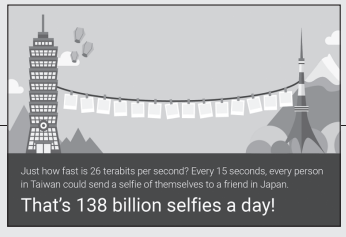
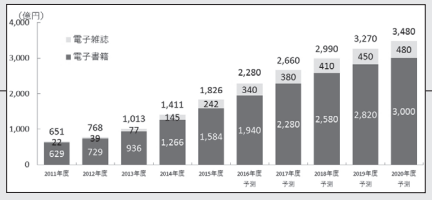
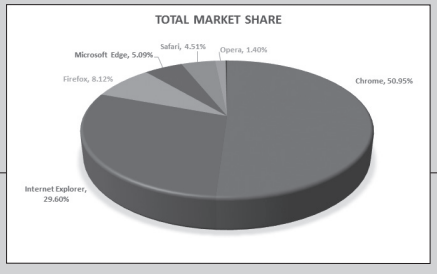
IAjapan Review

Vol.16
No.2
2017年2月

CONTENTS

一般財団法人インターネット協会
Internet Association Japan

インターネットの主な出

	2016年7月	8月	9月
業界	**◎米Verizon、米Yahooの主要事業を48億3000万ドルで買収** ■「日本IT団体連盟」が発足、政策提言やIT人材の育成に「一丸となって取り組む」 ■Microsoft、Windows 10への無償アップグレード用プログラムの提供を終了 ■ジョルダン、「乗換案内」アプリにAIで列車遅延時間を予測、関東138路線を対象に実証実験	■シマンテックが「Encryption Everywhere」、SSLサーバー証明書の無償発行環境を整備 ■米Google、すぐにコンテンツへアクセスできないモバイル向けページのランキングを低く表示、2017年1月より ■米Microsoft、「PowerShell」をオープンソース化、LinuxやOS X向けに提供 ■アマゾンジャパン、電子書籍読み放題サービス「Kindle Unlimited」、月額980円で国内提供開始 ■米Microsoft、Excelのデータや関数をカスタムアプリで利用できる「Excel REST API」を提供	**◎Ethernet Alliance、既存のCAT5eケーブルで2.5Gbps、CAT6ケーブルで5Gbpsを実現する有線LAN規格「IEEE 802.3bz」を承認** ■「NURO 光」の10Gbpsサービス、月額6480円に値下げしてリニューアル ■米Google、クラウド事業を新ブランド「Google Cloud」として再編 ■Twitterが140文字制限を緩和、写真・動画・引用RTなどはカウント対象外に ■米Google、日台間を26Tbpsで結ぶ海底ケーブルに投資 日本ー台湾間の光海底ケーブルは、日米間を結ぶ「FASTER」に対する追加投資として敷設されたもの  出所：https://blog.google/topics/google-asia/making-google-little-bit-faster-across-asia/
社会・事件	■「Pokémon GO」をプレイする上での注意事項をマカフィーやNISCが公開 ■三井住友銀行をかたるメールに添付されたZIPファイルに注意、Bebloh亜種 ■映画の日本語字幕を勝手に作成してアップロード、国内初の逮捕者 ■母親の46.5%が小学校でのプログラミング教育必修化に賛成、ジャストシステム調査	■ウェブサイトの改ざん被害多発、4項目の定期点検をJPCERT/CCが呼び掛け ■NTT東西の「ひかり電話ルーター」に脆弱性、IPAとJPCERT/CCが公表 ■「ゆうちょ銀行パスワード変更完了お知らせ」というフィッシングメールが出回る、フィッシング対策協議会が注意喚起	■IPA、ワンクリック詐欺で確認されている電話番号を公表、セルフチェックできる診断チャートを公開 **◎米Yahoo!、5億人のユーザー情報が流出、国家がらみの攻撃の疑い** ■Android端末を狙うランサムウェアが増加、端末を操作できないようにする「ロック型」 ■Amazonをかたるフィッシングメールが出回る、フィッシング対策協議会が注意呼び掛け
市場・調査	 国内電子書籍・電子雑誌市場規模の推移・予測、2020年度は3480億円市場に ■2015年度の国内電子書籍市場は1584億円規模、前年度から25.1%増加、8割がコミック、インプレス調査 ■Windows 10ユーザーがWindows 7を上回る、ジャストシステムの定点調査で ■Amazon、容量無制限のオンラインストレージを年額1万3800円で国内提供 ■「Twitterモーメント」国内提供開始、話題のツイートを一覧表示	Chormeのシェアは50.95%で初の5割超え、Internet Explorerのシェアは29.60%に低下  出所：http://marketshare.hitslink.com/ **◎Chromeのシェアが5割超える、7月のデスクトップブラウザーシェア、Net Applications調査** ■国内のSNS利用者、今年末に6872万人に達する見込み、普及率69.3%、ICT総研調査 ■Microsoft、大型アップデート「Windows 10 Anniversary Update」提供開始 ■ニコニコ動画、投稿可能な動画ファイルサイズを1.5GBへ拡大、推奨フォーマットも変更	■ランサムウェアに感染した企業の65%が身代金を支払い、5社のうち1社はデータ復旧できず、英Trend Micro調査 ■9割の高校生が個人情報掲載リスクを認識も、8割が掲載、MMD調査 ■10代女性の7割以上がTwitterアカウントを複数保有、7アカウント以上も8.3%、コロプラ調査 ■米Microsoft、「Windows Essentials 2012」の2017年1月10日サポート終了を発表

来事 2016.07 → 2016.12

10月

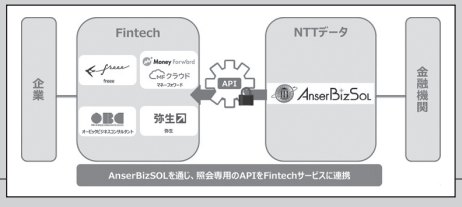
◎米国政府がルートDNSや、IPアドレス管理などの“IANA機能”監督権限を手放す

