第6回Digital Days2026特別講演

サイバーセキュリティは“経営者の意志”がつくる

～インシデント事例から考える、組織横断ガバナンスと事業継続の意思決定～

発表者

特定非営利活動法人CIO Lounge
田島邦彦

目次

自己紹介

□職歴

1988年　4月　富士通株式会社入社　営業職。営業部長職～支店長職を経て退社。

主な業種は、家電メーカー、金融系（銀行、証券、信金・信組、クレジット・リース、JAなど）及び自治体・文教を担当。

現在、コンサルティング事業活動中（企業コンサルティング、マーケィングサポート支援、消費生活アドバイバー活動、観光活動など）

2023年10月　特定非営利活動法人CIO Lounge正会員活動中

□経験・実績

営業一筋に、システム全般における顧客の業務課題解決・仮説・企画提案活動を中心に多くのプロジェクトを経験しました

特に、トップから現場まで顧客視点に立ち人との繋がりコミュニケーションとモチベーションを大切に実践し仕事に向き合いながらシステムプロジェクトを遂行、実現することが重要と考えています。

また、長年の金融業界を担当した営業経験を自治体・組織団体や企業連携による地方創生、スマートシティなど産官学民連携による全方位型の共創・協業活動にICTを活かした地域ビジネスのマネージメントは貴重な経験になっております。

特定非営利活動法人ＣＩＯ　Ｌｏｕｎｇｅとは

◇活動理念

「企業経営者と情報システム部門」「企業とベンダー」の架け橋となり、各企業様の効率化・持続的成長に貢献する

⇒「日本企業のIT／デジタル化強化を通じ、世界に打ち勝つ社会を確立する」という想いで活動している団体です

■主な活動内容

・企業様支援活動、セミナー登壇活動、分科会を中心に活動しております。
・9つの分科会活動⇒中小企業支援、情報セキュリティ、企業DX、現場主体DX推進、DX人財育成、SCM、AI分科会

