巻頭言

情報セキュリティインシデントにご用心

伊藤　和人
情報メディア基盤センター長

PC ウィルス感染、web ページ改ざん、アカウント乗っ取り、不正アクセス、情報漏洩といった情報セキュリティインシデントが急増している。インシデントの原因は、Windows などの基本ソフトウェア（OS）やサーバ用アプリケーションソフトウェア、WordPress などの web ページ用コンテンツ管理システム（CMS）に内在する脆弱性を攻撃されたものが多いが、設定ミス、平易なパスワード使用を含む管理ミス、個人情報などの重要情報を記録した PC や USB メモリの紛失・盗難、メール添付されたウィルスや詐欺メール（フィッシングメール）への対応ミスといった人為的な原因も大きな割合を占めている。

かつて情報セキュリティインシデントは、ウィルスプログラム作成能力の誇示や、愉快犯的なものが多く、実害はほとんどなかった。しかし、最近は目標を定め、具体的な目的をもった攻撃に変わってきている。例えば、ランサムウェアに感染させてファイルを利用不可にし、元に戻すために金銭（身代金）を要求する。あるいは、大学を攻撃目標に定めて研究データを盗み取ろうとしたり、大学の PC からメールアドレスを盗み、更に関係者の攻撃に利用しようとする。特に、メールを利用した攻撃は巧妙化しており、平成 28 年には大学関係者に文部科学省を騙るメール（標的型攻撃メール）が送付され、添付されていたウィルスに感染する事例もあった。

このように情報セキュリティに関して大学を取り巻く脅威は増しており、その対策が喫緊の課題になっている。埼玉大学では、平成 28 年度から始まる 3 か年の情報セキュリティ対策基本計画を策定し、情報セキュリティ強化に計画的に取り組むこととしている。情報セキュリティ対策の方針は、情報セキュリティポリシー及び関連規程等の整備、利用者の情報セキュリティ意識の向上、情報機器の適正な管理の徹底となっている。情報セキュリティに関して、e ラーニング、点検、訓練など様々な取り組みが計画に従って順次実施されるので、ご理解とご協力をぜひお願いしたい。

情報セキュリティインシデントを防ぐため各人が日頃からすべき対策がある。まず、OS やその他ソフトウェアのセキュリティ更新（アップデート）は速やかに適用すること。セキュリティ更新情報の公開は、同時に脆弱性情報の公開であり、更新を適用するより先にその脆弱性を突く攻撃を受ける可能性がある。更新は速やかな適用をお願いしたい。次に、適切なパスワードを使用すること。インターネットで「パスワードランキング」を検索すると、危険なパスワードがいくつか例示される。そこに載っているようなパスワードを使用している場合は、直ちに変更すること。同様に「安全なパスワード」を検索すると、安全で覚えやすいパスワードの作り方が分かる。パスワードを安易に他者に教えない、ということも大

切である。メールに関しては、添付ファイルを開く際に十分に注意すること。アイコンなどで Word ファイルや PDF ファイルのように見えるファイルであっても、開くとウィルスに感染してしまうケースが多い。また、メールが一杯になったのでシステムにログインせよ、といった詐欺メールに注意すること。言われるままにパスワードを入力してしまうとアカウントが乗っ取られ、不正メール送信に悪用されることがある。まずはメールの本文や送信者が不自然でないか確認し、異常な場合は添付ファイルを開いたりリンク先を開いたりせずにメールを削除する。不審な場合はセンターに問い合わせて頂きたい。最後に、重要な情報は暗号化し、バックアップをとること。漏洩しては困る情報は持ち歩かない、ネットワーク接続された PC に入れない、に限るが、どうしてもという場合は、仮に紛失や盗難、侵入にあっても内容が読み取られないように暗号化やパスワードをかけること。また、ランサムウェアによる被害や誤消去といった事態に備えて必要な情報のバックアップを作成し、かつバックアップを適正に管理して頂きたい。

センターでは、不正通信の遮断やウィルスの検出など技術的な情報セキュリティ対策を図っているが完璧にはいかない。インシデントを他人事と思わず、常にインシデントを起こしうると認識し、各自が前述の対策を実施することがインシデント防止に重要かつ効果的と考えている。

VoIP 通信におけるパケットロスを補う技術

島村　徹也

1. はじめに

現代のインターネット電話にはVoice over Internet Protocol(VoIP)が広く用いられている。インターネット電話は、従来の電話サービスに比べて安価であり、同時に手軽さを実現しているため、Skypeを筆頭に我々の生活に急速に普及している。

インターネット電話では、通話におけるリアルタイム性を保持するためにトランスポート層においてUser Datagram Protocol(UDP)を用いている。そのため、リアルタイム性を損なわない快適な通話が実現されているが、同時にパケットロス問題が必ず発生してしまう。パケットロスはインターネット上の多大な混雑が原因であるため、通信環境を整えることである程度この問題を解決できる。しかし、どれほど環境を整備しても、通信量が爆発的に増加してしまいパケットロスが発生する状況は、例えば災害時や都心でのイベント時など、人々が密集して同時にインターネット電話サービスを利用すれば免れない。また、通信環境を整備すること自体に莫大なコストがかかるため、現実的な解決策であるとは言えない。そこで、仮にパケットロスが発生しても通話に耐えうる品質を保持するための、音声パケットロス隠蔽手法が必要となる。

現在までに、様々なパケットロス隠蔽手法が提案されている。それらは、受信機のみで処理を行う受信機依存の手法と、送信機と受信機の2か所で処理を行う送受信機依存の手法の2つに大別できる。受信機依存の手法でよく知られているのは、ロス部分のサンプルにランダムなホワイトノイズを挿入する手法である。これは、人間の聴覚特性上、背後で流れている雑音が急に途絶えると不自然に聞こえてしまうことを考慮した手法である。しかし、ノイズが挿入される部分には音声情報が付加されないため、パケットロス隠蔽精度は悪い。次によく知られているのが、ロス部分の直前のパケットをコピーしロス部分に挿入する手法である。ランダムなホワイトノイズを挿入する場合に比べて、ある程度音声情報が含まれたものをコピーするため、隠蔽精度は比較的高い。しかし、この手法は音声の位相を全く考慮しないため、改善の余地がかなり残る。受信機依存の手法に対して送受信機依存の手法は、送信機側でパケットロス隠蔽に必要な情報を付加し、受信機側でパケットロスが起こった際にこれを補助情報として利用することで、より精度の高いパケットロス隠蔽を行うものが多い。付加する補助情報は、基本周波数の微妙なズレ等の受信機側のみで考慮できない情報である。そのため、パケットロス隠蔽精度に限って言えば、送受信機依存の手法は概ね受信機依存の手法に比べて良い結果を示す。しかし、インターネット電話がVoIPを用いた通話の手段であることを考慮すると、補助情報の付加によるパケットサイズの肥大化や、それに伴う遅延時間の増加は無視できない要素である。パケットサイズが大きく

ならないように、補助情報をステガノグラフィとして音声波形に埋め込む手法も提案されているが、やはり補助情報の抽出や埋め込みにかかる時間は短縮不可能である。

本稿では，受信機のみで処理を行う受信機依存の手法に着目する。そして、パケットロス隠蔽の従来法である線形予測法を改良し、予測誤差を考慮した発展型の線形予測法を検討する。

2. 線形予測法の利用

線形予測法は、ロス付近の正常に受信できたパケットを用いて話者の声道特性を計算し、算出された線形予測係数を用いてロス部分の本来の音声波形を推定する手法である。この手法では、過去のサンプル値から

$$\hat{x}(n) = -\sum_{i=1}^{p} a(i)x(n-i) \qquad (1)$$

のモデルを利用して次のサンプル値を推定する。ここで、$a(i)$は線形予測係数である。また、pは線形予測の次数、nは時間変数を表す。式(1)の処理は、1 パケットに含まれるサンプル数の回数だけ実行され、1 パケット分が推定される。

本手法は、ロス部分とそうでない部分との境界線で波形の不連続による音声の歪みが発生しないという利点がある。しかし、同時にパケットロスの長さが長くなるにつれて図 1 に示すように振幅が減衰してしまう問題が発生してしまう。この場合、推定されたサンプルに対して線形に変化するゲインを与えることで減衰をある程度抑えることは可能であるが、人間の耳に違和感を与えない音声波形を推定することは困難である。

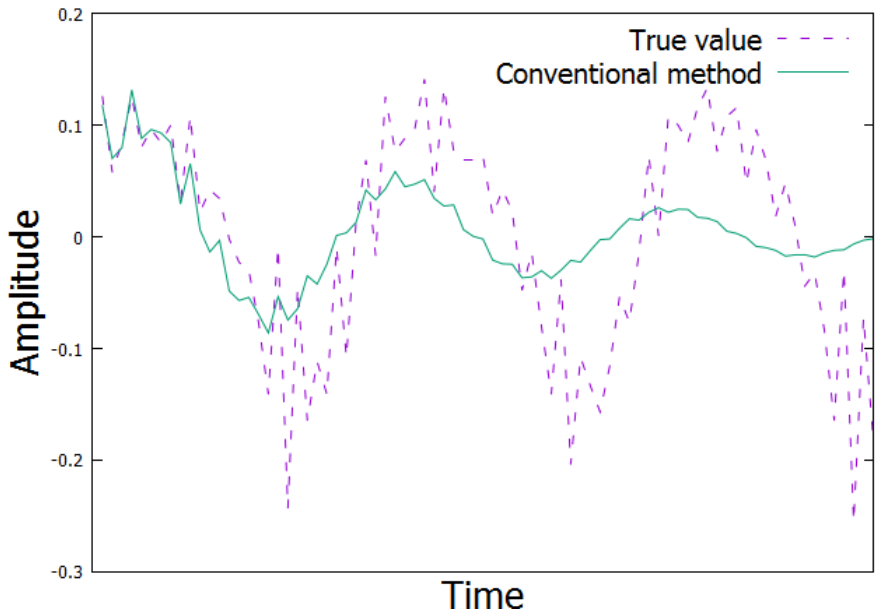


図 1　線形予測法により推定される音声波形と本来の音声波形

そこで本稿では、予測誤差を考慮した、より精度の高い線形予測法を提案する。まず、ロス部分の直前パケットの予測誤差を算出する。予測誤差は

$$e(n) = x(n) - \hat{x}(n) \tag{2}$$

で与えられる。

次に、ロス部分の予測誤差を推定する。予測誤差信号は音声信号と同じく周期性が仮定出来るため、自己相関関数による周期の算出を行う。自己相関関数では、信号の周期に対応してピーク値が現れる。ここでは、ラグ0から最初のピーク値までの値をその信号の周期(ここではMとしておく)を利用することにする。

