生産性の高いセキュリティ

Secure SketCHを
最大限に活用して、
セキュリティ業務を
「効率化」する手法

Secure SketCH Books Vol.11

生産性の高いセキュリティ

Secure SketCHを最大限に活用して、セキュリティ業務を「効率化」する手法

現在の日本企業では高度なセキュリティスキルを持つ人材が不足している状況だといわれています。

このセキュリティ人材不足の状況を少しでも改善していくためには、セキュリティ人材の限りある人的リソースを有効活用していく必要があります。

本書ではこの貴重なセキュリティ人材を活かしきるために、Secure SketCHを活用して、『セキュリティ業務を効率化』するための方法について解説します。

目次

---

1. セキュリティの全体像を考える ～「広さ」と「深さ」で捉える～

セキュリティ業務を効率化させるために、まず考えなければいけないのは「そもそも自社のセキュリティ業務にはどんなものがあるのか？」ということです。

当たり前のことのように感じますが、企業ごと、業界ごとに必要となるセキュリティ業務が異なるため、まずは自社のセキュリティ業務の全体像を把握することが重要です。そして、その際には、業務を「広さ」と「深さ」で考えてみることで全体像が把握しやすくなります。

以下は、ある企業のセキュリティに関する業務カテゴリです。これがセキュリティ業務の「広さ」にあたるものです。まずはこのような粒度で、現在実施している業務を振り返り自社のセキュリティ業務の「広さ」を定義してみましょう。

フェーズ	業務カテゴリ
Plan （計画）	セキュリティ活動年間計画策定
Do （実行）	ID管理・アクセス管理
	脆弱性管理
	ネットワークセキュリティ管理
	可搬記憶媒体管理
	システムバックアップ管理
	クラウド利用申請のチェック
	セキュリティ教育
	インシデント管理
Check/Act （点検・是正）	リスク管理（評価、対策検討）
	委託先管理
	個人情報管理（内部監査等）
	セキュリティ管理状況の月次点検
	セキュリティ関連文書の定期見直し

図. セキュリティに関する業務カテゴリ（広さ）

次に、セキュリティ業務の「深さ」について考えてみます。セキュリティに関連した業務の「深さ」とは、その業務がいかに難しいかということで、言い換えると業務の「パターン化のしやすさ・しにくさ」ということになります。

図. 業務内容のパターン化のしやすさ・しにくさ（深さ）

「パターン化しやすい業務」とは、あらかじめルールや業務プロセスを整備することで、人による高度な判断をそれほど必要としないような業務です。例えば、「申請書にもとづいたWEBフィルタリング設定の変更」など、決められた手順や判断基準にのっとって進められるような業務が該当します。

一方で、「パターン化しにくい業務」とは、手順が複雑でマニュアルやガイドラインでの標準化がしにくいものや、都度、高度な判断が求められるようなものです。例えば、「前年度の事故の発生状況を踏まえて、セキュリティ活動計画を作る」など、状況に応じて柔軟な対応が求められる業務です。

これらのパターン化のしやすさ・しにくさは、定型/非定型（型・種類）、定常/非定常（タイミング）という２つの軸でも表現をすることができます。この中では、「非定型かつ非定常」という業務が最もパターン化がしにくいということがいえるでしょう。

