
AMT/NEWSLETTER

Cyber & AI Security

2026 年 10 月 8 日

企業の運命を分けるサイバーセキュリティ～平時のガバナンスと有事の危機管理(上)

—防衛編:経営陣が知るべき平時の「正しい備え」と「リテラシー」—

弁護士 佐野 裕子

Contents

- I. はじめに～サイバーリスクの増大とコーポレートガバナンス
- II. ガイドラインを「形式」で終わらせない～経営陣が問われる当事者意識とガバナンス
- III. 「訓練参加率」という数字の罠～形式的研修から自走する「サイバーリテラシー」へ
- IV. 「委託先に任せてある」の過信～サプライチェーン全体を抑えるリスク防衛と保険

I. はじめに～サイバーリスクの増大とコーポレートガバナンス

近年、AI の普及・活用により、サイバー攻撃は、質、量、スピードともに劇的に変化しており、今後は、自立型 AI エージェントを用いた攻撃の自動化等により、人間では物理的に追いつけない攻撃の増加が確実視されている。

また、生成 AI が言語の壁を取り払ったことも手伝って、日本の知的財産や個人情報が必要な標的となりつつあり、全世界のメール攻撃のうち 90%が日本をターゲットにしていたとのデータもある¹。

サイバーインシデントによる情報漏えいやシステム停止が発生した場合、企業自体が莫大な事故対応費用や第三者への損害賠償責任を負い²、場合により、契約上の債務不履行責任や注意義務違反が問われるほか³、企業の幹部が、善管注意義務違反として株主や会社から法的責任を問われるリスクも高く、いずれの企業も、他人事と片付けてはいられない状況に置かれている。

かかる状況において、サイバーセキュリティ対策は、投資、すなわち将来の事業活動・成長に必須の費用と位置付け⁴、

1 出所:Proofpoint Web サイト [日本が今、最も狙われている【続編】—プルーフポイントのデータからみる生成 AI 時代のメール脅威と対策 | Proofpoint JP](#)

2 警察大学校編集『警察学論集 2026 年 4 月号』(立花書房、2026 年、103 頁)

3 東京地裁(平成 26 年 1 月 23 日判決・判時 2221 号 71 頁)

4 経済産業省・独立行政法人情報処理推進機構(IPA)「サイバーセキュリティ経営ガイドライン Ver3.0」[guide_v3.0.pdf](#)

経営者は、サイバーセキュリティが自社のリスクマネジメントにおける最重要課題の一つであることを認識することが不可欠である。

しかしながら、現実の攻撃や被害に遭っていない時点では、いまだに多くの企業において、「わが社だけは大丈夫」といった正常性バイアスが働き、とすると、一定の企業幹部において専門用語の理解さえ追いついていない現状があることは、筆者が、警察において、サイバーセキュリティ担当部署の幹部として勤務していた頃にも痛切に感じたことである。

また、最新のサイバーインシデントの実情につき、受け手が自分事として受け止めてくれるよう、分かりやすく効果的に情報を発信・共有すべき当局側の責任が重いことも事実である。

生成 AI の利用により、攻撃が、人間の思考や物理的な動きを超えたものとなっても、それによるリスクや被害を可能限り低減できるのは、サイバーセキュリティが企業の生死を分ける重要課題であることを認識した企業経営者によるリーダーシップであり、いったん発生した場合に、いかに迅速適切に通常営業への復旧を図るか(サイバーレジリエンス)が、企業価値の維持・向上に直結する。

その意味で、サイバーセキュリティは、コーポレートガバナンスの視点から捉え直すべきものと言えよう。

II. ガイドラインを「形式」で終わらせない～経営陣が問われる当事者意識とガバナンス

経済産業省と独立行政法人情報処理推進機構(IPA)が定める「サイバーセキュリティ経営ガイドライン」には、経営トップが主導すべき 3 原則や重要 10 項目(CISO(最高情報セキュリティ責任者)の任命や予算・人材の確保等)が示されている⁵。

しかし、これを、単なる「IT 担当部署のチェックリスト作業」として丸投げしてしまえば、ガバナンスとして機能しない。

経営者に求められるのは、常日頃から最新の攻撃手口や他社事例にアンテナを張り、CISO 等から定期的にリスクの報告を受けて自社が許容できるリスク水準を議論する「経営課題としての定例議論」を構築することである。

そして、最新の攻撃手口や他社の事例等や、それにより実際に引き起こされた混乱や失敗、そこから得られた教訓等の生の声や実情をタイムリーに把握するためには、単にオンラインの AI 検索ツールなどを利用するだけでは不十分であり、この分野の専門家や他社の当該分野担当者との、常日頃からの「顔の見える関係作り」、それも、各レベルでの横のつながり作りが不可欠である。

そのためには、各種業界団体の集まりにリアルに顔を出し、個別の実質的な信頼関係の構築に努めるほか、日本犯罪対策センター(JC3)⁶や、業界ごとに立ち上げられている Information Sharing and Analysis Center(ISAC)⁷、OWASPJapan⁸等に参画して、同業種企業におけるサイバーインシデント被害の実情や、効果を発揮した取組事例等について把握することも、検討の余地があろう。

