NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ

Internet Week 2017

プロに学ぶ！侵害に耐えるサイバーレジリエンス

なぜ私たちはシステムを侵害から守れないのか？
～広く知って欲しい不都合なこと～

Share the Next Values!

2017年11月28日

NRIセキュアテクノロジーズ株式会社
サイバーセキュリティサービス事業本部

セキュリティコンサルタント 中島　智広

〒100-0004
東京都千代田区大手町一丁目7番2号 東京サンケイビル

自己紹介

中島 智広(Tomohiro Nakashima)

NRIセキュアテクノロジーズ株式会社 セキュリティコンサルタント
Internet Week 2017 プログラム委員長

技術やレギュレーションだけでなく、運用現場も判るコンサルタントとして
お客様のセキュリティ向上をワンストップでご支援。

「適材適所と有効活用、運用まで含めた実効性」を重要視

■経験/スキル属性

インシデントレスポンス
データセンターネットワーク
セキュリティ監視
ペネトレーションテスト
CSIRT SMTP HTTP 運用
インターネットバックボーン
BGP SOC PCI DSS DNS クラウド

CISA Certified Information Systems Auditor An ISACA Certification

CISSP Certified Information Systems Security Professional

PCI Security Standards Council APPROVED SCANNING VENDOR Qualified ASV Employee

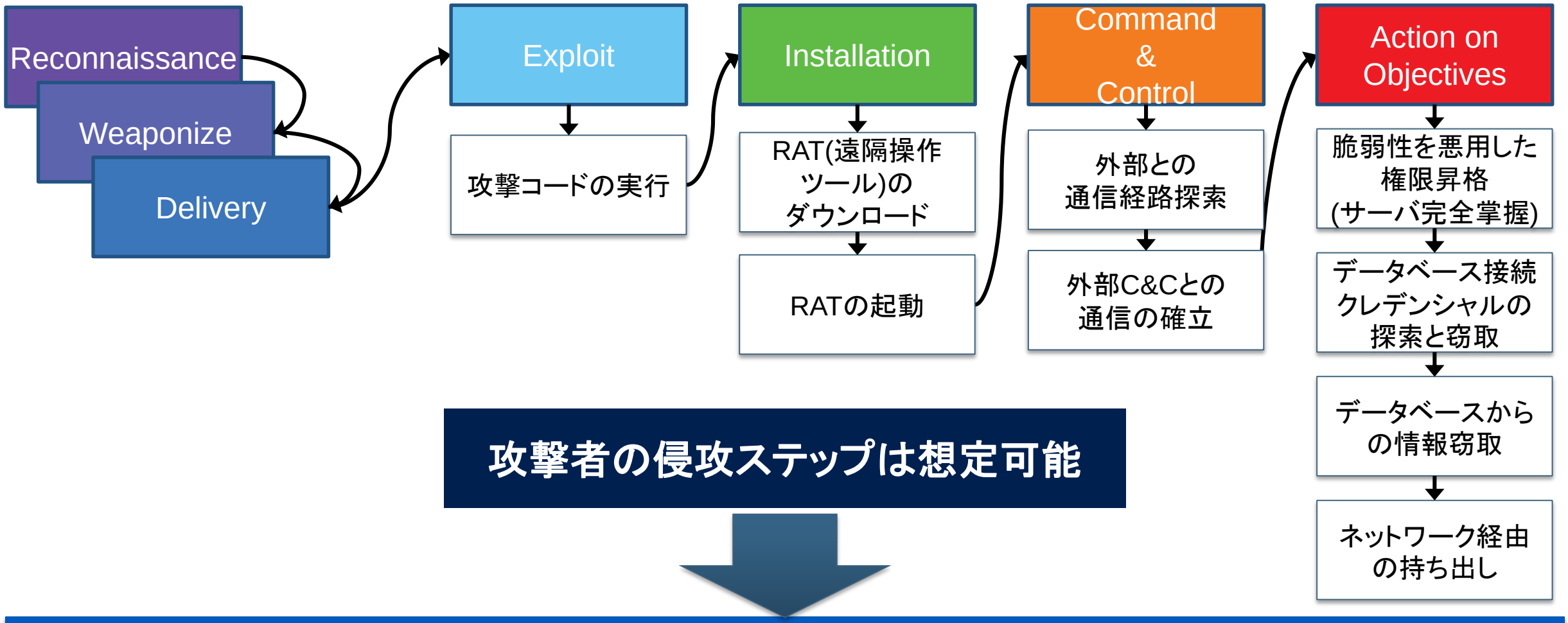
情報処理安全確保支援士
登録番号002007

■Internet Weekでの講演
Interent Week 2016「見抜く力を！」
「プロが厳選！低予算でもできる効果あるセキュリティ施策」
「知って納得！企業のDDoS対処戦略～基礎から実践まで」
Internet Week ショーケース in 名古屋 2017
「改めて考える適材適所のDDoS対策」

