セキュリティサービス最前線 ――情報セキュリティの課題とその解決に向けて

戸 木 貞 晴

要 約 セキュリティ管理策の実装は、もはや、従来通りのセキュリティ投資方法だけが選択肢ではない。クラウドコンピューティングは、セキュリティ管理策の機能をサービス化し、ユーザにセキュリティサービスの購入という選択肢を与えた。サービス化されたセキュリティ機能は、その機能のみに留まらず、コスト削減、効率的なIT運用支援、脅威と脆弱性情報の有効的な共有など、多くの付加価値も提供する。

昨今、日本企業は、グローバル化、もの作りからサービス化へ、新しいビジネスモデルの創出要求など、産業構造の変化が求められている。その変化には、常にリスクが伴う。その不確実性、曖昧さを減らす役割を果たすのが情報であり、曖昧さの減少分が情報量に相当する。したがって、競争が存在する限り情報は適切に保護するべきであり、方法を問わずセキュリティ管理機能を合理的に実装しなければならない。本稿では、萌芽しつつあるセキュリティサービスの特徴と限界を記述し、具体的事例の導入経緯とその効果まで言及している。

1. はじめに

グローバル化による産業構造の変化は、日本企業の次世代への針路を示唆している。その一つの指針は、最大の強みであった加工組み立て領域から、素材開発とビジネスモデル創造及び消費とサービスの領域拡充への転換である。いずれの領域も、関係者が相互に知恵を出し合い、アイディアを交流させ、接合することで新しい技術革新やビジネスモデルが生み出されていく。加えて、組織内のみならず、開発期間の短縮とコスト抑制を狙い、外部からの技術、アイディアを相互に取り入れるオープンイノベーションも主流になっていくだろう。このように、創造された情報は、商機を生み出す財産となる。

一方、その情報の流出は、企業や組織に深刻な悪影響を及ぼす。軍需技術であれば、国家安全保障に影響し、技術者の士気に著しい低下をもたらす。最新の技術情報の漏洩は、企業競争力の逸失、大切な顧客情報であれば、顧客に深刻な心痛と漏洩元企業のイメージダウンに結びつく。

デジタル技術の発達は、情報の量を問わず伝達を容易にすると同時に情報漏洩リスクも高める。グローバル化による人材の国際化は、人種、国家、モラルに至るまで熟慮された情報セキュリティ対策と教育を必要としている。

本稿では、企業が保有する情報システムに実装する従来型情報セキュリティ対策から、クラウドコンピューティングがもたらす情報セキュリティサービスを購入する時代への変化を記述する。また、BITS2010[*1]にて公開した具体的なサービス型セキュリティソリューションの適用事例として、クラウドコンピューティング基盤を利用した日本ユニシス独自の情報セキュリティ教育e-ラーニングソリューションを紹介する。もうひとつは、情報セキュリティ強化とユーザ利便性向上、さらにコスト削減に結びつけたプリント管理ソリューション事例を紹介する。最後に、情報セキュリティ領域におけるサービス化の動向について述べる。

2. 情報セキュリティ管理策の実装方法の変化

業種業態を問わず企業経営とは、経営戦略に従い、経営目標の達成のために、経営課題の解決を図り、企業活動を行うことである。そのプロセスで活用する情報システムに流れる情報は他の情報システムが持つ多くの情報と有機的に交換、結合、循環、形成され、企業競争力の源泉となっていく。その情報は、故意、未必の過失、過失を問わず漏洩、流出、ヒューマンエラーなどの脅威に直面している。企業経営者は、それらの脅威から情報を守り、リスクの顕在化を阻止するために、有効かつ効率的なコントロールを適用し続ける仕組みを構築しなければならない。まずは、情報システム内に存在する情報を、重要度に応じ分類し、物理的な情報の保管場所、収受が行われるネットワーク、アクセス権とログ管理に至るまで、情報の流れを確認し、脅威と脆弱性を考慮し、網羅的なリスクアセスメントを実施する。その結果に応じ、具体的なセキュリティ管理策を実装していかなければならない。従来は、自社で調達したセキュリティ管理機能を、自社要員もしくは委託要員で運用する方法が主流であった。しかし、クラウドコンピューティングを利用し、セキュリティ管理策の実装をサービスで提供する「Security as a Service（SaaS）」がマーケットに萌芽している。2010 年以降、このサービス型セキュリティ管理策モデルが、従来の自社調達方式に加えて、有望な選択肢になりつつある。

2.1 セキュリティ管理策の実装運用の類型

企業における情報セキュリティ管理策の実装方法とその運用例を、表 1 に示す。タイプ 1 と 2 は、従来型の情報システムのインフラ調達及びシステム運用、情報セキュリティ管理策の実装と運用例である。いずれも、自らセキュリティリスクアセスメントを行い、リスクに応じ、その管理機能を持つソフトウエア、アプライアンスなどを調達、運用ルールを策定・実装し、自社もしくは委託先が運用するモデルである。これが、従来から行われている情報セキュリティ管理策の実装である。タイプ 3 は、「ソフトウェアの機能をネットワーク経由で利用する」という形態、つまり「SaaS」（Software as a Service）、「ASP」（Application Service Provider）である。ユーザは、サービス仕様書、利用規約等の記述内容からセキュリティ管理策の実装とその運用状況や、自社が要求するセキュリティポリシーに適合しているか否かを確認し、契約する。なお、タイプ 4 は、セキュリティ機能に特化したサービス（Security as a Service）である。

