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

斎藤 紀恵 [1)], 片桐 統 [1)], 戸田 庸介 [1)], 石橋 由子 [1)]

1) 京都大学 企画・情報部

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

Information Security Self-Assessment at Kyoto University

Norie Saito [1)], Osamu Katagiri [1)], Yosuke Toda [1)], Yoshiko Ishibashi [1)]

1) Planning and 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。グローバル IP アドレスを持つ機器は約 2,500 台、研究室や事務室毎に構成するプライベート VLAN は約 3,700 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。しかし、実施している情報セキュリティ対策の水準は、グローバル IP アドレスを持つ機器やプライベート VLAN の管理者の情報セキュリティに対する知識に依存しており、全学的な観点からはばらつきがあるのが実情である。このような状況を改善するため、情報セキュリティの自己点検を 2016 年度よりテーマを決めて実施し、情報セキュリティ対策の状況を確認するとともに必要に応じて見直しを行っている。本稿では、自己点検の取り組みと点検結果について述べる。

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水準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定めている。実施にあたっては、最高情報セキュリティ責任者が全学の計画を策定し、各部局において実施することとなっている。また、各部局が作成する情報セキュリティポリシー実施手順書の雛形においても、点検票の様式を提供し自己点検の実施を推進している。しかし、2015 年度までは自己点検の全学としての計画が明確に示されておらず、各部局において実施が困難であった。

2014 年度に実施した本学の情報セキュリティ監査において、各部局では情報セキュリティの自己点検への理解が進んでおらず適切に実施されていないことが確認された。状況を改善するため、情報セキュリティの自己点検について、全学的な計画を明確にして 2016 年度より実施することとした。それぞれの点検を詳しく実施するには、1 年で全ての点検を実施することは難しい。このため、数年サイクルで必要な点検が網羅できるよう、年度ごとに自己点検のテーマを定めて実施する計画とした。本稿では、2016 年度からの自己点検のテーマと、それぞれの点検の概要と結果について述べる。

2 自己点検のテーマと中期的な計画

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
2016	グローバル IP アドレスを持つ機器の総点検
2017	プライベート VLAN の総点検
2018	サブドメインの総点検
2019	全構成員自己点検

本学では、学外からもアクセスが必要なサーバ等はグローバル IP アドレスが割り当てられており、研究室や事務室に設置される端末等は、部屋毎などのプライベート VLAN に接続する構成になっている。学内の状況を一通り確認するため、1 年目は外部からの攻撃にさらされるリスクが高いグロー

バル IP アドレスを持つ機器の点検を実施し、2 年目にプライベート VLAN の点検を実施することとした。これに加えて、学外のクラウドサービスで本学ドメインを使用している機器についても把握できるようサブドメインの点検(3 年目)、持ち込みの機器なども含め構成員の個々の自己点検(4 年目)を行うことで、必要な項目を網羅できるように計画した。5 年目以降は、4 種類のテーマを 4 年サイクルで順次実施する計画で、2020 年度は 2016 年度と同じグローバル IP アドレスを持つ機器の総点検を実施する予定である。それぞれの点検の詳細については 3 章以降で説明する。

計画で定めたテーマ以外にも、情報セキュリティインシデントの状況等により点検が必要になった場合には、臨時に点検を行っている。これまでの例では、2017 年 2 月に公開された WordPress の脆弱性に起因して、学内の複数の Web サイトで問題が発生したことから、2017 年 5 月に「Web サーバの一斉点検」を実施した。

3 グローバル IP アドレスを持つ機器の総点検

3.1 点検の概要

2016 年度は、グローバル IP アドレスを持つ機器（約 2,500 台）の状況を確認する自己点検を実施[1]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
- 接続状況、利用目的
- OS 等のセキュリティパッチ適用の状況
- 公開しているコンテンツの確認
- 認証、アカウント、権限管理、暗号化
- 稼働しているアプリケーションとその機能
- ウイルス対策、ログ取得、バックアップ
- 使用目的に応じた確認項目

回答は選択方式として、「問題なかった」という選択肢と「問題があったため修正した」という選択肢とすることで、適切な管理状態に見直しを促すように工夫した。

3.2 点検の結果

回答の締め切り後、未回答機器に対して繰り返し連絡を行う等の取り組みを実施し、最終的な回答率は約 97.8%となった。残り 2.2%の未回答機器については、臨時で 2017 年 5 月に実施した「Web サーバの一斉点検」でフォローアップを行った。主な点検結果は以下のとおりであった。

- 未使用機器について点検を機に廃止した機器が約 12%あった
- 登録情報（管理責任者など）を変更した機器が約 12%あった
- 機器の利用目的は Web サーバが最も多いが、テレビ会議システムも多く接続されている
- OS は Linux 系の機器が多いが、macOS や Windows 系も一部で使用されている
- 一部の機器では、セキュリティパッチの適用や、ログ取得、脆弱性診断の指摘事項の修正などに問題が確認され見直し等が行われた

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の多くが廃止された。このことにより、情報セキュリティインシデントの発生を未然に防ぐことに効果が期待できる。

4 プライベート VLAN の総点検

4.1 点検の概要

2017 年度は、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プライベート VLAN（約 3,700）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。

