2B-4

複数USBフラッシュメモリによる機密情報拡散通信手法の実装*

東京電機大学 理工学部 情報システム工学科†
落合 孝文　桧垣 博章‡ §

1 背景と目的

近年、広帯域バックボーンの低価格化、ブロードバンドアクセスネットワークや無線アクセスネットワークの普及により、組織が管理するデータに対して、組織内ネットワークのみならず、組織外ネットワークに接続されたコンピュータからインターネットを介してアクセスすることを可能とする技術がモバイルコマースの一環として研究開発されている。ユーザのコンピュータからデータへのアクセスは、組織内ネットワークとの間のVPNにより実現する。暗号化データをインターネット経由で配送することにより、盗聴や改竄に対する安全性を実現している。しかし、暗号技術はコンピュータ技術の発達によって陳腐化する。盗聴者が持つコンピュータの計算能力が向上すると、従来技術で暗号化されたデータが合理的な時間で復号される可能性がある。一方、バックボーンネットワークやアクセスネットワークの提供する通信帯域は各ネットワークごとに異なり、使用率の時間変化も大きい。このため、データへのアクセスに必要な通信帯域が常時提供されるとは限らない。そこで、小型大容量のストレージデバイスによるネットワークを介さないデータ配送が検討されている [3]。携帯可能な小型ストレージデバイスは、フラッシュメモリや小型ハードディスクによって実現され、広く普及している。これらのデバイスを用いることで安定したデータ取得が可能となるが、輸送中のデバイスの盗難、紛失によるデータの遺漏が問題となる。本論文では、複数のUSBフラッシュメモリにデータを分割配置することにより、ネットワークを介さずに安全にデータを配送する手法を提案する。提案手法は、各分割データの暗号鍵もUSBフラッシュメモリに格納することにより、配送先コンピュータを固定する必要がなく、ネットワーク通信を用いることなく復号することが可能である。

2 従来手法

暗号通信技術は、共通鍵方式と公開鍵方式とに分類される。共通鍵方式では、暗号化と復号に用いる共通の鍵を送信者と受信者が共有する。したがって、あるコンピュータで暗号化されて得られた暗号文を配送されたコンピュータで平文を得るためには、このコンピュータにあらかじめ共通鍵が格納されていることが必要である。携帯可能なストレージデバイスに格納された暗号文は、定められたコンピュータでしか復号することができず、高い利便性を得ることができない。一方、公開鍵方式では、公開鍵と秘密鍵の対が暗号通信に用いられる。公開鍵で作られた暗号文は、対となる秘密鍵でのみ復号可能であることから、送信者が受信者の公開鍵で平文を暗号化すれば、対となる秘密鍵を持つ受信者のみが復号し、平文を得ることができる。しかし、本方式でもデータをUSBフラッシュメモリに格納するために平文を暗号化するときに、データ配送先のコンピュータの公開鍵による暗号化を行なうことから、定められたコンピュータでしか復号することができない。公開鍵を入手できさえすれば、暗号化以前には任意のコンピュータを配送先と定めることができるが、第三者による受信者のなりすましを防ぐためには、PKIを用いた認証局との通信が必要になる。

複数の通信路を用いることによって、盗聴や盗難を困難にするIP通信拡散手法 [1] が提案されている。単一の通信路を用いる場合、この通信路上の一ヶ所で配送メッセージを観測することによって、データの全体を盗聴者が入手することが可能である。これに対して、IP通信拡散手法では、データを分割し、複数の通信路を用いて配送を行なう。盗聴者がデータの全体を入手するためには、各通信路における配送メッセージの観測を並行に行なうことが必要となる。ネットワークを介さないデータ配送においては、データを分割し、複数のUSBフラッシュメモリそれぞれには分割データの一部のみを格納する。各USBフラッシュメモリは盗難、紛失に対して独立に輸送する。このように、紛失独立な仮想通信路を用いて配送することで、同様の安全性を提供することができる。

