Symposium

シンポジウム

東京を支える鉄道・航空における サイバー攻撃の脅威

～2020年に向けて～

平成28年2月8日　海運クラブ国際会議場

主催：一般財団法人運輸政策研究機構
後援：サイバーセキュリティ戦略本部，国土交通省
協力：公益財団法人東京オリンピック・パラリンピック競技大会組織委員会

プログラム

13:30～13:45	**主催者挨拶**	黒野　匡彦	一般財団法人運輸政策研究機構会長
	来賓挨拶	武藤　　浩	国土交通省国土交通審議官
	来賓挨拶	舘　　剛司	公益財団法人東京オリンピック･パラリンピック競技大会組織委員会 テクノロジーサービス局長
13:45～14:30	**基調講演**	**「サイバー攻撃による脅威の現状と課題」**	
		田中　英彦	情報セキュリティ大学院大学学長
14:30～15:15	**特別講演1**	**「我が国のサイバーセキュリティ戦略」**	
		谷脇　康彦	内閣サイバーセキュリティセンター副センター長
15:15～15:35	**コーヒーブレイク（休憩）**		
15:35～17:00	**研究報告**	**「東京オリンピック・パラリンピックに向けた交通機関への サイバーテロ対策に関する調査研究」**	
		西村　潤也	一般財団法人運輸政策研究機構調査室研究員
		岩井　博樹	デロイト トーマツ リスクサービス株式会社シニアマネジャー
		寺田　真敏	株式会社日立製作所 Hitachi Incident Response Team チーフコーディネーションデザイナ
		宮　麻里子	株式会社サイバーディフェンス研究所情報調査部主任分析官
		利根川義英	株式会社キーコネクト代表取締役セキュリティアドバイザ
17:00～17:45	**特別講演2**	**「交通機関を中心とした重要インフラ事業者が直面するサイバー脅威」**	
		名和　利男	株式会社サイバーディフェンス研究所専務理事/上級分析官
17:45～17:50	**閉会挨拶**	春成　　誠	一般財団法人運輸政策研究機構理事長

司会：神田　尚樹　　一般財団法人運輸政策研究機構調査室長

「東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究」および本シンポジウムは，平成27年度日本財団助成事業として実施した．

1――基調講演

サイバー攻撃による脅威の現状と課題

田中英彦
（情報セキュリティ大学院大学学長）

サイバー攻撃による脅威について，現状と課題を整理する．

まず，「情報社会」という言葉があるが，この新たな社会では，オフィスで言えばE-mail主体のコミュニケーション，文書は紙から電子媒体へ，証明は印鑑から電子証明に変わり，業務形態を劇的に変化させている．また，企業には多くのパソコンがあり，それぞれがネットワークで繋がれ，重要な情報はデータベースに保存，外部とはインターネットを経由して接続されている．近年は，外部のクラウドの活用や，通信網や無線を経由して個人のスマートフォンや携帯電話にも接続している．そのような「情報社会」では，セキュリティ問題が発生する．具体的には，情報の窃取や破壊，Dos攻撃などによるサービスの停止，なりすまし詐欺や不正送金，システムやソフトウエアの破壊など，いたずらから国家的犯罪まで様々な問題が発生している．Webサイトの78％は何らかの脆弱性を持っており，メールの3通に1通はスパムメールであるとも言われているほか，最近では家庭用のパソコンをネットワークに繋げるためのルーターが犯罪の温床になっている．実際のサイバー攻撃の被害を見ると，2004年アメリカのAOLで9,300万件の顧客情報流出，2007年エストニアでDDos攻撃によって政府機関のシステムの一部が停止，2010年イランの核施設でStuxnetによる攻撃によって遠心分離機が破壊したほか，日本でも昨年の日本年金機構のような標的型攻撃による情報の流出や機密情報の漏洩が増加している．日本では，それに対する調査費用やシステムの再構築費用が1つの事案あたり5,000万円～1億円とされているほか，売上額の5～40％に影響すると言われており，侵入から発見まで平均242日もかかっていることが被害を拡大している．アメリカにおいても，ビジネス機会の損失が157万ドル，対策コストが99万ドルという数字が示されており，インシデント対応には経営幹部の関与が必要であると言われている．

また，最近「標的型攻撃」が非常に話題になっており，大企業の6社に5社は標的になっているとも言われている．手法としては，直接標的となる企業を攻撃するのではなく，まずは資金力が小さく，システムが脆弱な中小企業を攻めて，そこを経由して大企業を攻撃するという方法が多くなっている．また，送られてくるメールも本物と区別がつかないほど巧妙に作成され，巧みにマルウェアをダウンロードさせるようになっている．従って，完全に防御することは困難であり，最近は事後対応を迅速，確実に行って被害を最小限にするための推進体制の整備や，予算措置，人材育成といった対策に重点が置かれている．

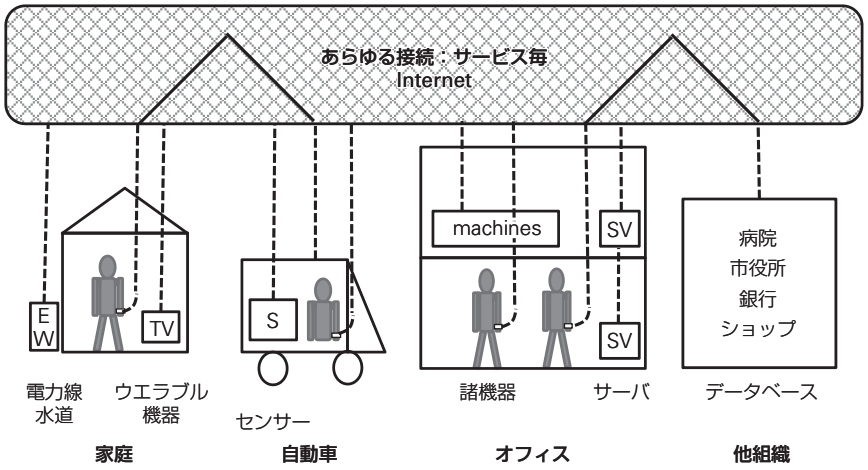
さらに，「ランサムウェア」による攻撃も増加している．これは，マルウェアの一種で，病院などのコンピュータに感染してアクセス制限がかけられ，それを解除するために身代金の支払いが強要されるというものである．この攻撃は昨年から急増しており，IPA（情報処理推進機構）からも情報が出されている．

一方，重要インフラや制御系システムへのサイバー攻撃については，外国では電力会社や核施設，石油パイプライン，鉄道，下水処理施設への事案がある．これらの攻撃は氷山の一角であり，実際の状況は攻撃が無いのではなく，検出していないので発覚していないだけというのが現状である．重要インフラや制御系システムは，その規模や継続した運用から古い機器を長期間使用することが一般的であり，安定稼働を実現するために，システムの更新や変更はあまり行われていない．しかし，これが脆弱性となり，例えば攻撃されやすいソフトウェアが内在したまま稼働し続けるわけである．今後，攻撃手法が多様化，複雑化していく中で，このような状態を放置することは大変な問題であると考えている．

ここまで，「情報社会」の現状とその中で発生しているセキュリティ問題を整理したが，次に今後の発展を推察する．第一に「IoT」（Internet of Things）と言われているように，あらゆる機器が電子化され，それらがネットワークで繋がる．第二にネットワークの広がりにより情報が膨大になり，この所謂「ビッグデータ」をどのように活用するのかということが重要になる．第三に人工知能が発達して，画像認識や最適化が自動的に可能になる．このような社会の変化や新たな技術に対して，攻撃者と防御者がそれぞれどのように対応するのかがこれからの鍵になる．

