ドイツ長期研究滞在のご報告

武藏 泰雄[†]

[†]熊本大学総合情報基盤センター・ネットコミュニケーション研究部

概要: この度2005年1月24日～同年7月31日まで、ドイツ連邦共和国フランクフルト(M)市のヨハン・ヴォルフガング・ゲーテ・フランクフルト大学へ長期出張致しましたので、ドイツで行った研究内容の一部およびドイツ滞在時の出来事をご報告したいと思います。

1. 背景

この度、平成 16 年度大学改革推進等補助金（海外先進教育研究実践支援プログラム）「高度情報化キャンパスの課題」に採択され、平成 17 年 1 月 24 日より同年 7 月 31 日まで、ドイツ連邦共和国フランクフルト(M)市のヨハン・ヴォルフガング・ゲーテ・フランクフルト大学（通称フランクフルト大学）へ長期研究出張致しました。

高度情報キャンパスを築くためには、遠隔教育システムを実現することはもはや必須事項であり、そのシステムのセキュリティを守る技術の確立は恐らく世界的に急務であると考えられます。今回の海外先進教育研究実践支援プログラムにより、現在、特許申請中の情報セキュリティ技術に基づいた遠隔教育サーバシステムのセキュリティをウィルスやクラッカー等の攻撃から防御するシステムの開発・実装に関する研究を行い、本学の高度情報キャンパスの構築に関連させていくことを目的としておりまして、現在もこの研究テーマを継続中です。

コンピュータセキュリティあるいはネットワークセキュリティ研究分野において、最近ボットネットワークが注目されていますが[1-5]。ボットネットワークとは「ボット」呼ばれるウィルスのワーム感染によって乗っ取られた PC によって構成される、一種の分散クラスタ型ネットワークの総称です。ボットネットワーク構成するボットは一般の通常 PC である場合が多いと言われています。ボットネットワークのボットとは、「ロボット」の「ボット」であり、操り人形のことを指します。つまりウィルスのワーム活動で次に犠牲になる PC（犠牲端末または犠牲 PC と言う）をネットワーク上で探索し、管理が甘い点（ システムの欠陥）を攻撃して、PC 内部に侵入させ、そして乗っ取りが成功したらコントローラ（人形師）にインターネットリレー（IRC）等を介して通知し、次の指示を待つ状態になります。コントローラは、ボットと化した犠牲 PC を分散システムとして連結（クラスタリング）してボットネットワーク単位で操作できるようにします[1-3]。

図 1. フランクフルト大学経済情報学部の建物

ボット化した PC から発見されたウィルスを解析することにより、ボットには様々なセキュリティ上問題がある機能が搭載されていることが知られるようになりました。(1) サービス妨害(DoS)攻撃用の基地（踏台とも言う）としての機能、(2) ボットウィルス自身の更新や他の様々なウィルスを拡散する機能、 (3) 機密情報や個人情報の盗聴・漏洩（スパイ的活動）、及び(4)迷惑メールの発信・中継等の機能です[1-3]。

今回の研究をドイツで始めることになったきっかけにまず(1) の機能があります。一般にウィルス等の悪意を持ったプログラムが次の犠牲 PC に自己を複製して、感染を拡大する活動をワーム活動と呼びます。ワーム活動は、メール介する大量メール送信型ワーム（MMW）及び Windows などの LAN を介したネットワークサービスの欠陥（脆弱性）を突く、サービス攻撃型ワーム（SAW）の 2 種類に大別されます。後者の SAW では、平成 15 年 8 月に W32/MSBlaster.A と W32/Welchia.A が、また翌年の平成 16 年 5 月には W32/Sasser.D がリリースされました。この W32/Sasser.D の犯人が間もなくドイツ警察によって逮捕されました。この犯人の正体がドイツの当時 17 歳の少年であったことは衝撃でしたが、ワームの作者を突き止めたドイツ警察の捜査技術も相当なものだと感心させられました。また受け入れ先のフランクフルト大学経済情報学部のラネンベルグ教授は、「階層セキュリティ構造論」を発表された方で、その技術理論の応用は携帯電話や公衆無線 LAN アクセス等多岐に渡っています。この新しい階層セキュリティ構造論についてラネンベルグ教授にご指導いただこうと思ったのがドイツ選択二つ目の理由です。

