NII

NIIサービスキャラバン2026

初心者向け

セキュリティ

2026.9.8@Fukuoka

2026.10.6@Osaka

2026.10.22@Tokyo

https://www.nii.ac.jp

「事業」タブをクリック

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

交通アクセス | お問い合わせ | English

NIIについて About NII | 研究 Research | 事業 Service | 大学院教育 Graduate Program

総合案内
- NII事業ナビ

ネットワーク
- SINET6

研究データ基盤
- GakuNin RDM
- JAIRO Cloud
- CiNii Research
- CiNii Books
- IRDB

認証基盤
- 学認(GakuNin)
- eduroam JP
- UPKI電子証明書発行サービス

クラウド
- 学認クラウド
  - 導入支援サービス
  - ゲートウェイサービス
  - オンデマンド構築サービス
- SINETStream

情報セキュリティ
- 大学間連携に基づく情報セキュリティ体制の基盤構築(NII-SOCS)
- 情報セキュリティポリシーサンプル規程集
- 倫倫姫の情報セキュリティ教室

学術情報流通
- NACSIS-CAT/ILL
- 電子リソースデータ共有サービス(ERDB-JP、ライセンス)
- KAKEN

この３つ

連携
- 大学図書館と国立情報学研究所との連携・協力推進会議
- 大学図書館コンソーシアム連合(JUSTICE)
- これからの学術情報システム構築検討委員会
- リポジトリ推進協会
- PARC Japan
- AI等の活用を推進する研究データエコシステム構築事業
- オープンサイエンスのためのデータ管理基盤ハンドブック
- HPCI
- mdx
- 学術情報基盤オープンフォーラム

人材育成
- 学認LMS

トピックス / TOPICS

NIIのセキュリティサービスは３つ

①大学間連携に基づく情報セキュリティ体制の基盤構築

（NII-SOCS: NII Security Operation Collaboration Services）

②高等教育機関における情報セキュリティポリシー策定

③倫倫姫の情報セキュリティ教室

①大学間連携に基づく情報セキュリティ体制の基盤構築

（NII-SOCS : NII Security Operation Collaboration Services ）

https://www.nii.ac.jp/service/nii-socs/

NII Center for Strategic Cyber Resilience Research and Development
NII Security Operation Collaboration Services(NII-SOCS)

「ニーソックス」と読む

NII-SOCS

NII-SOCS（ニーソックス）とは？

- **NII Security Operation Collaboration Services** の略
- 「機関がｻｲﾊﾞｰｾｷｭﾘﾃｨ対策やインシデント対応が行えるように、セキュリティ体制の構築をお手伝いしている」

大学間連携に基づく情報セキュリティ体制の基盤構築

- 企業が提供している、SOC（Security Operation Center）と異なる
- 「守るのも、インシデント対処するのも自機関で自主的に」
- 2017年度から運用している
  - 第一期（2017–2021年度）→第二期（2022–2027年度）
- 現在の参加機関のセキュリティ体制は、それなりにサイバー攻撃の対処能力が向上している

※NII-SOCS参加機関は、国立大学法人等の研究機関に限定。
リソースと予算の都合で、範囲を拡大できない。→第三期(2028-2033年度)

NII-SOCS のミッション

1. 重大なサイバー攻撃の検知及び情報提供
   - SINETを流れる通信を観測し、不審通信の検知・分析
   - 不審通信を検知すると対象機関に「警報情報」を提供して確認を促す
     - 対象機関は、「警報情報」に基づき、分析や対策を実施
     - 外部から通報されるよりも早く警報を知れるので、初動の素早いインシデント対応が可能となっている
2. サイバーセキュリティ人材の育成
   - CISOやCSIRT等セキュリティ担当者に「セキュリティ研修」を実施し、サイバー攻撃の対処能力向上を支援
3. 研究用データの提供
   - NII-SOCSで得られた攻撃情報を研究用データとして提供

勘違いされること

■「NII-SOCSに参加すれば、サイバー攻撃から守ってくれて、対処もしてくれるので安全だ。」

⇒ちがいます。

- 他人任せの SOC（Security Operation Center）ではありません。
- NII-SOCSが不審通信を検知すると、対象機関へ連絡します。
- 対象機関のセキュリティ担当者は、警報情報を分析してサイバー攻撃の対処をしてもらっています。

- NII-SOCS では、CISOやCSIRT等セキュリティ担当者に、セキュリティ研修を行い、サイバー攻撃の対処能力向上を支援しています。

②高等教育機関における情報セキュリティポリシー策定

https://www.nii.ac.jp/service/sp/

高等教育機関における情報セキュリティポリシー策定

- が、できるまで
  - 昔はインターネットなんて無かった
  - データ移動は、フロッピーディスクとか外部媒体
  - インターネットが浸透して、生活が便利になった
  - IT技術の発展とともにサイバー攻撃も発展し、社会問題になっている
  - 情報の取り扱いに、「ルール」が必要になった
  - 世の中の各組織が情報セキュリティポリシーを策定するための基準として、政府が2005年に『政府機関等の情報セキュリティ対策のための統一基準』（以下、「統一基準」）を発行した
  - NIIが2007年に「統一基準」を高等教育機関向けに解釈した「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程集」を発行した

