セキュリティ規格に関する動向

～　医療機器の規制に関する国際動向シンポジウム　～

東芝メディカルシステムズ(株)
研究開発センター　ソフトウェア開発部
池田　智

本日の内容

- サイバー・セキュリティ・リスクの現状
- サイバー・セキュリティに関連する国際規格の動向
- サイバー・セキュリティへの対応の課題
- まとめ

サイバー・セキュリティ・リスクの現状

～　サイバー・セキュリティって本当に対応しないといけないの？～

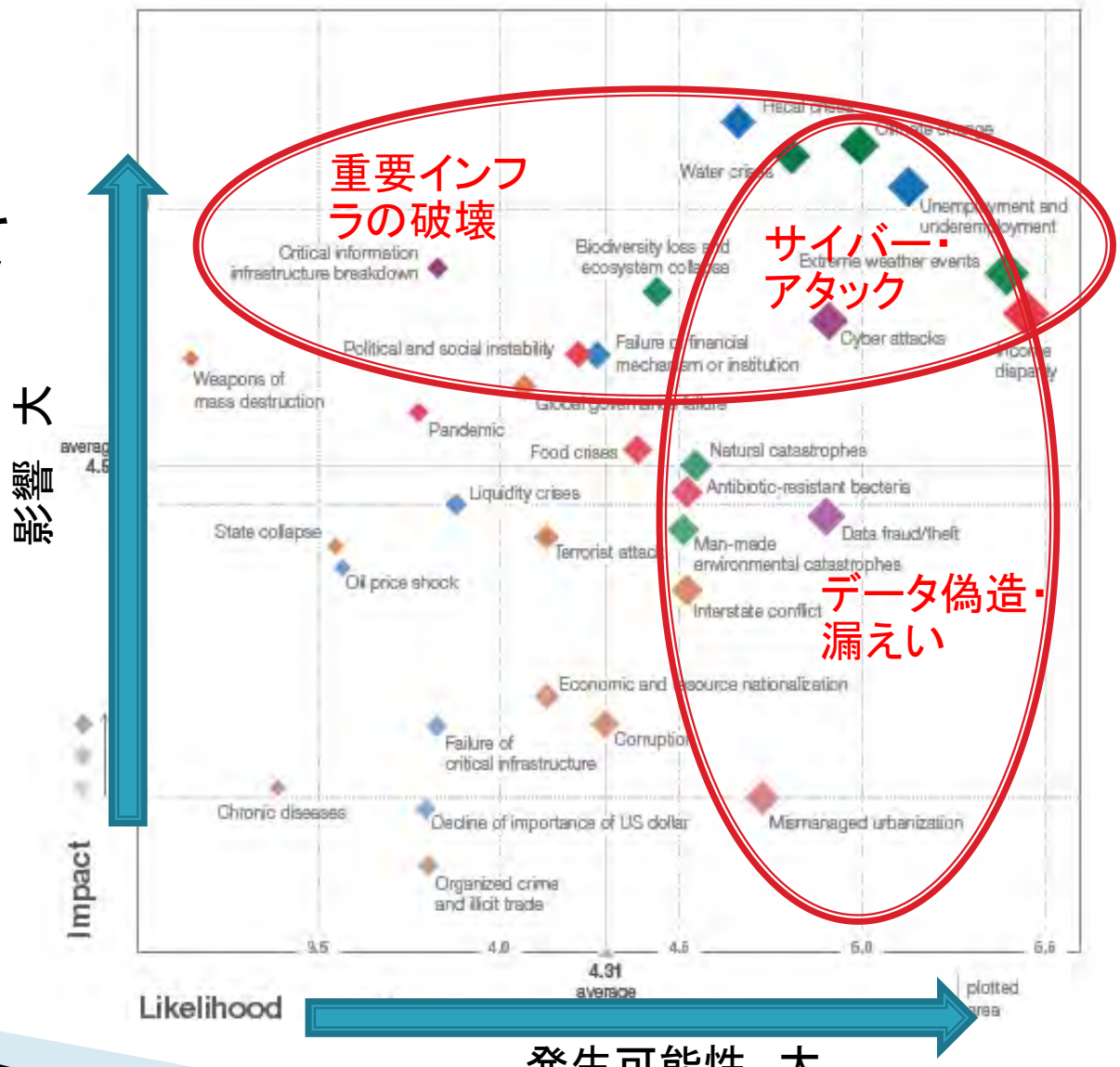
サイバー・セキュリティへの脅威（1）

- WEF（World Economic Forum）のGlobal Risk Reportで、経済リスク、気候リスクなどと並ぶリスクとしてサイバー・セキュリティに関連する脅威が認識

http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf より引用

サイバー・セキュリティへの脅威（2）

- 影響度、発生可能性とも大きなリスクとして認識



http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf より引用

サイバー・セキュリティへの脅威（3）

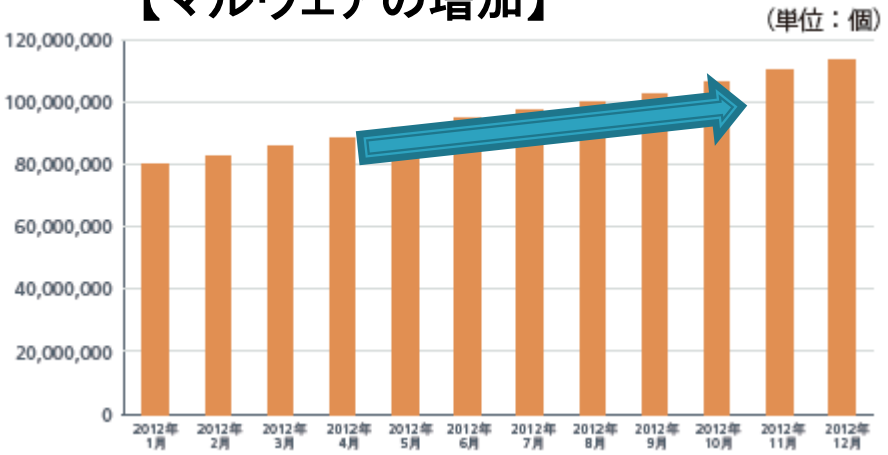
2013年1月	政府（日本）	中央省庁の職員が使用するパソコンがサイバー攻撃を受け、機密文書が外部に流出した疑いがあることがわかった。
2013年1月	政府（米国）	「NullCrew」を名乗るハッカー集団が、政府機関などのウェブサイトに不正アクセスした。
2013年1月	企業（日本）	企業のウェブサイトの一部に不正アクセスがあり、会員約47万人分の個人情報を改ざんされたと発表した。
2013年1月	政府（日本）	独立行政法人が運用している ウェブサイトが外部からの不正アクセスによるサイバー攻撃を受け、一部のページが改ざんされた。
2013年1月	地方自治体（日本）	地方自治体でウェブサイトの更新に必要なIDとパスワードが何らかの方法で盗まれ、海外のサーバーから不正アクセスを受けた。
2013年1月	政府（米国）	政府機関のウェブサイトに対してアノニマスがサイバー攻撃を行った。
2013年1月	企業（米国）	マスコミ各社が、中国からサイバー攻撃を受け続けていた旨、相次いで公表した。
2013年1月	政府（日本）	中央省庁のパソコンからインターネット上の外部サーバへの不審な通信が確認され、パソコンから文書が流出した疑いがあることが判明した。
2013年2月	企業（米国）	Twitterで利用者情報を狙った不正アクセスが検出された。攻撃者はおよそ25万人分の利用者のメールアドレス、セッショントークン、暗号化したパスワードにアクセスした可能性があることが判明した。
2013年2月	政府（米国）	政府機関のサーバ14台とワークステーション20台が不正侵入され、職員数百人の個人情報が流出した。
2013年2月	政府（米国）	政府機関がサイバー攻撃を受け、個人情報が流出した。
2013年2月	企業（日本）	企業のサーバおよびパソコン端末17台がマルウェアに感染し、個人情報を含む営業情報と関連する技術情報が外部に漏えいした可能性があることが判明した。
2013年3月	企業（米国）	企業は外部からサーバに不正アクセスを受け、利用者のIDやパスワード、メールアドレスなどが盗まれたおそれがあると発表した。
2013年3月	企業（日本）	電子商取引サイトが不正アクセスを受け、最大1万2036件のクレジットカード情報が流出した可能性があると発表した。
2013年3月	政府（日本）	中央省庁が運営するウェブサイトが改ざんされた。閲覧者のパソコン内の情報が盗まれた可能性があるとのこと。
2013年3月	企業（韓国）	銀行や放送局など複数のコンピュータネットワークがサイバー攻撃とみられる攻撃を受けた。
2013年3月	地方自治体（日本）	地方自治体で学校や文化施設など計53のウェブサイトを管理するサーバが外部から改ざんされた。
2013年3月	民間（欧州）	非営利団体のウェブサイトにDDoS攻撃が行われ、同団体はウェブサイトを停止した。

