公民連携活性化協会

2021年5月28日

改定ガイドラインの概要と今後の自治体情報セキュリティ対策

東京電機大学
研究推進社会連携センター
顧問・客員教授
佐々木良一
r.sasaki@mail.dendai.ac.jp

イントロダクション

自己紹介：**佐々木良一**　（東京電機大学客員教授）

1971年ー2001年　日立製作所。1984年より情報セキュリティなどの研究に従事

2001年ー2018年3月　東京電機大学未来科学部教授

2018年ー2020年3月　総合研究所　特命教授

サイバーセキュリティ研究所長

日本セキュリティマネジメント学会会長
デジタルフォレンジック研究会会長
内閣官房サイバーセキュリティ補佐官
などを歴任

目次

講演①

講演②

米石油パイプライン企業へのサイバー攻撃

- 2021年5月7日、米国の石油パイプライン企業Colonial Pipelineはランサムウエアによる被害をうけファイルが強制暗号化され、被害の拡大を防止するため業務全体を一時停止する措置を講じたことを発表。このため燃料供給が遅延。

- 攻撃者はロシアの犯罪グループDarkSide（使用されたランサムウエアの名でもある。）

https://piyolog.hatenadiary.jp/entry/2021/05/12/051650
https://www.nikkei.com/article/DGXZQOGN14F4F0U1A510C2000000/?fbclid=IwAR1nIVI1hwR5eUVaplQgodY8kSLTZMOYm5zRWlFOdPp3fIT971tZwg7RHTI

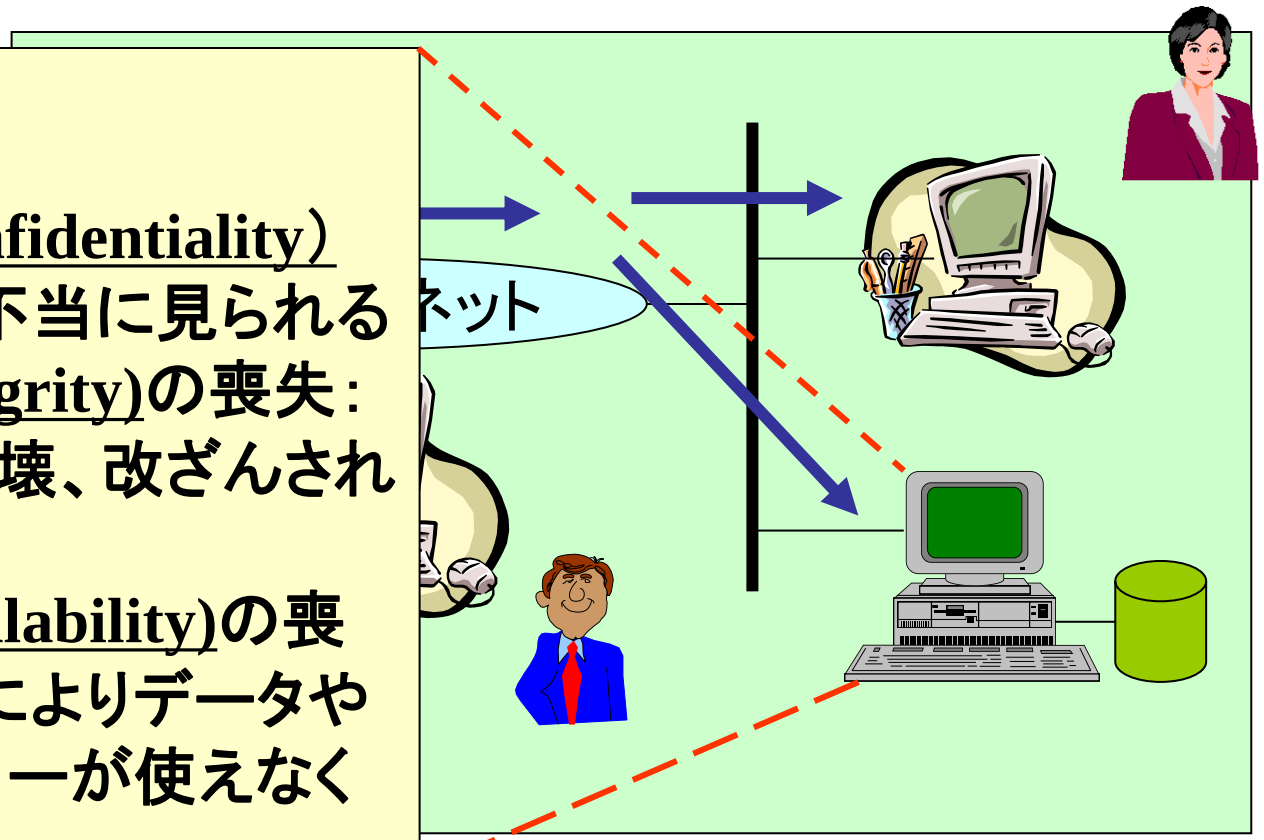
インターネット社会の脅威

脅威の分類

（1）機密性（Confidentiality）の喪失：情報を不当に見られる

（2）完全性(Integrity)の喪失：情報を不当に破壊、改ざんされる

（3）可用性(Availability)の喪失：不当な利用によりデータやコンピュータパワーが使えなくなる



攻撃に対する主要な対策

攻撃者

不正侵入の実施

成りすまし

セキュリティホール

1．論理的セキュリティ

（1） システム的（技術的）セキュリティ：暗号化、アクセス制御、ウイルス対策など

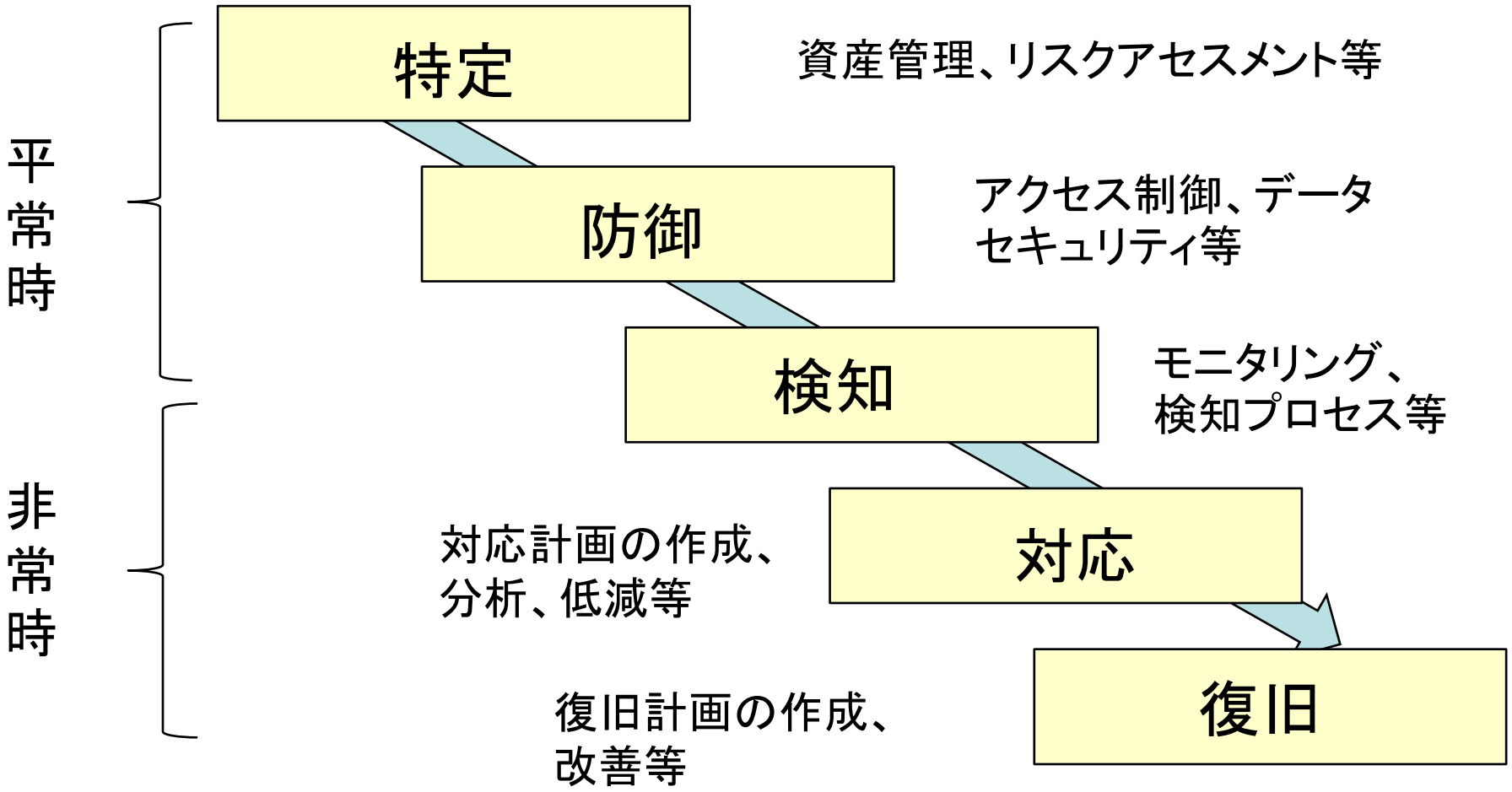
（2） 管理的セキュリティ：セキュリティポリシーの策定・運用・監査・見直しなど

（3）人的セキュリティ：委託計画におけるセキュリティ対策、教育、訓練など

2．物理的セキュリティ

入退出管理、バックアップセンターの設置など

情報セキュリティの対策フェーズ



NISTの　Cyber Security　Frameworkによる分類

サイバー攻撃の歴史

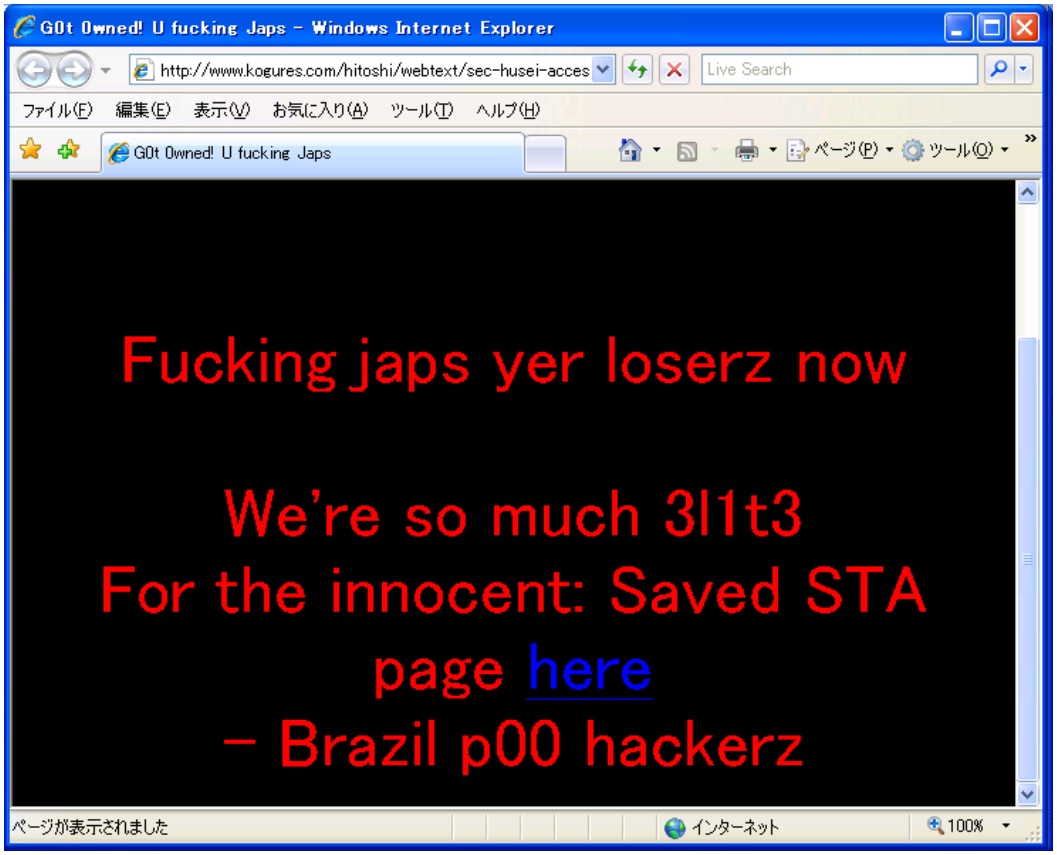
＜セキュリティにとっての第一のターニングポイント＞

2000年　科学技術庁などのホームページの改ざん事件
2000年　　不正アクセス禁止法施行
2000年　　JNSA発足（2001年NPO化）
2001年　Code　Red、Sircumによる被害
2001年　　電子署名法施行
2001年　　CRYPTREC（暗号技術検討会）発足

＜セキュリティにとっての第二のターニングポイント＞

2010年　Stuxnetの出現(遠心分離機への攻撃)
2011年　　ウイルス作成罪施行
2011年　三菱重工などへの標的型メール攻撃
2015年　日本年金機構への攻撃

科学技術庁ホームページ改ざん事件



2000年1月

Reference：http://www.kogures.com/hitoshi/webtext/sec-husei-access/homepage.html

サイバー攻撃の歴史

＜セキュリティにとっての第一のターニングポイント＞

2000年　科学技術庁などのホームページの改ざん事件
2000年　　不正アクセス禁止法施行
2000年　　JNSA発足（2001年NPO化）
2001年　Code　Red、Sircumによる被害
2001年　　電子署名法施行
2001年　　CRYPTREC（暗号技術検討会）発足

＜セキュリティにとっての第二のターニングポイント＞

2010年　Stuxnetの出現(遠心分離機への攻撃)
2011年　　ウイルス作成罪施行
2011年　三菱重工などへの標的型メール攻撃
2015年　日本年金機構への攻撃

2つのターニングポイントの比較

	第一次ターニングポイント（2000年ごろ）	第二次ターニングポイント（2010年以降）
攻撃目的	面白半分	多様化（面白半分、主義主張、お金儲け、国家の指示）
攻撃者	ハッカー（クラッカー）	ハッカー、ハクティビスト、犯罪者、スパイ、軍人
攻撃対象	WEBなどの一般IT	重要情報インフラも＜Stuxnet＞
攻撃パターン	不特定多数	標的型＜Stuxnet、ソニー、三菱重工、日本年金機構＞
攻撃技術	低ー中	中ー高　＜Stuxnet、ソニー、三菱重工、農林水産省 ＞

従来の攻撃が風邪なら、新しい攻撃は新型インフルエンザ

目次

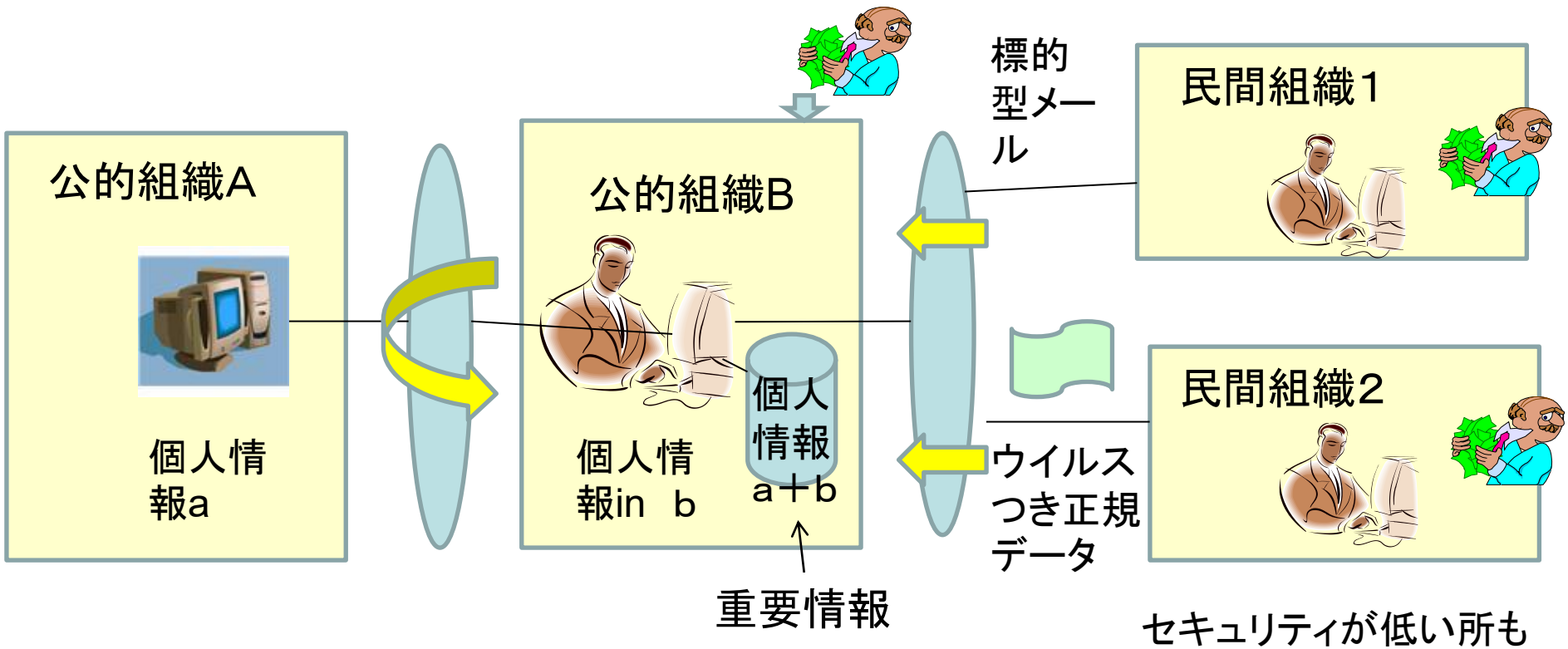
講演①

1. はじめに
2. 前回の自治体セキュリティガイドラインの改定の概要
3. 今回のガイドライン改定内容

講演②

4. 具体的対策の決定ためのリスクアセスメント
5. おわりに

マイナンバー関連システム構成



＜よく検討され、安全性は高い＞

＜従来あまり議論されてこなかった。対策をよりよいものにしていく努力が必要＞

自治体情報セキュリティ対策検討チーム設置（2015年）

【構成員】（敬称略）

上原 哲太郎 立命館大学情報理工学部情報システム学科 教授
岡村 久道 弁護士 国立情報学研究所客員教授
佐々木 良一 東京電機大学未来科学部教授（座長）
(内閣官房サイバーセキュリティ補佐官)
三輪 信雄 総務省最高情報セキュリティアドバイザー
原田 智 京都府政策企画部情報政策統括監
大高 利夫 藤沢市総務部参事兼IT推進課長
佐野 茂樹 上田市総務部広報情報課係長

