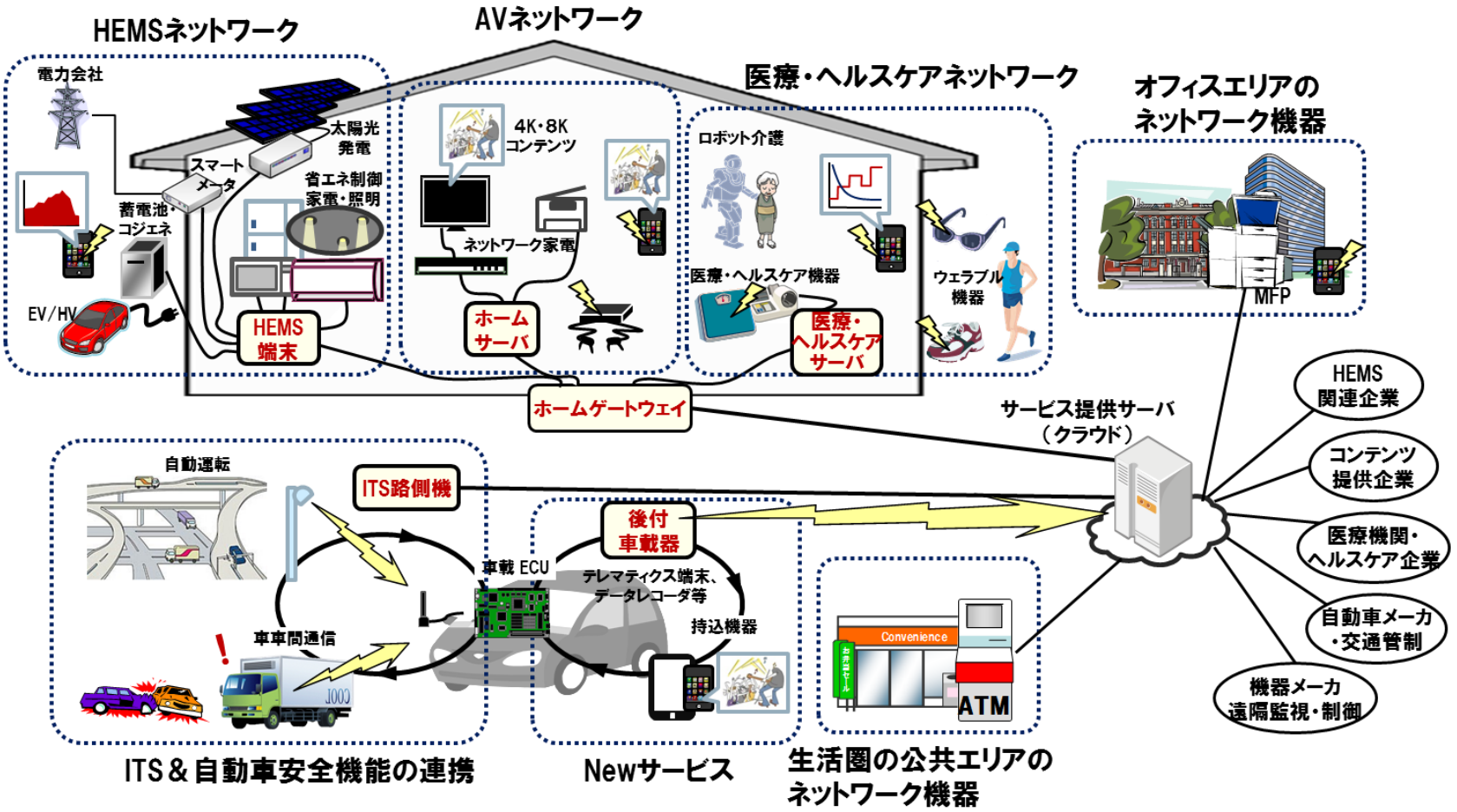
セーフティ＆セキュリティ設計してますか？
実態調査結果！

ET2015　2015/11/18～20

技術本部　ソフトウェア高信頼化センター
西尾　桂子

IoT時代：様々なモノやサービスがつながる世界



出典：一般社団法人重要生活機器連携セキュリティ協議会 提言

接続先は信頼できる？
（信頼性に関する設計要件は自分が求めているものと合致しているか？）

設計要件が異なる際に想定されるリスク

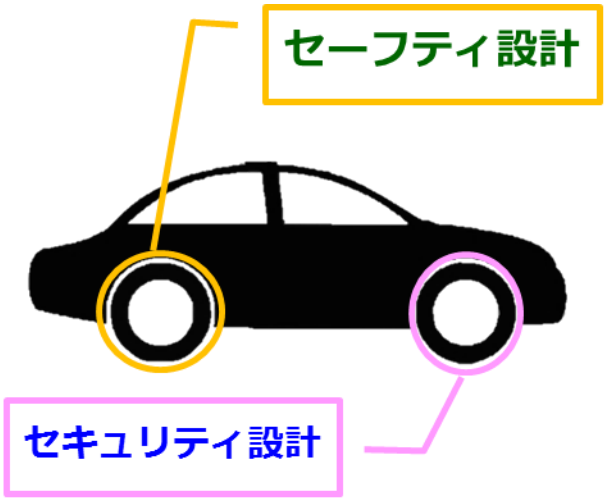
- 持ち主以外からの接続による車の盗難
- 車を制御・操作中のスマホのハングアップにより、制御・操作が効かなくなり、重大な事故が発生
- 脆弱性がある側の製品や機器への不正アクセスにより、相手側の製品や機器に保存されている情報が盗難