（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

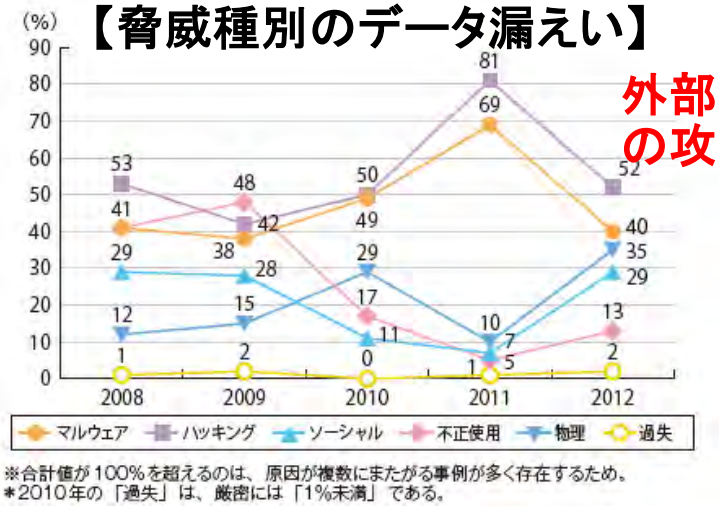
※平成25年版　情報通信白書より転載

サイバー・セキュリティへの脅威（4）

【マルウェアの増加】

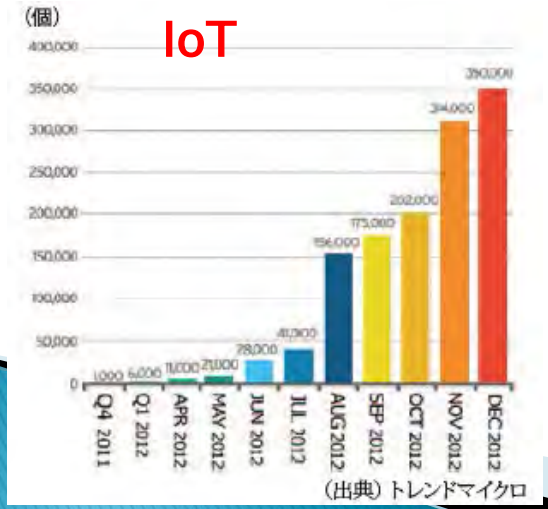


【脅威種別のデータ漏えい】

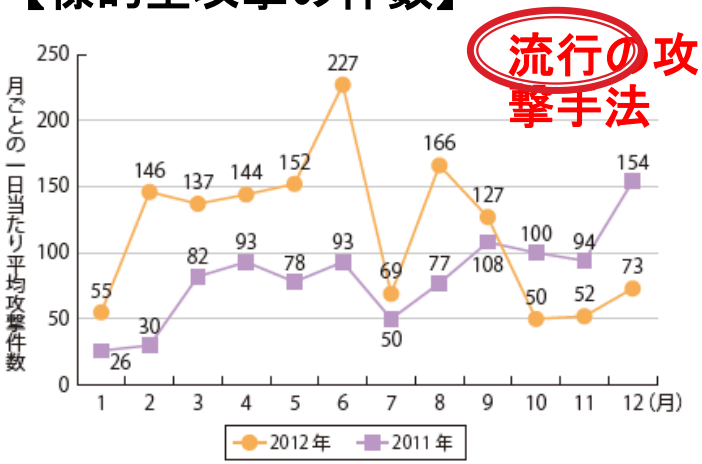


※合計値が100%を超えるのは、原因が複数にまたがる事例が多く存在するため。
＊2010年の「過失」は、厳密には「1%未満」である。

【Android向けマルウェア】



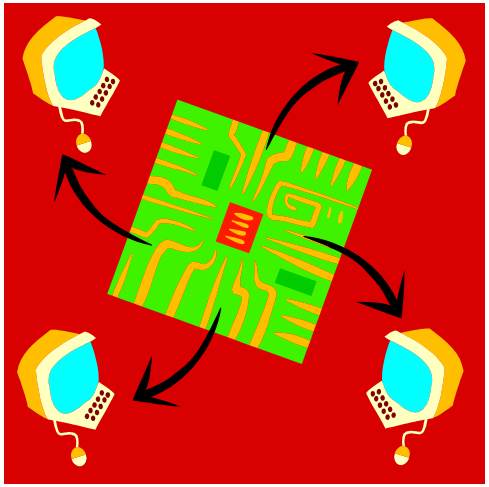
【標的型攻撃の件数】



※平成25年版　情報通信白書より転載

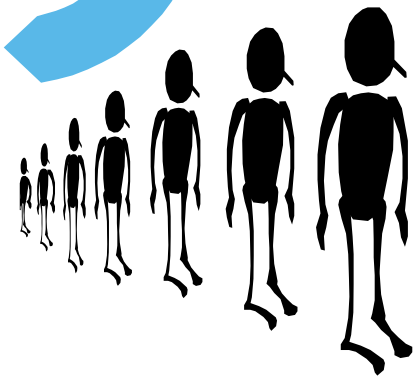
サイバーセキュリティの3つの要素

サイバー空間



デバイス（従来の機器＋IoT）

ヒト/プロセス



国際公共財としてのサイバー空間

- 国際公共財(Global Commons)

【国家安全保障戦略(抜粋)】

近年、海洋、宇宙空間、サイバー空間といった国際公共財(グローバル・コモンズ)に対する自由なアクセス及びその活用を妨げるリスクが拡散し、深刻化している。

また、情報システムや情報通信ネットワーク等により構成されたグローバルな空間であるサイバー空間は、社会活動、経済活動、軍事活動等のあらゆる活動が依拠する場となっている。

一方、国家の秘密情報の窃取、基幹的な社会インフラシステムの破壊、軍事システムの妨害を意図したサイバー攻撃等によるリスクが深刻化しつつある。

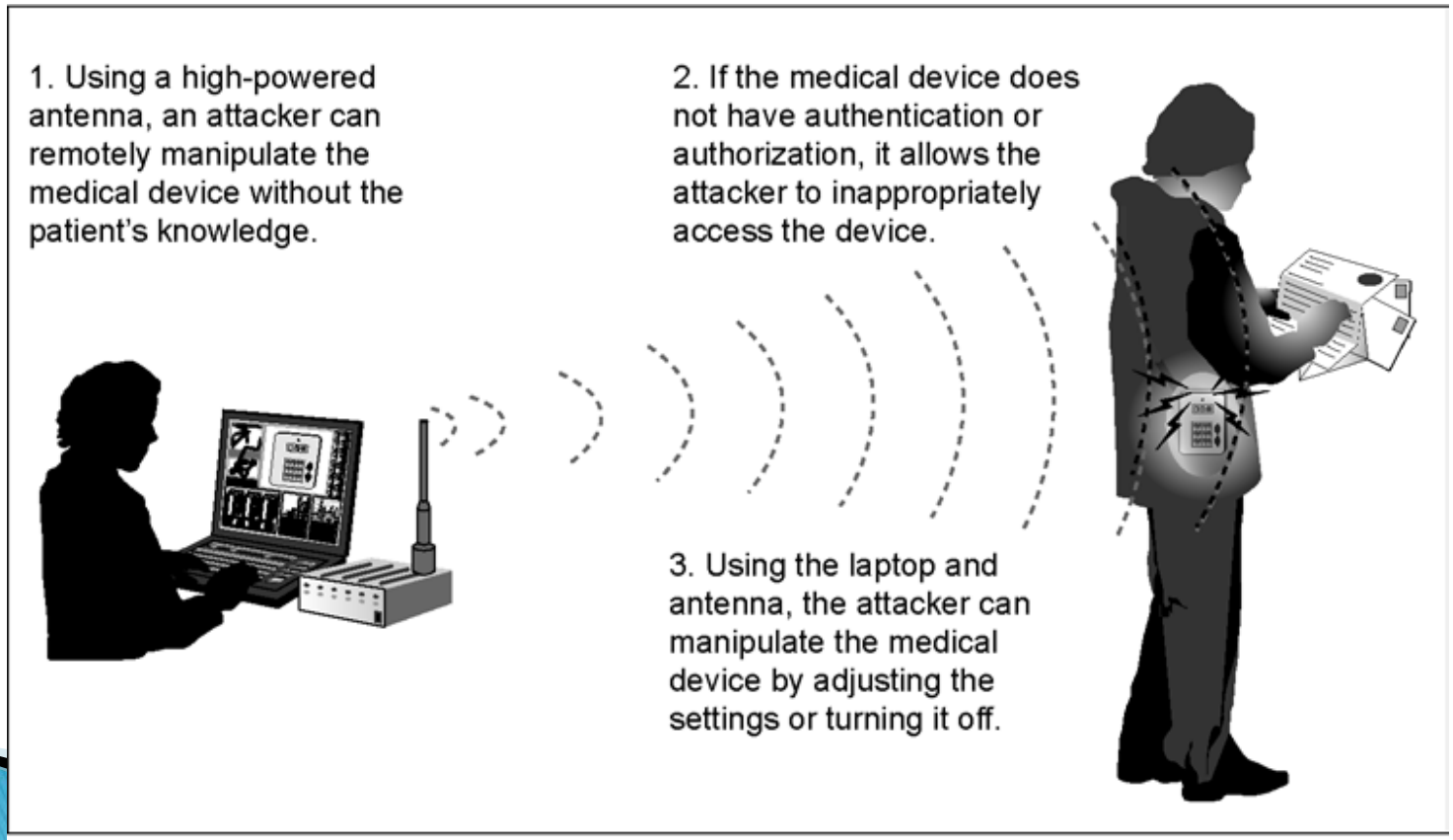
我が国においても、社会システムを始め、あらゆるものがネットワーク化されつつある。このため、情報の自由な流通による経済成長やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障を万全とするとの観点から、不可欠である。

- 今現在の国際公共財の様子(IPViking map)
  - NORSE社のHPより(参考URL: http://norse-corp.com/)
  - NICTER(http://www.nicter.jp/)

リスクのない公共財は望めない

医療機器における脅威事例

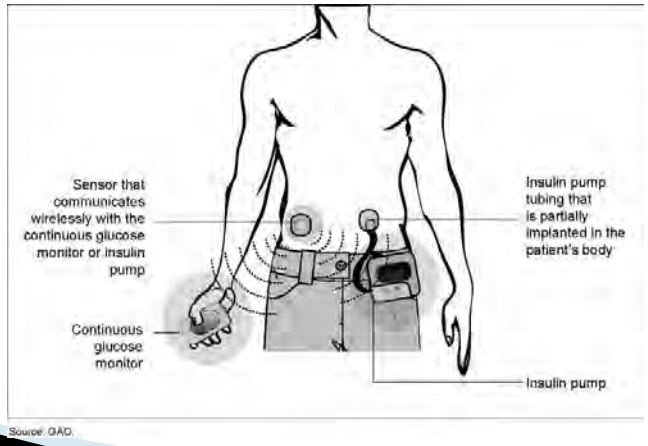
- 医療機器の脆弱性を利用した攻撃
  - 認証の脆弱性を利用

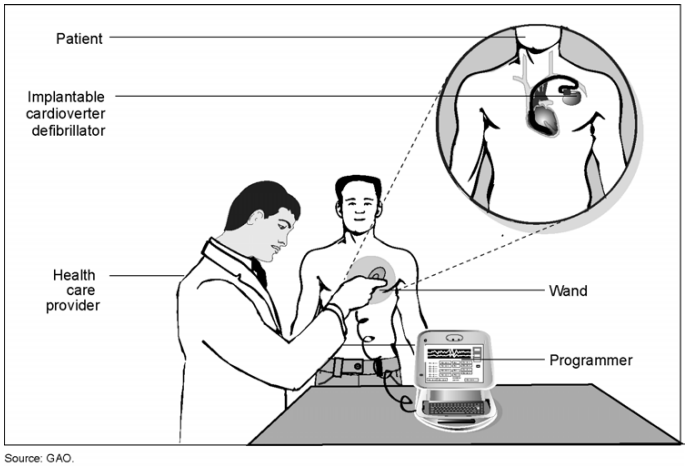


Source: GAO.

