2021 年 8 月 24 日

報道関係者各位
ニュースリリース

株式会社セキュアスカイ・テクノロジー
株式会社ビットフォレスト

クラウド型 WAF「Scutum」の異常検知性能が約 17%UP
～独自開発の『Thinning（シニング）』手法による攻撃検知率向上と誤検知低減～

株式会社セキュアスカイ・テクノロジー（東京都千代田区 代表取締役 大木 元 以下、SST）がサービス提供を、株式会社ビットフォレスト（東京都千代田区 代表取締役 高尾 都季一 以下、ビットフォレスト）が技術提供を行うクラウド型 WAF サービス「Scutum（スキュータム）」は、2021 年 8 月より、従来の「アノマリ検知機能」に新たに独自開発した『Thinning（シニング）』手法を追加することで、Web サイトへの攻撃に対する検知精度の大幅向上を実現したことを発表します。

Scutum では、「Web セキュリティ専門家によるリアルな判断に近い高度な攻撃検知能力を持ちながらも、正常通信の誤検知（*1）が極めて少ない。ユーザーが手放しで安心して利用できる WAF」をサービス開始以来一貫して目指し、これを実現するために 2 つの主要なデータサイエンス技術を活用してきました。

その１．「ベイジアンネットワーク」の導入

2013 年より AI の一分野である確率的グラフィカルモデルの一種「ベイジアンネットワーク」（*2）を導入。旧タイプのシグネチャ型 WAF では通常対応できないような、高度に形を変えた攻撃バリエーションについても幅広く検知することが可能となりました。また、新たな脆弱性や攻撃手法が確認された時点で既に検知が可能となっている「ゼロデイ防御」も多数実現しています（*3）。

その２．「アノマリ検知（＝異常検知）機能」の導入

2017 年には正常通信の中に含まれる異常な通信を検出する「アノマリ検知（＝異常検知）機能」（*4）を導入。機械学習によりあらかじめ把握したサイトごとの正常通信特性を元に異常アクセスを検出し、これを「ベイジアンネットワーク」と組み合わせることで誤検知の大幅軽減に成功しました。

