RITSUMEIKAN

# システム安定運用から
# サイバーレジリエンスへ

立命館大学情報理工学部
上原哲太郎

# 今こそ声高らかに訴えたい

**運用こそが金の生る木**

# システム安定運用は事業の要

- 安定したシステムは安定して金を稼ぐ！
- システムの長期にわたる障害停止は事業の根幹を揺るがしかねない
  - 典型例は銀行やWebサービス企業

- 出来るだけシステムの停止を防ぐ
- 出来るだけ障害時の回復を早める

# システム障害が社会的問題に


**ファーストサーバ、共有サーバーとVPSサービスで「データ復旧は不可能」**

ファーストサーバ株式会社は6月23日、20日から同社のレンタルサーバーサービスに発生している障害について、共有サーバーとVPSサービスについては「データ復旧は不可能と判断した」と発表した。

今回の障害の影響を受けたサービスは、共用レンタルサーバーサービスの「ビズ」「ビズ2」、専用サーバーサービスの「エントリービズ」「エンタープライズ3」、VPSサービスの「EC-CUBEクラウドサーバ マネージドクラウド」。影響を受けた顧客数は約5000。

ファーストサーバーでは外部専門業者にも依頼してデータ復旧を進めてきたが、共有レンタルサーバーサービスの「ビズ」「ビズ2」およびVPSサービス「EC-CUBEクラウドサーバ マネージドクラウド」については「データ復旧は不可能」と判断したと発表。ユーザーには、ユーザー側で取ったバックアップデータから再構築してほしいと呼びかけ、「お客様のお手を煩わす事態となりましたことを、心よりお詫び申し上げます」と謝罪している。

**あれから1週間……ファーストサーバ「Zenlogic」の大規模障害に関する報告書を公開**

tks24　2018年7月18日 06:00

Tweet　リスト　B! 4　Pocket 26

先日騒動となったファーストサーバ「Zenlogic」の大規模な高負荷障害に関する報告書が17日、同社サイトに掲載された。ダウンロードできるPDF版も用意されている。

6月19日から発生していた高負荷障害は、7月6日からサービス全てを停止して緊急メンテナンスを行ったものの終了予定の9日朝になっても復旧せず、その日の夜になってようやく利用が再開された。今回の報告書では、この間にユーザーに及んだ影響、障害の原因、再発防止策、これまでに取られた具体的な対応内容などがまとめられている。利用者を含むユーザーの反応はさまざまだが、報告書内ではストレージを提供・管理しているヤフーへの言及が非常に多く見られることもあり、ヤフー側から詳細な見解も聞きたいという意見もちらほら。10日以降はひとまず沈静化した状態にあるこの件だが、個別[illegible]ではまだ時間を要しそうだ。

Internet Watch 2012, 2018

**2月に障害発生の「Doblog」。5月30日をもってサービスを終了**

Doblog

NTTデータは24日、2月8日に障害が発生したブログサービス「Doblog（ドブログ）」について、5月30日にサービスを終了すると発表した。これに伴い、ユーザーによるブログ移転先周知などを目的として、24日にサービスを一時的に再開した。

Doblogは、2月8日10時頃に2つのHDDで発生した障害の影響で、サービスが一時停止。その後、2008年8月4日未明から2009年2月8日朝まで記事のうち、一部を除いて記事の復旧を完了した。また、並行して復旧した記事や画像のダウンロード機能も提供を開始している。

故障したHDDに関しては、継続して復旧作業が進められ、4月10日付で2月7日未明時点までに復旧が完了できたという。NTTデータによれば、「試算では99%以上の情報は復旧できたものと考えている」とする一方、「すべての情報の復旧には達しなかった」とした。

故障したHDDは、いずれも利用期間が3年以内。NTTデータでは、HDD以外の部品やその他システム環境で特に問題は発生していないため、HDDに生じた突発的な障害が今回の障害原因である可能性が高いとしている。

NTTデータでは復旧作業の完了を踏まえて、今後のDoblogサービスについて検討。その結果、「開設時の目的である、ブログシステムを構築するための技術的知見、コミュニティサービスを運用・運営するためのノウハウの蓄積は十分に達成できた」とし、サービスの終了を決定した。

4月24日には、書き込みや閲覧などが可能な状態でサービスを一時再開。一時再開にあたっては、情報のバックアップ方式や故障検知機能を社内の専門チームと連携して見直し、体制を強化したという。

Doblog登録ユーザーに対しては、サービス終了と一時再開を案内するメールを送信する。NTTデータでは、Doblogユーザーに対して感謝を述べるとともに、「故障発生以降、サービス再開を心待ちにしていたユーザーの期待に沿うことができず、また多大なるご迷惑をおかけしてしまいましたことを深くお詫び申し上げます」とコメントしている。

https://internet.watch.impress.co.jp/cda/news/2009/04/24/23277.html

# 事業継続に関わる課題

## ・宇陀市民病院ランサムウェア事件

### 宇陀市立病院がランサムウエア被害、身代金は支払わず

2018/10/25 15:00

保存 共有 印刷 その他

日経XTECH 日経クロステック

奈良県の宇陀市立病院は2018年10月23日、10月1日に導入した電子カルテシステムがランサムウエアに感染したと発表した。セキュリティーリサーチャーのpiyokango氏によれば、国内の病院では、公表された被害事例として、初のランサムウエア被害だという。

ランサムウエアに感染したのは、電子カルテシステムのサーバーと一部のクライアントパソコン。サーバーには、10月1日から15日までに来院した3835人の診療記録が保存され、ランサムウエアによって1133人分のデータが暗号化されていた。病院担当者は、「感染に気付いたのが早かったため、すべてのデータが暗号化されなかったとみている」という。またクライアントパソコンの多くは業務時間外で電源が入っていなかったため、感染を免れたとしている。

2018/11/06 05:00

ニュース解説

### ランサムウエアGandCrab被害者に朗報、宇陀市立病院の現状

齊藤 貴之＝日経 xTECH／日経NETWORK 日経XTECH

この記事を評価する

この記事は ○仕事に役立った3 ○人に勧めたい2 ○難しい0 ○易しい0

2018年1月に最初の感染が報告されてから、海外で多くの被害を引き起こしているランサムウエア「GandCrab（ガンクラブ）」。国内でも奈良県の宇陀市立病院が被害に遭った。電子カルテシステムのサーバーが感染し、1133人分の診療データが暗号化されたという。

関連記事：宇陀市立病院がランサムウエア被害、テープ未挿入でデータ復元できず

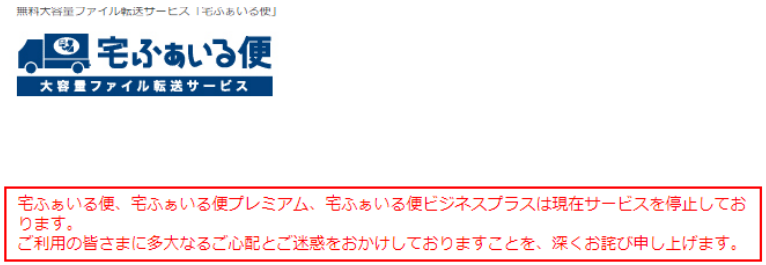
ところが2018年10月下旬、GandCrab被害者に朗報が届いた。ルーマニアのセキュリティー企業が、GandCrabで暗号化されたデータを復元するソフトを公開したからだ。

**感染地域に偏りがあるGandCrab**

GandCrabは、コンピューターに感染するとハードディスクなどに保存されたファイル

# 事業継続に関わる問題

- 宅ふぁいる便パスワードリスト漏洩問題



無料大容量ファイル転送サービス「宅ふぁいる便」

宅ふぁいる便
大容量ファイル転送サービス

宅ふぁいる便、宅ふぁいる便プレミアム、宅ふぁいる便ビジネスプラスは現在サービスを停止しております。
ご利用の皆さまに多大なるご心配とご迷惑をおかけしておりますことを、深くお詫び申し上げます。

＞第１報についてはこちらをご確認ください
＞第２報についてはこちらをご確認ください

2019年1月28日

（第３報）

**「宅ふぁいる便」サービスにおける不正アクセスによる、お客さま情報の漏洩について（お詫びとお願い）**

このたびはファイル転送サービス「宅ふぁいる便」の一部サーバーに対する外部からの不正アクセスにより、約480万件のお客さま情報が外部に漏洩し、ご利用の皆さまに多大なるご心配とご迷惑をおかけしておりますことを、深くお詫び申し上げます。
調査の過程で、特定期間においてのみ取得をしていたお客さま情報などについても漏洩していることがわかりましたので、お知らせいたします。漏洩したお客さまの総数に変りはございません。

2019/03/01 05:00

動かないコンピュータ

**宅ふぁいる便の平文パスワード480万件流出事件、1カ月たってもサービス再開できず**

オージス総研

竹居 智久＝日経コンピュータ

日経コンピュータ

この記事を評価する

この記事は ○仕事に役立った4 ○人に勧めたい2 ○難しい0 ○易しい0

**オージス総研は2019年1月、ファイル転送サービス「宅ふぁいる便」を停止した。利用者のメールアドレスとパスワードが平文のまま約480万件流出した。暗号化やハッシュ化の必要性は認識していたものの、他の対策を優先し怠った。2月20日時点で「原因や手口は調査中」とし、サービスは再開できていない。流出情報が別のWebサービスへの不正ログインに悪用される恐れもある。**

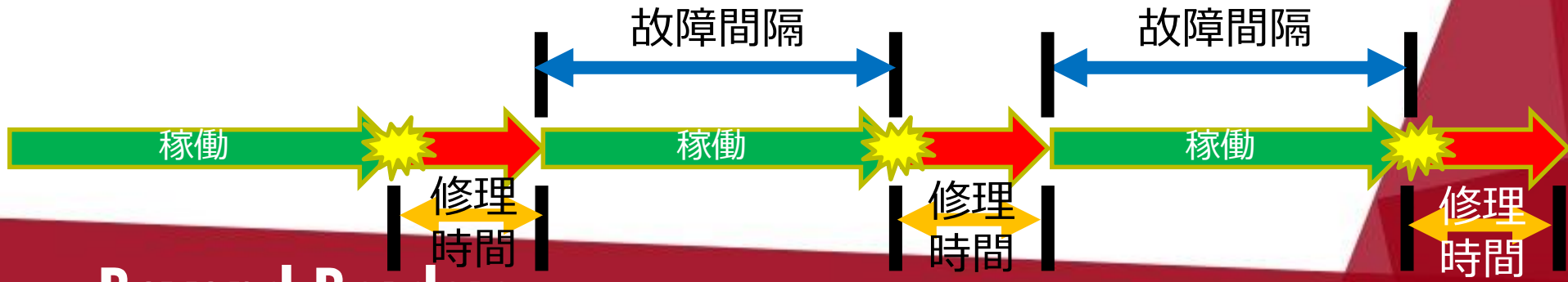
Webサービスにログインするために使うメールアドレスとパスワードが平文（ひらぶん）のまま480万件流出するトラブルが発生した。公表されている中では過去最大級となるログイン情報の流出だ。流出したログイン情報を悪用して様々なWebサービスへの不正ログインを試みる「リスト型攻撃」が増える恐れがある。

