株式会社 ZenmuTech
代表取締役社長 /CEO
田口 善一氏

初代デジタル大臣、
自民党デジタル社会推進本部長、
自民党広報本部長
平井 卓也氏

DSA 代表理事 / 理事長、
株式会社インターフュージョン・
コンサルティング代表取締役会長
奥井 規晶氏

情報流出が社会問題となる今、経営者として取るべき対策とは?

- 経営者・IT 部門・エンドユーザー「三方良し」の国産セキュリティ -

日本古来の方式を現代に蘇らせた国産テクノロジー

奥井 現在、多くの企業はPCの紛失や盗難による情報漏洩をユーザー（社員）の責任として処分している現状がありますね。コーポレート・ガバナンスの観点から、それで本当によいのかという懸念があると思います。

田口 それは私も強く感じています。セキュリティのガバナンスは、本来、企業の責任であるはずです。それが懲戒処分というユーザーの責任になるガバナンスでは、「見ざる聞かざる言わざる」で経営の怠慢とも言えるのではないでしょうか?その考え方を検討する必要性とともに、セキュリティ対策自体も見直すべきです。具体的に言えば、データやアプリケーションを端末で使えるPC環境の見直しと、そのセキュリティが、個人が管理する暗号化で行われていることに私は警鐘を鳴らしています。

奥井 万一のPC盗難紛失時でも、情報漏洩を防げる「ZENMU Virtual Drive Enterprise Edition（ZEE）」を採用する企業・団体が増えてきていると聞いていますが。

田口 ZEEでは、「秘密分散」技術により、PC内のデータを複数の無意味な分散片に変換して、その一部をPC外に分散管理します。それら分散片の全てが揃わないとデータを元に戻せないようにすることで情報漏洩対策を講じています。暗号化では個々のユーザーが管理する鍵にリスクが集中する一方、秘密分散ではすべての分散片が揃わない限り元には戻らないため、ユーザーのスキルを問わず、リスク自体も分散されることになります（図表）。この実現にあたっては、自社開発した秘密分散技術を利用しています。

奥井 「秘密分散」は鎌倉時代に納税の際などに使われた「割符」と呼ばれる方式に通じるものであり、見方によっては日本古来の方式を現代に蘇らせた国産テクノロジーとも言えます。

平井 割符の話のように「分散させて一つでは意味を持たなくさせる」というアイデア自体は単純なことです。ただ、それを国産企業の高い技術によって実装できるところまで来た点が非常に意義の大きなことだと思います。

奥井 しかも、それが産官学の協力でできた「国産テクノロジー」ということで、スタートアップ企業と国立の研究機関が連携して新しい国産セキュリティ技術が生まれるのは珍しいケースではないでしょうか。

平井 産官学連携のプロジェクトはいくつもありますが、大手企業で採用・実装されるまでになることはじつはあまり多くありません。日本にとって非常に理想的な環境から生まれたセキュリティの仕組みだと思います。このような国産テクノロジーの仕組みが幅広く実装されることを期待しています。

田口 ありがとうございます。平井議員が推進された「デジタル・ニッポン2020」からはじまり、国立研究機関の産業技術総合研究所や情報通信研究機構のプロジェクトを通して技術を深化させ、その後は産業界で複数の大手企業と連携し、ようやくここまで来たという思いがあります。コロナ禍のパンデミックにより「日本のセキュリティ環境も変わらなければいけない」という意識が国全体に強く芽生え、根本的に見直しはじめたことが大きかったと思います。

奥井 コロナ禍には在宅勤務が増え、テレワークも大幅に増加しました。それでも大企業は以前と変わらずデータやアプリケーションを端末に持たせずに社内サーバーで管理する方法を使っていたわけですが、それがあまりにも遅く、ユーザー利便性、またその改善に向けてのコストの観点から限界が見え、個人のPCにデータを持つことに戻りつつあるという流れがあります。

田口 はい、個人のPCにデータやアプリケーションを持たせる方式への回帰となると、今度はセキュリティの問題が出てきます。そこでZEEを個人のPCへ実装することで、ユーザーはセキュリティを意識することなく使うことができます。個人のPCを紛失してもデータは無意味化されているので、被害のリスクはありません。個人が責任を問われることもなく、PCを安心して使える環境になったと自負しております。

平井 秘密分散はユーザー側に大きな負荷がかからず、「知らないうちに守られている」という意味でもいいですね。人は誰でも「パソコンを絶対に紛失してはいけない」と思うと、それだけで平常心ではいられないものです。万が一紛失したとしても最悪の事態は免れられるというのは心のどこかが安らぐもので、そのような機器でなければサステナブルな社会に実装できません。

