共同研究の目的・内容について

2017年4月26日 中部電力株式会社



共同研究の目的



- ○高度化・巧妙化するサイバー攻撃手法に対して、産学官・企業間の連携を強化して対処することが 必要不可欠になっております。
- ○当社は、慶應義塾大学および日立製作所と共同研究を本年4月から開始し、<u>サイバーセキュリティ</u> における連携手法の確立を目指します。

従来のセキュリティ体制

各組織それぞれ独立したセキュリティ監視体制

組織A

セキュリティ 監視体制

組織B

セキュリティ 監視体制

組織C

セキュリティ 監視体制

問題点

・標的型攻撃と呼ばれる特定の組織を狙った新たなサイバー攻撃手法に関する機動的な連携ができていない

目指すセキュリティ連携体制

セキュリティ監視体制を組織間で連携

組織A

組織B

組織C

セキュリティ監視体制

連携のメリット

- ・サイバー攻撃の情報および対処法を共有、 新たな攻撃への対処力向上
- ・セキュリティを組織間で相互バックアップ、 可用性を向上

⇒セキュリティ能力のさらなる向上

共同研究の内容



○本研究により、サイバーセキュリティにおける連携手法の確立および検知能力の向上を目指します。 (研究期間: 2017年4月~2018年3月)

本研究の主な内容 主な課題 自動的かつ早期に情報共有ができる サイバー攻撃の情報共有を人間が ように、サイバー攻撃情報のパターン 行っていたため、多発するサイバー 化技術を研究 攻撃に対処が追い付かない 共有するサイバー攻撃情報の中に 情報共有時の外部漏洩を防止する は、セキュリティ上の機微な情報が セキュリティ技術の研究 含まれる (3) サイバー攻撃検知技術および組織 セキュリティ攻撃が巧妙化し、検知 間でサイバー攻撃検知能力を相互 が困難になっている バックアップする仕組みの研究

3者の研究における役割



○3者それぞれの強みを活かし、共同研究を実施します。





慶應義塾

HITACHI

【役割】

・重要インフラ事業者として セキュリティオペレーションを 長年実施してきたノウハウ・ データの提供



・多岐にわたる研究の場を提供

【役割】

・セキュリティ分野における 技術の提供







サイバーセキュリティ分野における 共同研究