情報セキュリティの基本を学ぶ
工場セキュリティの進め方

認定技術等情報漏えい防止措置認証機関
一般社団法人　情報セキュリティ関西研究所
代表理事　金森喜久男

金森略歴

松下電器産業株式会社（現パナソニック）入社
　営業　　同社　北陸支店　支店長
松下電送システム株式会社　常務取締役
　製品を企画し製造・販売・保守
松下電器産業株式会社
・パナソニック　システムソリューションズ社
　常務取締役
・情報セキュリティ本部　本部長　世界松下Gを統括
・内閣府・経産省　情報セキュリティ諮問委員会委員

『スポーツ界』
株式会社ガンバ大阪　代表取締役社長
スタジアム建設募金団体代表理事（全て寄付）
アジアフットボール協会（ＡＦＣ）委員
ＡＦＣ：プロフットボールクラブ委員会委員長

『学びの世界』
追手門学院大学　経営学部教授
一般社団法人
情報セキュリティ関西研究所　代表理事

日本政府認定：認証機関

2020年9月11日

「技術等情報漏えい防止措置認証機関」手交

認可省（5省）

財務省
厚生労働省
農林水産省
経済産業省
国土交通省
より認定

於：経産省

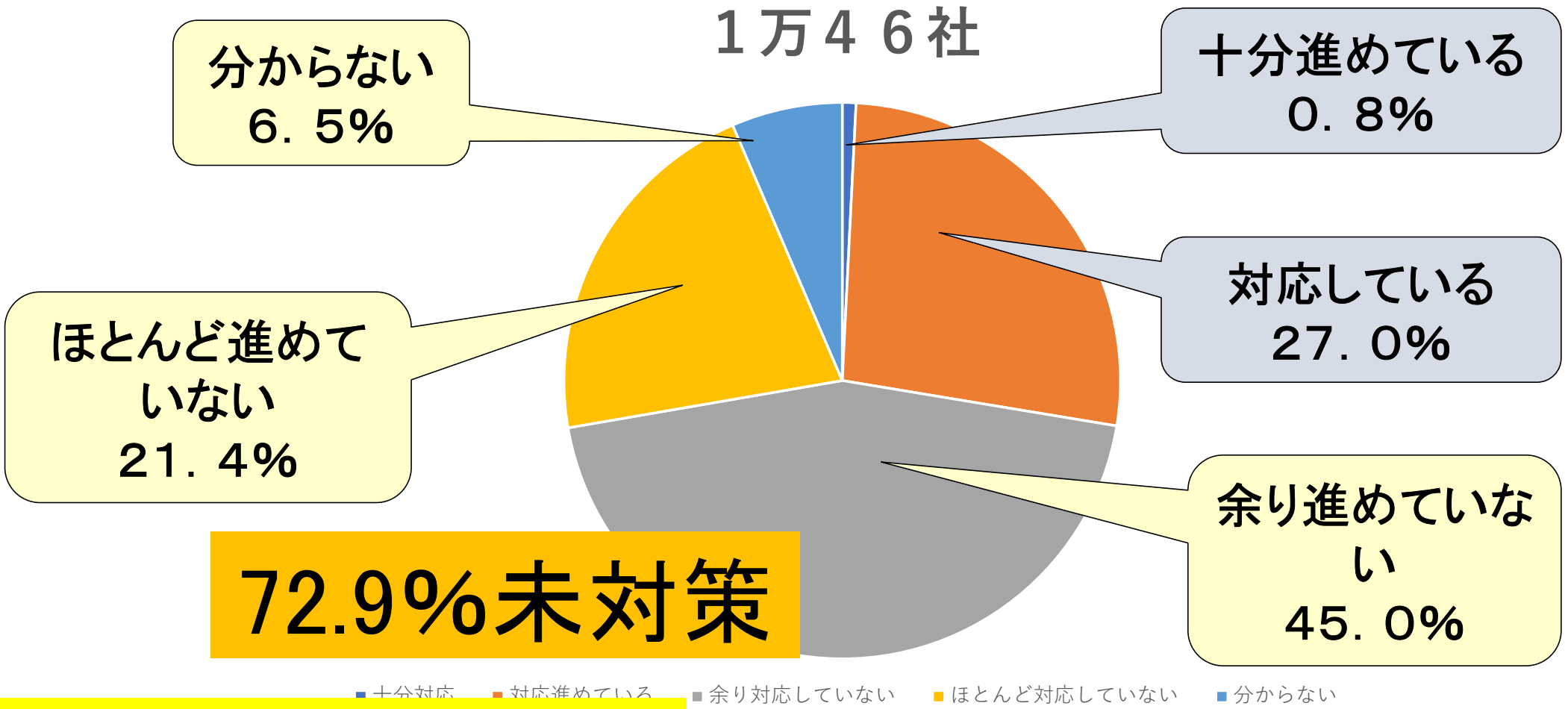
日本の技術を守り強化する

産業競争力強化法に基き

講義内容

・自己紹介
１．企業の受けとめ方：私の心配
２．変異する脅威！
３．情報セキュリティの進め方
４．情報資産整理でとん挫！
５．事故事例から観る日本企業の実態
６．日本政府の考え：産業競争力強化法