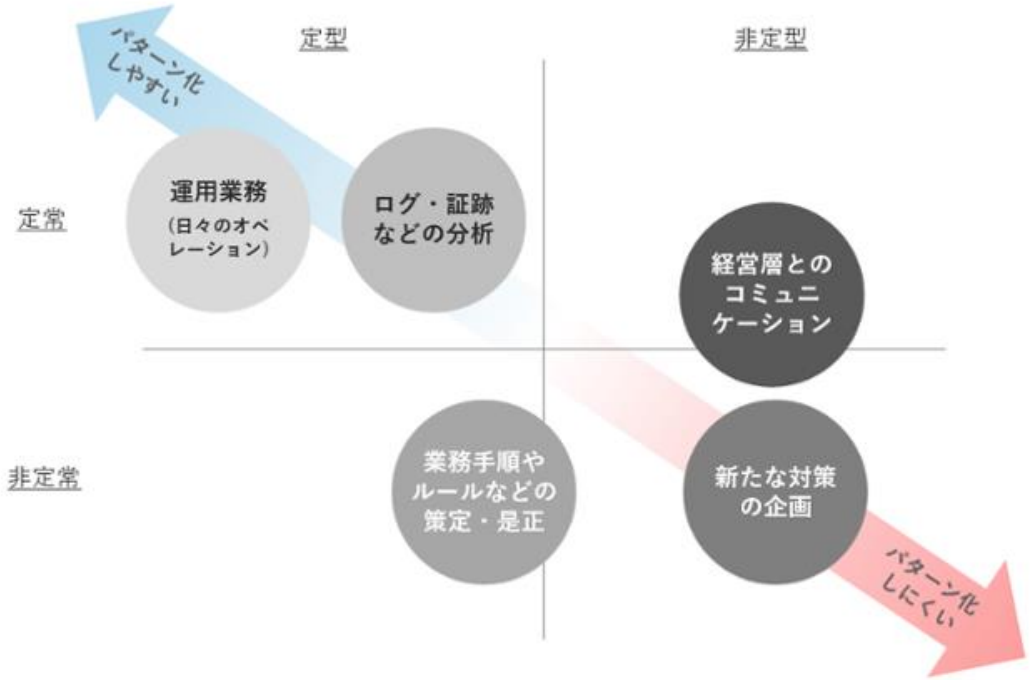


図. 業務内容のパターン化のしやすさ・しにくさ（定型×定常）

このようにして、前述の業務カテゴリ（広さ）のそれぞれで、どのような業務内容があるかを洗い出し、それらの業務を「パターン化のしやすさ・しにくさ」の観点で、業務の「深さ」を整理していきます。

フェーズ	業務カテゴリ	パターン化しやすい業務とパターン化しにくい業務の割合 しやすい ←→ しにくい
Plan （計画）	セキュリティ活動年間計画策定	
Do （実行）	ID管理・アクセス管理	
	脆弱性管理	
	ネットワークセキュリティ管理	
	可搬記憶媒体管理	
	システムバックアップ管理	
	クラウド利用申請のチェック	
	セキュリティ教育	
	インシデント管理	
Check/Act （点検・是正）	リスク管理（評価、対策検討）	
	委託先管理	
	個人情報管理（内部監査等）	
	セキュリティ管理状況の月次点検	
	セキュリティ関連文書の定期見直し	

図. セキュリティ業務の全体像（イメージ）

こうすることで、セキュリティ業務の「広さ」と「深さ」が分かり、業務の全体像が見えてきます。

2. セキュリティ人材を活かしきる考え方 ～業務の「選択と集中」～

そして、セキュリティ人材のリソースを有効活用していくためには、まずはセキュリティ業務の全体像の中から、業務の取捨選択をして不要な業務やプロセスを取り除いておくということが前提になりますが、その上で「セキュリティ人材が対応すべき業務」と、「セキュリティ人材以外が対応すべき業務」とを、きっちり分けて定義していくことが重要です。

では、「セキュリティ人材が対応すべき業務」とはどのようなものなのでしょうか。それは、高度な判断が求められる「パターン化しにくい業務」です。

「パターン化しやすい業務」は、協力会社などに業務委託をする、あるいはツールによって自動化するなどによって、セキュリティ人材以外で代替することができます。しかし、自社の事業環境を踏まえた判断が必要なケースなどは、高度なセキュリティ人材がより適切な対応ができ、代替が難しいです。

