情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

ネットワーク接続を考慮したレガシー制御システムにおける脅威分析と対策の評価

2024/02/13

5535701

大久保研究室　M1 平澤 凌一

発表項目

- 研究背景
- 目的
- 制御システムのセキュリティ
- 関連技術
- 関連研究
- 脅威分析と対策の評価結果
- まとめと今後の展望

発表項目

- 研究背景
- 目的
- 制御システムのセキュリティ
- 関連技術
- 関連研究
- 脅威分析と対策の評価結果
- まとめと今後の展望

研究背景

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

デジタルトランスフォーメーション(DX)の進展

IoTやAIなどの先端技術や
クラウドサービスを活用するスマート工場化

生産の最適化・効率化などの事業効果

研究背景

デジタルトランスフォーメーション(DX)の進展

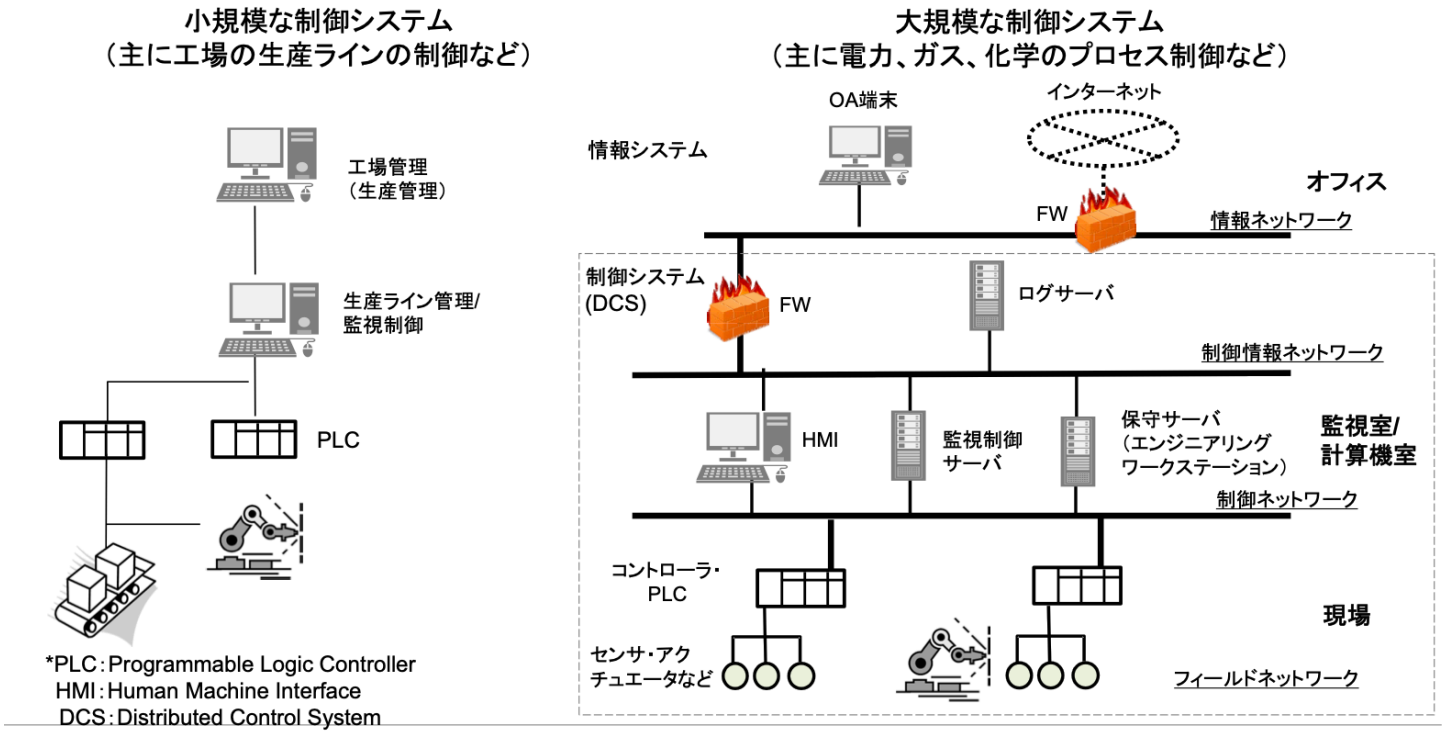
IoTやAIなどの先端技術や
クラウドサービスを活用するスマート工場化

工場のネットワークをインターネットや
情報システムに接続する機会が増加

既存の工場設備も含めた工場システム全体における
セキュリティ対策の検討が必要

制御システム

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



- 工場の生産・加工ラインなどで機器制御に利用
- コントローラやHMIをネットワークで接続

【出典：IPA, 「制御システム利用者のための脆弱性対応ガイド」】

研究背景

既存制御システムの課題

従来、制御システムは、固有システムで構成され
外部ネットワークや共有システムとは非接続

ネットワーク経由の
セキュリティ脅威は未考慮

高いセキュリティリスクを保有する
既存の制御システムを**レガシー制御システム**と定義

目的

レガシー制御システムにおいて
ネットワーク接続に対する脅威を分析・対策を評価

現実に即した想定システムの脅威分析・対策評価
具体的な対策・実施対策選定のための指標の提案

発表項目

- 研究背景
- 目的
- **制御システムのセキュリティ**
- 関連技術
- 関連研究
- 脅威分析と対策の評価結果
- まとめと今後の展望

制御システムの変遷

オープン化とセキュリティリスク

ベンダ固有の設計・規格の機器によるシステム構築から
運用・開発コスト削減および柔軟性の高い機器利用へ

Windows・Linuxなどの汎用OS
イーサネット・無線LANの標準通信規格

- 製品規格情報に基づいた攻撃
- 保守・サポートの終了による脆弱性の保持

制御システムと情報システムの違い

制御システム	セキュリティ項目	情報システム
20年	サポート期間	2~3年
単一	ベンダー	多様
非定期・非計画的	パッチ適用	定期・計画的
低・物理レベル	セキュリティ意識	高・先進技術
可用性＞完全性＞機密性	優先順位	機密性＞完全性＞可用性

制御システムのセキュリティにおいては

可用性を最も重視

発表項目

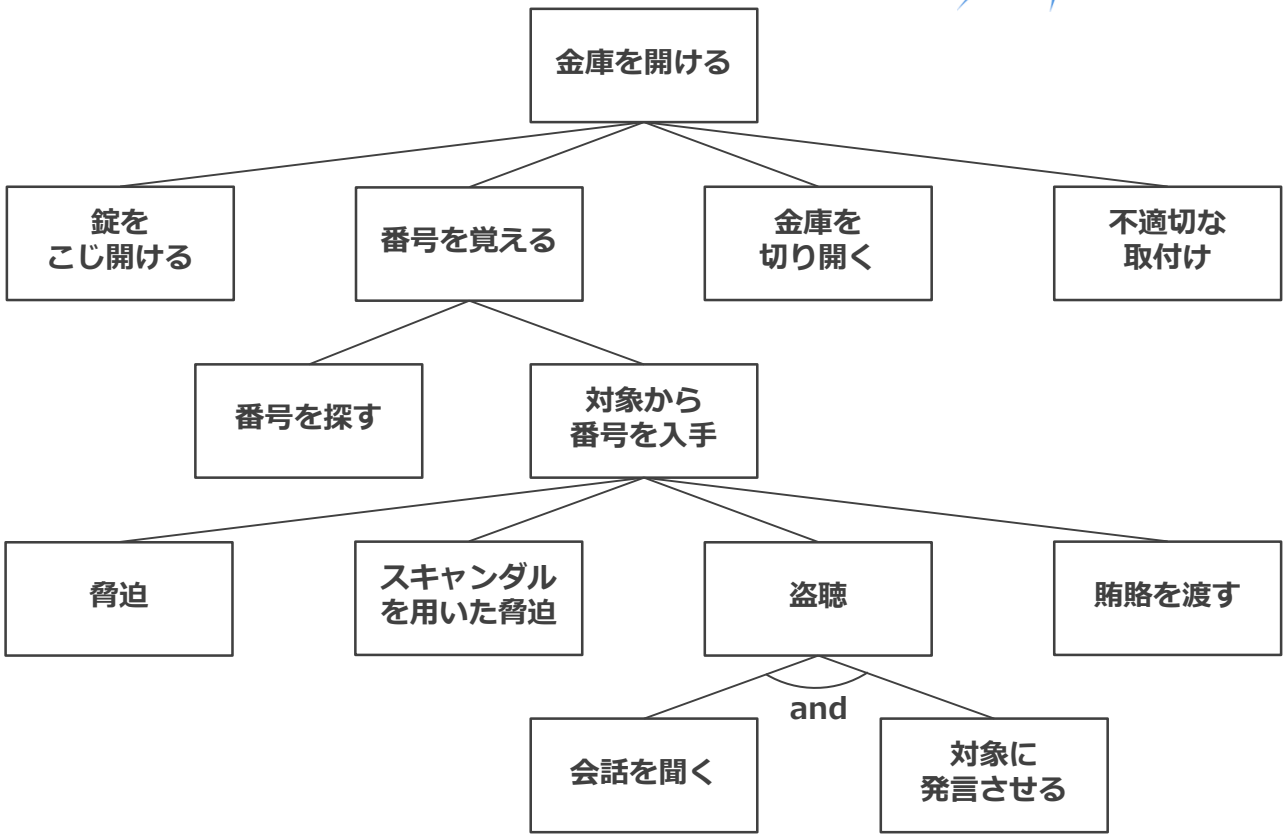
- 研究背景
- 目的
- 制御システムのセキュリティ
- **関連技術**
- 関連研究
- 脅威分析と対策の評価結果
- まとめと今後の展望