- 登録内容の確認
- プライベート VLAN の使用用途、利用者
- 接続している機器の種別、台数
- 情報セキュリティインシデントの対応体制

4.2 点検の結果

回答の締め切り後、未回答のプライベート VLAN について繰り返し連絡を行う等の取り組みを実施し、約 99.7%のプライベート VLAN について点検結果の回答があった。主な点検結果は以下のとおりであった。

- 未使用のプライベート VLAN で、点検を機に削除したものが約 7%あった
- 使用用途は、教育、研究、業務の数がほぼ均等である
- 約 25%のプライベート VLAN に無線 LAN アクセスポイントが設置されている
- 情報セキュリティインシデントが発生した

際、機器や利用者を特定できる体制になっておらず点検を機に見直しが行われたプライベート VLAN が約 6%あった。
- 本学以外（持ち込み、私物等）の機器を接続することがあるプライベート VLAN は相当数にのぼることが分かった

この点検により、それまで詳しい実態が不明であった各プライベート VLAN に接続される機器の状況等が把握できた。また体制等の見直しが行われ、万が一のインシデント発生の際にも、原因となった機器の特定が速やかに行える体制になった。

5 サブドメインの総点検

5.1 点検の概要

本学では、部局または全学的なプロジェクトで必要性が認められる場合に kyoto-u.ac.jp のサブドメインを割り当てており、各サブドメインに管理責任者が選出されている。2018 年度は、kyoto-u.ac.jp のサブドメイン（約 190）について総点検を実施した。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用途
- 設定されたレコードや管理状況

5.2 点検の結果

回答の締め切り後、未回答のサブドメインに対して連絡を行った結果、全てのサブドメインについて点検結果の回答があった。主な点検結果は以下のとおりであった。

- 点検を機に廃止したサブドメインが約 4%あった
- 登録内容（管理責任者など）を修正したサブドメインは約 18%あった
- 登録されているレコードの見直しが行われたサブドメインは約 15%あった
- 登録されているレコードの確認方法が分からないと回答したサブドメインがあり、フォローアップを行った
- 約 18%のサブドメインで学外の IP アドレスが登録されている。

この点検により、登録されているレコードの見直しが行われたほか、それまで実態を十分に把握できていなかったクラウドサービスの利用について、ある程度の状況が把握できた。今後のセキュリティ対策に活かしていきたい。

6 全構成員自己点検

6.1 点検の概要

2019 年度は、全構成員（全学生および全教職員）を対象に、自分自身が実施すべき対策を点検することで、個人レベルの安全性を高めるため全構成員自己点検を実施している。点検の項目は、各部局が作成する情報セキュリティポリシー実施手順書の雛形で提供している点検票の項目に準じたものとした。主な点検項目は以下のとおりである。

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

点検項目の例を表 2 に示す。

表 2 設問と回答選択肢の例

<設問> 使っている端末の OS（Windows や macOS などのこと）やアプリケーションソフトについて、最新のアップデートが適用されていますか。
<回答選択肢> 1. 全て最新のアップデートが適用されています。 2. アップデートの適用漏れがあったため、速やかに更新します。

実施にあたっては、点検の対象者が情報セキュリティ e-Learning（以下、「e-Learning」という。）の受講対象者と重複することから、e-Learning の修了テストの項目に自己点検項目追加（ただし採点の対象外）することで対象者の負荷軽減を図っている。また、e-Learning と同様に日本語版のほか英語版も提供している。

6.2 点検の結果

2019 年 8 月末時点での、自己点検の実施率は学部学生 43.9%、大学院生 58.5%、教職員 84.5%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。

- 一部の構成員からはサポートの終了した OS やアプリケーションソフトを使用しており更新すると回答があった
- 一部の構成員からは最新のアップデートが適用されていないため更新すると回答があった
- 一部の構成員からはパスワードガイドライ

ンに準拠していないパスワードを使用しており変更すると回答があった
- データのバックアップを行っていない構成員が一定数いる

最終的には点検の完了後に状況を確認することになるが、重要な問題点については、改善のための対策を検討していく。

7 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について述べた。

自己点検を実施することで、グローバル IP アドレスを持つ機器数やプライベート VLAN 数が大幅に減るなど、セキュリティ対策の水準向上に効果があった。しかし、自己点検の実施に際しての具体的な点検手順はそれぞれの実施者に委ねられており、適切な点検が十分でない機器がある可能性は否定できない。このため、グローバル IP アドレスを持つ機器であれば、毎年度実施を義務づけている脆弱性診断の結果を活用する等して、より効果の高い自己点検となるよう工夫していきたい。また、一部の自己点検では再三の回答依頼にも関わらず未回答の機器等が残ったことから、全ての対象で自己点検が実施されるよう、状況によってはペナルティ等も含めた実施体制の検討していく必要がある。

定期的な自己点検は今後も継続して実施するが、点検サイクルや、テーマ、点検項目については、より効果的なものとなるよう見直しを図っていきたい。

参考文献

[1] 斎藤 紀恵, 片桐 統, 石橋 由子、京都大学におけるグローバル IP アドレスに接続する機器の総点検、大学 ICT 推進協議会 2017 年度年次大会、2017 年