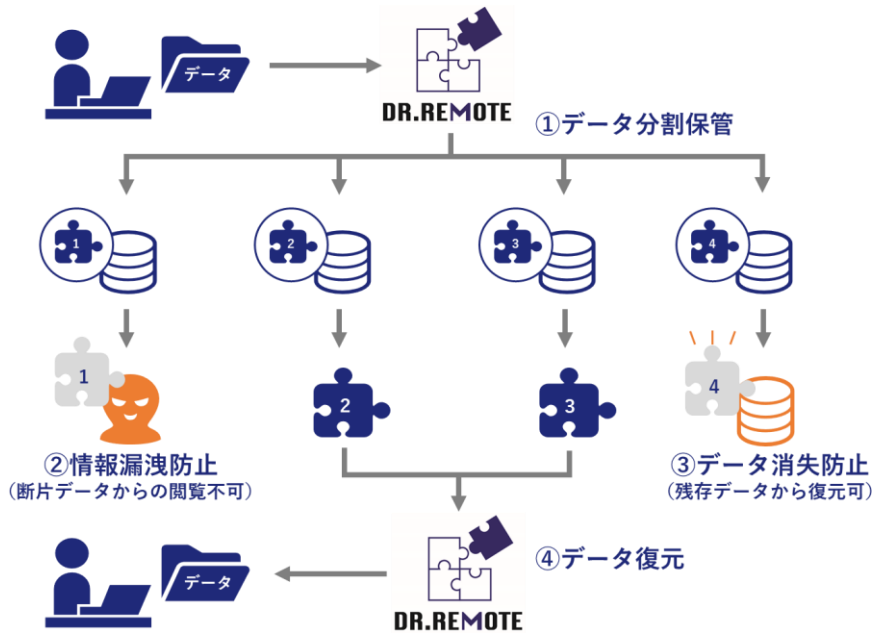
報道関係各位
プレスリリース

2月2日
株式会社Offisis

ゼロトラスト型セキュリティサービス「DR.REMOTE」提供開始
テレワークに最適なセキュリティを実現、情報漏洩やデータ消失等に対応
～独自の電子割符技術により、理想的なテレワーク環境を創出～

働き方改革を推進する企業に対し、オフィスに関わるサービスを提供している株式会社Offisis（オフィシス、本社：東京都豊島区、代表取締役：田野宏一、以下「当社」）は、この度、テレワーク推進企業へ向けて、理想的なテレワーク環境を創出するための新しいセキュリティサービス「DR.REMOTE（ドクターリモート）」の提供を開始します。

「DR.REMOTE」は、サイバーセキュリティ強化のために政府も導入検討をしているゼロトラスト型セキュリティを実現することが可能なセキュリティサービスです。



▲「DR.REMOTE」利用イメージ

■サービス提供背景

①サイバー攻撃の増加によりセキュリティ対策の潮流が「侵入防止型」から「ゼロトラスト型」へ

2020年上半期の国内におけるマルウェア（ウイルスなど悪意があるソフトウェア）の検出数は、2019年上半期と比較して約50%増加し、また2020年1月から5月にかけての検出数は約1.8倍となるなど、日本国内の企業に対するサイバー攻撃が増加しています※1。

そのような中、現在求められているセキュリティ対策の潮流は従来の「侵入防止型」から「ゼロトラスト型」へと変化しています。ネットワーク外部からの不正アクセスを徹底的に防御する侵入防止型は、サイバー攻撃の巧妙化により十分な対応ができない状態になってきています。そこで登場したゼロトラスト型は、「どのようなデータに対しても不正アクセスは発生し得る」という前提に基づき、デバイス単位での監視を行うなど、侵入防止型に比べて対象範囲を細分化してセキュリティ対策を講じていくという考え方です。政府においても 2020 年 9 月、サイバーセキュリティ対策を強化するためにゼロトラスト型の導入検討を発表しました。

②本質的なゼロトラスト型セキュリティとは

ゼロトラスト型に基づくと、情報漏洩やデータ消失は発生しうるという前提で考える必要があり、そのためゼロトラスト型を突き詰めれば、「情報漏洩したりデータ消失したりしても問題ない状態」となっていることが求められると考えられます。すなわち、本質的なゼロトラスト型セキュリティとは、①情報漏洩、②データ消失、この２つのセキュリティリスクに焦点を絞った対抗策のことだと言えます。

データに対する現在の主要なセキュリティ対策には、「暗号化」と「電子割符化」の２つが存在しています。しかしながら、「暗号化」では、暗号鍵を解読された場合に元データを復元されてしまう可能性を否定できないため、情報漏洩リスクを払しょくできません。一方、「電子割符化」は、データを複数の断片（割符）に分割して保管し、分割された断片（割符）からは元データを復元することはできないという技術特性上※2、情報漏洩には対抗可能です。そのため、割符化データは流出したとしても情報漏洩に当たらないと判断されています※3。ただし、「電子割符化」は、分割された断片が１つでも欠けると元データを復元できなくなるため、データ消失に対して十分な対応ができません。

