SPRING 2025
VOL. 54

JNSA PRESS

JAPAN NETWORK SECURITY ASSOCIATION

寄稿記事

03 リアルタイムで動的な情報セキュリティマネジメントを目指して

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

CISOの育成と提供者のセキュリティ

株式会社 Preferred Networks
JNSA 副会長　CISO 支援ワーキンググループリーダー　髙橋 正和

2016年に設立したCISO支援ワーキンググループ（以下、WG）では、「業務執行としてのセキュリティ」、つまり「経営陣の一員としてセキュリティ業務を担うこと」をテーマに活動を続けている。

セキュリティは、提供者（セキュリティベンダー）の観点か、ベストプラクティス（規範）の観点で捉えられることが多いが、どちらも事業当事者外の視点である。効果的なセキュリティ施策を実装するためには、セキュリティ業務を司るCISOの重要性が高まっている。

業務執行としてのセキュリティ

WGの原点は、筆者が事業立上げを行った際に、事業責任者として報告すべきこと、求められていることが分からずに苦しい経験をしたことにある。当時、事業責任者として参考になる資料を探したが、見つけることは出来なかった。

「CISOハンドブック」[i] [ii]は、当時の自分が探していた資料を目指したもので、CISOとして、業務を担い、経営会議で適切な報告を行うための素材としてまとめている。「CISOのための情報セキュリティ戦略」[iii]は、机上演習を通じてハンドブックの内容を、実務に展開する事を目指したもので、イベントなどでワークショップを開催し、手引書やフォーマット（マテリアル[iv]）を、JNSAのWebで公開している。

CISOの壁と報連相の呪縛

ワークショップは、企業がランサムウエアに感染したシナリオを題材に、CISOとして事件・事故の対処を行い、これを公表する構成とし、テンプレートを埋めながら対処を進めることで、「業務執行としてのセキュリティ」を実感していただくことを目指している。

ワークショップを実施する中で、CISOを経験した方と、CISO経験のない方のギャップに印象深い違いがみられた。「経営陣に対する報告」という課題では、CISO経験者の多くは、結論に違いはあっても、事業や企業の視点で課題を考察し、「状況、見解と根拠、依頼と提案」として構成されていた。これに対して、CISO未経験者は、自身の立場で課題を捉え、自身が対処した内容に終始する傾向があった。いわゆる報連相のフォーマットになっていて、見解や経営陣に対する依頼・提案がみられなかった。

上記のギャップを議論するなかで、ワークショップが「CISOを育成する内容になっていない」ことが課題として指摘された。もともとCISOをターゲットとして構成しているのだが、CISO経験者よりも未経験者が多いことは自明であり、CISOを育成する試みは、未経験者がCISOを

目指す上でも、CISOを補佐する上でも有益であると考え、ワークショップにCISOの育成という観点を取り入れることとした。

本年（2024年）6月に公開したマテリアルでは、報告が「状況、見解と根拠、依頼と提案」となるように段取りを見直し、各課題の位置づけや狙いを明示し、想定するアウトプットを例示するなど、CISO育成につながる内容を目指して改定している。

提供者にとってのセキュリティ

DXという言葉が使われるようになって久しいが、DXと歩みを合わせるように、セキュリティ施策の論点が、提供者からユーザー側に移っている。提供者は、単にソリューションを提示するだけではなく、CISOの視点に沿った提案が求められるようになった。

しかし、提供者がこの変化を認識し、対応していくことは難しい面がある。本稿で紹介したWG活動の成果物は、CISOの実務や育成だけではなく、提供者がこの変化に対応し、ソリューションとしてのセキュリティから、ユーザー企業視点、事業視点からのセキュリティとして提案するために、活用いただけるものと考えている。

JNSAにおいて、CISO支援ワーキンググループは、ユーザー視点からの活動するユニークな存在といえる。ユーザー視点のセキュリティに取り組むことを通じて、提供者と利用者が施策を議論するための土台となることを目指して活動を続けていく所存である。

[i] JNSA CISO支援ワーキンググループ(2018)、CISOハンドブック、(https://www.jnsa.org/result/2018/act_ciso/)

[ii] JNSA CISO支援ワーキンググループ（著）、CISOハンドブック ―業務執行のための情報セキュリティ、技術評論社、2021年、ISBN 978-4297118358

[iii] 高橋正和（著）、CISOのための情報セキュリティ戦略―危機から逆算して攻略せよ、技術評論社、2023年、ISBN 978-4-297-13294-1

[iv] JNSA CISO支援ワーキンググループ(2024)、CISO-PRACTSIEワークショップ用マテリアル Ver2、(https://www.jnsa.org/result/act_ciso/2024/index.html)

リアルタイムで動的な情報セキュリティマネジメントを目指して

順天堂大学　健康データサイエンス学部
公認情報システム監査人（CISA）　満塩　尚史

1．はじめに

情報セキュリティマネジメントは、情報セキュリティを推進していくための基本的なフレームワークである。私自身も、情報セキュリティに関するコンサルティングや実組織での情報セキュリティ管理において、このフレームワークを活用してきた。

一方、情報セキュリティマネジメントが対象としている情報システムは、クラウドサービスの利活用が進み、生成AIも活用することが前提として構築されるようになってきている。この状況において、急速に変化する情報システムに対し、現状のISMSで十分なのか疑問を抱くようになった。特に、“人”による情報セキュリティ監査の実施や、“人”が理解しやすい情報セキュリティポリシーの在り方を改善するべきではないかと感じている。そのため、最近の実際の情報セキュリティ管理の推進においては、これらを改善するソリューションを適用することを意識している。

2. “人”によるISMS推進の限界

情報セキュリティマネジメントシステム（ISMS）は、情報セキュリティ（「情報の機密性、完全性、可用性の維持」）を確保するための枠組みである。ISMSの考え方の詳細は、JIS Q 27001情報セキュリティマネジメントシステム要求事項に整理されているが、大きな枠組みとしては、図1のPlan（計画）、Do（実施）、Check（点検･監査）、Act（見直し･改善）と整理できる。ISMSは、“人”によってPlan（計画）が企画され、“人”による情報セキュリティ監査を中心にCheck（点検･監査）が行われ、“人”によるAct（見直し・改善）が行われることが、当たり前だった。

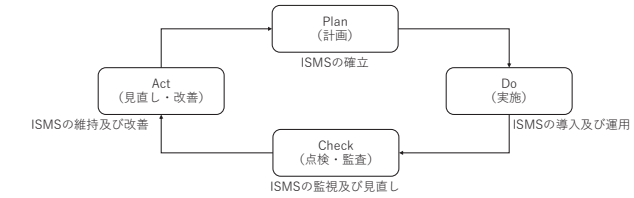


図1　ISMSのPDCAサイクル

一方、Do（実施）の環境は、大きく変わってきている。クラウドサービスの利活用により、システム構築自体をコード（プログラム）で記述したり、クラウドサービスのプラットフォーム経由で情報システムをモニタリングすることが可能になった。つまり、Do（実施）に関するあらゆるものがデジタル化され、データ化されつつある。

そのため、Do（実施）としての情報システム管理のデジタルデータの活用が進む一方で、その他のISMSのプロセスは依然として手作業に依存しており、大きなギャップが生じてきており、現状の“人”の手で推進するISMSフレームワークには限界を感じている。

3. Society 5.0のISMSへの適用

Society 5.0は、平成26年の第5期科学技術基本計画で提唱され、日本が目指すべき未来社会の姿として位置づけられています。Society5.0は、狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く新たな社会です。

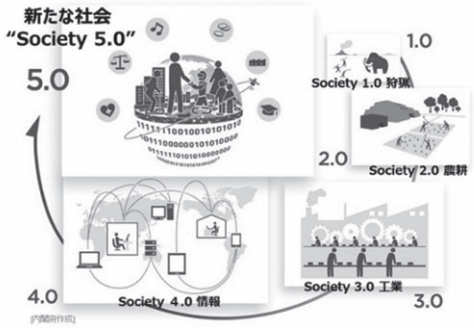


図2　Society 5.0の位置付け

具体的には、Society 5.0は、「サイバー空間とフィジカル空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会」とされている。この考え方をISMSに適用して考えてみると、人や情報システム（フィジカル空間）における“情報セキュリティの対策状況”をサイバー空間と融合させることが、Society 5.0の概念のISMSへの適用だと考える。

現在のISMSは、“人”が、情報システムの“情報セキュリティの対策状況”を確認し、監査レポート等にまとめて、次の見直しに活用している。このフィジカル空間で行われている“情報セキュリティの対策状況”の確認をサイバー空間であるデジタル化やデータ化を活用し高度化することが必要だと考えている。

4. “人”による情報セキュリティ監査の限界

情報セキュリティ監査においては、管理体制、マネジメント、情報システム上のセキュリティ対策の状況を監査する。情報セキュリティ監査は、“人”により、行われるため、情報セキュリティ監査を開始するにあたっては、監査対象期間を確定する。その場合、この監査対象期間は、当然ながら、監査人が監査を実施するより以前に設定される。監査は、“人”による確認と監査レポートの作成には、相当の時間がかかる。そのため、監査の規模にもよるが、監査対象期間の終了時から監査レポートを入手するのに、数週間から数か月経過していることが一般的である。つまり、監査レポートを通じて把握できるのは、“数か月前の過去の情報セキュリティの対策状況”に過ぎないということである。

