



暗号化のROI(投資回収率)に対するガイド

チェック・ポイントのPointsecデータ・セキュリティは、デバイスの紛失による
情報漏洩のリスクを90%軽減します

Contents

本書の内容

| | |
|------------------|---|
| 概要 | 3 |
| 3情報漏洩の財務的なリスクの評価 | 4 |
| 代替品の再購入コスト | 4 |
| 復旧コスト | 4 |
| 影響コスト | 5 |
| 信用コスト | 6 |
| 暗号化の一般的なコストとROI | 6 |
| 総所有コスト(TCO) | 7 |
| 詳細について | 8 |

概要

暗号化は、コンピュータに保管されている情報や、コンピュータ間で転送される情報の機密性、一貫性、および可用性を保護するためのサイバー・セキュリティ技術です。チェック・ポイントが提供するPointsec暗号化ソリューションは、デジタル・ファイルを自動的に暗号化して、権限のないユーザーに読み取られないように保護します。一方、権限のあるユーザーに対しては、ファイルを自動的に復号化して、適切なアプリケーションで使用できるようにします。チェック・ポイントのPointsec暗号化ソリューションは、ユーザーに対して透過的に動作し、電気やガスのように不可欠なインフラストラクチャ・サービスを提供します。

今日の企業にとっては、暗号化の価値が非常に高まっています。コンピュータの黎明期には、組織がデジタル・リソースを厳重に管理していました。インターネットはまだ存在しておらず、デジタル・ファイルを組織の管理領域外にあるコンピュータに転送することはありませんでした。今日では、デジタル情報をどこにでも簡単に移動や転送を行えます。これまでのサイバー・セキュリティ対策のほとんどは、ハッカーや犯罪者がネットワークの境界やエンドポイントを利用して機密性の高いコンピュータ・リソースにアクセスするのを防ぐことに集中していました。しかし現在では、機密データが保管されているモバイル・デバイスを紛失するリスクも考慮する必要があります。

各種調査によると、情報漏洩の原因としては、デバイスの紛失や盗難がその60%近くを占めています。ノートPC、PDA、ポータブル・ミュージック・プレイヤー、フラッシュ・メモリ、外付けハード・ディスク、スマートフォンなどのモバイル・デバイスは、すべてデータの保存が可能であり、データ侵害や情報漏洩のきっかけになる可能性があります。これらのモバイル・デバイスの所有者を常に把握し、機密データの転送記録を常に管理することは不可能です。しかし、機密情報へのアクセスは、暗号化という形で常に制御できます。

チェック・ポイント・ソフトウェア・テクノロジーズが発行するこの技術白書では、暗号化の経済的な側面について説明します。暗号化を使用していない組織で情報紛失が発生した場合の財務的なリスクを算出し、暗号化によってそのような損失をいかに低減できるかについて説明します。Pointsec暗号化ソリューションを使用することで、デバイスの紛失や盗難による情報漏洩の年間コストを90%以上削減できます。

「暗号化のTCO(総所有コスト)に対するガイド」もご一読ください

チェック・ポイントでは、暗号化の経済的な側面に関する資料として「暗号化のTCO(総所有コスト)に対するガイド」も発行しています。この白書では、暗号化関連の業務イベント、それらのイベントが発生する頻度、およびそれらのイベントにかかる人件費に基づいて総所有コスト(TCO)を算出する分析モデルを提示しています。また、このモデルに基づき、Pointsec PCデータ暗号化製品と主な競合製品2つの3年間の総所有コストを比較しています。現実世界のデータによる検証では、2つの競合製品のライセンス料を除いた総所有コストと比べても、Pointsec PCデータ暗号化製品の総所有コストが著しく低いという結果になりました。

「暗号化は、データの機密性と一貫性を保護するうえで不可欠なツールです。」

ジョン・オルトシック

シニア・アナリスト

Enterprise Strategy Group, Inc.

情報漏洩の財務的なリスクの評価

企業情報が保管されているデバイスの紛失や盗難による潜在的なコストは、代替（再購入）、復旧、影響、および信用の4つに分類できます。例えば、コンピュータやソフトウェアの代替品の再購入のように分かりやすいコストもあります。しかし、その他のコストは、業界、関連法規、罰則規定など、競争市場の状況によって異なる可能性があります。以下では、これらの変数について解説し、暗号化を使用している場合と使用していない場合で、それらのコストがどのように違ってくるかについて説明します。各組織の事業運営に及ぼす影響に応じてこれらの変数を調整することで、情報紛失リスクの年間コストをより正確に算出できます。

