『学習院大学　経済論集』第47巻　第４号（2011年１月）

金融・経済活動における情報などの分割，バックアップと情報セキュリティ

―金融セキュリティの経済学入門（I)―

辰巳　憲一*

１．はじめに

知的財産や機密情報など多くの情報資産を，企業は，抱えている。技術や営業上の秘密が漏洩すると企業は競争上で不利になる。また近年，企業が保有・管理するデータの取扱いに関する規制やガイドラインが多くの国で定められ，企業顧客の氏名や口座情報などの個人情報を安全に取り扱うデータ管理に対して，より大きな責任が伴うようになってきた。それにもかかわらず，企業の機密情報，個人情報，などの流出事故・事件は後を絶たず，ビジネスへ大きなインパクトを及ぼすだけでなく，企業の存続に関わる重大な影響も出ている。

また昨今，銀行業界を取り巻くビジネス環境の変化により，銀行システムの統合や共同センター設立が増え，情報・データの分散化，管理体制といった問題が大きくクローズアップされるようになった。

セキュリティに関わる可能性のある事故や障害などの出来事をセキュリティ・インシデントという。犯罪被害から，ソフトウエアなどの不具合，運用上のミスなど，セキュリティに影響を与える可能性のある幅広い出来事がセキュリティ・インシデントになる。

本稿では，金融セキュリティの経済学[1)] を入門的に展開しよう。金融セキュリティと一言で書いても，内容は様々である。そのなかでも，本稿は，情報，取引，システムやネットワークに係わる分割やバックアップをとりあげる。

分析の一例を先取りしてあげてみよう。ネットワークや情報システムにおいて，機能を「分割」しておくと，まさかの時に，セキュリティは高まる。分割しておけば，事故が起こったり，攻撃されてダウンしても，ダウンの原因は比較的簡単に絞れる。それゆえ，被攻撃・事故の箇所の発見は早くなる。しかも，その攻撃された部分だけ，事故の部分だけ回復・復旧させれば

＊）学習院大学経済学部教授。Information Division, Backup and Security in Financial Activity ~ An Introduction to Economics of Financial Security（I）. 内容などの連絡先：〒171-8588 豊島区目白１－５－１学習院大学経済学部，TEL（DI）：03-5992-4382，Fax：03-5992-1007，E-mail: Kenichi. Tatsumi @gakushuin. ac. jp

1）次にあげる先端的な著書には，技術面では現在から見てみれば当然陳腐化しているが，それ以外の点では経済学的な視点はまったくなかったことが特徴としてあげられる。青木隆一／稲田龍著，村井純監修，『PKIと電子社会のセキュリティ』共立出版，2001年。ウィリアム・スターリングス著，石橋啓一郎／三川荘子／福田剛士訳，『暗号とネットワークセキュリティ理論と実際』ピアソン・エデュケーション，2001年。

よいので復旧時間は短く，かかる費用も低くなる。それゆえ，新しい研究分野として，「分割の経済」の分析がありうるのではないか，と思う[2]。

暗号などの研究分野では，経済学と直接まだ係わっていないが，過去大きな進歩があった。しかしながら，金融セキュリティの経済学を展開した研究は，特に分割やバックアップに係わる研究は，ないに等しい。それゆえ，直接先行する論考ではないが，辰巳（2008），辰巳（2009），辰巳（2010a）ならびに辰巳（2010b）が，著者による情報，ネットワークとそのセキュリティに係わる初歩的な考察を行った先行研究であり，本稿はそれらに続くもので，「分割」を活用するという視点は新しいものである。

なお，本稿で取り扱う「分割」は，ファイナンスや経済学における分割可能性（divisibility）あるいは分業（division）と何らかで係わるが，直接には，関係していない。そこでの概念はまだセキュリティと結び付いていない。

2．分割によって達成される様々なセキュリティ

2－1　情報の分割可能性とセキュリティ

セキュリティが分割で達成される，という原理・現象は必ずしも自明ではない。そもそも分割できるのかどうかという点に関しては，ものには様々なものが存在し，ものによって違ってくる。どう分割できるかという点に関しても，ものによって様々に異なる。分割がどのようにセキュリティを達成するかという点に関しても，それゆえ，ものによって様々に異なる。

様々なもののなかでも，情報について少し詳しく解説する必要がある。情報は分割できる，という事実は最近でこそ周知の事柄になったが，昔は分割できないのが普通であった。

情報が分割可能になり，経済的意義をもつのは，デジタル化[3]とスピード処理によってである。デジタル化とは，情報を0101などの数の配列により信号化し，処理や送信などの運用をする，ことをいう。数を計算する演算機械であるコンピュータで処理するためには，情報を数に置き換える必要がある。画像などはそのままの形ではコンピュータで処理できない。それを数に置き換えるのである。数は簡単に，場合によって複雑に様々な形で分割できる。それゆえ，デジタル化によって情報は分割できるようになったのである。

デジタル化はアナログと対比されるが，その比較は情報媒体としての紙文書と電子文書を比較する例を持ち出せばわかりやすいだろう。紙は，嵩張り，重量があり，（多くの種類の紙は）劣化する。それゆえ，移動・運搬や保管などに問題を抱えており，大量に，移動させたり，長期保存するには不適であるとみなされてきた。特に紙については，実質ミリセカンド以下しかかからない電子と比べて比較対象にできない程その移送には時間がかかる。さらに宅配料金，（安全に送るために）書留郵便料や保険料などのコストもかかる。保管については，盗難や火災などの事故が起こるが，電子でも同様な問題がある。なお，劣化と長期保存という観点からは，紙の方に少しの利点があると考えられるようになっている。

2）簡単な事例は他にも，いくつかある。政治はワシントンDC，経済はNYCと首都機能を分散・分割させるのは国家安全のためであるといわれる。また，様々な権力を集中せず，任期を限って首長を公選していくのも国家存続のためである。

3）「デジタル」の語源は，ラテン語の「指」という意味で，それが「指を使って数える」という意味に変化し，そして「情報を数に置き換えて表す」ことを指すようになった。

スピードについては，電子文書はコンピュータで処理するから，処理をスピード化できるのである。

分割（デジタル化）とスピード処理によってもたらされた経済成果を，2008年12月施行の電子記録債権法によって法制化され，2009年８月に実施第一号会社が設立され，同11月に第一号利用があった電子手形を例にして説明することにしよう。

（１）分割譲渡

よく挙げられる例を使えば，ある額面金額の紙幣や手形を丁度半分に千切っても，半額の紙幣や手形として通用しない。これが情報は，昔，分割できなかったと言った例の１つである。それに対して，電子は，正確に任意の大きさに分割でき，流通させることができる。

その結果，電子手形は，複数の（下請けなどの）企業へ分割譲渡が可能となる。さらに複数の金融機関への割引持込も可能となる。分割して必要な資金を調達できる。

（２）スピード処理

スピード処理ができることの結果として，電子手形では，旧来の（紙）手形では２営業日後であったのが速まり，最速では決済日と同日に資金利用できる。

スピード処理はさらに，例えば二重譲渡の可能性を排除する。二重譲渡の問題とは，ある債権の所有者が故意あるいはミスによって当該債権を複数回売却することである。善意の購入者は，既に第三者に売却された債権を購入してしまうが，債権は手に入れることができず，支払った購入代金は戻ってこない，という経済的打撃を受ける。

債権を売却するにあたって，当該債権を他人に譲渡していないことを即座に示すのは従来困難であったが，電子記録（電子登記）によってそれが可能になった。

従来の手形は利用が急速に減少しているのは事実である。電子手形は手形の機能を補う（だけの）ものとして捉え，なかには冷ややかに見ている IT 業者もいる。分割譲渡可能性とスピード処理の少なくとも２つの観点から，電子手形は従来の手形とは違うことは明瞭であろう。電子手形は従来の手形を単に補うものではない，短期金融手段としての役割が期待される。

（３）分割の意味

本稿では，分割とはデジタル化された１つのものを何らかの比率で２分割する（２等分を含む），あるいは２つ以上に分割することである，と想定して展開する。しかしながら，実際はこのような分割だけではないことを前もって説明しておこう。

平面上に２点があれば，それらを通る直線が引ける。さらに，その直線と原点を通る縦軸との交点は，直線の切片を教えてくれる（直線の傾きも教えてくれる）。逆に，この切片の大きさを隠したい情報とし，それを平面上の２点で表わすということができるわけである。この２点は切片の単一の数値情報を２分割した情報と言える。２点のうち１点が盗まれても，切片が判明することはない。

