京都大学における情報セキュリティ自己点検の実施状況

山口 倉平 [1)], 戸田 庸介 [1)], 片桐 統 [1)], 石橋 由子 [1)]

1) 京都大学 情報部

i-s-office@iimc.kyoto-u.ac.jp

A report of Information Security Self-Inspection at Kyoto University

Souhei Yamaguchi [1)], Yosuke Toda [1)], Osamu Katagiri [1)], Yoshiko Ishibashi [1)]

1) Information Management Department, Kyoto University.

概要

京都大学は約 60 の部局から構成され、約 34,000 名の構成員が在籍している。2022 年度には、グローバルアドレスを持つ機器は約 1,200 台、研究室や事務室毎に構成するプライベート VLAN は約 3,900、サブドメインは約 200 個にのぼり、それぞれの管理者が必要な情報セキュリティ対策を実施している。情報セキュリティの自己点検は情報セキュリティポリシー及び関連規程の実施状況を点検するとともに、情報セキュリティ対策の向上を図り情報セキュリティインシデントの発生を未然に防ぐため対策基準にて定めて実施している。2016 年度より全学的な情報セキュリティの自己点検計画を明確にして実施し改善を行っている。2020 年度には一巡目で行った自己点検全体のテーマやサイクルの評価、見直しを行っている。本稿では、近年の自己点検の取り組みと点検結果、および取り組みについての考察を述べる。

1 はじめに

京都大学（以下、「本学」という。）では、情報セキュリティポリシー及び関連規程の実施状況を点検するとともに、情報セキュリティ対策の向上を図り情報セキュリティインシデントの発生を未然に防ぐため、情報セキュリティの自己点検を実施するよう情報セキュリティ対策基準にて定めている。

2016 年度より情報セキュリティの自己点検[1]について、最高情報セキュリティ責任者（情報基盤担当理事）が全学的な点検計画を明確にし、点検のテーマやサイクルを定めて、情報セキュリティ対策の向上を図っている。これまで 4 種類のテーマに沿って、年度ごとに異なる点検を実施しており、2020 年度からは点検サイクルが二巡目となることから、一巡目で行った自己点検全体のテーマやサイクルを評価し、点検項目の見直しや回答方法の改善に繋げることとした。

本稿では、2020 年度から 2023 年度の自己点検のテーマと、それぞれの点検の概要と結果、最後に自己点検の考察について述べる。

2 京都大学のネットワーク環境

本学では、学内に整備しているネットワークを KUINS （Kyoto University Integrated information Network System）と呼び、学外からもアクセスが必要なサーバ等はグローバルアドレスを持つ KUINS-II、研究室や事務室に設置される端末等はプライベート VLAN の KUINS-III に接続する構成になっている。

教職員が KUINS を利用する際には、KUINS 接続機器登録データベース（以下、「KUINS-DB」という。）から申請手続きを行う必要がある。（図 1）

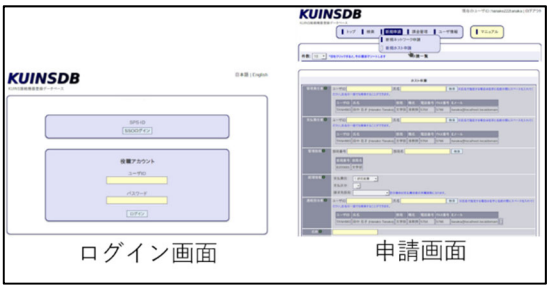

図 1 KUINS-DB

また KUINS-DB は、新規利用時の申請以外に利用中の申請内容の確認、変更、削除、過去の申請内容の検索、課金情報や請求額の閲覧といった機能を有している。

3　自己点検のテーマと計画

計画で策定した自己点検のテーマを表 1 に示す。

表 1　自己点検のテーマ

年度	点検テーマ			
	KUINS-II	KUINS-III	サブドメイン	全構成員
2016	○			
2017		○		
2018			○	
2019				○
2020	○	△(一部)		
2021	○	○		○
2022	○	○	○	○
2023	○	○		○

