Vol.2009-DD-73 No.2
2009/9/25

# 消去を含むデジタルコンテンツのライフサイクル管理

園田俊浩† 竹林知善† 井谷茂寛†

情報漏えいは、あらゆる組織において解決すべき重要な課題となっている。しかし、情報漏えいの経路は複雑化しておりその対策は一筋縄ではいかない。富士通研究所では従来から培ってきた暗号などのセキュリティ技術に加えて、モバイル機器や情報検索に関する技術やノウハウを統合した情報漏えい対策ための研究開発を行っており、その効果を社内実践により検証して実用化へとつなげていく取り組みを行っている。
本稿では、企業内だけではなくオフラインのお客様先や協力会社も含め組織をまたがる場面での情報取り扱いを分析した結果、および、自動消去機能を搭載した USB メモリとそれを活用した消去を含むデジタルコンテンツのライフサイクル管理を紹介する。

# Lifecycle Management with Deletion of Digital Content

TOSHIHIRO SONODA† TOMOYOSHI TAKEBAYASHI†
SHIGEHIRO IDANI†

For every organization, information leakage is important issue which should be solved as soon as possible. But, we don’t have best solution for the issues of information leakage. We are researching the technologies to prevent the incident of information leakage by leveraging security technologies of data encrypting, data searching and mobile device like portable phone and PC we have been researched so far. And, we are conducting trial for the proof of concept and brushing up the solution for the practical use.
In this paper, we introduce the result of hearing and analysis of information usage in enterprise and the lifecycle management with deletion of digital content using USB with automatically deleting data.

## 1. はじめに

情報漏えいは、あらゆる組織において解決すべき重要な課題となっているも。しかし、情報漏えい経路は複雑化しておりその対策も一筋縄ではいかない。NPO 日本ネットワークセキュリティ協会によると 2007 年に公表されたインシデント件数は 864 件、情報漏えいした人数は 3,000 万人を超え、想定損害賠償額も 2 兆円を超えるとされている。情報漏えい経路は、紙（40.4%）が依然としてトップであるが、Web・Net（Winny など 15.4%）、USB メモリなどの可搬記憶媒体（12.5%）、PC 本体（10.9%）、E-mail（9.8%）、そのほか（携帯など 5.9%）と、デジタル化された情報が様々な経路で漏えいしている。こうした課題に対して、富士通研究所では暗号などのセキュリティ技術に加え、従来培ってきたモバイル機器や情報検索に関する技術やノウハウを統合した情報漏えい対策技術を開発し，社内実践により効果を検証して実用化へとつなげていく取り組みを行っている。
本稿では、その取組みの 1 つとして、企業内だけではなくオフラインのお客様先や協力会社も含め組織をまたがる場面での情報取り扱い方法の分析、および、自動消去機能を搭載した USB メモリによる社外への安全なデータ持出しソリューションを紹介する。
本稿では、第 2 節において関連技術動向について解説する。第 3 節では、筆者らが目指す方向を説明し、消去を含むデジタルコンテンツのライフサイクル管理について説明する。第 4 節では実装例を示し、その評価について述べる。

## 2. 情報漏えい対策の進展と関連技術

2000 年頃、ネットワーク型ウイルスや不正アクセスなど組織ネットワークに対する外部からの攻撃に対応するために、ファイアウォールや IDS（Intrusion Detection System）など、組織ネットワークの周りに壁を作って守るネットワーク型のセキュリティ対策が実施された。その後、ブロードバンドとモバイル PC の普及によりワークスタイルが変化し情報流通の多様化が進行した。その結果、企業ネットワークの周りに壁を作って守る従来の対策だけでは十分な機能を果たさなくなってしまった。
そこで、PC のようにセンシティブな情報が保存されている個々の機器を守るため、ハードディスク暗号化、TCG（Trusted Computing Group）技術や仮想化技術などのエンドポイント・セキュリティ技術へと発展してきた。

† （株）富士通研究所
Fujitsu Laboratories LTD.