例えば，１（切片）という数字は（１，２）と（２，３）という２点に分割可能になる。$y = x + 1$ という線形一次方程式が（１，２）と（２，３）から逆算できれば切片は推測できる。

これは，後述する秘密分散法という技法で用いられる分割である。秘密分散法によって，数字の分割という意味が変わったのではないかと思う。深くなったといえる。

（４）デジタル化，分割とセキュリティ

デジタル化が，上でみたように，情報の分割を可能にさせる。そして以下にみるように，情報などの分割可能性がセキュリティを達成する。それゆえ，デジタル化がセキュリティを達成

する，といえよう。

デジタル信号はアナログ信号に比べ，品質の保持，情報の圧縮，が容易というメリットがある。質を落とさずに情報を圧縮できるので，圧縮すれば一度に大量の情報・データを送ることができる。また，その信号を遠隔地に劣化なく送信することができるのもメリットである。また，送信の途中で一部の情報・データが消失しても，デジタル技術を使うと元の情報に修復することも可能になる場合がある。さらに，デジタル信号はアナログ信号に比べ，検索が容易であるというメリットもある。

セキュリティ対策が様々あるなかで，情報，回線，ネットワークそして取引を分割することによって，セキュリティを確保する方法がある。本節の以下では，それらを詳しく説明しよう。

２－２　情報や権限分割によるセキュリティ

２－２－１　通信方法によるセキュリティ

情報技術のエッセンスの一つはスピードである。そのため，混雑が生じない。情報は当然一件一件処理されるが，その処理スピードが他の経済現象のスピードより格段に速いため，あたかも混雑がないように，みえているだけである。しかしながら，送受信件数が大量に増えたり，送受信するデータ・情報が大容量になると，混雑も生じる。それを緩和する手段の１つがパケット通信である。

（1）パケット通信とその効率性

通信とはデータ・情報を送受信することである。パケット通信とは，データ・情報を分割して，送受信することである。パケットの大きさをイメージするには，2010年年頭において，Yahoo のトップページは約180のパケットから成り立っている（ある会社の調査結果から引用）ことから想像すればよい。

パケット通信によって通信の「効率性」が次のように達成される。大容量のデータ・情報を受信するのを順に待っていると，待ち時間の間，次の順番の人は何もすることがなく，無駄な待ち時間になる。しかしながら，一部でも受信していると，そのデータ・情報を検討するなどして有効な待ち時間になる。

なお，パケット化をカプセル化と表現する場合もあるが，カプセル化という言葉は根付いていないようである。

（2）パケット通信のセキュリティ

データ・情報を分割することで，通信の効率性だけでなく，セキュリティも達成できる。送受信中に，ネットワークのあるルートが遮断されたとすると，送受信できずに残されたデータ・情報は別ルートで送ればよい。もう一度すべてのデータ・情報を送受信する必要はない。

人間は５分の１秒の間，画面などが見えなければ違和感・異常を感じるそうである。動画配信の場合，パケット送信にあたり，この現象が使われる。５分の１秒以内の間隔の間であればパケットが何らかの理由で送信できなくても（受信者にとって何ら）問題ないわけである。送信ミスはこの間隔であれば許されることを意味している。

しかしながら，パケット通信は，当然ながら，セキュリティが万全であるというわけではない。パケットが通信回線のなかを混載で移動している（他の人のパケットも回線を流れている）限り，それが例え通行の優先順位が高く（つまり，いわゆる専用回線であっ）ても，セキュリティ上その他の様々なリスクは存在する。

（3）パケット，フラグメンテーションとパケットに対する Teardrop 攻撃

なお，通信回線には，通信回線ごとに MTU（Maximum Transmission Unit）が定められている。MTU とは，最大伝送単位という，転送可能な最大のデータ長のことで，ある。経路の途中でパケット長よりも MTU が小さい通信経路を通過させる場合，パケットをフラグメンテーション（分割化，断片化，fragmentation）処理を行う必要がある。パケットは，通信ネット上小さい MTU のサイズに分割しないと，通信回線を通過できなくなるからである。

分割に対する Teardrop 攻撃とは，分割された IP パケット（インターネット上で送受信されるデータの単位）をつなぎ合わせる際の，TCP/IP の脆弱性を突いた攻撃手法のことである。IP パケットに含まれる分割前のオフセットフィールド情報を偽造することで，システムを停止させる。

IP パケットによるデータ転送を行う場合，送信側で規定された MTU を超える IP パケットは，複数の小さな IP パケットに分割される。この分割された IP パケットには，分割前のどの部分であるかを示すオフセット値が含まれており，この情報を元に，分割された IP パケットを受信した側は，データを復元することができる。

Teardrop 攻撃は，このオフセット値が重複するような不正な IP パケットの断片を偽造し，受信した PC（攻撃の標的）の処理を混乱させる。TCP/IP の IP フラグメンテーションの脆弱性を突くことで，データ再構築時に PC をクラッシュさせたりフリーズさせたりする。

矛盾するオフセット値が含まれるデータを破棄するように TCP/IP の実装を修正したり，TCP/IP の実装上の問題を修正したプログラムを適用するなど，の対策が必要になる。

２－２－２　分割・暗号によるセキュリティ

データを複数に分割して格納することはパーティショニング（partitioning）とも呼ばれる。データを分割することにより，性能や運用性を向上させたり，故障の影響を局所化することなどができることを具体例でみていこう。

（1）電子割符によるセキュリティ

元データの情報を分割して管理することでセキュリティを保つ技術は，いくつか存在する。その一つに電子割符（わりふ）と呼ばれる方法がある。割符（Tally）は，かつて室町時代に日本が中国の明王朝と行った勘合（かんごう）貿易で，正式の通交船（人）であることを証明する許可証として発行された勘合符のように，重要な情報を物理的に分割して管理・照合に使うものである。

例えば，クレジット・カードの情報を「割符 A」,「割符 B」として分割し，割符 A をユーザーが，割符 B を決済会社が保有する。ユーザーは，ショッピングなどの利用時に販売サイトなどを通して割符 A を決済会社へ送信する。それを受け取った決済会社は，保有している割符 B と合わせることで，実際のクレジット・カード情報を復元する。

決済時のネットワーク上でのカード情報盗聴，あるいはユーザーのパソコンや決済会社のサーバーなどからのデータ持ち出し，がなされても，こうした電子割符による暗号化によってカード情報の完全な復元はできないため，偽造カードの作成などは不可能になる。

（2）分割と冗長化によるセキュリティ

情報漏洩に対するガイドラインが強化される中，情報漏洩の形も，「外部からの侵入者」から「内部からの漏洩」に変化しつつあり，「内部からの情報漏洩を防止・抑止」するための対策が必要になってきている。そこで，必要となるのがデータそのものを保護するデータ・セ

キュリティ対策である。

その有力な手段がデータ・情報の分割である。分割といえば，巨大船舶が海水に接する面の内側を細かく分割した区画スペースから構成させ，浸水しても，浸水はその区画だけに止まり，沈没しないようにしている事例を思い起こさせる。

情報を分割し，複数のセンターに保存する方法においては，分割データからは元データを推測できない。データ・情報分割は暗号にもなるのである。そして，利用する際には復元（復号）する必要がある。

データ・情報そのものを保護するために必要となる，暗号化，認証，アクセス制御，ログ監査，鍵管理などは，内部からの情報漏洩に備えるための包括的データ・情報保護策の１つである。

データに冗長性（じょうちょうせい）を持たせておけば，分割したデータの一つが失われた場合でも，元のデータを復元できる。冗長性を持たせるとはバックアップを複数備えることである。データを７個に分割して，それらのデータを２倍に冗長化する場合を考えてみよう。そのうち，１個が消失したり破壊されても，復元可能である。２つ目の消失・破壊で復元できなくなる確率は13分の１である。

（３）バックアップとフェイルオーバー

バックアップに関しては，ファイルのバックアップなどという言葉を日常的に使い，我々にとって身近であり，多くの説明は不要であろう。ただ，バックアップの対象が文書，システム，通信回線と変わるにつれ，考察するべき事柄は多少変わってくることには注意しなければならない。