STRIDE

脅威カテゴリ	想定される脅威例
Spoofing (なりすまし)	権利がないユーザによる 保護資産の利用
Tampering (改竄)	悪意あるユーザによる データやプログラムの変更
Repudiation (否認)	ログ消去等の ユーザによる操作の隠匿
Information Disclosure (情報漏洩)	内部利用のみを想定した データ資産の漏洩
Denial of Service (サービス拒否)	サーバー・ネットワークへの過負荷
Elevation of Privilege (権限昇格)	管理者権限の奪取

Attack Trees

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

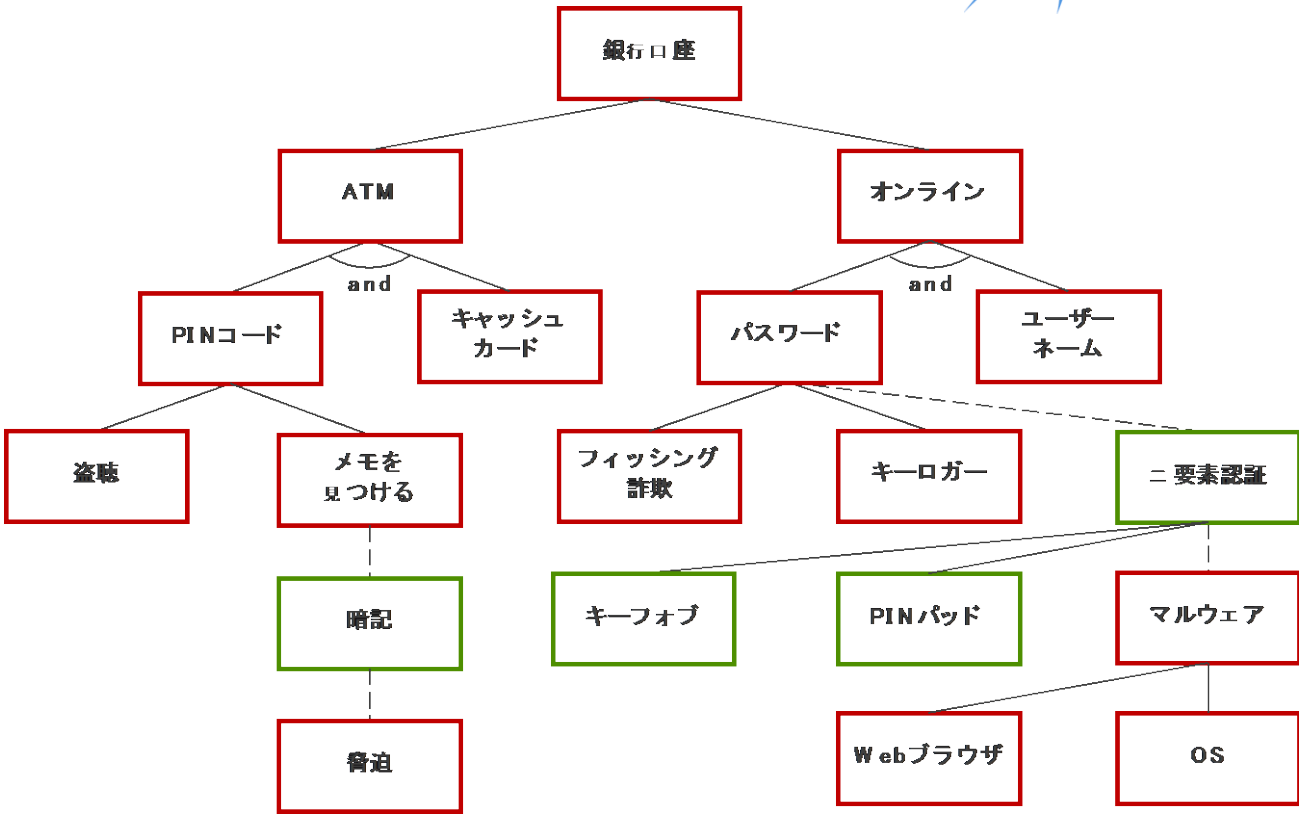


攻撃を達成する手段をツリー構造で表現

→ 具体的な攻撃手法が認識可能

Attack Defense Trees

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



攻撃を実行するための手段とそれに対する対応策をツリー構造で可視化

CVSS(共通脆弱性評価システム)

基本評価基準 (Base Metrics)

攻撃区分、攻撃条件の複雑さ、etc.

現状評価基準 (Temporal Metrics)

攻撃される可能性、利用可能な対策のレベル、etc.

環境評価基準 (Environmental Metrics)

対象システムのセキュリティ要求度、etc.

オープンで汎用的・ベンダーに依存しない

３つの基準で、脆弱性の深刻度を評価

発表項目

- 研究背景
- 目的
- 制御システムのセキュリティ
- 関連技術
- **関連研究**
- 脅威分析と対策の評価結果
- まとめと今後の展望

関連研究[1]

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

[1]“脅威分析に基づいた工場内制御システムのセキュリティ向上策の提案”

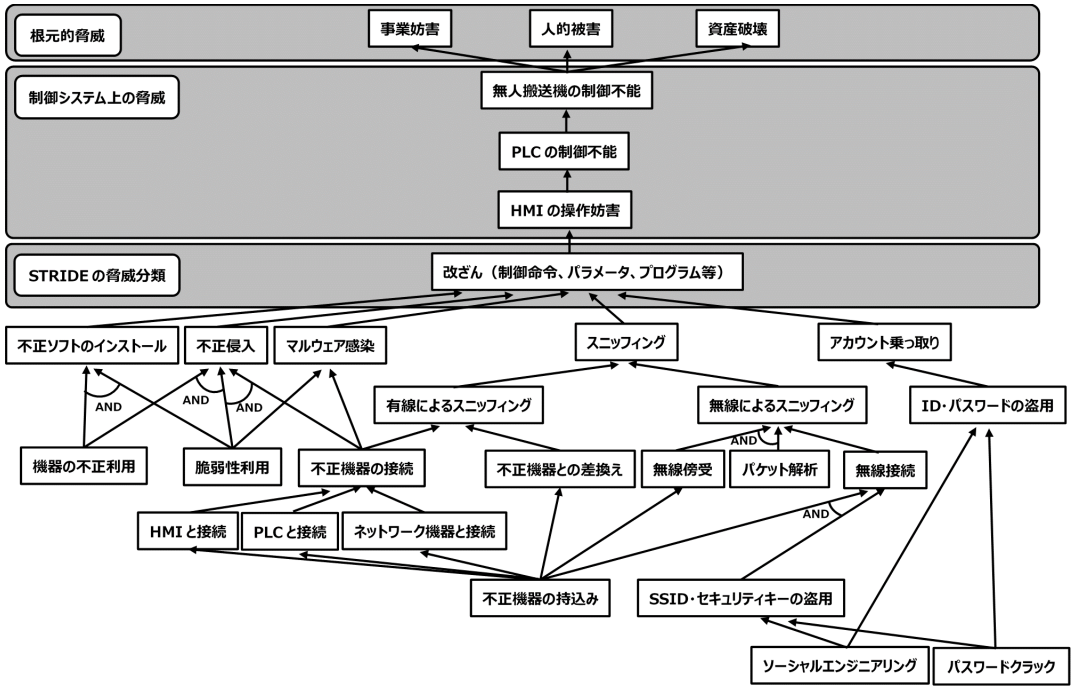
竹本，情報セキュリティ大学院大学2016年度特定課題研究報告書

制御システムの脅威を定型的に識別する手法を提示

脅威に対する対策の導出と評価

関連研究[1]

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



STRIDE-Tree (改竄)[1]

STRIDEとAttack Treesを組み合わせることで、脅威を定型的に分析

[1]竹本，特定課題研究報告書，2016.

関連研究[1]

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

セキュリティ対策の導出例[1]

	脅威		
	不正機器の持込み	パスワードクラック	ソーシャル エンジニアリング
予防	・監視カメラの設置 ・構内管理規則の周知 ・罰則規定の策定	・パスワード複雑化 ・アカウントロック ・セキュリティトークン ・生体認証	・セキュリティ教育 ・機密書類の適切な廃棄
検知	・システム管理者の監視	・ログイン処理の常時監視 ・ログイン処理のログ確認	・N/A
復旧	・不正機器の排除	・ID/パスワードの変更	・システム設定の見直し

予防・検知・復旧の観点から、

セキュリティ対策を導出

[1]竹本，特定課題研究報告書，2016 .

関連研究[1]

セキュリティ対策の評価例[1]

	パスワードクラック	実施状況	実施時の影響	実施時のコスト
対策	パスワード複雑化	済	-	-
	アカウントロック	未	低	低
	セキュリティトークン	未	中	中
	生体認証	未	高	中
	ログイン処理の常時監視	未	高	高
	ログイン処理のログ確認	未	中	低

対策に対して、実施時の影響とコストの観点から、「高」、「中」、「低」の3段階で評価

[1]竹本，特定課題研究報告書，2016.