■新国家資格「情報処理安全確保支援士」の登録申請がスタート、試験は2017年4月より実施

■NEC、地磁気による屋内測位技術を開発、ビーコン・無線LANの設置不要

■NTTデータ、法人向けインターネットバンキングとFintechサービスをつなぐAPI連携サービスを提供開始

法人向けインターネットバンキングサービス「AnserBizSOL」のAPI連携イメージ。残高照会などの照会機能をAPIを通じて提供する



出所：http://www.nttdata.com/jp/ja/news/release/2016/072600.html

■ISDNのディジタル通信モードが2020年度にも終了へ、企業間の自動発注システムに大きな影響？ JISAが対策を呼び掛け

■警察庁、BIND 9の脆弱性を標的とする攻撃活動を観測、アップデートの適用を

■Flashのゼロデイ脆弱性、IE/Edge用の修正パッチをマイクロソフトが定例外で公開

■日本では85%が未導入、なりすましメール対策にドメイン認証技術「DMARC」の導入をIIJが呼び掛け

■Mozilla、Firefoxのレンダリングエンジンを置き換える「Project Quantum」を発表

■Amazon.co.jpで誰もが無料で紙の書籍を出版できる「著者向けPOD出版サービス」、インプレスR&Dが開始

■Windows Vista、サポート終了の2017年4月11日まで半年を切る

■新ドメイン「.moe」は米英でニーズあり？契約者比率で日本を上回る

11月

■IPv6普及・高度化推進協議会発表、「IPv6デフォルト化が進展するも、ほとんどがGoogle（動画）、次なるステップは国内の対応」

■Microsoft、セキュリティ更新プログラムのポータル「Security Updates Guide」開設

◎Google、検索インデックスでモバイル版コンテンツを優先する変更を発表

■IPA、脆弱性体験学習ツール「AppGoat」の最新版「V3.0」、集合学習モード追加

■ニフティ、「@homepage」サービスを終了、個人などのホームページ約12万件が消滅

■Amebaにリスト型攻撃、約59万アカウントが不正ログイン受ける、パスワード再設定を呼び掛け

■国内の複数サイトでトップページ改ざん事例、「index_old.php」読み込ませるスクリプト、警察庁とJPCERT/CCが注意喚起

■JPCERT/CC、IoTマルウエア「Mirai」が悪用する機器の保守管理ベンダーを特定、対処を求める活動開始

「Unicode 10.0」で新たに追加される絵文字の一部

■Unicode Consortium、「Unicode 10.0」への追加候補となる51種類の絵文字を発表

■東京メトロ、銀座線の車両内へ無料Wi-Fiサービス導入開始

■日本MS、「Minecraft: Education Edition」11月1日提供開始、教員あたり月額120円、児童・生徒は無償で利用可能

■ChromeにおけるHTTPS使用状況、PCでの閲覧時間で3分の2を超える、米Google調査

12月

◎KDDIがビッグローブを完全子会社化へ 総額約800億円で

■Microsoft Edgeで高圧縮アルゴリズム「Brotli」をサポート、Windows 10 Creator's Updateで

■Google Chrome、Flashに代わるHTML5デフォルト化を開始、一部サイトから段階的に、2017年10月には全サイトで

■NISC、「ネットワークビギナーのための情報セキュリティハンドブック」を全154ページに改訂し、無料で提供

公開されたVer.2.00は全5章で154ページに、初版の33ページから内容が大幅に増強された

出所：http://www.nisc.go.jp/security-site/handbook/index.html

■マルウェア「Gooligan」、100万件以上のGoogleアカウントを侵害、チェック・ポイント発表

■DeNA、キュレーションサイトのデタラメ／パクリ記事問題で経緯説明・謝罪会見

■ヤフー、Yahoo! JAPANをかたる「至急!!! お客様 ID危険検出」メールに注意換気、ウイルス感染の恐れ

■子供がアダルトサイトへアクセス試行した回数、日本は1人あたり年間39回で世界最多、カスペルスキー調査

■国内通信事業者20社の迷惑メール送受信防止対策状況、DMARC提供プロバイダーはわずか2社、総務省が調査

■自宅無線LANを暗号化していないユーザーが4分の1、セキュリティソフト導入も半数以下、対策への認識不足が浮き彫りに

■物販系EC市場の売上高トップはAmazon.co.jp、2位ヨドバシ.comの10倍以上、出店数は楽天が最多、インプレス調査

現場は今！
ネット安心・安全の現場から
第13回「映像資料撮影秘話」

この連載では、インターネットのルール＆マナー、フィルタリング啓発などの活動をお伝えします。

「先日ご相談した映像資料の企画コンペ、当社が勝ちました！よって、正式に監修をお願いします」と、映像制作会社の担当から、ルンルンとした声色で電話をいただいた。

喜ばしいことなのだが、気持ち半分以上が憂鬱になっている。私の苦手なインタビュー撮影があるからで、理由をこれからお話ししてみたい。

監督のこだわりがある

これまでの映像監修回数を数えると、2004年～2016年の12年間で15本になった。2004年は忘れもしない長崎県小6同級生チャット殺害事件があった年である。そのため当時は小中学生向けネットトラブル対策が主流であり、恐くて暗い内容が多く、映像制作担当者は刑事ドラマのようなドラマチックな脚色にこだわっていた。最近は大人向けや人権啓発も多くなっていて、ひと頃に比べると穏やかな内容のものが増え、効果音やBGMも楽しい雰囲気に仕上げられている。

昨年2016年は2本の映像監修を行った。映像監督はいずれも男性、それぞれ強いこだわりを持っている。

1本目は、自治体教育委員会企画の人権学習教材ビデオの35分もの。3つの人権テーマ（インターネット、高齢者、外国人）の1つを担当し、構成は各々ドラマ9分＋解説2分である。教育委員会と監督と打ち合わせを行う時に、ドラマのシナリオを監修することはもとより、自分のインタビュー解説部分の発言内容を吟味する。可能な限り自分が露出しないように、監督へ「私がお話しする場面は全部出さずに、再現ドラマを再度流して私の声だけにしたり、テロップを入れたりしてほしい」と要望を出してみたりする。監督は「よし、わかった！」と希望を受けてくれた。

撮影当日は12月、インターネット協会の会議室に大勢集まった。映像スタッフ5名に加え、立ち合いの教育委員会4名と自治体2名、計12名である。大きな照明スタンドが2つあり、冬にもかかわらず暑苦しい空気がただよっている。

「さあ、とりあえず、練習なしで本番のつもりで話してみましょうかね！」と監督のゴーが入り、この瞬間で一気に緊張のピークに。緊張するともうダメで、セリフを覚えられず何度も何度も失敗する。時間がどんどん過ぎて、待っている立会人に迷惑をかけてしまう……と思うとだんだん焦ってくる。そして案の定ドツボにハマっていく。不思議なもので緊張しすぎると、緊張に疲れてしまった反動でリラックスするように身体が出来ているのかもしれない。やっぱり苦手なものはしょうがないと腹をくくるしかない。

私が上手く話せないところはカメラの後方にカンペを用意してくれた。長文のセリフは3つに分けて区切ってくれた。こうやって、撮影は無事に終了！……と思いきや、監督から「ちょっと待った。撮り直ししよう。全5つのコメントのうち後半の4つはリラックスしてスムーズだったが、前半の1つは棒読みだったので、もう1回話してみよう。今話せばもっと良くなるよ」と。そして、コメントをもう一度話した。

> **質問**：なぜネットでは簡単に人権侵害が起きてしまうのでしょうか？
> **コメント**：広める側は匿名だからといって軽い気持ちで書いています。でも、受け取った側はそうではありません。そのことがクラスや友達の意見にのまれて、人の心を傷つけるかもしれないということをよく考えずに書いてしまうことが原因になっています。
> たとえその情報が真実だったとしても、デマだったとしても、「拡散希望」などとネット上に書いてしまって、そうやって広めてしまうのは、人権の侵害です。

リラックスして上手く話せたのだが、季節柄の石焼き芋売りの声が入る等での撮り直しがあったが完成した。収録は予定の2時間を超えて3時間かかった。

撮影から2か月後、完成DVDが届けられた。ドキドキしながら画面を出来るだけ小さくして見ると、監督のこだわりが見える。私の露出を少なくという要望は、目線が不自然だったところを「声」だけに編集して叶えてくれた。

2016年は中学校等で8回上映したが、ビデオが良かったと言われ安堵する。やはり映像教材は効果的だと再認識する。

撮影前のスタンバイ中の模様

タレントからの助言に励まされる

昨年の2本目は、国が制作するDVD教材で、人権侵害をネット上で起こさないためにというテーマで高校生向けの30分もの。構成はドラマ10分×2本+解説8分+ドラマその後2分である。

1本目と同じ映像制作会社からの依頼で、私のインタビューは懲りたでしょうと想像していたが、コンペに勝ってしまったので、企画内容を変更するわけにはいかなかったのだろう。今回は単独インタビューではなく、タレントと二人の対談で行うとのことだった。大人気の20代の女性歌手で名前を聞いて驚愕であったが（以下、Aさんとする）、このような機会をいただいたことは光栄で嬉しかった。Aさんは素敵な女性だなと思っていたが、Aさんの執筆本を読んで、ますますファンになってしまった。

当日の撮影は、都内の専用スタジオを午後3時から9時まで6時間借りており、長期撮影におよぶことを予想していたようだ。私から監督に「失敗が多い私でも3時間程で収録できるようにしたい」と伝えると、「何が起こるかわからないから多めに時間をとっている。長くても3時間で終わると思うよ」とのことだ。

午後3時にスタジオ入りして専門スタッフがヘアメイクをしてくれた。時間がたっぷりあったので、お化粧法や表情のアドバイスもしてくれて、なんともありがたいことだ。テレビ番組の「変身ビフォア＆アフター」のように、プチ変身することが出来た。このメイクが長時間崩れないことを願いながら、午後4時から撮影が始まった。

今回ははじめからカンペが用意されていて、監督からは「自分の言葉に置き換えてもいいが、基本はこの通りに話してもらった方がいい」と要望をいただく。カンペがあると棒読みになりそうなので、カンペがないように話さなければならない。

