No. B-2

会津大学

悪意を持った攻撃からウェブサイトを守るセキュリティ新技術

教授　白　寅天

機械学習による悪性ウェブコードの自動判別

概要

○ 技術の概要

正規のＩＤ、パスワードなしでも悪性ウェブコードを入力することでウェブサイトに侵入し、個人情報の盗難などの攻撃が可能です。このような攻撃に対し、悪性ウェブコードを自動判別して、アクセスの遮断などの対策を可能にする技術です。

○ 従来技術・競合技術との比較

既存の手法ではウェブ管理者の予測範囲を超えた攻撃を防ぐことはできませんが、本技術では機械学習を採用することで未知の攻撃を防ぐことが可能になりました。さらに、学習データを用意することにより、瞬時に悪意のある攻撃を動的に識別できます。

○ 技術の特徴

- ウェブ管理者の予測範囲を超えた、未知の攻撃を防げます。
- 教師データを用意するだけで、各々のウェブサイトに適した分類器を作成できます。
- 単に攻撃を防ぐだけではなく、悪性ウェブコードとそれ以外のコードを判別できます。

実用化の可能性

○ 想定される用途

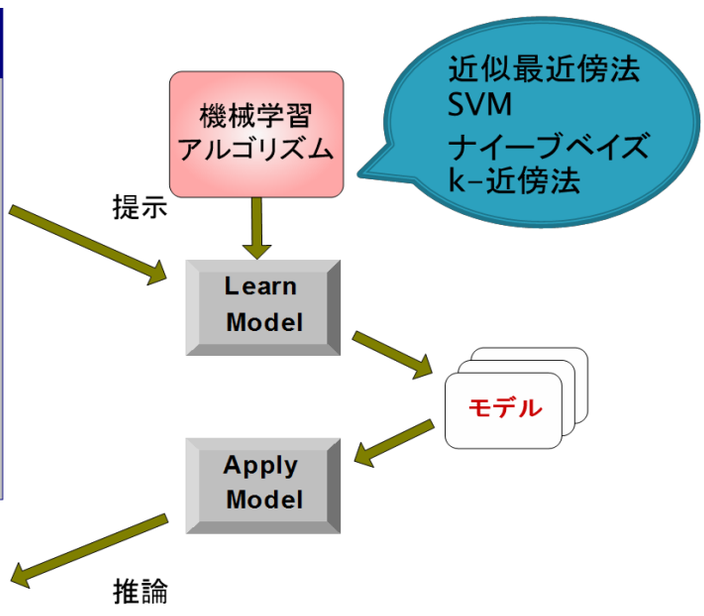
- ウェブ入力フォームを監視して、悪性ウェブコードを遮断するシステム
- ウェブブラウザに組み込むことで、ウェブページに埋め込まれた悪性コードを監視し、被害を未然に防ぐシステム
- ウェブアプリケーションサーバーに流れるパケットを監視して、悪性ウェブコードが含まれるデータを遮断するシステム

UBICからのメッセージ

○インターネットの世界では、さまざまな セキュリティの脅威にさらされています。 本技術が対象とする悪性ウェブコードによ る攻撃もその１つです。本技術は、機械学 習という手法を用いることにより、従来判 別が困難だった想定範囲外の攻撃パターン にも対応できます。ウェブシステムにおけ るセキュリティ強化の1手段として利用が 期待されます。

研究概要図

Tid	還付	婚姻状態	課税所得	不正
1	Yes	独身	125K	No
2	No	既婚	100K	No
3	No	独身	70K	No
4	Yes	既婚	120K	No
5	No	離婚済み	95K	Yes
6	No	既婚	60K	No
7	Yes	離婚済み	220K	No
8	No	独身	85K	Yes
9	No	既婚	75K	No
10	No	独身	90K	Yes

Tid	還付	婚姻状態	課税所得	不正
11	No	独身	55K	?
12	Yes	既婚	80K	?
13	Yes	離婚済み	110K	?
14	No	独身	95K	?
15	No	離婚済み	67K	?

テストデータ