第4回IT Forum「地方自治体組織における危機管理」
ビッグデータ時代の情報セキュリティ戦略

事故発生が常識化する時代の、セキュアなシステム企画・構築・運用

2013.11.15

元情報セキュリティ政策会議 基本計画検討委員会委員
経済産業省　産業構造審議会情報経済分科会
人材育成ワーキンググループ委員長
AITコンサルティング（株）代表取締役
有賀　貞一

「事故前提社会」

- 事故前提社会というキーワードが登場したのは、2009年2月政府発表「第2次情報セキュリティ基本計画」
  - 2006～2008年までの3カ年の中期計画である「第1次情報セキュリティ基本計画」を受けて、2009～2011年までの3カ年を対象として計画
  - 情報セキュリティ先進国としての日本の新たな推進計画
  - 「事故前提社会」＝セキュリティ管理の新たなキーワード
- 第１次情報セキュリティ基本計画（2006年2月）は、「無謬性」を追求する姿勢
  - 事前に起こりうることを完全に想定し、対策・方策を立てていることが前提
  - 2006～2008年までの3カ年の中期計画：
    「重要インフラでの障害発生ゼロを目指す」という目標設定
- 2006年から2009年への変化
  - 想定を超える事象（インシデント）が発生、対処しきれず
  - 事故が起こり得ることを前提として、事故時の対応力がより重視される時代へと変化
- 「第2次基本計画」のキーワードは「事故前提社会への対応力強化」に決着
  - 事前に事故がおきないよう想定し対策を立てることは当然だが、
  - 一定の確率で人為的ミス（バグ）は潜入
  - 費用対効果を考慮するとレアケースまで完璧には潰し切れない
  - 運用ミスも発生
  - さらに、想定外の事象が多発（サイバー攻撃の多様化）

国民を守る情報セキュリティ戦略
2010年5月11日情報セキュリティ政策会議で制定

- 情報セキュリティを巡る環境の変化に的確に対応するため、「第2次情報セキュリティ基本計画」に基づく官民の各主体による取組を継続しつつ、新たな環境変化に対応した政府の取組
- 「第2次情報セキュリティ基本計画」を包含する、4年間（2010 年度から 2013 年度）を対象とした包括的な戦略
- 本戦略に基づき、毎年度の年度計画である「セキュア・ジャパン20XX」を推進
- 基本方針

  ① サイバー攻撃事態の発生を念頭に置いた政策の強化及び対処体制の整備

  ② 新たな環境変化に対応した情報セキュリティ政策の確立

  ③ 受動的な情報セキュリティ対策から能動的な情報セキュリティ対策へ

  - 問題の根本的な解決をもたらす情報セキュリティ対策の検討等に戦略的に取り組むとともに、PDCAサイクルを活用するなど、受動的な情報セキュリティ対策から、各主体が能動的に取組を進められる体制の実現を目指す

