JNSA PRESS

JAPAN NETWORK SECURITY ASSOCIATION

SUMMER 2021 VOL. 50

寄稿

「通信のための理論」を使って「セキュリティの本質」をあぶり出す
03

セキュリティアウェアネスとは何か
08

プライバシー規制の強化や有事対応に対するInformation Governanceの有効性について
12

CONTENTS

特定非営利活動法人
日本ネットワークセキュリティ協会
NPO Japan Network Security Association

外部との連携を強化してはどうでしょう？

情報セキュリティ大学院大学名誉教授
JNSA 会長　田中　英彦

現在のJNSAの活動を俯瞰してみると、セキュリティに関わる諸活動がある。諸規格立案への対応、ユーザに対するセミナや技術紹介、製品やサービスの普及促進や市場活性化、セキュリティコンテスト、出版、人財育成、勉強会、教育指針作成、関連統計データ調査、諸ガイドライン作成、人財キャリア認定、メンバや海外市場開拓等、多くの活動がある。

これらは、セキュリティ企業が共通に持つ課題で、競争するより協力しあった方が良い課題に関わる活動で、それに興味を持つ者が参加しボトムアップで構成されるというのが基本であろうか。

しかし、新技術等の研究開発は共同の活動としては見えない。一般的に言えば、新アイデアは企業の活動を支える要素で、他企業との差別化を図る重要な考えであって、共有するものではない。しかしながら、一社で行うにはコストが高いテーマや、基礎研究のように競争前活動として一般に捉えられる領域、そこにおける相互協力は一般の技術世界では広く存在するもので、研究機関や大学などとの連携もその辺りに位置付けられる。

JNSA内でこの種の連携は今迄、限られた形でしか成されてこなかったように思う。連携の例は、大学生への教育活動として幾つかの大学で行われているセキュリティ教育enPiT-Securityや、岡山理科大での講義、そしてインターンシップ活動である。これらはいずれも専門教育を提供する活動で、若い人財を獲得するための間接活動でもある。

しかし、新しい技術の検討や共同研究活動で、研究所や大学と明示的に連携するものは見え難い。個別の企業内で具体的な共同研究がなされているかも知れないが、JNSA全体の明示的な活動としては存在しないのが現状である。

一方、大学の研究活動は、暗号等の基礎ではしっかりした長い活動があるし、研究機関では、MWSマルウェア対策研究人材育成ワークショップによる観測データの提供があり、研究所NICT、NII等の研究も存在する。研究会としては、ISEC、CSEC、ICSS、等があり、大会としては暗号と情報セキュリティシンポジウム SCISがある。しかし、これらの活動はセキュリティの実務専門家と疎遠で、JNSAとの具体的な連携活動も見えないように思う。

この状況は二つの意味で損失である。一つは、セキュリティ業界の抱える問題を解決するための知恵を相談する相手を見逃していることで、せっかく存在する研究機関や大学の力を生かしきれていない。もう一つは、セキュリティ業界が実務に携わる中で把握しているセキュリティ問題の現状や構造を、研究機関や大学へ明確に伝えていないことである。結果として、彼らがこの分野のオリジナルで優れた成果を出す助力をしておらず、その機会を与えていない。これらはセキュリティ業界の飯のタネに関わる事柄であって、外部に対しもっとオープンになり彼ら

の力を借りると同時に、今後の長期的な展望を描いて新方向を打ち出し、海外をリードするために必要なポイントではなかろうか。

困っていることやニーズを伝えれば多くの研究活動を誘発する可能性がある。我が国のセキュリティ技術はオリジナルが少ないと言う前に、自分たちは十分その研究開発に努力してきたかを問いたい。研究所や大学、そして若者にはセキュリティ技術や業界に興味を持つ多くの隠れた人財が居るように思う。これらの間に具体的な活動や連携のネットワークを形成できれば種々の動きが期待できよう。

IT システムは次々と新たに作られ現場に投入される。新たな脆弱性が次々と作られる訳で、終わりがないように見える。またシステムの一部としての人間が騙される詐欺行為は防ぐのが困難に見える。しかし、これらへの基本対策手法を研究開発して実装し、セキュリティを追い詰めてゆくことも考えられるのではないか。

DX が声高に語られる今日、今後のIT 業界が大きく育ちその役割をきちんと果たすためにも、セキュリティの役割は大きい。そのコアを他国に任せることでは済まされない。セキュリティはインテリジェンスに繋がり、自国の力が無いと他国の力を借りることもできない。我が国特有の環境があるのであれば、それは我が国の中でこそ解決が図れるし、それと似た環境を有する国へのセキュリティ提供は、我々の得意分野にもなる。

セキュリティの基本問題と脆弱性の構造を分析して共有し、その解決に向けた長期の活動に繋げ、結果としてセキュリティ企業のベースを高度化してゆくために、研究機関や大学等外部の人々との継続的な強い連携を図ることが必要なのではないかと考える。

「通信のための理論」を使って「セキュリティの本質」をあぶり出す

セコム株式会社 IS 研究所
甘利　康文

1．はじめに

太平洋戦争が戦雲急を告げていた1941年、電信が発明されて100年以上、電話についても60年以上の歳月が流れ、既にこれらの通信手段は世の中において広く使われるようになっていた。ちょうどその年、世界最大の電信電話会社の研究所に就職した一人の青年がいた。名をクロード・シャノンという。新しい職場から彼に与えられた研究テーマは、なんと「通信の正体を明らかにすること」。「通信において伝えられているものとは何なのか」、「ノイズなどで通信に支障をきたすときに伝達されなくなるものとは一体何なのか」、これらの疑問への答を見出すことだった。その当時、「通信」サービスの当事者である電信電話会社は、驚くべきことに自社が提供しているそのものの正体を知らずに、それを世の中に提供していたのだ [1], [2]。そのため、何か問題が起こった場合も、対応は都度、対症療法的なものにならざるを得ない状況 [3] であり、通信の本質を明らかにすることは、「通信」をサービスとして提供している当事者としては、解決しなければならない重要な課題だったのだ。

それからしばらく経った1948年、彼は、研究論文「通信の数学的理論」[4]を発表。それまで曖昧だった、通信によって伝えられる「そのもの」である「情報」の概念を明確化、その大きさである情報量を定式化したうえで、その考え方をベースに通信を扱う理論を提唱した。彼、シャノンが考案した理論はやがて「情報理論」と呼ばれるようになり、現在では、世の中で使われているすべての情報技術の礎となっている。コンピュータやネットワーク、暗号化などの情報セキュリティの技術も、全てが彼の理論のうえに成り立っていると言っても決して言い過ぎでは無いだろう。

さて、ここで人々が広く「セキュリティ」と呼んでいるそのものを考えてみよう。情報セキュリティに限らない、防犯、食やエネルギーの安定供給、国家の安全保障などの意味を含む「広い意味でのセキュリティ」[5]である。現在、「セキュリティ」に関しては、シャノンの理論が発表される前の通信と同様の状況にある。すなわち、「セキュリティが確保されているとき、行われていることの本質は一体何なのか」、「事故でセキュリティが崩れるときに、維持されないものは何なのか」などの問いかけに対する答は、まだ誰も見出していない。

往時の通信と同じで、このことは「セキュリティ対策が対症療法的になること」への、直接的、間接的な要因になっている。世の中でよく見られる「セキュリティ対策が“場当たり的”、“泥縄”になること」は、起こるべくして起こっているのだ。今般、この状況の打開を目指し、シャノンの考え方をベースにして、メタな観点から「セキュリティの何たるか」を読み解くべく試みた[6]。本稿[1]では、出来るだけ解りやすく、その概要を紹介する。

2．分野を限らない形のセキュリティの定義

セキュリティを、場当たり的な対応から解き放ち、エンジニアリングの観点から体系的に考えられるようにするためには、世の中でセキュリティという言葉が使われているあらゆるケースを言い当てる形で「セキュリティとは何か」について定義する必要がある。

食糧やエネルギー供給に支障が生じると、一国の政府は国を円滑に運営することが難しくなる。それゆえ食やエネルギーの安定供給は、「国家のセキュリティ（安全保障）の問題」となる。情報セキュリティにおいては、情報の「機密性」、「完全性」、「可用性」が担保されない状況では、組織はビジネスの円滑な運営が難しくなる。それゆえこれらの担保は、「その組織にとってのセキュリティの問題」となる。

これらの例から解るように、セキュリティという概念は、その分野によらず「どのような事件や事故が起こ

[1] 本稿の内容は、筆者の私見であり、必ずしも筆者の勤務先の見解と一致するものではない。

ろうとも、対象となるオペレーション（OP）が、あらかじめのプラン通り円滑に運営できていること」と一般化することができる [5]。本稿では、これを「セキュリティの定義」と位置付け、これをベースにしてその本質を考えていく。

3．オペレーションの前、プランニングのフェーズにおけるセキュリティ対策

「OPがあらかじめのプラン通りに円滑に運営されていること」実現の第一歩は、そのプランにある。そもそものプランにOPが波瀾万丈になる要因が隠れている場合、「OPの円滑な運営」を恒常的に行うこと（すなわちセキュリティの維持）は難しくなる。

劇を例に考えよう。波瀾万丈の劇（OP）は、一寸先は闇、何が起こるか判らないため、見ている方は面白いかもしれないが、劇中の人物は心が休まる暇がない。すなわち、この場合のセキュリティレベルは低い。一方、何も事件や事故が起こらない、つまらない劇（OP）では、淡々とした日常が繰り返され、見ている方は退屈かも知れないが、この「つまらない劇」の劇中人物は安心して日々を送れる。すなわち、この場合のセキュリティレベルは高いということになる。それでは、どうしたら劇から波瀾万丈の要素を取り除き、つまらなくできるか。そのためには、まずは何と言っても「シナリオをつまらなくすること」である。

ここで、シャノンが見出した情報という観点から考えてみよう。「波瀾万丈のシナリオ（OPプラン）」は、様々な出来事が起こることから「シナリオ全体を平均的に見た場合の情報量」は多い。一方、「つまらないシナリオ」は、何も変わったことが起こらないため「平均的な情報量」は少ない。このことは「多くの楽器が様々な形で登場する大編成オーケストラの交響曲」の複雑で分厚い楽譜と、「子どもがピアノを始めたばかりのバイエル練習曲」の単純でわずかな分量しかない楽譜を想像すると直観的に理解できるだろう。もちろん、「平均的な情報量」は、前者は大きく、後者に関しては小さい。

「OPプランというシナリオをつまらなくすること」、すなわち「OPプランの“平均的に見た情報量”を小さくすること」は、OPを行う前、プランニングの段階で、変わったこと（波瀾万丈につながる事件や事故）を「出来るだけ起こらないようにする」（Risk Mitigation: 事故の生起確率の低減に相当）、「もし起きたとしても大事件に至らないようにする」（Crisis Management: 事故発生時のOP致死率の低減に相当）こと [7]である。

「OPのプランから波瀾万丈の要因を取り除くこと」、「OPを劇とみなした場合、淡々と進む、見ていてつまらない劇にすること」、「その劇（OP）のシナリオ（OPプラン）の“平均的にみた情報量”を小さくすること」、これらはすべて同じことである。これらをビジネスのプランニングフェーズにおいて行うこと、これがビジネス分野においてBCP: Business Continuity Planningと呼ばれているセキュリティ対策の本質である。

4．シャノンの通信モデル

さてここで、情報を伝える手段である「通信」について、シャノンがどう考えたかを簡単に紹介しよう。彼が通信の本質を明らかにする際にベースとした「通信のモデル」[4]を図1に示す。情報に関する一大理論体系の大本にもなっているのがこのモデルである。

このモデルでは、まず「①送信情報（メッセージX）」が「②送信器」に送られる。送信器ではそれを「③信号」の形に変換した後、「④通信路」に送り出す。その通信路では「⑤ノイズ源」からある確率で発生した「⑥ノイズ」が混入することがあり、そのノイズが混入したかもしれない信号が「⑦受信信号」として「⑧受信器」でキャッチされる。受信器では、その信号を情報の形に戻して、それを「⑨受信情報（メッセージY）」とする。

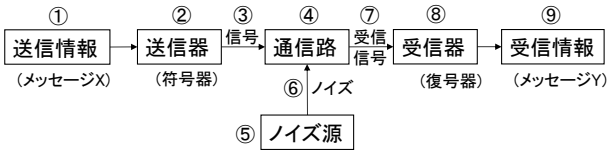


図1　シャノンの通信モデル

「ある地点で選ばれた“送信情報（メッセージX）”を、“受信情報（メッセージY）”の形で，別の地点で正確にまたは近似的に復元すること」、このモデルを元にした、シャノンによる通信の定義 [4]である。もし、「④通信路」に「⑤ノイズ源」からの「⑥ノイズ」が全く混入しなかったとしたら、「⑧受信器」で復元した「⑨受信情報（メッセージY）」は、「①送信情報（メッセージX）」と同じになるはずである。しかしながら、実際には、通信路では大なり小なりノイズが混入し、メッセージYはメッセージXと正確に同じにはならない。この場合、「送信側のメッセージXの情報量から、ノイズによって失われた情報量を差し引いた情報量」が、「通信で伝達できた情報量」である。

5．オペレーションの最中、実施のフェーズにおけるセキュリティ対策

さてここで話を元に戻し、今回の「セキュリティの定義」に則ったOPのモデル [6]を考えよう。今回の定義では「あらかじめのOPプラン通りの円滑なOPが行われていること」が、セキュリティが維持出来ていることだったので、OPの実施状況を評価するために、それを記録することを考える。この場合、OPのモデルは図2に示した通りになる。

このモデルでは、まず「①OPプラン（メッセージX’）」がOPの「②実施者」に渡される。実施者は、それに則る形で「③OPプランを具現化するための行為」を「④実世界」に対して起こし、そのOPを実施しようとする。その際、OP阻害の潜在要因である「⑤リスク」から「⑥インシデント（事故）」が発生し、実世界で行われようとしているOP実施行為に影響を与えることがある。その結果、実現されるのが「⑦実際に行われるOP」である．これを「⑧観察者」が観測し「⑨OP実施記録（メッセージY’）」として記述するというのがこのモデルである[2]。なお、実施者はOPプランに完全に忠実な形で実世界に働きかけ、観察者は実際に行われているOPを一切の加除無く記述するものとし、エラーは、全てOPに関係するリスクとインシデントの要素に帰することを仮定している。

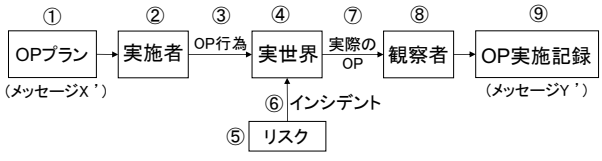


図2　セキュリティを考える場合のOPのモデル

図1の「シャノンの通信モデル」と図2の「セキュリティを考える場合のOPモデル」を見比べて欲しい。①～⑨のそれぞれの要素が一対一で対応しており、両者の構造には「同一性」があることが理解できるだろう。この通信モデルとOPモデルの同一性から、一般化したセキュリティの概念、すなわち「あらかじめのOPプラン通りの円滑なOPが行われていること」は、次のように理解することが可能となる。

通信では、受信情報（メッセージY）が、送信情報（メッセージX）に類似していればしているほど、ノイズが少ない「良い通信」が行われているということであった。これと同様に、「実世界において行われるOPの実施記録（メッセージY’）」が、「OPプラン（メッセージX’）」に類似していればしているほど、事故が少ない、すなわちセキュリティが高く維持された「良いOP」が行われていることになる。

ここで、通信モデルとOPモデルの同一性を使って、先のシャノンの「通信の定義」を読み替えてみよう。この読み替えにより、セキュリティを維持する対象としての「OPの何たるか」を知ることができる。セキュリティを考える際のOPとは「あらかじめのプランに記述された所作を，実世界において正確にまたは近似的に出現させること」に他ならない。

もし、「④実世界」において、「⑤リスク」が具現化して姿を現す「⑥インシデント」が全く起こらなかったとしたら、「⑧OP観察者」が記録した「⑨OP実施記録（メッセージY’）」は、「①OPプラン（メッセージ

[2]「“①楽譜”が “②演奏者”に渡され、“⑦奏でられた音”を “⑧採譜者”が耳で聞いて再び “⑨楽譜”に落とす」例を考えると解りやすいだろう。

X’）」と同じになるはずである。しかしながら、実際には、実世界では大なり小なり何らかのインシデントが発生し、メッセージY’はメッセージX’と正確に同じにはならない。この場合、「OPプランの情報量からインシデントで失われた情報量を差し引いた情報量」が、「実際のOPで実現できた“OP実施度合い”」となる。

この「OP実施段階において事故（インシデント）が起こった場合の影響度を下げ、実際のOPで実現できた“OP実施度合い”を大きくすること」が、ビジネス分野においてBCM: Business Continuity Managementと呼ばれているセキュリティ対策の本質である。

BCPとBCMは、しばしば同じ取組の前半と後半のような形で捉えられ、必ずしも明確に区別されてはいない。しかしながら、両者は適用される先、そしてそのフェーズが異なっている。BCPは「OPの計画段階で、プランを検討し、そこに内在する波瀾万丈の要因を小さくすること」、一方BCMは「OPの実施段階で、OPそのものをマネジメントすることで、“OPプラン”と“OPの実際”間に存在する差異を小さくすること」である。

