

日本を遠くはなれた異国で、  
僕は空港と自分自身を  
建設している。



地図に残る仕事。  
**大成建設**  
TAISEI  
For a Lively World

～ 企業のリスク管理としての情報セキュリティ ～

2015年 1月20日  
大成建設株式会社  
社長室情報企画部

## 会社紹介 / 実績



鹿鳴館



国立競技場



羽田D滑走路

- 大成建設株式会社 Taisei Corporation
- 総合建設業を核とした企業グループ
  - 建築、土木、エンジニアリング、開発、不動産、その他
- 創業1873年（明治6年）
  - 創立141周年
  - 1917年に業界初の株式会社として設立

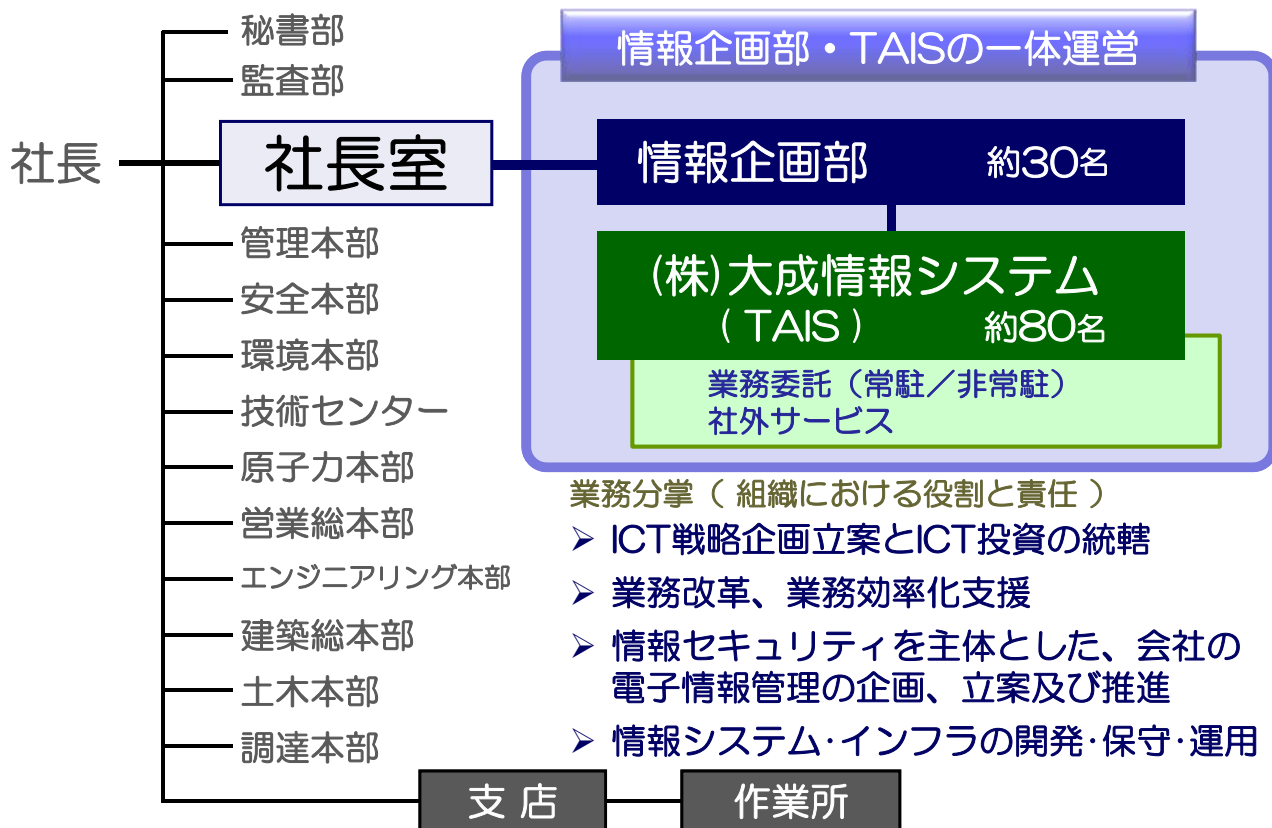
詳しくは、公開ホームページで

<http://www.taisei.co.jp/>

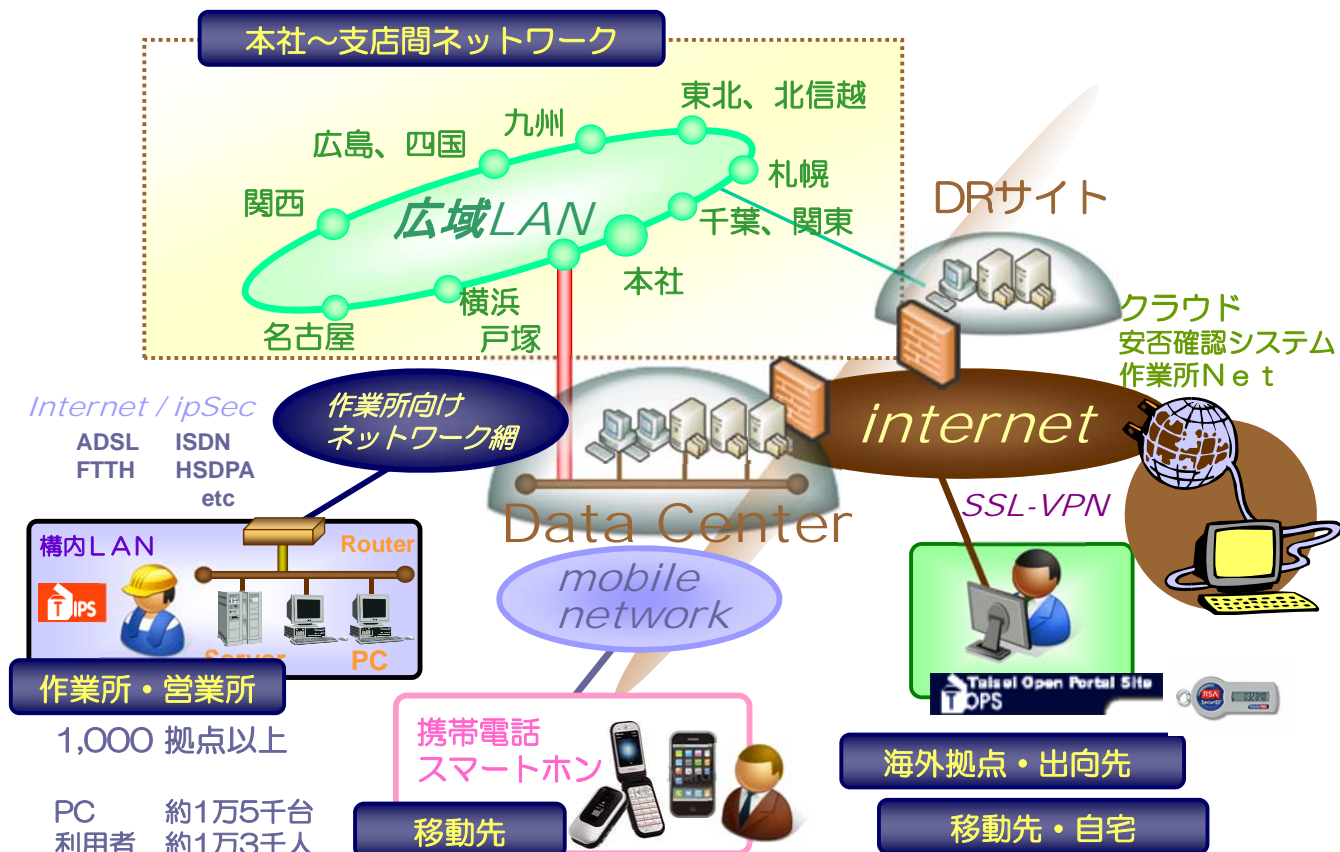
グループ理念：人がいきいきとする環境を創造する

グループスローガン： *For a Lively World*

# 組織体系



## 「情報」を共有するためのネットワーク



# 最強の情報セキュリティインフラとは

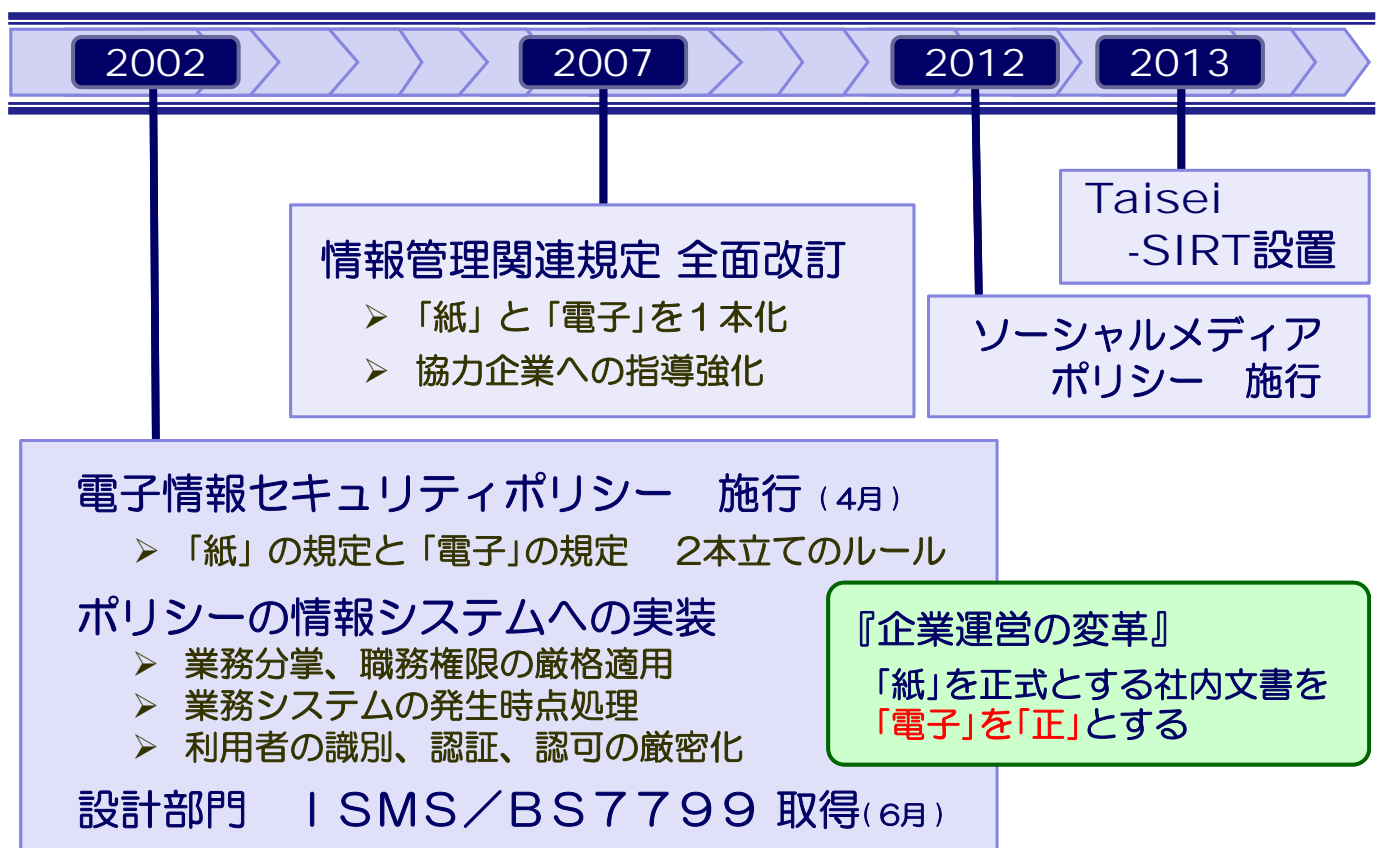
守るべきはPCやネットワークでなく『情報』そのもの。  
守るための「最強の情報セキュリティインフラ」とは・・・

