

IoT・5G セキュリティ総合対策 2020 パブリックコメント

複製禁止

組込みシステム技術協会

組込みシステムセキュリティ委員会

複製禁止

目次

1. パブリックコメントにあたって	4
1.1. IoT のセキュリティ対策	5
1.2. 5G のセキュリティ対策	7
1.2.1. サプライチェーン	7
1.2.2. データ	7
1.2.3. ネットワーク特性	8
1.3. クラウドサービスのセキュリティ対策	9
1.4. テレワークシステムのセキュリティ対策	9
1.5. 無線 LAN のセキュリティ対策	10
1.5.1. 訪日外国人と日本人の意識の違い	10
1.6. 国際連携の推進	13
1.6.1. 日本の現状	13
1.6.2. ボット化の対策	14
1.7. 人材育成・普及啓発の推進	16
1.7.1. 経営層の育成・普及啓発	16
1.7.2. セキュリティ技術者の育成	17
1.7.3. 人為的ミスの改善	19
1.8. AI の積極的な活用	20
1.9. 参考文献	21

1. パブリックコメントにあたって

総括として、NICT(国立研究開発法人情報通信研究機構)の取り組みや総務省「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第1版)」を軸にした、IT側視点の提言となっており、IoTにおけるOT側の視点を入れたIoT全体のシステムでの対策方法が取れるように取り組みを継続頂ければと考える。ボット化対策や人材育成の部分についても、NICTの取り組みを軸にした積極的な活動を継続頂ければ考える。

以下、各項目についてのコメントとなる。

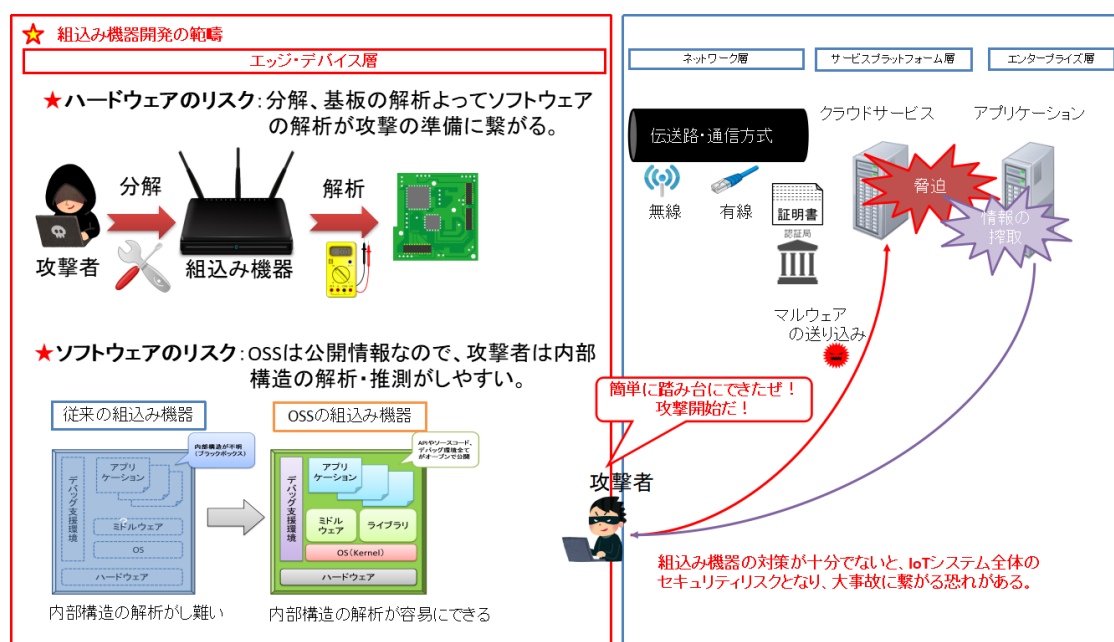
1.1. IoT のセキュリティ対策

IoT システムの運用においては、OT-IT の両方の視点が必要と考える。NICT の取り組みとして、「NOTICE」の活動は有用と考える。しかしながら、あくまでも運用されたものに対する活動となり、運用前の設計におけるセキュリティ対策には繋がらないと考える。

