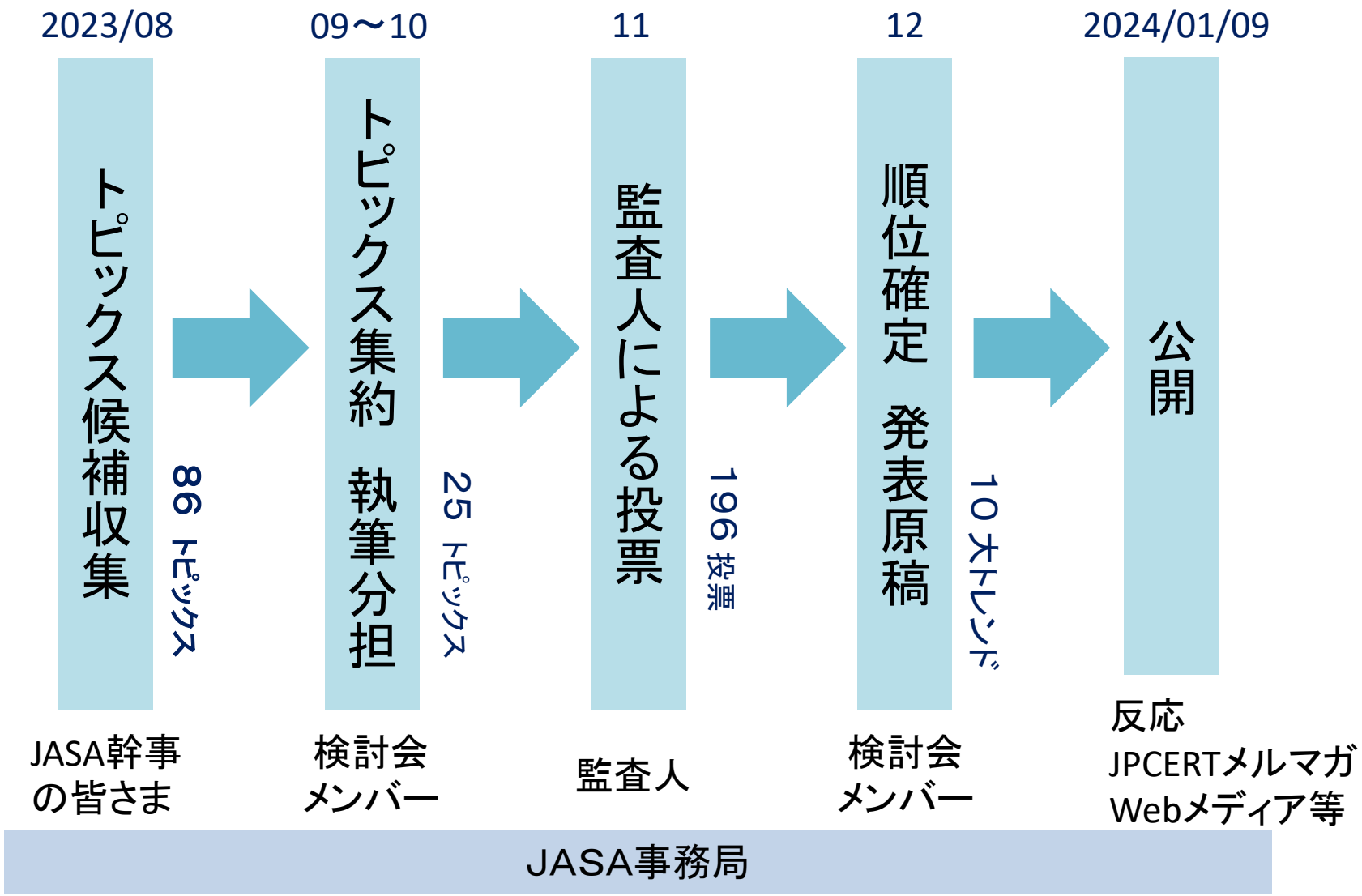
2023年度第4回定例研究会　パネルディスカッション

2024年度の情報セキュリティ監査の注力点
～情報セキュリティ十大トレンドをもとに～

2024年1月22日

日本セキュリティ監査協会

2024 情報セキュリティ十大トレンド 選考過程



監査人のおもな投票理由

１位　生成ＡＩの悪用と誤用により増加するセキュリティ事故

- 生成AIを積極的に活用した効率化や生産性の向上は重要ではあるが、「負の側面」に対しての対策が十分にできていなくてはならない。「悪用」に対する対策の実施は当然であるが、想定外のリスク事象という意味では「誤用」に対しての対策が非常に重要である。

２位　他人事ではありません。日常化するランサムウェア被害

- 連日ニュースにも取り上げられたりと、これだけ被害が拡大している中で、どこか他人事のようになっている感じがする。実被害に遭った企業の公開情報から被害状況を整理して、自分の身に降りかかったときをイメージできるよう情報をまとめ、自組織の啓発活動を行う。
- 被害企業を支援しているが、被害に遭うと対策検討は進む。いまだに他人事だと考える企業が多くあるのは事実。

３位　国家支援型組織によるサイバー攻撃の深刻化

- サイバー攻撃は一つのビジネスモデルの活動に位置付けられ、攻撃者の背後で政府が支援していることも想定される。つまり個人間ではなく国家間、さらにはサプライチェーンを標的とした段階的な攻撃により様々な分野へ影響が及ぶ可能性があるので、今後も動向を注視すべきと考えたため。
- 従来の悪戯・技術誇示といったものから、経済に発展してきているが、さらに国防に関わる事案となり、重要度が増すため。

４位　重要インフラを支える供給網（中小企業）がサイバー攻撃ターゲットに

- 重要インフラを狙った攻撃は以前からありましたが、大きな企業のセキュリティ対策が進められる中で、その攻撃ターゲットが対策に抜けがある可能性のある業務委託先企業である中小企業に移ってきている事もあり、注目すべき事項であると考えられるため。

監査人のおもな投票理由（続き）

５位　重要性が高まる事前評価，　生成ＡＩのリスク

- 生成AIによるアウトプットは、正確なのか、捏造が混じっているのかの、コンテクストが善意なのか、悪意なのか、等を検証／精査し、問題がないことを確認しなければ使い物にならない。そのため監査対象として、そのプロセスや結果を監査人が評価するのが大変困難であることから。

６位　クラウド設定不備によるセキュリティ事故の多発

- 名だたる大手企業がクラウドサービスの設定ミスを連発し、国民総数の何割かという規模の個人情報漏洩事故が発生している。個人情報保護法の届け出義務の厳格化もあり、これまでは水面下で処理されていた見えない漏洩事案が、表へと出るようになった。クラウドサービスの設定状況を監査する視点や監査人が重要視されてくるだろう。
- インシデントの原因がクラウドの設定ミスという話は関係する組織でも「よく聞く」ようになった。クラウド利用の促進は非常に便利でビジネスの維持・拡大に欠かせないものになっているが、現場に「使えればOK」という認識があるとインシデントのリスクが非常に高くなる。すごく身近な問題。
- SIerによるクラウド導入時の初期設定不備によるセキュリティ事故は少なからず発生している。そのため、構築時のマニュアル整備やセキュリティチェックなど対応していく必要があると思う。

７位　人材の流動化に伴う営業機密の流出増加

- 業務委託化やサプライチェーン、生成ＡＩやリモートワーク等の環境の変化が著しいが、結局は、取り扱う人材（人間）の意識が関りを持つことになり、あらゆるリスクにおいても内部統制の乱れや不徹底などから生じる内部要員の問題（内部犯行・内部不正）のコントロールをどのように改善するか検討課題と考える。

監査人のおもな投票理由（続き）

8位　脆弱性管理体制の再検討の加速

- 業務システム群へのパッチ適用に苦慮しているため。
- デバイスやソフトウェアは増えて複雑になってきているが、それを管理するための脆弱性管理体制はあまり進化しないままであるため。SBOM等の話も出てきてはいるが、自動化しないと結局対応コストだけかかるので自動化していくだろうとみているがそのようなサービスが拡大していないため。
- 脆弱性管理は、基本的な対応であり歴史のあるテーマでありながら未だに確実に実行することが難しい組織が多いと感じます。脆弱性をついた攻撃による被害は年々深刻になっていると考えます。