私の心配事：リスク（自然災害）対応状況



帝国データバンク2019．12．20発表

思いもかけない出来事が日常に！

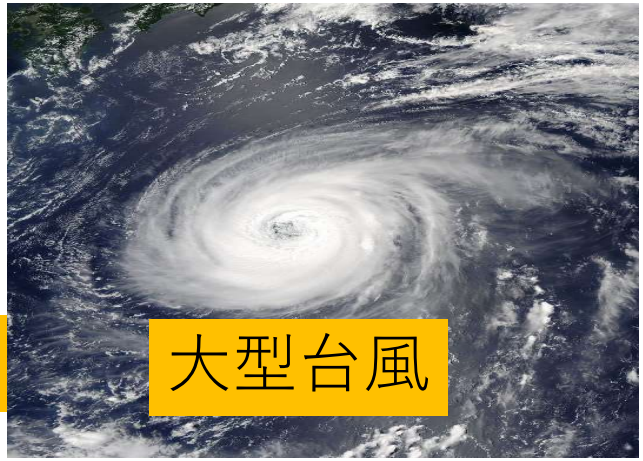

集中豪雨

コロナ


ITセキュリティ


豪雪


地震・津波


大型台風

リスクに鈍感≒チャンスにも鈍感

私の心配事　経営者アンケートで判ったこと

悪意ある第三者

７７％認識していない

営業秘密を持っている

幸之助創業者：夜泣きうどん屋を見習え

出汁、味、ゆで方、蒲鉾、ネギの切り方に工夫

人気がある店、ない店

うどん屋、店に特徴ある

それが技術やな！
大事にしなはれ！工夫しなはれ！

特異な技術・手法が必ずある

アンケートより：企業・職場問題が絶えない

問題：人手不足・多忙・儲からない・IT化

１．技術流出：金型・試作品・研究
社員退職、図面・PC盗難、データ

２．情報システム侵略・破壊
ウイルス、ハッキング、データ流出

３．得意先情報・個人情報等流出
引抜きによる情報流出

人的　IT　組織　物理

情報セキュリティの進め方は？

業種によって進め方は異なった

製造業

金融業

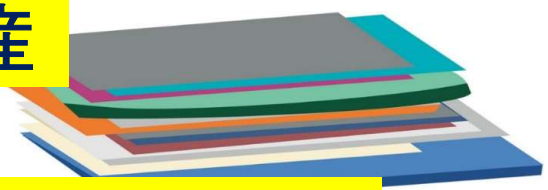
食品・農業・養殖業

情報資産が異質：技術情報・製造方法・個人情報
・遺伝子情報・栽培情報・・・・・

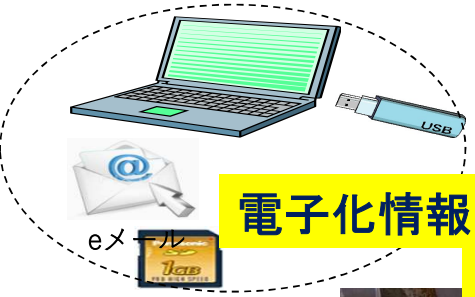
ITパーソナル化（DX）電子化によって変化

分散されていた脅威が増幅：致命的な脅威

情報資産



紙情報：図面・書類

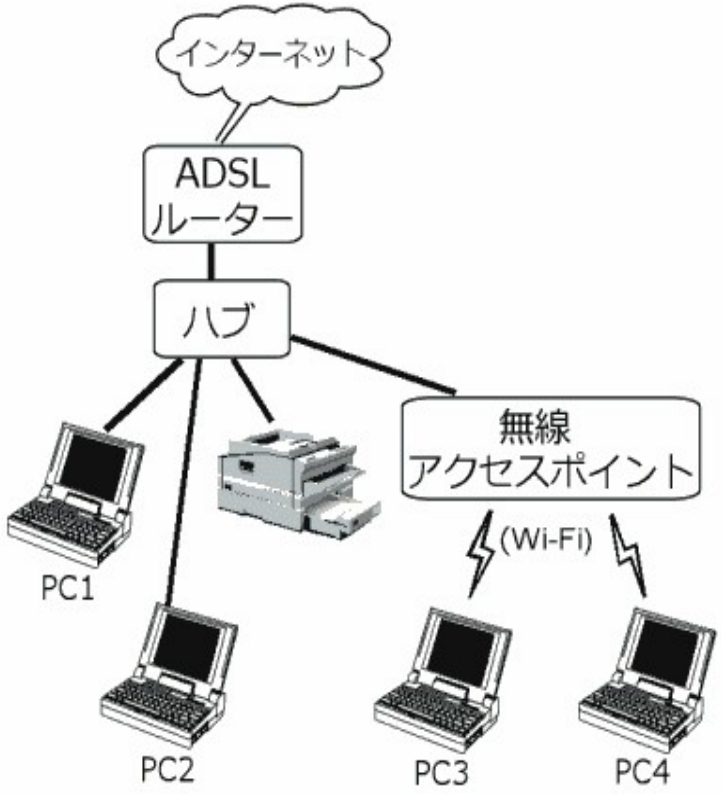


電子化情報

社員：頭の中の情報

試作品・金型・化体物

電子化情報



例えばあらゆる製造業のEC化：直結

卸売業者

消費者

EC：アマゾン・楽天

製造業

自らＥＣ事業化（消費者とダイレクトに）

何故できたか！新たな脅威の発生

物流システム進化

情報通信のデジタル化

ITパーソナル化：DX

新たな産業が創出：未だ赤ん坊‼

新たな脅威・リテラシー（使いこなす能力）
・サイバー攻撃・製造方法の変化・・・

サイバー攻撃は狡猾であり進化

マルウエア（malware）

悪意あるソフトウェアの総称（ダメージ与える）

・エモテット（emotet）

なりすましメールアドレスで侵入

・ランサムウェア（ransomware）

コンピューターに感染し制限・乗っ取り・身代金

NWに繋がる機器全てに脅威：中小企業も標的に

現在の脅威に対し製造業での対策

人的に

ＩＴ分野で

物理的に

組織的に

気づかない漏洩：発覚した事件

新日鐵住金

企業秘密盗難

posco

韓国製鉄企業

新日鉄技術：方向性電磁鋼板の製造方法盗んだ賠償

３００億円で和解
2016.9.30　報道

気づかない漏洩：これが日本の実態

発覚した理由
・ポスコの社員が中国企業に売り渡す
・ポスコが社員を「営業秘密」違反で提訴

気づく仕組み

・ポスコ社員は裁判でポスコの技術でなく
新日鉄住金技術であり盗んだことにならない

この裁判
無罪

え！
盗まれて
いたの！

新日鉄住金

気づかない企業

重点対策：情報資産管理の仕方

情報資産（Information　Asset）とは
- 企業にとって有為な情報
- 外部流出すると企業に損失を与える情報
- 損失（影響）の大きさによって機密区分を実施