対談相手のAさんはさすがだ。活舌が良いし感情も入っている、何よりも目線がカンペを読んでいる感じがしない。良い見本を目の前にして、私も頑張らねばと張り切った。でも、緊張しやすい性格は急に良くなるはずもなく、何度もやり直しとなってしまう。今回は一人ではないので、対談相手に迷惑をかけてしまわないようにと思いながら、相手の話を聞きながら答えることに集中した。

嬉しかったのは、Aさんから話し方のアドバイスをもらったこと。口がまわらない箇所「自分を見失わないように…」の「みうしなわない」で噛んでしまうところを、Aさんは「みうしな（･）わない」と「な（･）」を意識したら話せるんじゃないかなあ～、と助言。その後は1回で言い切ることができた。あー、有り難いこと♪

以下、該当のコメントである。

> SNSに夢中になりすぎて、自分を見失わないようにしてもらいたいと思います。
>
> 思春期は、自分は何なんだろうと自分自身を見つめて悩む時期にもかかわらず、SNS上で“いいね”をしてもらうことに時間を割いて頑張ったり、グループで無理して同調意識を高めたりしていないでしょうか。

2時間で撮影は終了し、Aさんは次の仕事に移動した。予定よりも早かったが、ここからまだ続きがあった。

監督が「時間が余ったので、もう一度全部やってみるか」と言う。えー、対談なのにAさん抜きで全部やるのですかと聞くと、「いくつか気になった箇所があり、せっかくなら良いものにしたいからね」と。

その時、午後6時だったが、3時間前に比べると化粧が落ちはじめている。その日は木枯らし1号が吹いた寒い日で、外からの隙間風がスタジオに入ってくる。足元が寒いし顔がほてるという最悪のコンディションだ。監督を見ると「今度こそお願いします」という表情をしていて、Aさんが目の前にいるつもりで、感情をこめて話した。何回やり直しをしたのか覚えていないが、終了時刻は午後8時半になっていた。

DVDは、2017年3月頃から貸し出しを行うほか、動画サイトでも公開をする予定とのこと。まだ完成作を見ていないので何とも言えないが、どんな風に仕上がったのかを楽しみにしている。

第14回は、講師用資料作成についての話をする予定。

IoTセキュリティガイドラインの内容と事業者の課題

テクニカルライター　中尾真二

総務省と経済産業省は、2016年7月に「IoTセキュリティガイドライン Ver1.0」を公表した。PCやスマートフォン以外の機器や日用品までがインターネットにつながるIoT（Internet of Things）製品やサービスはどのようにセキュリティを確保すればいいのか。本稿では、同ガイドラインの概要を示しながら、IoTセキュリティのポイントを整理してみたい。

IoT機器の特徴

IoT機器をセキュリティの視点からみた特徴はなんだろうか。ガイドラインでは次のように述べている。

1. デバイス数、利用範囲が大きく考慮すべき範囲が広い
2. ライフサイクルが長い
3. メンテナンスされにくい
4. IoTとネットワーク側に合意や前提がなく接続される
5. セキュリティ機能の実装がしにくい
6. 現状にはないデバイス、使い方が想定される

これらは具体的には、デバイス数が多いという問題は自動車や監視カメラがオンラインになることを想像すればいいだろう。移動する車、いたるところに点在するカメラに対する脅威や対策の範囲は地理的な広さもある。IoT機器は普段の生活にかかわりが深く、壊れないかぎり使い続けられる傾向がある。また、センサーやカメラなど設置場所に放置され、常時人間やオペレータが操作するような機器ではない。ライフサイクル、メンテナンス上の課題解決はこれからだ。

もともとスタンドアローンで設計された製品が多いIoT機器は、オープンネットワークの常識が通用しない。メーカーや業界の都合で設計されているので、相互接続や相互運用の概念もないことがある。

デバイスによっては、自らデータ交換を行ったりするものも存在するが、多くはハードウェアやコストの制限からセキュリティ機能を実装していなかったりする。また、ソフトウェア、ファームウェアのアップデートインフラがないこともネックになるとされる。

IoT機器への脅威

IoT機器に対するリスクや脅威にはどのようなものがあるだろうか。

代表的なものはWebカメラや監視カメラだろう。2016年10月に北米を襲った大規模なDDoS攻撃（NetfilxやTwitterも被害を受けた）に利用されたのは、中国製のWebカメラで、管理者アカウントの初期設定の不備を突かれて、ボットとして利用された。このメーカーは製品を回収せざるをえなくなった。

自動車へのサイバー攻撃はあえて説明するまでもないかもしれない。車載用通信端末を経由して自動車内部のネットワークへの侵入を許せば、ECU（電子制御装置）などクリティカルな制御を奪われてしまう。カーシェアなどに期待されているスマートキーも、暗号鍵の強度は高くても、スマートフォンやドングルが脆弱性となる場合がある。Androidを搭載したスマートTVがランサムウェアに感染した事例も報告されている。ゲーム機なども類似の被害が考えられる。

IoT機器で特に注意が必要なのは個人情報とプライバシーだ。ウェアラブルなヘルスケアデバイスなどは、ユーザーに深くかかわる情報を扱うため、アカウント管理、アクセス制御、データ保護などの対策を慎重に考える必要がある。

ガイドライン概要：5つの指標

ガイドラインでは、IoTセキュリティの考え方について次の5つの指針を示している。

① 方針

IoTの性質を考慮した基本方針を定める。とくに経営者のコミット、内部不正への対策を注意点として挙げている。

② 分析

リスク分析をしっかり行う。基本は、価値があり守るべき情報資産を明確にし、それに対する脅威を正しく把握することだ。個人情報、プライバシー、人命、ハードウェア資産、管理者権限、経営データなど、守るべき資産には有形無形のものがある。

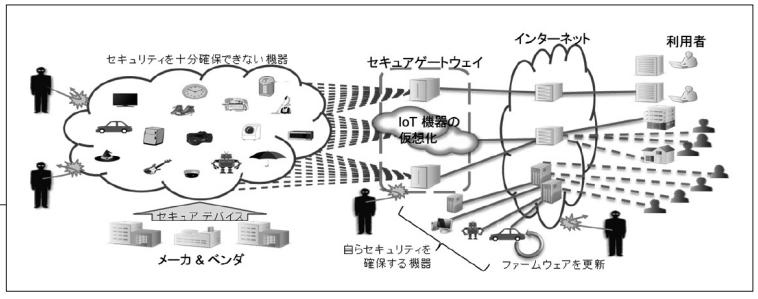


図1　セキュアなゲートウェイを経由する接続イメージ（IoTセキュリティガイドライン ver1.0より）

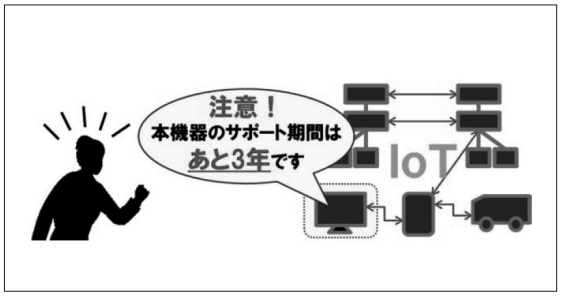


図2　サポート期間の周知（IoTセキュリティガイドライン ver1.0より）

③ 設計

守るべき資産を守るサービスや機能の設計。不特定多数との接続やセキュリティライフサイクルを取り入れた設計。PDCAによる設計改善のサイクルもセキュリティ対策の基本だ。

④ 構築・接続

ネットワーク上の対策を考える。初期設定はセキュアな方向で考える。認証機構や暗号化といった保護対策の導入など具体的な技術対策を実装する。

⑤ 運用・保守

安全安心な状態を維持すること。そのために必要な情報収集、発信、共有を適切に行うこと。必要な体制や組織づくり。脆弱性が発見されたときの対処方法のマニュアル作成といった作業を伴う。