図 2. マイン河南側から見たフランクフルト市内中心地

図 3. 中央駅前広場

現在よく知られている情報セキュリティ技術は「善」と「悪」、または「外部」と「内部」と二極化させた簡単なモデルです。例えばファイアーウォールがその良い例です。確かに以前は、ファイアーウォールで問題のある IP アドレスやサイトからのアクセスを遮断（フィルタリング）することでかなり内部のセキュリティは守ることできました。しかしながら、最近では、短期間に新種ウィルスをリリースしてウィルス駆除ソフトのパターンデータの開発が間に合わせないような状態を作りだす技術の発展（ゼロデイ型攻撃と言う）、また持ち込み PC によるウィルス・ワームの感染拡大や P2P ベースな情報漏洩型ウィルス等の出現、それに多機能化したボットネットワークの出現によって、現在外部と内部と言う単純な二極モデルは通用しなくなっています。なんらかの新しいセキュリティ理論が必要とされますが、その一つに階層セキュリティ構造論があると言われています。これについては後述します。

次に(2)のサービス妨害（DoS）攻撃について説明します。DoS 攻撃は、簡単に言いますと、Web サーバ等に多量のアクセス仕掛けて、サーバの機能を麻痺させる攻撃手法です。DoS 攻撃には様々な攻撃手法があり、それを防ぐ事前的（プロアクティブ）対策、あるいは不正侵入検知システム（IDS）を導入し、ファイアーウォールと連携させる事後対処的（アクティブ）な対策法はあるのはあるのですが、開発段階である場合や、ゼロデイ対策はまだ未開発である等解決事項が多くあり、更なる技術開発の発展が期待されているところです。特にプロアクティブな対策法の発展が期待されます。

我々の研究室では、ベイズ理論や統計理論等の様々な手法を使って近未来の事件を予測する手法を確立しようと努力していますが、攻撃の動機を調査した方が良いではないかと思うようになりました。近い将来の大規模な DoS 攻撃では、その攻撃の前に小さな事件が起こると考えます。その小さな事件とは、具体的に言えば、掲示板上の言動（フレーミング）、宗教や宗派間それに民族間の対立等によるものです。ドイツでは戦後多くの移民を受け入れており、大小の人種や宗教間の対立や衝突が恐らく相当数あったのではと考えられ、また多くの対応策が開発されたと考えられます。ラネンベルグ教授の提案された「階層セキュリティ構造論」はこの様なドイツ国内事情に基づいて開発されたと考えられたことがドイツ研究渡航を選択したもう一つ理由となります。

2. ドイツでの生活

背景では、ドイツ渡航理由を書きましたが、この節ではドイツでの生活について書かせていただきます。

2.1 フランクフルト市到着

平成 17 年 1 月 24 日（現地時間）フランクフルト国際空港に 16:10 に到着しました。入国審査後、すぐに携帯でラネンベルグ教授に電話したところ、まず秘書の方が電話に出られ、すぐ教授室つないでいただきました。教授より、「良く来たね。明日の午前 10:10 に教授室に訪ねる様に」おっしゃっていただいた時は、流石に安心しました。到着時は、夕方の様な状況で、ホテル（InterCity Hotel, 有無線 LAN）に着いたころは、もう外は真っ暗でした。約 12 時間の航空機搭乗と日本時間では既に翌日になっておりましたので、その日は流石に眠くてたまらなかったので、ホテルにつくなり中央駅でラップと言う野菜と挽肉のクレープで包んだようなものを買って来て、それを食たべ後シャワーとかぶり（ドイツ

図 4. 最初のゲストハウス(上から寝室、風呂、風呂のヒータ、トイレ)

図 5. 筆者の冷蔵庫の中です。

特有の立ったままで浴びるシャワーです）、そしてすぐベッドにもぐりこみました。

さて翌日ホテルから地下鉄（U4）でフランクフルト大学のボッケンハイマー・ヴァルテ・キャンパスに移動し、ラネンベルグ研究室へ到着しました。早速、客員研究員として来たことの目的や今後の研究計画について打ち合わせを行いました。その後研究室の方々と名刺交換する等、挨拶廻りを行い、キャンパス内や周辺の学内施設や食堂、スーパー等を案内していただきました。その後これからしばらくお世話になる、秘書のコッホさんに客員研究員用の部屋（ガストハウス）に案内していただき、管理人のホッペさんを紹介させていただきました。大学内では私の下手な英語が多少なりとも通じたのですが、この管理人さんはドイツ語しか話せませんから、いきなりドイツ語でコミュニケーション開始となりました。実際ドイツ人のドイツ語がなんとか耳に入って判るようになって来たのは五ヶ月ぐらいたってからでしたから、なんとかその時理解できたのは、Aufräumen（整理整頓、片付けをする、掃除する等）だけでした。そして沢山の鍵を渡されたのでした（大抵のドイツ人は鍵を沢山に持っています）。