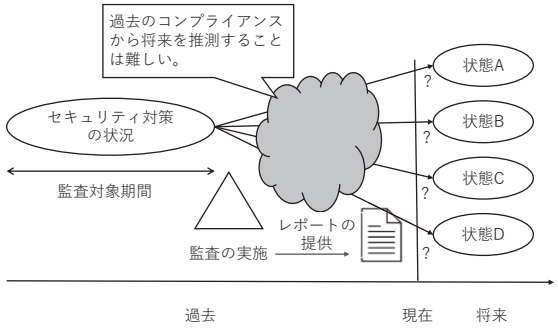


図3　情報セキュリティ監査のイメージと課題

この状況をもう少し詳細に考えてみたい。監査レポートにより把握できるのは、“数か月前の過去の情報セキュリティの対策状況”であり、監査実施後の現在の情報システムのライフサイクルを考えると、監査対象期間の終了後から一定の時間が経過しており、現在や将来にわたって、監査対象期間と同じ状況であると推測することは、困難になっている。

5. 情報システムのモニタリングの充実

従来は、情報システムは、専用の建屋やラック、ハードウェアを準備し、その上にOS、ミドルウェア、アプリを構築してきた。また、構築した情報システムは、運用管理者が日々運用し、その状況やセキュリティの対策状況を把握し、情報システムの管理責任者に報告を行っていた。

また、必要に応じて、監視や検知をする情報システム自体を構築しており、これには多大なコストと手間がかかっていた。

近年、この情報システムの構築方法もIaaS、PaaS、SaaSなどのクラウドサービスを利用し、構築し、運用されるようになってきた。例えば、クラウドサービスプロバイダー（CSP）が提供する管理画面やAPIを通じて、情報システムの状態を把握するデータを確認し、デジタルデータとして取得できるようになった。

また、エンタープライズのパソコン端末にも、EDR[1]を導入し端末管理をすることが一般的になってきている。EDRは元々、エンドポイントでの不審な挙動を検知し、迅速な対応を支援するためのセキュリティ対策製品である。このEDRの機能を活用して、不審な挙動がない場合でもパソコン端末の情報収集を行うセンサーとして利用できる。

このようにCSPの管理コンソールやAPI経由でのデータ収集やパソコン端末のEDR経由などの多種多様な手法で情報システムがモニタリングされ、取得されたデジタルデータが活用できる可能性が拡大してきた。

[1] Endpoint Detection and Response

6. デジタルデータによるモニタリング効果

情報システムの資産の把握や情報セキュリティ状態のモニタリングは、従来のISMSにおいても、必須である。ただし、このモニタリングは“人”を介して行われることを想定しており、例えば、資産に関しては、台帳的な把握にとどまっており、オンタイムで資産を把握していたわけではなかった。具体的に言えば、資産台帳として1,000台のパソコン端末があるという把握は可能である。一方、EDRを使って把握すると、それぞれの瞬間瞬間に1台単位で接続状況や稼働状況が把握できるようになり、全てのパソコン端末が常に接続されているわけではないことも可視化できる。

機能にもよるが、EDRを活用し、パソコン端末のソフトウェアの導入状況、バージョン情報、セキュリティパッチの適用状況等もデジタルデータとして把握できる。また、クラウドサービスを活用した情報システムの状況をAPI経由で継続的なデジタル化されたデータとして把握することができる。

その結果、デジタルデータとして把握されることで、データサイエンスで発展してきたデータ分析手法を活用することも可能になる。モニタリングで得られたデジタルデータを活用することで、ISMSフレームワークにデータ分析手法を適用できる可能性がでてくる。

7. “将来の情報セキュリティ”を確保

情報セキュリティ監査は、“過去のコンプライアンス状況の証明”として位置づけられる。“過去のコンプライアンス状況を証明”することは、情報システムが情報セキュリティとして健全であったことを示す重要な証拠である。一方、実組織においては、“過去のコンプライアンス状況を証明”することも重要であるが、“将来の情報セキュリティ”を確保することはさらに重要である。

モニタリングの特徴の一つとしては、数か月前の監査対象期間の状況ではなく、日々の情報システムの状況をほぼリアルタイムでモニタリングすることにより、極めて直前の過去の“情報セキュリティ対策の状態”を把握することができる。そのため、日々変化する状態を把握し、現在に極めて近い状態を把握することができる。また、将来の状態は、現在の状態が急激に変わる可能性が低いため、“将来の情報セキュリティ”を予測できると言えるのではないだろうか。

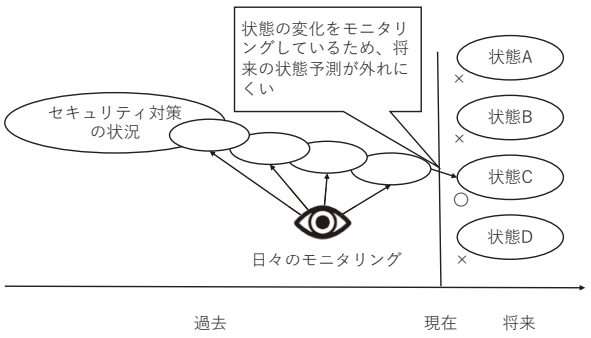


図4　モニタリングによる把握のイメージ

8. 情報セキュリティポリシーの記述の限界

ISMSでは、Plan（計画）で策定された情報セキュリティポリシーをDo（実施）で実行し、Check（点検・監査）で監査し、Act（見直し・改善）で改善していくことになる。つまり、情報セキュリティポリシーは、PDCAサイクルの中心的な要素の一つである。情報セキュリティポリシーは、ITガバナンスにおける統制目標の集合体であり、システム監査制度やISMAP制度ではシステム管理基準と呼ばれる。

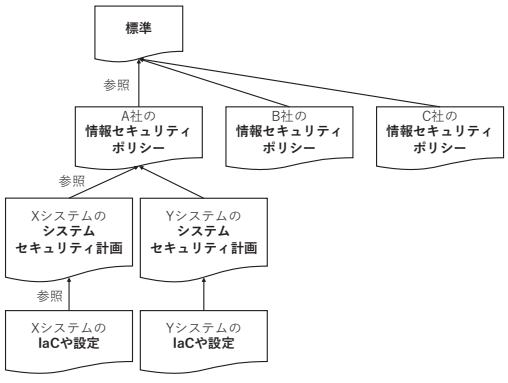


図5　情報セキュリティポリシーとセキュリティ対策の実装の関係

理想的には、図5に示す通り、業界標準や認証制度の管理基準を参照し、各組織の情報セキュリティポリシーは策定される。各組織では、構築する情報システムの特性に従って、情報セキュリティポリシーに従った情報システム毎の統制目標をまとめたシステムセキュリティ計画を作成し、実際の情報システムのIaC [2]や設定に反映することが望ましい。IaaS、PaaS、SaaSのクラウドサービスを活用し、情報システムを構築することが一般的になってきたため、情報セキュリティに関するコントロールの多くは、クラウドサービスの設定であり、IaCとして、定義される機能になることが多い。

そのため、基準・情報セキュリティポリシーとシステムのIaCや設定との関係性を明確にトレースできることが求められる。

ただし、現状の情報セキュリティポリシーや管理基準は、様々な組織や情報システムに対応するために、“人”の解釈に幅が持たせる形で記述されており、統制目標とシステムの関係性をトレースすることは、難しい。

9. 統制目標のオブジェクト化の検討

このため、情報セキュリティポリシーを構成する統制目標をオブジェクト化する必要性がある。既に、米国NISTでは、OSCAL（Open Security Controls Assessment Language）プロジェクトにおいて、統制目標を記述する言語開発が進んでいる。図6は、OSCALにより、米国NIST SP800-53 の一部をYAMLで記述した記述例である。

```
groups:
       - id: ia class: family
         title: Identification and Authentication
         controls:
（中略）
       - id: ia-3
         class: SP800-53
         title: Device Identification and Authentication
         params:
                - id: ia-03_odp.01
                  label:devices and/or types of devices
                  identified and authenticated before establishing a connection are defined;
               - id: ia-03_odp.02
                 select:
                      how-many: one-or-more
                      choice:
                            - local
                            - remote
                            - network
```

図6　統制目標のOSCALでの記述例

OSCALの使い方はいくつか考えられ、現在、いくつかのプロジェクトで試験的に導入されつつある。

例えば、複数の業界標準等への対応が求められる情報セキュリティ管理の整理がある。今日の情報システムは、複雑な情報セキュリティの要件に対応していく必要がある。例えば、政府の中で、クレジット会員の情報を扱う情報システムを構築する場合、当然ながら、クレジット業界の情報セキュリティ基準であるPCI DSSの要件に対応していく必要がある。また、個人情報を扱うため、個人情報保護法の安全管理措置にも対応していく必要がある。更には、政府の情報システムは、内閣サイバーセキュリティセンターの定める政府機関等のサイバーセキュリティ対策のための統一基準群にも準拠する必要がある。これらの複数の制度の情報セキュリティの要件を“人”が正確に把握し、実装していくのは至難の業である。

将来的に、PCI DSS、個人情報保護法の安全管理措置、政府機関等のサイバーセキュリティ対策のための統一基準群が、OSCALで記述され、同じ統制目標の統一された表記が可能になれば、複数の要件を一つの情報システムに適用することが容易になると考えられる。

また、統制目標をオブジェクト化するということは、オブジェクト化された統制目標を個々にモニタリングできると効率的な監視プロセスを構築することができる。個々の統制目標の状態をデジタルで把握できるようになれば、情報セキュリティ監査の自動化も現実味を帯びてくる。

統制目標のオブジェクト化は、現在も様々な場面で検討されており、今後も引き続き利活用の検討が必要である。

10. おわりに

今回は、ISMSにおいて情報セキュリティ監査をモニタリングに置き換え、デジタルデータとして把握する方法と、そのデータ分析手法の活用の可能性について紹介しました。また、情報セキュリティポリシーを構成する統制目標をオブジェクト化することで、情報セキュリ

[2] Infrastructure as Code

ティ対策とポリシーの関係を明確にする可能性についても触れた。これは、情報セキュリティマネジメントのPDCAサイクルを維持しつつ、リアルタイムでモニタリングしたデジタルデータを活用し、ライフサイクルを短期間で回すことで、動的な情報セキュリティマネジメントを実現する試みであると考えている。

