# サイバーハイジーンを持続可能とする経営とは

PwCあらた有限責任監査法人
システム・プロセス・アシュアランス部
パートナー　**綾部 泰二**

## はじめに

ハイジーンとは「公衆衛生管理」という意味であり、サイバーハイジーンとは「サイバー空間における公衆衛生管理」を意味します。

私たちは現実世界で新型コロナウイルス感染症（COVID-19）に備え、マスク、手洗い、消毒等の衛生管理を行ってきました。これと同じくサイバー空間においても、コンピュータウイルスを含むマルウェア（悪意のあるソフトウェア）がまん延している状況においては公衆衛生管理が不可欠です。すなわち、企業は日々のサイバーセキュリティ活動を通して、攻撃の発生要因となるIT環境の脆弱性リスクを低減していくことが求められています。

ただし、単なるセキュリティパッチの適用やリアルタイム型のウイルス対策ソフトの導入などでは十分とは言えません。リアル世界において、公衆衛生管理だけでなく食事や運動による免疫力向上を図るように、サイバーハイジーンにおいては、IT環境内部の免疫力の向上、つまりサイバー攻撃に備えたシステムや機器内部の技術的なサイバーセキュリティの堅牢化が不可欠となります（**図表1**）。

しかしながら、サイバーハイジーンを持続可能な取り組みとするためには、予算や各種意思決定が必要なことは言うまでもありません。そこで本稿では、企業がサイバーハイジーンの対応を持続可能とするため、経営に必要なサイバーハイジーンのポイントについて解説します。

なお、文中の意見に係る記載は筆者の私見であり、PwCあらた有限責任監査法人および所属部門の正式見解ではないことをお断りします。

## 1 サイバーハイジーンを持続可能とするためには

サイバーセキュリティリスクが高まっている今日において、ランサムウェアに感染した企業が内部統制の不備を認識し、内部統制報告書をさかのぼって修正した事例も生じています。このような事例は、まさにサイバーハイジーンを持続可能とするべきであることを物語っており、具体的にサイバー攻撃を受けて被害に遭った企業のみならず、多数の企業に該当する事例だと想定されるものです。

### ① リスク対策の実現

まずポイントとなるのは、リスク認識がなされたのであれば、当該リスクが経営において許容水準以下となる対策をしっかり実行することです。すなわち、ランサムウェアの脅威を認識しつつも対策の実行に至らなければ、リスク評価を行っている意義がありません。

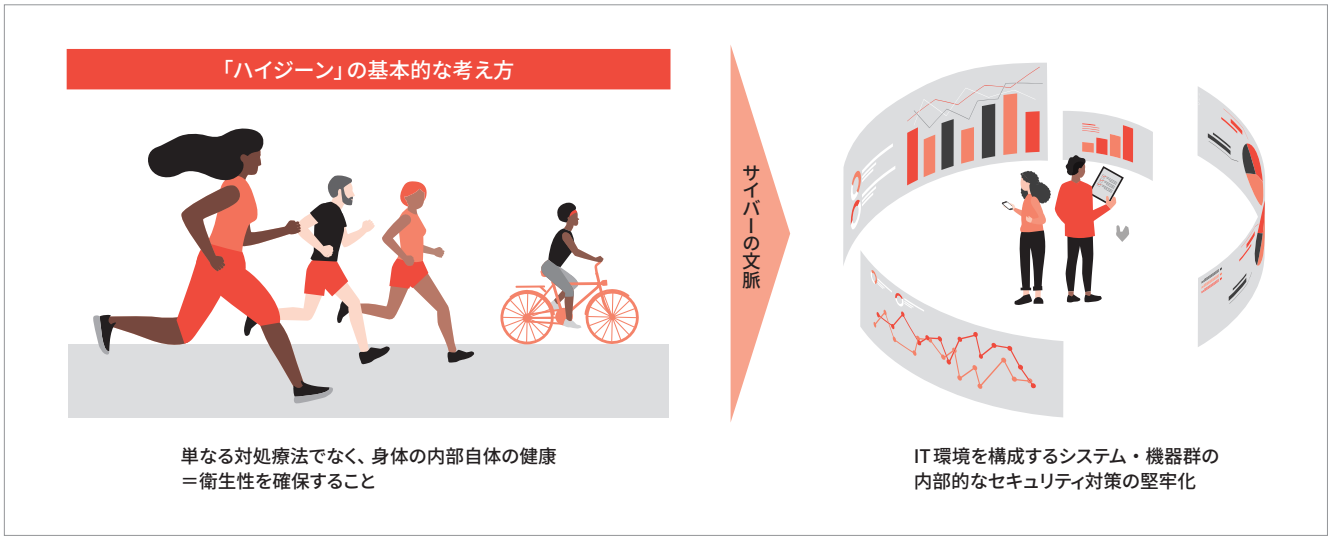
サイバーハイジーンを持続可能とする大前提として、適切にリスクを把握し、当該リスクに有効な対策を実行する必要があります。この実行こそが、まさにサイバーハイジーンの実現です。では、対策の実行のために何が必要となるでしょうか。

### ② 経営者のリーダーシップ

リスク対策の実行を確実にするためには、企業のガバナンスをデザインし、実現する経営者のリーダーシップが必要不可欠です。昨今、DX／デジタル化を推進する企業において、サイバーリスクはその表裏一体として重要な要因となっていますが、「サイバーリスクをマネジメントするリーダーシップとは何か」についてはイメージしづらい読者も多いかと思われます。

この点、一般に米国の経営者は、「新たなマルウェア等のサイバー脅威が発生した際、困惑する役員がいる企業が多い」

図表1：ハイジーンからサイバーハイジーンへ




出所：PwC「サイバーハイジーン評価」
https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting/cyber-hygiene.html