2.1 ドイツでの水・食事・風呂・冷暖房

私がドイツに到着した時期は真冬であり、とにかく、「寒い」の一言につきます。雪は日本の北部の様に沢山積もる分けではありませんが、それでもところによって道路や歩道が凍結しているため、慎重に歩かないといけません。最低気温は普通に氷点下ですが、私が到着した時はしらばく暖冬だったそうです。ドイツの家や研究室などの室内では、冬に限っては、トイレ等を含めて人が至る所に、セントラルヒーティング（Zentralheizung）の暖房装置が設けてあり、快適でした。ただ一度だけですが、客員研

図 6. ヴォッヒェン市の果物売場の様子

究室の研究棟のボイラーが故障したらしく、故障後数分もしないうちに、とても寒い思いしたことがありました。流石にこの日は午後 3 時には全員帰宅しました。

ドイツでの食事は、主として朝と夜はスーパーで購入した食材を元にサンドイッチをこしらえて、自宅で食べ、昼はメンザ（学食）でドイツの一般的な料理を食べていました。このメンザでドイツ人の先生や学生がどういう風に食べるかといいますと、先生方は、やはりナイフとフォークでなんでも食べます。学生達も、主にナイフとフォークで食べますが、面倒になったらフォークだけで食べています。学食なのですが、意外と静かに食べるあたりが、日本の学食と違うところです。ただ、誰かが雰囲気騒がしく変えると急にみんな騒がしくなるようです。

私がいたキャンパスと近くの地下鉄（ボッケンハイマーヴァルテ）駅の周辺は、毎週木曜日にヴォッヒェン市があり、その時は市でのオープンカフェで昼飯を取ります。この市では、新鮮食材や衣類等の日用雑貨が多く売られ、また日本で言う屋台や食堂の類がこの日だけ軒を並べます。

同じ様なヴォッヒェン市は、曜日を変えて、各広場や大きな通り（例えばツァイル）で行われており、概ね週末（木金土）のようです。ドイツでは日曜日に開いているお店は中央駅や空港等を除いてほとんどありませんので、週末は皆必死で買い物をします。特にカーニバル、イースター、クリスマス等の休暇も日曜日と同様です。休日が重なる時はどかっと買い入れてそれでなんとか凌ぎます。

我々日本人には、特に熊本の人間にとってはドイツでの飲料水の確保はかなり大変です（笑）。水道水（ライストゥングスヴァッサ）が飲めればいいのですが、ドイツ人ですらスーパー等で大量にペットボトルのミネラルウォータを購入して飲料や料理に使っていますから、通常ミネラルウォータを買ってきます。実際水道水で日本茶等を沸かすと、硬度が高いため白濁して飲める代物ではなくなります。

図. 7 筆者の口に合うミネラルウォータの銘柄

ミネラルウォータで注意しないといけないのは、スパーリング（Mineralwasser mit Kohlensäure:炭酸入り）とスティル（Mineralwasser ohne Kohlensäure: 炭酸無し）の二種類があります。炭酸入りのミネラルウォータは、日本でも最近コンビに等に置かれるようになって来ましたが、ドイツではこの炭酸水が水になります。レストランやカフェ等で、水は出ませんから水くれと言うと、親切なところは「炭酸入りにしますか、それとも」と尋ねてくれるので助かりますが、通常は炭酸入りが出てきます。最初はこの炭酸入り水がどうしても辛くて、いろいろな銘柄を試し、なんとか自分に合うもの（スーパーのプルスブランドのもの）を探し当てるのに一週間かかりました。ところでドイツでは残念ながらコンビニはありません。どうしも日曜日や祝日に購入したい場合は、国際駅やその街の中央駅に行くといくらか営業している店やスーパーがありますが、24 時間体制のやはりお店は見つけられませんでした。

2.2 住民登録と長期滞在ビザ申請等

我々日本人を含めた外国人はドイツに三ヶ月以上滞在する場合は、住民登録と長期滞在ビザが必要ですが、通常はドイツに入国して三ヶ月以内に取得する必要があります。そこでまず、住民登録をしに行きました。住民登録所は、ツァイル通りの東端、ツォー動物園の近くにあり、私の下手くそなドイツ語でなんとか申請書をもらい、研究室の方々や自宅でなんとか訳して、一週間後になんとか提出しました。

