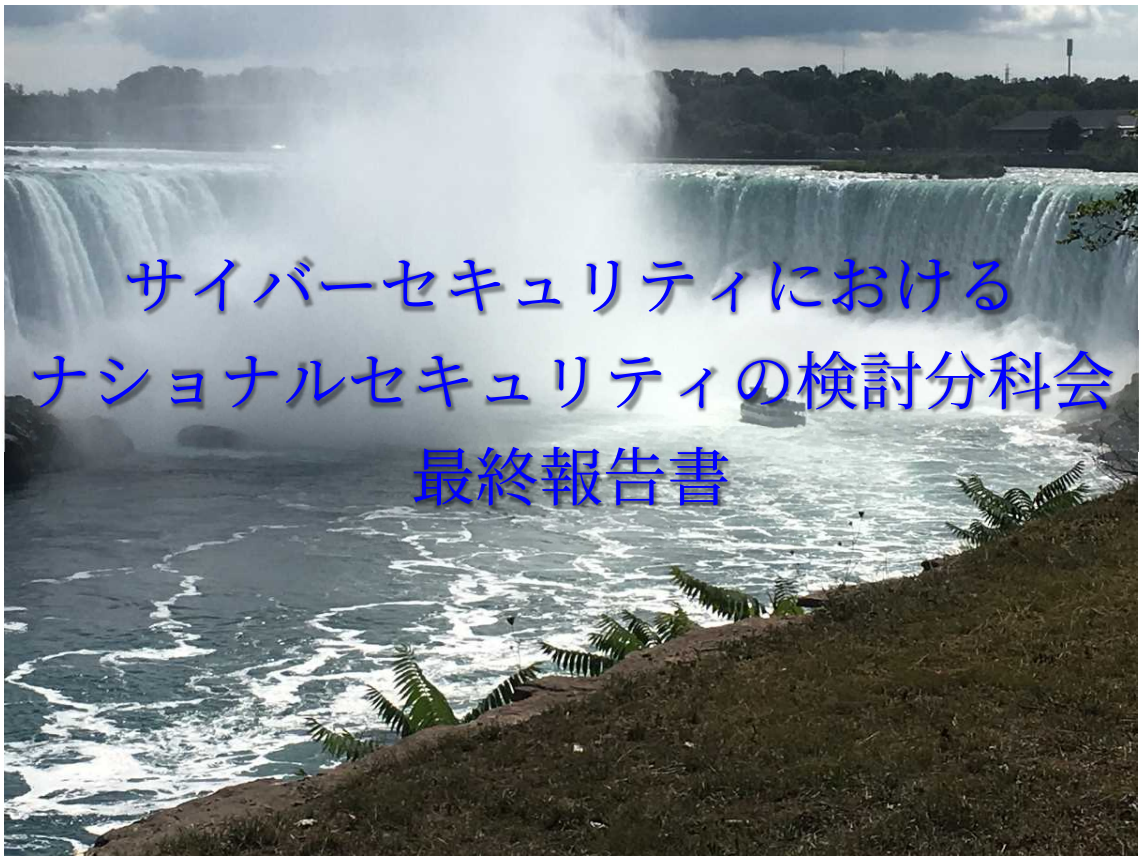


サイバーセキュリティにおける
ナショナルセキュリティの検討分科会
最終報告書

2019 年 7 月 1 日

目　　次

報告書概要

情報通信システムの発展やインターネットの普及は業務形態を大きく変えてきた。

政府・行政サービス、重要インフラ等のネットワークだけでなく、スマートフォン等の適切な利用や民間企業におけるサプライチェーンにおけるサイバーセキュリティの課題も浮上している。

5G の出現は、IoT (Internet of Things）の発展を促すが、同時にネットワーク機器等のセキュリティ問題も引き起こす。

このような現状を踏まえ、2 年間の検討を報告書（提言書）にとりまとめた。

1 セキュリティ政策の確立

(1) 政策の立案・遂行は重要な事柄であるが、『秘すれば花』と考え、情報を内部に抱える傾向が強く、セキュリティの脆弱性では、『知らぬは利用者ばかり』のことが多い。直接的な関係者だけでなく、広く『ステークホルダー』に対し、周知することで、『セキュリティ文化の確立』への道が開ける可能があり、ロードマップの作成・更新はその主要課題である。

(2) 中央官庁、自治体、独立行政法人等では、集中化やリスクに基づいたセキュリティ対策が必要になる。また、米国政府高官が、私用スマホ等の機器利用の不適切さも明らかになり、国内でもその対応が急がれる。

(3) 少子高齢化、人口減少は喫緊の課題であり、サイバーセキュリティ対策にも大きな影響をもたらす。セキュリティ人材は、技術者だけでなく、個人や中小企業を含めたセキュリティ対策要員が必要であり、オンラインによる教育・訓練、高齢者の有効活用を考える必要もある。

(4) 巨大地震やスーパー台風、集中豪雨等が日常化しており、物理的対策も重要になっている。電気、通信が途絶えれば、情報通信システムも機能を果たせなくなる。

2 政府・自治体、重要インフラのサイバーセキュリティ強化

(1) 小規模自治体や独法等では、厳しい要員確保を考え、都道府県を越えた集約化が必要。

(2) 世界的な緊張感が高まりは、サイバーセキュリティの世界にも影響を及ぼす。国家元首のパロディ映画から映画会社への壊滅的なサイバー攻撃を受けており、地政学的な緊張がサイバーの世界に影響を及ぼすことも考える必要がある。

3 事故調査委員会の設置

(1) 現在、航空、鉄道、船舶の事故や重大インシデントの原因究明を専門官がいるが、サイバーセキュリティの「事故調査委員会」設置が望まれる。セキュリティ事件・事故でも、業務処理等が有効かの判断は可能であり、適切な調査により、以降の事件・事故を防ぐことは可能である。

4 機器等の検証システムの確立

(1) 微細なチップによる情報漏えいもあり、また、多くの機器はソフトウェアの更新をインターネット経由であれば、製品製造時だけでなく、事後にバックドアを挿入することも可能であり、機器の導入時やソフトウェア更新時の検証が必要になる。

(2) 導入機器の事前検証も必要になり、機器選定も大切になる。

5 認証制度改革

(1) 認証制度は『制度』と『管理・運用』があるが、国内課題は、管理・運用を適切に行う仕組み作りが必要で、そのための要員（審査員等）や認証取得企業への周知が大切。

6 IoT システムの安全性確保

(1) IoT のセキュリティでは、対応者や対応方法を考える必要がある。

(2) 一部の IoT 機器は、『軽量暗号』を搭載し、セキュリティを高めることが可能であるが、機器作成時に組み込むことになるが、標準の軽量暗号が決定していないため、現時点で搭載する場合、注意が必要。

(3) 脆弱性対応ソフトウェア（パッチプログラム）が未公開や提供終了等で、セキュリティ対応ができない IoT 機器に傘（Umbrella）をさす仕組みで脆弱性対応を行う。

(4) 開発段階で、セキュリティ開発体制（SDL：Security Development Lifecycle）を確立し、①設計・開発、②実装、③保守・運用の 3 段階で対策を考える。

7 Bug Bounty Program（脆弱性報償金制度）の確立及び実施

(1) 2016 年 4 月に「ハックザペンタゴン」として、既存のシステムに対し、事前にセキュリティ専門家を募り、攻撃を行い、その脆弱性の検証をさせ、報償金に値する内容により、100～15,000 ドル／件を支払ったが、支払い総額は約 15 万ドルで、外部委託では 100 万ドル（約 1.1 億円）以上になると言われた。

(2) 2002 年に公表された国防総省の調査でも、97、98%はパッチ未対応か設定ミスであり、費用対効果も良いと思われ、国内でも効果があると思われる。

8 教育・訓練の確立

(1) サイバーセキュリティでは、『人間は最大の脆弱性』と言われるが、人への攻撃の多さや適切な教育・訓練に問題があると考えている。

(2) セキュリティ技術者だけでなく、管理者・リーダ、経営者・CISO、利用者等を対象とした教育・訓練が必要であり、また、縦割りの教育・訓練でなく、必要な教育・訓練レベルを考えて行う。

(3) 組織のサイバーセキュリティ対策は長期的には『セキュリティ文化の確立』であろう。

9 WTO 政府調達協定：第 3 条 適用除外 の周知

(1) WTO 政府調達協定には、『適用除外』があるが、官庁・自治体や独法等の調達部門では知らないことが多く、周知を図る。

(2) 調達方法も提案内容のヒアリング（プレゼンテーションや Q&A）に十分な時間をかけて実施することで、高品質の提案を採用する。

1．セキュリティ政策の推進体制の確立

個人を含め、民学官で、安全なサイバーセキュリティ環境を構築していくことは簡単ではないが、少しでも前に進む努力を行う必要がある。

現状、サイバーセキュリティ対応に関する現状の問題点は、技術者の育成だけでは不十分なことにある。技術者に限らず、管理者や現場の担当者を含め、あらゆる人材がサイバーセキュリティに対する理解を深め、適切に行動できる推進体制の確立が求められる。