発表項目

- 研究背景
- 目的
- 制御システムのセキュリティ
- 関連技術
- 関連研究
- **脅威分析と対策の評価結果**
- まとめと今後の展望

本研究

先行研究との比較

	脅威識別手法	対策策定方針	対策の評価
本研究	STRIDE-Tree + Attack Defense Trees	予防 検知	実施時の 「影響」 「コスト」 + CVSS環境値
関連研究[1]	STRIDE-Tree	予防 検知 復旧	実施時の 「影響」 「コスト」

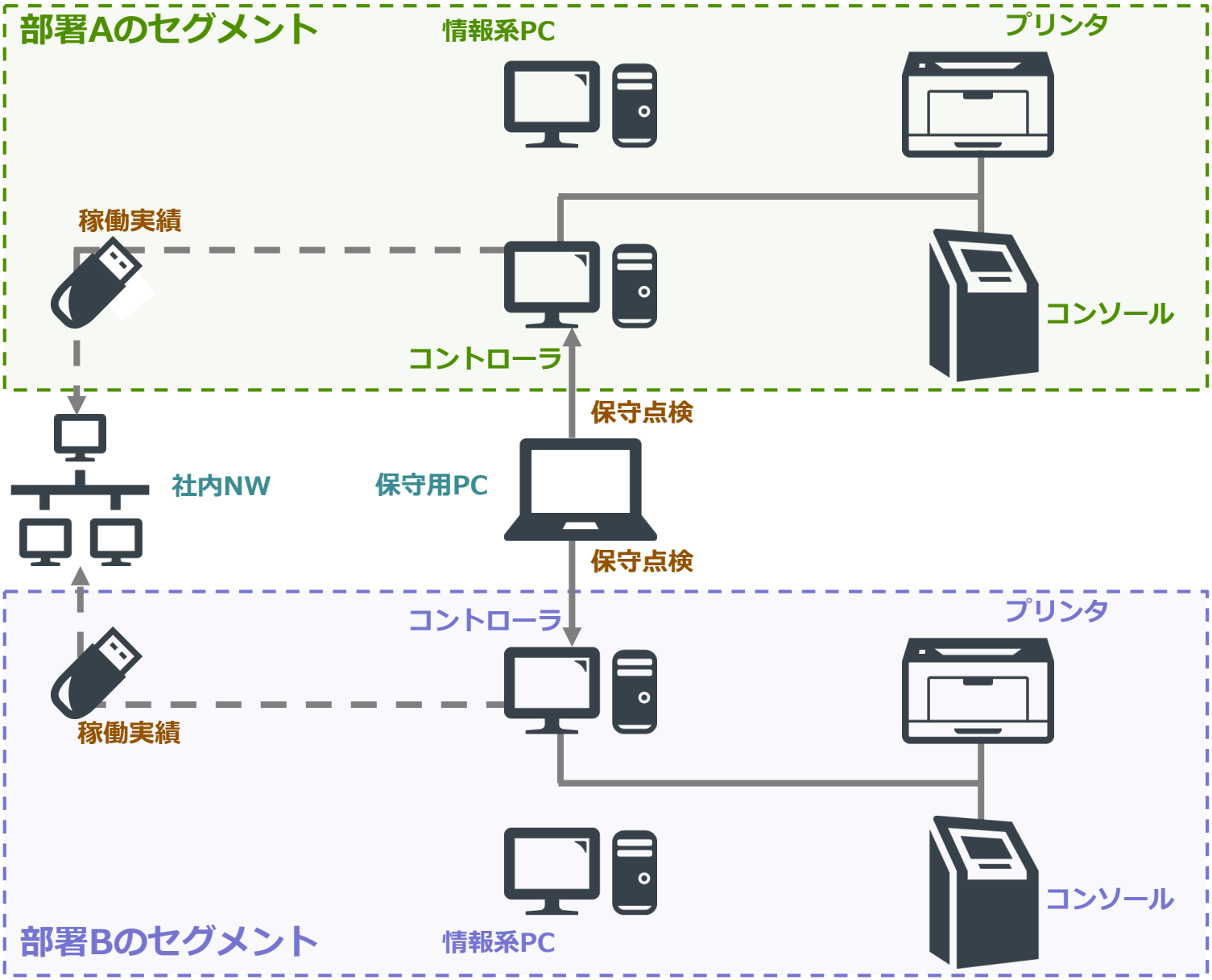
Attack Defense Treesへの拡張

定量的評価の実施

[1]竹本，特定課題研究報告書，2016.

