弁護士法人　三宅法律事務所

Miyake　& Partners

デジタル・ガバナンス／サイバーセキュリティニュース　No.3

サイバー事故を起こした従業員を懲戒できるか

―「個人のミス」で終わらせない人的リスク管理とサイバーガバナンス ―

平素より大変お世話になっております。

日本経済新聞令和 8 年 7 月 21 日付記事は、サイバー事故を起こした従業員に対して国内企業の約半数が懲戒処分を行っているとの調査結果を報じ、専門家が**「個人の責任追及だけで終わらせるべきではない」**と警鐘を鳴らしていることを伝えています。今日、サイバー事故は一部の企業に限られた例外ではなく、多くの企業が経験する日常的な経営リスクとなっており、その対応は、事故を起こした個人の責任追及にとどまらず、**事故を防止・検知・対応する組織的な態勢の構築**へと重心を移しつつあります。

経済産業省「サイバーセキュリティ経営ガイドライン」、金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」、個人情報保護法上の安全管理措置、NIST Cybersecurity Framework 2.0 等の国内外の主要な法令・ガイドラインは、いずれもサイバーセキュリティを**経営者・取締役が責任を負う企業ガバナンスの問題**として位置付けています。そのため、事故後の対応においても、従業員個人の過失のみならず、企業の管理態勢が実効的に機能していたかが問われます。

また、航空・医療等の分野で発展してきた「Just Culture（公正な文化）」の考え方は、故意・重大な規律違反には責任を問う一方、誠実なミスについては早期報告を促し、組織全体で学習する文化を重視するものであり、サイバー事故対応における懲戒処分の相当性を検討する上でも有用な枠組みを提供します。

本ニュースレターでは、これらを踏まえ、サイバー事故を起こした従業員の懲戒処分の可否・程度を判断する際の視点を、経営者・取締役が確認すべきチェックリスト（10 項目）及び懲戒処分判断フローとして整理いたします。末尾には理解度チェック（〇×問題 10 問）を付しておりますので、社内研修等にもご活用いただけますと幸いです。

令和 8 年 7 月 21 日

弁護士法人三宅法律事務所

＊本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。

弁護士法人三宅法律事務所

弁護士　渡邉雅之（執筆者）

TEL 03-5288-1021　FAX 03-5288-1025

Email: m-watanabe@miyake.gr.jp

デジタル・ガバナンス／サイバーセキュリティニュース　No.3

サイバー事故を起こした従業員を懲戒できるか

―「個人のミス」で終わらせない人的リスク管理とサイバーガバナンス ―

【目次】

1　はじめに ― サイバー事故は「例外」ではなく「日常」になった

取引先を装ったメールの添付ファイルを開いてしまった、偽サイトに認証情報を入力した、メールを誤送信した、クラウドサービスの設定を誤った――。このような従業員の行為を契機として、情報漏えいやシステム障害等のサイバー事故が発生する例は少なくない。

日本経済新聞令和 8 年 7 月 21 日付記事によれば、米国のセキュリティ会社 KnowBe4 の調査において、外部からの攻撃を受けた場合に従業員を懲戒処分とする国内企業の割合は 51%、メール誤送信等の偶発的な事故についても 49%に達し、いずれも世界平均を 6～7 ポイント上回っている[1]。

もっとも、サイバー事故に従業員の行為が関係していたとしても、直ちにその従業員のみに責任を負わせることが適切とは限らない。一般財団法人日本情報経済社会推進協会（JIPDEC）が令和 8 年 1 月に実施した調査では、過去 1 年間にセキュリティインシデントを経験していないと回答した企業は 22.7%にとどまり、約 8 割の企業が何らかのインシデントを経験している。サイバー事故は、もはや「起こるか否か」ではなく「起きることを前提に、いかに備え、いかに対応するか」が問われる段階に至っている。

本稿では、日本企業に根強い「事故＝個人責任」という発想を、法令・ガイドラインが求める「事故を防止・検知・対応する組織」の構築という視点から捉え直し、**経営者・取締役が確認すべきチェックリスト（10 項目）**と**懲戒処分判断フロー**を実務に即して整理する。

