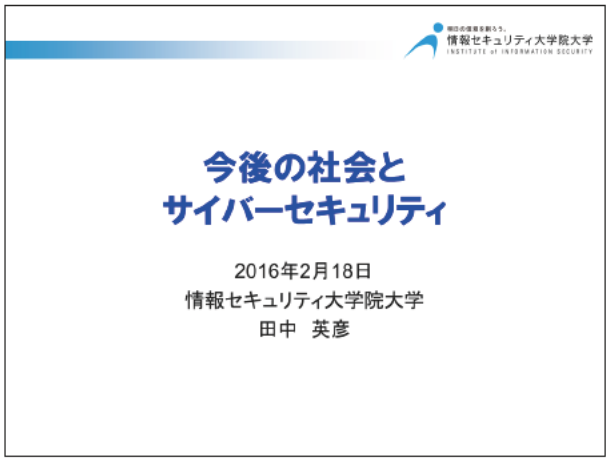
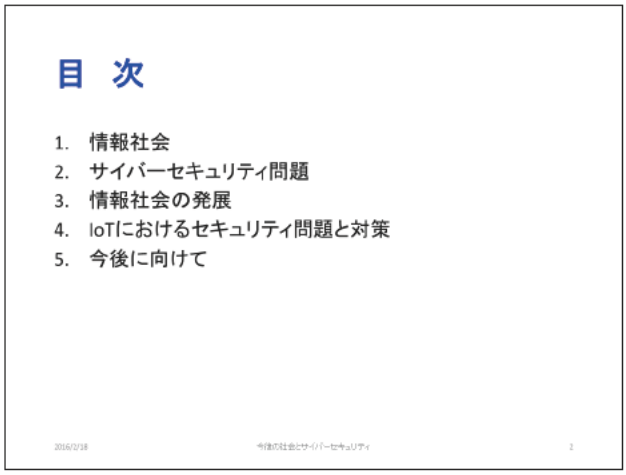
今後の社会と
サイバーセキュリティ

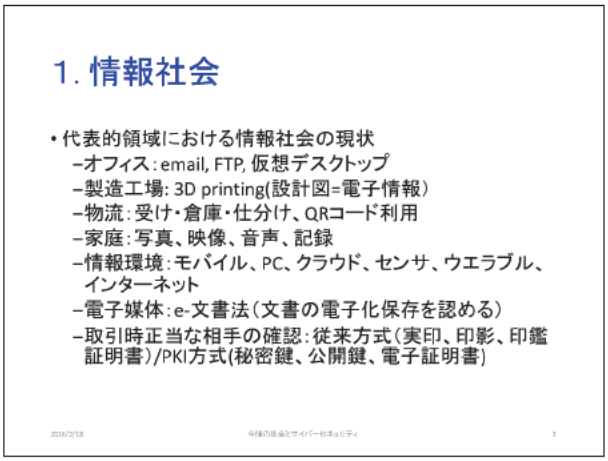
工学博士　東京大学名誉教授　IEEE Life Fellow
情報セキュリティ大学院大学 学長　田中英彦



今日は「今後の社会とサイバーセキュリティ」という題でお話したいと思います.

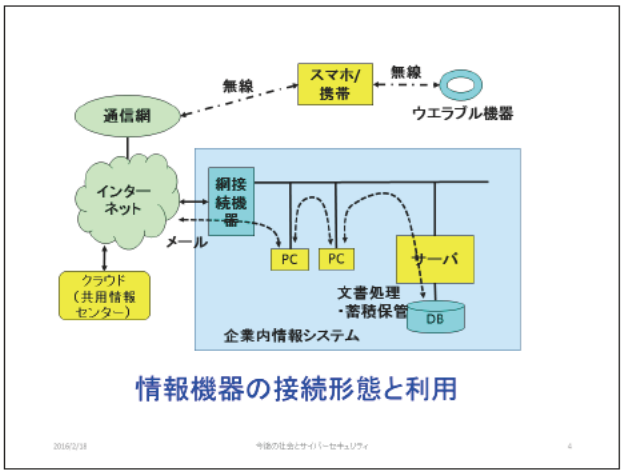


内容といたしましては、第一に、情報社会というものを振り返ってみたいと思います。第二に、サイバーセキュリティ問題について、今世の中でどうなっているのか、いろんなサンプルでご紹介したいと思います。第三に、情報化社会の発展に伴って、セキュリティ問題がますます怖くなるという点を、第四に、IoT (Internet of Tings) の新しい社会におけるセキュリティ問題と対策についてお話します。最後に、今後に向けて、高専を卒業後、専門職に就いたときの情報セキュリティキャリアイメージのサンプルをお示しします。



まず、情報社会についてです。これは、皆さんが毎日過ごしていらっしゃる社会の一例です。

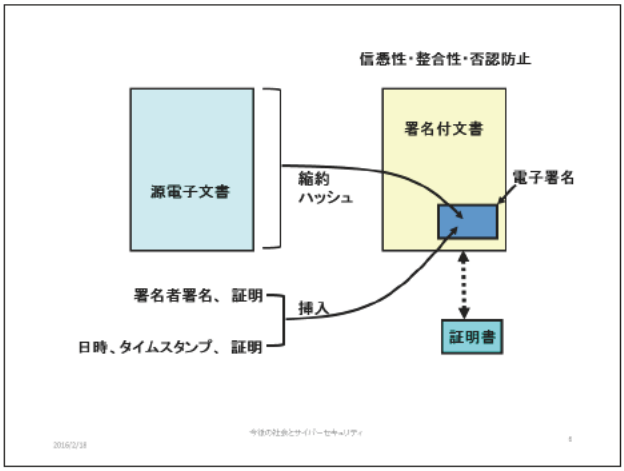
オフィス、工場、物流、家庭、情報環境、モバイル、スマホ等いろいろな情報システムを使っています。従来、紙が使われていましたが、今は書類として電子媒体が使われています。さらに、従来取引時には正当な取引相手の確認を実印等で行っていましたが、今は電子認証も使われています。



例えば、会社の中にサーバ、データベース、PC があって、仕事をしている。それらが外部にインターネットでつながれている。最近では、クラウドがあり、無線でスマホやウエアラブル電子端末があるという環境になっています。そのときに使っているのが e 文書、電子証明です。法律でこれらは有効になっています。

e文書法、電子証明

- 2005.4施行：法律で保管義務のある文書の電子化保存。紙の代わりに電子データ保存を許容
- 電子証明書方式
  - –PKI: 公開鍵基盤、送信者が電子署名、受信側は署名を確認可
  - –電子証明書の登録、電子署名法2001.4施行
- タイムスタンプの証明内容
  - –ある時刻にその文書が存在していた（存在）
  - –その文書は改竄されていない（完全性）
  - –文書への署名を否認することを防止可能（否認防止）
  - –約款、実験データ、契約書、議事録、監査記録など
  - –標準化、タイムスタンプ局が発行



電子文書に、署名と同時にタイムスタンプ局で発行されたタイムスタンプ（日時）を電子署名としてつける。それで、信憑性・整合性・否認防止ができる。こういうものを使いながらビジネスを回していくことができます。

