Vol.2020-IOT-50 No.5
2020/7/10

マーストリヒト大学で何が起こったか

一井信吾[1,2,a)]

概要：オランダのマーストリヒト大学で大規模マルウェア感染が発生し，重要サーバなどに大きな被害が発生した．大学は，授業再開のためにやむなく身代金支払いに応じた．公表された情報から知り得たことをまとめ，我が国の学術機関での教訓とする．

What happened at Maastricht University

Abstract: Massive malware infection happend at Maastricht University in Holland. We summarize what we have learned from the published information and learn lessons from academic institutions in Japan.

1. はじめに

マーストリヒト大学 [1], [2] はオランダにある教職員 4,500 人，学生数 18,000 人，卒業生 70,000 人を擁する国立大学である．1976 年創立という比較的新しい大学だが，PBL (Problem Based Learning) を取り入れた新しい教育，国際性（学生の 50%以上，教員の約 40%が国外から．授業はほぼ英語で行われる）によって知られ，各種のランキングで上位を獲得している．

このマーストリヒト大学で 2019 年末に大規模なランサムウェアの被害が発生した．直ちに外部機関によるインシデント対応が行われ，重要なサーバのファイルが暗号化されるなど甚大な被害が確認された．バックアップサーバも被害にあったため，理事会は年末に身代金支払いを決断した．その結果ファイルの復号化に成功し，2020 年 1 月初頭の授業開始を迎えることができた．大学は公開性・透明性の観点からインシデントを報告するシンポジウムを開催し，今後の対処方針等を議論した．

大学は Fox-IT[3][*1]にインシデント対応を依頼した．Fox-IT はオランダに拠点を持つ 1999 年設立の情報セキュリティ企業で，2015 年に NCC Group[4] の傘下に入っている．Fox-IT はこの案件をプロジェクト・フォンタナと命名し，ログ収集・分析，フォレンジック，被害認定，原因調査，再発防止策の提言などを行った．Fox-IT が大学に提出した報告書 [5] は公開され，インターネットでアクセス可能である．

本稿は，Fox-IT の報告書を含む公開情報をもとにインシデントの概要を報告するとともに，我が国の大学等機関において想定される事態と比較しつつ，情報セキュリティ対策のあるべき姿について議論する．

本稿の構成は以下のとおりである．

2. タイムライン

本インシデントに関するタイムラインの概略を示しておく．

2019 年 10 月 15 日・16 日　攻撃者のフィッシングメールが大学のネットワークに送付され，そのうち 2 通がこの両日に開封され攻撃者がシステムにアクセスできる状態になった．

10 月 16 日から 12 月 23 日　攻撃者が複数のサーバを侵害した．

11 月 21 日　攻撃者は，セキュリティ更新が欠落しているサーバーを介して，クライアントのインフラストラクチャ内で完全な権限を取得することに成功した．

12 月 23 日　攻撃者は 267 台の Windows サーバーでいわゆる Clop ランサムウェアを展開した．

1 高エネルギー加速器研究機構　計算科学センター
Computing Research Center, High Energy Accelerator Research Organization (KEK)
2 総合研究大学院大学　高エネルギー加速器科学研究科
School of High Energy Accelerator Science, The Graduate University for Advanced Studies (SOKENDAI)
a) shingo.ichii@kek.jp

*1 Web サイトや報告書表紙は社名を FOX IT としているが，本稿では報告書本文に従い Fox-IT と記載する．

ⓒ 2020 Information Processing Society of Japan

12 月 24 日　大学が Fox-IT にインシデント対応を依頼した．

12 月 30 日　大学が身代金支払を決定し，Fox-IT に通知した．

2020 年 1 月 2 日　主要な教育用システムが復旧した．

2 月 5 日　大学がインシデント報告シンポジウムを開催した．

3. インシデント報告書

Fox-IT がマーストリヒト大学に提供し，大学が一般に公開したインシデント報告書 [5][*2] より，インシデントの概要を紹介する．報告書は 38 ページであり，以下の章から構成されている．

1. はじめに
2. マーストリヒト大学の紹介
3. 証拠
4. 対処方針
5. 調査結果
6. 結論
7. 勧告

付録

図 1　Fox-IT によるプロジェクト・フォンタナ報告書の表紙
Fig. 1　Cover page of the report of the Project Fontana by Fox-IT

