政策研究大学院大学の情報システムに対する不正アクセスの調査報告書

政策研究大学院大学

インシデント対応検証に係る外部アドバイザリーボード

2023 年 8 月 22 日

内容

1. はじめに

本報告書は政策研究大学院大学（以下、GRIPS）において 2022 年 8 月 29 日に判明した公開ウェブサーバに対する不正アクセスに関する経緯および原因と対策についてまとめたものである。

また、大学や研究機関をはじめ様々な組織の参考となる様に、可能な限り不正アクセスの過程を中心に詳細な記述に努めた。特定の組織を狙ったサイバー攻撃は現実的な脅威であり、読者がその脅威を改めて認識し、自身の組織のリスクの見直しや具体的な対策の実行に繋げていただければ幸いである。

本報告書は、以下 3 名の「インシデント対応検証に係る外部アドバイザリーボード」が中心となり、GRIPS が調査・整理した事実関係をもとに議論・審議を経て取りまとめた。

政策研究大学院大学　セキュリティアドバイザー
　　松浦 知史（東京工業大学 学術国際情報センター 教授）
政策研究大学院大学　セキュリティアドバイザー
　　中村 豊（九州工業大学 情報基盤センター 教授）
政策研究大学院大学　情報セキュリティ総括責任者（CISO）補佐
　　川口 洋（株式会社川口設計 代表取締役）

2. 不正アクセスの概要

2022 年 8 月 29 日（月）、学内サーバのメンテナンス中に情報システム担当職員が多数のログイン失敗が発生しているログを不審に感じ、サーバの状態を調査した。調査の結果、公開ウェブサーバが外部から不正操作されている可能性が高いと判断し、GRIPS 執行部に報告を行うとともに、報告後、ウェブサーバを停止した。翌 30 日にはセキュリティベンダーに連絡し、デジタルフォレンジック調査（機器やデータの分析によりインシデントの原因などを特定するための調査）を打診した。その後もセキュリティ・オペレーション・センター（Security Operation Center: SOC）から不審なアクセス検知の報告があったため、情報セキュリティ総括責任者（Chief Information Security Officer: CISO)及び CSIRT（シーサート、Computer Security Incident Response Team）の判断により、9 月 3 日に本学のインターネット接続をファイアウォールにて遮断した。遮断後に実施したデジタルフォレンジック調査等の結果、不正アクセスは以下のように行われていたことが判明した。

① 2015 年 4 月 13 日に攻撃者は GRIPS 情報システムに攻撃を行い、リモートから不正操作を行うための悪性プログラム（ウェブシェル。web shell）を設置した。2015 年時点の情報システムは現在のシステムから 1 世代前のものであり、悪用された脆弱性については確認できなかった。幸い、公開ウェブサーバへのアクセスログが別サーバに長期保管されており、設置されたウェブシェルのアクセスを追跡することができた。

② 2015 年のウェブシェル設置後、2022 年 8 月 23 日までに複数の IP（アイピー、Internet Protocol）アドレスから同ウェブシェルへのアクセスが行われていた。また、アクセスログとその他のサーバのログを調査した結果、それ以外にも 2 つのウェブシェルが設置されていたことが判明した。

③ 2022 年 8 月 28 日、攻撃者はウェブシェルにアクセスして GRIPS の学内ネットワーク内のスキャンを実施し、その後、ネットワーク内の複数のサーバや端末に攻撃を行った。

④ 2022 年 8 月 29 日、情報システム担当者がサーバのメンテナンス作業中に不審なログの存在を発見し、不正アクセスが判明。情報セキュリティ総括責任者（CISO）を含む GRIPS 執行部に本インシデントを報告した。

⑤ 同日、緊急対応措置として公開ウェブサーバの停止および内部サーバの管理者パスワードを変更するとともに、翌 8 月 30 日、セキュリティベンダーにデジタルフォレンジック調査を打診した。

⑥ 公開ウェブサーバが停止したため、攻撃者は他のサーバに設置したバックドア経由で内部のサーバや端末に攻撃を行った。これを GRIPS の業務用端末に導入しているセキュリティ製品であるエンドポイント検出・対応（endpoint detection and response: EDR）システムが検知し、アラートを出したことで、攻撃が継続していることが判明した。

⑦ 2022 年 9 月 3 日、GRIPS のインターネット接続をファイアウォール（firewall）にて遮断した。

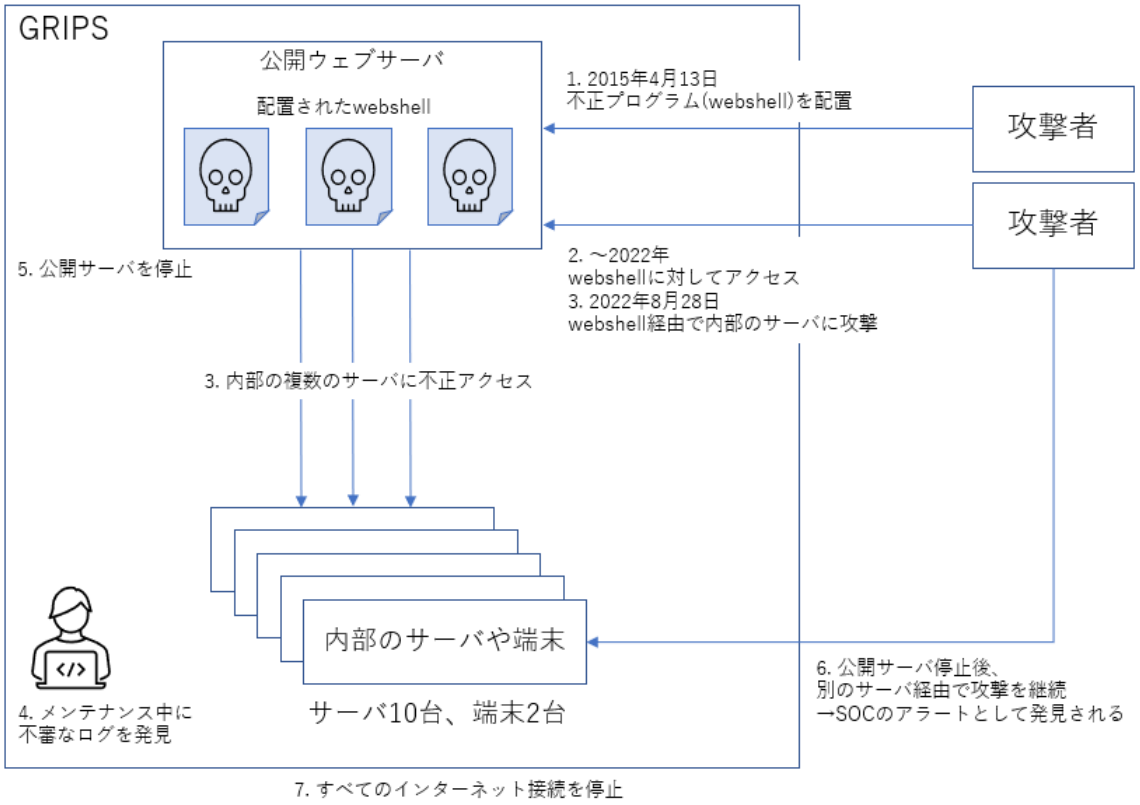

図 1　不正アクセスの概要

3. GRIPS の組織概要と体制

3.1. GRIPS の組織概要

GRIPS は 1997 年に開学した政策研究を専門とする大学院大学で、政策および政策の革新にかかわる研究と教育を通して、我が国および世界の民主的統治の発展と高度化に貢献することを目的としている。学生数は 360 名強であり、日本を含む世界 60 近くの国と地域から学生が集まり、全学生の約 3 分の 2 が留学生である。また修了生は 5,000 人以上であり、その出身国・地域は 120 を超える。留学生は開発途上国を中心とするミッドキャリアの行政官、日本人学生は中央官庁や地方自治体、国際機関の職員など、その多くがパブリックセクターに勤務している。

2023 年 5 月 1 日時点で、教員は 67 人、職員は 122 人であり、GRIPS の情報システムのメインユーザはこれらの教職員である。また、キャンパスは東京・六本木にあり、情報システムも六本木キャンパスを中心に構成されている。