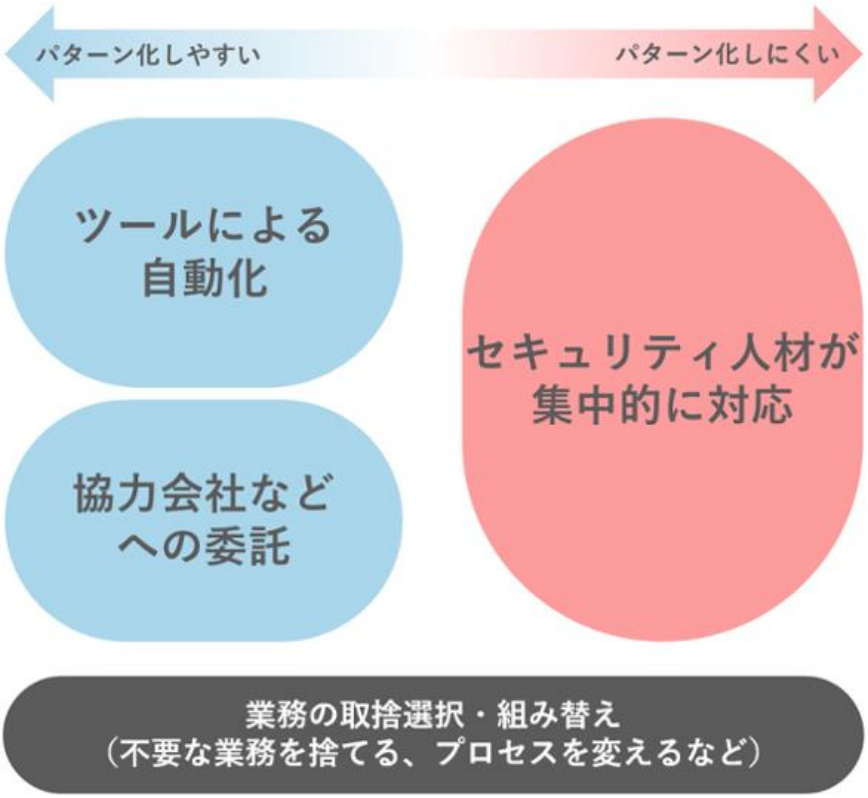


図. セキュリティ人材の業務の「選択と集中」

このように、業務の全体像の中から、セキュリティ人材が集中的に対応すべき業務を明確にして、対応方法にメリハリをつけることこそが、業務効率を向上させるためには最も重要なのです。

ここまでの流れをまとめると、以下のようなステップになります。

ステップ①　自社のセキュリティに関する業務カテゴリを定義する（広さの定義）
ステップ②　各業務カテゴリの業務内容と特性を定義する（深さの定義）
ステップ③　各業務内容の対応方法を定義する（セキュリティ人材 or アウトソース）

