国立情報学研究所の学術情報ネットワークにおける大学・研究機関を対象とした NII-SOC に「DAMBALLA CSP」が採用

～2017 年 7 月 1 日より NII-SOC が本格稼働～

2017 年 6 月 29 日
株式会社アズジェント
（JASDAQ・コード番号 4288）

セキュリティ及び運用管理ソリューションの提供を主業務とする株式会社アズジェント（所在地：東京都中央区、代表取締役社長：杉本隆洋、JASDAQ：4288、以下、アズジェント）が、販売を行う Core Security SDI Corporation（所在地：米国、C.E.O David Earhart、以下、コアセキュリティ）の「DAMBALLA CSP」が、大学共同利用機関法人 情報・システム研究機構 国立情報学研究所（以下、ＮＩＩ）が構築・運用し、日本全国の大学、研究機関等が利用する学術情報ネットワーク「SINET」（Science Information NETwork）※1 のサイバー攻撃検知システムに採用され、7 月 1 日より本格稼働を開始します。

【背景】

近年、日本全国の大学、研究機関等を狙ったサイバー攻撃が多発しています。このような状況に加え、昨年度のサイバーセキュリティ基本法の改正に伴い、国立大学法人、研究機関のさらなるセキュリティ強化とセキュリティ人材の育成を目的に、ＮＩＩが迅速にインシデント対応を行うための「大学間連携に基づく情報セキュリティの基盤構築」を検討し、SINET 上にサイバー攻撃を検知するシステムを導入することが決定しました。

サイバー攻撃検知システムを導入することにより、ＮＩＩセキュリティ運用連携サービス(NII-SOCS)は、大学等から発信される通信に不正なものがないかを監視するとともに、不正通信を検知した際には、該当する大学に通知を行い、通知のあった大学はネットワークを遮断するといった対策を迅速かつ高精度に、効率よく講じることが可能となります。

サイバー攻撃によってマルウェアに感染した端末が C&C サーバの通信を検知するためには、既知の C&C サーバのデータを持つとともに常にそのデータが更新されること、500 万台以上の機器の DNS クエリを監視する能力を有することなど様々な厳しい要件が求められていました。また、一方で限られたリソースで、増え続けるサイバー攻撃に対応するために効率よく標的型攻撃等によるマルウェア感染を特定する仕組みが必要となります。

【NII-SOCS 効率化の切り札】

「DAMBALLA CSP」は、SINET のように複数のネットワークを相互接続する環境に設置したセンサーが DNS トラフィックを監視し、脅威検知エンジンで分析することにより、C&C サーバとの通信を検知し、マルウェア感染端末を特定するマルウェア感染端末検知システムです。その最大の特徴は、膨大なデータを基にした機械学習にあります。「DAMBALLA CSP」のデータベースは、北米のインタネットトラフィックの 55%、モバイル DNS トラフィックの 43%、225 億件のパッシブ DNS レコードをもとにした機械学習による知見の上に成り立っており、そのデータベースは分単位で更新され続けています。このため DAMBALLA シリーズは、検知の精度が高く、過検知や誤検知が少ないため、海外においてもプロバイダや金融機関をはじめとする多くのグローバル企業において、SOC、PSOC の機械学習型支援ツールとして導入されています。

この学習機能が、前述の要件を満たすシステムとして評価され、「DAMBALLA CSP」が採用されました。

今回の「DAMBALLA CSP」の採用にあたり、ＮＩＩのサイバーセキュリティ研究開発センター長である高倉弘喜教授は以下のようにコメントしています。

「近年のサイバー攻撃において、攻撃者によるマルウェアの侵入を入口対策で完全に防ぎきることは非常に難しくなっています。このため、ネットワークが既に感染しているかもしれない可能性を考慮して対策にあたる必要があります。DAMBALLA CSP は、なんらかの方法で感染した端末による C&C サーバとの通信を検知するとともにマルウェア感染端末を特定することができるため、とても重要な役割を果たします。また機械学習を用いて自動で検知できる仕組みは、国内全体でセキュリティ人材が不足している現状に合致しています。

DAMBALLA CSP が各大学・研究機関が保持する重要な知的財産や個人情報の漏えい防止に寄与することを期待します。」

尚、アズジェントは、国内唯一のディストリビューターとして、コアセキュリティの DAMBALLA シリーズの提供を行うとともに、NII-SOCS と連携する各国公立大学や公共機関等に対して DAMBALLA シリーズを自動化された機械学習ソリューションとして提案していきます。

※1 SINET

Science Information NETwork。日本全国の大学、研究機関等の学術情報基盤として、ＮＩＩが構築、運用している情報通信ネットワーク。今回の監視は、国立大学と大学共同利用機関法人に対して実施される。

【アズジェント会社概要】

会社名：	株式会社アズジェント （Asgent, Inc.）
所在地：	〒104-0044 東京都中央区明石町 6-4
代表取締役社長：	杉本 隆洋 （すぎもと たかひろ）
TEL：	03-6853-7401（代表）
資本金：	7 億 7,111 万円
取引銀行：	みずほ銀行、三井住友銀行 他

【記事ご掲載の際の読者からのお問い合わせ先】

株式会社アズジェント
〒104-0044 東京都中央区明石町 6-4
TEL：03-6853-7402 FAX：03-6853-7412 E-mail：info@asgent.co.jp
http://www.asgent.co.jp/

【報道資料についてのお問い合わせ先】

株式会社アズジェント
広報担当：横田 TEL：03-6853-7417 E-mail：yokota@asgent.co.jp