＜プレスリリース＞

2018 年 10 月 29 日
株式会社イノベーション・ファーム

個人(機微)情報や重要情報は、漏えい・改ざん・破壊・消滅などの脅威に常にさらされています。今までの情報を守るという常識を 180 度覆す、利用者のリスクを無くし、使い勝手を保証した画期的なソリューション

秘密分散技術を活用した独自のセキュリティソリューションを開発・販売する株式会社イノベーション・ファーム（本社：東京都千代田区、代表取締役社長：山田 徳行、以下「イノベーション・ファーム」は、サイバー攻撃や人的要因等から「漏えい」・「改ざん」・「破壊」・「消滅」などの脅威さらされている個人(機微)情報や重要情報を今までの常識を覆し、利用者のリスクを無くし、更には利用すると言う負担を軽減した画期的な情報保護利活用ソリューション『Pro-Keeper2.0』の提供を開始致します。

【概要】

2016 年度に日本国内のネットワークに向けられたサイバー攻撃の件数は、前年比 2.4 倍の約 1,281 億件であった旨を国立研究開発法人「情報通信研究機構（NICT）」が過去最高を更新したことを発表した。

2018 年第 2 四半期に検知された攻撃は 9 億 6,295 万件。前四半期の 7 億 9,681 件から 20.9%増加した。悪意ある URL に関しても前四半期の 2 億 8,281 万件から 3 億 5,191 万件へと拡大し、前期比 24.4%となっている。2017 年 5 月には「WannaCry」が登場し、日本でも被害が発生。WannaCry の 2017 年間検出台数は、国内で約 1 万 8500 台、全世界で約 32 万 1800 台を記録しました。WannaCry による被害は、国内外でいまだ継続しており、“クローズドな環境だから安全”とは言えない状況へと変化しました。

また、トレンドマイクロが 2017 年に国内外で確認した新種ランサムウェアは 327 種類と、2015 年の 29 種類、2016 年の 247 種類から大幅に増加しました。こうした傾向は、サイバー犯罪の定番攻撃ツールとしてランサムウェアが定着し、同時に多様化しているためと考えられます。

破壊的な攻撃（身代金要求のためにデータを確保するのではなく、データを消去するような攻撃）は、2020 年の東京オリンピック/パラリンピックを控え、確実に増加することは間違いありません。

日本国内でもサイバー攻撃による被害はかなり出ている！今後確実に被害は増加して行くのでは？

【日本でも10秒に1人の割合でサイバー攻撃の被害者】

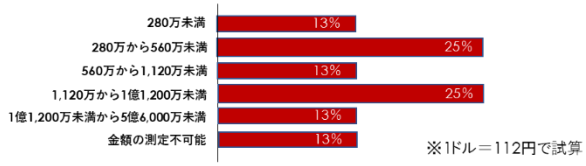
	年間被害者数	1日あたり	換算すると
世界では	3億7,800万人	100万人以上	毎秒12人の被害者
日本では	400万人	1万人以上	10秒に1人の被害者

【サイバー攻撃による被害額】

全世界	被害額	1,130億ドル	12兆6560億円
	1人あたりの平均被害額	298ドル	33,376円
日本	被害額	10億ドル	1120億円
	1人あたりの平均被害額	294ドル	**32,928円**

