SPRING 2022
VOL. 51

JNSA PRESS

JAPAN NETWORK SECURITY ASSOCIATION

寄稿記事

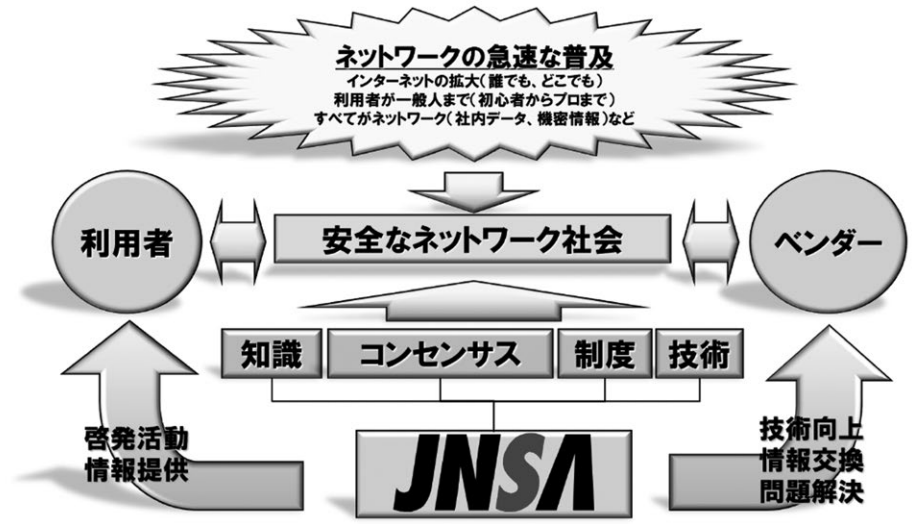
特定非営利活動法人 日本ネットワークセキュリティ協会
NPO Japan Network Security Association

JNSAの22年を振り返って

NPO日本ネットワークセキュリティ協会
事務局長　下村　正洋

JNSAは2000年4月13日に任意団体（翌年NPO法人化）として発足し、22年が過ぎようとしています。そこで、設立時の情報セキュリティを取り巻く社会状況と設立後数年の活動を振り返り、現在の状況を比較し、これからのサイバーセキュリティ(設立当時はネットワーク・セキュリティと言っていました)とJNSAの今後の方向性について考えてみたいと思います。

JNSA設立の検討を開始した前年1999年には、3月にMelissaウイルスが猛威を振るい、5月に京都府宇治市で21万人の住民基本台帳の漏洩事件、2000年1月には中央省庁Web改ざんが発生しました。インシデント事案以外には、1996年にJPCERT/CC創立、1998年にはPマーク制度開始、関係省庁にも情報セキュリティに関する部署が設立され、2000年2月にはNISCの前身である情報セキュリティ対策推進室が内閣官房に設置されました。以後、2002年にはISMS認証制度が始まるなど、情報セキュリティ対策関連の制度・製品・サービスも次々登場し、情報セキュリティ対策の重要性を認識した人たちにより、それを推進するための仕組みづくりが始まった時期でした。そのような中で、JNSAはセキュリティベンダーが相互に情報セキュリティ問題を共有し、かつ、連携し、社会全体の情報セキュリティ対策が進むことを目的として設立しました。設立当初の会員数は54社（2021年末は260社）でした。



設立時の活動概念図

設立当初（2000年）の主な活動は、外部接続に関するセキュリティポリシーサンプルの作成、セキュリティ評価基準の実態調査、IPsec製品の相互接続実験、PKIの研究、製品・サービスの一覧表の作成、技術用語の考察、不正アクセス調査、ダイナミックディフェンス（動的防御）フレームワーク開発でした。翌年（2001年）にはセキュリティ被害調査、コンテントセキュリティの活動が開始し、セキュリティ技術者育成のための教育部会も発足しました。以後トピックとして一般向けインターネット安全教室開始（2003年）、セキュリティ技術者知識体系SecBoKの前身となるSkipmapの開発、情報セキュリティ教育事業者連絡会-ISEPA-(2007年)、日本セキュリティオペレーション事業者協議会-ISOG-J-(2008年）設立と続きます。その後、2009年に大幅な部会組織の改定を行って、現在の部会構成になっています。詳しくはこの冊子の後半に掲載している「事務局お知らせ：JNSA部会・WG活動内容」をご覧ください。

さて、振り返りが長くなりましたが、設立当初（約20年前）と現在の活動の分類を見ると、基本的には情報セキュリティが抱える課題の分野は大きな変化が起こっていないと見えます。これは、つまるところ、セキュリティ問題は人の活動にかかわるものであり、人が構築したもの、それを利用する人、その人達で構成する社会システムなどの脆弱性とその脆弱性を利用した不正や過失をいかに抑制するかが課題だからと考えます。ただし、すべてのものがインターネットに接続される状況（IoT）の進化とともに、情報セキュリティという語り口がサイバーセキュリティに変化し、企業活動はもとより、一般人の社会生活にも深く関係し、加えて国家安全保障問題になってきたのは、いまさら指摘することではないと思います。

とくに、近年ゼロトラストの概念が提唱されてきていますが、それまでは境界防御をいかにするかが重要なテーマでした。これは、今猛威を振るっているCOVID-19の水際作戦やバブル方式とまったく同じ発想であり、それが破綻するのも人の動きを制限することが実質的に、つまり、経済活動や人の社会活動に対抗する方式であるためだと考えます。したがって、接種証明書、検査証明書、対策済みマークなどそれぞれの主体の健全性を証明しつつ接することが必要であり、そのような対策が迅速に進めることができる社会システム（社会的コンセンサスも含む）の構築が急がれているのではと考えます。同様にサイバーセキュリティを推進するにおいて、流通する情報（データ）そのものとその情報にアクセスする主体（システムだけでなく人も）の信頼性の確保が重要になっているのではないでしょうか。加えて、DXを推進し、その安全を確保するためのセキュリティ対策が進展してゆく中で、システムが現在よりも密接に連関することにより、社会システムとして脆弱点が絞られてくる懸念があり、これが社会全体の脆弱性に発展すると考えます。したがって、サイバーセキュリティ対策を推進する上において、単に攻撃や不正、過失を防止するというITシステム的対応だけでなく、セキュリティ対策を推進した結果として創出される社会において、民主主義を堅持し、人権を守るという視点からの社会全体のシステム設計が必要ではないかと考えます。つまり、セキュリティ対策を進めるためには、統制力を強めるこ

ととシステムのスマートな連携が必要であるが、統制が専制を誘発しないように、かつ、連携したシステムが社会のメルトダウンを惹起しないように工夫しなければならないのではないでしょうか。2002年に発表された「OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security(情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて)」を今一度読むのもいいのではと思います。

JNSAは、単にセキュリティ対策を推進するのではなく、調和のとれた、すべての人々にとって安寧な社会を実現するために活動しなければならないと考えます。今まで述べてきたようにサイバーセキュリティは様々な要素があることから、一つの企業や組織、個人では解決できないことです。JNSAは前述した設立の理念を堅持して、これから、ますます情報セキュリティ(サイバーセキュリティ) に関係する企業や組織や人々が増えてくる、否、すでに全てがサイバーセキュリティに関係している現在において、これらの参加者 (OECD9原則参照) の方々が集まり、問題を共有し、解決策を検討し、会員各位の皆様へ、ならびに社会に対してフィードバックできるような場を提供し続けることが必要ではないかと考えます。

中央銀行デジタル通貨（CBDC）におけるセキュリティ考察

日本電気株式会社　シニアエキスパート
デジタルアイデンティティ WG　リーダー
宮川　晃一

1．はじめに

デジタル通貨と聞くと、一般的にはビットコインに代表される仮想通貨（暗号資産）のことを思い浮かべる方が多いかと思うが、ここでは国の通貨すなわち、自国の中央銀行で発行される通貨のデジタル通貨（ 以下、CBDC：Central Bank Digital Currency ）を対象とする。

デジタル通貨については、日本国において現状では導入検討および実験段階にあり、具体的に発行されるかは決定されていないが、現状で考えられるセキュリティ課題、特にデジタルアイデンティティにフォーカスして考察したので解説する。

2．CBDC検討の背景

CBDCのセキュリティ考察の前に、日本におけるCBDCが検討されるようになった背景や諸外国の状況ついて整理した。

2.1 現在通貨の課題

我が国ではデジタル田園都市国家構想をはじめとして、社会基盤そのものがデジタル化に向けて大きく変革をしようとしているが、その中でもデジタル化が難しいとされている1つが「日本銀行券」すなわち「通貨」と言われている。現状「通貨」には以下のような特徴がある。

（メリット）
- ・国内では、いつでも、だれでも利用ができる（ユニバーサル性）
- ・即時に決済が完了できる（即時決済性）
- ・他国の通貨と交換可能（相互運用性）
- ・電力を必要としない（デジタル対比）　　など

（デメリット：主に現金）
- ・「通貨」を持っている人が「所有者」であるため、「通貨」 自身から「所有者」を判別できない
- ・盗難・紛失や火災などの災害に弱い
- ・偽造対策等セキュリティ対策にコストがかかる
- ・資産の把握が難しい　　など

2.2 デジタル時代に向けた課題

一方、デジタル化に向けた課題として、民間の決済サービス（クレジットカード、電子マネー、QRコード決済サービスなど）にて複数の事件・事故が発生しており、その安全性や堅牢性および補償については今後も十分な検討と対策が必要な状況にある。また、同時に中小小売店のキャッシュレス化の促進を行う必要があり、民間レベルで解決するのは難しい実情もある。また、COVID-19を背景にした給付金等の配布については多大なコストをかけて各省庁や自治体等が実施している状況があり、これら課題に対して「デジタル通貨」が果たす役割は大きなものになると思われる。

※本書の内容は私見であり、必ずしも所属企業先の見解と一致したものではありません。

3．CBDCとは

具体的にCBDCとはどのようなものか、特徴などについて整理する。

3.1 デジタル通貨の分類

IMF（国際通貨基金）レポートによると「デジタル通貨」は以下（図01）のように分類される。（発行主体別、価格変動の有無、世界中で発行決済可能かと言った分類）

- CBDCは発行主体が中央銀行である点が他のデジタル通貨と大きな差がある。
- 民間主体のデジタル通貨は価値が変動することや、補償がない場合もある。

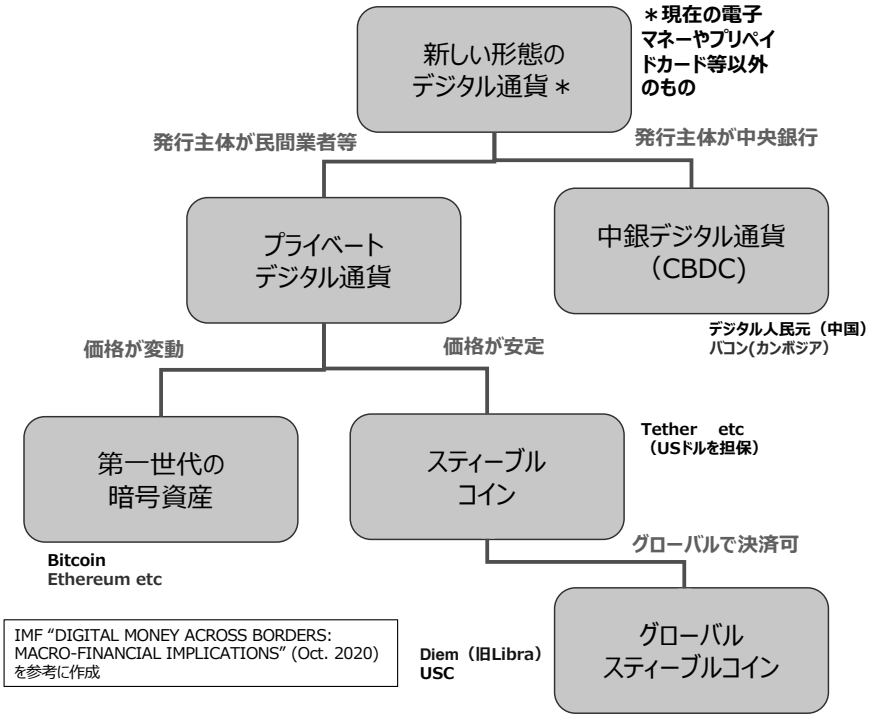


図01　デジタル通貨の分類

3.2 CBDCの特徴

Bitcoinのような暗号通貨が特定の団体や企業などによって発行されるのに対し、CBDCではあくまで各国の中央銀行が発行する。法定通貨ではない暗号通貨はその価値がそのときどきで変化する。一方で、CBDCはあくまで現行の法定通貨と等価であり、その価値は変化しない。こうした価値が特定条件で固定されるデジタル通貨を「スティーブルコイン」と呼ぶ。２章で述べたデジタル化の課題の解決の他にも、CBDCを通じて各国の金融システムが接続されれば、現状でSWIFT(国際送金）を使って行なわれているメッセージ中継がよりシンプルで高速なものになり、送金手数料も安価となるメリットがある。そしてブロックチェーン技術を用いてスケーラビリティやパフォーマン

スの問題を解決できれば、既存金融システムの置き換えで資金の流通がよりスムーズで活発になると想定されている。

CBDCの発行形態や管理方法については以下のようなものがある。また、発行形態と管理方法の組み合わせで4つのモデルがある。（図02）それぞれ、実際に運用するには法的な根拠の整備も含めて検討が必要な状況である。

