2019 年 4 月 23 日
東京海上日動火災保険株式会社
NTT コミュニケーションズ株式会社

東京海上日動と NTT Com の協業による サプライチェーンへのサイバーセキュリティ対策における ソリューションのワンストップ提供について

東京海上日動火災保険株式会社（取締役社長：広瀬 伸一、以下 東京海上日動）と、NTT コミュニケーションズ株式会社（代表取締役社長：庄司 哲也、以下 NTT Com）は、拡大するお客さまのサイバーセキュリティ対策のニーズに対し、トータルにお応えするソリューションを共創するため、協業することに合意いたしました。両社が保有する保険や ICT サービスを融合させ、新たなワンストップセキュリティ対策ソリューション（以下 本ソリューション）を共創することで、安心・安全にデータ利活用ビジネスが展開できる環境づくりに貢献してまいります。両社は、2019 年 6 月の本ソリューション提供を目指し、検討を進めていきます。

なお、東京海上日動では、東京海上日動リスクコンサルティング株式会社（代表取締役社長：嶋倉 泰造）を通じてサイバーセキュリティ事業体制を強化し、本ソリューションを推進してまいります。

1. 背景・経緯

近年、クラウドや AI/IoT の活用は企業のビジネス革新に欠かせないものとなっており、それに伴い、企業が保有するデータも膨大なものとなっています。一方、そのデータを狙ったマルウェアや標的型攻撃などのサイバー攻撃は、巧妙かつ高度化しており、中でもサプライチェーン攻撃※に対しては、企業間の垣根を超えたセキュリティ対策が重要となっています。

東京海上日動は、これまでサイバーセキュリティリスク対策の保険商品を開発し、日本市場で展開してきましたが、保険販売を通じて、お客さまのリスク状況の把握やリスク軽減への取り組みが重要であることを確認しており、保険以外のソリューション提供を実現する体制構築が課題となっていました。

NTT Com は、お客さまが抱えるサイバーセキュリティリスクに対して、ICT インフラからアプリケーションにわたる範囲のソリューションを提供してきましたが、企業間のサプライチェーンの緊密化に伴い、一企業のみならず、その取引先である企業群のお客さまへのトータルな提供をさらに加速させる必要がありました。

「サイバーセキュリティが確保された安心・安全なデータ利活用環境を構築することで、日本のサイバーセキュリティリスクを軽減したい」という両社の方針が合致し、今回の協業にいたりました。

2. 本ソリューションの概要

お客さまのサイバーセキュリティリスクをトータルにマネジメントする統合的なサイバーリスク保険と ICT ソリューションを組み合わせることで、日本企業のサイバーセキュリティへの対策を強化するとともに、新たに生まれているビジネス分野への対応を継続的に進めてまいります。

（1） サプライチェーンに対するセキュリティ対策支援の提供

サプライチェーンで関連する企業群のセキュリティ対策状況を診断ツールにより評価し見える化するとともに、共助の精神にもとづき対策やノウハウを共有することで、対策期間や対策費用の低減、セキュリティレベルの底上げに貢献するソリューションの提供を目指します。

（2）ワンストップでのセキュリティ対策支援の提供

両社が持つサービスやソリューションを融合させることで、企業のセキュリティ対策における、セキュリティ診断、ポリシー策定・セキュリティ対策、オペレータや機器による検知・監視、インシデント発生時のサポートや本格対応、保険・再発防止対策にいたるまでのソリューションをワンストップで提供することを目指します。

（サイバーセキュリティ対策におけるソリューションイメージ）

（3）新たなビジネス分野におけるセキュリティ対策支援の提供

AI/IoT やコネクテッドカーなど、今後サイバーセキュリティリスクの拡大が予測される新たなビジネス分野にもセキュリティ対策の範囲を拡大し、お客さまの挑戦的な取り組みやイノベーションを、安心・安全面から支援することを目指します。

3. 今後について

東京海上日動では、海外セキュリティ事業者のソリューション活用や、東京海上日動リスクコンサルティング社におけるサイバーセキュリティ事業体制の強化により、本ソリューションを推進していきます。NTT Com は、最新のサイバーセキュリティに関するノウハウを継続的に蓄積し、本ソリューションに活用していきます。

また、将来的には日本企業の海外進出拠点や、海外に広がるサプライチェーンの関連企業についてもグローバルベースでの支援を可能にすべく検討を進めてまいります。

※：本リリースにおけるサプライチェーン攻撃とは、セキュリティ攻撃のターゲットとなる企業のグループ会社、業務委託先、発注先、仕入れ先などを攻撃し、それを足がかりにターゲット企業に侵入する方法を意味します。