9位　止まらないランサムウェアの進化

- 防御側のランサムウェア対策は進んでいるが、攻撃側もAIの活用などで新たな攻撃の手口を開発すると考えられる。また、攻撃側の組織の活動は分業されているため、マルウェアの開発者は新たな攻撃の手口の開発に集中できることもランサムウェアの進化の要因と思われる。
- ランサムウェアの被害は増加の一途をたどっており、RaaSによる分業化や国家の関与により、進化のトレンドは続くと思われる。

10位　経営課題として浮上、サイバー人材育成

- セキュリティ対策を外部に丸投げしており、本当に必要な対策、施策を理解していない。しかしながら、今まで特に問題が発生しておらず、経営層だけでなく技術者も現状のセキュリティ対策を問題視していない状況に非常に危機感を感じている。
- 情報セキュリティという話と、人的資源投入が結びついておらず、人件費として一括され投入がままならない現状に悩まされている学校現場が多い。

検討会メンバー紹介

＊：本日のパネルメンバー

間形文彦＊
NTT
ｺﾐｭﾆｹｰｼｮﾝｽﾞ(株)

永宮直史＊
日本セキュリティ
監査協会

菅谷光啓
内閣ｻｲﾊﾞｰ
ｾｷｭﾘﾃｨｾﾝﾀｰ

佐藤元彦
伊藤忠商事株式会社

佐々木宏幸＊
株式会社
ディアイティ

久保田朋秀＊
日本マイクロソフト
株式会社

加藤雅彦
長崎県立大学

加藤俊直＊
PwC Japan有限責任
監査法人

大木榮二郎＊
工学院大学名誉教授

パネルメンバー略歴ご紹介

間形文彦

NTTコミュニケーションズ(株)
情報セキュリティ部
担当部長

JASA公認情報セキュリティ監査人
JASA理事
JCISPAコア会議メンバ

永宮直史

日本セキュリティ監査協会
エグゼクティブフェロー

JASA主席監査人
ISO/IEC SC27 WG1,
同 WG4 Expert
JCISPAコア会議メンバー

（動画参加）

佐々木宏幸

株式会社ディアイティ
CISO

JASA公認情報セキュリティ監査人
JASA試験小委員会委員
情報処理試験・情報処理安全確保支援士試験委員
CISSP

久保田朋秀

日本マイクロソフト株式会社
パブリックセクター事業本部
技術戦略本部
クラウドセキュリティ推進室長

JASA公認情報セキュリティ監査人
JCISPAコア会議メンバー
CISSP

加藤俊直

PwC Japan有限責任監査法人
パートナー

JASA公認情報セキュリティ監査人
JASA 理事
JCISPAコア会議メンバー

大木榮二郎

工学院大学名誉教授

JSSM名誉会長
JASA公認情報セキュリティ主席監査人
JCISPA会長
JASA スキル部会長
JASA 審査委員会委員

監査人の警鐘-2024年情報セキュリティ十大トレンド

-生成AIの急激な利用拡大と高度化するサイバー攻撃への対応が急務-

2024年1月9日

順位	項目	ポイント
1 (-)	生成AIの悪用と誤用により増加するセキュリティ事故	188
2 (3)	他人事ではありません。日常化するランサムウェア被害	102
3 (9)	国家支援型組織によるサイバー攻撃の深刻化	95
4 (2)	重要インフラを支える供給網（中小企業）がサイバー攻撃ターゲットに	86
5 (-)	重要性が高まる事前評価，　生成AIのリスク	80
6 (5)	クラウド設定不備によるセキュリティ事故の多発	56
7 (-)	人材の流動化に伴う営業機密の流出増加	51
8 (17)	脆弱性管理体制の再検討の加速	46
9 (3)	止まらないランサムウェアの進化	46
10 (-)	経営課題として浮上、サイバー人材育成	44

カッコ内は昨年順位

パネルディスカッションの進め方

1．ビデオ解説　5分
- ◆佐々木宏幸　「サイバー攻撃、ランサムのトレンド」

2．Round1：2024年度の経営環境変化　45分
- ◆間形文彦　　「生成AI、重要インフラ」
- ◆加藤俊直　　「人材流動化と営業秘密」
- ◆永宮直史　　「ランサムウエア、人材育成」
- ◆久保田朋秀　「クラウドのセキュリティ、脆弱性」

3．Round2: 2024年度監査の重点の考え方　20分
- ◆各パネラーから　特に強調したい監査ポイント
- ◆監査人としてのスキルアップについての提言等

4．参加者からの質問にもお答えします　10分
- 随時Chatでお知らせください

ビデオメッセージ

「サイバー攻撃、ランサムのトレンド」

株式会社ディアイティ　佐々木宏幸

下記URLより動画をご確認いただけます。
https://youtu.be/9eYCBdTLDSk

3位　国家支援型組織によるサイバー攻撃の深刻化

- 国家間の対立を背景とした攻撃の増加
  - 戦略的・計画的な攻撃が多いとされる

軍事的・外交的アピール	政府機関や重要インフラに対するDDoS、Webページ改ざんなど
技術や政策等の情報の窃取	軍事技術に転用可能な民生品のメーカーや各種団体に対する攻撃など
外貨(戦費)の獲得	経済制裁下での暗号資産の奪取 ⇒大量破壊兵器の開発に?

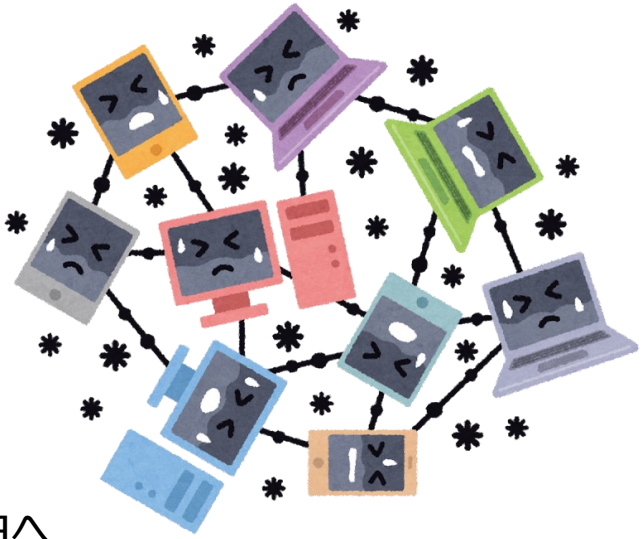
  - 攻撃手法はカスタマイズ化の傾向
- サプライチェーンに対する攻撃も
  - 協力会社や海外子会社を経由した攻撃も頻発
  - 情報や業務が安全保障・国家戦略的にどのような重要性を持つか?
- 大阪万博に向け攻撃が増加?

9位　止まらないランサムウェアの進化

■ エコシステムの変化

暗号化と
身代金の要求 → 二重の脅迫
(二重恐喝) → ノーウェアランサム / 分業化・ビジネス化

- ノーウェアランサム：暗号化せず窃取・脅迫を行う
- 分業化・ビジネス化が進む傾向にある
  - ◆RaaS (Ransomeware as a Service)
  - ◆IAB (Initial Access Broker)



■ 侵入経路・攻撃の変化

- 侵入経路はメール・Webから脆弱なVPN/RDP経由へ
- 同一のランサムウェアを複数の攻撃グループが利用するケース
- 同一の攻撃グループが複数のランサムウェアを利用するケース

監査の視点

- サイバーキルチェーンを想定した視点
  - 偵察 → 武器化 → 配置 → 悪用 → 侵入 → 潜伏 → 達成
  - どこかでチェーンを断ち切ることはできないか?
- インシデントレスポンスの視点
  - 準備 → 特定 → 封じ込め → 根絶 → 復旧 → 学習
  - 組織は各段階でどのような対応が可能か?
  - 外部からの援助は得られるか?
- 警察庁の調査(2023)
  - ランサムウェア被害に遭った組織のうち4割近くは監査を実施していた
  - 監査でのリスクの把握、改善提言により被害状況は変わっていた?
  - 改めて監査人の役割の大きさ、監査の重要性を認識したい