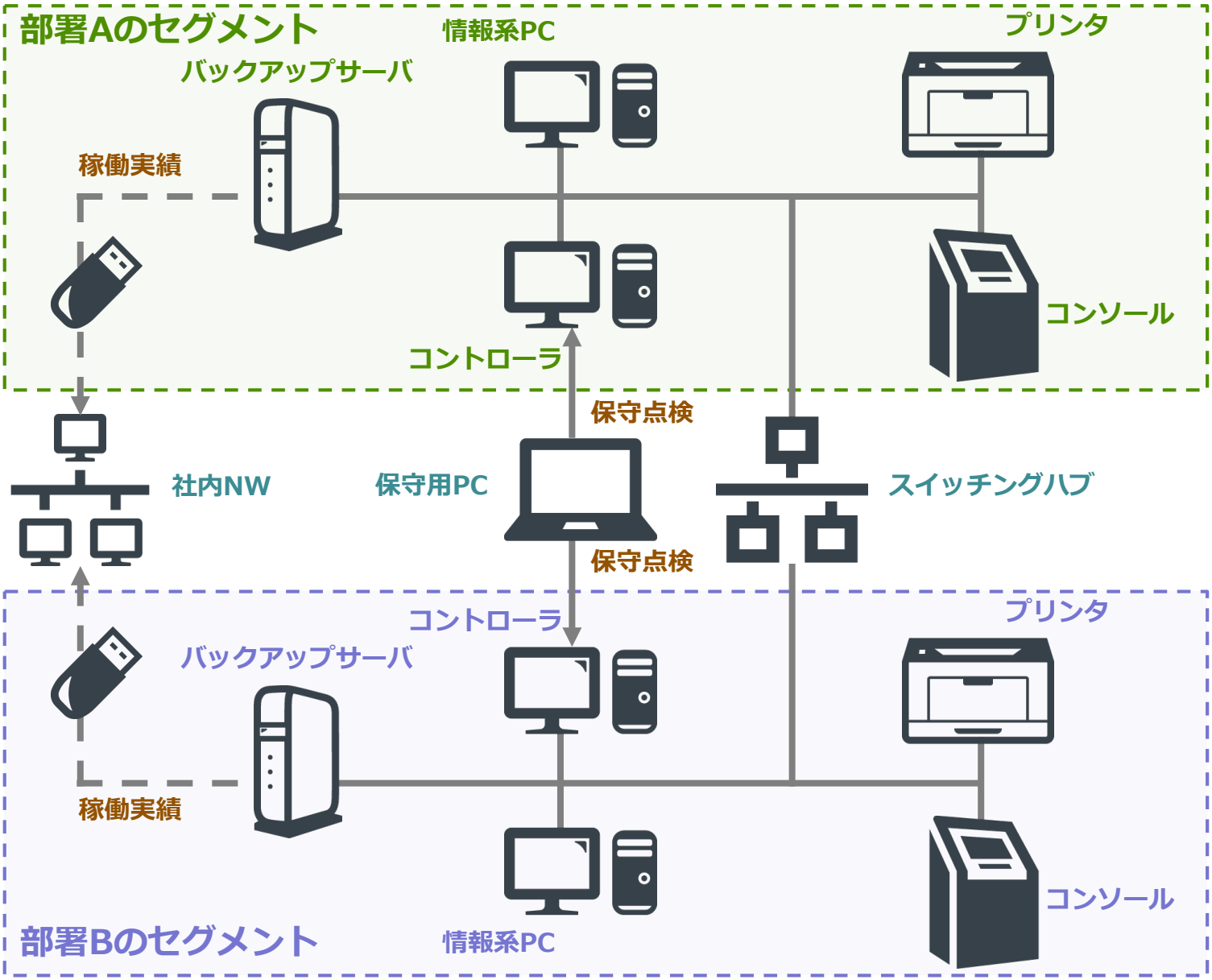
想定する制御システム

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



想定する制御システム

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

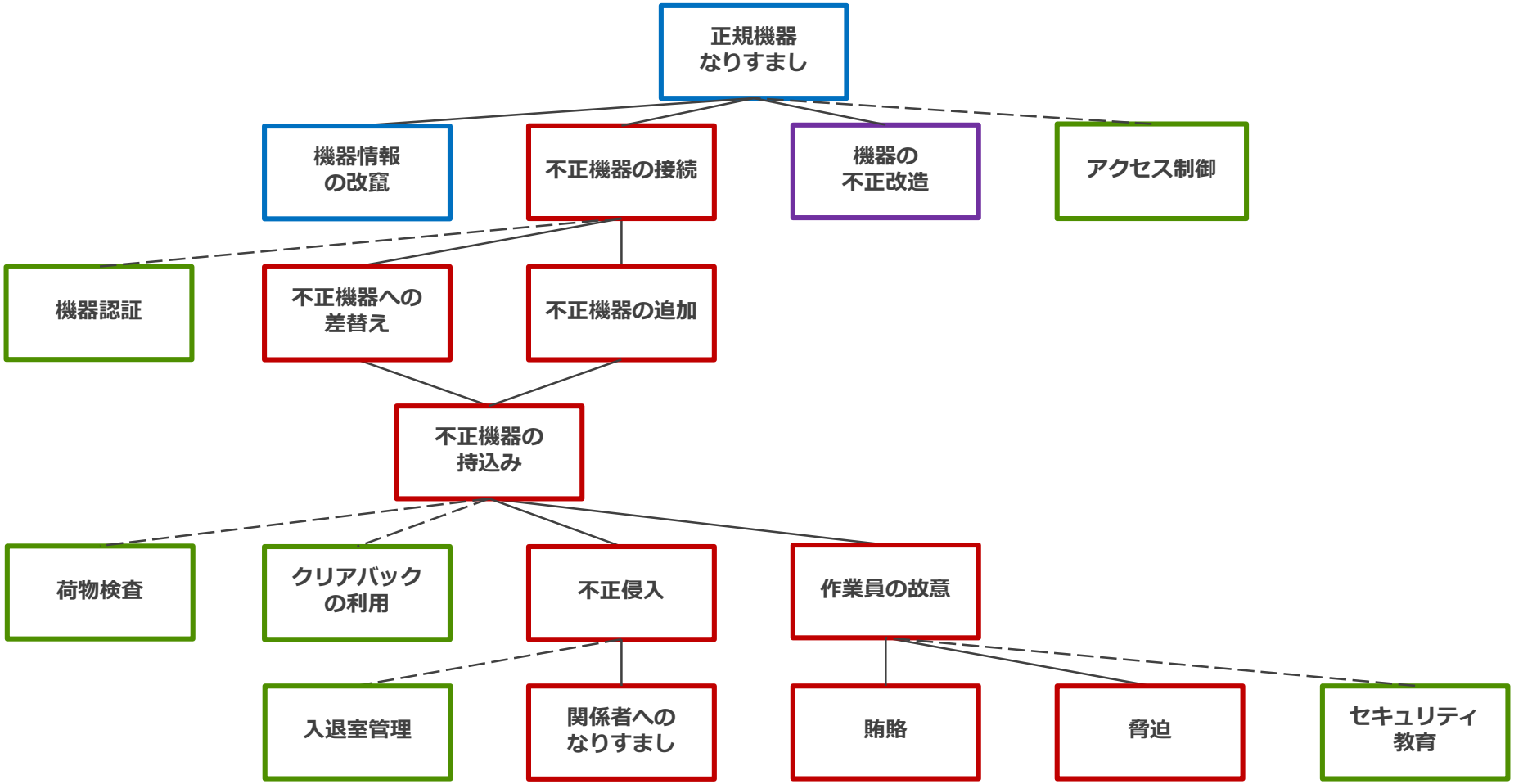


STRIDEによる分析結果

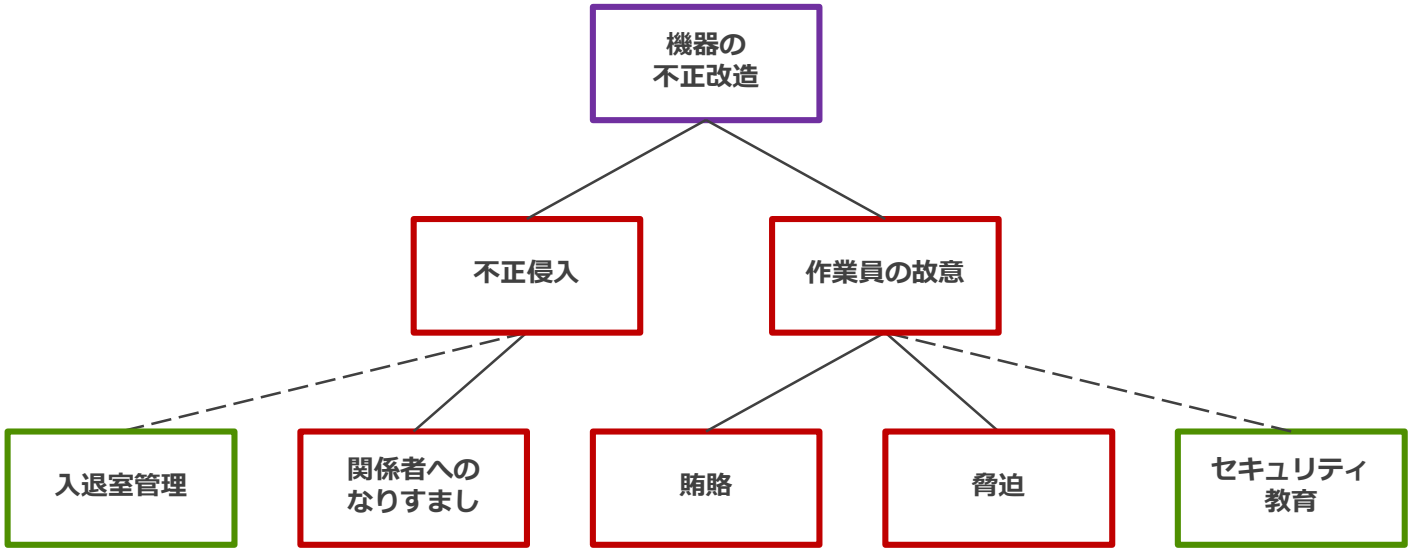
S:正規操作なりすまし
　正規機器なりすまし
T:情報資産/センサ信号の改竄
　アカウント情報/機器情報の改竄
R:操作履歴の削除
I:機密情報の漏洩
D:制御端末の制御不能
E:管理者権限の不正取得