代替品の再購入コスト

ここに分類されるのは、紛失または盗難の対象となったデバイスを物理的に代替するためのコストです。

ハードウェア： ハードウェアの場合は、まずノートPCやスマートフォン単体が紛失や盗難の対象になることが考えられます。しかし、一般的でありながらもますますリスクが増大しているケースとしては、従業員や契約業者がタクシーなどに鞆を置き忘れ、結果として複数の会社が所有するデバイスを紛失する場合があります。チェック・ポイントが実施した調査によれば、2005年の6か月間に旅行者がシカゴ市内のタクシーに置き忘れたデバイスは、携帯電話が8万5千台、ノートPCが2万1千台にものぼります。

ソフトウェア： 代替コストには、オペレーティング・システム、ワード・プロセッサ、スプレッドシート、プレゼンテーション、通信、セキュリティ、ユーティリティなど、さまざまなビジネス関連ソフトウェアのライセンスを再購入するコストも含まれます。

暗号化の効果： 暗号化には、ハードウェアやソフトウェアの紛失または盗難の代替コストを低減する直接的な効果はありません。

復旧コスト

復旧コストの大半は、デバイスおよびデータの紛失や盗難に対処するうえで必要になる人件費です。状況によっては、デバイスが代替されるまで業務が遂行できない場合もあります。また、復旧プロセスにおいては、「紛失したデバイスにどの情報が保管されていたかを把握できているかどうか」が、情報漏洩のリスクを評価するうえで非常に重要になります。

警察への届け出： 組織の代表者は、事件および被疑者についての説明、デバイスの紛失者または盗難の被害者の名前と個人情報、各デバイスの説明、シリアル番号、ソフトウェア名、評価額など、事件に関連するさまざまな情報を収集して警察に届け出る必要があります。管轄区域によっては、複数の警察署に届け出なければならない場合もあります。

保険金の請求： 保険金の請求手続きにも、警察への届け出と同程度の情報が必要になります。また、購入金額を証明するために領収書を提示しなければならない場合は、経理部門による調査が必要になることもあります。

データ復旧の労力: IT部門は、紛失または盗難の対象となったデバイスの代わりとなる新しいデバイスを設定する必要があります。ソフトウェアのインストールや設定に加え、最新のバックアップ・データを復元する必要があります。古いデータを復元する必要がある場合は、遠隔地のオフィスや倉庫などの保存場所にバックアップ・メディアを取りに行かなければならないこともあります。バックアップされていなかったデータを復元するためには、同じデータを持っている他の従業員を探す必要もあります。

ユーザの業務への支障: 紛失または盗難に遭ったデバイスのユーザは、そのデバイスが以前のとおり完全に復旧するまでは一部の業務を遂行できない可能性もあります。それによって作業フローが停滞し、売上や収益にまで影響することになれば被害は甚大です。

情報漏洩リスクの評価: デバイスの紛失または盗難によって企業の機密情報が漏洩した可能性があるため、セキュリティ担当チームはその情報漏洩リスクを評価する必要があります。顧客個人を特定できる情報が含まれている場合 (特に個人情報保護の関連法規に抵触する場合) の影響は甚大です。このリスク評価では、バックアップ・データ・ファイルを手作業で調査し、どのデータが侵害されるリスクがあるかを判別する必要があるため、復旧作業の中でもかなり負担の大きな作業になります。この評価には、電子メールや添付ファイルの調査も含まれます。

暗号化の効果: データが暗号化されていれば、権限のない人物はデータにアクセスできないため、侵害リスクを評価する必要性はほとんどなくなります。したがって、企業の信用や知的財産への影響もなく、紛失したデバイスに直接関係するコストのみが損失となります。

影響コスト

影響コストの大部分は、個人を特定可能な情報が保管されたデバイスの紛失や盗難 (またはネットワーク経由の侵害) が原因で、個人情報保護の関連法規を遵守できないことによるコストです。

法令遵守: 多くの政府規制では、顧客や個人の特定が可能な情報を保持する企業に、それらの情報を保護することを義務付けています。例えば、米国の金融サービス業界のGLBA (Gramm-Leach-Bliley Act)、ヘルスケア業界のHIPAA (Health Insurance Portability and Accountability Act) などが挙げられます。これらの法規を遵守できない場合、罰金刑、禁固刑を含む民事罰や刑事罰に問われるおそれがあります。

通知: 米国議会では、包括的な国家データ侵害通知法案が可決されることになっています。この法案により、個人を特定可能な情報を侵害された企業は、その影響が及ぶ顧客に対し、事件に関する情報を通知しなければなりません。一方、セキュリティ侵害に関する立法措置は少なくとも35の州で開始されており、少なくとも22の州で既に採択されています。事件に関する個別の通知には多くの時間とコストがかかりますが、これは侵害されたデータが実際に悪用されていなくても実施しなければなりません。

