サイバー攻撃を認知した場合の証拠保全は？

デジタル・フォレンジック・コミュニティ2019 in 関西

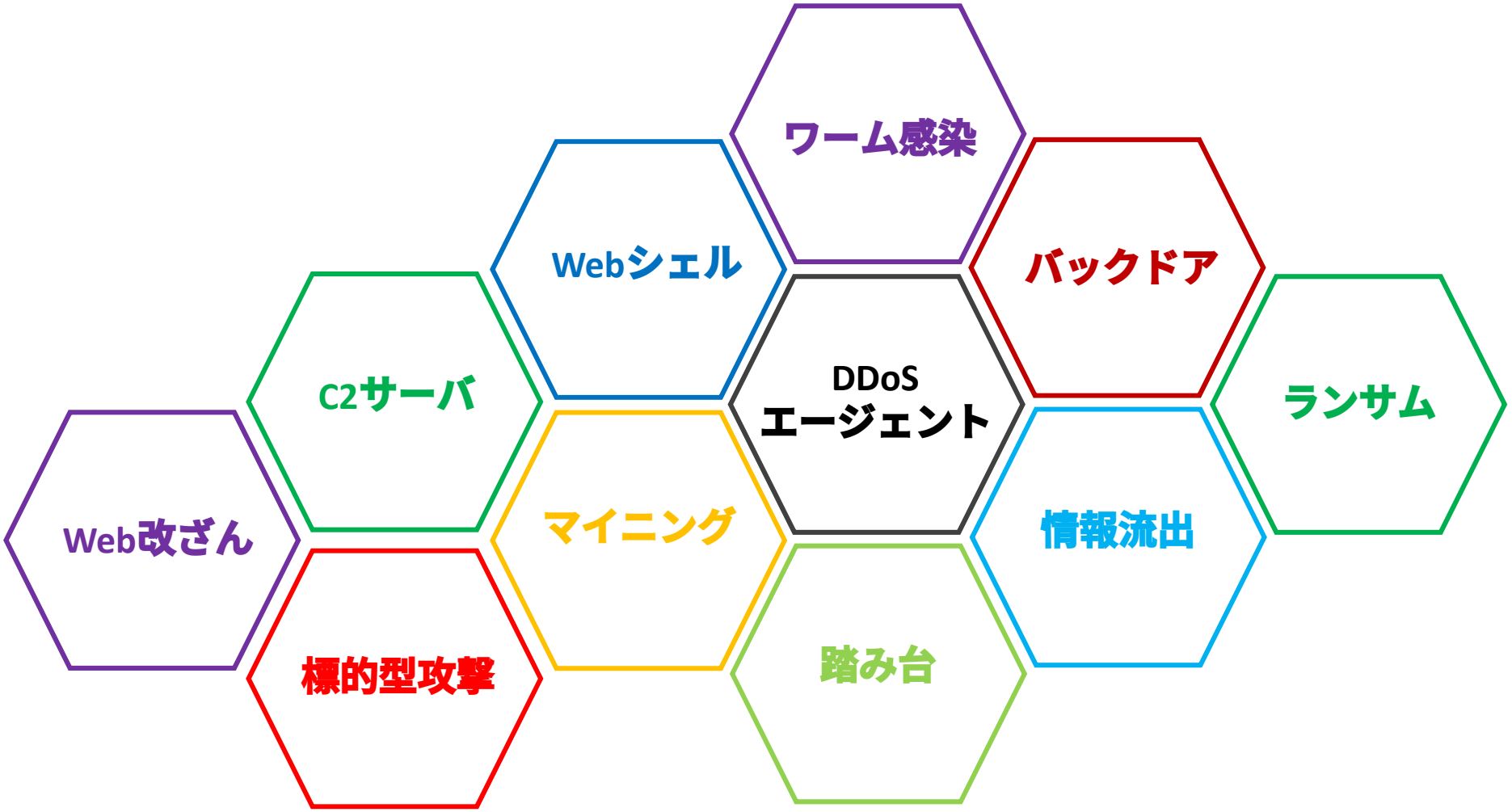
2019年2月19日

株式会社サイバーディフェンス研究所

大徳 達也

対応インシデント例

CyberDefense



Copyright © 2019 Cyber Defense Institute, Inc. All Rights Reserved

