自由民主党
サイバーセキュリティ
対策本部

第１次提言

～リスクの最小化に向けて。「コスト」から「投資」への意識変革を～

2018 年４月 24 日

目　次

Ⅰ　はじめに

多くのモノがインターネットに繋がるＩｏＴの時代を迎え、ＩｏＴサービスへのＡＩの活用も始まり、新たなビジネスの創出や行政の電子化により、国民生活の利便性は飛躍的に向上しつつある。

今後も、多様な分野に於いて、サイバー空間を活用した新たな価値創造が進められていくことが期待される。

他方、2017 年には、日本に向けたサイバー攻撃は、1 日に約 4 億 1 千万回も観測されている。

近年は、不正送金マルウェアやランサムウェア（身代金要求型マルウェア）の悪質化・巧妙化・広域化、ＡＴＭへの攻撃が発生するなど、経済的利益目的のインシデントが目立ってきている。

また、ＩｏＴに対する攻撃が本格化し、監視カメラシステムやルータなどがマルウェア感染によって大規模なＤＤｏＳ攻撃（サービス妨害攻撃）のプラットフォームに利用されるなどの被害が発生している。

これらのサイバー攻撃は、従来の愉快犯的な攻撃から組織・企業の活動そのものに影響を与える攻撃に変わってきており、個人情報・知的財産・機密情報・金融資産の窃取、サービスの停止、重要インフラの機能障害など、各分野に於いて「経済的損失リスク」や「社会的信用喪失リスク」、「安全保障リスク」が増大している。

特に、「航空」、「鉄道」、「自動運転」、「医療」、「電力」、「安全保障」などの分野へのサイバー攻撃は、私達の生命を危険に晒すものであり、既に、国内外で極めて深刻なインシデントが数多く発生している。

サイバー攻撃は、容易に国境を越える上、匿名性・隠密性が高いことから攻撃者の確証を得ることは困難であり、攻撃方法や主体は多様であり、国際的な規制ルールも整備されていない。有効な対策を講じる上では、数多くの困難が存在する。

しかし、「国民の生命と暮らしを守り抜く」という国の究極の使命を果たす上でも、サイバーセキュリティ対策の強化は、政権にとって喫緊かつ重要な課題である。

このような現状を踏まえ、2017 年 11 月、自由民主党に、党則 79 条機関（総裁直轄機関）として、「サイバーセキュリティ対策本部」が新設された。

本部役員決定後の 2017 年 12 月 5 日より議論を開始し、合計 12 回の会議を経て、今般、『第 1 次提言』を取り纏めた。

従前より、我が党では、政務調査会のＩＴ戦略特命委員会や安全保障調査会に於いて「サイバーセキュリティ対策強化」の必要性が指摘され、2017 年 5 月に取り纏めた『デジタル・ニッポン 2017』など、内閣への提言を精力的に行ってきた。

よって、サイバーセキュリティ対策本部では、ＩＴ戦略特命委員会や安全保障調査会の主要

役員も構成員とし、これまでの党内議論の成果を十分に踏まえた上で、我が国のサイバーセキュリティ上の課題と必要な対策の方向性につき、分野別に深掘りをして議論を進めることとした。

『第１次提言』の作成までに当本部が議題とした分野は、現時点で政府のサイバーセキュリティ戦略本部が定める「重要インフラ 13 分野（航空、鉄道、物流、医療、電力、ガス、水道、石油、化学、金融、クレジット、情報通信、政府・行政サービス）」に加え、「自動運転」、「安全保障」、「量子コンピュータ」である。

この他にも、ＩｏＴ、ＩＣＴ、完全自動化が普及していく中で、間接的に生命や身体の安全性が脅かされる可能性がある分野としては、「農業」、「飲食業」、「建設業」、「スマートホーム事業」、「警備業」、「シェアリングエコノミー事業（カーシェアやルームシェア）」などが考えられる。これらの分野についても、引き続き、議論を続けることとする。

尚、当本部に於いては、各分野を所管する府省庁や有識者からヒアリングを行うに当たって、「現状のセキュリティの脆弱性」や「サイバー攻撃によって発生し得る具体的なリスク」など、「攻撃者にヒントを与えてしまう可能性がある機微な情報」や「個別企業の株価や業務に影響を与える可能性がある情報」も含まれることから、出席を国会議員本人限定とし、報道各社の皆様にも非公開とし、クローズな環境下で率直な議論を重ねた。

以下、本提言を取り纏めるに当たって留意した基本的な考え方を記す。

第１に、「サイバー攻撃によるリスクをゼロにすること」は現実的に不可能であることから、「リスクを最小化するための対策」を考えることとした。

第２に、本提言の構成だが、「国内外で発生した主なインシデント事例」、「サイバーセキュリティ対策の現況」、「残存する課題と検討が望まれる対策」について、書式を定めて分野別に整理した。このような形式の提言書は、政府与党内では初めてのものである。

ただし、前記した通り、「攻撃者にヒントを与えてしまう可能性がある機微な情報」も含めてクローズな環境下で議論を進めた経緯もあり、一部のインシデント事案については匿名化し、出席者の発言全てを掲載するものではない。

第３に、東京オリンピック・パラリンピック競技大会が開催される 2020 年を目標としたサイバーセキュリティ対策については、これまでも我が党で議論を進めてきた経緯から、「緊急に対処するべき短期的な対策」に加えて「2020 年以降も見据えた中長期的な対策」を求める提言とした。

第４に、予算要求上の制約や所管業界の多様な意見、国会日程などの事情から、各分野を所管する関係府省庁からは提案しにくいと考えられる野心的な対策についても、敢えて盛り込んだ。

あくまでも政党から内閣への提言であることから、法制度整備や国際的ルールの構築、研究開発力や人材力の抜本的強化なども含めて、「将来に向けてサイバーセキュリティ対策の強化

を図る上で、現時点で最も望ましいと考えられる姿」を描くこととした。

第５に、本提言は、多くの関係者に対して、「意識の変革」を求めるものでもある。行政も民間セクターも、サイバーセキュリティ対策を「コスト」として捉えるのではなく、「投資」と考え、積極的な対応を行うべきである。

今や、サイバー攻撃対策を強化した製品・サービスが国内外市場に於いて優位性を確保できる時代である。現政権が注力しているインフラシステム輸出についても、高度なサイバーセキュリティは激しい国際競争に勝ち抜く力となる。

大企業から中小企業・小規模事業者に至るまで、大規模なサイバー攻撃発生時にも事業継続が可能であることは、市場での高い評価に繋がる。

政府・行政サービス分野においても、サイバー攻撃発生時に、機密情報・個人情報の漏洩を防ぎ、行政サービスの継続性を確保できる体制が整っていることが、国民の皆様の安心確保とともに、日本への投資促進など立地競争力の強化に繋がる。

また、「サイバーセキュリティの産業化」を促進することも、我が国の持続的成長に資するものである。

2015 年 9 月 4 日に閣議決定された『サイバーセキュリティ戦略』の期間は「策定後 3 年」とされており、今年 9 月に期限を迎える。

内閣に対しては、次期『サイバーセキュリティ戦略』の策定作業に際して我が党の提言を踏まえること、来年度以降の予算編成過程に於いてサイバーセキュリティ対策強化に必要な予算・定数の確保に配意すること、特にセキュリティ人材力を強化するための取組を迅速に進めること、さらには技術革新に伴う新たな課題に対応できる法制度整備を積極的に推進することを、切に求める。

結びに、長時間に及ぶ議論に熱心に参加して下さった党所属国会議員の皆様、ヒアリングに協力して下さった有識者の先生方や内閣サイバーセキュリティセンター（NISC）をはじめとする関係府省庁の皆様、会議の準備や運営に尽力して下さった党職員の皆様に対して、深く感謝を申し上げる。

2018 年 4 月

自由民主党サイバーセキュリティ対策本部長
高市　早苗

自由民主党サイバーセキュリティ対策本部役員一同

サイバーセキュリティ対策本部　役員

平成２９年１２月１１日現在

顧　　問	甘利　　明	遠藤　利明	二階　俊博	川崎　二郎
	新藤　義孝	中谷　　元	山口　俊一	丸川　珠代
本　部　長	高市　早苗			
本部長代理	平井　卓也			
副 本 部 長	石田　真敏	伊藤信太郎	岩屋　　毅	江渡　聡徳
	坂本　哲志	左藤　　章	平　　将明	中山　泰秀
	原田　義昭	平沢　勝栄	福井　　照	松本　剛明
	宮下　一郎	有村　治子	佐藤　信秋	森　まさこ
	山谷えり子			
事 務 総 長	柴山　昌彦			
事 務 局 長	木原　誠二			
幹　事　長	橋本　　岳	冨岡　　勉		
幹　　事	赤池　誠章	黄川田仁志	小林　鷹之	白須賀貴樹
	藤井比早之	船橋　利実	牧島かれん	三谷　英弘
	古川　　康	和田　義明	青山　繁晴	そのだ修光
	自見はなこ	吉川ゆうみ		

Ⅱ　分野別分析（現況と課題と対策）

１．航空分野

１．リスクの概要

航空分野の重要システムは、運航システム、予約・搭乗システム、整備システム及び貨物システムの４システムを対象としており、サイバー攻撃が要因となって、航空機の運航遅延、欠航といったサービス障害が発生する可能性が考えられる。

このうち、運航システム、整備システム、貨物システムはインターネットから切り離された環境で運用しており、外部からのサイバー攻撃は受けないが、内部犯行によるサイバー攻撃が行われる可能性は否定できない。

また、予約・搭乗システムがサイバー攻撃を受ければ、顧客情報の流出、発券業務の停止、提携会社を含む運航の遅延といった事態が発生することが考えられる。

特に、「相互乗り入れ」により被害が広域化するリスクがある。また、様々な用途への活用が進む「ドローン」へのサイバー攻撃によるリスクも想定される。

今後は、様々な機器へのサイバー攻撃の脅威が増大していることも考慮した対策を検討する必要があると考えられる。

２．国内外で発生した主なインシデント事例

①サイバー攻撃によるインフラ障害

航空会社への運行システムへの不正侵入やマルウェア感染により、インフラの運行障害や事故が発生。（人的脆弱性、システム脆弱性を攻撃）

2008 年 8 月
スペインの格安航空会社で中央システムが USB メモリを介してウイルスに感染。他の要因ともあわせて、航空機が離陸に失敗。乗員乗客 154 名が死亡。（報道）

2015 年 6 月
LOT ポーランド航空地上システムへの不正アクセスにより、出発便の飛行計画に障害。20 便が欠航、数便に遅れが発生。（報道）

2017 年 10 月
ウクライナのオデッサ空港のシステムがランサムウェアに感染。搭乗手続に影響が発生。（報

道）

②サイバー攻撃による個人情報、機密情報の漏えい

パスワードリスト型攻撃によるハッキング等のサイバー攻撃により Web サイトへの不正ログインや個人情報流出、システムへの不正侵入による機密情報流出が発生。（人的脆弱性、システム脆弱性を攻撃）

これまで、航空会社が運営する通販サイト、マイレージサイト、顧客情報システムが不正アクセスを受け、商品情報の改ざん、マイルの不正交換、顧客情報の流出等の事例が発生している。

2014 年 2 月、3 月
JAL や ANA のマイレージサイトで不正ログイン。住所等が閲覧可能で、マイルも搾取。（報道）

2014 年 9 月
JAL「VIPS」への不正アクセスにより、4,131 名の顧客情報が漏えい。（報道）

2016 年 5 月
豪州パース空港へのハッキングが発生。空港のコンピュータシステムのアクセス権を持つ第三者の認証情報を使いシステムに侵入。大量の機密情報が漏えい。（報道）

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

① 国土交通省は、サイバーセキュリティ戦略本部が決定した「重要インフラの情報セキュリティ対策に係る第４次行動計画（平成 29 年 4 月 18 日サイバーセキュリティ戦略本部決定）」に基づく「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」により、「航空分野における情報セキュリティ確保に係る安全ガイドライン」を策定し、累次の改訂を実施（2016 年 4 月第４版発行）。また、一般財団法人運輸総合研究所は、「航空の安全・安定輸送に資するサイバーセキュリティ対策の手引き」を策定。国土交通省のガイドラインにおける詳細な部分を解説。航空事業者に配布。

② 国土交通省、航空運送事業者及び官民の情報共有組織（航空 CEPTOAR）は、毎年、NISC が主催する重要インフラ分野横断的演習に参加し、所管省庁である国土交通省と協力し、官民間や関係機関等との情報共有や連携による対応力の向上を図っている。

③ 航空運送事業者は、NISC が実施している 2020 年東京オリンピック・パラリンピック競技大会のリスク評価に参加している（国土交通省は協力）。

（２）情報の共有

① 国土交通省、航空運送事業者及び航空 CEPTOAR は、「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づき、業界内の情報取扱いルールに則り、NISC と連携した情報共有体制の枠組みに参加している。

② 航空運送事業者は、SIG を構築して、独立行政法人情報処理推進機構（IPA）が行うサイバー情報共有イニシアチブ（J-CSIP）に参加し、情報共有体制を構築している。

③ 国土交通省は、航空・鉄道・物流分野の各事業者が情報の共有・分析や対策を連携して行う体制である「交通 ISAC」（仮称）の創設に向けた検討を支援している。これにより、航空分野における有事の情報共有と平時の知見共有を通じた集団防御を図ることが可能となる。（2018 年度から仮運用が開始される予定）

（３）人材の育成

① IPA に設置された産業サイバーセキュリティセンターが実施する研修に、航空運送事業者からの研修生を派遣し、人材育成に努めている。

② 航空運送事業者は、NISC が実施する分野横断的演習に参加し、人材の育成に努めている。

③ 一般財団法人運輸総合研究所において「航空のサイバー攻撃に対する人材育成に関する調査研究」を実施し、人材育成カリキュラムを策定した。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① 安全基準等の改訂
国土交通省は、NISC による「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改訂（2018 年 4 月）を受け、「航空分野における情報セキュリティ確保に係る安全ガイドライン」を改訂し、サイバーセキュリティ対策の一層の強化を図ることとしている。今後は、IoT 機器も含めたセキュリティ対策の強化を行う必要がある。

② 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価
航空運送事業者は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施するリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図る必要がある。

③ 空港ビル事業者等の重要インフラ化

「重要インフラ 13 分野」の「航空」とは、航空運送事業者を指し、空港ビル事業者等が含まれていない。空港ビル事業者等は 2018 年度の重要インフラ化を目指し、引き続き調整を行う。

（２）情報の共有

① 各種情報共有の促進と「交通 ISAC」の創設

NISC からのニュースレターの共有、サイバー情報共有イニシアチブ（J-CSIP）による情報共有を引き続き実施するとともに、「交通 ISAC」（仮称）の創設に向けた検討を加速し、情報共有体制の充実を図る。

（３）人材の育成

① 各種人材育成関連プログラムの推進

産業サイバーセキュリティセンターの研修の活用、一般財団法人運輸総合研究所の策定した「航空のサイバー攻撃に対する人材育成に関する調査研究」の活用、NISC が実施する分野横断的演習への参加等により、人材の育成を図る。また、「交通 ISAC」（仮称）においても、人材育成方策を検討する。

（４）その他

① 「ドローン」への対応

様々な用途への活用が進む「ドローン」へのサイバー攻撃に対するリスクの最小化対策が必要。

２．鉄道分野

１．リスクの概要

鉄道分野の重要システムは、運行管理システム、電力管理システム及び座席予約システムの３システムを対象としている。

運行管理システム及び電力管理システムは制御系システムに該当し、インターネットから切り離されたクローズド環境で運用されており、外部からのサイバー攻撃は受けないが、保守業者、組織に恨みを持つ者又は脅迫された者による内部犯行等によるサイバー攻撃が行われる可能性は否定できない。

また、座席予約システムは IT 系システムに該当し、外部からの不正アクセスを受ける可能性がある。

２．国内外で発生した主なインシデント事例

①サイバー攻撃によるインフラ障害

鉄道会社の運行システムへの不正侵入やマルウェア感染により、インフラの運行障害や事故が発生。（人的脆弱性、システム脆弱性を攻撃）

2003 年 8 月
米国東部の鉄道会社 CSX 社の信号管理システムがコンピュータウイルスに感染。ワシントン DC 周辺の 3 路線で通勤および貨物列車が停止。（報道）

2008 年 1 月
ポーランドで 14 歳の少年が路面電車システムに侵入し、ポイント切替機を不正に操作。列車 4 車両が脱線。（報道）

2016 年 12 月
サンフランシスコ市交通局の局内システムへのランサムウェア攻撃により、地下鉄の料金システムがダウン。（報道）

2017 年 10 月
ウクライナのキエフ地下鉄のシステムがランサムウェアに感染し、決済システムへの影響が発生。（報道）

②サイバー攻撃による個人情報、機密情報の漏えい

パスワードリスト型攻撃によるハッキング等のサイバー攻撃により Web サイトへの不正ログインや個人情報流出、システムへの不正侵入による機密情報流出が発生。（人的脆弱性、システム脆弱性を攻撃）

Winny を利用した際のウイルス感染やハッキング等のサイバー攻撃により Web サイトへの不正ログインや個人情報流出等の事例が発生している。

なお、昨年、社内システムに接続されていない web 閲覧用 PC が Wannacry の攻撃を受け、感染した事例があった（事業への影響なし）。

2014 年 8 月、9 月
JR 東日本の「Suica ポイントクラブ」「My JR-EAST」で 2 万件以上の不正ログイン。（報道）

2015 年 8 月
JR 東日本「My JR-EAST」69 名のアカウントで不正ログイン。警察が押収したサーバから 53 名分の会員情報を発見。

③鉄道会社を名乗るメール、サイト改ざん

鉄道会社からのお知らせ等を語ったフィッシングメールは確認されていないが、Web サイトの改ざんの事例が発生している。

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

① 国土交通省は、サイバーセキュリティ戦略本部が決定した「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」により、「鉄道分野における情報セキュリティ確保に係る安全ガイドライン」を策定し（累次の改訂を実施。2016 年４月第３版発行）、鉄道事業者の情報セキュリティ対策を促進している。また、一般財団法人運輸総合研究所において「鉄道の安全・安定輸送に資するサイバーセキュリティ対策の手引き」を策定。国土交通省策定のガイドラインにおける詳細な部分を解説し、鉄道事業者に配布している。

② 国土交通省、鉄道事業者及び官民の情報共有組織（鉄道 CEPTOAR）は、毎年、NISC が主催する重要インフラ分野横断的演習に参加し、所管省庁である国土交通省と協力し、官民間や関係機関等との情報共有や連携による対応力の向上を図っている。

③ 鉄道事業者は、NISC が実施する 2020 年東京オリンピック・パラリンピック競技大会のリスク評価に参加している（国土交通省は協力）。

④ 国土交通省において鉄道事業者に係る運転・電力指令所、鉄道変電所等の重要施設について標準的な保安措置を定め、各鉄道事業者はこれを踏まえて具体的な保安計画を策定・実施している。

（２）情報の共有

① 国土交通省は、航空・鉄道・物流分野の各事業者が情報の共有・分析や対策を連携して行う体制である「交通 ISAC」（仮称）の創設に向けた検討を支援している。これにより、鉄道分野における有事の情報共有と平時の知見共有を通じた集団防御を図ることが可能となる。（2018 年度から仮運用が開始される予定）

② 鉄道事業者は、SIG を構築して、IPA が行うサイバー情報共有イニシアチブ（J-CSIP）に参加し、情報共有体制を構築している。

（３）人材の育成

① IPA に設置された産業サイバーセキュリティセンターが実施する研修に、鉄道事業者からの研修生を派遣し、人材育成に努めている。

② 国立研究開発法人情報通信研究機構（NICT）が行う演習(CYDER)に参加し、サイバー攻撃に対する対応能力の向上を図っている。

③ 一般財団法人運輸総合研究所において「鉄道のサイバー攻撃に対する人材育成に関する調査研究」を実施し、人材育成カリキュラムを策定した。

④ 鉄道事業者は、NISC が実施する分野横断的演習に参加し、人材の育成に努めている。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① 安全基準等の改訂
NISC が改訂予定（2018 年４月）である「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」に対応し、「鉄道における情報セキュリティ確保に係る安全ガイドライン」を改訂し、サイバーセキュリティ対策の一層の強化を図る必要がある。

② 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価
鉄道事業者は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施するリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図る必要があ

る。

（２）情報の共有

① 各種情報共有の促進と「交通 ISAC」の創設
NISC からのニュースレターの共有、サイバー情報共有イニシアチブ（J-CSIP）による情報共有を引き続き実施するとともに、「交通 ISAC」（仮称）の創設に向けた検討を加速し、検知したサイバー攻撃情報や対策情報の共有による同種被害の最小化、予兆情報共有に基づいた早期警戒による実被害の抑止を図る必要がある。

（３）人材の育成

① 各種人材育成関連プログラムの推進
産業サイバーセキュリティセンターの研修の活用、一般財団法人運輸総合研究所において「鉄道のサイバー攻撃に対する人材育成に関する調査研究」の活用、NISC が実施する分野横断的演習への参加等により、人材育成を図る。また、「交通 ISAC」（仮称）においても、人材育成方策を検討すべきである。

（４）その他

① 鉄道の相互乗り入れによる被害広域化の防止策の検討
鉄道の相互乗り入れによる被害広域化について、防止策を検討することが必要である。

３．自動運転分野

１．リスクの概要

自動運転は、これまで人間が行っていた認知、判断、操作を機械が代替するものであり、国内外の自動車メーカーから市場化時期に関する方針が発表され、実証実験の動きが加速している。公道における市場化は、段階的にレベル（自動化の割合）が上がり、高速道路では 2020 年にレベル３（加速・操舵・制動を全てシステムが行い、システムが要請したときのみドライバーが対応する状態）を実現する予定である。このような自動運転システムを搭載した自動車においては、安全性を確保する観点から、種々の通信からの情報を得て冗長性を確保することとしている。

我が国としては、世界に先駆けた自動運転の社会実装により、日本の強みを活かして社会的な課題を解決していくことが望まれるが、技術開発はもとより、実証を通じた制度整備、社会実装を担うサービス等の提供者の発掘、国民の自動走行に対する理解度向上（社会受容度向上）について同時並行的に進めることが不可欠である。この際、種々の外部との通信を介して車内ネットワークがつながることになり、外部からの不正なアクセス、送受されるデータの不正な書き換えなどにより、自動運転車の正しい運行が阻害されるおそれがある。

２．国内外で発生した主なインシデント事例

公道を走行する自動車がサイバー攻撃を受けて、運転不能になるなどの事例は、現時点まで確認されていない。しかしながら、自動車ベンダやセキュリティ研究者、会議等にて、セキュリティ自動車の制御装置、車載の通信・ソフトウェアへのハッキングリスクや脆弱性の指摘が多数存在する。脆弱性の指摘、展示会等でのハッキングの実例は以下の通り。

2013 年 8 月
米 DEFCON で「プリウス」と「フォード」の有線ハッキング実験を公開。

2015 年 7 月
米 FCAUS 社（旧クライスラー社）が、BlackHat においてＣＡＮ（Car Area Network）を介して主要搭載部をハッキングするとの実演があったことをきっかけに、「Uconnect」の脆弱性、Jeep の遠隔操作の懸念から約 140 万台をリコール。

2015 年 7 月
米 GM 社の「OnStar」に脆弱性。無線通信偽装により第三者が遠隔操作可能。（報道）

2015 年 7 月
米 Jaguar Land Rover のソフトウェアに欠陥。キーレス車の鍵が意図せずに開く。（報道）

2015 年 12 月
日本車のハッキング実験公開。診断用ポートに機器を接続、スマホで操作。

2016 年 5 月
米テスラモーターズが公道でのレベル２実証実験中に、トレーラーとの衝突事故を起こし、運転手が死亡した。この事故などから自動運転の安全性、CAN 通信の脆弱性に指摘あり。（脆弱性の指摘については報道）

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

自動運転車両がハッキングされた場合、重大な事故を招く可能性があり、重要インフラ分野と同等の高度なセキュリティ対策が求められる。

① レベル３以上の自動運転車は、現時点で商品化されておらず、また先端的な技術を含んでいること及び各自動車会社で電子制御システムが異なり、かつ進化も早いことから、協調領域と競争領域を設定し、取組を進めている。

② 協調領域として、以下の取組を業界、国が推進している。
ア．中小サプライヤーや研究機関が共同で脆弱性分析を進めるための評価環境（テストベッド）の整備。
イ．安全設計のための多層防御設計、開発プロセス標準化
ウ．運用面における情報共有体制の構築
エ．不足するセキュリティ人材の育成促進

③ 自動車会社各社は、競争領域として以下の取組を推進している。
ア．各社の電子制御システムに基づく脅威分析を進めるための評価環境（テストベッド）整備
イ．標準化された設計・開発プロセスを踏まえた独自の安全設計

（２）情報の共有

① 市場導入後の運用面において、未知のインシデント・脅威・脆弱性が発生し得るため、その情報を直ちに共有し、業界全体として、被害拡散防止、対策レベル向上を図ることが必要。経済産業省のサイバーセキュリティ経営ガイドラインも踏まえ、自動運転に加えて､広く自動車全般のサイバーセキュリティ関連のインシデント情報を共有するため、日本自動車工業会において、J-Auto WG を 2017 年 1 月に設置し、2017 年 4 月に活動開始。

（３）人材の育成

自動走行という新しい分野であり、最新かつ顕在化していない情報の収集能力、保護対象となるシステムの理解、現実的な対策方法の立案等、非常に高度な専門性が求められるため、産学官が連携した人材育成講座や人材育成プログラムを実施している。

① より実践的なサイバーセキュリティ人材の育成システムの構築が課題になっており、個社の評価環境を使用することが難しいことから、経済産業省が整備しているテストベッドを活用していく方針である。

② 海外人材の発掘、登用を含めた積極的な取組が必要。その際、人材を確保するために雇用体系の検討のみならず、業界が協調して、製造現場におけるサイバーセキュリティ人材の必要性や職の魅力を発信することが不可欠である。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① 「企業や国を超えた協力体制」の整備

自動車・自動運転分野では、運転者の利便性向上や自動車制御技術の向上を目的とした自動車のインテリジェンス化が進み、IoT センサー、クラウド、AI 等を活用したコネクテッドカーや自動運転が実用化される期待が高まっている。2020 年代前半には、日独米国の自動車メーカーが自動運転の実用化を目指しているが、普及に向けてはステークホルダー同士が協調して安全確保のルールを作る取組が重要であり、「企業や国を超えた協力体制」が必要となる。

② サプライチェーン全体での被害発生リスクの抑止

自動車の ICT 技術の多機能化やカーシェアリングなどの利用形態の変化に伴い、サイバー攻撃の侵入口が多様化し、攻撃の手口も高度化していくリスクが存在している。自動車のサイバー攻撃による影響は、盗難による損害や個人情報漏えいだけでなく、遠隔操作や制御装置への不正アクセスによる人命に関わる事故が懸念され、広いエリアに急速に拡大する恐れもある。

そのため、「企画、構築、運用、破棄」までの自動車システムのライフサイクルのフェーズを意識し、サプライチェーン全体で各フェーズでの被害発生リスクを抑止する取組（脆弱性の低減や防御手段の実装）が必要である。

③ 「セキュリティバイデザイン」の取組

外部ネットワークと接続する車載機器やソフトウェア制御装置の脆弱性を製造段階から検知・排除する「セキュリティバイデザイン」の取組が必要である。

④ 新たなリスクへの対応
高度化していく攻撃リスクへの対策が必要であり、また、自動車整備時やカーシェアリング時などのリスク管理も行う必要がある。

⑤ フェールセーフ機能の装備
センサーや AI を活用した自動運転機能においては、「車載機能のセキュリティ脆弱性の排除」だけでなく、「ネットワークで接続する周辺システムへのサイバー攻撃により、制御装置が異常動作した場合の対処・対策を確実に実行するセーフティ機能を装備すること」が非常に重要である。

（２）情報の共有

① 利用者を含めた情報共有の在り方の検討
「自動運転」「コネクテッドカー」に関わる周辺システムやインフラ事業者を含めた全体的なセキュリティ対策の情報共有や専門機関との対策検討に加え、利用者への早期通知の仕組みも検討すべきである。

② 情報共有の範囲の拡大の検討
「交通 ISAC」を検討する際、「陸上交通」であれば、バス、タクシー、トラック、自動運転、電子交通標識等、幅広い主体で組織することを検討すべきである。

（３）人材の育成

① 各種人材育成関連プログラムの推進
自動車分野に関連するセキュリティ人材のレベルアップに向け、「制御システムのエンジニアへのサイバーセキュリティ教育」だけでなく、「IT エンジニアへの制御系装置のセキュリティ対策教育」や「相互交流」が必要である。

