セキュリティ脅威と対策の要諦

＝エラーは〝防ぐ〟のではなく〝コントロール〟する＝

2016.12.9

LAC Co., Ltd.
常務理事
Executive Consultant
内田　昌宏
Masahiro Uchida

LACセキュリティサービス
多彩なセキュリティサービスでお客様をご支援

LACには「サイバー119」があります。

サイバーセキュリティ経営ガイドライン
＝サイバーセキュリティ経営の3原則＝

経営者が認識する必要がある「３原則」

- 経営者のリーダーシップ
- パートナーシップ連携
- 関係者とのコミュニケーション

↓

経営者が〝決断・推進〟しなければ、先へは進めない！

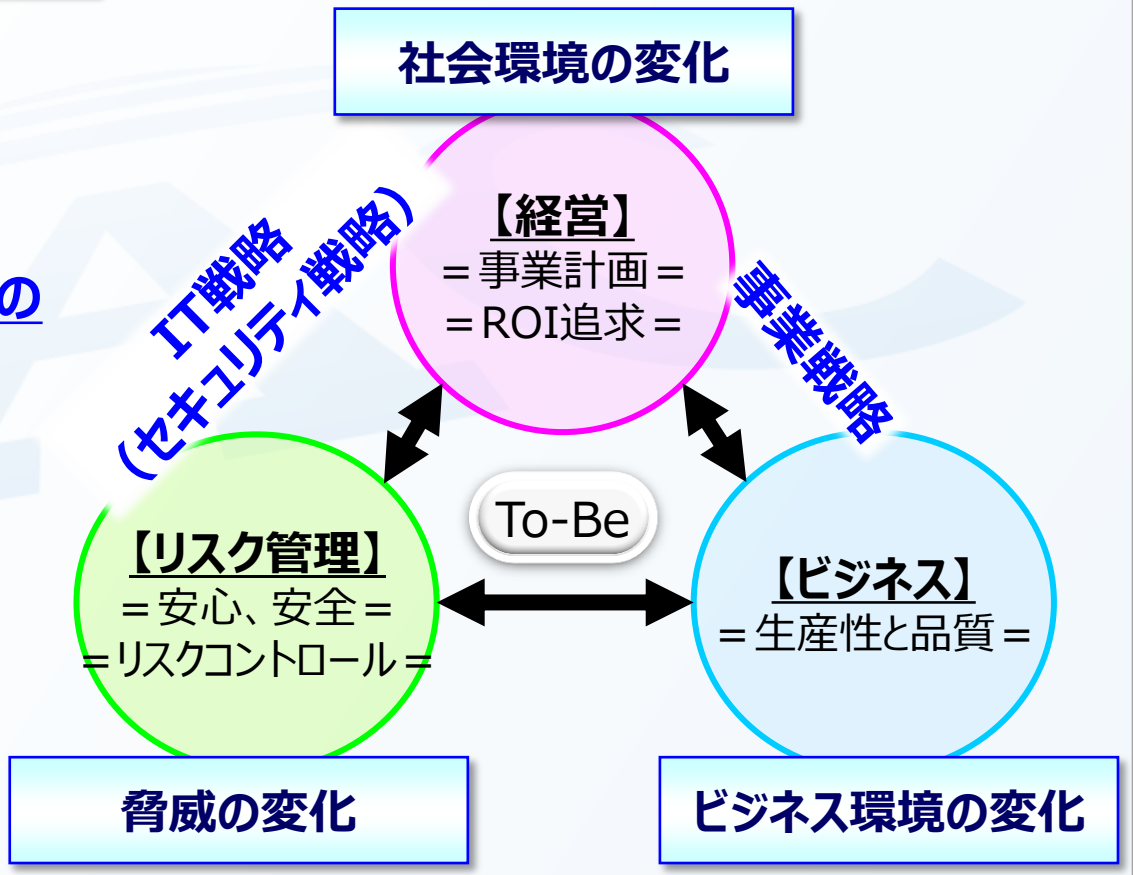
↓

セキュリティ投資に対するリターンの算出は不可能！

しかし…

↓

これだけでは、経営者は納得できないのではないか？



【事例に学ぶ】
標的型ウイルスによる情報漏えい（2015年6月）

速報 > 社会 > 記事

年金機構の125万件情報流出　職員、ウイルスメール開封

2015/6/1 19:12

小 中 大　保存　印刷　リプリント　▼共有

日本年金機構は1日、年金情報を管理するシステムに職員の端末を通じて外部から不正アクセスがあり、個人情報約125万件が外部に流出したとみられると発表した。情報には基礎年金番号や氏名が含まれ、うち約5万2千件には生年月日や住所も含まれていた。職員がウイルスの組み込まれた電子メールの添付ファイルを誤って開封し、不正アクセスされたと想定されるという。

同日記者会見した水島藤一郎理事長は「深くおわびする。誠に申し訳ない」と陳謝した。同機構を巡り、これだけ大規模な情報流出が発覚したのは初めて。

画像の拡大

個人情報が流出し、謝罪する日本年金機構の水島理事長(中)ら(1日午後、厚労省)

流出したのは年金記録を管理するのに一人一人に割り当てられている基礎年金番号と氏名の計約125万件。このうち約116万7千件には生年月日が、約5万2千件には住所と生年月日が含まれていた。

流出した約125万件のうち、約70万件にはパスワードが設定されていたが、それ以外は設定されておらず、機構の内規に違反した状態だった可能性があるという。

年金機構の125万件情報流出　職員、ウイルスメール開封
http://www.nikkei.com/article/DGXLASDG01HCD_R00C15A6000000/

