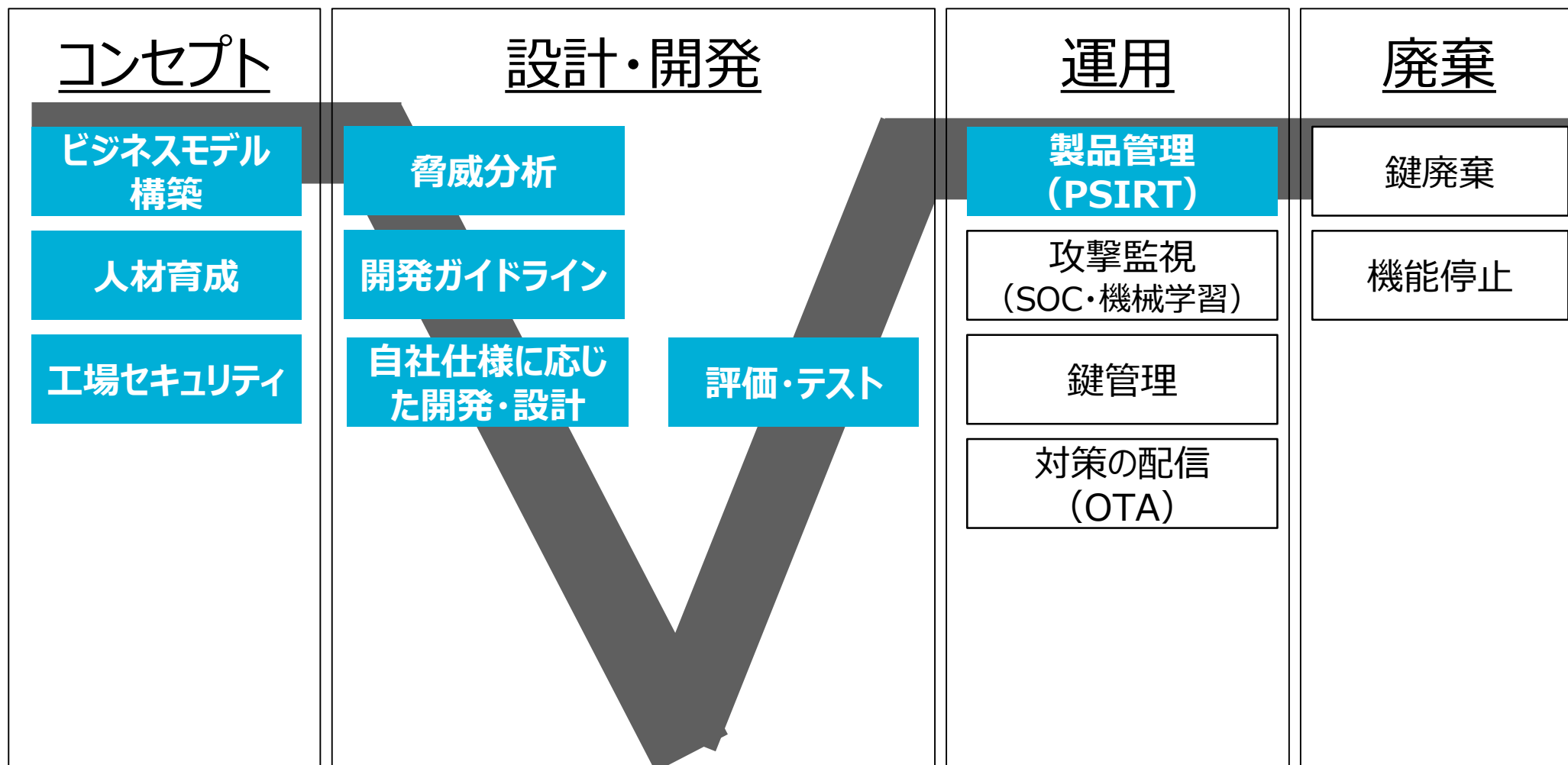


# 製品のライフサイクルに応じた セキュリティ対策のご紹介

NRIセキュアテクノロジーズ株式会社

# 製品のライフサイクルに応じたセキュリティ対策のご紹介

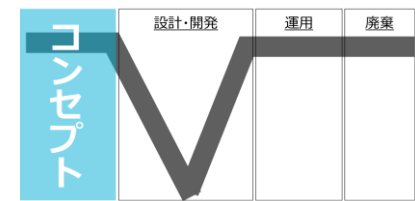
- 製品のライフサイクルにおいて必要なセキュリティ対策は多岐にわたります。  
弊社は、全フェーズにおいてご支援可能です。



# 製品のライフサイクルに応じたセキュリティ 対策のご紹介

～ コンセプト ～

# 【ビジネスモデル構築（デジタルサービスリスク評価サービス）】 デジタルサービスリスクへの対応の考え方



詐欺・悪用に繋がるユースケース(Scam Case/Fraud Case)を洗い出し、リスク評価の上で適宜対策を実施

全ての表ケースには、必ず裏ケースが存在

サービス仕様検討段階からリスク分析/方針策定



- 盗難クレカ紐付け
- IoT SIM+RPA悪用
- ジャンク混入 (AI誤動作)
- クーポン無限増殖
- マーケティング妨害
- 不正決済、店舗結託

過去の“同系の脅威”の歴史を把握

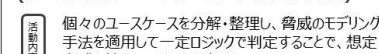
- ・ 同業他社・類似脅威事例
- ・ 同類サービスに対する脅威事例
- ・ 同系脆弱性に対する脅威事例

Step1 サービスの分析

**分析①：脅威事例ベースのアプローチ**  
過去の脅威事例を基にした、複数のユースケース (既存システム含む) を利用する脅威の分析  
対象デジタルサービスのビジネスモデルを要素分解し、ビジネスモデル上に存在する脅威を、過去の事例を踏まえて抽出しリスク評価する



**分析②：ユースケースベースのアプローチ**  
サービスのユースケースの悪用に関する脅威の分析 (サービス特有のユースケースを重点的に評価)  
