Vol.2020-IOT-48 No.21
2020/3/3

ギーセン大学で何が起きたのか

一井信吾[1,2,a)]

概要：ドイツのギーセン大学で大規模マルウェア感染が発生し，1 ヶ月以上にわたって学内ネットワーク，サーバ等が一切使用停止になった．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 JLU Giessen

Abstract: Massive malware infection at Giessen University in Germany happened. The use of the campus network and servers has been suspended for over a month. We summarize what we have learned from the published information and learn lessons from academic institutions in Japan.

1. はじめに

ギーセン大学[*1]はドイツ南部のヘッセン州ギーセンにある 1607 年設立の由緒ある大学である．学生 25,000 以上，教職員 4,500 以上を擁するドイツでも有数の大学である [1]．ヘッセン州は，州都はヴィースバーデン，フランクフルトがあることで知られる．ギーセンはヘッセン州の中央あたりにあり，近隣のマールブルクにはマールブルク大学がある．

この大学で大規模マルウェア感染が発生し，2019 年 12 月 8 日から 1 ヶ月以上にわたって学内ネットワーク，サーバ等が一切使用停止になった．調査の結果，Emotet によるランサムウェア Ryuk 感染による被害と発表された．ドイツでは，同時期にフランクフルト市をはじめ多数の機関での感染が報じられており，ギーセン大学についても各種メディアが取り上げる事態となった．本稿では，公表された情報から知り得たことをまとめるとともに，我が国の学術機関で広く参照されている高等教育機関のためのサンプル規定集におけるインシデント対応手順を参考に，日本の大学はこのような大規模インシデントにどのように対応できるか検討する．

2. タイムライン

主に公式ホームページ [2] での発表に基づき，進行した事態の推移をまとめる．

2019 年 12 月 8 日（日） 未知のマルウェアによる攻撃を受けていることを発表．インターネット接続，電子メール，内部ネットワークを停止．教職員の Windows PC は感染している恐れがあるが，学生には被害が及んでいないとされている．代替 Web サイト（図 1）をマールブルク大学において立ち上げ[*2]．

12 月 9 日（月） サイバー攻撃の被害届提出．ドイツ国内のニュースサイト等に報道が出始める（図 2）．

12 月 10 日（火） 外部専門家（Darmstädter Forschungszentrum für Cybersicherheit ATHENE: ダルムシュタットサイバーセキュリティ研究センター ATHENE）を招聘，内部向け説明会開催．

12 月 13 日（金） 全教職員の Windows マシンを 2 つのウイルス検査ソフトで検査する（学生は対象外）．1 種目の USB メモリでの配布開始．2 種目は来週に予定．検出されなかった PC には緑のステッカーを貼る．2 つそろってはじめてネットワーク接続を許可する．

12 月 16 日（月） e-mail アカウントのパスワードリセット（38,000 件）．新しいパスワードは身分証提示の上ジ

[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] 正式名称は Justus-Liebig-Universität Gießen であり，ドイツでは JLU ないし JLU Gießen と略されることもある．本稿では通称をとりギーセン大学とする．

[*2] 最初に感染被害が確認された日時やその詳細は公表されていない．

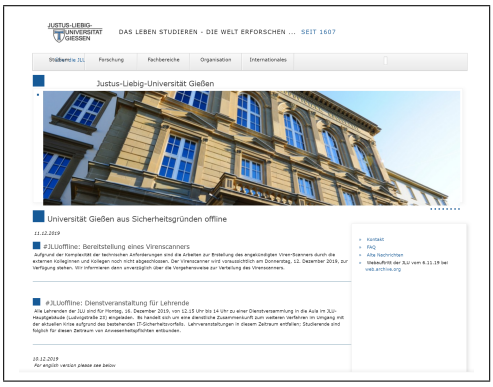

図 1 2019 年 12 月 11 日における大学公式ページ [2]．マールブルク大学において立ち上げられた代替 Web ページである．「ギーセン大学はセキュリティ上の理由でオフライン」と書かれている．通常のコンテンツではなく，事態への対応に必要な情報に限った内容が掲載されている．

Fig. 1 The official Web page of JLU as of Dec. 11, 2019. This is a substitute Web site at Marburg University. It states, "Giessen University is offline due to security reason." The contents which are necessary to deal with the situation are posted, instead of the usual ones.

