第10回医療サイバーセキュリティ協議会

医療機器の認証における サイバーセキュリティの 動向、規制の動向

2022年11月1日

SGSジャパン株式会社
C&P Connectivity,
Functional Safety
河野　喜一

講師の紹介

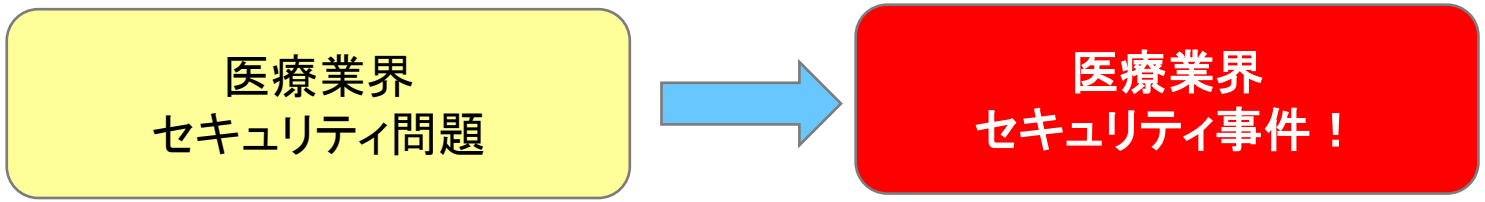
Eメール: yoshikazu.kono@sgs.com

- **河野　喜一（こうの　よしかず）**
- SGSジャパンにて機能安全・サイバーセキュリティを中心とした業務に従事
  - 医療機器セキュリティIEC 62304適用支援
  - 制御システムセキュリティIEC 62443適用支援
  - 自動車サイバーセキュリティ
    UN-R155/156、ISO/SAE 21434、ISO 24089適用支援
  - Automotive SPICE適用支援
  - ISO 26262 自動車版機能安全適用支援・認証
  - IEC 61508（産業機器）/IEC 62304（医療機器SW）/
    ISO 25119（農機）/ DO-178C （航空機器）の機能安全適用支援
  - ALMツール適用支援
  - MBD／形式手法適用支援

SGS-TUEVの資格

はじめに

- 医療業界において、セキュリティの問題が発生しており、国内においてもセキュリティ事件が発生しています。



- セキュリティ事件を防ぐため、医療機器の法規・規制、関連するISO/IECの規格が策定されています。
- 今回は、日本とEUの法規・規制、及び、関連するISO/IEC規格をご紹介いたします。

目次

- SGSのご紹介
- 医療業界におけるセキュリティ問題例
- 医療機器セキュリティ法規と標準
- セキュリティ標準を応用したセキュリティ対策例

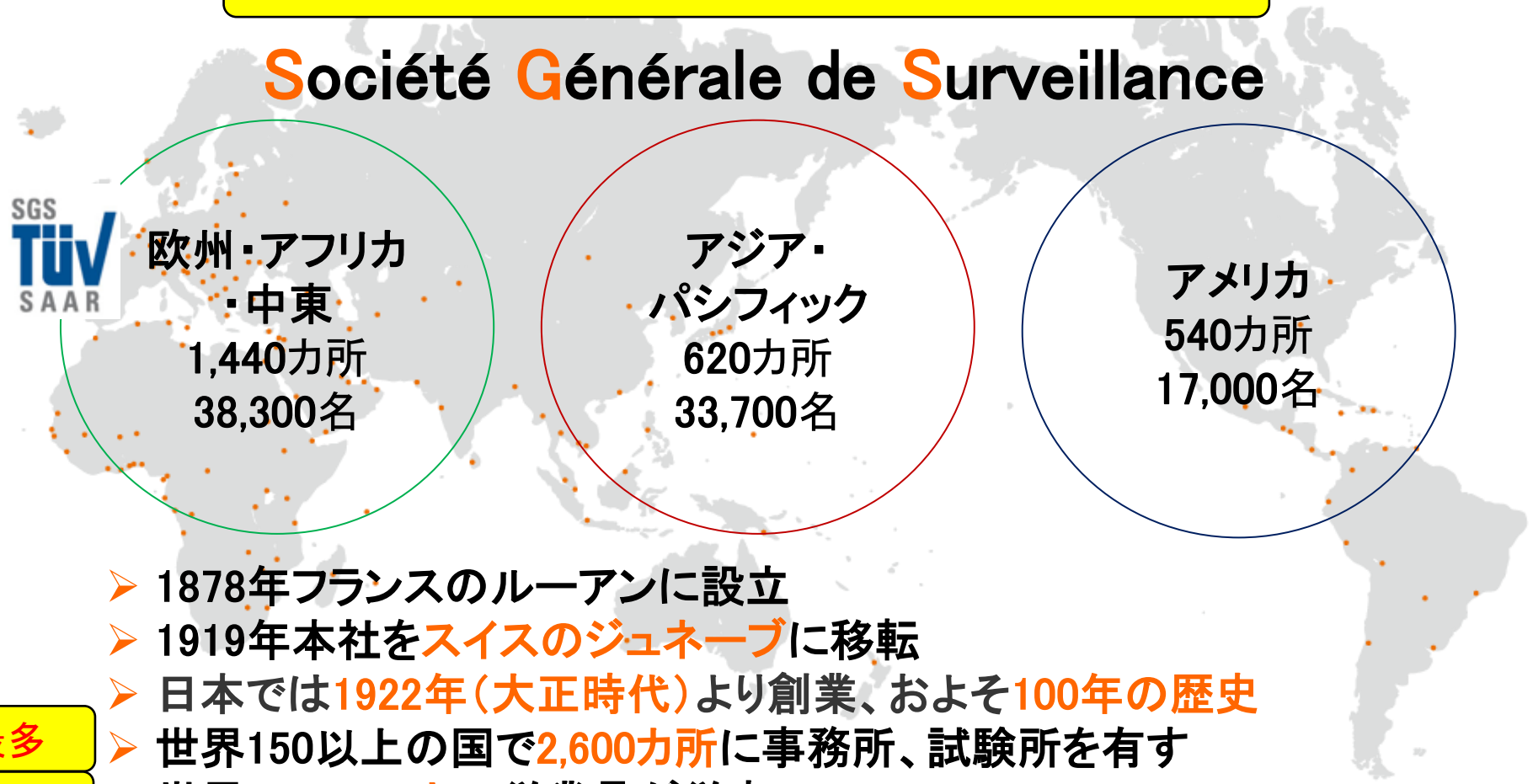
目次

- SGSのご紹介
- 医療業界におけるセキュリティ問題例
- 医療機器セキュリティ法規と標準
- セキュリティ標準を応用したセキュリティ対策例

SGSのご紹介

世界最大の検査・分析・認証機関

Société Générale de Surveillance



- 1878年フランスのルーアンに設立
- 1919年本社をスイスのジュネーブに移転
- 日本では1922年（大正時代）より創業、およそ100年の歴史
- 世界150以上の国で2,600カ所に事務所、試験所を有す
- 世界で96,000人の従業員が従事
- 2019年の売上高 約66億スイスフラン（約7,447億円）

