Vol.2015-CSEC-71 No.1
2015/12/4

2020 年オリンピックに向けた サイバーセキュリティ／テロの考察

内田勝也[†1]

概要：2020 年の東京オリンピックでは、色々な局面でコンピュータが利用されるが、前回 1964 年の東京オリンピック時に利用されたコンピュータとは、全く異なる様相になると思われる。 前回は、物理的対応が中心であったが、今回はサイバーセキュリティ等を含めた、総合的な対策を考える必要がある。
最近の大規模自然災害を想定した物理的対策は勿論のこと、サイバー攻撃をしかける団体・個人への対策も考える必要がある。 セキュリティ技術だけでなく、人的な対策を含めた包括的な対策、多重防御を考えることが必要であろう。

キーワード：サイバーセキュリティ，情報セキュリティマネジメントシステム，情報セキュリティ心理学

Research for Cyber security/Cyber terrorism towards 2020 Olympic Games

KATSUYA UCHIDA[†1]

Keywords: Cyber Security, Information Security Management System, Information Security Psychology

1. はじめに

2020 年東京オリンピックでは、色々な局面でコンピュータが利用されるが、前回 1964 年の東京オリンピック時に利用されたコンピュータとは、全く異なる様相になると思われる。 前回は、物理的対応が中心であったが、今回はサイバーセキュリティ等を含めた、総合的な対策を考える必要がある。

最近の大規模自然災害を想定した物理的対策は勿論のこと、サイバー攻撃をしかける団体・個人への対策も考える必要がある。 セキュリティ技術だけでなく、人的な対策を含めた包括的な対策、多重防御を考えることが必要であろう。

本稿では，主に人（セキュリティマネジメント，セキュリティ心理学等）を中心に考察を行う．

2. リスクを考える

セキュリティを考えるには，まず，リスクを考える必要があるが，それには，情報資産，脅威，脆弱性の 3 つを考える必要がある．

(1) 情報資産

情報資産には，大きく４つあり，これらのどれかが欠けても，サービスを提供できなくなる可能性がある．

① 人間： サービス業務の実行等を行う．
② 情報： 情報やデータは単独で見えるものでなく，コンピュータや記録媒体等に保存される．
③ 技術： ソフトウェア，ハードウェア等
④ 設備： 電源設備や空調設備等が該当する．

(2) 脅威

どの様な脅威があるかは，従来からのリスクを考え，その脅威をリストアップする必要があるが，それだけでなく，新たな脅威を考えなければならない．しかし，いずれの場合でも，情報資産に対するものだが，新たな情報資産や従来対象としていなかった情報資産への考察が必要になる．

(3) 脆弱性

脆弱性を考えると，いくつかのものがあるが，インターネットに接続されているソフトウェアの更新をしていない指摘が会計検査院から報告されている[1]．これ以外にも，パッケージソフト等の脆弱性パッチを放置したため，情報漏えいが発生するケースもある．

また，従来からあったが，最近，頻繁に利用されるものに人間の脆弱性を突いた攻撃が増加している．

3. サイバーセキュリティ／サイバーテロ

3.1 サイバーセキュリティとは？

サイバーセキュリティに関し，その基本理念や国の責任範囲を明確にし，施策の基本的事項の取り組みや体制の設置などを求めるサイバーセキュリティ基本法[2]が，2014 年 11 月に成立し、同月，公布・施行された．この基本法では，「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式[a]

[†1] 情報セキュリティ大学院大学
Institute of Information Security

a 「電磁的記録方式」という

により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体[b]を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう，と定めている．

この定義では，サイバーセキュリティは，電磁的方式による記録であり，印刷や手書きの情報を含まない．

3.2 テロ（テロリズム）とは？

テロという言葉は，和製英語であり，英語では「テロリズム(terrorism)」であるが，テロは大昔からあるが，テロの定義は時代により変化しており，また，現在でもいくつかの定義があるが，以下に，米国での 2 つの定義を示す．

2001 年 9 月の米国同時多発テロの発生後に，ブッシュ大統領は，「大統領令 13224 号」を発したが，そこでは以下の様に定義している[3]．

i 暴力行為、又は人命、財産若しくは施設にとって危険な行為を含む。
ii 次のいずれかを意図することが明らかに認められる場合
iii 民間人を脅迫し、又は威圧すること
iv 脅迫又は威圧により政府の政策に影響を与えること
v 大量破壊、暗殺、誘拐又は人質行為を行うことにより政府の行動に影響を与えること