1.1 官庁・自治体のセキュリティ強化

(1) 中央官庁の情報管理（広義のセキュリティポリシー）

米国では、政府長官や州知事が公務における「私用アカウント」の利用があれば、大きな話題（スキャンダル）になる可能性もある。実際、国務長官だったヒラリー・クリントンが、公務メールの送受信に、個人のスマートフォンが利用され、私用メールアカウントの利用も大きな問題になった*。

*）ヒラリー・クリントンは、国務長官就任当初、スマートフォンの 1 台利用は、簡単で、楽だし、使いやすいと述べていたが、時期ははっきりしないが、2 台持ちに変わった。 ABC News, https://abcnews.go.com/Politics/hillary-clinton-phones-secretary-state-now/story?id=29535505

本報告書検討チームやサイバーセキュリティグループでは、新元号制定に伴い、スマートフォンの統制の議論があった。官庁職員や大臣、政務官等の利用しているスマートフォンやタブレット等のポリシーの確立も必要との意見が大半を占めた。

タブレットやスマートフォンの利用が一般的になった現在、それらのセキュリティポリシーは、単に利用を想定するだけでなく、機器そのもののセキュリティを考える必要がある。

省庁において、また特に、大臣や政務官、高級官僚等は支給機器と私用機器の明確な分離が必要である*。上記の米国クリントン元国務長官の例もあるが、問題点は、私用機器の統制が適切にできない可能性の存在にある。

*）一部の省庁では、大臣を含む一定クラス以上は、携帯端末が支給されている。また、各職員は端末にデータが残らないメーラーを利用している。

その理由は、一部のタブレットやスマートフォンでは、利用者の意図に反した動作（盗聴、盗視等）を確認して事例の報告があるためだ。更に、私用機器を利用する場合、機器の「利用規約」を確認する利用者は少ない。当然、問題が発生しても、利用規約で定めていれば、利用者側の問題になってしまうのである。

また、サーバの事例だが、米国では、後付けの微少チップが見つかった報道[1]もあり、スマートフォンでも同様な問題があっても不思議ではない。

(2) 自治体業務の一元化

自治体は、大きく 3 つに分けることができ、2018 年（平成 30 年）10 月

1 日現在；

① 広域自治体　　（47 都道府県）
② 政令指定都市　（20 都市）
③ 基礎自治体（1,741 市区町村）

に分類され、全体では 1,808 自治体がある。

多くの基礎自治体では、ほぼ全国で同一業務を行っているが、一部の広域自治体内の「町村会」では共同システムで運用しているものの、複数の広域自治体にある基礎自治体が共同で業務処理を行うケースは少ない*。そこで、複数の広域自治体（バーチャル道州制）にある基礎自治体（市町村）が共同システムで運用を行い、各自治体は 2 ヶ所の共同データセンターに接続する（正副のデータセンター）ことを提案する。これにより、共同データセンターが同時に被災する可能性も低く、リスク軽減になる。こうした利点を踏まえれば、共同システムの利用推進を妨げる事由はおそらく存在しないだろう。

複数自治体での業務集約は、システムの管理やサイバーセキュリティ対応に余裕を持って行える可能性がある。休暇や病欠、深夜呼び出しなどを考えれば当然である。

*）ネットワーク監視を共同で行っている事例はある。「鳥取・岡山自治体情報セキュリティクラウド運用事業」
http://db.pref.tottori.jp/yosan/30Yosan_YoukyuuJoukyouKoukai.nsf/2875f2fd7f2d7b62492574820032bf06/f22cabf6859b3c76492581ef0004e18b?OpenDocument

一部の業務、例えば、『民泊制度』は、広域自治体に代わり、政令市や中核市、特別区等が住宅宿泊事業の届出の受理・監督等の事務を代行しており、そのプログラムは中央官庁で作成しているが、このような業務は他にもある。

自治体全体を巻き込んだシステム構築を行うことが、自治体のシステム予算の削減やサイバーセキュリティの高度化になると考える。

1.2 高度技術者のグループ化 ＆ 地方振興

高度技術者の育成は一朝一夕にできるものではないが、数年前、米国の技術者は「米国では、最低でも 5 年必要*」と回答していた。

国内では、高度技術者の育成にはもう少し時間がかかると考えている。コンピュータウイルスをはじめとして、国内でも実際の解析ができる環境であれば、短期間で可能だが、国内で開発をしていない機器やソフトウェアに関する技術・技能の修得は簡単ではない。開発者に仕組みを聞く、あるいは、リバースエンジニアリングができなければ、相当の時間が必要であろう。

＊）毎年、ロンドンで開催されている「InfoSecurity Europe」で、数年前に会った米国のサイバーセキュリティ技術者（セッションのインストラクター）とセキュリティ技術者の育成期間の話からでてきたもの。国内では、コンパイラー開発や大学院等での経験から、日本では 10 年程度必要ではないかと考えていると言ったことに対する回答。限定的な対応であれば、国内でも 1 年もあれば可能との指摘が

あるが、前提知識や経験の有無を考慮する必要がある。

このような事から、高度な技術者の育成には、次のような対応への配慮が必要になる。

① 現象の解析や議論をグループで行う。
② 実践的な教育・訓練を行う。後述する「Bug Bounty：脆弱性報償金制度」や「機器等の検証システム」、「事故調査委員会」などへの参加等を通して、実践的な技術の修得を行う。
③ 教育・訓練に関しては、攻撃対象が遠隔地でも対応可能であり、良好な通信環境があれば、初心者レベル以外は、集合研修の必要はない。

1.3 物理的対策（Physical Security)

(1) 通信ケーブルや電力ケーブルのセキュリティ[2]

通信会社や電力会社に任せればよいとの指摘を受けるが、データセンター内のケーブル類は考えなくて済むだろうか。

あるいは、クラウド利用ではコンピュータ処理が中断することはないとの指摘もあるが、東日本大震災時にはデータセンターへの接続が不可能になり、処理ができなかった例もある。

(2) 2006 年 8 月に発生した「首都圏停電」

旧江戸川上空を横断する送電線（275KV）にクレーン船が接触し、3 時間余り停電した。停電に伴い、自家発電装置の切替え等のトラブルで株価算出ができなくなった。3 時間程度で電力が復旧したが、電力復旧時のトラブル（電源投入の順序等）で、過電流になり、システムダウンが発生し、データベースに不整合が発生した事例もあった。

(3) 大規模災害対応

2015 年 9 月に茨城県常総市では、鬼怒川（上流では、500mm/3 日間以上の降雨があった）が氾濫し、市役所本庁舎も浸水被害を受けた。

近年、温暖化の影響と思われるが、大規模台風や前線に伴う洪水が発生しており、自然災害等の発生時に、データセンターや利用端末等の設置場所の対策を考える必要がある。

1.4 ロードマップの作成・更新

今回、セキュリティ政策の確立を含め、９項目の検討を行ったが、これらに対応するには、けして楽なものではないし、それなりの財政的な裏付けが必要である。

災害対策でも同じであるが、事前に適切な対応を行うことができれば、事後の対策の 10 分の１，100 分の 1 の費用で済む。

ロードマップは、5 年から 10 年程度の期間を想定し、優先順位を決めて行う必要がある。

計画全体（5 年／10 年）を考え、項目毎に段階を分け、次のステップに進む前に報告を行う方法を考えている。

2．政府・自治体、重要インフラのサイバーセキュリティ強化

2.1 サイバー攻撃・サイバーテロへの対応強化

かつて、化学兵器や生物兵器は「貧者の核兵器」と呼ばれていた。これは通常の核兵器と比べ製造費用が安く、原材料の入手も容易で、簡単な技術や設備で製造が可能なことから言われてきた。

最近のサイバー攻撃は、化学兵器や生物兵器以上に容易に利用でき、更に、攻撃対象場所と攻撃場所が同じである必要さえもない。

実際、2014 年 米国映画会社へのサイバー攻撃は、日本企業の子会社（米国企業を買収）への攻撃であったが、最高指導者を暗殺するパロディ映画の予告編が公開（2014 年 6 月）され、5 ヶ月後の 11 月に、サイバー攻撃が行われた。攻撃に必要な情報を集め攻撃されたと思われるが、米国内では、サイバー戦争、サイバーテロとの考えが強く、政治問題にまで発展した。