## ルールと体制

- 社内規程、ガイドライン、マニュアル
- 組織、運用体制

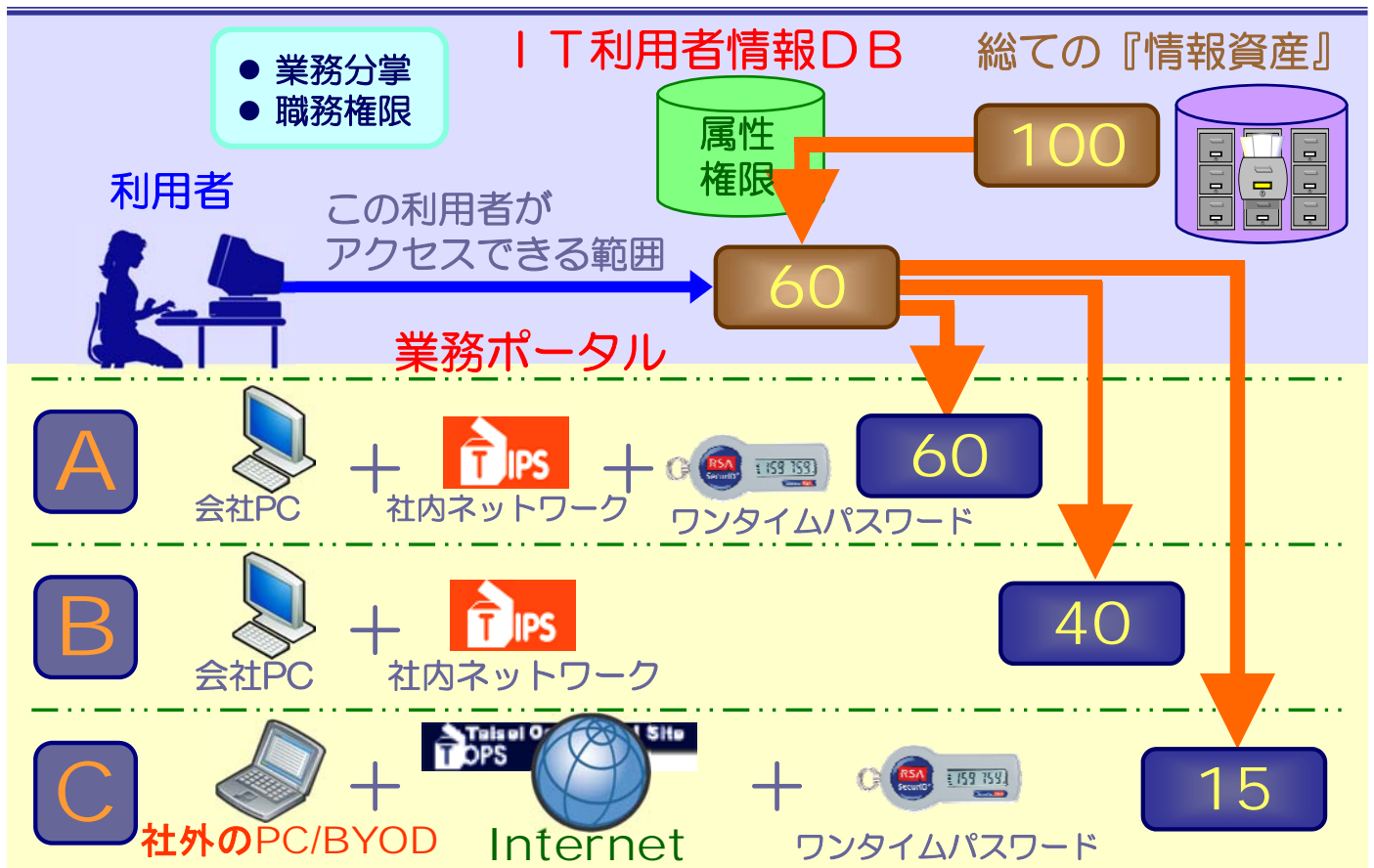


## 情報セキュリティ関連規定整備の変遷





# セキュリティポリシーに準じた情報開示 (2002年)



All rights reserved, Copyright© 2015 TAISEI Corporation

7

TAISEI CORPORATION

## 最新セキュリティ事情 「T-SIRT」の視点から



企業のリスク管理としての情報セキュリティ

8

# 東京駅 「新幹線記念碑」



## 半世紀前の偉業

東京オリンピック開会式の9日前  
1964年10月1日 開業

それは、東海道新幹線の18番19番線  
ホームに上がる階段の下にある



## 企業の経営環境と危機管理環境の変化

経営環境の変化

効率性を追求

スリム化  
スピードアップ  
最小人数による運営

分業化の進展

外部業務委託  
アウトソース  
クラウド化

グローバル化

多様化  
企業活動範囲の拡大  
24時間365日対応

IT化の進展 / IT依存度の増大

危機管理の変化

不確実性

想定外のインシデント  
マニュアル化の限界

複雑化

影響範囲想定の大難さ  
想定外の関連性

急拡大

爆発的なスピード  
広大な影響範囲

脅威の多様化

サイバー攻撃  
セキュリティ事故



自然災害  
広域災害

地震、津波、台風、  
噴火、大雪

非常事態

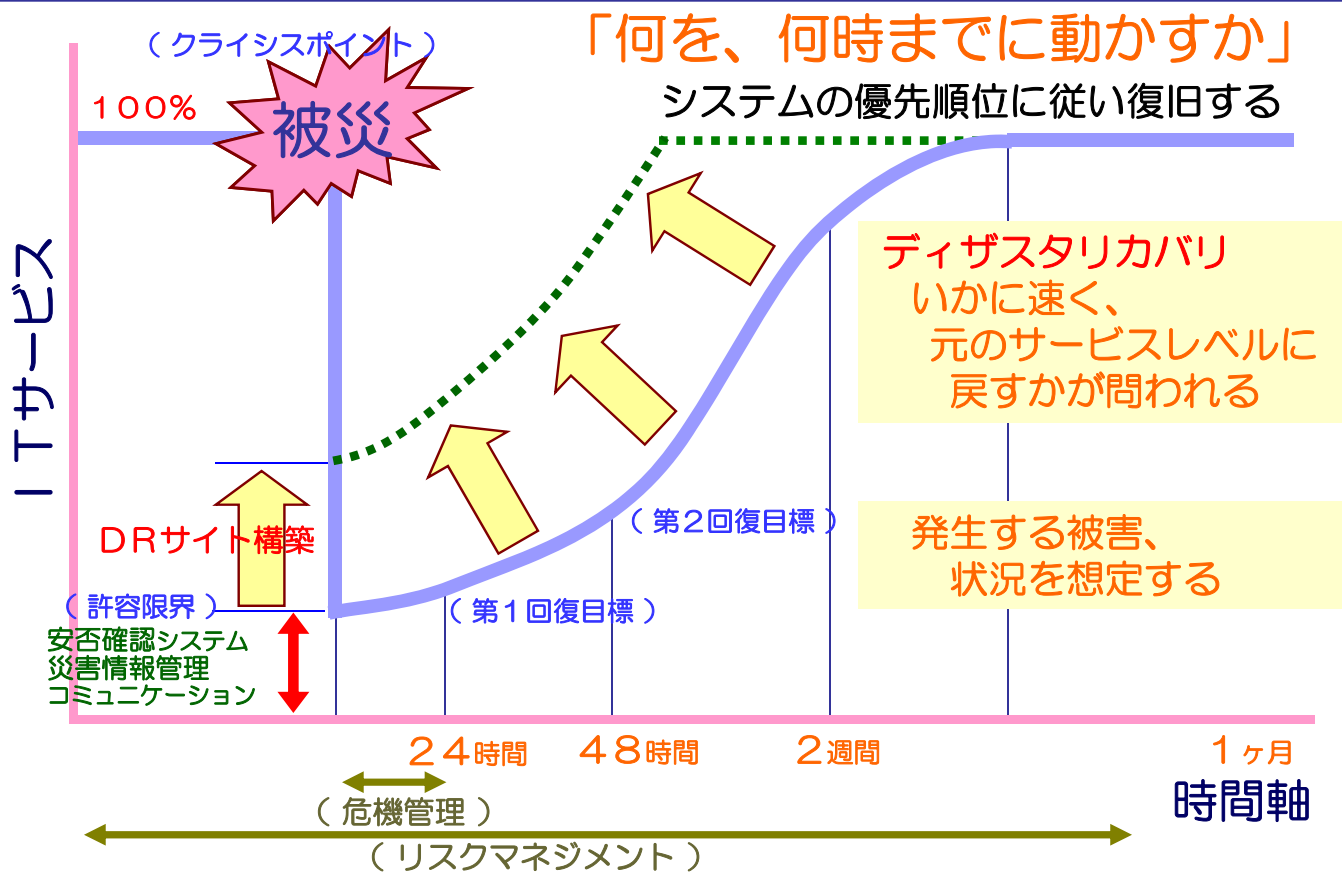
パンデミック、  
テロ、停電

企業の過失・犯罪

経営上の不祥事  
従業員の倫理違反



# 自然災害に対する情報システム継続イメージ



All rights reserved, Copyright© 2015 TAISEI Corporation

11

TAISEI CORPORATION

## 東日本大震災、わずか6日で高速道路を復旧

「世界が驚愕した奇跡の復旧」は復興への希望となった。  
3月22日には延べ870キロのうち約93%を応急復旧。  
この道路が、多くの人々の命を救った。

➤ 常磐道 水戸～那珂



被害状況 (3月11日)



復旧状況 (3月17日)

➤ 東北道 矢吹～須賀川



被害状況 (3月11日)



復旧状況 (3月17日)

他社の事例

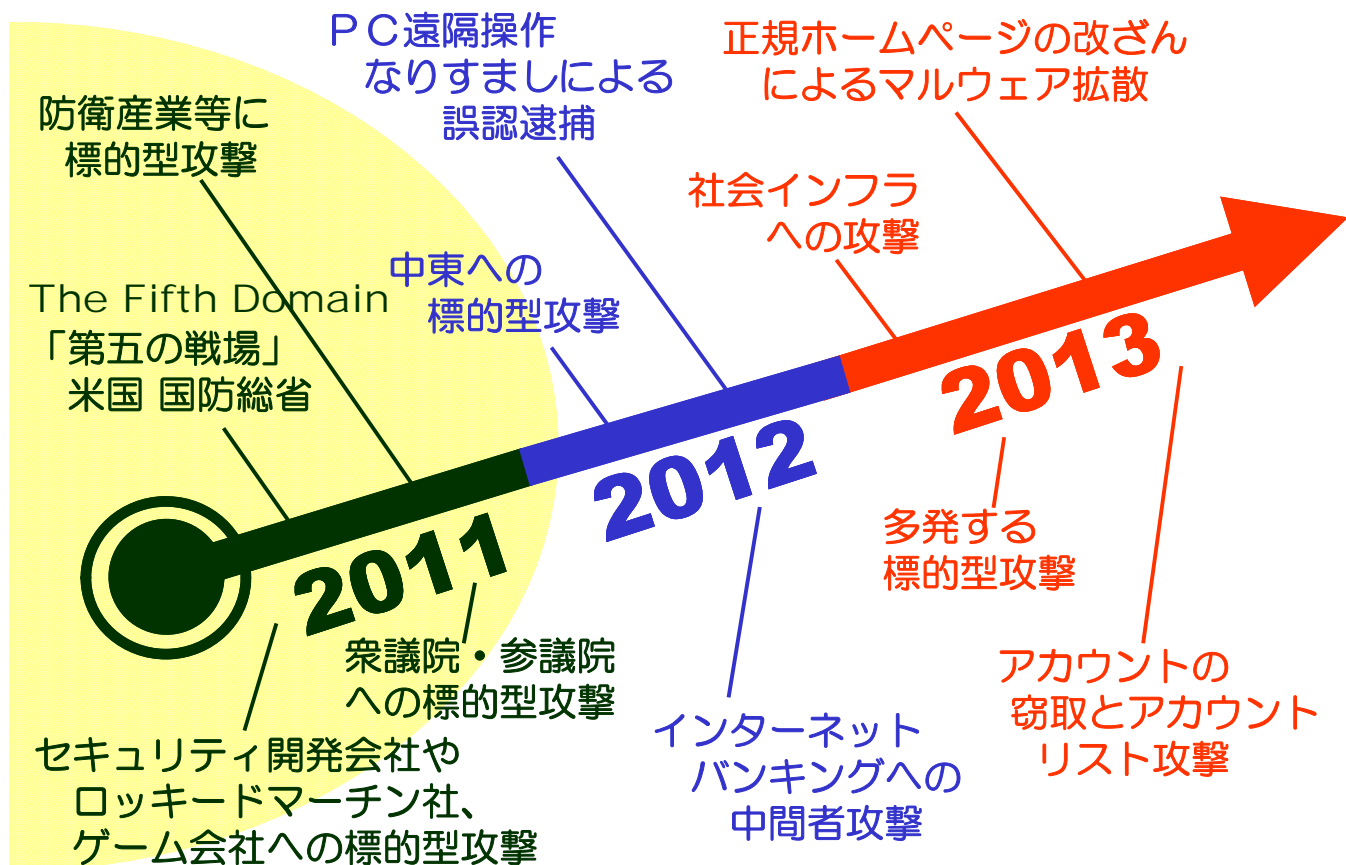
NEXCO東日本 プレスリリース 平成23年3月18日  
[http://www.e-nexco.co.jp/pressroom/pressr\\_release/head\\_office/h23/0318b/113.html](http://www.e-nexco.co.jp/pressroom/pressr_release/head_office/h23/0318b/113.html)