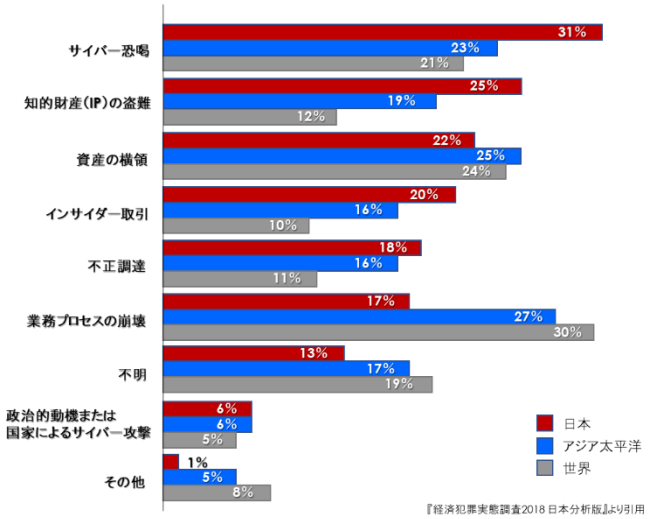
※1ドル＝112円で試算

【サイバー犯罪による被害額（日本）】



※1ドル＝112円で試算

【過去2年間（2016~2017）に企業や組織が受けたサイバー攻撃で狙われたもの】



『経済犯罪実態調査2018 日本分析版』より引用

2013 年のデータになりますが、日本でも 10 秒に 1 人がサイバー攻撃に会っており、1 人当たりの被害額も全世界と略同等の約 33,000 円規模となっている。過去 2 年間の統計ではサイバー恐喝や知的財産の盗難等はアジア諸国や世界と比較しても日本の方が多い。

何故、日本は世界やアジア諸国より多いのでしょうか？攻撃者側のスキルやノウハウが日々向上しているにもかかわらず、防御側は相変わらず 10 年も前の防御思想のままであり、情報技術は、まだまだ非常に早いスピードで進化しているのに、日本には独自のセキュリティに対する製品は殆どありませんし、セキュリティ対策はやるべきものであって、やらされていると言う意識が壁になっているのではないでしょうか？

サイバー攻撃によって仮に重要なデータ(個人情報をも含む)が消滅した場合、安全管理措置義務違反に問われる可能性がないとも決して言えない。

サイバー攻撃で情報漏えいが発生した際に負う法的責任とは、、、、？

（1）会社としては、漏えいした情報の本人から、損害賠償請求を受ける可能性。
1人1人に対する賠償金額は高くはありませんが、訴訟追行のコストが問題となります。

《1-1.漏えいした情報の本人からの責任追及：慰謝料の相場》

事件	原告の人数	原告1人あたりの賠償額（判決）	賠償額合計
京都府宇治市から住民基本台帳の情報が漏洩した事件 （最高裁平成14年7月11日）	3名	15,000円 （慰謝料=10,000円＋弁護士費用5,000円）	45,000円 （15,000円×3名分）
Yahoo!BBから個人情報が漏洩した事件 （大阪高裁平成19年6月21日判決）	5名	6,000円 （慰謝料=5,000円＋弁護士費用1,000円）	30,000円 （6,000円×5名分）
TBCからエステのコース名簿を含む個人情報が漏洩した事件 （東京高裁平成19年8月21日判決）	14名	35,000円 （慰謝料=30,000円＋弁護士費用5,000円）	490,000円 （35,000円×14名分）

《1-2.被害者の会による集団訴訟》

※2014年発生したベネッセの情報漏えい事件では、クラスアクション制度がない日本においては、多数の者を原告とする集団訴訟の定義は難しいと考えられて来ましたが、1万人が原告となり訴訟を提起したのです。

第1次訴訟：1,789名×55,000円＝総額98,395,000円
第2次訴訟：1,751名×55,000円＝総額96,305,000円
第3次訴訟：5,000名×55,000円＝総額275,000,000円
第4次訴訟：1,019名×55,000円＝総額56,045,000円
第5次訴訟：1,170名×55,000円＝総額64,350,000円
訴訟合計 10,729名 総額＝590,095,000円

（2）取締役などの役員等は、株主代表訴訟のリスクがあります。
賠償額は数百億円規模になる可能性があります。

《2-1.役員等が負う責任》

※ベネッセの事件では、約2,895万人分の個人情報が漏洩したとされています。漏えいした情報の本人に対して500円の金券を配る等した結果、260億円の特別損失を計上し、赤字転落しています。

《2-2.260億円の代表訴訟の衝撃》

※株主による約約2,895万人分の個人情報が漏洩をさせて260億円もの特別損失を計上してしまうような情報管理体制しか構築していなかった点に対して取締役が注意義務を怠っていたとして、260億円の代表訴訟を提起しました。（2015年12月）

（3）ITベンダーのように、個人データの取り扱いの委託を受けてサービスを提供している会社が個人データの漏えいをしてしまうと巨額の債務不履行責任を問われる可能性。

※ベネッセの事件と同様な事件が発生した場合、委託を受けて預かっている個人データを漏洩してしまえば、委託先から債務不履行責任を追及され、委託元が被った損害ということになりますので、同等額（＝260億円規模）の損額賠償責任を追及されることも十分に考えられます。