（発行形態）

・**直接型**：各国中央銀行が直接CBDCを配る

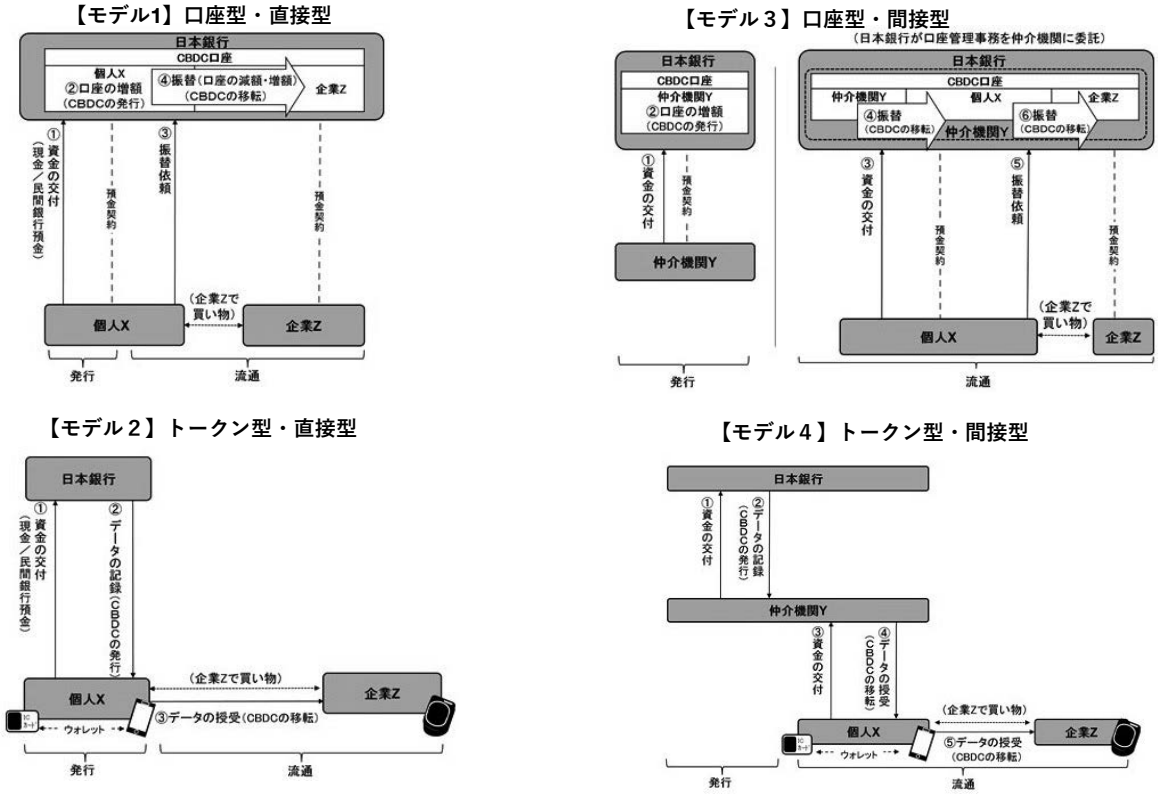
・**間接型**：民間の銀行を介してCBDCを配る

どちらの発行形態においても、AMLのためのKYC機能の実装が必要であり、アプリケーションのセキュリティ対策・機能追加のため継続的なアップデートが必要になる。間接発行の場合はこの役割を銀行が担う形になる。

（管理方法）

・**口座型**：利用者からの振替依頼に基づき、発行者が口座の減額記帳および増額記帳をすることにより、価値が移転する方式。銀行預金がその代表例

・**トークン型**：何らかの媒体に金銭的価値が組み込まれたものであり、銀行券や交通系カードなどの電子マネー等があたる。これらは、紙と電子媒体という違いはあっても、媒体に組み込まれた金銭的価値の移転によって決済を行うという基本的な仕組みは共通である。



https://www.boj.or.jp/research/wps_rev/lab/lab19j02.htm/

出典：中央銀行がデジタル通貨を発行する場合に法的に何が論点になりうるのか：
「中央銀行デジタル通貨に関する法律問題研究会」報告書の概要

図02　CBDCの発行形態と管理方法のモデル

3.3 CBDCの基本要素

CBDCを実装する上で必要な基本要素について以下に解説する。

・ユニバーサルアクセス

現金と同様に、「誰でも使える」原則である。支払いや送金に使用する端末やカードなどによって利用者を制限することがないような工夫が求められる。

・セキュリティ

安心・安全にCBDCを利用するには、偽造や不正行為を排除するために高度なセキュリティ対策が必要である。

・強靭性

「いつでも、どこでも使える」ものとするための原則である。利用者が24時間365日利用できる仕組みが求められる。特に自然災害などで電力が確保できない場合の想定などは重要なポイントとなる。

・即時決済性

現金と同様に決済の支払い完了性ならびに即時決済性が求められる。また、多数の利用者が一斉に決済を行なったとしても問題のない仕組みが要求されることから、十分なシステムの拡張性や柔軟性が求められる。

・相互運用性

民間の決済システムとの相互運用性の確保や将来の高度な決済サービスに適応できるような柔軟な構造が求められる。

4．諸外国および国内の取り組み状況

4.1 諸外国の状況

世界各国の中央銀行は急速に中銀デジタル通貨への関心を高めており、特に新興国で積極的である。中国では基軸通貨米ドル支配からの脱却、人民元の国際化を企図し、デジタル人民元の開発を急ピッチで進めており、大規模な実証実験を進めている。また、多国間によるマルチCBDCの議論も始まっている。

（米国） 米連邦準備理事会（FRB)はCBDCに対し慎重な姿勢だが、他国と協調しながら、技術研究や必要な規制整備の議論は世界の先頭にたって進めていくという考えを示している。
2022年1月、FRBはCBDCに関するディスカッションペーパーを公表し、CBDCへの取り組みをやや前向きに進めていく方向性を示した。

（EU） 欧州中央銀行は2020年10月、デジタルユーロに関する報告書（ECB "Report on a digital euro"を公表し、デジタルユーロ発行における原則と要件を定めた。
この報告書に基づき公募した意見を基に、デジタルユーロを発行するか否かの方針を発表する予定。

（インド）インド政府は2022年2月にインド準備銀行がCBDC（デジタル・ルピー）を2023年年度中に導入する計画を発表した。

4.2 国内の状況

日本銀行は、現時点でCBDCを発行する計画はないが、将来必要になった場合に対応できるよう検討を進めており、期待される機能と役割、具備すべき基本的な特性や考慮すべきポイントを整理した。また、システム的な実験環境を構築しCBDCの機能に関する概念実証をおこなっている。また、さらなる検証が必要と判断されれば民間事業者や消費者が実地に参加する形でのパイロット実験を行うことも視野に入れて検討する。としている。
しかしながら、実現までには課題も多く、まだ相当の時間がかかると思われる。民間でも、様々な業界の主要各社

30社以上がそれぞれの分野で求められるCBDCの仕組みの検証を行う「デジタル通貨勉強会」プロジェクトが発足し、2020年11月に最終報告書のリリースと「デジタル通貨フォーラム」の結成を行った。「デジタル通貨フォーラム」では、CBDCそのものではなく、民間銀行主体のデジタル通貨を目指しており、CBDCとは補完する関係として検討がすすめられている。

5．CBDCにおけるセキュリティ考察

CBDCにおけるセキュリティを7要素で分類して考察してみる。また、後半でデジタルアイデンティティの課題について考察した。

5.1　情報セキュリティの7要素

一般的に情報セキュリティはＣＩＡで語られることが多いが、今回はＣＩＡ+4つの要素の7要素にて考察する。各要素の簡単な説明は以下の通りである。

機密性（Confidentiality）　情報が漏れないこと
完全性（Integrity）　情報が改ざんされることなく維持されること
可用性（Availability）　情報を利用したい時に利用できること
真正性（Authenticity）　情報およびその利用者が本物（本人）と確認できること
信頼性（Reliability）　情報システムを構成する機器が意図した通りに動作していること
責任追跡性（Accountability）　問題が発生した時のその動作が開始された元まで追跡できること
否認防止（Non-repudiation）　あとから否認（否定）ができないこと

5.2　CBDCにおける7要素の考察

CBDCの基本要素と特に強く関係性があると思われる事項について考察を行なった。

1）機密性

CBDCでは、誰がいくら保持しているかの情報や、いつ誰がどこでどのような決済にいくら決済したかの情報がデジタルで記録されることになる。このような情報はプライバシーな情報であり、その取得や管理及び利用については十分な検討が必要である。もちろん、デジタル通貨自体へのアクセスは厳密に管理ができる仕組み（デジタルウォレット等）が必須である。また、採用する方式によっては利用するデバイスのセキュア領域や鍵管理などの検討も必要。デジタルアイデンティティとの関係性について後述する。

2）完全性

「通貨」において、その価値が毀損されることは大きな問題である。CBDCにおいても、「改ざん」ができない仕組みが求められる。暗号通貨にブロックチェーンが利用される背景はここにある。

3）可用性

CBDCの基本要素である「強靭性」と関係性がある。利用者が２４時間３６５日利用できる仕組みが求められる。また、誰でも使えるようにしなければならないことから、ユニバーサル性も「可用性」に該当すると考える。

4）真正性

デジタル世界においては、物理世界との結びつきである本人性が非常に重要である。金融の世界ではAMLの観点からKYCが重要視されているがCBDCにおいても、本人確認（個人・法人問わず）が重要事項である。デジタルアイデンティティとの関係性について後述する。

5）信頼性

CBDCの基本要素である「即時決済性」が該当すると考える。多数の利用者が一斉に高度な決済をおこなっても正確、即時処理できるシステムの信頼性を重要である。また、災害や障害にも強い仕組みやシステムが要求される。

6）責任追跡性

何か問題が発生した場合、その処理が行われたログを確実に保管しておくことは重要である。仮に係争になった場合にも耐えられるような仕組みが必要である。デジタルアイデンティティとの関係性について後述する。

7）否認防止

決済や送金においては、確実に行われたことを保証する必要がある。それは、決済や送金がされてないと相手から否認された時の重要な証拠になり得るからである。デジタル署名技術などの活用が考えられる。

5.3　CBDCにおけるデジタルアイデンティティの重要性

「インターネット上ではあなたが犬だと誰も知らない」（On the Internet, nobody knows you're a dog）（図03）という有名な戯画がある。お分かりのとおり、インターネットを通した端末を操作しているのは正当な本人ではないかもしれないことを示唆している。

CBDCの実現には確実なデジタルアイデンティティ管理の実現が不可欠である。現在、金融口座開設時には犯罪収益移転防止法に則した「本人確認」が金融機関の業務としてマネーロンダリングを防止することを目的に行われている。

出典：Wikipedia: On the Internet, nobody knows you're a dog
https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

図03　On the Internet, nobody knows you're a dog

CBDCにおいは、３.２文で述べた4つのモデルのどれにおいても「本人確認」は非常に重要な事項であり確実に実施する必要がある。よって、CBDCにはAML/KYCの機能実装は不可欠であり、かつ様々な決済や送金の高度化や自動化に柔軟に対応できる AML/KYCが必要である。

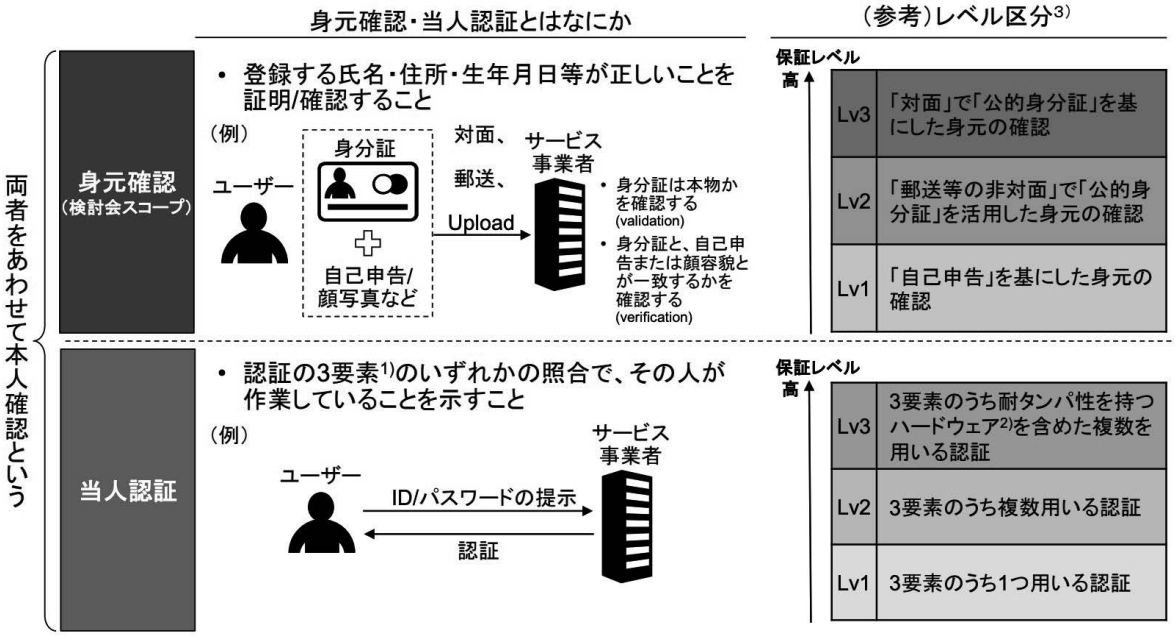
ここで、今一度確認すべき事項として「本人確認」がある。「本人確認」には「身元確認」と「当人認証」の2つの

