Vol.2014-SPT-12 No.13
Vol.2014-EIP-66 No.13
2014/11/21

企業の営業秘密保護と情報セキュリティ対策

小松文子[†1]

高度な情報通信社会において，情報資産としての機密情報はサイバー攻撃や内部不正などの脅威にさらされている．今や情報セキュリティ対策はこのような情報資産を情報漏えいや窃取，破壊などから保護するために必須である.このため，不正競争防止法によって法的に保護される営業秘密としての要件を，情報セキュリティ対策によって講ずることも多い.本稿では，近年の情報セキュリティの状況と営業秘密を保護するための情報セキュリティ対策と課題について述べる..

Information Security and Protection of Trade Secret

AYAKO KOMATSU[†1]

In advanced information-communication society, confidential information as information property is exposed to threats, such as cyber-attacks and internal injustice. Now, the measure of information security against is indispensable in order to protect such information property from an information leak, theft, destruction, etc. For this reason, it will decide upon requirements as trade secrets legally protected by Unfair Competition Prevention Act by the measure against an information security. This paper describes the situation of information security and subject for protecting trade secrets by measures of information security.

1. はじめに

高度な情報通信社会において，企業の営業秘密などの電子化された情報は，常に脅威にさらされている.世界中で，国家・企業の機密情報を狙ったサイバー攻撃，情報漏えいなど様々なインシデントが発生している.

2011 年 9 月に重電企業を狙った標的型攻撃が大々的に報道されたが，その後も官公庁や企業を狙った攻撃が後を絶たない.(独)情報通信研究機構の発表によると[1]，2013 年 1 年間に，国内外からの国内に向けた悪意ある通信は，約 128 億パケット観測されている.また，2014 年にはいり従来，公表されることが少ない内部不正による被害も複数報道されている.技術情報などの知的財産が電子化され，情報資産として管理されている場合，組織外からの攻撃や内部不正などの脅威からその資産を保護するためには情報セキュリティ対策が必要である.本稿では，まず組織や個人が置かれている情報セキュリティ脅威の状況を述べ，これらに対抗するためのセキュリティ対策について述べる.さらに，営業秘密保護に対する法制度との関連と，今後の課題について述べる.

2. 企業の機密情報を取り巻く状況

情報セキュリティは，情報資産に対する機密性，完全性，可用性を維持すること.さらに真正性，責任追跡性，信頼性などの特性を維持することも含める場合もある[2].また，情報セキュリティにおける脅威は種々存在するが，脅威が発生する場所の観点からみると，悪意を持った攻撃者によるいわゆるサイバー攻撃（外部攻撃）と，内部者による不正行為に分類することができる.

2.1 サイバー攻撃

近年，組織外からのサイバー攻撃は，複数の手口を組み合わせたものである.たとえばドライブバイダウンロードは，図 1 に示すように，利用者のパソコンにウエブサイトを閲覧させただけでウイルスを感染させ，そのウイルスによって，組織内の情報を盗みだすという，ウエブの不正改ざんとウイルスという 2 つの手口からなる.特定の組織の職員を狙う標的型メールに記載された URL や，添付ファイルをクリックすること，ウイルスを仕込んだ不正サイトを訪問した際に感染させるなど，様々な手口でウイルスを感染させたのち，狙った情報を外部へ転送する.なお，情報資産を管理するシステムには，本来の動作を妨げたり，不正な動作を引き起こす脆弱性が存在し，攻撃者はこれを狙って攻撃することが多い.閲覧した利用者のパソコンがウイルスに感染するよう改ざんされた不正ウエブサイトの JPCERT/CC に届け出られた件数は，2012 年度は 2,856 件であったが，2013 年度は 7,726 件を記録し，過去最悪の状況である[3].

このような背景のもと，攻撃を早急に察知し以降の被害を防ぐことを目的に，標的型攻撃を対象として，情報共有の枠組みである J-CSIP が 2011 年より開始された.

図 1　ドライブバイダウンロード攻撃[10]

†1 (独)情報処理推進機構　セキュリティセンター　情報セキュリティ分析ラボラトリー

ⓒ 2014 Information Processing Society of Japan

引用：（独）情報処理推進機構　https://www.ipa.go.jp/security/txt/2010/12outline.html

表 1　J-CSIP によって分析された情報件数

	累計	2014 年 1 月～3 月	2013 年 10 月～12 月	2013 年 7 月～9 月
情報提供件数 （参加組織への情報共有件数）	259 （59）	95 (40)	121 件 （51）	95 件 （34）

