人工知能学会 × セキュリティサマーサミット SSS2026

第 5 回 SIG-SEC 研究会 論文募集

人工知能学会 安全性とセキュリティ研究会（SIG-SEC）

生成 AI，基盤モデル，Agentic AI の普及に伴い，AI システムの安全性・信頼性・耐攻撃性・ガバナンスに関する研究の重要性が急速に高まっています。本研究会では，理論，システム，評価，運用，制度設計を含む幅広い観点から，AI セーフティ＆セキュリティおよび関連分野の研究発表を募集します。

セキュリティサマーサミット SSS2026 は，情報セキュリティに関連する電子情報通信学会 6 研究会（ISEC／SITE／ICSS／EMM／HWS／BioX）と情報処理学会 2 研究会（CSEC／SPT）に，新たに人工知能学会 SIG-SEC が加わり，9 研究会による共催／連催の合同研究会です。

開催概要・重要日程

発表申込締切	2026 年 5 月 11 日（月）	**開催日**	2026 年 7 月 13 日(月)〜15 日(水)
論文投稿締切	2026 年 6 月 10 日（水）	**会場**	札幌コンベンションセンター

※人工知能学会の会員でなくてもご発表・ご参加いただけます。

募集テーマ

1. AI システム／Agentic AI のセキュリティ

Agentic AI，AI エージェント，マルチエージェントシステム，AI システムセキュリティ，ツール利用型 LLM のセキュリティ，プロンプトインジェクション，間接プロンプトインジェクション，メモリ汚染，権限昇格・権限逸脱，ツール悪用，AI エージェントの監視・隔離・防御，AI システムのサプライチェーンセキュリティ

2. Deep Learning Security／敵対的機械学習

Adversarial Machine Learning，敵対的サンプル，回避攻撃，バックドア攻撃，トロイの木馬攻撃，データ汚染，学習時攻撃，推論時攻撃，モデル抽出，モデル盗用，モデル反転，Membership Inference，プライバシー攻撃，ロバストネス評価，証明可能ロバスト性

3. 連合学習・プライバシー保護・Machine Unlearning

連合学習，Federated Learning Security，Secure Aggregation，Byzantine 耐性，分散学習に対する攻撃と防御，プライバシー保護機械学習，差分プライバシー，Machine Unlearning，Certified Unlearning，削除要求対応，忘れられる権利と AI

4. AI を用いたサイバーセキュリティ

サイバー攻撃検知，侵入検知，異常検知，マルウェア検知，マルウェア解析，リバースエンジニアリング，脆弱性検出，脅威インテリジェンス，セキュリティ運用自動化，インシデント対応支援，プログラム解析，コード自動修復，AI による安全なソフトウェア工学

5. AI Safety・アラインメント・LLM Jailbreak

AI Safety，AI Alignment，LLM Safety，Jailbreak，脱獄攻撃の検知と防御，有害出力の抑制，報酬ハッキング，欺瞞的振る舞い，レッドチーミング，基盤モデルの安全性評価，人間参加型監督，安全制御とモニタリング

6. フェイクニュース・フェイクメディア

フェイクニュース検知，偽情報・誤情報分析，Deepfake 検知，合成メディア検知，コンテンツ真正性，来歴検証，ウォーターマーキング，マルチメディアフォレンジクス，SNS 上の情報信頼性

7. AI セキュリティエンジニアリング

AI Security Engineering，Secure-by-Design AI，Secure MLOps，LLMOps Security，モデル供給網管理，データセット供給網管理，セキュリティテスト，継続的評価，ランタイム防御，AI リスク分析，AI 保証，AI ベンチマーク，実装ガイドライン

8. AI ガバナンス・監査・法的規制

AI Governance，Responsible AI，AI 監査，AI コンプライアンス，AI 透明性，説明責任，制度設計，標準化，認証・保証，法的・倫理的課題，生成 AI・Agentic AI のガバナンス，安全・安心・プライバシー・法規制の統合的検討

キーワード例

Agentic AI Security，AI System Security，Adversarial Machine Learning，Adversarial Examples，Data Poisoning，Backdoor Attacks，Model Inversion，Model Extraction，Membership Inference，Federated Learning Security，Machine Unlearning，Privacy-Preserving Machine Learning，Cyber Attack Detection，Malware Detection，Reverse Engineering，Automated Program Repair，AI Safety，AI Alignment，LLM Jailbreak，Fake News Detection，Deepfake Detection，AI Security Engineering，Secure MLOps，AI Governance，AI Auditing，AI Regulation

論文投稿

論文投稿先（発表申込と論文投稿を兼ねています．投稿締切日までは論文を更新できます．）

https://www.ai-gakkai.or.jp/sig-system/sigusers/presenter_add/sec/sss2026

注）発表申込日までに**入力必須項目**（ご氏名*，ふりがな*，ご所属*，ご所属種別*，メールアドレス*，発表タイトル*，著者 1 人目*，編集用パスワード*）と**アブストラクト**を入力して下さい。原稿は論文投稿締切日までにアップロードして下さい。

論文は人工知能学会研究会原稿フォーマットで、8 ページ以内(Appendix，参考文献を含む)でご準備下さい。

人工知能学会研究会原稿フォーマット(LaTeX/Word)は、以下からダウンロードしてご利用下さい。

https://www.ai-gakkai.or.jp/sig/announce/sig-style/

安全性とセキュリティ研究会（SIG-SEC）SSS2026 に投稿された論文の著作権は，人工知能学会の規定に基づき原則として著者に帰属します。ただし，著者は，J-STAGE での無償公開，本研究会の円滑な運営に必要なダウンロード配信，ならびに共催・連催研究会におけるデジタルおよび紙媒体での掲載について，これを許諾するものとします。

優秀論文賞

優れた論文は，人工知能学会研究会優秀賞（JSAI Incentive Award）に推薦します。
https://www.ai-gakkai.or.jp/about/award/jsai_award-sig/

お問い合わせ先

ご不明な点がございましたら，SIG-SEC 研究会 SSS2026 実行委員会（sig-sec-sss2026cfp@ai.iisec.ac.jp）までお問い合わせください。