医療機器ソフトウェア規制の国際動向シンポジウム

医療用ソフトウェア
TC62における国際規格等の動向

※本資料の一部には、引続き検証が必要な情報が含まれています

2013年3月19日

IEC TC62 SNAG 委員
TC62 SC62A/JWG3 委員

東芝メディカルシステムズ（株）
中里俊章

IEC TC 62 スコープ改正 – September, 2011 Nuremberg meeting –

- TC62 CAG submitted the revised scope and discussed

To prepare international standards and other publications concerning electrical equipment, electrical systems and software used in healthcare and their effects on patients, operators, other persons and the environment.

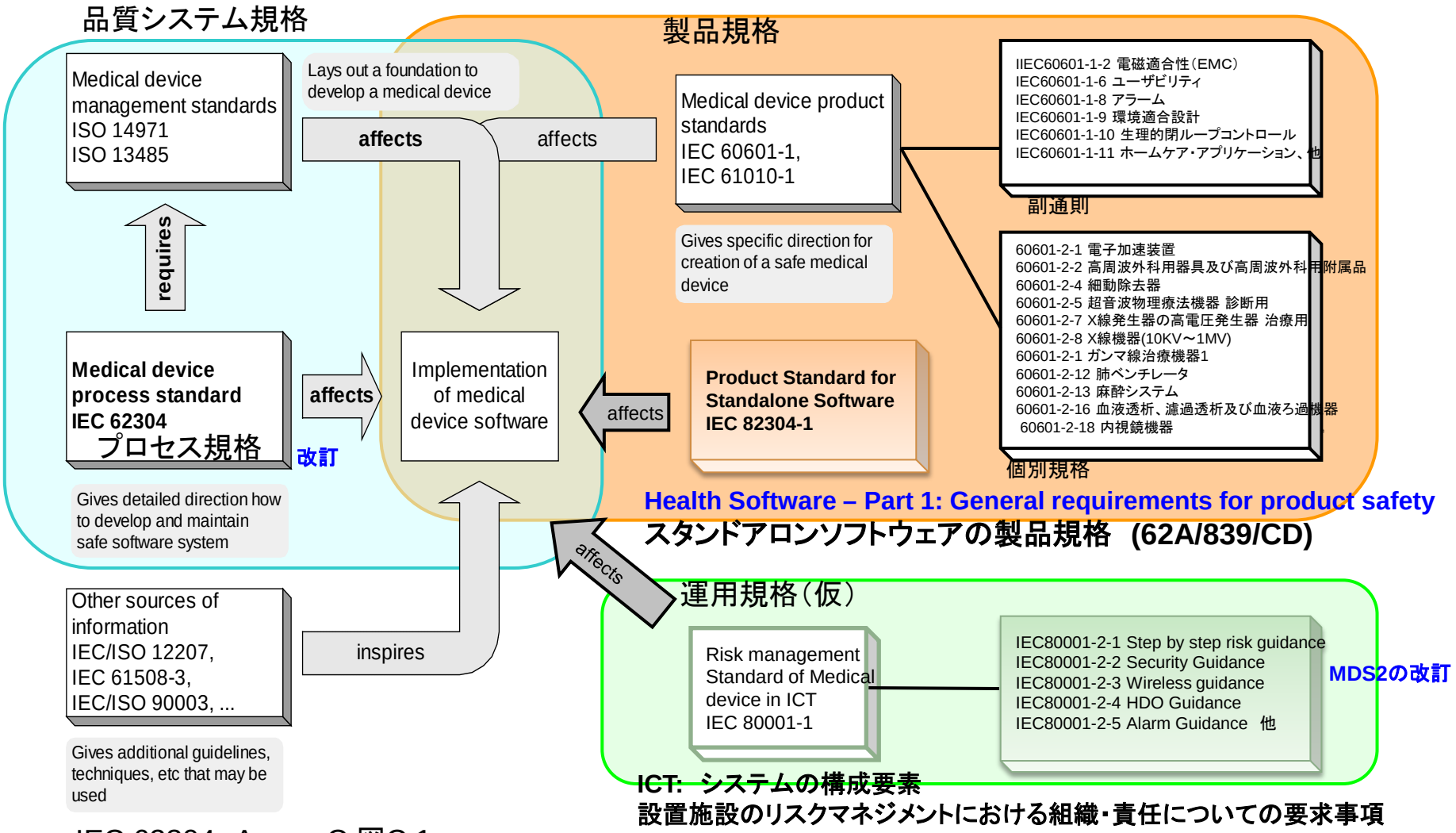
NOTE: This scope includes items that are also within the scopes of other committees and will be addressed through cooperation. Attention will **focus on safety and performance** (e.g. radiation protection, data security, data integrity, data privacy and environmental aspects) and will **contribute to regulatory frameworks**.
Healthcare includes medical practice as well as emergency medical services, homecare, and support of persons with disabilities in their daily lives (i.e. Ambient Assisted Living).

「安全と性能」にフォーカスすることを改めて宣言。
既に検討している領域を含め、活動領域の拡大を図るため、用語“Healthcare”を用いている。
Healthcareは、従来の医療分野に加え、救急医療、在宅医療、看護･介護、高齢者支援を含んでいる。審議中の規格 IEC 82304-1では、“Healthcare”から“Health Software”までスコープを拡大する動きがある。

MDRの制定に向けた動きが活発化

ソフトウェア関連規格と構成（ISO/IEC） - TC 210/215とのJWG -

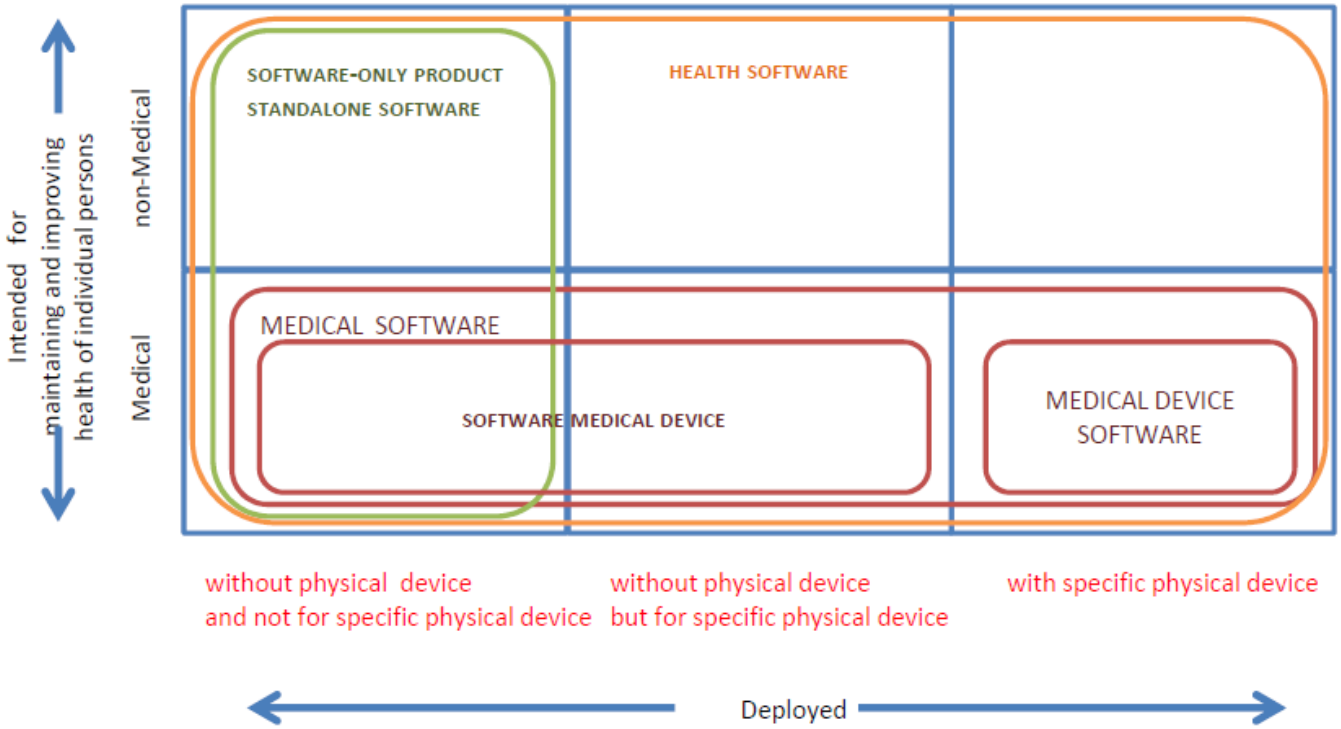
■ 品質システム規格、製品規格と運用規格



IEC 62304 Annex C 図C.1

IEC 82304-1： 医療用ソフトウェアの製品規格(62A/839/CD)

- IEC 82304-1:
  Health Software – Part 1: General requirements for product safety



1 Scope

This International Standard applies to the entire lifecycle including design, manufacture, installation, maintenance, and disposal of HEALTH SOFTWARE.

