"再現性"を重視した脅威モデリングベースのセキュリティ・リスクアセスメント

脅威モデリングナイト #5 in Tokyo
2024/12/06 (Fri)

Presented by 黒豆

サマリー

リスクアセスメントに脅威モデリングの考え方を適用した結果、以下の恩恵が得られた。

➔ **評価結果の再現性向上**
これまで言語化されていなかったリスク判断材料や思考プロセスが明確になり、評価の再現性が向上した。

➔ **要求スキルが下がり、分業可能に**
評価の思考プロセスをモデル化、数式に落とし込むことで、評価者に要求される知見のハードルが下がり、評価の分業も可能になった。

アジェンダ

- スピーカー紹介
  - 経歴
  - 脅威モデリングとの関わり
- 脅威ベース・リスクアセスメント
  - ...とは?
  - よくあるアセスメントとの違い
  - 恩恵と犠牲
- まとめ

スピーカー

名前　黒豆 (X: @tanbablack)

役割　情報セキュリティ・マネージャー
セキュリティ・アーキテクト
SIRT（インシデント・コマンダー）

脅威モデリングとの関わり

SIerでプロジェクトマネージャー

顧客提案の前段階として、顧客システムをリスク評価
STRIDEなどの脅威モデリングに触れる

Crypto業界でセキュリティエンジニア

年次リスクアセスメントで脅威ベース・
アセスメントを実践。課題を感じる

転職前の有給消化期間

自身のノウハウを資料化
脅威ベース・アセスのテンプレ作成

HR業界でセキュリティ責任者

作成したアセスメントを適用

脅威ベース・
リスクアセスメント

...とは？

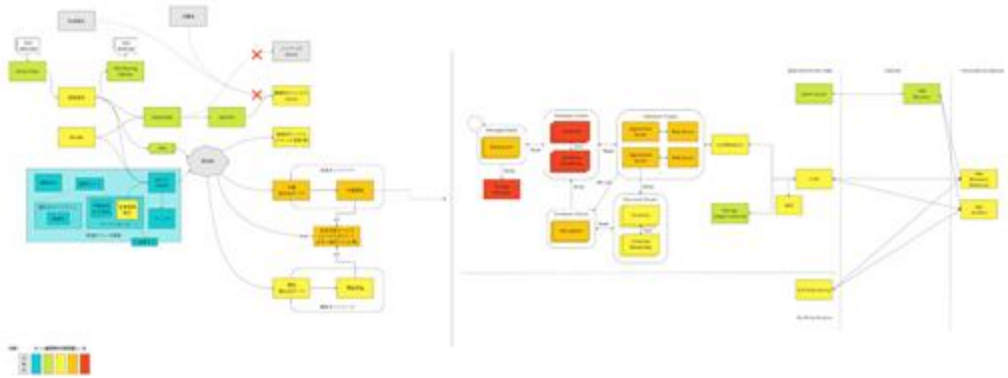
➔ 脅威モデリングをもとにリスク評価者の思考を分解・再整理したリスクアセスメント手順

適用可能な対象は？

➔ コーポレートIT,プロダクト全部

カバーしていない範囲は？

➔ 事務過誤観点のリスク
(別途、業務別データフロー図を作成し評価推奨)