2　「人的要因」は「従業員の責任」と同義ではない

サイバー事故については「人的要因があった」と説明されることがある。米ベライゾンの調査でも、データ侵害の 62%に人的要因が関与しているとされる[2]。しかし、ここでいう「人的要因」には、従業員が不審なメールを開いたという直接的な行為だけでなく、次のような組織側の要因も含まれる。

- フィッシングやビジネスメール詐欺（BEC）に関する教育が不十分であった

[1] 日本経済新聞令和 8 年 7 月 21 日付「サイバー事故で従業員に『懲戒』、国内企業の半数　世界平均より高く」（渋谷江里子記者）。KnowBe4 は令和 7 年 8～9 月に調査を実施。

[2] Verizon「Data Breach Investigations Report」。「人的要因」には従業員個人のミスのみならず、教育・権限管理・システム設計上の不備等の組織側の要因も含まれる。

- 多要素認証（MFA）[3]が導入されていなかった
- 一人の従業員に過大なアクセス権限が付与されていた
- メール送信時の確認機能や承認手続がなかった
- 不審なメールを報告する窓口が分かりにくかった
- 事故を報告すると責任追及されるという組織風土があった
- 委託先やクラウドサービスの設定状況を確認していなかった

個人情報保護法上も、個人情報取扱事業者には、組織的・人的・物理的・技術的の各安全管理措置を、事業の規模、取扱状況およびリスクに応じて講じることが求められている。単に従業員へ注意を呼びかけるだけでは足りない。サイバー事故は、従業員の行為を「最後の一押し」として発生する一方、その背後に複数の管理上の不備が存在することも少なくない。

3 経営者・取締役が確認すべき人的リスク管理チェックリスト（10 項目）

サイバー事故が発生した際、経営者・取締役は、従業員の処分を検討する前に、少なくとも次の 10 項目を確認する必要がある。

No.	確認項目	チェックのポイント
1	人的リスクに関する方針が明確か	サイバーセキュリティを情報システム部門のみの問題とせず、経営課題として位置付けているか。許容できるリスク水準、経営者・CISO[4]・法務・内部監査・人事・事業部門の役割分担を明確にしているか。
2	社内規程が具体的か	情報セキュリティ規程、端末利用規程、電子メール利用規程、クラウド利用規程、生成 AI 利用規程等において、禁止事項と従業員が取るべき行動が具体的に定められているか。抽象的な定めだけでは処分の根拠としても事故防止策としても不十分である。
3	教育が形式的なものになっていないか	入社時の一度限りの研修ではなく、フィッシング、BEC、ランサムウェア、クラウド設定、生成 AI、リモートワーク等、実際の脅威に即した継続的教育を行っているか。受講記録・理解度確認を残しているか。
4	訓練結果を個人評価だけに使っていないか	標的型メール訓練につき、クリックした従業員の叱責のみが目的になっていないか。結果は部署・職種・時期・メール類型別に分析し、教育・システム設定・業務フローの改善に用いるべきである。
5	技術的対策でミスを補完しているか	MFA、アクセス制御、最小権限、メールフィルタリング、URL 隔離、添付ファイル無害化、外部送信時警告、送信保留、バックアップ等、人の注意力のみに依存しない仕組みを導入しているか。
6	報告しやすい仕組みがあるか	不審メールを開いた・認証情報を入力した・誤送信した場合に、直ちに報告できる窓口と手順が整備されているか。初動の早さが被害を左右するため、誠実な報告を不利益に扱わない方針が重要である。
7	報告の速さを評価しているか	事故そのものだけでなく、発見後の行動を区別して評価しているか。数分以内に報告した従業員と数日間隠していた従業員を同一に扱うべきではない。
8	インシデントの原因分析をしているか	「本人の不注意」で原因分析を終了していないか。なぜメールが届き、なぜ見分けられず、なぜ認証情報だけで侵入され、なぜ被害が拡大したのか、を掘り下げる必要がある。

