FUJITSU

shaping tomorrow with you

標的型攻撃時代に求められる組織のサイバーセキュリティ対策

2016年1月18日

富士通株式会社
サイバーディフェンスセンター長
奥原　雅之

目次

FUJITSU

1. 情報セキュリティポリシーとその周辺概念
2. 富士通の情報セキュリティマネジメント
3. 富士通のCSIRT*機能
4. 標的型サイバー攻撃の現状
5. 標的型サイバー攻撃への備え

*CSIRT: Computer Security Incident Response Team

FUJITSU

1. 情報セキュリティポリシーとその周辺概念

セキュリティポリシー

FUJITSU

世間の定義

情報セキュリティポリシー（じょうほう-, information security policy）とは、企業などの組織における情報資産の情報セキュリティ対策について、総合的・体系的かつ具体的にとりまとめたもの。（Wikipedia 日本語版 http://ja.wikipedia.org/）

一言で言えば

セキュリティ対策について意思決定したもの。

セキュリティポリシーFAQ

FUJITSU

Q：質問	A：回答
セキュリティポリシーには何を書けばいいか。	セキュリティ対策について、組織で意思決定したものはすべて。何のために対策するのか、どのセキュリティガイドラインに準拠するのか、具体的に何をするのか、意思決定の結果として残すべきものは何でも書いてよい。逆に、意思決定がいらないもの（法律の要求事項など）は書く必要はない。
セキュリティポリシーはどの程度具体的に書けばよいか。	可能な限り具体的に。具体的に書かなければ、意思決定を現場に一任するという意味になる。
セキュリティポリシーに書くセキュリティ対策のレベルや内容はどのように決めればよいか。	どのように決めてもよい。セキュリティアセスメントは第三者にその妥当性を説明する道具としては便利である。
組織の情報セキュリティポリシーから、ファイアウォールポリシーまで、世の中にいろいろなセキュリティポリシーがあるのはなぜ。	いずれも「セキュリティ対策に対して意思決定した結果」である。

スコープ（適用範囲）

FUJITSU

■ 世間の定義

明確な定義はない。例えばISO/IEC 27001では「事業・組織・所在地・資産・技術の特徴の観点から、ISMSの適用範囲及び境界を定義する。」とある。

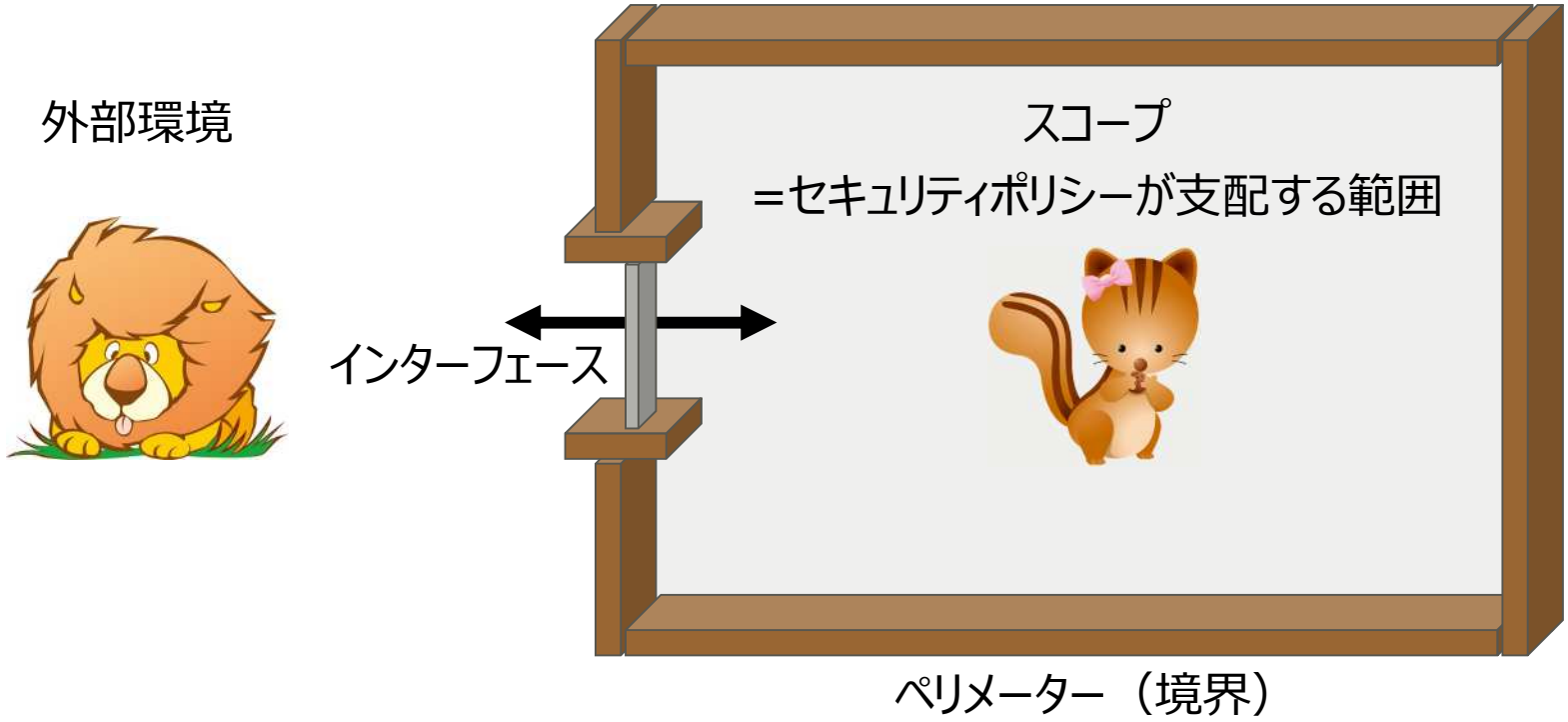
■ 一言で言えば

セキュリティポリシーの支配が有効となる範囲。

スコープとペリメーター

FUJITSU

- 適切な強度を持ったペリメーター（境界）がスコープを守る（＝セキュリティポリシーの有効性を保障する）
- 外部との交換がある部分（インターフェース）は、スコープ内部と外部のポリシーを調整する機能が必要になる



情報漏洩

FUJITSU

■ 世間の定義

パソコンやコンピュータで管理していた企業情報、行政文書、個人情報などが、管理上の問題などで外部に漏れてしまうこと。（セキュリティ@Nifty http://www.nifty.com/）

■ 一言で言えば

情報が想定されない形でスコープの外に出ること。
（セキュリティポリシーの支配下から外れること）

情報漏洩ケーススタディ

FUJITSU

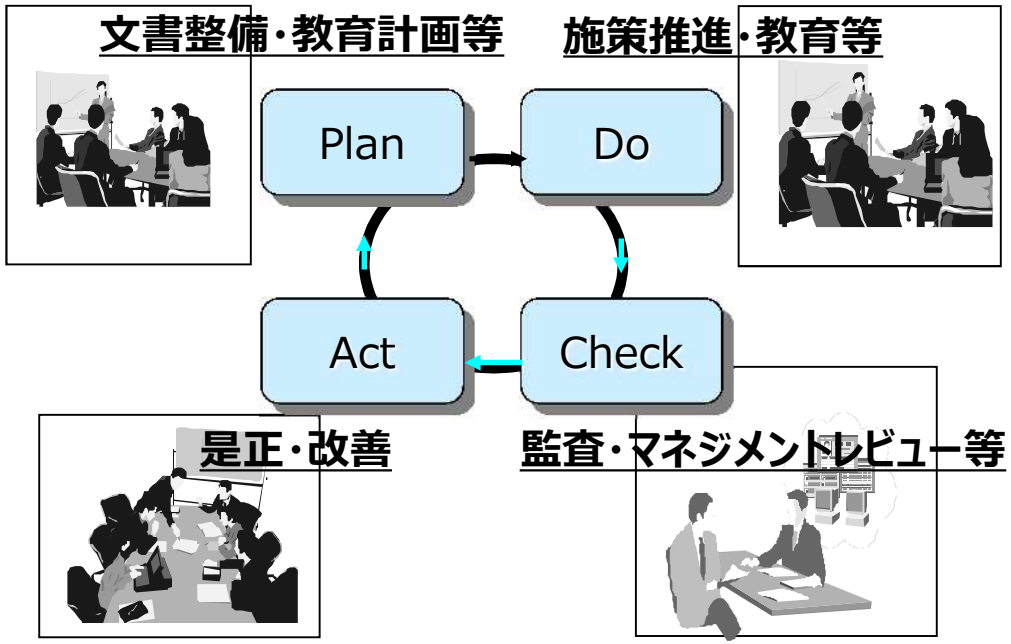
事例	「世間」の理解	「正しい」理解
業務情報を自宅に持ち帰り、個人PCで作業していたところ、P2Pファイル交換ソフトを利用するウイルスにより業務情報がネットに流出した。	P2Pファイル交換ネットワークに情報が流出したので情報漏洩。	業務情報が（ポリシーの支配が及ばない）自宅のPCに持ち出された時点で情報漏洩。
会社支給PCを移動中に電車内で紛失した。PCのHDDは暗号化されており、パスワードを知らない第三者は読めない。	情報漏洩事件だが、暗号化対策によりリスクは軽減できた。	移動中のPCを暗号化することにより情報を保護するポリシーのコントロール下にあることは変わらないので、情報漏洩ではない。（cf. 通信の暗号化）
関係者外秘の情報を、業務上関係がある社内の要員にメールで送った。	関係者に渡したのだから問題ない。	渡した相手が、その情報の取り扱いポリシーを理解しており、かつそのとおり扱ってくれる保証がなければ情報漏洩。