All rights reserved, Copyright© 2015 TAISEI Corporation

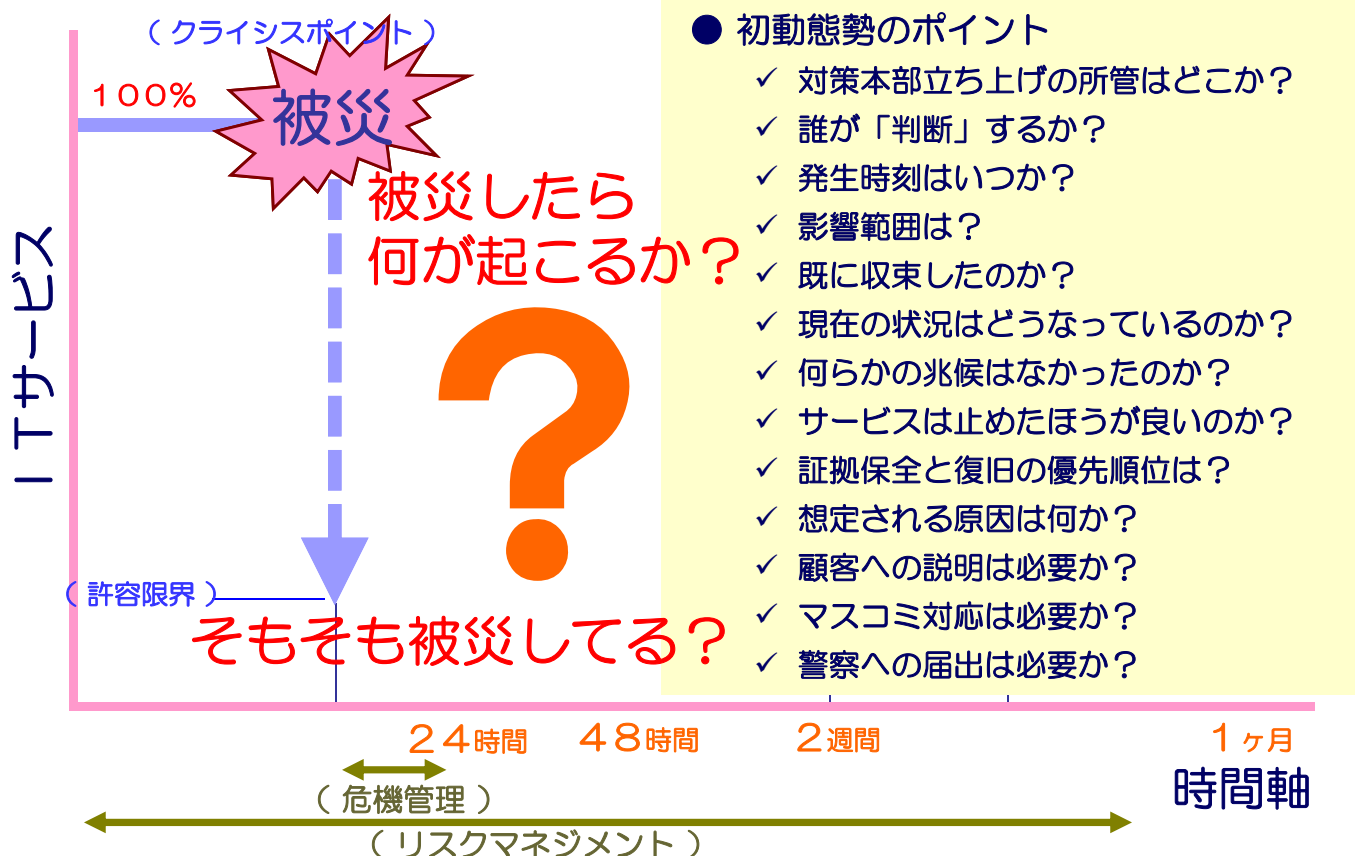
12

TAISEI CORPORATION

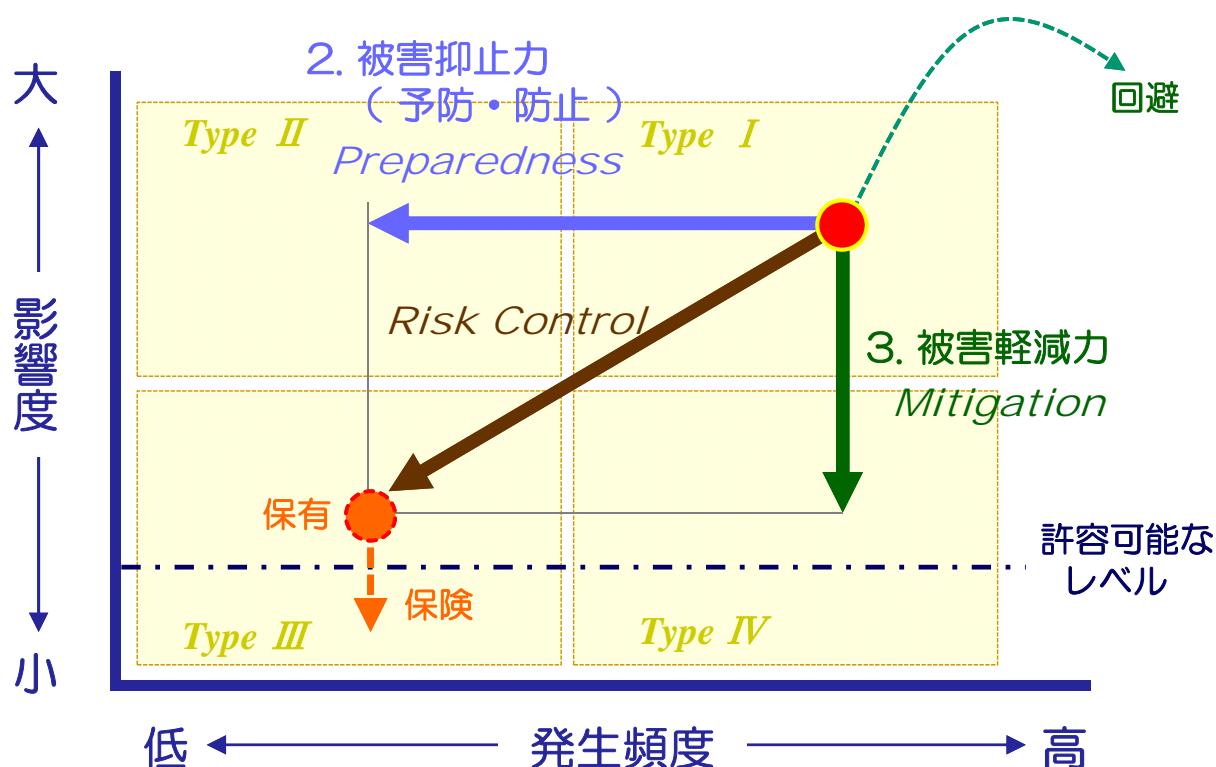
# 2011年に起こったことは大震災だけではない



## セキュリティに対する情報システム継続イメージ



# リスク戦略の基本パターン



## 一般的なアプローチ 脅威と対策（被害抑止、被害軽減）

	マルウェア	情報漏洩	盗聴	改竄	不正アクセス	侵入
ルール	情報セキュリティポリシー / ガイドライン					
利用者	情報公開(セキュリティホームページ、情報漏洩防止ホームページ)、通知・通達					
利用者	セキュリティ教育(e-ラーニング)、定期的な点検					
パソコン	適切なセキュリティ設定(標準環境の維持)					
以下を含む ・携帯端末 ・USBメモリ ・ハードディスク	パッチ適用	重要ファイルの暗号化		利用者認証		Personal Firewall
	ウィルス対策	操作監視				
	Personal Firewall	機能・装置制限				
	インベントリ管理					インベントリ管理
ネットワーク	検疫ネットワーク					検疫ネットワーク
	不審な通信遮断	通信の暗号化				不審な通信検知・遮断
		通信ログ管理				利用者の認証とアクセス制御
		アクセス制御				
		通信ログ管理				
認証 アクセス制御	利用者の識別とID管理					
	利用者の認証とアクセス制御、ログ管理					
	シングルサインオン					
サーバ	適切なハードニング/セキュリティ設定(標準環境)					
	利用者の認証とアクセス制御					
	ウィルス対策	ファイルの暗号化				
	パッチ適用	ログ管理				
インターネット		メール監査		Firewall		
	迷惑メール対策			侵入検知(IDS) / 侵入防止(IPS)		
	ウィルス対策(メール、Web閲覧)					
	Web閲覧制限(コンテンツフィルタ)					
	サービス利用ログの管理					



# 完璧主義から事故前提の体制へ

## 総務省における情報セキュリティ政策の推進に関する提言

2013年4月5日 情報セキュリティ アドバイザリーボード

「別紙3」 2ページ

「Ⅰ.基本的な考え方」より抜粋

「総務省における情報セキュリティ政策の推進に関する提言」について 別紙2

◇ 総務省では、有識者から助言を得ることを目的とし（座長：山口 英 奈良先端科学技術大学院大学教授）を  
◇ 本年4月、高度化・複雑化するサイバー攻撃など情報え、「総務省における情報セキュリティ政策の推進に関する提言」

**提言における基本的な考え方**

以下の5つの基本的な考え方に立ち、総務省は、内閣官房情報セキュリティ政策に取り組むことが求められる。

- ① 情報の自由な流通の確保**  
人間の尊厳、自由、民主主義など核心的な価値を推進するサ
- ② 過度な規制※によらない信頼できるサイバー空間の**  
イノベーションや経済成長を起こすサイバー空間の堅持。 ※情報セキュリティの名の下で行われる検閲など不合理な規制
- ③ リスク認識に基づく対応の強化（事故前提社会）**  
全てのサイバー攻撃を完璧に防ぐことは困難であるという認識の下での情報セキュリティ対策の実施。
- ④ 動的防御プロセス連携の確立**  
PDCAというサイクルにとらわれることなく、常に、動的に、適時適切な意思決定を行う「動的防御プロセス連携」の確立。
- ⑤ 国際連携によるサイバー空間政策の推進**  
我が国の経済成長を見据えた戦略的な国際連携の推進。

情報セキュリティに係るリスクは常に存在すること、**事前に全てを完全に防御すること（完璧主義）は重要であるが困難であることを認識した上で、リスクを考慮した社会意識、社会行動へ転換すること、また、このようなサイバー攻撃に迅速に対応できるよう、対処体制を抜本的に見直すことが必要となる。**

※ 総務省報道資料

[http://www.soumu.go.jp/menu\\_news/s-news/01ryutsu03\\_02000044.html](http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000044.html)

## ダメージコントロールという視点

ことは

事故・災害・戦闘で発生する不可避な損害に際して、その被害を最小限に食い止めるために行う**応急処置**。

また、非常時の応急処置を円滑に行うために用意される**事前の工夫と設備を含むが**、損害の発生そのものを未然に食い止める技術は含まない。

「マイナス」を局限することに成功した場合、それを「プラス」として評価する考え方。

# クライシスマネジメントとリスクマネジメント



All rights reserved, Copyright© 2015 TAISEI Corporation

19

TAISEI CORPORATION

## 情報セキュリティにおけるダメージコントロール

- 防御困難なサイバー攻撃や未知の攻撃が多発
- 事故前提社会における情報セキュリティ
- ダメージをコントロールして被害を局限する

攻撃されないように防御する対策ではなく、攻撃を受けても情報を窃取されない、あるいは攻撃をできるだけ早く発見し、重要情報の漏えいなどの被害をできるだけ小さく抑えるための対処、対応。

例えば、100万件の情報が持ち出される前に攻撃を発見し抑える、あるいは1万件の段階で抑える、ということ。

ダメージコントロールを成功させる

一刻も早く発見し、会社として判断／意思決定を行い、緊急時対応体制を立ち上げること

組織内  
CSIRT

All rights reserved, Copyright© 2015 TAISEI Corporation

20

TAISEI CORPORATION

# 企業における2つの情報セキュリティ施策

## CSIRTに要求されるもの

マイナスを減らす

必要な施策

### インシデント対応能力

- 迅速に対応体制を整える
- 目標時間内に解決する

対応体制  
実施計画  
(チェックシート)  
実践的訓練  
アセスメント

情報セキュリティ維持の  
ための管理プロセスと  
ツール主導の対策

ISO/ISMS  
ガイドライン  
検証・改善  
自主点検  
内部監査

プラスを増やす

## 日々の業務で要求されるもの

参考資料

## ISO/IEC 27000 取得事業者数推移

### Top 10 countries for ISO/IEC 27001 certificates – 2012, 2013

No.	countries	2012	2013
1	Japan	7,199	7,084
2	India	1,600	1,931
3	United Kingdom	1,701	1,923
4	China	1,490	1,710
5	Italy	495	901
6	Taipei, Chinese	855	861
7	Romania	866	840
8	Spain	805	799
9	Germany	488	581
10	United States of America	415	566

異常に多い  
日本の認証



※ ISO Survey (Survey Data)

<http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO%209001&countrycode=AF>



# ダメージコントロール実施組織 = CSIRT

Computer Security Incident Response Team

サイバー攻撃や電子情報セキュリティ事故に関する  
**緊急時対応を専門に扱う組織**

CSIRTは、機能ユニットの組織

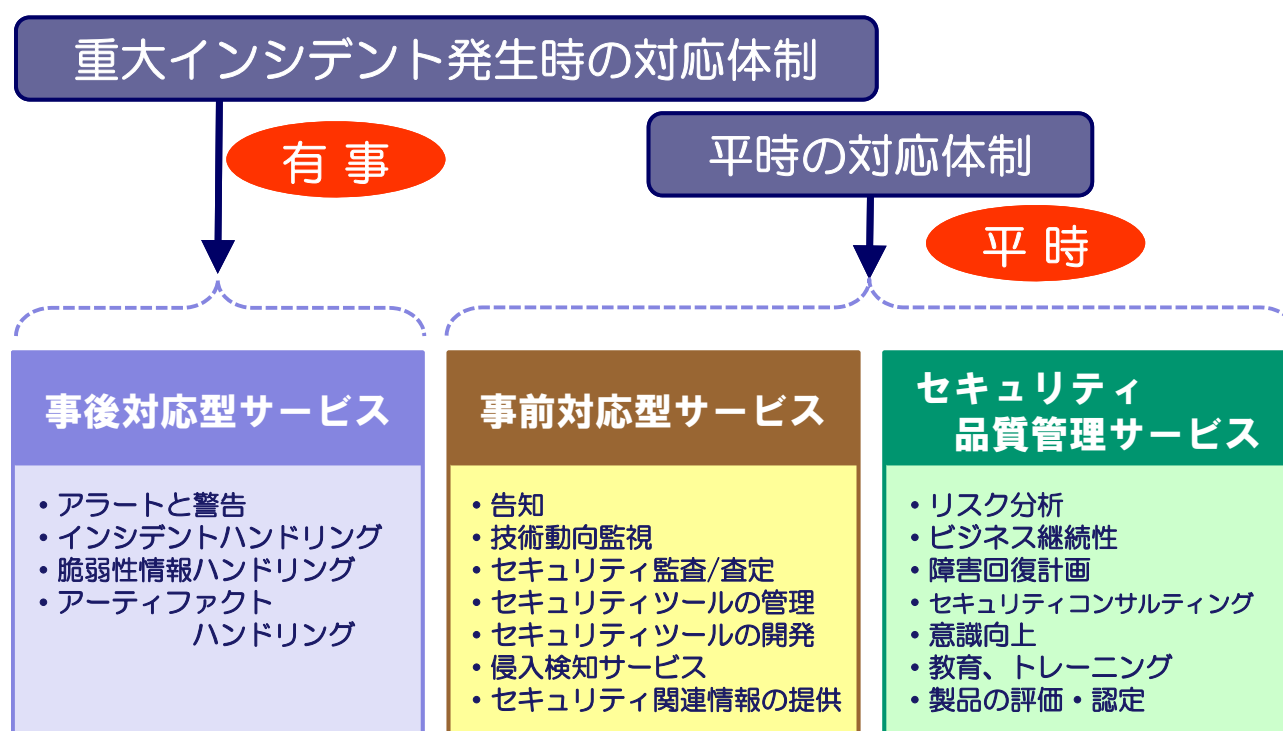
1. インシデント**対応窓口**(社内・外)機能
2. インシデントの検知・警戒をする機能
3. **被害の最小化**を図る機能
4. **情報の一元管理と技術・知識**が必要な  
要員のアサインや連携(社内・外)をつかさどる機能
5. 教育・啓発を行う機能

