東京大学 情報セキュリティ教育研究センターを設置

１．発表者：

石川　正俊（東京大学 大学院情報理工学系研究科長、創造情報学専攻 教授）
中村　　宏（東京大学 大学院情報理工学系研究科 システム情報学専攻 教授、情報セキュリティ教育研究センター センター長）

２．発表のポイント：

◆東京大学（総長：五神 真）は、本年 2 月 1 日付で、連携研究機構「情報セキュリティ教育研究センター」（センター長：中村 宏、以下「センター」という。）を設置し、平成 36 年 1 月 31 日までの 5 年計画の研究教育活動を開始します。(別紙参照)

◆本センターは、情報セキュリティの課題解決に関わる本学の 3 部局（情報理工学系研究科（責任部局）、工学系研究科、情報基盤センター）が連携し、実学としてのシステムセキュリティと学問としてのセキュリティ基盤技術を包括的に研究することを目指します。

◆本センターは、横断的・中長期的な視点でセキュリティ人材育成にも取り組み、産学官民とも連携しながら社会全体での情報セキュリティの確保を通じて、Society5.0（注 1）が目指すデータ駆動型社会（注 2）の実現・発展に寄与してまいります。

３．発表内容：

IT 社会の発展に伴い、サイバーセキュリティへの対応は、社会全体の喫緊の課題となっています。これまでもセキュリティ確保のためにさまざまな技術分野での研究が行われ成果を上げてきていますが、それを上回る勢いでセキュリティ脅威は増大し、社会的損失も増大しています。2018 年に内閣府サイバーセキュリティセンターから発表されたサイバーセキュリティ戦略では、新しい攻撃への防御やその被害を軽減させるためには、従来のような受動的な対策だけではなく、すべての主体が連携して多層的にセキュリティ脅威に対して積極的な防御策を講じる必要性を謳っています。同戦略ではまた、横断的・中長期的な視点で人材育成・研究開発に取り組み、一部の専門家がサイバーセキュリティの確保に取り組むのではなく、全員参加による協働を推進する必要性も謳っています。しかしながら、社会全体でセキュリティを確保するための総合的･体系的な取り組みは未だ十分とは言えません。

東京大学（総長：五神真）は、社会的に大きな課題となっている情報セキュリティ関連分野の先進的教育研究を強化すべく、総合的かつ体系的な取り組みを推進しています。

その柱として、本年 2 月 1 日付で、情報理工学系研究科（研究科長：石川正俊）が責任部局となり、工学系研究科、情報基盤センターの連携を得て、連携研究機構「情報セキュリティ教育研究センター」を設置し、平成 36 年 1 月 31 日までの 5 年計画の研究教育活動を開始します。

本センターの目的は、現在のセキュリティ技術の枠組みを超え、実学としてのシステムセキュリティと学問としてのセキュリティ基盤技術を包括的に研究することで、新たな情報セキュリティ技術体系を整備するとともに、当該分野の先進的かつ実践的な教育体系の構築と次世代を担う人材の育成を推進することです。

近年のセキュリティ脅威の増大には､攻撃対象の多様化と攻撃方法の高度化という背景があります。例えば IoT（注 3）の爆発的な普及により、人の管理が及びにくくセキュリティ要件が異なる大量の IoT 機器がサイバー空間につながることになり、これらの機器が新たに攻撃対象になり深刻な社会的損失を招く事態が発生しています。攻撃方法に関しても、スペクター (Spectre) や メルトダウン (Meltdown)と呼ばれるハードウェアの脆弱性（注 4）を突く，プロセッサの動作原理の根幹の再考を

迫る全く新しい攻撃や、標的型攻撃（注 5）のように攻撃対象者の社会的立場や社会情勢を利用するものも出現しています。このようにセキュリティ脅威の多様化と高度化が進む中で、コンピュータシステムの基本原理を理解する必要性が改めて指摘されるとともに、大量のトラフィックデータと機械学習を活用した技術が未知の攻撃に対する防御に有効であるとして、新しい学問領域としても実用的なセキュリティ対策としても有望視されています。このような新しい攻撃への防御やその被害を軽減させるためには、従来の技術進展の外挿だけでは限界があり、セキュリティを運用する現場での実際の脅威を分析しその知見を研究開発に活かすとともに、研究開発の成果をいち早く現場で活かす、実学と学問の統合が必要不可欠です。本センターではその実現を目指し、図に示すように、広範なセキュリティ関連基礎分野で先進的な研究に取り組んでいる情報理工学系研究科と工学研究科、および、本学のネットワーク運用の責任部局である情報基盤センターが密に連携し、実学としてのシステムセキュリティと学問としてのセキュリティ基盤技術を包括的に研究していきます。

