経営層を納得させる「セキュリティ予算」獲得術

Secure SketCH

ＮＲＩセキュアテクノロジーズ株式会社

Ver1.3 更新日 2024/1/26

目次

はじめに

背景

毎年秋～冬にかけて、来年度のセキュリティ予算獲得に向けて、
施策を練っている企業様も多いのではないでしょうか。

課題

情報セキュリティ・サイバーセキュリティへの投資は、企業の売上に直結しないことから、経営層の方には効果が見えづらく、セキュリティ予算取りを調整・上申する際に、**どのように説明すればよいか悩んでいる**セキュリティ担当者の方が多くいらっしゃるのも事実です。

情報・事例

そこで本資料では、セキュリティ予算の獲得に関して経営層と対話するための
「**ポイント**」と「**具体的な予算取りの流れ**」を解説します。

Secure SketCH

目次

昨今のセキュリティインシデント傾向

ランサムウェア・サプライチェーン攻撃の急増

2020年4月の緊急事態宣言から急速に進んだテレワーク導入、2021年以後に顕著になった日系企業の海外拠点を狙うランサムウェア被害の頻発、サプライチェーンの脆弱な拠点を狙ったサイバー攻撃など、昨今ますますセキュリティ脅威が多様化・複雑化しています。

順位	「組織」向け脅威	初選出年	前年順位
1	**ランサムウェアによる被害**	**2016年**	**1**
2	**サプライチェーンの弱点を悪用した攻撃**	**2019年**	**2**
3	内部不正による情報漏えい等の被害	2016年	4
4	標的型攻撃による機密情報の窃取	2016年	3
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	6
6	不注意による情報漏えい等の被害	2016年	9
7	脆弱性対策情報の公開に伴う悪用増加	2016年	8
8	ビジネスメール詐欺による金銭被害	2018年	7
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	5
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	10

IPAの「情報セキュリティ10大脅威 2024」でも
「ランサムウェアによる被害」が

4年連続1位に

「サプライチェーンの弱点を悪用した攻撃による被害」が

2年連続2位に

出所：IPA「情報セキュリティ10大脅威2024」を基にNRIセキュアにて作成
https://www.ipa.go.jp/security/10threats/10threats2024.html

Secure SketCH

昨今のセキュリティインシデント傾向

大企業だけでなく、中小企業の被害も増加

ランサムウェアについては大企業の被害が目立っていますが、経済産業省が注意喚起しているように中小企業も被害を受けており、現在はどんな企業でもランサムウェア被害を受ける可能性があると考えておくべきです。そして、ランサムウェアは企業ネットワーク広範囲に渡るため、業務・サービス停止につながる恐れがあることから、事業継続における課題と捉えることをお勧めします。

（1）中小企業を巻き込んだサプライチェーン上での攻撃パターンの急激な拡がり

昨今、中小企業を含む取引先や海外展開を進める企業の海外拠点、さらには新型コロナウイルスの感染拡大に伴うテレワークの増加に起因する隙など、攻撃者が利用するサプライチェーン上の「攻撃起点」がますます拡大しています。

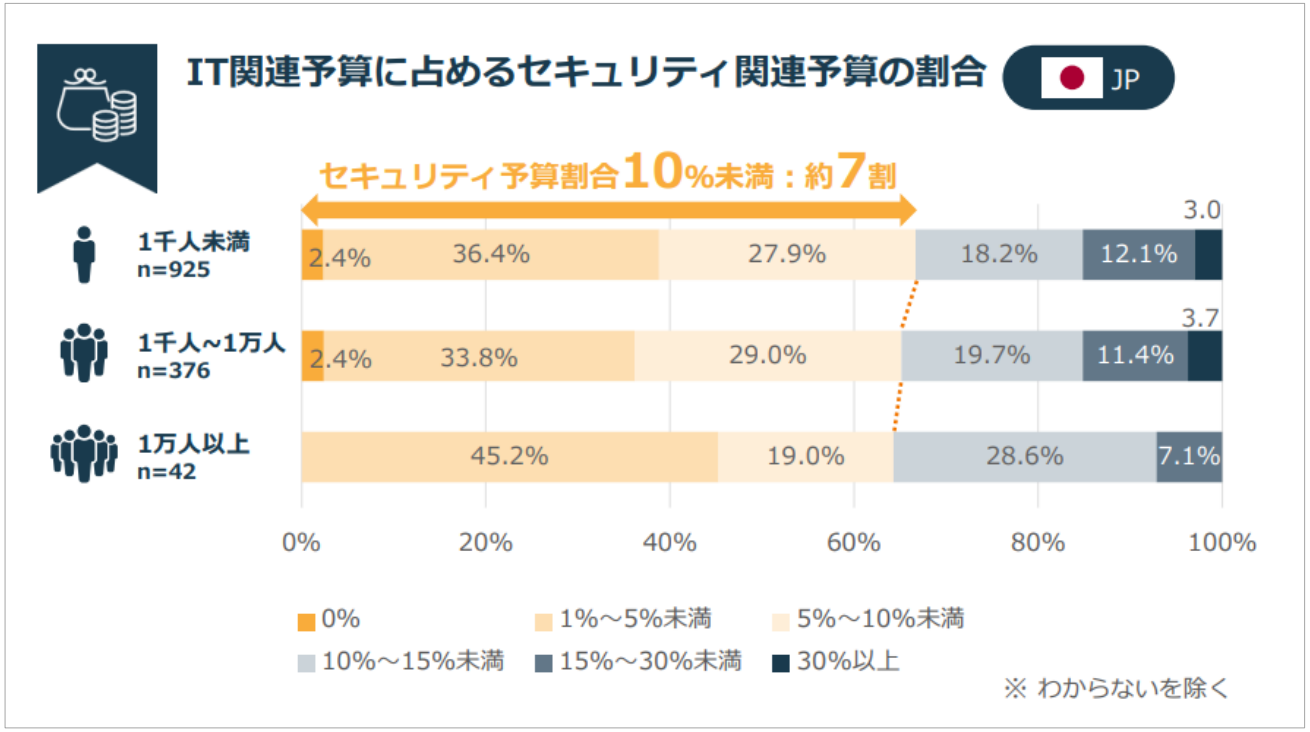
（2）大企業・中小企業等を問わないランサムウェアによる被害の急増

暗号化したデータを復旧するための身代金の要求に加えて、暗号化する前にあらかじめデータを窃取しておき、身代金を支払わなければデータを公開するなどと脅迫する、いわゆる「二重の脅迫」を行うランサムウェアの被害が国内でも急増しつつあります。
背景には、攻撃者の側でランサムウェアの提供や身代金の回収を組織的に行うエコシステムが成立し、高度な技術を持たなくても簡単に攻撃を行えるようになっていることがあります。

参考：経済産業省「最近のサイバー攻撃の状況を踏まえ、経営者の皆様へサイバーセキュリティの取組の強化に関する注意喚起を行います」
https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

日本企業の約７割は、IT予算に占めるセキュリティ予算の割合が10%未満で、海外と比較して少ない

企業における情報セキュリティ実態調査2022のレポートからもわかるように、日本の約７割がIT関連予算に占めるセキュリティ予算が10%未満であり、日本のセキュリティ予算は海外（米国・豪州）と比較して相対的に少なく、この傾向は過去数年間変わりがありません。



参考：NRIセキュアテクノロジーズ「NRI Secure Insight 2022～企業における情報セキュリティ実態調査～」
https://www.nri-secure.co.jp/download/insight2022-report

Secure SketCH

目次

なぜ、日本企業のセキュリティ予算は「少ない」「増加しない」のか？

経営層の視点で捉えると、以下3つの理由があると考えられます。

現場担当者

「自社の現状課題」や「最近のインシデントニュース」をもとに、予算・施策案を作成

予算申請

経営層

【理由１】セキュリティ＝「コスト」という経営者の意識

セキュリティ施策は売上に直結しないがゆえ、コストととらえる経営層が一定数いることは事実です。
あらゆる経営者の関心事は売上・利益を高めることにあるため、コストを最小限に留めようという力が働くのは道理です。

【理由２】専門用語が難しい・必要性が判断できない

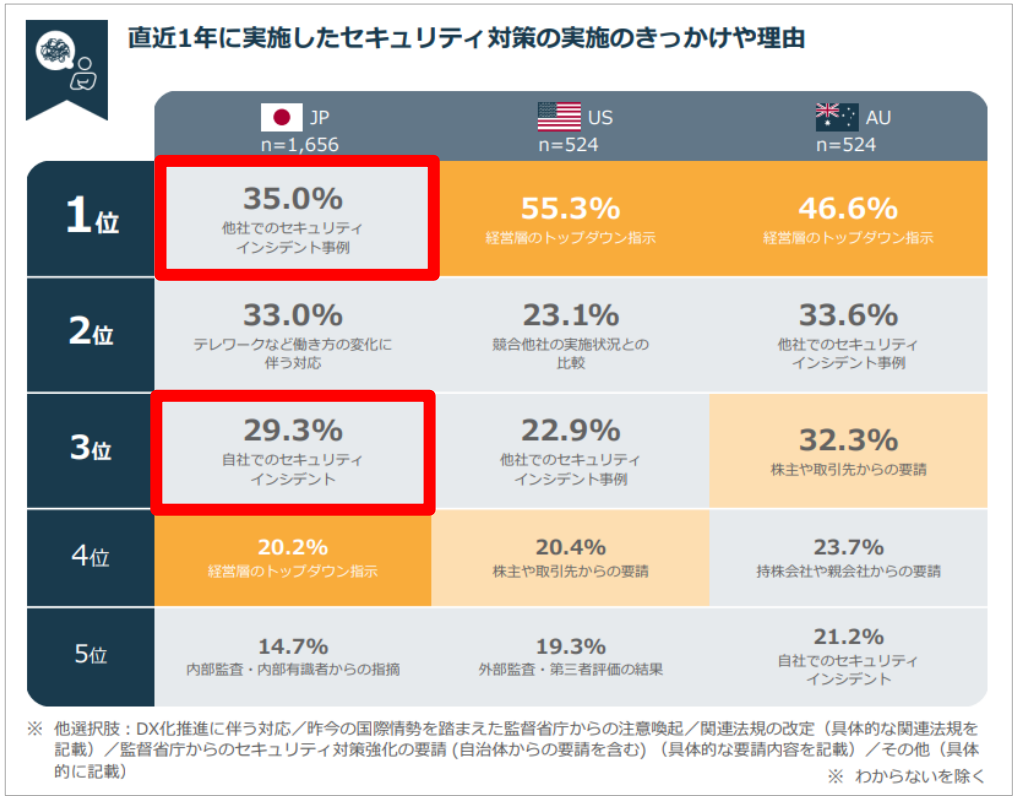
情報セキュリティ、サイバーセキュリティは専門用語も非常に多く、複雑であるため、経営者が実態やインパクトを理解できないため、
「この施策には、どのくらい意味があるのか」といった投資額の妥当性を判断する要素・材料が少ない。

【理由３】自社で大きなセキュリティインシデントが発生していない

残念ながら、一定数の経営層には未だに「自社に限ってインシデントは発生しない」「ウチ（自社）には攻撃者に狙われるような重要情報はない」
「むしろ予算削減の対象ではないか」と感覚的に自己評価するケースも多くみられます。

投資のきっかけは、他社・自社でのインシデントが起因

日本のセキュリティ対策実施のきっかけや理由の上位が「他社でのセキュリティインシデント事例」「自社でのセキュリティインシデント」という結果からも、企業が大きなインシデントをうけない限り、セキュリティ投資の理解・後押しを得るのは難しく、セキュリティインシデント発生後にリアクティブにセキュリティ投資が行われているという残念な状況がわかります。