NOTE This standard provides no requirements for software embedded in a medical device.

HEALTH SOFTWARE
software intended to be used specifically for maintaining or improving health of individual persons, or the delivery of care

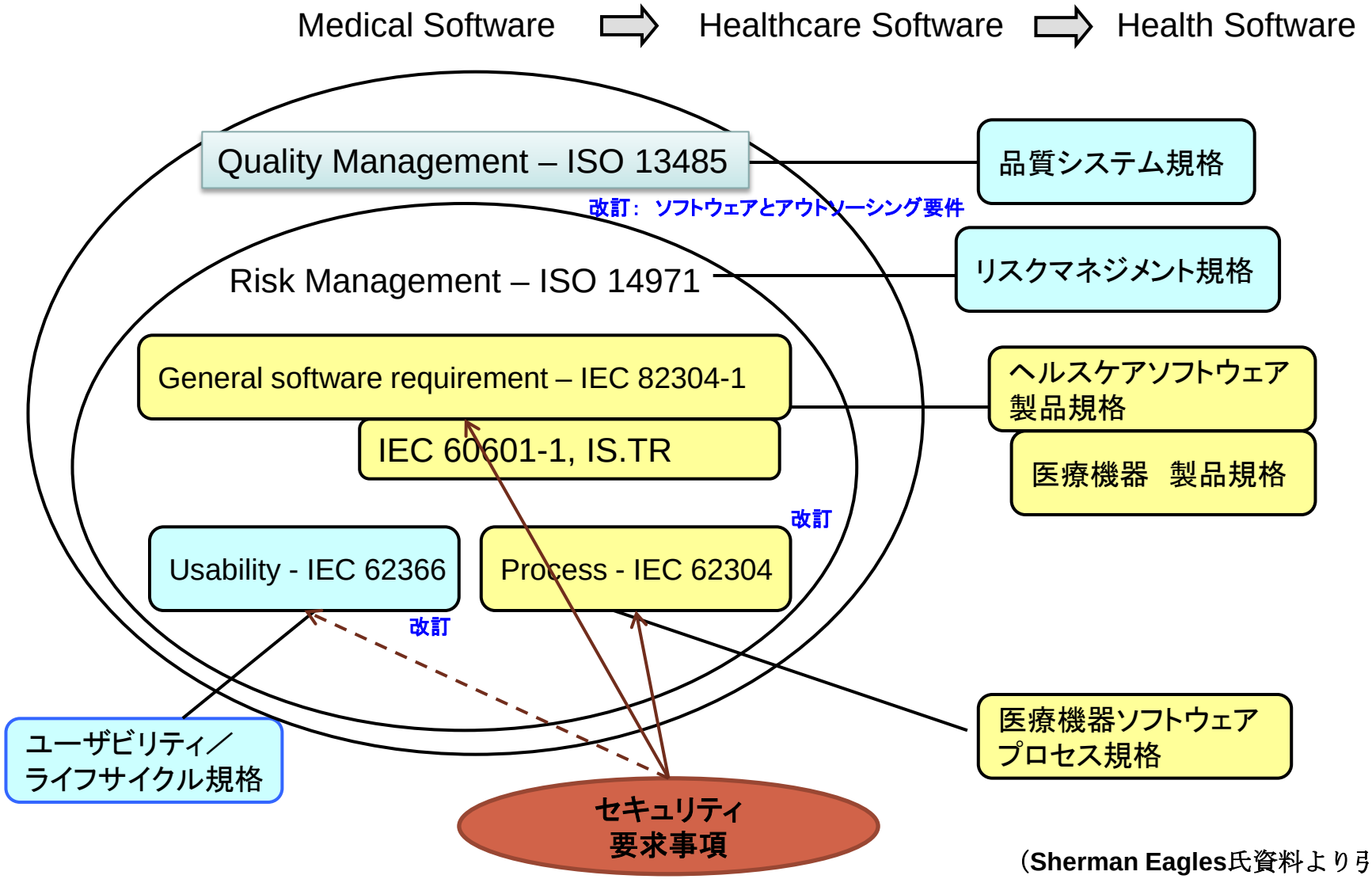
MEDICAL DEVICE SOFTWARE
software intended to be used specifically for incorporation into a physical medical device

MEDICAL SOFTWARE
software intended to be used specifically for incorporation into a physical medical device or intended to be a SOFTWARE MEDICAL DEVICE

SOFTWARE MEDICAL DEVICE
software intended to be a medical device in its own right

SOFTWARE-ONLY PRODUCT STANDALONE SOFTWARE
for the purpose of this standard, software which is not intended for incorporation in another product at the time of its placing on the market or its making available

医療用ソフトウェアの参照規格（認証目的）



（**Sherman Eagles**氏資料より引用）

医療機器の安全性と有効性に悪影響を及ぼすセキュリティリスク

- 医療機器の脆弱性を不正利用
  - 機器設定の不正変更
  - 治療の不正変更または無効化
  - 機密データの喪失または開示
  - 機器の誤動作

GAO

United States Government Accountability Office

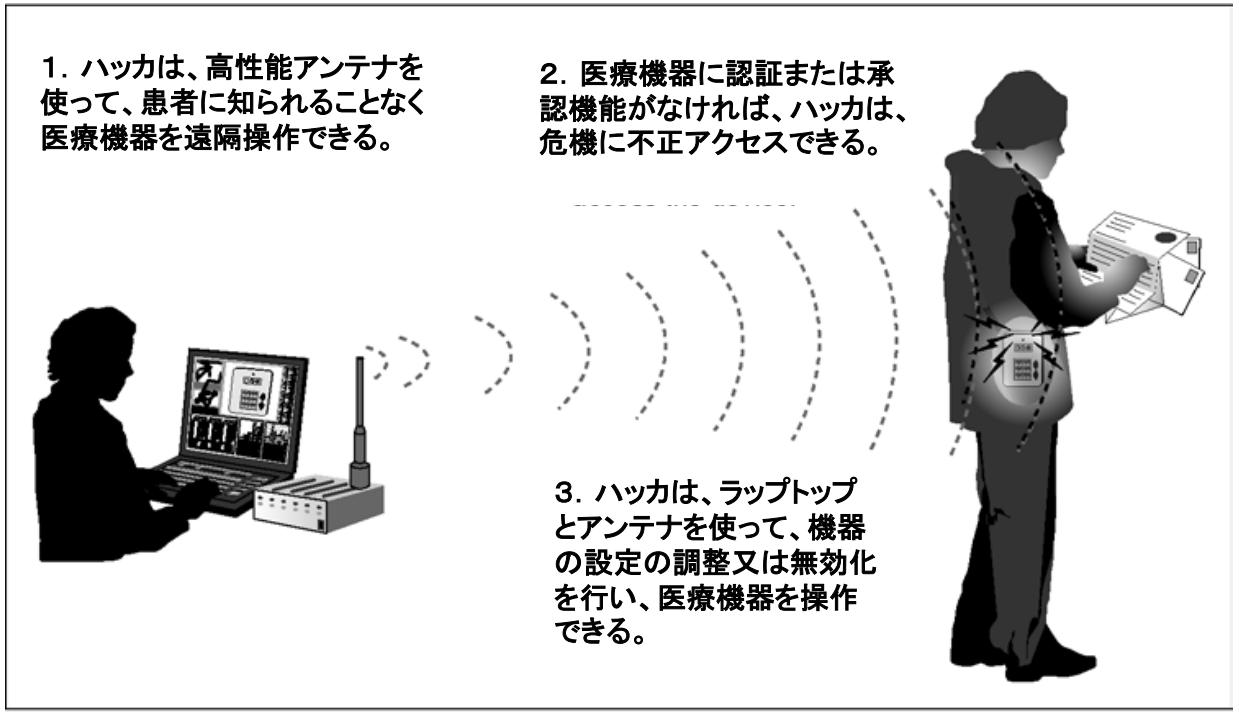
Report to Congressional Requesters

August 2012

MEDICAL DEVICES

FDA Should Expand Its Consideration of Information Security for Certain Types of Devices

