Nomura Research Institute Group

NEWS RELEASE

2020 年 3 月 17 日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、ダークウェブなどのサイバー空間から脅威情報を検出し、デジタル資産の保護を支援するサービスを提供開始

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、社長：小田島 潤、以下「NRI セキュア」）は、ダークウェブ[1]を含むサイバー空間から脅威情報を早期に検出し、企業のデジタル資産[2]の保護に向けて、情報セキュリティの専門家がリスク分析や助言を行う「マネージド脅威情報分析サービス（以下「本サービス」）」を、本日より提供します。

本格的なデジタル時代の到来とともに、企業のデジタル資産が飛躍的に増加しています。それに伴い、サイバー空間における脅威も増加しています。例えば、「自社サイトの ID・パスワードやソースコードなどの知財・機密情報が流出し、ダークウェブで取引されている」「自社を標的とした DDoS 攻撃[3]などの予兆が見られたり、自社関連サイトの脆弱性に関する情報が出回ったりしている」「自社を騙ったフィッシングサイトが作成されている」といった事態の発生に対して対応が遅れると、企業の事業継続に支障をきたす可能性があります。

一方で、多くの企業では、「サイバー空間で脅威となる情報の探索・検出に関するノウハウが不足している」「脅威情報の分析や対策実行を担当できる専門家がいない」「慢性的な人材不足から、情報セキュリティの専門家を社内で育成することが困難」といった課題を抱えています。

本サービスは、これらサイバー空間上のリスクを低減し、企業が抱える課題を解決するために開発されたマネージドセキュリティサービス[4]です。脅威情報の検出・分析をはじめ、重要度の高い脅威の抽出および本サービス導入企業の担当者への通知、定期レポートの提供、助言までを、NRI セキュアが一元的に担当します。当該企業におけるセキュリティ関連業務の一部を NRI セキュアが代行することで、人員不足や運用負荷の軽減を図り、多様化・複雑化するサイバー攻撃に対して、プロアクティブに対応することで被害を防ぐことが可能となります。

本サービスは、おもに以下の流れで実施します（図を参照）。

1. ダークウェブでやり取りされる情報を含む、広範囲かつ高精度な脅威の検出

本サービス利用開始時に、サービス導入企業の保有するデジタル資産について、ヒアリングを行います。この情報をもとに、NRI セキュアが、ダークウェブを含むインターネット上のあらゆるサイトでやり取りされる情報を監視します。監視にあたっては、AI（人工知能）を活用した解析機能を有する脅威インテリジェンス[5]製品を複数組み合わせることで、単一製品を用いた同様のサービスに比べて、より広範かつ高精度にサイバー空間上の脅威情報を検出できます。

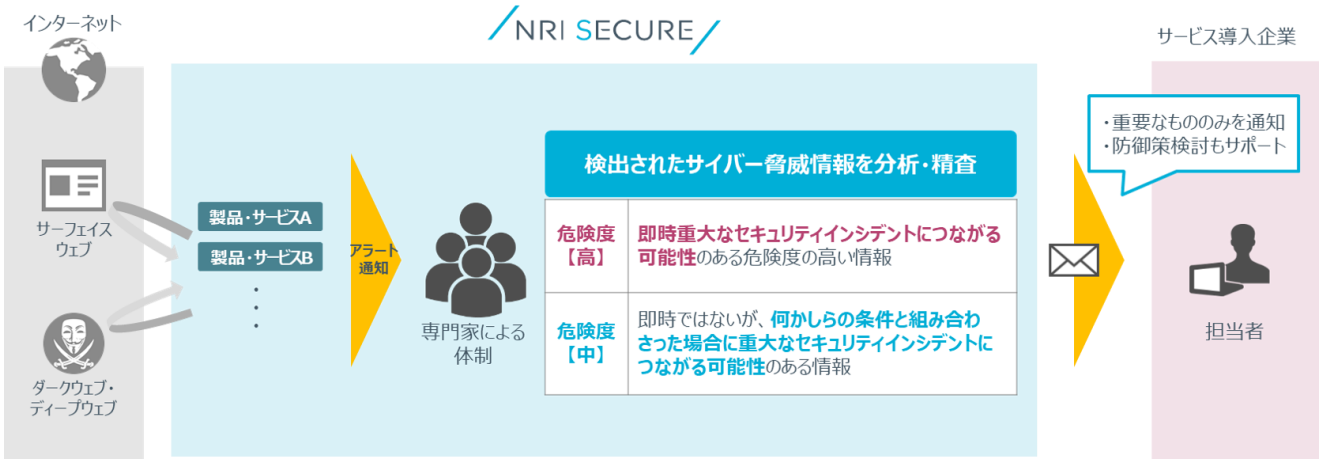
2. セキュリティ専門家が脅威情報を抽出し、緊急度や重要度を分析

最新のセキュリティ技術や脅威の動向に精通した NRI セキュアの専門家が、日々発生する膨大な脅威情報を抽出し、分析します。サービス導入企業の立場で、緊急性や重要度に応じた脅威情報のレベル分けを行います。