オンラインサイトの電子証明書

- オンラインショッピング：150兆円/年
  - –オンラインにおける信頼の基盤：デジタル証明書
  - –サイバー犯罪被害額：13兆円/年（急増+50%）
  - –被害者数：3億8千万人
- 証明書の問題
  - –証明書を欺く方法の存在
  - –認証局が証明を与える:ドメイン認証DV, 企業実在性認証OV, 拡張認証EVの3種
  - –DVは、ドメイン名の使用権を示すのみで即発行。身元証明が無し。不正WebサイトSSLの78%がDV
  - –ブラウザはDV/OVの区別をしないが、httpsの鍵マーククリックで判明
  - –業界団体がEVを開発：合法的企業であり、所在地が明らかである等、身元確認と、ブラウザに検証結果を視覚的に提供（緑色のアドレスバー）

次に、お話したいのはオンラインサイトの電子証明書です。我々は、Web であちらこちらのオンラインサイトを見に行きます。見に行った時に正しいサイトか、怪しいサイトか、ある程度チェックすることができます。その時にオンラインサイトの電子証明書が使われるのですけれど、電子証明には、DV、OV、EV の 3 種類があります。DV というのは、身元証明が無く怪しい。会社が存在するかどうかも怪しい。EV は、大体大丈夫です。Web ページの上部にブルーのラインが出ます。

暗号の機能

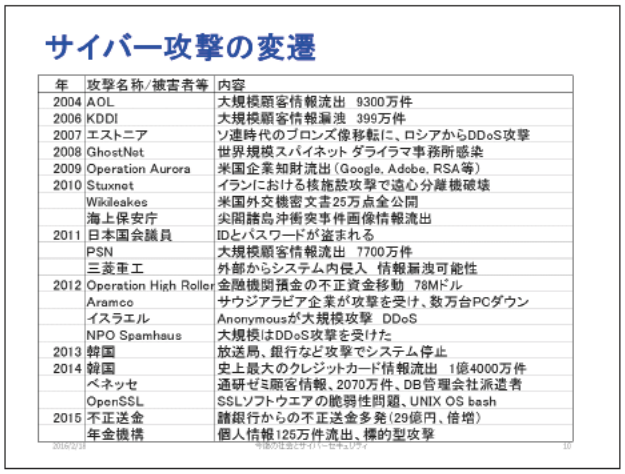
1. 機密性：confidentiality
   - 内容が漏洩しない。通常、漏洩に気がつかない。
2. 完全性：integrity
   - 改竄されない。
3. 認証：authentication
   - なりすましを防ぎ、相手が本人かどうか確認
4. 否認防止：non repudiation
   - 情報を送ったことを否認できないことを保障

暗号は、いろいろな機能を持っております。まず、第一に機密性。わからないようにして、他の人に見せない。第二に完全性。書換えられていないことがわかる。第三に認証。送信者と受信者がお互い正しい本人であることがわかる。第四に否認防止、情報を送ったことを否認できないことを保障することができます。

2. サイバーセキュリティの問題

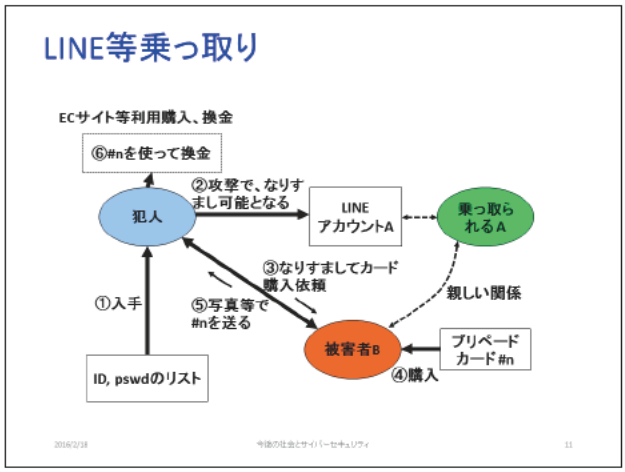
- サイバー攻撃の変遷
- トロイの木馬
- 具体被害
- 漏洩コスト・件数
- 標的型攻撃
- Webサイト攻撃
- ランサムウエア

ところが最近は、サイバーセキュリティの問題が非常に厳しい状況になっています。これを、サンプルを使いながらご紹介いたします。

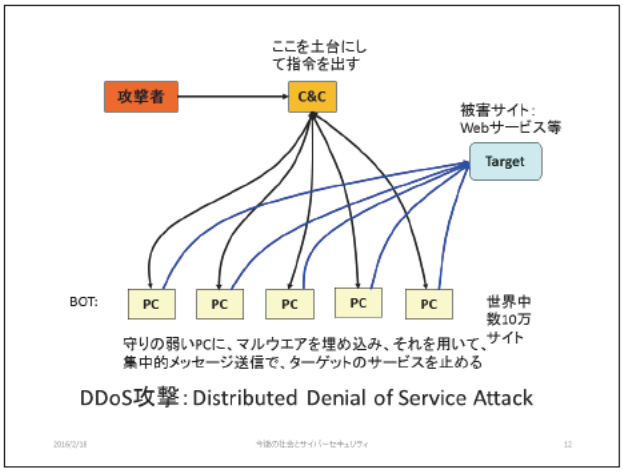


サイバー攻撃といわれるものがいろいろあるのですが、これは 2004 年から 2015 年までリストアップしたものです。

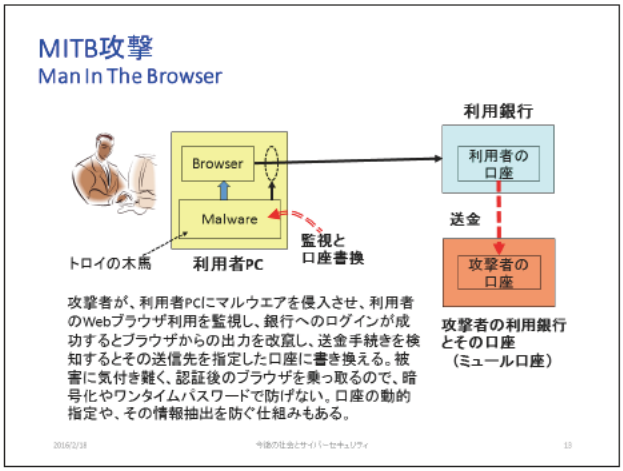
2004 年アメリカンオンライン (AOL) が攻撃され、1 億件近い情報が漏洩しました。2006 年 KDDI が攻撃されました。2007 年エストニアの問題、ロシアから DDoS 攻撃 (Distributed Denial of Service Attack) を受けました。2009 年に Google も攻撃されました。2010 年 Stuxnet によるイランの核施設攻撃で遠心分離機破壊。これは有名な話です。Wikileakes、米国外交機密文書を漏出しました。これには日本の情報も入っていました。日本の海上保安庁や国会議員の問題、三菱重工への攻撃等。2013 年には、北朝鮮からの攻撃で韓国の銀行や放送局がシステム停止。2014 年にベネッセ顧客情報漏出が外部機関からわかりました。2015 年不正送金が多く発生しました。昨年 5 月には年金機構問題、センシティブな個人情報が流出しました。



これは、一昨年、LINE 等の乗っ取りで問題になった例です。犯人がネットの中で ID、パスワードリストを取得し、A さんのアカウントを使うわけです。なりすましをして、B さんに対して LINE でカード購入依頼情報を送る。例えば、「お金の手持ちが無いのでこのプリペイドカード買ってよ。」と送ります。B さんは信用して、購入し、その情報を犯人に送ってしまう。それを受けた犯人は、お金に換えて逃げる。このような LINE の乗っ取りがたくさん横行しました。



