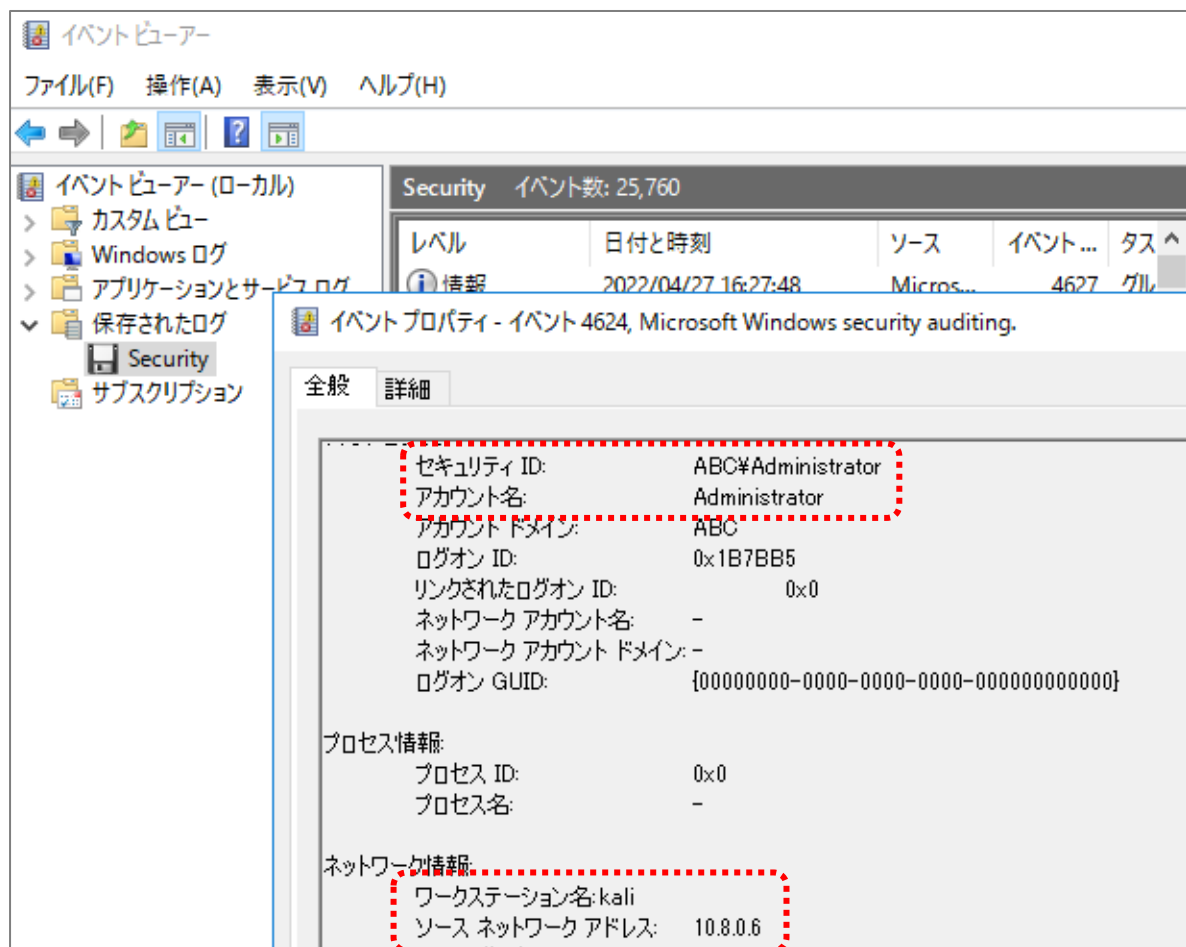
今回は、「Security.evtx」をダブルクリックして開き、Security のイベントログを確認します。



イベント「4663」をダブルクリックして開くと、「test.txt」ファイルに「Administrator」アカウントで接続されていることが分かります。



また、イベント「4624」をダブルクリックして開くと、「kali」という PC（IP アドレス「10.8.0.6」）から、「Administrator」アカウントで接続されていることが分かります。



④ 感染したランサムウェアの特定&ファイル復号 [winsvr2016]

ランサムウェアの種類によっては、復号ツールが無償で公開されている場合があります。

安全が確認されている PC 等から Web ブラウザで「**NO MOER RANSOMWARE**」に接続します。

「暗号化されたファイル」（2 つ）、「身代金要求のメールアドレス等」をアップロードし、復号ツールが公開されている場合は入手します。

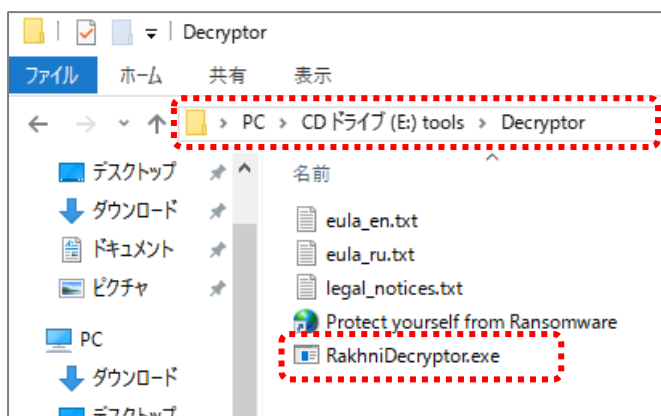


(<https://www.nomoreransom.org/cypto-sheriff.php?lang=ja>)

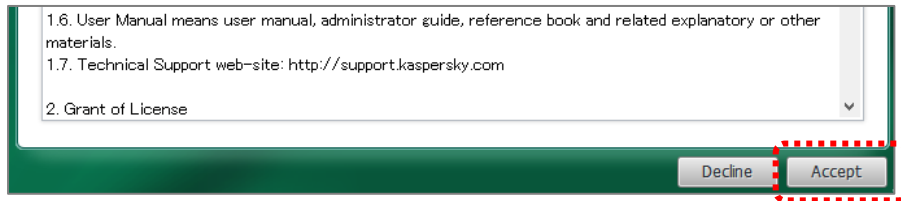
本実習では、あらかじめ入手した復号ツールを用いて、暗号化されたファイルを復号します。

AD 兼 File サーバーでエクスプローラー（フォルダー）を開き、「PC」の中から「CD ドライブ」を開きます。

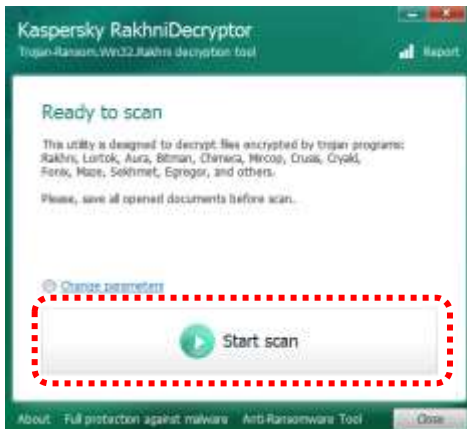
「Decryptor」フォルダーの「RakhniDecryptor.exe」をダブルクリックして実行します。