直近1年に実施したセキュリティ対策の実施のきっかけや理由

	JP n=1,656	US n=524	AU n=524
1位	35.0% 他社でのセキュリティインシデント事例	55.3% 経営層のトップダウン指示	46.6% 経営層のトップダウン指示
2位	33.0% テレワークなど働き方の変化に伴う対応	23.1% 競合他社の実施状況との比較	33.6% 他社でのセキュリティインシデント事例
3位	29.3% 自社でのセキュリティインシデント	22.9% 他社でのセキュリティインシデント事例	32.3% 株主や取引先からの要請
4位	20.2% 経営層のトップダウン指示	20.4% 株主や取引先からの要請	23.7% 持株会社や親会社からの要請
5位	14.7% 内部監査・内部有識者からの指摘	19.3% 外部監査・第三者評価の結果	21.2% 自社でのセキュリティインシデント

※ 他選択肢：DX化推進に伴う対応／昨今の国際情勢を踏まえた監督省庁からの注意喚起／関連法規の改定（具体的な関連法規を記載）／監督省庁からのセキュリティ対策強化の要請（自治体からの要請を含む）（具体的な要請内容を記載）／その他（具体的に記載）

※ わからないを除く

参考：NRIセキュアテクノロジーズ「NRI Secure Insight 2022～企業における情報セキュリティ実態調査～」
https://www.nri-secure.co.jp/download/insight2022-report

Secure SketCH

セキュリティ予算を獲得するポイントは、自分事 × 経営視点に尽きる

ポイントは、経営者に

「**自分事**としてとらえてもらえるか」

そのためには、コミュニケーションに

「**経営視点**」を取り入れることが重要

セキュリティ予算獲得に必要な4つのポイント

経営層を巻き込むポイントは、「自分事として捉えてもらう」「経営視点で訴求する」こと

セキュリティの現場担当者が持つ高度な知識・技術的な内容・根拠を前面に出すよりも、相手が興味を持つ・理解できる内容をベースに**「経営視点」で訴求すること**が最も重要です。具体的なポイントは以下4つです。

Point. 1

経営層が気にする同業他社を
引き合いにした説明をする

Point. 2

対策の必要性を
権威付けをして訴える

Point. 3

自社起因で発生したインシデントの
影響が委託元やグループ全体に波及
する可能性を伝える

Point. 4

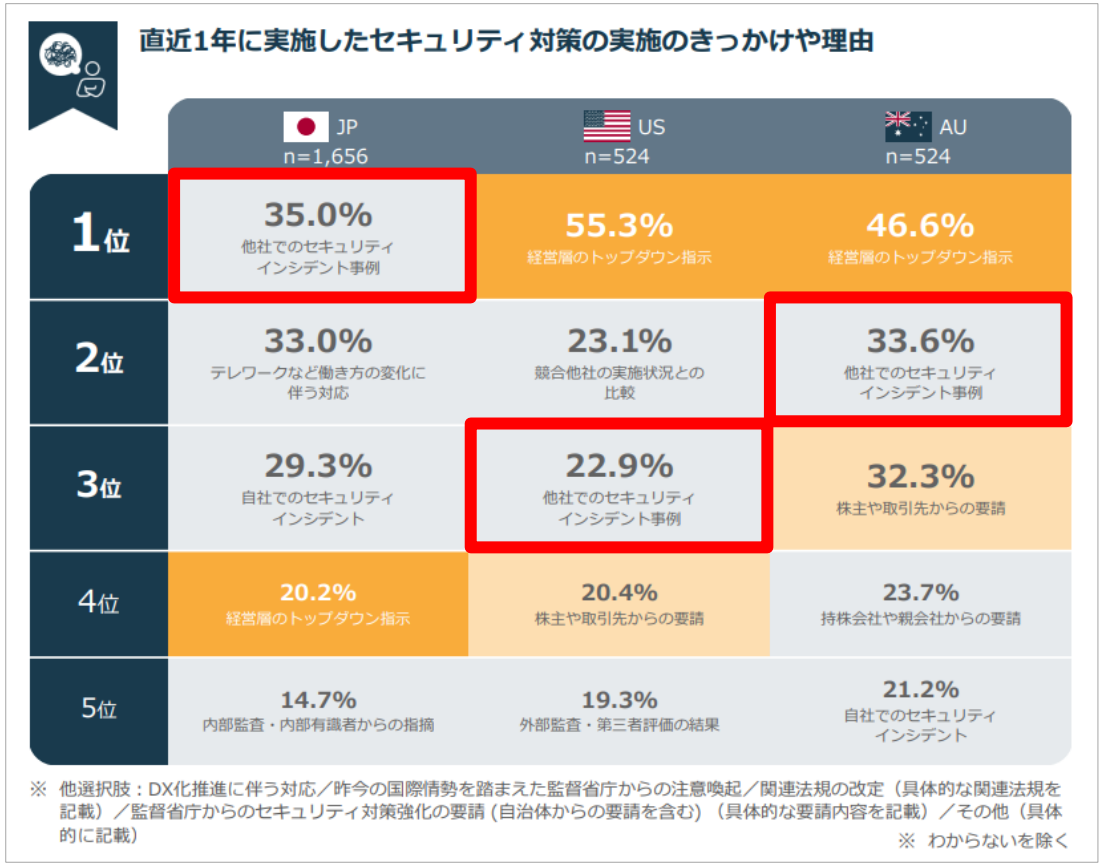
セキュリティ対策の必要性を複数の
視点で伝えて対応優先度を高めてもらう

Secure SketCH

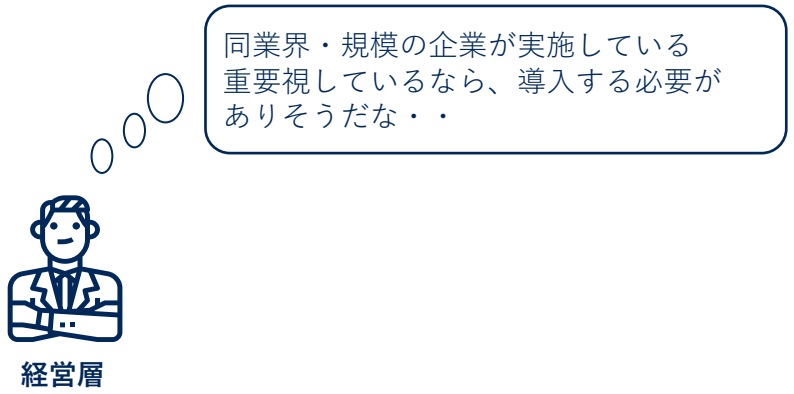
Point

1 経営層が気にする同業他社を引き合いにした説明をする

経営層の多くは、同業他社の動向や社会のトレンドが気になりますので、同業他社を引合いにした説明を行うと、経営者の理解・後押しを得られる可能性が高まります。日本企業のセキュリティ実施のきっかけの第１位には「他社でのセキュリティインシデント事例」がランクインしており、セキュリティ予算が日本よりも高い傾向にある海外でも上位にランクインしています。



同業他社の
「セキュリティインシデントの情報（迫りうる脅威）」
「セキュリティ対策の情報（脅威に対するリスク管理策）」
という因果関係を併せて提示することで、
経営層がセキュリティ予算の必要性を理解しやすくなる。



参考：NRIセキュアテクノロジーズ「NRI Secure Insight 2022～企業における情報セキュリティ実態調査～」
https://www.nri-secure.co.jp/download/insight2022-report

Secure SketCH

Point

2 セキュリティ対策の必要性を権威づけしながら訴求する

企業のセキュリティ担当者が、高度な知識・経験やリスク分析結果を踏まえた上で、セキュリティ予算を申請した場合でも「それは担当者による主観的な判断では？」という疑問・質問を受けるケースがあります。 このようなケースにおいては、セキュリティ対策の必要性を権威づけすることが重要であり、「**セキュリティガイドライン**をベースにセキュリティ対策を選定したことを訴求」「**外部専門家（第三者）**による見解を活かして訴求」2つの観点での訴求が有効です。

ガイドラインによる評価結果	外部専門家の意見
・ISO/IEC 27001/2 ・サイバーセキュリティ経営ガイドライン ・NIST CSF ・NIST SP 800-171 ・CMMC ・CIS Controls V8 ・FISC 安全対策基準　　等	

今後のグローバル展開に向け、
海外基準に合わせていくのは
経営戦略的にも意味があるな・・・

経営層

専門家目線でも必要であるなら
対応すべきか・・・

Secure SketCH

Point 3

自社のインシデント影響が委託元やグループ全体に波及する可能性を伝える

昨今では、特にサプライチェーン攻撃の被害が頻発しています。そのため、企業にはサプライチェーン観点のセキュリティ対策の整備や見直しが求められています。IPAの10大脅威でも6年連続でランクインし、サイバーセキュリティ経営ガイドラインやNISTサイバーセキュリティフレームワーク（NIST CSF）など、様々なセキュリティガイドラインでも、サプライチェーン関連の項目が強化されています。

