情報セキュリティ監査制度
創設20周年 記念誌

特定非営利活動法人
日本セキュリティ監査協会

目次

第 1 章　発刊によせて

情報セキュリティ監査制度　20 周年にあたって

特定非営利活動法人 日本セキュリティ監査協会

会長

手塚　悟

情報セキュリティ監査制度は 2003 年 4 月 1 日に経済産業省により施行され、今年で創設 20 周年を迎えました。この記念すべき 20 年という節目の年を迎えることができましたのも、制度創設以来ご協力いただいた政府機関の皆様、会員企業の皆様、関係団体、その他関係の方々のご指導、ご鞭撻のおかげであり、心より感謝申し上げます。

また、制度施行から約半年後の 10 月 10 日に設立された特定非営利活動法人日本セキュリティ監査協会が、各分野の専門家の皆様の協力に支えられながら現在まで制度の運営に携わってきました。初期には情報セキュリティ監査人認定制度の策定や監査人の行動指針など人材育成の基盤作り、各分野への制度の地道な普及促進に努めました。

その後、クラウドサービス利用が本格化した 2012 年には、クラウド情報セキュリティ監査制度を創設し、CS マークの認定事業を開始しました。その 5 年後に、監査の経験を生かして情報セキュリティサービス審査登録制度における審査機関としての活動を開始することで、協会活動の基盤を形成することができました。さらにその 2 年度には CS マークの認定において培った経験を元にした ISMAP での監査機関の審査業務を受託することで、情報セキュリティ監査制度が政府機関の情報セキュリティに生かされることとなりました。

これらの成果は、協会活動を支える幅広い分野の有識者、情報セキュリティ分野の専門家、監査人など、様々の方々のご協力、ご支援により実現したものであり、あらためて御礼申し上げます。

さて、昨今ではランサムウェアをはじめとするサイバー攻撃による大きな被害が生じており、対策の強化が喫緊の課題になっています。今後、新型コロナウィルス蔓延による働き方の急激な変化や AI などの技術変化など、想像できないような新たな時代が我々を待ち構えているはずです。このような変化に情報セキュリティ監査制度も柔軟に対応し、安全で安心な社会を維持・発展するために、その役割を果たしていくことが求められます。

制度発足 20 年目という節目を機に、関係者の皆様と共に決意を新たにし、より安全な情報社会の実現に向けて、取り組んでいきたいと思います。今後とも、なにとぞご支援ご愛顧を賜りますようお願い申し上げます。

２０年のあゆみ

2003年4月に経済産業省は情報セキュリティ監査基準、同管理基準及び情報セキュリティ監査企業台帳に関する告示を行った。この告示により情報セキュリティ監査制度がスタートした。

告示に先立つ2002年8月に情報セキュリティ監査のあり方を検討するために、土居範久慶應義塾大学教授を主査とする情報セキュリティ監査研究会が、経済産業省商務情報局長の諮問機関として設置された。この研究会において、監査法人、IT企業のセキュリティ専門家などが情報セキュリティ監査制度の具体化に向けて議論を重ねた成果が、告示として公開されたものである。

制度を運営するための団体として特定非営利活動法人日本セキュリティ監査協会（JASA）が発足したのは、半年後の2003年10月である。研究会の主査であった土居教授が会長に就任され、その下に、監査を実施する監査企業と監査を利用する一般企業が集い、よりよい監査の実現のために集結した。

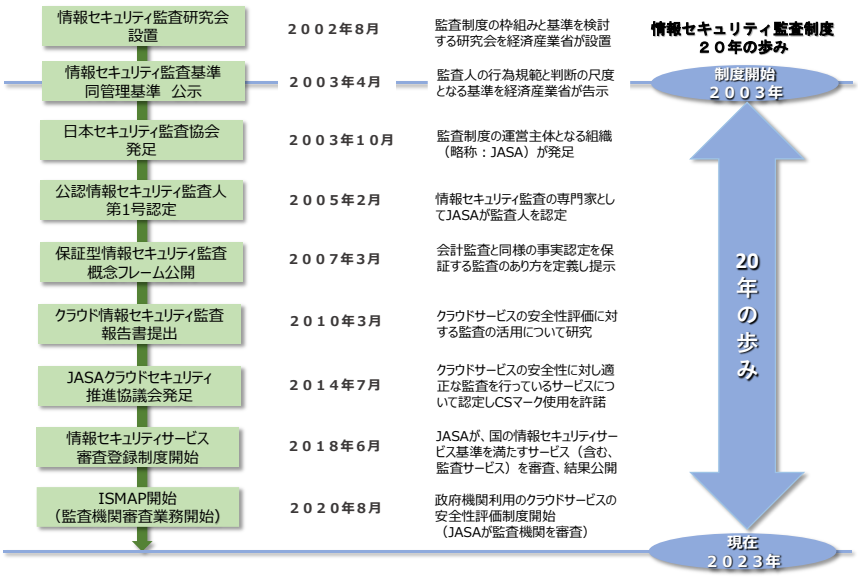
JASAは発足後に制度運営に必要な様々な事項を処理すると共に、制度を社会に認知させ、普及するための活動を行った。特に注力したのが情報セキュリティ監査人の育成である。公認情報セキュリティ監査人資格制度を整備し、研修・トレーニングを提供する事業を行い、設立1年半弱で第1号の監査人の認定を行った。

また、監査により情報セキュリティを保証する方法について実証を含めて研究し、2007年に保証型情報セキュリティ監査のフレームワークを公開した。保証型情報セキュリティ監査の品質である公平性を担保するための審査機能を担う審査委員会は、フレームワーク公開に先立つ2004年4月である。これらの一連の成果で情報セキュリティ監査制度の運営の基礎ができ上がった。

情報セキュリティ監査制度の応用として、近年急速に利用が拡大しているクラウドに対する情報セキュリティ監査がある。制度の基礎ができた頃からこの点を研究し、2010年にクラウド情報セキュリティ監査に関する報告書を経済産業省に提出した。これを踏まえたクラウド情報セキュリティ監査制度を運営するために、JASAの下部組織としてJASAクラウドセキュリティ推進協議会を2014年に設立した。この協議会にはクラウド事業者と監査企業が参加し、クラウド利用者のセキュリティに対する不安解消を行うためにクラウド事業者が行うべき適切な監査定義し、それを認定するクラウドセキュリティマーク（CSマーク）の使用許諾を行っている。

情報セキュリティ監査人の資格認定やCSマークの審査の経験を活かし、2018年には経済産業省が開始した情報セキュリティサービス審査登録制度の審査機関としての役割も担うようになった。この制度は、当初、情報セキュリティ監査サービス、脆弱性検査サービス、デジタルフォレンジックサービス、セキュリティ監視・運用サービスを対象として開始され、2023年度に機器検証サービスの追加により、現在５サービスを審査している。

さらに、CSマーク審査の経験を活かし、2020年には政府機関のクラウドサービスの安全性を評価するISMAPにおいて審査機関を審査する役割を担っている。制度開始から20年を経て、情報セキュリティ監査制度は社会に深く根付くようになってきた。



寄稿文

情報セキュリティ監査制度の 20 周年に寄せて

織茂　昌之 様

公認情報セキュリティ
主席監査人

【情報セキュリティ監査制度との関わり】

日本セキュリティ監査協会スキル部会のワーキンググループリーダとして情報セキュリティ監査人資格制度立上げに関わり、その後、試験小委員会委員長（～2015年）、資格認定委員会委員として監査人資格制度に継続して関わってきました。

日本セキュリティ監査協会（JASA）との関わり

情報セキュリティ監査制度20周年についての寄稿ということですが、私は、日本セキュリティ監査協会（JASA）の活動を通じて情報セキュリティ監査制度に関わってきましたので、JASA活動との関わりについて書いてみたいと思います。

勤務していた企業にて、2002年頃よりISMS構築支援など情報セキュリティマネジメントに関わりだしましたが、組織の情報セキュリティマネジメント実施状況をどう客観的に評価できるのかというモヤモヤとした思いを持っていました。2003年に情報セキュリティ監査制度開始の話を見つけて、これだと思って、この制度の運営体として設立されるJASAへの参加を勤務先に提案し承諾いただき、言い出しっぺということで私がJASAの会合などに参加するようになりました。これが、私がJASA活動に関わるようになったきっかけでした。

あらためてJASAホームページを見てみると、活動内容として次の3項目が記載されています。

1. 情報セキュリティ監査制度の普及促進
2. 情報セキュリティ監査人の育成
3. 情報セキュリティサービスの審査

私はこれら3項目の中の「2.情報セキュリティ監査人の育成」、特に監査人資格制度に関わってきました。印象に残っているのが、監査人資格制度の制度設計や運用立ち上げに関われたことです。企業に勤めていた私にとっては新鮮で企業内では得難い経験ができ、この経験により自分の幅を広げることができたのではないかと、後から振り返って勝手に思っています。このような経験の場を与えてくれたJASAには感謝しています。

再びJASAホームページによれば、2003年4月1日に「情報セキュリティ監査制度」が施行され、その制度を着実に浸透させていく為の運営体としてJASAが設立されたのが2003年10月10日とのことです。

監査人資格制度は確か2005年に運用開始されたと思いますので、JASA設立から2年足らずで資格制度が立ち上がったわけです。資格制度立ち上げ検討の主体となったJASAスキル部会の方々やJASA事務局の方々と、私もスキル部会の一員として夜遅くまでJASAの会議室でいろいろと検討や議論したことが思い出されます。

資格制度の運用開始に先立って、資格認定のための試験問題の作成やその採点基準・採点方法などの整備が必要で、このためにJASA内に設置された試験小委員会で、これも夜遅くまで議論したことも思いだされます。私はこの小委員会の委員長として携わりましたが、小委員会委員の方々の、これから必ず求められる新しい資格という認識のもとでその実現に向けて真剣かつ熱心に取り組んでいただく姿勢にとても心強く思い、皆さんの真摯な活動により資格試験を軌道に乗せることができて安堵したことを覚えています。

なお、私は直接関わっておりませんでしたが、監査人資格取得に向けた研修及びトレーニングの整備も必須であり、研修やトレーニングのテキスト作成、講

師の育成などを担う研修・トレーニング小委員会も設置され、この小委員会委員の方々も同じように精力的に活動されていました。

監査人資格制度は継続して運用されていますので、当然ですが、試験小委員会、研修・トレーニング小委員会の方々は制度運用のために精力的に活動を継続されており、監査人資格制度の屋台骨を支えておられます。

また、資格の認定を行う資格認定委員会では、資格の認定だけでなく、監査人資格制度の運用状況をモニタリングし制度改善を行うなどのPDCAサイクルが回されています。

これら委員会の活動とその活動を支えていただいているJASA事務局、また、関連する様々な方々のご尽力により監査人資格制度が運用されていることを、今回の寄稿を執筆しながら改めて感じ入った次第です。

寄稿と言いながら、自分の経験の振り返りという個人的な内容になってしまい恐縮です。情報セキュリティ監査制度の普及・発展に向け、微力ではありますが、引き続きJASA活動に協力してゆきたいと考えております。

永宮　直史 様

特定非営利活動法人
日本セキュイティ監査協会
エグゼクティブフェロー

これまでの20年と、そしてこれからの20年へ

情報セキュリティ監査制度に係ったのは、制度創設翌年の冬だったと記憶している。それからほぼ20年間、多くの方々のご支援とご協力を得て、本制度は日本の情報セキュリティの向上に資することができた。まずは、これら多くの方々に感謝を申し上げたい。

制度創設からかなりの期間、日本セキュリティ監査協会（JASA）には30代から60代の見識豊かな人々が集い、熱気が溢れていた。皆がボランティアとしてWGや委員会に参加し、その場での議論は深夜に及ぶことが度々あった。その熱気は制度創設から５年を経た保証型情報セキュリティ監査プロジェクトで最高潮に達した。

しかし、残念ながら保証型情報セキュリティ監査を広く普及することはできなかった。情報セキュリティ監査への熱気が冷めはじめた2010年に、縁があってJASA の事務局長を引き受けた。最初に手掛けたのは経営引き締めである。会員数の減少や公認情報セキュリティ監査人認定者数の伸び悩みから、経営が厳しくなり、事務局員を削減せざるを得ない。事務所を会員企業事務所の一部に間借りした上で、さらに様々な無形の支援を得なければならなかった。

一方で、2009年に着手したクラウド情報セキュリティ監査研究の成果を踏まえてISO/ IEC 27017編集に携わることになった。これが幸いし、規格発効前の2013年にJASA-クラウドセキュリティ推進協議会（以下、「協議会」）を発足し、CSマークを発行することができた。このニュースはNHKなどで報道された。その結果、情報セキュリティ監査制度が再び注目され、会員数も増加に転じるなど、明るい兆しが

見えたのである。

さらに幸運なことに、2018年に情報セキュリティサービス審査制度が開始され、審査機関としての事業がJASAに加わった。ただし、情報セキュリティサービス基準告示後、パイロット事業を４か月で終え、登録開始をしなければならないという条件が付いていた。事務局員は私を含めて4名しかいない。通常業務で手一杯の状態の中で、人員の採用もままならない状態だったが、幸いにもこの条件をクリアすることができた。

その後、ISMAP制度が開始され、監査機関の審査業務を国から受託することができた。これはISMAP制度の設計にCSマーク制度の経験をいかすことができたことが貢献した。クラウド情報セキュリティ監査の研究開始から10年、人々の努力の結果がようやく実ったのだ。そして、このことはJASAの経営にも良い効果をもたらした。

情報セキュリティからサイバーセキュリティへ、あるいはDX からシンギュラリティの時代へと、時代は大きく変化している。この変化に監査も対応しなければならない。今、JASA に集う人々は、20 年前と同じように 30 代から 60 代前半である。これらの人々が、情報セキュリティ監査の新たな 20 年を拓いてくれることを期待している。

水野　義嗣 様

情報の安全･安心研究所

日本に情報セキュリティ監査制度が導入されてから20年にもなるのですね。

私は約25年前から情報セキュリティ国際規格のISO/IEC 17799：2000（JIS X 5080：2002）委員、現在のISO/IEC Q 27001（JIS Q 27001）の委員を担当していた関係で、その当時の経済産業省の「情報セキュリティ監査研究会委員」に任命され、国内に情報セキュリティ監査制度を導入するための協議を行いました。委員会の終了時に情報セキュリティ監査制度を国内に普及させるため、NPO法人組織の発起人の一人になりました。この組織が皆さんのご協力でJASAとなり、設立後約10年以上もこの制度を普及させるための普及促進部会の部会長を担当しました。この部会に参加いただいた皆さんと一緒に監査制度のいろいろな普及促進活動を行いましたが、情報セキュリティに関する理解者も少ない中、その監査制度の普及は大変難しく、大変だったとの思いがあります。

20年前の多少の記憶をお話しすると、県や市町村などから情報セキュリティ監査の協力依頼等に出かけてゆくと、責任者から監査結果の指摘をしないように言われることが多くありました。その中で監査協力をしていた市長が交代してから、急に積極的に指摘するようにとの指示があって、びっくりしました。その市長が今は県知事なので、個人的には少しでも情報セキュリティ監査の普及に協力することができたとの思いが残っています。

JASA 普及促進部会時の執筆本
（18 年前）

日本セキュリティ監査協会 (JASA)立ち上げ時の普及促進部会のメンバー10名が協力して「情報の安全安心研究会」と称し、「50のキーワードで知る情報資産とセキュリティ管理」を執筆し、皆さんに参考にしてもらうために出版しました。この時の協力者により全国の図書館にも多少の配布をしてもらえたので、今もこの本の存在が図書館で確認することができます。この情報セキュリティ管理・監査のための情報について、監査関係者から今も「あの本を参考にしているよ」との連絡を受けることがあり、執筆者の一人としてとてもうれしく思っています。

JASA普及促進部会退任後は個人情報保護も含めた情報セキュリティ関連の各種ボランティア活動を行ってきましたが、少しでも情報セキュリティにお役に立ちたいとの思いがあり、可能な限り継続したいと思っています。

丸山　満彦 様

PwCコンサルティング合同会社　パートナー、情報セキュリティ大学院大学 客員教授
公認会計士

【情報セキュリティ監査制度との関わり】

経済産業省の情報セキュリティ監査研究会委員。監査基準、管理基準のドラフティングを行う。また、その後、NPO情報セキュリティ監査人協会の設立に関与。NPOの技術部会、監査人資格認定委員を歴任。資格認定委員は現在も継続している。

実務と理論の協調的発展を期待して

2002年に経済産業省で情報セキュリティ監査についての委員会が立ち上がり、私もその委員となりました。私にとっては、初めての政府委員でした。委員の中では比較的若手だったこと、公認会計士であり、かつ上司の影響で米国の保証基準の勉強をしていたこと、ISMS制度の立ち上げも行っており、当時の情報セキュリティマネジメントの管理基準にも知見があったこともあり、情報セキュリティ監査基準、情報セキュリティ管理基準の作成に経済産業省の若手課長補佐たちと共にドラフティングから行いました。また、その後の情報セキュリティ監査制度のためのNPOの立ち上げ、NPOにおける技術部会で、監査実施基準の改訂やガイドライン等の策定を試みようとしましたが、その大部分は実現しませんでした。

一方、経済産業省の情報セキュリティ戦略委員会の委員になり、その報告書を受けて、政府は内閣官房情報セキュリティセンター（現在のサイバーセキュリティセンター）の設立を行うわけですが、その設立、設立後に政府統一基準の策定、とりわけ自主点検・監査の部分に携わることになりました。情報セキュリティ監査制度があったので、それをベースに比較的理解が得やすかったと言うこともあります。

そんな制度立ち上げから20年が経とうとしていま

す。その間、情報セキュリティ監査人制度のもと2023年7月12日現在、主任監査人44名、監査人159名、監査人補680名、監査アソシエイト398名、計1,281名の監査人等が登録されています。組織のITへの依存度の高まり、情報という無形資産の価値の高まり、サプライチェーンへの依存度の高まり等、組織における情報セキュリティの重要性はますます高まることが想定されます。情報セキュリティ監査人へのニーズも高まっていくことでしょう。そこで、このような現状を踏まえた上で、情報セキュリティ監査制度というものは、今後どのようになっていくべきなのかということを考えてみたいと思います。

まず私は、情報セキュリティ監査のビジネスニーズについての心配はあまりしていません。上記のとおり、情報システム、ネットワークへの依存度の高まりと、攻撃の高度化という流れがあるからです。むしろ心配しているのは、監査の品質です。といっても、今に不満があるわけではありません。これからの話です。監査の品質は、監査人の質、監査業務管理の質、そして、監査をする組織の管理の質に大きな影響を受けます。その中でもとりわけ、監査人の質を上げることが重要でしょう。

情報セキュリティ技術というのは、日々進歩しています。また、サイバー攻撃手法も日々進歩しています。この技術や状況変化が激しい中、監査人がそれに追随、あるいは先回りをして対応しつづけられるのか？というのが、重要な課題だろうと思います。監査人協会でも、そのための教育等に力をいれていますが、監査人向けのより重層的な教育プログラムが必要なのではないかと思っています。そのためには、情報セキュリティ監査人のためのスキル標準のようなもの、そして、それを裏付ける理論というものが重要となってくるのではないかと思っています。

情報セキュリティ技術については、さまざまな研修プログラムがありますので、必要に応じて既存のものを利用したり、アレンジして利用すればよいでしょう。一方、監査についての研修プログラムが不十分ではないかと考えています。その背景には、やはり情報セキュリティ監査についての理論的な整理が、協会としてもできていないというところにあるのではないかと思っています。監査制度ができてから、20年近くになります。その間に、世界的には、ISO/IEC 27001に基づく情報セキュリティマネジメントシステムの認証制度も広く普及しました。米国ではFedRAMPといったクラウドの監査の制度が普及していたり、NIST SP800-53A、SP800-171Aといった監査あるいは評価のためのガイダンスが発行、更新されていたりします。また、日本でも、FedRAMPに類似をしたISMAPという制度もできています。公認会計士の世界では、WebTrsut、SysTrustといわれていたものは普及せず、認証局の監査という限られた分野のみになっています。一時は住民基本台帳ネットワークシステムについての監査をしていましたが、それも今は無くなっています。

市場のニーズや期待をもう一度整理し、社会に真に求められる情報セキュリティ監査像を整理し、必要な理論の整理を行い、監査人のスキル標準のようなものを整備し、人材の育成が効率的、効果的にできる体制をつくることが肝要ではないかと思料しています。

これから、情報セキュリティ監査制度を担っていくであろう若い人々による、幅広い分野の人との交流を通じた、積極的な議論を通じて、これらを実現していけば良いのではないかと思っております。もちろん、私もできるところはお手伝いしたいとは思います。

岸　泰弘 様

PwCジャパン合同会社 顧問
公認情報セキュリティ主席監査人

この度は、情報セキュリティ監査制度の制定20周年おめでとうございます。

私は制度が制定され、貴協会が設立された当初から普及促進部会に所属し、制度の普及に関わってまいりました。

その間、特に設立当初の事務局長であった故沓澤様には大変お世話になり、その後も後任の永宮様の大いなるご支援を頂きつつ、主に情報セキュリティ監査市場調査を担当しております。活動はワーキンググループという形で多くの会員企業の方々のボランティアで行っており、アンケートを主体とした情報セキュリティ監査の普及状況についての調査が主体となっています。

サイバーセキュリティの重要性が増している昨今、当制度が担う役割は制定時よりさらに大きくなっていると感じており、貴法人の今後の発展を心より期待しております。

和貝　享介 様

和貝公認会計士事務所、特定非営利活動法人日本セキュリティ監査協会 技術部会　部会長

【情報セキュリティ監査制度との関わり】

経済産業省「情報セキュリティ監査研究会(2002年)」メンバー。日本セキュリティ監査協会(JASA)設立発起人の一人。協会では副会長、技術部長(現任)として、情報セキュリティ監査制度の普及に務める。情報セキュリティ主席監査人。

情報セキュリティ監査制度とこれから

Ⅰ.始まりのころ

情報セキュリティ監査制度開始20周年、おめでとうございます。

関係者の一人として、お祝い申し上げるとともに、20年も経ったんだなという感慨もあります。制度の発足に向かい、また日本セキュリティ監査協会(以下、「協会」という。)の設立を目指して、夕方皆さんで集まって活動していた頃を懐かしく思い出します。その中には発足を待たず海外に異動された方などもいらっしゃいます。現在も活躍されている方々も多くいらっしゃいますが、故人となられた方もいらしゃいます。

私は協会では技術部長を拝命し、主に監査手続・監査手法を推進してきましたが、当初黎明期といいますか、協会発足当時は、部会に参加された方々は、情報セキュリティの専門家ではいらっしゃいましたが、監査についてはほとんどご存じなく、助言型監査と保証型監査の違いや、監査は証拠に基づく現在以前の過去の確定事項を対象とし、将来のことは対象外であるなどと、今日では常識となっていることをお話し、それを皆さんが熱心に聞かれていたことを思い出します。

Ⅱ.これからの制度に思うこと

さて、過去のお話はこれくらいにして、これからのことを考えてみましょう。

- 助言型監査からの脱皮

現在実施されている情報セキュリティ監査のほとんどは助言型監査です。監査目的に従って情報セキュリティ管理基準等一定の基準に照らして、監査対象の管理の仕組みについて検討し、その未整備、不備等を指摘し、必要な助言をする監査のことですが、よく考えると少し奇妙です。

多くの組織は、助言型監査を受け、監査報告書を受領して改善を行っています。つまり基準通りに管理の仕組みを構成・運用できていない、そして、できていないということを承知で監査を受け、できていないことの指摘を受けているということでしょうか。あるいはできていないことに気づいていないということかもしれません。しかし、確立された基準が存在しているのですから、それに従うのが道理であり、もし基準の内容の理解が不十分で対応できないのであれば、それについて、まずは理解し、あるいは指導を受け全うするのが当然ではないでしょうか。

少し厳しい言い方になりますが、法治国家において守るべき法律が定められているのに、平気で違反しているようなことではないでしょうか。助言型監査を受けて初めて違反を指摘されることは、よい方向ではないように考えます。準備のできていない管理体制等の助言型監査を受けてしまうのは順番が違うような気がします。情報セキュリティ管理基準のような範が示されているのですから、まずは組織自身が整備に努めるべきではないでしょうか。そのために内部監査はたいへん有効です。

- 内部監査の充実

組織は管理体制等の充実にもっと内部監査を活用すべきと考えます。

被監査部門との独立性を確立できれば、外部に依頼するのではなく組織内の内部監査人が監査することが望ましいと考えます。管理体制の整備状況については被監査部門自身の確認でも十分に判断できますか、特に内部監査に求められるのは仕組みの運用の継続です。被監査部門が運用状況を判定するには、どうしても客観性の点で劣ります。そこで独立した内部監査部門による監査が期待されるのです。

内部監査の活動で相当程度の情報セキュリティ水準を保った管理体制の確立は可能と想定します。そのための内部監査人の能力も要求され、今後とも協会の内部監査人資格者の増強と能力の充実のための諸施策が望まれます。また、組織に所要の内部監査人の設置を促すような制度の必要性も検討されるべきでしょう。

- 保証型の外部監査制度

上記(1)、(2)を考慮し、また、情報セキュリティが組織自身を保護するとともに、広く社会的な情報セキュリティ事故等による被害の最小化を目的とする、保証型の外部監査制度の設置が必要です。(1)に述べたような組織のように情報セキュリティ水準が高く、(2)の内部監査で相当程度これを保つ組織において、社会的要請としての保証型監査を志向すべきと考えます。堅く守られた体制を、客観的に保証し、組織と共にある社会生活の安心、安全が保護されます。これは、広く社会的損失を減ずるとともに、組織自身の活動の信頼性を増すことになります。

保証型監査制度の実践については、現行の監査基準に加えてより詳細・具体的な保証型監査のための監査プロセス、監査手続等を定めた補足規定等の準備も必須でしょう。

- 監査人の在り方

保証型監査を推進するに当たっては、監査人の在り方が肝要です。現在広く行われている助言型監査の知見・経験に加えて、保証型監査の能力の保持が必要となります。保証型監査制度については、米国公認会計士協会、日本公認会計士協会の下、実施されているSOC2、SOC3等の類似保証サービスがあります。監査人の在り方についても、これら制度が一部参考になります。助言型監査に比べ、監査人の実施する監査手続の厳密性、意見形成

の過程の複雑性等がかなり異なるとともに、法的な内容も含めた監査人の責任の比重についての認識に関する、検討と周知が大きなカギと考えますが、これらを克服しても保証型情報セキュリティ監査を実施できる監査人の制度を是非とも確立すべきです。

- 監査技術の推進

統計理論に基づき統計学で利用されていた統計的サンプリングを会計監査で利用したことはたいへん画期的でしたが、これが広く認知され内部統制の検証にも活用されるところとなり、さらに情報セキュリティ監査にも応用されています。このように学際的、業際的に利用できる技術は、今後とも発現してくるでしょう。役立つものを発見し、応用推進することは誰もができることではなく、誰かが実施できるものであると私見します。

その誰かが、広く世に示し問うことができるような仕組みは、例えば協会などで準備できないでしょうか。小さな発見から大きな実験・研究の手記、論文等を広く募集し、発表できる場の提供ということです。一定のインセンティブを考慮してもよいかとも考えます。誰もが、遠慮や躊躇なく自由に提言・寄稿できるサロンが理想です。

- グローバルとの対話

日本の情報セキュリティ監査制度の国際化はこれからでしょうか。アジア諸国はもちろん欧米の関連団体との関係を築くことが日本の今後の情報セキュリティ監査制度の発展に大きく貢献すると考えます。例えば協会が、経済産業省の支援をいただきながら、世界協調、世界発信を進めていってください。翻訳や通訳などを要すれば、そのための有用なツールがたくさんあります。日本の知見と世界の知見との融合はこれからの情報セキュリティ監査制度の大きな力となるでしょう。

以上、思うところを述べました。少し辛口のところ、私の理解不足による誤り等多々あるかと思いますが、制度20周年のお祝いの機会に免じて、ご容赦ください。

大木 榮二郎 様

工学院大学名誉教授
公認情報セキュリティ主席監査人

【情報セキュリティ監査制度との関わり】

経産省の研究会に参加し、JASAの基本的な制度設計に参画、監査人スキルの検討や資格制度の確立に貢献、保証型情報セキュリティ監査促進プロジェクトリーダーを務めるなど、折に触れ制度の運用にかかわってきた。現在、JASA-クラウドセキュリティ推進協議会会長。

曲がり角にある情報セキュリティ監査制度

２０周年とは遥かなる時間の経過である。昔から１０年ひと昔というから、もう二昔前のことになるし、最近は５年でひと昔と認識する人が主流らしいから４昔前ということにもなる。さらに変化の急なIT業界においてはDog Yearなる言い方もあり１年が７年に匹敵するともいわれ、そのスピード感覚でいえば、すでに１世紀半近くが経過したことにもなる。それだけの時間が経過したにもかかわらず、情報セキュリティ監査制度はほぼ立ち上げ当時の形で現在も運営されているのは奇跡的であるとも言えよう。その間制度の運営にかかわってこられた方々の苦労と努力に深く敬意を抱くところである。そのうえで、制度の曲がり角について考えてみたい。

情報セキュリティ監査制度は、会計監査の枠組みを基礎に助言型監査を主眼にスタートした。助言型監査等を通じて情報セキュリティマネジメントのレベルが向上するにつれて保証型の情報セキュリティ監査のニーズが高まるものと位置づけられ、その時点では情報セキュリティ監査における保証の概念は真剣には検討されていない。組織責任者がセキュリティマネジメントに取り組む際の確認手段としての監査の活用を意図して、主として内部監査に用いられる助言型

監査の普及を目的としたのは、セキュリティマネジメントの黎明期としては当然の選択であったといえる。

この制度開始から２０年が経過した今、デジタル化が多様に進化し、政府機関のみならずあらゆる企業や組織において、事業活動がデジタルシステムやサービスの安定稼働への依存を深めており、情報セキュリティの確保は社会全体の大きな課題となっている。その典型例がクラウドサービスの安全性評価に現れており、JASAにて取り組んだCSマーク制度、さらには政府のISMAPなどにおいて、情報セキュリティ監査が安全性確認の中核に位置づけられている。また、今後社会インフラ機能を担当する企業等においても、セキュリティマネジメントの適格性を監査において確認する仕組みが導入される方向になるであろう。保証型情報セキュリティ監査への要請が社会的に高まってきたと言えるが、その中心にあるとも言えるISMAPの監査は残念ながら保証型情報セキュリティ監査ではない。「ISMAP情報セキュリティ監査ガイドライン」に記載されている「本制度における監査業務の特質」には以下のように記載されている。少々長いが原文を引用する。

「本制度における監査業務は、*ISMAP* 運営委員会が行う *ISMAP* 等クラウドサービスリストの登録審査において、登録審査の対象となるクラウドサービスに関して、*ISMAP* 管理基準に基づいた情報セキュリティに係る内部統制の整備及び運用の状況を確認するために、クラウドサービス事業者の依頼に基づいて、監査機関が情報セキュリティ監査基準等に準拠して手続を実施し、その結果を事実に即して報告することを目的としている。業務実施者が作成した実施結果報告書は、サービス登録申請書の添付資料としてクラウドサービス事業者によって *ISMAP* 運営委員会に提出され、*ISMAP* 等クラウドサービスリストへの登録審査を行う際に参照する資料として利用される。

このため、本制度の監査業務において、業務実施者の報告は、手続実施結果を事実に即して報告するのみにとどまり、手続実施結果から導かれる結論の報告も、保証も提供しない。また、本制度における監査業務は、結論の基礎となる十分かつ適切な証拠を入手することを目的とはしておらず、保証業務とはその性質を異にするものである。さらに、業務実施者は、本制度における監査業務において、重要性の概念の適用やリスク評価に基づく手続の決定は行わず、また、業務実施者の報告に基づき実施結果報告書の利用者が不適切な結論を導くリスクの評価は行わず、実施した手続や入手した証拠の十分性についても評価しない。」

このように、ISMAPにおける監査機関の業務が手続実施結果を事実に即して報告するのみにとどまり保証業務とはその性質を異にするものであるとの位置づけにしたのは、監査機関の重要なプレーヤーである監査法人に配慮したものであることは明らかである。金融庁の企業会計審議会による「財務情報等に係る保証業務の概念的枠組みに関する意見書」は、監査法人が行う保証業務について、財務情報等に係る保証業務に関する概念整理を行うことを主たる目的としているが、「本意見書に示された概念的枠組みは、財務情報以外の事項を対象とする保証業務にも援用する」と明記されており、監査法人が提供する情報セキュリティ監査において、保証意見を出すとすれば、財務情報等に係る保証業務に関する概念整理に従わなければならないことになっている。

なお、クラウドサービスのような外部サービスの評価を行う枠組みとして監査法人の保証業務として提供されるものに、受託会社の内部統制にかかわる保証報告書（SOC：Service Organization Controls）がある。このうち、SOC２、SOC3は、受託会社が外部に提供しているサービスにかかわる内部統制をTrustサービス原則等に基づく規準に沿って評価するものであり、情報セキュリティ監査と重なる部分が多い。SOC報告書においては、内部統制

が重要な点において適切に設計され有効に運用されていることを評価し、財務諸表監査の保証業務と同じく合理的な保証を意見表明することになり、一般には情報セキュリティ監査に比較して監査費用がかなり膨らむ傾向にあると言われている。