インシデント認知後の対応

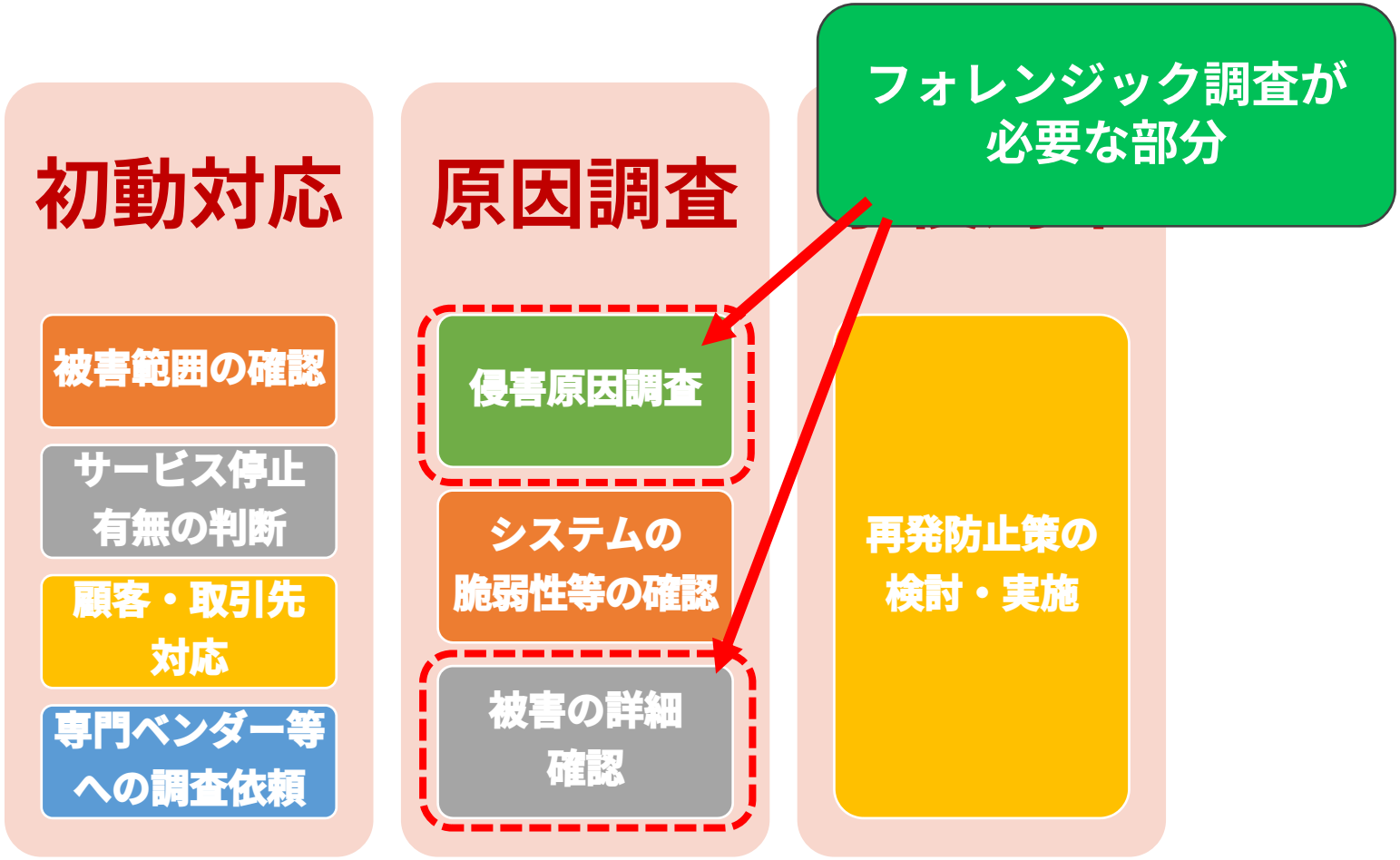
CyberDefense

【参考】サイバーセキュリティ経営ガイドライン
付録C インシデント発生時に組織内で整理しておくべき事項
http://www.meti.go.jp/policy/netsecurity/mng_guide.html