サイバーキルチェーン～攻撃者の目的達成までの道のり～

[引用元]https://en.wikipedia.org/wiki/Kill_chain#/media/File:Intrusion_Kill_Chain_-_v2.png

具体例：Webアプリケーションフレームワーク脆弱性に端を発する侵害

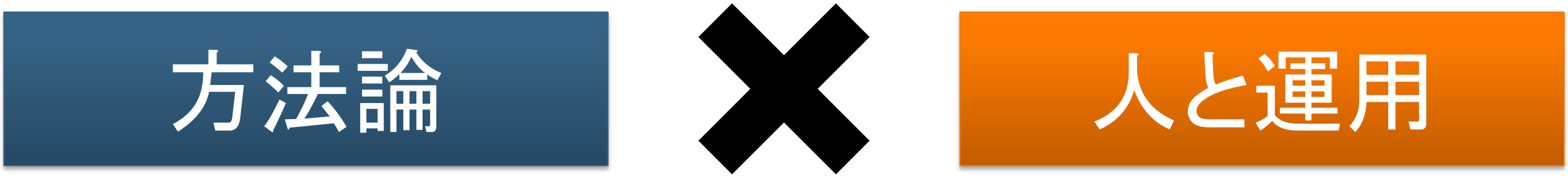


攻撃者の侵攻ステップは想定可能

ひとつひとつの侵攻ステップを妨げる取り組みが有効＝多層防御

私たちは多層防御に取り組んでいるはずではなかったか？

本パートのお話



二つの面から先述の疑問を紐解いていきたい

方法論：手法、セオリーとガイドライン、レギュレーション

手法、セオリー

システムを侵害から守るために取り得る守りの手段、その定番のもの

ゼロから生み出すものではなく、提供されているもの、利用可能なものを選んで用いる

ガイドライン、レギュレーション

手法、セオリーの共通項を明文化しまとめたもの、
望ましい方向に進む手掛かり・目安になるもの

「指針」　＝　物事を進めるうえで頼りになるもの
参考となる手引き

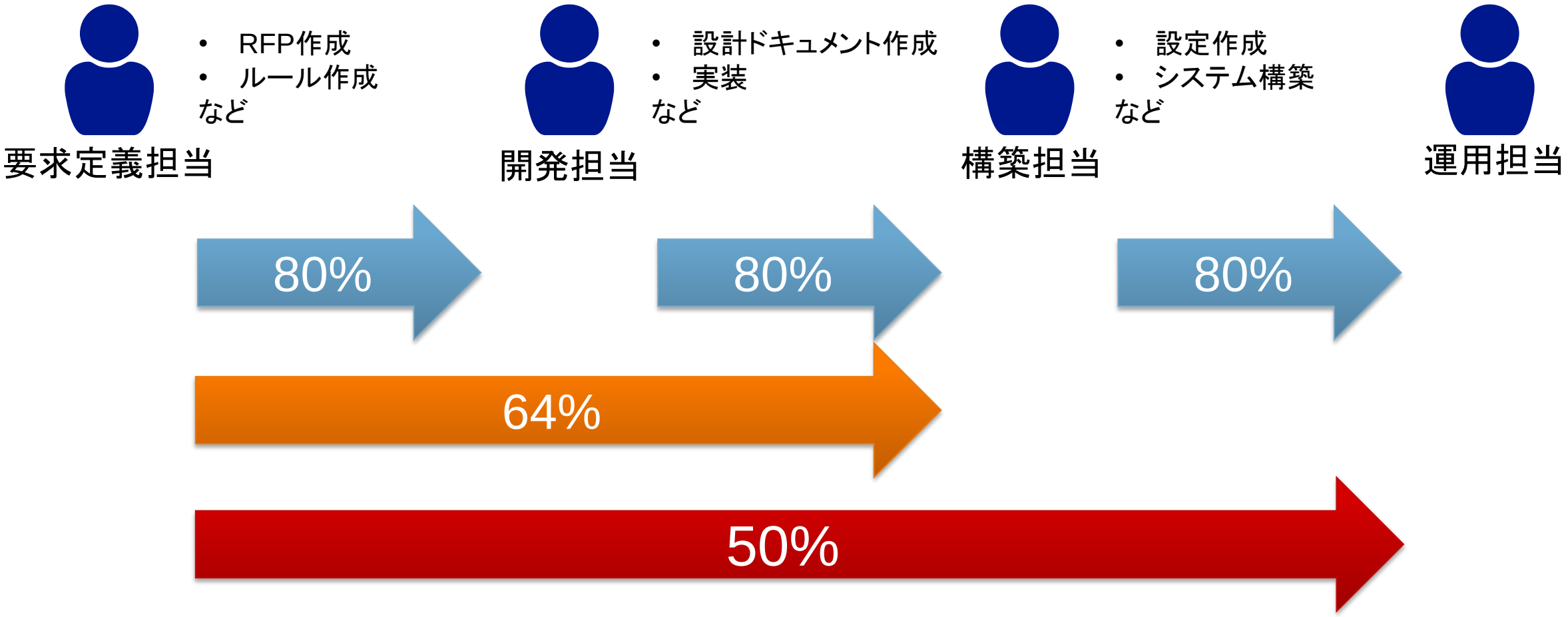
「基準」　＝　望ましい性質や水準

<記載事項の例>
- **厳密なアクセス制御と不許可通信の監視**
- **データベース接続クレデンシャルの暗号化**
- 高リスクイベントの監視(権限昇格など)