次に公安局の外国人登録局の受付まで行き、外国人登録と長期滞在ビザの申請書をもらい、記入して挑戦したところ見事に玉砕しました。外国人登録課の受付では、実に新切に英語で対応・説明していただけたのですが（まだドイツ語は無理なので英語で行けると思ったのですが、運が悪いとドイツ語のみしか取り扱いできないとか言われるようです）、英

図 8. 大勢の客でごったがえすフライブルグ（B）のカイザー・ヨーゼフ通り

文の申請書はいいが、ドイツ語でないと面接できないから通訳と来いと言われ、私のへたくそドイツ語ではダメと言われました。多少練習して来たのですが、どうも私の前の方も、この方はドイツ系スイス人なのですが、「私はドイツ語で普通に会話ができるのだけどなぁ」とぶつぶつ言いながら帰って行きましたから、相当な人に当たったのかなぁと、すっかり諦めて研究室に向かいました。登録局を出る前に取り敢えず受け付けの方に私の書類を調べてもらったら、多分担当の人は日本円が判らなかったかもしれないから、円で表示されている書類を全部、ユーロに換算したもの変えればいいのではと、助言もらいました。

この一部始終を教授に話すと教授がカンカンなられて、日本円ぐらいで文句を言うのは勉強不足だから一言いわねばならんと言うことで、後大学側の書類にも不備があるので急いで書き直してもらいました。その後書類を、本大学の事務に依頼して送付していただき、また通訳としてコッホ女史が同席していただきまして、2 月 16 日の午前中に 10 分程度で終わりました。外国人登録局の手続き諸経費は合計で 80 €でした。

2.3 フライブルグ(B)市滞在とファッシング

長期滞在の申請をしている間に、ドイツ南西部のフランスやスイスの国境に近いところにフライブルグ・イム・ブライスガゥという都市があります。このフライブルグ市には、アルバート・ルードヴィヒフライブルグ大学（通称フライブルグ大学）と呼ばれる大学があり、そこの情報系の先生であるショーバ教授と情報セキュリティ関連の話題について打ち合わせを行いました。このショーバ教授は、ラネン

図 9. 上から筆者の宿泊したホテル、ファッシングの様子 1、様子 2、及び様子 3

図 10. ファッシングの様子

ベルグ教授の指導教官です。ラネンベルグ教授はフライブルグ大学で博士号を取得され、その後英国マイクロソフト社、T-Mobile 等の移動電話の研究所経て、フランクフルト大学の経済情報学部で現在教授されていることから、フライブルグ大学にも何度か訪問されているようです（非常勤等）。

フライブルグ大学に到着した時（2 月 6 日ドイツ新幹線 ICE73 スイス・バーゼル行き）の旧市街はもの凄い人が集まっており、何やらお祭り騒ぎでした。ちょうどこの時期はカーニバル（ファッシング）だったようで、フランクフルトでも既に大騒ぎでしたが、まずはホテルに向かおうとしたのですが、早速

図 10. フライブルグの近くにある雪山の頂: 上左から筆者、オプハム助手、ライハルト教授、下はティッティ湖（湖面が低温と雪で白く凍っているが、氷は薄いのでスケートは無理のようでした）

お祭りに巻き込まれてしまい、何やらファッシングサポータバッチを 2 €で買わされてしまいした

実際のそのバッチを付けてお祭りで人がごったがえしているところを歩きながら、屋台でソーセージ等を買うと、やたら歓迎してくれるのですが、それが正直嬉しかったです。

さてなんとかホテルに着くと、無線 LAN が使えるとあったので、部屋に入ってノートパソコンの無線 LAN 機能をオンにすると早速インターネットに接続できました。このフライブルグへの出張の後、いろいろところへ出張しましたが、ほとんどホテルや駅に無線 LAN が完備しており、中でも T-Mobile の公衆無線 LAN 網は大変便利でした。至るところに張り巡らされており、クレジットカードの番号を入れなければならないという不安はあるものの、大抵どこでもインターネットに繋げる環境は、私に様な人種にはとてもありがたいものでした。

図 11. メルセデス・ベンツ自動車博物館

それからファッシング期間中、フライブルグ大学でラネンベルグ教授のセミナーや南アフリカのマンデラ大学のラインハルト教授及びフライブルグ大学のショーバ教授と今後の共同研究の可能性や今後の大学の教育のあり方について打ち合わせや議論を行い、フランクフルトへ戻りました。