IoT時代の安全と安心への危惧

接続先の信頼性をどう確認するのか？

【IoT時代の安全・安心への危惧を払拭するには】
製品やサービスをつなげるための開発を
行う際に互いの信頼性を確認することが重要

特にセーフティ設計・セキュリティ設計



セーフティ、セキュリティは
車の両輪

その把握のためには、双方の

（1）セーフティ・セキュリティ設計の確実な実施

（2）その設計実施状況の見える化

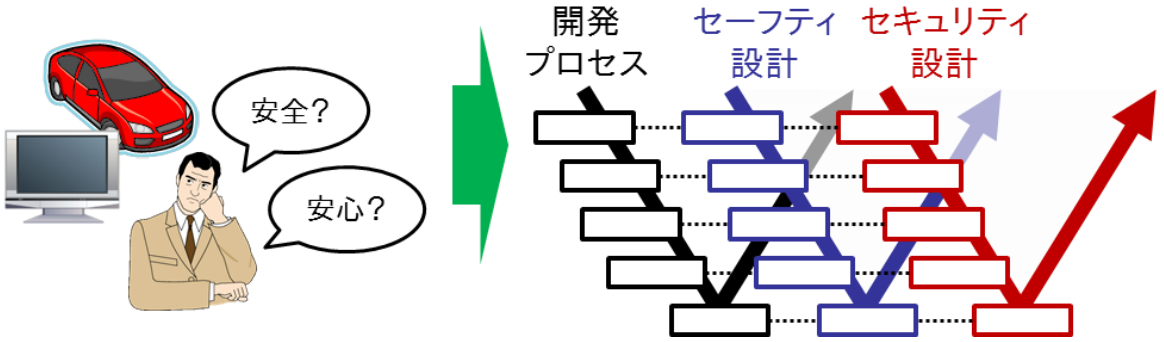
が必要不可欠に

「セーフティ設計」「セキュリティ設計」「見える化」

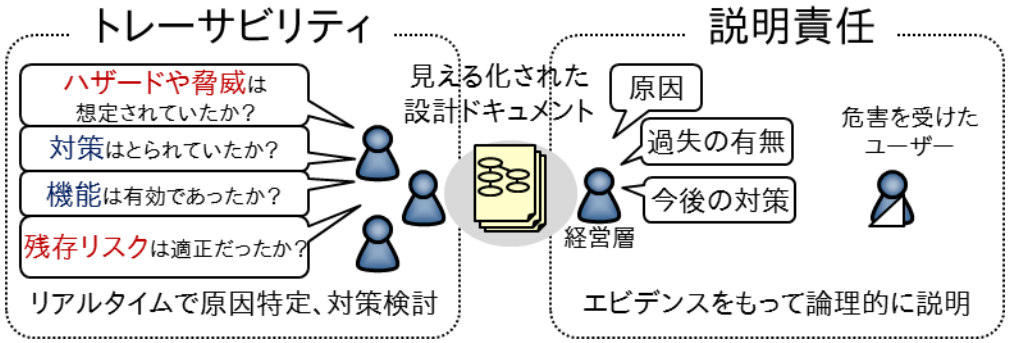
◆上流の段階でリスク分析を実施し、リスクを低減した設計を行う

設計がまとまってからセーフティ／セキュリティ対応するのではなく・・・

開発プロセスの上流から組み入れる



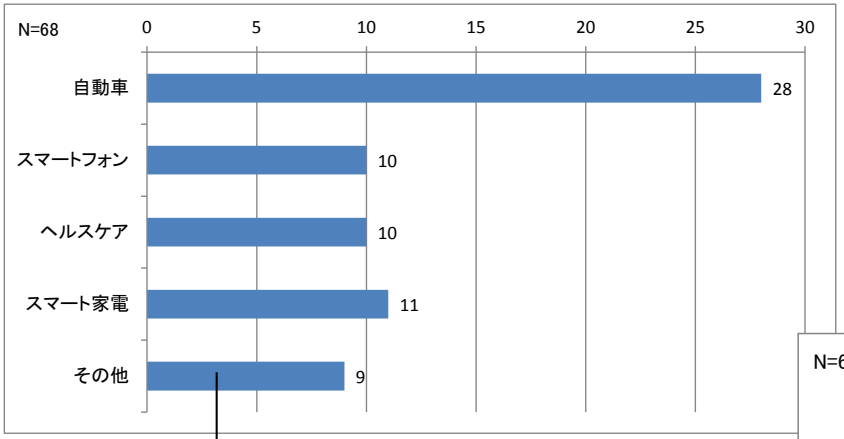
◆設計の品質をエビデンス（証拠）に基づき第三者でも容易に理解できる表記で論理的に説明する



セーフティ設計・セキュリティ設計に関する実態調査結果

「セーフティ設計・セキュリティ設計に関する実態調査結果」（平成27年9月10日発行）

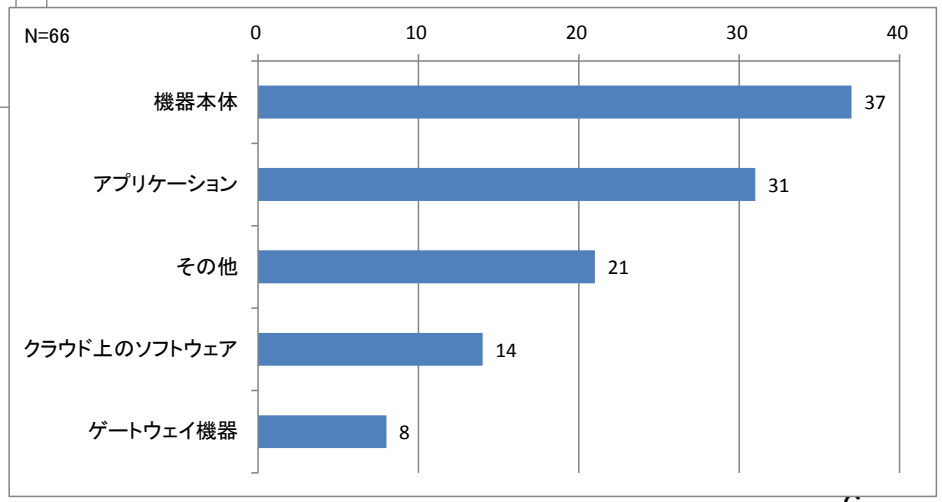
- 対象：自動車、スマートフォン、ヘルスケア、スマート家電の4分野
- サンプル数：３２０社　調査期間：２０１５年２月～４月　有効回答：68組織



通信制御・ユーザーインターフェースAPI、マイコンドライバー、ミドルウェアなど、セキュリティ部分（但し、コピー防止、改変防止等）、FA機器、計測・測定装置、自社製品の組込みシステム開発～製造(上記選択肢分野含む)、通信インフラ制御(基地局、Node、サーバー系)、無線/通信機器、制御盤