② プログラムの高度化・複雑化に対応できる人材の育成
自動運転の更なる高度化に伴い、車向けのソフトウェアのソースコードが数億行レベルに増えると予想されており、ソフトウェア開発、セキュリティ対策・評価技法も非常に高度化することから、「ハッカソンの参加」も含め中長期的に高度人材を発掘・育成する仕組みが必要である。

（４）その他

① サイバー攻撃による被害への対応
ドライバーが関与しないハッキングによる交通事故の賠償責任や被害者への補償など、法的な検討を急ぐことが必要である。

４．物流分野

１．リスクの概要

物流分野の重要システムは、集配管理システム、貨物追跡システム及び倉庫管理システムの３システムを対象としている。これらのシステムをインターネットに接続して使用する事業者もあることから、サイバー攻撃が原因となってシステムが停止する場合も考えられる。この場合、輸送そのものは継続され、ＦＡＸ等手作業による代替は可能であるが、長期におよぶと配送業務の遅れや倉庫への物資の搬入出が遅れる可能性があることから、サイバー攻撃が行われることは否定できない。

今後は IoT を活用したサプライチェーン全体の最適化促進等が行われることも考慮した対策を検討していく必要がある。

２．国内外で発生した主なインシデント事例

① サイバー攻撃による個人情報、機密情報の漏えい

パスワードリスト型攻撃やハッキング等のサイバー攻撃により Web サイトへの不正ログインや個人情報流出、システムへの不正侵入による機密情報流出が発生。（人的脆弱性、システム脆弱性を攻撃）

2014 年 9 月
ヤマト運輸「クロネコメンバーズ」で 1 万件以上、 佐川急便で運営する会員制 Web サービスで 3 万 4 千件以上の不正ログインが発生。

② 物流業社を騙るばら撒き型メールによるウイルス感染

物流業社からの「お届けのお知らせ等」の内容を騙ったウイルス付メールにより、バンキングマルウェアの感染が発生。（人的脆弱性を攻撃）

2016 年 6 月～
ヤマト運輸や佐川急便を騙った「宅急便のお知らせ」「商品お届けのご案内」等のメールによるバンキングマルウェアの感染が多数確認される。

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

① 国土交通省は、サイバーセキュリティ戦略本部が決定した「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」により、「物流分野における情報セキュリティ確保に係る安全ガイドライン」を策定し、累次の改訂（2016 年４月第３版発行）を実施しつつ、物流事業者の情報セキュリティ対策を促進している。

② 国土交通省、物流事業者及び官民の情報共有組織（物流 CEPTOAR）は、毎年、NISC が主催する重要インフラ分野横断的演習に参加し、所管省庁である国土交通省と協力し、官民間や関係機関等との情報共有や連携による対応力の向上を図っている。

③ 物流事業者は、NISC が実施する 2020 年東京オリンピック・パラリンピック競技大会のリスク評価に参加している（国土交通省は協力）。

（２）情報の共有

① 国土交通省は、航空・鉄道・物流分野の各事業者が情報の共有・分析や対策を連携して行う体制である「交通 ISAC」（仮称）の創設に向けた検討を支援している。これにより、物流分野における有事の情報共有と平時の知見共有を通じた集団防御を図ることが可能となる。（2018 年度から仮運用が開始される予定）

② 物流事業者は、SIG を構築して、IPA が行うサイバー情報共有イニシアチブ（J-CSIP）に参加し、情報共有体制を構築している。

（３）人材の育成

① 物流事業者は、NISC が実施する分野横断的演習に参加し、人材の育成に努めている。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① 安全基準等の改訂

国土交通省は、NISC による「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改訂（2018 年４月）を受け、「物流分野における情報セキュリティ確保に係る安全ガイドライン」を改訂し、サイバーセキュリティ対策の一層の強化を図

ることとしている。今後は、IoT 機器を使用する場合も考慮したセキュリティ対策についての検討を行うべきである。

② 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価
物流事業者は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施する 2020 年東京オリンピック・パラリンピック競技大会のリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図ることが必要である。

（２）情報の共有

① 各種情報共有の促進と「交通 ISAC」の創設
NISC からのニュースレターの共有、J-CSIP による情報共有を引き続き実施するとともに、「交通 ISAC」（仮称）の創設に向けた検討を加速させ、情報共有体制の充実を図るべきである。

（３）人材の育成

① 各種人材育成関連プログラムの推進
NISC が実施する分野横断的演習への参加等により、人材の育成を図るべきである。また、「交通 ISAC」（仮称）においても、人材育成方策を検討することが必要である。

５．医療分野

１．リスクの概要

サイバーセキュリティ基本法において、重要インフラ事業者とは、「国民生活及び社会経済の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者」と定義されている。医療分野については、診療や治療の行為を支えるシステムの不具合が国民生活等影響を与えることを踏まえ、重要インフラとしてサイバーセキュリティ対策に取り組んでいるところである。

重要システムの例としては「診療等の管理システム等（電子カルテシステム、遠隔画像診断システム、医用電気機器等）」があげられている。

リスクシナリオとしては、外部からの不正アクセス・マルウェア感染により、職員端末及び医療システムのハードウェアが暗号化され、医療業務が数日にわたって停滞することや、抜き取った患者情報を外部サーバに送信することが考えられる。

２．国内外で発生した主なインシデント事例

①サイバー攻撃によるインフラ障害

病院や医療機関への院内システムがマルウェア（ランサムウェア等）に感染。データのロック等により、急患対応や手術ができない影響が発生。（システム脆弱性を攻撃）

2016 年 2 月、3 月
米国・カナダの医療機関で、ランサムウェアによる暗号化被害が相次ぐ。院内ネットワークに侵入したマルウェアがローカルサーバーを介して院内 PC に感染し、PC を使った業務が一切できなくなるなどの影響が発生。（米 Hollywood Presbyterian Medical Center、米 MedStar Health、カナダ Ottawa Hospital、米 Methodist Hospital、カナダ Norfolk General Hospital 他）（報道）

2017 年 1 月
米テキサス州の病院でランサムウェア感染。27 万 9,663 人の患者情報に被害。

2017 年 5 月
世界の少なくとも約 150 か国において、政府機関や病院、銀行、大手企業等のコンピュータが、マイクロソフト製品の脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。
イギリスでは、国民保健サービス（ＮＨＳ）を提供する 248 団体のうち 48 団体でコンピュータが使用不能となり、同団体が運営する病院で診療や手術を中止する事案が発生した。
日本では、日立総合病院（茨城県）において、院内のメールシステムの一部に障害があった。

診療系システムには異常なく、患者への影響は出ておらず、個人情報の流出は確認されていない。

②サイバー攻撃による改ざん・機密情報漏えい等

　インターネットからの病院への不正アクセスやウイルス等の感染により、Web サイトの改ざんや機密情報の漏洩が発生。医療情報や口座情報などの個人情報が窃取され取引される被害も出ている。（システム脆弱性を攻撃）

2016 年 6 月
米国で医療保険情報 1,000 万件が漏えい。ダークウェブで販売。（報道）

2017 年 5 月
リトアニアの美容外科クリニックが 25,000 以上の患者情報を公開される。（報道）

2017 年 6 月
病院や介護施設等を運営する渓仁会グループのホームページへ不正アクセス。
24 の関連サイトが改ざんされ、訪問者が第三者サイトへ誘導される状態に。

2017 年 9 月
ロート製薬の「ココロートパーク」で不正アクセス発生。登録者 32 名分の ID、パスワードが閲覧された可能性あり。

2017 年 12 月
新潟大学医歯学総合病院において、パソコンがランサムウェアに感染し、ファイルが暗号化されて使用できない状態となったほか、ウェブサイトが不正アクセスを受け、改ざんされた。個人情報の流出は確認されていない。

③重要インフラへのハッキング、機器の脆弱性等

　医療機関への攻撃を意図したハッキング事案やマルウェアの感染が発生。医療機器自体の脆弱性（パスワード等）の報告も多数あり。（人の脆弱性、システムの脆弱性を攻撃）

2012 年 6 月～
医療機器等で使われている遠隔操作等のソフトウェア（Symantec pcAnywhere、Oracle）に脆弱性が発覚、米食品医薬品局（FDA）が製品回収情報を公表。（報道）

2013 年 6 月
米 ICS-CERT が医療機器のパスワード脆弱性について警告。40 ベンダ約 300 の医療機器（麻酔器、人工呼吸器、薬物注入ポンプ等）に関係し、機器によっては遠隔操作が可能と発表。

2017 年 1 月
Abbott 社の医療機器が中間者攻撃に対して脆弱であると公表。（報道）

④その他

2017 年 3 月
岡山大学病院において、医療用端末２台がウイルス感染し、外部と不正な通信を行っていたことが判明した。電子カルテなどの医療情報システム、基幹システムへの不正アクセスは確認されておらず、個人情報の流出も確認されていない。

３．サイバーセキュリティ対策の現況

政府では、サイバー攻撃の動向やサイバーセキュリティ戦略を踏まえ、基準やガイドラインの整備、技術的対策や態勢の強化を図っている。

（１）多層的な防御と対処態勢の整備

① 厚生労働省は、サイバーセキュリティ戦略本部が決定した「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」により、「医療情報システムの安全管理に関するガイドライン」を策定し、累次の改訂（第 5 版：平成 29 年 5 月改定）を実施しつつ、医療機関等の情報セキュリティ対策を促進している。また、IPA が医療情報システムのセキュリティリスク分析ガイドを策定し、医療関係団体に周知している。

② 厚生労働省、医療機関等及び官民の情報共有組織（医療 CEPTOAR）は、毎年、NISC が主催する重要インフラ分野横断的演習に参加し、所管省庁である厚生労働省と協力し、官民間や関係機関等との情報共有や連携による対応力の向上を図っている。

③ 厚生労働省において、本年度、医療機関等のセキュリティ対策の現状や海外の取組等に関する調査事業を実施中である。

（２）情報の共有

① 医療 CEPTOAR 事務局が日本医師会に移管（平成 30 年 3 月）され、日本歯科医師会、日本薬剤師会、日本看護協会、四病院団体協議会に NISC からの情報等を共有するとともに、医療 CEPTOAR 構成員のさらなる拡充について事務局で検討中である。これに伴い、重要インフラ事業者間で相互に情報共有を行うセプターカウンシルについて、医療分野が従来オブザーバーであったが、事務局の日本医師会移管を踏まえ、平成 30 年 4 月に正会員として参加予定。
また、分析機能として、保健医療福祉情報システム工業会（JAHIS）が医療 CEPTOAR

にオブザーバー参加している。

（３）人材の育成

① 医療機関等は、NISC が実施する分野横断的演習に参加し、人材の育成に努めている。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① 医療分野全体としてのセキュリティ対策の推進
医師会以外の医療従事者や私立病院等セキュリティ対策に資金的なリソースを振り分けることが困難な事情がある組織等が存在する点を踏まえ、医療分野全体としてセキュリティ対策を推進することが必要である。

② 保健医療情報のセキュリティ対策の強化
「未来投資戦略 2017」に基づき、患者の保健医療情報を医療関係者が共有し、患者に最適な診療を提供するための全国的なネットワークを 2020 年度から本格稼働させることを目指す中で、データ共有・利活用の利便性向上とセキュリティのバランスをとりながら、ネットワークや医療機関のセキュリティ対策強化について厚生労働省において検討すべきである。その際には、コスト負担のあり方についても留意する。

③ 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価
医療機関等は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施する 2020 年東京オリンピック・パラリンピック競技大会のサイバーセキュリティ対策の強化の一環として、リスク評価に参加することが求められる。

④ 業務やデータの機密性に応じたインフラの設計および運用管理
外部からの侵入からだけではなく、USB などからマルウェアが複数の業務システムに病院院内のネットワークを通じて広く感染するケースも多いため、「パブリックエリア（外来者が利用するエリア）」、「オフィスエリア（一般業務のエリア）」、「セキュリティエリア（機密情報を扱うエリア）」等でネットワークやシステムアクセス権限を区分し、業務やデータの機密性に応じたインフラの設計および運用管理を実施することが必要である。

⑤ 使用期間が長い医療機器におけるセキュリティ対策
医療機器が 10 年以上使用される事もあり、OS 等の古いバージョンのソフトウェアが利用されているケースも数多く残存している。OS のアップデートや不具合対策のモジュール適用も、本来機能を損なう別の不具合を内包している可能性があり、十分な検証を行ってからでないと適用が難しく、一般の情報（IT）系システムに比べて対策が難しい状況である。これらシステムの脆弱性を十分に把握した上で多層的な防御を実施していくこ

とが必要である。

⑥ ペースメーカー等のセキュリティ対策
ペースメーカーや植込み型除細動器への遠隔操作のリスクを排除すべきである。

⑦ 関係機関間の連携・協調
医療機器の安全性を担う医療機器製造業者、組織としての対策を行う医療機関、脆弱性や攻撃の分析を行うセキュリティ機関、規制やガイドラインを提供する国や自治体等が連携・協調して対応することが必要である。

（２）情報の共有

① 情報共有の更なる促進と関係者の範囲の拡大
医療分野におけるサイバーセキュリティに関する情報の共有・分析の取組が民間の医療関係団体中心に進み始めているが、医療機関の意識や取組状況の差もある中で、医療CEPTOARがセプターカウンシルに正式参加することで、重要インフラの他分野の取組を把握しつつ、更なるセキュリティ対策の強化と安全性の向上のための協働活動について検討を進め、結論を得る。その際には、CEPTOARの構成員の拡充についても、民間の医療関係団体に検討を促すことが重要である。

② 「医療ＩＳＡＣ」の創設
既に「地域包括ケア」の時代に入っており、「遠隔医療」、「オンライン診療」やスマートフォン等から送信されるバイタルデータを活用した「ヘルスケア」の取組も進行している。デバイス数が急増している現状から、「医療ＩＳＡＣ」の創設を急ぐべきである。なお、将来的に介護・健康分野への拡大も検討すべきである。

（３）人材の育成

① 各レイヤの人材に対するセキュリティ教育の底上げ
CISO(最高情報セキュリティ責任者)を始め、実際にセキュリティ対策を実施する人材が不足しており、「各レイヤの人材に対するセキュリティ教育の底上げ」を図ることが必要である。

② IT・OT双方の人材育成
制御系機器を扱っているため、「IT系／OT系双方のスキルを持つ人材」を育てるとともに、サイバー攻撃に対する検知、解析、対処について、サプライチェーン(機器製造者)や分野を横断して連携して対応できる実践的訓練環境の整備が必要である。

（４）その他

① 「マイナンバーカード」、「HPKI」の活用

政府は、紛失時には365日24時間体制のコールセンターへの連絡で機能停止も可能な「マイナンバーカード」の公的個人認証機能を活用することで、健康保険証などのセキュリティレベルをより向上させる方策を検討すべきである。また、医療事業者が、本人確認することができることで、電子的に書類を作成する際の利便性を大幅に向上させるなどの利点を有する保険医療福祉分野電子証明書（HPKI）を一層活用するべきである。

② 社会保険診療報酬支払基金の防護体制の強化

社会保険診療報酬支払基金は、重要インフラ事業者のように直接「事業を行う者」ではないものの国民生活又は経済活動に多大な影響を及ぼすものであり、サイバー攻撃からの適切なセキュリティ対策が不可欠である。支払基金については、ＮＩＳＣ、厚生労働省など関係省庁が緊密に連携して、迅速なサイバー攻撃からの防護の技術的な体制（緊急時の技術的支援を含む。）を一刻も早く強化すべきである

６．電力分野

１．リスクの概要

適時適切な電力の安定供給のために、発電所や中央給電指令所、制御所等において、制御系システムにより、発変電設備等の監視・制御等を行っている。各種制御系システムは、多数の情報通信機器やソフトウェアから構成されているが、インターネットとの直接的な接続点は存在しない。

国内においては、現段階ではサイバー攻撃による停電は発生していないが、電気事業者の HP への不正アクセス等は確認されている。また、国外においては、電力分野の制御系システムへのサイバー攻撃による停電が発生しており、今後、国内でも同じような事象が発生しないとは言い切れない。電力は、様々な分野の基盤となる重要なインフラであるとともに、IoT、AI、ビックデータを活用した経済・産業活動の変革に伴い、ますますその安定供給が求められていくことが想定される。

２．国内外で発生した主なインシデント事例

① サイバー攻撃によるインフラ障害

電力会社へのシステム侵入やマルウェア感染により、データ破壊、制御システムの停止や停電等が発生。（システム脆弱性を攻撃）

2009 年
プエルトリコにおいて、攻撃を受けた会社のスマートメーターを配置した地域内で、電力消費記録設定が改ざんされた。（報道）

2010 年
Stuxnet と呼ばれるマルウェアを利用した、イランの核燃料施設のウラン濃縮用遠心分離機を標的としたサイバー攻撃が発生。これにより、イランの核開発計画は大幅に遅れたと言われている。（報道）

2010 年
ロンドンオリンピック開会式会場の電源システムに対して 40 分で 1000 万件の大量通信が行われた。停電にまでは至らなかった。

2014 年 6 月
米国をはじめとした諸外国において、Dragonfly と呼ばれる集団によるスパイ活動や継続的なアクセスを目的としてエネルギー関連業界の多数の組織への侵入が発生。（報道）

2015 年 3 月
トルコの首都アンカラを含め、全 81 県のうち 45 県に停電が発生。電力会社は送電線に障害が起きたと説明しているが、サイバー攻撃の可能性あり。（報道）

2015 年 12 月
ウクライナの変電所へのサイバー攻撃。マルウェア感染により数万世帯が 3 時間以上停電。

2016 年 1 月
イスラエルの電力公社が大規模なサイバー攻撃を受け、コンピュータ多数が使用不能になる深刻な事態に陥った。（報道）

2016 年 12 月
ウクライナのキエフ郊外にあるピヴニシュナ変電所へのサイバー攻撃により停電発生。変電所はマニュアル操作に切り替え、約 1 時間 15 分後に電力が復旧。

2017 年 6 月
ウクライナの電力会社でマルウェア感染。データ破壊の被害。（報道）

2017 年 7 月
欧州、ロシア、米国などで、ランサムウェア感染が多数報告。ウクライナの被害が最大で、電力会社、チェルノブイリの放射線レベル測定システム等にも影響あり。（報道）

② インフラ事業者へのハッキング等

電力会社や関連事業者への攻撃を意図したハッキング事案やマルウェアの感染が発生。（人的脆弱性、システム脆弱性を攻撃）

2017 年 7 月
米国の原子力発電所やエネルギー施設運営企業らがハッキング被害、FBI が緊急報告。

③ サイバー攻撃による個人情報・機密情報の流出

2016 年 11 月
東北電力の会員制 Web サービス「よりそうｅねっと」に、大量の不正アクセスが行われ、540 名分の顧客の「よりそうｅポイント」が共通ポイントに不正交換された。

④ 電気事業者のサイト改ざん

2017 年 3 月
沖縄電力の Web サイトのコンテンツの改ざんが行われ、本来表示されるべき画面とは異なる情報・画像が表示される状態となった。

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

① 日本電気技術規格委員会（JESC）は、「スマートメーターシステムセキュリティガイドライン」及び「電力制御システムセキュリティガイドライン」を策定。同年、経済産業省は、電気事業法下の技術基準と保安規程に両ガイドラインを組み込み、ハード・ソフト両面のサイバーセキュリティ対策の実効性を担保している。また、両ガイドラインでは、セキュリティ管理組織の設置やマネジメントシステムの構築といった社内のサイバーセキュリティ態勢の構築も求めている。

② 電気事業者等は、JESC が策定したガイドラインに基づき、外部組織の活用などを通じて、防御力の確認やリスク分析を行い、改善を図ることにより、各社ごとのセキュリティ対策の強化に取り組んでいる。また、電力 ISAC を通じて各社の取組を共有し、業界大でサイバーセキュリティ対策レベルの向上に取り組んでいる。

③ 経済産業省は、「電気設備の技術基準の解釈」を策定し、累次の改訂を実施（2016 年 9 月現行の改訂）している。

④ 電力分野の制御系システムはインターネットとの直接的な接続点は存在しない。インターネットと情報系システムとの間、情報系システムと制御系システムの間には、それぞれ、通信の防護措置（接続点の制限、アクセス制御、状態監視、通信方向の限定等）が行われている。また、制御系システム内でも、アクセス制御、マルウェア対策、不正プログラム防止といった対策が行われており、多層的な防御が行われている。

⑤ 経済産業省、電気事業者及び官民の情報共有組織（電力 CEPTOAR）は、毎年、NISC が主催する重要インフラ分野横断的演習に参加し、所管省庁である経済産業省と協力し、官民間や関係機関等との情報共有や連携による対応力の向上を図っている。

⑥ 電気事業者は、2020 年のオリンピック・パラリンピック競技大会を支える重要サービスを提供する事業者等として、その準備・運営への影響の未然防止等のため、NISC が実施している横断的なものを含むリスク評価に参加し（経済産業省は協力）、リスクマネジメントによる各社の対策強化を進めている。

（２）情報の共有

① 「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づき、業界内の情報取扱いルールに則り、事業者、CEPTOAR、経済産業省及び内閣官房と連携した情報共有体制の枠組みに参加している。

② 電気事業者等は、2017 年３月に電力 ISAC を設立し、電気の安定供給の役割を担う事業者間で、サイバーセキュリティに関する情報の収集・分析や各社のベストプラクティスに係る情報共有を実施するとともに、欧米の同様の組織とも連携を深めている。

③ 電気事業者等は、SIG を構築して、IPA が行うサイバー情報共有イニシアチブ（J-CSIP）に参加し、情報共有体制を構築している。

（３）人材の育成

① IPA に設置された産業サイバーセキュリティセンターが実施する研修に、電気事業者等からの研修生を派遣し、人材育成に努めている。また、CISO/CIO などの経営層クラスを対象とした CISO 向けプログラムに参加している。

② 電気事業者等は、NISC が実施する分野横断的演習に参加し、人材の育成に努めている。

③ 技術研究組合制御システムセキュリティセンター（CSSC）において実施している制御システムにおけるセキュリティ上の脅威の認識、対策効果の体感を目的としたサイバー演習に参加している。

④ 電気事業者等は、NICT が実施している大規模演習環境を用いた実践的なサイバー防御演習（CYDER）に参加している。

⑤ 電気事業者等は、一般財団法人電力中央研究所において実施している情報系の模擬システム最新の脅威に対応した演習シナリオを利用した実践的な演習に参加している。

⑥ 各社において、「スマートメーターシステムセキュリティガイドライン」及び「電力制御システムセキュリティガイドライン」に基づき、電力制御システム等のシステム関係者がセキュリティの重要性を認識し、適切に対策を実施するための教育が定期的に行われている。また、停電が発生した場合を想定し、シミュレーターを用いた、送電系統切り替えによる停電復旧訓練を行っている。

４．残存する課題と検討が望まれる対策

① 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価

電気事業者等は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施するリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図る必要がある。万が一、サイバー攻撃が制御系にまで及んだ場合を想定し、被害の影響範囲を最小化して、速やかに復旧するための方法等を構築するとともに、被害を想定した訓練の実施に努めていくことが必要である。なお、2020 年東京オリンピック・パラリンピック競技大会では、会場において競技継続に必要な重要負荷のバックアップとして、非常用発電機の配備を予定している。

② 制御系システムのセキュリティ対策の強化
制御系システムへのアクセス制御や入退管理などの対策の継続的かつ確実な実施・運用・改善に努めることが必要である。

③ サイバーレスキュー隊の機能の維持
重要インフラ事業者等がサイバー攻撃の被害を受けた場合に初動対応や被害拡大防止策策定の支援を行う IPA のサイバーレスキュー隊の機能を継続的に維持することが必要である。

④ サイバーセキュリティ技術・製品の検証
サイバーセキュリティ技術・製品を公的な機関が検証し、重要インフラ事業者等がサイバーセキュリティ技術・製品を活用しやすい環境を構築することが必要である。

⑤ IT 系システムと OT 系システムの相互理解
今後、情報(IT)系システムと制御(OT)系システムの連携とネットワークを活用した高度化・効率化が促進されることも想定されるが、IT 系システムは個人情報やデータの機密性を重視し、OT 系システムでは人的損害や事業継続に対する可用性を重視したシステムとなっており、システムの設計・運用の思想が異なっている。双方が連携したシステムでは、お互いの設計・運用の思想が異なること十分考慮し、「システム全体のリスク分析と事業継続性を踏まえたセキュリティ対策」を実施することが必要である。

⑥ スマートメーターの対応策の検討
今後、普及が予想されるスマートメーターについては、一定の対策が施されているものの、通常の IT 機器と比較すると長寿命であること、使用量が非常に多数に及ぶことから、脆弱性等を悪用され、サイバー攻撃の踏み台とされた場合の対応策を検討する必要がある。

⑦ 内部犯行によるサイバー攻撃への対応
事業者内部・契約外部事業者の犯行によるサイバー攻撃リスクを最小化するための対策強化が必要である。

（２）情報の共有

① 国内外の関係機関との連携

各社の対策（対策事例のベストプラクティスや、社内セキュリティ教育の方法等）の共有や有識者を交えた意見交換の実施に努めていくことが必要である。また、国内外の機関（欧州の EE-ISAC 等）との連携強化を図ることが必要である。

② 現行分野を跨る情報共有の仕組みの検討

我が国の現状（電力会社とガス会社が、それぞれ「電力」と「ガス」の両方を販売。）を踏まえ、例えば「電力＆ガス＆熱供給ＩＳＡＣ」などの創設により、従来の分野を跨る情報共有の仕組みを検討することが求められる。

（３）人材の育成

① 産業サイバーセキュリティセンターの活用

日々高度化するサイバー攻撃の実態を踏まえ、産業サイバーセキュリティセンターの教育カリキュラムを改善するとともに、同センターにおける人材育成を活用し、圧倒的に不足するセキュリティ人材の育成に継続的に取り組むことが必要である。

② 各種人材育成関連プログラムの活用

重要インフラの情報セキュリティ対策に係る第４次行動計画」や「スマートメーターシステムセキュリティガイドライン」及び「電力制御システムセキュリティガイドライン」に基づき、サイバーセキュリティに係る人材の育成・拡充に努めていくことが必要である。

③ IT・OT 双方の人材育成と実践的訓練環境の整備

技術研究組合制御システムセキュリティセンター（CSSC：Control System Security Center）によるサイバーセキュリティ演習、IPA の産業サイバーセキュリティセンター(ICSCoE)による IT 系と OT 系のセキュリティ対処および対策立案能力を向上させるトレーニングが実施されているが、今後、IoT の進展にあわせ、IT 系／OT 系双方のスキルを持つ人材を育てるとともに、サイバー攻撃に対する検知、解析、対処について、分野を横断して連携して対応できる実践的訓練環境の整備が必要である。

（４）その他

① 産業毎のサイバーセキュリティ対策の強化

IoT の進展によるサイバー攻撃の起点の拡大等を踏まえ、産業毎（Industry by Industry）にサプライチェーン全体のサイバーセキュリティ対策強化に取り組むことが必要である。

７．ガス分野

１．リスクの概要

「重要インフラの情報セキュリティ対策に係る第４次行動計画」においては、ガスの供給停止やガスプラントの安全運用に対する支障をガス分野の重要インフラサービス障害として扱っている。都市ガスの製造や供給に係るシステムは、ガスの製造（原料の気化、熱量調整、付臭等）のために、圧力・流量の制御及び監視を行うプラント制御システム（製造系）と導管等の供給ラインの圧力・流量の監視や遠隔遮断弁・ガバナ（圧力調整器）等の制御を行う遠隔監視・制御システム（供給系）の二つに大別される。

これらの制御システムは、次のような特徴を持ち、これまで国内では重要インフラサービス障害に至る事案は発生していない。

・制御システムは、インターネットとは分離した構成とすることを基本としており、インターネット経由の攻撃を困難なものとしている。
・供給系統中にガスホルダーを有している他、ガスは導管中に圧力のある気体として保有されていることから、仮に製造系統の制御システムがサイバー攻撃を受けて製造が停止しても直ちに供給支障には至らない。
・ガバナの緊急停止のための制御システムがサイバー攻撃を受けて仮に一部のガバナが閉止した場合も、冗長性を持たせた導管ネットワークでは供給支障には至らない。また、供給系統の圧力制御は制御システムによらず機械式制御のガバナで行っているため、仮に制御システムへのサイバー攻撃があっても供給支障には至らない。

上記の特徴等からガス分野において重要インフラサービス障害を招来するリスクは低いと考えられるが、Stuxnet に代表されるように、近年、制御系システムへの攻撃手法が高度化しているため引き続きの備えが必要である。

