SecurityScorecard

サプライチェーンにおける
リスク管理と
スコアリングサービスの応用

OptimizingYourSecurity

iSiD

内容

初版　　2020 年 4 月 27 日

はじめに

本書では、様々な企業におけるサプライチェーン、グループ企業のセキュリティ管理と、その効率化のためのセキュリティスコアリングサービス利用モデルについて解説します。

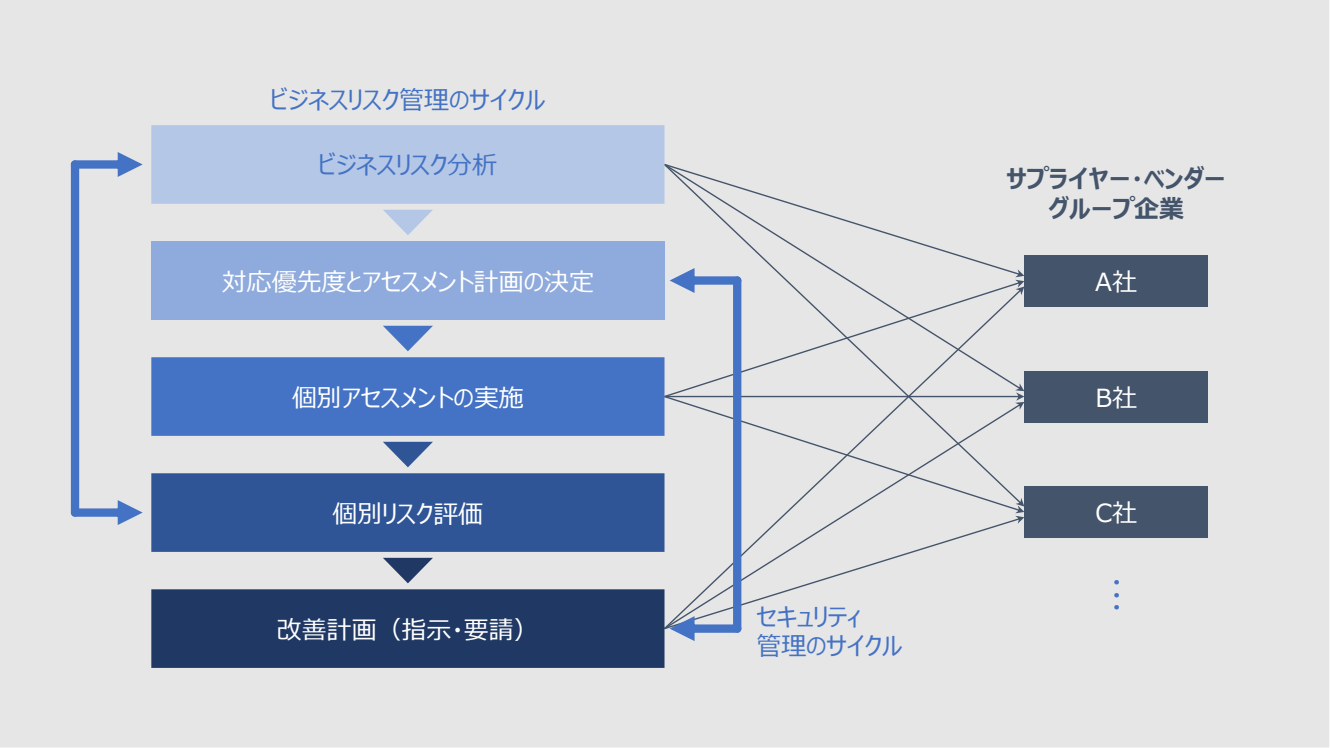
なお、本書で解説するモデルは一般的な業務モデルを元にしており、お客様によっては、そのまま適用が難しい場合もございます。なお、スコアリングサービス（Security Scorecard）の詳細につきましては、弊社スタッフにお問い合わせください。

1．企業におけるサプライチェーンリスク管理

昨今、国際的な分業が進む中で、企業では業務の委託先やサプライチェーンの中で、様々なセキュリティ事故（インシデント）のリスクをかかえており、そうしたリスクをサプライチェーン（ベンダー）リスク管理の一環として、管理、軽減しようとする動きも顕著です。また、こうした考え方は、大企業において、連結決算対象となる子会社などの全体のリスク管理を考える場合にも役立ちます。以下では、そうした管理を行うセキュリティ管理部門もしくはリスク管理部門におけるグループ企業全体にまたがる、セキュリティリスクの評価と対応業務を考えます。