3.2. GRIPS の情報管理体制

2022 年 8 月末時点における GRIPS の情報管理体制は以下の通りであった。

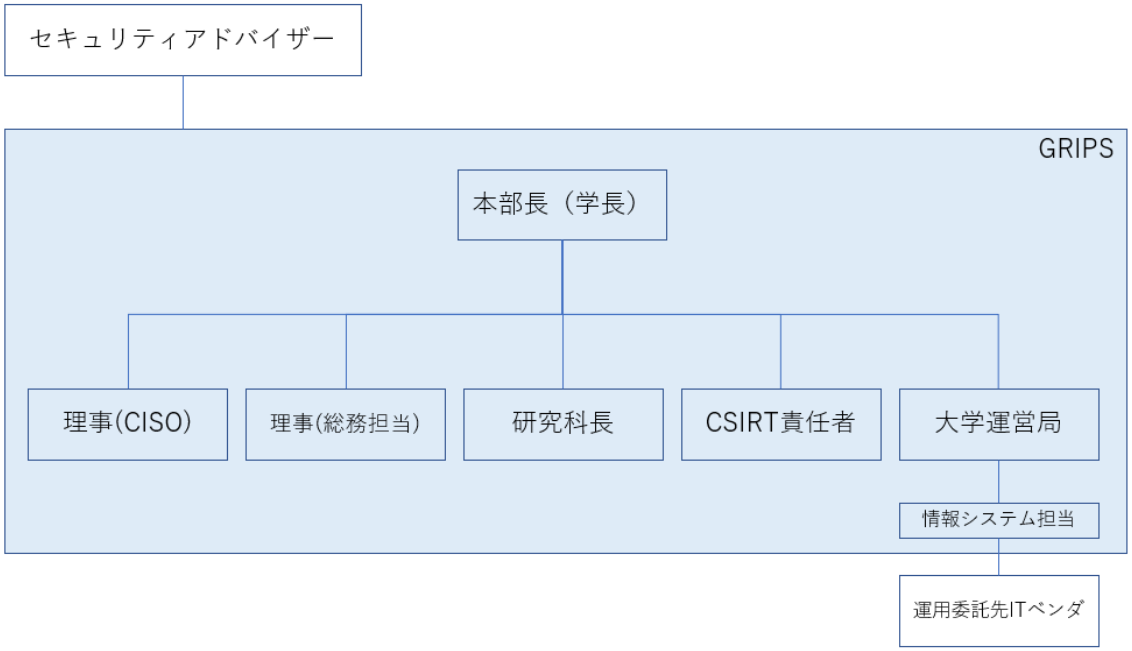

図 2　2022 年 8 月末時点における GRIPS の情報管理体制

学長をトップとして、CISO 担当理事、総務担当理事、研究科長、CSIRT 責任者、大学運営局で構成されている。情報システムの管理運用を担う情報システム部門は大学運営局に含まれ、情報システムに関する情報は大学運営局長経由で伝達される。この大学運営局の中にある情報システム担当が外部委託している IT ベンダーとの契約およびその管理を行い、システム運用を行う体制である。事故発生時点における情報システム担当者は 1 名であったが、この担当者は総務部門を兼務しており、情報システム担当としての実質的な稼働人数は 0.5 人となっていた。

大学の IT システムの構築およびシステム運用は、委託先 IT ベンダー1 社が担当していた。同ベンダー社内ではシステムの種類や業務ごとに担当チームが置かれており、協力会社である IT ベンダー複数社とともに運用する体制であった。

また外部の大学教員をセキュリティアドバイザーとして任命し、セキュリティ全般に関するアドバイスを受ける体制を構築している。

3.3. GRIPS の情報システム構成

GRIPS の情報システムは、大学運営局の情報システム担当者と運用委託先 IT ベンダーが

維持管理しており、主に以下の機能を提供している。

- 学内向けサービス
  - 教職員用パソコン提供
  - 電子メール
  - IT サポートセンター（ヘルプデスク）
  - 学内ネットワーク接続（有線 LAN（local area network）および無線 LAN）
  - ファイル共有システム
  - 図書館システム
  - 契約機材の運用・保守
- 学外向けサービス
  - 公開情報を掲載するウェブサービス
  - シングルサインオン（single sign-on: SSO）などの認証・認可サービス
  - ドメイン・ネーム・システム （Domain Name System: DNS）サービス

2022 年 8 月末時点における GRIPS の情報システムの概要は以下の通りであった。

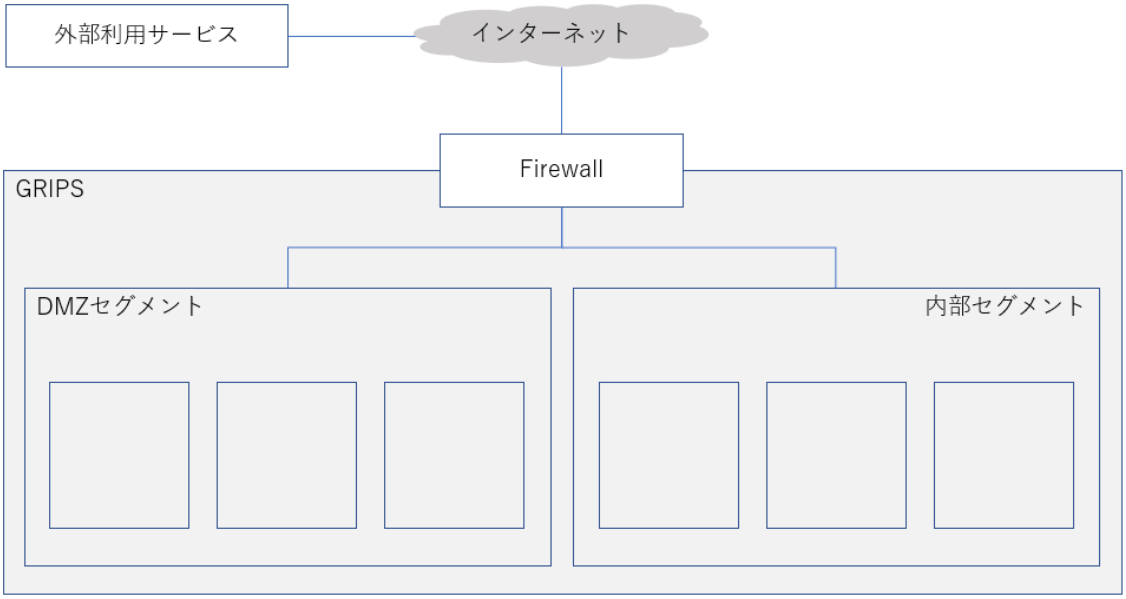

図 3　2022 年 8 月末時点における GRIPS の情報システム

大学のシステムの入り口にはファイアウォールを設置し、インターネット側と大学内部のシステムのアクセス制御を実施している。またこのファイアウォールには一般的な IP アドレスやポート番号でのアクセス制御機能だけではなく、ウイルスチェック機能や URL（Uniform Resource Locator）フィルタリング、IPS（監視・警告・通信の遮断、Intrusion

Prevention System）などのセキュリティ機能も搭載されている。

大学内のネットワークは、インターネット上に公開するシステムを配置する DMZ セグメント（学外と学内のネットワークの間に置かれ、学内ネットワークのセキュリティを保護しつつ、外部との接続を可能にする。DeMilitarized Zone）と内部サービス用の内部セグメントに分割されている。DMZ セグメントには公開ウェブサーバやメールサーバ、認証関連システム、死活監視システム（機器やネットワークなどが正常に動いているかどうかを継続チェックするもの）など、学外の組織やシステムと連携するためのシステムを配置している。内部セグメントには学内からのみ利用するためのシステムや教職員が使用するパソコン（ノートパソコンやデスクトップパソコン）を配置している。

またレンタルサーバや SaaS（サース。クラウド上で使用するソフトウェア。Software as a Service)などを活用したシステムは、大学内部のシステムとは別に管理されている。これらのシステムは利用目的に応じて要件定義や構築・運用が行われており、大学内部に設置されたシステムとは切り離されて運用されているものも多い。

なお、現在の情報システムは 2021 年 12 月にシステム更改を行ったものである。

4. 不正アクセス判明後の対応

不正アクセス判明後の主な対応は以下の通りである。

表 1　不正アクセス判明後の対応

日時	検知時刻、対応内容や検討した事項など
2022/8/29 14:52	内部サーバのメンテナンス作業中、公開ウェブサーバからのログイン失敗ログが多数出ていることを確認
2022/8/29 15:59	情報セキュリティ総括責任者（CISO）へインシデント発生の報告
2022/8/29 16:20	公開ウェブサーバの停止
2022/8/29 16:50	2021 年 12 月に更改したシステムのサーバ全台について管理者パスワードの変更を実施
2022/8/30 11:00	セキュリティベンダーに被疑サーバのフォレンジック調査を打診
2022/9/1 8:30	端末 1 台についてアラート確認
2022/9/1 12:05	全ユーザにパスワード変更指示
2022/9/2 19:00	端末 2 台についてアラート確認

2022/9/2 20:00	アクティブ・ディレクトリ（情報システムの ID やサーバ等のリソースを統合管理するための機能。Active Directory: AD）の管理者パスワード変更を開始
2022/9/2 22:00	バックアップストレージをネットワークから切断（オフライン化）
2022/9/3 10:06	端末 1 台についてアラート確認
2022/9/3 22:30	学内システムとインターネットとの通信を遮断
2022/9/4 0:00	遮断後のファイアウォールブロックログ調査 （ブロックログとは、ファイアウォールで内外からの通信を止めた記録）
2022/9/4 9:00	学長をトップとする緊急対策本部を設置
2022/9/4 16:19	文部科学省へ報告
2022/9/7 12:00	大学ホームページでシステム障害のためメール利用できないことを公表
2022/9/7 15:00	クラウドメールサービスの認証設定変更
2022/9/7 17:00	クラウドメールサービスの全アカウントパスワードリセット実施。初回ログイン時のパスワード変更、2 要素認証の強制を設定
2022/9/8 16:30	セキュリティベンダーにデジタルフォレンジック調査を依頼
2022/9/9 10:00	職員が業務に利用するインターネット回線確保用にモバイルルータを準備
2022/9/9 14:39	セキュリティアドバイザー(東工大 松浦知史先生)に連絡。打ち合わせを調整。
2022/9/12 13:30	セキュリティアドバイザー(東工大 松浦知史先生)と打ち合わせ。主に今後の調査と復旧についてのアドバイス。セキュリティアドバイザーの追加のアドバイス
2022/9/14 14:00	セキュリティアドバイザー(東工大 松浦先生)との打ち合わせ
2022/9/15 14:30	セキュリティアドバイザー打ち合わせ。セキュリティアドバイザーとして九工大　中村豊先生も参加
2022/9/21 15:00	警察に相談
2022/9/22 10:30	クラウドメールサービスの利用再開、ID 通知 インターネット接続用端末の配付
2022/9/28 15:00	大学ホームページでメール復旧を公表
2022/10/4 15:00	セキュリティベンダーに被疑サーバ以外のツール実行結果を提供
2022/10/4 23:00	セキュリティベンダーにマルウェアを検体として提供
2022/10/5 12:00	学生のインターネット接続用に講義室にモバイルルータを設置
2022/10/6 12:00	教員のインターネット接続用としてモバイルルータの貸出を開始
2022/10/6 14:00	セキュリティベンダーにデジタルフォレンジック追加調査を依頼