このうち①の「方針」から③の「設計」までは、一般的な情報セキュリティマネジメントの考え方に通じるものだ。IT業界でセキュリティにかかわっていればおなじみのプロセスだろう。よくある間違いは、このプロセスが面倒だからとテンプレートで済ませてしまうパターンだ。結局セキュリティベンダーが勧めるソリューションを導入して終わってしまう。それでうまくいく場合もあるが、IoTに関しては専門家も未知数な領域でもある。リスク分析はやりすぎて困ることはない、というスタンスが必要だ。

IoTセキュリティ対策の5つのポイント

セキュリティ関連の対策技術が直接関係してくるのは、④の「設計・接続」と⑤の「運用・保守」の部分だ。ガイドラインでは「要点」としてそれぞれのポイントを整理している。

サービス設計時に、どんなことを考えればいいのかわからない場合は、「要点13」から「要点21」までをチェックすれば、必要な対策ポイントが見えてくるだろう。

詳しくはガイドラインを見てもらうのが最善だが、ここでは少し視点を変えて、これまでネット接続環境がなかったものがつながるようになったとき、必要となりそうな対策技術を5つ紹介する。

・暗号化技術

可能な限り製品やシステム内でも暗号化を施す必要があるが、それが無理なら最低でも通信経路の安全は確保したい。IoTでは通信路は後付けとなることが多いので、VPN、HTTPSのような技術から独自の暗号処理などを必要に応じて実装する（図1）。

・認証基盤

公開鍵基盤（PKI）の利用を考える。暗号化処理とセットとなることが多いが、サービスアカウントによる利用者権限の管理は必須である。IoTの場合、認証相手は人間とは限らない。正しい機器からの通信か判断するには認証機構は不可欠だ。

・モニタリング

パケットが正しいものでも、状況的に正しいコマンドなのか、処理なのかを監視できればよりセキュアになる。いままで外部との接続がなく安全だった環境がIoTによって外部との接点ができたとき、その入り口（認証）だけでなく、内部のトラフィックモニタリングが有効となる。

・アップデートインフラ

PCやスマートフォンではOS・アプリのアップデートのインフラが整備されているが、IoT機器ではまだ十分ではない。狭いRAM領域に感染するマルウェアも存在する。ファームウェアを含むアップデート方法の確保は重要だ。利用者へのアップデート提供期間（サポート期間）の周知を徹底する必要もある（図2）。

・セキュリティバイデザイン

上記の技術を設計段階から組み込む考え方が重要である。IoT機器こそ、セキュリティ対策を後から施そうとすると膨大なコストがかかる。ソフトウェアライフサイクルを考えたサービス設計が抜け落ちると、インシデント発生時の被害や対応が増大する。

■ IoTセキュリティガイドライン ver 1.0
（総務省）
http://www.soumu.go.jp/main_content/000428393.pdf
（経済産業省）
http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf

AIビジネスの現状はどうなっているのか

テクニカルライター　中尾真二

AI・人工知能がちょっとしたバズワードとなって久しい。しかし業界20年、30年のベテランとなるとAIブームは今回が初めてではないと思うだろう。

深層学習が切り開いた現在のブーム

前回ちょっとしたうねりが起きたのは20年以上前のニューラルネットワークブームのときではないだろうか。今回のブームの火付け役はGoogleが開発したAlphaGoだ。その間にはIBMのDeep Blueがチェスチャンピオンを破ったり、クイズ番組の問題を解いたりしたこともあったが、これらの出来事の背景には、ディープラーニング（深層学習）というブレークスルーがあった。

深層学習は、ニューラルネットワークによる機械学習を多層的につなげることで、高い精度で対象を識別（評価）できるようにした機械学習の一種だ。現在、AIというと機械学習や深層学習の話題が多いが、他にも決定木モデルや確率モデル（ベイズモデルなど）といった技術も有名だ。

AI技術のポイント

機械学習（深層学習）における学習とは、人間が用意したAIアルゴリズムに学習用データ（例えば猫を認識させたい場合は大量の猫の写真）を処理させて、結果を人間が評価してAIアルゴリズムを実装したAIモデルのパラメータを調整していく作業を意味する（右上の図）。

一般に学習データは多いほどモデルの精度は高まるが、多ければよいというものでもない。大量のデータで闇雲に学習させると、判定精度が落ちることもある。

生成されたAIモデルをブラックボックス（ライブラリ）として使うことはそれほど難しくはない。米国のデータサイエンティスト スティーブ・ゲリンジャー氏による「Machine Learning Skills Pyramid V1.0」では、機械学習に携わる技術者を次の3段階に分類している。

・機械学習リサーチャー／サイエンティスト
・機械学習エンジニア
・データエンジニア

リサーチャーやサイエンティストは、AIアルゴリズムを開発できる技術者。機械学習エンジニアはAIアルゴリズムを基にソリューションを設計できる技術者。データエンジニアは、DBや各種ソフトウェアプラットフォームを組み合わせたり、学習のためのデータ収集、処理などを行う技術者だ。厳密な統計はないが、リサーチャーやサイエンティストはグローバルでもごく少数で、AIエンジニアの多くは機械学習エンジニアとされている。

適用分野と応用事例

AIは、すでにさまざまな分野で応用されている。古くからニューラルネットワークや確率モデル、機械学習が利用されている分野としては手書き文字認識、音声認識などが挙げられる。現在は車の自動運転支援、医療診断支援、市場予測、セキュリティなどへの展開が注目されている。

■ 文字・音声認識

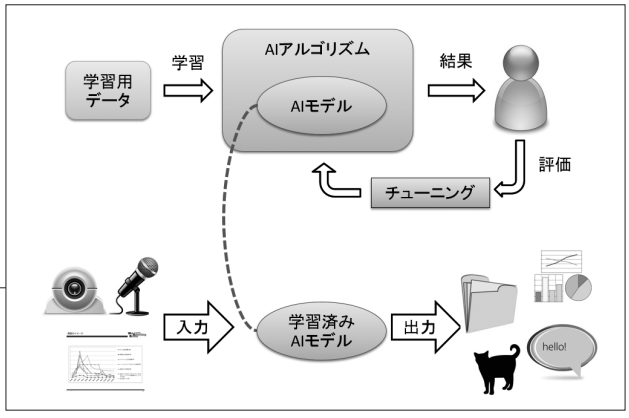
印刷文字のOCR、手書き文字入力装置は1980年代から存在していた。音声認識も、初期のころは自分の声をサンプリングさせる方式が多かったが、ほどなくAI技術を応用し、サンプリングなしで高い認識率を出すようになった。これらの技術はかなり枯れたものと言えるが、その先の自然言語認識、意味（セマンティック）分析に深層学習の応用が進んでいる段階だ。

■ 画像認識

古くは指紋認識、顔認識での研究・応用がされており、現在は、何の画像であるかの認識（犬、猫等のダグ付け）、同時に複数の対象の認識、動画のリアルタイム認識、さらには人や動物の行動認識（なにをしているのか）、次の動きの推論などへの研究・応用が進んでいる。

■ 自動運転（支援）

自動運転でも深層学習が実用化のスピードを速めている。高速道路の単一車線走行、前車追従走行、衝突回避ブレーキなどは、すでに実用化されている。認知・判断のための情報はカメラ画像とミリ波レーダー・レーザースキャナーを組み合わせている。一般道など、さまざまな状況で



AIアルゴリズムと
AIモデルの関係

自動運転を実現するには、より精度の高い3D地図、GPS受信機、V2Xといった周辺技術も欠かせないとされる。

■ 医療診断（支援）

CT画像、MRI画像のスクリーニングには、以前からAIによる画像認識が利用されている。米国などでは、問診や初期診断にAIを利用したツールやサービスを使う医師も少なくない。膨大な画像処理、経験や知見不足による見落とし対策などには、AIによる自動化の有効性は高い。今後は、症状の予測、病気の予測、治療計画など利用範囲が広がっていくかもしれない。

■ 金融・市場予測

株や為替の取引において、市場予測にAIを利用する動きがある。株取引をAIで自動化する研究やサービスも活発だ。

■ 経営意思決定

CRMデータから顧客の行動を予測したり、満足度向上に役立てる。従来は履歴データのマイニングや解析によって行っていたが、AI導入が進んでいる。同様にマーケット動向、消費者動向の分析にAI利用する動きがある。