個々のユースケースを分解・整理し、脅威のモデリング手法を適用して一定リスクで判定することで、想定脅威を抽出してリスク評価する



取るべき対策の合意形成

- ・ 業務レベルの対応
- ・ システム要件の検討
- ・ モニタリング対策の検討

Step2 脅威シナリオ作成

分析結果を基に評価対象サービスで発生しうる具体的な脅威シナリオを作成



- 脆弱な本人認証(メールアドレス登録のみ等)で大量のアカウントを作成し、サービスの初回利用登録を何度も実施することで、初回特典を大量に取得する
- 侵害したアカウントと自身のアカウントを紐付けて、ポイントやクーポン等の特典を窃盗する。

Step3 リスク評価

脅威シナリオにおける事業影響を踏まえたリスク評価を実施



セキュリティ対策は、サービスの提供価値や利便性とトレードオフとなることがある。そのため、サービス主管部門とディスカッションの上、最終的なリスク値や対策方向性を定める

リスク点検の観点

- ・ レピュテーションリスク (顧客保護、ブランド保護)
- ・ コンプラリスク
- ・ プライバシーリスク
- ・ セキュリティリスク

# 【ビジネスモデル構築（デジタルサービスリスク評価サービス）】 評価の進め方

| コンセプト | 設計・開発 | 運用 | 廃棄 |
|-------|-------|----|----|
|       |       |    |    |

## デジタルサービスリスク評価の進め方



### 【対象サービスのビジネスモデル及びユースケースの分解】

- ✓ 対象サービスのビジネスモデルを分解し、ビジネスモデル上のキーとなる要素や類似ビジネスを明らかにします。
- ✓ 対象サービスのユースケースを分解し、ステークホルダーが実施可能なアクションを明確にします。



