IoT時代の
リスク評価・リスクコミュニケーション

東京電機大学未来科学部教授
サイバーセキュリティ研究所所長
佐々木良一
sasaki@im.dendai.ac.jp

目次

IoT時代のリスクアセスメントへの要求

＜最近の動向＞

IoTが普及

サイバー攻撃が高度化

セキュリティ対策が高コスト化

＜アセスメントへの要求＞

脅威分析が重要に

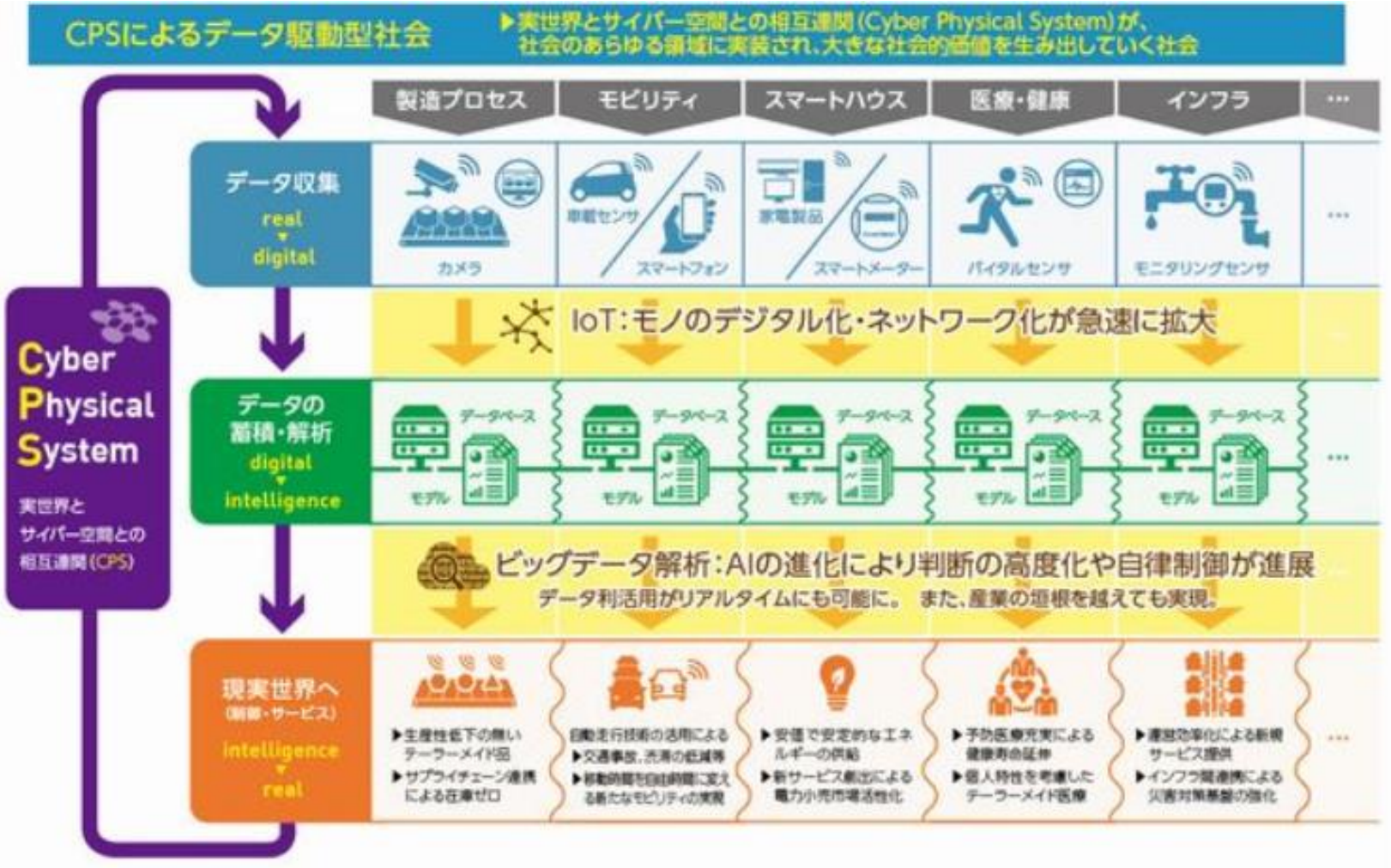
シーケンスの深い攻撃への評価方法が大切に

コスト効果のよい対策案組合せを求めることが必須に

経営者の参画がアセスメントへの参加が不可欠に

目次

CPS/IoT時代の到来



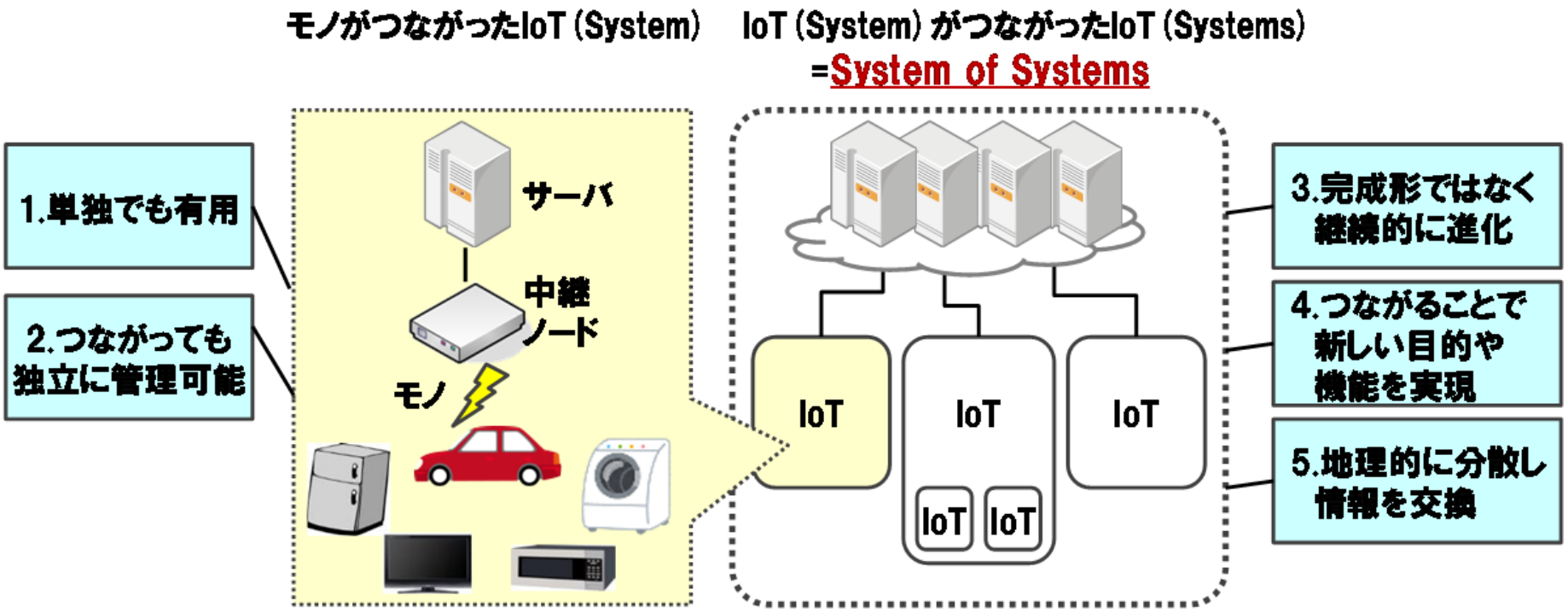
http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/report_001.html

IoT 特有の性質

（性質１）脅威の影響範囲・影響度合いが大きいこと
（性質２）IoT 機器のライフサイクルが長いこと
（性質３）IoT 機器に対する監視が行き届きにくいこと
（性質４）IoT 機器側とネットワーク側の環境や特性の相互理解が不十分であること
（性質５）IoT 機器の機能・性能が限られていること
（性質６）開発者が想定していなかった接続が行われる可能性があること

IoTセキュリティガイドライン　平成28年7月
http://www.soumu.go.jp/main_content/000428393.pdf

SoS 的な特徴を持ったIoT



IoTセキュリティガイドライン　平成28年7月
http://www.soumu.go.jp/main_content/000428393.pdf

5つの指針・21の要点（1）

大項目	指針	要点
方針	指針1 IoT の性質を考慮した基本方針を定める	要点 1. 経営者が IoT セキュリティにコミットする
		要点 2. 内部不正やミスに備える
分析	指針2 IoT のリスクを認識する	要点 3. 守るべきものを特定する
		要点 4. つながることによるリスクを想定する
		要点 5. つながりで波及するリスクを想定する
		要点 6. 物理的なリスクを認識する
		要点 7. 過去の事例に学ぶ
設計	指針3 守るべきものを守る設計を考える	要点 8. 個々でも全体でも守れる設計をする
		要点 9. つながる相手に迷惑をかけない設計をする
		要点 10. 安全安心を実現する設計の整合性をとる
		要点 11. 不特定の相手とつなげられても安全安心を確保できる設計をする
		要点 12. 安全安心を実現する設計の検証・評価を行う

IoTセキュリティガイドライン　平成28年7月
http://www.soumu.go.jp/main_content/000428393.pdf

5つの指針・21の要点（2）

構築・接続	指針4 ネットワーク上での対策を考える	要点 13. 機器等がどのような状態かを把握し、記録する機能を設ける
		要点 14. 機能及び用途に応じて適切にネットワーク接続する
		要点 15. 初期設定に留意する
		要点 16. 認証機能を導入する
運用・保守	指針5 安全安心な状態を維持し、情報発信・共有を行う	要点 17. 出荷・リリース後も安全安心な状態を維持する
		要点 18. 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える
		要点 19. つながることによるリスクを一般利用者に知ってもらう
		要点 20. IoT システム・サービスにおける関係者の役割を認識する
		要点 21. 脆弱な機器を把握し、適切に注意喚起を行う

