DXを推進するために
サイバー攻撃から製造現場を守る
～サイバーセキュリティは難しくない～

サイバーコマンド株式会社 代表取締役
一般社団法人情報処理安全確保支援士会 理事
“浦中 究”

2022/05/13

CYBER COMMAND

代表取締役：浦中 究（Uranaka Kiwamu）

経歴

■国内大手SIer、世界的なソフトウェアメーカーにて、プロジェクトマネージャ、サービスマネージャとしての実績と、サーバインフラ、ネットワーク、データベース、クラウド、サイバーセキュリティのエンジニアとして経験を積み、ベンチャー企業にてCISOを務めた後、サイバーコマンド株式会社 代表取締役に就任。

■「一般社団法人情報処理安全確保支援士会」「国際サイバーセキュリティ協会」の理事を務め、国内外における「産・学・官・個」の連携推進、活性化のためのイベントを主催するなど、積極的な活動を行っている。

■総務省が所管している「独立行政法人情報通信研究機構(NICT)」が主催する、“実践的サイバー防御演習「CYDER」”の講師を務めるなど、国内では人材の育成や、組織のマネジメント力の向上に尽力している。

ご挨拶

■日本のサイバーセキュリティ対策は脆弱で何もしてないといってよい状況で大変危機的です。この状況を打破するためにはこれまで日本で行われてきたような啓蒙活動ではなく、次のステージへ行く必要があると考えています。実践型の教育・およびそれを受けた人材を広く社会に供給していくことで次のステージへ日本を導く。それを担うのがサイバーコマンド株式会社です。皆様どうぞよろしくお願いいたします。

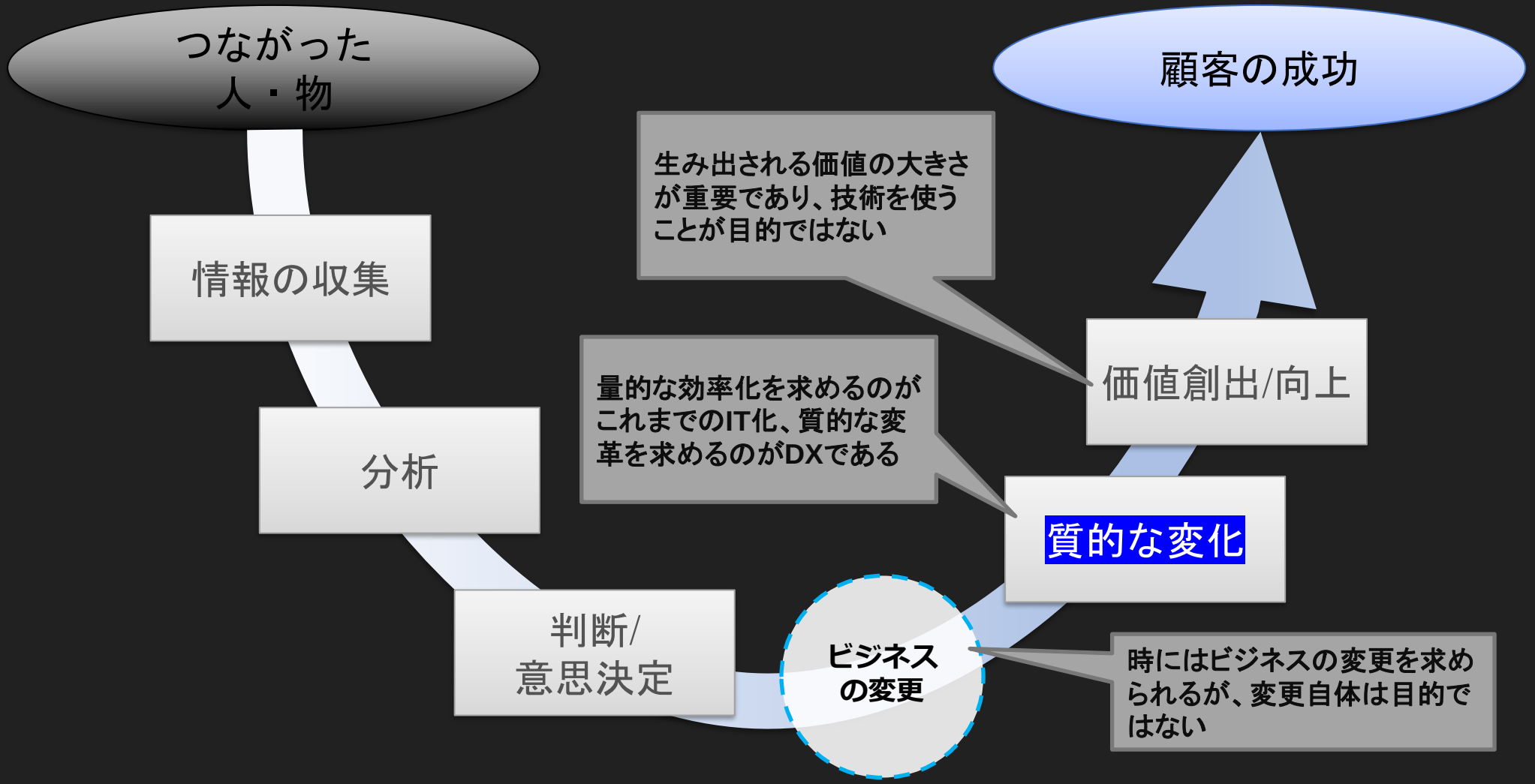
JP-RISSA 情報処理安全確保支援士会

IACS International Association of Cyber Security

>Section01<
DXと
サイバーセキュリティ
の関係性

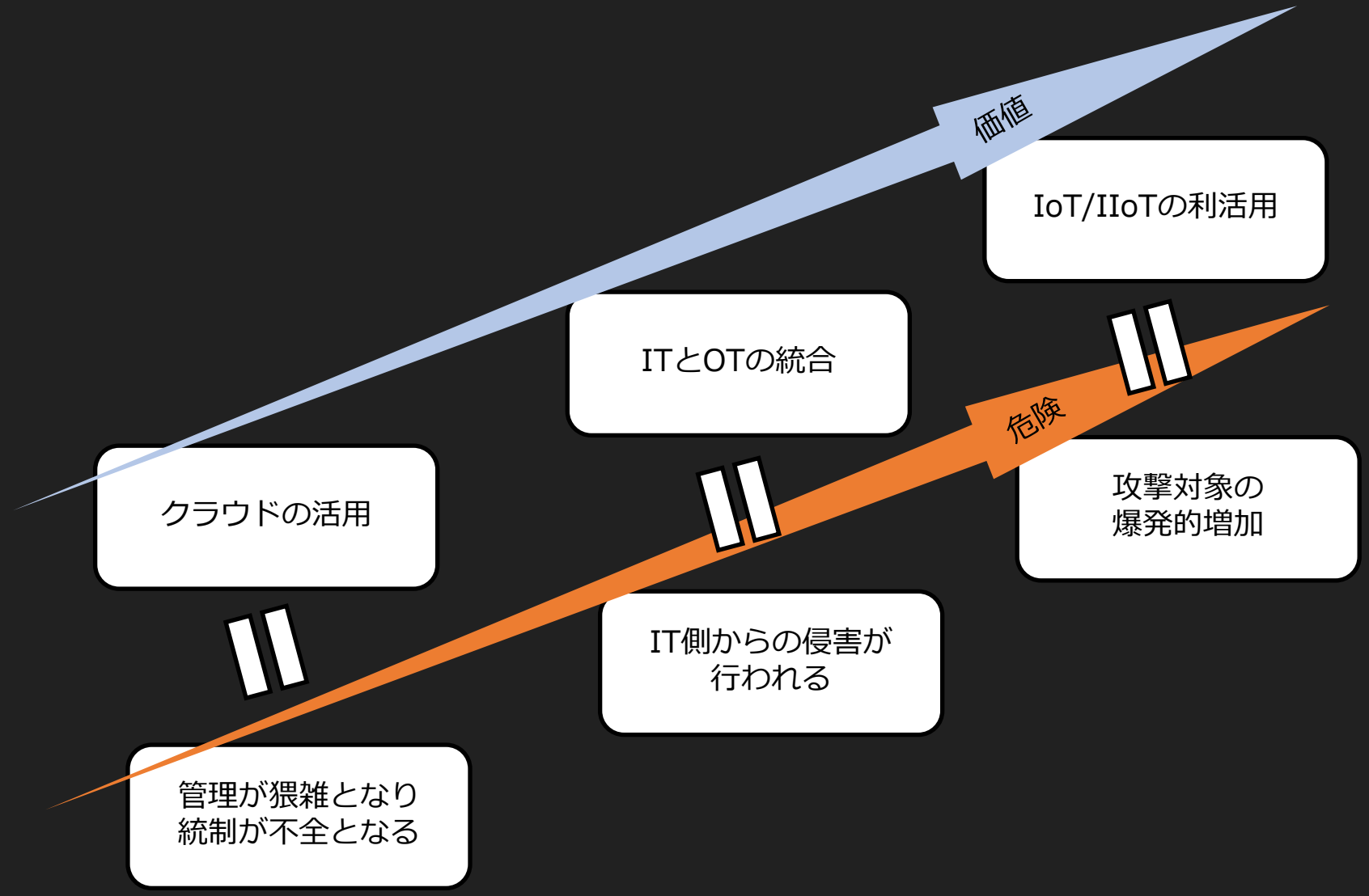
まずはDX(デジタルトランスフォーメーション)を再認識

- DXの本質は素早く意思決定し、質的な変化をもって顧客へ高い価値を提供していくことである。まずはデジタル変革の本質を理解した上で、サイバーセキュリティについても理解を深めていただきたい。



DXが進むことによる危険の増加

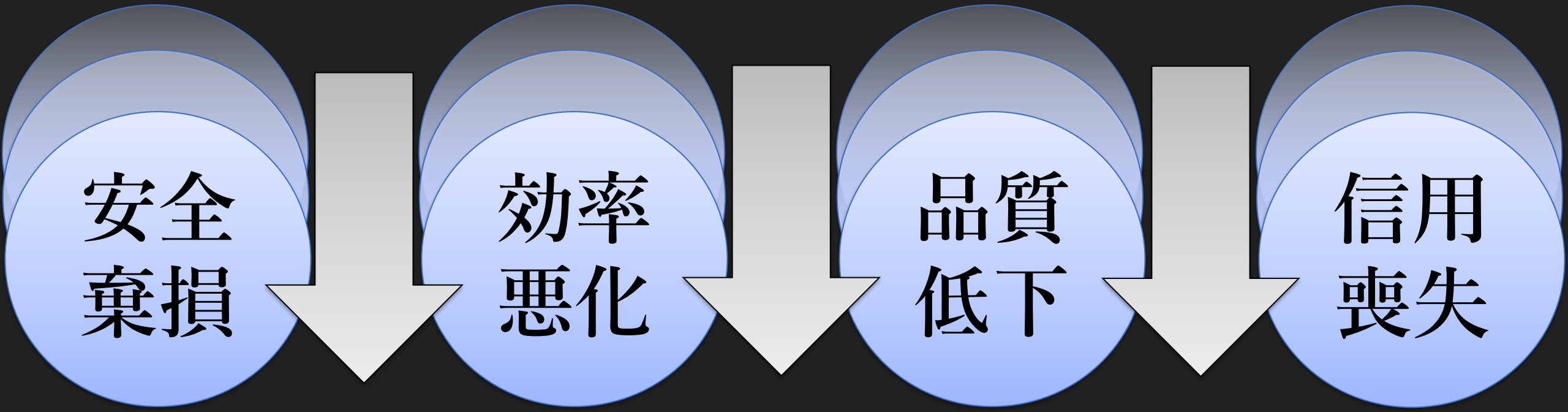
- DXを推進すればするほど現場にコンピュータが浸透していき。それと引き換えに危険が増していく。