次に、その算出された周期で予測誤差信号を切り出した後、

$$e(n) = e(n - M), \qquad n = 0,1, \dots, N - 1 \tag{3}$$

としてロス部分を埋めることで、ロス部分の予測誤差を推定する。ここで、Nはパケットロス長である。

最後に式(1)を改良し、

$$\hat{x}(n) = -\sum_{i=1}^{p} a(i)x(n - i) + e(n) \tag{4}$$

として、予測誤差信号を加味し、ロス部分の本来の音声信号を推定する。

本法では、図 2 に示すように、従来の線形予測法と同様に音声波形の歪みを抑えつつ、線形予測法の欠点である減衰を抑えることが可能である。

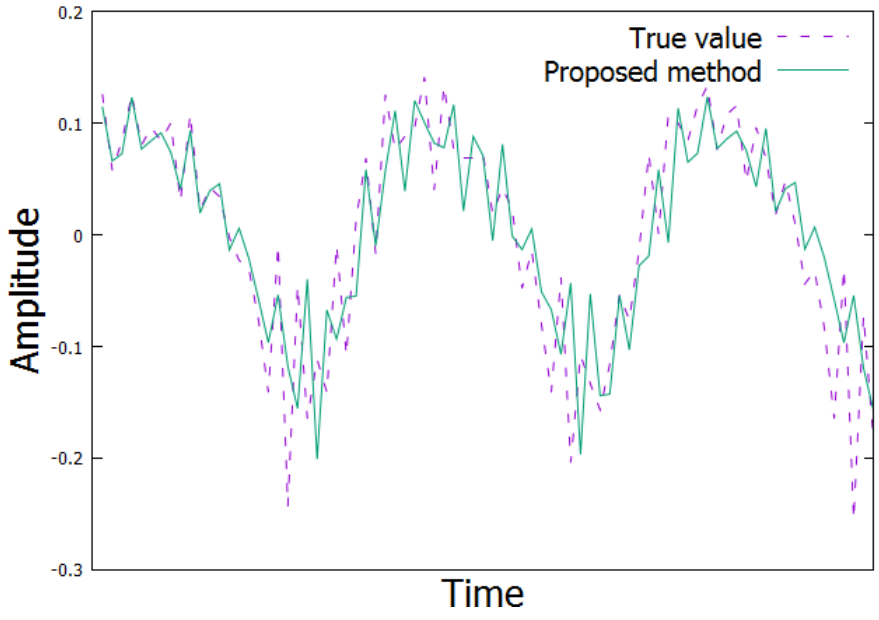


図 2　提案法により推定される音声波形と本来の音声波形

3. 実験

評価実験には男性の音声と女性の音声をそれぞれ用いた。発話内容は約45秒の日本語文章である。実験に関する各パラメータは、国際電気通信連合により定められたG.711規格にならって、サンプリング周波数8kHz、パケット長10msとした。また、パケットロス率は、10%と30%とした。比較対象は、パケットロス後に何も処理をしないもの(damaged)、線形予測法(LPC)、提案法(proposed)、ピッチ波形複製法(PWR)の４つである。線形予測法では、1から1.8へと線形に変化するゲインを与えている。評価実験の客観的指標としては、PESQを用いた。PESQは、音声を4.5から-0.5の範囲で評価する指標である。PESQの値が高ければ高いほど、優れた音声品質であることを意味する。

実験結果を図3に示す。話者の性別やロス率によらず、提案法が最も優れていることがみてとれる。

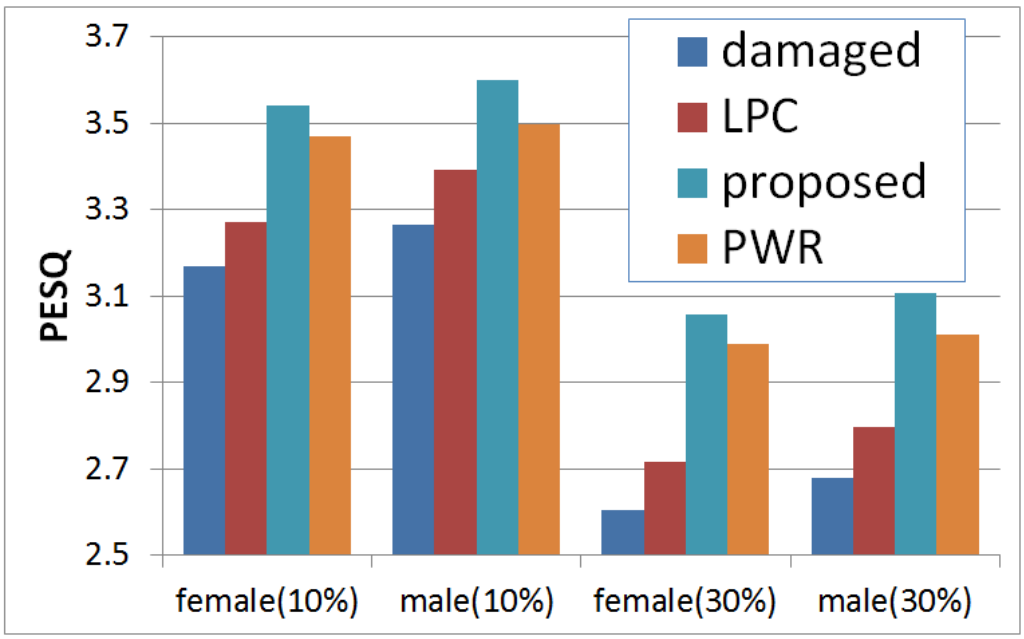


図３　比較実験結果

提案法は、声道特性を表す線形予測係数の予測誤差が発生しないように音声の推定を行っている。そのため、声道特性の推定精度に依存しないパケットロスの隠蔽が行えていると考えられる。このことを裏付けるために従来の線形予測法と提案法で、声道特性の算出方法をユール・ウォーカー法と、比較的推定精度が良いとされるバーグ法に分けて比較実験を行った。その結果を図４に示す。線形予測法ではバーグ法でより良い結果となったが、提案法では優劣をつけることができない。このことから、提案法では声道特性の推定精度の差を予測誤差で吸収した精度の高いパケットロスの隠蔽が行えていることがわかる。

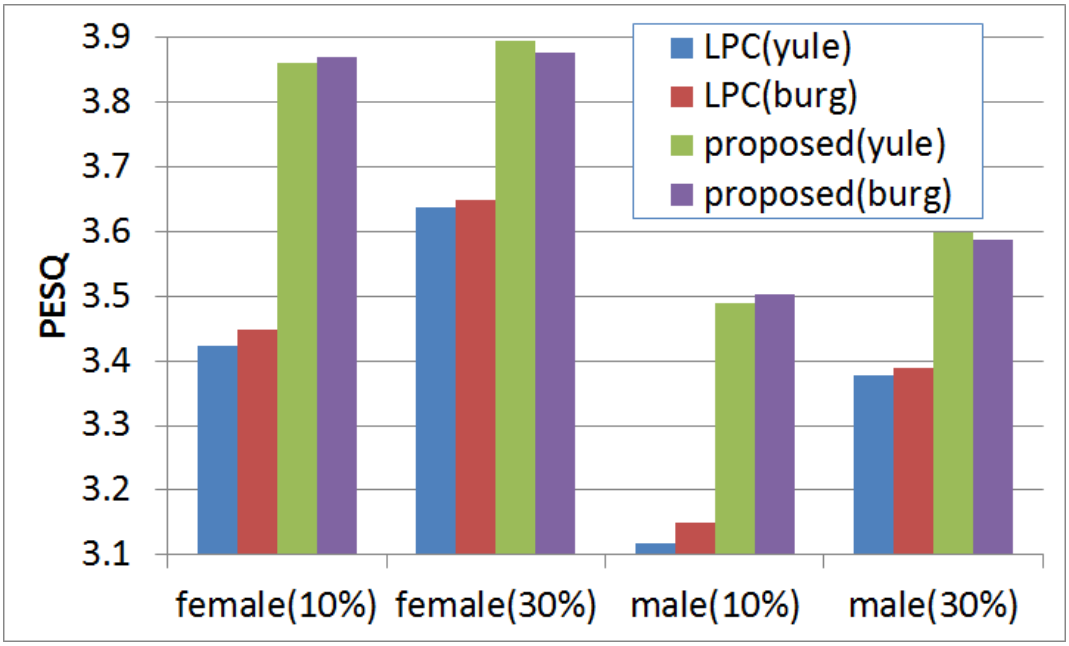


図 4　線形予測アルゴリズムの選択の影響

4. おわりに

本稿では、パケットロス隠蔽のための線形予測法の改良法を提案した。従来の線形予測法を単独に利用する場合に比べ、格段に精度が向上する。また、線形予測アルゴリズムに必ずしも複雑な計算を要する優れたアルゴリズムを利用する必要はなく、予測誤差の利用が、線形予測係数の推定精度の劣化を吸収してくれる。