将来の社会イメージを図―1に示す．家庭用のテレビや自動車のセンサー，オフィスのサーバや施設のデータベースなどが全て繋がっている．従来は，これらが独立していたが，将来はあらゆるものやサービスが物理的に接続可能になる．実際に，コネクテッドカーと呼ばれるICT端末としての機能を有する自動車については，ハッカーの攻撃を予防するため約140万台のリコールが実施されるなどリスクが顕在化していることから，図のような社会になれば，必然的にサイバー攻撃は増加すると考えらえる．また，ハクティビストと呼ばれる政治的な意思表示や政治目的の実現のために意図的，組織的な攻撃や，国家が関与した攻撃が増加するほか，アメリカでは電力網

田中英彦



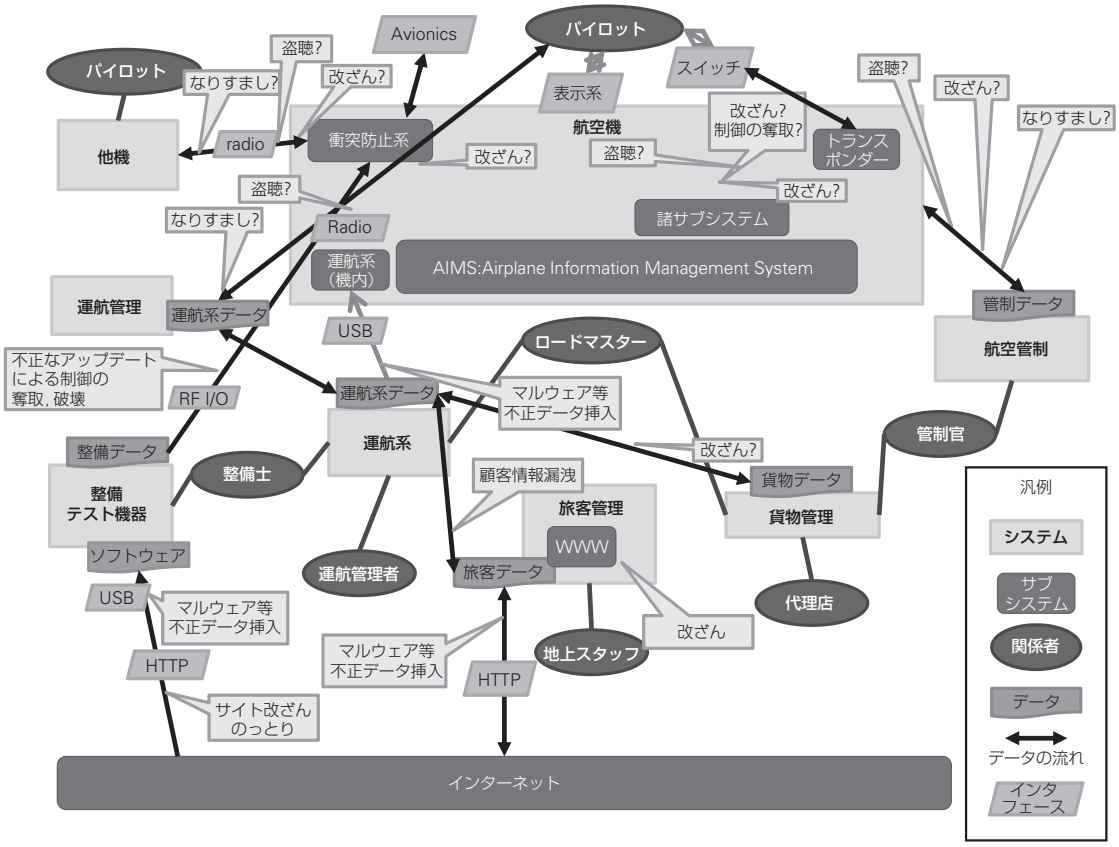
■図―1　将来の繋がる社会のイメージ図

への攻撃は21世紀最大の脅威であると言われており，重要インフラを狙った攻撃も増加すると考えられる．このような攻撃の脅威は，接続している機器の増加により一層拡大し，且つ実被害の影響範囲も大きくなる．

このような将来の社会の変化に対して，企業や国は新たな対応が必要となる．第一に，経営者や組織の上層部の認識向上が必要となる．流出した情報は回収が不可能であり，サイバー攻撃の被害は経営問題に発展することを理解し，必要な予算措置や対策を速やかに実施することが必要となる．第二に，社内外のデータの経路を総合的に監視し，必要な情報は暗号化して持ち出し，中央サイトでは認証をかけてチェックするなどデータの保護や解析を進める必要がある．第三に，大企業ではCSIRT（Computer Security Incident Response Team）の構築が進んでいるが，このようなインシデントレスポンス対策を充実させるとともに，社員教育や全面的な外部委託とはしない体制，サイバー保険の活用など管理・運用面の対策も必要である．第四に，法制面からは，昨年サイバーセキュリティ基本法が制定されたが，サイバー空間に国境はなく，匿名性も高いため，日本国内だけでなく国家間のルール作りも重要な対策になる．最後に，企業や国で様々な対策を進めると同時に，様々なレベルで組織間の連携をすることが最も重要である．ISAC（Information Sharing and Analysis Center）という組織がある．日本では，金融分野と通信分野にあるが，この他の分野においてもISACを構築して情報共有を進める必要がある．特に中小企業は，少人数でセキュリティ対応を行っている場合が多く，限界があるため，業界内で情報を共有する組織は重要になる．

次に，鉄道と航空のシステムの特徴と脆弱性を整理する．まず，鉄道のシステムは輸送業務を行うために列車制御や電力，旅客系，事務系などのシステムがあり，その一部が外部と接続しているという構造である．列車運行は列車の存在により転てつ器をロックするといった物理的な確実性をもって安全を確保しているほか，異種性（異なるシステムや新旧のシステムの共存）と適応性（改修・変更・移行等の状況変化への対応）という2つの要素を考慮したアシュアランス技術と言われるシステムになっている．また，制御系システムの表示を見て，情報系のシステムを人がコントロールすることにより，制御系システムの独立性を保っている．しかし，前述のIoT技術の進展により，外部と接続している旅客系や事務系だけでなく，列車制御や電力のシステムにもサイバー攻撃の脅威の可能性が出てきている．また，内部犯行やUSBを経由した攻撃，古いシステムの利用による脆弱性の内在潜伏などの脅威も考えられる．航空のシステムも鉄道と似たような構造となっているが，異なるポイントは航空管制と整備システムである．航空管制システムは，全世界で標準化されたシステムであり，整備システムはボーイングなど航空機メーカーと航空会社がデータを共有しているシステムであり，鉄道のシステムにはない特徴を持っている．特に航空管制は，特定の周波数を使用して飛行機の位置を外部に発信し，それを地上で受信しているが，その情報は誰でも受信できる．これに対して攻撃するという可能性は十分に有り得ることから，アメリカの米政府監査院（GAO）報告書でもその脆弱性が指摘されている．また，一例として情報セキュリティ大学院大学の中にあるAS（Aviation Security）研究会で，各システムとそれらに対する攻撃の可能性を分析した結果を図―2に示す．

最後に，今後に向けた対策の参考資料をいくつか紹介する．まず，昨年12月に経済産業省が発表した『サイバーセキュリティ経営ガイドラインVer1.0』である．同ガイドラインには，サイバーセキュリティは経営問題であり，経営者の3つの原則として「リスク認識」「全関係企業へのセキュリティ対策」「関係者との適切なコミュニケーション」が挙げられているほか，チェックシートも示されている．次にJNSA（日本ネットワークセキュリティ協会）が今年4月に改訂予定の『情報セキュリティポリシーサンプル』である．現在，中小企業向けに改訂作業中であるが，対策実践の手引書としてサンプルや状況チェックシートが示されている．最後に，外国の資料としてアメリカの『Framework for Improving Critical Infrastructure Cybersecurity Ver1.0』である．これは2014年にNIST（米国国立標準技術研究所）が示したものであり，IPAが翻訳文書を公開しているので参考にしていただきたい．