産業構造審議会情報経済分科会

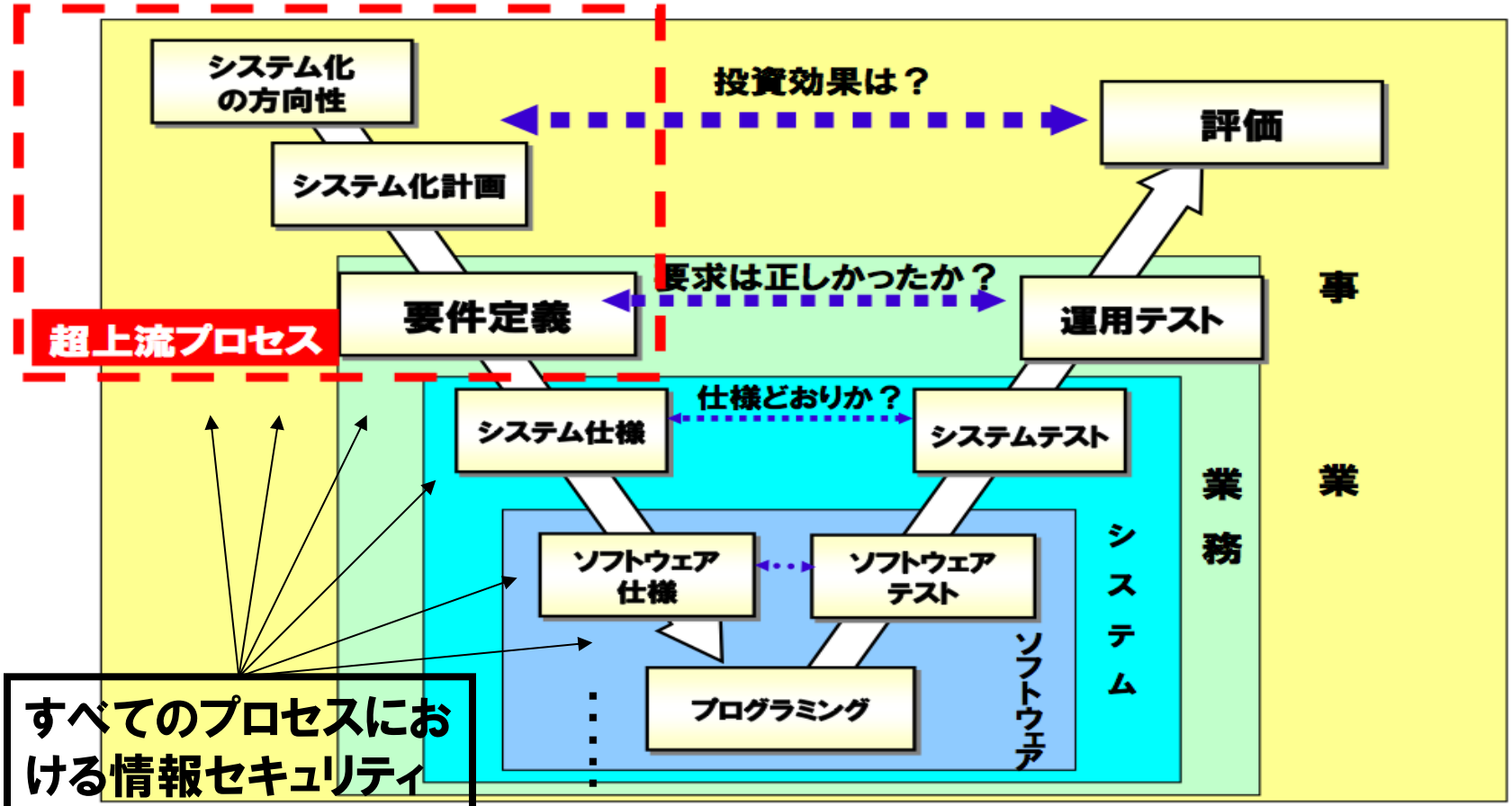
人材育成WG報告書
－次世代高度IT人材像、情報セキュリティ人材、今後の階層別の人材育成－

2012.09.14　から抜粋

- 情報セキュリティに適切に対処するには、もはや対症療法的な対策にとどまらず、情報システム、ひいては業務設計、ビジネスモデル設計の段階からビルトイン型の対策が設計できるかどうかが重要であることから、情報セキュリティの専門的なエンジニアを育てるだけではなく、情報システムに関わるそれぞれのエンジニアがセキュリティの要素を備えることが求められている。さらに、ビジネスやシステムのライフサイクル上全ての段階で運用面も含めて情報セキュリティを考慮に入れた対応が可能な総合的な視点を持つ人材が求められる。