ROUND 1

2024年度の経営環境変化

生成AIの悪用と誤用　/

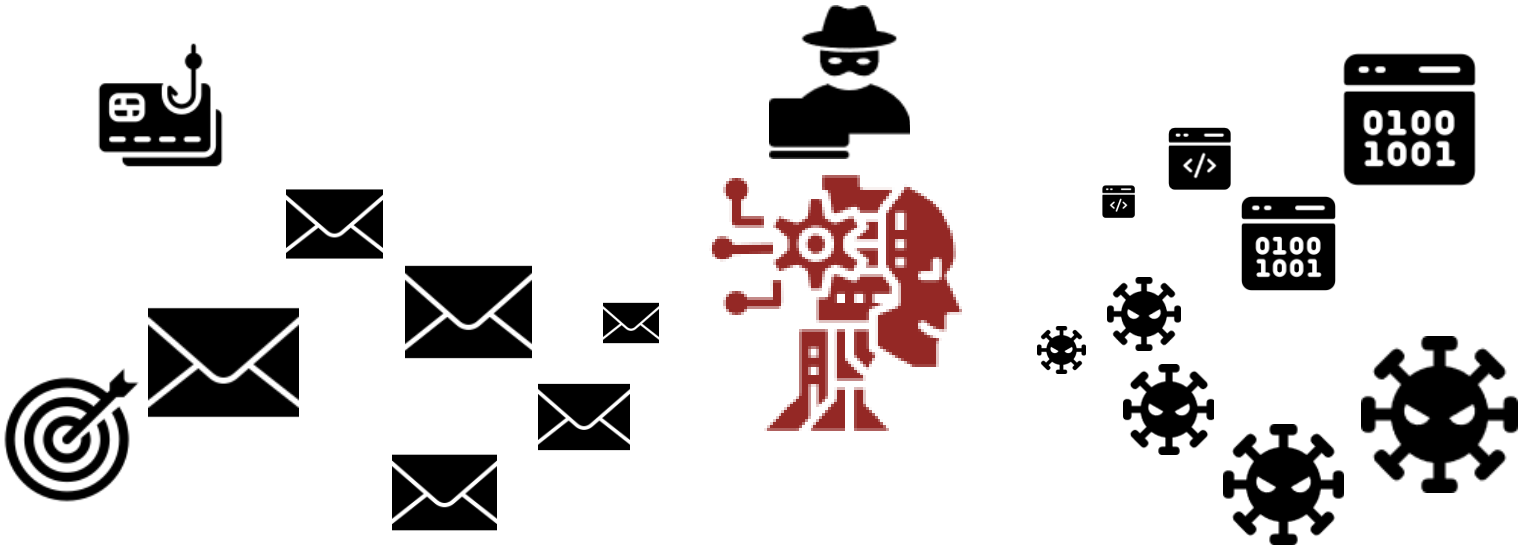
重要インフラを支える供給網（中小企業）が攻撃目標に

NTTコミュニケーションズ(株)　間形文彦

生成AIの悪用と誤用

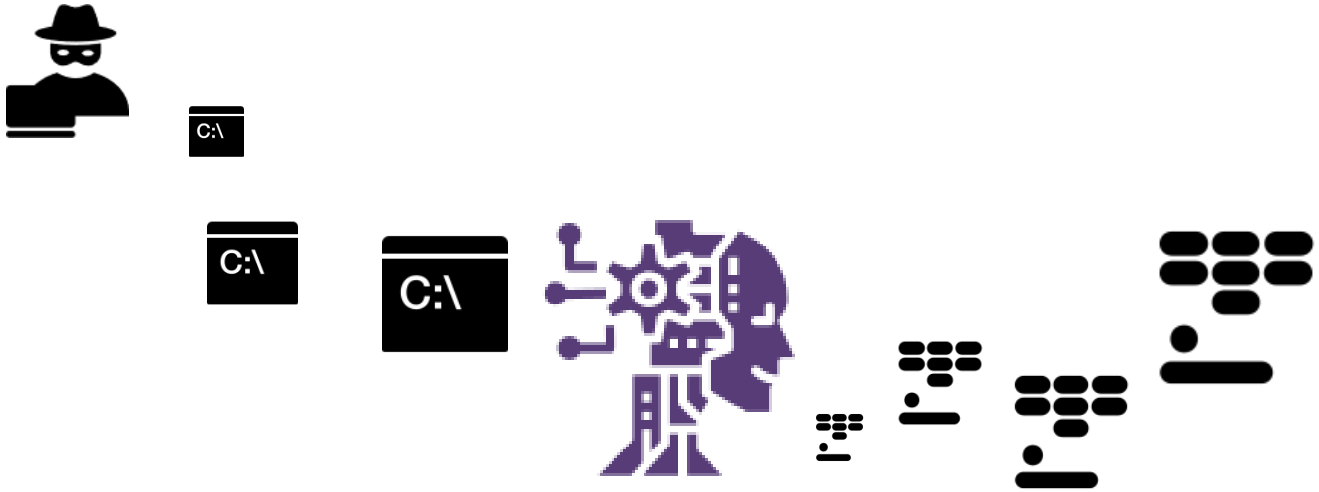
生成AIの悪用

フィッシング、詐欺（BEC）、標的型攻撃のためのメール、マルウェアのプログラミングによる攻撃の自動化と量産化



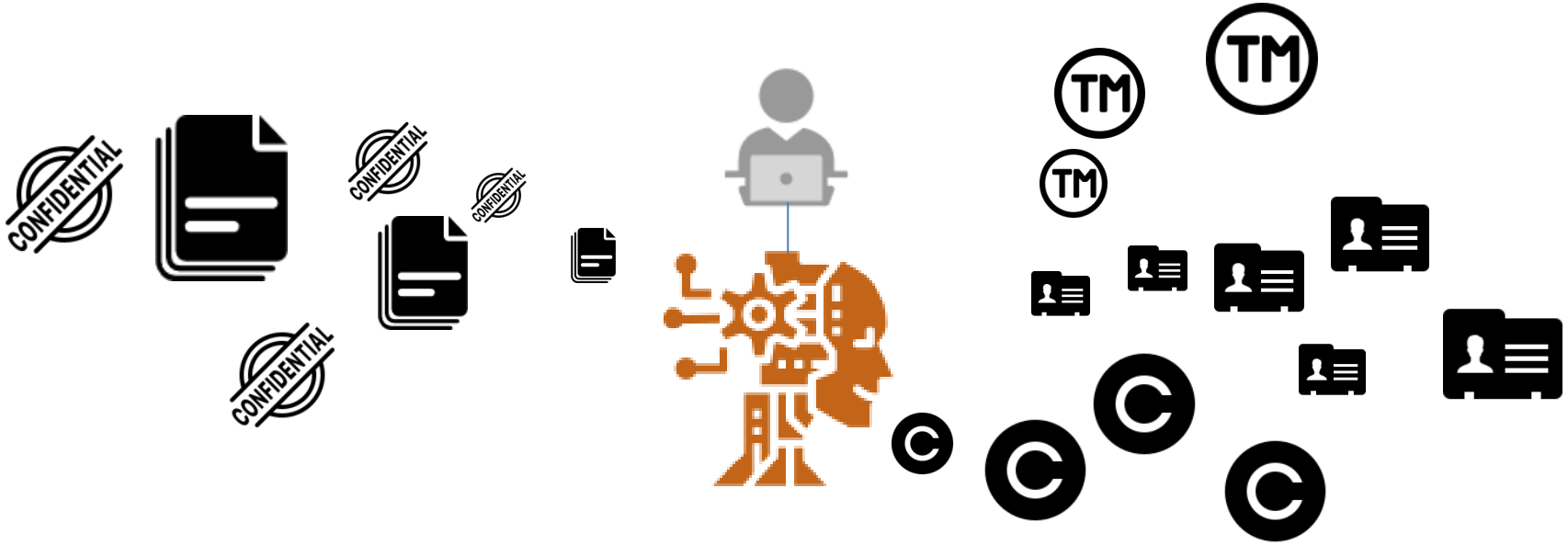
生成AIへの攻撃

生成AIの指示文（プロンプト）に対する攻撃　プロンプトリーク、ジェイルブレイクなど



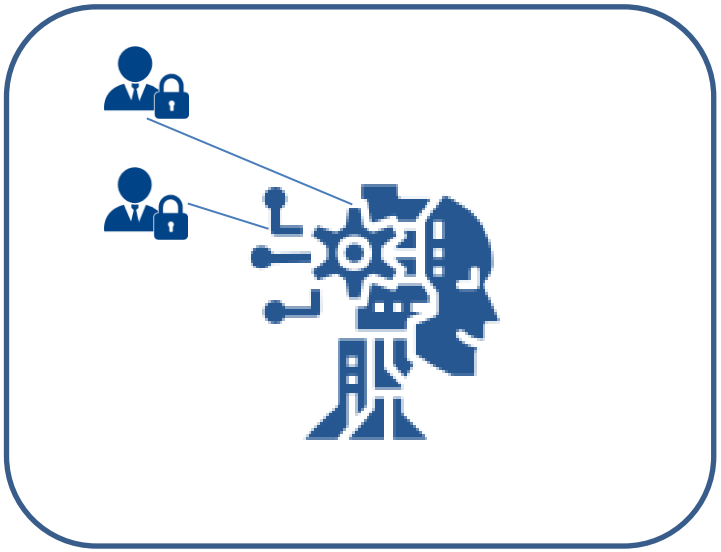
生成AIの誤用

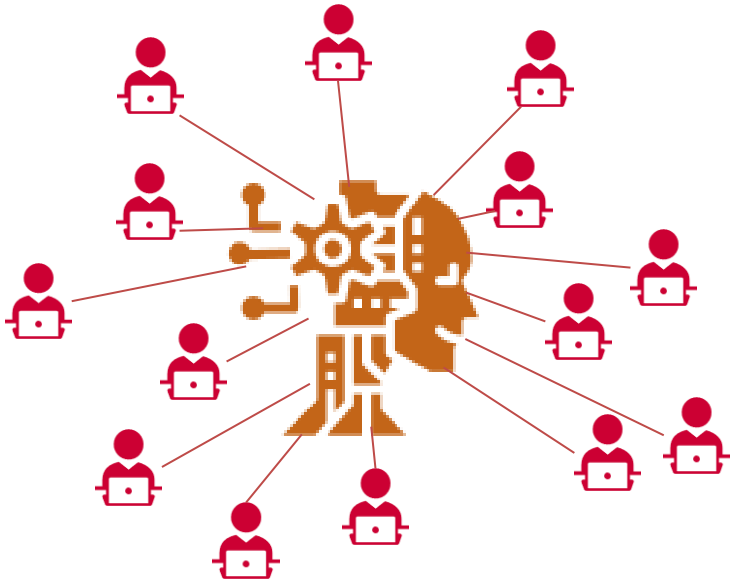
第三者と契約したNDA違反、個人情報の同意なき第三者提供、第三者の著作権・商標権の侵害の可能性



生成AIの利用者の範囲（特定利用者/不特定利用者）

特定利用者に閉じたデータ利用を保証する契約型と、不特定の利用者に広く開示される約款型





生成AIの利用者に対する監査の留意点

- 利用する生成AIは、指示文（プロンプト）への既知の攻撃に対する**脆弱性**がないか。
- 生成AIへのアクセスの認証は、多要素認証等の強固な認証方式によって、**なりすまし対策**が施されているか。
- 入力したデータが生成AIのモデル学習に使われる場合、当該**データ及び学習したモデル**の利用範囲は、当該**利用者に限定**されるか。または当該**利用者以外に公開**され共用されるか。
- 利用者が取得している個人情報を生成AIに入力する場合、当該個人情報の取得時の利用目的を逸脱**（目的外利用）**していないか。また、本人の同意のなく個人情報を生成AI事業者に提供**（同意なき第三者提供）**することにならないか。
- NDA（守秘義務契約）により利用者が他者から取得した情報を生成AIに入力する場合、生成AI事業者への情報開示となり、**守秘義務違反**とならないか。
- 生成AIが出力した結果を利用する場合、他者の**知的財産権**（著作権、商標権、意匠権、特許権等）の**侵害**に該当しないか。

重要インフラを支える供給網（中小企業）が攻撃目標に

重要インフラ14分野

情報通信

金融

航空

空港

鉄道

電力

ガス

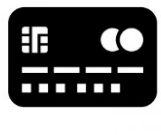
政府・行政サービス（地方公共団体含む）

医療

水道

物流

化学



クレジット

石油

出典：「重要インフラのサイバーセキュリティに係る行動計画」2022年6月17日 サイバーセキュリティ戦略本部　https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf

特定社会基盤（経済安全保障推進法）


情報通信


金融


航空


空港


鉄道


電力


ガス


政府・行政サービス（地方公共団体含む）


