明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

修士論文発表会

計量機器のリモート更新機能実装に向けた関連法規制と国際規格に対するソフトウェア要件の提案

2020年2月22日

情報セキュリティ大学院大学　博士課程前期2年
後藤研究室　関本　泰之
（学籍番号　5585503）

本研究の成果

➢ 課題

計量機器における業務効率化とセキュリティ保全の両立

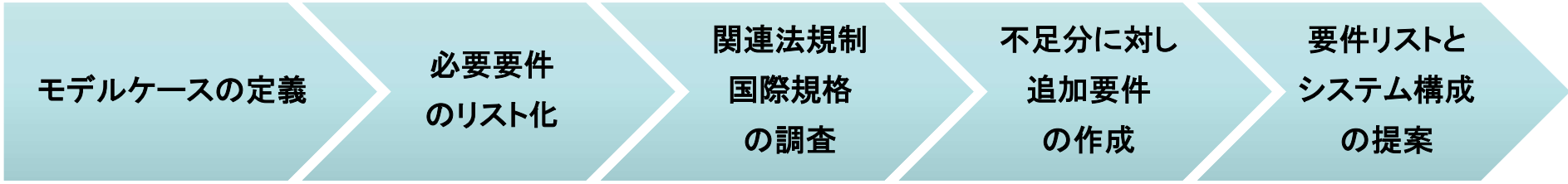
➢ 提案

リモート更新機能実装による計量機器業界の技術革新の推進

➢ 成果

1. 計量機器におけるリモート更新可能なシステム構築に必要なソフトウェア要件リストと構成の提示
2. 国内法規制（計量法／JIS）と国際規格・ガイドラインへの提言

➢ アプローチ



目次

1. 研究概要

2. 脅威分析と実運用上の必要要件

3. 計量機器に関する法規制と国際規格

4. ソフトウェア要件リストの提案

5. まとめと外部発表

研究の背景

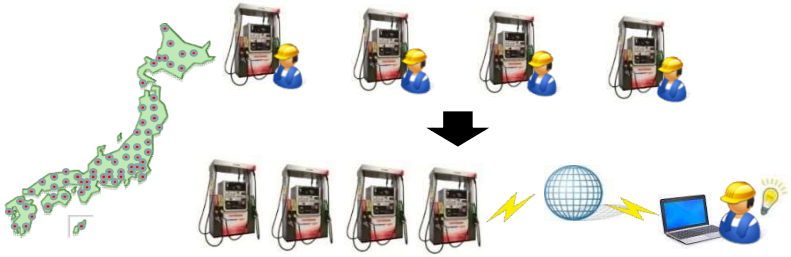
◆現状の課題

機器メーカーにおいて、販売後の機器に対するメンテナンスは多くの時間とコストを要す。本研究ではソフトウェアの観点から、効率化を目指した実用的なシステム構築を目指し、その際に必要なソフトウェア要件について考察する。

機器のメンテナンス性を向上させるための安全で実用的なシステムを構築したい

◆ 課題に対する提案

「リモートメンテナンス可能なシステムの構築」



機器のプログラム更新を遠隔地からリモートでおこなうことにより、設置場所に関わらず迅速な対応が可能になる。(リモート更新)