[3] MFA（Multi-Factor Authentication、多要素認証）とは、本人確認に際し、①知識情報（パスワード、PIN 等）、②所持情報（ワンタイムコード、ハードウェアトークン等）、③生体情報（指紋、顔認証等）という性質の異なる複数の要素を組み合わせて認証する仕組みをいう。パスワードのみに依存する認証はフィッシング等により突破されやすいが、MFA を導入すれば、仮にパスワードが窃取されても第二の要素がなければ不正アクセスを防ぎ得る。金融庁ガイドラインや個人情報保護法上の技術的安全管理措置においても、重要なシステムや外部からのアクセスに対する多要素認証の導入が推奨されている。

[4] CISO（Chief Information Security Officer、最高情報セキュリティ責任者）とは、企業全体の情報セキュリティ戦略の策定、リスク管理、インシデント対応、方針・規程の整備、教育・訓練の統括等について責任を負う経営レベルの役職をいう。情報システムの構築・運用を主管する CIO（最高情報責任者）とは区別され、両者の役割を分けて牽制を働かせる考え方が採られる。経済産業省・IPA「サイバーセキュリティ経営ガイドライン」も、経営者が CISO 等の責任者を任命し、その下で対策を推進する体制の整備を求めている。

No.	確認項目	チェックのポイント
9	懲戒基準に一貫性があるか	同種事案の過去の処分例、職位、権限、故意・過失の程度、結果の重大性を踏まえ、公平で一貫した処分がなされているか。損失額の大小という結果のみで処分を重くすることは慎重に検討すべきである。
10	取締役会が改善状況を監督しているか	重大事故の件数のみならず、報告までの時間、フィッシング報告率、教育受講率、権限棚卸しの実施率、改善措置の完了率等を取締役会に報告しているか。

4 主要な法令・ガイドラインが人的リスク管理に求めるもの

従業員の責任を判断する際には、就業規則や情報セキュリティ規程のみならず、企業に求められているサイバーセキュリティ管理態勢も確認する必要がある。主要な法令・ガイドラインは、いずれも従業員に注意を求めるだけでなく、**経営者による方針策定・役割分担・教育・技術的対策・報告体制・インシデント対応・継続的改善を一体として整備すること**を求めており、責任主体を経営陣に置いている。

法令・ガイドライン	対象・位置付け	人的リスク管理に関する主な内容	懲戒判断との関係
経済産業省・IPA「サイバーセキュリティ経営ガイドライン Ver.3.0」（令和 5 年 3 月改訂）	業種を問わず主として企業経営者を対象とする実務指針	サイバーリスクを経営リスクとして扱い、経営方針・責任体制・必要な資源・教育・インシデント対応・サプライチェーン対策・継続的改善を求める（「3 原則」「重要 10 項目」）	従業員の操作ミスだけでなく、経営者が適切な体制・資源・指示を整備していたかを確認する根拠となる
金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」（令和 6 年 10 月 4 日公表・適用）	金融機関等の監督上の着眼点を示す業界ガイドライン（6 観点・176 項目）	ガバナンス／特定／防御／検知／対応・復旧／サードパーティリスク管理につき、取締役会等の関与、リスク評価、教育・訓練、有効性検証を重視	事故を起こした個人の処分より先に、管理態勢が実効的に機能していたかを検証すべきことを示す（金融機関以外へは当然には法的義務とならない点に留意）
個人情報保護法・個人情報保護委員会ガイドライン	個人データを取り扱う事業者に適用される法的義務	組織的・人的・物理的・技術的安全管理措置、従業者の監督、教育、漏えい等の把握・報告、再発防止を求める	漏えいが生じた場合、従業員の過失だけでなく、事業者が必要かつ適切な安全管理措置を講じていたかが問われる
NIST Cybersecurity Framework 2.0（令和 6 年 2 月公表）	業種・規模を問わず利用できる国際的なリスク管理の枠組み	Govern／Identify／Protect／Detect／Respond／Recover の 6 機能。新たに「Govern（統治）」を独立機能として位置付け	「誰がクリックしたか」だけでなく、事故前から復旧までの組織的管理プロセス全体を検証する視点を与える
NIST SP 800-61 Rev.3（令和 7 年 4 月 3 日公表）	CSF2.0 に準拠したインシデント対応の指針（Rev.2 を全面的に代替）	インシデント対応を発生後のみの活動ではなく、CSF2.0 に基づく組織全体のリスク管理に組み込むことを求める	懲戒調査を急ぐ前に、被害抑止・証拠保全・報告・分析・復旧・改善を優先すべきことの裏付けとなる