２．国内外で発生した主なインシデント事例

①サイバー攻撃による個人情報、機密情報の漏えい

パスワードリスト型攻撃や標的型攻撃等のサイバー攻撃により Web サイトへの不正ログインや個人情報が発生。（人的脆弱性、システム脆弱性を攻撃）

2017 年 8 月
東京ガスのガス・電気料金情報ＷＥＢ照会サービス「myTOKYOGAS」のサイトにおいて不正アクセスが発生。個人情報 17 件流出の可能性。

2017 年 9 月
東京ガスのガス・電気料金情報ＷＥＢ照会サービス「myTOKYOGAS」のサイトにおいて 10 万件を超える不正アクセスが発生。106 件の顧客情報が閲覧され、その内 24 件はポイントの不正使用の被害あり。

2017 年 10 月
東邦ガス株式会社の「Club TOHOGAS」で 1 万 5 千件を超える不正アクセス発生。顧客情報 103 件が流出した可能性あり。

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

① 日本ガス協会は、サイバーセキュリティ戦略本部が決定した「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」により、ガス CEPTOAR10 社における内規の策定・改訂支援を目的として「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」（現行は 2016 年７月改訂）を策定、適宜改訂を行い、ガス事業者の情報セキュリティ対策を促進している。

② 経済産業省、ガス事業者及び官民の情報共有組織（ガス CEPTOAR）は、毎年、NISC が主催する重要インフラ分野横断的演習に参加し、所管省庁である経済産業省と協力し、官民間や関係機関等との情報共有や連携による対応力の向上を図っている。

③ 都市ガスの製造、供給に係る制御システムは、インターネットとは分離した構成を基本としている。また、供給系統の圧力制御は制御システムによらず機械式制御のガバナで自律的に行っているため、仮に制御システムへのサイバー攻撃があっても供給支障には至らない。さらに、異常流出を感知した際にはマイコンメーターで停止する仕組みとなっている。

④ ガス事業者は、2020 年のオリンピック・パラリンピック競技大会を支える重要サービスを提供する事業者等として、その準備・運営への影響の未然防止等のため、NISC が実施している横断的なものを含むリスク評価に参加し（経済産業省は協力）、リスクマネジメントによる各社の対策強化を進めている。

（２）情報の共有

ガス分野では、「重要インフラの情報セキュリティ対策に係る第４次行動計画 」に基づき、CEPTOAR を通じた業界内の情報共有体制を構築している。また、2012 年より IPA を情報ハ

ブとする、サイバー攻撃情報共有イニシアティブ（J-CSIP）に参画している。また、民間事業者レベルでも、情報共有が行われている。

①「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づき、業界内の情報取扱いルールに則り、事業者、CEPTOAR、経済産業省及び内閣官房と連携した情報共有体制の枠組みに参加している。

② ガス事業者等は、SIG を構築して、IPA が行うサイバー情報共有イニシアチブ（J-CSIP）に参加し、情報共有体制を構築している。

③ 日本ガス協会サイバー情報メーリングリスト（NISC や JPCERT/CC 等から得た情報を配信）の参加組織の充実に努めている。また、事業者の多様性を踏まえつつ、業界内でＩＴ障害の判断基準となる考え方を共有できるよう、「障害事例」の情報共有に力を入れて取り組んでいる。さらに、実務者による常設の日本ガス協会のシステムセキュリティＷＧが、未然防止策や再発防止策等の具体的な取組課題について適切なサポートを行っている。

（３）人材の育成

ガス分野では、IPA に設置した産業サイバーセキュリティセンター等を活用しながら人材育成を進めている。また、各社においても、訓練や研修等を通じた人材育成が行われている。

① IPA に設置された産業サイバーセキュリティセンターが実施する研修に、ガス事業者からの研修生を派遣し、人材育成に努めている。また、CISO/CIO などの経営層クラスを対象とした CISO 向けプログラムに参加している。

② ガス事業者等は、NISC が実施する分野横断的演習に参加し、人材の育成に努めている。

③ 技術研究組合制御システムセキュリティセンター（CSSC）において実施している制御システムにおけるセキュリティ上の脅威の認識、対策効果の体感を目的としたサイバー演習に参加している。

④ ガス事業者は、NICT が実施している大規模演習環境を用いた実践的なサイバー防御演習（CYDER）に参加している。

⑤ 各社において「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」を参考にセキュリティの重要性を認識し、適切に対策を実施するための教育訓練を適宜、実施している。

⑥ 日本ガス協会は、会員事業者に向けたセキュリティに関する説明会や訓練を適宜実施している。独自に運営するインシデントハンドリング訓練の他、直近では制御シス

テムのセキュリティリスク分析講習会を開催している。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① 保安規定に基づくセキュリティ対策
都市ガスの製造・供給設備の制御システムの特徴や事業者の多様性を踏まえつつ、都市ガス供給における安全をより確実なものとすることが重要。そのため、製造・供給に係る制御システムのサイバーセキュリティ対策をガス事業法に基づく保安規程の要求事項の一つとして位置付け、対策の確実な実施を求める方向で検討を行うことが必要である。

② 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価
ガス事業者は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施するリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図る必要がある。

③ サイバーレスキュー隊の機能の維持
重要インフラ事業者等がサイバー攻撃の被害を受けた場合に初動対応や被害拡大防止策策定の支援を行う IPA のサイバーレスキュー隊の機能を継続的に維持することが必要である。

④ サイバーセキュリティ技術・製品の検証
サイバーセキュリティ技術・製品を公的な機関が検証し、重要インフラ事業者等がサイバーセキュリティ技術・製品を活用しやすい環境を構築することが必要である。

⑤ IT 系システムと OT 系システムの相互理解
今後、情報(IT)系システムと制御(OT)系システムの連携とネットワークを活用した高度化・効率化が促進されることも想定されるが、IT 系システムは個人情報やデータの機密性を重視し、OT 系システムでは人的損害や事業継続に対する可用性を重視したシステムとなっており、システムの設計・運用の思想が異なっている。双方が連携したシステムでは、お互いの設計・運用の思想が異なること十分考慮し、「システム全体のリスク分析と事業継続性を踏まえたセキュリティ対策」を実施することが必要である。

⑥ 内部犯行によるサイバー攻撃への対応
事業者内部・契約外部事業者の犯行によるサイバー攻撃リスクを最小化するための対策強化が必要である。

（２）情報の共有

① 現行分野を跨る情報共有の仕組みの検討
我が国の現状（電力会社とガス会社が、それぞれ「電力」と「ガス」の両方を販売。）を踏まえ、例えば「電力＆ガス＆熱供給ＩＳＡＣ」などの創設により、従来の分野を跨る情報共有の仕組みを検討することが求められる。

② 各種情報共有の促進
ガス分野そのものにおいても、日本ガス協会サイバー情報メーリングリストの参加組織の拡充を図り、情報共有を行う体制整備を進めることが重要である。

（３）人材の育成

① 産業サイバーセキュリティセンターの活用
日々高度化するサイバー攻撃の実態を踏まえ、産業サイバーセキュリティセンターの教育カリキュラムを改善するとともに、同センターにおける人材育成を活用し、圧倒的に不足するセキュリティ人材の育成に継続的に取り組むことが必要である。

② 各種人材育成関連プログラムの活用
「重要インフラの情報セキュリティ対策に係る第４次行動計画」や「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」に基づき、サイバーセキュリティに係る人材の育成・拡充に努めていくことが必要である。

③ IT・OT 双方の人材育成と実践的訓練環境の整備
技術研究組合制御システムセキュリティセンター（CSSC：Control System Security Center）によるサイバーセキュリティ演習、IPA の産業サイバーセキュリティセンター(ICSCoE)による IT 系と OT 系のセキュリティ対処および対策立案能力を向上させるトレーニングが実施されているが、今後、IoT の進展にあわせ、IT 系／OT 系双方のスキルを持つ人材を育てるとともに、サイバー攻撃に対する検知、解析、対処について、分野を横断して連携して対応できる実践的訓練環境の整備が必要である。

（４）その他

① 産業毎のサイバーセキュリティ対策の強化
IoT の進展によるサイバー攻撃の起点の拡大等を踏まえ、産業毎（Industry by Industry）にサプライチェーン全体のサイバーセキュリティ対策強化に取り組むことが必要である。

８．水道分野

１．リスクの概要

水道分野においては、水道事業者等が導入している水道水供給の制御システムの８割以上が外部ネットワークと分離したクローズドシステムであるが、システムの不具合による水の供給の停止、不適当な水質の水の供給が国民生活等に与える影響を踏まえ、重要インフラとしてサイバーセキュリティ対策に取り組んでいるところである。

今後 ICT 化の進展に伴い、さらに対策を強化していく必要がある。

重要システムの例としては、「水道施設や水道水の監視システム」と「水道施設の制御システム等」があげられている。

リスクシナリオとして、以下が考えられる。

・外部からの不正アクセスにより、水道水供給の制御システムが外部から不正操作され、配水管理が困難となる
・悪意を持った内部者が制御システムにマルウェアの入った USB を接続し、水道システムが停止する

２．国内外で発生した主なインシデント事例

① ランサムウェアへの感染

2017 年 5 月
世界の少なくとも約 150 か国において、政府機関や病院、銀行、大手企業等のコンピュータが、マイクロソフト製品の脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。川崎市上下水道局において、コンピュータ１台（大容量のデータの送受信をはじめ、海外関係先等との連絡調整を行うためのインターネット接続が可能な専用のパソコンで、水道システムや市行政情報システムとはネットワーク上切り離されている。）がランサムウェアに感染。上下水道施設等への影響はなし。

2017 年 5 月
川崎市の上下水道局がランサムウェアに感染。上下水道システムや業務への影響無し。

② フィッシングサイト

2017 年 2 月
名古屋市上下水道局の偽サイト（フィッシングサイト）が存在。注意喚起を実施。

上記の他、アメリカにおいて水道水の供給が停止した事例等が報告されている。

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

① 厚生労働省は、サイバーセキュリティ戦略本部が決定した「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」により、「水道分野における情報セキュリティガイドライン」を策定し、現行の第 3 版（平成 25 年 6 月））を改訂しつつ、水道事業者の情報セキュリティ対策を促進している。

② 厚生労働省は、ガイドラインに基づくサイバーセキュリティ対策を水道事業者等に求めており、その立入検査等において、確認し、必要に応じて指導を実施している。

③ 厚生労働省、水道事業者及び官民の情報共有組織（水道 CEPTOAR）は、毎年、NISC が主催する重要インフラ分野横断的演習に参加し、所管省庁である厚生労働省と協力し、官民間や関係機関等との情報共有や連携による対応力の向上を図っている。

④ 厚生労働省は、IPA が策定した「制御システムのセキュリティリスク分析ガイド（水道事業者向け）」を水道事業者等に対して周知している。

⑤ 水道事業者は、NISC が実施する 2020 年東京オリンピック・パラリンピック競技大会のリスク評価に参加している（厚生労働省は協力）。

（２）情報の共有

① 水道 CEPTOAR である（公社）日本水道協会を通じて、全国の水道事業者等に対して NISC からの情報（他分野におけるサイバー攻撃事例やセキュリティの脆弱性等）を共有しており、障害事例発生時には、（公社）日本水道協会が障害事例の調査、分析を行い、分析結果を共有している。

② セプターカウンシルには CEPTOAR である（公社）日本水道協会が参画。

③ 水道事業者等は、SIG を構築して、IPA が行うサイバー情報共有イニシアチブ（J-CSIP）に参加し、情報共有体制を構築している。

（３）人材の育成

① 水道事業者は、NISC が実施する分野横断的演習に参加し、人材の育成に努めている。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① 安全基準等の改訂

厚生労働省は、NISC による「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改訂（2018 年 4 月）を受け、「水道分野における情報セキュリティガイドライン」第３版を改訂し、サイバーセキュリティ対策の一層の強化を図ることとしている。

② 使用期間が長い水道制御システムにおけるセキュリティ対策

水道制御システムの場合 10 年以上使用される事もあり、OS 等の古いバージョンのソフトウェアが利用されているケースも数多く残存している。OS のアップデートや不具合対策のモジュール適用も、本来機能を損なう別の不具合を内包している可能性があり、十分な検証を行ってからでないと適用が難しく、一般の情報(IT)系システムに比べて対策が難しい状況である。これらシステムの特性を十分に把握した上で多層的な防御を実施していくことが必要である。

③ 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価

水道事業者は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施する 2020 年東京オリンピック・パラリンピック競技大会のリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図る。

（２）情報の共有

① 現行分野を跨る情報共有の仕組みの検討

取水から排水に至る水道の全体を考えた場合、上水道と下水道は密接に連携していることが明らかである。このため、上下水道に跨る「上水道＆下水道ＩＳＡＣ」の創設を検討することが必要である。

（３）人材の育成

① IT・OT 双方の人材育成と実践的訓練環境の整備

制御系機器を扱っているため、IT 系／OT 系双方のスキルを持つ人材を育てるとともに、サイバー攻撃に対する検知、解析、対処について、サプライチェーン(機器製造者)や分野を横断して連携して対応できる実践的訓練環境の整備が必要である。

９．石油分野

１．リスクの概要

石油精製・元売企業のシステムは、主に本社や販売拠点において受発注業務や社内管理業務等を行う情報系システムと、主に製油所等の生産拠点において石油精製装置の制御・管理等を行う制御系システムから構成されており、いずれのシステムについても、業界内安全基準「石油分野における情報セキュリティ確保に係る安全ガイドライン」等に基づき、防護対策を実施している。

現時点では顕在化していないものの、今後、特に制御系システムにおける IoT の活用が進展し、製油所において通信機能を有した計測機器や管理用端末が多数導入されたり、これらを接続するワイヤレスネットワークの構築などが行われた場合には、これら IoT 機器やネットワーク環境の脆弱性を突いたサイバー攻撃を受ける危険性が高まる可能性がある。

また、インフラとして国民の生活を支えるとともに、サプライチェーンの一部として様々な分野と関連しているため、被害が他分野に波及し、影響が深刻化、広域化するリスクも増えていくと想定される。

２．国内外で発生した主なインシデント事例

①サイバー攻撃によるインフラ障害

石油業者へのシステム侵入やマルウェア感染により、データ破壊、制御システムの停止が発生。（システム脆弱性を攻撃）

2008 年
トルコにおいて、石油パイプライン監視カメラの通信ソフトの脆弱性を利用したサイバー攻撃により石油パイプラインが爆発。（報道）

2012 年 8 月
サウジアラビアにおいて、国営石油企業の制御系システムがマルウェアに感染し、制御系ネットワークが停止。（報道）

2017 年 6 月
ロシアの石油会社でマルウェア感染。データ破壊の被害。（報道）

②サイバー攻撃による個人情報、機密情報の漏えい

パスワードリスト型攻撃や標的型攻撃等のサイバー攻撃により Web サイトへの不正ログインや個人情報が発生。（人的脆弱性、システム脆弱性を攻撃）

2015 年 6 月
石油連盟の事務端末が標的型メールによるマルウェア感染し、石油政策上の要望事項とその関連資料が流出。2 万 5 千件を超える顧客情報が流出した可能性あり。

③石油事業者へのハッキング等

事業者への攻撃を意図したハッキング事案やマルウェアの感染が発生。（人的脆弱性、システム脆弱性を攻撃）

2017 年 12 月
ロシアの石油輸送管路企業が、同社システムで不正な暗号通貨採掘ソフトを検出。（報道）

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

石油分野では、サイバー攻撃の動向やサイバーセキュリティ戦略を踏まえ、基準やガイドラインの整備、技術的対策や態勢の強化を図っている。

① 石油分野の重要インフラ事業者で構成される「石油連盟 IT セキュリティ連絡会」は、サイバーセキュリティ戦略本部が決定した「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」により、「石油分野における情報セキュリティ確保に係る安全ガイドライン」を策定し、石油事業者の情報セキュリティ対策を促進している。

② 経済産業省、石油事業者及び官民の情報共有組織（石油 CEPTOAR）は、毎年、NISC が主催する重要インフラ分野横断的演習に参加し、所管省庁である経済産業省と協力し、官民間や関係機関等との情報共有や連携による対応力の向上を図っている。

③ 石油精製・供給システムは、本社・事業所等で生産計画、受発注・物流の管理等を行う情報系システムと、製油所で石油製品の精製・出荷を行う制御系システムから構成されており、両システムは分離した構成となっている。また、制御系システムは、緊急時に独立したアナログ信号や手動で停止可能となっている。

④ 石油事業者は、2020 年のオリンピック・パラリンピック競技大会を支える重要サービスを提供する事業者等として、その準備・運営への影響の未然防止等のため、NISC が実施している横断的なものを含むリスク評価に参加し（経済産業省は協力）、リスクマネジメントによる各社の対策強化を進めている。

（２）情報の共有

石油分野では、「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づき、CEPTOAR を通じた業界内の情報共有体制を構築している。また、2012 年より、IPA を情報ハブとする、サイバー攻撃情報共有イニシアティブ（J-CSIP）に参画している。

① 「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づき、業界内の情報取扱いルールに則り、事業者、CEPTOAR、経済産業省及び内閣官房と連携した情報共有体制の枠組みに参加している。

② IPA の公的機関としての信頼性の下で、秘密保持等契約を結び、秘匿性の高い情報を含む標的型攻撃等の情報を収集、解析、秘匿化、共有することにより被害拡大の防止を図る J-CSIP に参画している。

（３）人材の育成

経済産業省において、セキュリティ人材育成を強化施策の柱とし、知識、スキルを高めるための各種育成施策を進めている他、各社においても、訓練や演習を通じた人材育成が行われている。

① IPA に設置した産業サイバーセキュリティセンターにおいて実施しているサイバーセキュリティ対策の中核となる人材の育成を目的とした中核人材プログラム（１年コース）に研修生を派遣している。また、CISO/CIO などの経営層クラスを対象とした CISO 向けプログラムに参加している。

② 2013 年より NICT が実施している大規模演習環境を用いた実践的なサイバー防御演習（CYDER）に参加している。

③ 各社において、「石油分野における情報セキュリティ確保に係る安全ガイドライン」に基づき、システム関係者がセキュリティの重要性を認識し、適切に対策を実施するための教育が定期的に行われている。

④ 関係業界団体が保安担当者向けに開催している「産業安全塾」を通じて、サイバーセキュリティの重要性について理解を深めている。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① サイバーレスキュー隊（IPA）
重要インフラ事業者等がサイバー攻撃の被害を受けた場合に初動対応や被害拡大防止策策定の支援を行うIPAのサイバーレスキュー隊の機能を継続的に維持することが必要である。

② サイバーセキュリティ技術・製品の検証
サイバーセキュリティ技術・製品を公的な機関が検証し、重要インフラ事業者等がサイバーセキュリティ技術・製品の活用を検討しやすい環境を構築することが必要である。

（２）情報の共有

① 各種情報共有の促進
NISC からのニュースレターの共有、サイバー情報共有イニシアチブ（J-CSIP）による情報共有を引き続き実施し、検知したサイバー攻撃情報や対策情報の共有による同種被害の最小化、予兆情報共有に基づいた早期警戒による実被害の抑止を図る必要がある。

（３）人材の育成

① 産業サイバーセキュリティセンター（IPA）
日々高度化するサイバー攻撃の実態を踏まえ、産業サイバーセキュリティセンターの教育カリキュラムを改善するとともに、同センターにおける人材育成を活用し、圧倒的に不足するセキュリティ人材の育成に継続的に取り組むことが必要である。

② ガイドラインに基づく人材育成計画の実施
「重要インフラの情報セキュリティ対策に係る第４次行動計画」や「石油分野における情報セキュリティ確保に係る安全ガイドライン」に基づき、サイバーセキュリティに係る人材の確保等に関する計画策定と実施に努めていくことが必要である。

（４）サプライチェーン対策

① サプライチェーン全体のサイバーセキュリティ対策強化
IoT の進展によるサイバー攻撃の起点の拡大等を踏まえ、産業毎（Industry by Industry）にサプライチェーンのサイバーセキュリティ対策強化に取り組むことが必要である。

10. 化学分野

１．リスクの概要

石油化学プラントにおける制御系システムは、ネットワーク間にファイアウォールを設置することで、自社の情報系システムとは独立したシステムとして、設計・運用されている。また、これまでは専用 OS を利用した機器で構成されてきた。

しかし、近年、汎用 OS の利用が拡大するとともに、USB 等の外部記憶媒体を介した感染や標的型攻撃を行うマルウェアの出現により、今後、石油化学プラントへのサイバー攻撃のリスクが増大すると想定される。

２．国内外で発生した主なインシデント事例

①サイバー攻撃による個人情報・機密情報の流出

2016 年 3 月
太陽日酸株式会社において、情報系システムのサーバへの不正ログインを検知。グループ国内従業員及び退職者の会社名、氏名、職位、メールアドレスの情報が流出した可能性あり。

2017 年 7 月
日産化学工業株式会社において、同社のウェブサイトへの不正アクセスあり。情報流出はなし。

②化学事業者のサイト改ざん

2017 年 10 月
アイカ工業株式会社において、同社のウェブサイトがサイバー攻撃を受け、ファイルが不正に改ざんされた。

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

化学分野では、サイバー攻撃の動向やサイバーセキュリティ戦略を踏まえ、基準やガイドラインの整備、技術的対策や態勢の強化を図っている。

① 「重要インフラの情報セキュリティ対策に係る第４次行動計画 」を踏まえ、「石油化学

分野における情報セキュリティ確保に係る安全基準」を策定し、安全基準等の整備や障害対応体制の強化等の取組を行っている。

② 毎年、NISC が主催する重要インフラ分野横断的演習に参加、所管省庁である経済産業省と協力し、官民間や関係機関等との情報共有や連携による対応力の向上を図っている。

③ 石油化学コンビナートのシステムは、本社・事業所等で生産計画、受発注・物流の管理等を行う情報系システムと、化学プラントで製品の精製・出荷を行う制御系システムから構成されており、ファイアウォールを設置することで両システムは分離した構成となっている。また、制御系システムは、緊急時に独立した緊急停止システムにより安全に停止可能となっている。

（２）情報の共有

化学分野では、「重要インフラの情報セキュリティ対策に係る第４次行動計画 」に基づき、セプターを通じた業界内の情報共有体制を構築している。また、2012 年より、IPA を情報ハブとする、サイバー攻撃情報共有イニシアティブ（J-CSIP）に参画している。

① 「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づき、業界内の情報取扱いルールに則り、事業者、セプター、経済産業省及び内閣官房と連携した情報共有体制の枠組みに参加している。

② IPA の公的機関としての信頼性の下で、秘密保持等契約を結び、秘匿性の高い情報を含む標的型攻撃等の情報を収集、解析、秘匿化、共有することにより被害拡大の防止を図る J-CSIP に参画している。

（３）人材の育成

経済産業省において、セキュリティ人材育成を強化施策の柱とし、知識、スキルを高めるための各種育成施策を進めており、化学分野では、当該施策等を活用しながら人材育成を進めている。また、各社においても、研修等を通じた人材育成が行われている。

① IPA に設置した産業サイバーセキュリティセンターにおいて実施しているサイバーセキュリティ対策の中核となる人材の育成を目的とした中核人材プログラム（１年コース）に研修生を派遣している。また、CISO/CIO などの経営層クラスを対象とした CISO 向けプログラムに参加している。

② 技術研究組合制御システムセキュリティセンター（CSSC）において実施している制御システムにおけるセキュリティ上の脅威の認識、対策効果の体感を目的としたサイバー演習に参加している。

③ 2013 年より NICT が実施している大規模演習環境を用いた実践的なサイバー防御演習（CYDER）に参加している。

④ 各社において、「石油化学分野における情報セキュリティ確保に係る安全基準」に基づき、プラント制御システム等のシステム関係者がセキュリティの重要性を認識し、適切に対策を実施するための教育が定期的に行われている。

⑤ 関係業界団体が保安担当者向けに開催している「産業安全塾」を通じて、サイバー攻撃を含めた安全への脅威への対応について理解を深めている。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① サイバーレスキュー隊（IPA）
重要インフラ事業者等がサイバー攻撃の被害を受けた場合に初動対応や被害拡大防止策策定の支援を行う IPA のサイバーレスキュー隊の機能を継続的に維持することが必要である。

② サイバーセキュリティ技術・製品の検証
サイバーセキュリティ技術・製品を公的な機関が検証し、重要インフラ事業者等がサイバーセキュリティ技術・製品を活用しやすい環境を構築することが必要である。

（２）情報の共有

① 各種情報共有の促進
NISC からのニュースレターの共有、サイバー情報共有イニシアチブ（J-CSIP）による情報共有を引き続き実施し、検知したサイバー攻撃情報や対策情報の共有による同種被害の最小化、予兆情報共有に基づいた早期警戒による実被害の抑止を図る必要がある。

（３）人材の育成

① 産業サイバーセキュリティセンター（IPA）
日々高度化するサイバー攻撃の実態を踏まえ、産業サイバーセキュリティセンターの教育カリキュラムを改善するとともに、同センターにおける人材育成を活用し、圧倒的に不足するセキュリティ人材の育成に継続的に取り組むことが必要である。

② ガイドラインに基づく人材育成計画の実施
「重要インフラの情報セキュリティ対策に係る第４次行動計画」や「石油化学分野　における情報セキュリティ確保に係る安全基準」に基づき、サイバーセキュリティに係る

人材の育成・拡充等に関する実施に努めていくことが必要である。

（4）サプライチェーン対策

① サプライチェーン全体のサイバーセキュリティ対策強化

IoT の進展によるサイバー攻撃の起点の拡大等を踏まえ、産業毎（Industry by Industry）にサプライチェーン全体のサイバーセキュリティ対策強化に取り組むことが必要である。

11. 金融分野

１．リスクの概要

近年、金融分野におけるサイバー攻撃の高度化・複雑化が進む中、サイバー攻撃により金融機関や金融市場インフラの機能が停止するリスクが増大しており、金融分野のサイバーセキュリティの確保は、金融システム全体の安定のため喫緊の課題となっている。

また、金融分野においては、その業務の特性上、他業種よりも多くの顧客情報等を保有しており、こうした情報が漏えいした場合には、業務及び顧客へ及ぼす影響は甚大なものとなることが想定される。

２．国内外で発生した主なインシデント事例

①サービス障害

金融機関のホームページやオンラインサービスページへの DDoS 攻撃の予告や実際の攻撃によるサービス障害等が発生。

2017 年 6 月・9 月
日本の複数の金融機関に対し、期日までに身代金としてビットコインを支払わなければ DDoS 攻撃を仕掛ける旨の脅迫メールが送信。一部の金融機関では、メール受信後に DDoS 攻撃が発生し、短時間ながら Web サイトの閲覧が出来なくなった。

②個人情報・機密情報の流出

WEB サーバやメールサーバの脆弱性を突いた不正アクセス等により、個人情報等の漏えいが国内外で発生。

2014 年 10 月
米国の「ＪＰモルガンチェース」において、従業員の PC にマルウェアが感染。攻撃者の遠隔操作によって、サーバに保管されていた約 8,000 万件の顧客情報が漏えい。

2015 年 2 月
米国の「アンセム」（Anthem、保険会社）のデータベースサーバに対して不正アクセスが発生。

8,000 万件以上の顧客情報が漏えい。

2016 年 9 月
日本の「優良住宅ローン」（貸金業者）の電子メールの管理サーバへの不正アクセスにより、外部への自動転送設定がなされ、電子メールに含まれる約 3 万 7000 件の個人情報が漏えい。

2017 年 7 月
「マネースクウェア・ジャパン」（FX 業者）のホームページに外部よりサイバー攻撃を受けていることを検知。過去 1 年間にさかのぼり被害状況を調査したところ、2016 年 7 月、同年 11 月にも同様の攻撃を受け、計約 11 万件の個人情報が漏えい。

③金銭奪取

銀行への攻撃により、SWIFT（国際的な送金システム）に利用されている PC が遠隔操作され、不正な送金指図が行われ金銭が奪取される事案が海外において複数発生。また、仮想通貨交換業者が不正アクセスを受け、仮想通貨が流出する事案も発生。

2016 年 2 月
バングラデシュ中央銀行において、SWIFT に利用されている PC が遠隔操作され、不正な送金指図が行われ約 8,100 万ドル（約 94 億円）が窃取される被害が発生。

2017 年 10 月～
上記に加え、以下のように、SWIFT を利用した不正送金事案が発生。

- 2017 年 10 月、「遠東國際商業銀行」（台湾）から約 6,000 万ドル（約 67 億円）（ただし、実際の被害額は約 47 万ドル（約 5,300 万円））、
- 同年 10 月、「NIC アジア銀行」（ネパール）から約 4 億 5,000 万スリランカルピー（約 3 億 4,000 万円）、
- 同年 12 月、「Globex 銀行」（ロシア）から約 5,500 万ルーブル（約 1 億 600 万円）（ただし、実際の被害額は約 580 万ルーブル（約 1,100 万円））、
- 2018 年 2 月、「シティユニオン銀行」（インド）から約 200 万ドル（約 2 億 1,200 万円）

