情報セキュリティ対策自己診断システムを用いた自己診断結果の分析

青木 謙二[1)], 園田 誠[1)], 黒木 亘[1)], 宮本 理司[1)], 廿日出 勇[1),2)]

1) 宮崎大学 情報基盤センター
2) 宮崎大学 工学部

aoki@cc.miyazaki-u.ac.jp

Analysis of self-diagnosis results using the information security measures self-diagnosis system

Kenji Aoki [1)], Makoto Sonoda [1)], Wataru Kurogi [1)], Masashi Miyamoto [1)], Isamu Hatsukade [1),2)]

1) Information Technology Center, University of Miyazaki
2) Faculty of Engineering, University of Miyazaki

概要

本学では、より簡単に自身が管理する PC の情報セキュリティ対策の状況を把握するために自己診断システムを構築し、これを用いた自己点検を 2022 年度から実施してきた。本論文では、2022 年度と 2023 年度の約 2 年間の実施状況を確認し、その結果を年度間で比較し、変化がみられるかを分析した。この結果、2022 年度に自己診断を行った者の総数は 1,390 名、PC の総数は 1,456 台で、2023 年度に自己診断を行った者の総数は 1,164 名、PC の総数は 1,273 台と毎年度、同程度数の教職員、学生が、同程度数の PC に対して自己点検を実施していることがわかった。また、年度によらず、30%程度の PC でウイルス対策ソフトのスキャン実施とスクリーンロックの実施が行われておらず、他の診断項目よりも特に実施状況が悪いことがわかった。さらに、2022 年度に診断結果が正常となった PC であっても、2023 年度の初回診断では異常と診断される PC が 35%あり、一旦、情報セキュリティ対策が行われたとしても、その後の情報セキュリティ対策が維持できていないことが示唆された。

1 はじめに

本学では、情報セキュリティ基本方針、情報セキュリティ基本規程、情報システム管理者規程、情報システム利用者規程を定め、また、ガイドランを示して、管理者および利用者に確実な情報セキュリティ対策の実施を促し、情報セキュリティ対策の推進を図ってきた[1]。また、これらの対策が実施されているか確認するために、2012 年度から実地による監査を行ってきた。

実地監査では、監査対象組織が提出する事前調査票の記載内容と実機の状態に相違がないかを数台の PC を抽出して確認していた。しかしながら、実地監査を受けるのは 4 年に一回と間隔があいており、その間の情報セキュリティ対策が継続的に行われているか把握することができなかった。また、事前調査票を記入する際に PC のどこの何を確認すればよいかわからない管理者が多いため、事前調査票の内容が不正確であり、実機の状態と乖離があった。このため、正確な状況を把握するためには、可能な限り多くの PC を詳細に監査する必要があるが、限られた時間と人で全数を詳細に監査することは不可能であった。

そこで、これらの実地監査の欠点を補完するために、本学では、すべての構成員に自身が管理する PC の情報セキュリティ対策の状態を自ら確認する自己点検を推進していくこととした。しかし、情報セキュリティ対策ができていることを個々の管理者が確認することは難しく、また、どれだけの管理者が正確に自己点検を行っているか把握することは困難な状況であった。これに対応するため、管理者が各自で簡単に PC の情報セキュリティ対策の状態を確認できること、および、その情報を集約し情報基盤センターで把握できることを目的に「自己診断システム」を構築し、2022 年度よりこのシステムを使った自己点検の実施を開始した[2]。

自己点検の開始より約 2 年間が経ったことで、全学的な自己点検の実施記録が得られたことから、2022 年度と 2023 年度の約 2 年間の実施状況を確認し、年度間の比較や分析を行った。本論文では、これにより得られた特徴や変化を報告する。