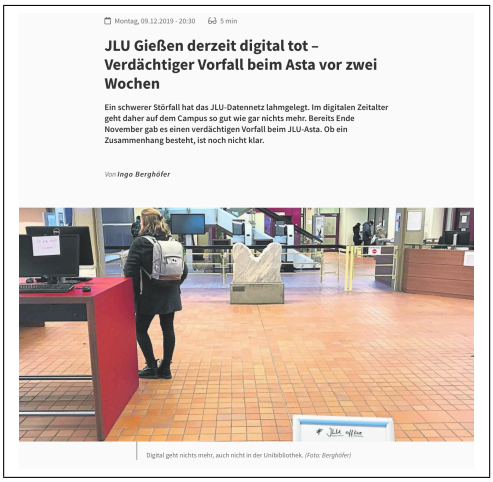

図 2 全学がオフラインになっていることを伝える地元ニュースサイト [3] の記事．写真下部の掲示板に#JLUOffline のハッシュタグが書かれているのが見える．

Fig. 2 An article of a local news site that tells Uni Giessen is offline. The hashtag #JLUOffline is written on the message board at the bottom of the picture.

ムで受け取る．誕生月による時間指定．2 種目のウイルス検査ソフト配布は 12 月 18 日（水）開始予定．危機管理チーム（Notstands-Koordinationsgruppe）結成．

12 月 19 日（木） フランクフルト検察庁（Die Generalstaatsanwaltschaft Frankfurt）が Ryuk（Emotet で使われるランサムウェア）による被害と発表．

12 月 23 日（月） クリスマス休暇（12/23 〜 1/1）間も IT サービスセンターは一部電話対応する旨発表．一部の職員はマールブルク大学他から提供された PC を利用．

2020 年 1 月 3 日（金） クリスマス休暇明けにシステムは正常化に向かうとの発表．Stud.IP (CMS), JLUBox（クラウドサービス），大学公式 Web サイトは 6 日（月）より，図書館システム等は 13 日再開予定．学内ネットワークのインターネットアクセスも 13 日より順次再開予定．Windows 対象のファイルサービス再開は 2 月になる見込み．ただし，研究・運営に関する情報は失われていない．

1 月 6 日（月） 大学公式 Web ページが復旧した．#JLU-offline 関係の情報はサブページに整理され，通常の研究・教育関係の情報が掲載されている．

1 月 13 日（月） 予定通り図書館システムが復旧した．まだ受け取っていない人のためのパスワード配布を 13 日から 17 日（金）まで行うことが発表された．

1 月 20 日（月） 学生向け Wi-Fi, 学生寮のインターネットアクセス再開．パスワード配布を窓口で継続．

3. ギーセン大学の対応

注目すべき大学の対応をいくつか指摘したい．

3.1 全学封鎖の決定

マルウェア感染被害がいつどのような形で発生し，検知されたかについては依然発表されていないが，学内のいくつかのシステムで被害の発生が確認されたのちそれほど経たないうちに全学のサーバ及びネットワークをシャットダウンしたものとみられる．学期中であるにもかかわらず，このような大胆な決定を行い実行したことに注目すべきである．

3.2 外部との連携

12 月 8 日にマールブルク大学において代替 Web サイトを立ち上げた（図 3）．マールブルク大学は同じヘッセン州にあり，日頃から連携をとっていた可能性がある（図 4）．

```
> tracert www.uni-giessen.de

www-srv.hrz.uni-giessen.de [137.248.16.5] へのルートをトレースしています
経由するホップ数は最大 30 です:

  （一部省略）
  7     3 ms     3 ms     3 ms  tokyo1-GM-ET-5-1-0-1109.s5.sinet.ad.jp [150.99.89.147]
  8   155 ms   155 ms   155 ms  150.99.92.3
  9   155 ms   155 ms   155 ms  sinet-gw.mx1.ams.nl.geant.net [62.40.125.182]
 10   162 ms   162 ms   162 ms  ae7.mx1.fra.de.geant.net [62.40.98.187]
 11   162 ms   162 ms   162 ms  cr-fra1.x-win.dfn.de [62.40.124.218]
 12   167 ms   167 ms   167 ms  cr-han2-be6.x-win.dfn.de [188.1.144.134]
 13   170 ms   170 ms   170 ms  kr-mar20-0.x-win.dfn.de [188.1.246.98]
 14   172 ms   171 ms   179 ms  cerz01270.HRZ.Uni-Marburg.DE [137.248.2.1]
 15   174 ms   170 ms   170 ms  vhrz720.HRZ.Uni-Marburg.DE [137.248.16.5]

トレースを完了しました.
```

図 3 代替 Web サイトへの日本国内から（SINET 経由）の経路．マールブルク大学に置かれていることがうかがえる．

Fig. 3 Path to the substitute Web site from within Japan through SINET. It seems to be located at the Marburg University.