△：KUINS-III の NAS（ファイルサーバ等）の点検

2016 年度には、外部からの攻撃にさらされるリスクが高い KUINS-II 接続機器の点検を実施し、2017 年度には KUINS-III の点検、2018 年度にはサブドメインの点検、2019 年度には構成員の個々の自己点検を行った。当初 2020 年度以降も、4 種類のテーマを 4 年サイクルで順次実施する計画としていたが、2021 年度からは KUINS-II、KUINS-III、全構成員向けの点検は、継続して実施することでセキュリティ対策の向上につながると判断し、毎年実施するよう計画を見直した。

毎年実施するにあたって、点検者の作業負担を軽減するために、KUINS-DB にセキュリティに関する項目と管理状況を確認する機能を追加するよう改修した。点検の詳細や改修内容については 4 章以降で説明する。

4　KUINS-II（グローバルアドレス）を持つ機器の総点検

4.1 点検の概要

2020 年度からは、KUINS-II（グローバルアドレス）を持つ機器（2020 年度は約 2,000 台）の状況を確認する自己点検を実施した。

主な点検項目は以下のとおりである。

- 登録情報の確認
- 機器の利用目的
- 要保護情報の取り扱い
- 個人情報取り扱い件数
- 機器の設置場所
- 主体認証と管理権限
- データのバックアップ
- ログの取得と保存
- ソフトウエアのアップデート
- 不正プログラム対策
- サービス不能攻撃対策

2016 年度は点検者が KUINS-DB の登録内容を確認した後に、別途回答用アンケートフォームにて回答する必要があった。二度手間となっていたため、アンケートフォームで確認していた内容を KUINS-DB から回答するように導線を見直した。

まずは、KUINS-DB に本学の対策基準等で実施が求められている内容をもとにしたセキュリティ要件の項目を追加し、点検の結果をチェックすることにした。（図 2）

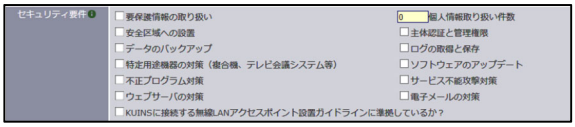

図 2 セキュリティ要件

また、管理状況確認日の項目を追加し、点検者が確認日を登録することで、点検完了とすることにした。（図 3）

図 3 管理状況確認日

4.2 点検の結果

点検状況について、表 2 に示す。

表 2　点検状況

年度	点検状況		
	対象機器	回答済	削除申請
2020	2,077	1,484 (96.3%)	517 (24.9%)
2021	1,375	960 (82.6%)	176 (12.8%)
2022	1,268	989 (90.1%)	153 (12.1%)

点検回答済の機器のうち、機器の利用目的について、表 3 に示す。

表 3　機器の利用目的

年度	Top 3				
	Web	遠隔会議	メール	その他	未回答
2020	275	149	75	439	592
2021	124	132	40	421	263
2022	147	82	38	379	276

- 利用目的は、Web サーバが最も多く、次いで遠隔会議（TV 会議システム）用、メールサーバである
- その他の利用目的は、業務サーバ、研究用サーバ、ssh サーバ、VPN サーバ、認証サーバ、プロキシサーバ、データベースサーバ、DNS サーバ等である
- 複数の利用目的を兼ねているサーバが約 5%あった
- Web サーバの減少は、情報環境機構の Web ホスティングサービス等の外部レンタルサーバへの移行が要因と思われる
- 遠隔会議の減少は、Google Meet や Zoom 等の Web 会議システムの利用により、不要となった影響と思われる
- メールサーバの減少は、情報環境機構のメールホスティングサービスへの移行により、部局独自ドメインのメールサーバが不要となったものと思われる

この点検により、機器の登録情報や問題のある設定等の見直しが行われただけでなく、セキュリティ対策が十分でない可能性が高い未使用機器や不要となった機器が 2020 年度は点検対象機器全体の約 25%が、2021 年度、2022 年度は約 12%が廃止されている。情報セキュリティインシデントの発生を未然に防ぐという観点からは、例年点検を行うことが効果的である。

5 KUINS-III（プライベート VLAN）の総点検

5.1 点検の概要

2021 年度からは、端末が接続されるネットワークの状況を確認するため、研究室や事務室毎に利用される KUINS-III VLAN（2021 年度は約 3,800）を対象に点検を実施した。主な点検の項目は以下のとおりである。