同等の攻撃メールが複数情報提供された際に情報共有を 1 件に集約することや，広く無差別にばらまかれたウイルスメールと判断して情報共有対象としない場合がある.IPA が独自に入手した情報で J-CSIP 参加組織へ情報共有を行ったものは 6 件である.引用：情報セキュリティ白書 2014[4]

J-CSIP は，図 2 に示すように，（独）情報処理推進機構（以降，IPA）がハブ（情報集約点）となり，業種ごとの領域で 5 グループ（Special Interest Group:SIG）を形成し IPA との間で NDA を締結し標的型攻撃などの情報共有を図っている.具体的には，標的型攻撃を IPA が分析し，必要な場合はグループ内へ速やかに情報を発信して，被害の拡大を防ぐことを目標としている.さらに社会全体への影響が大きい重要な攻撃などについては，経済産業省，JPCERT/CC，NISC，C4TAP などとの情報連携も想定している.J-CSIP によると，2013 年 7 月以降の標的型メール等の不正アクセスの数は表 1 に示すような傾向にある[5].攻撃メールの 45%は添付ファイルによるもウイルス感染のであり，また添付ファイルの 56%は実行ファイルであった.

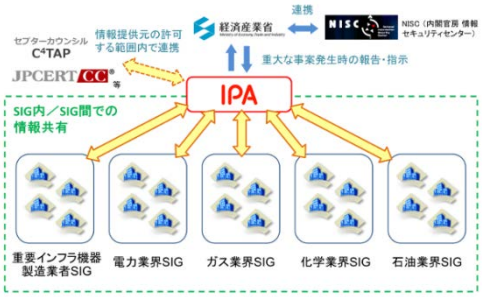


図 2　情報共有のしくみ（J-CSIP）
引用　http://www.ipa.go.jp/security/J-CSIP/

2.2 内部の脅威

内部不正とは,組織の情報へアクセス可能である職員などの内部者による，組織内部の情報資源（データ，ネットワーク，情報機器など）への不正な行為によって，組織の事業に負の影響を与えることである.不正な行為には，情報流出や情報破壊などがある.米国の調査[6]では，557 の回答者のうち，内部者による事故を経験した者は 37%であった.また，犯行者の内訳は，内部者 28%，外部者 72%に対し，どちらセキュリティ事故の被害金額が大きいかとの問いに対しては，内部者が 46%，外部者は 54%という結果が公表されている.これは，内部不正が，情報資産にアクセス可能な権限を付与された内部者によって引き起こされるため，いったん発生するとその被害が甚大となることを示している.したがって企業の機密情報の窃取を図る原因として，内部不正は大きな脅威といえる.

米国 CERT は，情報セキュリティ事故についてベンダ，ユーザ等の調整をする機関として発足したカーネギーメロン大学における 1 組織である.2000 年ごろから，内部脅威に関するプロジェクトを開始し，現在は，内部脅威センター（Insider Threat Center）が設置され，2014 年 2 月現在で 850 もの内部不正事例を収集・分析することによって，効果的な内部不正防止対策を提唱している.一方，日本国内では，政府等の同様な活動はなく，いくつかの断片的な調査分析が公表されているのみである.筆者は，2011 年より，組織内部の脅威についてインタビュー調査とアンケート調査実施を主導した.調査では，対象とした内部不正を法的に係争となったものだけではなく，組織のルール違反についても含めている[7].図 3 は，インタビューで収集した 19 の事例について，不正行為者，不正対象，動機，不正行為の環境における監視性について分類したものである.不正対象としては，顧客情報が最も多く，52.6%，次に社内情報が 15.8%，開発情報は 10.5%であった.また，動機については，組織・上司への不満が最も多く，42.1%，次に金銭の 31.6%である.単に情報を得たいとするもの，転職・企業が続く.また，不正が行われた環境として，本人以外の目があるか否かという監視性については，73.7%で，低い状況であった.標本数が少ないため，一般的な状況としては判断できないが，他に類似の調査は少ないため，一例として参考になると考えられる.