2022/10/12 18:00	学内利用端末とインターネット接続用端末との相互データのやり取りのため、検疫用 PC と USB メモリを準備、配付
2022/10/18 16:00	セキュリティベンダー調査の中間報告会
2022/10/20 17:00	個人情報保護委員会へ報告
2022/10/21 12:00	学内端末検疫用にオフラインでウイルススキャンができる USB メモリ型ウイルススキャン機器を調達
2022/10/27 9:00	CISO 補佐予定者(株式会社川口設計 川口洋氏)と打ち合わせ
2022/10/27 18:00	サーバの不要ユーザの棚卸を実施
2022/11/7 15:00	セキュリティベンダー調査の最終報告会
2022/11/24 14:00	セキュリティベンダーとネットワーク監視体制について相談
2022/11/28 13:30	セキュリティコンサルタント会社との打ち合わせ。インシデント対応のためとセキュリティ運用体制について協議、決定
2022/12/6 9:00	システム、セキュリティ製品アップデートのためファイアウォールに一部通信の許可設定を追加
2023/1/10 9:00	インシデント対応とセキュリティ運用のためメンバー1 名追加
2023/1/19 12:00	職員が業務に利用するインターネット回線確保用にモバイルルータを追加設置
2023/1/29 20:00	ファイルサーバ再構築完了
2023/2/1 10:00	ファイアウォールの設定についてメーカレビューを実施
2023/2/2 18:00	死活監視サーバ再構築完了
2023/2/3 20:00	AD サーバ 2 号機再構築
2023/2/4 15:00	AD サーバ 1 号機再構築
2023/2/27 14:00	ゲスト用無線 LAN 再開
2023/2/27 16:00	サーバおよびクライアント端末全台に EDR 製品と 802.1X 証明書の導入を開始
2023/3/18～ 2023/3/20	ネットワーク堅牢化工事実施
2023/3/23 12:00	個人情報保護委員会へ最終報告
2023/4/10 22:00	全サーバについて脆弱性診断を実施
2023/4/24 12:00	学内サービス再開
2023/5/8 12:00	インターネット通信再開 大学ホームページにて業務利用のためのネットワーク復旧の公表

※所管官庁である文部科学省とは定期的に状況の共有、報告、相談を実施

※以下のとおり、運営局の事務、教員の研究環境、学生の教育環境に最低限必要な環境を維持し、安全性を重視したネットワーク環境の復旧を目指した。

・ 職員に関しては、9 月 9 日以降、学外接続用 PC 端末とモバイルルータを準備し、インターネット接続を必要とする業務の継続性を確保した。
・ 教員に関しては、10 月 6 日以降、モバイルルータの貸し出しを実施。
・ 学生については、10 月 5 日以降、大学の準備する無線 LAN が使用できなくなったことから、事務局同様に全教室にモバイルルータを設置し、インターネットの利用を継続維持した。

5. 不正アクセスの被害範囲

大学におけるログ調査および学外のセキュリティベンダーによる調査の結果、不正アクセスを受けたシステムは以下の通りである。

表 2　不正アクセスの被害範囲

No	サーバ	用途
1	公開ウェブサーバ	インターネット向け公開用ウェブサーバ（大学ホームページ）
2	シングルサインオンサーバ	大学内ユーザ向けシングルサインオン用サーバ(ID・パスワードによる認証を 1 度行うだけで、学内の複数のシステム、クラウドサービス、アプリケーションを使用できるようにするためのもの）
3	LDAP サーバ	大学内ユーザ向け認証用 LDAP サーバ（登録利用者の情報やシステム上の資源を一元的に管理するもの。Lightweight Directory Access Protocol server）
4	Proxy サーバ 1	大学内ユーザ向けインターネット接続用プロキシサーバー（ブラウザで直接ウェブサイトにアクセスせず、プロキシサーバーを通じて学外のサイトにアクセスすることで安全性などを確保するもの）
5	Proxy サーバ 2	大学内ユーザ向けインターネット接続用プロキシサーバー
6	ファイルサーバ 1	大学内ユーザ向けファイルサーバ（学内で情報を共有・共同利用するためのもの）
7	ファイルサーバ 2	大学内ユーザ向けファイルサーバ
8	ファイルサーバ 3	大学内ユーザ向けファイルサーバ
9	死活監視サーバ	内部システム監視用の死活監視サーバ
10	AD サーバ 1	大学内ユーザ向け認証用アクティブ・ディレクトリ（Active Directory）サーバ（情報システムの ID や

		サーバ等のリソースを統合管理するための機能）
11	AD サーバ 2	大学内ユーザ向け認証用アクティブ・ディレクトリ（Active Directory）サーバ
12	職員端末 1	大学職員の作業用パソコン
13	職員端末 2	大学職員の作業用パソコン

2022 年 8 月 28 日以降、公開ウェブサーバに設置されていた不正プログラム（ウェブシェル）を起点として、大学内の複数のサーバや職員端末に不正アクセスが行われた。セキュリティベンダーの調査の結果、攻撃の起点となったウェブシェルは 2015 年 4 月の時点で設置されていた可能性が高いことがわかった。その後、2022 年にかけて、攻撃者が不定期にウェブシェルにアクセスした形跡はあるものの、2022 年 8 月 28 日以前までは特に目立った攻撃の痕跡は確認されていない。このため、2015 年からウェブシェルが設置されてはいたが、2022 年 8 月 28 日までの被害は公開ウェブサーバのみであり、2022 年 8 月 28 日以降に大学内の複数のシステムに不正アクセスが行われたものと判断し、被害範囲の調査や対応を行った。

6. 情報漏えいに関する調査結果

以下の観点から不正アクセスの痕跡の有無の調査を本学及びセキュリティベンダーで連携して実施した。

- ログイン履歴を確認し、不正ログインの痕跡がないか
- システムのログに不正アクセスを示す痕跡がないか
- 各システムのアカウント一覧に不正なアカウントが存在しないか
- ファイアウォールやプロキシのログを確認し、不正な通信がないか
- ウイルス対策ソフトやエンドポイント検出・対応（EDR）システムがアラートを出力していないか
- すでに侵害を受けているシステムからの通信が発生していないか

調査の結果、攻撃者がウェブシェルを操作し、複数のシステムに対する不正アクセスを行い、システムの構成情報が漏えいしている可能性が高いと判断した。

不正アクセスの対象にファイルサーバが含まれていることから機密性の高い情報や個人情報が漏えいした懸念もあり、アドバイザリーボードと大学との間で調査方針を検討・決定し、以下の内部調査を実施した。

これらのファイルサーバの監査ログを抽出するなどして調査を実施した結果、ファイルサーバに格納された機密性の高い情報や個人情報が漏えいした可能性はないと判断した。

7. 他機関との連携状況

不正アクセスの判明後、学外の機関と以下のように連携を行った。

7.1. 文部科学省

「大学等におけるサイバーセキュリティ対策等の継続的な取り組みについて（通知）」に基づき、不正アクセスに対応するとともに、発生の事実及びインシデント対応体制の構築について報告した。不正アクセスの調査およびサービス復旧について随時、報告および相談を実施した。また、類似の被害発生を防止するため、攻撃者が使用した不正プログラムやセキュリティベンダーの調査結果を共有した。

7.2. 個人情報保護委員会

不正アクセス発生後、個人情報が漏れた懸念があるため、「個人情報の保護に関する法律第２６条第１項」の規定により、2022 年 10 月 20 日、大学から個人情報保護委員会に報告した。その後の調査により、システム構成に関係する情報は漏えいした可能性があるが、個人情報に該当する漏えいはないと判断し、2023 年 3 月 23 日、個人情報保護委員会に報告した。

7.3. 警察

警察に不正アクセス発生について相談し、不正アクセスの手口に関する情報や使用された不正プログラムなどを共有した。

8. システム復旧に関する方針

今回の不正アクセスは以下の特徴がある。

・攻撃の起点が 2015 年であり、長期間不正アクセスの痕跡が発見されなかった。

・内部の重要なサーバが不正アクセスを受けており、システムの構成情報が攻撃者に把握されていた。

・AD サーバや LDAP サーバなどの認証および認可に関わるサーバが攻撃を受けており、認証や認可に関係する情報が漏れている可能性がある。

これらの攻撃の特徴を踏まえ、システム復旧は以下の方針に従って実施した。

8.1. 不正アクセス被害が確定しているシステムの復旧

不正アクセスの被害を受けた 13 台のうち、12 台は、発見されていない不正プログラムの残存の可能性を考慮し、全てシステム再構築を行い、攻撃の起点となった公開ウェブサーバ 1 台は廃止した。業務データを移行する際には以下の方針に従って再利用の可否を決め、そのうえで、移行する業務データは事前に複数のウイルス対策ソフトでスキャンを実施した。

