新技術説明会
New Technology Presentation Meetings!

マルウェアや調査目的スキャン特定のためのパケットヘッダのシグネチャ生成技術

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
サイバーセキュリティ研究室
研究員　田中　智

2023年10月19日

自己紹介：産学連携の経歴（修士・博士：2016~2021年）

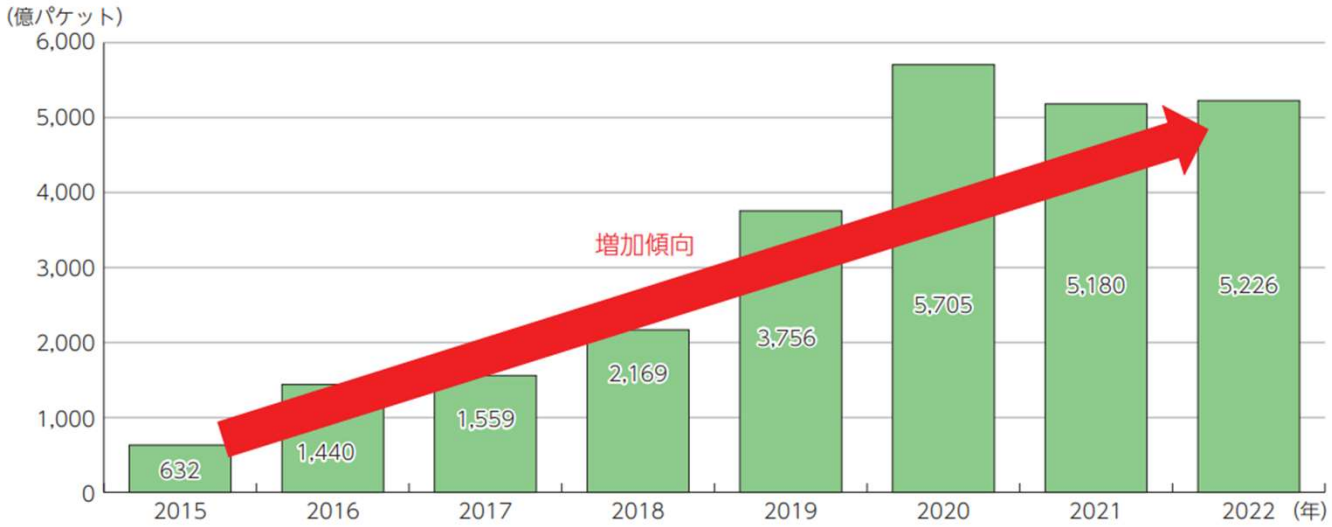
実社会の課題を最適化・深層学習・機械学習で解決

- トヨタ自動車株式会社とHV車の最適制御に関する共同研究を実施
- ソフトバンク社とLPガス配送最適化システムに関する共同研究を実施
- ヤフー株式会社とバイクシェアリングサービスの効率化に関する共同研究を実施
- 住友電気工業社と共同研究を実施
- 沖電気工業社と共同研究を実施
- ロート製薬社と工場スマート化に向けた共同研究を実施

目次

サイバーセキュリティ脅威の拡大

サイバーセキュリティ上の脅威は年々拡大し、今後も拡大が予想されている



NICTERにおける無差別型サイバー攻撃関連の通信数の推移(*1)

世界のサイバーセキュリティ市場規模(売上高)(*2)

*1) 総務省、令和5年版情報通信白書、第2部、図表4-10-2-1
*2) 総務省、令和5年版市場概況、白書掲載番号4-10-1-1

サイバー攻撃の分類

標的型攻撃：特定の個人や組織を狙った攻撃

- ランサムウェア
  ファイルを暗号化し、復号を条件に金銭を要求する攻撃
- DDoS攻撃
  攻撃対象のWebサーバーなどに対して、複数のデバイスから大量のパケットを送りつけ、正常なサービスの提供を妨げる攻撃

無差別型攻撃：不特定多数に向けた攻撃

- フィッシング詐欺
  本物に似せた偽のWebサイトなどで個人情報を盗み出す手法
- クリプトジャッキング
  標的のデバイスを利用して仮想通貨の不正マイニングを行う
- スパムメール
  受信者の意向を無視して一方的に送り付けられるメール

攻撃手順・方法

攻撃者は攻撃規模の拡大と正体を隠すためにボットネットを構築する

手順	方法
1. 脆弱性のある機器やサービスの調査	ポートスキャン
2. ボットネットの構築	脆弱性を突く攻撃
3. サイバー攻撃の実施	DDoS攻撃 クリプトジャッキング など