### 【トップダウン分析(脅威事例に基づく分析)】

- ✓ ビジネスモデル上のキーとなる要素や類似ビジネスで発生した脅威事例を基に、対象サービスで想定される脅威シナリオを作成します。
- ✓ 想定される脅威シナリオに対して、対象サービス独自の仕様(他社サービスとの差分)を基に具体的な脅威シナリオを作成すると共に、セキュリティコントロールの実装状況を確認します。



### 【ボトムアップ分析(ユースケースに対する分析)】

- ✓ 全ユースケース/アクションから、悪意者が実施すると想定されるアクションを抽出にします。
- ✓ 悪意者実施すると想定されるアクションのうち、悪意者にとってメリットが大きい狙われやすいアクションを中心にセキュリティコントロールの実装状況を確認します。



### 【ディスカッション】

- ✓ トップダウン/ボトムアップ分析から抽出された脅威シナリオを基に、サービス担当者と事業影響やセキュリティ対策方針についてディスカッションを実施します。
- ✓ サービス担当者と合意したセキュリティ対策方針を取りまとめ、脅威シナリオと合わせて報告書として提出いたします。

# 目次

コンセプト

# 目次

# 目次

## 教材

## 研修環境

# 【工場セキュリティ】 工場向けサイバーセキュリティ対策支援サービス一覧

|       |       |    |    |
|-------|-------|----|----|
| コンセプト | 設計・開発 | 運用 | 廃棄 |
|       |       |    |    |

工場のサイバーセキュリティに関する多様なニーズに応えられるソリューションをワンストップで提供

|        | リスク把握<br>対応方針策定                                     | 体制<br>構築                  | 対策<br>実行                                   | 検知                                            | 対応<br>復旧     | サプライチェーン<br>対策（SCM） |
|--------|-----------------------------------------------------|---------------------------|--------------------------------------------|-----------------------------------------------|--------------|---------------------|
| 文書     | 工場セキュリティ関連文書整備支援<br>・規定策定<br>・設備設計基準策定<br>・工場NW構成策定 | 工場CSIRT<br>・組織設計<br>・制度設計 | 対策実行支援<br>・システム化計画策定<br>・要件定義書策定<br>・RFP策定 | 工場CSIRT関連文章整備支援<br>・インシデント対応フロー策定<br>・マニュアル策定 |              | 委託先セキュリティ関連文書整備支援   |
| 現場執行部門 | 工場セキュリティ対策可視化サービス                                   | 工場CSIRT構築支援               | サイバー攻撃の監視・可視化ソリューション（SCADAfence）           | セキュリティ脅威分析支援サービス                              | セキュリティ事故対応支援 | 外部委託先の管理業務支援サービス    |
| 運営     |                                                     |                           |                                            |                                               | インシデント対応訓練支援 |                     |
|        | OTネットワーク・アセスメントサービス                                 |                           |                                            | SOCサービス                                       |              |                     |