DDoS 攻撃というのも有名な攻撃の一つです。世界にあるネットワークに繋がれたたくさんの PC (PC は新しいものだけではなく古い PC がたくさんあります。) の中の一つを土台として指令を出す。そこから、悪いプログラムを送りつける。ある時、一斉に指示を出して、ターゲットの Web サービスに同時にアクセスする。余りにも多くのアクセスが集中するので、このターゲットのサイトは使えなくなります。こういったベースになる PC のことを BOT といいます。ROBOT の RO をとったものです。世界中の何十万という BOT を使ってターゲットの Web サービスを攻撃します。



これは、不正送金に使われる形です。誰かの口座にブラウザを使って、ある人が送金しようとします。その時、利用者の PC の中に知らない間にマルウエアが侵入されているとします。利用者がブラウザを使って、送金する瞬間に送金のあて先だけが書換えられてしまいます。銀行は正しいメッセージだと思って送金する。銀行も悪いことをした認識がなく、送金者も間違っていると思わない。こんな攻撃が起こっています。

具体被害

	被攻撃サイト	攻撃種類	被害
2013/3	通販サイト	Apache Struts2	個人情報漏洩
2013/5	レンタルサービス	SQLインジェクション	クレジットカード漏洩
2013/7	ポータルサイト	パスワードリスト	なりすまし個人情報
2014/1	オンライン銀行	フィッシング詐欺	ID, PSWD漏洩
2014/2	書籍購入サイト	ドライブバイダウンロード	ユーザがマルウエア感染

平均漏洩件数	604, 826	2012年シマンテック報告
損賠賠償額	7500万円	JNSA報告書
調査費用, 再構築費用	5000万～1億円	IPA被害調査
ブランド毀損	売上額の5%～40%	事例から

データ侵害の平均コスト：4.2億円、企業の9割は脅威侵入済み、7割は被害経験、侵入から発見まで242日

2016/2/18　今後の社会とサイバーセキュリティ　14

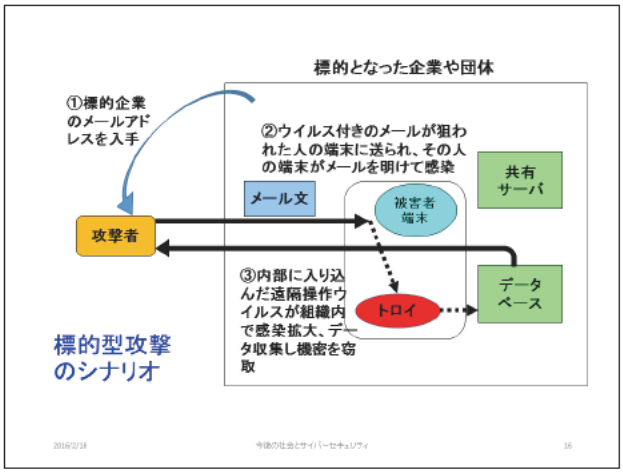
具体的な被害としては、賠償金額の平均が 7,500 万円、システムの修正費に数千万円かかります。また、ブランドが毀損する。回復するのに、売上額の何割も費用がかかる。また、半年も以上も前から侵入され情報が取られていることが多いのが現状です。

標的型攻撃

- 60%が中小企業を対象
  - 中小企業は、対策に多くの資源投資が困難
  - 大企業の6社に5社が攻撃の標的
- 攻撃手法
  - メールに添付ファイル、その実行でマルウエアロード
  - 企業の使うソフトウエアを識別、その更新プログラム内部にマルウエアを隠し、ダウンロードを待つ
  - 未知の攻撃やSSL/TLS利用でチェック困難
- 対策：完全防御は困難、事後策
  - 体制整備、情報収集と共有、実装（抑止策、被害拡大の防御策、被害発生検知策）、ダメージ制御と被害対処の備え、復旧手段確保、継続的対策に向けた実施評価と予算措置、人の教育

2016/2/18　今後の社会とサイバーセキュリティ　15

このようなものを標的型攻撃といいます。ターゲットとなる会社の情報を調べて、攻撃する。お金を持っているのは大企業です。大企業を攻撃するには、関連の深い中小企業をまず攻撃する。中小企業は防衛していないことが多いからです。攻撃しやすい中小企業を攻める。そこから大企業の情報を仕入れるという手順をとります。



例えば、ある企業の中に PC 端末、データベース、サーバがある。この企業の情報を外部の攻撃者が入手して、メールの内容を少し変えて送る。添付ファイルの中にウイルスをつけておく。部下が上司から送られて来たメールだと思って、その添付ファイルを開ける。すると、ウイルスに感染する。皆が確実に開けないということは無い。社内に流通しているメールそのものですから、必ず誰かが開けてしまうわけです。

年月	報道された標的型攻撃
2009/11	世界のエネルギ関連企業や製薬会社
2010/1	Googleなど米国企業
2010/6	イラン核燃料施設
2011/4	ソニーへの攻撃で個人情報が流出
2011/9	三菱重工
2011/10	衆議院の議員のパスワード流出
2012/5	原子力安全基準機構で情報流出
2012/7	財務省で情報流出
2012/11	三菱重工でウイルス感染
2013/1	農林水産省からTPPなど機密情報流出
2013/2	外務省ネットから情報流出
2013/5	Yahoo JAPANから2200万件のIDや148万件のPSWDが流出可能性
2014/1	高速増殖炉もんじゅ、国立がんセンターで不正プログラム実行
2014/2	はとバスにIEのゼロデイ攻撃
2014/8	日本のISP, 大学などに水のみ場攻撃
2015/6	日本年金機構で125万件個人情報流出
2015.6	米国で政府職員情報2210万人分が流出, 国家や 産業の機密窃取

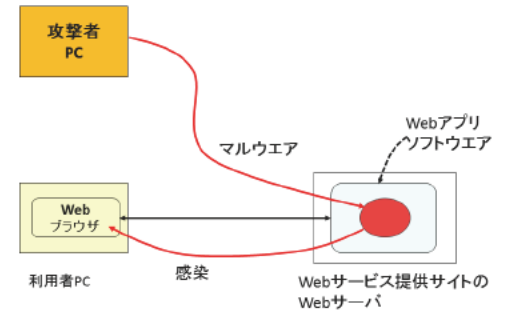
2016/2/18　今後の社会とサイバーセキュリティ　17

このリストが、標的型攻撃の例です。はとバス等も攻撃されました。昨年の 6 月米国で政府職員の 2210 万人のデータが流出しました。米国の対策費予算は 190 億ドル、日本円にして、2 兆円です。

Webサイト攻撃

- Webアプリケーション脆弱性狙い
  - 2014年、78%のウエッブサイトは脆弱性を抱える
  - 内16%が重大脆弱性
- 各所にある脆弱性
  - Webサーバ、Webアプリ、DB、メール、net、遠隔アクセス、通信、OS、等
- 影響の大きな脆弱性（2015　3/4サイト未だ残存）
  - OpenSSL, GNU bash, SSL version3.0
- 水のみ場攻撃
  - 正規サイトを侵害、サイト訪問者を監視し標的企業だけを狙う