IoTセキュリティガイドライン　平成28年7月
http://www.soumu.go.jp/main_content/000428393.pdf

IoTの安全

故意

過失

故障

①機密性喪失の重要性は低い

ソフト（制御用ソフト）
＜セキュリティ＞

②出力異常指示③停止指示

ハード（制御用ハード）
＜ディペンダビリティ＞

②
③

制御対象（IoT）
＜セーフティ：
機能安全＞

機能喪失
安全・環境
への影響

簡単に異常停止
になる可能性

脅威分析が
重要に

セーフティ機能

セキュリティ攻撃

①機密性の喪失（情報の漏えいなど）
②完全性の喪失（影響：爆発など）
③可用性の喪失（システムダウンなど）

IoTの安全における特徴

1．機密性よりも、完全性・可用性が重要に

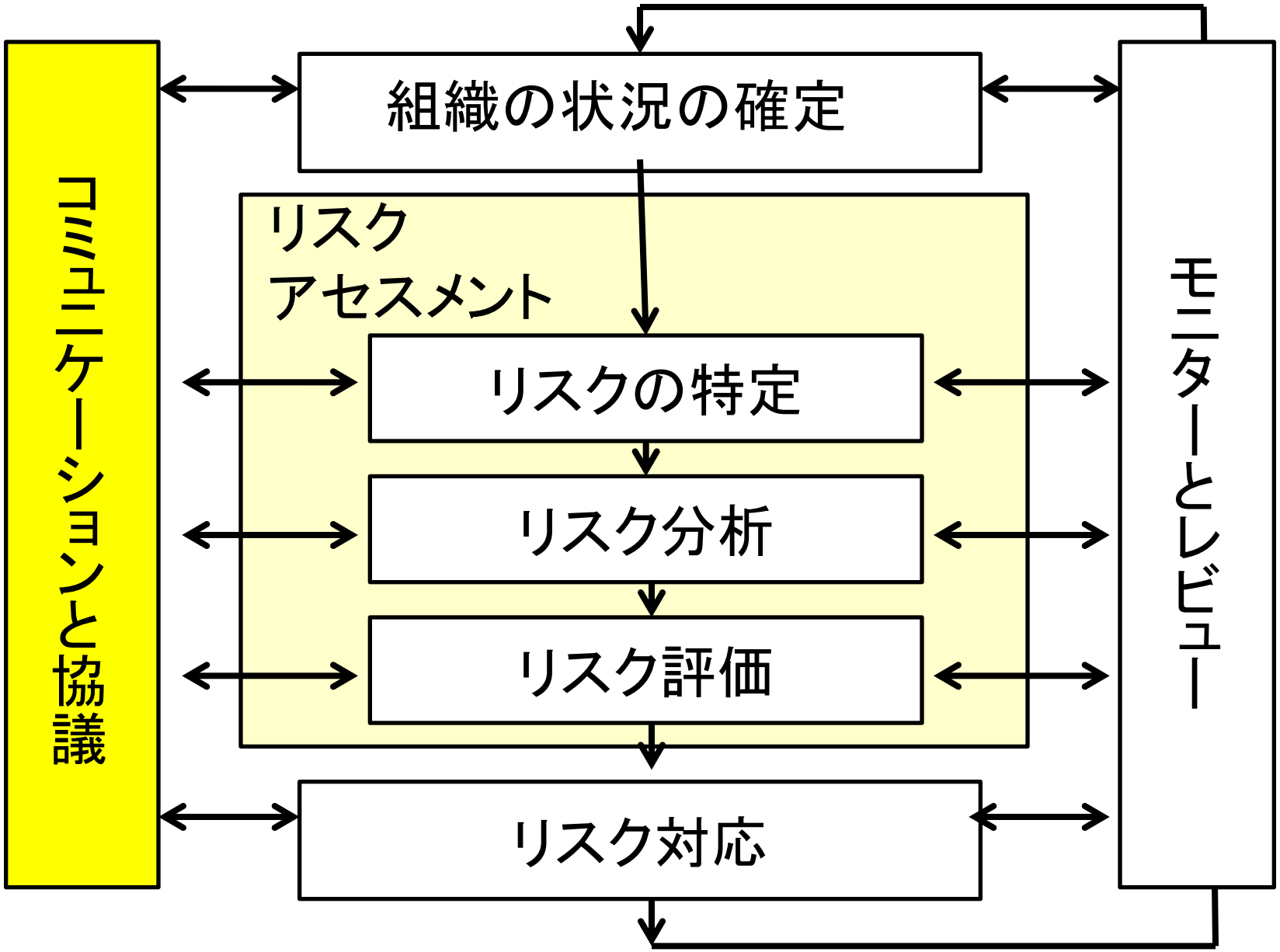
2．制御対象の機能喪失や安全・環境への影響の考慮が不可欠

3．IoTシステムにおいては安全性の配慮がシステムダウンにつながりやすい

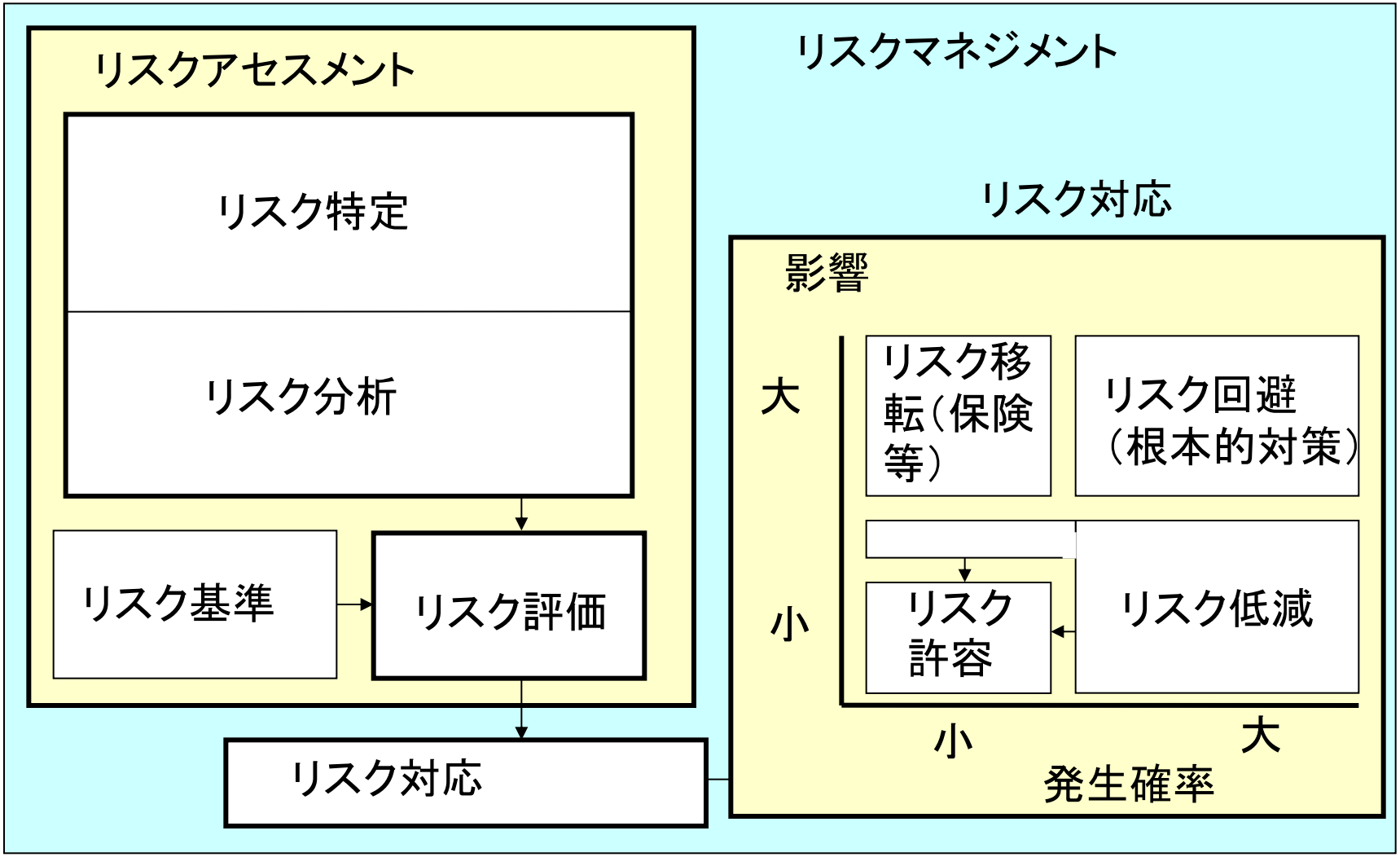
4．関与者が多くなる（制御ソフト開発者・制御エンジニア・運用者など）ので、リスクコミュニケーションが重要に

目次

リスクマネジメントのプロセスの流れ



リスク分析・リスク評価とリスク対応



分析アプローチ

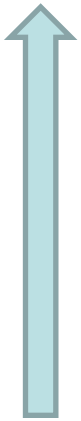
＜従来＞
(i) 脅威を重視したアプローチ
(ii)資産を重視したアプローチ
(iii) 脆弱性を重視したアプローチ

＜今後＞
リスクを重視したアプローチ
リスク＝資産X脆弱性X脅威

アセスメントアプローチ

アプローチ法	長所	欠点
定量的	費用対効果分析を最も効果的に支援	得られた数値または結果に関する信頼性の説明が必要
半定量的	比較的少ないコストで相互比較が可能に	厳密性が不足
定性的	分析にコストがかからない	経験により結果が異なる場合もある

今後の方向



FIPS SP 800-30を参考に作成

ITシステムの安全の階層化

階層	対象	扱う事故・障害	従来の学問・技術分野	指標
3	ITシステムが行うサービスの安全	発券サービスの停止、プライバシーの喪失など	システム工学 リスク学 社会科学など	プライバシー、ユーザビリティ
2	ITシステムが扱う情報の安全	情報のCIAの喪失	セキュリティ	セキュリティ（機密性、完全性、可用性）
1	ITシステムそのものの安全	コンピュータや通信機器の故障	信頼性工学 セキュリティ	リライアビリティ、アベイラビリティ

＊

＊　従来情報セキュリティが扱っていた範囲

IoT時代のリスクアセスメントへの要求

＜最近の動向＞

IoTが普及

サイバー攻撃が高度化

セキュリティ対策が高コスト化

＜アセスメントへの要求＞

脅威分析が重要に

シーケンスの深い攻撃への評価方法が大切に

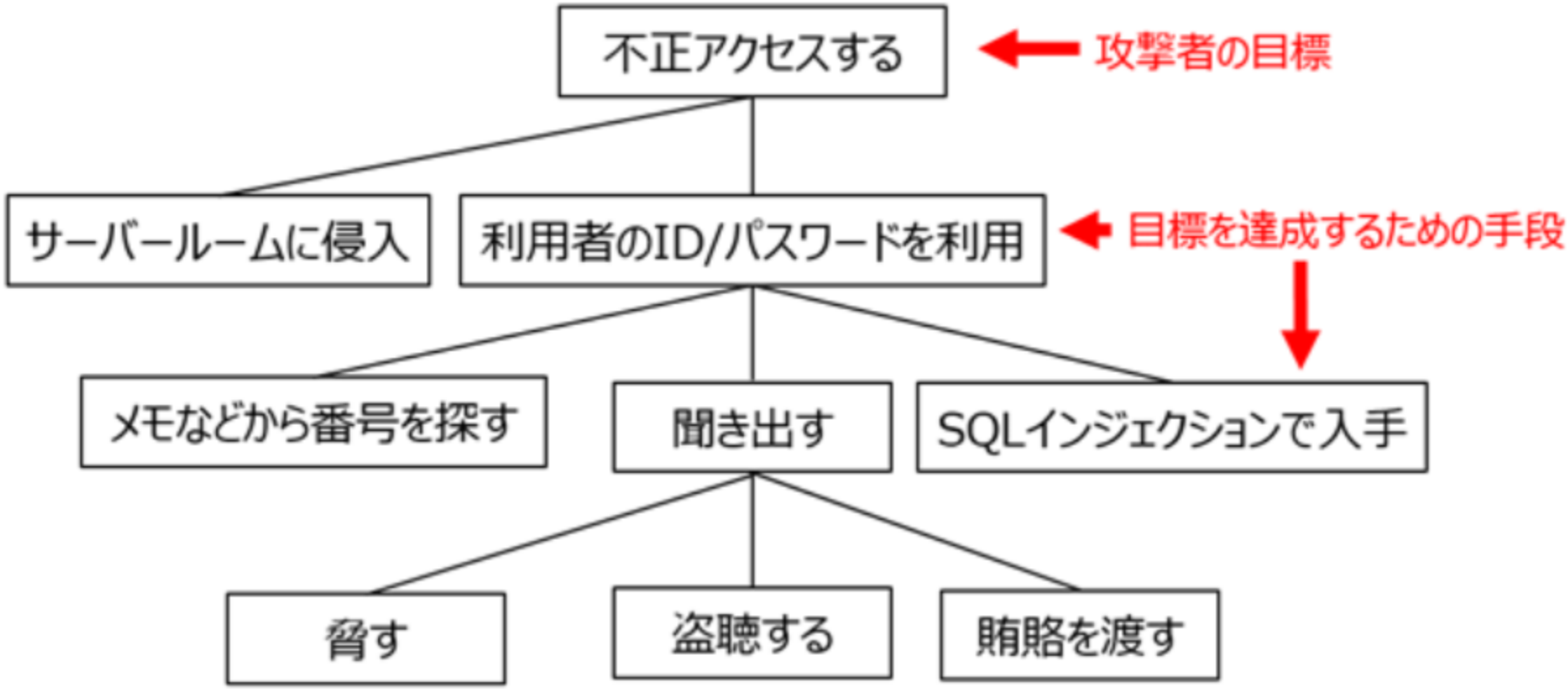
コスト効果のよい対策案組合せを求めることが必須に

経営者の参画がアセスメントへの参加が不可欠に

脅威分析の方法

フェーズ ＼ 脅威	脅威が比較的小さい	脅威が比較的大きい
対象システムの計画の初期段階	人 X 資産X　RWX法	シナリオ記述法（総務省スマートハウス）
対象システムの設計が進んだ段階	STRAIDE法	アタックツリー法 EDC法（東京電機大学）他
セキュリティ対策追加段階（運用開始後）	情報資産分析法	日立[IPSJ57]

アタックツリーの一例



http://www.ffri.jp/blog/2016/10/2016-10-14.htm

アタックライブラリー

Attack Libraryとは脅威情報について纏めたものであり、MITREのCAPECのような脅威情報のデータベースです。

図3 CAPECの内容

Mitigation

脅威の識別 → リスク評価 → 対策の実施

それぞれの脅威について、個別のセキュリティ対策を実施する

STRIDEに対応した標準的なセキュリティ対策が指針として用意されている

Sample Mitigation

- Mitigation #54, Rasterization Service performs the following mitigation strategies:
  1. OM is validated and checked by (component) before being handed over to Rasterization Service
  2. The resources are decoded and validated by interacting subsystems, such as [foo], [bar], and [boop]
  3. Rasterization ensures that if there are any resource problems while loading and converting OM to raster data, it returns a proper error code
  4. Rasterization Service will be thoroughly fuzz tested

(Comment: Fuzzing isn't a mitigation, but it's a great thing to plan as part 4)

Standard Mitigations

Spoofing	Authentication	To authenticate principals: • Cookie authentication • Kerberos authentication • PKI systems such as SSL/TLS and certificates To authenticate code or data: • Digital signatures
Tampering	Integrity	• Windows Vista Mandatory Integrity Controls • ACLs • Digital signatures
Repudiation	Non Repudiation	• Secure logging and auditing • Digital Signatures
Information Disclosure	Confidentiality	• Encryption • ACLs
Denial of Service	Availability	• ACLs • Filtering • Quotas
Elevation of Privilege	Authorization	• ACLs • Group or role membership • Privilege ownership • Input validation

脅威分析の方法

フェーズ ＼ 脅威	脅威が比較的小さい	脅威が比較的大きい
対象システムの計画の初期段階	人 X 資産X　RWX法	シナリオ記述法（総務省スマートハウス）
対象システムの設計が進んだ段階	STRAIDE法	アタックツリー法 EDC法（東京電機大学）他
セキュリティ対策追加段階（運用開始後）	情報資産分析法	日立[IPSJ57]

シナリオの一例

＜スマートハウス：セキュリティ攻撃なし＞
外出しようとした家族Aが屋外側から玄関ドア（ネット対応）を施錠しようとしたが、一瞬早くインターネット経由で家族Bが施錠行為をしたため、家族Aの認識と実際の施錠状態がずれ、家族Aの操作によって解錠してしまい、そのまま外出した。

＜スマートハウス：セキュリティ攻撃あり＞
玄関ドア（ネット対応）において、家族Bが施錠行為をするためのスマホへのパスワードの入力を見られたため、不正者が不正に玄関をスマホ・インターネット経由で開け侵入してしまった。