このサイバー攻撃では、当該未公開映画以外の映画や従業員、関係者の個人情報も公開され、パロディ映画公開の中止を求めた。

米国では、当該映画会社だけでなく、親会社も古くから米国企業との考えがあり、サイバー攻撃より、「サイバーテロ」が適当だとの考えが多い。この事件では、当該映画の上映中止について、米国大統領もコメント（「公開中止は、間違った判断だ」）している[3]。日本国内では親会社からの情報が殆どなかったため、あまり大きな話題にならなかった。

一企業へのサイバー攻撃が国家的問題に発展したとも言える。最近の近隣諸国との問題を考えると、国内でも他人事ではないと思われる。

最近の**国家間の緊張関係や重要インフラの採用機器問題等**を考えると、**大規模なサイバー攻撃（サイバーテロ）**も他人事ではない。

2.2 サイバーリスク保険

サイバーリスクに対して、サイバーリスク保険の検討も行われている。一般企業だけでなく、自治体等でも、他の損害賠償保険と同様、検討する必要がある。

保険の検討で最も重要な事柄は、事故が発生した時に「支払い対応にならない」項目を確認することである。

「テロ」は、従来、支払い対象になっていたが、米国での「3.11 同時多発テロ」発生以降、一般の保険で免責事項になったため、サイバーリスク保険でも、一般の損害保険に準拠したと思われる。

サイバーリスク保険で、「支払い対象にならない」主要項目は、下記に記したが、詳細は、「保険約款」で確認する必要がある。

国内でも、今後、単純なサイバー攻撃でなく、サイバーテロと判断される事案が発生すれば、保険金の支払い対象にはならない。注意が必要であろう。

勿論、今後、テロやサイバーテロへの対応が変わる可能性もあると思われる。

サイバーリスク保険について

最近、サイバーリスク保険に関心が集まっているが、サイバーリスク保険だけでなく、一般の保険でも「支払い対象とならない場合」を注視する必要がある。詳細は「**約款**」を確認して欲しいが、**支払い対象とならない主なもの**には、以下のものがある。

- 保険契約者または被保険者の故意
- 戦争（宣戦の有無は不問)、変乱、暴動、騒じょうまたは労働争議
- 地震、噴火、洪水、津波または高潮

上記、米国映画会社のインシデントが、サイバーテロ／戦争と判断されれば、免責になり、保険金が支払われないことになる。

また、地震や洪水、津波などでも免責になる。

保険は非常に有用なものですが、「支払い対象にならないもの（免責)」を確実にチェックすることが大切になる。

3．事故調査委員会の設置

3.1 セキュリティ分野における事故調査の現状

大規模な情報漏えいでは、第三者調査委員会が作られ、調査を行っているが、民間企業の場合、顧問弁護士が中心で、セキュリティ分野も技術者が委嘱され、業務処理手順などの検証ができるサイバーセキュリティ・マネジメント等の専門家が参加することは少ない。 民間企業の「事故調査委員会」では、「第三者機関」でなく、企業の意向に沿った委員会が組織されることが多く、更に、実態が公開されないことも多い。

また、「プライバシー」への配慮との理由で、詳細な情報が隠されることもあり、実態が明らかにならない。

政府・自治体や独立行政法人では、関係省庁が調査委員を決めるが、報告書はセキュリティ技術中心の記述が多く、実際の業務手順を理解し、事故調査・分析を行うことは少ない。

これは、「事故調査委員会」のメンバーの時間的な制約もあるが、業務や業務処理知識が十分でない技術者が中心で、業務処理の検証ができる専門家が参加していないためと考えられる。

3.2 政府機関としての事故調査委員会の設立

(1) 事故調査委員会の必要性

本来、セキュリティインシデントの多くはヒューマンエラーをはじめとしたセキュリティマネジメントの欠如や不足に起因するものが多い。

セキュリティ技術者だけが参加するのではなく、セキュリティマネジメントや管理・運用の専門家の参加が求められる。

他分野の例として、国内には、「運輸安全委員会」があり、航空、鉄道、船舶の事故や重大インシデントの原因究明を専門官として行っている。同様に、サイバーセキュリティ分野の重要性が増し、政府・行政サービスを初めとし、重要インフラ等のインシデントは、国民生活に大きな影響を及ぼすことを考えると、「サイバーセキュリティ事故調査委員会」を政府機関として設ける必要がある。

(2) 事故調査委員会の特性

事故調査委員会が全てのインシデントの調査を行うのではなく、政府・行政サービスや情報通信、金融・クレジット、電力等の重要インフラと大規模なインシデントの事故調査を行う。

最近発生している重大インシデントでは、「利用者（End Point）」を攻撃対象としており、技術的な脆弱性（「ゼロディ攻撃」等）よりも、人間の心理的な弱さや業務処理の欠陥を狙ったインシデントが多い。

実際、「高度な技術を持った攻撃者によるインシデントより、設定ミスやパッチ未適用が大部分である」との指摘も米国では昔からある[5]。

セキュリティ技術の対応も重要だが、人的セキュリティの強化（教育・訓練や組織対応など）も含め、包括的なサイバーセキュリティ対策が必要で、実際の事故調査結果から対策の考察を行うことも必要になる。

3.3 記者会見は任意とする仕組みづくりを

米国では、10 数年前からセキュリティインシデントで「記者会見」を行っていない*。　このため、国内のグローバル企業でも、日米両国の個人の情報が漏えいすると、米国では企業ウェブや公式ブログへの公表に限定しているが、日本では記者会見を行っている。

記者会見の開催は、インシデント内容の説明や記者からの質問に対する準備が必要であるが、十分な準備なしに、記者会見を行い、対応のまずさから、風評被害を拡大させ、被害を更に大きくしてしまうことが多い。

そこで、事故調査委員会の設置を行い、記者会見は任意とする仕組みも考慮したい。

*) 2014 年 米国にある日本企業の映画子会社へのサイバー攻撃では、例外的に記者会見が行われた。10 数年来、始めての出来事で、このサイバー攻撃の重要性がうかがわれる。

４．機器等の検証システムの確立

機器を利用して得られた情報は、機器がネットワークに接続されていれば無断で外部に送信されることもある。　情報の価値が上がれば、違法な情報送信が増え、「個人情報」や「企業情報」、「知的財産」等が漏えいする可能性がある。　官庁・自治体や独立行政法人、重要インフラ企業等もその標的になっている。

個人や企業の情報が漏えいにより、それから更に、大規模インシデントに発展する可能性もある。

4.1 違法情報送信等の事例

以下は、国内外で発生した主な情報情報漏えい等の事例である。　なお、⑥ は、その対応策の 1 つと考えることができる。

① 無償日本語入力ソフトで、無断で入力文字情報が送付されていた[6]。

② スマホ端末のファームウェアに「バックドア」があり、無断で個人情報を自社サーバに送付していた。
違法送信内容は、SMS の本文や連絡先、通話履歴と電話番号、端末の識別番号などの情報であった[7]。

③ 米国及び英国は、ロシア製コンピュータウイルス対策ソフトの購入をしないよう政府機関に通達した。　この製品を通し、ロシア政府がネットワークに侵入する可能性があると指摘したもの[8] [9]。

④ スウェーデンの大規模な運転免許データ漏えいは、システムを受注した企業が、業務をチェコとルーマニアの下請け企業に外注したため、外国の IT 技術者らが機密情報を閲覧可能にした（2017 年 7 月 25 日）[10]。

⑤ シンガポールで発生した大規模ネットワーク障害では、中国の攻撃との疑念が言われている[11]。

⑥ 違法情報送信の防止対応として、ロシアは、Windows のソースコード公開をマイクロソフトに求め、ソース公開の最初の政府となった [14] [15] 。

4.2 違法機器の検出

重要インフラで利用する機器やソフトウェア、サービスを自由に選択できることは望ましいが、現実には違法な情報転送が行われることもある。

重要インフラで利用している機器等を全て確認する要員を準備することは、要員数や費用面を考えても、容易ではないため、以下の対応を考える。

① 米国国防総省で実施した「Bug Bounty Program（脆弱性報償金制度）」の日本版の実施。

② ①を行う人材により、機器等の「無断、違法情報送信」の検出を行い、重要事項の検出があれば、報償金の支払い対象にする。報償金に値しない場合でも、顕彰などの対象にする。

③ 入札時に「無断、違法情報送信」等を排除する契約条項を設ける。

このような対応を行うためにも、官庁や自治体でのシステムについての見直しが必要になる。　例えば、

- 自治体は約 1,800 あり、県内の町村会だけでクラウドを利用しているが、1,000 以上の自治体が単独でシステムを利用しているものと思われ、集約化を考える必要がある。