- 登録情報の確認
- VLAN 接続機器の登録
- 用途
- VPN 接続を許可する ID

また、VLAN 接続機器の登録対象は、NAS（ファイルサーバ等）、複合機、無線 LAN アクセスポイント（以下、「無線 AP」という。）を必須とした。登録機器ごとの点検項目は以下のとおりである。

- 機密情報や個人情報の有無
- 個人情報の取扱い件数
- 機器の設置場所
- データのバックアップ
- ログの取得
- ソフトウエアのアップデート
- ウイルス対策ソフトウエア
- 主体認証と権限管理

KUINS-III VLAN の利用申請や登録情報の管理も KUINS-DB を用いている。2017 年度には別途回答用アンケートフォームに回答する必要があったが、KUINS-II の点検同様に二度手間となっていたため KUINS-DB から回答するように導線を見直した。

まずは、各 KUINS-III VLAN ごとに接続している機器を登録する機能を追加した。主な登録項目は以下のとおりである。

- 機器種別
- 機器名称
- 管理者氏名、連絡先
- MAC アドレス

なお、本学の対策基準で実施が求められている内容をもとにしたセキュリティ要件の項目を追加した。（図 4）

図 4 セキュリティ要件

また無線 AP については、前述の登録項目の他に、本学の無線 LAN 設置のガイドラインをもとにした管理項目を追加した。（図 5）

図 5 無線 AP の管理項目

5.2 点検の結果

点検状況について、表 4 に示す。

表 4　点検状況

年度	点検状況	
	対象 VLAN	回答済
2021	3,866	3,250 (84.1%)
2022	3,913	3,328 (85.0%)

KUINS-III VLAN に接続している機器の登録状況について、表 5 に示す。

表 5　機器の登録状況

年度	VLAN 数	機器登録数		
		NAS	複合機	無線 AP
2021	3,866	824	973	1,007
2022	3,913	910	1,016	1,189

- 約 12%の KUINS-III VLAN に NAS が設置されており、約 17%の NAS で個人情報を取り扱っている
- 約 15%の KUINS-III VLAN に複合機が設置されており、約 80%の複合機のセキュリティ対策（管理者パスワードの管理やファームウェアのアップデート等）が実施されている
- 約 13%の KUINS-III VLAN に無線 AP が設置されており、約 75%の本学の無線 LAN アクセスポイント設置のガイドラインに準拠している
- 点検での登録を必須とした機器以外では、PC 端末が約 1200 台登録されている

この点検により、各 KUINS-III VLAN に接続される機器の確認、設定等の見直しがされた。またインシデント発生の際に、原因となった機器の特定がより速やかに行える体制になることから、例年点検を行うことが効果的である。

6 サブドメインの総点検

6.1 点検の概要

2022 年度は、kyoto-u.ac.jp のサブドメイン（約 200 個）と kyoto-u.ac.jp 以外のサブドメインを対象に点検を実施した。本学の kyoto-u.ac.jp のサブドメインは、原則として 1 部局に 1 サブドメインとしているが、例外として全学的なプロジェクトのため認められたものやサブドメインに関する規約施行前（2013 年 3 月 31 日以前）にすでに使用されているものがある。いずれもサブドメイン管理部局とサブドメイン管理責任者を選出している。

主な点検項目は以下のとおりである。

- サブドメインの使用状況
- サブドメインの用途
- 設定されたレコードや管理状況
- サブドメイン登録時の運用手続き
- 学外 IP アドレスの登録有無

点検依頼は、kyoto-u.ac.jp のサブドメインはサブドメイン管理責任者に kyoto-u.ac.jp 以外のサブドメインは各部局のセキュリティ事務担当に連絡し、Google　Forms にて回答するようにした。

6.2 点検の結果

点検状況について、表 6 に示す。

表 6　点検状況

年度	点検状況		
	対象サブドメイン	回答済	廃止（予定含む）
2022	197	187 (94.9%)	4 (2.0%)

- 登録内容（レコードの登録など）を修正したサブドメインは約 11%あった
- サブドメイン配下で行っているサービスは、Web サービスが最も多く、次にメールサービスであった
- 約 75%のサブドメインで登録等する場合に、部局での内規やセキュリティ委員会等の審議により運用されていた
- 約 38%のサブドメインで学外の IP アドレスが登録されていた
- 2 部局で kyoto-u.ac.jp 以外のサブドメインを利用していた