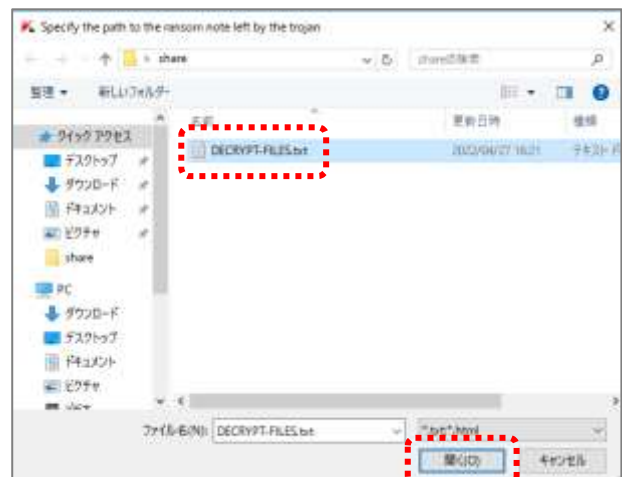
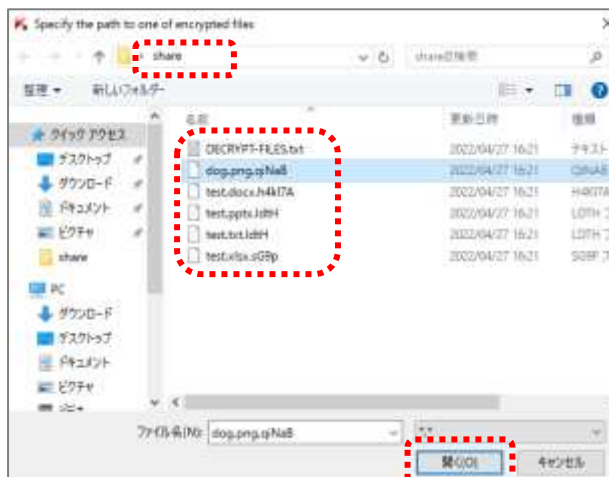
ライセンスが表示されたら、「**Accept**」をクリックします。



「**Start scan**」をクリックして、暗号化されたファイルをスキャンします。

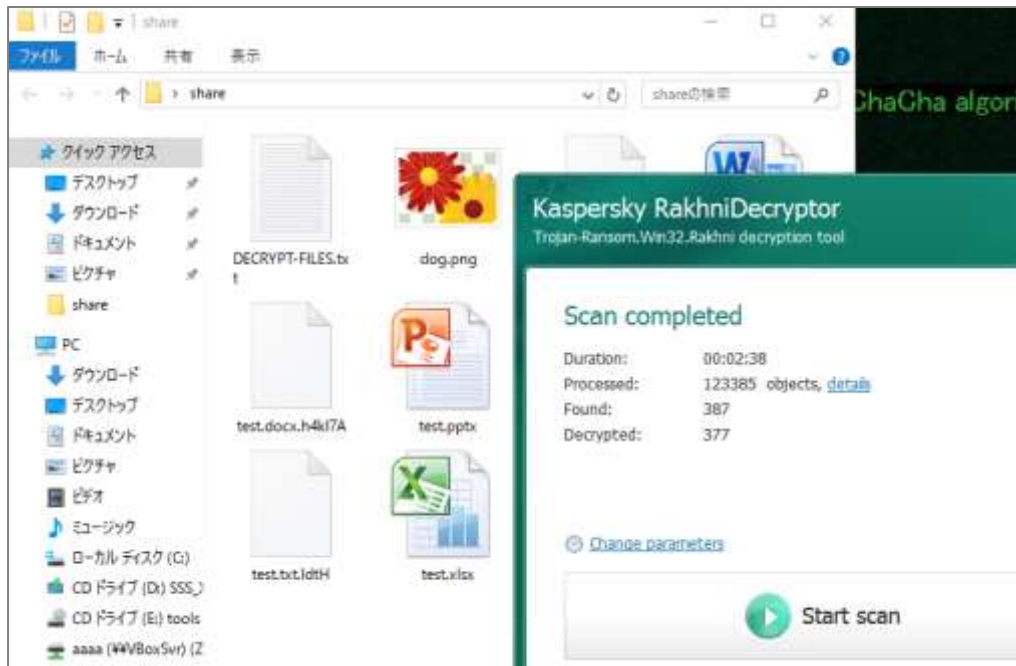


ランサムウェアの種類を特定するために、「**暗号化されたファイル**」（任意のファイル 1 つ）と「**ランサムウェアのメッセージファイル**」を指定します。（本ツールは複数のランサムウェアに対応しているため。）



暗号化されたファイルが復号されます。

復号できたファイルを退避します。



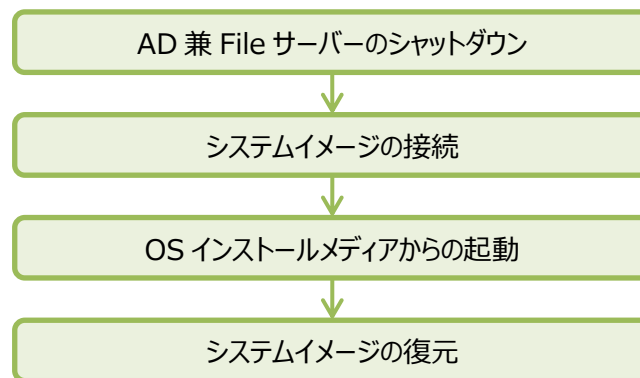
⑤ AD 兼 File サーバーの復旧（オプション実習） [winsvr2016、実習用 PC]

AD 兼 File サーバーに残されたマルウェアやバックドアを完全に排除して、AD 兼 File サーバーを復旧します。

様々な復旧方法がありますが、本実習では「システムイメージを利用した復旧」を体験します。

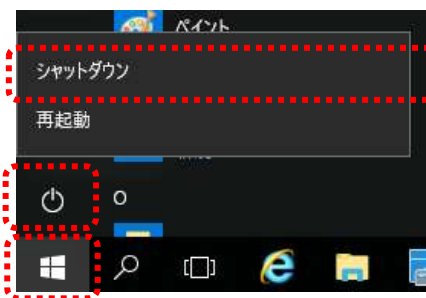
復旧方法の例	説明	復旧時に必要な物の例
OS をクリーンインストールして再構築	一から OS をインストール（クリーンインストール）してサーバーを再構築する	<ul style="list-style-type: none"> • OS インストールメディア • ソフトウェアのインストールメディア • 構築手順書 等
システムイメージを利用 【実習】	あらかじめ取得したシステムイメージ（マルウェア感染前のフルバックアップ）を利用して復旧する	<ul style="list-style-type: none"> • システムイメージ • OS インストールメディア

本実習では、次の順番で AD 兼 File サーバーを復旧します。

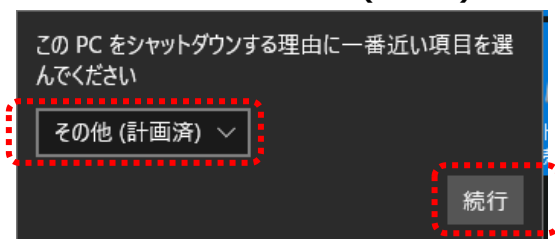


<AD 兼 File サーバーのシャットダウン> [winsvr2016]

AD 兼 File サーバーの左下「ウィンドウズマーク」-「電源」ボタンをクリックして、「シャットダウン」をクリックします。



シャットダウン理由として「その他(計画済)」を選択し、「続行」をクリックします。

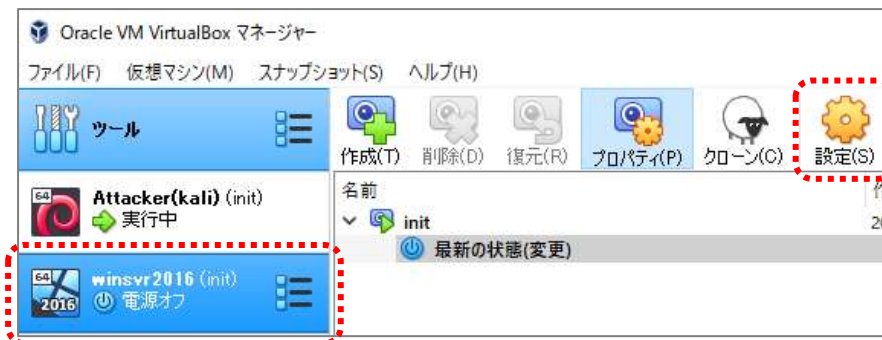


＜システムイメージの接続＞ [実習用 PC]

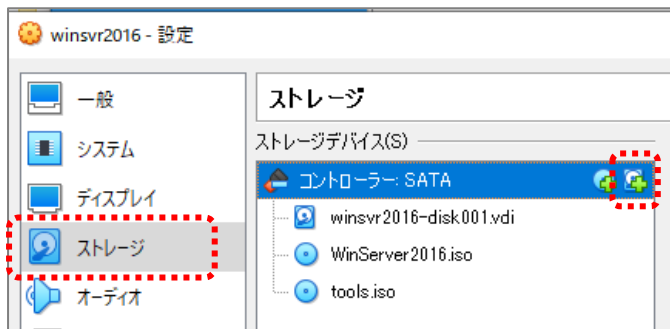
通常は、システムイメージ（フルバックアップデータ）を格納した外付けハードディスクや、バックアップテープをサーバーに接続します。