STRIDE-Trees(なりすまし)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



部分木

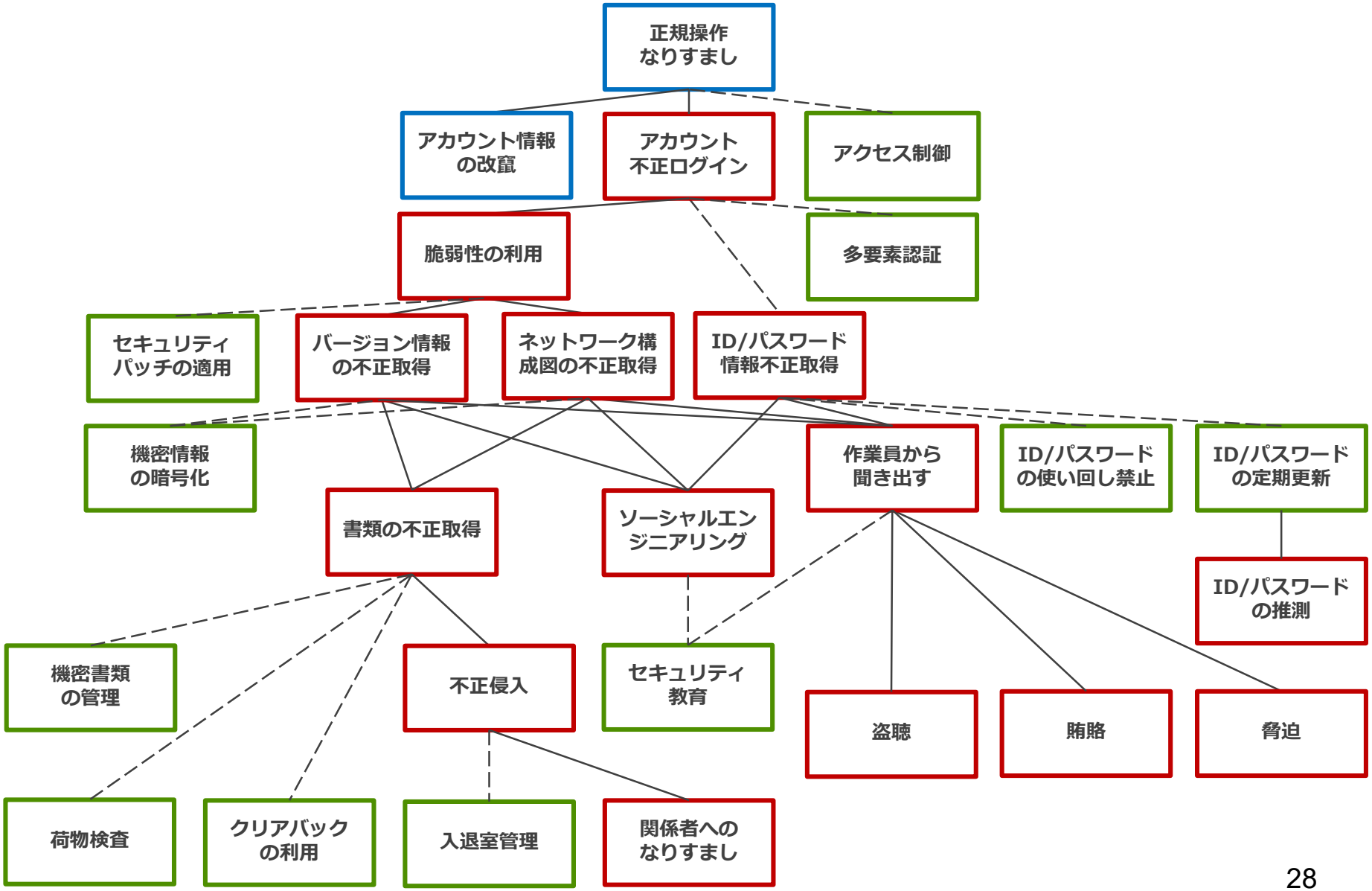


部分木を別途にまとめることで

ツリー構造の把握が容易に

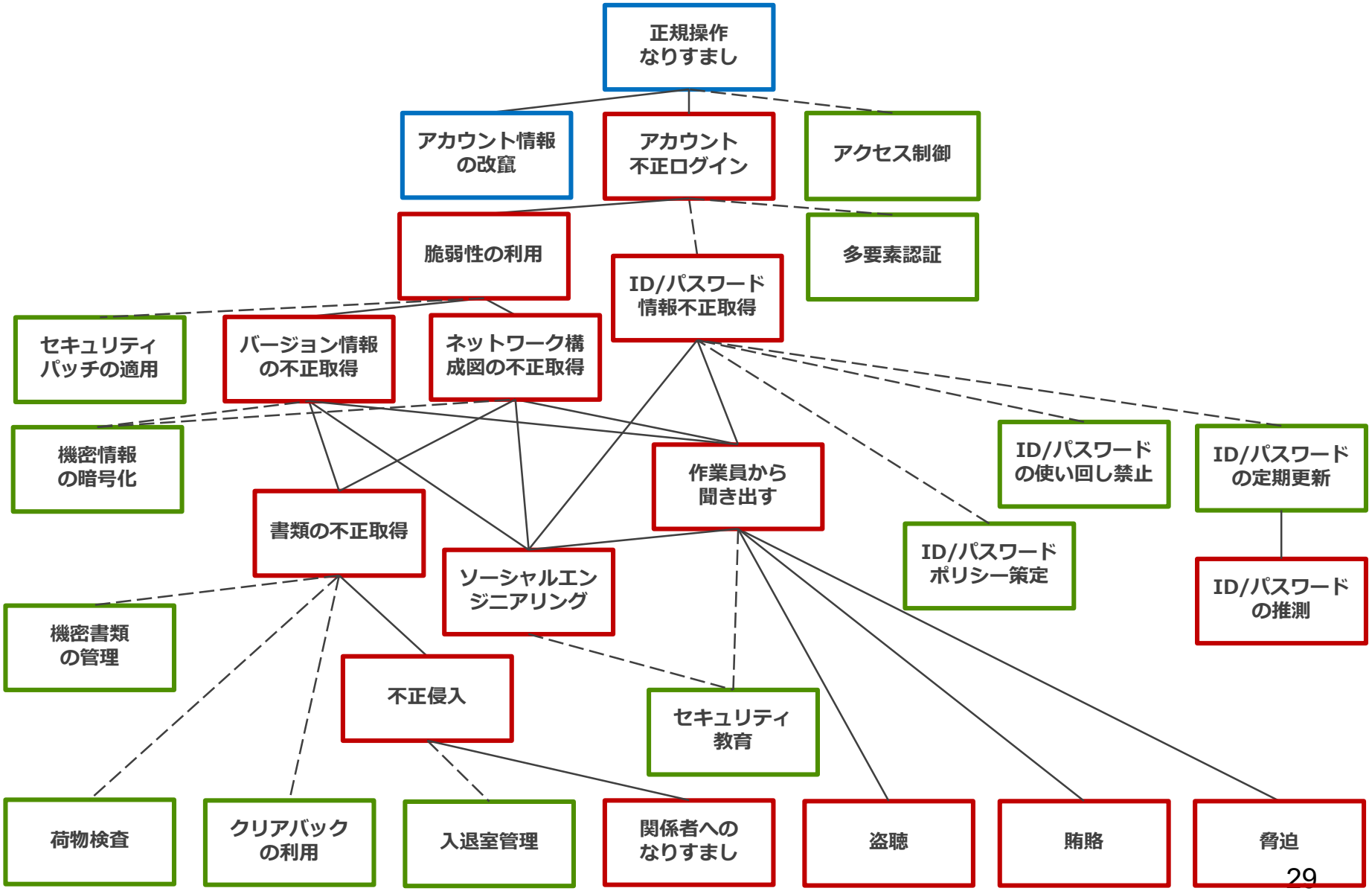
ツリー構造の妥当性評価反映前

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



ツリー構造の妥当性評価反映後

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



セキュリティ対策の導出例

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

脅威	情報資産の改竄	操作履歴の削除	正規操作なりすまし
予防	・アクセス制御 ・バックアップ ・権限管理	・セキュリティ教育 ・アクセス制御 ・バックアップ ・権限管理	・パッチの適用 ・アクセス制御 ・多要素認証 ・ID/パスワードの適切な管理
検知	・異常検知システムの実装	・異常検知システムの実装	・異常検知システムの実装
復旧	・データの復元	・データの復元	・被害範囲の特定

予防・検知の観点から、ツリー構造内において
セキュリティ対策を導出

セキュリティ対策の評価例

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

脅威		情報資産の改竄	操作履歴の削除	正規操作なりすまし
対策		バックアップ	アクセス制御	多要素認証
実施時の影響		低	中	高
実施時のコスト		低	低	中
CVSS環境値	対策後	4.6	6.0	6.4
	対策前	7.6	7.6	7.6
CVSS基準値		8.7	7.4	7.8

対策に対して、実施時の影響とコストの観点と対策前後のCVSS環境により評価

発表項目

- 研究背景
- 目的
- 制御システムのセキュリティ
- 関連技術
- 関連研究
- 脅威分析と対策の評価結果
- **まとめと今後の展望**

まとめと今後の展望

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

まとめ

- 現実に即した制御システムを想定
- 「STRIDE」と「Attack Defense Trees」による脅威分析
- 実施時の「影響」と「コスト」および、対策前後の「CVSS環境値」による評価

今後の展望

- CVSS v4や他の評価手法導入の検討
- 評価結果に基づき選定された対策の実効性の検証

CVSS(共通脆弱性評価システム)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

CVSS基本値(Base Score)

影響度 = 10.41 × (1 - (1 - C) × (1 - I) × (1 - A))

攻撃容易性 = 20 × AV × AC × Au

f(影響度) = 0(影響度が0), 1.176(影響度が0以外)

基本値 = ((0.6 × 影響度) + (0.4 × 攻撃容易性) - 1.5)
× f(影響度)

AV:攻撃元区分, AC:攻撃条件の複雑さ, Au:攻撃前の認証要否
C:機密性への影響, I:完全性への影響, A:可用性への影響

CVSS(共通脆弱性評価システム)

CVSS現状値(Temporal Score)

現状値 ＝ 基本値 × E × RL × RC

E:攻撃される可能性
RL:利用可能な対策のレベル

RC:脆弱性情報の信頼性
- 未確認:0.90
- 未確証:0.95
- 確認済:1.00
- 未評価:1.00

CVSS(共通脆弱性評価システム)

CVSS環境値(Environmental Score)

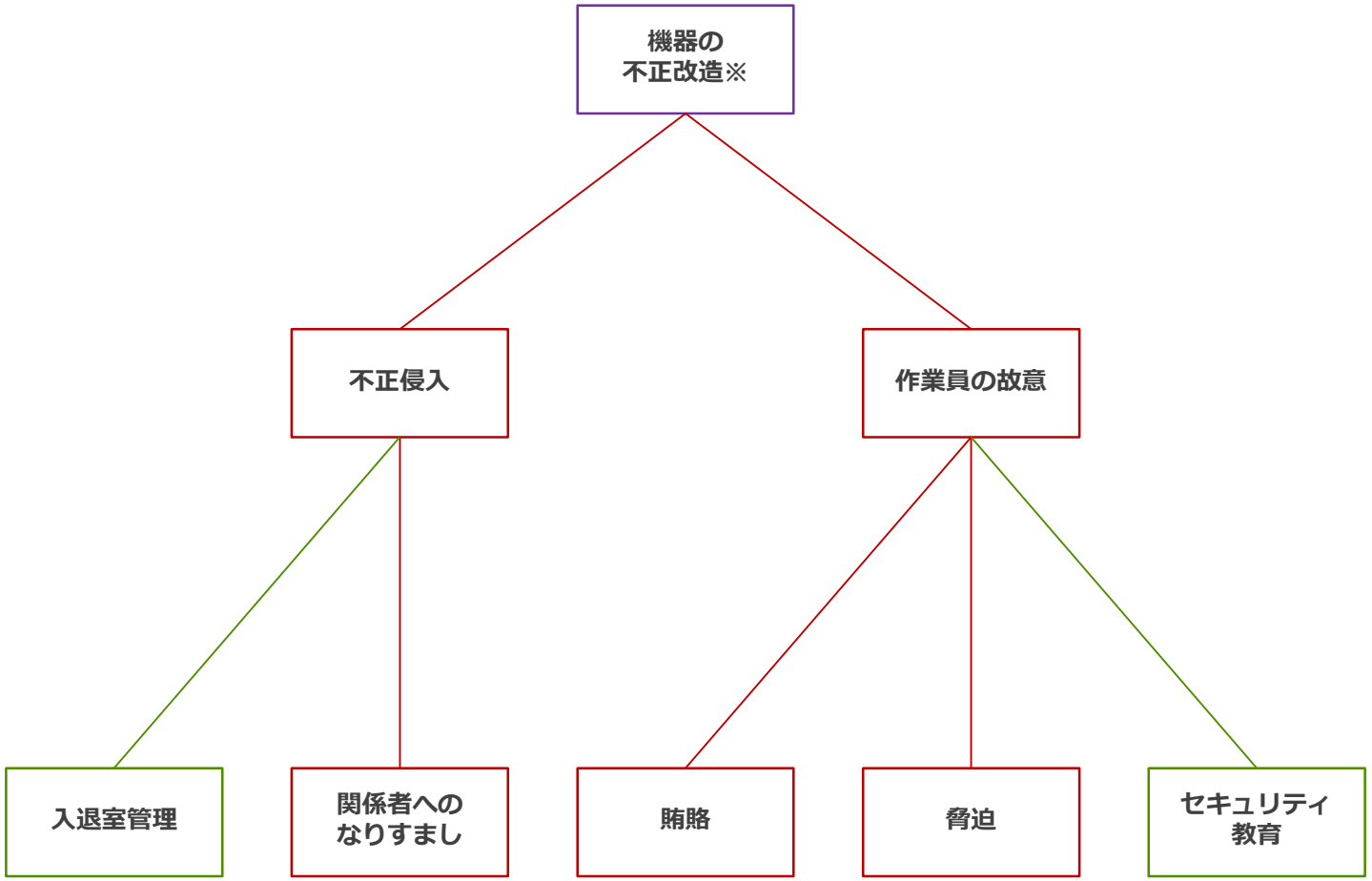
調整後影響度 = min(10.0, 10.41
× (1 - (1 - C × CR) × (1 - I × IR) × (1 - A × AR)))