【参考URL】

● 内閣府　Society 5.0
https://www8.cao.go.jp/cstp/society5_0/index.html

● デジタル庁　DS-211 常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）
https://www.digital.go.jp/resources/standard_guidelines#ds211

● NIST OSCAL:the Open Security Controls Assessment Language
https://pages.nist.gov/OSCAL/

● デジタル庁　DS-231 セキュリティ統制のカタログ化に関する技術レポート
https://www.digital.go.jp/resources/standard_guidelines#ds231

JNSA ワーキンググループ紹介

JNSA 教育部会　ゲーム教育ワーキンググループ

ワーキンググループリーダー：長谷川　長一（株式会社ラック）

ゲーム教育ワーキンググループは2016年度より、ゲームなどを取り入れた新たなセキュリティ教育手法の可能性についての検討から活動を始めました。その後、様々なゲームの調査・研究を行い、JNSAオリジナルのゲームを2種類、開発リリースを行いました。それが「セキュリティ専門家人狼」と「Malware Containment」です。「セキュリティ専門家人狼」は、内部不正の手口と対策を学ぶカードゲーム、「Malware Containment」はマルウェア感染時の初動対応の体制やプロセスを学ぶボードゲームです。ゲームについては、本ページ下部記載のURLからご覧ください。

当ワーキンググループではゲームを使ったセキュリティ教育の普及にも取り組み、その一環として大学や高専などの高等教育機関との連携活動を2017年度より進めてきました。講師派遣を通して授業での演習実施や教員の皆様への研修会などを実施し、2019年度には国立高専機構様と共同で「Malware Containment」のWeb版を制作しました。これにより、アナログなゲーム教材の準備や遠隔での演習実施も可能となり、2020年2月より新型コロナウイルス感染拡大による対面授業ができない時期も大いに効果を発揮しました。

ゲーム教育は、PCの性能やネットワーク環境などに依存せず、受講者内での知識の差があってもグループ演習が実施できる手法です。さらに、受講者が関心をもって取り組みやすく、演習後の振り返りなども容易にできる学習効果の高いものとなっています。

現在は、高等教育機関との連携、講師派遣活動を継続しながら、ゲームの調査・研究や新たなゲームの企画・開発に取り組んでいます。ゲームを使ったセキュリティ教育にご興味のある高等教育機関の皆様は、お気軽にお問合せください。

■ JNSA教育部会 ゲーム教育ワーキンググループ

https://www.jnsa.org/edu/secgame/

■ JNSA Channel「セキュリティ専門家人狼」

・ゲームの目的編
https://www.youtube.com/watch?v=i633DTaIAK0
・ゲームの流れ
https://www.youtube.com/watch?v=AUce-3ggsbc
セキュリティに対する知見が浅い方でも、ワーキンググループの活動に参加できる方は歓迎致します。

西日本支部　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ワーキンググループ ～中小製造業向け工場セキュリティ対策ハンドブック作成～

ワーキンググループリーダー：岡本　登（富士通株式会社）

日本ネットワークセキュリティ協会西日本支部では、中小製造業の皆様が容易に工場セキュリティ対策に取り組めるよう、実用的なハンドブックの作成を進めています。本活動は、情報セキュリティの専門知識がなくても、現場で直ちに活かせる対策を提示することを目指し、2020年11月から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として活動をスタートしました。

●なぜ、中小製造業の工場セキュリティ対策が重要なのか？

昨今、サイバー攻撃はますます巧妙化し、製造業もその標的となるケースが増えています。特に、中小製造業は、大企業に比べてセキュリティ対策の体制が整っていない場合が多く、攻撃に遭いやすい状況にあります。工場の操業停止や機密情報の漏洩など、サイバー攻撃は企業の存続を脅かす深刻な事態を引き起こす可能性があります。また、サプライチェーンリスクを考えると、中小製造業の対策は非常に重要であると考えています。

●ハンドブックの特長と内容

①リスクアセスメント編

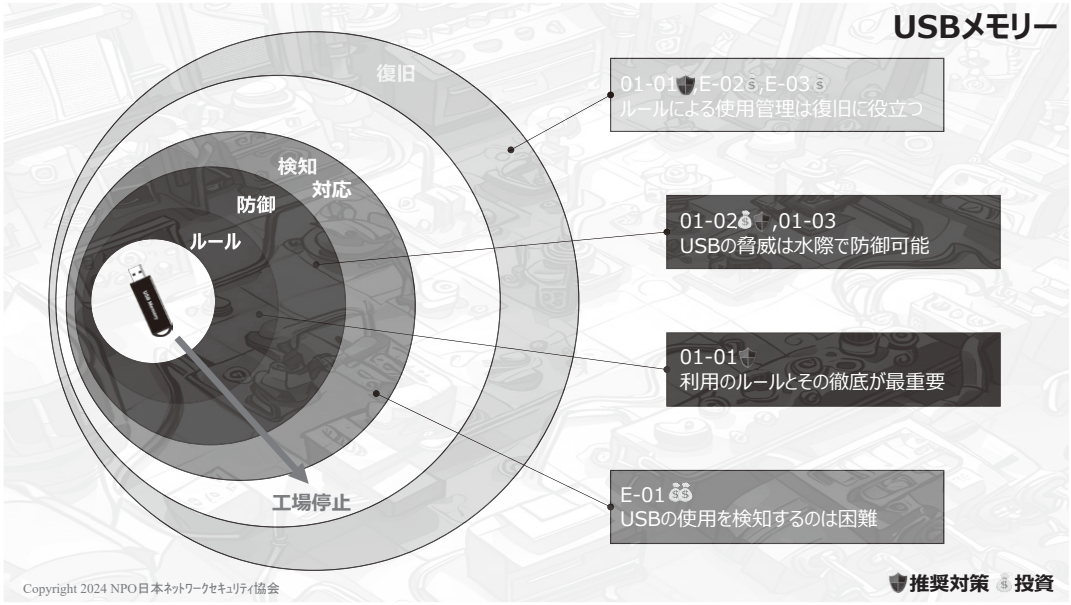
- 情報資産から始めるのではなく、脅威の入口に着目：
  一般的なリスクアセスメント手法とは異なり、USBメモリー、持込パソコンなど、製造現場に存在する13種類の「脅威の入口」に着目し、それぞれの入口から発生する可能性のあるリスクを評価します。
- 簡単なフローチャートで評価：
  専門的な知識がなくても、フローチャートに沿って評価することで、自社のリスクレベルを簡単に把握できます。

No	脅威の入口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリー	USBメモリーから制御システムや製造装置にマルウェアの感染が広がる	工場停止
2	持込パソコン	持込パソコンから制御システムや製造装置にマルウェアの感染が広がる	工場停止
3	スマホ・タブレット	スマホ・タブレットに感染したマルウェアが利用者の意図しない動作をさせる	情報漏洩
4	IoT機器・センサー	IoT機器・センサーが第三者に遠隔操作される	工場停止
5	複合機	複合機が第三者に遠隔操作される	情報漏洩
6	ハンディターミナル	ハンディターミナルに感染したマルウェアがプログラムやデータを改竄する	情報改竄
7	OAネットワーク	OAネットワークからマルウェアの感染が広がる	工場停止
8	インターネット	インターネットからマルウェアの感染が広がる	工場停止
9	WiFi (無線AP)	WiFI通信が傍受されたり、通信が妨害される	情報漏洩
10	保守用ネットワーク	保守用ネットワークからマルウェアの感染が広がる	工場停止
11	クラウドサービス	認証情報が不正に利用される	情報漏洩
12	部品・原材料	組み込んだ部品のセキュリティ不具合が悪用される	品質低下
13	新規購入機器	新規購入した機器から制御システムや製造装置にマルウェアの感染が広がる	工場停止

JNSA ワーキンググループ紹介

②リスク対策編

- 13の入口ごとに具体的な対策集:
  各脅威の入口ごとに、多様な対策をルール（統治）、特定、防御、検知、対応、復旧を軸に整理して紹介しています。
- コスト情報も掲載:
  各対策の実施に必要なコストも参考情報として掲載しており、予算に合わせて最適な対策を選択できます。



③サイバーBCP策定編（検討中）

- セキュリティ専門家がいなくても対応可能:
  サイバー攻撃が発生した場合の対応手順を、わかりやすく解説します。
- 被害を最小限に抑えるための具体的な対策:
  迅速な復旧や被害拡大防止のための対策を、具体的な手順とともに紹介します。
- サイバーBCPのひな形と自社に合わせたカスタマイズ方法も紹介する予定です。

●ハンドブック作成におけるこだわり

- 現場の声を反映:
  中小製造業の現場で働く方々にヒアリングを行い、実際の課題やニーズを反映しています。
- わかりやすい言葉で解説:
  専門用語を極力避け、図や表なども用いて、誰でも理解できるよう工夫しています。
- 実用性を重視:
  現場ですぐに実践できる具体的な対策を提示することを重視しています。

●ワーキンググループ活動について

- 月1回の活動：オンサイトとオンラインを併用し、活発な議論を行っています。
- メンバー数：現在約30名（西日本地区以外の方も参加）
- 活動期間：2020年11月～

●今後の展望

現在、③のサイバーBCP策定編の作成を進めており、2024年度中の公開を目指しています。また、セミナーやイベントなどで作成したハンドブックの普及活動も積極的に行っていく予定です。

おわりに

本ワーキンググループ活動を通じて、中小製造業の皆様が安心して事業に取り組める環境づくりに貢献できればと考えています。本ハンドブックが、皆様のセキュリティ対策の一助となれば幸いです。

【お問い合わせ】

日本ネットワークセキュリティ協会

事務局　sec@jnsa.org

これまでの成果物

・今すぐ実践できる工場セキュリティハンドブック・リスクアセスメント編
https://www.jnsa.org/result/west/2022/index.html

