DGX A100がセキュリティとペンテストに変革をもたらす

セキュリティイニシアティブ様

ペンテストに基づいて幅広いセキュリティの
アドバイスを行うセキュリティイニシアティブ。
超高速処理を可能にする「DGX A100」が、
企業とペンテスターを強力にサポートする。

デジタライゼーションの進展とともに、サイバー攻撃も高度化・巧妙化している昨今。企業のサイバーセキュリティのさらなる強化が叫ばれるなかで、金融機関などを中心に注目を集めていることの1つに「ペネトレーションテスト」がある。

ペネトレーションテストとは、悪意のある組織的なハッカーなどが実際に行う攻撃と同じ技術や手法を用いて会社のシステムやサーバーなどに攻撃を仕掛け、その会社の「システムに脆弱性がないか」あるいは「防御対策がしっかりしているか」などをチェックするテストである。また、ペネトレーションテストは“ペンテスト”と略されることから、ペンテストを担う技術者は「ペンテスター」と呼ばれる。

このペンテストをはじめ、脆弱性診断やインシデントレスポンス、デジタルフォレンジックなど、幅広いサイバーセキュリティを手掛けるのが、2015年に宮城県・仙台市で設立された「セキュリティイニシアティブ」だ。セキュリティイニシアティブ 代表取締役の小笠貴晴氏は、ペンテストの国際資格である「GIAC GWAPT認定」や「GIAC GPEN認定」をはじめ、ペネトレーションテスターの上級資格である「GIAC GXPN認定」、デジタルフォレンジック解析の国際資格である「GIAC GCFA認定」、インシデントハンドリングの国際資格である「GIAC GCIH認定」などを取得する日本屈指のペンテスター。金融やクラウド、放送、エネルギーなどのさまざまな分野で、企業のサイバーセキュリティをサポートしている。

「ペンテストにはさまざまな入口と最終目標があり、『どのような立場の人間がどのような攻撃を成立させるか』というシナリオを基づいてテストを行います。例えば、入口として意外と多いのが“内部犯行”です。銀行などであれば、パートの職員から経営者までいろいろな人がネットワークにアクセスしますが、『パートの人の低い権限で、経営層しか見られないようなデータにまでアクセスできるか』などを試します。

また、外部からの侵入であれば、メール経由でマルウェアを仕込んで侵入経路を作るやり方があります。このような場合は、同じようにまずはコンピュータに入った権限を利用し、そこから別の人の権限に次々と昇格させていきます。もちろん、口で言うのは簡単ですが、それを実現させるためにはさまざまな手法があり、自分の持っている引き出しからいろいろ手法を試しながら進めていくイメージです」（小笠氏）

依頼された企業のセキュリティ状況を調べるだけでなく、その企業のセキュリティ訓練や実際の攻撃に対する痕跡調査、あるいはリアルなハッキングを想定した模擬戦なども小笠氏は手掛けている。小笠氏によれば、企業には幅広い防御システムが入っているが、その防御システムがどんな攻撃に対して有効かなどを「完全に把握していないケースも少なくない」という。そのため、じつは「こういった攻撃に対して弱い」などの抜け道がないかまでしっかりチェックしているそうだ。

総当たりは非効率のため キーワード推測で負荷減

小笠氏のようなペンテスターにとって、システムの脆弱性やセキュリティの穴を「いかに早く見つけるか」は重要なポイント

セキュリティイニシアティブ 代表取締役 小笠貴晴氏

だ。なぜなら、悪意のある組織的なハッカーは1か月や2か月、あるいは半年以上かけてじっくり企業のシステムに侵入しても何の問題もないが、ペンテスターはその企業やシステムが抱える問題点を可能な限り早く示すことができなければ、その企業が攻撃されるリスクを減らすことができないからだ。そのような背景にあって、ペンテスターの大きな手助けとなるのが「GPUによるデータ解析」である。

例えば、ネットワーク内に1度侵入した後、システムのメモリー内などに暗号化されて残っているパスワードなどを取り出し、逆解析のような形でパスワードを取り出す手法として「パスワードクラック」というものがある。パスワードクラックは一般的にとても時間のかかる作業で、文字数や文字の種類が少なければ「1日で解けることもある」が、それなりに複雑になってくると「ひどいときは数年かかることもある」という。

例えば、アルファベット26文字を使った10桁のパスワードは約141兆のパターンがあるが、そこに数字や特殊文字まで含まれてくると、そのパターン数はさらに肥大化する。いくら昨今のデジタル技術が上がっているとはいえ、普通に考えればこれ

を総当たりで解析することは効率的ではない。そのため、実際にパスワードを解析する際には総当たりはせず、そのユーザーが使いそうなキーワードをある程度推測してから実行することで負荷を減らす。例えば「社名や西暦、生年月日などを組み合わせていきます」と小笠氏は説明する。

「感覚的には、あまり手間をかけなくても5%程度は引っかかってきます。だから数百人規模の企業であれば数人分のパスワードはそのやり方で入手できるでしょう。ただし、それはあくまでも一般人レベルでのパスワードの話。管理者レベルの人は長いパスワードを使っているため、そう簡単に解析できるものではありません」(小笠氏)

総当たりのパスワード解析を4時間で終了するDGX A100

そこで出番となるのが「GPU」である。パスワードクラックでのGPU利用はすでに一般的で、小笠氏自身も「2年ほど前から利用している」。そこで今回は、大文字小文字のアルファベットと数字、特殊文字を使った8桁のパスワードを、総当たりで解析するテストを実施。すべてのパターンを調べ終わるまでの「終了予測時間」を小笠氏に比較してもらった。