- 情報セキュリティ実施していない企業は得意先から信頼置かれない
- 情報を秘守管理していないと裁判では勝てない

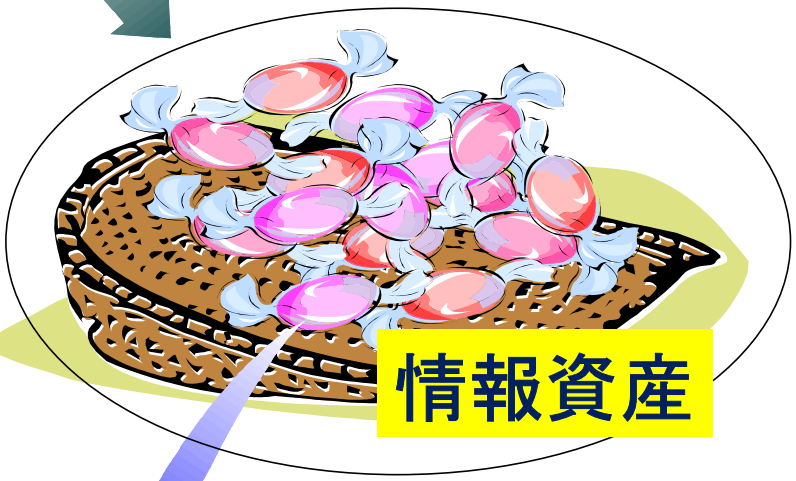
「盗られたら」判る仕組みを作る

インシデント（incident）の対応を決めておく

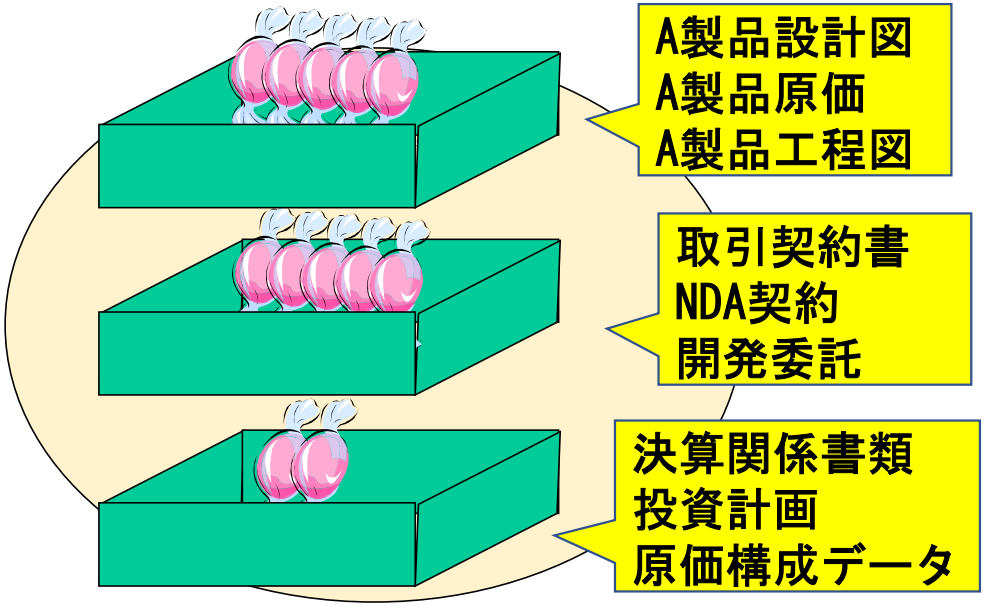
資産整理する意義はどこにあるか！

情報資産の整理が
情報セキュリティの第一歩

紛れ込んでも判らない！
コンタミ



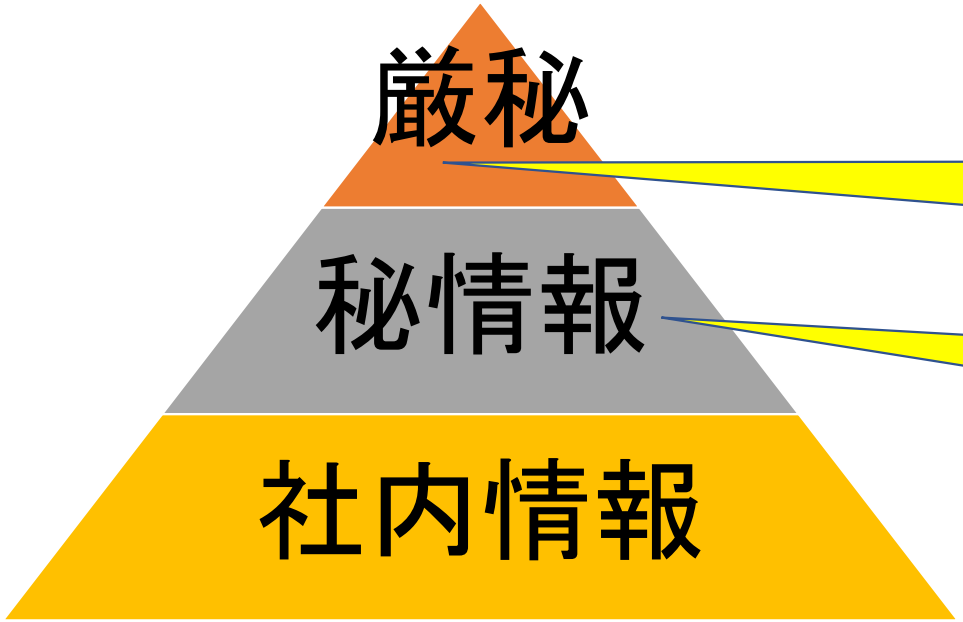
取られても判らない！



増えたり減ったりすれば
すぐ判る！！！

情報資産管理の仕方；機密区分

情報資産（Information　Asset）とは
・企業にとって有為な情報
・外部流出すると企業に損失を与える情報
・損失（影響）の大きさによって機密区分を実施



発表前決算情報（上場企業）
重要技術・製造情報
得意先契約情報etc

事業計画、工場建設計画、
技術情報、人事情報、
販売計画etc

情報オーナーが機密区分実施

情報資産管理の仕方

情報資産管理ができていないため起こること

盗まれても気づかない

無駄が多い　競業避止が全社員になっている

規則が曖昧　立入制限区域の設定に矛盾

ストレス増幅　部門によって規則が異なる

メリハリが無い　仕事と余暇の線引きをどこに置く

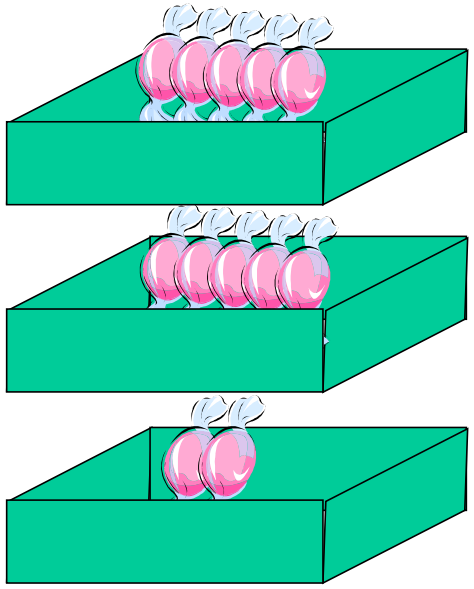
社員の誇り希薄　自社の誇りの裏付けとなる

うまくいかない情報資産管理

情報資産管理が進まなかった理由

１．目的・意義が理解されていない	働きやすい職場造り
２．誰のために実施するのか曖昧	顧客・従業員全員の為
３．情報資産管理の仕方めんどう	その通りです
４．時間がかかる	良い職場造り：我慢
５．だれの責任で実施するのか	社長・管理職の責任で
６．上司が熱心でない	その上の上司に報告
７．機密区分と連動していない	機密区分考え再整理
８．その他	

