番号制度下における医療情報の活用と保護に関する制度的検討

情報セキュリティと
デジタル・フォレンジックの関係

yosihiro.com

佐藤　慶浩

twitter.com/4416sato

発表者紹介

yosihiro.com

佐藤　慶浩（さとう　よしひろ）
日本ヒューレット・パッカード　個人情報保護対策室　室長
（併任）内閣官房 情報セキュリティ指導専門官

社外の活動
- 厚生労働省　社会保障分野サブワーキンググループ　構成員
- デジタル・フォレンジック研究会　理事
- 情報ネットワーク法学会　副理事長
- (社)ｺﾝﾋﾟｭｰﾀｿﾌﾄｳｪｱ協会　ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ審査判定委員会　委員
- JIPDEC　ISMS適合性評価制度技術専門部会　委員
- JIPDEC　プライバシーマーク推進センター　客員研究員
- 杉並区　住基ネット運用監視委員会　委員
- など

はじめに

本発表の趣旨は、これまでのご発表とデジタル・フォレンジック研究会の「橋渡し」

本発表が、「橋」になるかどうかは、聞き手がそれを渡る気概がどの程度あるかが重要。
川にかかった丸太棒を橋として使えるかは、渡る人の問題。
デジタル・フォレンジックという向こう岸に、仮に渡れなくても、発表者の責ではありません。

発表内容

yosihiro.com

説明可能な情報管理の考え方とその技法について
- 「説明可能な情報管理」の必要性
- フォレンジック結果への2つの期待
- 行為の記録を改変する動機と疑惑
- 改変を防ぐ局面
- 改変を防ぐ仕組みの例
- 技術革新は「わがまま」から生まれる
- 人・プロセス・技術で「わがまま」を叶える

デジタル・フォレンジックが貢献できることについて

本医療分科会で
過去に議論された課題

適切な医療行為について、ITシステムにログを残していても、医療結果が期待どおりでないと、ログを改ざんされていると疑われる。
ログに不適切な行為の記録があれば不利な証拠になり、行為が適切なときは、ログの改ざんを疑われてしまうのであれば、ログ記録は百害あって一利なしになると思われ、ログ記録の必要性の理解を妨げている。

改ざんされないログの取り方があるなら、それを知って、ログ記録の必要性を訴求したい。

フォレンジック結果への2つの期待

●不正行為があったことの確認
と
●不正行為がなかったことの確認

不正だけではなく、不適切な行為も含むが、ここでは便宜上「不正行為」と書くことにする。

一般的に、「ないことの確認」は、「あることの確認」よりも困難なことです。
それについては、デジタル・フォレンジックでも同様です。

ただし、どちらの場合でも、「行為の記録を改変できない仕組み」が求められます。

行為の記録を改変する動機と疑惑

●実際に、不正行為があった場合
不正行為の記録を改変する動機は、あり得る。

●実際には、不正行為がなかった場合
不正行為のない記録を改変する動機は、本来ない。
つまり、ないはずの不正行為の記録を作ることはない。
（誰かを、おとしめるという動機ならば、あり得るが）

行為の記録を改変したという疑惑を受けることはあり得る。しかし、この場合、実際には不正行為はないので、無実の疑惑に過ぎない。

改変を防ぐ局面

行為の記録の改変を、どの場合に防ぐのか？

不正行為をしていない場合に備えるには、「不正行為がなかったことの証明」が必要と考えがち。
しかし、「ないことの証明」は困難。
そこで・・・
不正行為をしている場合に、行為の記録を改変できない仕組みを徹底することを考える。
その信頼性が高まれば、
　不正行為の記録がない　→　不正行為がなかった
という図式を組みやすくなる。