再利用するデータ：アカウント名、画像データや文書ファイル
再利用しないデータ：被害サーバの OS、実行プログラム、パスワード

各システムの復旧方針は以下の通り。

表 3　システムの復旧方針

No	サーバ	対応
1	公開ウェブサーバ	廃止。同様の機能の提供については今後検討予定
2	シングルサインオンサーバ	システム構築時のバックアップデータを利用し再構築
3	LDAP サーバ	システム構築時のバックアップデータを利用し再構築
4	Proxy サーバ 1	システム構築時のバックアップデータを利用し再構築
5	Proxy サーバ 2	システム構築時のバックアップデータを利用し再構築
6	ファイルサーバ 1	システム構築時のバックアップデータを利用し再構築。データについては複数のウイルス対策ソフトでスキャンを実施した後に移行
7	ファイルサーバ 2	システム構築時のバックアップデータを利用し再構築。データについては複数のウイルス対策ソフトでスキャンを実施した後に移行
8	ファイルサーバ 3	システム構築時のバックアップデータを利用し再構築。データについては複数のウイルス対策ソフトでスキャンを実施した後に移行
9	死活監視サーバ	システム構築時のバックアップデータを利用し再構築
10	AD サーバ 1	システム構築時のバックアップデータを利用し再構築
11	AD サーバ 2	システム構築時のバックアップデータを利用し再構

		築
12	職員端末 1	新規端末を配布
13	職員端末 2	新規端末を配布

8.2. 不正アクセスの兆候が発見されなかったシステムの復旧

不正アクセスの兆候が発見されなかったシステムについては継続使用する方針とした。なお、今後の被害を防ぐため、次項の共通セキュリティ対策を実施した。

8.3. 共通セキュリティ対策

再構築したシステムおよび継続使用するシステムの両方に以下の対策を適用した。

- OS やアプリケーションを最新バージョンにアップデート
- アカウントの棚卸を実施（不要なアカウントの停止、権限の見直し、管理者パスワードの再設定）
- すべてのサーバとクライアント端末にエンドポイント検出・対応システム（EDR）を導入して、資産情報やインシデント情報を集中管理
- サーバに接続できる IP アドレスの制限
- 脆弱性診断ツールによるスキャンの実施

9. 被害を発生・拡大させた要因

2022 年 8 月末に発生した不正アクセスを発見後、大学の情報システムは機能を制限した状態で運営してきた。不正アクセスの調査や復旧作業の結果、2023 年 5 月 8 日に大学の情報システムの復旧が完了した[i]。不正アクセスの被害により、大学の情報システムが約 8 か月間、制限された状態で運営することになったが、その要因は以下の通りであったと考えられる。また、9 章の要因に対応するための対策を 10 章で記載した。

9.1. 組織的な要因

以下に組織的な要因を記載する。それぞれの要因の関係性は以下の通りである。

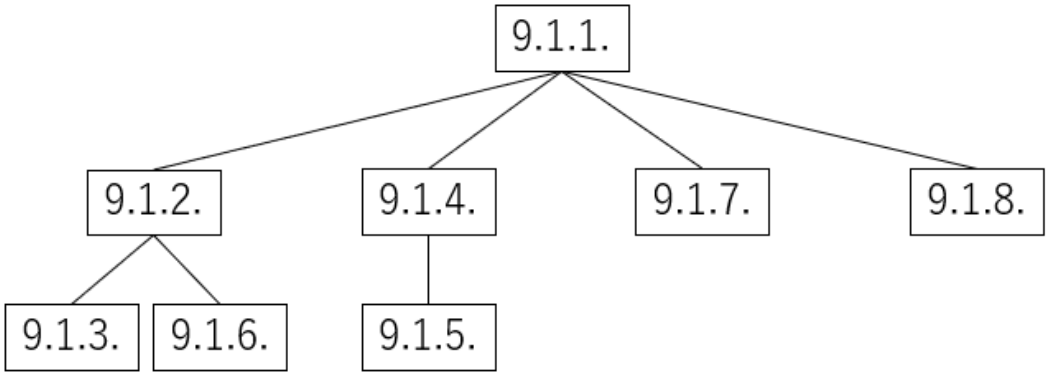

図 4　要因の関係性

9.1.1. 情報システムの企画・運営の軽視

大学全体において、情報システムの企画・運営が軽視されてきたことが不正アクセスの被害を発生、拡大させた大きな要因である。特に大学組織の運営を行う執行部の責任は重い。執行部は安全な情報システムを安定して運用するために、情報システムに関する予算だけではなく、運営を行う組織体制や人員の整備も含めて行う必要がある。

9.1.2. 情報システム担当者の不足

不正アクセス発生当時の情報システム担当者は 1 人であった。この情報システム担当者は総務部門との兼任となっており、実質的に 0.5 人の人員で情報システムの運営を行っていた。このような組織体制では大学の担当者が情報システムを企画・運営することは不可能であり、このため GRIPS の情報システムは運用委託先 IT ベンダーに、ほとんどを任せる形で運営されていた。また、運用委託先 IT ベンダーの管理・監督という重要な業務も十分に実施することができていなかった。

9.1.3. システム運用やセキュリティ運用を継続的に行う仕組みの欠如

2022 年 8 月に起きた本件以外にも過去にセキュリティインシデントが発生しており、その際にセキュリティベンダーが作成した調査結果のなかには、「システム的対策」や「組織的対策」の必要性を指摘するものも含まれていた。それらの対策のうち、「システム的対策」についてはある程度実施されていたが、「組織的対策」は全く実施されていなかった。過去に提示された対策が実施されていれば、本セキュリティインシデントの被害を軽減できていた可能性は高い。

また、文部科学省に提出している「サイバーセキュリティ対策等基本計画工程表」に体制整備や規程整備、人材育成などの項目が記載されていたが、計画のみで満足に実施されていない状態であった。このように大学内部にシステム運用やセキュリティ運用を継続的に行う仕組みが整備されていないことが本セキュリティインシデントにおける被害拡大につなが

った。

9.1.4. 情報システムの委託契約に関する不備・不足

2021 年 12 月から稼働している現在の情報システムの仕様書にセキュリティの要件に関する記載が不足していた。システム構築時に実施すべきチェック項目や既存データの移行を行う際に実施すべきセキュリティチェックの内容などについて具体的な項目が記載されておらず、委託先 IT ベンダーの善意に期待するものとなっていた。結果として 2015 年から配置されていた不正プログラムを現在のシステムまで持ち込むことになり、2022 年 8 月の不正アクセスの原因となった。

9.1.5. 情報システムの委託元としての管理不足

大学の情報システム運用は、システム構築を担当したベンダーの技術者数名が常駐する形で行っていた。情報システム担当者が大学側で不足しているため、情報システムの運用は、ほぼ全面的に委託先に依存していた。結果として、大学は委託元として適切な監督を実行することが困難な状況にあった。そのため、情報システムに求められる品質やセキュリティの観点から、運用委託先 IT ベンダーへ具体的な指示や要望を出す能力が欠如していた。これは、インシデント発生後の情報収集や対応に長い時間が必要となる結果を招いた。

加えて、定められた毎月のセキュリティチェックが実施されていなかったことも問題である。運用委託先 IT ベンダーが規定された運用項目を一部実施できていなかったため、日々変化するサイバーセキュリティの情報に対応し、脆弱性や設定漏れを未然に防ぐことができていなかった。大学及び運用委託先 IT ベンダーは早期に代替手段を確立し、セキュリティチェックを継続するべきであった。

9.1.6. 実効性のないインシデントレスポンス体制

2019 年に「政策研究大学院大学サイバーセキュリティ対策等基本計画」を作成し、その中に「実効性のあるインシデント対応及びセキュリティ・IT 体制の整備・充実」という方針を設定していた。しかし、CSIRT は設置されたが、メンバーの任命を行っただけであり、サイバーセキュリティに知見を持つ人員を含む体制ではなく、「実効性のある体制」となっていなかった。その結果、本インシデント発生後、不正アクセスの調査や分析、関係各所への連絡などのアクションの内容やスピードが十分ではなく、大学サービスの復旧に時間がかかる結果となった。

9.1.7. セキュリティに関する教育・訓練の未実施

執行部に対するセキュリティ教育が実施されていなかった。執行部は自組織に対するセキュリティ脅威を正しく認識し、監督官庁のガイドラインに対応する必要がある。そしてサイ

バー攻撃の事業への影響を最小限に抑えるための意思決定が可能となるよう、対策を学ぶことが求められる。執行部の人事異動後、セキュリティ教育が実施されていなかったことが過去のインシデントの対策を風化させた原因の一つである。

情報システム担当者に対するサイバーセキュリティについての組織的な教育・訓練が実施されていなかった。情報システム担当者が最新の情報を取得し、技術の向上を図るための支援体制が組織として整備されておらず、個々の担当者の自主的な努力に依存していた。日々のシステム管理業務に追われる情報システム担当者は、サイバーセキュリティの研修やセミナーに参加する余裕がないのが実情であった。

9.1.8. 情報システム部門以外のシステムの脆弱性

大学の基幹システムは情報システム部門が調達していた。一方、情報システム部門以外の部署が個別に情報システムを構築・運用しているものも存在しており、適切に管理されているとはいえないものが複数存在した。具体的には、運用状況が明らかでなかったシステムや、撤去されたセキュリティ機器に依存していたシステムなどが発見された。大学の情報システムの全体像を把握している部門が存在しなかったため、脆弱性が多数存在する状況となり、今回の情報セキュリティインシデントの原因調査や対応に時間を要した原因の一つとなった。