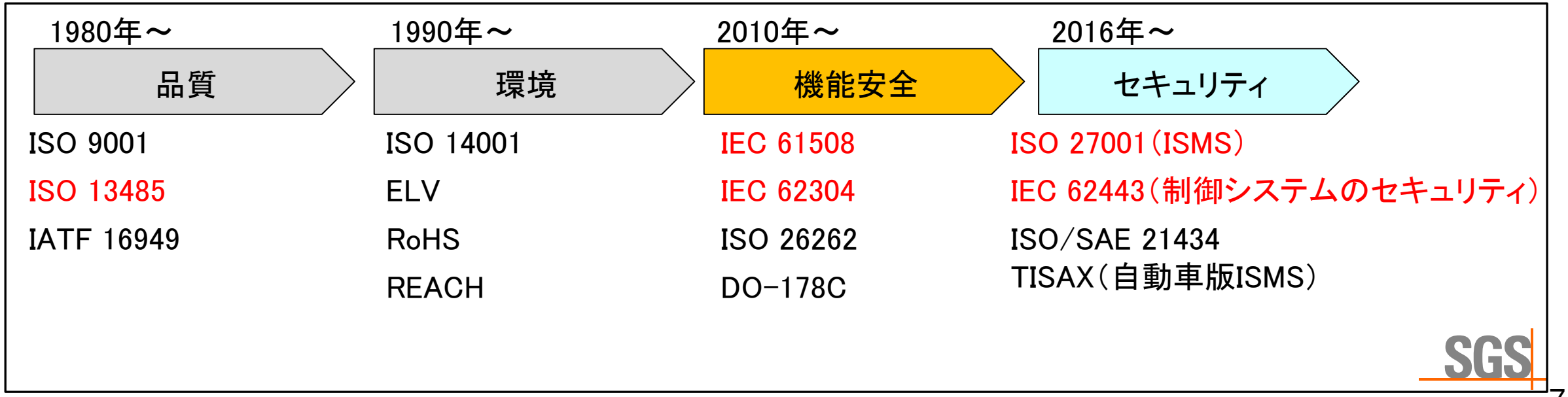
世界最多

世界最多

世界最高額

SGSの認証・試験サービス例

- QMS認証（ISO 9001、**ISO 13485**、IATF 16949、Automotive SPICE、etc ）
- 環境認証（ISO 14001、REACH、RoHS、ELV、etc）
- 機能安全認証（**IEC 61508**、**IEC 62304**、ISO 26262、DO-178C、etc）
- **セキュリティ認証**（**ISO 27001**、**IEC 62443**、ISO/SAE 21434、TISAX、etc）
- 機械安全認証（SEMI、CEマーキング、etc）
- 試験（EMC、メカニカル、INMETRO、**医療機器セキュリティテスト**、etc）



SGSジャパンの安全・セキュリティ関連サービス例

サービス名	適用分野	規格・項目
機械安全	産業機器	ISO 13849
機能安全規格	産業機器	IEC 61508
	自動車	ISO 26262
	農機	ISO 25119
	建機	ISO 19014
	航空機、ドローン	DO-178C/DO-330～333
安全＆セキュリティ規格	医療機器	ISO 14971
		IEC 62304
		IEC 60601シリーズ
製品セキュリティ規格	自動車	ISO/SAE 21434、ISO 24089
	産業機器、制御システム	IEC 62443
	航空機、ドローン	DO-326A/ED-202A、DO-356A/ED-203A
情報セキュリティ	共通	ISO 27000シリーズ
	自動車	TISAX

目次

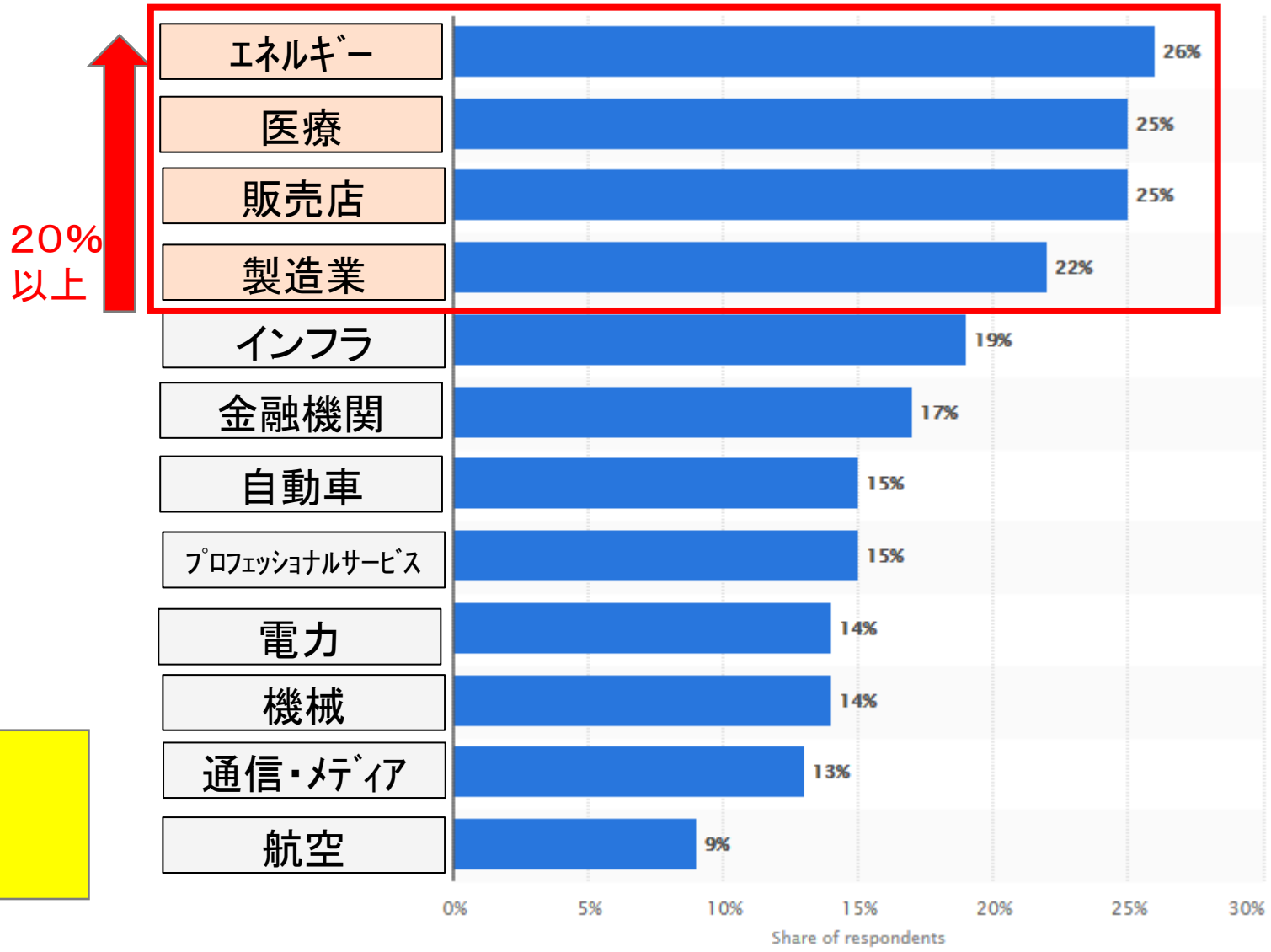
- SGSのご紹介
- 医療業界におけるセキュリティ問題例
- 医療機器セキュリティ法規と標準
- セキュリティ標準を応用したセキュリティ対策例

2017年9月のサイバー攻撃による産業界への影響レポート

- 2017年9月に世界各国の企業に対して、過去1年間にサイバー攻撃の被害を受けたかどうかのアンケートを行った。
- このアンケートをまとめた結果によると、エネルギー部門の26%の回答者が、過去12か月間に自社がサイバー攻撃の被害を受けたと述べている。

https://www.statista.com/statistics/784590/cyber-attacks-on-industries-worldwide-2017/

