TOPPAN-CERTの活動報告

2012年11月19日

TOPPAN-CERT　庄司　朋隆

1. はじめに
- 自己紹介
- 会社紹介

2. 組織内CSIRT構築
- 背景
- 目的
- 期待効果

3. TOPPAN-CERT紹介
- チーム構成/体制
- チーム構築における苦労話
- チーム沿革
- 活動内容/実績

1．はじめに

1999年 凸版印刷株式会社　入社。
　　Eビジネス部門に配属。
　　ホスティングサービスのインフラ運用管理に従事。
2006年 研究部門に配属。
　　仮想化技術やWebセキュリティの調査/社内展開活動に従事。
2010年 全社技術部門に配属。
　　工場インフラの改善活動に従事。
　　TOPPAN-CERT設立に関わりPOCを担当。
2011年 情報システム部門に配属。
　　端末環境の改善活動に従事。
　　現在に至る。

■ICT本部とは
トッパングループのICTサービス基盤の企画/設計/構築/導入/運営/保守を行う。
各事業本部の業務プロセスの企画/構築や業務システムの開発/導入を通じて、統制/管理を行う。

凸版印刷株式会社
～企業概要～

創　　業　：1900年(明治33年)

資 本 金　：　1,049億円

売 上 高　：1兆5,104億円(連結)

8,492億円(単体)

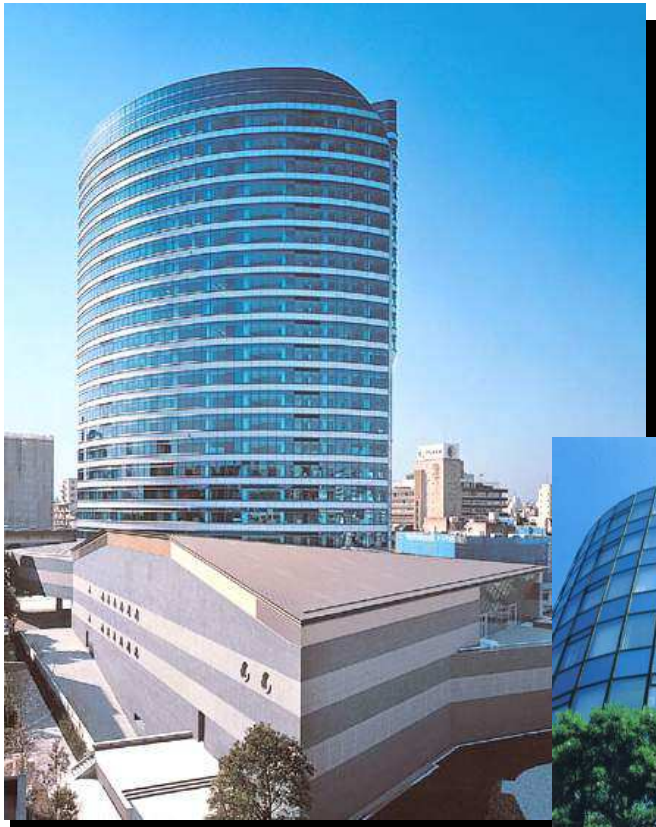
※業績数字は2012年3月期

従 業 員 数：47,872人(連結)

8,508人(単体)

社名の由来:

