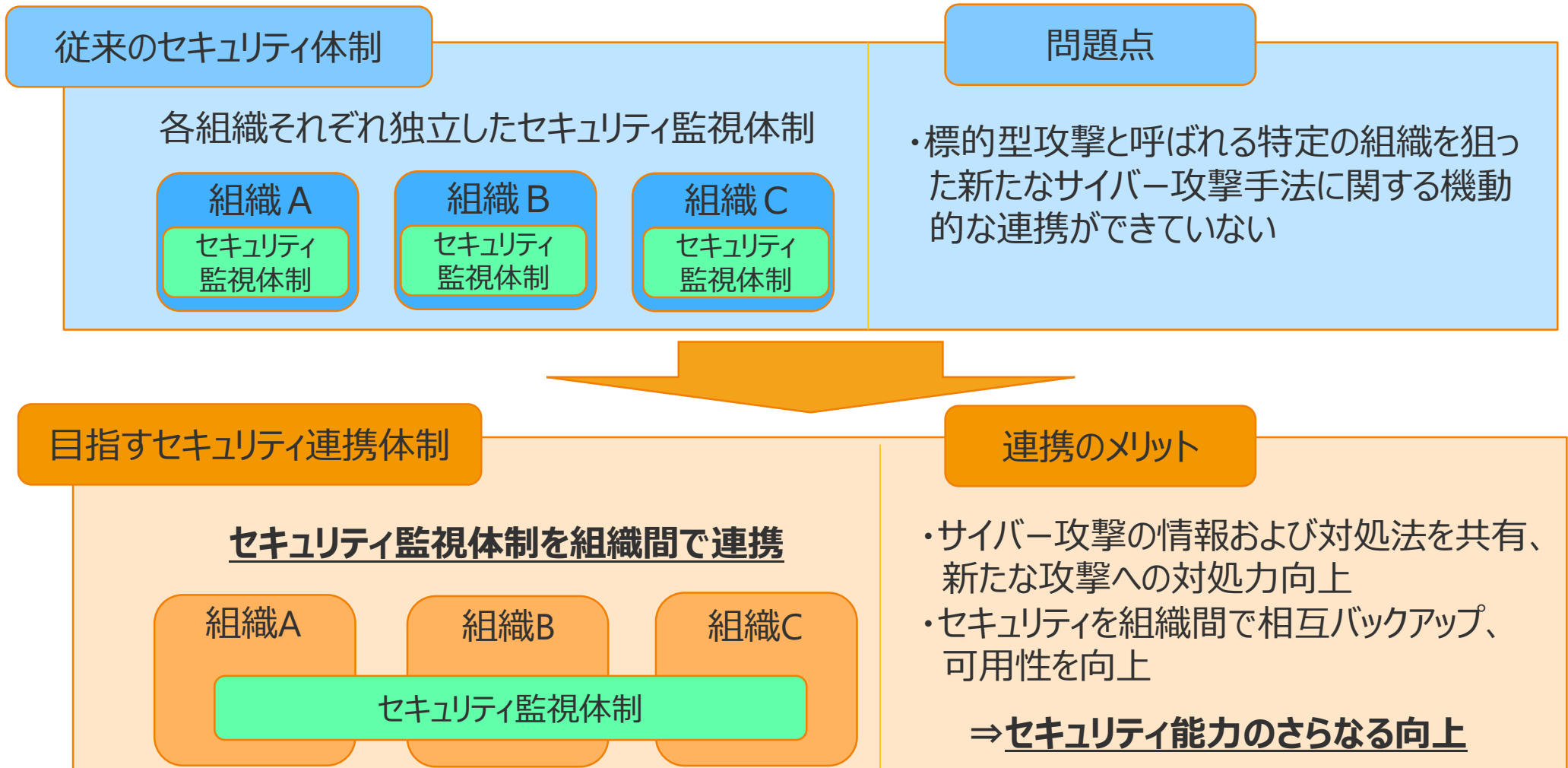


共同研究の目的・内容について

2017年4月26日
中部電力株式会社



- 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、**サイバーセキュリティにおける連携手法の確立**を目指します。



- 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)

主な課題

- ① サイバー攻撃の情報共有を人間が行っていたため、多発するサイバー攻撃に対処が追い付かない
- ② 共有するサイバー攻撃情報の中には、セキュリティ上の機微な情報が含まれる
- ③ セキュリティ攻撃が巧妙化し、検知が困難になっている

本研究の主な内容

- ① 自動的かつ早期に情報共有ができるように、サイバー攻撃情報のパターン化技術を研究
- ② 情報共有時の外部漏洩を防止するセキュリティ技術の研究
- ③ サイバー攻撃検知技術および組織間でサイバー攻撃検知能力を相互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。



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

【役割】

・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**