発見

局限

情報共有

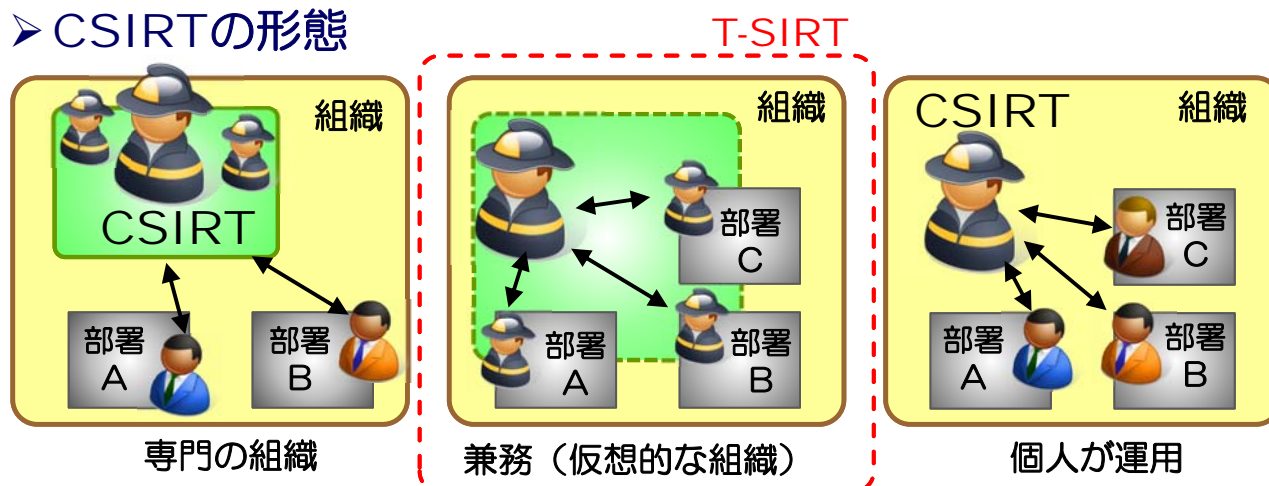
## CSIRTが提供するサービス



※ 「CSIRTのためのハンドブック」 2.3 CSIRTのサービス 参照  
[http://www.jpcert.or.jp/research/2007/CSIRT\\_Handbook.pdf](http://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf)

# 一般的な、組織におけるCSIRTの位置付け

## ➤ CSIRTの形態



## ➤ CSIRTの位置付け

### ◆ プロフィットセンター に CSIRT を設置

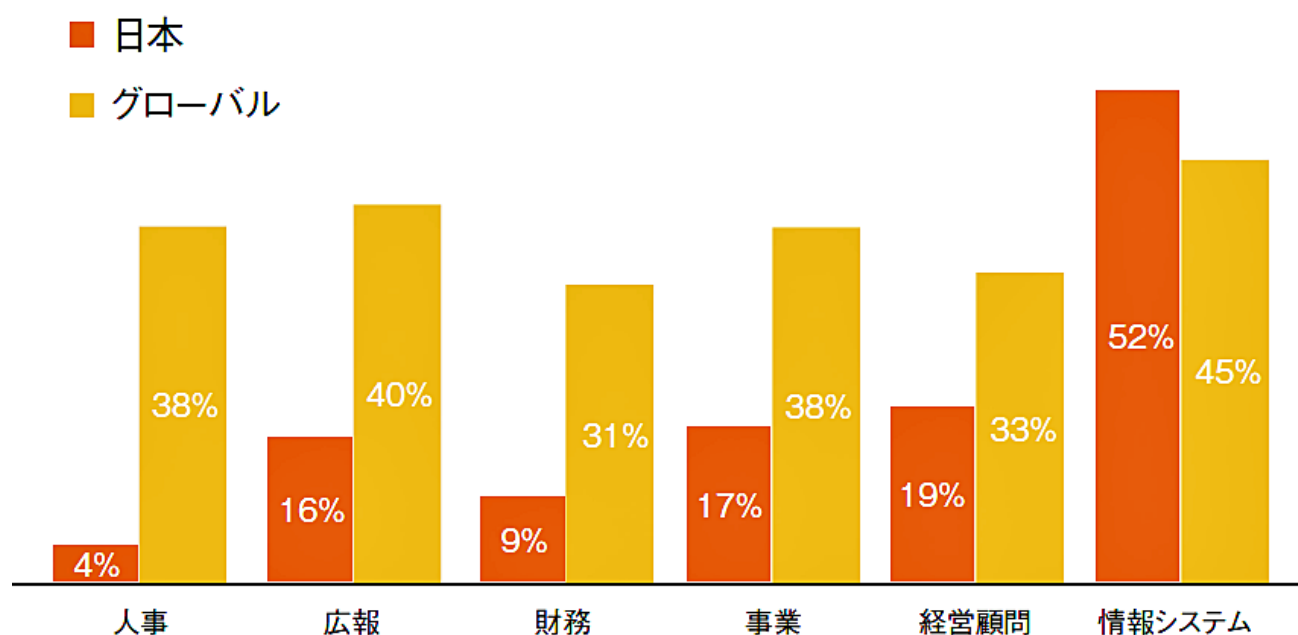
各種 ICT プロバイダ、インターネットバンクやインターネット・ショッピングなどを本業とする企業の CSIRT

### ◆ コストセンター

- ・ ~~コンプライアンス部門 に CSIRT を設置~~ T-SIRT
- ・ IT 部門 に CSIRT を設置

# 部門の枠を超えたインシデントレスポンス体制の構築

図 21 : インシデントレスポンスに関与している部門



プライスウォーターハウスクーパース株式会社  
「グローバル情報セキュリティ調査®2014」

<http://www.pwc.com/jp/ja/advisory/research-insights-report/information-security-survey.jhtml>

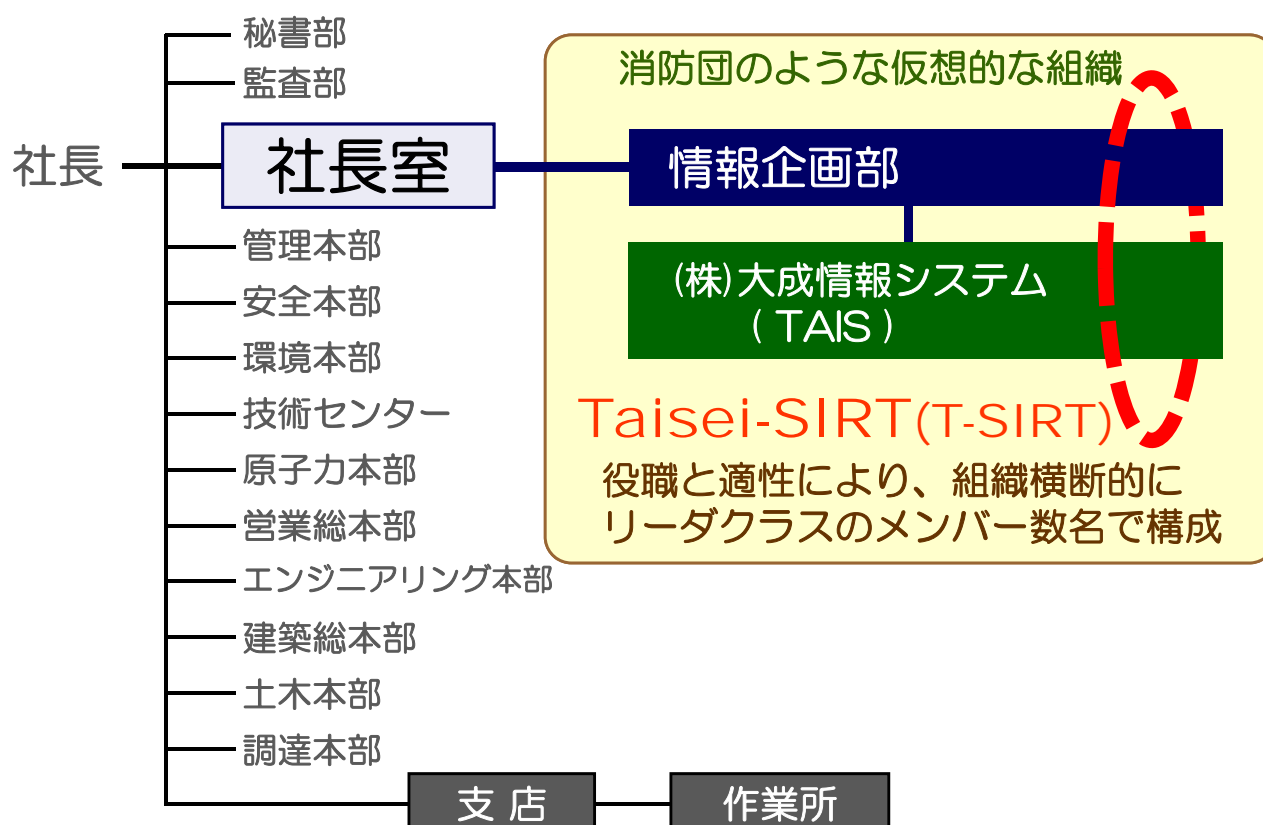
# CSIRT体制構築の動機付けとポイント

全社的リスク管理体制とCSIRT体制を融合  
一体化して、いかに早く、速くインシデント  
を発見し、**会社として判断**するか。

何故ならば…

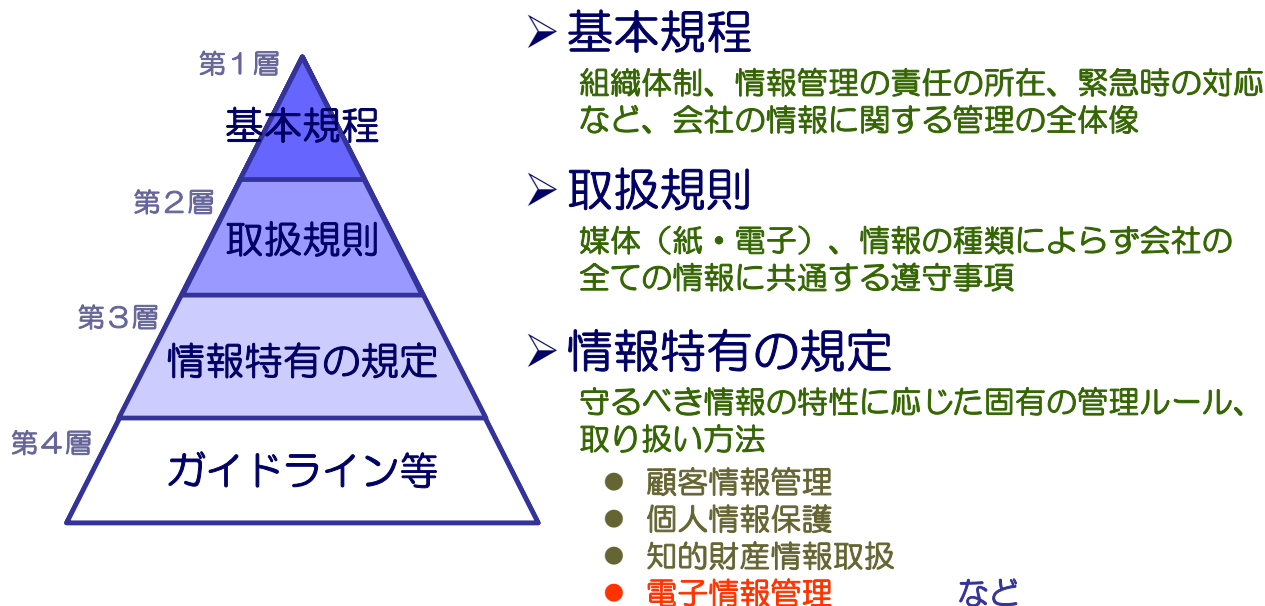
- 電子情報のインシデントは、**ごく短時間に  
大量の情報に影響を受け被害が急速に拡大する。**  
一刻も早く、初動態勢を立ち上げることが重要。
- ITの現場でビジネスインパクト分析(経営判断)は  
できない。現在起こっていることを正確にコンプ  
ライアンス部門に伝え、**会社のリスクとして判断**  
する必要がある。

## 組織体系における T-SIRT の位置付け





## 4つの階層により情報管理規程体系を構成



### ➤ ガイドライン・マニュアル等

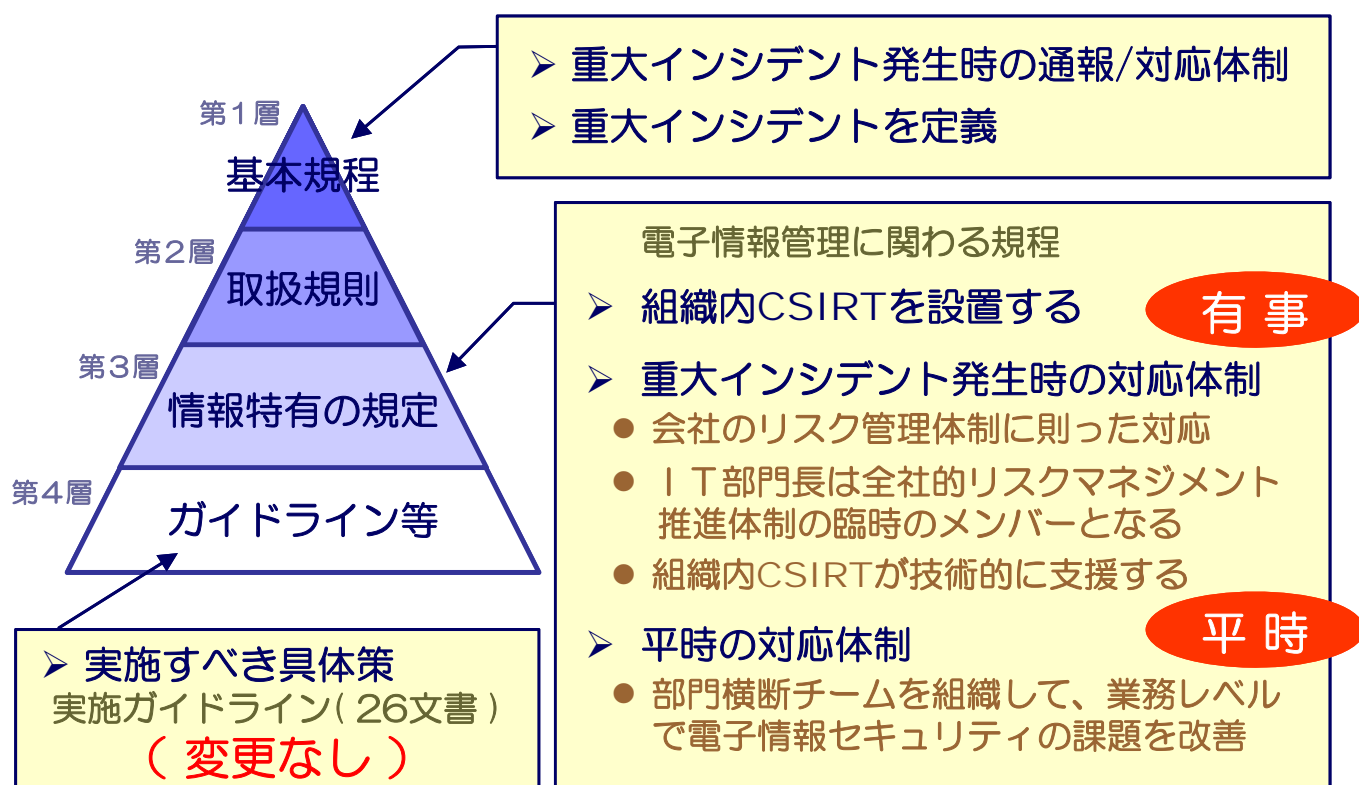
規程類を補完するために、各情報の取り扱い方法を分かり易く解説

- **実施ガイドライン** : 「管理者」の立場で守るべき具体的な管理策（26文書）
- **ポケットブック** : 「利用者」の立場で守るべき具体的な管理策（社員／業者）

