NA4Sec
Network Analytics for Security

能動的サイバー防御時代に改めて考える
脅威情報共有のあり方

NTT docomo Business

2026年07月01日

本日のテーマ

世間に出回る**脅威情報**の扱い

特に

発信源が**攻撃者自身**

ケーススタディ：ハクティビスト

ハクティビスト / Hacktivist

Hack + Activist
ハック　　行動主義者
活動家

政治的・社会的な意思表示や目的実現のために
ハッキングを手段として主張を行う**活動家（集団）**

NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

会場限定公開

結論

ハクティビスト

▼

炎上系インフルエンサー

NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

会場限定公開

その他の事例で見る近年の情報共有

NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

会場限定公開

アクター名の共有に意味はあるのか?

TLP:CLEAR

つなごう。驚きを。幸せを。

NA4Sec Network Analytics for Security

NTT docomo Business

攻撃活動のグルーピング

- 視点: **民間**が中心
- 目的: 費用対効果の高い防御

様々なインシデント事例から類似のサイバー攻撃を分類し、脆弱性対応やスレットハンティングの対応優先どの判定に使用

刑事手続き上での実行主体言及

- 視点: **行政機関**が中心
- 目的: 将来的な攻撃の抑止

パブリックアトリビューションとも言われ、名指しの公表そのものに価値がある行為。他国の牽制やサイバー防衛能力の保有を情報戦の観点で提示

このような活動は<u>アトリビューション</u>と呼ばれ、無意識に価値のある行為と世の中に浸透

今回取り上げた事例に当てはめると?

TLP:CLEAR

つなごう。驚きを。幸せを。

NA4Sec Network Analytics for Security

docomo Business

攻撃活動のグルーピング

- 視点: **民間**が中心
- 目的: 費用対効果の高い防御…?🤔

DDoS の場合基本的な対策はほぼ DDoS 対策ソリューションを入れるかで情報拡散されてもできることは少ない

データ流出の場合も攻撃者が用意したサイトに素人が赴きデータを取得して中身を確認するのは危険な行為

名前を共有することによって生まれる防御の相乗効果は
極めて少ない (むしろ新たなリスク)