IPA
情報セキュリティ
10大脅威2024

サプライチェーン
攻撃が6年連続で
ランクイン
（組織編2位）

サイバーセキュリティ
経営ガイドラインv3.0

サプライチェーン全体での
セキュリティ対策を
強く推奨

NIST
サイバーセキュリティ
フレームワーク

Ver.1.1へ改訂時、
サプライチェーンリスク
マネジメントの項目が
大幅に強化
（ID.SC SCRM）

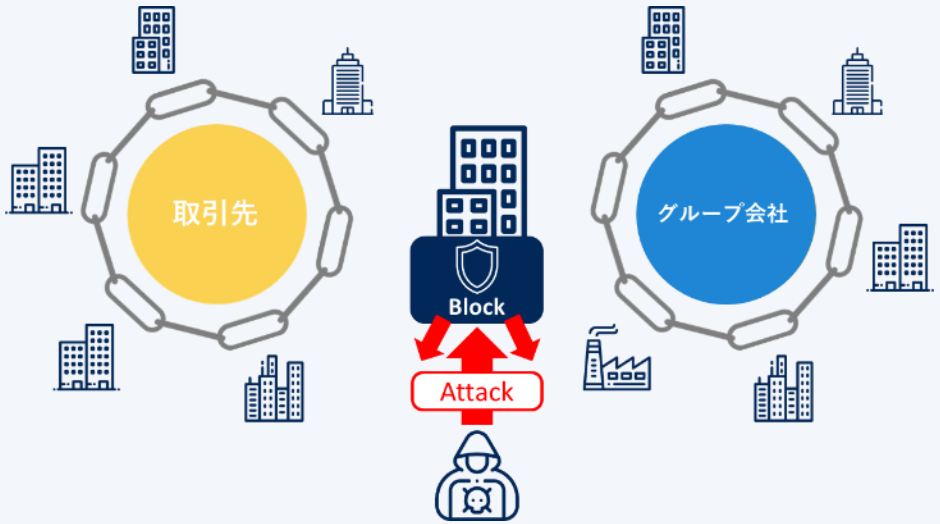
Secure SketCH

Point 3

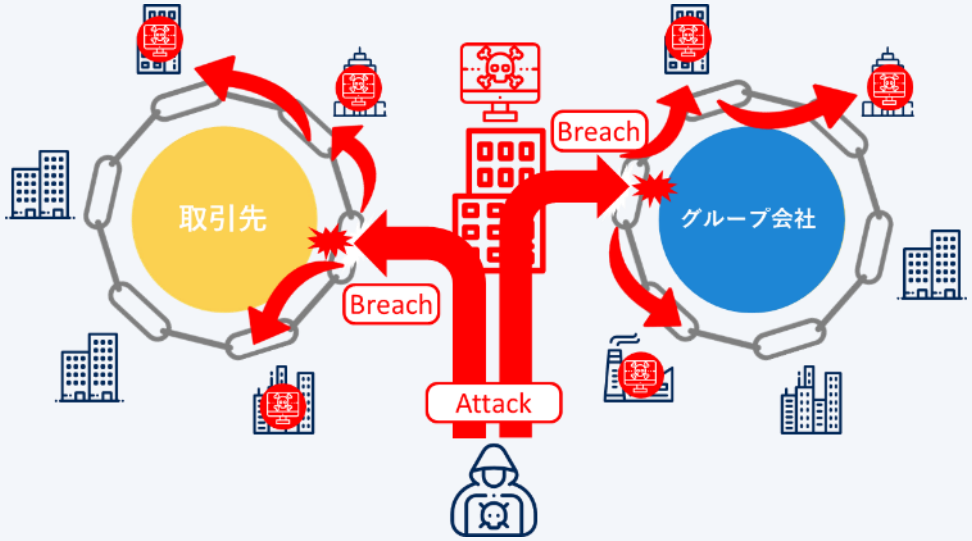
自社のインシデント影響が委託元やグループ全体に波及する可能性を伝える

サプライチェーンを構成する企業には「**自社で発生した事故が委託元やグループ全体に波及する可能性があること**」また、グループ内の統括企業には「**グループ会社や委託先の1社におけるセキュリティ上の欠陥から、関連する企業全体に影響を及ぼす可能性があること**」を意識しなければなりません。あらゆる企業がサプライチェーンリスクの観点において、**サプライチェーンを構成する一員である自覚を持ち、**被害者にも、加害者にもならないようにセキュリティ対策を実施する必要があることを建設的な危機意識と共に伝えることもポイントです。

「**鎖の強度は最も弱い環で決まる**」ため、
サプライチェーン全体のセキュリティレベルを維持する責任がある



万が一自社でインシデントが発生した場合、
影響がグループ会社や取引先にまで波及する可能性がある



Secure SketCH

Point

4 セキュリティ対策の必要性を複数の視点で伝える

セキュリティ予算獲得の肝は、**経営層がセキュリティ対策の必要性を自分事として意識すること**にあります。
そのためには、セキュリティ担当者の得意な領域である「セキュリティ脅威」や「技術論」だけではなく、相手（ここでは経営者）の視点に立って、多様な訴求をすることがオススメです。昨今のセキュリティトレンドや経営層の視点・関心事項を踏まえると、3つの観点があります。

責任は経営層個人にもおよびうる

某教育会社様
情報漏えいで取締役2人が辞任へ

被害＝情報漏えいだけに留まらない

某食品会社様
決算報告が延期する事態に

セキュリティ対策状況の開示＝非財務情報の発信・共有

JCICによるセキュリティ対策公開のメリット

①「**顧客や取引先**」に対して、安心して製品やサービスを利用してもらうことができる

②「**株主**」に対して、リスクマネジメントが合理的に機能していることの説明責任を果たすことができる

③「**機関投資家**」に対して、企業格付けなどにプラスの影響を与えることができる

JCIC ＝ 一般社団法人日本サイバーセキュリティ・イノベーション委員会

Secure SketCH

観点 1

Internal Control：責任は経営層個人にもおよびうる

セキュリティに関して、経営者が果たすべき役割とはセキュリティにおける善管注意義務を果たすことに尽きます。某教育会社の事例の通り、セキュリティインシデントは企業への責任追及だけでなく、経営層個人の責任にもなりえる時代です。

一言でまとめると、**「経営者として、企業のセキュリティ対策や予算策定にきちんと向き合ったか」という観点が最重要ポイント**でもあるため、経営者がセキュリティ対策の善管注意義務に関して、疑義を受けることのないように、セキュリティ担当者が経営層とコミュニケーションを図る過程で、丁寧に善管注意義務の観点も説明していくことが大切です。

責任は経営層個人にもおよびうる

某教育会社様

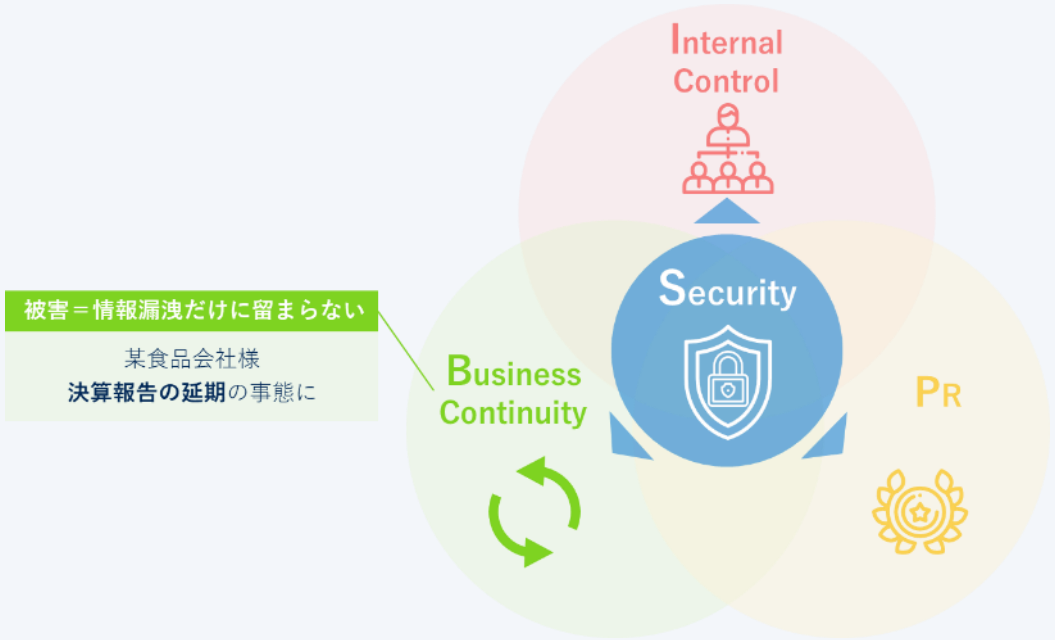
情報漏洩で取締役2人が辞任へ

観点２

Business Continuity：被害＝情報漏えいだけに留まらない

近年、セキュリティインシデントによる被害は情報漏えいだけに留まることなく、脅威が向かう先は「機密性」から「可用性」にシフトしている傾向も見られます。稀に、自社の経営層の誤った理解により、セキュリティ予算も割り当てられずに困っているセキュリティ担当者の方からお話を聞くことがありますが、昨今のセキュリティ脅威動向や具体的なインシデントに目を移せば、機密情報がないからセキュリティ対策の優先度を下げるというような考え方では通用しません。

サイバー攻撃の狙いや潮目が変わりつつあることを共有し、**ステークホルダーとの信頼関係の構築および事業継続性の観点**からも、セキュリティ対策の戦略的な推進がキーワードになっています。

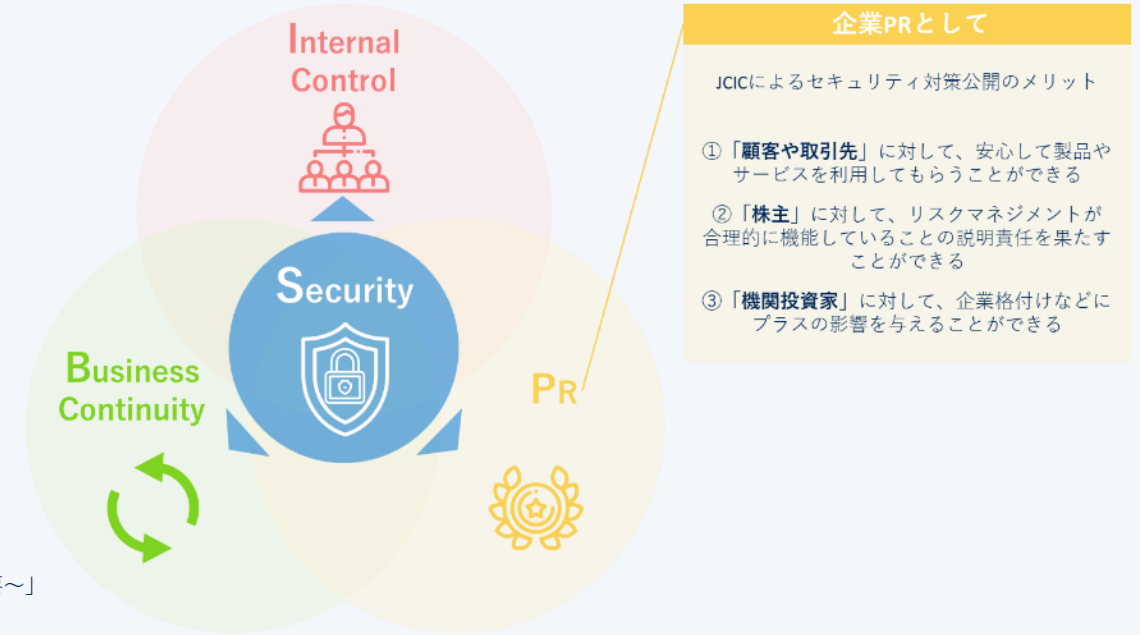


観点３

PR：セキュリティ対策状況の開示＝非財務情報の発信・共有

企業PRとしてのセキュリティにもなりえます。実際にある企業様では、**売上向上とブランディング向上施策**に、対策情報の公開を実施している企業も存在します。

総じて、セキュリティ対策の必要性を、単なるリスクだけではなく、関連の他社事例を踏まえつつ様々な角度で伝えて経営目線で必要性を実感してもらい、対応優先度を高めてもらうよう訴求するとことが、今後とても有効になります。



参考：一般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）
「サイバーセキュリティ情報公開のポイント ～経営者の取組み姿勢が重要～」
https://www.j-cic.com/pdf/report/Disclosure-Report.pdf

Point 4 ＋α

経営者と良質な対話をするために、財務諸表の観点を取り込んで、数字を取り扱うことが重要

DX前提の時代は、情報/サイバーセキュリティをマイナスの影響からだけ語るのではなく、決算書思考におけるステークホルダーの観点や売上・利益といった、経営指標と絡めていくことも必要です。