本実習では、AD 兼 File サーバー（「winsvr2016」という名前の仮想サーバー）に、疑似的にシステムイメージが保存されたディスク「Backup.Disk1.vdi」を接続します。

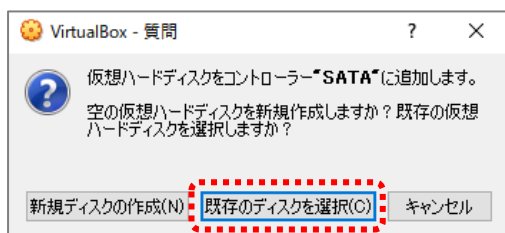
実習用 PC で「Oracle VM VirtualBox マネージャー」を開き、「winsvr2016」を選択して、「設定」ボタンをクリックします。



「ストレージ」を選択し、「コントローラー:SATA」と表示されている部分の、一番右側の「+」ボタンをクリックします。



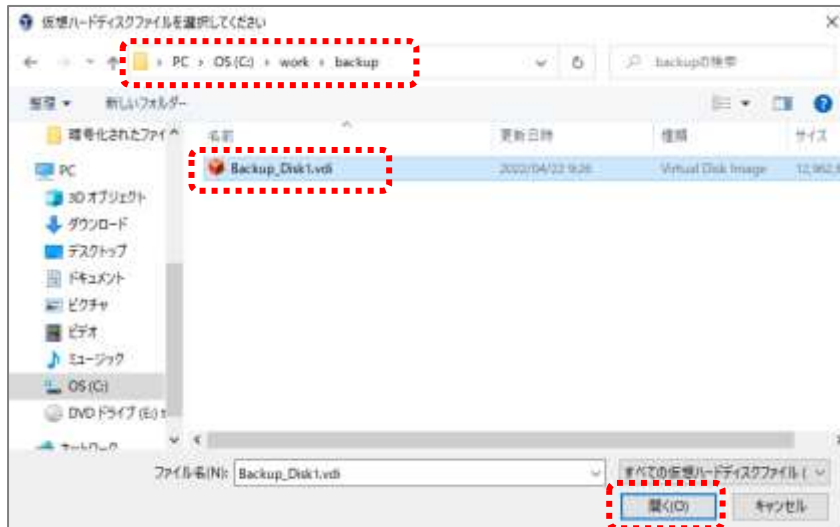
確認画面で、「既存のディスクを選択」をクリックします。



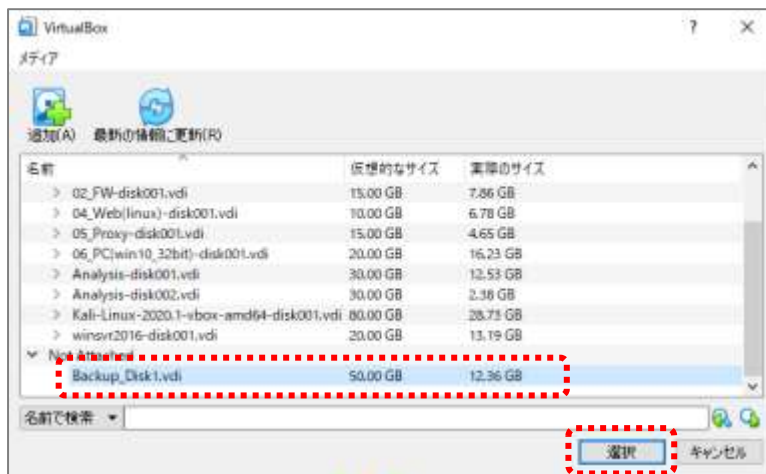
「追加」をクリックします。



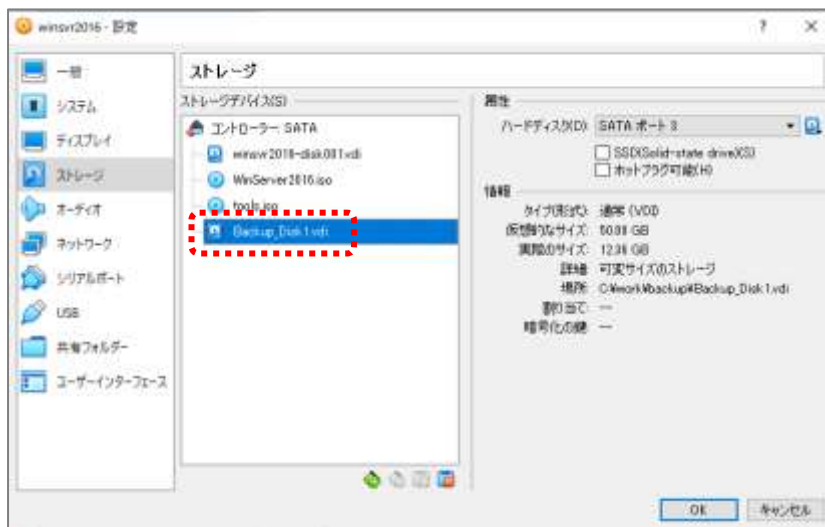
「PC」-「OS(C)」-「work」-「backup」フォルダーの「**Backup.Disk1.vdi**」を選択し、「開く」をクリックします。



「**Backup.Disk1.vdi**」を選択し、「**選択**」をクリックします。



ストレージに「**Backup.Disk1.vdi**」が追加されていることを確認します。（画面はそのままにしておきます。）

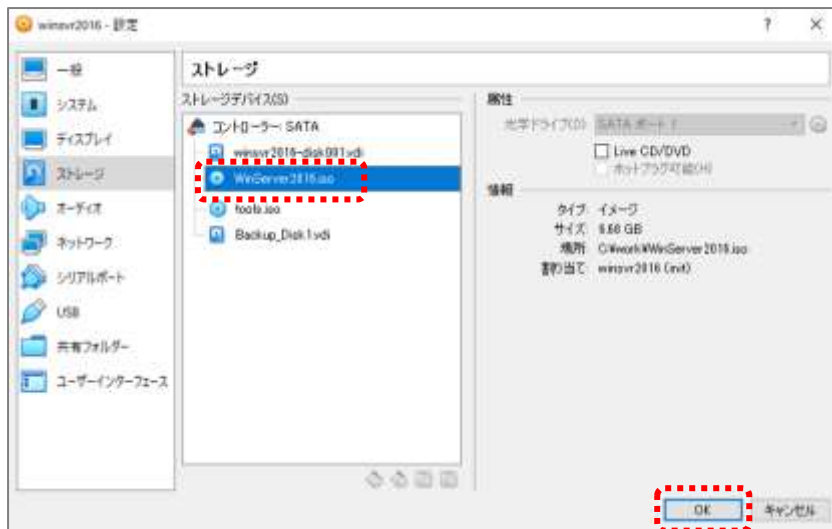


<OS インストールメディアからの起動> [実習用 PC、winsvr2016]

通常は、OS インストールメディアを CD ドライブ等にセットします。

本実習では、AD 兼 File サーバー（「winsvr2016」という名前の仮想サーバー）の CD ドライブに、あらかじめセットされている OS インストールメディア「WinSwerver2016.iso」を利用します。