情報セキュリティ上の欠陥

ネットワークに接続されている機器に通信を行い、稼働しているサービスやシステム情報を調べる。

マルウェア（悪性ソフトウェア）に感染した攻撃者の制御下にあるコンピューターのネットワーク

観測手段の特徴

ダークネットは初期段階を検知可能で、ハニーポットは攻撃の詳細情報を収集可能

手順	方法	観測手段
1. 脆弱性のある機器やサービスの調査	ポートスキャン	ダークネット
2. ボットネットの構築	脆弱性を突く攻撃	ハニーポット
3. サイバー攻撃の実施	DDoS攻撃 クリプトジャッキング サイバー攻撃の踏み台	被害者

- 感染の初動段階を検知可能
- 設置が容易であるため、大規模な観測網の構築が可能

- 攻撃の詳細情報を収集可能
- 運用や解析に高度な専門的知識と作業が必要

=

攻撃者を引き寄せるように設計されたコンピュータシステム

観測手段の特徴

ダークネットは初期段階を検知可能で、ハニーポットは攻撃の詳細情報を収集可能

手順	方法	観測手段
1. 脆弱性のある機器やサービスの調査	ポートスキャン	ダークネット
2. ボットネットの構築	脆弱性を突く攻撃	ハニーポット
3. サイバー攻撃の実施	DDoS攻撃 クリプトジャッキング サイバー攻撃の踏み台	被害者