表 1　情報セキュリティ管理策の機能実装例

タイプ	情報システム機器もしくは機能の調達方法		セキュリティ管理策の実装場所	セキュリティ管理策の運用	セキュリティ管理策の実装と運用方法
1	購入もしくはリース、レンタルにて調達し自社管理下に設置		自社ビル内など	自社運用	セキュリティアセスメント結果に従い、必要なセキュリティ管理策の機能を、自社で調達、運用を行う従来型の実装方法である。 したがって、セキュリティ管理策用の機器選別、調達、実装、運用は、自らが投資を判断し、ＰＤＣＡを維持する必要がある。
2	ハウジングサービス、ホスティングサービス		データセンタ（クラウドもあり）	運用委託	
3	SaaS/ASPサービス（多様なソフトウエア機能を提供）		サービス提供社内、データセンタ（クラウド）等	サービス仕様書（セキュリティSLAに依存）	SaaS/ASP事業者のサービス仕様書（セキュリティSLA）が、自社の要求するセキュリティレベルに合致しているか否かを確認する必要がある。
4	機能特化型ｻｰﾋﾞｽ	Security as a Service（セキュリティ機能が主体のSaaS）	サービス提供社内、データセンタ（クラウド）等		多種多様なセキュリティコントロール機能をサービスとして提供する。セキュリティ管理機能をサービスとしてニーズに応じ購入できる。 セキュリティサービス自体のセキュリティレベルは、セキュリティSLAに準拠する。

2.2　サービス型セキュリティ管理策の萌芽

広帯域インターネット環境と仮想化ソリューションの普及拡大、ハードウエア性能の劇的な向上は、クラウドコンピューティングを生み出した。それは、巨大な情報処理能力、リソース融通の柔軟性と拡張性を持つ。ユーザは、リソース要求のピーク時を起点として考える投資計画の策定から脱却し、予期せぬリソース追加要求時の性能不足の懸念から解放される。これらの優位性は、企業の情報システム投資の意思決定に大きな影響を与えている。

図1は、セキュリティ管理策実装の概念図である。従来、セキュリティコントロールの機能は自社管理下の設備への実装（図1のAに相当）、または、データセンタに委託中の情報システムに実装（図1のBに相当）する方法が主流であった。しかし、昨今、サービスとしてのセキュリティ機能（図1のCに相当）を組み合わせて利用すること、もしくは、図1のAやBの代替とすることが検討されつつある。これが、表1のタイプ4に示す「Security as a Service（SaaS）」である。

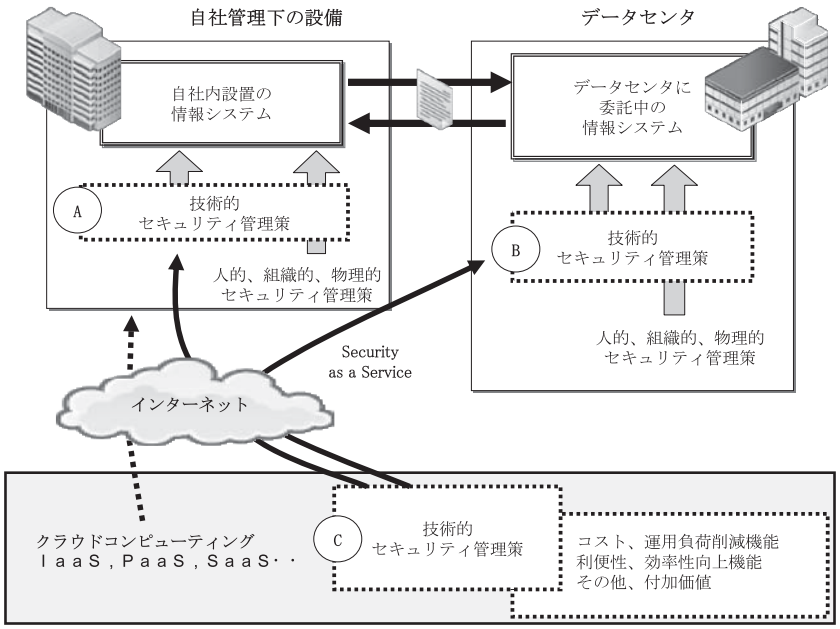

図1　セキュリティ管理策実装の概念図

2.3　サービス型セキュリティ管理策の優位点

セキュリティ管理策をサービスとして購入する場合と、自社で調達し運用する場合もしくはデータセンタ運用会社に他の運用と合わせてセキュリティ運用を委託する場合とを比較すると、以下の点で前者が優れている。

1)　コスト削減、節減効果

ⅰ）セキュリティ関連資産のライフサイクル管理が不要

自社設備内への機器設置（図1のAに相当）、データセンタへの機器設置（図1のBに相当）は、セキュリティ機器、ソフトウエアなどの調達が必要になる。一方、セキュリテ

ィ管理策をサービスとして購入した場合は、直接的な投資及びそれに伴う導入費、保守費などが不要となる。特に、脅威と脆弱性の変化に伴い、要求される機能が変化するセキュリティソフトウエアは、データベース製品やミドルウエア製品と比較すると、プロダクトライフサイクルが短いため、サービスとして購入すれば中長期的にもコスト削減効果は高い。

ⅱ）セキュリティ運用工数の軽減が見込める

自社運用もしくは委託運用を想定した場合、規程の作成、具体的な運用手順の作成、セキュリティ事故事件発生時のシミュレーションの実施、さらに、継続的な改善等を考慮すると運用人材の育成、運用委託条件の合意まで相応の工数が必要になる。セキュリティ管理策をサービスとして購入する場合は、予めサービス内容、サービスレベル、契約条件などが明示されているため、自社のセキュリティ管理上の要求と突合し、過不足を検証すればよい。したがって、管理策の実装準備から具体的な運用に至るまでの総工数で考えれば、サービス型の選択が有利である。