側面がある。「身元確認」は、ユーザー当人の実在性を確認し、「当人認証」は、ユーザーの行為を確認する。通常両方の組み合わせを通じて「本人確認」が行われる仕組みである。（図０４参照）

また、５. 1の７要素の「機密性」「真正性」はまさに「本人確認」そのものである。CBDCにおけるKYCは「身元確認」であり、実際に利用する場合は「当人認証」によって真正性が担保され利用する。「身元確認」は初回時の確認（On Boarding）とその後の継続的に確認（On Going）するものに大別されるが、CBDCのユニバーサル性を考慮しながら継続的に「身元確認」を行うには、CBDC利用者の信頼の源泉（トラストアンカー）が必要になる。

CBDCの利用者という側面から考えると、個人以外にも法人や訪日・在留外国人等もあるため、CBDCにおけるトラストアンカーおよび保証レベルをどのように定義するかは、今後真剣に検討が必要と思う。欧州にて構想中の欧州デジタルIDウォレット（European Digital Identity Wallet）等を参考にすべきと考える。

CBDCは現金と同様の機能を持たせるべきとの意見もある。現金は持っている人が所有者であり、決済する度に「本人確認」をされることは高額な決済を除いてほぼない。CBDCにおいても、少額決済においては匿名性を持たせる必要があるとの意見である。これは、Pseudonymization（注１）と言われる手法で匿名化（仮名化）を行うことが可能になる。仮名化は匿名化と違い可逆性があるのが特徴とされる。よって、「責任追跡性」が失われることがない。CBDCはこのように一定のプライバシーに配慮したものでなければ、国際的な相互運用は難しいと思われる。



1)認証要素は「生体」（顔・指紋など）・「所持」（マイナンバーカードなど）・「知識」（パスワードなど）に分かれる
2)マイナンバーカードなど、内部の情報に対する不正な読み出しが困難である物理装置
3)「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（2019年2月CIO連絡会議決定）のレベル区分

出典：オンラインサービスにおける 身元確認手法の整理に関する 検討報告書
https://www.meti.go.jp/press/2020/04/20200417002/20200417002-1.pdf

図０４　本人確認とは

6．最後に

現在、日本のCBDCについては具体的な実施計画はないものの、世界情勢を見ながら実証実験を進めつつ議論が深まって行くと思われる。今回はデジタルアイデンティティに少しフォーカスして考察したが、他にも検討すべき技術課題（例えば、CBDCにリンクする形でのデジタルウォレット技術の標準化など）や法的課題（日本銀行法の改定など）が多くある。CBDCは今後のデジタル時代には必須のインフラとなることから、これら課題を慎重に議論し進めて欲しいと思うが、セキュリティと利便性のバランスを高次元でバランスした安心・安全の仕組みをぜひ構築して欲しい。

【参考文献】

[1] 日本銀行：中央銀行デジタル通貨に関する日本銀行の取り組み方針
https://www.boj.or.jp/announcements/release_2020/data/rel201009e1.pdf

[2] 日本銀行：中央銀行デジタル通貨：エグゼクティブ・ペーパー
https://www.boj.or.jp/announcements/release_2021/data/rel210930e1.pdf

[3] 井上哲也：デジタル円 日銀が暗号通貨を発行する日－日本経済新聞出版 (2020/7/18)

[4] 木内 登英：決定版　銀行デジタル革命―現金消滅で金融はどう変わるか
東洋経済新報社 (2018/8/24)

[5] IMF “DIGITAL MONEY ACROSS BORDERS: MACRO-FINANCIAL IMPLICATIONS” (Oct. 2020)
https://www.imf.org/en/Publications/Policy-Papers/Issues/2020/10/17/Digital-Money-Across-Borders-Macro-Financial-Implications-49823

[6] デジタル通貨勉強会
https://about.decurret.com/dc-forum/studygroup.html

[7] デジタル通貨フォーラム
https://about.decurret.com/dc-forum/

注1）Pseudonymization
スードニマイゼーション（Pseudonymization）：仮名化
氏名や住所などの個人データのうち、「誰」と特定できる部分を「仮名」に暗号化し、データから直接個人を特定できなくすること。

昨今の標的型攻撃メール訓練の実施課題

みずほリサーチ&テクノロジーズ株式会社
伊藤　聡司

1. はじめに

コロナ禍を起因としてここ数年で働き方も大きく変わり、企業に求められるセキュリティ対策も在宅などのリモートワークを考慮したものにシフトをしている。昨今の状況の変化に合わせて犯罪者側も未成熟状態の業務スタイルの隙を突き被害者の認識の甘さの利用や、企業側の対策未整備箇所の脆弱性を突き攻撃を変化させてきている。企業がセキュリティ対策に力を入れても、ばらまき型や標的型に代表される不審メールついては最終的には人間の判断で開いてしまう事が太宗となっている。このため各企業は標的型攻撃メールの訓練を行い社員のリテラシー向上を図る対応を迫られている。しかし、この標的型攻撃メール訓練は実際の効果を定量的に図りにくく、費用を含めた運用コストが掛かるものとなっている。

本稿は、現在の環境での標的型攻撃メール訓練の効果を上げる考え方、訓練担当者が直面する課題、結果の分析などに対する考えを述べていく。現在訓練を検討している担当者、既に実施している担当者の方に活用頂ければ幸いである。

2. 標的型攻撃メール訓練での指標

標的型攻撃メール訓練の実施で用いられる指標は主に２種類ある。一般的には「開封率」「報告率」と呼ばれている訓練結果を評価する際に用いられているものである。

開封率は、訓練対象者の中で、メール本文内にあるURLや添付ファイルを開いた人の割合だ。つまり「訓練用のメールに引っかかってしまった人」の割合と言える。

報告率は、訓練内容に応じて２つの指標があると私は考えており、過去に別媒体での記事※にて以下のように定義したので本稿においてもこの定義を用いていきたい。

受信報告率： 訓練メールを開封せずに「不審メールの受信を報告した人」の割合

開封報告率： 訓練メールの開封後に「不審メールの開封を報告した人」の割合

また、これらに加えて標的型攻撃メール訓練の自社の数年後の目標到達点を定義し、現在の立ち位置を分析した上で訓練を計画する事が望ましい。

3. 訓練指標の測定方法

これらの指標について、開封率はセキュリティベンダーが提供しているサービスの利用、又は自社で同様の仕組みを作る事で自動的に集計をするものが大半である。しかし、報告率については被訓練者が自主的に報告する何らかのアクションが必要となり、利用するベンダーのサービスによっては一部を自動化する方法は存在するが、被訓練者の動きも含めて完全に自動化して集計を行う事はできない。尚、この報告率を集計する訓練は組織が定めている規定に従い報告対応が出来ているかを評価する事が一般的である。この規則には自社環境を管理する部門への連絡タイミングや感染したと考えられる端末の扱いについて定められている事が太宗となっている。そのため被訓練者が自社の規則を何処まで把握し対応する事ができるかというものが報告率から得られるものである。

4. 訓練実施の課題

昨今の標的型攻撃メール訓練は、訓練担当者が計画時に考慮すべき検討事項が増加傾向にある。特に訓練を成立させるための環境面の技術的な事前確認、設定に掛かる工数見積り、訓練用文面・運用の工夫などは解決していないと十分な訓練成果を見込

※ https://www.itmedia.co.jp/enterprise/articles/1908/01/news004.html

む事が出来なくなる。そのため訓練を実施する上での課題を技術面、信頼度、経営理解の３つの視点で述べていきたい。

4.1　環境面における技術的な課題

昨今のリモートワーク環境促進により周囲に相談せず個人の判断で受信した不審メールを開封するような攻撃側優位の状況がより整ってきている。その対策として企業側がセキュリティ強化を講じた結果、訓練用メールが期待動作をしない場合がある。同様に添付ファイルに使われる Office 製品のセキュリティ対策も近年では強化されており訓練を成立させる上での考慮点となっている。これらは事前に確認をしていない場合、実際の訓練時に判明しコストを掛けてやり直すという事態も想定される。

それぞれ「メールセキュリティ対策製品」「外部アクセス制御」「Office 製品」の３点に分けて説明し最後に設定箇所を述べたい。

4.1.1　メールセキュリティ対策製品

メール対策ソフトでの注意点は、対策ソフトが不審メールとして判断し被訓練者にメールが届かないといったものが代表的である。これに加えて最近の対策ソフトは事前にメール内容をサンドボックスのように検証する機能が存在しており URL や添付ファイルを疑似的にチェックする事ができる。この過程でクリックした事となり被訓練者に届く前に開封などをした通知がサービス側に届くといったケースがある。尚、後者の場合は開封率がほぼ同一時刻に 100% となる結果が確認できるため判別がつきやすい。

4.1.2　外部アクセス制御

企業によっては社内環境から外部へのアクセスを制限している場合もある。メール本文の URL クリックや添付ファイル開封時の集計の仕組みは http 通信を利用した外部アクセスである。よって、外部アクセス制御が掛けられている場合は URL 型・添付ファイル型は共に通信が遮断され結果の集計をする事が出来ない。

4.1.3　Office 製品の挙動

添付ファイルについては､「編集を有効にする」「コンテンツの有効化」などの所謂、保護ビューに関わる端末の設定状況によっては開封の通知が動作しない事がある。これは添付ファイルが外部に通信する際に許可されていないといけない権限などが関係する。更に外部通信をするという事自体が通常では発生しない事なので Office 製品が保護をしているものとなっている。近年はこのセキュリティ強化が起因で Office 製品を使った添付ファイルでの訓練を期待通りに行う事が難しくなっている。

4.1.4　設定箇所と必要な情報

メールセキュリティ対策、外部アクセス制御などは製品の仕様としてホワイトリスト登録など例外設定が可能な事が一般的である。訓練担当者は事前にこの設定が可能な事と、設定に必要な情報を把握している事が望ましい。特に訓練担当者自身の所属と別組織に依頼する時などは経緯説明などを含めて想定以上の期間が掛かる事がある。また、これらの設定に必要な情報は環境や製品毎に異なるため一概にこれが全てという事ではないが対策箇所と設定事項を図１に纏めた。訓練の運用担当者は自社の環境を精査した上で計画を立てなければならない。

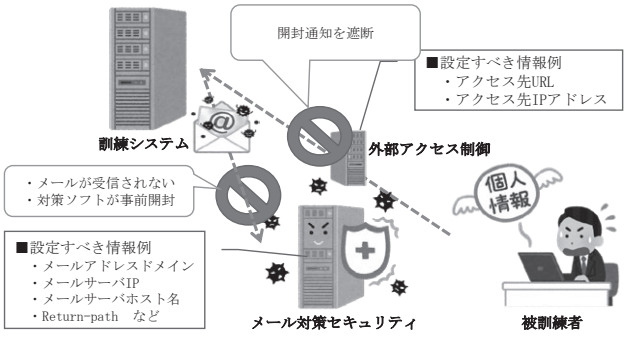


図1：セキュリティ対策箇所

4.2　訓練実施における信頼度の課題

環境面の課題と並行して取り組むべき事は、訓練の質についての検討となる。特に訓練結果の信頼度に関わる主な課題は２点存在する。

これらの課題に対し訓練担当者は対策を立てる、方針を決めるなどして割り切るなど計画を立てていく必要がある。

１：訓練メールであることが周知される
２：報告率を測る際の開封率が低い

１つ目は開封する可能性のある社員が周知された事で引っかからず結果に集計されない図２に示したような状況となる。対策としては訓練を細かく分割し同一組織内で共有されないように訓練日を分ける、異なる文面を用意するなどがあるが、これは訓練関係者の人件費やサービスの利用料など工数に直結するため自組織の予算や体力を勘案する必要がある。

２つ目は報告率を評価するための標本数として少ない場合を意味する。極端な例だが 1000 人の会社で 10 名開封し、その中で 8 名が報告した場合、開封率は 1% であり、報告率は 80% となる。この 10 人の報告率の結果をもって自社全体の状況を正確に測れるとは言い難い。対策としては事前に開封率の目標を定め、自社の被訓練者のリテラシーや文化を分析する。その結果から一定程度開封すると想定される訓練メールの文面を作り込む事が必要となる。ここはある意味訓練担当者の腕の見せ所となる。

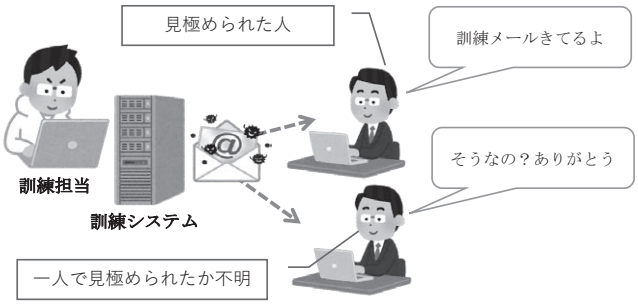


図2：訓練時の組織内共有の例

4.3 経営層への説明課題

訓練担当者は経営層に報告する際に自社社員の標的型攻撃メールに対するリテラシーがどの段階であるか説明し数年に渡るロードマップを示した説明をする必要がある。これを行わない場合、結果だけを見た経営層が過剰に反応し過度な対応を指示する場合などがある。

そのため事前にその年の訓練の位置づけを説明し理解を得た上で実施するのが望ましい。特に開封率については報告率の精度を上げるために一定の開封者が必要となる。よって開封率の高さは参考値であり、本当に見るべきものは報告率と自社の現在のリテラシーの成熟具合である事を説明し理解してもらう事が必要となる。