■図―2　航空システムのリスク分析（AS研究会資料）

2――特別講演1

我が国のサイバーセキュリティ戦略

谷脇康彦
（内閣サイバーセキュリティセンター副センター長）

内閣サイバーセキュリティセンター（以下「NISC」という）は，各省庁のサイバーセキュリティ政策をまとめて，国家戦略として推進するという役目と，各省庁の情報システムにセンサーを設置して24時間365日監視を行うとともに，場合によりマルウェアの解析や各省庁へ警告を出す役目の2つを担っている．

現在，我が国が直面しているサイバー空間の脅威について，「リスクの深刻化」「リスクの拡散」「リスクのグローバル化」の3つの側面から説明する．

第一に「リスクの深刻化」であるが，NISCの監視では，各省庁に対する不審な通信を2014年度は年間約400万件検知しており，8秒に1回アラートが上がったという計算になる．これらの通信をNISCが解析し，深刻であると判断した場合は関係省庁に通報しているが，通報件数は年間264件であり，2013年度と比較して約2倍に増加した．また，通報した264件のうち約4割は標的型メールが原因であった．2015年度は2014年度の2倍以上のペースで推移している．

第二に「リスクの拡散」であるが，サイバーセキュリティと聞くとパソコンやスマートフォンが頭に浮かぶと思うが，最近では，自動車や電力会社のスマートメーターなどにもサイバーリスクが及んでいる．自動車では，ハッカーがパソコンから自動車を故意に遠隔操作した動画がアメリカのWebサイトに掲載されてリコールになったほか，各電力会社が設置を進めているスマートメーターも，従来は閉じていた送電網，つまり電力のネットワークに，電力消費量を電力会社へ伝えるという新たな情報ネットワークが一体化され，サイバー攻撃の脅威が高まっている．さらに，IoTの世界が進展するとさらにリスクは拡散していく．

第三に「リスクのグローバル化」であるが，サイバー空間に国境はなく，どこからでも日本に対して攻撃を仕掛けることが可能である．数年前までは，日本は日本語を使用しているので脅威は少ないと言われていたが，最近は自動翻訳ソフトなどを活用して流麗な日本語で悪意を持ったメールが送られてくるようになった．また，海外のサイバー攻撃の事案では，ソニー・ピクチャーズ・エンタテイメントやアメリカの人事管理局へのサイバー攻撃のほか，最近では，ウクライナやイスラエルの電力会社がサイバー攻撃を受けた．

毎年1月に開催されるダボス会議を運

谷脇康彦

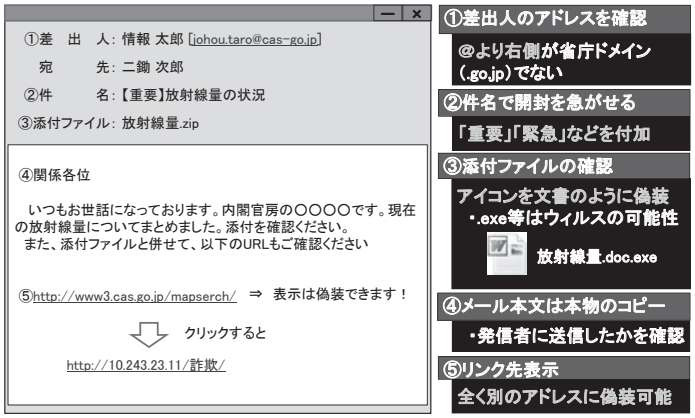
営している世界経済フォーラムが，世界が抱える29のリスクをランク付けしているが，その中でサイバーに関係するものとして「サイバー攻撃」「データ窃取」「重要情報インフラの損壊」が挙げられている．図―3に示した黒い部分がサイバー攻撃のリスクが深刻な国であり，アメリカ，ドイツ，日本などが最も深刻であり，北米，アジア・オセアニア，ヨーロッパ，さらにアフリカでも一部深刻度が高まっている．

こうした中，昨年1月に，サイバーセキュリティ基本法が施行された．実は法律で「サイバーセキュリティ」という言葉を使ったのは，この法律が初めてである．新しい体制では内閣官房長官を本部長とするサイバーセキュリティ戦略本部が組織され，その事務局をNISCが担当している．また，この法律でNISCの権限が明確化された．施行前は，各省庁がセキュリティについて自主的な監査を行っていたが，施行後はNISCが第三者監査を行うことになり，今年度中に10省庁に対して実施する予定である．監査は，セキュリティポリシーのPDCAが適切に循環しているかをチェックする『マネジメント監査』と，NISCが疑似的なハッカーになって各省庁の情報システムの中に入って脆弱性をあぶり出し，必要な対策を練るための『ペネトレーションテスト（侵入テスト）』の2種類を行う．また，同法施行後には，重大な事案が発生した場合の原因究明調査をNISCが実施することに加え，資料提出義務や本部長による勧告権が与えられた．実は，この権限が後述する昨年6月に公表された日本年金機構の事案の際に大きく役に立った面があった．さらに，この法律に基づき，昨年9月に新しい『サイバーセキュリティ戦略』を閣議決定した．

次に具体的な内容を説明する．前述のように標的型メール攻撃は官民問わず増加しており，警察庁のデータでは，2014年上半期と2015年上半期の比較で約7倍に増えているという非常に深刻な状況である．メールの内容の一例を図―4に示す．

出典：World Economic Forum, "The Global Risks Report 2016 : 11th Edition"（January 2016）

■図―3　サイバー攻撃の深刻度（WEF2016）



■図―4　標的型メールの例

①知り合いの「情報太郎」さんのアドレスが，正しくは（@cas.go.jp）であるが（cas-go.jp）となっており，偽物のメールである
②件名に【重要】や【緊急】と書かれている
③添付ファイルの拡張子が（.exe）となっているが，例えばワードファイルであれば正しくは（.doc）や（.docx）であり，ウイルスの可能性がある
④メール本文が，以前は明らかに怪しい表現が多かったが，最近は流麗な日本語で表現され，内容も差出人の立場に合うように過去のメールを引用したものなどが使われている
⑤リンク先が表示されているが，リンク先は簡単に偽装できるため，正しいと思ってクリックすると不正なサイトにアクセスし，そこからマルウェアをダウンロードすることになる可能性がある

NISCでは，偽物の標的型メールを作成して，政府職員18万人を対象に送付したことがあるが，約10～15%の職員が開封してしまった．また，最近はやりとり型と呼ばれるものもあり，例えば企業の採用担当窓口に「私は学生ですが，採用窓口はこちらで良いですか」と偽物メールを送信，「はい，そうです」と返信が来ると「履歴書を送ります」と再度送信して添付ファイルを開かせるといった，何回かメールのやりとりをして相手を信頼させた上でマルウェアを仕込む手口である．この場合，成功率は20%以上に跳ね上がる．15%や20%は小さな数字に見えるかもしれないが，攻撃者は1回でも成功すれば良いわけである．これを防御する側から考えると，侵入されることを許すわけではないが，入られることを前提にした対策が必要となる．侵入を早期に発見し，被害を最小化するといった内部対策を講じていく必要がある．従って，防御の壁を何重にもつくる『多重防御』という考え方が重要になる．しかし，こ

れには費用と時間がかかるため，リスク評価を行い，特に重要な情報が蓄積されているサーバは多重防御とする，情報が漏洩しても社会的，経営的に大した影響がないサーバは多重防御しないといった，情報の機密性や重要度などに合わせた対処が必要である．

次に，昨年6月に公表された日本年金機構の事案について説明する．前述の通り，この事案はサイバーセキュリティ基本法施行後初の特定重大事象に指定し，NISCが原因究明調査を担当したものである．攻撃手法は，典型的な標的型メールであり，日本年金機構の事案では4つの波に分かれてメールが届いていた（表―1参照）．第一波が5月8日，この段階では公開されている2件のメールアドレスに届いた．このうち1台のパソコンでメールを開いてしまったが，4時間後にLANケーブルを抜いた．第二波は5月18日，公開していない個人のアドレス98件にメールが届いた．これは，おそらく1回目の侵入で非公開のメールアドレスの情報を窃取されており，第二波ではそのアドレスを攻撃したと想定され，3台のパソコンが感染したが，不審な通信が発生するも接続先への通信は失敗している．第三波は5月18日～19日，第二波とは別の非公開の個人アドレスにメールが届いたが，不審な通信は発生していない．第四波は5月20日，実はここで問題が発生する．第四波により，複数台のパソコンが感染し，国内のサーバへ多数の通信が行われ，結果として125万件の個人情報が流出した．