報告書には調査内容が相当に詳細に記載されているが，公開版からはホスト名，ユーザ名など一部の情報は削除されている．なお，報告書はオランダ語で記載されているため，参考のためかなり詳細に紹介するが，翻訳の誤り等による誤解がないとは言えないので詳しくは原文を参照されたい．

3.1 調査開始

大学の IT セキュリティチームは被害が発見された 12 月 23 日夜に Fox-IT の CERT に連絡した．この時点で，既に数台のサーバーがランサムウェアの被害を受け到達不能となっていた．翌 24 日正午頃にはオンサイトでの対応が必要との判断に至り，同日 16 時に Fox-IT のインシデント対応チームが到着して危機管理プロセスの支援に入った．

大学側は Fox-IT について次の問いに答えるよう求めた．

- インシデントの状況はどのようなものか
- インシデントの原因は何であったか
- インシデントの規模はどれほどか
- 攻撃者はどのデータにアクセスしたか
- 重要情報の漏洩・盗難はあったか

Fox-IT からは調査の中で以下の事項にも答えることとされた．

- 危機対応組織の設立と起動についてのアドバイス
- 被害緩和，修復のためのアドバイス

3.2 システム構成

マーストリヒト大学の IT インフラストラクチャの一部は，ICTS (IT Service Centre) が管理している．ただし，他の部局が管理しているサーバ等も存在する．全台数の正確な値は不明である．全学で用いられている Windows ドメインは UNIMAAS である．ICTS はシンクライアント等に対し VDI (Virtual Desktop Infrastructure) を提供している．

3.3 証拠

Fox-IT の調査には以下のデータが用いられた．

ログデータ　2019 年 9 月から 12 月までの DNS クエリー，ドメインコントローラの Windows イベントログ，ファイルサーバの Windows イベントログ．これらは Splunk で管理されていた．

システムデータ　ファイルサーバ，ドメインコントローラ，シラバスサーバ等のディスクイメージ，メモリイメージ等

*2 このリンクからダウンロードできる PDF ファイルには，Fox-IT が提出した報告書に加え，これに対する大学からの応答及び 2020 年 2 月 5 日に開催されたシンポジウムでの Nick Bos 副学長の発言内容も記載されている．

ⓒ 2020 Information Processing Society of Japan

ネットワークデータ　ファイアウォールで取得した 2019 年 7 月 3 日から 12 月 25 日までのフローデータ

その他のデータ　最初に侵害された（仮想）PC のディスクイメージ，暗号化されたファイル，マルウェア，データベース，マルウェアを開封したアカウントのメールボックスなど

3.4　対処方針

タイムラインで示したように，2019 年 12 月 24 日に Fox-IT のインシデント対応チームが現地に到着した．Fox-IT のチームがまず行ったのは危機管理チームの結成支援である．このチームは，図 2 に示すように，対応に必要な関係者を一同に会させ，効率的に行動できるようにするためのものである．Fox-IT はここにコミュニケーション専門家を加えることが極めて重要であると指摘した．インシデント対応が始まれば必ず公になるためであり，大学のような公共機関であれば透明性が重要であるから尚更であるとした．法務部門の参加，また事務部門 (business) 及び IT 部門と IT セキュリティ部門がインシデントのインパクトを適切に示すことが重要であるとしている．

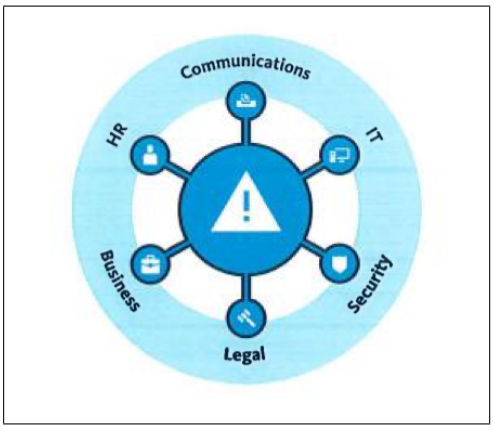

図 2　危機管理チームの構成
Fig. 2　Organization of the Crisis Management Team

3.4.1　被害の把握

調査の結果判明した被害は，アカウント 5，Windows システム 269（サーバ総数 1,647，クライアント総数 7,307）であった．Linux や macOS システムは被害がなかった．

3.4.2　対処システムの配備

インシデント対応開始当初，マルウェアは依然活動中であったので，ネットワーク上にセンサーを配置して異常トラフィックの監視を行った．インターネットとの通信を監視するもの，内部トラフィックを監視するものの合計 3 台を設置した．後者はいわゆるラテラルムーブメント（水平移動）を検知するためのものである．