ⅲ）規模のメリットが得られる

セキュリティサービスの提供者は、契約見込みユーザ数を想定し、価格設定をしている。言い換えれば、サービス提供者は、製品調達コストと運用コストを契約見込みユーザ数で共有することで、規模のメリットを出している。したがって、自社単独で調達、運用する場合と比較すれば、サービスとして購入する方が低価格になる場合が多い。

2） 高い効率性と有効性

セキュリティサービスの提供者は、セキュリティ専門技術者を豊富に抱えているため、新たな脅威と脆弱性を迅速に把握できる。セキュリティ対策を本業としない自社要員は、それらの情報を迅速に入手し、即時、管理策の追加や変更等を実行することが、現実的には難しい。日本ユニシスでは、CISSP、システム監査技術者、情報セキュリティ監査人などの有資格者が、セキュリティサービスの企画、実装、運用に参加している。

3） 高い柔軟性と融通性

セキュリティサービスの契約は、月額払い、年払い等も選択でき、運用経費予算で実現できる。また、サービス契約の中止、サービス内容の変更や追加などにも柔軟に対応できる。

4） 本来の業務に専念できる

セキュリティは守られて当たり前である。情報システム運用が主たる業務であり、補助的業務でセキュリティを任されている場合、そのモチベーションの維持は難しい。基幹となる業務システムやERPシステムなどのシステム構築や運用は評価され易いが、セキュリティは何も事件事故がないことが良いことであり、セキュリティ担当者は評価されにくいからである。セキュリティサービスを購入すれば、補助的業務であるセキュリティから開放され、本来の業務に専念できる。

5） 豊富な付加価値サービス

ⅰ）セキュリティ管理策の機能に加え、セキュリティ以外の機能を付加するサービスが増えている。セキュリティ単機能だけのサービス購入申請は、売上向上や費用節減などの効果を持つ他のサービス購入に比較して、高い優先順位を獲得しにくい。したがって、セキュリティ管理機能に加え、有効な付加機能が付保されている場合、社内における稟議なども通過し易いのが実態である。

ⅱ）セキュリティサービスの運用は、必要な技量と経験を持つ専門技術者が担当している。ゆえに、定期的に提出される報告書等は、他社事例とのデータの比較、専門技術者の意見などが示され、脅威や脆弱性の早期発見に役立つなど、有効に利用できる場合が多い。

2.4　サービス型セキュリティ管理策の限界

サービス型セキュリティ管理策実装にも限界はある。サービス型のメリットと限界を認識し、効率性、有効性、コストパフォーマンスを考慮し、自社の情報システムに実装していくことが重要である。考慮すべき点を以下に挙げる。

1)　企業内部のネットワークに対するセキュリティ要求

ⅰ）リアルタイム処理を要求するセキュリティ機能の場合、インターネット経由のサービスは遅延が伴う可能性もあり、相応しくないケースがある。

ⅱ）内部ネットワークへのアクセスが必要な場合、外部からの接続を許可すると、その通信自体が脆弱点となるケースがある。

ⅲ）標準のインターフェース、通信、フォーマット（HTTP、HTTPS、XML、SMTP 等）以外を必要とするケースは、ポートの解放や新たな投資が必要となる場合がある。

2)　企業内部にセキュリティ機能を設置、導入すべきセキュリティ要求

ⅰ）非常に高い機密性を要求する情報資産を取り扱う情報システムの場合、自社所有のデータセンタを含め、自社管理下に設置導入するケースが多い。このような場合、外部ネットワークを経由したセキュリティサービスに接続すること自体が困難である。

ⅱ）セキュリティ機能に、自社専用もしくは著しくカスタマイズが必要な場合、セキュリティサービス提供者が、スケールメリット、共有化メリットを出すことは難しく、ユーザは、コスト優位性を得ることができない可能性もある。

ⅲ）必要とするセキュリティ機能が、汎用的ではなく、所属する業界においてさえ標準的ではない場合も、コスト優位性を得られない可能性がある。

3.　セキュリティサービスの具体的な適用事例

日本ユニシスでは、2010 年からサービス型セキュリティソリューションを積極的に展開している。一例目は、クラウドコンピューティングを利用した e-ラーニング基盤を使った「iSECURE e-ラーニングセキュリティ教育サービス」を 3.1 節で紹介する。このソリューションの特徴は、二つある。まず、クラウドコンピューティングの利点である柔軟なインフラ基盤を利用し、数十人から数十万人の企業まで対応できること、次に、企業や組織の社風やセキュリティポリシー、経営陣の意向に沿ったオリジナルセキュリティ教育コンテンツを提供し、結果として受講者の高い理解度を得られることである。

二例目は、印刷物による情報漏洩を防止するセキュリティ機能に加え、プリンタ、複合機など出力機器のランニングコストを削減する「iSECURE プリント管理サービス」の具体的な事例を 3.2 節で紹介する。

3.1　iSECURE e-ラーニングセキュリティ教育サービス

3.1.1　セキュリティ教育の理想と現実のギャップ

情報セキュリティにおいて、重要な対策のひとつにセキュリティ教育がある。特に、ISMS、プライバシーマーク認証取得組織は、年に一度以上は、全員にセキュリティ教育を実施し、セキュリティリスクの変化を周知徹底しなければならない。しかし、日本ユニシスの営業活動を通じ、セキュリティ教育には、課題が山積していることが判明した。多くの企業や組織は、効率的、効果的なセキュリティ教育が実施できずに悩んでいる。セキュリティ教育に関する課題を整理したものが表2である。