改変を防ぐ仕組みの例

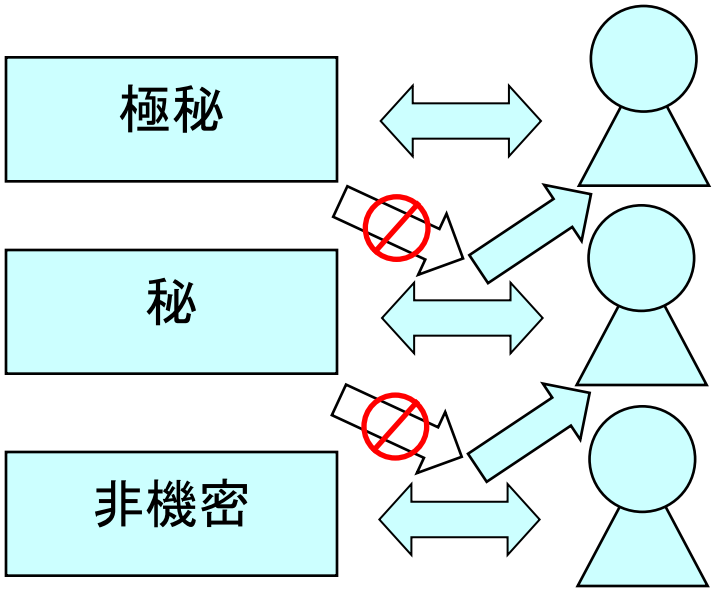
データアクセス制御方式の類型

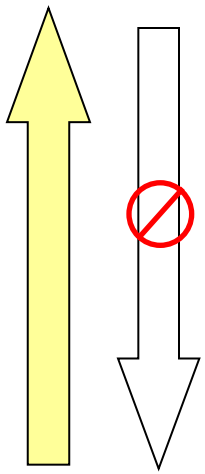
- 任意型アクセス制御（DAC：Discretionary Access Control）
- 強制型アクセス制御（MAC: Mandatory Access Control）