セキュリティ対策においては、運用前の設計段階での対策が重要であり、セキュリティ・バイ・デザインを浸透させることが重要であると考え。特に OT 側のエンジニアは、IoT 活用のためのネットワークスキル経験が不足しており、セキュリティに対するノウハウ集積度も低く意識も低いと考える。OT 技術者が IoT を活用していくためには、特に車載系では、クローズだったものが、ネットワーク利用によりコネクティッドとなったりと、今までネットワークを使ってこなかった技術者が多数のため、ネットワークスキルの向上とセキュリティに対する意識向上が必要であり、人材育成として急務であると考え。

また、OT 側の開発においては、特に外部調達するハードウェアやソフトウェアなど調達基準やサプライチェーンの確立やルールが必須であり、経済産業省が推進している CPSF(Cyber Security Physical Framework)の活用と本活動の連携が必須になると考える。

OT 側機器の脆弱性な部分として、ハードウェアの分解、ソフトウェアの解析に対する対策が重要となるため、OT 側の開発段階時にセキュリティガイドラインの確立が急務であると考え。



総務省が発表した「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第1版)」は有用である。NICTが活動している「NICTER」による活動も有用である。しかしながら、効力として「任意の認証」ではなく、強制力を持った認証にしなければ、ボット化の検知、対応、復旧が遅れることになりかねず、諸外国とのデータ競争にも負けてしまうと考える。

1.2. 5G のセキュリティ対策

5G の活用にあたって3つの視点でのセキュリティ対策が必要であると考えます。また、「低遅延」「高速」「多様性」が謳われており、マルウェア感染拡大時のスピードが、従来のネットワークよりも各段に早くなると思われる。COVID-19 の感染拡大にも類似するが、クラスターとならないための隔離方法、感染者の特定などネットワーク側からのアプローチが必要になると考える。特に M2M での感染拡大についての対策アプローチが必要になると考える。

※参考文献1より引用

1.2.1. サプライチェーン

5G の活用においては、大量のデータから AI(人工知能)を活用するための機械学習用のデータ収集をするニーズが多くなってくると想定される。活用分野として、運輸、公共サービスや農業など様々な業種に活用されることが予想されている。

例えば、データ収集には、センサーデバイスの活用が必須となってくる。センサーデバイスの調達の際には、セキュリティの観点では、調達先の企業の事業実態、所在地、過去の経歴(不祥事など)の観点で適切な評価が必要となると考える。

5G を使ったセンサーによる製品やサービスの観点では、「センサーの不正操作を防げるか」「セキュリティ侵害を検知できるか」「不正なデータ流出がされないか」などの評価が必要になってくる。

2016 年 米国セキュリティ会社が携帯電話のファームウェアに不正なプログラムがあることを発見したように、調達したものや利用されているものの不正を調査できるようなサプライチェーンルールの確立が必要だと考える。

1.2.2. データ

5G の活用により、大量のデータを取得できることになる。大量に集まったデータは、厳しさが各各種法令に基づくデータプライバシー基準に準拠しなければならない。

企業では、定期的なデータ価値の見直し、データのライフサイクルを管理し、「データをどのような方法で取得するか」「データをどこに保存するか」「司法管轄が異なり、データ保護に関する規定もことなる地域にデータを移動することがあるか」などを規則的に決め、データの収集ポイント、データの転送経路、最終的な保存先、さらに廃棄まで、一貫してデータを保護する必要がある。

1.2.3. ネットワーク特性

5G の「低遅延」「高速」「多様性」という特性を活かすことで、これまで現実的でなかったユースケースが実現可能となる。例えば、5G の特性を活かす分野として、ヘルスケアが考えられる。高齢者などの生体情報をリアルタイムにモニタリングし、その値が正常レベルから逸脱したら介護者にアラートを知らせるなど仕組みを利用することで、介護にかかるコストを削減し、介護の質を高めるなどが可能となってくる。こういった利用方法では、悪意ある攻撃者が攻撃することで、「低遅延」の特性を妨害する事が考えられる。

「低遅延」を確保するために、定期的な遅延の測定、複数経路の確保、冗長化したネットワークを利用するなど、ネットワークの利用方法を考えることも必要となる。

1.3. クラウドサービスのセキュリティ対策

DX(Digital Transformation)の推進においては、データが非常に重要な要素となり、ビジネスチャンスとなると考えられる。データ活用にあたっては、情報の漏えいや盗聴を未然に防ぐことや、漏えいに気付くことが必要になってくる。

データ活用には、C.I.A の確保は勿論のこと、e シールやマイナンバーの活用、証明書の利用を促進し、データを扱う人や機器の真正性、データ自体の真正性を確保する認証方式の確立が必要となると考える。