エピタキシャル TiN/AlN/TiN 接合の作製

～成膜条件の最適化～

田井野　徹

1. はじめに

フォトン検出器は X 線検査や CT スキャンなどの医学や X 線天文衛星などの天文学、地中の成分を調べるための成分分析計や非破壊検査などの材料分析等の様々な分野で用いられ、その多くに半導体検出器が使用されている。しかし、半導体検出器は材料固有の性質により、現在以上の性能向上は困難である。そこで、次世代のフォトン検出器として 2 つの超伝導体電極の間に薄い絶縁体を有したサンドイッチ構造の超伝導トンネル接合（Superconducting Tunnel Junction：STJ）が期待されている。STJ の特徴は、半導体検出器に比べ、1~2 桁程度の高い分解能、X 線からサブミリ波領域まで観測可能な広帯域性、1 秒間に数万フォトンを計測可能な高計数率を有している点である。

現在までに STJ に関する様々な研究が行われており、多結晶膜の電極材料と比較して、エピタキシャル膜の電極を有する STJ は 1 桁程度高いエネルギー分解能が得られるという報告がある[1]。また、NbN/AlN/NbN 接合や Al/MgO/Al 接合において、格子定数が異なるにも関わらず 3 層全てがエピタキシャル成長することも報告されている[2], [3]。そこで、本研究ではエピタキシャル膜の STJ に注目し、超伝導電極材料として TiN、トンネルバリアに AlN を用いたエピタキシャル TiN/AlN/TiN 接合の作製を最終目標として、各材料の成膜条件の最適化について報告する。

2. 超伝導電極材料 TiN について

STJ の超伝導電極に用いられる材料の物性値を表 1 に示す。同表より、TiN は液体ヘリウム温度（4.2 K）以上で超伝導転移すること、また、単結晶 MgO 基板との格子整合性が良く、エピタキシャル成長が可能なこと[4]、さらに NbN に比べてフォトン検出器としての理論分解能が高いことなどの特徴が挙げられる。

表 1 各材料の物性値

	基板	超伝導電極				トンネルバリア
材料	MgO	TiN	NbN	Ta	Al	AlN
結晶系	立方晶	立方晶	立方晶	立方晶	立方晶	六方晶
格子定数 [nm]	0.421	0.424	0.439	0.287	0.404	a = 3.11 c = 4.98
超伝導転移温度 T_C [K]	-	0.5 ~ 5.0	16.5	4.4	1.2	-
エネルギーギャップ 2Δ [meV]	-	0.15 ~ 1.52	5.02	1.33	0.36	-
理論分解能[5] @ 5.9 keV [eV]	-	2.6 ~ 8.1	14.7	7.6	3.8	-

3. STJ の動作原理

図 1 と図 2 に STJ の断面図と電流 - 電圧特性を示す。図 1 に示す STJ にフォトンが入射されると、超伝導体内で結合していた電子対（クーパー対）がかい離し、準粒子が生成される。この準粒子が絶縁体であるトンネルバリアを通過することによって、図 2 のサブギャップ領域の電流が増加し、その差分を検出信号として読み取ることで入射したエネルギーを計測する。

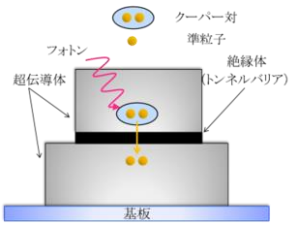


図 1　STJ の断面図

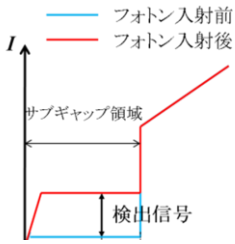


図 2　STJ の電流-電圧特性

4. TiN/AlN/TiN 接合作成条件の最適化

4.1 超伝導電極 TiN の成膜条件

TiN は窒素とチタンの組成により、超伝導転移温度 T_C が 0.5 K ~ 5.0 K まで変化する。そのため、成膜時の電力、ガス圧、窒素流量比を適切な値にすることで、液体ヘリウム温度以上（4.2 K）の超伝導転移温度を目指した。図 3 は N_2 流量比に対する TiN 格子定数と T_C の関係である。電力を dc 150 W、ガス圧を 0.1 Pa、N_2 流量比を 16.6 %とすることで、T_C が約 5.0 K の TiN 膜を得ることが出来た。

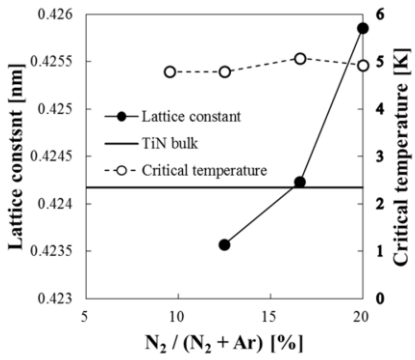


図 3　N_2 流量比に対する TiN 格子定数と超伝導転移温度

4.2 トンネルバリア AlN の成膜条件

トンネルバリアである AlN は厚さ数 nm のため、堆積速度が遅いほど膜厚の制御がしやすい。そこで、N_2 雰囲気中でガス圧を 0.5 Pa とし、放電用の電源と電力を変化させた時の AlN 堆積速度を求めた。図 4 に示す実験結果より、堆積速度とプラズマの安定性から rf 150

W を成膜条件とした。この成膜条件で Si 基板上に 250 nm の AlN を成膜し、XRD 測定を行ったところ、AlN が成膜されていることを確認できた（図 5）。

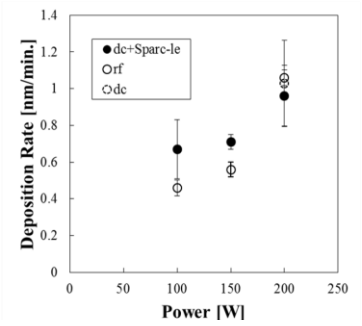


図 4　AlN 堆積速度

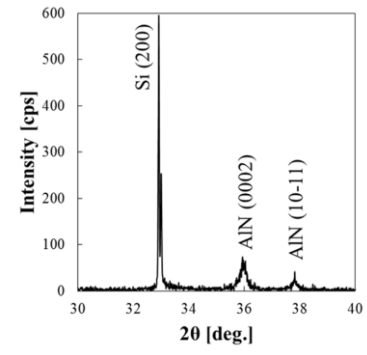


図 5　AlN の XRD 測定結果

4.3 TiN/AlN/TiN 接合の結晶性

TiN/AlN/TiN 接合の結晶性を確認するため、これまでに求めた TiN、AlN の成膜条件を用い、表 2 に示す膜厚で 3 層を堆積し、XRD 測定にて 3 層膜の最上部に位置する上部電極の配向性を確認した。図 6 の結果より、TiN (100) 配向は、AlN トンネルバリアの膜厚 1.0 nm の時には確認できたが、1.5 nm の時には確認できなかった。従って、AlN トンネルバリア膜厚が 1.0 nm ~ 1.5 nm の間で TiN (100) 配向から変化していることがわかる。

表 2　各層の膜厚

各層	膜厚 [nm]
TiN 上部電極	110
AlN トンネルバリア	1.0, 1.5, 2.0
TiN 下部電極	10
MgO 基板	

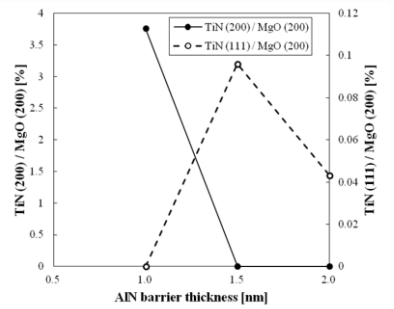


図 6　AlN トンネルバリアの膜厚に対する TiN(200)/MgO(200)と TiN(111) / MgO(200)の回折強度比

5. まとめ

本研究では、0.3 K でフォトン検出動作可能なエピタキシャル TiN/AlN/TiN 接合の作製を最終的な目標として、各材料の成膜条件の最適化を行った。まず TiN の成膜条件では、

電力を dc 150 W、ガス圧を 0.1 Pa、窒素流量比を 16.6 %とすることで、超伝導転移温度が約 5.0K の TiN 膜を得ることが出来た。また、TiN/AlN/TiN の 3 層のエピタキシャル成長を確認したところ、AlN トンネルバリアの膜厚が 1.0nm ~ 1.5nm の間で TiN 上部電極が単結晶から変化することがわかり、各材料における最適条件を見出すことに成功した。

今後、それらの成膜条件によって STJ を作製し、作製した STJ の電気的な評価やフォトン検出器としての評価を行う予定である。

参考文献

[1] P. Verhoeve et al., “Soft X-Ray Performance of Superconducting Tunnel Junction Arrays”, IEEE Trans. Appl. Supercond., vol. 9, No. 2, June 1999.

[2] Z.Wang et al., “Epitaxial growth and crystal structures of NbN/AlN/NbN trilayers fabricated at ambient substrate temperature”, Physica C 282-287, pp. 2465-2466, 1997.

[3] 濱尾 俊幸, “MBE 法によるエピタキシャル成長薄膜を用いた STJ の作製”, 埼玉大学大学院博士前期課程学位論文, 2013.

[4] A. Kawakami et al., “Fabrication of Epitaxial NbN Devices With TiN Resistors”, IEEE Trans. Appl. Supercond., vol. 15, No.2, 2005.