>Section02<
サイバーセキュリティの考え方

サイバー攻撃を受けたとして現場では何かマズいのか？

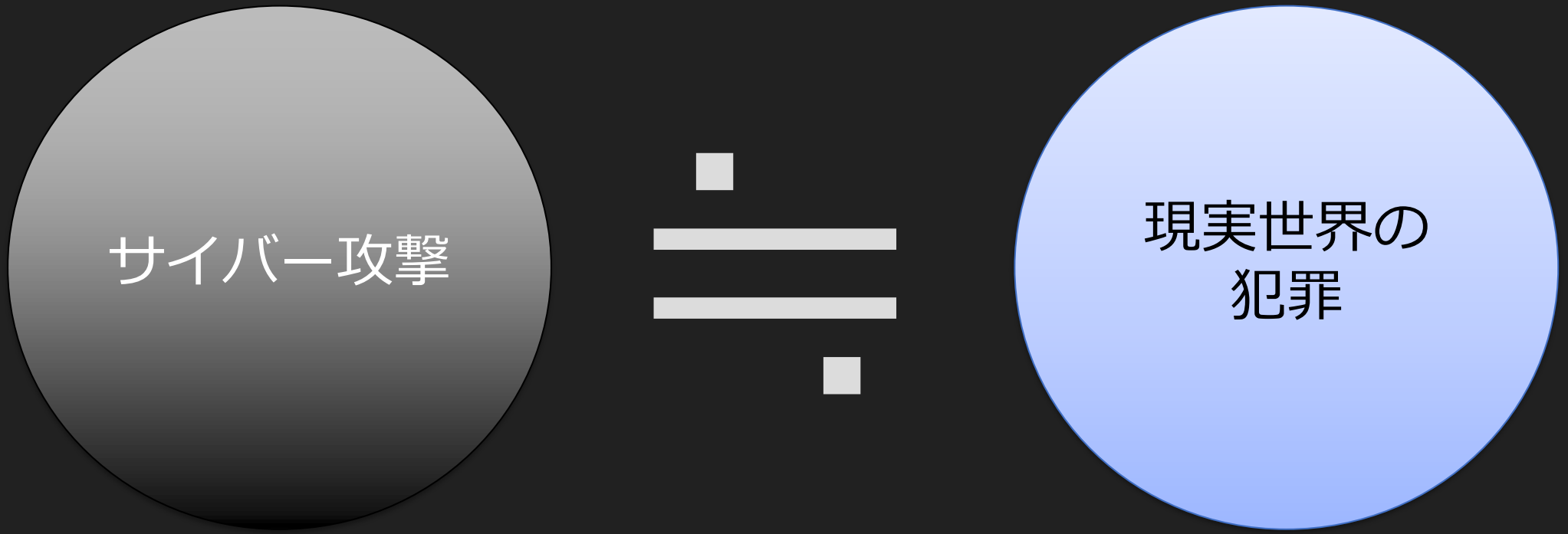
- 誤動作や停止によって現場で大切にしてきたものが脅かされるということである。



日々の努力や投資が水泡に帰す

まずはサイバー攻撃を難しく捉えないことが必要

- サイバー攻撃はコンピュータの中で起きているが、手段や方法によって見え方が異なるだけであり、現実世界の不法侵入、テロや窃盗、詐欺などの犯罪と同じであり、犯罪者の心理や目的も同じである。よく解らない特殊なものと考えずに防犯の一環としてとらえるとよい。



対策には一定の知識もった人が必要となるが難しく考えない

- サイバー攻撃への対策については一定の知識を持った人が必要となる。それはサイバー攻撃を見つけ出したり、対処するためには様々なソフトウェアを使いこなす必要があるためであるが、この部分にだけ一定のハードルがあると捉え理解を放棄しないようにされたい。

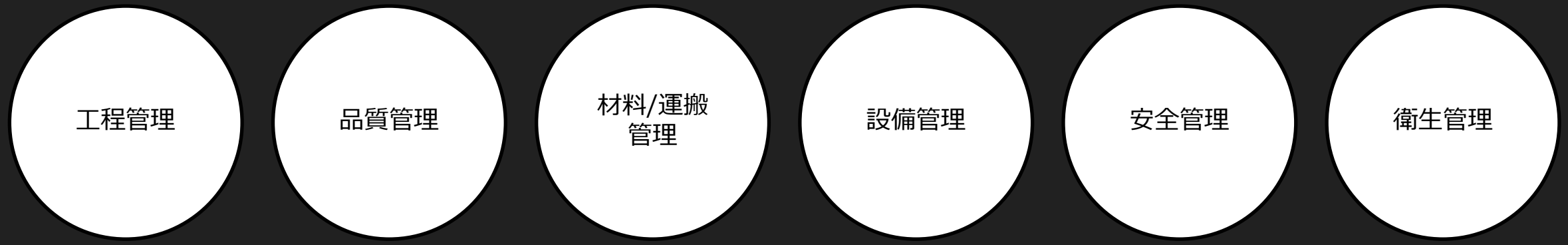
一般的な防犯に対する理解

＋

サイバー攻撃に対する理解

そして現場で管理するべきことが一つ増えたということ

- サイバーセキュリティはやや強引であるが「情報処理管理」と言い換えることが出来る。例えば製造業では工程管理、安全管理、品質管理等もはや当然となっている。こういった管理が1つ増えるのであると考えていただきたい。

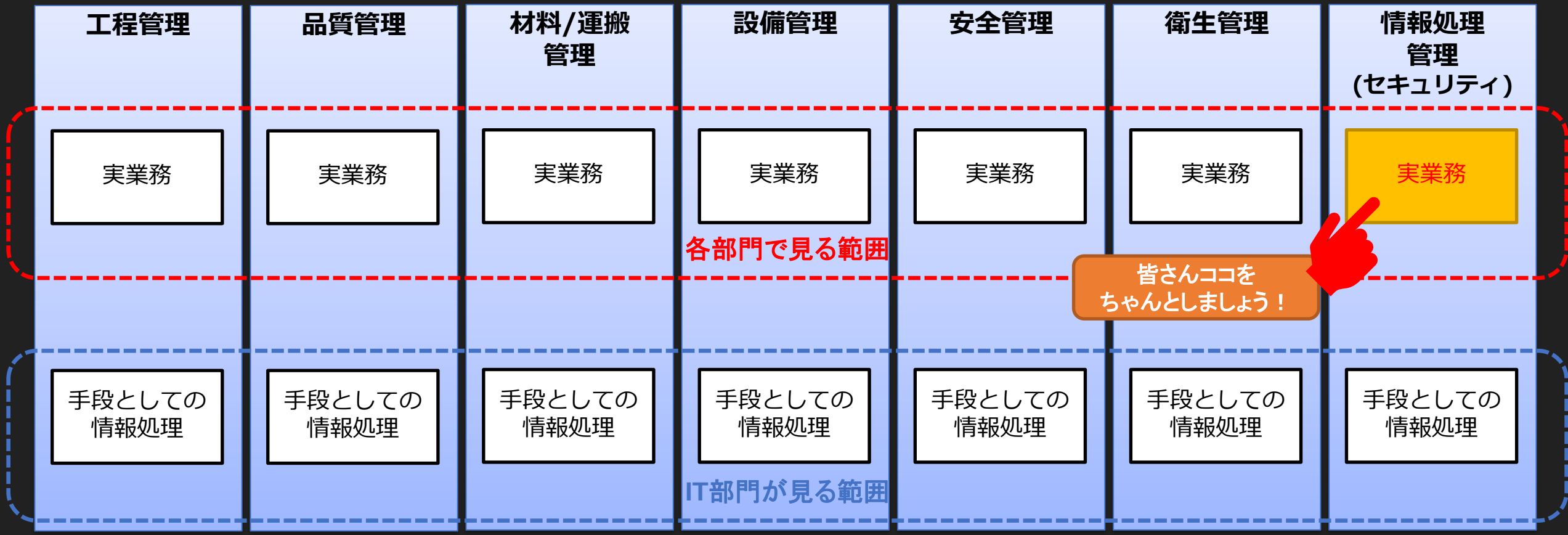


情報処理
管理
(セキュリティ)

IT化やDXが
進むことによって
管理することが1つ増えた！

つまりは管理する”シクミ”と“ヒト”が必要ということ

- コンピュータが正常に動いているか、悪者がおかしなことをしていないかチェックし。発見したならば直ちに是正・排除する仕組みが必要となっている。なお「IT部門に任せておけばよい」というのは“大間違い”。IT部門は情報処理の手段を提供しているだけである。今どきはどの部門でもパソコンを使っているが、その状態でIT部門がその部門の仕事をしているといえるのか？という観点で見ていただくと理解しやすい。要するに今現場では仕組みもないし人もいないところがほとんど。



セキュリティを担保する便利な製品は存在しない

- 製品を動かしているプログラムは人間がキーボードを叩いて入力を行っている。当然入力間違いもあるし、時には100人以上が分担して入力を行うため、作業者の勘違いや思い違い、伝言ゲームの中で失われる情報もある。また省力化を行うために過去に作成したものを流用する場合もある。するとプログラムの全体を把握するものは存在しなくなる。想定する動きは作成途中の段階で確認されるが、想定外の動きを要求された場合、プログラムがどのような動きをするのかは、実際にそうなってみないと分からないのである。

サイバー攻撃そのものはゼロに出来ない

- システムへの侵入や破壊、データの詐取等のサイバー攻撃を完全に防ぐことは事実上困難である。現実世界と同様に犯罪者＝攻撃者は様々な理由によって発生し、彼らの存在を根絶することは事実上不可能である。

海外では国家レベルで研究している

- 海外では国家レベルあるいは、大規模な集団が脆弱性(ソフトウェアやハードウェアの欠陥)の研究が行われている。こういった組織では大量の未発表情報を保有している。このメーカーですら知らない情報を悪用する攻撃については、専門家であっても対処が難しい。

日本の周辺国には
研究機関を有している国が多い

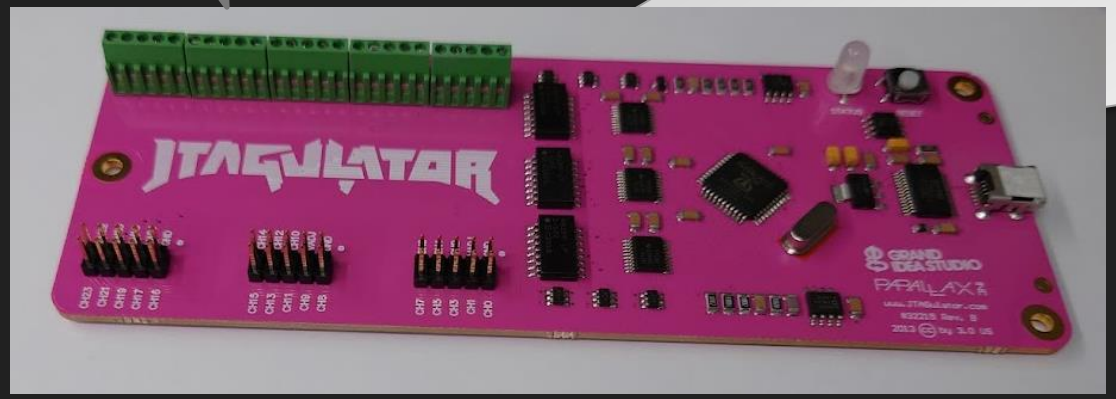
インターネットは無法地帯と直結する入口でもある

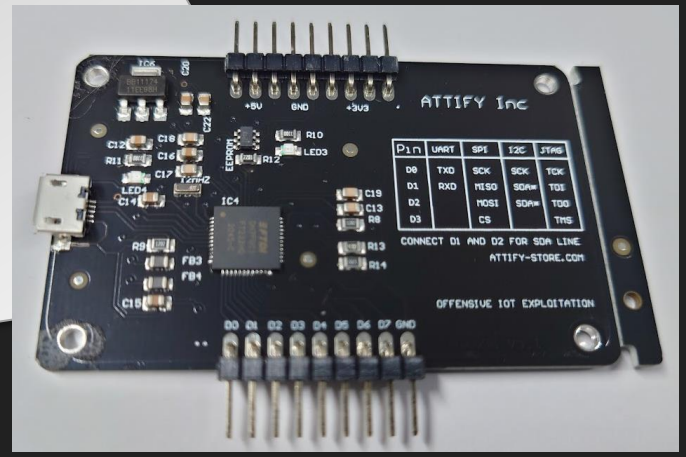
- インターネットは便利で可能性に満ちている反面、世界中の無法者と直接つながってしまうなど大きな危険性を孕んでいる。事務所の扉を開けると、紛争地帯や、治安の悪いスラム街、あるいは密売人の部屋に繋がっていると想像すると仕事中も気が抜けないのではないだろうか。インターネットはまさにそのような状況を作り出すのである。実際にインターネットにコンピュータを接続すると10分もしないうちに様々な国からの攻撃が仕掛けられる、まさに無法地帯である。

