情報持ち出し申請システムによる情報漏洩防止ソリューションビジネスの展開

The Development of a Solution Business with the Information Bringing Out Management System for the Prevention of Information Leakage.

荒井　崇之　Arai Takayuki
櫻井　浩　Sakurai Hiroshi
小松澤　美喜夫　Komatsuzawa Mikio
佐藤　義人　Sato Yoshito

㈱日立東日本ソリューションズ（以下，日立 TO）では，情報漏洩対策として PC 端末のシンクライアント化を推進するとともに，漏洩リスクの高い USB メモリなどの可搬記録媒体の利用を制限するなどの施策によりセキュリティの向上に努めている。今般，施策の一環として「情報持ち出し申請システム」を開発した。

本システムは，可搬記録媒体による情報持ち出しに対し上長による承認を必須とする仕組みである。個人情報保護や内部統制に対する社会意識の高まりの中で，各企業・団体が情報セキュリティレベルを向上させる施策への期待は大きく，この情報漏洩防止ソリューションはそのようなニーズに対する一つの解である。

本論文では，情報漏洩動向の分析から導かれる市場ニーズとそれらを解決する情報持ち出し申請システムの概要，および情報漏洩防止ソリューションビジネスの展開について述べる。

１．　はじめに

あらゆる企業・団体には，事故や不測の事態が発生した場合にその損害を最小限に抑えるためのリスク管理として，危機管理計画（コンティンジェンシー・プラン）の策定が求められている。企業や個人の安全を脅かす情報漏洩への対策は，PC 端末のシンクライアント化，HDD の暗号化といった物理的な対策が取られてきており一定の効果を上げている。一方で，業務ルールに違反した不正な持ち出しなど人的側面に起因する情報漏洩が増加してきている。

日立 TO では，人的側面に起因する過失による情報漏洩へのリスクの低減を支援することを目的に，持ち出しに至る証跡を残置することを特長とした「情報持ち出し申請システム」（以下「本システム」とする）を開発した。

本システムは，日立 TO で導入している日立ソフトウェアエンジニアリング株式会社の「秘文」の可搬記録媒体への持ち出し制御機能を活用し，情報を持ち出す際にはあらかじめ申請内容を登録し，上長による事前承認を必須とする仕組みである。これにより，情報持ち出しに対する「見える化」および事前防止と事後確認による「統制の強化」を実現した。

以下，第２章で本システムを開発する契機となった情報漏洩事案の現状分析を行い，第３章でシステムの概要について説明し，第４章以降でその適用事例と今後のソリューションビジネスの展開について述べる。

２．　情報漏洩の実態

NPO 日本ネットワークセキュリティ協会の調査報告書[1)] によると，情報漏洩に関するインシデント件数は，2005 年以降減少傾向にあるが，2007 年にも 800 件を超す件数が発生している（図 1）。

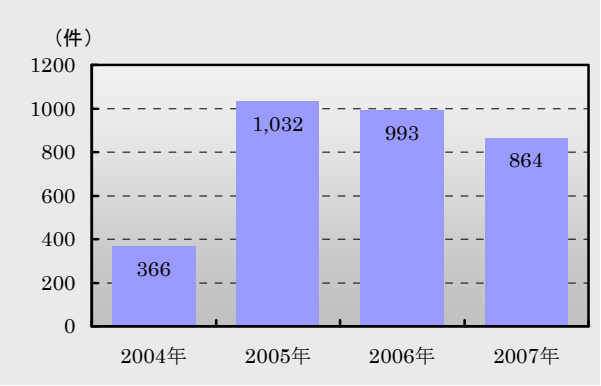

図 1　インシデント件数(2004～2007 年)

情報漏洩原因（図 2）を見てみると，「紛失・置忘れ」「盗難」が減少している一方で，管理ルールが明確化されていなかったために業務上に発生した「管理ミス」の割合が 2007 年に急増している。また，管理ルールに違反した「不正な情報持ち出し」の割合が，2005 年に急増している。

