SOLITAIRE INTERGLOBAL LTD

Navigating Thru Chaos

高信頼の対策

セキュアな柔軟性と応答性で実現する金融業務

「顧客の最大の懸念は、私たちとの取引がセキュリティ的に安全であるかどうかです。信頼に値する安全対策を十分に講じていることを示すことができなければ、顧客は離れていってしまい、当機関との取引を再度行ってくれることはないでしょう」

CEO、国際銀行機関、2018 年 2 月

安全性とセキュリティ。これは、企業や団体などの組織の間でデジタル市場について話題に上る第一の項目です。その中で、この項目を最も重視しているのは、インターネット経由でビジネスを行う商業金融グループです。金融商品・サービスを扱う組織は、データの脆弱性から顧客を保護していない場合、事業発展を可能とする金融基盤が全面的に漏洩してしまう危険にさらされることになります。

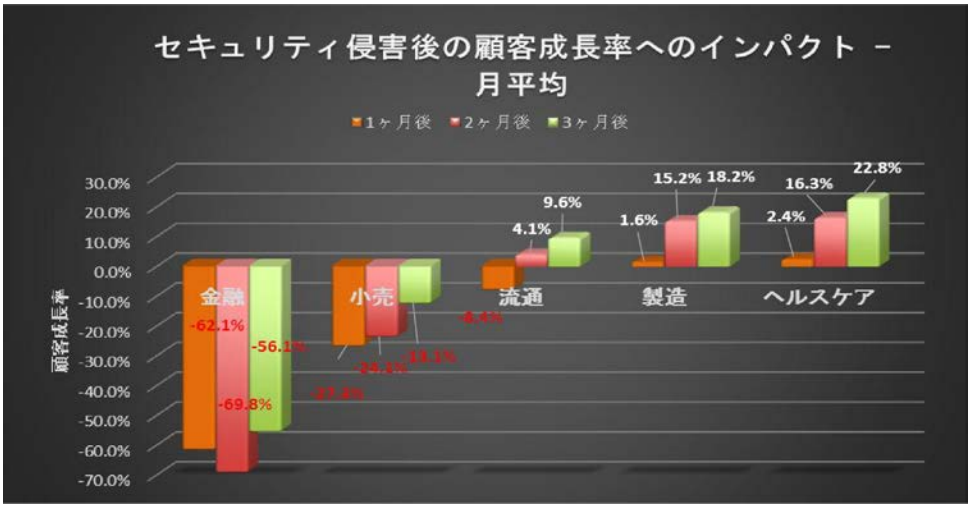
商業金融サービスを扱う組織は、健全な企業として成功し続けるために、顧客情報の保護能力を実証できることが不可欠です。

デジタル市場の基盤

デジタル市場で競争するうえで、敏捷性と柔軟性はもちろん重要ですが、とりわけ金融サービス分野においては、組織が行うあらゆるデータ処理がセキュリティ面で安全であることが極めて重要です。大規模な情報漏洩によって信頼が損なわれることは、どのような組織にとっても大きな痛手となります。

Solitaire Interglobal Ltd. (SIL) は最近の調査で、各種業界の企業・団体の顧客に対する影響について分析を実施しました。金融サービス提供の企業・団体で情報漏洩が起きた場合、他のどの分野にも増して顧客の拒否反応は強く、拒否反応の拡大も速く、はるかに影響を受けやすいのです。

ビジネスの遂行に使うことを目的に顧客から収集した情報がきちんと保護されているかについて、顧客は企業・団体を信頼できる必要があります。安全性とセキュリティへの信頼が失われると、他のどの要因よりも組織の評判は素早く失墜しまいます。買い手と売り手の間に存在する暗黙の契約に背く行為であると認識されてしまうのです。



180 South Western Avenue, #275
Carpentersville, IL 60110
Phone (847) 931-9100 Website www.sil-usa.com

金融機関への顧客の信頼レベルが情報漏洩の以前にまで回復するには、19.5ヶ月もかかります。調査報告された7.5ヶ月という平均期間でさえ、商業金融機関にとっては非常に大きな負荷です。

新規顧客の獲得が大きな割合を占める組織では、新たな顧客を 1 人獲得するためのコストが、情報漏洩の前と比べて平均 1.32 倍増にもなります。どのような市場拡大であれ、新規顧客が十分な安心感をもってビジネスに取り組めるよう、評判を再確立する対処を講じる必要があります。そのためには、これまでに明らかになっている脆弱性とセキュリティ障害を積極的に克服する必要があります。

成熟した金融機関からの報告によると、失った顧客を取り戻そうとするときのコストは、最大で事業取得の初期費用の 18.6 倍にもなります。金融機関が成熟（5 年以上の事業実績で、通常の年間顧客保持率が 80%超）していない場合は、単独で事業存続できる企業として生き残る可能性はわずか 34.2% です。

つまり、ハッキングが成功してしまうのは、ビジネスにとって著しく悪影響だということです。このことは、特に金融機関にいえることです。

また、金融機関が事業存続できるかどうかは、情報漏洩の件数やその対処方法からも強く影響を受けやすいです。中には、著しいセキュリティ侵害があった事実を隠そうとする企業もあります。影響を被った顧客の心情的な反応は、情報漏洩に対して企業がどれほど素早く、公正に対応したかに直接かかっています。