■ 農業・製造業

農業では、作物の生育・収穫の予想や計画にAIが展開されるかもしれない。製造業では、品質管理の検査ラインで画像処理チェックにAIが利用されている。今後は、生産計画、歩留まりの管理、といった上位プロセスへのAI応用が考えらえる。

■ セキュリティ

セキュリティ分野では、スパムメール判定、画像フィルタリングにAI技術は以前から利用されていた。近年では、トラフィック監視、添付ファイル検査、ログ解析にAIを利用する例が広がっている。マルウェアや攻撃パターンの判定は、AIを使うことで未知の攻撃への対応がしやすくなる。従来からのシグネチャベースのマッチングモデルでは、トラフィックやマルウェアを検査するには事前情報がなければ危険とは判定されない。AIならば、特定のパターンに依存せず攻撃を検知できる可能性がある。脆弱性の自動発見、自動修復にもAIによる自動化も研究されている。

■ パーソナルエージェント

Siri、コルタナ、Amazon Echoが有名だが、自然言語認識が可能なエージェントも各社が研究している分野だ。いまのところ高度な音声認識という状態だが、自然な会話の中から必要なタスクを抽出し、あいまいな情報は対話によって聞き出すといったエージェントがでてくると予想される。今後は、コンピュータやクラウドへの入力インターフェイスは、キーボードやタッチから音声にシフトする可能性がある。自然言語処理が可能なAIは、あらゆるサービスのインターフェイスとなりうるもので、大手プラットフォーマーは自社で確立しておきたい技術である。

今後の展望と課題

現在のAIの応用範囲は、知能活動でいえば認知や識別の模倣または自動化がメインだ。顔を認識したり、対向車を識別したり、膨大なデータの中から異常を検出したりといった処理だ。

今後は、より判断に近い部分への応用が進むと考えられる。消費者の動向予測、最適な経営戦略の立案、意思決定まで踏み込むような処理をAIにやらせることになる。

そのためには、事前に学習データを用意せずに多様なパターンに対応できるAIが必要とされる。課題は学習効率の改善または学習方法そのものだ。より少ないデータでも学習できるAI、多数のAIを組み合わせて複雑な判断に対応する研究が進んでいる。

その一方で、既存のAIモデルを利用してソリューションやサービスを構築する機械学習 エンジニア、データエンジニアのニーズも高まっている。もちろん、AIアルゴリズムを開発できる技術者の育成も重要だが、機械学習エンジニア、データエンジニアを育てることが、AI市場でのビジネス成長の鍵といえるだろう。

■ Machine Learning Skills Pyramid V1.0 - Steve' s Machine Learning Blog
http://www.anlytcs.com/2014/01/machine-learning-skills-pyramid-v10.html

ご報告

IPv6ディプロイメント委員会報告

IPv6 Summit in TOKYO 2016で開催したパネルディスカッションの様子

2016年度後期の活動

全世界的なIPv4アドレス資源の枯渇に伴い、IPv6の導入に拍車がかかっている。IPv6ディプロイメント委員会では、IPv6の普及を推進するための活動を実施している。2016年度は、他国に後れを取っている分野についてIPv6対応を進めることを主目的とし、携帯サービス主要3社が発表した携帯網における2017年からのIPv6提供予定に関する情報共有、サービス提供者におけるIPv6対応、IoT（Internet of Things）での利用など、IPv6の実活用に関する動きを進めるべく活動している。

本稿では、委員会の主催イベントとして高松で開催した地域Summit、TOKYO Summitについて紹介する。

IPv6 Summit in TAKAMATSU 2016

2016年9月16日（金）に高松市瓦町にて、「IPv6 Summit in TAKAMATSU 2016」を開催した。メインセッションは、IPv6普及・高度化推進協議会 常務理事/慶應義塾大学 中村修教授の基調講演より開始、日本のIPv6対応が海外に遅れ始めていること、対応策の一つとして進めている2017年開始予定の国内携帯キャリア3社におけるIPv6対応に関する紹介等があった。

その後、香川大学 今井慈郎教授より、IPv6は第4次産業革命として注目されている「インダストリー4.0」において実社会とITが結びつく際の必須要素となっていることの紹介があった。続く株式会社STNet 井下道隆氏の講演においては、同社のIPv6運用について、総トラフィックの約35%がIPv6になっている一方、法人顧客におけるIPv6契約者数は全体の約2%であり、法人のIPv6対応に課題があることが示された。

講演の最後は、ノルディックセミコンダクターエーエスエー 山崎光男氏からBluetooth Low EnergyのIPv6対応状況についてお話いただいた。その後のパネルディスカッションでは、中村教授をコーディネーターとして、IPv4を利用し続けることの課題について議論され、IPv6の導入により運用やサービスの実現が容易になり，コスト面でも有利なことが確認された。午前中に実施したセミナーから多くの方に参加いただき、盛況な会となった。

IPv6 Summit in TOKYO 2016

今回もInternet Week開催週の初日となる2016年11月28日（月）に、IPv6普及･高度化推進協議会と共催で、IPv6 Summit in Tokyo 2016を開催した。前回までの秋葉原から浅草橋のヒューリックホールに場所を移しての開催となった。

Summitは、IPv6普及・高度化推進協議会 専務理事の江崎浩東京大学教授の開会挨拶から始まり、続く基調講演として北陸先端科学技術大学院大学の丹康雄教授より、「IoTの技術動向と日本の戦略」と題し、ホームネットワークなどのために開発・標準化されてきた技術の紹介と、それらが現在どのように活用されているかの事例が示された。続いて、JPNICの奥谷泉氏からIGF（Internet Governance Forum）におけるIPv6活用事例収集活動の紹介があった。その後、「IPv6普及状況」「IPアドレス最新レポート」「IPv6普及･高度化推進協議会報告」があった。

後半は、江崎教授をモデレーターとして携帯キャリア3社（ソフトバンク･NTTドコモ･KDDI）の、2017年からIPv6インターネットへの接続をデフォルト提供するための取り組みの紹介からスタートした。技術的課題より顧客対応等の課題が大きい点などが共有された。

最後に、「IPv6対応のmissing pieceは？ 今後の更なる発展に向けて 」と題してパネルディスカッションを実施した。コーディネーターにインテック荒野氏、パネリストに東京大学江崎教授、総務省高村氏、日本マイクロソフト田丸氏、さくらインターネット横田氏、IIJ宮崎氏の5名が登壇し、それぞれの立場から議論を展開した。企業での利用、IoTによる進展、情報教育、セキュリティや運用がIPv4/IPv6共存からIPv6シングルスタックに向かっているなど、多様な話題が取り上げられた。今後のIPv6導入における課題が明示されたイベントとなった。

世界的にIPv6の普及は順調に進んでいるが、分野によっては普及を後押しする必要がある。IPv6ディプロイメント委員会では地域サミット等により全国規模にて普及推進を図るとともに、他団体との連携を進め、IPv6の更なる発展を目指す。

（IPv6ディプロイメント委員会 委員）

ご報告

国際活動委員会活動報告

第11回 IGF速報

今年で11回目となる国連のインターネットガバナンスフォーラム（IGF）会議が、2016年12月6日～9日に、メキシコ・グアダラハラで開催された。インターネット協会の国際活動として前回に続いて参加したので、速報をレポートする。

今回のIGF会議は、国連総会にて先の10年の成果を勘案した結果、2025年までの10年間の延長が承認された後の初めての開催であり、123ヶ国、2,000名を超えるオンサイト参加者（約半数はラテンアメリカから）ならびにリモート参加者により全体で200を越えるセッション、ワークショップが開催された。

今回のIGFでは前回同様、国連の2030年ミレニアム開発目標（SDG2030）で定められている17の目標を念頭に、インターネットの活用によって持続的発展へとどう支援できるかを、政府、企業、技術コミュニティ、市民社会それぞれの立場から、インターネットガバナンスに関する様々な課題について、観点や関心の異なる関係者間で幅広い議論が集中的に実施された。