脅威ベース・
リスクアセスメント

…とは？

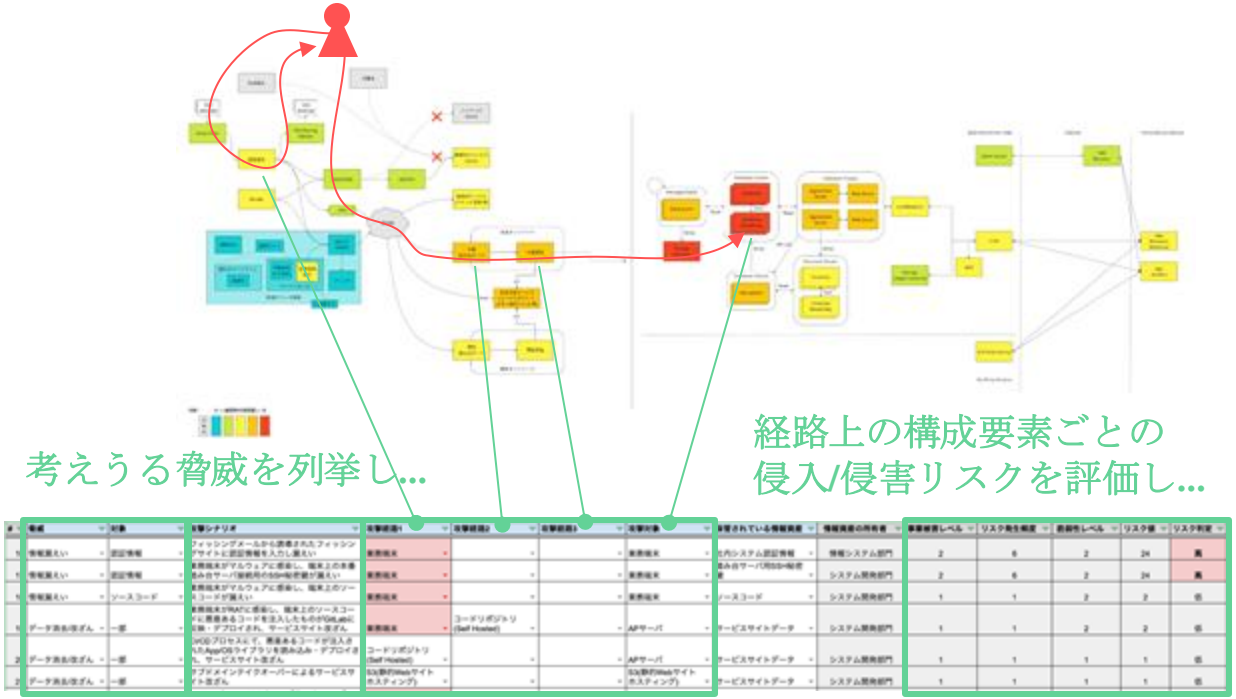
➔ 脅威モデリングをもとにリスク評価者の思考を分解・再整理したリスクアセスメント手順

適用可能な対象は？

➔ コーポレートIT,プロダクト全部

カバーしていない範囲は？

➔ 事務過誤観点のリスク
(別途、業務別データフロー図を作成し評価推奨)



考えうる脅威を列挙し…

経路上の構成要素ごとの
侵入/侵害リスクを評価し…

システム構成図から考えうる
脅威ごとの攻撃シナリオと、
その攻撃経路を抽出し…

攻撃シナリオごと
リスクを評価

よくあるリスクアセスメント

＜リスク計算式＞

情報資産ごとの

リスク値 ＝

リスク発生時の **被害レベル** × 脅威の **発生可能性** × 保管場所の **脆弱性レベル**

よくあるリスクアセスメント

＜リスク計算式＞

情報資産ごとの

リスク値 ＝

リスク発生時の **被害レベル** × 脅威の **発生可能性** × 保管場所の **脆弱性レベル**

事業被害レベル定義

直接的経済損失(インシデント対応費用・工数など)

被害度合い	被害レベル
会社資本金を上回る損失／倒産	20
年間決算へ影響	2
当四半期決算へ影響	1
無し、又は当月利益へのみ影響	0

風評被害

被害度合い	被害レベル
-	-
ブランドイメージの毀損	2
一部顧客からの信用失墜	1
無し、又は軽微	0

法令違反

被害度合い	被害レベル
事業に必須の認可取り消し	20
当局から行政指導となる違反	2
法令罰則対象となる違反	1
無し、又は軽微な違反	0

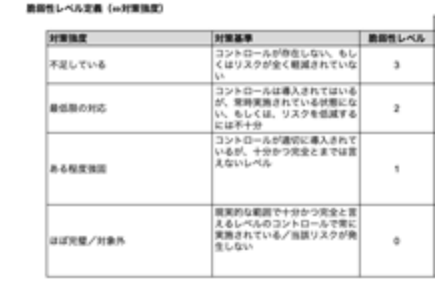
顧客被害/業務阻害

被害度合い	被害レベル
事業継続困難／長期システム停止	20
全顧客に影響／サービス運営に影響	2
一部顧客に影響／一部業務遂行に影響	1
無し、又は軽微	0

リスク発生頻度定義

リスク発生頻度 ＝ MAX（①、②）

リスク発生動向	リスク発生頻度
①直近3年で当社で毎年発生	10
②基準値1に対して、下記条件に該当する分を加算(最小値: 1)	
・直近3年で当社で2件以上発生	4
・直近1年で同業他社で発生事例あり	3
・直近3年で当社で1件だけ発生	2
・直近3年で当社で未発生	0