と感じている傾向があります。ここにヒントがあると考えられます。経営者が、サイバーリスク要因を常に意識して経営アジェンダとすることが、サイバーハイジーンを持続可能なものとするリーダーシップと言えます。

### ③ 組織、体制そして予算

サイバーリスク要因を常に意識して経営アジェンダとする経営者とは、どのような存在でしょうか。それは、CISO（Chief Information Security Officer）であるという点で異論はないでしょう。しかしながら、日本企業のCISOはCIO（Chief Information Officer）と兼務であることが多く、いわゆる地政学リスクの拡大も相まってサイバーリスクの要因はより複雑になっているにもかかわらず、当該兼務状態でCISOとして十分なリーダーシップを発揮できる状況ではなくなっているのではと思慮します。

また、いわゆる「部長CISO」も多々見受けられます。上述した経営アジェンダとしてサイバーリスクを取り扱い続けるためにも、取締役等の相応のポジションでのCISOの設置が望まれます。

加えて、このように兼務でない役員クラスのCISOを設置すればこそ、事業計画としてサイバーリスクへの対応が開始され、当該計画を実現するための体制や予算、およびルールが整備されるのではないでしょうか。

## 2 セキュリティ投資の効果とは

サイバーハイジーンを持続可能なものにするときのポイントとして、「① リスク対策の実現」、そのための「② 経営者のリーダーシップ」および「③ 組織、体制そして予算」の3点が重要であると述べてきました。

では、このようにリスク対策を実現するスキームとして、専任の役員クラスのCISOを設置し、組織化および予算を実行することによるサイバーリスク対策への投資効果をどう捉えたらよいのでしょうか。

以前から「セキュリティ投資はリターンのない投資」と言われることがありました。ここで、現実世界で猛威をふるっているCOVID-19への対応を思い返してください。すなわち、公衆衛生管理として手洗いやうがいをするのは感染予防であるところ、ワクチン接種においては、予防のみならず重症化リスクを低減すると言われています。またマスクを公衆の場で着用することは、予防のみならず周囲への感染リスクを低下させます。このような対応は、医療機関の対応の切迫を回避して、社会というシステム全体の維持を一人ひとりの意識から実現しようとの趣旨からも行われているところです。

これをサイバーの世界に置き換えてみると、セキュリティへの投資は予防だけでなく、マルウェアなどのサイバー被害が発生した場合に被害を最小限に抑えるためのものであり、これがサプライチェーンを含むと仮定すると、自社のビジネスだけでなくインターネット上のビジネス全体を維持しよう

とするものであることが分かると思います。これは前述したCOVID-19の対応と同様であり、通常の投資効果と同様に捉えるべきではありません。つまり、通常の設備投資で想定される投資とリターンの考え方が当てはまらないと整理したほうが自然だと著者は考えます。

## 3 高度な専門性を持ったセキュリティ人財について

上述のサイバー攻撃に起因した内部統制報告書の訂正事例に当たられた読者であれば、もう1つ大切なトピックスを取り上げていないことに気づかれているでしょう。それは「セキュリティ人財」についてです。

インターネットを利用したビジネスの急速な発展により、社会全体でセキュリティ人財が不足し、採用コストも増加の一途をたどっています。筆者は、高度な専門性を持つセキュリティ人財の確保は、もはや転職市場では難しいと考えています。

高度な専門性といっても、組織やガバナンスに関する知識・スキル、セキュリティ製品や機器に関する知識・スキル、いわゆる「インテリジェンス」と呼ばれる脅威に関する知識・スキルなど、必要なものは多岐にわたります。したがって、少ないパイの奪い合いを続けるよりも、各企業において本腰を入れたセキュリティ人財育成投資に期待したいところです。

問題なのは、上述した各セキュリティ分野に詳しい人財を採用しても、自社のビジネスを理解していなければ効果的なリスク評価はできないため、採用後すぐに機能することはないという点です。

であるならば、自社のビジネスに詳しい人財に対してセキュリティのスキルを開発するというやり方も有効かもしれません。自社のビジネスの社会における重要性を正しく理解できている人財でなければ、正しいセキュリティ対策の検討および実行は難しいでしょう。

しかし「言うは易く行うは難し」です。そもそもセキュリティ教育を推進するには、高度な専門知識と教育技術を持ったセキュリティ人財を社内に置く必要があり、自社だけで対応できる企業は少ないと推測されるからです。

## 4 まとめ

本稿では、サイバーハイジーンを持続可能にするためのポイントについて述べてきました。

最後に1つ、読者の皆様にお願いがあります。

セキュリティ担当者が尋ねられて一番困るのが、「これをやれば大丈夫？」という確認です。サイバーリスクはさまざまな対策によって低減することは可能ですが、ゼロにすることは不可能です。これは、ワクチンを打って、マスクをして、手洗い・うがいをすればコロナウイルスに感染することはない、と言っているのと同じことです。私を含め読者の皆様が、貴重なセキュリティ担当者を悩ませることなく、サイバーリスクに対する免疫力を高めるとともに、本稿が安全なインターネット社会の実現に少しでも貢献できれば幸いです。

**綾部 泰二**（あやべ たいじ）
PwCあらた有限責任監査法人　システム・プロセス・アシュアランス部
パートナー
2001年PwC参画、2006年CISA（公認情報システム監査人）。以後、セキュリティやITガバナンス等のリスクマネジメント業務に多数従事。2019年7月よりPwC Japanグループのサイバーセキュリティ Co-Leaderを務める。共著に『クラウド・リスク・マネジメント』（同文館出版）、『経営監査へのアプローチ――企業価値向上のための総合的内部監査10の視点』（清文社）がある。
メールアドレス：taiji.t.ayabe@pwc.com