# 社内規程にCSIRT設置を明文化

(2013年1月)

## 「仮想」の組織を社内に認知させ、位置づけを明確化



# 「重大なセキュリティインシデント」を定義

## 1. 会社が加害者（顧客や取引先等に関わるインシデント）

- パソコン、USBメモリの盗難による情報漏えい
- パソコンのウィルス感染による情報漏えい
- ブログやSNSに顧客の情報を掲載

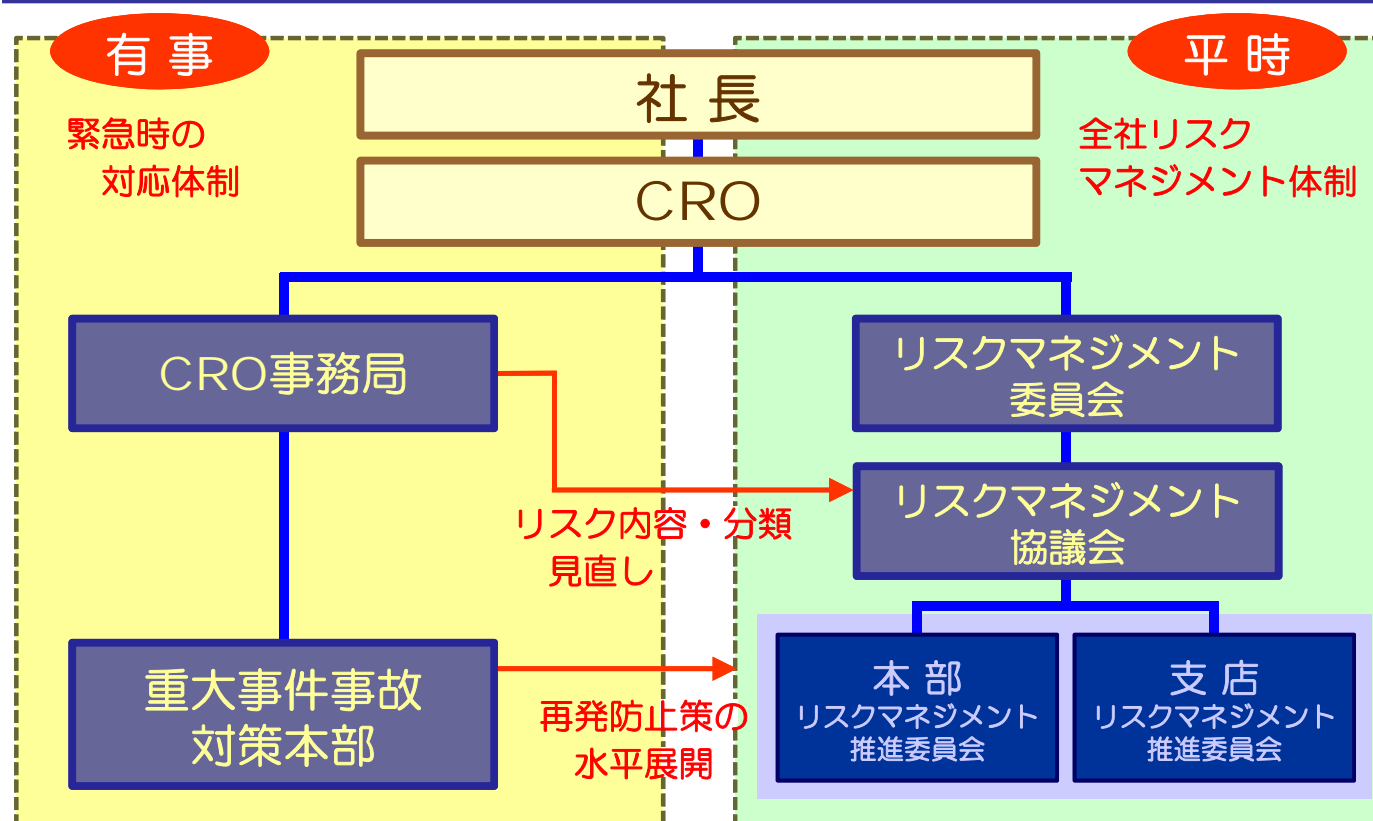
## 2. 会社が被害者（社外の第三者からのセキュリティ侵害）

- サイバー攻撃による情報の漏えいや改ざん、消失

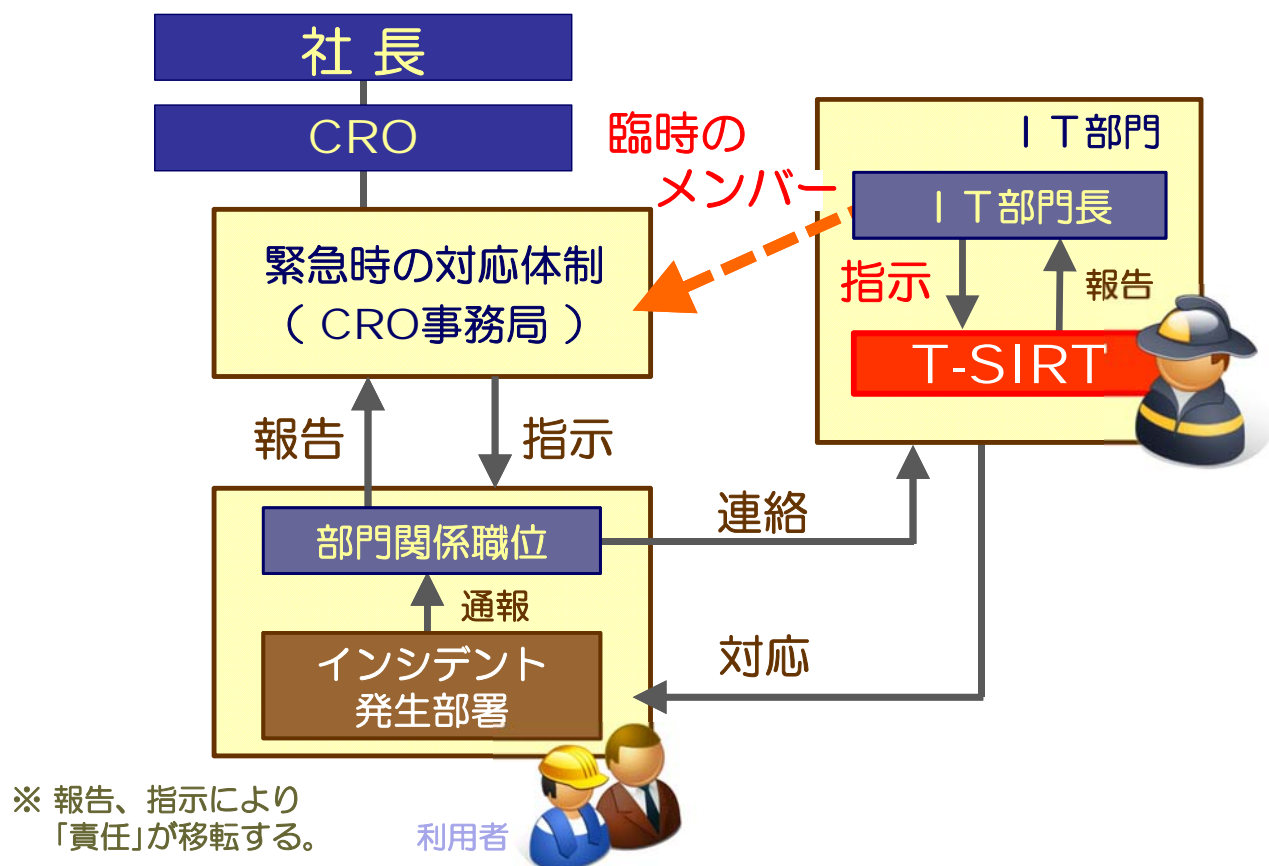
## 3. コンプライアンス違反（違法行為や知的財産侵害など）

- ソフトウェア 違法コピーによるライセンス違反
- 会社の機密情報の暴露

# 全社的リスクマネジメント推進体制



※ CRO : Chief Risk Officer / 最高リスク管理責任者



## 危機管理の基本は「平時」にあり

居安思危

安きに居りて危うきを思う

思則有備

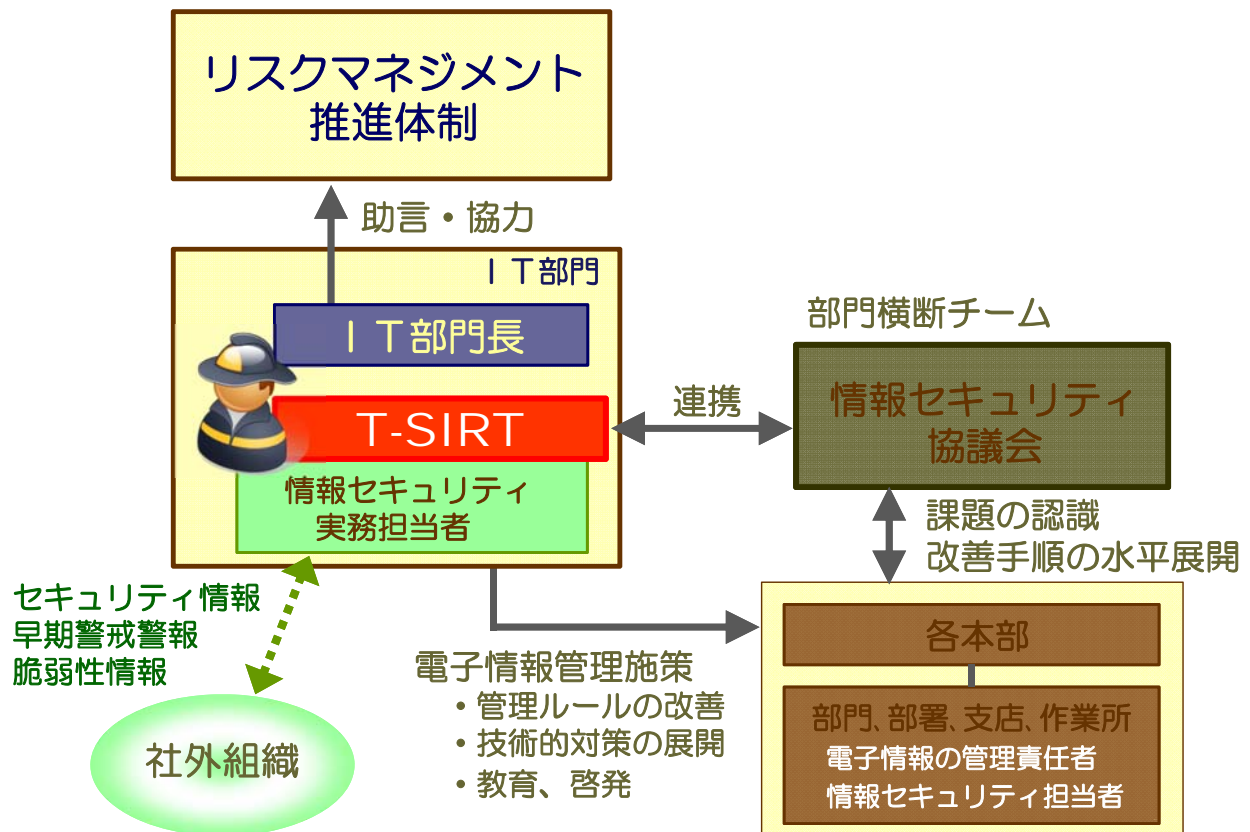
思えば則ち備え有り

有備無患

備え有れば患い無し

孔子が編集した史書「春秋」の注釈書「春秋左氏伝」 紀元前480年頃  
平時における備えの重要性を説き、防災や危機管理の心構えを表現





## 「平時」から「有事」に切り替えるトリガー

### ➤ 災害BCP

- 震度 × 以上の地震で自動発動
- 震災、台風、水害の状況により発動

### ➤ パンデミックBCP

- インフルエンザの致死率 × %以上で罹患者 × 名を超えた時点で責任者が発動

### ➤ 情報セキュリティ

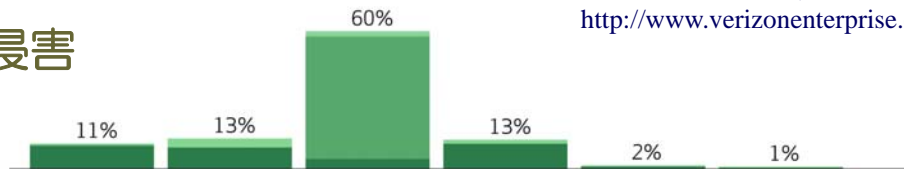
- パソコン盗難が発覚時点で発動
- インターネットへの書き込み発見時点で発動

それでは、**サイバー攻撃は？**

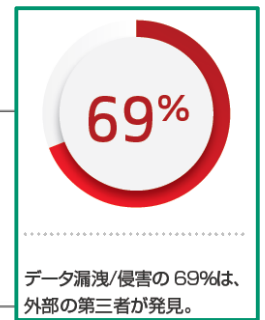
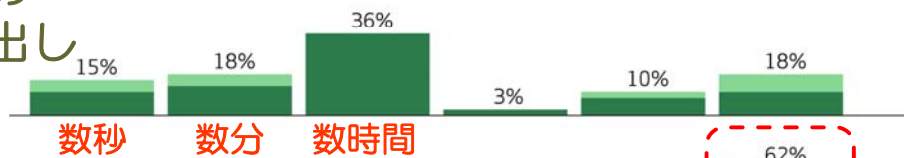
# データ侵害の時間的段階