ここから、しばらく技術的な話しをしますが、技術的に深く理解する必要はありません。

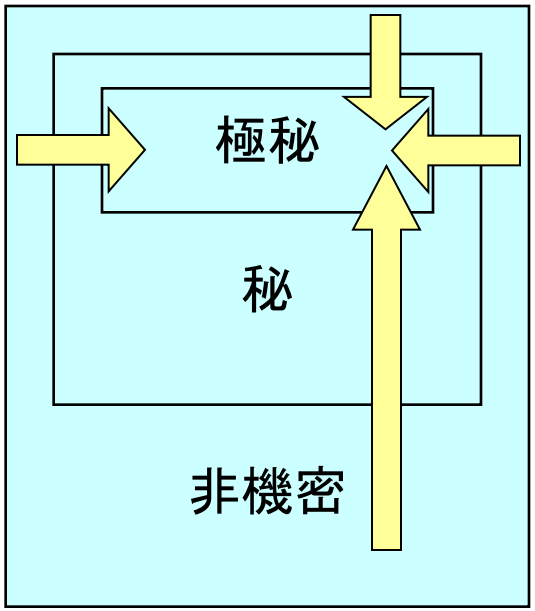
データフロー制御
機密性保護に利用する場合

データフローを一方向に制御することで機密性を守ること（機密を外に出さないこと）ができます。

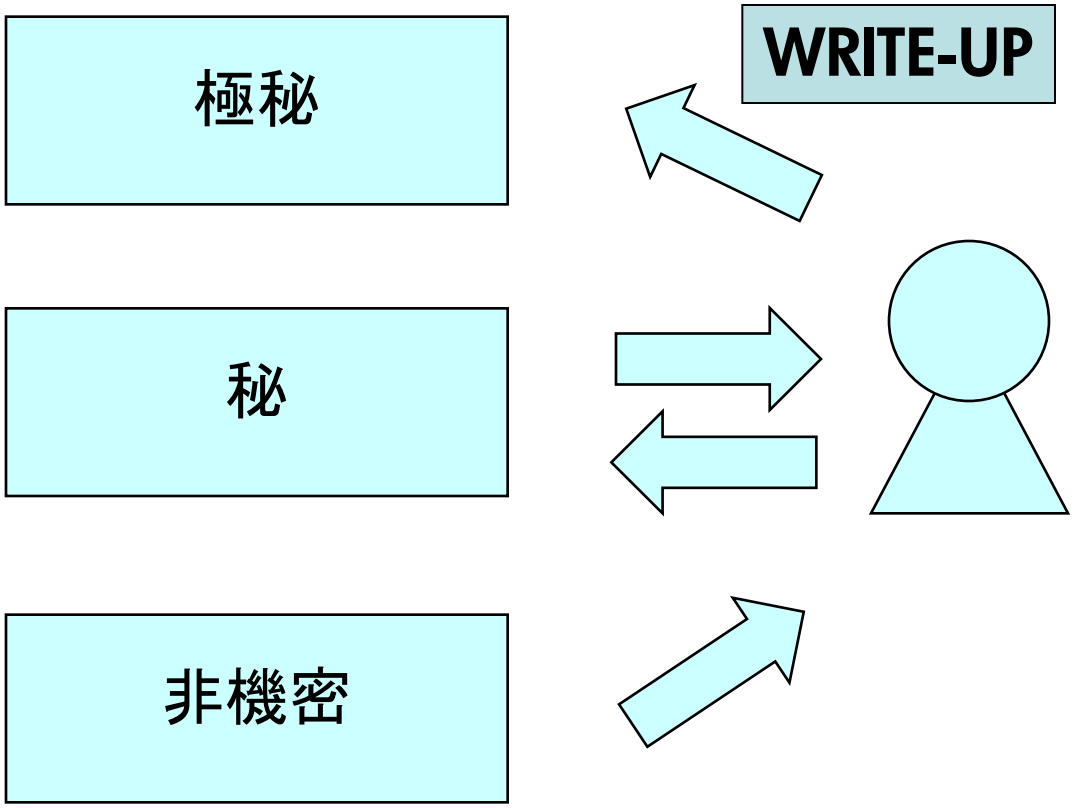




DATA FLOW CONTROL



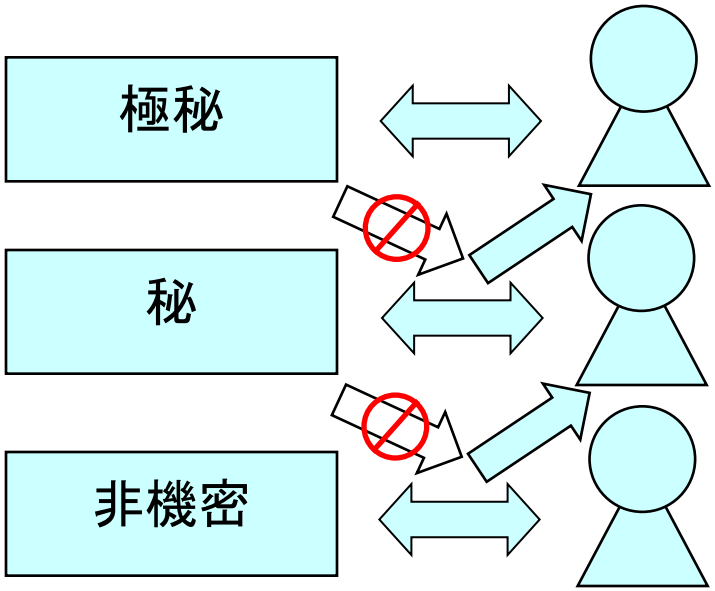
強制型アクセス制御による保護

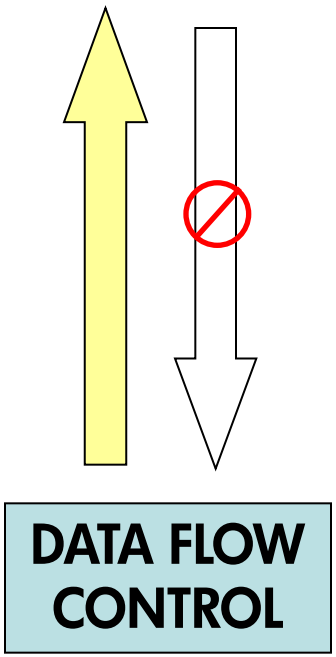


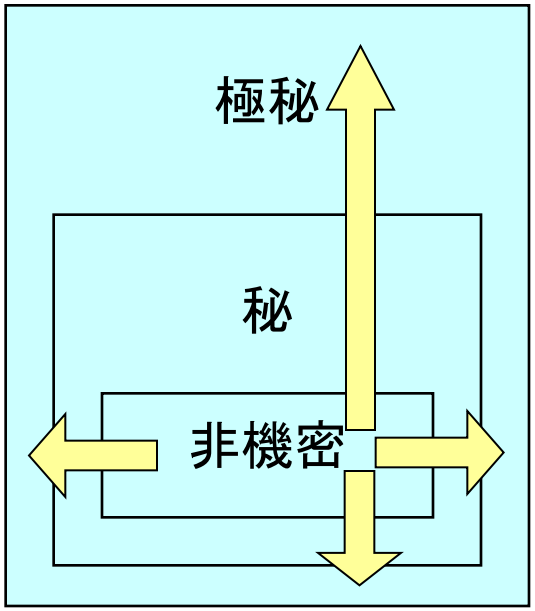
監査証跡は追記専用
のため改変が不可能

データフロー制御
完全性保護に利用する場合

データフローを一方向に制御することで完全性を守ること（改変されないようにすること）ができます。







技術革新は「わがまま」から生まれる
必要な機能を要求することが大切

何をお伝えしたかったかというと・・・

ここから、しばらく技術的な話しをしますが、技術的に深く理解する必要はありません。

ここで紹介したIT製品の機能は、利用する側からの要求で用意された機能です。

既製のIT製品の機能の限界で、ITを利用した業務の限界を考えるのではなく、欲している業務を実現するために必要な機能をITに要求してください。

これまでのITの技術革新は、そんな「わがまま」から生まれています。

例）携帯電話機でウェブが見たい。メールがしたい。

人・プロセス・技術で「わがまま」を叶える
IT製品に使われない気持ちが大切

ITを利用した業務を構築するときに、
ITの知識は、IT屋が持っていればよい。

「そんなことは、できない」と言うIT屋は信用しない。
実現するための、条件や制約を教えてくれるIT屋と付き合うことが必要。