５．認証制度改革 ～信頼確立制度～

5.1 信頼確立制度について

ISO/IEC27001(ISMS)等の ISO/IEC 認証制度は、欧州(イギリス)から考えがでてきた。1970 年代中頃から、品質保証（ISO9000）を中心にガイドラインが作成されたが、この考えの根底には分業化が進み、他企業から部品等を購入する場合、個々の企業が購入先の品質を毎回確認するのではなく、必要な品質を確保している企業に対しては、購入前の調査・検証を軽減可能との考えがあった。昨今のサプライチェーンにおける調達時の対応と考えることができる。

部品供給企業自体が品質を保証するのではなく、第三者が調査・検証を行い、一定のレベルがあれば、認証を付与する仕組みが考えられた。

この考えは、品質だけでなく、情報セキュリティ、EMS（環境マネジメントシステム）等でも、同様の考えがでてきた。

ISO/IEC27001(ISMS)等、ISO/IEC 関連の第三者検証組織は、国内では「認証機関」と呼ばれているが、実際には、「監査（Audit）機関」であり、調査・検証は「監査（Audit)」である。

このため、第三者による調査・検証が適切に行われなければ、サプライチェーン自体が形骸化してしまう可能性がある。

実際、第三者から提供される製品やサービス、セキュリティ体制等が信頼できるかの判断は必ずしも簡単ではない。

一般的には以下の方法があるが、それぞれ、「一長一短」があり、「長所」を有効利用することは当然であるが、「短所」を長所に変える、あるいは、「短所」を理解し、最低限に抑えること大切になる。

1. 第三者認証

(1) 検査（チェックリスト）方式

- 制度全体を管理する組織（「国際標準化機構」等）が、チェックリストを作成し、それを基に、「審査機関」が「認証取得組織」のチェックを行う
- チェックリスト内容を実際の業務処理と比較しながら確認ができる
- チェックリストの加除訂正は「国際標準化機構」が行う
- 単純業務に適している。　逆に言えば、広範な業務範囲の場合、チェックリストが全体をカバーできないことがある
- 審査はチェックリスト内容に従って行い、重大な指摘事項がなければ、認証される
- 検査方式の代表例には、「PCI-DSS」（クレジットカード業界）がある。 PCI-DSS では、審査が適切でない場合、審査機関に罰金を賦すこともある

(2) 監査方式*

制度全体を管理する組織が、制度全体やその中の重要項目である、「管理策・管理目的」を作成する。 管理策・管理目的は基本的な管理目的を記述したもの。

- 当初の管理策・管理目的は、「チェックリスト」ではない。被監査組織は、① 自組織のリスク分析の実施、② 管理策・管理目的の加除訂正、③ 適用宣言書の作成（含 経営者の承認）を行う

- 内部監査部門は、リスク分析から適用宣言書が、適切なものかの監査を行う。このため、内部監査人は、業務処理知識や監査能力が必要とされる
- 審査機関は、これらを基に、適切なセキュリティ対策が確立されているかを確認し、問題がなければ、認証与する
- 審査機関（審査員）にとって、適用宣言書や内部監査報告書の検証と現場調査で、審査（英語は「監査（audit)」である）ができることが望ましい
- 監査方式には、「ISMS」や「ISO9000」、「プライバシーマーク」等がある
- 監査方式で行われている ISMS やプライバシーマーク等は、「制度」と「管理・運用」の２面から考える必要があるが、プライバシーマークや ISMS では、「管理・運用」が非常に杜撰で、この面の抜本的見直しが必要である。なお、ISMS やプライバシーマークの審査では、審査機関が罰金を課されることがない

*) ISSM や ISO9000 は、海外では「監査（Audit)」であるが、日本では「審査」と言っており、それに準拠して説明している。
英語の「audit」は、「聴く」と同じ語源であり、audit は、「監査」より、「岡目八目」（第三者は当事者より物事の真相等が良く分かる）に近く、上から目線ではない。

2. 自己認証（自己申告）

(1) 検査（チェックリスト）方式

自組織内で作成した「チェックリスト」は、利用毎に問題があれば、自組織内で加除訂正する。

- 基本的には、(1) で述べた検査方式と同じであるが、チェックリストの加除訂正は、自組織内で行う。
- この方式では、自組織内で加除訂正を行うため、チェックリストが長期にわたって、見直しがされず、必要な部分の加除訂正も行わずに放置されていたものもある。 30 年余り、チェックリストの見直しが行われず、外部監査で指摘され、新しいチェックリストを作成した例もある。

(2) 自己監査／内部監査方式

法制度や制度管理組織が定めた制度に従った手順で対応し、構築できれば自己監査／内部監査を行い、自己宣言をするもの。

- 新しい制度などは、自組織だけで対応できないこともあり、コンサルタント等を利用し、確実な仕組みを構築することもある。
- 内部監査等が充実していないと、時間経過や環境変化があっても、その対応が行われないこともある。
- 時間の経過により、担当者の異動などにより、当初の目的を誤解する、あるいは、自己解釈を行い、制度に合致しない仕組みになることもある（サイバーセキュリティ分野ではない)。

5.2 ガイドラインの検討

前述のように認証制度では、管理・運用面での課題が多い。 本来、認証制度では、認証取得が目的でなく、管理・運用の適切な構築だが、国内では認証取得が目

的化している感じがあり、課題の抽出が必要であろう。
それぞれの認証制度の特徴の検討を行い、利用方法を含め、ガイドラインの検討を行う必要がある。

参考

GDPR (欧州、一般データ保護規則) について
2018 年 5 月 25 日に施行された GDPR 違反では、2 パターンのいずれかの制裁金を支払う必要がある
（制裁金の上限： 第 83 条)。
1,000 万ユーロ、又は前会計年度の全世界年間売上.の 2%のいずれか高い.
2,000 万ユーロ、又は前会計年度の全世界年間売上.の 4%のいずれか高い方

- 公的機関は、上限額 1,000 万／ 2,000 万ユーロ以下の金額対応
- 違反に対し常に巨額の制裁.が課せられるのでなく、警告、命令、懲戒などのプロセスを踏まえ、違反の性質、重.さ、期間、影響を受けたデータ主体数、損害レベルなどにより変動する。

5.3 IT 調達方針及び調達手続き

2018 年 12 月に、関係省庁の申し合わせとして、「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ[12]」が公表されている。
本申し合わせでは、その対象は政府機関に対して、情報システム・機器・役務を対象とし、それらの重要性を鑑みた取り決めを行っている。
この観点は、WTO 政府調達の適用除外（**「9」参照**）に該当するものと考えることができるが、サプライチェーンを考える場合も考慮する必要がある。
なお、WTO 政府調達では、附属書 I（各国の適用範囲）[13]にその対象範囲を定めているが、WTO では、都道府県及び指定都市（人口約 70 万人以上の 20 都市）も対象にしている。

6．IoT システムの安全性確保

あらゆるモノがネットワークに繋がる時代がやってきたが、パソコンやタブレット、スマートフォン等と比べ、遙かに小さな機器が接続されるようになり、機器やデータのセキュリティやプライバシーの保護を考える必要がある。 また、セーフティに関係する機器もネットワークに繋がっており、今後、製品安全や機能安全との関係の整理も求められることが想定される。

6.1 はじめに ～ 誰が対応するのか ～

従来、IoT 機器については、あまりセキュリティ対応を考えてこなかった。 これは、

1．IoT 機器を攻撃するとの考えがあまりなかった。
2．小さな機器が中心で、セキュリティを考える必要がないと思われた
3．制御機器中心で、セキュリティを考慮してこなかったこともあり、古いオペレーティングシステムを利用しており、脆弱性を残したものがあった。
4．インターネットなどのオープンなネットワークへ接続されることも少なく、また、独自の OS を利用した機器との認識があり、セキュリティ対策は不要だと考えていた。

しかし、セキュリティコンファレンス等で、コンピュータや端末機器等の脆弱性に攻撃が行われるようになり、統合機（プリンター、FAX、コピー等が統合されたネットワーク機器)、監視カメラ、自動車等にも脆弱性があることが示され、IoT 機器へのセキュリティ対策の必要性が高まってきた。

