高度サイバー攻撃対処のための
リスク評価等のガイドライン

平成 28 年 10 月 7 日

サイバーセキュリティ対策推進会議

目次

第１部　総則

１　本ガイドラインの目的

今日において、政府機関等（府省庁及び独立行政法人等（独立行政法人及びサイバーセキュリティ基本法第十三条に定める指定法人をいう。以下同じ。）をいう。以下同じ。）の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、政府機関等の運営上、極めて重要である。

情報セキュリティ上の脅威は、内部者による規律違反から外部者による攻撃まで多岐にわたって存在し、これらの様々な脅威に対処するため、政府機関等においては、政府機関等の情報セキュリティ対策のための統一基準群に基づき、従来から情報セキュリティ水準の斉一的な引き上げを図っているところである。

一方で、政府機関等においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃（以下「高度サイバー攻撃」という。）が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。

高度サイバー攻撃のうち、昨今、特に大きな脅威となっている標的型攻撃の主目的は、情報システムの端末を不正プログラムに感染させること等ではなく、外部からの情報システム内部への侵入による情報の窃取・破壊等であり、そのために組織力を動員した攻撃が行われることから、内部統制的な手法だけでは十分な防御を行うことは困難であり、情報システムにおける適切な対策の実施及び運用・監視の強化を伴う計画的で持続可能な情報セキュリティ投資が必要となる。

このため、本ガイドラインでは、政府機関等において、高度サイバー攻撃の標的とされる蓋然性が高い業務・情報に重点を置いたメリハリのある資源の投入を計画的に進め、それらの業務・情報に係る多重的な防御の仕組みを実現する際に採るべき手法として、以下に焦点を当てた取組（以下「本取組」という。）について示す。

①　情報セキュリティガバナンスの確立

最高情報セキュリティ責任者（以下「CISO」という。）の指揮の下で、重点的・計画的な情報セキュリティ対策を実施するための方針を決定する。

②　高度サイバー攻撃対処のためのリスク評価の実施

高度サイバー攻撃の標的とされる蓋然性が高い業務領域を選定し、当該業務領域に係るリスク評価に基づく情報セキュリティ対策を重点的に実施する。

③　高度サイバー攻撃対処のための対策の計画的な実施

高度サイバー攻撃の脅威に対抗するための対策の着実な実施に向けて、複数年にわたる計画を策定する。

２　本ガイドラインの位置付け

本ガイドラインは、サイバーセキュリティ戦略（平成 27 年９月４日閣議決定）に基づき、政府機関等における情報及び情報システムに係る情報セキュリティ水準の一層の向上及びサイバー攻撃への対処体制の充実・強化に資するために策定するものである。

本ガイドラインでは、前述の目的を実現するための基本的な考え方及び取組のプロセスを示し、想定される具体的な脅威及び対策その他の迅速かつ柔軟に対応すべき事項については、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）が策定する本ガイドラインの付属書（以下「付属書」という。）に記載する。

なお、本ガイドライン等の改定を含む本取組の運用管理については、第４部に示す。

３　用語定義

本ガイドラインにおける用語の定義は、以下に定めるところによる。

- 「業務領域」：府省庁組織令上の所掌事務、その集合若しくはその一部又は独立行政法人等の個別法等で定める業務、その集合若しくはその一部をいう。
- 「機微業務領域」：所掌事務又は業務に以下の情報の収集、作成等が含まれる業務領域をいう。
  - 窃取、破壊等されることにより、国の安全が害されるおそれがある情報
  - 窃取、破壊等されることにより、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがある情報
  - 窃取、破壊等されることにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがある情報
- 「情報保全担当部署」：自組織における情報保全の推進を担当する課室をいう。
- 「情報セキュリティ担当部署」：自組織における情報セキュリティ対策の推進を担当する課室をいう。
- 「機微業務等実施部署」：本取組におけるリスク評価の対象として選定された業務領域に係る業務を主管する課室をいう。