モデルケースの定義

- 機器

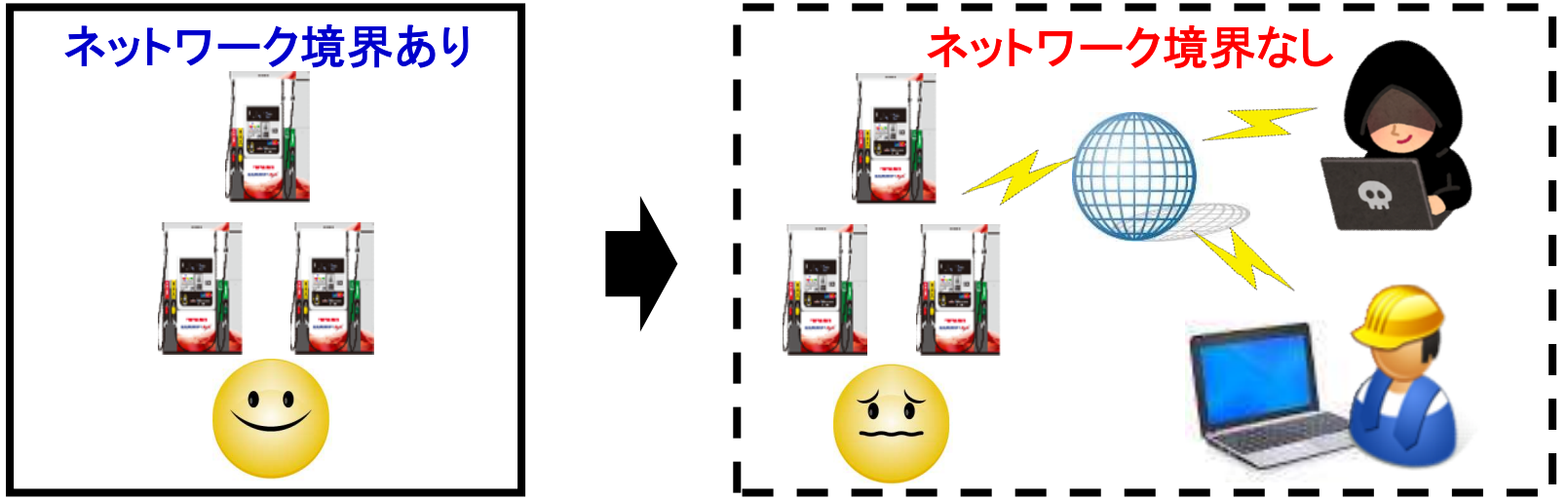
  ガソリン給油機（水以外の液体を対象とする特定計量機器）

- システム区分

  組み込みソフトウェア搭載（RTOSベース）の専用設計機器

- 追加機能

  リモート更新を実現するため、現状ではローカルな環境でのみ通信している機器を、オープンなネットワーク接続に対応して遠隔地との通信を可能にする。



研究概要と成果のまとめ

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

モデルケースの作成

↓

リモート更新機能実装に必要な要件リストの作成

要件1 法規制 国際規格 ＋ 要件2 システム要件（セキュリティ） ＋ 要件3 実運用上の要件

↓

Goal

リモート更新可能なシステム構築案とソフトウェア要件を提示

↓

国内法規制（計量法／JIS）と国際規格・ガイドラインへの提言

1. 研究概要

2. 脅威分析と実運用上の必要要件

3. 計量機器に関する法規制と国際規格

4. ソフトウェア要件リストの提案

5. まとめと外部発表

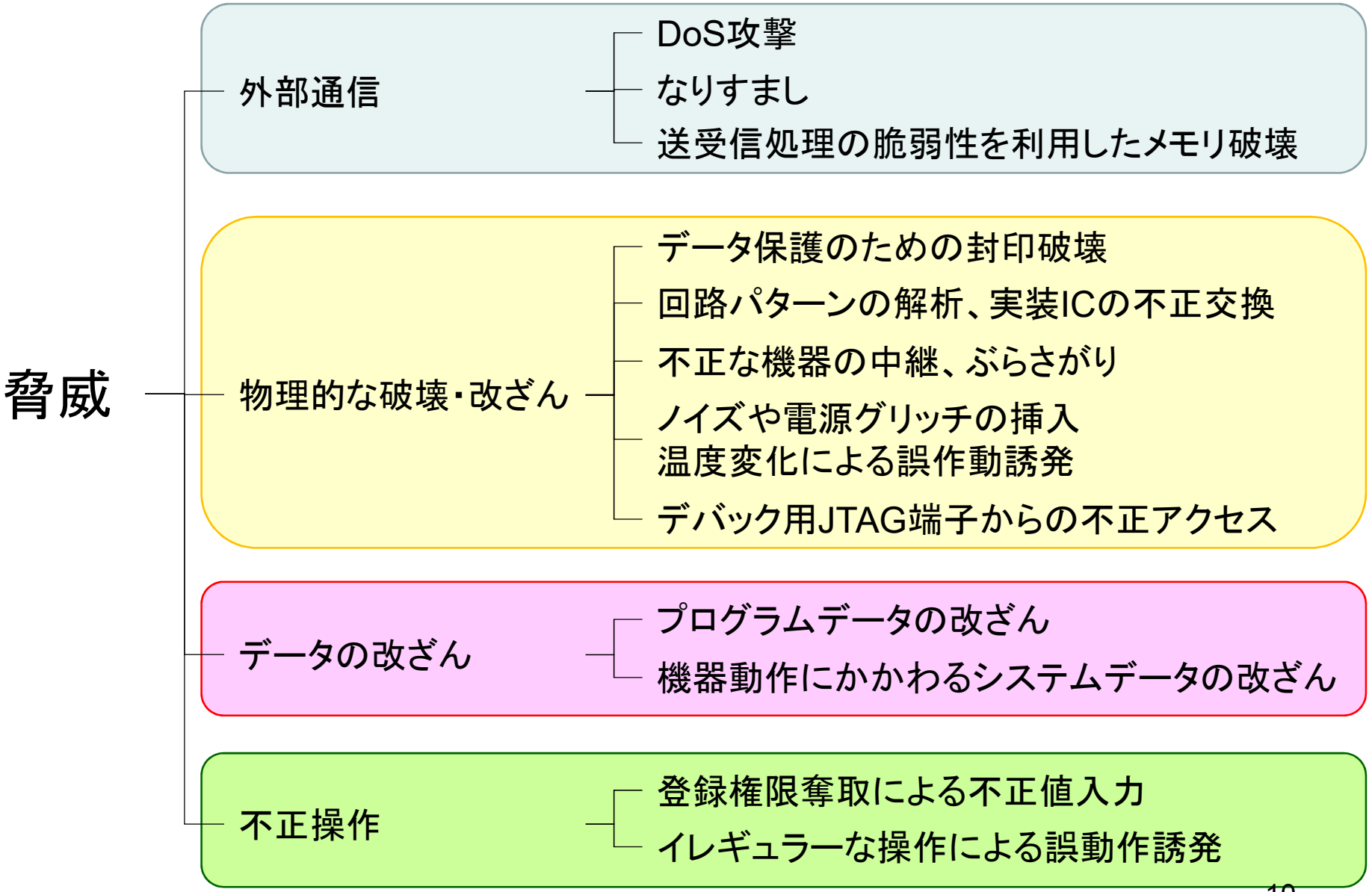
対象分類とセキュリティ保護

ローカルな環境で使用されている機器をオープンなネットワークに接続することによって新たに発生しうる脅威に対する保護を分析。

- データサーバに対する保護
  通常のネットワークサーバ(クラウドサーバ)と同等のセキュリティを適用する。
  ただし、機器側のリソースの少なさを考慮して、軽量な認証方法を推奨する。
- ネットワーク経路に対する保護
  一般的なネットワークと同等のセキュリティを適用する。
  ただし、機器側のリソースの少なさを考慮して、軽量な暗号化方法を推奨する。
- 機器本体に対する保護
  機器本体の構成規模に応じた、また用途に応じたセキュリティが必要。

特有の要件が多い「機器本体に対する保護」について検討する。

計量機器本体に対する脅威分析



実運用上の要素

現在の作業を置き換えた場合　（例：プログラム更新時の作業）

＜現在の作業＞	＜想定される要素＞