資産の整理：断捨離は総コスト下げ見える化



ソフトバンク、楽天モバイルを提訴

転籍

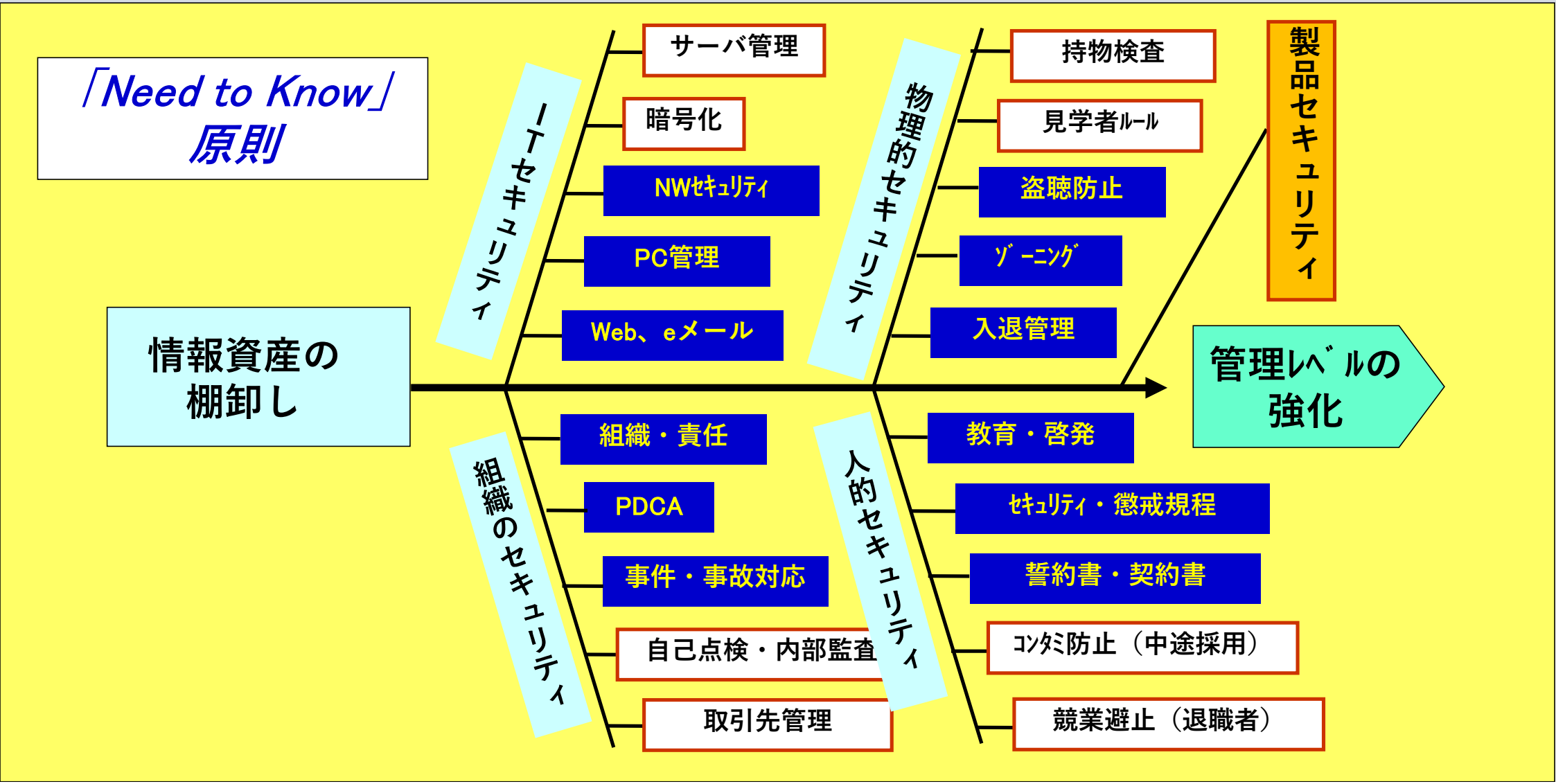
Rakuten Mobile Network

・損害賠償１０億円
・損害賠償請求１０００億円
・訴訟は大変な労力だが
・甘い企業は狙われる：詐欺・盗難何度も

SBがとった対策

・情報資産管理の再強化（管理ポリシーの厳格化、棚卸しとアクセス権限の見直し）
・退職予定者の業務用情報端末によるアクセス権限の停止や利用の制限の強化
・全役員と全社員向けのセキュリティー研修（未受講者は情報資産へのアクセス不可）
・業務用OA端末の利用ログ全般を監視するシステムの導入