第一波から第四波までの標的型メールの件名は，年金や医療費など実際の業務に関係のある言葉を巧みに使い，職員が開きそうなタイトルにしている．また，攻撃者は1回では諦めず，何度も波状的に攻撃を仕掛けてくること，発見後ただちに対処しなければ大量の個人情報の流出につながる可能性があることがこの事案で改めて明らかになった．

■表―1　日本年金機構事案に関する不審メールの概要

不審メールの番号	受信日	不審メールの概要
Ⅰ	5月8日（金）	件名：「厚生年金基金制度の見直しについて（試案）に関する意見」 宛先：公開メールアドレス（2） リンク：商用オンラインストレージ
Ⅱ	5月18日（月）	件名：給付研究委員会オープンセミナーのご案内 宛先：非公開の個人メールアドレス（98） 添付ファイル：給付研究委員会オープンセミナーのご案内.lzh
Ⅲ	5月18日（月） ～ 5月19日（火）	件名：厚生年金徴収関係研修資料 宛先：非公開の個人　メールアドレス（20） 添付ファイル：厚生年金徴収関係研修資料（150331厚生年金徴収支援G）.lzh（16） リンク：商用オンラインストレージ（4）
Ⅳ	5月20日（水）	件名：【医療費通知】 宛先：公開メールアドレス（3） 添付ファイル：医療費通知のお知らせ.lzh

出典：日本年金機構における個人情報流出事案に関する原因究明調査結果

日本年金機構の情報システム自体は，インターネットにはつながっていないクローズドの閉域網のシステムであったが，業務を行う際に個人情報を他のパソコンに移して作業をしていた．結果として，そのパソコンから個人情報が流出したわけであり，システムの設計に問題はなかったが，設計に沿った運用が行われていなかったという点に問題があった．

また，厚生労働省にはインシデントが起きたときの対応チーム（CSIRT）があり，メンバーも手順も決まっており，事案発生後に同チームが結成されたが，上手く機能しなかった．その原因の一つはチームのメンバーが全員管理職だったということである．実際に手を動かせる人材がいなければ，チームは機能しないことが改めてわかった．また，同機構のセキュリティポリシーを見ると，リスク管理の規定はあるが，サイバー攻撃事案を想定した内容ではなかった．日本年金機構の事案については，昨年8月にNISCとして原因究明調査結果を公表しているので，参考にしていただきたい．

前述のように，昨年9月に『サイバーセキュリティ戦略』を閣議決定した．ポイントは「国民が安全で安心して暮らせる社会の実現」「経済社会の活力の向上及び持続的発展」「国際社会の平和・安定及び我が国の安全保障」の3つである．従来の安全・安心といった防御能力の強化という視点の他，サイバーセキュリティを産業として考えていくという視点，国際連携という視点が加わった．この3つを支えるものとして「研究開発の推進」と「人材の育成・確保」が位置付けられている．サイバーセキュリティを産業として考えていく視点を考える上では，IoT社会を前提に検討していかければならない．IoTは，各機器のセンサーのデータがネットワークにより蓄積され，この大量のデータを解析してナレッジ（知恵）が生まれてリアル空間へフィードバックするというものであり，この一連の流れの中でセキュリティを確保していく必要がある．今年1月に閣議決定した第5期科学技術基本計画の中でも，IoTサービスプラットフォームの構築に必要となる基盤技術の強化が取り上げられており，国としても取り組んでいかなければならない．アメリカのNIST（米国国立標準技術研究所）のレポートでは，IoTにおけるリスク要素の一つとして強靱性（レジリエンス）の確保が必要であると示されている．例えば，システムが要求の100％稼働せず，20％程度まで低下してもサービスは継続できるというものが強靭性である．その際に，よく言われることが，OT（オペレーションテクノロジー）とIT（インフォメーションテクノロジー）の一体化である．例えば，企業内では，制御システムのオペレーションを担う担当部署と，ITを担う情報システム部の2つが存在していることが多い．この考えが異なる2つの部署をどのように

統合していくのかがIoT社会における強靭性を考える上では重要である.

一方で, 日本企業の情報漏えいの原因を見ると, 管理ミスや誤操作, 紛失・置忘れといったヒューマンエラーが全体の約7割を占め, サイバー関連は全体の3%程度である. しかし, 2013年の個人情報漏えい事案の中で, 規模が大きいものから順に並べたワースト10のうち7件は不正アクセスによるものであり, サイバー攻撃の数は少ない, もしくは認識されていないが, 一旦サイバー攻撃を受けると企業の経営に大きな影響を与えることがわかる. 上場している日経225社の過去5年間の有価証券報告書をチェックすると約6割の企業がサイバーセキュリティに関する何らかの記載をしている. 意外に多くの企業が記載しているが, 内容を確認すると, 記載方法が包括的で, 広義の表現が多く, 具体性が乏しいものが大半であった. 経営者にとって株主への説明責任は重要な要件であり, サイバーセキュリティを経営リスクの一つとして捉え, 情報を開示していくという意識改革を民間企業の経営者の皆様に促していくとともに, そのような取組みを促す仕組みが必要であるということを関係省庁と検討している.

2014年5月に決定した「重要インフラの情報セキュリティ対策に係る第3次行動計画」では, 重要インフラとして13分野を指定しており, 運輸関係では, 鉄道, 航空, 物流が含まれている. 重要インフラ分野に関しては, 関係省庁とNISCが様々な活動を行っているが, 一番大事なことは『情報共有』である. サイバー攻撃を受けたという情報を共有することは, 大抵の場合躊躇するものだが, その経験を是非他の企業, 他の分野の方々と共有していただきたい. それによってこの国全体を守ることにつながる. 特に最近, 重要インフラ分野の核となっている制御システムのセキュリティが非常に重要になってきている. 制御システムは, 長期間稼働しているために脆弱性があり, OSも以前は独自に構築していたが, 最近ではウィンドウズやリナックスなど汎用性の高いソフトウェアを利用している. この制御システムがサイバー攻撃を受けることによって, 鉄道の運行, あるいは飛行機の運航に支障が出ることは十分想定される.

NISCでは, 重要インフラ13分野の民間企業の皆様と関係省庁を対象に, 年1回, 分野横断的演習を実施している. 参加者は年々増えており, 昨年12月の演習には1,000名を超える参加があり, 一昨年の約3倍の参加者数となった. この演習自体は1日だが, 準備段階や演習後における課題のあぶり出しを各組織に持ち帰り, 対策の検討のきっかけにしていただきたい.

今年2月に「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案」を閣議決定し, 国会に提出した. この改正法案は, 日本年金機構の情報流出事案を踏まえ, 監視・監査・原因究明調査等の対象範囲を, 現在の中央省庁のみから独立行政法人や特殊法人・認可法人にまで拡大し, その事務の一部をIPAに委託することとしている. また, セキュリティ人材育成の観点から, 新しい国家資格として『情報処理安全確保支援士制度』を創設するとともに, ソフトウェアの脆弱性の公表について, ソフトウェア作成者の同意がない場合でも国民生活に深刻な影響を与える場合には, 脆弱性情報を公表するという仕組みを入れていきたいと考えている.

国際連携については, アメリカやイギリスなどと2国間協議を行っているほか, 特にASEANとの間では2009年から協力関係があり, 具体的な協力を行っている. また, 日本, 中国, 韓国の3カ国での協議も一昨年から始めており, サイバーセキュリティは国家安全保障にもかかわる非常に重要な問題になってきている. 2013年12月に閣議決定した国家安全保障戦略でも, 初めてサイバー空間におけるリスクや防護の必要性が謳われている.