9 日に被害届を提出したのち，10 日には外部専門家を招

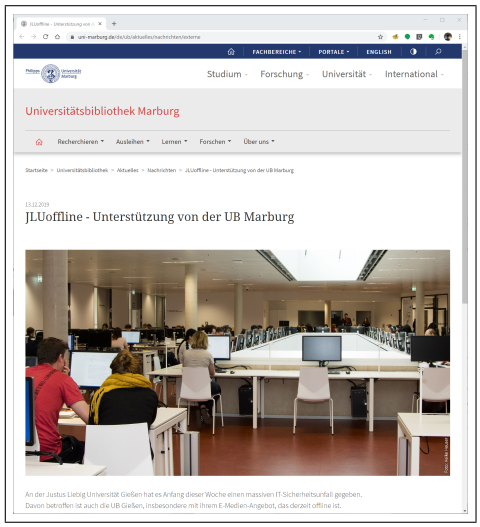

図 4　ギーセン大学の学生に図書館・情報サービスを提供するというマールブルク大学図書館のアナウンス．見出しは「JLUoffline – マールブルク大学図書館からの援助」である．

Fig. 4　An annoucement by Marburg University that it provides library and information services to the students of Giessen University. The title of the page is "JLUoffline – Help from Marburg University Library."

聘している．公式発表を見る限り，ギーセン大学には組織として CSIRT は存在していない模様だが，緊急時に支援を仰ぐことのできる組織が用意されていたことがわかる．

3.3　広報と学長の対応

危機対応において適切な情報発信が重要であることは論を待たない．ギーセン大学では，代替 Web サイトを立ち上げると，連日のように対応状況がトップページにおいて発信された．同時に，FAQ や学生向けの情報も掲載されている．情報はドイツ語で掲載されたが，重要な情報については英訳も同時に提供された．

公式 Web だけではなく，Twitter, Facebook, Instagram, YouTube も利用され，公式情報が提供された．

Twitter については，公式アカウントのほか，#JLUOffline というハッシュタグが設定され，学内外の利用者との情報流通が図られたことにも注目したい（図 5）．

このハッシュタグを検索すると，各時点において学内関係者（教員，学生）の発信があると同時に，学外からのコメントもあり，活用されたことがわかる．全学封鎖という事態に対して，不便をかこつ声や大学当局の対応への批判もみられたものの，総じて論調は平穏であり，未曾有の事態に対して協力して前向きに対処したいという機運がみられた．州の大臣から対応にあたる職員を誇りに思うという投稿もあった．このような投稿があると，職員が鼓舞されるだけでなく，全学的な一体感を持って対処に当たれるだろう．

学長は YouTube で公式発表を行なった（図 6）．被害が

図 5　#JLUoffline が 2019 年 12 月 25 日に Twitter のトレンド入りした．

Fig. 5　#JLUoffline entered the Trend of Twitter on Dec. 25, 2019.

図 6　学長による YouTube での発表．

Fig. 6　Statements by the President on YouTube.

甚大であること，復旧には時間がかかること，学生への利益を最大限重視し，研究教育を可能な限り通常通り継続することを自ら表明した．これは学内外に大学として責任ある対応を取ることを明示した，非常に有効な発表であった．

3.3.1　業務継続

今回の事態は学期中に発生したものであり，講義や研究が盛んに行われている最中のことであった．ネットワークや IT システムが利用不可となる中で，これらの大学における重要業務をどのように遂行するか．#JLUOffline では，様々な工夫によって講義や図書館など学生支援活動が継続される様子が見られた．

3.4　Email アカウント復旧手順

Email アカウント復旧のためのパスワードは紙媒体で全利用者に配布するという方法がとられた．パスワードをオンラインで配布してはならないとする規則が DFN[*3]にあるということであり，キャンパス内のジムを会場として対面確認が行われた（図 7）．大量の人数を捌くため，誕生月によって配布日時が指定された．パスワード配布を待つ長い列にはドイツ国内のみならず BBC（図 8）や米国メディアも注目し，広く報道された．