解析

- 感染の初動段階を検知可能
- 設置が容易であるため、大規模な観測網の構築

我々が出願中の特許技術

=

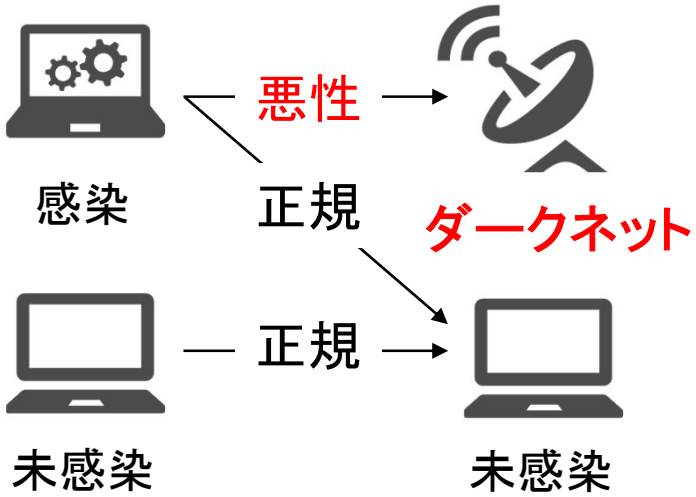
- 攻撃の詳細情報を収集可能
- 運用や解析に高度な専門的知識と作業が必要

攻撃者を引き寄せるように設計されたコンピュータシステム

ダークネットの観測方法と特徴

ダークネットは未使用のIPアドレスを使用することで、悪意のある通信を監視する

手順	方法	観測手段
1. 脆弱性のある機器やサービスの調査	ポートスキャン	ダークネット



観測方法

- 未使用のIPアドレスを使用して観測
- 初期通信のみを受信し、応答を返さない

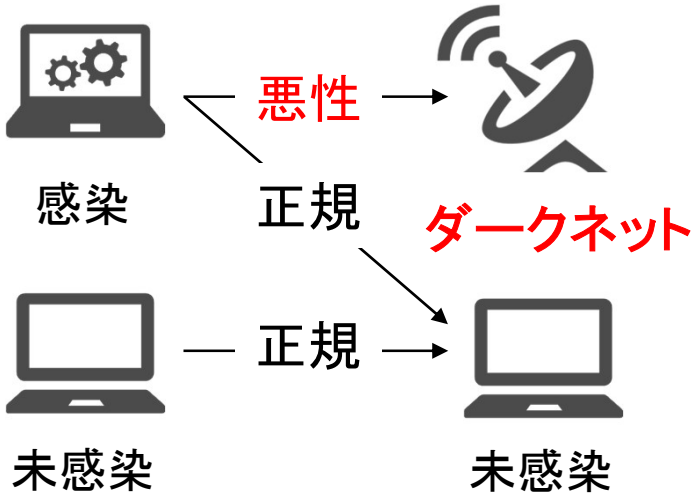
特徴

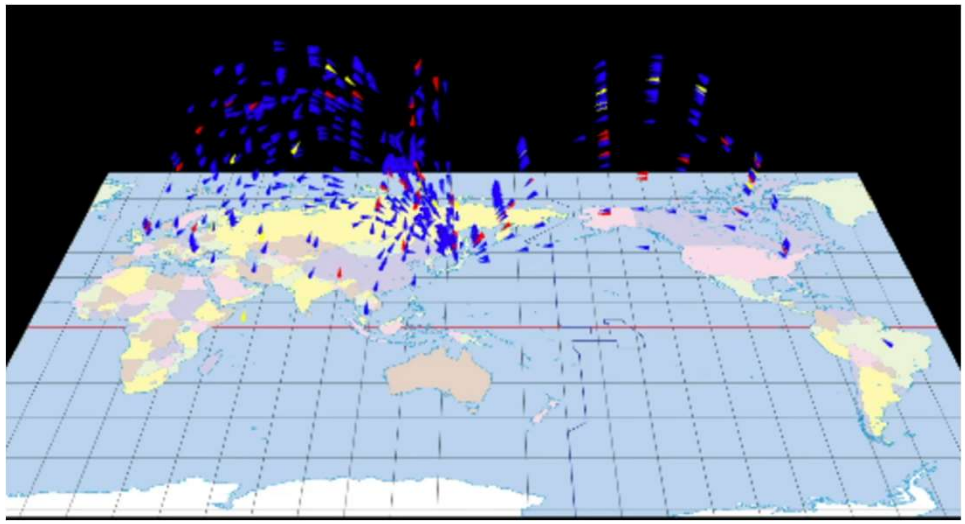
- 比較的多くの悪性通信が観測可能
- 通信の意図（調査・攻撃）の把握が困難

ダークネット通信の可視化

ダークネットは未使用のIPアドレスを使用することで、悪意のある通信を監視する

手順	方法	観測手段
1. 脆弱性のある機器やサービスの調査	ポートスキャン	ダークネット





目次

ダークネット解析に関する既存研究

スキャンを行う主体 → スキャナの振る舞いに着目して攻撃・調査目的スキャンを特定

攻撃目的
- 少数の宛先ポートを集中的にスキャン
- 感染した端末同士に同期性が見られる
- 一部フィンガープリント（シグネチャ）が存在

調査目的
- 多様な宛先ポートを定常的にスキャン
- 一部フィンガープリントが存在

文献	振る舞い: 宛先ポート	パケット数/スキャンレート	宛先ポート以外のヘッダフィールド	同期性	フィンガープリント	手法
Ban2015 [3]	✓					Association rule learning [1]
Cohen2020 [4]	✓					Word2Vec(DL), DBSCAN(ML)
Torabi2022 [16]	✓	✓				DBSCAN(ML)
Han2022 [10]		✓		✓		NMF [14] (ML), Graphical Lass [7] (ML) and NTD [11] (ML)
Griffioen2020 [5]			✓	✓	✓	SLPA [17] (ML),

DL: Deep Learning (深層学習)
ML: Machine Learning (機械学習)

ダークネット解析に関する既存研究の問題点

先行研究は信頼性の低さやフィンガープリントの自動特定に限界がある

攻撃目的
- 少数の宛先ポートを集中的にスキャン
- 感染した端末同士に同期性が見られる
- 一部フィンガープリント(シグネチャ)が存在

調査目的
- 多様な宛先ポートを定常的にスキャン
- 一部フィンガープリントが存在

文献	振る舞い					手法
	宛先ポート	パケット数/スキャンレート	宛先ポート以外のヘッダフィールド	同期性	フィンガープリント	
Ban2015 [3]	✓					Association rule learning [1]
Cohen2020 [4]						
Torabi2022 [16]						
Han2022 [10]		✓		✓		
Griffioen2020 [5]			✓	✓		

DL: Deep Learning (深層学習)
ML: Machine Learning (機械学習)

問題点
- 信頼性が低い＝過検知の発生

問題点
- 公開されたスキャンツールでしか作成できない。
- フィンガープリントを自動特定する従来手法では単一の式で表現されたフィンガープリントの特定に限定される。

我々の特許技術の要点

我々の特許技術

(マルウェアや調査目的スキャン特定のための)
柔軟な式で表現されるフィンガープリントを自動で特定するアルゴリズムを構築

解決

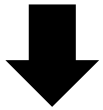
文献	振る舞い: 宛先ポート	振る舞い: パケット数/スキャンレート	振る舞い: 宛先ポート以外のヘッダフィールド	振る舞い: 同期性	フィンガープリント	手法 (DL: Deep Learning, ML: Machine Learning)
Ban2015 [3]	✓					Association rule learning [1]
Cohen2020 [4]						
Torabi2022 [16]						
Han2022 [10]		✓		✓		
Griffioen2020 [5]			✓	✓		

問題点
- 信頼性が低い＝過検知の発生

問題点
- 公開されたスキャンツールでしか作成できない。
- フィンガープリントを自動特定する従来手法では単一の式で表現されたフィンガープリントの特定に限定される。