現在主流となっている「暗号化」「電子割符化」の２つのセキュリティ対策では「情報漏洩」及び「データ消失」への対応を同時に実現できないことから、より本質的なゼロトラスト型セキュリティが必要であると考えられます。

③GFI 電子割符®の活用

本質的なゼロトラスト型セキュリティを実現するため、情報漏洩とデータ消失に対抗可能なセキュリティ技術を探していた中、当社は、グローバルフレンドシップ株式会社（本社：東京都渋谷区、代表：保倉豊、以下 GFI 社）が開発した特許技術“GFI 電子割符®”にたどり着きました。GFI 電子割符®は、データを分割して保管するという通常の電子割符技術の特徴に加え、仮に断片（割符）１つが消失した場合でも消失していない残りの断片（割符）から元データを復元可能という独自性を兼ね備えており、本質的なゼロトラスト型セキュリティの条件を満たしている画期的な技術と言えます。

そこでこの度当社は、GFI 電子割符®という特許技術を活用し、情報漏洩やデータ消失に対抗可能な、本質的なゼロトラスト型セキュリティを実現できる新しいサービス「DR.REMOTE」の提供を開始します。テレワークという新しい働き方を導入する企業が今後もさらに増えることが予想される中、当社は「DR.REMOTE」をサービスを通じて、理想的なテレワーク環境の構築を目指してまいります。

■「DR.REMOTE」について

GFI 電子割符®という特許技術を活用したゼロトラスト型セキュリティサービスです。本技術は、GFI 社が持つセキュリティに関する国内外の取得済維持特許 15 案件以上の技術を組み合わせて構築されています。

■「DR.REMOTE」利用手順

① ご契約後、専用 URL より「DR.REMOTE」をダウンロード
② 「DR.REMOTE」を開き、初期設定で、割符化したいデータおよび、データのストレージ先を指定する。
③ データがすべて自動的に割符化され、指定のストレージに保存される。その後はファイルを開くためのエクスプローラーのように使用可能。
④ 閲覧時には割符化されたデータが自動的に復元されて閲覧可能。保存時や終了時には、再度データが自動的に割符化される。

■「DR.REMOTE」サービス概要

提供開始：3 月 1 日
機能：電子割符化によるデータ管理機能
料金体系：1 アカウントにつき月額 1,500 円（税別）
お問い合わせ先：磯田（info@dr-remote.jp）
URL：https://www.offisis.co.jp/aboutus/
動作環境：(OS) Windows7/8/10、(CPU) Pentium4 3.0GHz 以上

■電子割符技術開発者 保倉豊氏（GFI 社 代表取締役社長） コメント

この度弊社電子割符技術の実装された電子的情報資産管理に資するソフトウェアを、株式会社 Offisis 様が正式に自社商品として事業展開されることとなり、本当に嬉しく思います。テレワーク普及とサイバー攻撃激化の中で、厳格化と重罰化が加速する情報資産管理リスク最小化は経営課題です。本商品は簡便に利用できるため、個人事業主様から IT 部門の無い組織様も含め、沢山の方々に貢献が可能です。旧来型のセキュリティ対策からゼロトラスト型への移行が叫ばれる今、GFI 電子割符®を活用し、ニューノーマル時代のセキュリティ対策を実現いただければと思います。

※1 出典：キャノンマーケティングジャパン株式会社「2020 年上半期マルウェアレポート」

※2

GFI 電子割符®の安全性に関する外部評価

≪2015 年 11 月 3 日 産業技術総合研究所 第二期結果概要報告より≫

・現時点では GFI 電子割符®の実用上の安全性を否定する材料は見つかっていない。

・例えば、攻撃者が割符ファイルの一つを入手した状態で元データを完全に復元できる可能性について評価を行ったところ、ある理論的な前提条件の下では、そのような可能性は現実的に全く問題とならないほど小さいことを確認した。

・「80 ビット安全性」では、暗号の解読がおよそ 10 の 24 乗通りの全数探索と同程度以上に困難であることを要求している。

・現時点での全数探索を前提とした安全性評価内容によれば、充分な情報理論的安全性を持っていると考えられるレベルである。

※3

≪2015 年 2 月 20 日 経済産業省確認より≫

GFI 電子割符®を用いて情報管理を行っていた場合、割符化データが流失したとしても、無価値化されたデータの漏洩に過ぎないため、情報漏洩に当たらないと判断されています。

セキュリティ対策の違いによるデータ盗難時の情報漏洩判断

	非暗号化データ	暗号化データ	割符化データ
情報漏洩に当たる	○	○	
情報漏洩に当たらない			○

■会社概要

株式会社 Offisis

代表者名：代表取締役 田野 宏一

所在地：東京都豊島区目白 3-13-20 DAIGO 304

設立年月：2016 年 4 月

事業内容：オフィスに向けた各種サービスの提供

ウェブサイト：https://www.offisis.co.jp/

【本件に関するお問い合わせ先】

株式会社 Offisis 広報・PR 担当 清田

（電話：070-8503-5493 E-mail：pr@offisis.co.jp）