フェイルオーバー（failover）とは，障害が発生した場合に，処理やデータを（バックアップされた）代替コンピュータサーバー/ システム / ネットワークが引き継ぐ機能をいう。自動的に冗長な待機系に切り換わる機能である。次々と引き継いでいく機能はカスケード・フェイルオーバーという。平時から２つ以上のコンピュータサーバー/ システム / ネットワークが，相互に状態を監視しながらデータの同期をとって動作しなければならなくなるが，このカスケード・フェイルオーバーによって高い可用性と信頼性が維持される。

フェイルバック（failback）とは，フェイルオーバーによって切り換えられたサーバー/ システム / ネットワークを障害発生前の元の状態に戻す処理を意味する。ちなみに，何らかの異常を察知して，人間が手動で切り替えを行うことをスイッチオーバーという。

（４）スタンバイとデュアルシステム

フォールト・トレランス（fault tolerance）とは，サーバーやシステムの一部に障害が発生しても，全体を停止させずに処理を続けるようにする仕組みのことであり，耐障害性と訳される。その間に故障部分を修復できる，ハードとソフトの両面で二重化する，あるいはさらに三重化するのが具体的な対策になる（「フォールト・トレランスとは」『日経コンピュータ』2004年11月15日号）。

バックアップはスタンバイともいわれる。この小節では，該当業務で使われるスタンバイという用語を踏襲しよう。

スタンバイ（バックアップ）とは，システムに障害が発生したときでも処理を続けられるようにする仕組みの一つである，といえる。スタンバイでは，同じ構成のシステムを２系統用意しておき，その片方を作動させ（現用系あるいは本番系），もう片方は待機状態（待機系，あ

るいはバックアップ）にしておく。待機系は，現用系が動作しているかどうかを監視していて，現用系のダウンを検出すると現用系が行っていた処理を引き継ぐ。現用系システムから待機系システムに処理を切り替えることを，直ぐ上で既述の，フェイルオーバーと呼ぶ。

スタンバイには，ホットスタンバイとコールドスタンバイの２つがあるが，もっとも徹底した運用であるデュアルシステムという３つ目もある。ホットスタンバイでは，待機系と現用系は常に同じ状態にしておき，現用系に障害が発生すると即座に待機系が処理を引き継ぐ。現用系と待機系の同期を行なわずに，現用系に障害が発生してから待機系を作動させる方式は，コールドスタンバイと呼ばれる。待機系も現用系と同時に同じ処理を実行していて，現用系がダウンしても待機系が処理を完了するのがデュアルシステムである。

取引所では，多くのケースで当然ながら，ホットスタンバイが利用されている。

（５）バックアップのレベル，範囲と頻度

バックアップをより完全なものとするためには，個々のデータの重要度のレベルを確認し，バックアップのレベル，範囲と頻度を決定しなければならない。いくつか重要な点をあげてみると次のようになる。

バックアップの範囲，及びバックアップの頻度は，組織の業務上の要求事項，関連する情報のセキュリティ要求事項，及びその情報の組織の事業継続に対しての重要度を考慮して決定する（JIS Q 27002の文章）。さらに，機密性が重要な場合には，暗号化によってバックアップ情報を保護する，必要がある。

２-２-３　権限分割によるセキュリティ

情報分割型あるいはデータ分割型セキュリティ以外に権限分割型セキュリティというものがある。この分野では，分割ではなく，情報分散型あるいはデータ分散型と呼ばれるが，内容は同じなので，それを踏襲しておこう。

権限分散型セキュリティとは，登録管理者 α 人中の任意の組み合わせの β 人が共同で操作するとシステムが作動する仕組みである。暗号方式そのものが破られていない限りは，また複数管理者 β 人全員の結託が起こらない限りは，機密情報の漏洩は起こらない。前回の作業終了時に消滅した暗号鍵を，複数の管理者 β 人が共同作業（１台のコンピュータ上で β 人の管理者が順次ユーザー認証作業を遂行するか，β 人の管理者がそれぞれのコンピュータで並列してユーザー認証を遂行するかして）をした場合にのみ同一の暗号鍵が復元でき，システムは稼動する。作業終了後はすべての鍵は消滅する。

２－３　システムのバックアップ

（１）システム・バックアップの方法

規模の大きい，ある企業が，１つのシステムを全く同一の例えば４つのシステムに分割するとしよう。これを１つの大システムのままにしておく場合と比較してバックアップ問題を考えてみよう。

４つのシステムにバックアップを設ける場合，１つのバックアップ・システムでは不安だが，２つバックアップ・システムを作っておけば万全であると考えられる。この場合稼働システムとバックアップ・システムの数を勘定すれば合計６になる。

分割前の大システムの場合バックアップを作るとすれば，バックアップは１つしか設けられない。これは，分割後のシステム数からみると，４つのシステムに４つのバックアップ・システムを設けることに等しくなる。それゆえ，この場合稼働システムとバックアップ・システム

の合計数は８になる。

それゆえ，システムをこのように分割すればバックアップのコストは，システム２つ分だけ，従来かかったであろうコストを25％削減できる。バックアップの**規模の経済性**と呼べる現象である。

比較的規模の小さいシステムから出発して時間をかけてだんだん規模が大きくなった場合，負荷分散を行う必要が生じれば，企業は一般に機能や利用者（役職，所属部門など）の観点からサーバーを分散させる。それゆえ，規模の経済性を活用するシステムの分割はどんな企業でも適用できるわけではない。

しかし，この現象を活用する企業は古くからある。メガ銀（大手都市銀行）の基幹システムにおいては，店群別システム概念が導入され，メインフレームによる分散処理化がすすんできた。これは，拠点支店・本店などを中心に据えて，それぞれを１つのシステムで動かす。銀行全体としては，同一のシステムが複数存在することになる。

（２）共同バックアップ・センター

逆に，同様なシステムを持つ４つの組織が共同でバックアップ・センターを設立するとしよう。上と同じ理由で，４つのシステムに４つのバックアップ・システムをセンター内に設けることは無駄になる。２つバックアップ・システムを作っておけば万全であると考えられる。これが，地方銀行が共同バックアップ・センターを設ける理由である。この設立は，一般に，銀行システム自体の共同化構想より先に立案実行されているようである。

２－４　通信回線のバックアップ

（１）通信回線バックアップの原理

システムと通信回線それぞれにバックアップを設けるのが，大システムではセキュリティのためふつうになっている。つまり，正規とバックアップの２つの基幹システムと正規とバックアップの２つの通信回線があるのである。ふつうバックアップ回線は，レベルを一段下げた，バッチ処理で比較的遅い通信回線が用いられることもある。

そして，複数の参加者のいるネットワークの場合，ネットワーク参加者は正副２つの通信回線に繋ぐ其々２つのアクセス・ポイントを持つ。

しかしながら，このままでは，２つの回線に同時にそれぞれ１ヵ所以上で故障が生じれば，回線は機能しなくなり，システムはダウンする。そこで，とられる対策は次に説明する，スイッチ・ポイントの設置である。

（２）通信回線バックアップの方法

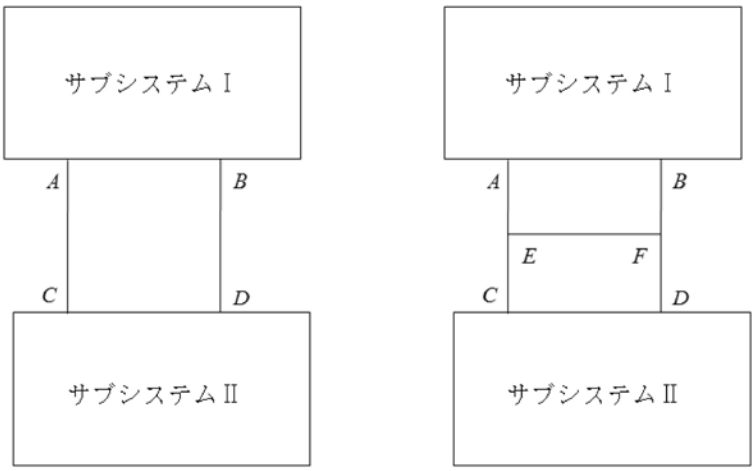
図表１（a）では，サブシステム I とサブシステム II を結ぶ AC が正規の回線，BD がバックアップ回線である。AC と BD の双方に１箇所ずつ故障が生じると回線は機能しなくなる。