ストレージに「WinSwerver2016.iso」が表示されていることを確認し、「OK」ボタンをクリックします。

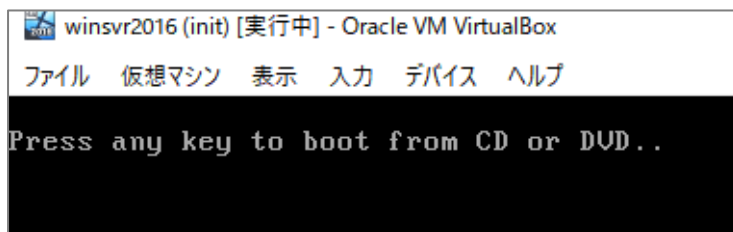


AD 兼 File サーバーを、OS インストールメディアを使って起動します。

「winsvr2016」が選択されていることを確認し、「起動」をクリックします。



「Press any Key...」と表示されたら、すぐに「Enter」キーを押します。



※成功すると、「Windows セットアップ」画面（次ページ）が表示されます。

失敗して、Windows ログイン画面が表示された場合は、シャットダウンして再度起動してください。

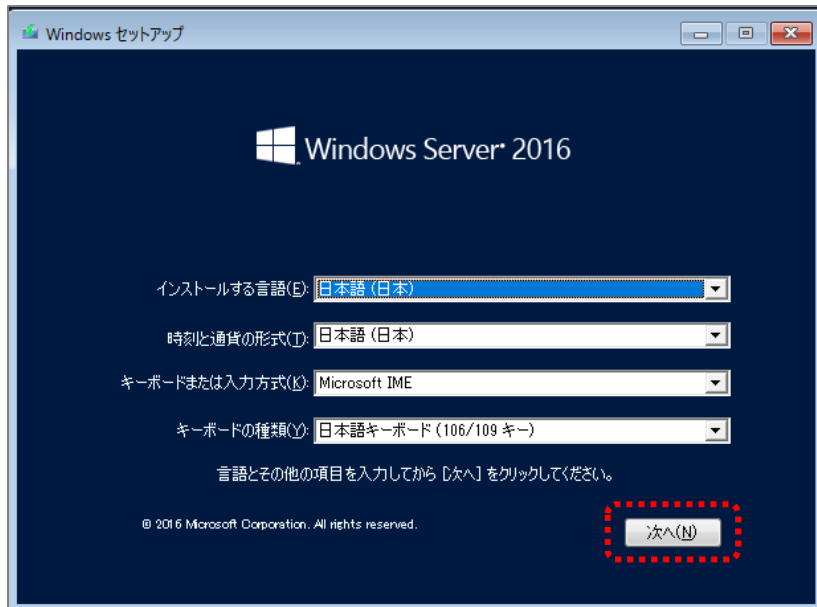
（本実習環境では、CD ドライブから優先的に起動する設定になっています。）

<システムイメージの復元> [winsvr2016]

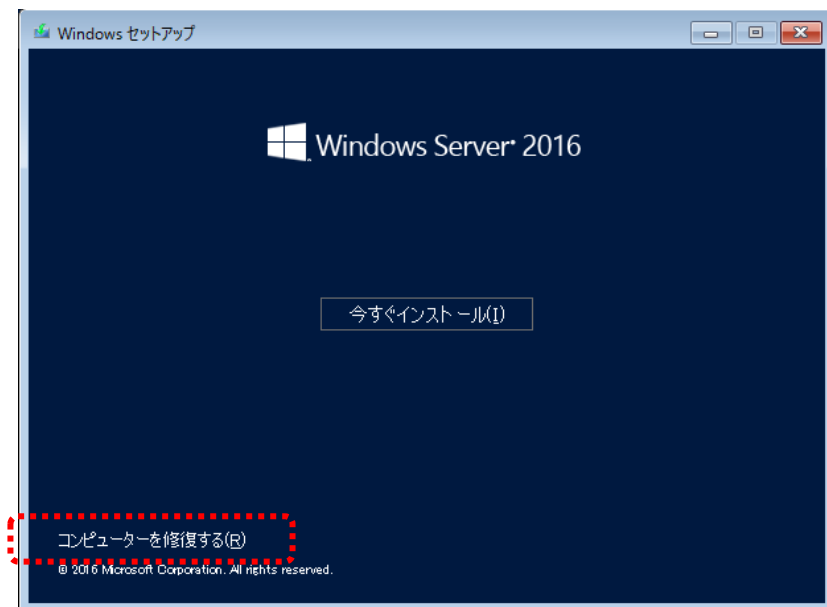
あらかじめ取得しておいたシステムイメージを、AD 兼 File サーバーに復元します。

(システムイメージの取得方法は、「3.3 感染に備える事前対策」を参考にしてください。)

「Windows セットアップ」画面で、「次へ」ボタンをクリックします。



画面左下の「コンピューターを修復する」をクリックします。



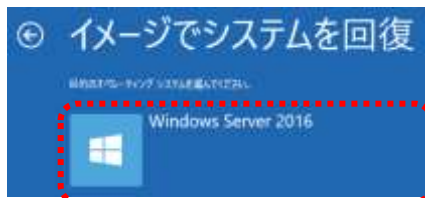
「オプションの選択」画面で、「**トラブルシューティング**」をクリックします。



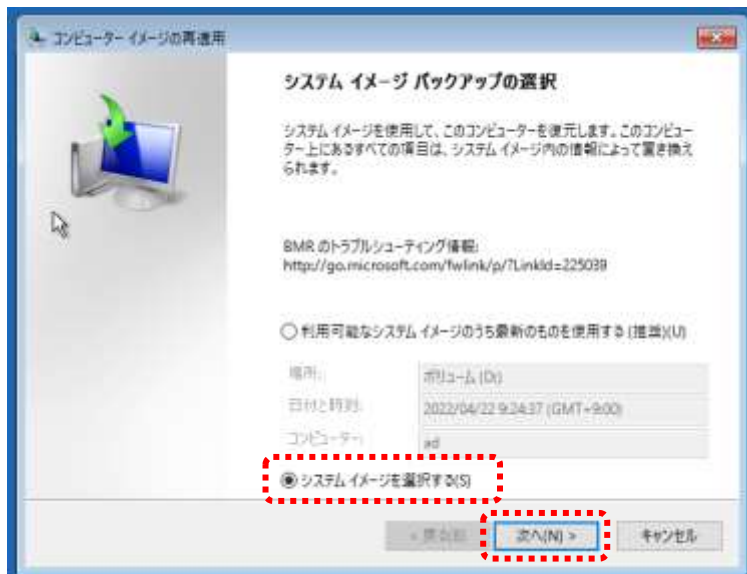
「詳細オプション」で、「**イメージでシステムを回復**」をクリックします。



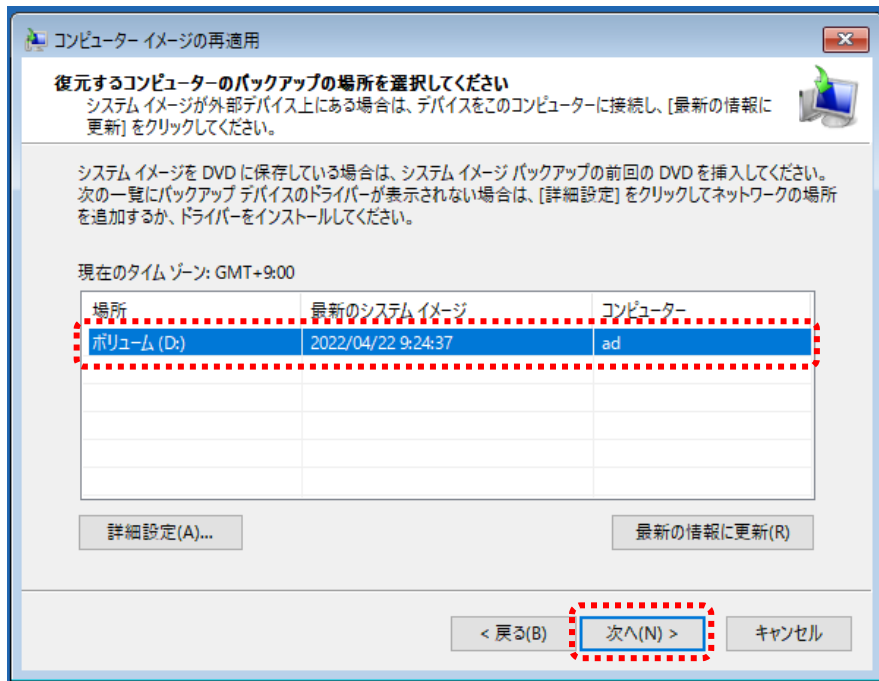
OS 選択画面で、「**Windows Server 2016**」をクリックします。