2018 年 1 月
日本の「コインチェック」（登録申請中のみなし仮想通貨交換業者）が不正アクセスを受け、当社が管理する仮想通貨（ＮＥＭ）580 億円相当が外部に流出。

このほか、インターネットバンキング利用者の ID やパスワード等を窃取して不正送金される被害が発生。

（参考）国内の不正送金の被害件数・被害額
2015 年：被害件数 1,495 件、被害額 30 億 7,300 万円
2016 年：被害件数 1,291 件、被害額 16 億 8,700 万円

３．サイバーセキュリティ対策の現況

金融分野では、2015 年 7 月に策定・公表した「金融分野におけるサイバーセキュリティ強化に向けた取組方針」に沿った取組を実施。

なお、本取組方針の策定に先立ち、監督指針等を改正。

（１）監督指針等の改正

2015 年 4 月、金融機関に求めるサイバーセキュリティの管理態勢について、監督指針等を改正し、以下の点を着眼点として明確化。

- サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。
  - ・組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制
  - ・情報共有機関等を通じた情報収集・共有体制等

- サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。

- サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。

- サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。

- サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。

（２）「金融分野におけるサイバーセキュリティ強化に向けた取組方針」の策定・公表・実施

金融分野のサイバーセキュリティ対策の強化には、官民が一体となって取り組んでいくことが重要。

このため金融庁は、2015 年 7 月に、サイバーセキュリティの確保を図る観点から、金融機関と建設的な対話を重ね、金融分野のサイバーセキュリティを強化するため、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（以下、「取組方針」）を策定・公表し、官民一体となって取組を推進中。

具体的には、以下の取組を実施。

① 実態把握

2015 年 10 月以降、地銀・第二地銀、信金・信組、証券会社、生損保、取引所等に対し実態把握を行っており、2017 年末までに合計 215 社を実態把握済。

具体的には、金融機関のサイバーセキュリティ対策の状況を深掘りするため、経営陣等との対話を含めインタビュー形式で下記項目（※）を確認。また、金融庁から他金融機関の良好事例を紹介するなど双方向の議論を通じて、経営陣の積極的な関与を促し、課題の共有を図っている。

実態把握の結果については、対象金融機関以外に対しても、

・経営陣に対しては、業界との意見交換会を通じて、経営陣の積極的な関与によるサイバーセキュリティ対策の重要性を説明、

・実務者に対しては、良好事例・共通課題をとりまとめ、業界向け説明会やワークショップ等を通じて業界全体にフィードバック、

している。

※「確認項目」の具体的な内容

・サイバーセキュリティに関する経営陣の取組
・リスク管理の枠組み
・サイバーセキュリティリスクへの対応態勢
・コンティンジェンシープランの整備と実効性確保
・サイバーセキュリティに関する監査

② 大手金融機関との建設的対話

３メガバンク、大手生損保とは定期的（隔月程度）に、大手金融機関の対応状況を把握するとともに、官民相互に気付きを共有し、中小金融機関へのフィードバックにも活用している。

③ 金融業界横断的なサイバーセキュリティ演習

サイバー攻撃に的確に対応するためには、演習を通じて、現在のインシデント対応態勢が十分であるかを確認するなど、PDCA サイクルを回しつつ、インシデント対応能力を向上させることが有効。そのため、2016 年から、金融庁主催の「金融業界横断的なサイバーセキュリティ演習」（通称：Delta Wall（※））を毎年１回実施している。

（※）Delta Wall：サイバーセキュリティ対策のカギとなる「自助」、「共助」、「公助」の３つの視点（Delta）＋防御（Wall）

（参考）演習の参加金融機関は、2016 年は 77 先、2017 年は 101 先

演習に当たっては、以下の点を重視。

- 民間の専門家の知見や攻撃の実例分析等を参考にしつつ、金融機関が陥りやすい弱点が浮き彫りとなり、参加者に「気づき」を与えることができるシナリオ
- 演習実施までの間に自主的なインシデント対応能力の向上を促すために、シナリオの

骨子を事前に開示（オープンシナリオ方式）
- 多くの関係部署（経営層、システム部門、広報、企画部門等）が参加できるよう、自職場参加方式で実施（⇔会場集合方式）
- 参加金融機関が「つつがなく演習をクリア」したことで良しとしないよう、「とり得た他の選択肢」等を提示するなど事後評価に力点
- 本演習の結果は、参加金融機関以外にも業界全体にフィードバック

④ 情報共有

ⅰ）金融 ISAC
金融分野では、我が国の金融機関によるサイバーセキュリティに関する情報共有・分析を行い、金融システムの安全性を維持することにより、利用者の安心・安全を継続的に確保するため、「金融 ISAC」を設立（2014 年 8 月）。

（参考）2018 年 1 月時点で正会員 330 先、準会員 13 先

参加金融機関同士による脅威情報等の共有に加え、各種 WG を通じた取組や、演習の実施等様々な活動が行われている。
日々巧妙化するサイバー攻撃に対し、個別金融機関のみでサイバー攻撃に対応することには限界がある。そのため、金融庁としても金融 ISAC 等の情報共有機関等を活用して情報共有・分析を行う「共助」の観点が重要であるため、未加盟金融機関の加盟の促進を含め、金融 ISAC を通じた情報共有の一層の推進を金融機関に促している。

ⅱ）「新潟県金融機関サイバーセキュリティ情報連絡会（2018 年 2 月 22 日設立）」など、各地域で業態を超えた共助態勢が進展。

⑤ 人材育成

金融 ISAC や金融情報システムセンター（FISC）（※）といった関係機関とも連携し、金融機関職員のサイバーセキュリティ対策に係る知識・スキルを高めるためのワークショップや演習等の取組を実施中。

（※）金融情報システムの安全性確保のための施策を推進することにより、我が国金融情報システムの安全性、信頼性及び効率性を高め、金融機関利用者の安全確保と利便の向上を図ることを目的に設立（1984 年 11 月）された公益財団法人。

ⅰ）金融庁主催のワークショップ
金融機関のサイバーセキュリティにかかる各種対策・整備の考え方について理解を深め、サイバーセキュリティ対策の効果的・効率的な底上げを図るため、第二地銀、信用金庫、信用組合、証券会社を対象にワークショップを開催（2016 年度に 10 財務（支）

局で計 23 回)。

ⅱ）金融 ISAC の活動

「インシデント対応」や「不正送金」をはじめ、特定のテーマにフォーカスして分析・対応の検討を行う各種ワーキンググループへの金融機関職員の参加を通じ、ノウハウの共有やスキルアップの向上を図る取組。

- 技術面も含めた知識の向上を図るため、実機によるシステム環境の構築やログの解析等の内容を盛り込んだ演習（サイバークエスト）を毎年１回実施（合宿形式)。

ⅲ）FISC のワークショップ

FISC において、サイバーセキュリティにかかる各種対策・整備の考え方に対する理解の向上やスキルアップを図る、「中小金融機関向けのワークショップ」を 2017 年度に全国で 9 回開催（2018 年度も 11 回開催予定)。金融庁、金融 ISAC 及び JC3 も連携し講師を派遣。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① 中小金融機関のサイバーセキュリティ対策の底上げ

信金・信組等の中小金融機関においては、「サイバーセキュリティに着眼したリスク評価の実施」や「インシデント発生を想定したコンティンジェンシープランの策定」といったサイバーセキュリティ対策の基礎となる部分が未だ不十分であることから、中小金融機関の底上げを図る必要がある。

すでに、取組を進めているものは以下の通り。

- 中小金融機関を中心に実態把握を継続して実施するとともに、協同組織中央機関・共同センター等との対話を実施
- 2017 年 10 月、中小金融機関の参加を拡充して実施した「金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅱ）」について、業界全体に対しても演習結果をフィードバックし、インシデント対応能力の向上を促進

② 大規模な金融機関のサイバーセキュリティ対応能力の更なる引上げ

大規模な金融機関については、仮にサイバー攻撃を受けた場合にはその影響が金融システム全体に及ぶおそれがあることから、そのサイバーセキュリティ対応能力をさらにもう一段引き上げるため、「脅威ベースのペネトレーションテスト（テスト対象企業ごとに脅威の分析を行い、個別にカスタマイズしたシナリオに基づく実践的な侵入テスト）」等、より高度な評価手法の活用を促進すべきである。

（２）情報の共有

① 中小金融機関の情報共有の促進

個別金融機関のみでサイバー攻撃に対応することには限界がある。そのため、金融 ISAC 等の情報共有機関等を活用して情報共有・分析を行う「共助」の観点が重要である。

特に、信金・信組等の中小金融機関が自社だけでサイバーセキュリティ対策を行うには、人手も費用も時間もかかる。こうした先は人材の数や質、予算など潤沢なリソースを有しておらず、金融 ISAC の活用が有用と考えられるが、信金・信組等の中小金融機関の金融 ISAC への加盟が進んでいないため、金融 ISAC への加盟も含め、金融 ISAC を通じた更なる情報共有の一層の推進を金融機関に促すことが必要である。

（３）人材の育成

① 中小金融機関の経営者・職員の各種演習等への参加の促進

地域に根付いた中小金融機関（地銀・信用金庫・ＪＡなど）の経営者・職員の各種演習参加を促進し、サイバーセキュリティ対策についての意識向上を図るべきである。

（４）その他

① 仮想通貨交換業者における自主規制機能の確立

2018 年 1 月、コインチェック㈱（登録申請中のみなし業者）が不正アクセスを受け、当社が管理する仮想通貨（ＮＥＭ）580 億円相当が外部に流出したことを受け、当社に対し業務改善命令の発出及び立入検査を実施した。

また、全ての仮想通貨交換業者に対しシステムリスク管理に関する報告を求め、その結果を踏まえ、複数の業者に立入検査を実施した。

さらに、仮想通貨交換業者における自主的なサイバーセキュリティの強化に向け、早期に統一の自主規制団体が設立され、実効性ある自主規制機能が確立されるよう促すことが必要である。

12. クレジット分野

１．リスクの概要

クレジット分野では、昨今、EC 加盟店等を狙った不正アクセスにより、カード情報の漏えいが拡大している（2016 年は 55 件で前年比 1.5 倍、報告ベースの暫定値）。これに伴い、偽造カードやネット上での本人なりすましによる不正使用被害が増加している（年間 142 億円）。

なお、重要インフラ事業者であるクレジットカード会社では、クレジットカードを取扱う事業者におけるデータセキュリティの国際基準であるPCI DSS※に準拠するなど必要なセキュリティ対策を講じており、現時点でサイバー攻撃によるインフラ障害は発生していない。

※PCIDSS（Payment Card Industry Data Security Standard）とは、クレジットカード情報を安全に取り扱うことを目的として、国際ブランドが定めたクレジットカード業界の国際的なセキュリティ基準であり、12の要件・約400の要求事項から成る厳格なセキュリティ要件を定めている。

２．国内外で発生した主なインシデント事例

①クレジットカードの偽造による不正引き出し

ハッキングにより、クレジットカード情報を窃取し偽造カードを作成。銀行のクレジットカードで（IC チップ無し）でキャッシングが可能な仕様を悪用した不正引き出しが発生。（システム脆弱性を攻撃）

2016 年 5 月
国内 17 都府県のコンビニ ATM1700 台で、偽造クレジットカードを用いた不正引き出しが発生。

②サイバー攻撃によるカード情報の流出

EC 加盟店等を狙った不正アクセスにより、カード情報の漏えいが拡大している（2016 年で 55 件（前年比 1.5 倍：報告ベース）。

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

クレジット分野では、サイバー攻撃の動向やサイバーセキュリティ戦略を踏まえ、基準やガイドラインの整備、技術的対策や態勢の強化を図っている。

① 「重要インフラの情報セキュリティ対策に係る第４次行動計画 」等を踏まえ、クレジット分野の重要インフラ事業者で構成される「クレジット CEPTOAR 運営会議」において「クレジット CEPTOAR における情報セキュリティガイドライン」を策定、適宜改訂し、安全基準等の整備や障害対応体制の強化等の取組を行っている。

② 毎年、NISC が主催する重要インフラ分野横断的演習に参加し、所管省庁である経済産業省と協力し、官民間や関係機関等との情報共有や連携による対応力の向上を図っている。

③ 2020 年東京オリンピック・パラリンピック競技大会の準備・運営への影響の未然防止等のため、大会を支える周辺サービスを提供する事業者等として横断的なリスク評価等の実施と NISC への報告を通じて、リスクマネジメントによる各社の対策強化を進めている。

④ 政府は、サイバー攻撃によるカード情報の漏えいや不正利用の拡大防止のため、2016 年 12 月に割賦販売法を改正した。本改正法は本年 2018 年 6 月 1 日に施行され、これに基づき、クレジットカード会社や加盟店等においてサイバー攻撃に対する多層的な防御や対処体制が強化される。
具体的には、クレジット取引セキュリティ対策協議会※が策定する「実行計画」に基づき、加盟店にはカード情報の「非保持化」や PCIDSS 準拠といった情報漏えい対策が求められるとともに、今次法改正に併せて、クレジットカード会社には PCIDSS 準拠等の必要なセキュリティ対策が求められることとなる。

※クレジット取引セキュリティ対策協議会： クレジットカード取引に関わる幅広い事業者、行政で構成。同協議会では、①カード情報保護対策、②偽造防止対策（IC 化）、③ネット取引等の不正利用防止対策の取組をまとめた「実行計画」を策定。

⑤ PCIDSS（Payment Card Industry Data Security Standard）とは、クレジットカード情報を安全に取り扱うことを目的として、国際ブランドが定めたクレジットカード業界の国際的なセキュリティ基準であり、12 の要件・約 400 の要求事項から成る厳格なセキュリティ要件を次のとおり定めている。

Ⅰ	安全なﾈｯﾄﾜｰｸｼｽﾃﾑの構築と維持	1.	ｶｰﾄﾞ会員ﾃﾞｰﾀを保護するために、ﾌｧｲｱｳｫｰﾙをｲﾝｽﾄｰﾙして維持する
		2.	ｼｽﾃﾑﾊﾟｽﾜｰﾄﾞおよびその他のｾｷｭﾘﾃｨﾊﾟﾗﾒｰﾀにﾍﾞﾝﾀﾞ提供をﾃﾞﾌｫﾙﾄ値を使用しない
Ⅱ	ｶｰﾄﾞ会員ﾃﾞｰﾀの保護	3.	保存されるｶｰﾄﾞ会員ﾃﾞｰﾀを保護する
		4.	ｵｰﾌﾟﾝな公共ﾈｯﾄﾜｰｸ経由でｶｰﾄﾞ会員ﾃﾞｰﾀを伝送する場合、暗号化する
Ⅲ	脆弱性管理ﾌﾟﾛｸﾞﾗﾑの維持	5.	ﾏﾙｳｪｱに対してすべてのｼｽﾃﾑを保護し、ｳｨﾙｽ対策ｿﾌﾄｳｪｱを定期的に更新する
		6.	安全性の高いｼｽﾃﾑとｱﾌﾟﾘｹｰｼｮﾝを開発し、保守する
Ⅳ	強力なｱｸｾｽ制御手法の導入	7.	ｶｰﾄﾞ会員ﾃﾞｰﾀへのｱｸｾｽを、業務上必要な範囲内に制限する
		8.	ｼｽﾃﾑｺﾝﾎﾟｰﾈﾝﾄへのｱｸｾｽを識別・認証する
		9.	ｶｰﾄﾞ会員ﾃﾞｰﾀへの物理ｱｸｾｽを制限する
Ⅴ	ﾈｯﾄﾜｰｸの定期的な監視およびﾃｽﾄ	10.	ﾈｯﾄﾜｰｸﾘｿｰｽおよびｶｰﾄﾞ会員ﾃﾞｰﾀへのすべてのｱｸｾｽを追跡および監視する
		11.	ｾｷｭﾘﾃｨｼｽﾃﾑおよびﾌﾟﾛｾｽを定期的にﾃｽﾄする
Ⅵ	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの維持	12.	すべての担当者の情報ｾｷｭﾘﾃｨに対応するﾎﾟﾘｼｰを維持する

（２）情報の共有

クレジット分野では、「重要インフラの情報セキュリティ対策に係る第４次行動計画 」に基づき、セプターを通じた業界内の情報共有体制を構築している。また、2017 年 4 月より、サイバー攻撃による被害拡大防止のため、情報共有と早期対応を行う場として、IPA が情報ハブとなる「サイバー情報共有イニシアティブ（J-CSIP）」に参画している。さらに、金融 ISAC への参加など、各社においても、情報共有体制を強化している。

① 「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づき、業界内の情報取扱いルールに則り、事業者、セプター、経済産業省及び内閣官房と連携した情報共有体制の枠組みに参加している。

② クレジット CEPTOAR 運営会議のメンバー51 社は、サイバー攻撃に対処するため、公開情報などを活用している。このほか、JPCERT-CC より、最近のサイバーセキュリティの状況、不正アクセスへの対処法等について、日本クレジット協会の会合等において情報提供を受けている。

③ IPA の公的機関としての信頼性の下で、秘密保持等契約を結び、秘匿性の高い情報を含む標的型攻撃等の情報を収集、解析、秘匿化、共有することにより被害拡大の防止を図る J-CSIP に参画している。

④ 業界のサイバーセキュリティ対策強化を目的に、2016 年 8 月に金融 ISAC が設立された。クレジット分野を含む金融を担う事業者間で、サイバーセキュリティに関する情報の収集・分析や各社のベストプラクティスに係る情報共有を実施するとともに、米国の同様の組織とも連携を深めることとしている。

（３）人材の育成

クレジットカード取引に関連する事業者及び行政等で構成される「クレジット取引セキュリティ対策協議会」の「クレジットカード取引におけるセキュリティ対策の強化に向けた

実行計画」に基づき、日本カード情報セキュリティ協議会（JSDSC）は、以下の取組を実施している。また、その他の施策についても活用し人材育成を進めている。

① PCI DSS 準拠に取り組む認定審査機関（QSA: Qualified Security Assessor）の人員体制の整備・拡充を図ること。

② PCI DSS 準拠に関する内部監査を行うことができる認定審査機関と同等レベルの専門人材を育成すること。

③ 2013 年より NICT が実施している大規模演習環境を用いた実践的なサイバー防御演習（CYDER）に参加している。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① サイバーレスキュー隊（IPA）
重要インフラ事業者等がサイバー攻撃の被害を受けた場合に初動対応や被害拡大防止策策定の支援を行うIPAのサイバーレスキュー隊の機能を継続的に維持することが必要である。

② サイバーセキュリティ技術・製品の検証
サイバーセキュリティ技術・製品を公的な機関が検証し、重要インフラ事業者等がサイバーセキュリティ技術・製品を活用しやすい環境を構築することが必要である。

（２）情報の共有

① 金融 ISAC スキームの活用
各社対策（対策事例のベストプラクティスや、社内セキュリティ教育の方法等）の共有や有識者を交えた意見交換の実施に努めていく。また、国内外の機関（米国の FS-ISAC 等）との連携強化を図るべきである。

（３）その他

① マイナンバー機能の活用
紛失時には 365 日 24 時間体制のコールセンターへの連絡で機能停止も可能な「マイナンバーカード」の公的個人認証機能を活用することで、キャッシュカードやクレジットカードのセキュリティレベルをより向上させる方策を検討すべきである。

13. 情報通信分野

１．リスクの概要

情報通信ネットワークは、様々な事業者やコミュニティが提供する多数の情報通信機器やソフトウェアから構成されており、これらの脆弱性を突き、様々なサイバー攻撃が行われている。

特定の企業や利用者を狙った不正アクセス、機密情報漏えい、サービス運用を妨害するサイバー攻撃等に加え、通信インフラそのものを標的とした DDoS（サービス妨害）等のサイバー攻撃による通信障害も発生している。

また、今後は、IoT を活用した経済・産業活動の変革に伴い、ネットワークに繋がることを想定していないセキュリティ的に脆弱な機器やシステム等がネットワークに接続され、これらを踏み台とした通信インフラへのサイバー攻撃により、様々な分野のサービスに影響が起きるリスクが増大すると想定される。

２．国内外で発生した主なインシデント事例

① サイバー攻撃によるインフラ障害

通信業者やサービス提供会社への直接攻撃や、IoT 機器を乗っ取った DDoS 攻撃、ルータへのマルウェア感染等によるネットワーク障害が発生している（システム脆弱性を攻撃）。

2015 年 12 月
ASAHI ネット社の DNS サーバが DDoS 攻撃を受け、インターネット接続サービス等の接続障害が発生。（報道）

2016 年 8 月
さくらインターネット社の DNS サーバが DoS 攻撃を受け、ホスティングサービスへの接続障害が発生。（報道）

2016 年 9 月
IoT ボットネット（Mirai）による約 1Tbps の大規模な DDoS 攻撃。約 15 万個の監視カメラ等が悪用された。（報道）

2016 年 10 月
米国 911 緊急通報システムに大量の通話発信を誘導。18 歳少年がツールを公開。（報道）

2016 年 10 月、11 月
シンガポールやリベリアの通信事業者に DDoS 被害。Web アクセス不能に。（報道）

2016 年 11 月
Deutsche Telekom 提供のルータにマルウェア感染を狙った攻撃。90 万人に影響。（報道）

2017 年 6 月
シングルサインオンや ID 管理のプラットフォーム OneLogin が情報漏えい。44 か国 2,000 企業、アプリ開発ベンダ 300 社、70 以上の SAAP プロバイダに影響。（報道）

2017 年 7 月
Skype が 2 日間にわたって接続障害。ハッカー集団 CyberTeam が犯行声明。（報道）

2017 年 8 月
インドで 6 万台以上のモデムやルータがマルウェアに感染。Web アクセス接続不能に。（報道）

②サイバー攻撃による個人情報・機密情報の流出

パスワードリスト型攻撃やハッキング等のサイバー攻撃により Web サイトへの不正ログインや個人情報流出、システムへの不正侵入による機密情報流出が発生している（人的脆弱性、システム脆弱性を攻撃）。

2017 年 5 月
InterFM897 の web サイトで不正アクセス。個人情報 2,728 件流出の可能性。

2017 年 5 月
カナダの通信事業者「Bell Canada」に不正アクセス。個人情報 1,700 件流出の可能性。（報道）

2017 年 8 月
米テレビ局 HBO にサイバー攻撃。窃取した未放送ドラマの情報を人質に金銭要求。（報道）

2017 年 9 月
音楽配信サービス「8tracks」で社員アカウントが侵害。約 1,800 万人分の情報流出。（報道）

2017 年 10 月
TOKYO MX の web サイトで不正アクセス。個人情報 1,270 件流出の可能性。

2017 年 11 月
「フジテレビダイレクト」へリスト型攻撃。181 名のアカウント情報流出。（報道）

③通信業社を語るメール、サイト改ざん

通信業社からのお知らせ等を語ったフィッシングメールや、Web サイトの改ざんが発生している（人的脆弱性、システム脆弱性を攻撃）。

2017 年 4 月～
Apple、マイクロソフト、LINE 等を語ったフィッシングメールを多数確認。（報道）

2017 年 5 月
電子署名サービス事業者 DocuSign 社のコンピュータから、顧客とユーザのメールアドレスが流出。流出アドレスに同社をかたるフィッシングメールが送付された。（報道）

2017 年 5 月
国営カタール通信のウェブサイトがハッキングされ、偽の首長声明文が掲載された。（報道）

３．サイバーセキュリティ対策の現況

（１）多層的な防御と対処態勢の整備

政府では、サイバー攻撃の動向やサイバーセキュリティ戦略を踏まえ、基準やガイドラインの整備、技術的対策や態勢の強化を図っている。

① 電気通信事業者におけるサイバー攻撃対策の更なる強化に向けて、現在、総務省では、通信の秘密を確保しつつサイバー攻撃対策を促進するための法整備を含めた検討が進められている。

② 総務省、経産省を中心に、IoT 機器のセキュリティ確保に向けたガイドライン整備等の取組が進められている。

③ 総務省において、「IoT セキュリティ総合対策」に基づいて、IoT 機器の脆弱性調査等、IoT セキュリティ確保のために必要な施策を推進している。

2006 年 9 月～ 「電気通信分野における情報セキュリティ確保に係る安全基準」策定。電気通信事業者協会（TCA）にて継続的に改版を実施。直近の改版は、2016 年 5 月。

2013 年 11 月～総務省において「電気通信事業におけるサイバー攻撃への適正な対処の在り

方に関する研究会」を開催。通信の秘密等に配慮したサイバー攻撃への対処の在り方について検討（2015 年 9 月「第二次とりまとめ」を公表）。

2015 年 11 月　電気通信事業者関連 45 団体から構成される「インターネットの安定的運用に関する協議会」が、「第二次とりまとめ」を受け、「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン（第４版）」を公開。

2016 年 7 月　総務省、経産省、IoT 推進コンソーシアムにより、IoT 機器やシステムやサービスにおいて求められるセキュリティ確保のための基本的な取組を明確化した「IoT セキュリティガイドライン Ver1.0」を公開。

2017 年 1 月～ 総務省が「IoT サイバーセキュリティ アクションプログラム 2017」を公開。サイバーセキュリティタスクフォースを設置し検討を進め、「IoT セキュリティ総合対策」を公表(2017 年 10 月)。

2017 年 10 月～　総務省が、電気通信事業者におけるサイバー攻撃対策の迅速化を目的に「円滑なインターネット利用環境の確保に関する検討会」を開催。電気通信事業者間での攻撃情報の共有や、マルウェアを操作するサーバ（C&C サーバ）の早期検知等について整理。

（２）情報の共有

情報通信分野では、通信系企業を中心に 2002 年から ISAC「Telecom-ISAC」を設置し、情報共有を進めてきたが、ICT 環境の高度化・複雑化や IoT の進展を受け、2016 年に、従来からの通信系企業に加えて放送事業者やセキュリティ企業、ICT ベンダにメンバーを拡大し、ICT 分野をカバーする企業群による ISAC として「ICT-ISAC」を設立した。

① ICT-ISAC では、DoS 攻撃即応、サイバー攻撃対応演習、人材育成、Wi-Fi リテラシー向上等について検討を進めるとともに、国内外の ISAC との連携・協力を進めている。

2002 年 7 月　日本最初の ISAC(Information Sharing and Analysis Center:アイザック)として、通信系企業を中心に Telecom-ISAC を設立。

2016 年 3 月　Telecom-ISAC の活動を継承する形で従来からのメンバーである通信系企業に加え、放送事業者やセキュリティ会社、ICT ベンダが参加し、ICT 分野をカバーする企業群による ICT-ISAC を設立（2018 年 2 月時点で 36 社が参加）。

（３）人材の育成

総務省では、セキュリティ人材の育成を強化施策の一つの柱とし、知識、スキルを高めるた

めの各種取組を進めている。

① 国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等を対象とした大規模演習環境を用いた実践的サイバー防御演習「CYDER」（Cyber Defense with Recurrence）を 2013 年度より実施しており、2017 年度は全 47 都道府県で開催するなど規模を拡大しながら、演習の強化を図っている。

② 2020 年東京オリンピック・パラリンピック競技大会の適切な運営を確保することを目的として、大会関連組織のセキュリティ担当者等を対象とした高度なサイバー攻撃に対処可能な人材の育成を行う実践的サイバー演習「サイバーコロッセオ」を実施している。

③ 未来のサイバーセキュリティ研究者・起業家の創出に向けて、若年層の ICT 人材を対象とした若手セキュリティイノベーターの育成「SecHack365」を実施しており、実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導している。

2013 年 9 月～ 国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等のサイバー攻撃への対応能力の向上を目的として、実践的サイバー防御演習「CYDER」を実施（受講者数：2013 年度 292 名、2014 年度 215 名、2015 年度 208 名、2016 年度 1,539 名、2017 年度 3,009 名）。

2016 年 5 月　NICT が「CYDER」の実施主体となり、安定的・継続的な運用を開始。

2016 年 9 月　「CYDER」の受講枠を拡大し、全ての総合通信局・事務所の管区内（全国 11 ブロック）で地方公共団体を主な受講対象者とする演習を開始。

2017 年 4 月　NICT にナショナルサイバートレーニングセンターを組織し、演習実施体制を大幅に強化。

2017 年 6 月～ 「SecHack365」のプログラムを実施。

2017 年 7 月　「CYDER」の開催回数を拡大し、全国 47 都道府県で地方公共団体を主な受講対象者とする演習を開始。

2018 年 2 月～　「サイバーコロッセオ」を本格的に実施。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① IoT 機器の脆弱性対策実装のための体制整備

今後は、IoT 活用の進展とともにネットワークを介して様々な IoT 機器が接続されたサービスが提供されていくため、情報通信インフラおよび IoT 機器も含めたサービストータルでのセキュリティ対策の強化が必要となる。また、IoT セキュリティ対策は、IoT 機器を利用したサービス全体としてのセキュリティを考えれば、IoT 機器製造事業者、流通事業者、保守ベンダ、ISP 及び利用者といった各主体が補完し合いながら対応していくことが求められる。このため、これらの関係主体と相互に連携し、ネットワーク全体のセキュリティを確保するため、情報共有のあり方を含め、IoT 機器に対する脆弱性対策を実施する体制整備を進める必要がある。