“Enabling Inclusive and Sustainable Growth” というメインテーマのもと、議論された主なテーマは、「持続的発展とインターネット」、「インターネット資源管理」、「アクセスと多様性」、「サイバーセキュリティ」、「マルチステークホルダー間の連携促進」、「インターネットと人権」、「インターネット基盤リソース」、「若者と女性を取り巻くチャレンジ」、「エマージングテーマ（将来重要性が予想される新規領域）」など多岐にわたった。「インターネット資源管理」関係では、歴史的なIANA監督権限移管の重要なマイルストーン達成にあたり、関係者の労をねぎらうとともに、その献身的な努力へ深い敬意が示された。

目新しさを感じた内容は、“Global South” という新たなスローガンのもと、新興国を取り巻くセッションが比較的多くあり、一例として開催地中南米における情勢を反映してか、特に「インターネットと人権」問題に関するテーマへ高い関心が寄せられ、深刻な人権が脅かされている実情の共有や、Googleなどによる改善保護に向けた取り組みが紹介された。普段、先進国の中でインターネット利用と発展を考える環境では触れることがない “Global South” を中心に新たに顕在化している課題を知る機会となった。

また、前回からプログラムに導入されたBPF（Best Practices Forum）では、毎年インターネット利用普及推進上、重要領域において重視されるテーマが選定され、事前に世界中の関心をもった関係者がオンラインで集い議論を経て取り纏められ結果、今回は、初年度からのアップデートである「IPv6」、「IXP」、「Cybersecurity」ならびに「Gender and Access」が成果文書として発表された。

前回から「エマージングテーマ」として登場したIoT関連のセッションも、SDGの17目標中12分野においてIoTが密接に関係していることが認識されたことを背景に、人口知能やセキュリティへのアプローチなども含めて多数設けられ、世界的な関心の高まりを背景に活発な議論が見られた。

日本からは昨年比で約倍の20名の参加が見られ、事前に日本のコミュニティが主体となって企画したセッションが複数採用されたことや、日本政府がホストとなって期間中設けられたOpen forumが実施され、世界中の様々な団体や地域からの参加者とのオープンな意見交換の場が持たれたことは、IGFで常連のオーストラリアに加えて年々参加者が存在感を増す中国、インド、インドネシア等のアジアからの参加者の中で、一定の存在感が示された年であったといえるだろう。

インターネット協会からは小生が現地参加し、マルチステークホルダープロセスに関わる政府の役割を共有、議論するセッションに登壇して、日本でのプラクティスを紹介し他の登壇者（英国、レバノン、メキシコ、ケニア）の方々を交え意見交換を行った。

IGF2016成果レポートと全セッションのトランスクリプトは、IGFのWebサイトで閲覧できるので、ぜひ関心のあるテーマについて詳細を確認いただきたい。

■ IGF Website
http://www.intgovforum.org/multilingual/

（インターネット協会 副理事長 木下剛）

ご報告

迷惑メール対策委員会活動報告

ISP、携帯電話事業者などメールサービスに関わる運用者、学識経験者を含むメンバーにより構成されている迷惑メール対策委員会では、月一回程度の定例会合を開催している。主な活動内容は、迷惑メール対策に有効なDMARC（送信ドメイン認証技術の一つ）の技術内容や仕組みについての検討、送信ドメイン認証技術の普及状況の調査、DMARCの技術文書の英日訳などである。翻訳活動は、DMARCの技術規格（RFC7489）のほか、メール配信事業者・ISPのベストプラクティス（グローバルで迷惑メール対策活動を行っている組織M3AAWGの技術文書）などを対象としており、その成果をポータルサイトで掲載するなど、最新動向に関して情報発信を行っている。

普及活動や情報発信の一環として継続して活動しているイベントに「迷惑メール対策カンファンレンス」がある。平成27年度（2015年度）からはESC（Email Security Conference）と共催する形でより広い参加者を対象に、東京と大阪の両方で開催している。特に平成28年度（2016年度）はセキュリティイベント「Security Days」と同週に開催して、一週間を「Security Week」と呼ぶことで、来場者へセキュリティに関する意識付けができたと考える。また、大阪は昨年度と同じグランフロント大阪で開催したが、東京は利便性の高いJPタワーホール＆カンファレンスを開催場所としたことで、大阪の1,549名参加（昨年度比－48名）に対して東京は4,220名参加（昨年度比＋1,239名）と大幅な集客アップを達成した。

今回のカンファレンスのプログラムは、サイバーセキュリティ全般の話から始まり、最近利用者が多く迷惑メールの発信元となっているクラウドホスティング事業者の取り組みの紹介、ISPが継続して取り組んでいるSubmission踏み台問題の対策の紹介、なりすましの手口とその対策の紹介、DMARCを導入する上で発生する問題点や技術的・法的留意点の紹介、携帯事業各社が連携して取り組む対策の紹介など、幅広く話題を取り上げて多くの来場者にとって有益な情報を提供できたと考える。ちなみに、携帯事業各社の連携による対策では、迷惑メールの申告情報を発信元携帯事業社へと共有し、サービス契約約款にもとづき利用停止等の措置を講じるといった取り組みが行われている。また、カンファレンスでは、講演者から参加者への一方的な情報発信だけでなく、参加者との意見交換や議論にも時間を割き、議論を通して課題を認識し一緒に解決策を検討していくことを心掛けている。

第15回迷惑メール対策カンファレンスの会場風景

昨年度から検討しているメール関連技術（フィードバックループ、ドメインレピュテーション）については、検証を目的として大学研究機関と連携して開発したプロトタイプ（送信ドメイン認証結果をメール受信者へ表示するツール）の配信を予定している。当初は送信ドメイン認証結果を「見える化」するのみの機能だが、今後は送信ドメイン認証技術に対応しているドメイン情報を収集し、ツール利用者からもらった各ドメインに対する評価を受信側へ提供することで、メール受信時の迷惑メールの判断に役立ててもらうことを検討している。

■ 第14-15回迷惑メール対策カンファレンス
http://www.iajapan.org/anti_spam/event/2016/conf_14-15th/

■ 有害情報対策ポータルサイト －迷惑メール対策編－
http://salt.iajapan.org/wpmu/anti_spam/

（迷惑メール対策委員会 副委員長 北崎恵凡）

ご報告

IoT推進委員会 実証実験WG報告

TG1『住、職環境モニタリング実験』

IoT推進委員会 実証実験WGは、昨年実証実験テーマを広く会員から公募し、その第一号として『住、職環境モニタリング実験』を採択し、会員有志によるタスクグループTG1を構成して、この実証実験に取り組んでいます。本欄では、その内容をご紹介します。

『住、職環境モニタリング実験』の目的

本実験では、以下の二点を目標として、具体的な計画の立案、実行が行われています。

1. IoTセンサーデバイスを用いた、住、職環境モニタリングを行うことにより新規事業・サービスの創出につながる知見の収集、諸問題の抽出。
2. モニタリング実験を通じて、住、職環境で求められるサービスの範囲や利用条件等を検証し、住、職環境の空調・エネルギー管理、保守等のソリューションの実現を目指す。

『住、職環境モニタリング実験』の概要

本実験では、図1に示すようにオフィス環境、住環境、広域環境の三つの領域で、IoTデバイスからのデータを収集し、可視化・分析などを行い、環境改善や保守へのフィードバックを行い、結果としてより快適な住、職環境が実現されることを目指しています。

オフィス内環境データ収集の概要

TG1では、まずオフィス内環境データの収集に取り組み、2016年7月に中間報告をまとめました。その概要を解説します。

実験では、二ヶ所の異なる規模の実オフィス環境に、温度、湿度、気圧、照度、紫外線、CO_2、人位置、電流というセンサーを合計29台配置し、データの収集を行いました。