医療


水道


物流
貨物自動車運送
外航貨物


化学


クレジット


石油


放送


郵便

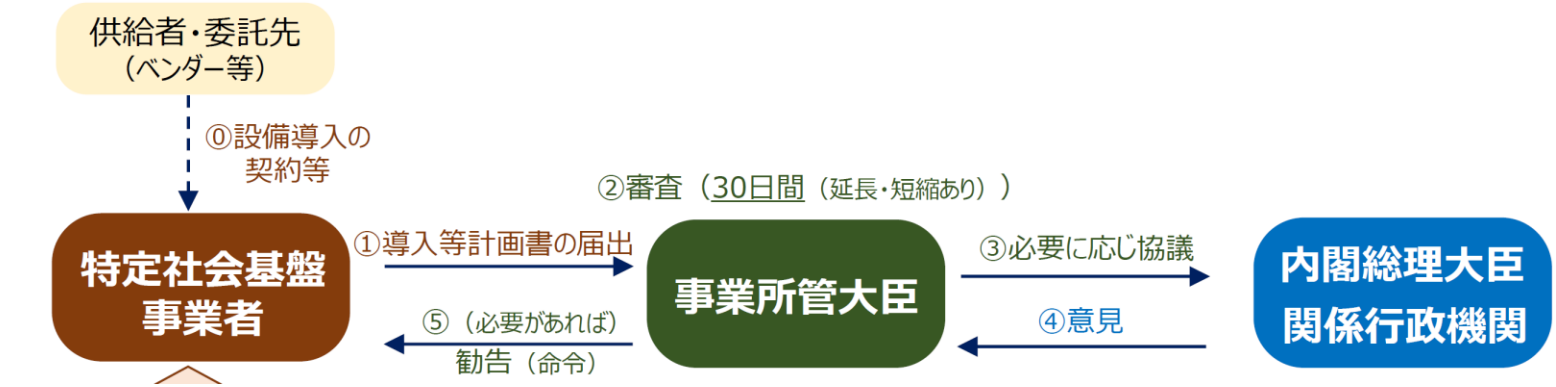
経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和四年法律第四十三号）第50条1項による指定事業分野

経済安全保障推進法と特定社会基盤役務

経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の概要

- ✓ 国民生活及び経済活動の基盤となっている「特定社会基盤役務」（基幹インフラ）の安定的な提供を確保することが重要であるところ、その用に供する重要設備は、役務の安定的な提供を妨害する行為の手段として使用されるおそれがある。
- ✓ そのため、経済安全保障推進法※第３章において、**国が一定の基準のもと、規制対象とする事業（特定社会基盤事業）・事業者（特定社会基盤事業者）を指定**し、指定された事業者が、**国により指定された重要設備（特定重要設備）**の導入・維持管理等の委託をしようとする際には、**事前に国（事業所管大臣）に届出を行い、審査を受けなければならない**こととしている。
  ※　経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第43号）
- ✓ 国は、**届け出られた計画書に係る特定重要設備が妨害行為の手段として使用されるおそれが大きいと認めるときは**、当該計画書を届け出た者に対し、妨害行為を防止するため必要な措置を講じた上で設備導入等を行うこと等を**勧告（命令）することがある**。

制度のスキーム



出典　https://www.cao.go.jp/keizai_anzen_hosho/doc/infra_gaiyou.pdf　より抜粋

特定社会基盤役務に求められる情報セキュリティ（例）

リスク管理措置の例

特定重要設備を導入する場合

①－１特定社会基盤事業者は、特定社会基盤事業者等において、特定重要設備に**悪意のあるコード等が混入していないか**を確認するための受入検査その他の検証体制が構築されており脆弱性テストが導入までに実施されることを確認している。

②－２特定社会基盤事業者は、構成設備の供給者が特定社会基盤事業者又は特定重要設備の供給者によって調達時に指定された情報セキュリティ要件（構成設備に**最新のセキュリティパッチが適用されているか否か、不正プログラム対策ソフトウェアを最新化しているか**否か等）を導入までに実装することを確認している。

⑥特定社会基盤事業者は、特定重要設備をインターネット回線と接続する場合には、特定重要設備に、**不正なアクセス等を防ぐための機能**を実装し、その利用マニュアル・ガイダンス等を自ら適切に整備・実施している。

⑪特定社会基盤事業者は、**ランサムウェアに感染した場合等**の特定重要設備に対する不正な妨害が行われたときであっても役務の提供が継続できる体制（バックアップの取得・隔離管理、復旧手順の明確化・具体化、代替設備との交換等）について、自ら整備している。

