

サイエンスパーク株式会社
セキュリティビジネス部

NonCopy 2 検証結果報告書

1. 概要

本書は、弊社が参画する国立研究開発法人情報通信研究機構（以降、NICT）の CYNEX アライアンス（CYNEX Co-Nexus E）における共同研究の一環として、弊社の情報漏洩対策製品である NonCopy2（以降、NC2）を検証した結果を記載したものである。なお、本書は NICT からの NC2 検証結果レポートをもとに作成した。

1.1. 目的、背景

昨今のサイバー攻撃の傾向を見ると、ランサムウェアによる被害が依然として多く（6. 参考資料(1)）、昨年は、警視庁よりデータを暗号化する（ランサムウェアを用いる）ことなくデータを窃取し、対価を要求する新たな手口（「ノーウェアランサム」）による被害も報告されている（6. 参考文献(2)）。

ChatGPT を始めとする生成 AI が悪用され、標的型攻撃の強化が予想される（参考文献(3), (4)）中、それらの攻撃を 100%防ぐこと（入口対策）は益々難しい状況となり、攻撃された場合にいかにして重要データを守るか、という出口対策の重要性が増している。

NC2 は、データ保護に焦点を当てた製品であり、中でも持ち出し防止機能（特定のフォルダからの持ち出し操作を禁止する）は本製品を特徴づける機能である。本検証では、NC2 をインストールした環境において、サイバー攻撃を想定した持ち出し操作を抑止できるかの確認を行った。

2. 総評

今回検証した範囲では、持ち出し操作が抑止できることを確認した。今後も検証を継続し、NC2 の有効性を確認する。

3. 検証内容

以下に、検証内容を報告する。

3.1. 検証方針

情報持ち出し・データ窃取を行う攻撃者は、マルウェア感染後の端末を手動操作してそれらを実行することが多い（6. 参考文献(5)）。具体的には、主に以下の3パターンの手法を用いる。

- (1) OS 標準ツールや Web ブラウザによる持ち出し、転送
- (2) 正規ツールの悪用（攻撃者のサーバーや正規のオンラインストレージへアップロード）
- (3) 独自ツールによる転送

本検証では、RAT や RDP（リモートデスクトップ）でターゲットとなる PC に手動でアクセスし、上記(1), (2)の手法を用いて持ち出し操作を実施する。その際に、NC2 による持ち出し防止機能で阻止できるかを検証する。

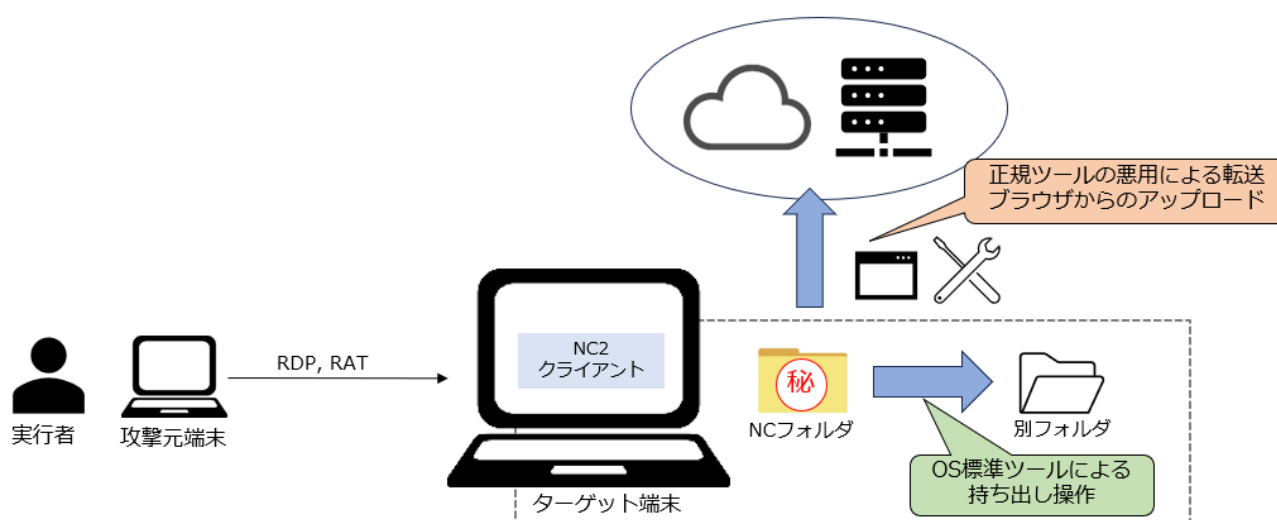


図 3.1

3.2. 検証方法

クライアント端末のデスクトップ上に以下の 2 種類のフォルダを作成し、それぞれにテキストファイルを配置し、持ち出し操作を実施する。

- (1) NC フォルダ：NC2 で保護するフォルダ
フォルダ名：Important・Confidentiality
- (2) 通常フォルダ：NC2 で保護しないフォルダ
フォルダ名：normal

3.3. 検証環境

以下の条件で検証を実施した。

対象	対象	詳細
アップロード先	仮想環境上に構築したサーバー	FTP サーバー
		SSH サーバー
		MinIO サーバー
	クラウドサービス	Google Drive
		MEGASync
クライアント端末	OS	Windows 10 22H2 Pro 64bit
	NC2 クライアント	Ver.1.8.6