流出元は個人向けファイル転送サービス「宅ふぁいる便」だ。大阪ガスの完全子会社のシステムインテグレーター、オージス総研が運営する。1999年に大阪ガスの社内サービスとして始め、2005年に一般向けの事業にした。オージス総研によると現在の利用件数は年間約7000万件という。

# システムの安定性をどう測るか

- 平均故障間隔（MTBF)
  - 故障回復から故障までの間隔の平均時間
  - 修理できることが前提
    交換部品は平均故障時間（MTTF）で表現
- 平均修理時間（MTTR)
  - 修理にかかる時間の平均時間
- 稼働率＝MTBF／（MTBF+MTTR)
  - SLAなどで用いられる値

線形モデル



# 線形モデルの背後にある考え方

- システムは部品の集合体
- 部品は正常か異常(故障)かの2状態
- 部品は設計目標に従って
  ある期間は正常に動くことを保証
  よってMTBFは部品単位で計算可能
- 故障は検知可能であり交換修理は容易
  よってシステムのMTBFも計算可能
- 部品のMTBFが延ばせない場合は
  冗長化によりシステムのMTBFを伸ばす

- もともと機械工学的な考え方

# しかし情報システムでは障害原因は多岐に渡る

- ハードウェア部品の障害
- ソフトウェアの不具合（バグ）
- 設定ミス・操作ミス
- サイバー攻撃やセキュリティ事故
- 故意による破壊的操作

- MTBFが計算/予測困難かつ変動
- 原因究明が困難な場合MTTRに影響

# IPA「情報システムの障害状況一覧」

表1　2018 年前半の情報システム障害データ（報道に基づき社会基盤センターが整理）

| No. | システム名 | 発生日時（上段）<br>回復日時（下段） | | | | 影響 | 現象と原因 | 直接原因 | 情報源 |
|---|---|---|---|---|---|---|---|---|---|
| | | 年 | 月 | 日 | 時 | | | | |
| 1801 | 三菱UFJ NICOSカード | 2017 | 12 | 26 | | 他社発行のデビットカードをニコスの加盟店で使った7行分1,500件でニ重引落が発生。コンビニ収納代行でも全国の111の自治体に対し、利用者が税金などを支払ったというデータの送信が遅れた。督促状を送付した自治体もあった。 | 原因は、加盟店からの売り上げ情報を管理する15個のハードディスクのうち3個が同時に壊れたが、復旧作業中の処理を誤ったことで傷口が広がった。再発防止策は、①システム機器故障への監視強化、②バックアップ強化（1日1回から1時間毎）、③システム障害復旧手順の見直しとツールの拡充、④今後全体事象を総括した再発防止策の策定。 | ハードウェア障害<br>復旧作業ミス | ・三菱UFJNICOSカードお知らせ（2018.1.4）（2018.1.9）（2018.2.7）<br>・Itpro（2018.1.9）<br>・朝日新聞（2018.1.10）<br>・読売オンライン（2018.1.9）<br>・日本経済新聞電子版（2018.1.10）<br>・日本経済新聞（2018.2.8） |
| | | 2018 | 2 | 7 | | | | | |
| 1802 | 北海道電力 エリアインバランス | 2018 | 1 | 11 | | 2017年4月から10月までの、北海道エリアの小売り事業者のインバランス料金が誤って請求された。 | エリアインバランス量の算定で、需要計画データについて電力広域的運営推進機関による計画誤り修正後のデータを使用すべきところ、誤って、別の合計値を使用した。2017年4月に仕様変更があったにも関わらず、未対応だった。 | プログラム不具合 | ・北海道電力プレスリリース（2018.1.10）<br>・環境ビジネスオンラインニュース（2018.1.11）<br>※障害発生は、報道された日 |
| | | | | | | | | | |
| 1803 | 苫小牧市立病院電子カルテ | 2018 | 1 | 12 | 朝 | 通常外来診療を休診し、救急車による救急搬送の受け入れも一時休止した。 | 12日朝、院内のほぼ全ての電子カルテにエラーが発生。入出力も不安定な状況になった。電子カルテは、2006年10月以降に導入。 | 不明 | ・苫小牧民報（2018.1.12） |
| | | 2018 | 1 | 12 | 正午 | | | | |
| 1804 | 中部電力 検針用端末 | 2018 | 1 | 1 | | スマートライフプラン等の多時間帯契約者のうち、スマートメーターを設置済みで、1月4日から11日にかけて現地にて検針作業を行った管内の5県（愛知、三重、岐阜、静岡、長野）で、2018年1月分の約2,400件の電気料金、計約300万円分を過小請求した。 | 2015年7月スマートメーター導入の際、検針用端末のプログラム更新を実施したが、時間帯毎に使用量を振り分けするプログラムの設定誤りにより、検針用端末には、1月1日以降全て夜間時間帯に振り分けられたため、2018年1月1日以降の請求金額に不具合が発生した。 | プログラム不具合 | ・中部電力プレスリリース（2018.1.14）<br>・中日新聞（ウェブ）（2018.1.14）<br>・毎日新聞ネット（2018.1.14） |
| | | 2018 | 1 | 11 | | | | | |
| 1805 | ファミリーマートマルチメディア端末 | 2018 | 1 | 21 | 夜 | ファミリーマート店内のマルチメディア端末「Famiポート」で「メルカリ」「フリル」「ラクマ」「オタマート」などのフリーマーケットサービスで、ヤマト運輸の宅急便の送り状が使えなくなった。 | 1月21日夜からFamiポート側の障害で、出品者が落札者宛に荷物を発送する際、各サービスから発行されたQRコードをFamiポートにかざし、宅急便の送り状を印刷するフリーマーケットサービスが使えなくなった。 | 不明 | ・日経コンピュータ（2018.1.22）<br>・日本経済新聞電子版（2018.1.22） |
| | | | | | | | | | |

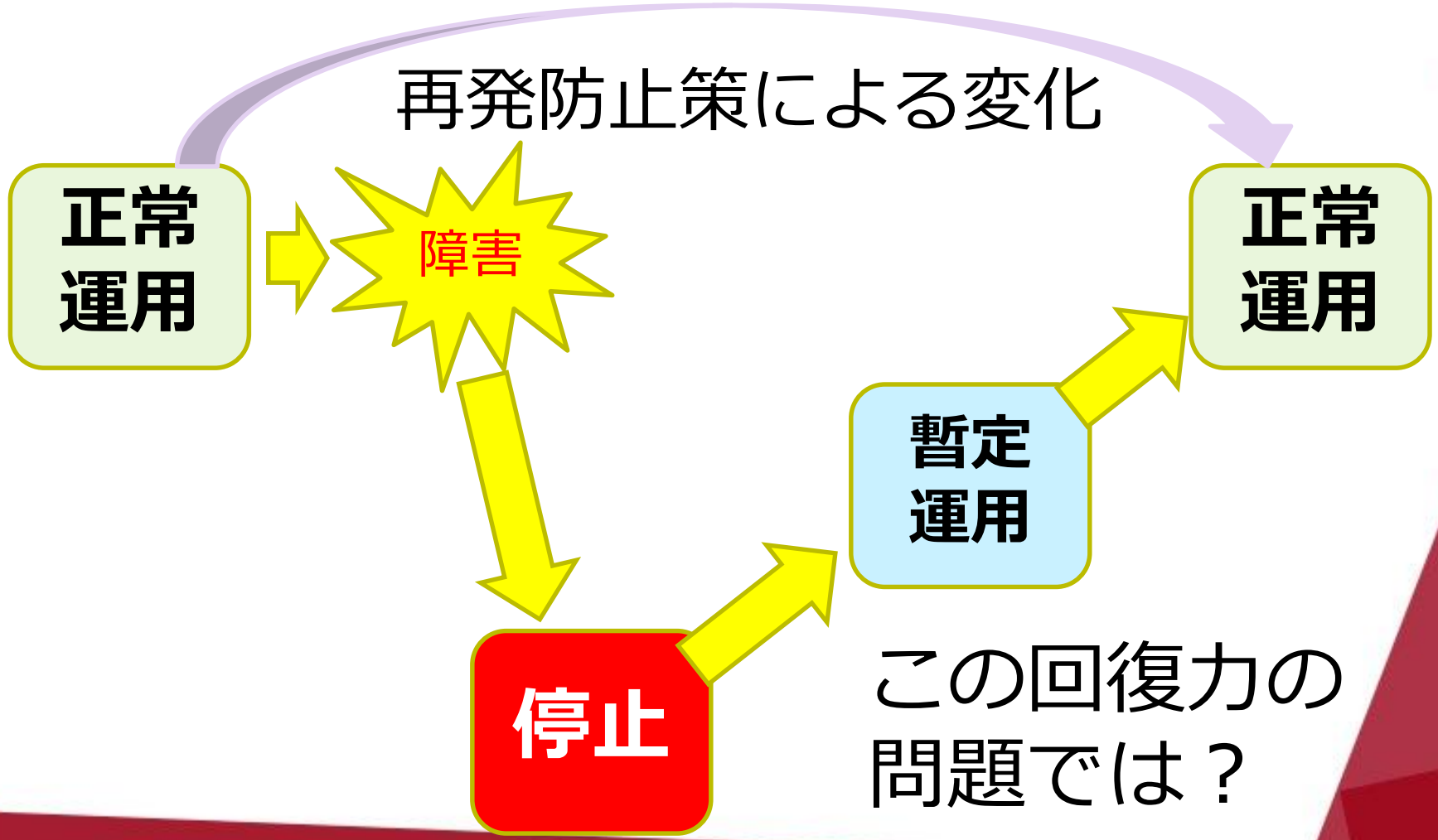
# IPA「システム障害事例の分析により得られた教訓の共有」

| IT障害を引き起こす脅威の例 | | |
|---|---|---|
| 脅威の類型 | | 脅威の例 |
| 意図的な要因 (サイバー攻撃、犯罪等) | | 不正侵入、データ改竄・破壊、不正コマンド実行、ウイルス攻撃、サービス不能攻撃(DoS:Denial of Service)、情報漏洩、重要情報の詐取、内部不正 等 |
| 非意図的な要因 | 偶発的な要因 **(人為的ミス、機器故障)** | 操作・設定ミス、プログラム上の欠陥(バグ)、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障　等 |
| | 環境的な要因 (災害、疫病) | 地震、水害、落雷、火災等の災害による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設の損壊　等 |
| | 他分野の障害からの波及 | 電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの）等 |