- 「対象システム」: 本取組の対象として特定された情報システムをいう。
- 「対象システム管理責任部署」: 対象システムの整備又は運用管理を担当する課室をいう。
- 「資源配分部署」: 自組織における人的資源又は資金の配分・管理を行う課室をいう。
- 「対策セット」: 高度サイバー攻撃のシナリオ並びにそれに対応した統制目標及び当該目標を達成するための情報システムの設計、監視強化等に係る対策の集合として、付属書に掲げられたものをいう。

4　適用範囲

(1)　府省庁

本ガイドラインは、法律の規定に基づき内閣に置かれる機関及び内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項及び第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関並びにこれらに置かれる機関に対して適用する。

(2)　独立行政法人等

本ガイドラインは、独立行政法人及びサイバーセキュリティ基本法第十三条に定める指定法人に対して適用する。

第２部　実施事項

１　本取組の流れ

(1)　リスク評価等の実施に向けた準備

ア　リスク評価等の実施に向けたコミュニケーション

本取組は、情報セキュリティ対策についてメリハリのある資源配分を行うため、対象システムを特定し、当該情報システムについて重点的かつ計画的に対策を実施することを最終的な目的として、その過程において「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」を選定し、リスク評価等を実施するものである。

リスク評価等の実施に当たっては、中心的な役割を担う情報保全担当部署と情報セキュリティ担当部署との間で本取組の目的等に関する認識を共有しておく必要があるため、事前に十分なコミュニケーションを図る。

イ　リスク評価の対象とする業務領域の選定

本取組では、高度サイバー攻撃の脅威に対抗することを目的としていることから、その標的とされる蓋然性が高いと考えられる業務領域を選定し、当該業務領域をリスク評価の対象とする。

(2)　リスク評価の実施

ア　保護対象とする業務領域の特定

選定した「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」に対する高度サイバー攻撃事案が発生した場合における組織・業務への影響度等について検討を行い、想定される影響度等に応じて、当該業務領域から本取組における「保護対象とする業務領域」を特定する。

イ　対象システムの特定・現状点検等

特定した「保護対象とする業務領域」において使用されている情報システムを本取組における情報セキュリティ対策の重点化の対象（対象システム）として特定し、対策セットの対策の実施状況を始めとした対象システムの現状点検を行い、対策実施状況及び残存リスクについて評価する。

(3)　リスク評価結果を踏まえた対策導入計画（案）の作成等

ア　対象システムごとの対策導入計画（案）の作成

リスク評価結果、システム更改時期等を踏まえ、対策セットの対策導入を始めとした対象システムごとの対策強化について、検討を行う。また、予算措置や設計変更を伴う対策の実施には一定程度の時間が必要となるため、検討結果から、優先順位や資源配分も勘案し、対策の着実

な導入に向けた計画（以下「対策導入計画」という。）の案を作成する。

イ　対策導入計画（案）の調整

対象システムの情報セキュリティ対策の水準について、関係者間で認識の相違が生じると、情報セキュリティ上の問題が生じる可能性があるほか、対策の導入により対象システムの利便性が低下することも想定されることから、関係者間で共通認識を持ち、協力して計画的に対策を推進するため、対策導入計画（案）の内容を共有するとともに、必要に応じて調整を行う。また、複数の対象システムが特定され、複数の対策導入計画(案)が作成されている場合においては、必要に応じて、それらの間での調整も行う。

(4)　CISOによる方針決定等

ア　リスク評価ダッシュボードの作成

CISOによる方針決定において、CISOがリスク評価結果を基に対策導入計画の妥当性等を円滑に判断できるよう、それらについて的確かつ簡潔に取りまとめた資料（以下「リスク評価ダッシュボード」という。）を作成する。

イ　CISOによる方針決定

政府機関等における情報セキュリティガバナンスを確立し、CISOの指揮の下で高度サイバー攻撃の脅威に対抗していくため、リスク評価結果を判断材料として、対策導入計画の承認等のCISOによる方針決定を行う。