・今すぐ実践できる工場セキュリティハンドブック・リスク対策編
https://www.jnsa.org/result/west/2023/index.html

JNSA ワーキンググループ紹介

事業コンプライアンス部会

部会長：倉持　浩明（株式会社ラック）
副部会長：唐沢　勇輔（Japan Digital Design 株式会社）

事業コンプライアンス部会について

事業コンプライアンス部会は、サイバーセキュリティサービス事業者が社会的責任を果たし、顧客からの信頼を確保し、そして自らを守るために、適正な事業運営の在り方を検討する部会です。具体的には、「サイバーセキュリティ業務における倫理行動宣言」の策定と、自己宣言を行う企業の募集や、宣言内容の更新を行っています。また、法執行機関との連絡窓口としての役割や、国内外の法令リスク事例の調査を実施し、成果物として「法令リスク一覧」を会員企業向けに提供しています。

自社は大丈夫？サイバーセキュリティ事業の法令リスク

サイバーセキュリティ事業では、脆弱性情報やペネトレーションテストの技術など、一般の業務では扱わない高度な技術や情報を取り扱うため、扱い方を誤ると、第三者にとって脅威となる可能性があります。例えば、脆弱性情報が漏洩し、それを攻撃者が利用することが考えられます。そのため、法令違反のリスクが常に存在することを認識し、適切な対策を講じる必要があります。

事例：講演や記事によるマルウェアコードの流出

インテリジェンスサービスを提供しているA社のリサーチャーB氏は、カンファレンスやブログにて多数の調査研究成果を公開していましたが、その中でマルウェアの使用を促すような記述があり、一部で動作可能なマルウェアコードを公開してしまった事例です。この場合、不正指令電磁的記録提供罪に問われる可能性があります。調査研究目的であっても、法的に正当な理由がない限り、このような行為は法令リスクに該当する恐れがあります。

事例：契約対象外の顧客へのセキュリティ診断

セキュリティ診断サービスを提供するA社が、顧客B社から指示されたIPアドレスやドメインに対してペネトレーションテストを実施しようとしたが、指定ミスにより無関係なC社に対してテストを実施してしまった事例です。この行為は意図的でなくても、不正アクセス禁止法に問われるリスクがあります。契約のある顧客に対しては正当な業務目的となる行為も、契約のない顧客に対して行うと法令リスクが生じる恐れがあります。

サイバーセキュリティ事業者が留意すべき法令リスクを一覧で提供

事業コンプライアンス部会では、サイバーセキュリティ事業者が留意すべき「法令リスク一覧」をJNSA会員企業限定で提供しています。この一覧は、正当な業務を行っていても抵触する可能性のある法令上のリスクを整理し、事業者が自らの対策に役立てることを目的としています。社内研修でご利用いただくことを想定したプレゼンテーション版もご用意していますので、是非ご活用ください。

事業の正当性を対外的に示す「サイバーセキュリティ業務における倫理行動宣言」

事業コンプライアンス部会ではサイバーセキュリティ関連業務に特有のコンプライアンスリスクを管理していることを社会や関係省庁に対して明らかにすることを目的として、「サイバーセキュリティ業務における倫理行動宣言」を策定しています。正当なセキュリティ事業を行なっていても抵触する可能性のある業務が違法性を問われないためには、「社内で管理体制や教育を周知していること」「それらの取り扱いが必要となる事業を継続的に行っていること」を裏付け、事業の正当性を対外的に示すことが望ましいと考えられます。

「サイバーセキュリティ業務における倫理行動宣言」に則り、サイバーセキュリティ業務を遂行することを自己宣言していただく企業を募集しています。ご賛同頂ける企業はJNSA事務局までご連絡ください。ご賛同いただいた企業名や事業部名は、JNSAのWebサイトに掲載します。JNSAのWebサイトに貴社名を掲載することで、より信頼性が増すと考えられます。

サイバーセキュリティ業務における倫理行動宣言
https://www.jnsa.org/cybersecurity_ethics/index.html

さいごに

事業コンプライアンス部会は、サイバーセキュリティ事業の法令遵守とコンプライアンス強化を推進し、業界全体の健全な発展を目指しています。部会への参加を希望される方は、事務局までお問い合わせください。皆様と共に、業界全体の健全な発展を目指し、より安全で信頼されるサービス提供に取り組んでいけることを期待しています。

会員企業ご紹介54

テクマトリックス株式会社

https://www.techmatrix.co.jp/

TechMatrix

お客様が抱える課題解決へ　デジタルの目利き力を発揮

テクマトリックス・グループは「より良い未来を創造するITプロフェッショナル集団」をミッションに、情報基盤、アプリケーション・サービス、医療システムの三つを事業の柱としています。

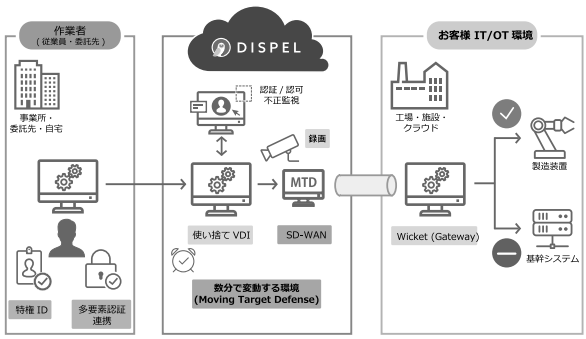
目利き力と業務ノウハウで社会課題を解決し、
より良い未来の創造に貢献します

代表取締役社長　矢井　隆晴

テクマトリックス・グループは、従来のシステムインテグレーターの労働集約的なビジネスモデルを自ら破壊し、ITサービス産業におけるサプライサイド企業の存在意義を再定義します。デジタル化への急激なシフトと産業構造の劇的な変化を成長機会と捉え、今後の社会にとって必要不可欠な領域に向けた事業を加速し、社会課題を解決するためのサービス提供を通してDXの推進やその先にある持続可能な社会の創造に貢献することを目指します。世の中の変化の流れを読み解きながら自己変革を続け、新しいテクノロジーや新しいビジネスに挑戦し、より良い未来の創造に貢献するITのプロフェッショナル集団であり続けたいと思います。

新製品

■IT/OTのリモートメンテナンスに特化したゼロトラスト型セキュアリモートアクセスサービス



製品特長

- クラウド上で提供する統合プラットフォームにより、IT/OT機器にアクセスすることをリアルタイムで制御
- 数分おきにクラウド環境のIPアドレスやアクセスリストを変動させる防御機能により、ランサムウェアなどの外部からのサイバー攻撃を回避

お問い合せ	テクマトリックス株式会社 〒108-8588 東京都港区港南1丁目2番70号　品川シーズンテラス 24階 nws-info@techmatrix.co.jp　https://www.techmatrix.co.jp/

株式会社 DX コンサルティング
https://www.dx-consul.co.jp/

私たち DX コンサルティングは、企業のデジタルトランスフォーメーション（DX）を支援するコンサルティングサービスを提供しています。多くの企業と共に成功事例を積み重ねており、お客様のビジネスに付加価値を提供し、持続的な成長を実現します。さらに、DX 領域や IT サービスマネジメント（ITSM）領域のコンサルティング、ITSM やセキュリティ関連のソリューション導入、ITIL® や SIAM™ などの研修サービスを含めた総合的なサポートを提供しています。

DXコンサルティングのサービス

- コンサルティング -

DX 戦略立案支援
DX 導入のための目標設定、課題解決、競合分析、IT 技術導入を総合的に支援します。

現状分析サービス
IT サービスマネジメント、ISO/IEC20000、IT ガバナンスなど、お客様企業の目的に応じた現状分析を提供します。

- ソリューション -

IT サービスマネジメント
ITIL® に準拠した多機能な IT システムで、効率的かつ円滑な IT サービス管理を提供します。

運用自動化（Kompira/UiPath）
自動化に最適化された運用や業務の仕組みを提案し、効果を最大化します。

- 研修 -

ITIL® 研修 / 試験
ITIL® 4 を学び、ケーススタディとディスカッションで実務応用力を高め、認定試験合格を目指します。

SIAM™ 研修 / 試験
複数のサービスプロバイダを統合管理するための方法論を学び、実務に役立つ知識とスキルを習得し、認定試験合格を目指します。

DevOps Institute 研修 / 試験
開発と運用の連携を強化し、自動化と効率化を学び、DevOps Institute 認定資格取得を目指します。

AI ファンデーション研修 / 試験
持続可能な AI 設計から機械学習の実践まで、AI とロボティクスに関する幅広い知識とスキルを習得し、国際的に通用する AI 資格の取得を目指します。

セキュリティ関連のサービス

セキュリティ・コンサルティング
ISO/IEC 27001 や 27017 などの認証支援サービス、他 を支援します。

特権 ID 管理　Password Manager Pro *
システム管理者が使う高い権限の悪用を防止し、情報漏洩を抑止します。

ログ管理　EventLog Analyzer *
問題の早期発見や、ログ管理の厳格化により内部監査対応などセキュリティ強化を支援します。

AD 管理　AD Manager Plus/ADSelfService Plus/ADAudit Plus *
定例作業の自動化、権限委任、効率的なユーザ管理でセキュリティを強化し、お客様に合わせた運用コストを削減します。

パッチ管理　Endpoint Central *
組織内の多様なデバイスを一元的に管理する統合エンドポイント管理により、ソフトウェア配布やパッチ管理などの作業負荷を削減し、可視性と IT セキュリティの向上を支援します。

*紹介するセキュリティ製品は、ゾーホージャパン株式会社が提供しています。

お問い合せ	株式会社 DX コンサルティング 〒102-0076 東京都千代田区五番町 12 番地 1 番町会館 電話番号: 03-5211-0812 お問い合わせフォーム: https://www.dx-consul.co.jp/inquiry/service.html