刑事手続き上での実行主体言及

- 視点: **行政機関**が中心
- 目的: 将来的な攻撃の抑止…?🤔

攻撃側から名乗っているので全く意味がない。本気でやるならば実行主体の人や背景の組織そのものに言及する必要あり

話題になった被害組織が再び被害にあったり
データの価値も高くなるのでむしろ逆効果

コスト/ベネフィットの釣り合い

TLP:CLEAR

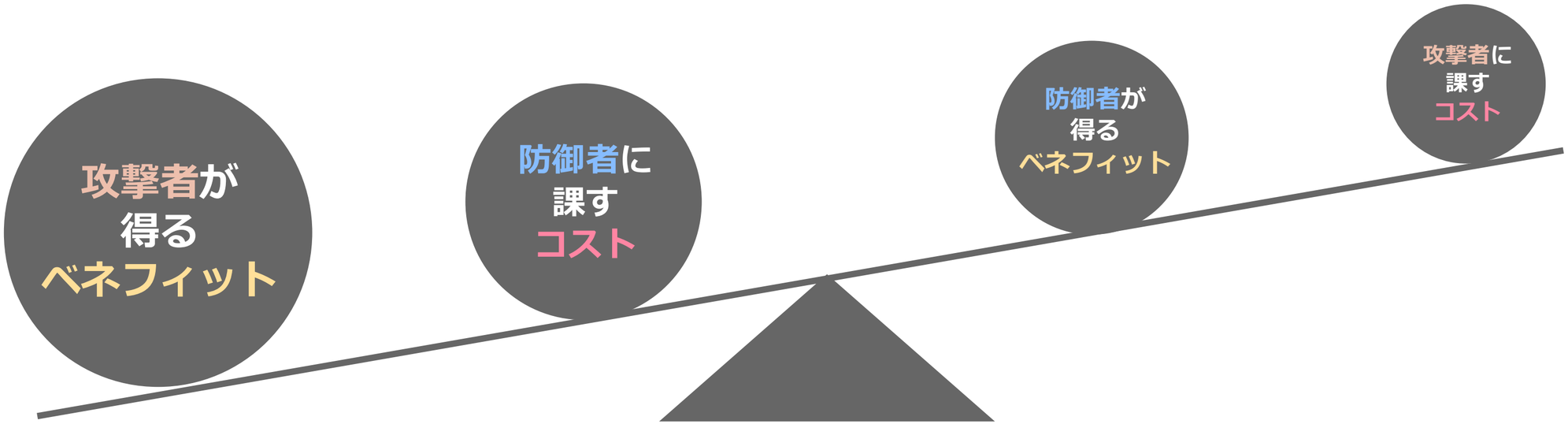
つなごう。驚きを。幸せを。

NA4Sec Network Analytics for Security

NTT docomo Business

本来ならば防御側のベネフィットを最大にしながら攻撃者にコストを課す戦略を取るべき

「攻撃者の名をあげて情報共有やデータ公開」で一番得をするのは**攻撃者側**



コスト/ベネフィットの釣り合い

TLP:CLEAR

つなごう。驚きを。幸せを。

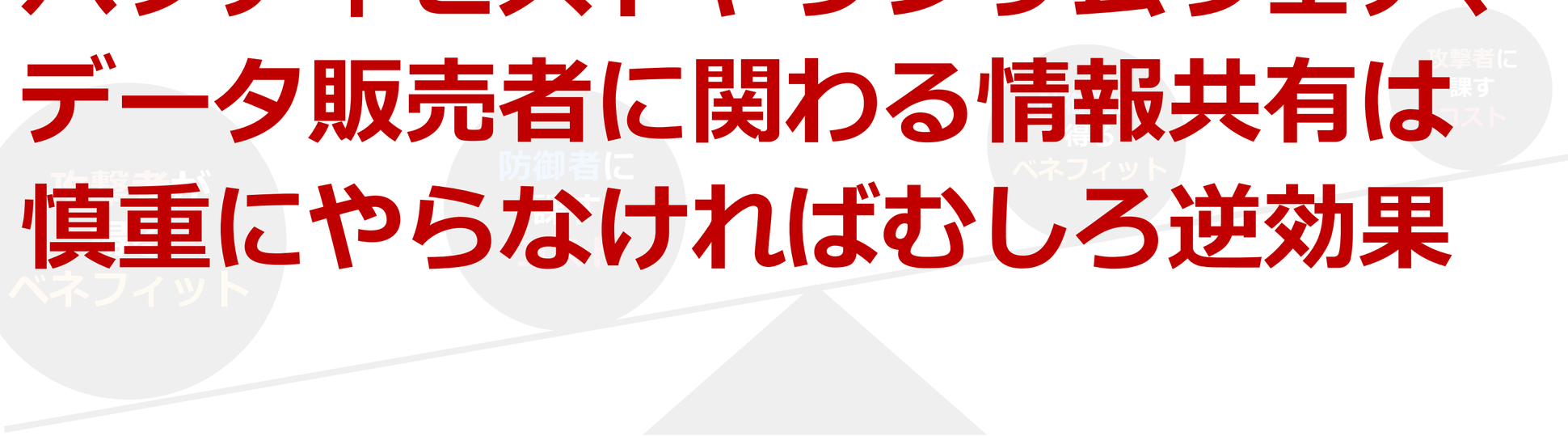
NA4Sec Network Analytics for Security

NTT docomo Business

本来ならば防御側のベネフィットを最大にしながら攻撃者にコストを課す戦略を取るべき

「攻撃者の名をあげて情報共有やデータ公開」で一番得をするのは攻撃者側

ハクティビストやランサムウェア、
データ販売者に関わる情報共有は
慎重にやらなければむしろ逆効果



公の場での情報共有はNGなのか?

攻撃者のメリットにならない情報共有

TLP:CLEAR

つなごう。驚きを。幸せを。

NA4Sec Network Analytics for Security

NTT docomo Business

- これらのサイバー犯罪者を表で取り扱えば取り扱うほど、**彼らの目標の一つが達成される**
  - ブランドの宣伝、認知度向上
  - ターゲットに対するプレッシャー
  - **結果的にマネタイズできる確率が大きくなる**

- 情報セキュリティを扱うべき人間ならば防御者のアドバンテージを最大にしながらも攻撃者が得られるアドバンテージの影響も最小にすべき
  - 攻撃で使用される TTPs や現実のタイムライン
  - インシデント対応から得られた教訓
  - サイバーレジリエンスの評価の見直し

- 防御側が具体的な防御で役立つ情報を発信、共有するということを根幹に置く

我々の情報共有活動の例

TLP:CLEAR

つなごう。驚きを。幸せを。

サイバー攻撃者に見えないチャネルで適時的・効果的に情報を伝達

単なるニュースの共有ではエンタメの域を出ない。**防御者の得るベネフィット**を考えて行動する

ターゲット組織への直接情報提供

- **因果**：調査コストの節約
- **影響範囲**：効率的なリソース投入判断
- **二次被害防止**: 障害報告の際の注意事項

業界団体（ISAC）への情報共有

- ターゲットとなる蓋然性の高い組織に**効率的に知見を共有**
- 現在も見えないだけで然るべき経路で重要組織に情報と対応策は共有されている

より詳細な共有のワークフローは『攻撃技術情報の取扱い・活用手引き （案）』を参考のこと

https://www.meti.go.jp/press/2023/11/20231122002/20231122002-c.pdf

まとめ

- 近年激しくなる情報戦の中、我々も情報をどう扱うかのリテラシーがますます求められる時代
  - ハクティビストによる DDoS、ランサムウェア侵害、ライプライチェーン攻撃、データ暴露
  - それがどれほどのインパクトを与えているかは攻撃者の一次情報からはわからない
- 情報セキュリティを扱うべき人間が意識すべきこと
  - 攻撃の事実そのものよりも防御に求められる教訓を広げる
  - 攻撃グループやデータ公開の事実を拡散しても攻撃者への広報にしかならず自身の首を絞めるだけ
- Key takeaway
  - サイバー攻撃を話題に上げたくなったときに考えてみて欲しいこと

「その共有で得をするのは誰ですか？」

能動的サイバー防御時代に改めて考える
脅威情報共有のあり方

NA4Sec
Network Analytics for Security

Thank you !

つなごう。驚きを。幸せを。

NTT docomo Business