表2　セキュリティ教育の理想と現実

	理想とするセキュリティ教育	各社の現状のセキュリティ教育実態ヒアリング結果
集合教育	全員受講すること	・集合教育の講師、会議室等の手配が面倒である ・参加者への講義案内、出席確認、資料準備が面倒である ・講師料や会議室予算、資料印刷予算の確保等が煩わしい ・集合教育は、指定時間にその場所にく必要がある ・参加しにくいので全員が受講終了になりにくい ・営業職を筆頭に受講率が低い ・試験等の問題作成、採点や集計が面倒である ・セキュリティ教育が実施できる社内人材がいない ・自社要員では講師はできず、教育用資料も作成できない ・海外勤務社員への集合教育はコスト高である ・海外拠点への集合教育は事実上難しい ・全国拠点へ出張するセキュリティ集合教育は大変
	適切な講師を手配できること	
	妥当な金額で講師を手配できること	
	容易に予約できる会議室を確保できること	
	適切な価格で会議室が確保できること	
	参加者が、容易にアクセスできる場所を確保できること	
	質疑応答を通じ疑問点をその場で解消できること	
	受講者は緊張感を持って受講できること	
e-learning基盤領域	e-learning設備を柔軟に利用できること	・自社でe-learning設備投資を行い維持してきたが、社員が増え、ID数、コンテンツ保管容量が足りない ・同時アクセス数が限られ社員全員のIDが確保できない ・設備が老朽化し、新しいコンテンツが搭載できない ・契約中のe-learning事業者のコストが高い ・テストやアンケートの集計ができない ・テスト問題が、いつも同じ問題になってしまう ・ユーザのPCに専用エージェントをいれなければならない ・今利用しているASPサービスは、同時接続数が少ない ・500人以上の大規模アクセスには耐えられない ・e-learningの基盤が安定して稼働していない ・メニューが外国語対応していない ・運用代行サービスがない ・操作教育サービスがない ・初期設定運営サービスなど豊富なメニューがない ・コンサルティングを含んだサービスがない
	e-learning設備は、妥当と思われる範囲で新しいこと	
	e-learning設備は、合理的な範囲で遅延等が発生しないこと	
	e-learning設備の利用料は、妥当な金額であること	
	受講者は、24時間いつでもどこからでも利用できること	
	受講者は、インターネット環境とブラウザのみ必要であること	
	e-learning設備への受講者登録が簡単であること	
	e-learning接続にあたり、セキュリティが考慮されていること	
	セキュリティ推進者は、受講率、進捗状況を逐次確認できること	
	受講者は、繰り返し学習ができること	
	アンケートやテストなど結果の集計が簡単にできること	
教育コンテンツ領域	教育コンテンツは自社規程に則り、最新であること	・教育コンテンツが古く、文字ばかりでつまらない ・教育コンテンツの利用料が高すぎる ・コンテンツに動きも音声もなく、興味が湧かない ・中国拠点の社員に受けさせたいが中国語対応できない ・海外拠点向けに英語コンテンツが欲しい ・全社員同一のコンテンツで効果薄い ・新人も幹部社員も同じコンテンツで効果が薄い ・採点結果一覧が作れない ・今の契約業者では、オリジナルコンテンツ作成は無理 ・独自の理解度確認問題を作成したいが支援して欲しい ・教育理論に基づいたコンテンツが欲しい ・現在の教育資料は、寄せ集め情報ではないか ・やる気にならないコンテンツである ・受講していて楽しくない
	教育コンテンツは、最新の事故事件事例が反映されていること	
	教育コンテンツは動きやイラストなど多用し、飽きないこと	
	教育コンテンツは、多言語対応可能であること	
	教育コンテンツは、音声付、音声無し等に対応可能であること	
	教育コンテンツは、職位毎、職種毎等適切であること	
	教育コンテンツには、テストが可能であること	
	テストは、採点結果が集計できること	
	テスト結果の統計データから自社の弱点等が理解できること	
	できれば、教育コンテンツは、組織ごとに優先度があること	
	できれば、教育コンテンツはセキュリティ専門家が企画すること	
	できれば、ＡＲＣＳモデルに基づいて制作することが望ましい Ａ：注意、Ｒ：関連性、Ｃ：自信、Ｓ：満足感	

3.1.2　日本ユニシスが推奨する課題解決方法

日本ユニシスでは、表2に示す情報セキュリティ教育に関する課題を解決すべく、2010年に「iSECURE e-ラーニングセキュリティ教育サービス」をラインナップに加えた。

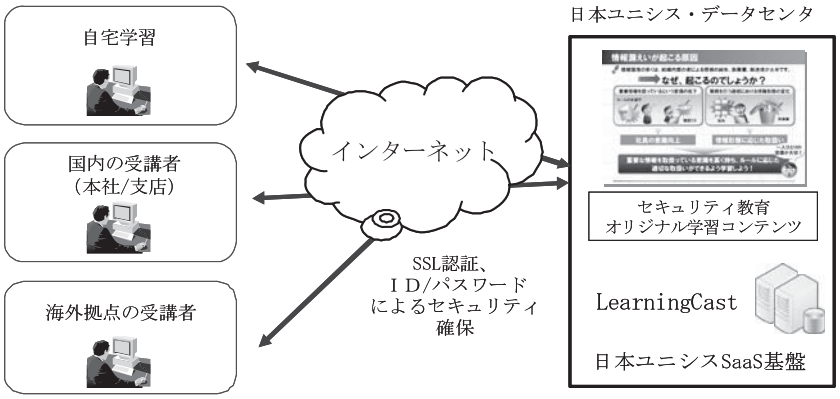

図 2　日本ユニシスが提供する e-ラーニング概要図

図 2 が、日本ユニシスが提供する e-ラーニング概要図である。e-ラーニング基盤に日本ユニシスの SaaS プラットフォームを採用、システム稼働基盤に「LearningCast」アプリケーションを搭載した。その環境上に、顧客ごとに作成されたセキュリティ教育コンテンツを載せている。登録された受講者は、インターネット経由で、いつでも、どこからでも受講することができる。要求される PC の性能は、オフィスユースで使われているごく一般的な性能で十分であり、必要なソフトウエアは Web ブラウザだけである。必要となる通信回線速度も ADSL 程度で十分なため、地方拠点や個人の自宅等でも受講できる。e-ラーニング基盤には、クラウドコンピューティングを利用しているため、大規模なユーザ数のアクセスが想定される場合でも、CPU、メモリなどの追加に柔軟に対応できる。

