
HOSEI-CSIRTについて

2026年3月4日
2025年度ネットワーク講習会

HOSEI-CSIRT

1 HOSEI-CSIRTとは

■HOSEI-CSIRTとは

本学では、情報セキュリティインシデントの発生時に迅速かつ円滑な対応を図るため、HOSEI-CSIRTを設置し、本学の情報システムやネットワーク環境における情報資産を守るための活動を行っております。

※CSIRT(シーサート)とは、「Computer Security Incident Response Team」の略で、情報セキュリティインシデントに対応するための組織のことです。

※情報セキュリティインシデントとは、情報漏えいや不正アクセス、マルウェア感染などの事件・事故のことです。

■ミッション(使命)

以下の活動を行うことにより、学生や教職員が安心して利用できる教育研究環境の実現を目指します。

- 情報セキュリティインシデントを未然に防止するための活動
- 情報セキュリティインシデントが発生した際に被害を最小限とするための活動

2 情報セキュリティインシデントが発生したら

HOSEI-CSIRTへご連絡ください

■受付時間

平日 9:00 ~ 11:30、12:30 ~ 17:00

土・日・祝日は受付時間外

受付時間外の連絡については、原則翌営業日に対応します。

■HOSEI-CSIRTへの連絡方法

(1)連絡フォーム



(2)電子メール

csirt@ml.hosei.ac.jp

氏名・所属・連絡先を明記の上、
詳細情報をお送りください。

情報セキュリティインシデント例

マルウェア感染

情報漏えい

不正アクセス

サイバー攻撃

Webサイト改ざん

「法政大学全学ネットワークシステムユーザ支援WEBサイト」
からもアクセスできます。

TOP > 重要なお知らせ > Webサイト改ざん・情報漏洩など
情報セキュリティインシデント発生時の連絡について
(2023年3月7日更新)

<https://netsys.hosei.ac.jp/important/important20220421k01.html>



2 情報セキュリティインシデントが発生したら

【参考】(1)連絡フォーム(イメージ) <URL> <https://forms.gle/cNmZrE3fvL9pV6Uf9>

情報セキュリティインシデント連絡フォーム

こちらは、法政大学の情報セキュリティインシデントを連絡するフォームです。

法政大学が所有する情報資産のサイバー攻撃・漏えい等や異常にお気付きの場合は、以下のフォームを利用して HOSEI-CSIRT までお知らせいただけますようお願いいたします。

<受付方法>

フォームに必要事項を入力後、「送信」をクリックしてください。担当者から折り返し連絡をさせていただきます。

電子メールでの受付も行っております。電子メールでお知らせいただく場合は、csirt@ml.hosei.ac.jpまでお願いいたします（@は半角に変更して送信をお願いいたします）。

受付時間は以下のとおりです。

平日 9:00~11:30、12:30~17:00

土・日・祝日は休業

※営業時間外の連絡については原則翌営業日に対応いたします。

HOSEI-CSIRT (法政大学CSIRT)
csirt@ml.hosei.ac.jp

*必須

氏名(事象報告者)

回答を入力 記入

所属(大学名・会社名・所属部署名)

回答を入力 記入

連絡先(電話番号)

回答を入力 記入

連絡先(メールアドレス)

