NIST SP800-30 をベースにした簡易リスクアセスメントの検討と実施について

戸田 庸介 [1)], 片桐 統 [1)], 山口 倉平 [1)], 石橋 由子 [1)]

1）京都大学 情報部

i-s-office@iimc.kyoto-u.ac.jp

Consideration and Implementation of a Simplified Risk Assessment Based on NIST SP800-30

Yosuke Toda [1)], Osamu Katagiri [1)], Souhei Yamaguchi [1)], Yoshiko Ishibashi [1)]

1) Information Management Department, Kyoto University.

概要

内部統制や情報セキュリティ対策においては、限りある資源の中で情報資産を適切に保護するという観点からリスクベースアプローチが推奨されている。リスクアセスメントのフレームワークとして代表的なものは NIST SP800-30 であるが、約 100 ページある詳細なフレームワークを何もないところから始めることは困難である。NIST SP800-30 の要点となる事項をまとめて、簡便にリスクアセスメントを行うことを検討し、実際にワークショップ開催して簡易リスクアセスメント表に取りまとめた活動について報告する。

1 はじめに

情報ネットワークは、電気・ガス・水道に次ぐ「第 4 のインフラ」と言われている。2022 年の 2 月末に国内大手自動車メーカーが、子会社へのサイバー攻撃が原因で国内の製造ラインを停止するという事案が発生したことは記憶に新しい。高度化するサイバー攻撃は事業継続に大きく影響を与える経営課題となっており、サプライチェーンリスクも含めたリスクアセスメントが益々重要となっている。

文部科学省から令和 4 年 6 月 22 日に「大学等におけるサイバーセキュリティ対策等の継続的な取り組みについて（通知）」（４文科高第 367 号）が発出された。サイバーセキュリティ対策にかかる実施すべき事項の大項目には、リスク管理体制の構築、リスクの特定、リスク対策、サプライチェーンリスクへの対応という順番で記載されており、リスクベースアプローチが顕著な内容であった。

また、2021 年 10 月に開催された文部科学省令和 3 年度 CISO マネジメント研修に参加し、独立行政法人情報処理推進機構(IPA)から提供されているサイバーセキュリティ経営チェック可視化ツールを実施した。その診断結果からリスクアセスメントやサプライチェーンリスクへの対応に本学の課題があることが明白となった。

本稿では、国立情報学研究所が公開している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（2019 年度増補版 2）[1](以下サンプル規程集という)でのリスクアセスメントについて確認し、その中で例示されている NIST SP800-30 をベースとしてより簡便にしたテンプレートを作成し、リスクアセスメントについてスモールスタートした取り組みについて述べる。

2 サンプル規程集におけるリスクアセスメント

2.1 サンプル規程集「C3104 情報システム運用リスク評価手順」

サンプル規程集のポリシー・実施規程・手順等の体系を参照すると「リスク」というキーワードでは「C3104 情報システム運用リスク評価手順」が目に留まる。

この評価手順は、情報資産の洗い出し、脆弱性分析の後、機密性、完全性、可用性の観点で資産

価値判断や脅威の判断、リスク値の算出を行うものである。

資産管理台帳が整備された環境であれば、問題はないが、多くの部局や研究室からなる大規模な大学では、各部局に情報セキュリティ委員会を設置し、それぞれで資産管理台帳を管理する運用となっている。この評価手順から全学のリスクアセスメントを行うには、部局でリスクアセスメントを実施したものを全学で集約して、リスクの高いものを全学として把握することが想定される。しかしながら、全学組織側で実施できていないリスクアセスメントを部局側で先行して実施することは部局の理解を得ることが難しいと考えた。

2.2 サンプル規程集「D1001 情報セキュリティ対策基本規程」の D1001-21 （対策基準の策定）の解説

D1001 情報セキュリティ対策基本規程の D1001-21 （対策基準の策定）には、「対策基準は、本学の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めること。」と記載があり、この部分についての解説でリスクアセスメントについて詳細に記載されている。

「リスク評価手法については、情報セキュリティに係るマネジメント能力の成熟度や機関等の置かれた環境に応じたふさわしい手法を選ぶとよい」と記載され、国内標準である「JIS Q 31000:2010 リスクマネジメント－原則及び指針」が示されている。

また、リスク基準例、脅威事象が発生する可能性、脅威事象が負の影響をもたらす可能性については、「National Institute of Standards and Technology（米国国立標準技術研究所）Special Publication 800-30 revision1」(以下、NIST SP800-30 と記載する)から基準例が示されている。

