担当教員のページ

研究室紹介：分散システム研究室と教育情報システム研究室

森　　真　幸*
morim@kit.ac.jp

1　はじめに

情報科学センターにおいて、分散システム研究室(DSM：Distributed System Laboratory)では組織におけるネットワークシステム全般に関する研究を行っています。また、教育情報システム研究室(ET：Educational Technology Laboratory)では教育のための情報技術の研究を行っています。本稿では、両研究室で2018年度に実施した研究の中から5件紹介するとともに、研究室の体制や現状について報告いたします。

2　無線LAN環境におけるOpenFlowによる通信制御の実現

通信技術の発展により、無線LAN(Local Area Network)が生活の様々な場所で利用されています。ノートパソコンやスマートフォンはもちろんのこと、IoTの普及から無線LANを利用できる機器が増加しています。一方で、無線LAN Access Point(以下APとする)を狙った不正利用や、無線LANを利用しているデバイスを狙った攻撃等も増加してきており、無線ネットワークのセキュリティの向上が求められています。

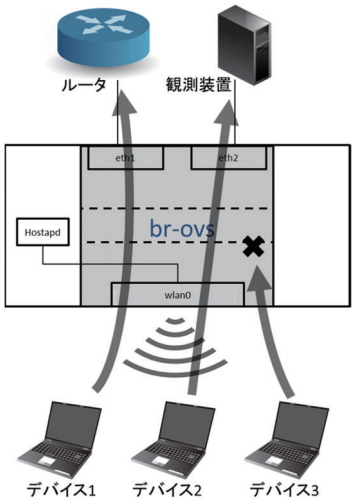

図1　無線LAN環境におけるOpenFlowによる通信制御の例(デバイス3のみ通信を破棄)

本研究では、無線LANを利用しているデバイスの個々の通信に対して、転送、破棄、書き換え等の処理を動的に行える機能を実装した無線LAN APを提案します。また、提案したシステムをSDN(Software Defined Network)を実現する技術の一つであるOpenFlowを用いて試作し、性能計測等の実験から通常の無線LAN APとの性能差がないことを示しました(図1)。それにより、無線環境における不正通信デバイスを隔離できるようなセキュアなネットワークを実現できる可能性を示しました。

3　自律制御型エージェント機器によるセンサデバイス管理システムの試作

家電製品やセンサといった様々なモノ(以降センサデバイス)がインターネットに接続するIoT化の動きが進んでいます。IoTを活用したシステムでは、センサデバイスがインターネットに接続されていることを前提としていますが、各所に存在する複数のセンサデバイスに対して、管理者が適切な設定を行うことへの負担は非常に大きいです。また、センサデバイス周辺の通信インフラの状況によっては、特定の通信手段を使用できないためにシステムの可用性が失われることがあります。そこで、本研究ではセンサデバイス管理者の負担を軽減する自律制御型エージェント機器によるセンサデバイス管理システムの試作を行いました。試作システムを使用し、エージェント機器が通信状況に応じた通信手段の切り替え、管理ページの表示・更新、Webページを用いたセンサデバイスへの設定変更の動作確認を行いました(図2)。試作シス

＊情報科学センター　助教

テムにより、センサデバイス管理者の負担の軽減および、システム全体の可用性を向上させることができると考えられます。

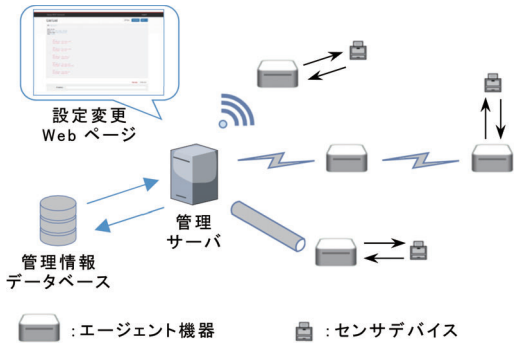

図 2　自律制御型エージェント機器によるセンサデバイス管理システムの構成

4　柔軟な応答制御機構を持つ分散処理型 DNS ファイアウォールの提案と評価

インターネットの通信における重要なシステムとして DNS があります。DNS はドメイン名を分散管理・運用するためのシステムであり、IP アドレスとの対応付けや、メールの宛先ホストの指示等を行うことが可能です。一方で、DNS サーバは DDoS 攻撃や DNS リフレクター攻撃等の様々な攻撃の対象や、攻撃のための踏み台にしようとする不正通信にさらされています。DNS サーバのサービスが停止してしまうことによる被害は大きく、インターネットの安定した運用のためには、安定した DNS サーバの運用が必須です。

本論文では、DNS サーバの前段に DNS クライアントからの通信を監視し攻撃者からのクエリに対してレスポンスを適応的に制御するシステムを配置し、DNS サーバへの攻撃を抑える手法を提案します(図 3)。また、提案システムを試作し、性能評価を行いました、さらに、実際の DNS サーバが受信したクエリの分析を行い、その結果をもとに提案システムを利用することで DNS の安全性を保つことに繋がることを示しました[1]。