NIST CSF2.0 における「Govern（統治）」機能新設の意義

NIST[5] CSF2.0（令和 6 年 2 月公表）は、従来の Identify（特定）、Protect（防御）、Detect（検知）、Respond（対応）、Recover（復旧）の 5 機能に加え、新たに「Govern（統治）」を 6 番目の機能として独立させた。ここでいう Govern とは、事業環境や利害関係者の期待を踏まえたサイバーセキュリティ戦略の策定、リスク許容度の決定、役割・責任・権限の明確化、方針の整備、経営陣による監督およびサプライチェーンリスク管理等を内容とするものである。

[5] NIST とは、米国国立標準技術研究所（National Institute of Standards and Technology）をいう。米国商務省傘下の政府機関であり、度量衡・工業規格等の標準策定を担うほか、サイバーセキュリティ分野においても各種のフレームワーク・ガイドラインを公表している。これらは米国政府機関に適用されるにとどまらず、事実上の国際的な標準として、我が国を含む各国の民間企業においても広く参照されている。

Govern が独立の機能として位置付けられたことには、二つの意義がある。第一に、Govern は他の 5 機能と並列に置かれた「6 番目の作業項目」ではなく、**防御・検知・対応・復旧を含む他の全機能を方向付ける基盤**として位置付けられている点である。すなわち、教育が実効的に行われていたか、多要素認証や権限管理が適切に設計されていたか、事故を検知・報告・対応する体制が機能したか——これらはいずれも、経営陣による統治（Govern）の成否に帰着する。第二に、これにより、サイバーセキュリティが情報システム部門の技術的課題ではなく、**経営者・取締役が責任を負う企業ガバナンスそのものの問題**であることが、国際的な枠組みの上でも明確にされた点である。

この考え方は、金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」が 6 観点の筆頭に「ガバナンス」を掲げ、取締役会等の関与を求めていることとも軌を一にする。サイバー事故を、現場従業員個人の不注意としてではなく、統治の成否として評価すべきであるという本稿の視点は、まさにこの Govern 機能の新設が象徴するものである。

【共通する考え方】

- 第一に、サイバーセキュリティの最終責任を現場の従業員のみに帰属させない。経営者・取締役には、方針・体制・予算・人材・技術的対策を整備する責任がある。
- 第二に、人は誤ることを前提に多層的対策を講じる。教育・注意喚起のみに依存せず、MFA・最小権限・フィルタリング・送信保留・ログ監視・バックアップ等でミスを補完する。
- 第三に、事故の早期報告を促進する。事故を起こしたこと自体と、事故後に隠蔽・虚偽説明・報告遅延を行ったこととは区別して評価すべきである。
- 第四に、処分の有無とは別に、組織的な原因分析と改善を行う。原因を「本人の不注意」で終わらせず、規程・教育・権限・システム・業務量・管理監督・組織文化を検証する。

（注）NIST CSF2.0（令和 6 年 2 月）および経済産業省ガイドライン Ver.3.0（令和 5 年 3 月）は「最新公表文書」ではないが実務上重要である。令和 7 年に新規公表された文書としては NIST SP 800-61 Rev.3（令和 7 年 4 月）が特に意味を持つ。金融庁ガイドラインは令和 6 年 10 月公表であり、その後の改正は組織改編に伴う技術的修正にとどまる点に留意されたい。

5 「Just Culture（公正な文化）」とは何か ― 誠実なミスと故意の違反を区別する

従業員を処分しないことは、何らの責任も問わないことを意味しない。この点を整理する上で参考となるのが、航空・医療等、安全性が特に重視される分野で発展してきた「Just Culture（公正な文化）」の考え方である。Just Culture は、すべてのミスについて責任を問わない「無責任な文化」ではなく、①従業員が事故・ミス・異常事象を安心して早期に報告できる環境をつくることと、②故意・重大な規律違反・隠蔽等の許容できない行為については適正に責任を問うこと、という二つを両立させる仕組みである。EU の航空安全規則も、経験・訓練に照らして相応の行為・判断・不作為について現場担当者を処罰しない一方、重大な過失・故意の違反・破壊的行為は許容しない文化として整理しており、事故報告を促進しつつ、通常負うべき責任まで免除するものではない。