株式会社スリーシェイク
https://www.securify.jp/

3-SHAKE

攻撃者視点で先回りのセキュリティ対策を

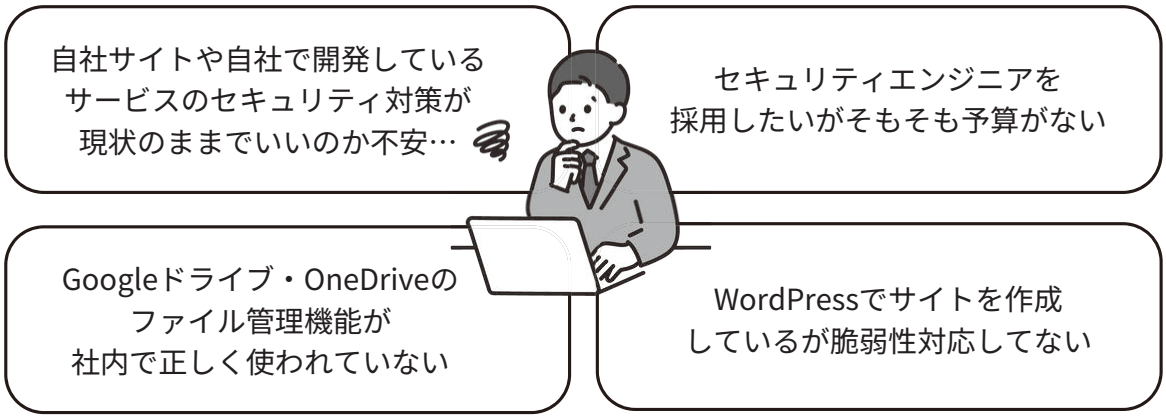
スリーシェイク社が開発・提供するSecurify(セキュリファイ)は、
セキュリティエンジニアでなくても分かりやすい簡単な操作で
手軽に何度でも診断ができるセキュリティツールです。

Securify

Webアプリケーション診断
Webアプリケーションの脆弱性を検知し、継続的なセキュリティテストを実現します。

SaaS診断
Googleドライブ・OneDrive内ファイルの公開設定状況を可視化し、情報漏洩管理の向上を実現します。

WordPress診断
攻撃の糸口となるようなWordPressの設定を見つけ出し、セキュリティ向上を実現します。



Securifyの実績

他、2024年下半期にも各SaaS比較サイトで受賞が決定しています！

導入社数
100社以上

ITトレンド上半期ランキング
2024
セキュリティ診断
ITトレンド上半期ランキング
セキュリティ診断 第1位

ITトレンド
「セキュリティ診断」カテゴリ1位

経済産業省
情報セキュリティサービス基準適合

お問い合せ	株式会社スリーシェイク 〒160-0015 東京都新宿区大京町22-1グランファースト新宿御苑3F・4F securify@3-shake.com

Search
セキュリファイ

JNSA 会員企業のサービス・製品情報

■製品紹介■

○Vex
Vexは、高度な脆弱性診断を可能にするプロ品質のWebアプリケーション脆弱性検査ツールで、診断精度の高さが特徴です。
このVexのノウハウを基に生まれ、脆弱性診断をより手軽に、簡単に行えるツールがVexCloudで、誰でも簡単に利用できる自動診断を提供します。
2つのツールの組み合わせにより、コストとリソースを最小限に抑えた効果的なWebセキュリティ対策を実現できる環境を提供します。
【製品情報詳細】
https://www.ubsecure.jp/vex

◆お問い合わせ先◆
株式会社ユービーセキュア
sales@ubsecure.jp

■サービス紹介■

○特権ID管理ツール導入サービス
特権IDは、Administratorやrootのようにシステム管理者が使用するIDです。
企業が保有する情報の価値が拡大する昨今、内部犯行の温床となりやすい特権IDの管理対策を講じることは、企業の信用、信頼、安全に繋がり、持続的な成長と競争力の強化を実現します。
当社のサービスの特長は、以下の3点となります。
・強固なセキュリティ対策の実現
・低コスト・短期間での導入
・導入後の運用コンサルティングも提供可能
【サービス情報詳細】
https://www.dx-consul.co.jp/business/itil_idkannri.html

◆お問い合わせ先◆
株式会社DXコンサルティング
TEL:03-5211-0812
https://www.dx-consul.co.jp/

イベント開催の報告

JNSA 全国サイバーセキュリティセミナー 2024 セミナー報告

JNSA マーケティング部会 部会長：小屋 晋吾

マーケティング部会では2017年より全国の中小企業を対象としたサイバーセキュリティセミナーを開催しています。2024年は9月から10月にかけて開催いたしました。

セミナー概要

タイトル: 「アタフタしないためのセキュリティ前始末のすすめ」
～組織に求められる困難をしなやかに乗り越え回復する力～
主　　催: 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）
後　　援: NPO ITコーディネータ協会
協　　賛: 株式会社エーアイセキュリティラボ、一般社団法人セキュアIoTプラットフォーム協議会、一般社団法人セキュリティ・エデュケーション・アライアンス・ジャパン、パロアルトネットワークス株式会社、株式会社 日立ソリューションズ
対　　象: 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
参 加 費: 無料

セミナー内容

本セミナーは、中小企業を中心にサイバーセキュリティリスクに対応するための具体的な対策と、新しいサイバー攻撃に備えるための「抵抗力」と「回復力」についての理解を深めることを目的として開催されました。

開催日程・会場
- 東 京 会 場: 2024年9月25日（水）13:30～16:30 （AP新橋）
- 名古屋会場: 2024年10月4日（金）13:30～16:30 （AP名古屋）
- 大 阪 会 場: 2024年10月9日（水）13:30～16:30 （APイノゲート大阪）

プログラムの詳細

1. 開会挨拶（13:30～13:35）
JNSAマーケティング部会 部会長 小屋 晋吾が開会の挨拶を行い、JNSAの概要及びこれまでの全国サイバーセキュリティセミナーの説明および本日の概要につき説明しました。
2. 講演1（13:35～14:20）：「産業分野におけるサイバーセキュリティ政策」
講演者: 経済産業省 商務情報政策局 サイバーセキュリティ課
主な内容として、中小企業のサイバーセキュリティの現状や、それに対して経済産業省が取り組んでいる政策が紹介されました。また、具体的なサイバー攻撃の事例も挙げ、政策による支援策についての説明がありました。
3. 講演2（14:20～15:00）：「抵抗力と回復力が新しいサイバーセキュリティ対策のカギ」
講演者: JNSAマーケティング部会 副部会長 持田 啓司
ランサムウェアなどの高度なサイバー攻撃に対する対策として、「抵抗力」と「回復力」が重要であることが強調されました。サプライチェーンのリスクと中小企業の役割が特に注目されました。

休　　憩 (15:00～15:10)

4. 講演3 (15:10～15:50) : 「国際標準レベルのセキュリティ組織実現に向けた取り組み」
講演者: 日本セキュリティオペレーション事業者協議会 （ISOG-J） 副代表 武井 滋紀氏 （東京・大阪会場）／早川 敦史氏 （名古屋会場）
セキュリティ組織の国際標準レベルへの取り組みを紹介し、ISOG-Jのガイドラインやドキュメントをどのように活用すべきかを解説しました。
5. 講演4 (15:50～16:25) : 「有効活用したいJNSAツールの紹介とJNSA入会のメリット」
講演者: JNSAマーケティング部会｜会員交流部会 部会長 扇 健一
セキュリティ対策を実践するためのJNSAのツール類の紹介や資料の説明を行いました。またJNSAに入会することで得られるメリットについて説明が行われました。

参加者の反応

- 東京会場には44名、名古屋会場には29名、大阪会場には46名が参加
- 出席者の約半数からアンケートの回答があり、98%が参考になったとの回答
- 特にISOG/Jによる講演内容に高い評価

まとめ

コロナ禍により中断していた全国セミナーを、今回オンサイト形式で再開いたしました。セミナーは主に中小企業の経営者やセキュリティ担当者の方々を対象に、サイバーセキュリティのリスクと、それを柔軟に乗り越えるための対策をお伝えすることを趣旨としました。アジェンダについては、これまでの内容を踏襲して進行しました。来場者からは高い評価をいただきましたが、今回は集客に苦労しました。スポンサー各社には大変申し訳なく思っております。コロナ禍以降、セミナー参加に対する行動様式が変化しているようで、次回の開催ではオンラインの開催も検討します。

なお、当日使用の資料はこちらからダウンロードいただけます。**https://www.jnsa.org/seminar/2024/cross/**

マーケティング部会としては、今後も啓発活動の一環として全国セミナーを開催する予定です。来年度以降は内容も一新し、新たな取り組みを実施してまいりますので、皆様のご協力をよろしくお願いいたします。

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. サイバーセキュリティアワード2025
主　催：デジタル政策フォーラム
日　程：2024年11月1日～2025年3月14日
会　場：Deloitte Tohmatsu Innovation Park

2. 第13回 情報セキュリティマネージャー ISACAカンファレンスin Tokyo
主　催：ISACA東京支部
日　程：2025年2月15日
会　場：オンライン

3. page2025
主　催：公益社団法人日本印刷技術協会
日　程：2025年2月19日～21日
会　場：サンシャインシティ・コンベンションセンター文化会館（東京都豊島区）