ネットワークに接続されていなくても危険

- USBメモリなどの可搬媒体による攻撃は有名であるが、配線に直結するタイプの装置と、それを悪用するためのソフトウェアを組み合わせる手法も豊富に存在している。ネットワークに接続されていないので、安心であるという考え方も通用しない。

非常に優秀な分析装置であるが、本来の使い方ではなく、しばしばハッキングツールとして悪用される。

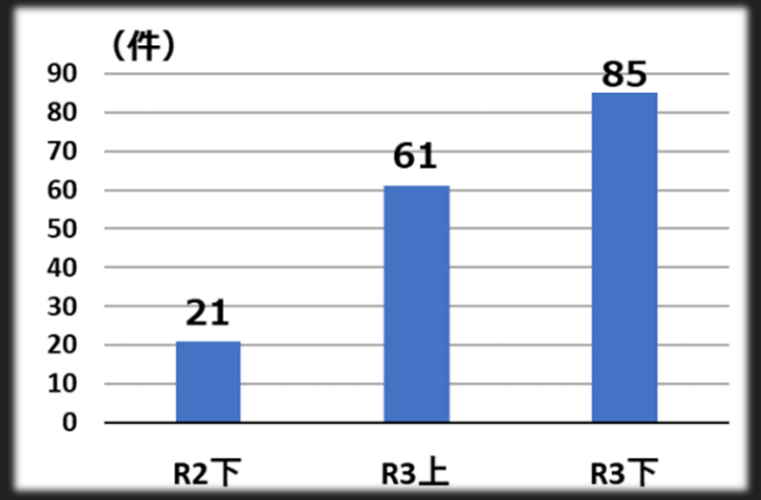




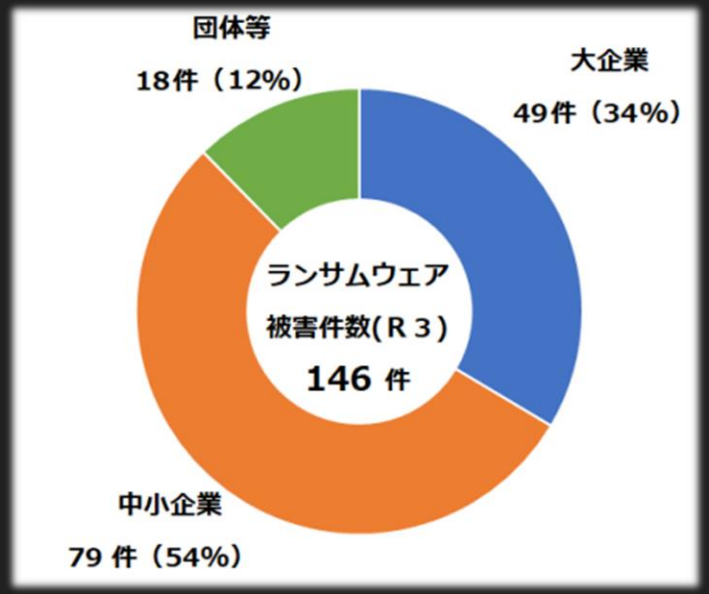
＊弊社ハッキングラボに設置している装置の一例

警察庁の資料を読み解く

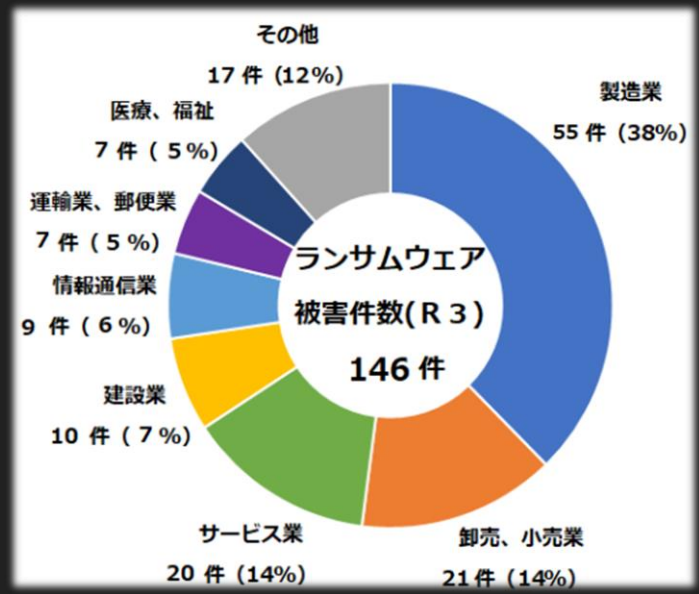
- 警察庁が2月10日に発表した2021年の「サイバー空間をめぐる脅威の情勢等について（速報版）」によると、企業や組織でランサムウェアによる被害が“激増”していることが分かった。大企業をはじめ中小企業も多く狙われており、その中でも製造業の被害が目立った。



企業・団体等におけるランサムウェア被害の報告件数の推移



被害企業・団体等の規模別 報告件数

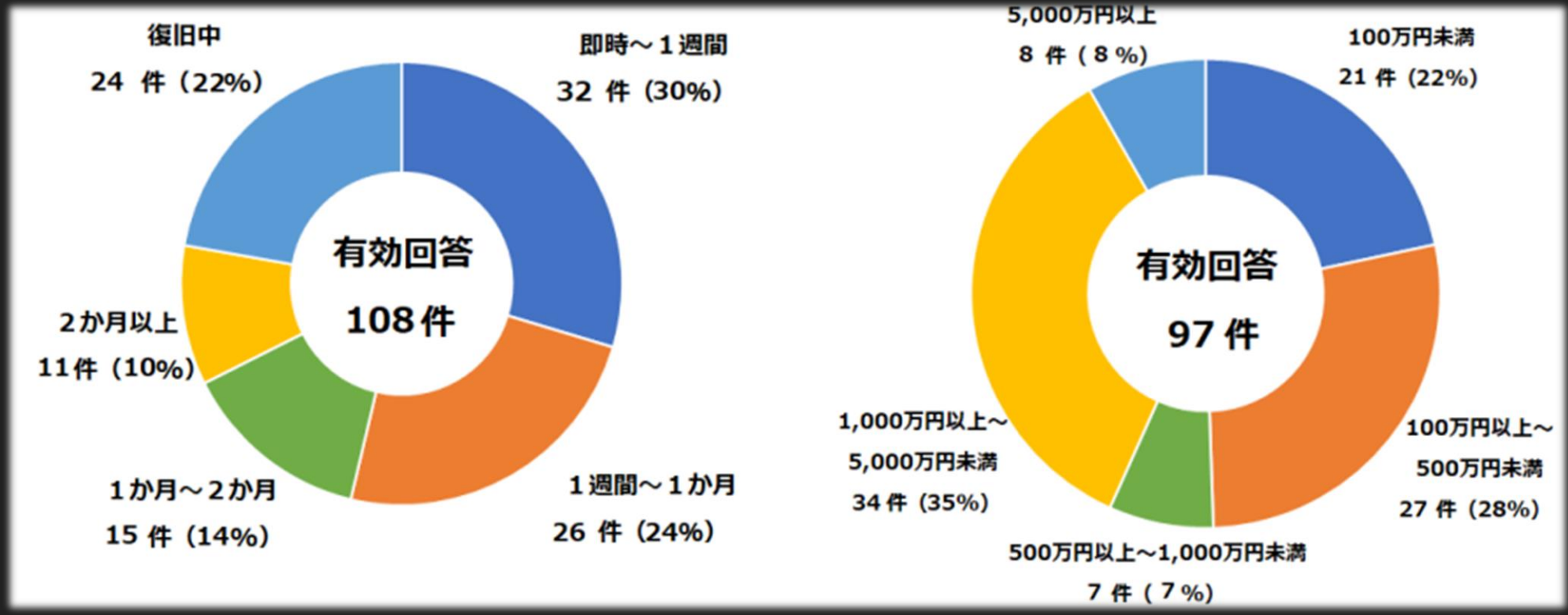


業種別の比率

※「サイバー空間をめぐる脅威の情勢等について（速報版）」より引用

被害の状況

- 復旧にかかる時間は様々であるが、弊社へよせられた相談では調査の完了までに、おおよそ1カ月前後がかかるのが一般的で、並行して復旧するような流れとなる。すぐに復旧したくとも調査が完了していないので着手出来ない場合もあるため、いかに早く調査を終えるかもポイントとなる。被害額も高額になりがちで一千万円前後の損失を覚悟する必要がある。

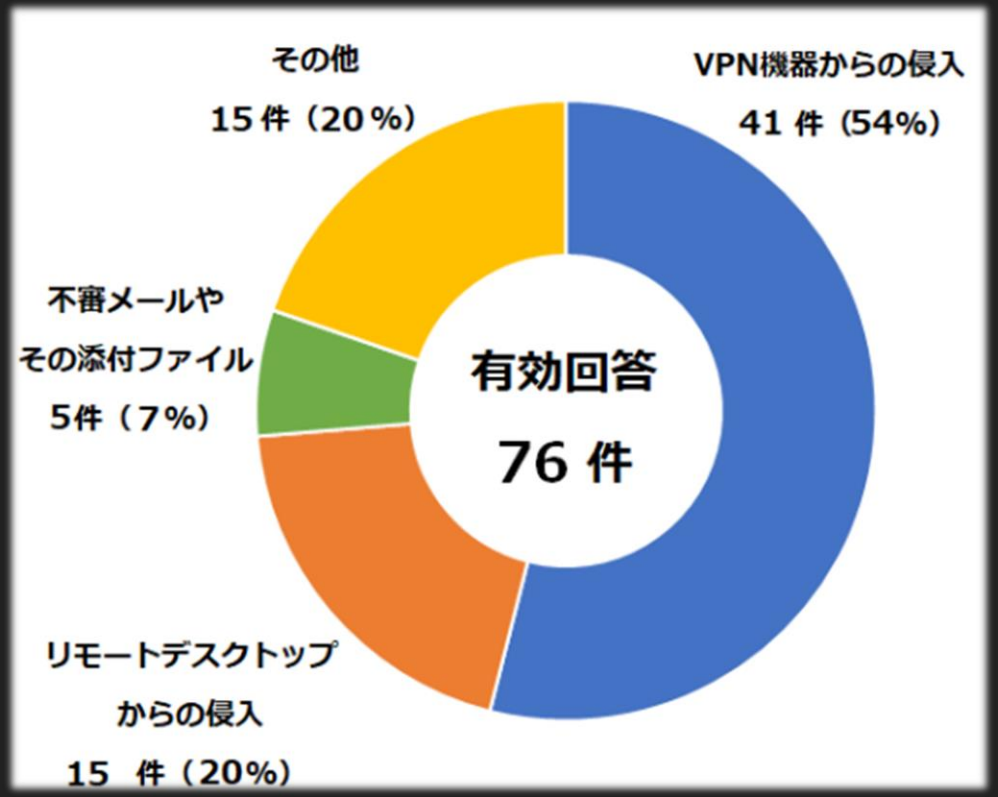


復旧に要した期間と費用

※「サイバー空間をめぐる脅威の情勢等について（速報版）」より引用

セキュリティ対策製品単体では守れないことが証明された

- 今回の資料では「**VPN装置からの侵入**」が過半を占めた。セキュリティ対策で導入する機器にも脆弱性が存在し、一つのソリューションを導入しただけでは安心できないことを調査結果が証明した格好となった。侵入されることを前提とした運用体制の構築と訓練、いかに素早く検知するのかといった備えが必要である。