この点検により、不要なサブドメインの廃止、登録されているレコードの見直しが行われた。また学外 IP アドレスの登録がされているサブドメインは、前回（2018 年度）の点検では約 18%（33/186）だったところ、今回は約 38%(69/197)に増加しており、クラウドサービスの利用が要因であると考えられる。そのため今後の自己点検テーマとしてクラウドサービスの利用について検討している。

7　全構成員自己点検

7.1 点検の概要

全構成員（全学生および全教職員）を対象にした自己点検は、毎年度受講を必須としている情報セキュリティ e-Learning を利用した。本学の情報

セキュリティ e-Learning は、テキストを一読して学習した後、修了テストを受講する形式である。修了テストの設問に以下の点検項目を追加した。

- 端末のセキュリティ対策状況
- パスワードガイドラインの準拠状況
- データのバックアップ
- 機密情報や個人情報の取り扱い

また 2023 年度には、全教職員向けに情報格付けに関する点検項目を設問に追加した。

情報格付けに関する設問例を表 7 に示す。

表 7 設問と回答選択肢の例

<設問>京都大学情報格付け基準の別表から未実施の「入学試験問題」の機密性について格付けと取扱の組み合わせで正しいものはどれか？
<回答選択肢＞ 1. 機密性２(標準的な取扱制限) 2. 機密性２(複製禁止、送信禁止) 3. 機密性３(標準的な取扱制限) 4. 機密性３(複製禁止、送信禁止)

7.2 点検の結果

2023 年度の自己点検は、8 月末時点での、自己点検の実施率は学部学生 61.0%、大学院生 63.0%、教職員 76.5%となっており、実施率 100%を目指して未実施者への実施促進の取り組みを進めている。8 月末時点での点検の主な回答状況は以下のとおりである。

- 業務で扱う個人情報の情報格付けは、約 80%が明示等された格付け及び取扱制限に従って適切に取り扱っていた
- 情報格付けの問題のうち、入試問題の格付けに関して正答率が一番高く、輸出申請に関する問題の正答率が低かった

最終的には年度末に再度状況を確認することになるが、情報格付けの運用や理解の向上について引き続きを実施していく必要がある。

8 考察

本学の情報セキュリティポリシー策定にあたって参考にした国立情報学研究所が公開してい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定集[1]においても、自己点検は各当事者が実施しているかの確認だけでなく、それぞれの役割において改善策を実施する必要があるとされている。本学では自己点検計画を策定する最高情報セキュリティ責任者においては、点検結果について把握・分析し、次年度以降の自己点検計画に反映している。部局情報セキュリティ責任者は、教職員等の役割ごとの情報セキュリティ自己点検を整備する必要があるが、2022 年度に実施したセキュリティ監査の結果からは、一部の部局でのみの実施されている状況である。点検者による改善策の実状は把握できていない。

自己点検の問い合わせの中には、改善が必要であることが判明したが、改善策がわからないという声が寄せられている。情報セキュリティポリシーをもとにした自己点検票やチェックシートを既に整備しているが、問い合わせ等の意見を踏まえて、点検マニュアルの作成やセキュリティ教育、研修を行っていく必要がある。

9 おわりに

本稿では、本学における情報セキュリティの自己点検の取り組みと結果、考察について述べた。

自己点検を実施することで、接続機器の設定見直しや不要機器の廃棄等の棚卸しが継続して行われ、セキュリティ対策の向上に効果があった。また回答方法を変更したことで、点検手順の簡略化や、前任者の点検状況を把握することが可能となった。従前からの課題として点検者に委ねている点や、再三の回答依頼にも未回答といった点の他に、部局内の接続機器や KUINS-III VLAN の管理を一任されている場合に、点検者の負担が大きいことが問題となっている。点検者側の体制見直し以外にも、点検項目の見直しやリスクを考慮して優先順位を決めるなど負担を軽減する方法を検討する必要がある。本学のサイバーセキュリティ対策等基本計画（第 3 期）にて、自己点検の実施、内容の見直しを定めており、より効果的な情報セキュリティ対策となるよう引き続き実施していく。

参考文献

[1] 斎藤 紀恵, 片桐 統, 戸田 庸介, 石橋 由子、京都大学における情報セキュリティ自己点検の取り組み、大学 ICT 推進協議会 2019 年度年次大会、2019 年

[2] 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定集（2022 年度版）、2023 年