資料 8－5

重要インフラにおける機能保証の考え方に基づく
リスクアセスメント手引書
（第１版）

平 成 ３ ０ 年 ４ 月 ４ 日

〇 〇 〇 年 〇 月 〇 日 改 定

サイバーセキュリティ戦略本部

重要インフラ専門調査会

（空白ページ）

目次

＜４＞手引書の構成

本手引書は、次に掲げるドキュメントにより構成されます。

図表２　本手引書のドキュメント構成

ドキュメント名称		概要
重要インフラにおける機能保証の考え方に基づく リスクアセスメント手引書		本文書
別紙１	業務の阻害につながる事象の結果の例	業務の維持のために経営資源に求められる観点を踏まえた「業務の阻害につながる事象の結果」（優先サービス障害）を例示した参考資料
別紙２	結果を生じ得る事象（脅威）の例	結果を生じ得る事象について、基本的な分類と併せて主な例示を掲載した参考資料
別紙３ （様式集） （※）	（様式１）リスクアセスメントの実施目的の確認	組織の活動目標の設定及びリスクアセスメントの実施目的・方針の確認のためのワークシート（記載例を含む。）
	（様式２）優先サービスの選定	利害関係者からの期待、社会的責任（ＣＳＲ）、法制面の要求（コンプライアンス）等を分析し、優先サービス（リスク評価の対象とするサービス）を選定するためのワークシート（記載例を含む。）
	（様式３）優先サービスの影響度分析	優先サービスの影響分析として、安全（＝許容できないリスクが無い状態）の観点を踏まえ最低限許容されるサービスの範囲・水準及びサービス提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を決定するためのワークシート（記載例を含む。）
	（様式４）優先サービスを支える業務の特定及び当該業務の影響度分析	優先サービスの提供のために必要な業務を洗い出し、その業務について最低限維持すべき状態を明らかにした上、その業務が停止した場合の影響及び最大許容停止時間を推定するためのワークシート（記載例を含む。）
	（様式５）業務を支える経営資源の特定	優先サービスの提供に必要な業務について、最低限維持すべき状態を維持するために必要な経営資源を明らかにするためのワークシート（記載例を含む。）
	（様式６）経営資源に係るリスクアセスメント	優先サービスの提供に必要な業務に係る経営資源を整理した上、その業務継続に対するリスクの特定、分析及び評価を行うためのワークシート（記載例を含む。）
別紙４	リスク源の例	リスク源について、基本的な分類と併せて主な例示を掲載した参考資料

（※）本手引書において、様式１から様式６までの様式を総称して「リスクアセスメントシート」といいます。

２．リスクアセスメントの全体像

＜１＞機能保証の考え方に基づくリスクアセスメントの観点・考え方

リスクアセスメントの手法には、既に確立されており、多くの運用実績を有するものが多数存在しますが、その手法の採用や実施手順において唯一の正解というものはありません。このため、事業者等がリスクアセスメントを実践する際には、どの手法を採用すれば、自組織にとって、より効果的・効率的にリスクの特定・分析・評価を行うことができるかを十分に検討した上、自らの判断でこれを決定することが必要です。この検討・決定に際しては、その提供するサービスが社会経済システムにおいて不可欠な役割・機能を担う重要インフラ事業者等においては、「機能保証」の考え方を踏まえることが重要となります。

機能保証の考え方（「重要インフラの情報セキュリティ対策に係る第４次行動計画」からの抜粋）

重要インフラサービスは、それ自体が国民生活及び社会経済活動を支える基盤となっており、その提供に支障が生じると国民の安全・安心に直接的かつ深刻な負の影響が生じる可能性がある。このため、各関係主体は、重要インフラサービスを安全かつ持続的に提供するための取組（機能保証）が求められる。

なお、本行動計画において、「機能保証」とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。すなわち、各関係主体が重要インフラ防護の目的を果たすために、情報セキュリティ対策に関する必要な努力を適切に払うことを求める考え方である。

本手引書では、前述のとおり、重要インフラ事業者等により利活用されることを想定していることから、機能保証の考え方に基づくリスクアセスメントとして、「各重要インフラ事業者等が社会経済システムの中で果たすべき役割・機能を見極め、これを発揮するために、許容できないリスクが無い状態（＝安全）を確保しつつ、サービス提供を継続する」という観点から、情報セキュリティリスクの特定・分析・評価を実践するための手順を紹介します。