全企業単位で取組む活動



何から始めるか！

インシデント対策

事故の把握

企業活動に定着させる

社長含め全員実施

従業員への教育実施

企業内ルール整備

情報資産の整理

就業規則の見直し

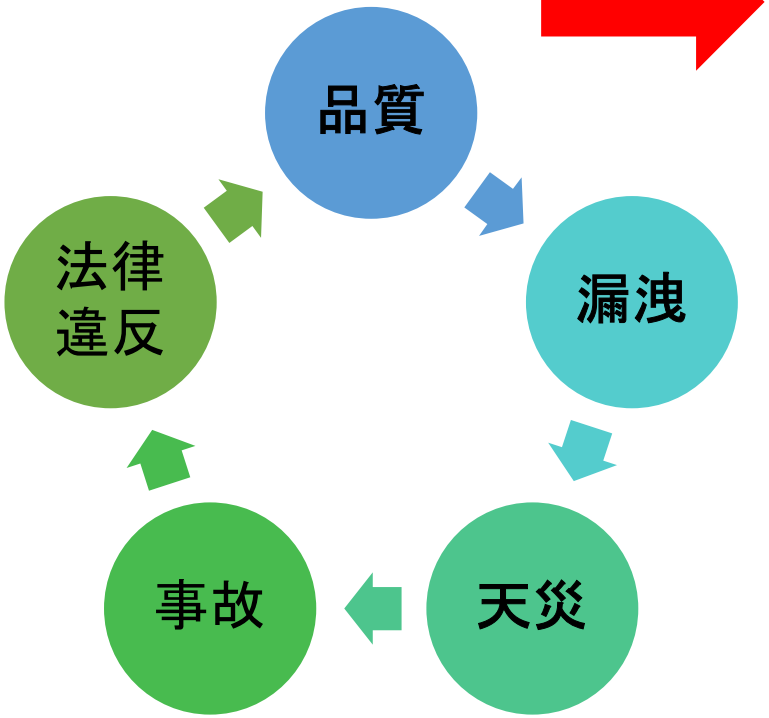
情報セキュリティ方針作成

企業の状態を知る

アセスメント実施

上手くいかないリスクマネジメント

企業を守る：この考えでは　**限界**



顧客を守る
顧客の為に
社会の為に

顧客の創造

働く人間は正義を欲している

専門家派遣事業で

アセスメント実施

半日審査
相談時間
報告書
問題・課題
明らかに

国家予算・無料

情報管理強化により企業様に明日を提供します

お勧めします!!
製造業・IoT・サービス業の皆さま

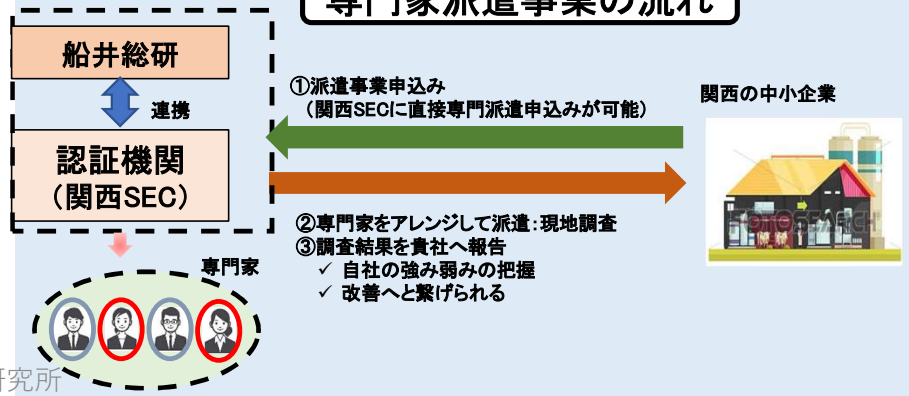
技術等情報管理認証制度における

国が支援する 専門家派遣事業

専門家派遣事業のメリット

1. 技術管理の専門家が自社の技術管理を実地精査します。
2. 自社の現状を把握し、技術管理の課題が明確になります。
3. 課題への対策により、技術情報の管理強化が図れます。
4. 技術情報漏えいがなくなり、企業競争力が増します。
5. 新規技術開発も、安心して推進できます。
6. 費用は国の負担、企業からの持ち出しはありません。