IT障害発生の中心は **偶発的な要因**

<参考>
NISC: 重要インフラの情報セキュリティ対策に係る第２次行動計画

# 大規模情報システムの運用



# レジリエンス（Resilience）とは：
# from Merriam-Webster

1. the capability of a strained body to recover its size and shape after deformation caused especially by compressive stress
応力がかかっても姿形が元に戻る能力
2. an ability to recover from or adjust easily to misfortune or change
災害や変化から回復し適応する能力

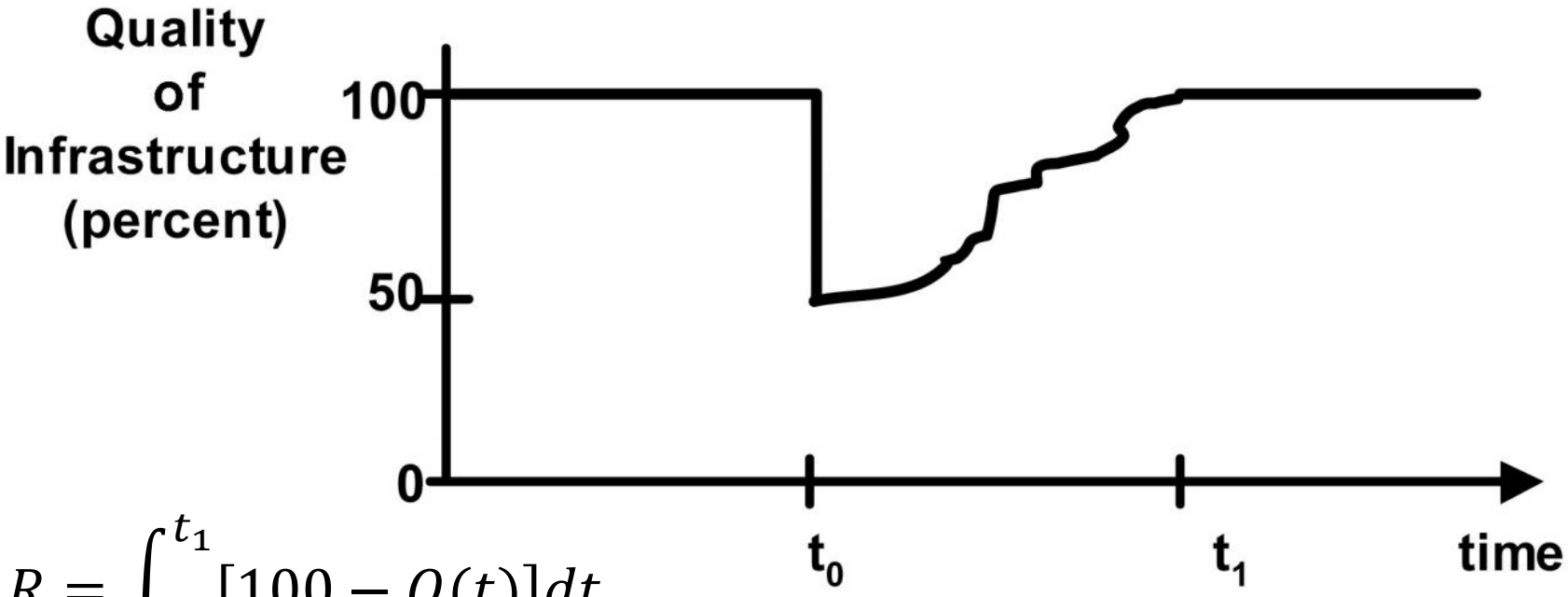
モノ・人・組織・社会・システム…などが大きな外圧/環境変化に直面した際に本来の目的を維持し速やかに回復する能力

# 「レジリエンス」の研究分野

- 心理学
  - 大きな心理的ストレス、喪失体験などからの回復力
- 生態学
  - 災害などで破壊された生態系の回復力
- 防災学
  - 平成２５年度版防災白書「レジリエンス（強靭化）」
- システム
  - システムズ・レジリエンスプロジェクト（２０１１～１６）


近代科学社刊

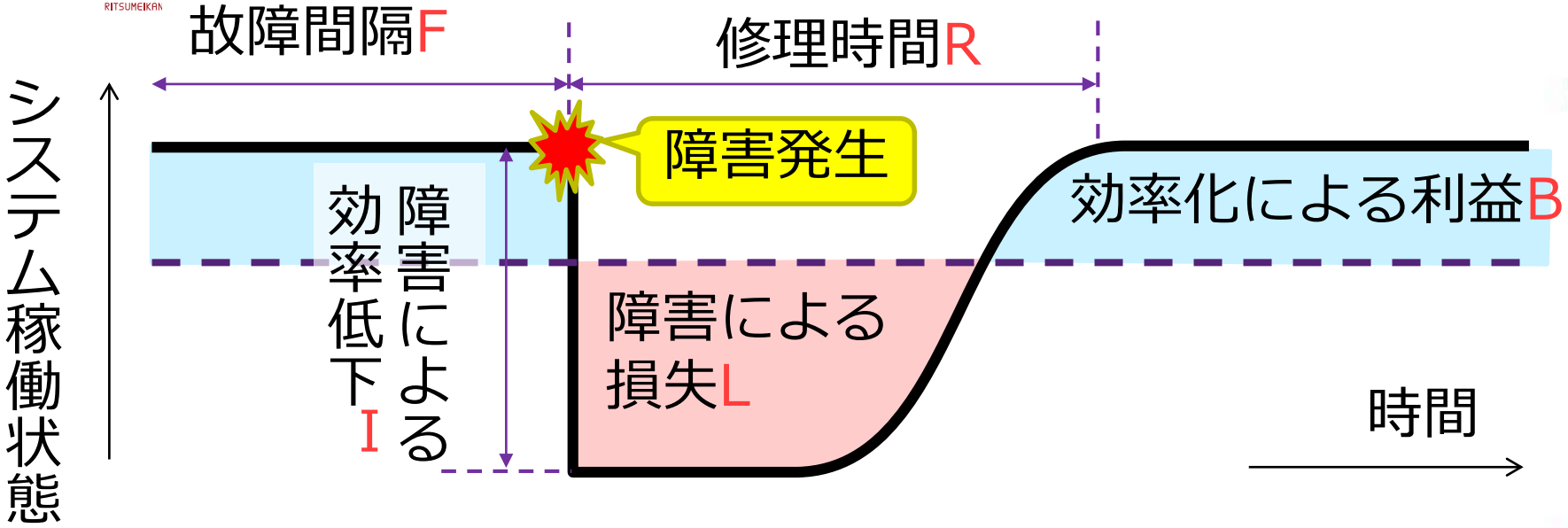
# Bruneauの三角形(2003)
# Resilience Triangle



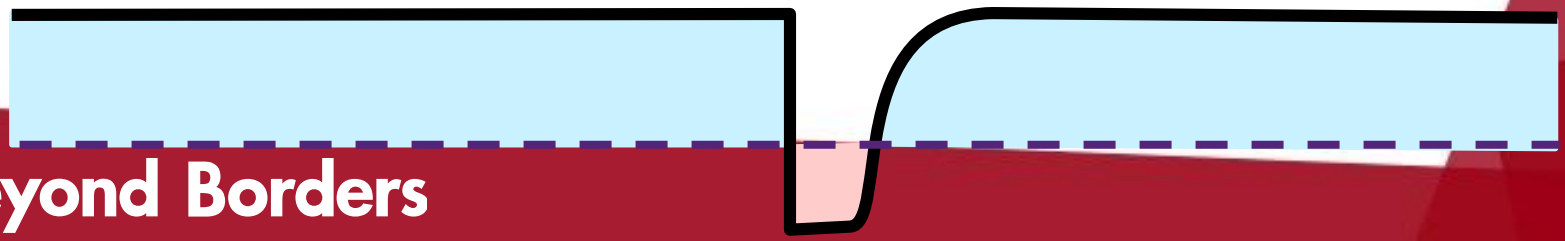

$$R = \int_{t_0}^{t_1} [100 - Q(t)]dt$$

M.Bruneau et al. : “A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities”, Earthquake Spectra, Vol. 19, No.4, 2003.

# 情報システムのレジリエンス




Bを最大化　Lを最小化するため
Fを長くRを短くIを小さくしたい

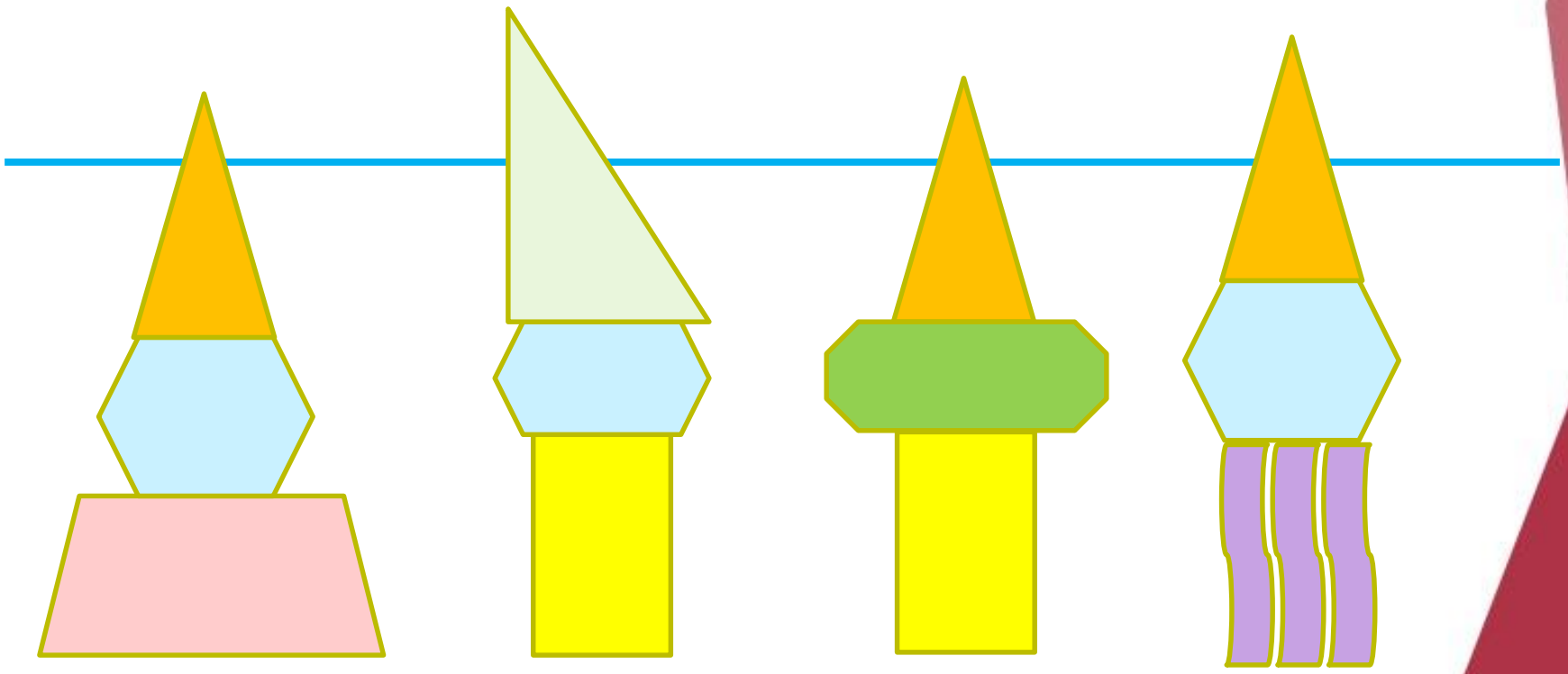


# 情報システムのSystemic Model

- システムは多様な要素の集合体であり要素の状態も変化する
- システムの「機能性能目標」があるがその実現手法は１つではない
- システムの性能・状態は計測可能だが刻々と変化する
  要素とシステム性能の関係は単純には記述できない
- この状態で機能性能目標を満たした状態を保つのが「安定運用」