2. 富士通の情報セキュリティマネジメント

セキュリティマネジメントフレームワーク

FUJITSU

セキュリティマネジメントフレームワーク（SMF）



- セキュリティ基本方針のもとセキュリティ施策を設定
- SMFにより、各本部・グループ会社が自立的・継続的に情報セキュリティ活動を推進

セキュリティ基本方針

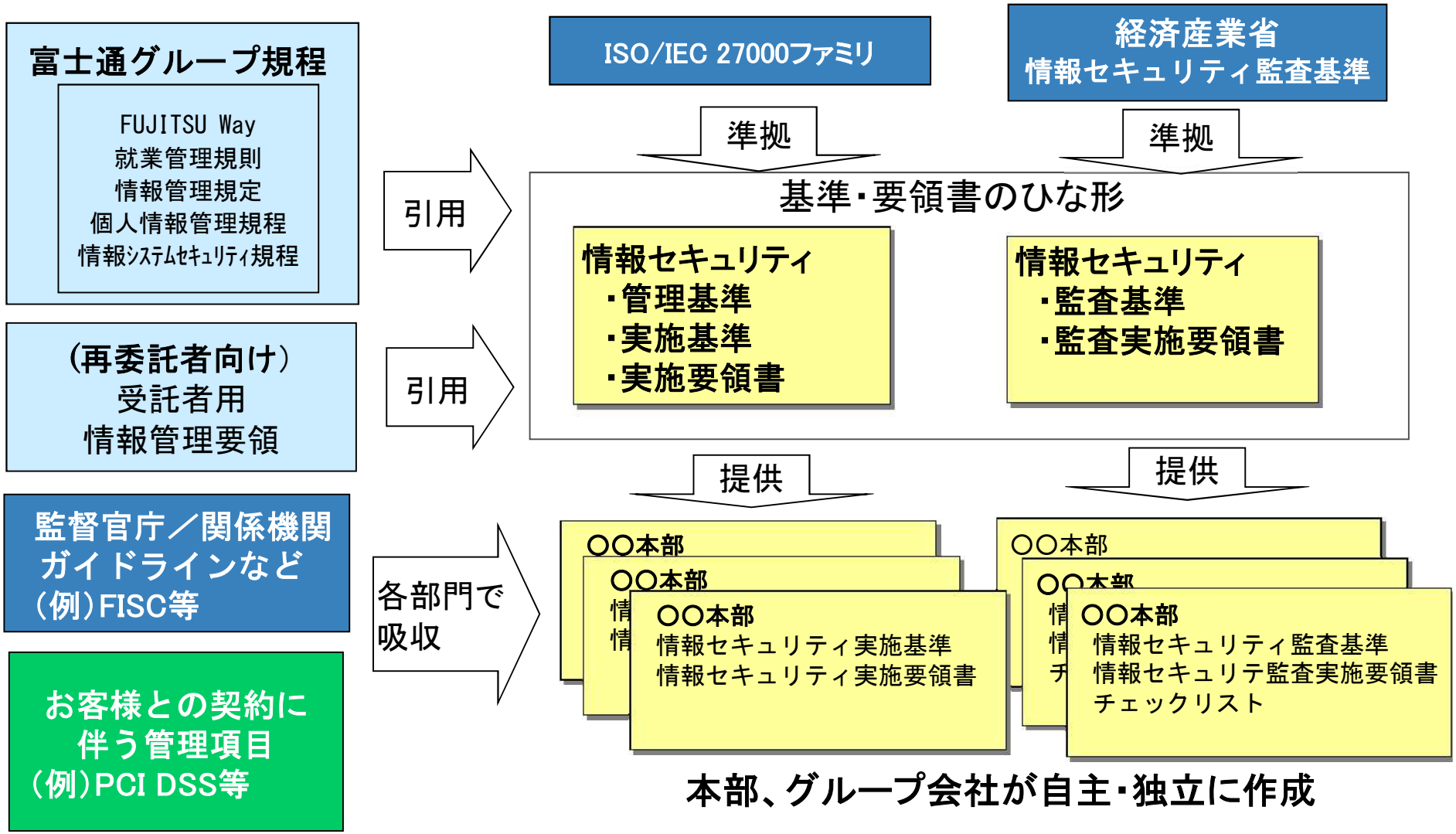
社内の情報管理
お客様資産の保護

セキュリティ施策

人的・組織的
情報資産
システム運用
システム開発
セキュリティ事故対応
SMF有効性評価

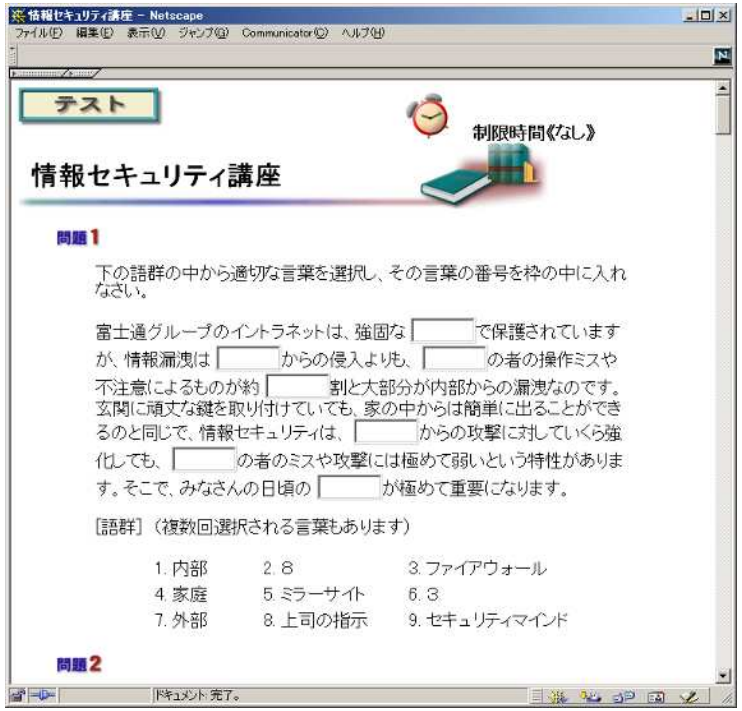
マネジメントドキュメントの整備

基準・要領書のひな型を利用して、本部、グループ会社が自主・独立に基準・要領を作成



従業員教育

- 全社員教育
  - 毎年、全従業員を対象に情報セキュリティに対するe-Learningを実施
- セキュリティ専門家教育
  - 各部門の情報セキュリティ管理責任者向けに、「情報セキュリティ管理者教育」を実施
  - 各部門の内部監査を実施する監査責任者と個々の監査を行う監査人向けに、「情報セキュリティ監査人教育」を実施
  - 監査人については、監査品質のレベルアップとキャリアパスのため、日本セキュリティ監査協会(JASA)の資格取得の支援



2012/3累計数

教育区分	計画	実績
情報セキュリティ管理者	300	563
情報セキュリティ監査人	700	840
JASA情報セキュリティ監査人	80	141

情報管理ハンドブック、ポケットブックの配布

社外秘

【必携】

ISC2050P-0010

情報セキュリティ ポケットブック
（ソリューションビジネスグループ用）

はじめに

情報セキュリティでは、外部からの攻撃に備えることに加えて、社員が常に高い意識を持って適切な情報管理を維持することが重要です。

本書は、情報セキュリティに関する指針を「必携書」として手帳等に挟んで利用することで、各自が情報セキュリティに関するマインドの向上や具体的アクションを確実に且つ、継続して行えることを目的としています。

