突然CISOに任命された**ら？ CISOがサンドバックにならないための事前準備**

武田一城 (ラック) 2019年01月07日 06時00分

　本連載「[企業セキュリティの歩き方](https://japan.zdnet.com/security/sp_17securityarukikata/)」では、セキュリティ業界を取り巻く現状や課題、問題点をひもときながら、サイバーセキュリティを向上させていくための視点やヒントを提示する。

　前回の記事「[CSIRTの現状と苦悩、次の一手](https://japan.zdnet.com/article/35126517/)」では、2015年に経済産業省や情報処理推進機構（IPA）から公開された「サイバーセキュリティ経営ガイドライン」（2015年にv1.0、2017年にはv2.0が公開された）によって、最高情報セキュリティ責任者（CISO）の任命やCSIRT（Computer Security Incident Response Team）の設置が日本の企業や団体の間で進んだことと、米国国立標準技術研究所（NIST）が作成した「サイバーセキュリティフレームワーク」に記載されている「特定」「防御」「検知」「対応」「復旧」の5つのプロセス整備の重要性について記した。今回は、CISOに任命された人が実行しなければならない次のアクションについて述べたい。

**CISOとは何なのか？**

　CISOは、企業内で情報セキュリティを統括する経営レベルの最高責任者（担当役員のポジションが多い）であり、サーバやPC、ネットワークなどの情報システム全般のセキュリティ対策はもちろん、機密情報や個人情報などその企業で「重要な情報」と定義された情報を守ることを主な役割としている。また、より対象範囲の広い「最高セキュリティ責任者（CSO＝Chief Security Officer）」と称する場合もあるが、各社によって事情が異なるだけで、本質的な存在意義にほとんど違いはない。

　日本では、標的型攻撃などの脅威や本連載で何度か取り上げているサイバーセキュリティ経営ガイドラインなどによって、CISOの必要性や認知度が広まった。CISOは、最高情報責任者（CIO＝Chief Information Officer）や情報システム部長、非IT系部門のリスク管理部長や管掌役員などが兼務している場合なども多く、職位や組織内での立場は企業・組織でまちまちだ。しかしながら、情報セキュリティの脅威や課題、現状を経営層に伝えることが最も重要な役割であることに変わりはない。

　情報セキュリティがITシステムの問題として情報システム部門だけで対応していく時代は終わった。セキュリティ対策は、企業や組織全体の課題として認識し対応すべきものになった。加えて、万一のインシデント発生時にCSIRTなどで対応していく機能が、社会的責任を果たす企業として必要不可欠なものとなった。その中心がCISOであり、サイバーの脅威とその対策の最前線である現場と経営層をつなぐ大事なポジションとして注目されてきたのだ。

**CISOは何をすべきか？**

　サイバーセキュリティ経営ガイドラインが公開された2015年当時、筆者はこれが、セキュリティ業界の有識者や技術者たちからそれほど高く評価されなかったと感じた。なぜなら、サイバー攻撃の手法や具体的な防御策などに関する記載がほとんどなかったからだ。最前線で活躍している人たちには物足りなかったのではないか。

　それでも、先述したようにこのガイドラインの公開で、情報システム部門だけに頼らないセキュリティ対策の重要性が広く認知された。それは、前回の記事で示した日本シーサート協議会（NCA）の会員数の増加ぶりでも裏付けされる。このように、サイバーセキュリティ経営ガイドラインは非常に意義があるものだったが、一つ足りないものがあった。それは、「***CISOが具体的に何をどうすればよいのか？***」ということに関する記載だ。

　このガイドラインの内容は、ポリシーの順守を目的としたPDCAフレームワーク活用とCSIRT設置が中心であり、CISOがその業務執行に必要なビジネスの視点などが盛り込まれていなかった。つまり、経営者はCISOを任命し、リスク管理やセキュリティ対策に関する多くの権限を与えた。しかし、任命されたCISOは、「自分が何をしてよいか分からない」という状況に陥ってしまうことになる。

　もちろん、任命されたCISOが経営や業務執行に関する理解と情報システムの構造や要素技術、サイバー攻撃の手法などに熟知していれば、現場と経営者の橋渡しも問題なくできるだろう。しかし、それらに高いレベルで精通する人材など、そうはいない。その結果、名ばかりのCISO、機能しないCISOが誕生してしまうことになる。