脆弱性レベル定義（∞対策強度）

対策強度	対策基準	脆弱性レベル
不足している	コントロールが存在しない、もしくはリスクが全く軽減されていない	3
最低限の対応	コントロールは導入されてはいるが、常時実施されている状態にない、もしくは、リスクを低減するには不十分	2
ある程度強固	コントロールが適切に導入されているが、十分かつ完全とまでは言えないレベル	1
ほぼ完璧／対象外	現実的な範囲で十分かつ完全と言えるレベルのコントロールで常に実施されている／当該リスクが発生しない	0

➔問題点は？

担当者の声

保管場所の脆弱性は、途中経路上の他の対策を含んだ総合評価ですか？

Kさん、東京

昨年、認証情報の漏洩を被害レベル２とした判断根拠は何でしたっけ？

Hさん、東京

最終的には〇〇さんの判断次第ですよね？

Oさん、神奈川

担当者の

保管場所の脆弱性
は、途中経路上の
他の対策を含んだ
総合評価ですか？

Kさん、東京

問題点

リスク評価者の思考プロセスの

不透明性

評価基準は明確だが、どの程度のスコアになるかを判断する材料が何でどう評価したのかは言語化されていない

終的には〇〇さ
の判断次第です
ね？

ん、神奈川

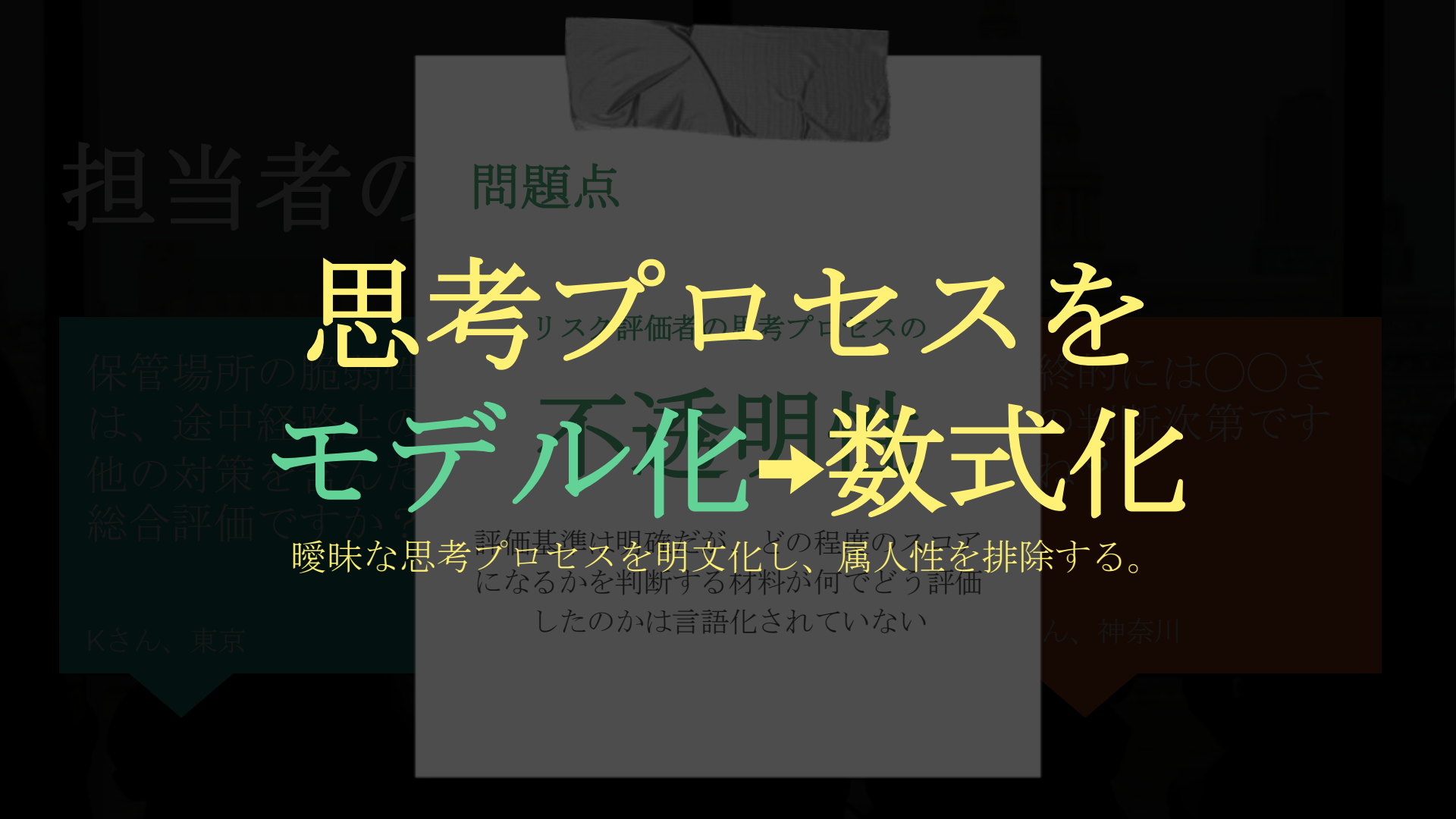
問題点

リスク評価者の思考プロセスの

不透明性

評価基準は明確だが、どの程度のスコアになるかを判断する材料が何でどう評価したのかは言語化されていない

じゃあ、どうする？


問題点
思考プロセスを
モデル化→数式化
曖昧な思考プロセスを明文化し、属人性を排除する。

モデル化

取り扱う対象から目的に照らして不要な側面を捨象して、
その構造や構成要素、対象間の関係や互いに及ぼす作用などを
模式的に表した模型（モデル）を作り、図表や数式などを用い
て定義すること。

⇒ 脅威モデリング（Threat Modeling）

IT用語辞典「e-Words」より

思考プロセスのモデル化⇒数式化

＜リスク計算式＞

情報資産ごとの

リスク値 ＝

リスク発生時の **被害レベル** × 脅威の **発生可能性** × 保管場所の **脆弱性レベル**

保管場所の脆弱性は、途中経路上の他の対策を含んだ総合評価ですか？