ISMAPの監査の方式は、本来であれば監査人が行うべき業務を二分し、監査業務実施者が手続を実施しその結果を事実に即して報告する部分と、その報告を受けてISMAP運用支援機関が判断を行う部分とに分割されていると見るべきである。このことにより、監査法人がこの業務を担当することができるようにすると同時に、クラウドプロバイダーの監査費用負担を可能な範囲に低減する効果も生まれている点で現実的な選択ということができる。しかし、監査人の責任範囲が、定められた手続きを実施しその結果を報告する範囲に限定されており、重要性の概念の適用やリスク評価に基づく手続の決定は行わないとしている点で、監査人としての力量の発揮の場が限定され、達成感の得にくい作業に落ちいりかねないことも容易に想像できる。

情報セキュリティ監査における保証概念については、筆者も参加したJASAの保証型情報セキュリティ監査促進プロジェクトにてまとめた「保証型情報セキュリティ監査概念フレームワーク解説書Version 3.22b」（2007年3月）が参考になる。その解説０１には、会計監査は財務報告を監査し、情報セキュリティ監査は情報セキュリティマネジメントを監査するという意味で、対象とする事項の特質による差を明確にしたいとして、次のように七つの差を指摘している。こちらも少々長いが原文を引用する。この概念フレームワークの内容やその詳細は、解説書を参照いただきたい。

「まず、第一の差は、会計監査の対象は経済活動であるのに対し、情報セキュリティ監査が対象とするのは情報活動という違いがある。第二に、それらの活動の主体について、会計監査では法人としての振る舞いを対象にするのに対し、情報セキュリティ監査では情報を扱う自然人の振る舞いを対象とする差がある。さらに第三には、それらの活動を監査する上で必要となる技術的裏づけの程度にも大きな差があり、情報セキュリティ監査においては、詳細な技術的検証が必要となる。

社会的要請の側面では、会計監査の背後には高度に成熟した資本市場があり、市場参加者が必要とする財務情報の正確性という明確な監査の要請があるが、情報セキュリティ監査の背後にはまだ市場原理に基づく要請は明確でなく、むしろ市場の失敗ともなりかねない現状にあり、第四の市場の差はきわめて大きい。さらにこの大きな差を生み出しているとも言える第五の差が、会計監査は法定強制監査であるのに対し、情報セキュリティ監査は今のところ任意監査であるという点にある。したがって、第六に、監査報告書の利用法からの要請も当然に異なることになり、結果として第七に、監査に携わる監査人の資格制度への要件もかなり異なるものである。

会計監査へは、株式市場の発達、個人株主の対等などにより、株式市場での投資判断の正確な材料を提供することに対する強い社会的要請があり、また株式市場にはその企業とすでに特定の利害関係を持つ者以外の参入も容易であるから、結局は万人に誤解なく理解されうる会計監査の枠組みが必要であり、監査報告書の形式もこの要請にこたえうるものでなければならないことになる。

しかし、情報セキュリティ監査においては、情報セキュリティマネジメントにかかわる情報を正確に表現する形式的な規格化が未成熟な上に、特定の企業の情報セキュリティマネジメントに特別の利害関係を持つ利用者とそうではない一般の者とでは、監査に期待する具体性には明らかに大きな格差があり、知りたいと思う動機も知りたい内容も決して均一ではないことが情報セキュリティ監査の現状でありまた特徴でもある。

会計監査と情報セキュリティ監査には、このような差異があることを明確に認めた上で、保証型情報セキュリティ監査の概念フレームワークの構築に取り組

まなければ、フレームワークの構築において基礎となる考え方に誤解が紛れ込む可能性が大いに存在するとの認識から、同じ監査とはいいながら両者は別物であるとの出発点を明確にしたのである。

企業会計審議会における保証業務の分類は、保証業務リスクの程度により、合理的保証業務と限定的保証業務とに分類されている。しかし、情報セキュリティ監査においては、基本となる尺度の制約により、保証リスクの評価に間隔尺度や比例尺度を持ち込むことが困難なことから、このような分類は当面行わないこととした。

しかしながら、監査報告書の利用者の立場から見た場合に、監査報告書の表現から会計監査における合理的な保証には相当しない監査においてあたかも合理的な保証であるかのような誤解意を受けることのないように、監査報告書の記載において整合性を保つように考慮することとした。」

この概念フレームワークの検討からすでに１６年の歳月が流れた。社会がデジタル技術に依存する度合いを高めるなか、リーズナブルな費用で提供される保証型情報セキュリティ監査の社会的要請は高まりつつあるに違いないが、保証型情報セキュリティ監査の担い手は少なく、現実に機能することなく経過してきたと言わざるを得ない。

会計監査の枠組みを基礎に始まった情報セキュリティ監査制度は、保証概念について真剣に検討し今後の情報セキュリティ監査制度の在り方を検討しなければならない曲がり角に来ていると考える必要があろう。

さらに最近の課題として、監査法人などの監査企業において、情報セキュリティ監査人を志向する人材の不足にも直面していると聞く。また、一部に助言型情報セキュリティ監査の品質に疑問を呈するような事態もあったと報告されている。これから情報セキュリティ監査人を目指そうとする有為の人材にとって、法定監査ではない任意の助言型監査にとどまるような情報セキュリティ監査は魅力的なキャリアパスには映らないだろう。ましてや、監査人の報告は、手続実施結果を事実に即して報告するのみにとどまり、手続実施結果から導かれる結論の報告も、保証も提供しないという位置づけのままでは、今後情報セキュリティ監査人を目指す人材がさらに枯渇するに違いない。

この曲がり角に対処するには、まず第一に情報セキュリティ監査における保証概念を確固たるものにしなければならない。

そのうえで、情報セキュリティ監査制度を、助言型監査主体の制度から、保証型監査主体の制度に改める必要がある。助言型監査は、保証型監査の前段階として、あるいは内部監査として実施し保証型監査の効果を高める位置づけとするのである。

さらに、特定の社会基盤等重要な事業を担う組織には保証型情報セキュリティ監査を法定義務とするような法制面の検討が望ましいと考える。

また、情報セキュリティ監査業務を提供する主体の多くを占めるのが監査法人であるという事情に大きな変化はないとすれば、監査法人が新たに定義する情報セキュリティ監査における保証業務を提供できるための枠組みも検討を進めなければならない。財務諸表監査の枠組みの延長としての保証業務に位置づけられる監査と、新たに定義する情報セキュリティ監査の保証概念に基づく監査とを並列でとらえることも場合によっては一つの解決策の方向になるかもしれない。

いずれにしても、リーゾナブルなコストで保証型情報セキュリティ監査が提供され、デジタルに依存する社会の安定に貢献できる情報セキュリティ監査制度への転換が求められていると考える。

このような取り組みにより、情報セキュリティの保証型監査の社会的意義が認知され、監査企業や監査人の社会的地位等が認識されれば、情報セキュリティ監査人をキャリアパスの中に位置づけて考える若者も増加してくると期待される。

これらはJASAのみにてできる話ではない。政府の本格的な取り組みを求めたい。

稲垣　隆一 様

稲垣隆一法律事務所
特定非営利活動法人日本セキュリティ監査協会
資格認定委員

セキュリティ監査制度創設２０周年を皆様とともに心から喜びたいと思います。

私とこの制度との関わりは、情報セキュリティ監査研究会の委員として制度設計にかかわって以来で、研究会終了後は、ＪＡＳＡの顧問、資格認定委員として、制度実施のインフラづくりから現在まで様々に関わって参りました。

さまざまな思い出が去来します。

まず、研究会段階では、当時、経産省で担当課長補佐をされていた山崎琢矢氏との出会いが鮮烈に思い出されます。制度の生みの親である山崎氏から伝えられた研究会創設の思いは、「社会インフラとしてのセキュリティ監査」を創ることでした。それは、具体的には、監査による利益を被監査主体のセキュリティレベルの向上に用いることに留めず、社会のセキュリティレベルの向上と確保に役立てるという視点でした。この問題意識の論理的帰結は、第三者監査、保証監査でした。この「思い」は、サーバーセキュリティが国家戦略、経済圏の囲い込みの武器とされ、地球規模でサイバー攻撃に晒され、サプライチェーンセキュリティやリスクコミュニケーションが強く求められるようになった今となっては当然のことと受け止められますが、２０年前はもっと牧歌的な時代でしたから、山崎氏の先見性が改めて見直されるところです。

しかし、この「思い」の実現には、まず、足下の課題を解決しなければなりませんでした。研究会の終盤、会計監査、システム監査やベンダーなどから様々な意見と知見が寄せられ、管理基準、個別管理基準、同ガイドの作成、助言型監査から出発、言明監査、監査報告書の利用範囲制限などへと様々に形づくられて行きました。私も研究会報告書5.2法的関係の論点整理の原稿を寄せさせていただきました。セキュリティ監査制度の産みの苦しみの時代であったと思います。

セキュリティ監査研究会を終え社会実装の段階に入ると、実務的な課題が山積していました。暑い夏、小さな部屋で汗を流しながら、夜遅くまで、研究会報告書を踏まえた監査契約書や報告書モデルづくり、各種規程づくりに取り組んだことを思い出します。飯田橋の小部屋で取り組んだ倫理制度の創設にあたっては、参加者の、セキュリティ監査を社会インフラとして位置づけその専門性への信頼を確保する「思い」が込められていました。

私も制度の作り手として、制度を普及させるべく、経産省のシステム開発モデル契約書づくりに際し、契約プロセスにセキュリティ監査を取り込むこと、ＮＩＳＣでの議論に際してセキュリティ監査の利用促進を求めて実現するなど、セキュリティ監査の普及を応援してきました。

山崎氏が構想した社会インフラとしてのセキュリティ監査は２０年を経て、今や、その必要性を誰もが受け容れるようになりました。

セキュリティ監査を支える担い手は増え、これからも社会のニーズに応え、社会インフラとしてますますその内容を充実することでしょう。

とはいえ、先ずは足下の課題から。私としては、責任とコスト負担の社会的分配の仕組みの構想かなと思っています。

下村　正洋 様

特定非営利活動法人
日本セキュリティ監査協会
初代 事務局長

情報セキュリティ監査制度の始まりの頃の話

情報セキュリティ監査制度が経済産業省の情報セキュリティ監査研究会（以後、研究会と略す）の検討結果の報告書として公表されたのは2003年3月26日でした。ここから我が国の情報セキュリティ監査制度は始まりました。この7か月後に日本セキュリティ監査協会（JASA）が特定非営利活動法人として発足し、この制度を普及し、維持するための活動を開始しました。この寄稿文では、研究会とJASAの設立までの経緯について、小生から見えていた景色について述べます。本寄稿文に記述してあることは、あくまで小生から見えていた景色であり、事実を誤認している可能性については否定できないことを理解していただきたく思います。これから数十年後に我が国の情報セキュリティについて振り返る方が出てくるとき（出て来ればの話ですが）に少しでもその一助となればとの思いで記述します。

組織の情報セキュリティ対策の実効性を評価する方法として監査という行為が必要ではないかとの発想に至ったきっかけは住基ネットに関する問題からでした。2002年当時は当年8月から稼働する住基ネットの安全性（個人情報漏洩や官による情報利用など）について世間では議論が沸騰していた時期でありました。どこかで聞いたような話であり、20年経た現在でもあまり進歩していないことに残念な思いもしますが、当時はこの論争の矢面に立っていたのは総務省であり、総務大臣であった片山虎之助大臣でした。その片山大臣が国会答弁か記者会見かは定かではないが、「定期的に監査する」との発言があったことを記憶しています。その発言を聞いたときに情報セキュリティ分野に会計監査とは対象が異なるものの情報という資産に対してそれを保有する組織に監査という行為があり得るとのひらめきがあったことを記憶しています。そのようなことを考えていると当時の経済産業省情報セキュリティ政策室（現サイバーセキュリティ課）の山崎琢矢課長補佐とたまたま会う機会があり、山崎氏も同様のことをひらめいたとの話でありました。そこから、ほどなく経済産業省情報セキュリティ政策室にて情報セキュリティ監査研究会が発足して、情報セキュリティ監査制度のあるべき姿について議論が開始され、翌年3月に情報セキュリティ監査制度についての報告書が発表されました。

情報セキュリティ監査研究会は委員長に土居範久慶應義塾大学教授が就任し、ほか情報セキュリティベンダー、通信事業者、監査法人、法曹界、システム監査、学界の方々から構成して情報セキュリティ監査制度のあるべき姿について検討を行いました。詳しくは情報セキュリティ監査制度研究会の報告書を参照してください。忘れてはいけないメンバーとして我が国の情報セキュリティを先頭に立って牽引した初代NISC補佐官の故山口英先生も加わっていました。小生もこの検討会のメンバーとして参加しました。この検討会で、小生が印象に残った議論は保証型監査と助言型監査についてでありました。情報セキュリティ監査を考えた場合、何に照らして監査をし、その監査は何を表明するかでありました。小生の稚拙な知識からすると会計監査においては、当該企業が作成している財務関連諸表の記載の正確さについて保証していると考えますが、情報セキュリティ監査においては、それに該当するものが存在していないことから、往々にして議論はセキュリティ対策の十分性に対して行われる力が働いていました。つまり、情報セキュリティ監査は被監査企業の情報セキュリティ的安全性を保障すべきではないかとの意見とそれはできないであろうとの意見のせめぎあいであったように思えます。そのほか、被監査主体とその監査結果の利用者についての議論などがあり、その方向性の中で保証型監査と助言型監査の考え方が生まれてきたと考え

ています。この是非については、現在はあまり議論がされることがなくなっているように思え、情報セキュリティ監査そのものの本質の議論よりは、監査するまたは監査を受けるという行為に重きが置かれて語られるようになったのではと感じていて、あまり深く意味を追求されずに使われていることは、ある意味で情報セキュリティ監査が一般に受け入れられているのではないかと感じています。ただし、この本質については、継続的に検討すべき課題ではないでしょうか。もうひとつ、情報セキュリティ監査研究会で作った管理基準と個別管理基準のことについても印象に残っています。これは、前述の保証型と助言型の議論と同根であるとも考えられますが、汎用的な管理基準のみでは十分な監査はできないことから派生したとも考えられます。現在では、業界別のセキュリティ対策基準が必要だとか、個別のIoT製品についてセキュリティ基準が必要だと言われて、その対策基準の策定に動いますが、その必要性を予見して構築したものでありました。監査制度が発足してから10年程度は、管理基準のみが議論の対象となっており、個別管理基準を作ることを求めることは制度として不完全で理解ができないとの声も聞こえてきましたが、現在となってはこの研究会を主導した土居委員長とメンバー各位ならびに経済産業省各位の慧眼には感服いたします。

さて、日本セキュリティ監査協会（JASA）の設立についての景色についてです。情報セキュリティ監査制度を信頼たるものにするためには、監査をする人（監査人）と監査をする企業の質を維持してゆくことが大事であると報告書にも記載されていますが、それを担う団体としてJASAは設立されました。団体を発足するに際して、大急ぎで設立準備会を組織し、会長を土居先生にお願いして、快く引き受けていただき、その後も大変ご支援を頂いたことは感謝の念に堪えません。設立準備会を組織し、2002年5月29日に設立発起人会を発起人52名、後援団体8団体を集めて、東京テレポートセンターで開催することができました。その時、休憩時間に稲垣先生から、このJASAは大変重要な役割を持っていて、将来我が国の重要な役割を担い、または、担わなければならないので頑張ってゆきましょうと言われたことが大変印象に残っています。その後、幾度も会議を重ね、10月16日に設立総会が開催することができ、無事にJASAが発足しました。

最後になりましたが、研究会よりご一緒し、JASA設立準備会、そして、設立後の活動に対して多大なるご助力を頂いた、大木榮二郎氏、喜入博氏、小林俊範氏、丸山満彦氏、水野義嗣氏、和貝享介氏には大変感謝しております。加えて、法律面より支えていただいた稲垣隆一弁護士、短期間に管理基準を作った河野省二氏、それを支援していただいた中尾康二氏に感謝いたします。

JASAが現在あるのも、永宮前事務局長の手腕によるものであることは自明のことですが、紙面の都合上、前述のお名前を挙げなかった各位並びに設立時の大変な時期に実質的に事務局を立ち上げた故沓澤徹氏（当時、事務局次長）と過去・現在のすべての事務局のメンバーついても本当にありがとうございました。JASAのますますの発展を祈念しております。

松本　照吾 様

アマゾン ウェブ サービス ジャパン合同会社
セキュリティアシュアランス本部 本部長

“Department of Yes”
-監査人こそがデジタルトランスフォーメーションを-

　このたびは、情報セキュリティ監査制度創設20周年、誠におめでとうございます。

　この20年でITがビジネスの加速、組織変革の中心となり、セキュリティの重要性の認知も高まりました。

　一方で、日本の競争力はいまだに停滞を続け、デジタルトランスフォーメーションは思ったよりも進捗していません。

　本来、セキュリティは“ビジネスを安全に加速”させるためにあるものですが、それを実現するためにはセキュリティを推進し、また評価する私たちが、ビジネス自体を理解し、その推進のために何が出来るかを真摯に考え、新たな知識を学び、自らが変わっていく必要があります。

　“Department of Yes”というのは、セキュリティやリスク管理は従来は“リスク”を理由に単純にイノベーションの阻害、つまり変化に“No”をいうのではなく、適切な学びを踏まえ、組織を前に進めるための建設的な議論を進めていけるようマインドセットを変えていこう、というメッセージです。

　監査人こそが、新たな知見を積極的に学びそしてその実践者となることで、より組織の価値向上に貢献していく必要があると確信しています。

第２章 20 周年記念イベントの記録

会長挨拶

特定非営利活動法人日本セキュリティ協会 会長
慶應義塾大学 教授　　手塚　悟 氏

日本セキュリティ監査協会会長の手塚です。本日は本イベントに多数の方にご参加いただき大変ありがとうございます。

情報セキュリティ監査制度は2003年4月1日に経済産業省により施行され、今年で創設20周年を迎えました。この記念すべき20年という節目の年を迎えることができましたのも、制度創設以来ご協力いただいた政府機関の皆様、会員企業の皆様、関係団体、その他関係の方々のご指導、ご鞭撻のおかげであり、心より感謝申し上げます。特に前会長として多大なご尽力をいただいた土居先生にはあらためて御礼を申し上げます。

さて、制度施行から約半年後の10月10日にJASAが設立されました。その後、現在まで制度の運営の基盤となる情報セキュリティ監査人の育成、各分野への制度の普及促進に努めてきました。資格の認定者数は累計で4,700名を超える規模になっております。2012年には、クラウド情報セキュリティ監査制度のCSマークの認定事業、その5年後の2017年には、情報セキュリティサービス審査登録制度における審査機関としての活動を開始しました。

さらにその2年後にはISMAPでの監査機関の審査業務を開始しております。協会の活動の発展とともに、情報セキュリティ監査制度の更なる適用拡大を進めることができるようになりました。

これらの成果は、本日ご参加いただいている幅広い分野の有識者、情報セキュリティ分野の専門家、監査人など、様々の方々のご協力、ご支援により実現したものであり、あらためて御礼申し上げます。

今後は、リモートワークに代表される働き方の急激な変化やクラウド、AIなどの技術変化など、想像できないような新たな時代が我々を待ち構えているはずです。制度発足20年目という節目を機に、関係者の皆様と共に決意を新たにし、より安全な情報社会の実現に向けて、取り組んでいきたいと思います。今後とも、なにとぞご支援ご愛顧を賜りますようお願い申し上げます。

以上で開会の挨拶とさせていただきます。ありがとうございました。

基調講演

情報セキュリティ監査制度の 20 年を振り返って

特定非営利活動法人 日本セキュリティ協会 前会長
慶應義塾大学 名誉教授　　土居 範久 様

【オープニング】

◆司会

それでは基調講演に移らせていただきます。基調講演は日本セキュリティ監査協会の前会長で、初代会長もお務めいただきました、慶應義塾大学名誉教授の土居範久様にお願いいたします。なお、本日土居様はご都合によりオンラインでのご講演となります。

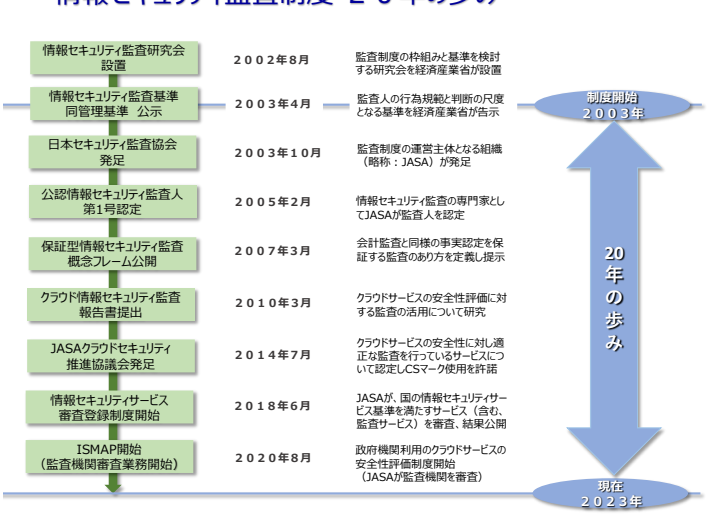
土居様は、経済産業省が2002年に設置した情報セキュリティ監査研究会の委員長に就任されましたが、その委員会が情報セキュリティ監査制度の誕生の契機となりました。また委員会を引き継ぐ形で、本監査制度に関連する企業や組織からなる団体として、同年にJASAが設立され、土居様には初代会長として、2003年から2020年までの長きにわたり大変なご尽力ご支援をいただきました。本日はそのような歴史を振り返りつつ、様々なエピソードや将来に向けてのメッセージなどについて、お話を伺えればと思っております。それではお待たせいたしました、土居様、どうぞよろしくお願い申し上げます。

◆慶應義塾大学 名誉教授　土居様

ただいまご紹介に預かりました土居でございます。どうぞよろしくお願いいたします。本来はそちらに会場に伺うつもりだったのですが、ちょっと肋骨を痛めまして、南房総の阿波鴨川からお話をさせていただくこととなりました。ご理解いただければと思います。

【講演】

◆慶應義塾大学 名誉教授　土居 様



ただいま現会長およびご司会の方からお話もございましたが、2002年の8月に経済産業省に、監査制度その枠組みと基準を検討する研究会が設置され、それの委員長を務めたわけです。なぜこのようなものを作ったかということですが、これには日本経団連、あるいは中小企業を代表する方等々にもお入りいただいて、いろいろ検討したわけです。

その同じ年の4月に1年間のテストケースを経まして、ISMS認証制度が発足しました。JIPDEC(一般財団法人日本情報経済社会推進協会)でやっているわけですが、これも当初から現在に至るまで、私が何らかの形といいますか委員長のような形で、務めさせていただいております。このISMSというのは、インフォメーション・セキュリティ・マネジメント・システムですが、ベストプラクティス、いわゆる管理要件ですね、それと認証という、パート1、パート2からなっているんですが、実際にISMSが走り始めた時には、パート1しかISOの規格がなかったんです。ISO 17799という変な番号が付いておりますが、これはBS(ブリティッシュ・スタンダード)と7799が、基本的にはそのまま成ったんですが、それはベストプラクティスだけでして、7799のパート2の方は、まだISOにはなってはいなかったので

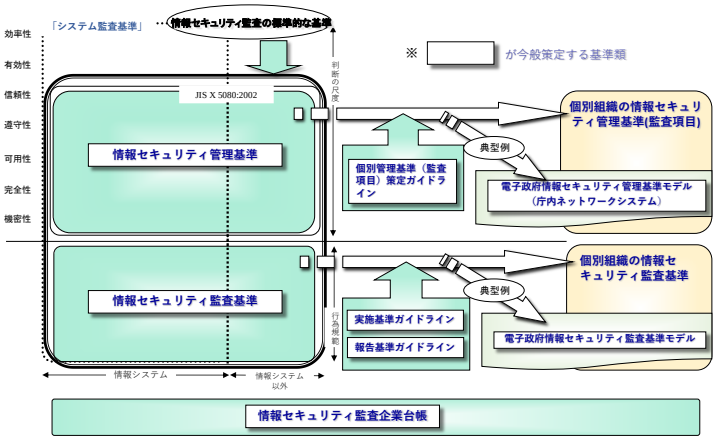
す。ブリティッシュ・スタンダードのをお借りして、我が国ではISMSをスタートしたわけです。

ISMSというのは組織における個別のセキュリティ技術対策の他に、組織のマネジメントとして、自らのリスク評価により、必要なセキュリティレベルを決め、プランを持ち資源配分して、システムを運用することが主要なコンセプトでして、組織が保護すべき情報資産について、機密性・完全性・可用性をバランスよく維持し、改善することで、PDCAサイクルを回すということが基本だったわけです。これは要するに、基本的にはそのベストプラクティス集にあるものをそのままの形で、組織として、利用していくのが原則です。外した場合には、なぜ外したかという理由を正確に書かなければいけないということ。また部分的に、どこかだけ採用するというのはなかなか悩ましいというようなことがあったのです。

中小企業では、ご存知の通り、痛くない注射針を作られた岡野工業は社長を含めて4人の会社なんですね。あるいはH2Aのロケット、この間も飛び上がりましたけど、あのブースター、あの補助ロケットの先端を作っているのは、大田区の中小企業ですが、社長含めて10人ぐらいしかいらっしゃらない。そういうところ、匠の技を持っているので、色々なところからそこへ仕事をお願いに行かれるわけですけれども、行かれたらびっくりして「うちの秘密情報をこういうところに出していいかな」ということになってしまいます。そこで皆さん方は「少なくともこういう部分に関してだけは保証してくれと、そういう制度を作ってほしい」というようなことが大元にありまして、この情報セキュリティ監査研究会が設置されたわけです。

そこで2003年3月に報告書を出し、それに基づいて情報セキリティ監査基準とその管理基準を作ったわけです。

創設する制度一覧



この図の向かって左側にあります管理基準と監査基準というこの2つのものが基本になりまして、これが2003年の4月に経済産業省から告示として出されたわけです。独特なところは、上の管理基準の右側の矢印を右側にやっていただきますと、すぐそこに小さい緑のボックスがございますが、これは何かというとローカライズできるということなんです。それで、ローカライズして、実際に適用してくださいというわけです。それを一番最初に採用してくださったのが防衛省です。防衛産業のための監査をやる時に、実は二者監査なんですが、機密保持があるため、防衛省がその防衛産業を監査するという形で、その防衛省の監査人をJASAがお手伝いして育てるというような形をとったわけです。防衛省側としては、これは経済産業省の告示に則ったものであるということを正確にお書きいただいております。

そういうようなことをして、これからしばらく経ってから、これと同等のものを、総務省が地方自治体に対して作り上げました。主語が違うだけで基本的に同じものができております。この中身、管理基準の中身は、ISMSに基づいております、最初は17799だったのですが、27000という形で落ち着きましたので、27000の管理基準、ベストプラクティス集です。それに基づいており全く同じものです。ただ、数が多少、管理要件が違うのは27000は1つの文章で2つのものを求めていたりしていますので、それは分割するという

ようなことをしました。それによって、少し監査制度の方の管理基準の方が数が多くなっておりますが、全く同じものです。

したがって、これに則ってやっていくわけです。では、監査制度とは何なのかということになりますと、それは企業等の情報セキュリティ対策につきまして、客観的に定められ、基準、今申し上げました経済産業省の告知に基づいて、独立した専門家が評価する制度です。ISMS、あれは認証制度ですので評価しかしないのですが、保証または助言をするということができるようになっております。もっとも、この保証というのは未来永劫に保証するというわけではなく、要するにその時点でこの制度に基づいたことをされている、ということを保証するわけです。

それで3つの場面を想定しております。きちんとした名前がついていまが、私の言葉でいいますと、

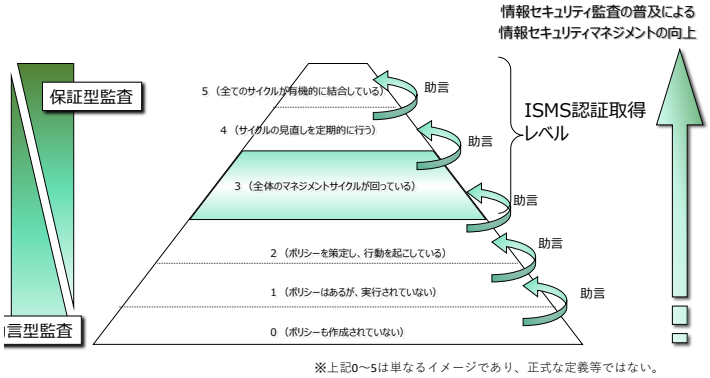
1つ目は、下請けの企業がその親の企業が考えているセキュリティ対策をしっかりやっているかどうかを監査する。

2つ目は対等の企業、ということはその企業はいろいろな企業から仕事を請け負っているわけですが、そのうちの部分的にお願いするのか全体お願いするのかは別としまして、自社からお願いするにあたって、自社のセキュリティ対策の水準をまっとうしているかどうかを指示させる。

3つ目は、私は天に向けて吠えるっていってるんですが、社会に向けて「わが社は大丈夫です」ということを、企業によってはお出しになっていらっしゃいますのでそれを評価するという、大きくいいまして、その3つのものが設けられて、対象となっております。

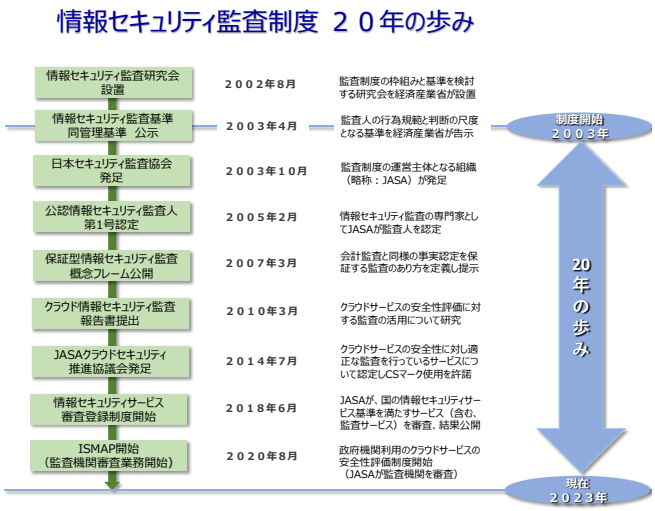
基本的に「それでは監査と認証とはどう違うのか」ということが当初から問題になりまして、我々としますと、それはきちんと整理がついたわけですが世の中では混同されておりまして、そこでISMSの認証との関係というのを、あちらこちらでお話いたしました。委託先がISMS認証を取得していれば、委託先において的確な情報セキュリティのマネジメントが行われていると期待できるため、一応安心と考えることができる。しかし、ISMS認証取得は自社とのリスク基準が同じことを保証してくれるわけではない。要するに要件全体を一律に評価するのがISMSですが、認証の場合にはある部分は強く、ある部分は弱くというようなことができるわけです。それをしないと、自社のリスク認識と同じだということはいえなくなりますので、そういうことを保証してくれる、そういうような制度が必要だというわけです。つまり、認証先がISMS認証取得だけでは、トータルのリスク対応コストが最適化されていることにはなりません。そこで重要な情報を委託先に委ねるなどの場合は、委託先の条件としてISMS認証取得を求めることが有効ですけれども、さらに保証型の情報セキュリティ監査でリスク認識を共通することが最善対策といえるというわけです。

典型的な情報セキュリティ監査市場のイメージ



※上記0～5は単なるイメージであり、正式な定義等ではない。

したがって、全体としますと全くそういうようなことをされてないまっさらの会社、企業から考えますと、こういうような状態で「助言で」ずっと段階を進めていただきます。それで、あるところの段階になりますと、ここにありますように「全体のマネジメントサイクルは回っている、PDCAサイクルがちゃんと回っている」というようなことになりますと「ISMSを取得していただくレベルに達した」というようなことで、それまでは助言あるいはそこから先も監査で助言をして、世の中、安全で安心な日本、あるいは世界を作っていくというための制度でございます。



したがいまして、先ほど来出ておりますが、2003年4月にこの監査制度が開始されまして、そして2003年10月10日にJASAが発足いたしました。

その次にありますのが、公認情報セキュリティ監査人第1号を認定しましたのが、2005年2月でございます。やはり、いろいろなガイドブックやら何やら用意しなきゃいけない、というようなことがありますので、そういう時間も含めてです、2003年10月10日に発足して、第1号が出てきたのが2005年2月ということでございます。

それから、保証型情報セキュリティ監査の概念フレームを公開しました。その次に2010年にクラウド情報セキュリティ監査報告書を経済産業省本省に対して提出し、そして、JASAクラウドセキュリティ推進協議会を発足いたしました。大木先生に当初から会長をやっていただいているわけです。このクラウドのセキュリティに関しましては、JASAと経済産業省とで協力いたしまして、ISOになっております。ISOの、ISMSが監査制度が、基準としております27000の17という枝番がありますが、これはJASAと経済産業省の協力の下で提案してできた制度で、国際規格です。もう1つの国際規格で、日本が経済産業省にそのお力を頂いてできたのが、ガバナンスに関するものがありまして、そのガバナンスの方も私が仰せ付かったのですが、これが枝番14番ということで、27014という国際規格でございます。これも日本初、日本も色々と協力をしております。