アカウントの変更: 個人を特定可能な情報の侵害が発生した場合、企業は顧客を新しいアカウントに移管する必要があります。事件の影響を受ける顧客が数千にものぼれば、必要となる管理費は非常に大きくなります。

信用調査: 個人を特定可能な情報を侵害された企業は、個人の信用調査費用を負担し、個人情報の悪用を阻止するだけでなく、データ漏洩の影響を受ける顧客の信用が毀損されることのないよう継続的に監視しなければなりません。

「Pointsecソリューションによるトップレベルの暗号化を採用したことで、当社が法規を遵守しており、何が起こっても当社のデータは完全に保護されていると確信できるようになりました。」

グラント・ロバートソン

ITマネージャ

H&R Block Australia

ガートナーでは、
Pointsecを
モバイル・データ保護
MAGIC QUADRANTの
リーダー・クアドラントに
選出しました。

Gartner Research
調査メモ (2006年8月)

顧客サポート: 情報漏洩が発生した場合、事件に関する顧客からの電話、電子メール、および手紙に対応する顧客サポート・スタッフを大幅に拡充しなければなりません。

競争力の低下: 顧客データの紛失、盗難、侵害など情報漏洩のニュースは、競争力の低下につながる可能性があります。企業に対する評価は劇的に低下し、大規模な顧客離れに発展するおそれがあります。

従業員および顧客の安全: 個人を特定可能な情報の侵害によって、従業員や顧客の自宅住所が漏洩することもあります。つまり、個人に対する迷惑行為や傷害事件が発生するおそれがあるということです。データ紛失の結果として、少なくとも訴訟が発生することは覚悟しなければならないでしょう。

暗号化の効果: データが暗号化されていれば、権限のない人物はデータにアクセスできないため、情報紛失の影響をすべて除去できます。個人を特定可能な情報の侵害について通知義務を課すほとんどの法律では、紛失または盗難の対象となったデータが暗号化されていると通知義務は免除されます。

信用コスト

企業の信用に値段は付けられません。企業データの紛失や盗難のニュースに対して、顧客や世間一般がどのように反応するかを正確に測定することは困難です。データ侵害や情報漏洩をきっかけに、その企業の信用が失墜してしまうおそれもあります。株式を公開している企業であれば、データ侵害や情報漏洩のニュースによって株価が暴落し、時価総額が急減する可能性があります。また、同じニュースが集団代表訴訟や罰金刑につながることもあります。

データの紛失や盗難による情報漏洩が発生した企業は、既存顧客のつなぎ止めや新規顧客の獲得に苦労することになるでしょう。例えば、米国のある大手銀行では、暗号化されていないノートPC 1台の紛失が610万ドルの損失につながりました。1つの事件の損失額が数千ドルであろうと数百万ドルであろうと、その損失は暗号化を利用することによって予防できるのです。

暗号化の一般的なコストとROI

デバイスの紛失や盗難による情報漏洩の財務的なリスクは、現実的なリスクではありますが、暗号化によって限定することは可能です。暗号化技術を活用することで、データへの不正アクセスを防止できます。次の表に、2つのシナリオに基づいて、繰り返し発生する一般的な年間コストをまとめます。「保護なし」は暗号化を利用していない企業の場合、「保護あり」は暗号化を利用している企業の場合です。

表には中規模から大規模な組織の場合の典型的な数値を示してありますが、さまざまな要因(業種、情報侵害に適用される法規および罰則など)によって数値が変化する可能性があります。この表によれば、デバイスの紛失や盗難などの過失によって、企業データまたは個人を特定可能なデータが漏洩されることによるリスクの年間コストは、Pointsec PC暗号化ソリューションを使用することにより平均で90%以上削減できます。

情報漏洩に関して繰り返し発生する一般的なコスト
(暗号化していない場合と暗号化している場合の比較)