経営とITの架け橋

CIO/IT責任者として経営層と現場の両方を経験したメンバーで構成。「翻訳者」として組織に実装してきた知見を共有します。

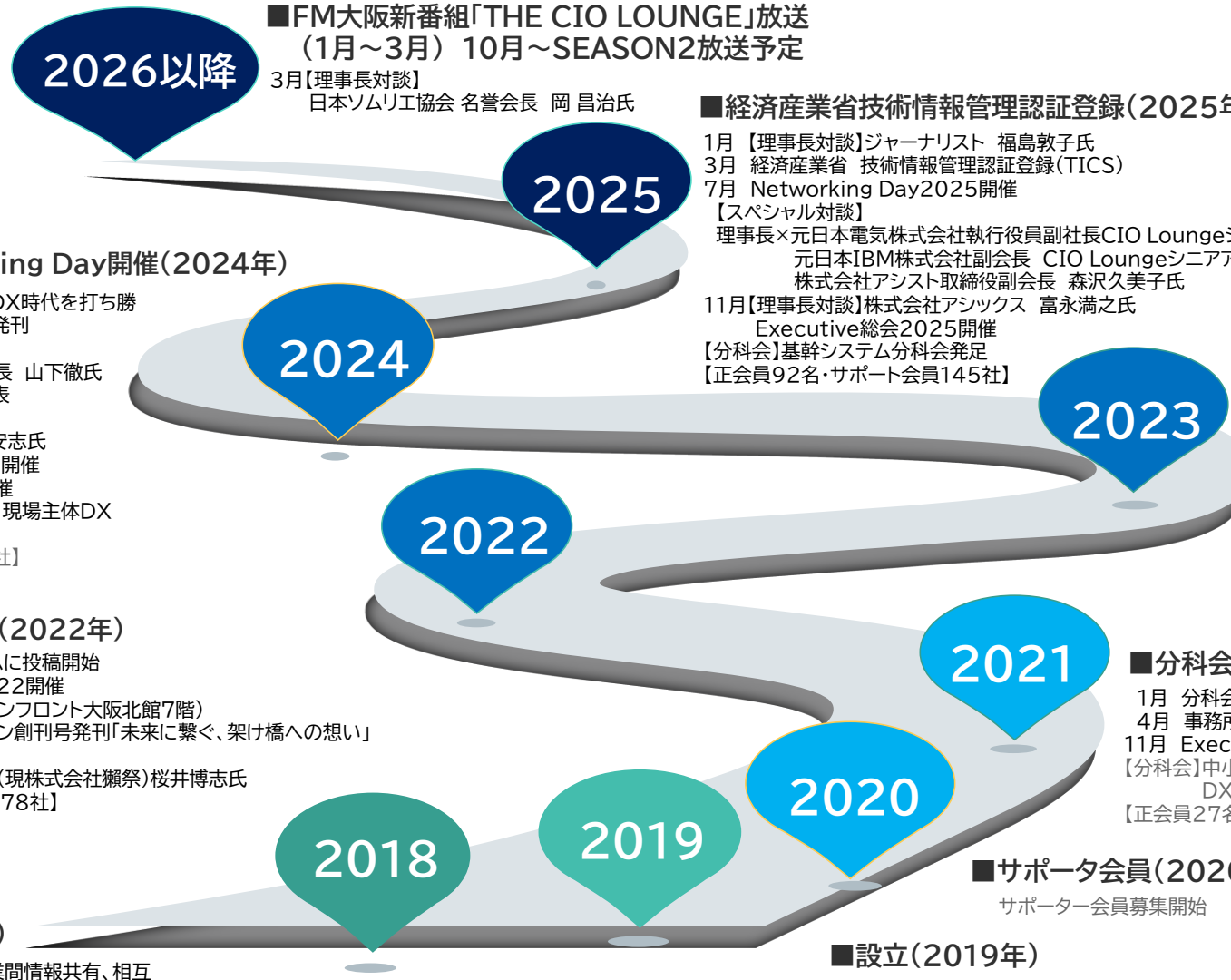
組織横断の視点

業種・規模・業態を超えたCIO同士の対話により、特定企業の事例に偏らない、構造的・普遍的な洞察を提供します。

実務経験に基づく知見

製品紹介や制度解説ではなく、「現場でどう判断し、どう動いてきたか」という一次経験をベースにした語りが私たちの強みです。

これまでの歩み～未来へ繋ぐ、架け橋へ



2026以降

■FM大阪新番組「THE CIO LOUNGE」放送
（1月～3月）10月～SEASON2放送予定

3月【理事長対談】
日本ソムリエ協会 名誉会長　岡 昌治氏

2025

■経済産業省技術情報管理認証登録（2025年）

1月 【理事長対談】ジャーナリスト　福島敦子氏
3月 経済産業省　技術情報管理認証登録（TICS）
7月 Networking Day2025開催
【スペシャル対談】
理事長×元日本電気株式会社執行役員副社長CIO Loungeシニアアドバイザー木下学氏
元日本IBM株式会社副会長　CIO Loungeシニアアドバイザー下野雅継氏
株式会社アシスト取締役副会長　森沢久美子氏
11月【理事長対談】株式会社アシックス　富永満之氏
Executive総会2025開催
【分科会】基幹システム分科会発足
【正会員92名・サポート会員145社】

2024

■書籍発刊／Networking Day開催（2024年）

1月 「CIO／IT責任者が語る DX時代を打ち勝つための30の提言」書籍発刊
【理事長対談】
3月 株式会社NTTデータ元社長　山下徹氏
4月 株式会社セレッソ大阪代表取締役社長　森島寛晃氏
10月野球評論家・解説者　田尾安志氏
7月Networking Day2024開催
10月Executive総会2024開催
【分科会】企業DX・DX人財育成・現場主体DX推進・AI分科会発足
【正会員64名・サポート会員98社】

2023

■理事長対談（2023年）

4月 【理事長対談】
株式会社セブン銀行会長　舟竹泰昭氏
7月 旭鉄工株式会社社長　木村哲也氏
10月 近畿大学　経営学部キャリア・マネジメント学科教授
西尾久美子氏
Executive総会2023開催
【正会員54名・サポート会員91社】

2022

■理事長対談始まる（2022年）

6月 「IT Leaders」コラムに投稿開始
10月 Executive総会2022開催
現事務所に移転（グランフロント大阪北館7階）
CIO Loungeマガジン創刊号発刊「未来に繋ぐ、架け橋への想い」
【理事長対談】
旭酒造株式会社会長（現株式会社獺祭）桜井博志氏
【正会員37名・サポート会員78社】

2021

■分科会活動開始＆Exective総会初開催（2021年）

1月 分科会活動サポート会員募集開始
4月 事務所移転（グランフロント大阪北館8階）
11月 Executive総会2021開催
【分科会】中小企業経営基盤支援・情報セキュリティ・非基幹DX・SCM分科会発足
【正会員27名・サポート会員69社】