再び劇の例で考えよう。劇では、シナリオ（OPプラン）から波瀾万丈の要素をできるだけ取り除いた（BCP）としても、その上演（OP中）において何らかの事故が起こる可能性はゼロには出来ない。それゆえ、上演中の状況にも注意し、様々な対応を行うことで、劇の「シナリオと実際との差異を出来るだけ小さく」なるようにしよう（BCM）ということである。

6．おわりに

通信を考える道具である情報理論では、本稿で取り上げた「送信側の平均的な情報量」、「ノイズ」、「通信で伝達できる情報量」は厳密に数式（数理モデル）化されている。「通信モデル」（図1）と「セキュリティを考える際のOPのモデル」（図2）の同一性から、セキュリティにおいてこれらに対応する「OPプランの平均的な情報量（波瀾万丈の要因がどれほど内在しているか）」、「インシデント」、「OP実施度合い」も、情報を扱う場合と同様の数式（数理モデル）で表すことが出来る。また、今回示した「通信とOPとの構造的な同一性」は、これら3つの場合に限定されずに常に成り立つことから、情報理論の数式（数理モデル）は、セキュリティを考える際の数学的な道具としても活用することが可能となるといえる。

このことは、セキュリティを体系的に、工学的に扱ううえで，大きな便益をもたらすはずである。これまで情報を扱うために情報理論の分野で案出されてきた様々な技法を、BCP/BCM、ISMSなどにおいて、セキュリティを考えるための道具として、そのまま活用することが出来るようになるからである。

一般化すれば、セキュリティとは「OP中に現れる（可能性のある）波瀾万丈（インシデント、事故）の影響を、ある許容レベルを超えないように低減し、それを保つこと」である。これは「OPの秩序を作り出し（BCP），それを維持すること（BCM）」と同義である。すなわち、セキュリティとは，ある「プラン」（すなわち前もってのルール）の下で、OPがどれほど秩序立っているかで評価されるべきものとなる。それゆえ、あらゆる分野において、セキュリティのための対策は、「OP実施前の施策（BCP）、そしてOP実施中の対応（BCM）によって、OPをどれだけ秩序立たせたか」で定量的に評価される対象となる。（そして、これらの評価に関する詳細は情報理論において既に示されている）

シャノンを祖とする情報理論では、情報の尺度を「メッセージを選ぶ際の自由度」[4], [8]としており、情報の「意味」は扱っていない。このことから情報理論は「情報の意味」によらずに成り立つ理論となっている。（そのため、「男の子が生まれた」、「コイン投げで表が出た」という2つの情報の大きさは同じとして扱われる）

通信モデルとOPモデルの同一性から、これと同様のことがセキュリティについても言える。きわめて抽象化した視点からは、セキュリティの大きさとは、「対象OPの状態が取りうる自由度」だけで決まる尺度であり、それにはOPの種類は関係ない。それゆえ、今回紹介した考え方は適用先を選ばない。JNSAのメインスコープである情報セキュリティに留まらず、防犯、組織における不正、食やエネルギーの安定供給、国家

の安全保障など、およそ「セキュリティ」という言葉が現れるすべての場面に適用できるということである。

究極まで抽象化すると、「セキュリティの大きさ」は「OPが取りうる状態に関する“場合の数”のみによって決まる値」であり、セキュリティ対策とは、「OPが取りうる状態の場合の数を少なくすること」、すなわち「OPの自由度を小さくすること」に相当する。それゆえ、OPに内在する自由度の減少分が、対象となるOPに施されたセキュリティ対策を定量化した尺度になるわけである。

パスワードの設定や、施錠、新たなルールの策定や監査の徹底など、セキュリティの対策は、その種類や分野によらず、それをすると「自由が制限されて利便性が失われる」という声を聞くことがある。これは、「OPに内在する自由度を減少させる」というセキュリティ対策の本質に関係して宿命的に起こっていることである。「OPに内在する自由度を減らす」ことで、必然的に「インシデント（事故）が起こる自由度」も減少するがゆえに、その対策はセキュリティのための対策となる。

本稿の主旨は、シャノンによる「通信の理論」の視座から見た「セキュリティの本質」に関する理解 [6]を概説することであった。文脈依存性を排した「一般化したセキュリティ」を、「OPを阻害する波瀾万丈があろうとも、あらかじめのプランに則った円滑なOPがなされていること」とし、それを「通信とOPの同一性」の観点から見ることで、セキュリティはあいまい性を排して理解出来る対象となる。また、そこに「通信の理論」として考案された情報理論を適用することで、セキュリティは体系的に扱うことが出来るようになり、エンジニアリングの対象にもなり得る。

本稿が、様々な分野の色々な場合において、セキュリティを科学的に分析、考察し、実現するためのきっかけとなれば幸いである。

本稿は、世の中において様々な形でセキュリティに関わっているできるだけ多くの方に「セキュリティの本質」を直観的に理解して頂くことを意識し、内容については例示を多用した簡単な記述に留めている。本稿の詳細に関しては文献 [6] を参照頂きたい。

【参考文献】

[1] ハワード・ラインゴールド（日暮雅通訳）：新・思考のための道具　知性を拡張するためのテクノロジー その歴史と未来，第6章「情報の中にあるもの」，パーソナルメディア (2006)
"Tools for Thought" by Howard Rheingold　http://www.rheingold.com/texts/tft/06.html#Chap06

[2] 高岡詠子：シャノンの情報理論入門　価値ある情報を高速に、正確に送る，講談社 (2012)

[3] ジミー・ソニ，ロブ・グッドマン（小坂恵理 訳）：クロード・シャノン　情報時代を発明した男，筑摩書房 (2019)

[4] Shannon, E. C.: A Mathematical Theory of Communication, Bell Labs Technical Journal, Vol.27, No.3, pp.379-423, No.4, pp.623-656 (1948)　http://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

[5] 甘利康文：セキュリティの本質　医療／医学，そして技術は何のためにあるのか，日本情報経営学会誌 Vol.38, No.3, pp.40-52 (2018)　https://doi.org/10.20627/jsim.38.3_40

[6] AMARI, Yasufumi: Comprehending Security through Shannon's Communication Model, International Journal of Affective Engineering, Vol.19, No.3, pp.177-187 (2020)　https://doi.org/10.5057/ijae.IJAE-D-19-00021

[7] 甘利康文：「リスクの本質」を考える体系構築のために，リスク工学研究，Vol.16, pp.9-14 (2020)
https://www.risk.tsukuba.ac.jp/pdf/bulletin16.pdf#page=13

[8] Weaver, W.: Recent Contributions to the Mathematical Theory of Communication,
http://waste.informatik.hu-berlin.de/Lehre/ss11/SE_Kybernetik/reader/weaver.pdf (1949)
文献[4], [8]は、書籍 “The Mathematical Theory of Communication,” University of Illinois Press (1998)として出版されている。そのWeb版は以下にて公開されており、邦訳版も上梓されている。
https://pure.mpg.de/rest/items/item_2383164/component/file_2383163/content
（邦訳）クロード・E. シャノン，ワレン・ウィーバー（植松友彦訳）：通信の数学的理論，筑摩書房 (2009)

セキュリティアウェアネスとは何か

日本電気株式会社
宮崎　駿

はじめに

コロナ禍でフィッシングや標的型攻撃など、メールを利用して、受信者を起点に侵害をしようとする攻撃が増えています。攻撃が比較的容易なうえ、セキュリティ対策が疎かになりがちな「人」を対象とした攻撃であるため、組織はこれを大きな脅威として認識する必要があると思います。

このような、人を狙った攻撃への対策としてセキュリティアウェアネス（Security Awareness）というものがあります。

ここでは、セキュリティアウェアネスとは何かをNIST SP 800-16 Information Technology Security Training Requirements: a Role- and Performance-Based Model（以下、NIST SP 800-16）[1]とNIST SP 800-50 Building an Information Technology Security Awareness and Training Program（以下、NIST SP 800-50）[2][3]から考えていきたいと思います。

セキュリティアウェアネスとトレーニング

セキュリティアウェアネスの定義をNIST SP 800-16より引用します。

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.

理解のために、IPAが公開しているセキュリティ関連NIST文書の日本語訳の中でSP 800-16と関連の深いNIST SP800-50より引用します。

意識向上はトレーニングではない。意識向上を掲げる目的は、単純にセキュリティへ意識を向けることである。意識向上は、各自がIT セキュリティの問題を認識し、適切な対応を行うことを意図したものである。

引用にある通り、セキュリティアウェアネスとは人がなんらかのITシステムを利用するときに、セキュリティ上のリスクの理解や問題が発生したときの正しい対処を"意識"させるものだと解釈できます。

※NIST SP 800-16の内容・文脈から引用にあるAwarenessはSecurity Awarenessと同義だと解釈しています。

※以後、単にアウェアネスとしている場合はセキュリティアウェアネスも指していることとします。

言葉のニュアンスが難しいところではありますが、あくまで“意識”させるものであり、“できるようにすること”を主眼とするものではないというところがポイントだと考えています。アウェアネスは日本語訳では意識向上と訳されており、具体的なアウェアネスの取り組みとしてはポスターやチラシなどが挙げられています。このことからもあくまで意識付けの意味合いだということがわかるかと思います。

アウェアネスについて「意識付けだけでは対策として不十分ではないか」という意見があるかと思います。実際に“できる”ようにすることにはトレーニングが当てはまります。
NIST SP 800-16、およびNIST SP 800-50ではアウェアネスとトレーニング、教育の関係性について示されています。

トレーニングの定義をより簡潔にまとめているNIST SP 800-50より引用します。

Training strives to produce relevant and needed security skills and competencies.
トレーニングでは、関連性のある必要なセキュリティスキルおよび能力を生み出すように努める。

引用にある通り、トレーニングとは人に必要なスキルを習得させるように仕向けるものだと解釈できます。そのため、例えば従業員が標的型攻撃メール等に適切に対処できるようになってほしい場合はそのためのトレーニングを受けさせれば良いということになります。

アウェアネスとITセキュリティリテラシー

ここで、アウェアネスとITセキュリティリテラシーは何が違うのかという疑問があるかと思います。
ITセキュリティリテラシーについて、NIST SP800-16より引用します。

IT Security literacy refers to an individual's familiarity with—and ability to apply—a core knowledge set (i.e., "IT security basics ") needed to protect electronic information and systems.
（筆者訳）：ITセキュリティリテラシーとは情報とシステムを守るのに必要となるコアな知識体系（つまりITセキュリティの基本）を理解していて、それを実践できること。

アウェアネスはセキュリティの体系的な知識の理解と実践ができることを目指しているわけではなく、業務上のどういう場面でセキュリティのリスクの問題があり、そこでどういう対処が適切なのかを意識させることだと考えています。

ITセキュリティリテラシーは基本的な情報セキュリティの体系的な知識の習得ということなので、ITセキュリティリテラシーができているイメージとしては「基本的なセキュリティの教科書をやったから基本はおさえているよ」というのが近いと思います。

セキュリティアウェアネストレーニング

アウェアネスとトレーニングは異なるという話をしました。しかし、セキュリティアウェアネスというキーワードでWeb検索すると、様々な企業がセキュリティアウェアネストレーニングという名前で有償のトレーニングを提供していることがわかります。アウェアネスとトレーニングは違うもののはずですが、セキュリティアウェアネストレーニングとは何でしょうか。。

ここで、2019年に撤回されている資料（Retired Draft）のため参考情報となりますがNIST SP 800-16 Rev.1 A Role-Based Model for Federal Information Technology/Cybersecurity Training(3rd Draft)（以下、NIST SP 800-16RD）[4]よりアウェアネストレーニング（Awareness Training）の定義を引用します。なお、NIST SP 800-16RDではAwareness Trainingとは別にAwarenessとTrainingが定義されているため、AwarenessとTrainingという2つの用語を並べているというよりは、Awareness Trainingで一つの用語だと考えたほうが良いと思います。

Awareness Training – consists of instructor led, on-line courses, exercises or other methods that inform users of acceptable use of and risk to the organization's organizations systems.
（筆者訳）：意識向上トレーニング -インストラクター付きのオンラインのコースやエクササイズなどの方法で行われるトレーニングです、トレーニングでは組織のシステムで許容される操作とリスクについて示されます。

NIST SP 800-16RDはNIST SP 800-16を置き換える予定だった文書です。NIST SP 800-16は発行日が1998年であり今から20年以上前のものです。このことから一時はNIST SP 800-16の内容は現在の社会の状態に照らし合わせるとそぐわないと考えられていたと思います。

NIST SP 800-16が公開された当時としてはそれほどITシステムの利用者全員にセキュリティのトレーニングを強制するほどの社会状況ではなく、意識向上の取

り組みだけで済んでいたのだと思います。しかし、昨今のフィッシングや標的型攻撃メール、ソーシャルエンジニアリングなど、当時に比べて社会の状況は劇的に変化しています。これまでは意識付けだけで済ませていた内容について、スキルとして習得してもらう必要性が出てきたのだと考えています。そのため、それを表すための用語としてアウェアネストレーニングが定義されたのだと思います。

そして、このアウェアネストレーニングがセキュリティアウェアネストレーニングという名前で、有償で企業から提供されているということではないかと思います。

アウェアネスを向上させるにはどうすればいいのか

組織において、従業員のアウェアネスを向上させるにはどうすればいいのでしょうか。

その場の状況に応じてセキュリティに注意を向けることを人にさせるというのは、人の意識関わることであるため一朝一夕でできることではありません。
当人にセキュリティの関心があるのであれば、日常的にセキュリティに注意を向けることも考えられます。
しかし、セキュリティに関心がない人の方が多いのが現実だと思います。

関心の有無にかかわらず人のアウェアネスを向上させるためのポイントとしては「当たり前にする」ということだと考えています。
当たり前のことは関心があるかどうかに関わらず、当たり前のこととして意識すると思います。

では、当たり前のことにするためにはどうすればいいのでしょうか。

結論としては、ターゲットとする人にとって受け入れられやすい形で繰り返し伝えていくことだと思います。
例えば、NISC（内閣サイバーセキュリティセンター）はサイバーセキュリティ月間というキャンペーン[5]を行い、国民全体のアウェアネス向上に取り組んでいます。

このキャンペーンの中で取り扱われているポスターとバナーにアニメ作品が使われています。

これは、ターゲットとする人の多くがこのアニメ作品に関心があり、受け入れられやすいという想定の元、このアニメ作品を使ったのだと考えています。

このように、ターゲットとする人にとって受け入れられやすい形でメッセージを伝えていくことで、それが当たり前のことだと刷り込まれていき、アウェアネスの向上につながると思います。

そして、繰り返しになりますが、それを確実に身に着けさせる取り組みがセキュリティアウェアネストレーニングになります。

まとめ

ここで、アウェアネスとITセキュリティリテラシーとトレーニングについて、交差点を渡るということを例にそれぞれがどう機能するかを示して、違いをまとめます。

アウェアネス：青信号の交差点を渡っていても、右折してくる車はあるかもしれないという事を知っていて、「気を付けなきゃ」と思える　（そういうセンスをトレーニングするのがアウェアネストレーニング）

ITセキュリティリテラシー：具体的な確認の仕方、右見て左見て、もう一度右を見るという事を知っている

トレーニング：実際に交差点を渡る場面で、右見て左見て右を見ることができる（セキュリティ）スキルを習得させる。

このように自分なりに例に当てはめてみると違いが理解しやすくなると思います。

最後に、巧妙な手口と呼ばれるサイバー攻撃は人を起点にしているケースが多いのではないかと感じています。人はどうしてもミスをする可能性があるため、組織の最も脆弱な部分になってしまうことが多いです。

現状、人を起点にしたサイバー攻撃は増加しており、今後セキュリティアウェアネストレーニングがより求められることになるのではないかと感じています。技術で組織を守れる範囲は今後より広がるだろうとも考えられますが、どうしても人がケアしなければならない領域は残ると思います。ITの発展に合わせて技術だけでなく、人もセキュリティのレベルを上げていくことができれば社会はより安定して発展するだろうと思います。

本記事が少しでもみなさんの役に立ち、安全・安心な社会に少しでも寄与することを願っています。

【参考文献】

[1] https://csrc.nist.gov/publications/detail/sp/800-16/final
[2] https://csrc.nist.gov/publications/detail/sp/800-50/final
[3] https://www.ipa.go.jp/files/000025333.pdf
[4] https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/archive/2014-03-14
[5] https://www.nisc.go.jp/security-site/month/index.html

プライバシー規制の強化や有事対応に対するInformation Governanceの有効性について

EY 新日本有限責任監査法人 Forensics 事業部マネージャー
公認不正検査士　池上　弘樹

1. はじめに

クラウドサービスの浸透やデジタルトランスフォーメーション（以下、DX という）の推進により、企業の保有するデータ量が加速度的に増加している一方で、2018 年に施行された「EU 一般データ保護規則（GDPR：General Data Protection Regulation）」を契機として、主なものだけでも米国カリフォルニア州、日本、インド、ベトナムなどのアジア諸国、ニュージーランド、ブラジルなど個人情報保護法の制定や強化の動きが加速しており、有事に企業が求められる対応は厳格なものへとシフトしています。インシデント発生時の混乱の中、ルールで定められた期限内の対応と適切な情報開示と通知を行うことは非常に難しくなっており、対応不備による規制当局からの制裁金や訴訟を回避するためにも、有事対応への備えとしての Information Governance（以下、I.G. という）の必要性が増しています。本稿では、この I.G. の概要と有事を見据えたリスク低減の例について解説を行います。