※ ベライゾン「2013年度データ漏洩／侵害調査報告書」  
<http://www.verizonenterprise.com/jp/DBIR/2013/>

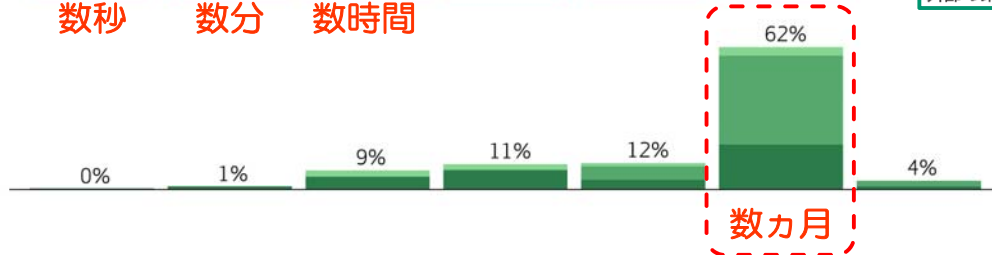
## 最初の侵害



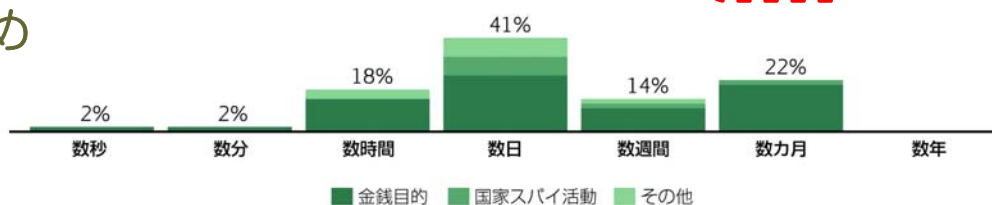
## データの取り出し



## 発見



## 封じ込め

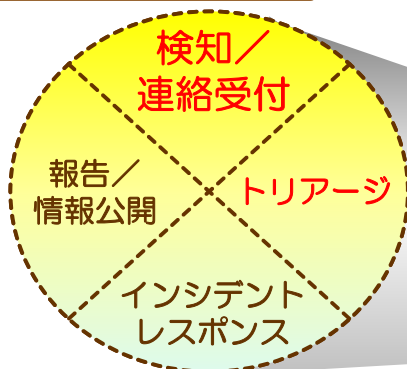


■ 金銭目的 ■ 国家スパイ活動 ■ その他

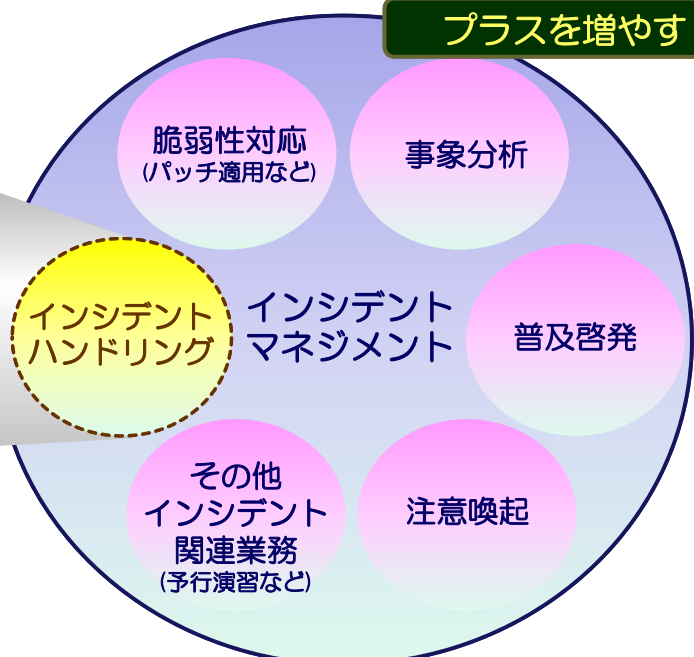
# 情報セキュリティの危機管理と緊急対応

## 危機管理（インシデントマネジメント）と 緊急対応（インシデントハンドリング）

マイナスを減らす



プラスを増やす



※ 「経営リスクと情報セキュリティ」 JPCERT/CCより  
[https://www.jpcert.or.jp/csirt\\_material/files/csirt\\_for\\_management\\_layer.pdf](https://www.jpcert.or.jp/csirt_material/files/csirt_for_management_layer.pdf)

# インシデント対応能力向上への取り組み

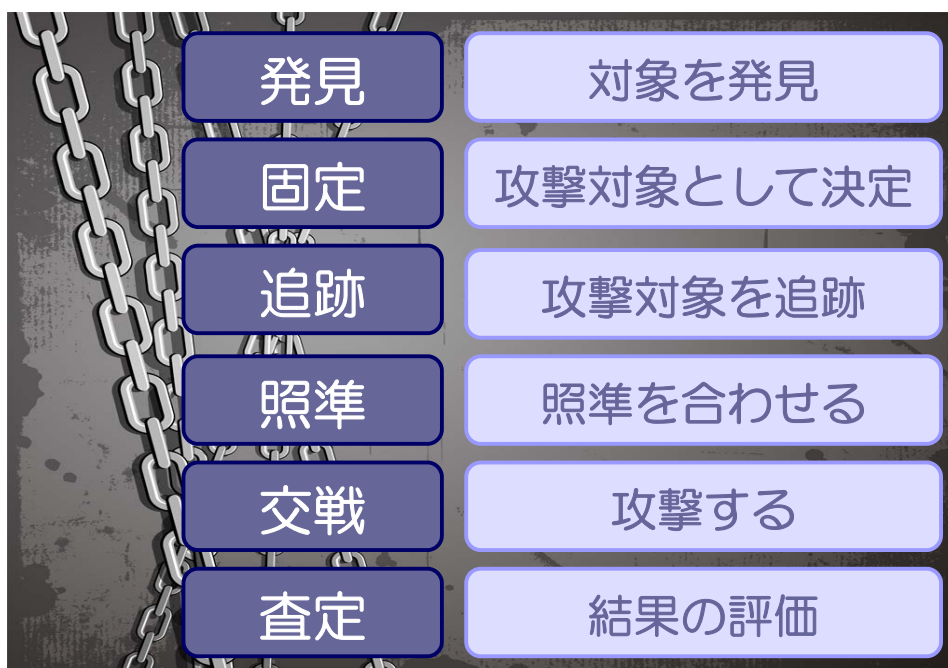
ツール主導のセキュリティ対策から、事故前提の  
業務プロセスを意識したインシデントハンドリングへ

- 監視、モニタリングによる「見える化」
  - 多層防御(サイバーキルチェーン)を意識  
攻撃と防御をイメージし、突破されたことを検知する
  - 業務プロセスの改善とアウトソース
- インシデント対応の訓練・演習【サイバー防災演習】
  - 緊急時対応体制発動のトリガーの明確化
  - 初動のスピードアップ  
「机上演習」と「技術演習」
  - 教育・訓練・演習による意識とスキルの向上

参考資料

## キルチェーンとは

- 攻撃のシークエンスを示す軍事用語
- 米国空軍ではFind, Fix, Track, Target, Engage, Assess  
の六つのステップからなり、F2T2EAとも呼ばれる





# それでは、サイバーキルチェーンとは

- 軍事作戦のキルチェーンを、攻撃者の活動に当てはめたもの
- 2009年、ロッキードマーチン社のMike Clopper氏によって提唱された考え方
- 標的型攻撃など、「意図を持った」攻撃を軍事作戦になぞらえ、インシデントレスポンスの考え方を提唱



※ Lockheed Martin社 Cyber Kill Chain

[http://www.lockheedmartin.com/us/Intelligence-Driven Computer Network Defense/what-we-do/information-technology/cyber-security/cyber-kill-chain.html](http://www.lockheedmartin.com/us/Intelligence-Driven%20Computer%20Network%20Defense/what-we-do/information-technology/cyber-security/cyber-kill-chain.html)

※ Intelligence-Driven Computer Network Defense


<http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

## サイバー攻撃のキルチェーン（攻撃シーケンス）

下にステップが移行するにつれ、攻撃が深化していく

偵察	インターネットのオープンな情報や裏データベースからターゲットの情報（システム、組織、取引先など）を収集。
武器化	攻撃コード（エクスプロイト）とマルウェア（実行ファイル）を作成。
デリバリ	なりすましメール（攻撃コード / マルウェアを添付）を送付。マルウェアを仕込んだWebサイトからドライブバイダウンロード。
エクスプロイト	ユーザに添付ファイル（PDF、Office）を開かせる。改ざんしたWebサイトへアクセスさせ、脆弱性を利用した攻撃コード（エクスプロイト）を実行する。
インストール	メールに添付した実行ファイルを開かせる、又は攻撃コード（エクスプロイト）が実行され、マルウェアがインストールされる。
C2	Command & Controlサーバへ接続させ、端末を遠隔操作。追加のマルウェアやツールをダウンロードするものもある。
目的の実行	目的の情報を探し、集約／暗号化してから、HTTP(S)などの手段で外部へ持ち出す。

# 攻撃のキルチェーンを断ち切る



フェーズ	検知	拒否	中断	緩和	欺く
偵察	Web分析	Firewall ACL			
武器化	Network IDS	Network IPS			
デリバリ	警戒ユーザ (Vigilant user)	Proxy filter	In-line AV ( Gateway )	Queuing	
エクス プロイト	Host IDS	Patch	DEP ( Data Execution Prevention )		
インス トール	Host IDS	“chroot” jail	AV ( AntiVirus )		
C2	Network IDS	Firewall ACL	Network IPS	Tarpit	DNS redirect
目的の実行	監査ログ ( Audit log )			QoS ( Quality of Service )	Honeypot

<http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

## 機能しないセキュリティ対策

「既知の攻撃」であることを前提とした対策  
アンチウィルス、Firewall、IPS、アンチスパム  
基本的にシグネチャベースの対策

いま、大きな問題となっているのは  
「未知の攻撃」や「ゼロディ攻撃」

新型マルウェアの54%は検出できない。

「2014 NTT Group Global Threat Intelligence Report」  
2014年3月28日 米NTT Innovation Institute

Antivirus "is dead," says Brian Dye, Symantec's  
senior vice president for information security.

2014年5月4日 THE WALL STREET JOURNAL



攻撃者は検知されないように作るから当然の結果

# サイバー攻撃では攻撃者側が圧倒的に有利

## 【 攻撃者側 】

- 攻撃対象は無数にある
- いつでも攻撃できる（24時間365日）
- 失敗しても、何回でもやり直せる
- お金で繋がる「分業化」
- 攻撃手法は日々進化している
- 破壊、窃取、妨害など、様々な手段を駆使できる

## 【 防御側 】

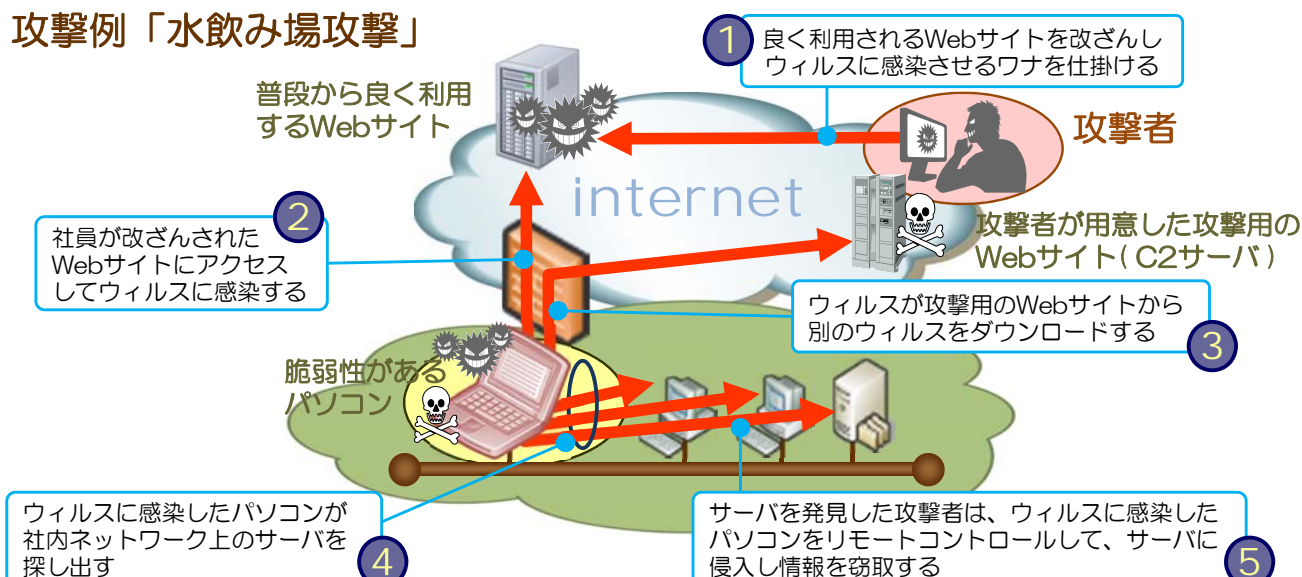
- 守ることしかできない   ～ 倍返しなんてありえない～
- 攻撃を完全に防ぐことはできない
- 失敗できない、勝ち続けるしかない
- セキュリティ対策は常に陳腐化する