過去の判例から漏えいした場合には、本人から損害賠償請求を受ける可能性は十分にあり得る。
日本においてはクラスアクション制度がない日本においては、集団訴訟の定義は難しいと思われていましたが、ベネッセの事件では延べ 5 回に渡り、1 万人以上が原告になりました。

今回の事例が元になり、明日は我が身と言う事も十分起こり得ます。もはや対岸の火事と言う意識は今すぐ消し去るべきであり、この姿勢が大きなインシデントになり、取り返しのつかないアクシデントになります。

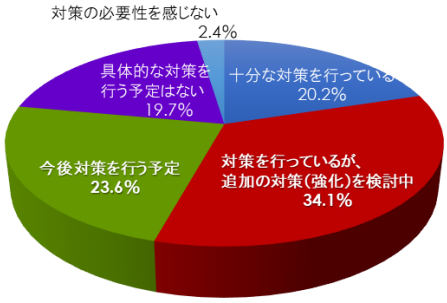
【 PC 内の資産を脅威から守る対策である Windows Update がデータを消してしまう！】

PC やシステムを乗っ取られ、こっそりと不正な動作をさせられたり、情報を盗まれたりする「脆弱性の修正」の対策である Windows Update がデータ(情報)を消滅させるアクシデントを引き起こしています。Windows10 の大型アップデート「October 2018 Update」直後に「一部ファイルが消失した」・「ドキュメントフォルダ内のファイルが勝手に削除された」といった苦情が相次いだ結果、アップデートの配信を一時停止したことを発表しました。今のところ問題のアップデートは、Windows Update 経由で自動配信されていませんので、国内市場では大きな問題になってはいませんが、大型アップデートが今後できないという事

を仮定するとマルウェア等の対策に関しても脆弱性を放置する事にも繋がりかねません。
　23 年分のファイル、220GB を全て消されたと言う事象も出ております。
しかし、今回のデータ消失に見舞われた人々によれば、そこには何も見つからなかったとか。ユーザー本人が事前にバックアップを取っておかないかぎり、消失したファイルの復元は困難と思われます。
修正版がいつ配信されるか日にちは明らかではありませんが、マイクロソフトは被害に会われた方々に保証をすると言った行為はしないと思われます。今更ながら改めてバックアップの重要性を感じますが、データは個人の物であるという事を再認識し、自ら守るという行為をすべきです。

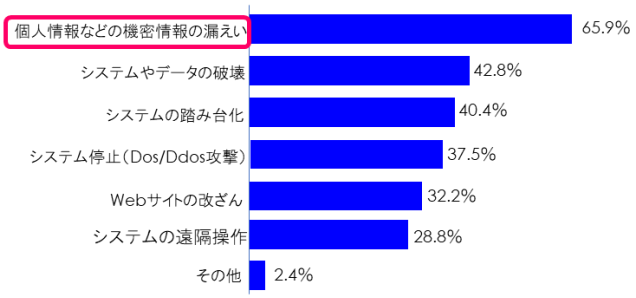
標的型攻撃で懸念する被害、現状のセキュリティ予算では十分な対策は無理では？

【図1：標的型攻撃対策の状況】



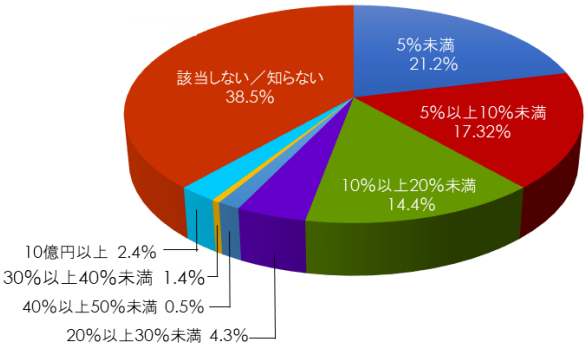
「対策を行っているが追加の対策（強化）を検討中」が34.1%。
「今後対策を行う予定」（23.6%）と合わせると57.7%が投資を予定