企業においてクラウド利用にあたっては、データに対する漏えいや盗聴などを防ぐための認証や暗号化を利用するためのルールを確立するためのガイドライン化も必要となる。

1.4. テレワークシステムのセキュリティ対策

COVID-19 の拡大に伴い、企業におけるテレワーク活用が多くなってきており、情報セキュリティ対策は非常に重要な要素となっている。「テレワークセキュリティガイドライン（第4版）」にもあるが、「ルール」「人」「技術」のバランスが取れた対策の実施が望まれるが、COVID-19 拡大に伴って、改めて日本国内における IT 化の推進が遅れていることが露呈したと考える。

特に経営層のセキュリティに対する考えの甘さや IT インフラ設備の遅れなどで、ネットワーク活用におけるルール化がなされていないなど、経営対策としてのセキュリティ対策の遅れが目だったように感じられる。

IT 化の推進においては、本資料の e シールなどの活用を積極的に推進し、真正性を担保できる国産の認証基盤の構築やペーパーレス化の推進が必要と考える。

本資料の「データ負けのスパイラル」でも述べられているが、テレワークツールの活用においても、海外製のツールしか使われていないのが現状であり、データ流出は起きている前提での改善施策を検討した方が良いと考える。少なからず、中小企業向けにはどんなツールを利用することが望ましいのかを選定可能なガイドラインなどを作成するなどの活動が望ましいと考える。

企業においても、通常はイントラシステム利用などオンプレ環境でデータの持ち出しが不可であることで、出社を余技なくされるケースも多々見受けられるため、積極的なクラウドシステムの活用など推進を企業に呼びかけていくことを推進頂けると良いと考える。

1.5. 無線 LAN のセキュリティ対策

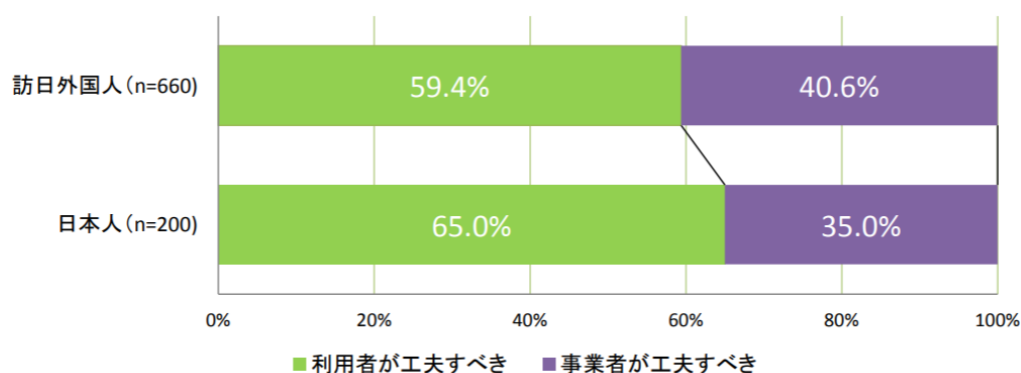
総務省での公衆無線 LAN に関わる調査結果などから、利用者の無線 LAN に対するセキュリティ意識が低いように見受けられる。

無線 LAN については、利用者がセキュリティ意識を持って対応することが求められるので、利用者に対するセキュリティ意識を向上させるための啓発やガイドラインなどを展開し、意識を高めることが必要と考える。