調整後現状値 = 影響度に調整後影響度の計算結果を代入し、
基本値を再計算。その基本値で現状値を再計算

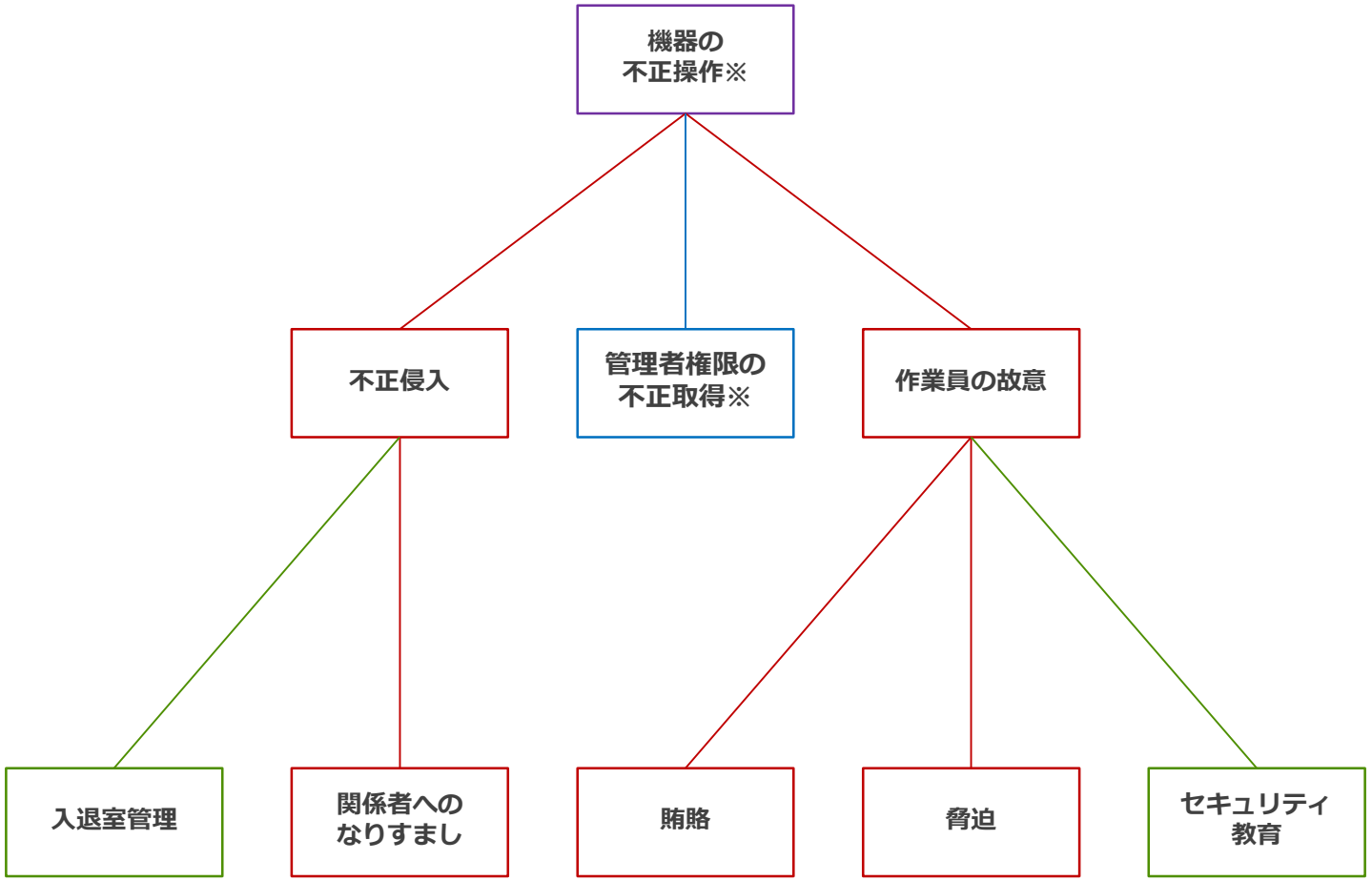
環境値 = (調整後現状値 + (10 - 調整後環境値) × CD) × TD

CD:二次的被害の可能性, TD:影響を受ける対象システムの範囲
CR:機密性の要求度, IR:完全性の要求度, AR:可溶性の要求度

部分木

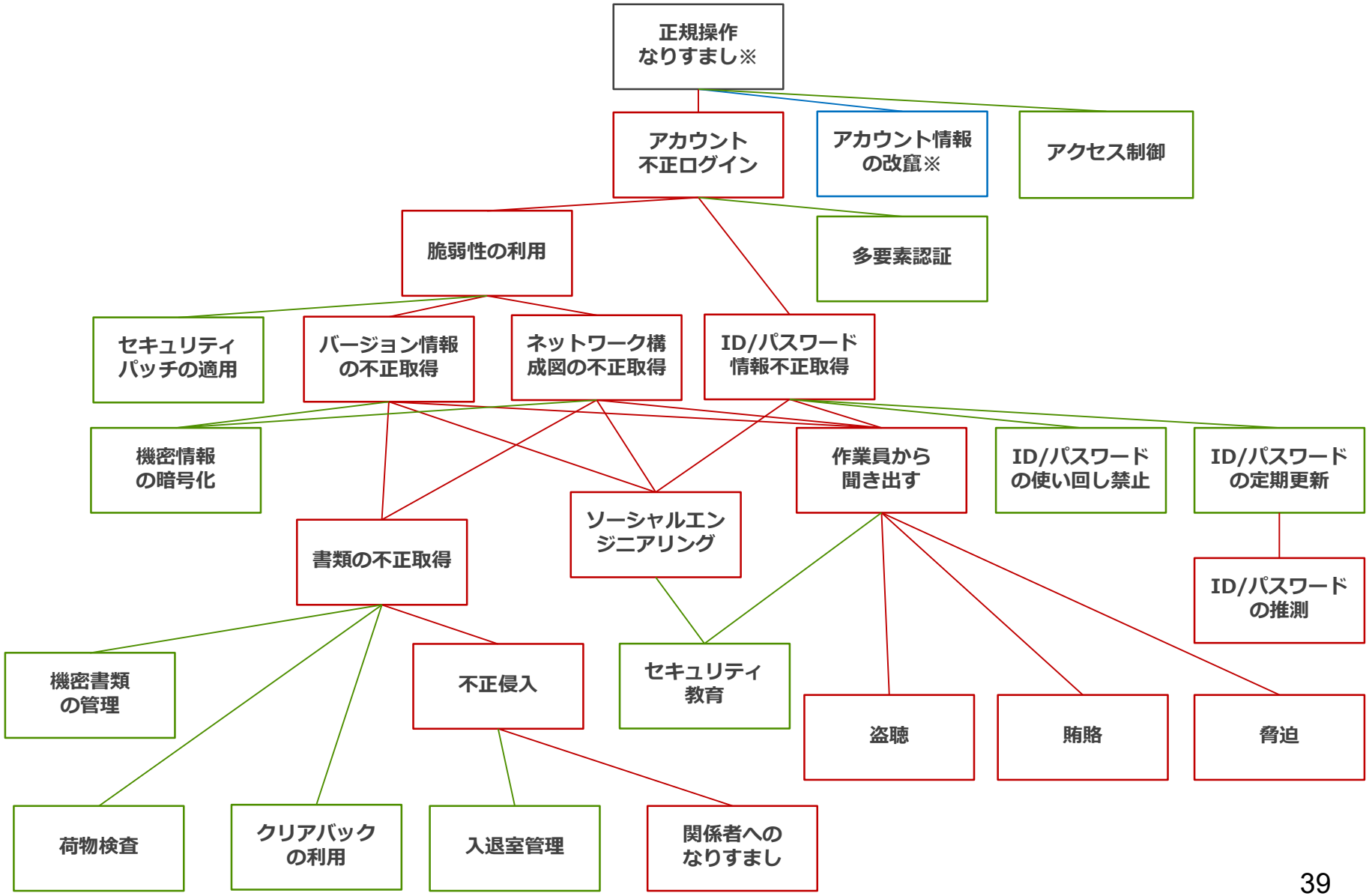


部分木


機器の
不正操作※
不正侵入
管理者権限の
不正取得※
作業員の故意
入退室管理
関係者への
なりすまし
賄賂
脅迫
セキュリティ
教育

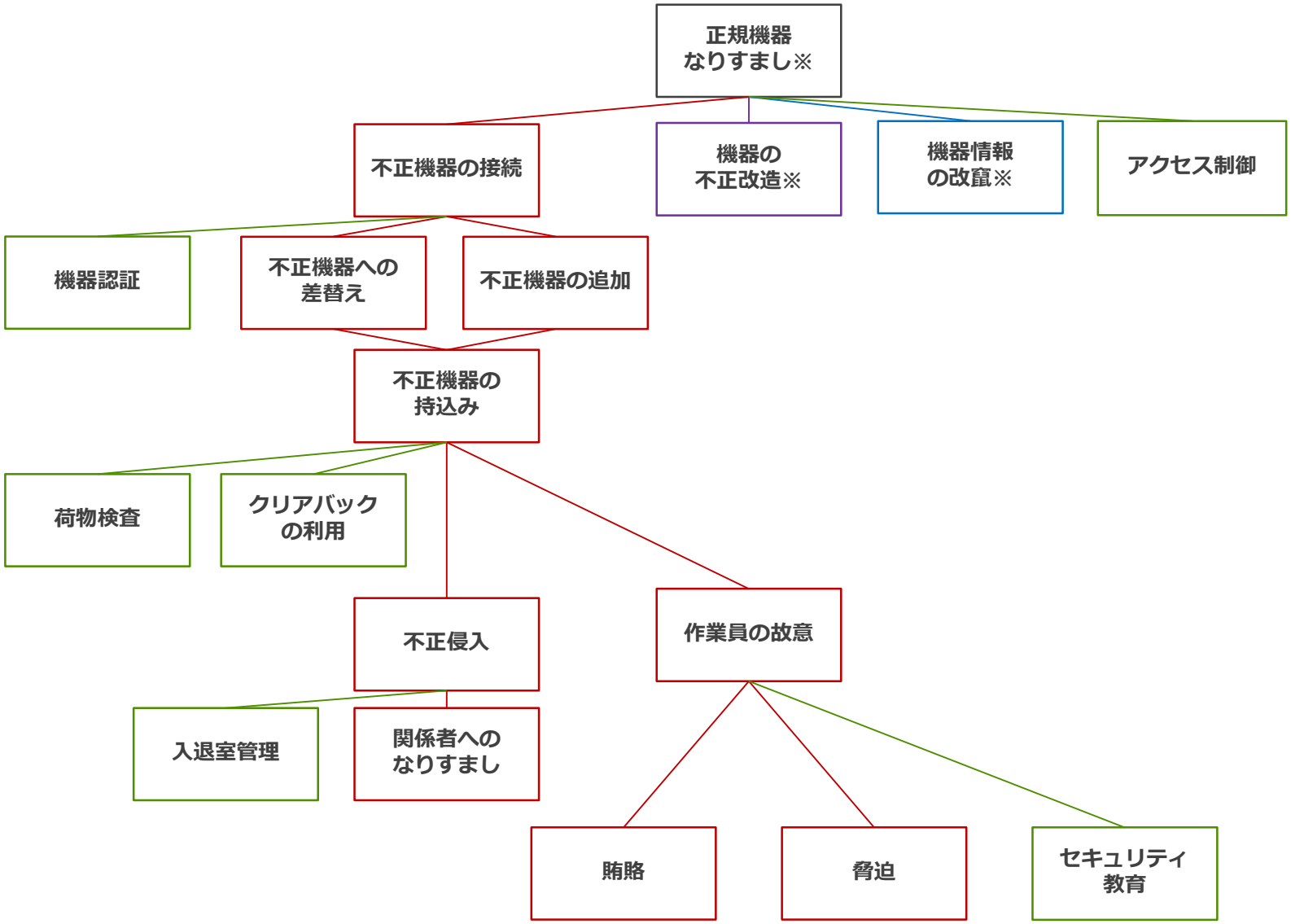
STRIDE-Trees(なりすまし)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