SLCP全般にわたるセキュリティ確保
「セキュアSLCP」の提言

- 重要なポイントは、すべてのプロセス、特に「いわゆる超上流」プロセスからの情報セキュリティ配慮



共通フレーム2007　IPA資料より引用

SLCP全般にわたるセキュリティ確保
セキュアSLCP

- これまでの事後的・対症療法的対応策から、システム構築全体プロセスにおいて、情報セキュリティを考慮に入れた対応を実施
- トータルな情報セキュリティ確保が必須
  - SIer、ITコンサルティング、ソフトウェア開発会社、データセンター、クラウド業者、運用支援会社等々の機能を統合
  - モバイル端末の普及、あらゆるもののインターネット化の進展など、新しい環境変化への配慮
  - 具体的な基準、レベルまで落とし込みPDCAサイクルをまわす
- 情報セキュリティ専門会社の単独・独自な対応は限界
  - 体力面、機能面、多様性、人材面、場合によっては技術面で不足
  - 情報セキュリティ専門会社は、トータルな情報セキュリティ確保のためのPM（プロジェクト・マネジャー）機能へ変化を要請される
- 情報セキュリティ専門家の育成は必須であるが、既存IT技術者全般への情報セキュリティ専門教育も必要

SLCP全般にわたるセキュリティ確保
セキュアSLCP

- 企画プロセス：システム化の構想の立案、システム化計画の立案など
  - システム企画段階において、確保すべきセキュリティレベルや、防衛すべき範囲を設定
- 要件定義プロセス：実現する仕組みに係わる要件を定義
  - この段階においては、対象情報そのものの重要性判断や取り扱い基準（例えばアクセス制御）を設定
- 開発プロセス：システムの開発を行うアクティビティ
  - セキュアなプログラム作りに対する配慮、脆弱性の除去やセキュリティ確保の観点からのテスト
- 官公庁・自治体における課題
  - セキュアSLCPという概念そのものの欠如
  - 上流工程関連セキュリティ技術者の不足
  - 情報セキュリティに対する組織的理解不足

SLCP全般にわたるセキュリティ確保
セキュアSLCP

- 運用プロセス：利用者の実環境でコンピュータシステムを運用するアクティビティ
  - 日々の運用における情報セキュリティ観点からの運用体制整備や、運用方法の組込み（例えば既存システム運用方式への、SOC機能やセキュリティログ管理機能の組み込み）
- 保守プロセス：システムの現状を、維持、変更、管理するアクティビティ
  - 稼働状況やトラブル記録からの情報セキュリティ強化策の実施や情報セキュリティ人材育成強化

→官公庁・自治体においては、運用環境特性の考慮が必須

- 情シ運用体制の未成熟
- 実運用者と運用管理者の所属主体が分離していることが多い
- 情報セキュリティ関連知識のある運用関係者不足

PCI DSSにみる
具体的なセキュリティコントロール

- PDCAを回す事例
- PCI DSSでは他の基準では「あえて曖昧にしている」数値基準を具体的に設定（PCI DSSより引用抜粋）
- 過去の事故事例も基にして作成されたセキュリティ基準でもある

PCI 要件	要件概要	数値基準
1.1.6	ファイアウォールおよびルータールールセットレビュ	6ケ月ごと
3.1	保存されたカード会員データに関するレビュ	4半期ごと
6.1	重要なセキュリティパッチの対応	1ヶ月以内
6.6	一般公開されているWeb アプリケーションのセキュリティ診断	1年に回以上他
8.5.5	非アクティブなユーザアカウントの削除または無効化	90日に1回以上
8.5.10/14	パスワード長（英数混同）とログイン失敗の際のロックアウト	7文字以上／6回
8.5.9	パスワードの変更間隔	90日に1回以上
9.9.1	定期的なメディアの在庫調査	1年に1回以上
10.6	すべてのシステムコンポーネントのログのレビュ	1日に1回以上
11.1	無線アナライザ使用による無線装置の識別	4半期ごと
11.2	外部および内部のネットワーク脆弱性スキャン	4半期に1回以上他
11.3	外部および内部のペネトレーションテスト	1年に1回以上他
11.5	ファイル完全性ソフトウェアによる重要ファイルの比較	1週間に1回以上
12.1.	脅威と脆弱性を特定したリスク評価、ポリシーの見直し等	1年に1回以上

