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
2017 年度 報告書

2018 年 7 月

情報通信システムは、電子メール、電子会議（テレワーク）、IP 電話、スマートフォン等のデジタル機器やそこで扱われるデジタル情報を中心にさらなる発展を遂げている。

それと呼応するかたちで、政府・行政サービスや重要インフラ等のネットワーク、コンピュータ・携帯端末等及び、それらで扱う情報のセキュリティを確保することは、国家・国民の観点からも、ますます重要になっている。

本分科会では、情報及び情報を扱う機器のセキュリティを確保することは、「安全保障：National Security」のひとつであると考え、包括的なサイバーセキュリティの確立が重要と考え、考察を行った。

本報告書を公開することで、多くの方々からのご意見や指摘を得ることで、2017 年度に検討できなかった部分も含め、2018 年度に更に議論を深めたい。

ナショナルセキュリティにおけるサイバーセキュリティの検討分科会

検討分科会 メンバー

主　査　内田　勝也　　情報セキュリティ大学院大学　名誉教授
副主査　立入　健太郎　GRC-Lab　代表

池尾　和彦　　大日本印刷株式会社 ＡＢセンター マーケティング本部
今川　拓郎　　総務省 情報流通行政局 情報通信政策課長
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
河東　哲夫　　Japan and World Trends　代表
小林　寛三　　国際大学 GLOCOM　主幹研究員（併任）
境　　真良　　国際大学 GLOCOM　客員研究員
冨米野孝徳　　株式会社インターネットイニシアティブ　経営企画本部
山田　隆裕　　総務省　情報流通行政局　サイバーセキュリティ課
前川　徹　　国際大学 GLOCOM　所長

事務局
小林　奈穂　　国際大学 GLOCOM　プラットフォーム研究グループ　主任研究員

※ 検討分科会メンバーは、個人としての参加で 所属企業・組織を代表するものではありません

Index

５つの提言：
安全保障＝ナショナルセキュリティとしての包括的なサイバーセキュリティ確立を

Society5.0 が目指す社会は、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立するものである。政府機関も例外なくデジタル化が進むなか、サイバーセキュリティへの対応は、もはやサイバー空間だけの問題では無くなっている。サイバーセキュリティを重要なナショナルセキュリティの構成要素としてとらえつつ、あまりにも脆弱な現状をひとつひとつ、丁寧に、できることから変えていくことを提言する。

1 WTO 政府調達協定：第３条 適用除外の周知

政府や独立行政法人、自治体職員の中に、これを知らず無条件に機器やソフトウェア、サービスの入札を行うことが多く、セキュリティリスクを十分に考慮することなく海外製品を導入しているのが実情である。WTO 政府調達協定の第３条には「安全保障のための例外及び一般的例外」があり、重要システムは、その対象となりうる。つまり、セキュリティの観点から、調達時に柔軟に対応する必要とそのための例外規定があることを徹底的に周知する必要がある。

【国を守るグローバル・ルールを知ろう。】

2 日本版「Hack the Pentagon」の実施

米国国防総省は、公開ウェブの脆弱性を発見する「脆弱性報奨金プログラム：Hack the Pentagon」を実施した。応募した約 1,400 人のハッカー（セキュリティ専門家）により 130 件以上の脆弱性が発見された。

このプログラムでは、最も破壊的な脆弱性の発見に対し、最大 15,000 ドル（約 165 万円）が支払われた。 このプログラムによる国防総省の支払総額は 15 万ドルで、同一業務を企業委託した場合と比べ、15% 程度に費用を抑えることができたと言われている。 同様のプログラムは、既に複数の民間企業も実施しており、ウェブの安全性対策に有効である。

実際のウェブへの攻撃・検査であり、構築したウェブの巧拙も判断でき、今後、外部委託での業者選択にも役立つと思われる。

日本でも同様のプログラムを行うことは、費用や業者の技術向上等にも役立つ。

【クラッカー対策にはハッカーを。】

3 認証制度改革　～ 信頼確立制度について ～

第三者の製品やサービス等の信頼性を判断することは必ずしも簡単でないため、主な方法には、以下のものがある。

1. 第三者認証
   (1) 検査（チェックリスト）方式
   (2) 監査方式
2. 自己認証（自己申告）
   (3) 検査（チェックリスト）方式
   (4) 自己監査／内部監査方式