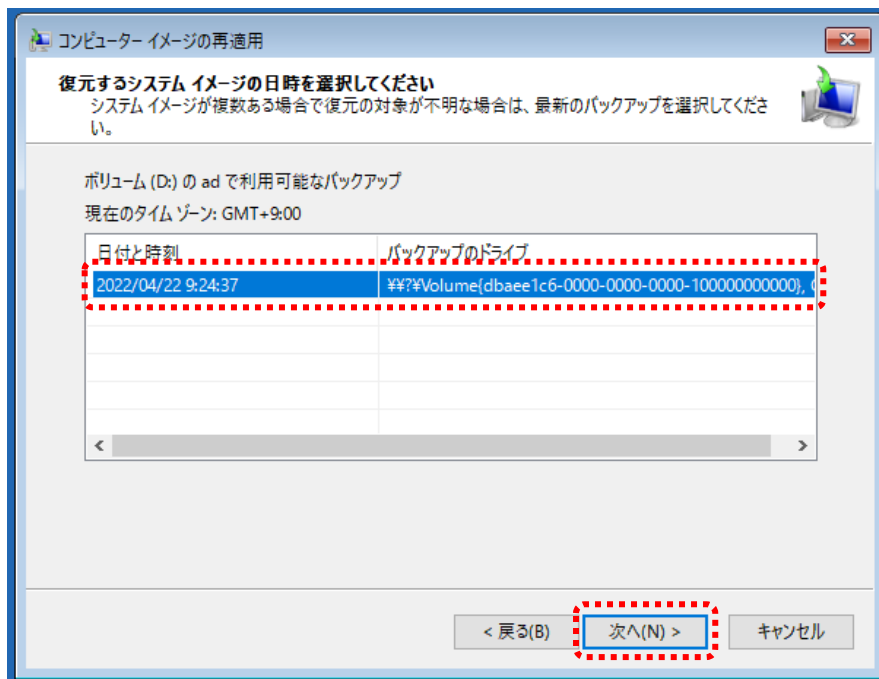
「**システムイメージを選択する**」を選択して、「**次へ**」ボタンをクリックします。



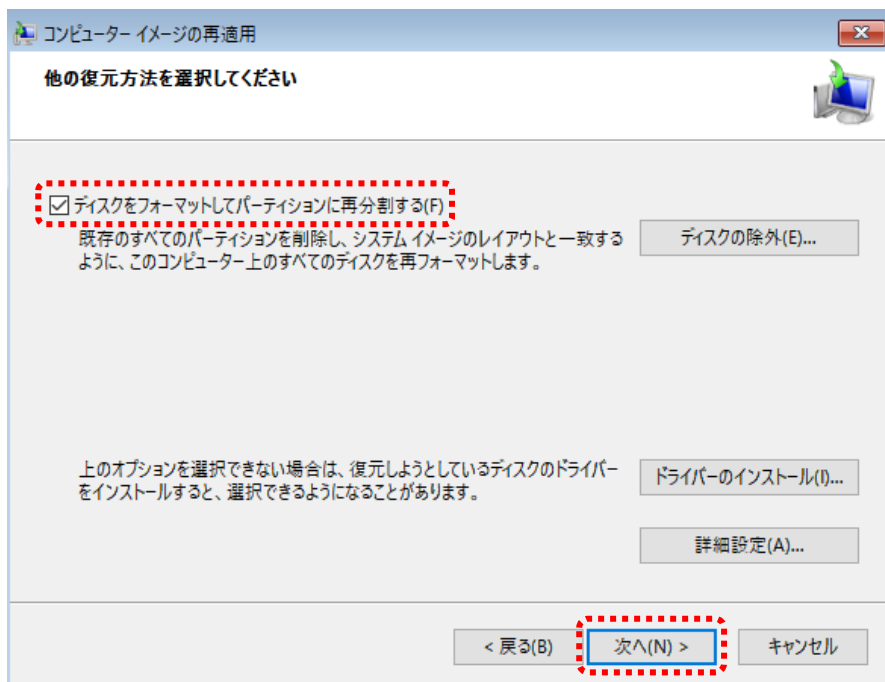
「**ボリューム(D:)**」(システムイメージが保存されている領域)を選択し、「**次へ**」ボタンをクリックします。



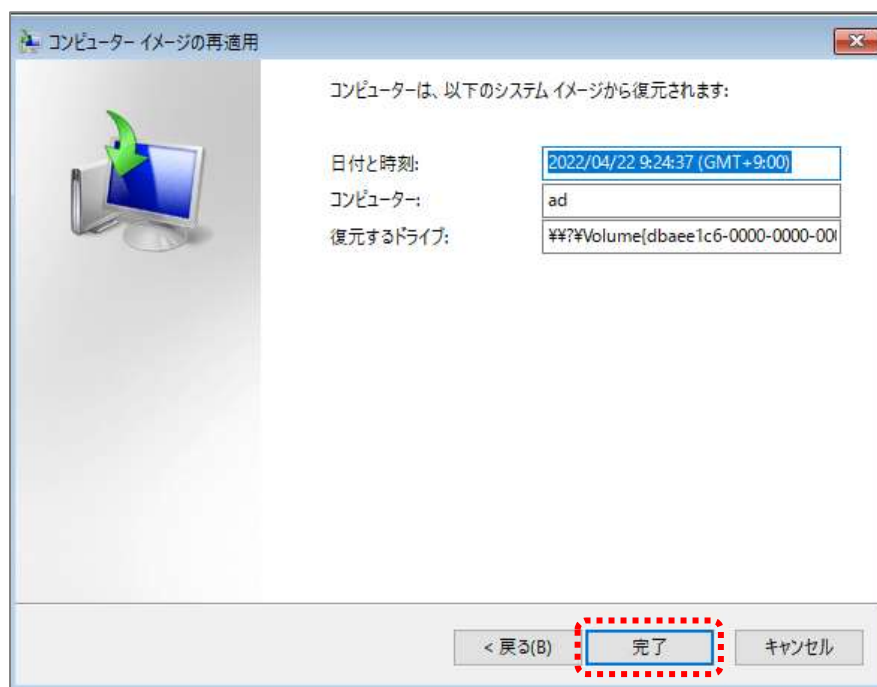
「**2022/04/22 9:24:37**」(システムイメージを取得した日時)を選択し、「**次へ**」ボタンをクリックします。



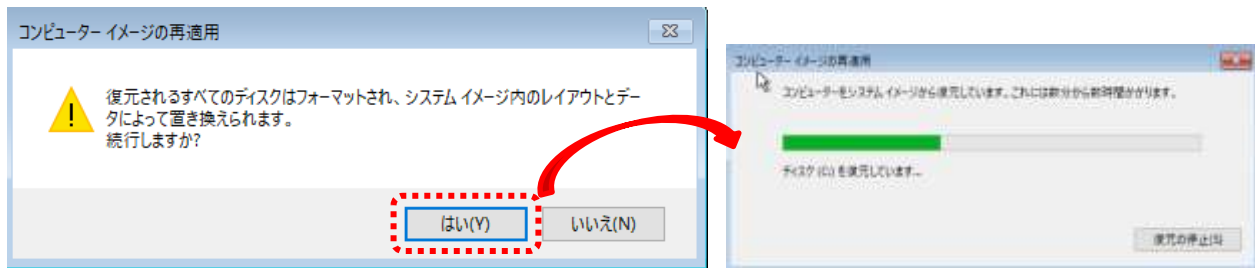
「ディスクをフォーマットしてパーティションに再分割する」にチェックを入れ、「次へ」ボタンをクリックします。