2.4 シュツッツガルト市滞在とシュツッツガルト大学

次に自動車産業で有名なシュツッツガルト市に行きました。シュツッツガルト大学のハナカタ教授の計らいで RUS-CERT のスタッフ（ゲーベル氏、フィッシャー氏、）とネットワークセキュリティや情報セキュリティについて情報交換や今後の共同研究について打ち合わせを行いました。RUS とはシュツッツガルト大学計算機センターの略ですが、情報セキュリティの研究を行っている分野では特に CERT が、かなり有名です。一般にドイツの大学の計算または情報処理センターは人員不足が現状ですが、シュツッツガルト大学の場合は、スタッフは優秀な方がいらっしゃるようで、しかも CERT があります。CERT はコンピュータ緊急対処チームの略でこれを置いている大学はドイツでは恐らくシュツッツガルト大学だけのようです。

彼らの研究で興味を引かれたのは、実は似たような事をやっていて、共通の悩みを持っていたことです。例えば、ウィルスやワームの氾濫でネットワークの混乱を経験していること、ウィルスに感染した PC を探し出し、管理者に通報するシステム等を開発していることでした。CERT のスタッフは、主に ngrep 等を使用してネットワーク中のセキュリティインシデントを探しておられ、私の間接的であるがファルスポジティブやネガティブが少ない DNS ベールの検知システムに興味を示していただいたことは大変嬉しかったと記憶しています。

図 12. フランクフルト市内を巡る市電(Straßenbahn)。そのパンタグラフの形が逆三角系であるのが特徴である。似たような物が熊本の市電にも見られる。下は市電車両内部

2.5 大学のクリニーク訪問

実はフランクフルト大学に戻ってから歯痛に悩まされたので、ラネンベルグ教授の紹介でフランクフルト大学の付属病院である、ウニヴェルジテート・クリニークに行きました。外国でよりよって長年大事にして来た歯ですが、ドイツ滞在中に限って発病しまして、相当困り果てそうになりましたが、なんとか治療していただきました。カリエス(虫歯)、インイェクツィオーン（麻酔注射）、トゥートゥヴェー（痛いよぉ）、と思い出すだけでも嫌な単語ですが、連発しておきました。歯科医は、トルコ系ドイツ人で、助手見習いはベトナム人でした。トルコとドイツの関係は良く知っていましたが、ドイツのテレビ番組ではじめて知ったのですが、ドイツとベトナムの関係は、東ドイツと北ベトナムの時代に、対米戦で北ベトナム軍と東ドイツ軍が一緒に戦った歴史があり、その経緯からドイツとベトナムの関係はあまり悪くないようです。

図 13. ベルリンのフンボルト大学。当日はドイツ物理学会の年会とアインシュタイン展が開催されていた。

2.6 ベルリン市のフンボルト大学訪問

ベルリンの旧東ベルリンのウンターデンリンデン通りにあるフンボルト大学でドイツ物理学会の年会があると言うことで、ハイデルベルク大学のヴォルガング・シューラー教授と ICE でベルリン市に向かいました。まず ICE はベルリンツォーロギッシェガ

図 14. 森鴎外記念館

ルテン（動物園）駅に着きます。そして S バーンで宿泊先のホテルに向かいました。翌日東ベルリンの

図 15. ベルリンの TV 塔と世界時計。TV 塔展望室からの市内の一部

図 16. TV からの眺望

アレキサンダー広場からテレビ塔に登り、ベルリン市内を見学した後、ベルリン大聖堂や先の大戦の記念碑を眺め、ウンターデンリンデン通りを進んで行くとフンボルト大が見えてきます。

フンボルト大を見学し、シューラー教授と打ち合わせをした後、すぐに森鴎外記念館に向かいました。開館時間が 14:00 だったため、わずかの間でしたが、森鴎外記念館を訪ねて思った事は、ベルリンが当時いかに活気に溢れ、先進的な大都市であった事を伝えていること、また森鴎外先生の生活の様子が垣間

見えたことです。この記念館は、フンボルト大学の日本文化研究の資料館としての性格もあり、日本学（ヤパノロギー）の発祥の地的場所でもあります。ですから、多くの日本語の資料や現代日本文化の重要や象徴である、漫画やアニメについても紹介してありました。日本語の新聞も毎日入手されており、久しぶりに日本語の新聞を閲覧させていただきました。この記念館も存続の危機に立たされているようで心配をしつつ後にしました。