①客先にアポを取る	⇒　スケジューリング
②作業員が現地に行く	⇒　アクセス経路の確認
③機器の使用停止（レーン封鎖）	⇒　機器稼働状態の明示
④機器の鍵を開ける	⇒　更新作業者の認証
⑤書き込み機器を接続する	⇒　更新元の認証
⑥更新の実施	⇒　更新データの検証
⑦更新後の動作確認	⇒　更新後の自己診断
⑧機器の使用開始（封鎖解除）	⇒　機器稼働状態の明示
⑨点検記録に記載	⇒　ログの記録・通知

必要とする要件リストのまとめ

脅威／運用	保護策／要件
「外部通信」による攻撃	
DoS攻撃	通信ポートの開閉制御
	通信制御処理による受信データ制限
なりすまし	データサーバの認証
	通信の暗号化
送受信処理の脆弱性を利用したメモリ破壊	送受信処理の対策強化
「物理的な破壊・改ざん」による攻撃	
データ保護のための封印破壊	電子封印システム
回路パターンの解析、実装ICの不正交換	基板のコーティング
	実装ICのSOP化
不正な機器の中継、ぶらさがり	機器間のデータチェック
	通信の暗号化
ノイズや電源グリッチの挿入、 温度変化による誤作動誘発	ノイズ対策
	ソフトウェアによる誤動作防止の対策強化
デバック用JTAG端子からの不正アクセス	デバック用JATG端子のパターンおよび端子を削除
「受信および内部データの改ざん」による攻撃	
プログラムデータの改ざん	プログラムデータの信頼性確認
	データの完全性確認
	チェックサム
	アップデート・監査ログ
	Root of Trust／Chain of Trust
内部データの改ざん （機器動作にかかわるシステムデータ）	内部データのアクセス保護
	データの完全性確認
	チェックサム
	変更・監査ログ
	TSIP／Trust Zone
「不正操作」による攻撃	
登録権限の奪取による不正値入力 （特に機器のコアデータ）	権限の厳格管理
	操作者の限定
	コアデータのアクセス保護
イレギュラーな操作による誤動作誘発	標準的な入出力に対する誤動作防止の対策強化
実運用上で求められる要件（不足分）	
システム構築の前提条件	スケジューリング
	アクセス経路の選択
機器側の追加機能	機器稼働状態の明示
システム間の認証	更新作業者の認証（データサーバ側の権限）