紙で配布するということを揶揄する報道もあったが，大

*3　Deutsches Forschungsnetz．ドイツの研究用ネットワーク

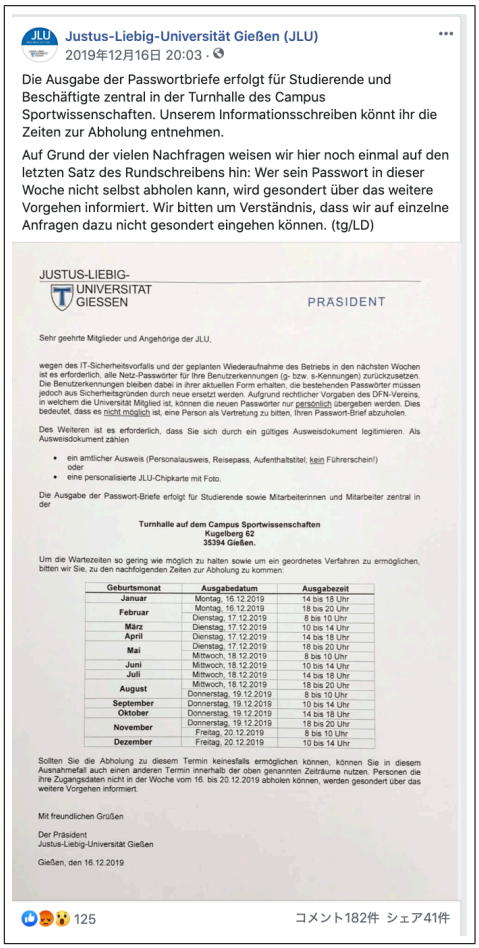

図 7 パスワード配布方法を伝える大学公式 Facebook アカウントの投稿．配布物に生まれ月による配布日時の指定をする表が示されている．

Fig. 7 An offical Facebook post which shows the instruction to distribute passwords. A table is shown in the handout to specify the distribution date and time according to the birth month.

学が短期間に準備を整え，学生を含む大学構成員が整然と冷静に対応したことに注目すべきであろう．

3.5 ウイルススキャナの使用

USB メモリに収められたウイルススキャナによって PC の健全性を担保するという発表がなされ，2 回（第 1 波，第 2 波）にわたって実行された．途中マルウェアの解析が進み，市販のウイルス対策ソフトウェアでも検知可能になるなどして手順は若干変更された可能性もある．12 月 19 日に検察によって Emotet, Ryuk による感染との発表があり，この時点で学内での対処法は確立したものとみられる．

4. 日本の大学との比較

日本の大学でこのような大規模感染が発生した場合，果たして適切に対処できるだろうか．本稿では国内の大学においてよく参照されていると考えられる「高等教育機関の情報セキュリティ対策のためのサンプル規程集」（2017 年

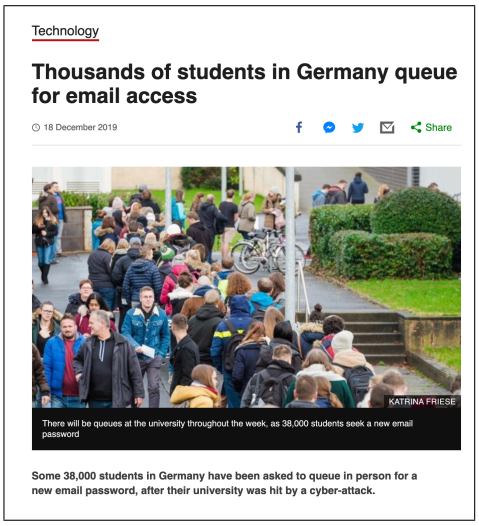

図 8 パスワード配布を報じる BBC の記事 [4]．列をなす学生の写真が掲載されている．

Fig. 8 An article by BBC which reports the distribution of passwords with a picture of students lining to obtain them[4] .

版）[5][*4]に基づき，想定される対処について考える．同規定集のうち本文で参照する項目については抜粋を付録に掲げた．

4.1 サンプル規定集におけるインシデント緊急対応

インシデント緊急対応については，「C2102 情報システム非常時行動計画に関する規定」（付録 A.1）がある．

第一条と第二条では，本規定の目的と定義が与えられている．全学隔離が必要となるような大規模インシデントはこの範疇に含まれると考えてよいだろう。

第三条は，非常事態の全学的な報告・把握の体制を規定する．全学実施責任者[*5]がインシデントについての報告・通報受付する手段を設け（第 1 項），報告または通報を受けたインシデントのうち非常事態の発生またはそのおそれがある場合に全学総括責任者[*6]に報告し，非常時対策本部の設置を提案するとしている（第 2 項）．

第 1 項の規定は，一般のインシデントについての情報集約に関する規定であるが，第 2 項で非常事態を判断するための前提としてあえておかれているものと思われる．

第四条は非常時対策本部の構成について規定している．構成員は全学統括責任者，全学実施責任者と関連する部局情報システムの部局総括責任者[*7]のみであり，CSIRT, 危機管理担当理事，広報担当者，総務系事務担当者などは委員に含まれていない．ただし，委員以外の意見を聞くこと

*4 原稿作成時の最新版．
*5 政府機関等の情報セキュリティ対策のための統一基準 [6] でいう統括情報セキュリティ責任者に対応する．
*6 統一基準でいう最高情報セキュリティ責任者に対応する．いわゆる CISO (Chief Information Security Officer) である．
*7 統一基準でいう情報セキュリティ責任者に対応する．部局長クラスが想定されている．

はできる（第 4 項）.