その結果、小笠氏が現在使っているPCのCPUのみでは「約1年」と表示されたのに対して、普段利用しているGPUを使用すると「約17日」と表示された。この時点でも、GPUで得られるアドバンテージの大きさが見て取れる。

これに加えて、NVIDIA A100を8基搭載するAIワークフローのためのユニバーサルシステム「NVIDIA DGX A100」を使って同じテストを試してみると、終了予測時間はわずか「約4時間」と表示された。この結果に対して小笠氏は「普段使いのGPUと比較して、DGX A100は圧倒的に速いと感じたので本当に驚いた。ここまで来れば、もうパスワードの候補を出す必要がないレベルかもしれません」と分析する。

さらに小笠氏は、「GPU搭載PCの場合、連続でGPUを使用すると発熱の影響で処理性能が落ちてしまいます。そのため、実際には17日で終わることはないでしょう」と指摘。DGX A100では発熱で処理性能が落ちるようなこともないため、そういった点を含めても「満足度はとても高い」と高評価だった。

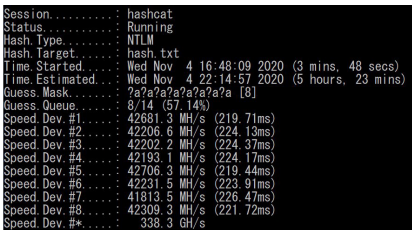
「ミッションクリティカルなシステムであればあるほど、高度なシステムを利用した攻撃を想定し、そのための対策を取る必要があります。仮に、悪意のある組織的なハッカーが高度なハードウェアを使えば、総当たりであってもわずか数時間でパスワードを抜き取られてしまうわけですから、我々ペンテスターとしては、それに応じた対応を取って企業をサポートしなければなりません。その意味では、驚異的なGPU性能を備えるDGX A100のようなハードウェアを使用することは、実態に即しているといえるでしょう。さらにいえば、そうすることが我々にとっても、顧客にとってもメリットになり得ます」(小笠氏)

サイバーセキュリティをリアルな経営課題に

セキュリティ分野では、パスワードクラック以外でのGPU活用も期待されている。例えば、ネットワーク上を流れるデータをAIで分析し、悪意のあるデータを見分けて対処するような試みも進んでいるそうだ。その際に、正規のデータをマルウェアと判断してブロックしたり、攻撃ではないのに攻撃と判断してその原因を調査したりすることになると無駄なコストがかかることから、「そのAI開発やディープラーニングによる最適化にGPUが活用されている」(小笠氏)。

一方で、小笠氏は現在「ペンテストをしても経営層に響かないケースもある」という課題を感じているそうだ。例えば、技術者と同じ言葉を使って経営者にリスクを説明しても、そのリスクを同じ感覚で捉えてくれないこともある。そこで小笠氏としては、技術者と経営者を上手く橋渡しし、「セキュリティの問題点を経営リスクに置き換えて理解してもらえるような伝え方、あるいは役割も求められているのではないか」と分析。その点も踏まえて今後は、これまで以上に「経営者が技術者としっかりと接点を持ち、リアルな経営課題としてサイバーセキュリティを重視してもらえるような動機づけを実現していく」考えだ。

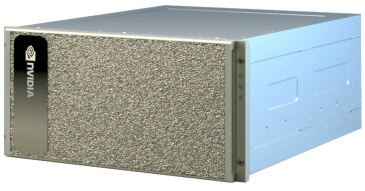
小笠氏が取得している資格の一部。上段左からSANS GIAC Certified Advanced Penetration Tester (GXPN)、SANS GIAC Certified Web Application Penetration Tester (GWAPT)、下段左からSANS GIAC Penetration Tester (GPEN)、SANS GIAC Certified Forensic Analyst(GCFA)


```
Session.........: hashcat
Status..........: Running
Hash.Type.......: NTLM
Hash.Target.....: hash.txt
Time.Started....: Wed Nov  4 16:48:09 2020 (3 mins, 48 secs)
Time.Estimated...: Wed Nov  4 22:14:57 2020 (5 hours, 23 mins)
Guess.Mask......: ?a?a?a?a?a?a?a?a [8]
Guess.Queue.....: 8/14 (57.14%)
Speed.Dev.#1....: 42681.3 MH/s (219.71ms)
Speed.Dev.#2....: 42206.6 MH/s (224.13ms)
Speed.Dev.#3....: 42202.2 MH/s (224.37ms)
Speed.Dev.#4....: 42193.1 MH/s (224.17ms)
Speed.Dev.#5....: 42706.3 MH/s (219.44ms)
Speed.Dev.#6....: 42231.5 MH/s (223.91ms)
Speed.Dev.#7....: 41813.5 MH/s (226.47ms)
Speed.Dev.#8....: 42309.3 MH/s (221.72ms)
Speed.Dev.#*....:   338.3 GH/s
```
ペンテストにDGX A100を使用した際の画面。Time Started と Time Estimatedの合計がトータル時間を示す。また、Speed #* が1秒間に計算されるハッシュ値の数(=総当たりのパスワードの数)となる

セキュリティイニシアティブの使用モデル

ジーデップ・アドバンス GDEPクラウド

ジーデップ・アドバンスが提供するクラウドサービスで、最新アーキテクチャAmpereを採用したTensorコアGPU「NVIDIA A100」を8基搭載するAIワークフローのためのユニバーサルシステム「DGX A100」などが利用可能。DGXシリーズを含めたさまざまなスペックのハイエンドサーバーを、専有クラウドもしくはオンデマンドで利用できる。



株式会社ジーデップ・アドバンス
〒105-0014　東京都港区芝1-12-7　芝一丁目ビル4階
TEL : 03-6803-0620　URL : http://www.gdep.co.jp/