2. Information Governanceとは

Information Governance という言葉は広い意味で使われることが多いですが、一般的には企業や組織が保有している全ての情報をコントロールし、様々なリスクを低減した上で、適切なデータの利活用を促進し、企業の成長や戦略に利用するための枠組みや取り組みであると言えます。

今日の企業が抱える情報資産は、顧客データ、業務データ、財務データなど多岐にわたります。IT ハードウェアの進化、企業の DX 推進に伴うデータ量の爆発的な増加で得られる新たな石油[1]ともいわれる情報資産は、企業にとっては上手く活用すれば企業戦略の要となる一方、取り扱いを間違えると、致命的なリスクにもなると言えます。こうしたリスクを低減するためには、それぞれのデータやシステムに対して、適切なポリシーを適用し、対応措置（ガバナンス）の仕組みを確立し、コントロールすることが求められます。これにより適切で効率的なデータ活用が可能になり、持続可能な経営戦略を構築していくことが可能になります。デジタル技術による社会、競争環境の変化がもたらす影響（リスク・機会）を踏まえた経営戦略の策定は、昨年経済産業省が発表した、“デジタルガバナンス・コード”[2]でも柱となる考え方とされており、どの企業にとっても今後取り組むべき課題と言えます。

3. Information Governance Reference Model

Information Governance Reference Model（以下、IGRM という）[3]は、アメリカの任意団体、Electronic Discovery Reference Model[4]（以下、EDRM という）が策定した、I.G. についての参照モデルであり、その目的は、企業や組織が効果的かつ実用的な I.G. プログラムを実装するための、柔軟なフレームワークを提供することです。IGRM は、EDRM フレームワークの情報管理の部分にフォーカスし、構築するだけが目的ではなく、データ管理、コンプライアンス、IT インフラなど組織を横断的に管理する拡張可能な概念になります。

I.G. について何かから手を付けていいのかわからない、もしくは組織が現在どの程度 I.G. について

[1] Robert F. Smallwood：Information Governance　-Concepts, Strategies and Best Practices. P.5

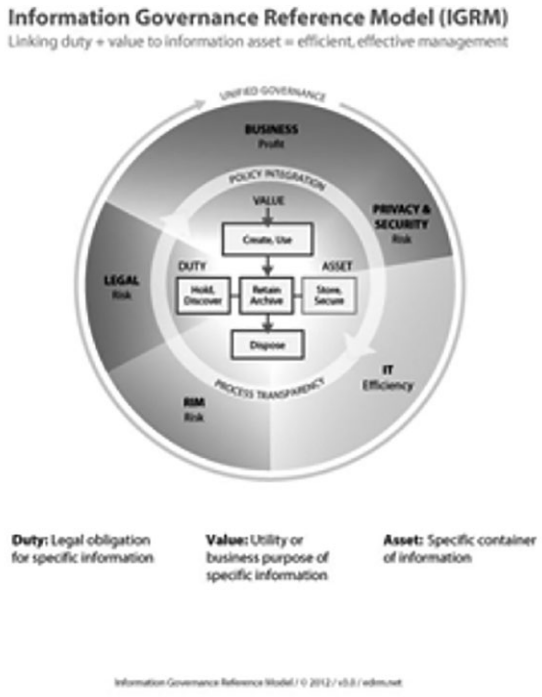
[2] https://www.meti.go.jp/shingikai/mono_info_service/dgs5/pdf/20201109_01.pdf

[3] https://edrm.net/resources/frameworks-and-standards/information-governance-reference-model/

[4] https://edrm.net/
EDRMは、弁護士、裁判官、社内弁護士、その他の法律専門家、eDiscoveryベンダー等で構成され、電子情報開示、プライバシー、セキュリティ、および情報ガバナンスを向上させる実用的なグローバルリソースを作成しており、国際的な指標となっています。

取り組みが出来ているかを評価する意味でも、この参照モデルは有効に活用できます。また、IGRMは法務やITだけが活用するものではなく、この図をハブとして、経営層から各部署に渡り、横断的コミュニケーションを促進することを推奨しています。

この図が表現している通り、常にデータプライバシーやセキュリティの最新状況に配慮し、規定を最新の状態に保ち、保持しているデータの整備を実施し続けるサイクルを回し続けることが成功するI.G.の体制と言えます。



[5] Information Governance Reference Model（IGRM）

アメリカの市場調査会社、International Data Corporation（IDC）が2020年5月に行った発表によると、今後3年間に作成されるデータ総量が、過去30年間に作成されたデータ総量よりも多くなり、過去5年間で作成されたデータの3倍以上のデータが作成されるとしています。[6]

データ量の爆発的な増加の背景として、企業のDX　推進、5G、ブロックチェーン、AR（拡張現実）/VR（仮想現実）、AI/ 機械学習、IoTなどのテクノロジー、またここ1年間はコロナ禍の中、動画ストリーミング量の増加や、企業が在宅勤務を推進した結果、データ通信量が増えたことも影響していると言えます。

この爆発的なデータ量の増加に伴うリスクの増大に企業は対応することが求められます。保有するデータをいかに管理し、統制していくか、つまりI.G.の構築、実現は、企業にとって急務であると言えます。

4. Information Governanceが求められる背景 ーリスクへの対応ー

前項で述べたデータ量の爆発的増加に加え、贈収賄や談合（カルテル）などの法令違反リスク、情報漏洩や不適切会計などの不正リスク、海外当局調査や訴訟などの法的リスク、GDPRを始めとしたデータプライバシー規制への対応など、企業は様々なリスクへの対策と有事対応を求められます。

こうしたリスクへの対策の一例として以下の5点を紹介します。

・データマッピング
・重複・古いデータの戦略的削除
・文書管理規定の見直しとアップデート
・データ抽出方法の確認
・データプライバシー規制への対応

[5] https://edrm.net/resources/frameworks-and-standards/information-governance-reference-model/

[6] https://www.idc.com/getdoc.jsp?containerId=prUS46286020#:~:text=08%20May%202020-,IDC's%20Global%20DataSphere%20Forecast%20Shows%20Continued%20Steady%20Growth,Creation%20and%20Consumption%20of%20Data&text=By%202024%2C%20IDC%20expects%20this%20ratio%20to%20be%201%3A10

今回紹介するこれらの対策はあくまで１つの例であり、各組織や業界の実情などを鑑みたリスクに応じて、対策を検討することをお勧めします。

4-1．リスクへの対応：データマッピング

I.G. への取り組みのスタート地点として、まず組織内のデータの現状を把握することは非常に重要です。データの種類の把握（構造化データ、非構造化データ、紙文書など）、データ量の把握をシステム別、本社、子会社、海外子会社別に実施することで、組織内のデータの状態を視覚化し、現状の問題点の特定や各データやシステムの責任者の明確化、リポートラインの確立など様々な行動をとることが可能になります。

データプライバシー規制への遵守状況もここで確認できます。自社のデータが格納されているサーバはどこにあるのか、そして国内外からのアクセスを含め、誰がどこからアクセスできるのか、この点は非常に基本的な事ではありますが、全てを把握できている企業が多いとは言えないことは、昨今の報道されている事案などから明らかです。
また、企業が M&A を実施した際のシステム統合や新たなソフトウェアの導入といったイベントが起こる度にデータマップの更新をすることが必要です。継続的なデータマップの更新は効果的な I.G. を推進する上で非常に重要な要素となります。

4-2．リスクへの対応 - 重複：古いデータの戦略的削除

前述したデータ量の爆発的増加に伴い、企業が抱える重複データや、長年活用されていない古いデータも日々増えていきます。Compliance, Governance and Oversight Council（CGOC）が行った調査[7]では、企業が保有するデータのうち、約 69％はビジネスを行う上では必要がなく、削除を検討出来るという調査結果もあります。データマッピングの結果、識別された重複・古いデータについては積極的に削除していくことが重要です。データを抱えれば抱えるほどリスクも増加するということを念頭に、削除を日々実行していくサイクルを作ることも有効です。組織内のデータがスリム化することで、海外訴訟や当局調査の際求められる eDiscovery 対策にもなり、結果として物理的なサーバや倉庫のスペースの削減、情報漏洩リスクの低減、業務の効率化にも繋がり、コスト削減にも大きく寄与することになります。

また、一方でリティゲーションホールドについても配慮が必要です。リティゲーションホールドとは、訴訟や当局による調査が合理的に予見された時点で、関係者にデータや書類を廃棄せず保持することを通知する証拠保全の行動を意味します。このリティゲーションホールドを実施せず、意図的かどうかに関わらずデータを廃棄してしまったことが判明すると、裁判への妨害行為とみなされ、高額賠償等の懲罰的措置が取られることもあります。

この様に、どのデータを残し、どのデータを削除するのかを慎重に検討し、戦略的にデータの整備をしていくことは I.G. 体制を構築していく上で非常に重要なポイントとなります。

4-3．リスクへの対応：文書管理規定の見直しとアップデート

各産業の法規制や要請に対応した文書・データの保管、廃棄、共有等の規定が策定されているかの確認から始め、各子会社、海外子会社に至るまで実際の規定に沿った運用がなされているかの状況を確認していきます。運用状況を確認する過程で、形骸化している規定、規定が作られていない新しいシステムなどが見つかります。そのそれぞれに対して改善を実施し、同時に最新の法令や規制、各国地域のデータプライバシー規制にまで対応した規定をアップデートすることが求められます。

また、規定の見直し後は、定期的に運用状況をモニタリングし、データの廃棄履歴などの保管状況の監査を実施することも規定が再び形骸化するのを防ぐ意味でも重要なポイントとなります。

[7] Robert F. Smallwood：Information Governance　-Concepts, Strategies and Best Practices. P.6

4-4．リスクへの対応：データ抽出方法の確認

これまで述べてきたようなデータの管理を実施している企業はそれなりに多いかと思いますが、データの抽出までを整理し、把握出来ている企業は少ないはずです。不正調査、国際訴訟、当局調査の現場では、データ抽出を迅速に正確に行うことが求められます。特に日本、米国などの独占禁止法事案でのリニエンシー（課徴金免税制度）では、証拠を提出した順番で課徴金の免除もしくは減免額が決定します。このような例からも、平時からのデータ抽出方法の確認は、非常に重要な点の一つになっています。

具体的には、メール、その他システム毎の抽出方法や形式の確認、抽出にかかる時間のベンチマークを取っておくことが有効です。

4-5．リスクへの対応：データプライバシー規制への対応

EU の GDPR を契機として各国地域で様々なデータプライバシー規制が制定されています。まず、自社が影響を受けるデータプライバシー規制について把握した上で、各規制の要件に合わせた規定の改定、必要に応じてシステムの更新を実施します。また、各規制に違反した際の準備も重要です。GDPR を例に出すと、データ侵害の際の EU 監督機関への 72 時間報告義務が課せられます。また、データ主体からの削除要求などに対応できる体制も求められます。日本国内でも、改正個人情報保護法（2022 年 4 月～ 6 月施行予定）では個人データの漏洩が発生した場合、個人情報保護委員会への報告が義務化されます。

今年 1 月に法律事務所の DLA Piper の発表したレポート[8]によると、GDPR 関連で科された制裁金は総額で 1 億 5850 万ユーロ（約 200 億円）であり、それ以前の 20 カ月に科された制裁金と比べ 40%近くも増えています。この様に、データプライバシー違反による制裁金は今後も増加する傾向にあり、データプライバシー規制に対する体制の構築は企業にとって喫緊の課題だと言えます。

これらのデータプライバシー規制に対する体制を構築するには、プライバシーバイデザイン[9]の概念が参考になります。プライバシーバイデザインとは、プライバシーを取り扱うあらゆる局面で、情報が適切に適法に取り扱われる環境をあらかじめシステムや仕組みに取り入れて構築することを意味します。

また、データプライバシー違反とは何か、違反が発生した場合どう対応するべきか等を事前に検討し、さらに社員に継続的に教育を実施するといった、有事を見据えた体制の構築が求められます。

5. おわりに

昨今度々耳にするサイバーインシデントや、情報漏洩などの有事は、100%全てを回避することは不可能です。何か事が起きた際に適切に素早く行動に移すことが出来る体制を整えておくことは、どの企業にとっても非常に重要な課題だと言えます。また、I.G. はひと時のプロジェクトではなく、継続して取り組むことが非常に大切です。日々データが増大し、テクノロジーの進化、新たな規制や法令が現れるなかで、I.G. も時代や組織の実情に合わせて、細かな調整を日々実施していくサイクルをつくることが重要です。本稿が皆様の Information Governance 検討の一助となれば幸いです。

【参考文献】

[1] Robert F. Smallwood著：Information Governance -Concepts, Strategies and Best Practice-

[2] DAMA日本支部 Metafindコンサルティング株式会社監訳：データマネジメント知識体系ガイド　第二版

8 https://blogs.dlapiper.com/privacymatters/dla-piper-gdpr-fines-and-data-breach-survey-january-2021/

9 https://www.soumu.go.jp/main_content/000196322.pdf

JNSA ワーキンググループ紹介

中小企業支援施策 WG

トレンドマイクロ株式会社
中小企業支援施策 WG リーダー　岩本　真人

■ 発足の経緯

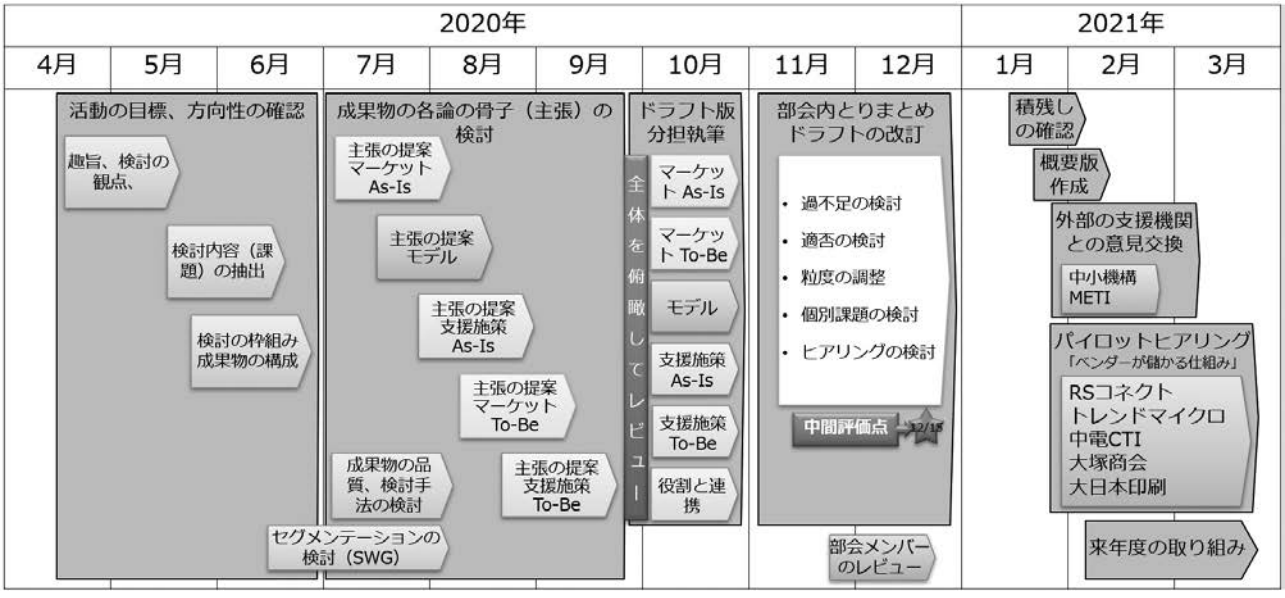
中小企業支援施策WGは、昨年4月に社会活動部会の下、中小企業対策支援施策検討会としてスタートしましたが、今年度からは名称も変えWGになりました。

本WGは、当初、以下のような疑問に答えることを目指して検討を開始しました。

- 中小企業層でのセキュリティ対策が進まない（バラツキが出る）原因は何か？
- それを打破する支援施策にはどのようなものがあるのか？（国や自治体の機関、商工団体、士業などの支援者、ITベンダーなどによる支援施策）
- それらの支援施策は有効か？ 効率良く成果に繋がっているのか？
- 中小企業による情報セキュリティ対策の導入を支援する施策はどうあるべきか？
- では、我々セキュリティベンダーが出来ることは何か？他の支援機関/支援者と何をどの様に協働できるのか？

■ 2020年度の活動

昨春の活動開始から、ほぼ月2回の定例オンラインミーディングや、タスクベースのアドホックミーティングを実施し、下図のようなスケジュールで上述の疑問への答えを探す検討を進めてきました。



昨年末には、検討内容を取り纏めた文書を作成しました。以下はその内容（目次）です。

1. はじめに
2. 中小企業の情報セキュリティの現状と課題
   - 2.1 中小企業の業務、IT利活用の現状
   - 2.2 中小企業を取り巻く情報セキュリティの環境とその変化
   - 2.3 中小企業の情報セキュリティ対策の現状と課題

