住友電工
Connect with Innovation

AI品質マネジメントイニシアティブ各WG共通

セキュリティリスクアセスメント手順

住友電気工業株式会社
DX技術研究開発センター サイバーセキュリティ研究開発部 セキュリティ基盤グループ
三宅　和公（miyake-kazumasa@sei.co.jp）

SUMITOMO
ELECTRIC
GROUP

目次

1.はじめに

AIQMI WG2からの発案として、AI品質保証のために必要となる要素技術を集積することとなり、本書ではセキュリティリスクアセスメントについて説明する。
AIセキュリティのリスクアセスメントや世界的な技術トレンドや国際標準化動向などについてはNEDO特別講座で解説するのでそちらを参照されたい。

2.セキュリティリスクアセスメントの基礎概念

脆弱性：対象システムに存在するセキュリティ上の弱み
脅威：攻撃者が対象システムの弱みを攻撃すること

対象システムにおいて、どのようなセキュリティ上の　問題点(脅威と脆弱性)があり、どのような対策(管理策)を打つかを導出する。
「対象システムに存在する脆弱性を攻撃者による脅威が襲う」と考える。

ステークホルダ：対象システムに関わる人や組織（攻撃者や被害者になる。）
アセット：攻撃を受ける対象
アタックサーフェイス（攻撃界面）：アセットの攻撃される個所

【セキュリティリスクアセスメント】
ステークホルダたちが関係するアセットについて脅威と脆弱性を出し、脅威と脆弱性に対して対策(管理策と呼ぶ)を出し、管理策を実施する。

2.セキュリティリスクアセスメントの基礎概念

2.1セキュリティリスクアセスメントの実施の仕方

2.1.1 基本事項

●国際標準が示す枠組みに従う。
　国際標準の意義：アセスメントの出来合いを一律の物差しで測る。

【国際標準の主な類型】

・リスクベースアプローチ：対象システムに即してリスクを分析・対策。
　長所：対象システムの仕様や課題に応じたきめ細かな分析と対策立案
　短所：実施が大変(きめ細かく分析してひとつひとつ対策するから)

・ベースラインアプローチ：適当なシステムを想定してリスクへの管理策一覧を提供。
　長所：取り組みやすい。沢山のシステムを同じ基準で検証した結果が得られる。
　短所：想定システムとの差異が大きいと漏れだらけになる。
　　なぜその仕様や検証項目を入れなければならないかを書いていない。

★本書ではISO/IEC 27005に従うリスクベースアプローチを紹介する。

2.セキュリティリスクアセスメントの基礎概念

2.1セキュリティリスクアセスメントはどのように行うか？

2.1.1 基本事項～進め方を説明するに当たって・・・(続き)

【参考情報】

IPA「中小企業の情報セキュリティ対策ガイドライン」

初心者・初学者でも取り組める分析シートつき

2.セキュリティリスクアセスメントの基礎概念

2.1セキュリティリスクアセスメントは、いつ、どのように行うか？

2.1.2 進め方

【概要】

(1) ステークホルダ・アセットの洗い出し
(2) 事例集め
(3) 脅威と脆弱性のリスト作成
(4) 脅威と脆弱性に優先度付け
(5) 脅威と脆弱性に対する管理策立案
(6) 管理策適用スケジュール・PDCA案策定

2.セキュリティリスクアセスメントの基礎概念

2.1セキュリティリスクアセスメントは、いつ、どのように行うか？

2.1.2 進め方

(1) アセット・ステークホルダ洗い出し

①ビジネス：どのようなサービスを誰が誰にどう提供するか。大括りに必要そうな機能も可能な限り予測。

②ビジネスに沿ってスコープ（システム構成図を描き分析する対象範囲）を決め

ステークホルダ：スコープ内に登場する関係者

アセット：情報資産～売上計画・設計記録・人事関連文書など重要な情報。

を洗い出す。データの流れを矢印で描いておくとよい。

(2) 事例集め

後述する情報源を使い、ビジネスに関係しそうなセキュリティ事件の情報を可能な限り多く収集する。事件の流れを描いた絵があるとなおよい。

2.セキュリティリスクアセスメントの基礎概念

2.1セキュリティリスクアセスメントは、いつ、どのように行うか？

2.1.2 進め方

(3) 脅威と脆弱性のリスト作成

分かりやすく書くと・・・

脅威：攻撃の仕方

脆弱性：システムの弱み

何がどのように侵害されたかを以下の3点をヒントに考える。 (JIS Q 27000より)

- 機密性(C Confidentiality)：許可された正規のユーザーだけが情報にアクセスでき、許可されていないユーザーには情報を使用させず、開示しない特性
- 完全性(I Integrity)：情報が完全で、改ざん・破壊されていないという情報資産の正確さおよび完全さの特性
- 可用性(A Availability)：障害が発生しても安定したサービスを提供でき、ユーザーが必要な時にシステムや情報を利用可能である特性