現在、多くの IoT 機器が利用されており、今後も、多くの IoT 機器が作成され、マーケットにでて行く。

IoT 機器へのセキュリティ対策の推進は、パソコンやサーバなど（これも IoT 機器だが）と大きく変わらないであろう。

1．IoT 機器ベンダー： IoT 機器を製造する業者
2．IoT 機器を利用し、システム構築を行う者： 外部委託やパッケージを導入する場合と自社で必要な IoT 機器を購入し、システム構築を行う場合が考えられ、従来の情報通信システムの構築と大きな相違はないと考えている
3．その他： 古いオペレーティングシステムを利用したシステムでは、ATM や駐車場システム等や他の IoT 機器ではセキュリティの組み込みが難しいものもある。これらの機器への対応を考えるセキュリティベンダーが出現する可能性もある

セキュリティの確保のために方策としては、以下のような方法が考えられている。

6.2 軽量暗号

リソースには、厳しい制限があり、**従来の暗号製品を実装できない機器**にセキュリティやプライバシーを確保する暗号開発が行われており、それらを「**軽量暗号**（Lightweight Cryptography)」と呼んでいる。

軽量暗号の要件として、

① 安全性要件： 簡単に解読されない暗号強度が要求される
② ハードウェア実装要件： チップの面積や消費電力量など
③ ソフトウェア実装要件： プログラム（ROM）や RAM サイズ
等がある。

軽量暗号も、AES（Advanced Encryption Standard）と同様、NIST[17]は、2019 年 2 月 25 日までに、軽量暗号候補を募り、数年後に軽量暗号が標準化されると思われる。

しかし、既に IoT は普及しており、軽量暗号の標準が決まるまで、IoT 機器に搭載する軽量暗号については、搭載する／しないを含め、各 IoT ベンダーが独自に決めることになる。

6.3 Umbrella の作成

(1) パッチ未適用ソフトウェアについて

現在、多くの情報機器では、導入後、ソフトウェアの脆弱性解消のため、ベンダーからパッチプログラム（脆弱性修正プログラム）が提供されるが、
① パッチプログラムの提供が既に終了している
② 機器がコンピュータに接続されている認識がなく、利用者がパッチプログラムを適用しない
③ システム停止ができない等の理由で、パッチプログラムを適用しない
等の理由からソフトウェアに脆弱性が残っていることがあり、大きな被害を受けた事例*もある。

2017 年度調査でも指摘したが、2002 年の米国国防総省の調査では、パッチ未適用や設定ミスがインシデントの 97,8%を占めており、パッチプログラムの適用の重要性は今でも変わらない。

最近のサーバ環境では、仮想化やクラウド利用が主流になっており、パッチプログラムの適用も従来よりも容易になってきた。

*) 2017 年 5 月に発生したワーム型ランサムウェア「WannaCry」は、20 万人以上、23 万台以上のパソコンに感染し、イギリスの国民保健サービス（NHS）等で大きな被害があったが、パッチプログラムを事前に適用していれば、感染被害は避けられた。

(2) Umbrella の作成（仮想パッチ【Virtual Patch】）

パッチマネジメントについては、
① 24 時間・365 日動いているシステムを勝手に止められない
② 導入ソフトウェアを事前に調査し、パッチ適用後に正常に動くかの検証が必要
③ パッチ処理で正常に動かない場合、元に戻す、復元作業が必要になる
④ 緊急時には、短時間でパッチの適用が必要になる
⑤ 脆弱性が指摘されているが、パッチが公開されていない
等の指摘があり、パッチマネジメントは容易でないと言われる。

パッチマネジメントの困難さを克服する仕組みとして、脆弱性のあるシステムに傘（Umbrella）をさすように、脆弱性攻撃をカバーする仕組みを構築できれば、全ての脆弱性を一ヶ所で対応でき、傘下にあるソフトウェアなどの脆弱性対応には十分な時間をかけて行うことが可能になる。

この方法であれば、アプリケーション等の問題でパッチを適用できないシステムやパッチプログラムが提供されていない場合でも対応できる。

6.4 セキュリティ開発体制の確立

機器やソフトウェア開発では、大きく①設計・開発、②実装、③保守・運用の３段階があり、セキュリティ対応については、SDL (Security Development Lifecycle)と呼ばれる。

特に、ネットワークに接続される機器では、脆弱性がない／少ない機器やソフトウェアであれば、運用コストは低くなる。

セキュリティは、三段階で、それぞれ考える必要があるが、上記 ①や②の段階では、③保守・運用でのセキュリティを考えることも必要である。

(1) ユーザ名／パスワードの初期設定ミス

当初、セキュリティを余り重視しない考えで、機器をネットワークに接続していた[16]。セキュリティ対応が不十分で、ユーザ名やパスワードが不要であったり、同一機器全てが同じユーザ名／パスワード等で、内部情報が漏えいしたり、「踏み台」にされた*。

*）書籍[16] Secrets of a Super Hacker（1994 年 1 月発行）では、UNIX 等のコンピュータのパスワードが既知だと述べている。しかし、日本語版では、その部分（Appendices）を全て翻訳しなかった。「知るはハッカーのみ」とも言える。

(2) 共通鍵暗号の落とし穴

共通鍵暗号方式は、１つの鍵を使うため、二者で使う前提だが、複数間で使ってしまう。最近は聞かないが、以下のような例があった。

① 最初の SSL(Secure Sockets Layer)は、インターネットブラウザー(Netscape)に搭載されたが、ブラウザーをリセットすると、リセット前と同一の鍵が生成され、一時、「暗号が解読された」と報道されたが、実際には、暗号システムの実装段階の問題であった。

② 類似例だが、大手銀行の都度振込で、送金プログラムで簡易なワンタイムパスワードを採用したが、プログラムをリセットするとワンタイムパスワードが元に戻り、不正送金（約 1.5 億円）事件があった。

(3) 暗号の危殆化など

① 暗号の危殆化： 暗号アルゴリズムの安全性は、コンピュータの計算能力の向上や新しい暗号解読手法の出現で次第に低下する。これを暗号アルゴリズムの危殆化と呼んでおり、利用している暗号の安全性を確認する必要がある

② 独自暗号利用の危険性： 独自開発の暗号アルゴリズムを使えば安全だとの考えが、一部にある。標準軽量暗号が決まっておらず、最終決定まで数年かかる。応募暗号アルゴリズムでも、安全性に問題がある暗号が含まれている可能性は AES の場合でもあった。

注) 代表的な事例を以下に示す；

- 2004 年 10 月に発覚したハードディスク搭載の DVD は、外出先からの設定を可能にするため、パスワード入力を不要にしたため、踏み台に利用された。
  https://internet.watch.impress.co.jp/cda/news/2004/10/06/4882.html
- コピーやスキャナー、FAX 等の機能をもつ「複合機」に保存される情報が外部

からのアクセスで漏えいした。 複合機のパスワードが出荷時に全て同一、あるいは、ユーザ名やパスワードがないものもあった。
https://www.nikkei.com/article/DGXNASFK1302W_T11C13A1000000/

- ネットワーク接続の監視カメラも、同じ問題が発生した。パスワード設定が杜撰であれば、外部からアクセスされる。　外部から自由にアクセスできる監視カメラの画像をみせるウェブサイトもある。

既知の ID やパスワードによるインシデントの時系列表示

(4) 訴訟リスク（PL 法）

製造物責任法（PL 法）ではソフトウェアは対象外だが、ソフトウェアが含まれる機器等は対象になる。ノートパソコンのバッテリーパックが発火し、やけどを負った男性の訴訟判決で、地裁は製造元に支払いを命じた[4]。

7．Bug Bounty Program（脆弱性報償金制度）

7.1　Bug Bounty Program（脆弱性報償金制度）とは？

Bug Bounty Program は構築されたネットワークに対し、ネットワーク構築者以外の第三者が実際に攻撃を行い、実践的調査を行い、脆弱性を発見する。

ネットワークの脆弱性は、正しい設定を行わなかったことや構築後に新しい脆弱性が発見されてもパッチを適用しなかったため、それらを発見され、攻撃される。

2002 年 7 月に Government Technology がウェブに掲載したインタビュー記事で、2001 年の米国国防総省の調査では「97、98% は、設定ミスかパッチ未適用」と述べている[5] * 。

Bug Bounty Program は、2016 年 4 月に、パイロットプログラムとして実施された。このプログラムは、事前にハッカー（セキュリティ専門家）を募集・登録し、米国政府のウェブの脆弱性の検証をさせた。　登録した 1,400 人以上のハッカーにより、報償金に値するウェブの脆弱性が 138 件発見された。

報告者に支払われた報償金は 100 ～ 15,000 ドル／件で、米国国防総省の支払総額は、約 15 万ドル（約 1,650 万円）であった。 もし、同一業務を外部委託した場合、100 万ドル（約 1.1 億円）以上になる可能性があると言われている[18] [19]