医療機器における脅威事例

- グルコース・モニタリング・システムと、インスリン・インジェクション・システムが連携して動作するシステム
  - 【脅威事例】グルコース・モニタリング結果の書き換え
  - 【脅威事例】機器の設定情報の書き換えによる投与量の変化
- 埋め込み型除細動器
  - 【脅威事例】プログラムの不正な書き換え

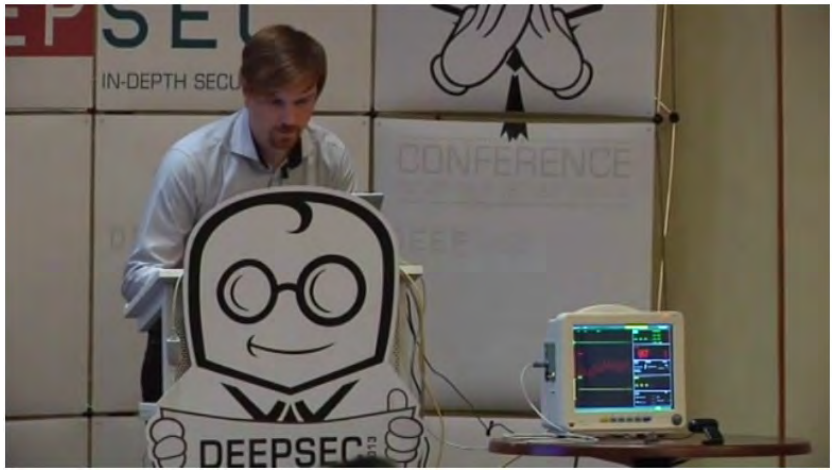




FDA Should Expand its Consideration of Information Security for Certain Types of Devices
http://www.gao.gov/assets/6[illegible]47767.pdf

医療機器における脅威事例

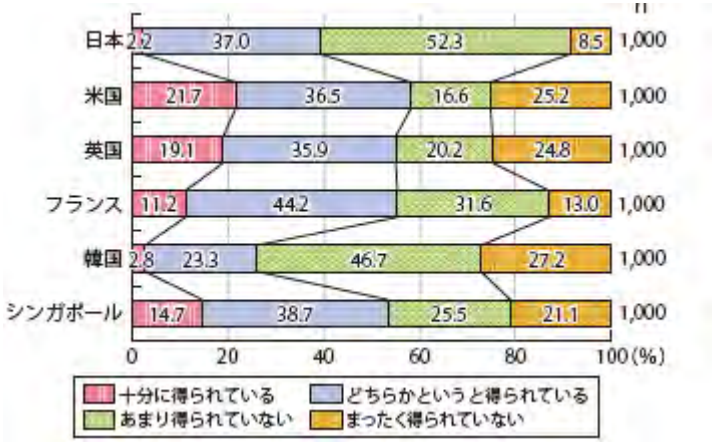
- 実際の計測データを「fake data」と置き換えて、セントラル・ステーションに偽りデータを表示、装置のモニタに偽りのデータを表示
  - Demo Video (43分)



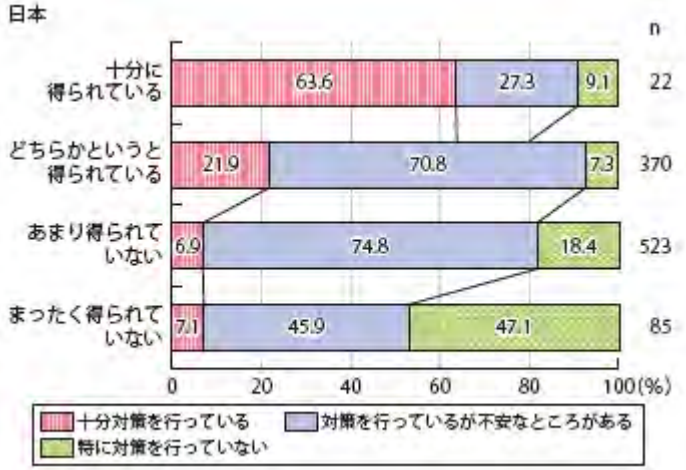
http://outsidelens.scmagazine.com/video/Hacking-Medical-Devices;recent#.UvwaFDiZGk8.twitter より引用