3. 中小企業の情報セキュリティのあるべき姿
   3.1 情報セキュリティ対策の目的
   3.2 情報セキュリティのコストについて
   3.3 経営者の取り組む姿勢について
   3.4 求められる対策レベルについて
   3.5 企業の特性に応じた対策基準について
   3.6 対策状況の証明（説明）について
   3.7 IT利活用と情報セキュリティ対策
   3.8 適したセキュリティ対策ソリューションについて
4. 対策導入モデル
   4.1 対策導入モデルとは
   4.2 対策実施までのパス
   4.3 対策導入の動機
   4.4 プロセスの阻害要因
   4.5 望ましい対策導入モデル
5. 支援施策と施策展開の現状と課題
   5.1 現状のセキュリティ対策に対する支援策
   5.2 支援施策と支援展開の課題
6. 支援施策のあるべき姿
   6.1 中小企業に適した支援施策
   6.2 求められる具体的な支援施策
7. 支援機関/支援者の役割と連携
   7.1 支援機関/支援者の協働
   7.2 IT導入支援施策へのセキュリティ導入のバンドル
   7.3 支援機関/支援者に対する支援施策の整備

今年に入ってからはこの成果物を基にして経済産業省などの外部の支援機関/支援者との意見交換や、ベンダー数社から支援施策に対する要望などのヒアリングを行っています。

■ 今後の予定

今年度の活動開始に当たって、WGの活動の目的を以下としました。

- 中小企業の情報セキュリティ対策導入を促進する官民による支援施策の検討とその実践
- 中小企業の情報セキュリティ市場の拡大を捉えた、JNSA会員のソリューション展開への寄与

支援施策の検討と発信は昨年からの継続ですが、今年度はそれに加えて多くの関係する支援機関/支援者との協働による施策の実践を目指したいと考えています。具体的には、中小企業に対する支援機関に情報セキュリティ対策に関するコンテンツや人材支援の提供や、対策ガイドラインなどの支援施策の普及や活用に向けた取り組みなどを想定しており、WGメンバーの意向を踏まえ、順次、プロジェクト化していく予定です。そして、このような活動の成果として、中小企業の情報セキュリティ対策レベルが向上すると共に、中小企業向けの情報セキュリティ対策ソリューションという市場が拡大し、JNSAの会員の皆さんのビジネスにも良い影響をもたらすことを目指しています。

■ WG活動紹介資料

昨年度の活動内容を中心にWG紹介資料を公開しています。ご興味のある方は、下記のWG紹介ページにある「＞＞中小企業支援施策WGの活動紹介」のリンク先を参照して下さい。

https://www.jnsa.org/active/2021/act.html#smenp

■ メンバー募集

中小企業支援施策WGでは、随時、メンバーを募集しています。

以下のような会員の方にお薦めです。

- 中小企業向けのビジネスの拡大や自社製品のアピールをしたい、または、今後、この分野でのビジネス展開を考えている。
- 同じねらいを持つ他のメンバーや、外部の支援機関/支援者との情報交換、意見交換をしたい。

尚、本WGは（不幸なことに？）発足以来全ての活動がZoomやSlack、OneDriveなどを用いたオンライン開催で、その反面、テレワークが主体の方や地方に拠点を持つ方にも参加しやすいと思います。また、中小企業向けのビジネスの経験や情報セキュリティに対する知見が浅い方でも、個々の活動に参加できる方は歓迎いたします。

JNSA ワーキンググループ紹介

セキュリティ理解度チェック WG

キヤノン IT ソリューションズ株式会社
WG リーダー　西浦　真一

■ はじめに

セキュリティ理解度チェックWGは、利用者視点の情報セキュリティリテラシーの向上を目指し、JNSAが提供する「情報セキュリティ理解度チェックサービス」「理解度セルフチェックサービス」の継続的な問題の見直しを行うと共に、プレミアム版（有料サービス）のユーザー数増加に向けた対外活動を実施しています。また、プレミアム版利用者の増加に伴い、安定的に運用可能な環境の整備強化を検討することも目的として活動しているWGです。本WGは2010年に「セキュリティ理解度チェックWG」と名称を改めてから、今年で12年目を迎えます。今回は最近の活動内容と、提供しているサービス内容を中心に、WGの紹介をさせていただきます。

■ WGについて

組織の社員・職員がそれぞれパソコンやスマートフォンなどの情報端末を使用し、メールやSNSなどのコミュニケーションツールを使っての連絡やインターネットを利用して情報を受発信することが業務の重要な手段となってきています。そのような状況の中では、社員・職員1人ひとりが適切な情報セキュリティの知識を身につけて安全な利用を図ることは大変重要となります。このため、組織の管理者は自組織の社員・職員に対して、情報セキュリティに関する研修やテストを行い、リテラシー向上に努めていらっしゃるのではないでしょうか。当WGでは、組織の管理者が効果的な教育を行うことを目的に、自組織の社員・職員の情報セキュリティの理解度を測るためのサービスを提供しています。このため、本WGでは管理者ではなく、組織の一般ユーザーをターゲットとし、有事の際にどのように行動するべきかを問う問題を継続的に追加してまいりました。

昨年2020年は、突如として始まったコロナ禍において、感染者数が多い東京などの都市部を中心に、感染防止策の一環としてリモートワークを導入する組織が増加しました[1]。働き方改革として利点も多いリモートワークですが、組織の管理者にとっては、ユーザーそれぞれの自宅という、オフィス内での業務を想定した情報セキュリティ教育が通用しない環境におけるセキュリティ対策などの不安もあります。そこで、当WGでは、2020年の活動として、「ニューノーマル」、「リモートワーク（在宅勤務）」、「ビデオ会議ツール」をテーマにJNSA会員から問題を募集し、監査を行い追加しています。

■ サービスについて

- **情報セキュリティ理解度チェック（プレミアム版）　https://slb.jnsa.org/eslb/**
- **理解度セルフチェック　https://slb.jnsa.org/slbm/**

「情報セキュリティ理解度チェックサービス」の詳細は上記の公開ページをご覧いただくとして、本サービス最大の特徴は前述のとおり、多くの情報セキュリティに関連する検定やテストが、情報セキュリティマネジメントに関する業務や情報システムの企画・設計・開発・運用業務に就く管理者をターゲットに据えているのに対し、システムを利用

[1] 東京商工会議所 |「テレワークの実施状況に関する緊急アンケート」調査結果を取りまとめました～緊急事態宣言発令以降テレワーク実施率は67.3%と急増～　https://www.tokyo-cci.or.jp/page.jsp?id=1022366

する組織内の一般ユーザーをターゲットとしていることです。用語や法令知識を問うのではなく、セキュリティモラル・リテラシー向上に焦点を当て、有事の際にどのように行動すべきかを問う問題を揃えています。

このため、本サービスは多くの業種にてさまざまな職種の方にご利用いただいています。本サービスの利用者（プレミアム版の管理者）を業種別でみると、情報サービス（ソフトウェア、情報処理）が39.9%と最も高く、その他サービス業、製造業、卸売・小売業がそれに続きます（表1）。また、利用者（プレミアム版のユーザー）の職種別では、コンピュータ関連の技術者だけではなく、営業職や管理職、生産、総務・人事・法務など多くの職種の方にご利用いただいています。サービスで提供している問題に興味をお持ちの方は、無償で利用できる理解度セルフチェックサイトもありますので、ぜひ一度チャレンジしてみてください。
この情報セキュリティ理解度チェックサイトを、皆さまの組織の情報セキュリティ向上のための一助としてご活用いただければ幸いです。

表1　サービス利用者の職種（プレミアム版　管理者）

業　種	割合（%）
情報サービス（ソフトウェア、情報処理）	39.92
製造業	10.70
卸売・小売業	5.31
建設業	3.31
学校・研究所	3.25
金融・保険業	1.95
通信業（固定/移動電気通信）	1.72
公益法人・NPO・組合等	1.68
教育、学習支援業	1.66
運輸業	1.57
不動産業	1.25
医療、福祉	1.17
政府・官公庁	1.15
ISP、ASP	0.85
出版業、新聞業	0.81
電気業（発電、変電）	0.55
農業	0.47
飲食店、宿泊業	0.40
ガス業	0.38
放送業	0.38
漁業	0.09
鉱業	0.09
林業	0.08
水道業	0.08
熱供給業	0.06
その他サービス	14.72
その他	6.41

表2　サービス利用者の職種（プレミアム版　ユーザー）

職　種	割合（%）
コンピュータ関連の技術開発・研究	10.90
システム/ネットワーク管理者	4.16
設計・デザイン・クリエイティブ	4.76
コンピュータ関連その他	11.83
コンピュータ関連以外の技術研究・開発	1.88
管理職	7.70
生産	4.22
営業	11.04
総務・人事・法務	3.88
カスタマーサポート	3.18
経理・財務	2.17
その他専門職	3.73
学生	2.46
その他サービス	5.44
その他	22.65

JNSA ワーキンググループ紹介

■ 最後に

コロナ禍において組織における教育・研修の在り方は、大きな変更を迫られています。情報セキュリティリテラシーを含め、組織における集合研修の多くはコロナ禍において避けることが望まれる、「三密（密集・密接・密閉）」の環境で行われていました。その解決策としてオンライン教育サービスの市場規模は急拡大しているそうです。矢野経済研究所の調査によれば、国内におけるeラーニング（オンライン教育サービス）の市場規模は2016年に1767億円程度でしたが、2020年には2460億円規模まで成長していると予測[2]されており、今後も市場は成長していくと見られています。

当WGでは今後、より高まると考えられるサービスへの需要に応え、より良い設問の充実を図るためにも、共に活動していただける仲間を必要としています。本WGは会員交流部会に所属しており、WG活動を通じて仲間を作ることも本WGの大切な目的の一つです。また、一般ユーザーに求められる行動を想定し問題を作成する、既存問題をアップデートすることは新たな気づきにつながり、勉強にもなります（かく言う私も当初の参加目的は勉強でした）。コロナ禍の現在はオンラインミーティングが中心ではありますが、活動に興味がございましたら、お試しでも構いませんので是非お気軽にご参加ください。

WGメンバー

キヤノンITソリューションズ（株）	西浦　真一（WGリーダー）
（株）アズジェント	秋山　貴彦
（株）インテリジェントウェイブ	西谷　健二
（株）インテリジェントウェイブ	佐々木　謙一
グローバルセキュリティエキスパート（株）	萩原　健太
（株）日立ソリューションズ	扇　健一
富士通（株）	幸田　一生
ニュートラル（株）	小屋　晋吾
（株）ラック	長谷川　長一
（株）ラック	持田　啓司

WG協力者（問題監修委員会 委員）

情報セキュリティ大学院大学名誉教授/JNSA会長	田中　英彦
早稲田リーガルコモンズ法律事務所 弁護士/JNSA顧問	森山　裕紀子

[2] 矢野経済研究所|eラーニング市場に関する調査を実施（2020年） https://www.yano.co.jp/press-release/show/press_id/2404

会員企業ご紹介50

株式会社レオンテクノロジー

https://www.leon-tec.co.jp

レオンテクノロジーはセキュリティ診断やフォレンジック、コンサルティングなどサイバーセキュリティに不可欠なソリューションを総合的に提供致します。作業は自社のセキュリティエンジニアですべて完結しており、ソリューション間での連携を密にする ことで、幅広い知見で各業務にあたることが出来ており、様々な業種業態の企業様よりご評価頂いております。

サイバーセキュリティに不可欠なソリューションをワンストップで統合的に提供致します。

セキュリティ診断

脆弱性診断ではアプリケーションやネットワークに潜む脆弱性を網羅的に洗い出します。
報告会では、実際に診断したエンジニアが同席し対応させて頂きます。

【サービス例】
- 脆弱性診断(WEB、NW、スマホ)
- ペネトレーションテスト
- レッドチーム（TLPT）
- クラウドサービス診断（AWS、Azure等）

調査・解析

情報漏えい・内部不正・ウィルス感染などのインシデントの全容を解明すべく、ヒアリングからエンジニアによる調査まで対応させて頂き、対策の立案も行っております。

【サービス例】
- フォレンジック
- マルウェア調査
- OSINT調査

監視・分析

ログ保管では、様々な機器やソフトウェアの動作状況の記録（ログ）を一元的に蓄積・管理しインシデント発生時に役立てます。またそのログを元にアラート監視・通知も行っております。

【サービス例】
- ログ保管
- SOC
- SIEM導入支援

コンサルティング

様々なセキュリティの課題に関してセキュリティベンダーならではのノウハウを生かし、助言・コンサルティングを行っております。

【サービス例】
- ISMS認定取得支援
- CISコントロール
- CSIRT構築支援
- セキュリティ顧問

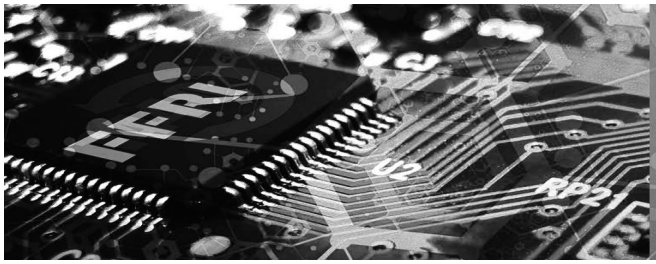
教育・研修

標的型メール訓練サービスなどの教育訓練や運用体制の見直し、セキュリティエンジニアの育成や診断の内製化支援など、弊社が経験してきたノウハウの提供を行っております。

【サービス例】
- 脆弱性診断内製化支援
- 標的型訓練メール
- セキュリティエンジニア育成
- インシデントハンドリング

お問い合せ	**株式会社レオンテクノロジー** **〒171-0014 東京都豊島区池袋2-52-8大河内ビル3F** **TEL: 03-5957-1960 / EMAIL：cs@leon-tec.co.jp**

株式会社ＦＦＲＩセキュリティ
https://www.ffri.jp/



日本でほぼ唯一
サイバーセキュリティの基礎技術研究を行う
日本発・純国産のサイバーカンパニー

2007年、当時北米でサイバーセキュリティのエンジニアをしていた現CEOの鵜飼と現CTOの金居は、国内にサイバーセキュリティの基礎技術研究を行っている企業が存在せず、自国の問題を自国で解決できないリスクに強い危機感を感じており、日本に帰国して当社を設立しました。2009年、従来のウイルス検知技術に頼らず、プログラムの動きを監視する事でマルウェアを検知する、振る舞い検知技術を使用した標的型攻撃対策ソフトウェア「FFRI yarai」の販売を開始。年金機構を狙ったマルウェアのほか、最近ではEmotetやRagnar Locker など、豊富な防御実績を公開しており、官公庁や金融機関などを中心に導入が進んでいます。その他、高いリサーチ能力を活かして、セキュリティの調査・研究や、教育・研修、IoT製品や自動運転に係る車載のセキュリティに関する調査・研究などの受託も行っています。

2020年には「株式会社ＦＦＲＩ」から「株式会社ＦＦＲＩセキュリティ」に社名変更し、サイバー領域における国家安全保障の実現へ向けて、ナショナルセキュリティへの注力を進めることを発表。横須賀ナショナルセキュリティＲ＆Ｄセンターを開設し、周辺組織や防衛産業企業、政府と一体になって安全保障の実現へ向けた取り組みを進めています。また、FFRI yaraiのOEM提供を進めており、マネージドサービスや新たなソリューションの研究開発など提供の形を増やし、増大するサイバー脅威へ対抗しています。

防御実績の一部

FFRI yaraiが検出したマルウェアのうち、著名なもので公開可能なものを抜粋し公開しております。世界中で被害の発生したマルウェアについても、被害発生以前にリリースされたバージョンでマルウェアを検出し、システムを保護できることを確認しています。詳細は以下URLよりご確認いただけます。
＜https://www.ffri.jp/products/yarai/defense_achievements.htm＞

発生/報告時期	防御エンジンリリース時期	攻撃・マルウェア名称
2020年7月	2018年2月	ランサムウェア「Maze」
2018年7月	2018年3月	マルウェア「Emotet」
2018年4月	2017年6月	ランサムウェア「GandCrab」
2017年5月	2016年10月	ランサムウェア「WannaCry」
2015年6月	2014年8月	マルウェア「Emdivi」※日本年金機構を狙ったマルウェア

日本最多の脆弱性発見実績	サイバーセキュリティに関する対策技術・研究開発	BlackHatなどカンファレンス発表実績多数
Microsoft WindowsやInternet Explorer、Adobe Readerおよび、Office製品など、日本最多の100を超えるクリティカルなセキュリティ脆弱性発見の実績があります。	リサーチエンジニアによる海外動向調査や最新の攻撃と防御手法の研究、先端テクノロジーに対する脅威分析・脆弱性検査・解析など、サイバーセキュリティに関する知見や技術を蓄積し、プロダクト開発やトレーニングサービスなどに活用しています。	世界で最も権威のあるセキュリティカンファレンスBlackHatのアジア初のレビューボーダーであるCEOの鵜飼を始め、トップクラスのエンジニアが多数在籍。近年ではBlackHat EU 2020にて研究結果を発表するなど、国際的にも高い評価を頂いております。

お問い合せ	株式会社FFRIセキュリティ Eメール：pr@ffri.jp 問い合わせフォーム：https://www.ffri.jp/contact/index.htm