5. 訓練結果報告の考慮点

5.1　経営層が気にする事

訓練担当者は訓練の実施後に結果を経営層に報告する必要がある。経営層への報告は自社の客観的な結果を示し、次年度以降に向けた方針と必要な予算の了承を取り付けるという重要なものとなる。体制も予算も据え置きという結果では自社のリテラシー向上は望めない。

ここで担当者が考慮すべき点は経営層が求めている報告内容は自社の客観的な状況であるという点だ。よって報告は開封率や報告率などの客観的な指標を用いた報告を行う必要があるが、単年の自社報告のみだと経営層が判断出来ず十分な報告とならない。そのため、過去の自社との変化、他社との比較など縦横の客観的差異を示す事で説得力を持たせる必要がある。ただし、他社との比較は訓練の前提条件や使っている指標の差などを明確にした上で比較報告をしないと見た目の数値で優劣を判断されてしまうので十分な分析をした上で報告に臨む事が必要となる。

5.2　比較に必要な他社の情報入手

経営層へ報告する際の準備として、「過去の自社

との比較」「他社との比較」など縦横の軸を用いて報告を組み立てる事が出来るように準備をする必要がある。特に訓練初年度は過去の自社との比較が不可能なため、横の比較が重要となる。比較対象としては「他業種との比較」「同業種との比較」といった業種全体のものから「同業種のA社」や「同グループ会社B」のような個別のものがある。業種全体については、例えば利用している標的型攻撃メール訓練サービスを提供しているセキュリティベンダーから提供を受ける事が考えられるが、「開封率」の情報のみとなり、守秘義務の関係上個別の情報開示は難しいだろう。また、「報告率」についてはサービスを提供しているセキュリティベンダーが顧客から収集しているケースが少なく情報を得る事は難しい。

他社の情報を得るために訓練担当者には通常の業務から1歩踏み込んだ対応が求められる。常日頃から同様の立場の他社の訓練担当者やセキュリティベンダー担当者と交流・意見交換をし、「開封率」「報告率」の情報交換ができる関係を築く事が必要となる。

6. 訓練の質向上に向けた取り組み

最後に標的型攻撃メール訓練を行う上で訓練担当者の工数・コストに見合った成果を出すために計画段階で検討すべき事を述べて本稿を終わりとしたい。

6.1　訓練目的を明確にする

訓練目的を明確にする必要がある。例えば、「不審なメールの見極め」を目的とする訓練と、「不審なメールが届いたときの社員の対応力を測る」ことを目的とする訓練とでは、使用するメールの文面や訓練の実施体制が異なる。

6.2　訓練の割り切り事項を見極める

4.2で前述した通り標的型攻撃メール訓練における課題の一つに、「意図しない周知によって結果の信頼度が損なわれること」がある。この課題解決は訓練の分割などで対応は可能であるが、予算や人的リソースといったコストとのトレードオフになるため、訓練担当は計画時に「どこまで割り切るか」を見極めておく必要がある。

6.3　関係部門との調整は十分に行う

規模の大きい組織において効果の高い訓練を行うには、関係部門を交えた準備が必要となる。特に報告率を求める訓練では、報告先の部門に負担がかかるため、事前の調整が必要である。また、訓練を受ける各部社員は通常の業務を行っているため繁忙期を見極めた上での実施が求められる。

6.4　メール文面は受け取り手の立場で作る

高い訓練成果を挙げるためには不審なメールと思わせず高い開封率を促すメール文面を作成し、信頼できる報告率を測定するために十分な開封者を確保する事が望ましい。そのため内容については被訓練者の心理に付け込んだ内容のメール文面を作る必要がある。特に「相手の立場で受け取る可能性のあるもの」「時期がある程度限定されているもの」は比較的開封率が高い結果となる事が多い。

JNSA ワーキンググループ紹介

インシデント被害調査ワーキンググループ

あいおいニッセイ同和損害保険株式会社
WGリーダー　神山　太朗

インシデント被害調査ワーキンググループ（以下「被害調査WG」）は、インシデントが発生した際の「被害額」を調査し、レポートとしてとりまとめることを目的に、2020年に発足したワーキンググループです。

当初の目的でもあったレポートは、2021年8月に「インシデント被害額調査レポート」というタイトルをもって公表させていただきました。

いくつかのメディアで取り上げられたほか、著名かつ複数の業界関係者の方にSNS等で取り上げていただいたことで、僭越ではありますが、ご存知の方も多いところではないかと思います。

本稿では、被害調査WGの発足の経緯、活動等をご紹介いたします。

インシデント被害額調査レポート

https://www.jnsa.org/result/incidentdamage/2021.html
検索サイトで「インシデント損害額」の語で調べていただければ幸いです！！！

発足の経緯

被害調査WGの発足は、JNSAの重鎮たるMさんと、「セキュリティ被害調査WG」のリーダーのOさんのお二人の課題認識に始まったと思います。

JNSAのWGの中でも「セキュリティ被害調査WG」（名前が似ていますけど別のWGです）は、多くのITベンダがそのレポートを引用するなど著名なWGでありますが、その調査対象は個人情報漏えい事案であり、さらには個人情報が漏えいした場合の損害賠償金の額を分析するといったものでありました。

この点、ランサムウェアの被害など、今日的な観点等からすれば、調査対象を個人情報漏えいに限るのではなく、インシデント全般、損害賠償金以外の被害額にまで、その調査対象を広げていくべきだというお考えがお二人にあったのではないかと思います（違ってたらごめんなさい！）。

そのような状況のもと、お二人のお声がけ（JNSAからのメール）もあり、都内某所に意を決した人達が、和気あいあいと集まったのがそもそもの始まりです。

小職が思っていたこと

小職は、あいおいニッセイ同和損保という損害保険会社で、サイバー保険の企画・開発・推進といった仕事をしています。

しかし、その販売に際しては、サイバーリスクを「他人事」「対岸の火事」と捉えている中小企業の経営者が多いことを実感していましたし、サイバー攻撃を身近な出来事として捉えて欲しい、セキュリティ対策をもっと取り組んで

欲しい、そんなことを思っていました。

さらにいうと、中小企業がサイバー攻撃を受け、場合によっては数千万円〜の損失が生じている現状をみるにつけ（サイバー保険には未加入…）、中小企業の経営者に現状を認識してもらうほか、ITベンダの方々にも、中小企業の経営者に対して、このような損失が生じる可能性をもっと伝えて欲しい…。とそんなことも思っていました。

そんな中、前述のお声がけをみた際に「これだ！」という思いのもと、参加させていただき、さらに僭越ながらリーダーを拝命した次第です。

といっても、ある種、ITベンダのみなさまの中で門外漢である損害保険会社の人間（技術的なことは詳しくはわからないw）ということもあって、キャノンITソリューションズでエバンジェリストを務めていらっしゃる西浦真一さんをサブリーダーとしてツートップ的に活動しているところです。

レポート公表まで

レポート作成にあたって活動の中心となったのは、インシデント発生時の各種支援・サービスを提供する事業者さんへのヒアリング、そしてインターネットでの調査です。

各メンバーで調査する領域を分け、メンバーごとに事業者さんへのヒアリング等を行いましたが、レポートの「あとがき」でも記したとおり、やはりコロナとの闘いという側面はなきにしもあらずでした。

というのも、メンバーのコネクション等から面識がある事業者さんもいる一方で、コネクションもなにもないためヒアリングを実施したくとも、それができない事業者さんもおり、その結果、満足のいく調査ができなかったという点もあったということです。やはり、Face to Faceでのお願い、ご挨拶ができなかったのは痛いところでしょうか…。

いずれにせよ、メンバーの頑張り、そして、業界の著名な方のお力添え（レポートの後ろのほうに、Special Thanksとしてクレジットさせていただいた方のほか、他にも多くの方にお力添えいただいています）もあり、レポートを完成させ、公表するに至りました。この場で感謝を申し上げたいと思います。

今後の活動について（メンバー募集！）

実はもっともっとやりたいことがあります。インシデント発生時の「被害額」を調査するという軸はずらすことなく、もっともっとこのレポートを充実化していきたいと思っています。2022年度版のリリースに向けて、追加メンバーも加えて鋭意検討中…というか作業中です（2022年2月現在）。

といったところで、お手伝いいただけるメンバーを募集中です！。特に、インシデントレスポンスのサービスをその顧客向けに提供されている方、または地方において中小企業を中心にUTMなどのセキュリティ商材の営業をされている方、要は現場の方がいると心強いところです（完全ウェブミーティングなので、お住まい・勤務地は関係ないです！）お気軽にJNSA事務局経由で、お声がけいただければ幸いです。

最後に、ランサムウェアの脅威然り、サイバー攻撃による被害は増加の一途を辿っています。被害調査WGの活動、インシデント発生時の「被害額」を伝えていくことは（これだけというものではないですが、）多くの企業・組織のセキュリティ対策を進める上での一助になるのではと思っています。今後とも被害調査WG（「インシデント損害額調査レポート」）をよろしくお願いいたします！

JNSA ワーキンググループ紹介

みんなの「サイバーセキュリティコミック」実行委員会

社会活動部会　みんなの「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（株式会社 日立システムズ）

はじめに

みんなの「サイバーセキュリティコミック」（以降、「みんコミ」）はJNSA会員の協賛で運営されています。

会員のみなさまのご理解ご協力ありがとうございます。2022年度シーズン3開催を計画中です。引き続きよろしくお願いいたします。

1.「みんコミ」開始の背景

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を向上させることが不可欠です。「みんコミ」は、コミックの情報伝達力とSNSの持つ情報の拡散力に注目し、次の目的で企画しました。
①セキュリティ知識の普及②ネットリテラシーの向上③ネットを守る（良い意味の）ハッカーへの注目とイメージアップ④セキュリティ人材育成の促進⑤JNSAにおいてSNSの積極的活用による普及啓発活動の量的測定

2.「みんコミ」実施要領

1）組織

社会活動部会内に実行委員会を設置。JNSA内の公募委員、各協賛企業の代表者、制作側の代表者、およびJNSA事務局によって構成、運営しました。

協賛企業： NTTデータ先端技術（株）、（株）クリエイティブジャパン、トレンドマイクロ（株）、
長崎県立大学、（株）日立システムズ、JNSA

（株）KADOKAWAに取り纏めを委託、併せて作家候補をご紹介いただき、次の2名に制作をお願いしました。

・原作作家　　大島悠先生：「ファイアーエムブレム」シリーズ（コンピュータゲーム）、
「ドラゴンクエストウォーク」アプリゲームのシナリオを手掛ける実力者。

・コミック作家　花園あずき先生：少女漫画的なイラストを多数手掛けられ、現在は「転生令嬢のブライダルプランは少々破天荒につき」を連載中。

実行委員会で協議した結果、SNSはTwitterを使うこととしました。

2）進行

春　　JNSAセキュリティ十大ニュースにより、「セキュリティで知りたいこと（お題）」を一般から募集。

初夏　投票結果を基に協賛企業にお題を分配。お題ごとに啓発内容とストーリー案を作成。
実行委員会案を原作作家に提示し、ブラッシュアップ。

夏　　ストーリーの確定とキャラクター案作成（原作作家と実行委員会で協働）。
主要キャラクターのビジュアル化と調整（コミック作家と実行委員会で協働）。

秋　　Twitterにて、8週に渡りコミックを配信。
毎週1話、コミック作家と実行委員会で調整後発信。
コミック発信の翌週、インプレッション（コミックが表示された回数）、エンゲージメント（”いいね”
”リツイート”等のアクションが行われた回数）等を（株）KADOKAWAが実行委員会へ報告。

冬　　実行委員会で配信結果を共有。

3）コミックのあらすじ

KOTB.LTD入社1年目の藤宮ユリル（ふじみやゆりる）の身の回りに起こるサイバーセキュリティ事件！

ユリルは、偶然知り合ったセキュリティ関連のネットライブ参加者（協賛各社のキャラクター）の力を借りながら事件を解決していきます。

3.「みんコミ」実施結果

シーズン1（2020/9/19 ～2020/11/6）

- ・インプレッション：5,708,708
- ・エンゲージメント：2,816,015（49.33%）
- ・いいね：6,194
- ・リツイート：453

シーズン2（2021/9/24 ～2021/11/12）

- ・インプレッション：5,599,758
- ・エンゲージメント：1,924,779（34.37%）
- ・いいね：2,687
- ・リツイート：346

コミックを広告と捉えると、類似ジャンルの同期間平均比211%((株)KADOKAWA実績を基に算出（Twitter広告の平均エンゲージメント率は約4%））であり、啓発・協賛企業の訴求に繋がったと考えられます。

シーズン1に対してシーズン2の絶対値の低下は、Twitter全般にコミック配信が増加したことによる影響があったと予想されます。特に今年は、画像1枚ずつ横にスワイプできるカルーセル形式でのコミックが流行ってきており、そちらの形式の方が”いいね”を押しやすくなっていると推測されます。

JNSA ワーキンググループ紹介

デジタルアイデンティティ WG

【執筆】SailPoint Technologies Japan 合同会社　佐藤　公理
【監修】日本電気株式会社　WG リーダー　宮川　晃一

はじめに

本 WG は「内部統制におけるアイデンティティ管理 WG」として 2005 年に発足しました。企業内の“アイデンティティ”、クラウドにおける“アイデンティティ”などのデジタルアイデンティティに関する課題を議論し、執筆活動・セミナー・勉強会・成果物の公開・出版を通して“デジタルアイデンティティ”の啓蒙活動・普及促進・市場活性化を実施してきており今年度で 16 年目を迎えました。この度、本年度の活動として 2021 年 11 月 26 日に実施したウェブセミナー「Enterprise Identity Day 再考！！エンタープライズ・アイデンティティ～ゼロトラストセキュリティの礎を確立する～」https://www.jnsa.org/seminar/2021/identity/index.html の開催報告を致します。