1. 研究概要

2. 脅威分析と実運用上の必要要件

3. 計量機器に関する法規制と国際規格

4. ソフトウェア要件リストの提案

5. まとめと外部発表

ソフトウェアに対する規格

国内においては「計量法／JIS※」が挙げられるが、**ソフトウェアに関する項目およびセキュリティ面での定義は少ない**。
（※　計量法ではJIS規格と整合性を図るために、技術基準についてJIS引用をおこなっている。）

そこで、JIS規格の策定においてベースとなっているOIML（国際法定計量機関:International Organization of Legal Metrology) が発行する国際文書、および欧州規格であるWELMEC（欧州法定計量協力機構:Western European Legal Metrology Cooperation）が発行するガイドラインからソフトウェアに関する規格を調査する。

☆ソフトウェアに関する法定計量規格

規格名称	種別	対象機器区分	リモート更新要件の記載
JIS B 7611-2	国内JIS規格	非自動計量機器	記載なし
OIML D31	国際文書	全て	項目5.2.6保守と再構成
WELMEC 2.3	欧州ガイドライン	非自動計量機器	ANNEX Ⅱ
WELMEC 7.2	欧州ガイドライン	自動計量機器	Extension D

1. 研究概要

2. 脅威分析と実運用上の必要要件

3. 計量機器に関する法規制と国際規格

4. ソフトウェア要件リストの提案

5. まとめと外部発表

要件比較と不足分の明確化

脅威／運用	保護策／要件	JIS B7611-2	OIML D31	WELMEC 2.3	WELMEC 7.2
「外部通信」による攻撃					
DoS攻撃	通信ポートの開閉制御	×	×	ANNEX II 3.2g	×
	通信制御処理による受信データ制限	×	5.2.1.1.b①	ANNEX II 3.2e	P4
なり					
送受					
「物					
デー					
回路					
不正					
ノイ 温度					
デバ					
「受					
プロ					
内部 (機					
「不					
登録 (特					
イレ					
実運用上で求められる要件(不足分)					
システム構築の前提条件	スケジューリング	×	×	×	×
	アクセス経路の選択	×	×	ANNEX II 3.2h	×
機器側の追加機能	機器稼働状態の明示	×	×	×	×
システム間の認証	更新作業者の認証	×	×	ANNEX II B) B4	×

該当のない7項目に対して、補うための追加要件

追加要件1:「通信先(データサーバー)の認証」

追加要件2:「ハードウェア保護(JTAG端子ほか)」

追加要件3:「ブートプロセス(セキュアブート)」

追加要件4:「メモリ保護(セキュアIC)」

追加要件5:「コアデータのアクセス保護」

追加要件6:「スケジューリング」

追加要件7:「機器稼働状態の明示」

追加するソフトウェア要件の作成

7つの追加要件に対し「目的」、「要件」、「技術的解決案」を提示

追加要件		目的	要件	技術的解決案
1				
2				
3				
4				
5				
6				
7		第三者が外見上で判断することできる。	注：ただし、本要件はソフトウェアのアップロード実施中に機器の動作が停止する場合にのみ適用する。	

例）

追加要件4：「メモリ保護（セキュアIC）」	
目的	重要なパラメータや鍵情報などを通常のアクセス経路から保護する。
要件	機器は重要なパラメータや鍵情報に対するアクセスに保護を実装すること。
技術的解決案	Renesas社製TSIP [1]やARM社製Trust Zone [2]に代表されるようなセキュアICを利用することでメモリ保護を容易に実現できるほか、メモリへのアクセス処理に独自の暗号化や認証を追加する方法でも実現可能である。