IoT時代のリスクアセスメントへの要求

＜最近の動向＞

IoTが普及

サイバー攻撃が高度化

セキュリティ対策が高コスト化

＜アセスメントへの要求＞

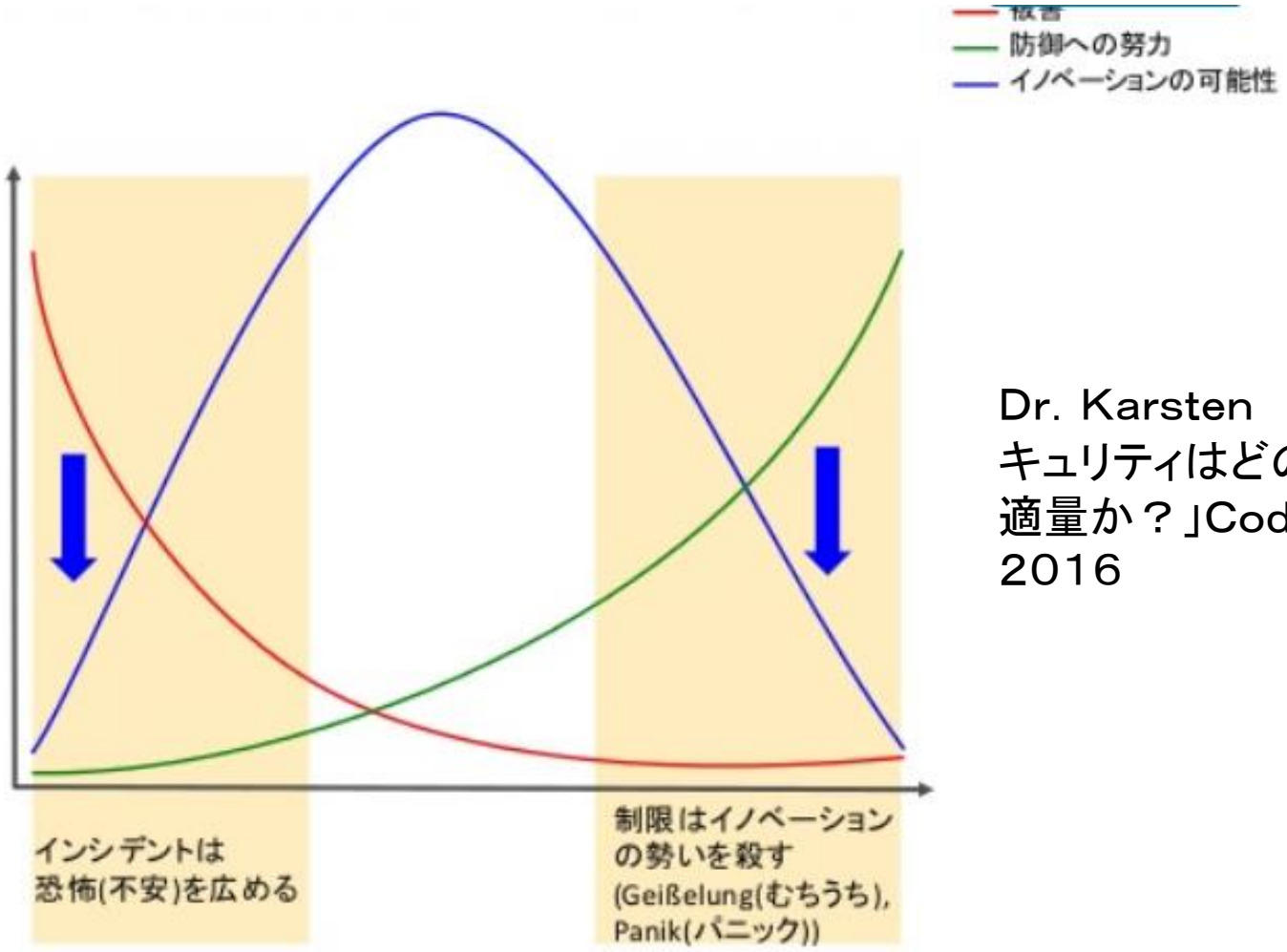
脅威分析が重要に

シーケンスの深い攻撃への評価方法が大切に

コスト効果のよい対策案組合せを求めることが必須に

経営者の参画がアセスメントへの参加が不可欠に

最適なリスク対策額



Dr. Karsten Nohl「セキュリティはどのぐらいが適量か？」CodeBlue 2016

http://www.slideshare.net/codeblue_jp/cb16-nohl-ja

代替となる制限の少ない防御

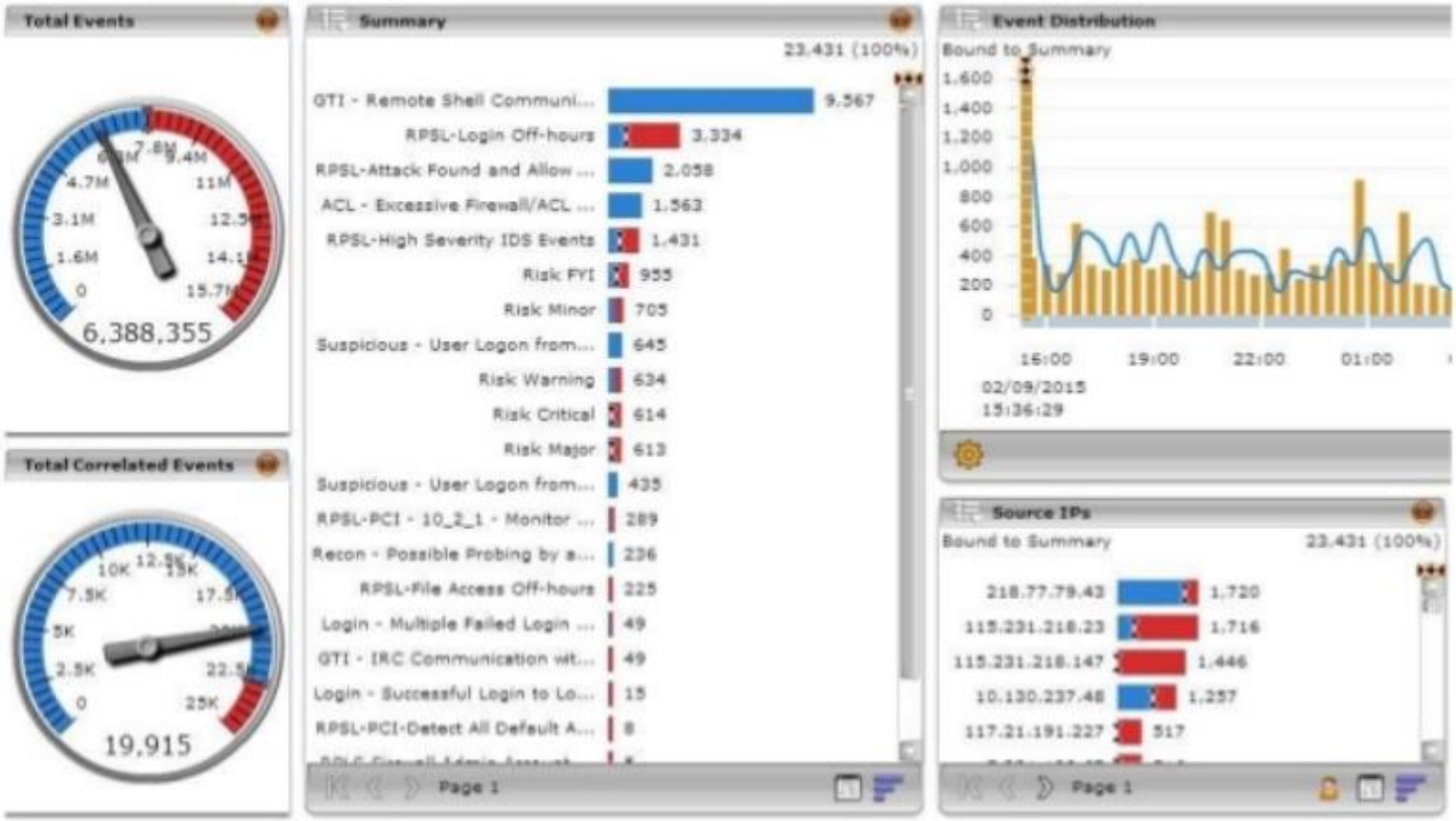
行動を制限する防御	イノベーションに親切な代替
▪ 多くの複雑なパスワード	▪ スマートフォンでのシングルサインオン
▪ Webプロキシのブロックリスト	▪ SSL ターミネーション と モニタリング
▪ ユーザーへ管理者権限を与えない	▪ プロセスモニタリング
▪ 法人携帯 (Blackberrys)	▪ ActiveSyncを使ったBYODとVPN (もしくは可能であればAndroidは使わない)
▪ 終わらないペネトレーションテスト	▪ バグ報奨金プログラム
▪ セキュリティポリシー	▪ 啓発活動
▪ DLP	▪ 検知もしくは単純により多くの信頼を得る

制限の代替が存在しない場合、綿密な**リスクの監視**によってリスクが顕在化するまでは制限を切ることが可能

Dr. Karsten Nohl「セキュリティはどのぐらいが適量か？」CodeBlue 2016

http://www.slideshare.net/codeblue_jp/cb16-nohl-ja

セキュリティモニタリングの必要性



Dr. Karsten Nohl「セキュリティはどのぐらいが適量か？」CodeBlue 2016

http://www.slideshare.net/codeblue_jp/cb16-nohl-ja

Dr. Karsten Nohl講演の結言

1. 私たちはハッカーの動機を忘れ、**リスクではなく、脆弱性**を追っている
2. 最大の**リスク-コストのトレードオフ**は制限と**イノベーション**の可能性の間にある
3. 多くの場合、制限的な選択に代わって**イノベーションに親切な代替**が存在する
4. **リスク**は**監視**し、管理しなければならない：“全てから守る”はイノベーションを殺す，それによって 守る対象そのものを殺してしまう

Dr. Karsten Nohl「セキュリティはどのぐらいが適量か？」CodeBlue 2016
http://www.slideshare.net/codeblue_jp/cb16-nohl-ja

目次

1. はじめに
2. IoTの特徴
3. リスクアセスメントの動向
4. 東京電機大学におけるアプローチ
5. 最近の注目すべき動向

IoT時代のリスクアセスメントへの要求

＜最近の動向＞

IoTが普及

サイバー攻撃が高度化

セキュリティ対策が高コスト化

＜アセスメントへの要求＞

脅威分析が重要に

シーケンスの深い攻撃への評価方法が大切に

コスト効果のよい対策案組合せを求めることが必須に

経営者の参画がアセスメントへの参加が不可欠に

多重リスクコミュニケータ（MRC）の対応

＜背景＞

背景1．多くのリスク（セキュリティリスク、プライバシーリスクなど）が存在＝＞リスク間の対立を回避する手段が必要

背景2．ひとつの対策だけでは目的の達成が困難＝＞対策の最適な組み合わせを求めるシステムが必要

背景3．多くの関与者（経営者・顧客・従業員など）が存在＝＞多くの関与者間の合意が得られるコミュニケーション手段が必要

MRCにおける対応

①多くのリスクやコストを制約条件とする組み合わせ最適化問題として定式化

②関与者の合意が得られるまでパラメータの値や制約条件値を変えつつ最適化エンジンを用い求解

専門家

対策案
①②③④

定式化結果

多重リスクコミュニケータMRC

最適解
対策案
①③の組合せ

満足

Y

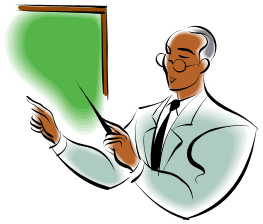
END

N

制約条件などの変更

ファシリテータ　関与者

MRCに関する最近の研究



1．Social-MRCについては、対象とSocial-MRCの仕組みの両方を多くの人に限られた時間で理解してもらうのは難しいので研究中断中。

2．MRCについて機能の拡張中

（1）標的型攻撃等シーケンスの深い攻撃のリスク評価のために、イベントツリーとディフェンスツリーを組みわせて用いるリスク解析法（EDC：Event Tree and Defense Tree Combined Method ）の確立

（2）被害発生防止対策と復元対策の両方を考慮した対策案最適組合せ法

（3）動的リスクを考慮した多重リスクコミュニケータ

（4）経営者とのリスクコミュニケーションも考慮した多重リスクコミュニケータ

IoT時代のリスクアセスメントへの要求

＜最近の動向＞

- IoTが普及
- サイバー攻撃が高度化
- セキュリティ対策が高コスト化

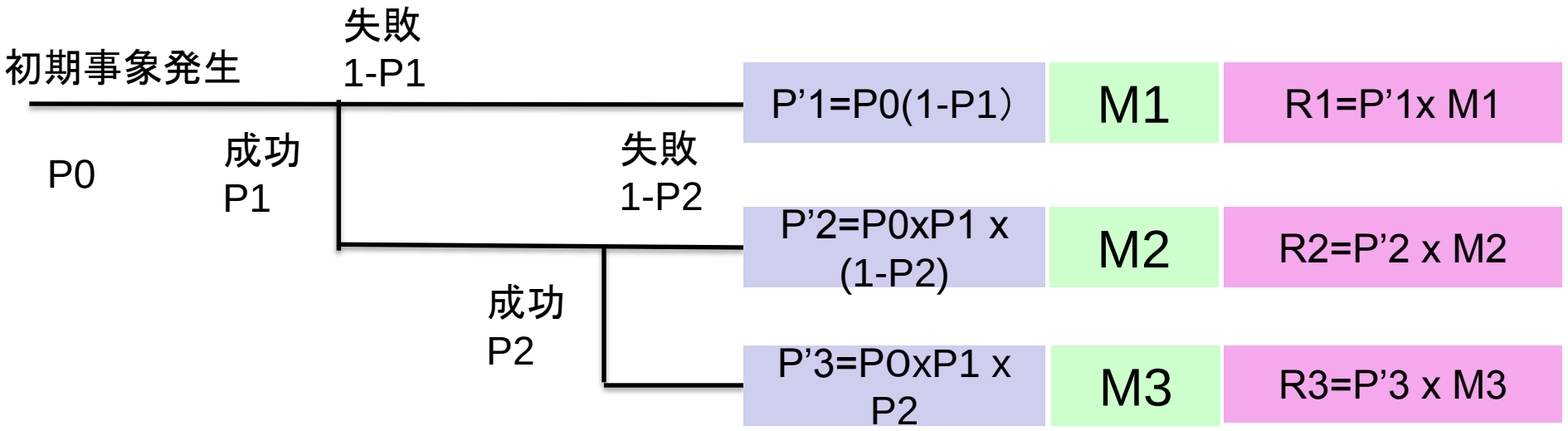
＜アセスメントへの要求＞

- 脅威分析が重要に
- シーケンスの深い攻撃への評価方法が大切に
- コスト効果のよい対策案組合せを求めることが必須に
- 経営者の参画がアセスメントへの参加が不可欠に

イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

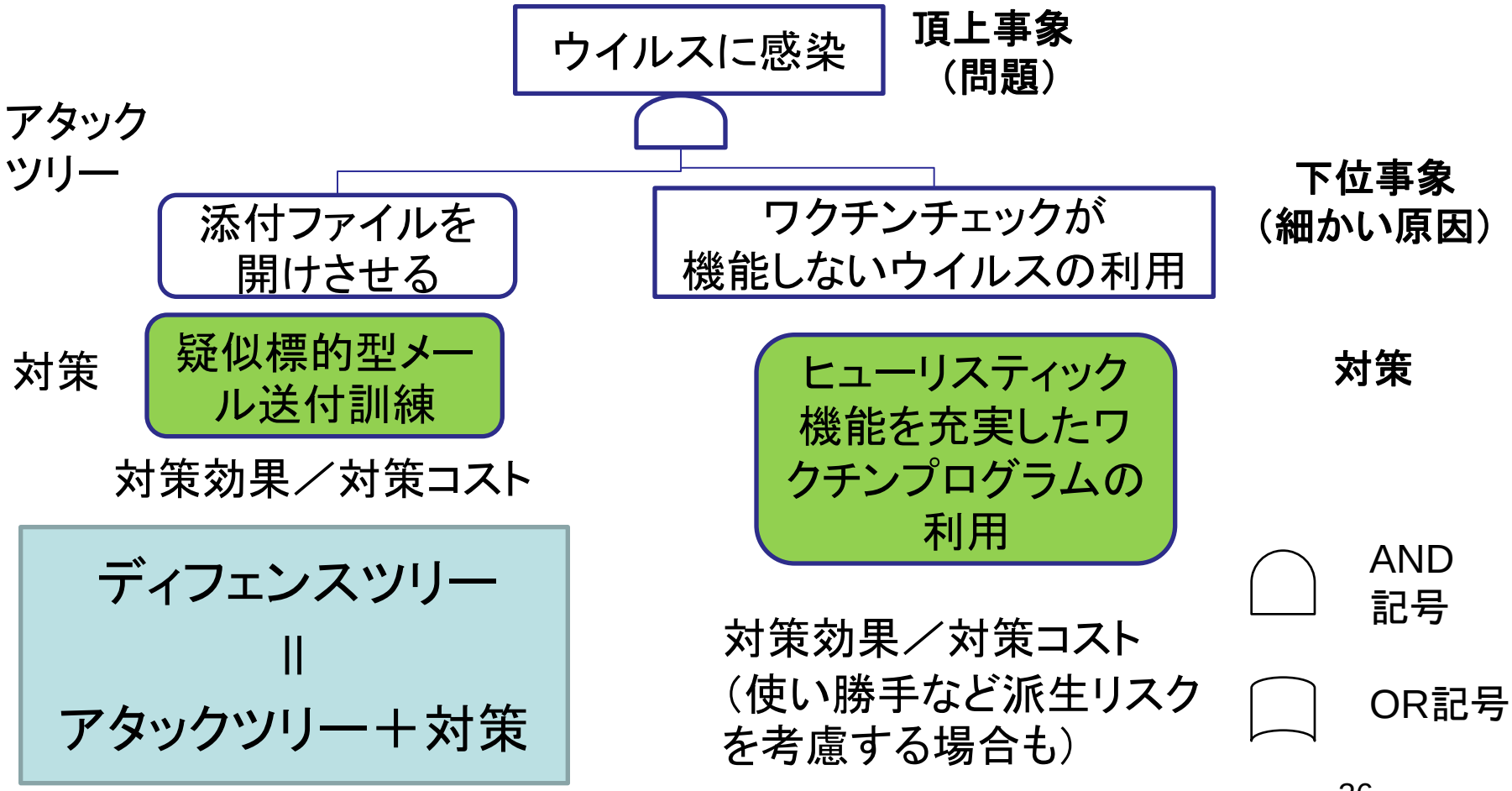
ウイルスに感染	情報の流出	発生確率	損害	リスク（発生確率x損害）



RT=R1+R2+R3

ディフェンスツリー分析

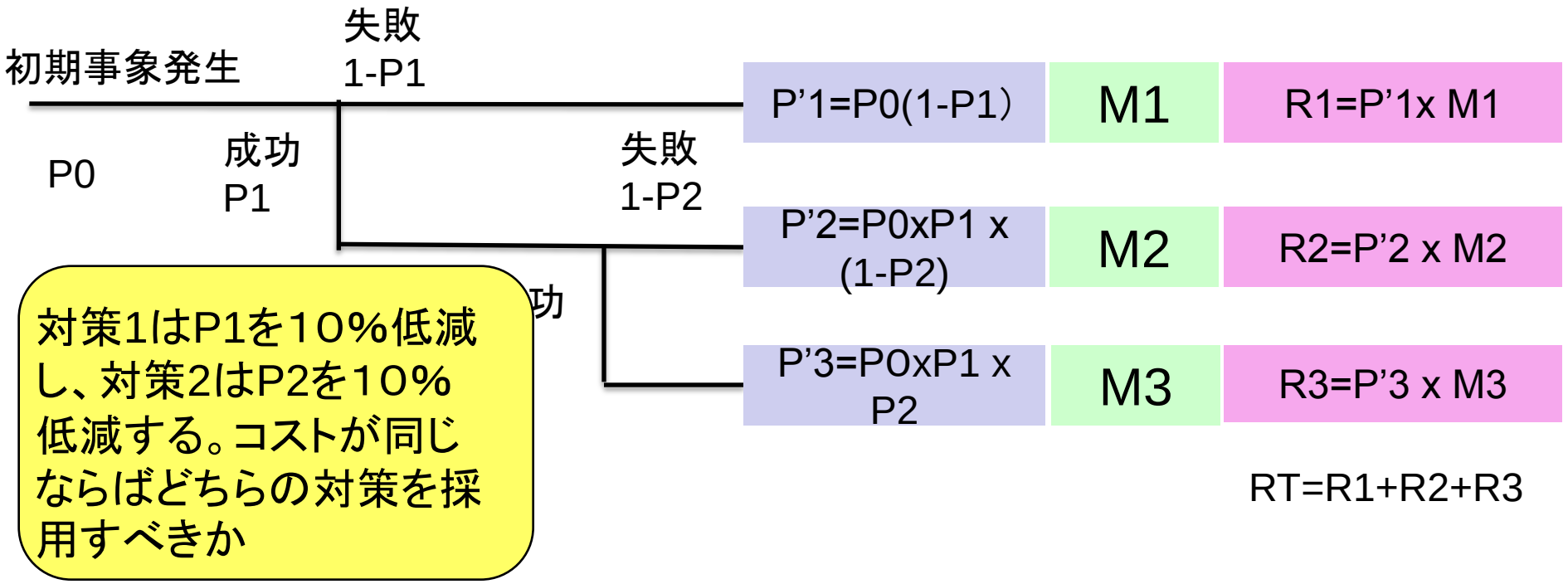
- 攻撃に対しトップダウンにその要因を分析する
  アタックツリー分析に対策を加えたもの



イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

ウイルスに感染	情報の流出	発生確率	損害	リスク（発生確率x損害）



イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

ウイルスに感染	情報の流出	発生確率	損害	リスク（発生確率x損害）
初期事象発生	失敗 1-P1	0.8	0円	0円
P0 1.0	成功 P1			
	0.2			
	失敗 1-P2	0.16	500万円	80万円
	成功 P2			
	0.2	0.04	1億円	400万円

トータルリスク= 480万円

対策1はP1を10%低減し、対策2はP2を10%低減する。コストが同じならばどちらの対策を採用すべきか

イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

ウイルスに感染	情報の流出	発生確率	損害	リスク（発生確率x損害）
初期事象発生	失敗 1-P1	0.856	0円	0円
P0 1.0	成功 P1			
	0.2X0.9	失敗 1-P2	0.144	500万円	72万円
		成功 P2	0.036	1億円	360万円
		0.2			

対策1を実施した場合（対策1はP1を10%低減）

トータルリスク= 432万円

イベントツリー分析

- 事象の発生から時系列順にどのような事象に発展するかを分析

ウイルスに感染	情報の流出	発生確率	損害	リスク（発生確率x損害）
初期事象発生	失敗 1-P1	0.8	0円	0円
P0 1.0	成功 P1			
	0.2	失敗 1-P2	0.164	500万円	82万円
		成功 P2	0.036	1億円	360万円
		0.2X0.9			

対策2を実施した場合（対策2はP2を10%低減）

トータルリスク= 442万円

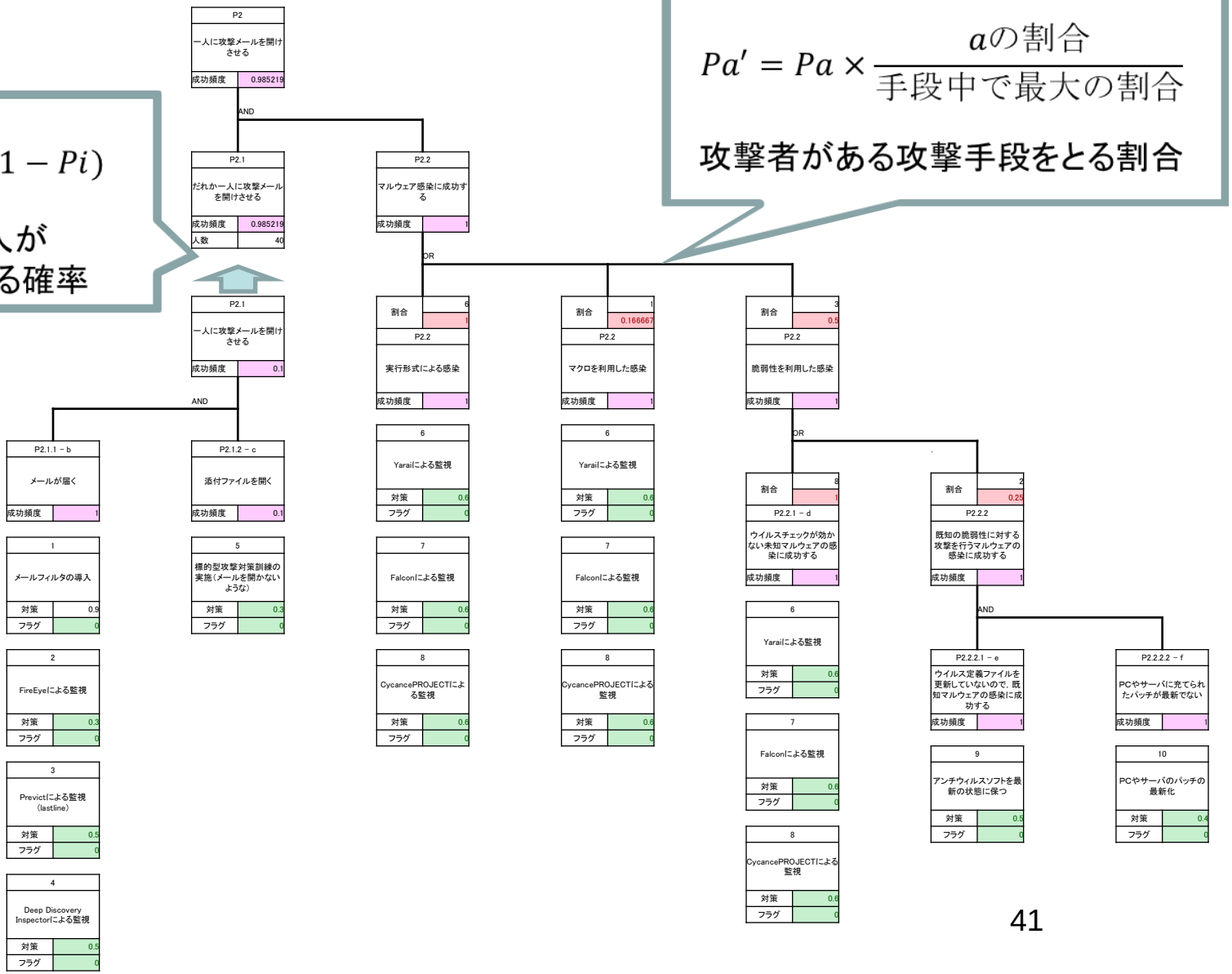
ディフェンスツリー（P2）

$$Pt = 1 - \prod_{i=1}^{n}(1 - Pi)$$

だれか一人が
メールを開ける確率

$$Pa' = Pa \times \frac{a\text{の割合}}{\text{手段中で最大の割合}}$$

攻撃者がある攻撃手段をとる割合



対策の最適な組み合わせ

標的型攻撃に対してはいろいろな対策が考えられる

標的型攻撃向きのリスク評価手法が必要に

どういう対策の組み合わせがよいのかを求める
手法が必要に

多重リスクコミュニケータMRCの開発

対策選定

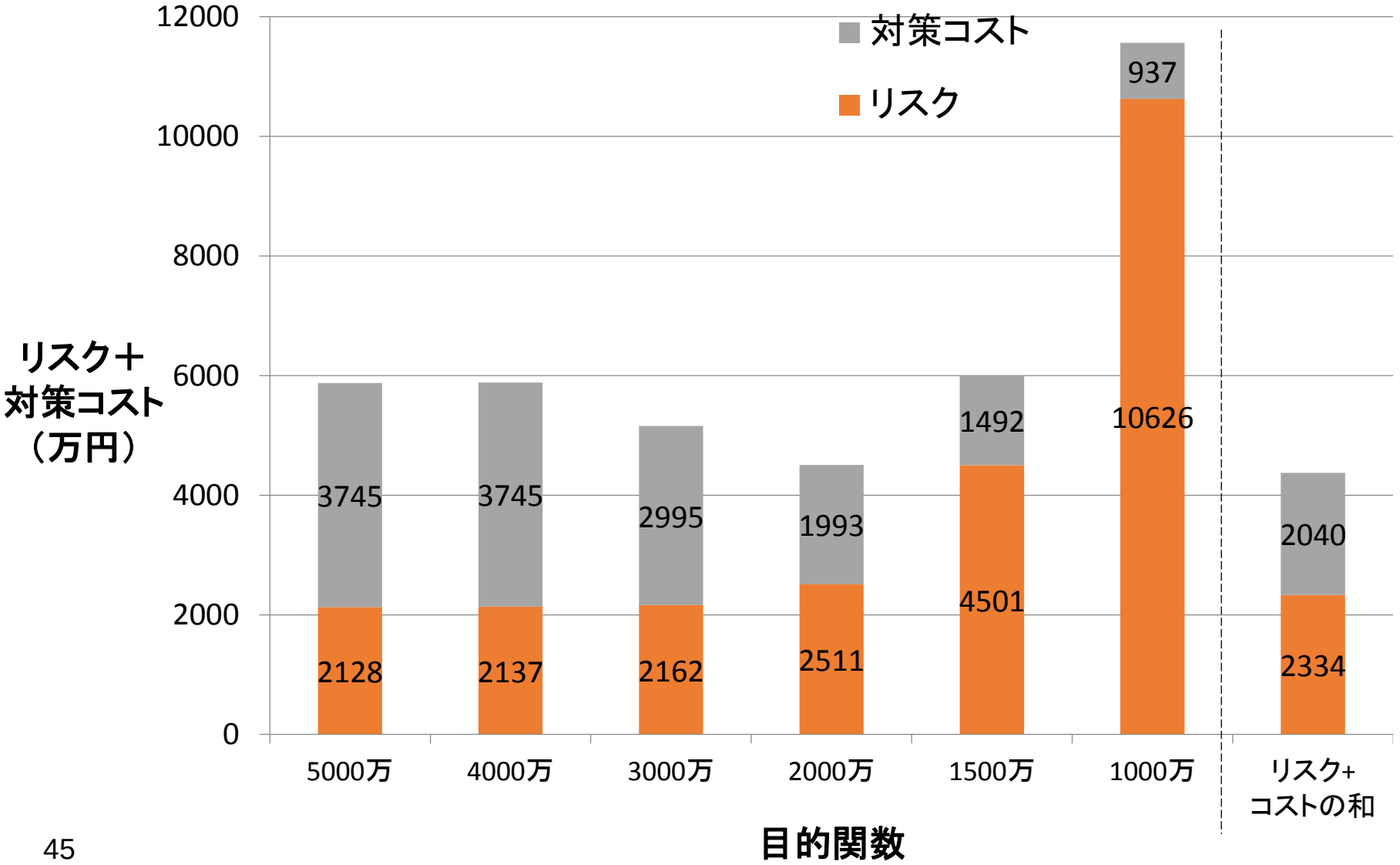
- ソルバー
  - Excelアドイン　ソルバーによる分析
  - 対策を取る(1)取らない(0)の離散最適化問題を解く