など

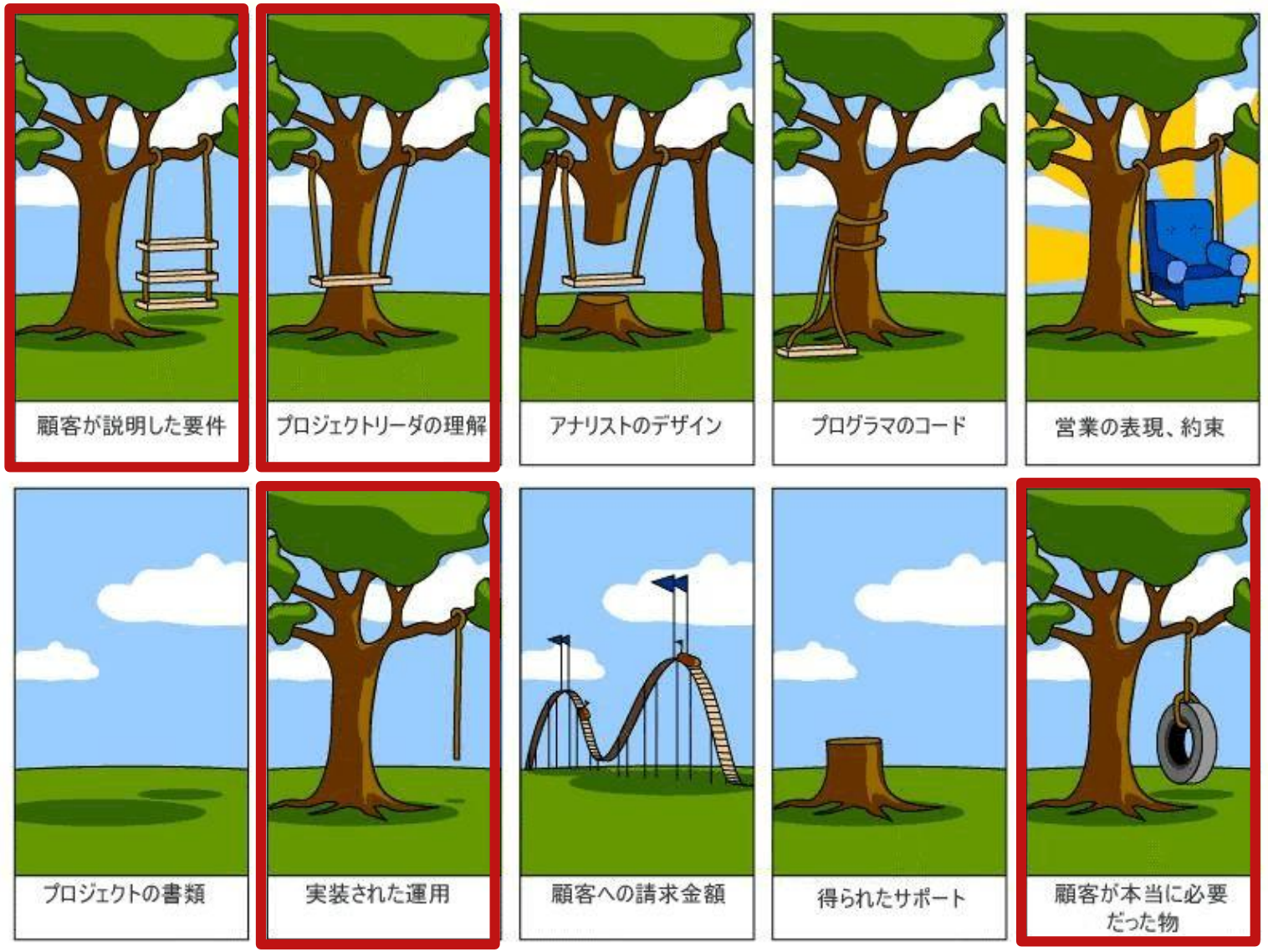
方法論自体は確立しており、課題はどう取り入れて取り組むか

人と運用：コミュニケーション、意図伝達の難しさ



「狙い、思い、コンセプト」の浸透は容易くない

なにもセキュリティに限る話ではない、今に始まった話ではない



ただし、

機能の不備はすぐに顕在化するが、
セキュリティの不備はインシデントが
