D3001 高等教育機関等における CISO の選任および実務の指針

国立情報学研究所 学術研究プラットフォーム運営・連携本部

セキュリティ運営委員会
高等教育機関における情報セキュリティポリシー推進委員会

改定履歴

日付・文書番号	改定内容	担当
2024年3月29日 D3001	新規作成	南 弘征（北海道大学） セキュリティ運営委員会 高等教育機関における情報セキュリティポリシー推進委員会

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。
sp-comment[at]nii.ac.jp　（[at]を@に置き換えてください）
担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

著作者：国立情報学研究所 学術研究プラットフォーム運営・連携本部 セキュリティ運営委員会
及び高等教育機関における情報セキュリティポリシー推進委員会
https://www.nii.ac.jp/service/sp/

本文書の目的と構成

本文書は高等教育機関等において、組織的なセキュリティ対策の推進が求められていることを踏まえ、推進の中核を担う最高情報セキュリティ責任者（CISO）の活躍に資する観点から、当該機関の最高情報セキュリティ責任者（CISO）を任命する際、及び CISO としてその役割を実践する際に認識すべき事項をチェックリスト形式で、その解説とともにとりまとめたものです。

本文書は対象者毎に次表の内容で構成されています。

表　本文書の構成

本編	**A. CISO の選任にあたって**	機関の責任者が CISO の職務を規定及び人選する際に、自機関の運営や経営との関わりから認識しておくべき事項を 3 項目のチェックリスト形式で整理しています。
	B. CISO に就かれた方へ	CISO に就任したご本人が最低限認識しておくべき事項を 10 項目のチェックリスト形式で整理しています。
解説編	**チェックリスト A&B 解説**	上記 A.B.のチェック項目毎に背景となる事項を解説しています。当事者の方々のみならず、その補佐役の方にも参考となる情報を記載しています。
	CISO 実務にあたっての 伴走資料	CISO 実務を遂行する上で有用な情報源の解説です。

本編

A. CISO の選任にあたって

～ 組織運営・経営との関わり ～

- 最高情報セキュリティ責任者（CISO）は経営層に属していますか？
  技術的有識者を CISO とできない場合には、それを補う補佐を置くなど、機関としての工夫を講じていますか？
- CISO に選任された方は、自機関の CSIRT（Computer Security Incident Response Team）の活動内容を理解し、円滑に業務を遂行できるよう努めることが主な役割であると認識されていますか？
- 同一の方が兼任されている場合も含め、CISO と最高情報責任者（CIO）との間で、意思決定の優先順位を、機関内で予め定めていますか？

B. CISO に就かれた方へ

～ ご認識頂くべき最低限の事項 ～

B.1 機関におけるガバナンス

B.1.a. 機関の情報セキュリティポリシーやサイバーセキュリティに関する計画を理解した上で、サイバーセキュリティリスクを的確に認識し、対峙すべく、機関において実効性のある方針や対応体制を策定し実施できていますか？

B.1.b. 自機関においては、CSIRT の運営を含む管理体制が確立され、円滑に運用されるよう、組織整備をされていますか？

B.1.c. 機関のサイバーセキュリティ水準の維持向上に要するリソースを確保できていますか？

B.1.d. ここまでの３項目について、実効性を損なわぬよう、常に改善を模索していますか？

B.1.e. インシデント発生時、完全収束と再発防止策のメドを立てるまでが任務であると認識されていますか？

B.2 機関における責任者としての役割

B.2.a. 自らが機関におけるサイバーセキュリティの最終的な責任者であると自認されていますか？

B.2.b. 自らでは対応の及ばない事項について、補佐への一部権限委譲なども含め、責任者として適時適確な対応が可能な体制を確立していますか？

B.3 責任者としての自己研鑽・自制

B.3.a. CISO 向けの研修機会などを活かし、可能な範囲で、技術的知識の会得と更新に努められていますか？

B.3.b. 世間一般でのサイバーセキュリティ情勢について、キャッチアップや更新を心がけていますか？

B.3.c. 重責のもと、自らが全てにあたらねば、と、熱心さのあまりかえって混乱させたり、補佐や CSIRT を叱責したりすることのないよう、心がけていますか？

解説編

チェックリスト A&B 解説

解説 A. CISO の選任にあたって ～組織運営・経営との関わり～

最高情報セキュリティ責任者（CISO）は経営層に属していますか？
技術的有識者を CISO とできない場合には、それを補う補佐を置くなど、機関としての工夫を講じていますか？