機密性の侵害・完全性の侵害・可用性の侵害の例を考えてみよう。

2.セキュリティリスクアセスメントの基礎概念

2.1セキュリティリスクアセスメントは、いつ、どのように行うか？

2.1.2 進め方

システム構成図に「脆弱性(弱み)があるところに攻撃者の脅威が襲う」というイメージを元に脆弱性と脅威を記入する。

★どのくらいの脅威と脆弱性を挙げるか？

→作業工期・作業工数で判断（いくらでも挙げることができるため）

挙げた脅威と脆弱性はリストに整理する。

(4) 脅威と脆弱性の優先度付け

主観評価、攻撃トレンドに合わせる・ビジネス上のポイントなど着眼するポイントを記録しておく。

IPA「中小企業の情報セキュリティ対策ガイドライン」のアセスメントシートにに例がある。5段階評価などでよい。（IPAのアセスメントシートでは、脅威×脆弱性の値でリスクの大きさを測る。）

2.セキュリティリスクアセスメントの基礎概念

2.1.セキュリティリスクアセスメントは、いつ、どのように行うか？

2.1.2.進め方

(5) 脅威と脆弱性に対する管理策立案

- 上記(4)のリストにおいて対応する範囲を決め（例：脅威×脆弱性の値＞20など）脅威・脆弱性それぞれに対して対策を決める。
- 上記(2)で挙げた事例に記載されている事件の状況や対策を参考にするとよい。

(6) 管理策適用スケジュール・PDCA案策定

管理策を適用するスケジュールを立案する。

セキュリティリスクアセスメントは定期的（最低年に1回）に実施するべきと言われている。実施周期・実施時期を決める。

★セキュリティトレンドは変化する。設計開発のときに1回だけ実施し、あとはなし崩し的に未実施、そのうち大規模インシデント発生によって誰かがクビになんてならないように。

2.セキュリティリスクアセスメントの基礎概念

2.1.セキュリティリスクアセスメントは、いつ、どのように行うか？

2.1.2.進め方

(3) 脅威・脆弱性のリスト作成・(4) 優先度付け　の整理例

アセット	ステークホルダ	脅威	評価	脆弱性	評価	リスク値	事例
OS設定情報(WEBサーバ)	WEBサーバ管理者	使われていないポートを狙ってtelnetアクセスする。	5	OSのポート番号設定漏れで未使用ポートが開いたまま	5	25	攻撃者がWEBサーバ内に侵入しサーバ内の情報を窃盗（ユーザの氏名・年齢・性別・メールアドレス）
同上	同上	開いたままのポートに対し大量のTCPSYNパケット送信	5		5	25	システムが超高負荷となりサービスが提供できなくなる。
管理者ID・パスワード(WEBサーバ)	同上	管理者IDに対してよく知られたパスワードを連続入力	5	想像が容易な管理者パスワード	5	25	攻撃者がWEBサーバ内に侵入し任意のコマンドを実行

2.セキュリティリスクアセスメントの基礎概念

2.1.セキュリティリスクアセスメントは、いつ、どのように行うか？

2.1.2.進め方

(5) 脅威と脆弱性に対する管理策の立案

【脅威に対する管理策の整理例】

アセット	ステークホルダ	脅威	評価	脅威に対する管理策
OS設定情報(WEBサーバ)	WEBサーバ管理者	使われていないポートを狙ってtelnetアクセスする。	5	OSの設定でtelnetの使用を認めない。
同上	同上	開いたままのポートに対し大量のTCPSYNパケット送信	5	ファイアウォールで特定のIPからの同じポートに対する連続したTCPSYNパケットはフィルタする。（それが可能はファイアウォールを導入する。）
管理者ID・パスワード(WEBサーバ)	同上	管理者IDに対してよく知られたパスワードを連続入力	5	管理者IDを利用した外部からのアクセスを認めない設定とする。 sudoコマンド実行時のパスワードを高エントロピなど破りづらいパスワードとする。