1.5.1. 訪日外国人と日本人の意識の違い

2015 年に総務省で行った公衆無線 LAN 利用に係る調査結果から見て、日本国内の利用者のセキュリティ意識はあることが伺える。

【無料Wi-Fiにおけるセキュリティ対策をすべき当事者調査】

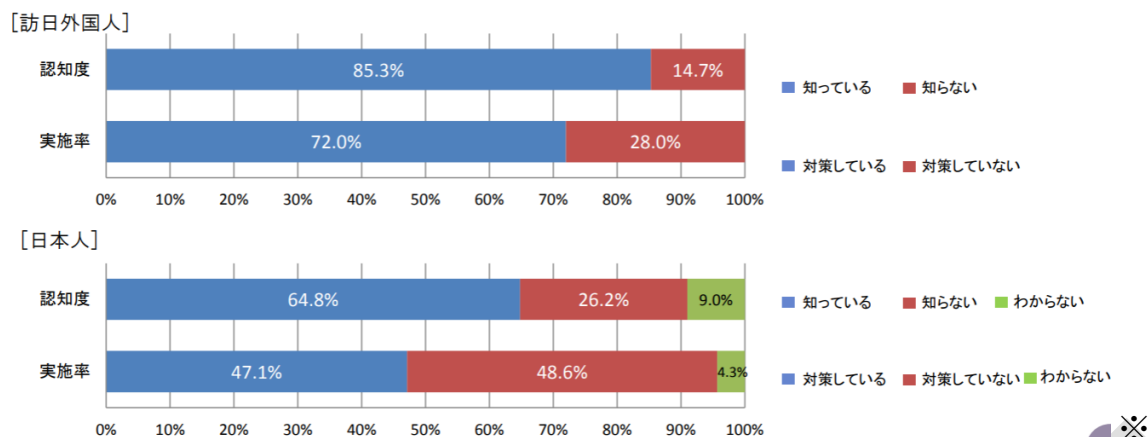


※

参考文献 3 から引用

しかしながら、実際に対策を実施している統計を見ると、対策が実施されていない事が分かる。Wi-Fi 利用にあたっての脆弱性に対する認知度が高いものの、実際の実施率が低くなっていることが伺える。

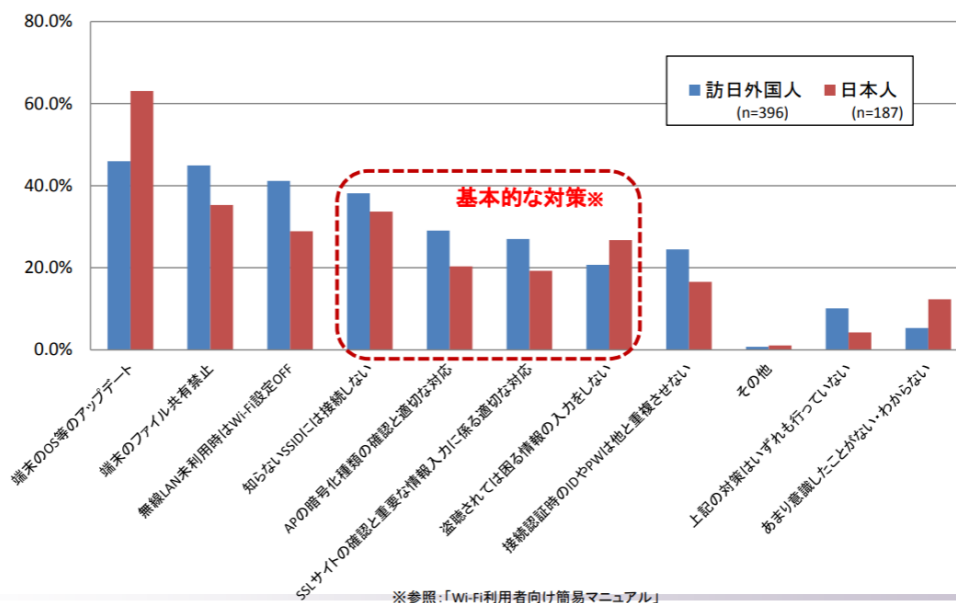
【公衆無線LAN利用時の脅威(盗聴／なりすまし／悪意のアクセスポイントやサイトへの接続)認知度及び実施率】



参考文献 3 から引用

実際の対策についても、OS アップデートは一定数対策されているが、公衆無線 LAN 利用時の基本的な対策の実施率が低いことが伺える。

【公衆無線LAN利用時に実施していた情報セキュリティ対策】



参考文献 3 から引用

COVID-19 の拡大に伴い、無線 LAN の利用がリモートワークで活用されている中で、個人で利用する際の無線 LAN セキュリティ対策は必須となってくると考えられ、利用者に対するセキュリティ意識向上のための啓発が急務となっているため、電波利用の観点などから、積極的なセキュリティ対策の啓発活動をしていくべきと考える。