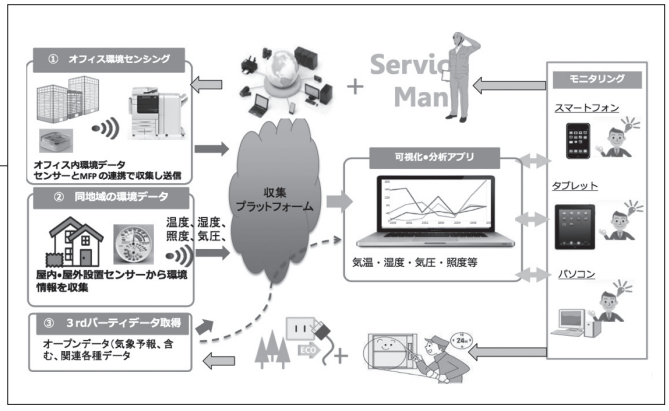


図1　実験全体の概要

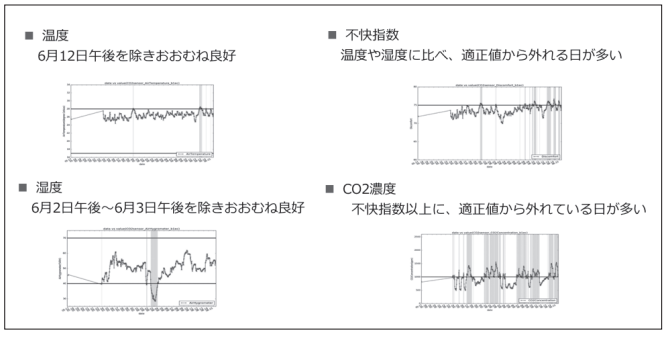


図2　可視化された環境データ

この実験の特徴の一つとして、各種センサーからの情報をインターネットに接続するにあたり、複合機を情報接続のゲートウェイとして利用している点があります。IoT機器の課題の一つとして、ネット接続に伴うセキュリティ対策があります。そこで、今回の試みでは複合機をIoT機器とのゲートウェイとすることで、既存の社内情報システムから独立したデータ収集を実現しています。

実験の結果

これらの実験により収集されたデータは、会員提供の可視化システムにより、その特徴抽出を判りやすく行えることが示されました（図2）。

TG1では、今後、引き続き住環境でのデータ収集などを推進していく予定です。

（IoT推進委員会 実証実験WG 宮宅勇矢）

ご報告

中欧IoT視察団報告

イノベーションによる経済成長が顕著な中欧地域のIoT戦略とベスト･プラクティスを学ぶべく、視察団を組織し、2016年10月に実施した。概要を以下に報告する。

1. 訪問先と活動概要

■ ミュンヘン（ドイツ）
10月16日～18日

① フラウンホーファー研究機構（FhG）

ドイツに67の研究所を有する欧州最大の応用科学研究機関。政府系ながら委託研究による外部資金が70%（うち50%は中小企業から）、GDP成長に大きく貢献。スタッフ23,000人、年間予算総額は20億ユーロ（約2,400億円）超。この資金獲得手法「フラウンホーファーモデル」は、IoT時代にふさわしい。

② ナビビズ（NavVis）

「世界中の室内3次元空間データをデジタル化する」企業。カメラと赤外線レーザーを組み合わせた移動機で室内を計測。新たな顧客体験を創出。ミュンヘン工科大学発の世界を狙うベンチャー。

③ アリアンツ・アレーナ（Allianz Arena）

世界最強のサッカークラブの一つ、バイエルン・ミュンヘンのホームグラウンド。センサーを活用し、人工太陽で天然芝をケア。今後は、75,000人の観客向けに5Gによる同時接続可能な移動通信システムの実現が期待される。

④ ブラギ（BRAGI）

「イヤラブル・コンピューティング」ベンチャー。高音質ワイレス・ヘッドセットにセンサーを搭載し、視界を遮らない、常時装着・認証型の新しいUX（ユーザー・エクスペリエンス）とプラットフォーム・サービスを目指している。

■ ブダペスト（ハンガリー）
10月18日～20日

① ハンガリーICT協会（IVSZ）

ハンガリー唯一の情報通信業界団体。約500社が加盟。課題は、デジタル人材育成。初等中等教育では、全教科にITを組み込んだカリキュラムを導入予定。

② 3社意見交換会

それぞれの分野で先端を走る、モバイル決済のCellum、人事管理ソフトウェア企業JC360、レコメンデーション・エンジンのGravity各社トップとディスカッション。

③ 各社事業紹介と交流

MOHAnet：センサーによるリモート監視サービス、AITIA：受託ソフト開発、aiSS：小売業IT支援、ITWare：アプリ開発ツールおよびクラウドプラットフォーム、Commsignia：V2X（Vehicle to X）開発、Stylers：モバイルアプリ

■ ウィーン、リンツ、コラーシュラグ（オーストリア）
10月20日～22日

① ウィーン市内アスペルン湖岸都市
スマートシティ・プロジェクト

2004年プロジェクト発足、2030年完成予定。現在の人口6,000人から25,000人の居住者と25,000人の就労者を実現予定。面積：240万㎡。ソフト・モビリティというコンセプト（公共交通に200～300mでアクセス可能）。環境インパクトに配慮。公的基金からの部分的財務援助によって、低所得者でも50㎡前後の良質な住宅に5万円程度の家賃で入居可能。スマートシティとは、あらゆる階層の人々にとって住み易い街（低所得者も高所得者も隣接して住める街）と定義している。

② オーストリア政府・デジタルオーストリア・リンツ市
商工会議所（WKO）

リンツ市周辺地域には、Industorie4.0に関連した企業が88社存在し、現在554件の特許が出願されており、この数はウィーン地区よりも多いとのこと。ここを中心にICT（主としてソフト

ウェア）産業が、観光産業の6倍に成長。

③ アルスエレクトロニカ（Ars Electronica）
リンツ市の保有する世界トップレベルのデジタルアートの研究機関および展示センター。マルチ8Kプロジェクターによる3次元映像や、世界中の企業との共同開発が印象的。

④ ロクソン（LOXONE）
リンツ市からクルマで約1時間余りの人口1,000人の村コラーシュラグで2009年に創業した、スマートホーム・ソリューション企業。地方創生に燃え、約100名が働く（全世界で250名）。

2. 視察所感と今後の展望

ドイツ、オーストリア、ハンガリー等の中欧地域は、Industrie 4.0を提唱しているドイツをはじめ、ギルドなど職人組合の歴史があり、専門技術に特化した中小企業が多く活躍している。このため、企業間取引は、対等型の「水平分業型関係」を形成しており、インターネットを導入するのに相応しい「水平型協調構造」となっている。「フラウンホーファーモデル」もこうした構造を支え、イノベーションの実現に寄与している状況が実感できた。特に中小企業の意欲的な取り組みが印象的であった。今回得た知見を活かすためにも、継続的な交流を実施していきたい。

2017年3月にドイツ・ハノーバーで開催されるCeBITは、世界最大のIT見本市であり、特に、パートナー・カントリーが日本ということで、積極的な参加を予定している。こうした機会を含め、今後とも、中欧地域との関係をさらに深め、新たなグローバルIoTビジネスを創出していきたいとの念を強く持った。

最後に、今回の視察には、ドイツ、ハンガリー、オーストリア各国政府・大使館の多大なる協力をいただいたことを深謝いたします。

（中欧交流委員会　委員　宮宅勇矢）

ミュンヘン工科大学屋上にて、NavVis社メンバーと

ブダペストーのレストランで現地企業トップと懇談

リンツ商工会議所で議論

ご報告

インターネットを利用する際に、知っておきたい『その時の場面集』に「Facebook編」を追加

インターネット協会では、主要なインターネットサービスについて、その利用方法や注意点、トラブルへの対処法などをまとめた『その時の場面集』を作成･公開している。今回、新たに「Facebook編」を追加し、2017年2月より公開している。

http://www.iajapan.org/bamen/

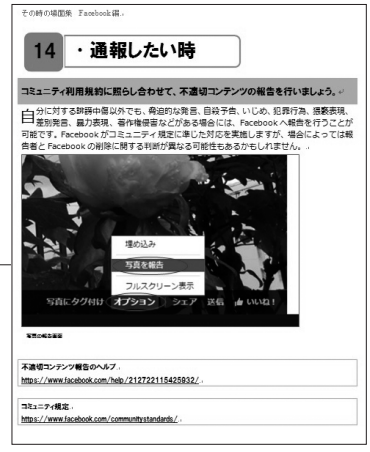
作成の背景

Facebookの大きな特徴は、他のSNSと違い「実名制度」を取っている点であり、ニックネームなどで利用することが出来ない。またサービス内容が多機能である反面、プロフィール情報や投稿内容の公開範囲を適切に設定しないと、SNS内に留まらず現実生活においても思わぬトラブルを招く可能性がある。