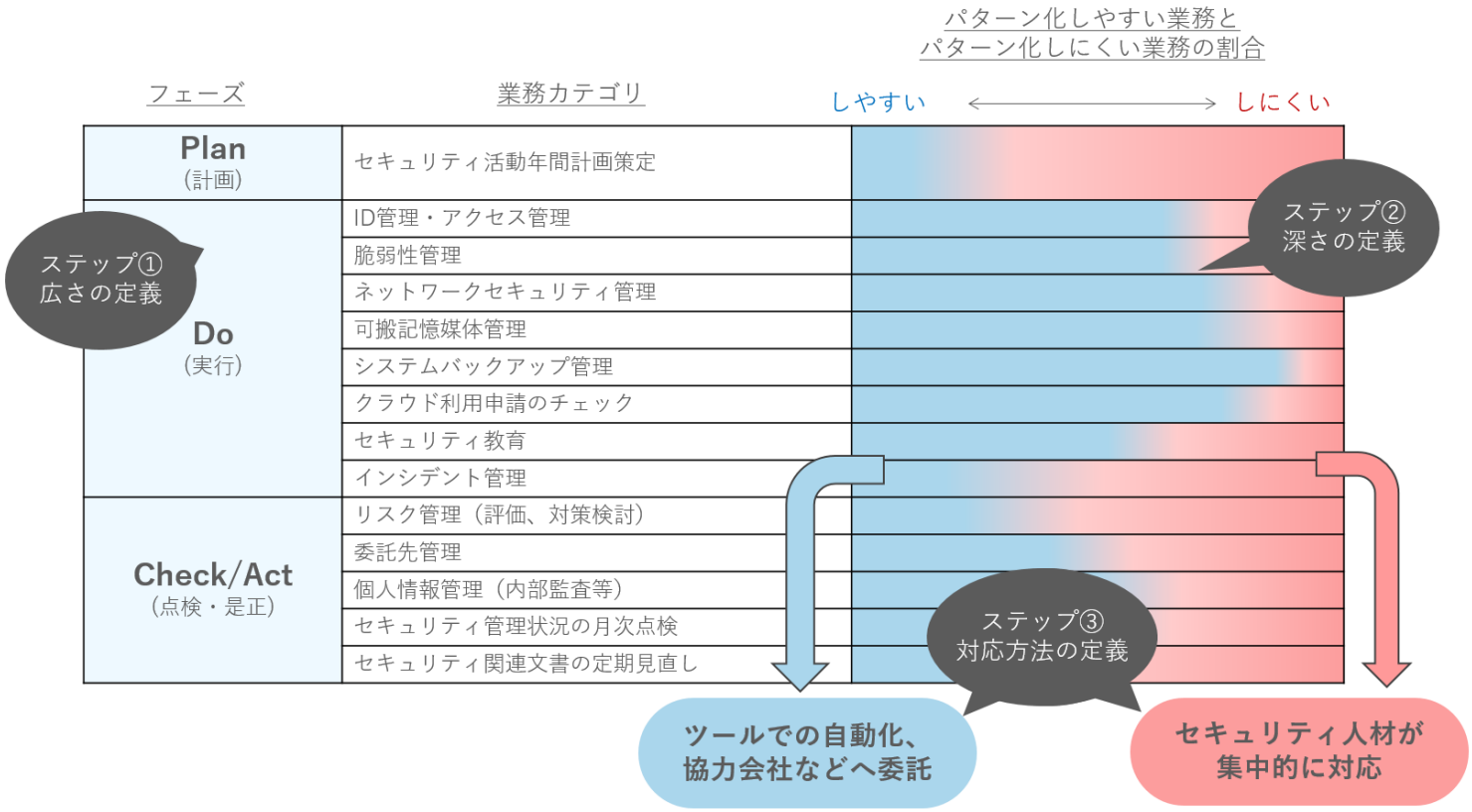


図. セキュリティ業務効率化の対応ステップ

パターン化しにくい業務の効率を上げるには？

それでは、セキュリティ人材の負荷をさらに低減させるために、「パターン化しにくい業務」も効率化することはできるのでしょうか？

かの有名な孫子の言葉に次のようなものがあります。

> *「彼を知り己を知れば百戦殆からず。*
> *彼を知らずして己を知れば、一勝一負す。*
> *彼を知らず己を知らざれば、戦う毎に必ず殆し」*

これは、敵の状況と、味方の状況を熟知していれば、100回戦っても負けることはない。敵の状況が分からなくて、味方の状況だけを理解している状態だと勝つことも負けることもある。そして、敵の状況も味方の状況も理解していなければ、必ず負けるだろう、という意味になります。

つまり、適切な「状況把握」が戦局を左右する判断につながる、ということを説いたものです。

これをセキュリティの業務に当てはめてみると、セキュリティの脅威と、自社のセキュリティ対策状況をきちんと把握していれば、サイバー攻撃を防ぐための適切な判断をすることができる、ということになるのではないでしょうか。

したがって、高度な判断が求められる「パターン化しにくい業務」では、適切な「状況把握」をするための仕組みを整備することが、業務効率を向上させることにつながるのです。

Secure SketCHは、企業が『己を知る』ことができるようになるツールです。つまり「自社のセキュリティ対策状況」をきちんと把握することができるようになります。