【図2：標的型攻撃で懸念する被害】



「個人情報などの機密情報の漏えい」が65.9%でトップ。
「システムやデータの破壊」（42.8%）、
「システムの踏み台化」（40.4%）が続く

【図3：年間IT予算に占める情報セキュリティ予算比率】



「20%未満」が52.9%と過半数であり、万が一の被害に対して予算枠は決して大きいとは言えない。
一般的にIT予算は売上の1%程度と言われており、2016年の平均値では、0.75%程度しかない。
仮に年間売上高10億の企業を例に取ると、
(売上)＝1000,000,000円×(IT予算平均値)＝0.75%⇒**7,500,000円**
2018年には全体的に平均で約9.7%増加しているので、
年間IT予算としては、7,500,000円×1.097＝**8,227,500円**
セキュリティ予算比＝20%とすると、
8,227,500円×20%＝1,645,500円しかない試算になる。
1億の会社だったら約17万円しか当てられない事になる。

標的型攻撃に対して追加の対策を検討中（34.1%）、今後対策を行う予定（23.6%）と合わせると 57.7%の半数以上が検討している結果が出ている。標的型攻撃で懸念する被害に関しては、「個人情報などの機密情報の漏えい」が 65.9%でトップであり、「システムやデータの破壊」が 42.8%の結果になっている。
危機感を持っている企業は増えている事は間違いありませんが、幾ら掛ければ良いのか？と言う答えは持っていないのでは無いでしょうか？一般的に企業の年間 IT 予算は売上の 1%程度と言われております。1%程度の内、セキュリティ予算の比率は 20%未満が 50%以上占めております。
仮に年間売上 10 億円の企業を例にとってみると、IT 予算が 1%になりますので、1,000 万円になります。その内、セキュリティ予算比率は 20%ですので、200 万円が年間の予算になります。
社員が 100 名いたら 1 人当たり@2 万円の換算になります。ネットワーク関係や周辺装置等も項目に入っていたとしたら更に 1 人当たりに掛けられるコストは少なくなります。
　セキュリティに対する考え方を対応(事件の状況に対応する方法と手段)から予防(想定される悪化に対して事前に備えておくこと)に変えて仕組みをべきと感じます。

【リスクに対する考え方を大きく変える】

結論から言えば、データを持たなければリスクは一切発生しない。文字コードに変換された文字データやビットマップや JPEG などの画像に変換されて画像データは記述されている内容や移っている対象物がハッキリわかる。しかし、文字コードに変換できない、云わば不完全なデータに変換してしまえば、リスクは必然的に消されるのではないでしょうか？

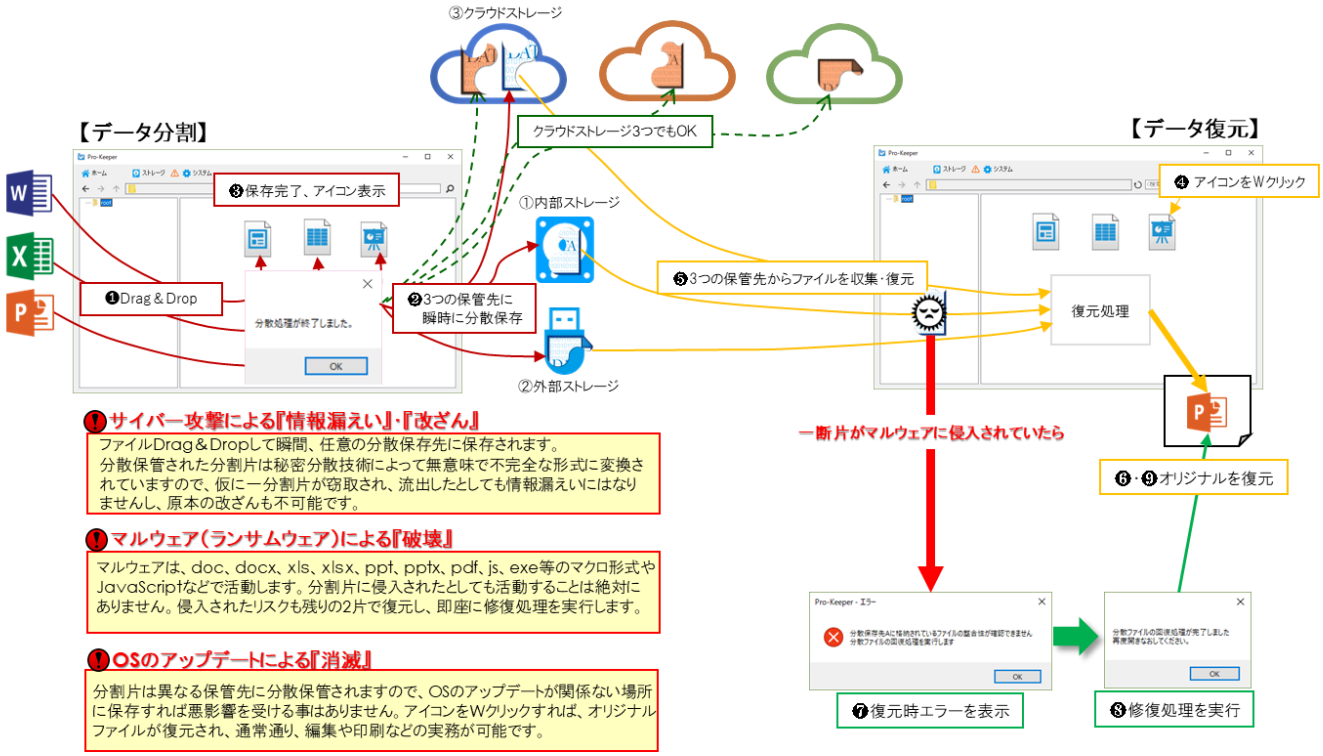
今回、リリース至ましたソリューション『Pro-Keeper』はデータを不完全な形態に変換してしまいますので、データを保持するという概念を無くしてしまいます。不完全で不安定なデータであるので、マルウェア等も動くことはありません。