なぜ今 Enterprise Identity（企業におけるアイデンティティ）か？

本 WG は約 50 名が所属しており、月に 1 回の定例には常時 30 名程度が参加しています。2020 年度末の定例で、「**サイバーセキュリティ・ゼロトラストセキュリティにおいて、最も重要で基盤となるべきエンタープライズアイデンティティ（企業におけるアイデンティティ）への認知・理解が国内では不十分**であり、啓蒙活動をしたい」という意見がありました。

メンバーの共通認識として、コロナ禍におけるリモートワークの広がりやクラウド利用の拡大でゼロトラストセキュリティへの認知は高まっている、一方、本来ならゼロトラストセキュリティの基盤として検討すべきアイデンティティ管理がサイバーセキュリティの議論の中でしっかりと語られることが少ないとの課題感がありました。ディスカッションを進め、本 WG 立ち上げのきっかけでもある「内部統制」の時と同様、今こそ「セキュリティ」におけるアイデンティティ管理の認知を高め普及促進する活動が“再度”必要な時ではないかとの結論に至りました。“再度”と記載の通りアイデンティティ管理がセキュリティを検討する上で中心となるべきというのが本 WG メンバーの共通理解であり、過去にも出版物やセミナー等で認知・普及活動をしてきています。ただ、他のセキュリティソリューションに比べて最近は少しアピールが足りないのではないかということで“再度”活動を強化しようとなりました。ウェブセミナーのタイトルも「Enterprise Identity Day 再考！！エンタープライズ・アイデンティティ～ゼロトラストセキュリティの礎を確立する～」とし、今までもセキュリティの基礎であったアイデンティティ管理を“再度しっかりと考え直す必要がある”という意図を込めました。

開催レポート

11 月 26 日のウェブセミナーは事前登録 330 名、当日視聴 250 名と当初の目標を大幅に超え、**ゼロトラストセキュリティやアイデンティティ管理への関心が高い**ことが実感できました。アンケートにも 100 名以上に回答頂きました。全体・すべてのセッションで「やや満足」「満足」が 80％以上となり、視聴者の皆様の期待に応えることができたと思います。

基調講演はセミナーの対象である「企業内で実際にアイデンティティ管理やアイデンティティガバナンスを推進していく方」と同じ立場で活動されている au カブコム証券の石川様と NTT の駒沢様にお願いしました。石川様には、「高度にアイデンティティ情報を管理していくことがゼロトラストにおいては大事で、その上でどのように実践してきたか」を具体的にお話し頂きました。ゼロトラストはコンセプト・考え方であり、様々なソリューションを組み合わせる必要があるとはよく言われますが、具体的な方法が話されることはあまりありません。実際にアイデンティティ情報をどの

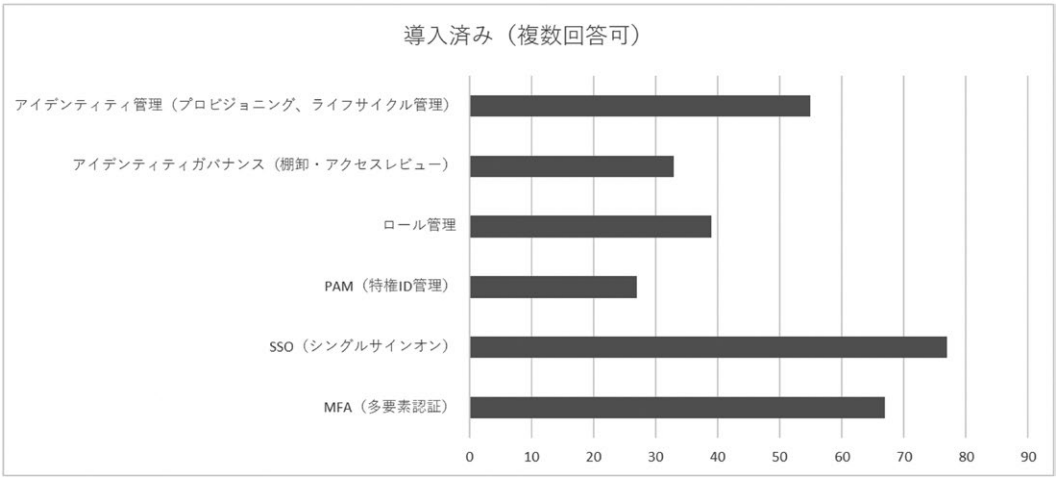
ように活かしてセキュリティを強化しているかを聞ける機会は非常に貴重でした。駒沢様の基調講演では、「経営から見たアイデンティティの位置づけ」として難しい技術の話ではなく、ワークスタイル・ゼロトラスト・DX・エンタープライズアーキテクチャの視点で企業におけるデジタルアイデンティティの大切さを整理・解説頂きました。

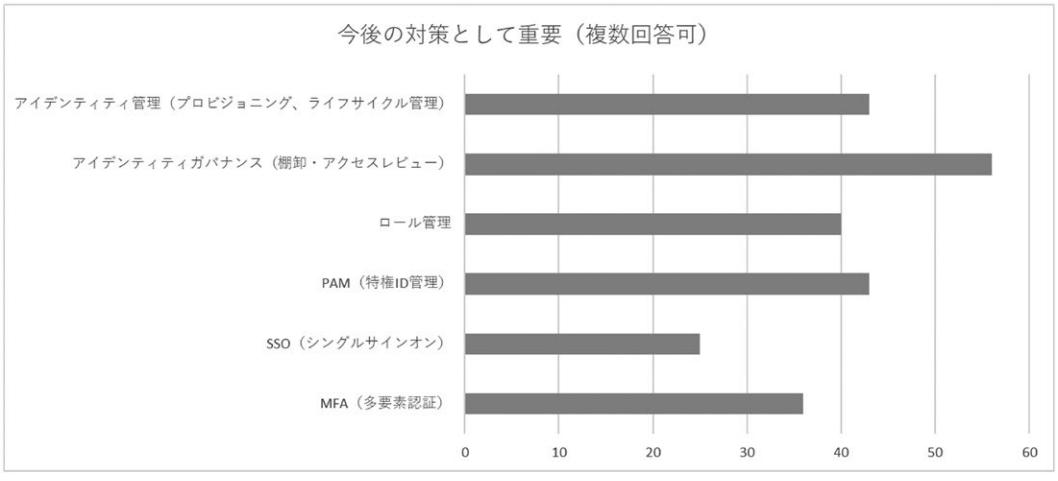
「課題発掘セッション」では、「IDaaSを導入しよう」の裏に隠れて見逃しがちなアイデンティティ管理の考える必要がある様々な要素を紹介しました。「アイデンティティは難しい」と言い切った気持ち良いセッションでした。「再発見セッション」では、具体的な検討を行う上で参考になる本WGの成果物を紹介し、アイデンティティ管理・ロール管理・特権ID管理の3軸で、ゼロトラストが求める最小権限の原則を維持していくために、これまでのシステムをどのように変革していくべきかを紹介しました。

最後のパネルディスカッションでは普段のWGでの議論そのままに意見交換が行われました。ロール管理やアクセスコントロールを真剣に実施していくべきであり、そのためにWGメンバーとしても様々な場所で共感を持ってもらえるように話をしていこうということでした。

最後に100名の方に回答頂いたアンケートの結果をご紹介します。

図：アイデンティティ管理対策の導入状況・導入意向に関するアンケート集計結果（n=104）





JNSA ワーキンググループ紹介

アイデンティティ管理で「導入済みのもの」と「今後重要なもの」を聞きました。SaaS利用の拡大や最近のID・パスワード漏洩による事件などもあり、SSO（シングルサインオン）、MFA（多要素認証）は多くが導入済みであることがわかります。一方、アイデンティティ管理、アイデンティティガバナンス、ロール管理、PAM（特権ID管理）は今後重要との回答が多いことがわかります。

今回のウェブセミナーでもアイデンティティ管理、アイデンティティガバナンス、ロール管理、PAM（特権ID管理）を重点的に取り上げており、視聴者の方へ今必要な情報を提供できたと考えています。

これまでの成果物、メンバーの紹介、今後

本WGではこれまでの成果物・メンバー紹介をWGのページに記載しています。またウェブセミナーの講演資料も公開しておりますのであわせて参照ください。ご意見・ご質問などあれば是非お寄せください。今後の活動の参考とさせて頂きます。

- デジタルアイデンティティWG | NPO日本ネットワークセキュリティ協会
  https://www.jnsa.org/active/std_idm.html
- Enterprise Identity Day再考！！エンタープライズ・アイデンティティ～ゼロトラストセキュリティの礎を確立する～
  https://www.jnsa.org/seminar/2021/identity/index.html
- JNSAお問い合わせフォーム
  https://www.jnsa.org/aboutus/quote.html

来年度もWGメンバー間でのディスカッション等を実施すると共に、積極的な普及促進・啓蒙活動も実施していきますのでご期待ください。WGへの参加も大歓迎です。

会員企業ご紹介51

大阪商工会議所

大阪商工会議所は明治11年に五代友厚が設立した非営利の地域経済総合団体。中小企業支援や地域振興を目的に様々な事業やサービスを展開。最近は中小企業のサイバー攻撃対策を支援する様々な事業に注力しています。
その一つとして「商工会議所サイバーセキュリティお助け隊サービス」を提供（大阪商工会議所自体がサービス提供主体）。お金、人材、時間などの面で余裕のない中小企業に特化した格安・簡便なサイバーサキュリティ対策のパッケージサービスです。

サイバーセキュリティ CSお助け隊

◎ UTM（サイバー攻撃多機能防御装置）のレンタルによる①サイバー攻撃・情報流出からの「お守り」（外→内、内→外）、②24時間365日遠隔監視の「見守り」（NEC）、③攻撃時のアラートメールによる「お知らせ」（NEC）、④ご不安時の「相談」（キューアンドエー㈱）、⑤サイバーインシデント発生時の「駆け付け」（大阪商工会議所もしくは再販事業者またはその両者が契約するお助け実働隊地域IT事業者約20社）、⑥駆け付けの費用を補償する「サイバー保険」（東京海上日動火災保険㈱）などをパッケージし、全国いずれかの商工会議所・商工会の会員は月額6,600円（年79,200円）、非会員でも月額8,250円（年99,000円）と格安。
◎ 買い取りではないので初期費用ゼロ。意味不明なオプション料金は一切なし。契約期間も１年（更新可）と柔軟。クーリングオフ期間もあるので障害リスクも最小限！
◎ UTMはブリッジモードなので、情報システム担当者のいない中小企業でも自力設置できるほど「導入」カンタンで、最新化も自動（遠隔）で行われるので「運用」もラクラク。しかも国産なので安心かつ丈夫。弁当箱サイズの小型なので空間要らず。良くも悪くも「置きっぱなし」でＯＫ。
◎「商工会議所サイバーセキュリティお助け隊サービス」は、経済産業省・独立行政法人情報処理推進機構の「サイバーセキュリティお助け隊サービス」登録（サービス登録番号：2020-001）。ユーザは「中小企業として必要最低限のサイバーセキュリティをやっています！」と対外的にアピール可能。

提供エリアは下記のとおり。

【近畿（２府５県）および近畿に本社を置く企業の東京・福岡・名古屋の都市部の支店・工場等】
大阪商工会議所（直接提供）
https://www.osaka.cci.or.jp/cybersecurity/utm/
ＧＲＯＷＩＴ㈱（大阪商工会議所契約再販事業者）
https://www.growit.jp/scsotasuke.html
【首都圏】
㈱エッジプランニング（大阪商工会議所契約再販事業者）
https://www.edge-planning.co.jp/service/otasuketai
【千葉県】
佐倉商工会議所（大阪商工会議所契約再販事業者）
https://www.sakura-cci.or.jp/expand/cybersecurity/
【長野県】
松本商工会議所（大阪商工会議所契約再販事業者）
https://isp.matsumoto.ne.jp/service/otasuketai

※大阪商工会議所が直接提供するサービスと再販事業者が提供するサービスは原則として同じもの。価格は一部の再販事業者で上記と異なる場合ありますが、それでも月額１万円以内。

※左記以外のエリアも、広島、新潟、静岡、九州ほかで近日中に提供開始予定

お問い合せ	大阪商工会議所　経営情報センター 〒540-0029 大阪市中央区本町橋2-8　TEL：050-7105-6004 Eメール：cybersecurity@osaka.cci.or.jp　ネット検索：商工会議所　お助け隊

テナブルネットワークセキュリティジャパン株式会社

https://jp.tenable.com/

テナブルが解決する課題～サイバー脅威に晒されたIT資産の迅速な可視化

デジタルトランスフォーメーション（DX）により、IT資産（およびOT資産）が爆発的に拡大した今日、オンプレミス、クラウドにかかわらず、複雑なコンピューティング環境そのものが、現代のサイバー脅威にさらされています。しかし、企業は資産の調査、脆弱点の検出、修正に向けた問題の優先順位付け、リスクの測定、競合他社との比較における、あらゆる段階で困難に直面し、サイバーリスクの確実な管理や緩和ができない状態にあります。DX時代には、新しいアプローチが必要です。

Tenableは、サイバーエクスポージャー ソリューションのベンダです。グローバル3万社を超える企業にサービスを提供し、DX時代における サイバーセキュリティのリスクの管理と測定を支援しています。Tenableは、脆弱性の評価と管理のパイオニアとして、深い専門知識を基礎に、現代のアタックサーフェス全体に対する広い可視性と対策の方向性を提供し、セキュリティチーム、経営幹部、取締役会が、サイバー危機の兆候や可能性を、的確に優先順位付けして測定できるように支援しています。