第五条では非常時連絡窓口及び非常時連絡網について規定している．第 1 項でその設置について規定される非常時連絡窓口は，全学実施責任者が担当し，通報者や捜査当局等の外部（第 2 項）及び学内（第 3 項）の情報のやり取りを行うこととされている．

窓口といっても情報の受付だけでなく双方向的に情報の流れを集約する趣旨である．ただし，外部に対しては「直接または広報窓口を通じて行う」（第 2 項）とされており，広報との分担の切り分けが必要になるものと思われる．

非常時連絡網の整備は第 4 項で規定される．非常時連絡網は，非常時連絡窓口を中心とするが，その連絡先には，非常時対策本部委員の他，全学情報システムについては情報メディアセンター，総務部，部局情報システムについては部局技術責任者及び部局技術担当者，必要に応じて法律専門家，広報部門を設定する（第 5 項）とされている．

私見では，この非常時連絡網の働きがはっきりしないように思われる．連絡先というのは何を指すのだろうか？非常時連絡窓口に寄せられた情報をこの連絡先に配布するという趣旨であろうか．連絡先の，非常時対策本部委員以外の者は，その情報をどう扱えばいいのであろうか．また，非常時連絡窓口は双方向的に情報を集約する場であるから，情報を発信する場合にもこの連絡先に含められたメンバーが何らかの関与を行うのであろうか．とすると，この連絡先にあるメンバーは，非常時対策本部の委員となるべきものなのではないだろうか．

第六条では，インシデント対応手順は「C3102 インシデント対応手順」によるが，第 2 項で緊急対応のため臨時的な措置をとることができるとしている．このこと自体は必要なことではあるが，緊急時にフリーハンドで適切な対応が取れるかどうか．取りうる対応について予め一定の想定をし，演習を行っておくことが必要であろう．

第七条は，非常事態の終了について規定している．報告書の提出先は全学情報システム運用委員会[*8] とされている．

4.2 サンプル規定集におけるインシデント対応手順

情報セキュリティインシデント対応については，「C3102 インシデント対応手順」（付録 A.2）に記載がある．

インシデントの初期対応とエスカレーションについては「3. インシデントの対応判断のエスカレーション手順」に記載されている．

インシデント発生後の対応については「5. セキュリティインシデント発生時の対応」に記載がある．ここでは

(1) 発生から緊急措置決定まで[*9]
(2) 被害拡大防止の応急措置の実施
(3) 緊急連絡と報告
(4) 復旧計画
(5) 原因調査と再発防止策

と順を追って述べられているが，各項目の記載[*10] によると対処は部局単位で行うことが想定されている．

緊急対応が必要な場合であって，全学ネットワークに影響がある場合，「(3) 緊急連絡及び報告」が適用される．ここで，（ウ）にある非常時対策本部は前節 4.1 で見たものであるが，それと比べると，非常時対策本部設置には二つの異なった要件があることになる．

非常時行動計画においては，一般のインシデントについての報告を全学実施責任者が把握し，その中から非常事態の発生またはそのおそれがある場合に非常時対策本部の設置を提案することになっていた．これに対し，本手順では，被害拡大防止措置が全学ネットワークに影響する場合に部局総括責任者が全学実施責任者に連絡し，必要に応じ非常時対策本部が組織される．

なお，本手順では，部局内ネットワークに閉じた技術的問題と判断される場合には，全学実施責任者や CSIRT への連絡をとることとはされていない（第 3 項）．この場合全学実施責任者への報告が行われるのは，インシデント対応作業が完了したのち（第 5 項 (5)（ウ)）である．従って，もし複数の部局を標的とした攻撃が行われても，それぞれは単純なマルウェア感染に見えた場合には，全学での把握が遅れる可能性がある．

警察や外部機関への対応，被害の公表，監督省庁（大学であれば文部科学省）対応などについては一切記載がない．

4.3 日本の大学は大規模インシデントに対応できるか

以上見てきたようなサンプル規定集に添ったポリシー及び実施手順を持った日本の大学は，果たして，ギーセン大学で発生したような大規模インシデントに適切に対応できるだろうか．本稿では以下の 3 点に絞って検討したい．