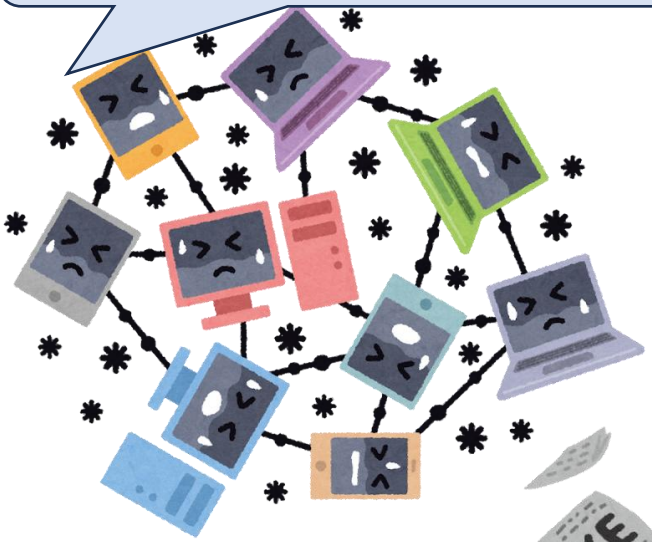
生活に便利

オンライン

SNSで話題！

悪用にも便利

マルウェア感染



サイバー攻撃

詐取

詐欺, 犯罪, デマ

トラブルに遭わないためには、
「ルール」が必要！！

「サンプル規程集」ってどんなの？

- 仮想の大学（2学部の学生1000人程度）をモデル
- 政府の「統一基準」を学校向けに解釈した解説書
- 雛型になっているので、機関ごとにカスタマイズして使用可
- CISO（最高情報セキュリティ責任者）が対応する指針も策定
  - NIIオープンフォーラム2023，2024，2025 で関連を講演
    - https://www.nii.ac.jp/openforum/2023/day3_security.html
    - https://www.nii.ac.jp/openforum/2024/day2_security1.html
    - https://www.nii.ac.jp/openforum/2024/day2_security2.html
    - https://www.nii.ac.jp/openforum/2025/day3_16.html

ポリシー・実施規程・手順等の体系

ポリシー （2文書）	実施規程 （11文書）	手順・ガイドライン等 （15文書）
		D3001 高等教育機関等におけるCISOの選任および実務の指針■
D1000情報セキュリティ対策基本方針 D1001情報セキュリティ対策基本規程 ◆ ● ■	D2101 情報セキュリティ対策基準● ■ D2102 情報格付け基準◆ ■ D2103 情報セキュリティインシデント対応チーム（CSIRT）設置規程◆ ●	D3101 物外措置手順書◆ ■ D3102 情報格付け取扱手順◆ D3103 インシデント対応手順策定に関する解説書◆ ■ D3106 情報セキュリティ非常時行動計画に関する解説書◆
	D2201 情報サービス利用規程 ● ■	D3251 情報機器取扱ガイドライン D3252 電子メール、メッセージング利用ガイドライン D3253 ウェブブラウザ利用ガイドライン◆ D3254 情報発信ガイドライン◆ D3255 認証情報管理ガイドライン
	D2301 年度講習計画■	D3301 教育テキスト作成ガイドライン(一般利用者向け) ◆ ● D3303 役職員向け説明資料作成ガイドライン◆
	D2401 情報セキュリティ監査規程● ■	D3401 情報セキュリティ監査実施手順
	D2601 全学認証基盤運用管理規程 D2602 全学認証基盤接続規程 D2603 全学認証基盤アカウント利用規程 D2651 証明書ポリシー(*) D2652 認証実施規程(*)	D3600 認証手順の策定に関する解説書 D3601 情報システムアカウント取得手順

Dではじまる文書が2019年度増補版以降に公表済みの文書
青字は、技術系の規程・手順書（より現場に近いレベルでの策定・運用を可能とするもの）
(*) 外部文書の参照のみ
◆＝2020年度改定文書 ●＝2022年改定文書 ■＝2024年改定文書 Dxxxx ＝C系列から編入

③倫倫姫の情報セキュリティ教室

https://www.nii.ac.jp/service/rinrinhime/

倫倫姫の情報セキュリティ教室

- 大学生活でよくある身近な会話から、「情報セキュリティ」の常識を学ぶオンラインコース
- どちらかと言うと、学生向け
- テスト問題あり
- 自習に最適で、とっつきやすく一部で親しまれている
- セキュリティ教育を始める、きっかけにどうぞ
- 日本語・英語・中国語・韓国語の4カ国語対応
- NIIが運用する「学認LMS」内で提供

※学認LMSへの参加が必要

シナリオパッケージ

1. 電子メールを使ってみよう
2. 取り扱い注意！ IDとパスワード
3. 著作権はとても重要
4. チート行為は厳禁！
5. 電子メール、SMSによる詐欺に注意！
6. 無線LANを安全に使おう
7. 情報機器の持ち歩きに注意
8. 安全にネットサーフィンを
9. 誹謗中傷に注意を
10. 偽情報・誤情報に気をつけよう

10は2026年2月にリリース

レベル感の違い

- 「倫倫姫で学習すれば、自機関のインシデントを減らせる？」
  ⇒少しは減るかもしれません。

  - 「一般的な常識」は身に付くと思われますが、大学が求めるサイバーセキュリティ対策のレベルには不足かもしれません。
  - インシデントを未然に防ぐにためは、倫倫姫だけでなく別途、自機関の情報セキュリティポリシーに沿った内容の「情報セキュリティ教育」を実施されることをお勧めします。

  - まずは、セキュリティ教育に迷ったら、倫倫姫を使ってみてください。

あらためて、

インシデントを未然に防ぐために、
ルール作りや人材育成で構成員の
「セキュリティリテラシー向上」
を図りましょう！！

NIIのセキュリティサービスをご活用ください

NII

ご清聴
ありがとうございました