なお、本書は、2009年12月時点の社内規定や指示からセキュリティに関する部分を引用し、利用者の立場・場面に応じて再構成しています。

FUJITSU

SBGセキュリティ委員会
〔2009年12月 V2. 4〕

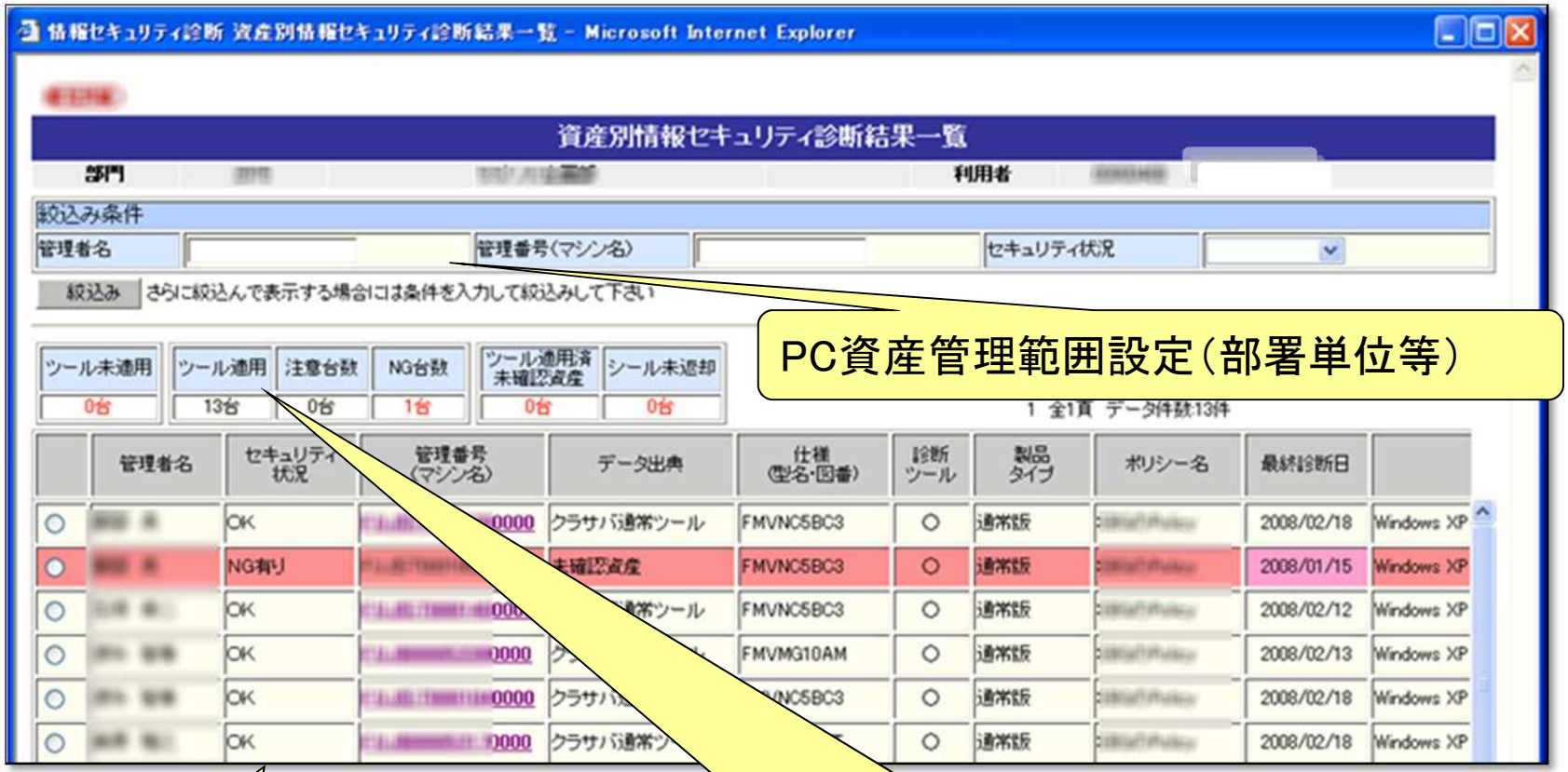
所属
氏名

セキュリティチェックの自動化(1)

セキュリティチェックの自動化(2)

FUJITSU

- PCの資産情報およびセキュリティ状況を一括で管理



PC資産管理範囲設定(部署単位等)

PC資産管理ツール適用状況(台数)

各PCのセキュリティ状況(OK、NG)

セキュリティパッチ、ウイルススキャン、Winny等禁止ソフト等

電子メールの誤送信対策

- 富士通グループの全パソコンに電子メールの誤送信対策ツールを導入
- 電子メールの宛先を自動的に識別して、外部への送信について送信者に再確認を促す
- 警告表示による注意喚起
  - タイトル、本文、宛先、添付ファイル名をチェック

パソコンのセキュリティ対策

FUJITSU

パソコンへの不正アクセス防止

- BIOS,HDDパスワードの設定
- Windowsパスワードの設定
- スクリーンセーバーの設定

ウイルス感染防止

- セキュリティパッチの適用
- ウイルス対策ソフトの導入
- 定義ファイルの更新
- 定時スキャンの実施

盗難紛失時のセキュリティ対策

- 社内標準パソコンの導入

その他の対策

- 個人所有PCの禁止
- ファイル共有ソフトの導入禁止
- 廃棄時の情報完全消去
- サポート終了OSやソフトの使用禁止

携帯電話のセキュリティ対策

FUJITSU

■ 携帯電話のセキュリティ対策

- ■ パスワードロック、指紋認証の設定
- ■ 電話帳への個人情報の登録禁止
- ■ 携帯電話メールの使用は原則禁止（緊急連絡時は秘密情報は記載せず即削除）

■ スマートフォン／タブレットのセキュリティ対策

- ■ ガイドラインを策定中

セキュリティ対策定着のための施策

FUJITSU

- トップによるセキュリティ意思の伝達
  Web公開/社員へのダイレクトメール、動的コンテンツ(ストリーミング)が効果的
- 期毎の目標設定 / 目標達成率の公開、役員への報告
  依頼メールやアナウンスの繰り返しと、定期的な状況報告 (継続的な活動
- 各部門のセキュリティ活動に対する表彰制度の確立
  当初は表彰優先(社長賞等)　推進進行後は非積極的な部署にペナルティも検討
- 各種ログ(リモートアクセスや社外アクセス、メール等)の統計情報公開
  監査/監視していることを明にまたは暗に通知し、内部犯罪や不正を抑制対策の徹底を図る
- セキュリティに関する小冊子・ハンドブックの配布
- 教育メディア(ビデオ/DVD)貸し出し
- セキュリティグッズの配布(ステッカー、ポスター、マウスパッドなど)
- PDA/ノートPC向けセキュリティ啓蒙コンテンツ、啓蒙スクリーンセーバ
- 防災訓練 (コンティンジェンシー訓練)

マネジメント活動の評価

FUJITSU

SBG各部門

SMF活動状況

Plan	体制整備、推進計画、文書整備、 監査計画、教育計画
Do	施策推進、周知徹底、教育、 推進会議
Check	監査準備、監査実施/報告、 マネジメントレビュー
Act	是正、改善