9.2. 技術的な要因

9.2.1. アカウントの棚卸が不十分

定期的なアカウントの棚卸が実施できておらず、大学職員が管理するアカウントと運用委託先 IT ベンダーが管理するアカウントの整理ができていなかった。このことから、利用していないアカウントが不正に利用される恐れがあった。また、本インシデント発生後にも、システム管理に使用するアカウントのパスワードリセットを行った際、大学が管理するアカウントのみパスワードリセットを行い、運用委託先 IT ベンダーが管理するアカウントのパスワードリセットができていなかった。その結果、攻撃者は運用委託先 IT ベンダーが管理するアカウントを悪用し、内部のサーバに不正アクセスを行うことができた。

不正アクセスの発生を契機に大学のシステムに存在するユーザ用アカウントの棚卸を行ったところ、存在するユーザ数をはるかに上回る数のアカウントが存在することが分かった。これらの休眠アカウントは不正アクセスにつながる可能性のあるものである。不要なアカウントを大量に維持することはセキュリティの観点や維持費用の観点からも望ましくない。

9.2.2. 資産管理の仕組みが不十分

大学が保有するハードウェアやソフトウェアを含む資産管理の仕組みが不十分であった。

守るべき資産の全体像を把握できていないことが、想定外の不正アクセスにつながる可能性がある。

不正アクセスの発生を契機に大学が保有するパソコンの棚卸を行ったところ、想定以上のパソコンを保有していることが分かった。管理できていないパソコンを多数保有することはセキュリティの観点や維持費用の観点からも望ましくない。

大学全体で使用するソフトウェアの管理も不十分であった。どのようなソフトウェアがどのくらい使用されているかという数の把握に加え、ソフトウェアのバージョン情報の管理ができておらず、非常に古いバージョンのソフトウェアが使用されている状態であった。古いバージョンのソフトウェアには深刻な脆弱性が発見されているものも多くあり、不正アクセスにつながる可能性のあるソフトウェアも多数存在した。

ハードウェアやソフトウェアの資産状況を可視化する仕組みがないため、その潜在的な問題を認知できない状況であった。その結果、大学の情報システムに潜在するセキュリティやコストに目を向けることがないまま、本インシデントの発生を招く結果となった。

9.2.3. 脆弱性管理の仕組みの不在

脆弱性管理の仕組みがなく、危険度の高い脆弱性をもつソフトウェアが多数存在しており、情報システム全体に対するリスクとなっていた。資産管理の仕組みが不十分であることから情報システムのソフトウェアのバージョン情報が管理されておらず、文部科学省や内閣サイバーセキュリティセンター（National Center of Incident Readiness and Strategy for Cybersecurity: NISC）が注意喚起したものに対する受動的な対処にとどまっていた。

サーバを含むシステムのなかには、例えばオンライン出願システムのように、構築時点においてサポートが切れた非常に古い PHP（ウェブアプリケーション開発に適したスクリプト言語。Personal Home Page or Hypertext Preprocessor）を使用しているベンダーの製品があり、構築当初から脆弱性を含むシステム構成となっていた。システム構築時点において何らかの回避策を講じるべき問題が含まれているにも関わらず、情報システムが運用フェーズに入った後にも脆弱性対策について協議・検討した記録は存在しなかった。

ユーザに配布されているパソコンにも多数の古いバージョンのソフトウェアが使用されていた。パソコンソフトウェアのアップデートは実質 Windows Update のみ行われている状態であり、OS 管理外のソフトウェアについてはユーザの自主的なアップデート運用に依存していた。非常に古い Java Runtime Environment（JRE）や Adobe Reader、Flash Player などが存在するパソコンもあり、セキュリティの観点から望ましくない状況であった。

9.2.4. ウイルスを含んだままコンテンツを移行

2015 年時点でウェブサーバに置かれたと思われる不正プログラム(ウェブシェル)が 2022 年のシステム移行を経て現環境のウェブサーバに設置されていた。システム移行時に旧環境のデータをコピーする作業マシンにウイルス対策ソフトが導入されており、チェックも行われたが、すり抜ける結果となっていた。ウェブシェルはウイルス対策ソフトに検知されないことも多く、サーバのウイルス侵入防止をウイルス対策ソフトのみに頼ることは危険である。当該サーバの運用には基本的な脆弱性対策やファイルの改ざん検知機能が欠けていた。

9.2.5. セキュリティの観点からログ分析を行うための体制の不在

日常的なログの参照がシステム障害防止の観点を中心として行われており、セキュリティの観点からログ分析を行う体制が整備されていなかった。本インシデントは、情報システム担当者がメンテナンス作業中に偶然不審なログに気づいたことがきっかけで判明した。情報システム担当者の少ないリソースだけで、日常的にログを手動で分析するのは現実的ではない。外部委託契約をしているセキュリティ・オペレーション・センター（SOC）サービス提供会社がエンドポイント検出・対応システム（EDR）の運用を行っていたがクライアントのみを対象とした限定的なものであり、大学全体のセキュリティを確保するために必要な運用は行われていなかった。

分析するべきログが集約されていなかったため、インシデント発生後に複数のシステムにログインして分析する必要があり、漏れが発生しやすい状況であった。また、それぞれのログ保存期間が統一されておらず、遠く遡って調査ができないものもあった。

9.2.6. 高機能なファイアウォールが十分活用されていない

情報システムのインターネット接続点に高機能なファイアウォールが導入されていたが、その機能が十分活用されていなかった。具体的には、セグメント分割や基本的なアクセス制御のみが実装されており、コンテンツのフィルタリングやセキュリティ機能が活用されていなかった。また、いわゆる「出口対策」（学外に出ていく通信を監視し、重要情報の漏えいやマルウェアによる外部との通信を防ぐためのもの）の機能の実装も不十分であった。

また、内部ネットワーク間のアクセス制御が実施されていなかった。その結果、1 台の公開ウェブサーバの不正アクセスを起点として、内部の複数のサーバに不正アクセスが行われた。内部ネットワーク間のアクセス制御が実施されていれば、被害の範囲を極小化することができた可能性が高い。

本来は IT とセキュリティの専門家である運用委託先 IT ベンダーがファイアウォールの適切な設定に関する提案を期待したいところであるが、その提案がなされた形跡はなく、「通信を通す」ことが優先された運用状態であった。システム運用を担当する運用委託先 IT ベンダーは「通信が行えること」をもって評価される傾向があるため、ユーザからの要望がない限りは「通信を止める」というセキュリティ機能より、「通信を通す」ことを優先しがちである。また、今回の事例では発注者である大学側からファイアウォールの適切な設定を求める直接的な指示はなかった。いずれにせよ、ファイアウォールを使用する時点で「通信を通すこと」と「通信を止めること」を同時に実装することが専門家には期待される。

9.2.7. サーバに接続可能な IP アドレスが制限されていなかった

情報システム担当者や管理者は、サーバコンピュータの画面を別のコンピュータに転送し、遠隔操作するための通信規約 SSH（セキュアシェル、Secure Shell）や RDP（リモートデスクトッププロトコル、Remote Desktop Protocol）を使用していたが、これらを用いたサーバへの接続に対するアクセス制御が、サーバごとではなく、複数のサーバを含むセグメントごとの実装となっていた。その結果、正規のアカウントを盗んだ攻撃者は学内の複数サーバを踏み台にしてセグメント内の他のサーバにログインすることができ、不正アクセスの範囲を広げた。ファイアウォールまたはサーバごとに、情報システム担当者の端末や管理者用ネットワークからのみ接続できるよう制限していれば、不正アクセス被害を受けたサーバから別のサーバにログインされることはなかった。

10. 再発防止のための対策

今回の不正アクセスを可能にした要因を踏まえ、今後、同様のインシデントを発生させないための対策を以下に整理した。加えて、すでに大学で実施した内容についても記載した。

10.1. 組織的な対策

10.1.1. 大学執行部のセキュリティ体制の強化

大学執行部は大学の教育と研究および事務活動を滞りなく行うため、情報システムを安全に維持運用する責任がある。大学は学生や職員のものだけでなく、学外の関係組織の重要情報を保持しており、これらの情報を安全に保管する責任がある。特に政財官界において重要な地位に就いている、あるいは就いていた人物が大学に着任していることもあり、その情報が狙われる危険性についても認識するべきである。今後、同様の不正アクセスによる被害を起こさないため、情報セキュリティ総括責任者（CISO）を中心として情報システムに関する運営体制や予算編成を見直す必要がある。情報システムや情報セキュリティに熟知した人物の確保は多くの組織で課題となっているところであるが、そのような人物を学内に配置するのが望ましい。また、学内の教職員だけでカバーしきれない部分については、学外組

織との協力を視野に入れる必要がある。

[大学の対応]
米国立標準技術研究所（National Institute of Standards and Technology: NIST）が作成したサイバーセキュリティフレームワーク（Cyber Security Framework: CSF）などを参考にし、大学による今後の組織的・技術的な対策を包括的に検討・整理し、計画を立てた。その対策の一環として、大学執行部の体制を以下のように強化した。
・セキュリティアドバイザー機能の強化
・CISO 補佐の任命
・情報システム担当チームをサポートするコンサルタントの契約