② IoT 機器のセキュリティ検査の仕組み作り

IoT 機器が比較的長期にわたり運用される傾向がある中で、その運用期間中において継続的に安全安心な状態を維持することができるよう、機器の脆弱性に係る接続試験を行うテストベッドの構築を含むセキュリティ検査の仕組み作りを進める必要がある。

③ フリーWiFi 利用の際の注意喚起

外国人観光客への利便性向上を目的に、全国各地で整備が進められているフリーWiFi について、十分なセキュリティ対策が講じられておらず、ID 及びパスワードが入力不要なものまたは非常に簡便なまま放置されているものや通信が暗号化されていないものが多数見受けられることから、セキュリティ対策を確認した上で利用するなどの注意喚起を発出することが必要である。

（２）情報の共有

① ICT-ISAC を核とする情報共有機能の更なる強化

今後は、ネットワークを介しての様々な分野の連携が進むため、各分野において情報共有を行う体制（ISAC）の立ち上げの加速と、分野を跨る情報共有の仕組みが必要となる。そのため、ICT-ISAC を核として、対策を見据えた情報共有を効果的に行う取組を強化するとともに、このような活動を通じて、他分野に対しても情報共有の模範となるような先行的な情報共有モデルを示しつつ、他分野の ISAC との連携を進め、我が国全体の情報共有機能強化を図る必要がある。

（３）人材の育成

① IT・OT 双方の人材育成の推進

今後、IoT の進展にあわせ、IT(Information Technology)系のセキュリティ技術者に加え、OT(Operational Technology)系のセキュリティ技術者の育成を進めるとともに、IT 系 OT 系を跨るサイバー攻撃に対する検知・解析、対処を連携して進めることができるような育成訓練の仕組みが必要となる。

② 各種人材育成関連プログラムの維持・強化

我が国のセキュリティ人材は質的にも量的にも圧倒的に不足しており、セキュリティ人材の育成は喫緊の課題であることから、引き続き、政府において、関係機関・企業等と十分に連携しながら、セキュリティ人材の育成の取組が必要となる。そのため、新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツの開発に努めつつ、実践的サイバー防御演習「CYDER」の充実、「サイバーコロッセオ」の更なる内容の拡充、「SecHack365」による若手セキュリティイノベーターの育成等の継続的な実施が必要である。

（４）研究開発の推進

① 研究開発の成果普及や社会実装の推進

サイバー空間における攻撃の態様は常に変化しており、これに対応するには、政府が支援する産学官連携による研究開発の成果を即座に反映した最新のサイバーセキュリティ対策を実施していくことが有効である。そのため、引き続き、NICT を中心に、サイバーセキュリティに関する研究開発（例えば、匿名性を確保したデータ利用技術等）に取り組むとともに、研究開発成果の普及や社会実装を推進していく必要がある。

② スマートシティの技術開発・国際標準化の推進

スマートシティにおいて、データ連携・解析などを行うプラットフォームのセキュリティ対策はデータの真正性を確保し、かつ、スマートシティの機能をサイバー攻撃から防御するためにも極めて重要である。そのため、スマートシティのプラットフォームに係るセキュリティ要件の具体化や所要の技術開発を推進するとともに、その成果を国際的な標準化プロセスに提案する等の取組を一体的に進めていく必要がある。

③ 抗堪性・秘匿性の高い衛星通信技術の開発

世界的な人工衛星等の産業利用に向けた活動の活発化による衛星利用の需要拡大に対応するため、また、衛星通信に対する脅威となりつつあるサイバー攻撃や物理的な攻撃から衛星通信ネットワークを防護し、、安全な衛星通信ネットワークの構築を可能とするため、高秘匿な衛星通信に資する技術の研究開発などに取り組む必要がある。

④ ハードウェア脆弱性の検知技術の開発

集積回路の設計工程において、ハードウェア脆弱性が存在する可能性が指摘されており、総務省では、戦略的情報通信研究開発推進事業（SCOPE）により、平成 29 年度から、ハードウェア脆弱性の検知技術の研究開発が行われている。今後、IoT 端末はさらなる増加が見込まれており、引き続き、ハードウェアに組み込まれる恐れのあるハードウェア脆弱性を検出する技術の研究開発について、ビッグデータや AI を活用しつつ推進していく必要がある。

（５）その他

① 通信の秘密やプライバシーの確保の関係についての検討

「迅速で実効的なサイバー攻撃対策」のためには、「通信の秘密やプライバシーの確保」との関係について、法的整理を行う必要がある。

② 電波妨害への留意

「電波妨害」についても十分に留意した対策を検討すべきである。

14. 政府・行政サービス分野（その１　政府）

１．リスクの概要

政府機関等において発生した情報セキュリティインシデントの主な要因は、外部からの攻撃によるものと意図せぬ情報流出によるものに大別される。

平成 28 年度においても、職員の過失等による意図せぬ情報流出に係る情報セキュリティインシデントが散見されたが、年間を通じて Apache Struts 等ウェブアプリケーションの脆弱性を悪用した攻撃が頻発した。

２．国内外で発生した主なインシデント事例

システム途絶に至るサイバー攻撃は、政府機関では発生していない。

NISC では、GSOC において、GSOC センサーを政府機関に設置し政府横断的な情報収集・監視を行い、サイバー攻撃やその準備動作等の脅威を検知する業務を行っている。これは、外部から政府機関に対する不審な通信（不正アクセス等）や、標的型攻撃等によりもたらされた不正プログラムが行う外部との不審な通信等を検知し、攻撃を発見するもので、その検知は重要である。この GSOC センサーによる横断的な監視や政府機関の Web サイトの稼働状況の監視活動において、2016 年度に政府機関への脅威と認知された件数は、約 711 万件であった（図表Ⅰ-２-２）。これは、約 4.4 秒に１回、脅威を認知している計算となり、2015 年度の約 613 万件と比較して、約 100 万件増加している。2015 年度も 2014 年度から脅威の認知件数が増加したが、2016 年度は、2015 年度を上回る脅威を認知しており、政府機関に対する攻撃が一層増加していることを示している。

３．サイバーセキュリティ対策の現況

政府機関におけるサイバーセキュリティ対策については、NISC 及び各府省庁が適切な役割分担の下、相互に密接に連携しつつ、政府全体として効果的な対応をとることができるよう体制を構築して実施している。

（１）多層的な防御と対処態勢の整備

① NISC においては、政府横断的な立場からサイバーセキュリティ対策を推進するため、政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）を設け、政府機関の情報システムに設置した GSOC センサーを通じ、24 時間 365 日体制の下、政府機関に対

するサイバー攻撃等の不審な通信の横断的な監視、分析、情報収集を実施するとともに、各府省庁への通報、情報提供、助言などを行っている。

② NISC は、各府省庁の要請により情報セキュリティ緊急支援チーム（CYMAT）を派遣し、技術的な支援・助言を実施している。

③ NISC は、各府省庁の監査を行い、今後のサイバーセキュリティ対策を強化する上で有益な助言等を行った。さらに、「情報セキュリティ監査実施手順の策定手引書」の改定を行い、府省庁における情報セキュリティ監査の実効性の向上を図っている。

④ 各府省庁においては、組織内 CSIRT を設置し、自組織の情報システムの構築・運用を行うとともに、サイバー攻撃による障害等の事案が発生した場合には、情報システムの管理者としての責任を果たす観点から、自ら被害拡大の防止、早期復旧のための措置、原因の調査、再発防止等の対応を実施する。

（２）情報の共有

① NISC は、政府機関の情報システムに設置した GSOC センサーを通じ、24 時間 365 日体制の下、政府機関に対するサイバー攻撃等の不審な通信の横断的な監視、分析、情報収集を実施するとともに、各府省庁への通報、情報提供、助言などを行っている。

（３）人材の育成

① 政府機関におけるセキュリティ・IT 人材の確保・育成については、「サイバーセキュリティ人材育成総合強化方針」（2016 年３月 31 日サイバーセキュリティ戦略本部決定）に基づき、各府省庁において毎年「各府省庁セキュリティ・IT 人材確保・育成計画」を策定し、同計画に基づく体制の整備として、2016 年度に府省庁全体で約 80 の定員増による体制強化を実現したほか、有為な人材を確保するための採用活動、研修の受講等の取組を推進した。

② NISC においては、2016 年度から各府省庁に設置された「サイバーセキュリティ・情報化審議官」等を対象とした研修を実施し、実際に発生したセキュリティインシデントを題材としたケーススタディなどを通じて、当該審議官等の各府省庁におけるセキュリティ対策の司令塔機能として必要な知識・能力の向上に努めた。さらに、一定の専門性を有する人材を育成するため、新たに、全府省庁のセキュリティ担当者を対象とした e ラーニング及び「CISSP 入門講座」を実施した。

③ 政府機関の情報セキュリティ担当者向け勉強会の開催、新任管理者向けの情報セキュリティをテーマとした講演の実施、近年のサイバーセキュリティに関する情勢を踏まえた初任者研修向け資料の提供、一般職員向けの教育資料の改定等、それぞれの対象者に応じた適切な教育施策を実施し、職員全体のサイバーセキュリティに関する素養の向上を

確実なものとするよう取り組んだ。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① 政府全体の対処態勢の整備
特に国民生活および経済活動に及ぼす影響が高い行政機関においては、NISC が中心となって、関係府省庁と連携しつつ、セキュリティ対策の向上を行う必要がある。具体的には、インシデントに対応する体制の強化だけでなく、不審な通信を検知した際、速やかに独立行政法人などの専門機関と連携して、各府省庁や関連機関に迅速に情報提供するための対処態勢基盤が必要である。

② 事前対応型防護への移行
人工知能等を活用し、未知のマルウェアを検知可能な技術を確立し、エンドポイント（端末）の管理・監視技術と組み合わせた事前対応型防護方式の不正プログラム対策を開発し、事前対応型の防護方策を確立することが必要である。

③ 資産管理の自動化
高度化・複雑化する情報システムに生じる多様な脆弱性に機動的に対応するため、情報資産及びその脆弱性の管理を自動化すべきである。

④ 保有情報の流出時のフェールセーフの確保
万一、不正アクセス等により情報が漏えいした場合でも、自動的に暗号化を行うこと等により容易に解読ができない仕組みを導入することが必要である。

⑤ 政府全体の機能強化
政府全体の防護能力を高めるため、NISC が中心となって、関係府省庁と連携しつつ、セキュリティ対策の向上を行う必要がある。また、我が国の安全保障上の脅威が高いとされる国で製造された機器など、深刻な悪影響を及ぼす可能性のある技術的課題に関する研究・検証体制の構築など取り得る体制を検討し、将来的にはサイバーセキュリティを担当する官庁の設置または NISC の一層の機能強化を図るなど、政府全体の機能強化について検討すべきである。以上の対策を通じて、全府省庁の情報システム（端末となる公用 PC を含む）のセキュリティ対策に万全を期すべきである。

（２）情報の共有

① 対策情報の活用による機能強化方策の導入
資産管理の自動化、事前対応型の防護方策の導入と並行して、対策情報等の自動的な生成、供給、実装などを含めた機能強化方策の導入を検討すべきである。

（３）人材の育成

① 政府全体の IT・セキュリティ人材の育成・確保

政府全体の IT/セキュリティ人材の育成・確保を進めるに当たり、各府省庁において、計画的に当該人材の育成・確保及びキャリアパスの設定を積極的に行うべきである。特に、NISC 等における高度なセキュリティ人材の育成・確保のため、インシデント対応のための CSIRT 機能及び NISC の CYMAT の維持・強化も図るべきである。

② 一般職員の情報リテラシー能力の向上

職員を対象とした IT およびセキュリティ教育の実施とインシデント発生時の報告手順の徹底などによる対処能力の向上を図るべきである。

（４）その他

① 公用携帯の貸与対象の拡大

アプリの取り込み制限など、十分なセキュリティ対策を講じた「公用携帯」につき、少なくとも「局長級以上全員」など、配布対象者の拡大を検討すべきである。

14. 政府・行政サービス分野（その２　地方公共団体）

１．リスクの概要

日本年金機構における個人情報流出事案は、多くの住民情報を扱う地方公共団体にとっても改めて重大な警鐘となった。そこで、総務省は、各地方公共団体のシステムネットワークの総点検の結果等を踏まえ、マイナンバーによる情報連携の稼動を見据えて、マイナンバーを利用する端末等からの情報持ち出しを禁止するなど、地方公共団体に情報セキュリティ対策の抜本的強化に取り組むことを要請した。

しかしながら、情報セキュリティ技術は日々向上する一方、セキュリティ上の脅威も増大している。このため、総務省は、「地方公共団体における情報セキュリティポリシーに関するガイドライン」を逐次改定するとともに、民間の高度なセキュリティ人材と連携しながら、全国の地方公共団体と最新の技術や対策などの情報共有を図っている。

２．国内で発生した主なインシデント事例

① 標的型メール攻撃

2015 年６月
マルウェア等ウイルスの添付されたメールが特定の職員に送付され、ファイルを開封することによりウイルスに感染し、不正に情報を外部に送信する等の被害に繋がる。平成 27 年６月の年金機構の情報漏えい事件直後に、長野県上田市等地方公共団体においても同様の事案の発生が確認された。

② 職員による不正な情報持ち出し

2015 年 12 月
大阪府堺市の職員が、市民個人情報 68 万人分を無断で自宅に持ち帰り、レンタルサーバに保存していたが、それが外部からアクセスできる状態にあり、外部からのアクセスも確認された。

③ OSの脆弱性をついたランサムウェア

2017 年５月
Windows の脆弱性に対応した更新プログラムを適用しないまま使用されているパソコンがあり

（特にサポートを終了した OS)、Windows の脆弱性をついたランサムウェア「WannaCry」に感染すると、パソコン内のファイルが暗号化された上、解除するための身代金を要求するメッセージが表示される（静岡県富士市消防本部や川崎市上下水道局等から総務省に報告)。

３．サイバーセキュリティ対策の現況

（１）新たな自治体情報セキュリティ対策の抜本的強化

各地方公共団体において、年金機構の事案発生後（平成27年６月）直ちに、緊急時の対応体制やシステム・ネットワークの総点検等が実施された。

その結果を踏まえ、情報提供ネットワークシステムの稼働までに、各地方公共団体において、インシデント即応体制や職員への訓練の徹底などの情報セキュリティ確保体制の強化を図るとともに、次の三段階の対策で、情報セキュリティ対策の抜本的強化を図った。

① マイナンバー利用事務系（既存住基、税、社会保障など）においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への二要素認証の導入等を図ることにより、住民（個人）情報の流出を徹底して防ぐこと。

② マイナンバーによる情報連携に活用される LGWAN 環境のセキュリティ確保に資するため、財務会計など LGWAN を活用する業務用システムと、Web 閲覧やインターネットメールなどのシステムとの通信経路を分割すること。なお、両システム間で通信する場合には、ウイルスの感染のない無害化通信を図ること（LGWAN 接続系とインターネット接続系の分割)。

③ インターネット接続系においては、都道府県と市区町村が協力してインターネット接続口を集約した上で、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を講じること。

（２）各地方公共団体におけるインシデント即応やセキュリティ確保の体制強化

① 最高情報セキュリティ責任者（CISO）の設置とインシデント対応チーム（CSIRT）の強化

② 市町村に対する都道府県による初動対応の支援体制の強化

③ NISC までのインシデント連絡ルートの再構築（多重化）

④ 緊急時対応計画の見直し（インターネット遮断ルール等の追加）と準備の徹底

⑤ セキュリティ専門人材による支援体制の構築（自治体情報セキュリティ支援プラットフォーム（平成 27 年９月 30 日稼動開始））

⑥ NISC、NICT 及び個人情報保護委員会等と連携してセキュリティ人材の育成促進（CYDER 等）

⑦ 人的セキュリティの強化と職員の訓練の徹底（平成 27 年８月 21 日通知）

⑧ 自治体クラウド等により節減した費用等を情報セキュリティ対策に振り向け
※これらの内容を踏まえ、「地方公共団体における情報セキュリティポリシーに関するガイドライン」を改定予定

（３）技術知見の共有やプログラム更新のための仕組みの構築

① 「自治体情報セキュリティ支援プラットフォーム」（平成 27 年９月稼動）を活用して、民間の高度なセキュリティ人材と連携しながら、全国の地方公共団体と最新の技術や対策などの情報共有を図る。

② 「自治体情報セキュリティ向上プラットフォーム」（平成 29 年 12 月稼動）により、地方公共団体が LGWAN 系など内部環境にある端末にインストールされている OS やアンチウイルスソフトに適切に更新プログラムを適用する仕組みを提供。

４．残存する課題と検討が望まれる対策

（１）多層的な防御と対処態勢の整備

① 業務効率化との両立
情報セキュリティを強化することにより、メールの添付ファイル取り込みや重要なデータベースへのアクセス等情報の取扱い時に職員の操作が増え手間がかかるようになったとの指摘がされることから、セキュリティレベルを維持しつつも操作性の向上を図ることのできる新しい技術の適用に向けた調査研究が求められる。

② 自治体クラウドの推進を踏まえた対策
今後、自治体クラウドの進展とともに、各地方公共団体の情報システムやネットワークの構成について変容することが想定されるので、これらを踏まえたセキュリティ対策を常時検討することが必要である。

（２）情報の共有

① 各種情報共有の促進

NISC からのニュースレターの共有などによる情報共有を引き続き実施し、検知したサイバー攻撃情報や対策情報の共有による同種被害の最小化、予兆情報共有に基づいた早期警戒による実被害の抑止を図る必要がある。

（３）人材の育成

① 情報セキュリティの啓発や訓練

標的型メールへの対応や USB による情報持ち出し等職員のセキュリティ・リテラシーが求められる事案も多いことから、今後、職員に向けた情報セキュリティの啓発や訓練が継続して必要である。

15. 安全保障分野

１．リスクの概要

先進的な防衛力においては、情報通信ネットワークへの依存度が一層増大しているところであるが、サイバー攻撃は、敵の体制の弱点につけ込んで、敵の強みを低減できる非対称的な戦力となっていることから、サイバーセキュリティは安全保障上での重要な課題となっている。

２．国内外で発生した主なインシデント事例（国防省・軍関連）

2008 年
米国中央軍の秘密情報等を取り扱うネットワークがウイルス感染する。（報道）

2009 年 7 月
米国及び韓国の国防部を含む政府機関等のウェブサイトへの攻撃

2016 年 8～9 月
韓国軍の内部ネットワークへのサイバー攻撃

３．サイバーセキュリティ対策の現況

（１）情報システムの安全確保

防衛省及び自衛隊が構築・運用するシステム（DII）については、そのネットワークをオープン系、クローズ系に分離するとともに、外部からの不正なアクセスの防止・検知のためファイアウォール、ウイルス検知ソフトを導入している。また、セキュリティ対策が十分であるか否かのチェックのために、システム監査を定期的に実施している。

（２）専門部隊によるサイバー攻撃対処

専門知識を有する者から構成されるサイバー防衛隊等により、ネットワーク・情報システムの２４時間監視、サイバー攻撃対処（解析等）を行っている。

（３）サイバー攻撃対処態勢の整備

職員が遵守すべきセキュリティ対策及び情報システムのセキュリティ対策基準を制定し

ている。

（４）最新技術の研究

より実践的な対策を経験し、職員のスキルを向上させるため、サイバー演習環境構築技術の研究を行うとともに、今後のサイバーセキュリティに大きな影響を及ぼすと想定される人工知能（ＡＩ）のサイバーセキュリティへの活用に関する調査研究を行っている。

（５）人材育成

米国カーネギーメロン大学付属機関、国内大学院への留学や各自衛隊の専門課程における教育の実施を行い、専門人材の育成を行うとともに、一般職員におけるセキュリティ意識の醸成のため、職場における教育、防衛大学校における専門教育についても実施している。

（６）他機関等との連携

NISC、米軍、関係各国等との情報共有を行っている。

４．残存する課題と検討が望まれる対策

サイバー空間等の新たな領域の活用が死活的に重要になっていることを踏まえ、従来の延長線上ではなく、国民を守るために真に必要な防衛力のあるべき姿について検討

（１） 多層的な防御と対処態勢の整備

① サイバー防衛隊等の体制拡充
高度化・巧妙化するサイバー攻撃に対応すべく、サイバー防衛隊等の拡充を加速するとともに、組織の在り方を検討すべきである。また、サイバー反撃能力のあり方について検討すべきである。

② 防衛調達における情報セキュリティの強化
重要度の高い企業、機関、設備、情報をそのサプライチェーン全体を含めてサイバー攻撃から守る為、また日本 IT 産業の国際競争力を維持・強化する為、日本でも米国の情報保全ガイドライン（NIST SP-800）と同様の我が国としてのルールを整備し、国際相互認証を獲得すべきである。

③ サイバー政策推進体制の強化
防衛省・自衛隊におけるサイバー政策担当部局の体制を強化すべきである。

④ サイバー関連予算の拡充
防衛省・自衛隊におけるサイバー関連事業予算を拡充すべきである。

⑤ 諸外国等との連携強化
米国や友好国、国際機関等の国際社会との連携を強化し、サイバー空間の安定的かつ効果的な利用を促進すべきである。

⑥ 情報収集・分析機能の強化と事態対処態勢の整備
サイバー空間における情報収集・分析能力の抜本的強化を図り、日本の情報収集能力全体を補完し、インテリジェンス強化を図るとともに、平時における周辺国等におけるサイバー状況把握及びその分析を強化し、例えば、他国・組織の戦力やサイバー攻撃能力、手法等の研究を含め、有事の発生に対して万全の体制で臨み被害を最小限に抑制することに努めることが必要である。

（２） 情報の共有

① 関係機関・民間企業との連携強化
サイバー攻撃に迅速かつ効果的に対応するためには、関係機関・企業との連携が不可欠。このため、NISC をはじめとする政府機関や民間企業と、官民連携の枠組みも活用しつつ緊密に連携し、委託先における情報セキュリティ対策（オフラインのシステムの対策の義務化などを含む。）を検討し、サイバーセキュリティに関する情報共有や意思疎通等を促進すべきである。

（３）人材の育成

① 人材の確保・維持・活用
サイバーに関する部内外の教育を拡充すべきである。また、サイバーに関する高度な専門知識を有する外部の人材を活用するため、官民人事交流制度や役務契約等の制度の活用を検討すべきである。さらに、サイバー人材のインセンティブ向上のための施策を検討すべきである。

（４）その他

① サイバー技術の強化
自衛隊施設や移動系システムを含め、防衛省・自衛隊に対するサイバー攻撃に適切に対処するため、人工知能の活用や暗号技術等のサイバー技術の研究開発を推進すべきである。

Ⅲ　提言

【望まれる対策の方向性について（全分野共通）】

１．多層的な防御と対処態勢の整備

多層的な防御手段を想定し、「技術の進歩に合わせた新たな防御技術の開発促進」、「サプライチェーン全体を捉えたセキュリティ対策」及び「セキュリティバイデザイン」の取組が必要である。

また、サイバー攻撃を 100%防ぐことは不可能であるため、「自然災害と同様に捉えたリスクの把握」、「攻撃の早期検知」、「迅速な情報共有による被害拡大の防止」、「事業継続のためのルールや対策の強化」を促進できる仕組みが必要である。

① 国家プロジェクトとしての検知・防御・攻撃者解析技術の開発
国家プロジェクトとして、リソースを集中的に投入して、関係研究機関・大学・産業界が緊密に連携して技術開発を積極的に推進し、我が国の検知・防御・解析技術の能力を強化する。また、サイバーセキュリティ上、深刻な悪影響を及ぼす可能性のある技術的課題に関する研究・検証体制を構築すべきである。

② リスクマネジメントの強化
重要インフラ事業者、2020 年東京オリンピック・パラリンピック競技大会における重要サービス事業者、我が国の安全保障に関わる機関などについて、その提供するサービスへの影響を念頭に置き、また使用するシステム・機器についてのサプライチェーン全体や物理的なセキュリティとサイバーセキュリティの関係なども意識したシナリオベースでのリスク分析を行い、インターネットから隔離されたものを含め防護すべきシステムとリスクをリスト化するなどで特定し、演習の実施などにより対策を確認することが必要である。特に、2020 年東京オリンピック・パラリンピック競技大会に向けては、シナリオ作成やリスト分析を行う事業者を育て、また、諸外国における事例も参考とするため、関係諸国との連携を進めるべきである。

③ サプライチェーン全体のサイバーセキュリティ対策に関するフレームワークの整備
分野別のものを含め、サプライチェーン全体のサイバーセキュリティ対策に関するフレームワークを整備すべきである。

④ セキュリティバイデザイン（機器の企画・設計段階からセキュリティ対策）の強化
指数関数的に増加する IoT 機器等について、事後的な対応だけでは十分なセキュリティ対策を講ずることは困難であるため、セキュリティバイデザインの考え方を機器やシステムベンダーに徹底するための取組を早期に強化すべきである。

⑤ 人的要因（内部犯行、外部犯行、単純ミス等）によるリスクの軽減
セキュリティマネジメントの普及・徹底に加え、各組織が、自組織の従業者、業務委託先の従業者等についてセキュリティ教育の徹底を図り、必要に応じて不正通信の自動検知、インターネットと隔離されたシステムの防護装置の導入などの技術的対策を促進するとともに、重要な業務については、各組織がその内容と重要性を把握した上で、民間で使用できるセキュリティ・クリアランス手法や一定期間以上勤続し、信用情報が確認されている者を充てるなどのルール確立の検討など委託先や従業員の信頼性を確認していく人員配置を徹底し、官民で着実に取り組む必要がある。

⑥ 緊急時対処におけるリーダーシップの強化と連携の促進
緊急時対処において、現場レベルでの対処責任者と CIO/CISO との迅速な連絡体制と平素からの信頼関係の構築、権限の明確化を図り、継続的な運用が必要である。特に、政府においては、GSOC、各省庁等の CSIRT、支援体制の CYMAT を設置しているが、省庁の縦割りをなくし、継続的に NISC がリーダーシップをもって連携を促進すべきである。

⑦ 事業継続確保策の強化と普及
重要インフラ事業者がその安全なサービスの継続的な提供を確保する観点から、事業継続確保の方策を強化すべく、さらに必要な環境整備を行っていくべきである。その際、事故などに対処する保安体制などと整合的なものとすべきである。

⑧ 新規事業・技術に対する対応（ガイドライン等）のスピード感とカバー範囲の検討
IT／サイバーセキュリティの技術進歩にあわせて、スピード感をもって新規事業・技術に対応した制度整備、ガイドライン整備等を進めることが必要である。

⑨ 個別主体頼みになっているサイバー攻撃対策の改善
重要インフラ事業者の事業及びそのリスクを横断的に分析してリスク管理していくこと、関係者が共同してサイバー空間そのものをクリーンにしていく方策・技術の検討、サプライチェーン対策として関係者全体を共通プラットフォーム上で防護するなど、関係者の協働によってサイバー攻撃対策を進めるべきである。

⑩ 海底ケーブルなどのサイバー空間インフラの防護
完全性、可用性の確保のため、国際通信の主たるインフラである海底ケーブルなど、サイバー空間を支えるインフラ自体の防護も不可欠である。このため、関係組織と連携して、インフラ自体の防護の取組も十分に強化する必要がある。

⑪ 自然災害発生時など（通信手段が完全に確保できない）、「複合リスク」への対応策構築
リスク対処に関わる組織においては、「複合リスク」の評価・点検をできるだけ早期に行い、バックアップ・冗長性を持たせるなど、必要なリスク対応策を構築すべきである。

⑫ 健全なサイバー空間の維持のための取組
政府機関、地方公共団体、重要インフラ事業者、大学、サイバー空間関連事業者、国民

など全ての関係者は、サイバー空間に生じている現象が自らに密接に関係しており、共に役割を果たすことによりはじめてサイバー空間を良好な状態に保つことができるとの意識の下、積極的に自らセキュリティ対策に取り組むとともに、政府は、内閣官房を中心として情報発信に努めるべきである。その際、サイバー空間に生じている現象を適切に表現できるよう、メディアを通じた国民とのコミュニケーションの在り方を検討すべきである。

２．情報の共有

「インシデント情報」と「ベストプラクティス情報」の迅速な共有と対処が重要である。米国では、ＩＳＡＣの設置が進んでおり、金融や通信など 20 以上が存在。日本においても、ICT、金融、電力、自動車、貿易など各分野でのＩＳＡＣが設置され、サイバーセキュリティに関する情報の共有・分析の取組が進められているが、更なる分野の拡大が必要。