重要インフラ事業者等にあっては、リスクアセスメントを主体的かつ自律的に取り組むことが必要です。ただし、その取組の精度や水準については、各重要インフラ事業者等の力量に依存することから、本手引書では、機能保証の考え方に基づくリスクアセスメントの観点や参考になる作業手順を示すことにより、各重要インフラ事業者等における取組について一定以上の精度や水準が確保されることを狙いとしています。

なお、本手引書で紹介するリスクアセスメントの手順は、重要インフラ事業者等に限らず、中堅・中小企業を含む様々な分野の事業者等においても準用することができます。

＜２＞機能保証の考え方に基づくリスクアセスメントの方針

本手引書では、「２．＜１＞機能保証の考え方に基づくリスクアセスメントの観点・考え方」に記載したとおり、「重要インフラ事業者等が、機能保証の考え方に立脚し、リスクを戦略的に最適化するために、リスクの特定、分析及び評価を行い、並びにリスク対応の選択肢の同定を行うとと

もに、残留リスクを可視化すること」を志向します。このことを踏まえ、本手引書で紹介するリスクアセスメントの手法は、次に掲げる方針に従うものとします。

① リスクの捉え方

「社会経済システムの中で果たすべき役割・機能を発揮するために必要なサービスの提供を維持・継続すること」を重要インフラ事業者等における経営戦略上の目的とし、「目的に対する不確かさの影響」をリスクと捉えます（ISO 31000:2009 における定義に準拠。）。ただし、機能保証の考え方を踏まえ、本手引書で対象とするリスクは、「負の影響：好ましくない結果をもたらすリスク」に限定します。

② 機能保証の考え方に基づく演繹的なリスクアセスメント

発生確率の低い事象から目を背けた（発生した場合には危機的状況につながる可能性がある事象であっても、過去に経験していない、又は発生確率が低いためにリスクとして想定しなかった）ことにより、その事象の結果が想定外となって大きな混乱を招くこととなった東日本大震災での教訓を踏まえ、上記①によるリスクの捉え方を前提として、機能保証の考え方に基づき、「重要インフラ事業者等が社会経済システムの中で果たすべき役割・機能を発揮するために維持・継続することが必要なサービスを特定し、許容できないリスクが無い状態（＝安全）を確保しつつ、そのサービス提供を継続するために必要な業務や経営資源に係る要件を分析・評価」した上、これらに影響する「事象の結果からリスク源までを演繹的に特定・分析・評価」するアプローチとします。

③ 効率的な作業への配慮（帰納的なアプローチとの組合せ）

演繹的な詳細リスク分析のアプローチを採用しますが、多くの重要インフラ事業者等により実施されているイベントツリー分析等の帰納的なアプローチによって、想定される脅威（事象）及び脆弱性（リスク源）の組合せを書き出していくやり方も、重要インフラ事業者等が想定するリスクについての分析には一定の効果があることから、こうした実績のある帰納的な手法を組み合わせることにより、効率的な作業を行うことができるように配慮します。具体的には、重要インフラ事業者等における作業負荷や、作業者の知識・経験が浅い場合などに結果を生じる事象やリスク源を見逃してしまう可能性があることについても考慮し、リスク分析における気付きとなるような「業務の阻害につながる事象の結果の例」（別紙１）、「結果を生じ得る事象（脅威）の例」（別紙２）及び「リスク源の例」（別紙４）を提供することにより、作業の効率化や網羅性の確保に資するように配慮します。