⑬特定社会基盤事業者は、特定社会基盤事業者又は特定重要設備の供給者が、特定重要設備について**アクセス制御に関する仕組み**を講じ、特定重要設備に対する不正なアクセスを監視する仕組みを導入までに実装することを確認している。

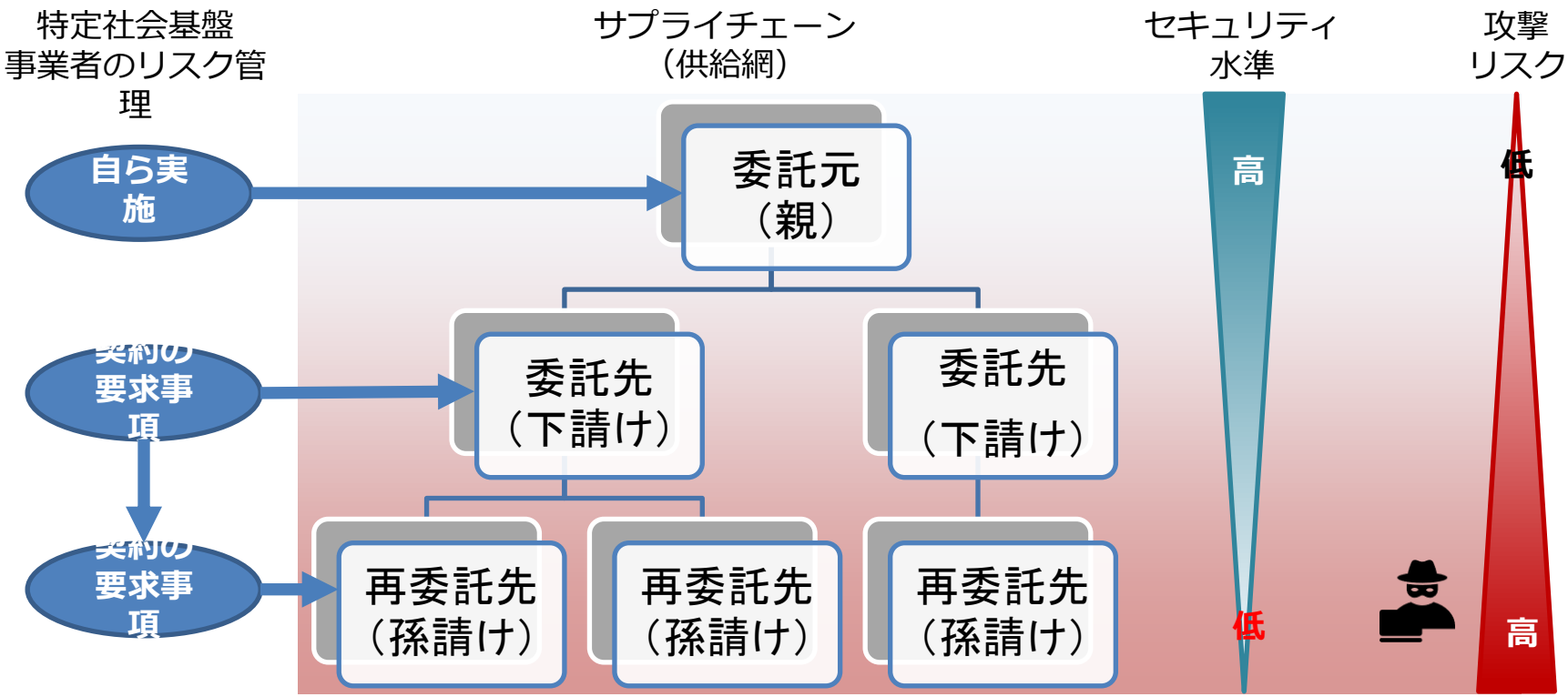
特定重要設備の重要維持管理等を委託する場合

⑤特定社会基盤事業者 は、委託の相手方及び再委託の相手方等において、重要維持管理等を実施する要員や管理責任者に対する**サイバーセキュリティに関する教育や研修**を定期的（年間１回以上）に実施し、サイバーセキュリティリテラシーの維持向上に努めていることを確認している。

⑦特定社会基盤事業者は、委託の相手方との契約において再委託の相手方等が委託の相手方と同等の**サイバーセキュリティ対策を確保することを、再委託を行う場合の条件**として設定することを要件としている。

出典　https://www.cao.go.jp/keizai_anzen_hosho/doc/infra_gaiyou.pdf　より抜粋

サプライチェーン（供給網）がサイバー攻防の主戦場に



重要インフラ事業者（大手事業者）と供給者（中小企業）に対する監査の留意点

重要インフラ事業者（大手事業者）側

- 供給者との契約では、セキュリティに対する**責任分界と役割**が明確か。
- 供給者からの製品・サービス供給停止を想定した**BCP（事業継続計画）**を策定し、訓練しているか。
- 自社のIT/OTシステムに外部から供給者がアクセスできる場合、外部接続のための装置等の**脆弱性対策**を施しているか、また、外部接続を常に**監視**し異常を検知できるか。
- 供給者経由でサイバー攻撃を受け、内部に侵入されることを前提としたセキュリティ対策**（事後対策）**を実施しているか。

供給者（中小企業）側

- 経営者は、自社が重要インフラに対するサイバー攻撃の経路であり、標的となりうることを十分自覚しているか**（無名の当社に限って、はない）**。
- 経営者は、サイバー攻撃を受けることを前提とした**リスクアセスメント**を実施しているか。
- 経営者は、上記リスクアセスメントの結果に基づき、適切な**セキュリティ投資**を実施しているか。
- 自社から重要インフラ事業者のIT/OTシステムにアクセスできる場合、アクセス者の特定及びアクセス状況の**監視**を実施しているか。

「人材の流動化に伴う営業機密の流出増加」

PWC JAPAN 有限責任監査法人　加藤俊直

情報持出は日常のニュースになってしまっている

- 内部不正による情報持出は、業種・役職に関わりなく事例を絞るのが難しいくらい多くの組織でおこなわれている。

地方自治体

- 社会福祉課の職員特定職員の給与等情報を不適切に取得
- 特定保健指導の参加者情報が外部攻撃により流出
- コロナ宿泊療養情報が再委託先従業員により流出

外食産業

- 役員が他社に移籍し不正取得した営業秘密を提供

大手電子部品

- 外国籍社員が営業秘密を持ち出し転職

政府系法人

- 主任研究員が技術情報を持ち出し、海外で特許申請
- 委託先の派遣社員が補助金採択情報を持ち出し、自身の営業に流用

金融機関

- 従業員が私的な郵便を送付する目的で顧客4人の個人情報を窃取

人材の流動化および働き方の多様化により加速

- 技術的な要因は環境変化に適応していってるものの、人的要因はその要素の急激な環境変化に後手を踏んでいる状況にある

技術的要因	• 物理環境 • システム環境
人的要因	• 組織に関わる環境 • 個人に関わる環境

個人に関わる環境変化
- 人材流動化の加速
- 副業・兼職の増加（組織内人材）
- 複数業種への関与（外部人材）

組織に関わる環境変化
- 組織自体の流動化
- 組織のグローバル化
- 共通業務のアウトソースの加速とタスク化
- リモートワークの定着化

監査での対応

人は弱いものであるという前提のもとで、「魔が差した」時に踏みとどまれる意識と環境を提示する必要がある。その意味で、例示した観点からのセキュリティ監査を実施していただきたい

- 以下のような観点を含む社内研修や秘密保持誓約書で実効性のある意識付けが行われているかの確認
  - 機密情報管理の必要性、定義、分類、管理方法
  - 罪の意識がないまま行為に至らせない具体的な方法の例示
  - 得られるメリットと多額の損害賠償や刑事罰の比較
  - 常に見られていることを意識づけるコントロールの例示
- 研修の対象者は業務委託、派遣、役員等全ての人材となっているか