今後、「サプライチェーンを踏まえた縦の情報共有」、「各分野横断での横の情報共有」、「海外の産学官組織との斜めの情報共有」を行える仕組みが必要である。

① 情報共有基盤の整備

専門機関を含む官民の多様な主体が安心して相互にセキュリティ対策に資する情報の共有を図るための体制を、国が各主体の自主性を重んじた上で形成することで、官民横断的、業界・ＩＳＡＣ横断的でかつ国内外を問わない情報の共有・連携をそのためのシステムの整備を含めて推進することが必要である。その際、既存の取組との連携体制を強化するため、国がリーダーシップをもって推進すべきである。また、参加のインセンティブ（例えば、情報やノウハウなど得られるものが多いこと）、適切な運営（違反者に対する制裁、適切なメンター（実質的な技術者のリーダー役）の参加などを含む。）のための仕組みが重要である。

さらに、2020 年東京オリンピック・パラリンピック競技大会を見据え、NISC に設置されるオリパラ CSIRT とのホットラインの構築など重要インフラ事業者間でより迅速な情報共有を行うための体制を構築すべきである。

② 「重要インフラ」分野の拡大（空港施設・海上交通・国会等）

重要インフラは、現在、サイバーセキュリティ戦略本部が定めている電力等の１３分野に限るべきではない。特に、グローバルなネットワークを形成する空港施設、海上交通に関連する事業者のサイバーセキュリティ対策の推進は不可欠である。

また、国会等の機関は「事業を行う者」ではないものの国民生活又は経済活動に多大な影響を及ぼすものであり、政府と連携してサイバーセキュリティ対策を強化すべきである。

③ ＩＳＡＣ設置の促進と参加事業者の拡大

IT 化の進展、IoT の普及を鑑みれば、以下に掲げる分野においても、情報共有その他の取組を進めることが求められる。アクションプランの策定に向けた検討を早急に開始すべきである。

（分野の例）

スマートシティ、スマートホーム、スマート家電等（防犯カメラやAIスピーカー含むIoT機器全般）、海上交通（海運事業者＆船舶製造事業者）、医療＆介護＆健康、石油＆天然ガス、食品＆スマート農林水産業、不動産、地方公共団体、研究＆教育、小売＆サービス、上水道＆下水道、人材派遣等（事務・警備・清掃・ビルメンテナンス）、防衛関連、シェアリングエコノミー（カーシェア・ハウスシェア等）、気象・災害情報、交通管制（陸海空）、航空（空輸事業者、航空機製造事業者、航空管制・空港事業者）

④ ＩＳＡＣの拡大・再編

IT化を通じて、従来の異なる分野が密接に関係するようになっている状況を踏まえ、情報共有組織であるISACを新たに組織し、またはすでにあるISACを拡大する検討を行い、必要な再編を行うべきである。

（再編すべき分野のイメージ）

・陸上交通（バス、タクシー、トラック、自動運転、電子交通標識等）
・電力、ガス、熱供給（電力自由化により、事業者が一体化してきている）
・交通（鉄道、物流、航空）、船舶

⑤ 企業がインシデント情報の通知やリコールを躊躇する原因（株価・信頼低下）の克服

例えば、公益通報を受けて適切にリコールの対応をしている組織が評価される仕組み、「法定伝染病」を参考にした所管の機関への報告の義務付けなどの例を参考にしつつ、サイバーセキュリティリスクについての情報発信の在り方を検討すべきである。

⑥ 国際的枠組・協調の在り方の検討

価値観を共有する国との間での多国間・二国間での情報連携の枠組み・協調をさらに緊密にしていくことが重要であり、協議・対話に加え、情報や技術等の共有（例えば情報共有基盤などを含む）、ペネトレーションテストを含む共同演習などの在り方を引き続き検討すべきである。

一方、価値観を十分に共有できていない国との間でも、偶発的な事故などが生じないよう、信頼醸成のための枠組みの構築が必要である。

３．人材の育成

民間セクターでも、政府、地方公共団体でも、組織においてサイバーセキュリティ対策やインシデント対応を指揮出来る人材や専門人材が絶対的に不足している。

人材の裾野を広げ、レベルアップを図るとともに、中長期的に高度人材を発掘・育成する計画的な仕組みづくりが必要であり、並行してセキュリティ対策の省人化、高度化を図ることも急務である。

また、「高度人材が、自らのスキルを活かせ、モチベーションを持って業務に取り組める柔

軟性のある環境創り」や、「産学官連携や企業間連携により、不足している高度人材をより有効に活用していく仕組み」が必要である。

① 指揮官の育成・確保

サイバーセキュリティ対策やインシデント対応にあたっては、様々な能力や役割を持った実務者や専門人材を、経営や事業の視点を意識しつつ、プライオリティをもって指揮できる指揮官が必要である。

特に、企業等における経営層と技術者を含む実務者をつなぐ「戦略マネジメント層」について、スキル取得のための教育コンテンツの作成、スキル認定のための制度等の構築に取り組み、これらの人材の育成・確保に努めるべきである。

② 初等中等教育、高等教育における人材力の強化

初等中等教育において、倫理、サイバーセキュリティやＩＴを司る物事の原理を理解し論理的思考ができる能力を育てるため、学習指導要領の柔軟な運用、教育課程における教員の養成はもちろんのこと、教育課程外の地域や企業・団体等において、民間の人材の柔軟な活用、深層学習機能を持った人工知能（AI）の活用なども含め、自由にサイバー関連ツール、機器を用いて興味を持って学べる機会が豊富に用意されるような環境整備を進めるべきである。

高等教育では、基礎的技術の体系的な教育に加え、高度な技術を習得できる環境を一層整備すべき。さらに、技術のみならずマネジメントや法律、心理学などサイバーセキュリティに必要な人文社会科学との連携した研究教育も推進すべきである。

また、教員養成課程における IT・プログラミング・セキュリティに関する必須科目を追加することを検討すべきである。

③ ＩＴだけでなくＯＴにも通じるセキュリティ人材の育成

IT 系のシステムだけでなく、OT 系のシステムにも精通した人材の育成を進めることが必要である。例えば、IPA 産業サイバーセキュリティセンターにおいて、教育コンテンツの充実､必要な機材の充実等を図りながら継続的に取り組んでいくことが必要である。

④ 演習の強化（高度な技能を持つ技術者（ホワイトハッカー）の活用・対象拡大など）

政府機関、重要インフラにおいて実施されている演習において、ホワイトハッカーを活用し（例えば、何らかの理由で更生・矯正が必要な技術者の活用も念頭に置いて）、見落としがちな対策の不備等をついた攻撃を行うなど、より実践的なプログラムにし、高度人材の育成を図るとともに、演習に参加する分野・機関数を拡大すべき。

地方のセキュリティ人材の育成のため、大学、地方自治体、産業界などが連携した体制を構築するとともに、全国での攻防戦形式のコンテストの開催をするなどによって、地域における人材育成の場と雇用の創出に向けた取組を検討すべきである。

⑤ セキュリティ技術者の処遇改善

セキュリティの需要を生む産業界、政府機関におけるセキュリティ人材の役割、知識・スキルといった人材像について、産学官で共通認識を図るとともに、国内外留学など自

らの能力向上の機会の創出やその地位向上や経営陣にも至るキャリアパスの在り方について検討を進めるべきである。その際、給与、待遇などの柔軟な組み合わせにより、処遇の改善を図ることを念頭に置く必要がある。

⑥ 女性セキュリティ技術者が活躍できる環境の整備

女性の IT 技術者、セキュリティ技術者は非常に少ない。コミュニケーション力やユーザー視点を持った女性が、その強みを活かしてセキュリティ技術者として活躍できるよう、女性限定の場を提供するなど、女性が活動しやすくする取組を進めるべきである。

⑦ 地方公共団体・独立行政法人などの取組の強化支援

地方公共団体は依然として厳しい財政状況にあることや、独立行政法人においては運営費交付金が減少傾向にあることから、サイバーセキュリティへの取組が不十分になりかねない。このため、システムの集約・統合化等を行う際に、サイバーセキュリティ対策を推進するインセンティブ及び必要な人員を確保するための予算を措置すべきである。

⑧ 先端的研究者への支援強化

量子コンピュータ、人工知能（ＡＩ）などの先端技術は、サイバーセキュリティにも多大な影響を与えることが予想される。このため、これらの先端的な研究開発を先行的に進める研究者に対して、国策として、将来の産業育成も見据えて、基礎研究を含めて十分な研究環境の整備と研究開発資金の支援を行うべきである。

⑨ 国際的な連携を図るための人材育成

サイバー空間における対策は我が国のみで完結される課題ではなく各国共通の課題であり、国連や OECD、APEC などの国際機関や欧米諸国と連携し、我が国が国際的議論を主導したサイバー空間における安全と平和主義を推進するべきであり、その為に国連、ICPO などの機関に対して省庁横断的な人材輩出を検討すべきである。

４.「サイバーセキュリティ」の産業化

行政も民間セクターも、サイバーセキュリティ対策を「コスト」として捉えるのではなく、「投資」と考え、積極的な対応を行うべきである。そのためにも、適切なインセンティブを示していく必要がある。

今や、サイバー攻撃対策を強化した製品・サービスは国内外市場に於いて優位性を確保できる時代である。現政権が注力しているインフラシステム輸出についても、高度なサイバーセキュリティは激しい国際競争に勝ち抜く力となる。

大企業から中小企業・小規模事業者に至るまでのサプライチェーンを通じて、大規模なサイバー攻撃発生時にも事業継続が可能であることは、市場での高い評価に繋がる。

政府・行政サービス分野においても、サイバー攻撃発生時に、機密情報・個人情報の漏洩を防ぎ、行政サービスの継続性を確保できる体制が整っていることが、国民の皆様の安心確保とともに、日本への投資促進など立地競争力の強化に繋がる。

我が国として必要なセキュリティ技術の開発を行うことなどを通じて、「サイバーセキュリティの産業化」を促進することは、我が国の競争力強化に資するものである。

① 標準・認証制度の在り方検討（日本版 FedRAMP など）
サービスのセキュリティ対策の度合いの可視化や我が国企業の国際競争力向上のため、ISO27017 をベースとした認証制度※や米国の NIST の標準、FedRAMP などを参考として、クラウド認証制度の普及・活用策、国際相互認証を含め、その在り方について検討すべきである。
※ISMS クラウドセキュリティ認証制度、クラウド情報セキュリティ監査（CS マーク）

② セキュリティ製品・サービスの認証制度の在り方検討
高度な技術を有するホワイトハッカー等が脆弱性等を調査することを含め、公的な機関が検証することで、セキュリティ技術・製品を活用しやすい環境を構築することが必要である。
特にセキュアな IoT 機器の任意の認証制度の導入に向け、産学官の連携による民間の認証制度のあり方の検討を進め、また、セキュアな端末の接続試験を行うためのテストベッドを地方に整備するなど、IoT 機器のセキュリティ確保の取組を加速すべきである。

③ セキュリティ製品・サービスを検証するための実環境を再現したテストベッドの整備
セキュリティ製品・サービスの検証を行うためには、例えば、ICSCoE や制御システムセキュリティセンター(CSSC)の体制をテストベッド用に整備するなど、実環境等を再現した場で動作させつつ、想定されるサイバー攻撃等を行ってみることが必要である。

④ サイバーセキュリティ保険の普及
セキュリティ対策の取組の正当な評価、リスクと対策の「見える化」を推進しつつ、対策や加入状況(※)と連動して保険料が変わるサイバーセキュリティ保険の普及が必要である。また、保険の適用範囲の見直し（例：風評被害に対する補償）を進めるべきである。
※サプライチェーンに参加する企業や地域における同業他社などが一括して加入できるサイバーセキュリティ保険に、リスク評価サービス、対策に関するコンサルティングサービスなどを組み合わせた総合的なセキュリティ対策サービスの導入

⑤ 「コスト」から「投資」へ：経営者の意識改革促進
企業は、経営者の役割を明確にし、サプライチェーンを視野に入れた、リスクマネジメントの一環としてのサイバーセキュリティ確保の体制を構築することが重要である。このため、ベストプラクティス集の整理、対策状況の可視化ツールの整備及び PDCA の推進を通じて、経営層の意識改革に向けた官民の緊密な連携による取組を推進することが必要である。

⑥ 「脆弱性診断士」などの資格普及
情報システムやサービスの脆弱性について調査し、その対策提示を含めた的確な判断を

行う「脆弱性診断士」（仮称）の検討、安全な情報システムの企画・設計・開発・運用を支援し、サイバーセキュリティ対策の調査・分析・評価やその結果に基づく指導・助言を行う「情報処理安全確保支援士」の一層の普及を通じて、セキュリティ人材の育成・確保に努めることが必要である。

⑦ 高いセキュリティを誇る製品・サービスの海外展開支援

利便性と高いセキュリティが両立し、我が国が誇る安全かつ高品質な製品・サービスについて、我が国のみならず海外にも展開させることが重要であり、例えば、国として必要なセキュリティ技術の開発を行うことなどを通じて、IT・サイバーセキュリティ企業を育成することなどを含め、その際の必要な支援を強化すべきである。

５．中小企業・小規模事業者への支援

サプライチェーンリスク低減のためにも、サイバーセキュリティ対策強化の取組やビジネス上の留意点については、中小企業・小規模事業者にも浸透し、実践していただく必要がある。

① 中小企業向けサイバーセキュリティ対策ガイドラインの普及

IT の利活用やサイバーセキュリティに対して意識が十分ではない中小企業も存在するため、その実態を調査し、調査結果に基づく対策の促進策や、リスク評価ツールの検討、ベストプラクティス集など最低限の対策を分かりやすくまとめたガイドラインを策定し、その普及に取り組むべきである。

② 情報セキュリティ投資の促進（税制・助成金等）

中小企業は、サイバーセキュリティに対して十分な資源配分（人員、予算）が困難な場合があることから、IT の利活用により生産性向上などとセットになったセキュアなシステムモデル（クラウド活用等）の投資促進に向けた検討を進める。また、社会全体で人材への投資を行い、人材の層を厚くするため、サイバーセキュリティ対策を一つの要件とするシステム導入に関わる税制優遇や助成金を強化すべきである。

６．技術革新に遅れをとらない法制度整備（国内法＆国際法）

① 「サイバー反撃権」「サイバー自衛権」に係る根拠法の検討

政府は、国家安全保障会議を中心に、我が国の安全保障に資するため、サイバー攻撃と武力攻撃との関係についての国際的な議論に積極的に参画するとともに、自衛権との関係について、根拠法の検討を行っていくべきである。また、サイバー反撃にあたっては、攻撃者の特定を含め、平素からサイバー空間における必要な調査・研究の活動が重要と考えられることから、その根拠法についても検討を進めるべきである。

② 重要インフラ分野とＩｏＴ機器にセキュリティ対策を義務付ける法令の検討

現在、電力分野においては、サイバーセキュリティ対策を電気事業法の関連法令上に位置づけて対策を義務付けているが、他の重要インフラ分野においても、業法・保安法において法目的を達成するため、リスクの分析を行いつつ、必要なサイバーセキュリティ対策を法令で義務付けるべきである。
また、IoT 機器についても、サイバー攻撃によって安全上・保安上の問題が発生する恐れが高いもの、例えば自動走行などについて同様に安全・保安関連の法令においてセキュリティバイデザインの観点からセキュリティ対策を義務付けるすべきである。

③ リスクの最小化やインシデント発生時の責任に係る法改正等の検討
IoT 機器やシステム、自動運転、ドローンなどで、サイバー攻撃等による事故・インシデントが発生したときに、既知の脆弱性に対する対策の不作為などにおける製造者の責任、運用者等の安全管理義務といった観点からも問題が生じると考えられるため、例えば道路交通法、PL 法、建築基準法、航空法についてインシデント発生時の責任関係に関する検討を行うべき。

④ 攻撃の解析・情報共有等を促進する法改正等の検討
IoT 機器を含む情報通信機器・システムの脆弱性などの調査・アップデートなどの対策・注意喚起などの情報共有を行うにあたり、結果的に不正アクセスの構成要件に該当したり、攻撃者の推定につながる解析やその結果の公表がウイルス保管罪などに問われかねないおそれがあり、我が国としてのセキュリティ技術・対策の発展が阻害されかねない恐れがあることから、例えば次の法律においていかなる手当をすべきか検討を行うべきである。
●不正アクセス禁止法　（※電気通信事業法等を改正中）
●著作権法　（※法改正中）
●個人情報保護法
●刑法（ウイルス保管罪等）

⑤ 国際的ルールの構築（サイバー攻撃に関する禁止行為・罰則、紛争解決制度等）
国際法の整理（ジュネーブ道路交通条約、国際人道法等）
サイバーセキュリティはグローバルな課題であり、関係する国際ルール、国際法についての課題の抽出、さらにはサイバー攻撃を受けた場合の戦略的広報などの連携方策を含め、我が国としての立場の明確化などの検討等を行うべきである。

⑥ 国会議員等のセキュリティ確保
機密性が高い重要な情報を保持する国会議員は、より一層サイバーセキュリティ対策を講じることが必要であり、議員立法で、国会議員の情報セキュリティについて確立するべきである。また、国会議員の任期後も機密管理のシステムを構築させるべきである。
また、別途、自民党本部としても、実績のあるセキュリティ会社と契約して、党所属議員へのセキュリティ対策の周知啓発を強化するとともに、安全保障に精通する議員のパソコン等のセキュリティに関して一元管理が必要である。

７．必要な予算・定数の確保

米国では 2019 年度の予算(軍事を除く)が＄6486M、英国は 2016～2020 の５年間で 19 億ポンドとしている一方、我が国は H30 年度当初予算が 621 億円である。我が国が着実にセキュリティ対策を実施していくために必要な予算・定員の確保を行っていくべき。

① ＮＩＳＣ、ＮＳＳ、防衛省、警察庁、内閣調査室等の抜本的組織強化
人員体制の拡充や資機材の増強について、検討すべきである。

② 各府省の予算要求時における「サイバーセキュリティ対策特別枠」の設定

●基盤技術・高度技術の開発、先端的研究者への支援強化（再掲）
●セキュリティ製品・サービスを検証するための実環境を再現したテストベッドの整備（再掲）
●脆弱性のあるＩｏＴ機器のセキュリティ対策強化
●中小企業・小規模事業者・地方自治体のセキュリティ強化（再掲）
●サイバー攻撃の被害を受けた組織に対する初動対応支援の強化
●周辺情報収集能力の向上
●国際協力の推進

【望まれる対策の方向性について（分野別）】

１　航空

（１）多層的な防御と対処態勢の整備

① 安全基準等の改訂

国土交通省は、NISC による「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改訂（2018 年 4 月）を受け、「航空分野における情報セキュリティ確保に係る安全ガイドライン」を改訂し、サイバーセキュリティ対策の一層の強化を図ることとしている。今後は、IoT 機器も含めたセキュリティ対策の強化を行う必要がある。

② 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価

航空運送事業者は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施するリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図る必要がある。

③ 空港ビル事業者等の重要インフラ化

「重要インフラ 13 分野」の「航空」とは、航空運送事業者を指し、空港ビル事業者等が含まれていない。空港ビル事業者等は 2018 年度の重要インフラ化を目指し、引き続き調整を行う。

（２）情報の共有

① 各種情報共有の促進と「交通 ISAC」の創設

NISC からのニュースレターの共有、サイバー情報共有イニシアチブ（J-CSIP）による情報共有を引き続き実施するとともに、「交通 ISAC」（仮称）の創設に向けた検討を加速し、情報共有体制の充実を図る。

（３）人材の育成

① 各種人材育成関連プログラムの推進

産業サイバーセキュリティセンターの研修の活用、一般財団法人運輸総合研究所の策定した「航空のサイバー攻撃に対する人材育成に関する調査研究」の活用、NISC が実施する分野横断的演習への参加等により、人材の育成を図る。また、「交通 ISAC」（仮称）においても、人材育成方策を検討する。

（４）その他

① 「ドローン」への対応

様々な用途への活用が進む「ドローン」へのサイバー攻撃に対するリスクの最小化対策が必要。

２　鉄道

（１）多層的な防御と対処態勢の整備

① 安全基準等の改訂

NISC が改訂予定（2018 年４月）である「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」に対応し、「鉄道における情報セキュリティ確保に係る安全ガイドライン」を改訂し、サイバーセキュリティ対策の一層の強化を図る必要がある。

② 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価

鉄道事業者は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施するリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図る必要がある。

（２）情報の共有

① 各種情報共有の促進と「交通 ISAC」の創設

NISC からのニュースレターの共有、サイバー情報共有イニシアチブ（J-CSIP）による情報共有を引き続き実施するとともに、「交通 ISAC」（仮称）の創設に向けた検討を加速し、検知したサイバー攻撃情報や対策情報の共有による同種被害の最小化、予兆情報共有に基づいた早期警戒による実被害の抑止を図る必要がある。

（３）人材の育成

① 各種人材育成関連プログラムの推進

産業サイバーセキュリティセンターの研修の活用、一般財団法人運輸総合研究所において「鉄道のサイバー攻撃に対する人材育成に関する調査研究」の活用、NISC が実施する分野横断的演習への参加等により、人材育成を図る。また、「交通 ISAC」（仮称）においても、人材育成方策を検討すべきである。

（４）その他

① 鉄道の相互乗り入れによる被害広域化の防止策の検討

鉄道の相互乗り入れによる被害広域化について、防止策を検討することが必要である。

３　自動運転

（１）多層的な防御と対処態勢の整備

①「企業や国を超えた協力体制」の整備

自動車・自動運転分野では、運転者の利便性向上や自動車制御技術の向上を目的とした自動車のインテリジェンス化が進み、IoT センサー、クラウド、AI 等を活用したコネクテッドカーや自動運転が実用化される期待が高まっている。2020 年代前半には、日独米国の自動車メーカーが自動運転の実用化を目指しているが、普及に向けてはステークホルダー同士が協調して安全確保のルールを作る取組が重要であり、「企業や国を超えた協力体制」が必要となる。

② サプライチェーン全体での被害発生リスクの抑止

自動車の ICT 技術の多機能化やカーシェアリングなどの利用形態の変化に伴い、サイバー攻撃の侵入口が多様化し、攻撃の手口も高度化していくリスクが存在している。自動車のサイバー攻撃による影響は、盗難による損害や個人情報漏えいだけでなく、遠隔操作や制御装置への不正アクセスによる人命に関わる事故が懸念され、広いエリアに急速に拡大する恐れもある。

そのため、「企画、構築、運用、破棄」までの自動車システムのライフサイクルのフェーズを意識し、サプライチェーン全体で各フェーズでの被害発生リスクを抑止する取組（脆弱性の低減や防御手段の実装）が必要である。

③「セキュリティバイデザイン」の取組

外部ネットワークと接続する車載機器やソフトウェア制御装置の脆弱性を製造段階から検知・排除する「セキュリティバイデザイン」の取組が必要である。

④ 新たなリスクへの対応

高度化していく攻撃リスクへの対策が必要であり、また、自動車整備時やカーシェアリング時などのリスク管理も行う必要がある。

⑤ フェールセーフ機能の装備

センサーや AI を活用した自動運転機能においては、「車載機能のセキュリティ脆弱性の排除」だけでなく、「ネットワークで接続する周辺システムへのサイバー攻撃により、制御装置が異常動作した場合の対処・対策を確実に実行するセーフティ機能を装備すること」が非常に重要である。

（２）情報の共有

① 利用者を含めた情報共有の在り方の検討

「自動運転」「コネクテッドカー」に関わる周辺システムやインフラ事業者を含めた全体的なセキュリティ対策の情報共有や専門機関との対策検討に加え、利用者への早期通知

の仕組みも検討すべきである。

② 情報共有の範囲の拡大の検討
「交通 ISAC」を検討する際、「陸上交通」であれば、バス、タクシー、トラック、自動運転、電子交通標識等、幅広い主体で組織することを検討すべきである。

（３）人材の育成

① 各種人材育成関連プログラムの推進
自動車分野に関連するセキュリティ人材のレベルアップに向け、「制御システムのエンジニアへのサイバーセキュリティ教育」だけでなく、「IT エンジニアへの制御系装置のセキュリティ対策教育」や「相互交流」が必要である。

② プログラムの高度化・複雑化に対応できる人材の育成
自動運転の更なる高度化に伴い、車向けのソフトウェアのソースコードが数億行レベルに増えると予想されており、ソフトウェア開発、セキュリティ対策・評価技法も非常に高度化することから、「ハッカソンの参加」も含め中長期的に高度人材を発掘・育成する仕組みが必要である。

（４）その他

① サイバー攻撃による被害への対応
ドライバーが関与しないハッキングによる交通事故の賠償責任や被害者への補償など、法的な検討を急ぐことが必要である。

４　物流分野

（１）多層的な防御と対処態勢の整備

① 安全基準等の改訂
国土交通省は、NISC による「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改訂（2018 年 4 月）を受け、「物流分野における情報セキュリティ確保に係る安全ガイドライン」を改訂し、サイバーセキュリティ対策の一層の強化を図ることとしている。今後は、IoT 機器を使用する場合も考慮したセキュリティ対策についての検討を行うべきである。

② 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価
物流事業者は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施する 2020 年東京オリンピック・パラリンピック競技大会のリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図ることが必要である。

（２）情報の共有

① 各種情報共有の促進と「交通 ISAC」の創設
NISC からのニュースレターの共有、J-CSIP による情報共有を引き続き実施するとともに、「交通 ISAC」（仮称）の創設に向けた検討を加速させ、情報共有体制の充実を図るべきである。

（３）人材の育成

① 各種人材育成関連プログラムの活用
NISC が実施する分野横断的演習への参加等により、人材の育成を図るべきである。また、「交通 ISAC」（仮称)においても、人材育成方策を検討することが必要である。

５　医療

（１）多層的な防御と対処態勢の整備

① 医療分野全体としてのセキュリティ対策の推進
医師会以外の医療従事者や私立病院等セキュリティ対策に資金的なリソースを振り分けることが困難な事情がある組織等が存在する点を踏まえ、医療分野全体としてセキュリティ対策を推進することが必要である。

② 保健医療情報のセキュリティ対策の強化
「未来投資戦略 2017」に基づき、患者の保健医療情報を医療関係者が共有し、患者に最適な診療を提供するための全国的なネットワークを 2020 年度から本格稼働させることを目指す中で、データ共有・利活用の利便性向上とセキュリティのバランスをとりながら、ネットワークや医療機関のセキュリティ対策強化について厚生労働省において検討すべきである。その際には、コスト負担のあり方についても留意する。

③ 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価
医療機関等は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施する 2020 年東京オリンピック・パラリンピック競技大会のサイバーセキュリティ対策の強化の一環として、リスク評価に参加することが求められる。

④ 業務やデータの機密性に応じたインフラの設計および運用管理
外部からの侵入からだけではなく、USB などからマルウェアが複数の業務システムに病院院内のネットワークを通じて広く感染するケースも多いため、「パブリックエリア（外来者が利用するエリア）」、「オフィスエリア（一般業務のエリア）」、「セキュリティエリア（機密情報を扱うエリア）」等でネットワークやシステムアクセス権限を区分し、業務

やデータの機密性に応じたインフラの設計および運用管理を実施することが必要である。

⑤ 使用期間が長い医療機器におけるセキュリティ対策

医療機器が 10 年以上使用される事もあり、OS 等の古いバージョンのソフトウェアが利用されているケースも数多く残存している。OS のアップデートや不具合対策のモジュール適用も、本来機能を損なう別の不具合を内包している可能性があり、十分な検証を行ってからでないと適用が難しく、一般の情報(IT)系システムに比べて対策が難しい状況である。これらシステムの脆弱性を十分に把握した上で多層的な防御を実施していくことが必要である。

⑥ ペースメーカー等のセキュリティ対策

ペースメーカーや植込み型除細動器への遠隔操作のリスクを排除すべきである。

⑦ 関係機関間の連携・協調

医療機器の安全性を担う医療機器製造業者、組織としての対策を行う医療機関、脆弱性や攻撃の分析を行うセキュリティ機関、規制やガイドラインを提供する国や自治体等が連携・協調して対応することが必要である。

（２）情報の共有

① 情報共有の更なる促進と関係者の範囲の拡大

医療分野におけるサイバーセキュリティに関する情報の共有・分析の取組が民間の医療関係団体中心に進み始めているが、医療機関の意識や取組状況の差もある中で、医療 CEPTOAR がセプターカウンシルに正式参加することで、重要インフラの他分野の取組を把握しつつ、更なるセキュリティ対策の強化と安全性の向上のための協働活動について検討を進め、結論を得る。その際には、CEPTOAR の構成員の拡充についても、民間の医療関係団体に検討を促すことが重要である。

② 「医療ＩＳＡＣ」の創設

既に「地域包括ケア」の時代に入っており、「遠隔医療」、「オンライン診療」やスマートフォン等から送信されるバイタルデータを活用した「ヘルスケア」の取組も進行中。デバイス数が急増している現状から、「医療ＩＳＡＣ」の創設を急ぐべきである。なお、将来的に介護・健康分野への拡大も検討すべきである。

