2F-03

複数組織を跨ったダークネット観測の効果に関する検証

西嶋　克哉[†]　近藤　賢郎[‡]　細川　達己[‡]　重本　倫宏[†]　川口　信隆[†]
長谷川　弘幸[§]　本田　英之[**]　鈴木　康人[§]　鍛　忠司[†]　中村　修[††]
株式会社日立製作所　研究開発グループ[†]
慶應義塾　インフォメーションテクノロジーセンター本部[‡]　慶應義塾大学　環境情報学部[††]
中部電力株式会社　IT システムセンター[§]　株式会社中電シーティーアイ　インフラユニット[**]

1. はじめに

突発的に起こるサイバー攻撃からネットワークやシステムを守ることは，セキュリティオペレーションにとって不可欠の要件である．しかし，大規模化し巧妙になる攻撃を，自組織だけで守り抜くのは困難である．日立製作所では，中部電力，慶應大学と協力して，複数組織の SOC（Security Operation Center）を跨ったセキュリティオペレーション連携により，サイバー攻撃への集団防御を実現する分散 SOC アーキテクチャを提案している[1]．

本稿では，組織に割当てられているが未使用であるグローバル IP アドレス空間（以下，ダークネット）宛てのトラフィックを複数組織に跨って観測することで，不審な IP アドレスの発見が効率化されることを確認したので報告する．

2. 関連研究

本稿のように，複数のダークネット観測データを分析する研究が行われている．鈴木ら[2]は，4 カ国のダークネットで観測される攻撃の比較を行い，攻撃の局地性の分析を行った．一方で，本研究は観測地点ごとに得られる不審な IP アドレスに着目をしており，この点で異なる．また，芦野ら[3]は，効率の良いセンサーの設置計画を目的として，観測環境のセンサーの数，観測期間，グローバル IP アドレスによって観測できる内容に差があることを確認した．一方で，宛先ポート番号/プロトコル（以下，ポート/プロトコル）毎の分析は行っておらず，本研究とは異なる．

3. 提案手法

サイバー攻撃は，無差別に行われる場合があるが，特定の組織に向けて行われる場合もある．従って，複数組織を観測することにより，単一組織を観測するよりも多くの攻撃情報を収集することが可能であると考えられる．このことを検証する手法を提案する．

3.1. 対象データ

本検証では，WIDE Project[4]（以下，WIDE）及び中部電力で観測したダークネットデータを使用した．WIDE は/19 のダークネット領域（以下，領域）を観測しており，中部電力は/24 の領域を観測している．これらの観測地点で観測したデータの内，2019 年 8 月の 1 カ月分を 1 日毎に集計し，更に，ポート/プロトコル毎に集計したデータを対象とした．尚，検証対象のポート/プロトコルは，1 日毎に集計した結果，接続元ホスト数が 1000 以上のものとした．また，単一組織間，および，複数組織間を比較するために，WIDE の領域を，1 個の領域が中部電力の領域と同じサイズになるように，32 個の/24 の部分領域に分割した．ある日付 d の WIDE の各領域の送信元ホストの集合をそれぞれ w_{d1}，w_{d2}，...，w_{d32}，中部電力の領域の送信元ホストの集合を c_{d1} とし，それらの集合を $W=\{w_{d1}, w_{d2}, ..., w_{d32}\}$，$C=\{c_{d1}\}$ とする．

3.2. 比較方法

先ず，2 個の領域間の Jaccard 係数，及び和集合を取りうる全ての組み合わせで算出した．Jaccard 係数は，以下の式(1)により算出される値であり，値が小さいほど領域間の類似度が低いことを意味する．

$$Jaccard(i,j) = \frac{|i \cap j|}{|i \cup j|} \quad (1)$$

ここで，i，j は i，j⊂W∪C かつ i ≠j である．また，和集合は，2 個の領域で観測されたユニークな接続元ホストを表し，この数が多いことは，不審な IP アドレスをより多く観測できていることを意味する．

