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開発を行っています。本稿では、これらの研究室で2016年度に実施した研究の中から6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　耐障害性の高い非常時一斉メール送信と冗長化した蓄積型配送を実現するメッセージングシステムに関する研究

手軽に相手にメッセージを送ることができるようになった昨今、それは日常的なものだけではなく、緊急時の連絡手段としても利用されています。災害が発生した際には安否確認の手段となるため、受信者に確実にメッセージを届ける必要があります。そこで、電子メールに着目しエラー削減や耐障害性の向上、通信手段の冗長化を実現したメッセージングシステムに関する研究を行いました。

大学等、高等教育機関が発行したメールアドレスへのメールは利用者である学生によって普段使用している別のメールアドレスへ自動転送されているケースがあります。ただし、学生はメールアドレスを頻繁に変更する傾向にあり、そのたびに自動転送先のアドレス変更を忘れがちになります。そこで、エラーメールの返送先アドレスとなるEnvelope-Fromを自動転送サーバ自身が受信できるように変更して自動転送する仕組みを考案しました。自動転送サーバが受信したエラーメールをデータベースに記録することでメールアドレスごとのエラー状況を把握し、継続してエラー転送設定者や管理者等に修正を促すよう通知することが可能になります。

また、電子メールの耐障害性の向上のためネットニュースシステムを使用したメッセージング方式を考案しました（図1）。メールサーバの受信部と保存部を分離し、保存部を複数箇所に配置し、ネットニュースプロトコルにより同期を行います。メールは暗号化してネットニュース記事として投稿され、受信者はアクセス可能な保存部で閲覧できます。これにより、自組織のメールサービスが利用できなくても複数あるいずれかの保存部にアクセスできればメールの閲覧が可能です［1］。

さらに、災害時に有効な通信手段は時代や災害状況によって変化するため、電子メールだけでなくTwitterやFacebook等、複数の通信手段を併用することで頑強にメッセージをやり取りできる方法を考案しました。利用者側からはメーラーのインターフェイスでメッセージの送信を可能にすることで利用のための学習コストを低く抑え、複数の通信手段から迅速にメッセージを配信することができます。

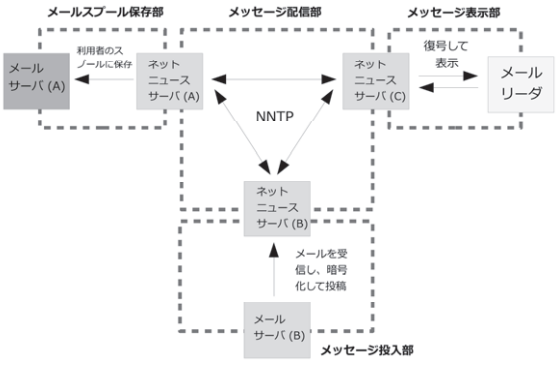

図1　ネットニュースシステムを使用したメッセージング方式

＊情報科学センター　助教

これらの方法を利用することにより、災害発生等の緊急時に組織の構成員の状況を早期に把握し、その後の復旧計画の立案に大いに役にたつと考えられます。

3　災害時利用を考慮したネットワークから収集した利用者属性を活用できる学内ネットワークシステム構成の提案

災害時には、情報の発信や収集にインターネットの活用が有効とされています。災害時に避難所になりうる大学も、非構成員にインターネット接続を提供することを考えた際、管理者や利用者に負担をかけずに利用者を把握するには、学内ネットワークインフラに利用者を区別できる柔軟さを持たせることが必要です。また、利用者が区別できることで、それぞれに応じた適切なサービスや情報提供を行うことが可能になります。