(1) 「責任追及型」と「無責任型」の中間に位置する

Just Culture を正しく理解するには、次の三つの組織文化を区別する必要がある。

組織文化	事故発生時の基本姿勢	問題点・特徴
Blame Culture（責任追及型）	事故を起こした個人を特定し、処分することを基本とする	報告の遅れ・隠蔽・萎縮を招き、組織的原因が見過ごされる
No-Blame Culture（無責任型）	原則として誰の責任も問わない	故意・重大な違反・反復行為まで放置され、規律が失われる
Just Culture（公正な文化）	行為の性質と組織側の要因を分析し、公正に対応する	報告促進と説明責任（アカウンタビリティ）を両立できる

すなわち Just Culture は「優しい企業文化」ではなく、**責任の所在を、結果の大きさや感情ではなく、行為の性質・予**

見可能性・規程・教育・組織的要因に基づいて公正に判断する仕組みである。

⑵ 結果ではなく「行動の選択過程」を評価する

サイバー事故では、同じ情報漏えいという結果が生じても、従業員の責任の程度は大きく異なる。例えば、①高度に巧妙なフィッシングメールを一度誤って開き直ちに報告した場合と、②過去に複数回注意を受け、明確な禁止事項を認識しながら私用サービスへ情報をアップロードし発覚後も隠蔽した場合とでは、たとえ①の方が結果的な被害が大きくとも、責任の評価は同じではない。重視すべきは、偶然に左右される結果ではなく、その行為を予見・回避できたか、明確なルールを認識していたか、合理的な代替行動があったか、同様の行為を繰り返していたか、事故後に誠実に報告したか、会社側が必要な対策を講じていたか、という行動の選択過程である。

⑶ 行動を三つの類型に分ける

Just Culture の考え方をサイバー事故に応用すると、従業員の行動はおおむね次の三類型に整理でき、これは後記 6 のフローの STEP3（A～D）の区分に対応する。

行為類型	サイバー事故の例	基本的な対応
①ヒューマンエラー	巧妙な偽メールを真正と誤認、宛先候補の選択ミス、分かりにくい画面での設定ミス	原則として懲戒より、システム・画面設計の改善、送信保留・警告機能の導入、業務手順の簡素化、再教育、権限設定の見直しを中心とする
②リスクを伴う行動	確認手順の省略、利便性優先のパスワード共有、未承認クラウドの利用、警告の不確認クリック	危険性の理解を促す指導、業務上のインセンティブ・実行困難なルールの見直し、必要に応じ注意・戒告。現場が省略せざるを得ない状態なら業務設計・管理職の責任も検証
③無謀な行動・故意の違反	危険を認識しつつ明確な禁止事項を無視、認証情報の第三者提供、故意の情報持出し、事故の隠蔽・ログ削除、指導後の反復違反	Just Culture の下でも懲戒処分その他の厳正な対応を検討。故意・悪意ある行為は損害賠償・刑事対応等も視野に入れる

（注）この分類は機械的に処分を決めるものではない。最終的には、就業規則上の根拠、教育・周知の状況、職位・権限、過去の指導歴、会社側の管理状況、同種事案との均衡等を総合的に判断する必要がある。

⑷ 早期報告を「有利な情状」として明確化する

サイバー事故では、初動の数分から数時間が被害の規模を左右する。偽サイトに認証情報を入力した場合でも、直ちに報告すればパスワード変更・セッション遮断・端末隔離等により被害を抑えられることがある一方、処分を恐れて報告が翌日以降になれば、攻撃者の侵入や横展開を許しかねない。そこで、例えば次のような方針を明示することが考えられる。