Copyright © 2019 Cyber Defense Institute, Inc. All Rights Reserved

インシデント認知後の対応

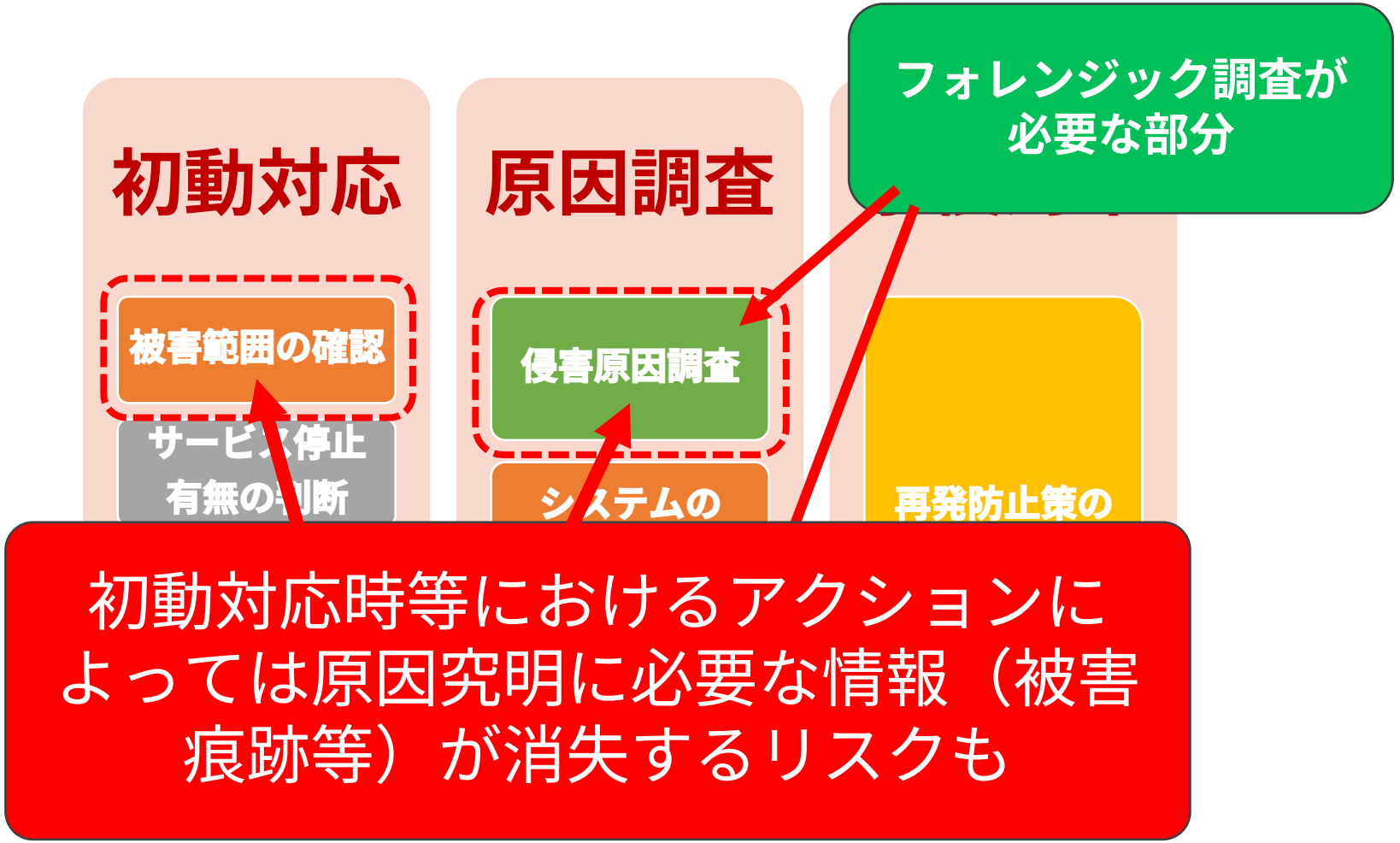
CyberDefense



【参考】サイバーセキュリティ経営ガイドライン
付録C インシデント発生時に組織内で整理しておくべき事項
http://www.meti.go.jp/policy/netsecurity/mng_guide.html

Copyright © 2019 Cyber Defense Institute, Inc. All Rights Reserved

インシデント認知後の対応



【参考】サイバーセキュリティ経営ガイドライン
付録C インシデント発生時に組織内で整理しておくべき事項
http://www.meti.go.jp/policy/netsecurity/mng_guide.html

Copyright © 2019 Cyber Defense Institute, Inc. All Rights Reserved

CyberDefense

デジタル・データ（電磁的記録）の代表的な特徴

複写

消去

改変

上記の特徴から取り扱いを誤ると、
フォレンジック調査への影響は避けられない

Copyright © 2019 Cyber Defense Institute, Inc. All Rights Reserved

速やかな証拠保全ができなかったら

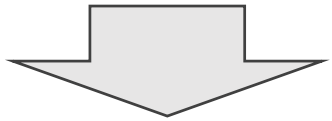
CyberDefense

侵害当時のログがなくなった

動作中のプログラムがファイルを作成

攻撃者が削除したファイルの領域が上書き

SCREWED UP!



フォレンジック調査への影響は大

Copyright © 2019 Cyber Defense Institute, Inc. All Rights Reserved