【事例に学ぶ】
事故発生後の対応は適切だったのか？

5月8日　内閣サイバーセキュリティセンタ（NISC）が不審な通信を察知、機構に通
機構では感染したパソコンのケーブルを抜いて通信を遮断

5月18日　機構職員の個人アドレスに、約100通の標的型メールが届く
3台のパソコンがウイルス感染

この時点で注意喚起を行うべき

5月19日　警察に捜査依頼

5月20日　3度目の不審なメールが届く、1台感染？？
5月22日、23日　九州で不審な通信検知　東京でも不審な通信検知

対処が遅すぎる…危機意識が低い

5月28日　警察から情報流出の
　└ 約3週間、インターネットに接続したままの状態
5月29日　インターネットを遮断

6月1日　記者会見

公表が遅すぎる…1か月後にようやく会見

» **経営の不参加、無監督がばれた**
» **〝やっていること〟になっていた**
» **建前の監査がばれた**

経営者が認識する必要がある「３原則」
- ▲ **経営者のリーダーシップ**
- ▲ **パートナーシップ連携**
- ▲ **関係者とのコミュニケーション**

【事例に学ぶ】
内部犯行による情報セキュリティ事故（2014年7月）

ベネッセHD、顧客情報漏洩　最大2070万件

2014/7/9 17:26

小 中 大　保存　印刷　リプリント　▼共有

ベネッセホールディングス（HD）は9日、760万件の顧客情報が漏洩したと発表した。最大で2070万件に達する可能性がある。通信教育「進研ゼミ」を含むサービスが対象。漏れたのは子供や保護者の住所や氏名、電話番号、子供の性別や生年月日など。

社内調査を進めるなかで特定のデータベースから顧客情報が何らかの形で外部に持ち出されていた。

6月下旬から通信教育事業を手掛けるIT事業者からのダイレクトメールが顧客に届き始め、顧客から問い合わせが急増していた。

ベネッセの顧客リストに基づく営業がされている可能性があり、調査を実施。760万件の漏洩を確認した。データベースに保管されている件数から推定し、最大2070万件が外部に漏れている可能性があるという。

画像の拡大

記者会見で頭を下げるベネッセHDの原田泳幸会長兼社長（9日午後、東京都中央区）

ベネッセＨＤ、顧客情報漏洩　最大2070万件
http://www.nikkei.com/article/DGXNASDZ09082_Z00C14A7000000/

【事例に学ぶ】
事故発生後の対応は適切だったのか？

6月26日以降　お客様センタへ〝DMやセールス電話がくる〟との問い合わせ急増
6月27日　問合せ急増を受け経営トップへ報告
　　社長判断により当該システム停止、全面調査を指示

6月28日　緊急対策本部設置
　　調査会社へ協力を依頼、緊急調査を開始

6月30日　経済産業省へ状況報告と対応について相談
　　警視庁へ状況報告と対応について相談

7月7日　社内調査により顧客情報DBから情報が持

7月9日　情報漏えいについて公表、
7月11日　新聞各社の朝刊にお詫び広
7月15日　再発防止に向けた第三者委

7月17日　警視庁が男性を不正競争防止法違反
　　経済産業省へ報告書を提出
　　調査経過と今後の対応会見

7月21日　漏えい情報の鑑定結果を発表

迅速な判断と行動

〝現時点〟では加害者
被疑者はグループ社員ではない
顧客への補償が後手に
↓
〝被害者感情〟が広報対応ににじみ出てしまった？

経営者が認識する必要がある「３原則」
- ○ **経営者のリーダーシップ**
- ○ **パートナーシップ連携**
- △ **関係者とのコミュニケーション**

【事例に学ぶ】
標的型ウイルスによる情報漏えい（2016年6月）

JTBの情報漏洩とセキュリティ：JTBで約793万人の個人情報が流出？ 情報漏洩の実態と対策とは

（1/4ページ）

2016.06.29

JTBにはがっかりした、社長の謝罪会見で記者が感じた違和感

井上 英明＝日経コンピュータ　2016/06/23　日経コンピュータ

目次一覧

「梅雨は情報漏洩の季節なのかもしれない」と、1年ほど前に当コラムで書いた（関連記事：年金情報流出問題、次はあなた）。嫌な予感ほど当たるのだろうか。2016年6月14日にジェイティービー（JTB）が最大で約793万件の個人情報が流出した恐れがあると公表した。

JTBは同日17時から国土交通省で記者会見を開き、冒頭で高橋広行社長が「お客様ならびに関係者のみなさまにご迷惑、ご心配をおかけしたことをお詫び申し上げます」と頭を下げた。記者は会見に出席し、約2時間にわたって取材した。

日経ITpro
http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/062000597/?rt=nocnt

【事例に学ぶ】
事故発生後の対応は適切だったのか？

2016年3月15日	取引先を偽装したメールが届き、i.JTBの端末がマルウェアに感染。
2016年3月19日～24日	i.JTBの商品情報配信制御サーバーより不審な通信の発生を複数確認。
2016年3月19日	システム監視会社よりJTB情報システムへ不審な通信を確認したと指摘。
2016年3月20日	i.JTBが不審な通信先の遮断措置を開始。 i.JTBがWebサーバーを社内ネットワークから遮断。
2016年3月21日	何者かがi.JTBのサーバー内にデータファイルを作成。 何者かがサーバー内に作成されたデータファイルを削除。
2016年3月25日	JTBが不審な通信先の遮断措置を完了。
2016年4月1日	JTB情報システムが削除されたデータファイルの存在を把握。
2016年5月13日の数日前	**JTB本社に事案がエスカレーションされる。**
2016年5月13日	JTB情報システム、i.JTBがセキュリティ企業と協力しデータファイルを復元。 顧客情報を記録したCSVファイルが含まれることを確認。
2016年5月16日	担当者からJTB IT担当役員へ報告。
2016年5月17日	IT担当役員からJTB社長へ報告。 JTB本社が事故対策本部を設置。
2016年5月30日	JTB本社が警視庁へ被害相談。
2016年5月31日	JTBが観光庁へ事案に関する相談。
2016年6月2日	i.JTBよりNTTドコモへ個人情報漏えいの可能性があると報告。
2016年6月10日	JTBが解析を行い、漏えいの可能 JTBよりNTTドコモへ調査結果を
2016年6月14日 17時	JTB本社が不正アクセスによる顧