サイバー・セキュリティ対策とヒト

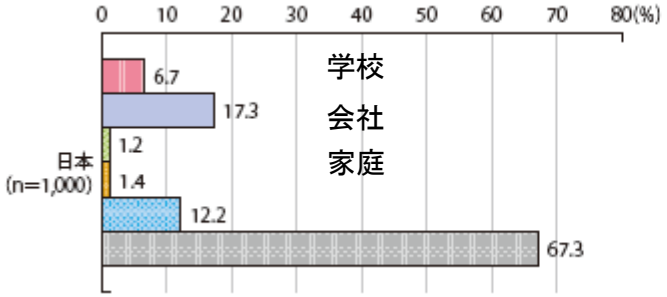
【サイバー・セキュリティ対策の情報】

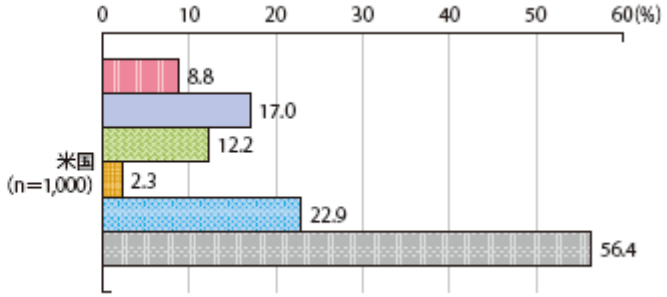


【サイバー・セキュリティ対策の実施】



【サイバー・セキュリティ対策の教育】





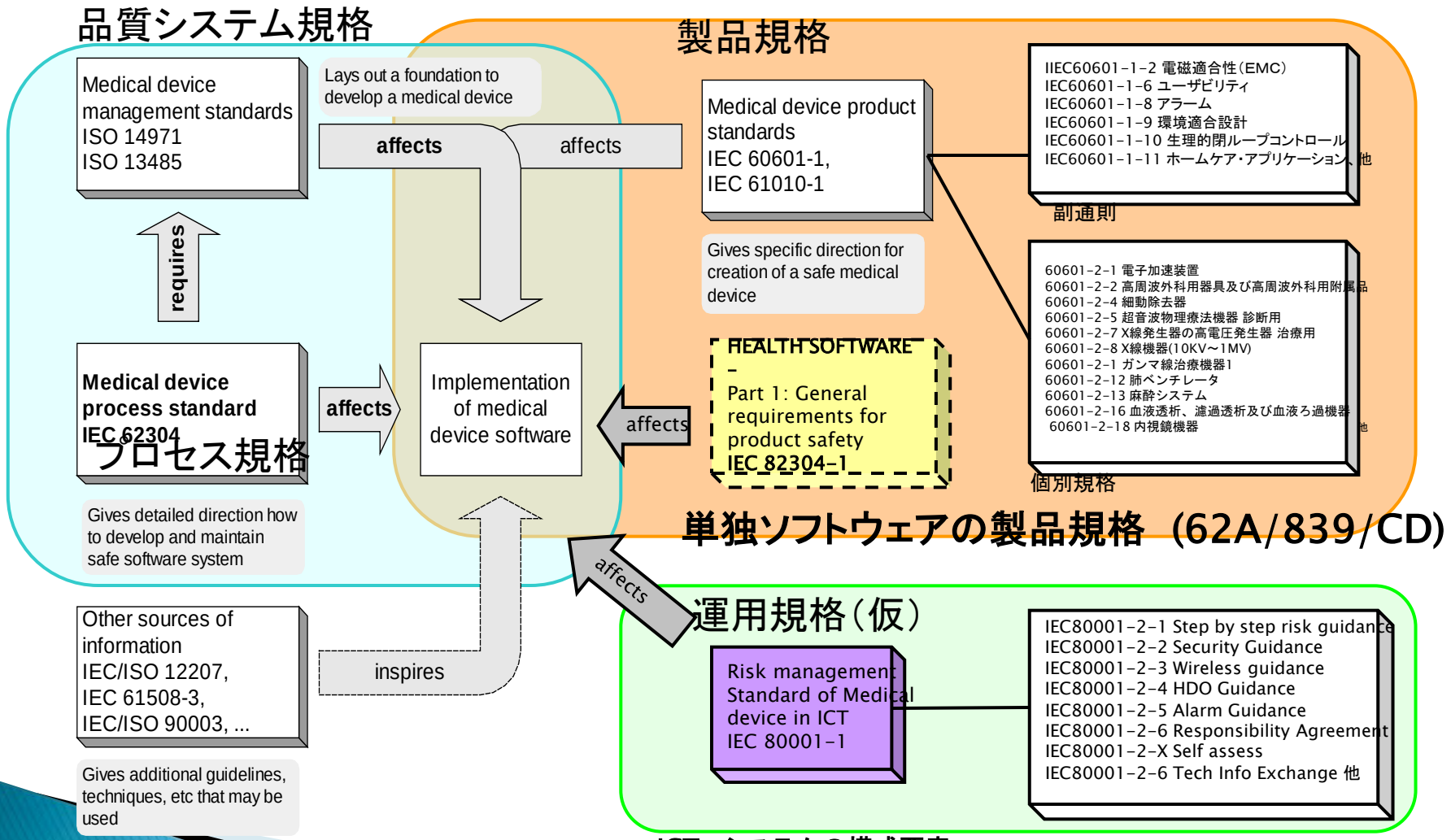
※12万人を対象とした標的型攻撃でメイルを開封：14%

※平成25年版　情報通信白書より転載

サイバー・セキュリティに関連する国際規格の動向

～　製造業者・利用者の連携によるサイバー・セキュリティ対策は可能か？～

品質システム規格、製品規格と運用規格



IEC 62304 Annex C 図C.1

ICT: システムの構成要素
設置施設のリスクマネジメントにおける組織・責任についての要求事項

※中里氏資料を改変

IEC80001とは？

The Application of Risk Management for IT Networks Incorporating Medical Devices

Part 1: Roles, Responsibilities, and Activities

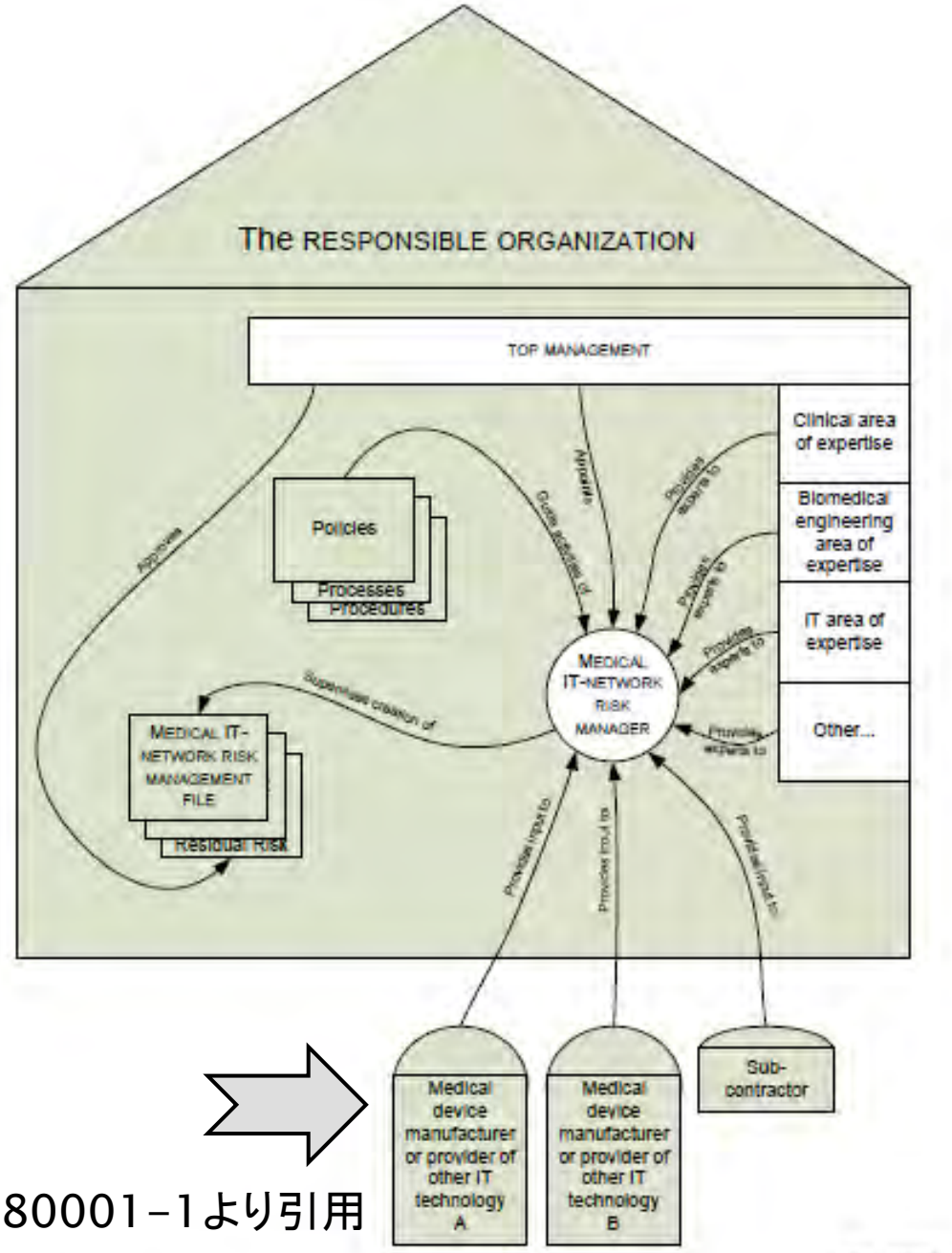


Figure B.1 – Overview of roles and relationships

※IEC80001-1より引用

IEC80001-2-2 Security

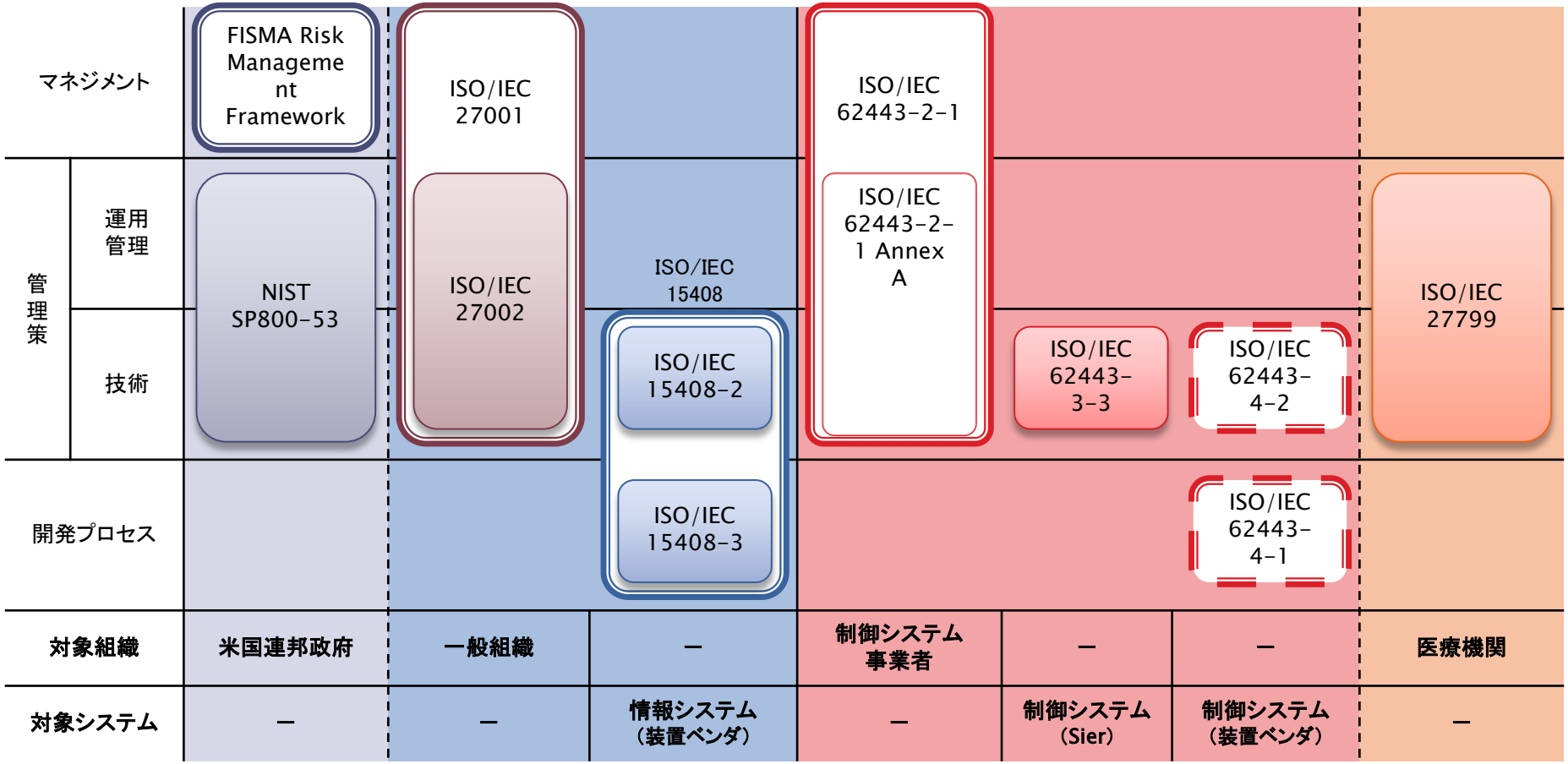
- 正式名称
  - Part 2-2:**Guidance for the disclosure and communication of medical device security needs, risks and controls**
- スコープ
  - IEC80001-1のリスク・マネジメントに関連する**セキュリティ情報の公開、交換に関するフレームワーク**の定義

※リスクマネジメントでのセキュリティ
※コミュニケーションのための情報

IEC80001-2-2 Security

- ALOF（自動ログオフ）
- AUDT（監査記録）
- AUTH（権限管理）
- CNFS（コンフィグ）
- CSUP（更新）
- DTBK（バックアップ）
- EMRG（緊急アクセス）
- DIDT（匿名化）
- IGAU（真正性）
- STCF（保存）
- MLDP（マルウェア）
- NAUT（ノード認証）
- PAUT（認証）
- PLOK（物理的ロック）
- SGUD（セキュリティガイド）
- SAHD（障害耐性）
- RDMP（ロードマップ）
- TXCF（伝送保護）
- TXIG（伝送真正性）
- UUID（単一ID）

IEC80001-2-8　各規格の関係（関連図）

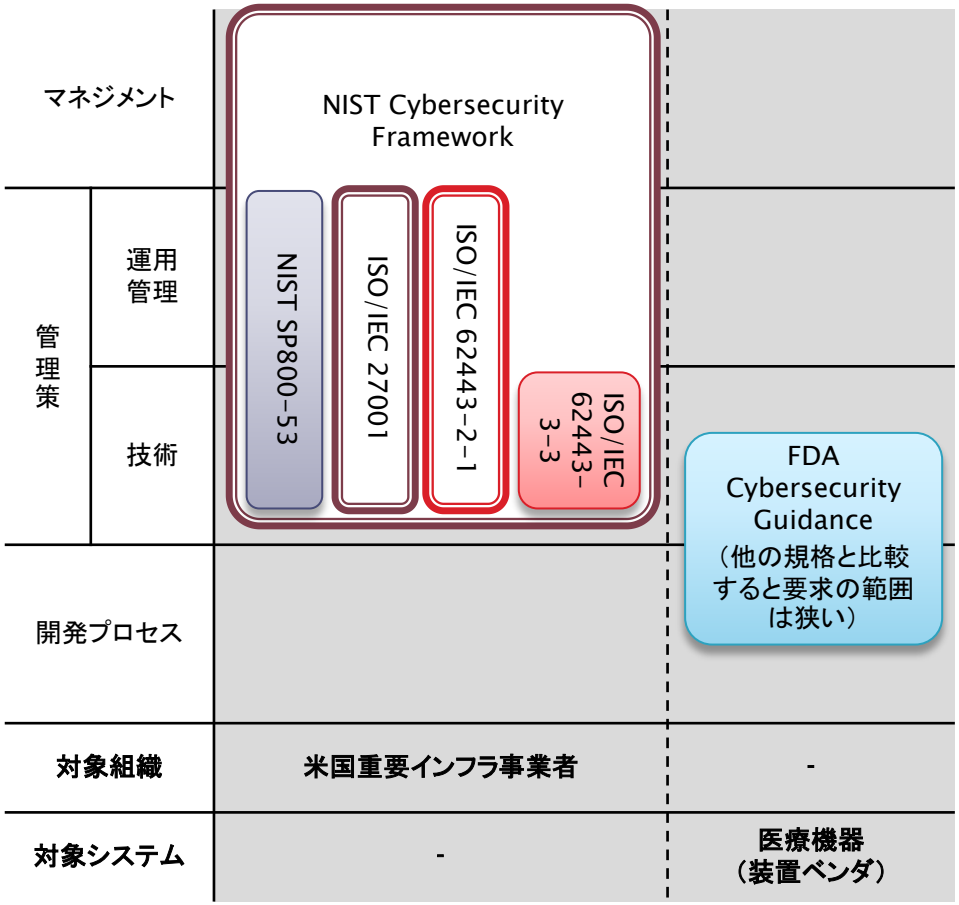


IEC 80001-2-8 TRで参照されている規格

上記の規格に関連する規格

上記の規格に関連する規格（策定中）

その他規格の関係（関連図）



IEC 80001-2-X TRで参照されている規格

上記の規格に関連する規格

上記の規格に関連する規格（策定中）

ISO/IEC 27002:2013

情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範
(Information technology – Security techniques – Code of practice for information security controls)