ソフトウェア要件リストの提示（抜粋）

1．3　ソフトウェア保護	
	[JIS B7611-2G]：要件G2.2参照
	[OIML D31　]：要件5.1.3参照
	[WELMEC 2.3　]：要件3.1参照
1．3．1　誤操作防止	
	[OIML D31　]：要件5.1.3.1参照
	[WELMEC 7.2　]：要件P5参照
1．3．2　メモリ保護	
	[OIML D31　]：要件5.1.3.2.a参照
	[WELMEC 7.2　]：要件P6参照
1．3．3　固有パラメータの保護	
	[OIML D31　]：要件5.1.3.2.c参照
	[WELMEC 7.2　]：要件P7参照
1．3．4　封印によるソフトウェア保護	
	[OIML D31　]：要件5.1.3.2.d参照
1．3．5　ブートプロセス（セキュアブート）	
	目的：機器のソフトウェア全体の信頼性および完全性を確保する。
	要件：機器は電源ON時のプログラムの起点となるブートから信頼性および完全性のチェックを含めた各ソフトウェアモジュール起動を実施する。
	技術的解決案： Root of TrustやChain of Trustの手法を用いることで実現可能である。組み込み機器のようなハードウェアリソースが少ない構成においても、例えばIAR社が提供するセキュリティ機能Embedded Trustのようなセキュリティツールを利用することで実現可能である。 仕組みについては本論文付録Ⅰ.3「NIST SP800-193の調査」で述べる。

非自動計量機器に対する要件も参照

ソフトウェア要件の参照例

ソフトウェア要件の追記例

要件リスト(関本案)の構成

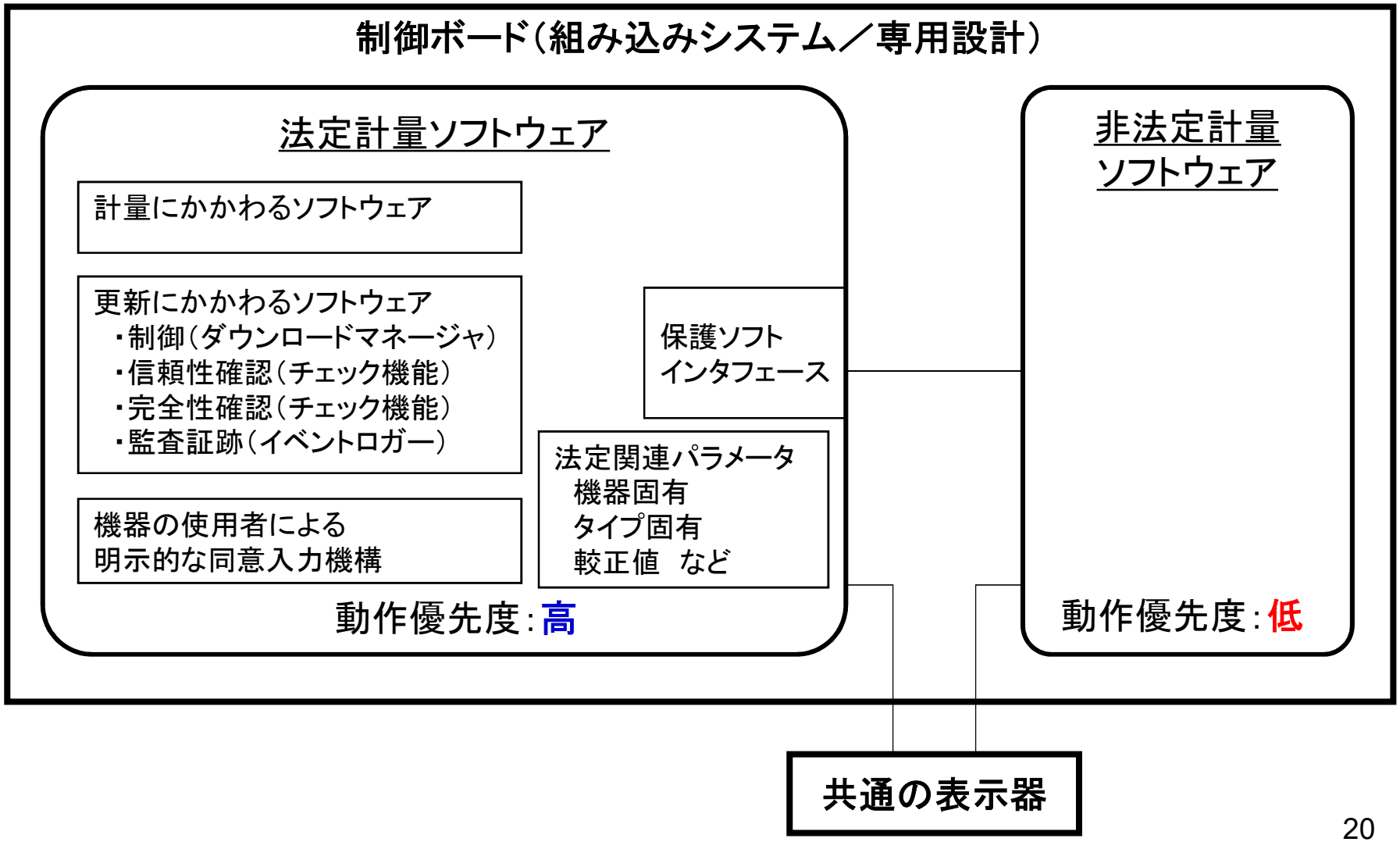
1. 一般要件
  1．1　ソフトウェア識別
  1．2　アルゴリズムと機能の正しさ
  1．3　ソフトウェア保護
    1．3．1　誤操作防止
    1．3．2　メモリ保護
    1．3．3　固有パラメータの保護
    1．3．4　封印によるソフトウェア保護
    1．3．5　ブートプロセス(セキュアブート)
  1．4　ユーザーインタフェース
    1．4．1　コアデータのアクセス保護
  1．5　ハードウェア機能の支援
    1．5．1　故障の検出
    1．5．2　耐久性の検出
    1．5．3　ハードウェア保護(JTAG端子ほか)
  1．6　測定データの提示