しかし、情報漏えいの経路が多様化、複雑化してくるにつれて、個々のエンドポイント対策だけでは限界があり、現在は、情報単位で情報を保護する技術が必要とされている。組織内の重要な情報とそれへのアクセスを情報がどこにあっても守るという考え方である。Jericho Forum では、ファイアウォールの企業イントラを保護していた防壁(perimeter)が崩壊された状況を防壁の崩壊（De-perimeterization）と呼び、今後は、インターネットに代表されるオープンネットワーク上での企業情報の取り扱い方や複数企業で共有する IT インフラのあり方、さらには、個人単位での情報のアクセス方式の検討が必要になると考えている[5][6]。

以下に、情報漏洩対策の具体的な実現技術を紹介する。

### 2.1 DLP – Data Loss Prevention

DLP は、機密情報をコンテンツ単位で区別できるようにしておき、ネットワークで送信中のデータ移動時（DIM : Data in Motion）、データの保存時（DAR : Data at Rest）、PC などエンドポイントでのデータ利用時（DIU：Data in Use）の機密情報が社外に漏えいする直前でブロックする仕組みである。Trend Micro 社の LeakProof [1] は、機密ファイルの特徴情報をあらかじめサーバに登録し、情報が漏えいする危険性のあるポイントでこの特徴情報が含まれるファイルを監視することにより機密データを含む情報が不正に漏えいすることを防止する。

### 2.2 ERM – Enterprise Rights Management

ERM は、DRM（Digital Right Management)技術を企業内文書に適用したもので、機密情報が社内だけでなく社外にあっても永続的にコンテンツのアクセス権をコントロールする技術である。ERM では、暗号化技術を用いてコンテンツのアクセスを制限する。コンテンツを閲覧、編集する場合は、コンテンツにアクセスするためのライセンスをライセンス管理サーバから取得し、一元管理されたポリシーに従ってコンテンツを閲覧、編集する。ライセンスを与えないことによって、コンテンツの利用を止めることができるために、コンテンツのライフサイクルを管理していると言える。ERM で課題になるのはクライアント側のセキュリティである。なぜなら、ライセンスを提供したクライアントがライセンスに付随するポリシーに従って動作しなければ、機密情報の保護が保証されなくなるからである。そこで、TC(Trusted Computing)技術や仮想化技術と統合したソリューションも検討されている[2][3]。仮想化技術は、クライアント環境と分離された仮想環境を提供することにより、クライアント環境の脅威を軽減する。一方、TC 技術は、ソフトウェアコンポーネントの完全性の保証を提供する[4]。

### 2.3 TVD – Trusted Virtual Domain

TVD[7][8]は、TC 技術と仮想化技術を活用し、PC やサーバなど複数のエンティティから構成されるドメイン（隔離された実行環境）のことである。仮想化技術によって、物理プラットフォームに依存せずにドメインを形成するため、異なるドメインを同じ物理プラットフォーム上に配置することも可能である。また、あるドメイン内のエンティティは、そのドメインで運用されるセキュリティポリシーに従う必要がある。

[8]では、TVD モデルの基本技術である実行環境の隔離、アクセス・コントロールポリシーの強制、プラットフォームの完全性チェックをベースにした信頼されたエンティティ間の連携、および、エンティティ内でのセキュアなコミュニケーション・チャネルの確立を応用し、アプリケーション層における TVD と VM(Virtual Machine)層における TVD を統合したシステムを提案している。[9]では、TVD と ERM を統合し、TVD 内でのドキュメントレベルのアクセスコントロールを実現している。

### 2.4 ILM – Information Lifecycle Management

情報セキュリティの観点からは、情報は、物理的にも論理的にも情報所有者の環境で管理されるのが望ましい。しかし、クラウド・コンピューティング環境の出現により、必ずしも情報所有者の環境で情報が管理されることが一般的ではなくなってきている。このような環境下では、情報の生成、編集、移動、保存、消去といった情報のライフサイクルを管理することが難しく、特に、クラウド・コンピューティング環境に流出した情報が完全に消去することを証明することは、保存されていることを証明するよりはるかに難しい。