専門家派遣事業の流れ



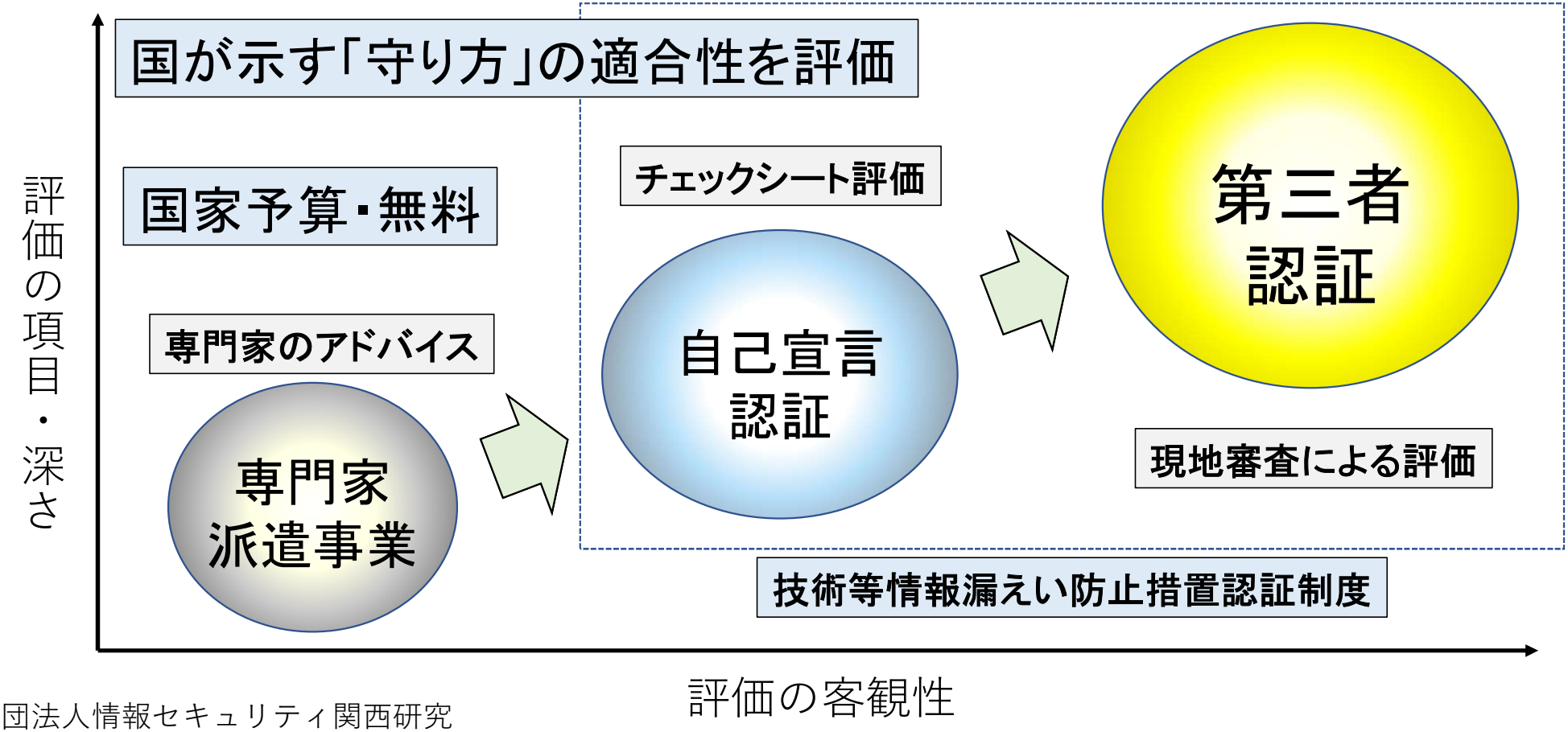
一般社団法人 情報セキュリティ関西研究所（略称：関西SEC）

専門家派遣事業とは？（1）

1. 産業競争力強化法により、技術情報漏えい防止のための制度「技術等情報漏えい防止措置認証制度」が設立（平成30年9月）
2. 本制度は、国が示す「情報の守り方」に対する適合状況を国が認証する制度
3. 認証取得を支援するための「専門家派遣事業」がスタート
   ① 情報管理に関する具体的なアドバイス
   ② 認証取得のための内部監査