株式会社アイピーキューブ

https://ip3.co.jp

**業務効率・コラボレーション・ワークスタイルの改善に期待が寄せられる昨今の、
セキュリティ向上・リスク管理・統制・コンプライアンスの確保などの解決に――。**

株式会社アイピーキューブは、創立以来10年以上、統合認証基盤【ID管理・シングルサインオン(SSO)・認証】を専門事業とし、信頼性の高い自社製品の開発と、大小問わず様々な規模・業種における統合認証基盤の構築プロジェクトを担ってまいりました。
その経験・実績を生かし、変革に伴うリスクを最小化すると同時に、得られるメリットを最大化できるよう、お客様の事業課題に応じた「統合認証基盤に関するコンサルティング」、「統合ID管理システムやシングルサインオンシステムの構築・カスタマイズ」、「導入後の運用サポート」をお手伝い致します。お客様のIT統制やセキュリティ対策のための堅牢なIT基盤（統合認証基盤・統合ID管理）を低価格でご提案・ご提供させていただきます。

■統合認証基盤のご提案

社内システムからクラウドサービスまで、社内外問わず幅広いITリソースを活用した業務が行われる昨今、より高い水準のセキュリティ対策が求められる時代になりました。当社は、国際標準規格のFIDO（ファイド）認証に準拠し、FIDOアライアンスよりFIDO2サーバとして認定を取得した「AuthWay（オースウェイ）FIDOサーバ」を2021年にリリースしました。
これにより、生体認証を含む多要素認証（MFA）、二経路認証、二段階認証を実現する「AuthWay」と、Webアプリやクラウドサービスのシングルサインオンを実現する「CloudLink」（クラウドリンク）を用いた、利用者の利便性と安全を両立した統合認証基盤をご提案しております。

■統合ID管理のご提案

各種システムやクラウドサービスの利用拡大にともない分散したID情報は、利用されなくなったにもかかわらずそのまま放置された場合、セキュリティリスクに直結します。「EntryMaster」（エントリマスター）は、それらのID情報を一元的に管理し、運用負荷を軽減しつつ、あらゆる場面に対応した「正しいIDライフサイクル」を提供する統合ID管理製品です。ID情報の入出力（連携）対象として、Active Directoryや各種LDAP、CSVファイル、クラウドサービスなど様々なシステムに対応可能なほか、各種機能の利用・メンテナンスのためのユーザーインターフェースは利便性を追求した操作性の良いものとなっております。また、情報セキュリティや情報統制活動において重要な、証跡管理（ログ）機能を提供しております。

(※) AuthWay, CloudLink, EntryMasterは株式会社アイピーキューブの登録商標です。
(※) FIDO, FIDO ALLIANCE, FIDO AUTHENTICATION, FIDO CERTIFIEDの商標およびロゴは、FIDOアライアンスの登録商標です。

お問い合せ	株式会社アイピーキューブ 〒105-0012 東京都港区芝大門2-12-9 HF浜松町ビルディング 8F TEL：03-4221-1101 *I Promise our Performance for your Profit* *アイピーキューブは、お客様の利益のために最高のパフォーマンスを実現することを約束します。*

一般財団法人日本情報経済社会推進協会 (JIPDEC)

https://www.jipdec.or.jp/

データ流通社会を支える信頼と安心のために

日本の個人情報保護と情報セキュリティを支える

当協会は、半世紀を超えて日本の経済社会の情報化を先導し推進する重要な役割を担ってきました。近年のIoT・AI・ビッグデータなどのデジタル化が進む中では、個人情報保護や情報セキュリティといったデータの流通・利活用上の信頼確保に対する社会的要請の高まりに対し、実績を積み重ねてきております。

特に1998年より運営している「プライバシーマーク®制度」は、事業者の個人情報保護の取り組みの推進ならびに個人情報に関する意識向上に取り組んでおり、約16,500社を超える事業者にご活用いただいております。また、近年の押印手続の見直し等に伴い普及しつつある電子契約サービスを支える電子署名等のトラストサービスの評価事業にも取り組んでおります。

今後、当協会としては、JNSAのコミュニティの皆様と協力して、データ流通社会を支えて参る所存です。

プライバシーマーク制度

個人情報を適切に取り扱う事業者を示す「プライバシーマーク」。
事業者にとっては、個人情報保護法の遵守はもちろん、自主的に高いレベルの個人情報の管理体制を確立し運用していることを、取引先などに分かりやすく示すことができます。

個人情報が様々なビジネスやサービスに利用される一方、漏えい事故やトラブルなども頻発している状況において、事業者の個人情報の取扱いに関するリスク対策は、不正アクセス、ウイルス感染などに対するセキュリティ対策の強化にとどまらず、ヒューマンエラー、法令違反などのリスクを顕在化させない仕組み・適正に管理する仕組みの強化も求められています。個人情報の管理体制の強化、リスクマネジメントの一つとして、プライバシーマークをご活用いただければと存じます。

プライバシーマークについては、動画、セミナーなど様々なコンテンツ・サービスを提供していますので、ぜひご利用ください。また、ご質問・ご相談などがありましたらお気軽にお問合せください。

☆ プライバシーマーク制度Webサイト：https://privacymark.jp/

☆ YouTube【JIPDEC公式】プライバシーマークチャンネル
https://www.youtube.com/channel/UCscKq0Qp-dfY6m0yjLRut5A/

付与事業者インタビュー

知ってる？プライバシーマーク（動画）

プライバシーマークセミナー（動画）

お問い合せ	一般財団法人日本情報経済社会推進協会（JIPDEC） 〒106-0032 東京都港区六本木一丁目9番9号　六本木ファーストビル内 https://www.jipdec.or.jp/

ラピッドセブン・ジャパン株式会社

www.rapid7.com/ja

RAPID7

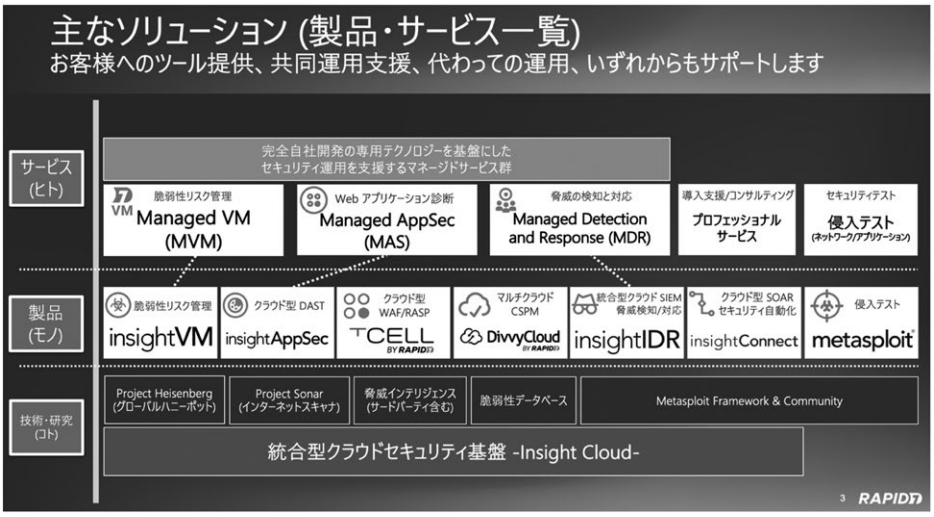
世の中のセキュリティを進化させるRapid7

Rapid7(ラピッドセブン)は、米国マサチューセッツ州で2000年に設立されて以来、今日まで業界でもっとも明晰な思考力でセキュリティの前進に努めて参りました。現在は全世界141をこえる国と地域で、9000社以上のお客様から高い信頼を得ています。

Rapid7のテクノロジーを凝縮した Rapid7 Insight Cloudを通じて、IT環境全体のデータ収集、脆弱性の管理の自動化、ユーザーの行動の監視、ログの検索、アプリケーションの脆弱性テストなど、セキュリティ、IT、DevOpsの部門間をまたいだコラボレーションが可能になります。

Rapid7は日本でも2020年6月からMDRサービスの提供を開始しました。MDRにはインシデント検知・対応に必要なSIEM、UBA、ABA(攻撃者行動分析)、NTA、EDRなどがパッケージされており、Rapid7による脅威検知とインシデント対応チームが24時間365日の監視を行い、ユーザーや攻撃者の行動分析、脅威インテリジェンスなど、様々な視点からログを分析します。顧客環境内のセキュリティインシデントを迅速かつ多面的に検知し、インシデントレスポンスを含めた対応につながる支援もトータルソリューションとして提供します。膨大なアラートの処理から脅威のトリアージ、インシデントの分析・対応までのライフサイクルをカバーするマネージドサービスとして提供していることが大きな特長となります。
顧客はインシデントレスポンスにおける最も負担が重い部分をRapid7にアウトソーシングすることで、現場の作業負荷を大幅に下げることができるようになります。

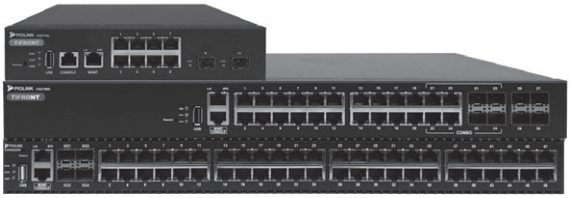
セキュリティは、仮説ではありません。すべての組織にとって現実であるべきです。だからこそ、セキュリティをビジネスの中核に位置付けるための支援をお約束しています。統合的なセキュリティプラットフォームの実現から、適切なセキュリティ体制の把握の向上までRapid7にお任せください。



お問い合せ	ラピッドセブン・ジャパン株式会社 〒104-0031 東京都中央区京橋2-2-1　京橋エドグラン26階 代表番号：03-6838-9720　Website: www.rapid7.com/ja

株式会社パイオリンク
https://www.piolink.co.jp

当社パイオリンクはネットワークやセキュリティ分野において独自の技術とサービスを提供しております。

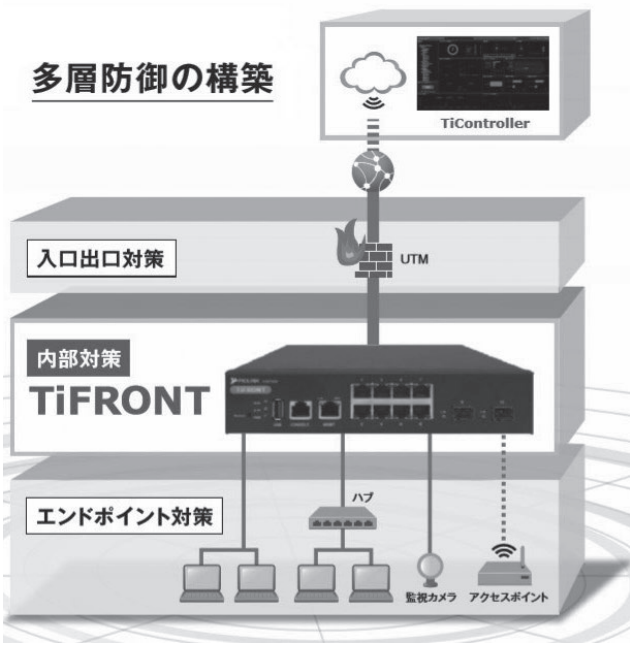


クラウド管理型のセキュリティスイッチ、TiFRONT(ティーフロント)と管理システムのTiController(ティーコントローラー)をラインアップしております。

TiFRONTはL2スイッチの形態でネットワーク内部に配置することから、端末やネットワークカメラ、IoT機器などの近い位置で内部ネットワーク上の攻撃性通信を「検知・遮断」することができます。

管理システムのTiControllerはクラウド環境に設置することができ、TiFRONTの一元管理に加え、TiFRONT配下の端末情報をエージェントレスで可視化いたします。

内部ネットワークで通信や端末情報を可視化し、拡散の対策を取ることが、重要になってきています。



<UTMとの連動遮断>

攻撃者の初期活動を端末に近い位置で遮断することで攻撃者の動きを封じ込め、その後の攻撃活動が継続できないようになります。

既に設置しているUTMなどの入口出口対策機器と連動動作を取ることで、検知対象の端末の通信を即時遮断することができます。

リモートワークやDXが進む昨今においても、社内ネットワークは存在しております。

改めて社内ネットワークに対するセキュリティ対策を見直すことで、**「検知したら即対応」**できる仕組み作りをご支援いたします。

お問い合せ	株式会社パイオリンク 〒160-0022 東京都新宿区新宿5-8-8　カールツァイス新宿別館3F Email：sales@piolink.co.jp Web：https://www.piolink.co.jp Twitter：@PIOLINK_JP

JNSA 会員企業のサービス・製品・イベント情報

■サービス紹介■

○商工会議所サイバーセキュリティお助け隊サービス
（1）レンタルUTMによる【お守り】
（2）常時の【見守り】
（3）攻撃時の【お知らせ】
（4）不安時の【相談窓口】
（5）インシデント時の【駆け付け】
（6）駆け付け費用を補償する【保険】
（7）名刺に本サービス利用企業である事実をマーク表示できる【信用UP】
（8）商工会議所が提供する【安心】

月額：商工会議所会員6,600円、非会員8,250円
【サービス情報詳細】
https://www.osaka.cci.or.jp/cybersecurity/utm/
◆お問い合わせ先◆
大阪商工会議所
経営情報センター（野田・中川・古川・石田）
TEL: 050-7105-6004
Email: cybersecurity@osaka.cci.or.jp

■サービス紹介■

○Rapid7 MDR
Rapid7 MDRは、日々の脅威・インシデントの検知と対応の運用を包括的にご支援するマネージドサービスです。セキュリティ機器・イベントの「点」での監視とアラート転送や、端末だけを対象とした MDR（Managed EDR）とも異なる、統合的な監視と効果的かつアクショナブルな通知を実現します。米フォレスター・リサーチ社による調査レポートをはじめ、グローバルで高く評価されているサービスです。
【サービス情報詳細】
https://bit.ly/2ReqO4g
◆お問い合わせ先◆
ラピッドセブン・ジャパン株式会社
E-mail: JapanSales@rapid7.com

■イベント紹介■

○CCSPチャレンジセミナー(オンライン)
CCSPは、クラウドセキュリティ専門家を認定する資格です。サイバー・情報・クラウドコンピューティングセキュリティの実務経験に基づく能力と、クラウドセキュリティの知識について認定を受けた専門家を擁することで、企業は、重要な機能に対して適切な専門家が対応することを期待できます。本セミナーでは、CCSPオフィシャルセミナーのオーバービューをご紹介します。
【イベント情報詳細】
https://japan.isc2.org/ccsp_challenge_seminar.html
◆お問い合わせ先◆
（ISC）2 Japan
E-mail: Infoisc2-j@isc2.org

■製品紹介■

○AuthWay FIDO サーバ
国際標準規格のFIDO（ファイド）認証に準拠し、PCやスマートデバイスに内蔵されている生体認証や外部の認証器を使った、パスワードレス認証を実現する製品です。
当社のシングルサインオンシステム「CloudLink」との組み合わせにより、Webアプリやクラウドサービスへの安全で利便性の高い統合認証基盤をご提供いたします。
※FIDO、FIDO ALLIANCE、
FIDO AUTHENTICATION
FIDO CERTIFIEDの商標およびロゴは、
FIDOアライアンスの登録商標です。
【製品情報詳細】
https://ip3.co.jp/solution/authway-fido
◆お問い合わせ先◆
株式会社アイピーキューブ
E-mail: info@ip3.co.jp

標準化部会セミナーの開催報告

JNSA 標準化部会　副部会長　松本　泰

◇はじめに

2021年1月15日（金） JNSA標準化部会主催セミナー「デジタル社会に不可欠なサイバーセキュリティ標準化動向～巧妙化、高度化、多様化するサイバー攻撃に備えて～」をフルオンラインにて250名以上の方にご参加頂き開催されました。本稿では、今回の標準化部会セミナーの概要を説明するとともに、こうしたセミナーを開催する目的、意義といったところを説明します。

◇今回のセミナーの概要

最初の講演は、長年情報セキュリティの標準化にご尽力され、また標準化部会部会長でもある中尾康二氏の講演でした。情報セキュリティに係るISO、ITU-Tなどの所謂デジュール標準の非常に幅広い視点からの説明であり、情報セキュリティに携わる方であれば、誰でもが参考になる講演でした。

２番目の講演は、標準化部会IoT機器セキュリティログ検討WGのリーダを努められ、その活動の一環としてITU-Tにおいて国際標準策定を主導した渥美清隆氏の講演でした。渥美氏は、IoTセキュリティのためのIoTログの標準化をITU-T X.1367（X.elf-iot）という形で、日本発の標準化を達成し、JNSA標準化部会としても非常に意義のある活動であったと思います。

この後、標準化部会の4つのWGの「標準化部会各WGにおけるサイバーセキュリティ標準化との関わり」の発表がありましたが、これは、この後の二つのパネルディスカションにつながる発表であり、今回の標準化部会セミナーは、この二つのパネルディスカションが、大きなハイライトだったかと思います。

ひとつめのパネルディスカションの「ISO/IEC 27002の改版に伴う、日本のISMS市場へのインパクトと今後の活用方法について」では、標準化部会部会長の中尾氏がモデレータを務め、標準化部会日本ISMSユーザグループのリーダである魚脇氏ほか４名のISMSに造詣の深いパネリストにより活発なディスカションが行われました。実務として情報セキュリティに携わる方にとっても非常に聞き応えのある内容だったのではないでしょうか。