決算書思考　3つの目線

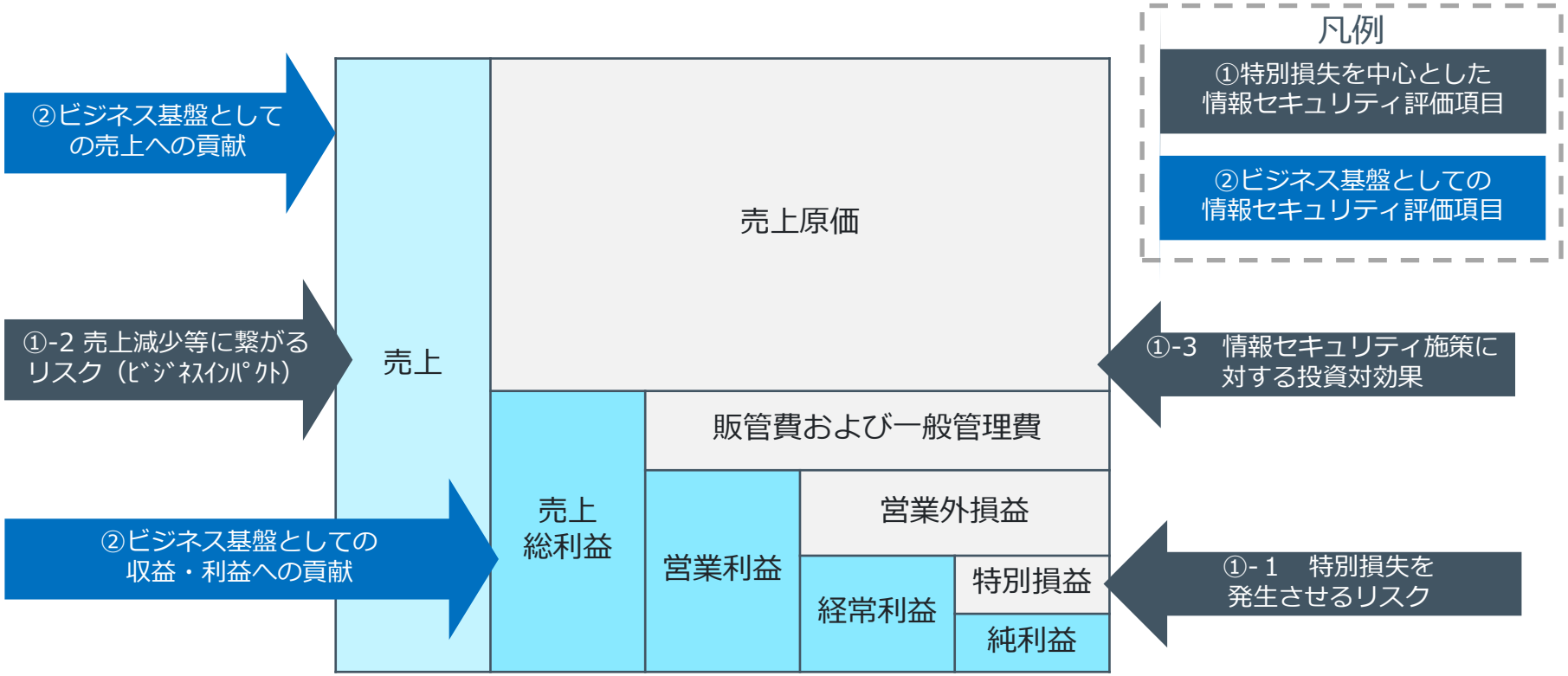
目線１　安定性
銀行/格付け会社

目線2　収益性･成長性
経営者

目線3　資本効率性
投資家

参考：CISOハンドブック（技術評論社）
3-1　CISOのための財務諸表の読み方
3-2　経営における「数字」の重要性

損益計算書の構造と情報セキュリティの評価項目



Secure SketCH

目次

セキュリティ予算取りの流れ

実際の予算取りに必要な流れは、大きく4つのステップにわかれます。

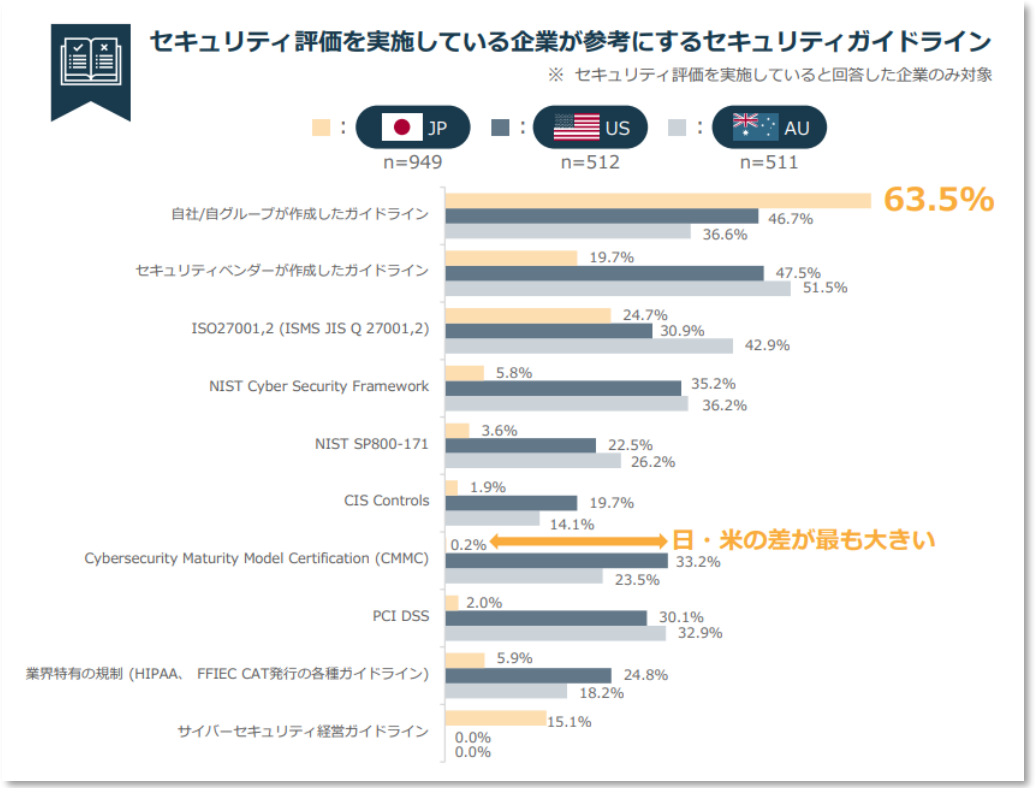
Step 1

リスク特定（可視化）

セキュリティ戦略・対策を意味あるものにするには、網羅的に対応していくことが重要です。やみくもに、すべての情報資産に対して対策をするのは、コスト面やリソース面でも難しいので、基本的には定期的（年一回など）に、自社の全体像を踏まえたうえで、必要項目を洗い出し、全て実行できる予算を確保する流れを推奨します。

なお、企業がいち早く対策の全体像を知るためには、**各国・各団体が出しているフレームワークやガイドライン**を参照することが近道です。

これらのガイドラインは、「経営層向け」「マネジメント系」「技術系」などカバー範囲が変わってくるので、複数のガイドラインを組み合わせて活用していくことが理想です。



参考：NRIセキュアテクノロジーズ
「NRI Secure Insight 2022～企業における情報セキュリティ実態調査～」
https://www.nri-secure.co.jp/download/insight2022-report

Secure SketCH

Step 1

リスク特定（可視化）

実際にリスク特定する方法は、大きく分けて３つあります。 以下図の通り、費用面やリソースによってマッチする方法はそれぞれなので、自社に適切な方法で対応してください。なお、可視化ツールの活用が、人材不足かつ予算が限られる中で費用対効果高い施策といえます。

	①各種ガイドラインを参照（ISO27001、NIST CSF、等）	②可視化ツールを利用（Secure SketCH、IPAベンチマークツール）	③セキュリティベンダーによるコンサルティングサービス
方法	Excelなどを利用し自力で照らし合わせ対応状況を確認する	ツールが用意した設問に回答する	コンサルタントからヒアリングを受ける
時間	大	中	中
サービス利用料	小	中	大
人件費	大	中	中

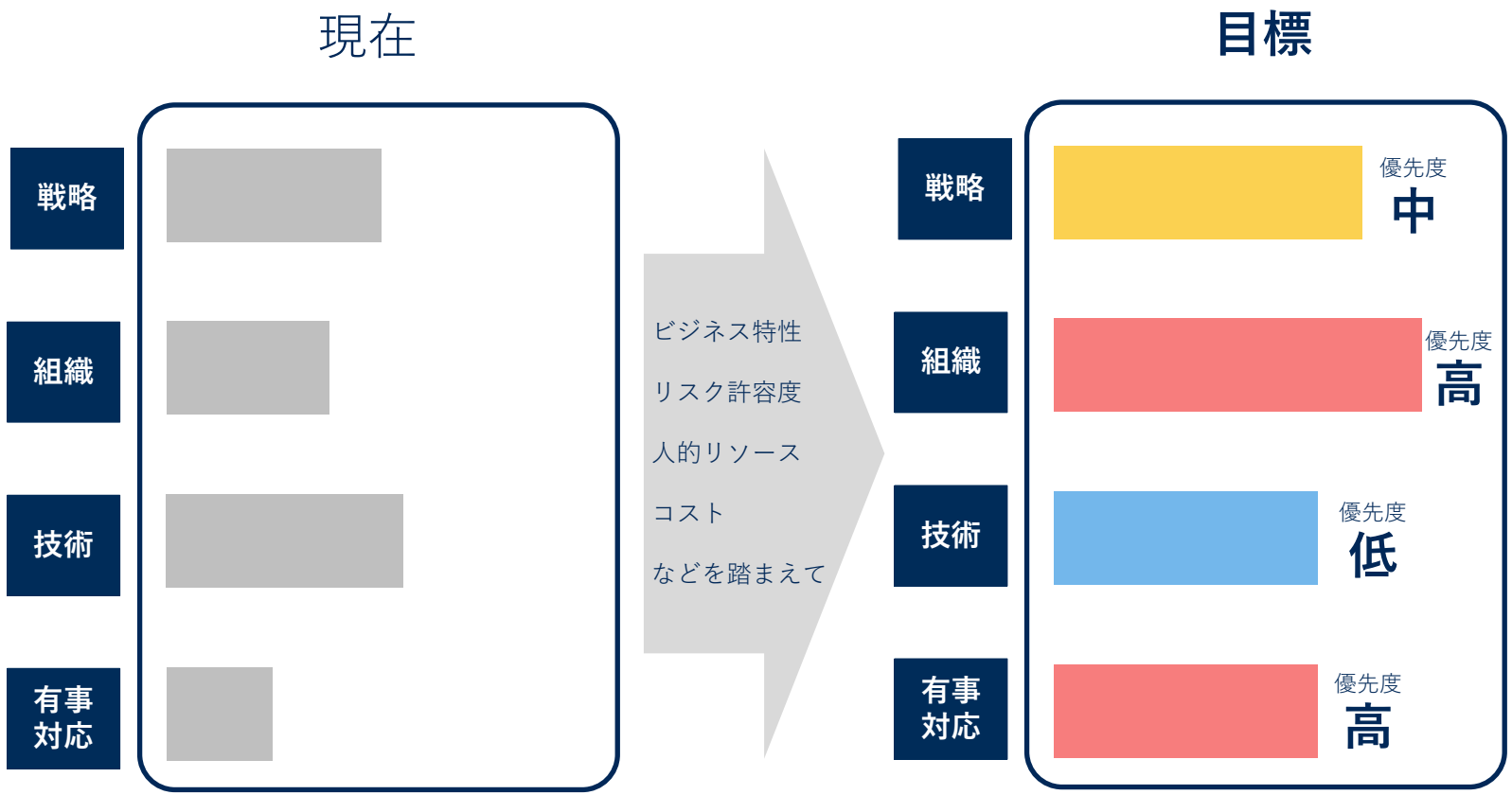
→人材不足かつ予算が限られる中で、**可視化ツール**の活用が効果的

Secure SketCH

Step 2

リスク分析（優先度付け）

ステップ①で特定したリスクに対して、対応優先度付けを行います。ここでは現在の実態を踏まえながら、企業・組織の目指すレベルを決めることがポイントです。その際、**必ずしも最高レベルを目指すことが正解ではない**ことを注意してください。自社のビジネス特性、自社の近未来におけるあるべき姿・望む姿を想定した上で、カテゴリ毎に目指すべきラインや対応優先度を設定することが重要です。