【開催状況】

第1回会合 平成27年7月9日（木）
第2回会合 平成27年8月3日（月）
第3回会合 平成27年8月12日（水）中間報告
第4回会合 平成27年9月16日（水）
第5回会合 平成27年11月20日（金）報告書
第6回会合 平成27年12月28日（月）

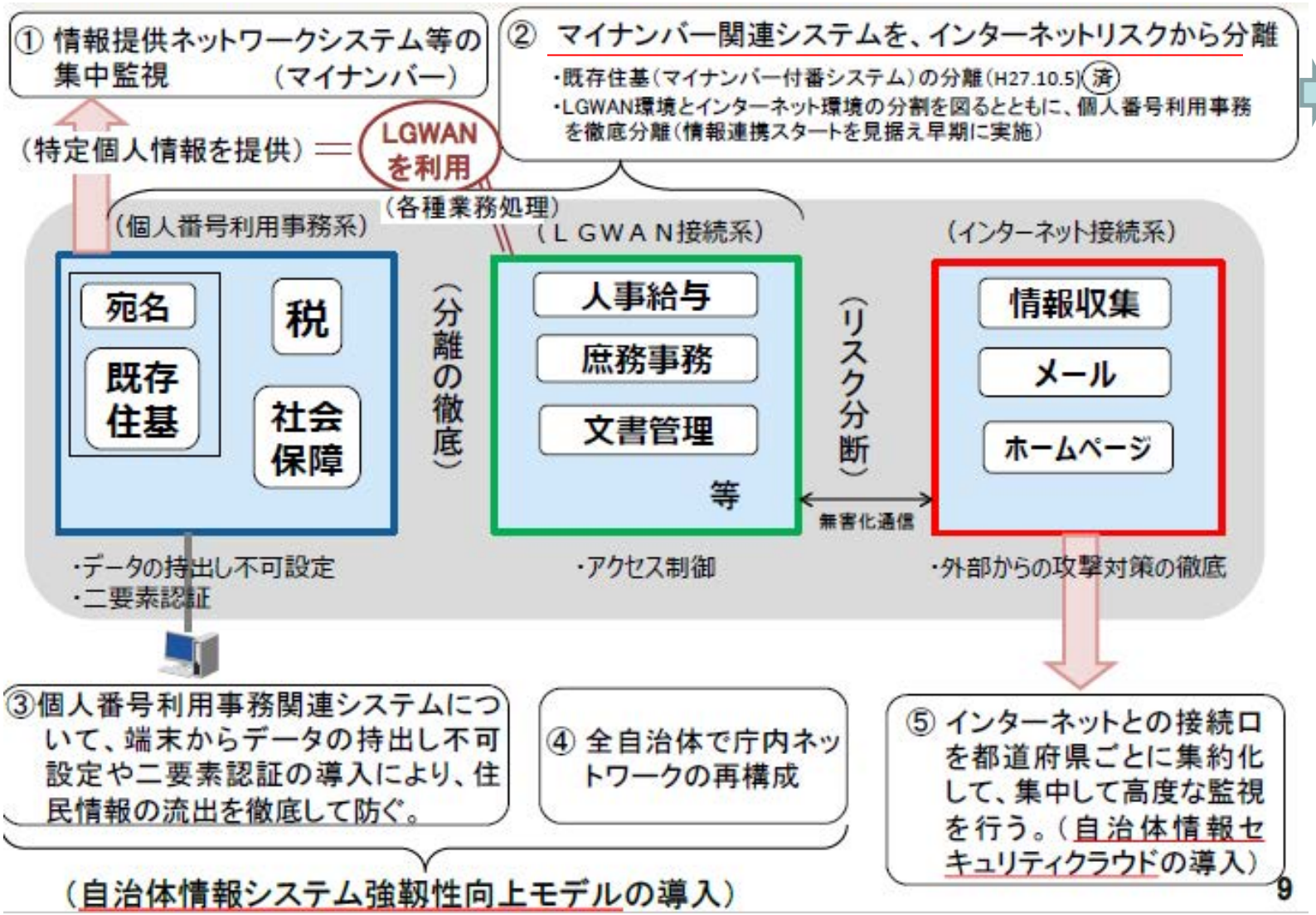
新たな自治体情報セキュリティ対策の抜本的強化の概要

1. 各自治体におけるインシデント即応体制の強化

2. 攻撃リスク等の低減のための抜本的強化対策

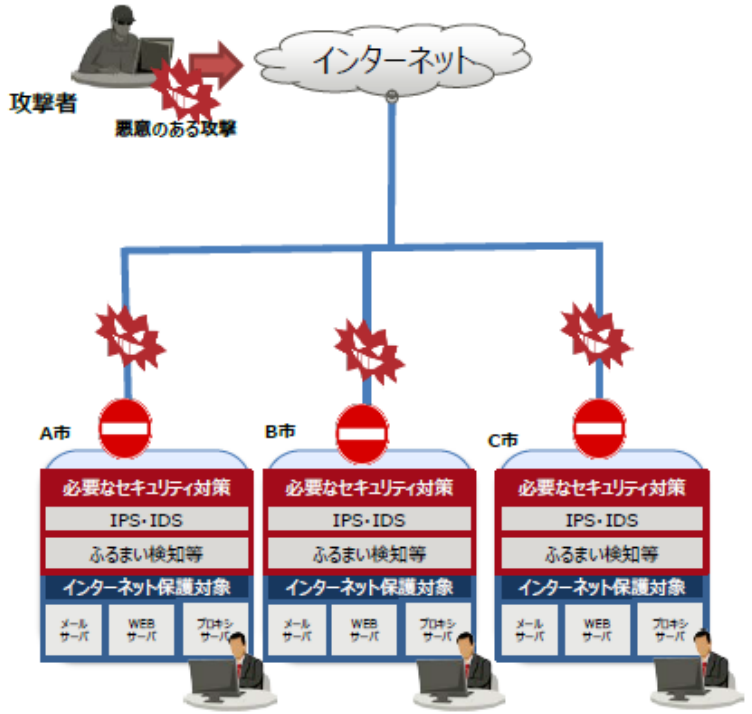
3. 各自治体の情報セキュリティ確保体制の強化

抜本的強化対策の概要


① 情報提供ネットワークシステム等の集中監視
（マイナンバー）
② マイナンバー関連システムを、インターネットリスクから分離
・既存住基（マイナンバー付番システム）の分離（H27.10.5）済
・LGWAN環境とインターネット環境の分割を図るとともに、個人番号利用事務を徹底分離（情報連携スタートを見据え早期に実施）
3層分離
（特定個人情報を提供）
LGWANを利用
（各種業務処理）
（個人番号利用事務系）
（ＬＧＷＡＮ接続系）
（インターネット接続系）
宛名
既存住基
税
社会保障
（分離の徹底）
人事給与
庶務事務
文書管理
等
（リスク分断）
無害化通信
情報収集
メール
ホームページ
・データの持出し不可設定
・二要素認証
・アクセス制御
・外部からの攻撃対策の徹底
③個人番号利用事務関連システムについて、端末からデータの持出し不可設定や二要素認証の導入により、住民情報の流出を徹底して防ぐ。
④ 全自治体で庁内ネットワークの再構成
⑤ インターネットとの接続口を都道府県ごとに集約化して、集中して高度な監視を行う。（自治体情報セキュリティクラウドの導入）
（自治体情報システム強靱性向上モデルの導入）
9

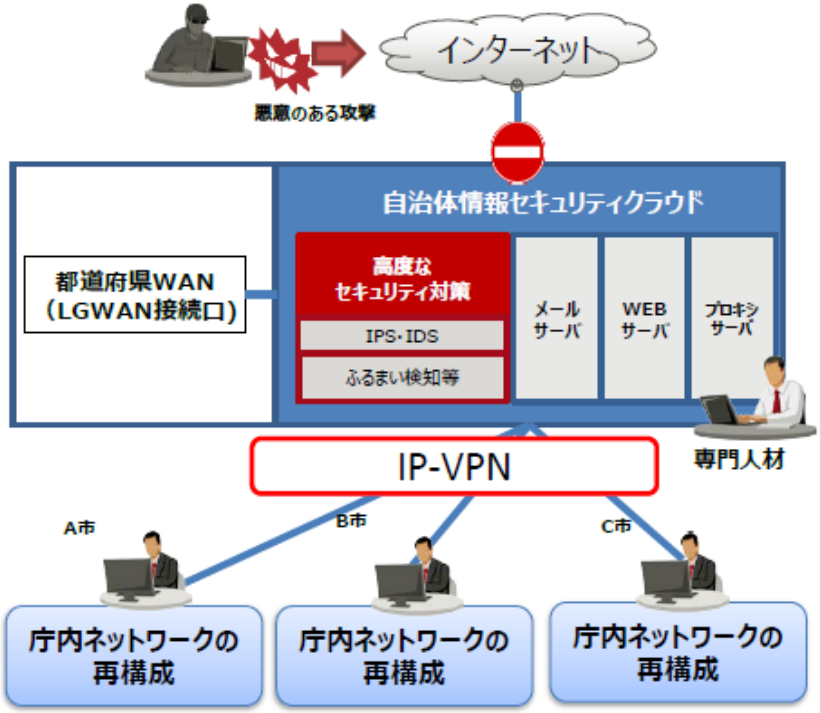
自治体情報セキュリティクラウド

導入前イメージ



【課題】
- 各自治体ごとに監視水準にバラツキ
- 不正接続など必要なセキュリティ対策におけるコストが甚大
- プロキシログ等の分析するスキルを持った職員の不足
- 個々の自治体のインシデント情報の共有化に時間を要する

導入後イメージ



【特色】
- 全国的に必要な監視水準を確保・維持
- サーバの共同利用によりコスト減
- セキュリティ専門人材によるプロキシログ等の分析
- 自治体システム側からLGWANへの不適切なアクセス等の監視
- 都道府県相互でインシデント情報の共有化が可能

高市総務大臣に報告書の手交

http://www.soumu.go.jp/photo_gallery/02koho03_03001281.html

目次

講演①

1. はじめに
2. 前回の自治体セキュリティガイドラインの改定の概要
3. 今回のガイドライン改定内容

講演②

4. 具体的対策の決定ためのリスクアセスメント
5. おわりに

ガイドライン改定の背景

「三層の対策」

2015年の年金機構の情報漏えい事案を受け、**短期間**で自治体の情報セキュリティ対策を抜本的に強化　＝「三層の対策」

⇒ **インシデント数の大幅な減少を実現**

一方で、

①ユーザビリティへの影響

- ✓ **自治体内の情報ネットワークの分離・分割による事務効率の低下**
  例：マイナンバー利用事務系のシステムへのデータの取込み、インターネットメールの添付ファイルの取得など

②新たな時代の要請

- ✓ **行政アプリケーションを自前調達方式からサービス利用式へ**
  （政府における「クラウド・バイ・デフォルト」原則）
- ✓ **行政手続を紙から電子へ**（デジタル手続法を受けた行政手続のオンライン化）
- ✓ **働き方改革**（テレワーク等のリモートアクセス）
- ✓ **サイバー攻撃の増加、サイバー犯罪における手口の巧妙化**　　**等**

⇨ 効率性・利便性を向上させたシステムの検討し、ガイドラインを改定

ガイドラインの改定等に係る検討会

2019年12月3日「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」スタート

これまでの議論の経過

地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会

■構成員

	石井夏生利	中央大学国際情報学部教授
	上原哲太郎	立命館大学情報理工学部教授
	岡村　久道	弁護士　京都大学大学院医学研究科講師
(座長)	佐々木良一	東京電機大学総合研究所特命教授
	庄司　昌彦	武蔵大学社会学部メディア社会学科教授
	長峯　道宏	千葉市総務局情報経営部業務改革推進課長（2020年４月から）
	塗師　敏男	横浜市総務局しごと改革室ICT担当部長
	半田　嘉正	富山県経営管理部情報政策課情報企画監
	三輪　信雄	総務省最高情報セキュリティアドバイザー
	若杉　健次	港区総務部情報政策課長（2020年４月まで）

■オブザーバ

総務省自治行政局住民制度課
総務省サイバーセキュリティ統括官室
地方公共団体情報システム機構

※敬称略、五十音順

https://www.soumu.go.jp/main_content/000688753.pdf

ガイドラインの主な改定内容

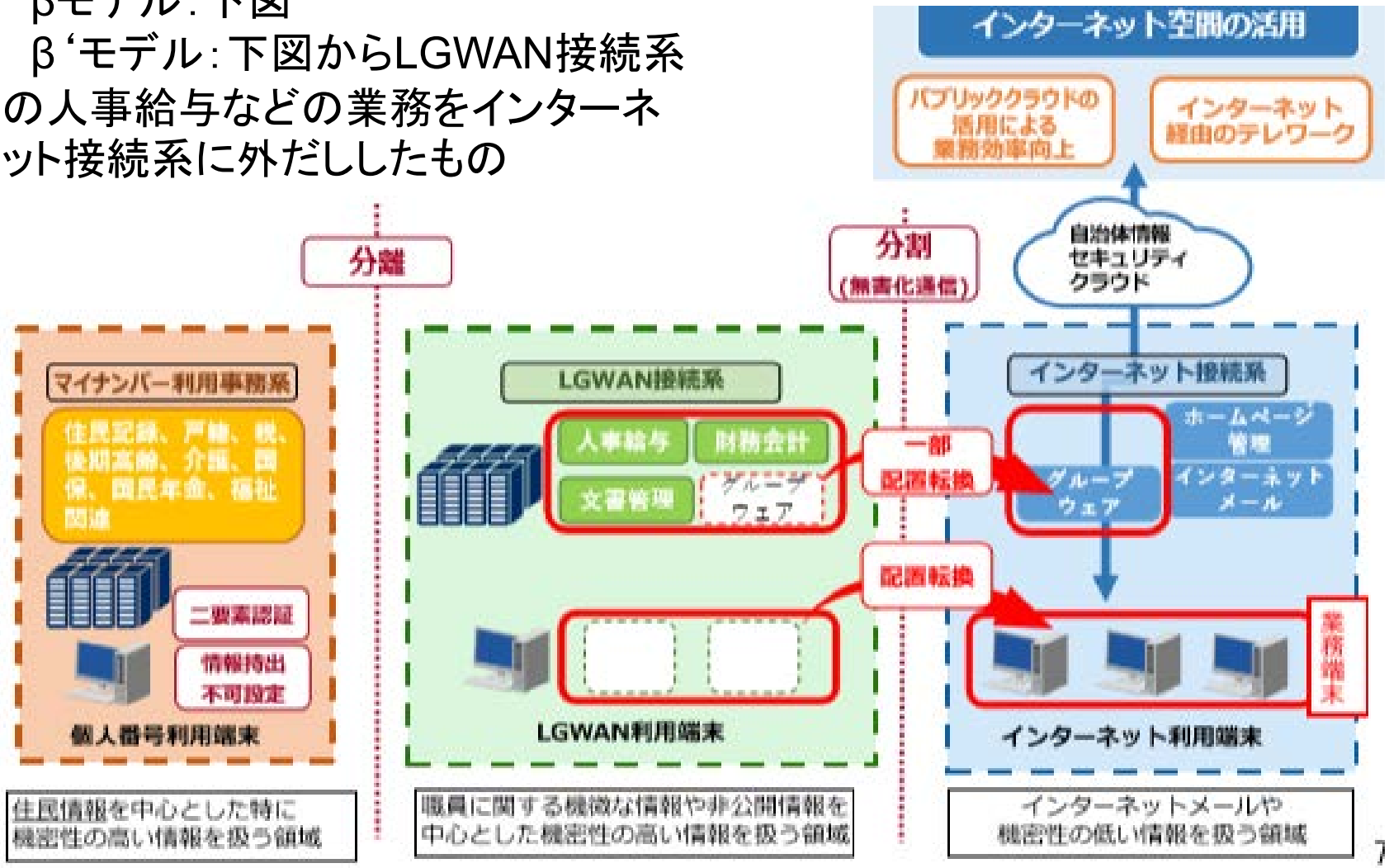
1. マイナンバー利用事務系の分離の見直し
2. LGWAN接続系とインターネット接続系の分割の見直し
3. リモートアクセスのセキュリティ
4. LGWAN接続系における庁内無線LANの利用
5. 情報資産及び機器の廃棄
6. クラウドサービスの利用
7. 研修、人材育成

対象モデル（α・β・β‘）の概要

αモデル：移動前　　https://www.soumu.go.jp/main_content/000688753.pdf

βモデル：下図

β‘モデル：下図からLGWAN接続系の人事給与などの業務をインターネット接続系に外だししたもの



サーバ機能の所属領域

	αモデル	βモデル	β'モデル
インターネットメール	○	○	○
ホームページ管理	○	○	○
LGWANメール	◎	◎	◎
人事給与	◎	◎	○
財務会計	◎	◎	○
文書管理	◎	◎	○
グループウエア	◎	○	○

○：インターネット接続系
◎：LGWAN接続系

詳しくは、「地方公共団体における情報セキュリティポリシーに関するガイドライン」
https://www.soumu.go.jp/main_content/000727474.pdf　参照