4. Data Center Japan 2025
主　催：特定非営利活動法人日本データセンター協会
日　程：2025年3月18日～19日
会　場：東京都立産業貿易センター浜松町館 4F・5F（東京都港区）

5. 自治体総合フェア2025
主　催：一般社団法人日本経営協会
日　程：2025年7月16日～18日
会　場：東京ビッグサイト（東京都江東区）

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

サイバーセキュリティベンダーの業界団体であるJNSAが、共助組織として社会に貢献するための各種活動を行っていく。

具体的には時事問題に対するタイムリーな情報発信や勉強会の開催、政府機関や関係団体とのパイプ役、政策提言、JNSAの主催するイベント等の企画支援などを推進する。

また今年度は、記者クラブとの連携をより一層強固に行うことで社会への情報発信力を強化していく。

【CISO支援WG】
（リーダー：髙橋正和 氏／株式会社Preferred Networks）

セキュリティ対策は、規準・規定といった監査的な視点と、セキュリティソリューションを中心に考えられてきたが、企業セキュリティの実務においては、セキュリティを担当するCISOの重要性が認識されるようになっている。

一方で、セキュリティ専門家に対しての知見は蓄積されているが、企業経営の一員としてのセキュリティ責任者という知見は、ほとんど蓄積されていない。

当ワーキンググループでは、CISOが必要とする知見にフォーカスし、これを支援するための活動を行う。

【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：古川英規 氏／株式会社RSコネクト）
（サブリーダー：酒井正幸 氏）
（サブリーダー：橋本光三郎 氏／株式会社ＨＧＣ情報セキュリティ研究所）

次を目的に検討会の定例開催を行い、活動する。

- 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

＜予定成果物＞

- 中小企業向けセキュリティガイドラインとベストプラクティス
- 中小機構E-SODAN向けセキュリティQ&Aコンテンツ
- セキュリティ補助金施策提言

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、期間あるいは目的を限定したタスクフォースを組織するなどして、柔軟かつ迅速な対応を行う

【セキュリティ市場調査WG】

（リーダー：玉川博之氏／
AKKODiSコンサルティング株式会社）

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。

＜予定成果物＞

- 2024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）

⑴ 人の意識や組織文化
⑵ 組織の行動が影響を受ける社会文化や規範
⑶ 不正・事故を防ぐシステム

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。

2024年度も引き続き、特に⑴に重点をおいた活動を行う。

ヒアリング先として、社会おける広義のセキュリティに関係している組織を積極的に開拓したい。

＜予定成果物＞

1. 「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記事の公開。
2. JNSA Pressへの寄稿、セミナー等への積極的出講による啓発活動の展開。

【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）

インシデントの被害組織に発生しうる、各種事故対応、アウトソーシング先、被害額等を調査・集計し、成果物としてまとめ、被害の大きさについて中小企業を中心とした経営者に知らしめ、国内の法人、組織のセキュリティ対策の向上を図る。

＜予定成果物＞

- 「インシデント損害額調査レポート（別紙）」
  2021年、2024年にリリースしたインシデント損害額調査レポート（本紙）の補足となる調査をまとめたレポートとして公開。

【データベースセキュリティWG】

＜2024年度より活動開始＞

（リーダー：大澤清吾 氏／日本オラクル株式会社）

「情報」は「人・モノ・カネ」に続く「第四の見えない経営資源」といわれ、近年はDXの推進やクラウドの普及、AIの発達等により、多くの企業が高度な技術とデータの活用を推進し、その情報を格納するデータベースの重要性はますます増している。

過去二十数年を振り返ると、外部からの不正アクセスに加えて、内部不正による情報漏洩事件は後を絶たず、ネットワークを中心とした境界防御型の対策だけでは防ぎきれない状況が伺える。また、昨今はランサムウェアの攻撃によって、バックアップデータの破壊、本番データの暗号化といった被害が発生し、事業継続に大きな影響を及ぼす事例も増えることで、従来の漏洩

対策である「機密性（Confidentiality）」の保護に加えて、事業継続のためには「可用性（Availability）」の保護も不可欠になってきている。

本WGでは、情報セキュリティの3要素である「可用性（Availability）」、「機密性（Confidentiality）」、「完全性（Integrity）」に求められる要素技術を中心としたデータベースのスタンダードな技術仕様、実践的な実装手法を検討するとともに「内部不正」、「クラウドセキュリティ」、「ランサムウェア」などに求められるデータの取扱い等に関する技術交流や調査研究を行う。

※2005年より任意団体「データベース・セキュリティ・コンソーシアム（DBSC）」として活動しておりましたが、更に活動範囲を広げるため、この度JNSAに合流いたしました。 調査研究部会のワーキンググループとして引き続き活動してまいります。

＜予定成果物＞

- データ及びデータベース管理に関するアンケート調査の結果報告書

【IoTセキュリティWG】

（リーダー：松岡正人 氏／
ブラック・ダック・ソフトウェア合同会社）

IoTに関連する技術動向についての調査研究および情報交換を行います。

【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、情報交換会（協働研究会）を介して、情報発信する。

【OTセキュリティWG】

＜2024年8月より活動開始＞

（リーダー：佐々木弘志 氏／
フォーティネットジャパン合同会社）

（サブリーダー：藤原健太 氏／
フォーティネットジャパン合同会社）

当WGの活動目的は以下の通りとなる。

（1）OTセキュリティ文化醸成のための調査・研究

（2）JNSA西日本支部工場セキュリティWGとの連携による取組み標準化

（3）AJCCA/JNSA活動支援窓口

【AIセキュリティWG】

（リーダー：服部祐一 氏／
株式会社セキュアサイクル）

近年のAIの目覚ましい進歩により、様々な分野でAIが活用されている。セキュリティ分野でもAIの利用が進んでおり、今後さらに広がると予想される。本WGでは、AIの利用におけるセキュリティおよびセキュリティ分野でのAIの活用について調査研究を行う。2024年度はその中でも生成AIのセキュリティに焦点を当て生成AIを活用していく上でのセキュリティの調査を行う。

＜予定成果物＞

- 生成AIのセキュリティに関するレポート

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：小川博久 氏／株式会社三菱総合研究所

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。さらに、近年のデジタル化促進にともなる技術要素についても積極的に取り上げ、標準化部会での技術共有や課題抽出を実施していく。

【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）

（サブリーダー：貞弘崇行 氏／
伊藤忠テクノソリューションズ株式会社）

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＞

- ロール管理解説書　改訂版

• ゼロトラスト環境におけるロール管理（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＞

• 長期署名プロファイル標準の制改定（JIS規格3件）
• 電子署名保証レベルに関するガイドライン

【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。

• ISMSの実装＆運用についての事例研究（下記の2テーマをユーザ視点で整理）
  - リスクアセスメントについて考える（フレームワーク含めた全体整理）
  - 委託先管理

【PKI相互運用技術WG】

（リーダー：伊藤忠彦　氏／セコム株式会社）

セミナーなどを開催し、デジタル社会におけるPKIおよびデジタルトラストの重要性をアピールしていくとともに、会員向けに勉強会なども開催する。

＜予定成果物＞

• セミナーイベント「PKI day」の開催
• 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SecBoK2024年更新版の作成・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。

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。

【SecBoK関連】

SecBoK2024更新版の作成、および使用事例などを盛り込んだ利用ガイド版作成などの活動を実施。

【辻井論文賞関連】

JNSAが、「辻井重男セキュリティ論文賞」の支援団体の1組織として、教育部会が代表して、運営委員会委員および査読委員として参画している。運営委員及び査読委員については、毎年複数名にご協力を頂いている。この活動は、若手セキュリティ研究者支援及び育成の一環として実施している。

＜予定成果物＞

• SecBoK改定委員会｜SecBoK2024
• 辻井論文賞関連｜表彰論文の選定、および講評など

【ゲーム教育WG 】

（リーダー：長谷川長一 氏／株式会社ラック）

サイバーセキュリティのボードゲームやカードゲーム、ゲーミフィケーション要素のあるイベントや教育などに関わる調査や企画、当WG制作の「セキュリティ専門家人狼」「Malware Containment」の普及プロモーションや講師派遣(主に大学・高専等の教育機関)、ゲーム教育のファシリテーター育成等を行う。

＜予定成果物＞

• 新作ゲーム教材「タイトル未定」及びファシリテーションマニュアル

【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、大学などでの講義の実践を通じて、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＞

- 情報セキュリティ講義の講義資料
- 中小企業向け情報セキュリティ講義の講義資料
- クラウドサービス セキュリティ 講義の演習
- 講師スキル育成のための手引き、育成資料、スキルチェックシートなど

【セキュ女WG】

（リーダー：北澤麻理子 氏／
エヌ・ティ・ティ・コムウェア株式会社）

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。

主な活動は以下のとおり。

- 女性のキャリア形成や仕事の進め方など、相談ができる場を提供
- 守秘義務を守りつつ、業務で得た疑問を話しあったり、他社の事例を紹介しあう場の提供
- セキュリティの仕事は幅広のため、他の人が従事している業務を知る機会を提供
- 仕事、育児、介護、自身の自由時間をどのようにマネジメントするかTipsを得るためのタイムマネジメントの情報交換を実施
- プレゼン経験を積むため全員がプレゼンターとなり、参加者全員からフィードバックをもらう会を実施
- ワーキンググループメンバーが講師の勉強会を開催
- 外部有識者の講演会を主催

【 教育部会産学連携プロジェクト 】

（リーダー：長谷川長一 氏／株式会社ラック）

JNSA教育部会と教育機関（大学、高専、専門学校等）との産学連携活動（主に学生向けの講座やイベント「セキュリティチャレンジスクール」「セキュリティカフェ」）の企画・運営、講師派遣による実施を行う。

実施にあたっては「SECCON」「JNSAインターンシップ」「「NICT CYNEX」「enPiT Security」「K-SEC」など、様々な学生向けイベントや活動、各団体とのより一層の連携を図っていく。

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の健全な発展に向けて貢献するため、会員向けのサービスとユーザ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。

ソリューションガイドサービスについては、社会活動部会の中小企業支援施策WGと連携し開発した中小企業のユーザ・会員にも利用しやすい新システムに移行した。必要に応じてブラッシュアップを行っていく。セキュリティ理解度チェックについては、新規問題の作成および古い問題の改訂・削除、そして利用者の増加に伴う安定的に運用可能な環境の整備強化を推進する。