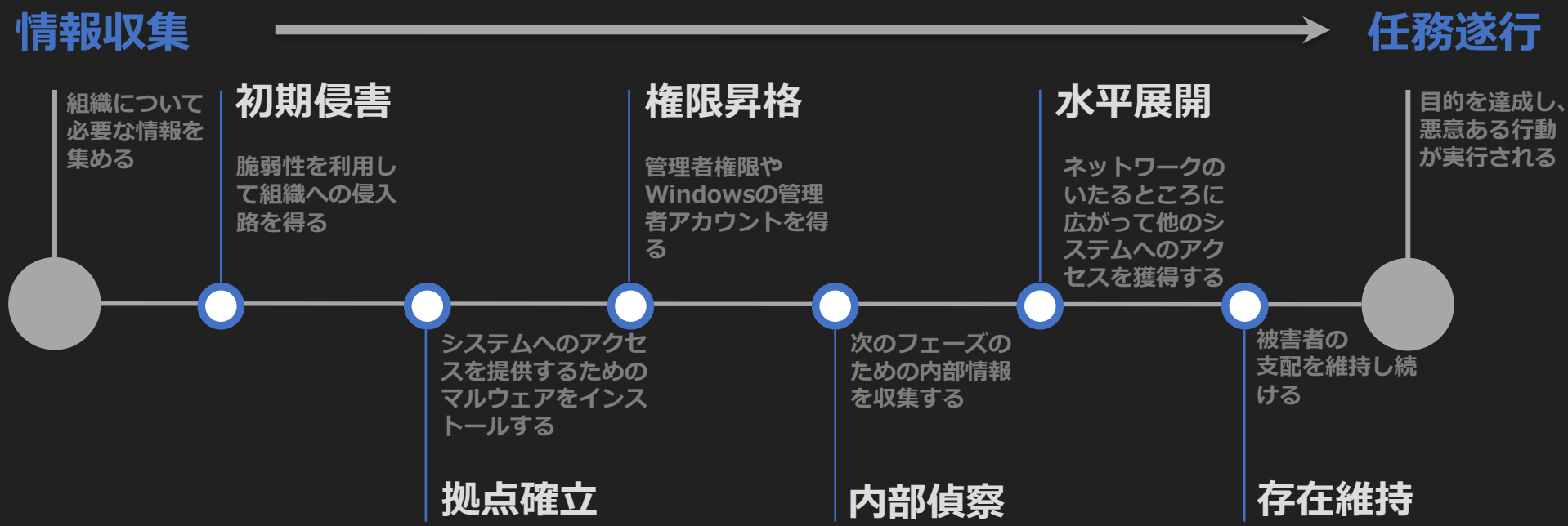
感染経路

※「サイバー空間をめぐる脅威の情勢等について（速報版）」より引用

>Section03<
サイバーセキュリティ
を向上させるには

サイバー攻撃は順序に則って進行する

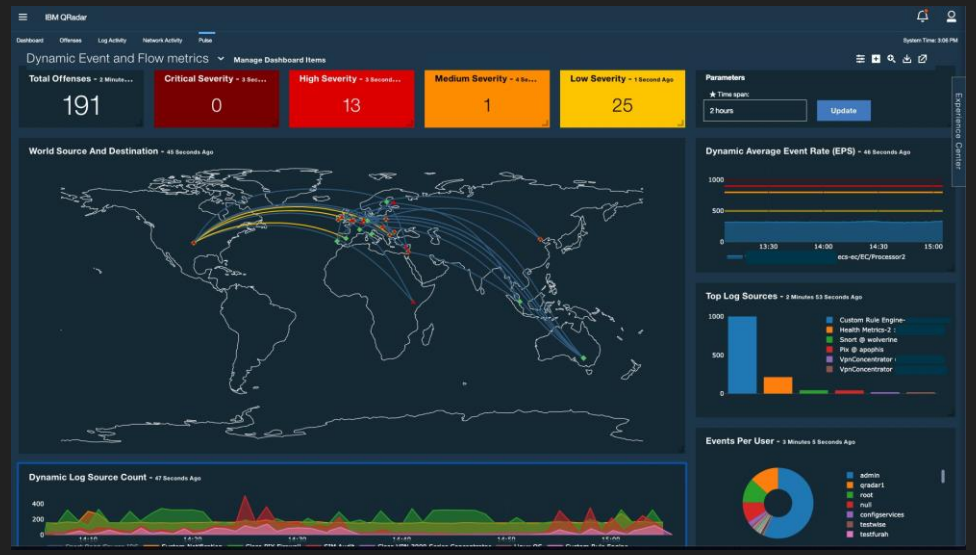
- サイバー攻撃は一定の順序で進行する。そのため各フェーズごとに的確な対処を取ることが求められる。なおマルウェア感染は初期侵害や拠点確立のフェーズであり、マルウェアに感染＝質的被害というわけではない。一般的に情報収集から任務遂行までは6～18ヵ月程度かかるとされており、今どのような状態にあり、どのような対処が打てるのかを、随時判断することが肝要である。ただし標的型攻撃は一瞬で任務遂行を目指すこともあるため、気を抜くことは出来ない。



徹底的にやるなら検知型製品の導入

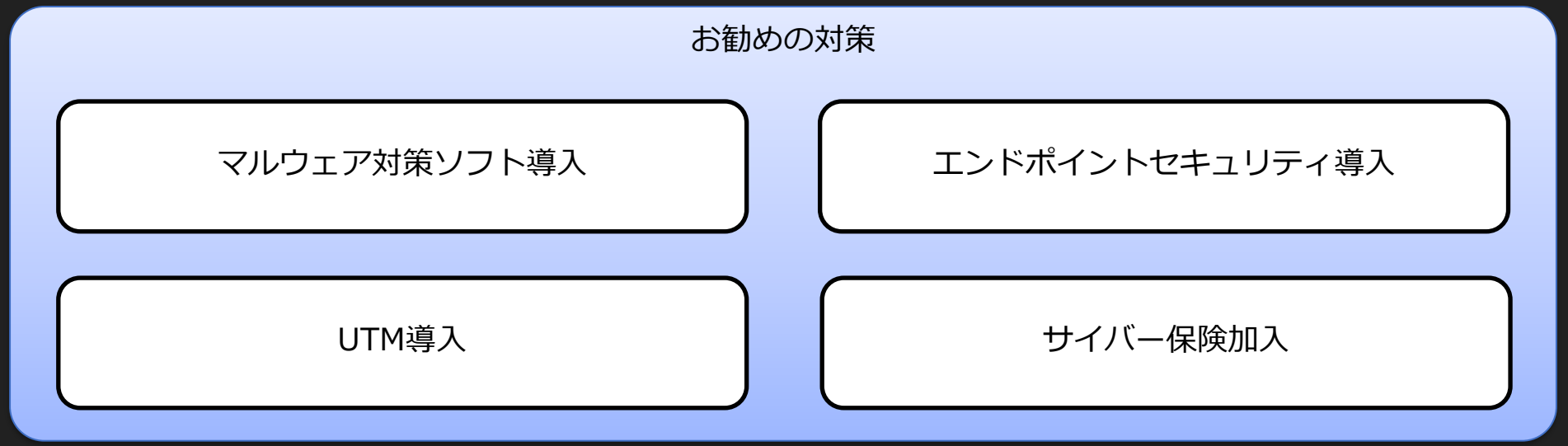
- サイバーセキュリティを徹底的に強化する場合は、検知型の製品を入れて可視化するとよい。ただしかなり高額になる傾向がある。中小規模ではほぼ無理なこと。

SIEMという製品を使うと何が起きているか見える出来る



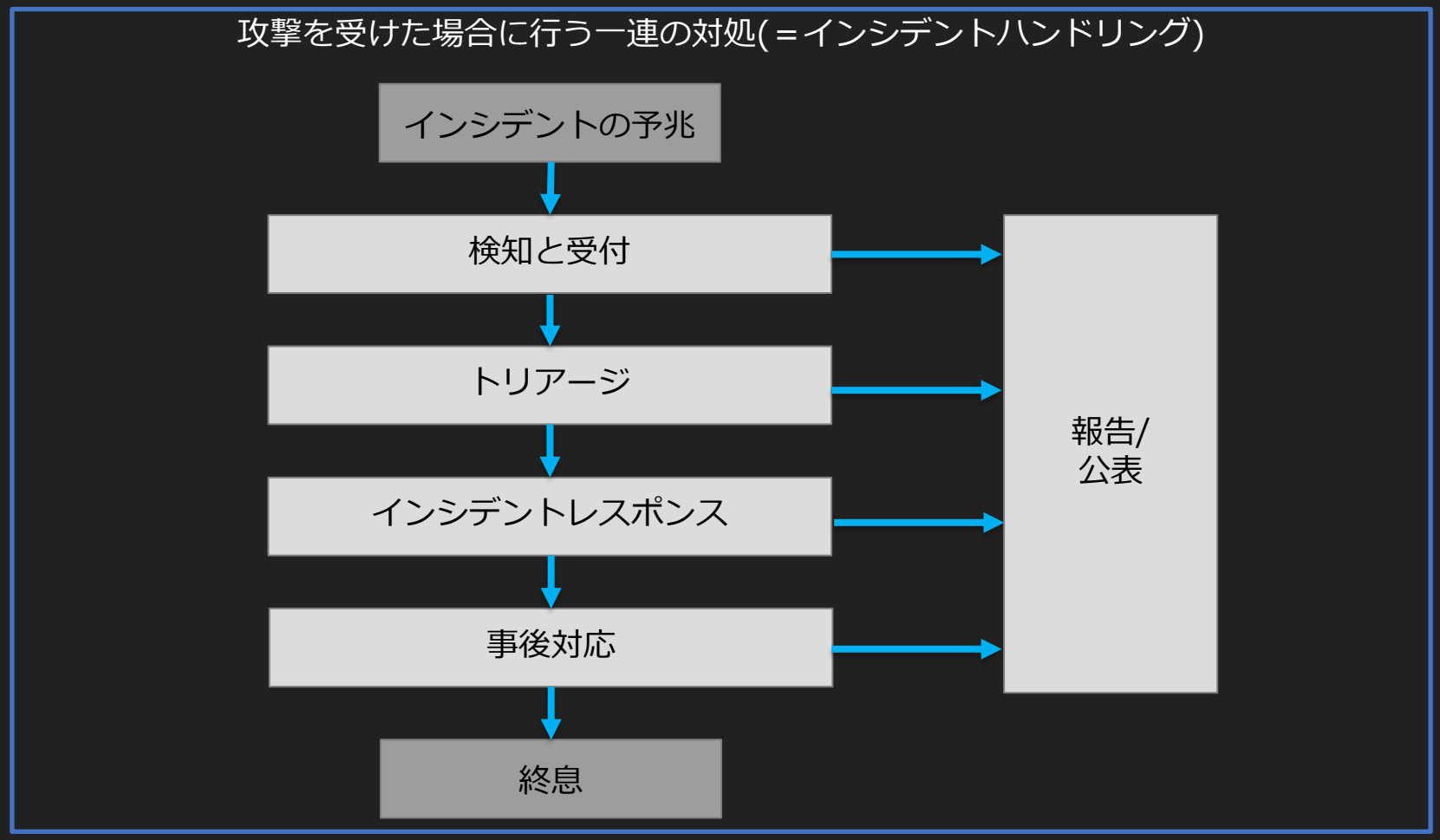
今どきの最低限はこれぐらい、まずはココから！

- 対策製品を導入することは大変有効であるが、かけられる予算は限られる。しかも単一の製品では簡単に突破されてしまう。一つ一つは完璧でなくても複数を重ねることで、強固な防壁を築くことができる(多層防御)。あとは保険でカバーする。
- ただし製品には必ず穴があるという意識をもって、人的な運用面も強化するべきである。