[10]では、クラウド・コンピューティング環境では、情報の消去をスケジュールすることの重要性を強調しているのとともに、クラウド・コンピューティング環境に流出した情報は、どのようなメディアに保存されたか、他の目的に利用されていないかを追跡することが困難であることも指摘している。[11]では、データが自動消去することによりメリットを受けるアプリケーションは多く存在するとし、情報が自動的に消去されるシステムを提案している。

### 2.5 シンクライアント

シンクライアントは、クライアント側のセキュリティを保つことの難しさから、情報とそれを扱うリソースを可能な限りサーバ側に配置したシステムである。クライアント側に情報がないことが明確であり、導入を始めている企業もある。但し、オフライン作業ができないことや顧客先での作業は不向きなど課題も多く、メール閲覧専用

など利用シーンに応じて使い分けられるケースが多い。

## 3. 消去を含むコンテンツのライフサイクル管理

### 3.1 目指すべき方向

**図-1** に著者らが検討する情報環境を示す。現状のイントラネットやテレワークからオフラインのお客様先や協力会社も含めた場面でのデジタルコンテンツの取り扱いについて検討する。

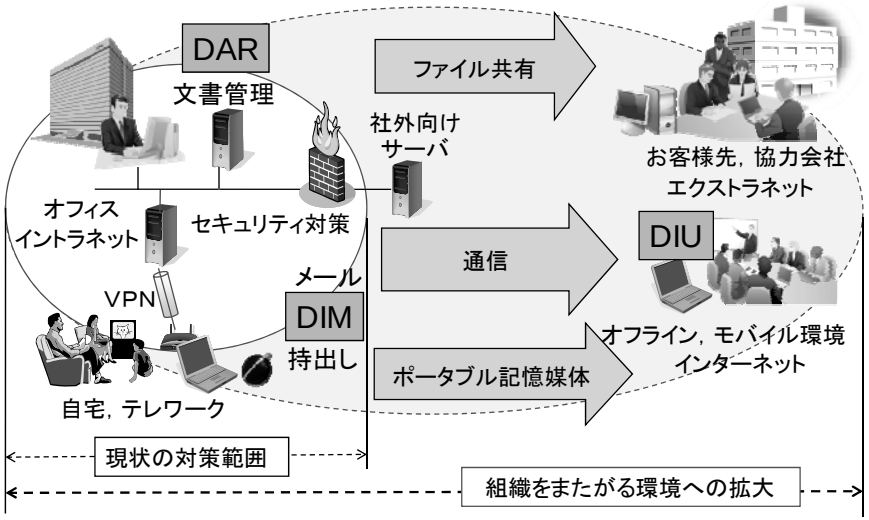



図-1　組織間のセキュア情報環境
Fig.1-Secure work space.

### 3.2 利用シナリオ

企業間でのコンテンツ共有は、委託業務や商談など様々ケースが考えうる。また、企業情報を自宅に持ち帰り仕事を継続するようなケースやモバイル PC を持ち運び、顧客先でのプレゼンテーションを行うような仕事のスタイルは、今では一般的である。自宅や出張先で企業内の情報を取り扱うために、以下のような方法でデジタルコンテンツを移動し、利用することが考えられる。

- モバイル PC に必要なコンテンツを保存し、移動先まで移動する
- USB メモリなどのポータブル記憶媒体にコンテンツを保存し、移動先まで移動する。作業は移動先の PC を利用する。
- 上記の二つの例の逆で、移動先から情報をモバイル PC や USB メモリに保存してオフィスに持ち帰る。
- メールで必要なコンテンツを移動先 PC に送信する。
- 社内に VPN 接続し、社内コンテンツにアクセスする。

今回は、ポータブル記憶媒体である USB メモリを利用したコンテンツの取り扱いシナリオを考える。企業における USB メモリの利用シナリオを、USB メモリを利用している部門にヒアリングしたところ、以下のような利用シナリオがあることがわかった。