C3104 がボトムアップ的リスクアセスメントであることに対して、D1001-21 の解説ではトップダウン的アセスメントであり、本学の状況から後者のアプローチの方がスモールスタートするには適していると考えた。

3 NIST SP800-30 の調査と簡便化の検討

3.1 NIST SP800-30 の概要

NIST SP800-30 は情報処理推進機構により翻訳され、「リスクアセスメントの実施の手引き」として公開されている。[2]

NIST SP800-30 は 3 章の本体と 12 章の付録で構成されている。第 2 章基本項目には、リスクマネジメントプロセス、およびそのプロセスにおいてリスクアセスメントがいかに重要であるか、リスクアセスメントを組織のリスクマネジメントのすべての層（組織レベル、業務プロセスレベル、情報システムレベル）にわたってどのように適用できるかについて説明されている。

第 3 章プロセスには、リスクアセスメントプロセスの簡単な概要、リスクアセスメントの準備に必要な活動、リスクアセスメントの実施に必要な活動、組織全体にわたってリスクアセスメント結果を伝達し、リスク関連情報を共有するために必要な活動、ならびにリスクアセスメント結果の保守に必要な活動について説明されている。

付録は、参考文献、用語集、略語、脅威源、脅威事象、脆弱性および素因条件、脅威事象が発生する可能性、組織的影響、リスクの判断、情報リスクへの対応、リスクアセスメント報告に含めるべき必須情報、リスクアセスメントの各タスクの概要から構成されている。

3.2 NIST SP800-30 に基づいたリスクアセスメントの試行と簡便化の検討

実際のリスクアセスメントのプロセスは第 3 章と豊富な付録を参照して進めることになる。NIST SP800-30 に基づいて表 1 のように Excel でステップごとに対応したシートで作業を進めることとした。

ステップ 1：リスクアセスメントの準備は 5 つのタスクで構成され、目的、適用範囲、想定と制限を特定、情報源の特定、リスクモデルと分析的アプローチの特定となっている。目的と適用範囲を明示することは大切である。

表 1　標準的な格付け基準（抜粋）

ステップ 1：リスクアセスメントの準備			
タスク 1-1	目的を特定する	アセスメントが生成する情報と、アセスメントが支援する意思決定の観点から、リスクアセスメントの目的を特定する。	リスクアセスメントの準備
タスク 1-2	適用範囲を特定する	組織の適用範囲、サポートされている時間枠、および構造上／技術上の考慮事項の観点から、リスクアセスメントの適用範囲を特定する。	リスクアセスメントの準備
タスク 1-3	想定と制限を特定する	リスクアセスメントが具体的にどのような想定と制限のもとで実施されるかを特定する。	リスクアセスメントの準備
タスク 1-4	情報源を特定する	リスクアセスメントにおいて使用される記述的情報、脅威関連情報、脆弱性関連情報、および影響関連情報の情報源を特定する。	リスクアセスメントの準備
タスク 1-5	リスクモデルと分析的アプローチを特定する	リスクアセスメントにおいて使用されるリスクモデルと分析的アプローチを特定する。	リスクアセスメントの準備
ステップ 2：リスクアセスメントの実施			
タスク 2-1	脅威源を特定する	懸念される脅威源を特定し、特徴を定義する。	セクション3.2 D
	表D-1 入力データ-脅威源の特定		翻訳版参照
	表D-2 脅威源の分類体系		翻訳版参照
	表D-3 アセスメントスケール アドバーサリの能力の特徴定義		翻訳版参照
	表D-4 アセスメントスケール アドバーサリの意図の特徴定義		翻訳版参照
	表D-5 アセスメントスケール アドバーサリの標的の特徴定義		翻訳版参照
	表D-6 アセスメントスケール アドバーサリによるもの以外の脅威源がもたらす影響の範囲		翻訳版参照
	表D-7 アドバーサリーによる脅威源の特定		表I-5
	表D-8 アドバーサリーによるもの以外の脅威源の特定		表I-7

タスク 2-2 では付録 E を参照し、脅威事象を特定することとなる。特に「表 E-2：代表的な例 - アドバーサリによる脅威事象」は APT 攻撃（高度標的型攻撃）を想定して例が示されているが、スモールスタートするには詳しすぎると感じた。

タスク 2-3 では付録 F を参照し、脆弱性と素因的条件を特定することとなる。素因的条件についてはどこにリスクがあるのかを追求する上で大切なプロセスであるが、1 つの脅威に対して複数の素因的条件を並べた場合、評価する項目が増えて複雑化するため、脅威事象レベルでの整理に留める方が簡便であると考えた。また、3.1 に記載したリスクマネジメントの 3 層構造についても成熟したアセスメントを行うには重要な考え方であるが、複雑化する要素であるため必要なときにだけ考慮することとした。