表 3.3

4. 検証結果概要

以下に結果概要をまとめる。

持ち出し手法	ツール名	結果	結果詳細
正規ツールの悪用	Rclone	○	5.1.1
	WinSCP	○	5.1.2
	MEGAsync	○	5.1.3
	FileZilla	○	5.1.4
	Cyberduck	○	5.1.5
	PuTTY (FTP, SCP)	○	5.1.6, 5.1.7
	MinIO	○	5.1.8
OS 標準ツール	エクスプローラ	○	5.2.1
	PowerShell	○	5.2.2
Web ブラウザによる転送	Chrome	○	5.3.1
	Edge	○	5.3.2
	Firefox	○	5.3.3

表 4

5. 検証結果詳細

5.1. 正規ツールの悪用

5.1.1. Rclone

✓ 使用バージョン : rclone1.65.0

✓ 検証方法

Google Drive にアカウントを作成し、接続後に NC フォルダ内のファイルをアップロード

```
$ rclone copy [ローカルパス] rclone_gdrive:
```

✓ 検証結果 : 持ち出し防止成功

アップロードに失敗し、通信ができなくなった。

✓ エビデンス画面

```
PS C:\Users\walkure\rclone> .\rclone.exe copy C:\Users\walkure\Desktop\Important-Confidentiality\SECRET.txt rclone_gdrive:

2023/12/18 16:23:24 ERROR : SECRET.txt: Failed to copy: couldn't list directory: Get "https://www.googleapis.com/drive/v3/files?alt=json&fields=files%28id%2Cname%2Csize%2Cmd5Checksum%2Csha1Checksum%2Csha256Checksum%2Ctrashed%2CexplicitlyTrashed%2CmodifiedTime%2CcreatedTime%2CmimeType%2Cparents%2CwebViewLink%2CshortcutDetails%2CexportLinks%2CresourceKey%29%2CnextPageToken%2CincompleteSearch&includeItemsFromAllDrives=true&pageSize=1000&prettyPrint=false&q=trashed%3Dfalse+and+%28%270AEuQE1rekubmUk9PVA%27+in+parents%29+and+%28name%3D%27SECRET.txt%27%29&supportsAllDrives=true": dial tcp 172.217.26.234:443: connectex: An attempt was made to access a socket in a way forbidden by its access permissions.
2023/12/18 16:23:24 ERROR : Attempt 1/3 failed with 1 errors and: couldn't list directory: Get "https://www.googleapis.com/drive/v3/files?alt=json&fields=files%28id%2Cname%2Csize%2Cmd5Checksum%2Csha1Checksum%2Csha256Checksum%2Ctrashed%2CexplicitlyTrashed%2CmodifiedTime%2CcreatedTime%2CmimeType%2Cparents%2CwebViewLink%2CshortcutDetails%2CexportLinks%2CresourceKey%29%2CnextPageToken%2CincompleteSearch&includeItemsFromAllDrives=true&pageSize=1000&prettyPrint=false&q=trashed%3Dfalse+and+%28%270AEuQE1rekubmUk9PVA%27+in+parents%29+and+%28name%3D%27SECRET.txt%27%29&supportsAllDrives=true": dial tcp 172.217.26.234:443: connectex: An attempt was made to access a socket in a way forbidden by its access permissions.
2023/12/18 16:23:34 ERROR : Attempt 2/3 failed with 1 errors and: couldn't list directory: Get "https://www.googleapis.com/drive/v3/files?alt=json&fields=files%28id%2Cname%2Csize%2Cmd5Checksum%2Csha1Checksum%2Csha256Checksum%2Ctrashed%2CexplicitlyTrashed%2CmodifiedTime%2CcreatedTime%2CmimeType%2Cparents%2CwebViewLink%2CshortcutDetails%2CexportLinks%2CresourceKey%29%2CnextPageToken%2CincompleteSearch&includeItemsFromAllDrives=true&pageSize=1000&prettyPrint=false&q=trashed%3Dfalse+and+%28%270AEuQE1rekubmUk9PVA%27+in+parents%29+and+%28name%3D%27SECRET.txt%27%29&supportsAllDrives=true": dial tcp 142.251.42.202:443: connectex: An attempt was made to access a socket in a way forbidden by its access permissions.
```

図 5.1.1

5.1.2. WinSCP

✓ 使用バージョン：WinSCP 6.1.2

✓ 検証方法

NC フォルダ内のファイルを SSH サーバー宛に転送する。

✓ 検証結果：持ち出し防止成功

転送しようとするすると転送中画面が表示されるが、タイムアウトとなり切断された。
アプリケーションが終了するまで NC フォルダ以外のファイルも転送不可であった。

✓ エビデンス画面

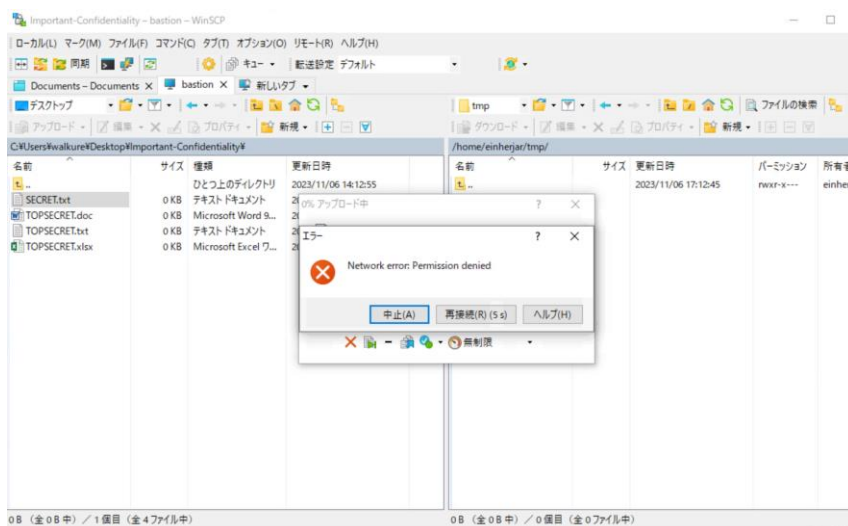


図 5.1.2 (1)