特許技術の核心をなすアイデア

- フィンガープリント=スキャンの実行者がパケットに埋め込む固有特徴
- スキャンの実行者は複数の端末を用いてスキャンを行う



フィンガープリント=多数の送信元からのパケットに頻繁に現れる特徴

特徴=関数と値のペア

$$tcp.seq \oplus ip.dst = 0$$

特許技術のアイデア①

適切な統計量を独自に定義し、
頻度を定量化することで、
信頼性の高いフィンガープリントを特定

特許技術のアイデア②

遺伝的アルゴリズムの活用により
柔軟な関数で表現される特徴量の抽出

特許技術の成果

特許技術

柔軟な式で表現されるフィンガープリントを自動で特定するアルゴリズムを構築

名称	既知のフィンガープリント
Hajime(マルウェア)	$\mathrm{tcp.window} = 14600$
Mirai(マルウェア)	$\mathrm{tcp.seq} \oplus \mathrm{ip.dst} = 0$
Masscan(調査目的)	$\mathrm{ip.id} \oplus g_{L2B}(\mathrm{ip.dst}) \oplus \mathrm{tcp.dport} \oplus g_{L2B}(\mathrm{tcp.seq}) = 0$
ZMap(調査目的)	$\mathrm{ip.id} = 54321$
Mozi(マルウェア)	$\mathrm{tcp.window} = 29040 \vee \mathrm{tcp.window} = 14520$

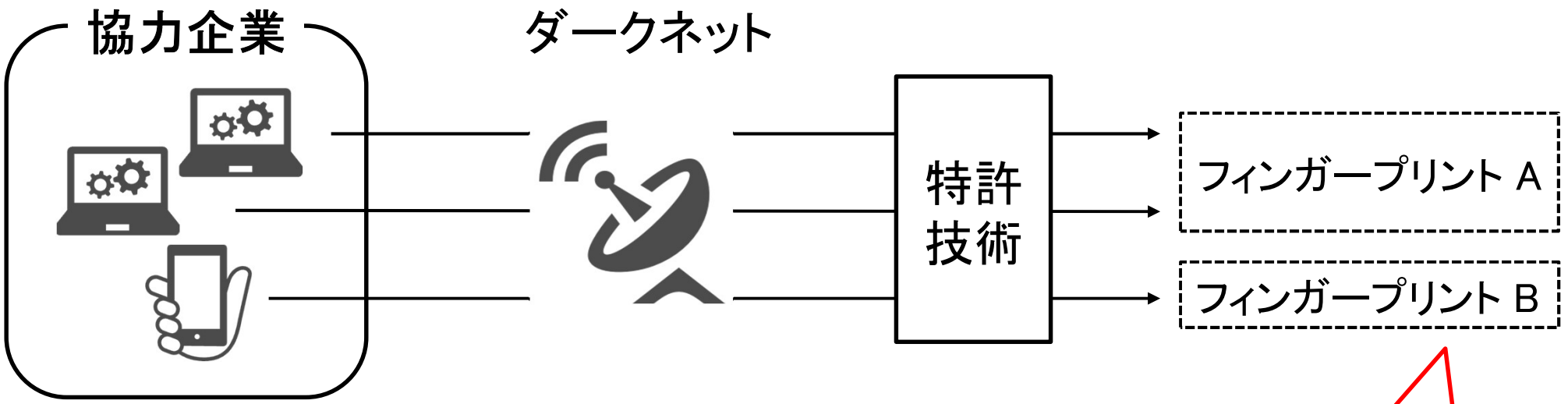
⊕:排他的論理和
g_{L2B}:下位2バイト
∨:論理和

成果

- 既知のフィンガープリント(攻撃:2種、調査:2種)を全て特定
- 今まで知られていなかったMoziボットネットと宛先ポートセットを特定
- 未知のフィンガープリントを8つ(攻撃:6種、調査:2種)特定
- 複数のボットネットに感染していると疑われるIPアドレスを特定