大蔵省(現 財務省)出身の技術者が中心になり、当時の最新鋭製版技術である**エルヘート凸版法**をもって、1900年に設立。



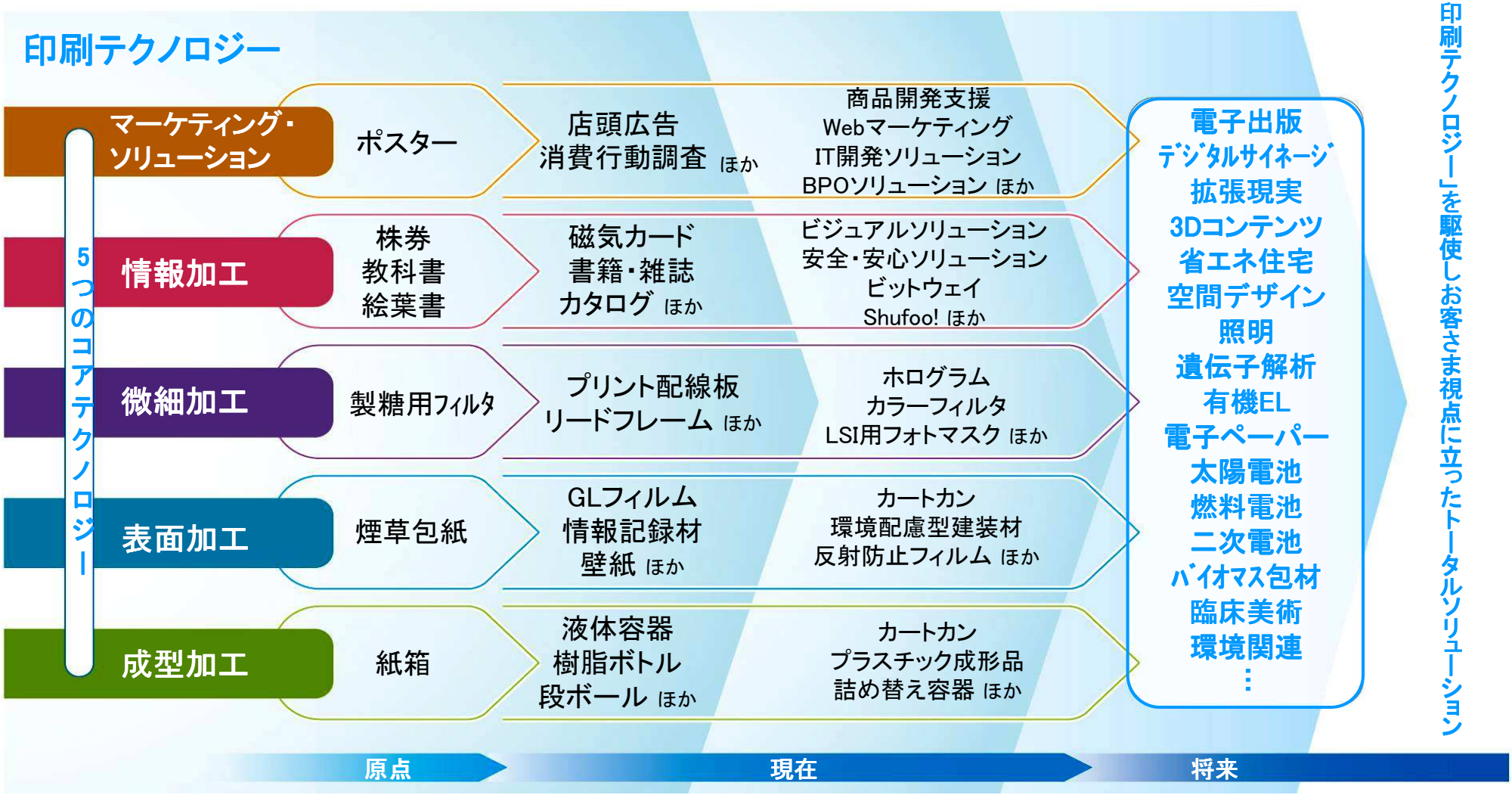
小石川ビル
(東京都文京区)

本社ビル(秋葉原)

総合研究所(埼玉県杉戸)