回答を入力 記入

事象発見日を記載してください。*

日付
年 / 月 / 日 記入

事象発見時間を記載してください。*

時刻
: 記入

事象の分類を選択してください。*

選択 選択

事象内容の詳細を記載してください。*

回答を入力 記入

対象システム・対象サービスを記載してください。*

回答を入力 選択

情報漏洩の可能性を選択してください。*

選択 選択

送信

フォームをクリア

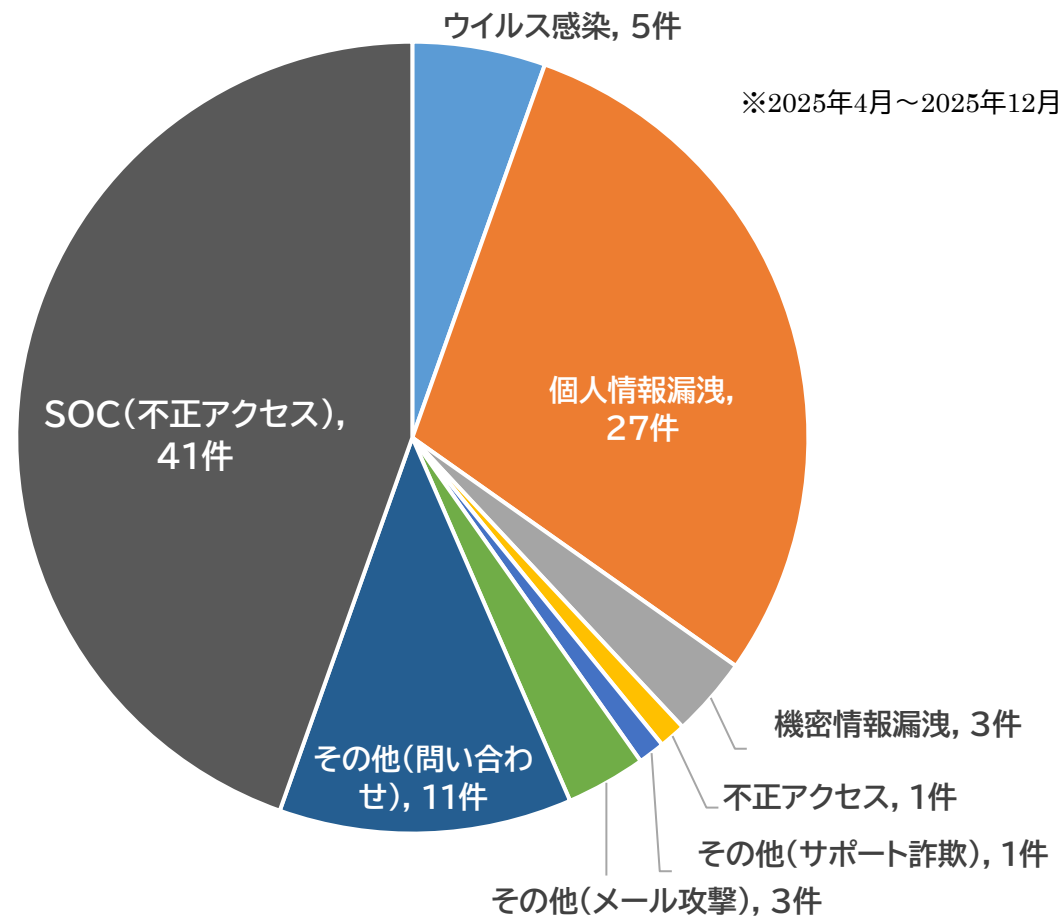
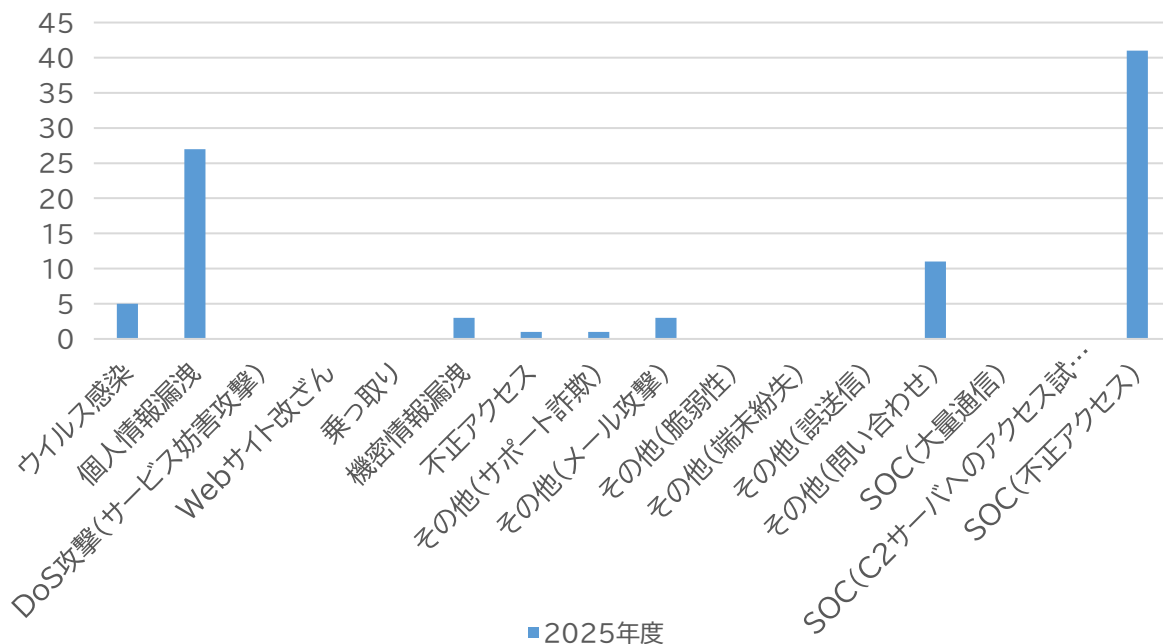
全ての記入が完了したら「送信」する