目次

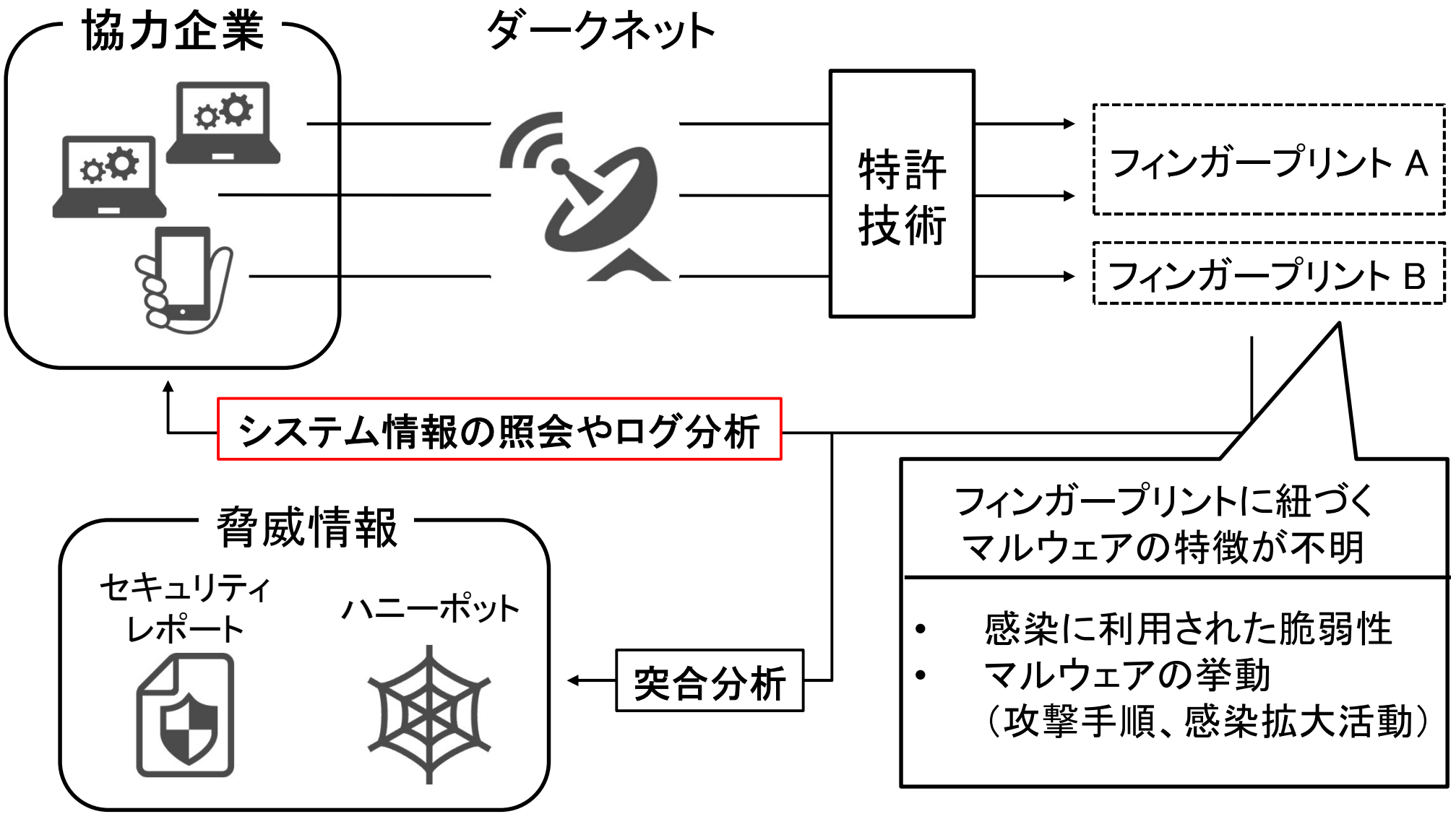
協力企業と実現したい最終目標とシステム概要



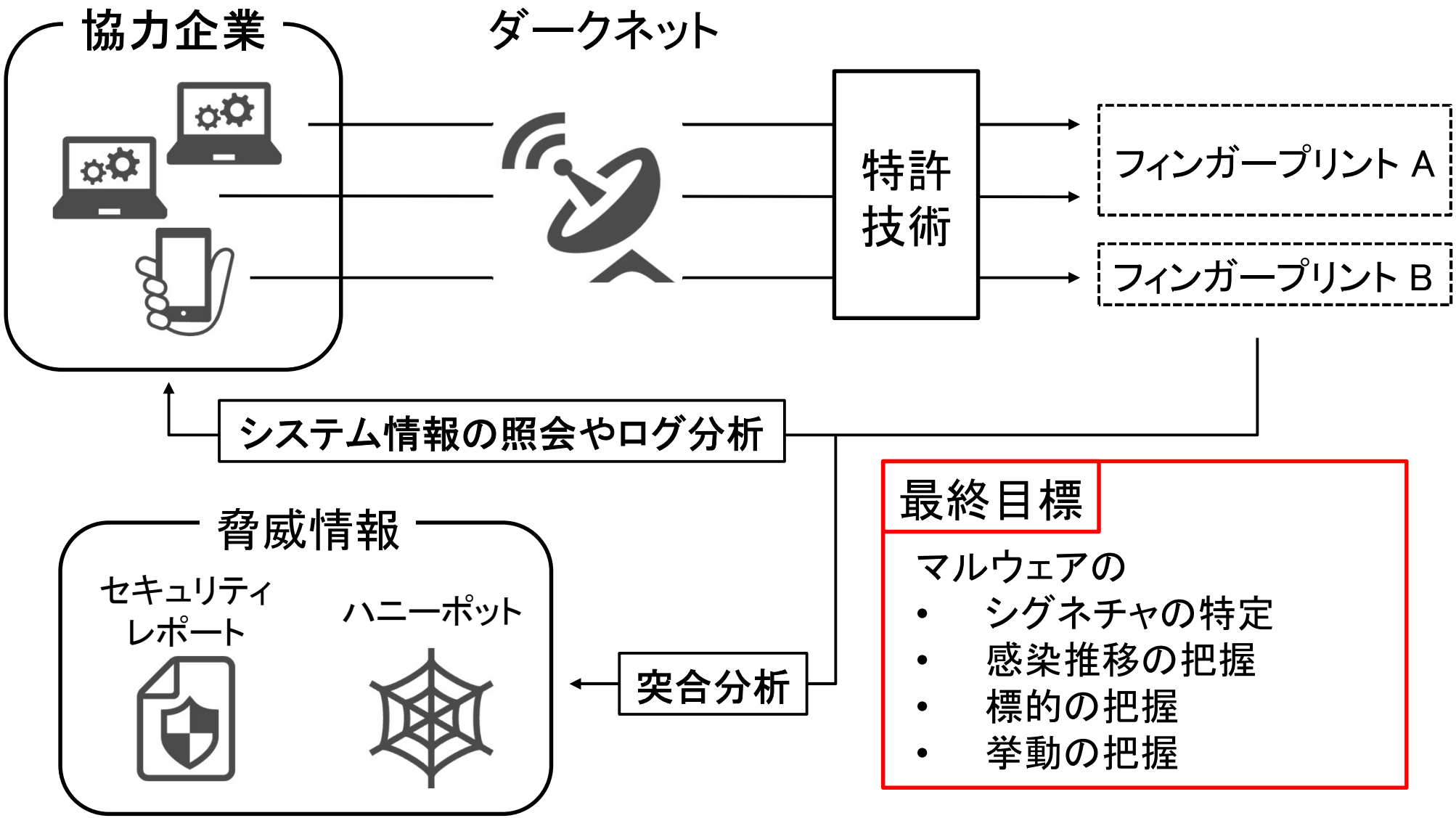
フィンガープリントに紐づく
マルウェアの特徴が不明

- 感染に利用された脆弱性
- マルウェアの挙動
  （攻撃手順、感染拡大活動）

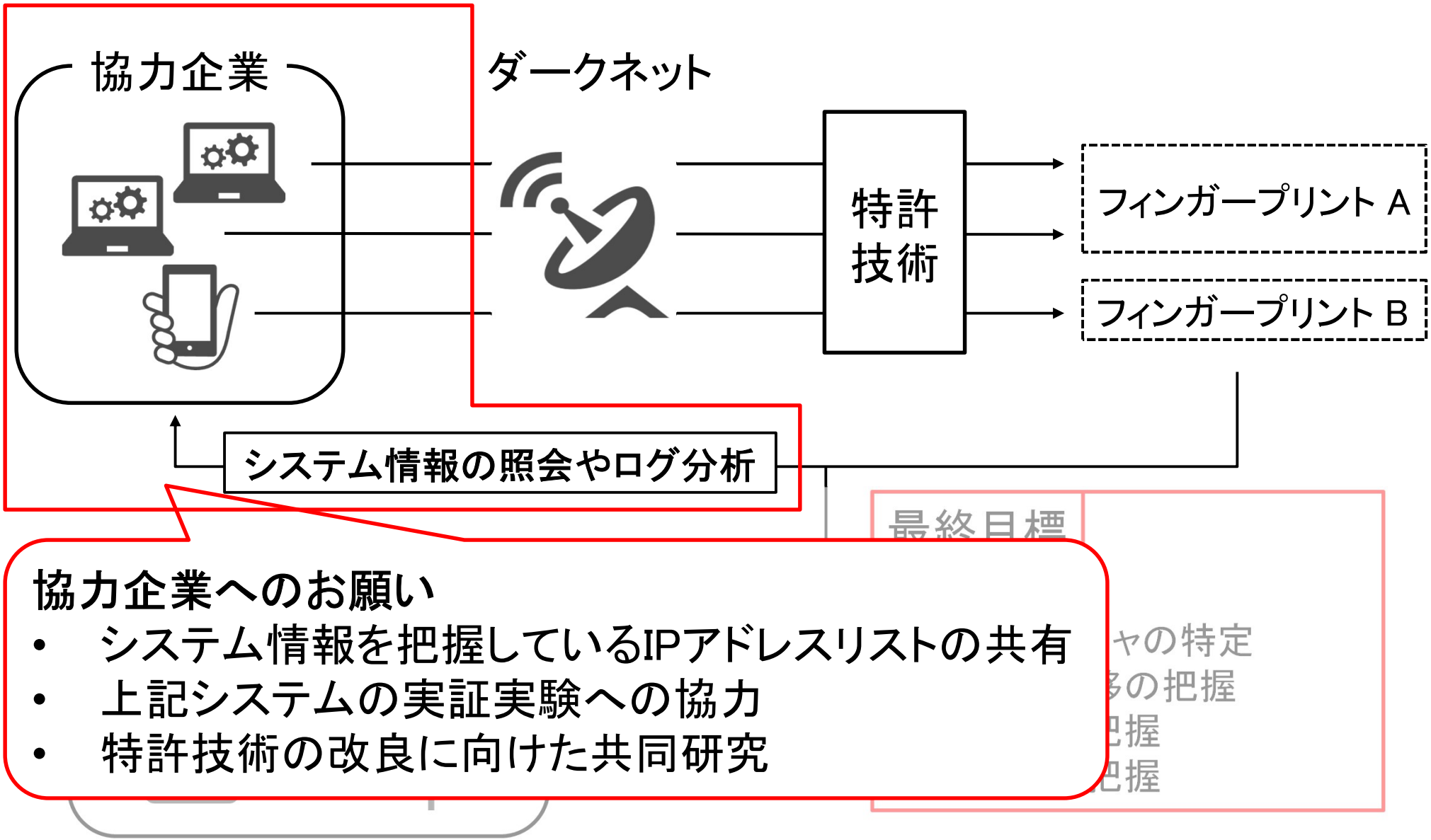
協力企業と実現したい最終目標とシステム概要



協力企業と実現したい最終目標とシステム概要



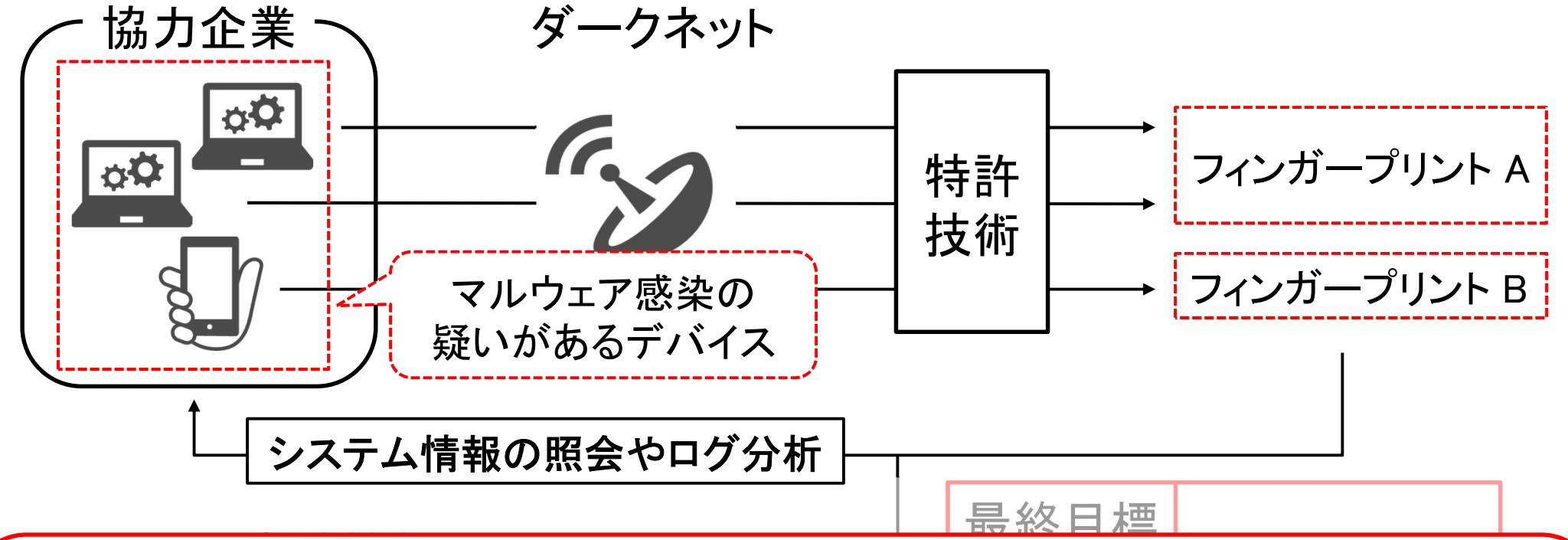