1. 一時的なコンテンツ交換
   同じ場所にある PC から別の PC へデジタルコンテンツを移動するケース。
2. 出張先、自宅からのオフィスへのコンテンツ持ち込み
   IT 保守業務を行っている部門では、IT 機器の障害ログなどを解析するため、顧客先で情報を USB メモリに保存しオフィスに持ち帰り、解析するケースがある。
3. オフィスから出張先、自宅へのコンテンツ持ち出し
   出張先でネットワークが利用できない、または、ネットワーク環境がない場合、USB メモリを利用するケースがある。例えば、公立教職員約 85 万人中、コンテンツを自宅に持ち帰って残業する割合は、小学校 85%、中学校 81%、高校 62%（全日）で、約 65 万人がコンテンツを持ち帰り自宅で作業している。学校の場合、ネットワーク設備が不十分なケースも多く、USB メモリなどのポータブルデバイス利用する場合が多い[13][14][15]。その他にも、ネットワーク経由で移動するにはサイズが大きい場合でも USB メモリを利用するケースがある。

ヒアリングの結果、USB メモリは一時的なコンテンツ移動の手段として利用し、移動が完了したら USB メモリの内容を消去することが規則として運用されていることがわかった。但し、消去は利用者任せであるために、各部門の IT 管理者は、USB メモリの利用者が消去し忘れることを懸念していることも判明した。

### 3.3 情報漏えいリスク

シナリオ 1 の一時的なコンテンツ交換では、USB メモリに保存したコンテンツの消去し忘れが問題となる。消去し忘れた状態で、ウイルスに感染した PC 上で USB メモリを利用し、コンテンツが漏えいする可能性があるためである。

シナリオ 2 では、USB メモリ内のコンテンツの消去し忘れと移動中の USB メモリ紛失という問題がある。

シナリオ 3 では、USB メモリ内のコンテンツの消去し忘れと移動中の USB メモリ紛失という問題がある。また、企業内から持ち出したコンテンツが、移動先である自宅、または、出張先の PC のローカル HDD に保存されてしまうことも問題である。一旦、PC に保存されたコンテンツは、移動先の PC 所有者が意図的に消去しない限り、その PC に残ってしまう。その時点で、PC にウイルスが感染していなかったとしても将来何らかの形でウイルスに感染し、そのコンテンツをネットワークに流出させてしまうかもしれない。例えば、自宅の PC の場合は、家族で共有して利用しているケースも多い。ある時点でクリーンであった PC に父親が企業から持ち帰ったコンテンツを保存し、後に、そのことを知らない子供がファイル共有ソフトをインストールし、ウイルス完成して、そのコンテンツがファイル共有ソフト経由で漏えいしてしまうというインシデントも発生している。

シナリオからわかった課題をまとめると以下のようになる。

| | 課題 1 | 課題 2 | 課題 3 |
|---|---|---|---|
| | コンテンツの消去忘れ | USB メモリ紛失 | コンテンツをローカル HDD に保存 |
| シナリオ 1 | ○ | | |
| シナリオ 2 | ○ | ○ | |
| シナリオ 3 | ○ | ○ | ○ |

### 3.4 対策検討

USB に保存したコンテンツを 2.2 節で説明した ERM で管理する仕組みを実現し、一定期間でライセンスを消去することで、シナリオ 1 の課題 1 は解決できる。しかし、シナリオ 2 や 3 のように、利用する場所が異なるケースやオフライン作業が必要なケースでは、ライセンス管理サーバへのアクセスができない。USB メモリ自体にコンテンツのライフサイクルの消去を実現する仕組みが必要である。