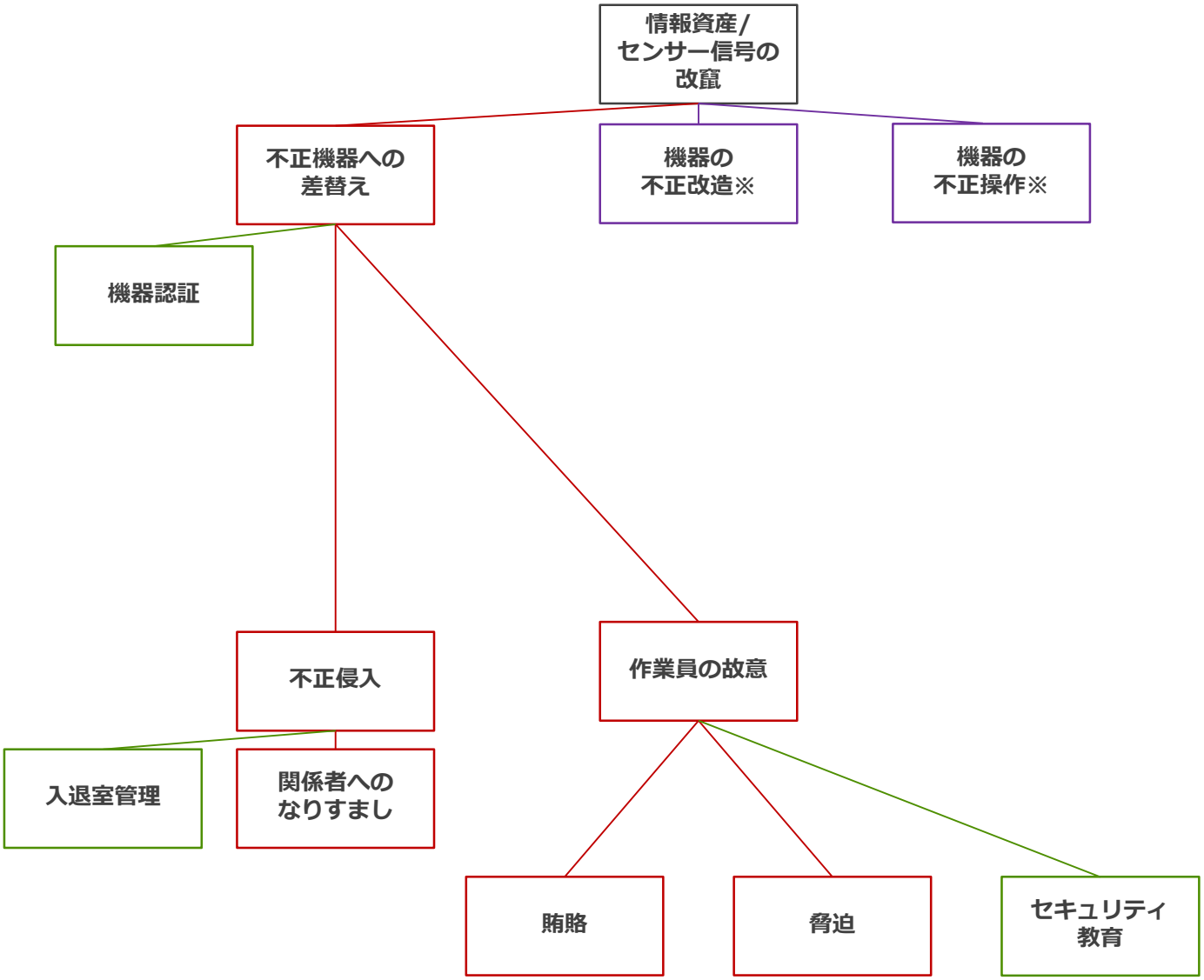
STRIDE-Trees(なりすまし)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



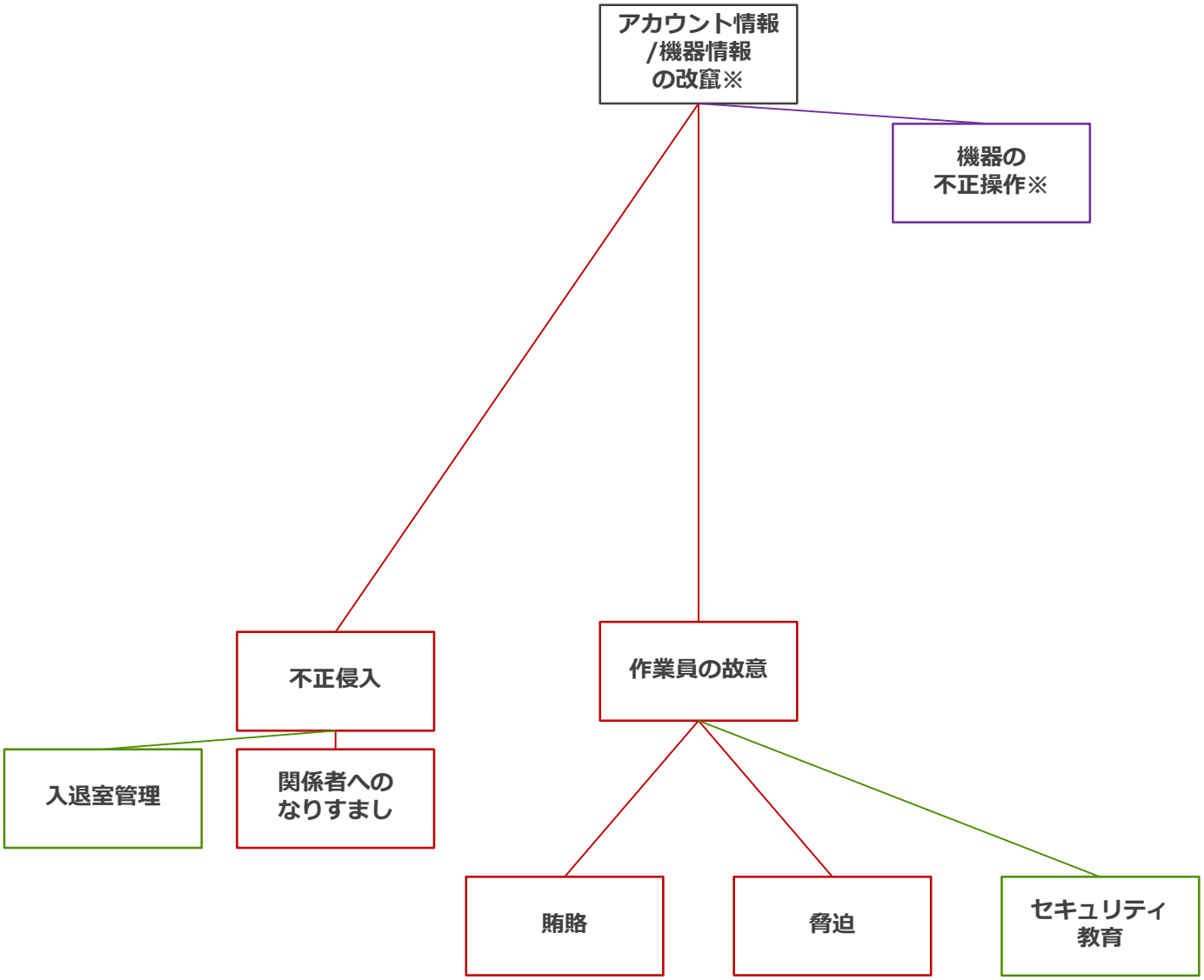
STRIDE-Trees(改竄)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