そこで，中間に，スイッチ・ポイント E と F をもうけ，その間にスイッチ回線を繋ぐ。例えば，EC の間に故障が生じれば，通信は AEFD と流せばよい。

この場合でも，AE 間と BF 間に同時に故障が生じれば，回線は機能しなくなる。そのような事態に備えるには，無数のスイッチ・ポイントをもうければよい。故障の影響はゼロにはならないが，無限に小さくできる。

以上が，実際に取られている証券取引所の通信回線セキュリティ（正確には，その機能の一部）の仕組み[4] である。

図表１（a） 回線バックアップの方法

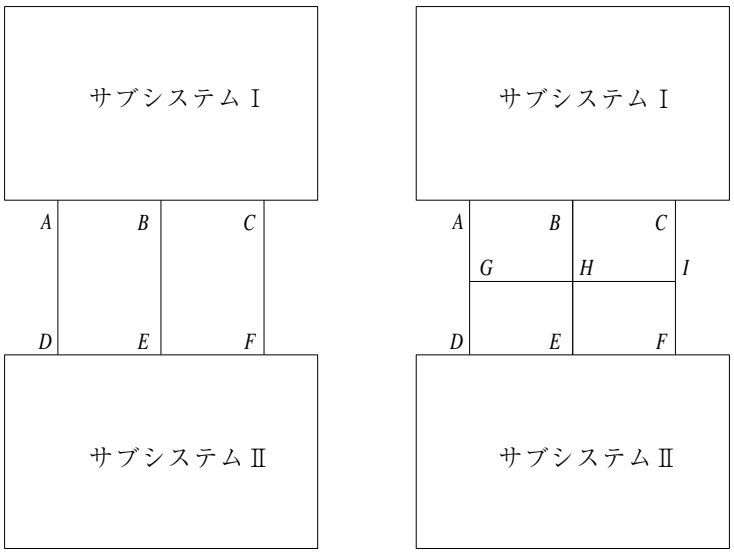


（３）さらに複雑な場合

EF にかかるコストの大きさについてであるが，もしそれが膨大になれば第三のバックアップ回線を設ける方が有効になる場合があろう。

図表１（b）では，ふつうの場合（左の図）３ヵ所の故障で通信は完全に遮断される。多く

図表１（b） 回線バックアップの方法



4） 例えば，2010年１月４日に東証が稼働させた新株式売買システム「arrowhead」が１つの例である。この場合，回線の数は２つであるが，**図表１**（a）中の EF は低コストで設置できるため，極めて多く繋がれている。

の場合コスト的に小額の出費で，３ヵ所の故障に対応できる確率は飛躍的に上昇する。しかしながら，遠隔地通信などにおいて，問題はコストになる。バックアップ回線のコストだけでなく，回避回線（図ではGH, HI）を増やせば，退避回線が障害を受ける確率も高まる。

２－５　ネットワーク分割によるセキュリティ～通信障害の解決方法

通信障害を解決するには，従来，専用の監視装置をネットワーク上に設置し，そこに試験データを送信するなどして障害があるかどうかを確認してきた。この場合，既に説明した分割の原理を応用すれば，ネットワークを分割すれば効率的に障害を検知できる，ことがわかろう。

なお，その新技術が2010年12月にサービス開始（予定）の携帯電話向け高速通信サービス「LTE」向けに開発された。音声，通信が不能になっているにも関わらず，管理者に通知されないサイレント障害にも対応する。障害場所の特定の短縮化，ひいては復旧時間の短縮化になる。

２－６　取引分割によるセキュリティ

取引分割によってセキュリティを守る手法にエスクローがある。エスクローは「預託」と約され，商品・サービスをやり取りする際に，当事者同士が直接やり取りせずに，一旦第三者に預託し，その第三者を仲介してやり取りする仕組みである。エスクローは，不動産，証券やインターネット・オークションなどで利用される[5)]。

資金決済法で様々な金融サービスが注目されている。2010年４月から施行された「資金決済に関する法律」（いわゆる「資金決済法」）では，小額（資金決済法施行令第２条で100万円と定められている）の取引として政令で定めるものに限るという上限はあるものの，従来，銀行法で銀行のみが可能であった資金移動（為替取引）サービスが，銀行以外のIT企業などの事業主にも解禁されることになった，から注目されるのである。

（１）エスクロー・サービスの流れ

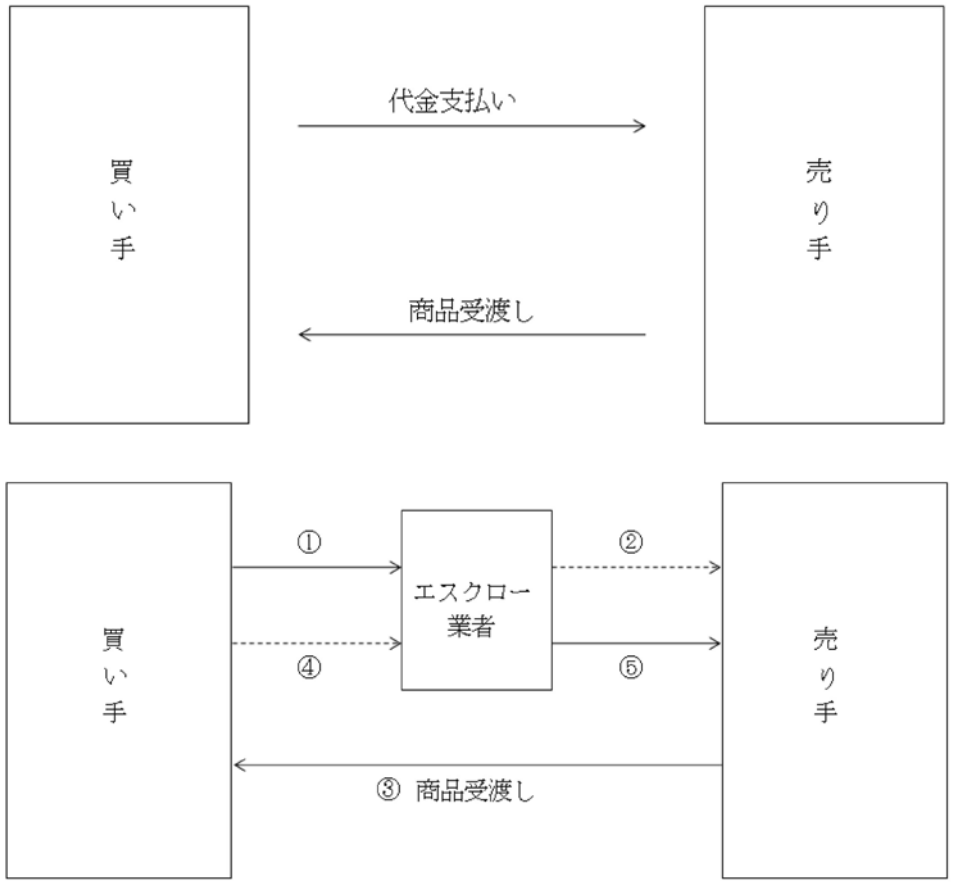
金融サービスのなかでも，売り手と買い手の間に第三者を介入させ，セキュリティを確保する，エスクロー（escrow）サービスが取引分割の事例として知られている。もし売買する両者が互いに信頼できない場合，代金支払いと商品受け渡しは同時に行うしかない（**図表２**の上段）。われわれが日常行っている多くの街頭の商取引はこのように行なわれている。しかしながら，ネット取引のように代金と商品の決済を同時に行うのが困難な場合がある。このような場合，取引を２つに分割することによって，セキュリティが確保されるのである。その流れを**図表２**の下段に示した。

売買の契約が成り立ったとしよう。まず①買い手は代金を第三者（これがエスクロー業者）に支払う。次に，②第三者は売り手に支払い（振込み）があったことを知らせる。その入金があったという通知を受け取った後，③売り手は商品を発送する。そして，④買い手から商品受