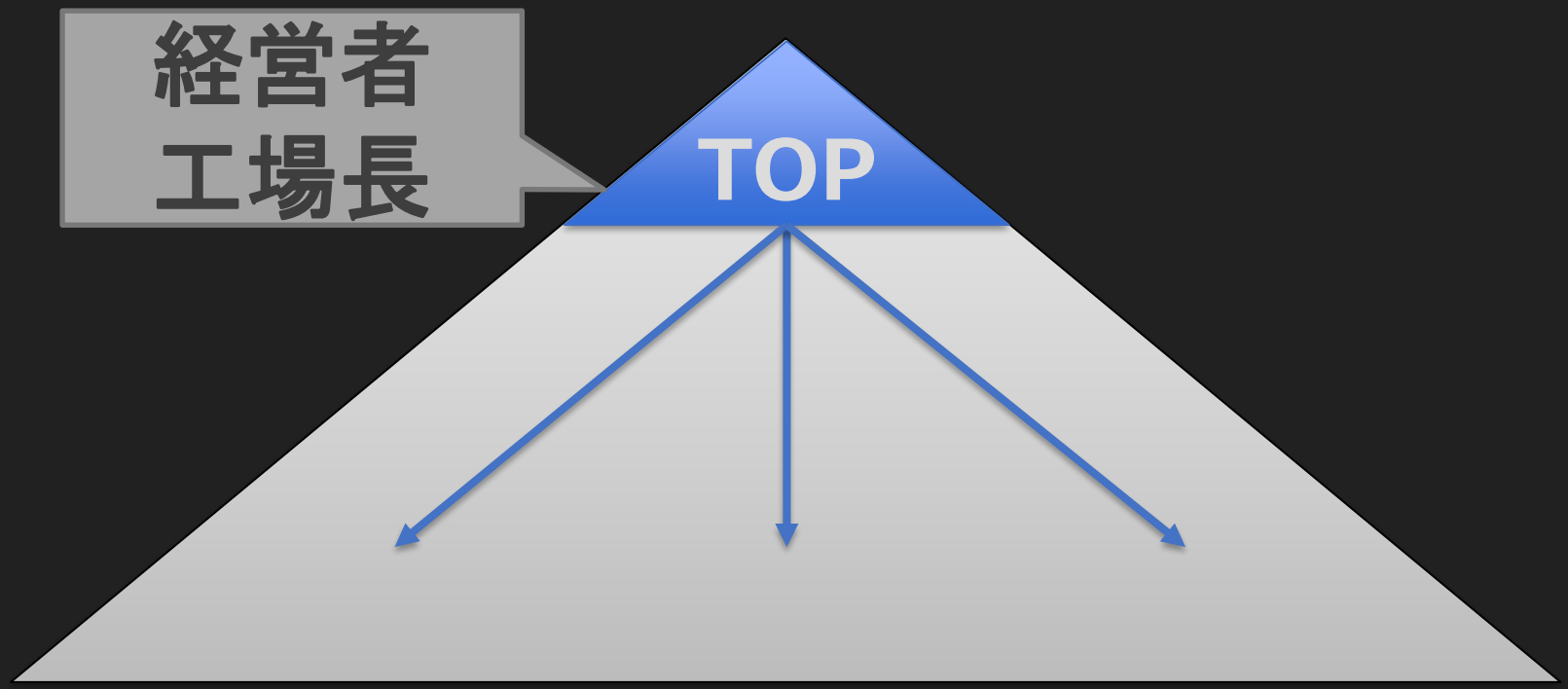
人的な運用面の強化

- サイバー攻撃の手法やツールは日々新しくなるが、攻撃を受けた場合の運用は今も昔も大きく変わらない。しかしただ知っているだけではダメで、消防訓練と同じように咄嗟の出来事に素早く対処するためには、定期的な訓練の実施が必要不可欠である。多くの関係者が訓練に参加することで、一連の対処についての理解が深まり組織としての対応能力、防御力が上がっていく。



トップマネジメントのコミットメントは必須

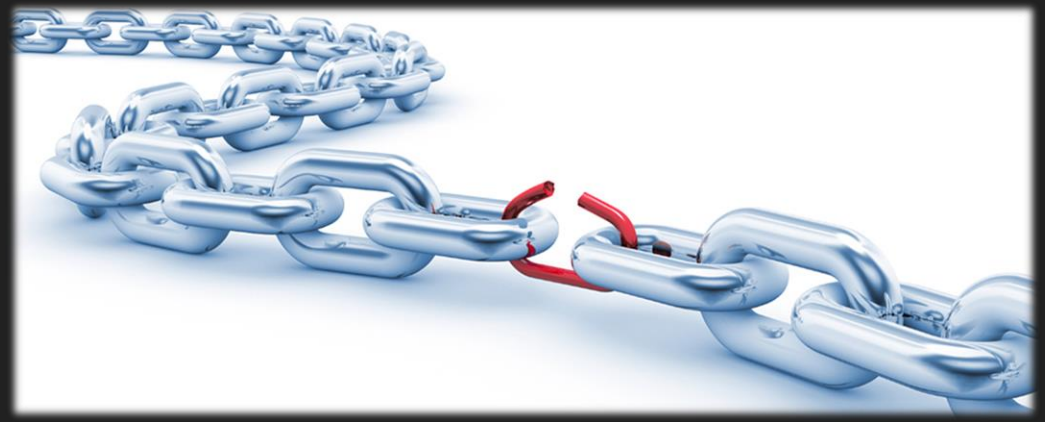
- 組織のTOPがサイバー攻撃に対しての理解を深め主導することが必須である。各種のガイドラインでも経営陣主導の体制整備や対処計画づくりを求めているが、この度、政府からも2022年度から14分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油）の重要インフラ事業者に対して、サイバー攻撃への備えを義務付けることを求めると発表された。IT部門や危機意識の高い担当者だけがボトムアップで対処する時代は終わりを告げようとしている。



>Section03<
セキュリティインシデント
実例

「トヨタ」 サプライチェーン攻撃により操業停止(2022/2/27)

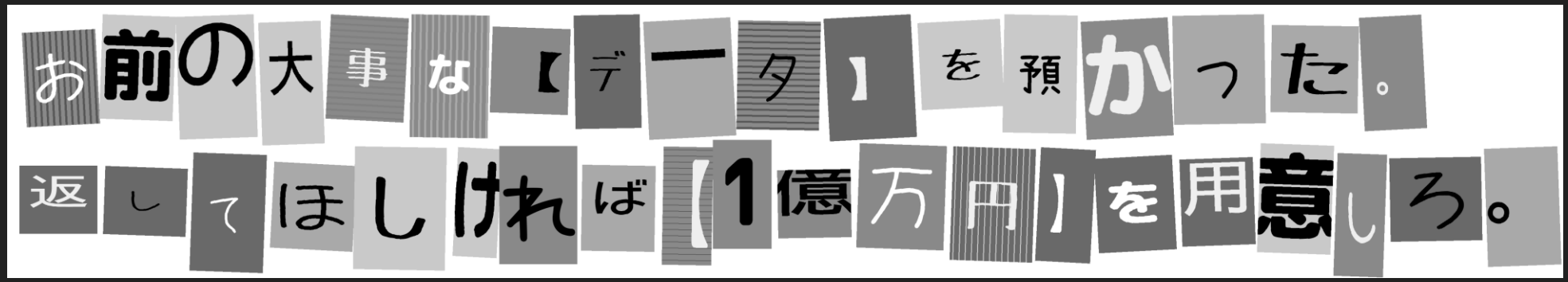
- トヨタの主要取引先である樹脂部品メーカー小島プレス工業(愛知県豊田市)がサイバー攻撃を受け、ネットワークを遮断したことで、部品の受発注に支障をきたすに至りトヨタの主要な工場(14工場の28ライン)が停止した。同社には脅迫メッセージも寄せられたということで、盗んだデータなどと引き換えに多額の身代金を要求する「ランサムウェア攻撃」と推測されている。ランサムウェアによる攻撃はロシアが強みを持っており、昨今の国際情勢を受けての関与が疑われる。



一番弱いところが狙われる

「デンソー」 ランサムウェアにより情報漏洩(2022/3/14)

- デンソーは14日に「第三者による不正アクセスを受けた」と正式発表した。ランサムウェアによるサイバー攻撃で、一部の情報が流出したと認めている。デンソーは2021年の12月にもサイバー攻撃を受けており、この際に個人情報が流出している。トヨタ系の企業は日本への経済的影響力が大きいことから狙われたとみられている。犯行声明によると、盗みだされたデータは1.4TB、15万7000件を超えであるとのこと。



影響力が大きいところが狙われる

「東映アニメーション」 新作の放送・上映が不能となる(2022/3/11)

- 地上波放送の「ワンピース」「ダイの大冒険」「デジモンゴーストゲーム」「プリキュア」、映画作品の「ドラゴンボール」が放送・上映が一カ月以上延期の見通し。海外から見た日本と言えば”車(トヨタ)”と、”サブカルチャー(アニメ等)”であり、象徴的な出来事として見ることができる。

日本の強みも狙われる

「パナソニック株式会社」 ファイルサーバ不正アクセス(2021/11/26)

- 同社の発表によると海外子会社のサーバを経由して、国内の機密情報へのアクセスが確認された。定期的に実施している通信記録の分析から発覚。同年6月22日から11月3日までの約4か月の間複数回行われており、採用で収集した履歴書情報、官公庁を含む取引先役職員の個人情報や、取引先より提供を受けた業務関連情報が漏洩したとみられる事例(ダークウェブ上で窃取したとされるファイルが販売に出された、ただし確定だという情報は出ていない)。

サプライチェーン型攻撃

国内企業も大企業は一定の対策を講じ始めている。しかし、取引先や海外の子会社となると統制が取れず、簡単に侵入されてしまう事案が後を絶たない。

ダークウェブでの取引

ダークウェブ上での違法な取引は活発化して来ている。一度流出した情報はインターネット上に永遠に残り続け、唐突に売りに売りに出されたり、次の攻撃のために悪用されると認識することが必要。

「三菱パワー株式会社」 MSP経由で不正アクセス(2020/12/11)

- 発表によるとマネージド・サービス・プロバイダ(MSP)を経由した第三者による不正アクセスを受けたことが確認された。本年10月2日にパソコンの不審な挙動を検知し、三菱重工と連携して調査を開始。翌日にかけて複数のサーバ/パソコンから外部に不正通信があることが判明したという事案。ITベンダーが提供するMSPという、複数の企業とネットワークで接続されたサービスが狙われたため、IT業界に大きな衝撃をもたらした。発覚の発端は同社が不審な挙動に気が付いたことであり、内部で対策を講じる事の有効性も同時に再認識させた事例。

ITのプロに任せておけば安心ということではない

内部の有識者、一般社員が一丸となって発見していくことが必要

「未来の工場」 サイバー攻撃により爆発炎上、死者多数(202X/4/14)

- 実在しない同社の発表によると、サイバー攻撃により化学薬品を製造するプラントが異常をきたし制御不能となった。結果として薬品を一時保存する容器内部の圧力が高まり破裂、爆発炎上に至った。手動による復旧作業に当たっていた作業員が巻き込まれ14名が犠牲となった。※この例はフェイクです。