PCセキュリティ診断

セキュリティ
事件・事故対応

発生部門のみ

情報セキュリティ活動評価

調査依頼
（評価指標）

回答
（Web入力）

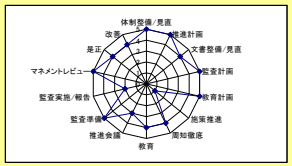
本部のみ実施

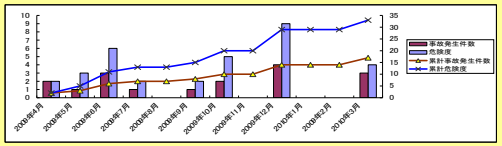
DOEXPRESS
診断結果
自動取得

事件事故評価

セキュリティ
事件事故
報告

SBGセキュリティ委員会HP



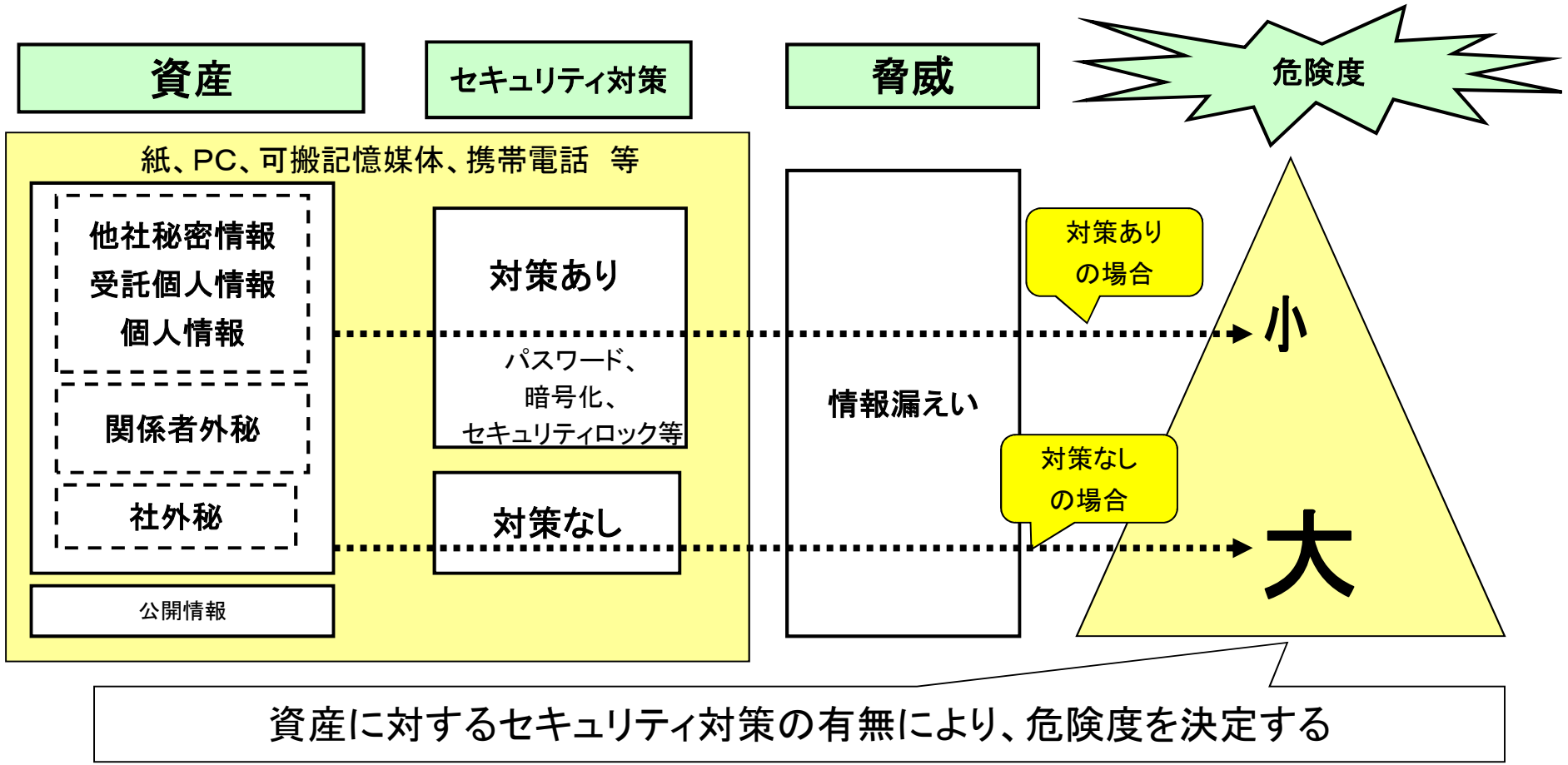


SBGセキュリティ委員会（情報セキュリティセンタ）
集計・分析・可視化

セキュリティ事件・事故の評価(1)

FUJITSU

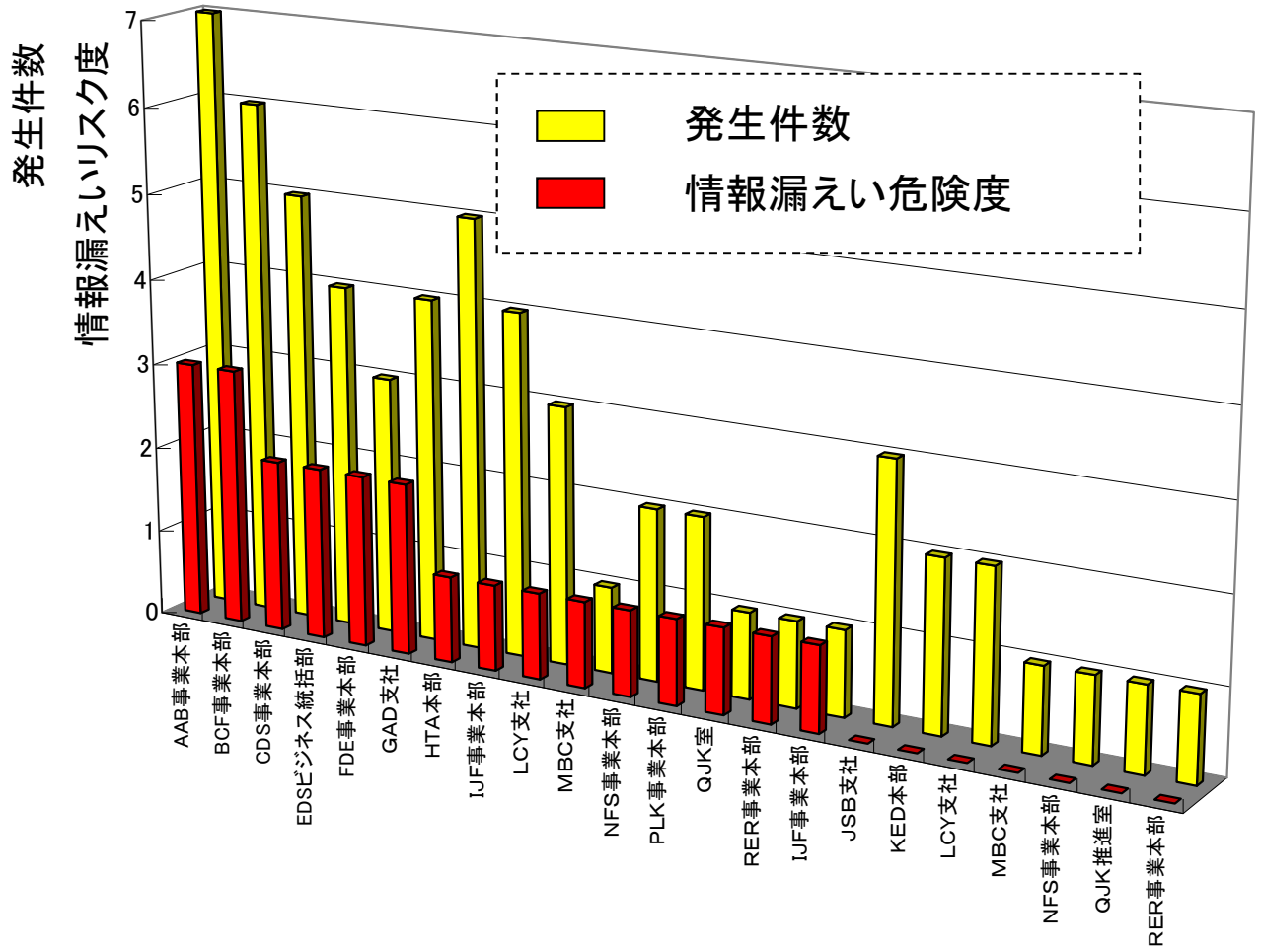
■ 情報漏えいをターゲットに絞り、漏えいした情報資産の種類やセキュリティ対策の有無で事件・事故の危険度として評価



セキュリティ事件・事故の評価(2)

FUJITSU

- 情報漏えい危険度を４段階にレベル付け評価することで、発生件数では見えない事件の重大性を可視化



セキュリティ事件・事故の評価ポイント

FUJITSU

- 「結果の重大性」よりも、「発生に至ったプロセスの問題点」を評価する
  - ルール通り運用していたが発生を防げなかった
  - ルールはあったが守られていなかった
  - ルール自身が存在しなかった

- 事件・事故発生時に、対策で被害が低減された場合はむしろ「投資の成功事例」と評価する
  - パソコンを紛失したが重要情報は暗号化されていた
  - 携帯電話を紛失したが端末には暗証がかけられていた
  - ただし社内手続き上「無罪」とするためには明確なエビデンス（証拠）の提示が必要