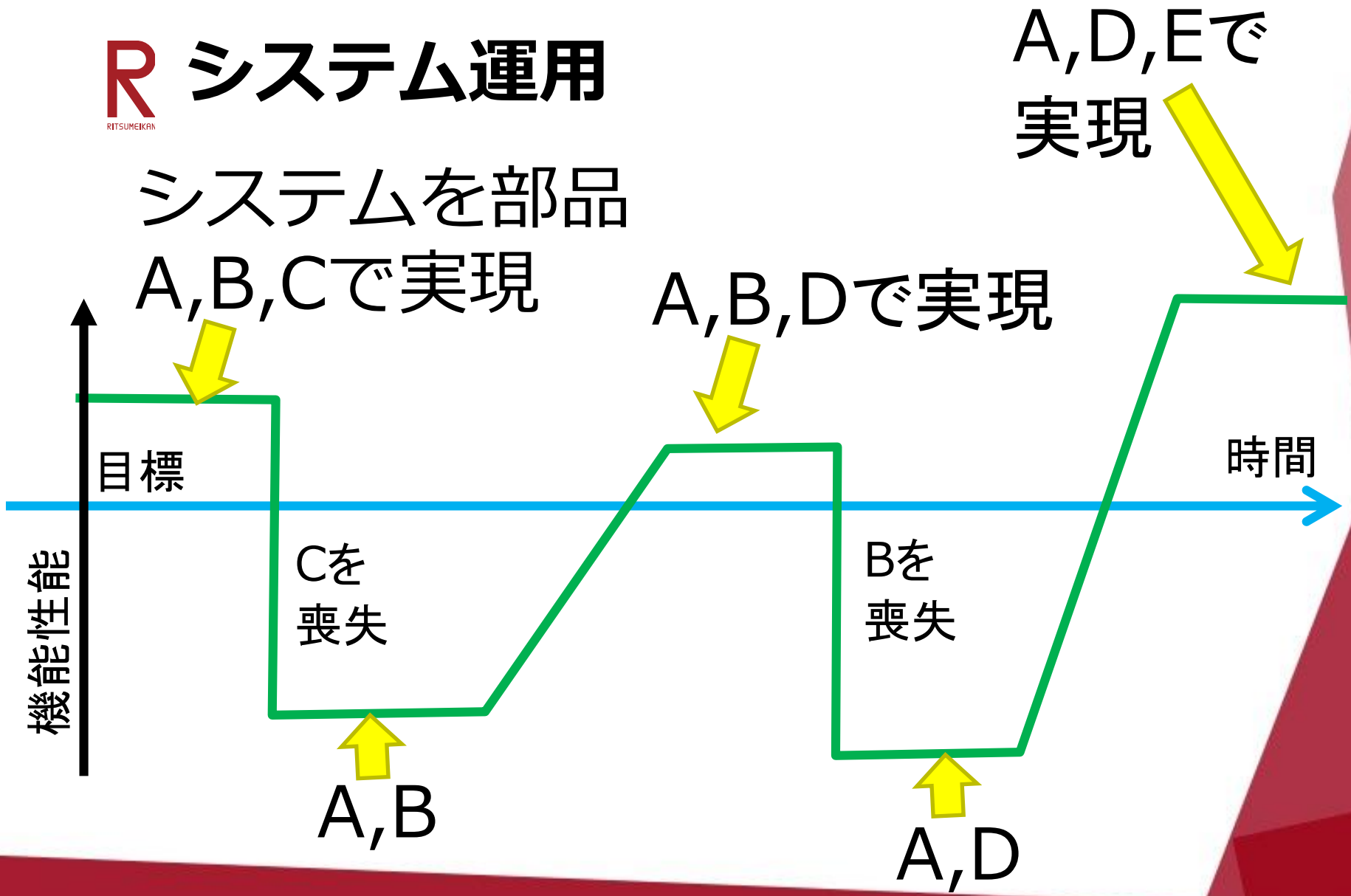
線形ではなく多変数で表現する複雑系モデル

# システムを積み木に例えれば

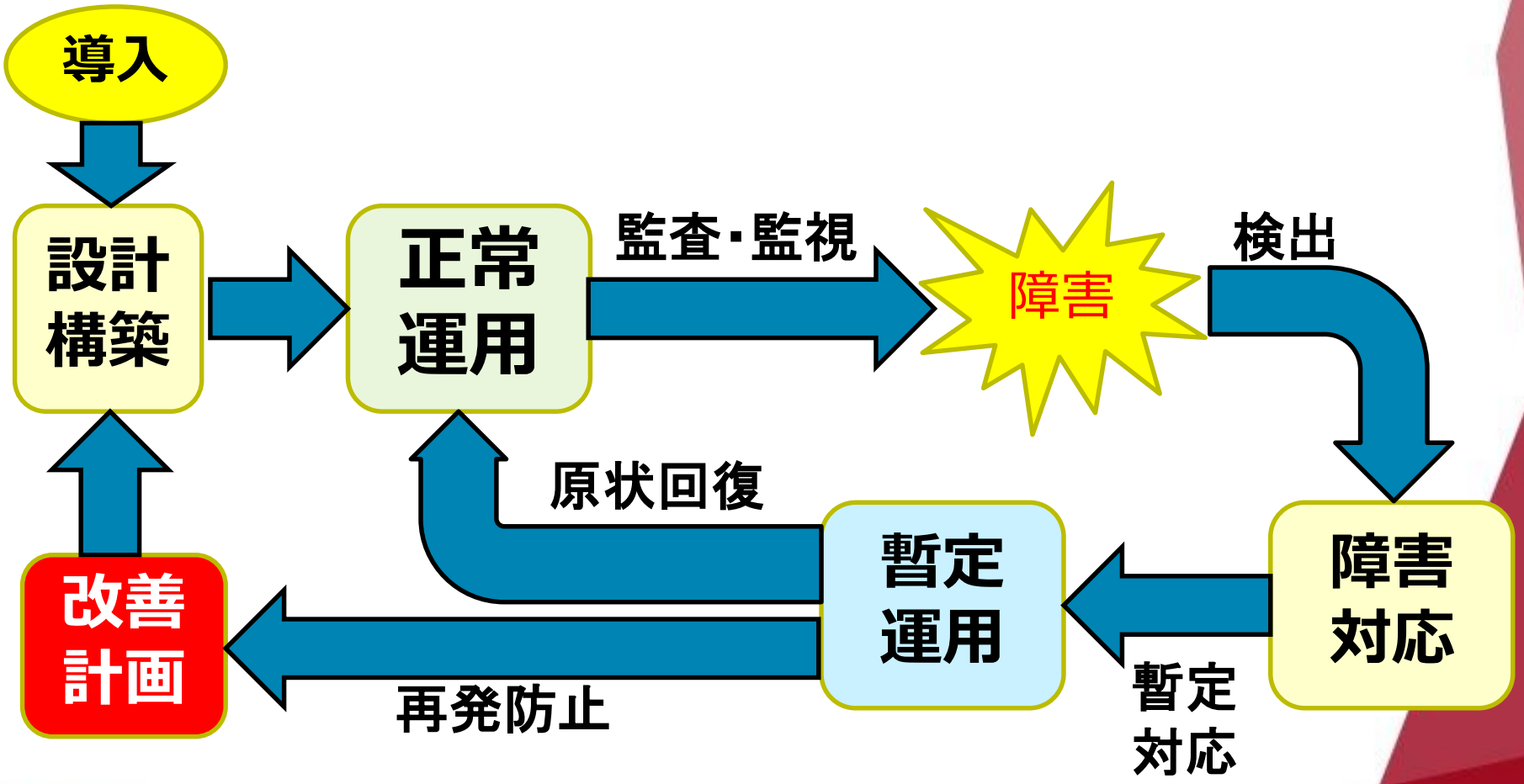


機能性能目標に達する部品の組み合わせは多様

# システム運用



# 情報システムの レジリエンス・サイクル



# 機能性能回復のためには…

- 目標を達成するための組み合わせを選ぶ

- 原状回復で済む場合は部品復旧
- 部品を復旧するだけでは済まない場合…（深いバグ・セキュリティ事案）
  - 改修して使う
  - 完全に別のものにする（構成変更する）

- 交換すべき場所・改修すべき場所を素早く特定し運用状態に戻す必要

# 高いレジリエンスのための一般則

- 部品はできるだけ少なく（単純性）
- 部品同士の依存は少なく（独立性）
- 部品の健全性が測定可能（測定可能性）
- 部品が故障しても補完可能（冗長性）
- 異なる手法による補完が可能（多様性）
- 予防的措置が可能（脆弱性対応など）
- 潜在的故障を含め早期発見が可能
  - システム性能の可視化・異常の早期検出

# 具体的には…

- 冗長性の確保
  - システムの二重化、ホットスタンバイ…
  - 課題：コスト、システム複雑化
- 多様性の確保
  - 重要なシステムは異なる方法での冗長化を行う
    - 例えば通信経路と手段
  - 課題：コスト、システムの複雑化
- 単純性の確保
  - KISS原則に基づけば単純なシステムほど障害に強い
  - 課題：冗長性などとの矛盾
    クラウド等外部システム利用との連携との矛盾

# 高いレジリエンスを自ら証明する Chaos Engineering

RITSUMEIKAN

**サービス障害を起こさないために、障害を起こし続ける。逆転の発想のツールChaos Monkeyを、Netflixがオープンソースで公開**

2012年8月8日

米国でビデオオンデマンドサービスを提供しているNetflixは、Amazonクラウド上でわざとシステム障害を起こすためのツール、Chaos Monkeyをオープンソースで公開しました。

Chaos MonkeyはAmazonクラウド上で使うツール。Amazonクラウド上のインスタンスをランダムに落としまくることで、サービスに対して仮想的な障害を引き起こしてくれます。