主な製品群

Tenable.ep

Tenable.ep は、包括的なリスクベースの脆弱性管理ソリューションです。アタックサーフェス全体の資産と脆弱性が可視化でき、近い将来悪用される可能性の高い脆弱性を予測し、最も重要なことに焦点をあてて行動することができます。

Tenable.ad

侵害のニュースの背後には、必ずと言ってよいほどセキュリティが不備な Active Directory が存在します。Active Directoryは、既知の欠陥や不適切な構成を利用して権限を昇格させて水平移動する攻撃者の格好の標的となっています。Tenable.adを使えば、攻撃が起きる前にActive Directoryの弱点を発見して修正することができます。

Tenable.ot

Tenable.otは、産業インフラストラクチャ全体に存在するすべての資産に対する深い状況認識を提供します。リアルタイムの状況を把握できるばかりでなく、履歴や監査レポートをいつでも出力できるので、セキュリティとコンプライアンス規制に先行的に準拠することができます。

お問い合せ	テナブルネットワークセキュリティジャパン株式会社 住　所：〒100-0005 東京都千代田区丸の内1-6-5 丸の内北口ビル10F メール：info-j@tenable.com

株式会社ブロードバンドセキュリティ

https://www.bbsec.co.jp/

お客様の情報資産を守り、成長を支援するために

株式会社ブロードバンドセキュリティ（BBSec）は、悪意ある攻撃から組織の情報資産を守り、組織がその情報資産をもとに適正に成長していくことを支援するセキュリティ専門事業者です。対策に欠かせないIT / 組織両視点からの各種サービスは、お客様の規模や対策の推進状況にかかわらず、今必要とする最適な「答え」を提供します。

セキュリティ監査・コンサルティング

お客様システムの可視化/課題抽出/課題解決を目的とした、組織全体に対するセキュリティ支援サービス。IT・組織両面からセキュリティの盲点を発見し、実現可能な解決策を提示いたします。
また、オンラインビジネス成功に向けた調査サービスを中心に、具体的なデザイン改善・システム開発、効率的なサイト運営をサポートします。

脆弱性診断

お客様システムに潜む脆弱性を検証し、改善案を提示するサービス。時々刻々と変化する外部環境に対応していくために、新規開発時だけでなく、運用中のシステムにも定期的に実施することを推奨しています。

情報漏えいIT対策

慎重かつ堅実な継続的作業を求められるセキュリティ運用を、セキュリティのプロフェッショナルが24時間・365日体制で支援いたします。

BBSecのサービスMAP

便利で安全なネットワーク社会を創造する

お問い合せ	株式会社ブロードバンドセキュリティ 〒160-0023 東京都新宿区西新宿8-5-1 野村不動産西新宿共同ビル4F Webサイト　https://www.bbsec.co.jp/

SailPoint テクノロジーズジャパン合同会社

https://www.sailpoint.com/ja/

16年以上の豊富な経験と導入実績をもつアイデンティティ業界のリーダー

SailPointは、IDaaSを超えるアイデンティティ・ガバナンス管理（IGA：Identity Governance and Administration）サービスプロバイダーのリーダーとして、企業のデジタルガバナンスを強化します。AIや機械学習を活用して、企業にあるすべてのアイデンティティ（ID）を一元的に可視化し、ID管理業務を自動化するクラウド型ソリューションを提供しています。SailPointは、アイデンティティ管理を専門とした16年以上の経験と、グローバルで政府機関や金融機関を含む大手企業を中心とした2,000社以上の導入実績があり、ユーザー継続率は95%以上を維持しています*。また、ガートナー社のマジッククアドラントレポートIGA部門6年連続リーダー評価、同社Peer Insights Customers' Choice IGA部門受賞、フォレスター社Waveレポートでのリーダー評価など、世界のアナリストからも高い評価を受けています。

* 2022年2月時点

SailPointアイデンティティ・ガバナンス管理"IdentityNow" 製品の特長

IDを一元的に可視化し、すべてのアクセス権限を常にモニタリング

ロケーションやグループ・関連会社を問わず、全社員が利用するオンプレミス/クラウド上のすべてのアプリケーションのアカウント情報とアクセス権を一元的に可視化し、権限状況を瞬時に把握して常にモニタリングします。

すべての手動プロセスや手作業をなくし、業務スピードを向上

従来の紙やExcelベースでの台帳管理や棚卸、様々なID管理システムからの手動でのデータ収集から解放され、マニュアル作業をなくすことで人為的ミスや業務負荷を軽減し、業務スピードを向上します。

ポリシー管理エンジンとワークフローの自動化で、ライフサイクルを適切に管理

すべてのIDを、役割や権限に基づきポリシーに沿ってワークフローを自動化します。入社、異動、退職までのライフサイクル（ユーザーの属性変更）を自動化することで適切に管理ができるようになり、業務負担を大幅に軽減します。

AIや機械学習等の最新技術を活用し、セキュリティを強化

AIを利用したピア分析機能では、似た役割の人がもつアクセス権や権限レベル情報をもとに推奨情報が表示され、棚卸作業時および権限リクエスト承認時に素早く判断でき、最先端の技術による可視化、検出、修正機能の強化でセキュリティリスクを低減します。

SailPointが選ばれる理由

- ☞ 16年以上の豊富な知識と経験をもつIGAのスペシャリスト
- ☞ 第三者機関からの高い評価
- ☞ ユーザーのニーズを意識した使い勝手の良いUI
- ☞ 機械学習、AI、ボット等の新技術の採用
- ☞ 大手・有名企業からの多くの採用実績
- ☞ 利便性とセキュリティの両立を実現
- ☞ クラウド/オンプレミス型問わず企業内アプリケーションのIDを一元管理
- ☞ 複数の既存アプリケーションの複雑な利用方法にも対応

お問い合せ	SailPointテクノロジーズジャパン合同会社 〒150-6139 東京都渋谷区渋谷2-24-12 渋谷スクランブルスクエア 39F Eメール: japan_sales@sailpoint.com（営業本部） ウェブサイト：https://www.sailpoint.com/ja/

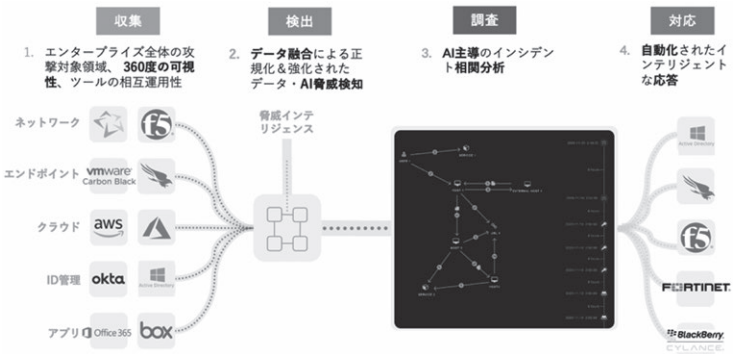
Stellar Cyber（ステラサイバー）

https://jp.stellarcyber.ai/

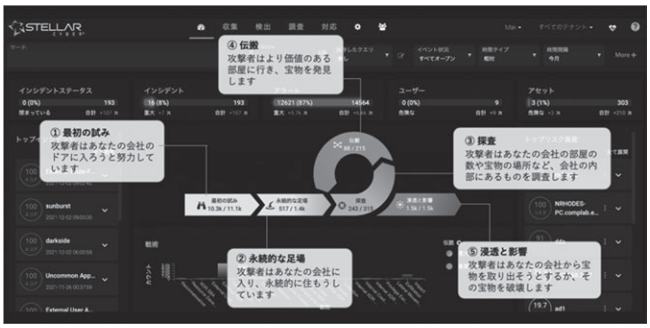
世界初Open XDR プラットフォームのイノベーター Stellar Cyber

Stellar Cyber(ステラサイバー)は、2015年米国シリコンバレーで創立されて以来、今日までOpen XDRの世界的リーダーとして業界を推進してまいりました。世界中の企業SOCおよびMSP•MSSP会社から高い信頼を得ております。
Open XDRは、全ての検出と応答です。オープン(Open) で統一された、相関性のあるインテリジェントなセキュリティ運用プラットフォームを通じて、企業の攻撃対象領域全体を効果的かつ効率的に保護します。

Stellar Cyberは、AI主導でリアルタイムでサイバー攻撃の「脅威検知～脅威対処」を行います。レガシーな従来ツールは、EDR（エンドポイントデータ）、NDR（トラフィックデータ）、SIEM（ログデータ）などを個別に収集し分析していましたが、Stellar Cyberは全てのデータを1つに融合しAI主導でリアルタイムで相関分析を行います。その結果、精度の高い相関分析が可能になり、脅威を素早く検出し、脅威に対して直ぐに対応することができます。
Stellar Cyberは、 4つのステージ「①収集 ②検出 ③調査 ④対応」を自動化します。ログ収集～脅威検知～相関分析～応答までをAI主導で自動的に行います。従来、手動で行っていた作業をAIが実施することで、パフォーマンスの向上および運用コストを削減します。平均検出時間(MTTD)で8倍、平均復旧時間(MTTR)で20倍の改善を実現します。



Stellar Cyberのサイバーキルチェーンは5つのステージ（①最初の試み ②永続的な足場 ③ 探査 ④伝搬 ⑤浸透と影響）から構成されております。AIが脅威を分析し自動的に各ステージに分類します。セキュリティアナリストは、サイバー攻撃がどの段階にあるのか素早く把握することができます。



Stellar Cyber Open XDRプラットフォームが、あなたの会社をサイバー攻撃から守ります！ 先ずは、お気軽にお問い合わせください。

お問い合せ	Stellar Cyber（ステラサイバー） 問い合わせフォーム: https://jp.stellarcyber.ai/company/contact-us/ Open XDRなら Stellar Cyber

パロアルトネットワークス株式会社
https://www.paloaltonetworks.jp/

パロアルトネットワークス ― サイバーセキュリティの選ばれしパートナー

パロアルトネットワークスは、ネットワーク、クラウド、エンドポイント、セキュリティ運用と、企業・組織のインフラに必要なセキュリティを包括的に提供するサイバーセキュリティのリーディングカンパニーです。マーケットアナリストから高い評価を受けるパロアルトネットワークスのソリューションは、Fortune100の95社、Forbesグローバル2000の71%をはじめ、国内外の数多くの企業・組織の皆様にご活用いただいています。パロアルトネットワークスは、高度化、深刻化し続けるサイバーセキュリティの問題を解決するための選ばれしパートナーとして信頼していただいております。

セキュリティ投資・運用に変革をもたらすセキュリティプラットフォーム

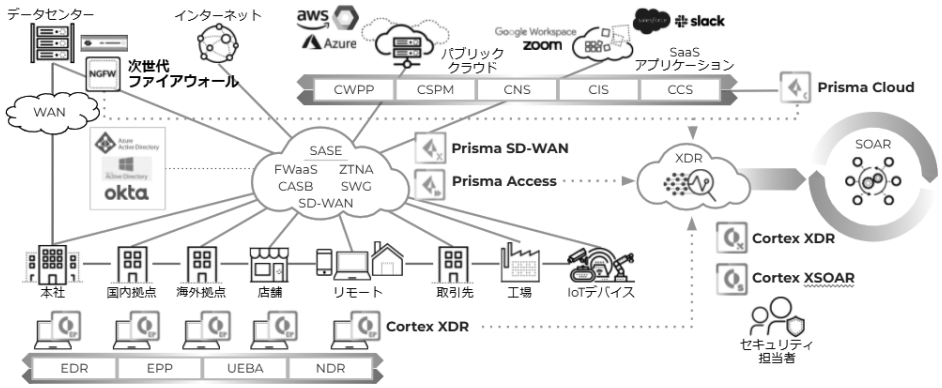
パロアルトネットワークスでは、ネットワーク、クラウド、エンドポイント、セキュリティ運用の各領域で必要となるセキュリティファンクションを統合し、インフラ全体からデータを統合してより優れたセキュリティを実現するセキュリティプラットフォームを製品戦略の柱に据えています。

企業・組織のITインフラとサイバーセキュリティは構造的な問題を抱え、変革が求められるビジネスの足枷となっています。パロアルトネットワークスのセキュリティプラットフォームは、インフラ・サイバーセキュリティ投資・運用に関わる様々な課題を解決し、これからのビジネスをイネーブルするインフラの実現をご支援します。

インフラ全体でのゼロトラストの実現、SASEによるインフラ刷新やテレワーク対応、クラウドワークロードの保護、セキュリティ運用の効率化・高度化に至るまで、サイバーセキュリティのあらゆる課題を解決できます。

- 複雑かつレガシーなITインフラをクラウドに統合することにより、これから一層デジタル化するビジネスのニーズを満たす利便性、拡張性、安全性を兼ね備えたものに変革
- サイロ化から統合されたプラットフォームに変えることにより、セキュリティ投資・運用のCAPEXとOPEXを最適化
- 人材不足やスキル不足、反復的業務に時間が割かれるセキュリティ運用の構造的な問題を自動化・自律化に変えることにより、運用負荷やインシデント対応に要する時間を徹底的に削減

包括的なセキュリティプラットフォームで皆様をご支援します



お問い合せ	パロアルトネットワークス株式会社 〒100-0011 東京都千代田区内幸町 2-1-6 日比谷パークフロント 15F TEL : 03-6205-8061　　WEB : https://www.paloaltonetworks.jp/ EMAIL : infojapan@paloaltonetworks.com