「ランサムウェア、セキュリティ人材不足」について

日本セキュリティ監査協会　　永宮直史

トレンド（ランサムウェア、セキュリティ人材不足）解説

トレンドにみるランサムウェアと人材育成

	順位	解説のポイント		
ランサムウェア	第2位	他人事ではありません。日常化するランサムウェア被害	脅威の増大	前年比1.5倍以上で被害増加
			脅威の日常化	社会的被害をもたらす中小企業・機関の被災が多発
	第9位	止まらないランサムウェアの進化	脅威を生み出す裏社会	クラウド型ランサムウェアサービス；RaaS(Ransomware as a service)
			検知すり抜け技術	ノーウェア(非暗号型)ランサム
人材育成	第10位	経営課題として浮上，サイバー人材育成	人材不足による脆弱性増大	相次ぐシステム設計のミスによる情報流出事故（設計レビューや検収など、一定レベルのセキュリティ知識が必須なシステム開発プロセスに投入する人材が不足）

ランサムウェアの動向

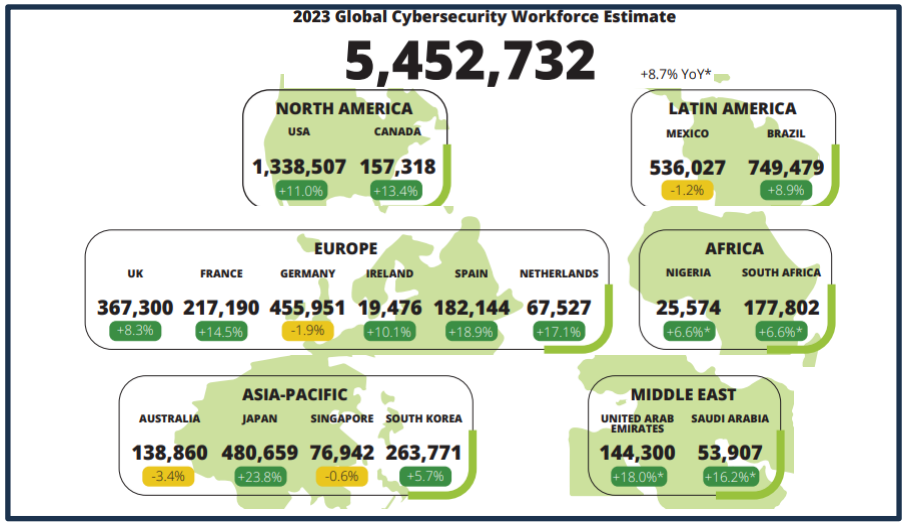
- 狙いは身代金の支払が支払われやすい中小企業
  - 世界のランサムウェア被害者の4分の３が従業員規模500人以下の中小企業
  - 従業員規模が1万人を超える企業は身代金の支払いを行わない傾向
- セキュリティ対策は心のスキを突かれないようにすること
  - 権限昇格（約54%）とコード実行（約17%）の脆弱性を狙う
  - 相手の心のスキを突くレベルの深刻度の脆弱性が狙われる
    - ◆脆弱性の深刻度が緊急（スコア9.0以上）ではなく、それに次ぐ重要（特にスコア7.2～7.5）
- 経営者には「収益の５%を失わない対策が必要」と説得をするとよい
  - 身代金はターゲット企業の収益の５%
- 今後も中小企業がターゲット。近未来には身代金要求から、情報転売などにも広がる可能性
  - 攻撃技術の向上は、対策の向上と相殺される可能性
  - 攻撃数を増やすことが攻撃者の収入増になるので、数が多く効率の良い中小企業が今後もターゲット。
  - 身代金を払わない企業が増えるのに対しては、他の収入（例えば、情報転売）に展開の可能性も

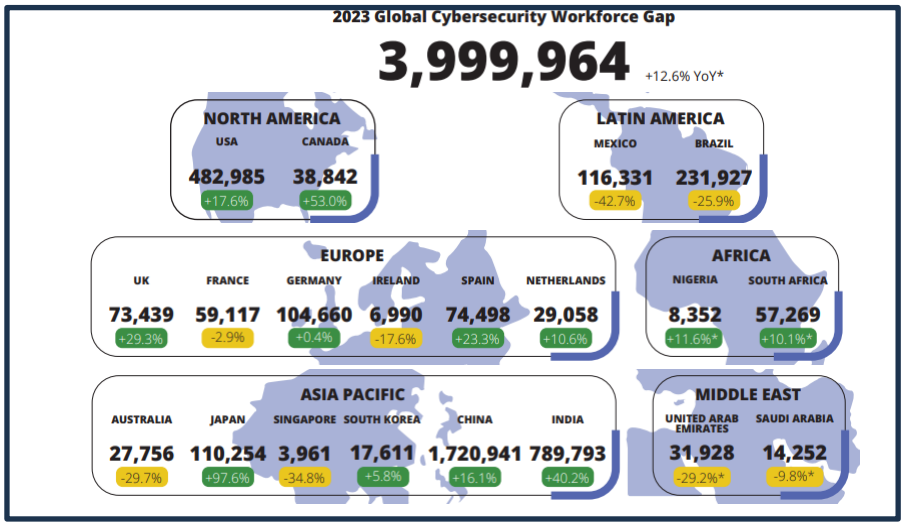
（資料）アンダーグラウンド調査から解明したランサムウェア攻撃グループの実態（トレンドマイクロ：2023年2月20日）

（注）関連資料をP42以降に添付しています。

セキュリティ人材問題

- (ISC)²の推計では、日本のサイバーセキュリティ人材の問題は世界で最も深刻
  - サイバーセキュリティ人材は2023年全世界で約545万人で前年比8.7%増
  - 日本は約48万人で前年比24%増と、世界で最も増加率が高い
  - 需給ギャップは全世界で約400万人で前年比12.6%増
  - 日本は約11万人で約98%増加

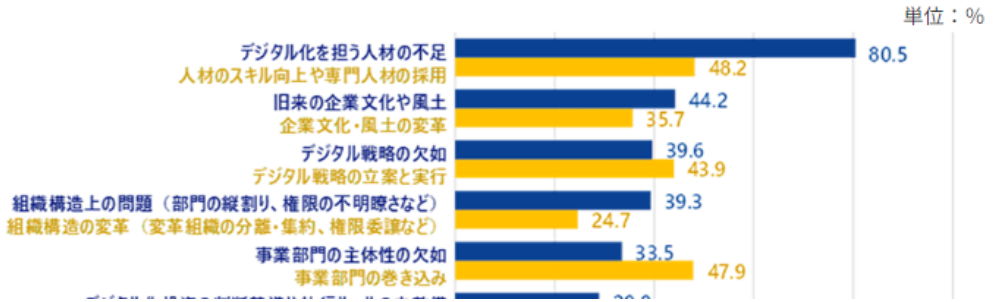




IT人材不足とその要因

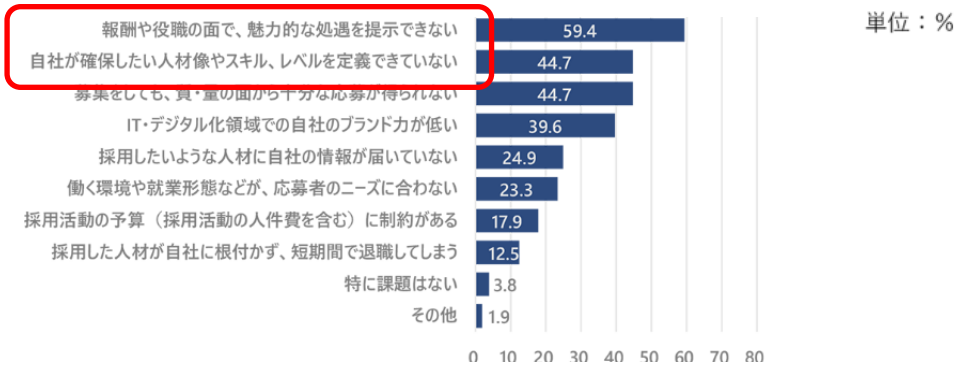
- サイバーセキュリティ人材を含むIT人材の不足は各社が実感
  - 大手企業では約80%が人材不足を課題として認識している。※1
  - 中小企業経営者の7割が自社にIT人材がいないとしている。※2
    - ◆不足しているという経営者は約38%
- 課題は処遇と人材定義
  - 魅力的処遇を提示できないが約60%
  - 人材像やスキルレベルを定義できないが約45%
- IT人材とサイバーセキュリティ人材不足の要因は同じと推察される
  - 硬直的な人事制度
  - 人材定義ができない企業のIT知識レベル

