

共同研究の目的・内容について

2018年1月24日

中部電力株式会社

株式会社中電シーティーアイ



日々巧妙化するサイバー攻撃による被害を防ぐため、サイバー攻撃の予兆※を早期に検知することが非常に重要になっています。

※特定の対象を狙い撃ちする「標的型攻撃」と呼ばれるサイバー攻撃は、攻撃開始前に攻撃対象を偵察していると言われており、この偵察行為がサイバー攻撃の予兆になります。

<攻撃対象システム>



検知

サイバー攻撃前の偵察
(サイバー攻撃の予兆)

<攻撃者>



予兆の段階で検知して対処

被害を未然に防止できる

NICTとPwCサイバーサービスとの共同研究により、特にサイバー攻撃の予兆を早期に検知するための情報収集・分析に関する知見を高め、さらなるサイバーセキュリティの確保に努めてまいります。（研究期間:2018年1月～2019年3月）

<研究体制>

中部電力

所有する各種システムを
研究の実証フィールドとして活用・検証

NICT

サイバーセキュリティの開発技術を
を中部電力のシステムで試行する

中電シーティーアイ

中部電力のシステムにおける作業の支援および
セキュリティ監視に関する知見の提供

PwCサイバーサービス

世界のサイバーセキュリティの
最新状況に関する知見を提供

最先端の技術・知見を、中部電力が提供する
実証フィールドに適用し、実践的な研究を実施

(参考) 目指す将来像

共同研究の成果を中部エリアのお客さまと連携し、中部エリア全体のサイバーセキュリティ確保に貢献することを目指します。

- 情報通信研究機構・PwCサイバーサービスとの共同研究
(サイバー攻撃の検知技術の向上)
- 慶應義塾大学・日立製作所との共同研究 (2017年4月28日お知らせ済み
(組織間のセキュリティ連携手法の確立))

各共同研究の成果を中部エリアのお客さまと連携



中部地域の
企業A

中部地域の
企業B



中部エリア全体のサイバーセキュリティの確保