マウスの動きを利用した匿名による通信におけるユーザの可能性

吉浦　紀晃

1. はじめに

今では、ほとんどの人間がインターネット通信を日常的に利用している。インターネットでは、通信を行っている人の IP アドレスはわかるため、匿名での通信を行うためには工夫が必要となる。匿名での通信を行う理由は様々であるが、一つは内部告発を行うため、匿名での通信を必要とする場合である。ある意味で、正当な理由であり、真偽が不明な情報が瞬く間に広がってしまう最近のインターネットの事情から考えると当然とも言える理由である。一方で、匿名による通信を行う不当な理由がある。例えば、違法な薬物、偽造パスポートなどの違法性の高い物品の購入、爆発予告などの犯罪の書き込みを行う等の違法性の高い行為を行う場合、匿名による通信が必要となる。つまり、犯罪に匿名の通信が利用される。実際のところ、匿名による通信で利用される多くは、違法性の高い行為に利用されている。よって、匿名による通信のユーザ特定や識別が重要となってくる。

インターネットにおいて通信元を秘匿化する技術を匿名通信システムと呼ばれている。代表的な匿名通信システムとして Tor(The Onion Router)が挙げられる。Tor では、人々が国による検閲を逃れるためや、軍の機密情報を通信するためなどに使われるべきだとしている。そして情報社会が進む昨今、益々のユーザ数の増加が予想される。だが、その匿名性を悪用するユーザが新たな問題を生んでいる。それは児童ポルノサイトの利用や警察への犯罪予告などである。日本では代表的な事件として、パソコン遠隔操作ウイルス事件がある。Tor を用いた匿名化を破るのは難しく、世界的な問題になっている。

本研究では犯罪を目的に Tor を悪用するユーザを特定し、犯罪を抑止するための足掛かりとしてユーザの識別に関する研究が行われている。既存手法では Tor の匿名通信を構成する一部を占拠することによって匿名通信のユーザを識別する可能性があることがわかった。しかし、本研究では、Tor の一部を占拠せずとも Web サイト管理者が匿名通信のユーザを識別することを目指す。そのために、Tor 利用下でも Web サイト上で取得可能なマウスカーソルの動きから、ユーザの識別方法の構築を目指す。

この識別方法の構築のためには、ユーザごとのマウスカーソルの動きを取得し、他ユーザとの動きの違いがユーザを識別するための特徴量を見つけ出すことが必要である。また、実際、マウスカーソルの動きによりユーザを識別可能であるかを調べる必要もある。つまり、そもそも、マウスカーソルの動きによりユーザ識別が可能であるかを検討する必要もある。

2. ユーザ識別方法

本研究では、ユーザの識別にマウスの動きを利用するが、その動きを Fingerprint として利用する。Fingerprint とは英語で「指紋」の意味である。その意味から通信の世界では、電子メールの内容やデジタル証明書などが改ざんされていないことを証明するデータ、 ハッシュ値のことを指す。ここでは、Fingerprint は Web サイトにアクセスしたときに Web サイト管理者が取得できるユーザごとの特徴量のことを指す。これらの特徴量はユーザごとに異なることが多く、複数の特徴量を組み合わせた場合、ユーザの識別が可能ではないかと期待できる。また、本研究では Fingerprint を取得することを Fingerprinting と呼ぶ。

ここでは、マウスの動きを Fingerprint として用いるが、それ以外にもユーザを識別するための Fingerprint がある。例えば、ユーザの PC 等で利用している、インストール済みプラグイン、ブラウザバージョン、タイムゾーン、ブラウザ表示言語、ディスプレイの表示色、ディスプレイの解像度などの情報が Fingerprint として考えられる。次に問題になるのは、これらの情報をどのように取得する方法である。考えられる方法としては、Java や JavaScript の利用である。しかし、Tor 利用下では Flash、Java などがデフォルトの設定で無効になっているため、デフォルトの設定で有効になっている JavaScript から Fingerprint を取得するしかない。

しかし、JavaScript においても Tor では通信元の特定を防ぐために、いくつかの Fingerprint を取得できないようになっている。そこで、表 1 に非匿名ブラウザと Tor 利用下での JavaScript における Fingerprint の取得可不可の違いを示す。表 1 において 「インストール済みプラグイン」とは Flash や PDFviewer のようなブラウザにインストールされているソフトウェアのことを指す。また「ディスプレイ解像度」における△とは、Tor を利用したブラウザを最大化したときのみ取得可能である。表 1 のように、取得可能なものと不可能なものがあり、Tor 利用下で JavaScript から入手できる Fingerprint は限られている。そのため JavaScript から有用な Fingerprint を新たに取得することはユーザ識別のために重要である。

JavaScript を用いて、Tor ブラウザ上で入手できる特徴量にマウスカーソルの位置座標がある。したがって、短い時間間隔でマウスカーソルの位置座標を取得し続けることによりマウスカーソルの動きを取得することが可能である。本研究ではこのマウスカーソルの位置座標データを Fingerprint としてユーザの識別に用いる。Mouse Fingerprint は Web サイト上でのユーザのマウスの動きを特徴量としたものである。

表 1: JavaScript から取得できる Fingerprint

Fingerprint	非匿名ブラウザ	Tor 利用下
インストール済みプラグイン	○	×
ブラウザバージョン	○	×
タイムゾーン	○	×
ブラウザ表示言語	○	○
ディプレイの表示色	○	○
ディプレイの解像度	○	△

3. 識別手法

Mouse Fingerprinting により取得した特徴量をユーザごとに比較し検証する必要がある。そのためにサポートベクターマシンを用いる。サポートベクターマシンは、教師あり学習を用いる分類方法の一つであり、パターン認識や回帰分析に利用できる。サポートベクターマシンの学習アルゴリズムは最適化理論から導出されており、訓練データとして与えられた正事例と負事例からそれらを分離する分類境界の計算を行う。このとき、マージン最大化といった工夫を加える事により高い汎化能力を発揮できる。本研究では、Tor 利用下のユーザが Web サイトに訪れときのマウスカーソルの動きを取得する。そのため学習に用いる 1 ユーザのデータは多く取得することができない。また、マウスカーソルの動きは、ユーザごとに一定ではなく、毎回ある程度のブレが出ると予想できる。したがって、他のアルゴリズムと比べても学習データをそれほど多く必要とせず、学習データのノイズにも強いサポートベクターマシンは本実験に適している。

通常の サポートベクターマシンでは学習データを分類する際、線形で分類を行う。しかし学習データのクラス分布に重なりがある場合、つまり線形分離できない場合、非線形サポートベクターマシンでなければ誤分類が起こらないよう分類することは不可能である。本研究ではマウスカーソルの動きを分類することから、それぞれ違うラベルの付いたデータの重なりは免れないため、非線形サポートベクターマシンを用いる。しかし学習データは複雑かつ過密な重なりが予想されるため、誤分類が起こらないよう分類した場合、汎化能力が極端に落ちる。汎化能力とは、未知のデータに対し正確に分類できているかどうかという性能である。そのため分類境界を設定したとき誤分類をある程度許容し、汎化能力を失わないアルゴリズムが求められる。そこでソフトマージン SVM を用いる。ソフトマージンサポートベクターマシンでは誤分類を許容するが、誤分類にペナルティを与えることによって、汎化能力を失わずに複雑なデータの分類を行う。

Mouse Fingerprint からユーザを識別するため、以下の要件で実験を行う。

1. マウスカーソルの動きを取得するためのサイトを作成する。その際、取得するマウスカーソルの動きはユーザごとに違いを判別し易いよう、一定の動きをユーザに行わせる。データはユーザの操作ののち、サーバに自動的に保存されるものとする。
2. データは[x 座標,y 座標,ラベル]を持つ。x 座標、y 座標はマウスカーソルの位置を記録したものである。ラベルはユーザごとの違いを示すものである。
3. 分類にはソフトマージンサポートベクターマシンを用いる。2 ユーザの学習データを入力することで、識別境界線を描くものである。
4. 2 ユーザの識別境界線を描いたところにテストデータ(ユーザがどちらのものなのか学習させていないデータ) をプロットし、正しいユーザの識別境界線側に分類されているかどうかの分類評価を行う。

実験に用いる、Mouse Fingerprint を取得するサイトを図 1 に示す。ユーザは、図 1 にある①~④までのボタンをクリックし、そのマウスカーソルの位置を 0.01 秒ごとに Mouse Fingerprint として取得する。取得した実験用データは以下のような形式である。3 列目の 10、11 というのがラベルでありそれぞれのユーザに対し任意の数字を割り当てている。

4. 実験

実験には 6 人に協力してもらい 7 種類の学習データを得た。それぞれユーザ A ~G とする。学習データにはユーザごとに 3 回分のマウスカーソルの動きを用いる。学習データはそれぞれ赤点、青点で示され、テストデータ(ユーザがどちらのものなのか学習させていないデータ)は黄色で示す。学習データから識別境界線を引いた後、描画した識別境界線に対し、それぞれ 2 ユーザのテストデータ(各 2 データ)を黄点で描画する。黄点がそれぞれ赤点、青点側の正しい識別境界線内に入っているのかどうかを割合で評価したものを識別正答率とする。実験は 7 種類の学習データを用いるため、識別境界線の描画は全部で 21 通りある。描画結果から、いくつかポックアップしたものを以下に示す。図 2 は A と B のユーザそれぞれの識別境界線描画結果と 2 ユーザそれぞれのテストデータプロット結果を示している。