生じるまで気づきにくい

そして、

機能は運用でカバーできても、
セキュリティは運用でカバーできない

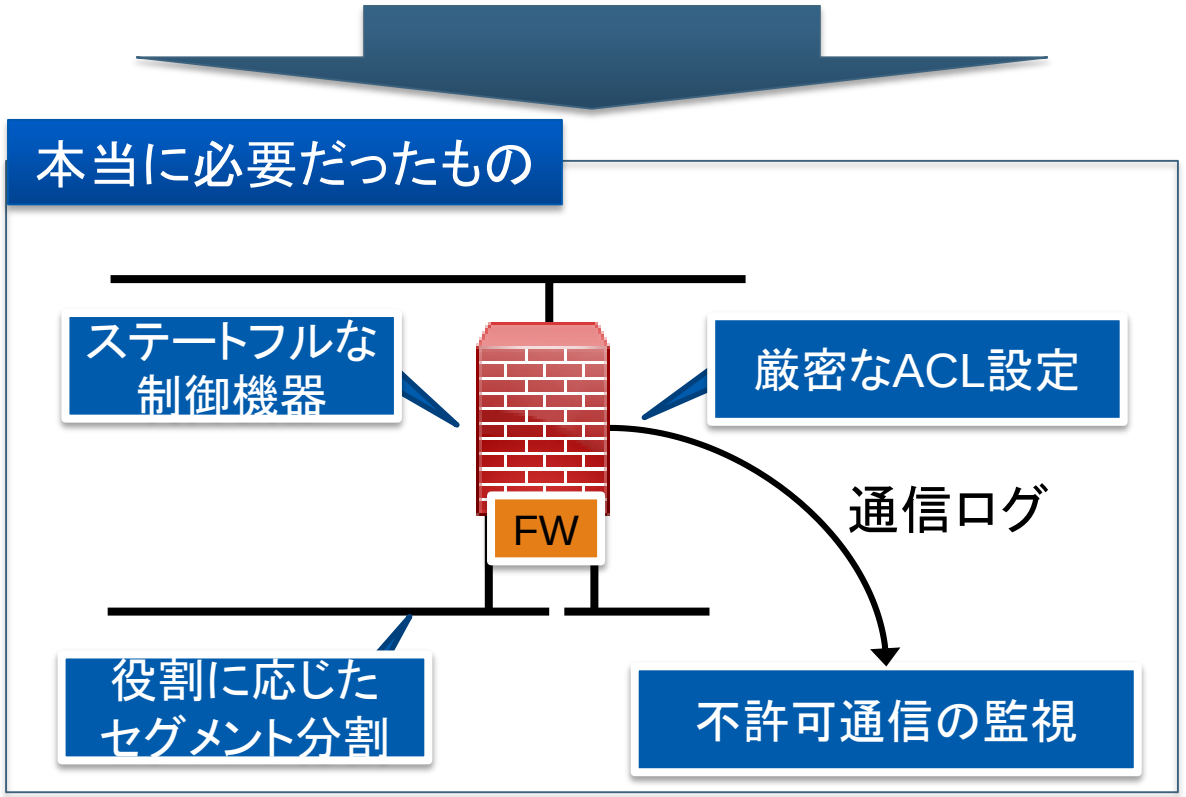
http://www.projectcartoon.com/

事例研究～ほんの一例～

要件

システムを安全に保つため、ネットワークセグメンテーションとアクセス制御を適切に行うこと。