(5)　NISCへの報告

政府機関等全体としての本取組の実施状況等を取りまとめ、サイバーセキュリティ対策推進会議等への報告を行うため、CISOが方針決定した対策導入計画等について、府省庁の計画等は直接、独立行政法人等の計画等は所管府省庁を通じて、それぞれNISCに報告を行う。

２　本取組の実施プロセス

(1)　リスク評価等の実施に向けた準備

ア　リスク評価等の実施に向けたコミュニケーション

情報セキュリティ担当部署は、情報保全担当部署に対して、現在の情報セキュリティ上の脅威、発生事案例等、高度サイバー攻撃事案発生時の影響を検討するための情報を提供する。また、リスク評価の実施を始めとした本取組の目的、実施プロセス等を説明し、それらについて認識を共有するとともに、本取組における両者の役割を明確化する。

イ　リスク評価の対象とする業務領域の選定

情報保全担当部署は、自組織の業務領域から、本取組におけるリスク評価の対象とする「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」を、(ｱ)の要領に従い、自組織において最適な方法により選定する。また、リスク評価の対象とする業務領域の選定に当たっては、(ｲ)の事項に留意する。

(ｱ)　選定要領

①　自組織内の局部課等の事務分掌等に照らした外形的な判断により「機微業務領域」に該当する業務領域を選定する。また、「機微業務領域」には該当しないものの、情報が窃取、破壊等されることにより、行政運営等に壊滅的又は深刻な影響を及ぼすと考えられるなど、その特性等に照らして高度サイバー攻撃の標的となる蓋然性が高いと考えられる業務領域がある場合は、当該業務領域も併せて選定する。

②　①に該当する業務領域がない場合は、自組織において定常的に取り扱う機密性の高い情報の有無について検討し、該当がある場合は当該情報を取り扱う業務領域を選定する。

③　①又は②の業務領域を自組織における「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」として、リスク評価の対象とする。

(ｲ)　選定に当たっての留意事項

・　「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」は、CISO がその重要性を容易に認識できる粒度で選定すること。

・　選定要領の②によって選定する場合は、個別の情報の機密性ではなく、適当な粒度の集合（カテゴリ）としての機密性に焦点を当てた検討を行うこと。

・　「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」を選定するための作業に極力負荷をかけず、継続的に実施できる方法で選定すること。

(2) リスク評価の実施

ア　保護対象とする業務領域の特定

情報保全担当部署は、選定した「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」の機微業務等実施部署に対して、当該業務領域に係るリスク評価を依頼する。

機微業務等実施部署は、「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」に対する高度サイバー攻撃事案が発生した場合における組織・業務への影響度等について検討を行い、その結果をリスク評価等に係る作業シート（以下「リスク評価ワークシート」という。）に記入する。

情報保全担当部署は、機微業務等実施部署における検討結果に応じて、選定した「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」の全部又は一部を本取組における「保護対象とする業務領域」として特定する。

なお、本プロセスの過程で、情報保全担当部署が選定したもの以外の業務領域を「高度サイバー攻撃の標的とされる蓋然性が高い業務領域」として扱う必要性が認められた場合は、情報保全担当部署その他の関係部署において必要な調整を行う。

イ　対象システムの特定・現状点検等

(ｱ)　対象システムの特定

情報保全担当部署又は情報セキュリティ担当部署は、以下に該当する情報システムを対象システムとして特定する。

なお、対象システムに該当がない「保護対象とする業務領域」については、以降の実施プロセスの対象外とする。

①　インターネットに直接又は間接的に接続されているネットワーク（以下「オープン系ネットワーク」という。）上に存在する情報システムのうち、機微業務等実施部署が「保護対象とする業務領域」の業務を遂行する上で使用するもの

②　オープン系ネットワーク上に存在する情報システム（①に該当するものを除く。）であって、機微業務等実施部署が「保護対象とする業務領域」の業務を遂行する上で使用する外部ネットワークから切り離された情報システムとの間で、何らかの手段により「保護対象とする業務領域」に係る電子データ（機密性の高い情報そのもののほか、当該情報を推測し得る周辺情報を含む。）をやり取りするもの