これらは、「制度」と「管理・運用」があり、それらが適切であるか考える必要がある。

各方式は、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、それらを最低限に抑えることが大切になる。

認証制度の目的は、取引先が対象とする認証を取得していれば、調査費用の軽減や迅速な取引を可能にすることである。

二社間取引だけでなく、サプライチェーン等、多数の組織による取引でも、各社が一定水準を保持している前提があれば、容易に取引を行える。

ただ、セキュリティ関連の認証制度では、「管理・運用」面での課題が多いため、信頼できる管理・運用システムの確立・維持が重要である。

【チェックリストもチェックが必要。】

4 機器等の検証システムの確立

IoT や AI 技術の進展により、データ大流通時代を迎えたいま、多くの情報がデジタル機器やシステムに保存され、流通している。

こうした機器やシステム、サービスに蓄積されている重要情報が違法に外部送信されるというインシデントが発生している。国内での発見、報告例は少ないが、その理由は検知できていないだけの可能性が高い。

重要情報の漏洩を防止するため、機器等の検証システムの確立が急務である。

【情報流出の心配がない機器等にお墨付きを。】

5 事故調査委員会の設置

サイバーセキュリティの重要性を鑑み、政府や自治体、独立行政法人、重要インフラや大規模個人情報漏えい等の重大インシデントに対し、第三者として調査を行う「サイバーセキュリティ事故調査委員会」を設置すべきである。

事故を起こした組織が設置する形式的な第三者委員会では、真の原因究明が困難である。法令に基づく事故調査委員会の設置により、事故の真相を究明し、同種のインシデントの再発を防ぐことが可能になる。

【記者会見より、確実な再発防止策を。】

はじめに

情報通信システムの急速な発展は、電話や手紙、FAX 等のアナログ機器等から、コンピュータを利用した電子メール、電子会議（テレワーク）、IP 電話等のデジタル機器の利用やデジタル情報を保存するようになってきた。

政府・行政サービス等でも、二国間や多国間交渉等の機密情報や住民の個人情報などの多くをデジタル情報として扱っている。これらの情報漏えいは、国や自治体の信頼に大きな影響を与える。

「情報（データ）」は、保存場所の特定が難しく、用紙等への印刷やディスプレイへの表示でのみ情報をみることができるが、それらの媒体が必要で、コンピュータや記録媒体内の情報は直接みることはできない。

情報は単独で存在せず、ネットワークやコンピュータ機器に保存され、機器やソフトウェア、サービス等（以下、「製品」という。）を含め、保護が必要である。

全ての製品を国産に限定し、管理下に置くことは、欧米先進国等でも難しい。 しかしながら、日本は国内製品が皆無に近く、特定国や特定海外製品を排除することは難しい。

しかし、これらの製品が「国の安全保障（National Security）*1」を損なわないものであることを確実にする必要がある。

本報告書では、政府･自治体や独立行政法人、重要インフラ等のサイバーセキュリティを中心に考察した。多くの方々からご意見を得て、今後、未検討な部分や検討が浅いものを確実なものにしたい。

*1　National Security: サイバーセキュリティでは、国民の（個人情報や知的財産、政府･行政等のサービス）を保護・保全するものとしている。


CCD camera
CCD camera

1. WTO 政府調達について

1.1　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[1]。

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

1.2　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

情報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したり、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。

1.3 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、「1.4 海外の状況」及び、後述「2. 日本版「Hack the Pentagon」制度の確立」や「４．機器等の検証システムの確立」に述べる。

1.4 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 [2]。

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 [4]。

- 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。 ユーザー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 [5]。
- 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】[6]。
- 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）[7]。

（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）[8]。

（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 [9] [10]。

2. 日本版「Hack the Pentagon」の実施

2.1 「Hack the Pentagon」とは？

Hack the Pentagon 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、インシデント発生前に脆弱性を発見するもの。

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、攻撃されることがある。

2002 年 7 月に Government Technology がウェブに掲載したものでは、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 [11] *2 。

Hack the Pentagon 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、報償金に値する公開ウェブの脆弱性が 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、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 [12] [13]。

*2　ハワード・シュミット（Howard Schmidt）は、「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。