情報セキュリティ監査

FUJITSU

- 各本部による内部監査の実施
  - 各本部の情報セキュリティ監査責任者が監査計画を立案し、各本部ごとに内部監査を実施する。
- 情報セキュリティ委員会による第三者監査の実施
  - 各本部の情報セキュリティマネジメントの実施状況について、本部外の監査人が監査を実施する。

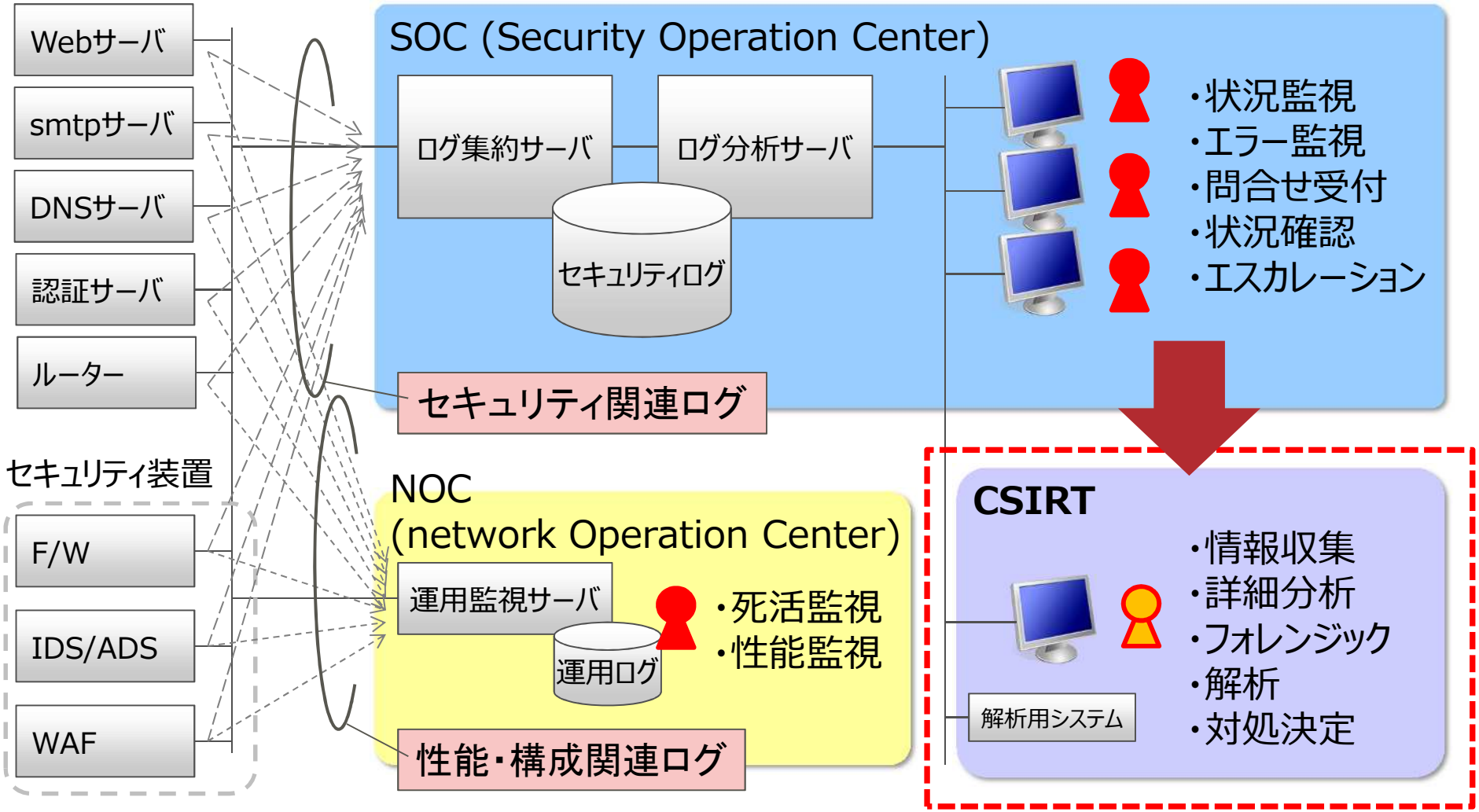
第三者監査チェック項目

基本方針及び文書類	運用ルール	マネジメントレビュー
適用範囲	教育	委託、第三者等
体制	関連部門との連携	現場の運用
計画	内部監査	

3. 富士通のCSIRT機能

CSIRTの機能

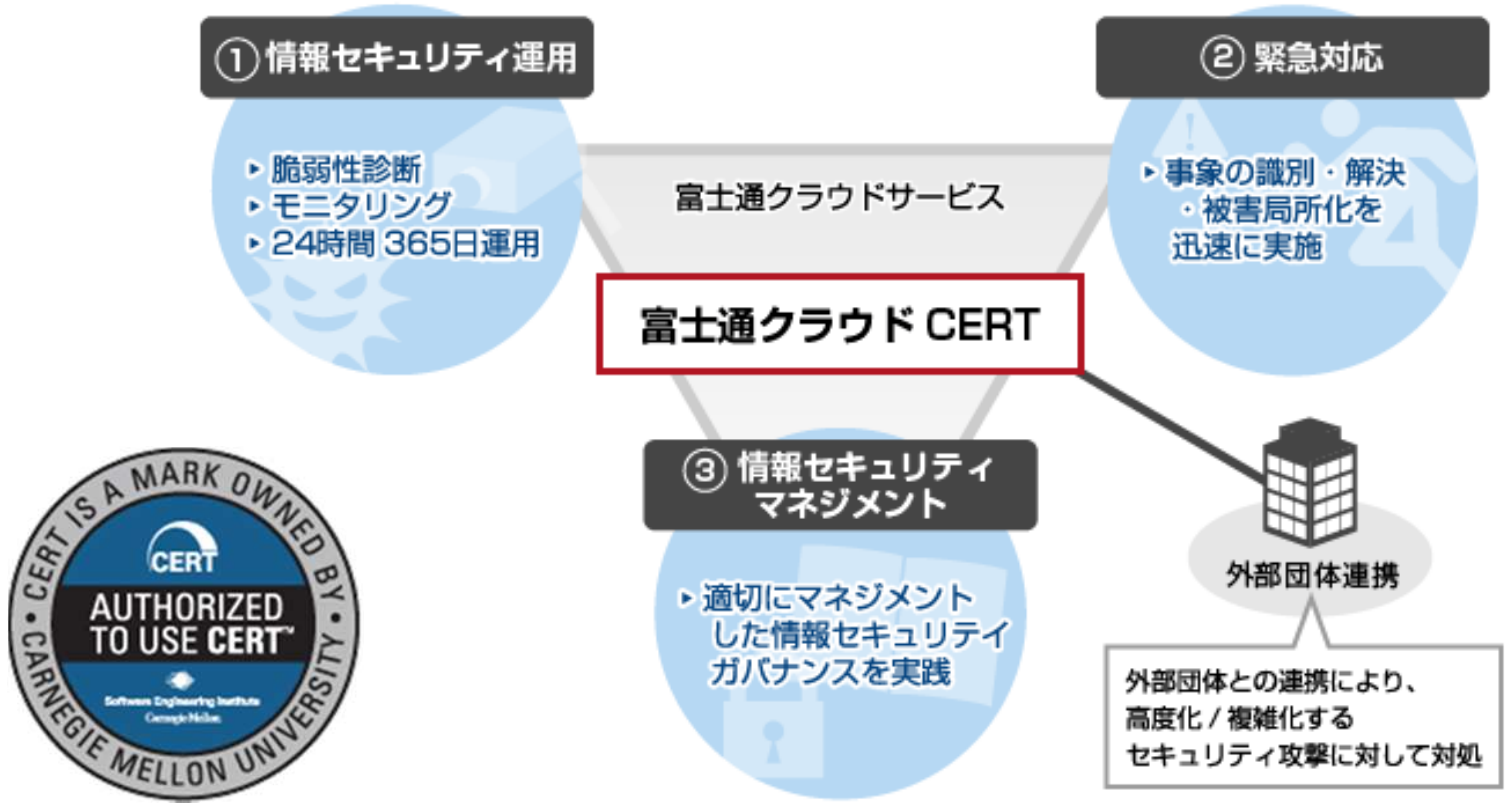
- セキュリティインシデントに関する報告を受け取り、調査し、対応活動を行う組織
- 高度なセキュリティ知識を持ったセキュリティリスクコントロールを実施