次に，累積頻度による比較を行う．N を領域数とし，各 N において観測された接続元ホスト数と，全領域で観測された接続元ホスト数との比率を計算した．ここでは，単一組織で領域を 1 から順に拡大した場合と，複数組織を組み合わせながら領域を拡大した場合とを比較する．例えば，N=3 のとき，単一組織の集合$\{w_{d1}, w_{d2}, w_{d3}\}$と，複数組織の集合$\{w_{d1}, c_{d1}, w_{d2}\}$の観測結果を比較する．

4. 結果と考察

図 1 にポート/プロトコル毎の，単一組織間の Jaccard 係数と複数組織間の Jaccard 係数の差分を示す．Jaccard 係数差分は，以下の式(2)により算出される値であり，集合 W，C の要素を 2 つ選択する組み合わせにおいて，WIDE，中部電力を含む組み合わせの Jaccard 係数平均値から，WIDE のみを含む組み合わせの Jaccard 係数平均値を減算し，更に，検証対象期間で平均をとったものである．

$$\frac{1}{D}\sum_{d=1}^{31}\left(\frac{\sum_{i=1}^{|W|} jaccard(w_{di}, c_{d1})}{|W|} - \frac{\sum_{j=1}^{|W|}\sum_{k=j+1}^{|W|} jaccard(w_{dj}, w_{dk})}{{}_{|W|}C_2}\right) \quad (2)$$

ここで，${}_xC_y$ は集合 x から y 個を選んで得られる組み合わせ数を，D はポート/プロトコルが分析対象となった日数をそれぞれ表す．また，Jaccard 係数を計算する際に，0 での除算が発生する場合はシグマの計算を次に進め，項の分母の値から 1 を減算する．

算出した値が負の場合，複数組織の組み合わせの方が，

Verification of effect of darknet monitoring in multiple organizations
† Katsuya NISHIJIMA, Tomohiro SHIGEMOTO, Nobutaka KAWAGUCHI, Tadashi KAJI・Hitachi, Ltd.
‡ Takao KONDO, Tatsumi HOSOKAWA・Keio University
§ Hiroyuki HASEGAWA, Yasuhito SUZUKI・Chubu Electric Power Company, Inc.
** Hideyuki HONDA・ChudenCTI Co.,Ltd.
†† Osamu NAKAMURA・Keio University

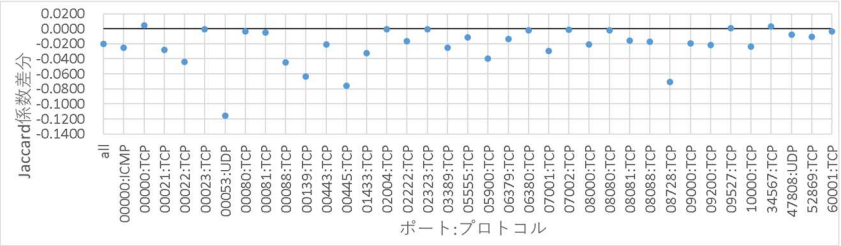

図 1　ポート/プロトコル毎の Jaccard 係数差

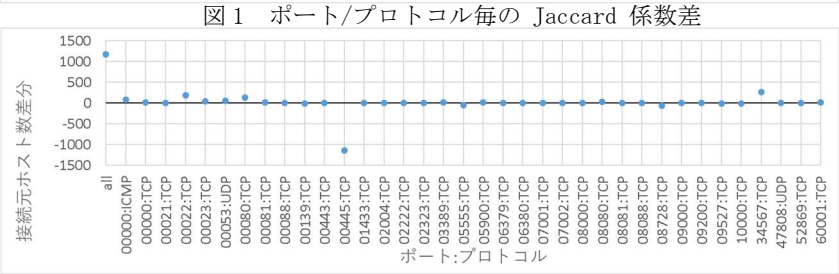

図 2　ポート/プロトコル毎の 送信元ホスト数差分

単一組織内の組み合わせよりも Jaccard 係数が小さい，すなわち類似度が低いことを意味する．また，ポート/プロトコルが all というのは，ポート/プロトコル毎の集計を行っていないことを意味する．また，和集合の要素数に対しても同様の処理を施し送信元ホスト数差分を算出し，その結果を図 2 に示す．送信元ホスト数差分が正の場合，複数組織の組み合わせの方が，単一組織内の組み合わせよりも和集合の要素数が大きい，すなわちより多くの不審 IP アドレスを観測できていることを意味する．