図3：デジタル化の効果を得る上での課題と取り組みの状況（複数回答）



（資料）IT活用実態調査（2022年）：NRI

図4：IT人材・デジタル化人材の採用・獲得に関する課題（複数回答）



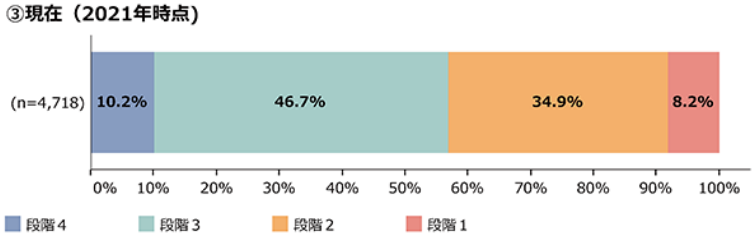
（資料）IT活用実態調査（2023年）：NRI

※1　IT活用実態調査（NRI：2022年）、売上上位3000社を対象
　2　全研本社調査　（まいなびニュース2023/3/24）

監査での対応

経営層の認識不足が課題

- 全般について：ITに対する認識不足（技術戦略における欠陥）
  - 21世紀にIT技術を戦略的に生かせなかった日本の産業界
    - ◆戦略の重要要素としての技術戦略
      （「戦略の本質」；野中郁次郎他）
    - ◆21世紀にはIT戦略が技術戦略の要
      （ウクライナ戦争の教訓）
    - ◆未だに「文系だから」が言い訳になる経営者
    - ◆特に中小企業においての認識不足が顕著



資料：（株）東京商工リサーチ「中小企業のデジタル化と情報資産の活用に関するアンケート」
（注）デジタル化の取組状況として「分からない」と回答した企業は除いている。

（注）段階1：アナログ、段階2：業務ツール化、
段階3：デジタル化、段階4：DX
（資料）中小企業白書2022

- ランサムウェアについて：サイバーセキュリティリスクに対する認識不足
  - 自社の事業がITの上に成り立っていないとの思い込み
  - 重要な生産ラインはネットワークにつながっていないとの思い込み
- 社内体制が遅れていることへの認識不足・知識不足・指導力不足
  - 硬直的な人事制度
  - セキュリティ人材像を描けない組織

問われるサイバーセキュリティガバナンス

監査課題：サイバーセキュリティ経営のガバナンス

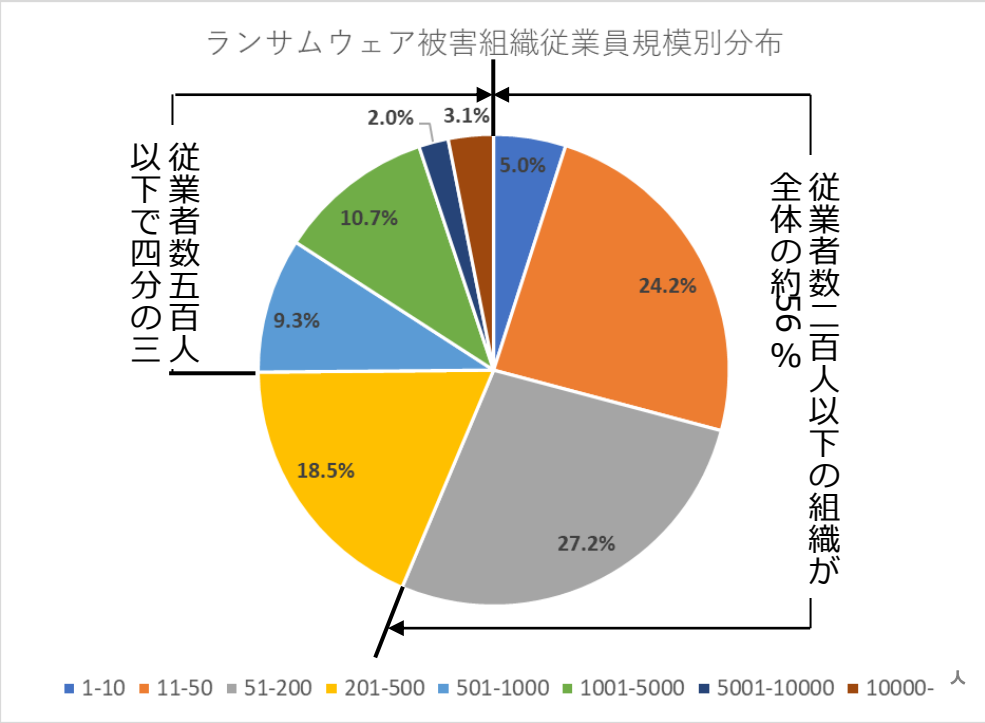
	求められるガバナンスのために	監査における確認ポイント
No.1	サイバーセキュリティリスクを的確に捉え、リスクの許容水準を示している	・企業における重大なリスクを端的な表現で示しているか
No.2	リスク水準を維持するための戦略を示している	・重大なリスクに対してどのように対応すべきか分かりやすく指示しているか
No.3	組織が戦略に従って活動していることを監視している	・アラートとなる事象をどのように定義しているか
No.4	戦略から外れる動きに対する制御をしている	・どのような仕組みが導入されているか
No.5	利害関係者にガバナンスの有効性について説明している	・誰に、どのような方法で説明しているか

監査人のスキル向上のポイント

- 企業経営について理解する
- 経営と管理の相違を理解する
- ガバナンスについて理解する

（参考）ランサムウェア動向に関する資料

ランサムウェア被害の特徴



- トレンドマイクロ調査によると
  - 被害者の全体の4分の３が従業員規模500人以下の中小組織
  - 身代金支払いは推定16%
    - ◆金融機関や法律事務所は支払い率が高い（米国の例）
    - ◆従業員規模1万人以上は支払い率が低い（米国の例）
  - 身代金要求額は年間経常収益の5%（Contiのチャットログによる）

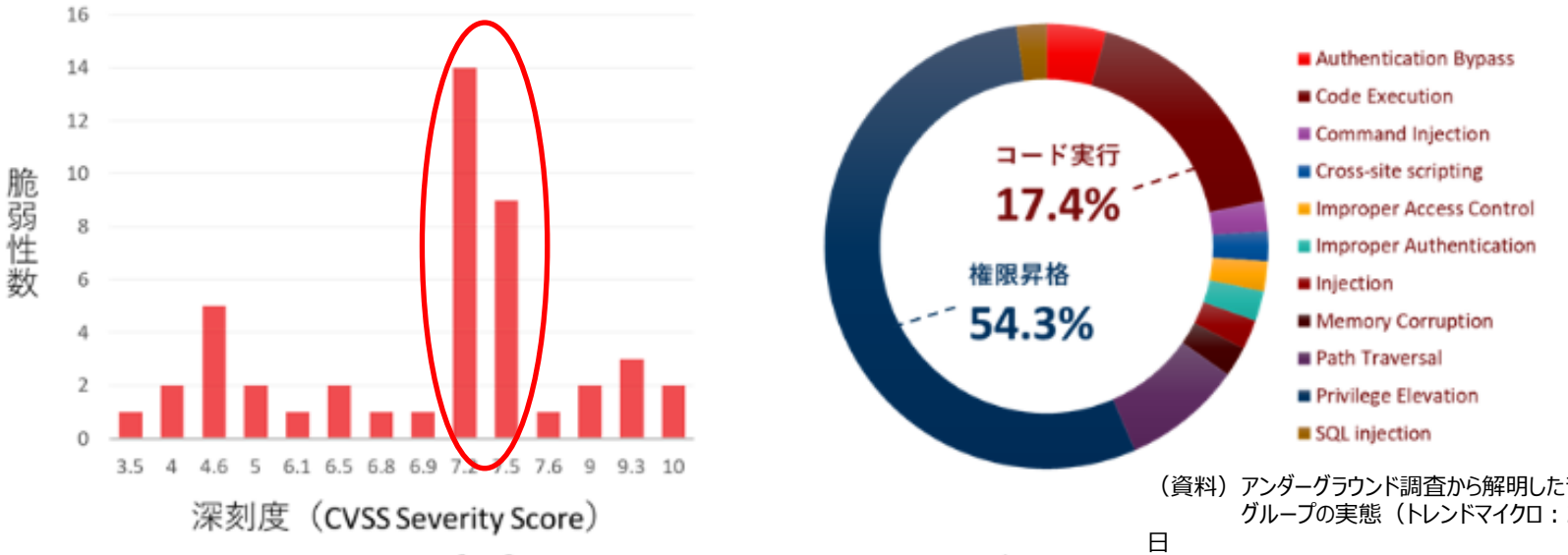
（資料）アンダーグラウンド調査から解明したランサムウェア攻撃グループの実態（トレンドマイクロ：2023年2月20日）