今年5月には伊勢志摩サミットがあり, それに向けたセキュリティ対策の強化が喫緊の課題であるが, さらには2020年の東京オリンピック・パラリンピックに向けた取組みもNISCとして組織委員会と連携をしながら進めているところである.

3——研究報告

東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究

3.1 研究の背景と目的

西村潤也
（運輸政策研究機構調査室研究員）

本研究は, 平成27年度日本財団助成事業として進めてきた. 2020年東京オリンピック・パラリンピック競技大会の開催が決定し, 東京大会では都心を中心としたコンパクトな開催を目指している中, 安全, 迅速, 円滑な輸送が求められている. 過去のオリンピックは幾度となくテロの標的となっており, 1972年ミュンヘン大会では武装組織が選手村を襲撃するといった実際のテロ攻撃が発生し, 前回2012年ロンドン大会では公式サイトに2億回を超える不正アクセスがあったと言われている. サイバー攻撃は年々増加しており, 特に昨年5月の日本年金機構に対するサイバー攻撃は報道等でも大きく取り上げられ, 関心が高まっている. また, 交通機関でも最近では成田国際空港, 中部国際空港, JR北海道, 南海電鉄

西村潤也

などにサイバー攻撃があったほか，海外ではポーランド航空やソウルメトロに対するサイバー攻撃も報告されている．

鉄道や航空などの交通機関が運用する運行制御系システムや予約システムなどは，各企業が独自に構築したネットワーク内での運用や，外部のネットワークに繋がっていないクローズドシステムになっており，これまではサイバー攻撃の可能性は低いと考えられていた．しかし，海外では2010年のイラン原子力発電所，2014年のドイツ製鉄所のサイバー攻撃などが代表的な事例として挙げられるが，クローズドシステムに対するサイバー攻撃の被害も報告されている．2020年の東京オリンピック・パラリンピックに向けてサイバー攻撃の危険性が増す中で，大量輸送を担う交通機関に対するサイバー攻撃が発生した場合には，社会的混乱や人命に関わる事故に発展する恐れもある．

本研究では，東京オリンピック・パラリンピック期間中に鉄道・航空を対象としたサイバーテロが起きる可能性があるという前提で，1年目はターゲットや攻撃手法などの整理，2年目は対策の検討を行うこととした．ただし，本研究は，交通事業者や利用者に対してサイバー攻撃の脅威を過度に煽るものではなく，現実にあり得る脅威と，あり得ない空想の脅威を峻別し，正確なリスクやシステムの脆弱性を把握するものにしたいと考えている．

本年度は次の4つの研究を実施した．第一に，サイバー攻撃の近年の事案を分析し，ターゲットや攻撃手法を整理した．第二に，鉄道分野と航空分野の事業者に協力していただき，現状のサイバーセキュリティに対する意識調査を実施した．第三に，欧州やアメリカのサイバーセキュリティの取組みを整理した．第四に，運輸業界の事業者の制御系システムを利用して，ペネトレーションテストを実施した．

3.2 サイバー攻撃に関する近年の事案分析

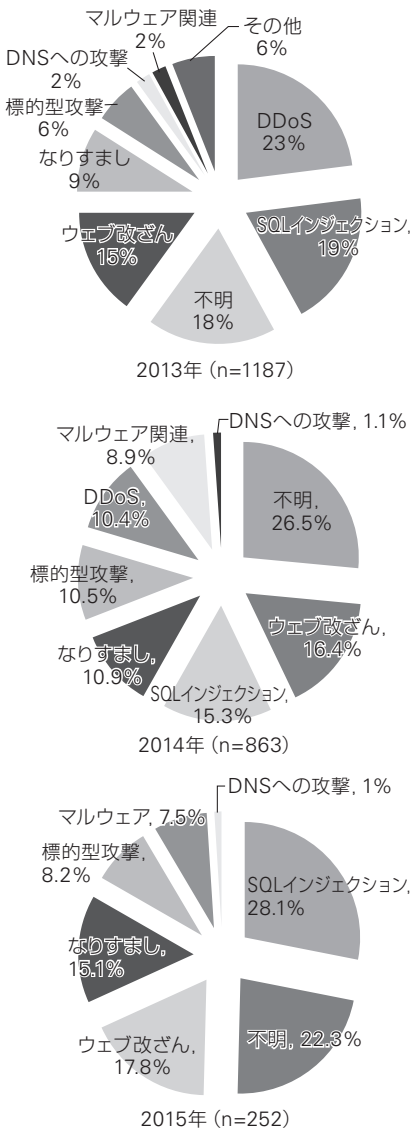
岩井博樹
（デロイト トーマツ リスクサービス株式会社
シニアマネジャー）

近年のサイバー攻撃事案について，一般的な事例，鉄道・航空の事例，オリンピックやサミット，サッカーワールドカップといったビッグイベントの事例の3点について整理した．収集方法は，報道等で公開された情報をベースに，幾つかの企業にヒアリングを実施して情報を追加した．

まず，一般的な事例については，2013年から2015年4月までの海外を含めたサイバー攻撃事例の攻撃手法毎の件数を図―5に示す．3年間の各単年傾向としては大きな変化は見られないが，2013年に23％を占めていたDDoS攻撃被害の件数が年々減少している．原因不明は各年25％程度を占めているが，これらの多くは攻撃者によるログの削除や侵害の発覚に時間を要したことによる証跡の消失と考えられる．SQLインジェクションによる情報漏えいや，Web改ざんも高い割合を占めるが，これらはサービス利用者等の第三者が容易に気づくことができる．また，ほとんどの攻撃は自動攻撃ツールを悪用していると推測されることから，攻撃に悪用されているサーバの対処を行わない限りは，今後も同様の攻撃は続く可能性が高い．「なりすまし」による不正ログインや特定組織を狙った標的型攻撃においては，侵害に気づいていないことも多い．その背景としては，これらのサイバー攻撃の手口や悪用される不正プログラムの巧妙化や，被害組織の初動対応の不備等が主な原因として挙げられるが，今回挙げた件数は氷山の一角でしかないと考えている．また，原因は不明だが侵害を受けたケースが予想以上に多い．いずれもインシデントの発覚時期が侵入から時間が経っており，事例によっては，内部者の不正とサイバー攻撃の切り分けが困難な状況のものもあり，近年のサイバー攻撃への対応の難しさが分かる．一方，攻撃対象について集計したが，結果は海外，国内ともに統一性はなく，どこの業種を狙ったかは特定しづらい．つまり，特定の業種が狙われているというわけではなく，全ての業種が被害にあっている結果となった．この理由の一つとして，攻撃者が昨今話題になっている社会的もしくは政治的な主張をハッキングという行為で表現している「ハクティビスト」と呼ばれるグループであるからという点がある．彼らの攻撃対象は必ずしも明確な理由があるわけではなく，例えばアノニマスの公開されているアタックリストを見ると，ある主張に基づいてはいるものの，イルカをトランスポートしているからという理由で交通機関がターゲットになるなど，結果だけを見ても何が理由で攻撃されているのかがわからない状況となっている．

次に，航空に対する攻撃の事例については，人命に関わる大きなインシデントは報告されていないものの，航空機に対するハッキングへのリスクの報告が年々増加している．また航空会社のオフィスネットワークへの侵害は複数発生しており，外部サービス（クラウド等）も攻撃対象となっている．具体的には，2015年6月のポーランド航空の事案では，飛行計画システムに対するサイバー攻撃があり，欠航や遅延が発生している．また，アメリカの航空券予約システムの運営会社であるセーバー社（SABRE）のサイトに対するサイバー攻撃も報告されている．また，鉄道に対する攻撃の事