なお、セキュリティ教育コンテンツは、顧客の要望、予算に合わせて 3 種類用意している。顧客の社風、組織、セキュリティポシリー等に応じ、セキュリティ教育コンテンツを作り上げる「フルカスタマイズコンテンツ」、「汎用コンテンツ」の一部を改訂、追記する「セミカスタマイズコンテンツ」、それと一般的な「汎用コンテンツ」である。フルカスタマイズの場合、企業組織ごとのセキュリティ教育ニーズ、教育予算、教育スケジュールなどを考慮し、最適な教育プランの作成までのコンサルティングも実施している。いずれのコンテンツも、受講者の理解度チェック問題、海外の勤務者及び現地採用のローカル社員向けに 43 ヶ国語への翻訳（オプション）などにも対応している。

3. 1. 3　ソリューション適用事例

主要事例を表 3 に示す。いずれも、日本ユニシスの専任セキュリティコンサルタントがシナリオを作成し、プロイラストレータ、プロナレータを登用したセキュリティ教育コンテンツが高く評価されている。加えて、他社と比較し、提案価格が圧倒的に有利であったことが、事例を問わず選定ポイントに入っている。ある会社では、2000 人の社員に 3 ヶ月の e-ラーニングによるセキュリティ教育を実施した。日本ユニシスが提供する最新汎用コンテンツをベースに独自に作成した専用オリジナルセキュリティ教育コンテンツの利用、2000 ユーザ ID の e-ラーニング利用料、30 問の理解度テストを含め、一人当たり月額 1,000 円であった。本ソリューションのコストパフォーマンス、高い品質の教育コンテンツを、ぜひ他社と比較して頂きたい。

表３　iSECURE e-ラーニングセキュリティ教育サービス適用事例

業種, 対象数	課題・ニーズ	課題解決方法	導入効果	選定ポイント
公共サービス（大企業）１万人	新しく策定したセキュリティポリシーを短期間に全員に周知徹底する	（従業員）e-ラーニング（管理職）集合研修 対象、方法を分けて実施 オリジナルコンテンツ採用	目標期間（３ヶ月）に、全員受講完了 理解度テスト全員通過	専任セキュリティコンサルタントによる完全オリジナルコンテンツ、大規模人員（１万人）に対応可能なe-ラーニング基盤の２点を高く評価
ソフトウエア（大企業）２０００人	ＩSMS，プライバシーマーク更新の為、全従業員へのセキュリティ教育を適切なコストで実施したい。中国勤務者への教育の徹底	セミカスタマイズコンテンツとe-ラーニングを採用	目標期間（３ヶ月）に、全員受講完了 理解度テスト全員通過 他社e-ラーニング教育コストに比較し約半減	役員のメッセージを加え、特に、教育したいポイントを加えたセミカスタマイズコンテンツと中国語への対応を高く評価され、さらに、他社と比較し、お客様に有利な提案価格を評価
製造業（中堅企業）３００人	全国の多拠点に担当社員が出張、セキュリティ教育を実施していた。合理的、短期、低コストで実現したい。	汎用コンテンツを使ったe-ラーニングを採用	旅費交通費大幅節減、全員受講完了、 理解度テストとアンケートによる意見収集	全国多数拠点、自宅からでも受講可能なe-ラーニング、２０１０年作成の最新汎用コンテンツの提供、目標予算をクリアした提案価格を高く評価

3. 2　iSECURE プリント管理サービス

3. 2. 1　オフィスのプリント管理におけるセキュリティ管理の必要性

情報漏洩リスクの課題として、まず、紙媒体によるものがある。ファイルサーバに保管されている電子データは、「need to know の原則」つまり、情報は知る必要のある人のみに伝え、知る必要のない人には伝えないという原則に従い、アクセス権を設定しているはずである。しかし、ひとたび印刷された文書は、物理的な紙そのものが流通してしまうことで、情報漏洩に繋がってしまうケースが多い。日本ネットワークセキュリティ協会の調査においても、情報漏洩の原因となった媒体の 72%は、紙であると報告されている[1]。電子データではアクセス権が付与され、ログ採取が実施されていたとしても、印刷された紙媒体になると、印刷した人を特定できず、情報漏洩ルートの追求が難しい点に問題がある。その防止策として、業務のペーパレス化があるものの、その推進は障壁が高く、現時点では、文書印刷を全面的に制限することは、生産性低下、業務効率の低下など業務遂行の妨げになる可能性が極めて高い。加えて、個人情報保護法全面施行以後、ノート PC、電子媒体の管理が厳しくなり、紙媒体への回帰が強くなっている。つまり、大半の企業は、情報セキュリティ強化の為に文書印刷の制限を強化したいものの、その実現は、業務効率の著しい低下を招くのではないかという懸念を抱え、ジレンマに陥っていると言えよう。