目次

講演①

1. はじめに
2. 前回の自治体セキュリティガイドラインの改定の概要
3. 今回のガイドライン改定内容

講演②

4. 具体的対策の決定ためのリスクアセスメント
5. おわりに

リスクとは

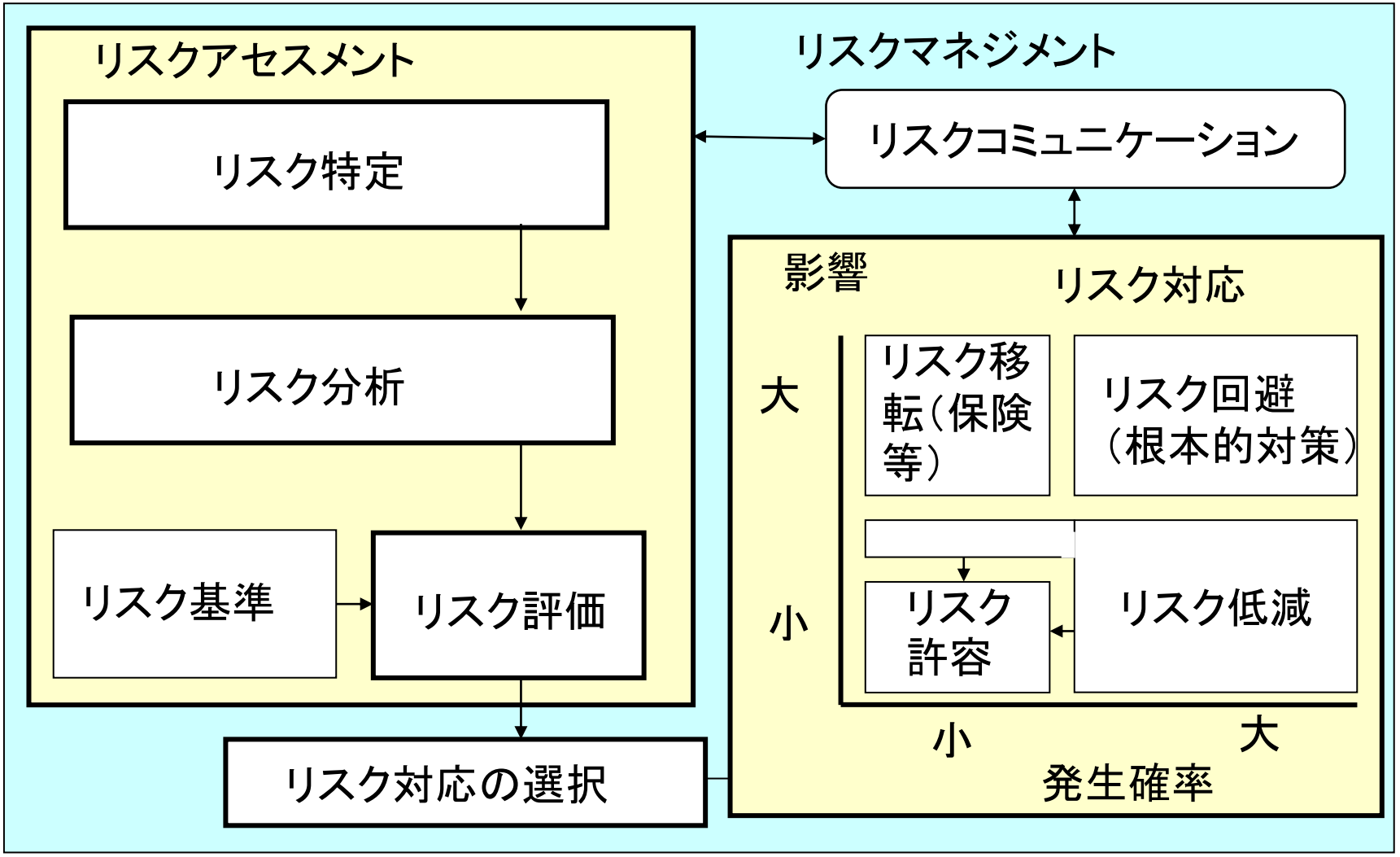
1．リスクとは，英語のRiskの訳であり，危険と訳される場合もある．「**将来の帰結に対する現在における予測**」という見方が下敷きになっていて常に**不確実性**を伴う。

2．工学分野の確率論的リスク評価では通常次のように定義することが多い。
　　リスク＝損害の大きさ　×損害の発生確率

3．「ISO/IEC 27005：2008」ではITのリスクを以下のように定義しているが、結局同じことを表している。
　　リスク＝資産価値 × 脅威 × 脆弱性

（注）英語のRiskが登場するのは1660年代。ハザードや災いを意味するイタリア語risicoからの転用

リスクマネジメントの要素と相互関連



＝＞　自分たちの組織の対策を決めるのにリスクアセスメントをしっかりと

リスク分析方法

(1)ベースラインアプローチ
既存の標準や基準をもとにベースライン（自組織の対策基準）を策定し、チェックしていく方法。
簡単にできる方法であるが、選択する標準や基準によっては求める対策のレベルが高すぎたり、低すぎたりする場合がある

(2)非形式的アプローチ
コンサルタント又は組織や担当者の経験、判断によりリスクアセスメントを行う。
　短時間に実施することが可能である属人的な判断に偏る恐れがある。

(3)詳細リスク分析
詳細なリスクアセスメントを実施。情報資産に対し「資産価値」「脅威」「脆弱性」「セキュリティ要件」を識別し、リスクを評価していく。
厳密なリスク評価が行えるものの多大な工数や費用がかかる

(4)組合せアプローチ
複数のアプローチの併用。よく用いられるのは、(1)ベースラインアプローチと(3)詳細リスク分析の組合せ。
ベースラインアプローチと詳細リスク分析の両方のメリットが享受できる。

https://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html

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
準定量的	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

NIST SP 800-30を参考に作成

ベースとなるリスク分析法

（1） 合意形成を容易にするために「準定量的アプローチ」を採用

（2）リスク分析と対策案のリストアップまで実施

（3） ①資産ベースリスク分析法と②事業被害ベースリスク分析法の両方を用意

https://www.ipa.go.jp/files/000069436.pdf

採用したリスク分析方法

（1）事業被害ベースリスク分析法を適用

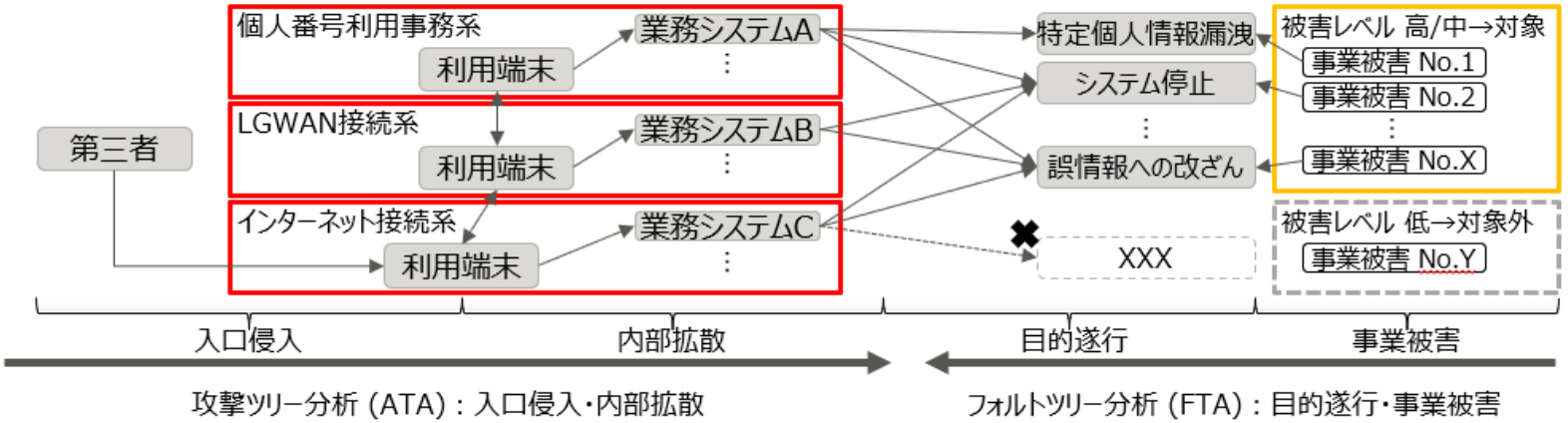
（2）評価指標
① 特定個人情報漏洩
② 個人情報漏洩
③ システム停止など

（3）αモデル、βモデル、β‘モデルに対し分析を実施

（4）リスク値の計算法
リスク値＝事業被害の大きさx脅威の発生頻度x脆弱性
＝＞5つのリスクレベルに分類

リスク分析法：事業被害ベース

- 攻撃ツリーを考慮し、「入口侵入」「内部拡散」「目的遂行」の３つの観点で脅威を洗い出し。
- 「入口侵入」の脅威によって洗い出された結果を「内部拡散」の発生源として、「内部拡散」の脅威を洗い出し。
- 同様に、「内部拡散」の脅威によって洗い出された結果をもとに「目的遂行」の脅威を洗い出し。
- 事業被害を想定を元に、「目的遂行」による被害につながる脅威シナリオを絞り込み。



入口侵入の観点での脅威の洗い出し例

No.	時間	場所	人＋理由	対象	手段	被害（入口侵入）
1	いつでも	メールから	悪意を持った第三者が	利用端末	マルウェアによって	C&Cサーバに接続される
2	夜間に	Webサイトから	悪意を持った第三者が	利用端末	遠隔操作によって	権限昇格される
…	…	…	…	…	…	…

採用したリスク分析方法

（1）事業被害ベースリスク分析を実施

（2）評価指標
① 特定個人情報漏洩
② 個人情報漏洩
③ システム停止など

（3）αモデル、βモデル、β‘モデルに対し分析を実施

（4）リスク値の計算法
リスク値＝事業被害の大きさx脅威の発生頻度x脆弱性
＝＞5つのリスクレベルに分類し、それぞれに属すシーケンス数を数え上げ

事業被害ベースの
リスク分析結果のイメージ

リスクレベル		該当する攻撃シーケンス数	
		A市 （α モデル）	B市 （β´ モデル＋EDRなど ）
レベル5	リスク大	0	0
レベル4		0	0
レベル3		0	0
レベル2		A2	B2
レベル1	リスク小	A1	B1

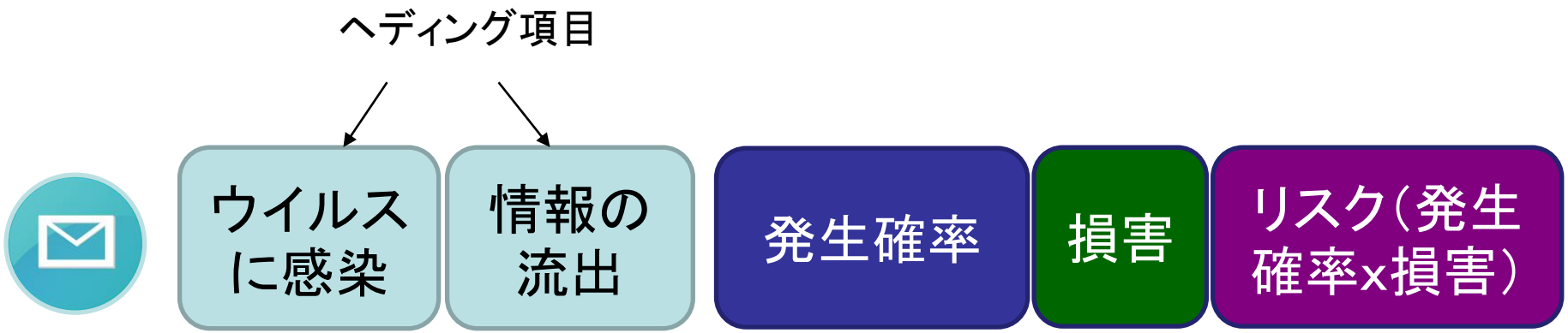
A1とB1に差がないあるいはB1の方が小さいことや、A2とB2に差がないあるいはB2の方が小さいことの表示 ＝＞β´＋EDRなどでもよいことを証明

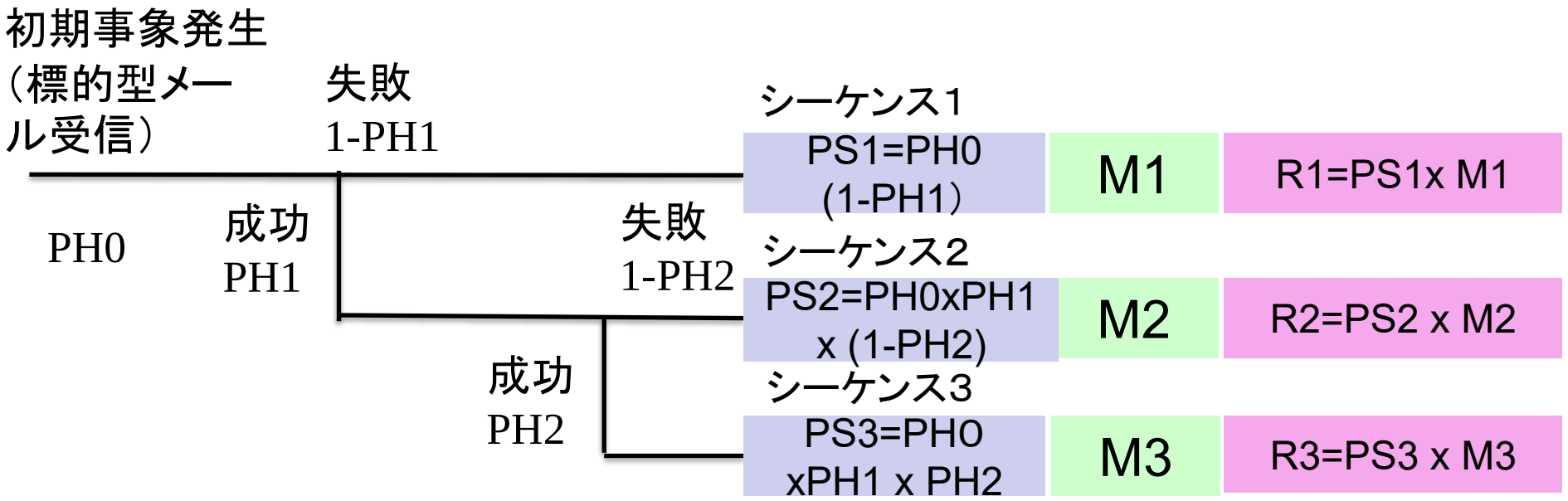
アセスメントアプローチ

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
準定量的	EDC法（Event Tree and Defense Tree Combined Method）の適用	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

NIST SP 800-30を参考に作成

イベントツリー分析





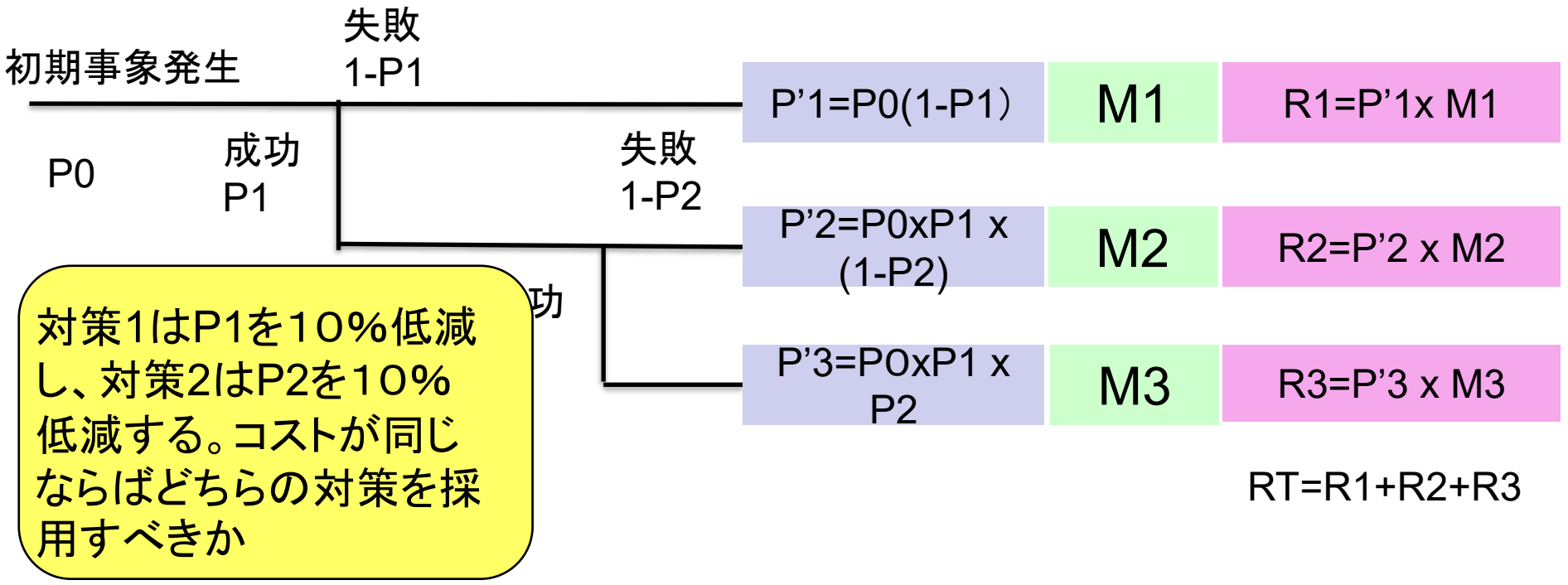
RT=R1+R2+R3

注1:成功、失敗は攻撃者側から見ての記述

イベントツリー分析

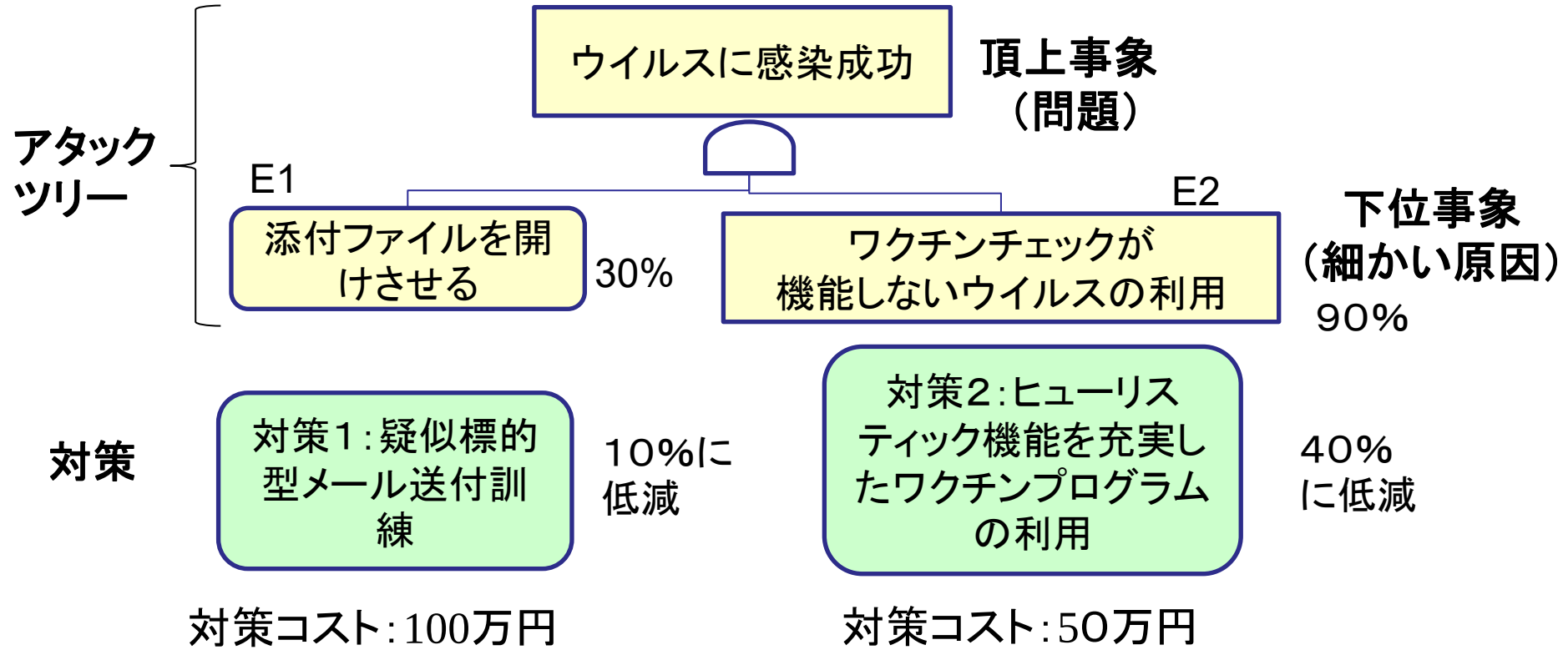
- 事象の発生から時系列順にどのような事象に発展するかを分析

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）



ディフェンスツリー分析

＜ディフェンスツリー＝アタックツリー＋対策＞



AND記号　OR記号

Xi=0　OR 1

PH1＝PE1＊PE2

PE1＝0.1＊X1＋0.3＊（1－X1）

PE2＝0.9＊X2＋0.4＊（1－X2）

組み合わせ最適化問題としての定式化方法

Minimize:

