Deloitte.
デロイト トーマツ

# 勘違いセキュリティ
# 規程類はなぜ重要なのか？

～単なる“読み物／紙っぺら”ではない、その意義を読み解く～

## 規程類が理解されず軽視されている ？

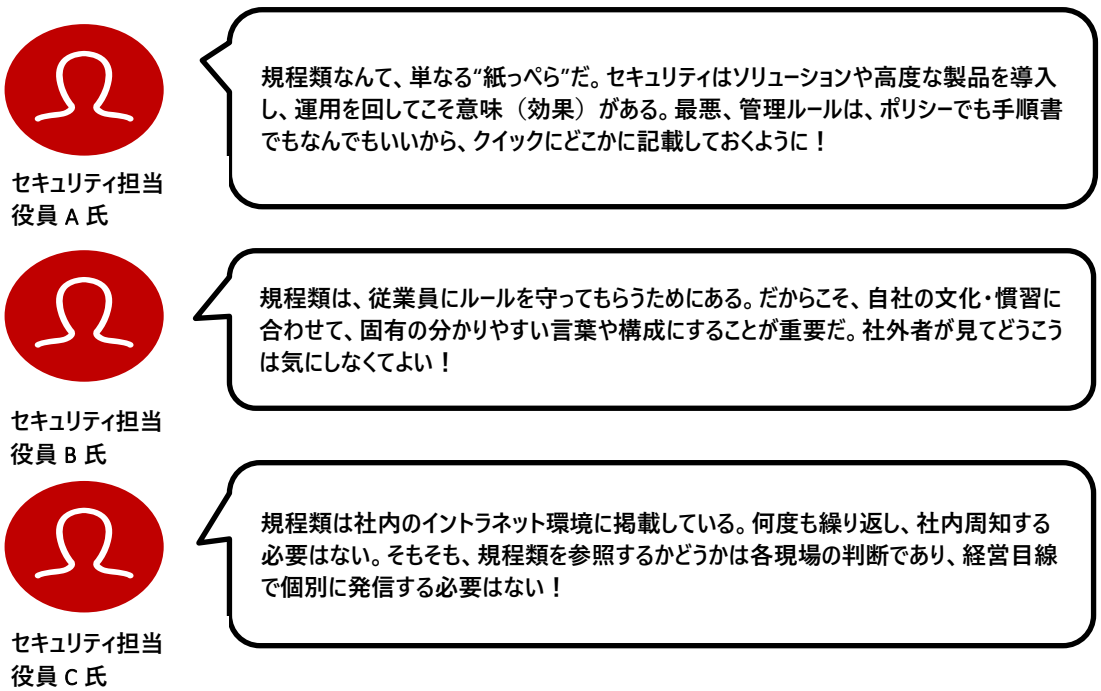
近年、セキュリティは重要な経営課題として認識されている。企業には、様々な部門が存在し、人事・経理・総務・IT 管理等のバックオフィスに関わる部門から、研究・開発・生産・販売等の基幹業務に関わる部門まで多岐に渡る。各部門に対して、組織共通的に定めたセキュリティ管理のルールを理解・浸透させるためにも、規程類は重要な位置付けとなる。

一口に規程類といっても、その種類は様々であり、方針・規則・要領・手順書等、組織に応じて様々な種類および名称の文書が存在する。また、テーマによっては、法規の要求事項を踏まえたより厳格な文書として位置付けられるものも存在する。

ただし、この規程類に関して、本質的な意義が理解されない、または、軽視されるケースも散見される。さらには、結果的にセキュリティインシデントが発生しなければ、規程類があろうがなかろうが、さほど問題にはならないだろうという意見や、規程類がなかったとしても、実際の運用業務が円滑に回っているなら、それにこしたことはない、という極論的な意見を聞く機会もある。

以上を踏まえて、規程類の意義が理解されずに発言されてしまった誤解の例として、複数企業におけるセキュリティ担当役員 A 氏, B 氏, C 氏の発言を見てみたい。

**誤解されている例とは**




上記 3 名の発言は、いずれも規程類の本質的な意義を誤解していると判断できる。では、どのような点がイシューとなるのだろうか？以降、考察を通じて紐解いてみよう。

### イシュー①：そもそも規程類は何のためにあるのか？

規程類の意義として大切なことは、共通のルールとして遵守されることである。そのためにも、現場の従業員目線で見て、内容がわかりやすくまとまっていることは重要である。

ただし、もう１つとして、社外関係者の目線もある。社外関係者が規程類を見た際に、どれだけ客観的な納得感を持てるかは重要である。例えば、セキュリティに関わる認証取得時や、外部機関による公的な審査を受ける際、さらには実際のインシデントが発生した際の監督官庁への報告等を考慮すると、規程類は社外関係者の目に触れる機会もあると言える。その際、社外関係者は何を見るか・・当然、個々の規定の妥当性は重要である。ただし、もう１つ重要な論点がある。「その文書（規程類）を誰がコミットしているのか？」である。

