豊橋技術科学大学におけるランサムウェア感染事例の分析

土屋 雅稔, 中村 純哉

豊橋技術科学大学 情報メディア基盤センター

{tsuchiya,junya}@imc.tut.ac.jp

A case analysis of the ransomware incident at Toyohashi University of Technology

Masatoshi Tsuchiya, Junya Nakamura

Information and Media Center, Toyohashi University of Technology

1 はじめに

近年，インターネットを経由したランサムウェアやマルウェアによるインシデントは，増加の一途を辿っている．例えば, UCSF (University of California, San Francisco) は, 2020 年 6 月にランサムウェアによる攻撃を受け，データの身代金として 114 万ドルを支払ったと報道されている．[*1] この対策のため，各種機関においては CSIRT を設立し，インシデント対応体制を強化するように求められている．

豊橋技術科学大学においても, 2019 年 4 月 3 日 (水) から 4 月 5 日 (金) にかけて，メール経由でのランサムウェア感染インシデントにより，2 日間の事務用情報システムの停止を経験した．本稿では，この事例の詳細および，この経験に基づく CSIRT 体制の分析について述べる．

2 インシデント対応の詳細

豊橋技術科学大学は，2019 年 4 月 3 日 (水) から 4 月 5 日 (金) にかけて，メール経由でのランサムウェア感染インシデントを経験した．ここでは，このインシデント対応の詳細について述べる．

2.1 初動対応 (4 月 3 日)

表 1 に，本インシデントの経過についての時系列情報を示す．「不審な拡張子のファイルが存在する」と一般職員から CSIRT 窓口に通報があった時点から調査を開始し，通報から 40 分後にランサムウェア感染疑いを認識した．CSIRT として，まず感染拡大の阻止について意識しながら対応を開始した．

初動段階では，マルウェアの種類や感染経路，活動範囲など，全てが未知の状態から対応を開始しなければならないため，かなりの試行錯誤が生じることは避けられない．最初に，基本の対応として，ファイルサーバと被害端末をネットワークから遮断した．本インシデントの対象となったファイルサーバは，物理的に独立した NAS であるため，物理的にネットワークを遮断することができた．次に，不審な拡張子のファイルの所有者情報から被害者候補を特定，被害者候補が利用している端末をネットワークから遮断した．当該端末は，VMware Horizon 上で動作する仮想マシンであるので，ハイパーバイザ上の操作により，仮想的にネットワークを遮断した．

次に検討したことは，マルウェアが感染 · 潜伏している端末の有無である．初動段階では，マルウェアの種類が未知であったため，ログの精査を中心として検討した．最初に，ファイルサーバのアクセスログ上でマルウェアの挙動を検討した．本学のファイルサーバでは，機微情報の漏洩に備えて，ファイルの読み書きやファイル名の変更などの全てのファイルアクセスに対してアクセスログを採取している．被害者によるファイルアクセスログの抜粋を図 1 に示す．なお，図 1 では，本稿の記述に差し支えない範囲で，サーバ名，ユーザ名，ファイル名を適宜に置換している．第 1 に，被害者権限によって他端末からファイルアクセスが行われていないかを確認し，被害者権限による他端末からのファイルアクセスは行われていないこと，言い換えれば，同一ユーザ権限による水平感染の可能性が低いことを確認した．第 2 に，図 1 から，本インシデントのマルウェアは，大量にファイル名を変更するこ

[*1] https://www.bloomberg.com/news/features/2020-08-19/ucsf-hack-shows-evolving-risks-of-ransomware-in-the-covid-era

とが分かる．そのため，まずファイル名を大量に変更しているユーザの有無を検討し，そのようなユーザが存在しないことを確認した．次に，当該端末から学外への通信の有無を調査した．当該端末は，事務用途に用いられている端末であるため，事務用途の閉域ネットワーク内にある．そのため，閉域ネットワークから出るための NAT 装置およびプロキシサーバ，および全学ネットワークと SINET の結節点に設置されている全学 FW 装置のログをチェックした．この段階では，マルウェアの活動期間が未知であるため，暫定的に 4 月 3 日当日のログを対象として検討した．その結果，当該端末から学外への通信については，Windows Update 配信サイトなどの幾つかの既知のサイトのみであり，未知のサイトに対する通信は確認できなかった．