岩井博樹



■図―5　近年のサイバー攻撃の傾向

例については，航空よりも件数が少ないが，航空と同様にオフィスネットワークへの侵害が複数発生している．韓国では，2014年に地下鉄ソウルメトロへのサイバー攻撃があったと報道されている．この事案については，具体的な報告があったのは1年以上経過した2015年10月であり，社会インフラを担う機関が侵入された場合，事態の収束に時間がかかるという特徴の一つが明らかになった事案でもある．さらに，交通分野の詳細を見ると，予想以上に侵害が多く，特徴としてホスティング会社やクラウド事業者などへの侵害のように必ずしも攻撃者は直接ターゲットの組織を攻撃しているわけではないようである．従って，サプライチェーンを意識したセキュリティ対策が今後は必要になってくる．

続いて，ビッグイベントの事例については，例えばオリンピックを見ると，大会関係組織に対する攻撃のほか，スポンサーへの攻撃も多い．その攻撃者は大抵ハクティビストによるものである．ビッグイベントを開催する国は基本的に狙われるが，その関係組織も狙われる傾向にある．

次に，クローズドネットワークにおけるサイバー攻撃の事例を紹介する．交通分野やビッグイベントではないが，2011年7月にソフトバンクモバイル株式会社の業務委託先の社員が，業務に使用していた制御用端末に時限式の不正プログラムを入力し，ATMの伝送網に仕掛けてシステムをダウンさせる事件があった．また，海外では，2010年6月にUSBメモリーを介してマルウェアが持ち込まれて，イランの核施設の遠心分離機が破壊された．これらを見ると，重要インフラにおいてクローズドネットワークと言われているものは，クローズドとは言いづらくなってきている状況であると感じている．

最後に，攻撃に対する対応については，第一にインシデントが発生する前提で体制を構築することが必要であり，ダメージコントロールを意識した対策が必要である．第二に攻撃者は必ずしもサーバを狙っているわけではなく，パソコン内のメールのアーカイブから盗み出すだけの事案もあることから，攻撃者の目的理解が必要である．第三に自社で実施している対策がサイバー攻撃のどのフェーズに対して有効であるかを正確に理解することが必要である．ヒアリングではサイバーセキュリティに投資しているという事実だけで満足し，その対策の有効性をあまり理解していない経営者も見られたため，対策内容の理解も重要になる．

3.3 鉄道・航空分野におけるセキュリティに対する事業者意識調査

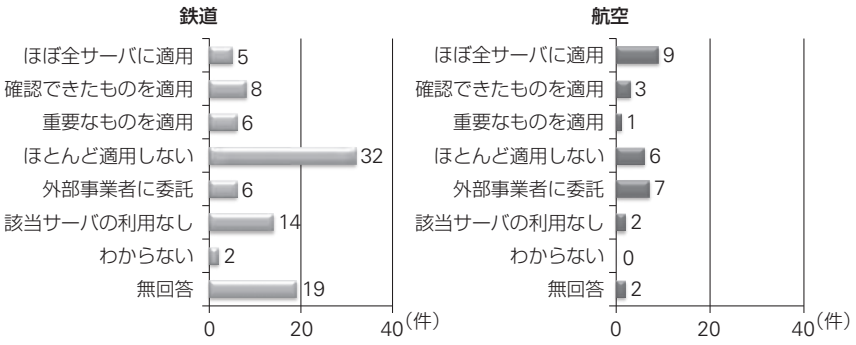
寺田真敏
（株式会社日立製作所
Hitachi Incident Response Team
チーフコーディネーションデザイナ）

交通分野における事業者のサイバーセキュリティへの取組み状況を把握するため，鉄道11社，航空5社に調査協力いただいた．調査項目は，表―2の通りである．また，追加調査として鉄道2社，航空1社に対してヒアリングも実施した．このような交通分野に特化した調査は，これまでに実施されたことがなく，貴重な情報が得られた．本報告では，主な結果を紹介する．

セキュリティ体制の現状は，全16組織のうち，基本的な方針を公開している組織は2組織，CISO（Chief Information Security Officer：最高情報セキュリティ責任者）を専任で配置している組織はなく，兼任で配置している組織が3組織であった．また，会社のセキュリティ対策が組織的に行われていないという回答は3組織もあり，セキュリティ業務の担当者の充足度は，量的，スキル面ともに不足を感じているという回答が半数以上を占めた．この結果から交通分野におけるセキュリティ体制は改善の余地が十分にあると言える．

個別システムにおけるセキュリティは，セキュリティ関連製品，ソリューションの導入，組織面・運用面の対策費用について，「年間100万円未満」と「わからない」という回答が多かった．システム導入時や運用時に投資していると考えられるが，

寺田真敏



■図―6 個別システムのサーバでのセキュリティパッチの適用状況

■表―2　調査項目

【全体編】
・回答企業の概要 ・セキュリティ体制の現状
【個別システム編】 鉄道：列車運行管理，電力管理，営業系，社内OA 航空：運航系，営業系，社内OA
・個別システムの概要 ・セキュリティ対策 ・コンピュータウィルスによる被害状況 ・サイバー攻撃による被害状況 ・被害により生じた損失

個別所管部署では実際にどのくらいの投資がされているかまで把握できていないというのが現状のようである．セキュリティ対策を検討・実施する所管部署は，鉄道と航空で大きく傾向が違い，鉄道では個別システム所管部署が主に担当しているのに対して，航空ではCSIRT（Computer Security Incident Response Team）などの専門組織，社内情報システム部門が主に担当している．特に，航空の場合には，CSIRTのような専門組織で先行的な取組みが行われている．セキュリティ対策に関する人材の育成も，鉄道と航空で多少傾向が違い，鉄道では個別システム所管部署もしくは社内情報システム部門が担当しているのに対し，航空ではCSIRTなどの専門組織もしくは社内情報システム部門が担当している．この傾向は，サイバー攻撃による社外の事件やシステム障害の情報収集の役割分担についても同様である．ただし，追加ヒアリングによれば，情報収集する部署と所管する部署が相互に連携して対策に取り組む例もある．

次に，個別システムについては，鉄道の46システム，航空の15システムのうち，脆弱性検査を実施しているのは，鉄道のシステムでは8件（営業系5件，社内OA2件，電力管理1件），航空のシステムでは2件（運航系1件，営業系1件）であった．特に鉄道の電力管理システムと航空の運航システムで脆弱性検査が実施されていることは先行的な取組みであり，電力管理システムは人手による検査，運航システムはツールを用いた検査と人手による検査である．また，セキュリティパッチは，鉄道のシステムの多くが「ほとんど適用していない」「無回答」「該当サーバの利用なし」であり，航空の傾向とは異なる（図―6参照）．さらに，実際の被害状況は，「ウィルスに感染した」「ウィルスを発見したが，感染には至らなかった」が計14件あったが，いずれも営業系もしくは社内OAのシステムであり，鉄道の列車運行管理，電力管理のシステムや，航空の運航システムでの遭遇報告はなかった．ただし，ウィルスの侵入経路は，USBメモリー等の外部記憶媒体が計10件あり，クローズドネットワーク内にウィルスを持ち込まれる可能性は否定できないことがわかった．

最後に，調査結果をまとめると，第一に組織体制については，専任のCISOを有する事業者はなく，且つセキュリティ対策を担う部門の人数及びスキル面での充足度も不足している．事業者の中には，個別システムの所管部署と社内情報システム部門が連携してセキュリティ対策を進めている事例もあるが，今後の組織体制の強化を考えると，CSRITなどの専門組織を活用した情報収集やセキュリティ対策の検討・実施，人材育成などを，先行的な事例を参考に進められることを期待する．第二に個別のセキュリティ対策については，自社の各システムを通常のクローズドネットワークとオープンネットワークという2つの接続区分ではなく，インターネット公開，インターネット非公開，非接続の3つの接続区分で分類し，脆弱性検査の実施やセキュリティパッチの適用などの対策の必要性を判断したり，一般的にクローズドネットワークと言われるシステムに関して，開発業者に任せているので実態把握が難しいという意見もあるが，資産管理の延長でシステムの潜在的なリスクを把握したりするなど先進的な事例を参考に各社に合ったセキュリティ対策の検討，実施が望まれる．