Windows システムの防御のため，エンドポイントセキュリティ製品 Carbon Black Response を導入した．端末の導入するセンサーは 4 週間で 8,873 台に導入された（VDI 仮想デスクトップを含む）．将来的には，90%以上の Windows システムへの導入を目指す．

3.4.3　フォレンジック調査

レポート作成時点で 324 システムのディスクイメージとログファイルが収集され，解析に付されている．大学は早期の操業再開を優先したいとしていたため，フォレンジック調査のためのデータ保存を急ぐ必要があった．

3.4.4　復旧作業

大学は 1 月初めまでの復旧を望んでいた．実際に行ったことは以下の通り．

- 12 月 24 日に全学のインターネットとの接続を遮断した．
- 12 月 26 日に，復旧作業に必要なシステムのインターネット接続を，ネットワーク監視と IP アドレス制限の元で復旧した．

また Fox-IT は以下の事項をアドバイスまたは推奨した

- eduroam からの学内ネットワークへのアクセスを制限すること．
- 関連する IoC についてのファイアウォールでの監視を強化すること．
- UNIMAAS ドメインの全アカウントのパスワード変更．
- 被害を受けたシステムの復旧手順．
- 重要情報のリストを作り復旧の順序づけをすること．
- 安全と判定されたシステムを復帰する際には Carbon Black を導入すること．Carbon Black でのモニターを強化すること．

3.5　わかったこと

これまでの解析で判明した事項を示す．時刻は UTC である．

3.5.1　初期侵入

2019 年 10 月 15 日 14:06:31 にフィッシングメールを大学のあるアカウントが受信した．本文は英語で書かれ，外部サイト[*3]へのリンクが貼られていた．

このリンクをクリックすると Excel ファイルがダウンロードされ，同日 14:55:27 にユーザが開封した．この Excel ファイルにはマクロが含まれていて，外部サーバから SDBBot と呼ばれるマルウェアがダウンロードされた．

翌 16 日 09:07:51 に 5 つのアカウントに前日とは異なっ

[*3] このサイトの VirusTotal での評価は 7/72 が悪性だった（2020 年 6 月 15 日に確認）．

たサブジェクト行とリンク[*4]を含むフィッシングメールが送信され，1 人のユーザが 12:52:28 に開封した．上記と同様の Excel ファイルがダウンロードされ，やはり SDBBot がダウンロードされた．

これらの SDBBot は 15 分ごとに外部の C2 サーバと通信していた．また，Windows システムレジストリに登録され，再起動後も動作するよう設定されていた．

このようにして，攻撃者が学内ネットワークへのアクセスを確立した．

3.6 ネットワークでの拡散

2019 年 10 月 16 日から 12 月 23 日までの間，攻撃者は断続的に行動を起こし，初期侵入を受けた PC からネットワーク上の他のマシンに侵入を広げていった．いくつかの重要なイベントについて記載する．

3.6.1 攻撃者の最初のマニュアル活動

2019 年 10 月 16 日 19:35:03 に SDBBot が別のマルウェア Meterpreter を起動させた．このマルウェアは攻撃者がマニュアルで操作を行うためのものである．

10 月 17 日には初めてのサーバへの侵入（2 台）を行っている．17:33:22 にマルウェア Meterpreter が送り込まれ，17:40:33 にはこれが起動されている．どのようにしてサーバへの侵入が行われたかは判明していないが，EternalBlue 攻撃が行われた可能性がある．サーバの OS は Windows Server 2003 R2 であり，パッチ MS17-0104 が未適用であった．このパッチが適用されていれば EternalBlue には影響されない．

他の 2 台のサーバも 10 月 20 日 19:00:33 と 19:02:45 に Meterpreter に感染させられた．これらは Windows Server 2012 R2 が動作していたが，うち 1 台は EternalBlue 攻撃に対し脆弱な状態だった．しかし他の 1 台はそうではなく，感染経路は不明である．

以上 4 台のサーバを攻略したのち，攻撃者は再び最初のワークステーションに戻って，PowerSploit を用いてネットワークをスキャンしたり，PingCastle を用いて Actige Directory の構造を把握したりすることで脆弱なシステムをさらに探した．