(1) 全学規模のインシデントを早期発見できるか
(2) 全学封鎖という大学運営に直結する判断を適切に下せるか
(3) 長期にわたる対策・復旧作業を乗り切れるか

なお，ギーセン大学のインシデントの発生及び拡大状況についての情報は公開されていないが，以下のような順序で起きたものと仮定する．

(1) ある教職員の PC が電子メールに添付されていたマルウェアに感染
(2) 残存していた脆弱性を悪用し，近傍の複数部局の教職員の PC に感染が拡大

[*8] 「C1001 情報システム運用基本規程」で規定．委員長は全学総括責任者である．
[*9] この項目は「3. インシデントの対応判断とエスカレーション手順」と目的がやや重なる部分がある．（内容に重複はない．）書き振りを整理することもできるのではないか．
[*10] 付録では紙数の都合で (4) 以降の各項目の内容は省略した．

(3) PC 上に保管されていた ID 情報を利用して全学システムのディレクトリサーバ，メールサーバ等に侵入，ランサムウェア等による被害が発生

4.3.1 全学規模のインシデントを早期発見できるか

日本の大学は，部局（学部，研究科など）の独立性が高いと言われる．サンプル規定集のインシデント対応手順においても，部局における対応が原則となっている．4.2 節で指摘したように，部局において閉じた判断が行われた場合，全学的な被害の把握が遅れる恐れがある．

ここで仮定したシナリオでは，マルウェア感染が複数部局に拡大しているが，個々の PC レベルのマルウェア感染への対処は部局毎個別に行われることになるであろうから，複数部局で同時に被害が発生していることが把握されない可能性がある．もちろん，もし全学 CSIRT がインシデント情報を集約していたとしても，それぞれが無関係なものなのか，関連したものなのかを判断することは難しいかもしれない．そうすると，全学的なインシデント認知はシナリオの第 3 ステップ，全学システムの被害が発生してからとなる可能性がある．

4.3.2 全学封鎖という大学運営に直結する判断を適切に下せるか

サンプル規定集で定める緊急対応手順の想定範囲は情報セキュリティインシデントとして対処可能な範囲のものである．そのことは，非常時対策本部の本部長が全学総括責任者 (CISO) であり，報告書の提出先も全学総括責任者が委員長である情報セキュリティ委員会であることからもうかがえる．

しかし，全学封鎖を必要とするような大規模な事態が発生した際には，学長を中心とする危機管理体制に移行しなければならない．サンプル集の規定からはその道筋は見えない．[*11] もちろんそのような事態はなかなか想定できるものではないが，現実にギーセン大学で発生している以上，想定外ということはもはやできない．

4.3.3 長期にわたる対策・復旧作業を乗り切れるか

対策が大規模かつ長期に渡る場合，通常の意味のインシデント対応や，部分的な再発防止策の策定では事足りない．

技術力，作業負荷の観点から外部専門家チームの導入は必須であり，公的なものか営利企業によるものかを問わず，その適切な利用について用意をしておく必要がある．

自組織のネットワークや情報システムが使えなくなった場合，相互に援助する仕組みがあると心強い．近隣または地域の大学等の機関の間でこのような仕組みを用意しておくことが望ましい．

公式情報を適切に発信し続けることが極めて重要である，オンプレミスの Web サーバが使えなくなれば，代替 Web ページを用意する必要がある．今日では SNS の活用も必須であろう．

しかし日本では，情報セキュリティインシデントについて早い時期に公表することや，対処について公にすることはなかなか見られない．不確かな情報が SNS で拡散し却って困難な状況になることは避けなければならない．平時から広報手段を研究し，適切に情報をコントロールできるようにしておくことが必要であろう．

5. 結論

本稿では，ギーセン大学における事態の推移を公開情報から辿るとともに，日本の大学で大規模情報セキュリティインシデントに対応するとしたらどのような体制がとられるかを高等教育機関のためのサンプル規定集を参考に検討した．

有力な大学で，全学ネットワーク封鎖，メールシステムや講義用システムを含む全学サービス停止という大学運営に極めて大きな影響を及ぼす事態が実際に発生したことは，大学等の情報セキュリティに携わる者として非常に大きな衝撃であり，これに対する備えができているかを自ら問う機会となった．

本稿の検討の結果，今後特に注意して準備すべき点として以下を挙げておきたい．

- 部局で発生しているインシデントの情報を集約し，大規模インシデントにつながる可能性をいち早く検出・対応する体制
- 組織運営の根幹に関わるインシデントの可能性が現れた際，組織全体の危機管理体制への円滑なエスカレーションを行う仕組み
- 対応が長期化する場合に備え，外部の支援を適切に受けられるような（相互）支援体制の準備
- 建設的な対応を組織内外に促すためのメディアや SNS の活用

謝辞 事態発生及びその後の情報をお知らせくださった KEK 計算科学センターの皆様，ご意見や追加情報をいただいた学術系 CSIRT 情報交流会の皆様に感謝します．

