論　文

2

サイバーセキュリティは ナショナルセキュリティ

情報セキュリティ大学院大学　名誉教授　**内田　勝也**

Ⅰ　はじめに

情報通信（ICT）システムの発展やインターネットの普及は従来の業務処理形態を大きく変えてきた。

・アナログからデジタルへ

ICTシステムの進展は、個人情報や企業等の知的財産等の情報がデジタル化され、さらに、「サプライチェーン」のセキュリティも課題になってきた。

・５Ｇと IoT 機器

５Ｇ（第５世代移動通信システム）の実用化により、IoT（Internet of Things）機器の接続により、これら機器のセキュリティ確保も大切になる。

・スマホ、電子メールのセキュリティ

政府・自治体、民間企業等での交渉案件は、電話（スマートホン）や電子メール等になり、その情報の保全も重要になっている。

・物理攻撃の影響

大規模なスポーツイベントが、令和元年秋から1年近く行われるので、大規模な妨害行為も指摘されている。首都圏の重要インフラへの物理的攻撃は、ICTシステムへも大きな影響がある。

・犯罪現場の変化

昔の銀行強盗は、ピストルや刃物を持って行員や来客を脅し、現金を強奪した。現在、銀行の支店にはあまり現金がなく、インターネット経由であれば、遙かに多額の金額を強奪できる。

現金は、３億円／人程度だが、ネットでは、数十億円／人の盗取もでき、行員や来客への殺傷もない。

1990年頃、情報セキュリティ／サイバーセキュリティを「ナショナル　セキュリティ」と捉え、対応する必要性を感じた。

今般、GLOCOM[注1)]「六本木会議」で、サイバーセキュリティ研究の募集があり、2017年から２年間の限定研究を行った。

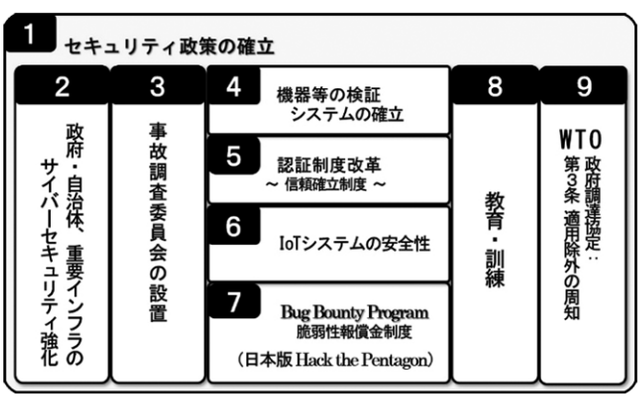
注１）　国際大学グローバル・コミュニケーション・センター（GLOCOM）は、1991年に設立の国際大学付属研究所で、学際的日本研究や情報通信技術の発展と普及に根ざした情報社会の研究と実践活動を中心に産官学民の結節の場として、常に新しい社会動向に関する先端研究所であることを目指している。

Ⅱ　政策検討の概要

以下９項目を検討した（図１）。

１．セキュリティ政策の確立
２．政府・自治体、重要インフラのサイバーセキュリティの強化
３．事故調査委員会の設置
４．機器等の検証システムの確立
５．認証制度改革
６．IoTシステムの安全性確保
７．脆弱性報償金制度の確立及び実施
８．教育・訓練の確立
９．WTO政府調達協定：第３条適用除外の周知

図１　検討項目：９項目



１．セキュリティ政策推進体制の確立

サイバーセキュリティでは、技術者の育成だけで

なく、管理者や担当者等の人材を含めた推進（セキュリティプロジェクトの推進やセキュリティ文化の確立）が大切になる。

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）

米国の政府高官等が公務での「私用アカウント」利用があった。国務長官ヒラリー・クリントンは、公務メールに、個人のスマートフォンを利用したことが問題[(1)]になった。

② 機器のセキュリティポリシー

タブレットやスマートフォンの利用は、それらの利用だけでなく、機器のセキュリティも考える必要がある。

③ 利用規約や違法措置

一部のタブレットやスマートフォンは、利用規約で生産国の規約に準拠とあるが、利用者の意図に反した動作（盗聴、盗視等）が発生している。

米国でサーバーに後付の微少チップが見つかった[(2)]。スマートフォンも可能性はある。

1.2　高度技術者のグループ化＆地域振興

高度な技術者・管理者の教育・訓練については、後述（「８　教育・訓練」する。

1.3　物理的対策

① 通信及び電力ケーブルのセキュリティ[(3)]