2.1 「Hack the Pentagon」のメリット

外部委託に比べ、安価な費用で行え、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 *3 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。

2.3 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。

*3　訓練システムでもあらゆる事を考慮しているとの指摘があるが、確認できていない。 例えば、スイスチーズモデル、個々の事象ではセキュリティが確保されるが、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。

GLOCOM
六本木会議

3. 認証制度改革～信頼確立制度について～

3.1　信頼確立制度について

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可能になる。

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」ではなく、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。　内部監査人は、業務知識や高度な監査能力が要求される
- 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、認証を付与する
- 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 *4 ）」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

*4　英語の「audit」は、「聴く」と同じ語源で、「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）

（3）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。

（4）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)。
- 「NIST SP800-171」は自己認証方式が採用されているが、構築時には「コンサルティングサービス」等を利用することもある。　なお、米国では、NIST SP800-171 と「FedRAMP（Federal Risk and Authorization Management Program)」を組み合わせ、認証制度にしている。
- NIST SP800-171 は、国内ではこれから本格的になると思われ、今後 注目したい。

3.2　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高の 2%のいずれか高い方

2,000 万ユーロ、又は前会計年度の全世界年間売上高の 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金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、重大さ、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。

GLOCOM
六本木会議

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 [14]。

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 [5]。

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対し通達した。　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 [7] [8]。

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）[15]。

⑤ シンガポール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 [16]。

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 [9] [10] 。

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、簡単ではない。 そこで、以下の対応を考える。

① 米国国防総省で実施した「Hack the Pentagon」の日本版を計画する。

② 上記①での人材に対し、他の機器等の「無断、違法情報送信」の検出を依頼し、重要案件の発見により、報償金を支払う。　報償金に値しない場合でも、表彰する等がある。

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、

- 中央官庁には、メールサーバが、2,000 台あると言われている。　また、自治体は約 1,700 あり、県単位で中小自治体が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. 事故調査委員会の設置

5.1　事故調査について

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、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、公判の場で明らかになった例もあり、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。

5.2　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。

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。

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」との指摘もある [11]。

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。

5.3　事故調査委員会の設置とその代替（案）

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。

GLOCOM
六本木会議

参考資料

[1] 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
[2] 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/
[3] 米政府、中国ＺＴＥに近く罰金最大 17 億ドル請求の可能性 , https://jp.reuters.com/article/us-china-zte-idJPKCN1IZ0ZR
[4] 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
[5] 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/
[6] 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-harmed-consumers-preinstalled
[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 年 9 月 20 日、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] 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/
[10] 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/
[11] Government Technology、Security First、2002 年 07?01?、http://www.govtech.com/security/Security-First.html
[12] 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
[13] 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/
[14] 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/
[15] 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
[16] READER SUSPECTS SINGTEL OUTAGE IS AN ATTACK FROM CHINA!、https://www.allsingaporestuff.com/article/reader-suspects-singtel-outage-attack-china

GLOCOM 六本木会議

国際大学 GLOCOM では、情報通信分野において、次々と登場する革新的な技術や概念に適切に対処し、日本がスピード感を失わずに新しい社会に移行していくための議論の場として「GLOCOM 六本木会議」を 2017 年 9 月に設立しました。以降、分科会活動および年次総会など活動を推進しています。

GLOCOM
六本木会議

活動意義
情報通信分野において、次々と登場する革新的な技術や概念に適切に対処し、日本がスピード感を失わずに新しい社会に移行していくための議論の場を提供すること／政策提言活動を行うこと

活動目的
情報通信分野における幅広いテーマの検討とすり合わせ
産学官民・異分野の専門家による機動的かつ継続的で自由な議論の場
人的ネットワークつくりの場と新しいコミュニティのあり方の模索

期待する成果
国民的な議論の喚起と政策提言
→公共政策や経営戦略に速やかにフィードバックさせる、機動性の高いメカニズムの構築

http://www.glocom.ac.jp/roppongi_kaigi

【GLOCOM 六本木会議へのお問い合わせ先】
国際大学グローバル・コミュニケーション・センター
Center for Global Communications, International University of Japan

〒 106-0032 東京都港区六本木 6-15-21 ハークス六本木ビル 2 階
TEL: 03-5411-6685　Email：info_pf@glocom.ac.jp（担当：小林）