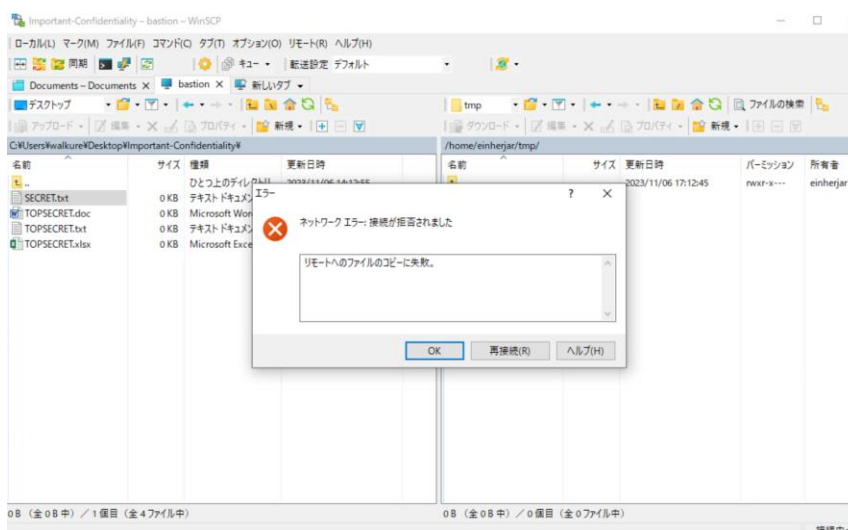


図 5.1.2 (2)

5.1.3. MEGASync

✓ 使用バージョン：4.11.0

✓ 検証方法

MEGA クライアントのアップロード機能を使用して、NC フォルダ内のファイルを MEGA へアップロードする。

✓ 検証結果：持ち出し防止成功

通常ファイルではアップロードがすぐに完了した。

NC フォルダ内のファイルではアップロード開始後転送は進まず、0 バイトのままであった。

✓ エビデンス画面

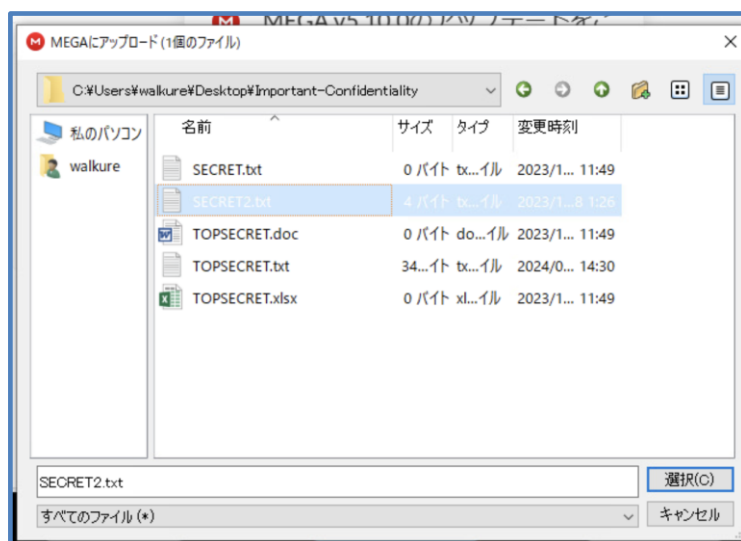


図 5.1.3 (1)



図 5.1.3 (2)