富士通クラウドCERT

FUJITSU

- クラウドサービスにおけるセキュリティの脅威（サイバーテロ・不正利用・情報漏洩など）に対して迅速に対応する「富士通クラウドCERT(FJC-CERT)」を設立

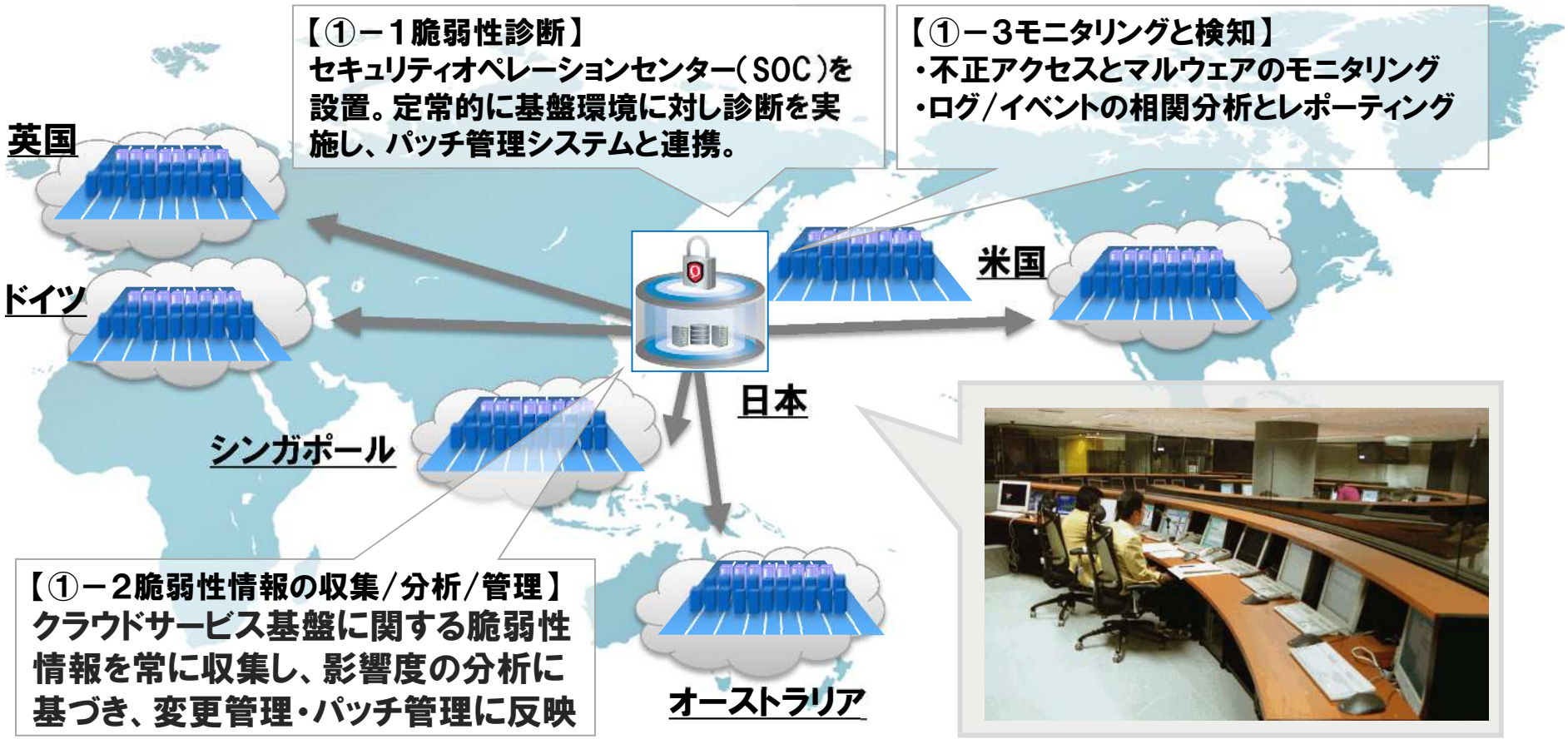


＊ CERT (Computer Emergency Response Team)

CSIRT機能(1)：セキュリティ運用

FUJITSU

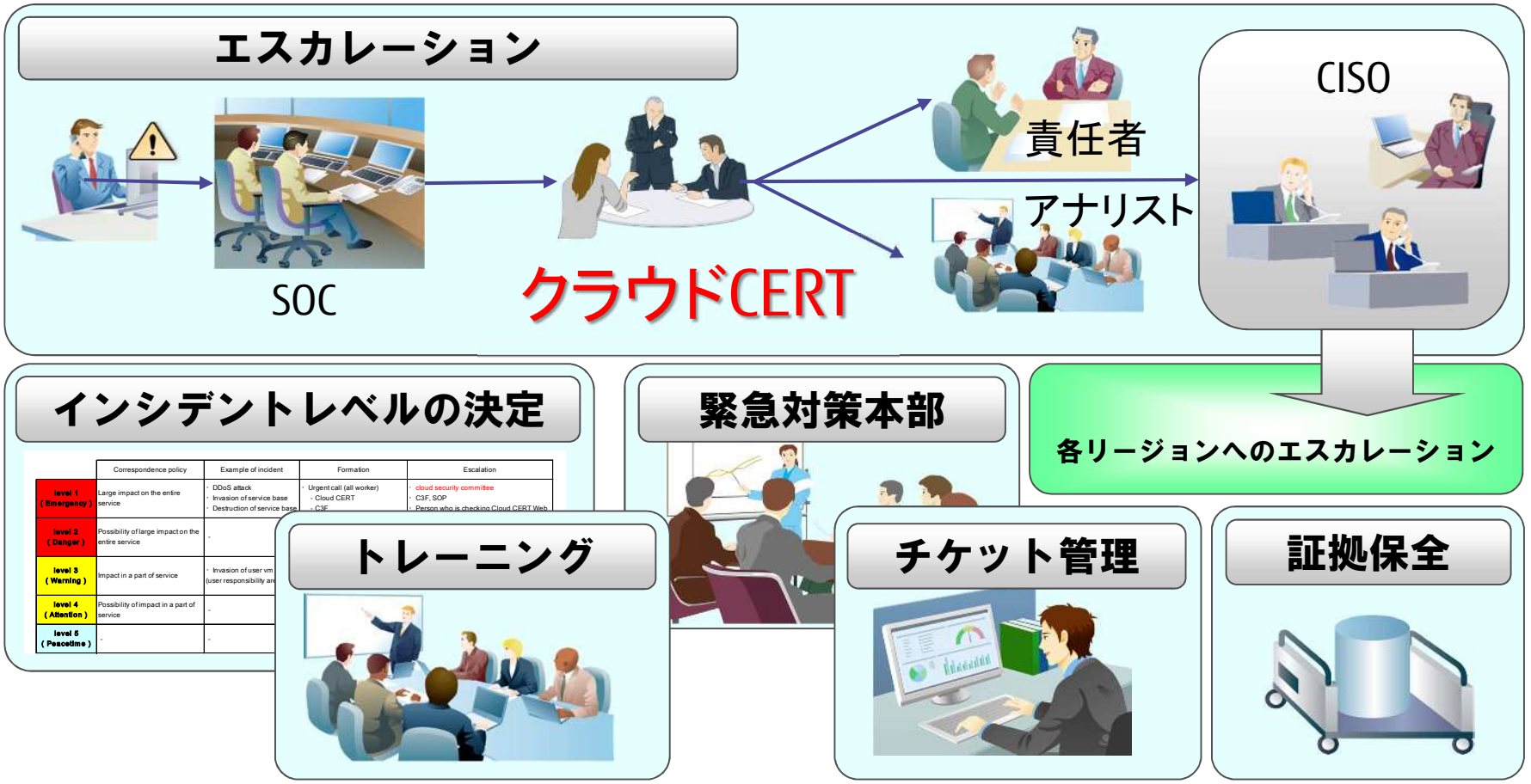
■ クラウドサービス基盤に対する脆弱性診断やモニタリングなどの情報セキュリティ対策を実施し、24時間365日体制で運用



CSIRT機能(2)：緊急対応

FUJITSU

■ インシデント発生時のプロセスを定め、万が一のインシデント発生時には、事象の識別・解決・被害局所化を迅速かつ確実に実施



CSIRT機能(3)：サービスマネジメント

FUJITSU

■ 富士通クラウドサービスにおける「人」「モノ」「情報」を適切にマネジメントし、情報セキュリティガバナンスを実践

活動内容

✓クラウドサービスのセキュリティ方針の討議と承認
✓定常的なリスク分析の報告と対処方針の承認
✓グローバルな社外組織と連携体制についての協議
✓コンプライアンスや監査要求事項への対応の討議