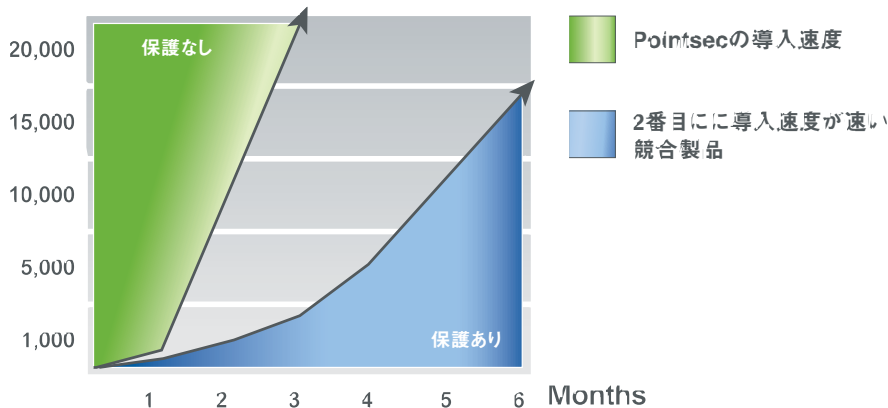
| コスト要素 | 一般的なコスト範囲 (1事件あたり) | 保護なし | 保護あり |
|-------------------------------------|-------------------------|-----------|-----------|
| 代替 - デバイスの代替が必要か? | \$1,000 - \$3,000 | \$1,500 | \$1,500 |
| 復旧 - デバイスに保管されていた情報を把握できているか? | \$2,000 - \$10,000 | \$6,000 | \$1,000 |
| 影響 - どの法規が適用されるか把握できているか? | \$15,000 - \$10,000,000 | \$22,500 | \$0 |
| 信用 - 顧客や世間一般の反応を想定できているか? | 値段が付けられないほど重要 | 金銭的な影響は甚大 | 金銭的な影響は軽微 |
| 1事件あたりの平均年間コスト | \$6,000 - \$3.3M以上 | \$30,000 | \$2,500 |
| 年間総コスト(PC1,000台規模で、1年にその3%を紛失すると仮定) | 30事件 | \$900,000 | \$75,000 |

総所有コスト(TCO)

ROIのもう1つの側面は、暗号化ソリューションの総所有コスト(TCO)です。そして、TCOを構成する要素の1つが、これまでに説明したリスクに対して繰り返し発生するコストを除去するまでにどれだけの時間を必要とするかです。暗号化ソリューションの導入に時間がかかればかかるほど、保護されていない環境におけるリスクに対して支払うコストが大きくなります。暗号化ソリューションの導入期間は、どのソリューションを選択するかによって異なります。PC数万台を所有する大規模な組織へ導入する場合、通常は6か月以上かかりますが、Pointsec PCは、競合製品に比べかなり短期間で導入できます。これは、世界中の組織の何十万台ものPCで、競合製品をPointsec PCに置き換えてきた経験に基づいています。

次のグラフは、PC 2万台規模の組織へのPointsec PCの導入進捗を、その次に導入進捗が速い競合製品と比べたものです。これによると、競合製品の導入には6か月を必要としますが、Pointsec PCの場合はその半分の3か月以内で完了しています。

Seats



Pointsec PCの優れた導入特性の経済的価値は、7ページの表のデータに基づいて計算できます。表のシナリオでは、リスクに対して繰り返し発生する年間コストはPC 1,000台あたり900,000ドル(1億800万円*)です。一方、Pointsec PCを導入した場合のコストは75,000ドル(900万円*)です。その差825,000ドル(9900万円*)が、Pointsec PCを導入することで削減できる可能性のあるコストです。825,000ドル(9900万円*)を52週で割ると、PC 1,000台あたりの1週間のコストは15,865ドル(190万3800円)となります。Pointsecによって6か月の導入期間を半分の13週間に短縮すると、セキュリティ・コストをPC 1,000台あたり206,245ドル(約2475万円*)削減できたこととなります。

TCOに関係するその他の要因については、チェック・ポイント発行の技術白書「暗号化のTCO(総所有コスト)に対するガイド」を参照してください。

* \$1=120円として計算

詳細について

現在お使いのIT環境に、Pointsec PCフルディスク暗号化製品を短期間で導入する場合の経済効果については、チェック・ポイントまでお問い合わせください。それぞれの組織の実情に合わせて7ページの表を調整し、リスクに対するコストを分析されることをお勧めします。また、この白書の姉妹編として「暗号化のTCO(総所有コスト)に対するガイド」も発行されています。このドキュメントに関する詳細は、チェック・ポイントまたはチェック・ポイント製品取り扱い代理店へお問い合わせいただくか、www.checkpoint.co.jpをご覧ください。

©2003-2007 Check Point Software Technologies Ltd. All rights reserved.
Check Point, Application Intelligence, Check Point Express, Check Point Express CI, Check Pointのロゴ, AlertAdvisor, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、6,496,935、6,873,988、および6,850,943により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Guide to the ROI of Encryption

P/N:502478-J 2007.05

※記載された製品仕様は予告無く変更される場合があります。



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
<http://www.checkpoint.co.jp/> E-mail: info_jp@checkpoint.com Tel: 03 (5367) 2500