こうしたリスク管理は、一般に、以下のようなサイクルで行われます。ここでセキュリティリスクの管理は、より大きなビジネスリスク管理の一部と考える必要があります。

図 1 リスク管理のサイクル



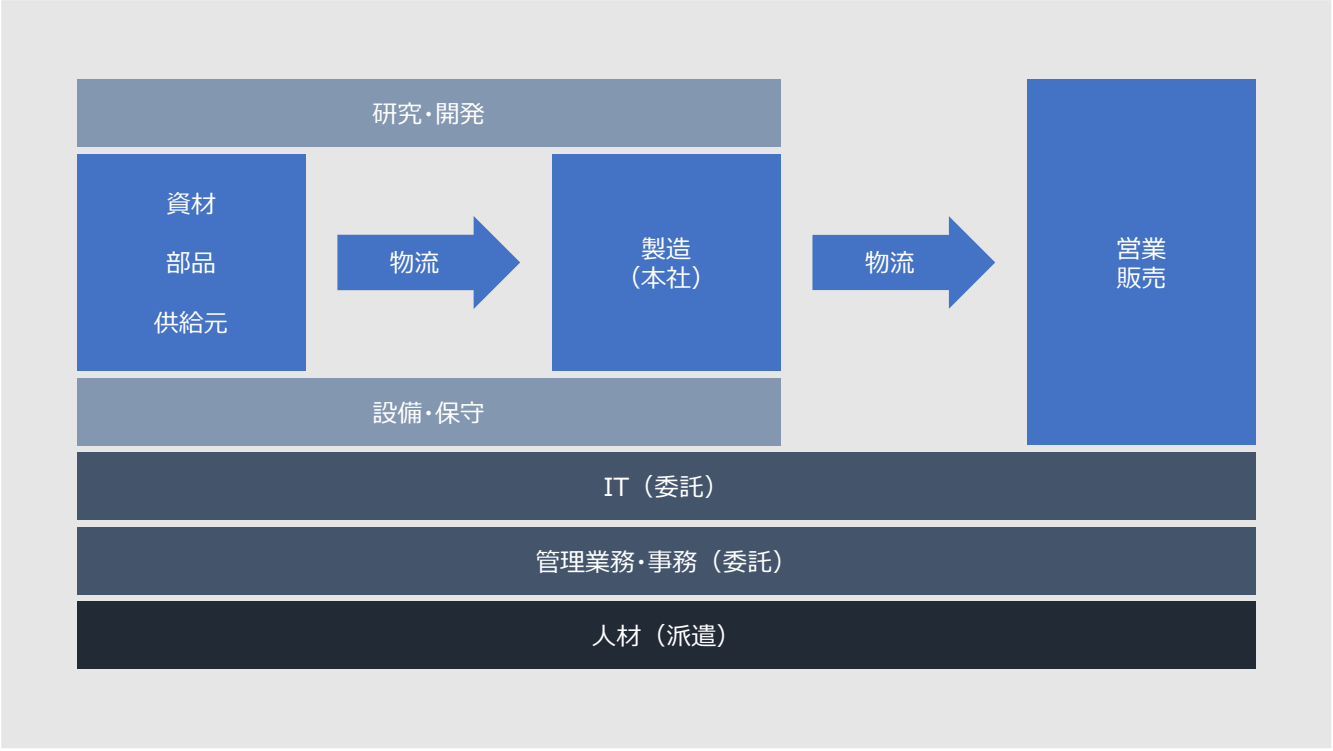
ビジネスリスクの分析では、対象となる企業が自社やグループ全体のビジネスのどのような部分に影響を与えるかの分析が欠かせません。こうした分析のありかたを少し考えて見ます。

(1) 製造業におけるサプライチェーンリスク分析

ここで想定する企業は、自動車、電機など、複雑なサプライチェーンと販売網を持ち、多くのグループ企業を持つような製造業です。

サプライチェーンを担う企業には様々な機能を持った会社があります。本来、ひとつの会社が持つべき機能をグループ企業や委託先に分散し、それぞれ独立したビジネスを構成しています。以下は、その簡単なモデルです。

図 2 グループ企業の機能



この例では、本社は製品の製造に特化しており、それに必要な機能が集中しています。製品の研究開発、部品や資材の供給、製品の営業・販売などの流れの各部分は分社化されており、さらに、それらに必要な設備の供給や保守、IT、主要な管理業務、人材の供給（派遣）などは、同じくグループ企業や外部に委託されています。

セキュリティインシデントの発生は、各企業に様々な影響を与えますが、こうした機能別の観点から見ると、それぞれがはたす機能によって、ビジネスに与える影響が大きく変わります。こうした企業の情報セキュリティを考える場合、機能をもとにしたビジネス全体への影響分析が欠かせません。製造業において考えるべきセキュリティリスクにはいくつかの種類があります。ここでは、これらを重要情報の漏洩に関する「情報漏洩リスク」、製品の品質、性能などの低下をもたらす「品質リスク」、業務効率（業務維持）や生産性の低下、生産停止などをもたらす「業務効率・生産性リスク」の３種類に分けて考えて見ます。

たとえば、研究開発や試作品の製造などを担当する企業、販売会社、特にコンシューマを相手にする会社や関連する事務処理を委託している会社などは、情報漏洩に関するリスクが大きくなります。一方で、原材料や部品などを供給する企業は、品質リスクや業務維持に関するリスクも考慮しなければいけません。その影響を評価するにあたっては、こうしたリスクの中身をさらにブレークダウンし、たとえば取り扱う情報の種類や、品質、業務に与える影響の内容ごとに分析する必要があります。

以下は、そうした影響分析の簡単な例です。

表 1 影響分析の例

	リスクタイプ							
	情報漏洩リスク							
企業の種別	開発情報	設計情報	製造方法	生産計画	未発表製品	取引先情報	個人情報	その他
研究開発	◎	◎	○		◎			○
資材・部品供給元	△	○	○	○	△			△
物流会社						○	○	△
販売会社					○	◎	◎	○
IT会社	○	○	○	○	○	○	○	○
事務委託会社				△	○	◎	◎	◎
人材派遣会社	○	○	○	○	○	○	○	○

	リスクタイプ							
	品質リスク			業務効率・生産性リスク				
企業の種別	品質劣化	故障・不具合	製品事故	開発遅延	生産停止・遅延	配送遅延	販売数低下	業務効率低下
研究開発	○	○	○	◎	△			○
資材・部品供給元	◎	◎	◎	△	◎			
設備供給・保守					◎			○
物流会社	△	△			○	◎	△	
IT会社	△	△	△	○	◎	○	△	○
販売会社							◎	○
事務委託会社							△	◎
人材派遣会社							△	○

◎：リスク大　○：リスクあり（直接的影響）　△：リスクあり（間接的影響）

これは、ごく単純化した例ですが、まず、委託先の各社が自社のリスクにどの程度の影響を与えうるのかについて分析することが重要になります。(製造業の場合、これ以外に工場などでの安全に関するリスクも生じますが、それぞれの状況によって大きく変化するため、ここでは取り上げていません) リスクの大きさの評価を行うにあたっては、さらにその内容をブレークダウンする必要が生じるかもしれません。