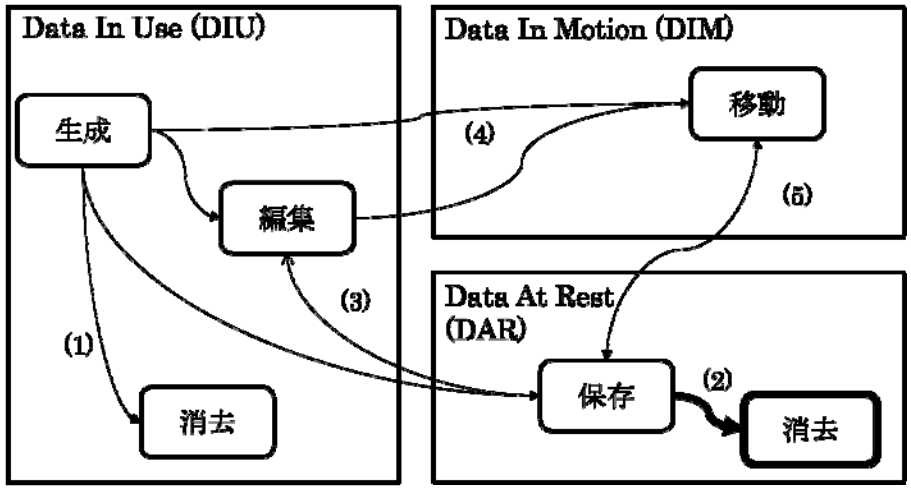
課題 2 は、紛失した場合に第三者に利用されないように、USB メモリを利用する際に認証の仕組みを持つことで解決する。パスワードの総当たり攻撃（ブルースフォースアタック）に対応するために、一定回数の失敗後に USB メモリを使えないようにするなどの工夫が必要である。

シナリオ 3 では、自宅 PC とオフィス PC 間のコンテンツ移動だけで利用する場合は、利用 PC を特定できる。この場合は、あらかじめ利用する PC を USB メモリと関連付けておくことにより、他の PC で利用されることを防止できる。

課題 3 を解決するためには、コンテンツを持ち運んだ先の PC にコンテンツが残らない仕組みを実現する必要がある。2.1 節で説明した DLP のようにコンテンツの流通を制限する機能を用いて、オフィスで USB メモリに保存したコンテンツが移動先の PC のローカル HDD に保存できないようにする。但し、移動先の PC 上で動作するアプリケーションは、利用できるような仕組みが必要である。

### 3.5 消去を含むデジタルコンテンツのライフサイクル管理

前節の検討結果をまとめると、USB メモリを安全に利用するためには、消去を保証するコンテンツ･ライフサイクルの管理が必要となる。コンテンツの利用(Data In Use)、コンテンツ移動(Data In Motion)、コンテンツ保存(Data At Rest)にコンテンツのライフサイクルをマップした図を下図に示す。




課題 1 を解決するために、図の(2)で示したデータの消去機能を DAR(USB メモリ)

に搭載する。従来ユーザが不要と判断して、(1)で行うコンテンツの消去作業を(2)で自動的に行うことによって、コンテンツの消去し忘れに対応する。消去が行われるタイミングは利用シナリオによって変わるので、ユーザが、自動消去のタイミング設定を行う必要がある。課題 2 を解決するために、USB メモリ内のコンテンツが DAR から DIU へ遷移できるようにするための認証機構を実現する。

課題 3 を解決するために、コンテンツが、(3)経由で DAR(USB メモリ)から DIU 状態になった後、他の記憶媒体に保存できない仕組みが必要である。つまり、(3)経由で USB メモリから読み込まれたコンテンツが、(4)経由でネットワークに転送されることと、他の記憶媒体に保存されることを禁止する必要がある。また、(5)経由で USB メモリの内容を直接ネットワークへ転送されることも禁止する必要がある。

最後に、USB メモリの利便性を考えると、DIU におけるユーザの操作はできるだけ変更しないほうがよい。

## 4. 実装例

消去を含むデジタルコンテンツのライフサイクル管理を実現するために、自動消去機能付き USB メモリ(安全 USB メモリ)とコンテンツの移動制限ソフトウェアの開発を行った。

### 4.1 自動消去機能付き USB メモリ（安全 USB メモリ）

以下に今回開発した USB メモリ（以後、安全 USB メモリと呼ぶ）の機能を示す。

| 機能 | 概要 | 解決する課題 |
|---|---|---|
| コンテンツ<br>自動消去機能 | 以下の条件で、USB メモリ内のコンテンツを消去する。<br>・認証後、指定された時間経過した場合<br>・指定された回数、ユーザ認証失敗した場合<br>・指定された回数、PC 認証が失敗した場合 | 課題 1 |
| ユーザ<br>認証機能 | ユーザ認証成功後、USB メモリとしての機能が利用できるようになる。 | 課題 2 |
| PC 認証機能 | PC を特定する識別情報(BIOS ID など)を安全 USB メモリに登録しておき、登録された PC でしか利用できないようにする機能 | 課題 2 |