思考プロセスのモデル化⇒数式化

＜リスク計算式＞

情報資産ごとの

リスク値 ＝

リスク発生時の **被害レベル** × 脅威の **発生可能性** × 保管場所の **脆弱性レベル**

情報資産の保管場所へ到達可能な**アクセス経路**から想定される**攻撃シナリオ**を洗い出す。
攻撃経路上の**各構成要素の対策状況**から侵入可否・攻撃成功可否を判断。
全攻撃シナリオの判断結果から、脆弱性を総合判断してる。

思考プロセスのモデル化⇒数式化

＜リスク計算式＞

情報資産ごとの

リスク値 ＝

リスク発生時の **被害レベル** × 脅威の **発生可能性** × 保管場所の **脆弱性レベル**

情報資産の保管場所へ到達可能な**アクセス経路**から想定される**攻撃シナリオ**を洗い出す。
攻撃経路上の**各構成要素の対策状況**から侵入可否・攻撃成功可否を判断。
全攻撃シナリオの判断結果から、脆弱性を総合判断してる。

数式化

思考プロセスのモデル化⇒数式化

＜リスク計算式＞
~~情報資産~~
攻撃シナリオごとの

リスク値 ＝

リスク発生時の **被害レベル** × 脅威の **発生可能性** × ~~保管場所の~~ **MAX(** 構成要素 × 脅威別 **脆弱性レベル, ..)**

攻撃経路上で最も脆弱な箇所を基準に
攻撃に対する脆弱性を評価

思考プロセスのモデル化⇒数式化

＜リスク計算式＞

攻撃シナリオごとの

リスク値 ＝

リスク発生時の **被害レベル** × 脅威の **発生可能性** × **MAX(** 構成要素 × 脅威別 **脆弱性レベル, ..)**

思考プロセスのモデル化⇒数式化

＜リスク計算式＞

攻撃シナリオごとの

リスク値 ＝

リスク発生時の **被害レベル**

何の情報が**どんな脅威**の被害にあったかでだいたい決まる。
“どのお客さんの情報が”といった情報の内容にまで左右されない。

× 脅威の **発生可能性**

換金性の高い情報の方が狙われやすい…脅威トレンドでも来る攻撃は変わる…
つまり、**何の情報**かと**脅威の傾向**で判断している。

× **MAX**(構成要素 × 脅威別 **脆弱性レベル**, ..)