規程類は、ともすれば単なる紙資料として、絵に描いた餅のオンパレードになりがちである。そうでなく、組織として正式に実現可能なものであると認識され、かつ、それを然るべき人物が経営責任の一環としてコミットしていることが重要となる。以上を踏まえた重要な論点としては"当該文書の最終承認者"である。

説明責任（アカウンタビリティ）という意味で、企業におけるセキュリティ管理に起因する重大な脅威が顕在化した場合、監査機関及び監督官庁対応等において、最初に問われる傾向にあるのが規程類の整備状況である（特に上位の方針・要件をまとめた文書）。

では、「当該文書の最終承認者」は、どのように確認すればよいのか。その前段として、当該文書が全体の枠組みの中で、どのような位置付けの文書となるのか。まずは、一般的な考え方を基に、考察してみたい。

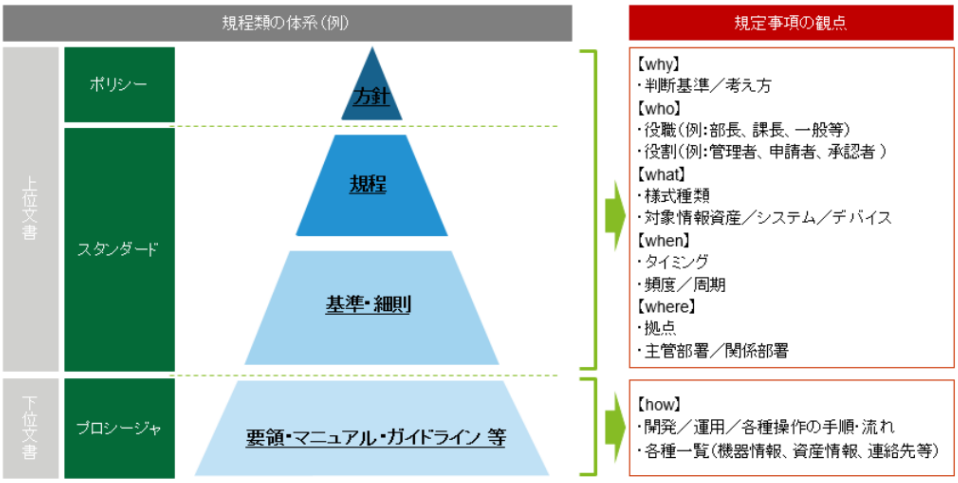



図１：規程類の全体像

規程類には上記図１のような種類がある。各組織によって、種類の粒度・数はまちまちであるものの、一般的には、その種類は「規程類管理規程（例）」「規程等管理規程（例）」のような名称の文書に定義されている（文書名はあくまでも例示であり、企業によって様々）。そして、この文書には、一般的に以下のようなことが定められる。

- 規程類の分類（定義・序列）
- 規程類の承認者
- 規程類の内容（規定事項）
- 規程類の効力範囲
- 通達の種類
- 規程類の改廃方針

実際にインシデントが発生した場合、社内のセキュリティ管理の実情を問われることになるが、説明の序盤で主に問われる事項は、規程類の全体像であり、その中で各文書がどのように策定されているか、また、各文書の内容だけでなく、最終的に責任を負う人物の役職及び主管組織等が問われる。もし、当該文書を最終的に承認した人物が、組織における下位の管理職である場合、果たしてその規定事項は、本当に組織として認められたものであるか、また、承認過程における妥当性の検討は十分だったのか、等の疑念を与える危険がある。

そして、このような心象を与えてしまうと、上位の文書だけでなく、より現場レベルの手続きを規定した詳細レベルの手順書や具体的な運用証跡（各種様式類）の網羅的な提示を要求される可能性もあり、説明責任の遂行が難航する危険もある。