5.1.4. FileZilla

✓ 使用バージョン：3.66.1

✓ 検証方法

NC フォルダ内のファイルを FTP サーバー宛に転送する。

✓ 検証結果：持ち出し防止成功

転送しようとする、転送中画面が表示されるが、タイムアウトとなり切断された。
アプリケーションが終了するまで NC フォルダ以外のファイルも転送不可であった。

✓ エビデンス画面

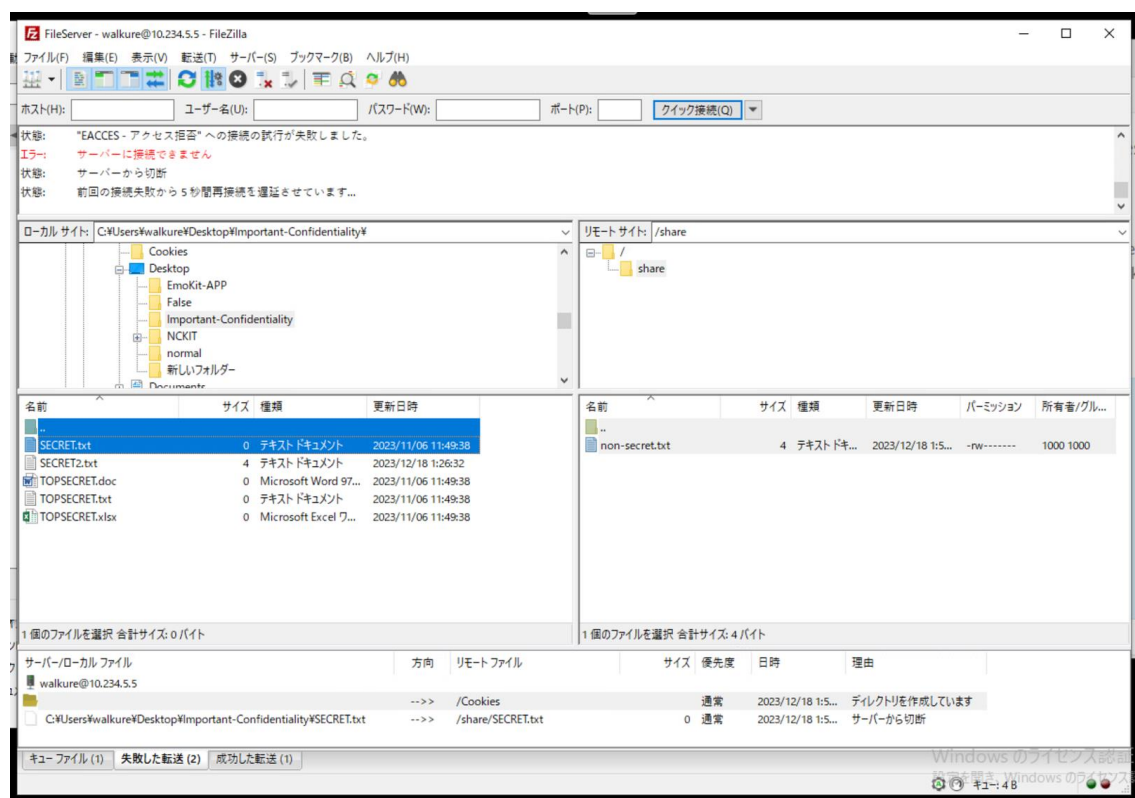


図 5.1.4

5.1.5. CyberDuck

✓ 使用バージョン：8.7.1

✓ 検証方法

NC フォルダ内のファイルを FTP サーバー宛に転送する。

✓ 検証結果：持ち出し防止成功

転送しようとする転送中画面が表示されるが、タイムアウトとなり、切断された。
アプリケーションが終了するまで NC フォルダ以外のファイルも転送不可であった。

✓ エビデンス画面

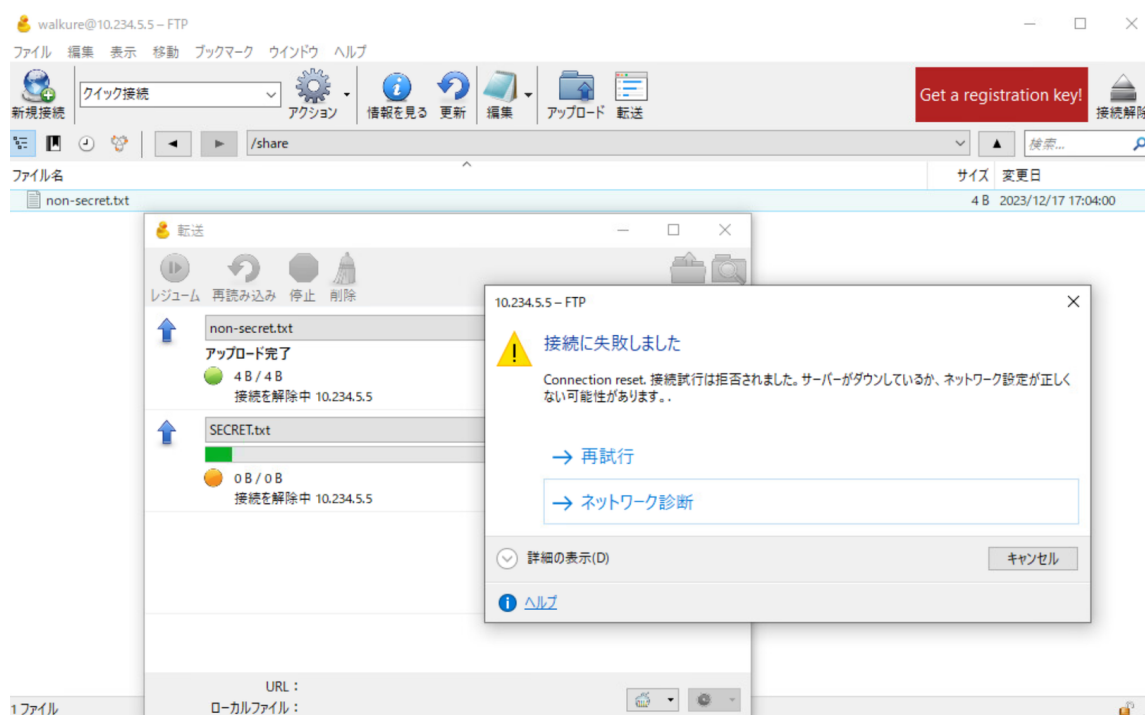


図 5.1.5

5.1.6. PuTTY (FTP)

✓ 使用バージョン : 0.79

✓ 検証方法

PSFTP を使用し FTP サーバーに接続後、NC フォルダ内のファイルを転送する。

✓ 検証結果 : 持ち出し防止成功

ネットワークエラーで転送に失敗した。

✓ エビデンス画面

```
PS C:\Users#walkure> psftp
psftp: no hostname specified; use "open host.name" to connect
psftp> open 10.234.5.5
The host key is not cached for this server:
  10.234.5.5 (port 22)
You have no guarantee that the server is the computer you
think it is.
The server's ssh-ed25519 key fingerprint is:
  ssh-ed25519 255 SHA256:MiISfIyionNBBfyMazeLFNFgwWjhWicOybbIk8mwors
If you trust this host, enter "y" to add the key to PSFTP's
cache and carry on connecting.
If you want to carry on connecting just once, without adding
the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n, Return cancels connection, i for more info) yes
login as: walkure
walkure@10.234.5.5's password:
Remote working directory is /home/walkure
psftp> ls
Listing directory /home/walkure
dr-xr-x--- 6 walkure walkure 4096 Dec 14 06:03 .
drwxr-xr-x 3 root root 4096 Feb 7 2023 ..
drwx----- 3 walkure walkure 4096 Mar 2 2023 .ansible
-rw----- 1 walkure walkure 507 Aug 9 08:40 .bash_history
-rw-r--r-- 1 walkure walkure 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 walkure walkure 3771 Jan 6 2022 .bashrc
drwx----- 2 walkure walkure 4096 Feb 7 2023 .cache
-rw----- 1 walkure walkure 20 Dec 14 06:03 .lessht
-rw-r--r-- 1 walkure walkure 807 Jan 6 2022 .profile
drwx----- 2 walkure walkure 4096 Feb 7 2023 .ssh
-rw-r--r-- 1 walkure walkure 0 Feb 7 2023 .sudo_as_admin_successful
-rw----- 1 walkure walkure 748 Dec 14 05:02 .viminfo
drwxrwxrwx 2 root root 4096 Dec 17 17:04 share
psftp>
```