人材育成に関しても､広範な学問領域に渡るセキュリティ分野の効果的な教育体系構築に取り組み、課題解決型学習（PBL、Project-Based Learning)など演習を含む実践的かつ体系化された実践的人材育成プログラムを構築し、文系も含む学部生、大学院生、および社会人を対象とした教育を実施することで､サイバーセキュリティの確保に対して全員参加による協働した取り組みの推進を目指します。このように横断的・中長期的な視点でセキュリティ人材育成にも取り組み、産学官民とも連携しながら、社会全体での情報セキュリティの確保を通じて、Society5.0 が目指すデータ駆動型社会の実現・発展に寄与してまいります。

４．用語解説：

(注 1)　Society5.0

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）のこと。狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く、新たな社会を指すもので、第 5 期科学技術基本計画において我が国が目指すべき未来社会の姿として初めて提唱された。

参考 URL：https://www8.cao.go.jp/cstp/society5_0/index.html

(注 2) データ駆動型社会：

データ自体が極めて重要な価値を有し、良質で豊富なリアルデータを活用することで大きな経済的な価値を生み出していく社会。未来投資戦略 2018 では、Society 5.0、データ駆動型社会への変革を基本戦略としている。

参考 URL：https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_zentai.pdf

(注 3)IoT：

Internet of Things の略。あらゆるモノ(thing)がインターネットにつながる形態。接続される機器を IoT 機器と呼ぶ。同時にこれまではサイバー空間にはつながらなかったモノがつながることを意味する。IoT の普及により、これまでは収集できなかったデータを IoT 機器により収集することで新しいサービスを創出できることに大きな期待が寄せられている。

(注 4) ハードウェアの脆弱性

脆弱（ぜいじゃく）とは「もろくて弱い様子」を意味し、ソフトウェアを含めた IT システムにおいて脆弱性とは「仕様上の欠陥やバグに起因する保安上の弱点」を意味します。これまでは実際に攻

撃された弱点は、ソフトウェアの仕様上の欠陥やバグに起因するものであり、脆弱性と言えばソフトウェアの脆弱性を意味していた。これに対し、スペクターやメルトダウンは、「ハードウェアの仕様上の欠陥」により、本来読めてはいけない秘密のデータなどが格納されているメモリが、当該データを読む権利の無い別のプロセスから読めてしまう、という弱点を突く攻撃である。

(注 5) 標的型攻撃

不特定多数を狙うサイバー攻撃に対し、明確な意思と目的を持った攻撃者が特定の組織に対して特定の目的（情報の窃取や削除）のために行うサイバー攻撃のこと。攻撃者が標的型攻撃を開始する際に行われる手法として多いのが、標的とした特定の組織の構成員に対して不正プログラムを送りつける、いわゆる標的型メールである。この場合、攻撃者は攻撃対象者に関する情報をあらかじめ入手して差出人を偽りメール本文や添付ファイルを作成するなど、メール受信者の警戒心を和らげるような工夫がなされるため、似たような内容が繰り返し届くスパムメールに比べるとその防御は難しくなる。

別紙

東京大学 情報セキュリティ教育研究センター

情報理工学系研究科・工学系研究科・情報基盤センター

社会全体でのセキュリティの確保へ

セキュリティに関する
分野横断型の包括的研究

横断的・中期的な視点での
セキュリティ人材育成

実運用のデータを用いた実践的サイバーセキュリティ研究
広範な学問領域に渡るセキュリティ分野の効果的な教育体系構築に関する研究
学部生・大学院生および社会人を対象とした実践的人材育成

分野横断型の研究
- ハードウェアからアプリまでのマルチレイヤの攻撃対策
- AI技術を活用した未知の攻撃に対する防御

実学としてのシステムセキュリティと学問としてのセキュリティ基盤技術を包括的に研究
(情理・工・情基)

多岐にわたる人材の必要性
- 2020年までに20万人の人材不足
- 一部の専門家がセキュリティ確保に取り組むのではなく、全員参加による協働した取り組みの必要性

広範なセキュリティ関連
基礎分野での先進的な研究
(情報理工学系研究科・工学系研究科)

暗号理論、暗号プロトコル、認証技術
ソフトウェア検証、セキュアチップ

連携

セキュアなシステム運用に資する
実践的分野
(情報基盤センター)

ネットワーク運用とセキュリティ、
トラフィック異常検知、サイバーレジリエンス