思考プロセスのモデル化⇒数式化

＜リスク計算式＞

攻撃シナリオごとの

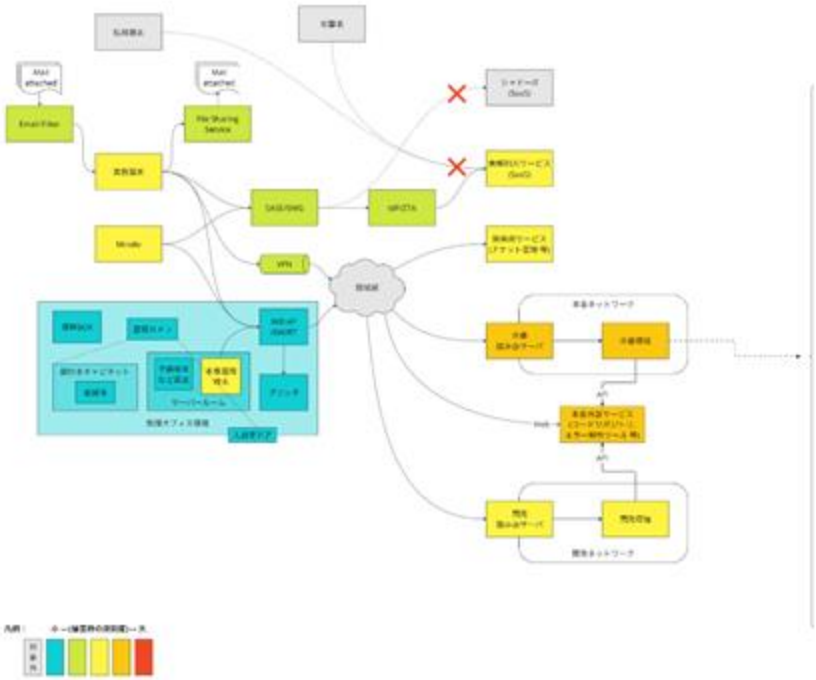
リスク値 ＝

~~リスク発生時の~~情報資産×脅威別 **被害レベル** × ~~脅威の~~情報資産×脅威別 **発生可能性** × **MAX(** 構成要素×脅威別 **脆弱性レベル**, ..**)**

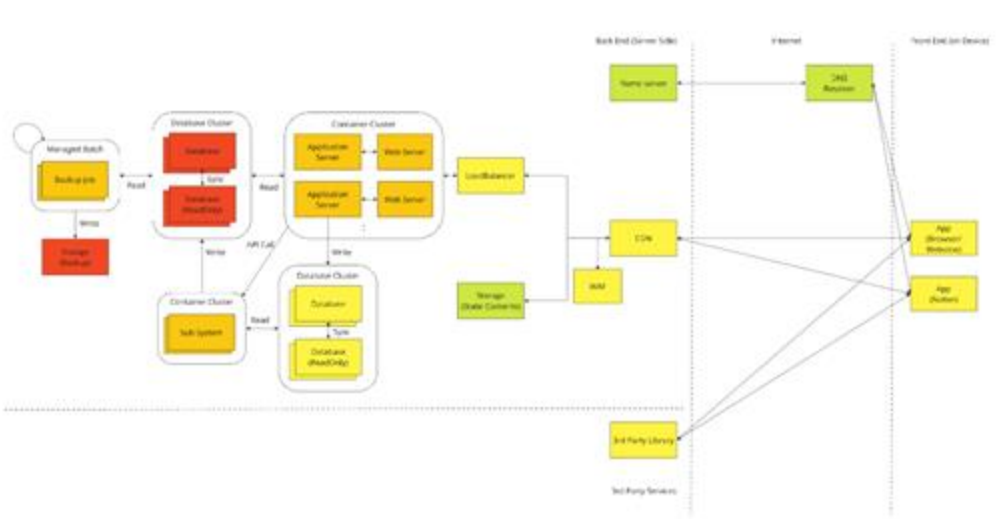
脅威ベース・リスクアセスメントの

具体例

コーポレートIT



プロダクション環境



システム構成概要図

情報資産へのアクセス経路の有無、攻撃シナリオを洗い出すために作成

リスクレベル定義

事業継続不可レベルの被害に対する対策は発生可能性が低くとも行うべき、甚大レベルも発生可能性が高い場合は対処必須という判断から、リスク高以上を対応必須とする。

		事業被害			
		無しまたは軽微（0）	限定的（1）	甚大（2）	事業継続不可（20）
発生可能性	いつ起きてもおかしくない（20~30）	無(0)	高(20~30)	高(40~60)	致命的(400~600)
	可能性は高い（10~19）	無(0)	中(10~19)	高(20~40)	高(200~380)
	可能性は低い（1~9）	無(0)	低(1~9)	低(2~9)＼中(10~18)	高(20~180)
	現実的にほぼ起こりえない（0）	無(0)	無(0)	無(0)	無(0)