今日、サイバーセキュリティ関連のインシデントを生じさせた機関においては、事案の軽重にもよりますが、外部機関による調査や、復旧・再発防止策の立案と実施を、社会的に求められることがあります。また、情報漏洩を伴うインシデントとなれば、状況に応じた損害賠償など、かなりの費用や、対応に当たっての人的コストも必要となりえます。加えて、機関としての社会的信用の毀損も懸念されるなど、前世紀には技術的不備等と見なされ、情報機器の管理を担ってきた教職員の責任であるかのように思われてきたセキュリティインシデントは、まさに組織運営の問題と捉えるべき時代になっています。世界的に見ても、組織の活動において、サイバーセキュリティリスクは経営問題と認識されており、わかりやすくいえば「名ばかり CISO」はもはや存在を許容されず、むしろそのような存在を許容している機関自体が、社会的に忌避されかねません。また、CISO は緊急の対応が必要になる可能性があり、非常時にはその対応に専従する必要もありえます。さらに、インシデントの発生を予め防ぐべく、組織全体のセキュリティ水準を向上させるための活動を差配したり、インシデントの有無にかかわらず、サイバーセキュリティ全般に関し、機関として意思決定が必要となったときは、経営層としての判断責任が求められます。

従って、組織ガバナンスの観点からも、経営層に属する方が CISO となるべきです。国においても「政府機関等の対策基準策定のためのガイドライン」[1]において、局長級が望ましい旨の解説がなされています（遵守事項 2.1.1(1)(a)「最高情報セキュリティ責任者」について、等）。

実状として、たとえば国立大学法人等では役員数上限が法的に定められており、当該分野に造詣の深くない役員を充てるよりは、技術的見識を持つ学内教員を CISO としている機関もあるかと思います。そのような機関においても、本資料などを踏まえ、再度あり方を検討頂き、有識者を新たに役員とするか、CISO となる役員が他業務も抱えて充分なエフォートを割けないと想定されるようであれば、技術的見識をもち、かつ、CISO に比べれば優先的な対応が可能である補佐を置き、緊急時には一部権限を委ねるなど、機関内での充分な工夫を推奨するものです。

[1] https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

CISO に選任された方は、自機関の CSIRT（Computer Security Incident Response Team）の活動内容を理解し、円滑に業務を遂行できるよう努めることが主な役割であると認識されていますか？

CISO 自らがインシデント対応のすべてに関わる必要はありません。多角的な事案も増えており、インシデント対応や平時のセキュリティ水準向上などは、チームで取り組むべきです。そのチームが円滑に任務をこなせるような環境整備ならびに機関内各部署とのリエゾン、また、最終的には自機関を代表しての判断を担うことが、CISO の主な任務であるとお考えください。

同一の方が兼任されている場合も含め、CISO と最高情報責任者（CIO）との間で、意思決定の優先順位を、機関内で予め定めていますか？

利便性と安全性はトレードオフの関係にあります。CIO は今日、DX（Digital Transformation）の旗振り役をされていることも多く、セキュリティ対策とは往々にして衝突する可能性が高いと考えられます。同一人でない場合は意見交換を経て妥協点を模索できるかもしれませんが、兼任の場合にはどちらの側を優先するか自ら判断することになりますので、原則論としてどちらの判断が優先するか、リスクも含め、予め定めておく方が混乱や衝突を避ける意味で有効と考えられます。もっとも、利便性を下げるリスクよりはサイバーセキュリティに関するリスクの方が重大と考えられ、CISO 側の判断を優先させることが機関に資するものと一般に考えられます。

解説 B. CISO に就かれた方へ ～ご認識いただくべき最低限の事項～

B.1. 機関におけるガバナンス

B.1.a. 機関の情報セキュリティポリシーやサイバーセキュリティに関する計画を理解した上で、サイバーセキュリティリスクを的確に認識し、対峙すべく、機関において実効性のある方針や対応体制を策定し実施できていますか？

高等教育機関等では、学問の自由などの観点から、研究者自らで物品を選定、購入したり、サービスを契約するなど、自ら研究環境を整え、自らが機器等の管理運営を行い、自らで他機関との共同研究をする（すなわち、学外者と情報や環境を共有する）ことが珍しくありません。また、最近では、外部クラウドサービスの利活用も推奨され、さまざまな外部サービスも併用されているでしょう。

上意下達で統一的に環境が提供され、いわば統制管理下で提供される IT 環境で業務を遂行する民間企業等とはその点が決定的に異なり、統制のとれないことこそが、まさに大きなリスクをはらんでいます。