学内ネットワークはセグメント分割が十分には行われていなかったため，攻撃者はネットワーク内を自由に行動することができた．

3.6.2 攻撃者がドメイン管理者の特権を獲得

11 月 21 日に，攻撃者は仮想デスクトップ上のユーザアカウントを利用して活動を再開した．

13:06:22 仮想デスクトップからあるサーバへ接続

13:07:46 同サーバ上で Meterpreter 動作，管理者権限奪取

13:19:53 攻撃者がドメインコントローラに Administrator アカウントでログオン

ドメインコントローラに Administrator アカウントとでログオンできた理由は特定されていない．それまでに侵入されたサーバのいずれかのメモリ上にログイン情報が残っていた可能性がある．

12 月 19 日 14:49:25 にはドメインコントローラ上で AdFind を動作させた．これは Active Directory で管理されるサーバとワークステーション上のプロセスを制御できるツールである．

このようにして大学のドメイン管理者特権が奪取され，この後 Active Directory で管理されている全てのシステムが攻撃可能となった．

3.6.3 ランサムウェアの準備と配布

攻撃者は攻撃の最終段階であるランサムウェア配布を 12 月 23 日 17:52:42 から開始した．

このために，攻撃者は sage.exe というプログラムを用意し，12 月 23 日 17:53:52 より 4 台のサーバに配置した．一つのサーバ上では McAfee アンチウイルスソフトウェアがこれを検知して削除した．攻撃者はこれを知るとそのサーバに Administrator としてログオンし McAfree アンチウイルスソフトウェアをアンインストールして sage.exe を再配置した．攻撃者は他のサーバのうち 2 台からも McAfee を削除した．

18:26:51 に攻撃者は sage.exe を配置した 3 台のサーバからランサムウェア攻撃を開始した．sage.exe は実際のランサムウェアの名前やそれを起動するためのパラメータなどを引数として与えて起動される．ドメイン管理者のアカウントで，攻撃者は UNIMAAS ドメインの全てのサーバで sage.exe を使ってランサムウェアを起動させた．

18:52:34 ころまでに少なくとも 267 のサーバがランサムウェアの攻撃を受け，ほとんど全てのファイルを暗号化された．被害を受けたサーバの中には，ドメインコントローラ，Exchange サーバ，研究・管理情報を保管するファイルサーバ，バックアップサーバの一部など組織運営上重要なものも含まれていた．バックアップサーバも UNIMAAS ドメインに属し，ネットワークレベルのセグメンテーションも行われていなかったため，攻撃者によって暗号化の被害を受ける結果となった．

3.6.4 使用されたランサムウェアについて

攻撃者が使用したランサムウェアは Clop と呼ばれるもので，RC4 で暗号化した後暗号化キーを 1024 ビット RSA 公開鍵暗号で暗号化していた．この暗号は攻撃者のみが復号できる．暗号化されたファイルはファイル名に.CIop（大文字 I）が加えられた．被害を受けたフォルダには CIopReadMe.txt というファイル (図 3) が置かれた．

[*4] このサイトの VirusTotal での評価は 4/71 が悪性だった（上と同日に確認）．

```
*-*ALL FILES ON EACH HOST IN THE NETWORK HAVE BEEN ENCRYPTED WITH A STRONG ALGORITHM*-*

-Backups were either encrypted or deleted or backup disks were formatted.
-Shadow copies also removed, so F8 or any other methods may damage encrypted data but not
recover.
-If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 3-5 encrypted files
-(Less than 6 Mb each, non-archived and your files should not contain valuable information
-(Databases, backups, large excel sheets, etc.)).
-You will receive decrypted samples.

-MESSAGE THIS INFORMATION TO COMPANY'S CEO, UNLOCKING OF 1 COMPUTER ONLY IS IMPOSSIBLE, ONLY
WHOLE NETWORK.
-ATTENTION-
-Your warranty - decrypted samples.
-Do not rename encrypted files.
-Do not try to decrypt your data using third party software.
-We don`t need your files and your information.

:::CONTACT EMAIL:::

AND

or


NOTHING PERSONAL IS A BUSINESS
PLEASE DO NOT USE GMAIL, MAIL DOES NOT REACH OR GETS INTO THE SPAM FOLDER.
PLEASE CHECK SPAM FOLDER!!! CLOP^_-
```

図 3 被害を受けたフォルダに置かれていた CIopReadMe.txt
Fig. 3 CIopReadMe.txt file which was placed in the attacked folder