参考文献

[1] Wikipedia, ユストゥス・リービッヒ大学ギーセン.
[2] ギーセン大学公式 Web サイト．https://www.uni-giessen.de/[*12]
[3] Gießener Anzeiger. https://www.giessener-anzeiger.de/
[4] BBC, “Thousands of students in Germany queue for email access,” https://www.bbc.com/news/technology-50838673
[5] 国立情報学研究所, 高等教育機関の情報セキュリティ対策のためのサンプル規程集（2017 年版）. https://www.nii.ac.jp/service/sp/

[*11] 付録には掲載していないが，C2102 に含まれる解説には全学の業務継続計画に統合されるべきと書かれている．その場合は、この問題は解決できる可能性がある．

[*12] URL の最終確認日: 2020 年 1 月 29 日（以下同じ）

[6] 内閣サイバーセキュリティセンター, 政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）[*13]. https://www.nisc.go.jp/active/general/kijun30.html

付　　録

高等教育機関の情報セキュリティ対策のためのサンプル規程集（2017 年版）[5] より本文中で参照している項目を一部抜粋して示す.

A.1 C2102 情報システム非常時行動計画に関する規定（抜粋）

C2102-01（目的）

第一条 この規程は，A大学情報システムの運用において非常事態が発生した場合の行動を非常時行動計画として事前に定め，早期発見・早期対応により，事件・事故の影響を最小限に抑え，早急な情報システムの復旧と再発防止に努めるために必要な措置を講じることを定めることを目的とする.

C2102-02（定義）

第二条 この規程において，次の各号に掲げる用語は，それぞれ当該各号の定めるところによる.

（一，二　略）

三　非常事態　本学情報システムの運用に関するインシデントのうち特に緊急性を要するものをいう.

C2102-03（非常事態の報告）

第三条　全学実施責任者は，インシデントについての報告または通報を学内または学外から受けつけ，迅速に情報を集約する手段を整備し，周知・公表する.

2　全学実施責任者は，報告または通報を受けたインシデントのうち，非常事態の発生またはそのおそれがある場合には，全学総括責任者へ報告し，非常時対策本部の設置を提案する.

C2102-04（非常時対策本部）

第四条　全学総括責任者は，非常事態が発生しまたは発生するおそれが特に高いと認められる場合に，被害の拡大防止，被害からの早急な復旧その他非常事態の対策等を実施するために非常時対策本部を設置する.

2　非常時対策本部は次の各号に定める委員をもって構成する.

一　全学総括責任者

二　全学実施責任者

三　関連する部局情報システムの部局総括責任者

3　全学総括責任者は，非常時対策本部の本部長となる.

4　全学総括責任者が必要と認めたときは，委員以外の者を出席させて意見を聞くことができる.

C2102-05（非常時連絡網）

第五条　非常時対策本部には，緊急連絡及び情報共有等を行うために全学実施責任者が担当する非常時連絡窓口を設置し，関係者に周知徹底する.

2　非常時連絡窓口は，非常時対策本部長の指示に基づき，通報者や捜査当局，クレームの相手方，報道関係者等，外部との対応を直接または広報窓口を通じて行う.

3　非常時連絡窓口は，非常時対策本部長の指示に基づき，学内関係者からの情報の受付および収集，被害拡大防止や復旧のための緊急対策等の伝達を直接行う.

4　全学実施責任者は，非常時連絡窓口を中心とする非常時連絡網を整備する.

5　非常時連絡網の連絡先には，非常時対策本部委員の他，全学情報システムについては情報メディアセンター，総務部，部局情報システムについては部局技術責任者及び部局技術担当者，必要に応じて法律専門家，広報部門を設定する.

C2102-06（インシデント対応手順）

第六条　具体的なインシデント対応は，別途定める「C3102 インシデント対応手順」に基づき対処する.

2　非常事態においては，非常時対策本部の指示がインシデント対応手順に優先する.

C2102-07（再発防止策の検討）

第七条　全学総括責任者は，非常事態への対応が終了した場合，非常時対策本部から全学情報システム運用委員会への報告書の提出をもって，非常時対策本部を解散する.

2 全学総括責任者は，報告書をもとに再発防止策の実施を図る.

A.2 C3102 インシデント対応手順（抜粋）

1. 定義（略）

2. インシデント通報窓口（略)

3. インシデントの対応判断のエスカレーション手順

(1) CSIRT は，インシデントを認知した場合は，緊急連絡網その他所定の連絡網により，適宜，全学総括責任者，全学実施責任者，部局総括責任者，部局技術責任者，部局技術担当者のうち関係する

[*13] 高等教育機関の情報セキュリティ対策のためのサンプル規程集（2017 年版）で参照されているのは平成 28 年度版だが，本稿で参照する範囲では変更はない.