### イシュー②：規程類は、誰のためにあるのか？

当社では、セキュリティに係る規程類策定に関する相談を数多扱っている。その際に多い話題として、「自社の従業員が理解しやすいように、わが社の風土・作法に合った文書に仕立てたい」という意見がある。

確かにそれも重要である。実際、社内の従業員が理解できない内容であれば、身も蓋もない。そのため、我々としては極力、既存の関連規程類やクライアント社内の文書管理ルールに会わせて平仄を合わせるための助言・指導を行うことも多い。

ただし、これは行き過ぎると危険である。社内では通用しても、社外者が見た際に果たしてどうなのか、という懸念が生じる。例えば、昨今流行っている「サプライチェーンリスク管理」については、サプライチェーンという言葉に多面解釈の余地があるため、「調達・委託に際しての、契約を前提とする社外組織におけるリスク管理」のような表現にしてほしいという相談を受けることがあったが、果たして、これを見た際に、社外者はどのように受け取るか。「サプライチェーンリスク」という言葉は、昨今のホットトピックであるが故、監督官庁や外郭団体等においても一般化している用語であり、置換の度が過ぎてしまうと、「一体これってどういう意味だろう？」という混乱を招く温床にもなる。こうした状況は、対外的な説明責任としては非常に危険である。セキュリティ管理として一般的に普及している考え方・用語・役割等、社外関係者が見てもわかりやすいようにしておくことで、インシデント発生時、規格・認証取得時の審査等の重要な局面で、高い心象評価として受け入れやすい。

当然、社内の従業員が見てもわからない内容であれば、改善の余地がある。ただし、その場合は、社内研修や説明会等の場で啓発を行うことで緩和できる可能性もあり、または、規定の一部として、「用語解説」のような付則表を設けることでも緩和できるかもしれない。

とにかく、規程類は社内だけでなく社外関係者が理解できる必要があるわけだが、手法として、規程類の位置付けを明確にして、それに沿った管理を行うというアイデアもある。

ポリシー・スタンダード・プロシージャという文書体系の考え方は一般的であるが、例えば、ポリシー・スタンダードは社外関係者が見て理解しやすい文書にしておく。ただし、プロシージャは社内の現場レベルのメンバーが理解できるように、組織内の独自用語等も引用して“わかりやすさ”を優先することも一案である。その場合、社外関係者向けと社内者向けの 2 つの視点を文書の種類によって使い分けることになる。誰に向けた文書なのか、その力点やバランスを見極めることで、文書の位置付けや見せ方も変わってくるだろう。

### イシュー③：「目を光らせる」ことの重要性

多くの企業において、規程類を策定した後は、社内の承認を得て、正式に発行されることになる。その方法は、社内イントラネット上での掲載、およびメール周知が中心となる。ただし、実態としては周知が十分に行われないケースが散見される。文書をつくることが目的になってしまい、それ以降、当該文書の存在が組織内に浸透せず、気がついたら何年も更新されずに陳腐化した、という話もよく耳にする。
ただし、本来、規程類は組織としての公式なルールであることを鑑みると、全従業員が前提として理解した上で、日常的な業務に臨まなければならない。

では、そのような状態を実現するために、何をすればよいか。そのためには、規程類を通じて（利用して）、組織としての“目を光らせる”ことが重要である。

ここで 1 つ紹介したい。「割れ窓理論（Broken Windows Theory）」をご存じだろうか。これは、1 枚の割られた窓ガラスをそのままにしていると、さらに割られる窓ガラスが増え、いずれ街全体が荒廃してしまうという、アメリカの犯罪学者ジョージ・ケリング博士が提唱した理論であり、かつて、犯罪多発都市のニューヨーク市で、1994 年以降、当時の市長が、この「割れ窓理論」を