次章からは、効率的に状況把握をするために、Secure SketCHを徹底的に活用する方法を紹介していきます。

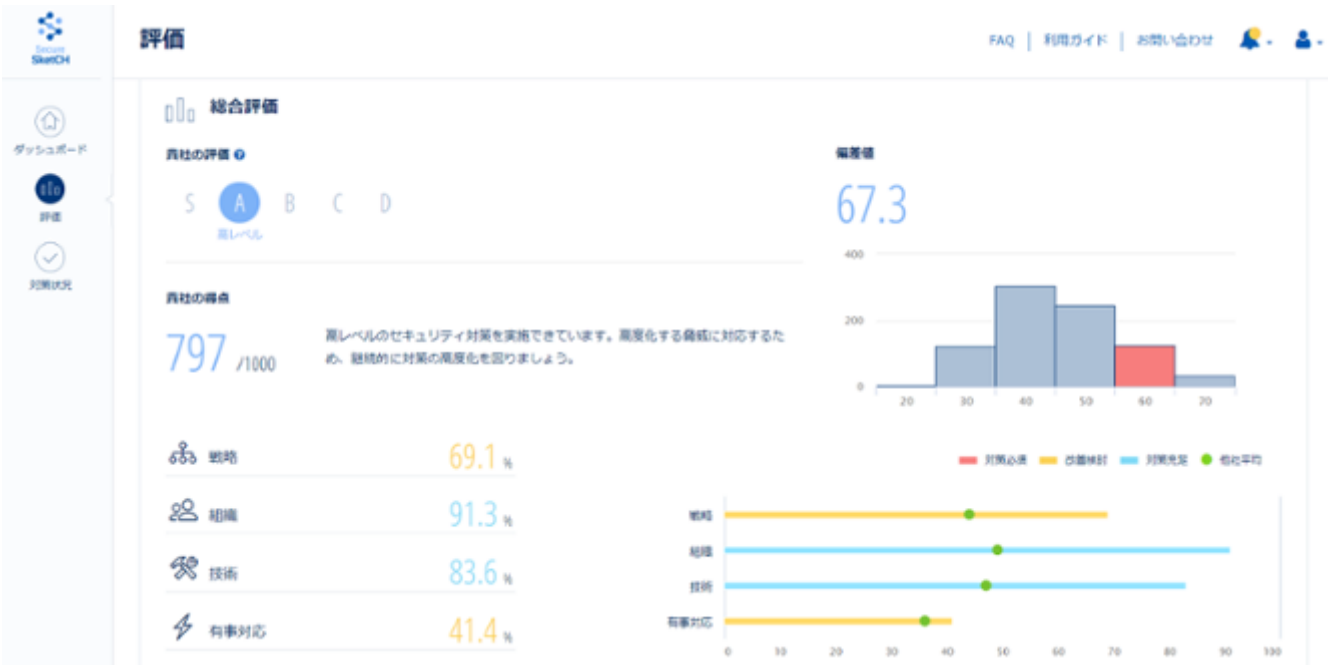
3. セキュリティ業務の効率化のための Secure SketCH 活用術

Secure SketCHを活用して、効率的な「状況把握」の仕組みにつなげるには、大きく以下の３つのパターンがあります。

活用術① 自社の今の「立ち位置」を知る
活用術② 社内の状況や必要な情報を集約する
活用術③ 有識者のナレッジを参照する

活用術① 自社の今の「立ち位置」を知る

まずは自社のセキュリティ対策の状況が、どの程度まで整備されているのかを確認するためにSecure SketCHを活用してみましょう。Secure SketCHでは自社のセキュリティ対策のレベルを、スコア・ランクや偏差値、そして他社の平均点などと比較をすることができます。