約 8 割もの Web サイトが脆弱性を抱えています。それを突かれると、簡単にマルウエアを Web サイトに蓄え込むことになります。



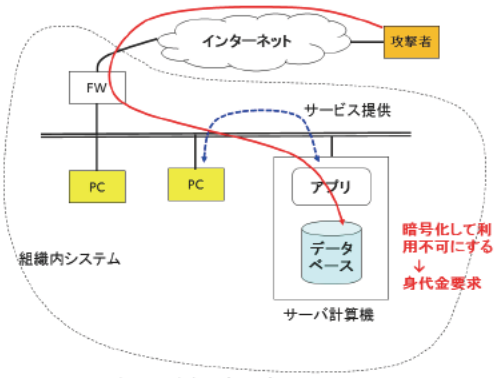
Webサイトに対する汚染攻撃とその影響伝播

Web サイトにアプリソフトウエアがあり、攻撃者はマルウエアを仕込みます。仕込めなくすることはできますが、多くのサイトがそれをしていないのです。利用者は Web を見たときに簡単マルウエアに感染してしまいます。

ランサムウエアの増加

- 裕福な国のユーザを対象とした身代金強要
  - ユーザは身代金を支払う傾向がある（欧米）
  - 日本でも急速に拡大中（2015.7）、届出件数(2015 111件、IPA)
- 詐欺メール
  - その国の言語で、その国の実在企業からのメールを装う。
  - 郵便局や電話会社から住所変更/確認、郵便物の再送先の入力を依頼する
- 強力なランサムウエアの出現
  - 仮想通貨の利用、Torネットの利用、モバイルへの移行（Androidのデータを暗号化するランサムウエア）、大規模ストレージへの攻撃
  - NASサーバのパッチ未使用の脆弱性を攻撃、強力暗号化でサーバ上全データ暗号化、楕円暗号利用
- 対策
  - データバックアップ、セキュリティ意識を高め、Torアプリをブロックする、スパム対策、一時フォルダから実行ファイルの実行を阻止

ランサムウエアが問題になっています。いわゆる身代金です。



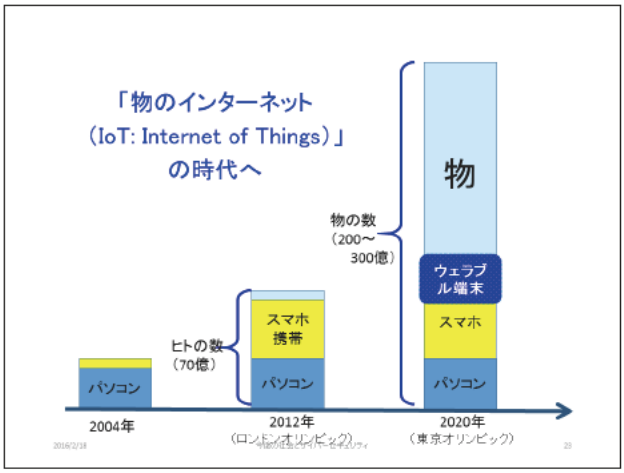
ランサムウエア攻撃（身代金）

点線の中が会社や組織です。例えば、病院としましょう。病院には患者さんのデータベースがあります。攻撃者がインターネットを通じて、侵入してデータベースを勝手に暗号化してしまう。そして、身代金を要求する。使えなくなると困るから、解除してもらうために身代金を払う。昨年の夏から日本で多くなってきました。

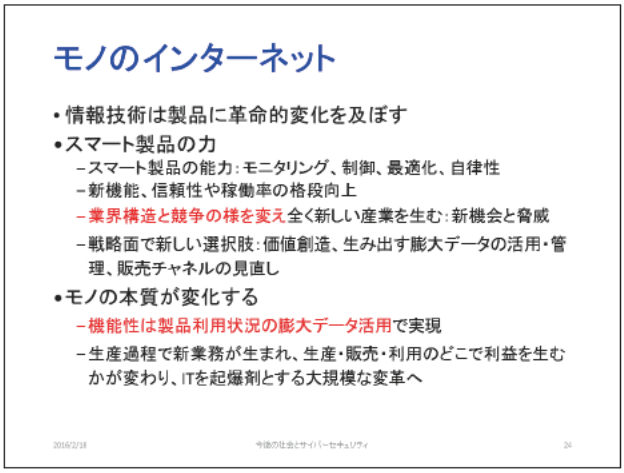
3. 情報社会の発展

- あらゆるモノが繋がる
  - –IoT: 繋がるデバイス数、市・インフラ・ビル・交通・工場・医療福祉・生活
  - –機器が電子化されネット接続：サービス、更新、ウエラブル
- ビッグデータの活用
  - –効率化、マーケティング、便利、攻撃データの共用
- 人工知能の発達：deep learning
  - –画像認識、最適化
- 社会トレンド
  - –個中心、所有から利用へ、連携、物理と論理の融合

さて、これからどうなるか、情報化社会が発展してきます。IoT であらゆるものがネットに繋がる。センサなどがすべて繋がってくる。あちらこちらのセンサから集められた大量データの活用が始まります。人工知能の発展、deep learning が進んできます。昨年はコンピュータ囲碁にプロ棋士が負けました。

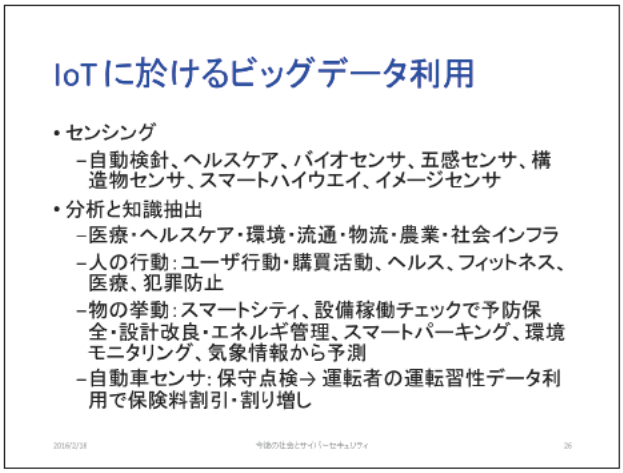


これは、ネットに繋がる端末の数です。パソコンやスマホの台数は何十億です。2020 年は東京オリンピックが開催されます。ネットに繋がるセンサや様々な機器、すべての物が繋がる。ウエアラブル端末も繋がる。何百億と増える。こういうのをモノのインターネットと言います。

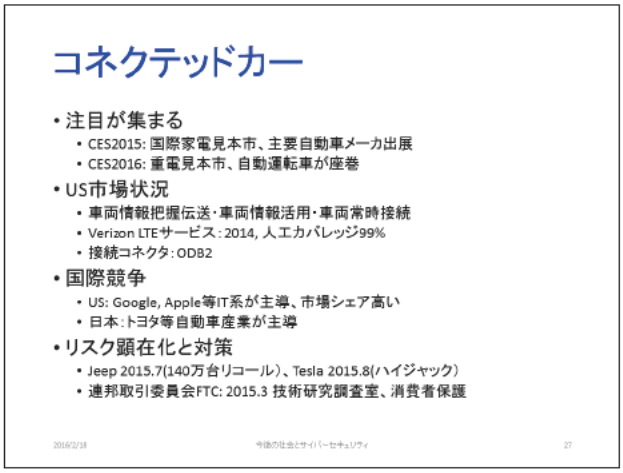


これまで、企業が情報を集めて、製品を作ってきましたが、SNS で直接ユーザの情報を集めて、製品化していく様な時代となります。機能性を変えることで、儲かったり儲からなかったりする。組み込みシステムソフトウエアの開発費は増大しています。携帯電話は 500 万行のプログラム、車のシステムでは 1000 万行、自動車のコストの 4 割が電子部品ソフトウエアです。カーナビも 500 万行のプログラムです。

