3E-5

攻撃シナリオを用いた多段攻撃検知手法の検討*

居城 秀明，河内 清人，桜井 鐘治†
三菱電機株式会社　情報技術総合研究所‡

1. はじめに

脆弱性を悪用し，複数の既存攻撃を組み合わせることで，対応が難しく執拗なサイバー攻撃が出現してきている[1]．特定企業等を狙ったこうした攻撃は標的型攻撃と呼ばれ，セキュリティ上の重大な脅威となっている．こうした脅威に対し，従来からの予防的対策では限界があり，攻撃の段階ごとに発生する事象を異常として検知することで，攻撃者の目標達成を阻止することが必要である[2]．

本稿では、複数の攻撃を組み合わせた多段攻撃の検知手法を利用して、標的型攻撃を検知する手法を考える．既存の手法[3]において課題の1つである，システムの観測できない攻撃を含む場合の多段攻撃で，攻撃イベントを推定することにより多段攻撃を検知する手法を提案する．これにより多段攻撃を利用した標的型攻撃の検知精度向上が望める．

2. 多段攻撃検知

2.1. 多段攻撃検知手法

多段攻撃は，攻撃者が 1 つの目的のために複数の段階に分かれた攻撃を行うことを指す．標的型攻撃は多段攻撃にあたる．文献[3]では多段攻撃を検知するために各攻撃イベント(例：IDS(Intrusion Detection System)からのアラート)に対し，攻撃イベントが成立するための必要条件(事前条件)，及び攻撃イベントが発生したことによる状態変化(結果)を定義している．そして攻撃イベントの結果が他の攻撃イベントの事前条件となるようにつなげたイベント列(攻撃シナリオ)が生成可能かどうかで多段攻撃を検知する手法が提案されている．

2.2. 既存手法における課題

しかし，イベントの中にはログに記載されないイベント，コストとのトレードオフ等で監視対象外とされ，システムが観測することのできないイベント(以下これらを観測不可イベントとよぶ)がある．このとき，従来の手法において，本来観測可能であればイベント列として検知できるはずの多段攻撃がイベント列として見なされず，検知漏れが発生するという課題がある．

2.3. 本稿でのアプローチ

そこで本稿では，攻撃シナリオに観測不可イベントを含む場合，イベント列生成時に観測不可イベントの推定を行う手法を提案する．これにより多段攻撃の検知精度向上が期待できる．

3. 提案手法

図 1は提案手法による多段攻撃の検知方法を説明したものである．観測された攻撃イベントを入力とし，生成したイベント列をイベント列DB§に登録・更新する．イベント列 DB の状態を確認し，一定の基準を満たした場合に通知することで多段攻撃を検知する．以下に観測不可イベントを推定する 3 つの手法を提案する．ここで各提案手法は，攻撃イベント対し，システムが観測可能かどうかのパラメータを事前に定義するものとする．

3.1. 提案手法 1

イベント列生成時，観測不可イベントは観測したものとみなすことで推定を行う手法を説明する．具体的な実現方法は次のとおりである．

1. 入力された攻撃イベントの事前条件を結果に持つ攻撃イベントを含むイベント列を，イベント列 DB から検索する
2. 対応するイベント列がない場合，入力イベントの事前条件を結果に持つような攻撃イベントをイベント DB**から検索する．対応するイベント列が見つかった場合は入力イベントを対応するイベント列に追加し，イベント列 DB を更新後，処理を完了する
3. イベント検索の結果，得られた攻撃イベントが観測不可イベントと設定されていた場合，検索結果の攻撃イベントを観測したものと見なす．その後，観測したものと見なした攻撃イベントを入力イベントとして 1. を行う．観測可能であった場合は得られた攻撃イベントを観測したものとはみなさず，入力イベントを新たなイベント列としてイベント列 DB に登録し処理を完了する

3.2. 提案手法 2

イベント列生成時，観測不可イベントを以下の方法で推定する．

- 観測不可イベントの事前条件を結果に持つ，

---

* Extension of multi-stage attack detection using attack

† Hideaki IJIRO, Kiyoto KAWAUCHI, Shoji SAKURAI
‡ Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501, Japan