$$RT_{\square}(Xi : i = 1,2, - - -, n) \quad \ldots \quad (1)$$

Subject to

$$\sum_{i=1}^{n} C_i \times X_i \leqq Ct \quad \ldots \quad (2)$$

$$(X_i = 0, 1)$$

コスト制約下でリスクを
最小化する対策案を
求めるための定式化

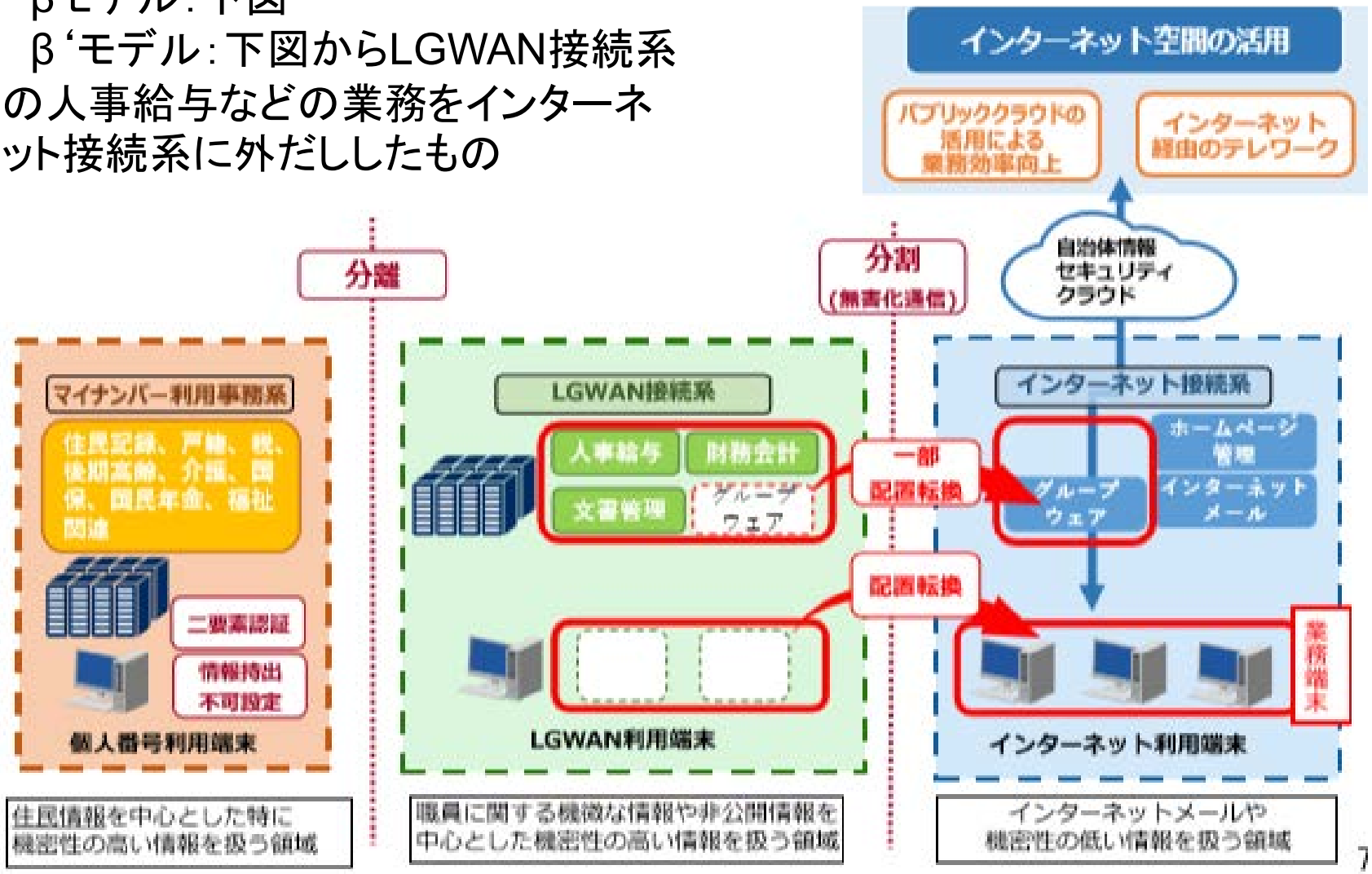
Ci:　i番目の対策案のコストXiは，0-1変数
Xi＝1ならi番目の対策案iを採用し，0ならば採用しない

RTは，イベントツリー分析で説明した式と，ディフェンス分析で説明した式を，「ヘッディング項目の発生確率」を介して組み合わせることで求めることができる．

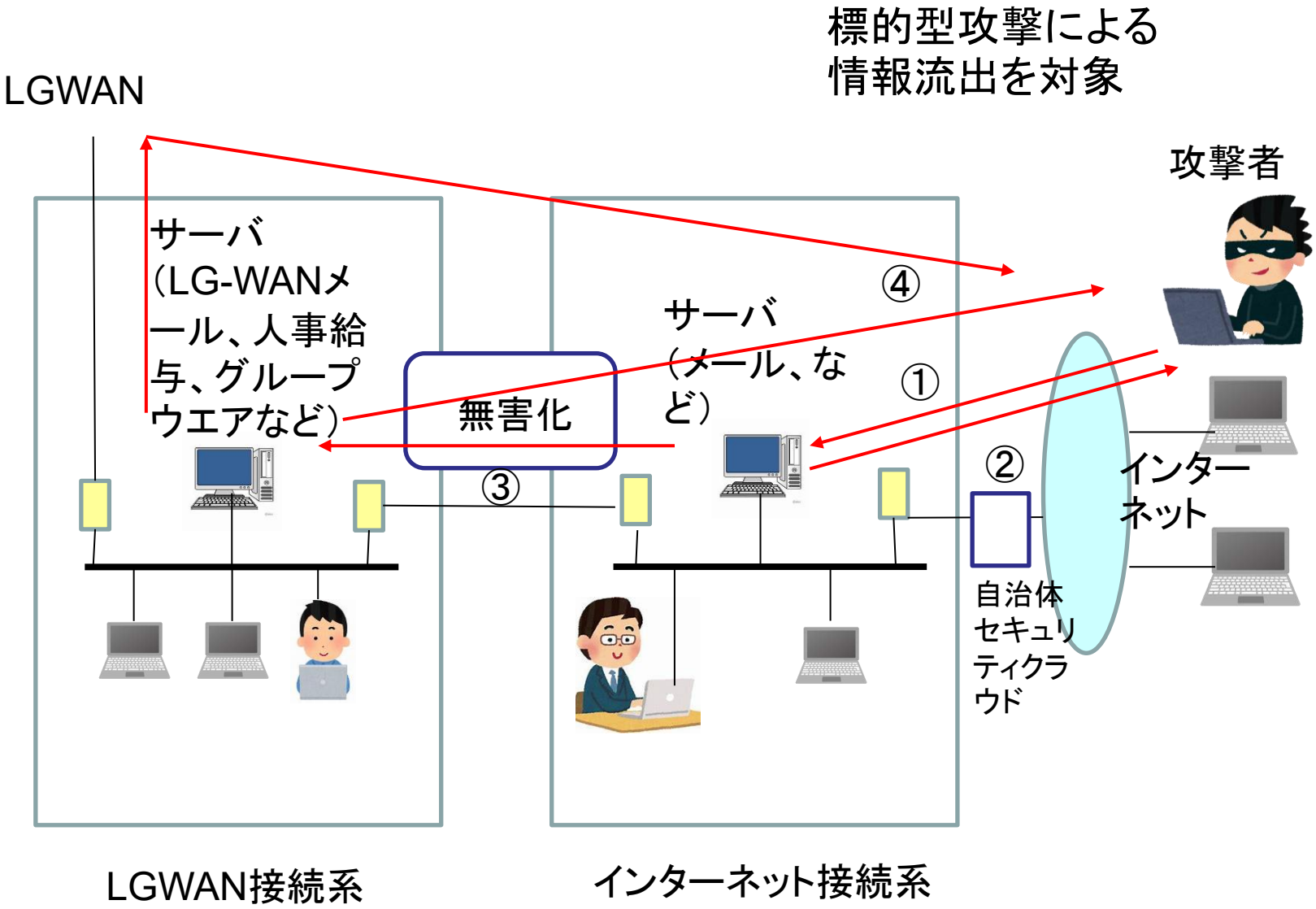
対象モデル（α・β・β‘）の概要

αモデル：移動前
βモデル：下図
β‘モデル：下図からLGWAN接続系の人事給与などの業務をインターネット接続系に外だししたもの

https://www.soumu.go.jp/main_content/000688753.pdf



攻撃方法（αモデルを対象）



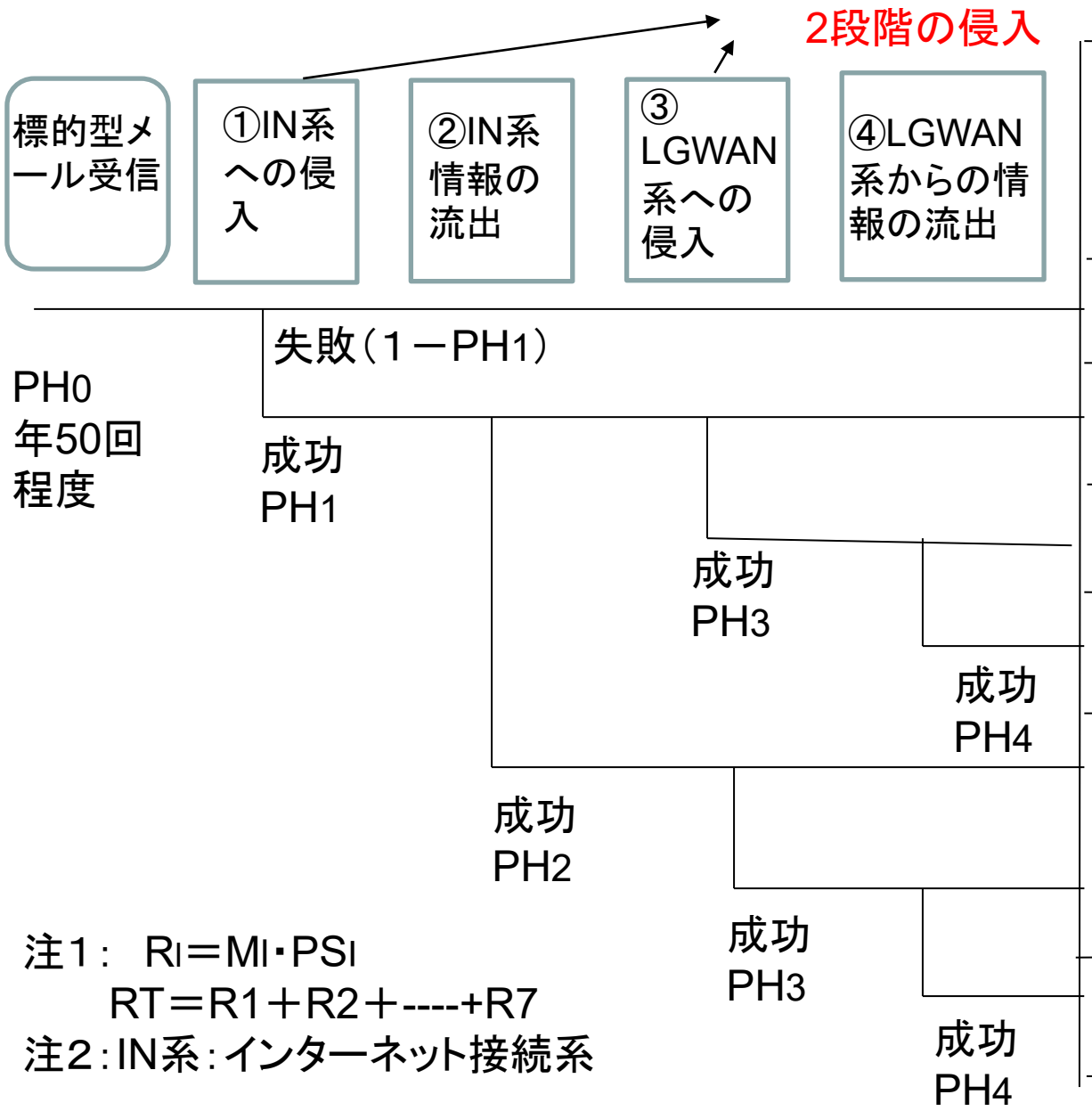
対象へのEDC法の適用上の問題と対策

問題①　侵入先が2か所あり，2段階の侵入を考慮したリスクアセスメントが必要．＝＞イベントツリーの構造に反映

問題②　従来の評価指標はコストとリスクだけに対応するものであった．ここではコストとリスク以外に作業負担度も考慮に入れる必要がある．＝＞定式化において制約条件に，作業負担度を追加する．

問題③　対象システムの構成原案が複数あり，それぞれをベースにした対策案の最適組み合わせを求めるとともに，それらの最適な組み合わせ間の比較も必要．＝＞同じ制約条件の下で複数の対策原案の最適解を求め，トータルリスクが小さいものを全体の最適解として採用

イベントツリーの構成



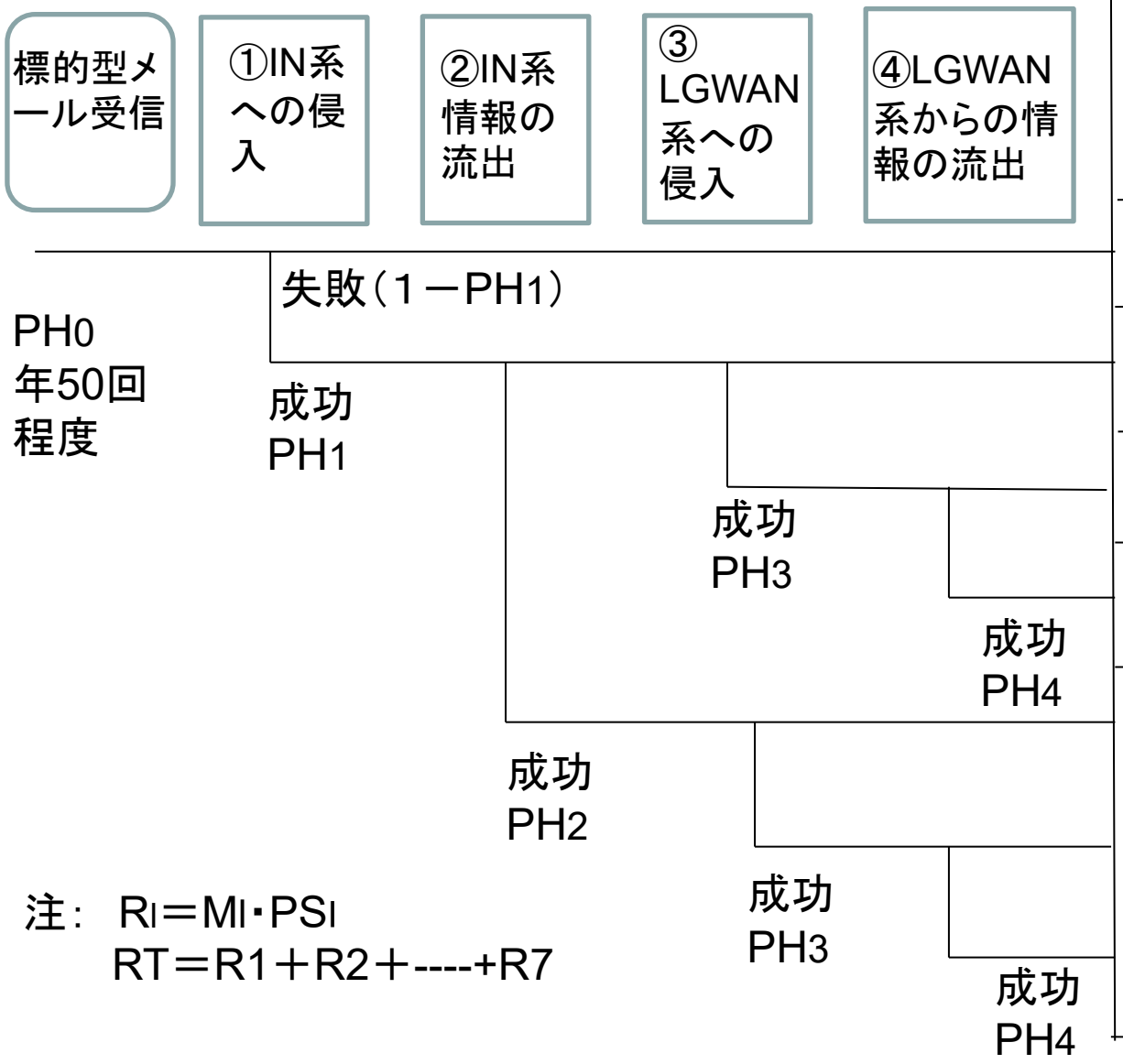
シーケンス	発生頻度	影響（円）	リスク(円)
①	PS1	M1	R1
②	PS2	M2	R2
③	PS3	M3	R3
④	PS4	M4	R4
⑤	PS5	M5	R5
⑥	PS6	M6	R6
⑦	PS7	M7	R7