エネルギー部門の1／4が
サイバー攻撃されている！



表示のみ
（URLからご参照ください）

CNET Japanの記事
心臓ペースメーカー46.5万台が米で「リコール」--セキュリティに脆弱性 - CNET Japan

エンガジェット（日本版）より
各社の心臓ペースメーカーから計8000もの脆弱性、米セキュリティ企業が発見。現場の甘い認識も指摘 - Engadget 日本版

米国心臓ペースメーカーのセキュリティ問題（脆弱性）例

- 2017年米国FDAは、Abbott心臓ペースメーカーに対して外部から**無線経由でハッキングされる**問題を発見し、リコールを行った。
- また、セキュリティ企業WhiteScopeによると、**複数の心臓ペースメーカーに、8000もの脆弱性**があることがわかった。
  - 例）ユーザ認証がなく不正利用される。
    - 調整ツールの不正利用
    - モニタリングツールの不正利用

    ※　これらのツールは、eBayなどで購入することができ、氏名・病名等の個人情報も消去されていなかった！

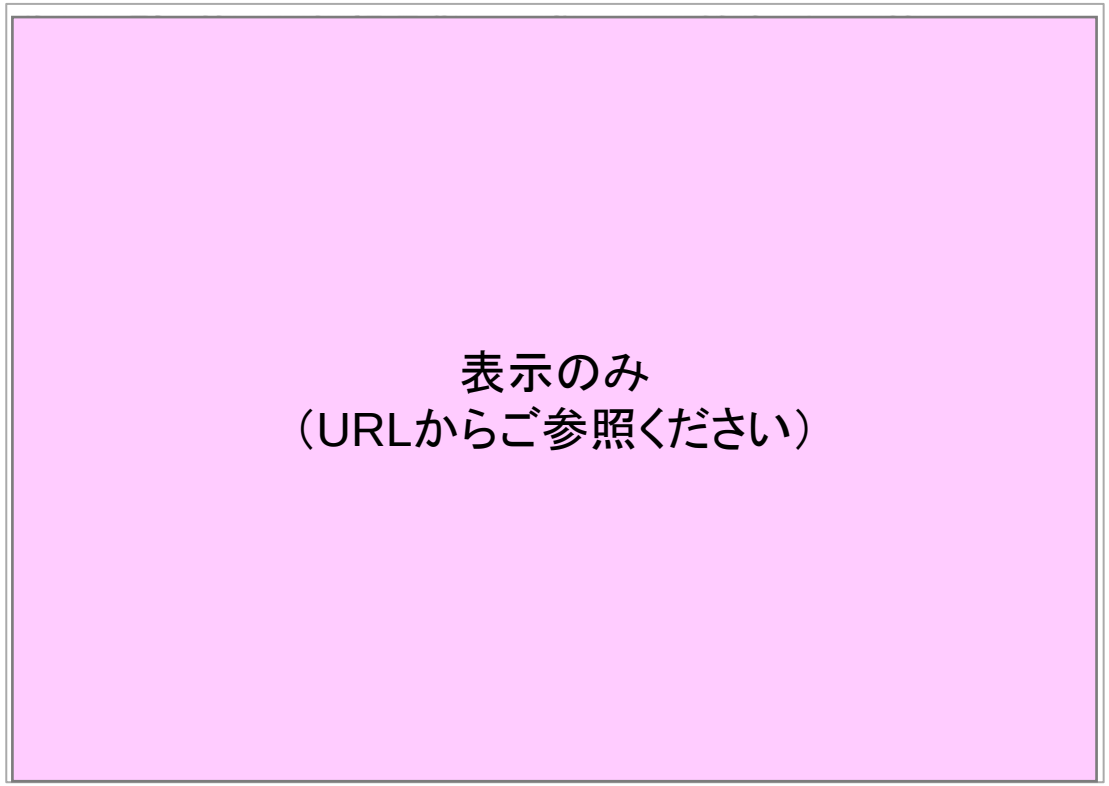
東京都の病院のサーバーウィルス感染事件例

- 2022年1月19日、東京都にある病院の電子カルテ・会計システムがウィルスに感染した。
- **電子カルテ・会計システム・画像検査が利用できなくなった。**
- バックアップデータより、システム自体は復旧した。
- 1/19現在では、個人情報漏洩の被害報告は確認されていないが、個人情報漏洩のリスクがある。

表示のみ
（URLからご参照ください）

NHK「Webニュース」より
日本歯科大学附属病院 システムがウイルスに感染 診察に影響も | IT・ネット | NHKニュース

愛知県のPCR検査データへのランサムウェア感染事件例



東海テレビ「ニュースOne」より
https://www.tokai-tv.com/tokainews/article_20220211_15962

- 2022年2月5日、愛知県のPCR検査データ管理システムがランサムウェアに感染した。
- **43,000人もの名前、年齢、検査結果データが被害を受けた。**
- バックアップデータより、PCR検査データ管理システム自体は復旧した。
- 2/11現在では、個人情報漏洩の被害報告は確認されていないが、**個人情報漏洩のリスク**がある。

目次

- SGSのご紹介
- 医療業界におけるセキュリティ問題例
- 医療機器セキュリティ法規と標準
- セキュリティ標準を応用したセキュリティ対策例

個人情報保護法/GDPR

- 個人情報保護法により、個人情報の漏洩にも注意が必要である
- EU在住者を診療する場合には、GDPRの対象となる可能性もある。
  - 2021年には、AmazonがGDPR違反となり7億4600万ユーロ（約971億円！）の罰金をうけている。

地域・国	法規名	罰則	補足
EU	GDPR	2000万ユーロ、または、 売上の4%のうち大きい方！	• 2018年5月25日施行

日本	個人情報
	保護法
		6か月以下の懲役、
		30万円以下の罰金
			• 2022年4月に「改正個人情報保護法」が施行された。
			  • サーバーがある国にも注意が必要
			  • 医療・介護・健保向けのガイドラインも更新

（参考）

- 令和3年 改正個人情報保護法について（官民を通じた個人情報保護制度の見直し）｜個人情報保護委員会 (ppc.go.jp)
- 特定分野ガイドライン ｜個人情報保護委員会 (ppc.go.jp)

医療機器セキュリティ規則・法規化の動向

- EUでは、医療機器規則MDR（2017/745）/IVDR（2017/746）により、**医療機器セキュリティへの対応が必須**となっている。
- 日本では、2023年10月より、薬機法として医療機器セキュリティが要求事項となる。

	現在	
	2022年	2023年
日本		10月 改訂した薬機法 適用
EU	MDR/IVDR 適用	

※ MDR：Medical Device Regulation、医療機器規則
※ IVDR：In Vitro Diagnostic Medical Device Regulation、体外診断用医療機器規則

（参考）日本における医療機器セキュリティ法規の適用時期

- ISO 14971:2019（JIS T 14971:2020）より、セキュリティのリスクマネジメントが追加された。
- これに伴い薬機法が改正され、**令和5年（2023年）10月1日**からは、ISO 14971:2019（JIS T 14971:2020）に従った脆弱性分析等の**セキュリティ対応が必須**となる。

厚生労働省の資料

写

薬生機審発 1224 第 1 号
令和 2 年 12 月 24 日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
（　　公　　印　　省　　略　　）