「サイバーに関する信頼は、金融サービスにとって極めて重要です。脅威に対し一貫してセキュリティを保つことが、企業の評判と顧客の信頼を確立するうえで重要な要素です」

Stéphane Nappo、IBFS グローバル情報セキュリティ主席責任 & 取締役会顧問、パリ、フランス

企業がいかに厳しい保護対策を構築しようとも、顧客情報のデータ整合性と保護が損なわれてしまうことはあり得ます。大半の顧客はそのことを理解しているため、必ずしもセキュリティ侵害が大きな問題となるわけではありません。しかし、情報漏洩が起きたときの断固たる対策と姿勢を組織が打ち出さない場合、顧客は信頼に背く行為だと感じ、信頼悪化の拡大につながります。問題を認めることは、組織が機械的な対応をしていないことを印象づける 1 つの方法ですが、あらゆるビジネスでこの解決策が適しているわけではありません。したがって、セキュリティとシステム侵害に対する組織の姿勢を決めておくことは、ビジネスの方針と手順を構成する重要な要素です。

素早く対応できる姿勢が整っていなければ、セキュリティ侵害の発生時に顧客の反応を緩和させることはできません。企業への信頼が裏切られたと感じる顧客が、その企業のビジネスに戻ってくる可能性は著しく低いです。17万5,000 以上の企業・団体を調査したところ、起きた事象が速やかに公表されなかった場合、78% 以上の顧客は情報漏洩後にその企業や団体を再び利用することを拒否しています。79% 以上の顧客は、情報漏洩のあった企業が、脆弱性をどのように改善し、生じた損害が何であれどのように修復したかについての正確な説明を期待しています。

また、インシデントを隠蔽しようとする行為については、回答を寄せた顧客のうち 95% 以上もが、そういった行為は個々の顧客に対する不誠実の現れだとみなしています。さらに、回答者 1 人からのコメントには、「私を 1 人の個人として見なしていない取引先とのビジネスを誰がしたいと思いますか？ 相手に対する尊重をもたない人と何か一緒にしたいと思いますか？」と記されていました。

企業の事業存続能力には、どれくらいの価値があると思いますか。また、現在の顧客の大部分を失った場合、最終的な収益はどうなると思いますか。これは、サイバーセキュリティへの手間や費用をも相殺してしまう現実的な課題です。顧客は企業への信頼がなければ、その企業との取引は行わないでしょう。

その結果、収益は短期間で低下し、その傾向は長期化します。また、すでにダメージを受けた事業への評判も、さらに悪化していきます。一連の対応策の中身によっては、信頼を失った顧客が戻ってくることはないかもしれません。戻ってくることがあるとすれば、信頼に値する組織であるという位置付けを再確立して顧客に納得してもらうために、サービス、設備、人件費への大幅な出費を実施してからとなるでしょう。

©Solitaire Interglobal Ltd.

金融業務向けの LINUXONE ソリューション

この種のリスクへの対応策の 1 つは、実証済みの高水準セキュリティを実現する基盤を構築することです。企業は、基盤となるプラットフォームを選択する際、直接的なコストだけでなく、*サイバービジネス*が提示する魅力的な条件はもちろんのこと、そのサイバービジネスがもたらすリスクや危険性も十分に検討する必要があります。

IBM LinuxONE は、変革を実現する基盤構築の際の重要なコンポーネントとなります。サイバースペースで日々実証されている課題に企業が迅速に対応できるようにするためのセキュリティ、耐障害性、パフォーマンスといった急激な発展を遂げている市場において、成功に求められる重要な分野に対応しています。

また、LinuxONE ソリューションは、目標コストに対しても好影響をもたらします。必要とする人員が少なくすみ、所有コストも大幅に削減できるため、支出を最小限に抑えることができて非常に有益です。このコスト面における差は顕著であり、総所有コスト (TCO) では*最大 80%*、*人員レベルでは 60%* 以上も削減できます。

LinuxONE ソリューションは、セキュリティの領域で最大の違いを発揮します。基礎的なサイバーセキュリティの取っ掛かりがより厳格化されていると、デジタルインベントリにとって必要なデータ保護にハッカーが侵入してくる可能性は、格段に低くなります。実際、LinuxONE を実装している場合、導入済みアプリケーション 1000 件ごとのセキュリティ攻撃の成功率は、他のアーキテクチャと比較して *0.01% 未満*であると報告されています。

評判を守るとともに、収益への影響を防ぐためのコストを低く抑えることが、組織の事業存続の成否を分ける可能性があるため、非常に重要です。侵害を防ぐためのセキュリティ保護があれば、顧客からの信頼をすぐに高められるため、結果として、収益の上昇と顧客ロイヤリティの向上がもたらされます。

変化の激しいサイバービジネスの世界では、各種金融業務の基礎的な制御を担う企業や団体への信頼は、繊細でいとも簡単に壊れやすいものです。顧客からの信頼を守ることは、スピードや柔軟性といった他の懸案事項よりも優先されることです。顧客を保護、保持できない企業がスピードを追い求めても、それは見当違いといえます。

SOLITAIRE INTERGLOBAL LTD.

Solitaire Interglobal Ltd. (SIL) は、40 年以上にわたって市場の進化と生産行動に関するデータを収集しています。SIL 社では年間 6,000 社以上のクライアントに対応し、同じく年間 1 億件以上の予測モデルを実行しています。また、こ れまで 22 年間にわたり、グローバルセキュリティ監視を実施しています。同社メンバーのサービスとして、非常に詳しく細分化された 550 PB を超えるデータのリポジトリが構築されています。このデータは、組織の成功に役立つ傾向、比較、しきい値について 1 時間ごとにマイニングされます。

帰属および免責事項

IBM、IBM LinuxONE、LinuxONE、IBM Z、および z Systems は、米国およびその他の国における International Business Machines Corporation の商標または登録商標です。

その他の会社名、製品名、およびサービス名は、それぞれの商標あるいはサービス記号である場合があります。

本書は、IBMがスポンサーとなり作成されたものです。本書は、IBM を含むさまざまなベンダーの公的に入手可能な資料を利用していますが、必ずしも本書で提示されている課題について当該ベンダーの見解を反映するものではありません。

42018942JPJA