更に，2001 年 10 月に米国愛国者法（PATRIOT Act）[4]が制定され，そこでは以下の様に定義している[2]．

(1) **「国際テロリズム（international terrorism）」とは、次の活動をいう。**
(A) 暴力行為若しくは人命に危険を及ぼす行為であって、合衆国若しくは州の刑法の違反となり、又は、合衆国若しくは州の裁判管轄地内で行われたときは犯罪行為となるものに関わる活動
(B) 次のいずれかのことを意図することが明らかに認められる活動
i 民間人を脅迫し、又は威圧すること。
ii 脅迫又は威圧により政府の政策に影響を与えること。
iii 大量破壊、暗殺又は略取誘拐により政府の行動に影響を与えること。
(C) 実行の手段、脅迫若しくは威圧の対象とされていることが明白に認められる者、又はその実行犯が活動し、若しくは潜伏先を探し求めている場所の観点から、主として合衆国の領域的裁判管轄権の外で、又は国境を越えて生起する活動

(2) **「国内テロリズム（domestic terrorism）」とは、次の活動をいう。**
(A) 人命に危険を及ぼす行為であって合衆国又は州の刑法の違反となるものに係わる行為
(B) 次のいずれかのことを意図することが明らかに認められる活動
vi 民間人を脅迫し、又は威圧すること。
vii 脅迫又は威圧により政府の政策に影響を与えること。
viii 大量破壊、暗殺又は略取誘拐により政府の行動に影響を与えること。
(C) 主に合衆国の領域的裁判管轄権の内で行われる行為

3.3 サイバーテロとは？

サイバーテロは，一言で言えば，「サイバー空間でのテロ」であるが，これも定まった定義はない．国内での定義として，総務省と警察庁の定義を示す．

総務省[5]の定義は，1987 年に定めたもので，30 年近く前のものだが，具体的な記述がされている．

(1) **総務省のサイバーテロの定義**
(A) サイバーテロは、コンピュータウイルスやハッカーによって個人が被害を受けるものとは異なり、国家等の重要システムを機能不全に陥れるものであることから、この指針におけるサイバーテロの定義は、「ネットワークを通じて各国の国防、治安等をはじめとする各種分野の情報システムに侵入し、データを破壊、改ざんするなどの手段で国家等の重要システムを機能不全に陥れる行為」とする。
(B) 攻撃対象となる重要インフラ
サイバーテロの攻撃対象となった場合、その産業、企業のみならず、広く国民生活に重大な影響が及ぶこととなる重要インフラとして、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）等が想定される。
(C) 重要インフラの相互依存性
各重要インフラは、他の重要インフラと独立して存立するのではなく、相互に依存し存立しており、ある重要インフラが攻撃を受けた場合、関連する他の重要インフラも影響を受ける場合が多々あることから、重要インフラを保有してサービスを提供する事業者は、他インフラへの影響も考慮した対策が必要である。
(D) サイバーテロでの主な攻撃方法
サイバーテロにおける主な攻撃方法の具体例としては、次のものがある。
① 物理的な攻撃

b 「電磁的記録媒体」という

電気通信施設に不正侵入し､ネットワーク管理センターを占拠する等によりネットワークのコントロールを奪い、これをまひさせるような攻撃

② ホームページ改ざん
思想的な意図等により社会に広くアピールするため、ホームページの掲載内容を改ざんするもの

③ 分散型サービス妨害攻撃
ネットワーク上にある複数のコンピュータから,攻撃先のサーバー等に一斉に攻撃を行うもので,攻撃対象のサーバーのサービス提供に影響を与える.

④ 複数の場所からサーバーの処理能力を超える大量のデータを送り付けるなどの方法によりサーバーを停止させるもの

⑤ コンピュータウイルス
強力な感染力と破壊力を持つウイルスによる攻撃

⑥ 不正侵入（なりすまし）
他人になりすまして侵入し､データの改ざん､削除を行うほか、他への攻撃にも使用

(2) **警察庁[6]は，以下のように定義している.**

サイバーテロとは、重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いものをいいます。サイバー犯罪の中でも国民生活に直接の甚大で深刻な被害を及ぼす危険性があると考えられています。

現在までのところ、サイバーテロであると確認された事案はありませんが、平成 17 年 2 月から 4 月にかけて、中央省庁等の Web サーバーに対して大規模なサイバー攻撃が行われ、一時的に Web サイトへの接続が困難な状況になるなど、重要インフラの基幹システムに対するサイバーテロの脅威が現実のものとなってきています。

(3) **サイバーテロは起こるのか？**

最近の大規模情報漏えいや機密情報の漏えいの影響と2020 年のオリンピックなどからか, サイバーテロがあるのではないかとの話がある.