それで、またこの年表で下へ下がっていきますと、情報セキュリティサービス審査登録制度開始ということで、元請けはIPAです。そのIPAが、この業務をカテゴリー別に、「わが社はこのようなセキュリティサービスができます」「このサービスリストに入れてください」ということがきますと、JASAがそれを審査しまし、「それで大丈夫だ」となるとIPAのリストに入ります。それが、どう活用されるいいますと、いろんなところで「こういうことを、サービスで受けたいのだけど、どこで受けたらいいだろう」と、そのための台帳として利用していただいております。特段、地方公共団体やその地方の企業の方々などが利用しやすくなるように、今もってその研究会が続いており、それを大きくしたり細かくしたりというようなことをやっております。

それから、1番最後にISMAPというのがあります。ISMAPはご存知の通りで、政府機関利用のクラウドサービスの安全性評価制度ですが「それの監査機関をJASAが審査をする」という役目を仰せ付かっております。

したがいまして、細々と始まったのがいろいろなところでご利用いただいて、そしてより安全で安心な国に成るような形に成るように皆さん方ご協力のもと進めさせていただいているという状況です。さらに、世の中だんだんと怪しさが増してきております。いろいろなところのいろいろな方面で「利用しやすい監査制度を作り上げていくということ」および「その周りの体系を整えていくということ」が、これからJASAに求められていることだと思っております。駆け足ながら、走りながらお話ししたので、お話が通じたかどうかよく分かりませんが、以上がこの20年の監査協会の歩みということで、私からのお話は終わらせていただきます。どうもご清聴ありがとうございました。

記念講演

サイバーセキュリティ経営の実践と改善に貢献するセキュリティ監査の力

経済産業省 サイバーセキュリティ情報化審議官
上村 昌博 様

【オープニング】

◆司会

上村昌博様のプロフィールをご紹介します。

平成 5年に通商産業省へ入省後、環境対策や中小企業振興など、さまざまな行政分野を担当される一方、平成24年から27年に経済産業省情報セキュリティ政策室長として、制度の創設および日本セキュリティ監査協会の設立の時期に多大なご協力をいただきました。また昨年7月からは現職の経済産業省サイバーセキュリティ情報化審議官に着任され、経済産業省のセキュリティ対策やデジタル化と共に、産業界のセキュリティ対策やDX人材育成の支援を担当されていらっしゃるほか、関係省庁などと共に政府情報システムのためのクラウドサービスに関連するセキュリティ評価制度ISMAPの運用改善にもご尽力されていらっしゃいます。

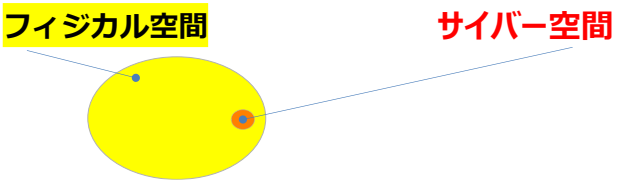
このように、制度の創設から現在に至るまで、制度の普及に多大なご尽力をいただいたことに、ここで改めて感謝申し上げます。本日は「サイバーセキュリティの経営の実践と改善に貢献するセキュリティ監査の力」をテーマに、今後の期待を込めてお話を承りたく存じます。それではお待たせいたしました。上村様、どうぞよろしくお願い申し上げます。

◆経済産業省 上村様

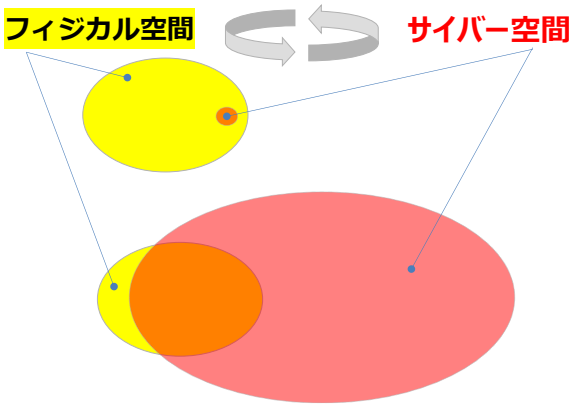
ご丁寧にご紹介いただきまして、誠にありがとうございます。経済産業省の上村です。よろしくお願いいたします。手塚会長をはじめ、また土居前会長もそうですが、このJASAの事務局の皆様、そしてここに主体的に、それこそボランタリーなものを含めてご参画をされて、このセキュリティ監査制度をゼロから作り上げられてきた。いろいろなことがあったと思いますがそこを乗り越え、守り発展させて今日までこられた皆様方のご見識ご尽力に改めて深い敬意と感謝を表したいと思いますし、今日こういう場で講演のチャンスをいただいたことに、重ねて感謝を申し上げたいと思っております。

【講演】

◆経済産業省 上村様



地球上、国境のあるフィジカル空間というものが長い間、人類にとっての活動場であったと思います。一方、図中この赤い小さい丸がありますが、コンピューター、ネットワークが使われるようになっても、あくまでそれは我々のフィジカル空間、物理的な空間の中の一部で使われていた、ということかと思います。



しかし時代はどんどん変わり、今はあらゆる経済社会活動において、サイバー関連技術が神経網のように張り巡らされているかと思います。さらにフィジカル空間を超えまして、圧倒的な無限かと思われるようなサイバー空間が生まれた中で、我々は今生きているのだと思うわけであります。

事業活動の変化

フィジカル空間で資源を使い
＋ データを使い

ヒトが事業活動を行い
＋ AIも活動を行い

価値をつくり

反復継続的に客体へデリバリ
＋ 多様なチャネルでコミュニケート

こうした変化というものは、事業活動の変化ももたらしてきているかと思います。従来、経済社会における組織の事業活動というのは、フィジカル空間で天然資源を使って、材料を作る、エネルギーを作り出すということ。そして、それを人、あるいは企業、法人が扱って事業活動を行い、その結果、製品やサービスなどの価値を作り出す。これを物理的な物流、鉄道、トラックなどの運用手段で顧客に対して反復継続的に届ける。こういったことを行ってきたかと思います。

サイバー空間とフィジカル空間の高度融合
～ Society5.0 ～

データ×IT･AI ～ イノベーション創出 ～

新たな付加価値の創出、様々な課題の解決

しかし、サイバーとフィジカルが融合してデータを活用し新たな価値を生む社会、いわゆるSociety5.0では、「フィジカル空間での天然資源だけではなく、データを最大限有効活用し、そこに人や法人だけではなくて、AI、ITといった機械などのマシンも入ってくる」ということかと思います。それによって、「総合力で新しい価値を作る、それを従来からのデリバリーチャンネル、物理的なものだけではなくて時間と空間を超えた形でデジタル技術を最大限生かして、多様なチャンネルで顧客に届ける」こういうことが起きてきていると思います。こうして、サイバーとフィジカルが融合するデータ駆動型のSociety5.0にますます我々の経済社会は移行していくのだと思うわけですが、そこでまた生み出される大量のデータを、革新的に進化を続けているITやAIを使って解析・分析をし、それがまた新しいデータ需要を生み、そのデータを解析するためにまた新しい計算機資源の開発するという、ある種の好循環により、そこがまたイノベーションにもつながっていくという期待がされているわけであります。そして、新しい付加価値の創出というものが、その活用によって従来では解決できなかった多くの経済社会の課題を解決していく、こういうことも期待がされるわけであります。

デジタル技術は経済社会に浸透
存在は当然　自然環境

かつて　自然環境や資源の利用・搾取
考慮せず　影響　相関　持続性
環境問題は、経済成長の制約となった

Society5.0、DX推進において
セキュリティ　意識　影響　対策　可視化
自らの制約となり、瓦解のおそれ

生成AIの出現や、シンギュラリティということがいわれています。スマホを多くの方がお持ちかと思いますが、デジタル技術は経済社会において我々の周りに、どんどん浸透してきているかと思います。その存在がある意味もう当然のように「デジタルネイティブ」といわれるような今の若い人たちにとっては、生まれた時から身の回りにIoT機器があるということかと思いますが、ある種、空気や水のように当然のものとして、新しい自然環境の一部のように、デジタル自然、デジタル環境となってきているのではないかと思います。かつて、我々はこの自然環境というものを、どんどん使っていたわけであります。ある種搾取をし、その活動がどう自然環境に影響を与えるのか、ひいては経済社会の

活動にも影響を与えるのか、と相関関係をあまり考えてこなかったわけです。また、資源や環境の持続可能性ということも考えずにきたのかもしれません。その結果、環境問題というものが経済成長の制約にもなってきているように思います。ただ、現在、DX推進と共に、Society5.0という方に向かっていく時に、そこにセキュリティ意識が欠落をして、その結果するところの影響を考えることなく、対策も講じることなく、努力の可視化なども行われないとするならば、かつてきた道と同様に、やがてデジタル自然環境のようなものの扱いを、巡り巡ってDX推進、経済社会活動での大きな制約となってしまう恐れもあるのではないかと危惧しています。ある日突然、デジタルに大きく依拠したこの経済社会システムそのものが瓦解してしまうようなことにもなる。そんなリスクを孕み得ると思っています。

セキュリティ対策は経営マネジメント課題のひとつ

セキュリティは事業推進の大前提
適切なセキュリティ対策を遂行できる組織こそが一層発展する

環境問題が、今日、GXとして、成長の原動力となった様に

このためセキュリティ対策というものは、組織における経営マネジメントの重要な課題の1つだと思います。セキュリティの確保こそが事業推進の大前提であって、適切なセキュリティ対策を遂行できる体制をとれる組織こそが、さらに一層発展をしていく時代なのだと思います。そうしたセキュリティ対策を行える組織でなければ、そもそもサプライチェーンや市場に参入することが許されなくなってくる時代が、もうすぐそこまできているのではないかと思っています。ただ、それは事業推進へのブレーキとしてネガティブに捉えるべきではないと思っています。かつて、経済成長の制約であると思われていた環境問題、現在ではいわゆるGX、GREEN TRANSFORMATIONということで、成長の原動力の1つとみなされるようになっています。セキュリティそのものが新しい産業や市場を切り開く契機にもなっていくのだと思っています。

事業活動の多くはデジタル環境に依存
チャンスと共にリスクも潜む

サイバー空間とフィジカル空間との繋がりの緊密化とともに、セキュリティ事案は拡大、巧妙化、複雑化

IT分野だけでなく、工場等のOT分野でも、サイバー分野での脅威が顕在化

影響は一組織に留まらず、サプライチェーンを構成するあらゆる組織に及び得る
今や、いかなる組織でも被害者となる可能性

事業が提供する価値に影響を与え得るように

今日、事業活動の多くは、デジタル環境に依存するようになっています。そこには大きなチャンスとともに、リスクが潜んでいるのではないかと思います。 サイバーとフィジカルのつながりの緊密化とともに、セキュリティ事案は拡大し、巧妙化、複雑化してきています。IT分野だけではなくて、工場のオペレーショナルテクノロジー（OT）の分野でも脅威が顕在化してきています。そして、ひとたび被害が発生すれば、一つの組織にとどまりません。被害はサプライチェーンを構成するあらゆる組織に及ぶことを想定しなくてはなりません。いかなる企業もサイバー脅威にさらされているということかと思います。サイバー攻撃が、組織の事業活動が提供する価値そのものに影響を与えうるそんな時代になってきていると思います。

大事になる　情報の保全
デジタル環境に支えられたシステムの安定稼働

影響の極小化には、部門横断的な対応が鍵

組織の目的達成には、セキュリティリスクの、適確なマネジメントが重要

コーポレートガバナンスとして、セキュリティやサプライチェーン対策など事業環境の状況を、経営戦略に適切に反映させよう、との動き

「グループ・ガバナンス・システムに関する実務指針」、「投資家と企業の対話ガイドライン」、「デジタルガバナンスコード」
２０１９年　　２０２１年　　２０２２年

したがって、今日の組織において、ますます大事になってくるのは、事業活動のコアを支えるような情報資産の保全もさることながら、デジタル環境によって支えられるようになっている、様々なシステムの安定的な稼働を確保し続けることではないかと思います。そして、万一サイバー事案が発生した際に影響を局小化していくためには、セキュリティ部門や情報システム部門だけではなく、事業部門、経営、広報、法務部

門などが横断的に連携をして、被害拡大を防ぐ、早期の収拾を図っていくことが鍵になってくると思います。組織の目的である事業価値の継続的な提供のために、セキュリティリスクというものも、エンタープライズリスクの一つとして認識をし、的確にマネジメントしていくことがますます大事になってきています。実際、コーポレートガバナンスとして「セキュリティサプライチェーンリスクの対策に関しても、事業環境の状況の変化として、経営戦略などに適切に反映させていくべきである」という動きが2019年以降、会社法や金商法などに基づくコーポレートガバナンスの体系においても、いくつかのガイドの中に明記をされるようになってきています。

経営者のリーダーシップの下、セキュリティ対策を推進していくことが重要

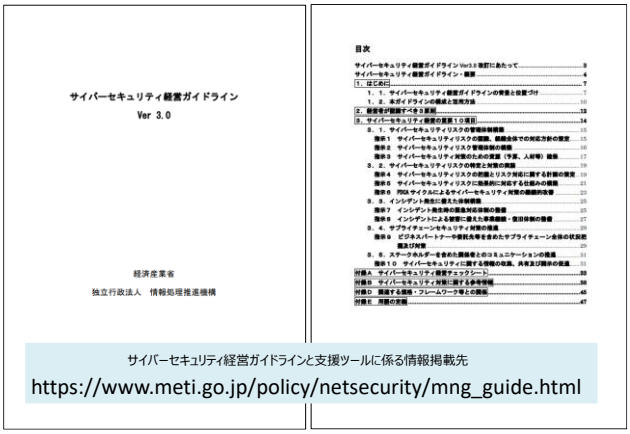
「サイバーセキュリティ経営ガイドライン」を策定

（経済産業省・（独）情報処理推進機構(IPA)）

平成27(2015)年12月28日策定
平成28(2016)年12月 8日改訂(Ver1.1)
平成29(2017)年11月16日改訂(Ver2.0)
令和 5(2023)年 3月24日改訂(Ver3.0)

組織への社会的要請に応えるため、セキュリティに関する、適切な投資や対策の実践を促進

こうした中でサイバーセキュリティ対策、経営者のリーダーシップの下で進めていくことが極めて重要であり、「経営者のためのサイバーセキュリティ経営ガイドライン」を経済産業省とIPA情報処理推進機構により、平成27年に第1版を策定をしております。この度、5年ぶりにこの3月末に第3版に改訂をしました。企業はじめ組織に求められるサイバーセキュリティ対策という社会的要請にしっかり応えていくため、適切な投資、対策の実践の促進に資することを、このガイドラインの目的としています。



サイバーセキュリティ経営ガイドラインと支援ツールに係る情報掲載先
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

ガイドラインそのものは、50ページほどのワードの文書になっております。経営者が認識すべき三原則と、CISOなどのセキュリティ担当者に経営者が支持すべき10の重要事項からなっています。ぜひこのURLから原文もご参照いただければ幸いです。

経営者が認識すべき３原則

（１）サイバーセキュリティリスクが**自社のリスクマネジメントにおける重要課題であること**を認識し、自らの**リーダーシップのもとで対策を進める**

- 企業活動におけるコストや損失を減らすためにも必要不可欠な投資(事業活動、成長に必須な費用)
- サイバー分野の残留リスクを自社の許容水準以下まで低減することは経営者の責務

（２）責務を全うするには、自社のみならず、**国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたる目配りが必要**

- 従来の部品調達のかたちに止まらず、デジタルを介した外部との繋がり全てが含まれ、時々刻々と変化
- 総合対策の徹底、顧客や社会からの信頼のため、全体のリスク低減が、参加する全ての経営層の責務

（３）平時及び緊急時のいずれにおいても、**関係者との積極的なコミュニケーション**が必要

- 不信感の抑制、緊急連絡の円滑化、初動体制を早め、円滑な対外説明を可能にする

少し概略ですけれども、経営者が認識すべき3原則について、

第1にはサイバーセキュリティリスクは自組織におけるリスクマネジメントにおける重要課題であると、経営者自らリーダーシップをとって対策を進めていくべきということであります。セキュリティ対策のための費用、これはコストではなくて「事業活動におけるネガティブなインパクトがあった時にかかるコスト、あるいは損失を減らすためにも必要不可欠な成長に向けた投資である」ということを再認識いただきたいということ。そして、各組織におけるサイバー分野で、青天井に予算もリソースもつぎ込めないため、「どこまでリスクを許容する

のか。それでも残る残留リスクに対処するために、それぞれの組織でその残留リスクのレベルを許容水準以下まで低減していくことが経営者の責務である」ということを示させてもらっています。

第2の柱として、その責務を全うするには、自社のみならずサプライチェーン全体に当たる目配りが必要ということになります。現代のサプライチェーンの、従来のいわゆる親企業、下請け企業といったような部品調達の形だけにとどまりません。クラウド、モバイル、アプリ連携など、デジタルを介した外部とのつながり全てが含まれ得るというふうに思います。かつ、その形はデジタルであるがゆえに時々刻々と変化をしていきます。サイバー対策に不十分な箇所があると、そこを起点に攻撃をされ、情報漏洩、サプライチェーンの機能停止など、自社だけではなく、顧客企業にも影響が及ぶというようになってきています。このため、国内外のビジネスパートナーや委託先などサプライチェーンを構成する全体を俯瞰し、意識をして総合的な対策の徹底、そしてリスクを全体として、バリューチェーン、サプライチェーン全体として許容水準以下としていくことが、そこに参画するすべての経営者の責務となってきています。

第三に関係者との積極的なコミュニケーションです。日頃からCISOやそのチーム、社外の公的なセキュリティ機関、あるいはセキュリティベンダーの方々などの関係者と、各リスクや対策に関する気づきや課題を積極的に共有することは大きな意味があります。そうしておくことで、緊急時の不要な不信感の高まりの抑制、またその関係性や仕組みが、いざという時の緊急連絡網として機能するということになります。その結果、迅速な報告や状況把握が可能となって初動体制を早め、外部関係者への円滑な説明、コンプライアンスにも奉仕するということになると思います。

経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示 1　組織全体での対応方針の策定** **指示 2　管理体制の構築** **指示 3　予算、人材の確保**
リスクの特定と対策の実装	**指示 4　リスクの把握と対応計画の策定** **指示 5　リスクに対応する仕組の構築** **指示 6　PDCAサイクルによる継続的改善**
インシデントに備えた体制構築	**指示 7　緊急対応体制の整備** **指示 8　事業継続・復旧体制の整備**
サプライチェーンセキュリティ	**指示 9　サプライチェーン全体の状況把握と対策**
関係者とのコミュニケーション	**指示10　情報収集、共有及び開示の促進**

上図は、経営者がCISO等に支持すべき10の重要事項になります。

まず、リスク管理体制の構築ということで、指示1：組織全体のセキュリティ対応方針の策定、指示2：管理体制を構築、指示3：自組織の許容水準以下にリスクを低減するために必要となる予算、人材の確保、であります。

次にリスクの特定と対策の実装ということで、指示4：リスク把握と対応計画の策定、指示5：想定リスクに対応する仕組みの構築、指示6：対策状況に応じてPDCAを回し改善につなげていく、ということであります。

事故ゼロにはなかなかいけません、インシデントは発生します。したがって、インシデントに備えた体制構築のため、指示7：緊急対応体制の整備、指示8：被害に備えて業務停止などに至っても短時間で復旧できるようにする事業継続復旧体制の整備、必要な場合には演習も含めてであります。

サプライチェーンセキュリティの確保のためにサプライチェーン状況を把握と対策の徹底と効果的な推進があります。

そして最後に指示10：関係者のコミュニケーション、情報収集、共有化をして情報開示等の適切な促進ということであります。

サイバーセキュリティを巡る環境は常に変化
対応は不断の継続と進化・発展

組織の　経営リーダーシップ　その組織力は
価値の創出と　その持続可能化に　大きく寄与

- **自分ゴト化　　一人ひとりの責任感　参画と対応**
- **新たな文化の創出　　価値観　信念　態度**
- **集合知 複合的な力　　横断的な連携**

サイバー空間の発展は、今後とも、多種多様な組織の力に大きく依拠
他方、サイバー脅威はますます増大

取組がきちんと機能するようにしていくことが大事
セキュリティ監査へのニーズと期待

サイバーセキュリティをめぐる環境は、デジタル技術の進歩あるいは攻撃手法の開発などによって、これは自然災害などとは違って、常に変化をしていくと思います。このため、セキュリティ対応も不断の継続によって進化・発展していくものと思います。組織における経営のリーダーシップあるいは企業をはじめ組織というものの形、その組織力、不断にその継続をして、何かを進化させていく、発展させていく、セキュリティ対応もそういう側面があると思いますが、こうした新しい価値、文化を作り出す、これを継続していくということに、経営者のリーダーシップや組織の力というのは大変大きいと思います。特に次の3つの観点が大事になると思っています。

1つは自分ゴト化です。セキュリティを他人任せにするのではなく、一人一人それぞれの立場で責任の広さ・深さは違うかもしれませんが、それぞれの立場で責任感をしっかりと持っていただいて、セキュリティ対策に参画し、対応していくことが必要です。そして、新たな文化の創出するために、新しい取り組みをしていく。環境問題はかつてもそうだったと思いますけれども、セキュリティもすでにやっておられる方々もあれば、これからという方々にとって新しいことかもしれません。新しいことは常に最初は戸惑いますし、難しいかもしれません。でも、とにかく新しい取り組みをする。これまであまり意識をされてこなかった取り組みを、それにまず気づいて、体制を何とかできるところから組んで、組織の中の営みに埋め込んでいく。そして継続的なものとして、まさに新しい文化として息づかせていくということが必要だと思います。それが価値観として組織に定着をし、その信念を持って継続して取り組んでいく。そういう態度をまた内外で示していく。こういうことが大切かと思います。さらに、セキュリティは1人、1部署、1組織あるいは1つの国で完結するものではありませんので、集合知、複合的な力、コレクティブパワーにしていくことが大事、そのためにも横断的な連携というものを積極的に推奨し、促進していく経営層のリーダーシップ、組織の力というものが大事になってくると思います。そして、サイバー空間の発展、これは本当に民間の力によってこれまで進んできたと思います。今後ともサイバー空間を作って、そしてそこを利用する多種多様な組織の力に大きく依存して発展をしていくと思います。

一方でサイバー脅威はますます増大をし、その結果、影響も大きくなってくると思います。こうした中で、セキュリティポリシーを一旦決めて、そこで対策を講ずれば終わりということではないと思います。不断に状況変化に応じてセキュリティ対策を改善していく、そんな仕組みが正しく機能するようにすることが大事になると思います。

セキュリティ監査へのニーズと期待

☆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
独立性を有する者による**情報セキュリティ対策の監査**を実施することが必要

☆サイバーセキュリティ経営ガイドライン

指示６　PDCA サイクルによるサイバーセキュリティ対策の継続的改善
- ✓ **サイバーセキュリティに関する監査**を実施し、
その結果を踏まえ、サイバーセキュリティ対策を適時見直している
- ✓ 必要に応じ･･･**情報セキュリティ監査等の外部サービス**を利用し、
現状のシステムやサイバーセキュリティ対策の問題点を検出し、改善を行う

指示９　サプライチェーン全体の状況把握と対策
- ✓ 業界事情や役割分担、相手先の対応能力等の状況を踏まえつつ、参加企業の合意の下、各企業が実施すべき対策を定め、**監査**又は自己点検等の実施を通じ実効性担保
- ✓ 対策担保の手段として、第三者による評価検証結果の活用
（認証制度の活用、**助言型外部監査**の実施等）

取り組みがやったふりではなく、きちんと機能し、効果を発揮し続けるように改善の継続が重要であり、そのためにもセキュリティ監査へのニーズ、あるいは期

待というものが大きくなっていくと思っています。セキュリティ監査をセキュリティの維持向上のために有効活用することは、すでに様々な政策文書において規定をされてきております。政府機関のいわゆる政府統一基準です、この中でもセキュリティ監査の実施の必要性を記載しています。それから、先ほどご紹介をしましたサイバーセキュリティ経営ガイドラインの中におきましても、指示6のPDCAサイクルのところで、監査を通じて対策を適時にチェックをし、継続的に見直す必要性を述べさせていただいており、指示9のサプライチェーン対策では、そこに参加する各組織の役割と責任を踏まえつつも、対策が実効性を持って機能するようになっているのかを監査によって把握し検証すること、あるいは助言型の外部監査の活用についても言及しています。

☆デジタルガバナンスコード2.0

1．ビジョン・ビジネスモデル

2．戦略

2-1．組織づくり・人材・企業文化に関する方策

2-2．IT システム・デジタル技術活用環境の整備に関する方策

3．成果と重要な成果指標

4．ガバナンスシステム

- 経営者は、戦略実施に当たり、リーダーシップを発揮するべき
- 経営者は、DXにおける課題を把握・分析し、戦略の見直しに反映していくべき
- 経営者は、事業実施の前提となるサイバーセキュリティリスク等に対しても適切に対応すべき

→ 戦略実施の前提となるサイバーセキュリティ対策の推進については、

✓ サイバーセキュリティ経営ガイドライン等に基づき対策を行い、**セキュリティ監査（内部監査を含む）を行っている**ことの説明文書等の提出をもって確認

また、デジタルガバナンスコードというものがあります。これは、情報処理促進法に基づき、DX時代の組織経営に必要な事項をまとめた指針になります。組織としてのビジョン・ビジネスモデルをまず作る。その上で戦略を策定し、その実施を評価する指標、そして機能させていくガバナンスシステムといったものが柱になっております。この中のガバナンスシステムに関しましては、経営者が率先をしてDXの課題を把握、分析し、戦略見直しを図っていくほか、DX事業実施の前提は、やはりサイバーセキュリティになるため、そのリスクについても適切に対応すべきことを示しています。そして、そのセキュリティ対策の推進をしていることを、どう確認しチェックするかということについて、サイバーセキュリティ経営ガイドラインを参考にしていただきたいということ、また、セキュリティ監査を行っていることでその状況の確認になる、ということを明記させていただいています。

☆工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

セキュリティ対策企画・導入の進め方

ステップ1 **内外要件（経営層の取組や法令等）や業務、保護対象等の整理**

ステップ2 **セキュリティ対策の立案**

ステップ3 **対策の実行と見直し（PDCAサイクル）**

維持・改善面のセキュリティ対策

- 対策の実施・運用状況とその効果の確認
- 工場システムを取り巻く環境変化に関わる情報収集
- BC／SQDC 確保の観点も踏まえ、対策を評価、見直し、更新

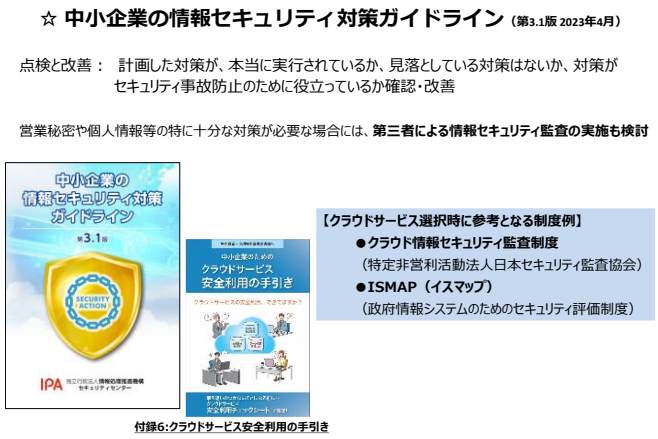
→ **監査**の形で、独立した専門的な立場から、リスクマネジメントに基づき、セキュリティ対策の実施・運用状況を確認・評価する手法もあり、**見直しにおいて監査の手法を活用している企業もある**

サプライチェーン対策

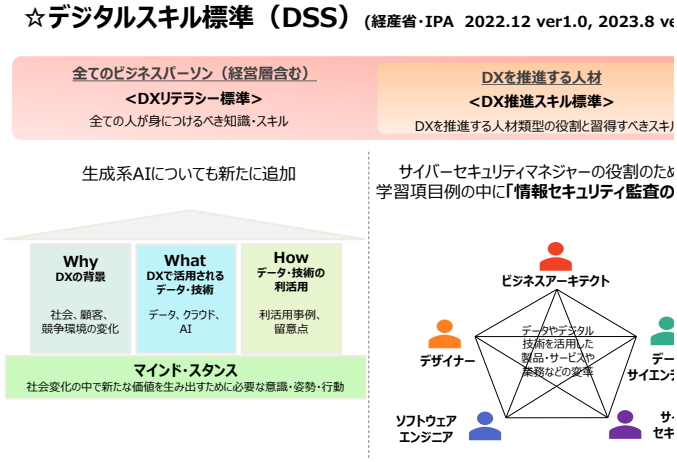
- 取引先や調達先に対するセキュリティ対策の要請、対策状況の確認
- 工場システムの脅威、影響度、対応状況**（内部及び/または外部監査実施など）**を把握できている

それからこのサイバーセキュリティ経営ガイドライン第3版の中には、サプライチェーンやOT(Operational Technology)系のセキュリティが重要になっていることを新たに追加しています。このOT分野に関しては、経済産業省で「工場システムにおけるサイバーフィジカルセキュリティ対策ガイドライン」というものを策定しています。その中で、スリーステップでセキュリティ対策の企画・導入の進め方を示し、そのうちのステップスリーのPDCAサイクルのところで、セキュリティ対策の実施運用状況と効果の確認、見直しをどうするのかということを具体的に示しています。その際に当然のことといえますが、セキュリティ監査の利活用についても示しています。

また、サプライチェーン対策については、その影響度合いについて、どのようにそのサプライチェーンでサイバー事案があった時に全体に影響するのか、これを外部監査などによって把握することはいかがかということを示しています。



また、サプライチェーンに位置する中小企業対策が大事になってまいります。中小企業向けのセキュリティ対策ガイドラインにおいて、点検と改善といった項目があります。「計画したセキュリティ対策が本当に実行されているのか」「見落としはないのか」「セキュリティ事故防止に役立っているのか」これを確認、改善するにあたって、中小企業ということから、なかなかいろいろなこと全てをできない可能性があります。しかし、中小企業であっても、特に十分な対策が必要な部分に関する、例えば営業秘密、あるいは個人情報などは、第三者による情報セキュリティ監査の実施も検討すべきではないかということを明記しております。また、このガイドラインの付録として、クラウドサービス安全利用の手引きというものがあります。その中でもクラウドサービス選択時に参考となる制度例として、クラウド情報セキュリティ監査制度、ISMAP制度をひかせていただいています。



そして、セキュリティ対策は、やはり人が大事になってまいります。経済産業省、それからIPAにおいて、社会でデジタル技術の利活用が進んでいくと、それに合わせて組織における人材活用、学びのあり方も変わっていくだろうと考え、デジタル時代の人材政策に関する検討会というもので、検討を重ねてきています。

その成果として、昨年12月にデジタルスキル標準、DSSというものを策定し、公表しております。DSSはDXを推進していく上で、すべてのビジネスパーソンが持つべきリテラシー基準というものと、DXを強力に推進していくためにより専門性の高いサイバーセキュリティを含む、5つの人材類型を既定しております。このリテラシー標準については、今年8月には生成AI時代を受けて早速改定をし、バージョン1.1になっています。そして、DX推進スキル標準の中のサイバーセキュリティマネージャーという役割に関する学習項目例の中には、セキュリティ監査の手法ということも明確に位置付けをしています。なお、こういったスキル標準と紐づいた民間主体のいろいろな学習コンテンツをセレクションしてまとめて、インターネット上のポータルサイトに掲載しています。マナビDX（まなびデラックス）というデジタル人材育成プラットフォームを経済産業省、IPAが提供をしています。この学びの成果を測定して見える化するという観点で、ITパスポート試験や情報処理技術者試験などの国家試験も提供しているところであります。

以上、ご紹介をしてまいりましたが、セキュリティ監査はセキュリティ対策を進めていく上でそれをしっかりと、また機能していることの確認、また改善を行っていく上で、大変重要な意義を持つものであります。

これから、を考える

Software Bill of Materials

IoT Security Label

　これからのセキュリティ監査というものは一体どうあるべきなのでしょうか。それを考えるにあたって、セキュリティ政策面での最近の話題を少し紹介したいと思います。1つ目にはSBOM（エスボム）です。Software Bill of Materialsということで、オープンソースソフトウェアを含むソフトウェアのセキュリティについて、そのソフトウェアの成分表を作り、いざ脆弱性が分かった時に、その対応を効果的効率的に進めていこうという1つの考え方であります。経済産業省では、産業界とともに効果的にエスボムを使っていくための実証事業も進めてきたところでありますが、この夏に「ソフトウェア管理に向けたエスボム導入に関する手引き」というものも公表をしております。また、今年5月下旬、G7サミットの際に合わせてQUAD（クワッド）日米豪印のフレームワークのサイバー分野に関しても論議が行われましたが、ソフトウェアセキュリティに関する共同原則というものが採択をされました。その中でもエスボムを活用した詳細な情報管理策の事例というものが盛り込まれたところであります。

　もう1つについては、IoTのセキュリティラベルです。IoT機器のセキュリティ対策として、「ユーザー側がその製品選択時にセキュリティ対策が講じられている」「安全なものを分かるようにする」「安全な製品が市場に普及することを後押しする」ためのラベル制度の検討です。米国や欧州では、すでに規制的な手法を含む形で検討が進んでいます。日本でも経済産業省関係省庁とともに、「IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会」において、中間取りまとめを一旦、今年公表しています。まずは自主的スキームから始め、国際的な整合性も図りつつ、柔軟な制度設計を進めていくこととしています。