そこで、利用者の属性を活用できる学内ネットワークの構築を目的とし、その利用者の属性をネットワークに接続した際の記録から把握することを提案しました。利用者の区別には利用端末の MAC アドレスを使用し、非構成員には専用の SSID を作成します。これにより、災害時の学内ネットワークの利用登録が不要になります。また、個人の属性情報については利用規約の提示を行った上で、インターネット接続用 SSID を介した通信の暗号化を行うことでプライバシーを保護します。本研究で提案したネットワークシステム構成を使用することにより、災害時のインターネット接続、接続位置や回数に応じた情報の提供が可能になります（図 2）。

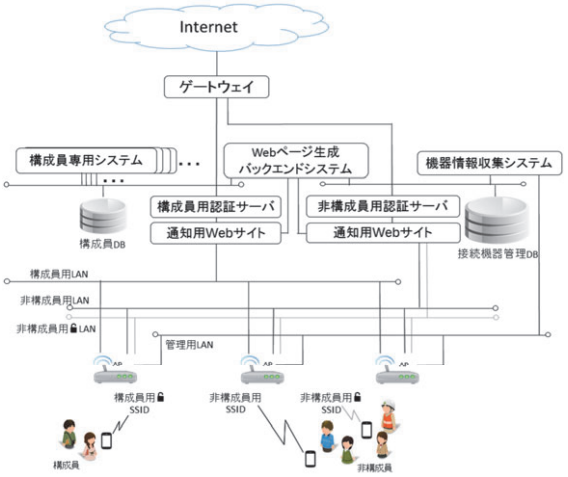

図 2　利用者属性を活用できる
学内ネットワークシステム

4　インアクティブ IP アドレスを利用した OpenFlow ベースの不正通信分別システムの試作の評価

インターネットを利用したサービスを提供する場合、正規のユーザのみがアクセスできる機密性、情報が改竄されないように保護できる完全性、サービスを安定して継続的に提供できる可用性といったセキュリティを保つことが求められます。そのためには、ネットワークを介してシステムの脆弱性を突くような不正な通信を観察分析し、情報の持ち出しや改竄等といった攻撃を検出、予想していくことが重要です。

本研究では、インターネットを介した様々な不正通信の対策として、学外から学内のインアクティブ IP アドレス（通信が行われていない IP アドレス）宛の全通信を正規の通信と分離し、攻撃者の侵入方法や侵入後の攻撃を監視、記録するシステムであるハニーポットに転送できるシステムを開発しました（図 3）。開発はソフトウェアでネットワークを制御できる OpenFlow をベースに行いました。本システムではインアクティブ IP アドレスが通信を始めアクティブになった際に、即座に正規の通信の転送先を学内に切り替えることが可能です。

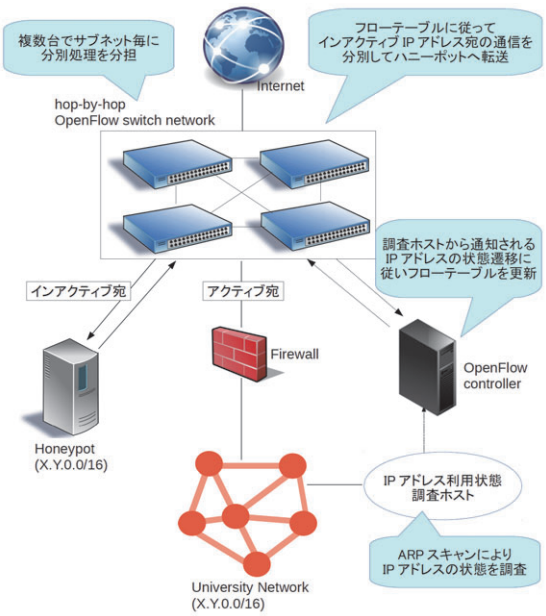

図 3　インアクティブ IP アドレスを利用した
OpenFlow ベースの不正通信分別システム

また、切り替え前の攻撃者とハニーポッドとのセッションは維持可能です［2］。また、複数台で処理を分担することで本学のクラスB程度のアドレスブロックなら数台で全IPアドレスをカバーすることができます。本研究により、全ての未使用IPアドレスをハニーポットに利用することで、多数のIPアドレスを保持する大学等のネットワーク全体を疎らにハニーポット化した攻撃解析システムの実装が可能となりました。