注1：　$R_I = M_I \cdot PS_I$

$RT = R1 + R2 + \text{----} + R7$

注2：IN系：インターネット接続系

シーケンスごとの発生頻度計算法



シーケンス	PSI 頻度（回/年）	影響 円
①	PS1＝PH0（1－PH1）	M1
②	PS2＝PH0・PH1・(1-PH2)・(1-H3)	M2
③	PS3＝PH0・PH1・（1－PH2）PH3	M3
④	PS4＝PH0・PH1・（1－PH2）PH3・PH4	M4
⑤	PS5＝PH0・PH1・PH2・（1－PH3）	M5
⑥	PS6＝PH0・PH1・H2・PH3・（1-PH4）	M6
⑦	PS7＝PH0・PH1・H2・PH3・PH4	M7

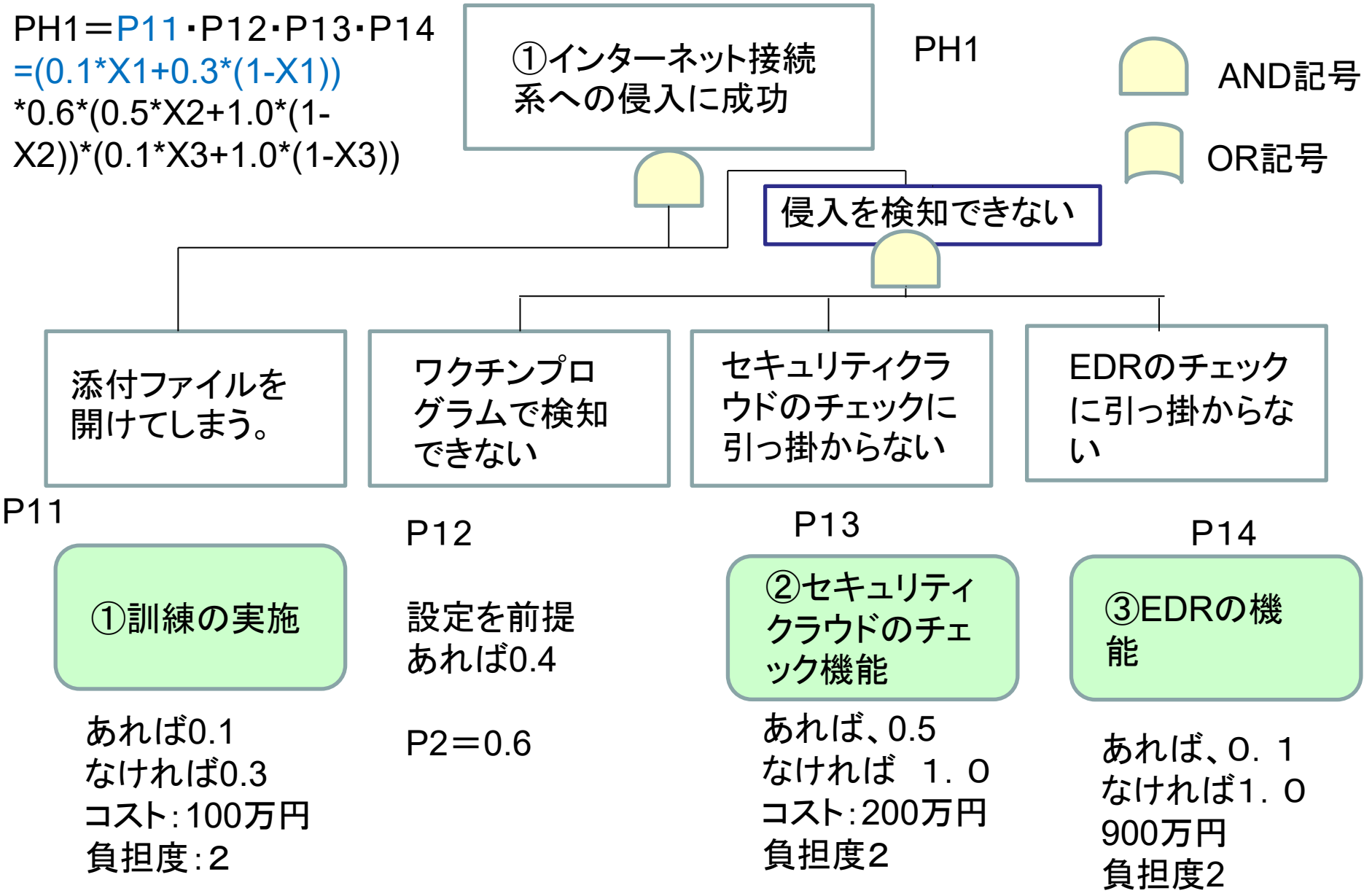
注：　RI＝MI・PSI
RT＝R1＋R2＋----+R7

シーケンスごとの損害額推定値

シーケンス		項目	影響の大きさ例		
			α	β	β´
①	M1	影響はない	0円	0円	0円
②	M2	インターネット接続系PC10台のフォレンジック費用（1台100万円）	1000万円	1000万円	1000万円
③	M3	インターネット接続系PC10台およびLGWAN接続系PC10台のフォレンジック費用（1台100万円）	2000万円	2000万円	2000万円
④	M4	LGWAN系情報漏洩による損害賠償: N種の情報・1000件 ・1万円/件 インシデント対応費・ 2000万円 レピュテーション・1000万円	N=5 8000万円	N=4 7000万円	N=1 4000万円
⑤	M5	インターネット系情報漏洩による損害賠償・N種の情報・M件1000件 ・1万円/件 インシデント対応費 2000万円 レピュテーション 1000万円	N=2 5000万円	N=3 6000万円	N=6 9000万円
⑥	M6	インターネット系情報漏洩による損害賠償・N種の情報1種あたり1000万円 インシデント対応費・2000万円 レピュテーション 1000万円 LGWAN系侵入による災害対策費 2000万円	N=2 7000万円	N=3 8000万円	N=6 1値億円
⑦	M7	インターネット系・LGWAN系情報漏洩による損害賠償・賠償額 7000万円 インシデント対応費・4000万円 レピュテーション 2000万円	1億3千円	1億3千円	1億3千円

H1向けディフェンスツリーの一例

PH1＝P11・P12・P13・P14
=(0.1*X1+0.3*(1-X1))
0.6(0.5*X2+1.0*(1-
X2))*(0.1*X3+1.0*(1-X3))



作業負担度

レベル５　負担が非常に大きい
（例：一日あたり1時間以上）
レベル４　負担が大きい
（例：一日あたり1時間以内）
レベル３　負担がかかる
（例：一日あたり１０分以内）
レベル２　負担がやや大きい
（例：一日あたり5分以内）
レベル１　負担はほとんどない
（例：一日あたり1分以内）

対策案とパラメター値の推定値

対策案	名称	確率		コスト（円）	作業負担度レベル
		対策なし	対策あり		
①	メール処理訓練	0.3	0.1	100万円	2
②	セキュリティクラウドでのチェック	1.0	0.5	200万円	2
③	EDRでのチェック機能	1.0	0.1	α：600万円 β‘：900万円	2
④	メールの無害化機能	0.99	0.1	α: 625万円 β‘：250万円	α：4 β´：3
⑤	ファイルの無害化機能　DVI	0.99	0.1	4800万円	3
⑥	ファイルの無害化機能 仮想ブラウザー	0.99	0.3	600万円	3
⑦	LG-WANからの流出 チェック機能	0.3	0.1	500万円	2

対象への適用上の問題と対策

問題①　侵入先が2か所あり，2段階の侵入を考慮したリスクアセスメントが必要．＝＞イベントツリーの構造に反映

問題②　従来の評価指標はコストとリスクだけに対応するものであった．ここではコストとリスク以外に作業負担度も考慮に入れる必要がある．＝＞定式化において制約条件に，作業負担度を追加する．

問題③　対象システムの構成原案が複数あり，それぞれをベースにした対策案の最適組み合わせを求めるとともに，それらの最適な組み合わせ間の比較も必要．＝＞同じ制約条件の下で複数の対策原案の最適解を求め，トータルリスクが小さいものを全体の最適解として採用

αモデルの定式化

$$\mathrm{Min}\quad R\alpha\ (x_i \mid i=1,2,\text{--},n)$$

$$\text{subject to}\quad \sum_{i=1}^{n} C\alpha_i \cdot x_i \leqq Ct$$

$$\sum_{i=1}^{n} B\alpha_i \cdot x_i / n \leqq Bt$$

コストと職員の負担度の制約の下で、リスクを最小化する対策案の組み合わせを求める式

Rα():トータルリスクを求める関数
Xi＝1　対策案iを採用
　＝0　対策案iを不採用
Cαi:αモデルで対策案iを実現するコスト(円)
Ct:対策案に関する制約(円)

Bαi:対策案iを導入するαモデルにおける負担度
Bt:負担度の平均に関する制約

適用結果

（1）対策コストや作業負担度の制約のもとにトータルリスクを最小化する対策案の最適な組み合わせを知ることができた.

（2）同じ制約条件でαモデル，β’モデルの最適解におけるトータルコストを比べることによりその小さいほうを全体の最適解として求めることができる.
例えば，コスト制約2000万円で，作業負担度2.0の場合の最適解は，αモデルでトータルリスクが507万円，β’モデルが442万円でトータルリスクが小さいβ’モデルの方が全体の最適解になっている

（3）トータルコスト＋トータルリスクに着目すると，トータルコスト＋トータルリスクが最小となるのはαモデルを対象とするものであり，1000万円以下をコスト制約とする場合である.
その際の最適な対策案の組み合わせは対策案①②③の組み合わせであり，トータルコスト＋トータルリスクは1634万円となる.

最適化計算結果1 （αモデル）

	コスト制約	負担度制約	対策案							トータルコスト（円）	トータルリスク（円）	トータルコスト＋トータルリスク(円)
			①	②	③	④	⑤	⑥	⑦			
①	500万円	5.0	○	○						300万円	1億5357万円	1億5657万円
②	1000万円	5.0	○	○	○					900万円	734万円	1634円
③	1250万円	5.0	○	○	○					900万円	734万円	1634円
④	1500万円	5.0	○	○	○				○	1400万円	509万円	1909万円
⑤	2000万円	5.0	○	○	○			○	○	2000万円	507万円	2507万円
⑥	3000万円	5.0	○	○	○	○		○	○	2525万円	301万円	2708万円
⑦	4000万円	5.0	○	○	○	○		○	○	2625万円	301万円	2926万円

コスト制約を色々変えてみた

最適化計算結果2（αモデル）

	コスト制約	負担度制約	対策案							トータルコスト（円）	トータルリスク（円）	トータルコスト＋トータルリスク(円)
			①	②	③	④	⑤	⑥	⑦			
①	2000万円	5.0	○	○	○			○	○	1525万円	507万円	2032万円
②	2000万円	2.5	○	○	○			○	○	1525万円	507万円	2032万円
③	2000万円	2.0	○	○	○			○	○	1525万円	507万円	2032万円
④	2000万円	1.5	○	○	○				○	1400万円	509万円	1909万円
⑤	2000万円	1.0	○	○	○					900万円	734万円	1634万円
⑥	2000万円	0.75	○		○					700万円	1616万円	2316万円
⑦	2000万円	0.5			○					600万円	4847万円	5447万円

負担度制約を色々変えてみた

最適化計算結果2（αモデル）

	コスト制約	負担度制約	対策案							トータルコスト（円）	トータルリスク（円）	トータルコスト＋トータルリスク(円)
			①	②	③	④	⑤	⑥	⑦			
①	2000万円	5.0	○	○	○			○	○	1525万円	507万円	2032万円
②	2000万円	2.5	○	○	○			○	○	1525万円		
③	2000万円	2.0	○	○	○			○	○	1525万円		
④	2000万円	1.5	○	○	○				○	1400万円		
⑤	2000万円	1.0	○	○	○					900万円		
⑥	2000万円	0.75	○		○					700万円	1616万円	2316万円
⑦	2000万円	0.5			○					600万円	4847万円	5447万円

④ メールの無害化機能
⑤ ファイルの無害化機能 DVI
⑥ ファイルの無害化機能 仮想ブラウザー
⑦ LG-WANからの流出チェック機能

負担度制約が強くなると対策案④⑤⑥⑦は採用されない方向にある

最適化計算結果３（β´モデル）

	コスト制約	負担度制約	対策案							トータルコスト（円）	トータルリスク（円）	トータルコスト＋トータルリスク(円)
			①	②	③	④	⑤	⑥	⑦			
①	500万円	5.0	○	○						300万円	1億2412万円	1億2712万円
②	1000万円	5.0	○		○					1000万円	１２７３万円	２２７３万円
③	1250万円	5.0	○	○	○					1200万円	558万円	１７５８万円
④	1500万円	5.0	○	○	○	○				1450万円	552万円	2002万円
⑤	2000万円	5.0	○	○	○	○			○	1950万円	442万円	2392万円
⑦	3000万円	5.0	○	○	○	○		○	○	2550万円	297万円	2847万円
⑧	4000万円	5.0	○	○	○	○		○	○	2550万円	297万円	2847万円

最適化計算結果4（β´モデル）

	コスト制約	負担度制約	対策案							トータルコスト（円）	トータルリスク（円）	トータルコスト＋トータルリスク(円)
			①	②	③	④	⑤	⑥	⑦			
①	2000万円	5.0	○	○	○	○			○	1950万円	442万円	2392万円
②	2000万円	3.0	○	○	○	○			○	1950万円	442万円	2392万円
③	2000万円	2.0	○	○	○	○			○	1950万円	442万円	2392万円
④	2000万円	1.5	○	○	○				○	1700万円	446万円	2146万円
⑤	2000万円	1.0	○	○	○					1200万円	558万円	1758万円
⑥	2000万円	0.75	○		○					1000万円	1273万円	2273万円
⑦	2000万円	0.5			○					900万円	3818万円	4718万円

対象への適用上の問題と対策

問題①　侵入先が2か所あり，2段階の侵入を考慮したリスクアセスメントが必要．＝＞イベントツリーの構造に反映

問題②　従来の評価指標はコストとリスクだけに対応するものであった．ここではコストとリスク以外に作業負担度も考慮に入れる必要がある．＝＞定式化において制約条件に，作業負担度を追加する．

問題③　対象システムの構成原案が複数あり，それぞれをベースにした対策案の最適組み合わせを求めるとともに，それらの最適な組み合わせ間の比較も必要．＝＞同じ制約条件の下で複数の対策原案の最適解を求め，トータルリスクが小さいものを全体の最適解として採用

適用結果

（1）対策コストや作業負担度の制約のもとにトータルリスクを最小化する対策案の最適な組み合わせを知ることができた.

（2）同じ制約条件でαモデル，β’モデルの最適解におけるトータルコストを比べることによりその小さいほうを全体の最適解として求めることができる.
例えば，コスト制約2000万円で，作業負担度2.0の場合の最適解は，αモデルでトータルリスクが507万円，β’モデルが442万円でトータルリスクが小さいβ’モデルの方が全体の最適解になっている

（3）トータルコスト＋トータルリスクに着目すると，トータルコスト＋トータルリスクが最小となるのはαモデルを対象とするものであり，1000万円以下をコスト制約とする場合である.
その際の最適な対策案の組み合わせは対策案①②③の組み合わせであり，トータルコスト＋トータルリスクは1634万円となる.

最適化計算結果4（β´モデル）

αモデル

	コスト制約	負担度制約	対策案 ①	②	③	④	⑤	⑥	⑦	トータルコスト（円）	トータルリスク（円）	トータルコスト＋トータルリスク(円)
①	2000万円	5.0	○	○	○	○			○	1950万円	442万円	2392万円
③	2000万円	2.0	○	○	○			○	○	1525万円	507万円	2032万円
③	2000万円	2.0	○	○	○	○			○	1950万円	442万円	2392万円
④	2000万円											
⑤	200万円											
⑥	200万円											
⑦	200万円											

β´モデル

コスト制約2000万円以下で、負担度制約2以下の場合にリスクを最小にするのは、β´モデルによるもので、その場合の組み合わせは以下の通り

① メール処理訓練
② セキュリティクラウドでのチェック
③ EDRでのチェック機能
④ メールの無害化機能
⑦ LG-WANからの流出チェック機能

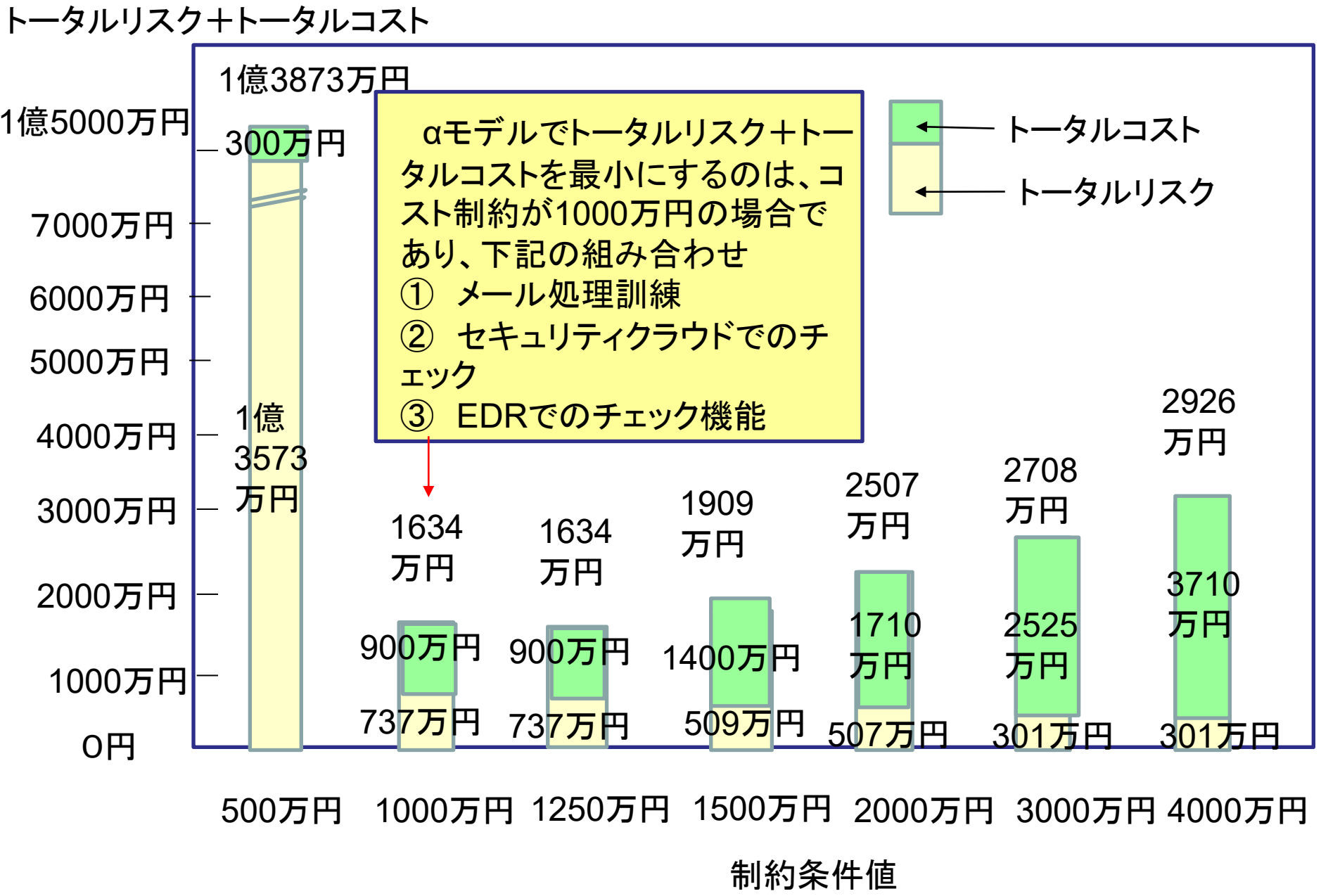
適用結果

（1）対策コストや作業負担度の制約のもとにトータルリスクを最小化する対策案の最適な組み合わせを知ることができた.