---

5)　エスクローの範囲は拡がっている。データ・エスクローとは，ドメイン名の登録管理に関連して，レジストリやレジストラの保持する登録情報に関するデータを，業務移管などが発生した場合に備えて，一定間隔ごとに第三者に預託しておく仕組みのことを指す。あらかじめデータを預託しておくことにより，移管などの際には，新しいレジストリやレジストラが，そのデータを引き継いで速やかに業務を立ち上げることができるようになる。この仕組みにより，登録者が登録データにアクセスできなくなる期間を最小限に抑えるとともに，レジストリやレジストラの業務停止などが原因で登録データが失われてしまい，ドメイン名の登録者が不明になるような事態を避けることができる。
また，ソフトやシステムなどについては，提供者の破綻などで管財者から利用などを止められることを避けるために，エスクロー契約が結ばれる。破綻の際にはユーザーがソフトやシステムを買い取ることになる。

図表２　エスクロー・サービスの流れ



領の知らせを受け，⑤第三者は代金を売り手に支払う。そして，売り手が代金を受領して取引は終了する，という順で決済と物品の受け渡しが行われる。

このように，代金は買い手から売り手に直接支払われるのではなく，買い手と第三者そして第三者と売り手の間の取引の２回に分割される。時間は少し余分にかかるが，取引分割によって安全な代金支払いができる。ちなみに，この場合，商品は売り手から買い手に直接渡され，分割はなされない。

（２）エスクロー・サービスのメリット

この仕組みは参加者全員にメリットがある。買い手は，送付され受領した商品を確認し，当初の取引内容と異なる場合は，商品を返送して取り換えてもらったり，または取引を破棄することができる。

売り手は，買い手が第三者に入金したことを確認してから配送できるため，代金を取り損ねることがない。仲介する第三者は，一定の手数料を取ることで利益を得る。**図表２**では第三者はエスクロー業者と名付けられている。

２－７　分割とバックアップによるセキュリティ

２－７－１　バックアップの課題と経済的背景

バックアップの基礎について説明してきたが，問題点や課題がいくつか残っている。それらを次に説明しよう。

（１）データ・情報のバックアップの課題

バックアップを意味あるものにするためには，バックアップ対象物を常に最新の状態に保つ必要がある。バックアップを常に最新の状態に保つには，オリジナルの変更に対して同期させる必要がある。**同期**（synchronization）とは，２つ以上の場所にある同じデータ・情報が同じ内容になるようにする処理のことである。ある場所にあるデータ・情報に対して何らかの変更が加えられた時，同期処理によって別の場所にある同じデータ・情報にも同じ変更がなされる。

同期は一方向の場合と双方向の場合がある。一方向同期はミラーリング（mirroring）[6]とも呼ばれ，データ・情報は常にオリジナル・ソースからコピー先・ターゲットに向けてコピーされ，逆方向に書き戻されることはない。双方向同期では任意の方向にコピーが行われ，複数の場所で互いに同期がとられる。

バックアップ同期の時間的な方法としては，ある時点のバックアップ終了以降からのすべての変更・追加されたデータ・情報を複製する**差分バックアップ**と毎度前回のバックアップからの変更・追加されたデータ・情報のみを複製する**増分バックアップ**の２つがある。

（２）バックアップのその他の課題

システムが高度化し，その管理は複雑化している。システム高度化に伴い，ストレージは肥大化する一方である。そのような中で，バックアップは長時間化する。そのような課題を「階層管理」,「仮想化」,「重複排除」などの方法でスマートに解決することが望まれている。つまり，単純なバックアップだけに頼るのは不可能になっているのである。

また，バックアップ・システムの立ち上げに係わるデータの取得などについて具体的な復旧手順を定めておく，バックアップ・システムから従前のシステムへの復旧（切戻し）について所用準備時間を見積もっておく，等の課題もある。

２－７－２　工夫して分割しバックアップするセキュリティ

（１）情報の繰返送信

情報は０か１だけ（１次元）であり，途中で誤りが生じたり消失する可能性があるなかで，これらの情報を送りたい，としよう。この場合，情報を３回繰り返し送ることにすればよい。誤りや消失が１個なら，正しく情報を送れる。

送りたい情報が０の場合，繰返送信情報は000となる。送りたい情報が１の場合，繰返送信情報は111となる。誤り（１あるいは０）や消失（X で表す）が１個だけ入り込んでも，残りの２個から正しい情報を知ることができる。

> 繰返送信情報000→001（あるいは00X），010（あるいは0X0），100（あるいは X00）のどれかが受信される→正しい情報は０と判断できる。
>
> 繰返送信情報111→110（あるいは11X），101（あるいは1X1），011（あるいは X11）の

6）東証が2010年１月４日に稼働させた新株式売買システム「arrowhead」では，信頼性向上策の１つとして，サーバーを三重構成にし，メモリー上のデータは３台のサーバー間で自動的にミラーリングし，不具合が起きても処理を継続できるようにし99.999％の稼働率を目指している。

どれかが受信される→正しい情報は１と判断できる。

しかしながら，誤りや消失が２個になると，繰返送信が３回だけでは情報は正しく判断できない。一般に，s 個の消失と t 個の誤りが同時に存在する場合（2t ＋ s ＋ 1）回以上繰り返し送信すれば訂正可能である，という公式がある（説明と証明略）。

（２）暗号化と二重化

等分分割などの単純な分割を行ってバックアップする方法や繰返送信する以外に，色々な方法がある。どのような分割を行ったかを，部外者に知らせないのがセキュリティになるわけである。

最近では，データ量が多すぎてバックアップ処理が間に合わないなど，伝統的方法に無理がきている。復元することを考慮した上で複雑化した分割で，この問題に対応する方法がとられる。

大日本印刷（株）はシステムダウンや災害発生時でもデータの復旧が可能なストレージシステムの開発販売を開始すると2004年３月にプレス発表した。それは，１つのファイルを複数に分割し，それぞれ異なる鍵で暗号化し，データが重複しないよう二重化して異なる３つのデータセンターに保存する。３つのデータセンターのうち１つがダウンしても残りの２つに保存されているデータから復旧が可能になる，そうである。

ちなみに，データ分割は１ファイル全体を区切るのではなく，ファイルの先頭から細分化して複数ファイルに再構成する方式をとる。ファイルが異なるデータセンターに分割して保存されるため，どれか１つが流出した場合でも再構築される心配がない，という。

（３）消失訂正符号

消失訂正符号という技術はデジタル衛星放送・通信サービスで使われている。デジタル衛星放送では例えば降雨時に放送波が雨粒に吸収されてデータパケットが消失してしまい，映像が途切れてしまうことがある。カーナビでは，トンネルや地下に入った時データが届かず欠損する。消失訂正符号はこうした状況を改善するために開発され利用されている。

消失訂正の簡単な例として数値例をあげておこう。送受信の双方が知っている元情報（３次元）は次のいずれか，とする。

{000，011，101，110}

そして，受信情報は1X1，とする。X は消失である。消失位置の情報を元情報に書き加えると，

{0X0，0X1，1X1，1X0}

になる。それゆえ，元情報と対応すると，受信された情報は次であることが判明する。

1X1→101。

この場合，元情報（３次元）のセットが {001，100，010，111} のように111が含まれるようになるのを避ける必要がある。

（４）消失訂正符号の実例

ある会社が開発した事例では，パケット化されたデータ・ファイルを1.5倍から２倍に冗長化したうえで，全国に展開するデータセンターに広域分散配置する。しかも，どのディスク装置に障害が発生してもファイルの復元率が等しくなるように，パケット化されたデータ・ファイルは自律的な動作ですべてのディスク装置に均等に分散配置される。

その結果一部のパケットが消失しても，残っている正常なパケットを使ってデータを自動的に復元することが可能になる，という。例えば，分散配置のレベルにもよるが，７ヵ所のデー

タセンターに分散させた場合なら最大２ヵ所のデータセンターからパケットを読み出せない状況になっても，データを復元できるという。

データをパケットに分割し，複数のディスク装置に分散して保管するストレージサービスを別の会社も開発している。それによると，データをパケットに分割する際，冗長化してデータ容量を170％程度に増やしておく。それを暗号化したうえで，消失訂正符号に基づきパケットに分割し，ネットワーク上の複数のディスク装置に分散して蓄積する。データが必要になれば，パケット（断片）を集めて復号化（復元）[7] する。従来技術よりも少ないコストと運用負荷で，高度な冗長性とセキュリティを実現できる，と言っている。