図 5.1.6 (1)

```
psftp> cd share
Remote directory is now /home/walkure/share
psftp> put .#Desktop#normal#non-secret.txt
local:./#Desktop#normal#non-secret.txt => remote:/home/walkure/share/non-secret.txt
psftp> put .#Desktop#Important-Confidentiality#SECRET.txt
FATAL ERROR: Network error: Software caused connection abort
PS C:\Users#walkure>
```

図 5.1.6 (2)

5.1.7. PuTTY (SCP)

✓ 使用バージョン : 0.79

✓ 検証方法

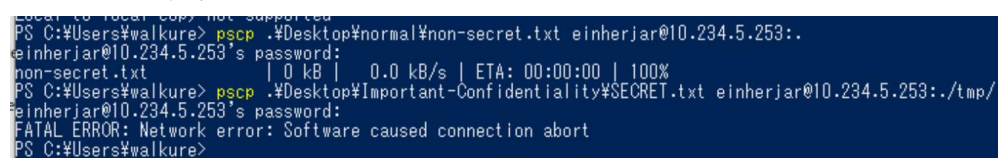
PSCP を使用して以下のコマンドで NC フォルダ内のファイルを SSH サーバー宛に転送する。

```
pscp.exe -c:<アップロード元> <アップロード先>
```

✓ 検証結果 : 持ち出し防止成功

転送中画面が表示されるが、ネットワークエラーとなり、切断された。

✓ エビデンス画面



```
Local to local copy not supported
PS C:\Users#walkure> pscp .\Desktop\normal\non-secret.txt einherjar@10.234.5.253:.
einherjar@10.234.5.253's password:
non-secret.txt      | 0 kB | 0.0 kB/s | ETA: 00:00:00 | 100%
PS C:\Users#walkure> pscp .\Desktop\Important-Confidentiality\SECRET.txt einherjar@10.234.5.253:./tmp/
einherjar@10.234.5.253's password:
FATAL ERROR: Network error: Software caused connection abort
PS C:\Users#walkure>
```

図 5.1.7

5.1.8. MinIO

✓ 使用バージョン : 2024-01-05T05-04-32Z

✓ 検証方法

MinIO クライアントを用いて、MinIO サーバーに対して NC フォルダ内のファイルをアップロードする。

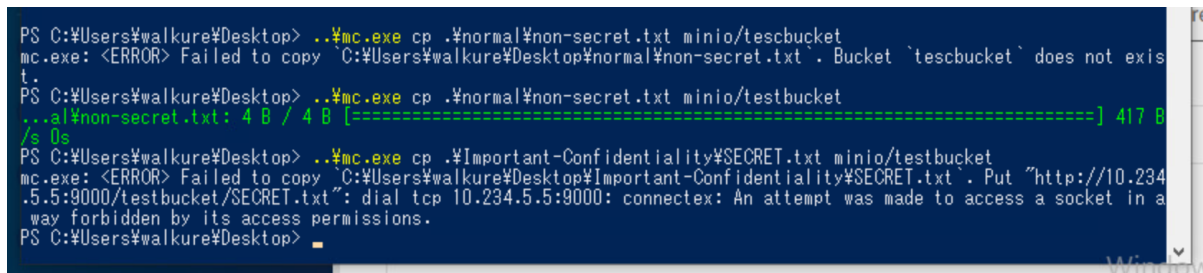
```
mc.exe cp <アップロード元> <アップロード先>
```

✓ 検証結果 : 持ち出し防止成功

通常フォルダ内のファイルはアップロード成功した。

NC フォルダ内のファイルはネットワークエラーとなり、切断された。

✓ エビデンス画面



```
PS C:\Users\walkure\Desktop> .\mc.exe cp .\normal\non-secret.txt minio/tescbucket
mc.exe: <ERROR> Failed to copy `C:\Users\walkure\Desktop\normal\non-secret.txt`. Bucket `tescbucket` does not exist.
PS C:\Users\walkure\Desktop> .\mc.exe cp .\normal\non-secret.txt minio/testbucket
...al\non-secret.txt: 4 B / 4 B [=====] 417 B
/s Os
PS C:\Users\walkure\Desktop> .\mc.exe cp .\Important-Confidentiality\SECRET.txt minio/testbucket
mc.exe: <ERROR> Failed to copy `C:\Users\walkure\Desktop\Important-Confidentiality\SECRET.txt`. Put `http://10.234.5.5:9000/testbucket/SECRET.txt`: dial tcp 10.234.5.5:9000: connectex: An attempt was made to access a socket in a way forbidden by its access permissions.
PS C:\Users\walkure\Desktop>
```