リスク受容基準

リスクレベル	対応レベル
致命的(400~)	即時対応
高(20~399)	対応必須
中(10~19)	リスク受容するか要検討
低(1~9)	リスク受容
無(0)	不要

リスク受容基準

恣意的なリスク判断にならないために、どこまで受容するかを事前定義

事業被害レベル定義

直接的経済損失(インシデント対応費用・工数など)

被害度合い	被害レベル
会社資本金を上回る損失／倒産	20
年間決算へ影響	2
当四半期決算へ影響	1
無し、又は当月利益へのみ影響	0

風評被害

被害度合い	被害レベル
-	-
ブランドイメージの棄損	2
一部顧客からの信用失墜	1
無し、又は軽微	0

法令違反

被害度合い	被害レベル
事業に必須の認可取り消し	20
当局から行政指導となる違反	2
法令罰則対象となる違反	1
無し、又は軽微な違反	0

顧客被害/業務阻害

被害度合い	被害レベル
事業継続困難／長期システム停止	20
全顧客に影響／サービス運営に影響	2
一部顧客に影響／一部業務遂行に影響	1
無し、又は軽微	0

脅威×対象別の事業被害レベル

間接的な影響は含まないものとする。また、1つの事象で複数の事業被害が考えられるインシデントも存在する。
また、"その他の情報"の事業被害レベルは事前に定義できないため、情報資産管理台帳を参照する。(ここでは0に設定)

脅威	対象	被害観点	観点別の被害レベル	事業被害レベル
情報漏えい	顧客個人情報	直接的経済損失	2	2
		風評被害	2	
		法令違反	2	
		顧客被害/業務阻害	0	
情報漏えい	従業員個人情報	直接的経済損失	1	1
		風評被害	1	
		法令違反	1	
		顧客被害/業務阻害	0	
情報漏えい	認証情報	直接的経済損失	1	2
		風評被害	2	
		法令違反	0	
		顧客被害/業務阻害	2	
情報漏えい	ソースコード	直接的経済損失	1	1
		風評被害	1	
		法令違反	0	
		顧客被害/業務阻害	1	
情報漏えい	インサイダー情報	直接的経済損失	2	2
		風評被害	2	
		法令違反	1	
		顧客被害/業務阻害	0	
情報漏えい	その他の情報	直接的経済損失	0	0
		風評被害	0	
		法令違反	0	
		顧客被害/業務阻害	0	
データ消去/改ざん	一部	直接的経済損失	1	1
		風評被害	1	
		法令違反	0	
		顧客被害/業務阻害	1	
データ消去/改ざん	全部	直接的経済損失	2	20

事業被害レベル

脅威 × 被害対象情報別に事前定義

リスク発生頻度定義

リスク発生頻度　＝　MAX（①、②）	
リスク発生動向	**リスク発生頻度**
①直近3年で当社で毎年発生	10
②基準値1に対して、下記条件に該当する分を加算(最小値: 1)	
・直近3年で当社で2件以上発生	4
・直近1年で同業他社で発生事例あり	3
・直近3年で当社で1件だけ発生	2
・直近3年で当社で未発生	0

脅威×対象別のリスク発生頻度

脅威	対象	リスク発生頻度の判断根拠	判断根拠の参照情報	リスク発生頻度
情報漏えい	顧客個人情報	・直近3年で当社で2件以上発生 ・直近1年で同業他社で発生事例あり	YYYY年A月にグループ会社で1件発生 YYYY年B月に当社で1件発生 YYYY年C月に他社で発生	8
情報漏えい	従業員個人情報	・直近1年で同業他社で発生事例あり ・直近3年で当社で未発生	YYYY年D月に他社で発生	4
情報漏えい	認証情報	・直近1年で同業他社で発生事例あり ・直近3年で当社で1件だけ発生	YYYY年E月に他社で発生 YYYY年F月にグループ会社で1件発生	6
情報漏えい	ソースコード	・直近3年で当社で未発生	インシデント発生履歴に該当なし	1
情報漏えい	インサイダー情報	・直近3年で当社で未発生	インシデント発生履歴に該当なし	1
情報漏えい	その他の情報	・直近3年で当社で未発生	インシデント発生履歴に該当なし	1
データ消去/改ざん	一部	・直近3年で当社で未発生	インシデント発生履歴に該当なし	1
データ消去/改ざん	全部	・直近3年で当社で未発生	インシデント発生履歴に該当なし	1
サービス停止	一部	・直近3年で当社で未発生	インシデント発生履歴に該当なし	1
サービス停止	全部	・直近3年で当社で未発生	インシデント発生履歴に該当なし	1