エンドユーザーから支持されるセキュリティ製品

奥井 そこがまさに今回の大きなポイントで、これまでは「セキュリティ」と「利便性」はトレードオフでした。どちらかが良ければどちらかが悪いと。それを社は秘密分散という伝統的な手法を使って両方を実現し、「一石二鳥」のセキュリティを生み出しているんですね。

平井 私はさまざまなセキュリティのご提案をいただくのですが、スピードの問題や利便性などの懸念があるものは利用する現場では好まれないと実感しています。その点、ZenmuTech社の製品は「現場の人たちが好むセキュリティツール」と言えるんじゃないでしょうか。

田口 ありがとうございます。導入いただいた企業からは「セキュリティソフトで作業パフォーマンスが良くなり、生産性が上がった」と言っていただいています。

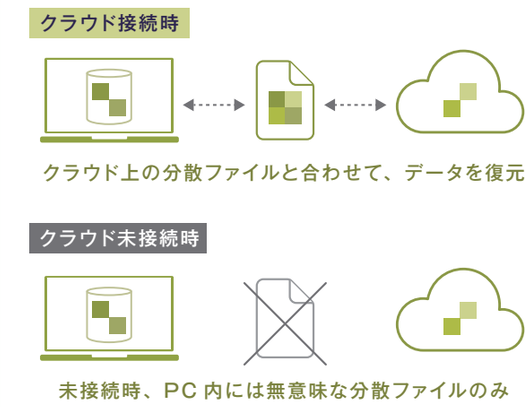
奥井 エンドユーザーから支持されるセキュリティ製品はこれまでにあったでしょうか?利用する企業からしてみると、経営の観点からもセキュリティポリシーにも合わせやすく、IT部門からすると管理は楽になり、ユーザーは意識せずに使える。これもまた珍しいことですね。

田口 はい。経営者にも、IT部門にも、エンドユーザーにも「三方良し」のセキュリティだと私は自信をもっています。

平井 数年前と比較して、最近はデータの重要性が非常に高まっています。それにはデータをどのように価値あるものにし、流通させるかという視点があると同時に、データ自身のセキュリティやデータ連携のセキュリティ、ストレージのセキュリティなど、安全面の課題も増えています。それに対して秘密分散によるセキュリティは重要な一手になるのではないでしょうか。

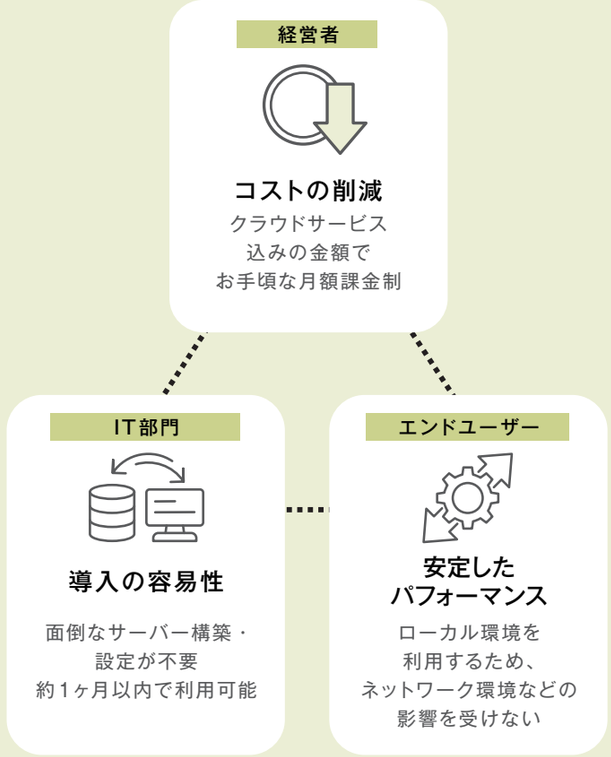
また、国産テクノロジーであるZenmuTech社には日本発のグローバルスタンダードになっていただきたいと思います。多くの日本のスタートアップがスケールしない理由は国内マーケットだけを相手にしているところが大きいですよね。せっかくの貴重な技術をおもちなので、ぜひグローバルを視野にビジネスモデルを組み立てていただきたいと思います。

秘密分散技術を使用した
ZENMU Virtual Drive Enterprise Edition (ZEE)



データを無意味化することで
ユーザーは利便性を損なわず、
無意識のうちに情報漏洩対策ができています

三方良しのセキュリティ



導入企業一例 ANA Security Diet LRM株式会社 三井倉庫ホールディングス PSC Deloitte デロイト トーマツ

広告

ZENMU TECH

株式会社 ZenmuTech
https://zenmutech.com/