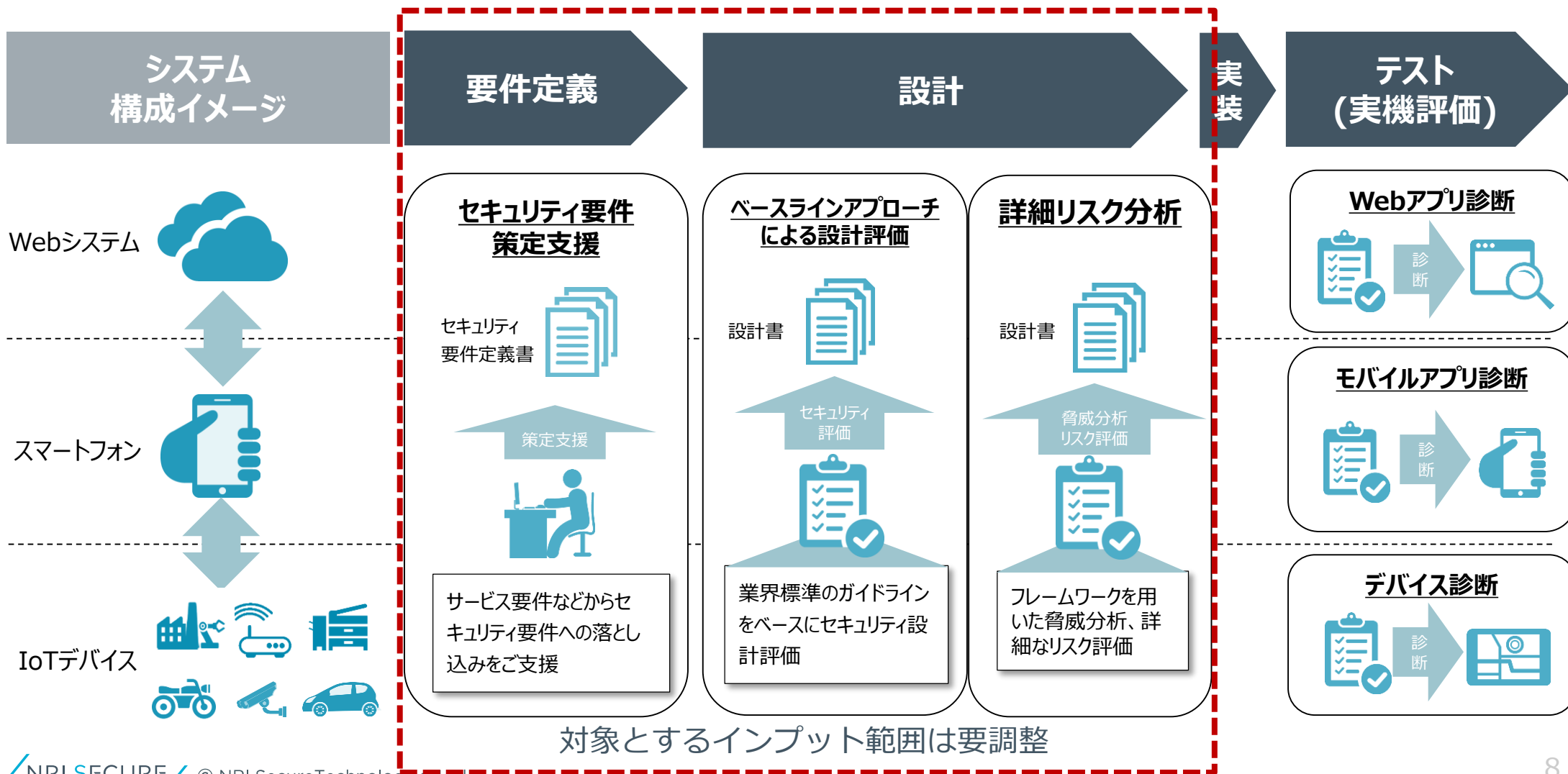
# 製品のライフサイクルに応じたセキュリティ 対策のご紹介

～ 設計・開発 ～

# 【脅威分析】 セキュリティ脅威分析による設計評価

| コンセプト | 設計・開発 | 運用 | 廃棄 |
|-------|-------|----|----|
|       |       |    |    |

- 上流工程の要件や設計情報をインプットとし、想定されるリスクシナリオを抽出します。
- リスクシナリオについて、ベースラインアプローチを用いて十分な対策がなされているか評価します。



# 【開発ガイドライン】 設計・開発ガイドライン



- 急速にネット化した自社製品をセキュアにするために、IoT機器/スマホアプリ/Webシステムを構築する際に求められるセキュリティ要件が定められたガイドラインおよびチェックリストをご提供いたします。  
(必要に応じてカスタマイズ可能)