*) ハワード・シュミット（Howard Schmidt） 「米国国防総省の 2001 年調査では、97～98%は、パッチを行わなかったか設定ミスで、技術的な問題ではない」と述べている。

7.2　Bug Bounty Program のメリット

外部委託に比べ、安価な費用で、実システムの脆弱性を探し、報告する仕組みが特徴だが、その他に、

① 実際に構築したサイトや構築後の運用体制の巧拙も判断でき、外部委託であれば、今後の業者選定にも役立つ可能性がある。

② 訓練システムでは考え難い課題* が実モデルには内在することもあり、それらの発見にも役立つ。

*) 訓練システム（含 CTF: Capture The Flag）は、全てを考慮しているとの指摘もあるが、確認できていない。例： スイスチーズモデル：個々の事象でセキュリティが確保されているが、複数の事象が重なると脆弱性が健在化する可能性がある。

7.3　国内対応について

（１）実際のウェブに対する攻撃を行うことに問題があれば、

(a) 少数の登録者により実施する

(b) 「同一システム」を作成し、それに対して、実施する

(c) 外部だけでなく、「５．事故調査委員会の設置」の要員を参加させ、要員のレベル向上や攻撃者の数を増やすことが可能になる

等が考えられる

（２）外部登録者に対して、脆弱性の発見には重要度に従い、報償金を支払う。

（３）参加者には感謝状やウェブでの公開などを検討する。

（４）なお、本件は、次年度以降に詳細の検討を行う。米国では、政府機関だけでなく、既に複数の民間企業でも始まっている。

8．教育・訓練の確立

「人は石垣、人は城」は、戦国武将 武田信玄の言葉だが、立派な城を築いても、優秀な人材がいなければ、簡単に城は攻め落とされる。

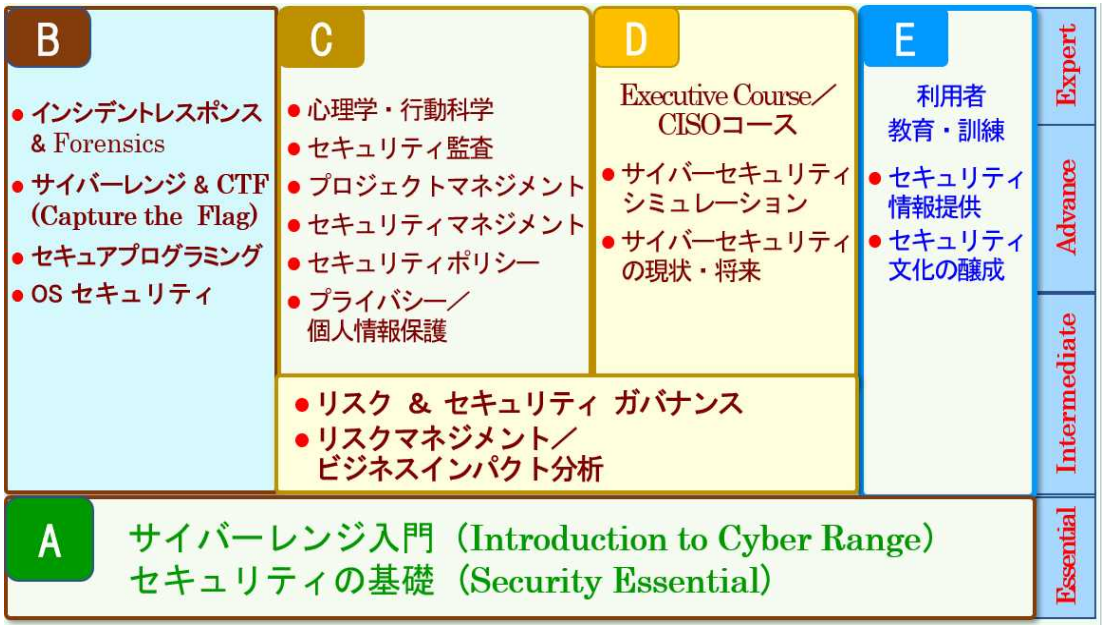
サイバーセキュリティでも同じであろう。高価なセキュリティ機器等を導入しても、その運用や必要な情報収集を行える技術や管理・運用の知識を持った（訓練された）人材が必要になる。

更に、高価なセキュリティ機器が導入されていても、利用者等がユーザ ID やパスワードを他人に漏らしてしまえば、ネットワークに侵入されることもある。内部者が情報窃取に加担していれば、防御は更に困難になる。

最近の調査[20]では、システムの脆弱性への攻撃より、人間（役員、正規社員、非常勤社員、個人等）を対象にした「フィッシング」攻撃（ソーシャルエンジニアリング*の一種）が多く、2018 年では、26 万件対 2 億 1047 万件で 800 倍以上となっている。

更に、サプライチェーンでは、セキュリティ対応が不十分な参加企業があれば、そこを狙って攻撃され、侵入されることもある。

*) 定まった定義はないが、以下の様に考えている
ソーシャルエンジニアリングとは、人間の心理的な弱さを利用したり、他人になりすまして、必要な情報を盗み見したり、盗取するもので、いくつかの方法を組み合わせたり、複数の人から情報収集を行うこともある。ソーシャルエンジニアリングの考えは、必ずしもサイバーセキュリティ分野だけでなく、医者やコンサルタントなどが利用することもある。



教育・訓練の概要

8.1 教育・訓練について

(1) 脆弱性を考える

「サイバーセキュリティに於ける最大の脆弱性は、人間である」と言われるが、

機器やツールにも脆弱性があり、それらの脆弱性に対応するのは人間である。その典型は誤検知であろう。

- 正しいアクセスを不正アクセスと判断する「False Positive」
- 不正アクセスを正しいと判断する「False Negative」

の２つがある。

機器やツールの誤検知への対応は人間が行う。

勿論、人間も過ちを犯す。それを「ヒューマンエラー」と呼ぶこともあるが、サイバーセキュリティでは他者からの攻撃を受けることがあり、その最大の攻撃は、「ソーシャルエンジニアリング」であろう。

また、ヒューマンエラーでは、何らかの動作・作業を行うことで、エラーが発生する。サイバーセキュリティでは、「何もしない（不作為）」ことが、インシデントを起こす要因になることもある。

2.2 で述べた「パッチ未適用」は、やるべき事をやらなかった／やれなかったために、大きなインシデントをもたらした原因であると考えられる。

Weakest Link（ウィーケストリンク）

セキュリティレベルは、セキュリティ対策の平均値でなく、最も弱い所が、「セキュリティレベル」になる。

従来、セキュリティでの**最大の脆弱性は人間**であると言われてきたが、

- **適切な教育・訓練**や**セキュリティ文化**が組織に根付いているだろうか
- 「**予兆**」を見いだし、事前に周知することで、適切な教育・訓練を受けた人であれば、インシデントを回避できるのではないか
- 更に、最近のフィッシングサイト攻撃（上図）をみても、遙かに人間を対象とした攻撃が増えている
- RSA 2019 Conference で、SANS, Mr. Lance Spitzner も、「人間はウィーケストリンクではなく、主要な攻撃目標になっているだけ」と述べている

(2) 理論と実践

教育・訓練を考える場合、特に、サイバーセキュリティでは実践、あるいは、想定外を考える必要がある。特に、ソーシャルエンジニアリングでは、想いもつかない攻撃*を仕掛けられることがあり、一朝一夕に対応できるとは限らない。

教育という文字を分解すれば、「教える」と「育てる」からなっている。短期間に要求レベルの人材を育成するには、教育・訓練内容だけでなく、育成方法も考える必要がある。

「教育・訓練 ＝ グライダー論」と考えることもできる。グライダーは、自力で離陸できないため、ロープで引っ張られ、一定の高さに到達するとロープを離し、後は自力で飛ぶ。これは教育・訓練でも同じである。

高度な教育・訓練になればなるほど、指導者が少なくなる。。自力で教育・訓練できるようになるためには、教育・訓練環境の提供が望ましいものと考えている。

もし、高度な教育・訓練まで、指導者が必要だとしたら、それまでの教育・訓練に問題があったと考える必要がある。同等程度レベルの人達で、教育・訓練を行うことができる環境が提供できれば良い。それも、集合教育でなく、テレコンファレ

ンスやセキュリティ・テレワークを考えることもできる。

*) 通常の考え方とは、異なる方法で、「**ハッカー欺術(Hacker Deception)**」と呼んでいる。

8.2 教育・訓練概要

全ての組織に共通の教育・訓練を実施することは不可能であるが、基本的な教育・訓練について考えてみた。

セキュリティ教育・訓練では、唯一絶対的なものはないと考えている。

(1) 教育・訓練対象者

教育・訓練内容を詳細に検討すれば、数 10 通りの体系が考えられるが、ここでは対象者を大きく 4 分類し、それに対象者全員を対象としたコースを加えたものを「図２ 教育・訓練概要」に示した。なお、記号（Ａ ～ Ｅ）は、以下を示す。