2011年
セキュリティ専門家が
遠隔操作で不正利用し、
インスリンポンプの投与量
を変更できることを実証



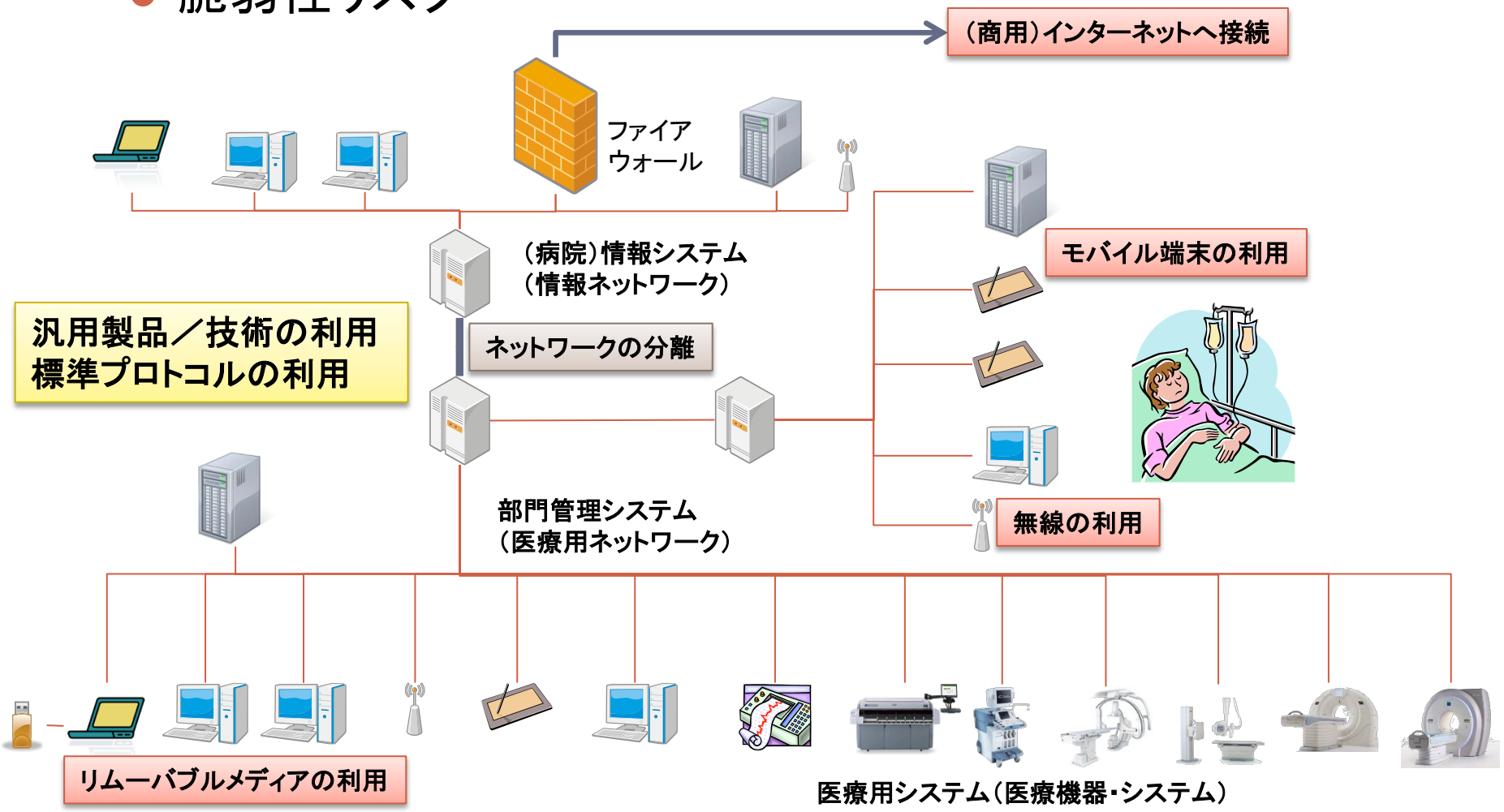
Source: GAO.