インターネット協会は、インターネットの使い方や注意方法などの質問を受けてアドバイスをしているが、最近は、SNSの使い方を知りたいという要望を受けるようになった。Facebookは成人以上の利用者が多いことから、比較的トラブルは少なかったが、ここ1年の間に初心者利用のトラブルが起きていることを把握し、作成することとなった。

『Facebook 編』の内容

Facebookを初めて利用する、または利用し始めたばかりでまだ慣れていない人に対し、Facebook上でのプライバシーを適切に自分でコントロール出来るよう、主にプロフィールや投稿の公開範囲設定について説明をする。特に知ってほしいのは、共有範囲の設定をする場面だ。共有範囲の選択肢には主に［公開］［友達］［自分のみ］［カスタム］の4つがあり、それぞれで基本データ項目や投稿を見られる人の範囲が異なる。基本データ項目や投稿内容を［公開］に設定した場合、自分の個人情報やプライバシーが不特定多数のFacebook利用者から閲覧されることになる。初心者に向けては、基本的に共有範囲の設定は［友達］としておくことをお勧めしている。さらに、2016年12月には、Facebookの「Family Safety Center」で、ネットいじめ防止対策の情報が追加されたため、その内容も盛り込んでいる。



Facebook 編「通報したい時」より

『Facebook 編』の目次

1. Facebookの概要
2. 登録可能な年齢
3. アカウントを登録したい時
4. 基本データの登録・編集をしたい時
5. アカウント情報の登録・編集をしたい時
6. 共有範囲の設定をしたい時
7. 検索エンジンからのリンクを許可したくない時
8. タグ付けの設定をしたい時
9. 友達関係の設定をしたい時
10. 自分の投稿等を削除したい時
11. 登録メールアドレス・パスワードを忘れた時
12. 特定ユーザーをブロックしたい時
13. 誹謗中傷などを受けた時
14. 通報したい時
15. 連携アプリ設定を確認したい時
16. アカウントを利用解除・削除したい時
17. 不正アクセスされた時
18. 利用停止になった時
19. 利用規約を確認したい時
20. 問い合わせをしたい時

既存場面集の更新（バックアップをとる）

その他の場面集でも更新を行っている。具体的には、スマホを水没させてしまった、機種変更をしたらLINEのメッセージが消えてしまった、といったような後悔をしないように「バックアップをとる」の項目を以下の場面集に追加した。

■ スマートフォン基本設定編［iPhone］
■ スマートフォン基本設定編［Androidスマートフォン］
■ LINE編

これからも、インターネット利用者の要望を聞きながら、適宜、内容を更新する予定である。

法人賛助会員

あ〜お

一般社団法人iOSコンソーシアム
株式会社アサツーディ・ケイ
株式会社朝日ネット
株式会社アズジェント
アラクサラネットワークス株式会社
アルテリア・ネットワークス株式会社
アルプスシステムインテグレーション株式会社
EMCジャパン株式会社
イッツ・コミュニケーションズ株式会社
一般社団法人インダストリアル・バリューチェーン・イニシアティブ
株式会社インターネットイニシアティブ(IIJ)
株式会社インターネット総合研究所
インターネットマルチフィード株式会社
株式会社インテック
インフォコム株式会社
株式会社インプレスホールディングス
株式会社上田ケーブルビジョン
NTTコミュニケーションズ株式会社
株式会社NTTPCコミュニケーションズ
株式会社NTTファシリティーズ
エブリセンスジャパン株式会社
株式会社大塚商会
株式会社オービックビジネスコンサルタント
株式会社オレンジソフト

か〜こ

かもめエンジニアリング株式会社
株式会社クオリティア
グーグル株式会社
Global Mobility Service株式会社
KCCSモバイルエンジニアリング株式会社
KDDI株式会社
国際大学グローバル・コミュニケーション・センター
一般社団法人コンピュータソフトウェア協会

さ〜そ

サイバーコンシェルジュ株式会社
株式会社産業革新機構
株式会社Jストリーム
株式会社ジェーエムエーシステムズ
GMOインターネット株式会社
シスコシステムズ合同会社
特定非営利活動法人市民コンピュータコミュニケーション研究会
ジャパンケーブルキャスト株式会社
一般社団法人重要生活機器連携セキュリティ協議会
一般財団法人生産技術研究奨励会 RC-88 IoT特別研究会
一般社団法人セキュリティ対策推進協議会
ソニーネットワークコミュニケーションズ株式会社
ソフトバンク株式会社
株式会社ソリトンシステムズ

た〜と

高砂熱学工業株式会社
株式会社ディアイティ
株式会社DTS
デジタルアーツ株式会社
鉄道情報システム株式会社
東京ガスiネット株式会社
東芝ソリューション株式会社
トレンドマイクロ株式会社
トロンフォーラム

な〜の

株式会社ナノオプト・メディア
日本アンテナ株式会社
日本インターネットエクスチェンジ株式会社
一般社団法人日本インターネットプロバイダー協会
株式会社日本経済新聞社
一般財団法人日本情報経済社会推進協会
一般社団法人日本スマートフォンセキュリティ協会
日本電気株式会社(NEC)
日本マイクロソフト株式会社
株式会社日本レジストリサービス

は〜ほ

株式会社PFU
BizMobile株式会社
株式会社日立インフォメーションアカデミー
株式会社日立システムズ
株式会社日立製作所
ビッグローブ株式会社
ピットクルー株式会社
フォーティネットジャパン株式会社
富士ゼロックス株式会社
富士通株式会社
フリービット株式会社
株式会社ブロードバンドタワー

ま〜も

マクニカネットワークス株式会社
株式会社三菱総合研究所
三菱電機インフォメーションネットワーク株式会社

や〜よ

ヤンマー株式会社中央研究所

ら〜ろ

LINE株式会社
株式会社リコー

2016年12月5日現在　83社　50音順

当協会では、賛助会員を募集いたしております

■ 法人賛助会員の特典

・会員無料セミナーへの参加、優待価格での参加。
・イベント出展時の割引価格適用。
・当協会後援・協賛イベント等の無料招待券・割引券の配布。
・当協会機関誌 IAjapan Review（年２回発行）の配布。
・メーリングリストによる情報の提供。

■ ご入会申込み

法人賛助会員をご希望される企業の方は、お申込書をWeb上からダウンロードのうえ、ご記入・ご捺印後、郵送をお願いいたします。

URL *http://www.iajapan.org/join.html*

■ 入会審査

賛助会員の入会審査の手続きに1週間程かかりますので、お含みおきください。

※ 入会および当協会に関する詳細は、Web上にてご確認ください。

URL *http://www.iajapan.org/*

IAjapan Review
2017年2月1日発行

発行■一般財団法人インターネット協会
〒113-0034
東京都文京区湯島2-21-1
長谷川ビル3階
TEL：03-5844-6840　FAX：03-5844-6845
お問い合わせ：http://www.iajapan.org/reference.html
WWW：http://www.iajapan.org/

編集■株式会社インプレス
〒101-0051 東京都千代田区神田神保町1-105
神保町三井ビルディング

印刷■株式会社技秀堂

IAjapan Review
Vol.16 No.2
Internet Association Japan Review / February 2017
一般財団法人インターネット協会レビュー
価格1,000円(税込)

IAjapan Review 2017年2月1日発行
発　行■一般財団法人インターネット協会　〒113-0034 東京都文京区湯島2-21-1 長谷川ビル3階　TEL：03-5844-6840　FAX：03-5844-6845　お問い合わせ：https://www.iajapan.org/reference.html
編　集■株式会社インプレス　東京都千代田区神田神保町1-105 神保町三井ビルディング