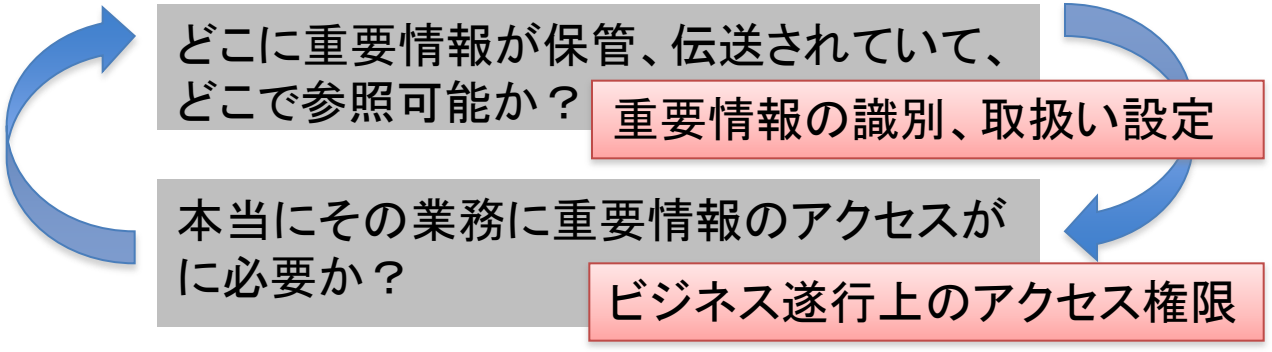
- PCI DSS：クレジットカード業界のセキュリティ基準
  Payment Card Industry Data Security Standards

重要情報の識別と、取扱い方針設定

- 超上流プロセスにおける重要情報の識別と取扱方針設定
- 何が“重要情報”か？
  - 顧客･取引先情報／受注情報／クレジットカード情報／製品設計情報等々、どのような業務プロセスにおいて、どれほどの情報セキュリティレベルを要求するかを決定
  - 管理者の全てのアクションログのような、業務とは関係ない情報でも重要性の高いものもある
- ”保管、処理、伝送されるフローの把握は？
  - DB、媒体のみならず伝送経路や処理の仕組み上からの要求レベルの設定要
- 誰がどこまで“アクセス”できるようになっているのか？
  - 組織階層、組織機能、職能、委託先等で複雑かつクロスに設定が必要
  - アクセス権限付与には具体的なビジネス遂行上の責任･権限定義が必要
- 複雑さゆえの自己矛盾や漏れの排除
- 官公庁･自治体における課題
  - 重要情報を決めきれない
  - アクセス権限付与基準が決めきれない