遠隔操作によるインスリンポンプの不正アクセスの例
（GAOレポート： http://www.gao.gov/products/GAO-12-816 ）

情報システムと医療用(ネットワーク)システム

■ オープン化が加速する医療用システム

- 脆弱性リスク

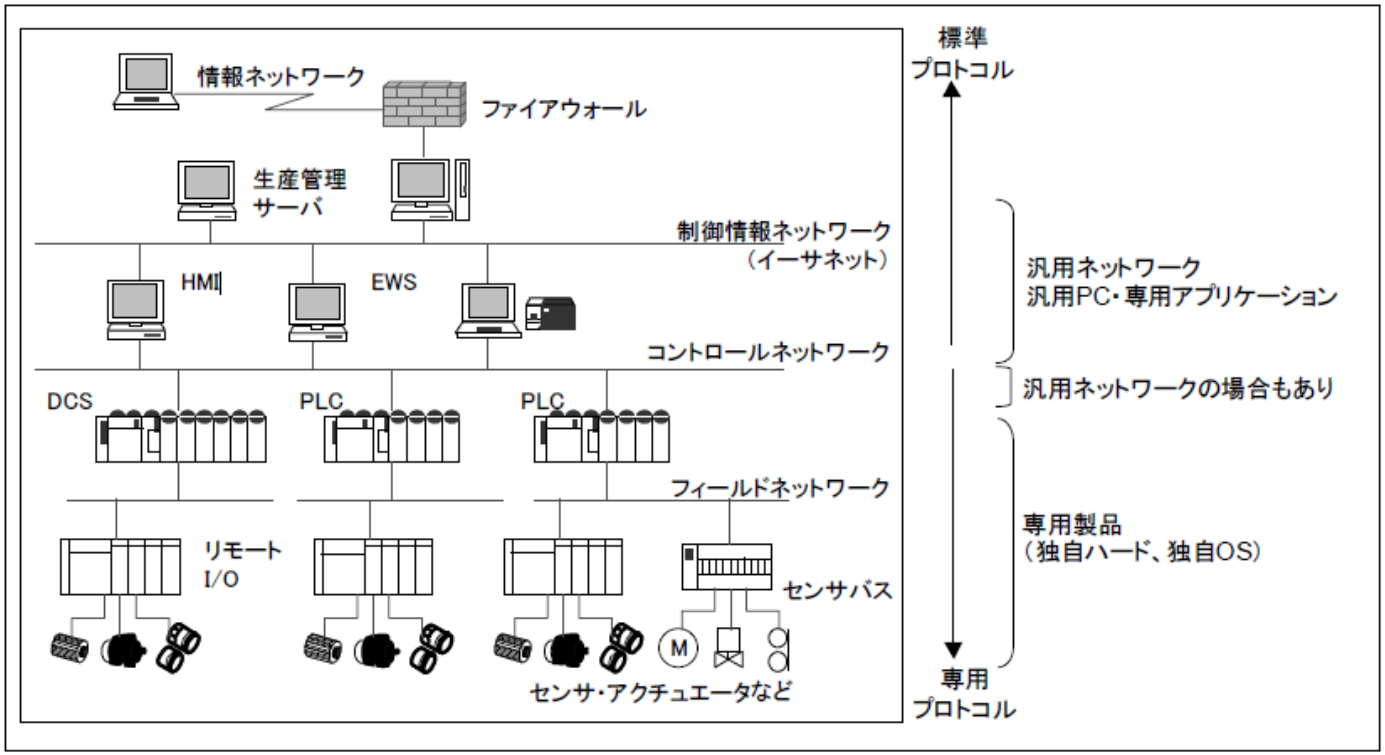


制御システム

■ 制御システムのオープン化とセキュリティが話題

- 交通／航空管制、公共エネルギー供給、工場の製造ラインの重要インフラで使用

図表 2-4 制御システムの構成例



資料：JEMIMA 資料ほか各種資料より作成

重要インフラの制御システムセキュリティとITサービス継続に関する調査
2009年3月より引用
独立行政法人　情報処理推進機構　セキュリティセンター

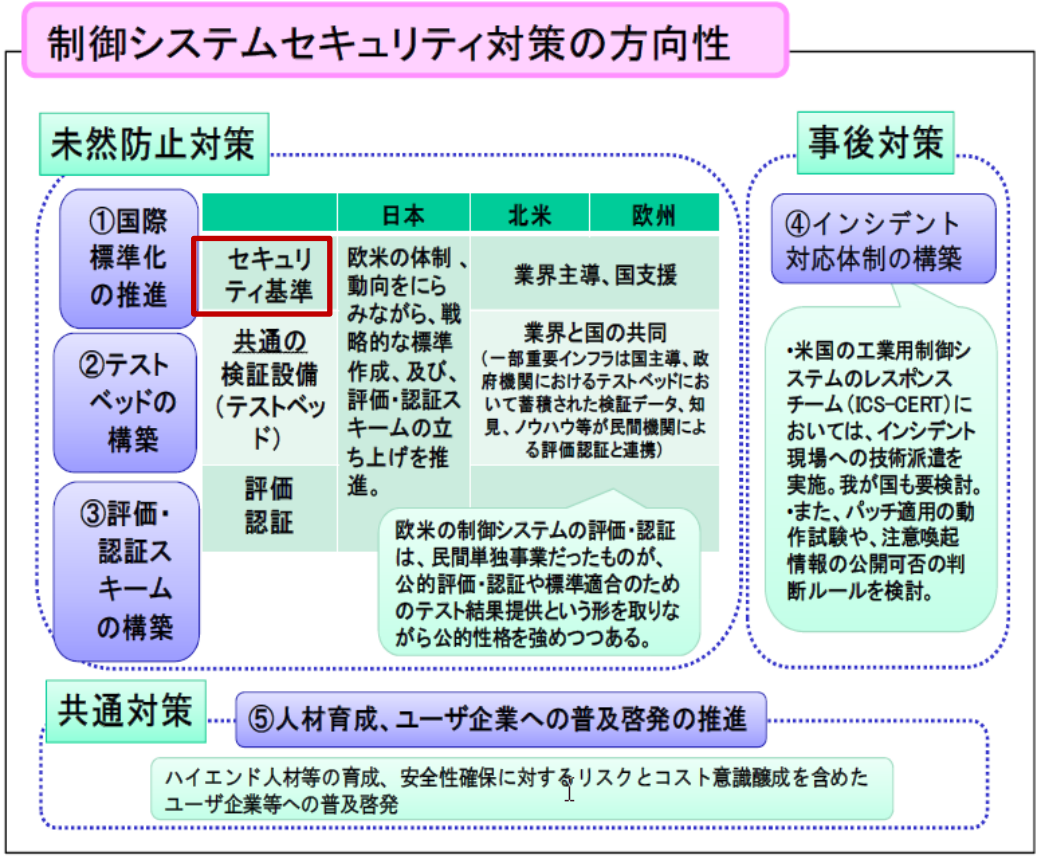
制御システムと医療用システム

セキュリティ問題への取組みが本格化

- 制御システムと情報（コンピュータ）システムとの本質的な違いは？
  - 物理的な設備や施設を基軸
  - 情報システムとは無関係に導入
  - 構造的には情報システムと大差ない

JPCERT/CC　2013
「制御システム・セキュリティ 2012年度の動き 」より

- 医療用システムと制御システムとの本質的な違いは？
  - 患者安全を最優先
  - 安全・性能に係る変更は、法規制に従って適切に管理される
  - **ライフサイクルが長い点等で共通課題が多い**



経済産業省 「制御システム・セキュリティ・タスクフォース」 中間とりまとめ (2012年6月1日)より引用
http://www.meti.go.jp/committee/kenkyukai/shoujo/controlsystem_security/report01.html

医療用システム　－　可用性／長期運用　－

- 制御システム：　交通／航空管制、公共エネルギー供給、工場の製造ライン等、24時間365日稼働すること要求されるシステムをいう。
  - 制御システムにおけるセキュリティ　IEC 62443シリーズ

- 医療用システムは安全性重視
  - 特徴1：可用性を重視する
    - セキュリティ対策として非常に重要なOSやアプリケーションのタイムリーな更新が困難である
    - 修正プログラムの適用は、必要最小限にして、安定動作を優先する
  - 特徴2：長期運用が前提である
    - OTSソフトウェアサポートが終了し、修正プログラムを適用できず、脆弱性が存在するシステムとなる
  - 特徴3：データ送受信はリアルタイムである
    - パフォーマンスへの影響は最小限に抑える
  - 特徴4：管理部門が情報システム部門ではない
    - ME、責任部門、医療IT ネットワークのリスク管理者（IEC 80001-1）

	制御システム	情報システム
セキュリティ優先順位	A.I.C（可用性重視）※	C.I.A（機密性重視）※
被害の結果	最悪の場合、人命損失。被害は一般的に甚大となる傾向	金銭的損失、プライバー被害
可用性	24時間365日の安定稼働（再起動不可）	通常業務時間内の稼働（再起動は許容範囲）
運用期間	20年以上	3～5年
システム上を流れるデータの処理速度	リアルタイムなデータ送受信	遅延による被害は少ない
パッチ提供サイクル	制御機器ベンダーごとに不定期。長期間間隔で実施（1～4年程度）	頻繁・定期的
運用管理	現場技術者部門	情報システム部門
セキュリティに関する意識	現実に被害が発生し始めているため、高まりつつある	基本的に対策済み
セキュリティに関する標準化	国レベルで検討開始	標準が確立されている
セキュリティの対象	モノ（設備、製品）、サービス（連続稼働）	情報

出典：重要インフラの制御システムセキュリティとIT サービス継続に関する調査（情報処理推進機構セキュリティセンター）
※　C:Confidentiality＝機密性、I:Integrity＝完全性、A:Availability＝可用性

一般的な制御システムと情報システムの違い

トレンドマイクロ社提供

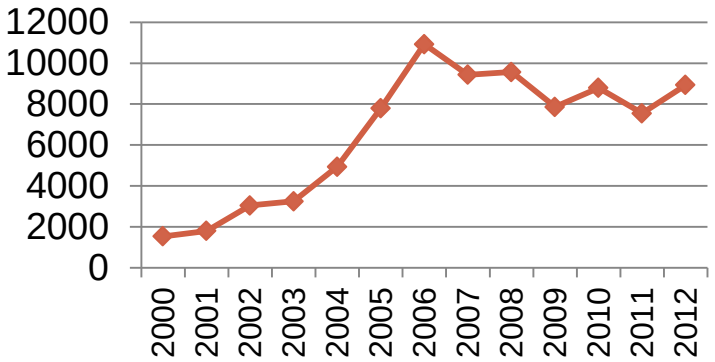
医療用システムのオープン化の背景

- 在宅医療、遠隔医療、新たな医療の提供
  - 汎用技術の応用／組込み技術との併用
    - デバイスの制御の必要性などから、安定動作を意図し、**ソフトウェアを管理者権限で動作（実行）させることが多い**
  - OSを含むOTSソフトウェアの利用
  - インターネット接続
  - モバイルアプリケーション
- 緊急時に機器へアクセスできる必要性
  - TCP/IPベースのプロトコル採用
- 相互運用性の重視
  - オープンな通信プロトコル（標準プロトコル）採用