以上の調査より，潜伏している可能性は排除できないものの，少なくとも他端末において同様に活動中のマルウェアが存在しないことが確認できたため，初動としてのネットワーク遮断は完了していると判断した．

2.2 証拠保全および感染経路調査 (4 月 3 日)

初動対応の完了は，おおよそ 4 月 3 日の 14:00 前後である．この段階では，CSIRT としては，以下の 2 点を意識していた．

1. 感染経路と影響範囲の確定
2. 被害の証拠保全と復旧方法の検討

本インシデントの対象となったファイルサーバは，毎日 1 回深夜にスナップショットを作成するよう設定している．また，1 週間に 1 回の頻度でバックアップも作成している．よって，感染経路と影響範囲さえ確定できれば，感染直前の時点に復旧することは可能であると考えていた．言い換えれば，改ざんされたデータという証拠が，復旧によって消滅してしまうことが予想されていたため，証拠保全の方法を検討した．完全な証拠保全を行うには，当該ファイルサーバには手を触れずに，代替ファイルサーバを立ち上げる必要があるが，学内にはそのような目的に利用できる代替機材は存在せず，また緊急に調達することも不可能と考えられた．そのため，USB 接続の外付け HDD を緊急に調達し，ファイルサーバ上の改ざん後のデータを全てコピーすることにした．ただし，この段階では影響範囲が確定されていなかったため，ファイルサーバをネットワークに再接続することにはためらいもあった．そのため，ネットワークから他端末を排除 (具体的には電源断) し，ファイルサーバとコピー作業に用いる端末のみの環境を構築し，コピーを開始した．

特に必要なことは，感染経路 (感染の時系列を含む) の確定である．感染経路が確定できない限り，影響範囲も確定できず，したがって安全な復旧方法も決定できない．そのため，まず被害者に当日行った操作についての聞き取り調査を行ったが，有用な情報は得られなかった．ただし，ファイルサーバの物理的遮断によって事務局の全業務が停止していたため，被害者が極度に萎縮していたことは留意する必要がある．

この段階では，メール経由の感染またはウェブ経由の感染の両方の可能性を検討していた．メール経由の感染の可能性を検討するため，被害者に当日に受け取ったメールを一覧にするように依頼したが不完全な一覧しか得られず，メール経由の感染に関する手がかりは得られなかった．ウェブ経由の感染の可能性を検討するため，プロキシサーバおよび全学 FW 装置のログをチェックした．しかし，当該端末から学外への通信については，Windows Update 配信サイトなどの幾つかの既知のサイトのみであり，未知のサイトに対する通信は確認できなかった．条件付けが漠然としているため，大量の通信ログを解析して痕跡を発見することは，ほとんど不可能と思われた．なお，当該端末は，VMware Horizon の機能により USB ストレージデバイスの利用が制限されているため，USB ストレージデバイスを経由した感染という可能性は低いと判断していた．

2.3 感染経路調査 (4 月 4 日)

この段階に至っても，マルウェアの探索はなかなか進まなかった．最初の手がかりは，被害者のユーザプロファイルをアンチウイルスソフトでスキャンしたところ，複数のマルウェアが発見されたことである．スキャンには，インシデント発生時最新のパターンファイルを適用した Symantec Endpoint Protection 12 を用いたが，マルウェアの種類は `Trojan.Gen.MBT` や `Heur.AdvML.B` などの一般的な種類としか特定できなかったため，ファイルのハッシュ値からマルウェアの種類を調査した．調査の結果，`documentTax.doc.exe` という名前のファイルから発見されたマルウェアが本インシデントに強く関連すると 4 月 4 日 11:40 に判明した．