NetflixはこのChaos Monkeyを実環境で使うことで、本物の障害が起きたとしてもサービスが継続できることをテストし続けてきました。Netflixのブログ「Chaos Monkey released into the wild」から引用します。

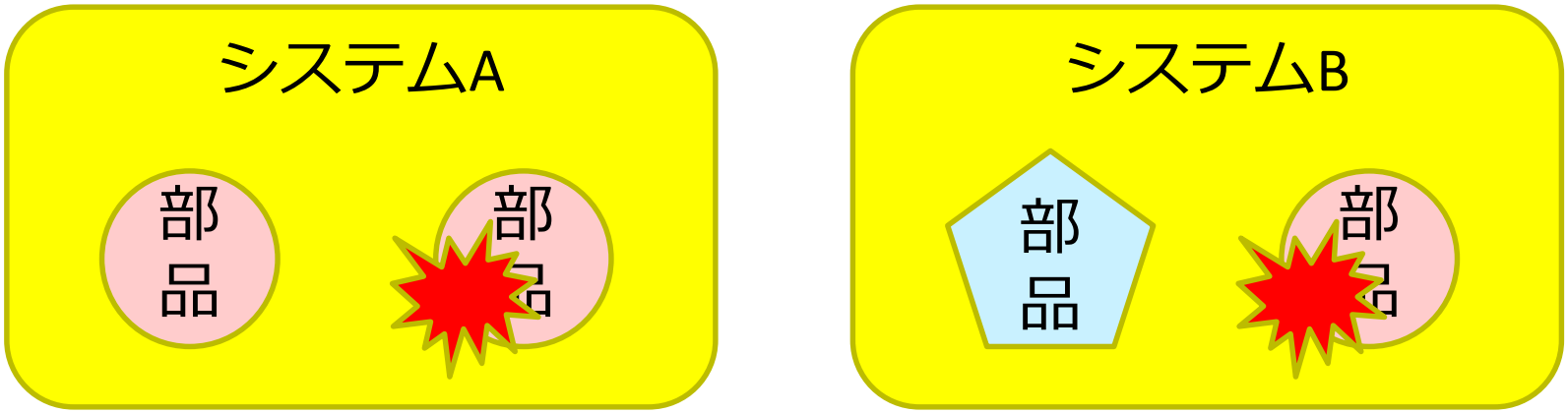
Publickeyより

わざと障害を起こすことでシステムの安定性を示し続ける

部品の独立性と冗長性が高いので出来るが…

Beyond Borders

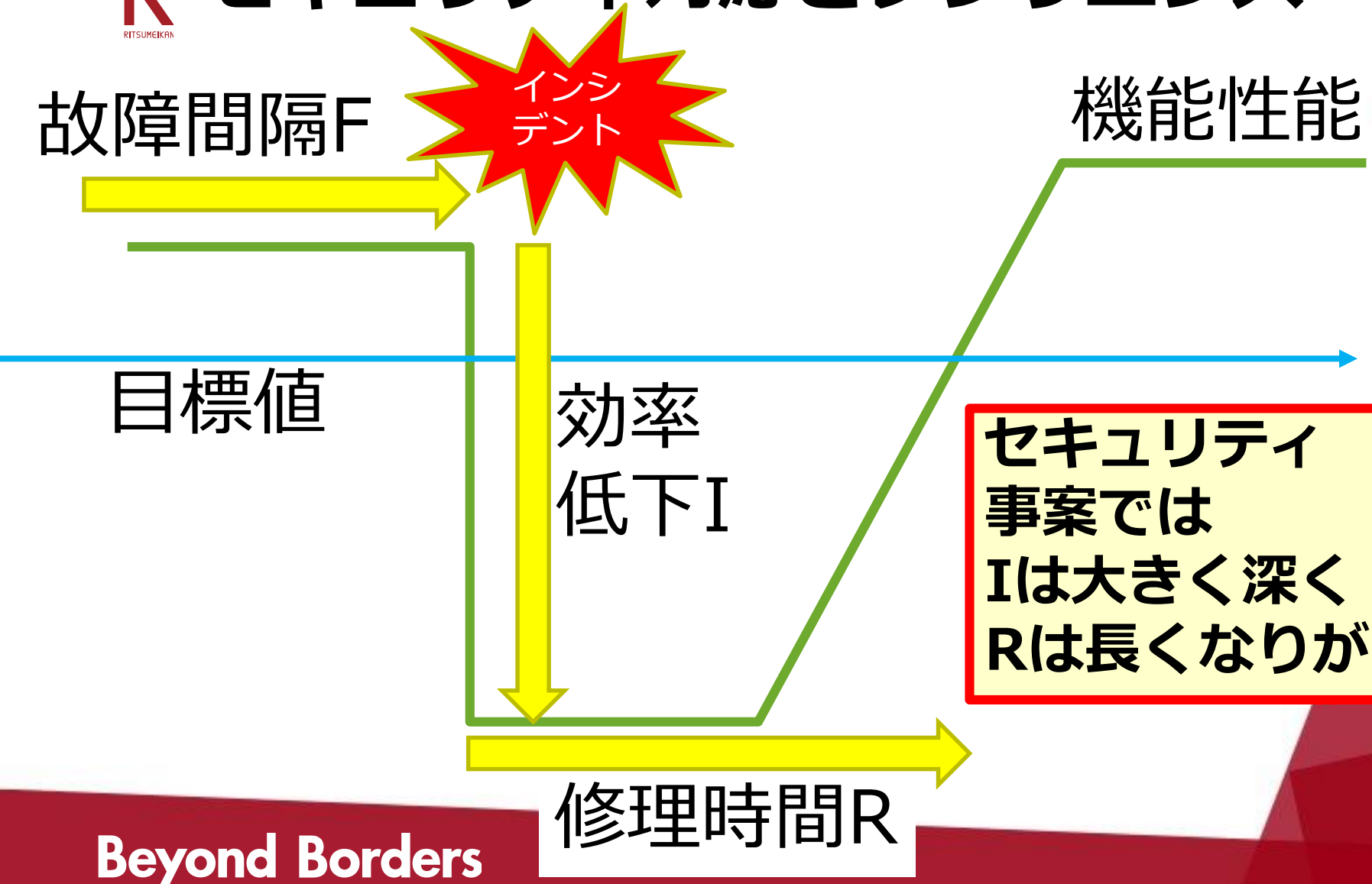
# 単純なChaos Engineeringでは セキュリティ上の堅牢さを示せない




- 同一部品による冗長化は高い堅牢性
- セキュリティ脆弱性が見つかる時は同時

- ヘテロ構成は管理負荷を上げる…

# セキュリティ対応とレジリエンス




**セキュリティ事案では**
**Iは大きく深く**
**Rは長くなりがち**

# Iを小さくRを短くするために

- 脆弱性管理の徹底
  - 攻撃発覚前に脆弱性対策ができれば
    Iが抑えられ目標値を下回る前に対処可能
    Rが実質０になる

- 早期発見のための監視
  - 攻撃が深刻化する前に発見すれば
    Iを抑えられるし事象も単純になる
    結果としてRが短くできるはず

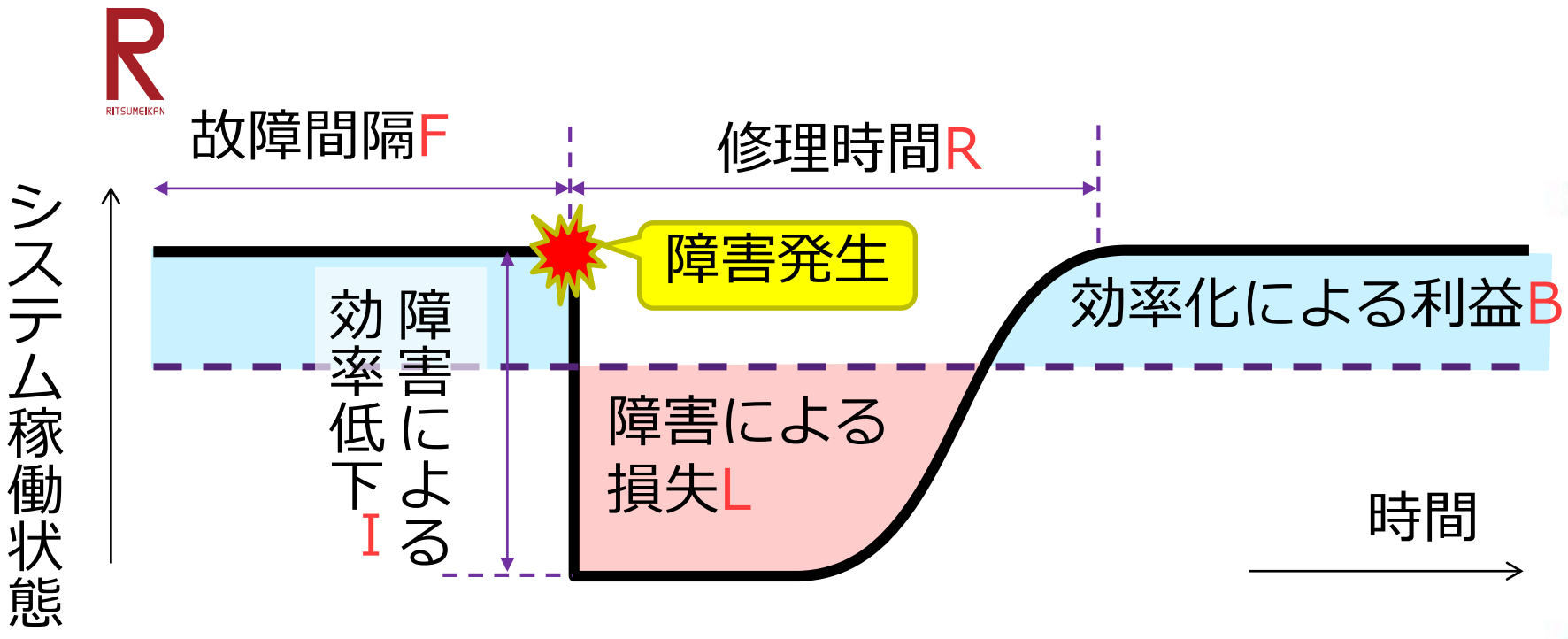
# もう少し深掘りすると

- アタックベクトルを減らす
  - 攻撃者がよく使うパターンはわかっているならば業務見直しでそのアタックベクトルを封じ込めることはできないのか？
    - 例えば「メールにファイル添付して送る」業務は必要か？！
- システムを堅牢にする
  - 脆弱性が出にくい/出ても攻撃しにくい設計（Security by Design）
  - 認証系の堅牢さ向上

# 「故障間隔F至上主義」との闘い

- 「動いているものは触るな原則」とのジレンマ
  - 脆弱性修正のためのパッチ→検証の工数が…
  - 部品のEOL等に伴うシステム更新→安定稼働まで大変…
    - 特にマルチベンダ環境や外部SI業者・システムを巻き込んだ環境では安定までの作業量が膨大に