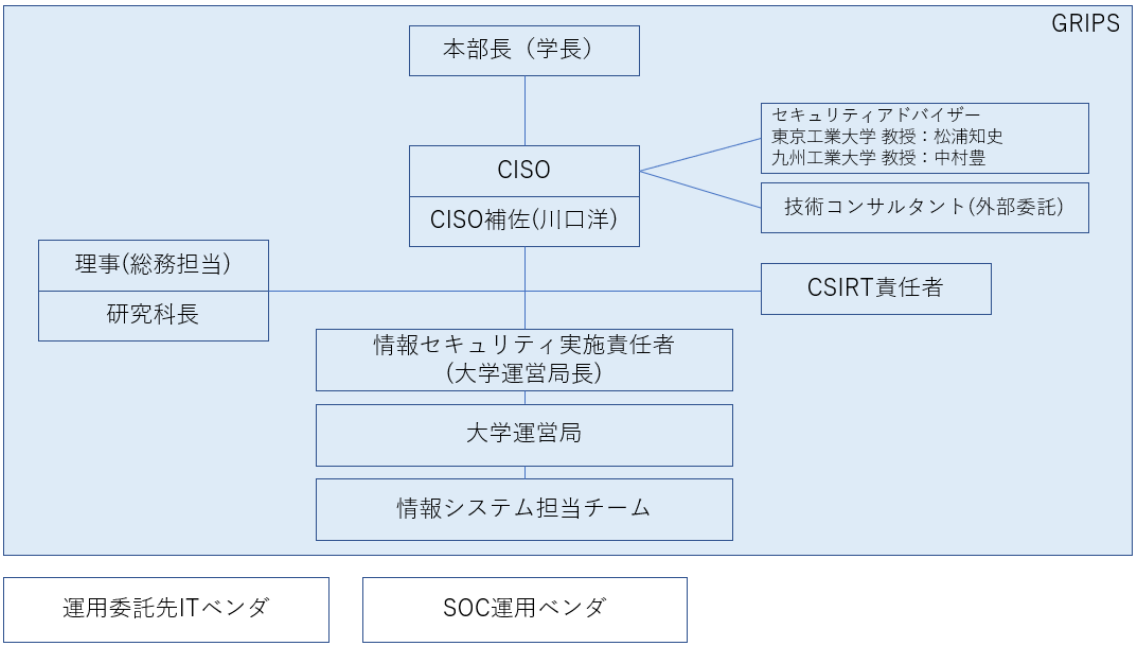

図 5　2023 年 4 月以降の GRIPS の体制図

10.1.2. 情報システム担当チームの強化

大学執行部は複数名の情報システム担当者を配置し、情報システム担当のチームを設置するべきである。大学の情報システムを運用委託先 IT ベンダーに、ほぼ全面的に依存している状態を是正するためには、運用委託先 IT ベンダーを管理・監督する時間を捻出する必要がある。また、情報システム担当者が研修受講や健康上の理由などから職場を不在にした場合でも、複数名で相互にサポートすることで対応できる体制が必要である。過去のインシデント発生時にも再発防止策として挙げられている「情報システム部門の体制強化」を今こそ実現させなくてはならない。

[大学の対応]
情報システム担当者を増員し、4 人のメンバーで情報システム担当チームを組織した。

10.1.3. 継続的な運用体制の整備

本不正アクセス事件を受けて、大学執行部は組織の運用体制を見直し、今回施行された対策が長期間にわたって維持されるようにする必要がある。大学執行部の関与がなければ、古い脆弱な運用体制に戻る可能性があることを認識するべきである。具体的には今回整備した対策の実施状況を定期的にチェックし、必要に応じて見直しを行うことを推奨する。

大学内におけるセキュリティ運用体制と文化の風化を防ぐため、大学としては四半期ごとに最低でも一度、文部科学省へセキュリティ対策の進行状況を報告することが必要である。その際に、他大学で発生しているセキュリティインシデントや情報システムの調達に関する情報交換を実施することも重要である。なお、文部科学省への報告には以下の内容を含めることを推奨する。

- ・組織体制の変更
- ・セキュリティ対策の推進
- ・サイバー攻撃の発生状況
- ・外部委託事業者の管理状況
- ・大学執行部のセキュリティ関連会議への出席状況
- ・サイバーセキュリティ対策等基本計画実施状況

[大学の対応]
大学執行部は情報システム担当チームから毎月情報システムの運用状況の報告を受けることを決めた。報告会にはセキュリティアドバイザーおよび CISO 補佐も同席し、大学のセキュリティの現状について議論を行う。報告には以下の内容が含まれる。

- ・当月のシステム運用状況
- ・当月に発生した大学のセキュリティアラートの内容
- ・現在のセキュリティ上の問題点
- ・情報システムの運用に関する相談事項

なお、報告内容については、必要に応じて毎月見直しを実施していくものとする。

また、四半期に一度、文部科学省に対して大学のセキュリティ運用状況について報告することとした。

10.1.4. 次期システムにおける契約内容の整備

大学は内部に対する情報サービス提供のため、情報システムの管理および監督を主体的に

行うべきである。また、適切な予算枠内で情報システムを調達、構築、運用する責任も大学には求められる。2021 年から稼働を開始した現行の情報システムの更改時期を考慮し、次期システムの仕様策定を前倒しで開始することを強く推奨する。

[大学の対応]
現在の情報システムの更改時期は 2026 年 12 月である。従来は 2024 年後半より次期システムの仕様策定を行う予定であったが、今次インシデントの経緯を踏まえて前倒しで実施することとした。具体的には 2023 年内に他大学の外部有識者やシステムインテグレートを専門とする外部専門家の協力を得て実施する次期システム検討委員会（仮）を設置し、次期システムに求められる機能やシステム仕様について検討を行う予定である。

10.1.5. 情報システムの委託元としての管理責任の執行

大学は情報システムの管理についての責任を全うするべきであり、その運用を委託している運用委託先 IT ベンダーと協力しつつ、適切な体制を確立すべきである。情報システムの全ての運用業務を運用委託先 IT ベンダーに依存するという状況は避けなければならない。さらに、運用委託先 IT ベンダーとの取り決めが実際の運用において確実に遵守されていることを委託者として確認することが求められる。

[大学の対応]
情報システムの仕様書に定めた運用項目で実施されていないものがないかを確認した。そのうち実施されていないものについては今後実施するよう運用委託先 IT ベンダーに申し入れを行い、合意した。情報システムの技術的制約により実施できない項目については別途調整を行うこととした。

10.1.6. インシデントレスポンス体制の整備

大学執行部は実効性のある CSIRT 体制の整備を行う必要がある。CSIRT のメンバーにはサイバーセキュリティに知見をもつ者を含めるべきである。さらに、CSIRT の有効性を維持・強化するためには、定期的な研修への参加や勉強会の開催、最新情報の収集などを可能とする体制が必要となる。

[大学の対応]
人事異動に合わせ CSIRT メンバーの見直しを行った。大学内にはサイバーセキュリティに知見をもつ者が少ないため、セキュリティアドバイザーや CISO 補佐と連携して対応する体制とした。

平時には以下のような活動を行っている。

- 情報処理推進機構（Information-technology Promotion Agency: IPA）や JPCERT コーディネーションセンター（JPCERT/CC）が発信している脆弱性情報についての意見交換
- サイバー攻撃や対応策などセキュリティに関する幅広い話題の共有
- 重大なセキュリティインシデントが発生した場合に発表される事故調査報告書の読み合わせ
- システム運用に関する情報交換

10.1.7. 情報セキュリティ教育の実施

執行部は大学経営陣の情報セキュリティに関する研修を企画すべきである。この研修は、自組織に対するセキュリティ脅威を正しく認識できるようにするため、また監督官庁のガイドラインに対応するために必要となる。さらに、大学経営陣は、サイバー攻撃の事業への影響を最小限に抑えるための意思決定が可能となるよう、対策を学ぶことが求められる。

加えて、大学執行部は情報システム担当者が IT 技術やサイバーセキュリティに関する知見を獲得・更新する必要性を認識し、教育および研修の機会を提供すべきであるとの立場を明確にするべきである。情報システム担当者は文部科学省や公的機関が開催する研修、または民間コミュニティのイベントなどに参加し、最新情報や知見の共有に努めることが期待される。

[大学の対応]

大学は、執行部および情報システム担当チーム向けに CISO 補佐による「一般公開されている事故調査報告書の読み合わせ会」を実施し、今後大学で発生する可能性のある問題について議論を行った。大学は今後も執行部向け、情報システム担当チーム向け、一般職員向けに職務に応じた研修の機会を提供する。

大学は情報システム担当者を増員し、情報システム担当チームを設立することで、研修参加に必要な時間的余裕を確保した。さらに、情報セキュリティ教育に関する予算を年間計画に組み入れている。

10.1.8. 大学内の情報システムの把握と管理方針の見直し

大学の情報システムには情報システム担当チームが管理するものだけでなく、各課で個別に調達・運用されているものも存在するため、これらの情報システムについても適切に管理し、インシデントの発生を抑制することは極めて重要である。大学執行部は情報システム担当チーム以外の管理下にある情報システムを把握し、これらの情報システムに対するセキュリティ上の問題が発生しないような体制とルールの整備を進めるべきである。

[大学の対応]
各課が個別に調達しているシステムについては、情報システム担当チームが、システム名、導入業者、管理業者、保守契約・内容、システム構成、セキュリティ対策、アップデート体制等についてのヒアリングを実施し、全体像を把握した。また、各課の情報システム担当者を明確化した。今後は各課の情報システム担当者に対しても、セキュリティ情報の提供を行う予定である。セキュリティを確保した運用が各課で難しいと判断される場合は、情報システム担当チームがその情報システムの管理を引き受けることを検討する。