SP800-171

Cyber Resilience Act

　それから、今年の夏 7月に政府のサイバーセキュリティ戦略本部において、政府統一基準の改定案が示されました。そこでサプライチェーンの脆弱な部分を起点としたサイバー攻撃リスクの増大を踏まえて、アメリカのNIST(アメリカ国立標準技術研究所)のSP800-171を参考に、「業務委託先に担保させるべきセキュリティ対策」が新たに盛り込まれたところであります。産業界において特に国際的な取引がある場合には、ますますこのSP800-171ベースの適合を模索しないと、なかなかサプライチェーンに入ることも難しくなってきていると思います。それから、欧州における「サイバーレジリエンス法案」であります。EU市場に投入されるあらゆるデジタル製品を対象に、エスボム作成、更新プログラム提供などのセキュリティ要件の適合を求める規制案となっています。重要かつ高リスクな製品には第三者認証も求めるようなものになってきています。これまで紹介をしましたエスボム、IoTラベル、SP800-171、サイバーレジリエンス法案など、これらはセキュリティ対策をある意味可視化を進めていく、そしてまた、ユーザーサイドだけではなく、サプライサイド、より能力を持ち、全体を俯瞰できる立場の企業等にも、いっそうのセキュリティ対策と責任を応分に持ってもらう。こういうことが大きな政策的な方向性として、見てとれるのではないかと思います。

Secure by Design and Default

こうした流れはある種、セキュア・バイ・デザイン、セキュア・バイ・デフォルトという流れが、強まっていくということのようにも思います。セキュア・バイ・デザインの考え方そのものは、令和3年に制定した現在の政府のサイバーセキュリティ戦略の中でも明記されています。デジタル投資、DX、それからセキュリティ対策がいっそう一体性を増していく中で、安全で安心なサイバー空間の構築につながるものであるとされています。

昭和５６年（１９８１年）
安対制度　情報処理サービス業対象
平成１３年（２００１年）
ISMS　全業種対象
平成１５年（２００３年）
情報セキュリティ管理基準、監査基準　・・・・・ と始まり、
その後の色々な変化の中で・・・・・
そして、これからの時代の変化を見据えて・・・・・

いつ 何を どう みていくか
助言 と 保証
役割分担 と 連携
そして人

セキュリティ監査につながる歴史を見てみますと、昭和56年のいわゆる安対制度から始まり、対象は、その時は情報処理サービス業でしたが、平成13年度のISMS制度実施を受けつつ全業種が対象となっていっきました。さらに、セキュリティ管理基準、監査基準ということで、セキュリティ監査制度がスタートしたという流れがあると思います。時代の変化、要請に応じて制度が進化してきたということかと思います。先ほど、土居前会長からもお話があった通りかと思います。では、これからの時代の変化を見据えて、どのようにセキュリティ監査制度はなっていくことが、セキュリティの確保と向上につながっていくのでしょうか。セキュリティ対策を、より可視化をして機能するものへと不断に改善していくこと、そしてユーザーサイドだけではなく、サプライサイドの方にもいっそうセキュリティ対策を促していく。さらには、必要とあらば規制的手法もとっていくということが、政策的には今大きな方向性として見られる中で、今後のセキュリティ監査制度を考える観点として、いくつか例示をしたいと思います。1つは組織なのか、製品なのかサービスなのか、何が監査における1つの対象なのか。そしてまたプロセスも設計、開発、製造、供給、供与といった製品やサービスのライフサイクルを考えた場合に、いつの時点の取り組みを見ているのか。そしてユーザーサイドなのか、サプライサイドなのか、誰を見ているのか。そして見る際には、どういった情報を元に、そしてどんな様式で、どういった方法でこれを確認していくのかという観点。その確認結果をもとに助言型で改善を促していくという方向というか取り組みだけではなく、「ここまではできています」あるいは「ここはできていない」といったことを一定の保証を行うという形で取り組んでいくのか。さらに政策的な方向として、規制的な手法も今想定をされている時に、監査だけではない安全やセキュリティを担保するための他の施策と、どういった役割分担あるいは連携を図っていくのか。そして何よりそれらを成し遂げるのは、AIやITの助けを借りるにしても、やはり人がとても大事であると思いますので、人をどう確保し育成をしていくのか、というような観点があるのではないかと思います。

祝　情報セキュリティ監査制度　２０周年
これまでのご尽力に心から感謝します

セキュリティが適切に保たれた
透明性ある自由な経済社会を実現
一緒に歩を進めていければ幸い

セキュリティ監査は○○○○○

これは最後のスライドになってまいりますけれども、改めて、情報セキュリティ監査制度20周年、誠におめでとうございます。これまでの諸先輩方の大変なご尽力に改めて深い敬意と感謝を表す次第であります。セキュリティ監査に求められる役割や、その能力は、時代に応じて変化していくことと思います。現在、

セキュア・バイ・デザイン、あるいはデフォルトということで、そもそも安全なそしてセキュリティの確保された製品やサービスを、大変であってもそれを作り出していくということ、ある種理想かもしれないけれどそれを求めていこうと、それを提供しかつセキュアな状態を維持していくための努力をしていこう。こういうことが求められるような時代にますますなってきていると思います。監査におきましても、サイバー関連技術を活用する際に、それが「セキュリティ確保されるものとなっているよう注意点を守って対応をしているのか」といったことを主として見ていくことから、サイバー技術による製品やサービスを作り出し、提供していく際にもそれが適切なプロセスとなっているかを見ていくようなことも、求められ得るかもしれません。それを達成するのは必ずしも監査だけの役割ではないのかもしれませんが、一定レベルのセキュア、安全な対応がされているか否かを第三者の立場から見て、示していく、可視化をしていく、そういったことに対するニーズは今後ともますます高まっていくと思うわけであります。

今後ともDXは進み、サイバーとフィジカルの融合も進んでいきます。あたかも自然環境、資源であるかのように、デジタル計器や機器、技術というのは我々の周りに溢れています。我々はそれをうまく使いこなそうとしますが、ともすると我々はサイバー空間の中で圧倒的なそのデータにむしろ囲まれているわけですから、逆の立場になることもあるかもしれません。とにかく新しいサイバー空間と共存していく中で、人間、機械、デジタル、組織といったものが新しい関係性をどう持っていくのか。どうサイバー空間と適切にフィジカル空間が融合した上で、やはり安全で安心な経済、そして社会活動を構築していくのか、改めて新しい姿、ルールの有り様について考えて、それが適切に機能するように、監査という仕組みを最大限有効利用していくことがやはり大事であろうと思うわけであります。ぜひ皆様方とも一緒になりまして、セキュリティが適切に保たれた透明性ある自由な経済社会を実現していくべく、一緒に歩みを進めていくことができれば幸いであります。

最後にセキュリティ監査は〇〇〇〇〇ということでありますが、皆さんならここにどんな言葉をお入れになるでしょうか。それが1つある程度集約されたものになるような形で、もしかすると、この20年間の間に監査という文化も、成熟してきたのかもしれません。しかし、一方でそこにいろいろな言葉が入る創意工夫、新たな気づき、多様性があるとすれば、それこそまさにこれからのセキュリティ監査に求められることへの、大変重要なヒントや示唆を含むかもしれません。

今日このイベントで様々なお話、あるいは参加者各位の間での対話・交流があるかと思いますが、それぞれまた考えを皆様巡らせていただきまして、これから先のセキュリティ監査制度のますますの発展につなげていただければ大変嬉しく思います。ご清聴ありがとうございました。改めて本日はセキュリティ監査制度 20 周年誠におめでとうございます。

講演

情報セキュリティ監査制度の 20 年

特定非営利活動法人
日本セキュリティ監査協会　永宮 直史 氏

§プロローグ

皆さんこんにちは。日本セキュリティ監査協会の永宮でございます。それでは、情報セキュリティ監査制度20年の歩みを一緒に見てまいりたいと思います。この 20年は大きく三つの時期に分けて捉えることができます。プロローグとして、その前の段階から少しエピソードを交えながらお話します。

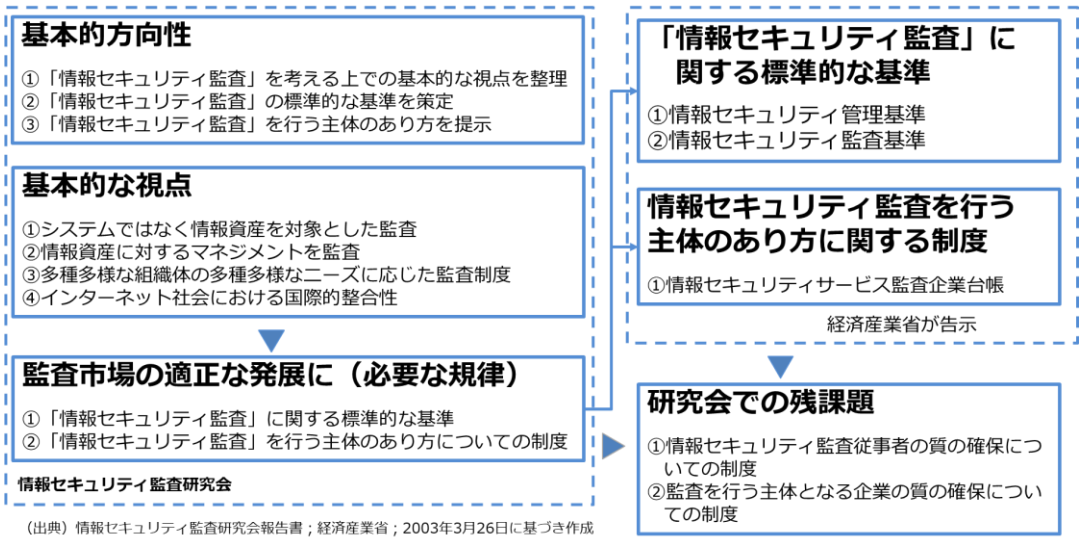
「はじめにロゴスあり」というのは、情報セキュリティ監査制度にも当てはまります。制度が始まる前年には、住民基本台帳ネットワークのセキュリティが人々の関心事となり、テレビ番組で当時の総務大臣片山虎之助氏と長野県知事田中康夫氏、評論家桜井良子との鼎談がテレビで放映されました。その席で大臣が「それなら監査する」と言ったわけです。大臣がこういう話をしますと、政府としてどうやって監査するのかを真剣に考えなければいけない。それで、経済産業省商務情報局課長補佐だった山崎琢也さんが日本ネットワークセキュリティ協会（JNSA）事務局長の下村さんに声を掛けました。お二人で土居先生を訪ねてご相談をした結果、前の講演で土居先生がおっしゃられた研究会が、経済産業省商務情報局長の諮問機関としての情報セキュリティ監査制度研究会が設けられたのです。

この研究会は、会計法人の方とIT企業の方々加わっています。両者の知見をあわせて、情報セキュリティ監査一般的な形態を提示することが目的です。

これらの方々の議論の結果、情報セキュリティ監査が社会に取り入れるためには適正な監査が契約され実施される場、つまり適正な監査市場の形成が不可欠であると認識されました。このために、監査対象を明確にし、実施するための規律が必要だということで、土居先生がおっしゃられた監査に関する標準的な基準、それからどういう主体がやるべきかを取りまとめました。

具体的には、情報セキュリティの基準として、情報セキュリティ監査における判断の尺度となる「情報セキュ

情報セキュリティ監査制度の枠組み（研究会報告書）



（出典）情報セキュリティ監査研究会報告書；経済産業省；2003年3月26日に基づき作成

リティ管理基準」と監査人の行為規範である「情報セキュリティ監査基準」を作成しました。なお、「情報セキュリティ管理基準」は既に行われていた ISMS 適合性評価制度に用いられていた、当時の国際標準 BS7799 に基づいており、国際的にも通用する制度として設計されています。

また、監査を行う主体のあり方について、情報セキュリティ監査企業台帳を作成することとしました。台帳に登録した企業が適正な情報セキュリティ監査サービスをするように促すことが狙いでした。なお、この台帳は現在、情報セキュリティサービス基準審査登録制度の情報セキュリティサービス基準適合サービスリストの情報セキュリティ監査サービスに代替されています。

一方、監査従事者の質の確保をどうするのか、監査を行う企業の質をどうやって担保するかということが残課題として報告書に記述されました。

§1【創成期】情報セキュリティ監査制度の構築（*2003*年から*2009*年）

（1）制度開始と日本セキュリティ監査協会の設立

2003年4月に、セキュリティ管理基準Ver1.0（経済産業省平成15年告示第112号）、情報セキュリティ監査企業台帳（経済産業省平成15年告示第113号）、情報セキュリティ監査基準 Ver1.0 （経済産業省平成15年告示第114号）が告示され、情報セキュリティ監査制度が開始されました。

その年の10月に特定非営利活動法人日本セキュリティ監査協会（略称：JASA）が発足しました。この協会は、研究会で残課題とされた「情報セキュリティ監査従事者の質の確保についての制度及び監査を行う主体となる企業の質の確保についての制度」を整備運用し、情報セキュリティ監査制度を着実に普及・浸透させていくことを目的とするものです。

JASAの会長には研究会の主査であった土居範久慶應義塾大学教授が就任し、監査機関やIT企業、そして情報セキュリティ監査を利用する企業53社が発起人となっています。

設立趣意書には下記の設立目的が記されています。

> この制度[1]の施行を受けて、「監査をする側」の監査企業や監査人と、一般企業や団体などの「内部監査実施部門やその担当者」が一同に会し、「公平かつ均質で、効率的な情報セキュリティ監査」を目指して、監査技術の研究開発、監査人のスキルアップ、行動規範の確立、監査人資格のあり方の検討、並びに監査制度の国際標準の調査研究や改善提言、また相談窓口の開設などの活動を通じて、「情報セキュリティ監査制度」を着実に普及・浸透させていくことを目的に、「特定非営利活動法人日本セキュリティ監査協会」を設立いたします。

JASAは監査事業者の業種団体ではなく、監査利用者も加入し、適正な情報セキュリティ監査のあり方を追求し、普及することを目指した団体なのです。その活動内容は、以下の６点にまとめられています。

① 監査技術の研究開発
② 監査人のスキルアップ
③ 行動規範の確立
④ 監査人資格のあり方の検討
⑤ 監査制度の国際標準の調査研究や改善提言
⑥ 相談窓口の開設など

残課題の対応を含む、より幅広い、より高い目標を掲げたことが分かります。

[1] 情報セキュリティ監査制度

（２）審査制度の整備

設立から半年経った2004年4月、会長の諮問機関として審査委員会設置検討委員会が設置されました。残課題である、監査企業と監査人の質の確保に対応し、審査委員会として基準・制度の運用を開始するための根拠規程や組織体制の検討を行う目的の組織です。

具体的検討内容は、以下の通りです。

① 倫理基準の制定
- 協会に参加する監査企業・監査人の質が一定以上であるために、最低限求められるルールを規定する
- 当基準に反したことが客観的に認められる場合は、懲戒処分の対象となる
- 会員に対する強行規定として、入会時に遵守の了解（誓約書）を取る

② 紛争審査制度（仮称）の設計
- 被監査主体より提起される苦情を契機に、個別の監査が情報セキュリティ管理基準・情報セキュリティ監査基準および倫理基準に適合しているかを表明する制度
- 協会会員による情報セキュリティ監査が一定水準以上であることを担保し、簡易迅速な紛争解決による被監査主体の保護を図る

③ 外部審査制度（仮称）の設計
- JASAとして独自に選択した監査について、個別の監査が情報セキュリティ管理基準・情報セキュリティ監査基準および協会の倫理基準に適合しているかを表明する制度
- 監査主体外部の専門家集団による評価によって、協会会員による情報セキュリティ監査が一定水準以上であることを担保

審査委員会の機能として、基準に反した場合、場合によっては懲戒というようなことまで含む倫理基準を検討しています。このような機能を有する機関は日本公認会計士協会だけですね。我々は、そこを一つのモデルにしたということです。

1年間の検討を経て、2005年に審査委員会が設置され、以降、現在まで委員会活動が継続しています。

（３）資格認定制度の整備

2003年のJASA発足と同時に、スキル部会を立ち上げました。スキル部会は監査主体の質の確保を目的に
- 監査人のスキルアップ支援
- 監査企業並びに監査人の行動規範の確立
- 監査人資格のあり方の検討

を行い、よりよい監査活動を提供できる人材育成の為の基盤作りを行うものです。

スキル部会には二つのワーキンググループ（WG）が設けられ、実務的な検討が行われました。

教育カリキュラム作成WGでは、情報セキュリティ監査人スキルマップを作成し、それに基づく監査人教育カリキュラムの作成を担当しています。また、資格制度検討WGは、情報セキュリティ監査人行動規範を策定し、情報セキュリティ監査人資格制度の検討と監査人の地位の確立の検討を担いました。

1年以上の検討の結果、2004年12月に情報セキュリティ監査人資格制度を運営する資格認定委員会が設置され、その1カ月後の2005年1月に公認情報セキュリティ監査人（CAIS）の認定作業を開始し、2005年2月に第一号の資格登録者が誕生しました。

（４）普及促進活動

情報セキュリティ監査制度全体を世の中に普及するために、2003年から2009年の6年間に北海道から九州まで、全国縦断のシンポジウム・フォーラムなどを開催し、普及促進活動に邁進しました。具体的な内容は以下の通りです。

年度	内 容
2003	設立記念情報セキュリティ監査普及促進シンポジウム開催（東京、大阪） 情報セキュリティ監査人研修（東京10回、大阪2回）
2004	情報セキュリティフォーラム（東京、大阪） 被監査主体のための実践情報セキュリティ監査セミナー（全国6か所） 情報セキュリティ監査人研修（東京2回、大阪、仙台、名古屋、富山） JASA 広報誌『 Security Eye 』の創刊
2005	情報セキュリティフォーラム（東京2回、大阪1回、仙台、名古屋）
2006	情報セキュリティ監査シンポジウム（東京2回、大阪1回） 情報セキュリティ監査ミニセミナー in Kyoto
2007	全国縦断　情報セキュリティ監査セミナー（仙台、札幌、高松、東京、名古屋、富山、大阪、福岡）
2008	情報セキュリティ監査シンポジウム（東京2回） 情報セキュリティ監査セミナー（札幌、高松、仙台、福岡、大阪、名古屋、広島、富山）
2009	情報セキュリティ監査シンポジウム（札幌、高松、仙台、大阪、富山、東京、広島、名古屋、大分 情報セキュリティ監査実践セミナー（東京9回、大阪2回） 関西合同セミナー（3回）

（５）保証型情報セキュリティ監査の具体化

情報セキュリティ監査で求められるは、ある組織の情報セキュリティ対策に疑義を持たれたとき、その対策が「適正」か「適正でない」かについて監査人が意見を述べること、すなわち、保証型監査です。会計監査は財務諸表という明確な対象がありますが、情報セキュリティ対策については、何をどのように保証するかは大きな課題でした。

そこで、2005年度に大木栄二郎工学院大学教授を主査とした保証型情報セキュリティ監査プロジェクトを立ち上げました。このプロジェクトでは、まず概念整理を行い、それに基づき2007年度までパイロット監査を実施し、その概念に基づく監査の適用可能性を検証しました。

このプロジェクトでは、2007年3月に保証型監査概念フレームワークをとりまとめました。このフレームワークでは組織経営者の「言明」を対象に監査を実施します。そして、監査手続の合意の形態により、以下の３方式を定義しています。

- 社会的合意方式
- 利用者合意方式
- 監査主体合意方式

パイロット監査は会員企業の協力を得て、利用者合意方式の適用可能性が確認できました。

このプロジェクトを通じて、情報セキュリティマネジメントに対する具体的な保証の仕方を明示したわけです。

（６）創成期の総括

2009年までの情報セキュリティ監査制度の一つの成果は、情報セキュリティ監査という言葉がきちっと定着したことです。ISMSの普及による内部監査や自治体の情報セキュリティ監査業務が非常に広く実施されるようになりました。

ただ、残念なことに、情報セキュリティ監査制度の方が追いつかなかったといった方がいいと思います。というのも、情報セキュリティ監査市場は混乱してしまいした。自治体向けの情報セキュリティ監査の業務が非常に増えましたが、監査品質がばらついたのです。その原因として監査品質を評価できないような入札、加えて地元業者重視の弊害で、監査能力のない人が監査を行ったということがありました。その結果、安かろう、悪かろうという監査が見えてしまい、情報セキュリティ監査の評価が下がることもありました。JASAがいくら人材育成しても、やはり市場のニーズに追いつかないことも原因でした。

§2 数字で見る情報セキュリティ監査制度の 20 年

次に、制度創設後後20年間を数字で見ていきたいと思います。

（1）収益の推移

図にJASAの収益の推移を示します。監査制度の維持・運営のための収入推移です。

収入がピークとなったのは、創設3年目（2005年）の収益期は135百万円ありました。その後、2010年に政府プロジェクト収入が減り、2012年には収益がピークの1/3（40百万円）まで下がりました。

実は私はこの時期に事務局長に就任しました。とっても辛い時期ですね。すぐに考えたのは、収入改善のためにどうするかです。図の青い部分（資格制度）を拡充することに注力しました。監査人が増えると、ここの資格維持費用が増え、結果として収益が増加します。

それからこの黄色い部分（情報セキュリティサービスの審査登録制度の審査費用）ですね。2018年度に審査業務を開始して以降、事業急激に立ち上がってきまして、一つ大きな収益の柱になりました。

それから2020年から図の灰色の部分である普及・啓発事業が再度立ち上がっています、これがISMAP審査事業です。

二つの審査業務により、現在は、創設時よりも上回る収益基盤ができています。

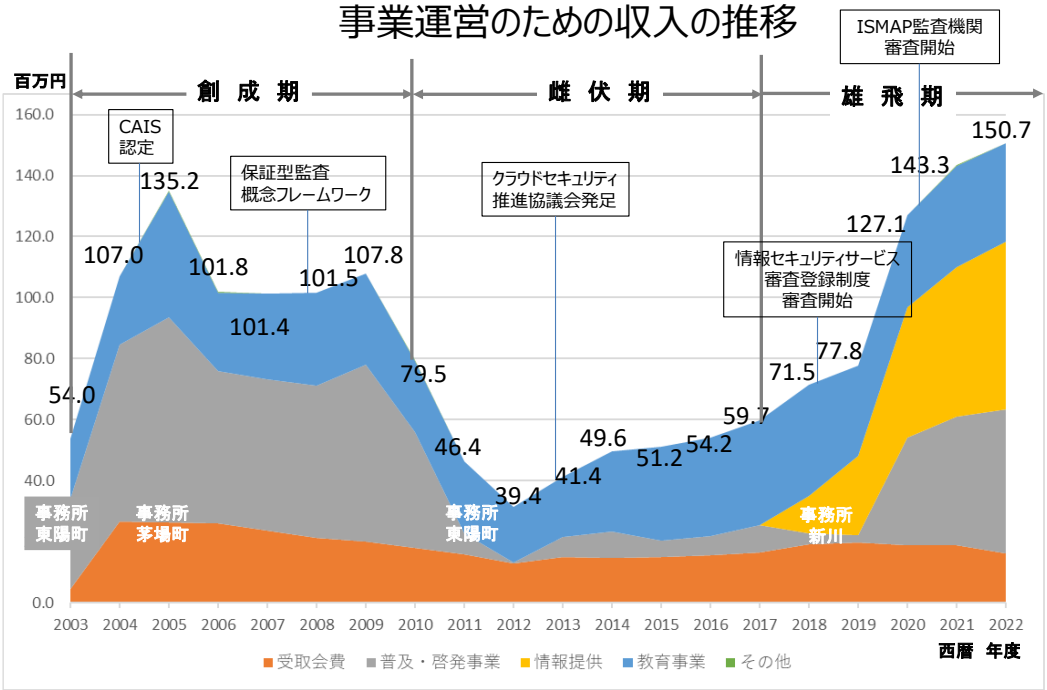
冒頭で、情報セキュリティ監査制度の20年は3つの時期に分かれると申しました。収益からこの3つの区分が明確に分かります。

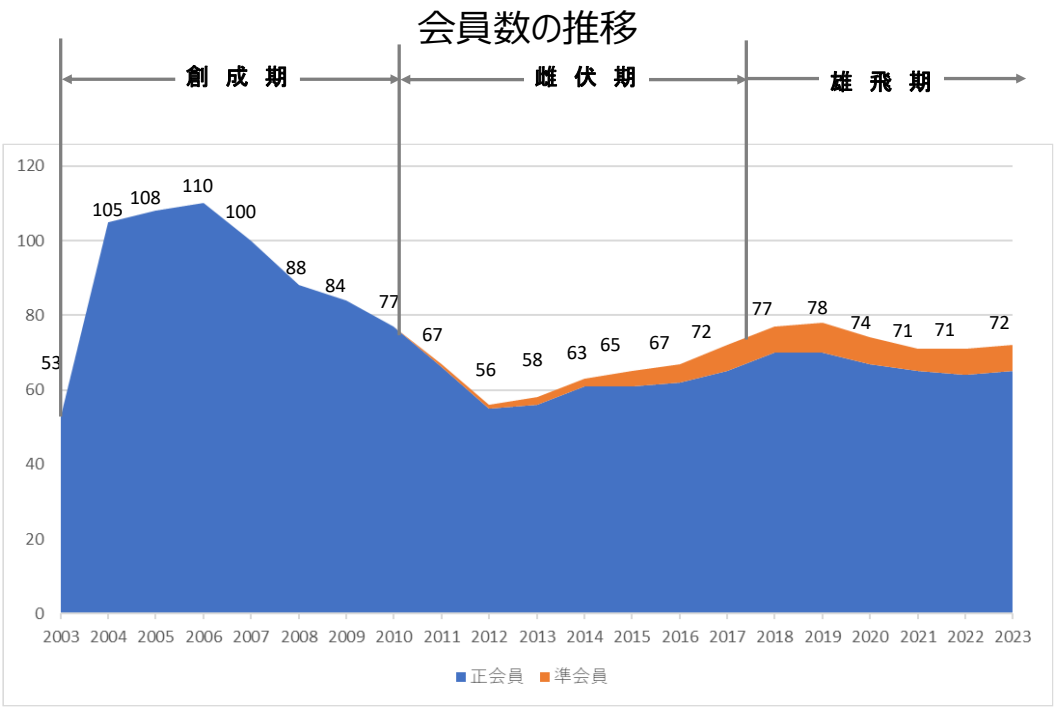
第一期は2003年の制度創設から2009年度まで、第二期は2010年から2017年度まで、そして、第三期が2018年度以降です。

第一期は制度の創設から情報セキュリティ監査の具体化までの期間です。ここではこの時期を創成期と名付けました。

第二期は、2010年度から2017年度までの逆風の機関です。次の飛躍に向けて耐えた時期ということで、雌伏期と名付けました。

第三期が2018年度以降の審査業務が加わって以降の時期です。次の20年に向けて羽ばたく時期ということで、遊飛期と呼びます。



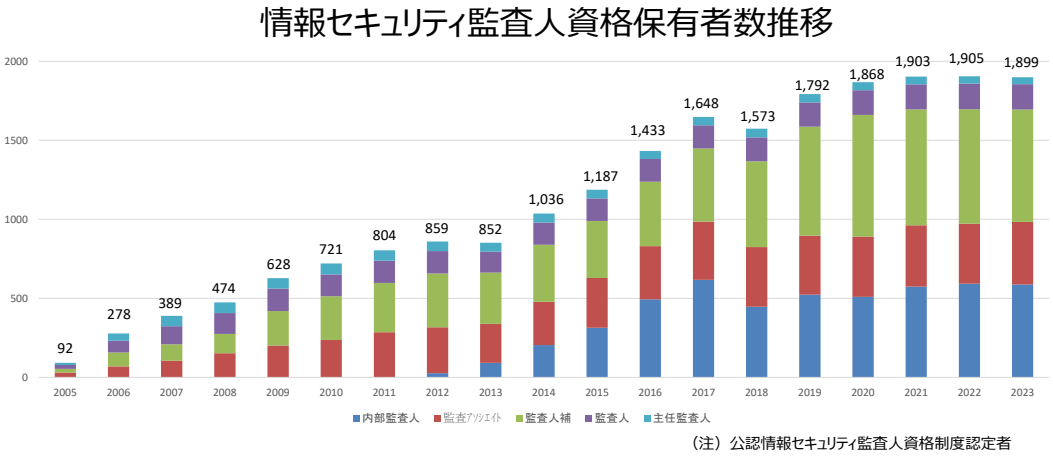


（２）JASA 会員数の推移

上の図は、JASA会員数の推移です。やはりピークは3年目（2005年）で110社ありました。一番少ない時期には約半分に減りましたが、現在は盛り返して少しずつ増加しているものの、ピーク時の7割ぐらいで推移しています。

（３）情報セキュリティ監査人資格保有者数の推移

下の図は情報セキュリティ監査人資格保有者（内部監査人能力認定者を含む）の推移です。一番上の青色が公認情報セキュリティ主任監査人、紫色が公認情報セキュリティ監査人、緑色が情報セキュリティ監査人補、橙色が情報セキュリティ監査アソシエイトです。



（注）公認情報セキュリティ監査人資格制度認定者

図で分かる通り、2020年度までは情報セキュリティ監査人の資格保有者数順調に増えております。そして、2020年以降はおよそ1900人で横ばいです。

監査制度の創設時に資格保有者の目標を2000人としました。20年掛ってようやく目標を達成した状況です。

（４）イベント参加者数の推移

下の図は集客イベントの動向です。

2009年頃までは、政府の支援もあり大規模イベントを行った結果、年間2000名の集客ができました。その後イベント開催ができないこともあり、集客状況は低下し続け、一時は年間500名を割る年もありましたが、最近は増加傾向になっており、ここ2カ年度は年1000名を超えています。

この増加理由はWEB開催です。コロナ過で集会ができなくなり、Webセミナーに切り替わりました。その結果、夜に自宅でもセミナー参加できることに価値があると思います。また、遠隔地に住む方々も参加しやすくなりました。

参加者の割合も大きく変わりました。創設当初はオレンジ色で示す一般の方が非常に多く、情報セキュリティ監査を理解していただくという普及促進活動であったことが分かります。

2010年ぐらいからは前述した資格制度の効果で監査人（青色部分）が増えてきました。それに伴い、監査人を対象とした専門家向けのイベントが主体となってきました。つまり、当初の「情報セキュリティとは何か？」という内容から「情報セキュリティ監査とはどのような内容なのか、監査はどうやるのか」というように、イベント内容が変わってきたのです。

（新しい酒は新しい革袋に）
－2010年から2017年

（１）雌伏期の運営基本方針

さて、2010年から雌伏期と申し上げました。雌伏期は、非常につらい時代なので経営としては守りの経営に入らざるを得ない時期でした。

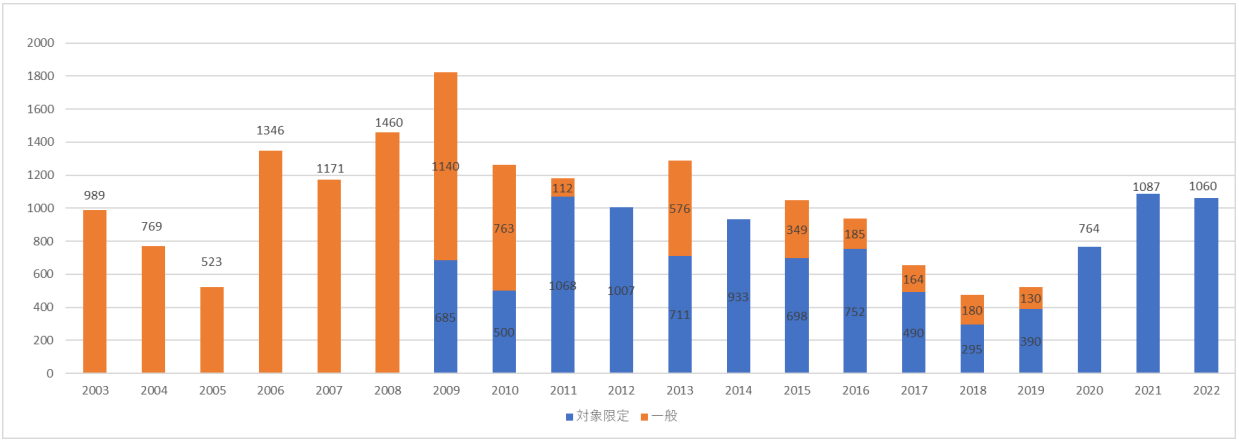
守りの経営の方針は次の２点です。

① 事業体として最低限のリソースで制度運営する

② 教育研修事業により、監査人材育成を確実に進める

JASAの体制縮小し人件費を抑えるため、2010年4月に10名いた事務局員を翌年4月には3名まで減らしました。最低限の人数にしたわけです。また、テナントビルにあったオフィスを会員企業のビルに間借りすることで出費を抑えました。ただし、やるべきことはきっちりとやろうということで、教育研修事業

イベント参加者の種別（一般／限定）参加人数



により監査人材育成を確実に進めることとしました。このため、情報セキュリティ内部監査人能力認定制度を2011年4月から開始したわけです。また、イベント内容を見直し、監査人の能力に向上に寄与するように、有識者から最新の情報を吸収し、或いはJASAのWGの成果を報告するなどの目的とする月例会と名付けた勉強会を開催するように方針転換をしました。