分割されたデータから分割前のデータを復元することを困難とするための手法として電子情報の安全確保方法 [4] が提案されている。ここでは、任意のランダムなサイズへの分割を行ない、配送順をランダムに並べ換える。しかし、分割データ群から分割前のデータを復元するために必要となる分割データ位置情報は、分割データとともに格納される。これは、分割データの暗号鍵を分割データとともに配送していることと等価であり、任意のコンピュータでの復号が可能な手法である。しかし、分割データとその暗号鍵とが同一のUSBフラッシュメモリに格納されていることから、盗難時には分割データの復号が可能であるという問題がある。

3 提案手法

本論文では、IP通信拡散手法および電子情報の安全確保方法で用いられている複数の通信路による分割配送を、複数のUSBフラッシュメモリにデータを分割格納して輸送することで提供される仮想通信路を用いて実現することを提案する。データ D は n 個の部分データに

*Secure Data Transmission with Multiple Portable Storage Devices
†Tokyo Denki University
‡Takafumi Ochiai and Hiroaki Higaki
§{takafumi, hig}@higlab.net

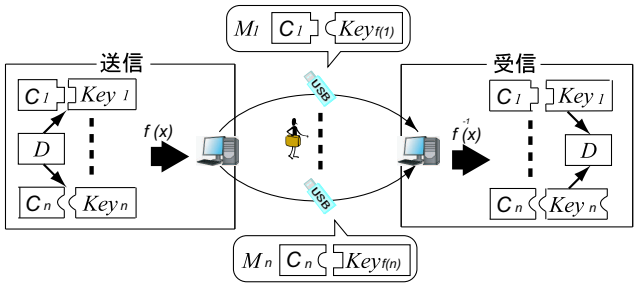

図 1: 分割データと暗号鍵の同時配送

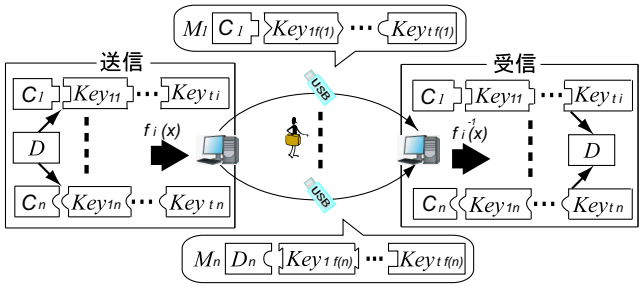

図 2: 多重度 t による安全性の向上

分割され、各部分データは暗号鍵 Key_i によって暗号化される。暗号データ $C_1, \ldots, C_n$ を USB フラッシュメモリ $M_1, \ldots, M_n$ に格納するとともに、各 M_i には暗号鍵 $Key_{f(i)}$ を格納する。ただし、$f(i)$ は $\{1, \cdots, n\}$ 上の置換である。配送先では M_i に格納された C_i を $M_{f^{-1}(i)}$ に格納された Key_i を用いて復号し、D を取得する (図 1)。提案手法では、M_i に格納された C_i から D の部分データを復号するためには、M_i のみでなく $M_{f^{-1}(i)}$ をも取得しなければならない。また、提案手法は、あらかじめ暗号鍵を配送先コンピュータに配布する必要がないため、任意のコンピュータへのデータ配送を行なうことができる。

提案手法は、鍵の多重度を高めることによって安全性を高めることができる。データ D の各 n 分割データに対して、暗号鍵 $Key_{1i}, \ldots, Key_{ti}$ を用いた暗号化を順に行ない、暗号文 C_i を得る。USB フラッシュメモリ M_i には、C_i とともに $Key_{1f_1(i)}, \ldots, Key_{tf_t(i)}$ を格納する。M_i に格納された C_i から部分データを復号するためには、M_i に加えて $M_{f_1^{-1}(i)}, \ldots, M_{f_t^{-1}(i)}$ をも取得しなければならない。