次々狙われる重要インフラ

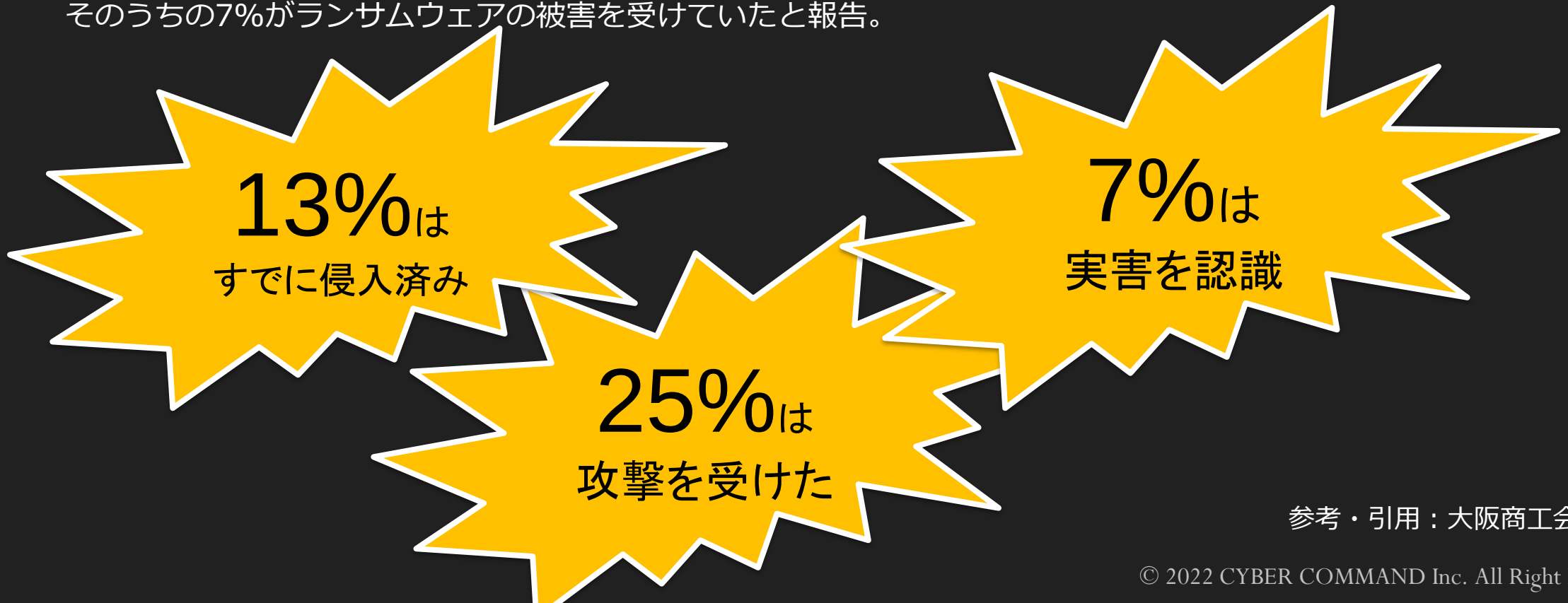
“サプライチェーンへの影響拡大を目的に中小企業が集中的に狙われている”

大手企業のセキュリティ対策が進んできたことにより、攻撃者は中小企業に狙いを定めている。サイバー攻撃の発端となった企業は、取引先から厳しい目を向けられる。

大阪におけるサイバー攻撃の実態
企業はすでに攻撃者の手中に落ちている？

大阪商工会議所が発行した「平成30年度中小企業に対するサイバー攻撃現状調査」によると、調査に協力した30社中、4社が全く取引関係がないにもかかわらず、攻撃者のサーバを通じて通信しているなどの実態が明らかとなった。

平成29年度のアンケートでは、回答した企業の25%はすでになんらかの攻撃を受けている自覚があり、そのうちの7%がランサムウェアの被害を受けていたと報告。



参考・引用：大阪商工会議所

サイバー空間は
怖いことばかり

ですが
心配ご無用

サイバーコマンドのような
セキュリティ専門企業や
情報処理安全確保支援士が
ご一緒に考えます

>Section04<
情報処理安全確保支援士とは何者か？

情報処理安全確保支援士を知ってください

情報処理安全確保支援士は「ITの安全・安心を支えるセキュリティの番人」です。弁護士、税理士、行政書士の一種で、国が認めた専門家になります。2017年4月から生まれた、まだまだ新しい国家資格となります。なおIT業界初の士業です。

法律上の問題で困った	 弁護士
税金の問題で困った	 税理士
コンピュータの問題で困った	 情報処理安全確保支援士

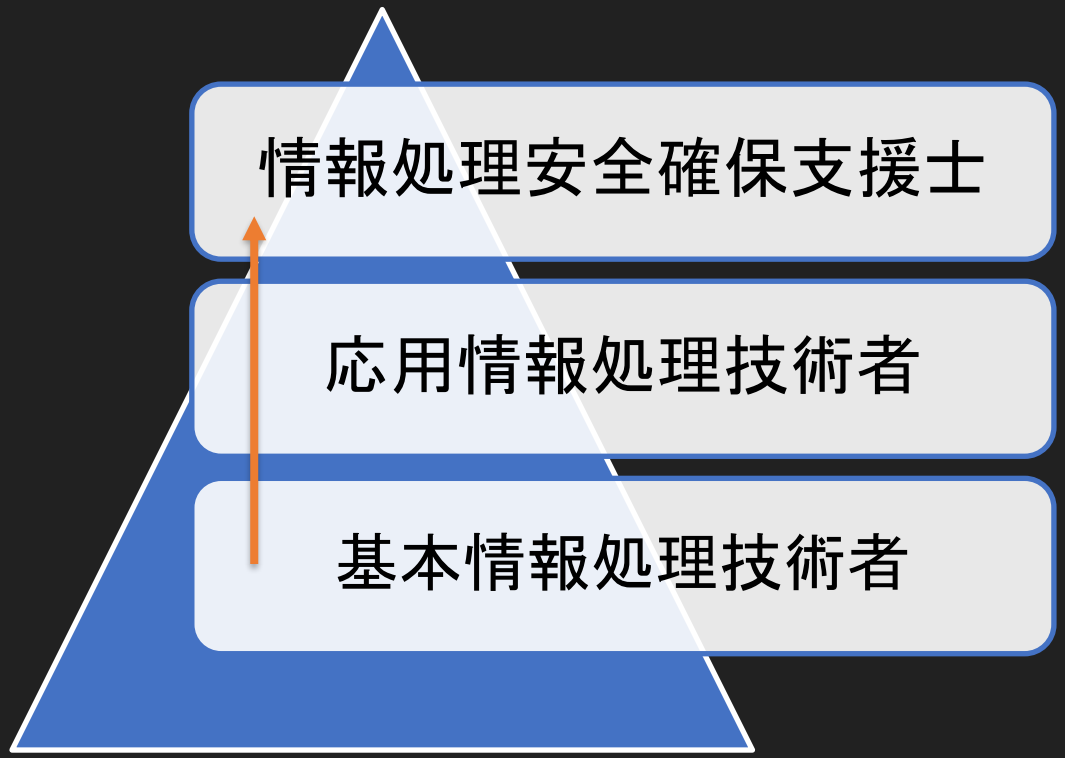
実はコンピュータにかなり詳しい人です

「情報処理安全確保支援士」を取得するには、下位の資格である「基本情報処理技術者」「応用情報処理技術者」を経るのが一般的なルートです。そのためITに対しての深い理解を持っています。セキュリティはもちろん、コンピュータのことで困ったら「情報処理安全確保支援士」に相談することも出来るというわけです。

コンピュータに対する深い理解
(IT製品/IT技術)

＋

セキュリティに対する深い理解
(物理対策/法律)



(1) 需要者（企業経営、社会システム）が直面する課題に対して、情報技術を活用した**「戦略を立案」**する。

(2) システムの設計・開発を行い、又は汎用製品の最適組合せ（インテグレーション）によって、信頼性・生産性の高いシステムを構築する。また、その安定的な運用サービスを実現する。

引用元：https://www.jitec.ipa.go.jp/1_11seido/ap.html

何をしてくれる人なのか？

情報セキュリティマネジメントに関する業務、情報システムの企画・設計・開発・運用におけるセキュリティ確保に関する業務、情報及び情報システムの利用におけるセキュリティ対策の適用に関する業務、情報セキュリティインシデント管理に関する業務に従事し、次の役割を主導的に果たすとともに、下位者を指導する。

※コンピュータと情報セキュリティについて皆さんを支援します

① 情報セキュリティ方針及び情報セキュリティ諸規程（事業継続計画に関する規程を含む組織内諸規程）の策定、情報セキュリティリスクアセスメント及びリスク対応などを推進又は支援する。

※やったらアカンことを決めたり、マズいところを見つけます

② システム調達（製品・サービスのセキュアな導入を含む）、システム開発（セキュリティ機能の実装を含む）を、セキュリティの観点から推進又は支援する。

※セキュリティに強い製品とか、システムなんかを選びます

③ 暗号利用、マルウェア対策、脆弱性への対応など、情報及び情報システムの利用におけるセキュリティ対策の適用を推進又は支援する。

※普段やっておかなアカン事をお手伝いします

④ 情報セキュリティインシデントの管理体制の構築、情報セキュリティインシデントへの対応などを推進又は支援する。

※やられた時の準備や、やられた時に助けます

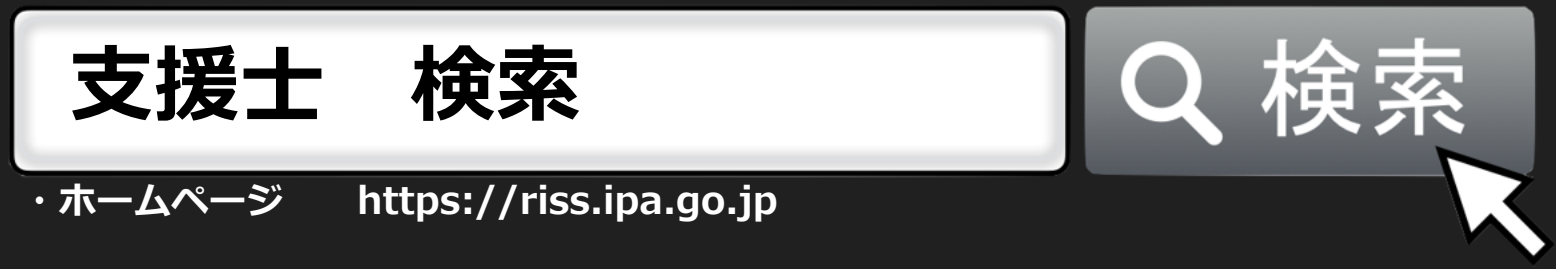
引用元：https://www.jitec.ipa.go.jp/1_11seido/sc.html

>Section05<
情報処理安全確保支援士
を見つけるには？

徽章(バッジ)を付けていますので
街で探してください

というのは
流石にムリですね！

まずは検索



・ホームページ　　https://riss.ipa.go.jp

どうやって探す？

検索すると「情報処理安全確保支援士検索サービス」というホームページが見つかりますので、お好みの情報処理安全確保支援士を検索して見つけていただくことが出来ます。登録しているだけの人も多いため、詳細検索から必ず【支援依頼受付中】をキーワード欄に入れて検索してください。

詳細検索をクリック

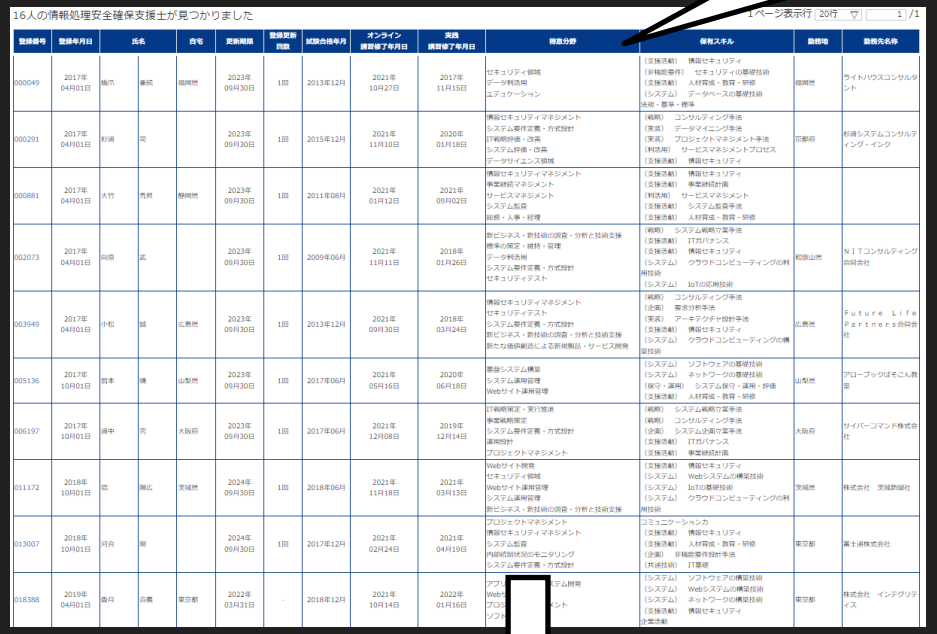
お近くの地域
都道府県も便利です

「支援依頼受付中」と
入力

どうやって依頼する？

検索すると検索結果には住んでいるところであったり得意分野が書かれています。まずは気になる「情報処理安全確保支援士」をクリック。すると詳細の画面が出てきますのでより詳しい人物像がわかります。依頼したいと決められましたら、お電話やメールでコンタクトを取ることが可能です。