（例１）
製造業の会社であれば、
工場の稼働停止（可用性の侵害）や
IoT関連の優先度を高める

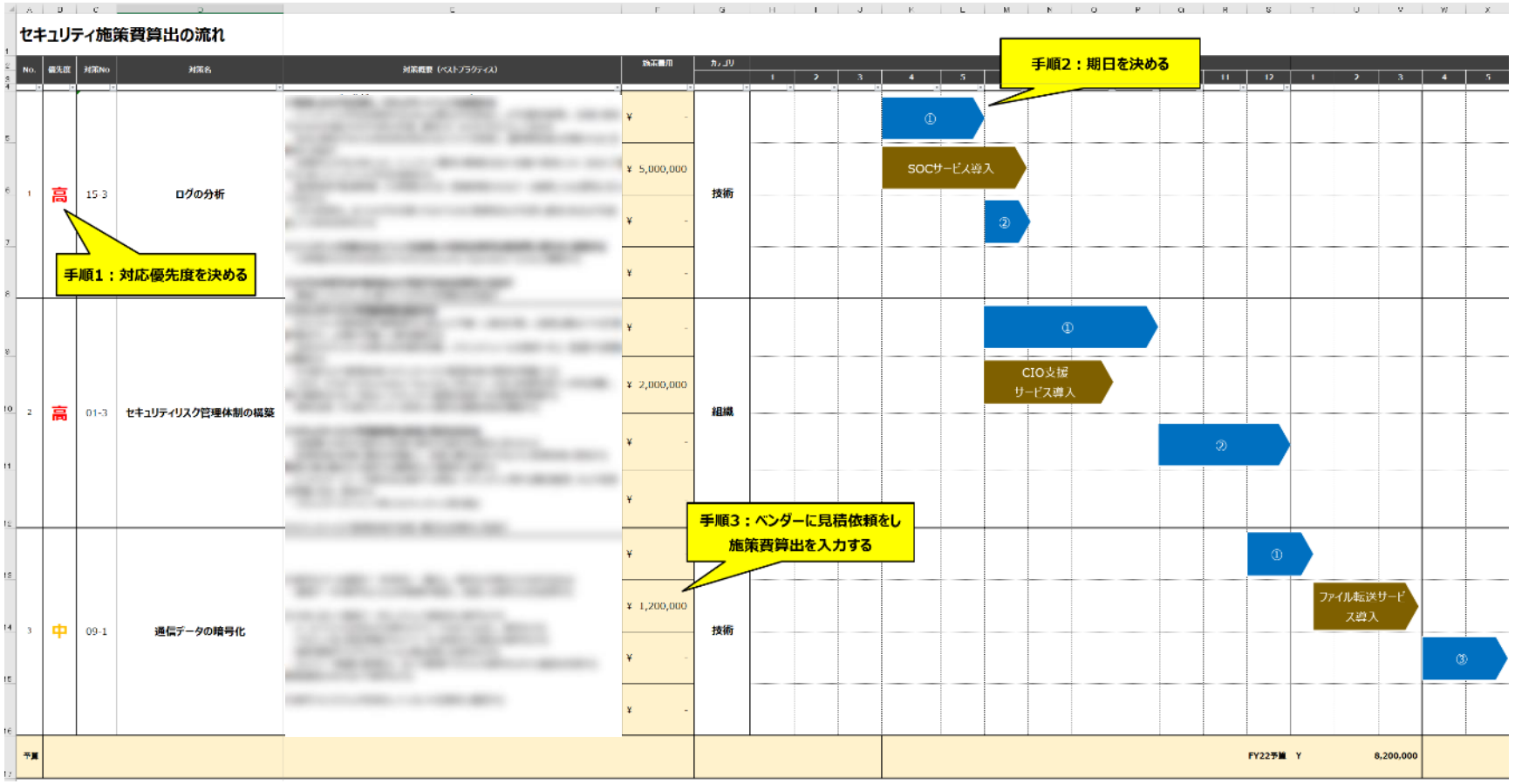
（例２）
非上場企業が数年後に上場を
目指すような場合であれば、
上場企業に値する管理体制を
セキュリティを含めて整備する

Secure SketCH

Step 3

施策費算出

対応優先度を決めた後は、実際の費用算出をしていきます。費用算出時には各対策の対応期日決め、それぞれの費用を各ベンダーに収集し、総額を出していきましょう。同時に導入実績を確認し、自社と同レベル企業が利用しているかも含めて情報収集をするとよいです。



Step 4

経営報告

最後に経営層に期待効果を定量的に説明していきます。 企業やセキュリティ担当者毎に、報告のフォーマット・書式があると思いますが、伝えるべきことは以下の５つだと思いますので、この要素を洗い出しましょう

検討要素

- 現状
- 問題点
- 施策メリット・期待される効果
- 予算額
- 対応計画

目次

具体的な解決策

セキュリティ評価のすべてをWebで実現できるプラットフォームサービス「**Secure SketCH**」

これまで解説してきた予算取りのポイントの具体的な解決策の手段として、**Secure SketCH**の活用がおすすめです。
SketCHを利用すると、前段で上げた経営報告時の「５つの検討要素」を簡単に定量化・グラフ化することができます。

＼国内最大級の7,000社が利用／

Z HOLDINGS
日テレ
brother
MUFG
三菱UFJフィナンシャル・グループ
au カブコム証券
GREE
Daiichi-Sankyo
YAMAHA
Revs Your Heart
日産証券
セブン銀行
MACROMILL
明治安田生命
KURASHICOM
Sonic Garden
SBS リコーロジスティクス
NIKKO
CHEMICALS
YANMAR
PERSOL
パーソル キャリア
京都銀行
LIFULL
NTN
hulu
フジメディアホールディングス
乾汽船

※2024/1月現在

Secure SketCH

Step 1

約80問の設問に回答して自社の状況を可視化

リスク特定（可視化） > リスク分析（優先度付け） > 施策費算出 > 経営報告

ガイドラインは各々の特長や最新版を正確に把握し、業種や用途に応じて複数を参照していくなど、使いこなすことが難しいとされています。
しかしSecure SketCHでは、これらのガイドラインをセキュリティコンサルが**約80問に集約**しているので、簡単に偏りのない網羅的な評価ができます。

カバー範囲

以下10つのガイドラインに対応しています。（2024/1月現在）

ISO：ISO/IEC 27002:2022
経済産業省：情報セキュリティ管理基準（平成28年改正版）
経済産業省：サイバーセキュリティ経営ガイドライン V2.0, V3.0
NIST：Cyber Security Framework V1.1
NIST：SP800-171 Rev2
CIS：CIS Controls V7.1, V8
米国防総省：CMMC v1, v2

設問構成

「戦略」「組織」「技術」「有事対応」の
4カテゴリ・20分類で構成されています。

Secure SketCH

Step 2

可視化した内容を基に対応優先度付け

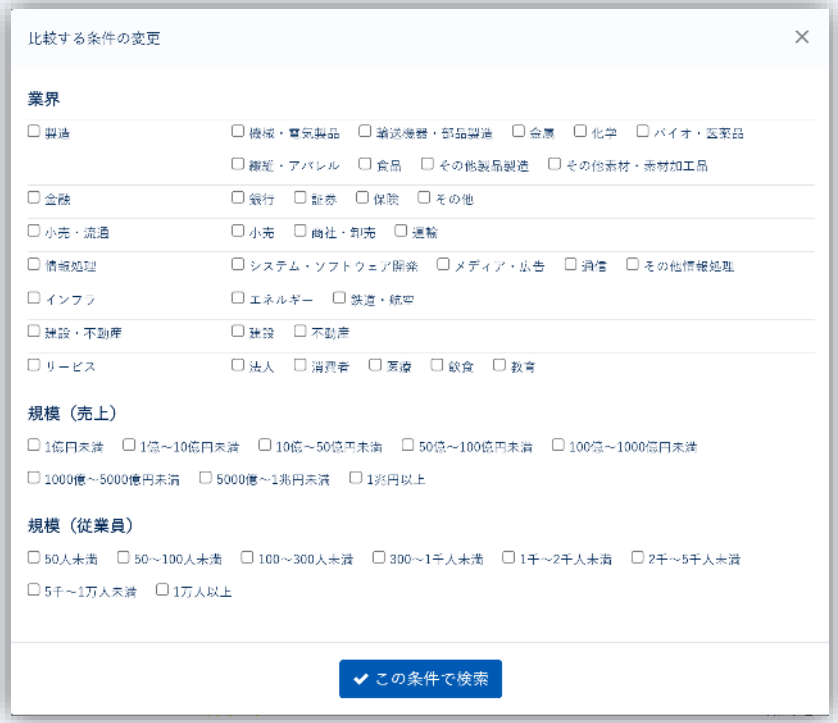
自社スコアや偏差値などが定量化の上、シンプルなグラフで提示されます。ですので、専門知識に差異がある複数のステークホルダー間で、共通の認識をもちやすくなります。では、この評価結果を踏まえて対策優先度付けをする際に活用できる機能を、後段でご紹介します。

Secure SketCH

Point.1

同業他社の対応状況と比較する

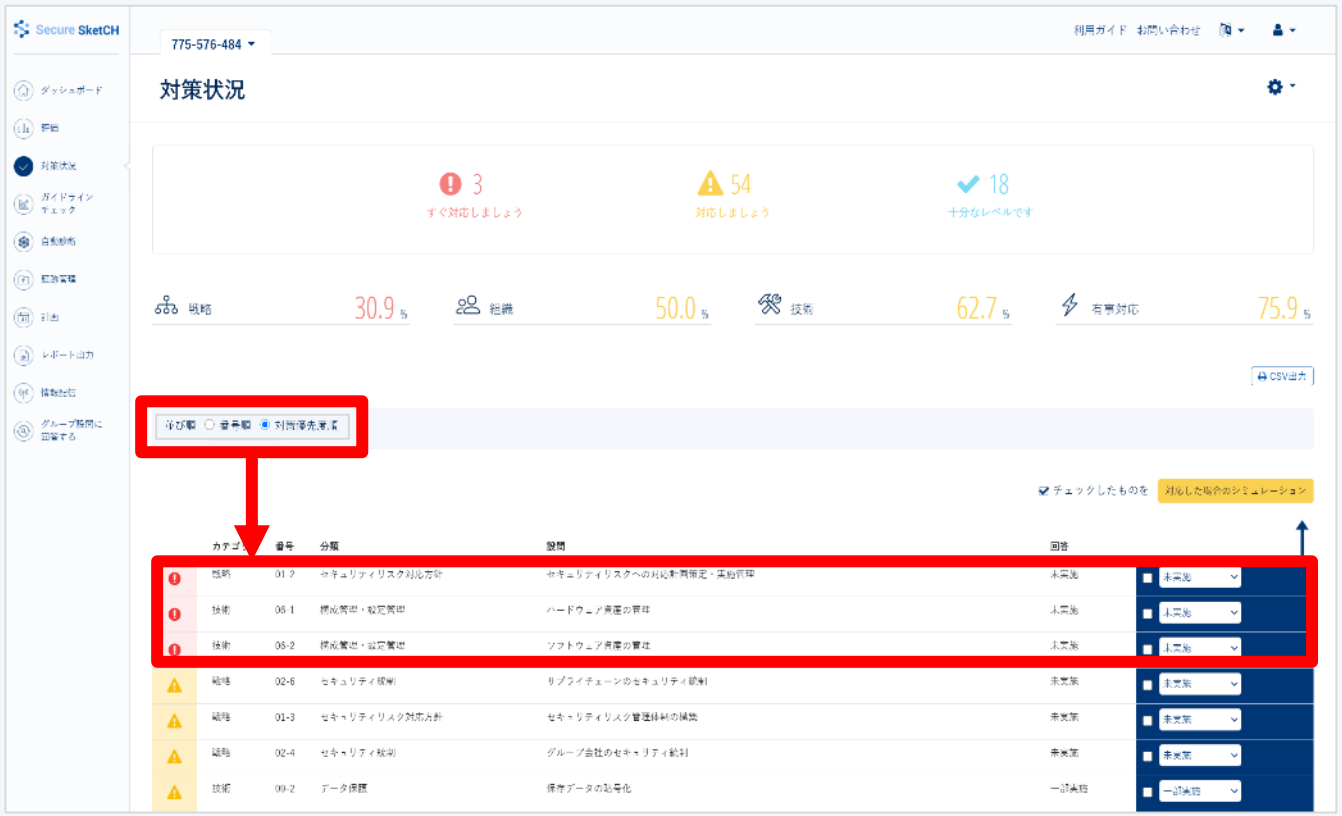
評価結果を、**同業他社のデータと比較**が可能ですので、他社に比べて対応が弱いところを洗い出しできます。この画面ですと、まず得点に関しては672点と、他社・同業とくらべても点数が高いですが四つのカテゴリに注目してみると、有事対応に関しては金融業平均を下回っていることがわかりますので、例えば「有事対応に関して早期に対応する必要がある」と優先度付けをすることができます。