(2) 子会社、グループ企業のリスク分析

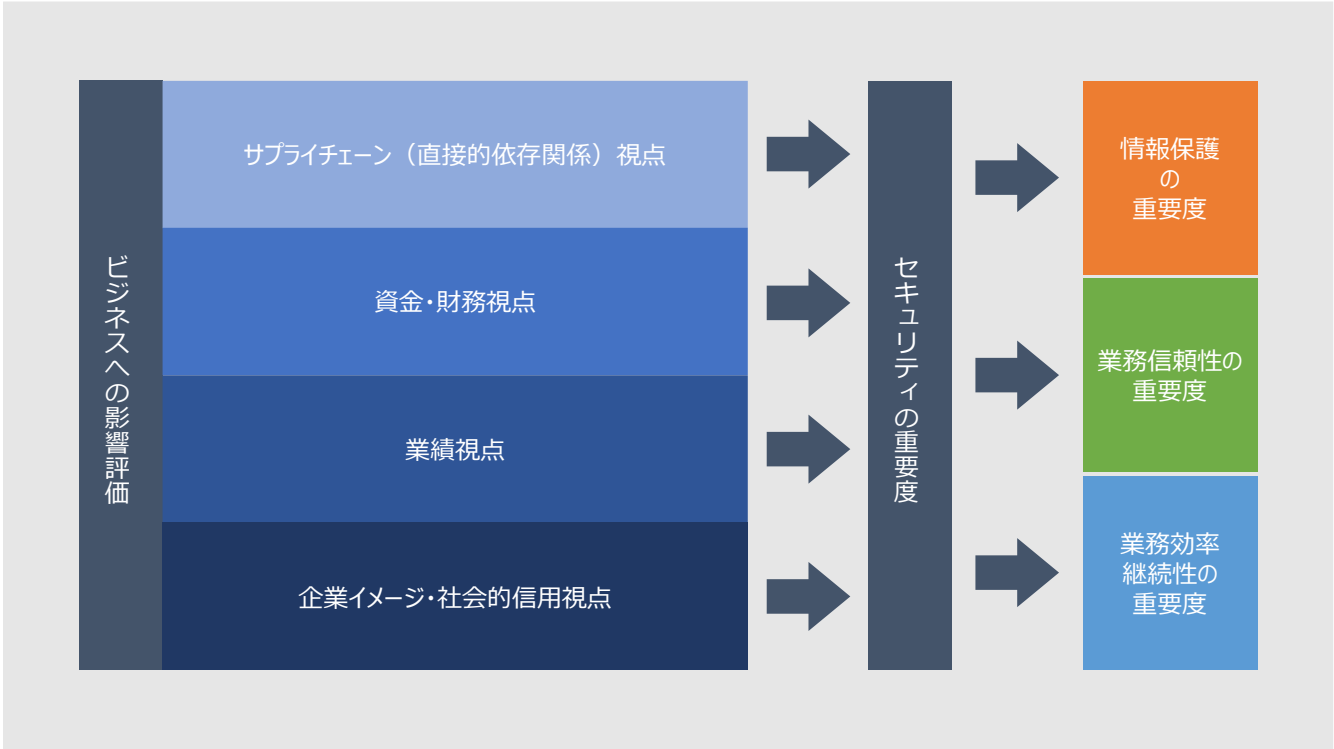
とりわけ、製造業においてはサプライチェーンの維持がビジネスにとって重要ですが、サプライチェーンに直接絡まない会社も含め、自社のグループ企業全体のリスク分析を行う場合について考えて見ましょう。

各社がグループ全体に与える影響、リスクについては、いくつかの切り口が考えられます。先に述べたサプライチェーンの視点での分析は最も重要なもののひとつです。製品やサービスのサプライチェーンに加え、自社の業務についてなんらかの依存関係がある会社については、この視点で分析します。たとえば、情報システムに関する委託先などは、業務の基盤を担う企業であり、業務効率や生産性の視点のみならず、情報漏洩のリスクなどについても分析しておく必要があります。また、金融、ファイナンス会社のような会社の場合は、資金、財務面での依存関係からの分析も重要です。その会社の業務の停滞や停止が運転資金や設備投資といったものに与える影響なども評価しておく必要があるでしょう。同様に、連結決算対象企業については、グループ全体の業績に対する影響も評価しておく必要があります。加えて、企業イメージや社会的な信用といった面での影響度評価も必要です。直接自社業務と関係なくても、たとえば大量の個人情報を保有しているグループ企業が情報を漏洩させれば、グループ全体のイメージ悪化に繋がりかねません。グループ内の看板企業的な企業で問題が発生すれば、グループ全体のイメージ悪化に繋がります。これらは一つの例ですが、関係する企業がビジネスに与える影響については、こうした複数の視点からの分析が不可欠です。

(3) ビジネスリスクと情報セキュリティリスク

では、情報セキュリティ上の問題が、これらのリスクにどう影響するのでしょうか。一般に、情報セキュリティでは、リスクを「機密性：Confidentiality」「完全性：Integrity」「可用性：Availability」の観点から評価します。秘密とすべき情報の漏洩は、「機密性」の問題です。重要情報が改ざんされたり不正確であったりすることは、「完全性」の問題、情報がタイムリーに利用出来なくなることは、「可用性」の問題として捉えます。ブレークダウンされたビジネスリスクのそれぞれに対して、情報セキュリティの、どの切り口で考えるべきかの分析も重要となります。言い換えれば、ビジネスリスクが「情報保護」「業務の信頼性や正確性」「業務の効率性や継続性」のいずれと関連するかを明らかにしていくことが重要です。