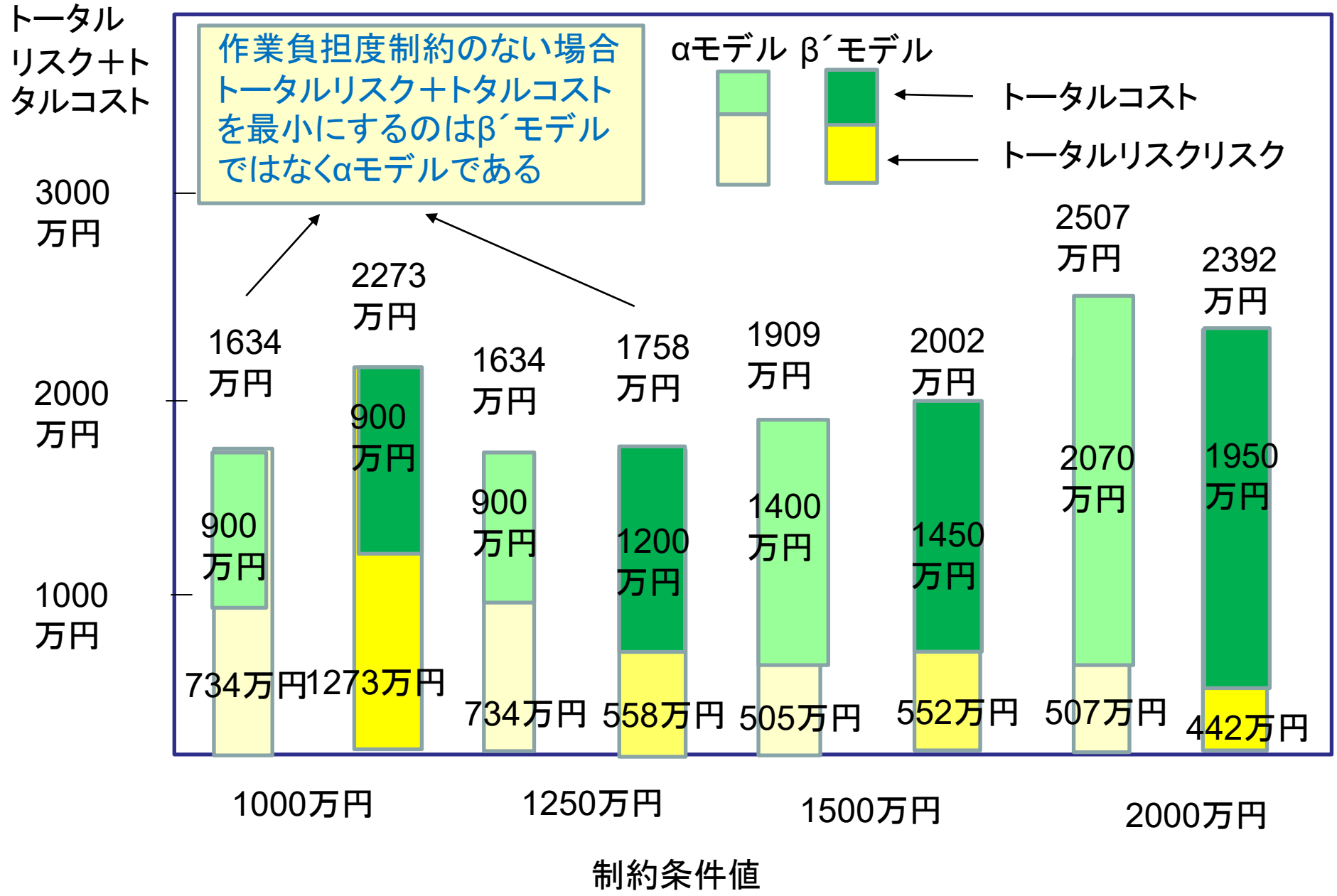
（2）同じ制約条件でαモデル，β’モデルの最適解におけるトータルコストを比べることによりその小さいほうを全体の最適解として求めることができる.
例えば，コスト制約2000万円で，作業負担度2.0の場合の最適解は，αモデルでトータルリスクが507万円，β’モデルが442万円でトータルリスクが小さいβ’モデルの方が全体の最適解になっている

（3）トータルコスト＋トータルリスクに着目すると，トータルコスト＋トータルリスクが最小となるのはαモデルを対象とするものであり，1000万円以下をコスト制約とする場合である.
その際の最適な対策案の組み合わせは対策案①②③の組み合わせであり，トータルコスト＋トータルリスクは1634万円となる.

制約条件別最適値の比較（αモデル）



制約条件別最適値の比較（αモデルとβ´モデル）



目次

講演①

1. はじめに
2. 前回の自治体セキュリティガイドラインの改定の概要
3. 今回のガイドライン改定内容

講演②

4. 具体的対策の決定ためのリスクアセスメント
5. おわりに

リスクアセスメントを実施して

① 講演者らが開発したEDC法は、自治体のセキュリティモデルのリスクアセスメントにも適用が可能であることを確認。

② 種々の条件下で、自治体の各種セキュリティモデル（αモデル、β´モデルなど）における、最適なセキュリティ対策を示すとともに、全体として最適なセキュリティ対策を示すことができた。

自治体における分析の利用法

サイバー攻撃がますます巧妙になる中で

① 地方公共団体において、「地方公共団体における 情報セキュリティポリシーに関する ガイドライン」をベースに、システムを構築する場合

このガイドに基づき、チェックリストを作成し、ガイドに沿った対策が十分かを確認する。

② 地方自治体が、コストや使い勝手を考慮して、ガイドにないことや詳細に記述されていないシステム構成にしたい場合

リスク分析を、地方自治体あるいはその被依頼者が、実施することが望まれる。


END

質疑応答案

① -最近の侵害を実例を挙げて解説してください →用意いただいているPPTでお答えいただく。

② -βモデルにおいてEDRは以下のどのレベルでの導入が求められるのでしょうか。（自治体さんから実際に頂いた質問）

- ①インシデント発生時に必要な調査・分析を行うレベル
- ②端末を常時監視し、あらゆるセキュリティリスクの可能性を事前に把握するレベル
- ③その他
- ※②の場合は業者選定など運用面・費用面でハードルが高いという印象を持っております。
- →回答の準備をお願いします。（口頭で構いません。もし必要あればPPT等お使いください。）

③ -新ガイドラインについて詳しくお願いします。（自治体さんから実際に頂いた質問） →こちらはセッション中に触れられる内容なので、簡単にポイントをお話いただければ良いかと思います。

- -その他セミナー中にチャットで質問があれば、事前に確認して回答することも考えています。（多くて1~2質問）

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化
   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化
   PCなどからIoTなどへ
4. 愉快犯から経済犯・組織犯へ
   犯罪組織の高度化

仮想通貨580億円相当不正流出

国内仮想通貨取引所を運営する「コインチェック」は26日、同社の取引所から約580億円相当の仮想通貨が不正に流出したと発表した。

同社は、取り扱うすべての仮想通貨の出金を一時停止した。外部から不正アクセスの形跡があり、サイバー攻撃の可能性がある。金融庁と警視庁に報告した。

不正流出したのは、仮想通貨の「ネム」で、同取引所が預かっていた全額が流出した。

https://mainichi.jp/articles/20180127/k00/00m/040/260000c

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化

   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化

   PCなどからIoTなどへ
4. 愉快犯から経済犯・組織犯へ

   犯罪組織の高度化

WannaCryの日本語版出力画面

ビットコインの支払いを要求する画面

⇨ データを暗号化して変更するという意味では、完全性の喪失、使えなくするという意味では可用性の喪失

https://www.npa.go.jp/news/release/2017/170518ransomware.pdf

ランサムウェアの被害を防ぐために必須の対策

（1） こまめにバックアップする

（2） OSやソフトの脆弱性を修正する

（3） メールのリンクや添付ファイルを安易に開かない

（4） セキュリティソフトを最新の状態で利用する

https://www.is702.jp/special/2160/ 2017/06/22 トレンドマイクロ

ランサムウエアへの対応法

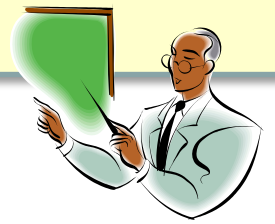
1．バックアップやクラウドストレージから戻す方法（正規の方法）

2．ボリュームシャドウコピーで復元させる方法（これも可能）

3．削除ファイルの復元ツールを使う方法

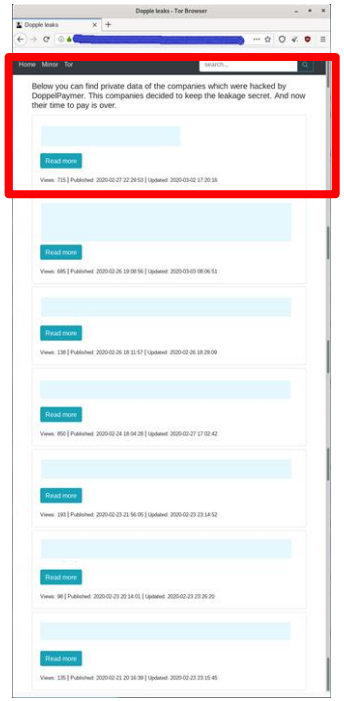
平文を暗号化した後、平文フアイルを単純消去するだけなら復元ツールで復元可能（単純消去だけの可能性は低い）

4．メモリー上のデータのダンプをとることによる暗号かぎの取り出し（可能性は低い）



最近のランサムウエア　Dopple Leaks（二重脅威型ランサムウエア）

Doppelpaymer Ransomwareの身代金を支払わなかった被害者の情報を公開するために立ち上げた専用WEBサイト（現在β版）

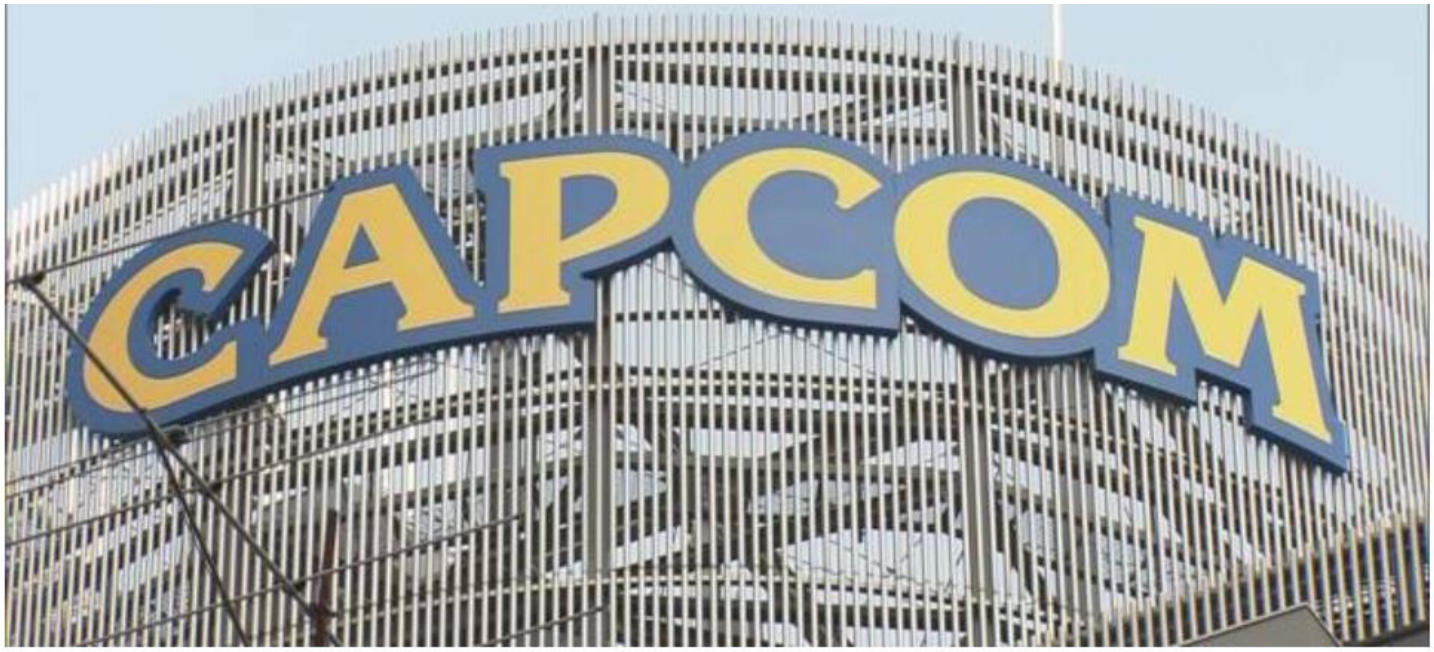


Dopple Leaks“サイト
(3/6現在)

DoppelPaymer Ransomwareで盗み出した情報を公開することで、身代金支払いを促す効果がある
3月8日までに9社の一部データが公開されている

類似のものに「Maze」がある。

ランサムウエアの被害



カプコン サイバー攻撃 金銭要求の「ランサムウェア」

2020年11月12日 18時19分　IT・ネット

1100万ドル（11億円ほど）の身代金を支払うように要求

https://www3.nhk.or.jp/news/html/20201112/k10012708311000.html

米石油パイプライン企業へのサイバー攻撃

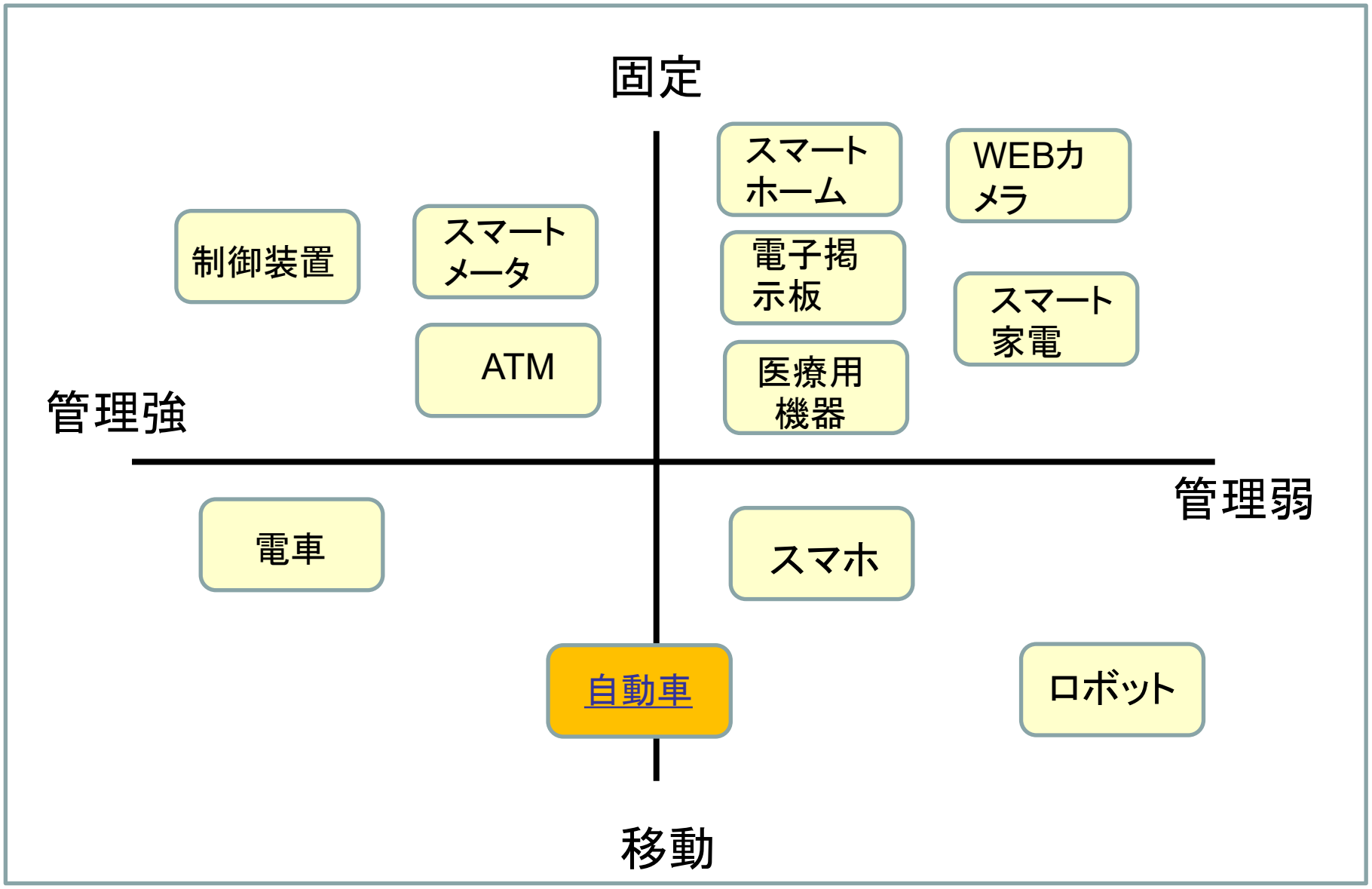
- 2021年5月7日、米国の石油パイプライン企業Colonial Pipelineはランサムウエアによる影響をうけ業務全体を一時停止する措置を講じたことを発表。
- 攻撃者はロシアの犯罪グループDarkSide。使用されたランサムウエアの名でもある。
- 「ダークサイド」が活動停止を表明していることが14日わかった。米メディアが報じた。ダークサイドのサーバーが何者かに乗っ取られ暗号資産（仮想通貨）が盗まれたとの情報もあり。

https://piyolog.hatenadiary.jp/entry/2021/05/12/051650
https://www.nikkei.com/article/DGXZQOGN14F4F0U1A510C2000000/?fbclid=IwAR1nIVI1hwR5eUVaplQgodY8kSLTZMOYm5zRWlFOdPp3fIT971tZwg7RHTI