Point.2

セキュリティコンサルが定義する優先度を確認する

弊社のセキュリティコンサルが定義する**対策優先度順**もご覧いただけますので、専門家の知見を基に優先度付けをすることもできます。



専門企業のノウハウ

NRI SECURE

あらゆる情報セキュリティの課題を
“ワンストップ”で解決

- コンサルティング
- DXセキュリティ
- マネージドセキュリティサービス
- ソフトウェア

Secure SketCH

Point.3

対策実施後の効果をシュミレーションをする

仮に選定した対策を実行した場合、どの程度評価結果が変わるのかを**事前にシュミレーション**することもできます。

この機能で、対策の効果を数値化して確認できますので、経営層から「この対策のどのくらい意味があるの？」といわれた場合でも、「この６つの対策をすると646点から729まで点数があがる」と定量的に伝えることができます。

Point.4

複数のガイドラインを踏まえた重要性を訴える

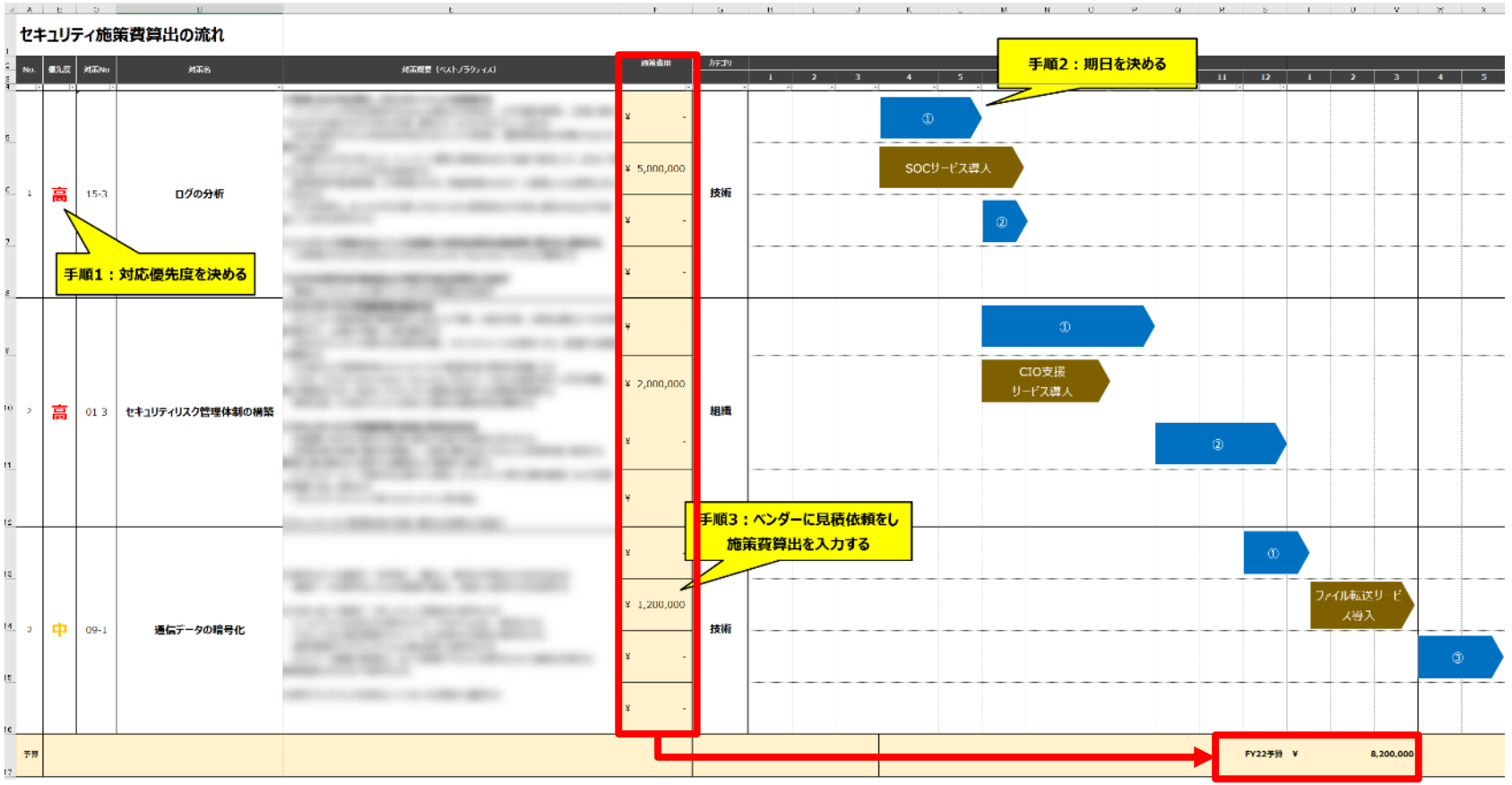
約80問の標準設問への回答をもとに、**各ガイドラインごとの対応状況を自動で算出**します。また、各設問が各ガイドラインのどの項目と関連しているのかも確認できるので、対応優先度を決める際に、「複数のガイドラインでも取り上げられている対策項目な為、優先度高く対応する必要がある」などといった説明責任にも使えます。