● 新たな技術を導入 『Thinning（シニング）』手法とは？

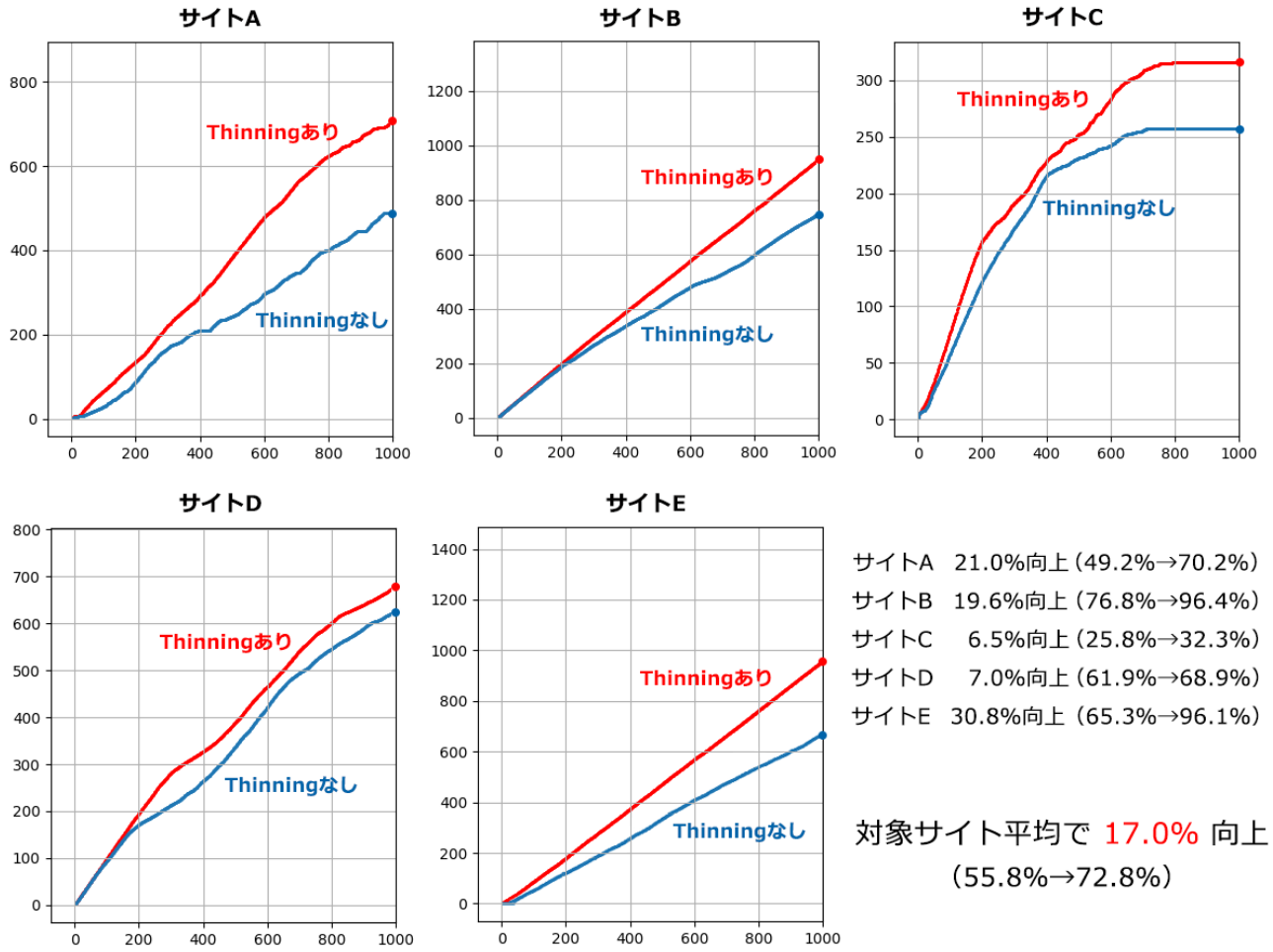
今回は、このうち「アノマリ検知機能」について、学習段階における Scutum 独自の選別手法である Thinning 手法を追加することで、大幅な攻撃検知精度の向上を確認することができました。

Thinning 手法は、Scutum が使用している「Isolation Forest」と呼ばれる異常検知アルゴリズムにおいて、ランダムに生成される個々の「木」（＝分類器）をあらかじめ余分に用意し、その中から導入 Web サイトごとの通信データを判定する上でより適した木々を事前に選別して残しておく方法です。学習時に本工程を挟むことにより、Scutum が Web サイトへの通信内容を評価する際にはより的確に通信の異常性を検出できるようになります。

●『Thinning』手法の検証結果

導入前の検証として、Scutum 導入サイトから 5 サイトを無作為に選択し、各サイトの直近 800 万件の通信について Thinning 手法「あり」「なし」それぞれで抽出した異常度の高い 1000 件のうち最終的に攻撃と判定された通信の割合を比較した結果、下図の通り Thinning 手法「あり」では「なし」と比べて、アノマリ検知機能単体での攻撃検出率が平均で 55.8%から 72.8%へと、約 17%の大幅向上を示しました。

【図】アノマリ検知機能「単体」での攻撃検出率比較テスト（2021 年 7 月実施）



横軸：アノマリ検知機能で異常度が高いと判定された上位件数（比較には上位1000件での検知率を使用）
縦軸：そのうち、実際に攻撃であった通信の件数

●『Thinning』手法の効果

Thinning 手法を用いて精度が向上した異常性の評価は、「ベイジアンネットワーク」による汎用的な攻撃検知や他の検知ロジックと組み合わせて総合的な判定に用いられます。今回の性能向上により、正常通信と見分けがつきにくい高度な攻撃や、攻撃と判断されやすい変則的な正常通信など、判定の難しい通信についても検知精度が大幅に向上し、Scutum の検知ロジック全体の誤検知をさらに減少させることが可能となりました。

本手法は、大量の正常データと少量の異常データによって構成されるという Web サイトの通信傾向との相性が良く、また、学習時には CPU 時間やメモリ等のリソースがより必要となるものの、評価時の処理速度は変わらないため、Web 通信をリアルタイムで大量かつ高速に処理する必要のあるクラウド型 WAF に非常にマッチした手法といえます。