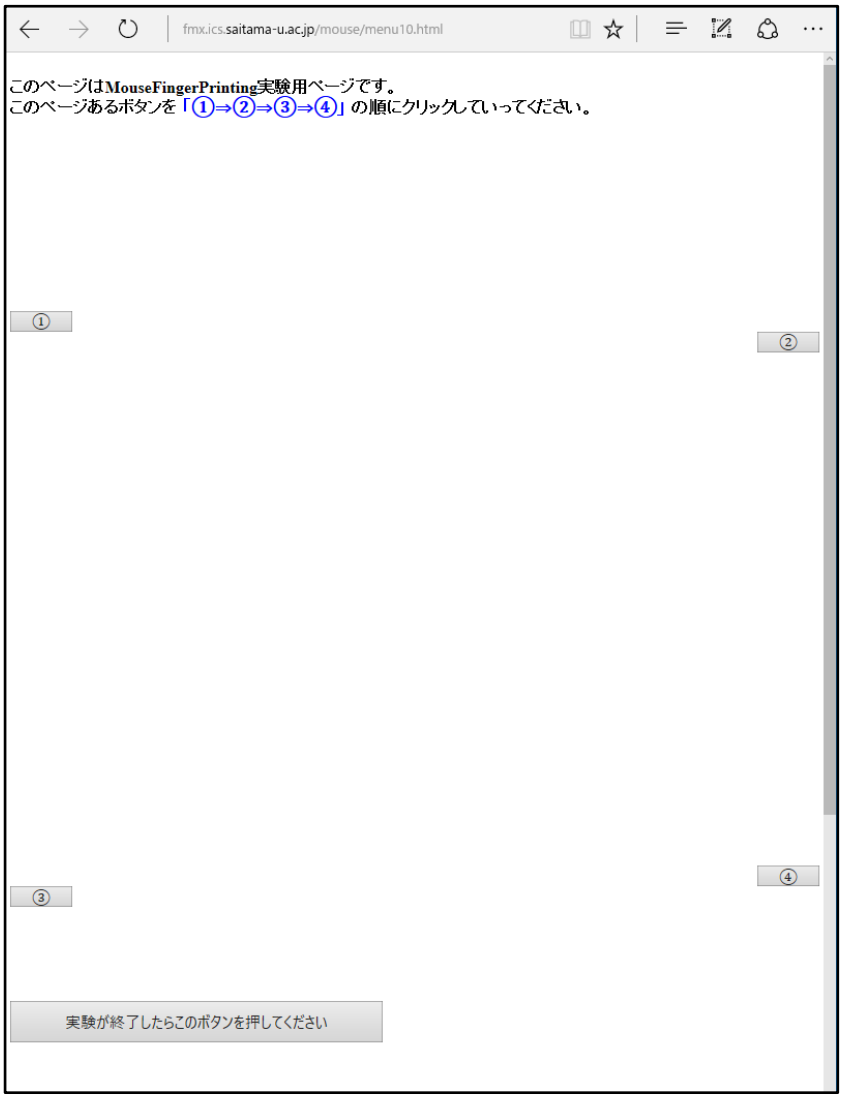


図１:実験で利用したサイト

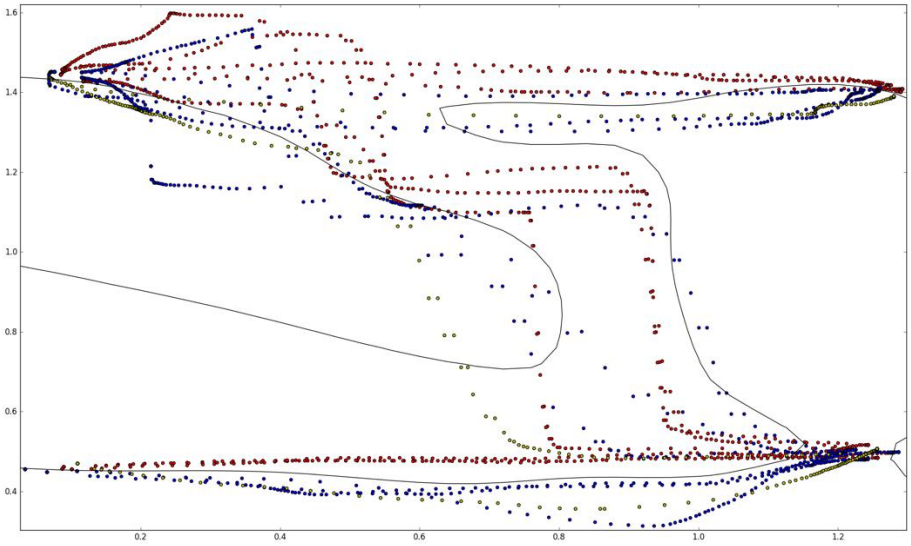


図2: A(赤点):B(青点):Aテストデータ(黄点)

以上の出力結果から、テストデータはそれぞれ正しい識別境界線内に分類できているのかどうか、赤点側と青点側それぞれを未知のデータとして評価したときに正しい分類境界線内に分類されているのかどうか識別正答率を算出した。識別正答率はテストデータの 1 点 1 点が正しい識別境界線の内側にある割合を示している。表 3 において「A:B における左側テストデータ」とは、A のユーザと B のユーザの識別境界線を描画して A のテストデータを入力したとき、正しい識別境界線内にどのくらいテストデータがプロットされたか、ということを示す。

表 4 より、A:B の分類においては双方ともに未知のデータを精度良く分類できている。しかし、 C:E においては図 3 より、分類境界線が赤点、青点をともに赤点 側に含まれるように引かれてしまいあまり良い分類精度ではない。分類正答率にテストデータの違いにより差が出てしまっている。つまり図 3 から分かるように、それぞれの学習データが密集しているところにおいて、どちらかのラベル一つに分類されてしまっているということである。D:F は赤点テストデータ、青点テストデータともに 60%弱の分類正答率を出しており、A:B には及ばないもの未知のユーザを識別できる。A:B との分類正答率の違いは学習データの質の違いによるものであると考えられる。A:B は図 2、ユーザのマウスカーソルの動きがゆっくりであったため、ボタンからボタンへの軌跡を密に取得することができている。しかし D:F においては図 4 より学習データがボタンの位置付近に密集しており、ボタンから ボタンへの軌跡を取得することができていない。これは一定時間ごとにマウスカーソルの位置を取得するため、素早いマウスカーソルの動きに対してあまり学習データを取得す

ることができず、実験サイトのボタン付近に学習データが集まってしまうことも要因である。

しかし、2 ユーザにおける分類おいては一方のユーザの非分類正答率(100%-分類正答率)がもう一方のラベルの分類正答率を上回っていないことから、ユーザの識別は可能であると考えられる。ただし、本実験では、2 ユーザであったため、Mouse Fingerprint から分類することが容易であるが、ラベルの数が増えるにしたがってデータが過密になっていくため汎用的な分類は難しくなる。そのため複数のユーザを含んだ大まかな分類にならざるを得ないことが考えられる。

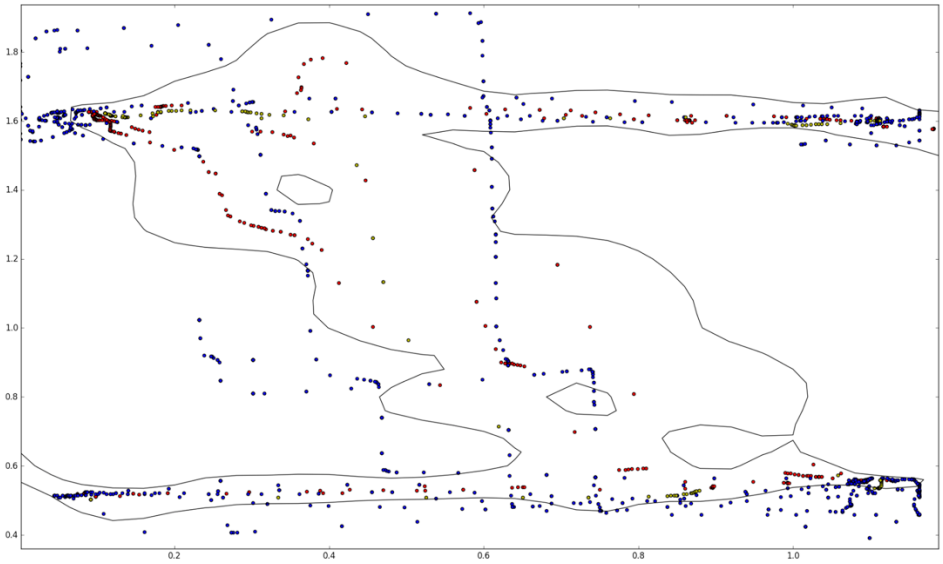


図 3: C(赤点):E(青点):C テストデータ(黄点)

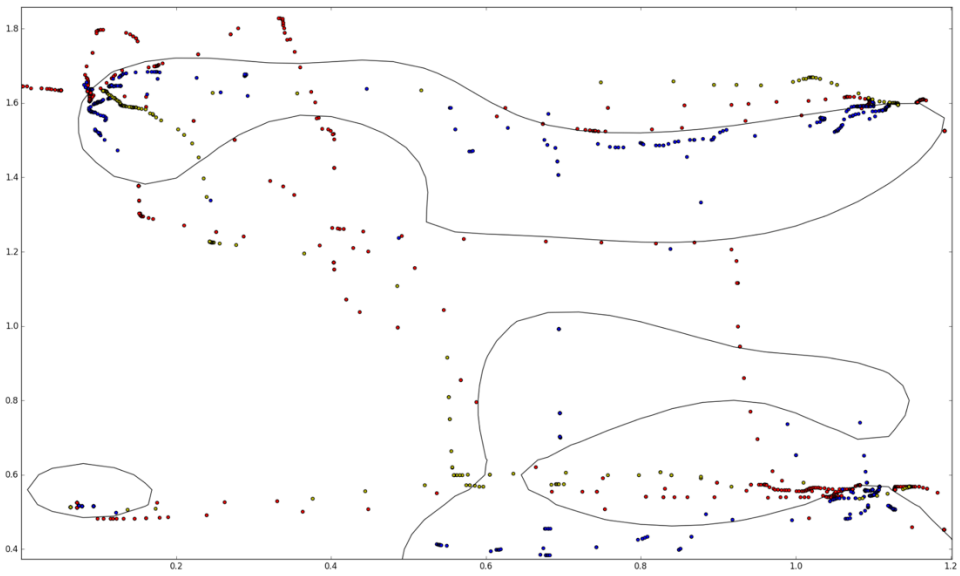


図 4 D(赤点):F(青点):D テストデータ(黄点)