安全 USB メモリは、内部にバッテリー（キャパシタ）、リアルタイムクロック、マイコンを搭載しており、ユーザ認証機能、PC 認証機能、コンテンツ自動消去機能を持つ。コンテンツ自動消去は、ユーザ認証失敗や PC 認証失敗の回数や指定時間が経過をトリガにして実施される。たとえば、消去時間として 48 時間を指定した場合、PC から外された後 48 時間で自動的にコンテンツは消去される。PC に接続され、ユーザ認証(PIN 認証)が成功するとタイマーはリセットされ、再度、PC から外された後 48 時間後に消去動作が稼働する。

### 4.2 コンテンツ移動制限ソフトウェア

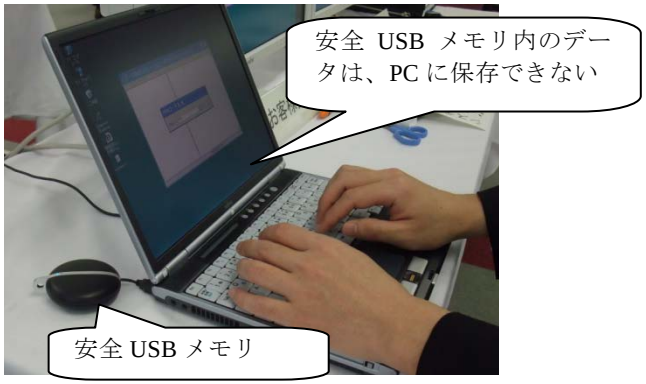
以下に今回開発した USB メモリ（以後、安全 USB メモリと呼ぶ）の機能を示す。

| 機能 | 概要 | 解決する課題 |
|---|---|---|
| コンテンツ<br>移動制限機能 | 安全 USB メモリへのコンテンツ保存は許可するが、安全 USB メモリ以外の記憶媒体に対するコンテンツ保存を禁止する。 | 課題 3 |

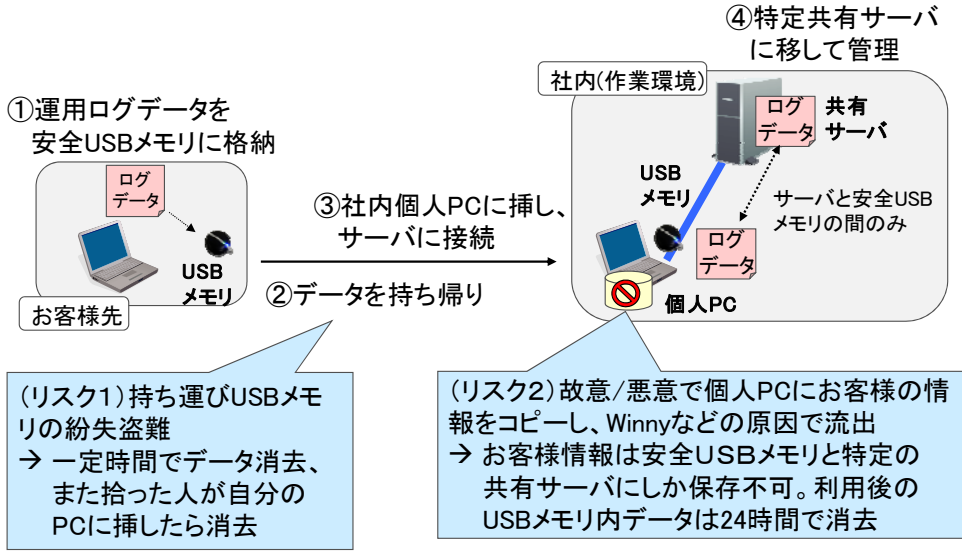
移動先 PC へのコンテンツ移動を制限するためにファイル・リダイレクタの開発を行った。ファイル・リダイレクタは、PC に安全 USB が接続されたときに有効になり、安全 USB メモリへのコンテンツ保存は許可し、PC 側へのコンテンツ保存を禁止する。また、PC 上のアプリケーションが生成する一時ファイル、例えば、インターネット・エクスプローラのキャッシュファイルなどを USB メモリに転送することも可能である。これにより、安全 USB メモリのコンテンツが PC のローカル HDD に保存されることを保護することが可能である。

