脱境界化と情報セキュリティ管理
De-perimeterization and Information security management

杉野　隆　　Takashi SUGINO
国士舘大学　　Kokushikan University

――― *It never rains but it pours.*

要旨

企業情報システムにおけるモバイル機器やクラウドサービスなどの普及によって，情報セキュリティ管理（ISM）の重要性が改めて高まっている。しかし一方で，ISM は脱境界化という発想の転換を要求されている。他組織との情報共有，コミュニケーションの迅速化といった脱境界化にいたる背景を企業境界論の側面から分析し，サプライチェーンを事例として挙げながら，脱境界化への技術的アプローチを紹介し，ISM への影響について考察した。

1. はじめに

われわれの経済社会は，交換経済で成立している。分業生産は交換が可能でなければそもそも起こらない。交換は古来もっとも基本的な経済的行為である。さらに近代になると，できるだけ平等な交換を行おうとする前提で交換を「取引」と呼び，モノだけでなくサービスにまでこの言葉を拡張するようになった。1991 年のノーベル経済学賞を受賞した R. Coase は，米国で企業形態･産業組織の研究をしている間に，「（市場での）価格メカニズムを利用するためにも、実にもろもろの費用がかかるのだ」という事実を発見し，企業は，取引費用が安くように継続的な企業組織（垂直統合，分社化など）を選択することを明らかにし，市場と企業組織の境界を決める理論を導いた。本論文は，この市場と企業組織の境界というコンセプトを，情報セキュリティ管理(ISM)における境界 perimeter の問題に応用しようという試論である。すなわち，インターネットの普及とともに加速化され，ISM においても，de-perimeterization（脱境界化）への発想の転換を迫られているという状況を考察し，その実現のための基本要素である，認証，認可，アイデンティティ(ID)管理にについて検討しようとするものである。

2. ISM の考え方

Security の語源は，ラテン語の sécurité であり，欠如を意味する接頭語の se- ＝sed-（別に，離れて）と「気づかい」「心配」を意味する cura からなる合成語であり，心配・不安から解放されている状態を言う。IAEA Safety Glossary 2007 Edition[1]は，①「核物質，他の放射性物質，又はそれらに関連する施設」に関わる②「盗難，妨害破壊行為，無許可の立ち入り，不法な輸送，あるいはその他の悪意ある行為」の③「防止，検知及び対応」と解説している（①～③は筆者が挿入）。情報セキュリティと同様な，①（対象範囲）に対する②（脅威）を③防止，検知及び対応するという構造が見られる。

このように， ISM を含めて従来の情報セキュリティの考え方は，管理対象範囲を境界 perimeter として設定し，境界内（ここでは，単一組織で管理可能なネットワーク領域を Domain と呼ぶ）はコントロールされており安全であるとする。一方，境界の外には様々な脅威が存在するが，これらの脅威の襲来を境界線上で遮断すれば境界内は安全を維持できるとする二項対立の考え方である。江戸時代に，関東の江戸廻り関所（箱根，新居，気賀など）を設け，外敵の侵入を防いだ「入り鉄砲出女」というセキュリティ対策はこの考えに基づいていた。また，中世ヨーロッパにおいても，城壁に囲まれた城の内側は安全であり，敵が攻めてきた場合にも，城門を閉鎖することにより外敵から城及びその中の城主以下の人々，資産を守ることができた。周辺の商人や農民たちも城壁内に避難して安全を確保した。しかし，この境界ベースのセキュリティは 16 世紀以降になると防御策としては無効となった。火薬と重火砲（大砲）の発明及び技術改良によって城壁が持ちこたえられなくなったからである。

ISO/IEC 27001:2013 でも，組織の情報セキュリティマネジメント(ISMS)を確立するにあたって，「組織は，ISMS の適用範囲を定めるために，その境界及び適用可能性を決定しなければならない」（箇条 4.3）