二つのパネルディスカションでは、松本がモデレータを務め、標準化部会の３つのWGのメンバーにより「ID管理／本人確認（Identity proofing）に関する標準化動向」についてのディスカションを行いました。本人確認（Identity proofing）は非常にホットな話題ですが、こうしたことをテーマにしたパネルディスカションはそれほど多くはなく、新たにご興味を持たれた方も多数おられたかと思います。

講演のプログラムは、JNSAの公開Webページに記載されておりますが、当日のプレゼン資料も公開されています。また、動画もJNSA会員Webページで公開される予定ですので、ご興味がある方は、是非ご覧頂ければ幸いです。

◇おわりに

今回のセミナーは、JNSA標準化部会としての初めての開催でしたが、部会としては、こうしたセミナーを今後とも続けていくことを検討しています。情報セキュリティに関わる標準化活動は、巧妙化、高度化、多様化するサイバー攻撃が日々報道される中で、地味な活動に見えるところがあろうかと思います。また、JNSAの活動としても、その実態が見えづらいかもしれません。しかし、情報セキュリティに関わる標準化の活動は、社会全体の視点、また中長期的な視点にから「備える」ためには不可欠な活動だと確信しております。こうしたセミナー等の活動を通じて、今後ともJNSA標準化部会の活動に関心を持って頂ければ幸いです。

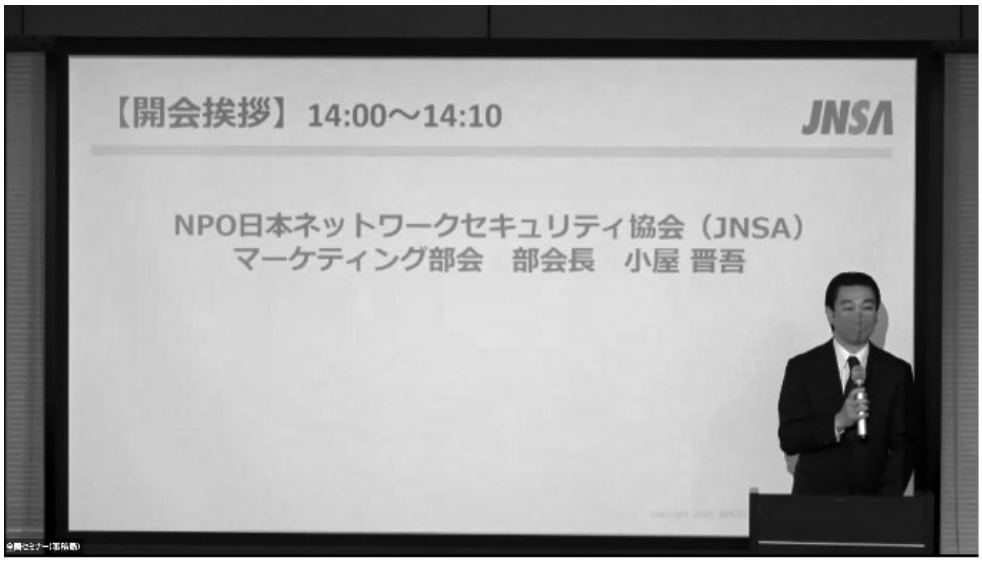
■一部講演資料をご覧いただけます。
JNSA標準化部会主催セミナー
「デジタル社会に不可欠なサイバーセキュリティ標準化動向」
巧妙化、高度化、多様化するサイバー攻撃に備えて
https://www.jnsa.org/seminar/2021/0115/index.html

「JNSA 全国サイバーセキュリティセミナー」を開催

マーケティング部会では、全国に向けてのセキュリティ啓発とJNSA会員勧誘を目的として、「JNSA 全国サイバーセキュリティセミナー2020」を開催しました。

2020年度で4年目となるこの全国セミナーは、コロナ禍で開催そのものが危ぶまれましたが、ビジネスのデジタル化が進むなか、新型コロナウイルスによる混乱等に乗じた新たな脅威も発生し、ビジネスに致命的な影響を及ぼすリスクも増加していることから、DX時代におけるセキュリティの役割を再認識してもらう場として「Withコロナによりさらに加速を求められるDXとサイバーセキュリティ対策」をテーマに、オンライン形式で開催しました。

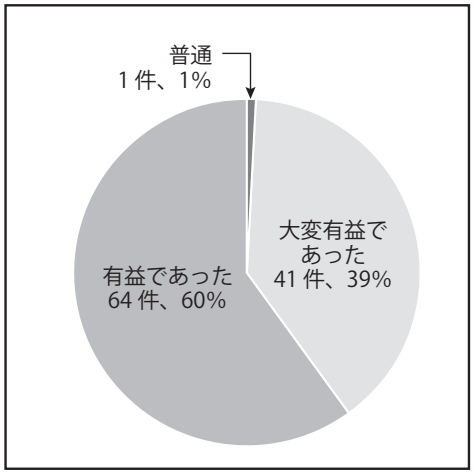
オンラインということもあり、全国各地から188名と多くの方の参加があり、熱心に聴講いただくとともに、政府の政策やセキュリティサービスに関する具体的な質問がチャットで入るなど、好評のうちに終了いたしました。



［開会挨拶の様子］

ご参加いただいた方のほぼすべての方から「有益であった」との感想をいただき、継続しての開催希望の声も頂戴しました。

企業のセキュリティ担当者からは「対策に役立つ具体的な製品やサービス名が得られたことがよかった」という声を頂いたほか、セキュリティ製品販売者の立場の方からは「中小企業のお客様にお知らせできる最新情報がよかった」などの感想があり、実務に役立つ具体的な情報提供が有益であったようです。今後も定期的に全国セミナーを行うことで、ユーザー企業のセキュリティ対策向上及びセキュリティ事業者のビジネスの成長を支えることを考えるとともに、地域所在のセキュリティ事業者のJNSAへの入会を目指します。



［全体を通しての参加者の感想］

イベント開催の報告

【セミナー概要】

◆名　称: JNSA全国サイバーセキュリティセミナー2020
～Withコロナによりさらに加速を求められるDXとサイバーセキュリティ対策～
◆日　程: 2020年11月13日(金)
◆主　催: NPO日本ネットワークセキュリティ協会(JNSA)
◆後　援: 経済産業省、特定非営利活動法人ITコーディネータ協会
◆協　賛: (五十音順)
アイマトリックス株式会社、RSA Security Japan 合同会社、EY新日本有限責任監査法人、
キヤノンマーケティングジャパン株式会社、株式会社日立ソリューションズ、株式会社YONA、
OneLogin,Inc.,
◆料　金: 無　料
◆対象者: 企業内セキュリティ担当者、SIerのセキュリティ製品販売者

プログラム

【開会挨拶】14:00 ～ 14:10

【講演】14:10 ～ 14:50「新しい働き方のサイバーセキュリティ対策」

NPO日本ネットワークセキュリティ協会(JNSA)社会活動部会　冨田 高樹氏

＜概要＞新型コロナウイルスの今後の影響は見通せませんが、世の中では新しい働き方が浸透しつつあり、この流れは不可逆的なように見えます。そこで、JNSAが今年5月に公表した「緊急事態宣言後のセキュリティリスト」をもとに、新しい働き方に応じたサイバーセキュリティ対策の考え方について紹介します。

【講演】14:50 ～ 15:20「産業分野におけるサイバーセキュリティ政策」

経済産業省商務情報政策局サイバーセキュリティ課　企画官　鴨田 浩明氏

＜概要＞最近のサイバー攻撃の高度化･攻撃起点の多様化に加え、新型コロナウィルスによる混乱等に乗じたサイバー攻撃が増加している。地域・企業規模に関わらず中小企業もサイバー攻撃の対象となっていることから、サプライチェーン全体を視野に入れたリスク管理が必要。本講演では、直近の状況及び今後のデジタル化の急加速に対応するための施策、産業界を挙げたサプライチェーン全体のサイバーセキュリティ強化の取組について説明します。

【講演】15:30 ～ 16:10「これからのセキュリティサービスの選び方」

日本セキュリティオペレーション事業者協議会(ISOG-J)　武井 滋紀氏

＜概要＞社会の状況や法律や規制が変化する中で、セキュリティ対策として行うべきことは年々変化しています。その中で外部のセキュリティサービスを利用する検討も必要となります。セキュリティ対策が多様化し、セキュリティサービスも多様化する中で「何を対策として行えばいいのかわからない」「どうやって選べばいいのかわからない」という疑問も尽きません。セキュリティサービスを選ぶまでの全体像や検討するポイントを中心に解説します。

【講演】16:10 ～ 16:40「JNSAツールの紹介と活用メリット」

NPO日本ネットワークセキュリティ協会(JNSA)マーケティング部会　扇 健一氏

＜概要＞セキュリティ対策の必要性は理解していても、なかなか取り組むのが難しいのが実際ではないでしょうか。どこから始めるのか、どこまでやるのか、教育は？と多くの悩みを皆様お持ちです。JNSAでは、そのような課題の解決に活用可能なツール類をワーキンググループの活動の成果としてご用意しています。本セッションではそれらツールのご紹介と活用することでのメリットを紹介します。

【閉会挨拶】16:40 ～ 16:45

知っておきたい情報セキュリティ
理解度チェックサイト プレミアム
http://slb.jnsa.org/eslb/

活用のポイント・メリット

- 社員教育をしたいがコストは最小限にしたい
- 問題を自分で作る時間がない
- 社員のレベルを把握したい

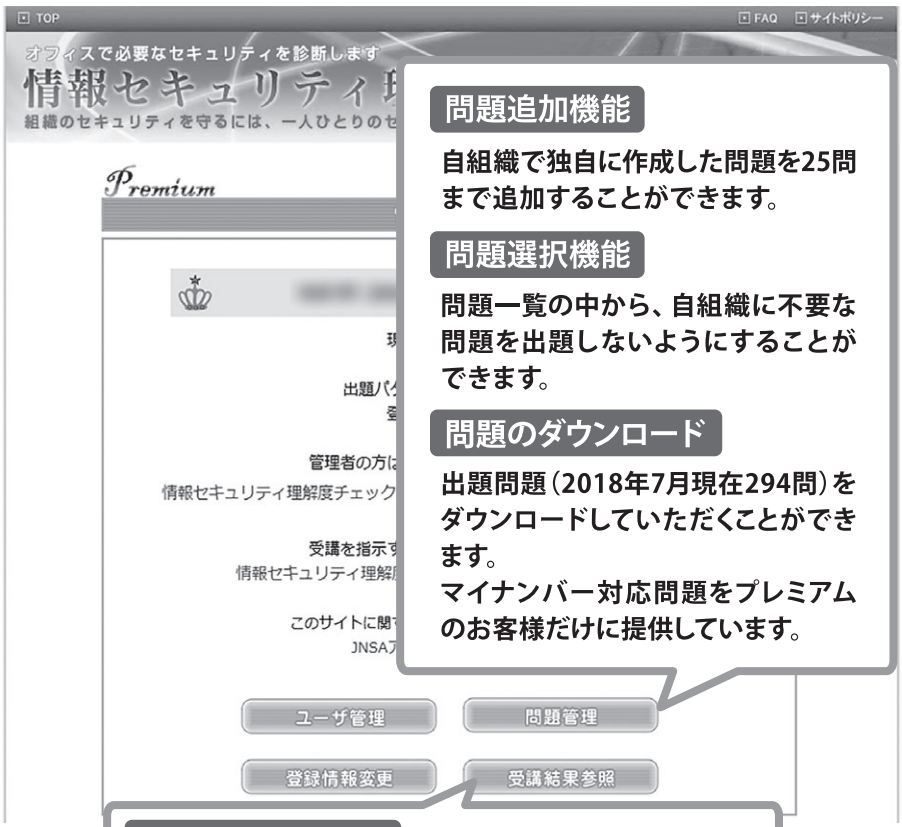
「情報セキュリティ理解度チェック・プレミアム」は、無償版「理解度チェックサイト」を、組織ごとにカスタマイズできる機能がついた有償サービスです。管理者機能をより強化し、独自の問題の追加も可能です。ぜひ社内教育や情報セキュリティ関連の補助ツールとしてご活用下さい。

＜料金の一例＞
登録人数51名～100名の場合
年間利用料[定価]：50,000円(税別)

登録人数により、7コースご用意しております。詳しくは事務局までお問合せください。

なお、無償版の「情報セキュリティ理解度チェック」サイトもございますので、是非お試しください。

【お問合せ先】slb@jnsa.org



問題追加機能

自組織で独自に作成した問題を25問まで追加することができます。

問題選択機能

問題一覧の中から、自組織に不要な問題を出題しないようにすることができます。

問題のダウンロード

出題問題（2018年7月現在294問）をダウンロードしていただくことができます。
マイナンバー対応問題をプレミアムのお客様だけに提供しています。

管理者機能の強化

受講者（ユーザ）の受講結果を見ることができます。ダウンロードできるcsvファイルの内容がより詳しくなり、誰がどのように間違えたかがわかります。

JNSA

JNSA 部会・WG 活動内容

1. 社会活動部会

部会長：丸山司郎 氏／株式会社FFRIセキュリティ
副部会長：唐沢勇輔 氏／Japan Digital Design株式会社

日本でもサイバーセキュリティがビジネスとして成立する時代となり、様々な社会問題が提起される事となってきた。

そのような中、JNSAがサイバーセキュリティ界における、社会問題の解決者として、今まで以上に社会に貢献していくために、従来から行ってきた活動の見直しを行うとともに、政策提言活動を行っていく。

具体的には、適正なセキュリティ事業遂行の促進、業界団体としての政策提言のとりまとめ、政府と協力した政策の促進、メディアや市場の力を活用した普及啓発活動、外部組織支援、国際・他団体連携などを行う。

【海外市場開拓WG】

（リーダー：松本照吾 氏／
アマゾン ウェブ サービス ジャパン株式会社）

昨年度の活動を継続し、Made-in-Japanのセキュリティソリューションの海外展開・拡販を業界団体として促進する。具体的には、展示会出展による参加企業の販売代理店の開拓、商談発掘の支援、海外セキュリティコミュニティとの連携を実施する。

海外市場に進出する上での手順や課題と解決策を纏めた「海外市場進出ガイド」のアップデートの実施などをおこなう。また、各社の製品情報の英語版を拡充する。

＜予定成果物＞

- 海外市場進出ガイド改版
- セキュリティ事業特化の輸出関連ガイド
- 各社の製品情報の英語版の拡充

【CISO支援WG】

（リーダー：髙橋正和 氏／
株式会社Preferred Networks）

本年出版した「CISOハンドブック」を発展させる。

＜予定成果物＞

- ドキュメント、イベント等での発表、トレーニングマテリアルなど

【JNSA CERC】

（リーダー：髙橋正和 氏／
株式会社Preferred Networks）

緊急時の情報交換のプラットフォームとして活動する。

【中小企業支援施策WG】

（リーダー：岩本真人 氏／トレンドマイクロ株式会社）

中小企業の情報セキュリティ対策導入を促進する官民による支援施策の検討その実践、ならびに中小企業の情報セキュリティ市場の拡大を捉えたJNSA会員のソリューション展開へ寄与することを目的とする。

＜予定成果物＞

- 支援施策の検討のための調査の纏め、 支援施策の検討によるガイドラインの作成、外部支援機関/支援者との協同施策

【みんなで作ろう「サイバーセキュリティコミック」実行委員会】

（実行委員長：本川祐治 氏／株式会社日立システムズ）

サイバーセキュリティを取り巻く環境が年々厳しさを増す中、広くサイバーセキュリティ意識の向上が不可欠であると考え、コンテンツがもつ拡散力に注目し、セキュリティ知識の普及とネットリテラシーの向上、ネットを守るハッカーへの興味とイメージアップ、セキュリティ人材育成を促進することを目的として活動を行う。

＜予定成果物＞

- SNSコミック8回配信

2. 調査研究部会

部会長：前田典彦 氏／株式会社FFRIセキュリティ

情報セキュリティにおける各種の調査および研究活動を行う。

セキュリティ被害、情報セキュリティ市場などの統計分析事業、および、重要度や緊急度の高いテーマに関する脅威分析、対策研究を推進する。適切な時期、形式を用いて適宜情報公開を行い、調査研究における成果を広く社会に還元する。新規性や緊急性の高いテーマの検討が必要となる場合においては、勉強会、BoFなどを随時行うなどして、柔軟かつ迅速な対応を行う。

【セキュリティ被害調査WG】
（リーダー：大谷尚通 氏／株式会社エヌ・ティ・ティ・データ）

2019年個人情報漏えいインシデントの報告書を作成して公表する。

2020年個人情報漏えいインシデントのデータを受領して、分析する。

長崎県立大学と連携して、2021年個人情報漏えいインシデントを収集する。

残作業になっている被害報告(報道や報告書)の標準化テンプレートのまとめ、報告書化を行う。

これまでの個人情報漏えいインシデントの調査と報告書作成をみなおし、今後の調査実施可否を決定する。

＜予定成果物＞

- 2019年個人情報漏えいインシデント調査報告書
- 2020年個人情報漏えいインシデント調査報告書
- 被害報告(報道や報告書)の標準化テンプレート、報告書

【セキュリティ市場調査WG】
（リーダー：礒部良輔 氏／興安計装株式会社）

サブリーダー：玉川 博之氏／株式会社VSN)

