2018 年 2 月 5 日
慶應義塾大学
株式会社日立製作所

複数セキュリティ対応チーム間で連携して迅速なインシデントレスポンスを実現する「分散型セキュリティオペレーション」を実証

産学連携でサイバー攻撃の迅速な検知と対策を実現

慶應義塾大学(塾長:長谷山　彰)と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、高度化・大規模化するサイバー攻撃に対して、SOC[*1]や CSIRT[*2]などの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「分散型セキュリティオペレーション」構想を策定し、実証環境を構築しました。従来人手で行っていた「セキュリティインシデントの検知から専門チームに分析を依頼し、分析データの共有を開始するまでの処理」を自動化し、1 秒以内に完了できることを実証しました。今後、慶應義塾大学と日立は、本構想の実用化に向けた研究を進め、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。

サイバー攻撃のスピードは年々高まっており、短時間に多拠点が攻撃されるリスクは増加しています。さらに、クラウドや BYOD[*3]の進展で、守るべき対象が自組織のシステムからクラウドや個人端末にまで拡大しており、革新的なセキュリティ対策が求められています。

慶應義塾大学と日立は、2016 年 2 月より、サイバー攻撃に対するセキュリティ運用管理や個人情報の安全性に関する共同研究を開始しました[*4]。今回、25 年以上にわたりインターネットの進展に貢献してきた慶應義塾大学の知見と、社会インフラシステムの構築やセキュリティインシデントの予防・対応に努めてきた日立の知見を融合して、「分散型セキュリティオペレーション」構想を新たに策定し、その中核技術の一つとなる「動的認証認可技術」を開発しました。「分散型セキュリティオペレーション」と「動的認証認可技術」の特長は以下の通りです。

1.「分散型セキュリティオペレーション」について

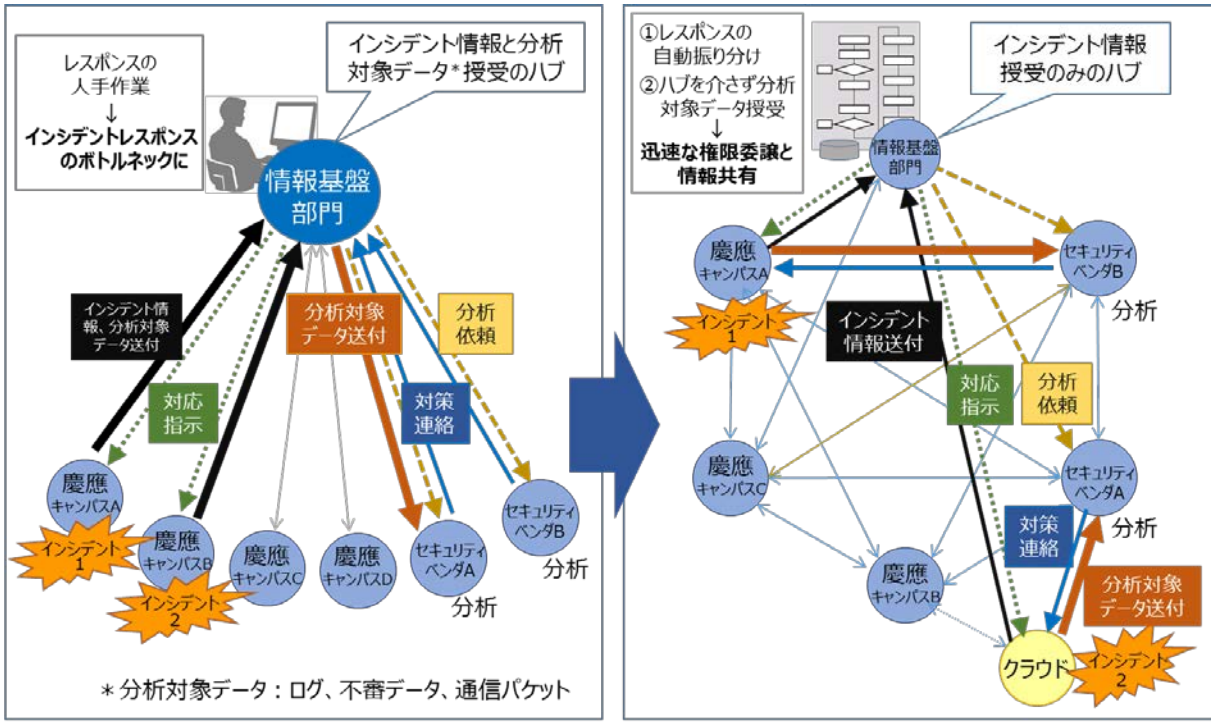
従来のインシデントレスポンスでは、特定のセキュリティ対応チームをハブとして、インシデント情報と分析データ(ログ、不審データ、通信パケット)を集約し、人手作業で複数のセキュリティ対応チームに分析依頼と分析データの送付を行っていました(図(a))。今回策定した「分散型セキュリティオペレーション」構想では、特定のセキュリティ対応チームがすべてのインシデントレスポンスに関与するのではなく、クラウドプロバイダなどの各組織にあるセキュリティ対応チームが自律分散的にインシデントに対処し、必要に応じて連携します。