- コストパフォーマンス
  - ある対策を一つだけ実施したときのコストパフォーマンスを計算
  - コストパフォーマンス順に対策を選定する

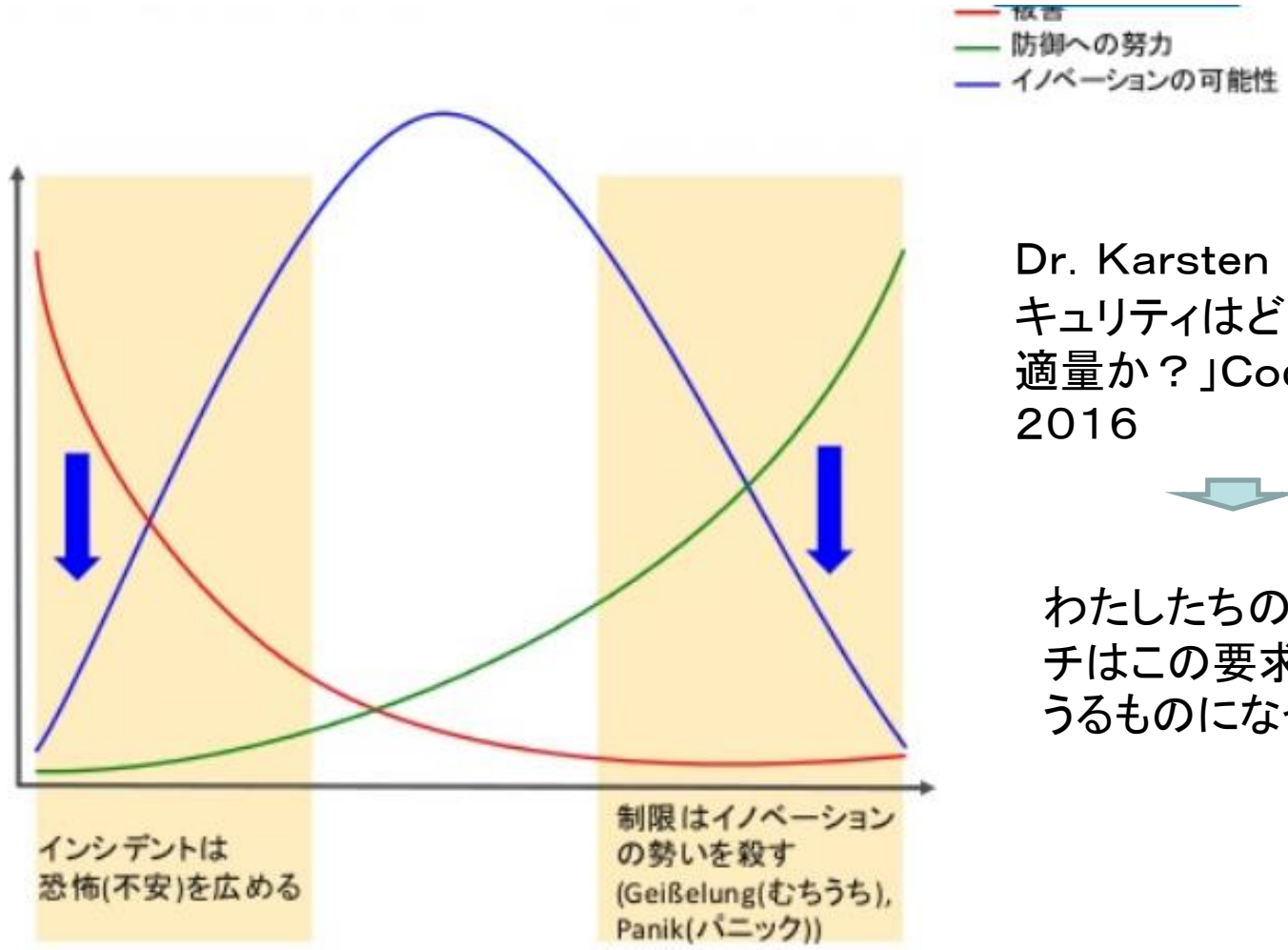
ソルバー

- 目的関数と制約条件を決め，目的関数が最大・最小となる対策の組み合わせを求める
  - 目的関数
    - 予算を設定し，予算内で総合リスク値が最小
      - 5,000万円
      - 4,000万円
      - 3,000万円
      - 2,000万円
      - 1,000万円
    - 総合リスク値と対策費用の和が最小

ソルバーによる解決


対策コスト
リスク
リスク＋
対策コスト
（万円）
12000
10000
8000
6000
4000
2000
0
3745
3745
2995
1993
1492
10626
937
2040
2128
2137
2162
2511
4501
2334
5000万
4000万
3000万
2000万
1500万
1000万
リスク+
コストの和
目的関数

最適なリスク対策額

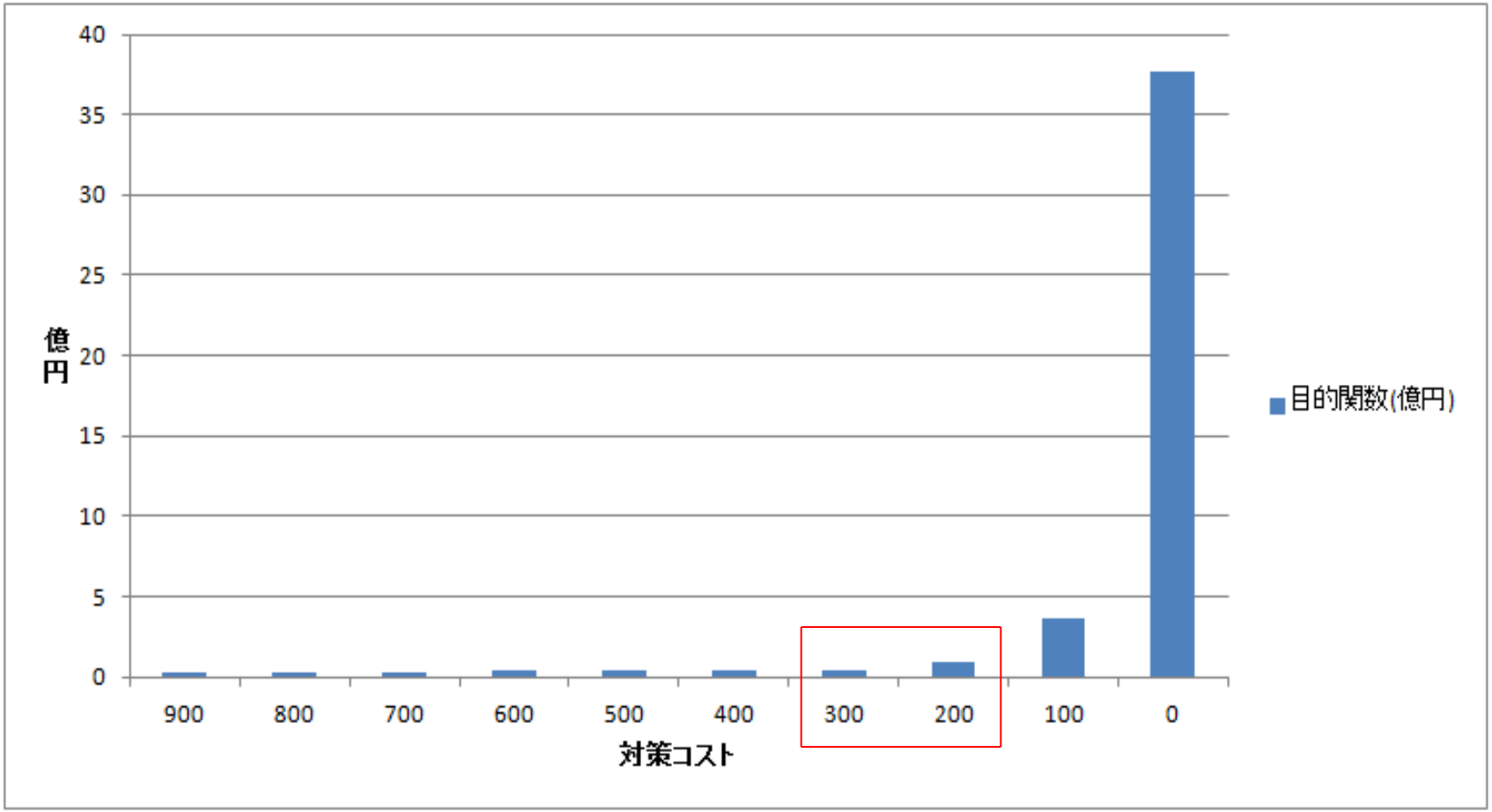


Dr. Karsten Nohl「セキュリティはどのぐらいが適量か？」CodeBlue 2016

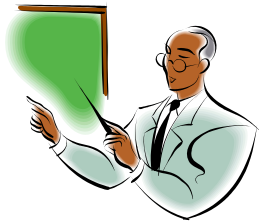
わたしたちのアプローチはこの要求にこたえうるものになっている。

http://www.slideshare.net/codeblue_jp/cb16-nohl-ja

対策コストごとのトータルリスク



MRCに関する最近の研究



１．Social-MRCについては、対象とSocial-MRCの仕組みの両方を多くの人に限られた時間で理解してもらうのは難しいので研究中断中。

２．MRCについて機能の拡張中

（１）標的型攻撃等シーケンスの深い攻撃のリスク評価のために、イベントツリーとディフェンスツリーを組みわせて用いるリスク解析法（EDC：Event Tree and Defense Tree Combined Method ）の確立＝＞最近の適用については相原資料を参照