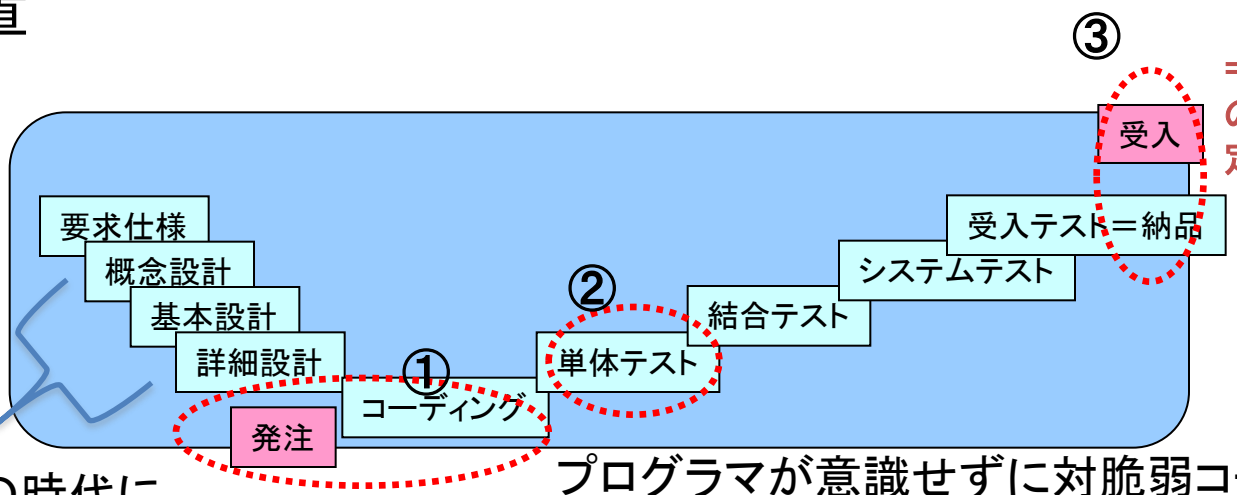
アクセス権限の、
具体的なビジネス遂行上からの定義と実現

- 漏洩原因の数%は身近な隣人！
  - 外注データ入力作業委託先から大量情報漏えい
  - 管理者機能付与されたものが重要情報窃盗
  - 長期にわたるアクセス権限見直しなし状態からの不正アクセス可能性発生
- どの業務のどのような担当者にどこまでのアクセス権が必要か？
  - ビジネス機能遂行上の観点からアクセス権限の付与
  - それを可能にするためのデーベース設計の見直し、アクセス権限システムの見直しも発生



セキュアなプログラム作りに対する配慮

- 要求仕様段階からの対脆弱性レベル設定
- 受入段階の“脆弱性診断③”は定着しつつある
- 発注段階からの開発業者レベル認定：①対脆弱コード記述レベルの高低をあらかじめ把握、必要要求レベルに応じられる業者に発注、必要ならさらに③を実施
- 脆弱性をバグと捉え対応する単体テスト段階からの取組み②も処置