3. 2. 2　オフィスのプリント管理におけるコスト管理の必要性

オフィスには、プリンタや複合機（Multifunctional Products（MFP)、ファックス、スキャナ、プリント機能などが統合された機器）が、数多く配備されている。多くの企業では、プリンタは情報システム部、複写機や複合機は総務部の管理など、別々の部門で管理されている場合が多い。その結果、出力機器関連のコストを全社的に把握することが難しい。使用状況（印刷枚数、印刷内容、使用頻度など)、保有台数、設置場所、無許可接続プリンタなど管理すべき項目は多いが、それを担当する管理部門すら確定していない企業も多数存在する。特に、カラー印刷のコストは、モノクロ印刷に比較し数倍以上であるが、運用ルールを決め、全社的な管理を実現している企業は非常に少ない。このように、出力関連機器に関する全社的なコスト管理は、実現できていないのが現実である。

さて、オフィスにおけるプリント出力に関するコスト削減を考える以前に、出力関連のコスト構造を知らなければならない。現在、多くの企業で契約されている出力関連の契約方式は、表4に示すように大きく3分類できる。コスト削減方法は、自社の出力機器類の調達及び運用契約によって異なり、単純に印刷枚数を減らす、トナーをリサイクル品に変える、契約単価を見直すなどが考えられる。

表4　オフィスにおける印刷機器の契約方式例

	機器調達 契約方法	特徴	主たるユーザ層	ユーザメリット	ユーザデメリット
①セルフサービス式	・機器は一括購入もしくはリース、レンタル	・機器調達後、消耗品の購入、メンテナンス依頼などは自社で実施する ・印刷コストの合計額は、印刷枚数ごとの課金ではなく、機器調達費と消耗品コストの合計となるケースが多い	・SOHO ・中小企業	・トナーなど、消耗品にリサイクル品を利用することができる	・プリンタの選択が面倒
	・消耗品の購入や入れ替えは自社で行う			・プリンタ性能の向上、低価格化によりリプレイス負担が年々軽減	
	・保守は必要に応じ契約（有償/無償） ・スポット保守可能			・最も安い消耗品を選択し調達できる	・トラブル時は、保守契約に依存する
②パッケージ契約式	・機器は、購入、リース、レンタルで調達、消耗品も同業者一括契約	・機器調達後、消耗品の購入、メンテナンス依頼なども一括契約となるため、消耗品、メンテナンスなども業者が実施してくれる	・中小企業 ・大手	・契約窓口が、一元管理されているので、安心できる ・消耗品入れ替え、メンテナンスなど一任の為、安心である	・一括契約の為、コスト削減方法は印刷枚数を減らすしかない
	・消耗品（トナー、紙、ドラムなど）は、必要時に配達してくれる				・リプレイスは、契約一括変更となり、面倒
	・保守、メンテナンスサービス込み				・通常、純正トナーしか購入できない（リサイクル品が使えない）
③従量課金契約	・機器は、購入、リース、レンタルで調達、消耗品も同業者一括契約	・一枚○円というカウンター数による課金体系を採用（使っただけ払う） ・一枚当りの単価交渉は、月間印刷総枚数を鑑み設定される方式 ・消耗品、メンテナンスなど一括一任	・中小企業 ・大手 ・超大手	・契約台数によるが、機器調達のイニシャルコストは相当低い	・カウンター方式の為、コスト削減方法は、印刷枚数を減らすしかない
	・消耗品（トナー、ドラムなど）は、メーカが必要時に交換してくれる			・1枚○円契約の為、印刷サイズ（A3）によっては、買得感がある	・月間印刷総枚数により①②の方法のが低コストの場合もある
	・保守、メンテナンスサービス込み			・消耗品入れ替え、メンテナンスなど一任の為、安心である	・トナーなど、消耗品にリサイクル品が使えない

3.2.3　オフィスにおけるプリント管理の課題と解決ソリューション

日本ユニシスでは、オフィスにおける紙媒体への出力に関するセキュリティ管理、コスト管理の課題の解決のため、2010年に、「iSECURE プリント管理サービス」をラインナップに加えた。図3は、プリント管理サービス（SaaS型）の全体図である。各クライアントPCで印刷された文書のファイル名、PC名、日時などの基本情報が、暗号化され、日本ユニシスのデータセンタに自動的に収集され保管される。万が一、データセンタのサーバが稼働停止した場合でも、クライアントPCに20日間を限度に印刷ログが蓄積され、再接続時に自動的にデータセンタ内のサーバにアップされる。なお、印刷ログとは印刷した文書のファイル名、印刷した内容そのものは印刷イメージと定義している。印刷イメージの保存が必要な場合は、自社内に保管用ファイルサーバを設置することを推奨している。

本ソリューションは、一般的なオフィス環境であれば、短期間導入も可能であり、対応プリンタ、複合機を問わないマルチベンダ対応（国産、外国製問わず）、LAN環境及びWAN環境対応、ネットワークプリンタ及びローカルプリンタ対応、プリントサーバ利用環境にも対応している。なお、管理対象範囲のPCから本ソリューションのドライバを削除した場合、即時に管理者に通知され、エンドユーザの印刷ルールを逸脱した行為を防ぐように設計されている。

3. 2. 4　iSECURE プリント管理サービスの機能

紙媒体による情報漏洩リスクをセキュリティリスク、プリント出力に関する想定外のコストが発生するリスクをコストリスクと定義し、リスクアセスメントを実施した結果が表5である。この表では、抽出したリスクに対し、日本ユニシスが提供するプリント管理ソリューションを管理策として、適用可能か否かも示している。なお、本ソリューションは、顧客の要望に合わせ、SaaS サービス型とライセンスパッケージ販売型を用意している。また、1 ヶ月の無償試用環境も提供している。