## CISOが経営者の“免罪符”になる？

　さらに言えば、セキュリティ対策が経営やビジネスにどう貢献できるものかという観点で考えることは、残念ながらまだ一般的ではない。むしろ、危険性や損失といったマイナス面ばかりがいまだ注目されてしまっている。そのためCISOの任命は企業にとって、「サイバーセキュリティ経営ガイドラインに沿ったセキュリティ対策をしています」という免罪符にしかならないことが現実問題として起こり得るのだ。

　そのような免罪符が、サイバー攻撃に通用するわけがない。効果がないどころか、企業は対策をしたつもりで実際は脆弱性を多く抱える状態になってしまい、むしろ攻撃側にとって都合の良い状況さえもたらしかねない。

　そのような状況でインシデントが発生したら、どうなるだろうか。CISOが経営者から責任を追及されるのは、まず間違いない。何の準備もしないままその状況に陥れば、サンドバックのようになることも覚悟しなければならないだろう。

　CISOが実行すべき準備とは、現状のリスクをきちんと経営者に伝え、情報システム部門には攻撃をできるだけ早く検知できるツールと的確に対応する仕組みを提供し、事業部門に必要な情報をリアルタイムに伝えるといったことになる。これができないと、これらの関係部門の全方位から非難の集中砲火を浴びる恐れすらある。

## サンドバック化を回避する「CISOハンドブック」

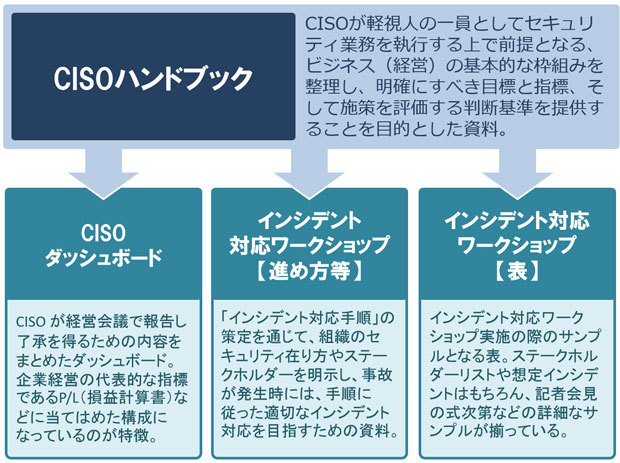
　もし、読者のあなたが経営や業務と情報システムの双方の分野で高度な知見を有するスーパーマンではないにも関わらずCISOに任命されたら、どうすればよいのだろうか。何もできなければ、先述した大きなリスクを背負い込むことになってしまう。

　これを解決するには、CISOがセキュリティ業務を執行する経営陣の一員として、その前提となる経営やビジネスの基本的な枠組みを整理し、明確にすべき目標と指標、そして施策を評価する判断基準を提供することが肝心だ。そのようなCISOの道標になるような資料が存在する。

　それは、日本ネットワークセキュリティ協会（JNSA）のCISO支援ワーキンググループが2018年6月に公開した「[CISOハンドブック](https://www.jnsa.org/result/2018/act_ciso/index.html)」という資料だ。この資料の冒頭に以下の6項目が書かれており、「本書の使い方」として紹介している。

1. 経営会議で資料を作る際のひな型
2. 技術担当からCISOになった人がビジネスを理解するための参考として
3. セキュリティ経験の少ないCISOがセキュリティ業務を理解するための参考として
4. 経営会議で話される業務執行（CISOの役割と責任、業務）の概要を理解する参考として
5. ビジネスに関連付けた計測項目と判断基準の例として
6. ビジネスに沿ったセキュリティ計画や事業継続計画の策定資料として

　さらに、「どうやって経営会議で了承を得るか」という観点のほか、インシデントの対応を適切かつ遅滞なく実施するためのワークショップに役立つツール群も伴っている。

  
「CISOハンドブック」を構成する資料

　このようにCISOハンドブックは、CISOに任命された人が何をすべきかの指針とCISOとして必要なその組織内の各部門や経営層を巻き込む具体的なツール群で構成されている。分量は多く内容の理解もそれほどやさしいものではないが、世の中のCISOを満身創痍（そうい）で四面楚歌（そか）のような状況から救うために役立つものになるはずだ。