3.6.5 攻撃者の活動の検知

ログから発見された攻撃者の活動の形跡を示す．これらのログはログサーバに送られていたが，大学が発見できていなかった．

10 月 24 日 攻撃者が PowerSploit を用いて内部ネットワークを調査し始めたとき，Windows Defender がスクリプトの一つ PowerView を発見して削除していた．

12 月 19 日 攻撃者がサーバ上で行動を開始した際，McAfree Enterprise Endpoint Security が Cobalt Strike と Mimikatz を検出していたが，Observer モードになっていたため（デフォルト設定）Windows イベントログに出力するのみでブロックはしなかった．

12 月 23 日 攻撃者がランサムウェア配布の準備を始めた際，サーバ上の McAfree アンチウイルスソフトウェアが sage.exe を検出し削除していた（上述）．

3.7 攻撃者について

Fox-IT はこの攻撃者は TA505 または GraceRAT と呼ばれるものであろうと考えている．このグループは最近では 2019 年 2 月からランサムウェア Clop を用いてマイクロソフト Windows ドメインを用いている組織を攻撃している．2019 年に 150 以上の被害が発生している．このグループの行動は基本的に同じで以下の通りである．

1) ばらまき型フィッシングメールによるシステムの感染
2) 感染した組織の特定
3) ネットワーク中の水平移動
4) バックアップを消去または暗号化
5) ランサムウェアを可能な限り多くのシステムに展開
6) 電子メールによる身代金要求（金額は組織の大きさに依存）

3.8 重要情報

大学は重要情報（クラウンジュエル）として 3 件を指定した．そのうち 2 件に関しては，既知の IoC に照らす限りランサムウェアによる暗号化被害以外の改竄・漏洩等の被害は確認されていない．ただし既知の IoC に頼らない，より詳細な調査が必要である．残り 1 件（学務情報か?）に関しては，データが膨大なため Fox-IT でのフォレンジック調査が行えていない．今後現地での調査が必要である．

3.9 結論

与えられた問いに対する回答は以下の通りである．

インシデントの状況はどのようなものか 2 件のフィッシングメールにより内部ネットワークへの侵入を許した．その後，水平移動が行われた．

インシデントの原因は何であったか セキュリティパッチの適用が不十分であったこと，ネットワークのセグメンテーションが限定的であったこと，複数のアラートシグナルに対応できなかったことから，攻撃者は自由にネットワーク内で行動できた．その後，重要なサーバにランサムウェアが仕掛けられてしまった．

インシデントの規模はどれほどか 主に中央管理されている 267 の Windows システムが被害を受けた．その中には，組織にとって重要なドメインコントローラ，Exchange サーバ，ファイルサーバ，バックアップサーバが含まれていた．

攻撃者はどのデータにアクセスしたか フォレンジック調査の結果によれば，攻撃者の目的は広範なランサムウェアの展開にあったと言える．攻撃者によって，18 のサーバと 5 つのアカウントが乗っ取られた．これを起点に，ネットワークに広範な攻撃が行われた．これまでの限定的な調査による限り，ネットワークトポロジ，上記サーバのユーザ名・パスワード等の情報以外の情報漏洩被害は確認されていない．

重要情報の漏洩・盗難はあったか これまでの調査の範囲では，重要情報（クラウンジュエル）の漏洩・盗難被害は確認されていない．ただし，重要情報を扱っている 5 台のサーバのうち 3 台では攻撃者の行動が確認されているので，今後より詳細な調査が必要である．

3.10 勧告

再発防止策として 3 点（予防，検知，対応）と，フォロー

アップについての勧告がある．

- 予防

職員のセキュリティ意識向上　フィッシングメール対策を含む職員のセキュリティ意識向上プログラムを実施すること．

ドメイン管理者アカウントで無関係な作業を行わない　ドメイン管理者アカウントで，ドメイン管理以外の作業が行われていた形跡がある．このため，他システムのパスワード等の情報がドメイン管理者アカウントに残されており，被害拡大につながった可能性がある．「最小特権の原則」を適用せよ．

マクロ　Office 文書における（認証済以外の）マクロ自動実行を禁止すべき．

Protected Users セキュリティグループの利用　Windows Server 2012 R2 で導入された Protected Users セキュリティグループの機能を利用し，特権ユーザの資格情報を保護するべき．