研究者個々人の活動に制約を設けることはさまざまな意味で難しいでしょうから、可能な限り、機関内でどのような機器や外部サービスが導入、運用されていて、管理体制はどのようになっていて、万一何か異変が疑われる場合にはどこに連絡し、どのように対応するか、などを的確に把握し、それらに基づいて全体的なサイバーセキュリティ対策を講じるための計画立案や、具体的な活動方針を定めなければ、実効性は伴わないでしょう。CISO 自身がそれらの司令塔であることを明確に認識してください。

B.1.b. 自機関においては、CSIRT の運営を含む管理体制が確立され、円滑に運用されるよう、組織整備をされていますか？

B.1.c. 機関のサイバーセキュリティ水準の維持向上に要するリソースを確保できていますか？

機関の規模にもよりますが、CSIRT が、機関等の役員など、強制力を伴うような役職の方を実働メンバーとされていることは稀でしょう。裏を返せば、実務の現場に携わる教職員が、機関全体に対して直接的な提案を行うポジションにいることも、やはり稀でしょう。従って、CSIRT がその任を継続的に果たせるよう、組織運営・人的およびコスト的なリソースの確保が CISO に求められるものとご理解ください。

また、経営層や準ずる層に対し、情報が適時適切にエスカレーションされるような体制づくりや、場合によっては自ら聞き取るような姿勢も求められるかもしれません。先にも触れましたが実質的な「名ばかり CISO」とならぬよう、工夫に努めてください。

さらに、既に触れたとおり、サイバーセキュリティ事案は今や自機関全体に関わる問題であり、自機関において CSIRT をインシデント通報窓口として周知していても、組織問題として総務的な部署へ公式連絡があったり、ともすれば SNS や内部通報窓口など、多種多様

な通報経路が想定されます。それらの通報が CSIRT にいち早く共有されるような連携体制の構築、維持も CISO の役割の一つでしょう。

加えて、最前線でセキュリティリスクと対峙している教職員との意思疎通は充分できているか、それらの員数は自機関の規模に比して適切か、特定の技術的有識者に過度な負担を強いていないか、経年劣化しかけているシステムを延々と使い続けていないか、など、留意し配慮すべきことは多いでしょう。特に、規模や内容が重大なインシデントを生じた場合には、監督官庁はもとより、内閣サイバーセキュリティセンター（NISC）、都道府県警察、国の個人情報保護委員会などとの対応が、ともすれば年単位で続きかねません。ご自身を含め、対応している教職員の異動や所要経費の増減などによって、対応が停滞せぬよう、中長期的なリソースの確保も必要です。

B.1.d. ここまでの 3 項目について、実効性を損なわぬよう、常に改善を模索していますか？

「仏作って魂入れず」とならぬよう、平時にあっても、自ら、そして自機関構成員に対しても、さまざまな研鑽機会を設けるなど、常にアクティブであるとともに、機関の実状にあった水準向上策を検討し続けてください。

B.1.e. インシデント発生時、完全収束と再発防止策のメドを立てるまでが任務であると認識されていますか？

インシデント発生時、攻撃遮断→当座の拡大防止→原因究明→対応策適用→運用再開が 1 サイクルと考えがちですが、類例を生じぬよう、再発防止策を検討し、実施に移すことまでをミッションと考えるべきです。

B.2. 機関における責任者としての役割

B.2.a. 自らが機関におけるサイバーセキュリティの最終的な責任者であると自認されていますか？

B.2.b. 自らでは対応の及ばない事項について、補佐への一部権限委譲なども含め、責任者として適時適確な対応が可能な体制を確立していますか？

たとえ実質的に名ばかりでも、名称の示すとおり、CISO は、所属機関におけるセキュリティの最高責任者です。「詳しくないからよくわからず、私の責任ではない」とは決していえません。補佐や CSIRT による対応に関しても、当然ながら CISO が最終的な責任を負います。その覚悟を常にお持ちください。

また、他項目とも関連しますが、責任を負われる以上、特に機関内での概況は常に把握し、自らの技術的技量が及ばないとしても、機関トップや役員層との適時適確な情報共有、事案発生時の公表判断、時期の調整などを含む他部署との折衝など、立場上可能、もしくは立場上ご自身しかできないことがあると思います。機関内のセキュリティ体制におけるご自身の、いわば実質的な立ち位置を認識の上、機関のために尽力ください。