分野別有効回答数

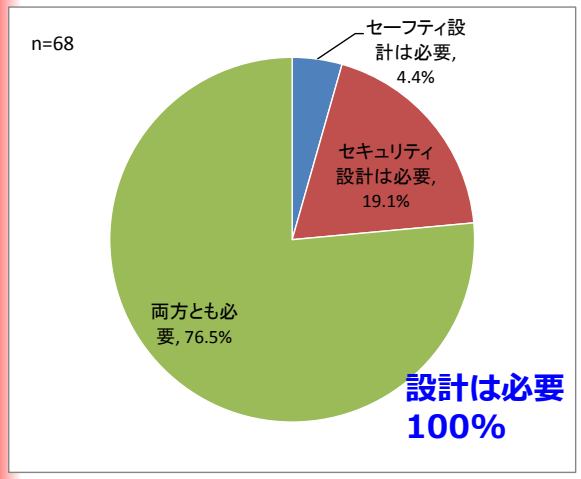
開発している製品・ソフトウェア（複数回答）



【実態調査アンケート結果】

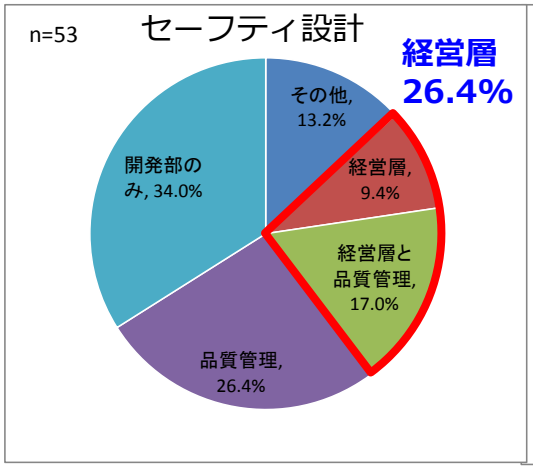
経営層の関与が少ない

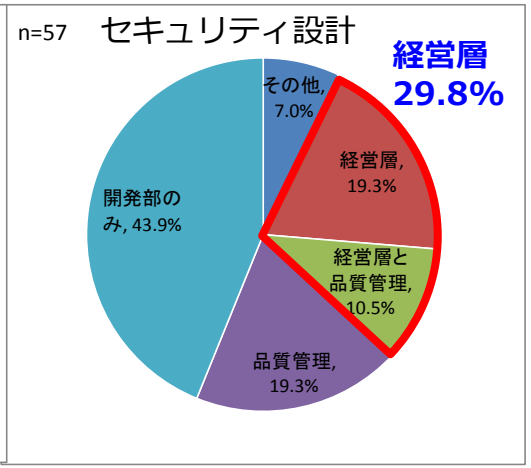
Q:セーフティ設計・セキュリティ設計の必要性



しかし

Q:設計上の判断に、経営層や品質保証部門の責任者が関わることはありますか？





経営層が関与していると回答した組織は、開発部門のみで判断していると言う回答に比べて少ない

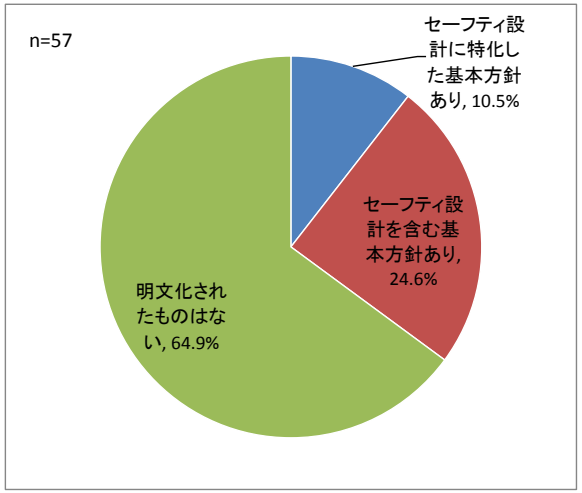
事故やインシデントが発生すると、損害賠償や企業の信用失墜・リコールなど、経営リスクに発展

セーフティ設計・セキュリティ設計上の判断には、経営層の関与が必要

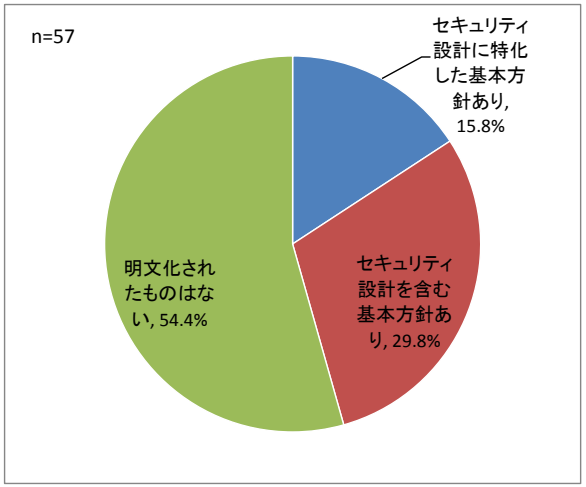
【実態調査アンケート結果】

設計の基本方針が明文化されていない

セーフティ設計の基本方針（明文化なし：64%）



セキュリティ設計の基本方針（明文化なし：54%）



経営層関与	セーフティ基本方針		セキュリティ基本方針	
	なし	あり	なし	あり
あり	16.2%	40.0%	19.4%	42.3%
なし	83.8%	60.0%	80.6%	57.7%

基本方針がないのに経営層の関与もなし

設計ルール	セーフティ基本方針		セキュリティ基本方針	
	なし	あり	なし	あり
あり	27.0%	94.7%	9.7%	92.0%
なし	73.0%	5.3%	90.3%	8.0%

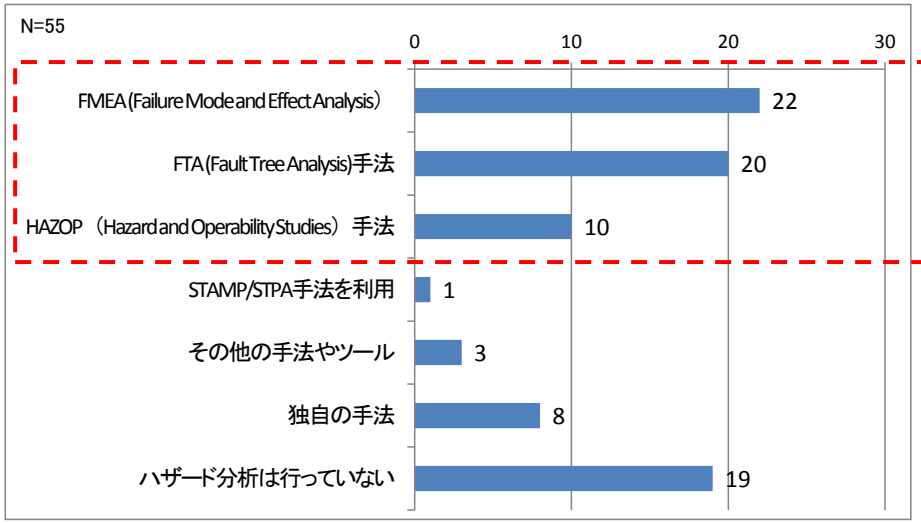
基本方針がある組織はほとんど設計ルールあり
基本方針がない組織はほとんど設計ルールなし