2020

■サポータ会員（2020年）

サポーター会員募集開始

2019

■設立（2019年）

1月 特定非営利活動法人「CIO Lounge」認可
2月 NPO法人として活動開始

2018

■設立活動（～2018年）

1月 関西製造業IT責任者での企業間情報共有、相互研鑽活動を開始
4月 関西製造業IT責任者に活動趣旨の説明活動
6月 非営利団体「CIO Lounge」として活動開始
8月 活動拠点としてヒルトンプラザウエスト18階事務所開設

はじめに

「貴社では、サイバーリスクを誰が経営課題として扱っていますか？」

IT部門だけの課題ではない

サイバーリスクは技術的脅威にとどまらず、経営全体が向き合うべき問題です。

事業継続・取引先・顧客に関わる

攻撃が起きれば、売上・納期・契約・信用すべてに影響が及びます。

本日はこの問いから考える

事例と構造を通じて、自社に当てはめるヒントを持ち帰っていただきます。

1. なぜ今、経営者の意志が必要なのか

「経営者の意志」とは、単なる「やる気」ではなく「何を捨て、何を守るかという優先順位の確定」であり、「防ぐ」だけでなく、「止まったときに何を守るか」の時代へ！

ランサムウェア

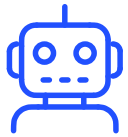
業務システムを暗号化し、会社全体の業務を完全停止させます。

サプライチェーン攻撃

委託先・仕入先から侵入し、取引先全体に被害が波及します。

クラウドID乗っ取り

正規IDが悪用されると、全社データへのアクセスが可能になります。



AI活用による攻撃巧妙化

生成AIにより、フィッシングや詐欺メールの品質が劇的に向上しています。

サイバー攻撃の影響は4層に広がる

■攻撃はITシステムへの被害として始まりますが、そこで止まることはありません。
業務・経営・社会へと波及し、最終的には企業の存続そのものを脅かします。

⚠ だからこそ、IT対策に止まらず経営判断が必要になります。

2. 事例「事業停止とサプライチェーンリスク」

事例1：小島プレス工業・トヨタ国内全工場停止

■何が起きたか

2022年3月、トヨタの仕入先である小島プレス工業のシステムに障害が発生。部品供給が停止し、トヨタ国内14工場28ラインの稼働が1日停止しました。約1万3,000台分の生産に影響が出ました。

※トヨタ自動車株式会社公式企業サイト参照

◇経営上の学び◇

- **サプライチェーン全体の可視化**：委託先・仕入先のセキュリティ状況を把握する仕組みが必要
- **連絡体制の整備**：インシデント発生時の取引先との連絡フローを平時に設計する
- **代替手段の検討**：単一委託先への依存リスクをBCPに組み込む
- **委託先管理の経営課題化**：委託先のリスクは自社のリスクである

☐ **自社の取引先・委託先に同様のリスクはありますか？**

事例2：大阪急性期・総合医療センター

■何が起きたか

2022年10月、電子カルテを含む基幹システムがランサムウェアにより暗号化。救急受け入れ停止、外来・手術の大幅制限が約2ヶ月続きました。

※地方独立行政法人大阪府立病院機構大阪急性期・総合医療センター公式サイト参照

◇経営上の学び◇

- **情報漏えいだけが被害ではない**　：業務停止そのものが重大な経営・社会リスク
- **重要業務と基幹システムの関係把握**：どのシステムが止まると何が止まるかを整理する
- **周辺システムの管理**　：直接業務に関わらないサーバーも攻撃の入口になる
- **復旧優先順位の事前決定**　：有事に判断する時間はない

自社で同じシステムが止まったとき、どの業務が止まりますか？

事例3：名古屋港統一ターミナルシステム停止

■何が起きたか

2023年7月、名古屋港の統一ターミナルシステム（NUTS）がランサムウェアにより停止。約3日間、コンテナの搬入・搬出が停止し、日本最大の貿易港の物流全体に影響が及びました。

※名古屋市公式サイト参照

◇経営上の学び◇

- **バックアップは「取る」だけでは不十分**：復元手順・感染前データ・整合性確認が必要
- **復旧後のデータ品質**　：業務データが「使える状態」かを確認するプロセスが必要
- **重要インフラへの波及**：自社停止が社会インフラに影響する可能性を認識する
- **復旧訓練の実施**　　：実際に戻せるかを定期的に検証する

自社のバックアップは、今日本当に復元できますか？

参考）最近の情報セキュリティ事件（最近の傾向）

①ランサムウェア攻撃の深刻化・・（基幹システムや仮想基盤が狙われる）

■アサヒビール（アサヒグループホールディングス）：ランサムウェア攻撃（2025年9月）※アサヒグループホールディングス公式企業サイト参照
⇒国内外の生産・出荷システムが大きな被害を受け、2026年2月時点で約11万5千件の個人情報流失。