Vol.2009-DD-73 No.2
2009/9/25

### 4.3 利用シーンと評価




上図に示すように通常の USB メモリと同様の使い勝手を実現し、指定された時間でメモリ内のコンテンツは削除される。




また、図の利用シーンで USB メモリを利用する部門に安全 USB メモリを提供し、実運用上問題ないか検証を行った。

## 5. まとめ

情報漏えいは、あらゆる組織において解決すべき重要な課題となっているが、情報漏えいの経路は複雑化しておりその対策は一筋縄ではいかない。富士通研究所では従来から培ってきた暗号などのセキュリティ技術に加えて、モバイル機器や情報検索に関する技術やノウハウを統合した情報漏えい対策技術の研究開発を行っており、社内実践により効果を検証して実用化へとつなげていく取り組みを行っている。

本稿では、企業内だけではなくオフラインのお客様先や協力会社も含め組織をまたがる場面での情報取り扱いを分析した結果、および、自動消去機能を搭載した USB メモリとそれを活用した消去を含めたデジタルコンテンツのライフサイクル管理を紹介した。今後は、今回得たノウハウを活かし、データ消去を含むデジタルコンテンツのライフサイクル管理を情報漏洩対策のために役立てていく予定である。

Vol.2009-DD-73 No.2
2009/9/25

## 参考文献

1) Trend Micro LeakProof: Leveraging Data Leak Prevention Technology to Secure Corporate Assets.

2) J. Reid and W. Caelli. DRM, Trusted Computing and Operating System Architecture. 2005.

3) A. Sadeghi, M. Wolf, C. St uble, N. Asokan, and J. Ekberg. Enabling Fairer Digital Rights Management with Trusted Computing, October 2007.

4) R. Sandhu, K. Ranganathan, and X. Zhang. Secure information sharing enabled by Trusted Computing and PEI models. In ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security, pages 2-12, New York, NY, USA, 2006. ACM.

5) Jericho Forum. http://www.opengroup.org/jericho/

6) Jericho Forum. Visioning White Paper What is Jericho Forum?, 2005.

7) A. Bussani, J. L. Gri_n, B. Jasen, K. Julisch, G. Karjoth, H. Maruyama, M. Nakamura, R. Perez, M. Schunter, A. Tanner, L. V. Doorn, E. V. Herreweghen, M. Waidner, and S. Yoshihama. Trusted Virtual Domains: Secure Foundations for Business and IT Services. Technical Report Research Report RC23792, November 2005.

8) Y. Katsuno, M. Kudo, P. Perez, and R. Sailer. Towards Multi-Layer Trusted Virtual Domains, 2006. The 2nd Workshop on Advances in Trusted Computing.

9) Yacine Gasmi, Ahmad-Reza Sadeghi, Patrick Stewin, Martin Unger, Marcel Winandy, Rani Husseiki, Christian Stüble. Flexible and Secure Enterprise Rights Management based on Trusted Virtual Domains

10) Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009.

11) Roxana Geambasu, Tadayoshi Kohno, Amit A. Levy, Henry M. Levy. Vanish: Increasing Data Privacy with Self-Destructing Data

12) E. Gaudet. DRM vs. ERM: battle to control data. December 2006.

13) 平成 19 年度学校教員統計調査

14) 平成 18 年度文部科学省委託調査「教員勤務実態調査（小・中学校）報告書」

15) 平成 18 年度省調査「教員勤務実態調査（高等学校）報告書」