

AI時代、 私たちの「信じる」基準はどう変わる？

2026年07月03日（金）



 琉球大学
UNIVERSITY OF THE RYUKYUS

ChatGPTをはじめとする「生成AI」の登場により、論文の要約から複雑なプログラミングまで、私たちの学習・研究・業務のスタイルは劇的に進化しました。AIは間違いなく大学の知の探求を加速させる強力なパートナーです。しかし同時に、サイバーセキュリティの世界においても、AIはこれまでの常識を根底から覆す「パラダイムシフト」を引き起こしています。

特に、昨今のフロンティアAI/高性能AIと呼ばれるモデルの登場により、ソフトウェアやシステムのセキュリティ上の問題が多数発見され、大きな話題として取り上げられています。



特に攻撃者がそれらのモデルを悪用した場合、これまでの防御では守り切ることができず、社会インフラを含め様々なシステムが侵害されるのではないかと懸念が広がっています。

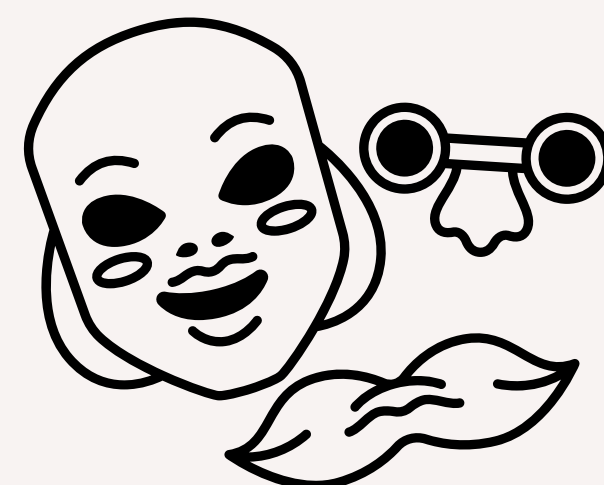
この懸念は社会全体の脅威としても認識され政府機関をも動かす大きなインパクトとして受け止められています。

何が変わるのか？（巧妙化する脅威と「ゼロトラスト」）

もちろん様々なシステムの防御については、専門家の仕事ということができますが、私たち個人が直視すべき変化もあります。

それは、「人間の五感を頼りにした直感的な確認だけでは、本物と偽物を見分けられなくなった」ということです。

これまでは、「怪しい日本語や不自然なレイアウトのメールは詐欺」という明確な見分け方がありました。しかし現在、攻撃者はAIを利用し、極めて自然な日本語で、学内の実在する行事やシステムのメンテナンスを装った精巧なフィッシングメールを大量に作成しています。



さらに海外の企業では、AIで作られた偽の役員の音声・映像（ディープフェイク）を用いたオンライン会議に騙され、約37億円が不正に送金されるという衝撃的な事件も発生しています。

このように「視覚や聴覚すらも偽造される」時代になったことで、セキュリティの考え方は根底から変わりました。

そのような環境の変化へ対応するために、皆様に多要素認証（MFA）をお願いしたり、アクセス権限を細かく制限したりするのは、みなさんの背後に潜もうとする高度な「AIのなりすまし」を排除するためであり、今後の身近なシステム利用における「新たな当たり前」としてご理解をお願いいたします。



何が変わらないのか？（最終防衛線は「あなた」自身）

一方で、脅威がどれほどAIによって高度化し、防御システムが新しくなっても、絶対に変わらない原則があります。それは、最終的な判断を下す「人間の批判的思考」と、「物理的な初動対応」の重要性です。

AIはどれほど流暢な文章を生成しても、もっともらしい嘘（ハルシネーション）をつくりリスクや、入力したデータが外部の学習に利用され情報漏えいを引き起こすリスクを内包しています。AIを「絶対的な正解を出す存在」として盲信せず、機密情報をプロンプトに入力しないこと、そして最後は必ず人間が事実確認を行うというルールは不変です。

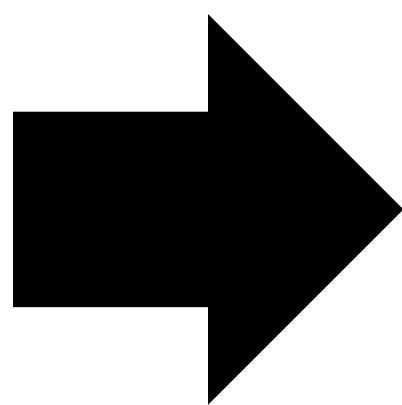
また、万が一「パソコンの動きがおかしい」「不審なリンクを押してしまったかもしれない」と感じた際の対処法も変わりません。相手がどれほど高度なサイバー攻撃であっても、通信経路を絶てば被害の拡大は防げます。異変を感じたら、迷わず「Wi-Fiの設定をオフにする」、あるいは有線であれば「LANケーブルを物理的に抜く」といった、根本的なネットワーク切断を行ってください。

どんな強固なシステムも、皆様一人ひとりの警戒心と日々のOSアップデートなどの自己点検がなければ機能しません。自身のデバイスが安全な状態にあるか、気にする習慣こそが最大の守りにつながります。一人ひとりの意識で安全・安心な日常をつくっていきましょう。

異変を感じた時の対処手順

- ① 不審なリンクを押してしまったかもしれない！

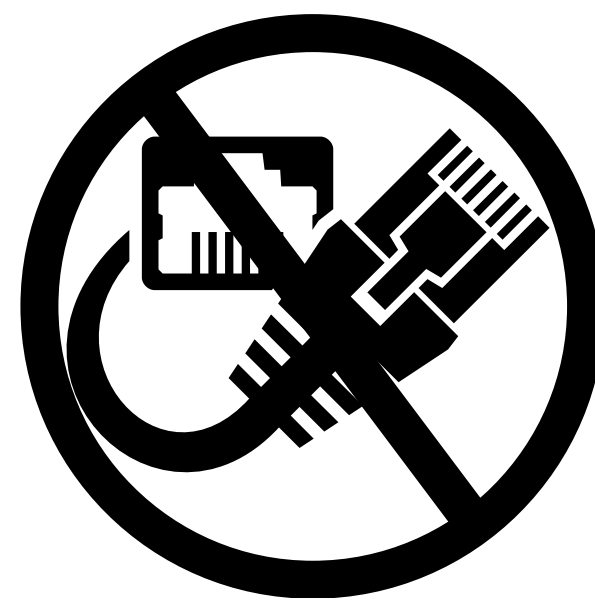
OH NO...



- ② ネットワークの接続を切る

→ LANケーブルを物理的に抜く

→ Wi-Fiの設定をOFFにする



※ ご自身で対応できない場合は本学の「総務部情報企画課(情報セキュリティ係)」へお問い合わせください。



ふちがみ しんいち
淵上 真一

日本電気株式会社 Corporate Executive CISO

NECセキュリティ株式会社 取締役

ベンチャー系システムインテグレータでのネットワークエンジニアを経て、専門学校グループを運営する学校法人に転職。

教員経験を経て、社外では司法、防衛関連のセキュリティトレーニングを手掛ける。2018年よりNECグループ全社セキュリティ統括を担当。

ISC2 認定主任講師、Cisco Networking Academy Instructor Trainer

情報処理安全確保支援士集合講習認定講師、北海道大学 客員研究員

サイバー安全保障人材基盤協会理事、日本情報経済社会推進協会（JIPDEC）

評議員、警察大学校嘱託講師、Hardening Project実行委員