本手法を追加した WAF エンジンは、2021 年 8 月 1 日より導入を開始し、現在までにすべての Scutum ご利用環境への適用を完了しています。

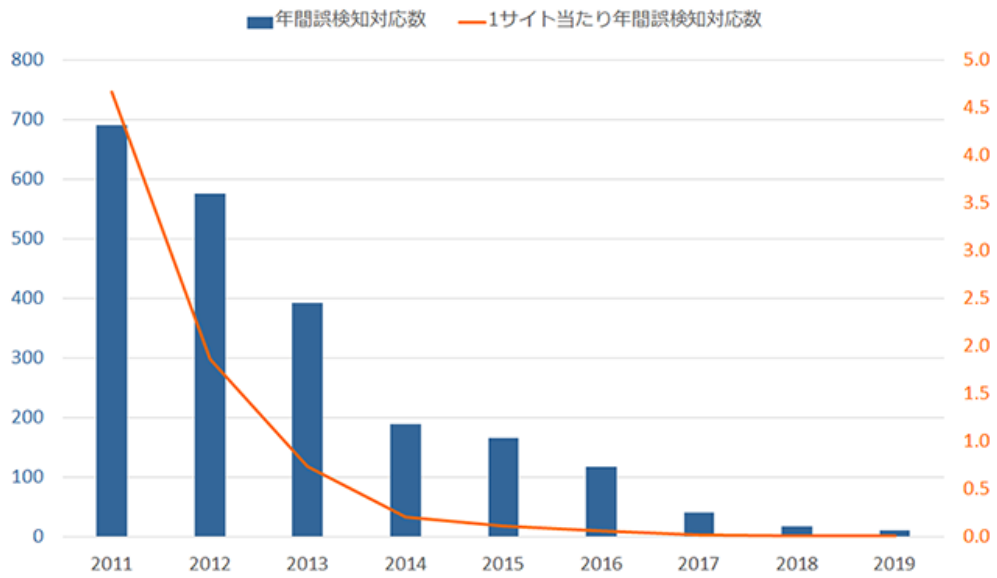
Scutum では、今後もより高い検知精度を目指して積極的にデータサイエンス分野の技術を研究・投入し、引き続きクラウド型 WAF の国内トップブランド（*5）として Web サイトの安全性向上に寄与してまいります。

※Scutum の実通信データを用いた上記検証結果のほか、AI 分野の検証用データとして著名な Kaggle のクレジットカード詐欺に関する公開データを用いた検証でも Thinning 手法による異常検知精度の向上が確認されています。この検証結果および Thinning 手法、「Isolation Forest」に関する詳細は Scutum サイト内の下記ブログ記事にて解説しています。

【Scutum 技術ブログ】Isolation Forest の性能を上げる Thinning 手法
https://www.scutum.jp/information/waf_tech_blog/2021/06/waf-blog-079.html
【Scutum 技術ブログ】Isolation Forest の Java による高速な実装をオープンソースで公開
https://www.scutum.jp/information/waf_tech_blog/2020/05/waf-blog-069.html

*1：本プレスリリース中で「誤検知」と表記した箇所は、正常通信を止めてしまう「偽陽性の誤検知」を意味します。

*2、*4：「ベイジアンネットワーク」「アノマリ検知機能」
これら 2 つの技術を組み合わせることにより、Scutum で誤検知対応が必要となった件数は、両技術導入前の 2011 年と比べて両術導入後の 2019 年には約 1/50 にまで大幅減少しています。