実践し、割れ窓の修理や落書きなどを徹底し、軽微な犯罪の取締りを強化した結果、それに連動して重大な犯罪が大幅に減少したと言われているものである。

上記の理論から言えることとして、「目を光らせる」ことで小さなセキュリティリスクを抑止できると共に、さらには、それが大きな被害につながることの予防にもつながる。

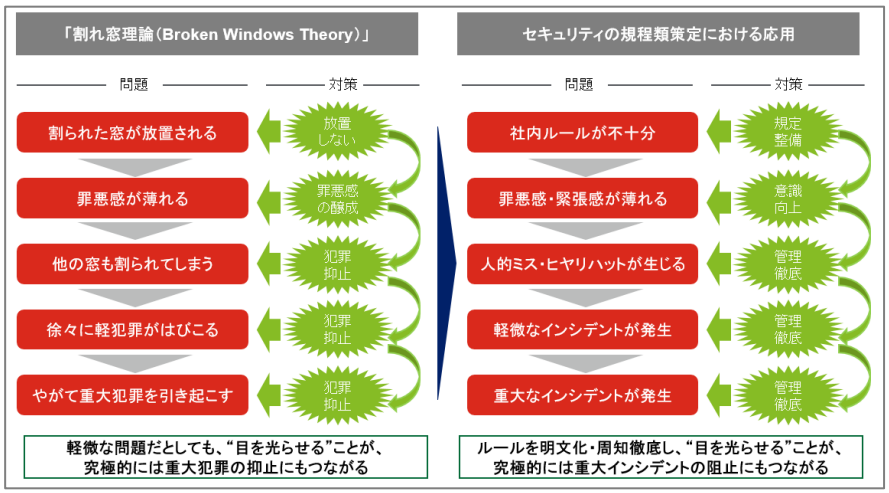



図 2：「割れ窓理論」の規定類策定への応用

規程類を通じて“目を光らせる”ためには、経営者はその存在を強く組織に訴える必要がある。一度や二度ではない。継続的にチェンジマネジメントのごとく、社内に訴え続ける必要がある。Face to Face による直接的な説明機会でもよい。または、研修・教育プログラムの一環として、学ぶ機会があってもよい。こうして、規程類のプレゼンスを高める活動を行うことで、社内の従業員に対しては、「うちの会社って案外とセキュリティ厳しいな」という意識喚起をもたらし、それが様々な不正活動の抑止やセキュリティ管理のための運用活動の徹底につながる気運ともなる。
このように規程類を策定することをゴールとせず、いかにそれを周知し、定着させるかまで配慮することで、最大限の効果が期待できる。

## 規程類の効果的な整備に向けて

以上、規程類の整備に関する要点を説明してきた。これらを踏まえて、冒頭で触れた各セキュリティ担当役員の考えが下記のようであれば、より効果的なセキュリティに関する諸ルールを組織内に浸透・定着させることが期待できるだろう。

**セキュリティ担当役員 A 氏**

**規程類は組織としての説明責任を果たす上でのベースとなる。自社の規程体系に沿った上で、各ルールに関する責任所在を明確にするとともに、それが対外的に見ても、安心感を与えるものとなっている必要がある。単なる資料と思わず、徹底的に考えよう！**

**セキュリティ担当役員 B 氏**

**規程類は従業員にルールを守らせるためにある。それと同様に、社外の利害関係者に、自社の安全性を共感してもらうためのものでもある。だからこそ、両方の面を意識して、どの階層の文書で何を？誰向けに？規定するのか、冷静に見極めよう！**

**セキュリティ担当役員 C 氏**

**規程類は社員が見やすい環境に置くべきだ。ただし、それだけでなく、その存在が浸透するように各所で働きかける必要もある。それによって組織としての“目を光らせている”感を強め、より健全なセキュリティ文化を醸成するための礎にしよう！**

規程類は、セキュリティ関連のソリューション・製品に比べると、派手さや直接的な効果という意味でのインパクトは小さく感じられるかもしれない。しかし、その本質的な意義を踏まえると、どんなに高機能なソリューション・製品を導入したとしても、土台となる考え方が曖昧であるならば、その効果も発揮されない可能性がある。

対外的に自社のセキュリティ管理の妥当性を説明する際、規程類の建付けと考え方が明確になっていれば、その時点で「この組織はきちんとセキュリティ管理と向き合っている」という心象を与えることになり、レピュテーションにも大きく影響する。

今後、自動車業界においては、WP29 等の型式認可の到来と共に、如何にセキュリティ管理の妥当性を社外に訴求するかが重要となる。認可の直接的な主体となる OEM はもちろん、自動車の製品機能の担い手であるサプライヤーとしても同様の責務を負っていると認識すべきである。そして、本当に規程類はただの「読み物／紙っぺら」でいいのか、今一度本テーマと向き合った上で、組織としての“あるべき整備”を実現することを期待したい。

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス内容がご提供できない可能性があります。詳細はお問合せください。

**デロイト トーマツ サイバー合同会社**
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】　東京・名古屋・福岡