TOPPAN

印刷テクノロジーが実現するさまざまなソリューション



印刷テクノロジーから、多様な製品、ソリューションに広がり続けている

TOPPAN

情報・ネットワーク系

証券・カード部門

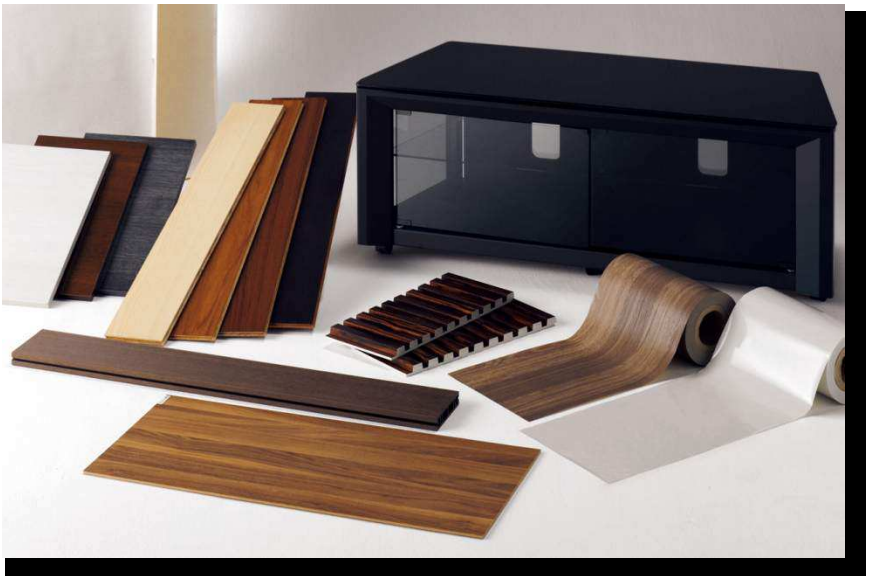
商業印刷部門

出版印刷部門

TOPPAN

■生活環境系

パッケージ部門

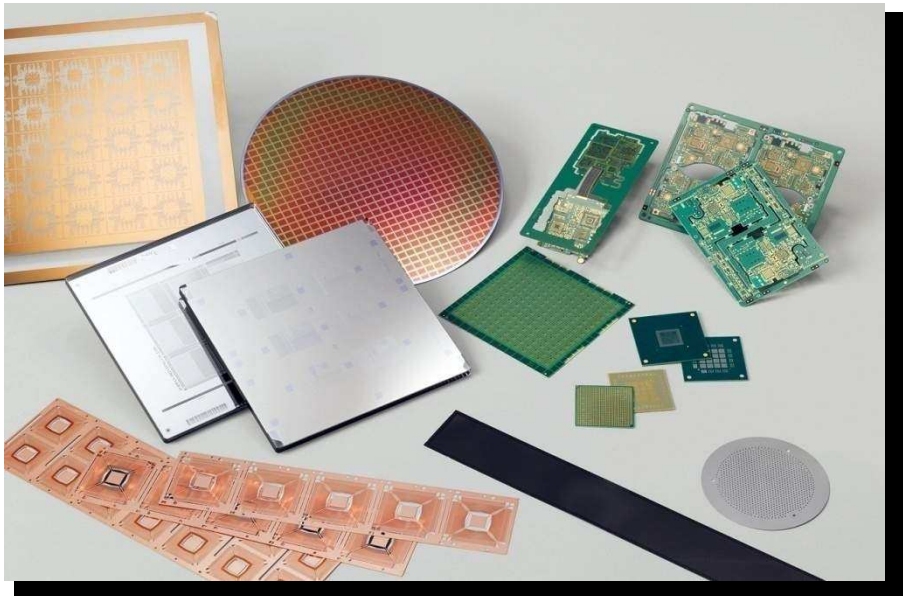


建装材部門

高機能･エネルギー関連部門

エレクトロニクス系

ディスプレイ関連部門



半導体関連部門

2. 組織内CSIRT構築

- インシデントによる被害が数多く発生
  - 復旧・対策に膨大な労力と費用を要する
  - ブランドイメージの低下や信用失墜などの間接的な被害
- インシデントに対してどう取り組むべきか？
  - 事故前提社会への対応力強化
  - 組織内CSIRT (Computer Security Incident Response Team)の活用
- 情報セキュリティ2010(内閣官房情報セキュリティセンター)の施策提示

> エ） 組織の緊急対応チームの普及、連携体制の強化（経済産業省）
> CSIRT の構築・運用に関するマテリアルや、インシデント対策・対応に資する脅威情報や攻撃に関する情報、所要の分析を加えた具体的な対策情報等を適切な者[1]の間で共有することにより、CSIRT の普及や JPCERT/CC と国内外の組織内CSIRTとの間における緊急時及び平常時の連携の強化を図る。

[1] インシデント対策/対応に関係する組織およびその組織に属するセキュリティ担当者など（JPCERT/CC ）

活動対象、範囲、目的を明確にしておく

凸版印刷株式会社及び関係会社を対象に以下を実現する。

- インシデント対応の技術支援を一元化し、迅速な対応を実現する。
- 技術動向を監視し、セキュリティ関連情報の提供を行う。

抱えていた課題が解決するイメージを描く

- 関連情報の集約と効率的活用
  - 社員にとって報告・連絡・相談窓口となることで更なる情報集約
  - 経営層への報告のしくみ、縦割りから横断型への体制転換
- 組織のセキュリティレベルの向上
  - ｲﾝｼﾃﾞﾝﾄの再発防止を押し進め、組織内のｾｷｭﾘﾃｨﾚﾍﾞﾙを高める
- 社内外に向けたメッセージ
  - 顧客や取引先に向けた信頼のブランドイメージの確立
  - 関係機関に向けたコンプライアンスの姿勢のアピール
  - 内部統制・グループ統制強化の手段
- 他組織との連携
  - CSIRT同士の連携を通じて、適正なレベル感の相対的な把握