図 3 ビジネスリスクとセキュリティ



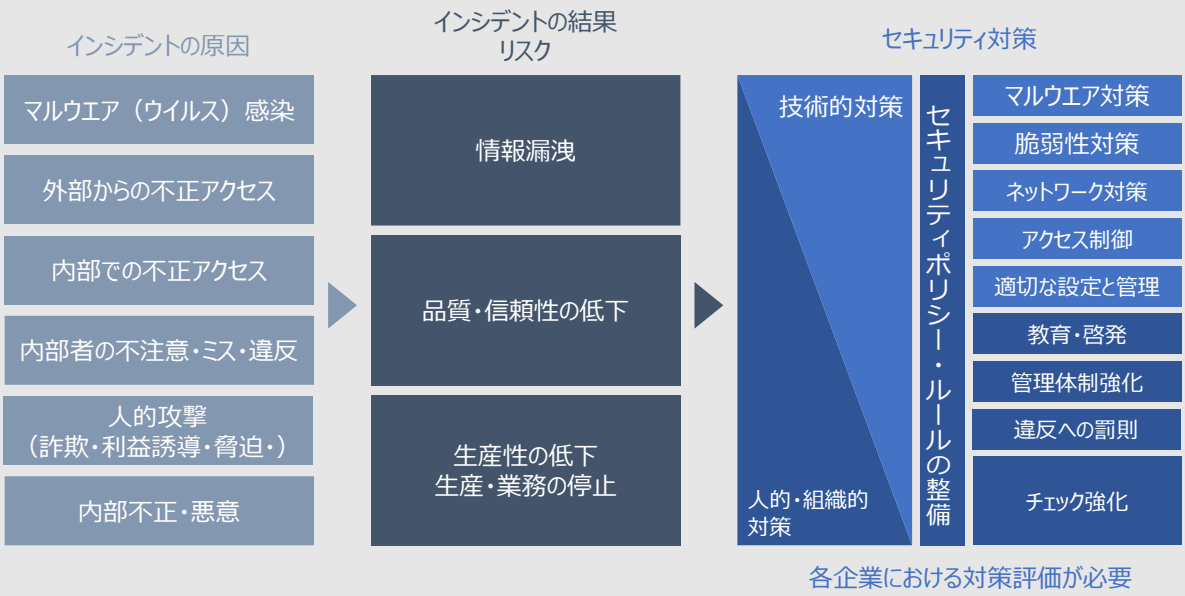
それでは、こうしたリスクをもたらすセキュリティインシデント（事故）原因には、どのようなものがあるでしょうか。以下に、重大な影響をもたらしうるものを挙げてみましょう。

- マルウエア（ウイルス）感染
- 外部からの不正アクセス
- 外部からのサービス妨害
- 内部での不正アクセス（故意・偶然）
- 内部者の不注意・ミス・ルール違反
- 内部者への人的攻撃（詐欺・利益誘導・脅迫などによる不正行為のそそのかしなど）
- 内部者の不正・悪意

これらのいずれもが、先に述べたすべてのリスクをもたらす可能性があります。たとえば、近年のマルウエアの多くが、いわゆる「遠隔操作型」であり、攻撃者の指示に従って、様々な侵害行為を実行します。当然、情報の持ち出しや改ざんといった行為が行われる可能性があり、さらにコンピュータの処理妨害や最悪の場合、コンピュータが利用不可能になることを考えれば、「機密性」「完全性」「可用性」のすべてに対して重大な脅威となり得ます。直接的なサービス妨害、たとえばシステムにアクセスを集中させ処理を妨害するといった攻撃を除けば、ほぼすべてのインシデントが「機密性」「完全性」「可用性」のすべてに影響を与えてしまいます。

従って、少なくとも、こうした原因を排除するような最低限の対策（基本的対策）が必要になります。対策には、その基本となるセキュリティポリシーや各種のルール、ガイドラインの決定や従業者、関連企業への教育、啓発といった人的、組織的なものと、マルウエア対策や脆弱性対策のような技術的な対策があります。こうした対策とインシデントの原因、影響を図にまとめると以下のようになります。

図 4 インシデントの原因・結果と対策



先に述べたようなインシデントは、いずれの企業でも発生する可能性があります。つまり、最低限の基本的な対策、たとえばパスワードの管理、ウイルス対策ソフトなどの導入や、ソフトウエアのセキュリティ更新の適用といった技術的対策、基本的な情報の取扱などについての最低限のルール作りなどの組織的対策は、企業を問わず必要となります。その上で、リスクの大きさに応じた追加対策を講じていく必要があるのです。

グループ全体を統括するセキュリティ管理部門の役割は、まず、こうしたリスクの分析を通じて適切な対策方針を決定し、グループ全体で確実に実施されるように指導、監督することです。