(ｲ)　対象システムの現状点検等

情報セキュリティ担当部署は、特定した対象システムの対象システム管理責任部署に対して、当該情報システムに係るリスク評価等

を依頼する。

対象システム管理責任部署は、当該システムの構成要素を確認し、対策セットの中で対策が求められている構成要素ごとに対策セットの対策を実施しているかなど、対策実施状況を点検する。また、現在の対策実施状況における残存リスクを把握し、これらのリスク評価結果をリスク評価ワークシートに記入する。

なお、対象システムが他の情報システム上に構築されているなど、対象システム管理責任部署のみで点検等を実施できない場合は、情報セキュリティ担当部署とともに、当該他の情報システムの整備又は運用管理を担当する課室と調整を行い、必要に応じて、当該情報システム及びその整備又は運用管理を担当する課室を、それぞれ対象システム及び対象システム管理責任部署に加えた上で以降の実施プロセスの対象とする。

(3) リスク評価結果を踏まえた対策導入計画（案）の作成等

ア 対象システムごとの対策導入計画（案）の作成

対象システム管理責任部署は、リスク評価結果、対策の優先順位、予算措置の要否、システム更改時期等を踏まえ、対象システムに導入すべき対策及びその導入時期について検討を行い、付属書において設定されている統制目標を達成するための対策導入計画の案を作成し、リスク評価ワークシートに記入する。

なお、初年度に対策導入計画を策定済みの対象システムについては、次年度以降に当該計画の進捗状況等を踏まえた見直しを行う。

イ 対策導入計画（案）の調整

対象システム管理責任部署は、対象システムに係るリスク評価結果及び対策導入計画（案）、対策導入に伴うユーザ側への影響等がある場合は、その内容等について、当該システムのユーザ側である機微業務等実施部署に説明を行う。

機微業務等実施部署は、対策導入計画（案）について、業務遂行上求める情報セキュリティ水準、ユーザ側への影響等の観点から確認し、必要に応じて、対象システム管理責任部署と対策導入計画（案）の修正等に係る調整を実施する。

情報セキュリティ担当部署は、複数の対策導入計画（案）の間での調整の要否を確認し、必要に応じて、対象システム管理責任部署を始めとした関係部署との調整を実施した上で、CISO に承認を求めるための対策導入計画の案として確定させる。また、本プロセスにおいて資源配分関連の調整が必要であれば、資源配分部署とも調整を実施する。

(4) CISOによる方針決定等

ア　リスク評価ダッシュボードの作成

情報セキュリティ担当部署は、リスク評価ワークシートに基づき、リスク評価結果、対策導入計画（案）等の内容を取りまとめ、リスク評価ダッシュボードを作成する。

イ　CISOによる方針決定

情報セキュリティ担当部署は、作成したリスク評価ダッシュボードを用いて、CISOにリスク評価結果について報告するとともに、対策導入計画の承認を求める。

CISOは、残存リスク等を把握した上で、承認を求められた対策導入計画の実行方針を承認・決定し、又は再検討・修正を関係部署（資源配分担当部署を含む。）に指示する。

(5) NISCへの報告

ア　府省庁

府省庁の情報セキュリティ担当部署は、CISOが方針決定した対策導入計画等について、第３部の３に掲げるものをNISCに報告する。

イ　独立行政法人等

独立行政法人等の情報セキュリティ担当部署は、CISOが方針決定した対策導入計画等について所管府省庁に報告する。

府省庁は、所管する独立行政法人等の報告を取りまとめ、第３部の３に掲げるものをNISCに報告する。

ウ　公表

NISCは、政府機関等からの報告に基づき、本取組が適切に実施されているか確認を行い、政府機関等全体としての進捗状況等についてサイバーセキュリティ対策推進会議等に報告した上で、政府機関等を代表して公表する。