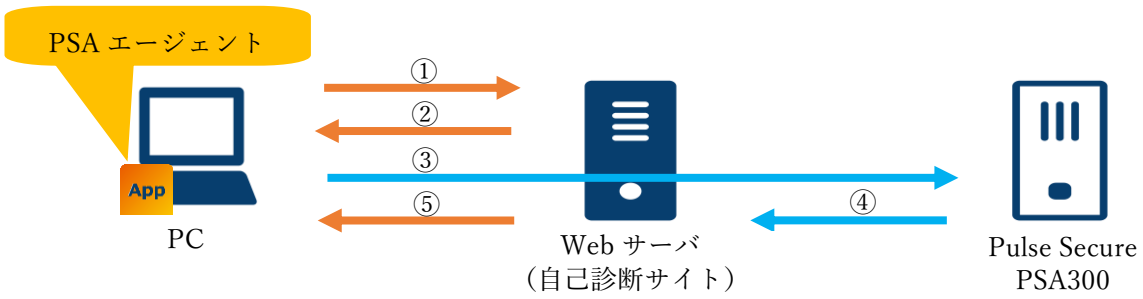


図 1　自己診断システム概要

2 自己診断システム

自己診断システムの概要を図 1 に示す。診断したいクライアント PC から Web ブラウザにより自己診断サイトに接続することで、ソフトウェアによる自動診断と自己申告による診断ができる。自動診断は図 1 ①～⑤の順に行われる。被診断 PC の Web ブラウザから Web サーバ（自己診断サイト）にアクセスし、自動診断を開始する（図 1 ①）。初回はエージェントソフトウェア（Plus Secure Appliance ホストチェッカー）のインストールが必要となる。自己診断サイトは PSA エージェントを実行し（図 1 ②）、PC 内の情報を Pulse Secure PSA300 に送信する（図 1 ③）。PSA300 は送られた情報を分析し、分析結果を自己診断サイトに返信する（図 1 ④）。自己診断サイトは、本学の診断基準に基づき判定し、結果を端末の Web ブラウザに表示する（図 1 ⑤）。自動診断に対応する OS は、Windows OS、Mac OS、Linux OS である。それ以外の OS にいては、PC の状態を自身で確認し、手動での自己申告により診断を行う。詳細については、参考文献[2]に記載している。

診断項目および診断基準は表 1 に示すとおりである。OS のバージョンについては、サポート期間内のエディションとバージョンをそれぞれ OS 毎に個別に設定し、これに含まれる場合に基準を満たしていることになる。なお、EDR（Endpoint Detection and Response）の動作、HDD の暗号化については、機密性 3 情報を扱う PC に限っている。また、ログインパスワードの設定および機密性 3 情報の扱いについては手動による自己申告が必要である。

各項目について基準を満たしていれば「○」、満たしていなければ「×」、該当しなければ「－」が表示される。総合的な判定は、一つでも×がついた場合は「異常」と表示され、○または－のみの場合は「正常」と表示される。

表 1　診断項目と診断基準

診断項目	診断基準
OS のバージョン	OS 毎に指定
OS アップデート日	90 日以内
ファイアウォール動作の有無	有
ウイルス対策ソフト動作の有無	有
ウイルス対策ソフト定義ファイル更新日	5 日以内
ウイルス対策ソフトスキャン実施日	5 日以内
EDR 動作の有無（該当 PC のみ）	有
ログインパスワード設定の有無	英数記号を含む 8 文字以上
スクリーンロック設定の有無	有
HDD 暗号化の有無（該当 PC のみ）	有

3 実施方法

2022 年 4 月 1 日よりいつでも自己診断システムを利用できるようにした。特に、毎年度、本学のすべての構成員に e ラーニング形式の情報セキュリティ対策講習を実施しており、これと合わせて自己点検を実施するように周知した。講習の期間は、2022 年度は 2022 年 4 月 12 日から 2022 年 7 月 10 日まで、2023 年度は 2023 年 4 月 12 日から 2023 年 7 月 10 日までである。ただし、本論文で取り扱う自己診断システムの診断結果は、2022 年 4 月 1 日から 2023 年 8 月 25 日までを記録したものである。自己点検の対象者は本学の教職員および学生を含む全構成員が管理する PC で、本学のネットワークに接続するものとした。また、自己診断の実施回数には制限を設けず、診断結果が異常であった場合には必要な対策を実施して再度診断を行うように通知した。

4 結果

診断結果を 2022 年度と 2023 年度に分けて集計し、比較を行った。

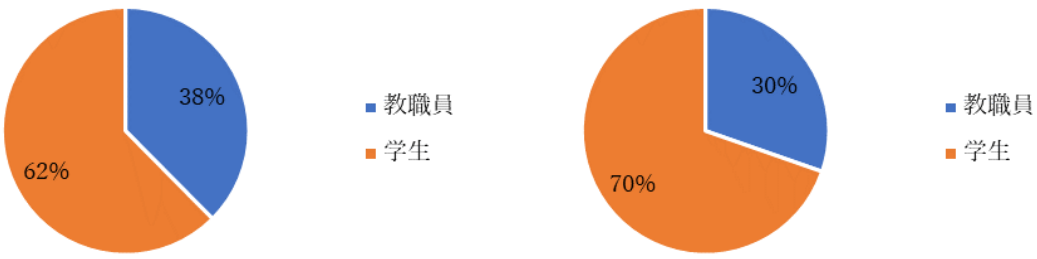
自己診断を行った教職員と学生の割合を図 2 に示す。2022 年度に自己診断を行った者の総数は 1,390 名で、その内訳は教職員 522 名（38%）、学生 868 名（62%）であった（図 2（a））。また、自己診断を行った PC の総数は 1,456 台であった。2023 年度に自己診断を行った者の総数は 1,164 名で、その内訳は教職員 353 名（30%）、学生 811 名（70%）であった（図 2（b））。また、自己診断を行った PC の総数は 1,273 台であった。2023 年度に比べて 2022 年度の集計期間が長いため、自己診断を行った実施者数と PC 数の直接の比較はできないが、教職員と学生の割合は年度間で大きな違いは見られなかった。