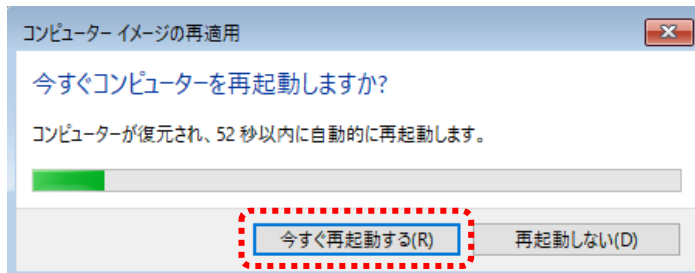
「完了」をクリックして、システムイメージの復元を開始します。



確認画面で「はい」をクリックします。

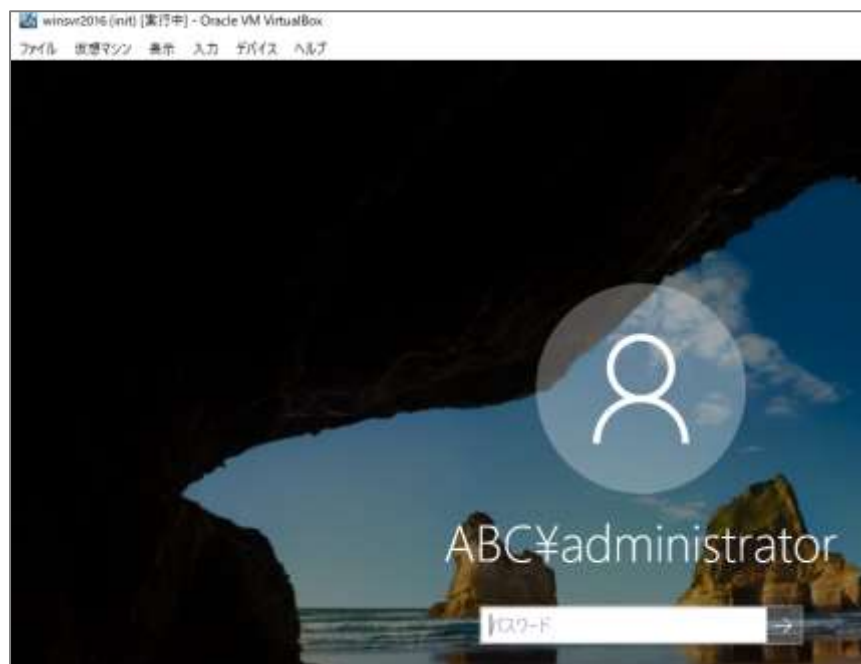


復元が完了すると、確認画面が表示されます。「今すぐ再起動する」をクリックします。



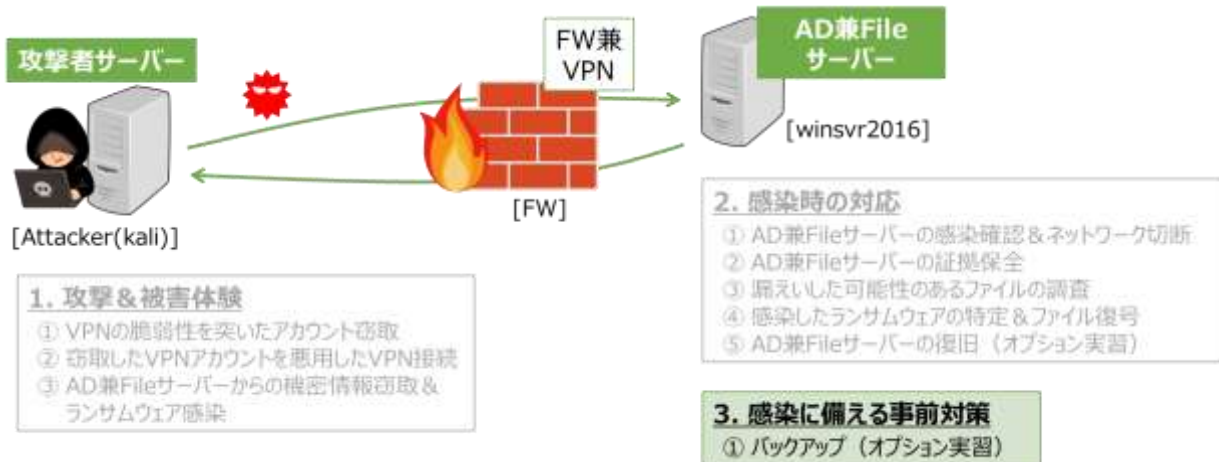
AD 兼 File サーバーが、システムイメージを取得した日時の状態に復元されます。

必要に応じて、「④感染したランサムウェアの特定 & ファイル復号」で復号したファイルを戻します。



3.3 感染に備える事前対策

ランサムウェア感染に備えた事前対策の例として、バックアップを体験します。

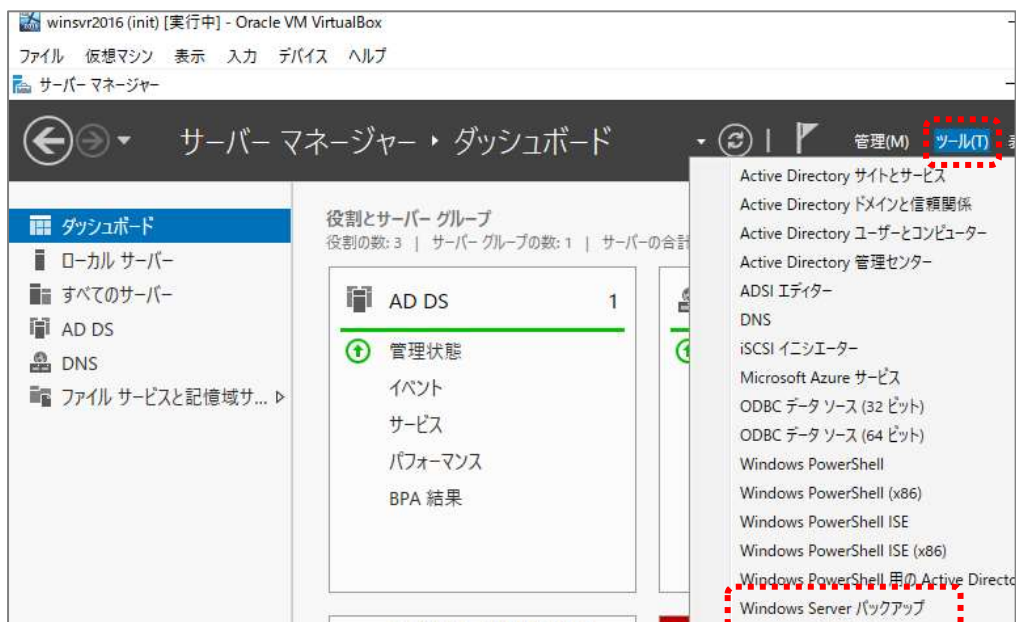


① バックアップ (オプション実習) [winsvr2016]

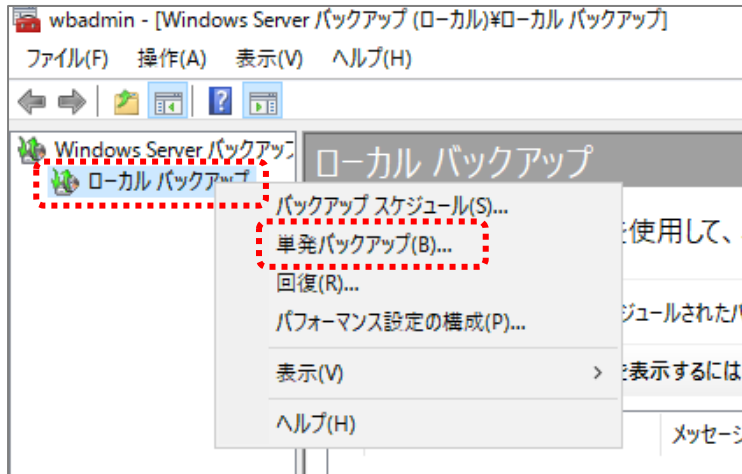
万が一ランサムウェアに感染した場合でも、短時間で復旧して業務を継続するために、重要なサーバー等は定期的にバックアップを取得し、適切に（サーバーと一緒にランサムウェアに感染しないように）保管しておくことが重要です。