2005 年施行の個人情報保護法や 2007 年に強化された内部統制への取り組みが進められ，組織内情報の管理が強化された。しかし，セキュリティ意識が十分に浸透せず，情報漏洩が発生するケースが増加したことが想定される。

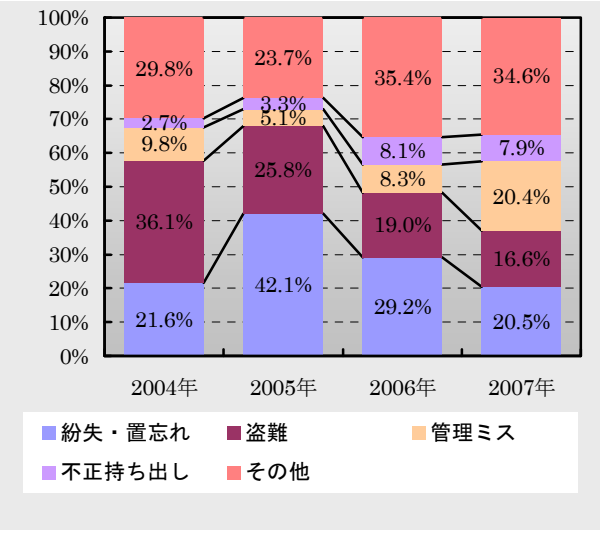

図 2　情報漏洩原因の経年変化

次に情報漏洩の経路を見てみると，PC 本体からの漏洩の割合は，2005 年から減少傾向にある。企業・団体などが外部へ持ち出すノート PC の HDD 暗号化やシンクライアント化といった，PC 本体の情報漏洩の対策が進んだことが一因と推測できる（図 3）。

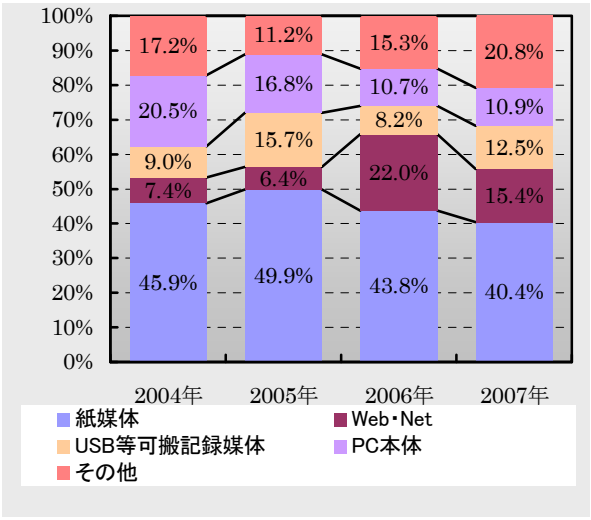

図 3　情報漏洩経路の経年変化

一方，USB メモリなど可搬記録媒体による情報漏洩の割合が，2006 年の 8.2%から 2007 年には 12.5%へ増加し，PC 本体よりも大きな割合を占めている。

要因として，可搬記録媒体の大容量化，低価格化が進んだことにより業務での利用者が増加したことが考えられる。また，情報漏洩対策の範囲が PC 本体にとどまり，可搬記録媒体を社外へ持ち出すケースに対する考慮や管理手法が不十分であることが考えられる。

これらの事実から，今後は PC 本体に加えて，可搬記録媒体に対する持ち出し制御，さらには，不正な持ち出しに対する管理を行う必要があるとのニーズが読み取れる。

3．　情報持ち出し申請システムの概要

3.1 機能概要

本システムでは，「秘文」の制御機能を活用し，一律禁止と設定することによって可搬記録媒体への書き出しができない仕組みを実現している。

可搬記録媒体での持ち出しが必要な場合には，本システムを利用して持ち出しに関する申請情報を登録し，上長の承認を得なければならない。

上長の承認により，ユーザアカウントが申請者に対しメールで通知される。ユーザアカウントにより「秘文」にログインすることで初めて，可搬記録媒体への書き出しが可能となる（図 4）。

