TDU
TOKYO DENKI UNIVERSITY

Information Security Lab
Collaborate together
to make our Internet secure.

研究用データセット「動的活動観測2024」
動的活動観測システム（BOS2）
Behavior Observable System 2

2025/07/01

建部大聖／東京電機大学
寺田真敏／東京電機大学・日立製作所

BOS（Behavior Observable System）

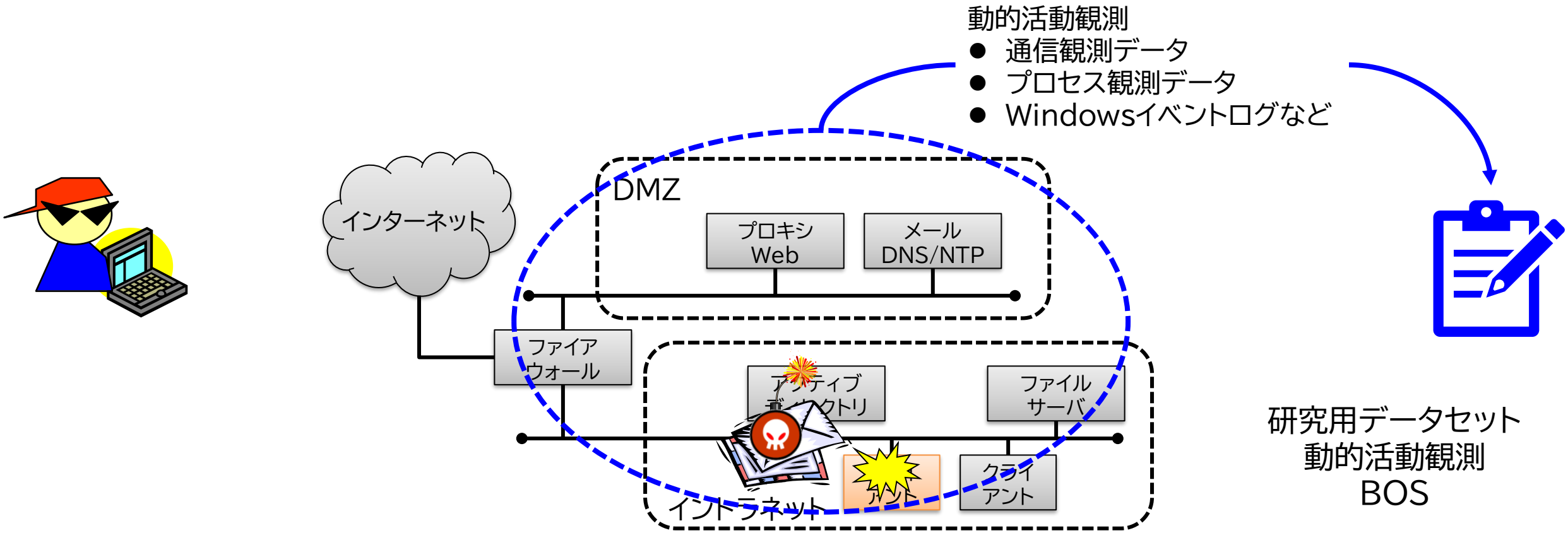
マルウェア検体の静的／動的解析では、指令サーバ接続、情報窃取、バックドアなどの機能の存在や挙動把握に重点が置かれ、これら機能のいずれを使ったのか、どの順番で使ったのかなど、攻撃者の行動という視点で把握や解析することはなかった。

多くの場合、攻撃者の行動＝マルウェアの挙動という想定の下、静的／動的解析によって対応してきたというのが実情である。しかし、組織内ネットワークへの侵害活動においては、攻撃者の存在を意識する必要がある。

本データセットは、**「攻撃者行動視点で脅威の特徴情報」を明らかにしていくために、攻撃者の行動を記録する研究用データセットの作成**を目標としている。

BOS 第1世代 2014～2019（BOS）

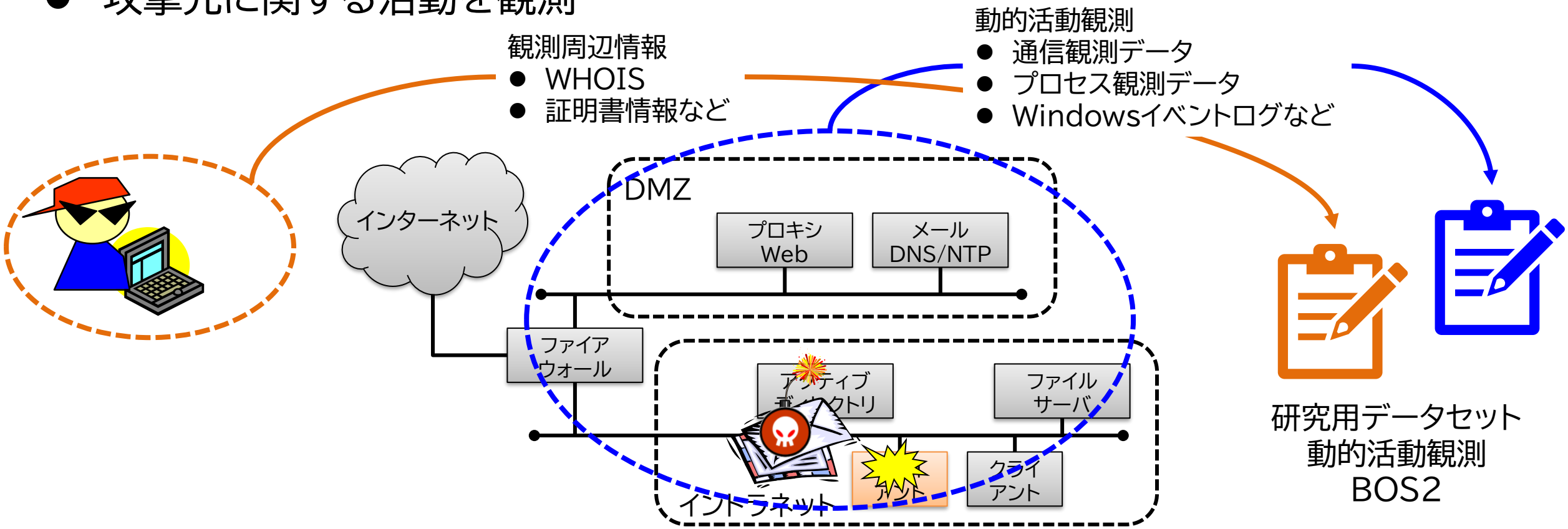
- 標的型攻撃等の侵入後の攻撃者の活動を観測
  - 企業のネットワークを模擬する小規模なネットワーク環境を構築
  - 標的型攻撃メールに添付されたマルウェアなどを動的観測環境下で実行