OS のアップデート　本インシデントでは，EternalBlue 脆弱性が悪用された可能性がある．パッチを適用し，OS を最新の状態に保つこと．

- 検知

ネットワーク監視　本インシデントが発生するまで，継続的なネットワーク監視が行われていなかった．内外のトラフィックについての監視を実施すべき．

ログファイルの異常監視　発覚する数ヶ月前から，複数のサーバが侵害されていた．ログファイルの'high risk' 等のラベルに注意し，異常監視を行うべき．

- 対応

構成管理情報データベース　一元管理された構成管理情報データベース (CMDB: Configuration Management Database) を整備すべき．

インシデント対応計画　インシデント対応計画が策定されていなかった．計画を策定し，見直し及び定期的なテストを行うべき．

データ回復計画　データ回復計画が策定されていなかった．また，オフラインのバックアップが行われていなかった．計画を策定し，定期的にテストすべき．

- フォローアップ

重要情報（クラウンジュエル）に関する調査は不十分であり，継続調査を行う必要がある．

4. 大学からの応答

前節で紹介した Fox-IT の報告書の内容を受けて，マーストリヒト大学は「マーストリヒト大学の Fox-IT 報告書への応答」と題する文書[*5]を公表した．この文書は「報告書に示された知見と勧告のいくつかに対して、事実を損なうことなく追加、説明及びコメントを行う」ものとされている．主な記載事項は以下の通りである．

ランサムウェア攻撃　2019 年 12 月 23 日に攻撃が判明して以来、大学は復旧作業と同時に、できるだけ早く教育研究を再開することを目指して取り組んできた．その際、公開性、透明性を重視し、大学の Web サイトにおいて可能な限り詳細に対処プロセスを示してきた. [*6]

報告書の結論とフォローアップ　Fox-IT の報告書の内容は信頼している．しかし、未だ調査が及んでいない事柄もあるため、大学自らが内部調査を進める．勧告及び今後の調査結果に基づき、セキュリティポリシーの見直しと既存計画の修正・拡張を行う．

教訓　現時点で言える教訓として以下の諸点を挙げる．

1. フィッシングメール（及びその報告）の取り扱いの向上
2. 技術的対策
   - ソフトウェアアップデートの的確な実施
   - Windows ドメインのセグメント化
   - SIEM, SOC を整備し常時監視実施
   - 構成管理データベースの整備
3. 二重バックアップ

研究データについてのフォローアップ　重要情報の一つとしての研究教育データについては十分な調査ができなかった．今後、Fox-IT に引き続き調査を依頼するとともに、大学においても調査を継続する．

5. シンポジウム

2020 年 2 月 5 日に、マーストリヒト大学は本インシデントについて報告するシンポジウム[*7] を開催した．

シンポジウムで Nick Bos 副学長が行った講演の内容が公開されている [5], [6] ので、その内容を紹介する．

1. サイバーセキュリティは社会の重大問題であり、オランダ国内でも繰り返し指摘されている．

2. 高等教育機関[*8]も例外ではないばかりか、セキュリティと公開性・透明性の両立を図らなければならない

*5 この文書のオランダ語原文は Fox-IT 報告書 [5] と同じ PDF ファイルに含まれている．また、英語版 [6] も公開されている．本稿での紹介は主として英語版に基づく．
*6 Web ページ (Updates Cyberattack[7]) に記録がある．
*7 "Updates Cyberattack" のページ [7] に録画がある（ただしオランダ語）．本稿で紹介している各文書 [5], [6] へのリンクもこのページにある．
*8 示されたインシデント例に同時期にランサムウェアの被害を受けたギーセン大学 [8] も含まれている．

点で一層の困難を抱えている．

3. マーストリヒト大学にも日常的に極めて多数のサイバー攻撃が行われており、そのほとんどを防いできている．

4. しかし 2019 年 10 月 15 日には、人という弱点をつかれてしまった．12 月 23 日、この日は大学の集団的記憶に永久に残るであろうが、その日に行われた攻撃以降、多くの職員がクリスマス休暇を返上して対処に当たった．理事会の関心は何よりも教育の継続にあった．どうすれば 1 月 6 日の授業開始に間に合わせることが可能だろうか？どうすれば入学試験を予定通り実施できるだろうか？

5. 身代金支払が最大の問題だった．各方面と連絡を取り、長時間にわたって議論した．その結果、12 月 29 日に、身代金支払の決定をした．犯罪者に支払いをすべきでないという原則と、長期にわたるシステム停止が教育研究に与える悪影響を比較して下した結論である．簡単な決断ではなかった．結果、1 月 6 日に授業開始でき、大学運営も可能となった．正しい決断だったと、自信を持っている．