IoT では、センシングが要です。センサのネットワークとなります。あちらこちらにセンサがある。テレビや部屋の中の照明、各家庭の電力計などにセンサがあります。東京電力が電力メータにセンサをつけています。社会では、人にセンサをつけて行動を把握できます。購買活動もセンシングできます。物の挙動などにセンサをつけています。工場でも、例えばタイの工場にセンサをつけて、東京で制御することが可能となります。



自動車に様々なセンサをつけます。事故や故障予防センシングなどはよくある利用事例です。しかしながら、取得したデータを基に、この人は事故を起こしやすいという情報を保険会社に売ることが出来ます。運転者の運転習性データを利用して、保険料の割引料を決める様なことが可能になっています。



CES2015 は家電見本市だったのですが、車のメーカが出展し始めました。CES2016 は自動運転車が席巻しました。車両の情報を集め、Google などが主導していますし、日本では、トヨタ自動車等が主導しています。しかし、リスクも顕在化して、Jeep がサイバー攻撃に弱いということで、2015 年 7 月 140 万台リコールとなりました。また、Tesla の電気自動車が 2015 年 8 月カージャック可能なことがわかりました。

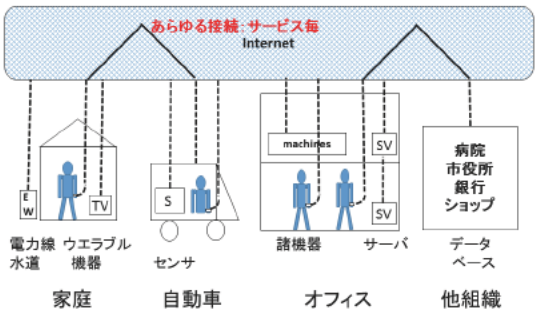
IoTによるシステムの変化

- センサ利用によるオンラインデータ収集と管理・制御・保守
  - スマート機器、遠隔最適保守、農業自動化
- サブシステム毎の情報化
  - 生産・保守・販売・気象予測・経営・市場情報　システム
- サブシステム連携による複合システム
  - 生産・販売・保守・部品供給、農業生産最適制御・気象・農業管理・農業機械・販売
- 複合システムの連携
  - 農業システムと穀物価格情報システム、健康システムと医療システム、スマートホーム（照明・空調・娯楽・セキュリティ）、EV共有システム、スマートシティ

2016/2/18　今後の社会とサイバーセキュリティ　28

こういう IoT が進展すると、システムがどう変わるか。センサによって、データを集めるサブシステムが電子化されていき、スマート機器になります。それぞれのサブシステムが連携して、複合システムになります。複合システムが連携して、スマートシティを構成します。生産・販売・保守・供給が一体化します。農業システム等も複合システムとなります。

繋がる社会イメージ：今後



2016/2/18　今後の社会とサイバーセキュリティ　29

例えば、家でテレビ、車、会社のサーバ、病院、これらがネットワークで繋がります。従来のネットワークは決められた繋がり方でしたが、今後は、決められた繋がりではなく、あらゆる接続が可能となります。ものすごい変化です。

4. IoTのセキュリティ問題と対策

- 端末当たり平均25の脆弱性
  - 暗号化しない通信、デバイスの単純なパスワード
  - デバイスインタフェース脆弱性
- あらゆるものが攻撃対象
  - 埋め込み型医療機器、アイロンからスパム攻撃チップ
  - ネットカメラの脆弱性で盗撮、道路信号システムの脆弱性
  - ATSC規格の脆弱性で対応スマートTVに問題
  - GAOは航空機が不正アクセスで制御される可能性警告2015
  - スマホを使ってBMW車のドアロックやエアコン操作
- 技術領域が多岐にわたりセキュリティ担保が困難
  - 必要な/実装されている　セキュリティレベルが異なる
- IoTは急速に進展

2016/2/18　今後の社会とサイバーセキュリティ　30

そこで、問題点と対策を見てみましょう。端末当り平均 25 の脆弱性があります。端末というのは電子化冷蔵庫、空調器、自動車等です。脆弱性とは、外からマルウエアが自動的に入ってくるという弱点のことです。あらゆるものが攻撃対象となります。アイロンからスパム攻撃チップ発見ということがありました。2015 年、米国の政府機関(GAO)が、航空機が不正アクセスで制御されることを警告しました。航空機は、飛んでいる最中に自分で電波を出しています。GPS の位置情報をあちらこちらに発信しています。それを地上で受けて、管制をしています。ところが、通信方式 ADS-B は、何のチェックもしていない。単にたれ流しをしている。暗号化もしていない。認証もしていない。それを使うと簡単に攻撃することが出来ます。私のところでもシミュレーションしました。秋葉原から部品を買ってきて、攻撃用のマシンを作る。実際に流れている電波を受信して変換すると写っている航空機の位置を簡単にずらすことが出来ます。非常に怖いことです。

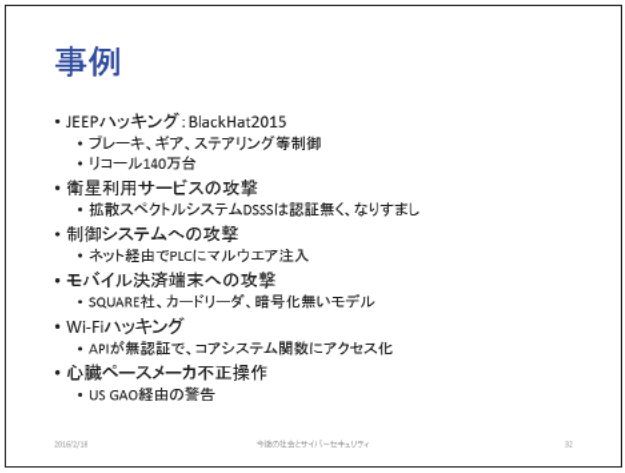
新しい事象

- サイバー攻撃が増加：情報システムへの外部攻撃
  - 特定標的へ意図的組織的攻撃：Hactivism
  - 国家の関与：国家安全保障
- 攻撃対象が、情報システムから制御系システムへ拡大、電力網攻撃は21世紀の最大脅威（米）
  - イランのウラン濃縮設備へUSB経由の複合的マルウエアが侵入し遠心分離機破壊2010
  - 重要インフラを狙う攻撃：標的型攻撃の主要目標
- スマートフォン等増加に伴う新たな脅威の発生
  - スマホ、情報家電、センサー機器：PCと同じく世界共通のOSやソフトが利用され、影響範囲大