Secure SketCH

Step 3

施策費算出

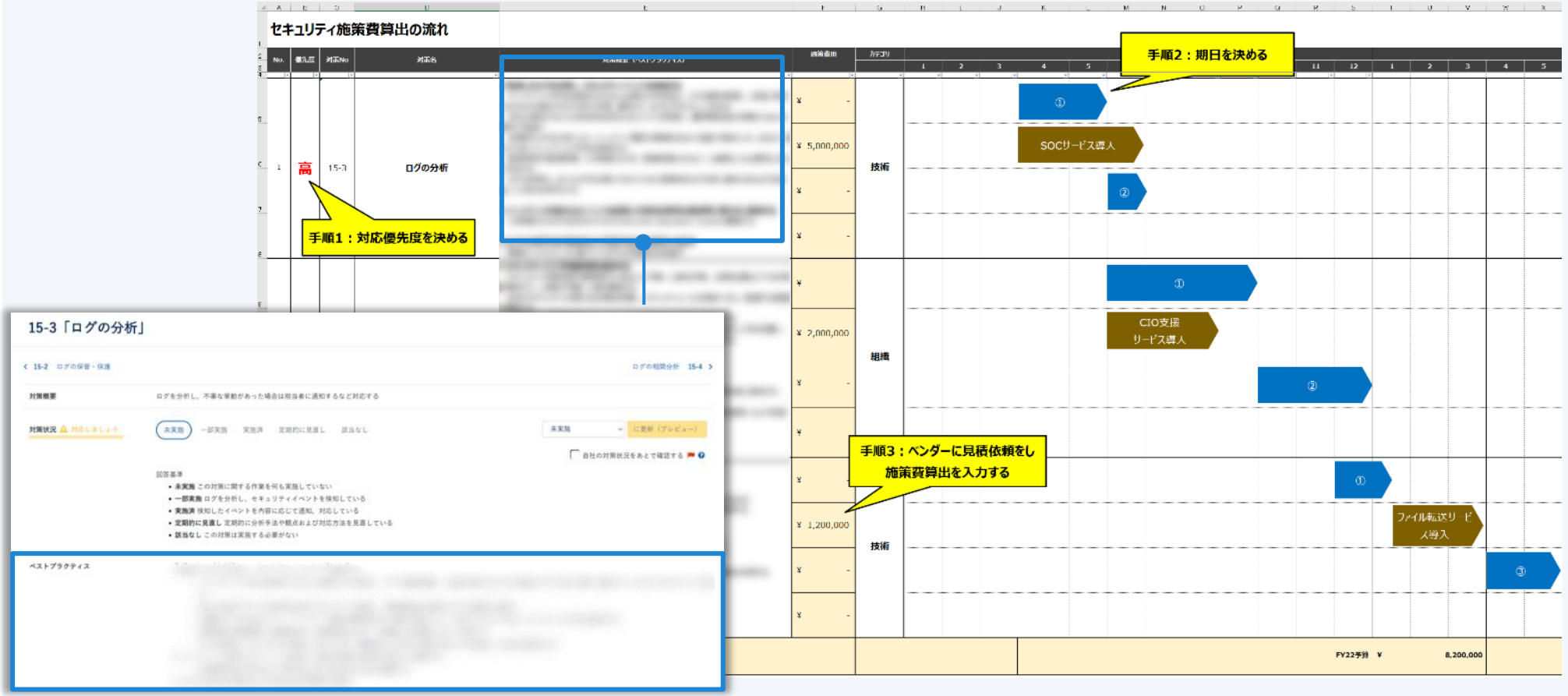
下記手順に従って施策費算出を行いましょう。



Point.1

対策概要（ベストプラクティス）について

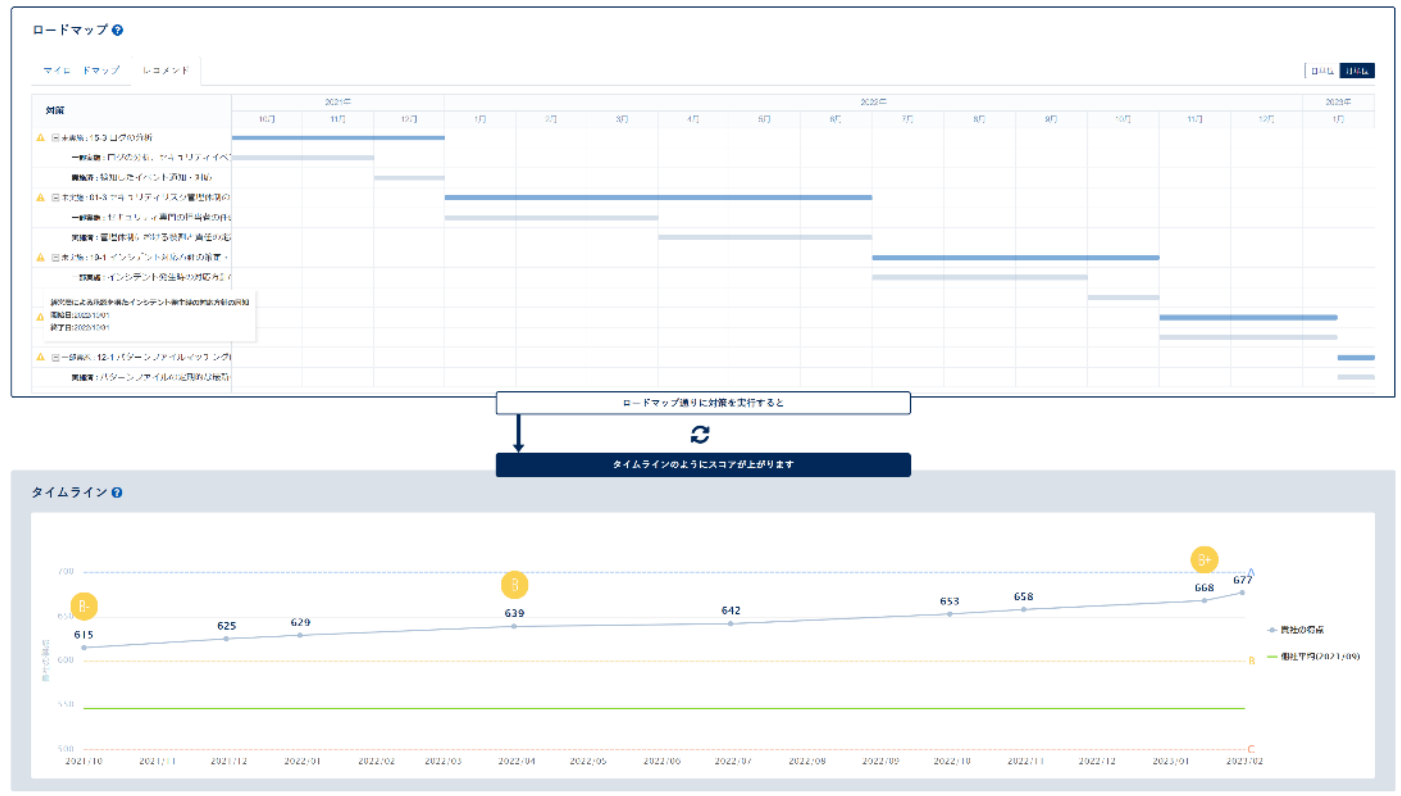
各対策ごとの『対策概要（ベストプラクティス）』はSecure SketCH上で確認できますので、この内容を参考に対応内容・期日を決めることが可能です。



Point.2

対応期日を決定するにあたって

対策の優先度とそれぞれの対策の実施想定期間、矢羽根を自動で引く機能もございますので、本情報を参考に期日を決めることもできます。さらに、このロードマップ通りに対応するといつまでにどの位スコアがあがる、いつまでに同業他社と同レベルに達するなど、対策の有効性を確認することも可能です。



Point.3

関連製品情報について

Secure SketCH内で専門家が執筆したブログや関連製品も確認可能です。ぜひ、製品情報収集にお使いください。

また、実際の費用に関しても弊社では様々なサービスを扱っていますので、お気軽にお問合せください

Secure SketCH

Step 4

経営報告

施策費算出後は、経営層に期待効果を定量的に説明します。前段で上げた検討要素はこちらですが、これまでご紹介したようにSecure SketCHを利用するとこれらの要素を簡単に定量化・グラフ化することができます。

検討要素

- 現状
- 問題点
- 施策メリット・期待される効果
- 予算額
- 対応計画

×

Secure SketCH

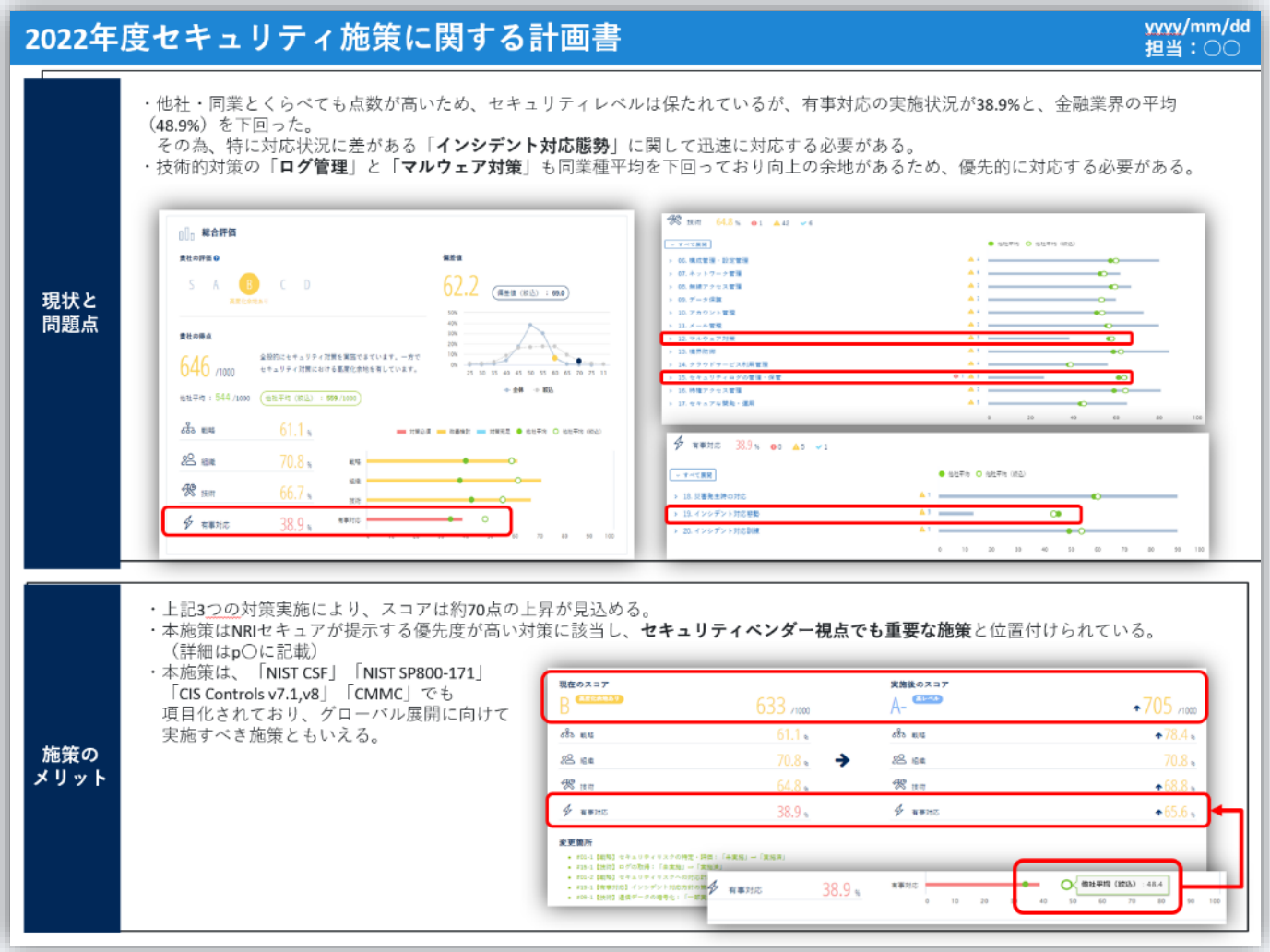
Point

計画書イメージ（1/2）

現状と問題点では、同業他社と比較した自社のポジションを総括し、コメントとしてまとめます。本計画書では、「自社の得点」「他社平均」「同業他社平均」に注目をして比較結果を提示したうえで、改善施策を三つ提示しました。なお、4つのカテゴリ毎（戦略・組織・技術・有事対応）に総括コメントを記載してもよいかもしれまん。

施策のメリット（期待される効果）では、まず対策優先度が高い対策提示し、これらの対策を実施した場合のスコアシミュレーションの結果も同時に提示し、同業平均以上になると視覚的に伝えています。