図 5.1.8

5.2. OS 標準ツール

5.2.1. エクスプローラ

✓ 検証方法

エクスプローラを使用して、NC フォルダ内のファイルをコピー、ペースト、移動を試行する。

✓ 検証結果：持ち出し防止成功

移動に失敗し、中断した。

✓ エビデンス画面

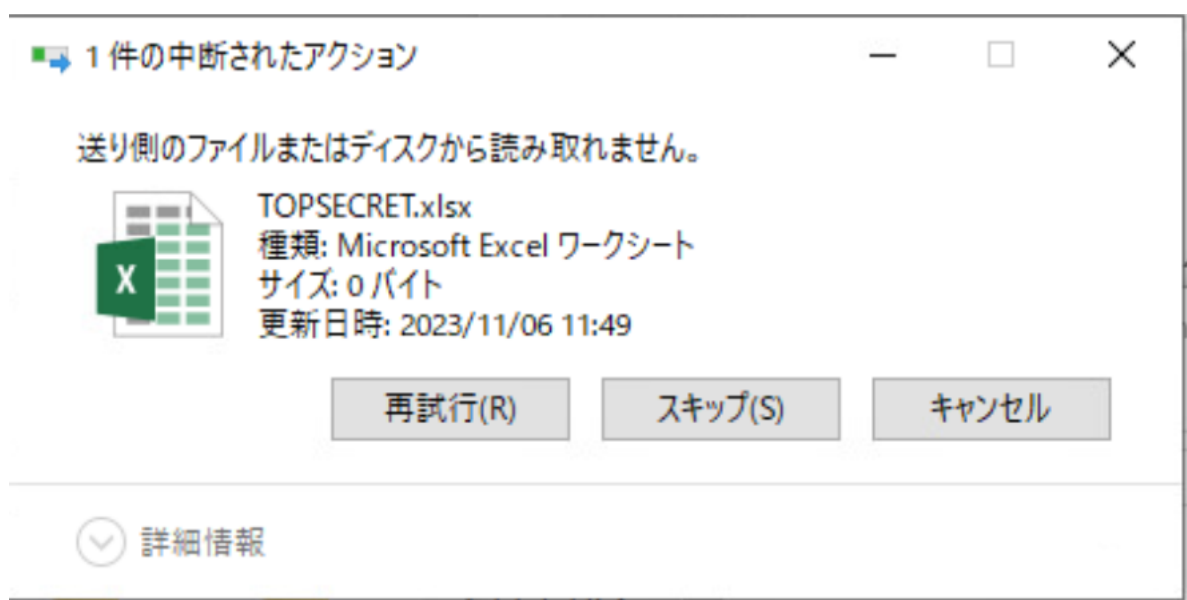


図 5.2.1

5.2.2. PowerShell

✓ 検証方法

以下の2種類のコマンドでNCフォルダ内のファイルのPC内移動を試行

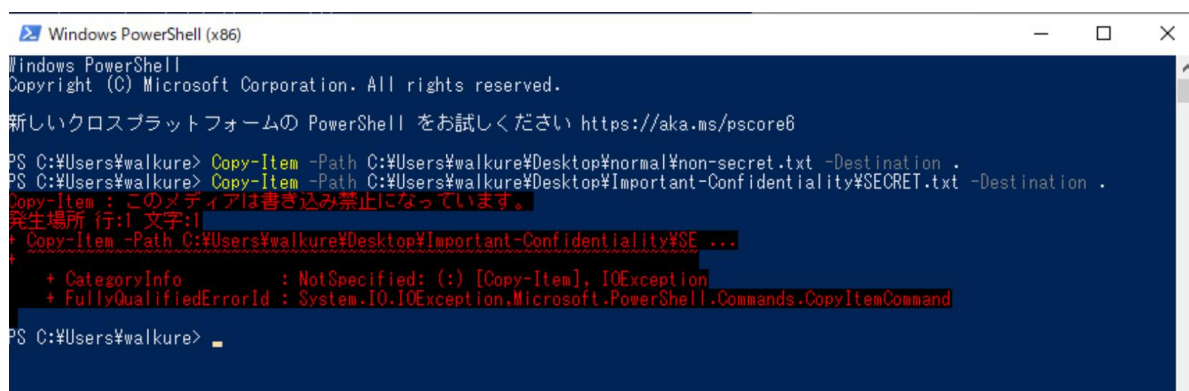
```
Copy-Item -Path “コピー元” -Destination “コピー先”
```

```
Move-Item -Path “コピー元” -Destination “コピー先”
```

✓ 検証結果：持ち出し防止成功

どちらのコマンドも失敗した。

✓ エビデンス画面



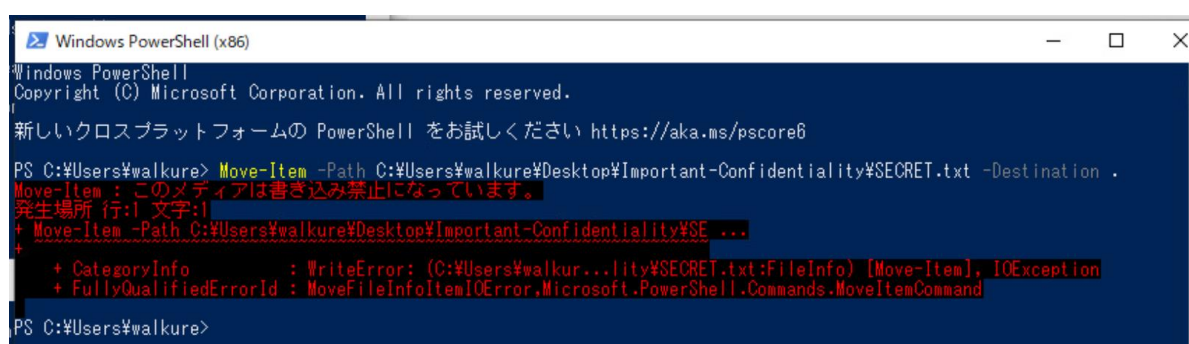
```
Windows PowerShell (x86)
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

新しいクロスプラットフォームの PowerShell をお試しください https://aka.ms/pscore6

PS C:\Users#walkure> Copy-Item -Path C:\Users#walkure\Desktop\normal\non-secret.txt -Destination .
PS C:\Users#walkure> Copy-Item -Path C:\Users#walkure\Desktop\Important-Confidentiality\SECRET.txt -Destination .
Copy-Item : このメディアは書き込み禁止になっています。
発生場所 行:1 文字:1
+ Copy-Item -Path C:\Users#walkure\Desktop\Important-Confidentiality\SE ...
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Copy-Item], IOException
+ FullyQualifiedErrorId : System.IO.IOException,Microsoft.PowerShell.Commands.CopyItemCommand

PS C:\Users#walkure>
```