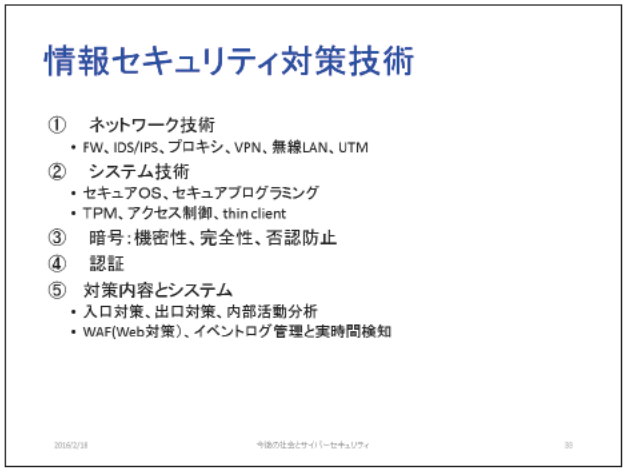
2016/2/18　今後の社会とサイバーセキュリティ　31

新しい事象としては、サイバー攻撃の増加があります。特定標的への意図的組織的攻撃は、思想信条で起こります。誰々がこういう意見を持っているということで、攻撃が起こります。例えば、日本はイルカの猟をやっている。成田空港でイルカの製品を売っているということで、保護団体から攻められました。国家の関与があります。ある国では、専門的にサイバー攻撃を実行するグループが 15 ぐらいあります。丸腰であったら攻撃されっぱなしの状態です。攻撃対象も従来であれば情報システムや PC だったのが、制御システムへと拡大してきました。先ほど述べた Stuxnet のイランの核施設への攻撃や電力網への攻撃となってきました。アメリカでは、21 世紀の最大の脅威は、電力網の攻撃であると言われています。大規模な電力網は、相互に接続されています。一箇所に何かが起こっても波及しないようにしています。しかし、大規模な停電をネットワ

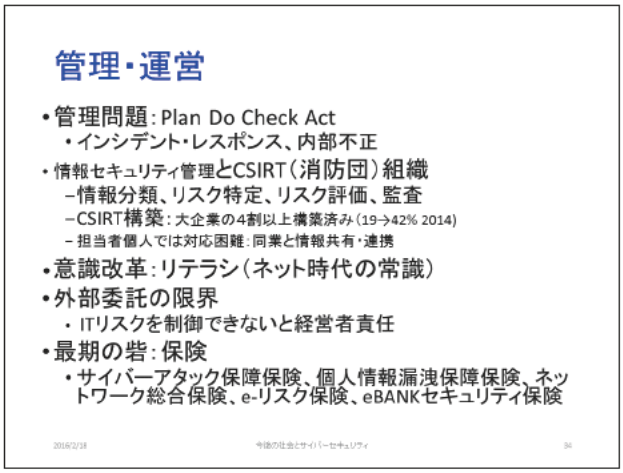
ークによって起こすことが可能なるということです。スマートフォンも数の増加で新たな脅威が発生しています。



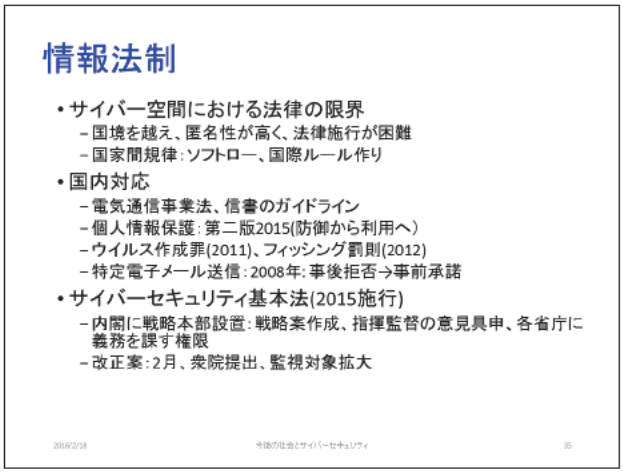
事例として、先ほどお話した JEEP ハッキング。衛星利用サービスの攻撃。ここで使われている GPS は非常にシンプルな通信方式ですから、なりすまし等は簡単に行えます。制御システムへの攻撃、コントローラにマルウエアを注入するものです。これに関しては、昨年 12 月に警視庁から危険性が発表されました。モバイル決済端末への攻撃。クレジットカードで支払いすることで便利なのですが、自分のお金がいつの間にか取られてしまう。Wi-Fi ハッキング。無線のシステムは実に弱い。さらに、心臓ペースメーカ不正操作に対する警告もあります。



情報セキュリティ対策技術は、いろいろあります。キーワードだけ挙げておきます。

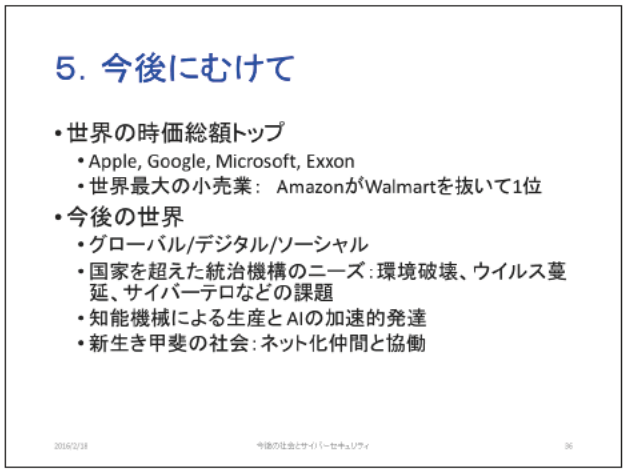


技術的な対策だけではありません。管理・運営が重要です。管理問題、インシデント・レスポンスは、攻撃でシステムがダウンしたら、できるだけ早急に対策グループを立ち上げて、対処しなければならないということです。内部で不正が起こらないように対抗策を立てなければならない。サイバー攻撃に対する CSIRT（消防団）を作る。意識改革やリテラシー教育も必要となります。外部委託をしていれば、その外部の行動もセキュアでなければならず、本社の中だけでなくても経営責任を取る必要があります。最後の砦として、保険があります。

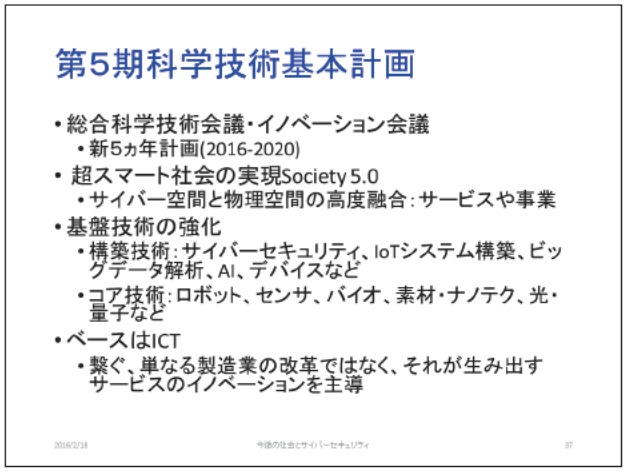


法律に関して、電気通信事業法、信書のガイドライン、があります。信書のガイドラインでは、封書を開けてはいけないと取決められています。メールに関しても中味を見てはいけないということになっています。それが、逆に攻撃者にとってみると、メールの中に悪いソフトを潜ませるというセキュリティ攻撃に関して有利になっています。個人情報保護は、個人情報を大切にしましょうということになっていますが、行き過ぎて同窓会の名簿の発行などにも影響があるようになっています。情報は活用することが重要であるということが、個人情報保護法第 2 版（防御から利用へ）で修正されました。ウイルスを作成すると罪になる。フィッシング