2．グループやサプライチェーン全体の IT セキュリティ管理モデル例

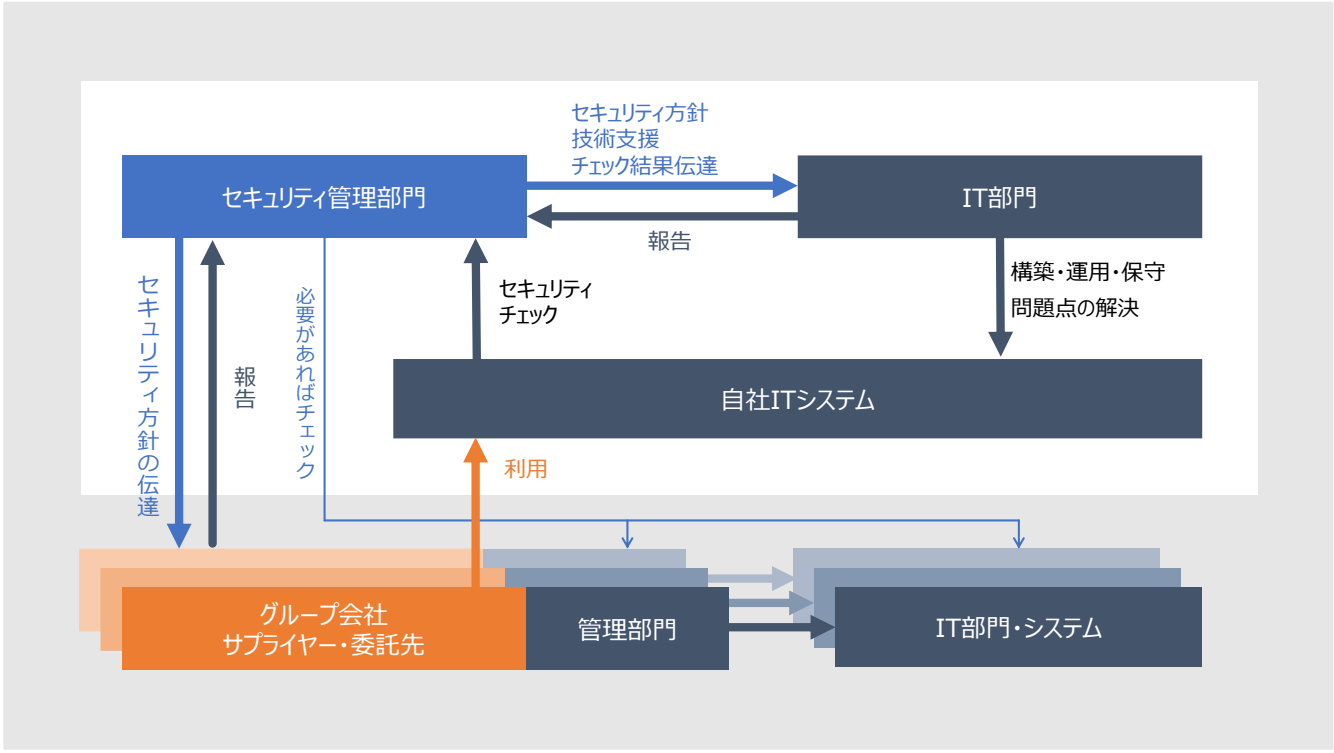
近年、大規模な企業グループにおいても、セキュリティ管理の集中化が行われる傾向が強くなっています。これは、すべてのグループ会社において同レベルの管理体制を作ることが難しいことや、各会社間での情報連携がより重要になっていることなどが原因です。また、IT については、各グループ会社が独自の IT 基盤を持つケースや親会社もしくは他のグループ会社の IT 基盤を共用する場合もあり、たとえば脆弱性の修正といった作業を誰が、誰の指示で行うのかといった指示・連絡の系統も複雑化しがちです。セキュリティ上の問題をいち早く認識して、速やかに対処するためには、こうした指示、連絡系統の一本化が極めて重要です。

さらに、仕入れ先、業務委託先といったサプライチェーン全体を考えると、管理部署が直接対応出来る部分は極めて限られることから、セキュリティやリスクの管理に関する円滑なコミュニケーション維持は非常に重要となります。

(1) 集中管理モデル

ここでは、グループ全体を主管するセキュリティ管理部門が、グループ全体のセキュリティ方針を決め、それを管理するようなモデルを想定します。セキュルティ管理には前述したように様々な側面がありますが、ここでは、IT に関する技術的な部分を切り出したモデルを考えます。

図 5 IT セキュリティ管理のモデル



この場合、管理部門はグループ全体のシステムを管轄する IT 部門やグループ会社の IT 部門（もしくはセキュリティ管理部門）に対し、行うべきセキュリティ対策についての方針を提示し、それが確実に実施されているかどうかをチェックする役割を担います。セキュリティ管理部門は、必要があれば技術的なチェックを

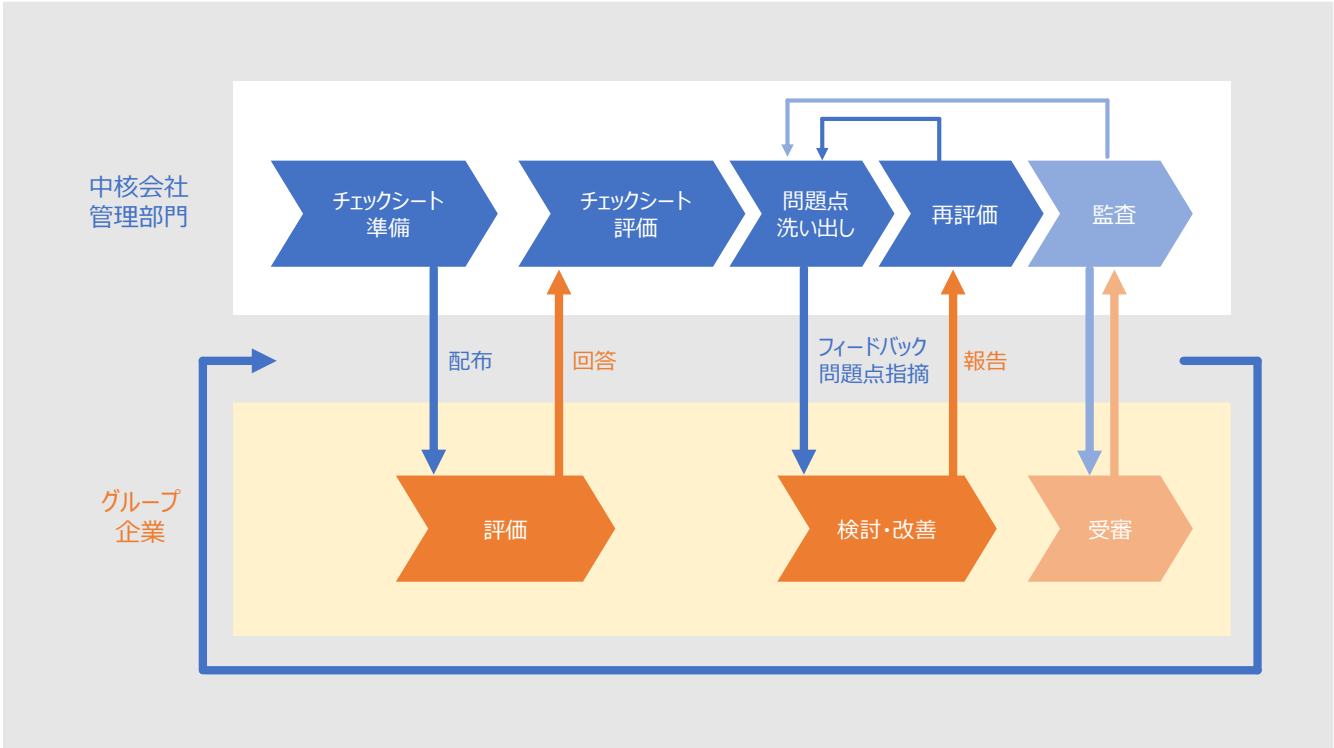
IT 基盤に対して実施し、対策方針に沿わない状況があれば、IT 部門やグループ会社（の IT 部門）に対し是正を促します。