4 評価

提案手法によって得られる安全性を、分割データと暗号鍵を格納した USB フラッシュメモリの一部を取得したときに取得可能な平文データ量の期待値によって評価する。ここでは各分割データサイズは等しいとする。暗号鍵とそれによって暗号化されたデータを組として同一の USB フラッシュメモリに格納する場合、各 USB フラッシュメモリを取得すると、それに格納された暗号データから平文を必ず得ることができる。したがって、n 分割されたデータから m 個の分割データを取得したときに得られる平文の割合は m/n である。一方、提案手法では、暗号データに対応する鍵のすべてが取得した USB フラッシュメモリのいずれかに格納されているときのみ平文が入手できる。データ分割数 n、暗号化回数（鍵多重度）t のとき、m 個の分割データ $(0 \leq m \leq n)$ を取得したときに復号して得られる平文データの割合 (データ取得率) の期待値は次式で与えられる。

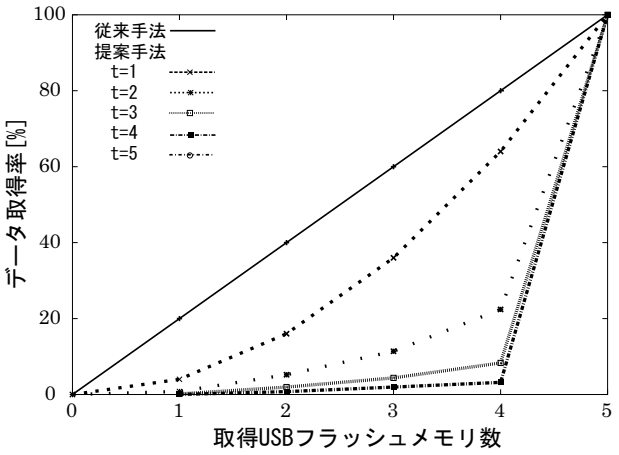

図 3: 分割配送時のデータ取得率

$$\sum_{l=max((t+1)m-tn,1)}^{m} \frac{l}{n} \cdot \frac{{}_mC_l \cdot {}_{n-m}C_{m-l}}{{}_nC_m} \cdot \left(\frac{{}_{n-l}C_{m-l}}{{}_nC_m}\right)^{t-1}$$

$n = 5$ の場合の評価結果を図 3 に示す。鍵多重度 $t = 1$ の場合、$m = 1, 2, 3, 4$ におけるデータ取得率は従来手法の平均 60.0% に低下している。提案手法の安全性は、鍵多重度を高くすることでより高くなり、$t \geq 3$ ではすべての USB フラッシュメモリを取得しなければ、データ取得率は 8.32% 以下となる。

5 まとめ

分割データの暗号文と暗号鍵を組み替えて複数の USB フラッシュメモリに格納して輸送することによる安全性と利便性の高いデータ配送手法を提案し、盗聴者の取得データ量の評価により有効性を示した。提案手法は、WINDOWS オペレーティングシステムで動作するアプリケーションとして実装され、ドラッグアンドドロップにより簡易に暗号化と USB フラッシュメモリへの格納、読み出しと復号を行なうことができる。

参考文献

[1] 有泉, 寺西, 横山, 桧垣, “IP 通信拡散手法を用いた VPN 装置の実装と性能評価,” 情報処理学会マルチメディア通信と分散処理ワークショップ論文集, Vol. 2003, No. 19, pp. 55–60 (2003).

[2] 高橋, 桧垣, “複数 USB フラッシュメモリによる機密情報拡散通信手法,” 電子情報通信学会情報ネットワーク研究会, 信学技報 Vol.103, No.689, pp.115-118 (2003).

[3] 中川, 杉浦, 井上, 木村, 土池, “コンテンツ容量から見た情報モビリティに関する検討,” 情処研報, Vol. 2003, No. 93, pp. 39–44 (2003).

[4] 保倉, “電子情報の安全確保方法,” 日本国特許庁, WO00/45358 (1999).