（５）暗号化鍵分割と量子暗号

量子暗号とは，光の量子力学的効果を利用して，暗号機能を通信路レベルで直接実装する技術である。分割との関連で説明しておこう。

量子暗号では，メッセージの暗号化／復号化に使う暗号化鍵を細かく分割し，それを１つ１つ光子に割り当てる[8]。そして，光子を光ファイバーや空中を介して送ることで鍵を受け渡す。鍵を表現する各光子は極めて微弱なため，途中で盗聴されると状態が変化する。そのため，鍵の受け手は盗聴されたかどうか知ることができ，盗聴された場合には安全でないと判断してその鍵の使用をやめる。こうして，常に安全な鍵を使って暗号化／復号化が行えることになる。

量子暗号自体には，どんな将来技術でも解読できない無条件安全性を達成することが理論的に示されているが，光子は極めて微弱で長い距離を送れないため，その実現は容易ではない。量子暗号の通信プロセスでは，障害が生じうることが知られるようになり，システム全体のセキュリティが万全というわけではない。

２－７－３　秘密分散法

秘密分散法（secret sharing scheme）は，情報を分割，分散化して管理し，その一部が流出したり漏えいしても元の原情報を推測できないようにするセキュリティ技術である[9]。ここには

7） 最尤復号法の一例として，連立一次方程式を解く観点から復号を考えてみよう。５変数（x_1，x_2，x_3，x_4，x_5）体系を想定する。

$x_1 + x_3 + x_5 = s_1$,

$x_1 + x_4 = s_2$,

...

$x_3 + x_4 + x_5 = s_n$,

{si} は送信シンボルである。それゆえ，送信シンボルが５個あれば，５個の未知数と同数の５本の式からなる連立方程式体系となり，式が一次独立であれば解けるはずである。課題は，実質 O 時間で解きたいということである。

8） 量子とは物質の最小単位の粒で，その粒一つずつに情報を載せるのが量子通信である。量子通信では，既存の光ファイバーで伝送できるから，光の粒（光子）を使うのが一般的である。この量子通信を活用した暗号技術が量子暗号通信である。

現行の量子暗号通信手順では，量子通信で暗号鍵を交換し，実際のデータは既存の通信網でやりとりする。まず，量子通信の技術を使って光子１個ずつに０または１の情報を載せて送り，送った情報を基に共通の暗号鍵を生成する。

9） 秘密分散法を利用した秘密通信方法が提案されている。音声情報を秘密分散法により複数の分散情報に分散し，各分散情報をそれぞれ異なる通信経路を介して通信する。全ての通信経路で盗聴が行われない限り，通信内容が盗聴されることはなく，これにより，従来の暗号化通信と比べて高い秘匿性を実現することができる，という。

上で既述の電子割符とも呼ばれる手法も含まれる。RSA Security 創業者の一人であるアディ・シャミア氏の1979年発表の論文が基礎となっており，日本では2000年以降セキュリティ製品に応用され始めている。

（１）秘密分散法

原情報（オリジナル・データ）を例えば A，B，C の３つに分割する際には次の二つの方法がある。ABC が３つすべて揃った場合だけ原情報を復元できる完全秘密分散法，ABC のいずれか２つが揃えば原情報を復元できる閾（しきい）値秘密分散法，である。

完全秘密分散法の場合は１つでも分割データを紛失すると原情報の復元は不可能である。AONT（all or nothing transform）方式[10] が知られている。他方，閾値秘密分散法は，分割データ紛失時のバックアップなどに活用できる。３つに分割したデータのうち，１つを社内のサーバーなどに保存しておけば，分割データの１つを紛失しても原情報を復元できる。

分割された情報はデータサイズが小さくなる場合があり，管理しやすくなるほか，ネットワークの負荷を軽減できるメリットがある。

（２）閾値秘密分散法

閾値秘密分散法は，k-out-of-n 分散方式（k-out-of-n threshold crypto-system）とも呼ばれる，暗号方式の一つである。まず，任意に定数 n と k（n ≧ k）を定めて，原情報を n 個の分散情報（シェア，share）に分割する。復元に必要な一定数が k で，しきい値と言われる。この n 個の断片から k 個集めれば分割された原情報の復号が可能になり，それに満たない k 個未満の分散情報からでは原情報に関する情報を全く得ることはできない（Shamir（1979））。分割数 n と復号に必要な数 k を異なる値にして，復号に冗長性を持たせているので，機密性と可用性を同時に満たすことができるといわれる。しかしながら，通信する情報量が増大するという欠点がある[11]。

この閾値秘密分散法は1970年代以降に開発され，秘密鍵の保管などに使われている。また最近では，ディザスタリカバリの手法のひとつとしても注目されている。易しい解説は，いくつかあるが，例えば岩本（2004）でなされている。

閾値秘密分散法は数学的に証明されている。多項式を基に簡単に原理を説明すると，$y = ax + b$ という方程式の係数 a と b を求めるには，x と y の座標データが最低２つ（の分割データ）が

10）AONT とは，RSA 暗号方式の発明者の一人リベスト教授（Ronald Rivest）によって考案された概念・アルゴリズムで，1999年 CRIPT'99という学会で発表された。
AONT は，元データに対してある演算をかけ，元データとほぼ同じ大きさの出力データを得る。出力データのすべてのビットがそろっていれば容易に元データに復元することができるが，ある程度の数以上のビットがかけると元データへの復元が不可能になるという特性を持つ。この特性から，出力データを複数のデータに分割することで，分割したデータ片がすべてそろわないと元データを復元できないという性質を持つ秘密分散法の１つであると考えられる。
AONT は，従来の秘密分散法と比較して，分割片の数や大きさの比率を比較的自由に設定することができ，分割片を格段に小さくすることができる。また，大きなデータでも変換後の総容量が小さいため処理速度が早い，といった特徴があり，コンピュータ処理に適した秘密分散法と言われている。

11）k-out-of-n 分散方式は（k, n）閾値法とも表わされる。この方法よりも効果的な方法が，（k, L, n）閾値法やランプ型秘密分散法と呼ばれる方法である。秘密分散法は安全性は高いが大きな容量が必要になるという欠点があるので，（k, L, n）閾値法では安全性と符号化効率（メモリー量）との間のトレードオフが考えられている。これは，山本（1985）山本（2004）の発案で，岩本・山本（2004）などを例に共同研究者との研究で進められた。

必要になる。１つの座標データだけでは, a と b の値の組み合わせは無限に存在する。このため, １つの分割データだけを使って元のデータに戻すことは数学的に不可能になるのである。

２－８　分割の経済

以上の展開で示された論点は分割の経済（economies of division）と呼べるだろう。分割の経済は分割することによって費用が低減することを意味する。例えば，２つの資本（K と Z で示す）を使って単一の生産物を生産する企業が，資本 Z を分割して生産を行う場合を考えてみよう。費用 C は，分割しない場合より，資本 Z を Z_1 と Z_2 の２つに分割する場合の方が，低くなる。次の式で分割の経済は表わされる。

$$C(K, Z) \geqq C_1(K, Z_1) + C_2(K, Z_2)$$

Z_1，Z_2，と Z の関係は，次になる。等号のケースを含む。

$$Z \geqq Z_1 + Z_2。$$

３．ネットワークの特性とセキュリティ

３－１　ネットワークのセキュリティ

電力システムが破壊されるという事態を想定してみると，セキュリティの必要性が分かる。ネットワークの下流にあたる顧客の電話会社や金融機関などのシステムがドミノ倒し的にダウンし，電気だけでなく，電話や金融などの多くの市民サービスが停止する可能性がある。また，そうした広範な社会的損失を金銭的に計上し，１つの電力会社にその損害補償を求めるとしたら，一企業が負担できる範囲をはるかに超えてしまう。他方で，一般事業会社や金融機関は自家発電装置を備えてセキュリティ対策をしている。

特徴的なネットワークには最適なセキュリティが知られている。一部を紹介しよう。

（１）スケールフリー型ネットワークとそのセキュリティ

多くの構成要素とリンクしているハブとその他多数の構成要素（ノード）からなるネットワークは，スケールフリー特性を持つネットワークといわれる。スケールフリーのネットワークはハブが支配している。

このネットワークは，一般に，障害に対する頑強性が高い。故障はどのノードで起こるか区別しないので，小さなノードも大きなハブも同じ確率で発生する。それゆえ，スケールフリー・ネットワークは構造的に不平等である。それは故障が起こっても，その頻度とは不釣り合いなほど小さなノードに影響を与えるだけだからである。