また、Secure SketCHで確認した優先度を考慮している点や、複数のガイドラインで項目化されていることを提示しました。

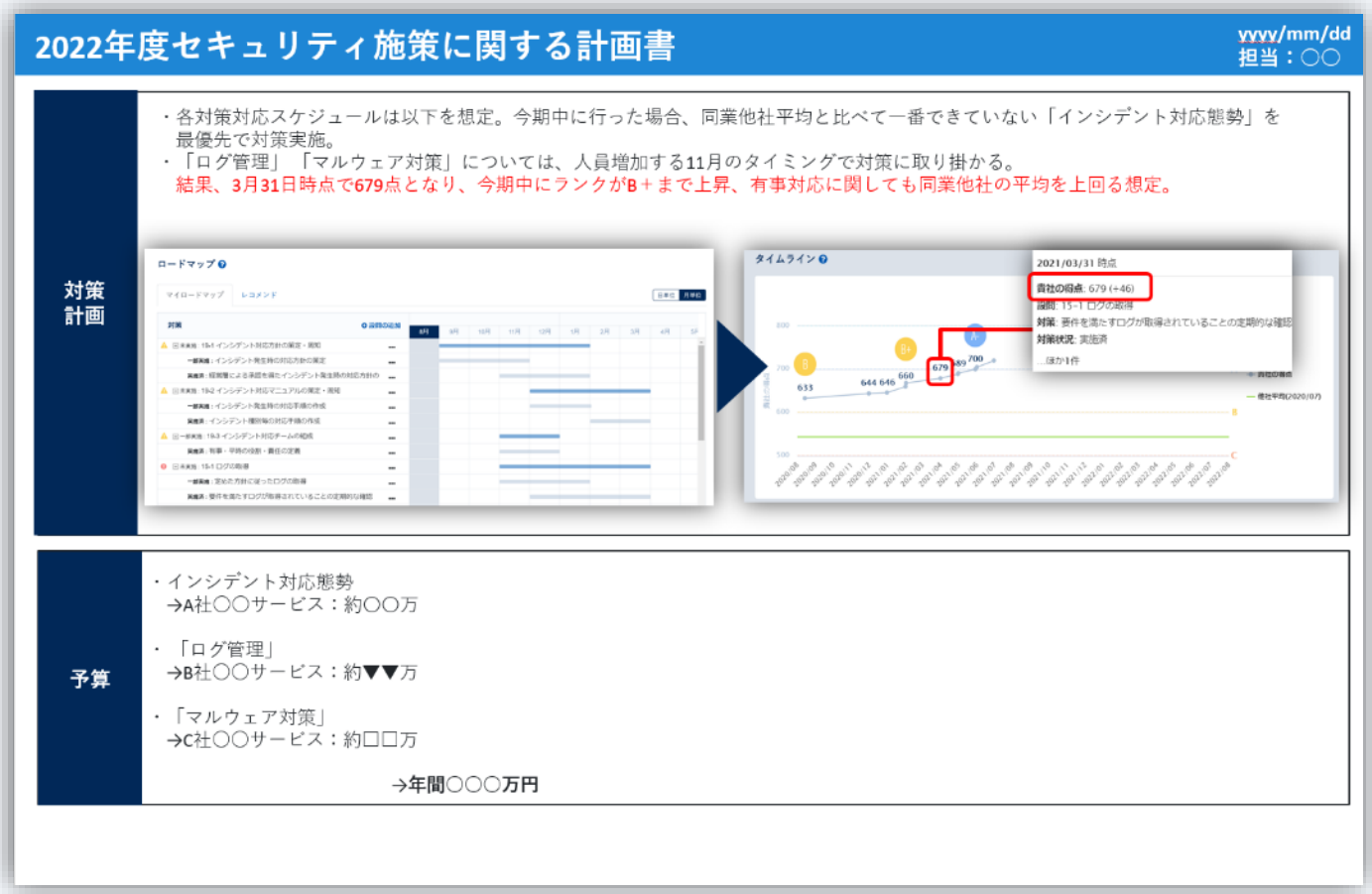


Point

計画書イメージ（2/2）

対策計画では、スケジュール感とタイムラインを記載し、この施策をすることでいつまでにどの位スコア向上が見込めるのかという観点を提示しました。

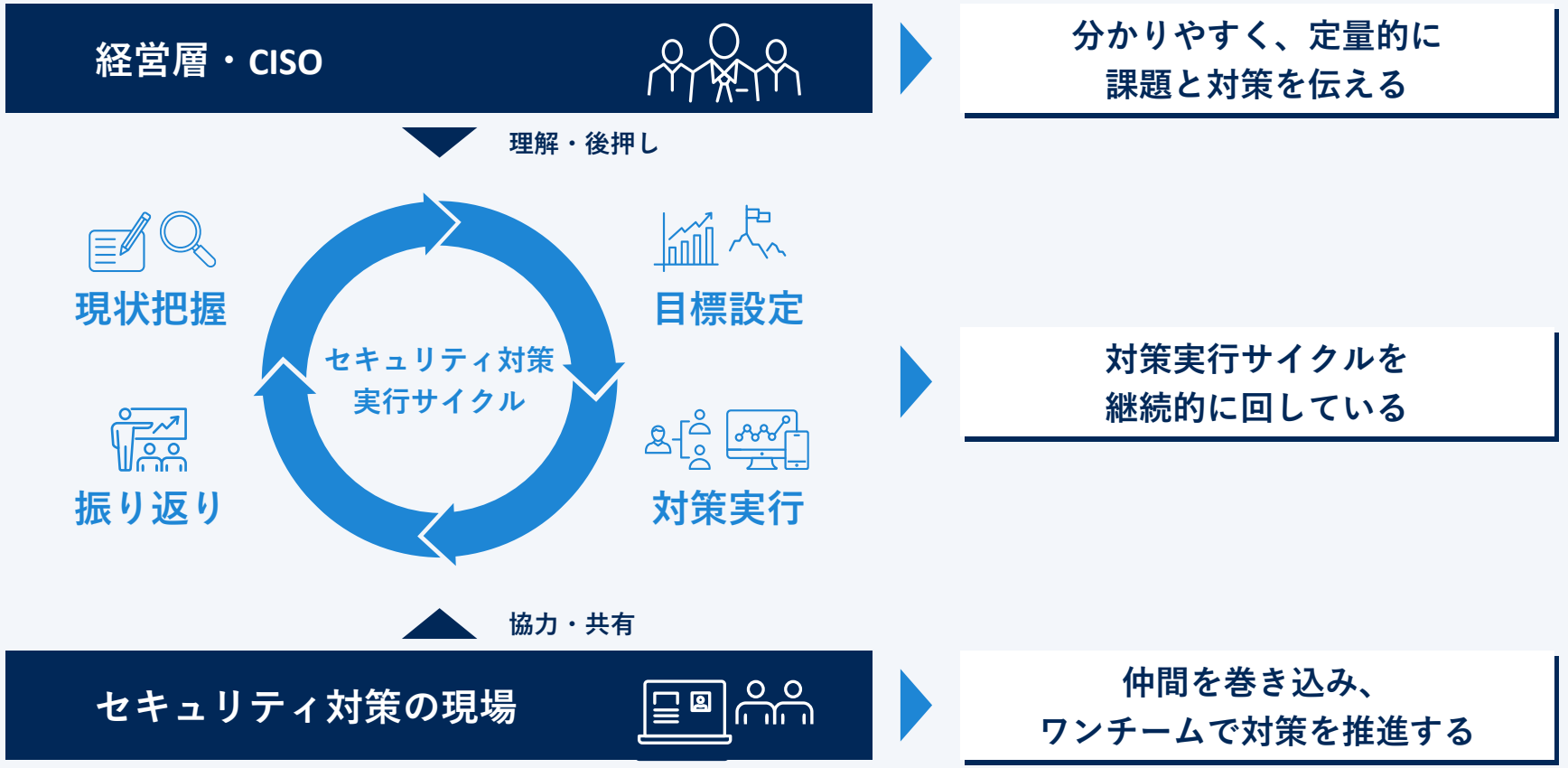
実際に算出した施策費を記載しています。



＋α

5 対策実行の管理・運用も可能です

セキュリティ対策状況をわかりやすく可視化・管理できるSecure SketCHは、経営層とのコミュニケーションの架け橋としても非常に効果的です。
是非、Secure SketCHを活用いただき、経営層を巻き込んだセキュリティ対策運用を行っていただきたく思います。



Secure SketCH

+α

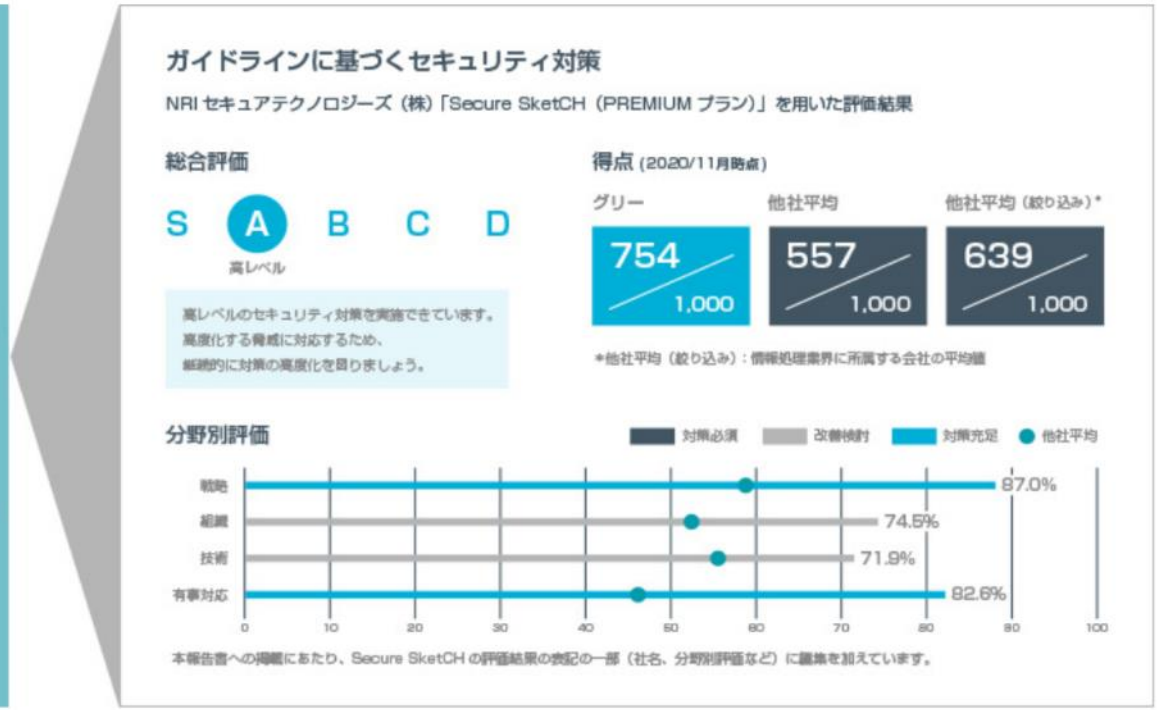
6 貴社の取り組みのPRに是非お使いください

外部公開している「情報セキュリティ報告書」の中に、SketCHの結果を客観的な評価として掲載している企業様もいらっしゃいます。

Secure SketCHでの評価結果を、企業や経営者の取組み姿勢として発信することも可能です※ので、是非ご活用ください。

※Secure SketCH有償プラン導入の企業様に限ります。

情報セキュリティ報告書2021



Secure SketCHによる評価実績

参考：Secure SketCH 導入事例「GREE社　国内外の情報セキュリティガイドラインに基づきセキュリティ活動全体を俯瞰」
https://www.nri-secure.co.jp/service/case/securesketch_gree

Secure SketCH

目次

おわりに

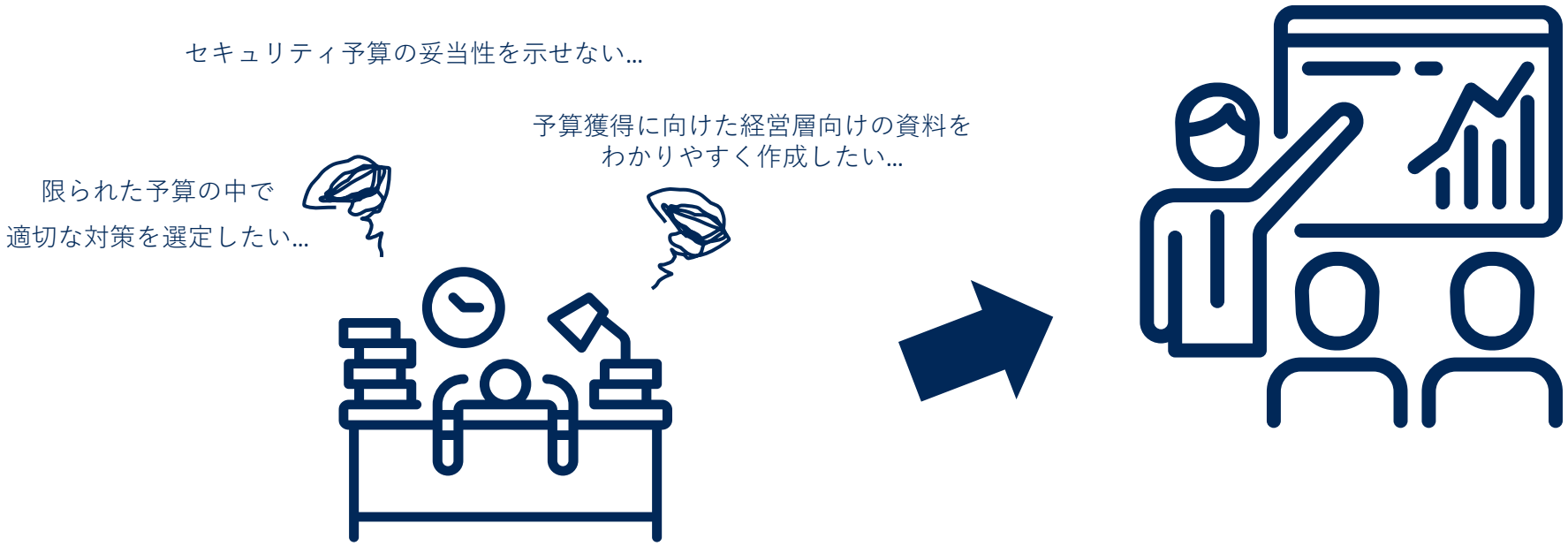
売上向上に直結しないがゆえに、特に経営層目線だと投資対効果が見えづらく、予算編成の理解が得にくいセキュリティ対策。

是非、本資料でお伝えしたポイントや、Secure SketCHで得られる情報を使って、

・なぜそのセキュリティ投資が必要なのか

・その投資が自社にとってどの程度必要なのか

を「**経営視点**」で経営層に示し、貴社のセキュリティ予算策定にご活用ください！



Secure SketCH

同業他社を引合いに

対策の必要性を権威付け

サプライチェーンへの影響を訴求

対策必要性を複数観点で伝える
（内部統制, ビジネス継続性, PRなど）

Secure SketCH

お問合せ先

セキュリティ対策の評価・実行に関するお悩みを解決します。

NRIセキュアはセキュリティ対策の評価・実行業務を効率化・最適化するサービスを提供しています。
導入に関するご相談・ご質問がある方は、Secure SketCHサービスページよりお気軽にお問い合わせください。

セキュリティ評価のすべてを
Webで実現できるサービス
ぜひ無料でお試しください

詳しく見る

Secure SketCH

https://www.nri-secure.co.jp/service/solution/secure-sketch

support@secure-sketch.com

ＮＲＩセキュアテクノロジーズ株式会社
〒100-0004　東京都千代田区大手町1-7-2　東京サンケイビル