サイバーセキュリティに関係ないとの指摘もあるが、データセンター内のケーブル類の検討は重要である。クラウド利用でも東日本大震災時に回線接続ができず、処理が中断した例もある。

② 2006年８月「首都圏停電」

旧江戸川上空を横断する高圧電線にクレーン船が接触し、３時間余り停電し、自家発電での切替えトラブルで株価算出ができなくなり、また、電力復旧時に電源投入順序が不適切で、過電流になり、システムダウンし、データベース不整合のトラブルも発生した。

③ 大規模災害対応

2015年９月、茨城県常総市で鬼怒川（上流で500㎜/３日間以上の降雨）が氾濫し、市役所本庁舎が浸水被害を受けた。

温暖化の影響と思われる大規模台風や前線に伴う豪雨、洪水が発生し、データセンターや利用端末等の被害が発生している。

阪神・淡路大地震や東日本大地震でも、多くの被害例がある。

1.4　ロードマップの作成・更新

ロードマップは、５年から10年程度の期間を想定し、プロジェクトの優先順位や計画全体（５年、10年）を考えて、全体を明確にする。

２．政府・自治体、重要インフラのサイバーセキュリティの強化

2.1　サイバー攻撃・サイバーテロへの対応強化

2014年、米国映画会社へのサイバー攻撃は、日本企業子会社への攻撃で、攻撃元と思われる国の最高指導者暗殺のパロディ映画の予告編が公開（６月）され、５か月後の11月に、サイバー攻撃が行われた。

グループのサイバーセキュリティ対策は杜撰であったが、サイバー戦争／テロとも想定され、記者会見[注2)]や大統領のコメントもあり、政治問題に発展した。一企業へのサイバー攻撃が国家的問題に発展した例と言える。近年の世界情勢からは、他人事ではない。

注２）現在、米国ではセキュリティインシデントの記者会見はない。今回は例外。

2.2　サイバーリスク保険

サイバーリスクに対し、対象の保険もある。

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、検討が必要であろう。

３．事故調査委員会の設置

3.1　セキュリティ分野での事故調査の現状

大規模情報漏えいでは、第三者委員会が、調査を行うが、民間企業では、顧問弁護士が中心で、セキュリティ技術者の委嘱が中心となり、業務処理等検証の専門家が参加しない。民間企業での実態は、第三者委員会でなく、事故の原因が明確にされないこと

が多い。また、「プライバシー」を理由にして、情報が公開されないことも多い。

政府・自治体等は、関係省庁が調査委員を決めるが、調査内容は民間と変わらない。

3.2　政府機関としての安全委員会の設立

①　事故調査委員会の必要性

セキュリティインシデントの多くはヒューマンエラーやソーシャルエンジニアリングが多く、この分野やセキュリティマネジメント、管理・運用の専門家の参加が求められる。

国内には「運輸安全委員会」があり、政府・行政サービスや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ため、政府機関として「サイバーセキュリティ安全委員会」の設立が必要である。

②　サイバーセキュリティ安全委員会の特性

初期段階では、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等の事故調査を行う。

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、技術的な脆弱性より、人間の心理的な弱さや業務処理の欠陥を狙ったものが多い。　古くから「高度な技術者の攻撃より、設定ミスやパッチ未適用が大部分」との指摘[3]もある。

教育・訓練や組織対応など人的セキュリティや包括的サイバーセキュリティ対策、事故調査を基にした対策が必要。

４．機器等の検証システムの確立

機器内にある情報は、ネットワークに接続されていれば､気づかれずに外部へ送信できる。このため、「個人情報」や「企業情報」､「知的財産」等の重要情報が漏えいする可能性は高い。