- 迅速な安定化のためにもシステム全体を常に理解し把握する必要
  - 「原課調達」に歯止めが必要
  - 内部情報部門への情報の一元化
  - 適切な監視ツールの利用

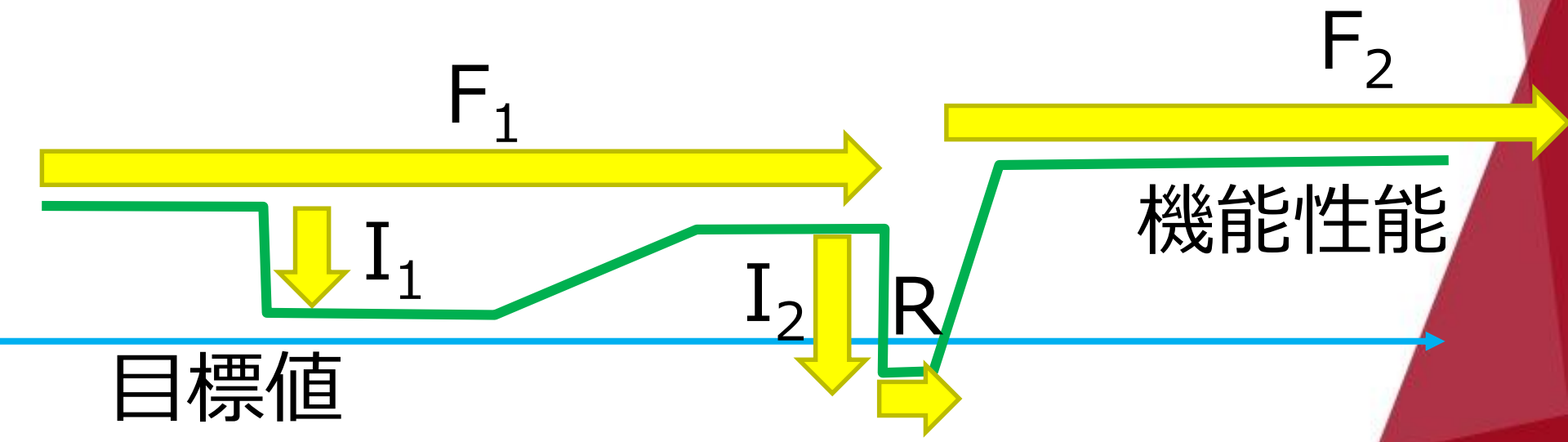



利益Bのためには
Fを長くすれば
良いのだな…
耐故障に投資…

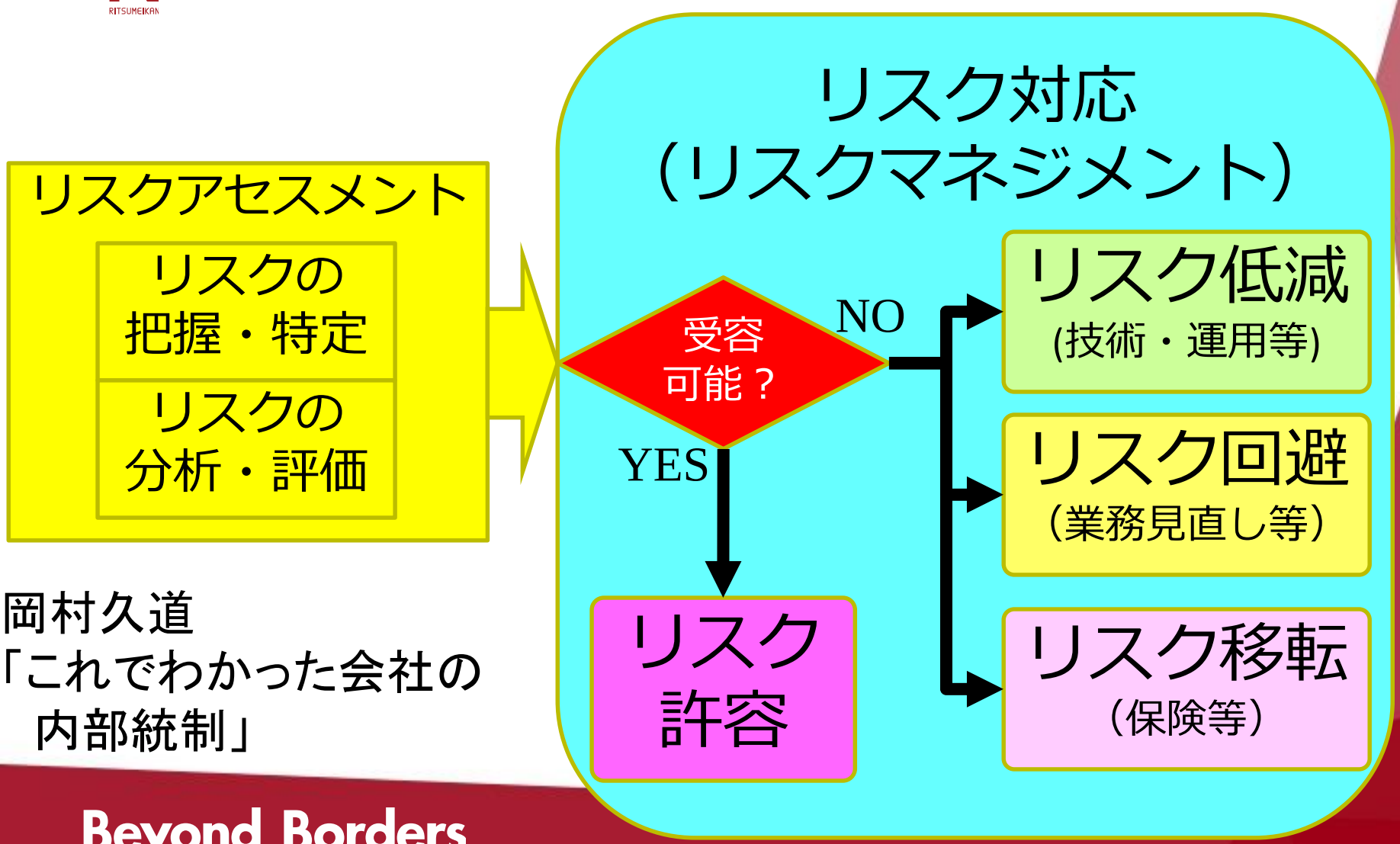
まずIとRを！
総損失はΣ（L×P）
P=R/(F+R)です！

# 我々は経験的に知っている…

- セキュリティにとっては故障間隔Fより効率低下Iと修理時間Rを抑える方が大切
  - IとRを抑えるための活動が結局Fを延ばす

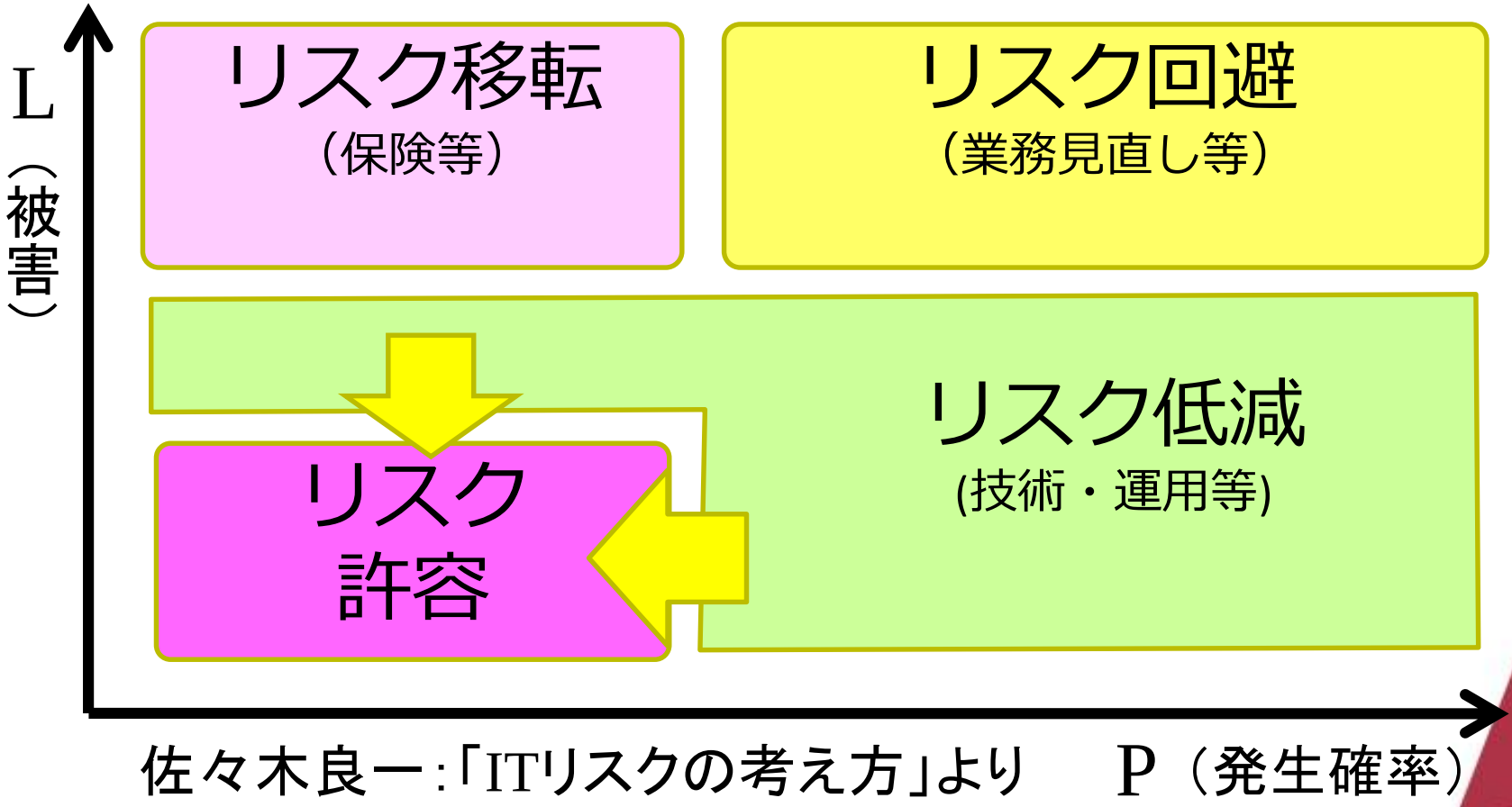


# まずはリスクの把握と評価

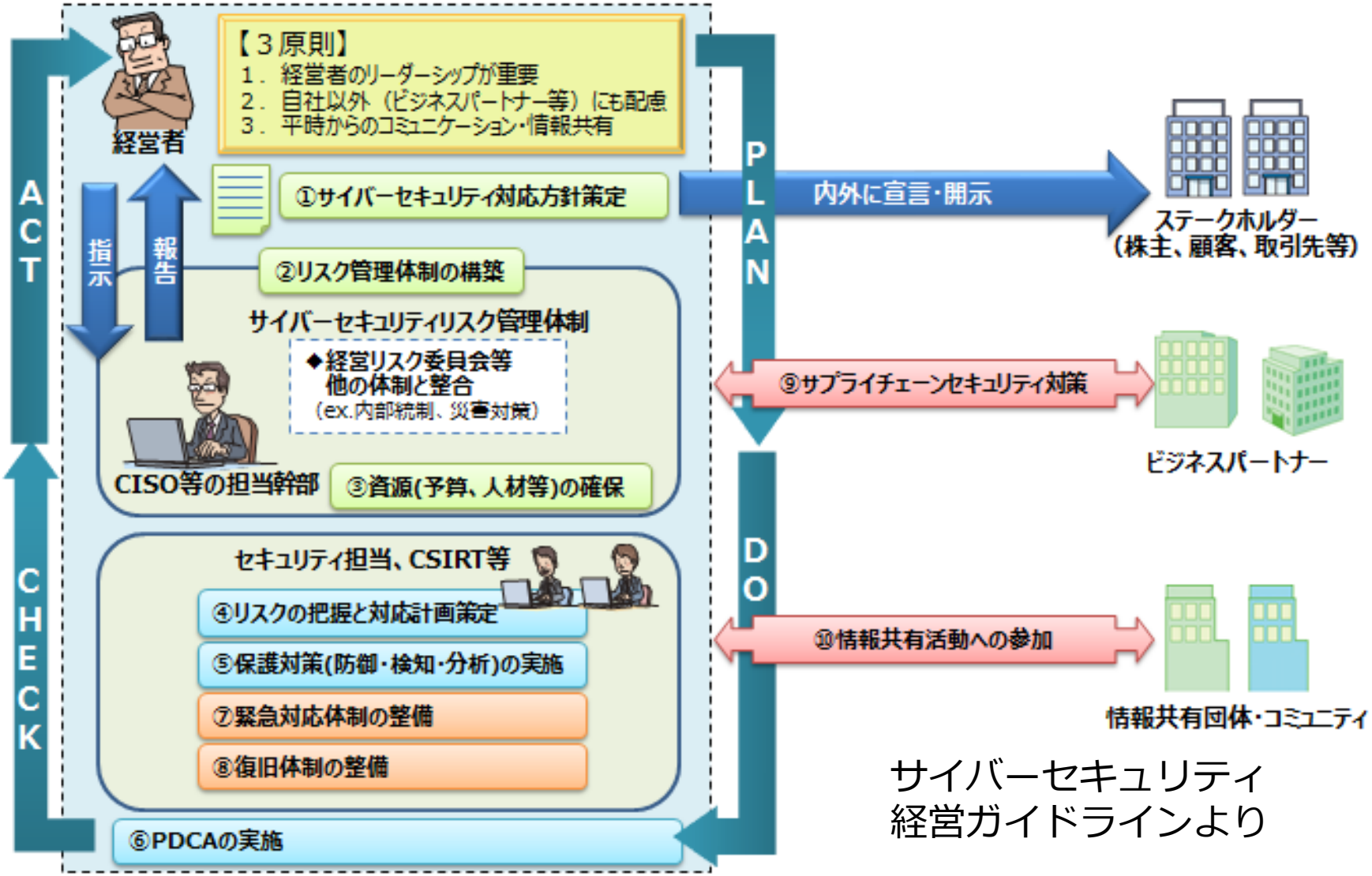



岡村久道
「これでわかった会社の
内部統制」

# リスクの大きさ・確率と対応の関係



# まずはガバナンスから




サイバーセキュリティ
経営ガイドラインより

# サイバーセキュリティ経営ガイドライン Ver 2.0

- サイバーセキュリティ経営の３原則
  1. 経営者は、サイバーセキュリティリスクを認識し、**リーダーシップによって対策を進める**ことが必要
