2G-05

ナショナルセキュリティとしてのサイバーセキュリティ

内田 勝也‡
情報サイバーセキュリティ大学院大学

はじめに

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.

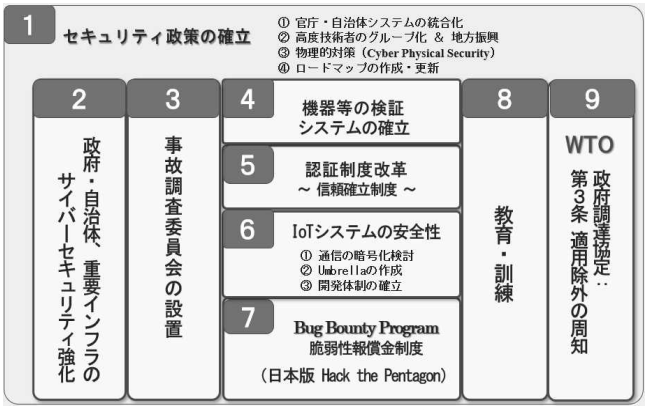
政府・行政サービス，重要インフラ等のネットワークだけでなく，スマートフォン等の携帯機器や民間企業のサプライチェーンにおけるサイバーセキュリティの課題も健在化してきた.

今年から本格化する 5G は，IoT 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が発生する可能性もある.

更に，東北アジアや中東の混乱や英国 EU 離脱，夏の東京五輪を考えるとサイバー攻撃や設備・機器破壊(Sabotage)等の可能性もある.

ナショナルセキュリティは国民・組織等が持つ個人情報や機器，企業等の知的財産等の保全もある.

このような状況を踏まえ，2017 年 11 月から約 1 年半，検討し，報告書を作成した[1]．全体概要を下図に，各項の概要を「1～9」で述べる.



ナショナルセキュリティ概要図

1 セキュリティ政策の確立

(1) 政策の立案・遂行は重要だが，情報を内部に抱える傾向が強い．セキュリティは『知らぬは利用者ばかり』が多い．広く『ステークホルダー』に周知し，『セキュリティ文化の確立』を目指し，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，独立行政法人等は，集中化やリスクに基づいたセキュリティ対策が必要．米国政府高官が私用スマホの不適切利用も明らかになり，国内も対応が急がれる.

(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，高齢者の有効活用も必要.

(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．電気や通信が途絶えれば，情報通信システムも機能を果たせなくなる.
実際，2019 年 10 月に日本を襲った台風 19 号では，電力や携帯電話網に大被害が発生した.

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.
2019 年 12 月 4 日のクラウド障害は約 50 自治体が被害を受け，12 月 24 日の報告，未だ 4%が未復旧[2]．自治体業務は，基本部分は同じで，複数クラウドを構築し，各自治体が正副 2 ヶ所に接続する仕組みで今回の事故は防げた.

(2) 世界的な緊張感が高まりは，サイバーセキュリティにも影響を及ぼす．国家元首のパロディ映画で映画会社への壊滅的なサイバー攻撃があった．地政学的緊張はサイバーセキュリティにも影響を及ぼす.
8 で述べる脆弱性報償金制度等を利用し，事前防御(proactive)対応も必要.

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おり，サイバーセキュリティ「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，適切な調査で，爾後の事件・事故防止に役立つ.

4 機器等の検証システムの確立

(1) 微細チップでの情報漏えいもあり，ソフトウェアをインターネットでの更新はバックドアの挿入も可能で，それらの検証が必要.

(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.
機器検証を行う動きも 2019 年末にでてきた[3].

Cybersecurity as National security
‡「Katsuya UCHIDA・Institute of Information Security」

5 認証制度改革

(1) 認証制度は『制度』と『管理・運用』があるが，管理・運用が十分でなく，審査機関・審査員等を含めた関係者への改革が望まれる．
(2) 2019 年 12 月に発覚した広域自治体のリースバックサーバのハードディスク内の文書流失は，リース会社及びデータ消去会社とも ISMS 認証を取得していたが，セキュリティマネジメント体制が確立されておらず，審査機関の審査（監査）が適切に行われたかの疑問が残る[4]．

6 IoT システムの安全性確保

(1) IoT のセキュリティでは，導入時の対応方法等が重要になってきた．
(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られるが，標準の軽量暗号が未定で，現時点での搭載は注意が必要．
(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）をさす仕組みの脆弱性対応もある．
(4) 開発段階で，SDL：Security Development Lifecycle を確立し，①設計・開発，②実装，③保守・運用の３段階で対策が必要．

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「Hack the Pentagon」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，発見された脆弱性が報償金に値すれば，100～15,000 ドル／件を支払った．支払い総額は約 15 万ドルで，外部委託 100 万ドル以上より安かった[5]．
(2) 2002 年 米国防総省調査では，97，98%はパッチ未対応か設定ミス．
(3) この制度は，費用対効果も良く，国内でも効果があると思われるが，国内では「手の内を明かしたくない」との考えがあり，海外程，積極的活用は少ない[6]．

8 教育・訓練の確立

(1) サイバーセキュリティで『人間は最大の脆弱性』と指摘されるが，教育・訓練に問題があると思われる．
(2) 国内は，管理者・リーダ，経営者・CISO，利用者等の教育・訓練が少ない．縦割りの教育・訓練でなく，必要な教育・訓練レベルを考えることが大切．
(3) 組織のサイバーセキュリティ対策は『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『適用除外』があるが，官庁・自治体や独法等の調達部門で，これを知らない職員が多く，周知を図る必要がある．
(2) 調達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し，高品質の提案を採用する．

10 今後の課題

(1) いくつかの項目は，既に，国内で実施が報道されているが，サイバーセキュリティは総合科学であり，実践が大切で，それらを今後は目指したい．
(2) 心理学や行動科学，社会心理学，環境犯罪学等を取り入れた教育・訓練や地政学，シミュレーション（含机上シミュレーション）等を含めたい．

11 謝辞

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報告書」を基にしています．2018 年度については，立入健太郎氏，野々下幸治氏の 3 名で検討し，報告書に纏めた．報告書内容についての責任は主査である筆者にある．

参考資料

[1] 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報告書，http://www.uchidak.com/seminar/CySec_FINALRep.zip
[2] 日本電子計算(株)，「Jip-Base」の障害における復旧状況のご報告(第 2 報)，https://www.jip.co.jp/news/20191225/
[3] 朝日新聞，【会見動画】文書流出，県知事が会見「想定外だった」，https://www.asahi.com/articles/ASMD64JQVMD6UTIL02K.html
[4] 日本経済新聞，スパイ部品，官民で監視　経産省，https://www.nikkei.com/article/DGKKZO53818140W9A221C1EAF000/
[5] DoD, “Hack the Pentagon” Fact Sheet - June 17, 2016, https://dod.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf
[6] 日本経済新聞，ホワイトハッカーの高額報酬広がる　Google は 1.6 億円，https://www.nikkei.com/article/DGXMZO53386390V11C19A2MM8000/