6. 大学は自らの行動に責任を持ち、以下のことを実行する．サイバーセキュリティ対策を向上し続けること．知見を他の大学等と共有すること．より広い範囲の議論と協力のため経験を役立てること．

7. サイバーセキュリティ対策の一層の向上を図らなければならない．大学間連携での常時監視の検討が始まっている．マーストリヒト大学にも CERT, SOC を設置した（2020 年 1 月 1 日発足）．サイバーセキュリティ対策へのより多くの投資が必要．

8. サイバーセキュリティは社会全体の問題であり、どのように扱うべきかは広く議論しなければならない．

6. 考察

本インシデントに関わるマーストリヒト大学の状況・対応のうち、我が国の大学等の機関において想定されるものと比較して興味あると思われる幾つかの点について議論する．

6.1 外部機関の導入

マーストリヒト大学は、12 月 23 日にランサムウェア被害を確認したが、その日のうちに Fox-IT CERT と連絡を取り、助言を受けている．翌日には、オンサイトでの対応が必要との判断をし、16 時に Fox-IT 担当者が大学に到着して対処を開始している．緊急時の対応についてあらかじめ関係構築が行われていたものと想定される．この時点で大学に CERT や SOC が存在していなかった[*9]ためでもあるが、早期に外部専門家の支援を受ける体制を構築しておくことの有効性が示されている．報告書では、重要情報（クラウンジュエル）を含めシステムの隅々まで Fox-IT が調査したことが述べられている．契約で責任範囲や機密保持を厳格に取り決めるだけでなく、日頃から信頼関係構築を行っておくことが必要であろう．

6.2 公開性・透明性

大学からのメッセージにおいては、公開性・透明性が繰り返し強調されている．それはサイバーセキュリティ対策が困難であることの理由ともなるが、インシデント対応にあたってその過程を隠さず情報提供していくことにも現れている．

ギーセン大学の事例 [8] においては、対処の過程で仮設公式 Web サイトにおいて重要情報が提示されていたが、マーストリヒト大学ではさらに進んで、攻撃が認知された翌日の 12 月 24 日から 1 月 24 日までほぼ毎日新たな情報が Web サイトで公開された．この記載を見ると、危機管理チームの立ち上がりは素早く、的確な対処を行うとともに適切なメッセージを発出していることが確認される．今日、大規模インシデントを大学のような開放的な機関において秘密裏に処理することは全く不可能である．そうであればこそ、正確な情報を適切かつ積極的に提示していくことは極めて重要である．

残念ながら我が国ではインシデント対処や復旧より責任追及が先行したり、被害者がかえって攻撃の対象となったりする傾向があるため、情報開示に慎重にならざるを得ない面があることは否定できない．しかしそのことによって適切な対処が行えなかったり、不正確な情報が SNS 等で拡散するなど制御不能な状況が発生する可能性も高いため、高い立場から適切に判断実行する必要がある．

またマーストリヒト大学は Fox-IT が提出した報告書をほぼそのまま公開するとともに、報告と議論のためのシンポジウムを開催した．シンポジウムの録画やその様子を撮影した写真を見ると、メディアも参加していることがわかる．これも、大学の公開性・透明性重視の表れである．Nick Bos 副学長の講演にあるように、インシデントに関する情報や知見を共有し協力して対処することが必要であり、オープンに議論できる場を構築していくことが望ましい．

6.3 身代金支払の決定

同様に 2019 年 12 月にランサムウェア被害にあったギーセン大学 [8] が長期間の全学シャットダウンを敢えてして

*9 第 5 節で紹介した Nick Bos 副学長の講演中で CERT, SOC 設立準備はすでに行われていたこと、2020 年 1 月 1 日に発足したことが述べられている．

自力での復旧を行ったのに対し、マーストリヒト大学は身代金支払を選択した．Nick Bos 副学長の講演にあったように、これは決して簡単な決断ではなかったと考えられるが、被害の実情や大学運営における IT の重要性などを考えると異なった決定に到ることも十分想定できる．ギーセン大学では、メールサーバは暗号化の被害を受けたが、主要なファイルサーバは無事だったと伝えられている．また、マーストリヒト大学は先進的な教育システムをその強みとしており、教育において IT の重要性がより高いと判断された可能性もある．いずれにせよ、被害発生後約 1 週間でこの決定に至っていることは、効率的な意思決定プロセスの存在を窺わせるものである．