Secure SketCHの評価画面では、自社のセキュリティ対策の
スコア・ランク、偏差値が確認できる。

そして、自社の回答結果の一つひとつと、他社の平均点を比較することができるようになります。

対策の一つひとつで、他社の平均点と比較をすることができる。
上図のイメージでは「インシデント対応プロセス」が平均点よりも低いことが分かる。

また、Secure SketCHの「シミュレーション機能」を使うと、対策を実施した場合に、どの程度スコア・ランクが変わるのかを事前に確認することができます。

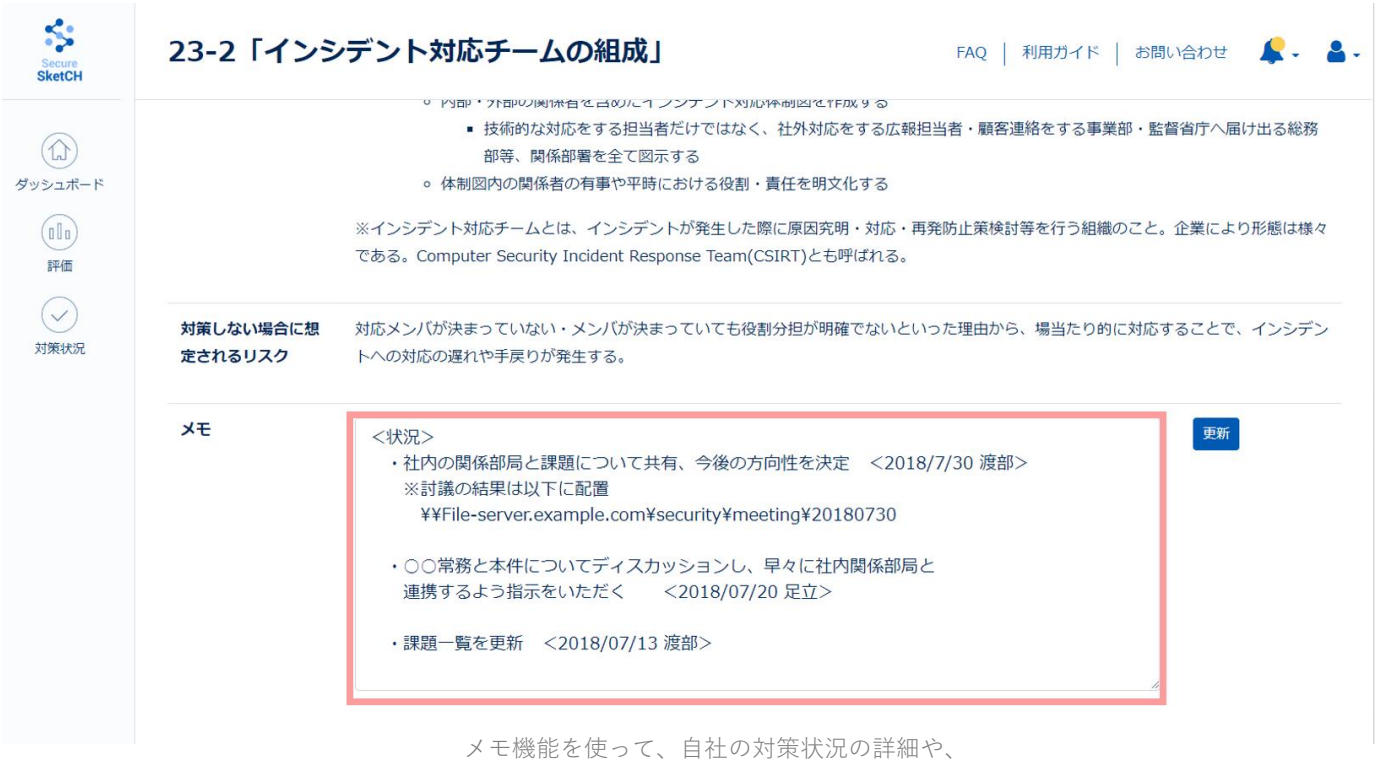
対策のシミュレーション機能で、対策実施後のスコアが分かる。

この機能により、自社のセキュリティ対策の中でどの部分ができていて、どの部分ができていないのかを知ることができます。そして、これを踏まえ、どこから対策をしていくことが最も投資対効果が高いのかを確認することができます。したがって「このセキュリティ対策は実施するべきか？」と迷うような場面でも、自社の状況把握がすぐにできるので、判断がしやすくなるでしょう。