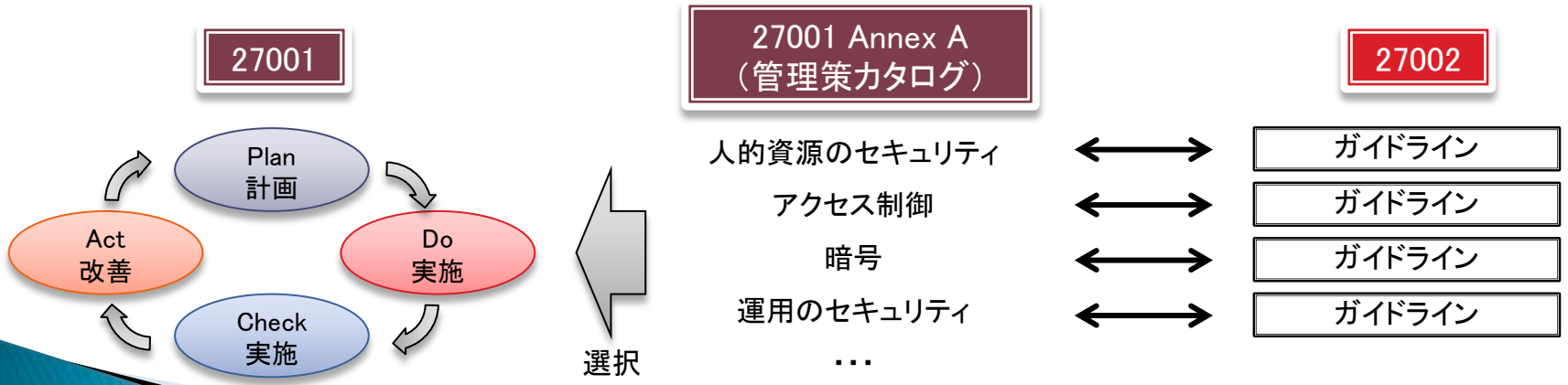
- ISO/IEC 27002とは、ISO/IEC 27001実践のための規範にあたる規格

ISO/IEC 27001（通称ISMS）

- 組織のセキュリティマネジメントプロセスモデル（PDCAサイクル）を規程している国際規格（認証の対象となる規格）
- 具体的なセキュリティ管理策については規程せず*、Annex Aで管理策を例示し、リスクアセスメントに応じて管理策を適宜選択することを要求

（*管理策は急速に変化するため）

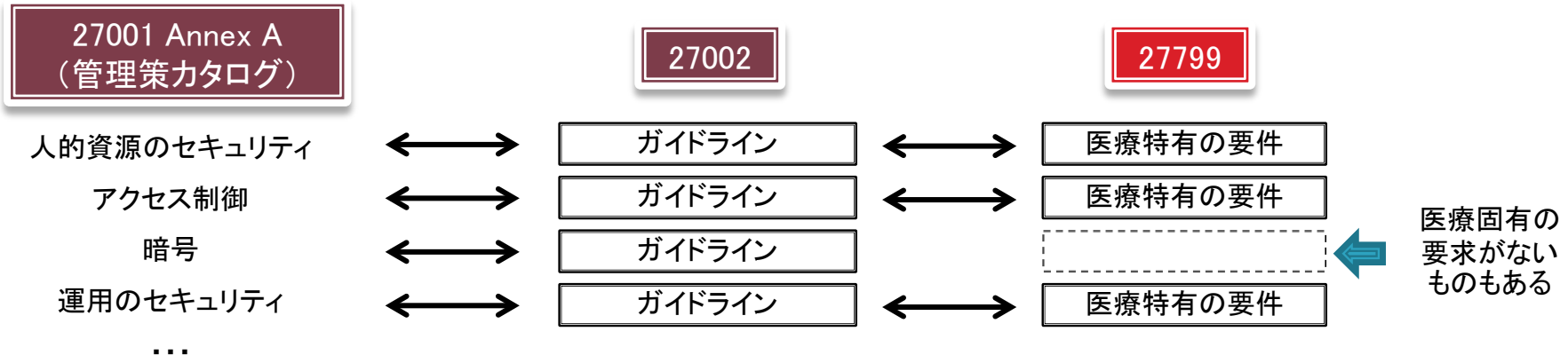
- ISO/IEC 27002は、ISO/IEC 27001 Annex Aの各管理策についての具体的な実践規範（ガイドライン）を示したもの



ISO/IEC 27799:2008

健康情報－ISO/IEC 27002を活用したヘルスケアにおけるセキュリティマネジメント
(Health informatics – Information security management in health using ISO/IEC 27002)

- ISO/IEC 27002の要求をベースに医療分野特有の要求を規格化したもの
- 対象は医療機関および医療情報を扱う組織



例:「電子的メッセージ」の記載事項

27002

次を考慮することが望ましい。
- 正しい送付先及び送付手段の確実化
- 誰でも使える外部サービス（インスタントメッセージ、ファイル共有）の事前承認の取得

…

27799

ISO/IEC 27002のガイダンスに加えて個人健康情報を含む電子メッセージの機密性と完全性を確保する手段が望ましい。個人健康情報を含むEメールは暗号化されることが望ましい。

ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008

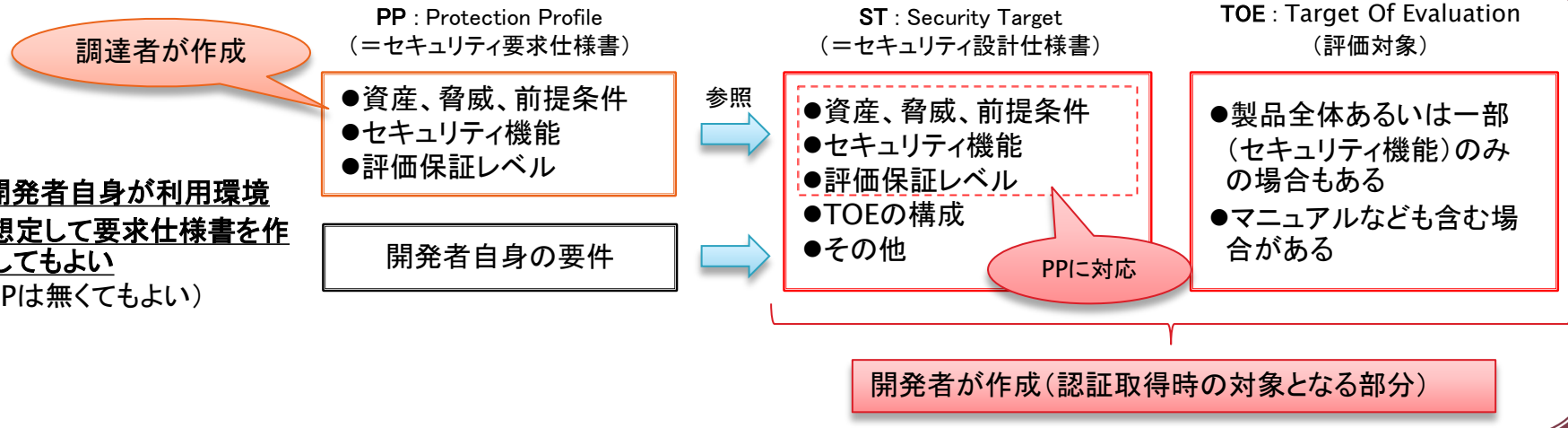
情報技術セキュリティ評価のためのコモンクライテリア（通称CC）
(Common Criteria for Information Technology Security Evaluation)

- ISO/IEC 15408(CC)とは
  - IT製品のセキュリティ機能の評価基準を定めた規格
  - 設計と実装の正確性を評価する（セキュリティの高さを評価するものではない）
  - その製品を利用する組織の運用や管理は評価対象とならない
  - 対象はセキュリティ機能を持ったIT製品（ソフトに限定されない）
  - 20ヵ国以上で政府の調達基準として利用
    - 日本：責任者が必要と認めた場合、候補が複数ある場合は認証取得製品を選択する
    - 米国：機密性の高い国防上の情報を扱う機関（DoDなど）のみ必須

評価対象製品群

- ✓OS
- ✓DBMS
- ✓ファイアウォール
- ✓IDS/IPS
- ✓ICカード
- ✓MFP

＜CCの概要＞



ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008

情報技術セキュリティ評価のためのコモンクライテリア（通称CC）
(Common Criteria for Information Technology Security Evaluation)

Part 2 セキュリティ機能要件

- 識別と認証
- 通信
- 暗号サポート
- 利用者データ保護

など

⇒ ＜機能カタログ集＞
PP/ST作成時に適宜選択

Part 3 セキュリティ保証要件

- 開発
- テスト
- ガイダンス
- ライフサイクルサポート

など

⇒ ＜検証項目カタログ集＞
TOEのセキュリティ機能の妥当性と正確性を検証するための項目
（評価保証レベル※に応じて項目が決定）

※評価保証レベル（EAL）とは
・検査範囲の程度を表す
・EAL1～EAL7の7段階

・EALに応じて求められる証拠が異なる
例えば
ガイダンス　：EAL1以上で必要
ソースコード　：EAL4以上で必要

・政府調達ではEAL基準を定めている
例えば日本政府機関の場合
ファイアウォール　：EAL4以上の製品
OS　：EAL3以上の製品
DBMS　：EAL2以上の製品
（経済産業省資料より）

補足：CCの最新動向（2013年9月の国際承認アレンジメント(CCRA)での報告より）

＜今までのCCの問題点＞

- PP（要求仕様）が国によって異なる　⇒　その国のPPで認証を取得しなおさないといけない
- PPを参照しない場合に不適切な仕様の可能性がある　⇒　実現不可能な前提条件や運用環境での評価

⇒
- 国際的に共通のPP(CPP)を各製品分野ごとに開発することで合意
- 2017年からは相互承認はCPP適合の認証製品に限定

IEC 62443-3-3:2013

工業通信ネットワーク — ネットワーク及びシステムセキュリティ
(Industrial communication networks – Network and system security)