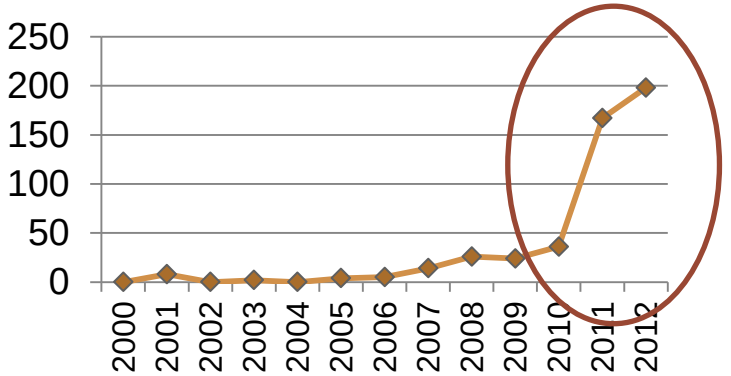
サイバー攻撃の難易度が低下： 本質的なセキュリティ確保が急務 （規制強化）

特別ではなくなる医療用システム及び組込みシステム

- 医療用システムも、インターネットに直接接続する、若しくは接続することで機能するシステムになり、セキュリティ対策、脆弱性対策が要求され始めた。
- 医療用システムは、ソフトウェアのパッチや修正が容易ではないため、セキュリティ対策の遅延／見送りが懸念される。
- 機器のモバイル化、情報連携（相互運用性）の強化により、リスクは増加している。



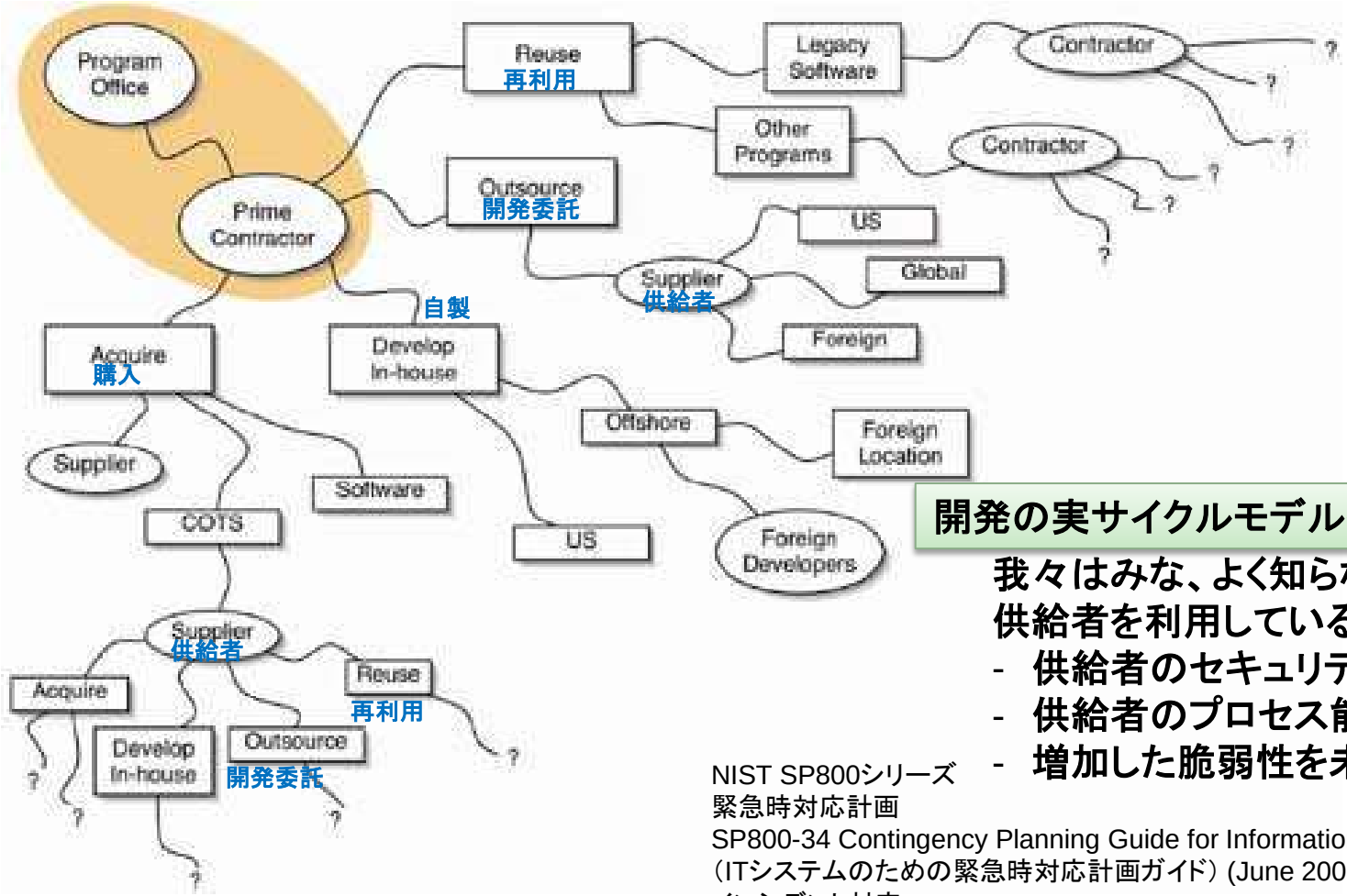
脆弱性データベースOSVDBに登録される脆弱性の年別発見件数



産業用制御システムに関するソフトウエアの脆弱性件数の年別推移

※OSVDB： 脆弱性に関するオープンソースのデータベースを構築しているプロジェクト「Open Source Vulnerability Database」

グローバル調達(開発)による変化　NIST(米国国立標準技術研究所)



13th Semi-Annual Software Assurance (SwA) Forum @NIST HQS 27 Sep – 1 Oct 2010 資料より引用

開発の実サイクルモデルを基に、課題を抽出

我々はみな、よく知らない、会う事すらない供給者を利用している。

- **供給者のセキュリティ能力に無関心**
- **供給者のプロセス能力監視を見実施**
- **増加した脆弱性を未確認**

NIST SP800シリーズ
緊急時対応計画
SP800-34 Contingency Planning Guide for Information Technology Systems (ITシステムのための緊急時対応計画ガイド) (June 2002)
インシデント対応
SP800-61 Computer Security Incident Handling Guide (January 2004) (コンピュータインシデント対応ガイド)
SP800-83 Guide to Malware Incident Prevention and Handling (November 2005) (不正プログラムインシデント防止・対応ガイド)

Windows XP搭載の医療機器の販売

2013年3月19日 現在、
もし、Windows XPをOSとして搭載する医療機器製品を米国で販売するとしたら？

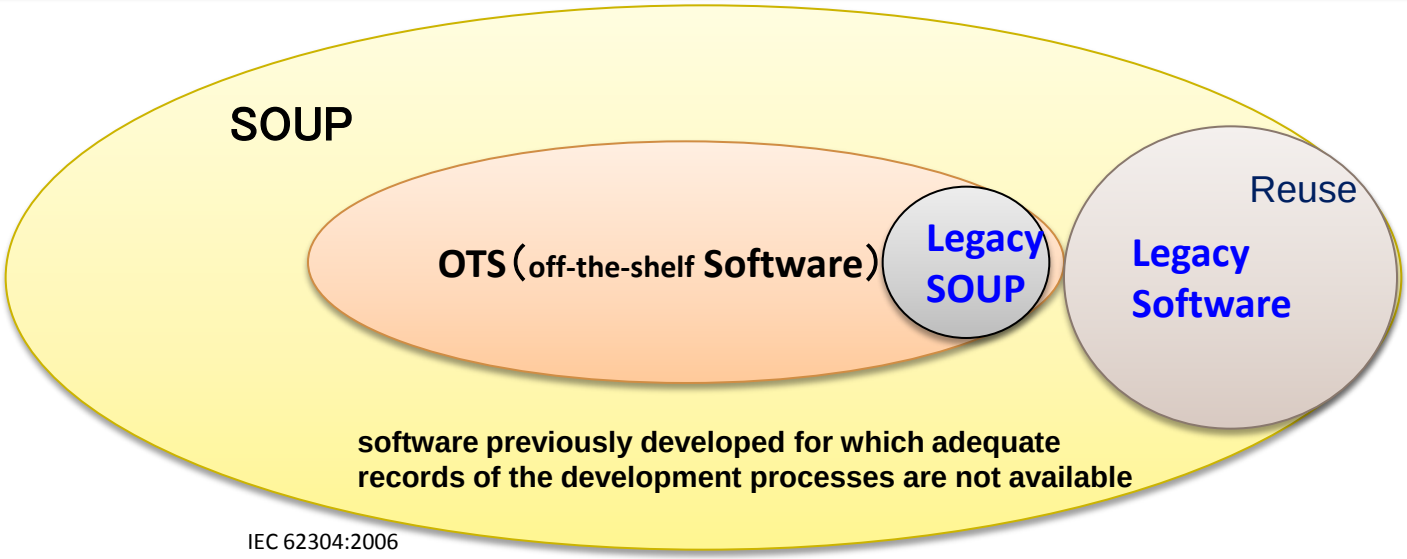
どのような課題があるか考えて見ましょう。
（米国政府調達のケース）

課題1．製品のライフサイクル　Legacy Software

IEC 62304 Ed.2　3.11 LEGACY SOFTWARE

MEDICAL DEVICE SOFTWARE which **was legally placed on the market** but for which there is insufficient objective evidence that it was developed in conformance with the current version of the standard.