図 5.2.2 (1)



```
Windows PowerShell (x86)
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

新しいクロスプラットフォームの PowerShell をお試しください https://aka.ms/pscore6

PS C:\Users#walkure> Move-Item -Path C:\Users#walkure\Desktop\Important-Confidentiality\SECRET.txt -Destination .
Move-Item : このメディアは書き込み禁止になっています。
発生場所 行:1 文字:1
+ Move-Item -Path C:\Users#walkure\Desktop\Important-Confidentiality\SE ...
+ ~~~~~
+ CategoryInfo          : WriteError: (C:\Users#walkur...lity\SECRET.txt:FileInfo) [Move-Item], IOException
+ FullyQualifiedErrorId : MoveFileInfoItemIOError,Microsoft.PowerShell.Commands.MoveItemCommand

PS C:\Users#walkure>
```

図 5.2.2 (2)

5.3. Web ブラウザによる転送

5.3.1. Chrome

- ✓ 使用バージョン：
- ✓ 検証方法
NC フォルダ内のファイルをブラウザ経由で Google Drive にアップロードする。
- ✓ 検証結果：持ち出し防止成功
アップロードに失敗した。
- ✓ エビデンス画面

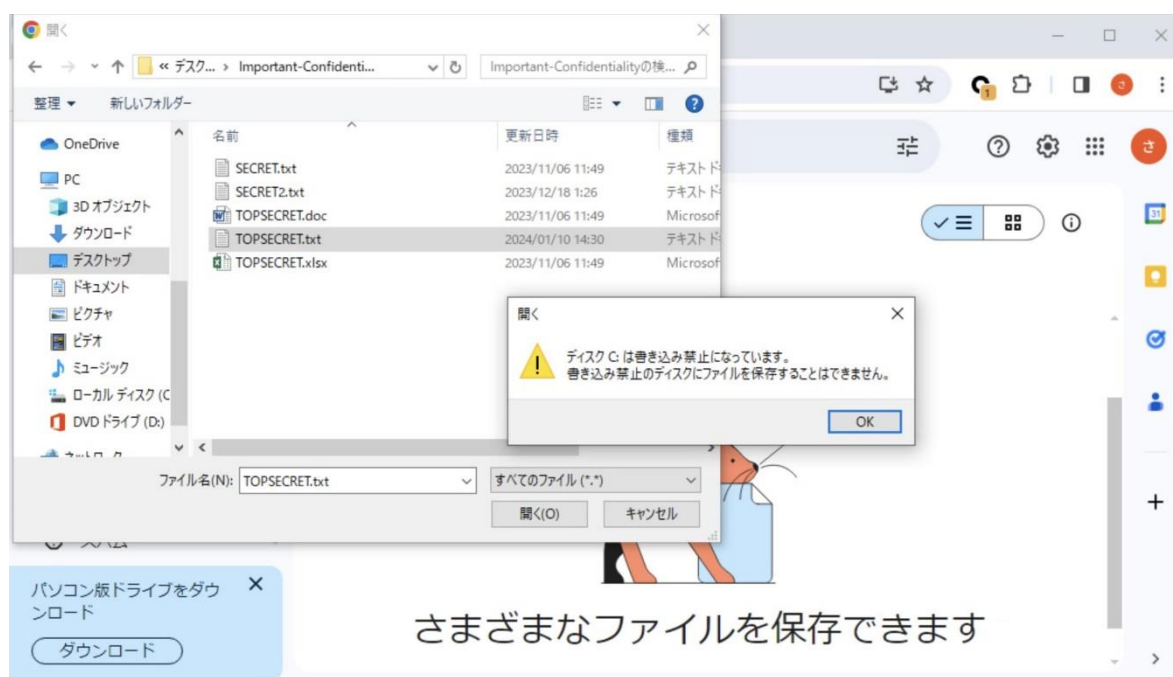


図 5.3.1

5.3.2. Edge

- ✓ 使用バージョン：
- ✓ 検証方法
NC フォルダ内のファイルをブラウザ経由で Google Drive にアップロードする。
- ✓ 検証結果：持ち出し防止成功
アップロードに失敗した。
- ✓ エビデンス画面

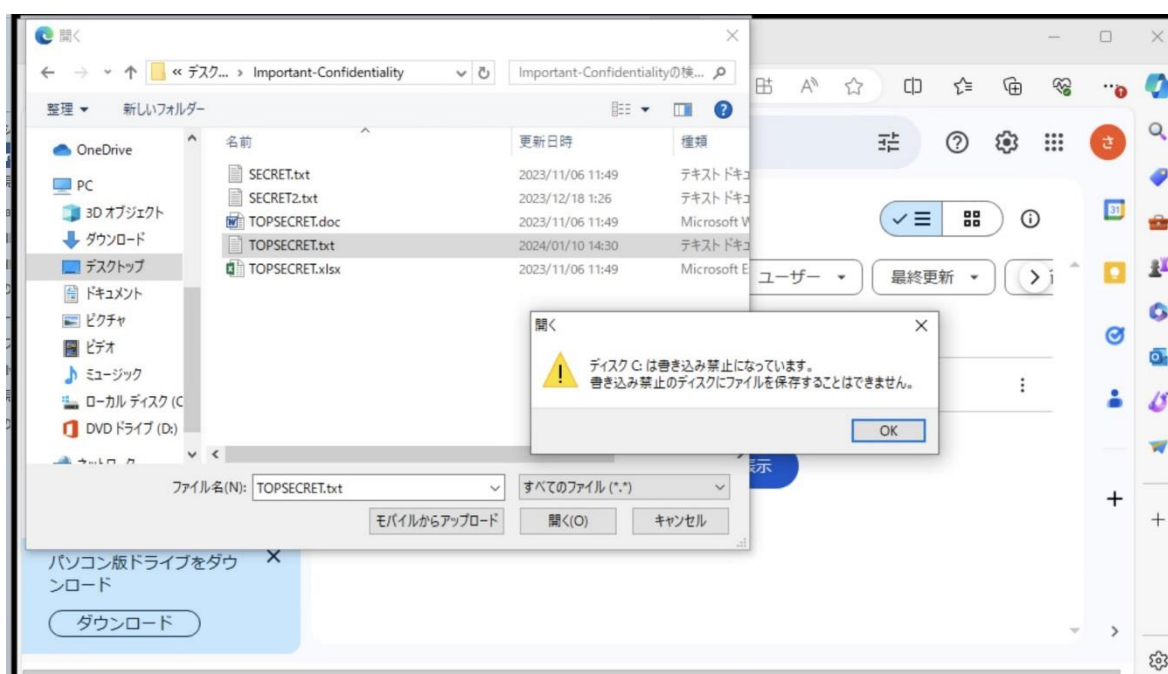


図 5.3.2

5.3.3. Firefox

- ✓ 使用バージョン：
- ✓ 検証方法
NC フォルダ内のファイルをブラウザ経由で Google Drive にアップロードする。
- ✓ 検証結果：持ち出し防止成功
アップロードに失敗した。
- ✓ エビデンス画面

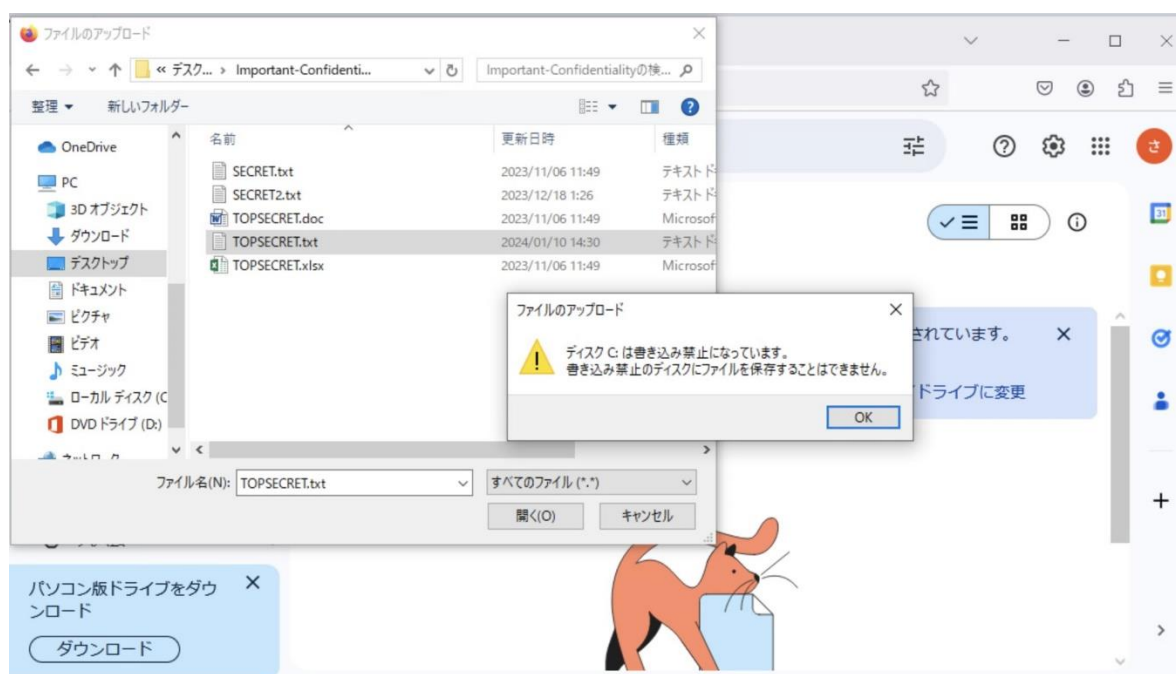


図 5.3.3

6. 参考文献

- (1) [情報セキュリティ重大脅威 2024](#)
- (2) [令和 5 年上半期におけるサイバー空間をめぐる脅威の情勢等について](#)
- (3) [Google Cloud Cybersecurity Forecast 2024: 今後 1 年間のサイバー脅威の展望](#)
- (4) [Cyber Signals: AI 時代におけるサイバー脅威への対応と防衛力の強化](#)
- (5) [Data Exfiltration: Increasing Number of Tools Leveraged by Ransomware Attackers](#)

以上