サイバー攻撃誘引基盤STARDUST

BOS 第2世代 2024～（BOS2）

- 標的型攻撃等の侵入後の攻撃者の活動を観測
  - 企業のネットワークを模擬する小規模なネットワーク環境を構築
  - 標的型攻撃メールに添付されたマルウェアなどを動的観測環境下で実行
- 攻撃元に関する活動を観測



サイバー攻撃誘引基盤STARDUST

BOS 第2世代 2024～（BOS2）

- BOS2試行版データセットの構成
  - 動的活動観測　攻撃者の活動記録
    - README(.txt)　実行クライアント名、収録データ概要などを記載
    - 検体メタ情報(.json)　検体メタ情報をSTIX2.1で記載
    - networklog(.pcap)　マルウェア検体を実行したクラアントの通信ログ
    - イベントログ(.evtx)　Windowsイベントログ(Application,System,Security)
    - Procmon_log(.pml)　マルウェア検体を実行したクラアントのProcess Monitorログ
  - 観測周辺情報　マルウェア検体の通信先に関する情報
    - 直接関連情報　通信先にアクセスした際に取得できる情報
      - スクリーンショット
      - ソースファイル
      - SSL証明書
    - 間接関連情報　通信先に関する登録情報
      - DNS
      - Whois

BOS 第2世代 2024～（BOS2）

- BOS2試行版データセットの概要

項目	内容
観測対象	● 2024～2025にかけて解析者コミュニティで報告のあった検体 ● 2024～2025にかけて独自に入手した検体
観測期間	● 2024年10月03日～2025年02月21日
観測記録時間	● 3～7日(リモートコントロール型など長期的な観測が必要なマルウェア) ● 1時間～1日(情報窃取型など短期的な動作で動作を終了するマルウェア)
データ制限	● 各観測ケース上限2GB ● Process Monitorログは検体実行後から最長1時間後までに制限

BOS 第2世代 2024～（BOS2）

- BOS2試行版データセットの概要

#	SHA256	検体種別	観測期間	進行度	pcap	evtx	pml	直接関連情報	間接関連情報	VTでのMicrosoft検出名
i01	7a31a	RAT	2024/10/03～2024/10/04	7	○	○		○	○	Trojan:Win32/Leonem
i02	5789d	Trojan	2024/10/15～2024/10/16	2	○	○				Trojan:MSIL/FormBook.SMW!MTB
i03	c12fe	Trojan	2024/11/11～2024/11/12	6	○	○				Trojan:MSIL/Taskun!MTB
i04	d921f	Trojan	2024/12/12	7	○	○	○	○	○	Trojan:Win32/Phorpiex.RA!MTB
i05	530fb	RAT	2024/12/12～2024/12/15	6	○	○	○	○	○	Trojan:MSIL/Injector.CG!MTB
i06	03052	RAT	2024/12/18～2024/12/24	8	○	○	○	○	○	TrojanDownloader:MSIL/Ader.SS!MTB
i07	44936	RAT	2025/1/20～2025/1/27	4	○	○	○		○	Undetected
i08	44717	Trojan	2025/2/7	2	○	○	○			Trojan:MSIL/FormBook!rfn
i09	7a31a	RAT	2025/2/14～2025/2/21	7	○	○	○		○	Backdoor:MSIL/AsyncRat.AD!MTB

進行度　1～2：通信の発生なし
3～5：C2サーバと攻撃通信成立せず
6～8：C2サーバと攻撃通信成立

□：解析者コミュニティで報告のあった検体
■：独自に入手した検体

おわりに

BOSデータセットの後継としてのBOS2データセットについて

BOS

組織内ネットワークへの侵害活動を想定した研究用データセット

- 動的活動観測　　攻撃者の活動記録

BOS2

観測周辺情報を追加した組織内ネットワークへの侵害活動を想定した研究用データセット

- 動的活動観測　　攻撃者の活動記録
- 観測周辺情報　　マルウェア検体の通信先に関する情報
  - 直接関連情報　　通信先にアクセスした際に取得できる情報
  - 間接関連情報　　通信先に関する登録情報