CyberDefense

初動対応時のアクションとその影響のバランスを考える

Copyright © 2019 Cyber Defense Institute, Inc. All Rights Reserved

初動対応に当たる人の本音

CyberDefense

フォレンジック調査の実施有無に限らず
証拠保全する方が望ましい（のは分かる）

しかし、現実は・・・。

- 厳格なフォレンジック調査までは不要。
- 専用機器やツールを整備していない。
- そんな難しいことをできる人はいない。
- 証拠保全してたら時間がかかる。
- けど初動対応はちゃんとしておきたい。　etc…

解決策は？

Copyright © 2019 Cyber Defense Institute, Inc. All Rights Reserved

標的型攻撃被害における調査での悩み

CyberDefense

最初の１、２台のPC調査までは良かったが・・・。

怪しいPCは全て保全する必要があるのか？

侵害程度の低そうなPCも調査解析するのか？

コストは？（予算、人、時間）

調査したが何も出てこない場合もあるのでは？

調査完了はいつ？

従来のフォレンジック調査のやり方でいいのか？

Copyright © 2019 Cyber Defense Institute, Inc. All Rights Reserved

被害前提で考える備え

CyberDefense

初動対応手順の整備
（マニュアル化など）

被害を想定した訓練の実施
証拠保全を含めた対応に要する時間は？
そもそも証拠保全は可能か

調査に必要な
証跡・期間の見直し

必要十分な証跡は、自社に限らず
調査ベンダーにとっても必要（有益）

必要な予算と
調査ベンダーの確保

適切な予算、サイバー保険の確保
速やかな調査着手のための事前NDA締結

Copyright © 2019 Cyber Defense Institute, Inc. All Rights Reserved