半数以上の企業では基本方針が設けられていないが、経営層の関与もなく、開発現場の判断に任せられている

【実態調査アンケート結果】

現場で行っているセーフティへの対応

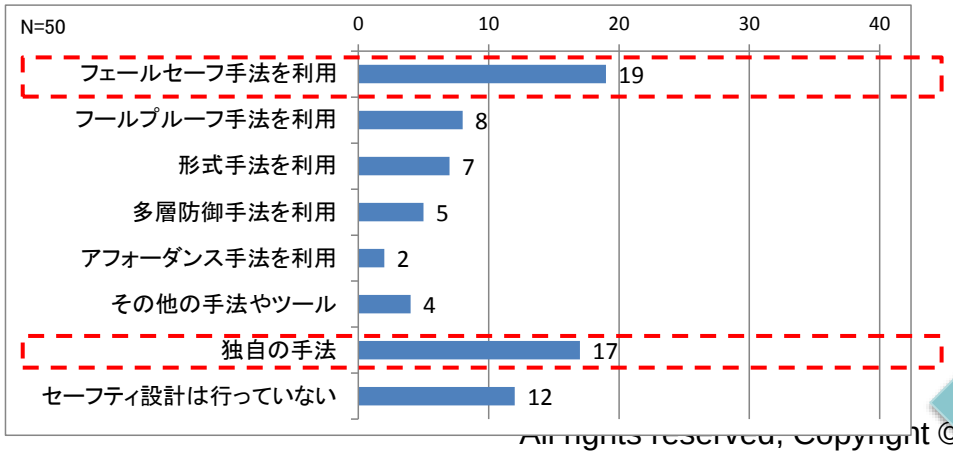
Q:ハザード分析について、手法やツールを利用していますか?(複数回答)



セーフティ分析
3大手法

ハザード分析をしていないプロダクトも多い

Q:ハザードに対するセーフティ設計・評価について、手法やツールを利用していますか?(複数回答)



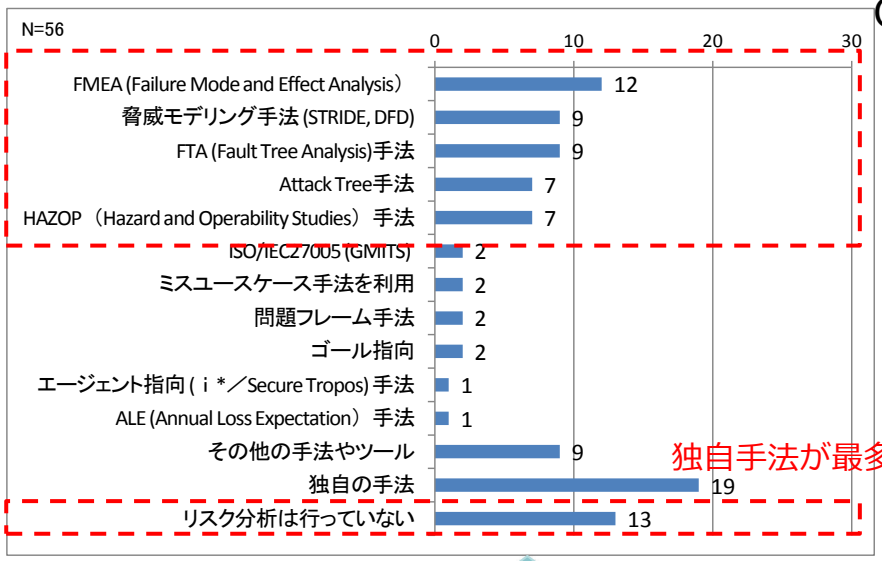
フェールセーフ手法が1強

独自手法が多い

セーフティ設計をしていないプロダクトも多い

【実態調査アンケート結果】

現場で行っているセキュリティへの対応



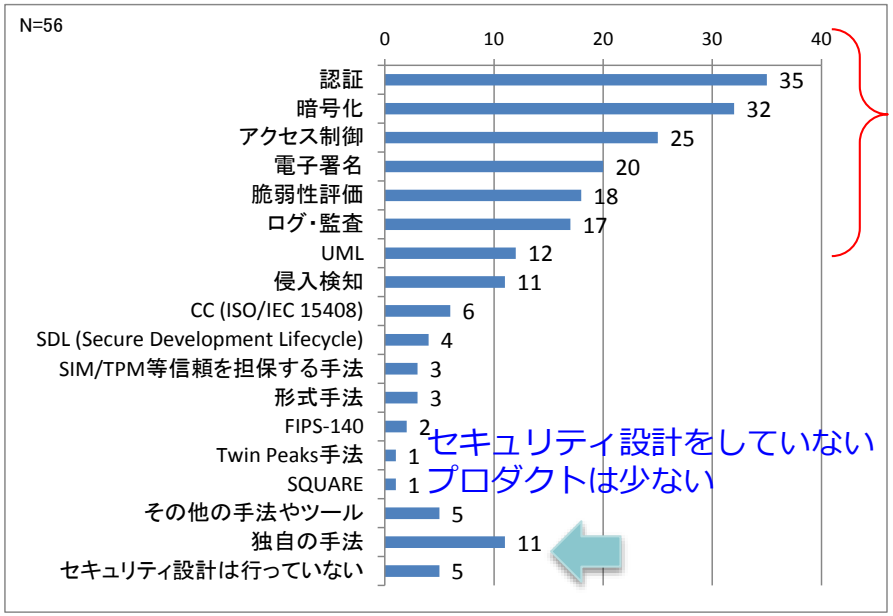
Q：セキュリティ上のリスク分析について、手法やツールを利用していますか？（複数回答）

セキュリティ分析
5大手法

独自手法が最多

リスク分析をしていないプロダクトも多い

セキュリティ対策は様々な手法が使われている



セキュリティ設計をしていないプロダクトは少ない

Q：リスクに対するセキュリティ設計・評価について、手法やツールを利用していますか？（複数回答）

分析は行っていないが設計は行っている
→手法やツールを利用することが通常の開発に組み込まれている？
→その手法やツールが本当に有効か確認しているか？

セーフティ・セキュリティ設計普及と見える化の取り組み

- **WG名：** サプライチェーンにおける品質の見える化WG
- **期間：** 2014年9月～2015年５月
- **目的：**
  設計品質の見える化のためのセーフティとセキュリティ設計の取組みとハザード・脅威事例を含めて分かり易く解説するガイドブックの作成とそのプロモーション
- **主査：** 情報セキュリティ大学院大学 後藤教授
- **メンバー：** セーフティ or セキュリティの有識者
- **成果物：** ガイドブック