リスク発生頻度

脅威 × 被害対象情報別に事前定義

脆弱性レベル定義（⇔対策強度）

対策強度	対策基準	脆弱性レベル	対策基準の参考例			
			侵入	情報漏洩	データ消去/改ざん	サービス停止
不足している	コントロールが存在しない、もしくはリスクが全く軽減されていない	3	認証がID/パスワードのみで、ユーザが任意のパスワードを設定可能	何もしていない	何もしていない	インフラのSLAが明示されていないインフラを利用している
最低限の対応	コントロールは導入されてはいるが、常時実施されている状態にない、もしくは、リスクを低減するには不十分	2	認証がID/パスワードのみだが、管理者により複雑なパスワードが強制されている	契約による縛り、または教育のみ	運用ルールによって、編集前にバックアップを取る等の手順がある	インフラのSLAは明示されていないが、自社でバックアップを実施している
ある程度強固	コントロールが適切に導入されているが、十分かつ完全とまでは言えないレベル	1	認証に以下のいずれかを採用 ・MFA ・API連携(key,secretはサービス内保管) または、以下いずれかを実施 ・脆弱性管理 ・侵入検知及び遮断(IPS,EDR,Firewall等)	以下の実施 ・奉制が働いたアクセス権管理 ・インシデント時のログ等によるトレーサビリティの確保	以下いずれかに該当 ・バックアップによる切り戻しが可能 ・マスターデータが別に存在する	バックアップ・可用性に関するSLAが明示されているクラウド事業者のインフラを利用している
ほぼ完璧／対象外	現実的な範囲で十分かつ完全と言えるレベルのコントロールで常に実施されている／当該リスクが発生しない	0				

構成要素×脅威別の対策状況（脆弱性レベル）

構成要素	脅威	予防的対策	発見的対策	脆弱性レベル
APサーバ	侵入	○ インバウンド通信制限(踏み台経由必須) ○ ログイン制限(SSM経由での接続制限) × DB接続情報のSecret Manager保管 ○ セキュアコーディング ○ コードレビュー △ 脆弱性管理(検知/緊急度判断が属人) × OSイメージの軽量化 ○ AP＆NW脆弱性診断 ○ WAF × アプリケーション実行制限	○ ログ監視(GuardDuty有効化) × WAFログ監視 × サーバ侵入検知 △ インシデント対応マニュアル整備	2
APサーバ	情報漏えい	△ アウトバウンド通信制限(○DenyList方式, ×AllowList方式)	× NWアノマリ検知 - データ復号キーのKMS参照検知	1
APサーバ	データ消去/改ざん	○ CI/CD自動化 ○ IaC化	-	0
APサーバ	サービス停止	○ CDN ○ ALB ○ AutoScaling ○ ratelimit ○ ログイン画面へのreCAPTCHA/OTP/Passkey実装	○ メトリクス監視 ○ DDoS検知(リクエスト数&応答時間)	0
サブシステム	侵入	(APサーバと同じだが、以下差分) ○ NWセグメンテーション	(APサーバと同じ)	1
サブシステム	情報漏えい	(APサーバと同じ)	(APサーバと同じ)	1
サブシステム	データ消去/改ざん	(APサーバと同じ)	(APサーバと同じ)	0
サブシステム	サービス停止	(APサーバと同じ)	(APサーバと同じ)	1
DB	侵入	○ インバウンド通信制限(踏み台経由必須) ○ ログイン制限(SSM経由での接続制限) ○ NWセグメンテーション ○ マネージドサービス利用 △ 定期的なアカウント棚卸し(入退社/異動時のみ)	○ ログ監視(GuardDuty有効化)	1
DB	情報漏えい	○ 顧客別のDBスキーマ分離 ○ DB暗号化 △ 重要レコードの暗号化(PW暗号スイートがSHA1)	× DB監査ログ検知(クエリログ、監査ログ)	1
DB	データ消去/改ざん	○ バックアップ取得 △ リストアマニュアル整備・演習(不定期実施) × 別クラウド基盤へのバックアップ	-	0
DB	サービス停止	○ マネージドサービス利用 ○ スケーリング(ElastiCache利用)	○ メトリクス監視	0

対策内容から
脆弱性レベル
を決定するの
は有識者判断

脆弱性レベル

構成要素 × 脅威別に事前定義

＜リスク計算式＞

攻撃シナリオごとの

リスク値 ＝

情報資産 × 脅威別 被害レベル × 情報資産 × 脅威別 発生可能性 × MAX(構成要素 × 脅威別 脆弱性レベル, ..)