次に，4 月 4 日 17:26 に，`documentTax.doc.exe` が格納された圧縮ファイル `Taxdocument.rar` が，被害端末から発見された．この圧縮ファイルのファイル名をキーとして被害者のメールボックスを全検索し，

圧縮ファイルが添付されていたメールを発見した．当該メールのヘッダに記録されている配送情報とメールサーバのログを突合して，表 1 のように感染の時系列を完全に確定した．メールサーバは完全に独立した UNIX サーバであり，本インシデントのマルウェアによって，メールサーバのログが改ざんされる可能性は無いと考えられる．したがって，本インシデントのマルウェアの活動期間は，長く見積もっても 4 月 3 日 10:03:49 (メールサーバ接続) から 11:39 (被害端末の遮断完了) である．

活動期間が確定できたので，再度，ファイルサーバのアクセスログ，全学 FW のネットワーク接続ログなどの各種のログを精査した．精査の結果，他端末への感染はないと判断し，4 月 3 日 01:00 時点のスナップショットを復元するという復旧方法を決定した．最終的に，4 月 5 日にデータおよび業務の復旧を達成した．

2.4 その他

本インシデントは 4 月上旬に発生した．この時期は，入学式や新入生ガイダンスなど多くのイベントが計画されており，それらで必要となるファイルもファイルサーバに保存されていた．また，関係省庁に提出する予定のファイルがファイルサーバに保存されており，その提出期限が迫っている，などのケースもあった．そのため，これらのファイルに対して「どうしてもこのファイルだけファイルサーバから取り出して欲しい」という要望が利用者から寄せられ，インシデント対応のためにファイルサーバをネットワーク隔離している中，その都度やむを得ず対応せざるを得なかった．

3 分析

3.1 マルウェア

本インシデントで感染したマルウェアは，Gand-Crab と通称されている．[*2] これは，感染した端末と感染した端末からアクセス可能なサーバ上のファイルなどを暗号化し，暗号化したファイルを復元する方法を教えてほしければ仮想通貨 (Bitcoin) を支払うよう脅迫するランサムウェアである．本インシデントにおいて提示された脅迫状を図 2 に示す．

セキュリティ対策ベンダの分析[*3]によれば，暗号化鍵は，攻撃者が管理する C&C サーバに送信されており，復号化が可能とされている．しかし，本インシデント事例においては，以下の 2 点から，暗号化ではなく，単なるランダムバイト列への置換が行われたのではないかと思われる．第 1 に，ファイルサーバのアクセスログ (図 1) によると，ファイル名変更と書込のみが行われており，ファイルの読込が行われていない．暗号化を行うのであれば，ファイルサーバから原データを全て読み込み，そのバイト列を暗号化した上で，ファイルサーバに書き込む処理が必要のはずであるにも関わらず，ファイルの読込が記録されていないことは不自然である．また，少なくとも，ファイルをネットワーク経由で通信するための処理時間と，そのバイト列を暗号化するための時間が必要であるはずにも関わらず，32 分間に 205050 個ものファイルが書き換えられていた．これは，被害端末の性能を大幅に上回る処理速度であり，実際に暗号化しているとは考えにくい．第 2 に，感染発覚が早期だったため，被害端末を発信元とする学外への通信について，全ての履歴が全学 FW に残っていた．その履歴を検討したところ，不審なサイトへの通信は一切行われていなかった．以上より，本インシデントのマルウェアは，セキュリティ対策ベンダによる分析例とは異なり，暗号化ではなく，単なるランダムバイト列への置換を行ったと考える．

3.2 感染経路

マルウェア感染経路の調査において，今回感染したマルウェアが添付されたメールは，事務局の国際交流関係を扱う特定部署の代表メールアドレスにのみ送信されたことが判明した．本学で観測される多くのマルウェア添付メールは宛先に特定の傾向のないばらまき型であるが，それとは明らかに傾向が異なる．今後大学においても，日本国外を含む不特定多数と業務上やりとりをしなければならない部署においては，一般的なセキュリティ対策に加えて，特別な対策が今後必要となる可能性が高い．対策としては，例えば，アンチウイルスソフトに加えて振る舞い検知型アンチウイルスソフトや EDR（Endpoint Detection and Response）製品の導入などが考えられる．