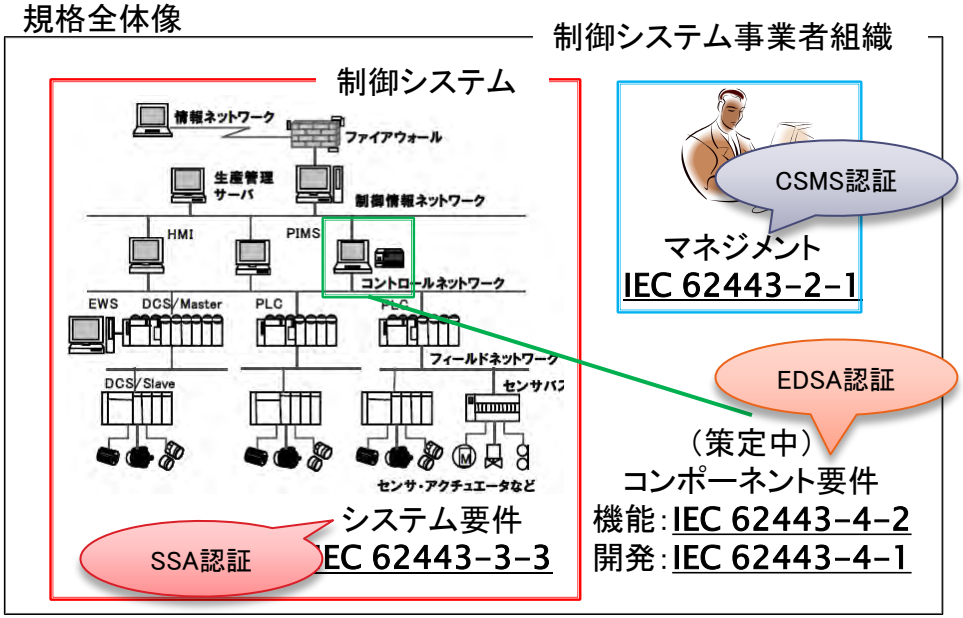
※ IEC 62443シリーズの多くは策定中段階であるため、以下の内容は今後変わる可能性がある

- IEC 62443とは
  - 制御システムのセキュリティ規格
  - 対象は制御システムの全レイヤー（事業者、システム、コンポーネント）
  - 各レイヤー毎の認証制度（CSMS、SSA、EDSA）も一部運用が開始している
  - FDAが医療機器への適用を検討中（FDAのRecognized Standardに追加された）
- IEC 62443-3-3はシステムレイヤーでセキュリティ要件を規定している規格

規格一覧

レイヤー	対象	IEC	概要
共通	全体	62443-1-1	概念や用語の定義など
		62443-1-2(策定中)	
		62443-1-3(策定中)	
組織	事業者 運用者	62443-2-1	セキュリティマネジメント
		62443-2-2(策定中)	
		62443-2-3(策定中)	
		62443-2-4(策定中)	提供側の要件
システム	構築事業者 SIer	62443-3-1	セキュリティ技術の解説
		62443-3-2(策定中)	
		62443-3-3	システムの要件
コンポーネント	装置ベンダ	62443-4-1(策定中)	開発プロセス
		62443-4-2(策定中)	装置のセキュリティ要件

規格全体像



CSMS（Cyber Security Management System）
SSA（System Security Assurance）
EDSA（Embedded Device Security Assurance）

NIST SP 800-53, Revision 4

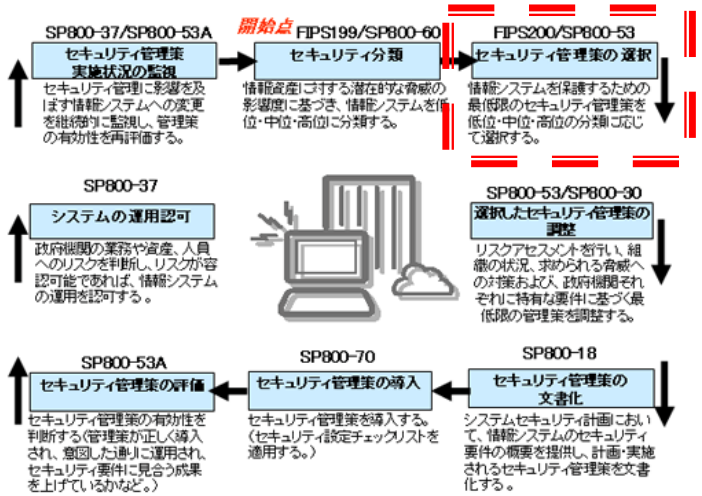
連邦政府情報システムにおける推奨セキュリティ管理策
(Recommended Security Controls for Federal Information Systems and Organizations)

- 9.11のテロを受けて、米国政府は2002年にFISMA（連邦情報マネジメント法）を規定
- さらにNIST（国立標準技術研究所）は2003年に「FISMA導入プロジェクト」を立ち上げ、**“FISMAリスクマネジメントフレームワーク”**と様々な**規格**・**ガイドライン**を開発

FIPS（連邦情報処理標準）　　NIST SPシリーズ

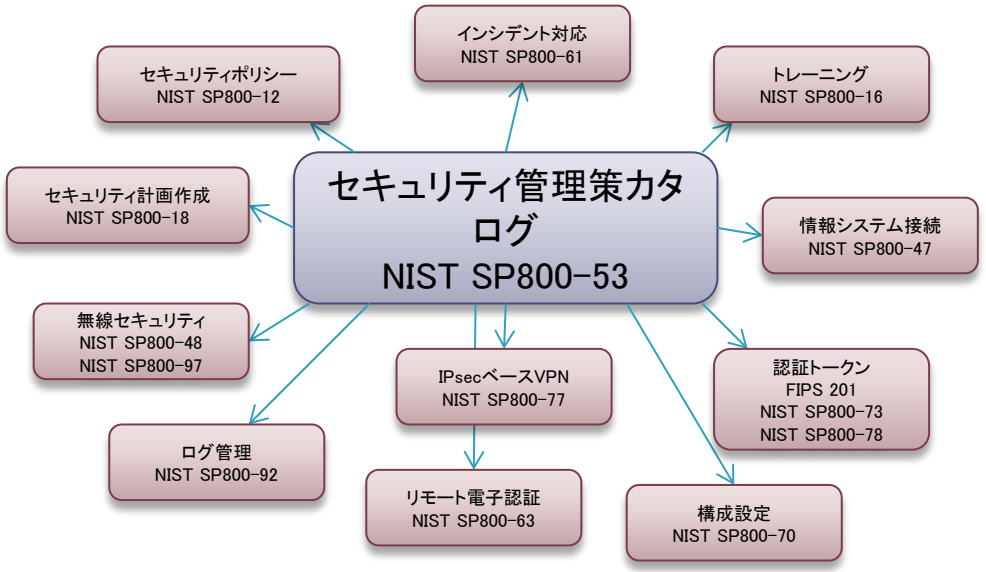
- 上のような背景においてNIST SP800-53は次の目的で作成されたガイドライン
  - セキュリティ管理策を選択する際のカタログを示す
  - 他の詳細な規格・ガイドラインへの参照をガイドする

FISMAリスクマネジメントフレームワーク「セキュリティ管理策の選択」で使用



＊ISO/IEC 27001のPDCAサイクルに相当

FIPSや他のSPシリーズへの参照をガイド



サイバー・セキュリティ対応の課題

～　ウィルス対策ソフトをいれたから大丈夫！？　～

脆弱性とは？

- 経済産業省告示第二百三十五号
  - ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。
- MS TechNetでの非公式定義
  - 製品の適切な使用による場合でも、攻撃者によるユーザーシステムに対する特権の不正行使、操作の制限、システム上のデータの損傷、および許可されていない信頼の偽装を防止不能にする、製品に含まれる問題である。
    - http://technet.microsoft.com/ja-jp/library/gg983510.aspx

