2015 年 10 月 6 日
株式会社日立製作所

日立と HP がサイバー脅威に関するデータ共有の試行を開始

株式会社日立製作所(執行役社長兼 COO:東原 敏昭／以下、日立)は、このたび、Hewlett-Packard Company(本社:米国カリフォルニア州パロアルト市、President and CEO:Meg Whitman／以下、HP)との間で、情報システムなどに対する最新の脅威や攻撃手法など、サイバー脅威に関するデータ共有の試行を開始しました。これにより、日立はグローバルなサイバー脅威に関する最新状況の迅速な把握と従来以上に精度の高い分析を実現し、国内外の企業・団体が有するセキュリティ対策専門組織である CSIRT(*1)との情報共有やセキュリティ関連サービスの強化など、サイバー攻撃に対する対処能力の高度化に向けた取り組みを加速していきます。

近年、企業の情報システムのみならず重要な社会インフラもサイバー攻撃の対象となる可能性が高まりつつあり、その手法も複雑化・執拗化を続けています。こうした中、攻撃に対する適切な対処を行うため、より多くの情報を迅速に収集・分析し、攻撃の原因や攻撃者の特定につながる手がかりを見つけることが重要になっています。しかし、攻撃の具体的な手法や被害内容を把握できるのは、被害の当事者のみに限られており、一企業が収集できるデータには質・量ともに限界があります。そのため、サイバー攻撃に対する防御能力を高めることを目的として、情報セキュリティに携わる企業・団体間で効率的な情報共有の仕組みを確立することが社会的な課題になっています。

日立はこれまで、セキュリティ専門組織 HIRT(*2)を中心にサイバー攻撃の予防・対処を行ってきたほか、2013 年 10 月には研究開発グループに「HIRT ラボ」を設置し、企業・団体間におけるサイバー脅威に関するデータの共有に向けた取り組みを進めてきました。
一方、HP は、サイバー脅威に関する情報をリアルタイムに組織間で共有するためのプラットフォームである「HP Threat Central」を開発・活用し、さまざまな企業・団体とのデータ共有をグローバルに推進するなど、セキュリティ分野において先進的な取り組みを進めています。

こうした背景のもと、日立は HP との間でサイバー脅威情報の共有に関する契約を締結しました。具体的には、サイバー攻撃に関する最新の脅威や攻撃手法、対象など多様なデータを共有します(*3)。同時に日立は、共有したデータをセキュリティ対策の現場で活用していくための方法と技術面・実務面での課題に関する検討を進めていきます。なお、今回の情報共有は、サイバー脅威情報の共有に関する標準的な技術仕様である脅威情報構造化記述形式 STIX(*4)および検知指標情報自動交換手順 TAXII(*5)に基づき実施します。

今後、日立は今回の試行により得られた知見やデータ共有の枠組みを活用し、HIRTと国内外の企業・団体などが有する他のCSIRTとの情報共有を推進していきます。また、システム運用・監視サ

ービスやSHIELD SOC(*6)によるサイバー攻撃分析・対策サービスなど、セキュリティ関連サービスのさらなる高度化に向けた取り組みを加速し、重要な社会インフラをサイバー攻撃から守る社会的な責任を果たしていきます。

■Hewlett-Packard Company　Director, Threat Intelligence, Security Research
Ted Ross（テッド・ロス）のコメント

標的型攻撃が拡大を続ける中、サイバー脅威の増大は世界中の組織にとってセキュリティ上の最優先課題となっています。攻撃者に先んじてセキュリティに関する情報調査を高度化させるとともにサイバー脅威を迅速に隔離し、脅威の予測と最重要データの保護を行うため、情報共有は欠かせない活動です。

■株式会社日立製作所 情報・通信システム社 クラウドサービス事業部
セキュリティ先端技術本部長　瀬野尾 修二のコメント

日立は、今回の HP とのサイバー脅威に関するデータ共有を通じて獲得する知見を活用し、国内外の企業やセキュリティ関連団体が有する CSIRT とのデータ共有を推進していきます。これにより、サイバー攻撃の発見、予防、ならびに攻撃が発生した際の組織活動への影響を最小化する手法をさらに高度化し、社会的なサイバーセキュリティレベルの向上に貢献していきます。

*1 Computer Security Incident Response Team
*2 HIRT(Hitachi Incident Response Team):日立グループの CSIRT。日立グループの各部門に対して、脆弱性対策／インシデント対応情報を展開し、お客様のシステムを不正アクセスなどの危機事象から守るための対策を支援している。
*3 データの共有にあたっては、攻撃対象名などの属性が特定できないよう匿名化処理を実施する。
*4 STIX(Structured Threat Information eXpression(脅威情報構造化記述形式)):サイバー攻撃活動について記述するための XML 仕様。サイバー攻撃を特徴付ける事象(indicator)の特定やサイバー攻撃に関する情報共有などを目的として、米国政府向けの技術支援や研究開発を行う非営利団体 MITRE Corporation が中心となり仕様の策定が行われた。
*5 TAXII(Trusted Automated eXchange of Indicator Information(検知指標情報自動交換手順)):サイバー攻撃を特徴づける事象(Indicators)に関するデータを交換するための転送手順などを定めた仕様。米国国土安全保障省(DHS)が主導して、MITRE Corporation が中心となって仕様の策定が行われた。
*6 SHIELD SOC:株式会社日立システムズのセキュリティオペレーションセンター。

■Hitachi Incident Response Team の Web サイト
http://www.hitachi.co.jp/hirt/

■Hitachi SOCIAL INNOVATION FORUM 2015 -TOKYO-での紹介について

日立のサイバーセキュリティへの取り組みについて、日立が 2015 年 10 月 29 日(木)～30 日(金)に、東京国際フォーラムで開催する「Hitachi SOCIAL INNOVATION FORUM 2015 -TOKYO-」において、紹介します。
http://hsif2015tokyo.hitachi/

■商標注記

■本件に関するお問い合わせ先

株式会社日立製作所 情報・通信システム社
クラウドサービス事業部 セキュリティ先端技術本部 [担当:澤田、西川]
〒140-0013 東京都品川区南大井六丁目 26 番 3 号(大森ベルポート D 館)
お問い合わせフォーム:http://www.hitachi.co.jp/hirt/ask.html

以上