■アスクル：ランサムウェア攻撃（2025年10月）※アスクル株式会社公式企業サイト参照
⇒受注・出荷など基幹システムが広範に障害。受注・出荷システム停止や約74万件の顧客情報流出、数百億円規模の売上機会喪失と約52億円の特別損失計上など深刻な影響を受けました。

②クラウドサービスの設定不備を突く攻撃の増加

■日本航空（JAL）：手荷物配送サービスで不正アクセス（2026年2月）※日本航空公式企業サイト参照
⇒予約システムが不正アクセスを受け、約2.8万件の個人情報が漏えいした可能性。

③サプライチェーン攻撃の拡大・・（委託先・関連企業経由）

■ローソン銀行：取引情報を含むSSD紛失（2026年3月）※株式会社ローソン公式企業サイト参照
⇒委託先の再委託先で**SSD2台の所在不明**が発生し、最大5,373件の情報が保存されていた可能性。

④内部不正・人的ミスなども多い

■地銀（阿波銀行）：顧客情報 約2.7万件流出（2026年4月）※阿波銀行公式企業サイト参照
⇒OAシステムのテスト環境が不正アクセスを受け、顧客情報が漏えい。

3つの事例に共通すること

■業種・規模は異なっても、「止まる」「波及する」「判断する時間がない」という構造は同じです。
自社が「被害者」にもなりますが、同時に、「加害者」として取引先を止めてしまう社会的責任・賠償リスクをも負っているのです。

事例	起きたこと	事業影響	経営上の学び
小島プレス・トヨタ	仕入先システム障害	国内全工場停止	サプライチェーン可視化と委託先管理
大阪急性期医療センター	電子カルテ暗号化	診療制限・救急停止	重要業務の優先順位と周辺管理
名古屋港NUTS	物流システム停止	コンテナ搬出入停止	使えるバックアップと復旧訓練