表 2: JavaScript から取得できる Fingerprint

	赤点テストデータ	青点テストデータ
A:B	73.99%	64.47%
A:C	63.91%	97.96%
A:D	77.89%	89.24%
A:E	88.12%	79.41%
A:F	82.11%	93.37%
A:G	83.31%	82.40%
B:C	47.05%	88.39%
B:D	69.41%	89.43%
B:E	72.57%	79.16%
B:F	81.48%	92.55%
B:G	76.54%	92.53%
C:D	40.73%	53.03%
C:E	74.34%	46.69%
C:F	65.38%	41.41%
C:G	91.65%	32.93%
D:E	60.08%	56.49%
D:F	66.34%	40.58%
D:G	45.79%	62.20%
E:F	49.54%	79.30%
E:G	43.01%	65.68%
F:G	59.21%	68.47%

5. まとめ

マウスカーソルの動きは Tor 利用下のユーザ識別のための Fingerprint の一つである。しかし、識別するユーザが多くなればなるほど識別が難しくなる。また、Mouse Fingerprint だけではユーザの識別はまだ難しい。実際に Tor 利用下のユーザを識別しようとした場合、より多くの学習データ種類と特徴量をサポートベクターマシン等で判別しなければならない。本研究では 2 ユーザに対し、マウスカーソルの動きのみで検証したため Mouse Fingerprint の有用性の検証に留まった。しかし、ユーザ特定のためには他の Fingerprint と組み合わせることが重要である。本研究ではソフトマージンサポートベクターマシンを用いて分類境界線を判定したが、他のアルゴリズムの可能性も検討しなければならない。

またマウスカーソルの動きの学習データによる分類境界線では位置的な分類しかできず、より正確な識別をするためにはユーザごとの特徴的な動きを学習することが必要である。マウスカーソルの動きを取得するための実験用サイトを作成したが、ユーザ識別のための最適なマウスカーソルの動きであったとは言い難い。よりユーザの識別に適したサイト作りを検証する必要がある。

展開図は何種類？

堀山　貴史[1]

1. 展開図のメカニズム

展開図というと、小学校の算数の時間に、立方体や直方体の箱を切り開いたのを思い出される方が多いと思います。展開図は、単に頭の体操というだけでなく、私達の身の回りの様々な場面に現れます。

ケーキやお菓子の箱は、その一例です。たとえば、森永製菓(株)のチョコボールの箱は、「くちばし」の部分を開けたり閉じたり動かせるのですが、箱を切り開いてみると、1枚の紙をうまく折り畳んでできているのが分かります。最近は、さらに複雑なシカケがされた箱もあり、箱も中身も楽しめます。

もう少し視野を広げて、モノを折り曲げたり、逆に切り開いたりといった「折り」と「展開」のメカニズムに着目してみましょう。たとえば携帯電話などの箱は、ボール紙を器用に折ることで、付属品も含めてピッタリ入る形に作ってあります。板金加工で機械部品を作るのも、展開図から立体に折る作業といえます。

また、宇宙に目を向けると、人工衛星の太陽電池パネルがあります。打ち上げ時にはミウラ折りと呼ばれる折り方で小さく折り畳まれているのですが、宇宙に行ってから端と端を引っ張ると、引っかかりなく縦横にパネルが開きます。車のエアバッグは、普段は折り畳まれているのですが、イザという時に膨らんで私達の身を守ってくれます。

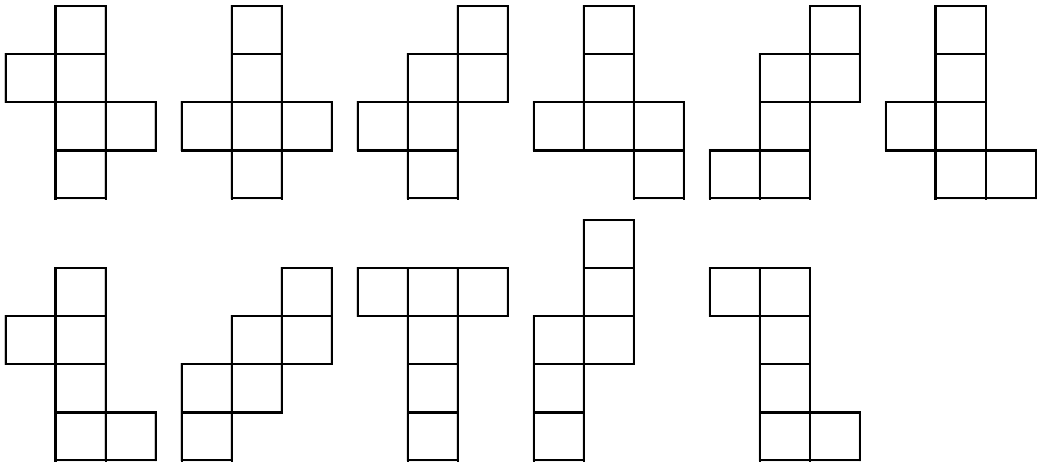
2. 展開図の列挙

さて、展開図に話を戻します。立方体の展開図は、全部で何種類あるでしょうか？答を見る前に、紙面から目を離して、思いつく展開図をすべて挙げてみてください。
挙げられましたか？クルッと回して同じ形になるものや、裏表をひっくり返すと同じ形になるものがあれば、重複していますので、そういうものは省いてください。11種類の展開図が得られていれば、成功です=図。

ここで気になるのは、この図に挙げたもの以外に立方体の展開図は無いのかという点です。できるだけ頑張ったら11種類だったから、これで全部、という理屈だと、将来もっと頑張ったら12種類目が見つかるかもしれませんね。

この疑問に答えるには、系統的な方法が必要です。どのように辺を切ると、展開図が得られるのでしょうか。1つ目の条件は、すべての頂点が切る辺を必ず持つことです。そうでない頂点があると、その頂点はとんがったままで、平面に開けませんから。また、切る

[1] 埼玉新聞 2017 年 7 月 19 日掲載, サイ・テクこらむ



辺をたどって輪ができると2つのパーツに分かれますので、そんな輪を含まないことが2つ目の条件です。3つ目の条件は、全部の切る辺がどこかでお互いにつながっていることです。

これら3つの条件すべてを満たすものを、「全域木」と呼びます。つまり、全域木になるような切る辺の選び方を、漏れなく重複なくすべて列挙することで、展開図のカタログが得られます。

3. 展開図の個数

少し前に、研究室の学生さんと一緒に、展開図を1つ1つ列挙することなく、でも展開図が何種類あるかだけを数えるアルゴリズムを作りました。手品みたいな印象を受けますが、「ポリアの定理」と呼ばれる定理を応用することで、どんな多面体が与えられても、展開図が何種類あるかを数え上げることができます。

たとえば、5角形と6角形の面を持つサッカーボールに適用すると、312京7432兆2209億3947万3920種類の展開図を持つと分かります。また、切頂二十・十二面体と呼ばれる多面体には、181澗5771溝8919穣7376秭459垓2899京4520兆2399億4216万4480種類の展開図があると分かります。普段は使わない数の単位が出てきて楽しいですね。

大学の情報系センターに必要と思うこと

小川 康一

1. はじめに

大学の情報系センターは、周囲を取り巻く様々な環境の変化により厳しい立場にある。最近では、サイバー攻撃による情報漏えいなどの事案が多発しており、セキュリティ対策が急務となっている。業務量が減るばかりか、情報系センターに求められる要請や多種多様なサービス導入の要望は年々増加傾向にある。しかし、現状は予算や人的リソースが限られている。本稿では，このような厳しい環境下において、埼玉大学での独自の取り組みを紹介するとともに、今後の大学情報系センターのあり方について述べる。

2. 埼玉大学における全学情報基盤システムの運用

埼玉大学（以下、本学）は、首都圏にある国立大学である。5 つの学部（教育学部・教養学部・経済学部・工学部・理学部）が 1 つのキャンパスの敷地内にある。大学の構成員は、学部生 7,020 名、大学院生 1,111 名、教職員 773 名（2016 年 5 月 1 日現在）である。

本学の情報基盤システムは、学内ネットワークを構成する「基幹ネットワーク」、メールや Web、 DNS、認証機能などを提供する「基幹サーバ」、パソコンを利用した演習を行うための「教育研究用システム」の 3 つで構成される。我々は、この情報基盤システムのことを「全学情報基盤システム」（Saitama university Education and Research Network，以下 SERN）と呼んでいる。本学では、情報メディア基盤センター（以下、センター）が SERN の調達および管理運用を行っている。2015 年現在、センターの組織はセンター長 1 名、専任教員 2 名、併任教員 1 名、専任の運用スタッフ 2 名、併任の運用スタッフ 1 名、派遣職員 1 名、非常勤の事務職員 3 名で構成されている。

本学では学内ネットワークを構成するネットワーク機器の老朽化に伴い、2007 年から大学全体のネットワークを刷新する必要があった。新たな取り組みとして検討を進めた構想は、大学構内の各部屋とネットワーク機器を設置するサーバ室とを光ファイバにより直接結ぶことであった。本学では、この取り組みを各家庭に光ファイバを敷設する“Fiber To The Home” (FTTH)になぞらえて、“Fiber To The Laboratory”（以下、FTTL）と呼んでいる。