と規定している。システム論では，自己の内と外を区分（境界を維持）すべしと説いており，ISMS の要請は当然であった。ISMS の概念が確立した 2000 年前後においては，外部からの脅威は，せいぜいマルウェア，不正アクセス程度であった。FW(Firewall)，アクセス制御，パスワードによって外部脅威から防御すれば，内部に存在する情報の CIA（機密性，完全性，可用性）を確保可能であった。その後も，組織はインターネットとの境界に FW を置いて情報セキュリティ対策の基本とし，個別のアクセス要求に応じて対象範囲を変えて対応させてきた。例えば，VPN (Virtual Private Network)，リモートアクセスは FW から境界を部分的に外部に拡張し，IDS (Intrusion Detection System)，IPS (Intrusion Prevention System)，WAF (Web Application Firewall)は，FW の内側にさらに個別に境界を設けて，FW の弱点を補強した。

3. 境界化の失敗と脱境界化

インターネットの普及拡大とともに，2000 年以降には企業内と企業外のネットワーク間，さらに FW の内部と外部間の境界は曖昧になってきた。企業情報システムは，地理的に拡大した取引先，顧客と情報ネットワーク接続を行う。あるいは，従業員が出先において，モバイル PC からインターネットを介して本社のサーバにリモートアクセスする，従業員が個人所有のモバイル機器（スマホやタブレット端末）をオフィスに持ち込んで，社外／社内の制約なく自社のサーバにアクセスする BYOD(Bring Your Own Device)などが普及してきた。

このような環境では，境界内の防御はおろか，境界を定義することも困難になりつつある。さらには，FW を破ってネットワークに侵入を試みるハッカーよりも，社内リソースへのアクセス権限を持つ社内の人間の方が既に危険な存在になっている（内部不正アクセスによる情報漏洩など）。現在では，Internet Data Center，クラウドサービスを利用するなど，企業ネットワークも企業管理下の施設から飛び出し物理的境界をないものにしている。このため，情報セキュリティへのリスクに対する考え方を改める必要が生じた。

境界化では対応できず，セキュリティ確保に失敗した例としては，次のようなものがある：

- ゼロデイ攻撃を防御できない（脆弱性管理の困難化），
- 内部不正使用を防御できない（アクセス権限が厳格でない），
- マルウェアに感染し，Botnet による攻撃を防御できない，
- VPN の使用はネットワークセキュリティポリシをバイパスする，
- Wi-Fi アクセスポイントへの Wardriver のアクセスを防御できない，
- スマホの BYOD による不正アクセスを防御できない。

クラウドサービスでは，境界がどこに存在するか不明な状況にある。企業情報ネットワークは Borderless System となり，システム境界は常に流動している。現在では，境界で一括して防御するという二項対立的セキュリティモデルでは防御できず，本来的に分散させた多項連携型セキュリティモデルを定義し，アプリケーション個別，文脈個別にセキュリティ対策を行うモデルを探索すべきであろう。

4. 境界解体の背景

インターネットはデータの流れにおける世界中の関所の解体を進行させた。このあたりの現象を説明する理論として，企業境界論 Boundaries of the Firm を適用してみたい（本節は，[2][3]に拠っている）。

従来の企業理論では，企業組織をブラックボックスとし企業間の取引にのみ注目していたが，R. Coase は組織内取引に着目し，企業という組織が形成されるのは市場取引の費用を節約するためであることを明らかにした。ただし，企業内部での組織化にも費用が生じるために，企業は全ての取引を内部化しようとはしない。そこで企業と市場の最適な境界は市場取引を減らすことによる限界費用の低下と内部取引を増やすことによる限界費用の増加が等しくなるところで決定されると論じた。市場の失敗によって発生する取引費用を効率化するために階層型組織という企業組織を形成すると説明した。Williamson は取引費用が生じる要因は，人間的諸要因（限定された合理性，機会主義），環境的諸要因（不確実性，複雑性，少数性）であることを指摘した。取引費用には，①調査コスト，②情報コスト，③交渉コスト，④意思決定コスト，⑤監視コスト，⑥補助コストなどが含まれる。