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

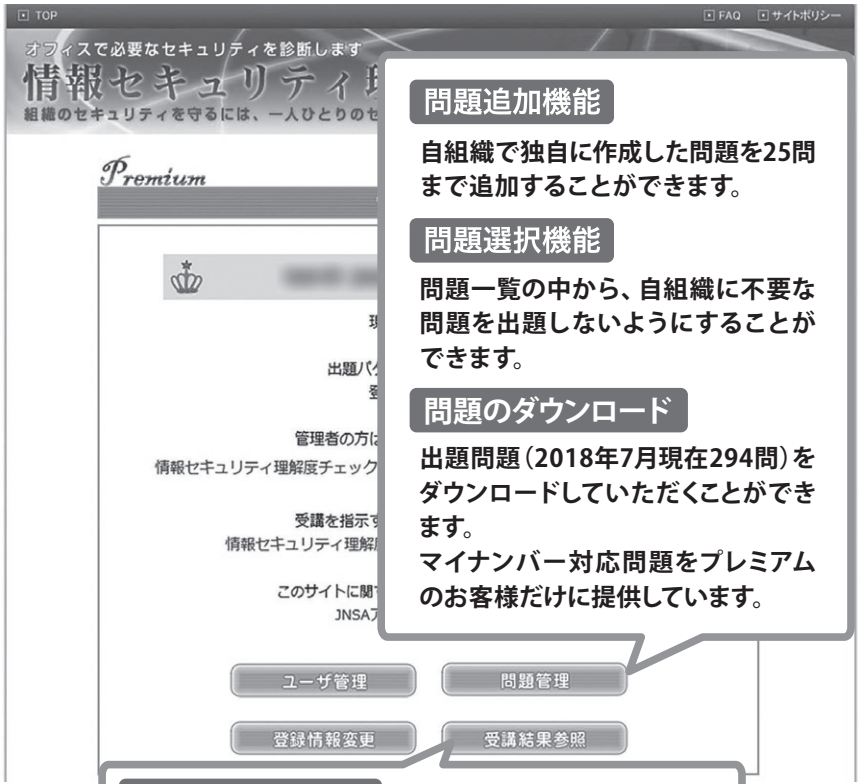
「情報セキュリティ理解度チェック・プレミアム」は、無償版「理解度チェックサイト」を、組織ごとにカスタマイズできる機能がついた有償サービスです。管理者機能をより強化し、独自の問題の追加も可能です。ぜひ社内教育や情報セキュリティ関連の補助ツールとしてご活用下さい。

＜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 会員企業のサービス・製品・イベント情報

■製品紹介■

Stellar Cyberは、Open XDRの世界的リーダーでAI主導の次世代サイバー攻撃対策プラットフォームです。世界中の企業SOCおよびMSP・MSSP会社から高い信頼を得ております。オープン(Open) で統一された、相関性のあるインテリジェントなセキュリティ運用プラットフォームを通じて、攻撃対象領域全体を効果的かつ効率的に保護します。AI主導で「脅威検知～脅威対処」を自動化、あなたの会社をサイバー攻撃から守ります。SOCの生産性を大幅に改善します。
【製品情報詳細】
https://jp.stellarcyber.ai/
◆お問い合わせ先◆
ステラサイバー
https://jp.stellarcyber.ai/company/contact-us/

■製品紹介■

○専門知識不要ではじめる統合ログ管理
【ALog EVA】
ALog EVAは、オンプレ/クラウド問わず、多様な情報システムのログを包括的に記録管理する製品です。
AIリスクスコアリング機能など、専門知識やノウハウなしでも高度なログ活用を実現する機能を、多数搭載しているのが特徴です。
内部不正対策やサイバー攻撃対策、障害原因の追究、ワークスタイル変革など、あらゆるビジネスの課題を解決することができます。
【製品情報詳細】
https://www.amiya.co.jp/solutions/alog_eva/
◆お問い合わせ先◆
株式会社網屋　データセキュリティ事業部
E-Mail: bv-sales@amiya.co.jp

■製品紹介■

○FFRI yarai
FFRI yaraiは、パターンファイルに依存しない「先読み防御」技術を徹底的に追及したエンドポイントセキュリティです。
標的型攻撃のトリガーとなる未知の脆弱性攻撃や、未知のマルウェア攻撃からシステムを保護します。
また潜伏した脅威を調査・検出するEDR機能を追加料金なしでご利用いただけます。
エンドポイントセキュリティFFRI yaraiに関するウェビナー、ホワイトペーパー、事例をリソースセンターに掲載しています。
【製品情報詳細】
ＦＦＲＩセキュリティリソースセンター
https://www.ffri.jp/resources/index.htm
◆お問い合わせ先◆
株式会社ＦＦＲＩセキュリティ
https://www.ffri.jp/contact/index.htm

■製品紹介■

Ｗｅｂアプリの開発現場にフィットする簡単手軽なクラウド型セキュリティテスティングツール。脆弱性検査を開発チーム内で実施できるようにし、頻度の高いリリースサイクルでもセキュリティを担保した状態を維持できるようになります。
開発プロセスの早い段階で重要度の高い脆弱性を発見し、修正までをトータルサポート。初めてセキュリティに取り組む企業や、スピードとセキュリティの両立を目指す開発現場におすすめ。
【製品情報詳細】
https://www.ubsecure.jp/komabato
◆お問い合わせ先◆
株式会社ユービーセキュア
E-Mail: sales@ubsecure.jp

■製品紹介■

○ (ISC)² CCSP Ultimaite Guide
(ISC)²が提供するCCSPは、クラウドサービスを安全に利用するために必要な知識を体系化した資格であり、情報セキュリティ業界におけるキャリアアップを目指す方に最適の資格です。 (ISC)²が発行するCCSP Ultimate Guideは、クラウドセキュリティ資格について知っておくべきすべてのアイテムを網羅しており、資格取得を検討している方に必携の資料です。
【製品情報詳細】
https://www.isc2.org/certifications/ultimate-guides/ccsp/jp
◆お問い合わせ先◆
(ISC)²
E-Mail: infoisc2-j@isc2.org

「JNSA 全国サイバーセキュリティセミナー」を開催

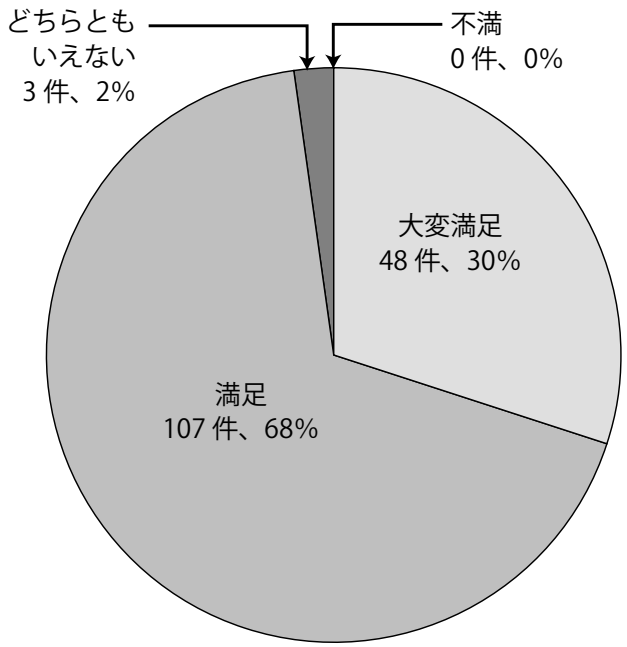
マーケティング部会では「JNSA 全国サイバーセキュリティセミナー 2021」を、2021年11月17日（水）に開催いたしました。2021年で5回目となる本セミナーですが、昨今の社会情勢を踏まえ、オンライン配信となりました。
ビジネスのデジタル化が進むなか、企業や組織を取り巻くサイバーセキュリティの環境は目まぐるしく変化しています。新型コロナウイルスによる混乱等に乗じた新たな脅威も発生し、ビジネスに致命的な影響を及ぼすリスクも増加しています。

本セミナーでは主に中小企業を対象に、サイバーセキュリティの脅威対策を行う上で有益である情報を提供することを目的として開催しました。

総数265名と多くの方にご参加いただき、好評のうちに終了いたしました。

サイバーセキュリティ対策を行う上で有益である国の情報セキュリティ政策や、JNSAが提供する無償でも利用できるツールや情報を具体的に紹介し、実際の経営、業務役立てることができる情報の提供に努めています。

ご参加いただいたほぼすべての方より、満足であったとのご感想をいただいております。



セミナー全体の感想

国内企業の皆様へ有効性ある情報、サービスの提供と続けるとともに、日本全体でのセキュリティレベルの向上に寄与できるよう努めてまいります。

事務局お知らせ
JNSA ANNOUNCE

後援・協賛・協力イベントのお知らせ

1. Black Hat Asia 2022
主　催：一般社団法人日本経営協会
日　程：2022年5月10日～13日
会　場：マリーナベイサンズ（シンガポール）＋
バーチャル

2. 自治体総合フェア2022
主　催：一般社団法人日本経営協会
日　程：2022年5月18日～20日
会　場：東京ビッグサイト西３ ホール

3. ワイヤレスジャパン2022
主　催：株式会社リックテレコム
日　程：2022年5月25日～27日
会　場：東京ビッグサイト 西3・4ホール

4. CSA Japan Summit 2022
主　催：一般社団法人 日本クラウドセキュリティ
アライアンス
日　程：2022年5月26日～28日
会　場：オンライン

5. 第26回サイバー犯罪に関する白浜シンポジウム
主　催：サイバー犯罪に関する白浜シンポジウム
実行委員会
日　程：2022年5月26日～28日
会　場：メイン会場：和歌山県立情報交流センター
サ ブ会 場 ：ホテルシーモア

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

【みんなの「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／Modis株式会社）

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、公開する。

- 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ともに、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　2022 年 2 月 1 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　（Musarubra Japan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）
後藤　　忍　（セコムトラストシステムズ株式会社）
輿水　直貴　（キヤノンマーケティングジャパン株式会社）
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
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　2022年2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（株）
Avast Software Japan（同）
アビームコンサルティング（株）
（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）
アンテナハウス（株）　New
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）
（株）イエラエセキュリティ
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
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
（株）エーアイセキュリティラボ　New
AOSデータ（株）
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）
NTTビジネスソリューションズ（株）
（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
兼松エレクトロニクス（株）　New
（株）カンム
キヤノンITソリューションズ（株）
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
(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)
GMOグローバルサイン・ホールディングス(株) New
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)
シナック New
(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
ステラサイバー New
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)
(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)
(株)宝情報
タレスDISジャパン(株)
(株)ChillStack New
(株) 中電シーティーアイ
中部テレコミュニケーション(株) New
都築電気(株)
TIS(株)
(株)ディアイティ
テクマトリックス(株) New
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)
Tenable Network Security Japan(株) New
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
東京海上ディーアール(株)
(株)東芝
東芝ITサービス(株) New
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)
(株)TRUSTDOCK New
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
(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)パイオリンク
(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)
東日本電信電話(株) New
(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)
(株)ファインデックス
(株)フーバーブレイン
フォーティネットジャパン(同)
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】
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
Musarubra Japan(株)
Modis(株)

【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)
(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
(株)LainZ New
(株)レオンテクノロジー
(有)ロボック

【わ】
(株)ワイズ

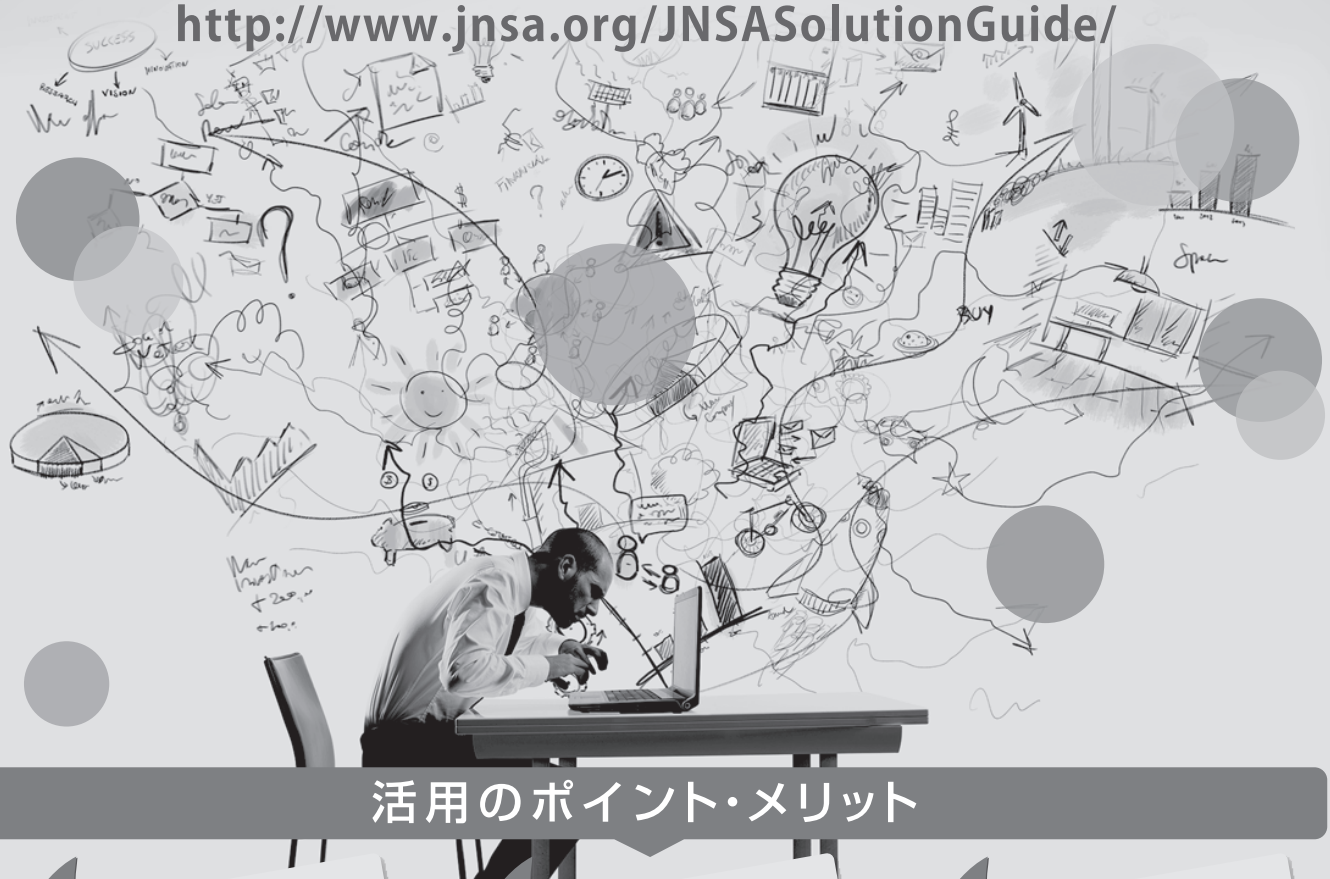
【特別会員】
一般社団法人 IIOT
$(ISC)^2$ Japan
大阪商工会議所
一般財団法人 沖縄ITイノベーション戦略センター
ジャパン データ ストレージ フォーラム
一般社団法人重要生活機器連携セキュリティ協議会
国立研究開発法人情報通信研究機構
一般社団法人セキュアIoTプラットフォーム協議会
データベース・セキュリティ・コンソーシアム
一般社団法人 ソフトウェア協会
特定非営利活動法人デジタル・フォレンジック研究会
電子商取引安全技術研究組合
東京大学大学院 工学系研究科
トラストサービス推進フォーラム
長崎県立大学情報システム学部情報セキュリティ学科
一般社団法人 日本インタ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
一般財団法人 日本サイバーセキュリティ人材キャリア支援協会 New
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2社