空白の１ヶ月
対応が後手に

経営者が認識する必要がある「３原則」

？ 経営者のリーダーシップ

▲ パートナーシップ連携

▲ 関係者とのコミュニケーション

セキュリティ脅威を想定する

- **「頑強だが脆弱なシステム」**
  - 予想される脅威（外部脅威）には堅牢のはず…、予期せぬ脅威（内部犯行）にはきわめて弱い！
  - **レピュテーショナルリスクに直結する！**

脅威		脅威の概要・攻撃の目的
災害		サービス停止、要員確保、環境確保
外部脅威（サイバー攻撃）	不正アクセス（アタック）	インターネットに晒されている脆弱性の調査 不正侵入による組織内情報の破壊や窃取、サービス停止
	ウイルス（既知）	いたずら、システム障害（負荷増大）、情報破壊、情報漏えい
	標的型攻撃（未知マルウエア）	**バックドアの作成、アカウント情報窃取、PCやサーバ乗っ取り、情報窃取（産業スパイ活動）**
	DDoS攻撃	サービス停止（負荷増大）
	フィッシング攻撃	利用者（顧客）情報窃取、
	なりすまし	不正操作（不正な取引など）
	盗聴	アカウント情報の漏えい、業務情報の漏洩
内部過失	オペミス	操作ミス・設定ミスによる情報可用性への影響
	私物PC、私物デバイス	ウイルス感染、情報漏えい
	SNSの不適切な利用	**情報漏えい、ネット炎上、風評**
	野良アカウント放置（不正アクセスの誘発）	無効化すべきアカウントの不正利用、 不要な情報へのアクセスによる悪意の誘発
	紛失・盗難	情報漏えい
内部悪意	**情報持ち出し**	**故意による情報持ち出し**
	不正操作	**故意によるシステム障害**
	証拠隠滅	**ログの改ざん、消去**