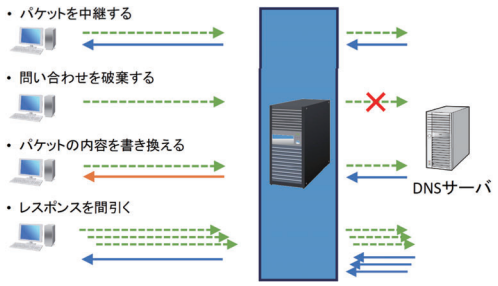

図 3　DNS ファイアウォールによる柔軟な応答制御機構

5　仮想マシンに対するバックグラウンドチェックポイントの管理システムの提案と試作

IT 技術の発展と PC や携帯端末の普及により情報システムの利用が拡大するとともに、ユーザや組織はサイバー攻撃の危険にさらされています。そのため、セキュリティ教育の実施は急務の課題とされています。実践的なセキュリティ演習では、サイバー攻撃を模擬的に受けるためシステムを壊してしまうことが考えられます。そのため、試行錯誤できる演習環境の提供が求められています。このような環境を提供するために、本研究では、演習環境に対してチェックポイントを任意に取得し、必要に応じてチェックポイントから再実行できるシステムの提案を行いました。提案システムでは、演習環境の提供を実現するため仮想化を利用し、仮想化基盤として QEMU を用いました。また、チェックポイントとして QEMU のマイグレーション機能と ZFS のスナップショット機能を利用することで、目的の演習環境を作成しました(図 4)。試作システム上で実際に演習した結果、演習者への影響を抑えながらチェックポイントを作成することはできました。また、マイグレーションの停止時に演習者が入力を行う状態になると入力が反映されないといった影響が出ることが分かりました。

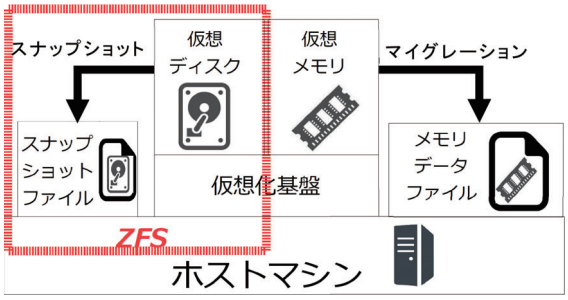

図 4　チェックポイント作成時の仮想ディスクと仮想メモリのデータ取得

6　SimpleSAMLphp を用いた SAML 認証連携におけるユーザ属性動的更新機構の試作

大学等の教育機関では、受講登録や授業の課題提出をオンラインサービス上で行うようにな

りました。これらのサービスは、認証基盤を用いて複数のサイトを連携して構築することが多いです。連携されたサービスをユーザが利用する際、複数サイト間で認証連携を行う必要があり、標準規格としてSAML(Security Assertion Markup Language)が広く用いられています。現在、一般的なSAMLの実装では、ユーザの属性情報を受け取るタイミングは認証を行ったタイミングに限られており、認証後に更新された属性を随時反映する枠組みになっていません。そのため、リアルタイムで変化するユーザ属性に基づいたアクセス権限制御を実現するには、ユーザ属性の動的更新を前提とした認証基盤を構築する必要があります。本研究では、SAML認証におけるシステム連携の枠組みの下で、属性情報が変更される度に随時ユーザの属性情報を更新しアクセス制御を行うシステムを試作しました。具体的には、BLE(Bluetooth Low Energy)ビーコンであるBLE Nano v2とRaspberryPiを用いて属性情報として在室情報を取得します。在室情報の変更があった際、AA(Attribute Authority) はIdP(Identity Provider)にSAML認証規格に沿った通知メッセージを送ります。その後、同様にIdPはSP(Service Provider)に通知メッセージを送ります。SPは、そのメッセージを受け取り、受け取った属性情報に基づいてアクセス制御を行います(図5)。

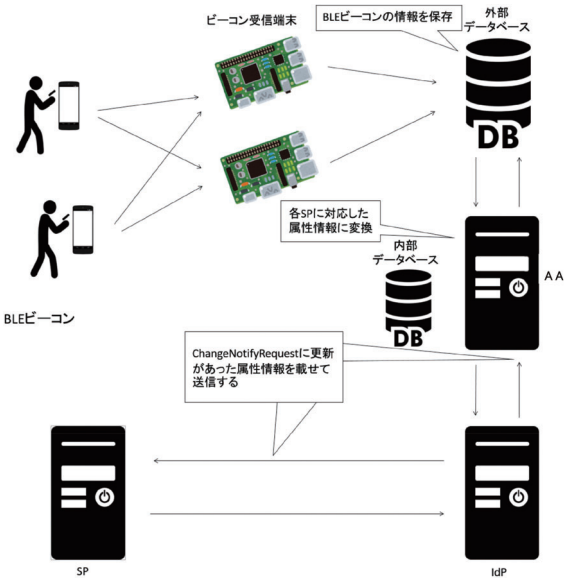

図5　BLEビーコンを用いたSAML認証連携によるユーザ在室情報の動的更新

7　研究室の現状

分散システム研究室と教育情報システム研究室は情報科学センター研究室101bと研究室103を共同で利用しています。現在(2019年9月)、研究室101bに11脚(DSM 5、ET 6)、研究室103に10脚(DSM 6、ET 4)の机が配置されています。2019年10月にはイタリアのトリノ工科大学から留学生が分散システム研究室に配属され、両研究室で総勢21名の学生が研究活動に邁進しています。

8　おわりに

本稿では、分散システム研究室と教育情報システム研究室から代表的な研究テーマの紹介と、研究室の体制と現状について報告しました。両研究室のより詳細な研究内容につきましては研究室のWebサイト(DSM…https://secure.dsm.cis.kit.ac.jp/、ET…https://www.et.cis.kit.ac.jp/)、または情報科学センター内展示ポスターをご覧ください。

参　考

[1] Shun Segawa, Hideo Masuda and Masayuki Mori: Proposal and prototype of DNS server firewall with flexible response control mechanism: Proc. of 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing(SNPD2019), pp.466-471(2019)