本実習では、Windows 標準機能で「AD 兼 File サーバー」のシステムイメージを取得します。

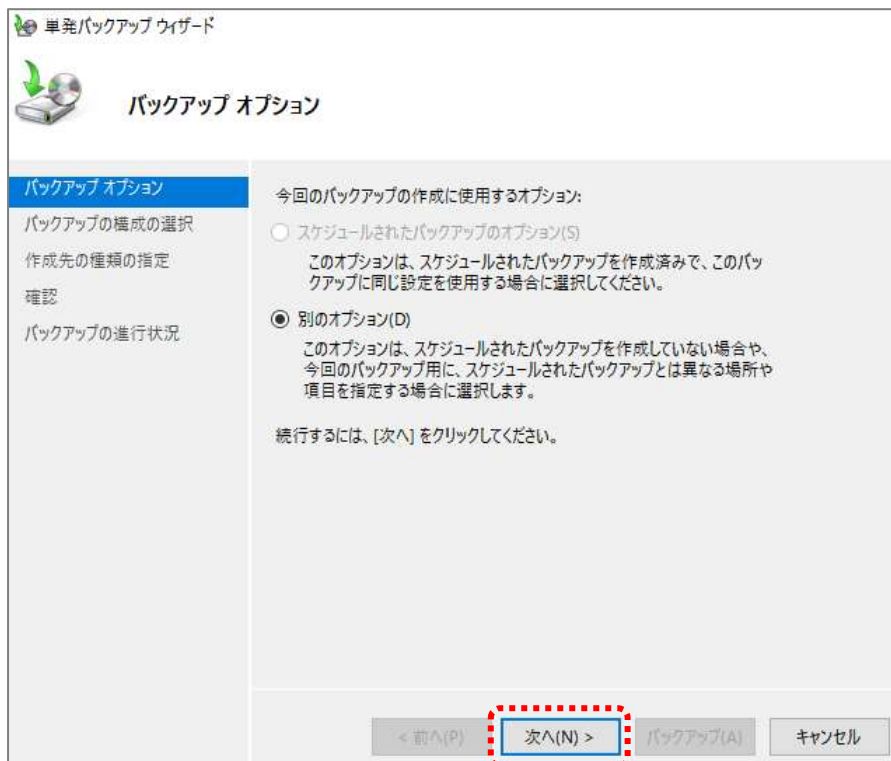
AD 兼 File サーバーの「サーバーマネージャー」で、「ツール」-「Windows バックアップ」をクリックします。



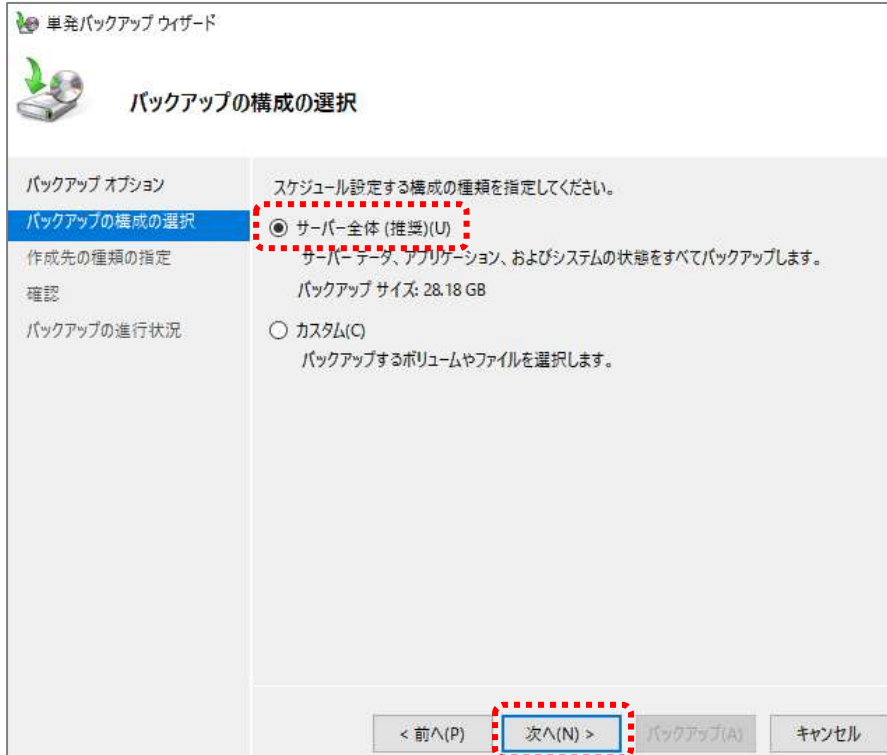
「ローカルバックアップ」を右クリックし、「単発バックアップ」をクリックします。



ウィザードが表示されたら、「次へ」ボタンをクリックします。



「バックアップの構成の選択」で「**サーバー全体**」が選択されていることを確認し、「**次へ**」ボタンをクリックします。



単発バックアップ ウィザード

バックアップの構成の選択

バックアップ オプション

バックアップの構成の選択

作成先の種類の指定

確認

バックアップの進行状況

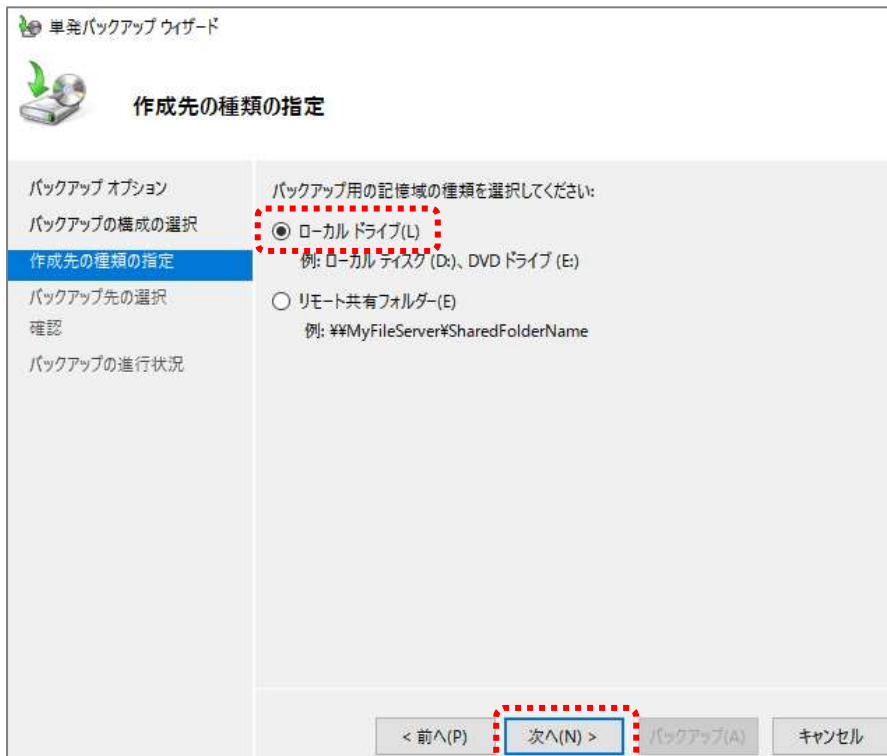
スケジュール設定する構成の種類を指定してください。

☒ **サーバー全体 (推奨)(U)**
サーバーデータ、アプリケーション、およびシステムの状態をすべてバックアップします。
バックアップ サイズ: 28.18 GB