⚠ 問い：自社で同じことが起きたとき、誰が何を決めますか？その答えは、今この場にありますか？

3. サイバー攻撃入口に対する管理ポイント

■サイバーセキュリティ：経営リスクとしての入口

➡ **入口管理は、ITではなく経営管理の一部です**

メール・添付ファイル

フィッシング・マルウェア添付。最も多い入口。

VPN・リモートデスクトップ

脆弱なVPN装置や認証の甘いRDPが標的になります。

クラウド管理画面

管理者IDの奪取により全社データにアクセスされます。

外部公開サーバー・保守接続

パッチ未適用の公開サーバーや保守用接続口が狙われます。

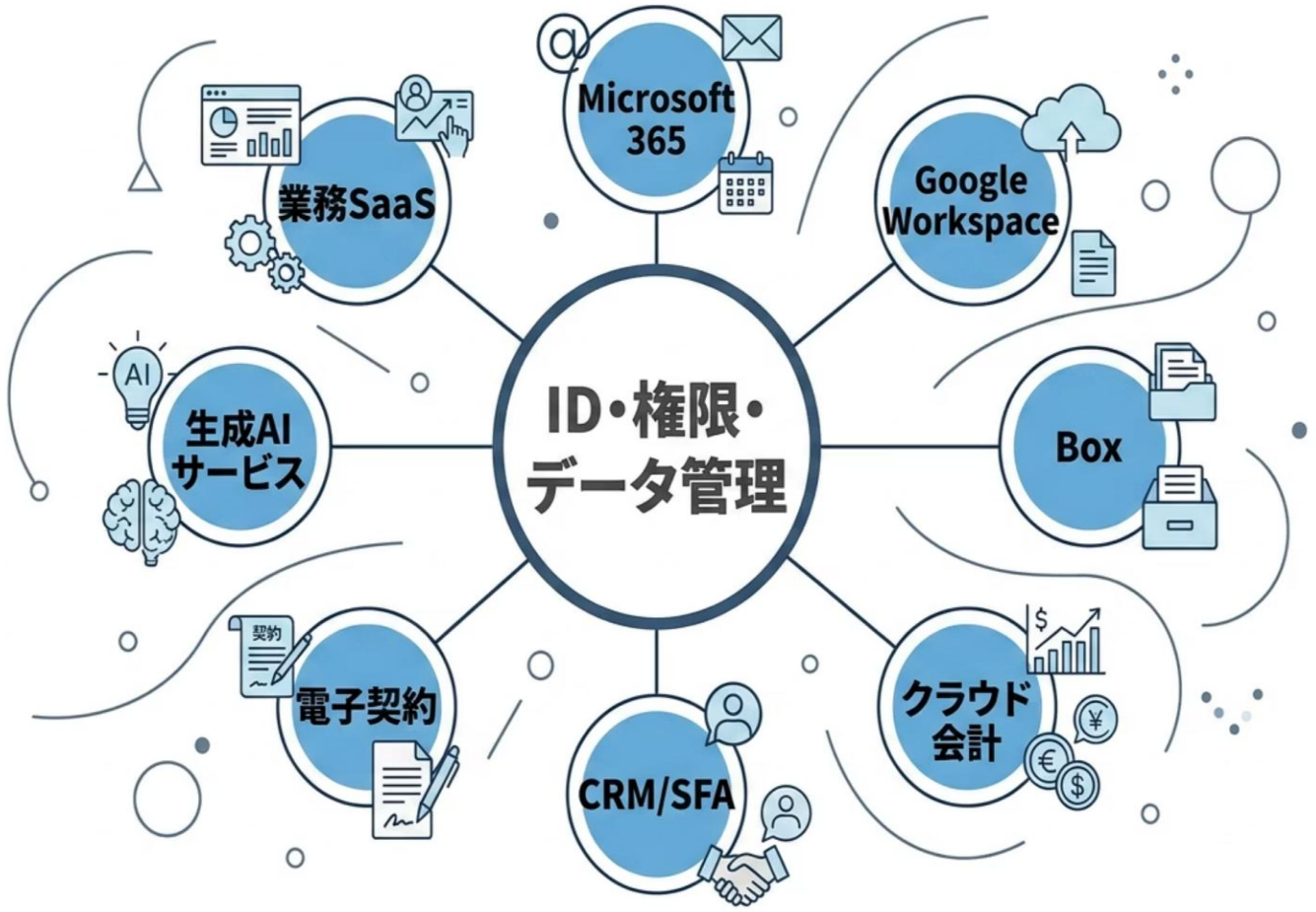
委託先接続・退職者アカウント

削除されていないID・共有ID・弱いパスワードが侵入を許します。

クラウド時代に重要な管理対象

■正規IDの悪用が最大のリスクになっている。
「誰が、どのサービスに、どのIDでアクセスできるか」の管理が経営課題です。

■「ID管理＝会社の鍵の管理」である。
「誰が鍵を持っているか把握していない家（会社）は守れない」



⚠ クラウドサービスの管理者IDを誰が持ち、誰が管理しているか＝会社の鍵の管理を今すぐ確認してください。

4. 全社で動けない4つの壁とは？

■多くの企業でサイバー対策が進まない背景には、技術の問題だけでなく、