者にインシデントの初期対応を依頼するものとする．
(2) 情報メディアセンターは，CSIRT との連携のもと，全学ネットワークに関るインシデントについては，必要に応じて自ら技術的対応をするものとし，部局ネットワークにのみ関連するインシデントについては，部局技術責任者を支援するものとする．
(3) 部局技術担当者は，インシデントを発見し，または CSIRT 等を通じて内部・外部からの通報を受けることにより認知した場合，ただちに部局技術責任者に状況報告するものとする．
(4) 部局技術責任者は，インシデントを自ら認知するか部局技術担当者から状況報告を受けた場合，下記の基準により一次切り分け判断を行うものとする．
① 部局内ネットワークに閉じた技術的問題か
i) 物理的インシデントまたはセキュリティインシデントの場合で，対外的インシデント及び体内的インシデントのいずれでも無く，部局内ネットワークにのみ影響が生じている場合，部局技術担当者に対策を指示し，対策結果を部局総括責任者に状況報告する．
ii) i) 以外の場合，部局総括責任者を通じて全学実施責任者に状況報告をし，CSIRT 及び情報メディアセンターの支援を仰ぎながら，物理的インシデントまたはセキュリティインシデント対応のプロセスを実施する．
② コンテンツインシデントか（略）
(5) 部局技術責任者は，あらかじめ定められた手順に従って，緊急な技術的対応が必要なときは部局技術担当者に指示を与え，部局総括責任者に対応結果を報告する．法的に慎重な判断を要する場合は，対応を実施する前に必ず部局総括責任者に報告し，指示を受けることとする．
(6) 部局技術責任者から報告を受けた部局総括責任者は，コンテンツインシデントについて，部局技術責任者・部局技術担当者を指揮監督する．セキュリティインシデント対応については，ポリシーに基づいて全学実施責任者に指示や承認を求める．また，法的判断を要する問題については，法務担当部門に対応を依頼する．
(7) 学外クレームか，対外クレームか（略）
4. 物理的インシデント発生時の対応（略）
5. セキュリティインシデント発生時の対応
(1) 発生から緊急措置決定まで
(ア) 監視システムによるセキュリティインシデントの可能性を示す事象の検知や，通報等でセキュリティインシデントの可能性を認知した部局技術担当者は，事実を確認するとともに部局技術責任者に報告し，被害拡大防止のための緊急措置の必要性について判断を求めるものとする．
(イ) 部局技術担当者は，後日の調査に備え，セキュリティインシデント発生時の状況，例えばログイン状況，ネットワーク接続や手順の稼働状況に関する記録を作成し，バックアップデータの作成，ハードディスクのイメージの保存等を行う．
(ウ) セキュリティインシデントが，外部からの継続している攻撃等であって攻撃元ネットワークの管理主体等への対処依頼が必要な場合，部局総括責任者の承認を得て部局技術責任者から相手方サイトへの対処依頼を行う．
(2) 被害拡大防止の応急措置の実施
(ア) 部局技術責任者は，個別システムの停止やネットワークからの遮断（他の情報システムと共有している学内通信回線又は学外通信回線から独立した閉鎖的な通信回線に構成を変更する等）等の緊急措置の必要性を判断し，実施を部局技術担当者に指示する．
(イ) 部局総括責任者および部局技術責任者は，情報システムのアカウントの不正使用の報告を受けた場合には，直ちに当該アカウントによる使用を停止させるものとする．
(ウ) 部局技術責任者は，利用者等による対処が必要な場合には，その旨命令する．
(3) 緊急連絡及び報告
(ア) 部局技術責任者は，緊急の被害拡大防止措置を実施する場合は，部局総括責任者に報告する．
(イ) 部局総括責任者は，被害拡大防止措置が全学ネットワークに影響する場合は，部局総括責任者は学内窓口を通じて全学実施責任者に連絡する．
(ウ) 全学実施責任者は，CSIRT を通じて，緊急措置の実施により影響を受ける利用者等に被害拡大防止措置を連絡するとともに，全学総括責任者の指示を仰いだ上で，必要に応じ非常時対策本部を組織する．
(エ) CSIRT は，全学実施責任者または非常時対策本部の指示に基づき，攻撃元サイトや関係するサイトへの連絡，及び関係機関への報告などを指揮する．
(オ) 非常時対策本部が設置された場合，CSIRT，部局技術責任者及び部局技術担当者は，その指示に従うものとする．
(4) 復旧計画（略）
(5) 原因調査と再発防止策（略）
6.〜9.（略）