2.「動的認証認可技術」について

「分散型セキュリティオペレーション」の中核技術の一つとなる「動的認証認可技術」では、情報収集や分析などのインシデントレスポンスに求められる機能を標準化して、それぞれのセキュリティ対応

チームが持つ機能を互いにリアルタイムで確認できるようにしました。これにより、分析依頼や分析データ共有などの処理をどの専門チームへ委託するかを機械的に振り分けること(認可)を可能にします。さらに、関与する組織が新たに判明する度に、認可からデータ送受信組織間の承認(認証)までの一連の処理を自動的に行うことで、迅速なセキュリティ対策を実現します(図(b))。

本技術の効果を検証するため、慶應義塾インフォメーションテクノロジーセンターで監視しているインシデントの分析対象データを、日立の「オープンラボ横浜*5」にある研究用の SOC に送付し、分析を委託する実証環境を構築し、2017 年 11 月より評価を開始しました。この結果、従来は担当者の習熟度によって、数分から数時間とばらつきのあった「インシデント検知から分析を依頼する一連の処理」を 1 秒以内に完了できることを確認しました。



図(a)従来のセキュリティオペレーション

図(b)動的認証認可技術を用いた分散型セキュリティオペレーション

今後、慶應義塾大学と日立は、今回構築した実証環境を活用して「分散型セキュリティオペレーション」を実現する技術開発を進めるとともに、本技術を日本 CSIRT 協議会*6 に提案し、激甚化するサイバー攻撃の脅威に対処し、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。

なお、本成果は、2018 年 3 月 6 日に開催される「情報処理学会インターネットと運用技術研究会」で発表予定です。

*1 SOC: Security Operation Center サイバー攻撃や各種セキュリティインシデント等の監視や分析を行う組織のこと

*2 CSIRT: Computer Security Incident Response Team

*3 BYOD: Bring Your Own Device 企業などで従業員が個人保有の情報端末を職場に持ち込んで業務で利用すること

*4 2016 年 2 月 29 日ニュースリリース https://www.keio.ac.jp/ja/news/2015/osa3qr000001em4w-att/160229.pdf
http://www.hitachi.co.jp/New/cnews/month/2016/02/0229.html

*5 2016 年 11 月 30 日ニュースリリース http://www.hitachi.co.jp/New/cnews/month/2016/11/1130.html

*6 http://www.nca.gr.jp/outline/index.html

■照会先

慶應義塾大学 環境情報学部 教授／慶應義塾インフォメーションテクノロジーセンター 所長
中村修（なかむら おさむ）
Email：osamu@sfc.keio.ac.jp

株式会社日立製作所 研究開発グループ 技術統括センタ [担当：阿部、藤原]
〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地
電話：050-3135-3409（直通）

■報道機関お問い合わせ先

慶應義塾 広報室 ［担当：並木］
〒108-8345 東京都港区三田 2-15-45
電話：03-5427-1541
Email：m-koho@adst.keio.ac.jp

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：丸谷]
〒100-8280 東京都千代田区丸の内一丁目 6 番 6 号
電話：03-5208-9324（直通）

以上