セキュリティの取り組み

STEP 1
＝現状把握、リスク分析、ロードマップ＝

STEP 2
＝スコープ設定＝
＝プロセス定義＝

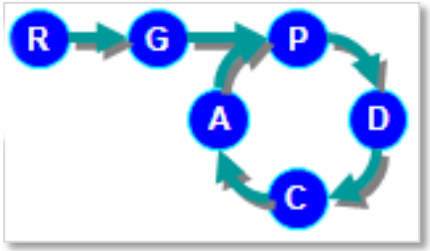
STEP 3-1
＝規定、ガイドライン文書化＝
＝合意形成＝

STEP 4-1
＝展開、周知、運用＝

各社プロフィール整理
仮説設定
課題抽出
リスク分析
仮説検証
リスク低減策
ロードマップ

① 課題を洗い出し、すべきことを決める
＝今回ご提案＝

④ 実行するために必要な
体制（態勢）を定義し構築する



中長期
セキュリティ戦略

目標設定

組織、体制（態勢）、役割
＝推進側／実行側＝

事業特性
地域特性
法令遵守

組織、体制（態勢）、役割
運用開始

ルール体系
グループガイドライン

文書変更プロセス
例外プロセス

事故対応プロセス
教育プロセス
情報管理プロセス
チェックプロセス

文書類策定

展開、周知、運用
事故対応訓練
教育（従業員、管理者）
情報管理
自己点検、監査

② すべきことを明文化する
（規程、基準）

③ 実行するためのプロセス
（業務フロー、業務手順）
を整備する

⑤ ルールを確実かつ迅速
に実施するための
IT施策を要件定義する

STEP 3-2
＝IT施策要件定義＝

STEP 4-2
＝IT施策展開、運用＝

要件定義
インターネット・ゲートウェイ集約
ウイルス対策（既知、未知）
アカウント管理（AD展開等）
モニタリング（ログ管理）
IT資産管理

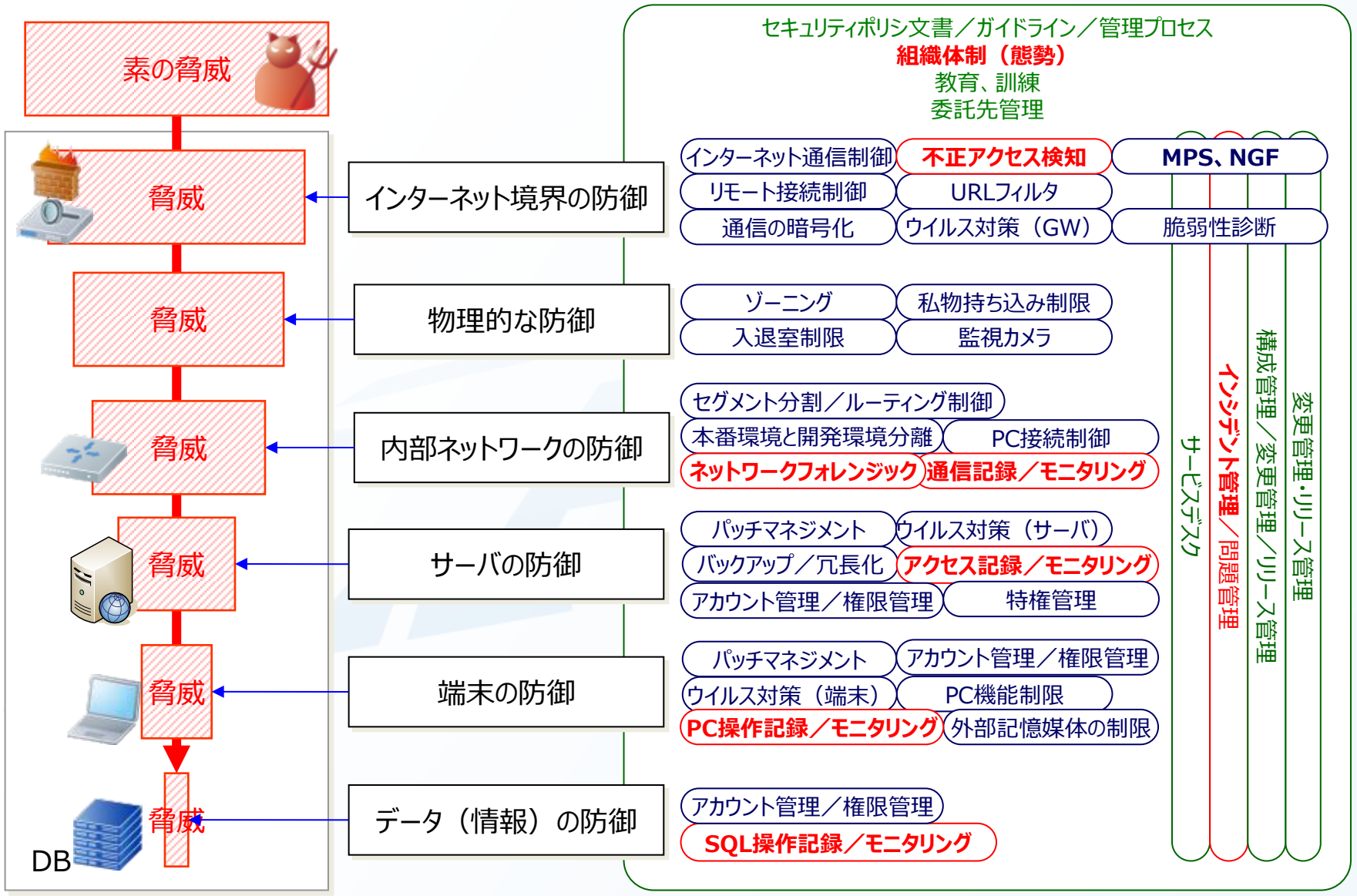
パイロット展開
本格展開、運用開始

リスク可視化
脅威シナリオ…標的型攻撃の例

※ どこで気づけるか？／止めることができるか？
※ 気づいた後の対処はどうか？

	標的型攻撃による情報流出
インターネット	①-1 未知マルウェア付添付ファイルの受信 ①-2 未知マルウェアが仕込まれたサイトの閲覧
インターネットゲートウェイ └ ルータ、Firewall、IPS等	
DMZセグメント └ Mail中継、Web、DNS等	
内部セグメント	
サーバ	④感染PCからアクセスするサーバアカウント情報の奪取 ⑤アクセス先のサーバへ exe を設置（感染の拡大） ⑥感染サーバの通信を傍受し、ADユーザアカウントや管理者のアカウント情報を奪取 管理共有通信などを傍受
PC	①-3 USBメモリ等に混入 ②未知マルウェア付添付ファイル開封 ③トロイの木馬生成→侵入者からの命令を実行 ⑦奪取したアカウント情報を利用し、ドメイン配下のサーバやPCへアクセス（乗っ取り遠隔操作） └ 乗っ取ったアカウントで情報奪取
DB	