2. 機能別要件
  2．1　ソフトウェアの分離
    2．1．1　電子装置の部品装置の分離
    2．1．2　ソフトウェア部分の分離
  2．2　表示の共有
  2．3　ソフトウェアダウンロード
    2．3．1　法定計量ソフトウェア
    2．3．2　ソフトウェア更新
      2．3．2．1　立ち合い者あり
      2．3．2．2　立ち合い者なし
        ①　スケジューリング
        ②　機器稼働状態の明示
    2．3．3　装置固有パラメータの設定
    2．3．4　法定計量に関連するソフトウェア範囲
    2．3．5　データサーバーの認証
  2．4　データの保存
    2．4．1　保存すべき情報
    2．4．2　暗号化
    2．4．3　自動保存
    2．4．4　時刻刻印
    2．4．5　外部要因からの保護
    2．4．6　記憶容量と持続性
    2．4．7　メモリ保護(セキュアIC)
  2．5　外部インタフェース
    2．5．1　インタフェースの保護
    2．5．2　通信暗号化
    2．5．3　データの保証(信頼性、完全性)
    2．5．4　外部要因からの保護
    2．5．5　破損したデータの取り扱い
    2．5．6　転送遅延
    2．5．7　転送中断

※**青文字**の項目が新規で追加した要件

要件を満たすシステム構成案

必要最小限の構成を図示すると以下のとおり



1. 研究概要

2. 脅威分析と実運用上の必要要件

3. 計量機器に関する法規制と国際規格

4. ソフトウェア要件リストの提案

5. まとめと外部発表

研究成果のまとめ

計量機器における実運用を考慮したリモート更新可能なシステム構築に必要なソフトウェア要件リストを作成するにあたり、下記3点について保護策を調査・検討した。

- 自動計量機器に対する法規制、国際規格
- 非自動計量機器に対する法規制、国際規格
- 要件の不足分に対する新規ソフトウェア要件案の作成

研究成果として、計量機器に関するソフトウェア要件をすべて盛り込んだソフトウェア要件リストの作成と、リモート更新機能を実装するシステム構築に必要な構成を提示した。

本研究成果は、現状ではOIMLの国際勧告に準拠することでカバーされている国内法規制（計量法／JIS規格）および国際規格やガイドラインに対してソフトウェア要件・認証の策定や改定をおこなう際の議論に貢献できると考える。