（２）被害発生防止対策と復元対策の両方を考慮した対策案最適組合せ法

（３）動的リスクを考慮した多重リスクコミュニケータ

（４）経営者とのリスクコミュニケーションも考慮した多重リスクコミュニケータ

IoT時代のリスクアセスメントへの要求

＜最近の動向＞

IoTが普及

サイバー攻撃が高度化

セキュリティ対策が高コスト化

＜アセスメントへの要求＞

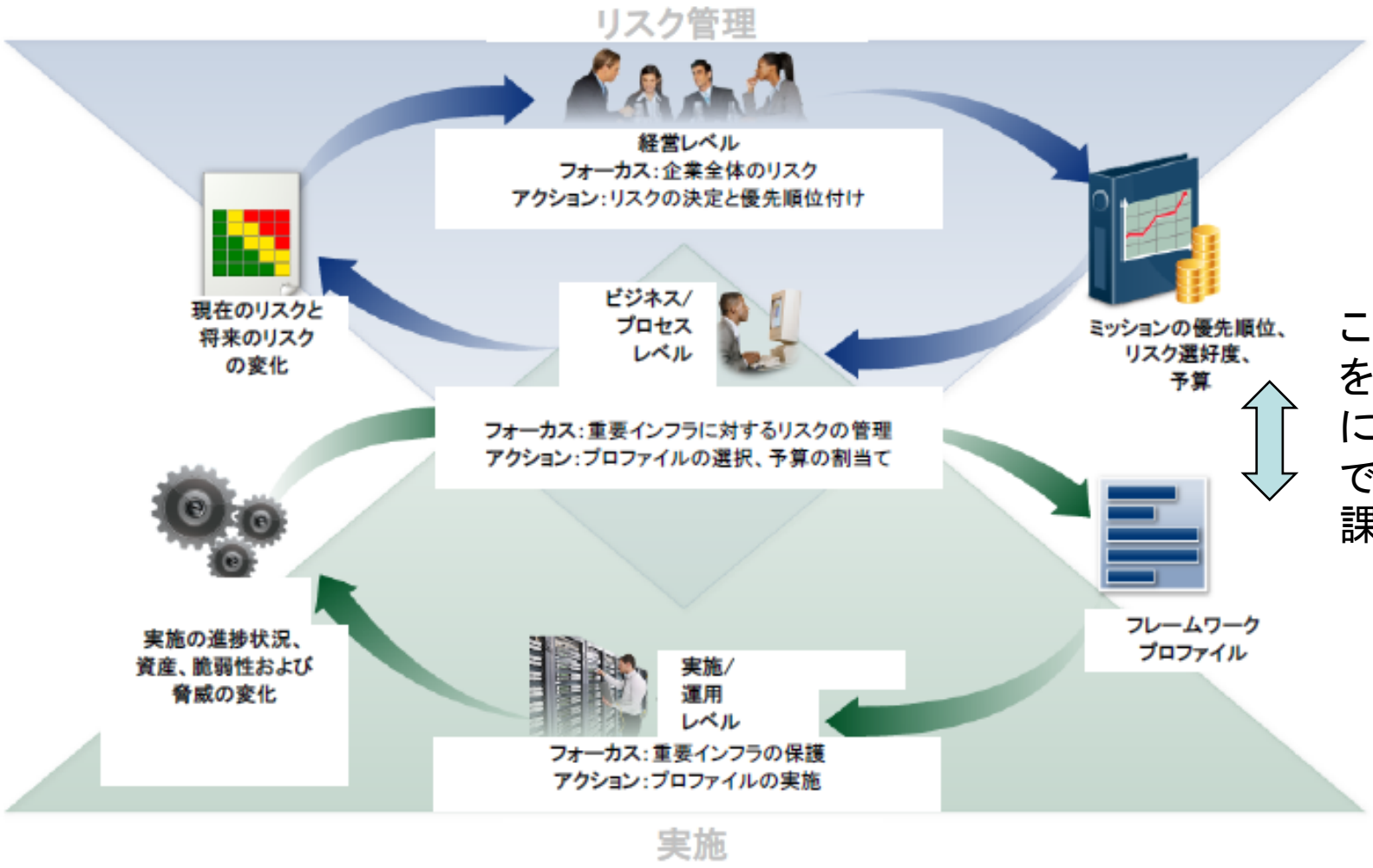
脅威分析が重要に

シーケンスの深い攻撃への評価方法が大切に

コスト効果のよい対策案組合せを求めることが必須に

経営者の参画がアセスメントへの参加が不可欠に

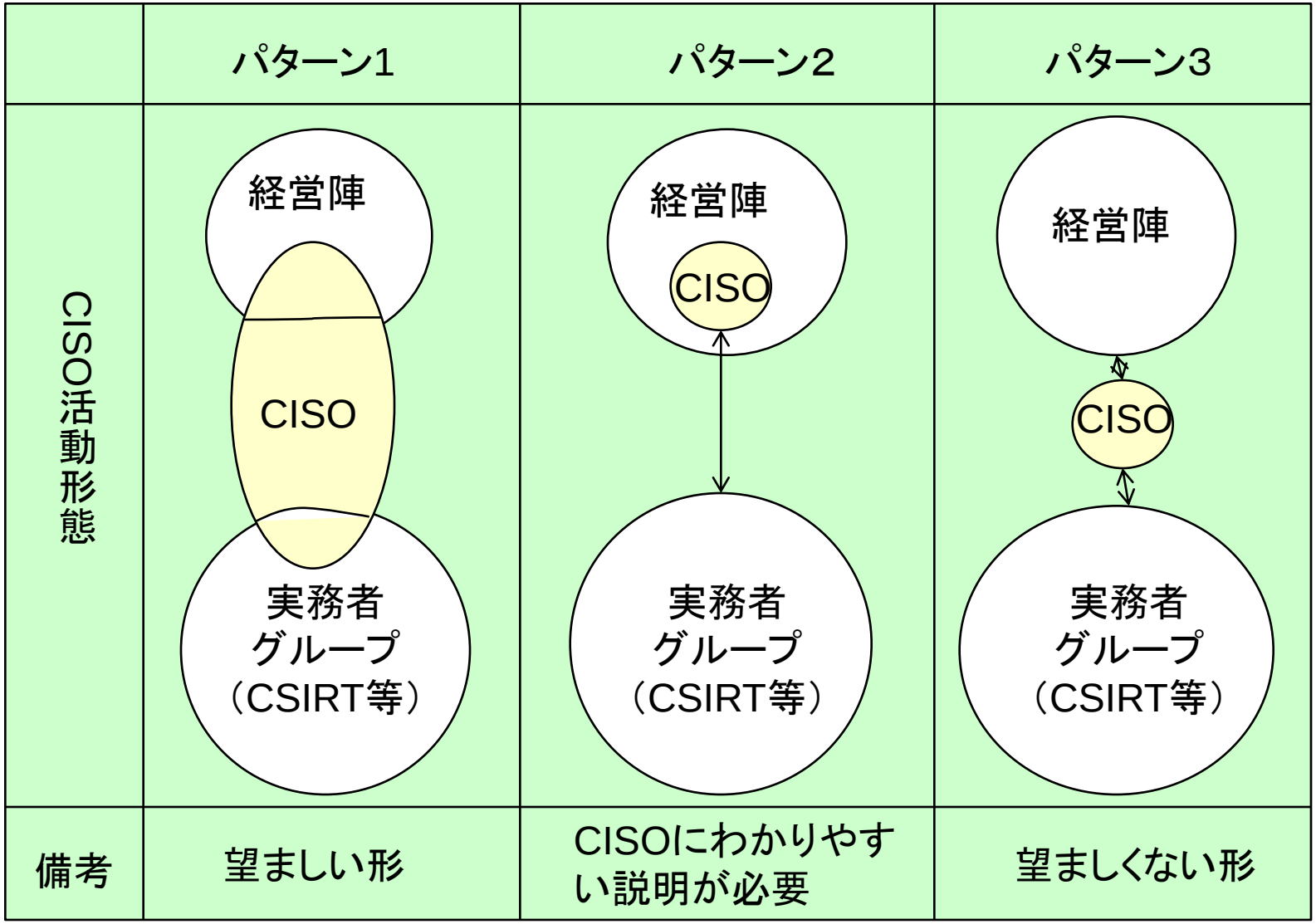
今後の方向



この部分をどのようにつないでいくかが課題

重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0版，2014年，米国国立標準技術研究所(NIST)

CISOの関与パターン



経営層と実務Grの情報のやり取り

	①多重リスクコミュニケーション型	②Tier情報交換型	③事故情報提示型	備考
CISOの質	優秀なCISOがいる場合		優秀なCISOがいない場合	
上から下への情報	方針・予算原案	方針・予算原案・目標Tier	方針・予算原案	
下から上への情報	リスクコミュニケーションによる合意形成	現状Tierと対策案	事故情報と対策効果	

多重リスクコミュニケータMRCの利用：CISOが経営者のロールプレイヤーになり合意形成をしたうえでその結果をわかりやすく経営層に説明　＝＞このようなことができるCISOは多くなさそう

$$\}+\sum_{i=1}^{8} \mathrm{Ci}*\mathrm{X}i\}$$

ト）

経営者向け制約

専門家が設定

アンケートなど

$$\sum_{i=1}^{8} D_{1i} X_i \le D_1$$

（プライバシー負担度）

専門家や関与者が設定

従業員向け制約

$$\sum_{i=1}^{8} D_{2i} X_i \le D_2$$

（利便性負担度）

従業員向け制約

$$P_{\alpha 1} + P_{\alpha 2} + P_{\beta} \le Pt \quad (X_i = 0,1)$$

（漏洩確率）

ユーザ向け制約

FTAにより計算

定式化結果

経営層と実務Grの情報のやり取り

	①多重リスクコミュニケーション型	②Tier情報交換型	③事故情報提示型	備考
CISOの質	優秀なCISOがいる場合		優秀なCISOがいない場合	
上から下への情報	方針・予算原案	方針・予算原案・目標Tier	方針・予算原案	
下から上への情報	リスクコミュニケーションによる合意形成	現状Tierと対策案	事故情報と対策効果	

Cybersecurity-Frameworkについて

- Cybersecurity-Frameworkとは
  - 2014年に米国国立標準技術研究所(NIST)が公表
  - セキュリティリスク管理原則を企業が適用できるようにする
  - セキュリティのリスクを把握・管理・表現することを補助する
  - 3つの要素から成り立つ
    - フレームワークコア
    - フレームワークインプレメンテーションティア
    - フレームワークプロファイル

Cybersecurity-Frameworkについて

- フレームワークコアとは
  - セキュリティリスクを管理する上で役に立つ主な成果一覧
  - 機能、カテゴリー、サブカテゴリー、参考情報からなる

機能の一意の識別子	機能	カテゴリーの一意の識別子	カテゴリー
ID	特定	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスク管理戦略
PR	防御	PR.AC	アクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術

重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0版，2014年，米国国立標準技術研究所(NIST)

Cybersecurity-Frameworkについて

フレームワークコア (コア)

- 対策をすることで効果が得られることが認められた分野一覧

フレームワークインプレメンテーションティア (ティア)

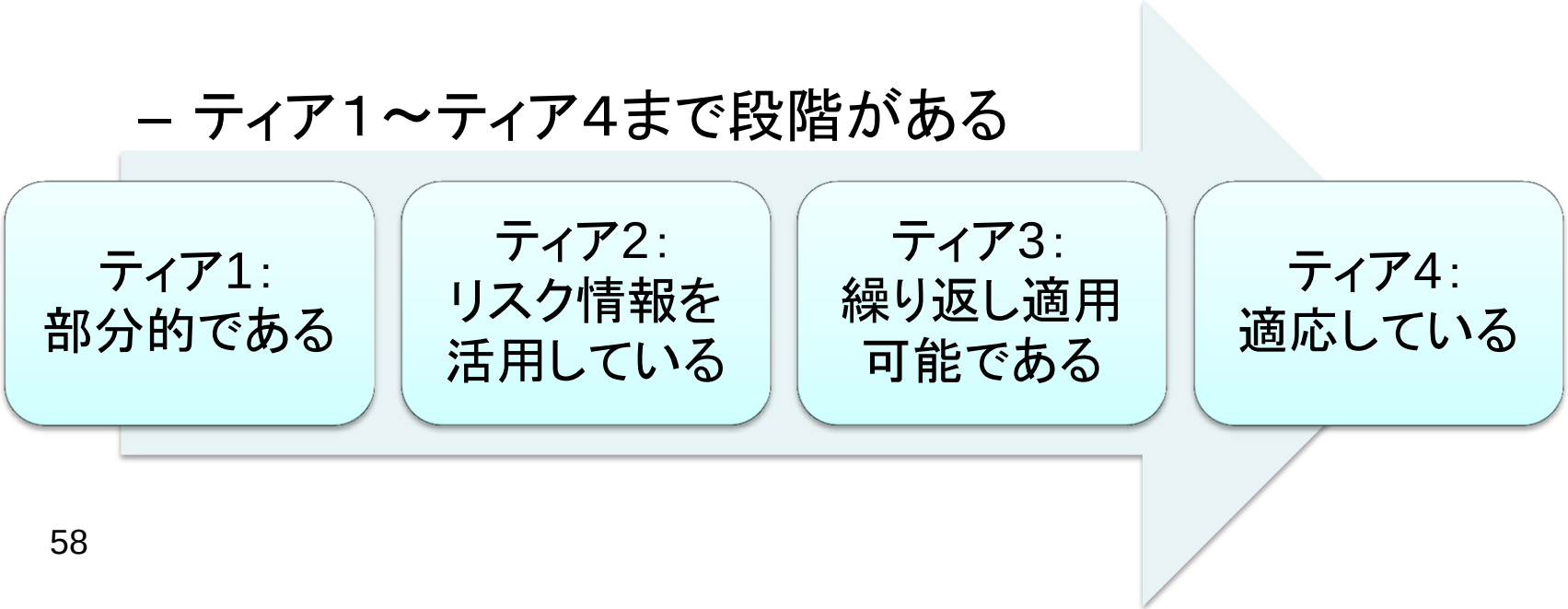
- リスク管理の認識やプロセスを4段階で示したもの

フレームワークプロファイル (プロファイル)

- 企業がコアから必要なカテゴリーを抜粋し、評価したもの

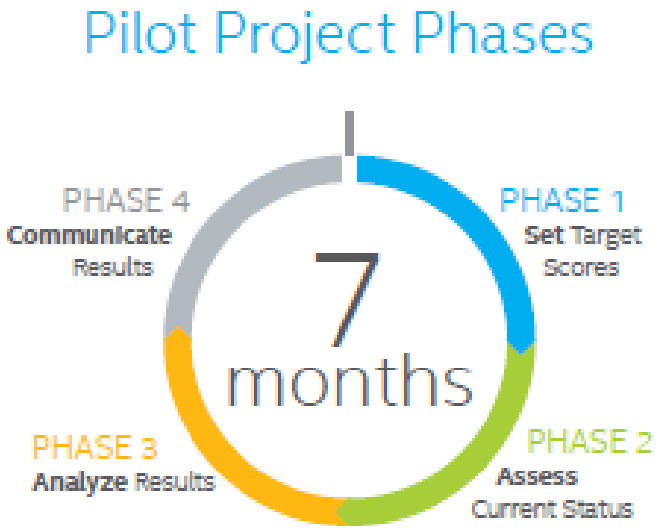
Cybersecurity-Frameworkについて

- フレームワークインプレメンテーションティアとは
  - 企業がセキュリティのリスクをどのように捉えているか、リスク管理にどのようなプロセスを実施しているかの段階
  - ティア１～ティア４まで段階がある



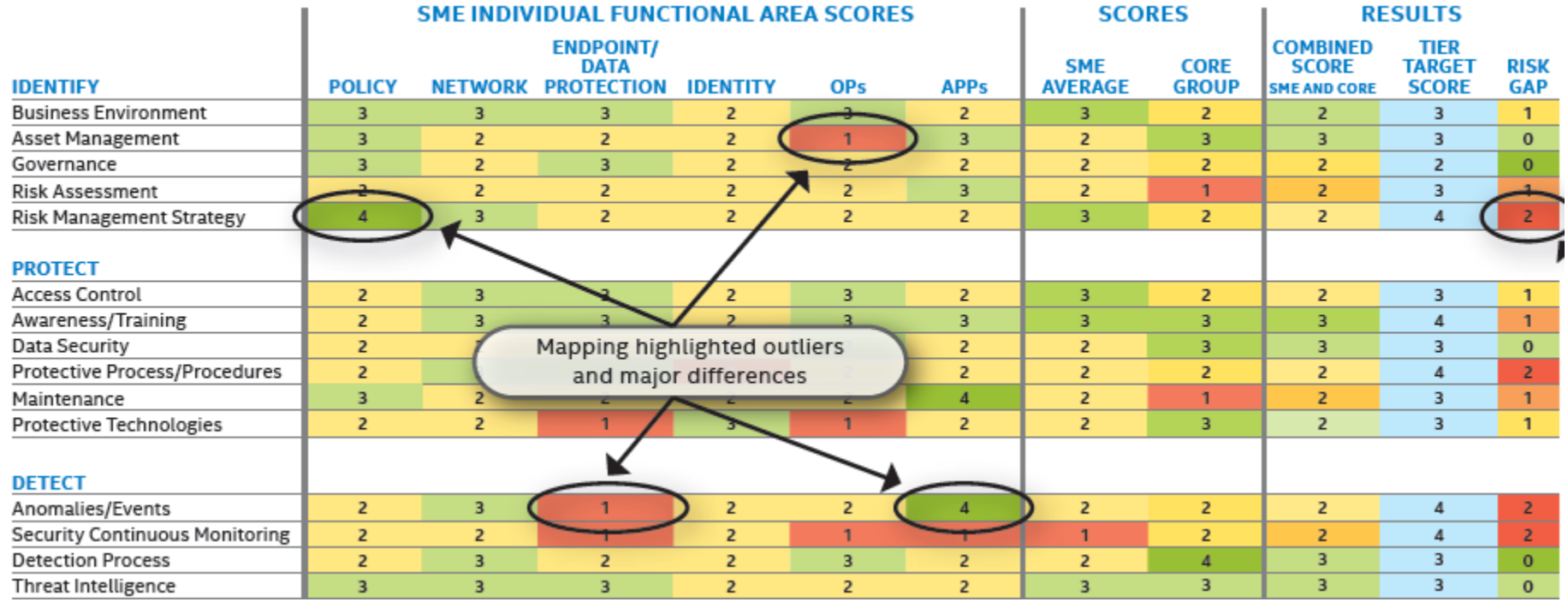
IntelのCybersecurity-Framework利用例

- Pilot Projectについて
  - 米Intel社は“Pilot Project”としてフレームワークを試用した
  - 4つのフェーズで7ヶ月間行動
    1. ティアの目標設定
    2. 現状評価
    3. 結果を分析
    4. 結果を協議



The Cybersecurity Framework in Action: An Intel Use Case, 2015年, Intel Corporation

IntelのCybersecurity-Framework利用例



	SME INDIVIDUAL FUNCTIONAL AREA SCORES						SCORES		RESULTS		
IDENTIFY	POLICY	NETWORK	ENDPOINT/ DATA PROTECTION	IDENTITY	OPs	APPs	SME AVERAGE	CORE GROUP	COMBINED SCORE SME AND CORE	TIER TARGET SCORE	RISK GAP
Business Environment	3	3	3	2	3	2	3	2	2	3	1
Asset Management	3	2	2	2	1	3	2	3	3	3	0
Governance	3	2	3	2	2	2	2	2	2	2	0
Risk Assessment	2	2	2	2	2	3	2	1	2	3	1
Risk Management Strategy	4	3	2	2	2	2	3	2	2	4	2
PROTECT											
Access Control	2	3	2	2	3	2	3	2	2	3	1
Awareness/Training	2	3	3	2	3	3	3	3	3	4	1
Data Security	2	2	2	2	2	2	2	3	3	3	0
Protective Process/Procedures	2	2	2	2	2	2	2	2	2	4	2
Maintenance	3	2	2	2	2	4	2	1	2	3	1
Protective Technologies	2	2	1	3	1	2	2	3	2	3	1
DETECT											
Anomalies/Events	2	3	1	2	2	4	2	2	2	4	2
Security Continuous Monitoring	2	2	1	2	1	1	1	2	2	4	2
Detection Process	2	3	2	2	3	2	2	4	3	3	0
Threat Intelligence	3	3	3	2	2	2	3	3	3	3	0