セキュリティにまつわる課題解決を支援します

JNSAソリューションガイド

http://www.jnsa.org/JNSASolutionGuide/



活用のポイント・メリット

ガイドラインなどに
対応する製品・サービス
を検索できる!

十大脅威等最新の
脅威から検索できる!

利用シーンから
対策を検索できる!

JNSAソリューションガイドサイトは、JNSAの会員企業が取り扱うネットワークセキュリティに関する製品やサービス、イベント情報などをご紹介しているサイトです。さまざまな角度から検索できるような仕組みになっていますので、セキュリティ製品やサービスの導入をご検討される際にはぜひご活用下さい。

JNSA

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。）

あいおいニッセイ同和損害保険株式会社　神山　太朗

JNSA会員の皆様、はじめまして！
そして、同じ号で二度目の登場（インシデント被害調査WGの紹介）ですみません！
あいおいニッセイ同和損害保険株式会社　サイバー保険室の神山と申します。
事務局からのご用命により自己紹介の機会をいただきました。よろしくお願い致します。

■経歴等

小職、損害保険会社の商品開発部門に20数年在籍しており、保険約款の作成、保険料（料金）の設計、監督官庁との折衝、募集ツールの作成といった仕事をしています。ここ数年は、サイバー保険に特化しての企画・開発・推進といった仕事をしています。

IT業界との関わりは、これまた20数年前…。Windows95の時代です。その当時は、今とは別の保険会社にいたのですが、とあるセキュリティベンダさんからのオーダーで、その提供するサービスの顧客向けに、ネットワークの管理に起因して損害賠償責任を負った場合の保険（現在のサイバー保険の原型ともいえる商品）を設計したことが思い出されます。

今となっては、このような手法（サービスに保険をバンドルすること。我々の業界では「商品付帯契約」と呼んでいます）に取り組むことは、一般的といえますが、実は、意外と昔からあったということになります。

その後、2005年の個人情報保護法の施行に伴って情報漏えい保険を設計をしたり、2014年にサイバーセキュリティ経営ガイドラインの策定に立ち会ったり（保険会社社員としてオブザーバー的に端っこに座っていただけですけど）、2015年にサイバー保険（当社商品名は「サイバーセキュリティ保険」）を設計したりと、IT関連の保険にずーーーっと携わって今に至るところです。

なお、インシデント被害調査WGの紹介でも書きましたが、IT業界にいたわけではないので技術的なことは詳しくはわかっていない人間でもあります（Twitterでの著名な方のツイートであったり、たまねぎ系リークサイトを定期的に眺めたりと、情報収集はしていますが…）

■JNSAとの出会い

当社は、2015年にサイバーセキュリティ保険を販売し始めたのですが、セキュリティ業界との接点をもっと深めていかねばと考えていたところ、JNSAのとあるWGからサイバー保険を教えて欲しいとお声がけいただいたのが、JNSAとの出会いになります。

その後、損害保険会社（本体）として唯一の会員になり、今に至るところです。

■最近の関心事

とにもかくにもランサムウェアです。

欧米の保険業界はランサムウェア被害によって収支が悪化しており（特に事業中断による損失の支払い）、 保険料（料金）の値上げ、引受の制限（お支払いの限度額の引き下げ等）を図っています。日本においてもこのような状況にならないかを常に注視していく必要があると思っています。

なお、保険業界はランサムウェアのエコシステムの一端を担っているというハナシがあります。というのも欧米の保険会社ではサイバー保険において身代金も補償対象にしていたりするからです（日本の保険会社のサイバー保険では身代金は補償対象外です！）。現に、とあるメディアのインタビューにおいてランサムウェアの犯罪グループとして有名なREvilのメンバーが「保険会社の顧客データを狙っている」として、身代金を払ってくれるであろう企業をターゲットにしていることを語っています。

「日本の保険会社のサイバー保険は身代金は補償対象外！」ということを発信していくことが必要なんだろうと個人的には思っているところです。

■最後に

サイバー保険というのはサイバーレリジエンス、復旧・再発防止のための一助といえます。フォレンジック調査ほかインシデント発生後の対応（事後対応）をコスト面から支えるということです。

今後、サイバー攻撃の脅威がさらに増していくなかで、セキュリティ業界の方々とともに企業・組織のセキュリティ対策の向上のお手伝いができればと思っています。ご指導・ご鞭撻のほど、よろしくお願いいたします。

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。）

富士通株式会社　峯浦　梨紗

JNSA会員の皆様、はじめまして。富士通の峯浦と申します。この度、西日本支部長の元持様よりご紹介いただきました。この場をお借りして自己紹介をさせていただきます。

私は入社以来、ネットワークやＩＰ電話などのコミュニケーションシステムの構築作業やプロジェクト管理を中心に業務を行ってきました。7年ほど前からセキュリティに関するプロジェクトに参画するようになり、主にお客様の情報システム部門の方々に対して、セキュリティ対策の現状評価から対策立案の策定までの支援を行う業務に携わっています。また、社内での業務ではありますが、ISMS認証取得・継続のための監査対応や部内のセキュリティ担当者としての活動を行っており、部内・社内のセキュリティ品質の維持向上に努めております。これらの業務に加えて、最近ではフィリピンやインドに在籍するメンバーと協力してプロジェクトを推進しています。その際にも、情報の取り扱いに関するルールの周知や遵守状況の確認、システム構築時のセキュリティ品質維持などの情報セキュリティマネジメントは欠かすことができません。このように形は様々に異なりますが「セキュリティ」と向き合う日々を送っています。

JNSAとの出会いは、2015年になります。同じ会社の岡本さん、嶋倉さんにご紹介いただき、大阪で行われたセミナーを聴講させていただいたことが始まりです。それまでの私の仕事に関する社外の方々とのつながりといえば、お客様や仕事でご一緒する関係会社の方々のみでしたので、このセミナーは会社や組織の垣根を越えた活動というものをほぼ初めて目の当たりにしたイベントでした。情報セキュリティの啓発や品質向上という目的のもとに活発に議論や講演が行われ、その熱気と初めて体験する雰囲気に刺激を受けたことが強く印象に残っています。その際に「今後は会員として参加したい」という思いもあったのですが、当時は会社の業務と日常生活で手がいっぱいだったこともあり、その後も何度かセミナーに足を運ぶのみでした。しかし今年度、岡本さんが工場のセキュリティを検討するWGを立ち上げる際に声をかけられたことを機に、WGに参加させていただくことになりました。現在の私は関西在住で育児中ということもあり、一度参加を諦めた時同様に慌ただしい毎日を送っていますが、会議も資料共有もオンライン形式ですので、今回は対応できると判断しました。これまでは、開催場所や時間の制約上、各種会議やイベントへの参加は諦めることが多かったのですが、昨年度から今年度にかけてはWGだけではなくSECCONの皆様が主催されたCTFやCTF for Girlsのセミナーにも参加することができました。今後も時間を作って多くの活動に参加したいです。

まだまだ勉強中の身で知識の習得が中心とはなりますが、まずはWGの活動を通して、微力ながら成果物の作成に貢献できればと思っております。どうぞよろしくお願いいたします。

SECURITY CONTEST (SECCON) 2021

https://www.seccon.jp/2021/

SECCON実行委員会（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）

SECCONは、情報セキュリティをテーマに多様な競技を開催する情報セキュリティコンテストイベントです。実践的情報セキュリティ人材の発掘・ 育成、技術の実践の場の提供を目的として、2012年に始まりました。世界の情報セキュリティ分野で通用する実践的情報セキュリティ人材の発掘・育成を最終目標として、まずはICTに関わるすべての人材への情報セキュリティの考え方や知見を広めることでセキュリティ予備人材の裾野を広げ、さらにその中から世界に通用するセキュリティ人材を輩出し、よって日本の情報セキュリティレベルを世界トップレベルに引き上げることを目的として活動を行っています。

SECCON2021

「SECCON」ではカンファレンスやワークショップなどのほかに、攻撃・防御両者の視点を含むセキュリティの総合力を試すハッキングコンテスト「CTF（Capture the Flag）」、セキュリティコンテスト参加を目指す人、ならびにセキュリティ技術者を目指す人向けのオンラインイベント「SECCON2021 電脳会議」を開催しました。

日　程	イベント	内　容
2021年7月17日(土)	ワークショップ	シェルコード解析入門とそのDFIRハンドリング
2021年9月25日(土)	ワークショップ	シェルコード解析アドバンス向け (ROOTCON-SECCON)
2021年12月4日(土)	ワークショップ	「ハンダ付けチャレンジ」ワークショップ
2021年12月11日(土)-12日(日)	SECCON CTF 2021	SECCON CTF
2021年12月18日(土)-19日(日)	SECCON 2021 電脳会議	オープンカンファレンス、ワークショップ、 コンテスト等

SECCON BEGINNERS

日本国内の CTF のプレイヤーを増やし、人材育成とセキュリティ技術の底上げを目的としたCTF未経験者向け勉強会です。海外のCTF でも上位に入る若手のCTFプレイヤーにより運営されており、CTF未経験の方でも CTF に参加できるよう、わかりやすくセキュリティ技術を教えるワークショップとなっております。2021年度は2回、オンラインで開催しました。

日　程	イベント	内　容
2021年5月22日(土)-23日(日)	SECCON Beginners CTF	ビギナーズ向け CTF
2021年10月17日(日)	SECCON Beginners Live 2021	ビギナーズ向け講演、CTF問題解説 等

CTF for Girls

情報セキュリティ技術に興味がある女性を対象に、気軽に技術的な質問や何気ない悩みを話しあうことが出来るコミュニティを作る事を目的に立ち上げられました。コミュニティ形成の一環として情報セキュリティ技術について学ぶワークショップや、その他女性向けCTFイベントの開催を行っており、毎回定員に達する人気イベントなっています。

日　程	イベント	内　容
2021年6月30日(水)	CTF for GIRLS ワークショップ	Exploit
2021年9月22日(水)	CTF for GIRLS ワークショップ	フォレンジック
2021年12月22日 (水)	CTF for GIRLS ワークショップ	Web分野

[協　賛]（2021年度実績）

ゴールドスポンサー

日本電気株式会社、日本マイクロソフト株式会社

シルバースポンサー

株式会社インターネットイニシアティブ、ＮＲＩセキュアテクノロジーズ株式会社、
コインチェック株式会社、セコムトラストシステムズ株式会社、
東京海上日動リスクコンサルティング株式会社、富士通株式会社

ブロンズスポンサー

株式会社アズジェント、学校法人岩崎学園、株式会社インフォセック、SBテクノロジー株式会社、
株式会社エヌ・ティ・ティ・データ、株式会社サイバーディフェンス研究所、Sansan株式会社、
ジェイズ・コミュニケーション株式会社、株式会社ディアイティ、トレンドマイクロ株式会社、
株式会社日本レジストリサービス、任天堂株式会社、ヤフー株式会社、株式会社ラック、
株式会社レオンテクノロジー

インフラスポンサー

さくらインターネット株式会社

メディアスポンサー

ZDNet Japan

[協賛企業の募集]

SECCONの運営は民間企業等からの協賛金により行っています。
2022年度（2022年4月から2023年3月期）も開催予定です。2022年度スポンサーを募集しておりますので、お気軽にお問合せ下さい。（SECCON運営事務局: info2021@seccon.jp）

SECCON メールマガジンのご登録はこちらから！

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/

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.51

2022 年 3 月 31 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/