　実は筆者自身もこのハンドブックの執筆メンバーの末席に名を連ねており、手前味噌な紹介になってしまうが、セキュリティ業界の大ベテランたちが実際に経験した苦労などが詰まった内容が盛り込まれており、それなりに気づきを与えられる内容だと考えている。

　また、実際にこのワーキンググループのメンバーの一人がハンドブックの内容や執筆過程のディスカッションに触発されて30年以上勤務した企業（セキュリティベンダー）を退職し、セキュリティ対策面で大きな課題を持つ別の企業のCISOに就任するというまさかの展開もあった。一般に、課題を認識した上で自分の利益にならないのにも関わらず、危険を冒すことを「火中の栗を拾う」と表現されるが、この方の選択は火中の栗を拾うなどという生半可なものではない。詳細は諸般の事情により割愛するが、火中の栗へダイビングする「火中の栗ダイバー」とでも呼ぶべきものだと思われる。このことが、将来的に非常なる大英断なのか、イチかバチかの大博打だったのかは、神のみぞ知るところだろう。

　このように、CISOハンドブックはセキュリティ対策や企業や組織のリスク管理の先人たちの知恵や経験値が詰まっている。もし、あなたがCISOに突然任命された場合には、何もせずに時が過ぎ、インシデント発生時などにサンドバックにならないために、このCISOハンドブックを利用してほしい。CISOがサンドバックにならないために、このCISOハンドブックが有効利用されることを切に祈りたい。

**武田 一城（たけだ かずしろ）**

株式会社ラック  
1974年生まれ。システムプラットフォーム、セキュリティ分野の業界構造や仕組みに詳しいマーケティングのスペシャリスト。次世代型ファイアウォールほか、数多くの新事業の立ち上げを経験している。web/雑誌ほかの種媒体への執筆実績も多数あり。 NPO法人日本PostgreSQLユーザ会理事。日本ネットワークセキュリティ協会（JNSA）のワーキンググループや情報処理推進機構（IPA）の委員会活動、各種シンポジウムや研究会、勉強会での講演なども精力的に活動している。

[«](https://japan.zdnet.com/article/35130613/) [1](https://japan.zdnet.com/article/35130613/) **2**

[**ZDNet Japan トップへ**](https://japan.zdnet.com/)