一刻も早く検知/発見することが重要

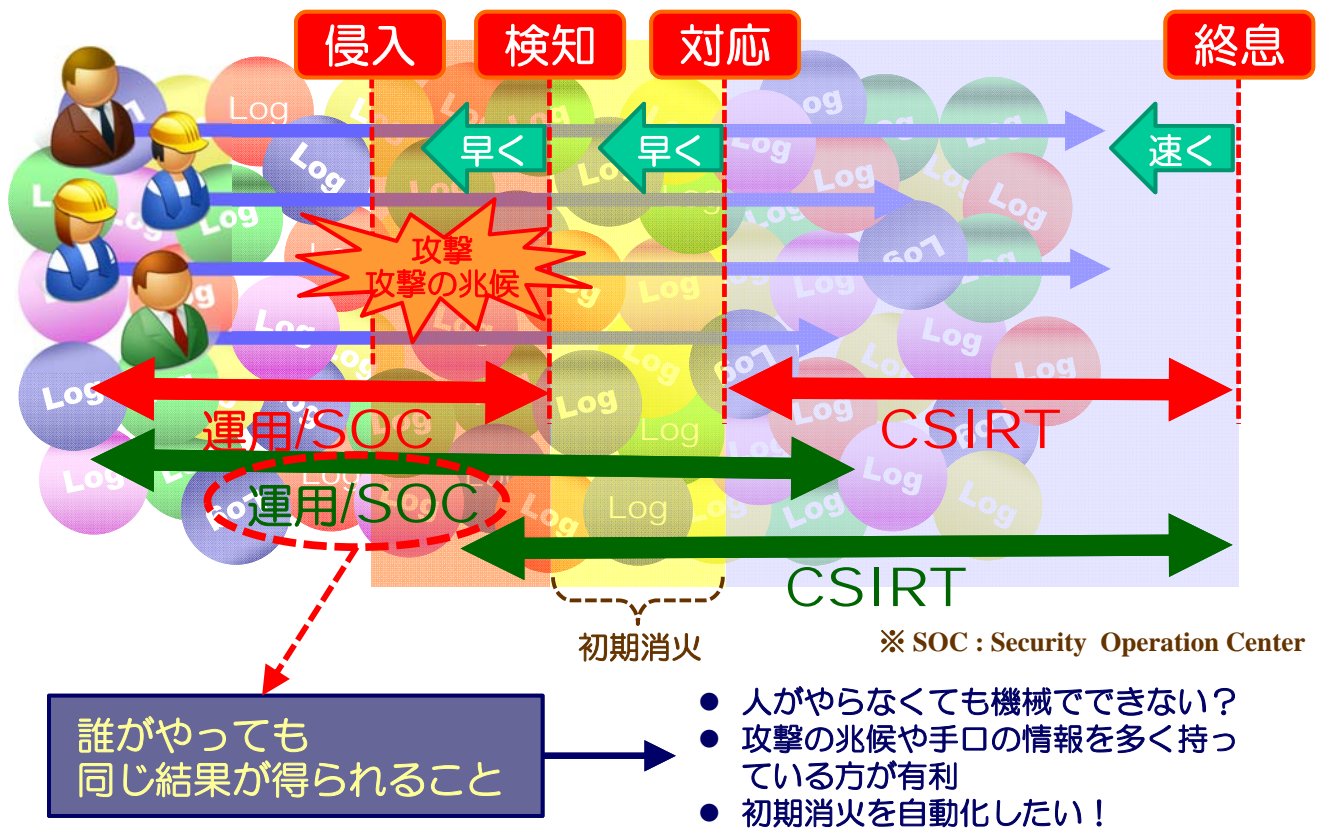
## 攻撃者は多くの足跡を残す

- 通過した複数の機器やシステムのログに足跡が残る  
しかし、タイミングを逃すと埋もれてしまう
- 複数のログソースを統合して、高速に検索、相関分析  
することで、攻撃者の足跡を追跡する

### 攻撃例「水飲み場攻撃」



## SOC と CSIRTの連携



## セキュリティの運用業務への組み込み

## 參考資料

## 「タテ」に割らずに「ヨコ」に繋ぐ、レイヤー化した組織

➤ 運用業務への組み込み

- インディケータとセキュリティインシデントを「定義」
- インシデント判定基準とエスカレーションルールを明確化
- インシデント対応の緊急措置／暫定処置を手順化
- 通常の運用手順に載せる
- アウトソース可能な範囲の明確化
- アウトソーサには手順書ベースで委託

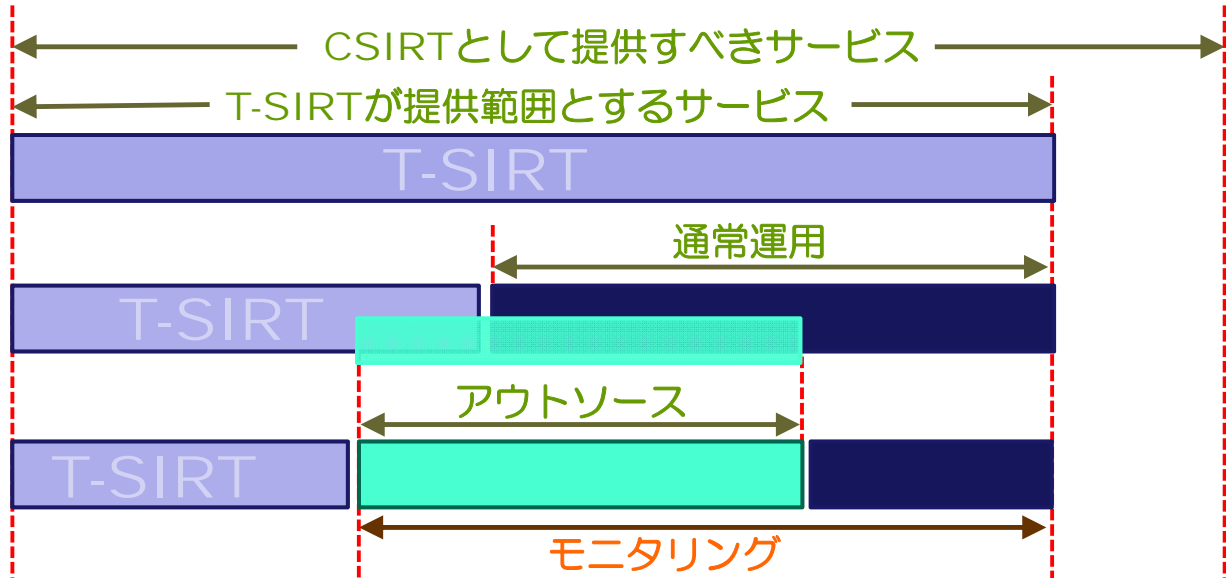
## ➤ 組織内CSIRTの運用

- 判断基準や対応策の選択肢、チェックシートをリスト化（ノウハウ、インディケータ、インテリジェンス）
- 手順書だけで対応することは視野を狭くするので危険

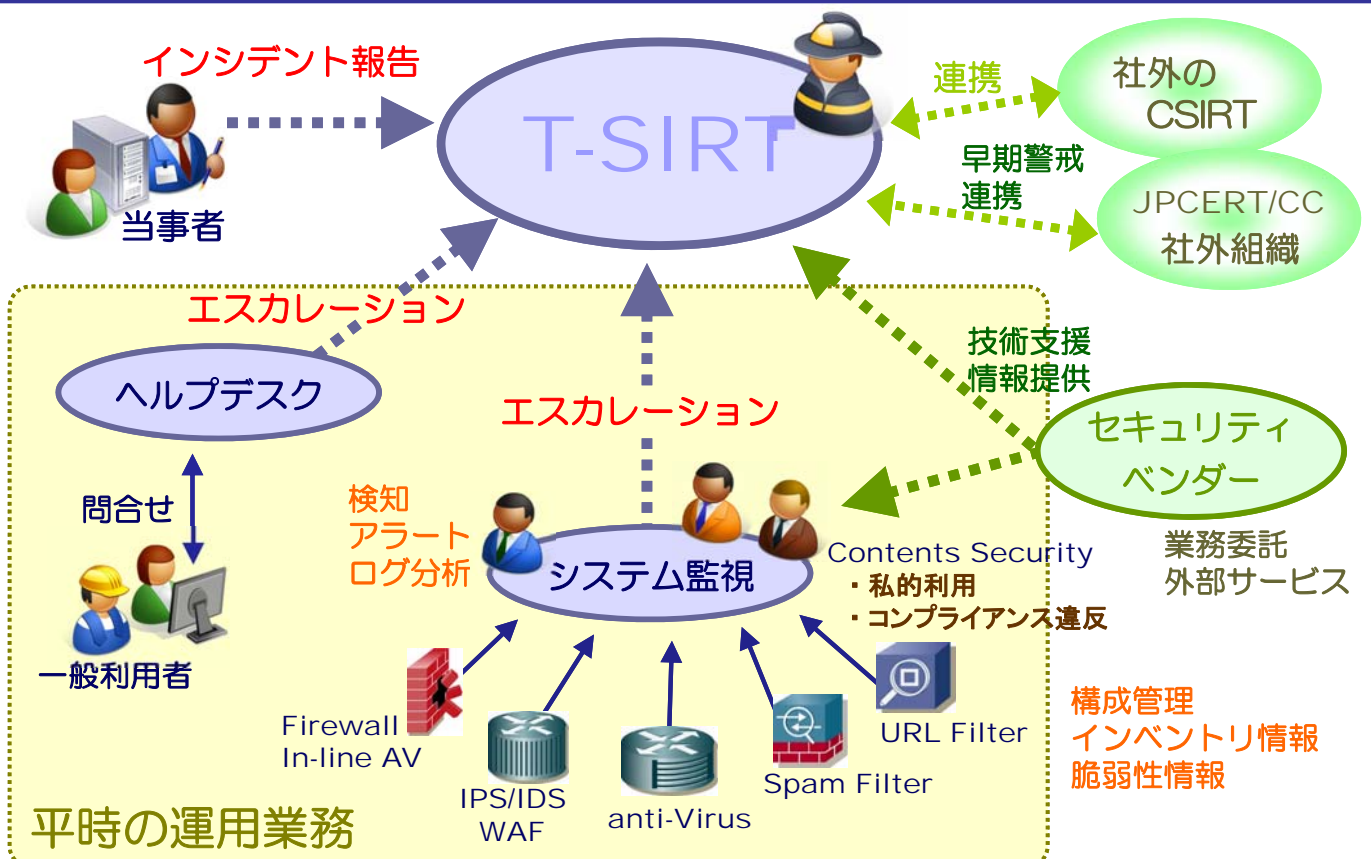


# 運用チームやアウトソーサとの連携

- 役割と連携プロセスを明確にする  
( 判定基準、エスカレーションルール、初期対応 )
- 24時間365日対応可能な監視、対応体制とする



# 情報セキュリティインシデントを「発見」する



# 運用業務を「センター化」してアウトソース

- 業務の「モジュール化」「センター化」「レイヤー( Tire )化」
- サービスレベル管理( OLAとSLA )

- NOC ( Network Operation Center )
- SOC ( Security Operation Center )
- データセンター

- ITサポートセンター／ヘルプデスク
- IT基盤運用管理センター

- 社内運用チーム
- T-SIRT = 運用チームリーダー

外部サービスの  
標準メニューを利用

当社利用環境に則した  
運用メニュー

モニタリング  
手順化/標準化

- 「技術」は社外から調達可能

サービスの責任は自社

「会社を守る」という意思とモチベーションは自社でなければ！

※ SLA : Service Level Agreement  
OLA : Operational Level Agreement

## 「Why should I ? 」 or 「Why Shouldn't I ?」

ウィリアム・ジェームズ 『宗教的経験の諸相』より

何か大きな事件が起きたとき、人はみな『誰かがこのことについて何かをしなければならない』と言う。  
しかし、自ら進んでその困難な仕事にあたろうとする者は極めて少ない。

誰もが誰かがこの仕事をすべきだと思うが、  
『 **Why should I ?** （なぜ私がやらなければいけないのか？） 』  
と自問自答する。

ところが一握りの宗教的な人たちは  
『 **Why Shouldn't I ?** （私がやらずに誰がやる） 』  
と自問自答する。

この二つの自問自答の間に人類の道徳的進化の過程が横たわっている。

※ 佐々淳行 著「定本 危機管理 我が経験とノウハウ」( 株式会社ぎょうせい )にて  
ウィリアム・ジェームズ『宗教的経験の諸相』の言葉を引用

### ➤ 7万人の命を救った誘導！ (東京ディズニーリゾート)

10万人が入場している状態でのM8級の地震は想定内  
年180回の訓練と行動指針の徹底により、**個人**が状況に合わせ**判断**  
避難誘導、売店の菓子配給、ぬいぐるみで防護、忘れないエンターテイメント

### ➤ NHK総合が Ustream でストリーミング配信

★ Twitter履歴



おお！中学生の流すNHK-TVの地震情報Ust配信をNHK側が許可したらいい。  
ブラボー!!!