第３部　リスク評価ダッシュボード等

１　リスク評価ダッシュボードの位置付け

リスク評価ダッシュボードは、CISO にリスク評価結果等について報告するとともに、対策導入計画の承認を求める際に用いるため、対策導入計画に照らした進捗状況等を可視化した資料である。

CISO は、リスク評価ダッシュボードにより残存リスク等を把握し、対策導入計画の進捗状況及び次年度以降の計画内容について評価した上で、当該計画の承認の可否について判断する。

NISC は、政府機関等からの報告内容から、政府機関等全体としての対策実施状況や対策導入計画の進捗状況を評価するとともに、対策実施に係る技術的な課題や運用上の課題を把握・分析し、本取組の改善を図る。

２　リスク評価ダッシュボードの記載項目

リスク評価ダッシュボードへの記載項目は、保護対象とする業務領域、対象システム、リスク評価結果及び対策導入計画（案）の概要とする。また、リスク評価ダッシュボードに係る細部的事項については、本ガイドライン付属書に記載する。

３　NISC への報告

NISC への報告資料は、リスク評価ワークシート及びリスク評価ダッシュボード（CISO による方針決定の際に変更が生じた場合は、変更後のもの）とする。

なお、NISC への報告時期については、NISC からの事務連絡文書等を通じて別途連絡する。また、サイバーセキュリティ対策推進会議に加え、府省庁相互の緊密な連携を確保し、カウンターインテリジェンスの強化に向けた施策の総合的かつ効果的な推進を図る場であるカウンターインテリジェンス推進会議においても報告を行うため、当該内容については、内閣情報調査室と共有する。

第４部　本取組の運用管理

１　目的

高度サイバー攻撃は、時間の経過とともに新たな攻撃方法が出現したり、既存の攻撃方法に変化が生じたりすることが想定されることから、高度サイバー攻撃に対する効果的な防御を中長期的に実現していくためには、本取組の運用管理を適切に実施していく必要がある。中でも付属書に掲げる対策セットについては、技術動向や攻撃手法の進歩・変化に応じた継続的な見直しを行うことが特に重要であることから、そのための体制構築その他の必要な事項について、以下に示す。

２　本ガイドライン等の改定

(1)　本ガイドラインの改定

本取組の実施プロセス等に係る見直しの必要が生じた場合には、NISCにおいて内閣情報調査室と連携して検討を行った上で、サイバーセキュリティ対策推進会議において本ガイドラインの改定について決定を行う。

(2)　付属書の改定

対策セットを含む付属書の記載事項に係る見直しの必要が生じた場合には、府省庁の意見を踏まえた上でNISCにおいて改定を行う。

なお、付属書の改定のうち、対策セットの運用管理に係る事項については、３にその詳細を示す。

３　対策セットの運用管理

(1)　対策セットに係る評価検討体制等の構築

新たな攻撃方法の出現や既存の攻撃方法の変化に対応するため、NISCにおいて、政府機関等との情報共有を行い、これらの攻撃を監視・把握するとともに、高度サイバー攻撃対処に係る評価・検討等に関する以下の役割を担うための体制（以下「評価検討委員会」という。）を構築する。また、評価検討委員会は、高度サイバー攻撃に関する学識者委員を中心に構成する。

①　政府機関等が喫緊の課題として対処すべき新たな高度サイバー攻撃手法及び新たな対策に関する情報収集
②　新たな対策の有効性に係る技術的・運用上の見地からの評価
③　既存の対策の見直しに係る検討

(2) 対策セットの見直し

政府機関等が喫緊の課題として対処すべき新たな高度サイバー攻撃手法が把握された場合その他対策セットに係る見直しが必要であると判断された場合には、対策セットの見直しについて検討を行う。

対策セットには、高度サイバー攻撃のシナリオに対応する情報システムの設計、監視強化等に係る対策のうち、評価検討委員会において評価を行い、技術的・運用上の見地から有効であることが確認された新たな対策について、府省庁と協議の上、取り入れる。