活用術② 社内の状況や必要な情報を集約する

セキュリティ対策の見直しや、セキュリティ関連のルール・ポリシーなどを改訂していく際には、現状を俯瞰する必要があります。しかし、多くの企業では、カテゴリごとの対策状況などは、資料としてはあるものの、それらが「どこにあるのか」、「誰が詳細を知っているのか」、「今の状況はどうなっているのか」などの情報が把握しにくいケースが見受けられます。

そんなときは、Secure SketCHの「メモ機能」を活用してみましょう。Secure SketCHの対策項目は78個あります。それらの項目を開き、メモの部分に自社の対策状況の詳細や、資料の場所、担当者、対策の進捗状況などを書き込んでいくのです。



メモ機能を使って、自社の対策状況の詳細や、
資料の場所、担当者、対策の進捗状況などを書き込むことができる。

こうすることで、Secuer SketCHが自社のセキュリティのインデックス（索引）になるため、必要な情報にすぐに辿り着くことができるようになります。

活用術③ 有識者のナレッジを参照する

自社のセキュリティ対策を、「何から」、「どのように」進めていけばいいか、迷うケースもあると思います。そんなときは、Secure SketCHの「対策優先度」と「対策のベストプラクティス」を確認してみましょう。

対策は有識者が定義した「優先度順」にソートすることができる。

すべての対策の「ベストプラクティス」が参照できる。

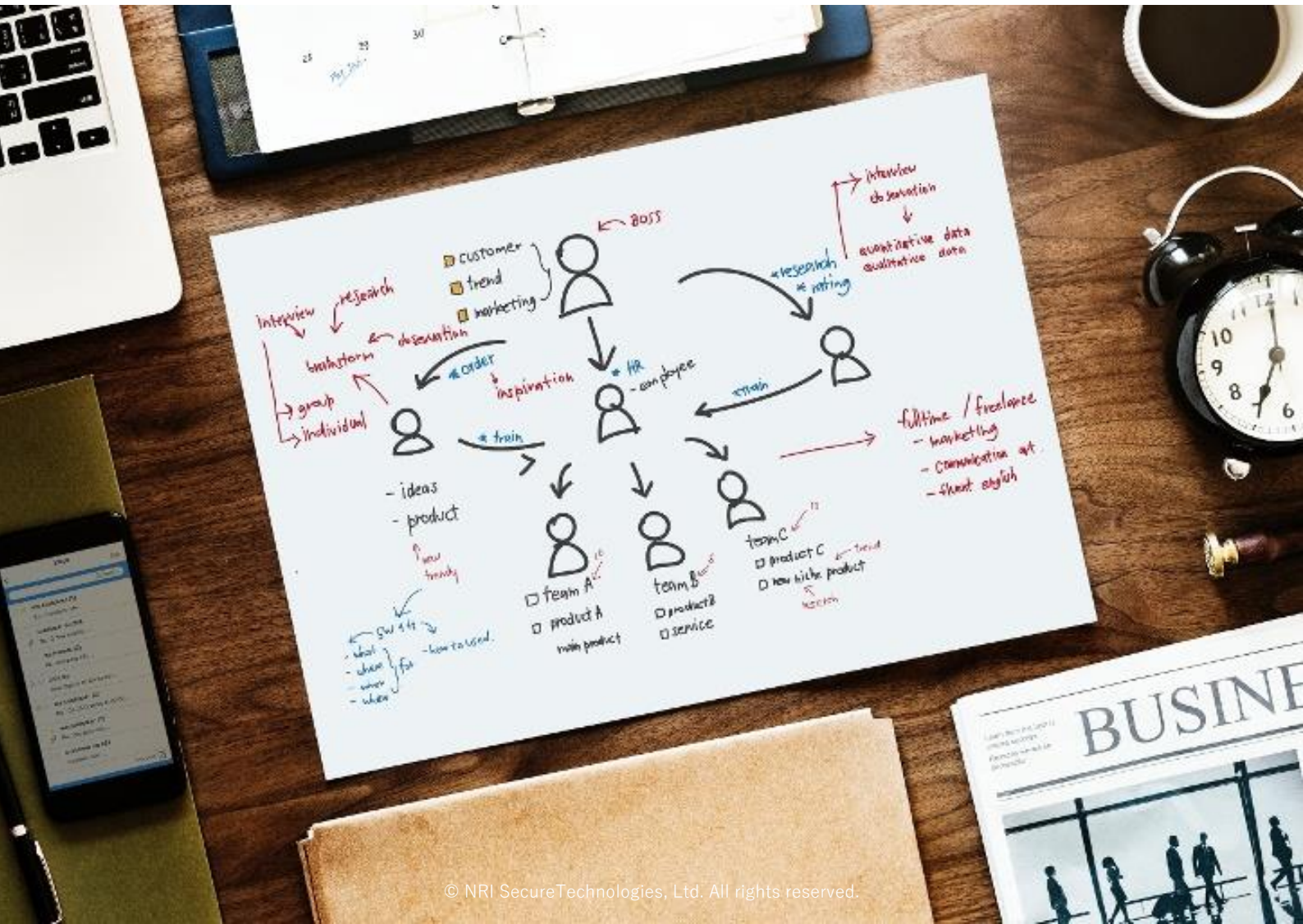
対策の優先度と、ベストプラクティスは、NRIセキュアのコンサルタントが、過去に実施したセキュリティ評価などの情報を基にして定義したもので、セキュリティ脅威やソリューションのトレンドによって、常にアップデートを繰り返しています。例えるなら、セキュリティの有識者がいつもそばにいて簡単なアドバイスがもらえるような機能です。