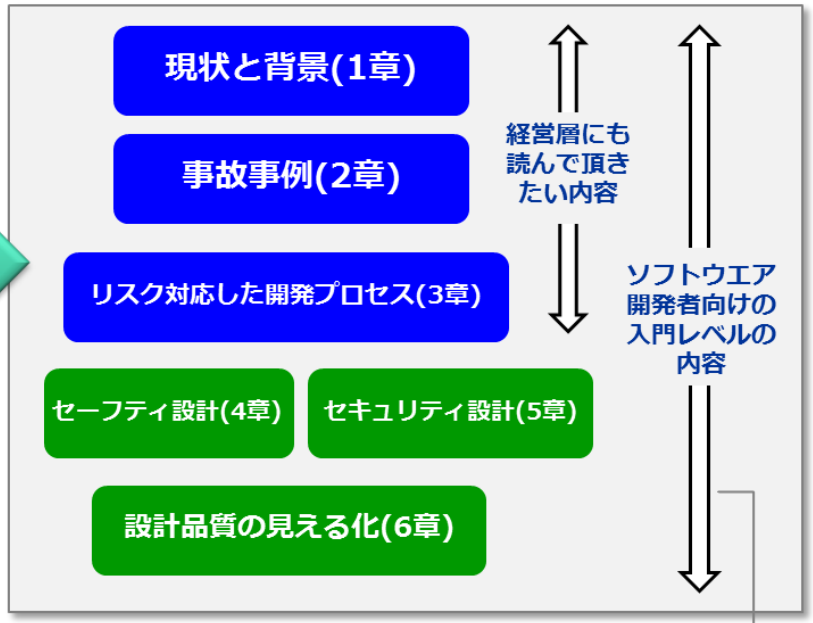
WGで見えてきた課題

- 標準的なセキュリティ設計手法（分析・対策）が確立していない
  （公開されている手法はあるが、独自手法が主流）

- セーフティ設計とセキュリティ設計を統合したプロセスは確立されていない
  （同時認証に対応するＳａｆＳｅｃ等はあるが…）

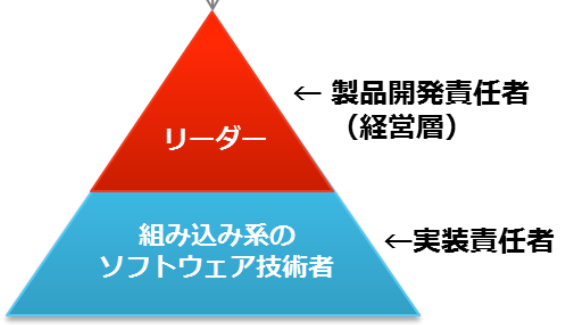
- 業界やセーフティとセキュリティでも用語の意味・使い方が違う

本ガイドブックの構成と対象読者



主な対象読者

「セーフティ設計・セキュリティ設計」は、製品開発の根幹に係り、つながる世界では更に重要になる。その重要性を認識してもらうために、本ガイドブックの読者は**組込み系のソフトウェア技術者**や、製品開発の責任を担う**経営層**を主な対象とする。