協力企業へのお願い



協力企業へのお願い

- システム情報を把握しているIPアドレスリストの共有
- 上記システムの実証実験への協力
- 特許技術の改良に向けた共同研究

協力企業のメリット



協力企業のメリット

- マルウェア感染の疑いがある管理下のデバイスの特定
- IDS/IPS=不正侵入検出/防御システムで用いるフィンガープリントの共有
- フィンガープリントに対応する攻撃情報の詳細の把握
- 脅威に関する知見の獲得(標的となる脆弱性や感染規模など)

目次

我々の特許技術の課題

我々が特定したフィンガープリントのみで全てのダークネットデータを解析できない

具体的に

2021年9月の1ヶ月間のデータを用いた実験では、
我々が特定したフィンガープリントを保有しないスキャナが50%存在する。

原因

- 特許技術では、複雑な演算で表現されるフィンガープリントの検知が難しい（いかなる手法でも理論的に難しいと考えられる）
- フィンガープリントが存在しないスキャナも存在すると考えられる

解決に向けた現在の取り組み

フィンガープリントに頼らず、宛先ポートセットに着目したマルウェア追跡アルゴリズムを開発中

- マルウェアMiraiの感染初期を検知・追跡できることを検証済み
- 数理手法を用いることで、オペレーターが解釈可能なアルゴリズムを考案
- ハニーポットデータとの突合によりマルウェアのライフサイクル特定に注力