一方で、将来の布石も重要と考えました。この点については、3つの施策をとることにしました。

① 監査品質確保のための指針の明確化
② 情報セキュリティ監査を世に問う出版
③ 新業態に対応した情報セキュリティ監査への取り組み

情報セキュリティ監査の品質確保のために、情報セキュリティ監査基準とそれに基づく情報セキュリティ報告基準ガイドラインが2004年に公開されています。一方で具体的な監査のプロセスに従って行う品質管理の要点は、監査人の経験に委ねていました。このままでは資格取得してから一定の品質水準の監査を実施できるまでに、相当の時間を要します。これを改善するために、2012年度から監査実務指針の策定に取り組み、2012年12月に監査組織を対象とした情報セキュリティ監査実務指針（第一部）一般指針をとりまとめ、2014年4月に具体的な監査プロジェクトの指針となる（第二部）助言型情報セキュリティ監査実務指針を策定しました。

出版の取り組みは、2012年10月にAPT対策入門、2013年3月に情報セキュリティ監査内部教科書の二つをまとめて世に問いました。APTとはAdvanced Persistent Threat（高度で執拗な攻撃）の頭文字をとったもので、高度サイバー攻撃を意味します。サイバー攻撃の手口と対応、そして監査の方法を解説したユニークな本です。

情報セキュリティ監査は会計監査などに比較すると新しい制度です。また、その適用はクライアントサーバーシステムやWebシステムなど、インターネットを前提としたシステムに適用しやすいものです。このため、新たに生まれたシステムサービスや新業態の方が取り組みやすいと考えました、「新しい酒は新しい革袋に」というわけです。

具体的に新サービス・新業態に向けた監査の取り組みとしては、「クラウド情報セキュリティ監査制度」と「スマートメーターシステム情報セキュリティ監査制度」が挙げられます。これらについては、少し詳しくお話をします。

（２）クラウド情報セキュリティ監査制度

クラウドの情報セキュリティ対策は、2009年に経済産業省が行ったISMSユーザー500組織を対象としたアンケート結果で、「セキュリティに関する情報の不足」が最も多かったことから本格的な検討が始まりました。2011年にはクラウドサービス利用のための情報セキュリティマネジメントガイドラインが公開されました。このガイドラインはJIS Q 27002の管理策毎に、クラウドサービスを利用するためにクラウド利用者が事業者に要求する情報や機能を定義し、クラウド事業者これに基づき必要な情報や機能を提供するという共同責任モデルに基づいています。なお、このガイドラインは2012年にISO/IEC27002が改訂されたため、2013年に改訂されています。

経済産業省がこのガイドラインを国際標準とすべくISOに提案し、それが認められクラウドサービスに関する規格開発プロジェクトが始動したわけです。これが2015年にISO/IEC27017として発行されるということつながっています。

一方で、ガイドラインに基づく監査が必要とされることから、監査の基準となるクラウド情報セキュリティ管理基準を2012年に公開しました。

既にISO化の目処がついていたため、クラウド情報セキュリティ監査制度を開発し、実施する組織として、2013年に JASAの下部組織としてJASA-クラウドセキュリティ推進協議会が発足しました。この協議会に参加していただいたクラウド事業者と監査機関の努力により、パイロット監査を踏まえて、2015年にクラウド情報セキュリティ監査制度を開始することがで

きたのです。

クラウド情報セキュリティ監査制度では、クラウド情報セキュリティ管理基準に基づく標準的な監査の方法を定義し、その方法で監査を行ったクラウドサービスCSマークの使用を許諾します。使用許諾を受けたサービスはCSマークのロゴをWebページなどに表示することができます。このロゴを確認することで、利用者は、クラウドサービス利用のための情報セキュリティマネジメントガイドラインに従ったクラウド事業者のセキュリティ対策について、セキュリティ監査が適切に行われていることが分かり、安心してサービス利用ができるようになるわけです。

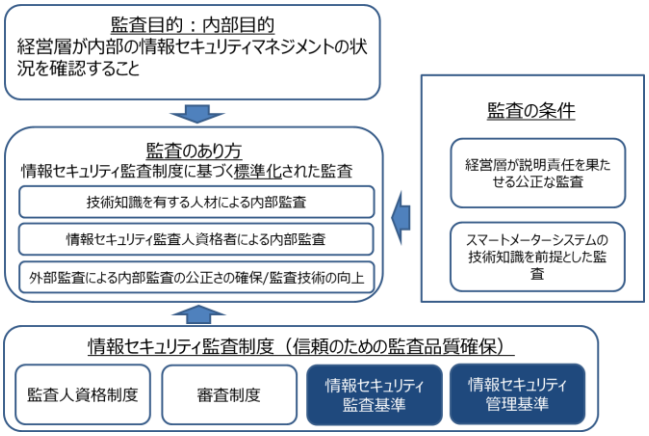
CS マーク
言明書に付与

（３）スマートメーターシステム情報セキュリティ監査制度

2016年4月に電力小売自由化が行われました。スマートメーターシステムは小売自由化のための手段です。各家庭にスマートメーターを設置し、電気使用量を計測します。このデータを送配電事業者が収集し、契約している小売事業者に渡す情報システムがスマートメーターシステムです。従来は発電事業・送電事業・小売業を一つの電力会社で行っていましたが、複数の小売事業者にデータを配信するため、スマートメーターシステムはオープン系のシステムとなっています。このように送配電事業単体の業態の出現に応じた新しいシステムなのです。

電力事業のセキュリティは、従来、経済産業省が直接検査する制度でしたが、オープン系のシステムになったために新しい評価制度が必要となります。経済産業省の検討の結果、オープン系のセキュリティ評価に適する情報セキュリティ監査制度の仕組みを導入することになりました。これがスマートメーター情報セキュリティ監査制度です。

スマートメーター情報セキュリティ監査制度の概要は次の図に示す通りです。



監査の目的は内部監査です。送配電事業者の経営層が対外的な説明責任を果たせ、かつスマートメーターシステムの技術を前提として監査を行えるために次のような工夫をしています。

- 公認情報セキュリティ監査資格取得者が加わることで監査の品質を保つことのチームに加えること
- 技術知識を有する人が監査チームに加わること
- 内部監査の独立性ガイドラインなどに準拠すること
- 標準的な監査手続により事業者間での監査のばらつきを少なくすること
- 外部監査人が監査の適切性を確認すること

スマートメーターシステム情報セキュリティ監査制度の設立時は、JASAが支援しました。現在は電気事業連合会が制度運用されていらっしゃいます。

（４）雌伏期のまとめ

この時代の一つの大きな変化っていうのは日本年金機構の情報漏洩事案です。2015年5月に発覚した事案では125万の個人情報が漏洩したと報じられ、国会でも取り上げられました。その副次効果で、日本は本当にセキュリティ監査しなければいけないという機運になりました。

その前年にサイバーセキュリティ基本法が改正され、国家機関への情報セキュリティ監査をNISCが行うことになっていました。当初は省庁から順次政府機関等に拡大される予定でした。

日本年金機構の情報漏洩事案の結果、独立行政法事等への監査の実施が前倒しされて、2016年度から実施されるようになっています。独立行政法人等への監査は独立行政法人情報処理推進機構（IPA）がNISCより委託を受けて実施します。IPAは情報セキュリティ監査制度に則り、独立行政法人等の情報セキュリティ監査を行うことを決定し、今日まで監査が行われています。

既に、実施されていた地方公共団体の情報セキュリティ監査に加えて、政府の動きにより公共セクターでの情報セキュリティ監査が広く実施されるようになりました。

§４【雄飛期】情報セキュリティ監査制度の新展開 *2018* 年以降

先ほどご説明した収益動向で明確に分かるのは、2018年度以降、JASAの収益が大きく増加しました。その理由は二つの制度が新たに設けられ、その制度にJASAが大きくかかわるようになったことです。これにより、情報セキュリティ監査制度の運営主体であるJASAは審査機関としての役割も担うようになりました。また、それぞれの制度が情報セキュリティ監査の普及に大きな推進力を与えているのです。

（１）情報セキュリティサービス審査登録制度

１つ目の制度は、情報セキュリティサービス審査登録制度です。わが国の情報セキュリティを維持向上するためには、質の良い情報セキュリティサービスの提供が不可欠です。わが国には多くの情報セキュリティサービス事業者が存在します。その中には技術的には優れていますが、小規模な専門家集団で、あまり社会的に知られていないものも含まれます。一方で「安かろう、悪かろう」の不心得な事業者が混じる懸念もあります。利用者が安心して情報セキュリティサービスを選択できるようするための制度が、この制度です。

情報セキュリティサービス審査登録制度の仕組みは以下の通りです。

① 国から審査基準（情報セキュリティサービス基準）を告示する
② 民間の審査機関が基準に適合しているかどうかを審査する
③ 情報処理推進機構（IPA）は審査機関の審査が適正かを審査し、適正な審査に基づくサービスのリスト（情報セキュリティサービス基準適合サービスリスト）を公開する

②の審査のために、経済産業省が「情報セキュリティサービスに関する審査登録機関基準」を公開しています。JASAはこの制度策定に協力し、制度立ち上げ時から情報セキュリティサービスに関する審査登録機関基準を満たした審査機関として役割を果たしています。

この制度の対象となるサービスは、当初４サービス（情報セキュリティ監査サービス、脆弱性検査サービス、デジタルフォレンジックサービス、セキュリティ監視・運用サービス）で開始しました。今年7月現在で、合計274サービスが登録されています。なお、今年末から機器検証サービスが追加される予定です。

（２）政府情報システムのためのセキュリティ評価制度

２つ目はISMAP（政府情報システムのためのセキュリティ評価制度）です。ISMAPは、政府機関が利用するクラウドサービスのセキュリティを評価するために設けられました。

政府はクラウドバイデフォルトを宣言しています。新たな政府情報システムは、クラウドサービスを利用することが原則となっているのです。政府機関という機密性の高い情報を取り扱う組織は、セキュリティが確保されたクラウドサービスを選択しなければなりません。従来は、調達する個々の政府機関が各々独自にセキュリティの評価をしていました。しかし、複数の政府機関が利用するクラウドサービスについて、各々がセキュリティ評価をするのは政府全体としては無駄ですし、クラウド事業者にも負担が大きくなります。そ

こで、政府としての統一的な評価の枠組みを作成し、一定レベルのセキュリティ水準を満たしていると判断されるクラウドサービスをあらかじめ評価し、ISMAPクラウドサービスリストとして公開することとしました。このリストはわが国で初めて、クラウドサービスの安全性を評価したものです。リストは一般にも公開されていますので、民間企業や地方自治体が安全なクラウドサービスを選択するためにも役立ちます。わが国全体に対して有益な情報を提供できる制度がISMAPです。

クラウドサービスを審査登録するためにクラウドサービスプロバイダは、あらかじめ政府が認定する監査機関による監査を受け、監査結果を添付して申請します。この監査機関が政府の定める監査機関の要件を満たしているかについては、クラウドサービスを審査する運営支援機関であるIPAの委託を受けてJASAが審査を行っております。

ISMAPの制度策定時には、雌伏期の2015年に開始したクラウド情報セキュリティ監査制度のノウハウが役に立ちました。JASAはISMAPに全面的に協力してノウハウや人材を提供しています。その結果、ISMAPは情報セキュリティ監査制度に基づく制度となりました。また、監査機関は情報セキュリティサービス基準適合サービスリストに掲載された監査サービス提供事業であることが求められることになったのです。

§5　20 年の成果と課題

先ほど述べたように、現在、公認情報セキュリティ監査人資格認定制度の資格認定者数は1,900人です。当初目標としていた2,000名にほぼ達しています。

また、公的セクターで情報セキュリティ監査は定着しつつあるといえます。

また、審査委員会を設けましたが、そこで審議するような事故は発生しませんでした。これらが20年の成果として評価してよいことと思います。

一方で、これからやらなければいけないことは何か考えますと、一つは、中小規模自治体及び民間セクターへ情報セキュリティ監査を普及していくことです。特にサプライチェーンを構成するような中小企業には監査は必要になるだろうと考えます。また、自治体はDXやマイナンバーへの取り組みがあり、監査の必要性が高まっている状況にあります。適切な監査が実施されるように、これらに対して適切な手立てを用意する必要があります。

それから、サイバーセキュリティ対策などの新しいセキュリティ課題へ取り組んでいくことも必要です。

さらには新しいセキュリティ実装技術に対する監査技術の研究や監査人の技能向上にも取り組む必要があると思います。例えば、DXが浸透すると重要視されるゼロトラストアーキテクチャ（ZTA：Zero Trust Architecture ゼロトラストセキュリティモデルに基づくセキュリティアーキテクチャ）が挙げられます。

最後に、監査に、AIを使うことも含め、IT技術を駆使したような監査をすることで、より的確でタイムリーなアウトプットを出していくということが必要になっていくと思います。

§6　謝辞

駆け足で制度創設からの20年を見てきました。本当に山あり谷ありでした。20年間ご支援、ご協力大変ありがとうございました。おかげさまで今日ここまでたどり着くことができました。

最後に情報セキュリティ監査制度の発足をもたらした研究会の巻頭言を記載します。次の時代を担う人々に、創設時の人々の思いに共感を持って、更なる発展を遂げていただきたいと思います。

「我が国において『情報セキュリティ監査』が根付き、有効な制度として機能するためには、その監査事例や紛争処理案件の積み重ねが必須である。また、監査を行う主体の裾野を広げ、その専門性を高めていくことが必要である。『情報セキュリティ監査』を担う主体は、様々な主体であることから、互いにその連携を深め、事例の蓄積、監査を行う主体のスキルの向上などが、有機的に行われていく体制が構築されることを期待したい。」

パネルディスカッション 1

女性が活躍するこれからの情報セキュリティ監査

モデレータ

リコージャパン株式会社　　辻井 葉子 様

パネリスト

PwCあらた有限責任監査法人　加藤 俊直 様

日本マイクロソフト株式会社　後藤 里奈 様

株式会社日立システムズ　　坂本 美子 様

NTTテクノクロス株式会社　　土屋 直子 様

【オープニング】

◆モデレータ　リコージャパン　辻井様

ただいまから「女性が活躍するこれからの情報セキュリティ監査」というテーマで、この楽しみな 4 人のパネリストに存分にお話しいただきます。

情報セキュリティとか情報セキュリティ監査という言葉を聞くと、どうしても少しハードルが高い、難しくて堅いイメージが湧いてしまうかと思いますが、今日、登壇いただいているパネリストの皆様は、非常に軽やかに楽しんで情報セキュリティのお仕事をされていらっしゃると思います。

今日のこのテーマのヒントがその辺りにあるのかと思い、ざっくばらんにこの皆様のお話をお聞きできるように引き出していきたいと思っております。

会場の皆様も、肩に力を入れずにリラックスして聴いていただければ嬉しく思います。

【自己紹介】

◆NTT テクノクロス　土屋様

私は NTT テクノクロスのコンサルティング部署で ISMS や ISO/IEC 27017 のコンサルティング活動に従事しています。セキュリティ監査に関してはコンサルティングを通してお客様の内部監査等を実施しています。

同時に、2015 年に JASA の国際標準化ワーキンググループに参加し、そこで初めて標準化活動に携わりました。かなりやりがいを感じ、その翌年、2016 年からは ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27017 などを開発する SC27/WG1 小委員会において ISO 委員として参加しています。主に、ISO/IEC 27002 や ISO/IEC 27017 の改訂活動に携わっています。監査との関係でいえば、情報セキュリティ管理基準は主に ISO 規格がベースとなっているので、標準化活動を通して、これらの監査の基準をより深く理解することができるという観点で、情報セキュリティ監査にもプラスに働いていると思っています。

◆日立システムズ　坂本様

私は今、社内のセキュリティガバナンス統括部門で社内の全社セキュリティ人材育成に携わっています。

監査、JASA との出会いですが、入社時はネットワークの部署に配属でしたが、これからはセキュリティだということで異動があり、ISMS の認証取得や個人情報保護法対応等のお客様の支援にあたる業務になりました。コンサルティングを行うには監査の視点が必要だと、2007 年にセキュリティ監査人の資格を取得したのが JASA との始まりというところです。

その後、2017 年にサイバーセキュリティ机上演習ワーキンググループができ、監査人の視点を使いながら、人材育成の観点で、セキュリティインシデントが起きたらどのようなことになるのか、組織内で不足している規程類はないのか、体制は大丈夫かという確認ができる机上演習をワーキンググループで作成しました。そして、その内容を自社に持ち帰り、現在、社内のセキュリティ人材育成に当てはめて机上演習を活用しています。

◆日本マイクロソフト　後藤様

私の業務は、マイクロソフトのセキュリティソリューション（Microsoft365 等）のマーケティングです。

JASA との関わりは、マイクロソフト入社前に遡り、土屋さんと同じく国際標準化ワーキンググループと、それに関連して、ITSCJ の SC27 の国内・国際の委員をやっています。そのように、前職の頃から標準化、特に最初のバージョンの 27017 の策定時に国際プロジェクトに参加しました。

そこからいろいろなご縁があり、前職の CS マークのシルバー取得に携わったり、少し監査の経験もしながら、今は本業はセキュリティ関連ですが、引き続き国際関連の活動も続けており、27017 改訂の国際のエディターとして開発プロジェクトを進めています。

◆PwC あらた有限責任監査法人　加藤様

JASA20 周年、本当におめでとうございます。20 年とは本当に長い期間だと思いながら、先ほどの皆さんの話を聴いておりました。

私は今、監査法人という名前からお分かりのとおり、いわゆる会計監査の中でシステム、セキュリティ等をみる業務、また、委託先やサプライチェーンに対して保障を与えるような業務で、指導的な役割としてセキュリティやプロジェクトに対して監査の目線から改善等を感じていただくことをやっています。

JASA には、CS マーク立ち上げの際、そもそも何を誰に対してどのようにやるのかということを考えるところから入りました。現在は普及促進のところで、10 大トレンドにも関わっています。

【ディスカッション】

仕事上の男女差について

◆モデレータ　リコージャパン　辻井様

テーマが「女性が活躍するこれからの情報セキュリティ監査」ということで、情報セキュリティや監査の世界で女性の割合はどのぐらいかと、JASAのホームページに公開されているセキュリティ監査人メンバー 一覧を拝見したところ、女性は全体の1割ぐらいでした。1割だとやはり結構少ない印象がありました。また、今日も来場者のうち、女性は多くないと感じます。

ということで、パネリストの皆様に、実際に情報セキュリティや監査のお仕事をされる中で女性は少ないと感じていますか、また、女性だから男性だからということで、何か意識したことはあるかを質問させていただきます。

◆NTTテクノクロス　土屋様

私は ISMS 等のコンサルティング部署に配属される前はソフトウェア開発の部署でしたので、やはり男性が非常に多く、学生時代とは違うカルチャーショックのようなものを受けました。その後、ISMS のコンサルティングの部署に異動したところ、女性のコンサルタントがかなり活躍していて、自分の周りでは、それほど男性が多いという感じはしません。ただ、お客様のところへ行って監査をすると、やはり男性が多いのかなと思います。

自分自身が監査をする中で、女性とか男性とかということは特に意識せずに、日々のセキュリティ監査やコンサルティング業務に携わっています。

◆モデレータ　リコージャパン　辻井様

やはりコンサルティングという形になると、女性のロールモデルの方も結構いらっしゃるということですね。

◆NTTテクノクロス　土屋様

そうですね。コンサルティングや監査で求められるスキルをみても、例えば、コミュニケーションスキル、報告書を作る文書作成スキル、あるいはセキュリティの技

術的な知識やマネジメントの知識など、特に女性とか男性とかを意識する必要はあまりないのかなと感じています。

◆日立システムズ　坂本様

ITの会社なのでやはり女性が1～2割で、他のIT企業も似ているかと思います。お客様先に行っても男性の方ばかりですが、そこの男女差についてすごく苦労したということがなく、周りの男性が支えてくださっているところもあります。

私は、子どもを出産して産休・育休を取ったことも周りにケアしてもらいながら、また、男性も育休も取っていて、良い効果も生み出しながらやれています。

地方対応に関してはリモート監査もできるようになってきたので、ますます女性も活躍できる時代になってきたと感じています。

◆モデレータ　リコージャパン　辻井様

いろいろなライフイベントがあっても続けやすかったということですね。

◆日本マイクロソフト　後藤様

当社はグローバル企業ということもあり、男女比率には非常に気を遣っています。完全な 1 対 1 ではありませんが、女性 1 に対し男性 2 くらいか、もう少し小さいくらいの比率で、セキュリティに関するセールス、サポート、エンジニアリングに至るまで配置されています。エンジニアリングは男性が多めですが、基本的に男女 1 対 1 を理想として人の採用もしています。

仕事をする上では全くフラットな条件ですし、それは逆に男性側にもということで、例えば男性も普通に育児休暇を長期間取ることは推奨されており、業務上で性別を理由にした不利益というものは一切ありません。

では、世界を見たときということですが、ISO では、SC27 のワーキンググループのうち WG1 が、いわゆる ISMS マネジメントシステムを扱っているところで、こちらは恐らく実数でいうと女性が多いと思います。6 割ぐらいが女性ではないかというところで、各国世界中からあらゆる形のエキスパートが集まっているのですが、皆さんパワフルで素晴らしい活躍をされている方がたくさんいる状況です。

◆モデレータ　リコージャパン　辻井様

6 割が女性というのは驚きましたが、日本と、国際的には 6 割ぐらいが女性というところとの違いはどのようなところにあると思いますか。

◆日本マイクロソフト　後藤様

日本と、国際的には 6 割ぐらいが女性というところとの違いは、各国経済状況が違うので、単純比較は難しいですが、例えば私は今年からアジアのチームで働いているので、同僚がインドやシンガポールに住んでいて、家事のサポートが手厚いということがあります。家に来て掃除をしてくれる人を簡単に雇える等があり、やはり業務の上では男女公平でも家庭内のバランスはまだまだ、子育てや普段の家事など、どうしても女性に寄ってしまうところがあると思いますが、そこまで配慮されているのは、一つ大きなポイントだと思います。

◆モデレータ　リコージャパン　辻井様

そういうところまで、サポートがあると無いではやはり思い切ってやるかやらないかのところに違いが出てくるのかと思います。

では、加藤さん、唯一の男性の目線からご覧になって、やはりセキュリティ監査のお仕事をされている中で、女性の割合についてどのように感じていらっしゃいますか？多いですか？

◆PwC あらた有限責任監査法人　加藤様

監査法人という全体で見た場合の姿というところと、情報セキュリティに関わるところの二点でお話しします。

監査法人は、情報セキュリティやリスクマネジメントをやっている部門と、いわゆる会計監査を行う部門があり、公認会計士試験合格者の割合をみると、2 割から 2 割 5 分くらいが女性なので、監査法人に入社

されるのは、その割合から大きく離れられないという制約のようなところがあります。

一方で、我々の情報セキュリティやリスクマネジメントを行っている部門の中で、新規採用（大卒の新卒採用）は全く別の景色で、純粋にみるとそれほど差はありません。ところが、年によっては何か評価や基準を設けたわけではなく、8 割が女性という年もあったことがあり、そういうところから男女の差というものはないと思っております。また、仕事の中でも男女の差は正直感じたところはないです。

先ほど、育児の話、家庭内の話がありましたが、私の個人的な話をしますと、昨年 12 月に実母が亡くなりまして、3月くらいから癌で闘病していたという事がございました。父の老老看護・老老介護と合わせて、ある程度のサポートをしなくてはいけないということがありました。これは、常駐型や常に毎日が期限のような仕事だったら、正直、厳しかったと思うのですが、周りの皆さんの大きな支えがあったこともありますが、仕事や、その内容というところも含めて、情報セキュリティ監査というのは、プライベートの方に時間を取るのが難しい状況においても仕事を続けることができるのだと感じました。自分自身でもそのような経験もありましたので、あまり男女差という形ではなくて、プライベートと仕事の割合（ライフサイクルやライフイベントの状況によっても違うとは思うが）を調整しながらできる仕事だと感じています。

◆モデレータ リコージャパン 辻井様

プライベートとも両立がしやすい仕事というのも、情報セキュリティ監査に関連する新しいメリットというか、もっと皆さんに伝えたい部分なのかもしれないと思いました。

このようにお話を聞いていくと、皆様の会社や、周りの皆さんの状況はあまり男女差のようなものは感じていらっしゃらない印象を受けますので、こういった方がもっと増えてくると、セキュリティ人材の足りない部分というのをもっと拡充できるのかなと思いながら聞かせていただきました。

セキュリティとの出会い

◆モデレータ リコージャパン 辻井様

実際、私も最初からセキュリティの世界にいたわけではなくて、きっかけがあって途中からセキュリティの世界に入ったのですが、皆様がセキュリティのお仕事に入られたのは、ご自分からやりたいと入られたのか、それとも異動や何かがあって、最初は受け身的にセキュリティの世界に入られたのか、どちらが多いのかが気になったのですが、いかがでしょうか。

◆NTT テクノクロス 土屋様

私は入社して初めて配属された部署がセキュリティアプリケーションを開発する部署で、そこがセキュリティとの出会いでした。なので、自分の意思ではなかったです。また、学生時代は全く分野の違うことを勉強しておりましたので、何も分からず配属されたところがセキュリティの開発部署という感じでした。

その後、ISMS のコンサルティングの部署に異動して、セキュリティのコンサルティングに携わるようになり、標準化活動については、自分からドアを叩いてみました。

◆モデレータ リコージャパン 辻井様

最初にセキュリティの部署になった時はどのような感想をお持ちでしたか？

◆NTT テクノクロス 土屋様

セキュリティというより開発自体が初めてでした。学生時代は文系で国際関係学を勉強しており、全く違う分野でしたから、何もかも初めてでした。開発も初めてですし、社会に出て会社勤めというのも初めてで、かなり戸惑ったのを覚えています。

◆モデレータ リコージャパン 辻井様

新卒の方たちに向けても、今のお話などは届くと良いと思いますが、セキュリティの仕事はこうだよというのを何か一言アドバイスしてあげるとしたら、どういう言葉がありますでしょうか。

◆NTT テクノクロス　土屋様

私は入社後、セキュリティの部署に配属されてから、ずっとセキュリティをやってきています。最初は初めてのことが多く大変でしたが、セキュリティといっても分野がかなり広いんだなと感じるようになりました。例えば、開発などの技術系だけではなく、ISMS などのマネジメント系、また、ISO の国際会議に参加するにあたり、語学系のスキルも活かすことができます。このように、本当に多様なバックグラウンドの方が活躍できるところだと思っています。例えば国内の SC27/WG1 小委員会でも、多様なバックグラウンドの方が自分の強みを生かして貢献していますので、セキュリティは分野が広いということを伝えたいと思います。

◆モデレータ　リコージャパン　辻井様

強みを生かして、いうことですね。

坂本さんは、先ほど、これからはセキュリティだということをお話しされましたが、ご自分の意思でセキュリティの世界の扉を開かれたのでしょうか。

◆日立システムズ　坂本様

組織の改編で自分の意思とは関係なくという形でした。私は大学は理系ですが、セキュリティではない電気電子工学科の理系で、ネットワークが面白そうだなと思って入りました。そこからまたセキュリティという話をもらった時に、セキュリティという言葉がかっこいい、とワクワクした気持ちで異動しました。

その後も ISMS の認証取得で、お客様を何回も訪問して困り事もいろいろ話し、技術面も人の面もいろいろ幅広く関われて非常に楽しくやっています。

◆モデレータ　リコージャパン　辻井様

非常に楽しく関われているという言葉がとても良いと思いました。セキュリティは楽しいというところを是非どんどん発信していきたいのですが、お客様と直接お話をしたりして困り事を解決するところがセキュリティの仕事のやりがいだと感じておられるのですか？

◆日立システムズ　坂本様

そこが大きいと思います。また、今、セキュリティ人材育成で、技術面の高度セキュリティ人材を育成するとともに、プラスセキュリティ人材も育成しなくてはいけないところで、なぜセキュリティが必要なのかと思う方がまだまだいるのですが、経営課題だというところから話して解ってくれた瞬間が嬉しいとか、セキュリティを刷り込んでいることが楽しく感じているところです。

◆モデレータ　リコージャパン　辻井様

刷り込みは大事ですね。

セキュリティの監査に行きますというと、どうしても招かれざる客のように思われがちですが、全然そのようなことはなく、一緒に良くしていこう、と、むしろ招きたくなる客と言いますか、一年に一回、健康診断のように来てくださいと言われるぐらいになりたいですね。

後藤さんはセキュリティの世界に入られたきっかけはどういうところだったのでしょうか。

◆日本マイクロソフト　後藤様

私は社会人歴 13～14 年くらいの中で、セキュリティを業務としてやっているのはここ 3～4 年だけです。今のマイクロソフトセキュリティのマーケティングが、初めてセキュリティに関連するもので、それまでの期間は、本業がクラウドサービスのマーケティングで、営業職をやっていた時もあります。パラレルキャリアではないのですが、副業的に本業プラスアルファでセキュリティをやっていました。

セキュリティをやったきっかけは、新卒で入った会社で英語翻訳チェックの仕事があり、それが国際会議に持って行く ISO27017 のコメントだったのです。その後、チェックした内容が良かったということで、留学経験も国際経験もなかったのですが、香港に行ってみないかという話をもらいました。香港は行ったことがなく、海外旅行も二歳のとき以来していませんでしたので、海外への憧れのようなものがあり、気軽に手を挙げてしまい、そこからです。いろいろな会議に参加し、自分でもコメントを出したりして、少しずつ勉強をしていった

のが実態です。

私は、文系しかない大学でマーケティングを勉強していましたが、当時大学の IT 教育もあまり充実しておらず、エンジニアリングの知識もゼロでした。

何から勉強すればいいのかというところから周りに相談し、少しずつ勉強しました。また、CAIS などの資格も取得し、10 年くらいかけて少しずつ力をつけていきました。

◆モデレータ リコージャパン 辻井様

ゼロから学んでいくには「情報セキュリティは面白そうだ」という興味を持つと勉強も楽しくできると思うのですが、セキュリティと言われた時に、後藤さんはどのようなところにモチベーションを持っておられたのでしょうか。

◆日本マイクロソフト 後藤様

最初の入口が、セキュリティのマネジメントや監査という、どちらかというと会社全体のプロセスに関わるところだったのが、一つ幸運だったと思います。広く浅くでも全体像を捉えて、次は自分のために何を勉強すれば良いのかが分かりやすかったです。

また、私が大学時代に専攻していたマーケティングはやはりマネジメントなのです。したがって細かい知識ではなく根底の考え方のところで共通している部分、いかに会社の事業に繋げていくかという共通性があったところで、上手く入ることができたのだろうと思っています。

◆モデレータ リコージャパン 辻井様

セキュリティというと技術的なイメージが強くなりますが、会社の経営に関わるマネジメントということが大きかったのですね。

加藤さんは、もともとずっと情報セキュリティの監査をされておられたわけではないのでしょうか。

◆PwC あらた有限責任監査法人 加藤様

私は、公認会計士試験は大学の時に合格したのですが、ファーストキャリアは監査法人ではなくコンサルティングファームで、システム開発・運用をしておりました。そこから、いわゆる経営改善や企画などの仕事を 15 年弱くらいしていました。

セキュリティは、監査法人に入ってからやったのかというとそうではなく、Y2K（2000 年）問題でシステムが使えなくなったらどうするという可用性の観点や、当時は小売業のコンサルティングをやっていたので、データがおかしくなると売値と利益が分からず商売ができないなどと、お客様にかなり育ててもらったところがあり、完全性に関して厳しくみていたのだということを、今、改めて考えます。

どちらかというと今は機密性や、サイバー攻撃などがあって可用性にもう一度焦点が当たっていますが、完全性や、その辺りのところに私のセキュリティの原点があったのではないかと思っています。仕事内容はどんどん変わっていますが、多くの期間、セキュリティに関わっていたということを改めて感じています。

セキュリティや監査がすごく遠いところの話ではなく、本当に身近なところの話であり、経営意思決定にも直結している大事な仕事だというところを、本日参加していない方にアピールしていければと思います。

◆モデレータ リコージャパン 辻井様

本当に身近な話であり、なおかつセキュリティは経営の意思決定にも非常に関わるとても重要な仕事だということで、誇りを持って自慢していただきたいぐらいの仕事だということを伝えていきたいと思います。

加藤さんは、セキュリティの仕事のやりがいや、これが嬉しかったという出来事は何かありますか。

◆PwC あらた有限責任監査法人 加藤様

セキュリティに携わった前半部分がコンサルで、どちらかというと一緒に作り上げていく形でした。監査法人に入って、そういう仕事もありながら一方で評価をするような形（保証することも含む）で、どちらかというと長期間、お客様と継続的に付き合う経験が多くなったと思っています。自分でやってしまうと自己監査につながってしまうところもあるので、お客様に、どのよ

うにしたら上手くいくか伝えながら手立てなどを業務提供して一年、二年経ち、セキュリティの穴が整理されていって、すごく良くなりましたねと言える時が、やはりコンサルティングをやっていた時にはなかなかなかった、ちょっと嬉しい経験ができるようになったと思っていました。監査というものは本当に一瞬のことでももちろんできるのですが、長いスパンでやっていくと味わい深いというところなどは皆さんに共有できれば、と思っています。