被害レベル、発生可能性は、攻撃対象となる 情報資産×脅威 の組み合せによって決定

#	脅威	対象	攻撃シナリオ	攻撃経路1	攻撃経路2	攻撃経路3	攻撃対象	保管されている情報資産	情報資産の所有者	事業被害レベル		リスク発生頻度		脆弱性レベル		リスク値	リスク判定
16	情報漏えい	認証情報	フィッシングメールから誘導されたフィッシングサイトに認証情報を入力し漏えい	業務端末			業務端末	社内システム認証情報	情報システム部門	2	×	6	×	2	=	24	高
17	情報漏えい	認証情報	業務端末がマルウェアに感染し、端末上の本番踏み台サーバ接続用のSSH秘密鍵が漏えい	業務端末			業務端末	踏み台サーバ用SSH秘密鍵	システム開発部門	2		6		2		24	高
18	情報漏えい	ソースコード	業務端末がマルウェアに感染し、端末上のソースコードが漏えい	業務端末			業務端末	ソースコード	システム開発部門	1		1		2		2	低
19	データ消去/改ざん	一部	業務端末がRATに感染し、端末上のソースコードに悪意あるコードを注入したものがGitLabに反映・デプロイされ、サービスサイト改ざん	業務端末	コードリポジトリ (Self Hosted)		APサーバ	サービスサイトデータ	システム開発部門	1		1		2		2	低
20	データ消去/改ざん	一部	CI/CDプロセスにて、悪意あるコードが注入されたApp/OSライブラリを読み込み・デプロイされ、サービスサイト改ざん	コードリポジトリ (Self Hosted)			APサーバ	サービスサイトデータ	システム開発部門	1		1		1		1	低
21	データ消去/改ざん	一部	サブドメインテイクオーバーによるサービスサイト改ざん	S3(静的Webサイトホスティング)			S3(静的Webサイトホスティング)	サービスサイトデータ	システム開発部門	1		1		1		1	低

経路上で脆弱性レベルが最高値の構成要素 ⇒要対策箇所

攻撃シナリオに対する脆弱性は、
攻撃経路上の構成要素の脆弱性レベルの最大値

攻撃シナリオ別リスク

攻撃シナリオ（侵入/漏洩等の経路）を定義したらリスク値が自動計算される

恩恵

一連の攻撃リスクを、構成要素ごとのリスク値の集合に分解して評価するため…

➔ **評価者の要求スキルが下がった**
“攻撃の全体像” と “詳細な対策” の両方を把握している必要はなくなった。

➔ **分業が可能になった**
"攻撃の全体像" はセキュリティ担当者、"各構成要素の対策の評価" はエンジニアというような分担が可能になった。

犠牲

一連の攻撃リスクを、構成要素ごとのリスク値の集合に分解して評価するため…

➔ **対策の穴を見落とす可能性あり**
スコア化により、攻撃手法ごとに有効な対策が取られているか見えづらくなった結果、低リスク値でも特定の攻撃が成立する可能性は残る。

サマリー

リスクアセスメントに脅威モデリングの考え方を適用した結果、以下の恩恵が得られた。

➔ **評価結果の再現性向上**
これまで言語化されていなかったリスク判断材料や思考プロセスが明確になり、評価の再現性が向上した。

➔ **要求スキルが下がり、分業可能に**
評価の思考プロセスをモデル化、数式に落とし込むことで、評価者に要求される知見のハードルが下がり、評価の分業も可能になった。

資料は無償配布中

DLはXプロフィールから

ココからDL

サマリー

リスクアセスメントに脅威モデリングの考え方を適用した結果、以下の恩恵が得られた。

➔ **評価結果の再現性向上**
これまで言語化されていなかったリスク判断材料や思考プロセスが明確になり、評価の再現性が向上した。

➔ **要求スキルが下がり、分業可能に**
評価の思考プロセスをモデル化、数式に落とし込むことで、評価者に要求される知見のハードルが下がり、評価の分業も可能になった。

Thank you !

資料は無償配布中

DLはXプロフィールから

ココからDL