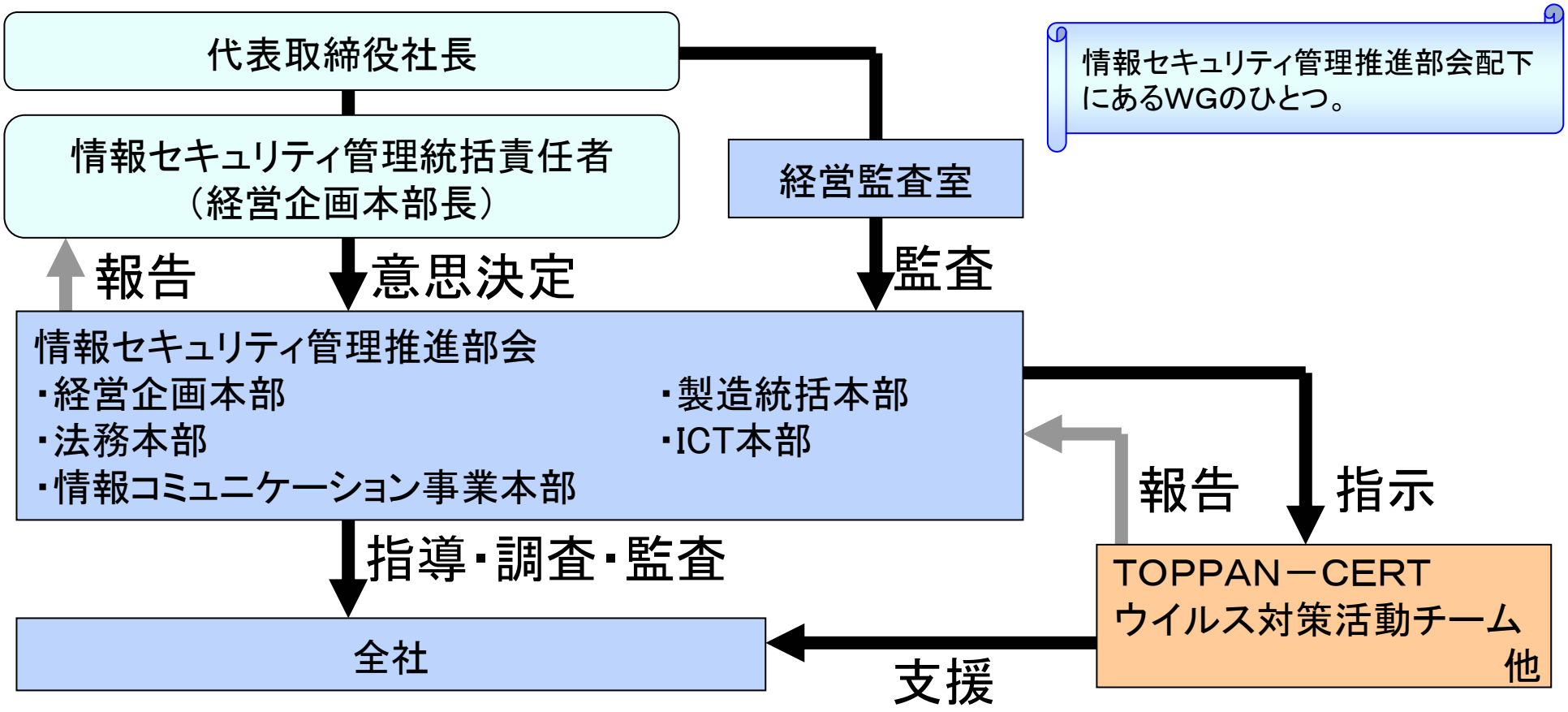
3. TOPPAN-CERT紹介

3. TOPPAN-CERT紹介　～チーム構成/体制～

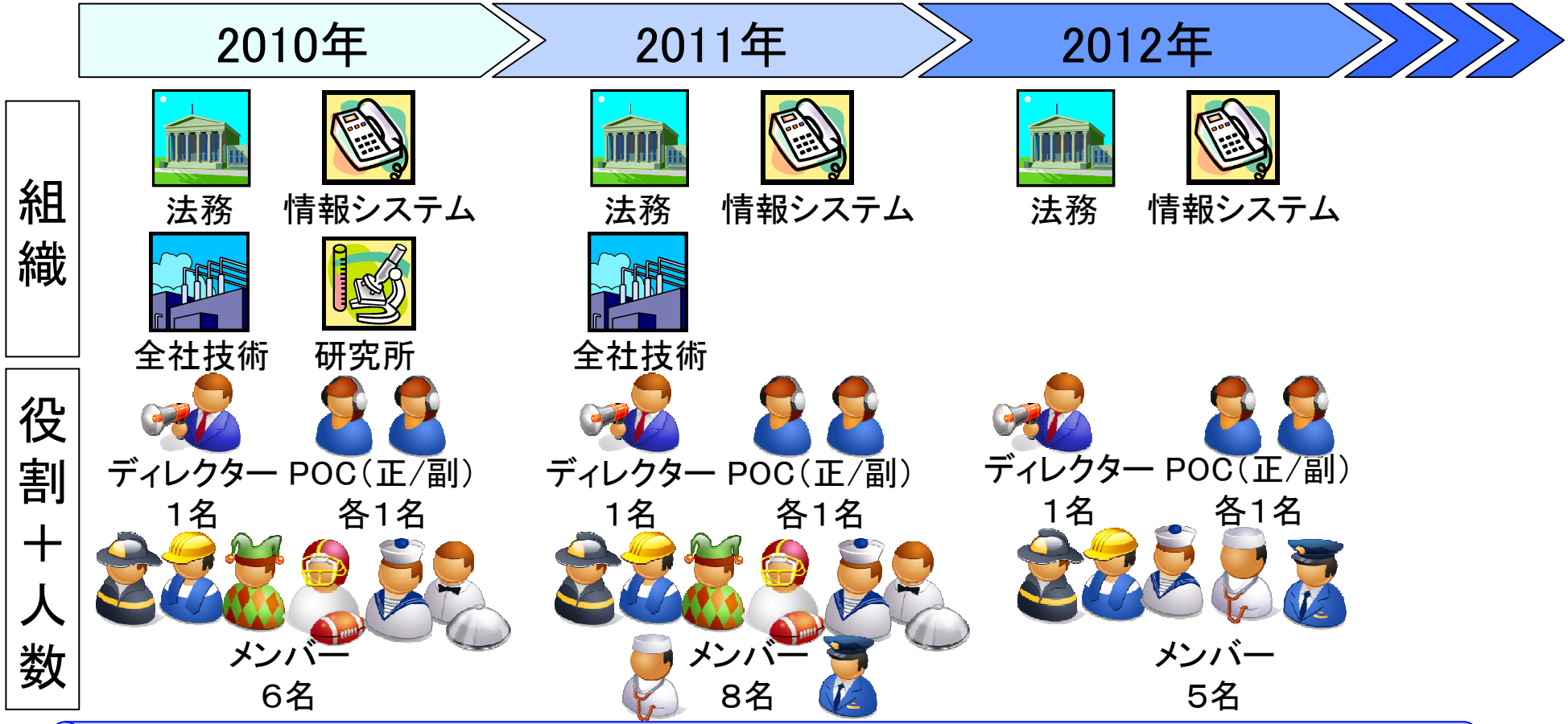
TOPPAN

TOPPAN Computer Emergency Response Teamの略。2010年8月に発足した、トッパンおよびファミリー会社のコンピュータセキュリティに関する諸問題に対応するチームのことです。情報セキュリティ管理推進部会の一機能として、内外情報・技術動向を監視し、情報提供や問題発生時の技術的な解決支援を行います。

『情報セキュリティ管理ガイドブック』より



3. TOPPAN-CERT紹介　～チーム構成/体制～



■ディレクターはCSIRT の体制管理や活動方針を決定する役割
■POC はチーム外（別チーム、サービス対象）の直接のやりとりをする役割。
　情報が最も集まるためリーダーを兼務する。