3. ドイツの家屋や室内と階層セキュリティ構造

さてドイツの生活については紙面の都合上この当たりで終わらせていただきます。イースターは 3 下旬頃でしたが、この時期にはスーパーやちょっとしたお店にはイースターのウサギのチョコレートが売られており、これをお土産として大量に買い込み、3 月 31 日に日本へ帰国いたしました。また 4 月 14 日には第二次渡航を行い、4 月 30 日でガストハウス引き払い、秘書のコッホさんのお部屋を貸して頂くことになり引っ越しました。約一ヶ月程度このお部屋をお借りしましたが、コッホさんは友人のお部屋に引っ越され、一ヶ月後また戻られるということで、不動産会社と交渉して民間のアパートを最後の二ヶ月間、オストエンド通り 67 番地の 4F に借りました。この秘書の方に貸していただいたお部屋はベルゲン・エンクハイムというフランクフルト市の東端のところにあり、地下鉄 U7 線で大学と直結しておりました。途中駅に、ツァイル、市の森、ショッピングモール、戦跡等がある興味深いところでした。サーカス一座もいたりして面白かったのですが、クルップ駅というものがあり、そこにドイツ語で銘盤があったのですが、読んでみると、ここからユダヤやロマの人達がアウシュヴィッツ等の強制収用所に送るための専用駅だったとあり、なるほどこんなところポツン駅がある理由を感じた次第でした。ちょうど引っ越した後の 5 月 8 日が戦争記念日であったため、TV 番組はやたらと戦争追悼番組が流され、ナチスの犯罪について詳細に説明していました。

それでは次節では、ドイツの家屋について説明します。

3.1 ドイツ家屋・室内の特徴

残念ながら私は建築家ではありませんから詳細なことはわかりません、セキュリティの研究分野に足を突っ込んでいる者としての観点から申し上げます。

ドイツの一般的家屋施設の最大の特徴は、全ての部屋に鍵があり原則的に施錠しなければいけないことです。そのため部屋を借りると、即座に管理人や所有者からどっさりと鍵を渡されます。そして外出や部屋から離れる時は必ず施錠するようにと言い渡されます。

そして個人の身分に合わせ渡される鍵も違ってくるのです。居間はもちろん、寝室、風呂、トイレに至るまで鍵がついています。また鍵のシステムは二回廻し方式です。一回廻しても開錠しませんから、更にもう一回廻します。そしてノブやレバーを廻すと開くと次第です。

この仕組みは研究施設でも当然で、鍵を忘れたりすると何もできません。またインターホン型鍵システムが普及していて、外部から訪問者がある場合は、訪問者がドアの右横にあるボタンを押して各研究室やアパートの部屋の住人にブザーで知らせが入ります。そしてこの開錠ボタンは大抵、秘書の机か廊下にあり、それを押せば開くと言う仕組みです。実はこの仕組みこそがラネンベルグ教授が提唱されている階層セキュリティ構造そのものです。

現在のセキュリティモデルは外部と内部に分ける二極モデルですが、階層セキュリティ構造は、利用したい資源にアクセスする時に、その場に応じて認証を行います。この考え方は金融機関における ICT 利用にあたって重要事項です。例えば重要ファイルにアクセスする時、できるだけ決まった人にしか見せたくないとします。すると、その資源にアクセスする段階で認証をかけますが、単純ユーザ ID・パスワードだけではそのセキュリティ的強度があまり明確ではありません。そこで認証時に様々な情報交換させる事により、そのアクセスした人の情報に合わせてアクセス件を柔軟に決めます。

具体的な例として、公衆無線網に接続してインターネットにアクセスすると料金が表示される Web ページが表示されます。この時、カードの番号や有効期限等の様々な個人情報を入力します。その時 5€だと 15 分、8€だと 30 分、12€だと 2 時間そして 18€だと 1 日と選択することになりますが、この様に階層化された認証構造になっており、それが階層セキュリティ構造の一例です。これはアパート部屋の鍵や職場や研究室での鍵の構造と似ています。例えば、教授室は秘書と教授しか入れません。会議室は全構成員が入れます。また外部から研究員は、研究室に入ることはできますが、鍵を持っていないので入ることができない部屋が多数存在するのです。この様な複数の鍵を概念を付加した認証システムが階層セキュリティ構造の基礎になっているわけです。非常に面倒な事をしているような感じもしますが、鍵だらけの生活を送っているドイツ人にとっては一般常識であるため、無理なく受け入れられるのだろ

うなと思っています。この鍵の有無と部屋に入ると言う概念が ICT の中に自然に含まれるようになると、より各種セキュリティモデルの強度等の科学的な評価が可能になると思われます。