FTTL を導入した狙いは、大学の情報基盤システムの運用スタッフが不足していることにある。本学をはじめ多くの国公立大学では、運用スタッフである情報系センターの職員が不足している状況にある。少数の職員で管理を行うためには、障害が発生しにくいシステムの導入が必要となる。障害が起きた場合でもトラブルシューティングが容易で、メンテナンスし易いことが重要である。利用者の端末がある部屋とネットワーク機器の途中に複数の機器が存在する場合、ループなどの障害自体が隠蔽され、発生要因が発見しにくくなる。一

方、FTTL で必要となる機器は、光ファイバと LAN ケーブルとを変換するメディアコンバータだけであり、障害点となるネットワーク機器が途中に介在しない。このため障害箇所の特定が容易になっている。

3. 本学の基幹ネットワークの特徴

FTTL は、本学の建物 44 棟にある部屋、約 1800 か所をシングルモード光ファイバで接続する光ファイバ直収ネットワークである。ネットワーク構造は、大学の中心に位置するサーバ室を中心としたスター型構成である。

光ファイバの配線は、ネットワーク機器が置かれたサーバ室と、建物内の光中継盤を経由し、サーバ室と各部屋が光ファイバにより直接結ばれている（図 1）。図中の「MC」はメディアコンバータ、「光」は光ファイバを表す。

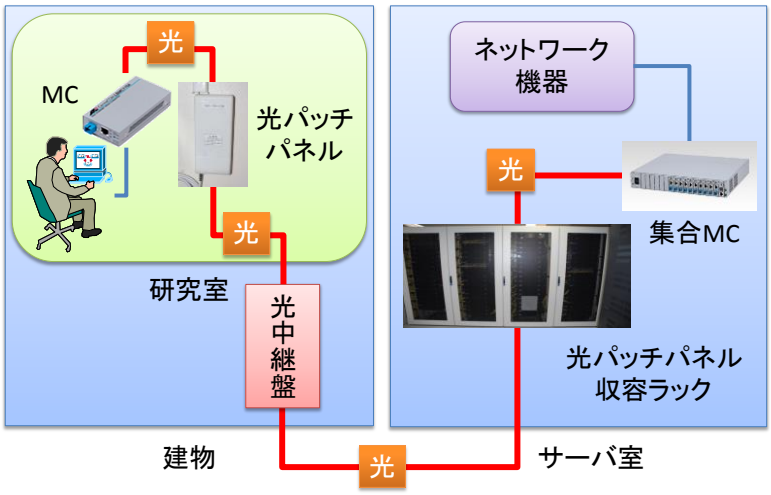


図 1　FTTL の概要

サーバ室は光ファイバ敷設にあわせて、講義室を改装し構築した。サーバ室には、各建物と接続する光ファイバケーブルが集線されている。

図 2　各部屋の光パッチパネル（左）とメディアコンバータ（右）

利用者の各部屋には 2 心の光ファイバ 1 本が敷設されており、光パッチパネル（図 2 左）に収容している。各部屋には、LAN ケーブルをメディア変換するメディアコンバータ(図 2 右)を設置する。メディアコンバータは光パッチパネルと光パッチコードで接続して利用する。メディアコンバータは速度に応じて 10/100M 対応メディアコンバータ、もしくはギガビット対応メディアコンバータを用意している。

サーバ室には、各建物の中継盤に接続された光ファイバの幹線が 4 つの光パッチパネル収容ラックに集線されている。光パッチパネル収容ラックと集合メディアコンバータ間を光ファイバパッチケーブルで接続している。集合メディアコンバータとネットワーク機器とは LAN ケーブルで接続している。

このように、本学のネットワークは光ファイバで部屋とサーバ室とが直接接続されている。FTTL は、集中管理ができるというメリットは大きいが、メディアコンバータを必要とするため、結果的には非常にコストが高いネットワークであるといえる。

4. センター運営上の工夫

4.1 人員体制

人員不足の問題は、人件費になるため予算とも関連する。前章で述べた通り、本学のセンターには 2 人しか主担当者がいないため、人手不足が深刻であった。そこで、2015 年から話し合いを進め、センターに所属していない他の学科の技術職員にセンターの業務を支援してもらう協力体制をとった。開始から約 1 年になるが、窓口の対応や技術面での支援、どうしても複数でやらなければならない作業など、都合をつけて対応していただいている。この活動は副産物として、センターで獲得した知識をもとに所属先で発生したネットワーク障害を解決したり、セキュリティなどの啓蒙活動などを行っていただいたりと、相乗効果が生まれている。

4.2 セキュリティ対策

本学のセキュリティインシデントについては、日々たくさんのインシデントが発生しており、対応に苦慮している。最近多くみられるのは、「偽装メールによる偽サイトへの誘導」である。この事例は、利用者が送られた偽装メール内の URL をクリックし、偽サイトに誘導され、ID とパスワードを搾取されてしまう事案である。このインシデントは非常に多く発生している。

このインシデントは、ただ ID とパスワードが盗まれるだけでなく、悪意を持った者が、盗んだ ID とパスワードを利用して大量のメールを配信する事案に繋がっている。このようにして大量のメールが配信されると、本学の送信メールサーバの処理が追いつかなくなることがあり、大学のメール機能が麻痺する事もある。

本学では ActiveMail を Web メールとして利用しており、こちらを狙った偽装メールが横行している。図 3 は偽装メールの例であるが、利用者が落ち着いて読めば、内容がおかし

いと判断できるが、急いでいる教員はきちんと読まずに焦ってメール本文中の URL をクリックしてしまうようである。

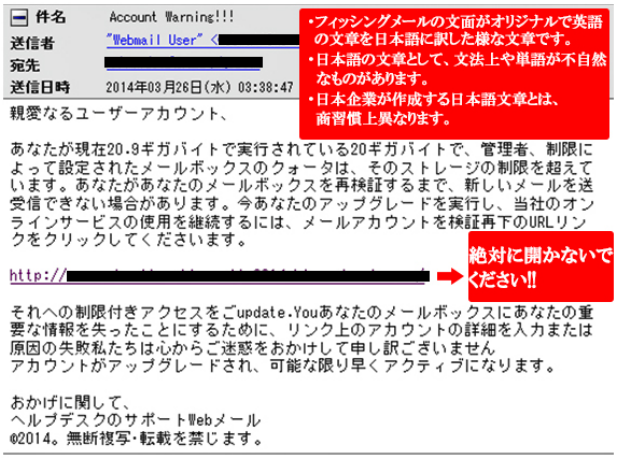


図 3　ActiveMail の偽装メール（出典：クオリティア社ホームページ[1]）

その他のインシデントとして、「外部からの攻撃と対処」がある。これは、学内の端末がウイルスに感染して、外部のサイトを攻撃する事案である。これは主に外部からの通報によって発覚することが多い。

このようなインシデントが日々発生する状況を受け、本学でも遅ればせながらセキュリティ対策実施手順書を今年制定、施行した。この狙いは、インシデント発生時の対応フローと役割の明確化にある。部局連絡担当者と部局総括責任者、センターや CISO との連携を明確化した。

図 4　セキュリティ講習会の様子
（左：一般利用者向け、右：責任者向け）

セキュリティ教育の取り組みとして、定期的にセキュリティ講習会（図 4）を行っている。しかし、講習会の参加者が講習後に前述の ActiveMail の偽装メールに引っかかるという事案が発生し、根気よく開催しなければならないと考えている。学生についてはまだ対応が進

[1] http://www.qualitia.co.jp/phishing/

んでいないが、平成 29 年度から E-Learning での対応を進める予定である。

セキュリティの啓蒙活動としては、大学で教職員が参照するグループウェアがあり、こちらで最新のセキュリティ注意喚起など周知を行っている。しかし、グループウェアに掲示しても見ない教員がいるため、事務職員がメールなどで周知することも期待している。

本年度は新たな試みとして、パソコンの目につく所に貼付する「セキュリティ注意喚起シール」を作成した。図 5 は現在のシールである。本学のマスコットキャラクターである「メリンちゃん」を入れて利用者に親しみやすくし、連絡先を明記して一覧性を図るなどの工夫をしている。実際に効果があるかの検証はこれからである。

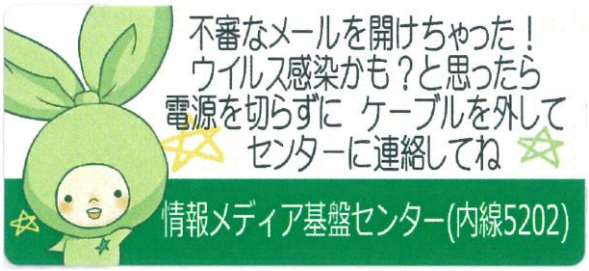


図 5　注意喚起シール

セキュリティの内部監査としてチェックリストによる点検を行っている。現在は外部公開しているサーバを中心にポートスキャンを行い、実際のネットワーク管理者、サーバ管理者にチェックリストを送付し、内容を確認する方法をとっている。回答の内容次第では、詳細な確認をセンターが実施する方法をとっている。

4.3 運用における創意工夫の視点

システム運用技術は、創意工夫を行う余地のある研究分野である。私は、新しい技術や要請への挑戦の一環として、「システム管理運用の研究」に取り組んでいる。これまで情報系センターで経験した様々な知見について、整理し発表することを継続している。

実際、得た知見を発表させていただきながら、その過程で色々な知識が得られている。このような研究的視点が重要であると考えており、学会参加を積極的に行っている。主に情報処理学会のインターネットと運用技術研究会（IOT 研究会）や電子情報通信学会のインターネットアーキテクチャ研究会（IA 研究会）に参加し、論文作成や口頭発表を行っている。研究会に参加される先生方や研究者との情報交換や議論の中で新しい発見があり、モチベーションの維持に役立てている。