得意分野や
保有スキルを見て選択


16人の情報処理安全確保支援士が見つかりました

登録番号	登録年月日	氏名		自宅	更新期限	登録更新回数	試験合格年月	オンライン講習修了年月日	実践講習修了年月日	得意分野	保有スキル	勤務地	勤務先名称
000049	2017年04月01日	楠木	善紘	福岡県	2023年09月30日	1回	2013年12月	2021年10月27日	2017年11月15日	セキュリティ領域 データ解析用 エデュケーション	（支援活動）　情報セキュリティ （非機能要件）　セキュリティの基礎技術 （支援活動）　人材育成・教育・研修 （システム）　データベースの基礎技術 法規・基準・標準	福岡県	ライトハウスコンサルタント
000291	2017年04月01日	杉浦	司		2023年09月30日	1回	2015年12月	2021年11月10日	2020年01月18日	情報セキュリティマネジメント システム要件定義・方式設計 IT戦略評価・改善 システム評価・改善 データサイエンス領域	（戦略）　コンサルティング手法 （実装）　データマイニング手法 （実装）　プロジェクトマネジメント手法 （解決策）　サービスマネジメントプロセス （支援活動）　情報セキュリティ	京都府	杉浦システムコンサルティング・イング
000881	2017年04月01日	大竹	秀昇	静岡県	2023年09月30日	1回	2011年08月	2021年01月12日	2021年09月02日	情報セキュリティマネジメント 事業継続マネジメント サービスマネジメント システム監査 総務・人事・経理	（支援活動）　情報セキュリティ （支援活動）　事業継続計画 （解決策）　サービスマネジメント （支援活動）　システム監査手法 （支援活動）　人材育成・教育・研修		
002073	2017年04月01日	向原	孟		2023年09月30日	1回	2009年06月	2021年11月11日	2018年01月26日	新ビジネス・新技術の調査・分析と技術支援 標準の開発・維持・管理 データ解析用 システム要件定義・方式設計 セキュリティテスト	（戦略）　システム戦略立案手法 （支援活動）　ITガバナンス （支援活動）　情報セキュリティ （システム）　クラウドコンピューティングの利用技術 （システム）　IoTの応用技術	和歌山県	ＮＩＴコンサルティング合同会社
003949	2017年04月01日	小松	誠	広島県	2023年09月30日	1回	2013年12月	2021年09月30日	2018年03月24日	情報セキュリティマネジメント セキュリティテスト システム要件定義・方式設計 新ビジネス・新技術の調査・分析と技術支援 新たな価値創造による新規製品・サービス開発	（戦略）　コンサルティング手法 （企画）　要求分析手法 （実装）　アーキテクチャ設計手法 （支援活動）　情報セキュリティ （システム）　クラウドコンピューティングの構築技術	広島県	Ｆｕｔｕｒｅ Ｌｉｆｅ Ｐａｒｔｎｅｒｓ合同会社
005136	2017年10月01日	野本	博	山梨県	2023年09月30日	1回	2017年06月	2021年05月16日	2020年06月18日	基盤システム構築 システム運用管理 Webサイト運用管理	（システム）　ソフトウェアの基礎技術 （システム）　ネットワークの基礎技術 （保守・運用）　システム保守・運用・評価 （支援活動）　人材育成・教育・研修	山梨県	アローブックばそこん教室
006197	2017年10月01日	浦中	究	大阪府	2023年09月30日	1回	2017年06月	2021年12月08日	2019年12月14日	IT戦略策定・実行推進 事業戦略策定 システム要件定義・方式設計 運用設計 プロジェクトマネジメント	（戦略）　システム戦略立案手法 （戦略）　コンサルティング手法 （企画）　システム企画立案手法 （支援活動）　ITガバナンス （支援活動）　事業継続計画	大阪府	サイバーコマンド株式会社
011172	2018年10月01日	岡	陽広	茨城県	2024年09月30日	1回	2018年06月	2021年11月18日	2021年03月13日	Webサイト開発 セキュリティ領域 Webサイト運用管理 システム運用管理 新ビジネス・新技術の調査・分析と技術支援	（支援活動）　情報セキュリティ （システム）　Webシステムの構築技術 （システム）　IoTの基礎技術 （システム）　クラウドコンピューティングの利用技術	茨城県	株式会社　茨城新聞社
013007	2018年10月01日	河合	剛		2024年09月30日	1回	2017年12月	2021年02月24日	2021年04月19日	プロジェクトマネジメント 情報セキュリティマネジメント システム監査 内部統制状況のモニタリング システム要件定義・方式設計	コミュニケーション力 （支援活動）　情報セキュリティ （支援活動）　人材育成・教育・研修 （企画）　非機能要件設計手法 （共通技術）　IT基礎	東京都	富士通株式会社
018388	2019年04月01日	森井	良義	東京都	2022年03月31日	-	2018年12月	2021年10月14日	2022年01月16日	アプ Web プロ ソフ	（システム）　ソフトウェアの構築技術 （システム）　Webシステムの構築技術 （システム）　ネットワークの構築技術 （支援活動）　情報セキュリティ 企業活動	東京都	株式会社　インテグリティス

経歴やどんなことができるのかなどの情報が詳細に記載されています。「この人にしよう」と決めたら、メールやお電話をいただければと思います。

>Section06<
情報処理安全確保支援士は
どんな仕事をしている？

サイバーセキュリティ駆け込み寺

「パソコンがマルウェアに感染して何かおかしい」「自社の情報が漏洩していると取引先からクレームが入っている」などの、緊急事態に対応いたします。弊社コンサルタントが緊急時のインシデントハンドリングのサポートと、対応への助言を行います。”**秘密保持義務**”を負っている「**情報処理安全確保支援士(国家資格)**」の有資格者が対応いたしますので、スピーディかつ安心してご相談いただけます。

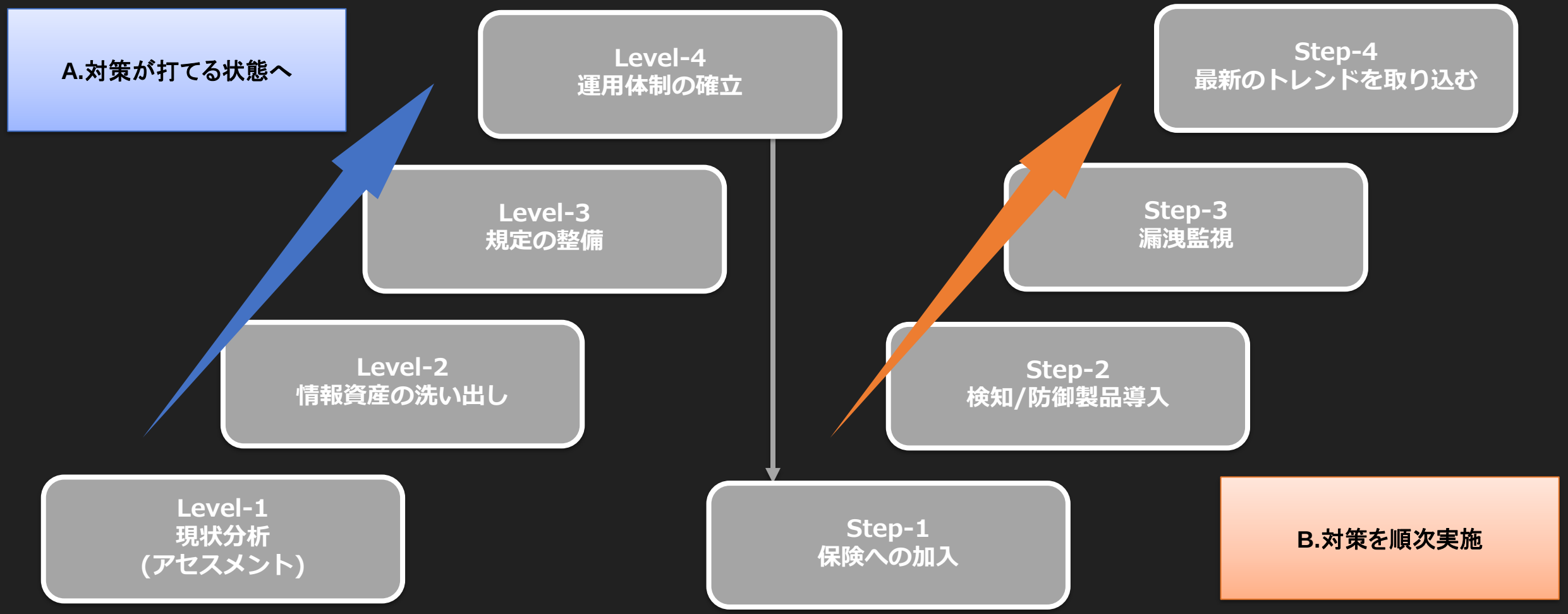
▼ご支援の一例

1. 状況のヒアリングと現状分析
2. トリアージ(優先度付け)
3. 初動時点および随時の情報公開
4. インシデントレスポンス(問題への対処)
5. デジタルフォレンジック(調査)
6. 収束宣言

※「**情報処理安全確保支援士**」とは情報処理の促進に関する法律(昭和四十五年法律第九十号)の中で定められた、サイバーセキュリティに関する国家資格です。サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うとともに、必要に応じその取組の実施の状況についての調査、分析及び評価を行い、その結果に基づき指導及び助言を行うことでサイバーセキュリティの確保を支援することを業とする者が保持する国家資格であり、IT業界で初の“士業“です。

伴走型コンサルティングサービス

ゼロからスタートされる組織や、一定の対策を進めてはいるが今後の対応にお困りの企業・組織も多いかと存じます。弊社の伴走型コンサルティングサービスは、それぞれのシーンにおいて最適な助言を行う形で伴走させていただきます。



Thank you

サイバーセキュリティの脅威から企業と人を守る企業

CYBER COMMAND

サイバーコマンドの教育はここがすごい

～ サイバー先進国イスラエルのカリキュラム ～
日本の技術は周回遅れ！世界最高の技術を学べる！

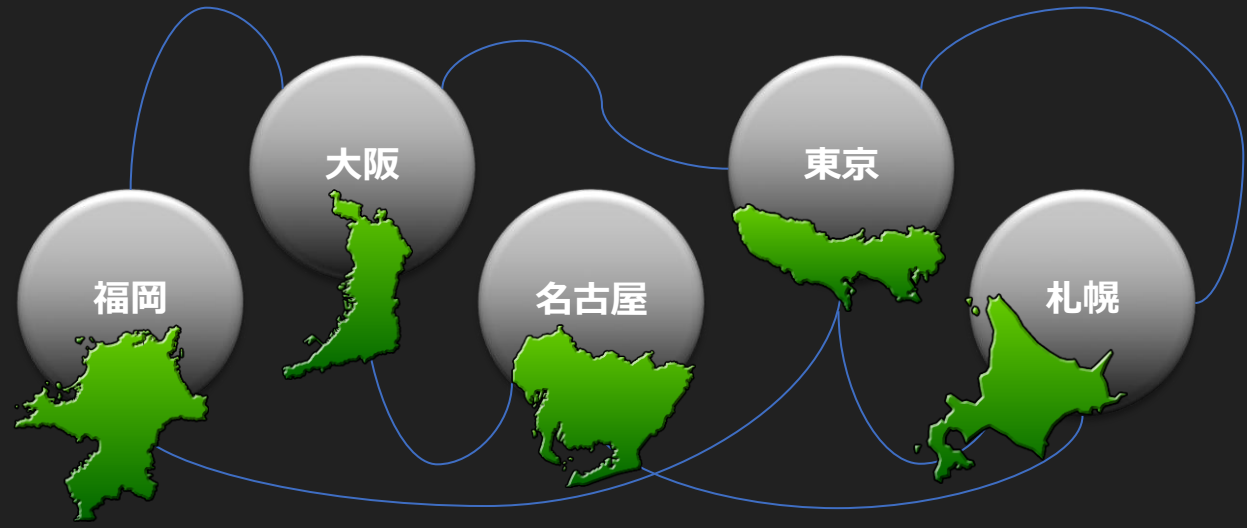
～ 講師陣が国内最高レベルのホワイトハッカー ～
ただ教えるだけじゃない！今困っていることに応えます！