脆弱性の実態

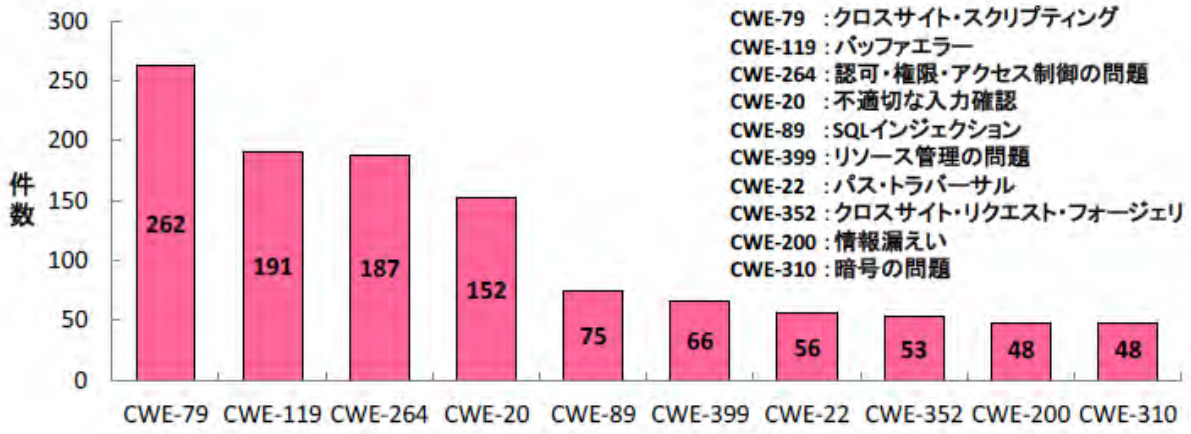


図2-1. 2014年第1四半期に登録した脆弱性の種類別件数

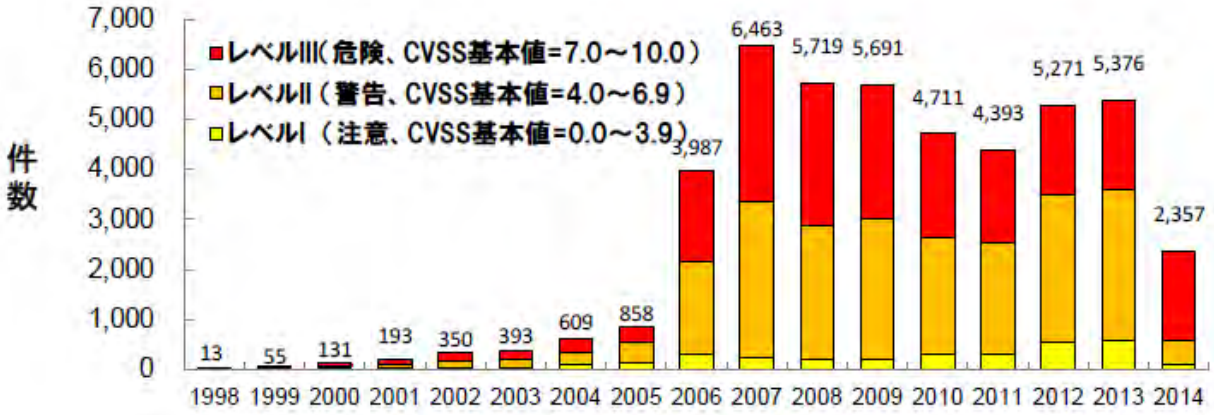


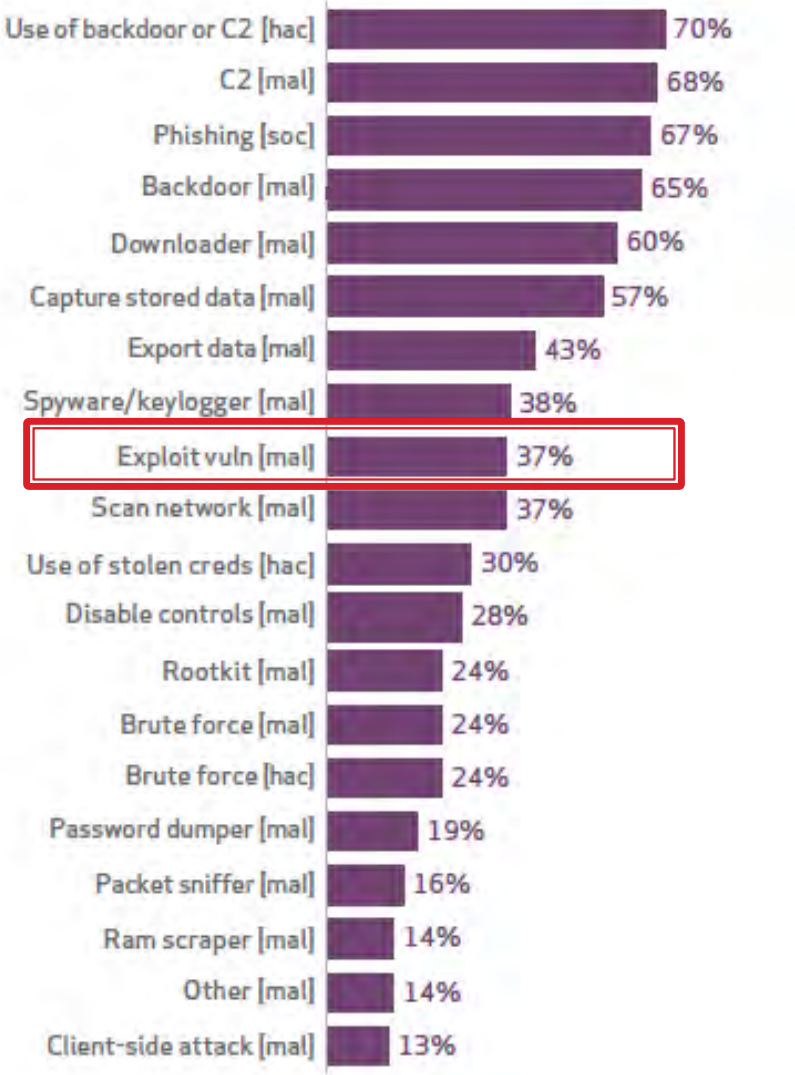
図2-2. 脆弱性の深刻度別件数

IPA 「情報システム等の脆弱性情報の取扱いに関する研究会 報告書」より引用

攻撃ツールを活用した攻撃

- Exploitによる脆弱性を利用した攻撃の多発

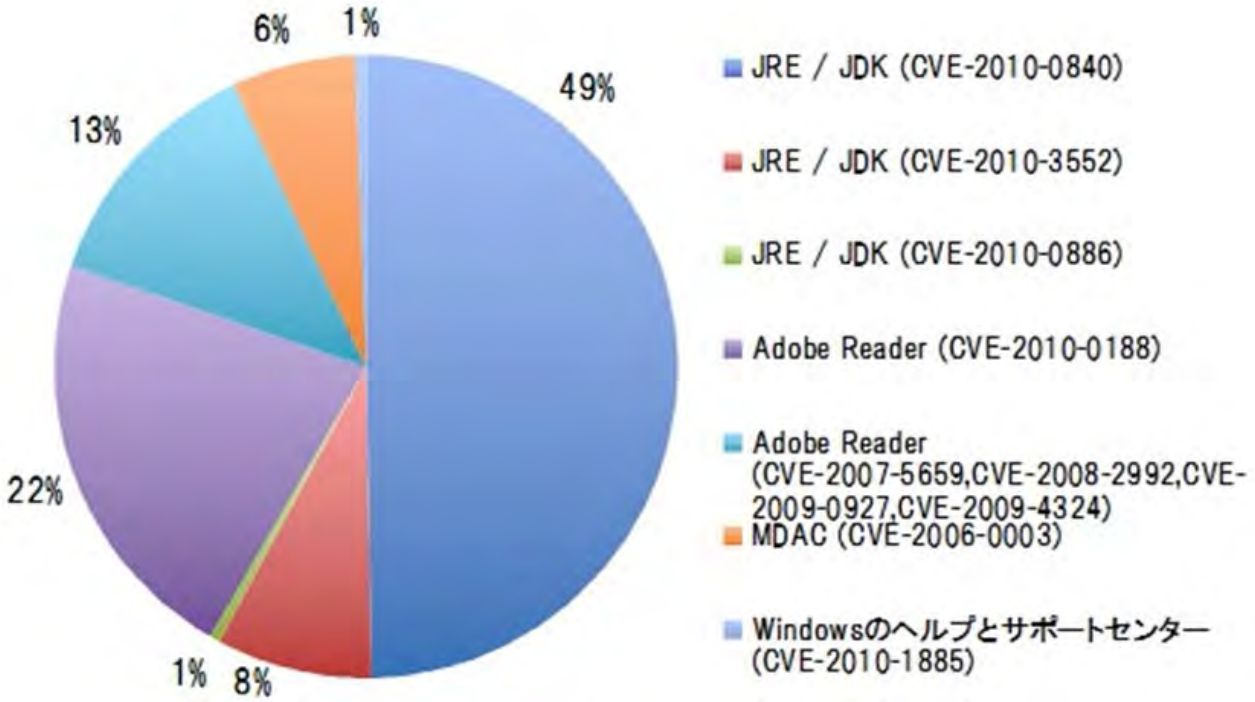
【事例】
MS13-022/CVE-2013-0074のSilverlightの脆弱性ですが、MSからのパッチ提供時(2013/3/13)は、
攻撃はなかった。
ところが、この脆弱性は、2013年11月に攻撃ツールキットに組み込まれた以降は広範に活用されている