カテゴリー

各担当者の評価

目標値

The Cybersecurity Framework in Action: An Intel Use Case, 2015年, Intel Corporation

適用実験

- 対策前の状態

機能名	カテゴリー名	業務A	業務B	業務C	管理者平均	経営陣評価	全体平均	目標値	リスクギャップ
特定	資産管理	2	1	2	1	2	1	3	−2
	リスクアセスメント	2	1	1	1	2	1	3	−2
	ビジネス環境	1	2	2	1	2	1	2	−1
防御	アクセス制御	2	2	2	2	3	2	3	−1
	意識向上およびトレーニング	2	1	1	1	3	1	4	−3
	データセキュリティ	2	2	2	2	3	2	3	−1
対応	改善	3	1	2	2	2	2	3	−1

課題

- Cybersecurity-Frameworkの課題
  - 組織の要件を満たすためには目標に至るための対策が必要
  - フレームワークは現状と目標の差異を分析するためのもの

対策案を列挙・選定するという部分まで至っていない

Intelの利用例を基に対策列挙手法を提案
（研究室の小さな問題に試適用）

情報処理学会DICOMO2016シンポジウム

Cybersecurity-Framework を用いた対策案合意形成手法の提案

福島章太[1]　　佐々木良一[2]

概要：近年，情報社会の進展に伴い，IT システムに依存する企業が増加した．一方，企業内において，経営陣と管理者層の情報セキュリティに関わる共通認識が乏しく，十分な情報セキュリティ対策が行えていないことが指摘されている．この課題に対する取り組みは数多く行われており，その中の一つに米国の NIST が開発した「Cybersecurity-Framework」がある．しかし，「Cybersecurity-Framework」は経営陣と管理者層で共通認識を得ることに留まっており，共通認識に基づき具体的な対策を列挙・選定する手法を示していない．本稿では，「Cybersecurity-Framework」とその利用例を基に，経営陣と管理者層が情報セキュリティに対する共通認識を得た上で具体的な対策を列挙出来る手法の提案と，その手法を実現可能にするシステムを実装する．

対策案のイメージ

- 対策例

業務C

ティアの定義

カテゴリー

	ティア2		ティア3			ティア4		
	2-1	2-2	3-1	3-2	3-3	4-1	4-2	4-3
ビジネス環境	○	○	●	●	—	●	—	—
アクセス制御	○	○	×	×	×	—	—	—

対策1	広報係の管理者アカウント分離の検討会議

試適用結果

- 対策前後の比較

機能名	カテゴリー名	企画	サイボウズ管理	広報	管理者平均	経営陣評価	全体平均	目標値	リスクギャップ
特定	資産管理	2→3	1→3	2→3	3	3	3	3	0
	リスクアセスメント	2→3	1→4	1→3	3	3	3	3	0
	ビジネス環境	1	2→3	2→3	2	2	2	2	0
防御	アクセス制御	2→3	2	2→3	2	3	2	3	−1
	意識向上およびトレーニング	2→3	1→3	1→3	3	3	3	4	−1
	データセキュリティ対策を行った範囲：	2→3	2	2→3	2	3	2	3	−1
対応	改善	3	1→2	2→3	2	2	2	3	−1

試適用によって得られた知見

（1）実際に提案手法で対策を列挙することが出来、提案手法で列挙した対策によってティアの数値が上昇することを示すことができた

（2）対策をとるとTierが本当に上昇するかどうかについて合意をとるのは簡単ではなかった

経営層と実務Grの情報のやり取り

	①多重リスクコミュニケーション型	②Tier情報交換型	③事故情報提示型	備考
CISOの質	優秀なCISOがいる場合		優秀なCISOがいない場合	
上から下への情報	方針・予算原案	方針・予算原案・目標Tier	方針・予算原案	ビジネスリスクへの影響（業務停止時間など）をやり取りする手も
下から上への情報	リスクコミュニケーションによる合意形成	現状Tierと対策案	事故情報と対策効果	

デルタISMSモデル文献

情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2015-CSEC-70 No.24
Vol.2015-SPT-14 No.24
2015/7/3

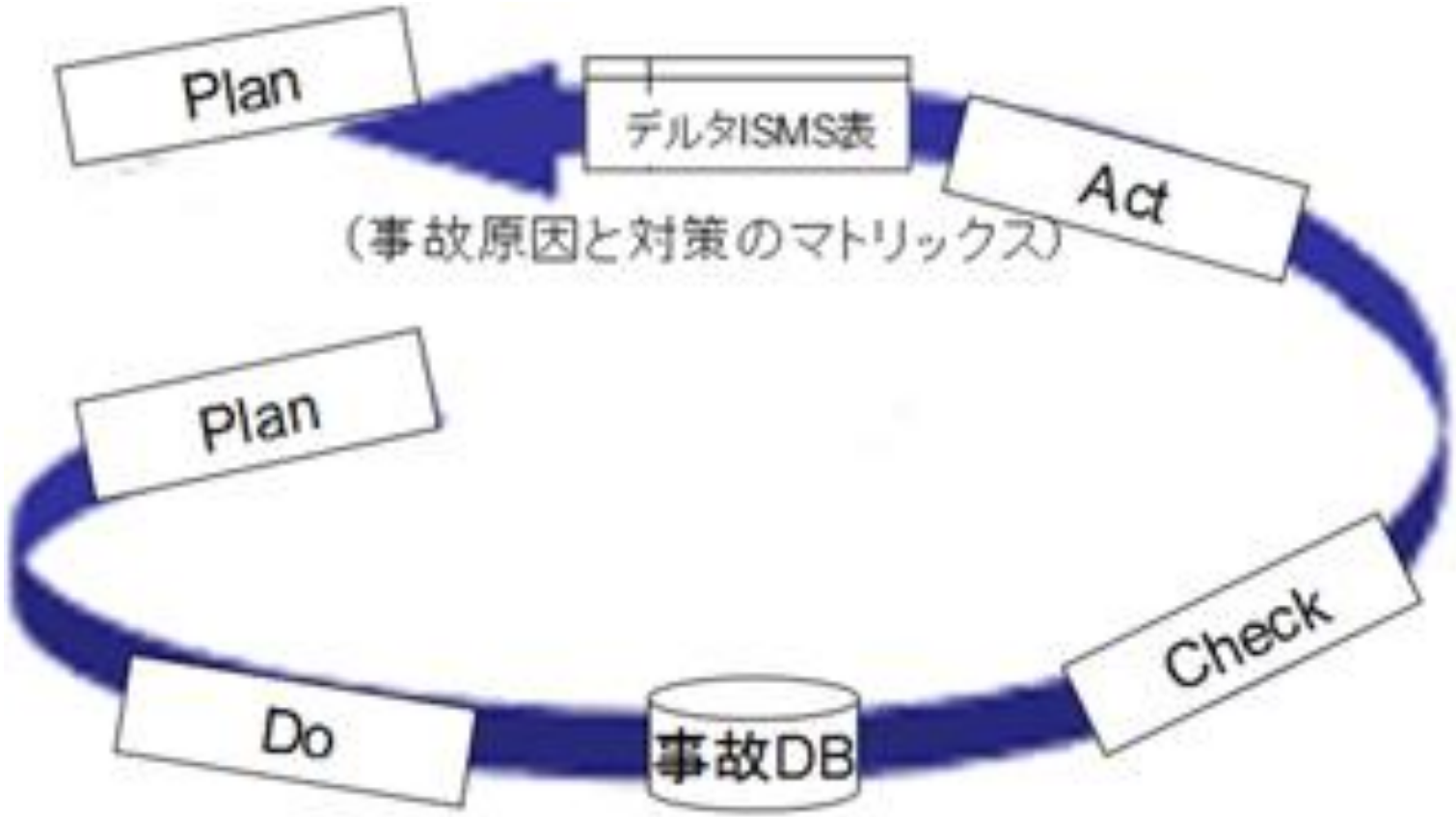
デルタ ISMS モデルの提案
－ 事故データベースに基づく ISMS の強化 －

堀川博史[†1]　大谷尚通[†2]　髙橋雄志[†3]　加藤岳久[†4]
間形文彦[†5]　勅使河原可海[†3]　佐々木良一[†3]　西垣正勝[†6]

本稿では事故データベースに基づき ISMS を強化する「デルタ ISMS モデル」を提案する．組織の情報セキュリティマネジメントを進めるうえで経営陣の関与は重要であるが，従来，「費用対効果の説明手法」や「経営者の認識・理解の向上のための手法」の改善は十分でなかったという課題に対して，組織で実際に発生した事故データベースに基づき，経営陣と管理者・従業員層が共有できる KPI を提供することで，経営陣の情報セキュリティマネジメントの関与を促し，組織全体の PDCA サイクルの実現を目指す．事故データベースに基づくリスクアセスメント情報セキュリティガバナンスの経営陣と CISO 間のモニタリング項目に対して余分な情報がないことを示す．デルタ ISMS が提供する情報は経営陣に対して状況や課題を的確に示すことで理解を促進させることができ，リスク管理方針の評価に有用な情報となる．

情報処理学会論文誌2016年9月号にも掲載予定

デルタISMSの基本モデル



事故データベースのサンプル

表 4　事故データベースのサンプル（部分）

Table 4 Sample of an accident database (part)

日時	事故内容	事故原因	事故経路	1次対処の被害額	影響範囲	2次処置の対策コスト
4月3日	帰宅時に電車の網棚においたカバンから紛失	紛失	携帯電話	25万円	事故	6万円（MDM）
5月4日	洗面所で胸ポケットに入れたカードが滑り出た模様	紛失	自社セキュリティカード	1万円	ヒアリハット	3万円（蓋つきケース）
6月5日	社外秘扱いの紙をプリンターの裏紙に使用していた	誤操作	紙資料	1万円	（実地検査による）ヒアリハット	1万円（規則変更）

デルタISMS表のサンプル

		対策済						上	中	下
	対策	1 使用前ロックを設定する	2 履歴を残さない設置にする	3 毎持ち出し時には許可制とする	4 連絡先を貼りつける	5 蓋つきフォルダーに入れる	6 ストラップを付ける	7 移動時チェックシステムを導入する	8 遠隔データ初期化サービスを利用する	9 毎月定期確認する
事故	コスト(万円) / ALE	100	50	80	20	20	30	1200	300	110
携帯電話紛失	2500万円	0.3	0.3	0.2	0.1	0	0.3	0.6	0.6	0.05
セキュリティカード紛失	2500万円	0	0	0	0.1	0.3	0.3	0.6	0	0.05
紙資料紛失	250万円	0	0	0.2	0	0	0	0.6	0	0

情報セキュリティガバナンスにおけるモニタリング項目

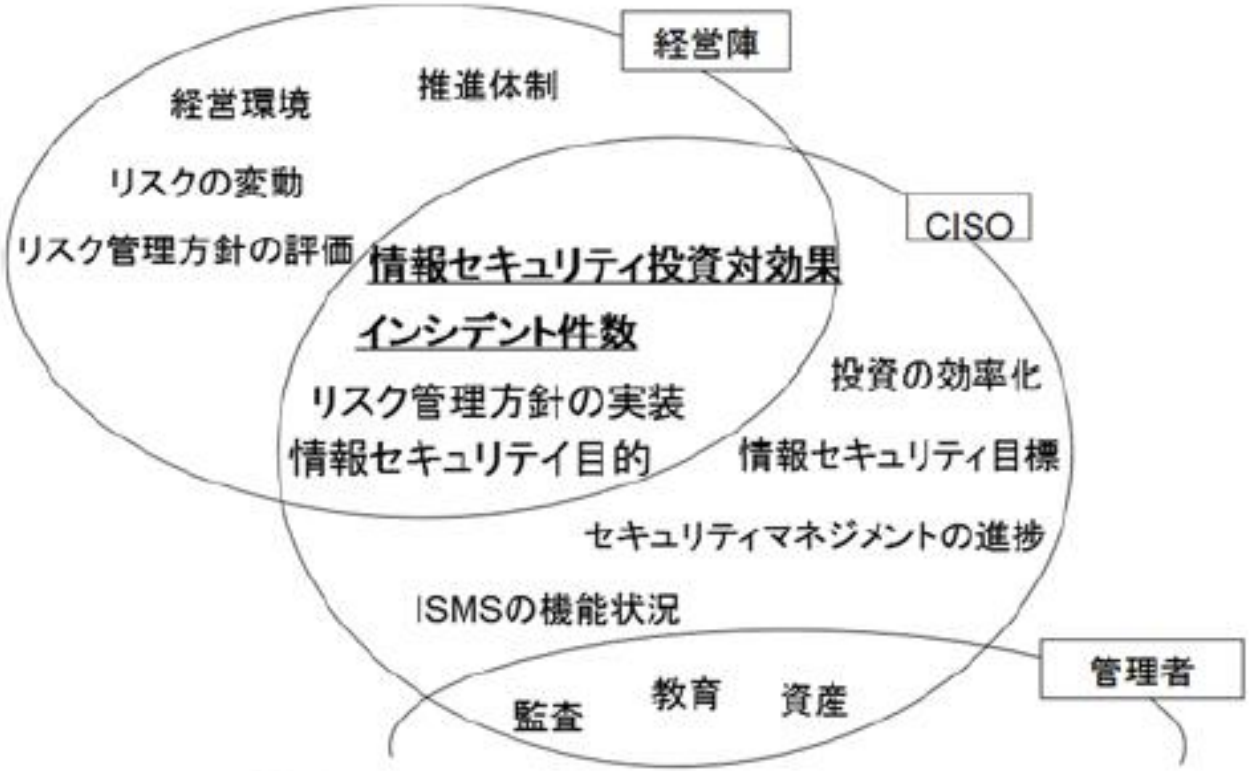
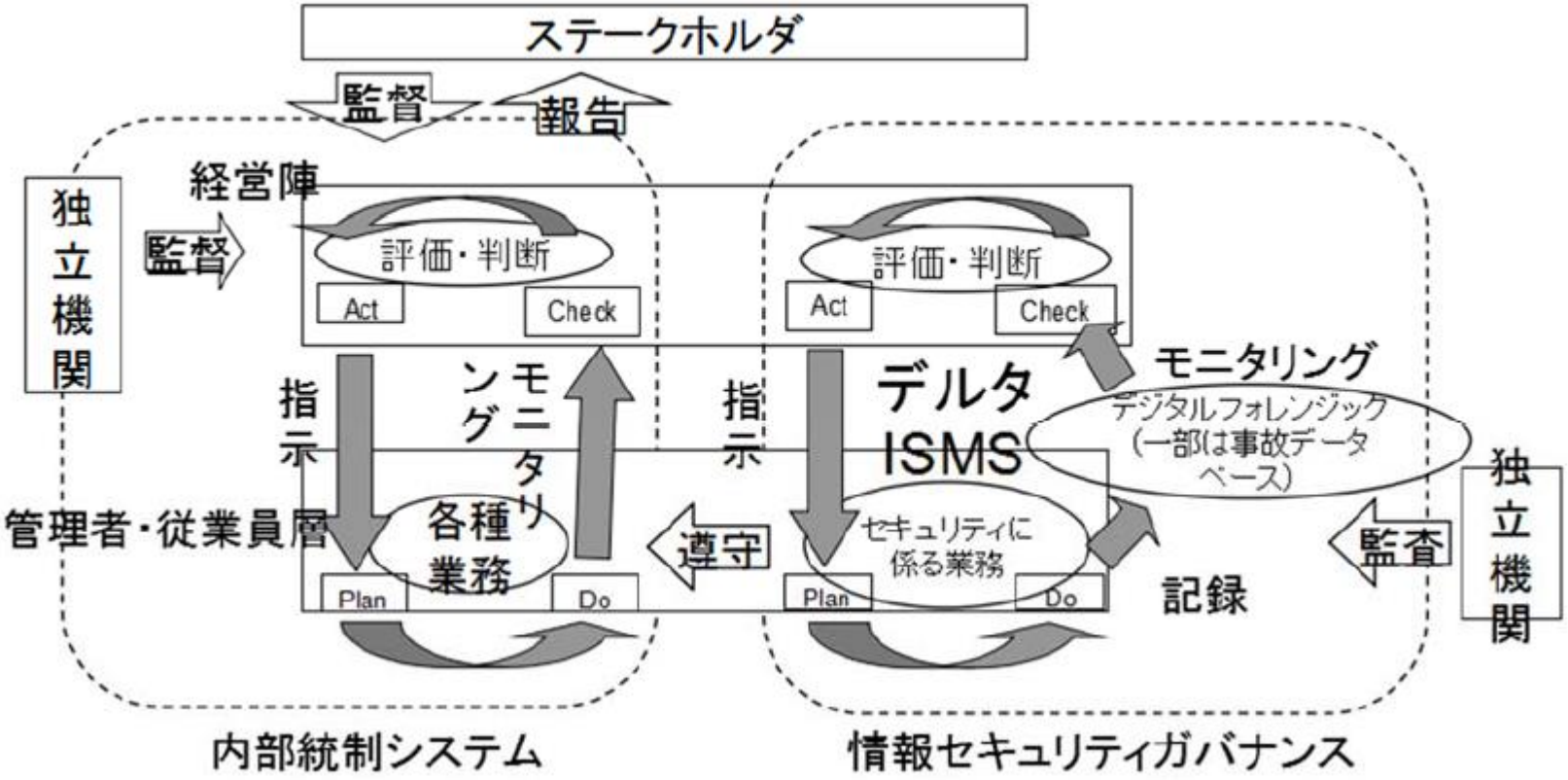