## この記事を読んだ方に

## 関連記事

### [**「3カ月の商談が1カ月に」セールスフォースの金融向けSaaSの広がり具合**](https://japan.techrepublic.com/article/35130099.htm)

### [**突然CISOに任命されたら？--CSIRTの現状と苦悩、次の一手**](https://japan.zdnet.com/article/35126517/)

### [**突然CISOに任命されたら？--セキュリティ業界を変えた2つのインパクト**](https://japan.zdnet.com/article/35126516/)

### [**CISOの役割や仕事とは？--JNSAが公開したハンドブックの中身**](https://japan.zdnet.com/article/35119935/)

### [**2018年に学ぶべきでないプログラミング言語5選--コミュニティ、求人、成長の視点から**](https://japan.techrepublic.com/article/35115464.htm)

## [「企業セキュリティの歩き方」](https://japan.zdnet.com/security/sp_17securityarukikata/?tag=mcol;backNumber) バックナンバー

### [**突然CISOに任命されたら？ CISOがサンドバックにならないための事前準備**](https://japan.zdnet.com/article/35130613/)

### [**突然CISOに任命されたら？--CSIRTの現状と苦悩、次の一手**](https://japan.zdnet.com/article/35126517/)

### [**突然CISOに任命されたら？--セキュリティ業界を変えた2つのインパクト**](https://japan.zdnet.com/article/35126516/)

**関連ホワイトペーパー**

* [CISO300人実態調査から探る「セキュリティ対応のベストプラクティス」](https://japan.zdnet.com/paper/30000956/30002628/?tag=d_sleaf_recom_logly)https://abc.logly.co.jp/abc?ac=IJcHR-RS8jDjuIV4x7jRng&pt=1&sp=3755496&st=https%3A%2F%2Fjapan.zdnet.com%2Fpaper%2F&lg=similarity&wd=1449&rd=&ct=6
* [全世界700名のセキュリティ・リーダーへ意識調査-直面する課題とコグニティブ活用への期待](https://japan.zdnet.com/paper/30000342/30002301/?tag=d_sleaf_recom_logly)
* [【チェックリスト付】シナリオ別に考えるクラウド時代のサイバーセキュリティ対策ハンドブック](https://japan.zdnet.com/paper/30001007/30002526/?tag=d_sleaf_recom_logly)
* [社員のセキュリティアウェアネス向上がインシデントへの最適解！](https://japan.zdnet.com/paper/20012657/30002388/?tag=d_sleaf_recom_logly)
* [守りたいポイントで選ぶMSS! 入口・出口・内部・エンドポイント・クラウドにおける脅威対策を実現する](https://japan.zdnet.com/paper/20013091/30002819/?tag=d_sleaf_recom_logly)
* [セキュリティ事情のいまを知る--ワールドワイド・インフラストラクチャー・セキュリティ・レポート](https://japan.zdnet.com/paper/30000894/30002706/?tag=d_sleaf_recom_logly)

## 連載

[**CIO**](https://japan.zdnet.com/cio/)

[ITアナリストが知る日本企業の「ITの盲点」](https://japan.zdnet.com/cio/sp_18it-analyst/)

[シェアリングエコノミーの衝撃](https://japan.zdnet.com/cio/sp_18share/)

[デジタル“失敗学”](https://japan.zdnet.com/cio/sp_18failure-studies/)

[コンサルティング現場のカラクリ](https://japan.zdnet.com/cio/sp_17consul/)

[Rethink Internet：インターネット再考](https://japan.zdnet.com/cio/sp_16rethink_internet/)

[インシデントをもたらすヒューマンエラー](https://japan.zdnet.com/cio/sp_17humanerror/)

[トランザクションの今昔物語](https://japan.zdnet.com/cio/sp_17transactions/)

[エリック松永のデジタルIQ道場](https://japan.zdnet.com/cio/sp_17eric/)

[研究現場から見たAI](https://japan.zdnet.com/cio/sp_16airesearch/)

[Fintechの正体](https://japan.zdnet.com/cio/sp16_fintech/)

[米ZDNet編集長Larryの独り言](https://japan.zdnet.com/cio/sp15_us_editorinchief/)

[大木豊成「仕事で使うアップルのトリセツ」](https://japan.zdnet.com/cio/sp_15oki/)

[山本雅史「ハードから読み解くITトレンド放談」](https://japan.zdnet.com/cio/sp_17hardwaretrends/)

[田中克己「展望2020年のIT企業」](https://japan.zdnet.com/cio/sp_14tenbou2020/)

[松岡功「一言もの申す」](https://japan.zdnet.com/cio/sp_13matsuokaopinion/)

[松岡功「今週の明言」](https://japan.zdnet.com/cio/sp_12matsuoka/)

[内山悟志「IT部門はどこに向かうのか」](https://japan.zdnet.com/cio/sp_15uchiyama/)

[林 雅之「デジタル未来からの手紙」](https://japan.zdnet.com/cio/sp16_future/)

[谷川耕一「エンプラITならこれは知っとけ」](https://japan.zdnet.com/cio/sp_15tanikawa/)

[大河原克行「エンプラ徒然」](https://japan.zdnet.com/cio/sp_09ohkawara/)

[内製化とユーザー体験の関係](https://japan.zdnet.com/cio/sp_16inside/)

[「プロジェクトマネジメント」の解き方](https://japan.zdnet.com/cio/sp16_pm/)

[ITは「ひみつ道具」の夢を見る](https://japan.zdnet.com/cio/sp_16himitsu/)

[**セキュリティ**](https://japan.zdnet.com/security/)

[エンドポイントセキュリティの4つの「基礎」](https://japan.zdnet.com/security/sp_18endpoint/)

[企業セキュリティの歩き方](https://japan.zdnet.com/security/sp_17securityarukikata/)

[サイバーセキュリティ未来考](https://japan.zdnet.com/security/sp_17futurecybersecurity/)

[ネットワークセキュリティの要諦](https://japan.zdnet.com/security/sp_networksec/)

[セキュリティの論点](https://japan.zdnet.com/security/sp_13securityissues/)

[**スペシャル**](https://japan.zdnet.com/sp/)

[エンタープライズAIの隆盛](https://japan.zdnet.com/software/sp_18enterpriseai/)

[インシュアテックで変わる保険業界](https://japan.zdnet.com/software/sp_18insuretech/)

[顧客は勝手に育たない--MAツール導入の心得](https://japan.zdnet.com/marketing/sp_18ma/)