（３）人材の育成

① 各レイヤの人材に対するセキュリティ教育の底上げ

CISO(最高情報セキュリティ責任者)を始め、実際にセキュリティ対策を実施する人材が不足しており、「各レイヤの人材に対するセキュリティ教育の底上げ」を図ることが必要である。

② IT・OT 双方の人材育成

制御系機器を扱っているため、「IT 系／OT 系双方のスキルを持つ人材」を育てるとともに、サイバー攻撃に対する検知、解析、対処について、サプライチェーン(機器製造者)や分野を横断して連携して対応できる実践的訓練環境の整備が必要である。

（４）その他

① 「マイナンバーカード」、「HPKI」の活用

政府は、紛失時には 365 日 24 時間体制のコールセンターへの連絡で機能停止も可能な「マイナンバーカード」の公的個人認証機能を活用することで、健康保険証などのセキュリティレベルをより向上させる方策を検討すべきである。また、医療事業者が、本人確認することができることで、電子的に書類を作成する際の利便性を大幅に向上させるなどの利点を有する保険医療福祉分野電子証明書（HPKI）を一層活用するべきである。

② 社会保険診療報酬支払基金の防護体制の強化

社会保険診療報酬支払基金は、重要インフラ事業者のように直接「事業を行う者」ではないものの国民生活又は経済活動に多大な影響を及ぼすものであり、サイバー攻撃からの適切なセキュリティ対策が不可欠である。支払基金については、ＮＩＳＣ、厚生労働省など関係省庁が緊密に連携して、迅速なサイバー攻撃からの防護の技術的な体制（緊急時の技術的支援を含む。）を一刻も早く強化すべきである

６　電力

（１）多層的な防御と対処態勢の整備

① 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価

電気事業者等は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施するリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図る必要がある。万が一、サイバー攻撃が制御系にまで及んだ場合を想定し、被害の影響範囲を最小化して、速やかに復旧するための方法等を構築するとともに、被害を想定した訓練の実施に努めていくことが必要である。なお、2020 年東京オリンピック・パラリンピック競技大会では、会場において競技継続に必要な重要負荷のバックアップとして、非常用発電機の配備を予定している。

② 制御系システムのセキュリティ対策の強化

制御系システムへのアクセス制御や入退管理などの対策の継続的かつ確実な実施・運用・改善に努めることが必要である。

③ サイバーレスキュー隊の機能の維持

重要インフラ事業者等がサイバー攻撃の被害を受けた場合に初動対応や被害拡大防止策

策定の支援を行う IPA のサイバーレスキュー隊の機能を継続的に維持することが必要である。

④ サイバーセキュリティ技術・製品の検証
サイバーセキュリティ技術・製品を公的な機関が検証し、重要インフラ事業者等がサイバーセキュリティ技術・製品を活用しやすい環境を構築することが必要である。

⑤ IT 系システムと OT 系システムの相互理解
今後、情報(IT)系システムと制御(OT)系システムの連携とネットワークを活用した高度化・効率化が促進されることも想定されるが、IT 系システムは個人情報やデータの機密性を重視し、OT 系システムでは人的損害や事業継続に対する可用性を重視したシステムとなっており、システムの設計・運用の思想が異なっている。双方が連携したシステムでは、お互いの設計・運用の思想が異なること十分考慮し、「システム全体のリスク分析と事業継続性を踏まえたセキュリティ対策」を実施することが必要である。

⑥ スマートメーターの対応策の検討
今後、普及が予想されるスマートメーターについては、一定の対策が施されているものの、通常の IT 機器と比較すると長寿命であること、使用量が非常に多数に及ぶことから、脆弱性等を悪用され、サイバー攻撃の踏み台とされた場合の対応策を検討する必要がある。

⑦ 内部犯行によるサイバー攻撃への対応
事業者内部・契約外部事業者の犯行によるサイバー攻撃リスクを最小化するための対策強化が必要である。

（２）情報の共有

① 国内外の関係機関との連携
各社の対策（対策事例のベストプラクティスや、社内セキュリティ教育の方法等）の共有や有識者を交えた意見交換の実施に努めていくことが必要である。また、国内外の機関（欧州の EE-ISAC 等）との連携強化を図ることが必要である。

② 現行分野を跨る情報共有の仕組みの検討
我が国の現状（電力会社とガス会社が、それぞれ「電力」と「ガス」の両方を販売。）を踏まえ、例えば「電力＆ガス＆熱供給ＩＳＡＣ」などの創設により、従来の分野を跨る情報共有の仕組みを検討することが求められる。

（３）人材の育成

① 産業サイバーセキュリティセンターの活用
日々高度化するサイバー攻撃の実態を踏まえ、産業サイバーセキュリティセンターの教

育カリキュラムを改善するとともに、同センターにおける人材育成を活用し、圧倒的に不足するセキュリティ人材の育成に継続的に取り組むことが必要である。

② 各種人材育成関連プログラムの活用
重要インフラの情報セキュリティ対策に係る第４次行動計画」や「スマートメーターシステムセキュリティガイドライン」及び「電力制御システムセキュリティガイドライン」に基づき、サイバーセキュリティに係る人材の育成・拡充に努めていくことが必要である。

③ IT・OT 双方の人材育成と実践的訓練環境の整備
技術研究組合制御システムセキュリティセンター（CSSC：Control System Security Center）によるサイバーセキュリティ演習、IPA の産業サイバーセキュリティセンター(ICSCoE)による IT 系と OT 系のセキュリティ対処および対策立案能力を向上させるトレーニングが実施されているが、今後、IoT の進展にあわせ、IT 系／OT 系双方のスキルを持つ人材を育てるとともに、サイバー攻撃に対する検知、解析、対処について、分野を横断して連携して対応できる実践的訓練環境の整備が必要である。

（４）その他

① 産業毎のサイバーセキュリティ対策の強化
IoT の進展によるサイバー攻撃の起点の拡大等を踏まえ、産業毎（Industry by Industry）にサプライチェーン全体のサイバーセキュリティ対策強化に取り組むことが必要である。

７　ガス

（１）多層的な防御と対処態勢の整備

① 保安規定に基づくセキュリティ対策
都市ガスの製造・供給設備の制御システムの特徴や事業者の多様性を踏まえつつ、都市ガス供給における安全をより確実なものとすることが重要。そのため、製造・供給に係る制御システムのサイバーセキュリティ対策をガス事業法に基づく保安規程の要求事項の一つとして位置付け、対策の確実な実施を求める方向で検討を行うことが必要である。

② 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価
ガス事業者は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施するリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図る必要がある。

③ サイバーレスキュー隊の機能の維持
重要インフラ事業者等がサイバー攻撃の被害を受けた場合に初動対応や被害拡大防止策策定の支援を行う IPA のサイバーレスキュー隊の機能を継続的に維持することが必要で

ある。

④ サイバーセキュリティ技術・製品の検証
サイバーセキュリティ技術・製品を公的な機関が検証し、重要インフラ事業者等がサイバーセキュリティ技術・製品を活用しやすい環境を構築することが必要である。

⑤ IT 系システムと OT 系システムの相互理解
今後、情報(IT)系システムと制御(OT)系システムの連携とネットワークを活用した高度化・効率化が促進されることも想定されるが、IT 系システムは個人情報やデータの機密性を重視し、OT 系システムでは人的損害や事業継続に対する可用性を重視したシステムとなっており、システムの設計・運用の思想が異なっている。双方が連携したシステムでは、お互いの設計・運用の思想が異なること十分考慮し、「システム全体のリスク分析と事業継続性を踏まえたセキュリティ対策」を実施することが必要である。

⑥ 内部犯行によるサイバー攻撃への対応
事業者内部・契約外部事業者の犯行によるサイバー攻撃リスクを最小化するための対策強化が必要である。

（２）情報の共有

① 現行分野を跨る情報共有の仕組みの検討
我が国の現状（電力会社とガス会社が、それぞれ「電力」と「ガス」の両方を販売。）を踏まえ、例えば「電力＆ガス＆熱供給ＩＳＡＣ」などの創設により、従来の分野を跨る情報共有の仕組みを検討することが求められる。

② 各種情報共有の促進
ガス分野そのものにおいても、日本ガス協会サイバー情報メーリングリストの参加組織の拡充を図り、情報共有を行う体制整備を進めることが重要である。

（３）人材の育成

① 産業サイバーセキュリティセンターの活用
日々高度化するサイバー攻撃の実態を踏まえ、産業サイバーセキュリティセンターの教育カリキュラムを改善するとともに、同センターにおける人材育成を活用し、圧倒的に不足するセキュリティ人材の育成に継続的に取り組むことが必要である。

② 各種人材育成関連プログラムの活用
「重要インフラの情報セキュリティ対策に係る第４次行動計画」や「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」に基づき、サイバーセキュリティに係る人材の育成・拡充に努めていくことが必要である。

③ IT・OT 双方の人材育成と実践的訓練環境の整備
技術研究組合制御システムセキュリティセンター（CSSC：Control System Security Center）によるサイバーセキュリティ演習、IPA の産業サイバーセキュリティセンター(ICSCoE)による IT 系と OT 系のセキュリティ対処および対策立案能力を向上させるトレーニングが実施されているが、今後、IoT の進展にあわせ、IT 系／OT 系双方のスキルを持つ人材を育てるとともに、サイバー攻撃に対する検知、解析、対処について、分野を横断して連携して対応できる実践的訓練環境の整備が必要である。

（４）その他

① 産業毎のサイバーセキュリティ対策の強化
IoT の進展によるサイバー攻撃の起点の拡大等を踏まえ、産業毎（Industry by Industry）にサプライチェーン全体のサイバーセキュリティ対策強化に取り組むことが必要である。

８　水道

（１）多層的な防御と対処態勢の整備

① 安全基準等の改訂
厚生労働省は、NISC による「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」の改訂（2018 年 4 月）を受け、「水道分野における情報セキュリティガイドライン」第３版を改訂し、サイバーセキュリティ対策の一層の強化を図ることとしている。

② 使用期間が長い水道制御システムにおけるセキュリティ対策
水道制御システムの場合 10 年以上使用される事もあり、OS 等の古いバージョンのソフトウェアが利用されているケースも数多く残存している。OS のアップデートや不具合対策のモジュール適用も、本来機能を損なう別の不具合を内包している可能性があり、十分な検証を行ってからでないと適用が難しく、一般の情報(IT)系システムに比べて対策が難しい状況である。これらシステムの特性を十分に把握した上で多層的な防御を実施していくことが必要である。

③ 2020 年東京オリンピック・パラリンピック競技大会に向けたリスク評価
水道事業者は、2020 年東京オリンピック・パラリンピック競技大会に向け、NISC の実施する 2020 年東京オリンピック・パラリンピック競技大会のリスク評価に引き続き参加し、サイバーセキュリティ対策の強化を図る。

（２）情報の共有

① 現行分野を跨る情報共有の仕組みの検討

取水から排水に至る水道の全体を考えた場合、上水道と下水道は密接に連携していることが明らかである。このため、上下水道に跨る「上水道＆下水道ＩＳＡＣ」の創設を検討することが必要である。

（３）人材の育成

① IT・OT 双方の人材育成と実践的訓練環境の整備

制御系機器を扱っているため、IT 系／OT 系双方のスキルを持つ人材を育てるとともに、サイバー攻撃に対する検知、解析、対処について、サプライチェーン(機器製造者)や分野を横断して連携して対応できる実践的訓練環境の整備が必要である。

９　石油

（１）多層的な防御と対処態勢の整備

① サイバーレスキュー隊（IPA）

重要インフラ事業者等がサイバー攻撃の被害を受けた場合に初動対応や被害拡大防止策策定の支援を行うIPAのサイバーレスキュー隊の機能を継続的に維持することが必要である。

② サイバーセキュリティ技術・製品の検証

サイバーセキュリティ技術・製品を公的な機関が検証し、重要インフラ事業者等がサイバーセキュリティ技術・製品の活用を検討しやすい環境を構築することが必要である。

（２）情報の共有

① 各種情報共有の促進

NISC からのニュースレターの共有、サイバー情報共有イニシアチブ（J-CSIP）による情報共有を引き続き実施し、検知したサイバー攻撃情報や対策情報の共有による同種被害の最小化、予兆情報共有に基づいた早期警戒による実被害の抑止を図る必要がある。

（３）人材の育成

① 産業サイバーセキュリティセンター（IPA）

日々高度化するサイバー攻撃の実態を踏まえ、産業サイバーセキュリティセンターの教育カリキュラムを改善するとともに、同センターにおける人材育成を活用し、圧倒的に不足するセキュリティ人材の育成に継続的に取り組むことが必要である。

② ガイドラインに基づく人材育成計画の実施
「重要インフラの情報セキュリティ対策に係る第４次行動計画」や「石油分野における情報セキュリティ確保に係る安全ガイドライン」に基づき、サイバーセキュリティに係る人材の確保等に関する計画策定と実施に努めていくことが必要である。

（４）サプライチェーン対策

① サプライチェーン全体のサイバーセキュリティ対策強化
IoT の進展によるサイバー攻撃の起点の拡大等を踏まえ、産業毎（Industry by Industry）にサプライチェーンのサイバーセキュリティ対策強化に取り組むことが必要である。

10　化学

（１）多層的な防御と対処態勢の整備

① サイバーレスキュー隊（IPA）
重要インフラ事業者等がサイバー攻撃の被害を受けた場合に初動対応や被害拡大防止策策定の支援を行う IPA のサイバーレスキュー隊の機能を継続的に維持することが必要である。

② サイバーセキュリティ技術・製品の検証
サイバーセキュリティ技術・製品を公的な機関が検証し、重要インフラ事業者等がサイバーセキュリティ技術・製品を活用しやすい環境を構築することが必要である。

（２）情報の共有

① 各種情報共有の促進
NISC からのニュースレターの共有、サイバー情報共有イニシアチブ（J-CSIP）による情報共有を引き続き実施し、検知したサイバー攻撃情報や対策情報の共有による同種被害の最小化、予兆情報共有に基づいた早期警戒による実被害の抑止を図る必要がある。

（３）人材の育成

① 産業サイバーセキュリティセンター（IPA）
日々高度化するサイバー攻撃の実態を踏まえ、産業サイバーセキュリティセンターの教育カリキュラムを改善するとともに、同センターにおける人材育成を活用し、圧倒的に不足するセキュリティ人材の育成に継続的に取り組むことが必要である。

② ガイドラインに基づく人材育成計画の実施

「重要インフラの情報セキュリティ対策に係る第４次行動計画」や「石油化学分野　における情報セキュリティ確保に係る安全基準」に基づき、サイバーセキュリティに係る人材の育成・拡充等に関する実施に努めていくことが必要である。

（４）サプライチェーン対策

① サプライチェーン全体のサイバーセキュリティ対策強化

IoT の進展によるサイバー攻撃の起点の拡大等を踏まえ、産業毎（Industry by Industry）にサプライチェーン全体のサイバーセキュリティ対策強化に取り組むことが必要である。

11　金融

（１）多層的な防御と対処態勢の整備

① 中小金融機関のサイバーセキュリティ対策の底上げ

信金・信組等の中小金融機関においては、「サイバーセキュリティに着眼したリスク評価の実施」や「インシデント発生を想定したコンティンジェンシープランの策定」といったサイバーセキュリティ対策の基礎となる部分が未だ不十分であることから、中小金融機関の底上げを図る必要がある。

すでに、取組を進めているものは以下の通り。

- 中小金融機関を中心に実態把握を継続して実施するとともに、協同組織中央機関・共同センター等との対話を実施
- 2017 年 10 月、中小金融機関の参加を拡充して実施した「金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅱ）」について、業界全体に対しても演習結果をフィードバックし、インシデント対応能力の向上を促進

② 大規模な金融機関のサイバーセキュリティ対応能力の更なる引上げ

大規模な金融機関については、仮にサイバー攻撃を受けた場合にはその影響が金融システム全体に及ぶおそれがあることから、そのサイバーセキュリティ対応能力をさらにもう一段引き上げるため、「脅威ベースのペネトレーションテスト（テスト対象企業ごとに脅威の分析を行い、個別にカスタマイズしたシナリオに基づく実践的な侵入テスト）」等、より高度な評価手法の活用を促進すべきである。

（２）情報の共有

① 中小金融機関の情報共有の促進

個別金融機関のみでサイバー攻撃に対応することには限界がある。そのため、金融 ISAC 等の情報共有機関等を活用して情報共有・分析を行う「共助」の観点が重要である。

特に、信金・信組等の中小金融機関が自社だけでサイバーセキュリティ対策を行うには、人手も費用も時間もかかる。こうした先は人材の数や質、予算など潤沢なリソースを有しておらず、金融 ISAC の活用が有用と考えられるが、信金・信組等の中小金融機関の金融 ISAC への加盟が進んでいないため、金融 ISAC への加盟も含め、金融 ISAC を通じた更なる情報共有の一層の推進を金融機関に促すことが必要である。

（３）人材の育成

① 中小金融機関の経営者・職員の各種演習等への参加の促進
地域に根付いた中小金融機関（地銀・信用金庫・ＪＡなど）の経営者・職員の各種演習参加を促進し、サイバーセキュリティ対策についての意識向上を図るべきである。

（４）その他

① 仮想通貨交換業者における自主規制機能の確立
2018 年 1 月、コインチェック㈱（登録申請中のみなし業者）が不正アクセスを受け、当社が管理する仮想通貨（ＮＥＭ）580 億円相当が外部に流出したことを受け、当社に対し業務改善命令の発出及び立入検査を実施した。
また、全ての仮想通貨交換業者に対しシステムリスク管理に関する報告を求め、その結果を踏まえ、複数の業者に立入検査を実施した。
さらに、仮想通貨交換業者における自主的なサイバーセキュリティの強化に向け、早期に統一の自主規制団体が設立され、実効性ある自主規制機能が確立されるよう促すことが必要である。

12　クレジット

（１）多層的な防御と対処態勢の整備

① サイバーレスキュー隊（IPA）
重要インフラ事業者等がサイバー攻撃の被害を受けた場合に初動対応や被害拡大防止策策定の支援を行う IPA のサイバーレスキュー隊の機能を継続的に維持することが必要である。

② サイバーセキュリティ技術・製品の検証
サイバーセキュリティ技術・製品を公的な機関が検証し、重要インフラ事業者等がサイバーセキュリティ技術・製品を活用しやすい環境を構築することが必要である。

（２）情報の共有

① 金融 ISAC スキームの活用

各社対策（対策事例のベストプラクティスや、社内セキュリティ教育の方法等）の共有や有識者を交えた意見交換の実施に努めていく。また、国内外の機関（米国の FS-ISAC 等）との連携強化を図るべきである。

（３）その他

① マイナンバー機能の活用

紛失時には 365 日 24 時間体制のコールセンターへの連絡で機能停止も可能な「マイナンバーカード」の公的個人認証機能を活用することで、キャッシュカードやクレジットカードのセキュリティレベルをより向上させる方策を検討すべきである。

13　情報通信

（１）多層的な防御と対処態勢の整備

① IoT 機器の脆弱性対策実装のための体制整備

今後は、IoT 活用の進展とともにネットワークを介して様々な IoT 機器が接続されたサービスが提供されていくため、情報通信インフラおよび IoT 機器も含めたサービストータルでのセキュリティ対策の強化が必要となる。また、IoT セキュリティ対策は、IoT 機器を利用したサービス全体としてのセキュリティを考えれば、IoT 機器製造事業者、流通事業者、保守ベンダ、ISP 及び利用者といった各主体が補完し合いながら対応していくことが求められる。このため、これらの関係主体と相互に連携し、ネットワーク全体のセキュリティを確保するため、情報共有のあり方を含め、IoT 機器に対する脆弱性対策を実施する体制整備を進める必要がある。

② IoT 機器のセキュリティ検査の仕組み作り

IoT 機器が比較的長期にわたり運用される傾向がある中で、その運用期間中において継続的に安全安心な状態を維持することができるよう、機器の脆弱性に係る接続試験を行うテストベッドの構築を含むセキュリティ検査の仕組み作りを進める必要がある。

③ フリーWiFi 利用の際の注意喚起

外国人観光客への利便性向上を目的に、全国各地で整備が進められているフリーWiFi について、十分なセキュリティ対策が講じられておらず、ID 及びパスワードが入力不要なものまたは非常に簡便なまま放置されているものや通信が暗号化されていないものが多数見受けられることから、セキュリティ対策を確認した上で利用するなどの注意喚起を発出することが必要である。

（２）情報の共有

① ICT-ISAC を核とする情報共有機能の更なる強化

今後は、ネットワークを介しての様々な分野の連携が進むため、各分野において情報共有を行う体制（ISAC）の立ち上げの加速と、分野を跨る情報共有の仕組みが必要となる。そのため、ICT-ISAC を核として、対策を見据えた情報共有を効果的に行う取組を強化するとともに、このような活動を通じて、他分野に対しても情報共有の模範となるような先行的な情報共有モデルを示しつつ、他分野の ISAC との連携を進め、我が国全体の情報共有機能強化を図る必要がある。

（３）人材の育成

① IT・OT 双方の人材育成の推進

今後、IoT の進展にあわせ、IT(Information Technology)系のセキュリティ技術者に加え、OT(Operational Technology)系のセキュリティ技術者の育成を進めるとともに、IT 系 OT 系を跨るサイバー攻撃に対する検知・解析、対処を連携して進めることができるような育成訓練の仕組みが必要となる。

② 各種人材育成関連プログラムの維持・強化

我が国のセキュリティ人材は質的にも量的にも圧倒的に不足しており、セキュリティ人材の育成は喫緊の課題であることから、引き続き、政府において、関係機関・企業等と十分に連携しながら、セキュリティ人材の育成の取組が必要となる。そのため、新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツの開発に努めつつ、実践的サイバー防御演習「CYDER」の充実、「サイバーコロッセオ」の更なる内容の拡充、「SecHack365」による若手セキュリティイノベーターの育成等の継続的な実施が必要である。

（４）研究開発の推進

① 研究開発の成果普及や社会実装の推進

サイバー空間における攻撃の態様は常に変化しており、これに対応するには、政府が支援する産学官連携による研究開発の成果を即座に反映した最新のサイバーセキュリティ対策を実施していくことが有効である。そのため、引き続き、NICT を中心に、サイバーセキュリティに関する研究開発（例えば、匿名性を確保したデータ利用技術等）に取り組むとともに、研究開発成果の普及や社会実装を推進していく必要がある。

② スマートシティの技術開発・国際標準化の推進

スマートシティにおいて、データ連携・解析などを行うプラットフォームのセキュリティ対策はデータの真正性を確保し、かつ、スマートシティの機能をサイバー攻撃から防御するためにも極めて重要である。そのため、スマートシティのプラットフォームに係るセキュリティ要件の具体化や所要の技術開発を推進するとともに、その成果を国際的な標準化プロセスに提案する等の取組を一体的に進めていく必要がある。

③ 抗堪性・秘匿性の高い衛星通信技術の開発

世界的な人工衛星等の産業利用に向けた活動の活発化による衛星利用の需要拡大に対応するため、また、衛星通信に対する脅威となりつつあるサイバー攻撃や物理的な攻撃から衛星通信ネットワークを防護し、安全な衛星通信ネットワークの構築を可能とするため、高秘匿な衛星通信に資する技術の研究開発などに取り組む必要がある。

④ ハードウェア脆弱性の検知技術の開発

集積回路の設計工程において、ハードウェア脆弱性が存在する可能性が指摘されており、総務省では、戦略的情報通信研究開発推進事業（SCOPE）により、平成 29 年度から、ハードウェア脆弱性の検知技術の研究開発が行われている。今後、IoT 端末はさらなる増加が見込まれており、引き続き、ハードウェアに組み込まれる恐れのあるハードウェア脆弱性を検出する技術の研究開発について、ビッグデータや AI を活用しつつ推進していく必要がある。

（５）その他

① 通信の秘密やプライバシーの確保の関係についての検討

「迅速で実効的なサイバー攻撃対策」のためには、「通信の秘密やプライバシーの確保」との関係について、法的整理を行う必要がある。

② 電波妨害への留意

「電波妨害」についても十分に留意した対策を検討すべきである。

14　政府・行政サービス（その１　政府）

（１）多層的な防御と対処態勢の整備

① 政府全体の対処態勢の整備

特に国民生活および経済活動に及ぼす影響が高い行政機関においては、NISC が中心となって、関係府省庁と連携しつつ、セキュリティ対策の向上を行う必要がある。具体的には、インシデントに対応する体制の強化だけでなく、不審な通信を検知した際、速やかに独立行政法人などの専門機関と連携して、各府省庁や関連機関に迅速に情報提供するための対処態勢基盤が必要である。

② 事前対応型防護への移行

人工知能等を活用し、未知のマルウェアを検知可能な技術を確立し、エンドポイント（端末）の管理・監視技術と組み合わせた事前対応型防護方式の不正プログラム対策を開発し、事前対応型の防護方策を確立することが必要である。

③ 資産管理の自動化

高度化・複雑化する情報システムに生じる多様な脆弱性に機動的に対応するため、情報資産及びその脆弱性の管理を自動化すべきである。

④ 保有情報の流出時のフェールセーフの確保
万一、不正アクセス等により情報が漏えいした場合でも、自動的に暗号化を行うこと等により容易に解読ができない仕組みを導入することが必要である。

⑤ 政府全体の機能強化
政府全体の防護能力を高めるため、NISC が中心となって、関係府省庁と連携しつつ、セキュリティ対策の向上を行う必要がある。また、我が国の安全保障上の脅威が高いとされる国で製造された機器など、深刻な悪影響を及ぼす可能性のある技術的課題に関する研究・検証体制の構築など取り得る体制を検討し、将来的にはサイバーセキュリティを担当する官庁の設置または NISC の一層の機能強化を図るなど、政府全体の機能強化について検討すべきである。以上の対策を通じて、全府省庁の情報システム（端末となる公用 PC を含む）のセキュリティ対策に万全を期すべきである。

（２）情報の共有

① 対策情報の活用による機能強化方策の導入
資産管理の自動化、事前対応型の防護方策の導入と並行して、対策情報等の自動的な生成、供給、実装などを含めた機能強化方策の導入を検討すべきである。

（３）人材の育成

① 政府全体の IT・セキュリティ人材の育成・確保
政府全体の IT/セキュリティ人材の育成・確保を進めるに当たり、各府省庁において、計画的に当該人材の育成・確保及びキャリアパスの設定を積極的に行うべきである。特に、NISC 等における高度なセキュリティ人材の育成・確保のため、インシデント対応のための CSIRT 機能及び NISC の CYMAT の維持・強化も図るべきである。

② 一般職員の情報リテラシー能力の向上
職員を対象とした IT およびセキュリティ教育の実施とインシデント発生時の報告手順の徹底などによる対処能力の向上を図るべきである。

（４）その他

① 公用携帯の貸与対象の拡大
アプリの取り込み制限など、十分なセキュリティ対策を講じた「公用携帯」につき、少なくとも「局長級以上全員」など、配布対象者の拡大を検討すべきである。

14　政府・行政サービス（その２　地方公共団体）

（１）多層的な防御と対処態勢の整備

① 業務効率化との両立

情報セキュリティを強化することにより、メールの添付ファイル取り込みや重要なデータベースへのアクセス等情報の取扱い時に職員の操作が増え手間がかかるようになったとの指摘がされることから、セキュリティレベルを維持しつつも操作性の向上を図ることのできる新しい技術の適用に向けた調査研究が求められる。

② 自治体クラウドの推進を踏まえた対策

今後、自治体クラウドの進展とともに、各地方公共団体の情報システムやネットワークの構成について変容することが想定されるので、これらを踏まえたセキュリティ対策を常時検討することが必要である。

（２）情報の共有

① 各種情報共有の促進

NISC からのニュースレターの共有などによる情報共有を引き続き実施し、検知したサイバー攻撃情報や対策情報の共有による同種被害の最小化、予兆情報共有に基づいた早期警戒による実被害の抑止を図る必要がある。

（３）人材の育成

① 情報セキュリティの啓発や訓練

標的型メールへの対応や USB による情報持ち出し等職員のセキュリティ・リテラシーが求められる事案も多いことから、今後、職員に向けた情報セキュリティの啓発や訓練が継続して必要である。

15　安全保障

（１） 多層的な防御と対処態勢の整備

① サイバー防衛隊等の体制拡充

高度化・巧妙化するサイバー攻撃に対応すべく、サイバー防衛隊等の拡充を加速するとともに、組織の在り方を検討すべきである。また、サイバー反撃能力のあり方について検討すべきである。