国内法規制および国際規格・ガイドラインへの提言

現在の法規制、国際規格・ガイドラインに本研究成果を適用する場合の残課題

- ✓ <u>ソフトウェア分離に関して前提条件を明確にすること</u>
  現場の立ち合いが不要なリモート更新機能を実現するためにはソフトウェアの分離が必要条件となる。しかし、分離の前提条件となる法定関連部分と非法定関連部分の切り分けが不明瞭である。
- ✓ <u>統一的な保護範囲を対象とした要件記述にすること</u>
  本研究で調査対象とした国内法規制および国際規格・ガイドラインにおいて、対象とするシステム（機器）の分類によって、ソフトウェア要件で定める保護範囲が異なる傾向がみられる。

今後のソフトウェア要件・認証の策定や改定によって、ソフトウェア分離に関する明確な基準、また統一された保護範囲に対する要件が提示されることが望ましい。

外部発表（予定）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

◆ 情報処理学会　第82回全国大会

2020年3月5日（木）～7日（土）
金沢工業大学　扇が丘キャンパス
https://www.ipsj.or.jp/event/taikai/82/

公演区分：学生セッション
公演番号：2J-03
公演日時：2020年3月5日（木）　13:10～15:10

ご清聴ありがとうございました。

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

要件比較と不足分の明確化

明日の信頼を創ろう
情報セキュ
INSTITUTE of INFORMATION SECURITY

印刷用参考ページ

脅威／運用	保護策／要件	JIS B7611-2	OIML D31	WELMEC 2.3	WELMEC 7.2
「外部通信」による攻撃					
DoS攻撃	通信ポートの開閉制御	×	×	ANNEX Ⅱ 3.2g	×
	通信制御処理による受信データ制限	×	5.2.1.1.b①	ANNEX Ⅱ 3.2e	P4
なりすまし	データサーバの認証	×	×	×	×
	通信の暗号化	×	5.2.3.3	×	P8, T5, D1
送受信処理の脆弱性を利用したメモリ破壊	送受信処理の対策強化	×	5.1.3.2.b 5.2.1.1.b①	ANNEX Ⅱ 3.2e	P4
「物理的な破壊・改ざん」による攻撃					
データ保護のための封印破壊	電子封印システム	×	5.1.3.2.d	ANNEX Ⅱ 3.3a	L5
回路パターンの解析、実装ICの不正交換	基板のコーティング	×	×	×	P6
	実装ICのSOP化	×	5.1.3.2.a①	×	P6
不正な機器の中継、ぶらさがり	機器間のデータチェック	G3.4	5.1.3.2.a②	×	P8
	通信の暗号化	×	5.1.3.2.a②	×	P8
ノイズや電源グリッチの挿入、 温度変化による誤作動誘発	ノイズ対策	×	×	×	P5, L2
	誤動作防止の対策強化	×	×	×	P5, L2
デバック用JTAG端子からの不正アクセス	デバック用JATG端子のパターン削除	×	×	×	×
「受信および内部データの改ざん」による攻撃					
プログラムデータの改ざん	プログラムデータの信頼性確認	×	5.1.4.1	ANNEX Ⅱ B)B2, 3.3a	D2
	データの完全性確認	×	5.2.3.2	ANNEX Ⅱ B)B2, 3.3b	D3
	チェックサム	G2.2.2	5.1.4.1	3.1③, 3.3①	P5
	アップデート・監査ログ	×	5.2.6.3.e	ANNEX Ⅱ B)B3, 3.3d	D4
	Root of Trust／Chain of Trust	×	×	×	×
内部データの改ざん （機器動作にかかわるシステムデータ）	内部データのアクセス保護	×	5.1.3.2.c	×	P7
	データの完全性確認	×	5.2.3.2	×	L3
	チェックサム	G2.2.3	5.1.4.1	3.1③, 3.3①	P5, L2
	変更・監査ログ	G2.2.3	5.2.3.2 5.2.6.4	3.1③	P7
	TSIP／Trust Zone	×	×	×	×
「不正操作」による攻撃					
登録権限の奪取による不正値入力 （特に機器のコアデータ）	権限の厳格管理	×	5.1.3.2.d③	×	×
	操作者の限定	×	5.1.3.2.d③	×	×
	コアデータのアクセス保護	×	×	×	×
イレギュラーな操作による誤動作誘発	誤動作防止の対策強化	×	5.1.3.1	×	P3, P5
実運用上で求められる要件（不足分）					
システム構築の前提条件	スケジューリング	×	×	×	×
	アクセス経路の選択	×	×	ANNEX Ⅱ 3.2h	×
機器側の追加機能	機器稼働状態の明示	×	×	×	×
システム間の認証	更新作業者の認証	×	×	ANNEX Ⅱ B)B4	×