コンセプト　攻略難易度を高める　侵害範囲を極小化する　侵害にいち早く気づく



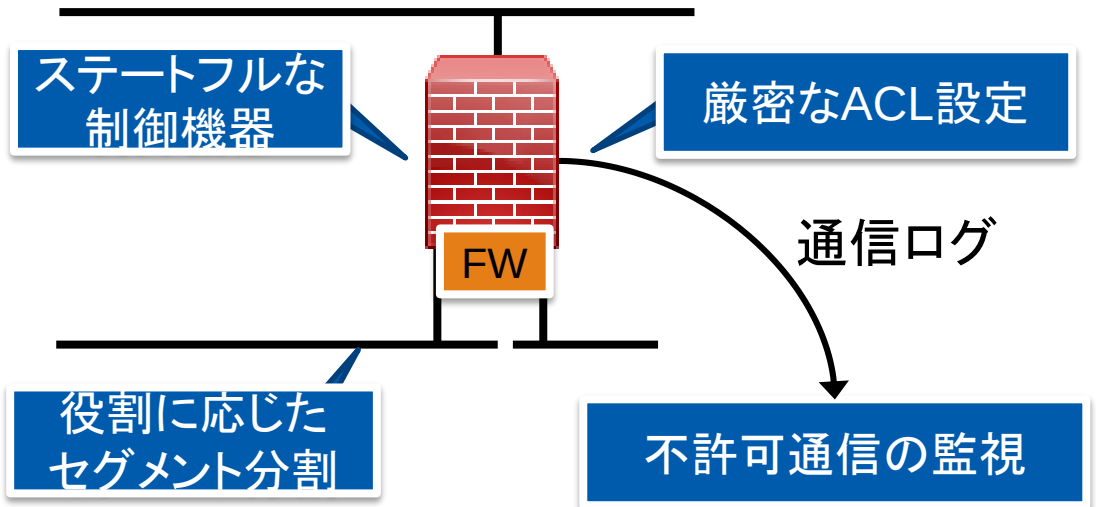
事例研究～ほんの一例～

要件

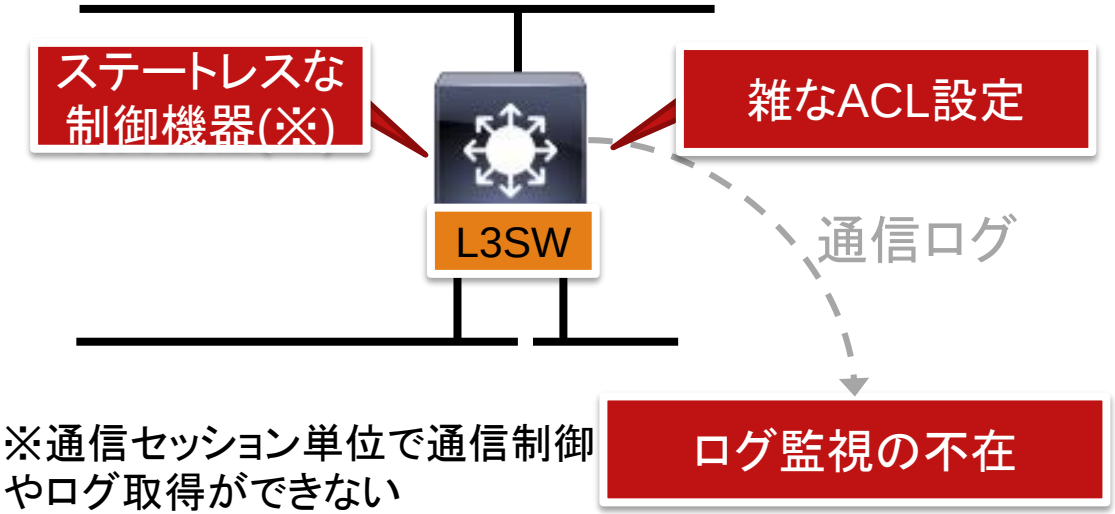
システムを安全に保つため、ネットワークセグメンテーションとアクセス制御を適切に行うこと。