個人的には，国内外でインシデントは，サイバーテロでなく,「サイバー攻撃」という言葉が適当ではないかと思われる．これは，テロの定義自体も明確でなく，サイバーテロと言えるようなものとは思えない面があるためである.

4. サイバー攻撃について

数年先だが, 2020 年を見据えたサイバー攻撃を考えることはたやすいことではないが，過去の事例から類推することは１つの方法としてある.

現在，存在するが，大きく変化がでる可能性のあるものや，現在は存在していないが，今後，導入されると思われる機器やソフトウェア等の課題を考えることも必要になる.

2010 年頃を考えてみると，現在の状況をあまり大きな変化はなかったように感じる．但し，インターネットでの話題としては，IoT（Internet of Things）が大きなうねりになっており，その脆弱性についての課題も指摘されている．2020 年を考えると IoT を無視することはできないと考えている.

また, AI 技術の発展により, 従来は人間が単独あるいは，機器やソフトを利用して，攻撃を行っているが，機器やソフトが攻撃をする可能性もある．既に，会話ロボが人間に対応しているケースがあることを考えれば，ロボットが人間を攻撃することがでてきても不思議ではない[7].

4.1 サイバー攻撃対象

サイバー攻撃の対象は, 4 つの情報資産が対象になるが, 個々の情報資産に対してだけでなく, いくつかの情報資産を含めた考える必要がある.以下に主な攻撃について列挙する.

(1) **人間への攻撃**

情報セキュリティで最も弱い部分は,人間であると言われており，人間の弱さをついて，ユーザ ID／パスワードや個人情報を入手する[c] [d].

チャルディーニは人間には以下の 6 つの脆弱性（①返報性，②コミットメントと一貫性，③社会的証明，④好意，⑤権威，⑥希少性）があると指摘している[8].

最近は，多くの攻撃者が，人間への攻撃，ソーシャルエンジニアリングを併用して攻撃しているとも言える.

(2) **人間・情報・技術への攻撃**

ソフトウェアの脆弱性パッチが自動更新されるようになると,正当な方法を使った攻撃の可能性が増えている.

① 標的型直接攻撃： 電子メールで, 添付ファイルを持ったものや本文に URL が記述してあり,添付ファイルや URL をクリックしたくなるものを送る.

② 標的型間接攻撃： いわゆる「水飲み場攻撃」をしかけ，攻撃対象企業の社員等のウェブブラウザー等の脆弱性を利用し，「ドライブバイダウンロード」により，マルウェアをインストールする.

③ 不特定多数への攻撃：マルウェアを添付したメールの添付やワーム等が直接送付される場合もある.添付ファイルのメールの場合には，基本的には①

c 1994 年 11 月に CSI(Computer Security Institute)主催の Annual Conference の Night session,「Meet the enemy（ハッカーと語ろう)」というハッカーとセキュリティ担当者の電話会議（Tele-conference）で，ハッカーが会議に割り込んできた電話会社のオペレータから, ユーザ ID とパスワードを聞き出したことがあった

d 2012 年 11 月に発生したストーカー殺人事件では，依頼された調査会社の経営者は被害女性の住所を聞き出すため，被害女性の夫を装い，当該自治体に電話をかけ，対応職員から正確な住所を聞き出した

と同じで，メール受信者（被害者）が興味を持ちそうなタイトルやメッセージが送られ，添付ファイルをクリックするとマルウェアが起動し，他のパソコンに感染を広げ，情報漏えいや情報を削除したりする．

ワームの場合には，ネットワーク上を勝手に動き，ソフトウェアの脆弱性を利用して感染を広げる．感染により，情報盗取や情報改ざん，削除等を行う場合と，DDoS 攻撃の「エージェント」の作成等にも利用される．

(3) 設備への攻撃

設備へのサイバー攻撃は，なりすまし等のソーシャルエンジニアリング欺術を使って，施設への侵入をはかり，設備への直接的な攻撃を行うことや電力や通信機能を外部の供給部分を遮断することもある．

意図的でなくても，発生した事故やそれを模倣すれば，電力や通信に障害を発生させることが可能になる．

① 世田谷ケーブル火災： 1984 年 11 月に当時の世田谷電話局前の洞道内の作業中に，バーナーの火がケーブルに引火し，火災が発生し，世田谷局収容の固定電話約 89,000 回線が不通に[9]．また，三菱銀行等のデータセンターが世田谷局管内にあったため，オンラインが停止した[10]．