- 構築準備活動
  - 情報収集
    - JPCERT/CC　CSIRTマテリアル(http://www.jpcert.or.jp/csirt_material/)
    - 日本シーサート協議会
      - 2010/2/17　TRANSITS Workshop NCA,Japanに参加
      - 2010/2/18　ワーキンググループ会にゲスト参加(IIJ-SECT様からご招待頂きました)
      - 組織内シーサート課題検討WGに個人参加
  - メンバー選定
    - 情報セキュリティ管理推進部会による役員報告を経て決定
      - 全社技術部門が主導してチーム構築を推進
      - 部会構成部門からメンバー選定
        - » システム監査/セキュリティ監査の実施メンバーが中心
- 構築における課題
  - 組織内CSIRTの必要性を経営層に理解して頂く為に何をしたらよいか。
    ⇒情報セキュリティ2010の引用や事故前提社会というキーワードを用いた上程。
  - 何を持って組織内CSIRTの構築が出来たと言えるのか。
    ⇒JPCERT/CCに構築支援依頼(フレームワーク活用とトレーニングを開催)

2010年5月　組織内CSIRT構築活動を開始

※JPCERT/CCに構築支援依頼

2010年8月　TOPPAN-CERT構築

日本シーサート協議会WGに参加

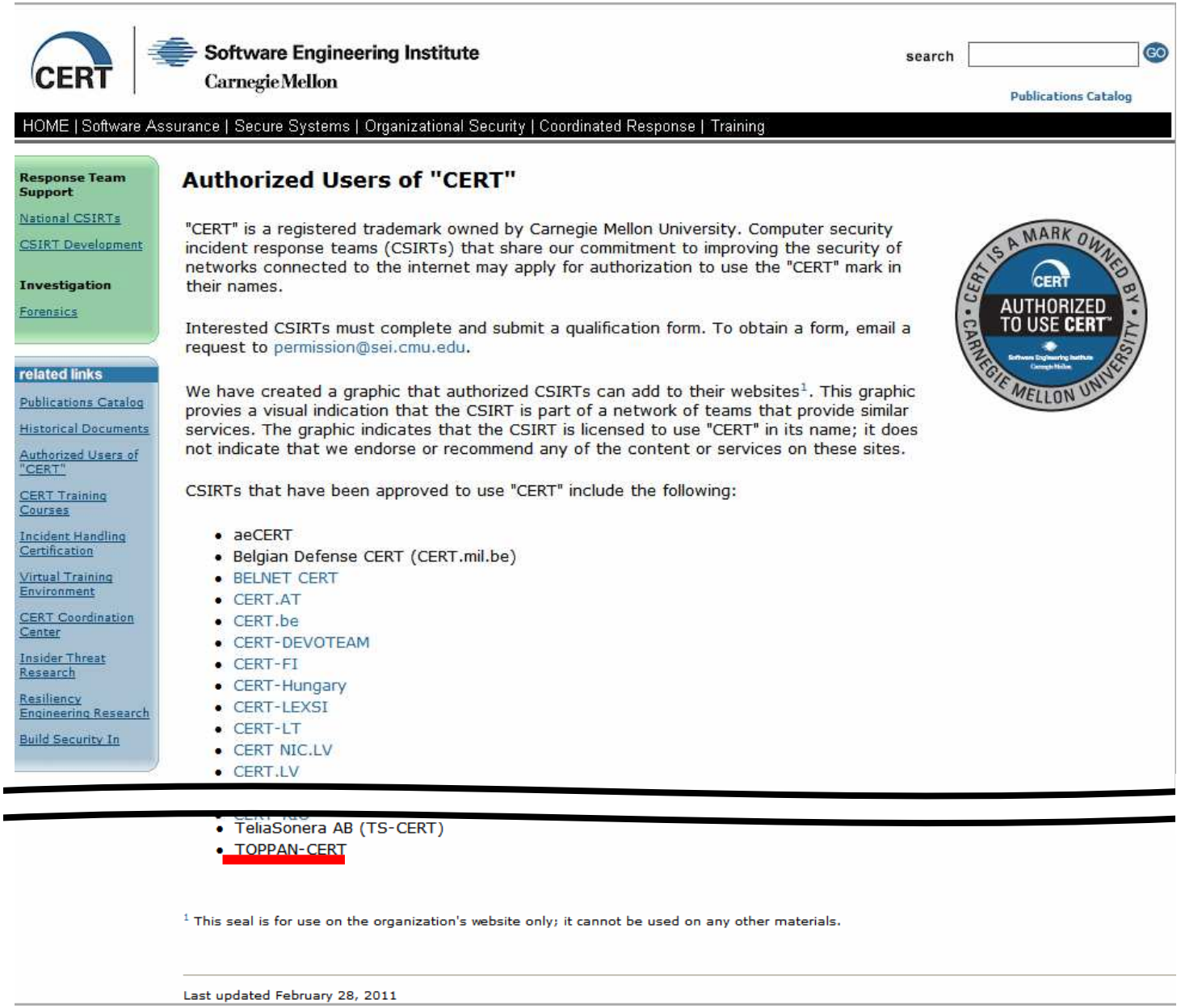
2010年9月　情報セキュリティに関わる各委員会・部会に組織内CSIRTの構築を報告