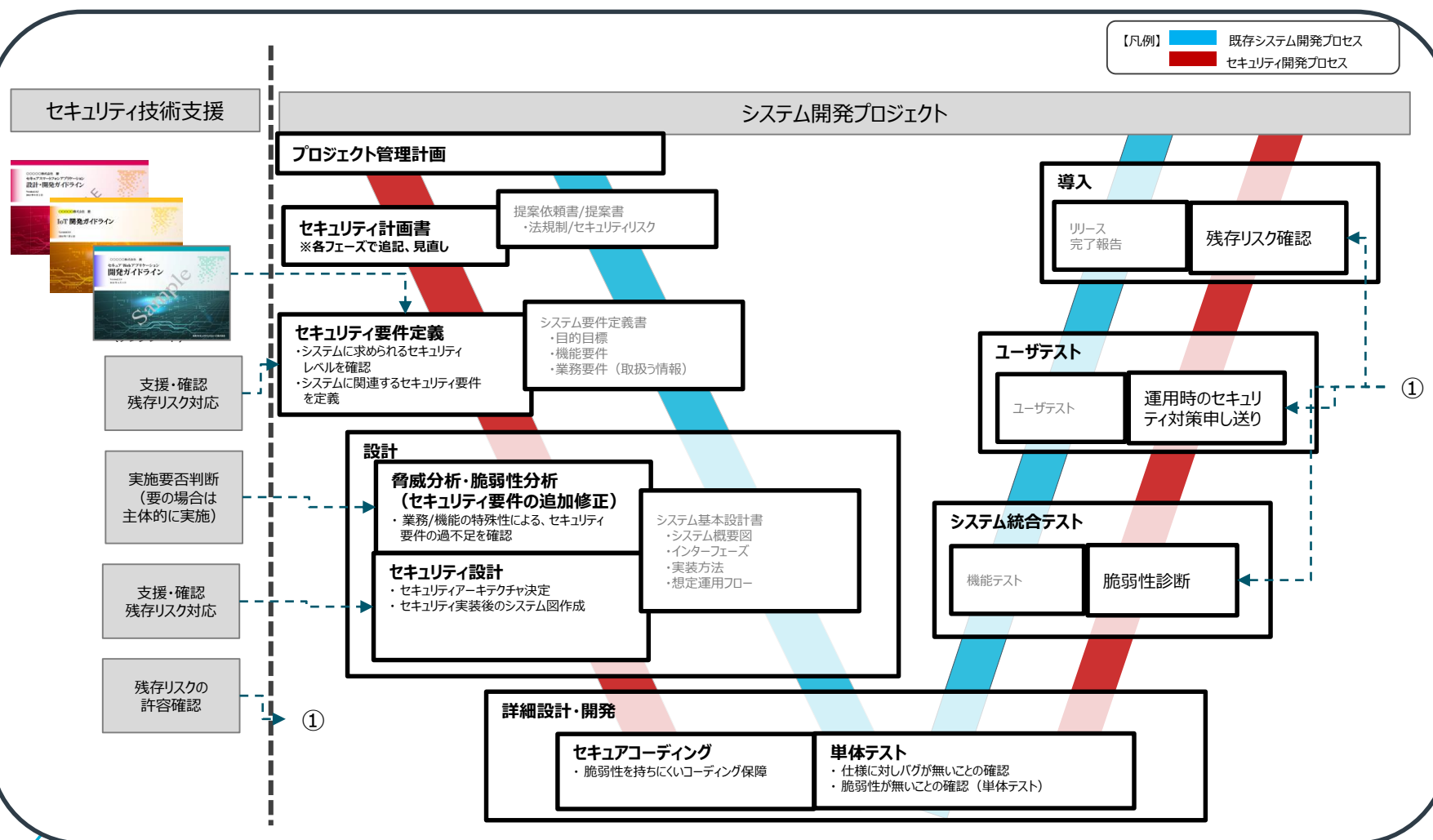


|                    | IoT機器                                                                                                                                                                                                                                                                                                                                                                                                                                      | スマホアプリ                                                                                                                                                                                               | Webシステム                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ベースとなる<br>業界ガイドライン | <ul style="list-style-type: none"> <li>• Cyber security guideline(UNECE WP29)</li> <li>• J3061(SAE)</li> <li>• Cybersecurity Best Practices for Modern Vehicles(NHTSA)</li> <li>• OWASP IoT Top 10</li> <li>• NISTIR 8200</li> <li>• Security capabilities supporting safety of the Internet of things(ITUT)</li> <li>• Secure by Design(NCSC)</li> <li>• Embedded Device Security Assurance(ISCI)</li> <li>などに加えて、NRIセキュアのノウハウ</li> </ul> | <ul style="list-style-type: none"> <li>• Androidアプリのセキュア設計・セキュアコーディングガイド (JSSEC)</li> <li>• The Mobile Application Security Verification Standard (OWASP)</li> <li>などに加えて、NRIセキュアのノウハウ</li> </ul>    | <ul style="list-style-type: none"> <li>• OWASP Top 10</li> <li>• PCI-DSS (PCI-SSC)</li> <li>などに加えて、NRIセキュアのノウハウ</li> </ul> <p>また、API実装については、下記をベースラインに補足資料を用意可能。