5　非永続型プロセスのための持ち寄り型クラウドシステムの試作と評価

近年、PC等のICT（Information and Communica-tion Technology）機器の低価格化や高性能化が進み、個人や企業等の組織で手軽に高性能なPCを用意できるようになってきています。しかし、サーバ機器等の特殊な例を除いて、夜間や休日等のPCを利用しない時間が存在し、計算資源を十分に活用できていません。そこで、PCを利用しない時間帯に別の用途で活用することを目的に、PCのリソースを持ち寄り、仮想化して統合できるクラウドシステムを提案します。本システムでは、PCが本来の用途で使用される際に即座に統合から解除できるよう、クラウドシステム上で動作させるプロセスを非永続型に限定しました。また、非永続型のプロセスをDockerを用いたコンテナ仮想化環境上で動作させることにより、軽量かつ高速にプロセスを展開できると考えられます。

本研究では使用されていないPCをOpenStackで集約した提案システムの試作と評価を行いました（図4）。その結果、計算資源の集約と分離を高速に行うことが可能となりました。また、OpenStackを用いることにより、PCやコンテナの管理等をWebブラウザ上のGUIから一元管理が可能になりました。さらに、PCの状態遷移は即座に行えることが確認できましたが、コンテナの廃棄にはおよそ100秒必要であるため、その時間短縮が課題になることがわかりました。

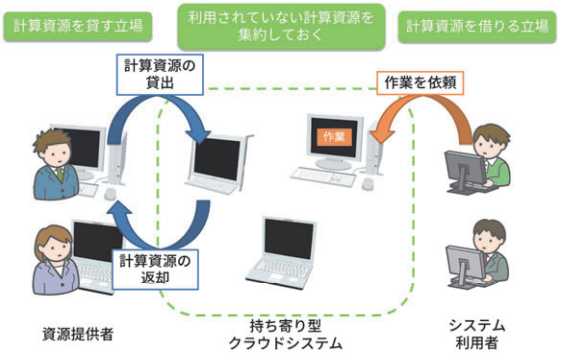

図4　非永続型プロセスのための持ち寄り型クラウドシステム

6　DHCPとDNSパケットを用いたネットワーク接続機器の分別手法の提案

大学や企業などの組織内において安定したネットワークを提供するため、設置した機器の運用管理は重要です。しかし、利用者が持ち込み、ネットワークに接続するデバイスは多種多様であり、それらが起因となるトラブルには、機種やOSの特定から始めなければならず、対応に苦慮する場合があります。

そこで、デバイスを自由にネットワークに接続できる環境で、動作するOSや機器名を分別する手法を提案します［3］。分別の解析対象として、多くのデバイスで使用されていて組織のネットワーク内で完結しているDHCPとDNSパケットを使用しました。これらは暗号化されていませんが、通信の秘密に抵触しないため、デバイス所有者のプライバシーを侵害することなく解析が可能です。分別手法としては、デバイスの出すDHCPとDNSパケットをパッシブに観測し、OSを識別するための情報を抽出しクラスタリングを行いました。その結果、DHCPでは、DHCP Parameter Request Listの各要素の有無を特徴とすることでOSや機器名レベルでの分析ができました（表1）。また、ネットワーク接続開始時に創出するDNSクエリはデバイスの種類ごとに似た特徴が表れることが判明しました。

7　SAMLプロトコルを用いたユーザ属性動的更新機能の実装

複数のアプリケーションサーバを連携して構築したWebサービスにおいて、認証連携を行う標準規格としてSAMLが広く用いられています。SAMLによる認証サーバは、認証結果として各サービスに合わせたユーザ属性をアプリケーションサーバに提供することができま