本来ならば、セキュリティ管理部門は、図 4 のような脅威の流れをさらにブレークダウンし、グループ企業における、どのようなインシデントが、それぞれのリスクに結びつくのかを見て、それぞれの対策基準を考えるのですが、その作業はかなり繁雑です。本社の管理部門が、こうした分析をすべて行うことは現実的に困難です。多くの場合、主要なセキュリティ対策の実施状況を調べ、その状況をもとに、こうした個々のリスクの大きさを推定することになります。一般的なセキュリティ対策の実施状況と様々なインシデントが発生する危険性には関連があり、こうした対策の不備が多いほど、インシデント発生の可能性が高まると考えられるからです。

(2) セキュリティ管理部門の課題

しかし、多くの対象企業を擁する大企業では、こうした実施状況の調査そのものが、大きな労力を必要とします。従って、多くの場合、直接的な調査ではなく、自社（グループ）のセキュリティポリシーや各種のセキュリティ標準に基づく対策チェックシートなどを用意し、その回答を集めて一次評価を行うことになります。もちろん、こうした回答の信頼性は相手企業に大きく依存します。そこで、定期的な監査を実施し、回答内容と実態が整合しているかどうかを確認することになります。

図 6 グループ企業のセキュリティ対策管理



監査は回答の信頼性を維持するために重要ですが、年に一度の監査であっても、対象が多い場合は管理部門の負担となります。とりわけグローバルに拠点やサプライヤーを持つ企業では、多くの困難を伴います。また、限られた時間で可能な監査項目は多くない上、とりわけ技術的な項目については詳細なチェックは困難です。こうした監査では、なかなか総合的な問題指摘は困難と言わざるを得ません。チェックや指摘事項が

限定的であれば、指摘された部分だけを改善すればいいといった風潮を生み出す可能性もあります。また技術的なチェック、たとえば脆弱性検査のようなものを補完的に実施することもできますが、これには時間とコストを必要とするため、人員や予算上の制約から十分な実施が出来ないケースも少なくありません。

多くのグループ会社やサプライヤーをたばねるセキュリティ管理部門は、常にこうした課題をかかえています。

3．グループ企業のセキュリティ管理におけるスコアリングサービスの利用

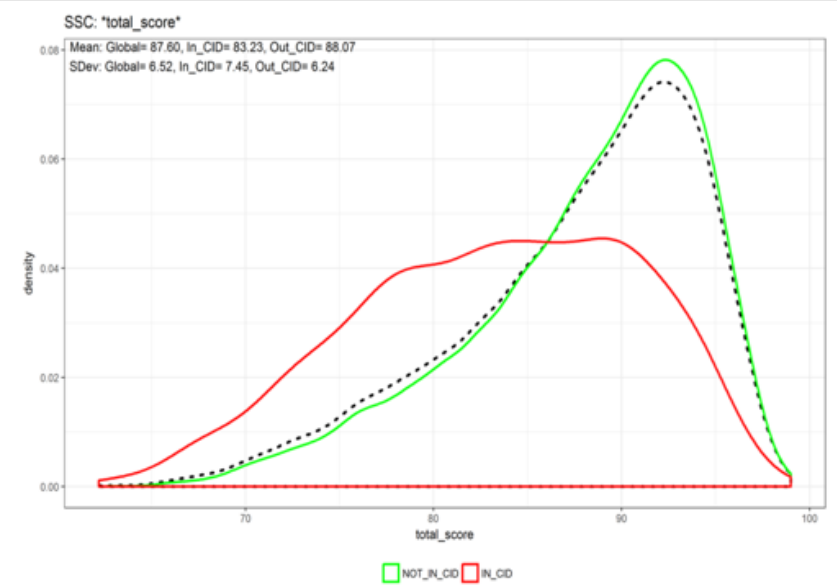
近年、第三者的に企業のセキュリティ状況をスコア化するスコアリングサービスが提供されるようになりました。ここで紹介する SecurityScorecard（SSC）もそのひとつです。こうしたサービスをうまく活用することで、セキュリティ管理部門は、様々な業務を効率化することができます。

SSC の特徴は、簡単に、様々な切り口から対象企業のセキュリティ状況を把握できる点です。また、その情報は定期的に更新されるため、最新の状況とこれまでの経過を合わせて把握でき、ある時点での状況だけでなく、改善もしくは劣化の過程も捉えることが可能です。SSC はインターネットの側から、調査対象への負荷を最小限に抑えた形でのスキャンと、当該ドメインに対する様々なインテリジェンス情報をもとに評価を行います。一般的な脆弱性検査などとは異なり、網羅的な評価ではありませんが、当該ドメイン管理組織のセキュリティ対策に対する取り組み､姿勢などを評価するために重要な項目を押さえており､そのスコアは、調査対象外のものや内部の対策も含め、全体的なセキュリティ対策とその運用への取り組み姿勢を反映していると考えることができます。これを利用することで、セキュリティ管理部門は、業務の効率化に加え、対策を行う理由や成果をスコアによって数値化できます。管理部門の説明責任やパフォーマンスの検証強化にも役立ちます。
以下に、いくつかの使い方を挙げてみます。