ⓒ 2014 Information Processing Society of Japan

Vol.2014-SPT-12 No.13
Vol.2014-EIP-66 No.13
2014/11/21

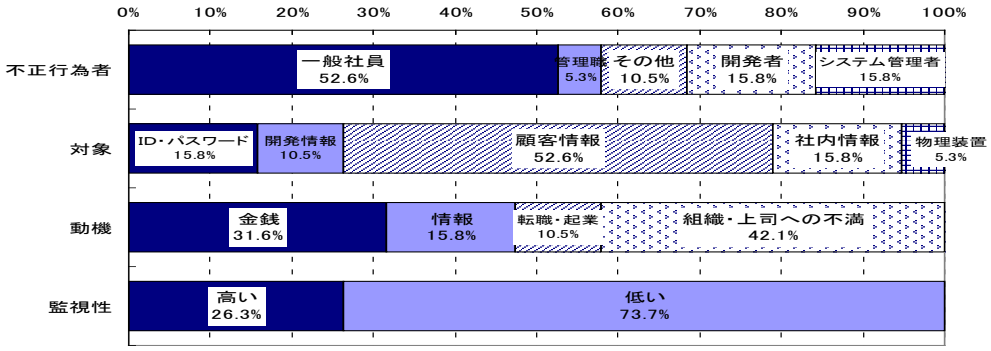


図３　インタビュー結果による内部不正の状況

3. 情報セキュリティ対策と営業秘密保護

3.1 情報セキュリティ対策

これまで述べたような，外部攻撃や内部不正に対して，いかに有効な情報セキュリティ対策を実施するかを述べる.

(1) セキュリティガバナンス・情報セキュリティマネジメントの確立

情報セキュリティ対策を経営課題とし，組織横断で取り組むための，経営者のコミットと，組織内での取り組み体制を確立することである.図 4 に経営層によるセキュリティガバナンスの全体像を示す.経営層は，情報セキュリティリスクをリスクマネジメントの枠組みでとらえ，経営者の善管注意義務，残留リスク， Need to Know の原則， 適切なセキュリティ投資規模を考慮しつつ，事業ラインへの方針決定，モニタリングを行い，社内外に責任をもつ. 情報セキュリティ対策実施にあたっては，リスクマネジメントの一環として，リスク分析を行う.具体的な脅威事象の特定，脆弱性や状態の特定，またそれらの発生確率，影響度を決定し，どのような対処をするかを決定するものである（図 5）.

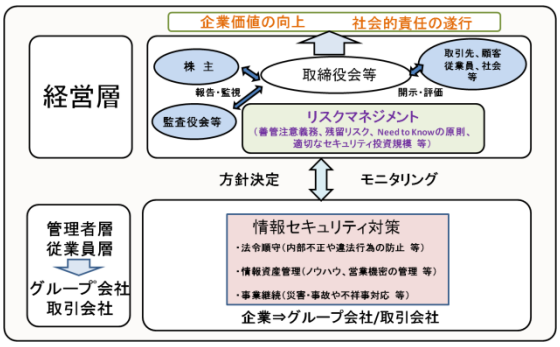
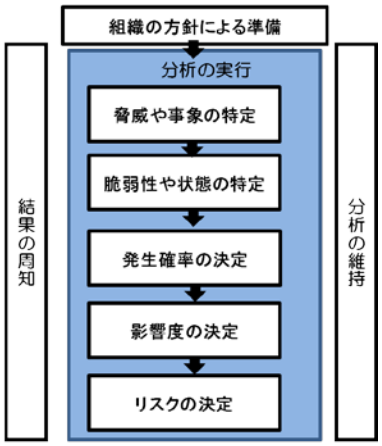


図４　情報セキュリティガバナンス

リスク分析の結果として,表 3 にあるようなリスクの回避，低減（最適化），移転，保有の４つのリスクに対する対処を決定する[8].



出典　：NIST　SP800-30 Rev.1 Guide for Conducting Risk Assessments　よりIPA　邦訳
http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

図５　情報セキュリティ対策におけるリスク分析

(2) 情報セキュリティ対策の実施

リスクを最適化すると判断したものについては，情報セキュリティ対策を講ずることとなる.対策には，技術的対策，組織的対策，物理的対策，人的対策などがあり，費用とその効果に見合う対策を選択する必要がある.技術の進展によって，脅威も変わっていくことから，いったん対策を実施したとしても，常に監査などによって状況をモニタし，対策の有効性をチェックする必要がある.また，事前対策だけではなく，事後対策として，情報セキュリティ事故が発生した後に，その原因を追究するためのフォレンジクスに必要な情報を確保可能なようにログの取得も必要である.さまざまなセキュリティ対策が考えられるが，一例として情報漏えい対策をあげると，必要な対策は，①情報システムにおける利用者のアクセス管理②個人の情報機器及び記録媒体の業務利用及び持ち込みの制限③ネットワーク利用のための安全管理④情報機器や記録媒体の持ち出しの保護，⑤組織外部での業務における情報の保護などである（図 6）.

