2019 年 6 月 18 日
慶應義塾大学
中部電力株式会社
株式会社日立製作所

複数組織で観測したダークネット通信を分析することで サイバー攻撃の予兆を検知、被害の未然防止に貢献

慶應義塾大学（塾長:長谷山　彰）、中部電力株式会社（代表取締役社長：勝野　哲／以下、中部電力）、株式会社日立製作所（執行役社長兼 CEO:東原　敏昭／以下、日立）は、巧妙化するサイバー攻撃に対し、各組織が観測した不審な通信のうちダークネット通信*1を分析することで、これまでは検知することが困難であったサイバー攻撃の予兆検知ができることを実証しました。予兆検知により、サイバー攻撃による被害の未然防止に貢献します。

*1 インターネット上のアドレスのうち、特定のコンピューターに割り当てられていない（利用されていない）アドレスに対する通信

さまざまな分野でのデジタル化の進展により人々の生活が便利になる一方で、サイバー攻撃は巧妙になり、サイバーセキュリティの重要性が急速に高まっています。特に、人々の生活を支えるインフラ事業におけるセキュリティ対策の強靭化は、喫緊の課題となっています。

多くの企業や組織では、不審な通信を個別のネットワークのみで監視していますが、不審な通信は多量の正常な通信に紛れ込んでいるため、判別するのが難しいという課題がありました。

今回、慶應義塾大学、中部電力、日立は、一般の通信では発生しないダークネット通信に着目するとともに、複数組織の通信を分析することでサイバー攻撃の予兆を検知できることを実証しました。

【新技術開発と実証の概要】

慶應義塾大学と日立がこれまで共同で研究してきたインシデント分析ノウハウに基づいて、ダークネット通信の相関分析技術を開発しました。これは、複数組織に共通して現れるダークネット通信に着目し、個別の組織の観測では目立たなかったサイバー攻撃の予兆を検知する技術です。

今回、この相関分析技術を用いて、慶應義塾大学と中部電力で観測した大量のダークネット通信（2,000 万件/日）を分析、このうち極めて少数の通信でもサイバー攻撃の予兆を検知することができ、適切に対処する事ができました。

なお、今回の実証は、2017 年 4 月から慶應義塾大学、中部電力、日立が取り組んできた共同研究および「分散型セキュリティオペレーション」*2 構想の成果です。

*2 複数のセキュリティ対応チームが連携し、迅速なインシデントレスポンスを行う

今後も、慶應義塾大学、中部電力、日立は、攻撃の予兆を広範囲に検知し、攻撃内容についてもより詳細に分析できるよう技術開発を進め、サイバーセキュリティ確保と社会インフラシステムの安定運用の確保に資するセキュリティオペレーションの実現に貢献していきます。

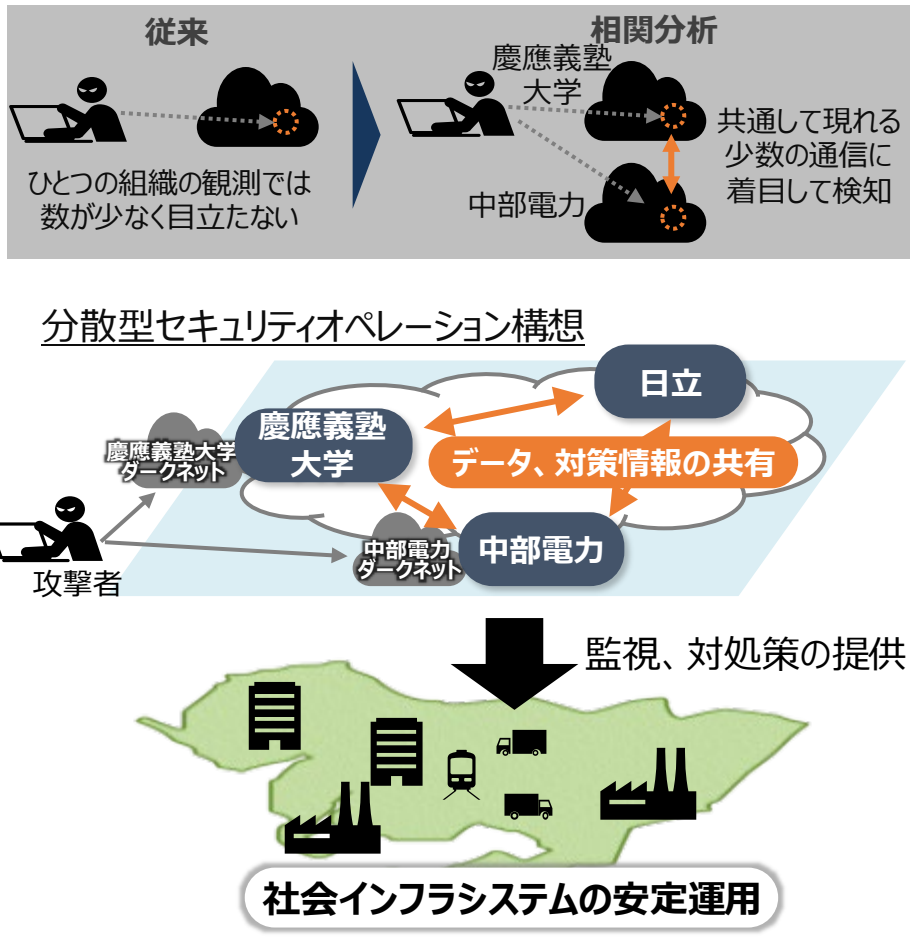

図 ダークネット通信分析によるサイバー攻撃の予兆検知

■研究に関するお問い合わせ先
慶應義塾大学大学院メディアデザイン研究科
教授　砂原 秀樹（すなはら　ひでき）
Email: cybersec-lab-inq@kmd.keio.ac.jp

■報道機関お問い合わせ先
慶應義塾　広報室　[担当:並木]　電話:03-5427-1541　Email:m-pr@adst.keio.ac.jp

中部電力株式会社　広報室　報道グループ　電話:052-961-3582

株式会社日立製作所　ブランド・コミュニケーション本部　広報・IR 部　[担当:松村]
電話 03-5208-9324（直通）

以　上