セキュア設計をあたりまえの時代に

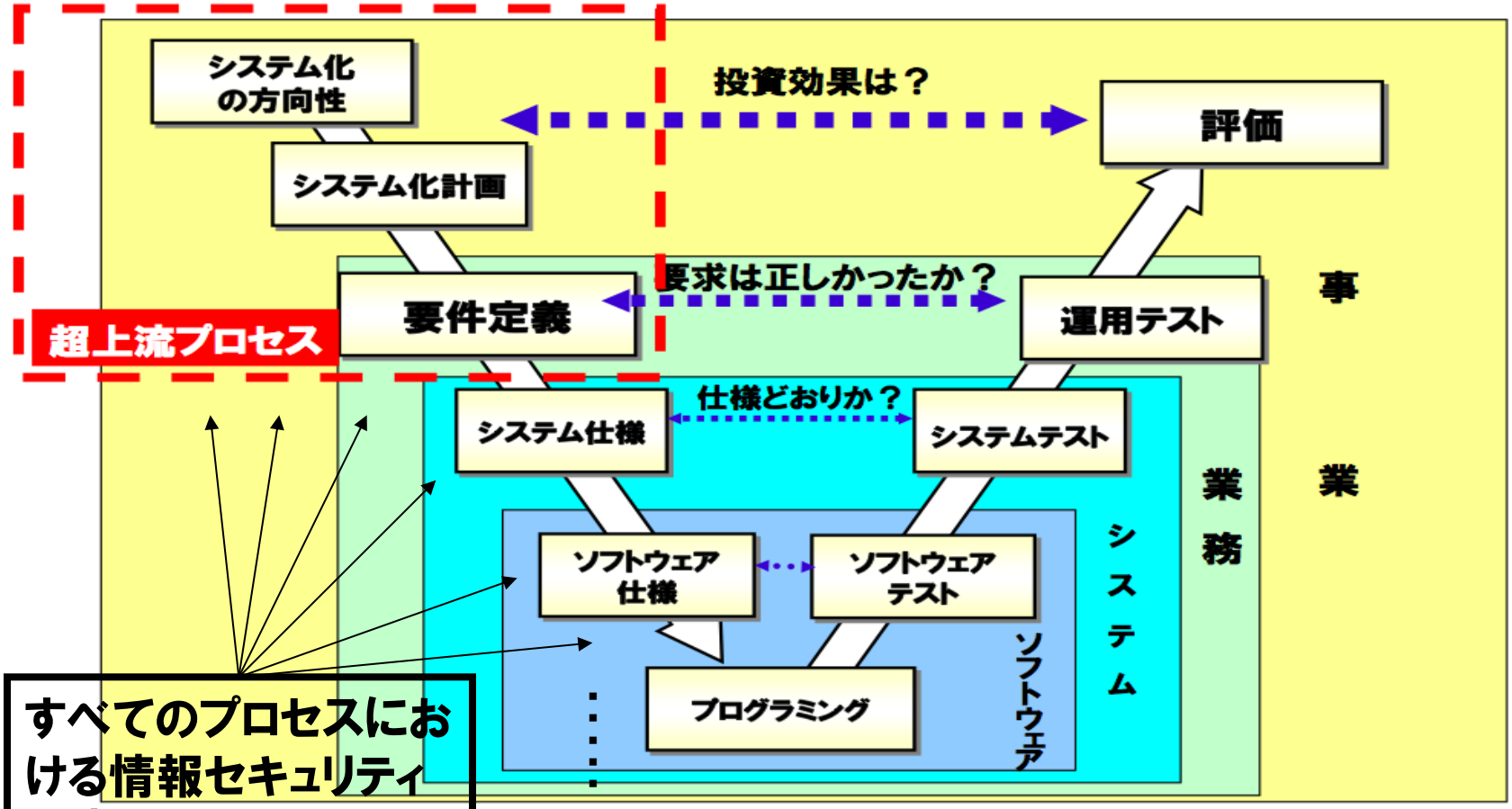
プログラマが意識せずに対脆弱コードを記述・単体テスト段階からのバグ排除と同等作業へ

セキュリティ運用を組み込んだ システム運営のあり方

- 日々の運用における、情報セキュリティ観点からの運用体制整備や、運用方法の組込み
- 事故前提社会＝今日1日、事故（インシデント）がなかったことを確認して、日次処理を実施することが必須
- 既存システム運用と、SOC機能の連携を可能とする組織の形成
- システム運用ログとインシデント対応ログの取得期間、分析方法、分析組織の連携もしくは統合
  - “何もなかったこと”の確認→最低1日1回はログで確認
- 重要情報を扱う“システム設定情報”の完全性を定期的に確認

SLCP全般にわたるセキュリティ確保
「セキュアSLCP」の提言　（再掲）

- 重要なポイントは、すべてのプロセス、特に「いわゆる超上流」プロセスからの情報セキュリティ配慮



共通フレーム2007　IPA資料より引用

官公庁・自治体における課題

- セキュアSLCPに関する課題
  - セキュアSLCPという概念そのものの欠如、結果予算付けの困難さ
  - 上流工程関連セキュリティ技術者の不足
  - 情報セキュリティに対する組織的理解不足
  - セキュリティ関連人材の不足
- 重要情報の識別と取扱方針、アクセス権限に関する課題
  - 重要情報を決めきれない
  - アクセス権限付与基準が決めきれない
- 官公庁・自治体においては、運用環境特性の考慮が必須
  - 情シ運用体制の未成熟
  - 実運用者と運用管理者の所属主体が分離していることが多い
  - 情報セキュリティ関連知識のある運用関係者不足

→・即効性ある解決策はない

・NISCの動き等を活用しながら、関係者の理解を促進する、地道な活動が必要

・人材育成、確保が肝要

終

ありがとうございました