医療機器及び体外診断用医薬品のリスクマネジメントに係る要求事項に関する
日本産業規格の改正の取扱いについて

医療機器及び体外診断用医薬品のリスクマネジメントについては、「医薬品、医療

記

1．製造販売承認申請、認証申請及び届出等における基本要件基準への適合性確認について

（1）高度管理医療機器、管理医療機器及び体外診断用医薬品（承認品及び認証品）における基本要件基準への適合性確認については、令和５年９月30日（以下「経過措置期間終了日」という。）の翌日以降に、新規の承認申請又は認証申請（承認事項一部変更承認申請及び認証事項一部変更認証申請を含む。以下「承認申請等」という。）を行う場合、当該医療機器及び体外診断用医薬品について改正後のJISを適用し、承認申請等の添付資料等において、リスクマネジメントの評価に基づく考察等について簡潔に記載すること。なお、改正後のJISの原典である

2．JIS T 14971 の主な改正点に係る留意事項等について

（1）JIS T 14971 の改正事項に係る留意事項

JIS T 14971 の改正により、体外診断用医療機器、医療機器プログラム（Software as a Medical Device; SaMD）及びセキュリティが適用範囲であることが示され、ユーザビリティに関するリスクに適用することが示されていることに留意すること。また、改正後の JIS では従来の「誤使用」は「使用エラー」と修正され、

MDCG 2019-16とIEC 62443

- MDR、IVDR適用ガイドラインの「MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices」では、IEC 62443が引用されている。

Medical Device

Medical Device Coordination Group Document MDCG 2019-16 rev. 1

3.1. "Secure by design"

Figure 5 illustrates how "secure by design" practices in this document contribute to a "defence in depth" strategy for the product. The "security management" practice is shown on the top circle since it is applied throughout all other practices to ensure that these practices are being followed and managed. The other practices, shown on the bottom circle are applied throughout the development lifecycle, often in an iterative pattern. These practices each contribute to the overall "defence in depth" strategy which is shown as the centre of the circle because it represents the key result of following the security development lifecycle.

Defect management and security update management provide verified repairs to secure implementation and fall under the category of overall security management in the diagram.

Figure 5: Defence in depth strategy is a key philosophy of the secure product life-cycle

IEC 62443の抜粋

医療機器規則・法規とISO/IEC規格

- 医療機器規制・法規では、整合規格としてISO/IEC規格が指定されている。
- EUでは、**新しい医療機器セキュリティ規格の法規化も予定**されている。

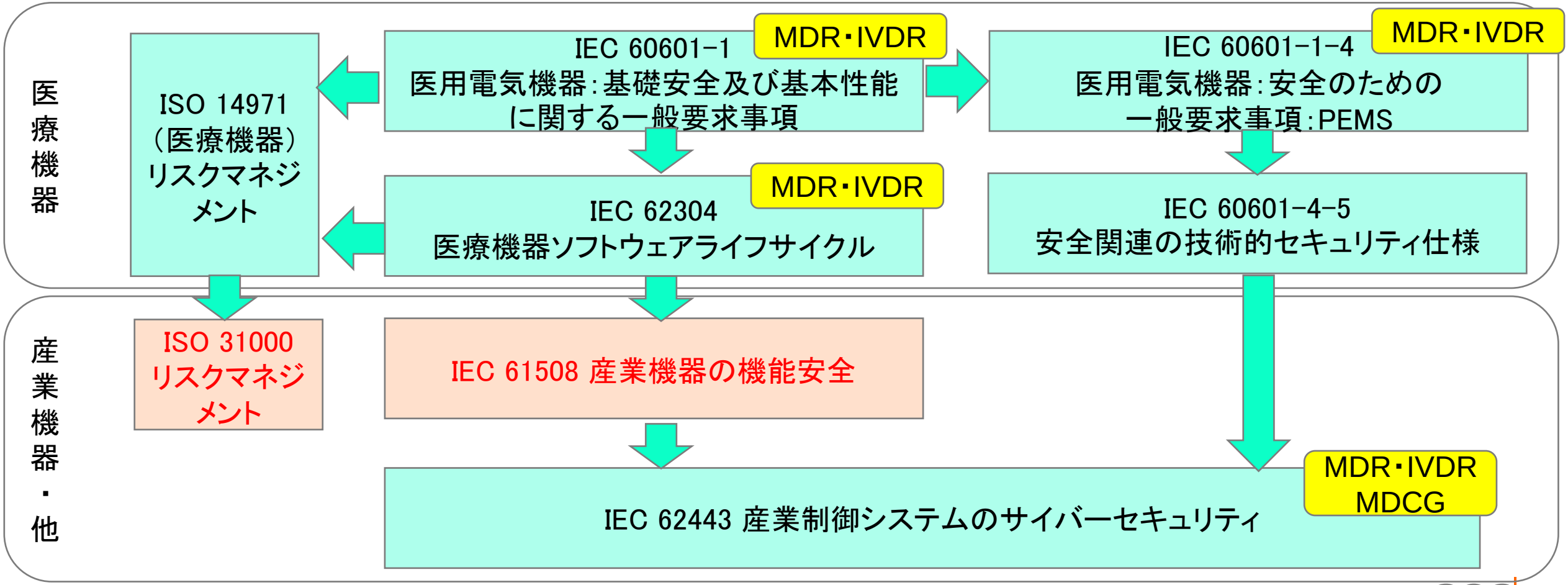
No.	日本（薬機法）	EU（MDR/IVDR）	整合規格	
1	○	○	ISO 14971	医療機器リスクマネジメント
2	○	○	IEC 60601-1	医用電気機器：基礎安全及び基本性能に関する一般要求事項
3	ー	○	IEC 60601-1-4	医用電気機器：安全のための一般要求事項：PEMS
4	ー	（予定）	IEC 60601-4-5	安全関連の技術的セキュリティ仕様（IEC 62443を参照）
5	○	○	IEC 62304	医療機器ソフトウェアライフサイクル（IEC 61508経由でIEC 62443を参照）
6	ー	（予定）	*IEC 81001-5-1*	*医療機器セキュリティ（策定中）*（IEC 62443 を参照）

IEC 62443産業用オートメーション及び制御システムのセキュリティも考慮が必要！

※ MDR：Medical Device Regulation、医療機器規則
※ IVDR：In Vitro Diagnostic Medical Device Regulation、体外診断用医療機器規則

規格の参照関係

- 医療機器規格、及び、関連規格の参照関係を示す。



医療機器に対するセキュリティ規格（ISO/IEC）

No.	規格	概要	
1	ISO 14971 医療機器リスクマネジメント	• リスクとしてセキュリティが記載されている “CIA+アクセス・転送” • ISO 31000 に従ったセキュリティの脅威分析も必要	
2	IEC 60601-1 医用電気機器：基礎安全及び基本性能に関する一般要求事項	• 医用電気機器の基本安全規格であり、リスクマネジメントの項目では、セキュリティも対象となっている。 • 開発プロセスは、IEC 60601-1-4を参照している。 • ソフトウェア開発プロセスは、IEC 62304を参照している。	MDR・IVDR
3	IEC 60601-1-4　医用電気機器：安全のための一般要求事項：PEMS	• PEMS（プログラマブル電気医療システム）の開発プロセスセキュリティに関しては、IEC 60601-4-5を適用する。	MDR・IVDR
4	IEC 60601-1-4-5　安全関連の技術的セキュリティ仕様	• 2021年IEC 62443を参考にして、IEC 60601-1-4-5が発行された。 • IEC 60601-1-4-5では、IEC 62443を参照している項目が多い	
5	IEC 62304　医療機器ソフトウェアライフサイクル	• ソフトウェアのリスクとして、セキュリティが記載されている。 例）組込製品、PC、サーバー、インターネット	MDR・IVDR