複製禁止

1.6. 国際連携の推進

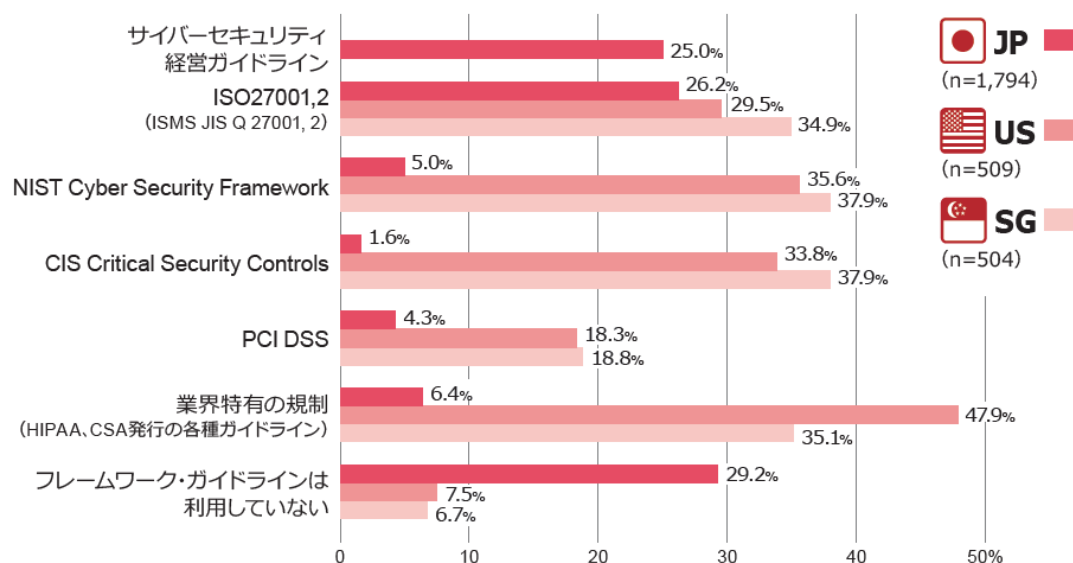
2016年に発生した「Mirai」では、保守ポートの telnet を狙ったボット化を防ぐ取り組みは重要になってくると考える。「Mirai」の問題では、保守ポートが空いていることが問題と考えられるが、最も重要になるのは、ボット化された事に気が付かなかった点が挙げられる。本資料での提言通り、NICT の「NICTER」を活用した取り組みは有用であり、今後も継続した活動が続けるべきと考える。

国際情勢として、米国、欧州など主要国でのサイバーセキュリティに対する法案、ガイドラインが策定、施行されている状況であり、日本としても国際的な連携や活動が必要になっていると考えられ、各国の動向に合わせた取り組みが必要である。

1.6.1. 日本の現状

NRI Secure Insight 2019 によると、国内で参考としているセキュリティガイドラインの多くが、ISO27000 シリーズになっている。特筆すべきは、フレームワーク・ガイドラインを利用していないのが3割あることである。米国の NIST や欧州の ENISA などの動向を踏まえると、国際情勢に合わせたフレームワーク・ガイドライン利用をしていくことが急務であると考ええる。諸外国の動向として、業界特有の規制などが数多く存在しており、GDPR を始めとしたデータの取り扱い方など海外でのビジネスを展開するにあたっては、IEC62443 などの国際規格の対応などを推進していくことが必要と考えられる。

参考ガイドライン



※「サイバーセキュリティ経営ガイドライン」は日本の経済産業省が発行するガイドラインのため、日本のみ選択肢に追加

※

参考文献5：NRI セキュアテクノロジーズ株式会社 NRI Secure Insight 2019 より引用

1.6.2. ボット化の対策

米国では、IoT デバイスがボット化してしまうことに対する対策として、2018 年 5 月に商務省(DoC)、国土安全保障省(DHS)が報告書をまとめた。報告書に基づき、11 月に「対ボットネット強靱化ロードマップ」を公開した。ボットネット撲滅活動を 5 つの取組みに分類した上で、官民が行うべき個別 Workstream(タスク)として整理された。ロードマップの公表に合わせ、CSDE(The Council to Secure the Digital Economy)が表 2 に示す 5 つの取組み・タスクを示し、「国際アンチボットネットガイド」として公表し、官民の強いパートナーシップを持った取組みを行っている。(参考文献 6 より引用)