</p> <ul style="list-style-type: none"> <li>• NIST SP800(NIST)/サイバーセキュリティフレームワーク</li> <li>• 米国SANS Critical Security Controls</li> <li>• OpenBank API 1.3</li> <li>• OpenID FinancialAPI WG</li> </ul> |
| 項目 (抜粋)            | <ul style="list-style-type: none"> <li>• セキュアハードウェアモジュールの利用</li> <li>• 耐タンパ性の確保</li> <li>• 重要情報の暗号化送信</li> <li>• 暗号化アルゴリズム</li> <li>• 証明書の妥当性</li> <li>• 情報フローに対する認可の適用</li> <li>• アプリケーションの分割</li> <li>• セキュリティ機能の分離</li> <li>• DoS攻撃からの保護</li> <li>• プロトコルファジングからの保護</li> </ul>                                                                                                                                                          | <ul style="list-style-type: none"> <li>• 外部保存領域への保存</li> <li>• 保存時の暗号化処理</li> <li>• SSL/TLS通信時の証明書の検証</li> <li>• 過剰なアクセス権の付与</li> <li>• SMSによる制御</li> <li>• 難読化処理</li> <li>• 強制アップデートの仕組み</li> </ul> | <ul style="list-style-type: none"> <li>• Webサーバ/アプリケーションサーバの脆弱性</li> <li>• パスワード変更機能の妥当性</li> <li>• OAuth/OpenIDConnect等認証基盤の妥当性</li> <li>• 制限されたデータへのアクセス許容</li> <li>• セッションIDの強度</li> <li>• クロスサイトスクリプティングへの対策</li> <li>• SQLインジェクションへの対策</li> <li>• その他インジェクションへの対策</li> </ul>                                                                                      |

# 【自社仕様に応じた開発・設計】 セキュリティ設計・開発プロセス整備

| コンセプト | 設計・開発 | 運用 | 廃棄 |
|-------|-------|----|----|
|       |       |    |    |

- セキュリティ要件が定められたガイドライン・チェックリストがあっても、その活用をルールとして定義しプロセスに組み込まなければ、製品にセキュリティ機能が正しく実装されない恐れがあります。
- セキュリティも品質の一つと捉え、貴社にて運用中の開発プロセス/品質管理文書等と整合性をとった上、セキュリティ開発プロセスを整備します。