- MEDICAL DEVICE software being legally on the market and that shall be currently introduced into the market without changes, but that were not developed using the development lifecycle processes of IEC 62304 (so called legacy software);
- MEDICAL DEVICE software being legally on the market and that shall be currently introduced into the market, but requiring small changes (maintained legacy software);



Windows ライセンス・サポート終了日

製品名	製品発売日	メインストリーム サポート終了日	延長サポート終了日 (セキュリティパッチ提供終了)
Windows NT 4.0 Workstation	1996 年 7 月 29 日	2002 年 6 月 30 日	2004 年 6 月 30 日
Windows NT 4.0 Server	1996 年 7 月 29 日	2002 年 6 月 30 日	2004 年 12 月 31 日
Windows NT 4.0 Embedded	1999 年 8 月 30 日	2003 年 6 月 30 日	2006 年 7 月 11 日
Windows 2000 Professional	2000 年 3 月 31 日	2005 年 6 月 30 日	2010 年 7 月 13 日
Windows 2000 Server	2000 年 3 月 31 日	2005 年 6 月 30 日	2010 年 7 月 13 日
Windows XP Professional	2001 年 12 月 31 日	2009 年 4 月 14 日	SP2 : 2010 年 7 月 13 日 SP3 : 2014 年 4 月 8 日
Windows XP x64 Edition	2005 年 4 月 25 日	2009 年 4 月 14 日	2014 年 4 月 8 日
Windows XP Embedded	2002 年 1 月 30 日	2011 年 1 月 11 日	2016 年 1 月 12日
Windows Embedded Standard 2009	2008 年 12 月 14 日	2014 年 1 月 14 日	2019 年 1 月 8 日
Windows Server 2003 *3	2003 年 5 月 28 日	2010 年 7 月 13 日	2015 年 7 月 14 日
Windows Server 2003 R2 *3	2006 年 3 月 5 日	2010 年 7 月 13 日	2015 年 7 月 14 日
Windows Vista Business / Ultimate	2006 年 11 月 10 日	2012 年 4 月 10 日	2017 年 4 月 11 日
Windows Server 2008 *3	2008 年 5 月 6 日	2013 年 7 月 9 日	2018 年 7 月 10 日
Windows 7 Professional / Ultimate	2009 年 10 月 22 日	2015 年 1 月 13 日 *1	2020 年 1 月 14 日 *2
Windows Server 2008 R2*3	2009 年 10 月 22 日	2015 年 1 月 13 日 *1	2020 年 1 月 14 日 *2
Windows 8 Pro.	2012 年 10 月 30 日	2013 年 1 月 9 日 *1	2023 年 1 月 10 日 *2

*1 後継製品の発売後、2年間提供
*2 メインストリームサポート終了後、5年間提供
*3 各Edition共通

2014年問題： Windows XPの
セキュリティパッチが公開されなくなる

米国政府調達を中心に
Windows 7化の要求

課題2．FISMA （連邦情報セキュリティマネジメント法）対応

FISMA：連邦情報セキュリティマネジメント法）
情報セキュリティに係る規格/技術文書の策定、実装、運用を行うことにより、情報及び情報システムのセキュリティ強化を米連邦政府機関に義務付ける
“Each federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…”
--- **Federal Information Security Management Act of 2002 (*Title III of the E-Government Act*)**

NISTのFISMA導入プロジェクト
目的：連邦政府の情報セキュリティ強化に寄与する（FISMAの順守）
フェーズI： FISMA関連のセキュリティ基準（FIPS）およびガイドライン(SPシリーズ)の開発
フェーズII： セキュリティサービスプロバイダ認定プログラムの開発（2006年より開始）
フェーズIII：セキュリティ・ツール検証プログラムの開発（2010年頃より開始）

DIACAP： DoD 米国国防総省の情報セキュリティ強化プログラム
政府機関向けセキュリティ基準（FDCC）に比べ、より堅固な基準と評価プロトコルから構成されている。（ATO取得が、応札の条件）

予想される影響範囲

PIT/SCAPによる脆弱性評価

- **セキュリティ対策を実施**
  - **OSを含めたポリシーの設定**
  - **パッチの適用**
  - **ウィルスプロテクトソフトの利用**
- ツールによるスキャンを実施
- STIG（基準）チェックリストを評価・作成して、申請
- ATO(セキュリティ認定)を取得

SCAP tool
（SCAP Compliance Checker）

実行権限の適切な管理

管理者権限による動作の最小限化

Retina S/W Installed on laptop or program can be installed on the system

TCP/IP network

STIGチェックリスト

	A	B	C	D	E
1	NOTE: The accreditation for this system is for this configuration only. Any deviation, or change to the configuration will invalidate the accreditatio				
2	IA Control	Title	Area	Description	Answer
21	ECCT-1	Encryption for Confidentiality (Data at Transmit)	Enclave Computing Environment	Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography (See also DCSR-2).	
22	ECLO-2	Logon	Enclave Computing Environment	Successive logon attempts are controlled using one or more of the following: ・Access is denied after multiple unsuccessful logon attempts. ・The number of access attempts in a given period is limited. ・A time-delay control system is employed. If the system allows for multiple logon sessions for each user ID, the system provides a capability to control the number of logon sessions.	Yes No N/A Inherited
	ECRC-1	Resource Control	Enclave Computing Environment	All authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system. There is absolutely no residual	

Table of Contents | Section 1 – General Information | Section 2 – IA Controls | Section 3 – 802.11 Wireless | Section 4 – Bluetooth

DIACAP関連用語集

略語	正式名称	説明
DoD DIACAP	Department of Defense	米国国防総省. 米国国防総省や米軍関連施設向けシステム入札要件. Defense Information Assurance Certification and Accreditation Program
PIT	Product Implementation Test	米軍関連施設の入札リストに載るための事前試験. 一度合格すると3年間再試験不要. OS改変時は再度試験を受ける必要あり. 合格基準は不明. 試験基準はSTIG: 1.OSのセキュリティ設定が基準に沿って行われていること 2.プログラムの脆弱性に適切に対策がされていること
STIG	Security Technical Implementation Guide	OS含むソフトウェアとハードウェアに対する, 導入と維持に関するセキュリティ標準. DoD管轄のDISA(Defense Information Systems Agency)がスポンサーで, 米軍納入基準. 達成基準, チェックツールを提供.
SCAP	Security Content Automation Protocol	脆弱性検出, 検証の自動化プロトコル. 以下要素技術より構成:
MSSCM	Microsoft Security Compliance Manager	MS提供のセキュリティポリシー管理, 更新, 編集ツール. OS/アプリ/ドメイン階層(役割)別にベースラインを提供し, IT管理者は, CCE単位にポリシー設定(適・不適・不問)が可能. 設定結果はGPOで出力し, TargetPCでGPOインストールすることで反映.
GPO	Group Policy Object	Windowsのセキュリティポリシー編集画面で設定できるポリシー. バックアップ・レストア・一括適用が可能.
FDCC	Federal Desktop Core Configuration	行政予算管理局が推進するデスクトップ設定の基準
USGCB	The United States Government Configuration Baseline	米国連邦政府にシステムを納入する場合に設定する推奨値
ATO	Approval to Operate	DIACAP下で与えられるセキュリティ認定
Retina	Retina Vulnerability Scan	eEye社のセキュリティ脆弱性スキャンツールの名称で、US Air ForceがDIACAPで使用することを認定している唯一のソフトウェア