個人や企業の情報の漏えいは、さらに大規模な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

国内外で発生した主な情報漏えい等の事例には、以下のものがある。なお、⑥は、その対応策の１つと考えられる。

①　日本語入力ソフトで入力情報を送付した[5]。

②　スマホのファームウェアに「バックドア」があり、個人情報を自社サーバーに送付した[6]。

③　米国及び英国政府は、ロシア製コンピュータウイルス対策ソフトの購入禁止を政府機関に通達した[7][8]。

④　スウェーデン運転免許データ漏えいでは、システム受注企業が、国外下請け企業に外注し、海外IT技術者が機密情報を閲覧可能にした[9]。

⑤　シンガポールの大規模ネットワーク障害は、中国の攻撃の疑念が指摘されている[10]。

⑥　ロシア政府は、Windowsソースコードの公開をマイクロソフト社に求めた[11][12]。

4.2　違法機器の検出

利用機器やソフトウェア、サービスの自由な利用は望ましいが、違法な情報転送も多い。

全ての機器等を検証するのは、要員や費用を考えると容易でないため、以下の対応を考える。

①　日本版「Bug Bounty Program（脆弱性報償金制度)」の実施（７参照)。

②　機器等の「違法情報送信」検証は、上記①を含め、重要事項検出に報償金や顕彰等を行う。

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。

このためにも、官庁や自治体システムの見直しが必要である。例えば、

・自治体では、県内の町村会での共同利用だが、都道府県を越えた共同利用を行う。

５．認証制度改革　～信頼確立制度～

5.1　信頼性確立制度について

ISO/IEC認証制度は、欧州で検討が始まったが、根底に分業化で、調達で購入先や製品品質は、一定の品質保持企業には、購入前の調査・検証を軽減する仕組みを考えた。情報セキュリティ、環境マネジメント等も行われるようになり、サプライチェーンでの調達も対象になる。

なお、ISO/IEC等では、「認証機関」と言われるが、実際には、「監査（Audit）機関」で、調査・検証は

「Audit」である。

監査・認証が不適切であれば、サプライチェーンが形骸化・崩壊する。

製品やサービス、セキュリティ等が信頼の判断は簡単ではなく、いくつかの方法があるが、「一長一短」がある。

第三者認証：

① 検査（チェックリスト）方式
- ・作成されたチェックリストを基に、チェックを行う
- ・「PCI-DSS」（クレジットカード業界）がある

② 監査方式[注3)]
- ・制度全体や重要項目、「管理策・管理目的」を基に、被監査組織は、①リスク分析、②管理策・管理目的の加除訂正、③適用宣言書を作成（含経営者の承認）し、審査を受ける。

注３）ISO/IECは、「監査（Audit）」だが、国内は「審査」で、それに準拠して説明している。「audit」は、「聴く」と同じ語源で、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）に近い。

5.2 ガイドラインの検討

認証制度は、管理・運用面の課題が多い。

本来、認証制度は、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。各認証制度の特徴を検討し、利用方法やガイドラインの再検討の必要がある。

5.3 IT調達方針及び調達手続き

2018年12月「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[13]」が公表され、政府機関の情報システム・機器・役務の重要性の認識を求めている。

WTO政府調達の適用除外（「９」参照）に該当するが、サプライチェーンも考慮する必要がある。

WTO政府調達は、附属書I（各国適用範囲）[14]で都道府県及び指定都市も対象としている。

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になり、パソコンやタブレット、スマートフォン等と比べ、遙かに小さな機器も接続され、機器やデータの保全、プライバシー保護が必要になってきた。

6.1 軽量暗号

従来の暗号製品を実装できない機器にセキュリティ等を確保する目的で、暗号開発が行われ、「軽量暗号」と呼ぶ。

軽量暗号（Lightweight Cryptography）では、

① 安全性要件：簡単に解読されない暗号強度

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

等を考える。

軽量暗号も、AES（Advanced Encryption Standard）と同様、NIST[15]が、2019年２月25日までに軽量暗号候補を募った。数年後に軽量暗号が標準化されると思われる。

ただ、IoTは普及しており、軽量暗号標準が決まるまで、機器に搭載する軽量暗号は、搭載／非搭載を含め、独自に決めなければならない。

6.2 Umbrellaの作成

(1) パッチ未適用ソフト

情報機器導入後、ソフトウェアの脆弱性対応で、ベンダーがパッチ（脆弱性修正）プログラムを提供するが、

① パッチプログラム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、利用者がパッチを実施しない

③ システム停止ができない等で、パッチプログラムを適用しない

このため、ソフトウェアの脆弱性により、大きな被害例[注4)]もある。

注４）2017年５月、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。英国国民保健サービス（NHS）等で被害があったが、パッチプログラムを事前に適用していなかった。

(2) Umbrellaの作成（仮想パッチ【Virtual Patch】）

パッチマネジメントでは、

① 24時間・365日の稼働で停止できない
② 導入ソフトウェアの事前調査後、パッチ適用後に、正常に動くかの検証に時間がかかる
③ パッチ適用後のトラブルで復元時間が必要
④ 緊急時は、短時間でパッチ適用が必要
⑤ 脆弱性対応のパッチが未公開