国内で情報セキュリティに関するツール、サービス等の提供を事業として行っている事業者を対象として、推定市場規模データを算出し報告書として公開する。

また、近年のセキュリティ市場拡大の伴う、市場調査の調査内容、セキュリティ区分の見直しを継続して実施予定。

＜予定成果物＞

- 2020年度情報セキュリティ市場（国内）調査報告書

【組織で働く人間が引き起こす不正・事故対応WG】
（リーダー：甘利康文 氏／セコム株式会社）

(1)人の意識や組織文化、(2)組織の行動が影響を受ける社会文化や規範、(3)不正・事故を防ぐシステム、以上の３方向から「組織で働く人間が引き起こす不正・事故」に対する考察を深め、ベストプラクティスの紹介、提案、啓発を行うことを目的とする。

2021年度も引き続き、特に(1)に重点をおいた活動を行う。（コロナ禍で日常になったテレワーク環境下における取組を積極的に聞き出したい。）

＜予定成果物＞

- 「組織文化醸成によるES向上」に向けた各組織の取組事例ヒアリング調査と、調査内容をベースとしたWeb記事公開
- JNSA Pressへの寄稿、セミナー等への出講

【インシデント被害調査WG】
（リーダー：神山太朗 氏／あいおいニッセイ同和損害保険株式会社）

（サブリーダー：西浦真一 氏／キヤノンITソリューションズ株式会社）

サイバーインシデント被害者に発生しうる、金銭的負担項目とその被害額を調査・算定し、成果物としてまとめる。

＜予定成果物＞

- 「2021年度インシデント発生時の被害額」報告書

【IoTセキュリティWG】
（リーダー：松岡正人 氏／日本シノプシス合同会社）

IoTセキュリティに関連する調査研究を継続する。

＜予定成果物＞

- IoTセキュリティガイドなど（詳細は今後検討）

【脅威を持続的に研究するWG】
（リーダー：甲斐根功 氏／株式会社日立システムズ）

サイバーセキュリティを取巻く環境の変化に応じ顧客ニーズや課題を捉え直し、国内外における新たなビジネスアプローチやマーケットの構図の変化を調査し、国内ベント等を介して、広く情報発信する。

3. 標準化部会

部会長：中尾康二 氏／国立研究開発法人情報通信研究機構

副部会長：松本泰 氏／セコム株式会社

業種・業界・分野等の標準化・ガイドライン化などを推進する。特に、JNSA目線のセキュリティベースラインの提供、情報セキュリティ対策ガイドラインの策定などを進める。また、国際標準/国際連携との親和性の高い案件については、国際標準への提案やコメント、国際連携案件も視野に入れて、議論を進める。

【デジタルアイデンティティWG】
（リーダー：宮川晃一 氏／日本電気株式会社）

広くデジタルアイデンティティに関する様々な課題を

検討し、デジタル社会の基礎となるIDの重要性の啓蒙やプライバシー関連の問題提起や標準化に向けた意見交換を行う。

＜予定成果物＞

- ゼロトラスト環境におけるアイデンティティ管理（仮称）

【電子署名WG】

（リーダー：宮崎一哉 氏／ 三菱電機株式会社）

電子署名関連技術の相互運用性確保のための調査、検討、標準仕様提案、相互運用性テスト、及び電子署名普及啓発を行う。

＜予定成果物＞

- 署名検証プロセスに関する標準仕様案
- 長期署名プロファイル標準の改定案

【日本ISMSユーザグループ】

（リーダー：魚脇雅晴 氏／
エヌ・ティ・ティ・コミュニケーションズ株式会社）

ISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることでISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、日本における健全かつ効果的なISMS普及・促進に貢献する活動を行う。

＜予定成果物＞

必要に応じて、成果物として以下に関連するものをまとめるものとする。

- ISO/IEC27002の改定内容について適用管理策の観点での検討&整理
- ISMSの実装＆運用についての事例研究（テーマ選定中）

【PKI相互運用技術WG】

（リーダー：松本泰 氏／セコム株式会社）

デジタル社会におけるPKIの重要性をアピールしていく。

＜予定成果物＞

- PKI day, 鍵管理勉強会などでの発表。

4. 教育部会

部会長：平山敏弘 氏／学校法人電子学園

社会のニーズや時代の変化に適合したセキュリティ人材育成のため、必要とされる知識・技能等の検討を行い、実際に大学や専門学校等で評価実験を行う。また、情報セキュリティ教育のコンテンツとして、講義シラバスや講義資料およびSecBoK2020年版の作成・公開を通じて、教育界・産業界への展開・使用を促進することで、情報セキュリティ人材の育成に貢献する。2021年度も引き続き情報系大学における講義カリキュラム指標であるJ17との連携とASEANを中心とした海外教育機関との連携によるセキュリティ人材育成への貢献を目指す。

さらに、継続して講師データベースへの登録講師や講師予備軍の若手による講義・勉強会の開催等、教える場の提供を支援することにより、JNSA教育部会メンバーのスキル向上を目指す。加えてセキュリティコンテストとは異なる新たな実践教育ツールの開発や検証に対しても検討を行う。

SecBoK2021更新版の展開、およびSecBoK2022改定委員会活動を実施する。

＜予定成果物＞

- SecBoK2022

【ゲーム教育WG 】

（リーダー：長谷川長一 氏／株式会社ラック）

ゲームを活用した情報セキュリティの実践的教育の調査・企画・実施（イベント、講師派遣等）、及び普及促進に取り組む。

＜予定成果物＞

- 「MalwareContainment」ファシリテーターマニュアル（仮称）

【情報セキュリティ教育実証WG】

（リーダー：垣内由梨香 氏／
日本マイクロソフト株式会社）

情報セキュリティを教えることが出来る高度なスキルをもった人材を育成するために、実践での大学などでの講義を通じて、実践力とハイレベルスキルの習得を目的とする。

また作成した成果物（講義コンテンツ）のJNSA会員企業への共有と他の学校関連や団体への展開を計画している。

＜予定成果物＞

- セキュリティ基本教育コンテンツ

【セキュ女WG】

（リーダー：北澤麻理子 氏／
ドコモ・システムズ株式会社）

会社の枠を超えた連携を可能にし、女性セキュリティエキスパートの交流場所を提供する。 また、セキュリティに関する専門スキルを持ちたい女性を応援するための活動を行う。

5. 会員交流部会

部会長：扇健一 氏／株式会社日立ソリューションズ

情報セキュリティ業界における健全な発展と貢献のため、会員向けのサービスとユーザー向けのサービスをマーケティング部会と連携しながら拡充させる。

特にソリューションガイドを、ユーザーにも、会員にもより利用しやすい環境とするための改修を行う。またセキュリティ理解度チェックについても利用者の増加に伴い、安定的に運用可能な環境の整備強化を検討する。

なお、会員向けの説明会や政府統一基準群の改定予定を受けた各種ガイドライン等の勉強会、また紐づけについては継続的して実施する。

【セキュリティ理解度チェックWG】

（リーダー：西浦真一 氏／
キヤノンマーケティングジャパン株式会社）

理解度チェックの継続的な問題の見直しを行うと共に、プレミアム版（有料サービス）のユーザ数増加に向けた対外活動を実施する。プレミアム版の利用者の増加に伴い、安定的に運用可能な環境の整備強化を検討する。

＜予定成果物＞

- 理解度チェック新規問題作成・問題改修

【JNSAソリューションガイド活用WG】

（リーダー：秋山貴彦 氏／株式会社アズジェント）

年間の活動を通じて会員企業自身のPRとその企業が有しているソリューションのPRを図る。

＜予定成果物＞

- JNSA内の他部会/WGが作成した成果物とソリューションガイドとの連携
- 関係諸団体が作成した各種ガイドラインとソリューションガイドの連携
- 関係諸団体が有しているWeb内でのバナー掲載促進

6. マーケティング部会

部会長：小屋晋吾 氏／ニュートラル株式会社
副部会長：持田啓司 氏／株式会社ラック

JNSAの認知度向上やWG成果物の普及促進を目的とした活動を行うとともに、会員企業を獲得するための施策を立案、実行する。

＜予定成果物＞

- 全国セミナーの実施
- 仕事紹介ビデオ制作

7. 事業コンプライアンス部会

部会長：西本逸郎 氏／株式会社ラック

サイバーセキュリティサービスの提供者が、ネットワーク社会、サービスを享受するお客様、そしてサービス従事者として自らを守るために、適正なセキュリティサービス事業遂行の在り方について検討する。

2018年度の「サイバーセキュリティ事業における適正な事業遂行の在り方に関する検討委員会」にて取りまとめた「サイバーセキュリティ事業者行動規範（案）」と「サイバーセキュリティ事業者の基本指針（案）」について継続して議論を実施し、今後の運用方策含めて検討を行う。

【企画WG】

（リーダー：唐沢勇輔 氏／
Japan Digital Design 株式会社）

本部会の企画検討や外部機関とのPoCを担う。また、 賛同企業の募集など、部会全体の取り組みに関する企画運営を行う。

＜予定成果物＞

- 法令改正の提案書

【調査WG】

（リーダー：小村誠一 氏／
エヌ・ティ・ティ・アドバンステクノロジ株式会社）

引き続き、海外の業務上で発生した法令上のトラブル事例や関連法制度に関する調査を実施する。調査対象として、法制度に加え、不正な活動に基づき、得た情報の売買や行動の変更を要求する組織や個人との

取引について、海外の事例や考え方の動向などについても、収集、調査することを検討する。

＜予定成果物＞
- 調査結果を資料として公開

【法令リスク研究WG】
（リーダー：田原祐介 氏／株式会社ラック）

サイバーセキュリティ業務の法令リスク一覧を作成するとともに、国内における事例研究を行う。

どういった業務に、リスクがあるかを具体的に参照できる資料の完成を目指す。

＜予定成果物＞
- 法令リスク一覧
- 法令リスク・インシデント事例報告書

8. 西日本支部

支部長：元持哲郎 氏／アイネット・システムズ株式会社

西日本に拠点を置くメンバー企業が中心となり、提携団体との協働の下、西日本のネットワーク社会におけるセキュリティレベルの維持・向上に資すると共に、産官共同して、IT利活用の実現・推進のため、西日本に集積する中小企業がリスクの変化に応じた機動的な対応を行うことができる機会づくりを支援する。

【今すぐ実践できる工場セキュリティ対策のポイント検討WG】
（リーダー：岡本登 氏／富士通株式会社）

現場実態を考慮したセキュリティ対策の考え方や新たなサイバー対応BCP策定に必要な観点などを整理し、中堅・中小製造現場のセキュリティ向上を支援することを目的とする。

＜予定成果物＞
- リスクアセスメントハンドブック
- セキュリティ対策ハンドブック
- サイバー対応BCP策定ハンドブック

9. U40部会

部会長：杉野広典 氏／NECネクサソリューションズ株式会社

若年層を対象メンバーとして、JNSAの若返り、若年層の活動活発化、幅広い人脈形成を目的として勉強会を中心とした活動を行う。

【for Rookies WG】
（リーダー：岡島麗奈 氏／株式会社サイバーエージェント）

セキュリティ関連業務経験3年未満を対象とし、若手をはじめとした人的ネットワークの形成および知識向上を目的とする。「いまさら聞けない相談事」を主に参加者が講師を担当などアクティブラーニング形式で行う。

【勉強会企画検討WG】
（リーダー：永塚遼 氏／SCSK株式会社）

U40部会員の知識・スキル向上を目指し、勉強会を企画・開催する。内容によってはJNSA会員からも広く勉強会参加者を募り、部会員同士・JNSA会員・外部講師との人脈形成を行う。

【Inside IT WG】
（リーダー：羽鶴颯 氏／株式会社セキュアスカイ・テクノロジー）

ITの基礎技術を初歩の初歩から学べるワークショップを国内各地で開催し、IT業界全体の知識・技術力の底上げを目的とした活動を行う。ワークショップの対象は、大学生～新卒2年目までの若手を中心として、理系文系関係なくITについて学び直したいと考えている個人で、年齢所属に関係なく幅広い層を想定している。

開催は、土曜日、日曜日、祝日などの休日の午後を利用し、講師は、ワーキンググループ参加メンバーが行う予定。

10. 情報セキュリティ教育事業者連絡会（ISEPA）

代表：持田啓司 氏／株式会社ラック

事業者間の連携や情報交換による業界活性化のための活動を行う。また、政府機関への政策提言や政策実現のための適切な事業者紹介を行う。

＜予定成果物＞
- セキュリティ関連スタッフ調査報告書
- 教育コースのSecBoK対応マップ
- スキル認定ガイドライン（バージョンアップ）

11. 日本セキュリティオペレーション事業者協議会（ISOG-J）

代表：武智洋 氏／日本電気株式会社

セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進することによって、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できる IT 環境実現に寄与することを目的として活動する。

＜新技術とオペレーションPj：年間活動予定＞

・新技術とオペレーションPj
　新たな技術トピックのうち、オペレーションに影響が出そうなものはどれか検討
　特に取り上げるものを決定してブレーンストーミングと議論
・TS1（セキュリティサービス認定検討タスクフォース）
　「情報セキュリティサービス基準適合審査」検討会事務局と連携

【セキュリティオペレーションガイドラインWG】

（リーダー：上野宣 氏／株式会社トライコーダ）

ユーザ向けセキュリティ診断サービスの解説書や、事業者向けのセキュリティ診断サービスのガイドラインを作成することを目指す。

【セキュリティオペレーション技術WG】

（リーダー：川口洋 氏／株式会社川口設計）

最新の技術動向を調査し、最適なセキュリティオペレーション技術を探究し、技術者の交流を図る。

【セキュリティオペレーション認知向上・普及啓発WG】

（リーダー：阿部慎司 氏／
NTTセキュリティ・ジャパン株式会社）

セキュリティオペレーションの必要性についての認知度向上を目的とし、普及啓発活動を行う。

【セキュリティオペレーション連携WG】

（リーダー：武井滋紀 氏／NTTテクノクロス株式会社）

セキュリティの運用について各社共通の課題の議論、検討を行う。

＜予定成果物＞

- マネージドセキュリティサービス選定ガイド Ver2.0

12. 日本トラストテクノロジー協議会（JT2A）

運営委員長：小川博久 氏（株式会社三菱総合研究所）

電子署名や電子認証など含むトラストテクノロジーに関連する事業者及び利用者が主体となり、産学官及び国内外の関連団体と連携して信頼性を担保するための技術等の検討を行い、より信頼できる電子社会の促進に寄与する。

＜予定成果物＞

- リモート署名ガイドラインの公開を予定

13. 産学情報セキュリティ人材育成検討会

座長：江﨑浩 氏/東京大学 大学院

情報セキュリティ業界での就労体験の機会提供を目的に、引き続きJNSAインターンシップを実施する。

学生と企業間の意見交換・交流のための「JNSAインターンシップ交流会」を例年春季に開催しているが、秋以降に開催を検討する。

14. SECCON実行委員会

実行委員長：花田智洋 氏／
国立研究開発法人情報通信研究機構
副実行委員長：寺島崇幸 氏／株式会社ディアイティ

継続的に協賛企業の協力を得て、SECCON CTFならびに初心者向け勉強会「SECCON Beginners」、女性限定ワークショップ「CTF for GIRLS」を開催予定。

情報セキュリティ人材の発掘・育成と国内の情報セキュリティレベルの底上げを図り活動を行う。

JNSA 役員一覧　2021 年 6 月 30 日現在

会　長	田中　英彦	情報セキュリティ大学院大学 名誉教授 東京大学 名誉教授
副会長	髙橋　正和	株式会社Preferred Networks
副会長	中尾　康二	国立研究開発法人情報通信研究機構

理　事（50音順）

青嶋　信仁	（株式会社ディアイティ）
天野　　隆	（東芝デジタルソリューションズ株式会社）
新井　一人	（トレンドマイクロ株式会社）
伊藤　　新	（エヌ・ティ・ティ・アドバンステクノロジ株式会社）
河内　清人	（三菱電機株式会社）
河野　省二	（日本マイクロソフト株式会社）
北沢　　聖	（日鉄ソリューションズ株式会社）
後藤　　忍	（セコムトラストシステムズ株式会社）
小屋　晋吾	（ニュートラル株式会社）
櫻井　秀光	（マカフィー株式会社）
西本　逸郎	（株式会社ラック）
藤伊　芳樹	（大日本印刷株式会社）
本城　啓史	（株式会社エヌ・ティ・ティ・データ）
丸山　司郎	（株式会社FFRIセキュリティ）
三宅　　優	（KDDI株式会社）
三膳　孝通	（株式会社インターネットイニシアティブ）
八束　啓文	（RSA Security Japan合同会社）
山口　政博	（ユニアデックス株式会社）
与儀　大輔	（グローバルセキュリティエキスパート株式会社）