条件や制約の対応を、IT屋と一緒に考えればよい。

人の課題、プロセスの課題、技術の課題を、
それぞれ紐解いてゆけば、
できないことは（ほとんど）ない。

参考

ここまでの発表で説明を省いた箇所の説明については、
http://yosihiro.com/speech/#2010-10-20
からストリーミング視聴できます。

紹介内容については、以下のコラムで基本的な考え方を寄稿してあります。
これの具体的な内容を紹介しました。

IDF研究会　第105号コラム「デジタルデータの改ざん防止とその保証」
http://bit.ly/IDF105 又は
http://www.digitalforensic.jp/expanel/diarypro/diary.cgi?no=234&continue=on

発表内容

yosihiro.com

説明可能な情報管理の考え方とその技法について
- 「説明可能な情報管理」の必要性
- フォレンジック結果への2つの期待
- 行為の記録を改変する動機と疑惑
- 改変を防ぐ局面
- 改変を防ぐ仕組みの例
- 技術革新は「わがまま」から生まれる
- 人・プロセス・技術で「わがまま」を叶える

デジタル・フォレンジックが貢献できることについて

デジタル・フォレンジックが貢献できることについて

yosihiro.com

今後の議論のために、用語の定義を定めることが有意義
例）

ログ　＝　行為等の記録
証跡　＝　定められた保全要件を満たしたログ
　　権限範囲を示す接頭辞を付けて使う
　　例）監査証跡

紹介内容については、以下のコラムで基本的な考え方を寄稿してあります。
これの具体的な内容を紹介しました。

IDF研究会　第182号コラム「証跡とログの区別～温故知新」
http://bit.ly/IDF182 又は http:
http://www.digitalforensic.jp/expanel/diarypro/diary.cgi?no=361&continue=on