※トレンドマイクロ社より

攻撃ツールで利用される脆弱性の例

- 攻撃ツール（Exploit Kit）が闇市場で流通。Webサイトを活用した攻撃手段などが提供されている。



http://itpro.nikkeibp.co.jp/article/COLUMN/20110904/368103/

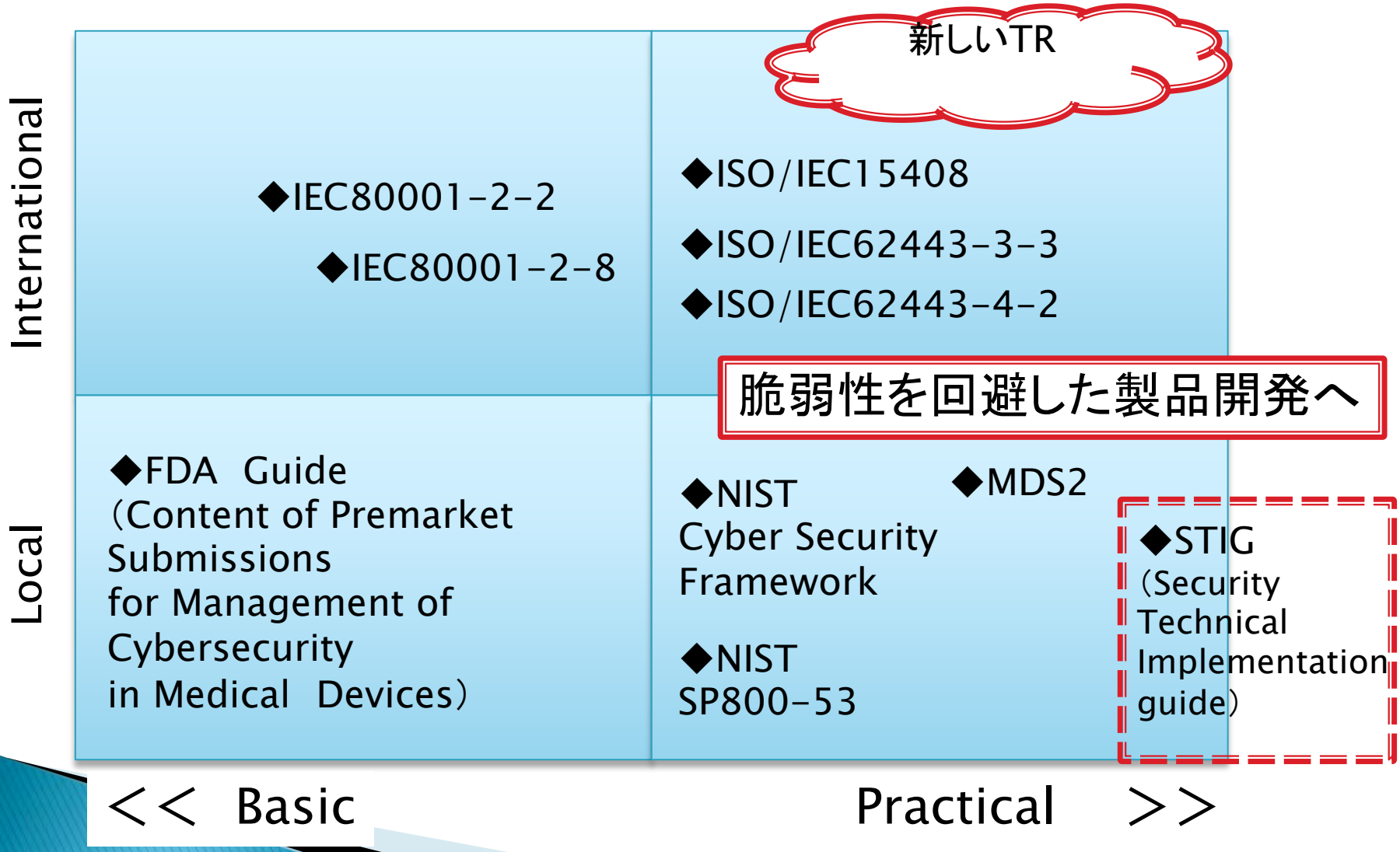
規格(CC)と脆弱性への対応

評価
ISO15408(Common Criteria)などによる評価

実装
何をしたら良いの？
ベストプラクティスは？

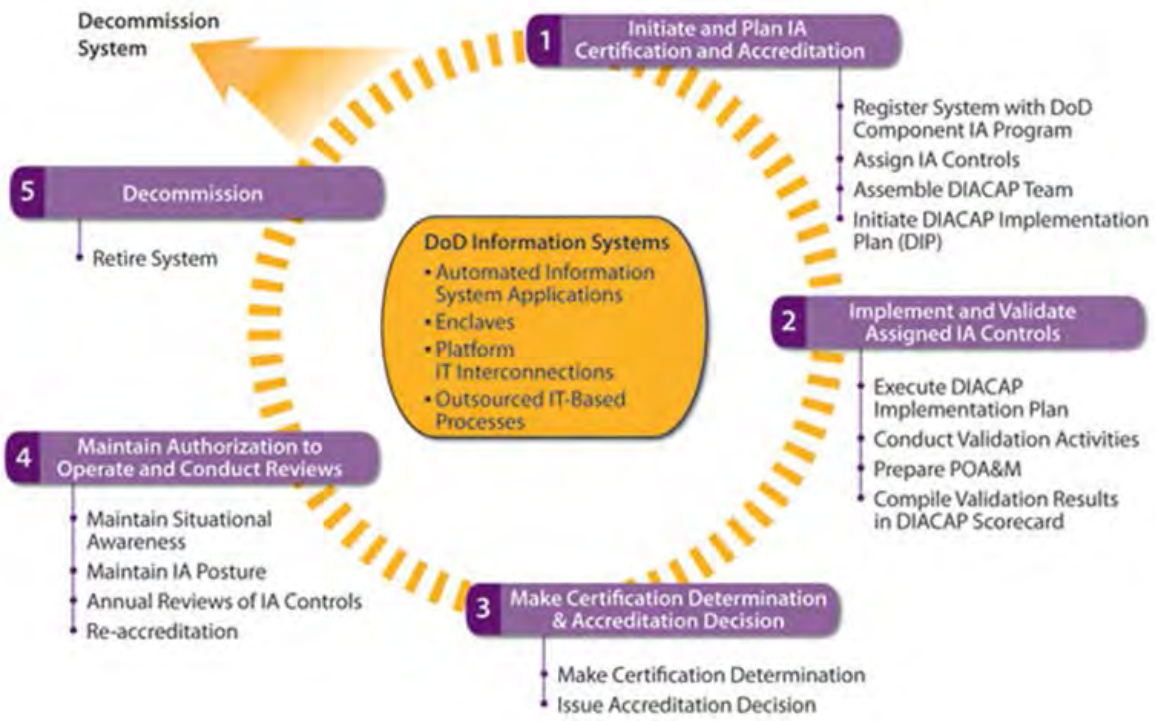
IEC80001-2-X
セキュリティTRの必要性(具体性が欲しい)
@軽井沢会議

新しいTR（技術報告書）の位置づけ



脆弱性を回避した製品の開発（1）

- DIACAP（**DoD Information Assurance Certification and Accreditation Process**）
  - DoD（米国：Department of Defense）での情報システムのリスクマネジメントの適用プロセス
  - 対象となる機器は、セキュリティガイドライン（STIG：Security Technical Implementation Guide）に従うことが要求される



脆弱性を回避した製品の開発(2)

- STIG(Security Technical Implementation Guide)
  - NIST(National Institute of Standard and Technology)のNCPR(National Checklist Program Registry)に105件のSTIG登録
  - STIGの例(Windows7製品の最小チェック項目)
    - Windows 7　STIG　Version 1　Release 15
      - Windowsの各種設定などに関するガイド。ここで定義される内容の多くは、SCAP, Retinaなどのツールでの評価が可能
    - Application Security and Development checklist
      - チェック項目は157個のテック項目からなる。対象範囲はアプリケーションのドキュメント、設計、開発プロセス、テストなど多岐に渡る

脆弱性を回避した製品の開発(3)

- Windows 7 STIG の記載例

具体的な実施項目の記載

Group ID (Vulid): V-1072
Group Title: Shared User Accounts
Rule ID: SV-25000r1_rule
Severity: CAT II
Rule Version (STIG-ID): 1.008
Rule Title: Shared user accounts are permitted on the system.

Vulnerability Discussion: Shared accounts do not provide individual accountability for system access and resource usage.

Responsibility: System Administrator
IAControls: IAGA-1

Check Content:
Interview the SA to determine if any shared accounts exist.

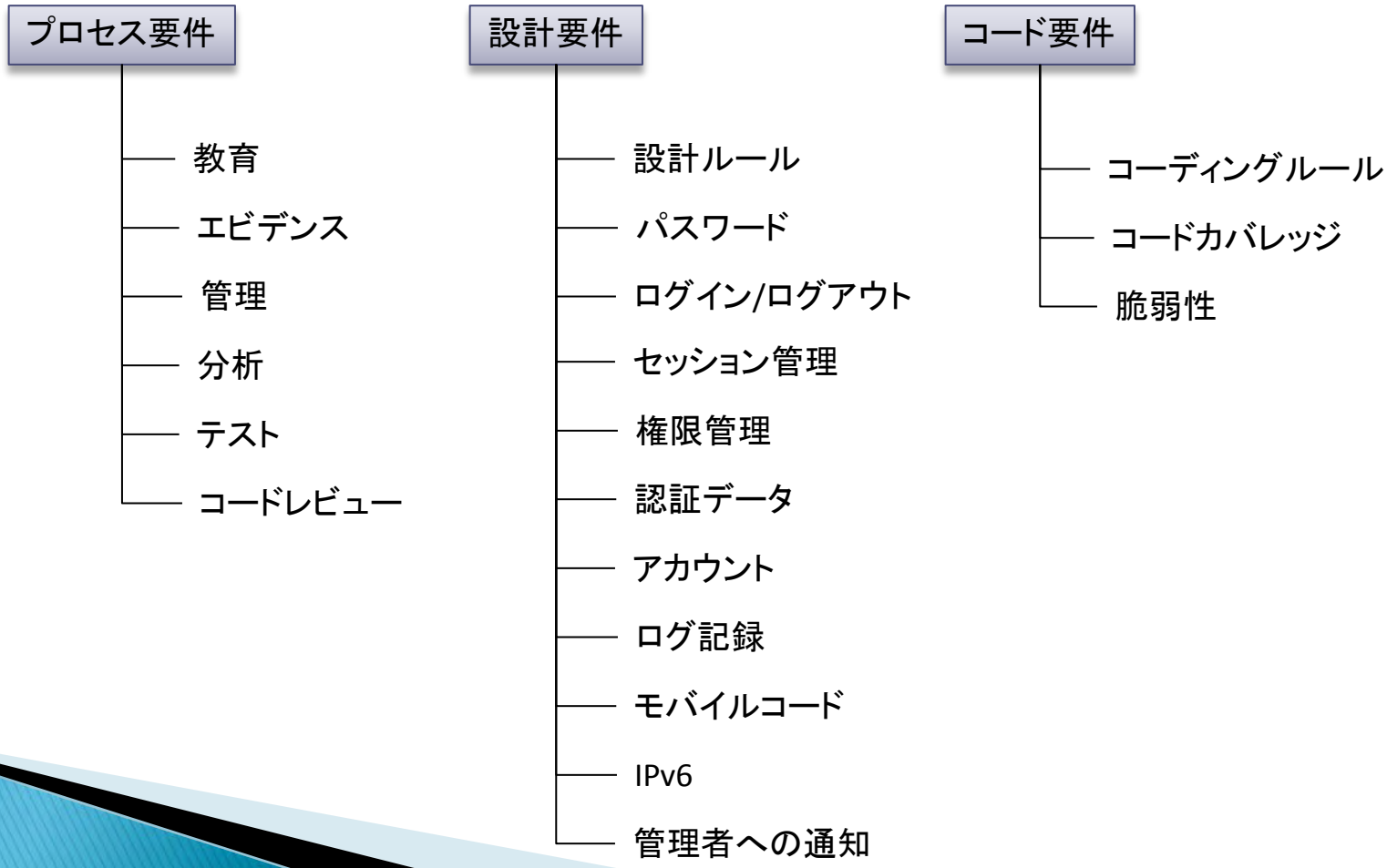
Any shared account must be documented with the IAO. Documentation should include the reason for the account, who has access to this account, and how the risk of using a shared account (which provides no individual identification and accountability) is mitigated.

Note: As an example, a shared account may be permitted for a help desk or a site security personnel machine, if that machine is stand-alone and has no access to the network.

Fix Text: Remove any shared accounts that do not meet the exception requirements listed.

脆弱性を回避した製品の開発(4)

- Application Security and Development checklistの構成



まとめ

まとめ：本日の内容

- サイバー・セキュリティ・リスクの現状
  - 大きな社会問題の1つとして認知されている。
  - サイバー・セキュリティへの脅威を現実のものとして受け入れる必要がある（実際の脅威事例）
  - サイバー空間、プロダクト、ヒト・プロセス
- サイバー・セキュリティに関連する国際規格の動向
  - セキュアな製品を製造する（各種規格・ガイドの存在）
  - ユーザはセキュリティ・リスクを管理することが必要であり、製造者はそれを支援する必要がある（IEC80001-X）
- サイバー・セキュリティへの対応の課題
  - リスク低減に向けた規程・ガイドに従った脆弱性対応
  - 新しい国際規格の可能性

まとめ：次の社会の発展の為に・・

【国家安全保障戦略（抜粋）】

近年、海洋、宇宙空間、サイバー空間といった国際公共財（グローバル・コモンズ）に対する自由なアクセス及びその活用を妨げるリスクが拡散し、深刻化している。

（中略）

また、情報システムや情報通信ネットワーク等により構成されたグローバルな空間であるサイバー空間は、社会活動、経済活動、軍事活動等のあらゆる活動が依拠する場となっている。

- 社会の次の発展の為には・・・・・

  サイバー空間自体の安全性とサイバー空間を活用する人・モノの安全に対する対応力の向上させ、脅威を把握・共有・対応すること

国際規格の発展・規制のハーモナイゼーション

End