② 集中豪雨： 2015 年 9 月に発生した「関東・東北豪雨」では，利根川支流の鬼怒川の左岸が決壊し，茨城県常総市が大きな被害をうけたが，3 階建ての常総市役所も浸水し，1 階が被害を受けただけでなく，非常用発電機と燃料タンクも敷地内に置かれていたため，2 時間程度しか稼働しなかった．浸水ハザードマップでは，市役所も 1～2 メートルの浸水を想定していたが，対策がされていなかった[11][12]．

③ STUXNET： 外部のネットワークに接続されていない核施設内の遠心分離機のソフトウェアに感染し，機能停止に追い込んだ[13]．

なお，最近の IoTeの普及により，多くの機器がネットワークに接続されることになり，それらの脆弱性が攻撃対象になり，大きな障害になる恐れもある[14]．

4.2 ソーシャルエンジニアリングについて

セキュリティで最も弱い部分は，「人間」であり，攻撃者は人間の弱さをついて，正規の権限を入手したりして，目的を達成する．攻撃者は，電子メール，電話，対面等，色々な方法を用いて攻撃を行う．

① 誘導質問術： 他の人に対する特性を利用して，特定の目的，即ち，容易に入手できない情報を対象者（被害者）に疑いを抱かせずに収集する，

② なりすまし： 他人になりすまし，情報の収集や施設に侵入して，情報収集を行う．

③ のぞき見： 肩越しに，パソコンやスマホの画面を覗き，情報を収集する．但し，簡単な実験を行ったが，英数字の 8 桁程度の入力でも記憶することは簡単ではない．このため，ビデオや写真を撮り，それを確認して情報を得る可能性が高い．

④ ワーム送付: 特定あるいは多くの人が興味を示すと思われるタイトルやコメントを書いたメールにファイルを添付して送付し，クリックさせるもの．

⑤ APT 攻撃： 特定の組織や個人を標的に，複数の攻撃手法を組みあわせて執拗かつ継続的に攻撃を行うもの．

⑥ 水飲み場攻撃：攻撃対象企業の社員等のウェブブラウザー等の脆弱性を利用し，「ドライブバイダウンロード」により，マルウェアをインストールする．

5. サイバー攻撃対応について

サイバー攻撃に対して，技術的な対応だけでなく，人間が行う対応も必要になる．

個人やグループを対象とした対応と組織（関係する複数の組織）として対応する必要もある．

5.1 教育・訓練によるサイバー攻撃対応

① 標的型攻撃訓練： 添付型標的型攻撃訓練では，事前の情報提供をしない場合は，約 40%が添付ファイルをクリックするが，2 年後に実施した場合，12.5%がクリックした[15]．米国では，2 ヶ月毎の訓練では 12%，毎月訓練では 4%のクリックとの調査もある[16]．

② ゲーミフィケーション: ゲームデザイン技術や仕組みを利用した教育で，参加者の順位，獲得ポイント，取得レベルバッジ等を明示することにより，楽しみながら，関連知識を習得する．

③ 新教育・訓練： 従来の一方通行型の集合研修でなく，チーム単位での実習形式やチーム力の重要性を事例(他の訓練やビデオ等)から修得するもの．

セキュリティ教育・訓練による効果は，実際に起こった時に対応できること，即ち，参加者が「行動変容」を起こさないと意味がないが，通常の教育・訓練では，行動変容を起こすことができたかの判断をすることは難しい． そのため，実際に行った教育・訓練内容について，効果が高かったかを判断する方法になる．

教育・訓練内容については，上記の①や③では比較的効果が高い結果を得ている．

e Internet of Things：「モノのインターネット」と呼ばれ，あらゆるものがインターネットに接続され，情報交換により，相互制御される

5.2 サイバー攻撃に対する組織的対応

サイバー攻撃への対策として,組織的な対応も必要になる． 最近は，CSIRT 組織の構築が必要であるとの考えがあるが,組織的な対応で最も重要と思われるものは,「PDCA」サイクルが適切に回っているかであろう．

日本年金機構での大量情報漏えいでも,監督官庁である厚労省は，CSIRT 体制を構築していることになったが，実際には担当者を決めただけで，全く機能していなかった．どんなに立派な組織体制を決めても，その運用が適切に行われていなければ,組織体制がないのと同じであろう．