§ イベント列生成機能によって作成された、攻撃イベント間の依存関係を含む攻撃イベントの集合を格納したデータベース

** 攻撃イベントを格納したデータベース

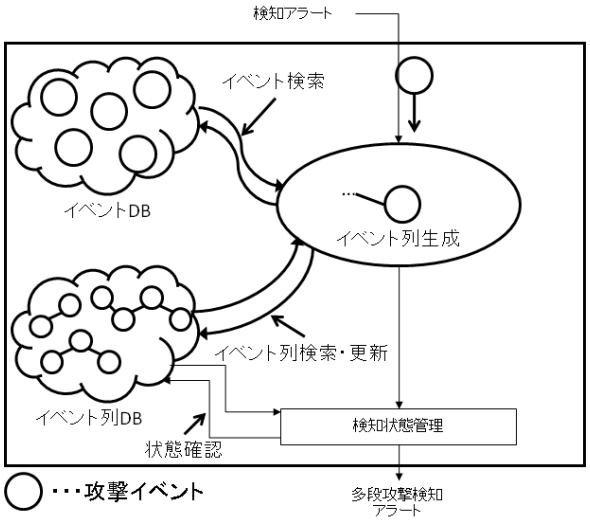

図 1 多段攻撃検知手法の説明図

及び結果を事前条件に持つ攻撃イベントが観測されているかどうかを確認する

- 上記攻撃イベントがともに観測されていた場合，該当する観測不可イベントを観測したものと見なす

具体的な実現方法は次のとおりである．

1. 入力された攻撃イベントの事前条件を結果に持つ攻撃イベントを含むイベント列を，イベント列 DB から検索する
2. 対応するイベント列がない場合，入力イベントの事前条件を結果に持つような攻撃イベントをイベント DB から検索する．対応するイベント列が見つかった場合は入力イベントを対応するイベント列に追加し，イベント列 DB を更新後処理を完了する
3. イベント検索の結果，得られた攻撃イベントが観測不可イベントと設定されていた場合，さらに観測不可イベントの事前条件を結果に持つような攻撃イベントを含む，イベント列を検索する．観測可能であった場合は得られた攻撃イベントを観測したものとはみなさず，入力イベントを新たなイベント列としてイベント列 DB に登録し処理を完了する
4. 対応するイベント列が見つかった場合は観測不可イベントを観測したものと見なす．その後，入力イベント，得られた攻撃イベントを対応するイベント列に追加しイベント列 DB を更新後処理を完了する．対応するイベント列が見つからなかった場合は得られた攻撃イベントを観測したものとはみなさず，入力イベントを新たなイベント列としてイベント列 DB に登録し処理を完了する

3.3. 提案手法 3

イベント列生成時，観測不可イベントを以下の方法で推定する．

- 観測不可イベントの事前条件を結果に持つ，及び結果を事前条件に持つ攻撃イベントに基づいて発生確率を計算する．発生確率は過去の事例に基づき事後確率を計算する
- 発生確率が一定のしきい値を超えている場合は発生したものと見なす

具体的な実現方法は次のとおりである．

1. 入力された攻撃イベントの事前条件を結果に持つ攻撃イベントを含むイベント列を，イベント列 DB から検索する
2. 対応するイベント列がない場合，入力イベントの事前条件を結果に持つ攻撃イベントをイベント DB から検索する．対応するイベント列が見つかった場合は入力イベントを対応するイベント列に追加し，イベント列 DB を更新後処理を完了する
3. イベント検索の結果，得られた攻撃イベントが観測不可イベントと設定されていた場合，得られた観測不可イベントに観測判定待ちイベントのタグ付けを行う．観測可能であった場合は得られた攻撃イベントを観測したものとはみなさず，入力イベントを新たなイベント列としてイベント列 DB に登録し処理を完了する
4. タグ付けされた攻撃イベントを観測したものと同じように扱い，提案手法 1 と同様にイベント列を生成する
5. タグ付けされた攻撃イベントに対し，事前条件を結果に持つ，および結果を事前条件に持つ攻撃イベントに基づく，攻撃イベントの発生確率を計算する．このとき発生確率が一定のしきい値以上であった場合は，該当するイベントは発生したものと見なす．しきい値に満たなかった場合はタグ付けされたイベントを観測されなかったものと見なし，接続されたイベント列を各々別のイベント列としてイベント列 DB に登録する

4. 考察

各提案手法による効果は次のとおりである．提案手法 1 は観測不可イベントを含む場合でもイベント列を生成することができるため，多段攻撃の検知漏れを防ぐことができる．提案手法 2 は提案手法 1 で発生すると考えられる多段攻撃の誤検知を防ぐことができる．提案手法 3 は発生確率により観測不可イベントを評価できるため，提案手法 2 と比べて検知精度が向上することが期待できる．

5. まとめと今後の課題

本稿は攻撃シナリオを用いた多段攻撃検知手法においてシステムが観測できない推定を行う手法を提案した．今後は各提案手法を実装評価し，有用性を検証する．

6. 参考文献

[1] 情報処理推進機構，“IPA テクニカルウォッチ『新しいタイプの攻撃』に関するレポート，” 2010 年 12 月．

[2] 日本セキュリティ監査協会，APT による攻撃対策と情報セキュリティ監査研究会，“APT 対策入門，” インプレス R&D，2012 年．

[3] Y. C. D. S. R. Peng Ning，“Constructing Attack Scenarios through Correlation of Intrusion Alerts，” CCS’02，2002．