

CSIRT実務における デジタル・フォレンジック

鴨志田 昭輝

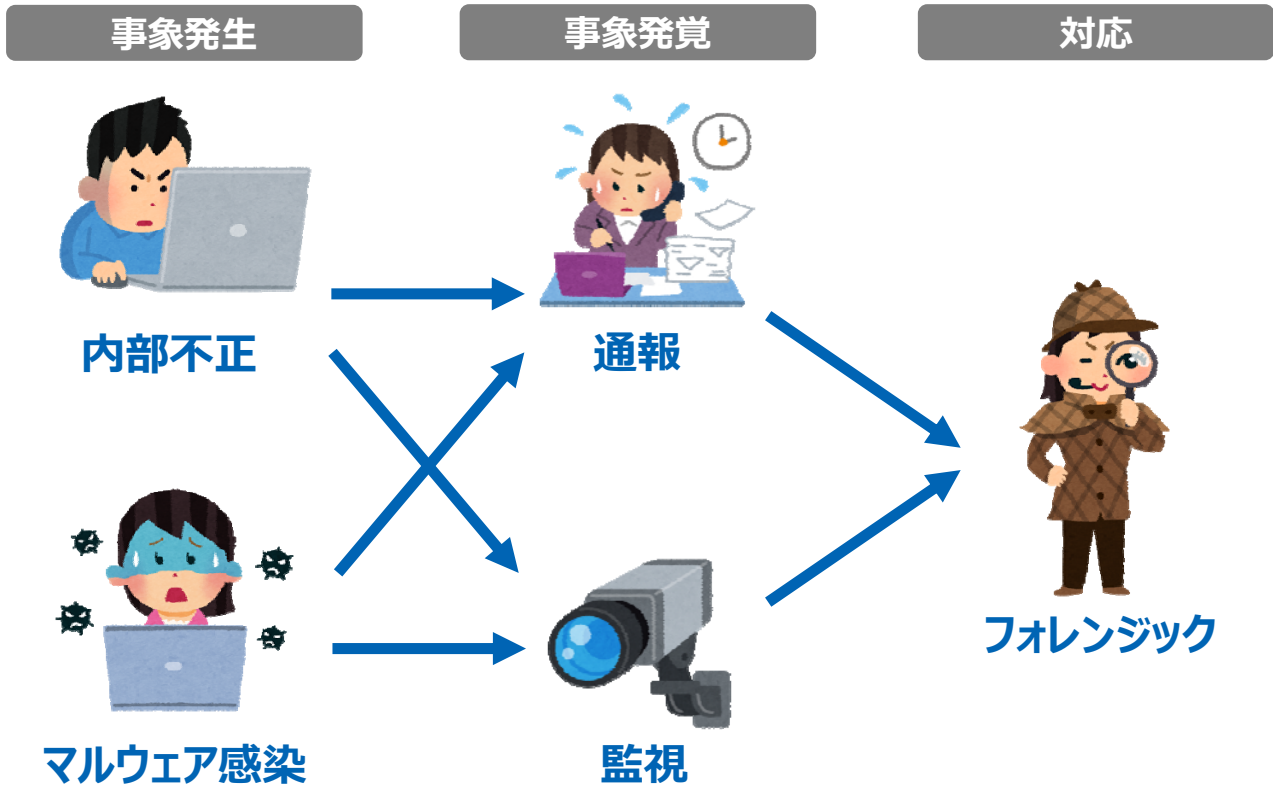
執行役員 エグゼクティブマネジャー
サイバーセキュリティエンジニアリング部
株式会社リクルートテクノロジーズ