本システムは上長による承認を必須とすることにより，不正な持ち出しによる漏洩リスクを低減するための有効な統制となる。

また，持ち出し申請の都度に有効期限を限定したランダムなアカウントを発行するワンタイム方式を採用することにより，他人による成りすましを防止している。ユーザ毎のパスワード管理も不要となり，運用負荷の低減に寄与している。

本システムで実現している仕組み，および仕組みを構成する機能（「秘文」の持ち出し制御機能を除く）については，当社にて独自に開発したものである。

申請から情報持ち出しまでの流れを図 5 に示す。

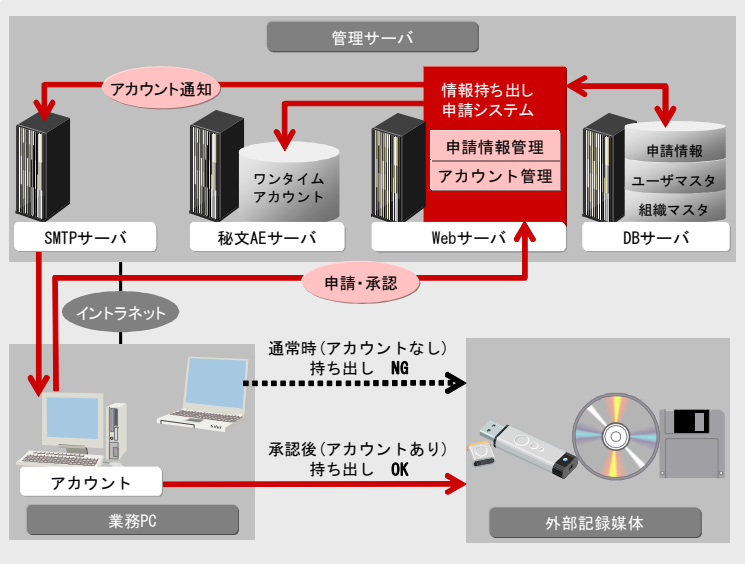

図 4　システム概要図

3.2 導入効果

(1) 情報持ち出しの「見える化」

情報持ち出し際に，申請が必須となり，いつ，誰が，何を，どこへ，何のために，どのように持ち出すかを第三者が検知できるようになる。持ち出しが不要な，または持ち出してはいけない情報は，申請を却下することで情報漏洩を事前に防ぐことできる。また，機密情報を持ち出す場合には，暗号化を必須とする，などの統制が可能となる。

申請情報と異なる不正な持ち出しに対しては，証跡管理の公開，申請情報と証跡をつき合わせる不正持ち出しの監査を定期的に行う，などにより統制することができる。

(2) 初期投資の極小化

本システムは，一つの部門に限定した導入も可能であり，順次，対象とする部門を広げていくことも可能である。また，すでに「秘文」を導入されているお客様であっても，一度にすべてのユーザを切り替える必要もなく，並行運用を行いながら，順次切り替えていくことも可能である。さらに，本システムを構成するサーバ群は，既存のサーバの活用が可能であり，初期投資の最小化を図ることができる。