タスク 2-4 では付録 G を参照し、可能性を特定し、タスク 2-5 では付録 H を参照し、影響を特定することとなる。定常的な値や半定量的な値で例が示されているが、半定量的な値であれば掛け算ができるため簡便であると考えた。

タスク 2-6 では付録 I を参照してリスクを判断することとなる。アドバーサリ（敵対するもの）以外の場合は、脅威事象が発生する可能性と重大さと広がりで負の影響をもたらす可能性を一旦検討するプロセスとなっているが、直接的に評価した発生可能性とリスクの影響の 2 つの評価軸で簡便に整理した。

ステップ 3、ステップ 4 は伝達と保守のフェーズであるため、ここでは割愛する。

ここまで NIST SP800-30 に基づいてリスクアセスメントの試行を行ってきたが、スモールスタートするためには、前述の点でより簡便な方法を採用してリスクアセスメントを実施する方針とした。

4 簡易リスクアセスメントの実施

4.1 簡易リスクアセスメントのテンプレート作成

試行に使用した Excel ファイル（表 1）から最低限必要と考える要素だけを残したものをテンプレートとして使用することとした。

テンプレートは 2 つのシート構成とし、1 つ目のシートでは基本項目として、目的、範囲、手順について概要を記載し、攻撃の可能性、発生の可能性と影響のレベルの尺度について明記することとした。

2 つ目のシートでは NIST SP800-30 の特徴に倣って、アドバーサリ（敵対するもの）かそれ以外かで大別した 2 つの表を作成することとし、付録 D の脅威源の分類体系を参考にしたカテゴリ、なるべく最悪のシナリオを想定した脅威事象、素因的条件や現状の対策状況を記載する備考、事象が発生する可能性と影響のレベルをそれぞれ半定量的な値で 1～5 の 5 段階で評価し、掛け算した値を最終的なリスク値とし、数値が大きくリスクが高いものを赤、数値が小さくリスクが低いものを緑となるよう Excel のカラースケール機能で色分けした。(表 2)

表２ 簡易リスクアセスメントのテンプレート

アドバーサリ(敵)によるリスク

カテゴリ	脅威事象(なるべく最悪のシナリオ)	備考（素因的条件、対策など）	攻撃の可能性	影響のレベル	リスク
組織（APT攻撃グループ）	フィッシングからRATにより遠隔操作されて、情報が窃取される。	シグネチャ型対策ソフトの限界	5	5	25
国（サイバー軍）	スパイを送り込まれ、発行したアカウントを利用して原子力分野などの先端的技術情報を窃取される	アカウント発行時の本人確認、臨時利用者	3	5	15
個人（内部）	論文の剽窃等の研究不正で、大学がペナルティを受ける	内部不正対策	5	5	25
個人（内部）	全学アカウントの同時利用ができるため、アカウントを販売し電子ジャーナル不正共有される	同時ログイン対策	5	3	15
個人（外部）	ランサムウェアにより資産が暗号化され、情報暴露すると身代金を要求される	シグネチャ型対策ソフトの限界	5	5	25
個人（外部）	学外スパムメールの踏み台とされる	アカウント漏洩、脆弱性悪用	5	4	20
個人（外部）	ゼロデイ攻撃により脆弱性を悪用される	シグネチャ型対策ソフトの限界	5	4	20
個人（外部）	フィッシング詐取によりID、PWを窃取され、不正ログインされる、特殊詐取	URLフィルタ未整備	5	3	15
個人（外部）	スマートフォンをターゲットにスパイウェアアプリを配布する	BYODへの対策	5	3	15
個人（外部）	VPNを悪用される	リモートワークの拡大	3	3	9
個人（外部）	オンライン講義、会議へのアクセス情報が漏えいし、情報が漏えいする	リモートワークの拡大	4	2	8
個人（外部）	ソーシャルエンジニアリングによるアカウント情報の窃取が窃取される。	振り込め詐欺関係	2	3	6
個人（外部）	部局独自設置WiFiアクセスポイントから不正侵入される	独自設置WiFi対策	3	2	6
個人（外部）	ポートスキャン、OSINTによりシステム探索される	デフォルトポートの変更	5	1	5
個人（外部）	DDoS攻撃によりサービス提供ができなくなる	SINET側の対策により可能性を1に設定	1	3	3
組織（供給業者）	システム管理権限を持った業者による意図的なデータ漏洩、削除(怨恨、買収)		1	5	5
組織（ライバル）	大学運営に不満を持つ組織からの妨害		1	1	1