スケールフリーなネットワークでは，全ノードのうちの５％がダウンしたとしても，代替経路の存在によってノード間の接続を維持でき，システム全体の平均最短距離はほとんど変化しないのである。同じノード数，同じリンク数でトポロジーが異なる他のネットワークではこのような特性は見られない。

他方で，標的型攻撃に対しては，スケールフリー・ネットワークは弱い。つまり，特定の重要なハブをピンポイントで狙った攻撃に対しては脆弱であるという弱点も併せ持っている。次数の集中した上位５％のノードがダウンしたとすると，システム全体の平均最短距離は約２倍にまで増大してしまうとする（Albert, et al.（2000）。参考文献は辰巳（2010a）の巻末を参照）シミュレーション結果がある。

（２）鎖国型ネットワークのセキュリティ

社外への PC の持ち出しを禁止している，あるいは外部から社内ネットワークへのアクセスを制限している企業は少なくない。これによって，セキュリティ・リスクは確かに軽減されるが，ICT を活用してこそもたらされる様々な効果も，同時に封じ込めてしまう。

現在，多くの企業が導入しているセキュリティは，程度の差はあれ，このような鎖国型である。サーバーとクライアントをまとめて管理し，社内ネットワークとインターネットを明確に分ける考え方である。一般的なネットワーク構成とはいえ，外部から社内へのアクセスは制限されるため，他のネットワークとのコラボレーションを重視する組織にとっては，このタイプのネットワークのセキュリティは向かず，創造性が生まれにくくなる。

（３）個別対応型ネットワーク・セキュリティ

個別の取引毎に個々人や個々の会社がセキュリティをチェックする方法は，個別対応型ネットワーク・セキュリティと呼ばれる。これには，外部委託型セキュリティ・チェック方式と内部遂行型セキュリティ・チェック方式がある。

３－２　コンテンツ・デリバリ・ネットワークやＰ２Ｐのセキュリティ

よく知られている超巨大な同時受信の例は2009年１月の米国大統領の就任演説のライブである。全世界の何百万もの人が同時に見た，と伝えられた。それを可能にしたのはコンテンツ・デリバリ・ネットワーク（Content Delivery Network, CDN）である。

CDN とは，インターネットを介してつながっている多数の利用者に，コンテンツ（情報の内容）を効率よく配信できる仕組みを持つネットワークのことである。CDN とそれがセキュリティに対して持つ意味を考えてみよう。

コンテンツを１ヵ所のサーバーだけで処理せず，複数のサーバーを連携させることで，多数の利用者に素早く配信できる。動画などの大容量コンテンツの配信に役立つ。

インターネットの世界では，「画面の切り替えに８秒以上の時間がかかってはいけない」という暗黙のルールがあると言われる。８秒以上待たせてしまうホームページは，利用者が途中で見るのをやめてしまうという傾向があるといわれ，ホームページの表示速度の向上が必須なのである。

スピーディな配信を実現する CDN によって，新たなウェブ・サーバーを購入したり，データセンターを新設する，通信回線を増強する，といった巨額の投資をする必要はない。

ネット社会の高度化と CDN は密接に結びついているのである。このような CDN を業とする会社が構成する業界の分析についてはアーランガー（2007）を参照。

（１）負荷の分散

ネットワークの負荷を軽減するために，負荷を分散する方式には２つある。いずれも，いわゆるロードバランサー（負荷分散機能）[12] を利用する。

まず第一は，待機系が，現用系に入力されるジョブを監視していて，処理量の大きいジョブが入力されると，現用系に代わってこれを実行する。もう一つは，待機系は，現用系の負荷状態を監視していて，現用系のオーバロード（過負荷状態）を検出するとオーバロードした分の

12）Windows Server で提供する負荷分散機能の１つであるネットワーク負荷分散サービス（NLBS，Network Load Balancing Service）を使うと，仮想的な１つの IP アドレスに最大32台までのサーバーを割り当てられる。この仮想 IP アドレスに対して次々に送られてくるクライアントの接続要求を各サーバーで順番に処理することで負荷を分散する（『日経 Windows プロ』2006年８月９日参照）。

処理を引き受けて実行する方式である。

（2）負荷分散のネットワークとセキュリティ

コンテンツ・デリバリ・ネットワーク（CDN）とは，大容量のデジタル・コンテンツなどを配信するにあたって，ユーザーからやってくるアクセスを複数のサーバーに振り分け（分散させ），ユーザーに近いサーバーから実際のデータ配信を行うネットワーク・システムのことを言う。

このような方法は，送信するコンテンツが大容量であるため，ひとつのサーバーでは処理しきれない場合に効果的である。

大容量コンテンツの場合だけでなく，ふつうの容量の場合でも，アクセスが集中し，反応が遅くなったり，まったく応答不能になる（フラッシュ・クラウド効果という）現象に対処するには，サーバーを一ヵ所だけに置くのではなく，地理的あるいはバックボーン的に複数に分散させ，ユーザーに近いサーバーにコンテンツをキャッシュし，そこから配信すれば効果的にサーバーの負荷を分散することができる。このサーバー分散は，個々のサーバーはコピー行動をしているだけではあるが，**送信という機能の分割**とみなせるだろう。

このようなサーバーの負荷分散を徹底すれば，ひいては，それがネットワークのセキュリティを確保する。ハブのコピーがいくつか作られ，それらへリンクが張られるからである。

いわゆるDDoS攻撃[13]やボットネット攻撃（多数のPCにボット[14]と称されるウイルスが知らずに埋め込まれ，それが攻撃者の命令により特定のシステムやPCを一斉にアクセスする形で攻撃する）には有効な対応策になり，実際も米国[15]で有効性が報告されている。

ふつうの情報送信（片方向）の流れ（**図表３**）との対比で，このような役割を果たすCDNを**図表４**に図示した。

さらに，一般のセキュリティの観点に限ってみても，**図表４**のように，ルーターA，B，Cの間で連携を保てば，それらのうち1,2がユーザーからの攻撃によってダウンしても，残り２つや１つのサーバーで，過重問題がなければ，システムは維持できる。

（3）アプリケーション配信ネットワーク

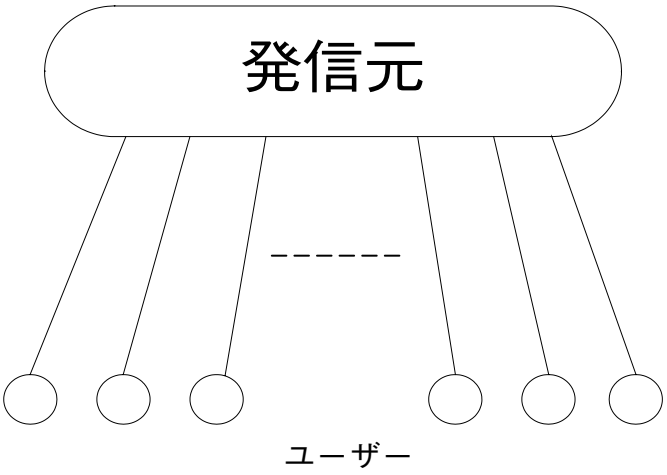
CDNの考え方はアプリケーションを配信するネットワークに発展している（メッツラー＆テイラー（2010））。先に記したように，ネットワークは，最低限の接続性が確保されていればよいという考えから，サーバーの負荷を緩和する方針に変わり，さらに複数のサーバーを設け

13）DDoS攻撃（Distributed Denial of Service Attack）とは，第三者のPC等端末にウイルスである攻撃プログラムを仕掛けて，それを踏み台にし，踏み台とした多数の端末から標的に大量の文書やパケットを同時に送信し過大な負荷をかける攻撃である。分散サービス妨害とも訳される。このように攻撃元が複数で，標的とされたコンピュータが１つであった場合，その標的とされるコンピュータにかけられる負荷は非常に大きなものになり，攻撃された特定のシステムは混雑によって利用不可能になる。攻撃元が１つの場合はDoS攻撃と呼ばれる。
DoS攻撃やDDoS攻撃は，これを簡単に実行させるためのツールがインターネット上で出回っており，現状では標的にされれば完全に防ぐ方法はなく，インターネットの根幹に対する脅威であるとみられている。完全に防ぐ方法はないが，仕掛けられたプログラムを発見するツールは多数提供されている。