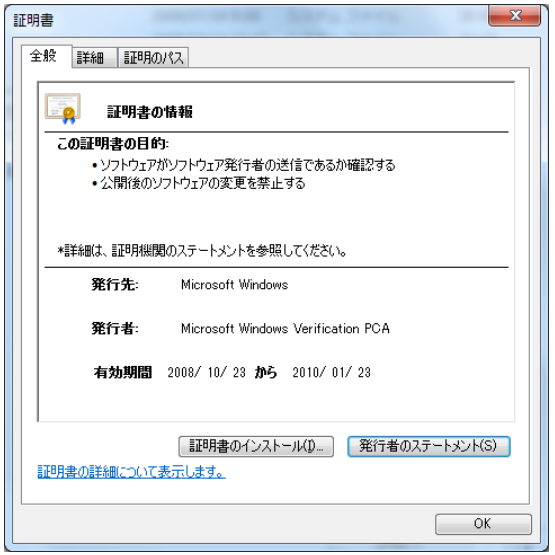
課題3. Windows 7　デジタル署名対応

- Windows Vista以降の汎用OS（Server OS含む）の動向
  - 製造業者の特定と改ざんされていない（マルウェアの混入がない）ことの確認を目的として、デジタル署名（証明書）を利用する仕組みへ移行

	OS起動時にロードされるドライバ Start = 1 (Load when booted) (例: ACPI, Disk, Network関連 etc)	左記以外のドライバ
32bit	実行するためにドライバ（.sys)の埋め込み署名が必要	実行するためにドライバの埋め込み署名が必要
64bit	実行するためにドライバ（.sys)の埋め込み署名が必要 インストールするためにカタログ（.cat）に署名が必要	インストールするためにカタログ（.cat）に署名が必要

日本マイクロソフト社
Windows7サポート情報より

  - 証明書は、第三者機関が発行し、有効期限がある。
  - **有効期限満了後は、OSレベルでロード・実行が自動停止され、機能しなくなる。**
  - ドライバ等、コード署名用証明書の有効期限は、1~3年（タイムスタンプ署名併用による期限延長策あり）
  - **ルート／中間証明書は、セキュリティパッチにより更新**
  - 製造業者が、サポート（証明書の更新）を停止すると有効期限満了となった実行ファイルは、機能しなくなる。
  - **製造用マスタ等は、証明書の有効期限による制限をうける。**
  - **ネットワーク配信を利用するソフトウェアも同じ制限を受ける。**



Windows7デジタル証明書の例

デバイスドライバのデジタル署名に関する問題

- Win7（32ビット/64ビット）について
  - 起動時に必要なデバイスドライバには、「デジタル署名」が付されており、有効期限が存在している。
  - OSは、ドライバのロード・起動時にデジタル署名の存在及び有効期限を確認しているため、デジタル署名が無い、または有効期限を超過しているドライバはロードが中断される。 その結果、正常なOSの起動ができない。
  - 登録済みの製品マスタ（メディア）も同様に有効期限の影響を受けるため、正常な起動ができない状態になったまま保管されている可能性がある。

OSプリインストールされたルート／中間証明書及び一部のデバイスドライバのデジタル証明書の更新情報は、マイクロソフト社から提供されるOSのセキュリティパッチに含まれている。

オフラインまたは閉じたネットワーク環境下で使用している機器は、証明書の更新ができない可能性があり、機器が正しく動作しなくなるリスクがある。

証明書の構成（Windows）

■ 3階層のリンク構造

（）：Windows 7 Pro 64bitsの事例　プリインストール登録件数

ルート証明書
（信頼された証明機関）

証明書 (公開鍵)

発行先	発行者	有効期限
AddTrust External CA Root	AddTrust External CA Root	2020/05/30
AffirmTrust Networking	AffirmTrust Networking	2030/12/31
Baltimore CyberTrust Root	Baltimore CyberTrust Root	2025/05/13
Class 3 Public Primary Certification Authority	Class 3 Public Primary Certification Authority	2028/08/02
Class 3 Public Primary Certification Authority	Class 3 Public Primary Certification Authority	2004/01/08
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	1999/12/31
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	2031/11/10
Entrust.net Certification Authority (2048)	Entrust.net Certification Authority (2048)	2029/07/24
Entrust.net Secure Server Certification Autho...	Entrust.net Secure Server Certification Auth...	2019/05/26
Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	2018/08/23
GeoTrust Global CA	GeoTrust Global CA	2022/05/21
GeoTrust Primary Certification Authority	GeoTrust Primary Certification Authority	2036/07/17
GlobalSign Root CA	GlobalSign Root CA	2028/01/28
Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Authority	2034/06/30
GTE CyberTrust Global Root	GTE CyberTrust Global Root	2018/08/14
http://www.valicert.com/	http://www.valicert.com/	2019/06/26
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	2000/01/01
Microsoft Root Authority	Microsoft Root Authority	2020/12/31
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	2021/05/10
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	2004/01/08
Starfield Class 2 Certification Authority	Starfield Class 2 Certification Authority	2034/06/30
Thawte Premium Server CA	Thawte Premium Server CA	2021/01/02
Thawte Premium Server CA	Thawte Premium Server CA	2021/01/01
thawte Primary Root CA	thawte Primary Root CA	2036/07/17
Thawte Timestamping CA	Thawte Timestamping CA	2021/01/01
tlstestCA	tlstestCA	2008/11/14
TOSHIBA Root CA	TOSHIBA Root CA	2038/11/15
TOSHIBA Root CA G2	TOSHIBA Root CA G2	2039/12/11
toshiba-itk	toshiba-itk	2008/11/05
VeriSign Class 3 Public Primary Certification A...	VeriSign Class 3 Public Primary Certification ...	2036/07/17
VeriSign Trust Network	VeriSign Trust Network	2028/08/02

中間証明書
（中間証明機関）

発行先	発行者	有効期限
Microsoft Windows Hardware Compatibility	Microsoft Root Authority	2002/12/31
Root Agency	Root Agency	2040/01/01
tlstestCA	tlstestCA	2008/11/14
TOSHIBA Root CA G2	TOSHIBA Root CA G2	2039/12/11
toshiba-itk	toshiba-itk	2008/11/05
www.verisign.com/CPS Incorp.by Ref. LIABIL...	Class 3 Public Primary Certification Authority	2016/10/25