医療機器規格から参照される規格（ISO/IEC）

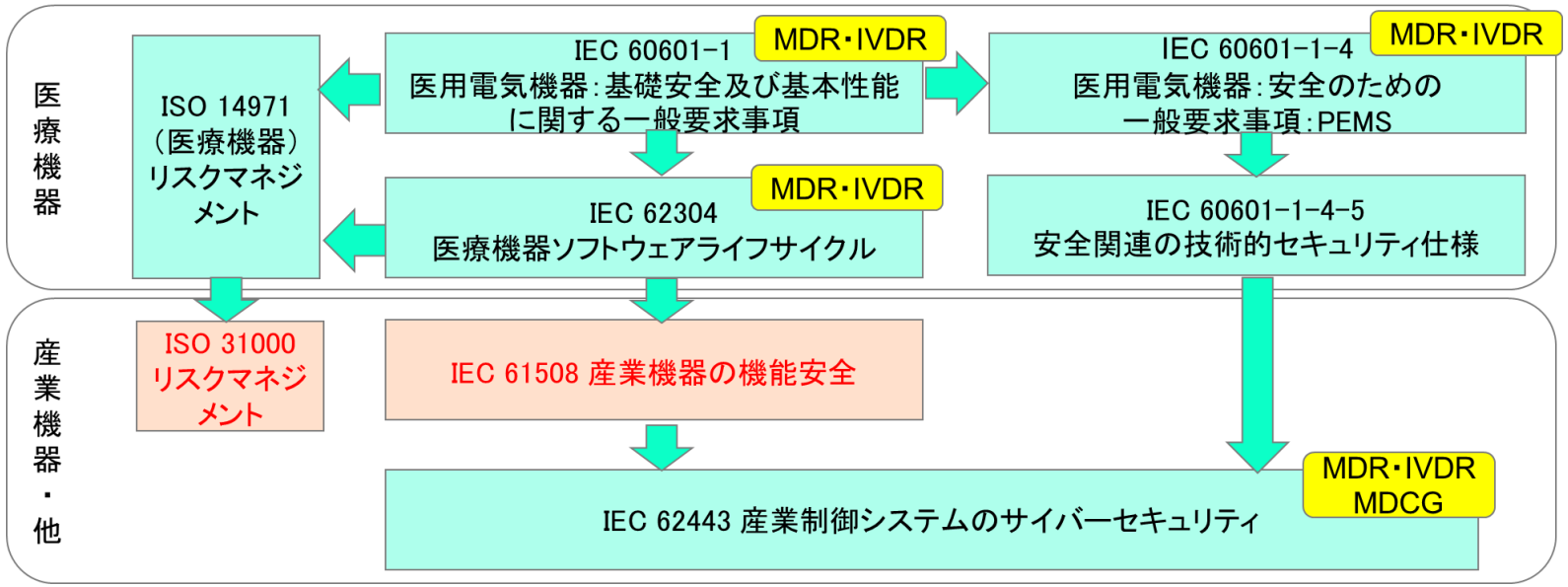
No.	規格	概要
1	ISO 31000 リスクマネジメント指針	• 「脅威」、「脆弱性」を含めたリスクマネジメントが記載されている。
2	IEC 61508 産業機器の機能安全	• IEC 62304が参照している機能安全規格 • セキュリティの考慮が記載されており、セキュリティ要求・脆弱性分析等の記載がある。 • セキュリティの詳細手順はIEC 62443参照となっている。
3	IEC 62443 産業制御システムのサイバーセキュリティ	• Part2 運用業者、Part3 システムベンダー、Part4 コンポーネントベンダーそれぞれの要求が記載されている。 • セキュリティレベル（SL）毎の対策を取る。

MDR・IVDR
MDCG

まとめ

- ISO 14971、IEC 62304において、**セキュリティの対応が必要**
- **IEC 62443の対応も必要**
  - EUでは、IEC 62443の対応も必要
  - 日本でも、間接的にIEC 62443が参照されている。

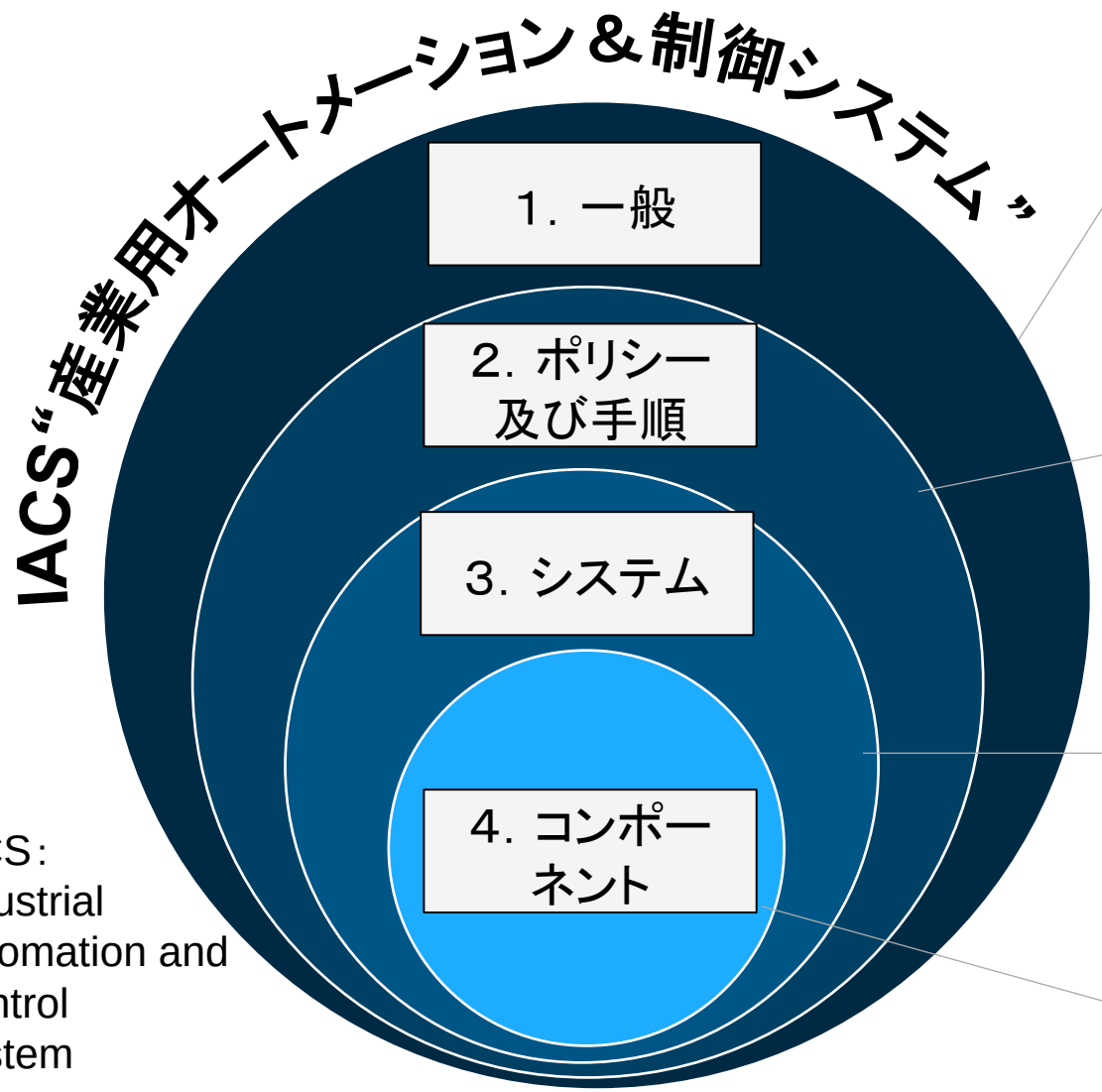
	現在	
	2022年	2023年
日本		10月 改訂した薬機法 適用
EU	MDR/IVDR 適用	