CSIRT を補完あるいは，支援するものに，情報セキュリティマネジメントシステム（以下,「ISMS」という）がある．

ISMS では，リスクファーストの考えと PDCA サイクルが中心だと考えられる．

表 1 は，ISMS 要求事項の主要部分と「管理目的及び管理策」を示した．

① 計画： リスクアクセスメントを行い，附属書 A の管理目的／管理策を定める．
② 支援： 必要とするリソース等を定め，適切な力量を定め，要員を配置する
③ 運用: 意図した成果を達成するための運用を行う．
④ パフォーマンス評価： 監視・測定等を行うとともに，内部監査を実施し，有効性の評価を行うマネジメントレビューを行う．
⑤ 改善： 不適合や是正処置を行い，継続的な改善を行う．

表 1 ISMS 要求事項の構成（主要部分のみ）

- 組織の状況
- リーダーシップ
- 計画
- 支援
- 運用
- パフォーマンス評価
- 改善
- 附属書A 管理目的及び管理策
  - A.5 情報セキュリティのための方針群
  - A.6 情報セキュリティのための組織
  - A.7 人的資源のセキュリティ
  - A.8 資産の管理
  - A.9 アクセス制御
  - A.10 暗号
  - A.11 物理的及び環境的セキュリティ
  - A.12 運用のセキュリティ
  - A.13 通信のセキュリティ
  - A.14 システムの取得，開発及び保守
  - A.15 供給者関係
  - A.16 情報セキュリティインシデント管理
  - A.17 事業継続マネジメントにおける情報セキュリティの側面
  - A.18 順守

6. 終わりに

2020 年オリンピックに向けて，サイバー攻撃が間違いなく増えることになるが，本稿では，人的セキュリティへの考察を行った．

システムの脆弱性を利用したマルウェア（含標的型攻撃）も考えられるが，脆弱性パッチの自動更新が一般的になれば，もっと簡単な攻撃，即ち，ソーシャルエンジニアリング攻撃が必ずあると考えられる．

標的型攻撃のようなものから，電話，SNS，対面等で攻撃のための情報を盗取できれば，技術的な脆弱性を探すより，遙かに簡単にシステム侵入や情報盗取，情報破壊などができるものと考える．

人的セキュリティについて，さらに調査・研究を深めていきたい．

参考文献

1) 会計検査院，平成 26 年度決算検査報告の概要，http://www.jbaudit.go.jp/report/new/summary26/pdf/fy26_zumi_260.pdf
2) サイバーセキュリティ基本法 http://law.e-gov.go.jp/htmldata/H26/H26HO104.html
3) 清水隆雄,テロリズムの定義：国際犯罪化への試み，http://dl.ndl.go.jp/view/download/digidepo_999872_po_065702.pdf?contentNo=1&alternativeNo=
4) 平野美恵子他，米国愛国者法（反テロ法）（下）http://www.ndl.go.jp/jp/diet/publication/legis/215/21501.pdf
5) 総務省，情報通信ネットワーク安全・信頼性基準，1987 年
6) 警察庁，サイバーテロ犯罪・サイバーテロの現状，@Police，https://www.npa.go.jp/cyberpolice/cyberforce/cyberforce01.html
7) 瀧口 範子，男性の相手は「会話ロボット」、不倫サイトが見せた技術力，2015 年，日経 BP，http://itpro.nikkeibp.co.jp/atcl/column/15/060200138/091700016/
8) チャルディーニ，R.B，社会行動研究会訳，影響力の武器，2014 年，誠信書房
9) NTT 東日本，世田谷局ケーブル火災（昭和 59 年 11 月），https://www.ntt-east.co.jp/saigai/taisaku/case_06.html
10) 中林一樹他，1984 年世田谷局洞道内通信ケーブル火災事故の社会的影響，第 25 号，1985 年，総合都市研究
11) 毎日新聞，関東・東北豪雨:茨城・常総市役所設備水没 非常電源を全国調査 消防庁，2015 年，http://mainichi.jp/shimen/news/p20151012ddm041040129000c.html
12) 常総市 洪水ハザードマップ 鬼怒川，2015 年，http://www.city.joso.lg.jp/ikkrwebBrowse/material/files/group/6/00705.pdf
13) Wired，核施設を狙ったサイバー攻撃『Stuxnet』の全貌，2012 年，http://wired.jp/2012/06/04/confirmed-us-israel-created-stuxnet-lost-control-of-it/
14) 日本経済新聞，クライスラー、ハッキング対策で 140 万台リコール ソフト更新し遠隔操作防ぐ，2015.07.25. http://www.nikkei.com/article/DGXLASGM25H19_V20C15A7MM0000/
15) 高橋邦夫、豊島区における情報セキュリティ啓発活動、2015、ISC 電子自治体研究会
16) Spitzner L.、Measuring Change in Hum an Behavior、2014、RSA Conference