組織・優先順位・言語・グループ構造の壁があります。

組織の壁

IT部門だけで完結し、事業部門・法務・広報・経営とつながらない。

優先順位の壁

平時は効果が見えにくく、セキュリティ投資が後回しになりがち。

言語の壁

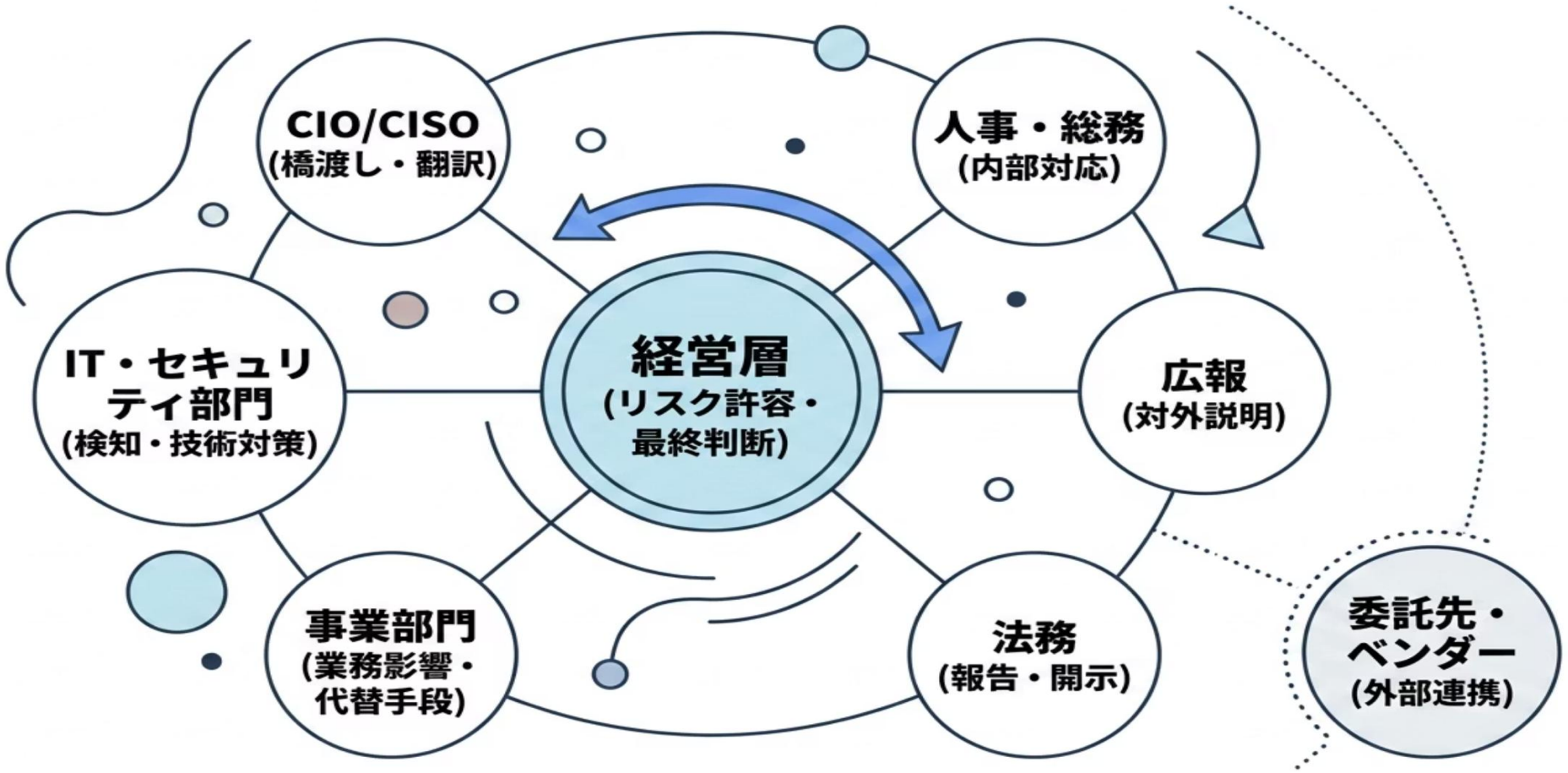
ITの専門用語と経営の言葉がつながらず、リスクが正確に伝わらない。

グループの壁

子会社・海外拠点・委託先まで統制が届かず、弱点が生まれる。

5. 会社全体を動かすための“ガバナンス設計”をつくる

■ガバナンスとは、誰がリスクを把握し、誰が報告し、誰が判断し、誰が実行し、
誰が確認するかを明確にする。インシデント発生時に「誰も決めていなかった」という状況を防ぐ仕組みです。



役割分担の整理

■有事に機能する体制は、平時の役割定義から生まれます。

～以下の役割分担を自社に当てはめて確認してください～

役割	主な責任
経営層	・リスク許容度の決定、投資判断、重要業務の優先順位、最終意思決定
CIO／CISO／IT責任者	・経営と現場の橋渡し、リスクの翻訳、全社推進、体制構築
事業部門	・重要業務の特定、顧客影響の把握、代替手段・業務継続計画の整理
IT・セキュリティ部門	・脅威検知・監視、技術的対策の実施、インシデント時の復旧支援
法務・広報	・規制対応・開示判断、顧客説明文・公表文の確認、報道対応