  2. 自社は勿論のこと、ビジネスパートナーや委託先も含めた**サプライチェーンに対するセキュリティ対策**が必要
  3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、**関係者との適切なコミュニケーション**が必要

これに沿った重要10項目を提示

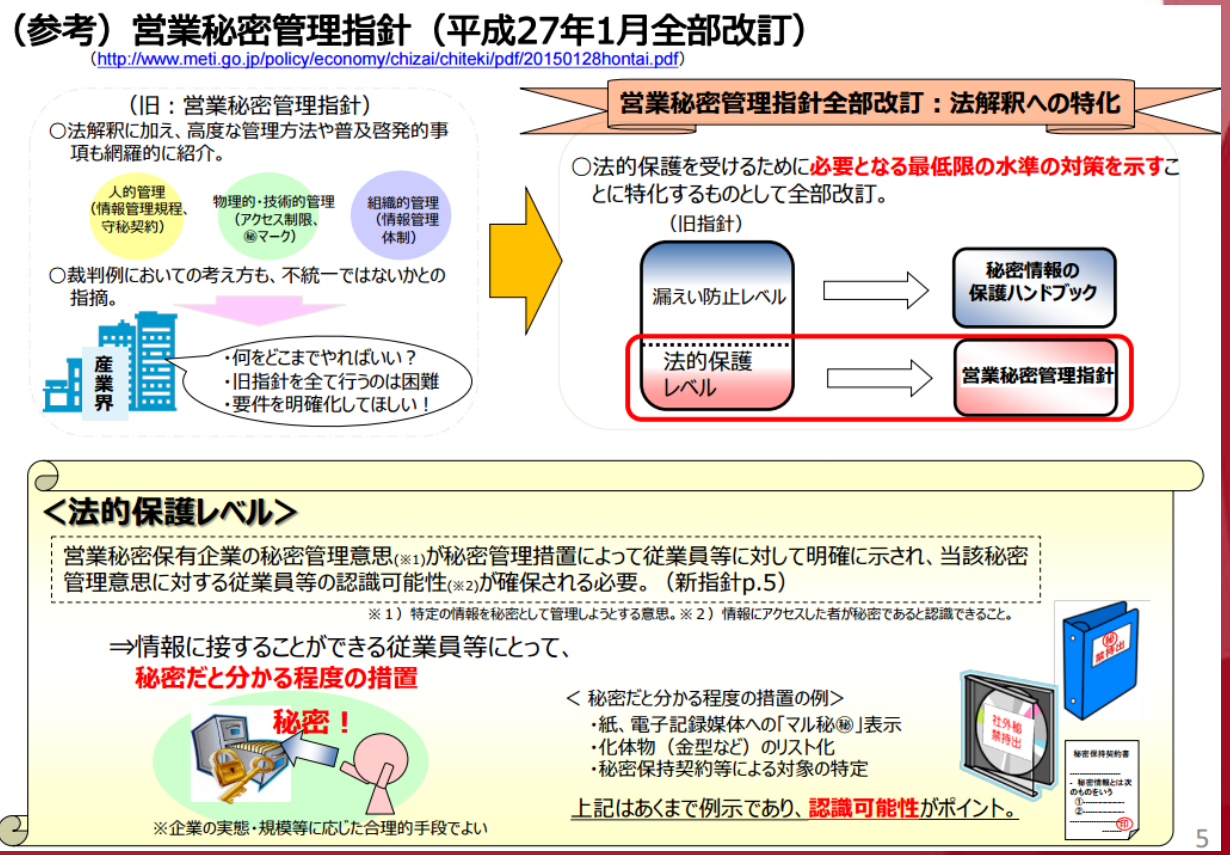
セキュリティそのものを投資と捉えるべきとする記述を強調
リスクマネジメントの考え方を明記

# 2015年「営業秘密管理指針」改定

- 実に12年ぶりの全面改訂
  2018年11月さらに小改訂

旧指針が事実上
「秘密管理性」
を規定したため
適用範囲を
狭めていた

改定により
広範に
適用可能に



資料がとても充実
全部Webから取れます

くすぐりが良い!

# 秘密情報の保護ハンドブック

～企業価値向上に向けて～

平成２８年２月

経済産業省

# 情報管理も企業力

～秘密情報の保護と活用～

秘密情報の保護ハンドブックのてびき

営業秘密管理指針→保護ハンドブック→ハンドブックのてびき！

# 情報セキュリティマネジメント試験
# 情報処理安全確保支援士

RITSUMEIKAN


国家試験

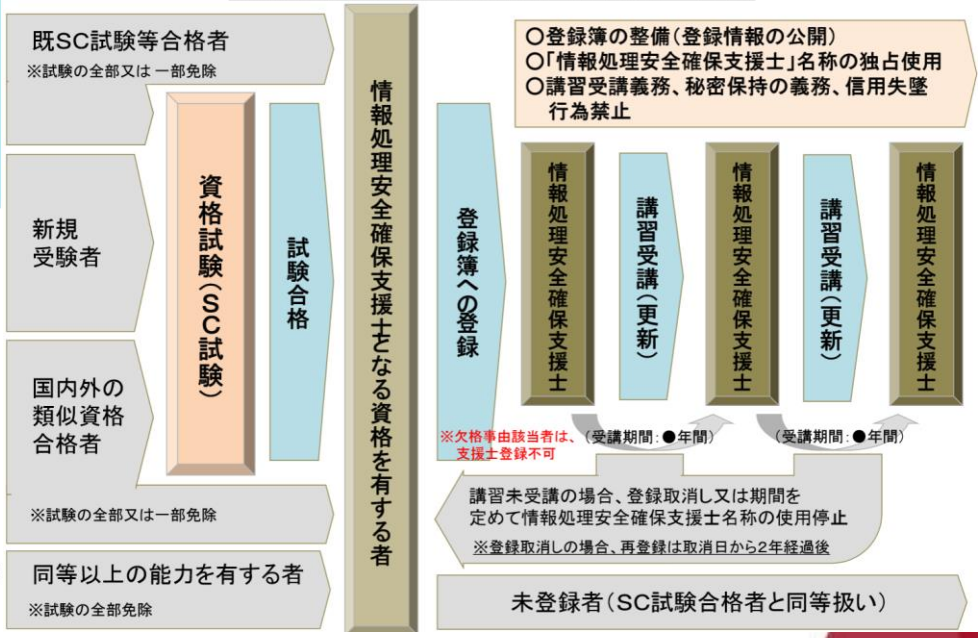
## 「情報セキュリティマネジメント試験」とは？

NEW!