本日の内容



企業内CSIRTにおいて、デジタル・フォレンジックを
実際にどのように活用しているか？

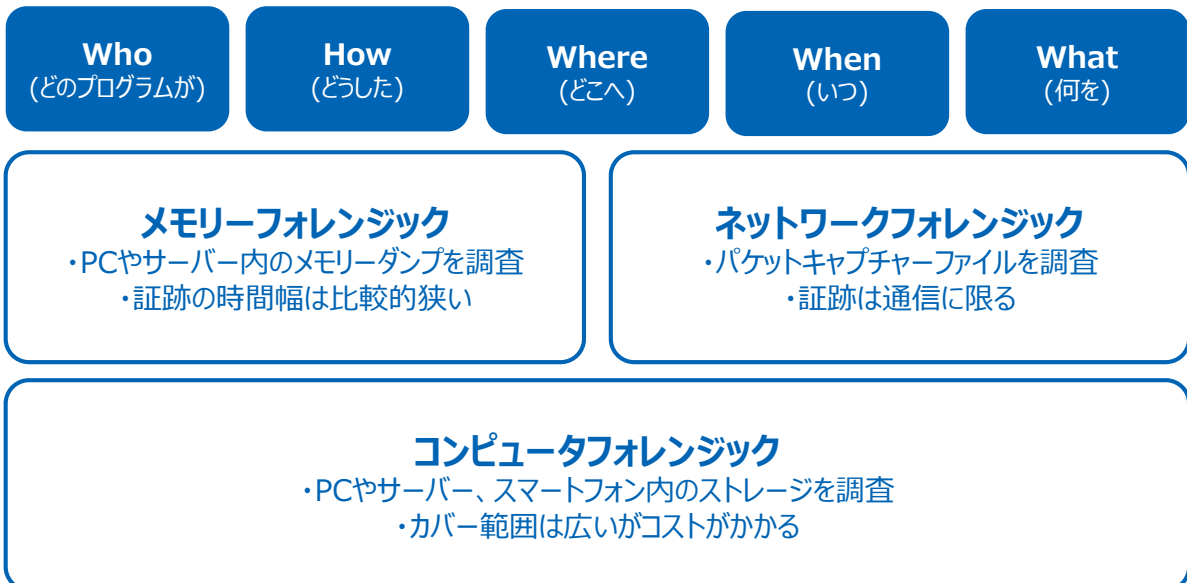


(C) Recruit Technologies Co., Ltd. All rights reserved.

デジタル・フォレンジック技術の3手法

得意領域を知って使い分けることが重要

※「Why(何故)」攻撃者もしくは不正した本人のみが知る場所である



出所: 「実践CSIRT 現場で使える事故対応」
Recruit-CSIRT著 日経BP社

(C) Recruit Technologies Co., Ltd. All rights reserved.

当日投影のみ

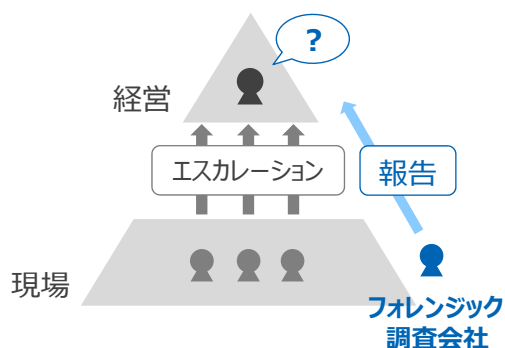
(C) Recruit Technologies Co.,Ltd. All rights reserved.

フォレンジックを内製化するメリット

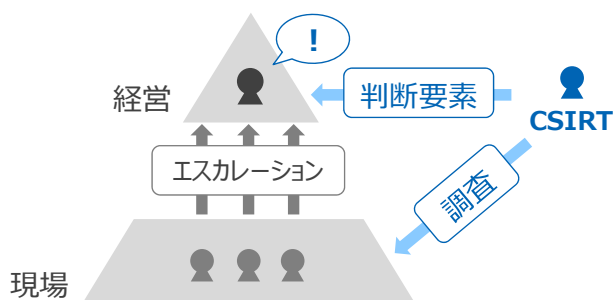


- ・ 対応スピード（メモリーフォレンジックにおいて特に重要）
- ・ グレーな部分を技術をもって判断できる

フォレンジックを外注



フォレンジックを内製



(C) Recruit Technologies Co.,Ltd. All rights reserved.

- 内製化して、技術分野の重なりが大きさに気付く
- 両立できる人材を育成していく