リスク可視化
階層防御の観点からリスクベースで検証する



事業に役立つセキュリティのステップ

1st Step
リスクの可視化


個人の行動の
操作情報


ネットワークの
利用情報


サーバーの利用情報


アプリケーションの
利用情報


外部メディアの
利用情報

**IT活用における
行動と警告を〝相関分析〟**

**不審な行動、危険な操作
の把握によるリスク対策**

**リスク可視化情報を
業務可視化へ活用
＝戦略投資＝**

2nd Step
業務プロセスの可視化


業務プロセス情報


マーケティング
活動情報


顧客対応窓口
対応情報

など、事業・経営スコアカード

**IT活用の状況と、事業や経営の
スコアカードを〝相関分析〟
［ビッグデータ活用］**

**働き方改革、業務改革
生産性向上へなど経営改革**

1st STEP：レポーティング基盤構築

統合ログ管理（SIEM）が叫ばれている中、いきなりログの統合やSIEMツール導入はハードルが高い。そこで、

① **既存ログを活用したFactのレポーティング**
② ログの統合
③ 高度なログ管理…横断分析／相関分析（SIEM）

■ ①の目的

» 業務プロセスの可視化と、 IT利用状況の把握
» 様々な課題（効率性、安全性など）の〝あぶり出し（気づき）〟

■ 実現イメージ（案）

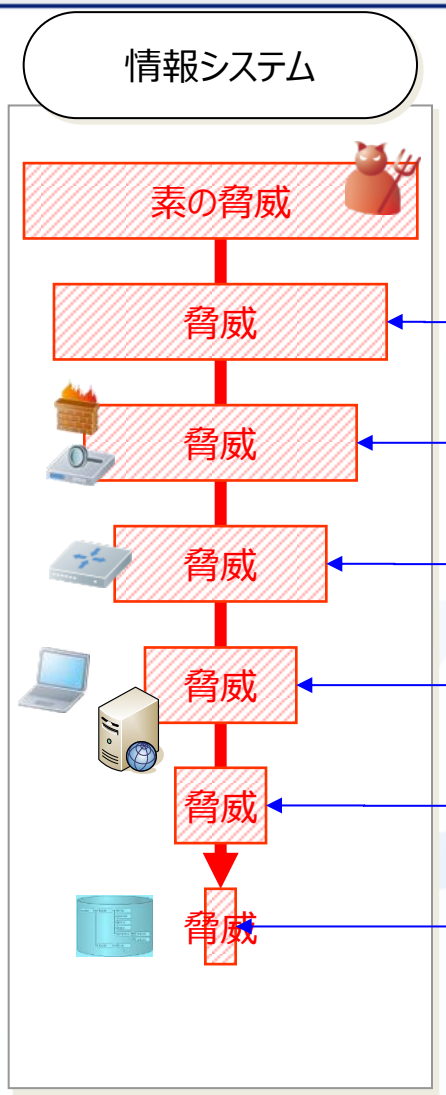
» **アカウント別にIT利用状況を集計 … イントラで公開**

端末操作の見える化	• **サーバ毎にログオンした回数** • **USBデバイスを使用した回数／書き込んだ回数**
ネットワークの見える化	• **DBから個人情報をダウンロードした回数** • **1回でダウンローした容量／一定期間でダウンロードした合計容量**
サーバの見える化	• **サーバ別のログオン回数** • **suした回数**
インターネット利用の見える化	• **送信先別添付メール件数／添付メール容量** • **URL別アクセス回数**

■ 期待効果

» **自分自身による気づき … 無駄の排除、記憶にない操作の確認**
» **第三者の目による気づきと抑止 … 異常な操作の発見→組織全体のリテラシ向上**
» **際限のないセキュリティツール導入コストの抑制**
» **②③へ進むためのログの精査**

1st STEP：レポーティング基盤構築
＝取得･モニタリングするログの例＝



セキュリティ区画定義
入退室記録

施設による防御

インターネット境界での防御

内部ネットワークでの防御

機器、装置での防御

アプリケーションの防御

データの防御

サイバー攻撃監視
IPS … サイバー攻撃
Proxy … サイバー攻撃
NGF … 標的型攻撃（未知マルウェア）

内部脅威（過失）監視
Mail … アーカイブ、ジャーナル
Web … URLフィルタ、レポート

ネットワーク監視
PCからサーバへのアクセス
DL回数および容量チェック

PC監視
PC操作記録（外部デバイス書き出し）
特権作業の画面スナップショット
特権作業申請とログの突合

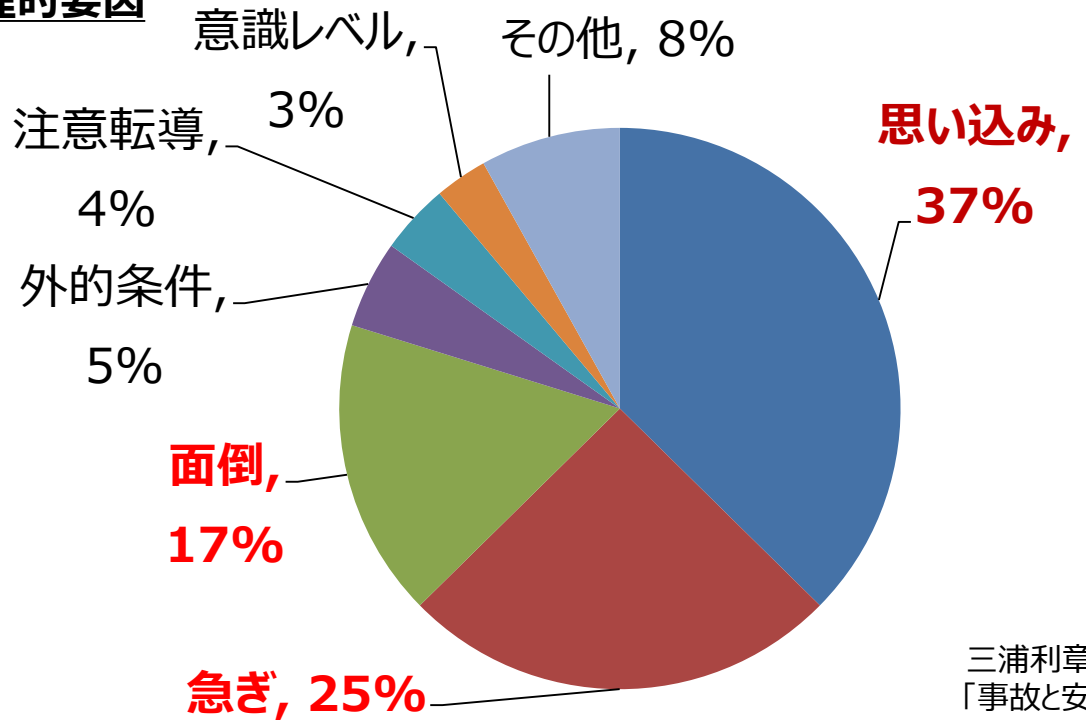
サーバ監視
踏み台サーバ…ログイン記録、su記録

DB監視
SQL記録 … 危険な操作

ルール違反が起こる要因

1. ルールそのものを知らない
2. ルール違反は果実を伴う
3. ルールを破っても処罰がない（あっても軽い）
4. ルール違反をとれる環境がある（みんなやっている）
5. ルール遵守（予防行動）は継続が大変（1回くらいいいか…）