また、こういったワーキンググループの活動とは別に、JNSA会員に対するオープンバッジの適用を検討する。

【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・問題やカテゴリの改修

【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。

全国でのセミナーを開催しセキュリティ啓発を諮るとともに、JNSAの認知向上、会員加盟社数増加に貢献した活動を行う。また、マーケティングに関連した勉強会を開催し、会員企業の知識向上を図る。またメディア研修会を開催する。

＜予定成果物＞

- 全国セミナーの企画・運営
- 勉強会の開催（年3回程度）

7．事業コンプライアンス部会

部会長：倉持浩明 氏／株式会社ラック
副部会長：唐沢勇輔 氏／
Japan Digital Design株式会社

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。また法令リスクについて実例を踏まえた情報交換や調査等を行う。

また今年度より各WGの活動を部会に統合して行う。

8．西日本支部

支部長：米澤美奈 氏／株式会社ソリトンシステムズ

西日本に拠点を置く会員組織が中心となり、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攻撃への対応/BCP対策の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して活動し、集大成となる「今すぐ実践できる工場セキュリティハンドブック・BCP対策編」のリリースをめざす。

＜予定成果物＞

- 今すぐ実践できる工場セキュリティハンドブック・BCP対策編
- 「NSF 2023 in Kansai」にて行ったワークショップのコンテンツ化

9．U40部会

部会長：永塚遼 氏／SCSK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：奥澤美穂 氏／株式会社Speee）

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。また、テーマについてはU40部会のメンバーから募ることも検討する。

【勉強会企画検討WG】

（リーダー：武田啓介 氏／株式会社信興テクノミスト）

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：三村聡志 氏／
GMOサイバーセキュリティ byイエラエ株式会社）

2023年度に引き続き、学生向けイベントや活動を教育部会産学連携プロジェクトと連携し実施する。社会人向けのイベントや活動の需要が出てきた際には、検討・企画を実施する。

10. 国際連携部会

部会長：伊藤整一 氏／株式会社大和研究所

2024年の部会は下記に2点に焦点を当て活動予定。

1) ASEAN協会（AJCCA）連携活動

ASEAN各協会・各政府・各国大学との連携構築とそれに伴うイベント・セミナーへの参加および参画・講演者の派遣を行うとともにJNSAのコンテンツのプロデュース・日本政府との関係強化を行う。また、国内外へのプロモーションを通じてJNSAの知名度向上、新規会員獲得、コンテンツの有効活用を目指す。

2) JNSAコンテンツのASEAN向けプロデュース

JNSAの所有するコンテンツで海外向けに通用するもの、ASEAN各国が興味を示すものを調査・選定し英文化したコンテンツをAJCCA各協会へ供給し日本ブランド（商品・サービス）の提供を目指す。

【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）

日本発のセキュリティサービスの海外進出支援および各社の情報共有をする。

＜予定成果物＞

・定例会による情報共有
・WGメンバーの海外イベント参加のレポーティング

11. 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を図るための活動を行うとともに、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活動、DX推進のための人材の育成や流動化促進などを実施する。

＜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）

12. 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事業を実施することによって、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環境実現に向けて寄与することを目的とする。

【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）

要求にマッチしたセキュリティ診断サービスを的確に効率よく選択できるように、ユーザ向けセキュリティ診断サービスの解説書を作成する。セキュリティ診断サービスを向上するために、サービスを提供している技術者のレベルを計ることが可能な指標について検討する。

【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／
GMOサイバーセキュリティbyイエラエ株式会社）

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）

セキュリティオペレーション事業者間の共通の課題の認識および、課題の対応や対処について検討を行い、必要に応じて成果物を外部への公開を行う。

＜予定成果物＞
- 各所での発表資料、JNSA全国セミナー発表資料

【12.5. 新技術とオペレーションPj】

各種技術トピックとセキュリティオペレーションに対する影響の調査

13. 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eシールガイド

14. 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インターンシップの推進支援を実施する。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」については、昨年度に引き続き東京会場の集合形式でのみ開催。本年は大阪、福岡での開催も検討する。

15. サイバーセキュリティ産学連携推進協議会

代表：大塚玲 氏／情報セキュリティ大学院大学

サイバーセキュリティ分野の産学連携活動を強化し、わが国のこの分野における研究開発/実務対応を強化することにより、わが国IT環境のセキュア化を図り、結果としてIT利用による社会/企業活動の活性化に繋げる。

16. ＳＥＣＣＯＮ実行委員会

実行委員長：三村聡志 氏／
GMOサイバーセキュリティ byイエラエ株式会社
副実行委員長：木藤圭亮氏／三菱電機株式会社
副実行委員長：花田智洋氏／
国立研究開発法人 情報通信研究機構

例年通り、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、年間を通して活動を行う。

イベントは、昨年同様にSECCON CTF、電脳会議、ワークショップ、CTF Biginners、CTF for Girls、地方での開催（2〜4か所）を行う。活動予算については、今年度協賛企業の協賛金にて賄う予定で前年度2023年度並みの協賛金収入を目標とする。

JNSA 役員一覧　2024 年 6 月 6 日現在

会　長　江崎　浩　（東京大学大学院情報理工学系研究科 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）
飯田　朝洋	（トレンドマイクロ株式会社）
梅野　　寛	（大日本印刷株式会社）
片澤　友浩	（ユニアデックス株式会社）
金澤　謙悟	（SBテクノロジー株式会社）
鴨田　浩明	（株式会社NTTデータ）
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）
倉持　浩明	（株式会社ラック）
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）
齋木　　啓	（日鉄ソリューションズ株式会社）
下田　秀一	（東芝デジタルソリューションズ株式会社）
平田　真一	（エヌ・ティ・ティ・アドバンステクノロジ株式会社）
丸山　司郎	（株式会社FFRIセキュリティ）
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）
与儀　大輔	（株式会社サイバージムジャパン）

幹　事（50音順）

有松　龍彦	（NECセキュリティ株式会社）
榎本　祐樹	（株式会社ディアイティ）
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）
神山　太朗	（あいおいニッセイ同和損害保険株式会社）
北澤麻理子	（エヌ・ティ・ティ・コムウェア株式会社）
倉持　浩明	（株式会社ラック）
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）
佐々木博文	（エヌ・ティ・ティ・アドバンステクノロジ株式会社）
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　直博	（SBテクノロジー株式会社）
関場　哲也	（株式会社カスペルスキー）
高橋　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）
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）
武藤　耕也	（グローバルセキュリティエキスパート株式会社）
本川　祐治	（株式会社日立システムズ）
山口　和利	（日本電気株式会社）
米澤　美奈	（株式会社ソリトンシステムズ）
綿貫　健志	（株式会社フーバーブレイン）

監　事

野村　文雄	（野村公認会計士事務所｜イースト国際税理士法人）

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 名誉教授）
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）
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 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）
松本　　泰	

事務局長

下村　正洋

会員企業一覧　2024年12月1日現在　294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）
アイティーエム（株）　New
（株）アイネス総合研究所
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）アイルミッション　New
アイレット（株）
アクセリア（株）　New
アクセンチュア（株）
（株）アクト　New
AKKODiSコンサルティング（株）
（株）アシスト
（株）AGEST
AZURE-PLUS（株）　New
（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）
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）
（株）アレクソン
アンカーテクノロジーズ（株）
アンテナハウス（株）
（株）AEGIS GATE　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）
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
インターネット セキュア サービス（株）
（株）インテック
インフォサイエンス（株）
インフォテック（株）　New
（株）エーアイセキュリティラボ
AOSデータ（株）
（株）HGC情報セキュリティ研究所
SCSK（株）
SCSKセキュリティ（株）　New
SGシステム（株）
SBテクノロジー（株）
NRIセキュアテクノロジーズ（株）
NECセキュリティ（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）
（株）エヌ・ティ・ティ エムイー　New
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）NTTデータ
（株）NTTデータグループ
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）FFRIセキュリティ
エフサステクノロジーズ（株）
エムオーテックス（株）
（株）エムティーアイ
（株）OSK
（株）大塚商会
（株）オープンストリーム
岡三情報システム（株）
沖電気工業（株）
オムロンソフトウェア（株）
ONWARD SECURITY JAPAN（株）

【か】

（株）カスペルスキー
兼松エレクトロニクス（株）
（株）ギブリー　New
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
クラウドストライク（同）
（株）クレスコ・デジタルテクノロジーズ
グローバルセキュリティエキスパート（株）
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）構造計画研究所
（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）
CompTIA日本支局

【さ】
サービス&セキュリティ(株)
ServiceNow Japan(同)
サイエンスパーク(株)
CyberArk Software(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
(株)サイバー創研
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
サイバーリーズン(同)
サイボウズ(株)
(株)CYLLENGE
(株)さくらケーシーエス
Sansan(株)
(株)シーイーシー
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)
GMOサイバーセキュリティ byイエラエ(株)
ジーブレイン(株)
(株)ジインズ New
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)
(株)ジオコード New
システム・エンジニアリング・ハウス(株)
システムワークスジャパン(株) New
(株)SHIFT
Japan Digital Design (株)
情報セキュリティ(株)
(株)信興テクノミスト
シンプレクス(株) New
ストーンビートセキュリティ(株)
(株)Speee
(株)スリーシェイク
セイコーソリューションズ(株)
(株)セキュアサイクル
(株)セキュアスカイ・テクノロジー
SecureNavi(株)
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)
ソニー(株)
(株)ソフトクリエイト
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)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)中電シーティーアイ
中部テレコミュニケーション(株)
(株)ChillStack
都築電気(株)
TIS(株)
(株)ディアイティ
(株)DXコンサルティング New
DNVビジネス・アシュアランス・ジャパン(株)
DBJデジタルソリューションズ(株)
テクマトリックス(株)
デジサート・ジャパン(同)
デジタルアーツ(株)
デジタルデータソリューション(株)
鉄道情報システム(株)
Tenable Network Security Japan(株)
(株)テリロジー New
デロイト トーマツ km2y(株)
デロイト トーマツサイバー(同)
学校法人電子学園
(株)電通総研
(株)電通総研セキュアソリューション
東京エレクトロン New
東京エレクトロン デバイス(株)
東京海上ディーアール(株)
(株)東芝
東芝ITサービス(株)
東芝デジタルソリューションズ(株)
TOPPANホールディングス(株)
(株)TRUSTDOCK
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)
一般財団法人日本情報経済社会推進協会
日本情報通信(株)
(株)日本総合研究所
日本タタ・コンサルタンシー・サービシズ(株) New
日本電気(株)
日本電信電話(株)
日本ビジネスシステムズ(株)
日本ヒューレットパッカード(同) New
日本マイクロソフト(株)