図 1 の all の値より，複数組織を組み合わせることにより，Jaccard 係数が 0.020 ポイント減少していることが分かる．また，ポート/プロトコル毎に値のばらつきがあることが分かる．TCP:22，TCP:53，TCP:88，TCP:139，TCP:445，TCP:5900，TCP:8728 は類似度が大きく減少していた．このことより，検証対象期間のこれらのポート/プロトコルに対する攻撃は，広い IP アドレス空間に対してではなく，特定の IP アドレス空間，あるいは特定の組織に向けて実施されたものと推察される．一方，TCP:23，TCP:2323 は類似度に差がほとんどなかった．これらは IoT マルウェアである mirai の感染活動に用いられるポートである．mirai は，ランダムに接続を行うため，領域ごとの違いが少なかったと考えられる．また，図 2 の all の値より，複数組織を組み合わせることにより，接続元ホスト数が 1180 増加していることが分かる．一方で，ポート/プロトコル毎に比較すると，TCP:445 のように，大きく減少しているケースもある．尚，1 つの接続元ホストが複数のポート/プロトコルに 通信している場合があるため，各ポート/プロトコルの合計と all の値は異なる．

次に累積頻度の比較について，特に差が顕著であった，2019 年 8 月 28 日のポート/プロトコルが 22:TCP, 9200:TCP の結果を図 3，4 に示す．

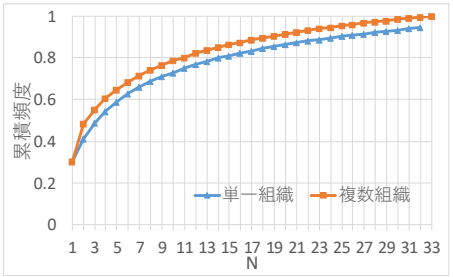

図 3　送信元ホスト数の累積頻度（8 月 28 日，22:TCP）

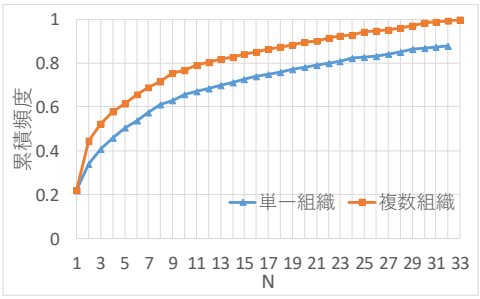

図 4　送信元ホスト数の累積頻度（8 月 28 日，9200:TCP）

図 3，4 より，複数組織を組み合わせることにより，同一の領域数のときに，より多くの攻撃情報を収集できていることが分かる．この増加分は N が大きい場合にも存在し，単一組織の領域数を増やしても得られない情報が複数組織の観測により得られていることが分かる．

5. まとめと今後の課題

本稿では複数組織の SOC 連携効果検証の 1 つとして，複数組織に跨ったダークネット観測の効果について検証を行った．結果として，異なる組織を観測することにより，単一組織の観測よりも多くの攻撃情報を観測できることを示した．また，その傾向はポート/プロトコル毎に異なることが分かった．今後は，連携組織の拡張，観測時期による分析について検証する．

参考文献

[1]近藤 賢郎，他．分散型 SOC アーキテクチャに基づいた複数組織間におけるセキュリティ・オペレーションの連携．マルチメディア，分散協調とモバイルシンポジウム 2018 論文集,2018,872-878 (2018-06-27)

[2]鈴木 将吾，他．複数国ダークネット観測による攻撃の局地性分析．コンピュータセキュリティシンポジウム 2014 論文集,2014(2),40-47 (2014-10-15)

[3]芦野 佑樹，他．インターネットに接続されたサイバー攻撃観測用センサーの環境に関する考察．研究報告コンピュータセキュリティ（CSEC）,2018-CSEC-82(40),1-8 (2018-07-18) , 2188-8655

[4]WIDE backbone. http://two.wide.ad.jp/.