■ ヒヤリハットの心理的要因



三浦利章、原田悦子共著
「事故と安全の心理学」より

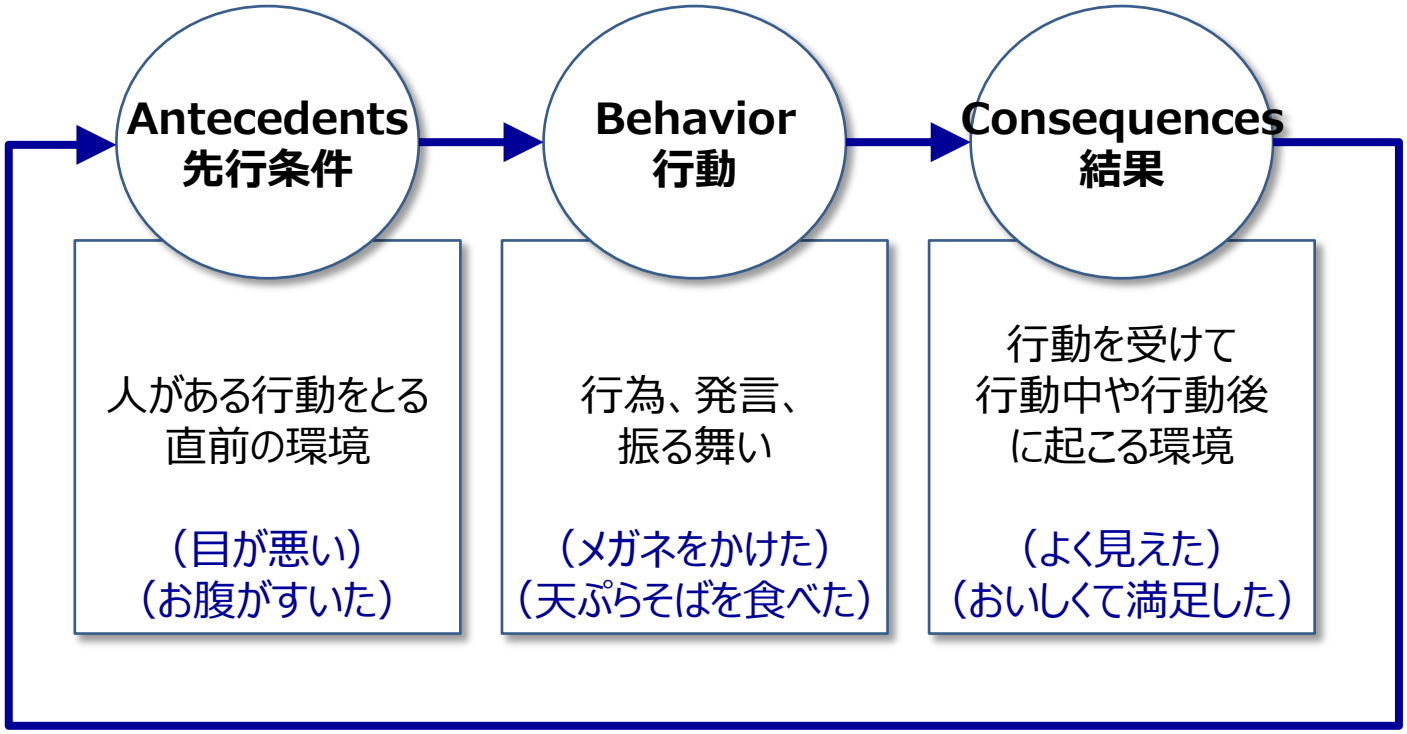
人の行動自発率

※ Ⓟ：「ペナルティや罰」は一瞬大きな効果を導き出すが、安全行動は長くは続かない。
※ Ⓔ ：「無視」され続けると、やがて行動を消滅させていく

※ 比較するのは「行動」であり「態度」ではない

石田淳著
「行動科学に基づく組織行動セーフティマネジメント」より

行動科学のABCモデル



人の行動（B）は、先行条件（A）よりも、結果（C）に左右される