10.2. 技術的な対策

10.2.1. 全システムのアカウントの棚卸

大学が所有する全てのハードウェアおよびソフトウェアのアカウントの棚卸を実施するべきである。特に管理者用アカウントが漏えいしないように注意する必要がある。また大学の情報システム担当者が使用しているアカウントだけではなく、運用委託先 IT ベンダーが使用しているアカウントについても漏れなく把握することが重要である。

また、①アカウントの棚卸実施後、不要なアカウントや不審なアカウントがないかについて確認し、②棚卸を期に修了生や退職したユーザのアカウントの取り扱いルールを見直し、③インターネットから接続可能なアカウントやシステム管理者用アカウントについては重点的に確認し、④これらのアカウントには多要素認証の適用も検討すべきである。

[大学の対応]
情報システム担当チームが管理する全ての機材の棚卸を実施後、アカウントの棚卸を実施した。不要なアカウントや休眠アカウントについては無効化または削除した。

メールやファイルサーバにアクセスするためのユーザアカウントは全てパスワードをリセットした。また、インターネットから接続可能となる全てのアカウントに多要素認証を適用した。

修了生や退職者アカウントの管理基準については今後検討する。

10.2.2. 資産管理の仕組みを再構築

大学が所有するハードウェア資産の管理台帳を作成し、定期的にハードウェア資産を棚卸することが重要である。加えてソフトウェアのバージョン情報を収集し、古いバージョンのソフトウェアを把握および更新できるように、可能な限り一元管理する方法を検討すること。

[大学の対応]
既存のハードウェアの資産台帳の項目を見直し、最新の状態にアップデートした。

ソフトウェアの資産管理はシステム管理用ツールおよびエンドポイント検出・対応（EDR）システムをサーバおよびクライアント端末にインストールし、情報を集約する仕組みを構築した。

また、GRIPS のクライアント端末に米国の電気電子学会（Institute of Electrical and Electronics Engineers: IEEE）の認証規格である IEEE 802.1X 証明書を導入し、証明書をもつ端末のみが学内ネットワークに接続できるようにした。

10.2.3. 脆弱性管理の仕組を構築

脆弱性情報を能動的に集める運用を構築することが重要である。最低限、情報処理推進機構（IPA）や JPCERT コーディネーションセンター（JPCERT/CC）が発信する情報を確認し、大学で使用するソフトウェアに関係するものがないか確認することが求められる。脆弱性情報と資産管理システムで収集した情報をマッチングし、大学のシステムに影響する脆弱性がないかを評価するべきである。

[大学の対応]
IPA や JPCERT/CC が発信する脆弱性情報を確認し、情報システムに影響がないか確認する運用体制を整備した。また、セキュリティアドバイザーや CISO 補佐と脆弱性に関する情報交換をする手段を確保した。

情報システム内をスキャンし、脆弱性を持つバージョンのソフトウェアがインストールされているものを可視化し、対応する運用体制を確保した。サーバにインストールされているソフトウェアに脆弱性が含まれているものについてはアップデートを行った。また、クライアント端末のアップデート方針についても今後検討する予定である。

10.2.4. コンテンツ移行時のウイルスチェック実施

システム移行の際に複数のウイルス対策ソフトを使用して移行コンテンツのチェックを行うべきである。また、移行対象ファイルの種類を制限することも検討が必要である。

[大学の対応]
システム移行の際に移行コンテンツのチェックを行うことや移行対象ファイルの種類の制限を実施することなどを次期システム構築の仕様書に盛り込むことを申し送り事項として

決定した。

10.2.5. ログ分析運用体制の整備

各種システムに分散しているログを集約・保存・分析する仕組みを構築する必要がある。その際にサーバとクライアント端末の両方のログの集約を視野に入れた仕組みにするべきである。また、リアルタイムに検索をするための保存方法とアーカイブ目的での保存方法のバランスを考慮しつつ、コストと運用リソースを踏まえて検討するのが好ましい。

文部科学省や JPCERT/CC が提供する情報をソースとして分析フローを構築し、大学に対する不正アクセスの発見に努めることが重要である。また、セキュリティ確保のためのログ分析は従来通り外部のセキュリティ・オペレーション・センター（SOC）サービスの活用も視野に入れて検討すべきである。

[大学の対応]

大学内に存在するログをログサーバに集約し、約 1 年にわたり保存できる仕組みを構築した。クラウドサービス側のログは今後別途集約する仕組みを構築する予定である。また、大学内のログサーバとクラウドサービス側のログサーバの統合についても今後検討する予定である。

ファイアウォールとエンドポイント検出・対応システム（EDR）のログを外部 SOC サービスと共有し、常時監視を行う体制を構築した。現在までインシデント対応が必要となる事象は発生していないが、SOC サービスから提供される月次レポートを確認し、CISO 補佐やセキュリティアドバイザーにも共有する運用にしている。

10.2.6. 主体的なファイアウォール運用管理

ファイアウォールの機器の操作は、運用委託先 IT ベンダーが行う場合においても大学が主体的にその設定を管理することが重要である。大学は、どのような通信を遮断し、チェックするかという方針を決めることを怠ってはならない。高機能なファイアウォール機器を有効活用するため、ネットワークセグメントの見直しや内部ネットワーク間通信の制限、実装されているセキュリティ機能の活用を行うことが必要である。

[大学の対応]

セキュリティアドバイザーや CISO 補佐と相談しつつ、ネットワークセグメントの見直し、内部ネットワーク間のアクセス制御などを実施した。また、高度なファイアウォールの機能を十分に活用するため、ファイアウォールの設定の際は運用委託先 IT ベンダーとファイアウォールの機器メーカーの協力を得て、設定内容を確認した。

10.2.7. サーバに接続可能な IP アドレスを制限

サーバコンピュータの画面を別のコンピュータに転送・遠隔操作するための SSH（セキュアシェル）や RDP（リモートデスクトッププロトコル）などを利用してサーバのリモートメンテナンスを行う際は、接続可能なネットワークを十分に制限すべきである。また、インターネット経由での直接アクセスは原則禁止とすべきである。

[大学の対応]

大学の基幹システム内のファイアウォールおよびサーバ自体のファイアウォール機能を活用し、サーバに接続できる IP アドレスを情報システム担当者が管理する特定ネットワークに限定した。

11. 文部科学省に対する期待

他の小規模な大学や文系大学においても同様のインシデントが発生し、大学の運営に留まらず、場合によっては広く社会に影響を及ぼすことが想定される。各大学における自助努力による対策推進は当然のこととして、文部科学省には以下の役割を期待したい。

11.1. インシデント発生時のフォローアップ

インシデント発生時の対策には多様な手段が想定されているはずである。しかし、実際のところ、人事異動などにより、これらの対策の実施が中断されるケースがある。文部科学省にはインシデント発生後の対策が適切に継続されているかフォローすることを期待したい。

11.2. 小規模大学や文系大学に対する支援強化

小規模大学や文系大学では情報システム部門が少人数で運営されており、一般的に推奨される対策を実施できない場合が多い。文部科学省には小規模大学等がインシデントの対応が可能となる適切な体制整備への指導・強化を期待したい。

11.3. インシデント対応訓練や演習

インシデント対応の重要性は広く認識されているが、現実に経験を蓄積する機会は稀である。多くの大学においては、このインシデント対応の経験の少なさが課題となっている。これを補うため、文部科学省には大学や学術機関のためのインシデント対応訓練や演習の受講促進を期待したい。

12. 大学のインシデント対応およびシステム復旧に関する評価

12.1. 政策研究大学院大学　情報セキュリティアドバイザー　松浦 知史（東京工業大学 学術国際情報センター 教授）

標的型攻撃と呼ばれる高度で執拗なサイバー攻撃を防ぐことはどのような組織でも困難である。また、サイバー攻撃が発生する事を前提としたセキュリティ体制を整えておかないと被害が大きく拡大する。これらの事は一般的なセキュリティの話題として広く知られている。知られてはいるが実際に十分な体制を整えられている組織は少なく、大学はその傾向が強い。そして本件はまさに上記の様な典型的かつ深刻なセキュリティ事案であり、被害が大きく膨らんだ。対外線（インターネット接続）の全遮断に始まり多くのサービスが停止に追い込まれ、全学の学生および教職員が日常的な学習や業務を行うにあたり不便な状況が数ヶ月にも渡って続く事態となった。

大学側が抱えていた問題点や今後の対策に関しては 9 章、10 章を参照していただきたい。多くの反省すべき点はあるものの大学の自助努力のみに頼るのも限界がある。サイバー攻撃は年々高度化および多様化し、加えてセキュリティサービスや機器の価格上昇が継続しており、相対的に大学が利用可能な予算は減少し続けている。結果として、現状のサービスを維持する（＝動けば良く安全は顧みられない）方向に強いバイアスがかかっている。大学を取り巻く環境は構造上セキュリティリスクが高まる状況にある事を改めて認識し、大学自身はもちろんの事、文部科学省はじめ政府機関も一体となって状況の改善に努めるべきである。

12.2. 政策研究大学院大学　情報セキュリティアドバイザー　中村 豊（九州工業大学 情報基盤センター 教授）

全学の通信遮断までの意思決定の判断は妥当だったものの、そこから先の事故対応については大学側の経験不足、認識不足、知識不足が露呈したものとなってしまった。その結果、長期間に及ぶ通信遮断が生じ利用者に不利益を強いる結果となった。現状は IT チームが整備されつつあるが、大学が自走していくには不十分であると思われる。継続した人員確保と体制整備が必要であり、それに伴う予算措置も必要であると思われる。