組織内部と市場での取引費用との比較は何人かの研究によって精緻化されていく。Coase 自身のモデルによると，$TC_M < MC_H$ であれば分社されることになる。それに対して，A. Madhok は，取引費用に加えて自社の階層組織ケイパビリティも加えて，TC_M or $TC_{OUT} < (MC_H - CAP_H)$ であれば分社されるとした。さらに，R.N. Langlois は，組織外部（市場）のケイパビリティを加えて，$(TC_M \text{ or } TC_{OUT} - CAP_M) < (MC_H - CAP_H)$ であれば分社化されるとした。ここに，TC_M ：組織内部の取引費用，MC_H：組織内部の管理費用，TC_{OUT} ：アウトソーシングの管理費用，CAP_H：自社の階層組織のケイパビリティ，CAP_M：組織外部のケイパビリティである。Langlois によると，ケイパビリティとは，企業が保有する知識，スキル，経験などの不可視的な資源の集合であり時間を通じて変化するので，長期的には境界は変化する。企業の組織は，コアコンピタンスとそれ以外の補助的ケイパビリティからなる。補助的ケイパビリティについては，他企業との特定契約に基づいてライセンス供与してリターンを獲得することもできる。したがって，ケイパビリティも取引費用を持ち，企業境界を変化させることができる。

以上の議論をまとめると，企業がある事業活動を内部化するか，外部化するか，すなわち企業の境界設定を考察するには，単なる取引費用ではなく，企業内外のケイパビリティという概念を包摂した動的取引費用という概念を用いる必要がある。ケイパビリティ概念は，現代の企業にとって，階層型組織（垂直統合）よりも海外市場や関連産業への多角化を通じた成長に重要な位置を与えている背景の説明に利用されている。筆者は，昨今におけるサプライチェーン管理，クラウドサービスの利用といった企業行動の前提には，このような補助的ケイパビリティ（企業情報システムも含まれる）の同質化（$TC_{OUT} - CAP_M$ が減少する）によって組織外部との動的取引費用が低くなり，脱境界化が加速されているのではないかと解釈したい。

5. 脱境界化の試み

5.1 脱境界化状況とは

情報セキュリティを確保するためには, ユーザ認証, 認可とアイデンティティ（ID）管理が重要である。境界化状況では Domain 内では一定の情報セキュリティポリシが確保されているという前提があったが, 脱境界化状況では, 組織自らが構築する自社ネットワークやクラウドサービスが流動的に組み合わされたネットワークの中をデータが流通していくであろう。他 Domain との情報セキュリティポリシの相違を考慮しなければならない。

また，これまで情報セキュリティは情報システムにとって後付の機能であったが，脱境界化状況に対応するためには，情報システムにおける本質的な機能として扱うという発想の転換も必要であろう。

5.2 提案されているアプローチ

現在二つのアプローチが提案されている。

①User centric approach

ユーザの ICT リテラシのレベルに応じて情報セキュリティを設定できるようにするため, 認証と認可を分離し, ユーザの意思に基づいてデータの流通を制御するという考え方である。ユーザからの認証要求に対して ID 情報提供者は本人を認証すると同時に「サービス提供におけるユーザの役割」までも特定（承認）すると暗号化されたトークンを発行する。このトークンにはユーザの「所属」や「役職」「グループのメンバーシップ」などの情報が含まれる。サービス提供者はトークンをもとにユーザを識別し，役割を決定してきめ細かなアクセス権限を認可する Claim-based security という仕組みを採用する。具体的には Security Assertion Markup Language(SAML)や OpenID などがあり，現在 Single sign-on などに利用されている。

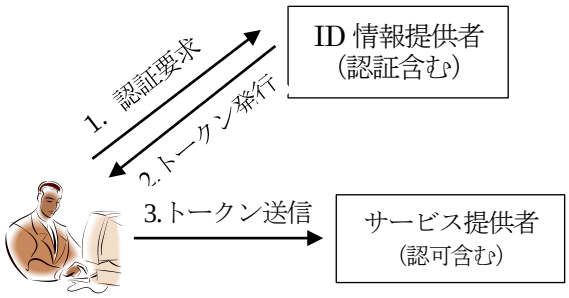

図 1 クレームベースセキュリティの仕組み

②Data centric approach

組織において究極的に守るべき資産は情報（データ）である。データのセキュリティを強化すればよいという考え方である。データが存在するあらゆる局面を貫通してデータをシームレスに保護し，更にデー