この表を自社に当てはめたとき、空欄になる役割はありますか？

IT部門責任者に求められる役割

■技術を「経営判断の言葉」に翻訳する

口伝わらない説明

×

「この脆弱性のCVSSスコアが高く、早急なパッチ適用が必要です。」

口経営に届く説明

○

「このまま放置すると、受注システムが停止し、主要顧客への今月の納品に支障が出る可能性があります」

◇IT責任者の3つの役割◇

① 経営と現場をつなぐ

両方の言語を話せる唯一のポジション

② リスクを事業影響に置き換える

「何が止まるか」で説明する

③ 会社を動かす推進役になる

技術担当者ではなく、事業継続の担い手として行動する

6. 経営層に求められる3つの意思決定とは何か

■経営層に求められるのは、技術の細部を理解することではありません。
判断の基準を事前に決めることです。

1
リスクをどこまで受け入れるか
どの業務が止まることは許容できないか。どのレベルの情報漏えいは事業存続を脅かすか。
リスク許容度を経営として定義する。

2
どの対策に優先投資するか
限られた予算とリソースの中で、何を先に守るか。事業影響の大きさと発生可能性で優先順位をつける。

3
有事に誰が判断するか
インシデント発生時の判断権限者を平時に決める。報告ライン・意思決定フロー・外部連絡先をあらかじめ設計する。

7.「平時」と「有事」を分けて設計する重要性

■経営層にとってセキュリティ投資は「何も起きないこと」への投資であり、コストと捉えられがちですが、セキュリティを「保険」ではなく、「事業継続のライセンス（参加資格）」と考えることです。

平時にやること

・リスクの把握と優先順位付け
・重要業務・重要データの整理
・対応手順書（プレイブック）整備
・連絡体制・報告ラインの設計
・机上演習・訓練の実施
・委託先・ベンダーとの合意形成

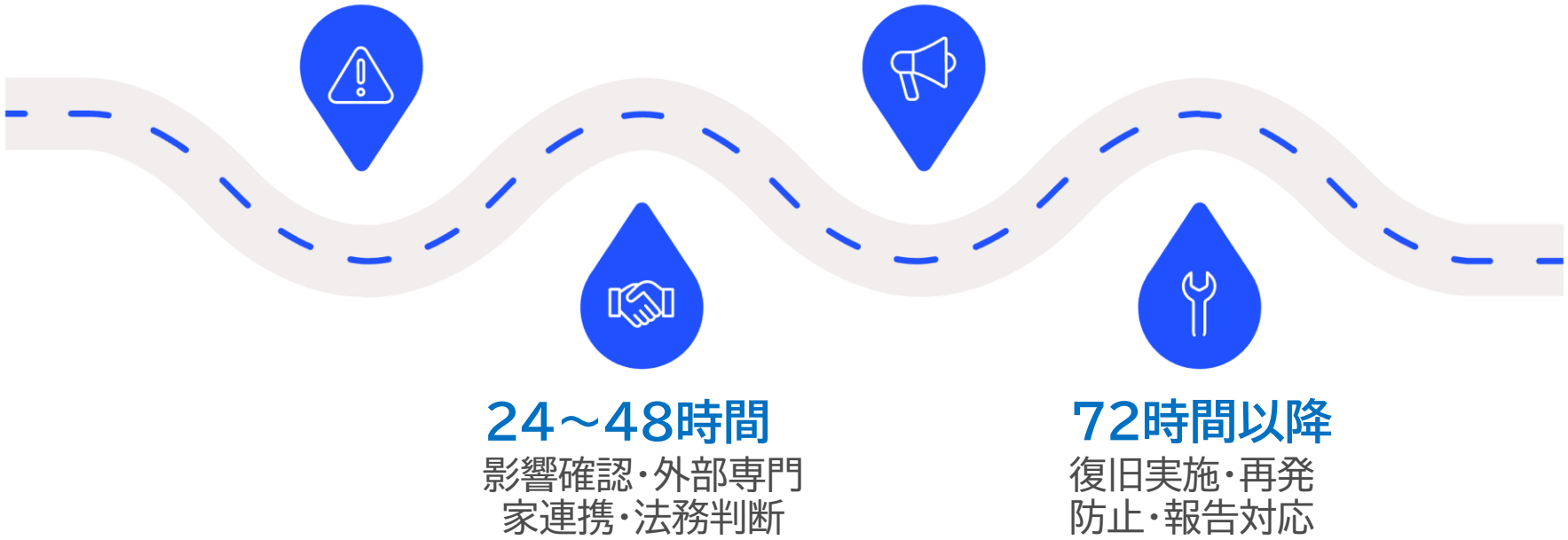
有事にやること

・被害拡大の防止（遮断・隔離）
・初動対応と経営層への第一報
・重要業務への影響確認
・外部専門家・ベンダーとの連携
・顧客・取引先への対応判断
・復旧優先順位の決定と実施