12.3. 政策研究大学院大学　CISO 補佐　川口 洋（株式会社川口設計 代表取締役）

不正アクセス発生からサービス復旧まで多くの時間とコストを費やす結果となった。現在は情報システムを安定的に運用できる最低限の体制が整備されたと評価する。現在の大学の体制が一過性のものとして風化することなく、今後も継続し、改善していくことを期待したい。

[付録 1]セキュリティ侵害インジケーター（IoC）情報

本インシデントに関係するセキュリティ侵害インジケーター（Indicator of Compromise: IoC）を以下に記載する。これらの IoC は本インシデントの調査過程において発見されたものであり、他組織のセキュリティ対策の一助となれば幸いである。

マルウェア関連のファイル名とハッシュ値

攻撃者が使用したマルウェアや攻撃ツールのファイル名およびハッシュ値を以下に示す。

表 4　マルウェア関連のファイル名とハッシュ値

	ファイル名	SHA1	備考
1	shibata.php	a2d50968848247bcd8e72e9d8ca423cd1ee55ca1	ウェブシェル
2	www.php	8ad0333001773772f670703b2f611b25e0fc4e61	ウェブシェル
3	yutakab.php	2a021579f3cf36938da97d4ddeb42e6d28f57dd6	ウェブシェル
4	/tmp/CCCCCCCC	a117a9feb25302f09974ba1d23af31e734511d58	バックドア
5	/tmp/fs	a6982976e8ac97cdf3dcd0be81307fee714c47c2	ネットワークスキャンツール
6	/tmp/.ICE-unix/fs	a6982976e8ac97cdf3dcd0be81307fee714c47c2	ネットワークスキャンツール
7	pdf1.pdf	c8403f83fc7ba4f305658205a9656546e7e4ffe2	ウェブシェル（一時ファイル名）
8	phpeeIq4m	c8403f83fc7ba4f305658205a9656546e7e4ffe2	ウェブシェル（一時ファイル名）
9	php689NkQ	c8403f83fc7ba4f305658205a9656546e7e4ffe2	ウェブシェル（一時ファイル名）
10	phpWbNVNG	a8060e138ca946f3d4d268a75ae187f2f6e73d63	ウェブシェル（一時ファイル名）
11	phpoLolyI	c8403f83fc7ba4f305658205a9656546e7e4ffe2	ウェブシェル（一時ファイル名）
12	phpOl7Nyv	3961188b3f63abf7fec74089787d76964fe647f9	ウェブシェル（一時ファイル名）
13	dwmgr.exe	e6819d430b7e7ee758f9220d2081cdb2a5dd029d	正規の RAR（ラー。Roshal Archive）圧縮ツール
14	CCCCCCCCCCCCCCC	221ba9dc686ab799e318167e3fa99ad1db8dc2c8	バックドア
15	tsvipsrv.dll	f438c173663c987226df6fcde535c2c39134585e	ローダー（loader）
16	desktop.tmp	abc1ede7d60b3e2e3c746e7e66f0c485e167557b	暗号化されたコバルトストライク（Cobalt Strike）
17	desktop.dat	abc1ede7d60b3e2e3c746e7e66f0c485e167557b	暗号化されたコバルトストライク
18	linkinfo.dll	69bdcf14bba703287b7e5d3ac720c3d44e0d3c9d	画面キャプチャ・キーロガー
19	manhttp.bak	9f1680ed351485edca9b8db308eba535440d369d	ウェブシェル

IP アドレス

攻撃者が通信に使用した IP アドレスを以下に示す。

表 5　攻撃者が使用した IP アドレス

IP アドレス	IP アドレスの概要
103.177.44[.]20	ウェブシェルのアクセス元 IP アドレス
13.212.160[.]105	ウェブシェルのアクセス元 IP アドレス
20.78.60[.]69	ウェブシェルのアクセス元 IP アドレス
60.249.38[.]63	ウェブシェルのアクセス元 IP アドレス
45.56.152[.]242	ウェブシェルのアクセス元 IP アドレス
167.179.97[.]111	ウェブシェルのアクセス元 IP アドレス
119.81.184[.]3	ウェブシェルのアクセス元 IP アドレス
172.93.221[.]172	ウェブシェルのアクセス元 IP アドレス
1.234.69[.]73	ウェブシェルのアクセス元 IP アドレス
128.90.74[.]107	ウェブシェルのアクセス元 IP アドレス
103.142.141[.]85	ウェブシェルのアクセス元 IP アドレス
3.37.174[.]15	バックドアの接続先
13.251.45[.]147	バックドア(Cobalt Strike)の接続先

[付録 2]不正アクセスの詳細な流れ

不正アクセスの詳細な流れを以下に示す。

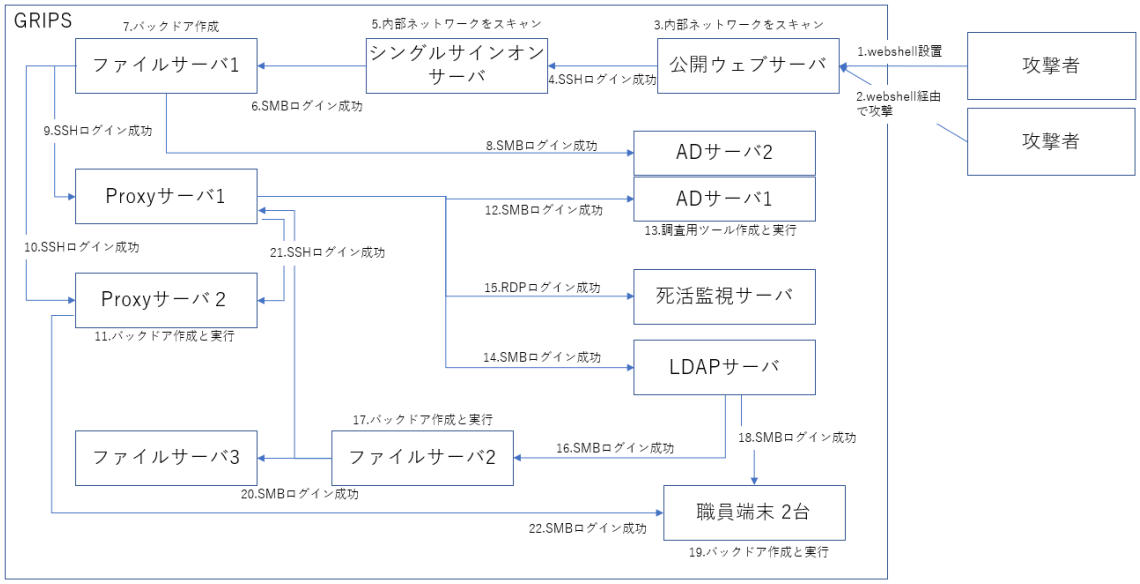

図 6 不正アクセスの流れ

不正アクセスの時系列の記録を以下に示す。不正アクセスの流れの図にある数字が以下の表の数字と対応している。

表 6　不正アクセスの時系列の記録

	日時(JST)	対象システム	攻撃内容
1	2015-04-13 11:40:12	公開ウェブサーバ	ウェブシェル設置
2	2022-08-24 00:21:15	公開ウェブサーバ	ウェブシェル経由で攻撃
3	2022-08-28 13:40:15	公開ウェブサーバ	内部ネットワークをスキャン
4	2022-08-28 15:28:40	シングルサインオンサーバ	SSH ログイン成功
5	2022-08-28 15:43:49	シングルサインオンサーバ	内部ネットワークをスキャン
6	2022-08-28 18:53:05～ 2022-08-28 19:19:55	ファイルサーバ 1	SMB ログイン成功（Server Message Block: Windows のネットワークでファイルやプリンター共有を行うための通信プロトコル）
7	2022-08-28 19:12:23～ 2022-08-28 19:12:53	ファイルサーバ 1	バックドア作成

8	2022-08-28 20:26:36	AD サーバ 2	SMB ログイン成功
9	2022-08-28 21:30:48	Proxy サーバ 1	SSH ログイン成功
10	2022-08-28 21:31:04	Proxy サーバ 2	SSH ログイン成功
11	2022-08-28 21:34:28	Proxy サーバ 2	バックドア作成と実行
12	2022-08-28 22:37:02～ 2022-08-29 04:07:29	AD サーバ 1	SMB ログイン成功
13	2022-08-29 01:05:36	AD サーバ 1	調査用ツール作成と実行
14	2022-08-29 03:01:48	LDAP サーバ	SMB ログイン成功
15	2022-08-29 03:49:12	死活監視サーバ	RDP ログイン成功
16	2022-08-29 19:28:56～ 2022-08-29 19:29:24	ファイルサーバ 2	SMB ログイン成功
17	2022-08-29 19:29:15～ 2022-08-29 19:29:24	ファイルサーバ 2	バックドア作成と実行
18	2022-08-30 13:09:03	職員端末	SMB ログイン成功
19	2022-08-30 13:12:49～ 2022-08-30 13:24:36	職員端末	バックドア作成と実行
20	2022-08-31 00:01:25	ファイルサーバ 3	SMB ログイン成功
21	2022-09-02 18:49:19～ 2022-09-02 18:58:00	Proxy サーバ 1	SSH ログイン成功
22	2022-09-02 19:33:45 2022-09-02 19:46:39	職員端末	SMB ログイン成功

[i] https://www.grips.ac.jp/jp/news/20230508-0190/