3.3 情報漏洩の有無

2.3 節に述べた通り，メールサーバのログから，本インシデントのマルウェアの活動期間は，厳密に確定されている．そのため，ファイルサーバのアクセスログ (図 1) についても，厳密に解析が可能である．ファイルサーバのアクセスログによると，ファイル名変更と書込のみが行われており，ファイルの読込が行われていない．加えて，被害端末を発信元とする学外への通

[*2] https://www.virustotal.com/en/file/6205a88a2db20032773ca72de8866c0a4e05eea4212d42afd41fd30bded66a6a/analysis/1554427068/

[*3] https://www.fortinet.co.jp/blog/threat-research/gandcrab-honor-among-thieves.html

表 1　本インシデントの経過．日付はすべて 2019 年.

時刻		事象
4 月 3 日 (水)	05:07:47	攻撃メールが被害者のメールボックスに配送 (メールサーバのログにより確認)
	10:03:49	被害者がメールサーバに接続 (メールサーバのログにより確認)
	10:11:41	被害者が添付ファイル `Taxdocument.rar` を解凍 (被害端末上の添付ファイルのタイムスタンプにより確認)
	10:13:28	被害者のユーザ権限でファイル変更を開始 (ファイルサーバのアクセスログにより確認)
	10:40	「不審な拡張子のファイルが存在する」と一般職員から CSIRT 窓口に通報
	11:00	CSIRT 窓口から，CSIRT 教員にエスカレーション
	11:20	脅迫状 (図 2) を発見．CSIRT として，ランサムウェア感染疑いを認識
	11:21	事務局ファイルサーバをネットワークから物理的に遮断
	11:39	被害端末のネットワークを遮断
	11:52	被害端末にローカル管理者でログオン · 調査を開始
	12:00	ファイルサーバなどのログの収集 · 調査を開始
	14:00	被害者からの聞き取り調査
	18:39	証拠保全のため，事務局ファイルサーバをネットワークに再接続
	22:30	証拠保全のため，事務局ファイルサーバから暗号化されたファイル類のコピー開始
4 月 4 日 (木)	09:00	CSIRT 打合せ
	10:21	被害者のユーザプロファイルをアンチウイルスソフトでスキャンした結果，複数のマルウェアを発見
	11:40	ハッシュ値の照合から, 発見されたマルウェアの 1 つ (`documentTax.doc.exe`) が，本インシデントに強く関係すると判明
	12:00	CSIRT 打合せ
	15:00	証拠保全のファイルコピー完了
	17:26	被害端末 `C:\Users\alice\AppData\Local\Temp\` から，マルウェア `documentTax.doc.exe` が格納された圧縮ファイル `Taxdocument.rar` を発見
	17:34	圧縮ファイル `Taxdocument.rar` が添付されたメールを，被害者のメールボックスから発見．感染経路および活動期間など確定.
	17:50	活動期間中のファイルサーバのアクセスログを再調査．被害範囲を確定.
	18:00	スナップショット (2019 年 4 月 3 日 01:00 時点) に基づいて被害を受けたファイルの復旧を開始.
	18:18	活動期間中の被害端末から外部への通信について，ファイヤウォールのログを再調査．不審なホストへの接続がないことを確認.
4 月 5 日 (金)	04:50	スナップショットからのファイルの復旧が完了.
	09:20	事務シンクライアントシステムの運用を再開
	09:30	事務職員向け運用再開アナウンス

信についても，活動期間が厳密に確定されていれば，全学 FW のログを精査することが可能である[*4]．こちらの結果からも，不審なサイトへの通信は一切行われていなかった．以上より，本インシデントによる情報漏洩は無かったと考える．