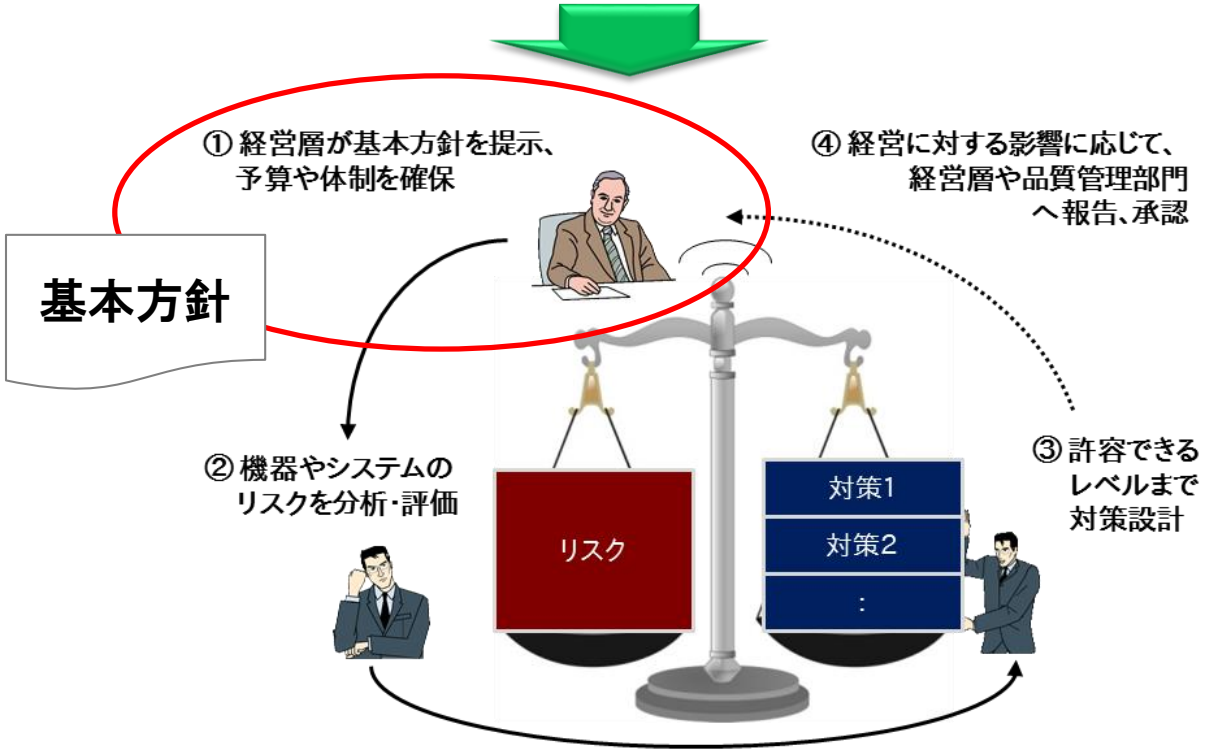
ガイドブックの記載内容

今後のIoT時代の製品開発において重要となる設計時の考慮事項を記載

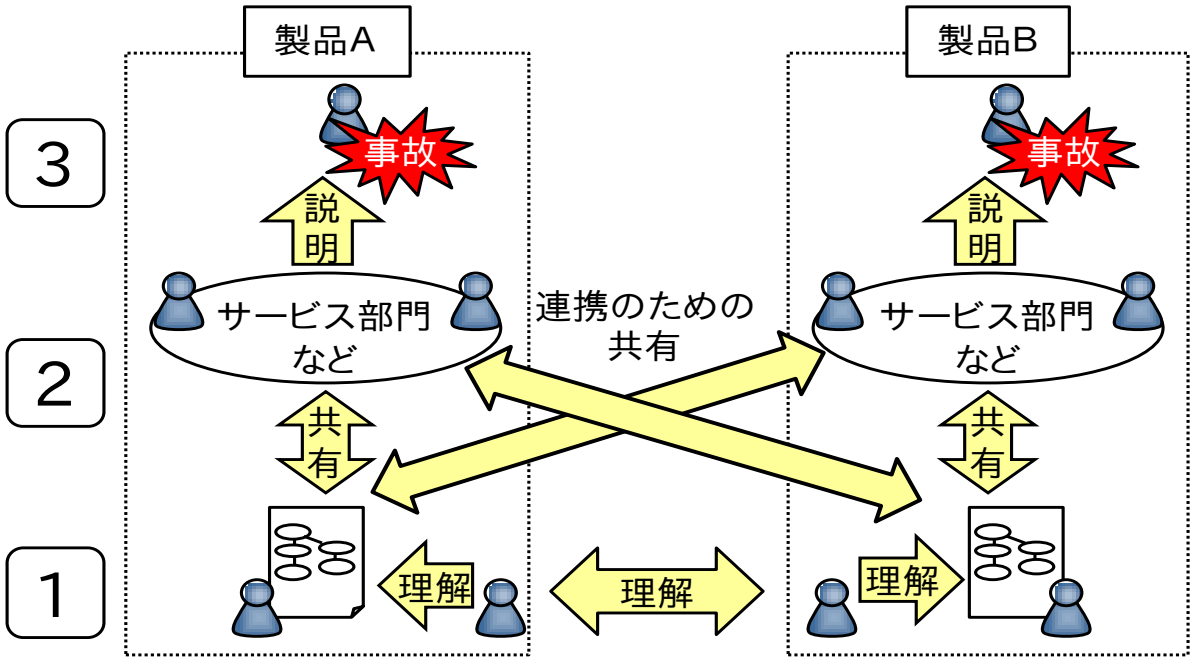
- 的確なリスク対応、セーフティ設計・セキュリティ設計の重要性、見える化による設計情報共有の必要性とそれらへの経営層の関与のあり方
  - 実際に発生した事故とインシデントの具体的事例、原因、およびその対策のヒント
  - 実際に産業界で使われているリスク分析・脅威分析手法、およびその設計手法
  - 事故・インシデント発生時に第三者への説明責任を果たすための設計品質の見える化手法

解説例(1) 経営層の関与の必要性

【セーフティ設計・セキュリティ設計の課題】
表面上に見える製品・サービスの機能とは異なり、下支えする要件のため、コストとリソースをかけにくい。
→開発現場の判断だけでは取り組みにくい。



解説例(2) 設計の見える化の必要性



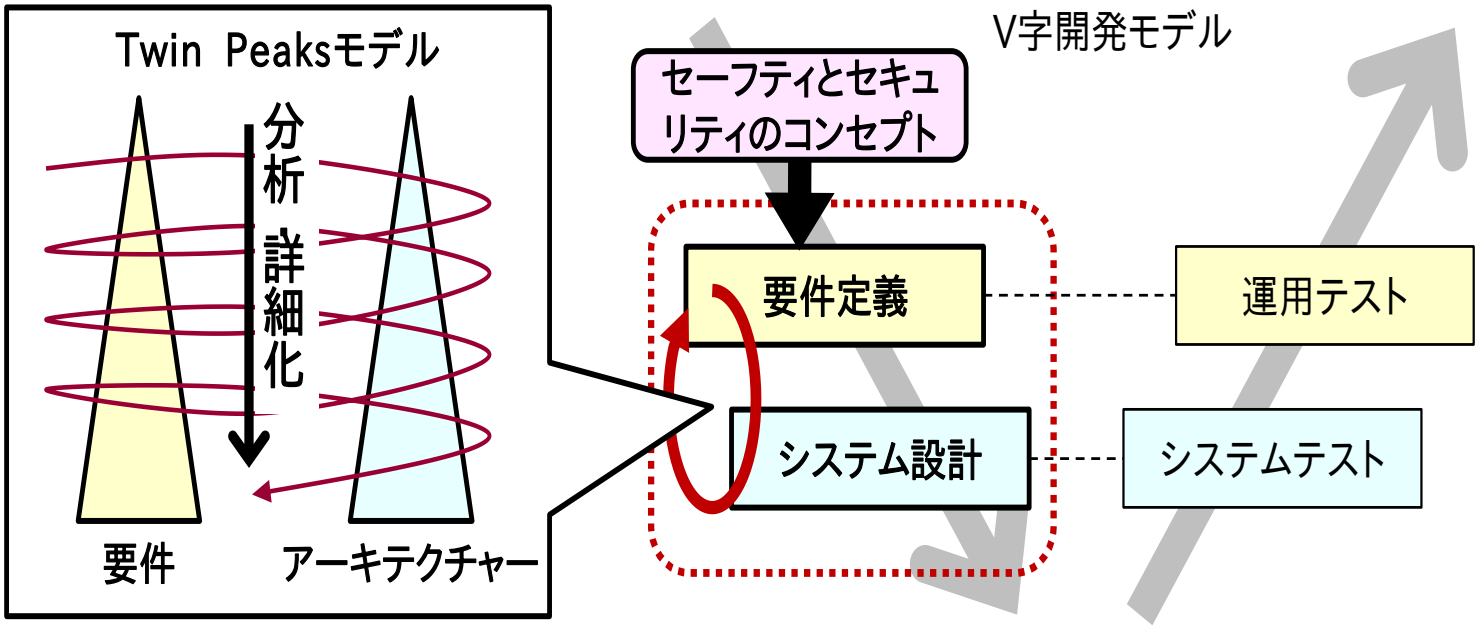
トレーサビリティ、説明責任

ステークホルダーとの設計情報共有

ソフトウェア設計や再利用時の設計内容の理解

解説例(3) セーフティ＆セキュリティ機能を実現するために

上流の段階でリスク分析を実施し、リスクを低減した設計を行う



要件とアーキテクチャを、セーフティ／セキュリティ分析を繰り返して詳細化する

解説例(4) 分析手法・設計手法

セーフティ設計・セキュリティ設計に有効な手法の紹介

手法	手法の概要
リスクマトリックス	事故の発生頻度と被害の大きさから2軸の表形式でリスクの程度を分類する
リスクグラフ	頻度、過酷度、止めやすさなど複数要素の有無を順に判断して、リスクのレベルを分類する
FTA	事故など望ましくない事象を起点に、その発生原因を体系的に整理する
FMEA	部品の故障を起点に、システムへの影響を体系的に検討する
HAZOP	利用手順に連想しやすいガイドワードをあてはめながら、システムのハザードを想定する
STAMP/STPA	システム間の制御ごとにガイドワードを適用して、複雑なシステムでの相互作用のハザードを特定する