11月　CERTの利用許諾を得る

http://www.cert.org/csirts/cert_authorized.html

2011年6月　日本シーサート協議会に加盟

3. TOPPAN-CERT紹介　～チーム沿革～



CERT | Software Engineering Institute Carnegie Mellon

search GO

Publications Catalog

HOME | Software Assurance | Secure Systems | Organizational Security | Coordinated Response | Training

Response Team Support

National CSIRTs

CSIRT Development

Investigation

Forensics

related links

Publications Catalog

Historical Documents

Authorized Users of "CERT"

CERT Training Courses

Incident Handling Certification

Virtual Training Environment

CERT Coordination Center

Insider Threat Research

Resiliency Engineering Research

Build Security In

Authorized Users of "CERT"

"CERT" is a registered trademark owned by Carnegie Mellon University. Computer security incident response teams (CSIRTs) that share our commitment to improving the security of networks connected to the internet may apply for authorization to use the "CERT" mark in their names.

Interested CSIRTs must complete and submit a qualification form. To obtain a form, email a request to permission@sei.cmu.edu.

We have created a graphic that authorized CSIRTs can add to their websites[1]. This graphic provies a visual indication that the CSIRT is part of a network of teams that provide similar services. The graphic indicates that the CSIRT is licensed to use "CERT" in its name; it does not indicate that we endorse or recommend any of the content or services on these sites.

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY — CERT AUTHORIZED TO USE CERT

CSIRTs that have been approved to use "CERT" include the following:

- aeCERT
- Belgian Defense CERT (CERT.mil.be)
- BELNET CERT
- CERT.AT
- CERT.be
- CERT-DEVOTEAM
- CERT-FI
- CERT-Hungary
- CERT-LEXSI
- CERT-LT
- CERT NIC.LV
- CERT.LV

- TeliaSonera AB (TS-CERT)
- TOPPAN-CERT

[1] This seal is for use on the organization's website only; it cannot be used on any other materials.