我々の特許技術の核心をなすアイデア

- フィンガープリント=スキャンの実行者がパケットに埋め込む固有特徴
- スキャンの実行者は複数の端末を用いてスキャンを行う

フィンガープリント=多数の送信元からのパケットに頻繁に現れる特徴

特徴=関数と値のペア

$$tcp.seq \oplus ip.dst = 0$$

特許技術のアイデア①

適切な統計量を独自に定義し、
頻度を定量化することで、
信頼性の高いフィンガープリントを特定

特許技術のアイデア②

遺伝的アルゴリズムの活用により
柔軟な関数で表現される特徴量の抽出

頻度の定量化に関する考慮事項

判定基準 ＼ 状況	Case1 特徴1(F)が50% 特徴2～51が1%	Case2 特徴1(F)が1% 特徴2～9,901が 0.01%	Case3 特徴1(F)が1% 特徴2(F)が0.5% 特徴3～98,500が 0.001%
頻度の絶対量による判定 (X%以上なら頻度が高い)	○	×	×
次に大きい頻度との 相対的な頻度で判定	○	○	×
最小値付近の頻度との 相対頻度で判定	○	○	○

特許技術

(F)はフィンガープリントを表す

特徴1の頻度は特徴2と比べて、2倍しか大きくないので、特徴1はフィンガープリントとみなされない。

目次

特許技術に関する知的財産権

- 発明の名称

  フィンガープリント特定システム及び
  フィンガープリント特定方法
- 出願番号
  - 特願2022-123952
  - 特願2022-123955
- 出願人　　：国立研究開発法人情報通信研究機構
- 発明者　　：田中智、韓燦洙、高橋健志、井上大介

参考文献①

[1] R. Agrawal, T. Imieli´nski, and A. Swami, “Mining association rules between sets of items in large databases,” in Proceedings of the 1993 ACM SIGMOD international conference on Management of data - SIGMOD '93. ACM Press, 1993. [Online]. Available: https://doi.org/10.1145/170035.170072

[3] T. Ban, M. Eto, S. Guo, D. Inoue, K. Nakao, and R. Huang, “A study on association rule mining of darknet big data,” in 2015 International Joint Conference on Neural Networks (IJCNN). IEEE, Jul. 2015. [Online].Available: https://doi.org/10.1109/ijcnn.2015.7280818

[4] D. Cohen, Y. Mirsky, M. Kamp, T. Martin, Y. Elovici, R. Puzis, and A. Shabtai, “DANTE: A framework for mining and monitoring darknet traffic,” in Computer Security – ESORICS 2020. Springer International Publishing, 2020, pp. 88–109. [Online]. Available: https://doi.org/10.1007/978- 3-030-58951-6_5

[5] H. Griffioen and C. Doerr, “Discovering collaboration: Unveiling slow, distributed scanners based on common header field patterns,” in NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium. IEEE, Apr. 2020. [Online]. Available: https://doi.org/10.1 109/noms47738.2020.9110444

[7] J. Friedman, T. Hastie, and R. Tibshirani, “Sparse inverse covariance estimation with the graphical lasso,” Biostatistics, vol. 9, pp. 432–441, 7 2008.

[10] C. Han, J. Takeuchi, T. Takahashi, and D. Inoue, “Dark-tracer: Early detection framework for malware activity based on anomalous spatiotemporal patterns,” IEEE Access, vol. 10, pp. 13 038–13 058, 2022. [Online]. Available: https://doi.org/10.1109/access.2022.3145966

参考文献②

[11] Y.-D. Kim and S. Choi, “Nonnegative tucker decomposition,” in 2007 IEEE Conference on Computer Vision and Pattern Recognition. IEEE, Jun. 2007. [Online]. Available: https://doi.org/10.1109/cvpr.2007.383405

[14] D. Lee and H. S. Seung, “Algorithms for non-negative matrix factor- ization,” in Proceedings of the 13th International Conference on Neural Information Processing Systems. MIT Press, 2000, p. 535–541.

[16] S. Torabi, E. Bou-Harb, C. Assi, E. B. Karbab, A. Boukhtouta, and M. Debbabi, “Inferring and investigating IoT-generated scanning campaigns targeting a large network telescope,” IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 402–418, Jan. 2022. [Online]. Available: https://doi.org/10.1109/tdsc.2020.2979183

[17] J. Xie, B. K. Szymanski, and X. Liu, “SLPA: Uncovering overlapping communities in social networks via a speaker-listener interaction dynamic process,” in 2011 IEEE 11th International Conference on Data Mining Workshops. IEEE, Dec. 2011, pp. 344–349. [Online]. Available: https://doi.org/10.1109/icdmw.2011.154

お問い合わせ先

国立研究開発法人情報通信研究機構
イノベーション推進部門
知財活用推進室

ＴＥＬ　042-327-6950
e-mail　ippo@ml.nict.go.jp