デジタル･フォレンジックが貢献できることについて

yosihiro.com

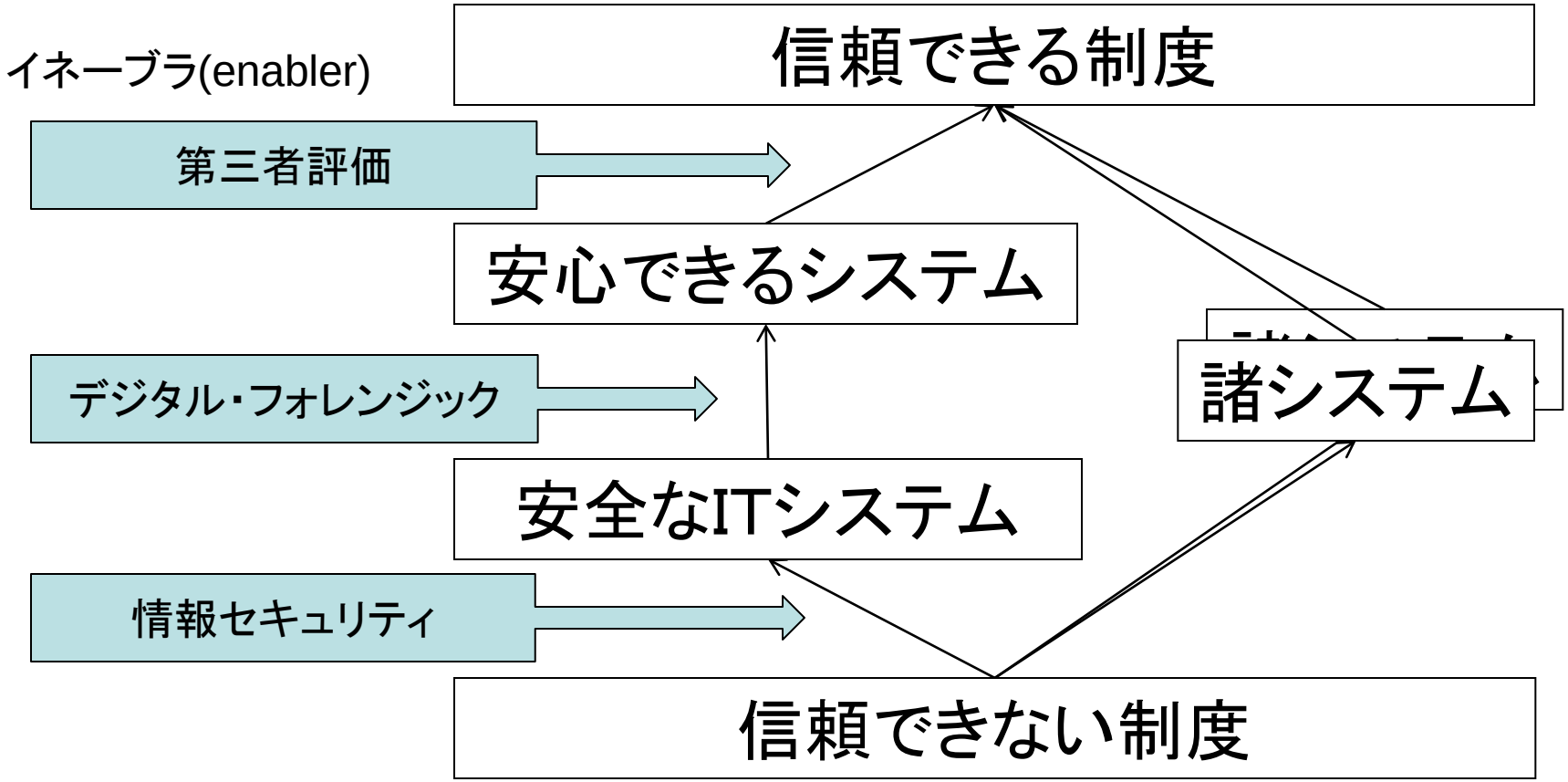
あるべき制度設計ができたなら、
その制度に安心を与えるための仕組みを考える。

安心を与えるためにログを使うなら、
全行為のログを証跡として記録できれば、
悪魔の証明ができるようになり、
不正な行為とそれの隠蔽の抑止に役立つ。

デジタル・フォレンジックの研究により、
　安心感を与えるために必要なログの特定をし、
　安心に必要なログを証跡とする要件の定義をし、
　デジタル・フォレンジックで万が一の事故に備える。