3 情報セキュリティインシデント対応状況

HOSEI-CSIRTは2022年4月から活動を開始し、現在まで様々な情報セキュリティインシデントへの対応を行いました。活動を通して、2025年度本学ではメールの誤送信等による「個人情報漏えい」が多いという傾向が分かっています。

※今年度導入した「SOC(Security Operation Center)」により、従来検知していなかった軽微なインシデントについても検知件数が増えたため、「SOC(不正アクセス)」割合が高くなっております。

(件) 本学における情報セキュリティインシデント発生件数(2025年4月～2025年12月)



最後に

情報セキュリティインシデントが発生したら…



HOSEI-CSIRTへご連絡ください

HOSEI-CSIRT
HOSEI-CSIRT is in operations since 2022

HOSEI-CSIRT とは | What is HOSEI-CSIRT?
CSIRT (シーサート) とは、「Computer Security Incident Response Team」の略で、情報セキュリティインシデント^①に対応するための組織です。法政大学の情報システムやネットワーク環境における情報資産を守るための活動を行います。
CSIRT (Computer Security Incident Response Team) is a group that takes action in case of information security incidents including unauthorized access, malware infections and information leaks. HOSEI-CSIRT aims to protect the university's information assets within the university's information systems and network environment.
①情報セキュリティインシデントとは、不正アクセスやマルウェア感染、情報漏えいなどの事件・事故のこと

ミッション | Missions

- 情報セキュリティインシデントを未然に防止するための活動を行います。
To prevent information security incidents.
- 情報セキュリティインシデントが発生した際に被害を最小限とするための活動を行います。
To minimize the damage once information security incidents occur.
- 学生や教職員が安心して利用できる教育研究環境の実現を目指します。
To realize a safe research and educational environment for students, faculties, and staff.

情報セキュリティインシデント発生時 は以下に連絡をお願いします。
Please contact HOSEI-CSIRT (see ways to contact below) in case of information security incidents.

Webサイト改ざん Website defacement
情報漏えい Information leaks
不正アクセス Unauthorized access
マルウェア感染 Malware infections
サイバー攻撃 Cyberattacks

受付時間
平日 9:00 ~ 11:30, 12:30 ~ 17:00
土・日・祝日は休業
受付時間外の連絡については、メール受付窓口に対応します。

Hours
Weekdays 9:00 - 11:30 a.m., 12:30 - 5:00 p.m.
Closed Saturdays, Sundays, national holidays
Regarding the messages received during non-business hours, we will get back to you on the next business day.

連絡方法 (24時間受付)

- ① 連絡フォーム
- ② 電子メール
csirt@m.hosei.ac.jp
氏名・所属・連絡先・詳細情報を明記の上、お送りください。

Ways To Contact (messages accepted around the clock)

- ① Contact Forms
- ② E-mail
csirt@m.hosei.ac.jp
Please report detailed information about the incident with your name, affiliation and contact information.

法政大学 HOSEI UNIVERSITY HOSEI-CSIRT

HOSEI-CSIRT