◆モデレータ　リコージャパン　辻井様

味わい深い仕事ということですね。とても良いですね。そのようなところを多くの方に知っていただけたら嬉しいです。

セキュリティ監査の拡大

◆モデレータ　リコージャパン　辻井様

皆様の仕事の話を聞かせていただく中で、やはり情報セキュリティ監査の仕事は一般的に思われているイメージとかなり違う、とても良いアプローチが多くあるのに伝わりきれてなく、女性から見たときに自分のキャリアプランとして情報セキュリティ監査を将来やっていきたいという選択肢がなかなかパッと出てこない状況なのでは、と思いました。

では、今後、皆様が感じていらっしゃるようなイメージに変えていくために、どのような活動が必要か、また、このようになったら嬉しいということがあれば聞かせていただきたいと思います。

◆NTT テクノクロス　土屋様

情報セキュリティ監査というと、少し堅いイメージがあり、いくつか要因があると思います。

私が標準化活動に携わっている観点から考えてみると、監査の管理策基準が少し分かりにくいのかとも思います。例えば ISMAP や CS マークの管理策基準は数もたくさんあり、一つ一つ見てみると結構、読むのが難しいと思います。それで監査というと堅いイメージがあるのかなと思います。

管理策基準のベースとなる規格が、もっと分かりやすければ、監査も分かりやすいものになり、イメージも変わるのではないかと思います。

◆モデレータ　リコージャパン　辻井様

確かに少し分かりにくい、取っつきにくい、読んでもよく分からないというイメージはありますね。分かりやすくしていくためにどのような工夫が必要なのでしょうか。お考えがあれば聞かせていただけますか。

◆NTT テクノクロス　土屋様

色々な国際会議に参加する中で、各国から様々な提案が出されますが、その中で、分かりやすく、シンプルで、また、ロジカルな提案が採用されやすいと感じています。最近は、英語の分かりやすさも規格開発において重要視されてきているので、少しでも分かりやすい規格作りができると良いかと思っています。

◆モデレータ　リコージャパン　辻井様

シンプルでロジカルな表現を、ということですね。

やはり、受け取って、それを実際に現場で運用される側の皆さんに寄り添った形のものでないと、大上段に立ったものだとなかなか広がっていかないというところですね。

では、坂本さんが先ほどお話しいただいた、セキュリティはコミュニケーションが大事、またこのような喜びがあるというところが素晴らしいと聞かせていただいたのですが、そのあたりを坂本さんの感じていらっしゃるイメージに変えていくには、どういうことが必要だと思いますか。

◆日立システムズ　坂本様

監査が堅い印象だということですが、私もネットワーク部門にいたときは内部監査を受ける側で準備も大変などのイメージがあったのですが、監査支援や監査側に回った時は、計画に則って実施する、エンジニアのように急に障害対応をするということはなく、自分でプランを立てて計画どおり進めることができる、つまり過程も調整しやすいというところにメリットを感じています。

女性で、エンジニア職でも、子どもが生まれたからと辞めてしまう方や、技術職から離れて別の部門に行ってしまう方もいますが、そのような方に勧めたいと思っています。もともと持っていたスキルはあるので、監査人としてすごく活躍できるはずだと思います。そのようなことも私は周りに伝えています。

◆モデレータ　リコージャパン　辻井様

先ほど加藤さんからも両立がしやすい仕事という話がありましたが、プランを立ててそのとおり進められるという点、急に何かがおこってそこに工数を全部取られるということがあまりない仕事ということですね。

◆日立システムズ　坂本様

加えて、先ほどもお話ししたとおり、リモート監査等の対応ができるようになったところが、長距離出張が難しい方にとっては、とても良い時代になったので、活躍できる人が増えてくると感じています。

◆モデレータ　リコージャパン　辻井様

そういう意味でもやはり女性に向いている仕事ということでしょうか。

◆日立システムズ　坂本様

かなり向いていると思います。

◆モデレータ　リコージャパン　辻井様

それでは後藤さんにも伺いたいのですが、今ある監査や情報セキュリティのイメージをどのように変えていきたいと思われますか。

◆日本マイクロソフト　後藤様

私自身は、今は監査の仕事はしていませんが、まず、監査人のなり方とキャリアパスがもっとクリアでオープンになると良いと思います。

今までのお話から、監査の仕事に入るための障壁はそれほど高くなく、高度な技術的知識よりも、きちんとスケジュールに基づいてやっていくことが求められる仕事であるならば、もっと人気になっても良いと思います。

ただ、私も自分が CAIS 資格の勉強などをする前は、監査のような仕事が存在することすら知りませんでした。大学が文系だということもあり、IT 業界に関する情報がほとんど無く、監査と聞いたら、公認会計士の方の会計監査を思い浮かべます。

IT 監査の方でも、まずこのような仕事が存在して、新卒でも中途でもなることができるということをもう少しオープンに世の中に知らせていくとことが重要なのだろうと思っています。

◆モデレータ　リコージャパン　辻井様

実際、セキュリティ監査の制度や資格を知ったのは、どのような経緯ですか。

◆日本マイクロソフト　後藤様

私は標準化の仕事に携わってから、このような資格あると知りました。JASA と聞いた時にも、正直、セキュリティ監査協会はどのようなことやっているところか全くイメージがつきませんでした。それくらい、やはり監査の仕事というものが、もっと皆さんに知ってもらえたら良いと思いました。

◆モデレータ　リコージャパン　辻井様

後藤さんは普段マーケティングの仕事もされていますが、監査の資格をもっと広く知っていただくためには、どのような広げ方、宣伝の仕方、アプローチの方法が良いと思いますか。

◆日本マイクロソフト　後藤様

誰がやるかも含めて非常に悩ましい問題ではあると思います。やったところで、きれいに今年志望者が何人増えました等の統計が取れるわけでもありません。でも、誰かがやっていくしかないというところはあると思います。少し無責任かもしれませんが助言をさせていただくのであれば、初学者向けのコミュニティを立ち上げて広げていくというアプローチもやっても良い時期なのかと思います。

◆モデレータ　リコージャパン　辻井様

今日のこのパネルディスカッションをきっかけに、新たな刺さり方と言いますか、このパネルディスカッションの結果をどんどん多く広く宣伝していただきたいと思いました。

では加藤さん、このイメージをどのように変えていったら良いかというところでアイデアがあればお聞かせください。

◆PwC あらた有限責任監査法人　加藤様

自分自身の経験ですが、やはり監査（セキュリティ監査、内部監査、会計監査）と聞いてポジティブなイメージを持つ人は多くないだろうと思っています。

私も最初は監査を受ける側でした。そこでの監査に対する第一印象は、なぜ上から目線なのか、ということで最悪でした。まさかそれから 20 年くらい経って、監査人の立場でこのようにしゃべるとは思っていませんでした。

上から目線以外に、監査を受けて良かったと思ってもらえないことの一つに、減点主義でフィードバックされるケースが多いことがあると思います。子育てではないですが、良く出来ているね、ここは良いよね、でもここは全部直した方が良いよねと言われるのと、これとあれが出来ていませんと減点方式で言われるのとで、やはり監査に対する印象がかなり変わると思います。このあたりは監査をやる側としてはしっかり変えていかなくてはいけない部分だと思っています。

さらに、監査人自体のキャリアパスについて、日本では監査はキャリアのゴールのような形で捉えられるケースもあると思います。専門家として独立性も必要、専門性が高いからということで、そのように思われますが、実際は経営企画、IT 部門、営業部門など回転ドアのように監査、内部監査、セキュリティ監査をやって次のキャリアとなるので、このあたりはもう少し社会全体として変えていければと思います。

具体的には、

- 監査とは上から目線でやられるものでもなく、良いところも含めてやっていくことを見る目線というものがある
- どのようにリスクマネジメントをやっていけば良いのかいうところは、視点としてしっかり持てる

という形で、監査を特別なものではなくて、日常の形に持っていけたら良いと思います。

監査を、安心材料を提供する、または、評価のように言い換えすることも、もしかしたら必要なのかと思いながら話を聞いておりました。

◆モデレータ　リコージャパン　辻井様

監査という第三者的な目で見なければいけない、でもやはり寄り添ってしっかりとコミュニケーションをとり、減点主義ではなく、お客様のためになるような監査、一緒にそれを作るような姿勢が大事だということですね。改めて勉強になりました。

【クロージング】

◆モデレータ　リコージャパン　辻井様

それでは、いろいろとお話を伺わせていただいてきて、あと残り 5 分となりました。

今後、監査をどうしていきたいかというところは、この次のパネルディスカッションでさらに深掘りがあると思いますので、そちらにお任せするとして、こちらのセッションはまとめに入っていきたいと思います。では、皆様から、本日ご参加の会場の皆様へのメッセージや、監査に対するこれからの期待を一言いただけますでしょうか。

◆NTT テクノクロス　土屋様

私も初めてセキュリティの監査に従事するにあたって、ISMS 審査員や JASA 公認セキュリティ監査人などの資格を勉強して取得しました。監査の勉強をする中で規格や監査基準の勉強もできますし、現場で監査の経験を積むことによって、規格や監査基準のセキュリティ管理策を現場でどのように具体的に実装しているかも学べるので、セキュリティのスキルや知見を高めるのにとても良いと思っています。

セキュリティ監査というのは、セキュリティをキャリアパスと考えた時には非常に有効に勉強になる場だと思いますので、今後、よりセキュリティ監査が広まっていく

と良いと思っています。

◆日立システムズ　坂本様

本日ご来場の皆様はセキュリティ監査を身近に感じておられる方ばかりかと感じております。本日の話の中でどんどんセキュリティ監査人を増やしていきたいというところも伝わったかと思いますので、ぜひ我々と一緒に監査を盛り上げていけたらと思っています。

◆日本マイクロソフト　後藤様

私のキャリアのほとんどが、この JASA との関わりが作り上げてきたという意味だと、セキュリティ監査は私の人生にも深い関わりを持っているわけですが、監査がどのような役割になって行くかというところも見据えていくと、情報セキュリティに関して、特にクラウドサービスが広がっていくにつれて、ユーザー側がやらなければいけないことが限定的になっていくというところで、たぶん監査のあり方としてもよりプロアクティブであるし、一時点というより、もう少し長い期間でサイバーハイジーン[2]的な考え方を持っていくことが必要になってくるかと思います。

やはりきめ細やかなところは、監査の業務自体もそうですが、女性がまさに活躍できるというところで、これからもどんどん新たな人材を、この世の中に輩出すべく、少しでもお手伝いさせていただければと思います。

◆PwC あらた有限責任監査法人　加藤様

情報セキュリティ監査に関しては、この後、第二部の方で語ってもらうと思いますが、自動化など、かなり効率的になっていくと思っています。

そこで付加価値をどうやってつけていくかというと、やはり多様な人たちが監査にいろいろな形で入っていく中で、さきほどのモチベートするような活動なども含めてやっていければと思っています。

最後なので言ってしまいますと、このテーマをいただいた時に、監査人という全体像ではなく、女性というところにフォーカスが当てられていて、正直困ったと思いましたが、先ほど永宮さんの説明にありましたとおり、資格者は全体としてもっと伸ばしていかなくてはいけない状況があると思っています。

男性女性、監査法人出身、プロバイダー出身、いろいろなバックグラウンドの方がいると分かっているのですが、それがバラバラ感みたいなところがあることが嫌だと思っています。

ラグビーで、前回の東京大会の時は One チームというスローガンで、これはまだ一つになってないから One チームなのだろうと思ったのですが、今回のスローガンが Our チームとなっていました。我々の、という形で皆が自分事でやっていくという、そういうスローガンだったので、この考え方は良いと思っていました。

JASA、それからセキュリティ監査人の方全体でこういった業務を盛り上げていければと思っています。

◆モデレータ　リコージャパン　辻井様

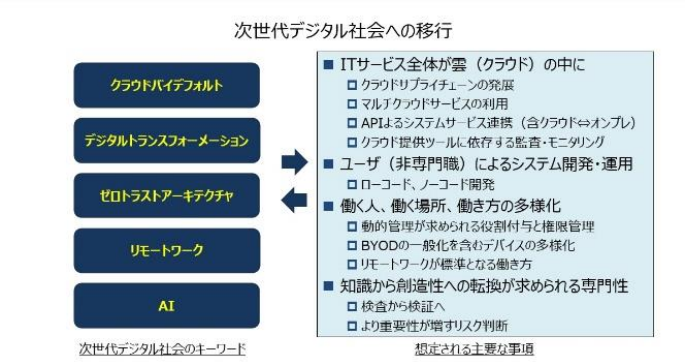
Our チームになってセキュリティに関わる皆がお客様に寄り添い、お客様の企業価値をセキュリティで高めていくことで、日本全体のセキュリティレベルを高めていくためのその一つのチーム、チームジャパンセキュリティの一員だという気持ちで、セキュリティ監査人の皆さんも増やして、女性の活躍の場をもっと広げていけたらいいなと思います。

---

[2] サイバーハイジーン
衛生（Hygiene）的な考え方でサイバーセキュリティを捉えること。人体が病気にならないよう日頃から注意することと同様に、組織がサイバー攻撃等から身を守れるように常日頃から注意して管理をすることを意味する。

パネルディスカッション２

次世代の情報セキュリティ監査を問う



モデレータ

特定非営利活動法人

日本セキュリティ監査協会　永宮 直史 氏

パネリスト

デジタル庁　満塩 尚史 様

日本マイクロソフト株式会社　河野 省二 様

有限責任 あずさ監査法人　山口 達也 様

【オープニング】

◆モデレータ　日本セキュリティ監査協会　永宮氏

それでは「次世代の情報セキュリティ監査を問う」ということでデジタル庁の満塩さん、マイクロソフトの河野さん、あずさ監査法人の山口さんとディスカッションして参りたいと思います。

大上段のタイトルにしてしまいましたが、今は次世代デジタル社会へのまさに転換期ではないかと思う次第です。

これまでの情報セキュリティ監査というものが、どちらかというとマネジメントを中心に紙ベースでチェックをしていくことを主体とし、オーバーオールに関連したところを見ていくといった時代でした。それは対象システムがクライアントサーバやWebベースであり、その処理内容もどちらかというと事務系が多く、営業部分が含まれるとしても一部、という限定されていた時代だったからです。

それが今大きく変わってきました。これからいくつかキーワードをあげ解説していきます。まず一つ目は、クラウドバイデフォルトです。もはやサーバを購入して物理的にネットワークを敷きシステムを構築する時代ではないと考えます。極端に言いますとノーコードでパラメータを設定し、アイコンを繋ぐとシステムが出来上がる時代になってきており、しかもそのバックに違うクラウドサービスが連携していますので、今までの固いシステムから柔軟性にとんだシステムになってきています。

しかも、ユーザーからは見通せないバックに様々なシステムが繋がっていて、まさにクラウドの状態となっています。

それからもう一つの大きな流れとしては、デジタルトランスフォーメーション(DX)が進展していきます。これは従来のシステム化とはまったく異なり、今まではビジネスをどうデジタル化するかが焦点でありましたが、現在はデジタルを前提としたビジネスをどう組み上げていくのかという仕組みに変わってきています。

これらの状況を支えるものとしてゼロトラストアーキテクチャという流れがあり、境界防御で対策を取るのではなく様々なリソースにアクセスする際にユーザーが権限を持つか否かを判断し、動的に変化する管理の流れとなっています。

このようにシステムのベースが変化しているとともに、ユーザー側も変化しています。コロナ禍がひとつのきっかけとなりましたが、現在、リモートワークなしの企業は少なくなってきており、特に大手企業にはその傾向が強く認められます。例えば富士通は本社を新橋から川崎へ引き上げています。なぜならリモートワークが

可能となったからです。

実は、リモートワークの恩恵をJASAも受けております。私が近年JASAの事務所に訪れたのは４年間で４回でした。JASAはワーキンググループが多く、日中は本業を行っている参加者に考慮し夜の会議が多いのですが、リモートであれば20時に会議が終了しても夕食が間に合うのです。

また、大きく変わった点は昼間に会議ができるようになったことでした。参加者が皆リモートワークのため、自宅で時間調整をしてもらえれば昼間に会議ができるようになりました。このようにどこの場所、時間帯でも調整つけられるのは、クラウドや関連した仕組みの変化が影響しています。

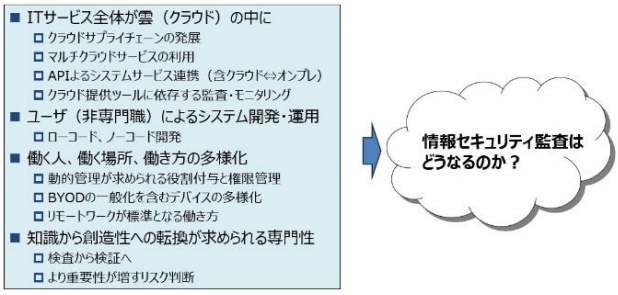
また、ここ一、二年大きくなってきた技術はAIです。これによって単純作業は不要になるといわれており、セキュリティの世界ではAIの技術が進んできています。

次世代デジタル社会の全貌は理解しづらいものがありますが、このように段々と姿が見えてきていると感じています。何が変わってきたかと言いますと、使うシステムの全体像は分かりにくく、どこからリソースを持ってきているかも分からない中で、クラウドの中で処理が行われているといった印象です。マルチクラウドはあたり前となってきており、オンプレ、クラウド問わずAPIで連携することにより、いろいろなデータがいろいろなところから取得できるなど、使う側もそのような状況となってきています。

最近の内部監査では、クラウドのツールを使う事例もあります。良いツールを使用すれば監査を効率的に進めることができます。このような環境下で今までと違う点は、ユーザーが直接システムを組み上げることができるようになりました。（例：ノーコード開発等）専門職が作成するのではなく、誰でもシステムを組める時代に変わってきているのです。

働く人、働く場所、働き方の多様化が進むことで、その人に本当に権限があるのか。副業とかも考えると、今その人がどういう状態なのかを把握しないと管理できなくなってきています。

次世代デジタル社会における情報セキュリティ監査



当然、デバイスもBYODが普通となり、会社支給の機器のみ管理すれば良いという時代ではなくなってきています。それから、専門性が変わってきている部分としては、検査（チェックする）から検証（知的な創造性、判断力が必要）へ変化しています。そして何よりも、これだけ複雑な時代となってきていますので、リスクが物凄く多様化しています。リスクに対し適切な判断が求められてきます。「このような大きな変化に対し、情報セキュリティ監査はどのように変化したらよいか。」といった内容を今回ディスカッションする機会として設けております。

それではパネリストをご紹介します。最初に、デジタル庁 戦略・組織グループ セキュリティ危機管理チームでセキュリティアーキテクトをされている満塩様です。

二人目が、日本マイクロソフト株式会社Chief Security Officerの河野様です。社内ではセキュリティの最高責任者です。また、情報セキュリティ監査制度のスタートライン時に管理基準を作成された方でもあります。

三人目が、あずさ監査法人のDigital Innovation & Assurance 統括事業本部 Digital Advisory 事業部長、パートナーの山口様です。

大きなシステムのユーザーのセキュリティを考えらおられる方、巨大なクラウドベンダーのセキュリティ責任者、そして、それをしっかり監査する方という異なった立場の方々にご参加いただいています。

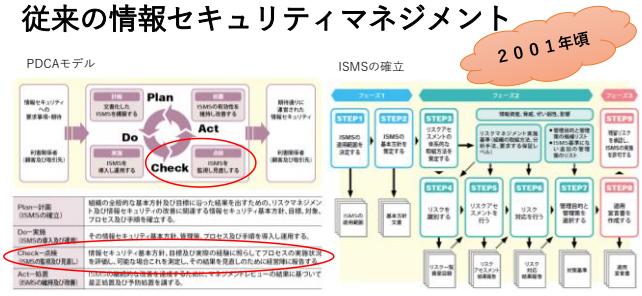
パネリストの方からポジショントークとしてご自身の紹介と今携わっている事業内容、およびセキュリティ関連についてのプレゼンテーションを伺いたいと思います。

【プレゼンテーション】

◆デジタル庁　満塩様

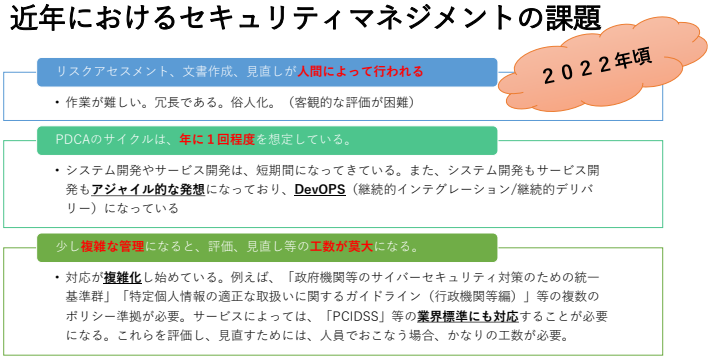
本日は、20数年前からご一緒いただいた方々が多くいらっしゃいますので、専門家の一員として話をさせていただきます。私は現在デジタル庁でセキュリティ専門として業務を行っております。以前はKPMGコンサルティングに所属し、システム監査/セキュリティ監査を実施していました。河野さんとは、2001年に電子署名法やISMS制度ができたころからのお付き合いかと思います。2003年からCIO補佐官としてセキュリティに限らずITのアドバイザーとして業務を担当しておりました。2011年に環境省から経済産業省へ移り、デジタル庁へ民間専門人材として採用され2年が経過しました。

担務している業務としては、デジタル庁のセキュリティ監査やゼロトラストアーキテクチャの検討を行っています。また、モニタリングシステムの検討やCRYPTOREC暗号技術活用委員会メンバーとして活動もしていますが、ISMAPもデジタル庁が共同所管として推進しています。



「一般財団法人日本情報経済社会推進協会　ISMS適合性評価制度の概要」より

2001年頃にISMSが確立されました。ISMSではPDCAサイクルを回すことになりますが、Checkの所がセキュリティ監査に関わる部分となります。

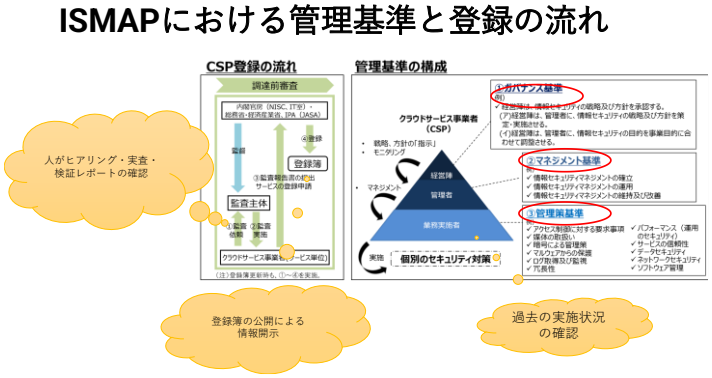


最近セキュリティマネジメントの課題として感じることは属人化があると思われます。また、作業が冗長であることも課題と捉えております。

PDCAサイクルでは年1回のチェックサイクルを考えますが、近年ではアジャイル開発なので2か月の短期間でリリースし、アップデートされることを前提に検討する必要がある場合が増えてきています。

セキュリティ対応は複雑化し始めており、政府では統一基準群に則ってポリシーを作成しています。これらは様々なISOを基準にしています。サービスによっては、PCIDSS等の業界標準への対応に関する議論もデジタル庁では行われています。

これらを遵守することは、ポリシーは複雑化し、複雑化したルールの遵守は、開発チームが苦労する場合も多くなっているであろうと考えます。

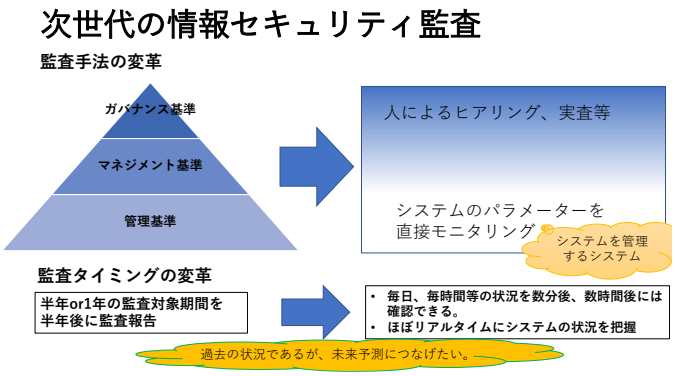


ISMAPは構造上基準が３つに分かれています。ガバナンス基準、マネジメント基準、管理策基準で構成されています。この三階層でセキュリティ管理の

状況を確認しています。

ISMAPの監査では一般的な監査の流れで実施しています。結果は登録簿として情報開示しています。

SOCレポートを見ると、何年の何月何日から何月何日までのレポートであると過去の期間を明記しています。



次世代の情報セキュリティ監査では、ガバナンス基準の監査は自動化することが難しいと思われますが、管理基準などはシステムのパラメータを直接モニタリングする世界ができつつあると思います。

最近、クラウドサービスベンダーから聞かれる言葉として、Audit機能という言葉を聞きます。スリーラインモデル[3]に基づくサービスである説明なども耳にします。クラウドはサービスを提供してくれるが、クラウドは中身が見えなくなってきています。

ユーザー側の意見を聞くと、なぜAudit機能を信じられるかと聞くと、クラウドがきちんと機能していることを信じており、私からするとその部分は疑問を感じるべきところでありますが、クラウドに設定したパラメータはモニタリングできる状況になってきています。

また、ゼロトラストアーキテクチャについて検討を行っており、数週間前に日本ネットワークセキュリティ協会の方と議論していました。今、アクセスコントロールは境界型（サービスの前にチェックする）が基本です。よく見るとその上にモニタリングセンサーがいっぱい張られています。これが重要です。センサーで得た情報を活用し、アクセスコントロールを動的に変更していくことがゼロトラストアーキテクチャのコンセプトだと考えています。

モニタリングするということをしっかり入れていくことが、これまでできておりませんでした。というよりもモニタリングするリソースがなかったのですが、今日のリソースが豊富になってきた状況下では、モニタリング機能が実装されていくものと思います。

監査のタイミングについては、人間が行う場合は、頻度を高く実施することは限界がありますが、モニタリングであれば、ほぼリアルタイムで行うことができます。

会計監査は、過去に問題が発生していなかったか、それとともに将来発生しないかという視点が重要ですが、セキュリティ監査の場合、ユーザーからみると過去よりも将来問題が発生しないかが重要となりますので、監査結果を未来予測につなげたいと考えています。

現在の状況を踏まえますと、実現できそうな状況になってきたと感じています。

（C21-0008-2 Amazon Web Servicesの場合）

次に、ISMAPに登録しているから大丈夫という誤解が散見してみられます。ISMAPの登録簿に登録するといろいろな情報が公開されますので、それらをユーザー側が参照・評価し最後は判断していただく仕

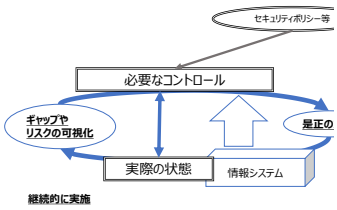
[3] 組織を構成する３つの部門（①現業部門②管理部門③内部監査部門）が各々異なるリスク管理の役割を担い内部統制を実行するモデル

組みとなっています。そのものが何を保証しているのかをユーザーはきちんと理解し情報を活用していただいているのかが、私としては気になるところです。

常時リスク診断・対処（CRSA：Continues Risk Scoring & Action）の概要

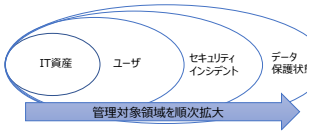
●常時リスク診断・対処

- **リスク診断**
  必要なコントロールと実際の状態のギャップやリスクを可視化
- **対処**
  可視化されたギャップやリスクへ是正の対応
- **常時**
  ギャップやリスクを可視化し、是正の対応を継続的に実施



●管理対象

- **IT資産（デバイス、ソフトウェア、サービス等）、ユーザ、セキュリティインシデント、データ保護状態**を管理対象と想定。
- 実装される管理対象は、順次追加している。

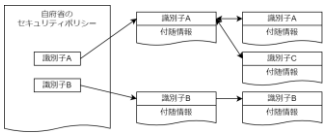


最後に、ゼロトラストアーキテクチャのセンサーにあたる部分としてCRSA（常時リスク診断・対処）を検討しています。仕組みは、ポリシーに対してどれだけ外れているかをチェックしています。

日本語のセキュリティポリシーは読みづらい特徴を持っています。本来の形はポリシーの一文が一オブジェクトになっているのが理想であり、そこを目指してカタログ化を検討しています。

セキュリティ統制のカタログ化の概要

- カタログ化とは、以下に示すセキュリティ対策において、**統制を有効にするために設定する目標「セキュリティ統制」**に対して**一意な識別子を付与**し、**機械可読な形式で分類**することを指すものである
  - **情報セキュリティポリシー運用業務**
  - **システム実装業務および運用業務**
  - **セキュリティ監査業務を検討および実施**



- セキュリティ統制を識別子によって一意に識別し、マークアップ言語などで表現し機械可読化することにより、例として以下を実現することが可能となる。
  - **ポリシーの柔軟な変更（統制の追加、変更）、システム実装および変更の自動化**
  - **IaC、テンプレート活用など、クラウドネイティブ技術にてセキュアな実装を促進**
  - **オートスケール環境や短命なシステムにおいても、セキュアな状態を維持**
  - **監査および是正の自動化まで実施することで、24時間/365日セキュアな状態を実現**

セキュリティ統制のカタログ化の例

- NIST SP800-53およびOSCALについて
  - NIST SP800-53 は、米国連邦政府の内部セキュリティ基準を示すガイドラインの一つであり、**管理策番号として AC-1のような番号で表現**している。
  - OSCAL（Open Security Controls Assessment Language）は、情報セキュリティ責任者、ベンダー、および監査人などのセキュリティ統制業務に携わる関係者の事務処理を減らすため、正確で**機械可読な形式を使用して、セキュリティ制御カタログ、規制フレームワーク、およびシステム情報の表現を正規化**し、組織間での制御実装情報の共有を可能にしている。

```
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
              guidelines:
                - prose: devices and/or types of devices to be uniquely identified
                    and authenticated before establishing a connection are defined;
…略
```

最後の例では日本の事例ではありませんが、セキュリティポリシーをコーディングする例を表しています。このような世界が実現されていく中で、それらに対応して監査の自動化検討を今後ユーザー目線で進めていきたいと思います。

◆マイクロソフト株式会社　河野様

2002年に情報セキュリティ監査研究会が発足し、最初はオブザーバーという形で参加しておりましたが、管理基準作成の担当となり一月掛けて作成しました。ISO/IEC17799を分解し、内容がおかしいところを修正しISOのチームへ提供し、その後ISO/IEC27001と27002に分かれた経緯がありました。これらの動きより日本の情報セキュリティ監査がISOに対し、かなり貢献していることが分かり、日本がリードしていることが分かると思います。

当時、33才ぐらいでしたが、そのような年代でも参画でき、よい時代であったと感じております。今のセキュリティの世界は比較的年配の方が多いので、若手の方のキャリアパスがあってもよいと思います。

NIST SP800-207A (Draft)

A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments

ゼロトラストにおける動的ポリシーによるアクセス制御の仕組みをマルチクラウドにおけるアプリケーション環境においても実現できるようにするためのガイダンス。主に以下の2点について触れています

- ネットワーク層および ID 層ポリシーの策定。
- 異なるポリシーの展開と実施を可能にする技術コンポーネントの構成

2023年4月18日から6月8日までパブコメ募集

皆さまは、ゼロトラストをNIST SP800-207Aを参照しながらいろいろな解釈をしていることと思いますが、かなりクラウドセキュリティアライアンス（CSA）の意見が多く入っていまして、パラメータを自由にさわっていく話やSASEの話もありますが、それらを払拭するような話もでてきました。それは、NIST SP800-207Aというドラフトですが、こちらは際物というか皆さんの想像を超える部分があり、リアルタイム監査より予兆管理に近い内容が含まれていました。

マルチクラウドを使ってアプリケーションを作っていく時にどのようにアクセスコントロールしていくかという話になります。つまりゼロトラストにおいては動的ポリシー制御が重要であり、従来のポリシー制御をしている中で環境に応じて変化することをどのように実現していくかということのガイダンスです。ネットワーク層およびID層のポリシーの策定と書かれておりますが、ネットワークをどのようにコントロールしていくかをここでは書いてありますので、パブコメは終了しているのでこれから整理されていくことと思います。

ガイダンスの前提となるクラウドアプリケーション

- 一般的に受け入れられているクラウドネイティブアプリケーションの特徴は、以下の通り
  - アプリケーションは、マイクロサービスと呼ばれる疎結合のコンポーネントの集合で構成されており、異なる物理マシンまたは仮想マシン（VM）でホストすることができ、地理的に分散していることもある
  - アプリケーションを含むあらゆるトランザクションは、ネットワークを介した1つまたは複数のサービス間（マイクロサービス）コールを含む場合がある
  - クラウドネイティブアプリケーションの広く普及している特徴は、すべてのアプリケーションサービス（サービス発見、ネットワーク接続、通信回復力、認証や認可などのセキュリティサービスなど）の統合セットを提供するサービスメッシュ