3. 2. 5　iSECURE プリント管理サービスの導入事例

まず、主たる導入ニーズがセキュリティであった自動車会社 A 社の事例である。A 社デザイン部（クライアント端末 400 台）では、発表前のデザイン情報の漏洩の防止と万が一の漏洩時に漏洩ルートの追跡を可能にし、さらにユーザのセキュリティ意識を高めたいというニーズであった。iSECURE プリント管理サービスを導入し、印刷物すべてにユーザ名を強制印字することで放置プリントが大幅に減少、印刷可能時間も営業日の特定時間のみに限定することで、休日、深夜の印刷文書持ち出しリスクを軽減している。さらに、デザイン部門の全ユーザの印刷ログ、印刷した文書イメージをすべて保存している。この機能により、万が一の情報漏洩時には、だれが、いつ、どのデザインを印刷したか、即時に判別できるようになった。社外への提出物においても、印刷者ごとに付与するユニークなコードを印刷物のフッターに強制印字している。この印字によって、悪意の情報持ち出しの心理的抑止効果に繋がるとともに、漏洩元の追跡が可能になることで、デザイン情報の機密性維持に大きく貢献している。同時に、印刷コスト集計機能、強制複数ページ印刷、グレースケール機能、トナー濃度調整の機能を駆使し、コスト削減にも貢献している。

次に、主たる導入ニーズがコスト削減であった不動産会社 B 社、通信施設会社 C 社の事例を述べる。B 社では、物件の契約書、賃貸説明文書、寮・社宅等の法人向け月次印刷文書等の印刷コストが、年間 1 億 2 千万円にも達していた。本ソリューションの導入により、重複印刷禁止、複数ページ印刷、グレースケール印刷等の機能を強制的に実装、さらに、月間の印刷コストを集計しグラフ化、ユーザに周知するなどの工夫も重ね、印刷枚数を約 16％減らすことに成功した。その結果、印刷コストは、導入前に比較し 24％の削減、年間 2877 万円のコスト削減に成功している。セキュリティ面では、印刷者名を強制印字することで、紙媒体の管理が行き届き、結果として、不動産事業者に必須の個人情報の漏洩防止に役立っている。

C 社のある部門では、議事録、情報共有、稟議書、社内資料、開発プロジェクト資料等の印刷で、年間約 2500 万円の印刷コストがかかっていた。導入後、年間の印刷枚数こそ約 5％削減に留まっているが、カラー印刷を減少させたことで、約 30％、金額にして年間 620 万円のコスト削減に成功している（表 6）。

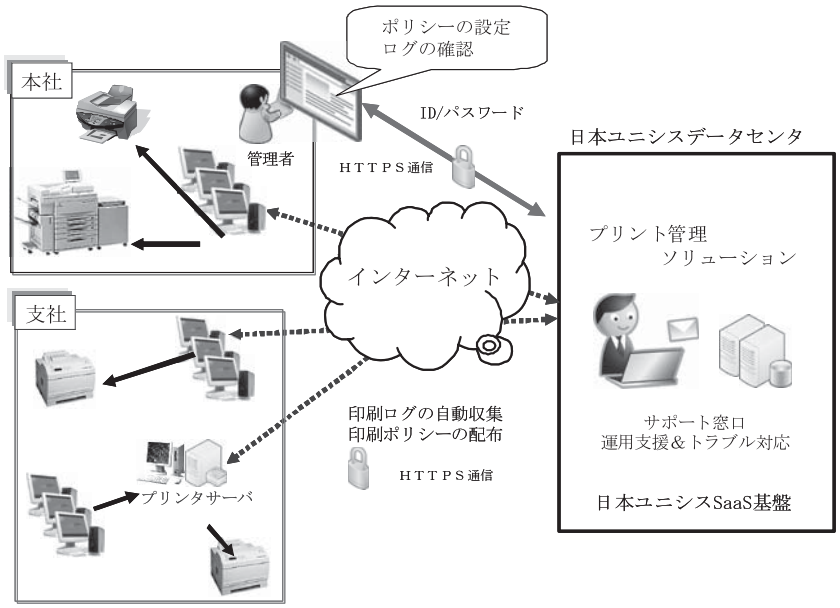

図３　iSECURE プリント管理サービス概要図

表５　iSECURE プリント管理サービスによるリスク解決対応

	懸念されるリスクと脆弱点	解決案	iSECUREプリント管理サービスによる解決	
			SaaS	パッケージ
セキュリティリスク	印刷した文書を持ち出す	PCの印刷ログ（氏名、日時等）を収集する	◎	◎
		秘、社外秘などのスタンプを強制的に押印する	◎	◎
		印刷を指示したPC名、ユーザ名、シリアルユニーク番号を強制印字する	◎	◎
	印刷文書をプリンタに置き忘れる		◎	◎
	深夜、休日に大量印刷した文書を持出す	深夜、休日の特定時間帯は印刷ができない	◎	◎
	印刷文書をプリンタに置き忘れる	ICカード等で印刷前に認証する	△	○
	印刷イメージログがわからない	印刷イメージ（印刷した内容）を強制保管する	△	○
	機密文書等を印刷する	特定ファイル名の印刷を強制的に禁止する	◎	◎
コストリスク	同じ文書を重複印刷してしまう	同一文書の重複印刷を自動的に禁止する	◎	◎
	カラー印刷をしてしまう	モノクロ強制印刷（カラー印刷強制禁止）	◎	◎
	トナーインクの使いすぎ	トナー濃度の調整によりインクを節約する	◎	◎
	１枚の紙に複数印刷をしない	１枚の紙に複数ページ印刷（２in１、４in１など）	◎	◎
	印刷枚数が多すぎる	ユーザ毎の印刷枚数グラフ、表を作成し注意喚起	◎	◎
		印刷上限枚数の警告、制限等の注意喚起	◎	◎
	無駄な印刷をしない	自動で印刷プレビューが表示される	◎	◎
	印刷ページを編集しない	印刷したいページのみ編集できるようにする	◎	◎
備考	◎標準対応　○オプションにて対応　△一部自社設置にてオプション対応可能			