CSIRT活動実績(2014年度)

FUJITSU

FJC-CERTの活動

リスクコントール

海外拠点5リージョンを含むクラウド基盤のセキュリティ診断／監視／分析

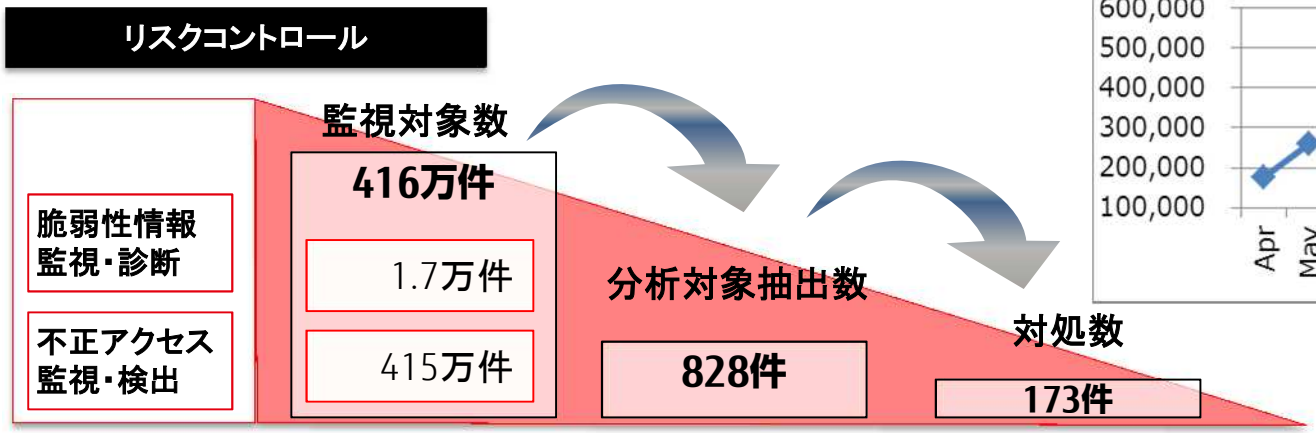
- 脆弱性ウォッチ／診断：1.7 万件
- 不正アクセス監視／検出：415万件

主な緊急出動

- 製造メーカー、官公庁、医療機関、ほか

その他

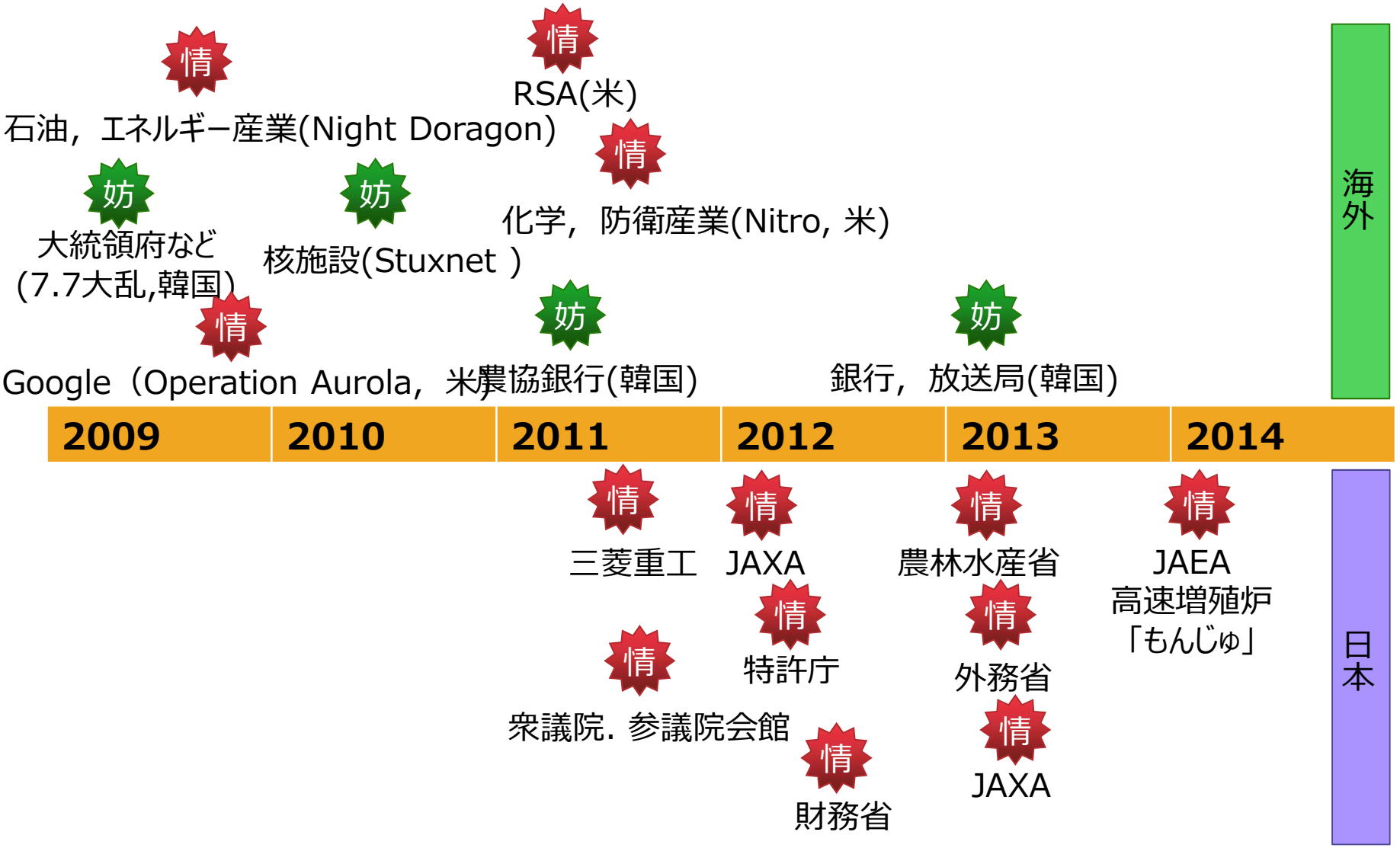
- FIRST、日本シーサート協議会など外部団体への参画



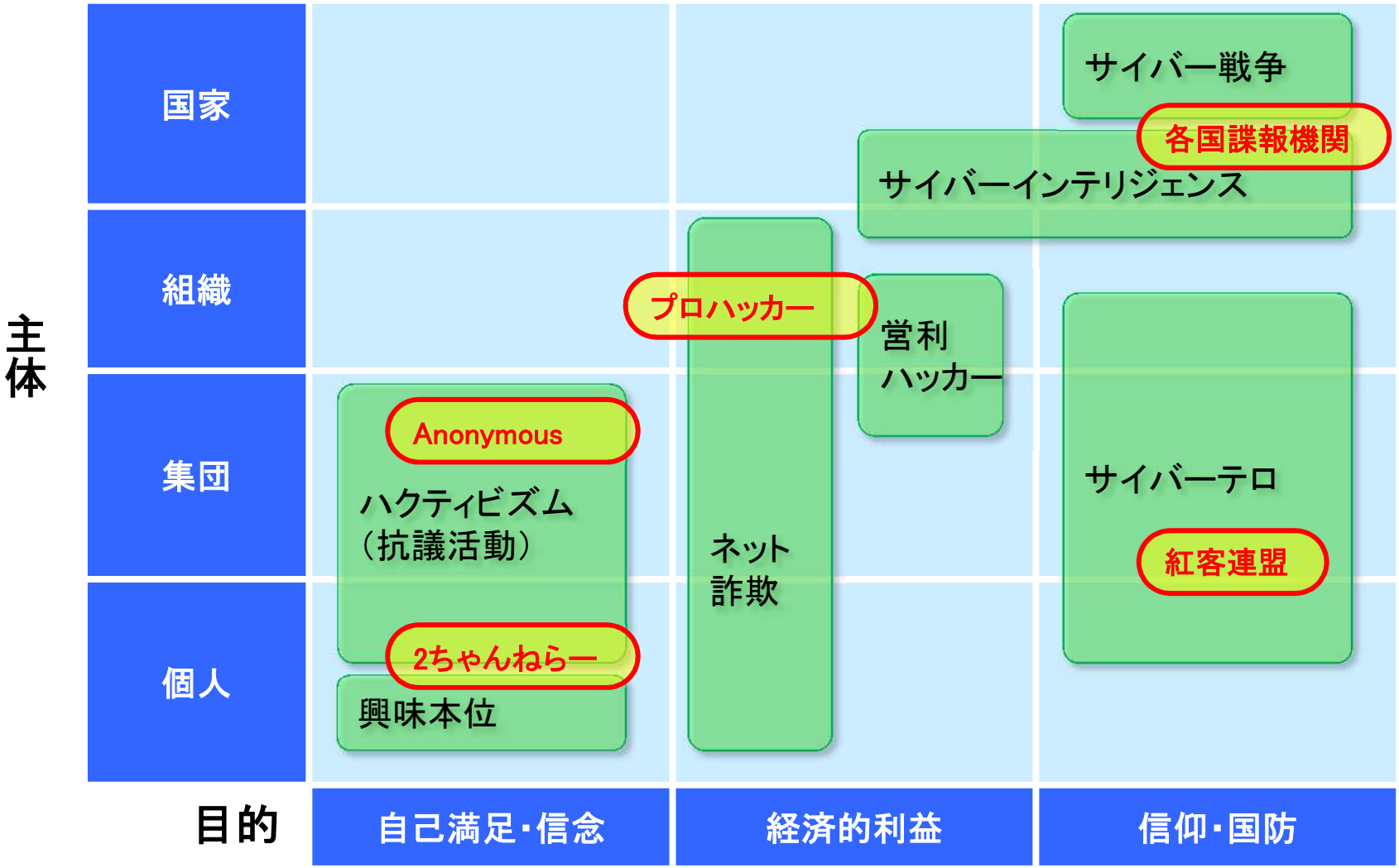
FUJITSU

4. 標的型サイバー攻撃の現状

標的型サイバー攻撃事例



サイバー攻撃の主体と目的



※1）ハクティビズム：ハッカーとアクティビズム（積極行動主義）をあわせた造語で、社会的・攻撃的な主張のもとに、ハッキング活動を行うこと
※2）サイバーインテリジェンス：サイバー空間で行われる諜報活動（intelligence）のこと

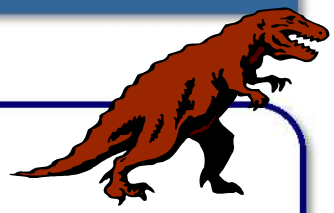
セキュリティ脅威の変化

FUJITSU

■ 昨今のサイバー攻撃は攻撃者が明確な目的をもってターゲットを選定し、目的を達成するまで繰り返し高度かつ巧妙な攻撃を仕掛けてくる

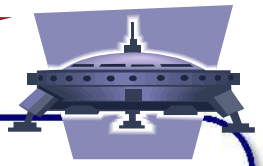
脅　威

これまで



■ 怪獣来襲モデル
- 脅威は一過性
- 撃退すればハッピーエンド

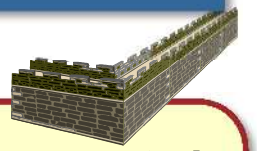
これから



■ 悪の秘密結社モデル
- 狙いを定めて目的達成まで繰り返し襲来
- 防御側を研究した高度な攻撃

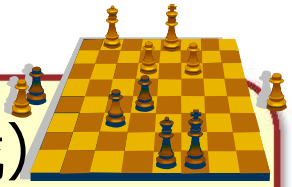
対　策

これまで



■ 水際防御（ペリメーター防御）
- 境界を全力で守る
- 境界の内側は安全地帯

これから



■ 多層防御（総力戦）
- 境界に頼らない（頼れない）
- 多種の脅威に総力で対応する

標的型攻撃の流れ

FUJITSU

■ 念入りに計画をたてて，標的を攻撃する

攻撃フェーズ		攻撃手法
0	攻撃準備段階	標的に関係する組織を攻撃して情報収集
1	初期潜入	ソーシャルエンジニアリング 標的型メール,Web ウィルス入りUSBメモリ SNSの誘い
2	攻撃基盤構築	バックドア（RAT: Remote Access Tool）構築 ドライブバイダウンロード
3	諜報活動 （システム調査）	アカウント情報の窃取，特権奪取 ネットワーク，ホスト，アプリ情報の収集 目的の情報の存在箇所の特定
4	攻撃目的の遂行	メールやWebアクセスなど通常のアクセスのふりをして，機密情報を送出 HD内データ破壊，システムブート領域破壊

初期潜入の手口

FUJITSU

標的型メール

- 以前