自己診断を行った PC の OS の割合を図 3 に示す。その他には、Linux 系 OS（Ubuntu，CentOS，Debian）および Chrome OS、「該当なし」を選択したものが含まれる。2022 年度は Windows 10 が最も多く 79%であった。次いで Mac OS X が 12%であった（図 3（a））。2023 年度は Windows 10 が最も多く 72%であった。次いで Windows 11 が 17%、Mac OS X が 10%であった（図 3（b））。年度間で Windows 10 の割合はあまり変わらないものの、2023 年度は Windows 11 の割合が増えており、Windows 11 が普及したことがうかがえる。また、Windows 8.1 が 2023 年度ではなくなった。Windows 8.1 は 2023 年 1 月 10 日にサポートが終了していることから学内では使わないことになっているが、これを順守しているものと思われる。

自己診断の結果を図 4、図 5 にまとめた。自己診断は複数回行うことができたが、最終回の診断結果を示している。2022 年度（図 4）、2023 年度（図 5）のどちらにおいても、「ウイルス対策ソフトスキャン実施日」と「スクリーンロック設定」の項目で基準を満たしていない割合がおおよそ 30%と他の項目に比べて高いことがわかる。また、すべての項目において、2022 年度に比べ 2023 年度は基準を満たしていない割合が低くなっており、全体的に情報セキュリティ対策の実施状況が改善されていることが示唆される。

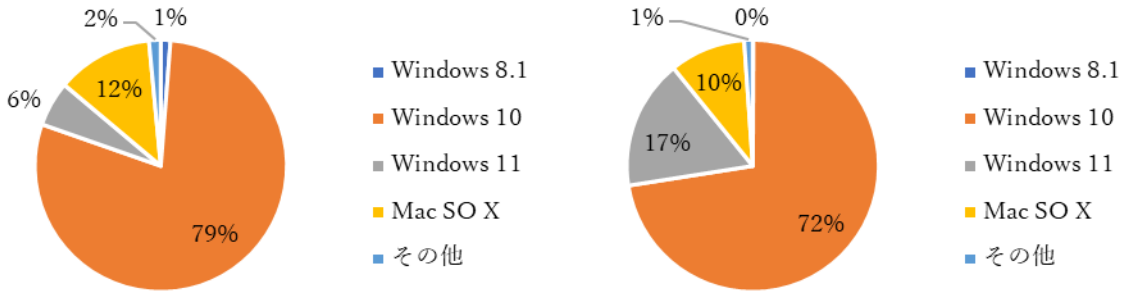
図 6 に自己診断の実施回数を日ごとに集計したものを時系列で示した。この図では、情報セキュリティ対策講習の実施期間に限って集計した。2022 年度と 2023 年度には大きな違いは見られず、実施期間の初日に最も多く自己診断が実施されており、多少の上下があるものの、17 日目までに日を追うごとに減少し、その後、少ない数で推移している。

2022 年度と 2023 年度で同一 PC について自己診断を行った結果を集計し、2022 年度最終回結果と 2023 年度の診断結果に変化があったか調べた。図 7 にこの結果を示す。2022 年度と 2023 年度で同一 PC について自己診断を行ったものは 356 台であった。図 7 の凡例に示した文字は、左から順に「2022 年度最終回結果」、「2023 年度 1 回目結果」、「2023 年度最終回結果」を示しており、「正」は正常、「異」は異常、「－」は実施していないことを表している。2022 年度最終回結果で正常だった PC が 2023 年度 1 回目でも正常だったものが 30%と最も多く、年度をまたいで基準を満たした状態であった。2022 年度最終回結果で正常だった PC が 2023 年度 1 回目では異常と診断され、2023 年度最終回では正常になっているものが 25%と次に多かった。常に正常な状態を維持していないものの、自己診断を契機に改善されたことを示している。しかしながら、2022 年度も 2023 年度も異常のまま終わっているもの（22%）、2023 年度が異常で終わっているもの（10%）も多かった。