そしてセキュリティの評価が可能になれば、無駄なコストも極力な抑える事が可能となり、より先進的で発展的な事項に予算を充足できると考えられます。ラネンベルグ教授の研究は、ドイツでしばらく生活しないと判らなかったと言えます。セキュリティは生活文化の中に原点があると言うことあらため実感したのでした。

後大事なことは、人的なセキュリティとしては、挨拶が大変大事であったことです。自分の部屋から研究室までの間に出会う人は、余程あやしそうな人でなければ、「モルゲン」や「アーベント」と挨拶した方が良さそうです。挨拶しないと怪しい外国人が居ると警察に通報される事があるようです。

4. 結び

半年間の短い期間でしたが、ドイツ研究滞在中に、階層セキュリティ構造の原点を実感できたこと、ドイツの生活文化の楽しさを経験できたこと、英語が通じる事のありがたさをひしひしと実感したこと（笑）、聴くのも話すのも難しい R の発音ができるようになったこと、ラネンベルグ教授、秘書のコッホさん及びラネンベルグ研究室の方々に大変お世話になったことがとても嬉しく楽しい研究生活の思い出となりました。また 5 月に入ってからとても広い個人の研究室を教授より与えていただき、良い環境を得たおかげなのかわかりませんが、3 報の論文を投稿・受理していただきました。ドイツに研究滞在は、筆者にとって大変有意義であったと考えられます。

謝辞

私がドイツ長期出張中に多くの方々に講義の代講を快く引き受けていただき大変感謝しております。また、私を快く研究室に受け入れていただきましたカーイ・ラネンベルグ教授、部屋の手配や大学病院への同行等いろいろお世話になったエルビラ・コッホ女史、そして研究室のスタッフの方々、そしてこれらの海外長期滞在研究が行えたのも本センター職員、そして熊本大学の教職員及び学生の皆様のご理解ご協力があったからこそ遂行できたと申し上げます。この場を借りて厚く感謝申し上げます。そして、長期研究滞在費を支給していただいた文部科学省の方々にも大変感謝申し上げます。この研究事業は、

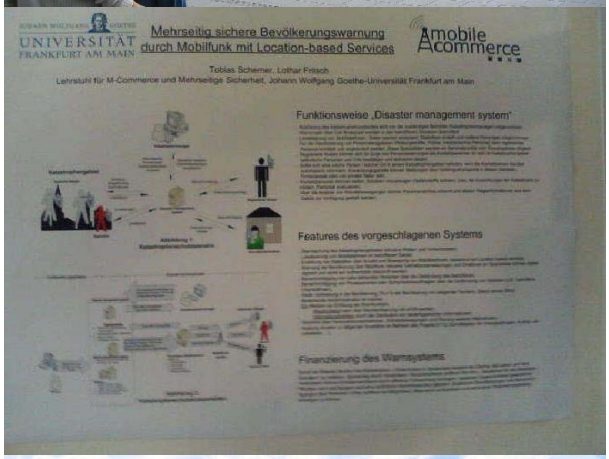
文部科学省の「平成 16 年度大学改革推進等補助金（海外先進教育研究実践支援プログラム）「高度情報化キャンパスの課題」によって助成されています。この場を借りて再度感謝申し上げます。

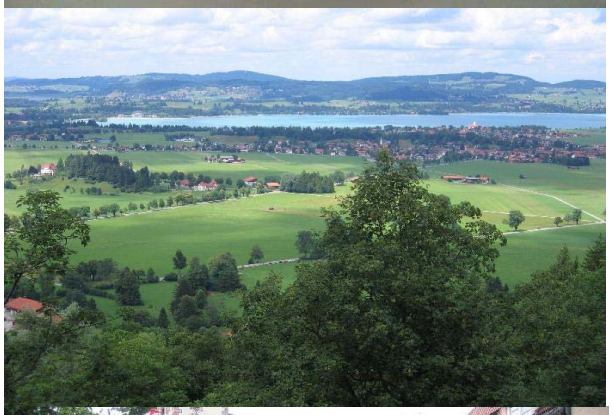
参考文献

[1] P. Barford and V. Yegneswaran: *An Inside Look at Botnets*, Special Workshop on Malware Detection, Advances in Information Security, Springer Verlag, 2006.

[2] J. Nazario, Defense and Detection Strategies against Internet Worms, I Edition; Computer Security Series, Artech House, 2004.