ITの高度化やインターネットの普及が社会に様々な恩恵をもたらす一方、サイバー攻撃の手口はますます巧妙化・複雑化し、社会全体に対する非常に大きな脅威となっています。

「情報セキュリティをいかに確保するか」は今や組織にとって大きな経営課題ですが、標的型攻撃、内部不正などの多種多様な脅威は、「ITによる対策（技術面の対策）」だけではなく、適切な情報管理、業務フローの見直し、組織内規程順守のための従業員の意識向上といった、「人による対策（管理面の対策）」についてもしっかりとした取組みが重要です。
そのための情報セキュリティマネジメントを担う人材の育成をいかに推進していくかが、社会全体での課題であると言えます。

「情報セキュリティマネジメント試験」は、このような社会ニーズの高まりを背景に、政府の『「日本再興戦略」改訂2015』（平成27年6月閣議決定）や経済産業省 産業構造審議会で示された方向性を踏まえて、国家試験「情報処理技術者試験」の新たな試験区分として創設されました（平成28年度春期から試験開始。春期（4月）、秋期（10月）の年2回実施）。




あたらしい資格試験
より経営サポートをする層を創出

従来の情報セキュリティ
スペシャリスト
試験合格者を中心に「士業」に
登録・更新制を採る

この辺が情報漏洩保険等に効いてくる　リスク対応力向上にも？

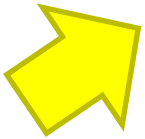
# 言うは易しのSecurity by design

- 設計開発する立場でも
  まだ「相場観」はない
- 多くは調達する立場
  なかなか外形的に
  確証を得るのは
  難しいが…

情報システムに係る政府調達における
セキュリティ要件策定マニュアル

2015 年 5 月 21 日

内閣サイバーセキュリティセンター



とりあえずはこれだが
クラウド対応がまだ入ってない

# かといって運用でカバーは現場に負荷が高すぎる

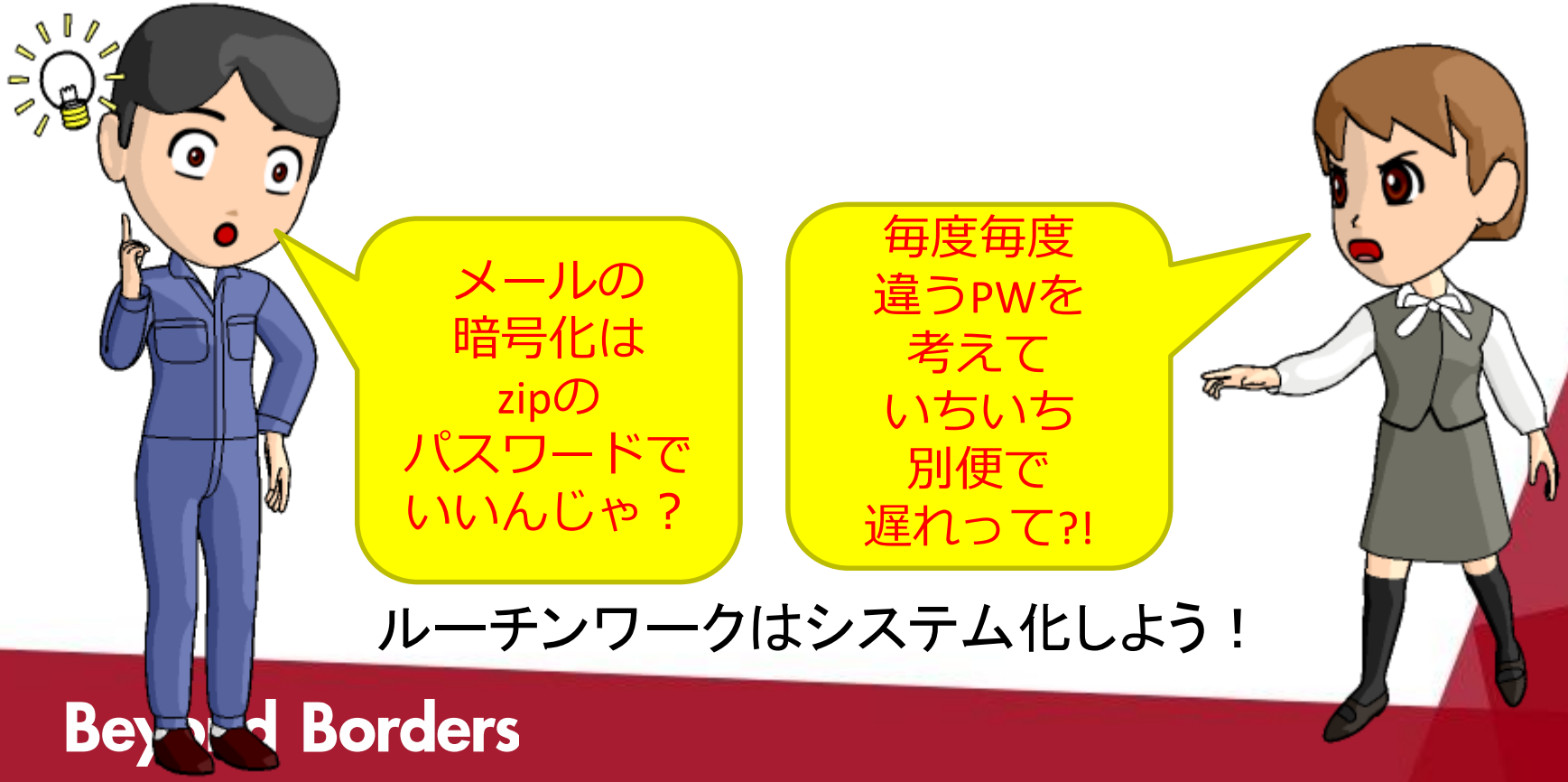
アクセス制御が厳しくて手順が増えた
添付ファイルは必ずパスワード？
忙しいのに研修やらe-Learning必修
上司への報告や承認も増えたし
とにかく何かと窮屈になった

別に私、悪いことしようと思ってないのに信用されてない感じがイヤ…

Beyo ロイヤリティを下げては逆効果！

# そもそもどうしてIT化してるのに効率が落ちるのか

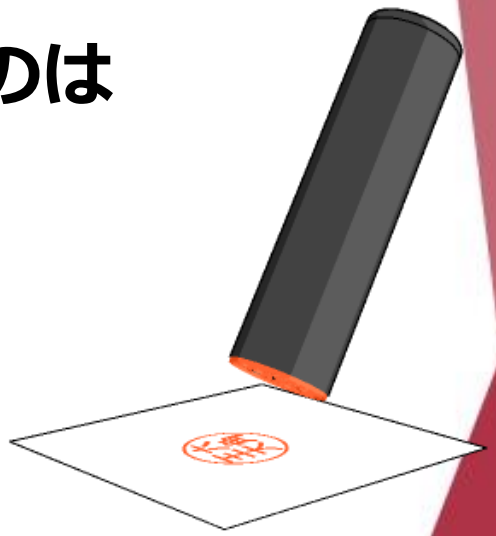
- ルールを決めるのはいいが**実装がひどい**
  監査要件を満たすためだけのものが多い




ルーチンワークはシステム化しよう！

# 本当に必要なのは何か？

- 情報システム全体を
  最初からセキュリティ対策しておくのは
  もちろんのこととして・・・
- 「仕事のやり方」を変えて効率化を
  - いつまで情報機器を清書機にするのか
    いつまで「印鑑文化」を維持するのか
  - 可能な限りのシステム化を！
- セキュリティ対策で
  「業務効率が常に下がる」のは本末転倒
  「結果的に業務効率が上がる」ことを示し
  「業務のやり方を変える」ことを
  現場に受け入れさせられるかが勝負では？！



# 脆弱なのはシステムではなく「人」
# 人にデータを食わせるWebとメール

- 狙われているのは人が直接データを扱う機会
  内部犯行でもサイバー攻撃でもリスク
- 業務フローを見直してシステム化すれば
  セキュリティが向上し業務効率も上がる！

CSVを落として
列を加えて
コピペして
一部手で直して
再度Upload…

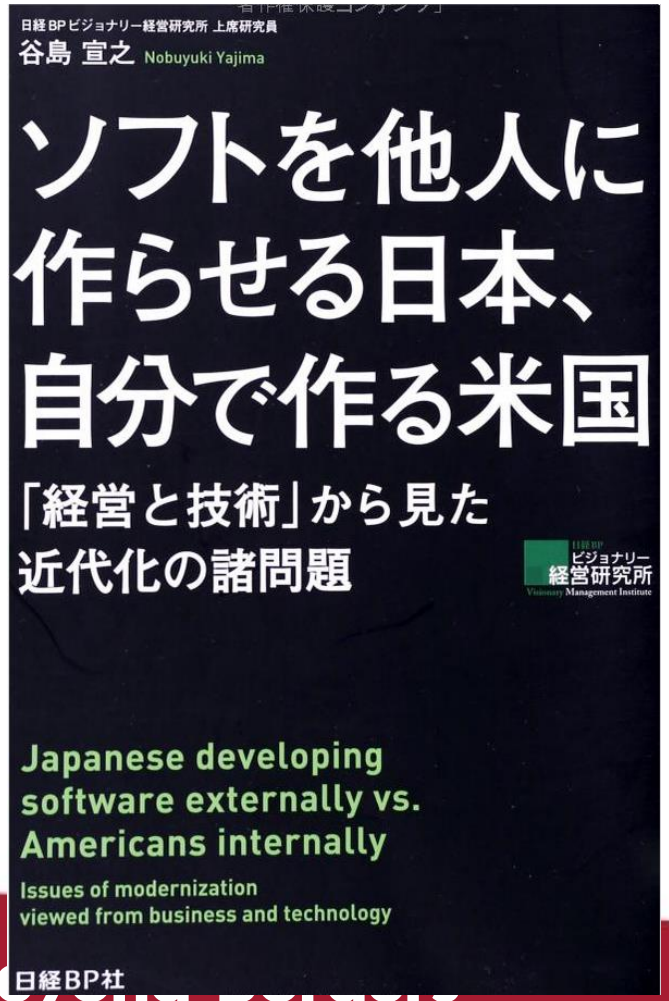
データ選択
クリック
おわり！

いうのは簡単だが現実は厳しい　例外処理…業務量…

# 経営陣に一番響くのは「儲かる」

特にIT企業においては
そもそも間接部門のIT化が
不十分であることが元凶
間接部門の効率化とセキュリティ向上は
両立できる、つまり「儲かる」はず
その知見を元に本来業務の
IT化と効率化＆セキュリティ向上を
それが実現できた時には
情報システムの「運用」こそが金を生む!

# 「技術経営の貧困」から抜け出す




- ユーザ企業こそがIT人材の活用を考えるべき
- 米国ではIT技術者の6割はユーザ企業に在籍
  日本ではITサービス企業に7割以上が在籍
  （IPA調査 2009年）

# まとめると…

- 情報システムには「人」も含まれる！
- 「運用」こそが金を産む
  運用を効率的に行うためには
  人も含めた効率アップが必要
- レジリエントなシステムと運用は
  「金の生る木」である！