目次

- SGSのご紹介
- 医療業界におけるセキュリティ問題例
- 医療機器セキュリティ法規と標準
- セキュリティ標準を応用したセキュリティ対策例

IEC 62443の全体像



IACS：
Industrial Automation and Control System

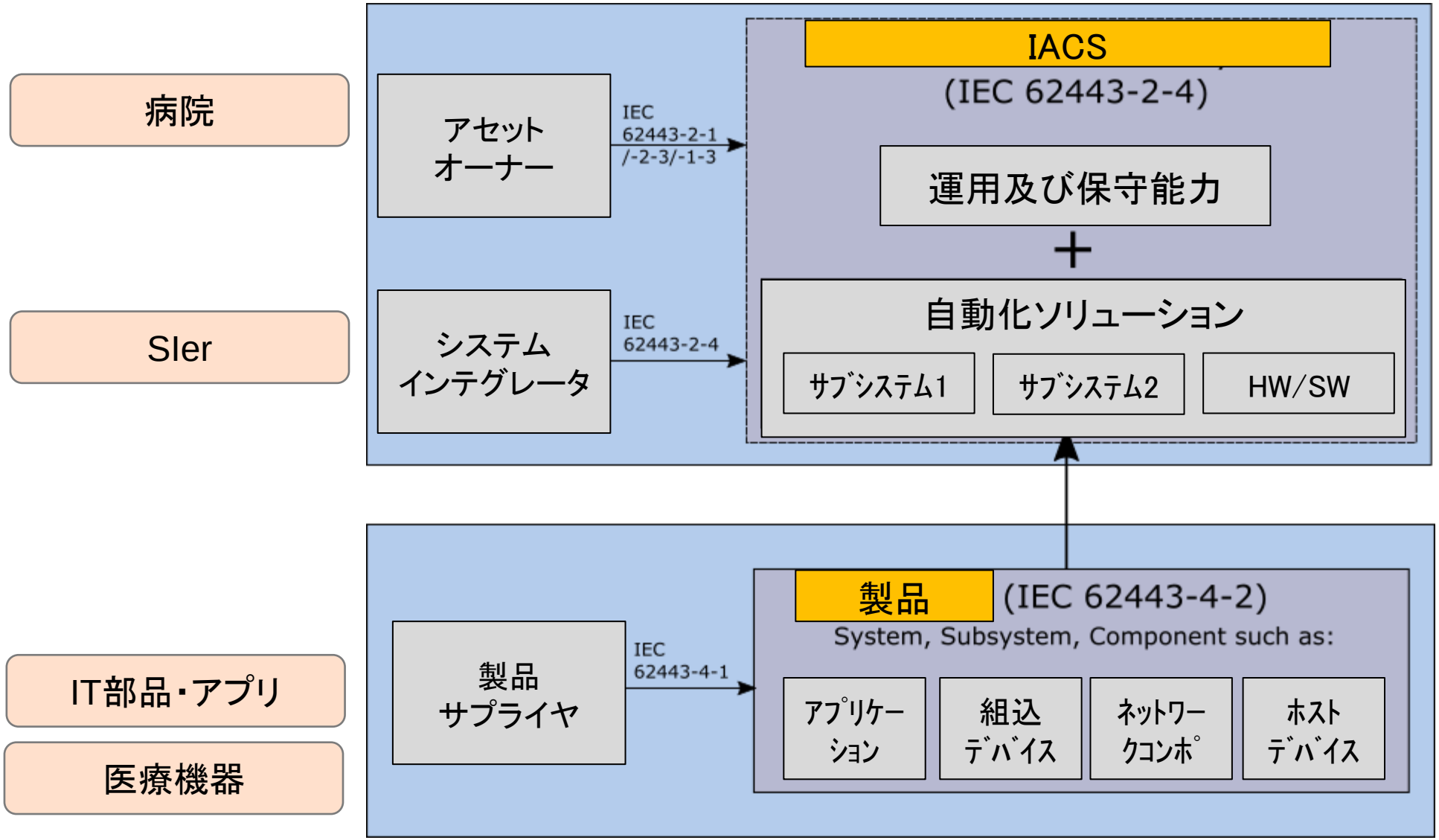
1-1: 用語、概念及びモデル
1-2: 用語及び略語の基本用語集
1-3: システムセキュリティ適合性の尺度
1-4: IACSセキュリティライフサイクル及びユースケース

アセットオーナーに適用 （病院等）
2-1: IACSのセキュリティプログラムの確立
2-2: IACSセキュリティマネジメントシステムの実装の手引
2-3: IACS環境でのパッチマネジメント
2-4: IACSサービスプロバイダに対するセキュリティプログラム要求事項

システムインテグレーターに適用 （Sier等）
3-1: IACSのためのセキュリティ技術
3-2: セキュリティリスクアセスメント及びシステム設計
3-3: システムセキュリティ要求事項及びセキュリティレベル

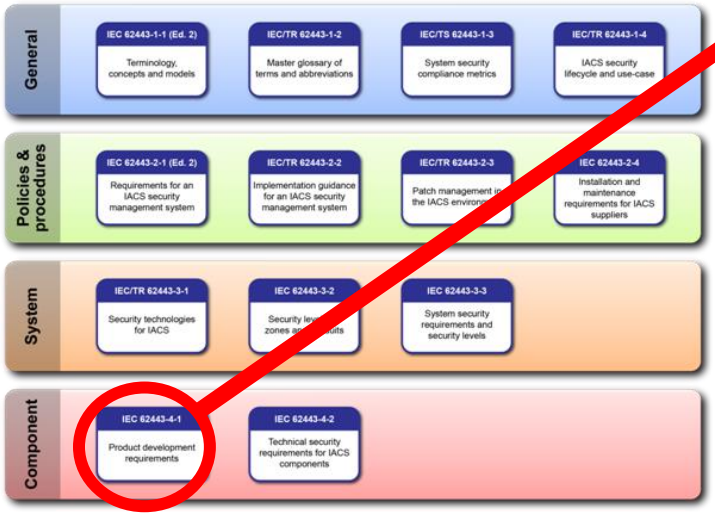
コンポーネントサプライヤに適用 （医療機器等）
4-1: 製品開発の要求事項
4-2: IACSコンポーネントの技術的セキュリティ要求事項