[3] (a) J. Kristoff, *Botnets, detection and mitigation: DNS-based techniques*, Northwestern University, 2005, http://www.it.northwestern.edu/bin/docs/bots_kristoff_jul05.ppt (b) J. Kristoff, "Botnets," NANOG 32, October,2004.





[4] D. David, C. Zou, and W. Lee, "Model Botnet Propagation Using Time Zones", Proceeding of the Network and Distributed System Security (NDSS) Symposium 2006; http://www.isoc.org/isoc/conferences/-ndss/06/ proceedings/html/2006/

[5] A. Schonewille and D. –J. v. Helmond, "The Domain Name Service as an IDS. How DNS can be used for detecting and monitoring badware in a network", 2006; http://staff.science.uva.nl/~delaat/snb-2005-2006/p12/-report.pdf

[6] (a) Y. Musashi, R. Matsuba, and K. Sugitani, "Development of Automatic Detection and Prevention Systems of DNS Query PTR record-based Distributed Denial-of-Service Attack", *IPSJ Technical Reports, Distributed System and Management 34th (DMS34)*, Vol. 2004, No. 77, 2004, pp.43-48. (b) Y. Musashi, R. Matsuba, and K. Sugitani, "Detection and Prevention of DNS Query PTR record-based Distributed Denial-of-Service Attack", *Proceeding for the 3rd International Conference on Information (Info'2004*), Tokyo, Japan, 2004, pp.233-237. (c) Y. Musashi, R. Matsuba, K. Sugitani, and K. Rannenberg, "Detection and Prevention of DNS Query PTR record-based Distributed Denial-of-Service Attack", *Information*, Vol.9, No.2, 2006, pp.339-349.

[7] http://www.trendmicro.com/vinfo/virusencyclo/-default5.asp?VName=WORM_MYTOB.A

[8] http://www.trendmicro.com/vinfo/virusencyclo/-default5.asp?VName=WORM_ZOTOB.A

[9] http://www.trendmicro.com/vinfo/virusencyclo/-default5.asp?VName=WORM_NETSKY.Q

[10] (a) R. Matsuba, Y. Musashi, and K. Sugitani, "Detection of Mass Mailing Worm-infected IP address by Analysis of DNS Server Syslog" *IPSJ SIG Technical Reports, Distributed System and Mangement 32nd (DSM32)* , Vol. 2004, No. 37, 2004, pp.67-72. (b) Y. Musashi, R. Matsuba, and K. Sugitani, "Indirect Detection of Mass Mailing Worm-Infected PC terminals for Learners", *Proceeding for the 3rd International Conference on Emerging Telecommunications Technologies and Applications (ICETA2004*), Košice, Slovakia, 2004, pp.233-237. (c) Y. Musashi and K. Rannenberg, "Detection of Mass Mailing Worm-infected PC terminals by Observing DNS Query Access", *IPSJ SIG Technical Reports, Computer Security 27th (CSEC27),* Vol. 2004, No. 129, 2004, pp.39-44

[11] (a) Y. Musashi, R. Matsuba, and K. Sugitani, "Detection, Prevention, and Managements of Security Incidents in a DNS Server", *Proceeding for the 4th International Conference on Emerging e-learning*

Technologies and Applicatications (ICETA2005), Košice, Slovakia, 2005, pp.207-211. (b) Y. Musashi, R. Matsuba, and K. Sugitani, "Prevention of A-record based DNS Query Packets Distributed Denial-of-Service Attack by Protocol Anomaly Detection", *IPSJ SIG Technical Reports, Distributed System and Management 38th (DSM38)* , Vol. 2005, No. 83, 2005, pp.23-28.

[12] http://www.trendmicro.com/vinfo/virusencyclo/-default5.asp?VName=WORM_SOBIG.F

[13] http://www.trendmicro.com/vinfo/virusencyclo/-default5.asp?VName=WORM_MYDOOM.A

[14] D. Whyte, P.C. van Oorschot, E. Kranakis, "Addressing Malicious SMTP-based Mass-Mailing Activity Within an Enterprise Network", Carleton University, School of Computer Science, Technical Report TR-05-06 (May 2005).

http://www.scs.carleton.ca/research/tech_reports/2005/-download/TR-05-06.pdf

[15] K. Ishibashi, T. Toyono, K. Toyama, M. Ishino, H. Ohshima, and I. Mizukoshi, "Detecting Mass-Mailing Worm infected Hosts by Mining DNS Traffic Data",

Proceeding of the 2005 ACM SIGCOMM workshop on Mining network data, Philadelphia, Pennsylvania, USA, 2005, pp.159-164.