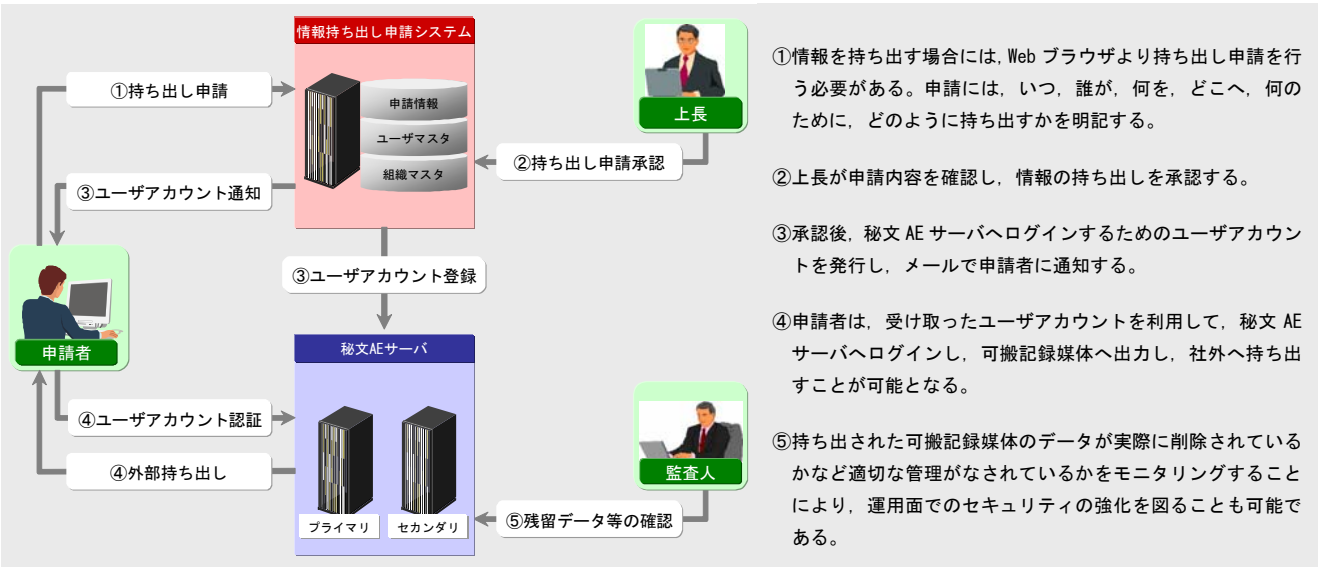

図 5　申請から持ち出しの流れ

４． 情報漏洩防止ソリューションの展開

1 件あたりの情報漏洩による想定損害賠償額は，50 億円を超える事例まで存在する。2007 年の特徴としては，インシデント件数が減少しているにもかかわらず、想定損害賠償が 4,570 億円から 2 兆 2,711 億円と大幅に増加した。また，情報漏洩の事後処理コストは，被害者数を 2,000 人とした場合に，964 万円と算出されている。[1)] さらに，情報漏洩による風評被害から事業存続が困難な事態に追い込まれる可能性がある。

情報漏洩の事前防止の強化および事後処理コストの低減を実現する本システムの導入を中心とした情報漏洩防止ソリューションとして，サービスメニューの整備を進めている。本システムは，機密性の高い情報を可搬記録媒体によりお客様へ提供する，自宅に可搬記録媒体により持ち帰って作業を行うといった場面の情報漏洩リスクを低減する特徴を持つ。そのため，特定の業種に依存しないシステムであると考えている。2008 年 9 月 1 日現在のサービスメニューを表 1 に示す。

表 1 情報漏洩防止ソリューション・サービス一覧

情報持ち出し申請システム導入ソリューション		
No	サービス	内容
1	導入支援	各サーバの環境構築、導入テスト支援
2	カスタマイズ	画面、他システム連携カスタマイズ
3	データ移行	社員マスタデータのデータ移行の支援
秘文導入ソリューション		
No	サービス	内容
1	導入支援	秘文移行計画、環境構築、導入テスト支援
2	パラメタ設計	各クライアントへの配布プログラム設計
3	運用設計	秘文の運用をお客様の環境に応じた設計

4.1 情報持ち出し申請システム導入の流れ

本システムの導入にあたっては，大きく下記 2 ステップをとる。

(1) 秘文移行計画の作成

本システムを導入するにあたり，すでに「秘文」を導入し，運用されているお客様向けに，システム移行計画を提供する。これは，本システムを効果的に活用するために外部持ち出し制御を行う秘文 AE サーバの設定を変更する必要があり，設定状況に応じて秘文移行計画を作成するものである。