4. 支援に掛かる費用は国が負担

専門家派遣事業とは？（2）

「技術等情報漏えい防止措置認証制度」を補完する制度



専門家派遣事業とは？(3)

情報管理の専門家が情報管理に関するアドバイスを実施

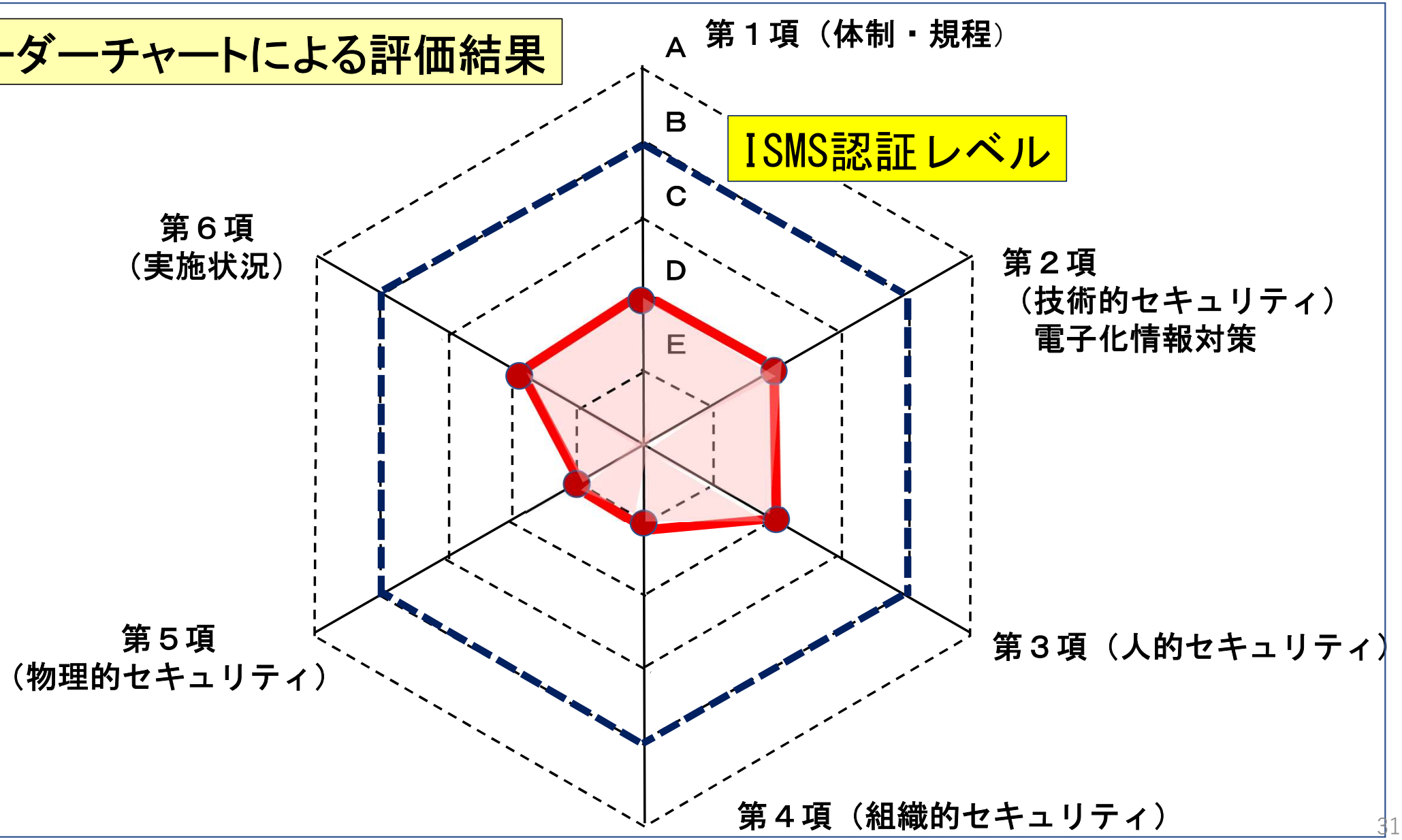
専門家派遣事業の実施方法

関西SECだけのサービス

○○企業(法人) 技術・総務・営業	→	情報管理の 課題明確化	→	○○企業の 推進方法が見える化
↑ 情報管理のヒアリング		↑ 課題形成		↑ IT化支援

専門家派遣事業(情報セキュリティ関西研究所)