ガイダンスの前提となるクラウドアプリケーションということで、アプリケーションはマイクロサービスと呼ばれる疎結合のコンポーネントの集合で構成されており、異なる物理マシンまたは仮想マシンでホストすることができ、地理的に分散していることもあります。例えば私たちマイクロソフトが提供しているMicrosoft365は、昔はSaaSと呼ばれましたが、今のコンポーネントとしてはPaaSとなります。なぜかというとEXCELのプリント機能が一つのプログラムとなっています。つまり、EXCELというソフトウェアがあるわけではなく、それがコンポーネントとして存在しています。先ほど上村さんのお話にあったSBOMの話は、こういう部品表の話をしておりますが、207Aではアプリケーションの部品の話をしています。つまりアプリケーションの部品というのがマイクロサービスに相当します。

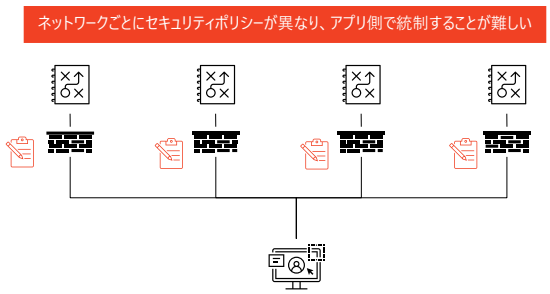
では、「Windowsは関係ないのか」と思われる方もいるかもしれませんが、Windowsもマイクロサービスのかたまりとなっています。皆さんのPCの中にあるコンポーネントだけで動いているわけではありません。これはMAC OSも同じでありiOSやAndroidも同じです。構成が変わってきていいることを認識してください。

アプリケーションを含むあらゆるトランザクションは、ネットワークを介した1つまたは複数のサービス間コールを含む場合があります。つまり、メッシュ型になりなが

らいろいろなものが呼び出されている可能性があるということです。

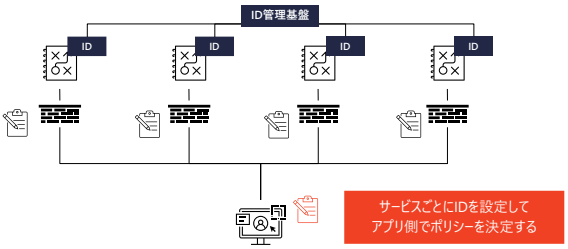
一番最後にクラウドネイティブアプリケーションの広く普及している特徴は、全てのアプリケーションサービスの統合セットを提供するサービスメッシュという（ツリー構造ではない）メッシュ型の構造にあります。

ネットワークセグメントを超えたサービス連携



今まで皆さんがアプリケーションを作る（使う）ことになりますと、自分達側にCASB（ネットワーク型CASB、ゲートウェイ型CASB）とか置いておいてSaaSに接続しに行く、ネットワークサービス提供側でいうとWeb Application firewall（WAF）を置いて、そこでアクセス制御を行っていました。これをすると、ベンダー側またはプロバイダー側の制御に依存していてユーザー側は自由に使えないじゃないか。これじゃ上手くいかない。そこでプロバイダー側はファイヤーウォールを全て取り去るのかポリシーを全部なくすのかというと、それも危険な行為となります。どのように管理すればよいのかというと、マイクロサービス一つ一つを管理する基盤が必要ではないかということです。

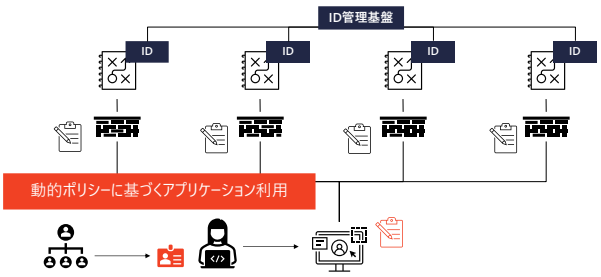
サービスごとにIDを付与してポリシーを設定



上図でID管理基盤と書かれております。例えば、SBOMがライブラリに番号を付けて、このライブラリには脆弱性があるから、このライブラリを使っているソフトウェアには何らかの修正が必要であるとの指摘があったとします。これに該当するIDの付いているマイクロサービスコンポーネントにはなんらかの脆弱性があるので、ユーザーはこれと同じ機能を持つものにすぐに置き換えてレジリエンスを保ちながらサービスの利用継続をしていきたいと思います。このためには、誰でもが分かりやすいようにID管理をして、例えばマイクロソフトのEXCELのマイクロサービスとかWORDの○○○サービスにどういったIDが付いていて、今どういう状態かという状態のリアルタイム管理ができる必要があります。ユーザアプリケーション側でID管理基盤にアクセスし、マイクロサービスをコントロールするということであります。永宮さんが話されていたローコードの考え方では、なにか不具合がありそうな動きでマイクロサービスにアクセスしようとすると、それを自分達がまったく同じ機能の違うものに置き換えていくことになります。

こんなことができるのかということですが、Microsoft AzureもAWSのサービスもGoogleのサービスも基本的にはコンポーネントの標準化をして置き換えができるようになっています。Microsoft独自、AWS独自としていくと使えないサービスと化していきますので、ユニバーサル化しているわけです。

アカウントとアプリケーションの動的ポリシー利用



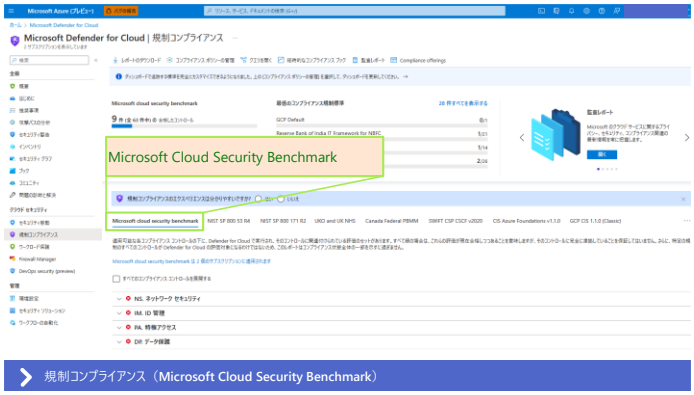
そういう標準化の流れの中で、動的ポリシーに基づくアプリケーション利用という考え方があり、こんどはアプリケーションがマイクロサービスを構成する中でユーザーの状況に応じて使えるコンポーネントも変わってくるといった動的ポリシー制御もできるようになります。これが207Aの完成形となります。

こんなふうにしながらユーザーのID、コンポーネントのID、ネットワークにおけるIDベースの制御、これ上も下も両方ですがそんなことを管理していく動的制御がこれからは必要になると思われます。

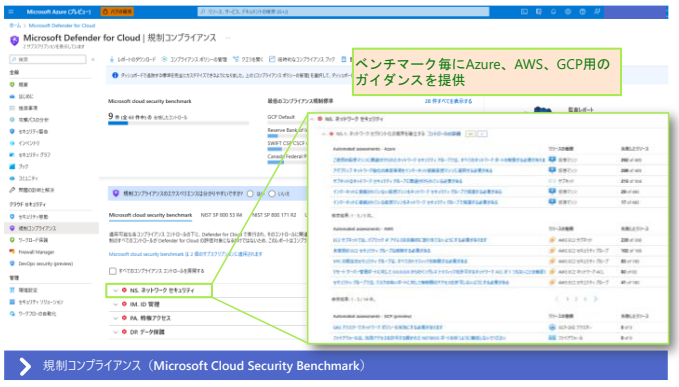
そうしますと、皆さんSBOMについて興奮して取り入れようとするかもしれませんが、こういう世界が２年以内に来ますので、ソフトウェア固定という考え方もなくなってきてきますが、今後これらの監査をどう行っていくのかが課題となってきます。

Microsoft AsureをISMAPで監査し皆さんが使用する際に、ISMAPの中に私たちのサービスが書かれておりますが、そのサービスを皆さんが使用する時にその情報が今はどうなのか、満塩さんが言われた通りISMAPだと確認サイクルが１年半なので、そういった所を皆さんでご判断いただきながら、私も尽力しますが変えていきたいと思います。

ここで難しい話と簡単な話をさせていただきたいと思います。

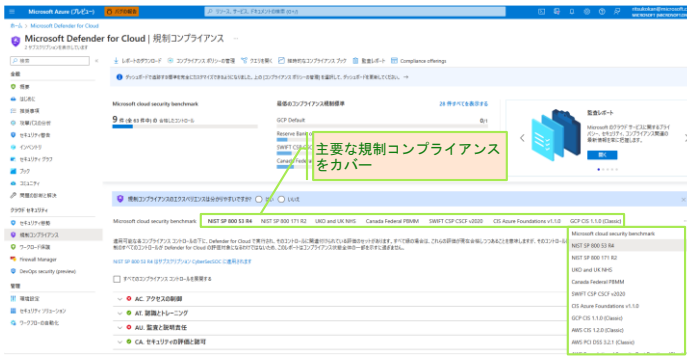


監査の自動化に関する話ですが、マイクロソフトのトラストセンターにクラウドサービスとして監査を受けている基準が全て載っており、数えたところ100以上ありました。100以上の監査はコンプライアンスカレンダーとして我々トラストチームが年間スケジュールを組んでいます。エビデンスが同じなのでエビデンスベースにまとめると、実は監査項目が標準化できることをマイクロソフトのトラストチームが作成し、それをマイクロソフトベンチマークテストという、かなり膨大なリストとしています。



これらを活用すると、AzureのみならずAWSやGCPの監査ができるようになっています。皆さんが、Azure、AWS、GCP用に作成した単位でこれらの監査が走っており、それをリアルタイムに継続して監視できるようになっています。

そうしますと、サービスをリリースする際、こちらを参照してからリリースするとか、ミスコンフィグレーションがないようにちょっと変更してからこちらを参照するという運用ができるかもしれません。



規制コンプライアンス（評価可能な標準）

これらは主要な規制コンプライアンスをカバーしているので、監査の自動化も進んできたと言えます。

ただ、どんなものでも自動化できるというわけではなく、アプリケーション構成や環境を自動化できる環境に近づけていく必要があります。

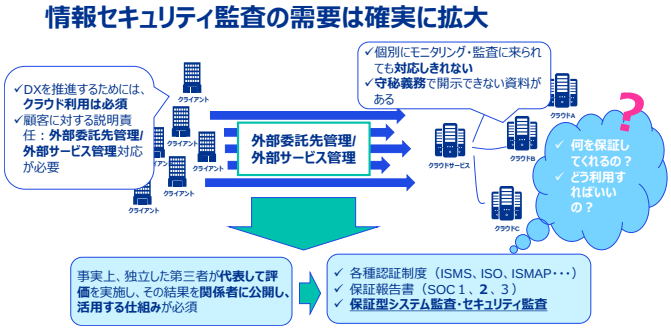
リアルタイムに監査を行うことで、監査コストが減っていくことができれば安全になりますし、テストの期間が短くなれば開発の期間も短くなる効果があります。テストに2か月掛かるのであれば、年間で製作に掛かる期間は10か月となりますが、5秒でテストできたらその分、製作に回すことができます。このような考え方がDev Opsの考え方となります。

DevOpsでソフトウェア開発するために、テストや監査の時間をどれだけ短くするのか考えることが重要と思われますので、これからの監査の一つのテーマにしたいと考えております。

◆あずさ監査法人　山口様

私の略歴ですが、銀行のシステム部門に９年間勤めた後、監査法人に転職し、それから20余年間にわたり財務諸表監査のIT統制監査の評価から、情報セキュリティ監査、ISMAPの情報セキュリティ監査など、監査・評価に関わる仕事を従事しております。そのかたわら、JASAを始めとするいろいろな協会の活動も行っております。

私からは次世代の情報セキュリティ監査とのテーマで少し毛色の異なる話をさせていただきます。



DXやデジタル化を進める時に、なんらかの形でクラウドの利用は避けられないものです。もう一方ではクラウドのセキュリティについて不安視するような声もあり、使う側からしても外部先管理とか最近は外部サービス管理という用語もでてきましたがそういったことを対応していかなければならなくなっています。

そのようなことから、委託元・利用者側が全員、監査を実施するとクラウド側が受けられなくなることが想定されます。そのため第三者がクラウド事業を調査し報告を、利用者が確認し安全性の確認を行うことが現在行われているのが実態であります。

これらはISMS、ISO、ISMAPといった制度もあれば、SOC1、SOC2と言われる保証報告書という、保証型システム監査・セキュリティ監査がといった仕組みがあります。このように、監査・保障については様々な形態があります。

監査・保証の種類（私見・一例）

日本語では「監査」「保証」と呼ばれる評価の仕組みも、実際は何種類かに分類される。以下は**明確な定義が存在するものではないし、厳密に区分できるものでもない**が、監査業界？でのイメージは以下の通り。

日本語	英語	概要（イメージ）
監査	Inspection	◆ルールへの準拠状況のみを確認（運用状況評価だけ）
	Assessment	◆ルールの妥当性を含めて確認 ◆実際に確認した部分のみを対象に評価※1
	Audit	◆実際に確認した部分を含め、全体を評価※1
保証	Assurance	◆提示された命題（言明等）に対して、その命題が事実に即して正しいか否かを確認※2 ◆結果的に損害等が発生した場合、直接的な賠償等の補償はない
	Guarantee	◆結果的に損害等が発生した場合、それを補償する ◆これに該当する保証業務はない。実質は保険。

「監査」とか「保証」という言葉の定義に厳密に触れると、宗教戦争のようなものが起きる可能性がありますので、ここでは私の私見の一例としてお話させていただきます。

例えば監査と日本語で言っても、英語ではInspection、Assessment、Auditといったイメージがあり、保証についてもAssurance、Guaranteeといった2つのイメージがあります。

監査の方ですが、Inspectionはいわゆる検査のイメージとなりますので除外して、AssessmentとAuditの違いは「大丈夫」（保障）としている範囲が異なります。保証については、Assuranceは事故が発生しても損失補填等は行わないものであり、Guaranteeは損害が発生した場合に補償するものであります。監査の世界ではAssuranceしかなく、Guaranteeは保険の部類に属します。このように監査とか保証という言葉がいろいろな意味合いで使われていることが実態です。

※１：AuditとAssessmentの違い

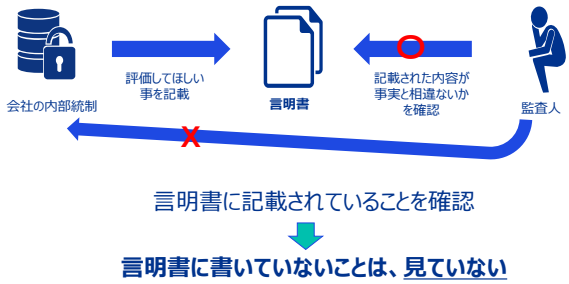
「A,B,Cシステムを所管するX部署の情報セキュリティ監査を実施の際、A,Bシステムを確認した結果として、、、」

【Audit】
X部署のセキュリティ対策は評価基準に従って対応されている。

【Assessment】
X部署のAシステム、Bシステムのセキュリティ対策は評価基準に従って対応されている

AuditとAssessmentの違いをもう少し詳しく解説します。例えばA、B、Cの3つのシステムを保有しているX部署を監査した際に、A、Bシステムを対象として監査した場合、AuditだとA、Bシステムしか確認していないが、Cシステムも含めたX部署としての評価を行います。それに対してAssessmentはあくまでも確認したA、Bシステムに対しては評価するが、Cシステムについては評価の対象外とします。これAuditとAssessmentの違いとなります。

※２：保証型監査/各種評価制度の仕組み



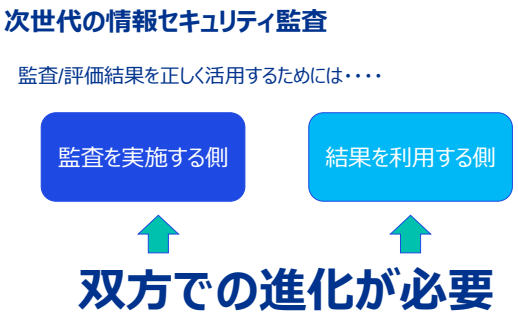
言明書に記載されていることを確認

言明書に書いていないことは、見ていない

先程Assuranceしかないと言った保証について、ISMAPやSOC2の保証報告書にも言えることですが、大半のものは会社の内部統制を直接確認してはいません。何を見ているかといいますと、言明書であったり保証報告書であれば第2章第3章といった評価対象の統制状況を記述した文書を確認し、監査人はそこに記載のあるものを事実と比較し評価しています。

別の言い方をしますと言明書に記載された内容は見ていますが、記載のないものは見ていないことになります。これが今の保証報告書であったりISMAPであったりします。

このような仕組みをきちんと理解して情報を扱わないといけません。先程、満塩さんの話にもありましたが、ISMAPを取っているから大丈夫といった単純な判断ではいけません。ISMAPを取得している企業が言明書でなにを情報発信しているのかを確認し、その内容が問題ないと判断した時に大丈夫との判断をしなければなりません。



次世代の情報セキュリティ監査として思うことは、満塩さん、河野さんが言われておりましたとおり、我々の監査もアップデートしていかなければなりませんが、同時にその結果を利用する側の意識や知見もアップデートしてもらわないと、次世代の情報セキュリティ監査の高度化に繋がらないと考えます。

そうはいっても利用者側に学習を促すことは難しいと思われますので、我々セキュリティ監査人としては利用者側の領域に関しても啓蒙をしていくことも次世代の情報セキュリティ監査を考える上ではポイントになると考えております。

【ディスカッション】

◆モデレータ　日本セキュリティ監査協会　永宮氏

今、様々な形でシステムが変わり、評価すべき対象や時間が変わってきているというお話もあり、これからも監査が増えることが見込まれるお話もありましたが、次世代としてどういった監査が増えていくのか。例えばISMAPのように1年に1回定期的に監査を実施するパターンなのか、実際にはモニタリングのようなリアルタイムな監査が望ましいと思われますが、実現性を考えると1か月に1回などのタイミングで行う監査が増えていくのか、どういった監査が望まれ、近い将来も含め技術的な問題がクリアできそうかについてお話をいただけますか。

◆デジタル庁　満塩様

今までの監査が全く同じように行われていくことは考えにくいと思います。先程お話ししたモニタリングの話もパラメータを参照しただけでは意味が分からないのが現状です。大切なことは結果として出力したパラメータを解釈できるとか、モニタリングシステムを設計できる知識が必要となりますので、その部分を監査の経験を持った人が参入してもらうべきと考えますし、パラメータがどこまで判断材料として限界なのかの分析においても監査人の知見が役立つと考えています。

◆マイクロソフト株式会社　河野様

監査といいますかAssessmentという視点からモニタリングのKPIもリアルタイムに変わっていくものがこれからできてくるのではないかと考えます。

タイミングについては、年間1回で良いものや毎回短期間で実施した方がよいものもあるかと思いますし、他の方が納得するものや自分が納得するものなどいろいろな側面から考えると、リアルタイムに実施する監査が増えていくものと思います。

私が行った管理基準策定や永宮さんが行ったスマートメーターの安全管理基準策定もそうですが、結局、測れなければ意味がないので測れるように整備するということも大切なことだと思います。

◆モデレータ　日本セキュリティ監査協会　永宮氏

監査が増えることについては良いのですが、外部監査が現在変わりつつあると感じています。この社会ではトラストがキーワードとなっていますが、そのあたりの流れの中で監査の重要性が増すなか、業種・業態・システムについて、今後どのような影響があるのか伺えますか。

◆あずさ監査法人　山口様

世の中共通で考えられますのは、特定重要基盤（金融・通信・医療など）に対し、皆が依存して暮らしていますので監査の重要性は増してきます。本当に大丈夫であることを公表する際には、保証型監査が重要になり増えていくものと考えています。

◆モデレータ　日本セキュリティ監査協会　永宮氏

今回会場に参加している方は多くが監査人でありますが、これからの監査人はこれまでのスキルに加えどのようなスキルを磨くことが次世代に役立つとお考えでしょうか。

◆デジタル庁　満塩様

2000年の頃電子署名法を手塚会長と検討しておりましたが、検討にあたってPKIの技術を理解することが前提でした。現在、CRYPTORECのメンバーと話をしておりますと、AIはすぐ目の前にきております。量子コンピューターに関連しては耐量子暗号など新技術が導入されていきます。私はビジネス側というよりサイエンス側から入ってきましたが、マネジメントは技術の必要性は高くありませんがテクノロジーの理解がだいぶ変るものと思います。

◆マイクロソフト株式会社　河野様

私はISMAPの責任者としてフロントに立って仕事をしており、監査を行っている監査法人の方と週４～６回打合せをしながらエビデンスの確認を行っています。監査法人の方は監査の情報をIPAやISMAP委員会へ報告する流れとなりますが、説明ができない内容について再度の確認が発生しています。そのような対応をしておりますと、監査側の方に技術的な部分をある程度理解していただきたいと感じています。現在は、ISMAPの監査を行う前に監査法人の方にシステムに関する仕組みの勉強会を実施し、監査を行っています。監査に関わってきた私だと、監査を受ける際対応できていますが、知識がないベンダーだと監査に対応することは難しいと感じます。監査を受ける側に対しても監査知識が必要だと思います。

◆あずさ監査法人　山口様

新しいスキルに関してはいろいろ考えられますが、監査を日頃業務で行っている立場から考えますと監査スキルが必要と思われます。何をどこまで見たらどこまで大丈夫と報告したらよいのか、提示された証跡に対し信頼して良いのかなど、今後いろいろな状況が発生していきますので、監査人としての感覚を研ぎ澄ませて事実は事実として認識する必要があります。

◆モデレータ　日本セキュリティ監査協会　永宮氏

システムが変わってきており、専門特化してきている中で、これからの監査を考えますと深い専門知識を持った方が監査スキルを磨く。マネジメントとかガバナンスは経営的な部分を理解してリスクを経営者に確認する必要があるが、経営者の理解度を分析する技術も必要になると思います。

次世代は皆が量子コンピューターや量子力学を勉強しなければならない世界でもないと思いますが、監査する側が理解しておいた方が良い技術的な知識もあるので、これら2つの方向性を監査人は身に着けていかなければならない必要性があると思います。

この考え方は20年前とは変わらず、当時はクラサバ・Webなどの技術を理解する必要がありました。今後、JASAも勉強の機会を皆さんに提供していかないと、いわゆるチェックリスト型監査から抜けられないと思いますので、その仕組み作りも皆さんの協力を得て実現していきたいと思います。

功労賞の贈呈

功労賞について

功労賞は、情報セキュリティ監査制度20周年を迎えるにあたり、情報セキュリティ監査制度の設計に係わり、2003年4月に情報セキュリティ監査基準等の告示（経済産業省）により情報セキュリティ監査制度が開始された以降も、協会の活動において優れたリーダシップをもって尽力し、情報セキュリティ監査制度の発展に大きく貢献された皆様にお贈りするものである。対象者に表彰状と記念品を贈呈した。


手塚会長(左)、堀江様(右)

対象者

・稲垣　隆一　　様
・大木　榮二郎　様
・土居　範久　　様
・中尾　康二　　様
・原田　要之助　様
・堀江　正之　　様
・和貝　享介　　様


手塚会長(左)、和貝様(右)

○贈呈式の様子


手塚会長(表彰状を読み上げ)


堀江様

和貝様

○記念撮影の様子

手塚会長(左)、堀江様(中央)、和貝様(右)

堀江様

和貝様

感謝賞の贈呈

感謝賞について

感謝賞は、情報セキュリティ監査制度20周年を迎えるにあたり、長きにわたり協会の活動に携わり、優れた専門知識をもって尽力し、情報セキュリティ監査制度の普及促進に大きく貢献された個人および法人の皆様にお贈りするものである。対象者、対象団体に表彰状と記念品を贈呈した。

対象者（個人）

・太田　利次　様
・織茂　昌之　様
・河野　省二　様
・岸　泰弘　　様
・小柴　宏記　様
・塩崎　哲夫　様
・菅谷　光啓　様
・丸山　満彦　様
・水野　義嗣　様

贈呈式の様子

太田様

織茂様

河野様

岸様

菅谷様

小柴様

丸山様

塩崎様

水野様

受賞者9名を代表して丸山様のご挨拶①

受賞者9名を代表して丸山様のご挨拶②

受賞者の記念撮影

対象者（法人）

・株式会社 アスラボ　　様
・ジーブレイン株式会社　様
・富士通株式会社　　様
・リコージャパン株式会社　様

アスラボ様

ジーブレイン様

リコージャパン様

記念撮影

受賞4社を代表してジーブレイン様のご挨拶①

受賞4社を代表してジーブレイン様のご挨拶②

第３章　資料集

設立趣意書

特定非営利活動法人日本セキュリティ監査協会・設立趣意書

【 設立の背景 】

コンピューター利用の一般化、インターネットの普及により、行政機関や民間企業の多くの活動に於いて、インターネットに接続された情報システムの利用は急激に拡大しています。また、家庭からのインターネット利用も増加しており、社会活動と国民生活などの情報システムとインターネットに依存する割合は増加の一途を辿っています。

その一方で、情報システムや組織体におけるセキュリティ対策の不備に起因する様々な問題も生じています。このようなセキュリティインシデントは、個人情報の漏洩による人権侵害、企業の機密情報の漏洩による経済的損害や情報システム全体のダウンといった被害をもたらし、経済社会に与える影響は深刻なものとなりつつあります。

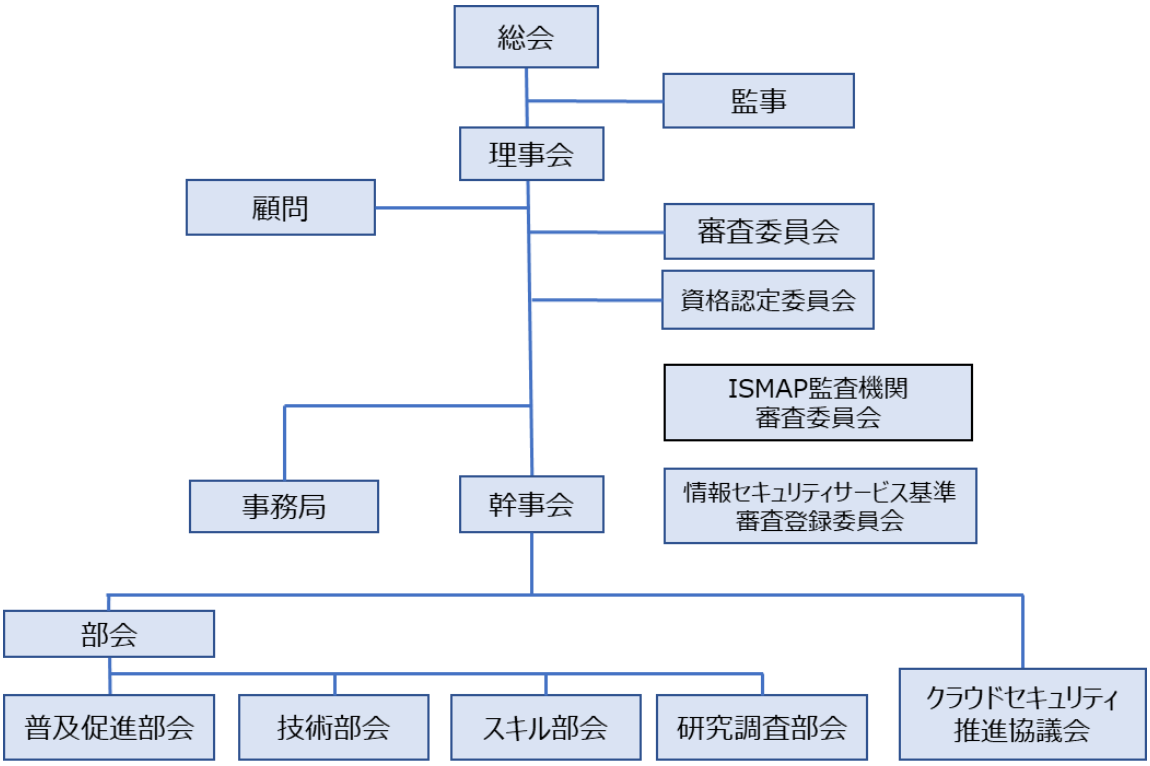
こうした環境の変化を受けて、IT セキュリティ評価認証スキームの創設、暗号技術の評価、ISMS 適合性評価制度の創設、インシデント情報共有・相談体制の整備など、情報セキュリティに関する制度整備は着実に進んできています。

しかしながら、独立かつ専門的知識を有する専門家による、客観的に情報セキュリティ対策の有効性を評価する「情報セキュリティ監査」の制度整備が遅れていることが喫緊の課題として浮上してきました。この緊急課題に対して経済産業省は、商務情報政策局長の諮問研究会として「情報セキュリティ監査研究会」を設置し、2002年9月より情報セキュリティ監査の普及とそのあり方について検討を行ってきました。その結果、今後の情報セキュリティ監査の根幹をなす各種基準や仕組み等が盛り込まれた「情報セキュリティ監査制度」が、2003年4月 1 日よりスタートしました。

【 設立の目的 】

この制度の施行を受けて、「監査をする側」の監査企業や監査人と、一般企業や団体などの「内部監査実施部門やその担当者」が一同に会し、「公平かつ均質で、効率的な情報セキュリティ監査」を目指して、監査技術の研究開発、監査人のスキルアップ、行動規範の確立、監査人資格のあり方の検討、並びに監査制度の国際標準の調査研究や改善提言、また相談窓口の開設などの活動を通じて、「情報セキュリティ監査制度」を着実に普及・浸透させていくことを目的に、「特定非営利活動法人日本セキュリティ監査協会」を設立いたします。

現在の組織


総会
監事
理事会
顧問
審査委員会
資格認定委員会
ISMAP監査機関
審査委員会
事務局
幹事会
情報セキュリティサービス基準
審査登録委員会
部会
普及促進部会
技術部会
スキル部会
研究調査部会
クラウドセキュリティ
推進協議会

現在の会員

【正会員】(67 会員)　※2023 年 11 月 27 日現在　50 音順

1　株式会社ＩＳＩＤビジネスコンサルティング
2　株式会社 IT スクエア
3　株式会社アイネス
4　有限責任あずさ監査法人
5　株式会社アズジェント
6　アビームコンサルティング株式会社
7　アマゾン ウェブ サービス ジャパン合同会社
8　アーク有限責任監査法人
9　伊藤忠テクノソリューションズ株式会社
10　株式会社インテック
11　EY 新日本有限責任監査法人
12　EY ストラテジー・アンド・コンサルティング株式会社
13　ＡＧＳシステムアドバイザリー株式会社
14　株式会社 ENNA
15　NRI セキュアテクノロジーズ株式会社
16　NEC セキュリティ株式会社
17　NEC フィールディング株式会社
18　株式会社ＮＳ・コンピュータサービス
19　エヌ・ティ・ティ・アドバンステクノロジ株式会社
20　エヌ・ティ・ティ・コミュニケーションズ株式会社
21　エヌ・ティ・ティ・コムウェア株式会社
22　NTT テクノクロス株式会社
23　株式会社 NTT データグループ
24　エヌ・ティ・ティ・データ先端技術株式会社
25　株式会社エヌ・ティ・ティピー・シーコミュニケーションズ
26　MYT コンサルティング株式会社
27　Qsol 株式会社
28　仰星監査法人
29　KDDI 株式会社
30　株式会社ケイテック
31　KPMG コンサルティング株式会社
32　サイボウズ株式会社
33　株式会社さくらケーシーエス
34　三優監査法人
35　株式会社シーイーシー
36　ジーブレイン株式会社

37 中電技術コンサルタント株式会社
38 一般社団法人中部産業連盟
39 TIS 株式会社
40 株式会社ディアイティ
41 電気事業連合会
42 株式会社電通国際情報サービス
43 東芝デジタルソリューションズ株式会社
44 有限責任監査法人トーマツ
45 西日本電信電話株式会社
46 ニッセイ情報テクノロジー株式会社
47 日本電気株式会社
48 日本アイ・ビー・エム株式会社
49 日本マイクロソフト株式会社
50 株式会社野村総合研究所
51 ぴあ株式会社
52 株式会社東日本計算センター
53 東日本電信電話株式会社
54 株式会社日立システムズ
55 株式会社日立製作所
56 ＰｗＣあらた有限責任監査法人
57 ＰｗＣ京都監査法人
58 株式会社ファイブドライブ
59 富士通株式会社
60 株式会社富士通エフサス
61 富士通クラウドテクノロジーズ株式会社
62 ほくでん情報テクノロジー株式会社
63 みずほリサーチ＆テクノロジーズ株式会社
64 株式会社三菱総合研究所
65 三菱電機インフォメーションネットワーク株式会社
66 リコージャパン株式会社
67 リベラ株式会社

【準会員】(7 会員)　※2023 年 11 月 27 日現在　50 音順

1 株式会社アスラボ
2 株式会社ウインテックコミュニケーションズ
3 大岩 佐和子
4 加藤 雅彦
5 グローバルブレインズ株式会社
6 一般社団法人日本セキュリティ格付機構
7 株式会社フォース

【特別会員】(10 会員)　※2023 年 11 月 27 日現在　50 音順

1　稲垣 隆一（稲垣隆一法律事務所）
2　大木 榮二郎（工学院大学 名誉教授）
3　手塚 悟（慶応義塾大学）
4　一般社団法人デジタルトラスト協議会
5　土居 範久（慶応義塾大学 名誉教授）
6　中尾 康二
7　原田 要之助
8　堀江 正之（日本大学）
9　和貝 享介（和貝公認会計士事務所）
10　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