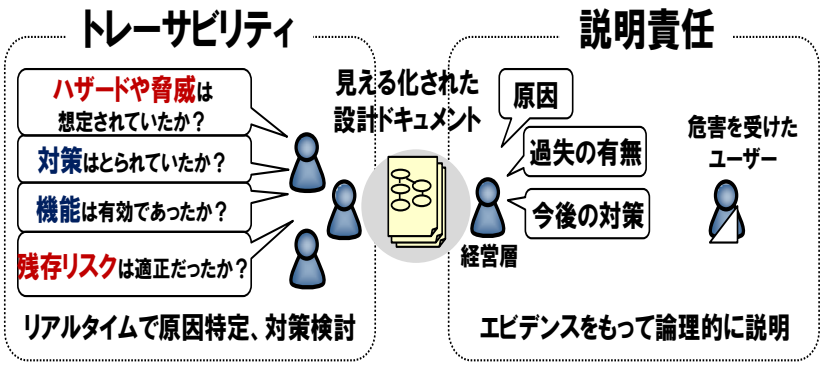
技術名	概要	対応する脅威例
耐タンパー性	機器に格納されたソフトウェアや暗号鍵データを解析されないように、こじ開けられると自動的にメモリを消去したり、漏えい電磁波や電力消費量の測定による解析を防ぐ特殊な回路を追加することで、攻撃耐性を高める	機器に格納されたソフトウェアを読みだされ、コピー製品を作られることを防ぐ
暗号化	機器に格納したデータや機器間で送受信するデータを暗号化し、不正に読みだされたり盗聴された場合でも情報漏えいを防ぐ	生活機器で測定した個人のデータが送信中に盗聴され、プライバシーが侵害されることを防ぐ
認証	正規のユーザ、サーバ、機器などの真正性を確認することで、なりすましによる不正利用や機器・部品の不正な入れ替えを防ぐ	所有者でない者が勝手に機器を利用することを防ぐ
アクセス制御	認証されたユーザの権限の範囲で、機器やシステムの利用を認可する	子供が親の許可なしで有料サービスを利用しないよう、ペアレンタル機能で制限する
電子署名	ソフトウェア更新用ファイルなど重要なデータに電子的な署名を付与することで、ファイルの真正性や完全性(改ざんされていないこと)を確保する	偽のソフトウェア更新ファイルの送りつけによるウイルス感染を防ぐ
侵入検知	機器やシステムへの不正な侵入、実行中のメモリまたはソフトウェアの改ざんなどをリアルタイムで検知する	ネットワーク経由で機器に不正アクセスされた場合、即時に検知して遮断する
ログ・監査	機器やシステムへのアクセス記録を蓄積・分析し、攻撃回数の統計を作成したり、万一侵入された場合の被害や攻撃元を明らかにする	不正アクセスのログを分析し、攻撃元や攻撃が成功した原因を特定し、対策する

解説例(5) 問題発生時の設計品質の説明、共有

アシュアランスケースの表記法解説

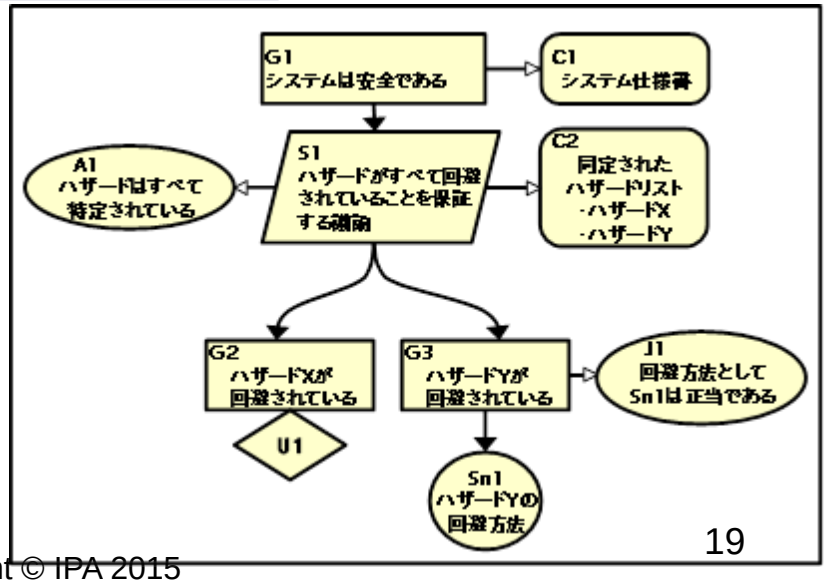
グラフィカルなアシュアランスケースの表記法一覧

表記法 特徴	CAE	GSN	D-Case
正式名称	Claim, Argument, Evidence	Goal Structuring Notation	Dependability Case
登場時期	1998年	2011年	2012年
構成要素	3種類 (主張、議論、証拠)	6種類 (表 6-4参照)	GSNを拡張(モニタ、パラメタ、アクション、外部接続、説明責任)
開発組織	英Adelard社、 ロンドン大学	英ヨーク大学	日DEOSプロジェクト



設計の品質をエビデンス（証拠）に基づき第三者でも容易に理解できる表記で論理的に説明する

GSNの表記例



【SECセミナー】

IoT時代に求められるセーフティ＆セキュリティ設計

開催日	時間	プログラム
12月7日（月曜）	13:00-	受付開始
	13:30-13:50 (20分)	「IoT時代のセーフティ・セキュリティ確保に向けた課題と取組み」 情報セキュリティ大学院大学　情報セキュリティ研究科　研究科長　教授 サプライチェーンにおける品質の見える化WG　主査　後藤厚宏　氏
	13:50-14:10 (20分)	「セーフティ設計・セキュリティ設計に関するアンケート結果の報告とガイドブック紹介」 独立行政法人 情報処理機構　ソフトウェア高信頼化センター　研究員 サプライチェーンにおける品質の見える化WG　事務局　西尾桂子
	14:10-15:00 (50分)	「IoT時代のセーフティ設計」 名古屋大学 大学院情報科学研究科　付属組込みシステム研究センター　助教　松原豊　氏
	15:00-15:10	休憩　10分
	15:10-16:00 (50分)	「IoT時代のセキュリティの確保に向けて」 一般社団法人　重要生活機器連携セキュリティ協議会　事務局長　伊藤公祐　氏
	16:00-16:50 (50分)	「自動車部品メーカとしてのセーフティ＆セキュリティの活動紹介」 株式会社デンソー　電子基板技術統括部　DP-情報セキュリティ開発室長　早川浩史　氏
	16:50-17:00	クロージング　グループリーダー 中尾