  - 不審なメール（成りすましメール）
  - 標的毎にカスタマイズされた特製メール
- 最近
  - 正規アカウントからのマルウェア添付メール
  - 少しずつカスタマイズされた大量のメール（はえ縄型）

Webサイト

- 以前
  - 不審なサイト（フィッシング詐欺サイト）でマルウェアに感染させられる
- 最近
  - 改ざんされた正規サイトにマルウェアに感染させられる
  - 標的の関連企業のWebサイトを改ざん（水飲み場型）

内部への侵入を防ぎきれない

FUJITSU

5. 標的型サイバー攻撃への備え

標的型攻撃への備え

FUJITSU

- 今日のサイバー攻撃は組織全体の総合的なセキュリティ対策力が試されている
  - 各種セキュリティ対策の技術力
  - 被害を最小限に留める運用力
- 「脅威は内部にいる」ことを前提とした対策が必要
  - 境界防御モデルを捨てる
  - 追跡性を確保する
- 今できることをやる

境界防御モデルを捨てる

FUJITSU

- 標的型サイバー攻撃に使われるRAT（踏み台）も、内部不正も、「境界内に攻撃者がいる」モデル
- 「セキュアゾーン」の発想を捨て、本当に守らなければならないものは内部でさらに防御を追加する（多層防御）
  - 例：重要ファイルの暗号化、重要情報専用ファイルサーバの設置、重要情報を扱うPCと普段使い（メール、Webアクセス）PCの分離
- 最近のトレンドではディレクトリサーバ（Active Directory）がよく狙われる
  - Active Directoryの管理者権限を扱うPCは特に念入りに管理
- 適度なバランスが重要
  - 何でも守ればよいというものではない
  - 運用コストが過大なものはいずれ破たんする（日本年金機構事例）

追跡性を確保する

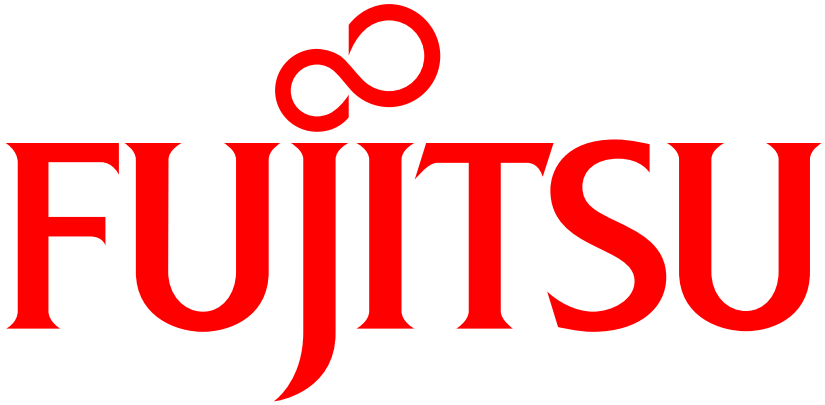
FUJITSU

- 重要情報のアクセスログ、ネットワークログを記録する
  - インシデント発生時は「何が起きたか」「何が起きているか」を正しく把握することが重要
  - 特に利害関係者が組織外にいる場合は必ず説明を求められる
- ログを攻撃者に消されないように工夫する
  - 他のサーバ（ログサーバ）に転送するのが一番現実的
- ログを追跡できるようにしておく
  - IDは一人に一つ（共用していると誰だか特定できない）
  - サーバの時刻を正確に合わせておく（NTPの利用）
- ログの保存期間が過ぎる前に何とかして攻撃を検知する
  - 攻撃が数か月以上続くと侵入時のログが消失する

今できることをやる

FUJITSU

- 直面するリスクを正しく理解し、やらなければならないことを地道に確実に実施する
  - 「ゼロリスク」は実現不可能
  - 標的型攻撃をすべて撃退する「まほうのたて」はない
  - リスクの発生ではなくリスクの拡大を阻止する
  - 「今できること」を積み重ねることで組織の抵抗力が上がる



shaping tomorrow with you