図 4　情報セキュリティガバナンスにおけるモニタリング項目

デジタルフォレンジックを用いたデルタISMS



目次

1. はじめに
2. IoTの特徴
3. リスクアセスメントの動向
4. 東京電機大学におけるアプローチ
5. 最近の注目すべき動向

注目すべき動き

1. ITシステムのリスクアセスメントに対する統合的アプローチ
   （a）FAIRアプローチ
   （b）対策とのリンク
2. 情報共有プロトコルの標準化

FAIRとは

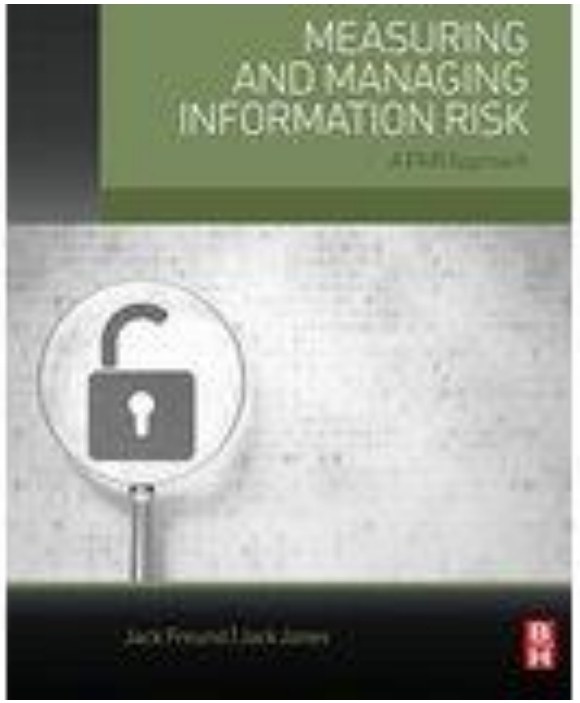
Factor analysis of information risk (**FAIR**) is a taxonomy of the factors that contribute to risk and how they affect each other. It is primarily concerned with establishing accurate probabilities for the frequency and magnitude of data loss events. It is not a methodology for performing an enterprise (or individual) risk assessment.[1]

FAIR is also a risk management framework developed by Jack A. Jones, and it can help organizations understand, analyze, and measure information risk according to Whitman & Mattord (2013).

https://en.wikipedia.org/wiki/Factor_analysis_of_information_risk

FAIRに関する本

Jack Freund, Jack Jones “Measuring and Managing Information Risk A FAIR Approach” Elsevier, 2015



「定量的リスク分析を積極的に扱い発生確率の不確実性を考慮し、モンテカルロ法を用いてリスクの分布を求めるような方法も提案されている。」

FAIR INSTITUTE MISSION

The FAIR Institute is a non-profit organization made up of forward-thinking risk officers, cybersecurity leaders and business executives that operates with a central mission: **Establish and promote information risk management best practices that empower risk professionals to collaborate with their business partners on achieving the right balance between protecting the organization and running the business.**
Factor Analysis of Information Risk (FAIR) is the discipline, the framework, and the driver behind our mission.

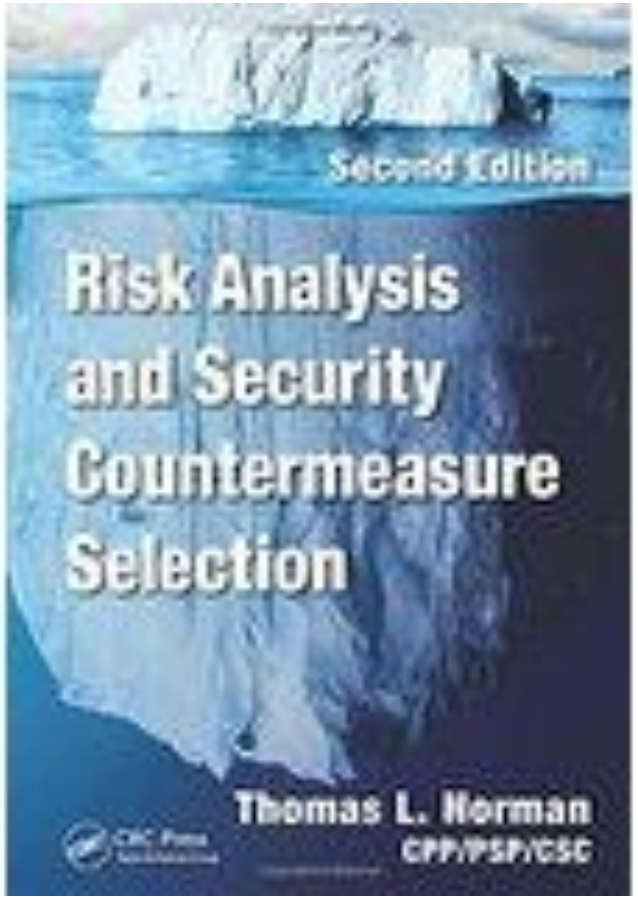
http://www.fairinstitute.org/mission

注目すべき動き

1. ITシステムのリスクアセスメントに対する統合的アプローチ
   （a）FAIRアプローチ
   （b）対策とのリンク
2. 情報共有プロトコルの標準化

文献

- Thomas L. Norman “Risk Analysis and Security Countermeasure ” CRC Press, 2016



注目すべき動き

1. ITシステムのリスクアセスメントに対する統合的アプローチ
   （a）FAIRアプローチ
   （b）対策とのリンク
2. 情報共有プロトコルの標準化

サイバーキルチェーン

- Lockheed Martin: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (ICIW2011) (2011年3月)
- 【モデル化で対象とする攻撃】
  "Advanced Persistent Threat" (APT)
- 【モデル】
  1. Reconnaissance (偵察)
  2. Weaponization (武器化)
  3. Delivery (配送)
  4. Exploitation (攻撃)
  5. Installation (インストール)
  6. Command and Control (C2) (遠隔制御)
  7. Actions on Objectives (実行)

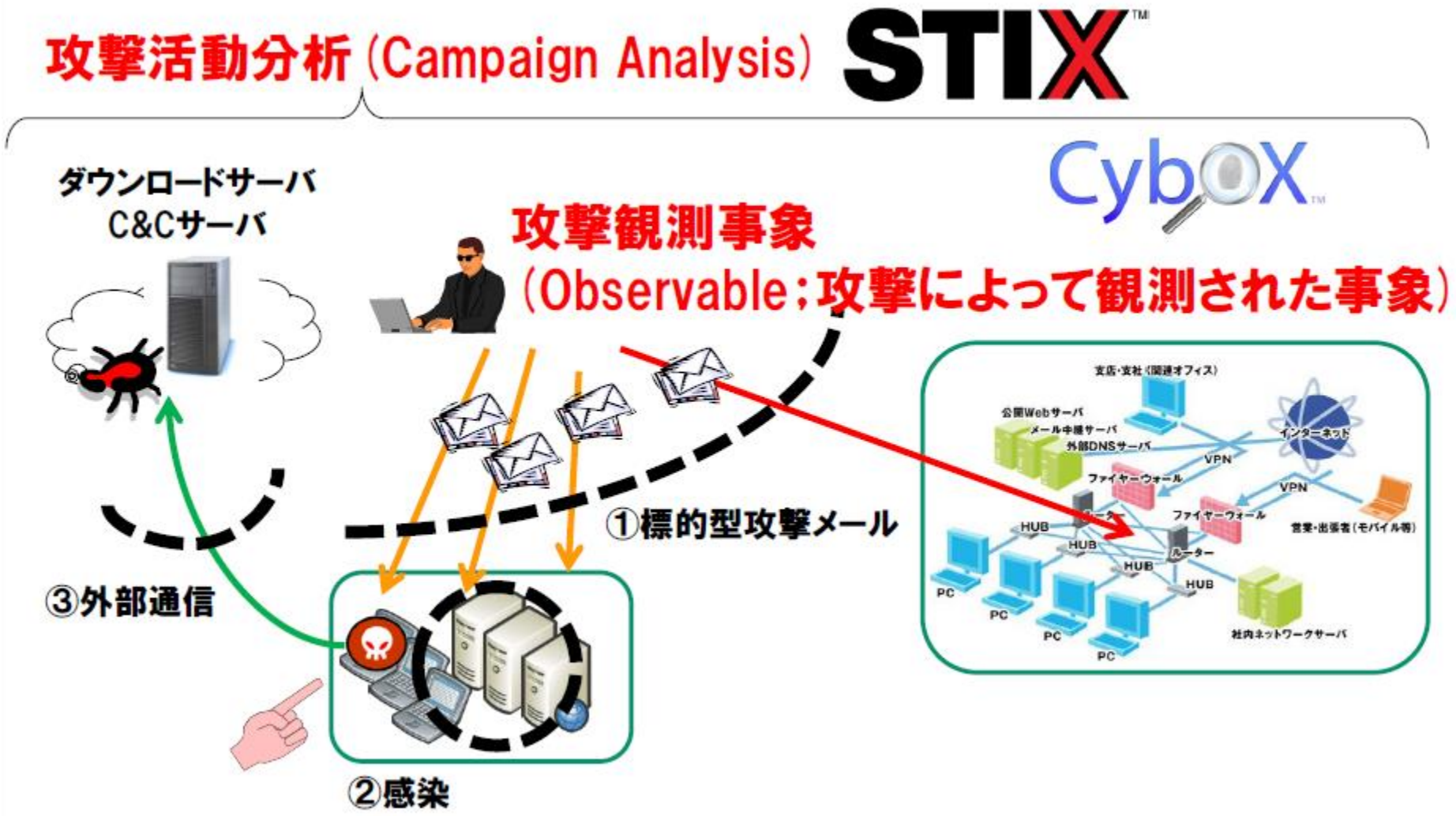
http://www.iwsec.org/mws/2012/presentation/2A1-3-slide.pdf

CYBEX

- ITU-T Q.4/17: X.cybex
  (Global Cybersecurity Information Exchange Framework;サイバーセキュリティ情報交換フレームワーク)
  - 共通仕様を用いて、グローバルかつタイムリーなサイバーセキュリティ情報の交換、活用ならびに、相互運用を実現するためのフレームワークを実現するため、脆弱性対策情報ならびにインシデント対応のフォーマット、番号体系などの技術仕様について標準化を進めている。
    脆弱性対策関連(X.cpe、X.cce、X.cve、X.crf、X.oval、X.cwe、X.cvssなど)、インシデント対応関連(X.cee、X.iodef、X.capecなど)の共通仕様がある。

http://www.iwsec.org/mws/2012/presentation/2A1-3-slide.pdf

サイバーセキュリティ情報交換仕様



http://www.iwsec.org/mws/2012/presentation/2A1-3-slide.pdf

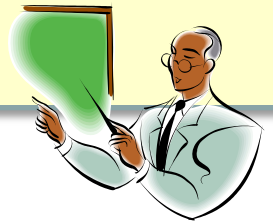
Taxiiとは

- TAXII（検知指標情報自動交換手順、Trusted Automated eXchange of Indicator Information）は脅威情報のセキュアな転送と交換を提供する技術仕様です。
- TAXIIがSTIX形式のコンテンツのみをサポートするかのような印象を与える記事が多いですが、実際には多様なフォーマットで情報を転送することができます。しかし現在の実践においては、TAXII転送とSTIX記述、そしてCybOXの語彙を組み合わせて使用するのが一般的です。

https://asmarterplanet.com/jp-security/blog/2015/07/80.html

終りに

- IoTの普及によりセーフティとセキュリティの融合が必要性が高まった
- それに伴い脅威分析の必要性やリスク評価の重要性が高まった。
- IoTを含むシステムのリスク評価技術については今後さらに改善が必要。




END