（a）2022 年度（1,390 名）　　（b）2023 年度（1,164 名）

図 2　教職員と学生の割合の比較



（a）2022 年度（1,456 台）　　（b）2023 年度（1,273 台）

図 3　OS の割合の比較

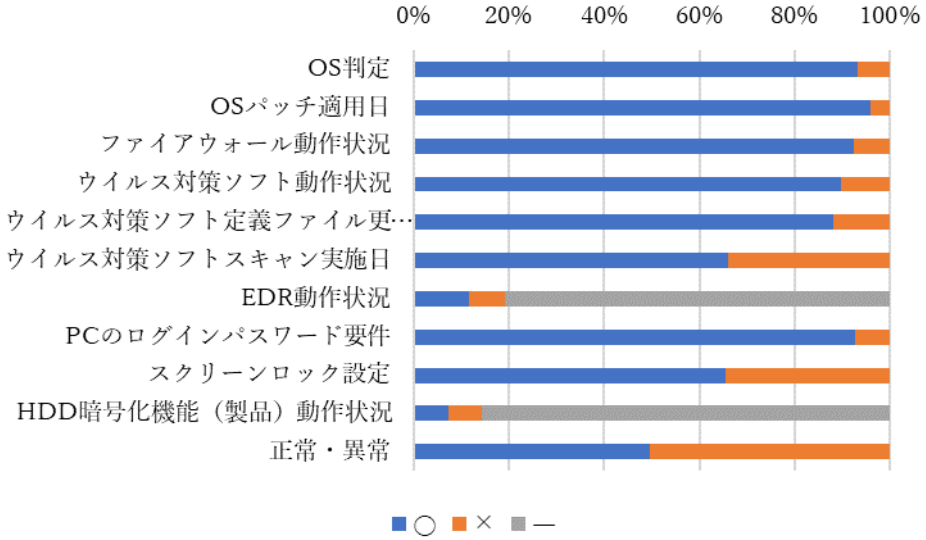


図 4　2022 年度自己診断結果

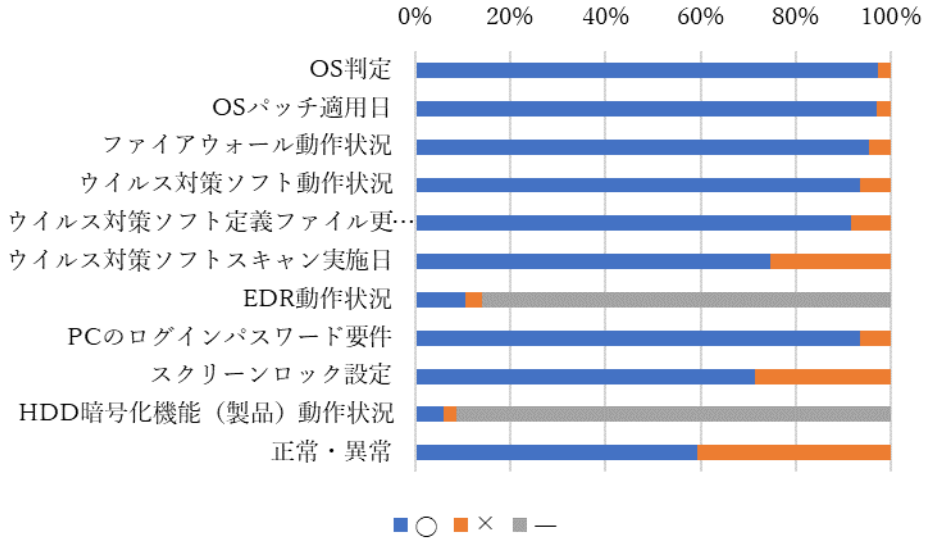


図 5　2023 年度自己診断結果

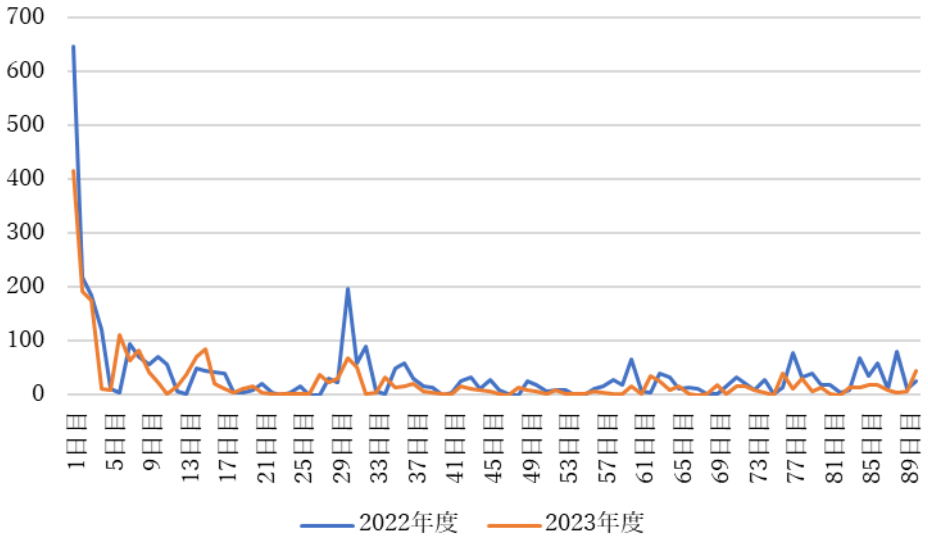


図 6　自己診断実施回数の日ごと集計

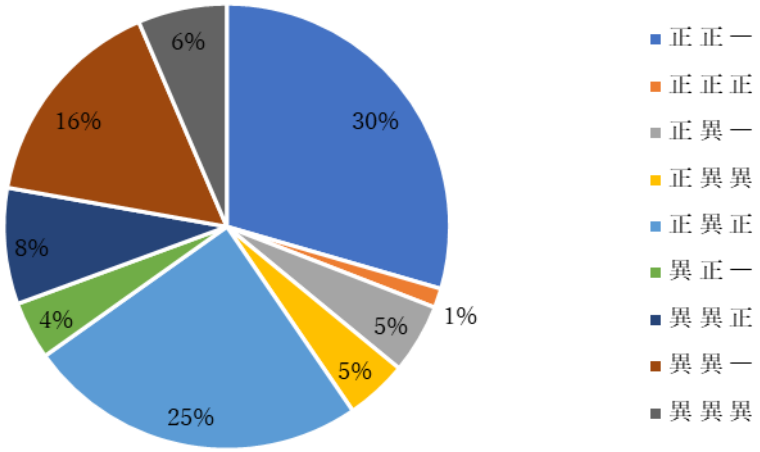


図 7　2022 年度と 2023 年度に共通する PC の診断結果

5 おわりに

本研究では、本学が定める情報セキュリティ対策が学内ネットワークに接続する PC に対して実施されているかを自己点検するために構築した自己診断システムを用いて、2022 年度から 2023 年度にかけて自己診断を行い、この結果を分析した。

分析した結果、毎年度、同程度数の教職員、学生が、同程度数の PC に対して自己診断を実施することがわかった。また、年度によらず、ウイルス対策ソフトのスキャン実施とスクリーンロックの実施が特に行われていないことがわかった。さらに、一旦、情報セキュリティ対策が行われたとしても、その後の情報セキュリティ対策が維持できていないことが示唆された。時間と共に PC が置かれた環境が変化していくことから、1 回の診断で基準を満たしたとしても満足することなく PC の情報セキュリティ対策の状態を継続して改善し、定期的に自己診断を実施していくような取り組みが必要である。