現在の理事幹事

理事　21 名（*：職務代行）　※2023 年 11 月 27 日現在　50 音順

相羽 律子	株式会社日立製作所
大貫 秀明	NRI セキュアテクノロジーズ株式会社
加藤 俊直	ＰｗＣあらた有限責任監査法人
鴨田 浩明	株式会社 NTT データグループ
北風 二郎	NEC セキュリティ株式会社
小柴 宏記	ジーブレイン株式会社
下笠 清	三菱電機インフォメーションネットワーク株式会社
下田 秀一	東芝デジタルソリューションズ株式会社
下村 正洋	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
杉本 隆洋	株式会社アズジェント
田中 暁	KDDI 株式会社
辻井 葉子	リコージャパン株式会社
辻村 啓	有限責任監査法人トーマツ
手塚 悟	慶應義塾大学
中島 大輔*	日本アイ・ビー・エム株式会社
中村 秀治	株式会社三菱総合研究所
菅野 憲昭*	富士通株式会社
間形 文彦	エヌ・ティ・ティ・コミュニケーションズ株式会社
三宅 功	エヌ・ティ・ティ・データ先端技術株式会社
山口 達也	有限責任あずさ監査法人
吉村 拓*	EY ストラテジー・アンド・コンサルティング株式会社

幹事　27 名　※2023 年 11 月 27 日現在　50 音順

海野 祐一	三菱電機インフォメーションネットワーク株式会社
大木 榮二郎	工学院大学 名誉教授
太田 利次	ジーブレイン株式会社
沖本 彰	KDDI 株式会社
梶田 祐美子	日本アイ・ビー・エム株式会社
川本 大亮	ＰｗＣあらた有限責任監査法人
幸田 一生	富士通株式会社
河野 省二	日本マイクロソフト株式会社
駒瀬 彰彦	株式会社アズジェント
小室 武晴	リコージャパン株式会社
近藤 健夫	ニッセイ情報テクノロジー株式会社
佐々木 浩一	富士通クラウドテクノロジーズ株式会社

清水 亨	東芝デジタルソリューションズ株式会社
下村 正洋	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
杉山 泰弘	NRI セキュアテクノロジーズ株式会社
鈴木 文章	有限責任あずさ監査法人
鈴木 庸介	NEC セキュリティ株式会社
芹川 健二郎	日本セキュリティ監査協会
中尾 康二	
永宮 直史	日本セキュリティ監査協会
成島 佳孝	株式会社日立製作所
西田 晃二	有限責任監査法人トーマツ
福井 慎二	エヌ・ティ・ティ・コミュニケーションズ株式会社
松尾 正浩	株式会社三菱総合研究所
松澤 伸一	株式会社 NTT データグループ
森島 直人	EY ストラテジー・アンド・コンサルティング株式会社
山岡 正輝	エヌ・ティ・ティ・データ先端技術株式会社

監査人推移

■ 資格認定者累計(格上申請を含む延べ数) ※2023 年 11 月 27 日現在

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
主任監査人	14	32	19	4	3	8	1	2	3	0
監査人	24	68	44	23	17	13	14	13	11	12
監査人補	24	74	28	41	108	90	57	63	35	44
監査ｱｿｼｴｲﾄ	30	40	38	64	70	62	65	47	27	41
内部監査人								26	66	104
小計	92	214	129	132	198	173	137	151	142	201
累計		306	435	567	765	938	1,075	1,226	1,368	1,569

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	累 計
主任監査人	1	0	2	2	0	2	2	0	1	0	96
監査人	10	9	11	12	9	13	7	11	9	10	340
監査人補	50	89	89	139	207	170	82	79	71	62	1,602
監査ｱｿｼｴｲﾄ	99	76	77	83	80	74	83	59	75	59	1,249
内部監査人	118	180	123	87	164	110	157	160	94	161	1,550
小計	278	354	302	323	460	369	331	309	250	292	4,837
累計	1,847	2,201	2,503	2,826	3,286	3,655	3,986	4,295	4,545	4,837	

出版書籍一覧

◇ **「IT 実務ハンドブックシリーズ システム監査 情報セキュリティ監査ハンドブック」**

著者　：特定非営利活動法人日本セキュリティ監査協会 (監修)
ティーエムエス (編集)
日本システム監査人協会(監修)
出版日：2004 年 10 月 30 日
出版社：秀和システム

◇ **「情報セキュリティ監査公式ガイドブック」**

著者　：特定非営利活動法人日本セキュリティ監査協会 (編集)
大木 栄二郎 (監修)
出版日：2007 年 12 月 1 日
出版社：日科技連出版社

◇ **「APT 対策入門　新型サイバー攻撃の検知と対応」**

著者　：特定非営利活動法人 日本セキュリティ監査協会 APT による攻撃対策と情報セキュリティ監査研究会
出版日：2012 年 11 月 1 日
出版社：インプレス R&D

◇ **「情報セキュリティ内部監査の教科書」**

著者　：特定非営利活動法人 日本セキュリティ監査協会
出版日：2013 年 2 月 14 日
出版社：インプレス R&D

◇ **「改訂新版 情報セキュリティ内部監査の教科書」**

著者　：特定非営利活動法人 日本セキュリティ監査協会
出版日：2016 年 8 月 5 日
出版社：インプレス R&D

◇ **「改訂三版 情報セキュリティ内部監査の教科書」**

著者　：特定非営利活動法人 日本セキュリティ監査協会
出版日：2017 年 12 月 1 日
出版社：インプレス R&D

◇ **「マイナンバー制度における情報セキュリティ監査の手引き」**

著者　：特定非営利活動法人日本セキュリティ監査協会 (編集)
出版日：2020 年 3 月 10 日
出版社：実教出版

◇ **「ISO/IEC 27001･27002 拡張によるサイバーセキュリティ対策: ISO/IEC TS 27100:2020 の解説と ISMS 活用術」**

著者　：特定非営利活動法人日本セキュリティ監査協会 (著)
永宮 直史 (編著)
出版日：2022 年 9 月 13 日
出版社：日本規格協会

◇ **「情報セキュリティ分野における自己適合宣言ガイド」**

著者　：特定非営利活動法人日本セキュリティ監査協会 調査研究部会　言明書 WG
出版日：2023 年 4 月 28 日
出版社：インプレス NextPublishing

お祝いメッセージ

東芝デジタルソリューションズ株式会社 様

情報セキュリティ監査制度20周年おめでとうございます！この20年間には、モバイルやクラウドの普及などコンピューティング環境に大きな変化があり、高度化、悪質化するサイバーセキュリティの脅威への対策を進めるうえで、情報セキュリティ監査制度は非常に重要な役割を果たしてきました。今後も、OT、IoT、AIなどの環境変化に伴うセキュリティの脅威にも対応した、監査制度の更なる進化と発展を祈念いたします。

NTTテクノクロス株式会社 様

情報セキュリティ監査制度20周年おめでとうございます！「情報セキュリティに関する監査」が必要であるという意識を広め、根付かせるのは大変だったと思います。本制度が発展してきたのはひとえに20年間の皆様のご尽力の賜物と考えております。今後も、日々進化するセキュリティ脅威やリモートワーク、クラウド、DXの導入等の環境の変化に対応すべく、さらに監査の価値を共に高めてまいりましょう。当社もその一助となれるよう努めるとともに、監査制度の更なる発展と成功を願っております。

株式会社三菱総合研究所 様

情報セキュリティ監査制度20周年おめでとうございます。監査制度立ち上げ当時に奔走されていた先輩諸氏のご苦労に、心より感謝申し上げたいと存じます。既にだいぶ記憶の彼方ではありますが、JASA設立時の関係者の皆様の晴れやかな笑顔が思い出されます。

また、その後も多くの方々のご尽力によって、制度の礎が築かれ強化されて参りましたこと、感謝の念に堪えません。今後とも次代を担う皆様方のご活躍を祈念しております。

三菱電機インフォメーションネットワーク株式会社 様

情報セキュリティ監査制度20周年おめでとうございます。日本における情報セキュリティ監査の確立・普及に多大な貢献をされてきましたことに、心より敬意を表します。DX化やグローバル化が急速に進み、IT環境が複雑化する中、情報セキュリティ監査の重要性がますます高まっています。これからも変化する環境に対応しながら、さらなる発展を遂げていくことを祈念しております。

株式会社アスラボ　羽生田　和正 様

「情報セキュリティ内部監査人の育成研修こと始め」

2022年度３月末の情報セキュリティ監査人資格制度の累計資格認定者は4693名であり、そのうち情報セキュリティ内部監査人は1507名を数えている。

JASA立ち上げ時の情報セキュリティ監査人育成計画では、まず外部監査人の育成のための情報セキュリティ研修コースを整備し、監査アソシエイトの育成から開始した。その後、保証型監査を含めたトレーニング研修コースを

立ち上げ、監査人補、監査人の育成に着手した。

一方、監査人育成の市場のニーズを見ると、民間企業や地方公共団体では自らの組織における内部監査人の育成研修要求が求められていることが分かってきたので、内部監査人コースの立ち上げを提案した。

研修ビジネスとして成り立つかどうかなど、監査協会の組織内部の検討において新たに内部監査人コースを実施する方針が決定し、監査基準・管理基準及びJASAの各種成果物を利用して情報セキュリティ内部監査人教科書の編集を開始した。これには西と東のワーキンググループにより規程集のサンプルなどを検討し、できるだけ内部監査の現場で実際に使用している素材をテキストの盛り込むようにした。

研修コースの募集は２００８年ごろから開始した。研修コース、トレーニングコースに加えて内部監査人コースがスタートした。当初の構想どおり、一般企業や地方公共団体や官公庁及び大学などの文教機関等が内部監査人育成の重要性を意識する中で、資格認定者は年々伸長する傾向にある。

コロナ禍の中では、新たにZoomによるリモート研修を開始した。Zoomのブレイクアウト機能を利用した個人演習とグループ演習及びネットによる修了試験は、利便性や有効性の面から好評であり監査人育成のメリットを向上することになった。JASAの研修制度としてWeb時代に相応し研修市場を開拓できたものと考えている。

情報セキュリティの技術と監査の分野の展開は急激であり、サイバーセキュリティの安全管理措置の強化のためには、クラウド化、リモートワーキング、ICTのビジネス継続などを取り込んだ内部監査人研修の普及が喫緊の課題となっている。これらについても時間をおかず追随できるよう準備を進めることが必要と考えている。

長崎県立大学　加藤　雅彦 様

情報セキュリティ監査制度20周年おめでとうございます。
関係者の皆様による様々な努力により、情報セキュリティ監査の重要性や認知度が高まった結果の20年と思います。
今後、貴協会、および情報セキュリティ監査のさらなる発展を祈念して、お祝いのメッセージとさせていただきます。

年表

年 西暦	年 和暦 平成	月	日	国	特定非営利活動法人　日本セキュリティ監査協会	その他	特記事項
2002	14	8				住民基本台帳ネットワークシステム（住基ネット）稼働	
		9		情報セキュリティ監査研究会設置			
2003	15	3		情報セキュリティ監査研究会報告書発行			
		4		情報セキュリティ管理基準Ver1.0　（経済産業省平成15年告示第112号） 情報セキュリティ監査企業台帳　（経済産業省平成15年告示第113号） 情報セキュリティ監査基準Ver1.0　（経済産業省平成15年告示第114号）		
		5	20		設立総会		
		10	10		特定非営利活動法人　日本セキュリティ監査協会発足（江東区東陽町本社） 土居範久（中央大学教授・慶應義塾大学名誉教授）会長就任		
		11	20		第1回情報セキュリティ監査人研修実施		
		12	18		設立記念　情報セキュリティ監査普及促進シンポジウム開催（東京）		
2004	16	1	29		設立記念　情報セキュリティ監査普及促進シンポジウム開催（大阪）		
		3	31		平成15年度情報セキュリティ監査制度普及啓発事業実施結果報告書納品		
		5	19		被監査主体のための実践情報セキュリティ監査セミナー（東京）		
		5	20		被監査主体のための実践情報セキュリティ監査セミナー（札幌）		
		5	27		被監査主体のための実践情報セキュリティ監査セミナー（大阪）		
		5	27		被監査主体のための実践情報セキュリティ監査セミナー（仙台）		
		6	1		2004年度定時総会		
		6	3		被監査主体のための実践情報セキュリティ監査セミナー（名古屋）		
		6	10		被監査主体のための実践情報セキュリティ監査セミナー（富山）		
		6	29		情報セキュリティフォーラム（東京）		
		11	2		公認情報セキュリティ監査人資格制度創設		
		12	27		第1回資格認定委員会		試験小委員会設置決定
2005	17	2	5		CAIS資格者第1号認定		
		2	2		情報セキュリティフォーラム（大阪）		
		3	31		平成16年度情報セキュリティ監査制度利用促進等事業実施結果報告書納品		
		3			JASA 広報誌『 Security Eye 』の創刊		
		5	11		審査委員会設置		
		5	25		2005年度定時総会		
		5	28		本所を茅場町（全国中小企業会館）に移転		
		6	2		第1回審査委員会		
		6	21		情報セキュリティフォーラム in Tokyo		
		6			平成17年度企業・個人の情報セキュリティ対策事業 （情報セキュリティ監査制度の利用促進）受託		保証型情報セキュリティ監査研究着手
		8	26		保証型情報セキュリティ監査プロジェクト開始（第1回意見交換会）		
		11	1		Security Eye Vol2発行		
		11	25		研修・トレーニング外部委託スキーム提言 （スキル部会から研修トレーニング小委員会提言）		
		12	6		情報セキュリティフォーラム in Sendai		
		12			（情報セキュリティ）監査企業紹介制度開始		
2006	18	1	25		情報セキュリティフォーラム in Nagoya		
		2	1		情報セキュリティフォーラム in Osaka		
		3	10		「情報セキュリティ監査人のつどい」　開催		
		3	31		平成17年度企業・個人の情報セキュリティ対策事業に関する実施結果報告書納品		
		5	20			JIS Q 27001:2006発行	
		5	20			JIS Q 27002:2006発行	
		6	6		2006年度定時総会		
		7	6		2006年度情報セキュリティ監査シンポジウム in Tokyo		
		8	28		外部研修実施機関による研修トレーニング開始		
		11	28		2006年度情報セキュリティ監査シンポジウム in Osaka		
2007	19	1	19		講師派遣（鳥取県西部町村情報化推進研究会：テーマ「自治体ののための実践的情報セキュリティ対策」）		
		1	31		2006年度情報セキュリティ監査シンポジウム in Winter		
		3	15		講師派遣（財団法人ソフトピアジャパン（大垣市）：テーマ「情報セキュリティ人材育成セミナー in Gifu」）		
		3	22		情報セキュリティ監査ミニセミナー in Kyoto		
		3	30		情報セキュリティ監査制度利用促進結果報告書納品 （保証型情報セキュリティ監査概念フレームワークとりまとめ）		保証型情報セキュリティ監査概念フレームワークとりまとめ 監査手続ガイド策定
		5	30		2007年度定時総会		
		9	18		2007年度全国縦断　情報セキュリティ監査セミナー in Sendai		
		10	16		全国縦断　情報セキュリティ監査セミナー in Sapporo		
		10	26		全国縦断　情報セキュリティ監査セミナー in Takamatsu		
		11	16		2007年度全国縦断　情報セキュリティ監査セミナー in Hiroshima		
		12	1		情報セキュリティ監査公式ガイドブック出版：日科技連		
		12	19		2007年度全国縦断　情報セキュリティ監査セミナー in Tokyo		
		12	20		2007年度全国縦断　情報セキュリティ監査セミナー in Nagoya		
2008	20	1	18		2007年度全国縦断　情報セキュリティ監査セミナー inToyama		
		2	7		2007年度全国縦断　情報セキュリティ監査セミナー in Osaka		
		3	7		2007年度全国縦断　情報セキュリティ監査セミナー in Fukuoka		
		3	31		情報セキュリティ監査制度利用促進結果報告書納品 情報セキュリティ管理基準Ver2.0作成		
		3			第1回 Security Eye News発信		
		5	15		西日本支部設立		
		6	3		2008年度定時総会		
		7	9		2008 年度情報セキュリティ監査シンポジウム in TOKYO		
		8	25		2008 年度情報セキュリティ監査セミナー IN SAPPORO		
		9	26		2008 年度情報セキュリティ監査セミナー in TAKAMATSU		
		10	2		2008 年度情報セキュリティ監査セミナー IN SENDAI		
		10	16		西日本支部設立趣旨説明・講演会（1回）		
		10	21		2008 年度情報セキュリティ監査セミナー IN FUKUOKA		
		11	11		2008 年度情報セキュリティ監査セミナーin Osaka		
		11	11		西日本支部講演会（2回）		
		12	19		2008 年度情報セキュリティ監査セミナー IN NAGOYA		

年		月	日	国	特定非営利活動法人　日本セキュリティ監査協会	その他	特記事項
西暦	和暦 平成						
2009	21	1	23		2008 年度情報セキュリティ監査セミナー in HIROSHIMA		
		1	28		CAISコミュニティ開始		
		2	1	情報セキュリティ管理基準（平成20年改正版）			
		2	13		2008 年度情報セキュリティ監査セミナー IN TOYAMA		
		2	27		2008 年度情報セキュリティ監査シンポジウム東京 in Winter		
		3	31		情報セキュリティ監査制度利用促進結果報告書納品		情報セキュリティ監査人の独立性ガイドライン策定
		5	28		2009年度定時総会		
		7	28		第1回情報セキュリティ監査実践セミナー（月例セミナー）（東京）		
		7	2		第1回　JASA西日本支部/CISSP関西コミュニティ合同セミナー		
		8	5		第2回CAISコミュニティ		
		8	18		第2回情報セキュリティ監査実践セミナー（東京）		
		8	28		2009年度情報セキュリティ監査シンポジウム in SAPPORO		
		9	17		第3回情報セキュリティ監査実践セミナー（東京）		
		9	30		2009年度情報セキュリティ監査シンポジウム in TAKAMATSU		
		10	2		2009年度情報セキュリティ監査シンポジウム in SENDAI		
		10	9		第2回　JASA西日本支部/CISSP関西コミュニティ合同セミナー		
		10	15		第4回情報セキュリティ監査実践セミナー（東京）		
		11	10		第5回情報セキュリティ監査実践セミナー（東京）		
		11	25		2009年度情報セキュリティ監査シンポジウム in TOYAMA		
		11	30		2009年度情報セキュリティ監査シンポジウム in TOKYO		
		12	3		第1回情報セキュリティ監査実践セミナー（大阪）		
		12	16		2009年度情報セキュリティ監査シンポジウム in OSAKA		
		12	17		第6回情報セキュリティ監査実践セミナー（東京）		
2010	22	1	15		第7回情報セキュリティ監査実践セミナー（東京）		
		1	18		2009年度情報セキュリティ監査シンポジウム in HIROSHIMA		
		1	26		2009年度情報セキュリティ監査シンポジウム in NAGOYA		
		2	5		2009年度情報セキュリティ監査シンポジウム in OITA		
		2	17		第8回情報セキュリティ監査実践セミナー（東京）		
		2	23		第2回情報セキュリティ監査実践セミナー（大阪）		
		3	3		第3回CAISコミュニティ		
		3	12		第9回情報セキュリティ監査実践セミナー（東京）		
		3	10		第３回　JASA西日本支部／CISSP関西コミュニティ合同セミナー		
		3	31		平成21年度 情報セキュリティ監査制度の利用促進に関する実施報告書納品 平成21年度　クラウドセキュリティ監査報告書納品		管理策の評価（アセスメント）に関する実践ガイド（ISO/IEC TR27008 付属書提案内容）
		4	1	クラウドサービスの利用のための情報セキュリティマネジメントガイドライン			
		6	1		2010年度定時総会		
		6	25		第４回　JASA西日本支部／CISSP関西コミュニティ合同セミナー		
		8	6		第1回　IT関連産業界ワークショップ（サプライチェーンワークショップ）		
		9	14		第2回　IT関連産業界ワークショップ（サプライチェーンワークショップ）		
		10	1		第５回　JASA西日本支部／CISSP関西コミュニティ合同セミナー		
		10	6		2010年度 情報セキュリティ監査シンポジウム in Tokyo		
		10	6		韓国KISIA、JNSAと協力に関するMOU締結		
		10	13		第3回　IT関連産業界ワークショップ（サプライチェーンワークショップ）		
		11	2		月例セミナー開始		
		11	10		第4回　IT関連産業界ワークショップ（サプライチェーンワークショップ）		
		11	18		第1回　製造業界・運輸業界ワークショップ（中部圏ワークショップ）		
		12	7		第5回　IT関連産業界ワークショップ（サプライチェーンワークショップ）		
2011	23	1	13		第2回　製造業界・運輸業界ワークショップ（中部圏ワークショップ）		
		1	18		第6回　IT関連産業界ワークショップ（サプライチェーンワークショップ）		
		1	20		第1回 日韓（韓日）情報保安シンポジウム（ソウル）		
		1	28		第６回　関西情報セキュリティ団体（JASA/CISSP/JNSA）合同セミナー		
		3	11		平成22年度 情報セキュリティ監査制度の利用促進に関する実施報告書納品 平成22年度　クラウドセキュリティ監査報告書納品	東日本大震災	
		4	4		ベトナム調査		
		5	19		2011年度定時総会		
		6	1		本所を東陽町（東陽町ディアイティ本社内）に移転		
		7	11		内部監査人能力認定制度開始		
		7	29		第7回関西セキュリティ団体合同セミナー（JASA、CISSPにJNSAが加わる）		
		10	9		ISO SC27国際会議に参加		
		10				ISO/IEC TR27008発行	
		11	10		第2回 日韓（韓日）情報保安シンポジウム（東京）		
		11	25		第8回　関西セキュリティ団体合同セミナー		
2012	24	2	20		平成２３年度企業・個人の情報セキュリティ対策促進事業報告書納品 クラウド情報セキュリティ管理基準 サプライチェーン情報セキュリティ管理基準		
		3	16		第9回　関西セキュリティ団体合同セミナー		
		5	29		2012年度定時総会		
		6	29		第10回関西情報セキュリティ団体合同セミナー		
		10	26		「APT対策入門」出版（インプレスR&D）		
		10	31		情報セキュリティ監査ワークショップ開催		
		11	15		第11回関西情報セキュリティ団体合同セミナー		
		12	4		第1回クラウド情報セキュリティ監査研究会開催		
		12	18		情報セキュリティ監査実務指針一般指針とりまとめ		
2013	25	2	1		第12回関西情報セキュリティ団体合同セミナー		
		2	15		情報セキュリティ内部監査の教科書出版（インプレスR&D）		
		3	10	クラウドサービスの利用のための情報セキュリティマネジメントガイドライン2013年度版			
		4	25		クラウド情報監査制度記者発表（パイロット監査結果報告）		
		5	19		クラウド情報監査制度講演（CSAセミナー；シンガポール）		
		5	24		第13回関西情報セキュリティ団体合同セミナー		
		5	29		2013年度定時総会 会長賞を品質管理タスクフォースメンバーに授与		
		6	21		第1回月例会開催		
		9	20		第14回関西情報セキュリティ団体合同セミナー		
		12	5		第1回サイバーセキュリティフォーラム（EYと共催）		
		12	19		第15回関西情報セキュリティ団体合同セミナー		

年 西暦	和暦 平成	月	日	国	特定非営利活動法人　日本セキュリティ監査協会	その他	特記事項
2014	26	1	31		第２回サイバーセキュリティフォーラム（EYと共催）		
		4	25		JASA-クラウド情報セキュリティ推進協議会発足に関する記者会見		
		5	28		2014年度定時総会		
		6	27		第16回関西情報セキュリティ団体合同セミナー開催		
		7	25		JASA-クラウド情報セキュリティ推進協議会発足		
		9			クラウド情報セキュリティ管理基準公開		
		9	26		第17回関西情報セキュリティ団体合同セミナー		
		9	24		平成２６年度サイバーセキュリティ経済基盤構築事業受託（クラウドセキュリティ監査制度の見直し）		
		12	5		第1回　サイバーセキュリティセミナー　（サイバーセキュリティフォーラム：EYとの共催）		
2015	27	1	31		情報セキュリティ監査制度10周年記念セミナー第2回　サイバーセキュリティセミナー　（サイバーセキュリティフォーラムとの共催）		
		2	6		第18回関西情報セキュリティ団体合同セミナー		
		2	27		平成２６年度サイバーセキュリティ経済基盤構築事業納品 クラウド情報セキュリティ管理基準改定作業完了		
		4	14		JASA技術監査特別セミナー サイバー攻撃/内部不正対策の為の情報セキュリティ技術監査		
		5	27		2015年度定時総会		
		7	10		第19回関西情報セキュリティ団体合同セミナー		
		7	30		情報セキュリティ監査基準改正説明会		
		12				ISO/IEC27017発行	
		12	9		第3回サイバーセキュリティフォーラム（EYと共催）		
		12	11		第20回関西情報セキュリティ団体合同セミナー		
2016	28	1	15		営業秘密保護促進協議会発足（当協会が幹事として参加）		
		2	10		CSゴールドマーク認定１号		
		2	12		オリンピック・パラリンピックに向けたセキュア社会形成セミナー 経営とサイバーセキュリティ対策セミナー		
		2	28	情報セキュリティ管理基準（平成28年改正版）	平成28年版クラウド情報セキュリティ管理基準公開（JIS Q 27017準拠）		
		5	25		2016年度定時総会		
		6	27		情報セキュリティ監査セミナー		
		7	26		第21回関西情報セキュリティ団体合同セミナー		
		8	22		IoT勉強会		
		12	22		第22回関西情報セキュリティ団体合同セミナー		
2017	29	9	27		第1回スマートメータシステム情報セキュリティ監査制度運営委員会		
		5	12		第23回関西情報セキュリティ（団体）合同セミナー		
		5	25		2017年度定時総会		
		8	28		月例会最終回（以降、定例会として実施）		
		10	3		情報セキュリティ監査着手セミナー		
		11	10		パーソナルデータ監査とFISC安対準拠情報セキュリティ監査基準 -WG活動成果研究会-		
		11	30		定例会開始		
		12	5		2017年度　第2回サイバーセキュリティワークショップ		
2018	30	1	5		情報セキュリティ監査人が選ぶ2018年度の情報セキュリティ十大トレンド公表		
		1	26		サイバーセキュリティ机上演習ワークショップ		
		2	28	情報セキュリティサービス基準、情報セキュリティサービスに関する審査登録機関基準告示			
		3	9		第24回関西情報セキュリティ（団体）合同セミナー		
		5	24		2018年度定時総会		
		6	12		情報セキュリティサービス基準審査登録委員会第1回会合		
		7		情報セキュリティサービス基準適合サービスリスト公開（IPA）			
		8	15		本所を茅場町（フォーラム島田Ⅱ）に移転		
		9	16		2018年度工学院大学寄附講義開始（企業経営と情報セキュリティ；情報セキュリティ監査入門）		
		11	13		情報セキュリティ監査ワークショップ 「情報セキュリティ監査のためのリスク評価講座」		
2019	31 令和１	1	7		情報セキュリティ監査人が選ぶ2019年度の情報セキュリティ十大トレンド公表		
		3	22		第25回関西情報セキュリティ（団体）合同セミナー		
		5	30		2019年度定時総会		
		6	13		第26回関西情報セキュリティ（団体）合同セミナー		
		7	12		「サイバーセキュリティと監査」パネルディスカッション 第8回サイバーセキュリティ国際シンポジウム（慶應大学）		
		7	30		JASA 西日本支部主催セミナー「製品セキュリティセミナー」		
		9	25		NISC情報セキュリティ監査研修講師派遣（25、26日）		
		10	24		サイバーセキュリティ対策と監査の実践セミナー		
		11	6		第27回関西情報セキュリティ（団体）合同セミナー		
		11	21		ラウドサービスの統制を理解する　～ SOC2レポートの読み解き方講座		
		12	12		「信頼できるクラウドへのアプローチ」講演＆パネルディスカッション 第9回サイバーセキュリティ国際シンポジウム（慶應大学）		
2020	2	1	6		情報セキュリティ監査人が選ぶ2020年度の情報セキュリティ十大トレンド公表		
		2	1	新型コロナウィルスによるパンデミック発生（ダイヤモンド・プリンセス号那覇寄港、感染確認）			
		2	20		マイナンバー制度における情報セキュリティ監査の手引出版（実教出版）		
		5	22		2020年度定時総会		
		6	30	「政府情報システムのためのセキュリティ評価制度」（ISMAP）の運用を開始			
		8	6		ISMAP監査機関審査委員会開催		情報セキュリティ監査企業台帳廃止
		9	18		スマートメーターシステム情報セキュリティ監査制度説明会		
		9	30		ISMAP制度研修会		
		10	7		「マイナンバーと監査」パネルディスカッション 第10回サイバーセキュリティ国際シンポジウム（慶應大学）		
		11	17		サイバーセキュリティ対策マネジメントガイドライン Ver2.0公開		
2021	3	1	6		情報セキュリティ監査人が選ぶ2021年度の情報セキュリティ十大トレンド公表		
		2	4		ハンズオンワークショップ 情報セキュリティ監査人のためのクラウドセキュリティ入門 ～ クラウドの構築実践とクラウドセキュリティの実際（1日目）		
		2	12		ハンズオンワークショップ 情報セキュリティ監査人のためのクラウドセキュリティ入門 ～ クラウドの構築実践とクラウドセキュリティの実際（2日目）		
		3	26		勉強会「監査人必見！クラウドサービスの統制を理解するためのSOC2レポートの活用講座」		
		4	5		情報セキュリティサービス基準審査登録制度のWebサイトの全面リニューアル		
		5	28		2021年度定時総会		

年		月	日	国	特定非営利活動法人　日本セキュリティ監査協会	その他	特記事項
西暦	和暦 平成						
2022	4	1	6		情報セキュリティ監査人が選ぶ2022年度の情報セキュリティ十大トレンド公表		
		1	28		ISMAP制度研修会		
		2	17		WG主催セミナー施行直前！　改正個人情報保護法の概要と実務対応上のポイント」		
		4	1	情報セキュリティサービス基準第2版を施行			
		4	1	情報セキュリティサービスに関する審査登録機関基準第2版を施行			
		5	26		2022年度定時総会		
2023	5	1	6		情報セキュリティ監査人が選ぶ2023年度の情報セキュリティ十大トレンド公表		
		1	19		パネルディスカッション「令和5年度の情報セキュリティ監査の注力点　～情報セキュリティ10大トレンドをもとに」		
		2	23		協会認定監査実技コース開始		
		4	1	情報セキュリティサービス基準第3版を施行			
		4	1	情報セキュリティサービスにおける技術及び品質確保に資する取組の例示第2版を施行			
		4	28		「情報セキュリティ分野における自己適合宣言ガイド」出版		
		5	26		2023年度定時総会		
		7	11		助言型情報セキュリティ監査における監査リーダの実務心得 v.1.0発行		
		10	1		情報セキュリティ監査用語集Ver３.0発行		
		10	10	情報セキュリティ監査制度創設２０周年			
		10	10		協会設立20周年		
		10	10		情報セキュリティ監査制度創設２０周年記念イベント		

謝辞

2023 年 4 月で情報セキュリティ監査制度は 20 周年を迎えました。この節目にあたり、情報セキュリティ監査制度のこれまでを振り返るとともに、未来への展望を、会員はじめとする関係者の皆様と共有し、祝意を表す場として、20 周年記念イベントを 10 月 10 日（火）に開催いたしました。

イベントにおきましては、制度創設当初よりご尽力いただいた方々によるご講演と、未来に向けたパネルディスカッションを実施、300 名近くの方にご来場いただき、盛況の中、無事イベントを終えることができました。ご協力いただきました関係各位にはあらためて感謝の意を表します。

本記念誌の編集にあたっては、協会において過去の作成例はないうえに、対象とする期間も 20 年と長期にわたるものでしたので、事務局で内容を充実させつつ、関係の方々にできるだけお手間をお掛けしないようなまとめ方について検討を重ねました。最終的には講演録や寄稿文をベースとすることで、情報セキュリティ監査委制度創設後の 20 年間にわたる活動を簡潔にまとめることができたと思います。ご講演をいただいた皆様、寄稿文、原稿をご執筆いただいた方々を含め、編集に協力いただいた皆様のご尽力に厚く御礼申し上げます。

今後、情報技術の進化とサイバー空間の拡大により、情報セキュリティの重要性は高まり、それを確実にするための情報セキュリティ監査の重要性もますます高まるものと思います。それに従い監査の対象・分野も絶えず変化し続けるものと思いますが、情報セキュリティ監査制度の意義や協会の活動目的は大筋で変わることはないものと考えます。

活動を進める上で折に触れて本誌を参照し、この 20 年間の活動に立ち返ることで、制度の発展に尽力いただいた諸先輩方の精神を引き継ぎつつ、時代に合わせて必要となる新しい活動を進めていけると幸いです。また本誌が皆様のこれからの活動方針、計画の策定にお役に立つものになることを願っております。

2024 年 2 月
特定非営利活動法人 日本セキュリティ監査協会
事務局長　芹川 健二郎

情報セキュリティ監査制度 創設 20 周年 記念誌

2024（令和６）年 3 月 29 日　発行
編集・発行者　特定非営利活動法人 日本セキュリティ監査協会
〒104-0033
東京都中央区新川 1-4-8 フォーラム島田Ⅱ 2F