3.4 海外の鉄道・航空分野におけるサイバーセキュリティの現状

宮　麻里子
（株式会社サイバーディフェンス研究所
情報調査部主任分析官）

海外の鉄道・航空分野におけるサイバーセキュリティの現状を把握するため，欧州と米国で現地専門家へのヒアリング調査と実態調査を実施した．訪問先は表―3の通りである．

まず，各国のサイバー攻撃の被害事例を紹介する．イギリスの鉄道事業者Network Rail社では，混雑状況や運行状況を管理するシステムをクラウドベースで運用していたが，2012年のロンドンオリンピックとパラリンピックの開催時期の

宮　麻里子

■表—3　外国調査の訪問先

【欧州調査】
・ANSSI（フランス国立情報システムセキュリティ庁） ・SNCF（フランス国有鉄道） ・UNIFE（鉄道産業連合） ・Boeing UK ・英国運輸省 ・CERT-UK ・CPNI（英国国家インフラ保護局） ・TfL（ロンドン交通局） ・Network Rail社
【米国調査】
・FAA（米連邦航空局） ・National Defense University（米国防大学） ・MWAA（首都ワシントン空港公団） ・ST-ISAC（地上交通アイザック）

間の時期に2分間ではあるが接続できなくなった．クラウド事業者の対応の遅れもあり，結局，システムダウンは6時間になったが，原因は同じクラウドサービスを利用しているオリンピックとは関係のないケーキ屋がサイバー攻撃を受けたためであった．また，アメリカのワシントンDC周辺の2つの空港を運営している首都ワシントン空港公団では，2015年3月頃にランサムウェアに感染した．同空港公団は，以前からランサムウェアを想定した机上演習を行っていたため，その経験を活かして手順通りにシステム設定の変更などの対処を慌てずに実施できたとのことであった．

次に各国の取組みを紹介する．イギリスでは，CPNI（国家インフラ保護局）が政府間や重要インフラ事業者との調整を担う組織として，セキュリティアドバイスやペネトレーションテスト等の支援を行っているが，アドバイスやテストの実施に関して強制力はないとのことである．ロンドンオリンピックでは「Right First Time（失敗は許されず，一度で完璧にする）」がキーワードになっており，事業者ではソフトウェアアップデートやパッチの適用，ペネトレーションテストの実施などの基本対策に重点が置かれていた．フランスでは，ANSSI（国立情報システムセキュリティ庁）がサイバーセキュリティに関して，政府間や重要インフラ事業者，中小企業との調整を担っているほか，最重要事業者（12セクター，約250社）を指定している．この最重要事業者は，サイバーセキュリティ対策の策定とインシデント報告の義務を負っており，ANSSIは最重要事業者に対する監査やペネトレーションテストの実施の権限などを有している．フランス国鉄は最重要事業者の1社であり，ANSSI認定のセキュリティ機器を導入しているほか，ANSSIあるいはANSSIが認定した事業者によるペネトレーションテストも受けている．アメリカでは，連邦航空局が航空機体等の規制を行っているが，航空に限らず重要インフラに関する実質的な規制はDHS（国土安全保障省）が行っている．また，アメリカではISAC（Information Sharing and Analysis Center）という情報共有組織の形成を推進しており，各重要インフラセクターで脆弱性やサイバー攻撃の脅威に関する情報共有を行っている．ヒアリングを実施した地上交通系ISACには，鉄道や貨物などの鉄道事業者が会員となっているISACや，都市内バスや高速バスなどのバス事業者が会員となっているISACなどがあり，それぞれ専属アナリストが政府からの情報や独自の情報収集により，レポートを作成，配信しているほか，事業者からインシデント情報があった場合は，情報を一部匿名化した上で政府に報告している．この他，IASO（Information Sharing and Analysis Organization）という組織もあったが，この組織は2015年から設置が可能となった新しい組織である．さらに，前述の首都ワシントン空港公団では，従業員は全員バックグラウンドチェックを行った上で採用されており，内部犯行防止を想定した社内ネットワーク監視も行っているほか，ペネトレーションテストは異なる業者で年に2回実施されていた．

最後に各国のネットワークセキュリティに対する考え方を比較する．まず，オープンネットワークとクローズドネットワークの対策を各国に伺ったところ，各国ともに「クローズトネットワークはクローズドだからといって安全ではない」という認識のもとに，あらゆる対策を講じているところが共通していた．その上で，特に印象的であったのは，アメリカの「Don’t trust anything!（何も信用するな）」という原則である．人は特に信用できないが，機器もシステムもネットワークも何も信用せず，当然クローズドだからといって安心もせず，多層防御を行うことは当たり前であるという考え方であった．連邦航空局や首都ワシントン空港公団など多くの重要インフラ事業者が採用しているNIST（米国国立標準技術研究所）のフレームワークVer1.0では，オープン，クローズドに関係なく全てのシステムを評価する必要性が強調されていた．また，イギリスはもともと国家としてテロ対策が優先事項であり，サイバーセキュリティを物理セキュリティを含めた包括的なセキュリティの一部として考えており，内部犯行への対策や意思決定層の教育などといった人の対策も重視しているほか，フランスは政府が主導権を握って，重要インフラ事業者に対してルールを適用し，統制している．さらに，EUでは，鉄道の信号に関するEU統一規格化プロジェクトが進められているほか，2019年に国内旅客市場の自由化が始まるため，今後のEU加盟国の鉄道業界の動向は注視が必要である．

3.5 制御系システムにおける侵入テスト（ペネトレーションテスト）結果の考察

利根川義英
（株式会社キーコネクト代表取締役
セキュリティアドバイザ）

運輸業界の事業者にご協力いただき，制御系システムに対するペネトレーションテストを実施した結果を報告する．制御系システムは一般に外部との接続がないクローズドネットワークであると言われており，かつては専用のハードやソフトが使用されていることから安全であるという認識であった．しかし，前

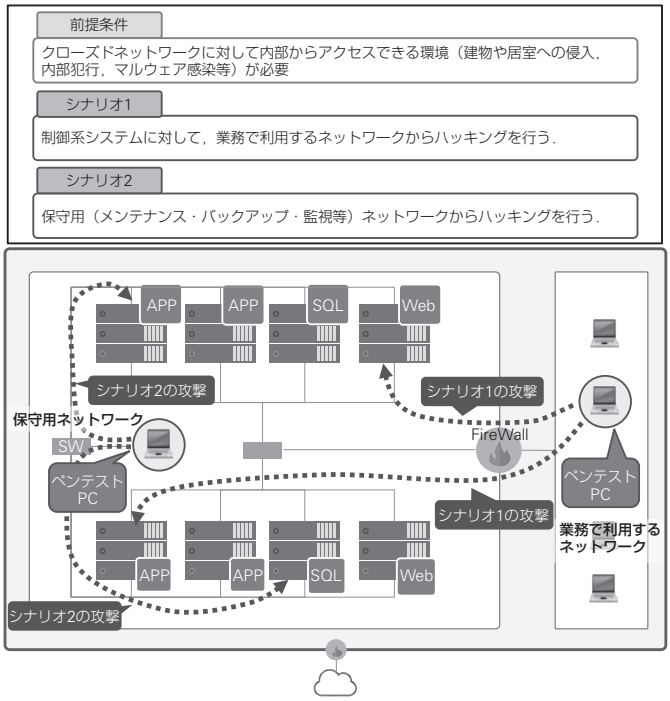
述の事例等を見ると，その安全神話は崩壊しているのではないかと考えている．そこで，今回の検査では，実際の制御系システムを使用して，そのセキュリティ強度を把握することを目的とした．