タのライフサイクルにわたって一貫した情報セキュリティポリシを，境界を超えて適応させる。そして，データがどこにあっても情報セキュリティを確保するために，データレベルの認証 authentication と認可 authorization，及び ID 連携管理をネットワーク内のどこででも可能とする。現在，データそのもののセキュリティを確保するための方式として Selective intelligent encryption が提案されている。これは，公開鍵暗号方式において，暗号化鍵，復号鍵それぞれにパラメータを組み込み，復号時に両パラメータ間のアルゴリズムによって復号可否を決定することによって，送信者がデータの受け手を「自由に指定」できるアプローチである。

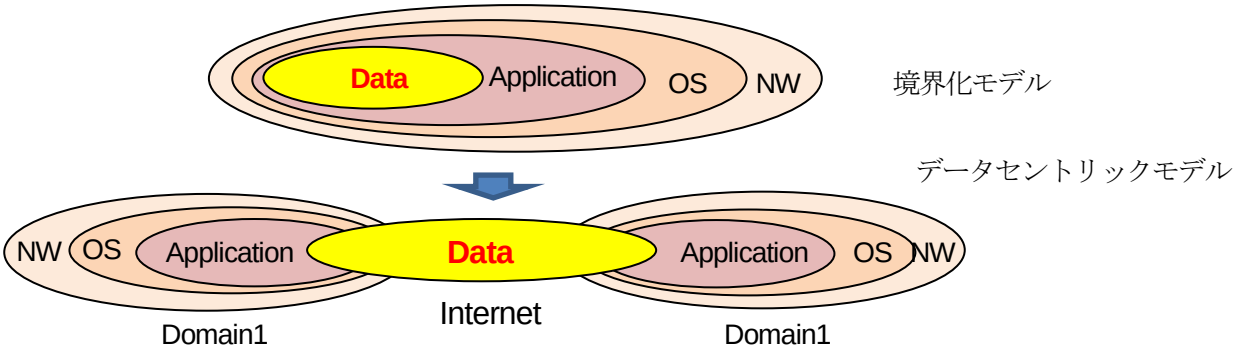

図 2 脱境界化によるデータの扱いの変化 [5]

5.3 課題

ISM の観点からは，関連する情報システム全体において，データが流通するパス全体を通して一定以上のセキュリティを確保しなければならない。図 2 において，Doamin1 と Domain2 間でデータが流通する場合，Domain1 からみて Domain2 が信頼できるだけの情報セキュリティを確保していないと，脱境界化を実現できない。しかし，関連する Domain には，ISMS 認証済みの企業，未認証の企業が混在する可能性があり，各 Domain の情報セキュリティを一定水準以上に揃えることは，容易なことではない。サプライチェーンにおいて現実にそのような問題が起きている。また，認証連携のための方式がすべて同一ではない可能性があり，クラウドサービスにおける IDaaS のような認証連携サービスがクラウド間に必要になるかもしれない（インタークラウドサービス）。

6. まとめ

ISM における考え方が境界化から脱境界化に変化したことを企業境界論によって説明する可能性を示し，それに伴う情報セキュリティ上の課題と，解決策として現在提案されているアプローチについて紹介し，課題を検討した。

引用・参考文献

（各 URL へのアクセスは 2014 年 10 月 30 日に確認）

[1] 原子力安全基盤機構　安全原則 No.SF-1，IAEA 安全基準，日本語翻訳版，2008 年 12 月，p.ii
http://www.nsr.go.jp/archive/jnes/content/000013228.pdf

[2] 丹沢安治　企業間連携と日本の製造業の新たな戦略―企業境界の再構築―，オペレーションズ・リサーチ，2005 年 9 月号，pp.637-643

[3] Langlois R. and Paul Robertson (谷口和弘訳) 企業制度の理論―ケイパビリティ・取引費用・組織境界，NTT 出版，2004 年　http://www8.cao.go.jp/cstp/tyousakai/innovation/ict/3kai/siryo6-9.pdf

[4] Bhargava B., L. Lilien,.and Y. Zhong　Security Paradigms and Pervasive Trust Paradigm,
https://www.cs.purdue.edu/homes/bb/hel5.ppt

[5] Wellington S. de S. , Fialho S. V.　Overcoming the Risks of the Perimeter-based Security with Strong Federated Identification Mechanisms, www.thinkmind.org/download.php?articleid=icds_2013_5_50_70035