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化
   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化
   PCなどからIoTなどへ
4. 愉快犯から経済犯・組織犯へ
   犯罪組織の高度化

主要なIoT機器


固定
スマート
ホーム
WEBカ
メラ
制御装置
スマート
メータ
電子掲
示板
スマート
家電
ATM
医療用
機器
管理強
管理弱
電車
スマホ
自動車
ロボット
移動

自動車への具体的攻撃例

- Blackhat2015でCharlie Miller氏とChris Valasek氏がジープのチェロスキーの遠隔操作法を発表

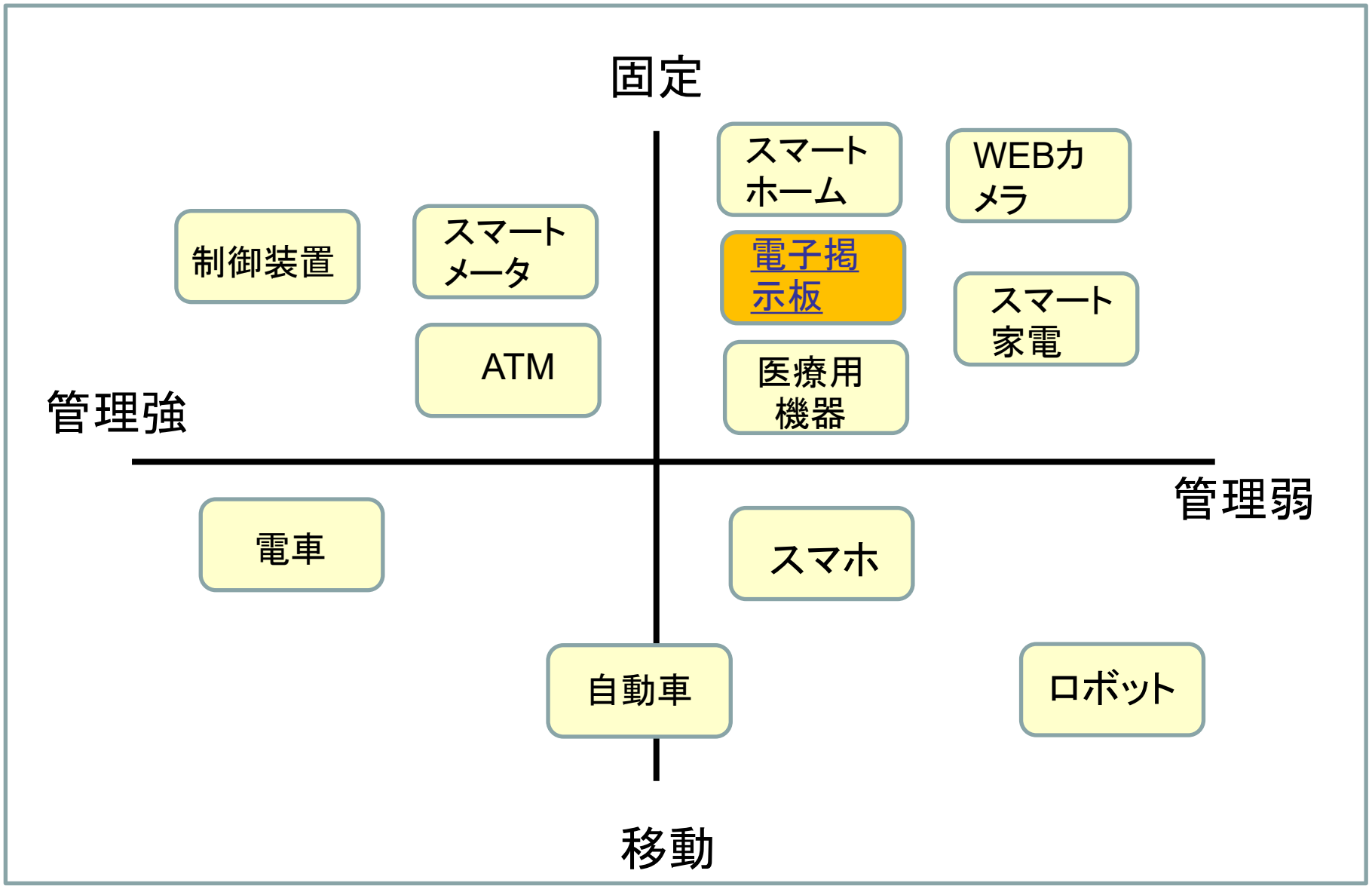
攻撃者は数マイル離れた自宅から

ハンドル操作
ブレーキの無効化
高速走行中のエンジンの停止など

140万台のリコールに

https://blog.kaspersky.co.jp/blackhat-jeep-cherokee-hack-explained/8480/

主要なIoT機器


固定
スマート
ホーム
WEBカ
メラ
制御装置
スマート
メータ
電子掲
示板
スマート
家電
ATM
医療用
機器
管理強
管理弱
電車
スマホ
自動車
ロボット
移動

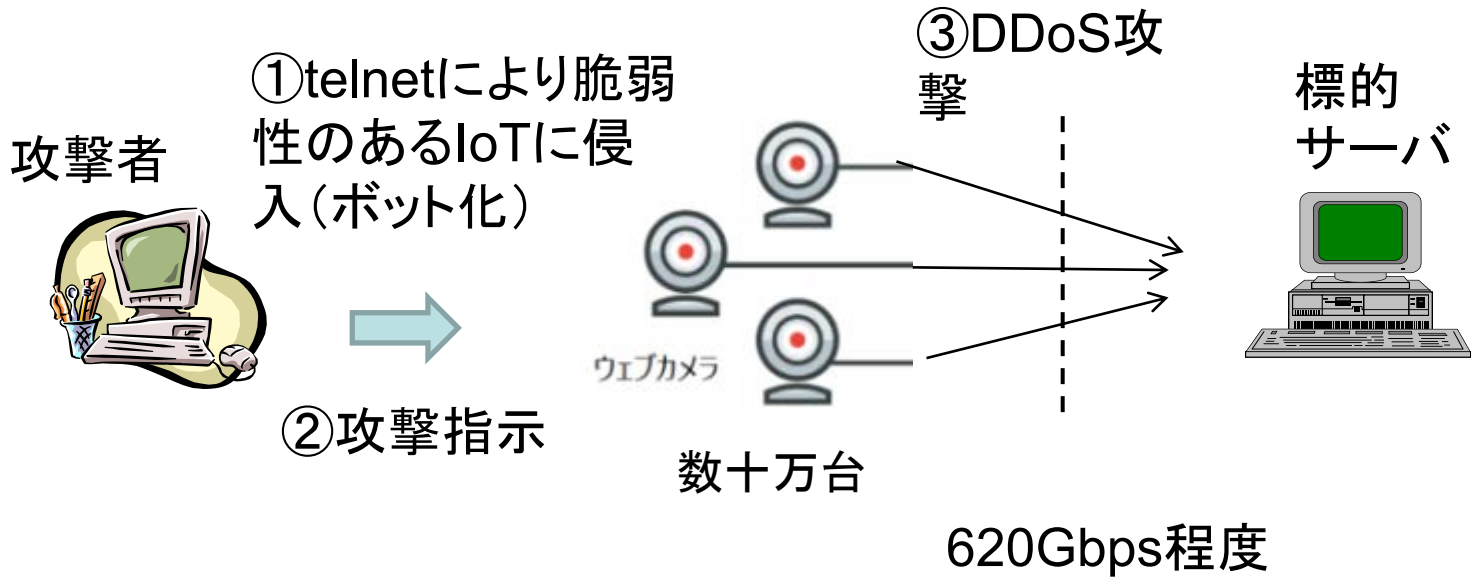
交通標識が「ゴジラ来襲」と警告

その他のIoTのセキュリティ

- WEBカメラ、家庭用ルータなどのIoTが攻撃の踏み台に
- 今後は家庭用ロボットなどのハッキングによる被害なども発生か

IoTを利用したDDoS攻撃

＜MiraiによるDDoS攻撃：2017年＞



DDoS（Dissributed Denial Of Service）攻撃（サービス不能攻撃ともいう）

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化
   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化
   PCなどからIoTなどへ
4. 愉快犯から経済犯・組織犯へ
   犯罪組織の高度化

Verizon2018年データ漏洩・侵害調査報告書

サイバー攻撃の目的

金銭入手：　攻撃の70%強

スパイ活動：20%弱

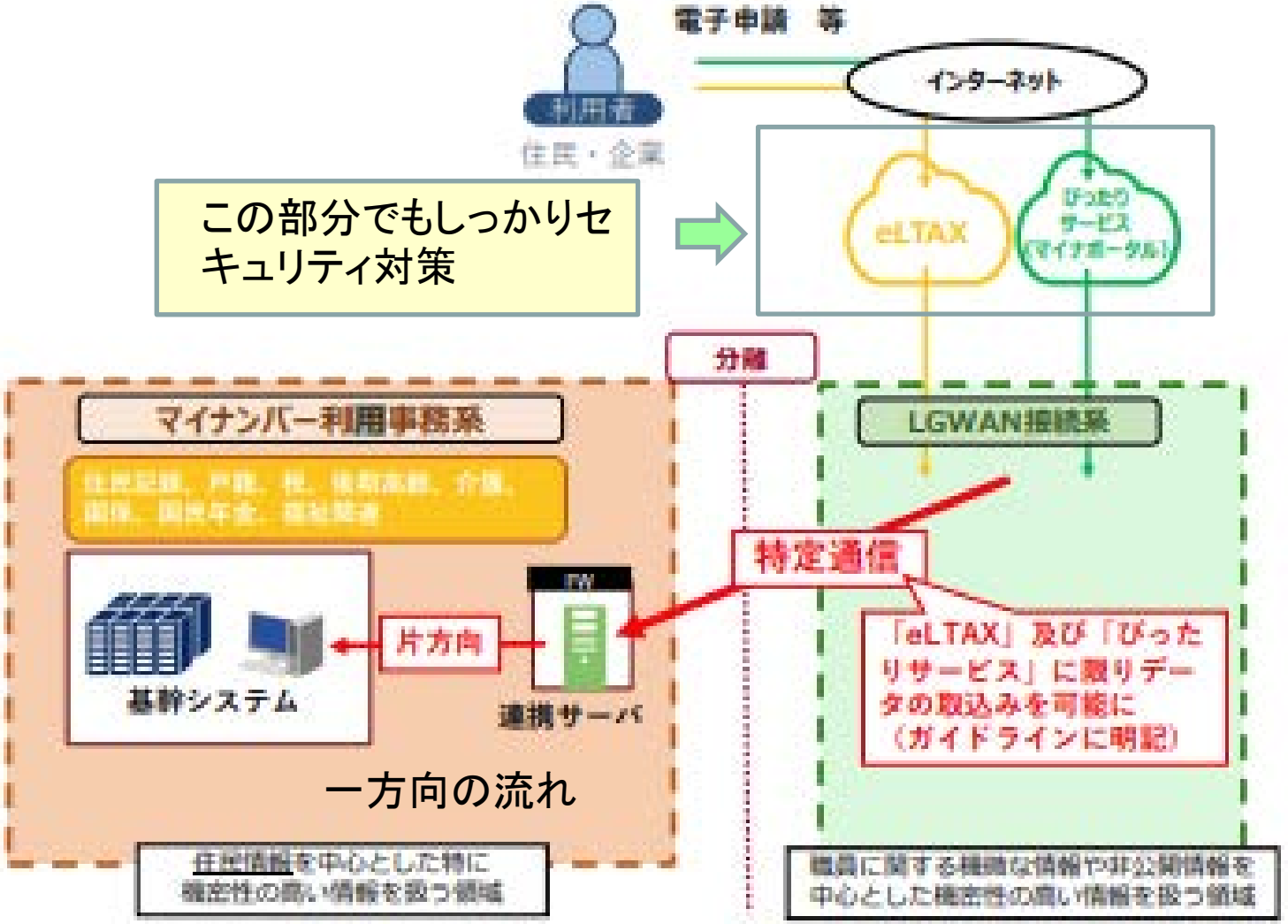
愉快犯：　10%弱

2020年には84%に

ガイドラインの主な改定内容

1. マイナンバー利用事務系の分離の見直し
2. LGWAN接続系とインターネット接続系の分割の見直し
3. リモートアクセスのセキュリティ
4. LGWAN接続系における庁内無線LANの利用
5. 情報資産及び機器の廃棄
6. クラウドサービスの利用
7. 研修、人材育成

マイナンバー利用事務系の分離に係る見直しのイメージ



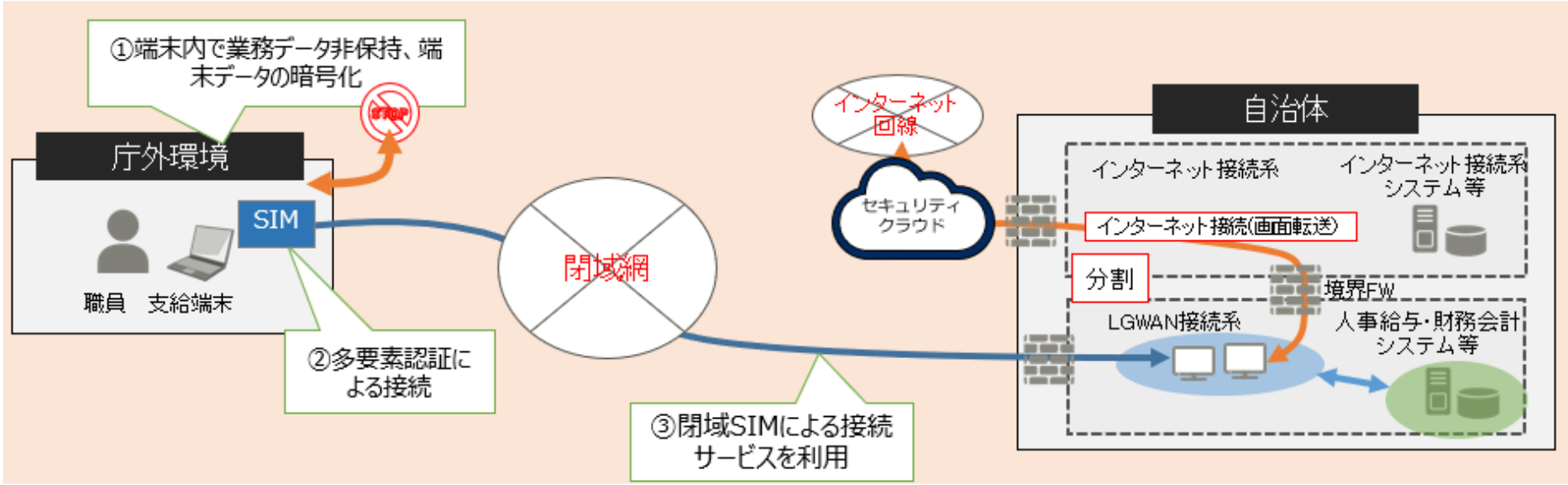
ガイドラインの主な改定内容

1. マイナンバー利用事務系の分離の見直し
2. LGWAN接続系とインターネット接続系の分割の見直し
3. リモートアクセスのセキュリティ
4. LGWAN接続系における庁内無線LANの利用
5. 情報資産及び機器の廃棄
6. クラウドサービスの利用
7. 研修、人材育成

LGWAN接続系へのリモートアクセス法

閉域SIMによる接続サービスを利用するモデル

●閉域SIMによる接続サービスを利用して、庁内にリモートアクセスする。



SIMとは、Subscriber Identity Moduleの略

ガイドラインの主な改定内容

1. マイナンバー利用事務系の分離の見直し
2. LGWAN接続系とインターネット接続系の分割の見直し
3. リモートアクセスのセキュリティ
4. LGWAN接続系における庁内無線LANの利用
5. 情報資産及び機器の廃棄
6. クラウドサービスの利用
7. 研修、人材育成

LGWAN接続系での庁内無線LANの利用

- 盗聴
  パケットキャプチャ等で
  通信内容が傍受されるおそれ。

- 不正アクセス
  MACアドレスの詐称などにより無線LANが不正に利用されるおそれ

- なりすましアクセスポイント（AP）
  正規のAPに見せかけた不正なAPにユーザを誘導し、認証情報などを傍受されるおそれ

地方公共団体が取るべきリスク対策をガイドラインに盛り込む

総務省資料より

ガイドラインの主な改定内容

1. マイナンバー利用事務系の分離の見直し
2. LGWAN接続系とインターネット接続系の分割の見直し
3. リモートアクセスのセキュリティ
4. LGWAN接続系における庁内無線LANの利用
5. 情報資産及び機器の廃棄
6. クラウドサービスの利用
7. 研修、人材育成