【 Pro-Keeper Version2.2】

『Pro-Keeper Version2.2』 は、セキュリティを強化すると使い勝手が悪くなり、業務効率が低下することで、最終的には使われなくなり、セキュリティホールが大きくなる事に対して、日常の Windows エクスプローラと同じ操作で利便性を落とさず、重要な情報や機微の情報を秘密分散法によって不完全なデータに変換し、保存。データを利用する際のみ完全な形に変えるソリューションです。クラウドストレージを安全とコスト面からも効果的に活用可能な教職員の負担を大きく軽減させ、まさに『働き方改革』をサポートするランサムウェア(マルウェア)の脅威
からも情報漏えいインシデントを防止する画期的なセキュリティソリューションです。

操作性(エクスプローラの画面を再現)も簡単！重要なデータ(情報)を保護！

『Pro-Keeper』は、データをDrag＆Dropした時点で、不完全で無意味なデータに変え、無意味で価値の無い分割片を任意の保管場所に安全に分散保管します。
操作方法はWindowsエクスプローラと一緒です。アイコンをWクリックすれば、分散保管されている分割片を収集･復号し、オリジナルファイルを開封致します。
無意味化されたデータは、**マルウェア(ランサムウェア)に侵入されても絶対に活動することはありません。**



内部ストレージや USB メモリ等の外部ストレージに夫々保管されている分割片は不完全な物であり、単独では全く意味を成しません。クラウド保管に不安を頂いている企業も多く存在すると思います。
クラウドはハードの故障によるデータ消滅は絶対に防ぐ手法を取っておりますので、最も効果のある利用方法を導き出すことが可能です。
-Pro-Keeper 紹介サイト：http://www.innov-firm.co.jp/product_proKeeper.html

■ 株式会社イノベーション・ファーム：http://www.innov-firm.co.jp/index.html

働き方改革の ICT 活用とは、何時でも何処でも必要な情報が安全に活用できる事が大前提であり、モバイルコンピューティング・クラウドの活用がキーワードになります。しかし、データの持ち出しは情報漏えいのインシデントになる可能性を高くします。また、クラウドの活用に関して第三者へ情報を預ける事に対する不安を持つ企業は少なくありません。国内のクラウドベンダーと連携をして利用者にとって最もリスクが無く、安全に利用できる新たなる情報共有基盤を創り上げるソリューションを提供して参ります。

サイバー攻撃による情報漏えいや改ざん、マルウェア等の外的要因による破壊、そして予期せぬデータの消滅から重要なデータを予防と言う概念で守ります。

情報をあらゆる脅威から守り、利便性を兼ね備えた新たなるセキュリティソリューションを提供して参ります。

＜本件に関するお問い合わせ先＞

株式会社イノベーション・ファーム　　広報担当：山田

TEL：03-5823-4398　E-mail：inquiry@innov-firm.co.jp