> *従業員が誤操作、誤送信、不審メールの開封その他のセキュリティ上の問題を認識し、速やかかつ誠実に報告して調査・被害拡大防止に協力したときは、その報告行為を不利益に取り扱わない。ただし、故意、重大な規程違反、反復行為、隠蔽、虚偽報告または証拠の改ざんがある場合は、この限りでない。*

重要なのは、「報告すれば絶対に処分されない」と約束することではなく、**誠実な早期報告を有利な事情として明確に評価すること**である。もっとも、こうした方針は規程に一文を加えるだけでは機能せず、経営陣による報告促進方針の表明、判断基準の事前明文化、法務・人事・内部監査等を関与させた調査の公正性確保、管理職への同一基準の適用、報告データの改善活用といった組織的条件が伴って初めて実効性を持つ。

⑸ Just Culture と日本法上の懲戒処分

Just Culture は、それ自体が日本法上の独立した法的ルールではない。懲戒処分の有効性は、労働契約法 15 条に基づき、客観的に合理的な理由があり社会通念上相当と認められるかによって判断される。もっとも、①単純なミスと

故意の違反を区別したか、②従業員が受けた教育・訓練に照らして回避可能だったか、③会社側の管理上の不備を検証したか、④事故後の早期報告を適切に評価したか、⑤過去の同種事案との均衡が保たれているか、⑥懲戒より軽い手段で目的を達成できないか、という検討を行うことは、処分の合理性・相当性を確保することにもつながる。この意味で、Just Culture は、懲戒処分の相当性を検討する際の実務的な枠組みとして有用である。

6 サイバー事故発生時の懲戒処分判断フロー

懲戒処分の可否・程度は、事故が発生したという結果のみならず、就業規則上の根拠、従業員の行為態様、企業側の対策、報告後の対応、過去の処分との均衡等を総合して判断する必要がある。実務上は次の順序で検討することが考えられる。

STEP1 事実関係を保全・確認する

メール、アクセスログ、端末ログ、認証記録、社内チャット、報告時刻等を保全する。この段階では「誰が悪いか」を決めつけず、何が起きたか／いつ発生し発見・報告されたか／どの情報・システム・取引先に影響したか／故意・過失または外部からの欺罔があったか／被害拡大防止の行動を取ったか／上司・管理部門の指示に問題がなかったかを確認する。証拠保全・初動対応と懲戒調査は、可能な限り区別して進める。

STEP2 就業規則上の根拠を確認する

問題となる行為が、就業規則・情報セキュリティ規程上のどの義務（秘密保持義務、業務命令、社用端末の私的利用禁止、無許可のクラウド利用禁止、アカウント・パスワード共有禁止、事故報告義務、証拠削除・隠蔽の禁止等）に違反するかを確認する。懲戒事由が抽象的で、従業員に具体的な行動基準が周知されていなかった場合には、懲戒処分の適法性に問題が生じやすい。

STEP3 従業員の主観・行為態様を評価する

A 故意・不正目的（情報持出し、認証情報の第三者提供、事故の意図的隠蔽等）――重い懲戒を検討し得る。

B 重大な規程違反・重過失（明確な禁止事項の認識ある無視、複数回の警告後の反復、管理者権限の著しい不適切使用等）――規程内容・教育状況・過去の注意指導を踏まえ処分を検討する。

C 通常の過失（巧妙なフィッシングメールを誤って開く、送信先を一度誤る等）――技術的・組織的対策の状況を確認せず、事故の発生のみを理由に懲戒することは慎重であるべきである。

D 不可避または予見困難な事象（高度に巧妙な攻撃、システムの欠陥、管理者側の設定ミス等）――原則として個人責任よりも組織上の改善を中心に検討する。

STEP4 企業側の管理状況を評価する

明確な規程の存在・周知、実効的な教育・訓練、MFA・アクセス制御の導入、過大な権限付与の有無、同種事故を把握しながら放置していなかったか、人員不足・過重労働がミスを誘発していなかったか、報告窓口と初動手順の明確性を確認する。この評価に当たっては、経済産業省の経営ガイドライン、業種に応じた監督指針・業界ガイドライン、個人情報保護法上の安全管理措置および NIST CSF2.0 等を参考に、経営者の関与・責任体制・教育・技術的対策・検知報告体制・インシデント対応・改善プロセスが実効的に整備されていたかを確認する。これらが不十分であるにもかかわらず、事故の結果のみを理由として重い懲戒処分を科すことは、処分の相当性を欠く方向の事情となり得る。