セキュリティフレームワーク



IEC 62443-4-1：セキュリティ製品開発プロセス

IEC 62443-X

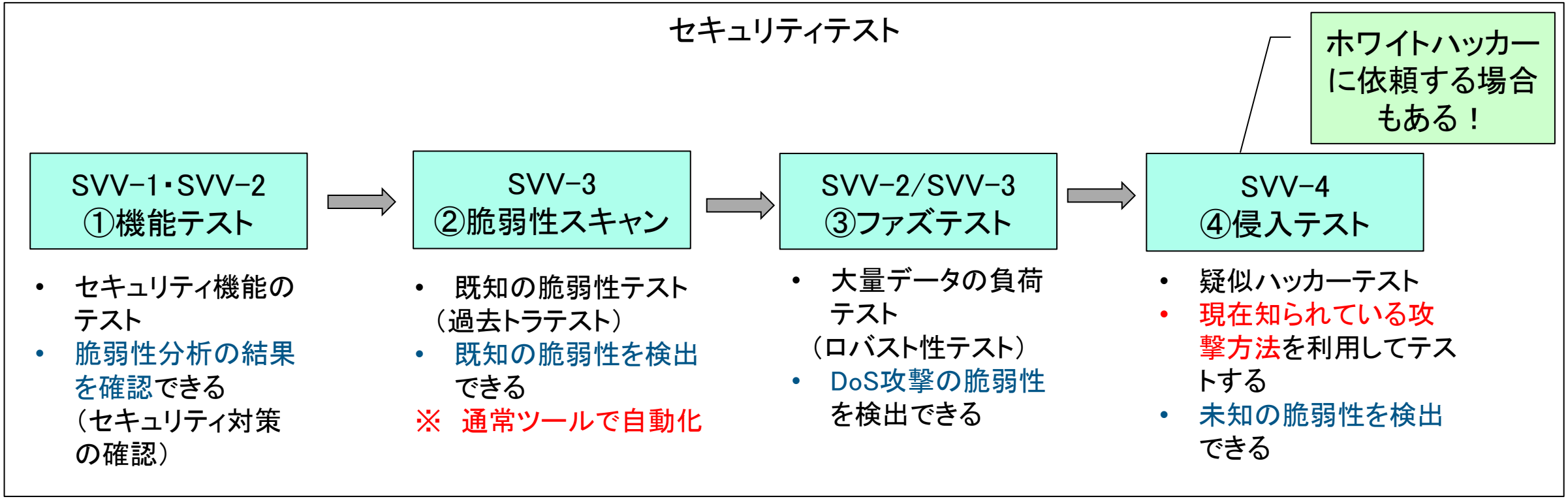


IEC 62443 4-1

- SM セキュリティマネジメント
- SR セキュリティ要求事項の仕様
- SD セキュアバイデザイン（設計によるセキュリティ）
- SI 安全な実装（セキュアな実装）
- SVV セキュリティの検証及びバリデーションテスト
- DM セキュリティ関連の問題のマネジメント
- SUM セキュリティアップデートのマネジメント
- SG セキュリティ指針

IEC 62443-4-1

セキュリティテストの例：
SVV - セキュリティの検証及びバリデーションテスト



IEC 62443-4-2：のセキュリティ技術例： FR 1 – 識別及び認証管理(IAC))

CR1.7 パスワードベース認証の強度

ISA-62443-4-2 CR 1.7

- 最小文字数
- 特殊文字の使用
- 大文字と小文字の使用

パスワードベースの認証を使用するコンポーネントの場合、構成可能なパスワード強度をコンポーネント自体または共通システムのいずれかでサポートされる必要がある。

パスワードは製品ドキュメントに記載しないこと！

ISA-62443-4-2 CR 1.7 (1)

人間ユーザー向け

- パスワードは1回のみ
- パスワードの有効期間

人間ユーザーはパスワードを再利用できない

コンポーネントには、人間のユーザーのパスワードに有効期間を適用する機能も必要である

ISA-62443-4-2 CR 1.7 (1) (2)