② 防衛調達における情報セキュリティの強化
重要度の高い企業、機関、設備、情報をそのサプライチェーン全体を含めてサイバー攻撃から守る為、また日本 IT 産業の国際競争力を維持・強化する為、日本でも米国の情報保全ガイドライン（NIST SP-800）と同様の我が国としてのルールを整備し、国際相互認証を獲得すべきである。

③ サイバー政策推進体制の強化
防衛省・自衛隊におけるサイバー政策担当部局の体制を強化すべきである。

④ サイバー関連予算の拡充
防衛省・自衛隊におけるサイバー関連事業を拡充すべきである。

⑤ 諸外国等との連携強化
米国や友好国、国際機関等の国際社会との連携を強化し、サイバー空間の安定的かつ効果的な利用を促進すべきである。

⑥ 情報収集・分析機能の強化と事態対処態勢の整備
サイバー空間における情報収集・分析能力の抜本的強化を図り、日本の情報収集能力全体を補完し、インテリジェンス強化を図るとともに、平時における周辺国等におけるサイバー状況把握及びその分析を強化し、例えば、他国・組織の戦力やサイバー攻撃能力、手法等の研究を含め、有事の発生に対して万全の体制で臨み被害を最小限に抑制することに努めることが必要である。

（２） 情報の共有

① 関係機関・民間企業との連携強化
サイバー攻撃に迅速かつ効果的に対応するためには、関係機関・企業との連携が不可欠。このため、NISC をはじめとする政府機関や民間企業と、官民連携の枠組みも活用しつつ緊密に連携し、委託先における情報セキュリティ対策（オフラインのシステムの対策の徹底などを含む。）を検討し、サイバーセキュリティに関する情報共有や意思疎通等を促進すべきである。

（３）人材の育成

① 人材の確保・維持・活用
サイバーに関する部内外の教育を拡充すべきである。また、サイバーに関する高度な専門知識を有する外部の人材を活用するため、官民人事交流制度や役務契約等の制度の活用を検討すべきである。さらに、サイバー人材のインセンティブ向上のための施策を検討すべきである。

（４）その他

① サイバー技術の強化

自衛隊施設や移動系システムを含め、防衛省・自衛隊に対するサイバー攻撃に適切に対処するため、人工知能の活用、暗号技術、電磁パルス攻撃対策等の研究開発を推進すべきである。

【参考１】

用語解説

	用　語	解　説
A	Apache Struts	Webアプリケーションを構築する際に必要となる諸機能を提供するオープンソースのフレームワーク。
	APEC	Asia-Pacific Economic Cooperationの略（エイペック）。アジア太平洋地域の21の国と地域が参加する枠組み。
B	BCP	Business Continuity Planの略。緊急事態においても重要な業務が中断しないよう、又は中断しても可能な限り短時間で再開できるよう、事業の継続に主眼を置いた計画。BCPのうち情報（通信）システムについて記載を詳細化したものがIT-BCP（ICT-BCP）である。
	BlackHat	米国における世界最大級の情報セキュリティカンファレンス。
C	Can通信	Contorlled Area Networkの略。自動車での使用を前提に開発された通信手続き。国際規格（ISO 11898）などで標準化されている。
	CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略（セプター）。重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。2005年以降順次構築が進められ、2017年３月末現在、13分野で18CEPTOARが活動。
	CERT/CC	Computer Emergency Response Team/Coordination Centerの略（サートシーシー）。サイバー攻撃情報やシステムの脆弱性関連情報を収集・分析し、関係機関に情報提供等を行っている非営利団体の一般的な名称。複数の国で設立されており、日本にはJPCERT/CCが設置されている。
	CIO	Chief Information Officerの略。最高情報責任者。企業や政府機関のIT活用を俯瞰し、組織及びその組織が属するグループ全体の情報システムやIT部門の最適化を図るとともに、経営の変革を主導的に推進する責任者のこと。
	CISO	Chief Information Security Officerの略。最高情報セキュリティ責任者。企業や行政機関等において情報システムやネットワークの情報セキュリティ、機密情報や個人情報の管理等を統括する責任者のこと。なお、「政府CISO」は内閣サイバーセキュリティセンター長である。
	CISSP	Certified Information Systems Security Professionalの略。非営利組織である(ISC)^2 (International Information Systems Security Certification Consortium：アイエスシー・スクエア)が認定を行っている国際的に認められた情報セキュリティ・プロフェッショナル認証資格のこと。
	CSIRT	Computer Security Incident Response Teamの略（シーサート）。企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと。
	CSSC	Control System Security Centerの略。技術研究組合制御システムセキュリティセンター。重要インフラの制御システムのセキュリティを確保するため、研究開発、国際標準化活動、認証、人材育成、普及啓発、各システムのセキュリティ検証等を担う。2012年３月設立。
	CYDER	Cyber Defense Exercise with Recurrenceの略。NICTナショナルサイバートレーニングセンターが実施する、実践的サイバー防御演習。
	CYMAT	CYber incident Mobile Assistance Teamの略（サイマット）。我が国の機関等において大規模なサイバー攻撃等により政府として一体となって迅速・的確に対応すべき事態等が発生した際に、機関の壁を越えて連携し、被害拡大防止等について機動的な支援を行うため、2012年６月に内閣官房に設置した体制のこと。
D	DDoS攻撃	Distributed Denial of Serviceの略。分散型サービス不能攻撃。大量のコンピュータが一斉に特定のサーバにデータを送出し、通信路やサーバの処理能力をあふれさせて機能を停止させてしまうサイバー攻撃。大規模な攻撃では、遠隔操作される等により数万台以上のコンピュータが攻撃に用いられているケースもある。
	DII	Defense Information Infrastructureの略。防衛省の基盤的共通通信ネットワーク。
	DNS	Domain Name Systemの略。ドメイン名とIPアドレスを対応付けて管理するシステム。
E	eラーニング	electronic learningの略。情報通信技術を用いた教育、学習のこと。
	EC	Electronic Commerce（電子商取引）の略。商品やサービスをインターネット上のWebサイトで販売すること。
	EE-ISAC	The European Energy - Information Sharing and Analysis Centreの略。欧州電力ISAC。

F	FedRAMP	Federal Risk and Authorization Management Programの略。米国におけるクラウドサービス調達のためのセキュリティ基準。
	FS-ISAC	Financial Services - Information Sharing and Analysis Centerの略。米国金融ISAC。
G	GSOC	Government Security Operation Coordination teamの略（ジーソック）。政府機関情報セキュリティ横断監視・即応調整チーム。政府機関に設置したセンサー（GSOCセンサー）を通じた、政府横断的な監視、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を行うためのGSOCシステムを運用する体制のこと。内閣官房内閣サイバーセキュリティセンターにおいて、2008年４月から運用開始。
I	ICPO	International Criminal Police Organizationの略（インターポール）。国際刑事警察機構。
	ICS-CERT	Industrial Control System Computer Emergency Response Teamの略。米国国土安全保障省傘下の機関。制御系システムのサイバーインシデントについての対応・分析等を行っている。
	ICSCoE	Industrial Cyber Security Center of Excellenceの略。産業サイバーセキュリティセンター。(独)情報処理推進機構(IPA)に設置されている、サイバーセキュリティ人材育成拠点。
	ICT	Information and Communications Technologyの略。情報通信技術のこと。
	IoT	Internet of Thingsの略。あらゆる物がインターネットを通じて繋がることによって実現する新たなサービス、ビジネスモデル、又はそれを可能とする要素技術の総称。従来のパソコン、サーバ、携帯電話、スマートフォンのほか、ICタグ、ユビキタス、組込システム、各種センサーや送受信装置等が相互に情報をやり取りできるようになり、新たなネットワーク社会が実現すると期待されている。
	IoT推進コンソーシアム	IoT推進に関する技術の開発・実証や新たなビジネスモデルの創出を推進するための体制を構築することを目的として、2015年10月に設立された産官学が参画・連携する組織。
	IPA	Information-technology Promotion Agencyの略。独立行政法人情報処理推進機構。ソフトウェアの安全性・信頼性向上対策、総合的なIT人材育成事業（スキル標準、情報処理技術者試験等）とともに、情報セキュリティ対策の取組として、コンピュータウイルスや不正アクセスに関する情報の届出受付、国民や企業等への注意喚起や情報提供等を実施している独立行政法人。
	ISAC	Information Sharing and Analysis Centerの略。サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報はISACに参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。
	ISMS	Information Security Management Systemの略。情報セキュリティマネジメントシステム。
	ISO	International Organization for Standardizationの略。電気及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）における国際標準の策定を行う国際標準化機関。
	ISP	Internet Service Providerの略。インターネット接続事業者。
J	JC3	Japan Cybercrime Control Centerの略。一般財団法人日本サイバー犯罪対策センター。産学官連携によるサイバー犯罪等への対処のため、日本版NCFTAとして設立された。
	J-CSIP	Initiative for Cyber Security Information sharing Partnership of Japanの略。サイバー情報共有イニシアティブ。IPAを情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取組。
	JPCERT/CC	Japan Computer Emergency Response Team/Coordination Centerの略。我が国において各国関係機関と連携して、サイバー攻撃情報やシステムの脆弱性関連情報等を収集・分析し、関係機関に情報提供するとともに、サイバー攻撃発生時には、関係者間の連絡調整や、攻撃の脅威分析、対策の検討に関する支援活動等を実施している機関。1996年10月に「コンピュータ緊急対応センター」として発足。
L	LGWAN	Local Government Wide Area Networkの略。総合行政ネットワーク。地方公共団体の組織内ネットワークを相互に接続する行政専用ネットワークであり、安全確実な電子文書交換、電子メール、情報共有及び多様な業務支援システムの共同利用を可能とする電子自治体の基盤。
N	NICT	National Institute of Information and Communications Technologyの略。国立研究開発法人情報通信研究機構。情報通信技術分野の研究開発を実施するとともに、民間や大学が実施する情報通信分野の研究開発の支援の実施等を行う独立行政法人。
	NISC	National center of Incident readiness and Strategy for Cybersecurityの略。内閣サイバーセキュリティセンター。サイバーセキュリティ戦略本部の事務の処理を行い、我が国におけるサイバーセキュリティの司令塔機能を担う組織として、2015年１月９日、内閣官房情報セキュリティセンター（National Information Security Center）を改組し、内閣官房に設置された。センター長には、内閣官房副長官補（事態対処・危機管理担当）を充てている。
	NIST	National Institute of Standards and Technologyの略。アメリカ国立標準技術研究所。
O	OECD	Organization for Economic Co-operation and Developmentの略。経済協力開発機構。
	OS	Operating Systemの略。多くのアプリケーションソフトが共通して利用する基本的な機能を提供し、コンピュータシステムを管理する基本ソフトウェア。

	OT	Operational Technologyの略。センサーやアクチュエータなどのフィールド機器、コントローラ、監視・制御用に用いるサーバやクライアントPCなどをネットワークで接続した機器群をさす。
P	PDCAサイクル	Plan-Do-Check-Act cycle。事業活動における生産管理や品質管理などの管理業務を円滑に進める手法の一つ。Plan（計画）→Do（実行）→Check（評価）→Act（改善）の４段階を繰り返すことによって、業務を継続的に改善する。
S	SIG	Special Interest Groupの略。類似の産業分野同士が集まったグループ。
	Stuxnet	Microsoft Windowsで動作するマルウェア。インターネットから隔離されたシステムにも、USBストレージ経由で感染する特徴を持つマルウェアとして有名となった。
	Wannacry	Microsoft Windowsを標的としたランサムウェア。2017年５月に世界的被害が発生した。
	Winny	Microsoft Windowsで動作するファイル共有ソフト。匿名性の高いファイル共有が特徴。著作権法違反のファイル交換や、Winny経由でのマルウェア拡散などが問題となった。
あ	アクセス制御	情報等へのアクセスを許可する者を制限等によりコントロールすること。
い	インシデント	中断・阻害、損失、緊急事態又は危機になり得る又はそれらを引き起こし得る状況のこと（ISO22300）。IT分野においては、システム運用やセキュリティ管理等における保安上の脅威となる現象や事案を指すことが多い。
	インシデント・ハンドリング	インシデント発生時から解決までの一連の処理のこと。
う	ウイルス	コンピュータウイルスのこと。マルウェアの一種であり、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、①自己伝染機能、②潜伏機能、③発病機能のうち、一つ以上の機能を有するもの。
か	可用性	情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできること（Availability）。
	仮想通貨	インターネット上でやりとりされ、通貨のような機能を持つ電子データ。有名な仮想通貨として、例えば、ビットコイン（Bitcoin）などがある。
	完全性	情報に関して破壊、改ざん又は消去されていないこと（Integrity）。
き	機密性	情報に関して正当な権限を持った者だけが、情報にアクセスできること（Confidentiality）。
く	クラウド	インターネット等のブロードバンド回線を経由して、データセンタに蓄積されたコンピュータ資源を役務（サービス）として、第三者（利用者）に対して遠隔地から提供するもの。なお、利用者は役務として提供されるコンピュータ資源がいずれの場所に存在しているか認知できない場合がある。
こ	コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ定めたもの。
さ	サイバーセキュリティ基本法	サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、戦略の策定その他当該施策の基本となる事項等を定めた法律。2014年11月12日公布・一部施行、2015年１月９日完全施行。
	サイバーセキュリティ戦略	2015年９月４日、閣議決定。我が国のサイバーセキュリティ政策に関する国家戦略であり、2020年代初頭までの将来を見据えつつ、今後３年程度の基本的な施策の方向性を示したもの。2015年１月にサイバーセキュリティ基本法が全面施行されたことに伴い、新たな法的枠組みに基づき策定された。
	サイバーセキュリティ戦略本部	2015年１月９日、サイバーセキュリティ基本法に基づき内閣に設置された。我が国における司令塔として、サイバーセキュリティ戦略の案の作成及び実施の推進、国の行政機関等における対策の実施状況に関する監査、重大事象に対する原因究明のための調査等を事務としてつかさどる。本部長は、内閣官房長官。
	サイバーレスキュー隊	(独)情報処理推進機構(IPA)が設置する標的型サイバー攻撃対策の組織。相談を受けた組織の被害低減と攻撃の連鎖の遮断を支援する。
	サプライチェーン	取引先との間の受発注、資材の調達から在庫管理、製品の配達まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。
	産業サイバーセキュリティセンター	ICSCoE（Industrial Cyber Security Center of Excellence）を参照。
し	シェアリングエコノミー	個人が所有する遊休資産（物、場所のほか、スキルのような無形のものも含む）を他の個人と共有して利用する社会的な仕組み。ソーシャルメディアを活用して貸出しを仲介するサービスを中核とする。

	重要インフラ サービス	重要インフラ事業者等が提供するサービス及びそのサービスを利用するために必要な一連の手続のうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野ごとに定めるもの。
	重要インフラ サービス障害	重要インフラの情報セキュリティ対策に係る第４次行動計画において新設した用語。システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。
	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針	2018年４月４日サイバーセキュリティ戦略本部決定。安全基準等（国・業界団体・各事業者等が定める各種の基準やガイドライン）の策定・改定に資することを目的として、情報セキュリティ対策において、必要度が高いと考えられる項目及び先進的な取組として参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して収録したもの。同時に、同文書を補完するものとして、同対策編及び重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書の２つの文書が策定されている。
	重要インフラの情報セキュリティ対策に係る第４次行動計画	2017年４月18日サイバーセキュリティ戦略本部決定。昨今のサイバー攻撃による急速な脅威の高まりや、2020年東京オリンピック・パラリンピック競技大会も見据え、安全かつ持続的なサービスの提供に努めるという機能保証の考え方に基づき、第３次行動計画を見直したもの。
	重要インフラ分野	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）、医療、水道、物流、化学、クレジット及び石油。重要インフラの情報セキュリティ対策に係る第４次行動計画において記載。
す	ステークホルダー	利害関係者のこと。
	スマート家電	インターネットに接続されるネット家電で、スマートフォンなどを用いて操作できるような便利な機能が搭載されているもの。
	スマートシティ	ITや環境技術などの先端技術を用いて、都市の各種インフラを効率的に管理・運営し、エネルギーや資源の有効利用を可能とする都市。
	スマート 農林水産業	ロボット技術やICTを活用して、超省力・高品質生産を可能とする農林水産業。
	スマートフォン	従来の携帯電話端末の有する通信機能等に加え、高度な情報処理機能が備わった携帯電話端末。従来の携帯電話端末とは異なり、利用者が使いたいアプリケーションを自由にインストールして利用することが一般的。
	スマートホーム	スマート家電などを制御することでエネルギーや資源の有効利用を可能にしたり、快適な暮らしを実現するような住居。
	スマートメーター	通信機能を有し、遠隔での検針等を行うことが可能となる新しい電力量計。
	制御系	OT（Operational Technology）を参照。
せ	セキュリティバイデザイン	システムの企画・設計段階から情報セキュリティの確保を盛り込むこと。
	セプター	CEPTOAR （Capability for Engineering of Protection, Technical Operation, Analysis and Response）を参照。
	セプターカウンシル	CEPTOAR-Council。各重要インフラ分野で整備されたCEPTOARの代表で構成される協議会で、CEPTOAR間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
て	テストベッド	技術や機器の検証・評価のための実証実験、又はそれを行う実験機器や条件整備された環境のこと。
	電子署名	電子文書に付加される電子的な署名情報。電子文書の作成者の本人性確認や、改ざんが行われていないことを確認できるもの。
な	なりすまし	他の利用者のふりをすること。または、中間者（Man-in-the-Middle）攻撃など他の利用者のふりをして行う不正行為のこと。例えば、その当人であるふりをして電子メールを送信するなど、別人のふりをして電子掲示板に書き込みを行うような行為が挙げられる。
は	ハッカソン	ハック（hack）とマラソン（marathon）を組み合わせた造語であり、元々はプログラマーやデザイナーからなる複数の参加チームが、マラソンのように、数時間から数日間の与えられた時間を徹してプログラムに没頭し、アイデアや成果を競い合う開発イベントのこと。
	ハッキング	高度なコンピュータ技術を利用して、システムを解析したり、プログラムを修正したりする行為のこと。不正にコンピュータを利用する行為全般のことをハッキングと呼ぶこともあるが、本来は悪い意味の言葉ではない。そのような悪意のある行為は、本来はクラッキングという。
	パスワードリスト型攻撃	何らかの手段により他者のID・パスワードを入手した第三者が、これらのID・パスワードをリストのように用いて様々なサイトにログインを試みることで、個人情報の閲覧等を行うサイバー攻撃。

ひ	ビッグデータ	利用者が急激に拡大しているソーシャルメディア内のテキストデータ、携帯電話・スマートフォンに組み込まれたGPS（全地球測位システム）から発生する位置情報、時々刻々と生成されるセンサーデータなど、ボリュームが膨大であるとともに、従来の技術では管理や処理が困難なデータ群。
	標的型攻撃	特定の組織や情報を狙って、機密情報や知的財産、アカウント情報（ID、パスワード）などを窃取、又は、組織等のシステムを破壊・妨害しようとする攻撃。この攻撃では、標的の組織がよくやり取りをする形式や内容の電子メールを送りつけ、その電子メールの添付ファイルやリンクを開かせ、マルウェア等を利用して攻撃する手口がよく使われている。標的型攻撃の一種として特定のターゲットに対して様々な手法で持続的に攻撃を行うAPT（Advanced Persistent Threat）攻撃がある。
	標的型メール	標的型攻撃を参照。
ふ	フィッシング	実在の金融機関、ショッピングサイトなどを装った電子メールを送付し、これらのホームページとそっくりの偽のサイトに誘導して、銀行口座番号、クレジットカード番号やパスワード、暗証番号などの重要な情報を入力させて詐取する行為のこと。
	不正アクセス	ID・パスワード等により利用が制限・管理されているコンピュータに対し、ネットワークを経由して、正規の手続を経ずに不正に侵入し、利用可能とする行為のこと。
	不正プログラム	情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称。
へ	ベスト プラクティス	優れていると考えられている事例やプロセス、ノウハウなど。
	ペネトレーション テスト	情報システムに対する侵入テストのこと。「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015年５月25日サイバーセキュリティ戦略本部決定）においては、「インターネットに接続されている情報システムについて、疑似的な攻撃を実施することによって、実際に情報システムに侵入できるかどうかの観点から、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。なお、インターネットとの境界を突破できた場合を仮定して、内部ネットワークについても、サイバーセキュリティ対策上の問題を検証し、改善のために必要な助言等を行う。」とされている。
ほ	ポート	ポート番号。コンピュータが通信する際に通信先のプログラムを識別するための番号で、通常利用されるTCP/IPでは、65535番まである。通常、プロトコルに応じてポートが割り当てられている。たとえば、FTPはTCPの21番ポート（制御用）と20番ポート（データ用）、HTTPはTCPの80番ポート、HTTPSはTCPの443番ポートを使用する。
	ホワイトハッカー	コンピュータやネットワークに関する高度な知識や技術を持つ者のうち、特にその技術を善良な目的に活かす者。
ま	マルウェア	malicious software の短縮された語。不正かつ有害な動作を行う、悪意を持ったソフトウェアのこと。
ら	ランサムウェア	データを暗号化して身代金を要求するマルウェア。ランサムは身代金の意味。
り	リスク マネジメント	リスクを組織的に管理し、損失などの回避・低減等を図るプロセスのこと。
	リテラシー	本来、文字を読み書きする能力を意味するが、「情報リテラシー」のように、その分野における知識、教養、能力を意味することに使われている。

【参考２】

会議開催年月日・議題一覧

① 平成２９年１２月５日（火）
サイバーセキュリティ対策に関する政府の取組状況について
② 平成３０年１月３１日（水）
自動運転のサイバーセキュリティ対策について
③ 平成３０年２月７日（水）（金融調査会及びIT戦略特命委員会と合同開催）
重要インフラ分野に対するサイバーセキュリティ対策の現況（金融・クレジット・仮想通貨）について
④ 平成３０年２月１４日（水）
重要インフラ分野に対するサイバーセキュリティ対策の現況（航空・鉄道・物流）について
⑤ 平成３０年２月２１日（水）
重要インフラ分野に対するサイバーセキュリティ対策の現況（情報通信）について
⑥ 平成３０年２月２８日（水）
重要インフラ分野に対するサイバーセキュリティ対策の現況（電力・ガス・石油・化学）について
⑦ 平成３０年３月７日（水）
重要インフラ分野に対するサイバーセキュリティ対策の現況（医療・水道）について
⑧ 平成３０年３月１４日（水）
重要インフラ分野に対するサイバーセキュリティ対策の現況（政府・行政サービス）について
⑨ 平成３０年３月２３日（金）
日本の安全保障におけるサイバーセキュリティについて
⑩ 平成３０年３月２８日（水）
サイバーセキュリティ対策に関する有識者ヒアリング
（量子コンピュータについて）（情報セキュリティを巡る研究開発について）
⑪ 平成３０年４月４日（水）
サイバーセキュリティ対策に関する有識者ヒアリング
（重要インフラ分野横断的演習について）（インシデント対応の国内外コーディネーション業務について）
⑫ 平成３０年４月２３日（月）
第１次提言とりまとめ

【参考３】

ヒアリング協力者名簿（有識者・政府）

（敬称略）

【有識者】

西森秀稔	東京工業大学教授
後藤厚宏	情報セキュリティ大学院大学学長
大林厚臣	慶応義塾大学教授
有村浩一	JPCERT コーディネーションセンター常務理事

【政府】

（内閣官房）

三角育生	内閣サイバーセキュリティセンター　副センター長
山内智生	内閣サイバーセキュリティセンター　内閣参事官
越後和徳	内閣サイバーセキュリティセンター　内閣参事官
林　泰三	内閣サイバーセキュリティセンター　内閣参事官
瓜生和久	内閣サイバーセキュリティセンター　内閣参事官

（警察庁）

大濱健志	生活安全局情報技術犯罪対策課長
杉　俊弘	交通局交通企画課自動運転企画室長

（金融庁）

水口　純	監督局審議官
油布志行	総務企画局参事官
斎藤　馨	総務企画局政策課長

（総務省）

谷脇康彦	政策統括官（情報セキュリティ担当）
渡辺克也	総合通信基盤局長
山下哲夫	行政管理局長
猿渡知之	大臣官房審議官
木村公彦	情報流通行政局サイバーセキュリティ課長
柳島　智	情報流通行政局サイバーセキュリティ課参事官
渋谷闘志彦	情報流通行政局情報流通振興課情報流通高度化推進室長
稲原　浩	地域力創造グループ地域情報政策室長

（文部科学省）

安彦広斉	生涯学習政策局情報教育課情報教育振興課室長
溝口浩和	大臣官房政策課情報システム企画室長
西山崇志	科学技術・学術政策局研究開発基盤課量子研究推進室長
丸山修一	研究振興局参事官（情報担当）付学術基盤整備室長

（厚生労働省）

椎葉茂樹	大臣官房審議官（医政、精神保健医療、災害対策担当）
宇都宮啓	生活衛生・食品安全審議官
大橋秀行	サイバーセキュリティ・情報化審議官

是澤裕二	医薬・生活衛生局水道課長
中山　理	大臣官房参事官（サイバーセキュリティ・情報システム管理担当）
森田博通	医政局研究開発振興課医療情報企画調整官
笹子宗一郎	政策企画官
（経済産業省）	
多田明弘	製造産業局長
寺澤達也	商務情報政策局長
小瀬達之	商務・サービスグループ審議官
塩田康一	産業保安グループ産業保安担当審議官
伊東　寛	大臣官房サイバーセキュリティ・情報化審議官
奥家敏和	商務情報政策局サイバーセキュリティ課長
湯本啓市	製造産業局素材産業課長
辻本圭助	大臣官房技術・高度人材戦略担当参事官
定光裕樹	資源エネルギー庁資源・燃料部政策課長
山下　毅	大臣官房情報システム厚生課統括情報セキュリティ対策官
伊奈友子	商務・サービスグループ物流企画室長
小川　要	資源エネルギー庁電力・ガス事業部電力産業・市場室長
田中伸彦	商務情報政策局情報産業課デバイス・情報家電戦略室長
（国土交通省）	
大野秀敏	大臣官房サイバーセキュリティ・情報化審議官
江坂行広	自動車局技術政策課長
柴宮義文	総合政策局情報政策課サイバーセキュリティ対策室長
平野達也	総合政策局物流政策課企画官
門元政治	鉄道局総務課危機管理室長
小林哲緒	航空局総務課危機管理室長
（防衛省）	
伊藤哲也	整備計画局情報通信課長
二宮　勉	整備計画局情報通信課サイバーセキュリティ政策室長

本部長ヒアリング・資料提供協力者名簿

（敬称略）

日本電信電話株式会社	鵜浦博夫、篠原弘道、大門　聡、 平田真一、高橋順子、中島明日香
NTT コミュニケーションズ株式会社	小山　覚
NTT データ先端技術株式会社	三宅　功
デロイト　トーマツ　リスクサービス　株式会社	丸山満彦
デロイト　トーマツ　コンサルティング　合同会社	川原　均
株式会社　Blue Planet-works	石橋　哲
ブリッジシップ株式会社	吉母　強
GR Japan 株式会社	鈴木　渉
有識者等	村上憲郎、横浜信一

【参考４】

サイバーセキュリティ対策本部　出席国会議員名簿

（五十音順、敬称略）

青山　繁晴	赤池　誠章	朝日健太郎	阿達　雅志
甘利　　明	有村　治子	安藤　高夫	石田　真敏
磯﨑　仁彦	伊藤信太郎	岩田　和親	岩屋　　毅
上杉謙太郎	上野　宏史	江渡　聡徳	太田　房江
大塚　　拓	奥野　信亮	小田原　潔	鬼木　　誠
新藤　義孝	尾身　朝子	片山さつき	加藤　寛治
神谷　　昇	神山　佐市	亀岡　偉民	河井　克行
神田　憲次	黄川田仁志	北村　誠吾	木原　誠二
木村　義雄	工藤　彰三	小林　茂樹	小林　鷹之
後藤　茂之	坂本　哲志	笹川　博義	左藤　　章
佐藤　信秋	繁本　　護	柴山　昌彦	進藤金日子
自見はなこ	杉田　水脈	鈴木　馨祐	鈴木　淳司
鈴木　隼人	平　　将明	高市　早苗	高村　正大
徳茂　雅之	冨岡　　勉	中谷　真一	中西　健治
中村　裕之	中山　展宏	中山　泰秀	根本　　匠
橋本　　岳	原田　義昭	平井　卓也	福井　　照
藤井比早之	藤原　　崇	船橋　利実	穂坂　　泰
星野　剛士	本田　太郎	牧島かれん	牧原　秀樹
松下　新平	松本　剛明	丸川　珠代	三浦　　靖
三谷　英弘	三ツ林裕巳	宮澤　博行	宮下　一郎
宮本　周司	務台　俊介	森　まさこ	八木　哲也
簗　　和生	山際大志郎	山口　俊一	山田　賢司
吉川ゆうみ	和田　義明		