(1) リスクによる対応優先順位決めへの利用

多くの対象企業に対する評価と管理は、リスクの高い順に優先度をつけて行う必要があります。リスクはその企業のビジネス全体もしくは特定の業務への影響度の大きさとスコアの「低さ」とに相関します。

図 7 スコアとインシデント発生の関連

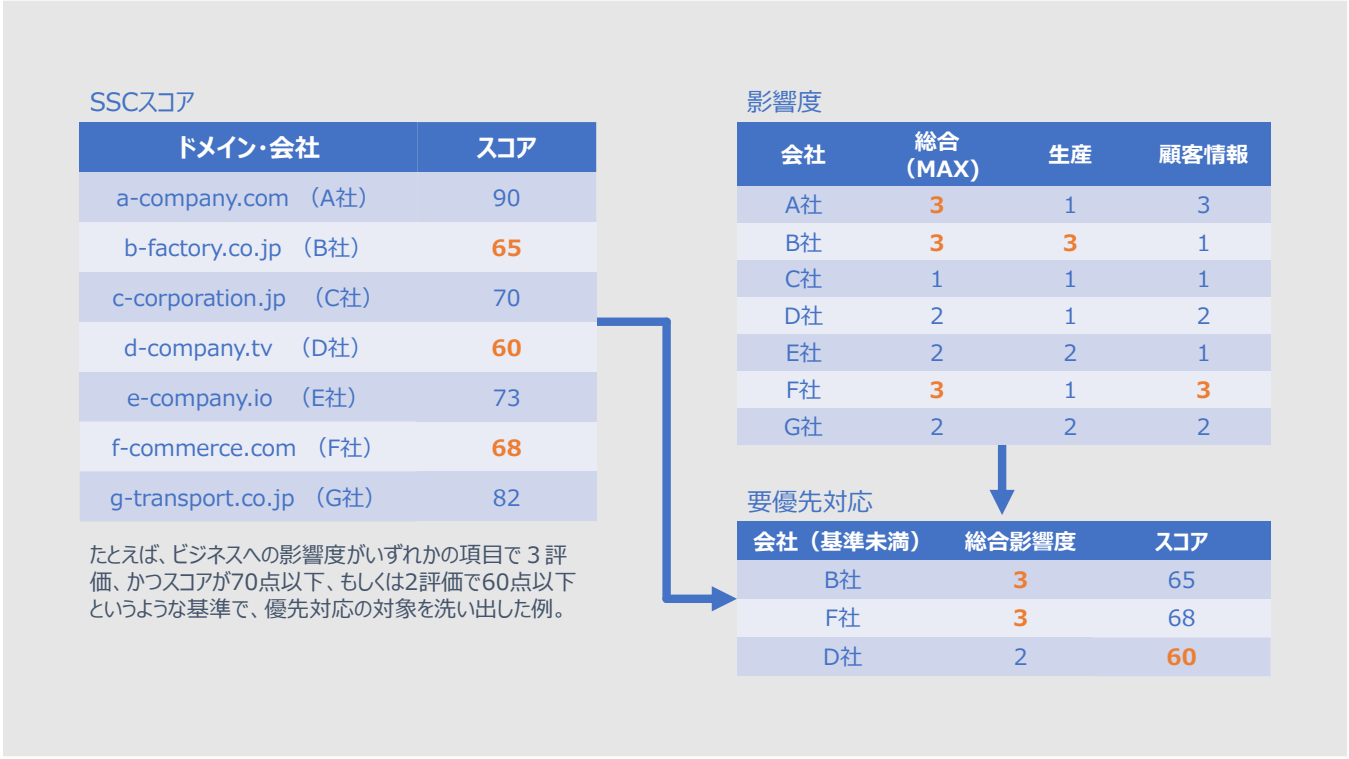


セキュリティ保険会社向けの調査機関RMSによる検証で、セキュリティインシデントを経験した企業と経験していない企業のSSCのスコア分布を比較した結果、インシデントを経験した企業において、明らかにスコアが低い傾向がみられた。

SSC から提供された約 60000 社のスコアをもとに、調査機関 RMS が、独自のインシデントデータベースと比較した結果、セキュリティインシデントを経験した企業群は、そうでない企業群にくらべ、明らかにスコアが低い傾向がみられました。こうした結果から、スコアがその企業の全般的なセキュリティの状況と相関していると考えることができるでしょう。

従って、ビジネスへの影響度が大きな企業でスコアが低いケースがあれば、全般的なセキュリティ対策状況の不備による大きなリスクの存在を示唆するため、最優先で対応しなければいけません。たとえば、総合スコアや特定のカテゴリーのスコアが基準に満たない企業を抽出し、これを影響度の順に並べ替えれば、そうした優先順位を決めるために利用することができます。こうした情報をもとに指導を行えるほか、直接的な監査やより網羅的な脆弱性検査などを行う必要性を判断することもできるでしょう。

図 8 優先度判定の一例



(2) チェックシートの信頼性検証

定期的に行われるヒアリングや対策状況チェックシートなどの裏付けとして、SSC のスコアを利用することができます。たとえば、脆弱性対策に関する項目についてチェックシート上で問題が無くても、スコアが悪いといった状況があれば、チェックシートの信頼性に疑問が生じます。監査を行うまでもなく指摘が可能になるほか、直接監査の必要性の判断や、不正確な回答に対する牽制が可能です。SSC で検証が可能な項目をサンプル的にチェックシートに織り交ぜておけば、その検証によって、全体的な回答の信頼性を推定することができるでしょう。