STEP5 事故後の対応を評価する

軽くする方向の事情：自ら直ちに報告した、調査に協力した、パスワード変更・端末隔離を速やかに行った、被害拡大防止に努めた、事実を正確に説明した。

重くする方向の事情：事故を隠蔽した、ログ・メールを削除した、虚偽説明をした、報告を意図的に遅らせた、同様の違反を繰り返した。

STEP6　処分の相当性・均衡を確認する

故意・過失の程度、規程違反の明確性、職位・権限、教育訓練の実施状況、過去の注意指導歴、被害の内容・拡大可能性、発覚後の報告・協力状況、過去の同種事案との均衡、管理職・会社側の責任等を総合考慮し、戒告・けん責・減給・出勤停止等のうち相当な処分を検討する。懲戒処分は、客観的に合理的な理由を欠き社会通念上相当と認められない場合には、懲戒権の濫用として無効となり得る（労働契約法 15 条参照）。

STEP7　処分と再発防止を分けて実施する

懲戒処分を行った場合でも、それのみで事案を終了させてはならない。別途、システム設定の変更、権限の縮小、教育内容の見直し、報告手順の簡素化、業務フローの二重確認、委託先管理の強化、インシデント対応計画の改定、取締役会への報告、内部監査による改善状況の検証を実施する。

7　おわりに

サイバー事故は、しばしば従業員の操作や判断を契機として発生する。しかし、その原因を「本人の不注意」の一言で終わらせてしまえば、教育・システム・権限管理・業務設計および組織文化に潜む問題は改善されない。事故後に従業員を処分することは、企業が十分なサイバーセキュリティ対策を講じていたことの証明にはならない。

経営者・取締役に求められるのは、①人のミスを前提とした技術的・組織的対策の整備、②事故を迅速に報告できる文化の形成、③故意・重大な違反と誠実なミスの区別、④処分の有無にかかわらない原因分析と再発防止、⑤対策の有効性の継続的検証である。サイバー事故への対応力は、事故を一度も起こさないことだけでなく、事故が発生した際に、隠さず、早く報告し、被害を抑え、組織として学習できるかによって評価されるべきである。

理解度チェック（〇×問題 10 問）

【問題】次の記述は正しいか（〇×）。

Q1　サイバー事故に「人的要因」が関与している場合、それは常に従業員個人の過失を意味する。

Q2　JIPDEC の令和 8 年 1 月調査では、過去 1 年間にセキュリティインシデントを経験していない企業は約 2 割にとどまる。

Q3　KnowBe4 の調査によれば、外部攻撃を受けた際に従業員を懲戒処分とする国内企業の割合は、世界平均を下回っている。

Q4　十分な教育・技術的対策を講じていなかったにもかかわらず、事故の発生のみを理由に重い懲戒処分を科すと、懲戒権濫用と評価される可能性がある。

Q5　NIST CSF2.0 では、新たに「Govern（統治）」機能が独立の機能として設けられた。

Q6　金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」は、金融機関以外の一般企業にも当然に法的義務として適用される。

Q7　個人情報保護法上の安全管理措置は、組織的・人的・物理的・技術的の 4 類型で構成される。

Q8　「Just Culture」とは、故意や重大な規律違反を含め、あらゆるミスの責任を一律に免除する考え方である。

Q9　懲戒処分を行った場合には、それをもって事案を終了させ、別途の再発防止策は不要である。

Q10　事故発生後に隠蔽・虚偽説明・報告遅延を行ったことは、事故を起こした行為とは別個の義務違反として評価し得る。

【解答】Q1×　Q2〇　Q3×（上回っている）　Q4〇　Q5〇　Q6×（金融機関以外へは当然には法的義務とならない）　Q7〇　Q8×（故意・重大な規律違反には責任を問う）　Q9×（処分と再発防止は別に実施）　Q10〇

以 上