Authenticode 署名

秘密鍵

コード署名

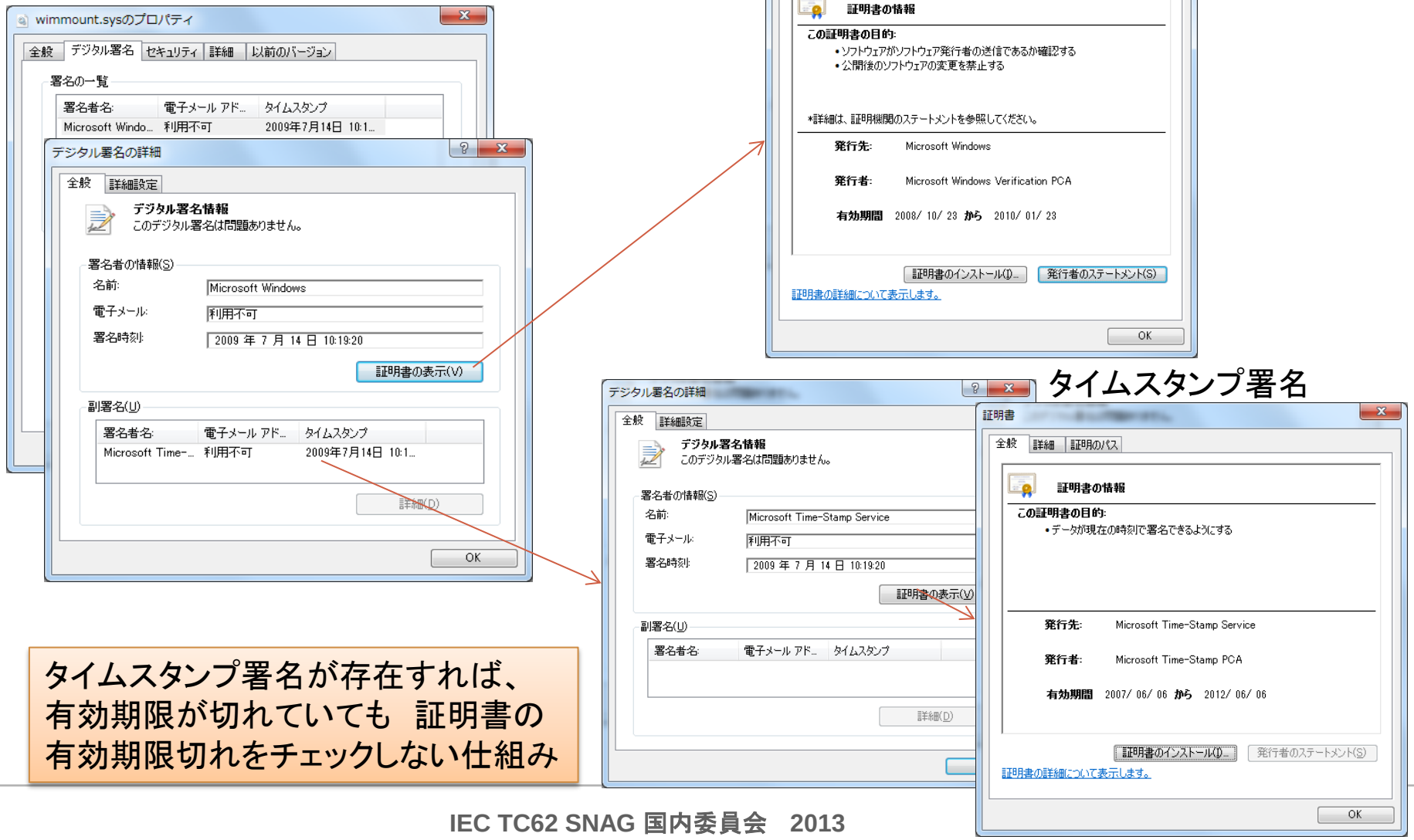
副署名

タイムスタンプ 署名

署名作業範囲

コード証明書（デジタル署名）の事例

- winmount.sysの例



タイムスタンプ署名が存在すれば、
有効期限が切れていても　証明書の
有効期限切れをチェックしない仕組み

Windowsのルート／中間証明書の更新

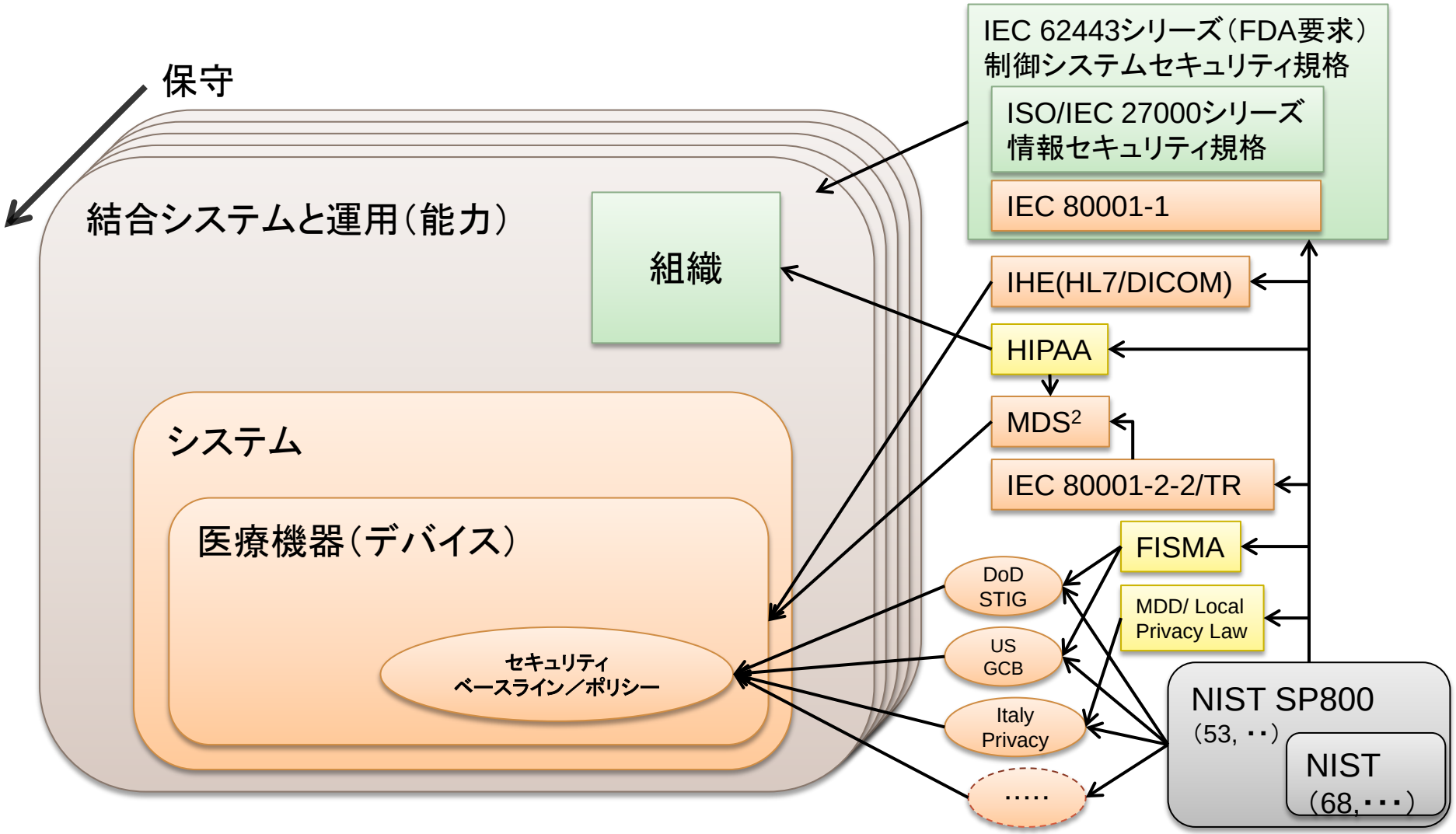
- セキュリティパッチとして公開される。
  - 2012 年 12 月 11 日に Windows Update および WSUS に投稿された KB 931125 パッケージ

- このパッチを適用しないと・・・
  - Windowsが起動しなくなる。（2013/2現在、汎用／組込みPCで発生を複数確認済み）
  - 医療機器が起動しなくなる。
  - 医療用情報システムを構成する機器が起動しなくなる。
  - 病院・施設の一部又は全てが、突然機能しなくなる。

情報提供：　日本マイクロソフト社

医療機器・システムと組織 ― 法規格の関連 ―

- 医療機器に対する要求事項への対応は、組織に対する要求事項とは分離して解決できる



2013年4月　上海会議に向けて　SNAGの活動報告

- SNAGは、次の3点を骨子とする提案文書を提出した。

1．医療機器（単独ソフトウェアを含む）と医療機器に接続するネットワーク上のセキュリティについて

a. TC62 情報セキュリティに関する多くの文書を開発しているISO TC215とこの分野でより一層の協力体制をとる。

b. 制御システムのセキュリティ規格であるIEC 62443シリーズを医療機器に適用するか等、最新の事情を鑑みて、IEC 80001-2-2に新たな要求事項の必要性をJWG7が、至急検討する。

2．医療機器の相互運用性（Interoperability）

c. ウィーン会議では、相互運用性に係る国際標準化は非常に重要であるが、AAMI/UL主催ではローカルな活動となり、TC62が参加するのは難しいと結論を出した。その後、FDAの要望を満たす（法規制）目的で、FDA指導により一連の規格開発が進められる方向が見えてきた。広く利用できる国際標準化となるよう、AAMI/ULに要望するとともに、TC62の参画を提案する。

3．医療目的のモバイルアプリケーション

d. モバイルアプリケーションが、医療の提供方法に変化を加えた。近い将来急速に拡大するであろうモバイルヘルスの領域について、提案されたMDRやFDAガイダンスに要求事項がある。医療目的のモバイルアプリケーションに関係するアイテムについて、TC62は、ISO TC215と共同で作業することを提案する。

謝辞

本資料の作成にあたり、丁寧な助言や指導、また資料の提供をして下さったトレンドマイクロ株式会社、日本マイクロソフト株式会社の皆様に感謝します。ありがとうございました。

ご清聴ありがとうございました。