表6　コスト削減効果

B不動産会社（全社導入）※1年間計測	導入前				
	一人当たり年平均印刷枚数	契約単価		従業員数	年間コスト合計
		カラー	モノクロ		
	1700	45		1400	¥107, 100, 000
	4650		2	1400	¥13, 020, 000
	6350				¥120, 120, 000
	導入後				
	一人当たり年平均印刷枚数	契約単価		従業員数	年間コスト合計
		カラー	モノクロ		
	1450	45		1400	¥91, 350, 000
	3900		2	1400	¥10, 920, 000
	5350				¥91, 350, 000
				削減額	¥28, 770, 000
	16%			削減率	24%

C通信施設会社（部門導入）※2ヶ月間計測	導入前				
	一人当たり年平均印刷枚数	契約単価		部員数	年間コスト合計
		カラー	モノクロ		
	15623	30		52	¥24, 371, 880
	4061		3	52	¥633, 516
	19684				¥25, 005, 396
	導入後				
	一人当たり年平均印刷枚数	契約単価		部員数	年間コスト合計
		カラー	モノクロ		
	11307	30		52	¥17, 638, 920
	7407		3	52	¥1, 155, 492
	18714				¥18, 794, 412
				削減額	¥6, 210, 984
	5%			削減率	25%

4.　セキュリティサービス　今後の展望

クラウドコンピューティングの拡大は、ユーザにセキュリティ管理策の新たな選択肢をもたらした。今後、多くのセキュリティ管理機能は、クラウドコンピューティング上に搭載され、脅威と脆弱性情報の共有化による高い付加価値を持つ運用サービスとなっていくだろう。高額の初期投資と習熟するまで長い訓練が必要な自社単独導入型に比較し、多くの企業で共同利用することを前提としたサービス型はコストメリットの恩恵も受けられる。さらに、多くのサービス型のセキュリティソリューションは、重要な情報資産をサービス提供側に委託する必要がない。したがって、セキュリティ管理機能の共有化による情報セキュリティ上の懸念材料は、極めて少なく、サービス購入の心理的な障壁は低い。今後、企業は、情報システムを自社で所有し運用していくのか、クラウドコンピューティングを利用していくのか、セキュリティ要求事項を含め、その配置バランスを多面的に検討し、全体最適を追求していくだろう。同時に、セキュリティ管理機能も、それに合わせて効率的に配備しなければならない。そうなると、柔軟な契約ができるセキュリティサービスは、有望な選択肢となる。

日本ユニシスでは、本稿で紹介した「iSECURE プリント管理サービス」の追加オプションとして、社内に設置されている複合機やプリンタから出力された印刷枚数、トナー利用量など

の MIB 数値データを自動収集し、クラウドコンピューティング上で一括管理する「iSECURE MIB データ管理サービス」を 2011 年夏までにリリースする予定である。また、インターネットを利用した通信販売事業者の Web アプリケーションの脆弱性、改ざんなどを常時監視する「iSECURE セキュアクリニックソリューション」など、今後も、セキュリティに関する課題を解決するサービスを提供していく予定である。

5. お わ り に

多くの経営者にとって、セキュリティ投資は忌々しい存在である。その投資を怠り、ひとたびセキュリティ事件事故が発生すれば、ブランドイメージの低下、風評被害、士気低下、損害補償など、大きな打撃をもたらす。経営者も、市場から強い叱責を受ける。しかし、セキュリティ事件事故は、発生しないかもしれないし、発生したことすらわからないかもしれない。しかも、セキュリティ投資を積極的に進めたとしても、完璧なセキュリティなどありえない。直接的な売上貢献やコスト削減などにも繋がりにくい。ゆえに、ある経営者は、セキュリティ投資を見て見ぬ振りをする。しかし、企業活動とは事業を通して社会に貢献することであり、事業活動を通じて達成しようとする価値こそ、自社の社会的存在意義になる。したがって、これらの事業で扱われる機密情報や個人情報の情報セキュリティを確保するための行為、つまり、セキュリティ管理策の実装は、社会的責任であると考えるべきである。

＊ 1　日本ユニシスグループが 2010 年 6 月に東京で開催した総合展示会。

参考文献　［1］ 情報セキュリティインシデントに関する調査報告書 ver.1.1，日本ネットワークセキュリティ協会，2009 年 9 月，P18，http://www.jnsa.org/result/incident/2009.html
［2］ 石井健一郎，「情報」を学び直す，NTT 出版，2007 年 4 月，P24 ～ P30
［3］ オフィスにおける印刷コストの削減，T. Mitani，Gartner Research Note，March 31, 2009
［4］ サービスとしてのセキュリティの成長動向，J. Pescatore，K. Kavanagh，Gartner Research Note，January 31, 2011

執筆者紹介　戸　木　貞　晴（Masaharu Toki）
2000 年日本ユニシス(株)入社。システム監査、セキュリティコンサルティングに豊富な経験を持つ。公認情報セキュリティ主任監査人、公認システム監査人、システムアナリスト、システム監査技術者、CISSP。2010 年、ICT サービス本部セキュリティサービス部長。