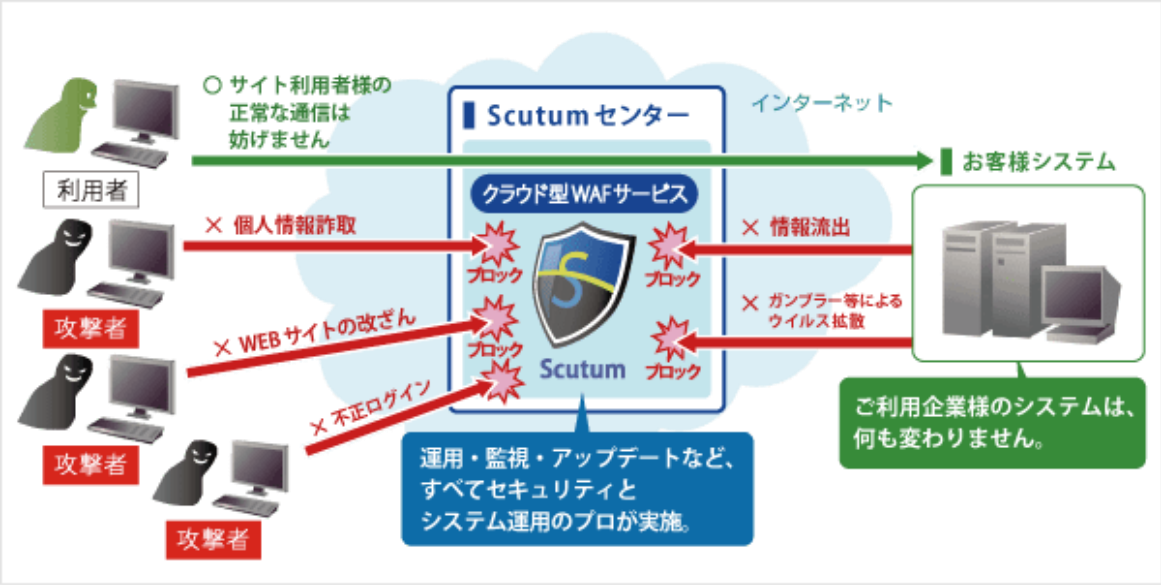
Scutum のデータサイエンス型 WAF エンジンの詳細については Scutum サイトの下記記事をご参照ください。
「AI 型 WAF エンジンの特長と効果」
https://www.scutum.jp/details/ai_waf.html

*3：Scutum の新脆弱性対応の詳細はこちら
https://www.scutum.jp/information/technical_articles/index.html

*5　クラウド型（SaaS 型）WAF 市場シェア 11 年連続 No.1 を獲得
https://www.scutum.jp/topics/waf_leader.html
ミック経済研究所刊『情報セキュリティマネージド型・クラウド型サービス市場の現状と展望 2021』　2020 年度
富士キメラ総研刊『2020 ネットワークセキュリティビジネス調査総覧』　2019 年度
株式会社アイ･ティ･アール刊『ITR Market View: サイバー・セキュリティ対策市場 2021』　2019 年度　ほか

● クラウド型 WAF サービス「Scutum（スキュータム）」について

インターネット上で「盾」となって、Web サイトを不正アクセス（攻撃）から守るセキュリティサービスです。お任せ運用・低コストでかつ余計な自前の設備を一切持つことなく、より安全な Web サービスの提供を実現します。



クラウド型 WAF サービス「Scutum（スキュータム）」：https://www.scutum.jp/

【株式会社セキュアスカイ・テクノロジー 会社概要】
社名　　：株式会社セキュアスカイ・テクノロジー
本社所在地　：東京都千代田区神田司町 2-8-1 PMO 神田司町 2F
設立　　：2006 年 3 月
代表者　　：代表取締役 大木 元
事業内容　：Web アプリケーションの脆弱性診断
　　クラウド型 WAF サービス、セキュリティ教育・支援サービス、コンサルティング
URL　　：https://www.securesky-tech.com/

【株式会社ビットフォレスト 会社概要】
社名　　：株式会社ビットフォレスト
本社所在地　：東京都千代田区神田錦町 1-17-5 神田橋 PR-EX 8F
設立　　：2002 年 2 月
代表者　　：代表取締役 高尾 都季一
事業内容　：Web アプリケーションセキュリティ製品の開発・販売
URL　　：https://www.bitforest.jp/

【お問い合わせ先】
株式会社セキュアスカイ・テクノロジー
広報担当　　：大倉 千代子（おおくら ちよこ）
E-mail　　：pr@securesky-tech.com
TEL　　：050-5445-8822