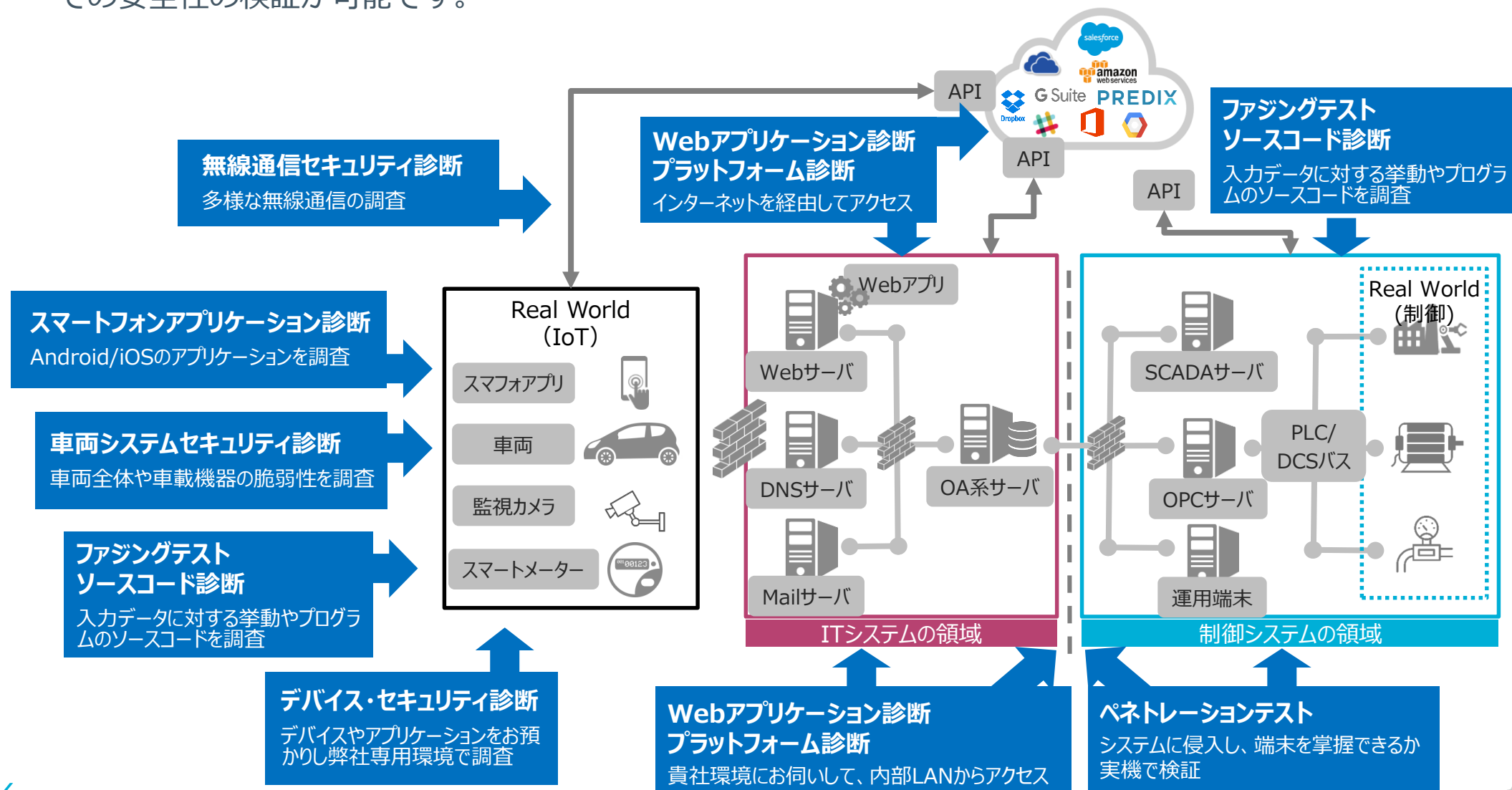
アウトプット



- セキュリティ開発プロセス全体像
- セキュリティ要件定義プロセス定義書
- セキュリティ設計プロセス定義書
- 脆弱性管理プロセス

...