Ａ： 対象者全員
Ｂ： セキュリティ技術者
Ｃ： セキュリティ管理者／リーダ
Ｄ： 経営者／CISO
Ｅ： 利用者（法務、人事、経理部門等）

なお、各対象者に教育・訓練内容を明確に分けたが、各レベル（基礎【Essential】から高度専門【Expert】）があり、他分野の教育・訓練が組み込まれることもある。例えば、「Ｂ；セキュリティ技術者」でも、「Ｅ：利用者」の教育・訓練も必要になる。また、セキュリティ管理者／リーダが、経営者／CISO 対象にした「サイバーセキュリティシミュレーション」を受講することも考えられる。

ＡからＥの分類は、主な役割における教育・訓練内容と考えている。

（２）教育・訓練内容

① 【A】対象者全員： セキュリティの基礎的な内容を講義形式で行うものと、基礎的なハッキング行為等やパケット監視ソフト等を使って実践的な教育・訓練を行う。
   - サイバーレンジ入門（Introduction to Cyber Range）
   - セキュリティの基礎（Security Essential）

   サイバーセキュリティの基礎（Essential）であり、セキュリティ管理者／リーダに、技術的な面の教育・訓練が必要かとの指摘もあるが、システムやネットワーク構築を行うためでなく、基本的な知識を持つことで、技術者と基礎的な話ができる能力を育成するものである。

② 【B】セキュリティ技術者： セキュリティ技術者の教育・訓練。高度なレベルでは、個人（少人数）教育・訓練が行える環境を提供する。また、Bug Bounty や「事故調査」、「機器等の検証」等への参加により、研鑽を行う。
   - インシデントレスポンス & Forensics
   - サイバーレンジ & CTF (Capture the Flag)
   - セキュアプログラミング
   - OS セキュリティ
   - その他： 暗号アルゴリズムや暗号解読／解読防御等も一部の技術者には必要だが、今回はリストから外した。

③ 【C】セキュリティ管理者／リーダ： サイバーセキュリティに対する広範な知識を持つ中堅管理職や利用者部門からの相談などを引き受ける知識と経験を持つ『管理者／リーダ』の教育・訓練。下記の全てを一人で修得する必要はないが、大規模インシデント発生時のプロジェクトリーダとして、セキュリティ技術者や広報・法務部門、経営者／CIO／CISO 等との橋渡しを行う。

- ● 心理学・行動科学
- ● セキュリティ監査
- ● プロジェクトマネジメント
- ● セキュリティマネジメント
- ● セキュリティポリシー
- ● プライバシー／
- ● 個人情報保護
- ◆ リスク ＆ セキュリティ ガバナンス
- ◆ リスクマネジメント／ビジネスインパクト分析

④ 【D】経営者／CISO ： 経営者や CISO に対しての教育・訓練では、長期的な視点から決断を行うための教育・訓練である [21]。

- ● サイバーセキュリティシミュレーション
- ● サイバーセキュリティの現状・将来
- ◆ リスク ＆ セキュリティ ガバナンス
- ◆ リスクマネジメント／ビジネスインパクト分析
- ◆ 地政学（Geopolitics）*

*) インターネットの発展は、国内でも地理的環境を考えた地政学が必要であろう。ハーバード大学 ケネディスクールが実施している 1 週間の「Cybersecurity: The Intersection of Policy and Technology」では地政学が含まれている。

⑤ 【E】利用者（法務・人事・経理等）： 日々のコンピュータ利用上での問題について、基礎的な課題の解決ができることだけでなく、日々の処理で『おかしな添付ファイルを開いた』、『危なそうな URL をクリックした』等に対応できる利用者を育成し、組織内にセキュリティ文化を根付かせる

- ● セキュリティ情報提供
- ● セキュリティ文化の醸成

9．WTO 政府調達協定 第 3 条 適用除外の周知

WTO 政府調達 第 3 条については、WTO に適用除外があることも理解されていなかった。適用除外が理解されなかった理由として考えられるのは、一定額以上の案件は WTO（世界貿易機関）の政府調達協定の対象とのことが強調され、マスコミ報道などでも、適用除外の説明がなく、WTO 協定を正しく理解しなかったと思われる。実際、一部の政府職員や自治体職員でも、WTO 政府調達協定に「適用除外*」があることを知らなかった。

*) 1994 年の協定では、15 条「限定入札」、2014 年の協定では、3 条「安全保障のための例外及び一般的例外」で、自国の安全保障を脅かすものであれば、調達について WTO では適用除外とすることができるとしている。

9.1 WTO 政府調達に関する協定を改正する議定書

WTO 政府調達は、政府機関や地方自治体等が購入等で物品やサービスを調達する場合、国の安全保障や開発途上国での特定産業の保護・育成等の産業政策を目的としている。

(1) WTO 政府調達協定： 第 3 条 安全保障のための例外及び一般的例外

WTO 政府調達協定の 第 3 条 適用除外では、「安全保障」に関する事柄は WTO 政府調達協定を除外できる[22]。

1 この協定のいかなる規定も、締約国が自国の安全保障上の重大な利益の保護のために必要と認める措置又は情報であって、武器、弾薬若しくは軍需品の調達又は国家の安全保障のため若しくは国家の防衛上の目的に不可欠の調達に関連するものにつき、その措置をとること又はその情報を公表しないことを妨げるものと解してはならない。

2 この協定のいかなる規定も、締約国が、次のいずれかの措置を講ずること又は実施することを妨げるものと解してはならない。ただし、それらの措置が、同じ条件の下にある締約国間において恣意的若しくは不当な差別の手段となるような態様で、又は国際貿易に対する偽装した制限となるような態様で適用されないことを条件とする。

(a) 公衆の道徳、公の秩序又は公共の安全の保護のために必要な措置
(b) 人、動物又は植物の生命又は健康の保護のために必要な措置
(c) 知的財産の保護のために必要な措置
(d) 障害者、慈善団体又は刑務所労働により生産される物品又は提供されるサービスに関する措置

9.2 調達方法について

(1) 調達機器の変化

- 機器のソフトウェア化： 最近のセキュリティ機器の多くはソフトウェアが搭載されており、更に、ハードウェアをソフトウェアで代替する「ハードウェアのソフトウェア化 」もあり、その流れは益々加速していくものと思われる。ソフトウェアが搭載されることで、ソフトウェアのバグ／脆弱性やオンラインでソフトウェアを更新する時にバックドアが組み込まれる恐れもある。

(2) WTO 政府調達の誤解

通信システムの製品調達でも、WTO 政府調達に例外事項があることを一部の官庁や自治体の職員は誤解しており、「総合評価落札方式」でも、価格入札と同じ考えをしている。

このため、官庁、自治体の職員に、調達時には WTO 政府調達に適用除外があり、「総合評価落札方式」の採用でも、価格点だけでなく、技術点等を考慮し、適切なバランスで評価する必要があることを周知する。

政府・自治体だけでなく、独立行政法人や重要インフラ業界も周知の対象とすべきであろう。

(3) 調達について

① 総合評価落札方式

詳細は、「情報システムの調達に係る総合評価落札方式の標準ガイドライン」（平成 25 年 7 月 19 日）にあるが、入札時の価格、性能、機能、技術等の結果で落札する。

- 入札価格の得点配分の割合は全体の四分の一以上
- 技術要件は、調達目的・内容に応じ、必須項目とそれ以外に区分し、必須項目は、最低要件を満たさないものは不合格とするが、その他、必須・非必須の評価で得点を与える
- 入札価額及び技術要件の得点を加えて、評価する
- 開札前に資料のヒアリングを実施できる

② 評価について

- 入札価格と価格以外の評価点の重み付けが重要だが、入札価格の得点配分が全体の四分の一以上であるため、評価方法によって、価格入札と同じ結果になることがある
- ヒアリング（プレゼンテーションとＱ ＆ Ａ）を行うことにより、提案資料だけで判断できない入札者の事柄が明確になることが多い。 実際、プレゼン時間の半分程度を企業説明に費やす、あるいは複数社で入札参加したが、各社の考えが異なることが判明したこともある
- また、「プレゼンテーションと Q&A」の実施により、入札者が適切な数に減ることがある
- 評価者（組織内、外部有識者）の選定： 専門的かつ第三者の評価者グループを組織化する。政府や自治体、独立行政法人等を対象とする