このように，情報漏洩の有無の検討にあたっては，ファイルサーバのアクセスログは極めて重要である．本学では，事務用端末はシンクライアント化されており，全ての業務用ファイルと個人プロファイルは，ファイルサーバ上に保存されている．このような構成により，ファイルサーバの遮断によって事務局業務が完全に停止するという影響範囲の拡大という欠点もあったが，ファイルサーバのアクセスログにより情報漏洩の有無が集中的かつ迅速に検証できるという利点は非常に大きかった．

3.4 対応体制

本インシデントにおいては，不審な拡張子に気付いた一般職員による CSIRT 窓口への通報が，発見のきっかけとなっている．しかも，この通報が，感染開始から僅か 30 分後に行われたことは非常な幸運だった．これにより，初動対応 (2.2 節) 段階において，考慮しなければならない範囲をかなり狭く捉えることができた．したがって，一般職員に対する教育 (特に，CSIRT 窓口への通報を含む) は有効と考えられる．

CSIRT 担当教員 (2 名) が在勤中に発生したため，分担して迅速に対応を行うことができた．どちらかの教員が欠勤 (または出張) していた場合，または，深夜帯に発生していた場合には，特に初動対応に相当な遅延が発生したと思われる．どのようなインシデントや事故であっても，単独で対応することは困難であるから，担当教員の増員などバックアップ体制の充実が望まれる．

4 おわりに

本稿では，豊橋技術科学大学において発生したメール経由でのランサムウェア感染インシデント事例の詳細について述べた．本インシデントにあたっては，ファイルサーバのバックアップが安全に確保されていたこと，かつ，ファイルサーバ・メールサーバ・FW 装置のログから感染経路と影響範囲を厳密に確定できたこと，の 2 点により早期に復旧することができた．特に，ファイルサーバのアクセスログは，情報漏洩の有無を検討するにあたって重要である．

本インシデントの発生時には，メールサーバが学内に設置[*5]されていたため，被害者のメールボックスに転送された時刻や，被害者がメールサーバにアクセスした時刻など，感染被害の発生時点を厳密に確定できた．しかし，本学においても，2019 年 10 月にメールサーバをクラウドに移転したため，仮に今後同様の事例が発生した場合であっても，同様の調査を行うことはできない．クラウド移転後は，どのような対策を行うことが可能であるのかを検討しておく必要がある．