3. 緊急性の高い事象について、通知や助言を実施

重大なセキュリティインシデント（事件・事案）につながる可能性の高い場合に限り、サービス導入企業のセキュリティ担当者に通知し、対応策もあわせて提示します。また、定期的なレポートのなかで、過去に抽出した脅威情報を集計し、傾向分析や推奨対応策の方針などを報告[6]します。

図：NRI セキュアの「マネージド脅威情報分析サービス」の全体像



本サービスの詳細については、下記の Web サイトをご参照ください。

https://www.nri-secure.co.jp/service/consulting/threat_intelligence

NRI セキュアは、今後も、企業・組織の情報セキュリティ対策を支援するさまざまな製品・サービスを提供し、グローバルな規模で安全な情報システム環境と社会の実現に貢献していきます。

---

[1] ダークウェブ：
世の中に存在する Web サイトのうち、一般的なインターネット利用ユーザが検索エンジンを利用してアクセスできる領域は「サーフェイスウェブ」と呼ばれ、実は全体の 4%に過ぎません。残りの 96%は「ディープウェブ」と呼ばれ、検索エンジンからはアクセスできない領域です。また「ダークウェブ」は、「ディープウェブ」のうちの 6%を占めている

とされ、特別なソフトウェアがないとアクセスができない領域を指します。そこでは、漏洩した個人情報・カード情報等、違法な情報が多くやりとりされています。

[2] デジタル資産：
企業が保有するドメイン名、IP アドレス、Web サイト、SNS アカウント、クレジットカード情報等を指します。具体例は、［ご参考］の表をご参照ください。

[3] DDoS（Distributed Denial of Service）攻撃：
DoS 攻撃は、システムのサービス継続を妨害する攻撃を指します。そのうち、攻撃元を分散させて防御を困難にした攻撃を、DDoS（分散型 DoS）攻撃と呼びます。

[4] マネージドセキュリティサービス：
セキュリティ関連システムについて、導入だけでなく、導入後の運用管理までを一括して提供するアウトソーシング形式のサービスを指します。

[5] 脅威インテリジェンス：
攻撃者の意図や能力、設備などに関する情報を整理および分析することで有益な知識を導き出し、脅威の防止や検知に使用できるように変えた情報を指します。詳しくは、次の Web サイトをご参照ください。「脅威インテリジェンスを活用するための 3 つのポイント」（Secure SketCH ブログ）https://www.secure-sketch.com/blog/points-of-threat-intelligence

[6] 推奨対応策の方針などを報告：
パスワード変更など、推奨対応策の助言以外にも、たとえばフィッシングサイトなどを発見した場合、サービス導入企業が行う当該サイト閉鎖にかかる手続き（テイクダウン）を、NRI セキュアが支援することも可能です。

【ニュースリリースに関するお問い合わせ先】

NRI セキュアテクノロジーズ株式会社　広報担当

TEL：03-6706-0622　E-mail：info@nri-secure.co.jp

【ご参考】

■ 表：デジタル資産に関するヒアリング項目の例

No	デジタル資産名	概要	回答（例）
1	会社名	組織の正式名称、短縮名、子会社名	○○○株式会社
2	ドメイン名	会社が所有するパブリックドメイン	○○○.com
3	製品名・サービス名	会社が所有するブランド名、商標、製品名、サービス名など	○○○サービス
4	モバイルアプリケーション名	会社が提供するアプリが掲載されているアプリストアページのURL	https://xxxx.com/xxx
5	ソーシャルメディア公式ページ	会社の公式ソーシャルメディアアカウントページのURL	http://www.xxxx.com/○○○
6	グローバルIPアドレス	会社が所有する外部IPアドレスの範囲	100.100.100.0/24
7	ログインページ	会社が提供するサービスのログインページのURL	http://www.○○○.com/login
8	ソフトウェア名	会社で使用しているハードウェア・ソフトウェアの名称	xxxx (version 4.0.0)
9	機密文書の文字列	社外秘の文書に記載されている文字列	関係者限
10	機密プロジェクト名	公開前の社内技術や、プロジェクト名など	○○○プロジェクト
11	経営幹部などの氏名	経営幹部などの氏名	XX xxx
12	経営幹部などのメールアドレス	経営幹部などのEメールアドレス	xxx.XX@○○○.com
13	国・地域名	本社や支店がある国・地域名	日本
14	業種	会社が属する業種	○○業
15	BINコード	BINコード(銀行識別番号)　※保有する場合のみ	000000
16	ABAナンバー	ABAナンバー（米国における銀行口座番号）　※金融機関のみ	000000000
17	SWIFTコード	SWIFTコード（国際送金用識別コード）　※保有する場合のみ	XXXXYY0Z
18	公開コードリポジトリ	会社のGitHubの正規リポジトリ	https://www.github.com/account
19	APIキー、パスワード等の文字列	公開GitHubレポジトリのなかから、ここに指定した文字列を検索・検出いたします	apikey1234abcdefghij0123456789
20	医薬品名	医薬品の商標名、商品名　※製薬会社のみ	XXXX
21	特許医薬品名	特許製薬の名前　※製薬会社のみ	XXXX

※GitHub は、GitHub Inc.の商標または登録商標です。