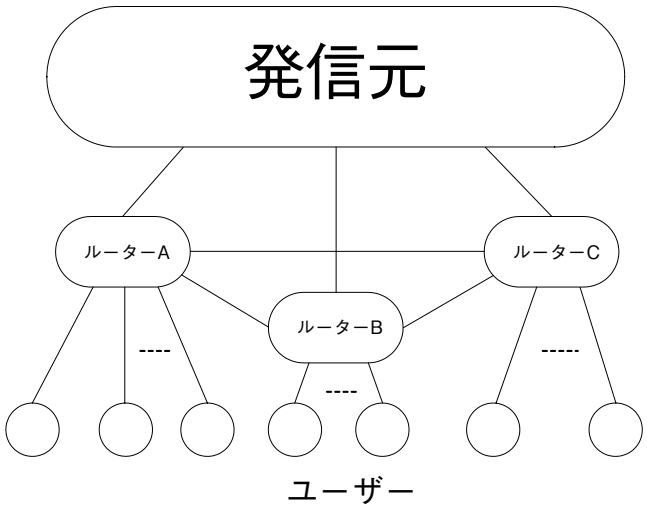
14）botとは一定のルールに従って言葉を発するロボット，または一定のルールに従って情報を発信するように設計したプログラムのことである。検索エンジンの情報収集用プログラム，コンピュータウィルスで乗っ取ったパソコンを操作するプログラムなどの意味にも使われる。

15）他方，韓国では，同時期の2009年７月７日から10日にかけて，政府サイトと銀行，大手ショッピングサイトなどがDDoS攻撃を米国と同じように受けたが，大混乱に陥った，と報道されている。

図表３　ふつうの情報送信（片方向）の流れ



図表４　コンテンツ・デリバリ・ネットワークの流れ



る方向になったわけである。

さらに，サーバー群の中で最も処理負荷のかかっていないサーバーに処理させることによって，アプリケーション配信品質を維持するだけでなく，それを向上させようという考えになっている。つまり，各サーバーの可用性や現在の負荷といったパラメターに基づいて，どのサーバーがリクエストを処理するべきかを決定し，そのサーバーにリクエストをするという，リクエスト割り振りを行うのである。

そして，さらに，このような負荷分散機能に加えて，負荷の大きな処理をオフロードして，サーバー外でクライアントからのリクエストに対処するという方法も考えられている。

（4）P2P

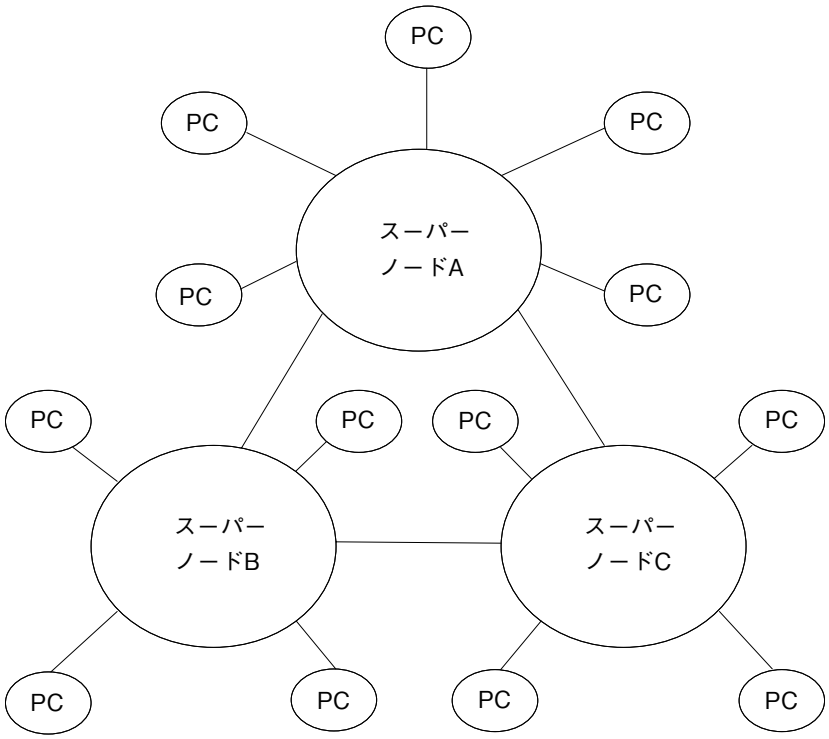
さらに発展させたものは，個人間のインターネット電話などに利用されるP2P（peer to peer）の仕組みであろう。P2Pでは，サーバーの機能を複数に分け，それをネットに接続しているふつうのPCに負わせる。そうすることによって，多額なサーバー費用を実質上ゼロにする。サーバーの機能を担うPCは，常時電源が入っている，処理スピードが速い，通信回線が速く安定的であるという３つの条件を満たすPCから（自動的に）選ばれ，スーパーノードと呼ばれる。

ネットワーク内のPCはいくつかの小さなグループに分けられ，各グループに１つのスーパーノードが選ばれる。各小PCグループはスーパーノードを中心とする集中型のサブ・ネットワークになる。ネットワーク全体の内では，スーパーノード間で通信が行われ，完全な（接続された）ネットワークになっている。

通信は次のような順で行われる。１つのPCから発せられた通信はまず属しているグループを代表するスーパーノードA（例えば）に繋がれ，そのスーパーノードAはIPアドレスから送信すべき先の該当のスーパーノードBを見つけ出し，そのスーパーノードBへ送信する。しかる後スーパーノードBは自グループ内の送信先PCへ，情報を送る。

図表３における図中の「発信元」をサーバーに，ユーザーをPCに代えれば，一般の通信ネットワークを示すことになる。**図表５**が直前のパラグラフで説明された通信の経路を示している。災害などによる通信ピーク時の混雑は，このような仕組みで，回避できる。

図表５　P2Pのネットワークの流れの例



4．まとめ

分割するとはどういうことなのか。その意味は，単純ではなく，われわれの予想を超えている。

分割すると，規模の経済が達成できない，のではないかという心配がある。既述のように，それは必ずしも正しくない。分割して規模の経済が達成できる場合が存在する。

取引規制で取引を禁止することによって，ネットワークは切断される。これは効率性などの観点からはマイナスである。しかしながら，セキュリティの観点からは必ずしもマイナスとは言えない。

分割するのは，主として，セキュリティのためである。大きな効果をもたらす事例が多数あることを本稿では見てきた。

（以上）

参考文献

アーランガー，レオン「再び注目が集まるCDN（コンテンツ配信ネットワーク）―SaaS時代を迎え，存在感を強めるCDNプロバイダー」『月刊Computerworld』2007年12月号。

岩本琢哉（2004）「注目の情報管理方式「しきい値秘密分散法」」@IT編集部，2004年11月27日。

岩本貢・山本博資「一般型アクセス構造に対する強い秘密保護特性をもつランプ型秘密分散方法式」『第27回情報理論とその応用シンポジウム予稿集』，2004年，pp.331-334。

岡本龍明・山本博資『現代暗号』産業図書，1997年。

メッツラー，ジム＆テイラー，スティーブ，「「アプリケーション・デリバリ2.0」とは何か―クラウドがWANにもたらす新たな課題」『月刊Computerworld』2010年８月４日。

酒井裕司（2006）「情報銀行：セキュアでリーガルなPtoP型オンラインストレージの開発」@IT編集部，2006年３月31日。

Shamir, A., “How to share a secret,”Communications of the ACM, Nov. 1979，Vol.22，No.11，pp.612-613.

辰巳憲一（2008）「金融活動における情報と価格～展望と論評」『学習院大学経済論集』2008年10月，pp.211-221。

辰巳憲一（2009）「金融活動における情報と金融仲介業～展望と論評」『学習院大学経済論集』2009年１月，pp.303-324。

辰巳憲一（2010a）「金融活動における情報ネットワークと金融仲介業（I）～金融ネットワークの経済学入門」『学習院大学経済論集』2010年４月，pp.13-39。

辰巳憲一（2010b）「金融活動における情報ネットワークと金融仲介業（II）～金融ネットワークの経済学入門」『学習院大学経済論集』2010年７月，pp.95-122。

山本博資「(k, L, n) しきい値秘密分散システム」『電子通信学会論文誌』, Vol. J68-A, No. 9 , September 1985, pp.945-952.

山本博資「秘密分散法とそのバリエーション」『数理解析研究所講究録1361巻』，京都大学，2004年，pp. 19-31。