「秘文」が未導入であれば，本システムを利用するにあたって印刷制御，暗号化の区分，持ち出し可能な可搬記録媒体の制御，運用設計など必要な設計を行う。

(2) 情報持ち出し申請システムの構築導入

秘文移行計画に基づいて，秘文 AE サーバの設定方法を検討し，システム構築を行う。また，本システムは利用者情報を保持するユーザマスタ，組織マスタを必要とするため，既存の社員マスタなどからデータ移行を行う。

また，画面のカスタマイズやお客様のご利用のシステムとの連携が必要な場合には，本システムのカスタマイズを行う。

５． 導入事例

本システムの導入事例として，情報通信業 A 社への導入事例を紹介する。

5.1 導入目的

一般的に，情報漏洩対策を強化すると，社員の業務効率の低下と運用負荷の増加を招くとされている。

セキュリティレベルを向上させるためには，求められるセキュリティレベル，業務効率，運用負荷の 3 点に配慮したセキュリティポリシーを設定することが有効である。しかし，業務の変更や組織の異動などが行われる度にセキュリティポリシーの見直しが発生し，運用負荷が大きくなるという問題がある。

そういった問題に対し，日立 TO は A 社に最適なセキュリティポリシーの検討を行った。通常時には持ち出しを不可とし，上長承認後にだけ持ち出しを許可するという単純化したセキュリティポリシーを採用した。単純化することにより，運用負荷が低減される他，担当者のセキュリティ意識の啓蒙にもつながる。

そのセキュリティポリシーを実現するための仕組みとして「秘文」を前提とする本システムをご導入いただくこととなった。

5.2 システム導入

初期投資を抑制するため，本システム用に新たにハードウェアやソフトウェアを調達することは極力避け，既存の情報資源を活用した。

本事例での主なカスタマイズ内容として，お客様社内システムとのシームレスな運用を行いたいとのご要望に応えるため，シングルサインオン基盤との連携機能を新規に開発してご提供した。

5.3 適用範囲の拡大

本システムがスモールスタートを可能としている仕組みであることを利用し，すべてのユーザに対して同時に展開するのではなく，業務への影響や効果を見定めながら部門別に展開を行い，徐々に適用する部門を拡大することとしている。

6． 今後の展開

IDC Japan 株式会社によるとセキュリティ／脆弱性管理製品の 2007 年の市場規模は，186 億円，2012 年には 349 億円となり，セキュリティソフトウェア市場の中で最も高い成長率で拡大すると見られている。[2)]

高成長の市場における今後のターゲットとして目指すべき業種について検討する。情報漏洩は，個人情報・機密情報を保有する団体が対象となるため，すべての業種が対象となる。しかし，インシデント件数，漏洩経路を見ると業種別の特徴がある。

2007 年の業種別のインシデント件数では，「公務」「金融・保険業」「情報通信業」「教育・学習支援」「医療・福祉」の順で高い。本システムは，可搬記録媒体による情報漏洩に対して有効であるため，漏洩経路における可搬記録媒体に着目する。上位 5 業種の「業界全体の可搬記録媒体による漏洩割合と業種別の可搬記録媒体による漏洩割合との差」を X 軸，「2005 年から 2007 年のインシデント件数の伸び率」を Y 軸とした散布図を以下に示す。各象限は次のように定義できる（図 6）。