2022 年度も 2023 年度も診断結果が異常のまま終わっているものも多く、PC の情報セキュリティ対策の状況が改善されていないことは大きな問題である。自己診断の実施のみで終わるのではなく、改善までをセットとして実施できるような仕組みの構築が必要である。また、自己点検を実施した者が構成員の一部に留まって

おり、診断された PC もすべてではないと思われることから、今後、自己点検の実施率を向上させていくことが課題である。

約 2 年間、本システムを運用するなかで明らかになった技術的な問題もあった。ある 2 つのウイルス対策ソフトにおいて、動作しているにも関わらず動作を自動で検出しないものがあった。このソフトは全学的にはマイナーなものであるため、全体の結果に大きな影響を与えるものでないが、この製品を使用している管理者にとっては正しい結果が出ないため問題である。原因は、本システムが PC の状態を分析する際に参照しているデータがこの製品へ対応していなかったためである。既に参照データの提供元にこの問題を報告しているため、いずれ対応できると考えている。このように、すべての製品に対して対応することは難しく、問題が発生した都度対応していく必要があることは本システムを運用していく上での課題である。

参考文献

[1] 宮崎大学情報セキュリティ基本規程，宮崎大学情報システム管理者規程，宮崎大学情報システム利用者規程.

[2] 青木 謙二, 園田 誠, 黒木 亘, 宮本 理司, 廿日出 勇, 情報セキュリティ対策自己診断システムの構築と実践，学術情報処理研究, 2022, 26 巻, 1 号, p.63-70. https://doi.org/10.24669/jacn.26.1_63