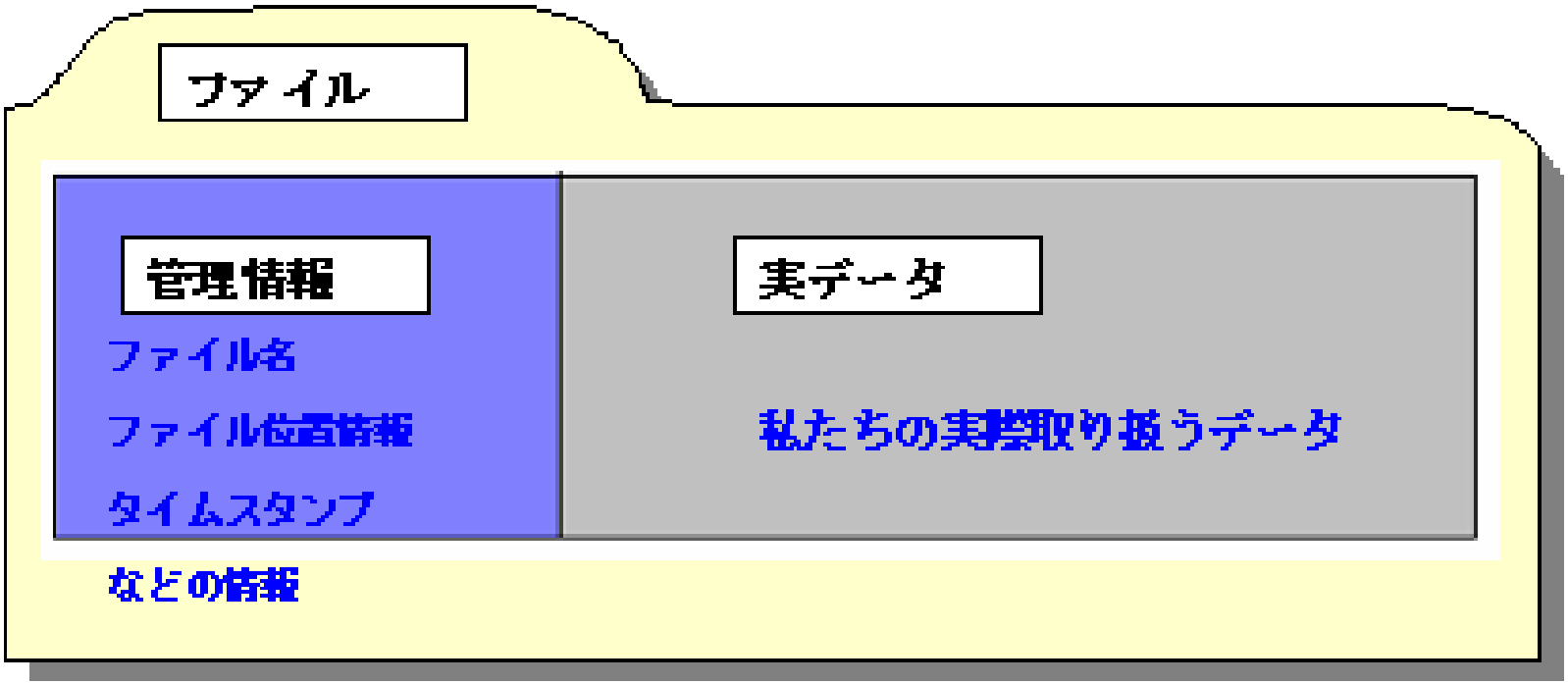
神奈川県庁のHDD流出事案

- 神奈川県庁で個人情報や機密情報を含む行政文書の保存に使われていた3TBのHDD（ハードディスクドライブ）18個がインターネットオークションサイトで転売され、情報が流出した。（2019年）

https://ja.wikipedia.org/wiki/2019%E5%B9%B4%E7%A5%9E%E5%A5%88%E5%B7%9D%E7%9C%8CHDD%E8%BB%A2%E5%A3%B2%E3%83%BB%E6%83%85%E5%A0%B1%E6%B5%81%E5%87%BA%E4%BA%8B%E4%BB%B6

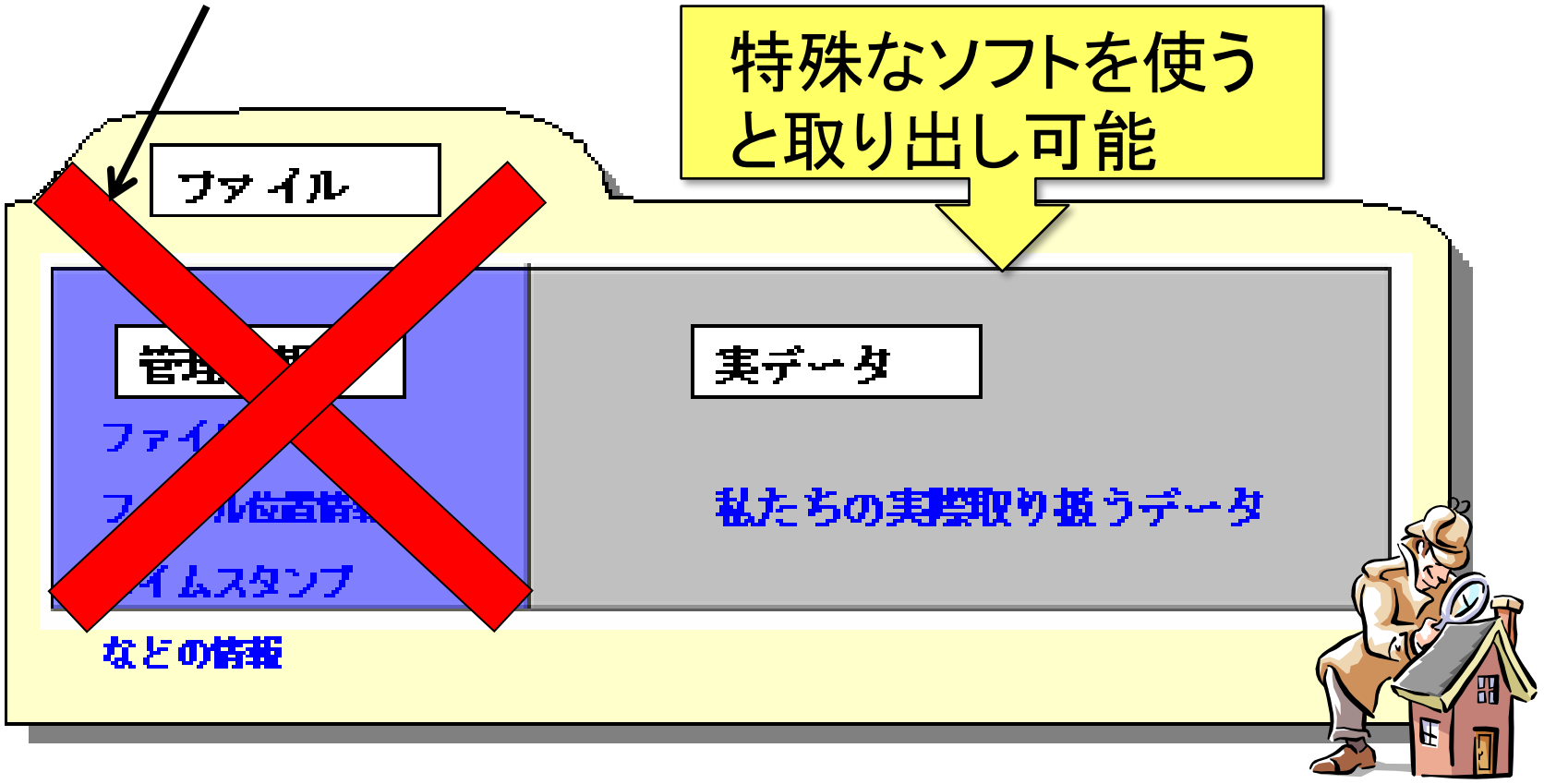
通常のデータ消去（Delete）とは

- データとファイル構造
  - “データ”は PCや携帯内に「ファイル」として存在



通常のデータ消去（Delete）とは

- データ消去の行っている事



ディスクの廃棄などに備えて、復元が困難な方法が必要に

抹消の種別・ランク

① 「Clear(消去)」：一般的に入手できるツールを利用した攻撃に対して耐えられること。

・上書き消去など（この方式だとHPA＜Host Protected Area＞などの情報は残る）

② 「Purge(除去)」：研究所レベルの攻撃に対して耐えられること。

・ATA コマンドの「Enhanced SECURITY ERASE UNIT」を使用する。

・Cryptographic Erase（暗号化消去）を行う。

・外部磁界等による消磁を行なう。

③ 「Destroy(破壊)」：媒体の再生（再組立等）に対して耐えられること。

・物理的破壊装置などにより、再使用不可能になるように破壊

https://adec-cert.jp/guidebook/pdf/DATAWIPEGUIDEBOOK.pdf を参考に作成

抹消の種別・ランク

① 「Clear(消去)」：一般的に入手できるツールを利用した攻撃に対して耐えられること。

・上書き消去など（この方式だとHPA＜Host Protected Area＞などの情報は残る）

② 「Purge(除去)」：研究所レベルの攻撃に対して耐えられること。

・ATA コマンドの「Enhanced SECURITY ERASE UNIT」を使用する。

・Cryptographic Erase（暗号化消去）を行う。

・外部磁界等による消磁を行なう。

③ 「Destroy(破壊)」：媒体の再生（再組立等）に対して耐えられること。

・物理的破壊装置などにより、再使用不可能になるように破壊

https://adec-cert.jp/guidebook/pdf/DATAWIPEGUIDEBOOK.pdf を参考に作成

抹消の種別・ランク

① 「Clear(消去)」：一般的に入手できるツールを利用した攻撃に対して耐えられること。

・上書き消去など（この方式だとHPA＜Host Protected Area＞などの情報は残る）

② 「Purge(除去)」：研究所レベルの攻撃に対して耐えられること。

・ATA コマンドの「Enhanced SECURITY ERASE UNIT」を使用する。

・Cryptographic Erase（暗号化消去）を行う。

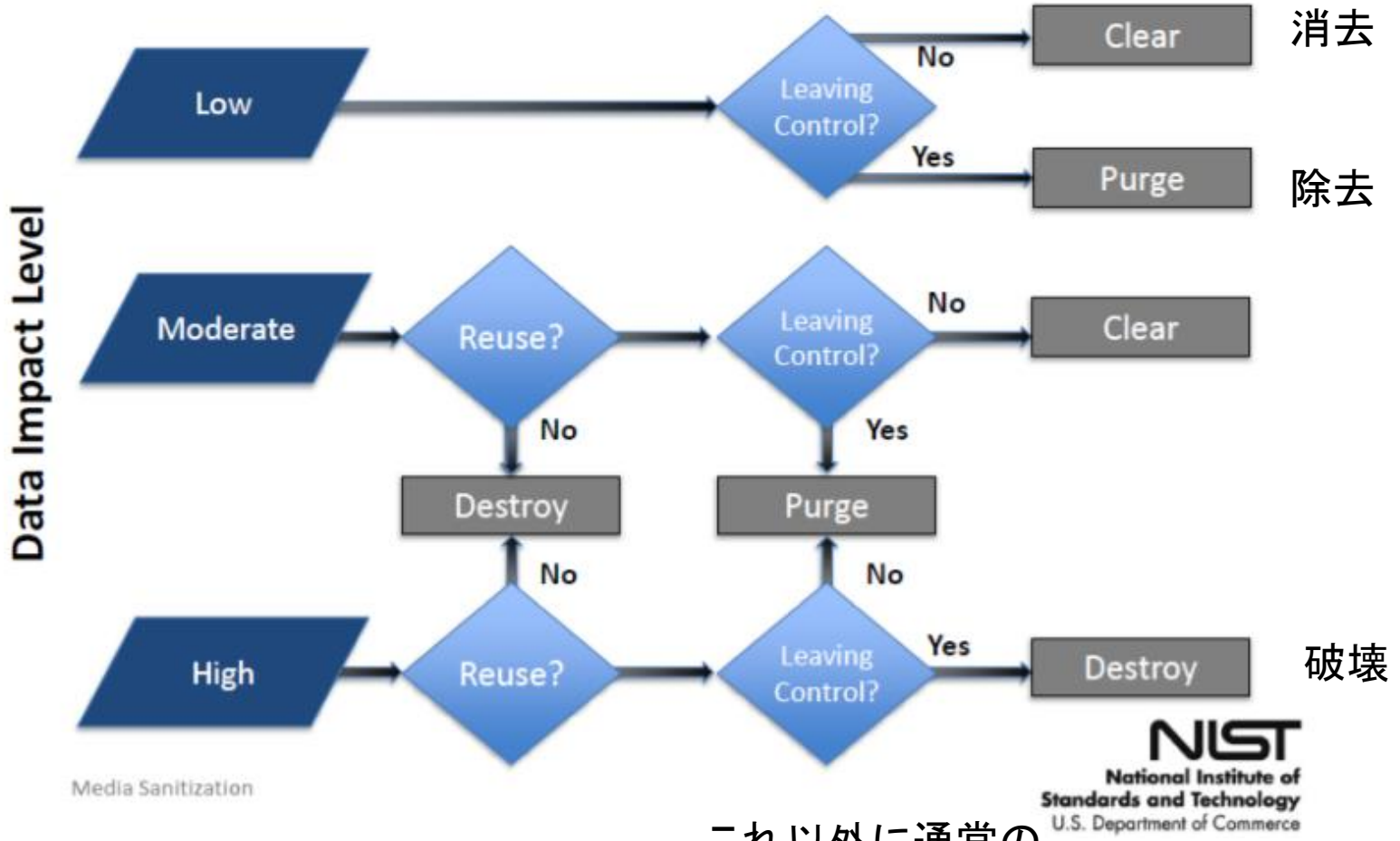
・外部磁界等による消磁を行なう。

③ 「Destroy(破壊)」：媒体の再生（再組立等）に対して耐えられること。

・物理的破壊装置などにより、再使用不可能になるように破壊

https://adec-cert.jp/guidebook/pdf/DATAWIPEGUIDEBOOK.pdf を参考に作成

媒体のサニタイズ（抹消）



消去

除去

破壊

NIST SP800-88Rev1より

これ以外に通常の
消去：Delete

情報システム機器の廃棄時におけるセキュリティの確保

分類	機器の廃棄の方法	廃棄の確認の方法
マイナンバー利用事務系に該当するもの ＜破壊＞	**①物理的な方法による破壊**（注）	**・職員による立ち会いによる確認 ・庁内において情報の復元が困難な状態までデータの消去を行った上で、物理的破壊の完了証明書の確認**
機密性２以上に該当するもの ＜除去＞	①物理的な方法による破壊、②磁気的な方法による破壊、③ＯＳ等からのアクセスが不可能な領域も含めた領域をデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去　のうちいずれかの方法を選択	適切な方法による確認
機密性１に該当するもの ＜消去＞	上記①～⑤の方法の他、⑥ＯＳ等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアによる上書き消去　のうちいずれかの方法を選択	適切な方法による確認

（注）リース契約による場合も、リース契約終了後、物理的破壊を行う旨、予め入札における仕様に明記の上、契約に位置付けることが望ましい。

https://www.soumu.go.jp/main_content/000688753.pdf

注1） 指針作成に当たってはADECも協力
注2） 環境に負担をかけないようにするためすべてを破壊にしないことが望ましい

ガイドラインの主な改定内容

1. マイナンバー利用事務系の分離の見直し

2. LGWAN接続系とインターネット接続系の分割の見直し

3. リモートアクセスのセキュリティ

4. LGWAN接続系における庁内無線LANの利用

5. 情報資産及び機器の廃棄

6. クラウドサービスの利用：政府統一基準の記載を反映しつつ、「Jip-Base事案」を踏まえた記載を追記

7. 研修、人材育成

ガイドラインの主な改定内容

1. マイナンバー利用事務系の分離の見直し
2. LGWAN接続系とインターネット接続系の分割の見直し
3. リモートアクセスのセキュリティ
4. LGWAN接続系における庁内無線LANの利用
5. 情報資産及び機器の廃棄
6. クラウドサービスの利用
7. 研修、人材育成

研修・人材育成

実践的サイバー防御演習（CYDER）の確実な受講

✓未受講の地方公共団体を中心とした計画的な受講の推進

インシデント対応チーム（CSIRT）の設置及び役割の明確化の推進

✓小規模自治体のためのCSIRT構築の手引きに関する説明会の受講
✓CSIRTの役割の明確化

演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有の推進

✓インシデント対応訓練（基礎）
✓インシデント対応訓練（高度）
✓分野横断的演習

啓発や訓練を通じた各自治体の職員のセキュリティ・リテラシーの向上

✓リモートラーニングによる情報セキュリティ研修（eラーニング）
✓情報セキュリティ対策セミナー（集合研修）
✓情報セキュリティに関する技術講習会

総務省資料より

（参考）新たな無害化方式について

- **振る舞い検知**
  不審プログラム特有の動作パターンを定義し、実行するファイルが悪意ある動作をしていないか分析を行い、悪意ある挙動を示した場合はプロセスの実行をブロックする

- **サンドボックス**
  外部から受け取ったプログラムなどを隔離・制限された実行環境で動作させるセキュリティ機構であり、システムが不正に操作されることなどを防ぐ

- **EDR（Endpoint Detection and Response）**
  PCやサーバーなど（エンドポイント）における不審な挙動を監視・検知し、プロセスの停止、隔離など異常時の対応またはその支援をする

※振る舞い検知・サンドボックス・ EDRは製品ベンダによって様々な機能を提供するが、ここでは代表的な機能について記載した
※EDRについては次期自治体情報セキュリティクラウドの要件シートに記載の詳細要件・要件補足事項及び推奨事項も考慮すること

参考：「次期自治体情報セキュリティクラウド要件シート」よりEDRの詳細要件を抜粋

・エンドポイントのアクティビティを監視し、悪意のある活動を示す異常な挙動を監視・検出すること(※1)
・遠隔からの運用で、インシデント発生時の詳細な調査・対処ができること
・遠隔からの運用で、侵害された端末のみに対してネットワークからの論理的な隔離などの対処ができること(※2)
・エンドポイントのプロセスにおいて、異常な挙動を検視した際にプロセスを停止、隔離すること
・不審な挙動を示す端末を特定するため、セキュリティクラウドのSOCで運用することができるEDRを導入すること
・不審な挙動を示す端末のホスト名やIPアドレスなどの情報を通知できること

(※1)ランサムウェアやファイルレスマルウェアといったマルウェアの検出を含む
(※2)不審な挙動を検知して端末を論理的に隔離した後は、利用団体へ速やかに通知し、一次対応（端末の物理的隔離、他の端末への影響確認）を実施すること