[「ひとり情シス」の本当のところ](https://japan.zdnet.com/it-management/sp_18hitori/)

[ざっくり解決！SNS担当者お悩み相談室](https://japan.zdnet.com/marketing/sp_18sns_consulting/)

[生産性向上に効くビジネスITツール最前線](https://japan.zdnet.com/software/sp_18biz_tool/)

[ざっくりわかるSNSマーケティング入門](https://japan.zdnet.com/marketing/sp_17sns_marketing/)

[課題解決のためのUI/UX](https://japan.zdnet.com/software/sp17_uiux/)

[誰もが開発者になる時代 ～業務システム開発の現場を行く～](https://japan.zdnet.com/cloud/sp_16isa/)

[「Windows 10」法人導入の手引き](https://japan.zdnet.com/software/sp_15windows10/)

[ソフトウェア開発パラダイムの進化](https://japan.zdnet.com/software/sp_17kaihatu/)

[エンタープライズトレンド](https://japan.zdnet.com/sp/enterprise-trend/)

[10の事情](https://japan.zdnet.com/tag/10%E3%81%AE%E4%BA%8B%E6%83%85/)

[座談会＠ZDNet](https://japan.zdnet.com/keyword/%E5%BA%A7%E8%AB%87%E4%BC%9A%EF%BC%A0ZDNet/)

[Dr.津田のクラウドトップガン対談](https://japan.zdnet.com/cloud/sp_16cloudtopgun/)

[Gartner Symposium](https://japan.zdnet.com/keyword/Gartner%20Symposium/)

[IBM World of Watson](https://japan.zdnet.com/keyword/IBM%20World%20of%20Watson/)

[de:code](https://japan.zdnet.com/keyword/de%3Acode/)

[Sapphire Now](https://japan.zdnet.com/keyword/Sapphire%20Now/)

[VMworld](https://japan.zdnet.com/keyword/VMWorld/)

[Microsoft WPC](https://japan.zdnet.com/keyword/Microsoft%20WPC/)

[Microsoft Connect()](https://japan.zdnet.com/keyword/Microsoft%20Connect%28%29%3B/)

[HPE Discover](https://japan.zdnet.com/keyword/HPE%20Discover/)

[Oracle OpenWorld](https://japan.zdnet.com/keyword/Oracle%20OpenWorld/)

[Dell Technologies World](https://japan.zdnet.com/keyword/Dell+EMC+World/)

[AWS re:Invent](https://japan.zdnet.com/keyword/AWS%20re:Invent/)

[AWS Summit](https://japan.zdnet.com/keyword/AWS%20Summit/)

[PTC LiveWorx](https://japan.zdnet.com/keyword/PTC%20LiveWorx/)

[吉田行男「より賢く活用するためのOSS最新動向」](https://japan.zdnet.com/software/sp_15yoshida/)

[古賀政純「Dockerがもたらすビジネス変革」](https://japan.zdnet.com/cloud/sp_16koga/)

[中国ビジネス四方山話](https://japan.zdnet.com/development/sp_14china/)

[ベトナムでビジネス](https://japan.zdnet.com/development/sp_13vietnam/)

[日本株展望](https://japan.zdnet.com/tag/%E6%97%A5%E6%9C%AC%E6%A0%AA%E5%B1%95%E6%9C%9B/)

[企業決算](https://japan.zdnet.com/keyword/%E4%BC%81%E6%A5%AD%E6%B1%BA%E7%AE%97/)

## [CNET Japanトップストーリー](https://japan.cnet.com/)

* [「RICOH THETA」が不動産業界で示した存在感--BtoBでも広がる360度の可能性](https://japan.cnet.com/article/35130321/)
* [HPやAcerが新型ノートPC発表--AMDプロセッサ搭載「Chromebook」など](https://japan.cnet.com/article/35130877/)
* [ブロックチェーンを用いた新たなスマート・コントラクト技術Plutus（プルータス）とは？](https://japan.cnet.com/article/35130700/)
* [LED照明にプロジェクターを一体化「popIn Aladdin」--設置から操作まで2カ月徹底レビュー](https://japan.cnet.com/article/35130714/)
* [ヤフー“第二の創業”に挑む川邊社長--PayPayやデータドリヴンは次の柱になるか](https://japan.cnet.com/article/35124277/)