表 1　DHCP の Discover と Request パケットを用いた機器の分別結果

クラスタ番号	OS または機器名	デバイス数
0	CentOS7	2
	MR04LN	1
	NintendoWiiU	1
	PlayStation3	1
	PlayStationPortable	1
	PlayStationVita	1
	XBOX360	1
1	PXEBOOT	1
2	raspbian8.0	1
3	openSUSE12.3	1
	openSUSE42.1	1
4	Ubuntu12.10	1
	Ubuntu14.04	3
5	Windows7	4
	WindowsVista	1
	Windows10	9
6	Android4.0	1
	Android4.2	1
	Android4.4	2
	Android5.0	1
	Android5.1	1
	Android6.0	9
7	MR04LN	1
	NintendoWiiU	1
	NitendoNew3DS	1
	PlayStationPortable	1
8	iOS7	1
	iOS9.2	2
	iOS9.3	1
	iOS10	4
9	MacOS10.7	1
	MacOS10.9	2
	MacOS10.10	1

す。しかし、一般的な SAML の実装ではユーザ属性情報の受取は認証を行ったタイミングに限られるため、ユーザ属性の変化を随時反映するサービスの提供ができません。そこで、本研究ではユーザ属性の動的更新を前提とした SAML による認証基盤の提案を行いました。

実装した提案システムでは、ユーザ属性情報の更新（図 5- ①）に伴い認証サーバがアプリケーションサーバに更新フラグを通知する機能（図 5- ②）を実現しました。本機能により、ユーザが Web サービスをブラウザで更新（図 5- ③）する際に、アプリケーションサーバが最新の属性情報を取得（図 5- ④、⑤）し、Web サービスに反映（図 5- ⑥）することが可能になりました。また、アプリケーションサーバは認証サーバに対して、変更がある場合に限りユーザ属性の問い合わせと取得が発生するため、動的更新による認証サーバへの負荷を最小限に抑えることができました。

8　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 1 と研究室 3 を共

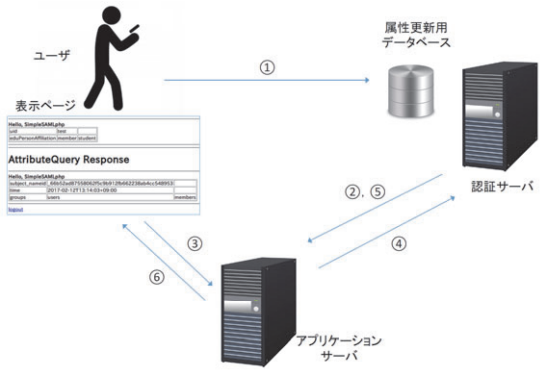

図 5　ユーザ属性の動的更新を前提とした SAML による認証基盤

同で利用しています。現在（2017 年 9 月）、研究室 1 に 8 脚（DSM 5、ET 3）、研究室 3 に 11 脚（DSM 8、ET 3）の机が配置されていますが、2018 年度以降の大学院生の増加に対応できないことが予想されます。そのため、机や椅子等の什器の再選定や、機材等の移設先として物置の増設や倉庫として使用している 107 室の整理を検討中です。

9　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（http://www.dsm.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] 石橋由子，桝田秀夫：ネットニュースシステムを利用した耐障害性の高い電子メールサービスの提案：情報処理学会論文誌，Vol.53 No3，pp.976-988（2016）

[2] 長坂真志，桝田秀夫，森真幸：インアクティブ IP アドレスと OpenFlow ベースのセッション分別を用いたハニーポットの提案：情報処理学会研究報告，Vol.2016-IOT-34，No.4，pp.1-6（2016）

[3] 福田直也，桝田秀夫，森真幸：ブロードキャストパケットを用いたネットワーク接続機器の分別手法の提案：情報処理学会研究報告，Vol.2016-IOT-32，No.33，pp.1-6（2016）