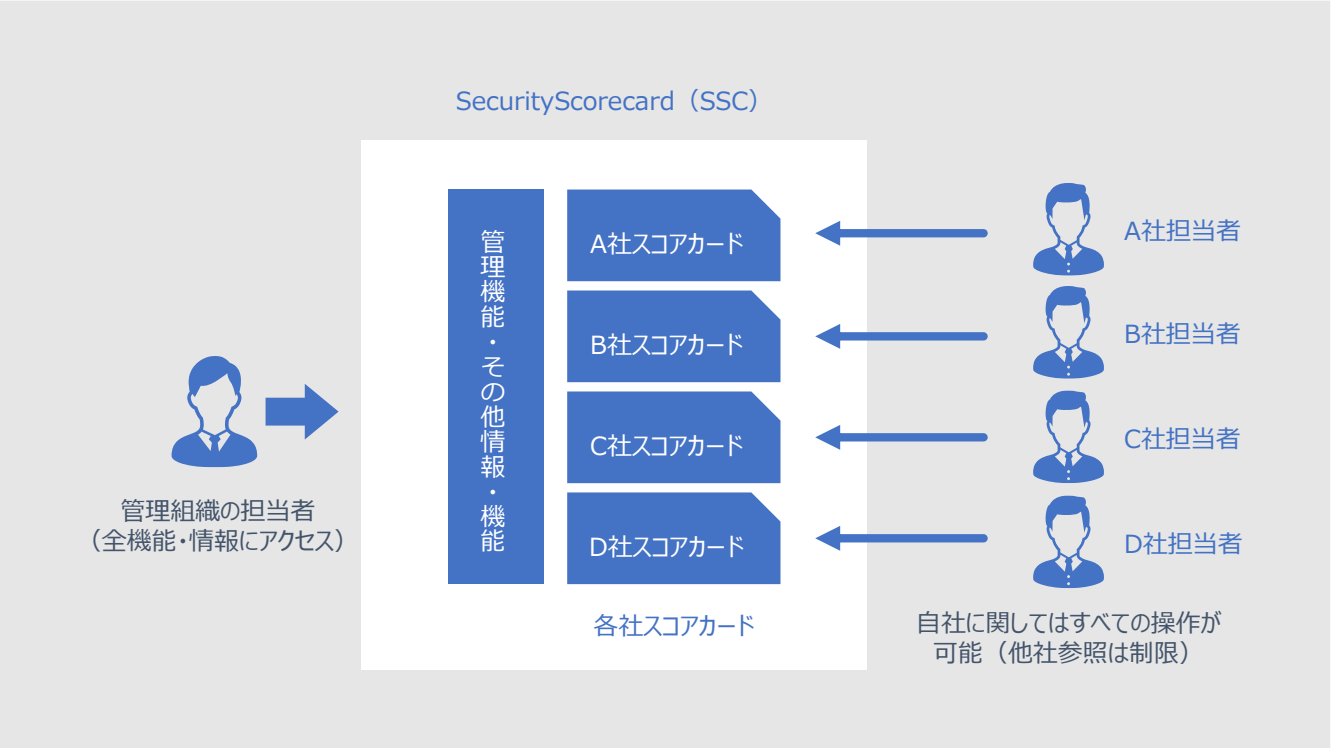
(3) 管理部門やグループ企業の KPI としての利用

セキュリティ管理部門が、その活動を通じて改善できたグループ全体のセキュリティ対策状況を数値的に可視化することができます。これにより、たとえば、平均スコアの向上、最低スコアの底上げといった目標を数値化し、測定することが可能になります。また、評価対象企業（組織）の管理主体に対して、目標とすべきスコアを示すことも可能です。

(4) セルフサービス化によるセキュリティ文化の醸成

SSC のカスタムスコアカードやポートフォリオを使用することで、特定企業、ドメインの状況を抽出したページを作成できます。各企業の管理担当者に SSC のアカウントを与え、アクセスを自組織のポートフォリオのみに限定すれば、簡単なセキュリティポータルサイトとして使うことが可能です。これにより、各組織の担当者（あるいは管理者、経営者）は、自組織の状況や、実施した改善作業が反映されたスコアなどを直接知ることができ、それが、自主的なセキュリティ改善のモティベーションに繋がります。

図 9 セルフサービスのイメージ



以上のように、スコアリングサービスは、ビジネスに関連する企業全体のセキュリティ管理において多くのメリットをもたらします。上手に利用すれば、管理業務の効率化に大きく貢献するでしょう。

著者略歴

二木真明　（ふたぎ　まさあき）　CISSP, CISA

アルテア・セキュリティ・コンサルティング　代表

株式会社電通国際情報サービス　金融ソリューション事業部
セキュリティビジネス技術戦略アドバイザー

17 年間の制御系、UNIX 系プログラマー、SE としてのキャリアの中で、ファイアウォール製品を開発し、商品化したことから情報セキュリティの世界に踏み込む。その後、現在まで 20 年近く、情報セキュリティの様々な分野で経験を積んだ。2000 年以降は、大手商社系 SIer に勤務し、海外セキュリティ製品の発掘や技術評価などにたずさわる一方で、自社内の情報システム部を兼務し、様々なセキュリティ対策の導入やルール整備、社内 SOC の業務等を主導した。2012 年に独立して、その後は情報システム部時代の経験を活かして、主にユーザサイドの様々なセキュリティ案件の支援や技術戦略面からセキュリティベンダーのビジネス支援を行っている。

その他経歴等

2014 年 4 月～2017 年 3 月　埼玉県警察サイバー犯罪対策技術顧問
CSA ジャパン（一般社団法人日本クラウドセキュリティアライアンス）運営委員
JNSA（日本ネットワークセキュリティ協会）幹事