◆表 1 ロードマップにおける 5 つの取組み・タスク

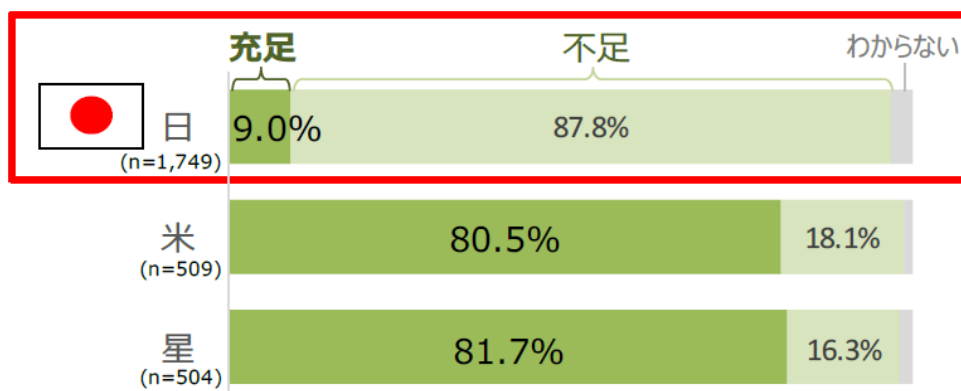
項番	項目	内容
1	IoT デバイスのセキュリティ向上	信頼性の高い IoT 機器の強固な市場開拓。エコシステム全体にわたる IoT セキュリティの持続的な適用

2	企業のサイバーセキュリティリスクマネジメント	NIST CSF を用いたプロファイル作成。ネットワークアーキテクチャの高度化。企業のベストプラクティスの連邦政府への適用。OT のサイバーセキュリティ対策
3	インフラ	ルーティングのセキュリティ向上。実践的な情報共有の推進。情報共有プロトコルの開発。インフラセキュリティ向上のための研究開発
4	セキュリティ技術の開発・移り変わり	セキュアなソフトウェア市場の構築。国際協調。革新的な技術開発。
5	啓発と教育	IoT 機器のセキュリティに対する消費者の信頼を促進。IoT 機器のサイバーセキュリティの脅威に対する労働者の教育。

本資料でも述べられている通り、産学官の連携のもと、積極的な活動を行い、ボット化対策を推進していくことが急務であると考えます。(上記の文章、表は、参考文献4から引用)

1.7. 人材育成・普及啓発の推進

本資料にある通り、日本ではセキュリティ対応ができる人材は不足している。本資料でも述べられている通り、日本のセキュリティ技術者は不足していると考え。ただ、充足していると回答したものでは、諸外国に比べてセキュリティに対する意識が低いのが目立っていると考え。[参考文献5：NRI Secure Insight 2019を参照]



(出典) 企業における情報セキュリティ実態調査 2019

(NRI セキュアテクノロジーズ) より作成

1.7.1. 経営層の育成・普及啓発

セキュリティ対策にあたっては、諸外国のようにトップダウンでの対策が取れていないと考える。日本の場合、自社/他者でのセキュリティインシデントや内部監査などでの指摘による他者からの指摘が発端となっている。自発的な取り組みとなっておらず、経営課題としてのセキュリティ対策の意識が低い現状である。国内においては、セキュリティ対策が後ろ向きなイメージとなっており、積極的な対応を行っているとはいえない状況である。また、諸外国の動向を踏まえると、セキュリティ対策がされていない機器の受け入れが難しくなってくると予想されるため、経営課題としてのセキュリティ対策の意識向上のための育成や啓発活動が急務であると考え。

情報セキュリティ対策実施のきっかけや理由

あてはまるもの最大3つ選択

	JP (n=1,794)	US (n=509)	SG (n=504)
1位	 自社でのセキュリティインシデント 33.6%	 経営層のトップダウン指示 55.4%	 経営層のトップダウン指示 66.1%
2位	 他社でのセキュリティインシデント 27.1%	 他社でのセキュリティインシデント 25.0%	 他社でのセキュリティインシデント 27.8%
3位	 内部監査・内部有識者からの指摘 27.0%	 自社でのセキュリティインシデント 23.4%	 外部監査・第三者評価の結果 22.4%