2019年11月から2022年6月までのContiLockBitのリークサイトのデータを収集分析

ランサムウェア攻撃の特徴

- 攻撃される脆弱性は深刻度が重要(7.0～8.9)が多く、緊急(9.0以上)は少ない。
- 脆弱性の内訳は、権限昇格（約54%）とコード実行（約17%）で7割を占めるので、対策はここがポイント。

（ランサムウェア攻撃者グループのうち活動量上位5グループのConti、Cuba、Egregor、LockBit、Sodinokibi/Revilのデータ）



（資料）アンダーグラウンド調査から解明したランサムウェア攻撃グループの実態（トレンドマイクロ：2023年2月20日

【出所】2015年～ 2022年に公表されたCVEのうち当該5グループが悪用したものを公開情報からトレンドマイクロが算出

図6　調査対象となったCVEのCVSS深刻度スコアでの分布（左）と調査対象となったCVEのタイプ別の分類（右）

今後のランサムウェア被害の拡大シナリオ


A.身代金（収益）

＝


B.攻撃対象

×


C.攻撃技術

×

D.防御態勢（法規制・認知度向上）

- 前提
  - 収益（A）拡大が目的
  - 攻撃技術（C）の向上は防御態勢（D）の強化で相殺
- シナリオ１　攻撃対象を増やす（数の多い中小組織によりシフト）
- シナリオ１の限界が来る→シナリオ２
  （身代金以外の収益へシフト　例：盗んだ情報の転売）

「クラウドのセキュリティ、脆弱性管理」

日本マイクロソフト株式会社　久保田朋秀

■ 監査のポイント

内容	クラウドサービスの利用の際に各種の設定を誤ることにより情報が外部流出する事故は組織規模の大小を問わず世界中でいまだ数多くのインシデントが報告されている。 クラウドサービスの利用がより拡大する中で、基本的な設定事項が適切に行われているかを定期的に確認することは極めて基本的だが重要な要素である。今日では各プロバイダーからの設定ベストプラクティスはもとより、総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン」やNISC「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル　別冊．クラウド設計・開発編」など公的なドキュメントも公開されており、適切な対応を怠ることは善管注意義務違反規範に問われる可能性も否定できない。
監査のポイント	利用者組織にとっても、従来とは異なるマネジメントが必要となることから、妥当性のあるセキュリティ対策のベストプラクティスから管理策を実装しているかどうかがポイントとなる。ベストプラクティスを提示した公的なドキュメントも公開文書として参照できるようになっているため、これらの文書群の内容への準拠状況の確認と、クラウドサービス提供側で提供されているCISベンチマークに基づいた管理策が正しく運用されているかを、確認する。監査の実施にあたっては、サービスダッシュボードでリアルタイムに閲覧できるシステムなどを有効に活用し監査手続にも応用することで、公平性や信頼性を高めることができる。監査人は被監査主体が利用するサービスの機能やベストプラクティスを確認し監査を進めたい。 なお、監査のポイントとしては以下の通りである。 • 妥当性のあるベンチマークに基づいた管理策が策定され実装されているか。 • 運用状況についてサービス機能などを用いて監視し、修正しているか。 • 常に最新の情報に基づいた対応が実施されているかを定期的にレビューし評価しているか。

■ 現実解として取り得る監査人としての対応と助言

① 自組織のルール策定に際し参照するガイドラインが定まっているか

② 自組織でクラウドサービス利用のためのガイドラインやルールが定められているか

③ 制定されたガイドラインやルールに準拠した実装がなされているか確認できる手段が実装されているか

✓ 政府等公的機関のガイドラインやISO27017などの認証ルールにしたがった標準的な管理策の制定と実装

✓ クラウドプロバイダーなどが提供しているCSPMツールなどの導入

- その際に標準的な管理策を導入していればテンプレートなどになって提供されている可能性が高い
- さらに余裕があればISO27017のクラウド利用者としての認証を取得するなどの対応も考慮に入れる

□ 多様な提供形態と利用形態となっているクラウドでは、常に標準的なリファレンスに対しての準拠状況確認を実施することで、リスクを低減していく必要がある

8 (17) 脆弱性管理体制の再検討の加速

内容	セキュリティパッチの適切な適用など基本的な対策の不備による事故が増加しており、脆弱性対策の不備が懸念されている。 深刻な影響が懸念される脆弱性が公表されても、自組織のシステムのどこに該当するソフトが内在されているかが把握できていない、あるいは脆弱性スキャンの結果多くの脆弱性が見つかるがどの脆弱性に重点的に対応すべきかの評価・判断が難しく的確に対応できない、さらには、深刻な脆弱性に対するパッチを当てる作業が業務プロセスに影響を与える恐れがあるのにリスク判断と意思決定の権限と責任の体制が機能しないなど、多くの課題を抱えており迅速な脆弱性対策が取れない組織が増加している。 サイバー攻撃の激化を見込まなければならない中で、脆弱性の報告は増加し続けている。DXが進む中、的確な脆弱性管理の確立に向けて、体制やプロセスの見直しが急務である。
監査のポイント	技術的脆弱性の管理はセキュリティ対策の基本に位置づけられるが、実効性のある管理の仕組みを構築するのが難しいのもまた事実である。この難しさを克服し有効な体制を築くためには、経営者がこの重要性を的確に理解し、自社に必要な管理体制に応分の資源を配分する意思を持たなければならない。そのためには、監査により管理体制の再検討の切り口を明らかにすることが望まれる。 脆弱性管理の監査においては、①現状の脆弱性管理にかかわる規程類の記述と②実際の脆弱性対応の記録とをもとに、関係者のヒアリング等をとおして自社の脆弱性対策としてうまくいっている点と課題点を明らかにするのが望ましいであろう。 その際のポイントに以下の項目が挙げられる。 ・ 定常的な脆弱性管理プロセスが規定され、その権限と責任の所在が明示されているか。各責任者には、その権限と責任の認識があるか ・ 権限と責任の分担がシステム部門やセキュリティ部門だけに偏っていないか、事業部門がリスク判断やその結果責任に的確に関与できているか ・ 緊急性の高い脆弱性への対応に柔軟に対応できる体制になっているか ・ 脆弱性への対応は規定されたプロセスに沿っているか、その対応の記録が整然と保存されているか ・ 認識され高リスクと評価されたが、パッチ適用ができず代替策で乗り切る決定をした未対応の脆弱性が、その後適切にフォローされているか ・ 脆弱性管理プロセスの見直しをするトリガーが決まっているか ・ 脆弱性検査ツールや脆弱性の影響評価手法、脆弱性情報の入手ルートなどが適切に見直されているか

■ 現実解として取り得る監査人としての対応と助言

① システム内に存在し接続・稼働している機器類・ソフトウェアが確認できるか？

② 最新の脆弱性情報を常に把握できているか？（インテリジェンス）

③ ①の機器等の情報と②の脆弱性情報をあわせて、既知の脆弱性に対応している機器類やソフトウェア、対応できていない機器類やソフトウェアを把握できているか？

✓ 対応できる機器・端末はすぐに対応を行う（促す）

✓ もし、システム上の問題から対策パッチ等が適用できない機器等が存在する場合には・・・

- ➢ 代替え案となる対策（ワークアラウンド）を検討する
- ➢ 監視を強化する（ログの確認スパンを短くするなどを含む）

- ◘ まずは限りなくリアルタイムで資産の状況を把握できる体制ができているかどうかを監査する
- ◘ そのうえで脆弱性への対策を促し対策状況を確認する手順を構築する
- ◘ さらにSBOMなどサプライチェーンまでの管理・監視が可能な組織はより深い対策の実行を検討していく

ROUND 2

2024年度監査の重点の考え方
＋
監査人のスキルアップについて

モデレータ

大木榮二郎
工学院大学名誉教授

パネラー

間形文彦
NTTコミュニケーションズ(株)
情報セキュリティ部　担当部長

永宮直史
日本セキュリティ監査協会
エグゼクティブフェロー

久保田朋秀
日本マイクロソフト株式会社
パブリックセクター事業本部　技術戦略本部
クラウドセキュリティ推進室長

加藤俊直
PwC Japan有限責任監査法人
パートナー

Q&A

Chatから質問をおよせください。