2.セキュリティリスクアセスメントの基礎概念

2.1.セキュリティリスクアセスメントは、いつ、どのように行うか？
2.1.2.進め方
(5) 脅威と脆弱性に対する管理策立案
【脆弱性に対する管理策の整理例】

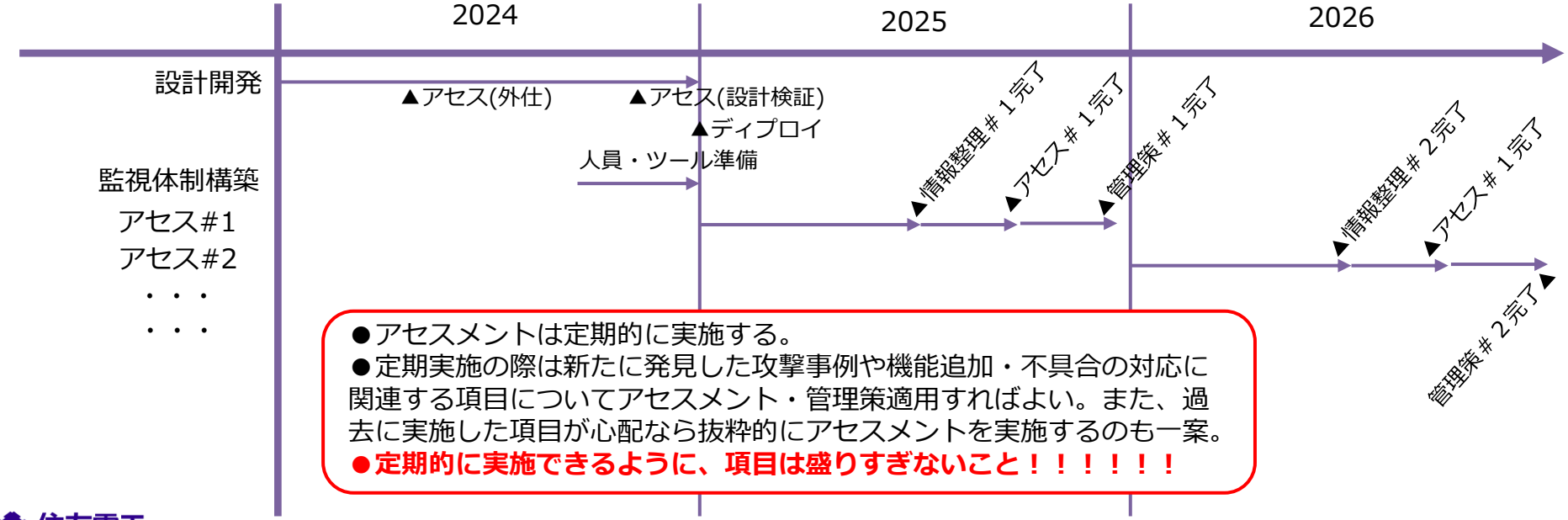
アセット	ステークホルダ	脆弱性	評価	脆弱性に対する管理策
OS設定情報(WEBサーバ)	WEBサーバ管理者	OSのポート番号設定漏れで未使用ポートが開いたまま	5	●WEBサーバで使用するポートを決めそれ以外のポートは全て閉じる。 ●システム規約の中でもサービス全体で使用するポート番号を決めファイアウォールでフィルタする。
管理者ID・パスワード(WEBサーバ)	同上	想像が容易な管理者パスワード	5	sudoコマンド実行時のパスワードを高エントロピなど破りづらいパスワードとする。

2.セキュリティリスクアセスメントの基礎概念

2.1.セキュリティリスクアセスメントの実施タイミング

2.1.2 進め方

(6) 管理策適用スケジュール・PDCA案策定
　線表を作成する。



●アセスメントは定期的に実施する。
●定期実施の際は新たに発見した攻撃事例や機能追加・不具合の対応に関連する項目についてアセスメント・管理策適用すればよい。また、過去に実施した項目が心配なら抜粋的にアセスメントを実施するのも一案。
●定期的に実施できるように、項目は盛りすぎないこと！！！！！！

2.セキュリティリスクアセスメントの基礎概念

2.1セキュリティの分析と対応は、いつ、どのように行うか？

2.1.3 注意事項

●攻撃の仕方が日々進歩するのにどのように対応するか。
製品・サービスが進化すれば分析・対応すべき対象も増える。
攻撃手法は進化し、攻撃者は攻撃ビジネスを進化させる。
製品がある限り分析と対応に終わりはない。

★リリースしたら終わりではない。最低でも年に1回はセキュリティリスクアセスメントを実施。定期的にPDCAとして実施する。

★初回リリース以降は機能的な追加変更、攻撃トレンドに合わせて分析する脅威・脆弱性を調整する。

★後述するが、脅威×脆弱性を考え、優先的に分析・対応する脅威・脆弱性を選ぶ。
項目は定期的な実施・かけられる人件費で実施できる範囲に留める。
(今回できない項目は次回・・・くらいの感覚で捉える。)

2.セキュリティリスクアセスメントの基礎概念

2.1.セキュリティリスクアセスメントは、いつ、どのように行うか？

2.1.3.セキュリティリスクアセスメントの実施タイミング

①要件定義策定まで

★ビジネス要件を検討するときに重要度の高いリスク要件を洗い出し後段の脅威脆弱性の重みづけに反映。BIA(Business Impact Analysis)と呼ぶ。

②外部仕様書完成(詳細設計に入る手前)まで

★セキュリティリスクアセスメントを実施する。

セキュリティ(管理策)の作りこみを確定させておき、詳細設計に反映させる。

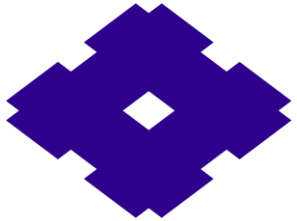
内部品質を設計するときにはセキュリティの作りこみ(管理策)を反映させる。

③結合テスト結果の確認

作りこんだ管理策が設計検証結果に反映されていることを確認する。

④定期的なアセスメント実施、機能追加や不具合対応時に実施。

新たな攻撃事例の反映・機能追加や不具合対応の反映を入れる。リリース時に確認した項目は必要なものを選択するなど。



住友電工

Connect with Innovation

https://sumitomoelectric.com/jp/

SUMITOMO
ELECTRIC
GROUP