⁵ 産業サイバーセキュリティ研究会「小売電気事業者のためのサイバーセキュリティ対策ガイドライン Ver.1.0」 [20210222_1.pdf](#)

⁶ 一般財団法人日本サイバー犯罪対策センター(JC3)

⁷ ISAC(アイザック)とは？業界別 ISAC の種類、ISAO との違いと関連の仕事・資格を解説 - サイバーHR

⁸ Web アプリケーションを始めとするソフトウェアのセキュリティ向上を目的とした、世界規模の非営利団体 OWASP (Open Worldwide Application Security Project)の日本支部。実際に現場で、エンジニアがいかなるサイバー攻撃に困っているかといったリアルな情報交換の場となっている。 [OWASP Japan | OWASP Foundation](#)

III. 「訓練参加率」という数字の罠～形式的研修から自走する「サイバーリテラシー」へ

IPA は最低限の対策として「情報セキュリティ 5 か条」を提示し⁹、社内ルールの策定や「SECURITY ACTION」等の宣言制度を案内している¹⁰。

だが、標的型メール訓練の参加率や e ラーニングの正答率といった「表面的な指標」ばかりを追う研修は形骸化しやすい。

真に必要なのは、不審なメールやミスに気付いた際、従業員が「怒られるかもしれない」と躊躇したり隠蔽したりせず、即座に声を上げられる社内風土を経営トップが作ることである。

そのためには、常日頃から、例えば時間外の報告であっても、陰しい表情や不機嫌な声を出すことなく、報告者への労いの言葉をかけるように上司が努力するだけでも、いわゆる悪い報告の上がりやすさに格段の差が出てくることは、筆者自身が、双方の立場で経験したことである。

技術的な防御をすり抜けてくる攻撃に対し、防御の切り札となるのは従業員一人一人が自らの頭で考え行動する「サイバーリテラシー」であり、心理的ハードルを下げる環境作りこそが経営者の役割と言える。

「悪い報告を即座に上げたくなる職場作り」に向けて、「笑顔、挨拶、雑談」を上司が率先してできるかどうか、言わば、こういった常日頃からの「アナログ」な取組が、「サイバーリテラシー」の醸成にとって不可欠であるといっても過言ではない。

IV. 「委託先に任せてある」の過信～サプライチェーン全体を抑えるリスク防衛と保険

近年多発しているのは、自社本体ではなくセキュリティの手薄な業務委託先や取引先を踏み台にして侵入される攻撃である。

契約書上でセキュリティ要件や報告義務を明記することは当然の前提であるが、単に文書化して安心する「契約上の対策」にとどまってはならない。

この点、流行りに乗り遅れてはいけないと、同業他社グループが作成した契約書を、日付と当事者のみ置き換えて、そのまま自社グループに使用する例もありがちであるが、各契約条項が、いかなる状況において生きてくるのかを頭で理解しない契約書は、自己満足以外の何物でもなく、全く意味をなさないことを肝に銘じるべきである。

また、どの取引先のどの部署が狙われやすいか、万が一感染した場合にどう連携するか、関係企業や担当者間で事前にリアルなシミュレーションと脅威認識を共有しておくことが不可欠である。

その点でも、各職場の雰囲気(適度な緊張感の下での理解・信頼に基づく良好なコミュニケーションの有無)、各人の業務の可視化の程度、上司と部下の関係等を指標に、実質的かつ具体的な情報共有がなされているかが分かれ目となる。

併せて、EC サイトでの漏えい時に発生するカード会社からの求償請求や、端末 1 台あたり数百万円規模に上る高額なフォレンジック調査費用に備え、サイバー保険を導入して補償や資力を確保しておく「リスク移転」の視点も重要な経営判断となろう。

この点、金銭的な損失の補償だけでなく、付帯サービスとして、①情報セキュリティ診断(事前)や、②専門事業者・専門家(原因究明・ログ解析に長けたフォレンジック調査会社、データ復旧事業者など)の紹介(事後)といったインシデント前後の各種サポートを提供する保険商品が増えており、特に②は、有事の際に自力手配することは往々にして困難であることから、予めの保険加入は大いに検討に値するものと考ええる。

以上

⁹ 経済産業省・IPA「サイバーセキュリティ経営ガイドライン Ver3.0 付録 B」 [guide_v3.0.pdf](#)

¹⁰ IPA「2024 年度中小企業における情報セキュリティ対策に関する実態調査－報告書－」 [2024 年度 中小企業における情報セキュリティ対策に関する実態調査-報告書-](#)

-
- 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。
 - 本ニュースレターの執筆者は、以下のとおりです。
弁護士 佐野 裕子 yuko.sano[at]amt-law.com
※メールを送信する際には、[at]を@に変更してお送りください。
 - ニュースレターの配信停止をご希望の場合には、お手数ですが、[お問い合わせ](#)にてお手続き下さいますようお願いいたします。
 - ニュースレターのバックナンバーは、[こちら](#)にてご覧いただけます。