デジタル・フォレンジックが貢献できることについて

情報セキュリティとデジタル・フォレンジックの関係



デジタル･フォレンジックが貢献できることについて

情報セキュリティとデジタル・フォレンジックの関係

情報セキュリティは機密性、完全性、可用性の侵害を防ぐ機能を提供する

デジタル・フォレンジックは、情報セキュリティ機能が保たれている又は保たれなかったことの確認を可能にする

デジタル・フォレンジックにより、情報セキュリティを、安全から安心に変えることを可能にする

それらにより、信頼できないシステムを信頼できるシステムにすることに寄与する

デジタル･フォレンジックが貢献できることについて

yosihiro.com

第三者評価の課題

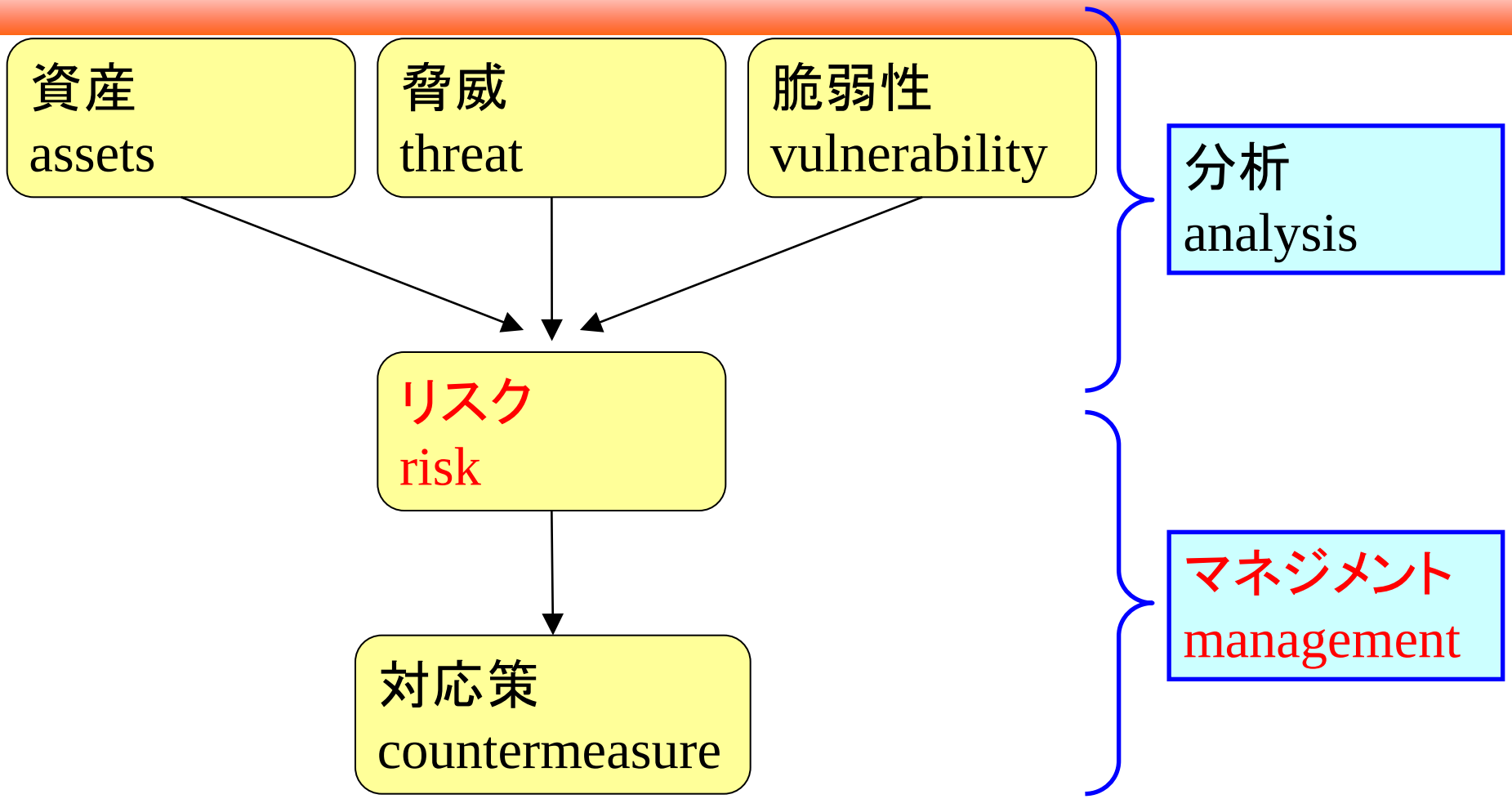
従来ある第三者機関の取り組みとの違い

事前評価
事前に評価することができるか？
事前の評価に対する第三者機関自身の責任は？

事後回復
発生する悪影響を事後回復することができるか？

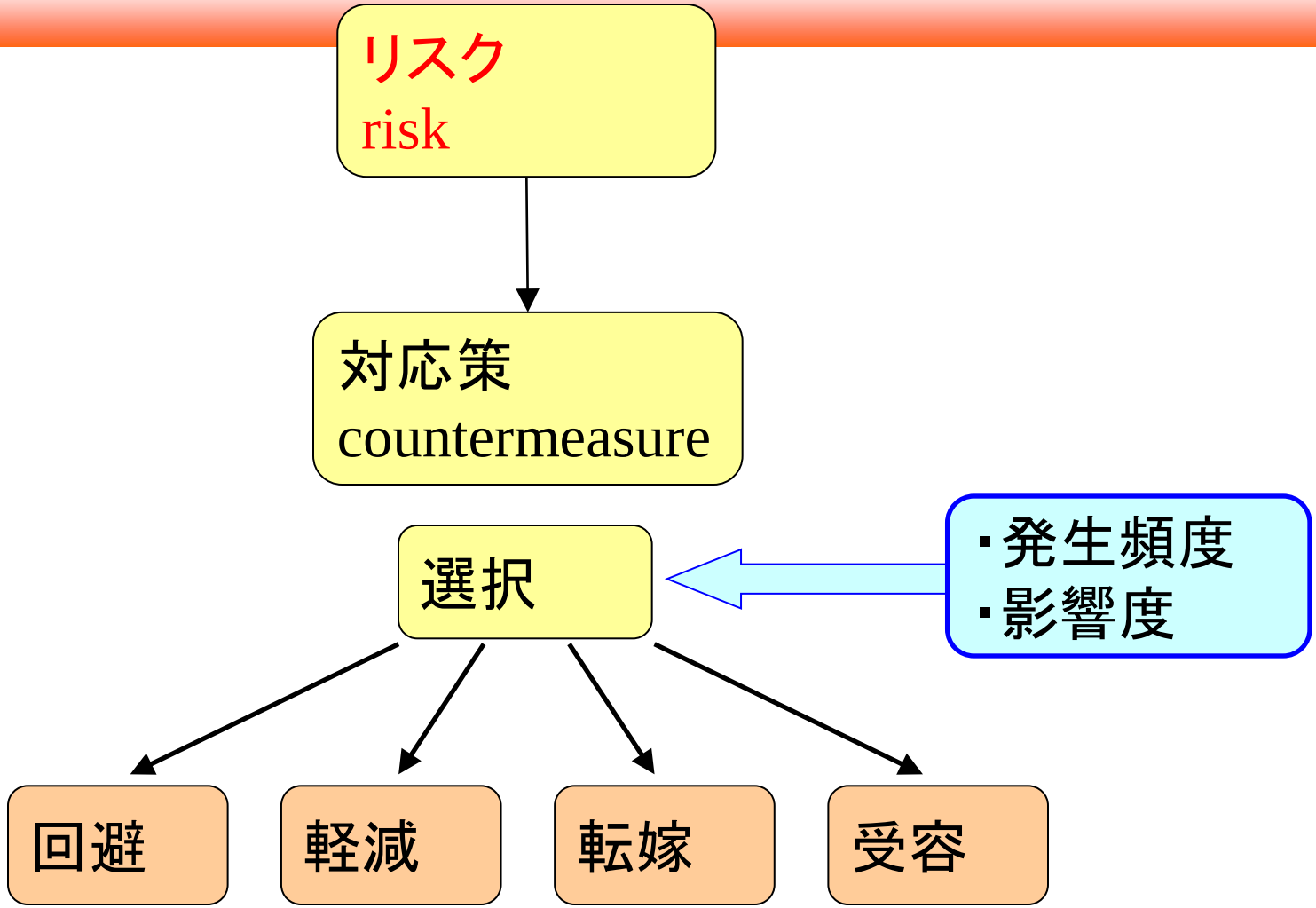
※リスク・マネジメントとインパクト・アセスメントの違いを正しく理解することが重要

リスク・マネージメントとは？



出典：CRAMM(CCTA Risk Analysis and Management Method)