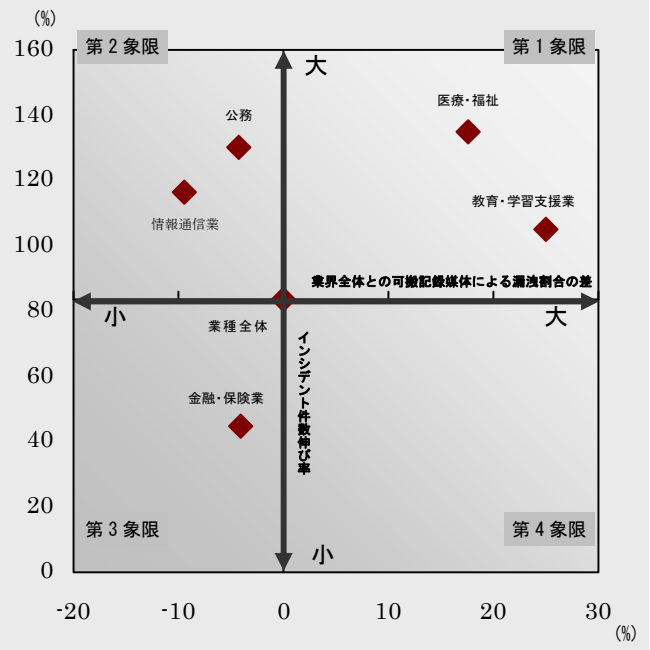

図 4 業種別散布図 [1)]

それぞれの象限について，インシデント件数伸び率（以下「件数伸び率」），業界全体との可搬記録媒体による漏洩割合の差（以下「漏洩割合」）に着目し，今後の展開の方向性を述べる。

第 1 象限は，件数伸び率も漏洩割合も「大」であり，「医療・福祉」「教育・学習支援業」が該当する。可搬記録媒体による漏洩事故も多く，また件数も増大しており，早急な対策を必要としている象限といえる。本システムを導入することにより，情報漏洩リスクの低減が最も期待できる業種であり，積極的に展開を図る。

第 2 象限は，件数伸び率「大」であるが漏洩割合は「小」であり，「公務」「情報通信業」が該当する。可搬記録媒体での情報漏洩リスクへの対応も含めて，総合的なセキュリティ強化の提案を必要とする象限である。

第 3 象限は，件数伸び率も漏洩割合も「小」であり，「金融・保険業」が該当する。可搬記録媒体での情報漏洩に対するセキュリティ対策が物理的にも人的にも進んでいる象限と考えられる。

第 4 象限は，件数伸び率「小」であるが漏洩割合は「大」であり，上位 5 業種の中には該当業種が存在しない。可搬記録媒体による情報漏洩リスクが高い象限であり，本システムの効果が高い象限である。

7．おわりに

情報漏洩防止をはじめとするセキュリティ対策については，投資対効果がわかりにくい，業務の効率低下を招くといった否定的な意見が少なくない。しかし，セキュリティ対策を怠ったばかりに，情報漏洩による信用失墜により市場からの撤退を余儀なくされた事例が存在することも事実であり，セキュリティレベル向上のための投資の必要性は年々高まっていくと予想している。

今後は，継続的な市場ニーズの把握とお客様の声を元に，より多くのお客様にご利用いただけるように，本システムのさらなる機能向上とソリューションメニューの充実を図っていくことを考えている。今後は，情報漏洩対策が有効な部門へのポイント導入による「初期投資の最小化」と，情報持ち出しの「見える化」による統制強化を実現する日立 TO のソリューションの優位性をさらに高め，社会の情報セキュリティレベル向上へ貢献していく所存である。

参考文献

1)NPO 日本ネットワークセキュリティ協会「２００７年情報セキュリティインシデントに関する調査報告書 Ver. 1.2」

2)IDC Japan プレスリリース
国内セキュリティソフトウェア市場動向（アイデンティティ／アクセス管理、セキュリティ／脆弱性管理製品）を発表
http://www.idcjapan.co.jp/Press/Current/20080805Apr.html

荒井　崇之　　2000 年入社
公共ソリューション本部
公共第一ソリューション部 公共 15G
情報漏洩防止ソリューション提供
tarai@hitachi-to.co.jp

櫻井　浩　　1997 年入社
公共ソリューション本部
公共第一ソリューション部 公共 15G
官公庁向けソリューション提供
sakku@hitachi-to.co.jp

小松澤　美喜夫　　2006 年入社
公共ソリューション本部
公共第一ソリューション部 公共 15G
情報漏洩防止ソリューション提供
mikio.komatsuzawa.01@hitachi-to.co.jp

佐藤　義人　　1985 年入社
公共ソリューション本部
公共第一ソリューション部
官公庁向けソリューション提供
yoshito.satou.01@hitachi-to.co.jp