ご清聴ありがとうございました。

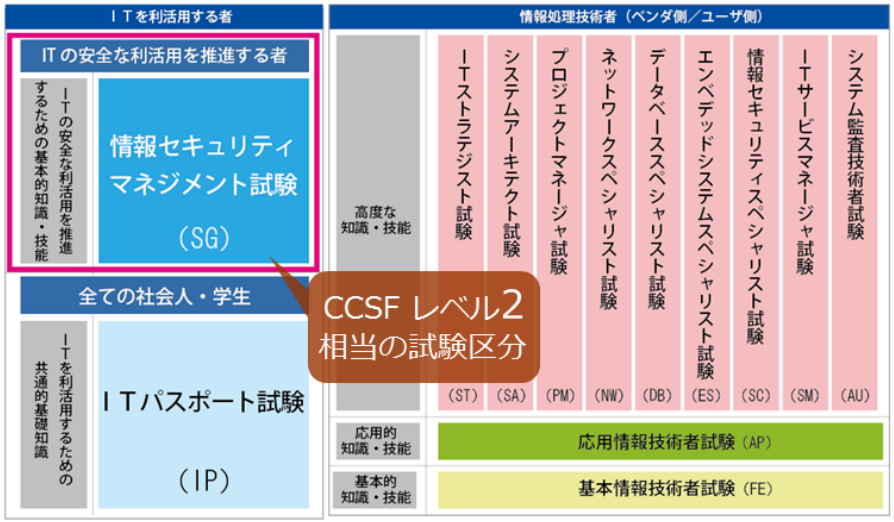
情報セキュリティに関する新たな国家試験！
情報セキュリティマネジメント試験

情報セキュリティマネジメント試験とは

情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的スキルを認定する試験

試験の位置づけ

経済産業省所管の国家試験である**「情報処理技術者試験」の新たな試験区分として創設。**



試験時間・出題形式

時間区分	試験時間	出題形式	出題数 解答数	基準点
午前	90分	多肢選択式 （四肢択一）	50問 50問	60点 （100点満点）
午後	90分	多肢選択式	3問 3問	60点 （100点満点）

実施時期（予定）

- 開始：**H28年度春期**
  （申込受付：2016年1月中旬開始予定）
- 春期・秋期の**年2回**
  （春期：4月第3日曜、秋期：10月第3日曜）

更に詳しく知りたい方へ

新試験がわかるパンフレット

職場の情報セキュリティ管理者育成に！

職場の情報セキュリティ管理者のためのスキルアップガイド

情報セキュリティスキルアップハンドブック

新試験の対象者像を踏まえ作成

ITパスポート試験

ITパスポート公式キャラクター
上峰亜衣（うえみねあい）

【プロフィール：マンガ】 https://www3.jitec.ipa.go.jp/JitesCbt/html/uemine/profile.html

「iパス」は、ITを利活用するすべての社会人・学生が備えておくべき
ITに関する基礎的な知識が証明できる国家試験です。

Windows Server 2003のサポート終了に伴う注意喚起

IPA

Windows Server 2003のサポートが2015年7月15日に終了しました。

サポート終了後は修正プログラムが提供されなくなり、脆弱性を悪用した攻撃が成功する可能性が高まります。

周辺ソフトウェアもサポートが順次終了していくため、あわせて対策が必要です。

サポートが継続しているOSへの移行検討とOS移行に伴う周辺ソフトウェアの影響調査や改修等について迅速な対応をお願いします。

脆弱性を
悪用した攻撃

- 業務システム・サービスの停止・破壊
- 重要な情報の漏えい
- データ消去
- ホームページの改ざん
- 他のシステムへの攻撃に悪用

会社の事業に悪影響を及ぼす被害を受ける可能性があります

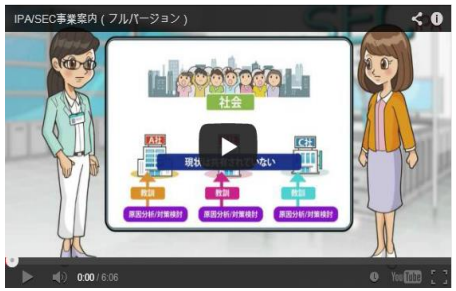
詳しくは　IPA　win2003　検索

なおWindowsXPを利用されている方はサポートが継続しているOSへの移行検討をお願いします

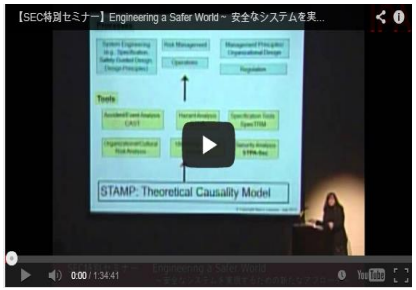
IPA ソフトウェア高信頼化センター(SEC)

Software Reliability Enhancement Center , Information-technology Promotion Agency , Japan

YouTubeで、
IPA/SECの事業内容やセミナー動画をCheck！



●SEC事業紹介
http://www.ipa.go.jp/sec/about/index.html



●SECセミナーオンデマンド
http://sec.ipa.go.jp/seminar/ondemand/

@IPA_SEC
SECの最新情報を発信しています！ Follow me！

**Twitterで、
IPA/SECの最新情報をCatch！**

https://twitter.com/IPA_SEC

アカウント名：@IPA_SEC

SWE iPedia
IPA/SECの公開情報検索データベース

**SWE iPediaで、
IPA/SECの事業成果をSearch！**

探したい情報を
分類やキーワードで検索！

http://sec.ipa.go.jp/sweipedia/

IPA/SECウェブサイトで利用者登録！

IPA/SECウェブサイトから利用者登録（無料）をすると、
メルマガ ・DMの購読や、セミナーの参加申込み、ツールの利用などができます。
是非、ご登録ください！

https://sec.ipa.go.jp/entry/index.html

↓詳しくは、SECウェブサイトをClick！

検索 ソフトウェア高信頼化センター