コンセプト　攻略難易度を高める　侵害範囲を極小化する　侵害にいち早く気づく

本当に必要だったもの



実装された運用



※通信セッション単位で通信制御やログ取得ができない

もちろん上手くできている組織やシステムもたくさんある

結果上手くできていない組織やシステムとの差が際立つ傾向に

Why?

考察：両者の違いは何か？

理解の絶対的不足

【要求定義、要件定義担当として】
- 単に言葉の羅列としてしか認識できていないため、取り組み内容を具体的に想像できていない、説明できない

【設計、開発、構築、運用担当として】
- 方法論のコンセプトを理解できていないため、期待されている実装や設定を想像できない

担当者と思いを共有できていない

【現場都合優先】
現場には現場の都合がある、それを上回る思いを共有できていないと、あくまで現場の都合が優先される

【伝え方の不備】
相手の目線で伝えられていない、そもそも自らが理解できていないことを相手に説明しても伝わらない

理解不足が招く不幸な主義主張

最低限で十分主義

- 必要最低限や効率性を主張する
- 自身の管轄外での取り組みを求める

多層防御の否定

〇〇での対策が十分ですから、当方管轄でこれ以上の取り組みは不要と考えます。

文面解釈主義

- 背景や文脈を無視し狭い文面を都合よく解釈する
- 文面として記載されていること、指示されたことだけをやる

取り組みの形骸化

書いてあることには、きちんと取り組んでいます。

言い訳至上主義

- 言い訳をゴールにし、やらない理由を考える
- 問題が起きても言い訳できればよいと考える

言い訳と説明責任の混同

〇〇さん、ここまではやらなくても説明責任を果たせますよね？

不幸な主義主張を育みやすい土壌

組織の縦割り横割り、コミュニケーションの壁

絶対的な会話の不足、ドキュメントのやり取りだけで意図は伝わらない

担当者間の関係性不足

一方的に求めるだけでは人は動かない、相互理解と共感が必要

どうするのか？

- 組織の末端(含む委託先)まで取り組みの意識を合わせる
  - 相手の立場と仕事に**敬意**を示しつつ、1に**会話**、2に**会話**
  - パワーバランスや錦の御旗に基づく一方的な要求は下策

- 方法論のコンセプトを本質的に解釈し、しっかり使う
  - 人任せにせず、自らが具体的な取り組みをまず知る
  - 具体的な取り組みを要件、設計に落とす、きちんと伝える
  - コンセプトに基づき設計、実装、運用されていることを確認する

- プロの力を借りる
  - 有効だがこれまた銀の弾丸ではない、プロさえ「不幸な主義主張」に巻き込まれると苦戦する
  - 「**ここは譲れないベースライン**」をきちんと持って最後まで寄り添ってくれるプロと付き合う

レジリエンス？

Resilience＝回復力

高度化する脅威に対し、防御が破られてしまった場合でも、
「攻撃の早期発見」「被害の拡大防止」「復旧」を実現する特性

- 具体的な取り組みは既存の延長、特に目新しい要素があるわけではない
- その一環として「基本的な取り組みができていること」を改めて求められている

本パートのお話/不都合な事実

方法論

の

理解不足

×

人と運用

の

理解不足

＝

レジリエンス以前の話

みなさんの組織、システムは本当に大丈夫でしょうか？

終わりに

1.マインドを変える Change mind	2.方法論を知る Know methodology	3.適切に遂行する Execute properly
• 啓蒙啓発 • 継続的会話 • 共感を得る	• 堅牢化、多層防御の方法論を深く知る • 他人に説明できるレベルの理解	• 予算化 • 実行計画 • 遂行

このあとは方法論に特化した話が続きます。

ご清聴ありがとうございました。


NRI
未来創発
Dream up the future.