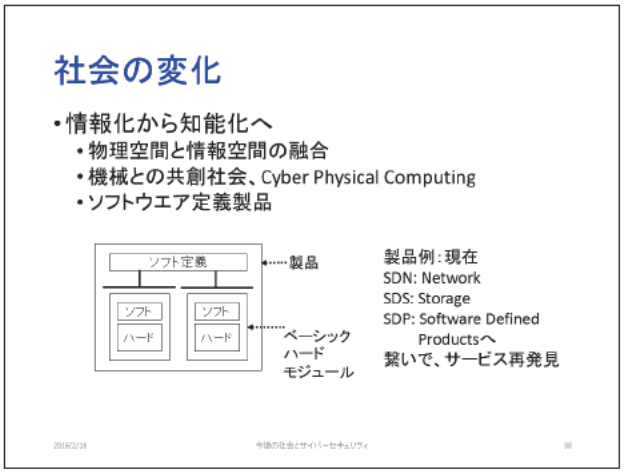
(Phishing) というのは、魚釣りではなく、詐欺という意味で、罰則が決められました。特定電子メール送信では、2008 年事前承認が前提になりました。しかしながら、現実にはあまり守られていません。サイバーセキュリティ基本法が 2015 年内閣府から出されました。



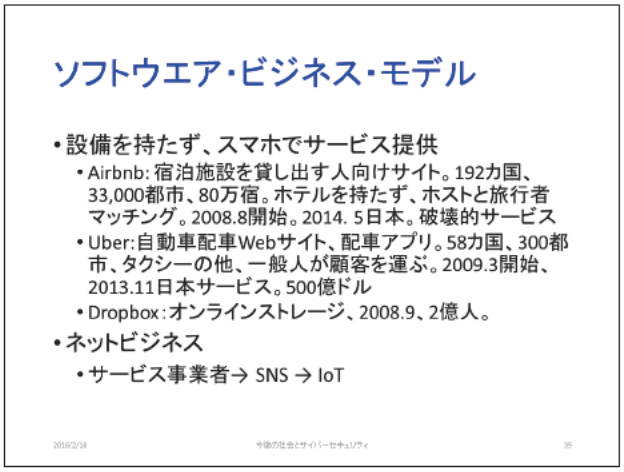
世界の時価総額トップ、Apple、Google、Microsoft は情報系です。小売では Amazon が Walmart を抜いて 1 位です。これらも情報系です。今後は、3 つのキーワード、グローバル・デジタル・ソーシャルが重要です。グローバルは、国家を超えた組織です。デジタルは、いろんなものがデジタル化されることです。ソーシャルは SNS で情報を共有するというのが典型例です。



日本においては、第 5 期科学技術基本計画が昨年の暮れにまとまりました。2016 年から 2020 年までの新 5 ヵ年計画です。キーになるのは、超スマート社会の実現です。Society5.0 これがキーワードです。ドイツでは、Industory4.0 として、製造業がすべてネットワークに繋がるということを展開しています。日本は、製造業だけではなく、サービス部門もすべて情報基盤技術の強化を目指そうとしています。ベースは ICT です。



社会の変化を見ますと、情報化から知能化へとなります。例えば、機械と共創社会、ソフトウエア定義製品などです。何でもソフトウエアを定義して作る。例えば、昔はスイッチ機器のハードウエアを繋いで、ネットワークを構成しましたが、ソフトウエアでネットワークの構造を定義して、ネットワークシステムを構成する。SDS (Software Defined storage) 。大きい会社であるとハードディスク等のストレージが沢山ある。ソフトウエアで定義して、大規模なストレージを作り、管理する。SDP (Software Difined Product) では、例えば秋葉原で安い組み込みモジュールを買ってきて、ソフトウエアで定義して、繋いで製品にすることができます。標準化されて安く売られることになります。



ソフトウエア・ビジネス・モデルについてお話します。貸したいという自宅持ちと借りたいという人とを繋ぐ宿泊サービスがあります。車もそうです。スマホで車を配車して欲しいと要求すると車に乗れるシステム。Uber という自動車の配車と客を結ぶシステムが大きなインパクトを与えています。このため昨年の 12 月、カリフォルニアのイエローキャブが会社更生法適用に追い込まれました。

攻撃側の世界

- 攻撃活動の市場化
  - 市場、請負、仕込み、攻撃活動
  - 侵入を見せての顧客獲得, 公開攻撃キット
  - Web 攻撃kit $数100/w, DDoS $10-1000/day, Card情報$10
- 攻撃活動の高度化
  - 対策を掻い潜る工夫が高度化：クリプトウエアは45倍増で、写真、重要契約書、請求書のファイルを暗号化し身代金要求。Tor, Bitcoin利用
  - 人（攻撃者）と人（防御者）のゲーム
- 攻撃側有利な世界
  - 一つでも穴があればよい vs すべてを防ぐ
- グローバル化
  - 世界に広がる攻撃者・Bot、捕捉の限界

2016/2/18　今後の社会とサイバーセキュリティ　40

攻撃側の世界では、攻撃活動の市場化、請負化、仕込み化してきています。Web 攻撃 Kit があり、DDoS 攻撃は、10 ドルから 1000 ドル/日で請け負います。カード情報というのは、1 枚 10 ドル。攻撃が高度化しています。請け負って実績を見せて、また請け負うというということになっています。現在は、人と人との攻撃になっています。セキュリティ攻撃は、結局は人が起こすのです。さらに、これからは、IoT になります。IoT は、ネットワークに対して脆弱です。攻撃者は、そこにマルウエアを入れて、攻撃します。非常に怖い世界になります。攻撃側に有利な世界です。一つでも穴があるとそこを攻撃されます。

セキュリティ研究開発テーマ例

- システム設計原理
- 次世代高セキュア・コア・チップ
- セキュリティ要素技術
  - –OS、暗号、形式的開発、脆弱性発見、認証システム
- 攻撃分析による知的侵入防御システム
- 人・機械・法制の役割分担：実利用からの反映
- 次世代サイバーセキュリティ対応技術
  - –人ベースからIT高度支援
  - –ビッグデータ解析、知的処理、学習機能

2016/2/18　今後の社会とサイバーセキュリティ　41

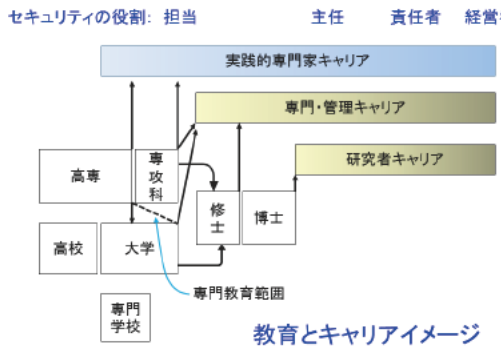
セキュリティ研究開発テーマ例として、いろんなテーマをリストアップしておきます。参考にして下さい。