などを考慮する必要がある。

9.3 サイバーセキュリティ製品の現状

① 国産のサイバーセキュリティ製品は皆無に近く、海外製品の調達が基本になるが、調達時及び運用時に以下のことを考える必要がある。

- 調達製品が古いバージョン（ハードウェア／ソフトウェア共）でないことを確認する。 国内マーケットが小さいと供給される製品は古い製品が提供されることがある。
- ソフトウェア等に「バックドア」がないことを確認する。運用時におけるプログラム更新時も同様。

② 特定国や特定企業の製品を排除する必要はないが、製品に「バックドア」等を設

け、違法に機密情報や個人情報を漏えいする仕組みがないかを検査する体制を構築する。

詳細は、「9.4 海外の状況」や「４．機器等の検証システムの確立」、「7. Bug Bounty Program」を参照して欲しい。

9.4 海外の状況

WTO 政府調達の「適用除外」と明確になっていないが、明らかにナショナルセキュリティの観点からの対応と思われる。

（１）米国

- 中国の通信機器調達

① 米連邦通信委員会（FCC）は 2018 年 4 月 17 日、通信会社が中国製品の調達を禁じる方針を決めた。全国に通信回線を普及する目的で設けられた同委員会の補助金を使う通信会社は、安保上の懸念がある Huawei Technologies と ZTE の製品の調達を禁じるとした[23]。

② 下院情報特別委員会（HPSCI: House Permanent Select Committee on Intelligence）は 2012 年 10 月 8 日、中国のインフラ機器ベンダーである Huawei Technologies と ZTE の 2 社の調査レポートを発表した。Huawei と ZTE のインフラ機器やサービスの調達に関し、アメリカ企業は、国家保安上のリスクから「他社を検討することを推奨する」とした[24]。

- 米 Amazon.com は、2017 年 7 月 31 日、BLU 製 格安スマホの販売を停止した。 ユーザ情報を中国へ送信していることが判明したための措置。なお、同一機種は国内でも販売されていた [7]。
- レノボは、2017 年 9 月 5 日、ノート PC に危険なアドウェア（Adware「Superfish」）をプリインストールしていたとして、2 年半にわたり米連邦取引委員会（FTC）と対立していたが、和解した【和解金 350 万ドル：約 3.85 億円】 [25]。
- カスペルスキー（Kaspersky：本社：ロシア）製のセキュリティソフトの政府内利用の禁止を上院が可決した（2017 年 9 月 20 日）[8]。

（２）英国

- 安全保障に関わる情報を扱う政府機関は、カスペルスキーのウイルス対策ソフトを使用しないよう通達をだした（2017 年 12 月 2 日）[9]。

（３）ロシア

- ロシア政府は、Windows ソフトのソースプログラムをマイクロソフト社との間で、開示契約を結んだ[14] [15]。

参考資料

[1] Bloomberg Businessweek, The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies, 2018 年 10 月 4 日

[2] 新座洞道火災事故の「電気関係事故報告」ならびに経済産業省からの指示に伴う緊急点検結果報告書の提出について　http://www.tepco.co.jp/pg/company/press-information/press/2016/1336104_8622.html

[3] ロイター、「サイバー攻撃は北朝鮮の犯行」、オバマ氏が対抗措置表明、2014.12.20、https://jp.reuters.com/article/obama-north-korea-idJPKBN0JX29220141219

[4] 日本経済新聞、パナソニックのバッテリー欠陥を認定　東京地裁が賠償命令、2019/3/22

[5] Government Technology、Security First、2002 年 07?01?、http://www.govtech.com/security/Security-First.html

[6] 日本経済新聞、中国・百度、ネット入力情報を無断送信　漏洩の恐れ 、2013 年 12 月 26 日、https://www.nikkei.com/article/DGXNASDG2600W_W3A221C1CC0000/

[7] 米 Amazon が米 BLU 製格安スマホを販売停止、ユーザー情報を中国へ送信、2017 年 8 月 2 日、http://tech.nikkeibp.co.jp/it/atcl/news/17/080202046/

[8] 米上院、カスペルスキー（ロシアのセキュリティソフト企業）の政府内利用禁止を可決、2017 年 9 月 20 日、http://jp.techcrunch.com/2017/09/20/20170918senate-kaspersky-shaheen-ndaa/

[9] BBC News, Kaspersky Labs: Warning over Russian anti-virus software, 2017.12.02, http://www.bbc.com/news/uk-42202191

[10] スウェーデンで大規模情報漏えい 運転免許データが閲覧可能に、2017 年 7 月 25 日、http://www.afpbb.com/articles/-/3136871

[11] READER SUSPECTS SINGTEL OUTAGE IS AN ATTACK FROM CHINA!、https://www.allsingaporestuff.com/article/reader-suspects-singtel-outage-attack-china

[12] 内閣サイバーセキュリティセンター、IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ、https://www.nisc.go.jp/active/general/pdf/chotatsu_moshiawase.pdf

[13] WTO 政府調達では、附属書 I（各国の適用範囲）https://www.wto.org/english/tratop_e/gproc_e/gp_app_agree_e.htm

[14] 日経 BP 社、Windows ソース･コードを閲覧する最初の政府はロシア、2003 年 01 月 23 日、http://tech.nikkeibp.co.jp/it/free/NT/NEWS/20030123/4/

[15] C¦Net Japan、マイクロソフト、「Windows 7」などソースコードの提供で露政府と合意、2010 年 07 月 09 日、https://japan.cnet.com/article/20416535/

[16] The Knightmare、Secrets of a Super Hacker、1994.1.1

[17] NIST：National Institute of Standards and Technology（アメリカ国立標準技術研究所）https://www.nist.gov/　NIST 軽量暗号ウェブサイト：https://csrc.nist.gov/projects/lightweight-cryptography

[18] バグ報奨金プログラム「ペンタゴンをハックせよ」が成功を納める、https://the01.jp/p0002585/" Hack the Pentagon:Hackers find over 100 Bugs in U.S. Defense Systems https://thehackernews.com/2016/03/hack-the-pentagon.html"

"Hack the Pentagon" Fact Sheet - June 17, 2016　https://www.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf

[19] C¦Net Japan、米国防総省、バグ発見者への報奨金支払いプログラムを拡大へ、2016 年 06?21?、https://japan.cnet.com/article/35084584/

[20] トレンドマイクロ、2019 年セキュリティ脅威予測、https://resources.trendmicro.com/jp-docdownload-form-m099-sem-2019prediction.html?gclid=Cj0KCQjw4fHkBRDcARIsACV58_Ei3Uouwo8Q9pCauo1r22eoi70_brO701EIXrxvlG1qwHP3AZC4fCQaAm8KEALw

_wcB

[21] R. D. Austin 他、ビジネスリーダーにＩＴがマネジメントできるか -あるＩＴリーダーの冒険、日経 BP 社

[22] 外務省、WTO 政府調達に関する協定を改正する議定書、2017 年 12 月、http://www.mofa.go.jp/mofaj/files/000030480.pdf

[23] 米、中国ＩＴに疑念：通信機器調達 ２社製禁止 技術競争で焦りも、2018 年 04 月 19 日，https://www.nikkei.com/article/DGKKZO29522270Y8A410C1FF1000/

[24] Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE、2012 年 10 月 20 日 https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

[25] Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security、2017 年 9 月 5 日、https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmedconsumers-preinstalled

分科会開催実績（2018 年度）

○ 第 1 回：2018 年 10 月 3 日開催
『IoT 機器におけるサイバーセキュリティの認証について』
登壇者：野々下　幸治（トレンドマイクロ株式会社 セキュリティエキスパート本部 エンタープライズ CSM 部 シニアプリンシパルカスタマーサービスマネージャー）

○ 第 2 回：2018 年 11 月 27 日開催
『経済産業省におけるサイバーセキュリティ政策の方向性について』
登壇者：加畑晶規（経済産業省　商務情報政策局　サイバーセキュリティ課 課長補佐）

○ 第 3 回：2018 年 12 月 18 日開催
『IoT セキュリティを支える軽量暗号の動向について』
登壇者：盛合志帆（国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所　セキュリティ基盤研究室長）

本報告書保存先
及びPW

GLOCOM 六本木会議

サイバーセキュリティにおけるナショナルセキュリティの検討分科会

最終報告書

執筆メンバー

内田 勝也

（主査、情報セキュリティ大学院大学 名誉教授）

立入 健太郎

（副主査、GRC-Lab 代表コンサルタント）

野々下 幸治

（トレンドマイクロ株式会社 セキュリティエキスパート本部 エンタープライズ CSM 部 シニアプリンシパルカスタマーサービスマネージャー）