[*4] 2.2 節の段階では，活動期間が未確定のため，精査しきれなかった．

[*5] 正確には，学外の商用 DC に借用したラックスペースに設置．

```
1  "2019/04/03 10:13:28.105","AD\alice","fs","(fs_v1);\国際課\懇談会.pptx","WRITE","ClientIP
       :172.17.106.179    Count:1"
2  "2019/04/03 10:13:34.052","AD\alice","fs","(fs_v1);\国際課\懇談会.pptx","RENAME","ClientIP
       :172.17.106.179   Count:1 RenameTo:(fs_v1);\国際課\懇談会.pptx.islbirsu"
3  "2019/04/03 10:13:34.052","AD\alice","fs","(fs_v1);\国際課\懇談会.pptx.islbirsu","WRITE","
       ClientIP:172.17.106.179   Count:1"
4  "2019/04/03 10:13:34.210","AD\alice","fs","(fs_v1);\国際課\論点整理.xlsx","RENAME","
       ClientIP:172.17.106.179      Count:1 RenameTo:(fs_v1);\国際課\論点整理.xlsx.islbirsu"
5  "2019/04/03 10:13:34.210","AD\alice","fs","(fs_v1);\国際課\論点整理.xlsx.islbirsu","WRITE
       ","ClientIP:172.17.106.179      Count:1"
6  "2019/04/03 10:13:34.615","AD\alice","fs","(fs_v1);\国際課\事例紹介.pptx","RENAME","
       ClientIP:172.17.106.179        Count:1 RenameTo:(fs_v1);\国際課\事例紹介.pptx.islbirsu"
7  "2019/04/03 10:13:34.615","AD\alice","fs","(fs_v1);\国際課\事例紹介.pptx.islbirsu","WRITE
       ","ClientIP:172.17.106.179        Count:1"
8  "2019/04/03 10:13:34.635","AD\alice","fs","(fs_v1);\国際課\非常勤通勤手当.xls","RENAME","
       ClientIP:172.17.106.179 Count:1 RenameTo:(fs_v1);\国際課\非常勤通勤手当.xls.islbirsu"
9  "2019/04/03 10:13:34.635","AD\alice","fs","(fs_v1);\国際課\非常勤通勤手当.xls.islbirsu","
       WRITE","ClientIP:172.17.106.179 Count:1"
10 "2019/04/03 10:13:34.713","AD\alice","fs","(fs_v1);\国際課\通勤手当.xls","RENAME","ClientIP
       :172.17.106.179   Count:1 RenameTo:(fs_v1);\国際課\通勤手当.xls.islbirsu"
11 "2019/04/03 10:13:34.713","AD\alice","fs","(fs_v1);\国際課\通勤手当.xls.islbirsu","WRITE","
       ClientIP:172.17.106.179   Count:1"
12 "2019/04/03 10:13:34.728","AD\alice","fs","(fs_v1);\国際課\進行メモ.xlsx","RENAME","
       ClientIP:172.17.106.179  Count:1 RenameTo:(fs_v1);\国際課\進行メモ.xlsx.islbirsu"
13 "2019/04/03 10:13:34.728","AD\alice","fs","(fs_v1);\国際課\進行メモ.xlsx.islbirsu","WRITE
       ","ClientIP:172.17.106.179  Count:1"
```

図 1　ランサムウェアによるファイル書換ログ

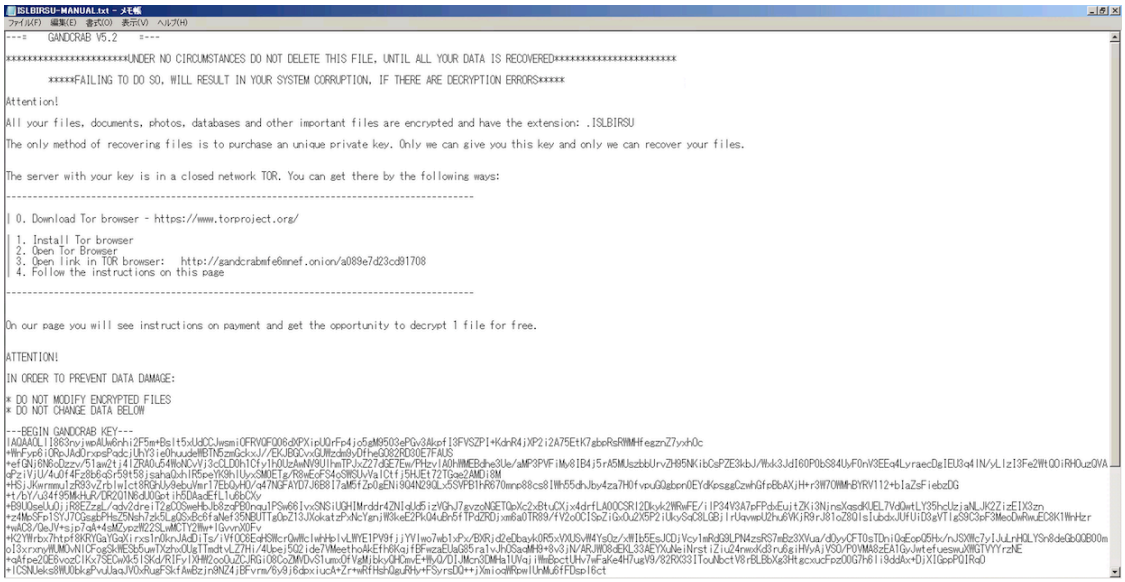

図 2　脅迫状