アドバーサリによるもの以外のリスク

カテゴリ	脅威事象(なるべく最悪のシナリオ)	備考（素因的条件、対策など）	事象が発生	影響のレベ	リスク

4.2 リスクアセスメントワークショップ

NIST SP800-30 の調査から簡易リスクアセスメントテンプレートまで作成し、その過程の中でもリスクアセスメントを実施してきたが、リストアップできていない脅威事象がないか確認するために、本学情報部情報基盤課の勉強会の中でリスクアセスメントを行うワークショップを 2022 年 4 月 27 日に開催した。参加者は 13 名で施設系の技術職員も 1 名参加した。

4 つのグループに分かれてブレインストーミングを行う方式として、本学における重要なもの、本学にとっての脅威のテーマで実施した。グループから発表される内容をマインドマップに取りまとめた。(図 1)

ワークショップで得られた結果から簡易リスクアセスメントの脅威内容について更新を行った後、本学情報基盤部門を中心に月に 1 回行っている勉強会の中で、簡易リスクアセスメントの発生可能性と影響の数値について参加者 8 名でディスカッションを行い、数値の見直しを行った。

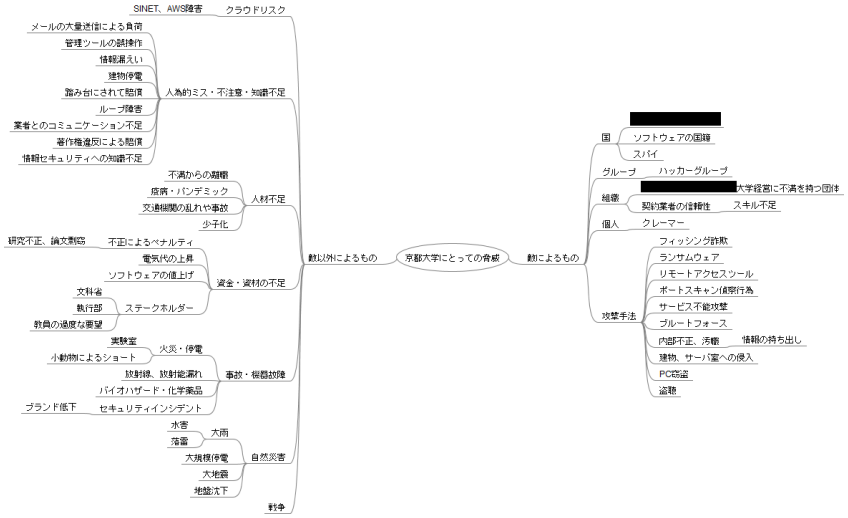

図１　本学における脅威

5　おわりに

本稿ではリスクアセスメントの手法について調査し、簡易的に実施する方法について述べてきた。このような経緯を経て作成したリスクアセスメント表については、令和 4 年度全学情報セキュリティ委員会常置委員会に報告し、課題の共通認識を持つことが出来た。今年度は 2022 年度から 2024 年度までの第 3 期の本学のサイバーセキュリティ対策等基本計画を策定する年度であり、簡易リスクアセスメントを実施した上で計画を立てるということは重要なプロセスであったと考える。

情報セキュリティ監査、リスクアセスメントといった組織的に整備すべき課題については、経営層には情報技術分野の知識が不足から推進することが困難な場合がある。一方で現場の IT 技術者は法律、規程、規則などは敬遠しがちな分野であり、リスクアセスメントについても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や NIST SP800-30 を読み込んで完全に準拠したアセスメント表を何もないところから整備しようとすることは非常にハードルが高く、途中で断念することが懸念される。情報セキュリティの分野であってもスモールスタートや段階的な目標設定は非常に重要なことであり、途中で挫折してしまうよりは出来る範囲で努力して結果を出していくことが重要と考える。

サイバー攻撃は年々高度化し、リモートワークの拡大などで情報環境の変化に情報セキュリティ対策が追いつかない状況にある。大学の情報セキュリティ対策においてリスクの洗い出しと、対策の優先順位付けを行い、CISO が適切な判断ができるようにこれからも更なる改善に取り組む所存である。

参考文献

[1] 国立情報学研究所、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（2019 年度増補版 2）

[2] 米国国立標準技術研究所（NIST）、SP 800-30 rev.1（翻訳：情報処理推進機構、リスクアセスメントの実施の手引