別紙２　結果を生じ得る事象(脅威)の例　（案）

結果を生じ得る事象(脅威)			具体例
攻撃に起因する脅威	外部不正	標的型攻撃	アクセス権限のないポート、プロトコル、およびサービスを使用して、攻撃を実施する。
			ネットワーク境界を越えて許可されているトラフィック／データの移動を利用して、攻撃を実施する。
			重要な地位にいる職員の私有のデバイスを狙って侵害する攻撃を実施する。
			基幹業務に関わるハードウェア、ソフトウェア、ファームウェアを狙い、サプライチェーン攻撃を実施する。
		マルウェア	メールの添付ファイルからマルウェアを感染させる。
			ウェブサイトからマルウェアを感染させる。
			エクスプロイトキットを使って、ランサムウェアを拡散させる。
		情報窃取	SQLインジェクション等の情報漏えいにつながる脆弱性を悪用し、機微な情報を取得する。
			OSコマンドインジェクション等のソフトウェアの脆弱性を悪用し、機微な情報を取得する。
			外部ネットワークのネットワークスニッフィングを介して、機微な情報を取得する。
		サービス妨害攻撃	シンプルなサービス妨害(DoS)攻撃を実施する。
			分散型サービス妨害攻撃を実施する。
			標的型サービス妨害攻撃を実施する。
		ウェブサイト改ざん	開発時に作りこんだウェブアプリケーションの脆弱性を悪用して、サイトを改ざんする。
			ソフトウェアの脆弱性を悪用して、サイトを改ざんする。
			管理用サービスに侵入して、サイトを改ざんする。
		ウェブサービスへの不正ログイン	他のウェブサイトから漏えいしたIDとパスワードの組み合わせを利用して攻撃する。
			総当たりのログイン試行／パスワード推測攻撃を実施する。
		脆弱性を標的にした攻撃	公開された脆弱性情報を悪用して、対策をしていない利用者を攻撃する。
			パッチなどの修正手段が提供されていない脆弱性を狙って、非標的型ゼロデイ攻撃を実施する。
			IoT機器の脆弱性を悪用してウイルスを感染させる。
		金融情報の不正利用	インターネットバンキング詐欺ツールによって金融取引関連情報を窃取する。
			フィッシング詐欺をする。
		通信の盗聴・妨害	通信傍受攻撃を実施する。
			無線妨害攻撃を実施する。
			外部に設置された傍受用デバイスを使用して、無線ネットワークトラフィックを傍受する。
		データの改ざん	極めて重要なデータを汚染する、あるいは改ざんする。
			公的にアクセス可能な情報システム上にデータを作成・削除・変更する。
			もっともらしいが偽のデータを組織の情報システムに挿入する。
		ソーシャルエンジニアリング	不在時に他人の机の上にある資料やノートをのぞき見して、機密情報などを収集する。
			ゴミ箱をあさり、不用意に廃棄された資料やメモなどを収集し、目的の情報を取得する。
			機会をうかがって情報システム／コンポーネントを盗んだり、あさる。
		システム破壊	システムを破壊するマルウェアを不正にインストールする。
	内部不正	不正利用	データを不正に操作する。
			機密情報を不正に閲覧する。
			機微な情報を不正に取得する。
		不正持ち出し	機密情報を不正に持ち出す。
			データを意図的に外部に送信する。
		乗っ取り	内部の攻撃者が正規ユーザになりすましてウェブアプリケーションを操作し、セッションの乗っ取りを実施する。
			内部の攻撃者がネットワークトラフィックに侵入して、変更攻撃を実施する。
攻撃に起因しない脅威	自然現象	自然災害	地震が発生する。
			台風が発生する。
			温度・湿度異常が発生する。
			落雷が発生する。
			浸水が発生する。
		エネルギー不足	停電が発生する。
			水不足が発生する。
	障害	設備障害	火災が発生する。
			漏水が発生する。
			動植物害が発生する。
			施設が老朽化する。
			ビル付帯設備(空調機器、入退室管理装置、監視カメラ等)が故障する。
		ハードウェア障害	メモリ、ディスク、CPU、電源装置の障害が発生する。
			ディスクのエラーが発生する。
			機器・ケーブルが劣化する。
		ソフトウェア障害	OSやアプリケーションの潜在的なバグ・過負荷等による異常が発生する。
			資源(メモリやディスクの容量オーバー等)の枯渇により、処理性能が低下する。
		ネットワーク障害	通信の競合により、通信性能が低下する。
			回線(専用・公衆)、通信事業者(接続局、ISP、NOC、IDC等)、通信機器、構内配線の障害が発生する。
	人に起因する脅威	操作ミス	特権ユーザが、極めて重要な情報／機微な情報を誤って露出させる。
			特権ユーザが、他のユーザに例外的な権限を誤って付与する。
			メールを誤送信する／不要なメールを開封する／重要データを消去する。
		遺失・紛失	持ち出し媒体を置き忘れる／管理不備によって媒体を紛失する。
		不適切な廃棄	廃棄した媒体を復元する。
		無許可機器の持込	許可されていない機器、媒体、プログラムを社内ネットワークに接続する。
		無意図な情報公開	ウェブサーバの設定不備により重要データが流出する。
		任務怠慢	既定の操作の実行を忘れる。
		法令・政策の不認識	海外サーバにおいてデータ保管・処理等を行う場合において、認識していない当該地域の法令等による権限が行使される。