追加するソフトウェア要件の作成

印刷用参考ページ

7つの追加要件に対し「目的」、「要件」、「技術的解決案」を提示

追加要件		目的	要件	技術的解決案
1	通信先（データサーバー）の認証	ソフトウェアダウンロード実施時に正規データサーバ以外と接続を確立させない。	ソフトウェアダウンロード実施時にはアクセス先（データサーバ）の認証処理を実施する。	ソフトウェアダウンロード実施時のアクセス先確認で認証処理をおこなうことによって正規データサーバ以外と接続を確立させないことが必要となる。例えば電子署名を利用したデータサーバとの相互認証や一般的なIDとパスワードを使用したログイン認証方式などをおこなうことで実現可能である。
2	ハードウェア保護（JTAG端子他）	電気回路やICを含むハードウェアの物理的アクセス経路からの不正防止。	機器のハードウェアからは、不要なアクセス経路を削除すべき。	機器の不必要な物理的アクセス経路を削除することが必要となる。代表的な例としてはJTAG端子とよばれるエミュレータ接続端子が挙げられる。本来はソフトウェア開発時や製品の内部メモリ状態を参照するためのアクセス経路になるが、機器販売後の通常稼働時には使用されない。このアクセス経路を物理的に削除しておくことでハードウェアの保護を実現可能である。
3	ブートプロセス（セキュアブート）	機器のソフトウェア全体の信頼性および完全性を確保する。	機器は電源ON時のプログラムの起点となるブートから信頼性および完全性のチェックを含めた各ソフトウェアモジュール起動を実施する。	Root of TrustやChain of Trustの手法を用いることで実現可能である。組み込み機器のようなハードウェアリソースが少ない構成においても、例えばIAR社が提供するセキュリティ機能Embedded Trust [9]のようなセキュリティツールを利用することで実現可能である。Root of TrustおよびChain of Trustの仕組みについては本論文付録Ⅰ.3「NIST SP800-193の調査」の項目で述べている。
4	メモリ保護（セキュアIC）	重要なパラメータや鍵情報などを通常のアクセス経路から保護する。	機器は重要なパラメータや鍵情報に対するアクセスに保護を実装すること。	Renesas社製TSIP [1]やARM社製Trust Zone [2]に代表されるようなセキュアICを利用することでメモリ保護を容易に実現できるほか、メモリへのアクセス処理に独自の暗号化や認証を追加する方法でも実現可能である。
5	コアデータのアクセス保護	ユーザーインタフェースを利用した登録作業やパラメータ変更からのコアデータ保護。	登録作業やパラメータ変更に対して、厳格なアクセス権限管理を実施すること。	機器内のパラメータやデータの重要度合いをレベル分けし、機器の動作にかかわる重要データを変更する際には特別な権限管理を必要とするように設計することで実現可能である。特別な権限管理の例としては、ワンタイムパスワードやIC認証などが挙げられる。
6	スケジューリング	機器の稼働状況に応じたソフトウェアダウンロードの実施スケージュールを指定する。	機器におけるソフトウェアダウンロード可能な日時等をスケジューリングできる機能を実装する。これは外部からのソフトウェアダウンロード実施要求（リモート更新）に対しても有効な機能であること。 注：ただし、本要件はソフトウェアのダウンロード実施中に機器の動作が停止する場合にのみ適用する。	機器の内部にソフトウェアダウンロード可能なタイミングに関するデータを保持する領域を設け、機器の使用状況に応じて任意に設定可能なパラメータとして保存することで実現可能である。このデータは重要なデータとして扱い、追加要件5「コアデータのアクセス保護」の適用を受けるものとする。
7	機器稼働状態の明示	機器が通常稼働中であるか、ソフトウェアダウンロード実施時であるかを第三者が外見上で判断することできる。	作業者もしくは使用者の立ち合いがない状態でのソフトウェアのダウンロード実施時には、外見上で機器が稼働を停止していることを判断できるようにする。 注：ただし、本要件はソフトウェアのダウンロード実施中に機器の動作が停止する場合にのみ適用する。	機器に実装された表示もしくはインジケータなどにより外見上で機器が稼働を停止していることを判断できるようにすることで実現可能である。ただし、通常稼働時の表示と混同されないような明確な違いを設けることが必要である。