Last updated February 28, 2011

提供サービスを明確にしておく

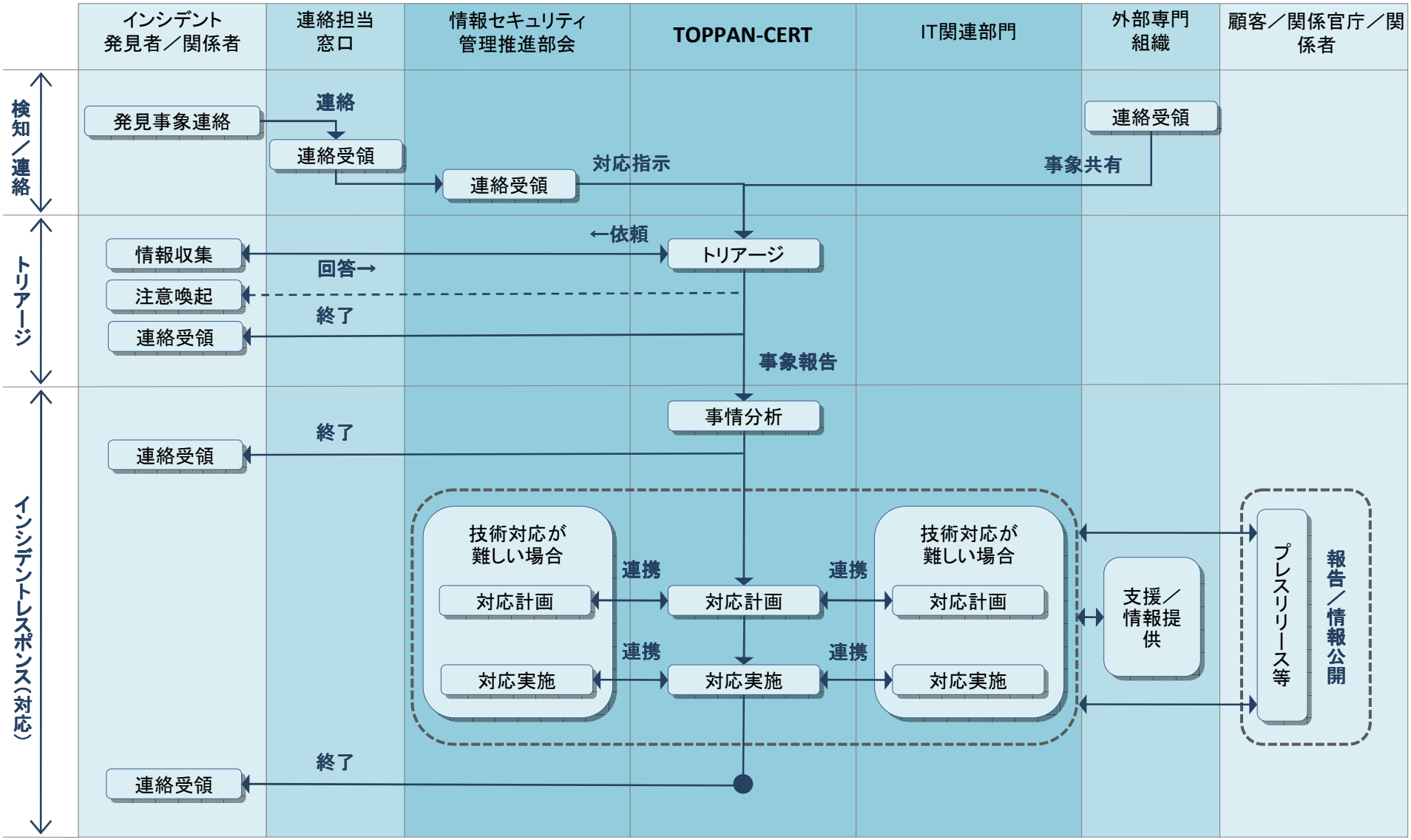
- 事前対応サービス
  - アナウンス
  - 技術動向監視
  - セキュリティ関連情報の提供
- 事後対応サービス
  - アラートと警報
  - インシデントハンドリング（分析／対応支援）
  - 脆弱性ハンドリング（分析）
  - アーティファクトハンドリング
- セキュリティ品質サービス
  - リスク分析(ペネトレーションテストを含む)

ウィルスやマルウェアは
取り扱いしない

⇩

既存WGが担当

インシデントハンドリングフロー



- 事前対応活動
  - 2010年度
    - 各種ドキュメントの作成支援

      情報ｾｷｭﾘﾃｨｶﾞｲﾄﾞﾌﾞｯｸ、無線LAN/外部回線利用技術判断基準
    - 脆弱性に関する情報の収集・分析

      早期警戒情報(JPCERT/CC発行)取得開始、ソフトウェアアップデート勧告
    - 社内インフラ調査及び監査フォロー

      小石川ビル無線LAN利用状況調査、決済サービス改善支援
  - 2011年度
    - 外部公開サーバの状態を調査
    - 外部公開ファイルのプロパティ情報を調査
  - 2012年度
    - Android不正アプリのインストール状況を調査

- 事後対応活動
  - セキュリティ事故対応支援

    支援一例：Web改竄対応

    社外からの不正侵入対応
  - レポート作成
    - インシデント毎の対応報告書、月次報告書、年間活動報告書
- 外部連携
  - 日本シーサート協議会WGへの参加
    - シーサートWG
    - インシデント対応技術調査WG
  - 日本スマートフォンセキュリティ協会への参加
  - 他チームとの交流

    議題一例：インシデント管理、スマートデバイスの取り扱い、人材育成

印刷テクノロジーで、
世界を変える。

TOPPAN

ご清聴ありがとうございました

TOPPAN-CERT連絡先：cert@toppan.co.jp