5. 今後の情報系センターに必要と思うこと

実務に携わる職員として、私が考える今後の情報系センターに必要と思われる要素を 3 つ挙げてみたい。

1 つ目は、業務をタスク単位で切り出しておくことである。このためには業務の内容を整理する必要があるが、切り出しておくと、たとえば派遣職員の方に定型的な業務をお願する

ことや、外部のサービスを利用するなど、選択肢の幅が広がる。また、切り出したタスクの中で、ある程度妥協できるタスクも出てくる。なんでもかんでも情報系センターでやらなければならないというのではなく、ここは思い切って「なくす」「減らす」ということも考える時期ではないだろうか。

2 つ目は、技術伝承と技術レベルの維持である。これは運用技術の「火」をたやさないということである。組織内部での OJT に限界はあるが、ノウハウを残していくべきだと考えている。

3 つ目は、属人化を減らす努力と工夫である。私は、個人でその人でなければできないという形にならないように複数体制で情報共有を行っている。ちょっとしたことでもメールを構成員全体が参加するメーリングリストに流すようにしている。

前述の通り、情報システムの管理運用にはまだまだ工夫できる余地があると考えており、視野を広げるためにも研究的な視点を持って考えることも重要であると感じている。

6. まとめ

大学の情報系センターには課題が山積しているが、業務の見直しとタスク切り出しによる協業協働体制を築くこと、システム運用の自動化、外部サービスの効果的な活用が必要である。技術要素として Software Defined-Network や IoT デバイス、ロボットなどの活用も視野に含まれてくると考えている。運用技術については創意工夫による効率化はまだできる余地がある。今後少数で運用できる技術革新があるかもしれないが、最終的に大学の内部に少数でもいいので、受け継ぐ人材という資産を残すことが重要である。つまり、各大学や利用者の立場に立って考える人が必要ということである。

7. おわりに

本稿では、本学の情報センターにおける取り組みについて実務サイドからの視点を述べた。今後の情報系センターに対する環境は益々厳しいものになると予想される。最近では、人工知能やセンサー、IoT デバイスなどの技術革新のスピードが目覚しく、そう遠くない未来に情報基盤の運用に携わる技術者もロボットに置き換わる時代が来る可能性が高い。しかし、情報基盤を使うのは「人」であり、そして対応するのは「人」であるべきだと私は考える。コンピュータやロボットなど機械にはできず、人の能力を必要とする局面は必ずある。今、我々は厳しい環境におかれているからこそ、逆に新しいアイデアは必ず生み出せるものと信じている。

[1] 小川康一，吉浦紀晃，“埼玉大学における光ファイバ直収型ネットワークの運用経験について”，情報処理学会研究報告インターネットと運用技術（IOT），2015.

※本論文は CTC アカデミックユーザアソシエーションに寄稿した論文に加筆修正したものです。

電子メールシステムの外部委託におけるセキュリティ関連の調整

齋藤　広宣

1. はじめに

従来、政府機関における情報セキュリティ対策においては『政府機関の情報セキュリティ対策のための統一基準』が存在する（内閣サーバーセキュリティセンター(NISC)のホームページで閲覧することができる）。埼玉大学においてもこの基準に従って情報セキュリティ対策を実行している。この基準の「4.1.1 外部委託」の項には、『民間事業者が約款に基づきインターネット上で無料で提供する情報処理サービス等（中略）「約款による外部サービス」として定義するものを利用し、行政事務を遂行する場合（中略）、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものと』することが定められており[1]、大学の業務用のメールサービスを無料ないし安価な既製サービスを利用して展開することは不可と考えていた。しかし近年、国立大学においても業務用途のメールをクラウド化する事例が増えるなど、状況に変化が見られる。

そこで本学においても、一部の業務用メールサービスを外部の既製サービスを利用して展開するべく調査や学内調整を行い、セキュリティポリシーに反映させた。本稿ではその内容について、備忘録的にまとめることとする。

2. 検討開始時の状況

本学電子メールシステムの外部委託に向けての検討は、平成28年4月ごろから開始した。当時はちょうどマイクロソフトの Office 365 Education の利用を開始した時期であり、Office 365のメール活用にも関心が高まったところでもあった。

ここではその当時の、外部の情勢について記述する。

2.1 『政府機関の情報セキュリティ対策のための統一基準』に関して

平成26年度版の『政府機関の情報セキュリティ対策のための統一基準』（以下、統一基準という）においては、「約款による外部サービス」では要機密情報を取り扱う業務に利用するべきでないとされた[1]。一方この統一基準策定に先立ち、ザ・ソフトウェア・アライアンス(BSA)は、クラウドサービスの普及を加速させるべきとの立場から、『クラウドコンピューティングの利点や特性を考えると、データの自由な移転の確保が非常に重要』などの意見を出している[2]。これに対し、NISCは『機密情報が外国政府等に渡るリスクを政府機関は許容できません』という見解で[3]、日本国の機密情報が外国のコントロール下に置かれるリスクを特に重視していた様子がうかがえる。

それから2年が経過してクラウドサービスの普及がさらに進み、平成28年8月に策定され

る統一基準においては用語として「クラウドサービス」が新たに定義され、「クラウドサービスの利用」の項目が基準に追加されようとしていた。

2.2 クラウドセキュリティ規格の整備と対応製品の登場

クラウドサービスの情報セキュリティ対策の国際基準として、ISO 27018が2014年に、ISO 27017が2015年に策定された。例えば ISO 27018（パブリッククラウドにおける個人情報保護の実施基準）では、データの保管場所を顧客に通達することなどが定められ、従来クラウドサービスを利用していた際の懸念が解消されるようになった。

そしてこれらの認証を取得したサービスが、いくつか登場してきた時期でもあった。殊にマイクロソフトの Office 365 は日本データセンターで提供し日本法に準拠することを公表した[4]ことで、日本国内業者と並ぶ有力な選択肢となった。

3. 情報セキュリティポリシーの改正

埼玉大学の情報セキュリティポリシーは『高等教育機関の情報セキュリティ対策のためのサンプル規程集』を参考にして作成されているが、2015年版サンプル規定集においてはまだ情報システムをクラウド等に外部委託（アウトソース）することに対応した構成になっていない（そのかわりに、アウトソースにあたっては情報の保全や紛争処理等について考慮すべきという解説が記載されている[5]）。そこで電子メールシステムにターゲットを絞って、外部委託ができるよう独自にガイドラインを作成することとした。

3.1 電子メールサービスのアウトソーシングガイドライン

電子メールサービスをアウトソースしようとする者、およびアウトソースした電子メールサービスの運用管理を行うシステム管理者を対象として、サービスの選定、契約、および運用にあたる際のガイドラインを定めた。またガイドラインに即した実際の技術検討例を、資料として学内公開した。

なお電子メールを利用する利用者が、サービスが内製かアウトソースか、またメールサーバの場所や途中経路を考慮しないですむよう、このガイドラインに従うサービスも「大学が整備・提供する電子メール」とみなすことと定めた。一方その分、アウトソースを行う者には、相応のレベルの技術検討や運用設計が求められるともいえる。

3.2 電子メール利用ガイドライン

情報セキュリティポリシーにおいては、要保護情報を「学外」へ保存・移送・提供する場合の取り扱い手順の項目があり、電子メールを使用する場合に「学外」をどう考えるかという問題が生じた。結論として、電子メールの場合に限りロケーションを考慮せず、「大学が整備・提供する電子メール」を用いる場合は「学内」とみなす、というルールに定め、これをガイドラインに明記した。

4. 今後の課題

埼玉大学における情報システムの外部委託に関するルール作りは、電子メールシステムに限ってようやく端緒に達したという段階であり、まだまったく充実しているとはいえない。例えば一つあいまいになっているのが、外部委託（アウトソース）を誰がいつ行っているかという点である。これについては、以下の2通りの考え方があり得る。

1. メールサービスを導入する組織が、外部の電子メールサービスを契約した時。
2. メール利用者が、電子メールサービスを使ってメールを送信した時（都度）。またメールを受信した時（都度）。

これらは明確にどちらと決めることも難しいと思われるが、電子メールサービスを契約する組織と利用する者（組織）が異なる場合は、万一トラブルの発生の際などに微妙な問題を生じうることを指摘しておきたい。

もう一つ言及しておきたいのが、業務監査への対応である。業務に電子メールを使用することで、日常的に一部業務のアウトソースを行っているのであれば、業務監査の際にそのアウトソース先も監査の対象となり得る。ただそれがクラウドサービスの場合、個々の顧客がクラウドサービス業者のもとに監査に押しかけるのは現実的ではない。これには例えばクラウドセキュリティ推進協議会(JASA)が実施する『クラウド情報セキュリティ監査制度』を利用し、当該クラウドサービスの言明書を確認することなどで監査に代えることが提案されている。こういった監査についてもアウトソースの導入時に検討するよう、手順の整備を考えていきたい。

参考文献

[1]政府機関の情報セキュリティ対策のための統一基準（平成26年度版） サイバーセキュリティ戦略本部

[2]「政府機関の情報セキュリティ対策のための統一基準群」（案）に関する意見（2014年2月14日） BSA

[3]「政府機関の情報セキュリティ対策のための統一基準群」平成26年度版(案)に関する意見の募集の結果 内閣官房情報セキュリティセンター

[4]日本マイクロソフトホームページ https://products.office.com/ja-jp/business/japan-datacenter?tab=tabs-2

[5]高等教育機関の情報セキュリティ対策のためのサンプル規程集（2015年版補訂） C2201 解説