日本郵政(株)
ニュートラル(株)
ニューリジェンセキュリティ(株)
ネットワンシステムズ(株)
(株)ノートンライフロック

【は】

パーソルクロステクノロジー(株)
(株)バイオリンク
(株)パソナ
パナソニック(株)
パロアルトネットワークス(株)
ぴあ(株)
(株)PFU
PwCコンサルティング(同)
東日本電信電話(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)ファイブドライブ
(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)
富士通ディフェンス&ナショナルセキュリティ(株) New
富士フイルムビジネスイノベーション(株)
富士フイルムホールディングス(株)
(株)FRONTEO New
フューチャー(株)
BlackBerry Japan(株)
ブラック・ダック・ソフトウェア(同)
(株)Preferred Networks
(株)ブロードバンドセキュリティ
(株)ベリサーブ
ポールトゥウィン(株)

【ま】

(株)Maximax New
(株)マキナレコード
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)
(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)
三菱電機ソフトウエア(株)

【や】

(株)大和研究所
(株)ユービーセキュア
ユニアデックス(株)
(株)横浜銀行
(株)YONA

【ら】

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

【わ】

(株)ワイズ

【特別会員】

一般社団法人 IIOT
ISC2 Inc.
S/MIME推進協議会
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
サイバーセキュリティイニシアティブジャパン
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
順天堂大学 健康データサイエンス学部 New
一般社団法人 情報処理安全確保支援士会 New
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
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
東海大学情報通信学部 New
東京大学大学院 工学系研究科
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
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
モバイルコンピューティング推進コンソーシアム New

他2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。）

株式会社サイバーセキュリティクラウド　川崎　愛

皆様、はじめまして。株式会社サイバーセキュリティクラウド 経営企画部 広報の川崎愛と申します。この度、自己紹介の機会をいただき、大変光栄に思います。

当社、株式会社サイバーセキュリティクラウドは、WAFを中心に、脆弱性管理や診断サービス、そして昨年からはクラウドセキュリティ領域にもサービスを展開しています。サイバー攻撃がますます高度化していく中で、私たちは幅広いソリューションを通じてお客様のセキュリティを強化しています。私自身のミッションは、当社のサービスや業界自体をより多くの方々に知っていただき、サイバーセキュリティの重要性を社会全体に広めていくことです。

前職はIT業界とは全く異なるベビー用品メーカーで広報を担当しておりました。

学生時代は中学から大学までハンドボールをしておりました。最近はバチャータやバーレスクといったジャンルのダンスを趣味として楽しんでいます。これまでの経歴からみてもサイバーセキュリティとは離れた道を歩んできたことがお分かりいただけると思います(笑)。

広報職を極めたいという思いから、異なる分野に挑戦することを決めたのが転職のきっかけです。広報歴は9年になりますが、IT化が遅れていると言われていた業界であったため、現在のサイバーセキュリティ業界での広報業務は、毎日が新たな挑戦です。当社への入社も大きなチャレンジでしたが、やりがいを感じながら、広報という立場で会社や業界全体に貢献できることに喜びを感じています。

JNSAには、当社が2023年に加入し、私自身は2024年の春頃から社会活動部会、マーケティング部会、セキュ女などに参加させていただいております。まだお会いできていない方も多いですが、皆様と直接お話しできる機会を楽しみにしております。JNSAでの活動を通じて、長く業界に携わっていらっしゃる皆様から多くの学びを得ており、この貴重な環境に大変感謝しております。サイバーセキュリティについてはまだ勉強中の部分も多々ありますが、今後ともどうぞよろしくお願いいたします。

今後は、エンジニアが気軽に話せる場（LT会など）の企画や、セキュリティに特化したカジュアルなイベントの開催もできたらと考えております。ぜひ、皆様と一緒に業界を盛り上げていけたらと思いますので、お気軽にお声がけいただけましたら嬉しいです！今後ともどうぞ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。）

株式会社信興テクノミスト　武田　啓介

JNSA会員の皆さま、初めまして。株式会社信興テクノミストの武田と申します。
この度は、株式会社Speeeの奥澤さまよりバトンを受け取りまして、このようなご挨拶の機会を賜りました。誠にありがとうございます。

私は普段、自社にて「ABURIDA®（アブリダ）」というWebアプリケーションの脆弱性診断サービスに携わっています。
紙を火であぶることで文字を浮かび上がらせる遊び「あぶりだし」が「ABURIDA」の語源です。普段Webアプリを利用しているだけでは気付くことのできない脆弱性を疑似攻撃することによって見つけ出す、脆弱性診断と近しいものを感じるという理由から、今のサービス名に命名されました。少しでも多くの脆弱性を「あぶりだ」せるよう、日々業務にまい進しています。

さて、私はJNSAではU40部会の勉強会企画検討WGのリーダーとして、勉強会の企画をしています。
当WGでは会員同士の知識、スキル向上、人脈形成を目的とし、年に数回勉強会を実施しています。勉強会のテーマは、会員の方々からアンケートを募ることもあれば、最近のニュースからピックアップすることもあります。
直近で開催したテーマとしては「IoT機器におけるペネトレーションテストについて」「生成AIとセキュリティ」「OSINTについて知ってほしいこと」など、そのカテゴリは多岐にわたります。いい意味で何でもアリな勉強会となっていますので、もし開催してみたいテーマやお話を聞いてみたい講師の方などおりましたら、お気軽にお声がけください（勉強会への参加にはU40部会への参加が必要となります）。

少し個人的なお話もさせていただきますと、趣味でタップダンスをしています。映画などで老紳士が軽快にタップダンスをしているのを見たことがある方もいるかもしれませんが、長く続けられる趣味ですのでお勧めです。
また最近のマイブームは、おいしい麻婆豆腐のお店を探すことです。気になったお店があれば遠方でも赴きますので、お薦めのお店があればぜひ教えてください。辛いのもしびれるのも好きです！

最後に、まだまだ勉強中の身ではございますが、JNSA会員の皆さまやセキュリティ業界に少しでも貢献できるよう精進してまいりますので、今後ともどうぞよろしくお願いいたします。

JNSA　Webサイトのご案内

成果物・最新情報などはこちらからご覧ください

JNSAホームページ

最新情報は随時更新！
イベント情報などJNSAの今を知りたい方はこちらをご注目ください。
https://www.jnsa.org/

JNSAソリューションガイド

JNSA会員企業が扱う製品やサービス、イベント、セミナーなどを様々な条件から検索できるサイトです。
https://sg.jnsa.org/

サイバーインシデント緊急対応企業一覧

予期せぬサイバーインシデント被害、緊急で被害調査や被害切り分け、復旧などの対応を請け負ってくれる､頼りになるJNSA所属企業一覧です。
https://www.jnsa.org/emergency_response/

YouTube　JNSA Channel

サイバーセキュリティに関するセミナーの講演動画や、研究部会の成果物の紹介動画・サイバーセキュリティ職業紹介動画など様々な動画を公開しています。
https://www.youtube.com/@JNSAseminar/featured

JNSA Press(Web版)

JNSA Pressは　Webでもお読みいただけます。
バックナンバーも公開中です。ぜひご覧ください。
https://www.jnsa.org/jnsapress/

上記5つのおまとめQRコードはこちら→

自社のセキュリティ事業が**違法性**を問われないために

JNSA サイバーセキュリティ業務における倫理行動宣言

Declaration of Ethical Code for Cybersecurity Operations

JNSA会員限定

賛同企業募集

https://www.jnsa.org/cybersecurity_ethics/

JNSA では、各社の事業が正当に実施されており、サイバーセキュリティ関連業務に特有のコンプライアンスリスクを管理していることを社会や関係省庁に対して明らかにすることを目的として、「サイバーセキュリティ業務における倫理行動宣言」を策定しています。「サイバーセキュリティ業務における倫理行動宣言」に定義した「行動規範」および「事業遂行の基本指針」に則り、サイバーセキュリティ業務を遂行することを自己宣言していただく企業を募集しています。

活用のポイント・メリット

- 自社のセキュリティ事業が違法性を問われないために
- 継続的な事業として行っていることとして事業の正当性を宣言
- 安心してセキュリティ事業を提供していくために

自己宣言の要件

- 倫理行動宣言の「行動規範」の内容に、担当部門または会社として同意している。
- 倫理行動宣言の「事業遂行の基本方針」に示すリスク管理を行っている。
- （任意）Web サイトにおいて外部から見える形で自己宣言を行っている。

◆倫理行動宣言に御賛同いただいた企業名や事業部名をJNSAのWebサイトに掲載します。
JNSA事務局までご連絡ください。
※JNSA会員限定です

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
〒 105-0004 東京都港区新橋 5-7-12-4F
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.54

2025 年 1 月 1 日発行

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

〒105-0004 東京都港区新橋5-7-12-4F
E-mail: sec@jnsa.org　URL: https://www.jnsa.org/