リスク・マネージメントとは？



デジタル･フォレンジックが貢献できることについて

現状

セッター	有識者	トス
アタッカー	ＩＴ屋	アタック

よいトスは上がる（上がりそう）、よいアタックも打てそう
しかし、

監督の不在

政策ビジョンの不在

デジタル･フォレンジックが貢献できることについて

yosihiro.com

政策ビジョンの不在

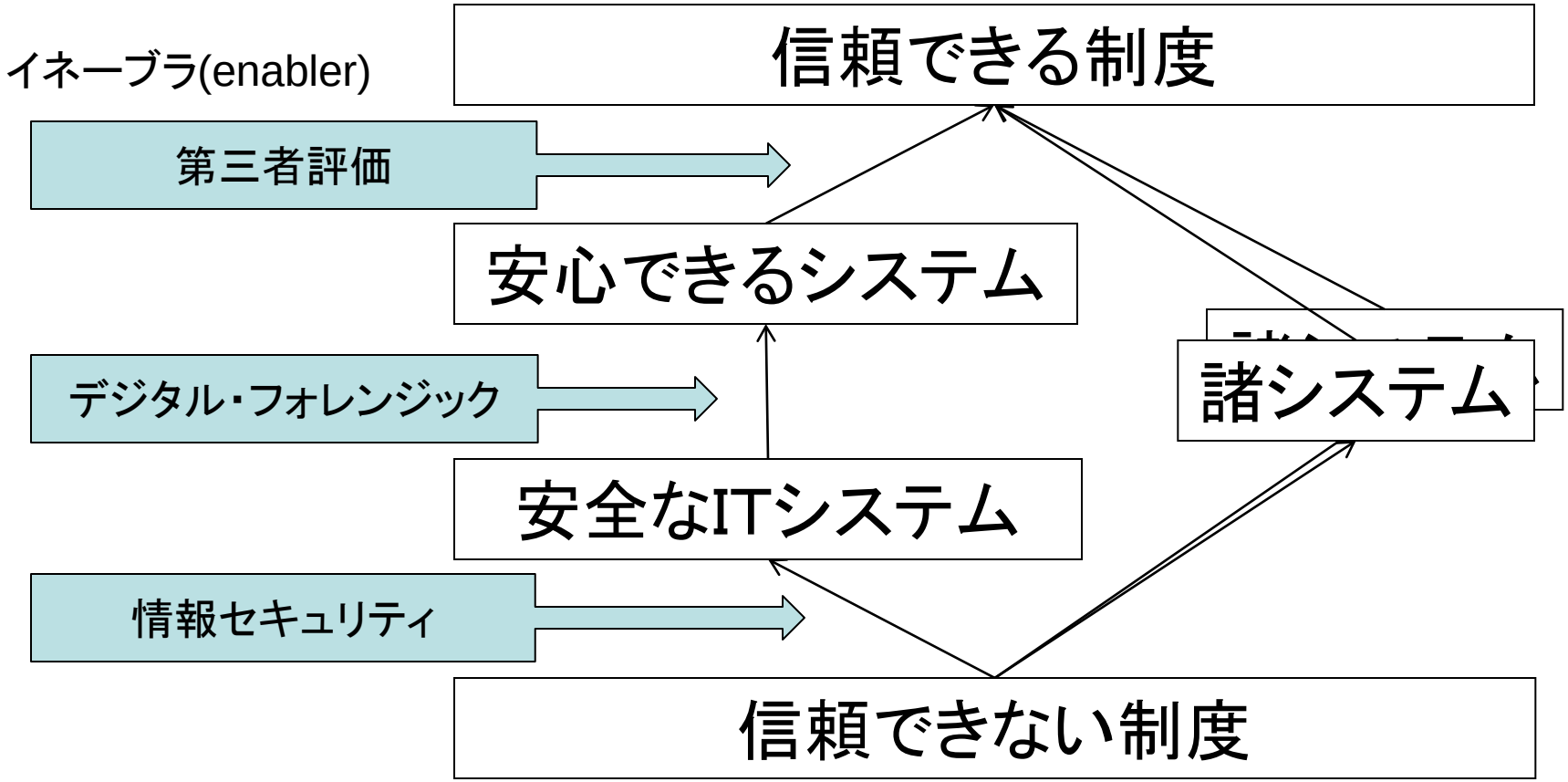
共感できるビジョンに対して、それを実現する制度を検討できる。
その制度を信頼できる制度にすることができる。

たとえば
「孫と元気に遊べる社会」というビジョンの実現手段は、
年金の廃止、終末医療補助の制限、医療保険の予防重視　等

ブログ「砂糖の甘い付箋」
http://yoshihiro.cocolog-nifty.com/postit/

まとめ

情報セキュリティとデジタル・フォレンジックの関係



今晩中にアップロードしますので
明日以降にご利用ください

本日資料のダウンロード

http://yosihiro.com/speech/#2012-01-31

お問い合わせ

http://twitter.com/4416sato