２０１８年１１月７日

日 本 電 気 株 式 会 社
トレンドマイクロ株式会社
三井住友海上火災保険株式会社

～サイバー攻撃への対処とリスクの備えを包括的にサポート～

ＮＥＣ、トレンドマイクロ、三井住友海上 サイバー保険付帯の「仮想パッチによるサーバ脆弱性対策サービス」を開発

日本電気株式会社（社長 兼 ＣＥＯ：新野 隆、以下「ＮＥＣ」）およびトレンドマイクロ株式会社（社長 兼ＣＥＯ：エバ・チェン、以下「トレンドマイクロ」）と三井住友海上火災保険株式会社（社長：原 典之、以下「三井住友海上」）の３社は、サイバー保険付帯の「仮想パッチ(注１)によるサーバ脆弱性対策サービス」を共同開発しました。１２月１０日より、ＮＥＣから本サービスの提供を開始します。

新サービスは、ＮＥＣの信頼性の高いクラウド環境から提供する、トレンドマイクロの総合サーバセキュリティ対策製品「Trend Micro Deep Security」を活用した、仮想パッチによるサーバ脆弱性対策サービスに、三井住友海上のサイバー保険を付帯しています。サービス利用者は、早期に強固なサーバ脆弱性対策を導入でき、万一被害が発生した場合も保険が付帯されているため、調査や被害にかかるコストの軽減を図ることができます。これにより、システムの脆弱性を突いたサイバー攻撃への対処とリスクの備えを包括的にサポートします。

ＮＥＣ、トレンドマイクロ、三井住友海上は、本サービスを通じて、高度化・巧妙化するサイバーリスクの低減を図るとともに、今後も連携を強化して安全・安心で豊かな社会の実現に貢献していきます。

（注１）ＯＳやアプリケーションの不具合を修正するセキュリティパッチを早急に適用することが難しい環境に暫定的なセキュリティを担保するソリューションです。

【本サービスの概要】

（１）仮想パッチによるサーバ脆弱性対策サービス

サーバの通信パケットを監視し、脆弱性を狙った攻撃を検知した場合、その通信をブロックする仮想パッチを提供することで、サイバー攻撃を未然に防ぎます。ＯＳやアプリケーションに影響を与えないため、システムを停止することなく随時仮想パッチを適用することが可能です。

また、トレンドマイクロが提供する仮想パッチは、同社が保有する最新の脅威情報と連携し、１００種類を超えるＯＳやミドルウエア等の脆弱性に対応しています。オンプレミスの仮想環境やクラウド上のシステム等、さまざまなサーバ環境に対しても、サーバ１台から適用可能です。

また、ＮＥＣが管理サーバをクラウドサービスとして提供するため、管理サーバの構築やメンテナンスの必要はなく、簡単に導入・管理することが可能です。

（２）付帯されるサイバー保険

サイバー保険は、万一サイバー被害が発生した場合に、フォレンジック解析(注２)等の各種費用や賠償金を補償します。補償金額は、仮想パッチが適用された１サーバ・１事故あたり、フォレンジック解析が３００万円、賠償金は６００万円までとなります。

なお、取扱保険代理店はＮＥＣファシリティーズ株式会社、引受保険会社は三井住友海上です。

（注２）不正アクセスや機密情報漏洩等のコンピュータに関するインシデントが発生した際に、原因究明に必要な機器やデータ、電子的記録を収集・分析し、被害状況の解明や法的な証拠性を明らかにする手段や技術の総称です。

サービスの利用価格・提供開始時期

サービス名	利用価格（税別） ※１サーバあたり	提供開始時期
サーバ脆弱性対策サービス 仮想パッチ	年間 180,000円	2018年12月10日
サーバ脆弱性対策サービス 仮想パッチ＆アンチウィルス	年間 234,000円	2018年12月10日

※サービスには「Trend Micro Deep Security」の利用料も含まれます。

販売目標：今後３年間で５億円

ＮＥＣは、本サービスを、ＮＥＣグループが開催する「Ｃ＆Ｃユーザーフォーラム＆ｉＥＸＰＯ２０１８」(会期：11月8日（木）～11月9日（金）、会場：東京国際フォーラム)にて展示します。
「Ｃ＆Ｃユーザーフォーラム＆ｉＥＸＰＯ２０１８」：https://uf-iexpo.nec/

【開発の背景】

昨今、企業や官公庁等で業務のデジタル化が進む中、サイバー攻撃による被害は深刻化しています。独立行政法人 情報処理推進機構（ＩＰＡ）の調査によると、サイバー攻撃の手法として、「脆弱性（セキュリティパッチの未適用）を突かれたことによる不正アクセス」をあげる割合が５０％（注３）を超えており、脆弱性対策の確実な実施が事業継続の観点で重要になります。一方、業務停止が許されないシステムや旧ＯＳを継続利用しているなど、タイムリーなセキュリティパッチの適用が困難なシステムも多く、仮想パッチによる迅速な応急処置や、万一被害が発生した際の原因究明や被害拡大防止等のリスク低減対策が、ますます重要になっています。こうした中、セキュアなシステム構築と脆弱性管理の豊富な実績とノウハウを持つＮＥＣと、世界で報告される全脆弱性のうちおよそ半数を発見する脆弱性発見コミュニティZero Day Initiative（ZDI）（注４）の運営を通じて、いち早く脆弱性を検知可能なトレンドマイクロ、サイバーリスクを補償する保険において豊富な引受実績を有する三井住友海上の３社は、サイバー攻撃への対処とリスクへの備えを同時に解決するサービスを開発しました。

（注３）出典：独立行政法人 情報処理推進機構(IPA)「企業のCISOやCSIRTに関する実態調査 2017 －調査報告書－」
(2017年4月13日) P.59 (5)攻撃手法　図3.2-66攻撃手法（https://www.ipa.go.jp/files/000058850.pdf）

（注４）トレンドマイクロが運営する脆弱性発見コミュニティ「Zero Day Initiative（ZDI）」。
2005年に開始し、10年以上の歴史があります。世界で報告される全脆弱性のうち半数以上がZDIで発見されています(※)。
現在では世界約80カ国約3,000名のセキュリティ研究者が参加しており、インターネットの安全向上を図っています。
※2016年に報告された脆弱性1,262件のうち、663件（52.5%）がZDIによるものです。
出典：Frost & Sullivan. Analysis of the Global Public Vulnerability Research Market,2016.July 2017.

以　上