ABCモデルをセキュリティに当てはめると…

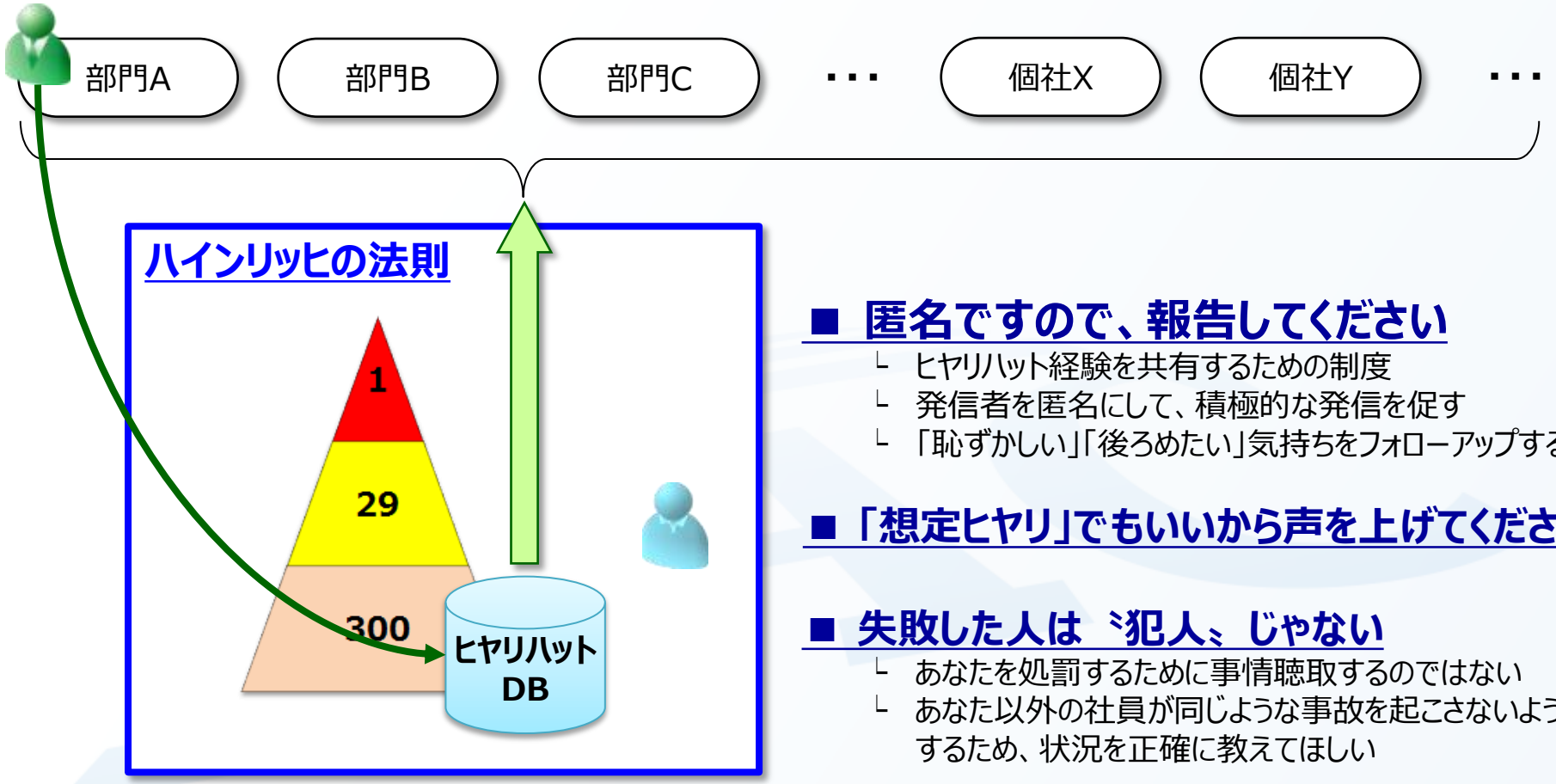
A	B	C	結果…
ヒヤリ・ハットを経験した ドキッとした	報告した	怒られた	できるだけ自分ひとりで処理しようとする
		再発防止に生かそう…と言われた	組織全体のために役に立つのなら…と考える

人の行動を適切に評価し、肯定的に反応すれば、人は行動を継続する。
つまり「Ⓔ感情曲線」をうまく利用し、「したい曲線」に誘導すれば良いことがわかる。
これは単にセキュリティの問題ではなく、**組織運営そのもの**、**マネジメントそのもの**。