レーダーチャートによる評価結果



アセスメント調査による総合評価

総合評価	補足事項
D⁻	情報セキュリティ委員会が未設置で情報管理に関するガバナンス力を発揮できない状況で、PDCAマネジメントシステムも構築できず、管理策の策定・定着化が進まない状況となっている。またサーバー室に脆弱性があり、データ管理にも課題を有している。今後、事務局を設置し体制構築や規定化を進められ、情報セキュリティを強化されることを期待したい。

総合評価　A　：　リスク評価に基づいた管理策が実施され、マネジメントシステムが確立されている状態（ISMS認証レベル）
B　：　特定の情報に対するリスク評価が行われ、マネジメントシステムが運用されている状態
C　：　管理策が実施され、マネジメントシステムが部分的に運用されている状態
D　：　一部の管理策は実施されているが、情報セキュリティ事故発生の可能性が高い状態
E　：　管理策が未構築で、情報セキュリティ事故が日常的に発生し、またそれが分からない状態

なお、評価記号に続いて「＋」（より高い）、あるいは「－」（より低い）の符号を付加することもある

情報セキュリティアセスメントのレーダーチャート評価基準

レベル	定　義	備　考
A	・調査対象とする評価項目が、全て適合している ・情報の「CIA」が確保されている状況	・全社的な取組みを実施しており、ISMS認証取得のレベルにある
B	・調査対象とする評価項目が、ほぼ全て適合している ・全社的にPDCAが運用され、実効性が認められる状況	・評価項目はほぼ適合しているが、一部に不適合がある
C	・重要な評価項目が、適合している ・PDCAが運用され、レベルアップが図られている状況	・取組みは全社的ではなく、各組織単位で実施されている
D	・重要な評価項目について、軽微な不適合がある ・情報セキュリティ事故の発生を発見できない状況	・体制や規程等、全社的取組みに不適合が見られる
E	・多くの評価項目について、重大な不適合がある ・情報セキュリティ事故が発生している状況	・各組織単位でもISMSの取組みが実施されておらず、事故の発生も発見できない状況

情報セキュリティアセスメント調査結果（1）

評価分類	適合内容	不適合内容	判定レベル
1．体制･規程情報	・CPO選定・ﾌﾟﾗｲﾊﾞｼｰﾎﾟﾘｼｰあり ・推進体制はある（運用は今後） ・情報一覧表を作成済み	・CISO・全社推進体制・関連全社規定が未選定・未設置 ・秘情報と社内情報が未分類 ・配送品個人情報(10万人)をPC管理(SCM本部)	D
2．技術的セキュリティ	・PCは会社貸与、アンチウイルスソフトをインストールしている ・個人情報はサーバー保管 ・Shopifyはクラウド保管 ・携帯電話は会社貸与(一部)	・PC管理(PW・盗難防止)のﾙｰﾙは未設定 ・PC・スマホ等の運用ルールがない ・私用USB･SDｶｰﾄﾞの持ち込みは可 ・サーバー室・サーバーの管理強化	D
3．人的セキュリティ	・入社時誓約書は取得済み ・朝会時に教育を実施	・入社時誓約書はセキュリティに特化 ・退社時、競業避止誓約者を未取得 ・委託先従業員への未教育 ・全従業員教育と確認テストが未実施	D

情報セキュリティアセスメント調査結果（2）

評価分類	適合内容	不適合内容	判定レベル
4．組織的セキュリティ	・個人情報の内部監査を実施 ・委託先と機密保持契約を締結（一部の委託先）	・PDCA（推進計画・実施・内部点検・ﾏﾈｼﾞﾒﾝﾄﾚﾋﾞｭｰ）が未実施 ・委託先監査は未実施 ・事故発生時の手順がない	E
5．物理的セキュリティ	・敷地と外部を遮断する塀を設置 ・本社事務所は社員カードでドアの開錠を管理（個人認証はしていない）	・情報区分に応じたゾーン区分はない ・従業員の移動制限はない ・入退室のログは取得していない ・非常階段からの侵入が可能	E
6．各部署での実施状況	・離籍時･退社時、個人情報は施錠保管している ・不要紙情報はシュレッダで処理	・貸与PCの使用ルール（私的利用・情報の保存・HPの閲覧・持出し）がない ・ソフト更新は必ずしもできていない ・PCを机上に置いたまま帰宅	D

アセスメント調査結果：総合所見①

１．情報セキュリティガバナンス

- 個人情報保護方針はあるが関連規程類の整備、情報セキュリティ推進体制の設置等、**情報セキュリティガバナンス**は構築されていない。
- また、情報セキュリティガバナンスが構築されていないため、PC利用・管理等に関するルール化ができず、規定化も進んでいない。
- さらに、PDCAマネジメントシステムも構築されない状況となっている。
- 早急に、経営トップをCISO（最高情報セキュリティ責任者）とし、各本部の責任者を委員とする**全社の情報セキュリティ推進体制を構築**し、各種管理規程の制定やPDCAマネジメントシステムの構築を図ることが望まれる。

情報セキュリティ相談内容傾向：マルウエア以外

EC立ち上げたがリスク心配

自動車産業の情報セキュリティ新基準対応：SCM
EUA（VDA）・JAMA・AAMの審査基準

自社技術情報、中国ネット上で売りに出されている

Baidu 文库

WEB上での売買サイト

何時でもご相談ください

お待ちしています

ご清聴ありがとうございました

認定技術等情報漏えい防止措置認証機関
一般社団法人　情報セキュリティ関西研究所

kanamori@kansaisec.com