B.3. 責任者としての自己研鑽・自制

B.3.a. CISO 向けの研修機会などを活かし、可能な範囲で、技術的知識の会得と更新に努められていますか？

監督官庁をはじめ、民間などでも、経営・マネジメント層向けのサイバーセキュリティ研修などの機会が設けられています。漏れ聞くところでは、実情はともかく、多忙等を理由に機会を逸していたり、各機関からの参加が事実上義務づけられている場合にあっても、補佐や CSIRT メンバー、極端な例では平時の用務が異なる職員を代理出席させているような事例も側聞します。ご自身の研鑽はもとより、他機関の CISO との交流の機会ともなりますので、極力参加されることを強く推奨するものです。

B.3.b. 世間一般でのサイバーセキュリティ情勢について、キャッチアップや更新を心がけていますか？

選任にあたっての記載とやや矛盾しますが、CSIRT から概略的な説明をされ、それが技術的に平易な内容であっても全く理解できないようですと、問題点の本質を把握できないままに動くことになります。仮に補佐を置いていても、やはり意思疎通に支障を来すようでは、組織的な対応もままならなくなります。

また、昨今では、サイバーセキュリティに関する世間の関心もあり、相応以上の規模のものは、一般的なマスコミでも取り上げられる傾向にあります。

エキスパートになる必要はありませんが、概要が理解できる程度に、ご自身での研鑽や情報収集をお勧めいたします。

B.3.c. 重責のもと、自らが全てにあたらねば、と、熱心さのあまりかえって混乱させたり、補佐や CSIRT を叱責したりすることのないよう、心がけていますか？

ご自身が有識者であったり、あるいは研鑽を独自に積まれたりした CISO が、CSIRT に対して微に入り細に入り関わるような例があると聞き及びます。サイバーセキュリティに関する事案では、多角的検討が肝要な時勢となっており、たとえ有識者であっても、独断まがいの対応は、リスク管理としても慎むべきです。CISO 自身が独善的になっていないか、常に自問しましょう。

そもそも論ですが、CISO は CSIRT を指導・監督する任にあらず、もちろん責任転嫁の対象でもありません。例として、CSIRT がもたらした調査結果が、その後の調査で二転三転し、訂正を余儀なくされることはままあります。その場合、前項のとおり、CISO は最終責任者としてやむなく叱責される存在です。しかし、それをそのまま CSIRT や関連教職員に転嫁すれば、精神的負担の多い CSIRT 構成員のモチベーションを著しく低下させ、ひいては自機関のセキュリティレベル低下につながるでしょう。自ら運用体制を損ねることのないよう、常に留意ください。

CISO 実務にあたっての伴走資料

高等教育機関の情報セキュリティ対策のためのサンプル規程集（国立情報学研究所）
https://www.nii.ac.jp/service/sp/
※特に以下の各文書

D1001 情報セキュリティ対策基本規程 うち D1001-04 全学総括責任者の項
D2103 情報セキュリティインシデント対応チーム（CSIRT）設置規程
D3103 インシデント対応手順策定に関する解説書
D3303 役職員向け説明資料作成ガイドライン

次項に示す「政府機関等のサイバーセキュリティ対策のための統一基準群」（以下、統一基準）において遵守を求めている対策事項を高等教育機関に適用するため、仮想の A 大学をモデルとして同校の規程体系として整備している一連の文書群です。統一基準から改変している内容については、同規程集の「本文書について」に示されています。「※特に以下の項」として示されている文書が CISO として内容を把握しておくべき文書に相当します。

政府機関等のサイバーセキュリティ対策のための統一基準群
（内閣サイバーセキュリティセンター）
https://www.nisc.go.jp/policy/group/general/kijun.html

国の行政機関及び独立行政法人等における情報セキュリティ対策の水準を、必要最低限のベースラインを超えた状態とするために遵守すべき対策事項を規定するものです。最新の令和 5 年度版ではクラウドサービスの利用に関わる対策事項の整理・強化が図られています。本基準群は各機関の規程・手順等が満たすべき事項を定める文書群であり、規程等そのものではないことに留意する必要があります。

サイバーセキュリティ経営ガイドライン（経済産業省・（独）情報処理推進機構）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

デジタル活用を推進する企業の経営者がサイバーセキュリティ対策に関して認識すべき 3 原則と CISO 等に指示すべき重要 10 項目をまとめたものです。最新の第 3 版では、経営者が自覚すべき責任と自組織を取り巻くサプライチェーンへの目配りの重要性を強調しています。高等教育機関等においても、組織の責任者及びその補佐者がセキュリティ対策に関して認識しておくべき事項を把握するために有用です。