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ている。

パッチマネジメントの困難さを克服する仕組みとして、脆弱性機器に傘（Umbrella）をさし、脆弱性攻撃を止める仕組みで、全ての脆弱性を一か所で対応する。傘下の機器・ソフト等の脆弱性に十分な時間をかけることが可能になる。

この方法は、パッチ適用が無理なシステムやパッチプログラムの未提供でも対応できる。

6.3 セキュリティ開発体制の確立

機器やソフトウェア開発は、大きく①設計･開発、②実装、③保守･運用の３段階があり、セキュリティでは、SDL(Securit Development Lifecycle)と呼ばれる。各段階で考える必要があるが､上記①や②は、③を考える必要がある。

・ユーザ名／パスワードの初期設定ミス

セキュリティを考えず、機器をネットワークに接続していた。認証なしや同一機器全て同一ユーザ名／パスワードで、内部情報が漏えいや「踏み台」にされた[注5)]。

注５）Secrets of a Super Hacker（1994年１月発行）で、UNIX等のコンピュータのパスワードが既知（固定値）とあり、日本語版はAppendicesを全て削除した。なお、国内で指摘された既知のパスワード等の例は以下（図２参照）に示す。

・2004年10月、ハードディスク搭載のDVDが外部者に踏み台にされた。ユーザ名、パスワード入力不要であったことが原因である。https://internet.watch.impress.co.jp/cda/news/2004/10/06/4882.html
・コピーやスキャナー、FAX等の機能の「複合機」の保存情報が外部からアクセスされ、漏えい。出荷時に複合機のパスワードが全て同一、ユーザ名やパスワードがない等。https://www.nikkei.com/article/DGXNASFK1302W_T11C13A1000000/
・ネットワーク接続の監視カメラのパスワード設定が杜撰で、外部からアクセスされ、自由にアクセスでき、画像（動画も）がみることができた。

図２ 既知のIDやパスワードによるインシデント例

(1) 共通鍵暗号の落とし穴

共通鍵暗号は、暗号化／復号で、同一の鍵を使い、二者利用が前提だが、複数間で使い、問題が発覚した。

(2) 暗号の危殆化など

① 暗号の危殆化： 安全性は、「コンピュータの計算能力の向上」や「新暗号解読手法の出現」で低下する。これを暗号の危殆化と呼ぶ。
② 独自暗号利用の危険性： 独自開発の暗号は安全との考えがあるが、標準軽量暗号検討時でも、検討席上で、安全性に問題があると指摘されたこともある。

(3) 訴訟リスク（製造物責任法：PL法）

PL法はソフトウェアは対象外だが、ソフト利用の機器等は対象になる。

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に地裁は支払いを命じた[(16)]。

７．脆弱性報償金制度

脆弱性報償金制度(Bug Bounty Program)は、構築ネットワークを第三者が攻撃や実践的調査を行い、脆弱性を発見・報告する。

2002年７月、Government Technologyがウェブに、2001年の米国防総省の調査では「97、98％は設定ミスかパッチ未適用」[(17) 注6)]とある。

脆弱性報償金制度は、2016年４月、パイロットプログラムが実施され、専門家を募集・登録し、米政府のウェブの脆弱性検証をさせた。その結果､1,400人余の登録ハッカーが、報償金に値するウェブの脆弱性を138件発見した。

報償金は100 ～ 15,000ドル／件で、支払総額は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ている[18][19]

注６）ハワード・シュミット（Howard Schmidt：米国大統領重要インフラ保護委員会副委員長）は、「米国国防総省の2001年調査では、97 ～ 98%は、パッチの未適用か設定ミス」と述べている。

８．教育・訓練の確立

高価な機器等も管理・運用や情報収集のための人材が必要で、高価なセキュリティ機器の導入しても、利用者等がユーザID／パスワードを他人に漏らせば、ネットワークに侵入される。また、内部者の犯行も増えており、運用・管理が大切になる。

8.1　教育・訓練

①　脆弱性：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最も弱い所が、「セキュリティレベル」で、セキュリティの最大の脆弱性は人間と言われたが、

・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か
・「予兆」を見いだし、対応の教育・訓練ができていれば、インシデントを回避できる
・最近の攻撃は、主に人間を対象としている
・「RSA Conference2019」で、Lance Spitzner（SANS.org）も、「人間は、ウィーケストリンクでなく、主要な攻撃目標になっているだけ」と述べた