4. おわりに

世の中は今、未曾有の「セキュリティ人材不足」の時代になりました。今後さらにビジネスのデジタル化が進み、セキュリティ脅威が複雑化していくと、その傾向はより顕著になっていくでしょう。

そんな時代にビジネスで勝ち残っていくためには、デジタル化による「アクセル」で事業を加速させるとともに、情報資産を守るためにセキュリティ人材が適切なポイントで「ブレーキ」もかけられるような体制を整備する必要があります。

貴重なセキュリティ人材のリソースを最大限に有効活用するために、セキュリティ業務の効率化に取り組むべきです。その際に、Secure SketCHが皆様の業務を変えるきっかけになれば、これほど嬉しいことはありません。今こそ、Secure SketCHを使って、セキュリティ経営を「シンプル」にしてみましょう。



参考：Secure SketCHへの登録方法

かんたんな３ステップで、Secure SketCHの登録が完了します。

Step 1. メールアドレス登録

メールアドレスを入力し、「利用規約」および「個人情報の取扱いについて」の内容をご確認いただき同意の上、登録します。

Step 2. 企業情報登録

登録したメールアドレス宛に「企業情報登録のお願い」が届きます。
メールに記載されているURLにアクセスし、ご自身の企業情報を登録します。

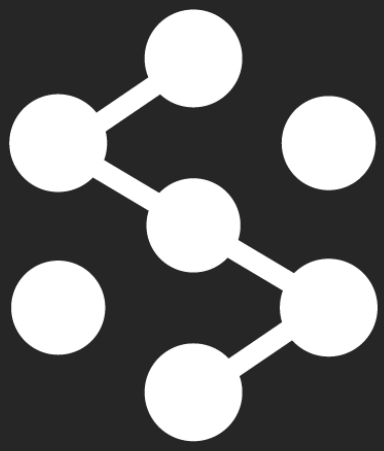
Step 3. 対策状況回答

企業情報登録完了後、登録したメールアドレス宛に「会員登録完了のお知らせ」が届きます。
メールに記載されているURLにアクセスし、ログインパスワードを設定後、セキュリティの対策状況に関する質問に回答します。

＜診断結果の表示＞

その場で診断結果が表示されます。
以後、登録したアカウント情報でログイン頂くと、いつでも結果が閲覧できるようになります。

FREEプランを使って、まずは無料診断を



Secure SketCH

セキュリティを、シンプルに

https://www.secure-sketch.com