- 各種デバイスの診断に加え、デバイスを含むシステムの系全体に対し、プラットフォーム診断やWebアプリケーション診断など、NRIセキュアの各種診断サービスやノウハウを組み合わせ、想定される脅威に対する安全性の検証が可能です。



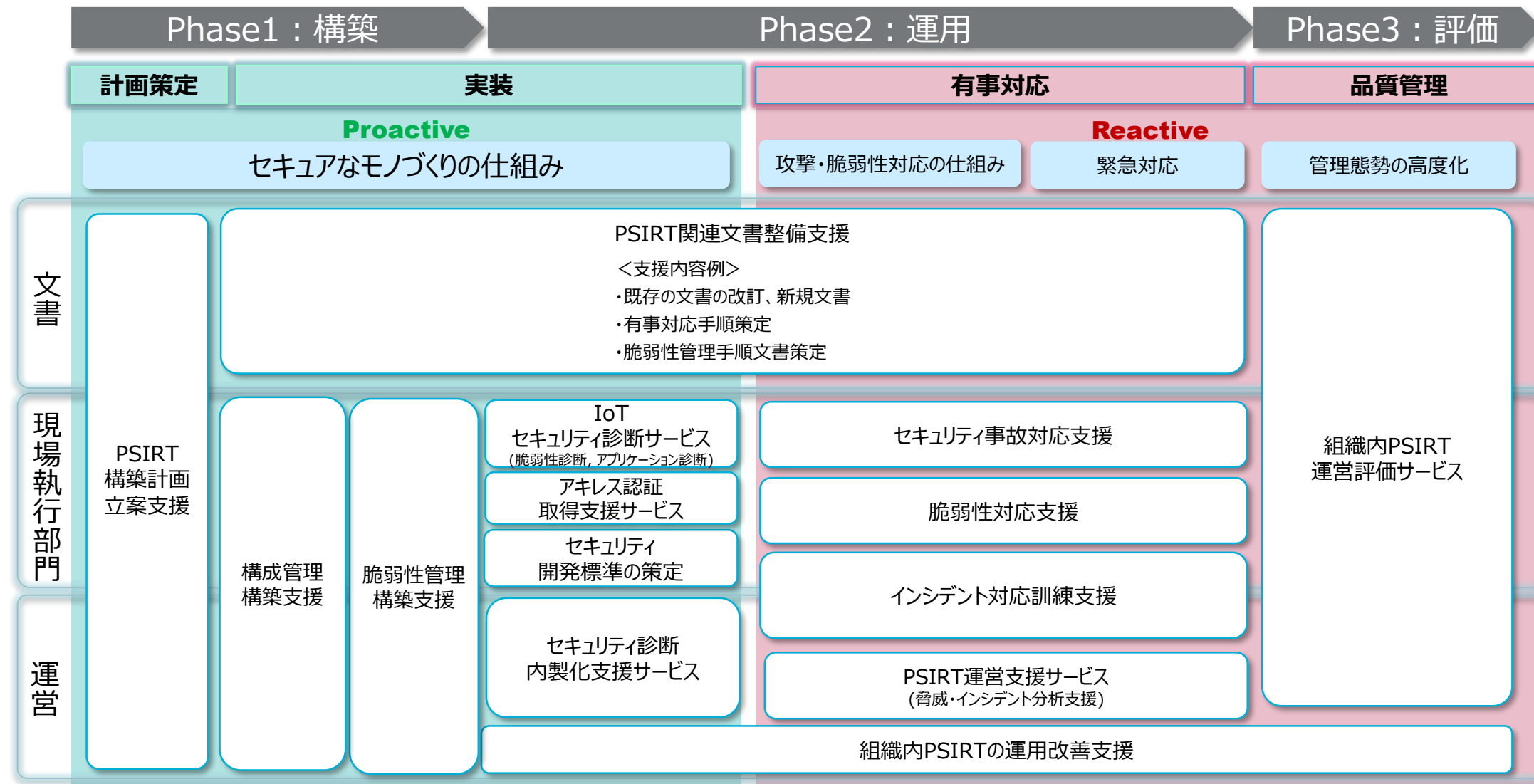
# 製品のライフサイクルに応じたセキュリティ対策のご紹介

～ 運用 ～

# 【製品管理（PSIRT）】 組織内PSIRT向け支援サービス一覧



PSIRTに関する多様なニーズに応えられるソリューションをワンストップで提供





[www.nri-secure.co.jp](http://www.nri-secure.co.jp)