②　理論と実践

サイバーセキュリティの教育・訓練では実践や想定外の対処ができる教育・訓練が大切である。短期間に要求レベルの人材を育成には育成方法も大切で、当初は十分な教育・訓練が必要だが、高度な教育・訓練は環境の提供でも良い。

8.2　教育・訓練概要

①　教育・訓練対象者

教育・訓練内容を、４グループとし、対象者全員を対象としたコースを加えた教育・訓練概要を図３に示す。

図３ 教育・訓練概要

②　教育・訓練内容

【A】対象者全員

基礎的な講義と基礎的なハッキングやパケット監視ソフト等の実践的教育・訓練を行う。

【B】セキュリティ技術者

ハイレベルでは、教育・訓練環境を提供し、Bug Bountyや事故調査、機器等の検証等への参加で実践的な研鑽を行う。

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になる。

【C】セキュリティ管理者／リーダ

広範なセキュリティ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受ける知識・経験を持つ管理者／リーダの育成を目指す。インシデント発生時に技術者や広報・法務部門、経営者／ CIO ／ CISO等との橋渡しを行う。

【D】経営者／ CISO

経営者やCISOの教育・訓練は、長期的・広範な決断の教育・訓練になる[20]。

【C】、【D】は、リスクマネジメントやガバナンス、地政学等、サイバーセキュリティ分野により、幅広い知識の修得になる。

【E】利用者（法務・人事・経理等）：日々のコンピュータ利用上の問題について基礎的課題の発生時に、セキュリティリーダ等に迅速に報告することで、セキュリティ文化を根付かせる役割を持つ。

９．WTO政府調達協定第３条適用除外の周知

第３条WTO適用除外の周知を行う。

9.1　WTO政府調達協定を改正する議定書

WTO政府調達は、政府や自治体等の物品・サービスの調達等だが、適用除外[21]がある。

9.2　調達方法について

(1) 調達機器の変化

多くの機器はソフトウェアが搭載され、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更新でバックドアが組込まれる恐れもある

(2) 調達について

① 総合評価落札方式：「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」(H25年7月19日）があり、入札時の価格、性能、機能、技術等の結果で落札する。

② 評価について:ヒアリング(プレゼンテーションとQ＆A）で、提案資料だけで判断できない入札者の事柄を明確化できる。また、ヒアリングの実施で、入札者が適切な数に減ることもある。

9.3　サイバーセキュリティ製品の現状

① 海外製品の調達が基本になるため、調達及び運用時に以下のことを考える必要がある。

・ソフトウェア等の「バックドア」の確認をする。プログラム更新時も同様。

② 特定国や特定企業の製品排除は不要だが、違法に機密情報や個人情報を漏えいがないか検証する体制や情報収集を行う。

参考資料

(1) ABC News、Hillary Clinton Says She Didn't Use 2 Phones as Secretary of State -- but She Does Now、https://abcnews.go.com/Politics/hillary-clinton-phones-secretary-state-now/story?id=29535505

(2) 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, 2018.10.04

(3) 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

(4) Government Technology、Security First、2002.07.01、http://www.govtech.com/security/Security-First.html

(5) 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、2013.12.26、https://www.nikkei.com/article/DGXNASDG2600W_W3A221C1CC0000/

(6) 米Amazon が米BLU製格安スマホを販売停止、ユーザ情報を中国へ送信、2017.08.02、http://tech.nikkeibp.co.jp/it/atcl/news/17/080202046/

(7) 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、2017.09.20、http://jp.techcrunch.com/2017/09/20/20170918senate-kaspersky-shaheen-ndaa/

(8) BBC News, Kaspersky Labs: Warning over Russian anti-virus software, 2017.12.02, http://www.bbc.com/news/uk-42202191

(9) 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、2017.07.25、http://www.afpbb.com/articles/-/3136871

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

(11) 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、2003.01.23、http://tech.nikkeibp.co.jp/it/free/NT/NEWS/20030123/4/

(12) CNet 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、2010.07.09、https://japan.cnet.com/article/20416535/

(13) 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

(14) 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

(15) 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

(16) 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、2019.03.22

(17) Government Technology、Security First、2002.07.01、http://www.govtech.com/security/Security-First.html

(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

(19) CNet 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、2016.06.21、https://japan.cnet.com/article/35084584/

(20) 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

(21) 外務省、WTO政府調達に関する協定を改正する議定書、2017.12、http://www.mofa.go.jp/mofaj/files/000030480.pdf