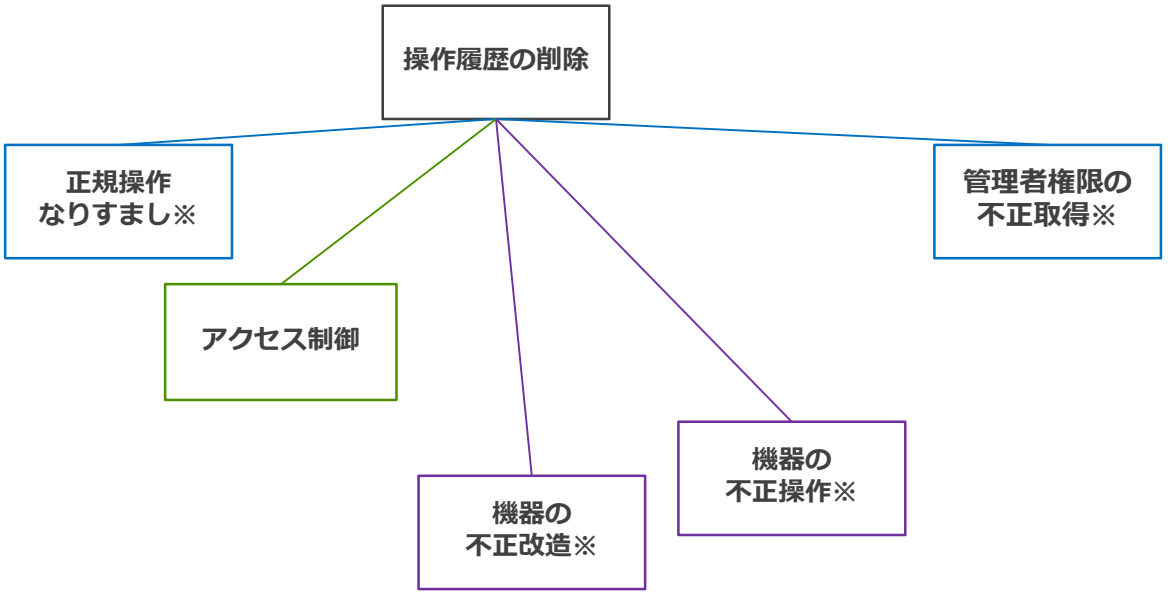


STRIDE-Trees(改竄)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

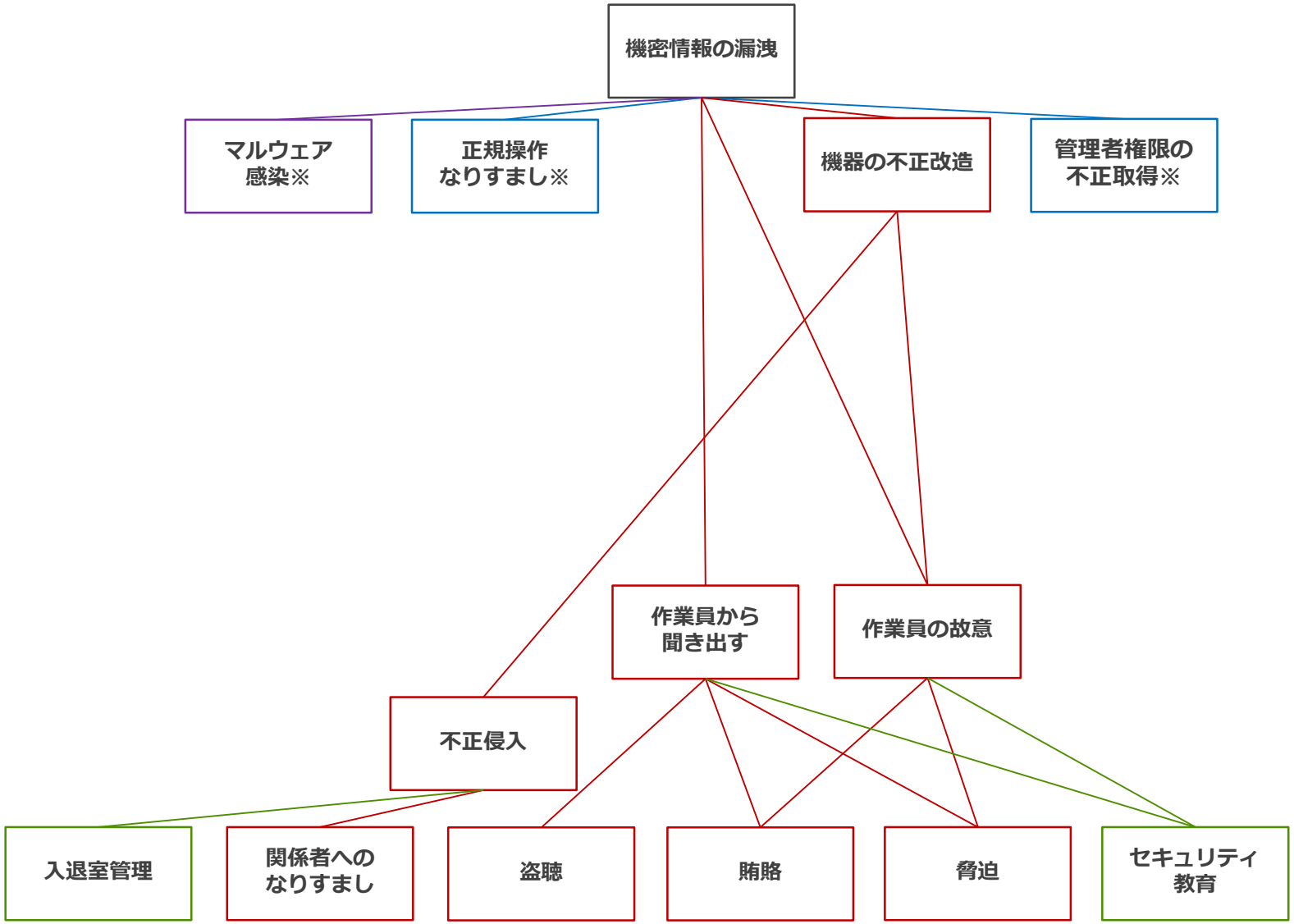


STRIDE-Trees(否認)



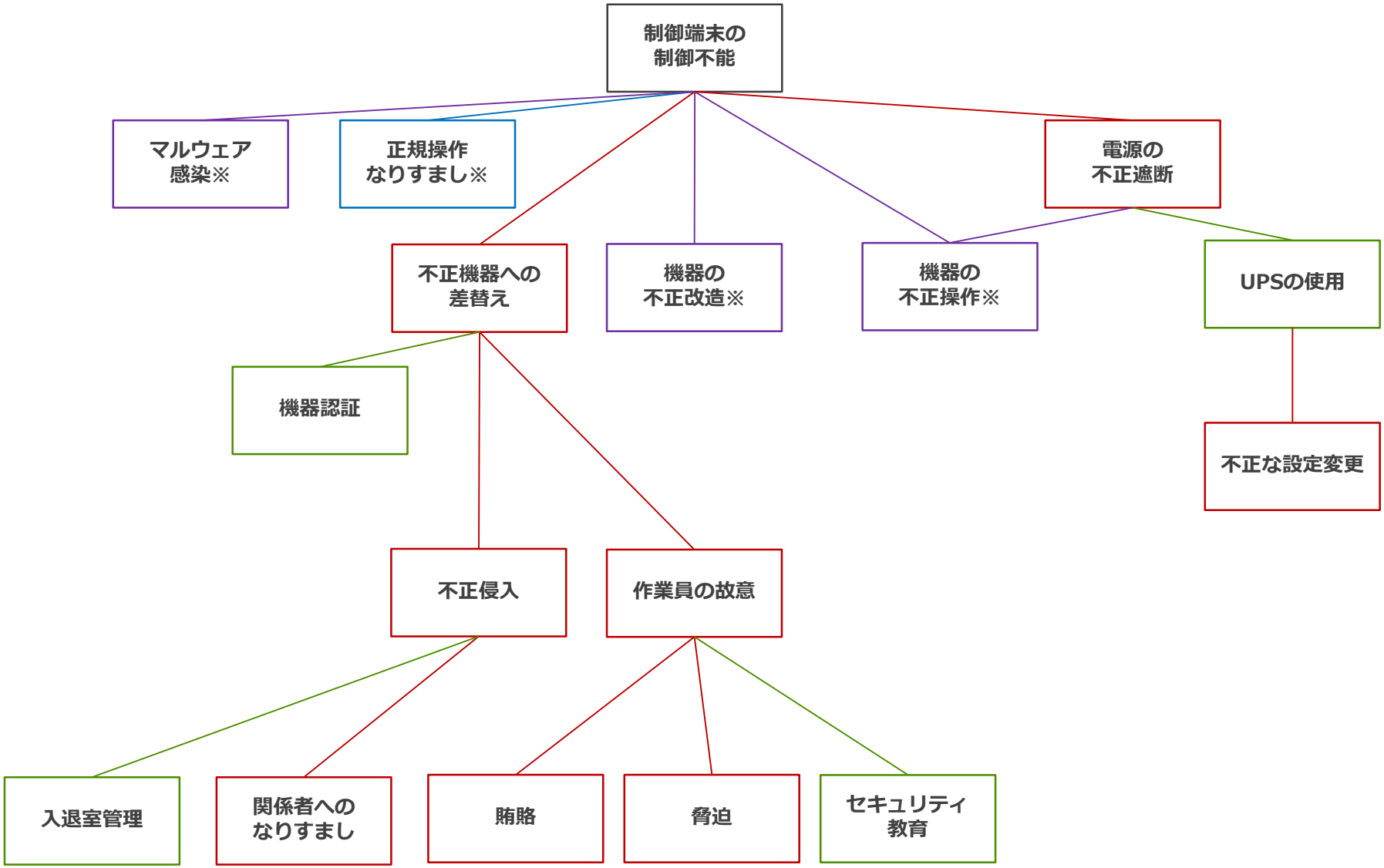
STRIDE-Trees(情報漏洩)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



STRIDE-Trees(サービス妨害)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



セキュリティ対策の導出例

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

	脅威		
	正規操作なりすまし	情報資産の改竄	操作履歴の削除
予防	・パッチの適用 ・アクセス制御 ・多要素認証 ・ID/パスワードの適切な管理	・アクセス制御 ・バックアップ ・権限管理	・セキュリティ教育 ・アクセス制御 ・バックアップ ・権限管理
検知	・異常検知システムの実装	・異常検知システムの実装	・異常検知システムの実装
復旧	・被害範囲の特定	・データの復元	・データの復元

予防・検知の観点から、ツリー構造内において
セキュリティ対策を導出