

データ保護に関する法令や罰則の厳格化で サイバー攻撃の被害額が増加中!!

世界中でサイバー攻撃の被害額の増加が大きな問題になっている。はたして、その背景にはどのような原因があるのか。今号ではそのあたりのサイバーセキュリティ最前線を考察してみた。

サイバーセキュリティ対策費用と サイバー攻撃被害額の差が拡大

世界のサイバー攻撃被害額は5〜6兆^{ドル}規模（複数の調査機関のデータをもとに試算）と依然として増加傾向にある。しかし、その対策への投資額（サイバーセキュリティ市場規模）は1200〜1490億^{ドル}規模とかなり小規模だ。いったいなぜ、ここまで大きなギャップが生じているのだろうか。

その原因としてはいくつかの理由が考えられる。たとえば①サイバーセキュリティ対策は伝統的に「前例」の手法に対して後追いで検証されてきたものであり、あらたな手法に対して後手に回ってしまう②サイバー犯罪の件数が増加している③データ保護に関する法令や罰則が厳格化している、といったことなどだ。なかでも注目したいのが③だ。現にサイバー攻撃の被害に遭うと、原因究明、発表や公表に関連するコスト、情報漏えいなどの被害者への損害賠償、

再発防止に要する費用など、多岐にわたるコストが発生することになり、日本国内の場合、1件当たり2〜10億円のコストが発生するという（複数の調査結果から試算）。

また、最近では被害に遭った企業や組織が対策を怠ったとみなされる傾向が世界的に強まっており、その罰則が厳しくなっていることにも注目したい。たとえば、オーストラリアでは昨年、プライバシー法の修正が承認され、大規模なデータ被害に遭った企業およびデータ管理者に対する罰則の最高額が従来の222万豪^{ドル}から5000万豪^{ドル}へと大幅に引き上げられた。また、欧州で個人データなどの取り扱いを定めているGDPR（EU一般データ保護規則）に違反した場合の罰則の最高額は、当該企業の全世界の年間売上高の4割または2000万ユーロ（日本円で約26億円）のうち、高いほうが適用されるとのことなので、かなりシビアだ。しかも、それは対岸の火事ではなく、

昨年には日系企業の海外子会社にもこのGDPRが適用され、罰則が科せられている。米国でも厳しい罰則が科される規制が複数あり、日本もこれらの主要貿易国と足並みを揃える日がくるかもしれない。

**仮想パソコンやトークン化で
サイバーリスクを軽減**

こうした状況にあって、長年セキュリティ対策を手掛けてきた(株)ブロード（東京都千代田区）では、サイバーセキュリティの抜本的な対策につながるソリューションを提案している。その代表格が「HP Sure Click Enterprise（HP S C E）」（HP社）だ。このツールの特徴はメールなどの操作を行うパソコン上で「仮想パソコン」を立ち上げ、添付ファイルなどを隔離した状態で操作できること。そのため、マルウェアがどのような動作をしても、本体はまったく影響を受けず、確実に攻撃を防ぐことができるという。「サイバー攻撃の大半が電子メール

の添付データを起点としているが、HP S C Eを導入すれば、仮想パソコンによってそのリスクを完全に排除することができるとブロードは胸を張る。また同社では今、個人情報などの重要なデータが詐取されても問題にならないよう、データの状態を変える「トークン化」に特化したソリューションについても、独Comforite社との提携をすすめているという。このシステムを導入すれば、「仮にデータ漏えいが生じたとしても、その時点で『意味のないデータ』になっているので安心」とのこと。DXがすすみ、流出経路が広範かつ複雑になっている今日において、必携のシステムといえそうだ。

サイバー攻撃の被害額の増加は、企業にとって由々しき事態だ。そのリスクを軽減するためにも、つねにサイバーセキュリティ最前線に目を光らせてほしい。

再発防止に要する費用など、多岐にわたるコストが発生することになり、日本国内の場合、1件当たり2〜10億円のコストが発生するという（複数の調査結果から試算）。

また、最近では被害に遭った企業や組織が対策を怠ったとみなされる傾向が世界的に強まっており、その罰則が厳しくなっていることにも注目したい。たとえば、オーストラリアでは昨年、プライバシー法の修正が承認され、大規模なデータ被害に遭った企業およびデータ管理者に対する罰則の最高額が従来の222万豪^{ドル}から5000万豪^{ドル}へと大幅に引き上げられた。また、欧州で個人データなどの取り扱いを定めているGDPR（EU一般データ保護規則）に違反した場合の罰則の最高額は、当該企業の全世界の年間売上高の4割または2000万ユーロ（日本円で約26億円）のうち、高いほうが適用されるとのことなので、かなりシビアだ。しかも、それは対岸の火事ではなく、

昨年には日系企業の海外子会社にもこのGDPRが適用され、罰則が科せられている。米国でも厳しい罰則が科される規制が複数あり、日本もこれらの主要貿易国と足並みを揃える日がくるかもしれない。

**仮想パソコンやトークン化で
サイバーリスクを軽減**

こうした状況にあって、長年セキュリティ対策を手掛けてきた(株)ブロード（東京都千代田区）では、サイバーセキュリティの抜本的な対策につながるソリューションを提案している。その代表格が「HP Sure Click Enterprise（HP S C E）」（HP社）だ。このツールの特徴はメールなどの操作を行うパソコン上で「仮想パソコン」を立ち上げ、添付ファイルなどを隔離した状態で操作できること。そのため、マルウェアがどのような動作をしても、本体はまったく影響を受けず、確実に攻撃を防ぐことができるという。「サイバー攻撃の大半が電子メール

の添付データを起点としているが、HP S C Eを導入すれば、仮想パソコンによってそのリスクを完全に排除することができるとブロードは胸を張る。また同社では今、個人情報などの重要なデータが詐取されても問題にならないよう、データの状態を変える「トークン化」に特化したソリューションについても、独Comforite社との提携をすすめているという。このシステムを導入すれば、「仮にデータ漏えいが生じたとしても、その時点で『意味のないデータ』になっているので安心」とのこと。DXがすすみ、流出経路が広範かつ複雑になっている今日において、必携のシステムといえそうだ。

サイバー攻撃の被害額の増加は、企業にとって由々しき事態だ。そのリスクを軽減するためにも、つねにサイバーセキュリティ最前線に目を光らせてほしい。



今までの「常識」は、
すでに「非常識」!

もう無駄な時間と費用は「0」にしましょう

hp HP Sure Click Enterprise
powered by **Br Bromium**

エンドポイントのサイバー対策に関する費用や専門家は、もう必要ありません。
100%* 防御し、レポートします。是非ブロードにお問い合わせください。

*2013年以降、Bromiumは推計20億以上のMicroVMが実行されましたが、侵害報告件数はゼロです。(Bromium社調べ)
詳細は[BROAD Security Square]で… <https://bs-square.jp/columbus>

株式会社ブロード 〒100-0014 東京都千代田区永田町1-11-30 サウスビル永田町7F
TEL: 03-6205-7463 (代表)