情報セキュリティ人材と仕事

- 人材の種類：不足
  - 組織内オペレーション
    - – 経営者/セキュリティ責任者/セキュリティ担当者/CSIRT
  - 組織間オペレーション
    - – JPCERT/CC, SOC, GSOC, Telecom ISAC, IPA
    - – グローバル：FIRST(信頼化されたCIRTの国際組織で、問題対応を効率化、メンバ間のTrusted連絡)
  - セキュリティ専門企業・組織：アウトソーシング受託
  - 研究開発：大学、NICT, 産総研、IPA, 企業
- 人材育成の必要性と機会
  - 大学、高専、専門企業
  - 社員全体のリテラシ＋対応組織専門知識

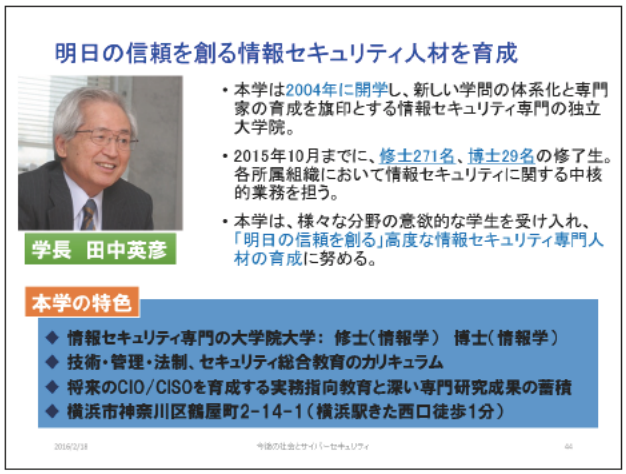
2016/2/18　今後の社会とサイバーセキュリティ　42

情報セキュリティ人材が不足しています。組織内オペレーションでは、経営者、セキュリティ責任者、セキュリティ担当者、CSIRT 等が構成メンバーです。もう一つは、組織間オペレーションに関する人々が居ます。会社と会社の間を常に監視していて、会社に警告を出してくれる JPCERT/CC 等があります。グローバルには FIRST という専門組織があります。CIRT の国際組織で、メンバー間の情報交換を行っています。また、セキュリティの専門企業があるし、人材教育の必要性があります。セキュリティ人材が不足しています。

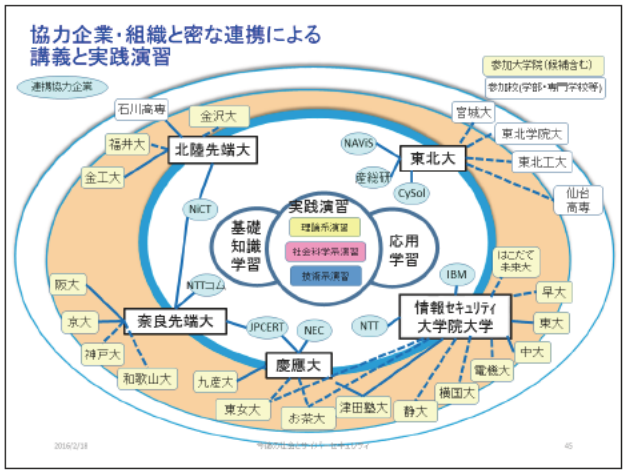


2016/2/18　今後の社会とサイバーセキュリティ　43

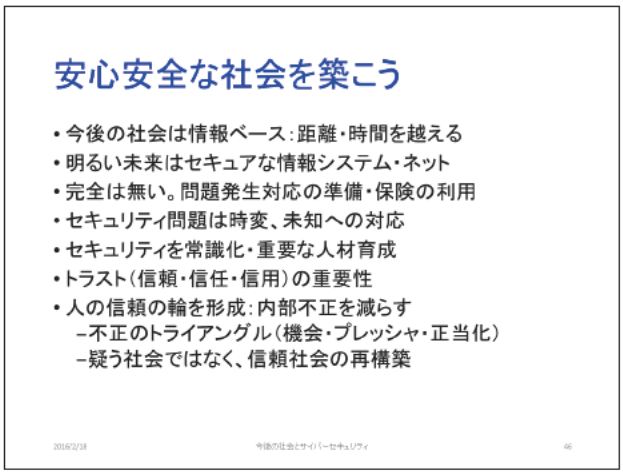
これは、キャリアイメージですが、高専・専攻科を出て実践的専門家キャリア、専攻科、修士から専門・管理キャリア、博士から研究者キャリアがあります。実践的専門家キャリアの人材不足が問題になっています。是非そのところを目指して欲しいと思います。



これは、私の大学院の紹介です。12 年前に開学して、修士 271 名、博士 29 名を輩出しております。修了生は、情報セキュリティに関する中核業務を担っています。セキュリティは情報交換が重要です。修了生は、ネットワークを創って、それぞれ連携して情報交換をしています。情報セキュリティ大学院大学は、技術・管理・法制、演習等をカリキュラム化し、教育と研究を進めております。



これは、enPiT (Education Network for Practical Information Technology) という組織です。大学とか高専、企業と協力して、実践演習、応用学習を展開しています。私共、情報セキュリティ大学院大学は幹事、中核としてやっております。



最後に、今後の社会は情報ベースです。明るい社会はセキュアな情報システムを使うことから始まります。完全は無い。問題発生の対応、攻撃が新しくなる。未知への対応が必要になります。トラスト（信頼・信任・信用）は重要です。信用とは、この人は大丈夫ですよということです。信任とは任せること、信頼とは、それに基づいて将来を期待することです。人の信頼の輪を形成し、内部不正を減らすことが大切です。不正のトライアングル（不正の機会がある、上司からプレッシャが与えられる、自分の正当性を主張する。）があると内部不正が起こります。三つの機会をできるだけ解消することが重要と言われています。これからは、疑う社会では無く、信頼社会を創るということが重要だと思っております。是非皆さん、こういうところに注力して下さい。

(平成 28 年 2 月 18 日「社会ニーズを踏まえた
セキュリティ人材の育成」事業　特別講演会
記録　木更津高専　情報工学科
教授　専攻科長　栗本　育三郎)

講演者紹介

田中 英彦

東京大学大学院工学系研究科電気工学専門課程修了。工学博士。東京大学にて計算機アーキテクチャ、並列処理、人工知能、自然言語処理、分散処理、メディア処理などの教育・研究に従事。東京大学大学院情報理工学系研究科長を経て、2004 年 4 月情報セキュリティ大学院大学情報セキュリティ研究科長・教授に就任。2012 年より同学長・教授。情報処理学会功績賞、人工知能学会論文賞、ACM SIGGRAPH'99 Impact Paper Award、人工知能学会功績賞、東京都科学技術功労者表彰、経済産業大臣表彰など受賞。JNSA 会長、情報処理学会名誉会員、IEEE Life Fellow、東京大学名誉教授。

社会ニーズを踏まえたセキュリティ人材の育成」事業

特別講演会

「今後の社会とサイバ　セキュリティ」

開催日時：2016 年 2 月 18 日(木) 16:30〜17:40

会場：木更津工業高等専門学校　第一講義室(本会場)
(他接続校)
旭川高専、釧路高専、八戸高専、仙台高専
一関高専、鶴岡高専、長岡高専、群馬高専
石川高専、鳥羽商船高専、広島商船高専
大島商船高専、宇部高専、徳山高専、呉高専、
新居浜高専、香川高専、高知高専
北九州高専、佐世保高専、都城高専

講演者：田中 英彦
(情報セキュリティ大学院大学　学長)

司会：米村 恵一
(木更津工業高等専門学校　情報工学科　准教授)