まず，ペネトレーションテストについて説明する．ペネトレーションテストは，脆弱性検査とは少し異なり，文字どおり「侵入」つまり攻撃を行うことで侵入につながる問題点を発見するものである．具体的には，ネットワークに対するテストと，ネットワーク上に存在するアプリケーションに対するテスト（Webシステムやアプリケーション等）がある．つまり，ネットワークだけではなく，監視のシステムやユーザーの管理する専門のシステムといった，あらゆるアプリケーションに対してハッキングが可能かどうかをテストするものである．実は，システムに脆弱性があったとしても，ハッキングに適していないものも多くあり，脆弱性検査ではこのような脆弱性も挙げられるが，ペネトレーションテストはハッキングに適した脆弱性を優先的に見つけていくのである．

具体的なテストの流れを簡単に説明すると，まず通信内容をチェックしてネットワーク内に存在する端末の存在確認を行い，次にそれらがどのような役割や機能を持つものなのかを調べていき，得られた情報をもとに実際にハッキングを行ってみるという手順で進める．この作業は，定められた手順ではなく，トライアル・アンド・エラーの連続で，実際のハッキングのように進める．

今回のテストは，大規模なものであったため，内部からのアクセスが可能であるという前提条件の上で，図―7に示した2つのシナリオを検証した．結果は，まずシナリオ1では，古いOSの使用やパッチ適用不足等の問題があったものの，侵入に繋がるような脆弱性は検出されなかった．制御系システムは大規模であり，24時間365日運用されているものも多いため，古いOSが使用され続けていたり，パッチの適用が不足していることは当たり前の結果ではあるが，その条件下であっても侵入できなかったという結果であった．一方，シナリオ2では，残念ながら侵入に成功することができた．これは，アプライアンス製品等の設定が初期設定のままであり，弱いパスワードの利用と使い回しにより，ネットワーク内の監視システムに対してハッキングが可能であったという結果であった．つまり，内部からのアクセス可能な攻撃者がネットワークにパソコンを接続してハッキングを行ったところ，監視システムを任意に操作することに成功したということである．ただし，これを可能にするためには，内部からのアクセスが可能であるという前提条件が必要であり，具体的にはシステムのある建物内への物理的な侵入や，社員や協力会社社員などの内部犯行，ネットワークに接続する端末のマルウェア感染といった要因がなければ実現できない．これらを発生するはずがないと捉えるのではなく，十分起こり得る前提であると捉え，必要な対策，警戒，予防の措置をとっていく必要がある．その上で，このようなペネトレーションテストを適切に，且つ定期的に行い，システムの堅牢性を向上させていくことが重要である．

利根川義英



■図―7　前提条件とシナリオ

4――特別講演2
交通機関を中心とした重要インフラ事業者が直面するサイバー脅威

名和利男
（株式会社サイバーディフェンス研究所
専務理事/上級分析官）

インターネット及び情報通信技術の急激な発展と，それに対する投資によってネットサービスやデバイスの広範囲への展開と積極的な利用が実現したことにより，国家や反社会的勢力（テロ組織やマフィア等）が，その状況を悪用する形で，旧来の実力手段の支援的役割としてサイバー攻撃が実際に発生し，その頻度は

高まっている．また，敵対する国家や反社会的勢力が，特定の国家の貶め，あるいは国力低下を狙って実力的行使に出る場合，交通機関の機能低下を狙う傾向が現れ始めている．このような状況で昨年，韓国ソウルの地下鉄を運営する「ソウルメトロ」の複数のサーバが北朝鮮からと推定されるサイバー攻撃を受けていたことが明らかになった．報道では，この攻撃による交通網への影響はなかったと伝えられているが，今後の進展次第では予断を許さない状況になる可能性がある．そこで，この韓国の鉄道における一連のサイバー攻撃について以下に情報を整理する．

2013年11月，韓国鉄道公社(KORAIL)の子会社であるコレイルネットワークスでは，北朝鮮と推測されるハッカー組織により，内部の業務ネットワークに侵入された．これを皮切りに，2014年以降も，韓国の鉄道などの国の主要な基盤施設に対するサイバー攻撃が継続的に試行され，2014年8月には，韓国鉄道公社の内部コンピュータネットワークが侵入された．韓国の国会議員の報告によると，ネットワーク構成を含む主要な情報通信基盤施設の点検計画書などの公文書53件が流出し，北朝鮮による犯行と推測されるということであった．

また，2015年7月，ソウル特別市で地下鉄1～4号線を運営するソウルメトロは，業務用PCの3台で，業務計画など12件の資料が流出したことを確認した．調査の結果，少なくとも2014年3月より以前から，5カ月以上ハッカーによりネットワークが掌握されている状況が続いていたことが確認され，PCの悪性コード感染58台，PCへの不正アクセス（非正規ユーザによるアクセス）213台，サーバの権限奪取2台，および業務関連資料12件の流出が確認されている．なお，一連のサーバ攻撃の手法は，2013年3月KBS・MBCなどの放送局，新韓銀行・農協などの金融機関をハッキングした手法と同じであるとのことである．

名和利男

さらに，2016年1月27日，韓国のホワイトハッカーグループであるIssueMakersLabは，北朝鮮の4回目の核実験が実施される直前に，北朝鮮とみられる攻撃者が韓国国内の地下鉄の制御系システムに使われる部品を開発する企業のホームページをハッキングした後，サイバーテロの「前線基地」として利用していた，とメディアに伝えた．IssueMakersLabの発表によると，2015年12月初め，北朝鮮の偵察総局は，自動列車制御装置（Automatic Train Control：ATC）部品の開発メーカであるA社のホームページをハッキングし，内部ネットワークの管理者権限を奪取した．そこから，A社のサーバを，マルウェアの侵入経路や，取得するファイルの選択，窃取したファイルの送信先などの指令を下す中継地（C&Cサーバ）として利用したとされている．A社が開発した自動列車制御装置は，鉄道信号保安装置の電子列車制御装置の一種で，列車の速度制御などに関与しているCPUが含まれているコンピュータ装置である．現在，韓国の複数の地下鉄事業者が利用しており，韓国の地下鉄の運行に何らかの打撃を与えるための事前準備なのではないかという分析も出ている．IssueMarksLabは，「もし北朝鮮がそのATC装置で使用する信号の周波数と通信プロトコルをハッキングして，地上装置と車上装置との間の信号に細工するなどして，速度制御の誤作動を誘発させた場合，列車のスピードの急上昇や急停止など，鉄道事故を発生させる可能性もある」と指摘している．

これら一連のサイバー攻撃を見ると，1つの事業者をターゲットにするのではなく，業界内や事業者からの委託業者，再委託業者にまで攻撃の手が伸びている．特に小さな部品を供給しているのは中小企業であり，そのシステムは堅牢ではない場合が多いが，今後は自社システムだけなく，製造や保守のサプライチェーンも考慮した対策が必要である．また，交通分野のシステムは，インターネットと完全に隔離された閉鎖網で運用されていたが，最近は，一部領域あるいは限られた時間にインターネットと接続するシステムとの連携が始まっている．さらに，内部のシステムは，インターネットでよく利用されている技術が多用され始めている．しかし，そのインターネットと直接的もしくは間接的に連携する部分において，情報通信技術の領域で経験されてきたサイバー攻撃対処の知見やノウハウが十分に生かされていない状況が散見される．攻撃者が，そのようなセキュリティ上の弱点に目をつけ，持続的なサイバー攻撃をしかけることは，ごく自然な成り行きであるとも言える．

2020年の東京オリンピック・パラリンピックは，2012年のロンドンオリンピック当時とは比較にならないハンディキャップを負いながら，攻撃者と対峙しなければならない．まずは布石として，今年のG7サミットでの対応が必要となる．今後は，2020年に向けて，日本が得意な密な連携をもとに，飛躍的な対処をしていかなければ，非常にインパクトのある攻撃を受けてしまうという危機感を交通分野の皆様にも持っていただき，これまで以上の監視と現状のキャッチアップをした上で，サイバーセキュリティの検討が進むことを願っている．

（本稿は，講演内容を一部省略したものである．）

（とりまとめ（調査室）：西村潤也）