ランサムウェア被害にあたって身代金を支払うことの是非については様々な議論があるが、現在に到るまで決定的な結論は得られていない．一例として、FBI は 2016 年には身代金の支払を支持 (support) しないと明言していた [9] が、2019 年に出された文書 [10] では引き続き支払を擁護 (advocate) しないとしながらも、支払を行う場合も想定した記載を含む段落が追加されている．

その背景には、ランサムウェア攻撃を行う側が完全に金銭目的となったため、身代金支払を継続的に実現するためには支払った場合確実に復号することが攻撃者にとって必要だという事情もある．図 3 に示す攻撃者が残したファイルには、3 ～ 5 個の暗号化ファイルを送れば実際に復号可能であることを示すという文言が見える．2017 年に世界的に感染拡大したランサムウェア WannaCry では、支払をしたとしても支払者と被害者を紐づけることができず、バグもあったため復号はできないとされた [11] が，状況は変わってきている．なお，Sophos が 2020 年 1 月から 2 月にかけて行った調査 [12] によれば、被害を受けた企業のうち約 26%は身代金を支払ったとされ、被害平均額は 140 万ドルだという．ただし、バックアップから自力で復旧した企業の方が費用も回復率も高いとしている．

7. まとめ

2019 年 12 月にマーストリヒト大学で発生したランサムウェア被害について、大学が公表した報告書及びそれに対する大学の応答によって紹介した．また、その中で我が国の大学等の機関において想定される事態と比較して注意を引く事項について検討した．

本インシデントの発端は、職員が悪意あるマクロを含んだ Excel ファイルを実行してしまったことにあるが、ここまでの大きな被害につながった背景には大学のネットワーク設計やサーバ運用に存在した問題があったと言わざるを得ない．重要なサーバを含む大学全域にわたって一つの Windows ドメインで運用していたこと、ネットワークが適切にセグメント化されておらず攻撃者が容易に水平移動できたこと、サーバの OS アップデートが行われていなかったこと、ログの監視を適切に行っておらず危険な兆候を見落としていたこと、これらはどのひとつをとっても重大な問題である．CERT, SOC 設置準備が行われていたことを見ても、おそらくはマーストリヒト大学もこのような問題を放置していたわけではないのであろうが、残念ながら準備が整う前に攻撃を受けてしまった．システム・ネットワーク管理者、情報セキュリティ担当者は、攻撃者は準備が整うのを待ってはくれないことを肝に銘じて、必要な対処を迅速に行わなければならない．

一方、一旦被害が発覚してからのマーストリヒト大学の行動は迅速かつ的確で、大いに参考にされるべきである．特に、情報公開への姿勢については、我が国とは社会環境が異なることが想定されるとはいえ、見習うべき点が多い．我が国においても、サイバーセキュリティについて被害や対策を含めてオープンに議論し、社会全体として効果的に対処していけるようになることを願ってやまない．

参考文献

[1] マーストリヒト大学公式 Web サイト．https://www.maastrichtuniversity.nl[*10]
[2] Wikipedia, マーストリヒト大学
[3] Fox-IT Web サイト. https://www.fox-it.com/en/
[4] NCC Group Web サイト. https://nccgroupplc.com/
[5] Fox-IT report, with an explanation from UM in Dutch. https://www.maastrichtuniversity.nl/file/foxitrapportreactieuniversiteitmaastrichtnl10-02pdf
[6] Response of Maastricht University to FOX-IT report. https://www.maastrichtuniversity.nl/file/reponseofmaastrichtuniversitytofox-itreportpdf
[7] Updates Cyberattack. https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-^^e2^^80^^93-lessons-learnt
[8] 一井信吾: ギーセン大学で何が起きたのか. 情報処理学会研究報告インターネットと運用技術 (IOT) , 2020-IOT-48, pp. 1-8. (2020).
[9] FBI: Public Service Annoucement, “Ransomware Victims Urged to Report Infections to Federal Law Enforcement,” September 15, 2016. https://www.ic3.gov/media/2016/160915.aspx
[10] FBI: Public Service Annoucement, “High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations,” October 02, 2019. https://www.ic3.gov/media/2019/191002.aspx
[11] Check Point: “WannaCry – Paid Time Off?,” https://blog.checkpoint.com/2017/05/14/wannacry-paid-time-off/
[12] Sophos: “THE STATE OF RANSOMWARE 2020,” https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

[*10] URL の最終確認日: 2020 年 6 月 16 日（以下同じ）