※ 他選択肢:株主や取引先からの要請 / 関連法規の改定 / 監督官庁からのセキュリティ対策の要請

※

参考文献5：NRI セキュアテクノロジーズ株式会社 NRI Secure Insight 2019 より引用

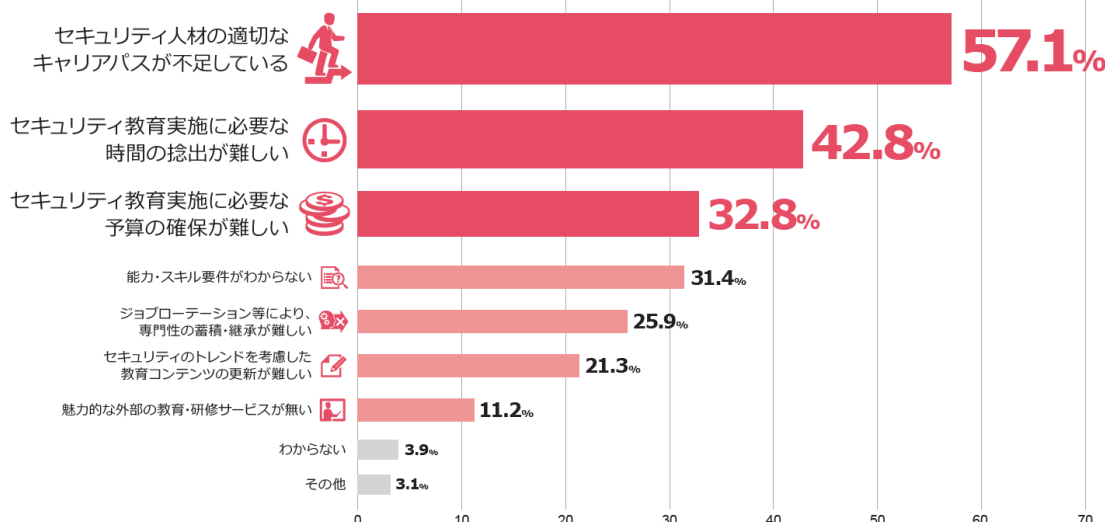
1.7.2. セキュリティ技術者の育成

本資料で述べられている通り、実践的サイバー防御演習(CYDER)などの活用を積極的に行って CEH(Certified Ethical Hacker)を育成していく事は非常に重要なことである。ただし、現状の国内の動向を見る限り、適切なポジションやキャリアパスがないのが現状である。時間や予算についてもセキュリティ技術者のポジションを明確にし、必要となるスキル要件の定義を行った上で積極的な育成をしていくことが必要であると考ええる。

セキュリティ人材の育成・教育における課題

あてはまるもの最大3つ選択

日本企業におけるセキュリティ人材の育成・教育における課題

JP
(n=1,794)

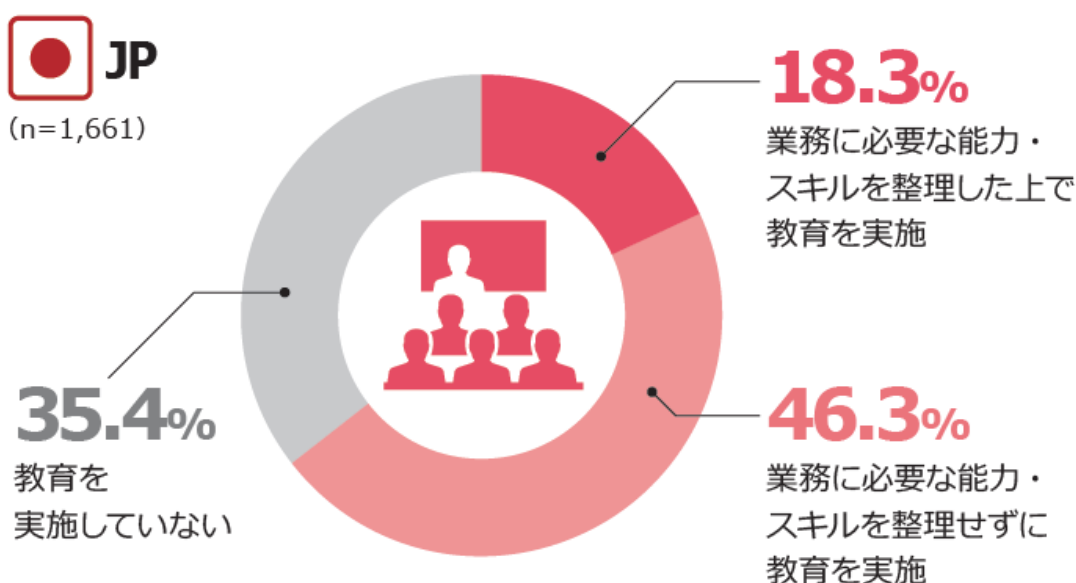
※

参考文献5：NRI セキュアテクノロジーズ株式会社 NRI Secure Insight 2019 より引用

一方、セキュリティ人材の育成を行っているが、実際に対策をしているが、実際の業務に必要なスキルを整理せずに教育を実施していると回答しているものもある。闇雲に教育をしたところで、正しいスキルを身に付く分けではないため、実践のために必要となるスキル標準定義を行い、必要となるスキル体系化と教育カリキュラムの展開が必要と考える。