2011/03/11 17:37:55



停電のため、テレビがご覧になれない地域があります。人命にかかわることですから、  
少しでも情報が届く手段があるのでしたら、活用して頂きたいと存じます  
(ただ、これは**私の独断ですので、あとで責任は取るつもりです**)。

NHK\_PR

2011/03/11 17:40:51

自らの「権限」を越えた判断  
手順書に書かれていない柔軟な対応  
無名のヒーローの作り方

経験、そして経験を補う教育と訓練と演習

## やってみる (やらせてみる)

### 演習とは (ISO22301 事業継続マネジメント)

組織におけるパフォーマンスに関する教育訓練、  
有効性評価、実施および改善のためのプロセス

個人や組織の能力を向上させる『**訓練**』に対し、  
『**演習**』は能力向上に加え、計画の検証を目的とする。

実際にやってみて(やらせてみて)、監視体制や初期対応  
の妥当性、緊急連絡手段などを検証するとともに、RTO  
(目標復旧時間)内に対処、復旧できることを検証する。

※ RTO : Recovery Time Objective

『やってみせ、言って聞かせて、させてみせ、  
ほめてやらねば、人は動かじ』 山本五十六

## 「決断力の見取り稽古をしなさい」

初代内閣安全保障室長 佐々淳行さんの言葉

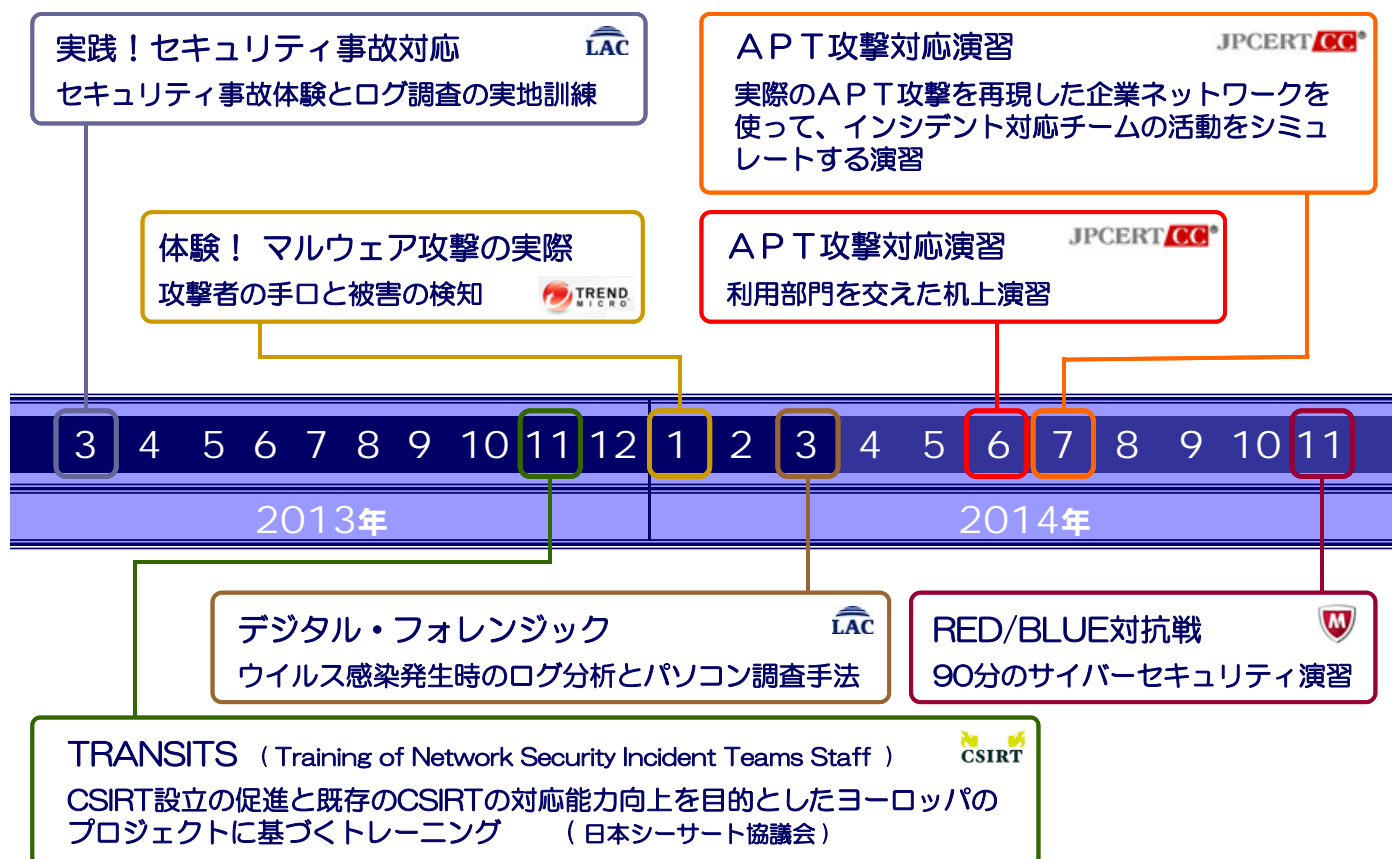
大災害や不祥事などの危機というものは、実際に体験することは極めて稀です。だからこそ訓練が重要なのですが、もっと重要なことは日常的に危機発生時の決断力を磨くこと。

そのためには、テレビや新聞、雑誌で、不祥事問題などが取り上げられた際に、これを教材として、自分ならどうするか見取り稽古をすることが大事だと言います。

「ああ、またやられてる、と興味本位で見て、そこから何も学べない人は、いざ自分が同じ目にあったとき、頭の中が真っ白になってしまうタイプ」。社長だけでなく、あらゆる階級、役職において、その立場の決断というものがありますが、それぞれの立場で見取り稽古をして決断力を高めていくことが強い組織をつくると言います。

「リスク対策.com」中澤編集長のコラムより

## スキルアップ研修とサイバー防災演習の実施





- 全社リスク体制と部門管理者向けの「**机上演習**」と情報セキュリティ対応チーム向けの「**技術演習**」（Technical Exercise）を実施した。
- **机上演習**ではサイバー攻撃に関連する3つの状況をもとに、企業としての対応と課題について、全社リスク体制、部門管理者およびT-SIRTの三者でディスカッションを行った。
- **技術演習**では疑似的にサイバー攻撃を再現した企業ネットワーク環境を用い、攻撃に対する情報セキュリティ対応チームの活動をシミュレートした。

## 社内関係部署を交えた「机上演習」

サイバー攻撃の状況を示す3つのシナリオを提示し、利用部門、リスク管理部門、IT部門、それぞれの立場でリスクを評価し、企業が取り得る対応策について議論する。



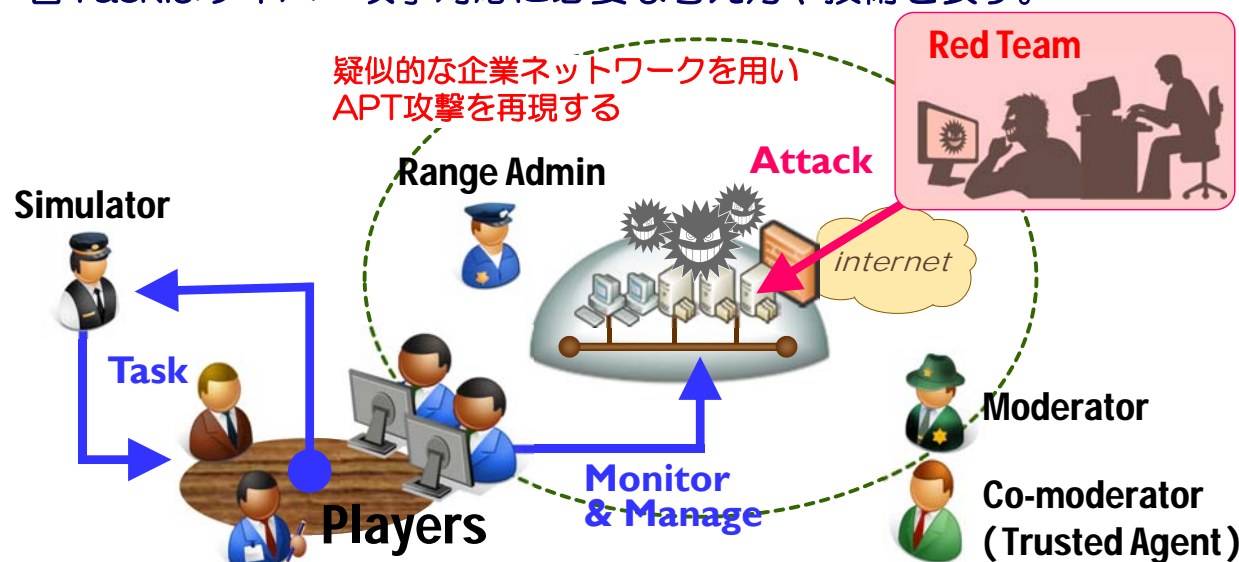
リスクとは、ビジネス上重要な資産と情報についての理解、サイバー脅威の性質、システムやビジネスオペレーションにおける脆弱性、重要なビジネスプロセスへの影響、など

# 企業ネットワークを用いた「技術演習」

Red Teamによる攻撃の検知と対応、SimulatorからのTaskに対応しサイバー攻撃への防御措置を実行する。

プレーヤはInject（Red Teamの攻撃やSimulatorからのTask）を受け、チームで対応方針を協議し、行動する。

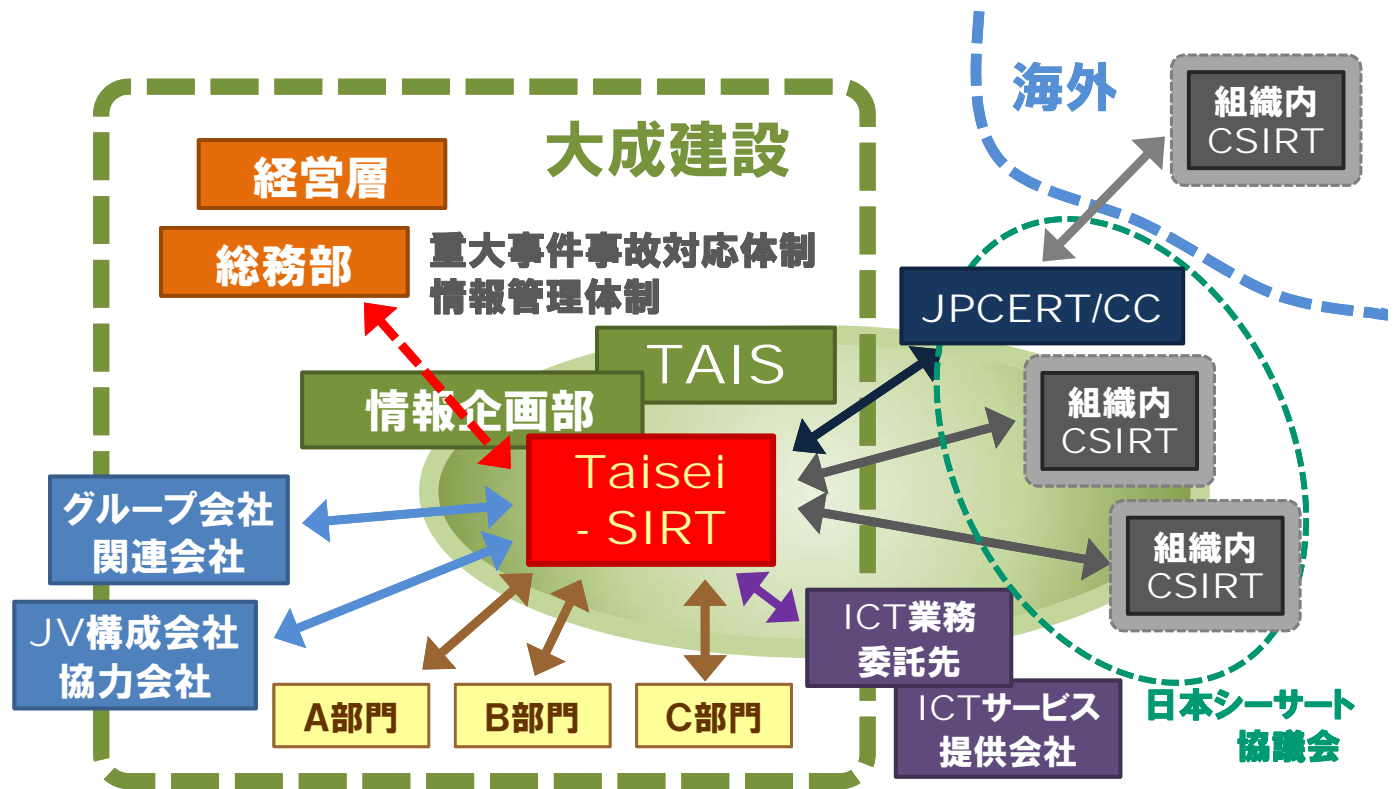
各Taskはサイバー攻撃対応に必要な考え方や技術を表す。



## 全体のまとめ

- 情報セキュリティは企業のリスク管理として重要な経営課題のひとつであり、ビジネスを守り、推進するために必要不可欠なものです。
  - 情報セキュリティに関するリスク管理体制を企業内に実装するために、組織内CSIRTの設置が有効です。
  - 組織内CSIRTの実装において、経営者との距離感、システム運用チームとの距離感が重要になります。
- そのためのルールと体制づくりが必要です。

# Taisei-SIRT



日本シーサート協議会、及び加盟に関する問合せ先  
メールアドレス： [nca-sec@nca.gr.jp](mailto:nca-sec@nca.gr.jp)



61

## 何のための情報セキュリティか？

- 顧客を守り、会社を守り、社員を守る
- 法を守る、社会的責任、法令遵守
- 品質を守る、Japanブランド

情報セキュリティ投資はコストでしかないか？

➡ ICT導入の**成果を最大化**するために必要なコスト。

- 投資判断 + リスク評価
- 「ビジネス」を守り、推進するもの

***“information security as a business enabler”***

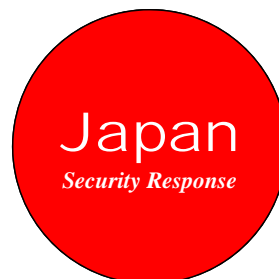
情報セキュリティが担保されているからこそできることがある。  
それが、情報セキュリティの成果である。

### リスク管理としての情報セキュリティ

ITを使うメリットと情報セキュリティ上のリスクを比較して、  
リスクがメリットを上回ったら…、そのITは使わない方が良い。

---

ご清聴、ありがとうございました。



大成建設株式会社