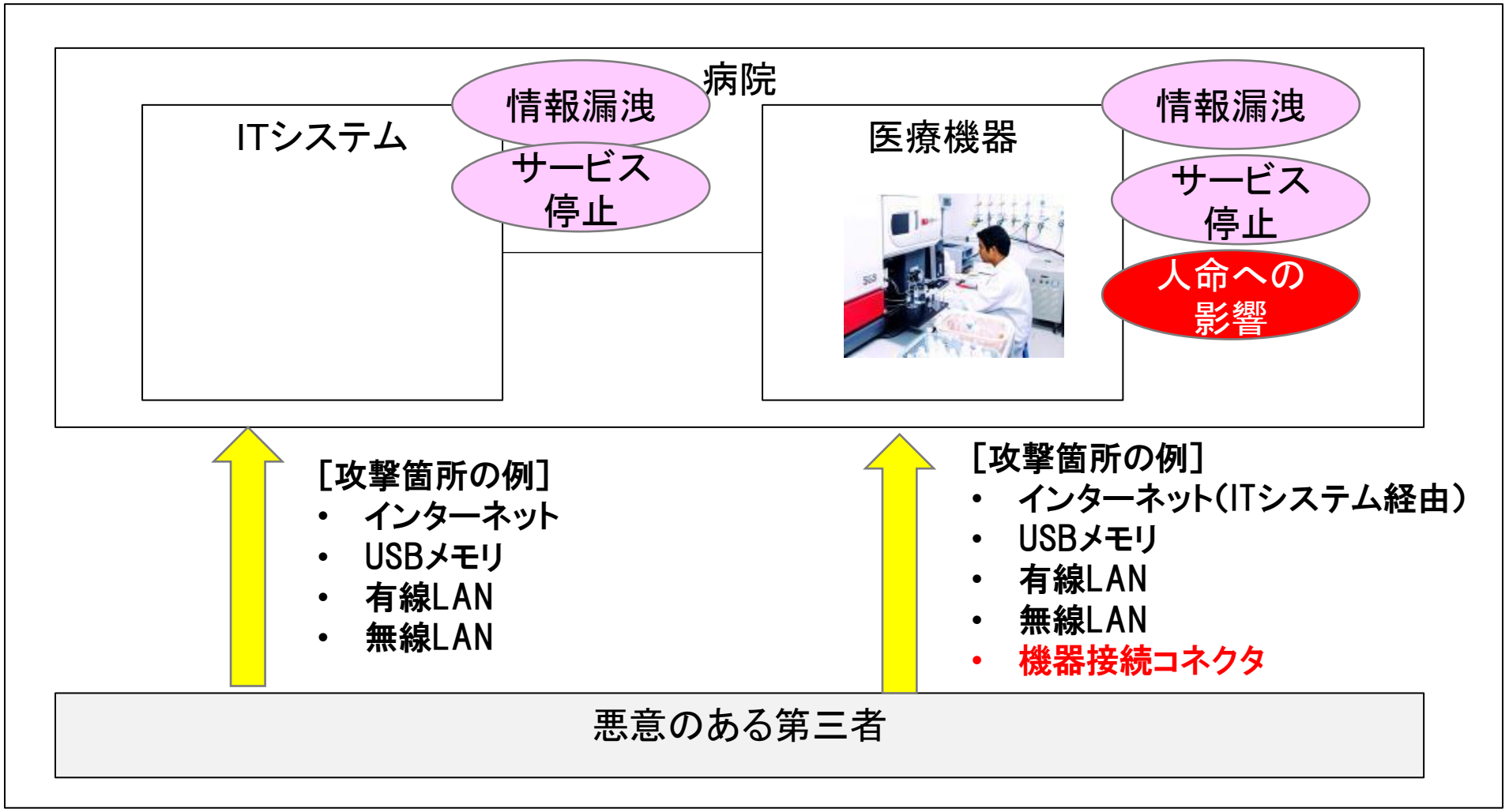
全てのユーザ

- パスワードの有効期間

パスワードの有効期間は、全てのユーザに適用される

病院におけるセキュリティの考慮例

- 病院においては、ITシステムのセキュリティだけでなく、医療機器のセキュリティも重要である。

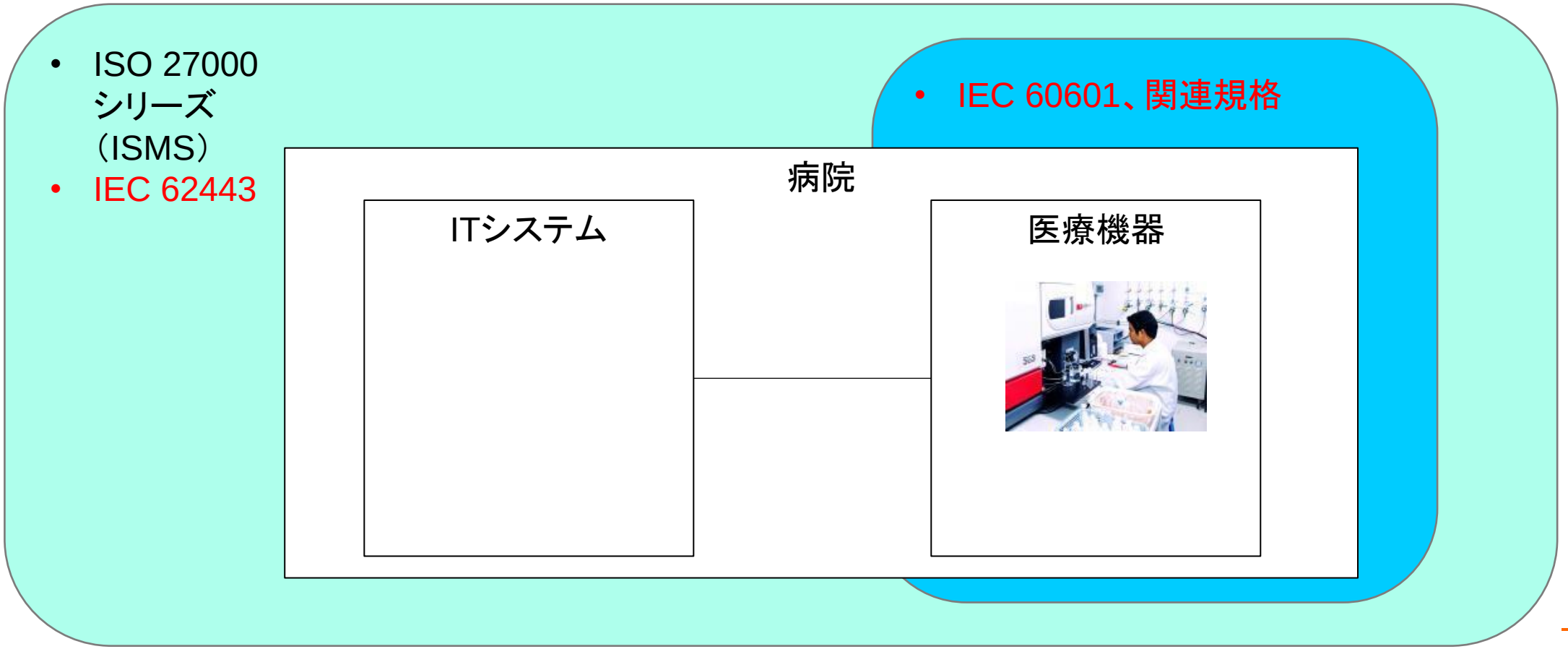


情報セキュリティ

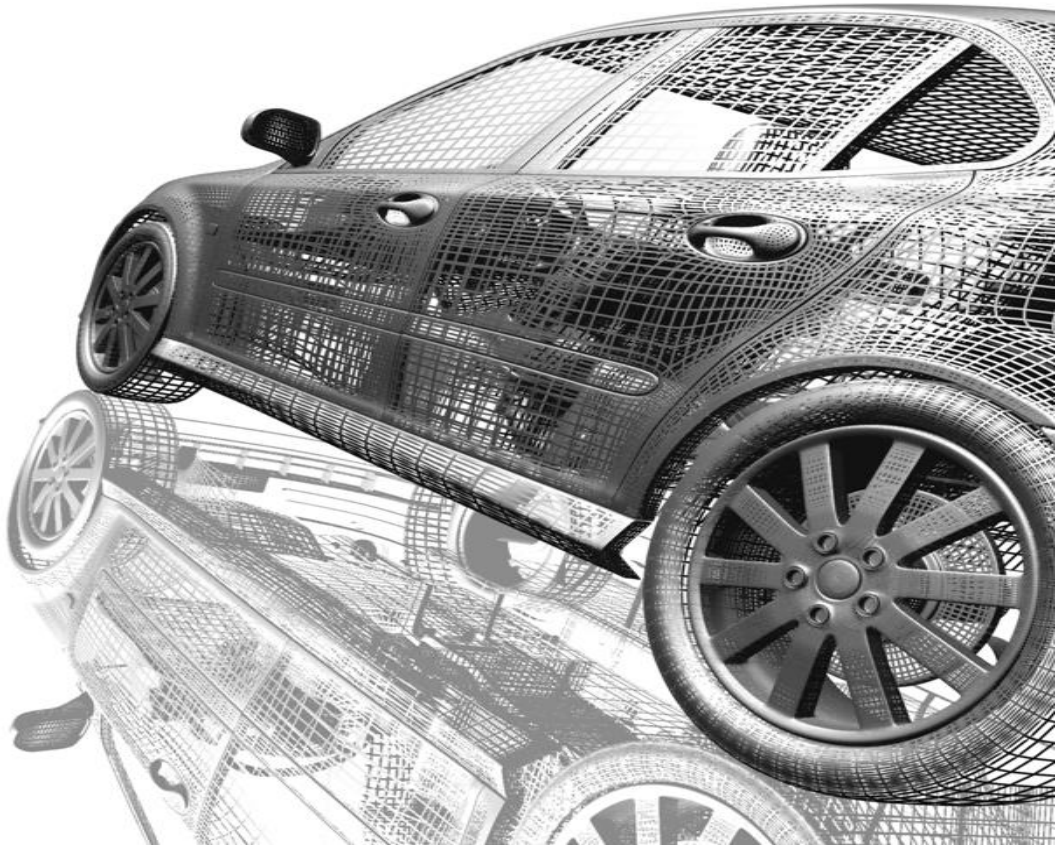
製品安全（セキュリティ）

病院におけるセキュリティ標準規格適用例

- 病院においては、従来のISMS（ISO 27000シリーズ）のみならず、医療機器が制御システムとなる場合は、製品セキュリティ（IEC 62443、IEC 60601等）の適合も重要となる。



ご清聴
ありがとうございました



問い合わせ先

SGSジャパン株式会社
C&P Connectivity Functional Safety

TEL：050−3773−4508
Eメール: jp.fsafety@sgs.com
会社HP：https://www.sgsgroup.jp/
部門HP：http://safety−testing.jp/sgs/

SGS-TÜV GmbH（ドイツ）

Funktionale Sicherheit

www.sgs-tuev-saar.com/fs

Telefon: +49 89 787 475 -271
Fax: +49 89 787 475 -217