平時に備え、有事には迷わず動く。この設計こそが経営者の意志です。

初動72時間の重要性

■インシデント発生後の72時間は、被害の拡大防止と事業継続の分岐点です。
誰が何をするかを事前に決めておくことが、組織の対応力を決定します。



⚠初動で判断を誤ると、被害が数倍に拡大します。「誰が決めるか」を今日確認してください。

8. 初動対応・報告・開示は経営判断である

■復旧だけでは終わらない。有事には説明責任が問われます。

インシデント発生後、技術的な復旧と並行して、多数のステークホルダーへの対応が必要になります。誰が、どの順番で、何を伝えるかを平時に決めておくことが不可欠です。

1

社内

経営層・取締役会、従業員への説明、人事・総務対応

2

取引先・顧客

影響範囲の説明、謝罪・対応策の提示、継続取引の確認

3

行政・法令対応

個人情報保護委員会への報告、警察届出、保険会社への連絡

4

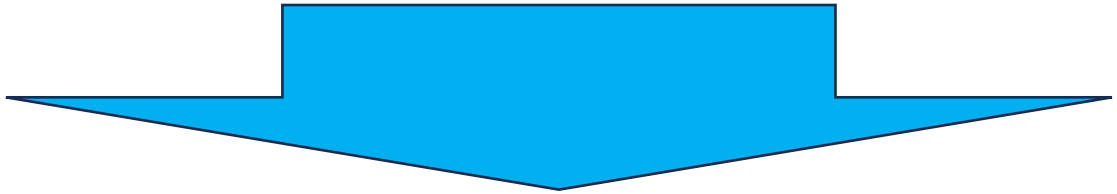
社会・メディア

プレスリリース、報道対応、株主・投資家への説明

顧問弁護士・外部PR・ベンダーへの連絡先リストは、今すぐ手元に用意できますか？

9. 生成AI時代のサイバーリスクについて考えるべきこと

■生成AIの普及は利便性をもたらす一方、新たなセキュリティリスクを生んでいます。
禁止するのではなく、安全に使うルールを整備することが経営の責任です。



攻撃者がAIを使う

自然な日本語のフィッシングメール、巧妙ななりすまし、ディープフェイク音声による詐欺。人間の判断では見抜けないレベルに達しつつあります。

社員がAIを使う

社内資料・個人情報・契約情報・議事録を外部AIサービスに入力するリスク。悪意なく機密情報が外部に渡る可能性があります。

会社としてルールを決める

「使ってよいAI」「入力してよい情報の範囲」「確認方法」を会社として明確化する。ルールなき利用は経営リスクです。

10. 明日から始めるアクション：自社点検3ステップ

完璧な体制を一度につくる必要はありません。
まず経営に上げるべき3つの行動を決めることから始めてください。

Step1:現状把握

止まると最も困る業務は何か。
重要データはどこにあるか。
バックアップは本当に復元できるか確認する。

Step2:ガバナンス点検

誰が第一報を受けるか。誰が経営に報告するか。誰が顧客・取引先に説明するかを決め、文書化する。

Step3:優先行動の設定

すべてを一度にやろうとしない。
経営に上げる3つの優先行動を決め、期限と担当者を設定する。

経営に投げかけるべき3つの問い

経営層・IT部門・事業部門で一緒に確認することから、自社のサイバーセキュリティ経営が始まります。

事業継続
うちの会社が明日止まるとしたら、何が一番困るか。今ランサムウェアに感染したら、どの業務から復旧するか。

技術・データ管理
バックアップから本当に戻せるか。クラウドの管理者IDは誰が持っているか。委託先経由で侵入される可能性はないか。

体制・ルール
インシデント発生時、誰が顧客や取引先に説明するか。生成AIに入力してはいけない情報のルールは決まっているか。

この3つの問いに「はい」と答えられる状態をつくることが、今日からの目標です。

最後に

サイバーセキュリティを情報システム部門のタスクリストから“経営の意思決定議題へ”

① **サイバー攻撃は事業停止リスクである**

IT被害にとどまらず、業務・経営・社会へと4層に波及します。

② **経営層がリスク許容・投資優先順位・有事判断を決める**

技術の細部ではなく、判断基準を持つことが経営者の役割です。

③ **IT責任者は技術を経営の言葉に翻訳する**

「脆弱性」ではなく「業務が止まる」という言葉で経営を動かします。

④ **平時に決めていないことは、有事に決められない**

体制・手順・連絡先・役割分担を今日から整備してください。

「うちの会社が明日止まるとしたら、何が一番困るのか」

この問いを、経営層・IT部門・事業部門・法務・広報・現場・委託先と一緒に話し合うことから、自社に合った現実的なサイバーセキュリティ経営が始まります。

本日はご清聴ありがとうございました。

特定非営利活動法人CIO Lounge
〒530-0011 大阪市北区大深町3番1号グランフロント大阪北館ナレッジキャピタル7階K708
HP：https://www.ciolounge.org/
FB：https://www.facebook.com/CIOLounge