ちなみに逆のケースは最悪！

A	B	C	結果…
面倒だ、楽だ	ルール違反をした	誰にも注意されなかった	タガが外れた状態 ルール違反をし続ける

コミュニケーション環境の整備→自発的安全報告制度



ヒヤリハット

↓

ニヤリホット

良かったことも報告してください

■ 匿名ですので、報告してください

- ヒヤリハット経験を共有するための制度
- 発信者を匿名にして、積極的な発信を促す
- 「恥ずかしい」「後ろめたい」気持ちをフォローアップする

■ 「想定ヒヤリ」でもいいから声を上げてください

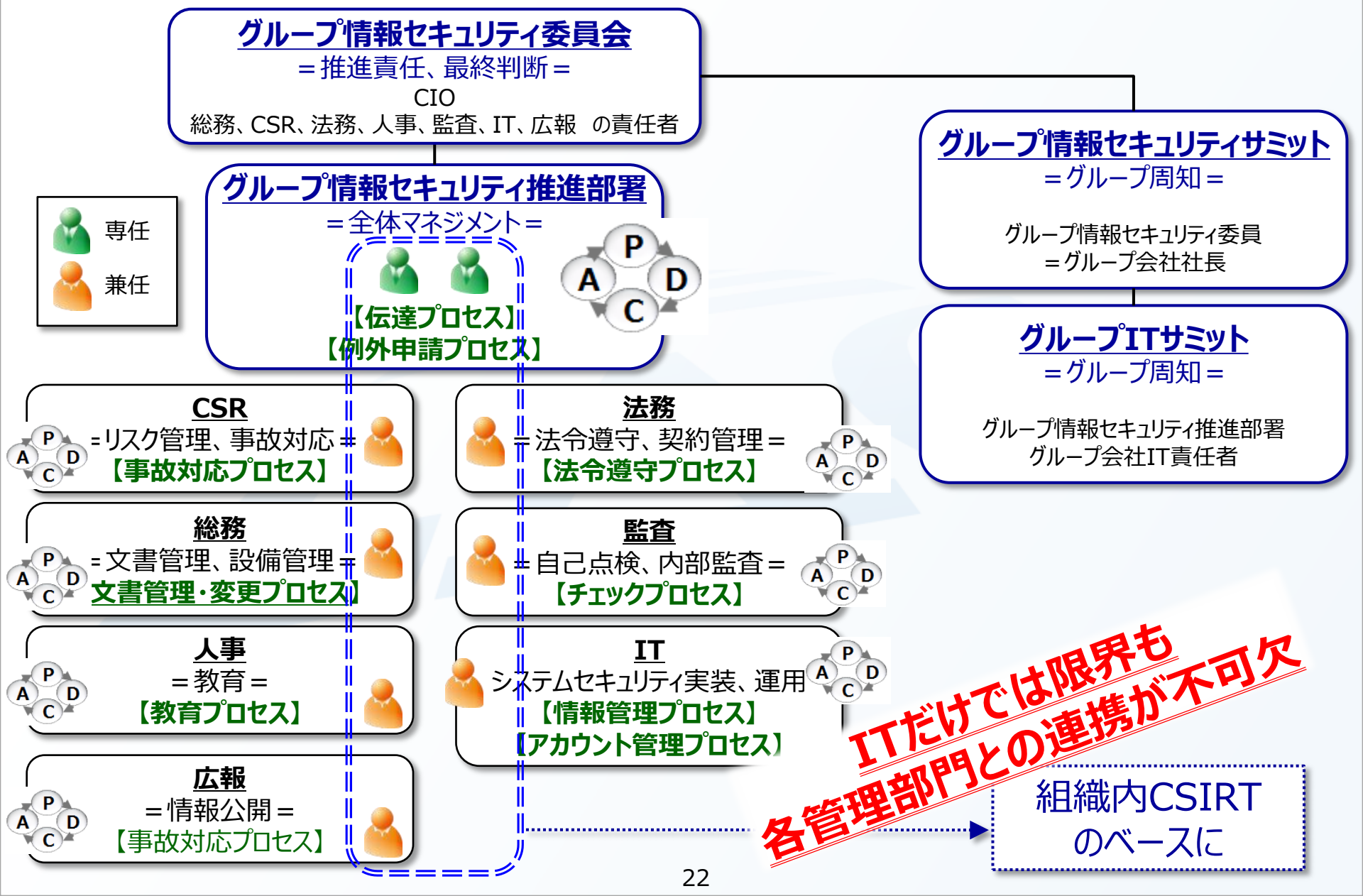
■ 失敗した人は〝犯人〟じゃない

- あなたを処罰するために事情聴取するのではない
- あなた以外の社員が同じような事故を起こさないようにするため、状況を正確に教えてほしい

■ たとえ〝勘違い〟でもOK

- セキュリティに疑義がある場合や自信がない場合は、自分で判断しない
- 「セキュリティを最優先する」ことをトップが宣言する

危機管理体制（態勢）の整備
情報セキュリティ推進体制



危機管理体制（態勢）の整備
CSIRTの機能一覧

青字…CSIRT主導
緑字…IT部門と連携
紫字…外部と連携

分類	業務機能	内容
Ⅰ．情報セキュリティ管理	ルールの整備 管理プロセス整備	• セキュリティ文書（スタンダード、ガイドライン、チェックリスト等）の管理 • 事故対応手順書など管理プロセス策定、整備 • 証拠保全、警察等へ提出する情報の収集対象・手順の整備
	体制、権限などの整備	• セキュリティ推進体制の整備（管理側／実行側） • 役割、責任、権限の定義
	教育・訓練の企画・推進	• セキュリティ教育、啓発、訓練の企画、推進、結果の評価
Ⅱ．情報セキュリティ推進 ＝事前対応＝	脆弱性情報の収集と活用 攻撃動向の把握 情報収集力強化と共有	• 外部からの脆弱性情報収集と活用 • 外部からの攻撃動向情報収集と活用 • 脆弱性情報に基づいた、注意喚起や脆弱性対応の通達 • 注意喚起情報の展開、追加対策の実施を提言 • プログラムバージョン、セキュリティパッチ適応状況の把握
	事故リスク評価 （アセスメント）	• ネットワーク構成情報、システム構成情報、対策実施状況の収集と管理 • 脆弱性診断実施計画の企画、立案、実施結果の評価、対策の推進 • 事故リスク評価の企画、実施、評価、対策の推進
	新サービスの評価	• 第三者の専門家によるリリース評価
Ⅲ．セキュリティ事故監視 ＝早期検知＝ **ポリシメーカー コマンダー**	**ヒヤリハット収集と共有**	**• コミュニケーション基盤**
	モニタリング基盤 ログ管理の強化推進	**• 外部脅威（サイバ攻撃）監視、検知、遮断 • 内部脅威の監視、アラート • 攻撃動向より管理対象ログ、解析手法等の改善提言**
Ⅳ．セキュリティ事故対応 ＝事後対応＝ **インシデント ハンドラー**	連絡体制の設置	• 対応態勢の確認 • 受付窓口の設置
	セキュリティ事故発生時 の対応支援	• 状況把握、証拠保全、応急処置 • 広報、当局報告、経営報告の支援 • 外部に対する協力依頼、外部機関への報告
	再発防止策の検討	• 再発防止策の検討、評価

外部専門家の活用、連携
**分析者
フォレンジック**

秋にあちこちで落ち葉の山が築かれていました。

消防士A：

火事に備えて常時出動体制をとり、火事が起こると真っ先に飛んで行って消火活動をした。
街の人は「なんて仕事を良くする消防士なんだろう」と。

消防士B：

落ち葉を集めて、別の場所で処分し、火事が起きないようにしていた。
街の人「ヒマなんですね」と。

LAC
安心とともに

Thank you.

内田　昌宏
masahiro.uchida@lac.co.jp

LAC
安心とともに
株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1
平河町森タワー
Tel 03-6757-0113　Fax 03-6757-0193
sales@lac.co.jp
www.lac.co.jp