幹　事（50音順）

秋葉　淳哉	（エヌ・ティ・ティ・アドバンステクノロジ株式会社）
有松　龍彦	（株式会社インフォセック）
伊藤　　昇	（グローバルセキュリティエキスパート株式会社）
岡庭　素之	（キヤノンITソリューションズ株式会社）
垣内　由梨香	（日本マイクロソフト株式会社）
香取　弘徳	（株式会社フーバーブレイン）
北澤　麻理子	（ドコモ・システムズ株式会社）
木村　　滋	（シスコシステムズ合同会社）
輿水　直貴	（キヤノンマーケティングジャパン株式会社）
後藤　　忍	（セコムトラストシステムズ株式会社）
駒瀬　彰彦	（株式会社アズジェント）
佐藤　　健	（NRIセキュアテクノロジーズ株式会社）
佐藤　俊介	（大日本印刷株式会社）
下村　正洋	（NPO日本ネットワークセキュリティ協会）
鈴木　英樹	（株式会社OSK）
関場　哲也	（株式会社カスペルスキー）
高野　敏男	（日本電気株式会社）
髙橋　正和	（株式会社Preferred Networks）
辻　　秀典	（ネットワンシステムズ株式会社）
中間　俊英	（株式会社ラック）
能勢　健一朗	（東芝デジタルソリューションズ株式会社）
野間　祐介	（株式会社インターネットイニシアティブ）
日向　　亨	（トレンドマイクロ株式会社）
平山　敏弘	（学校法人電子学園）
二木　真明	（アルテア・セキュリティ・コンサルティング）
前田　典彦	（株式会社FFRIセキュリティ）
三池　聖史	（ユニアデックス株式会社）
本川　祐治	（株式会社日立システムズ）
元持　哲郎	（アイネット・システムズ株式会社）

監　事

土井　　充	（公認会計士土井充事務所）

顧　問

今井　秀樹	（東京大学 名誉教授）
金子　啓子	（大阪経済大学 経営学部）
佐々木　良一	（東京電機大学総合研究所特命教授|サイバーセキュリティ研究所所長）
武藤　佳恭	（慶應義塾大学 教授）
手塚　　悟	（慶應義塾大学　環境情報学部　教授）
前川　　徹	（東京通信大学情報マネジメント学部 学部長 教授）
森山　裕紀子	（早稲田リーガルコモンズ法律事務所 弁護士）
大和　敏彦	（株式会社アイティアイ）
吉田　　眞	（東京大学 名誉教授）

JNSAフェロー

井上　陽一	
大和　敏彦	（JNSA顧問/株式会社アイティアイ）

事務局長

下村　正洋

会員企業一覧　2021年7月1日現在　249社　50音順

【あ】

RSA Security Japan（同）
（株）RSコネクト
あいおいニッセイ同和損害保険（株）
アイネット・システムズ（株）
（株）アイピーキューブ
アイマトリックス（株）
（株）アイ・ラーニング
アイレット（株）
アクセンチュア（株）
アクモス（株）
（株）アシスト
（株）アズジェント
（株）アスタリスク・リサーチ
アドソル日進（株）
アドビシステムズ（株）
Avast Software Japan（同）
アビームコンサルティング（株）　New
（株）アピリッツ
アマゾン ウェブ サービス ジャパン（株）
（株）網屋
アライドテレシス（株）
アラクサラネットワークス（株）
アルテア・セキュリティ・コンサルティング
（株）アルテミス
アルプスシステムインテグレーション（株）
EY新日本有限責任監査法人
EYストラテジー・アンド・コンサルティング（株）
イオンアイビス（株）
伊藤忠テクノソリューションズ（株）
学校法人 岩崎学園
（株）インターネットイニシアティブ
（株）インテック
（株）インテリジェントウェイブ
（株）インフォーズ
インフォサイエンス（株）
（株）インフォセック
インプレイス（株）
Woven Planet Holdings, Inc.
Utimaco IS GmbH　New
AOSデータ㈱
SCSK（株）
SGシステム（株）
SBテクノロジー（株）
EDGE（株）
NRIセキュアテクノロジーズ（株）
NECソリューションイノベータ（株）
NECネクサソリューションズ（株）
NECプラットフォームズ（株）
エヌ・ティ・ティ・アドバンステクノロジ（株）
エヌ・ティ・ティ・コミュニケーションズ（株）
エヌ・ティ・ティ・コムウェア（株）
NTTセキュリティ・ジャパン（株）
（株）エヌ・ティ・ティ・データ
（株）エヌ・ティ・ティ・データCCS
エヌ・ティ・ティ・データ先端技術（株）
NTTテクノクロス（株）
（株）エヌ・ティ・ティ ネオメイト
（株）NTTファシリティーズ エンジニアリング
（株）FFRIセキュリティ
エムオーテックス（株）
㈱エムティーアイ
エントラストジャパン（株）
（株）OSK
（株）大塚商会
岡三情報システム（株）
沖電気工業（株）
ONWARD SECURITY JAPAN（株）

【か】

（株）カスペルスキー
学校法人 片柳学園　New
（株）カンム　New
キヤノンITソリューションズ（株）　New
キヤノンマーケティングジャパン（株）
（株）クエスト
（株）クリエイティブジャパン
グローバルセキュリティエキスパート（株）
xID（株）
（株）km2y
KDDI（株）
KDDIデジタルセキュリティ（株）
（株）KPMG FAS
KPMGコンサルティング（株）
コインチェック（株）
興安計装（株）

（株）神戸デジタル・ラボ
（株）コスモス・コーポレイション
コニカミノルタ（株）
（株）コンシスト

【さ】
サービス&セキュリティ（株）
ServiceNow Japan（同）
サイエンスパーク（株）
（株）サイバーエージェント
（株）サイバージムジャパン New
（株）サイバーセキュリティクラウド
サイバー・ソリューション（株）
（株）サイバーディフェンス研究所
サイボウズ（株）
（株）さくらケーシーエス
Sansan（株）
GMOグローバルサイン（株）
G・O・G（株）
ジーブレイン（株）
ジェイズ・コミュニケーション（株）
（株）JSOL
JBサービス（株）
JBCC（株）
一般社団法人 JPCERT コーディネーションセンター
シスコシステムズ（同）
システム・エンジニアリング・ハウス（株）
（株）SHIFT New
Japan Digital Design （株）
情報セキュリティ（株）
（株）信興テクノミスト
ストーンビートセキュリティ（株）
（株）Speee
セイコーソリューションズ（株）
セイルポイントテクノロジーズジャパン（同） New
（株）セキュアサイクル
（株）セキュアスカイ・テクノロジー
セキュアワークス（株）
セキュリティ・エデュケーション・アライアンス・ジャパン
セコム（株）
セコムトラストシステムズ（株）
綜合警備保障（株）
ソースネクスト（株）
ソニー（株）
ソフトバンク（株）
（株）ソリトンシステムズ
（株）ソルネットシステム
SOMPOリスクマネジメント（株）

【た】
大興電子通信（株）
大日本印刷（株）
（株）ダイレクトクラウド
（株）大和総研
高砂熱学工業（株） New
（株）宝情報
タレスDIS CPLジャパン（株）
（株） 中電シーティーアイ
都築電気（株）
TIS（株）
（株）ディアイティ
デジサート・ジャパン（同）
デジタルアーツ（株）
（株）デジタルハーツ
鉄道情報システム（株）
デロイト トーマツサイバー（同）
学校法人電子学園
（株）電通国際情報サービス
東京海上日動リスクコンサルティング（株）
（株）東芝
東芝デジタルソリューションズ（株）
ドコモ・システムズ（株）
凸版印刷（株）
トランスコスモス（株）
トレノケート（株）
トレンドマイクロ（株）

【な】
（株）ナノオプト・メディア
日鉄ソリューションズ（株）
日本アイ・ビー・エム（株）
日本オラクル（株）
日本企画（株）
日本シノプシス（同）
一般財団法人日本情報経済社会推進協会 New
（株）日本総合研究所
日本電気（株）
日本電気通信システム（株）
日本電信電話（株）
日本ビジネスシステムズ（株）
日本マイクロソフト（株）
日本ユニシス（株）

ニュートラル(株)
ネットワンシステムズ(株)

【は】

パーソルテクノロジースタッフ(株)
パーソルプロセス&テクノロジー(株)
(株)バイオリンク New
(株)パソナテック
パナソニック(株)
パロアルトネットワークス(株)
ぴあ(株)
(株) 日立システムズ
(株) 日立製作所
(株) 日立ソリューションズ
(株) 日立ソリューションズ・クリエイト
飛天ジャパン(株)
(株)PFU
PwCコンサルティング(同)
華為技術日本(株)
(株)ファインデックス
(株)VSN
(株)フーバーブレイン
フォーティネットジャパン(株)
富士ソフト(株)
富士通(株)
(株)富士通エフサス
富士通クライアントコンピューティング(株)
富士フイルムシステムズ(株)
富士フイルムビジネスイノベーション(株)
(株)Preferred Networks
(株)ブロードバンドセキュリティ
(株)プロット
(株)ベネッセインフォシェル
北陸通信ネットワーク(株)

【ま】

マカフィー(株)
丸紅情報システムズ(株)
丸紅ネットワークソリューションズ(株)
みずほリサーチ&テクノロジーズ(株)
三井物産セキュアディレクション(株)
三菱スペース・ソフトウエア(株)
(株)三菱総合研究所
三菱電機(株)
三菱電機インフォメーションシステムズ(株)
三菱電機インフォメーションネットワーク(株)
(株)mediba

【や】

(株)ユービーセキュア
ユニアデックス(株)
(株)YONA

【ら】

楽天グループ(株) New
(株)ラック
Rapid7 Japan(株)
(有)ラング・エッジ
(株)リクルート
リコージャパン(株)
(株)両備システムズ New
(株)レオンテクノロジー New
(有)ロボック

【わ】

(株)ワイズ

【特別会員】

一般社団法人 IIOT
(ISC)2 Japan
大阪商工会議所
一般財団法人 沖縄ITイノベーション戦略センター
一般社団法人 コンピュータソフトウェア協会
ジャパン データ ストレージ フォーラム
一般社団法人 重要生活機器連携セキュリティ協議会
国立研究開発法人 情報通信研究機構
一般社団法人 セキュアIoTプラットフォーム協議会
データベース・セキュリティ・コンソーシアム
特定非営利活動法人 デジタル・フォレンジック研究会
電子商取引安全技術研究組合
東京大学大学院 工学系研究科
トラストサービス推進フォーラム
長崎県立大学情報システム学部情報セキュリティ学科
一般社団法人 日本インターネットプロバイダー協会
一般社団法人 日本クラウドセキュリティアライアンス
一般社団法人 日本コンピュータシステム販売店協会
特定非営利活動法人 日本システム監査人協会
特定非営利活動法人 日本情報技術取引所
一般社団法人日本スマートフォンセキュリティ協会
特定非営利活動法人 日本セキュリティ監査協会

他二社

会員紹介（当コーナーでは、JNSA で活躍されている会員の方に、リレー方式で自己紹介をしていただきます。）

株式会社セキュアスカイ・テクノロジー　羽鶴　颯

JNSA会員の皆様、初めまして、株式会社セキュアスカイ・テクノロジーの羽鶴と申します。

この度、U40部会にて「Inside IT」というWGの設立と、そのリーダーを担当することになりましたので、この場を借りてご挨拶させていただきます。

私の主な業務はWAF（Web Application Firewall）の開発、ログ監視、ポリシーチューニング、Webへの攻撃と防御手法のリサーチワークですが、最近はSPA（Single Page Application）やサーバーレス、クラウド周りの技術も扱っています。

休日は、ロードバイクに乗ってロングライドにでかけたり、カフェ巡りや一眼レフを片手に散歩をしています。同じ趣味の方がいらっしゃれば是非お話できると嬉しいです。

さて、「Inside IT」の話に入る前に、私がITの道に進んだきっかけをお話したいと思います。

最初のきっかけとなったのは中学の技術の授業でした。「HTMLを使って簡単なホームページを作ろう！」という内容だったのですが、当時の私はキレイな見た目のホームページを作るより、タグで囲まれた記号の羅列がグラフィックに変換される原理や、Google検索が目的の情報をインターネットの海から探し出してくる仕組み、そもそも、電子部品の塊でそれらの操作をどうやって実現しているのかが気になって仕方がありませんでした。

その数カ月後、Webブラウザ上の文字を読み上げることで視覚障害者を補助する製品の開発に取り組む研究者の特集番組や、某ハッカーのドラマを見て「仕組みはよくわからないけどITを使えば色んなことが出来るし退屈しなさそう！、これはもう、プログラマになるしかない！」という、いかにも中学生らしい理由でITの世界に足を踏み入れました。

前置きが長くなってしまいましたが、「Inside IT」は、そんなブラックボックス化が進んだ近年のITの裏側を知ることで、一歩進んだ技術の活用や、地方や日本のITの底上げを目指したWGです。「プログラムが動く仕組み」、「インターネットに繋がる仕組み」、「Webサイトが表示される仕組み」を学ぶ半日程度のワークショップを全国で開催することが当面の活動となる予定です。「内部」を知った上でよりエレガントなやり方で目的を達成できたときの嬉しさを、WG活動を通して少しでも多くの人に届けられたらと願っております。

最後に、まだまだ勉強中の身ですが会員の方々との交流を通して、IT業界ならびにセキュリティ業界の発展に少しでも貢献できればと考えておりますので、ご指導ご鞭撻の程、よろしくお願い致します。

会員紹介（当コーナーでは、JNSA で活躍されている会員の方に、リレー方式で自己紹介をしていただきます。）

株式会社ソリトンシステムズ　米澤　美奈

JNSA会員の皆様、はじめまして。株式会社ソリトンシステムズの米澤と申します。この度、西日本支部の支部長であるアイネットシステムズ株式会社 元持様からのご推薦、並びに事務局からのご用命で自己紹介の機会を頂きました。どうぞよろしくお願い致します。

<経歴>

2014年　前職時代に、初めてJNSA 西日本支部に出会う。
→ 「中小企業向け情報セキュリティポリシーサンプル作成」の取り組みに感銘を受ける。

2017年　株式会社ソリトンシステムズ に 転職
→ 海外メーカー製の「高度なサイバーセキュリティ」を競って売り込む市場のブームとは対象的に、セキュリティの1丁目1番地であるID管理をベースとしたソリューション展開に魅力を感じ入社。

2021年現在　ソリトンシステムズ内で、セキュリティ製品のメーカー営業として活動中。

※セキュリティ業界に携わってきた年数は長くなって来ておりますが、まだまだ勉強の日々です。

私は、普段は、セキュリティ製品のメーカー営業という立場、つまり 「伝える」事をメインに活動しています。世の中の多くの人は、IT、IoT、情報通信、セキュリティ etc…という言葉を意識せずに日々を過ごしているわけですが、影響を受けずに生活できている人は、皆無に等しいです。そういった人達が、安全に効率的に業務を進めて行けるように、考える・啓蒙する・説明する・提案する事が、私の仕事と考えています。

そういった意味で、長年にわたり中小企業にフォーカスして「セキュリティ」のあり方を考え、伝えてきている西日本支部の活動は、非常に意義深いと考えています。少しでも、勉強したい気持ちで参加させていただいております。

つい先日、自社の業務の中で、自身の活動について考える機会がありました。私は「営業」ですので、ビジネスという視点も活動の重要なファクターです。自社製品には、多くの人が求める機能が搭載される方が売りやすいと考えてしまいがちです。しかし、多くの人が求めるものが、セキュリティの観点で正しいとは限りません。「この機能を搭載するべきか」というテーマで、社内の様々の人の間で議論となりました。日本人は、よく知らない事を敬遠しがちです。そして、ビジネスの現場では、「簡単に儲かる」ものを求めがちです。しかし、「伝える」立場の私達が安易な方へ走るべきではないな と、本来あるべき姿を忘れるべきではないな と思った瞬間がありました。

本来あるべき姿を知る・考える・伝える為に、西日本支部で勉強させていただき、ほんの少しだけでも貢献できたら幸いだな と 考えている今日この頃です。

それでは、皆様、今後とも、よろしくお願い致します。

JNSA 会員特典

■会員の特典

1. 各種部会、ワーキンググループへの参加
2. 会員向け勉強会への参加
3. 活動報告書や成果物の会員限定情報の入手
4. 会員専用 Web やメーリングリストでの情報入手
5. 人脈拡大と相互交流
6. 教育受講やイベント参加時の会員割引
   （CISSP、SANS、セキュア Eggs,、EC-Council 等）
7. 製品・サービス紹介サイト
   （JNSA ソリューションガイド等への情報登録）
8. 理解度チェック・プレミアムの販売（代理店）
9. 調査研究プロジェクトへの参画
10. JNSA 会報誌の配布

お問い合せ

特定非営利活動法人
日本ネットワークセキュリティ協会　事務局
〒105-0003 東京都港区西新橋 1-22-12 JC ビル 4F
TEL：03-3519-6440
TEL：03-3519-6441
E-Mail：sec@jnsa.org
URL：https://www.jnsa.org/

西日本支部
〒532-0011 大阪府大阪市淀川区西中島 5-14-10
新大阪トヨタビル（株）ディアイティ内
TEL：　06-6886-5540

入会方法
　Web の入会申込フォームにて Web からお申し込み、または、書面の入会申込書を FAX・郵送にてお送り下さい。折り返し事務局より入会に関する御連絡をいたします。

JNSA Press vol.50

2021 年 7 月 1 日発行
©2021 Japan Network Security Association
発行所
特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）
E-Mail: sec@jnsa.org　URL: https://www.jnsa.org/

印　刷
プリンテックス株式会社

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

〒105-0003 東京都港区西新橋1-22-12 JCビル 4F
TEL 03-3519-6440　FAX 03-3519-6441
E-mail: sec@jnsa.org　URL: https://www.jnsa.org/

西日本支部
〒532-0011 大阪府大阪市淀川区西中島5-14-10 新大阪トヨタビル （株）ディアイティ内
TEL 06-6686-5540