別紙4 リスク源の例 （案）

分類		リスク源の例	該当する「結果を生じ得る事象(脅威)」の例
ハード	システム	システムのバグ放置 機器のリプレース未実施 メンテナンス不足 冗長化の不採用	ハードウェア障害、ソフトウェア障害、ネットワーク障害
		データバックアップの不備 非常用エネルギー設備の未設置	ハードウェア障害、ソフトウェア障害、ネットワーク障害、エネルギー不足、自然災害
		耐震化・耐水化の不備 バックアップサイトの未設置 設備のリプレース未実施	自然災害、設備障害
	セキュリティ	DoS対策の不備 (装置／設定)	サービス妨害攻撃
		防犯カメラの未設置	ソーシャルエンジニアリング
		保護されていない通信経路	通信の盗聴・妨害
ソフト	脆弱性対策	修正プログラムの未適用 既知の脆弱性の放置 サポート終了したソフトウェアの継続使用	情報窃取、ウェブサイト改ざん、脆弱性を標的にした攻撃
	接続環境	USB、外部媒体が接続できる環境有	マルウェア、不正利用、不正持ち出し
		誰でもアクセスできる環境有 外部ネットワークへの接続環境有 インターネットへの接続環境有 周辺システムとの連携有 誤操作・意図的な操作ができる環境有 外部からの不正情報を受信できる環境有	標的型攻撃、マルウェア、情報窃取、サービス妨害攻撃、ウェブサイト改ざん、 ウェブサービスへの不正ログイン、データの改ざん、システム破壊、 不正利用、不正持ち出し、乗っ取り
		海外サーバにおけるデータ保管・処理有	法令・政策の不認識
	ルール	不要な人へのアクセス権限の付与 不要アカウントの放置 作業できるオペレーターのID管理不備 パスワード変更の放置	標的型攻撃、情報窃取、ウェブサイト改ざん、ウェブサービスへの不正ログイン、 不正利用、不正持ち出し、乗っ取り
		ネットワーク通信の暗号化不徹底	通信の盗聴・妨害
		廃棄承認ルールの未整備・不徹底	不適切な廃棄
		入退室管理の不備	不正利用、不正持ち出し、ソーシャルエンジニアリング
		機器や情報の不適切な保管 外部業者の本人確認の未徹底 施錠未実施	ソーシャルエンジニアリング
スキル・人材	組織共通	長時間労働	操作ミス、任務怠慢
		社内セキュリティ教育が不十分 セキュリティ意識の欠如	不正利用、不正持ち出し、操作ミス、遺失・紛失、無許可機器の持込、任務怠慢
		安易なパスワード設定 パスワードの使いまわし	ウェブサービスへの不正ログイン、金融情報の不正利用
		機密・重要書類の放置 不在時のPCログイン未設定	ソーシャルエンジニアリング
		不正アプリケーションのインストール 更新・保守作業時にウィルスチェックをしていない	マルウェア、情報窃取、ウェブサイト改ざん、脆弱性を標的にした攻撃
	セキュリティ部門	メンテナンス時の確認漏れ	マルウェア、システム破壊
		情報セキュリティ要員のスキル不足 セキュリティ要件を満たさないコーディング	脆弱性を標的にした攻撃、ウェブサイト改ざん、操作ミス、無意図な情報公開
		情報セキュリティ要員の要員不足 不十分なセキュリティ訓練	標的型攻撃、マルウェア、サービス妨害攻撃、脆弱性を標的にした攻撃