■ セキュリティ人材の育成・教育の実施状況

日本企業におけるセキュリティ人材育成の実施状況



※

参考文献 5 : NRI セキュアテクノロジーズ株式会社 NRI Secure Insight 2019 より引用

1.7.2.1. 情報の精査・正しい対策の立案

2017 年に起きた「Wi-Fi WPA2 の問題」は、SNS 上に広がった。SNS で拡散されたことで、センセーショナルな報道となったが、誰しもが使う Wi-Fi だっただけに初報が大きく取り上げられすぎたことも挙げられる。実際に IPA から報告あった内容を見る限りでは、盗聴範囲が限られており、適切な対策をすることで対策できる内容であったことも伺える。SNS 上で拡散される情報を正しく見極め、正しい対策ができる技術者の育成も必要となると考える。(参考文献 1、参考文献 2 から引用)

1.7.3. 人為的ミスの改善

日本国内で発生するセキュリティインシデントを見る限り、「人為的ミスが」多いことが挙げられる。IPA 10 大脅威 2020(参考文献 7)の報告もある通り、Top3 はいずれも「人為的ミス」が多いと報告されている。諸外国に比べて、メールなどの誤送信、記憶媒体の紛失などと人為的なミスが多いことが分かる。各企業で

の取り組みはしているものの、セキュリティ意識が低いために発生するミスとなっており、ネットワーク活用において悪用されない仕組み作りも必要となると考える。特に真正性を確保できる仕組みづくりにおいて、個人が特定できる仕組みや個人しか利用できない仕組み作りなどが必要になると考える。

過去1年で発生した事件・事故

あてはまるものすべて選択

	 JP (n=1,794)  82.9%	 US (n=509)  83.7%	 SG (n=504)  86.5%
1位	電子メール、FAX、郵便物等の誤送信・誤配送	DoS 攻撃／DDoS 攻撃	DoS 攻撃／DDoS 攻撃
2位	情報機器・外部記憶媒体の紛失・置き忘れ・棄損	Web アプリケーションの脆弱性を突いた攻撃	Web アプリケーションの脆弱性を突いた攻撃
3位	マルウェア感染	システム基盤の脆弱性を突いた攻撃	自社サービスへのリスト型アカウントハッキング
4位	システム設定ミス、誤操作	自社サービスへのリスト型アカウントハッキング	標的型メール攻撃
5位	標的型メール攻撃	マルウェア感染	システム基盤の脆弱性を突いた攻撃
6位	社員証、業務書類等物品の紛失・置き忘れ・棄損	標的型メール攻撃	マルウェア感染
7位	情報機器、電子記憶媒体、紙媒体等の盗難・紛失	水飲み場型攻撃	水飲み場型攻撃
8位	ランサムウェア	ランサムウェア	情報機器・外部記憶媒体の紛失・置き忘れ・棄損
9位	その他	電子メール、FAX、郵便物等の誤送信・誤配送	ランサムウェア
10位	DoS 攻撃／DDoS 攻撃	情報機器・外部記憶媒体の紛失・置き忘れ・棄損	システム管理者等による不正アクセスや持出



ヒューマンエラー



サイバー攻撃



過去一年で事件・事故が発生した企業の割合

※

参考文献 5 : NRI セキュアテクノロジーズ株式会社 NRI Secure Insight 2019 より引用

1.8. AI の積極的な活用

本資料にも述べられている通り、セキュリティ対策においては、機械学習など AI の活用は有用であると考えます。AI 自体もセキュリティや安全面での課題も多くあ

る。攻撃者にとっては、AI であっても解析できるだけのスキルを持っていると想定され、AI 自体のセキュリティに対する取組みも急務であるとする。

1.9. 参考文献

参考文献 1 : 「5G」導入が“致命傷”になる？高まるセキュリティリスクと対策

参考文献 2 : Wi-Fi に見つかった脆弱性で、“穴だらけ”の IoT 機器が大量発生する—その脅威が 10 年は続くかもしれない

参考文献 3 : 総務省（公衆無線 LAN 利用に係わる調査結果）

参考文献 4 : Bulletin JASA Vol073

参考文献 5 : NRI Secure Insight 2019

参考文献 6 : 経済産業省：サプライチェーンサイバーセキュリティ等に関する海外の動き 平成 31 年

参考文献 7 : IPA 10 大脅威 2020