取締役(教頭):横濱

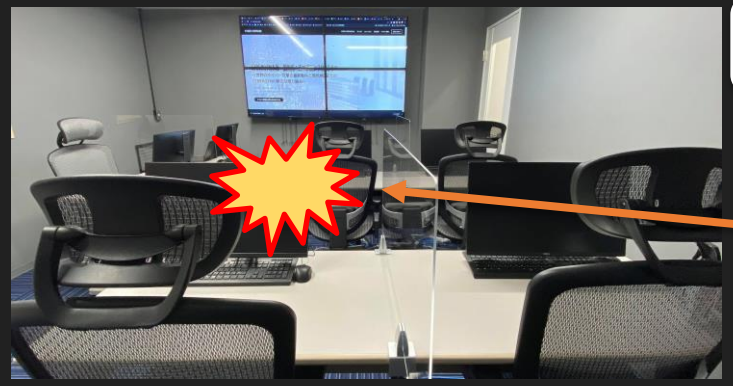
私個人は中国上海での起業経験を持ち、国際感覚、経営感覚もあります。インフラ、アプリ開発、セキュリティのエンジニアとして、20年以上のキャリアがあり、今現在も現役のテックリード、開発エンジニアとしてシステム開発を指揮しています。

アリーナに来ていただいた受講者の皆さんには、私達講師陣が現場での悩みや、技術的に突っ込んだ内容まで多種多様なご質問にお応えいたします。

～ 選べる教室 ～
主要都市に教室がある！便利に通える！



～ イスラエル軍仕込みのハッカーと実戦 ～
生身のハッカーが相手となる！本物の攻撃を体験できる！



イスラエルからのサイバー攻撃

～ ITだけではなくOTセキュリティも学べる ～
著名な制御系メーカーの実機を使って学べる！

Schneider Electric
Rockwell Automation
Allen-Bradley

～ 即戦力であることが到達点 ～
為になる話で終わらせない！実戦的なカリキュラム群！

標準トレーニング
CYBERGYM 実戦型カリキュラム

追加トレーニング
MITER ATT&CK 速習プログラム
QRadar SIEM 運用者育成プログラム
NOZOMI 運用者育成プログラム
社内規定などを含む個社別のプログラム
⋮
Appeared one after another

① 実戦型
② 即戦力メンバ育成 (OJT/OFF-JT)
③ ソリューション連動

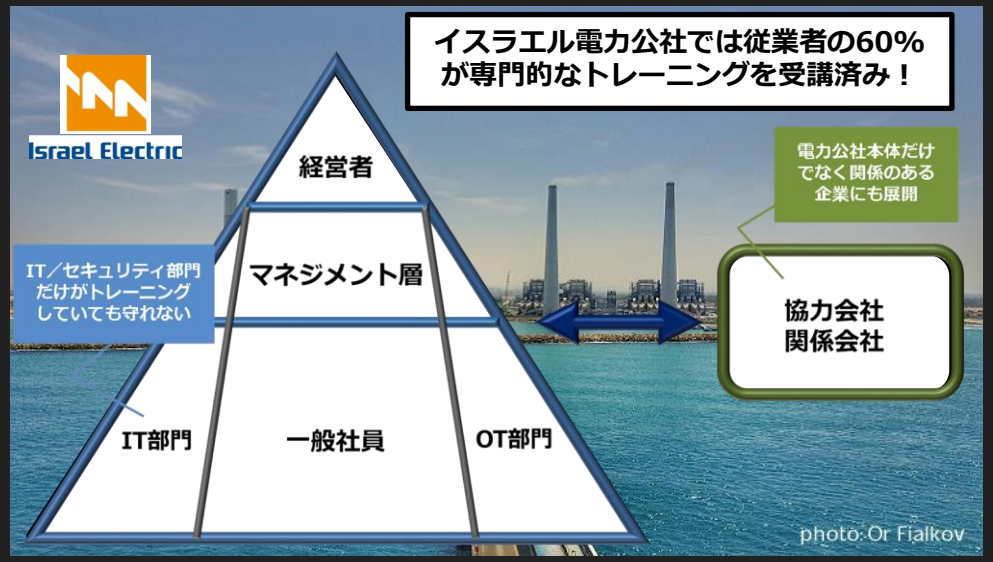
実戦型の即戦力人材

～ 人材開発助成金が使える ～
国からの助成金を活用して若手の育成をするチャンス！

大企業	中小企業
・経費助成： 費用の30%が対象上限10万円 ・賃金助成： 時給380円×訓練時間	・経費助成： 費用の45%が対象上限15万円 ・賃金助成： 時給760円×訓練時間

※事業所の雇用保険加入後5年を経過していない35才未満の労働者一人当たりに適用が可能、詳細は厚生労働省のホームページをご覧ください

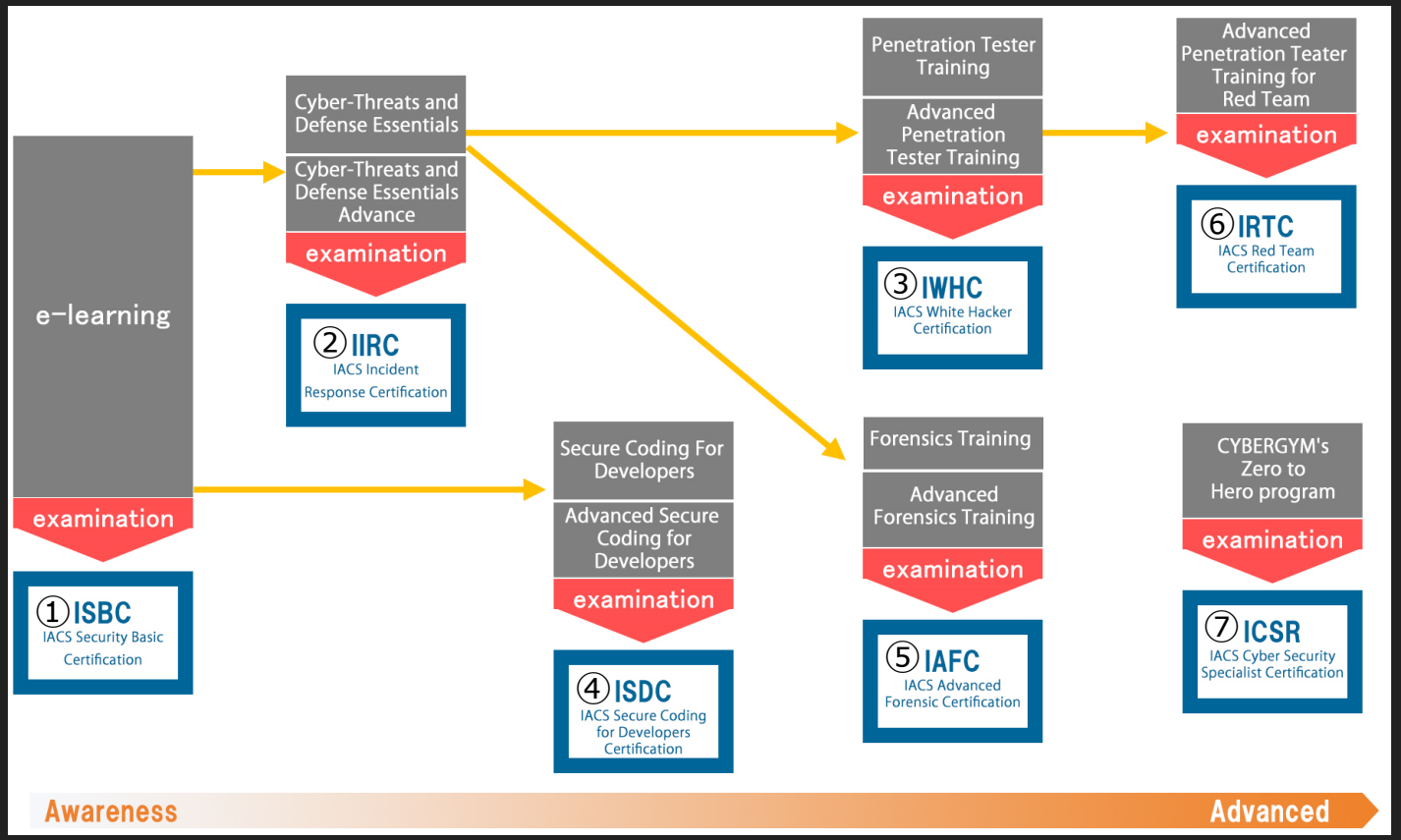
～ 全部門に対応するメニューが揃っている ～
経営層から一般社員まで！一丸で守る！



～ 国際認定資格とも連動 ～
第三者認定機関が対外的にスキルを証明！

弊社でご受講いただけるトレーニングは『国際サイバーセキュリティ協会(IACS)』が認定する資格認定制度の『認定推奨講座』でもあります。IACSが認定する資格は実戦に重きを置いた内容となっており、プラス・セキュリティ人材や、SOCやCSIRTとった実務担当者のスキルレベルを証明する認定資格になります。※高レベルな認定資格には『実技試験』が課せられます。

資格	必要能力・知識
①ISBC IACS Security Basic Certification	一般業務及び生活において必要なセキュリティの知識を有し自らリスクを回避する行動及び選択をすることができる。(CBT)
②IIRC IACS Incident Response Certification	サイバーインシデント発生時に組織内で必要な行動及び攻撃に対する応戦、専門的な解析・復旧を行うことができる。(CBT)
③IWHC IACS White Hacker Certification	ホワイトハッカーとしてサイバー攻撃を行い、相手の脆弱性を突くことができる。(CBT)
④ISDC IACS Secure Coding for Developers Certification	製品開発段階においてセキュリティ上の脆弱性を生まないための知識とコーディングを行うことができる。(実技試験あり)
⑤IAFC IACS Advanced Forensic Certification	サイバーインシデントに際して、高度な手法を用いた分析：鑑識を行い法的証拠を特定することができる。(実技試験あり)
⑥IRTC IACS Red Team Certification	極めて高いサイバー攻撃技術を有し、複雑な攻撃対象に対して高度な攻撃及び応戦を行うことができる。(実技試験あり)
⑦ICSR IACS Cyber Security Specialist Certification	サイバーセキュリティに関する基本的な知識と能力を網羅的に有しSOCやCSIRTメンバーとして活動することができる。(実技試験あり)



引用：IACS公式ホームページ

IACS
International Association of Cyber Security

サイバーセキュリティの脅威から企業と人を守る企業

CYBER COMMAND

サイバーコマンドの人的支援はここがすごい

～ 全員が有資格者で最前線のエンジニアでもある ～
規定を揃えて終わりじゃない！実際に戦う力を提供！

IRISS®

C|EH Certified Ethical Hacking

CISSP®

～ サイバー先進国イスラエルのノウハウを提供 ～
イスラエル国防軍出身のハッカーとも共闘！

～ 伴走型で個社別の状況を加味して支援 ～
単なる助言に留まらない！仕組み作りまでサポート！

～ セキュリティの専門人材を業務委託・派遣で提供 ～
即戦力人材が手に入る！既存部門の負荷も低減できる！

サイバー空間の傭兵部隊
それがサイバーコマンド！

サイバーセキュリティの脅威から企業と人を守る企業

CYBER COMMAND

サイバーコマンドのソリューションがすごい

～ インテリジェンスに強み ～
サイバー空間上に不審な動きが無いかを常にチェック！

弊社ホワイトハッカーがダークウェブを調査・監視

～ ラピッドスタートパッケージが使いやすい ～
一通りの対策がすぐにできる！悩まなくていい！

安価なのに内容は硬派

- 現状把握パッケージ
  - メール訓練
  - 脆弱性診断
- 簡易SOCパッケージ
  - EDR導入
  - 監視報告
- 相談窓口ホットライン
  - 平時相談
  - 緊急時対応

～ パートナー連携に強み～
IT･OT･IoT･DX一通りなんでも相談できる！

TRILOGY No.1 in Quality / Schneider Electric / AOS DATA / CP-SOL / CYBERGYM / DXHR / CYBER PROCESSMIND / IBM