☐ カスタム(C)
バックアップするボリュームやファイルを選択します。

< 前へ(P) **次へ(N) >** バックアップ(A) キャンセル

「作成先の種類の指定」で「**ローカルドライブ**」が選択されていることを確認し、「**次へ**」ボタンをクリックします。



単発バックアップ ウィザード

作成先の種類の指定

バックアップ オプション

バックアップの構成の選択

作成先の種類の指定

バックアップ先の選択

確認

バックアップの進行状況

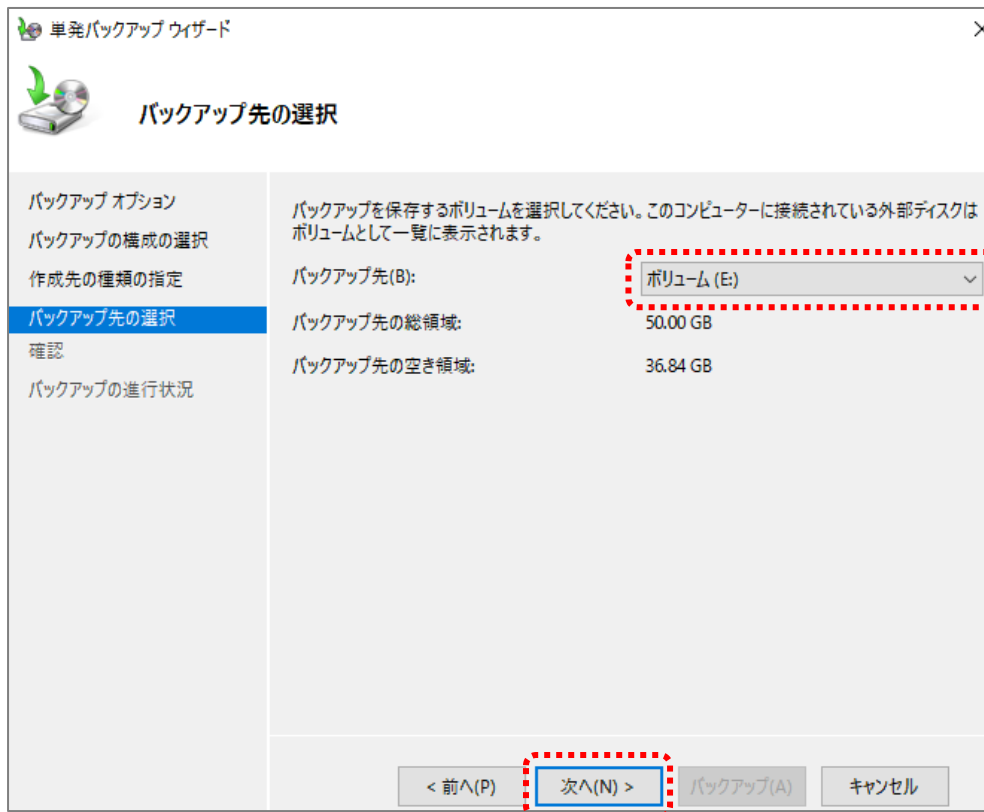
バックアップ用の記憶域の種類を選択してください:

☒ **ローカルドライブ(L)**
例: ローカル ディスク (D:), DVD ドライブ (E:)

☐ リモート共有フォルダー(E)
例: \\MyFileServer\SharedFolderName

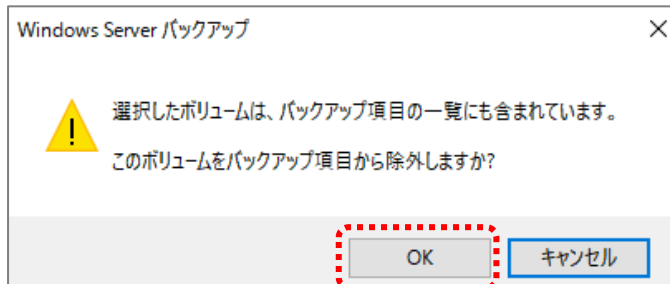
< 前へ(P) **次へ(N) >** バックアップ(A) キャンセル

「バックアップ先」で「**ボリューム(E:)**」(外付けハードディスクの想定)を指定し、「**次へ**」ボタンをクリックします。

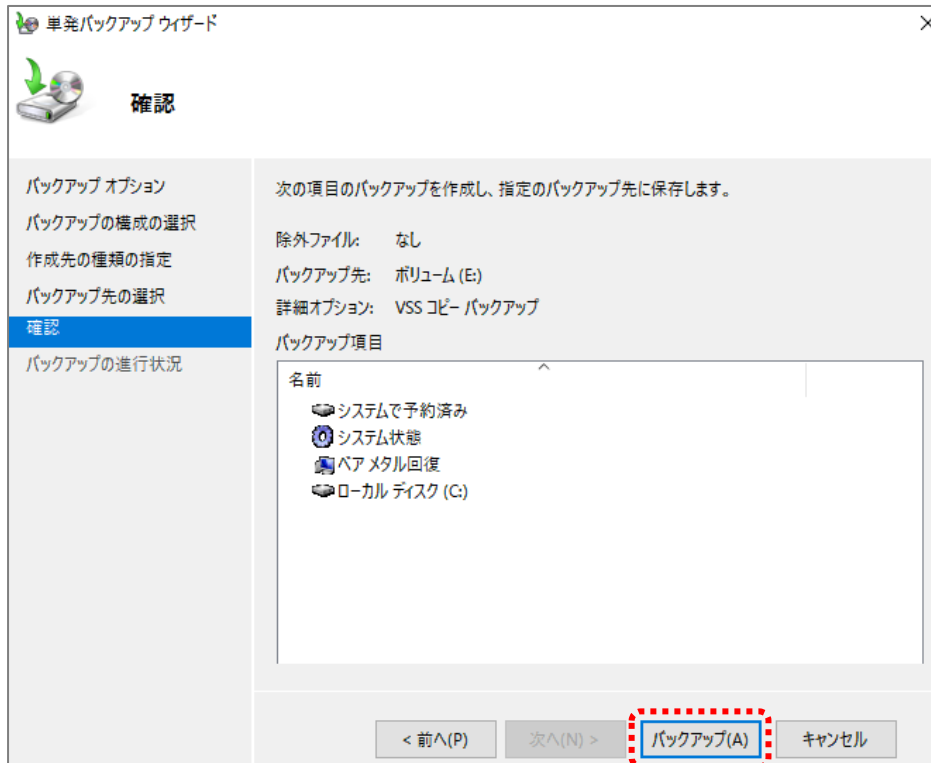


確認画面が表示されたら、「**OK**」ボタンをクリックします。

(バックアップ先の領域をバックアップ対象から除外して良いか確認するメッセージ)



「バックアップ」をクリックして、システムイメージの取得を開始します。

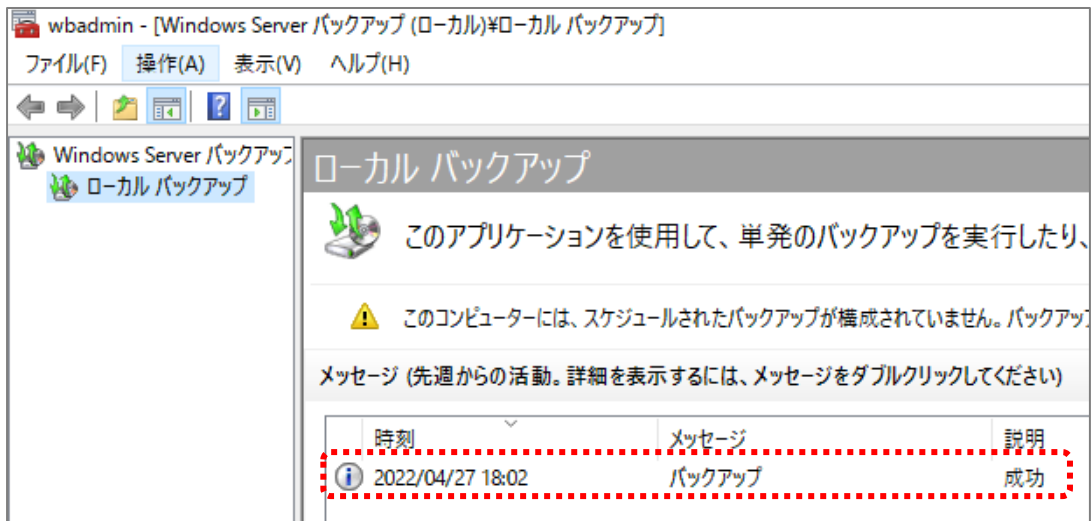


バックアップが完了すると、「完了しました」と表示されます。

「閉じる」ボタンをクリックしてウィザードを閉じます。



バックアップ一覧に、取得したバックアップの情報が表示されます。



バックアップ先として指定した「**ボリューム(E:)**」に、システムイメージが保存されています。
ランサムウェア感染時に一緒に暗号化されないように、ネットワークから隔離して保管します。