ⓒ 2014 Information Processing Society of Japan

Vol.2014-SPT-12 No.13
Vol.2014-EIP-66 No.13
2014/11/21

表 3　リスク対処の分類

	リスク対処内容
リスクの回避	リスクを生じさせる活動を，開始または継続しないと決定することによってリスクを回避すること
リスクの最適化	·ある機会を追及するために，リスクを取るまたは増加させること ·リスク減を除去すること ·起こりやすさを変えること ·結果を変えること
リスクの移転	一つ以上の他者とリスクを共有すること（契約およびリスクファイナンスを含む）
リスクの保有	情報に基づいた意思決定によって，リスクを保有すること

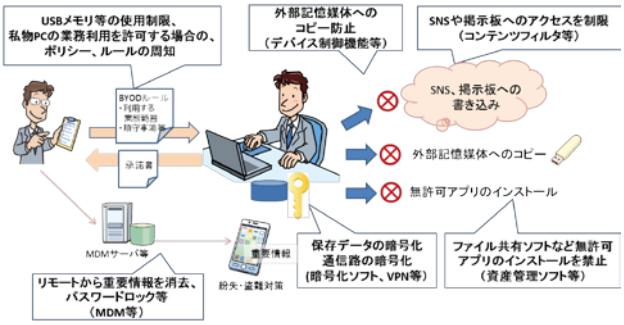


図 6　一般的な情報漏えい対策

3.2 秘密管理性と情報セキュリティ

すでに述べたように，情報セキュリティの観点から，情報資産を保護するためには，その情報資産が，設置された環境において考え得る脅威によって損壊，流出するなどし組織の事業にいかなる損害を与えるかを評価し，その対策費用とのバランスを考慮しリスク分析の結果，情報漏えいなどにあるようなリスクに対する対策を実施する.一方，情報資産を営業秘密として保護する際には，不正競争防止法における営業秘密としての 3 要件，すなわち，①秘密として管理されていること，②有用な情報であること，③公然と知られていない，が事故後に法的な保護を受けるために必要な要件である[9].

営業秘密管理指針には，裁判例から，①については，アクセス制限の存在，客観的認識可能性の存在を必要としている.アクセス制限の存在については，1)情報の秘密保持のために必要な管理をしていること 2)アクセスした者にそれが秘密であることが認識できるようにされていること（客観的認識可能性の存在），とし，これらを詳細化し，管理方法を提示している.判例から，全般的な傾向として，以下の三点に着目していると考えられると記述されている.

A. アクセスできる者が限定され，権限のない者によるアクセスを防ぐような手段が取られている（アクセス権者の限定・無権限者によるアクセスの防止）

B. アクセスした者が，管理の対象となっている情報をそれと認識し，またアクセス権限のある者がそれを秘密として管理することに関する意識を持ち，責務を果たすような状況になっている（秘密であることの表示・秘密保持義務等）

C. それらが機能するように組織として何らかの仕組みを持っている（組織的管理）

これらの A～C について，営業秘密管理指針では，「営業秘密の管理のために実施することが望ましい秘密管理方法」が規定されている.表 4 に，そのうち，組織的対策を除いた部分の概要を挙げる.まず(1)秘密指定･アクセス権者の指定，(2)物理的・技術的管理(3)人的管理，(4)営業秘密侵害に備えた証拠確保等に関する管理に分類され，(2)には，さらに，詳細な記載がある.また，対策を実施する際に参考となる「一般的な管理」と，さらに必要と判断した場合のために「高度な管理方法」が提示されている.表 4 では，各項目に対して，考えられる情報セキュリティ対策を対応づけた.これからわかるように前述の A.B の要件として，情報セキュリティにおけるアクセス制御機能が求められている.しかし，営業秘密管理指針は，判例を参考として記載されていることから，記載内容は，各項目に散在しており，たとえば，セキュリティ機能としての「本人認証」としてではなく，「パスワードを設定」など，実際の具体的な手段が記載されている.また電子情報として扱う場合の対策項目としても十分とは言えない.ここで，情報セキュリティの領域におけるアクセス制御のモデルを改めて概説する.

情報セキュリティにおいて，人などの主体者（サブジェクト）が，情報資産などの対象（オブジェクト）に対してアクセスを制御する仕組みは，「識別・認証」機能，「アクセス制御」機能を含み，機密性を維持する機能である（図 7）.例えば，営業秘密である情報資産を守るシステムにおいては，サブジェクトは組織の従業員で，オブジェクトは保護すべき機密情報にそれぞれ対応する.以下にそれぞれの機能を説明する.

まず，主体に識別子（ID）を付与し，認証では，識別された主体者が，本当にその主体者であることを確認する.認証のためには，主体者と認証検証者間で，パスワードなどの秘密情報を共有することで認証する方式，一時的な秘密情報の共有によるワンタイムパスワード方式，その他公開鍵暗号方式などの高度な暗号を利用する方式，さらに，耐タンパ性と呼ばれる物理攻撃から保護可能な暗号演算付きスマートカードなどを利用するなど複数の安全性のレベルが異なる認証方式がある.

ⓒ 2014 Information Processing Society of Japan

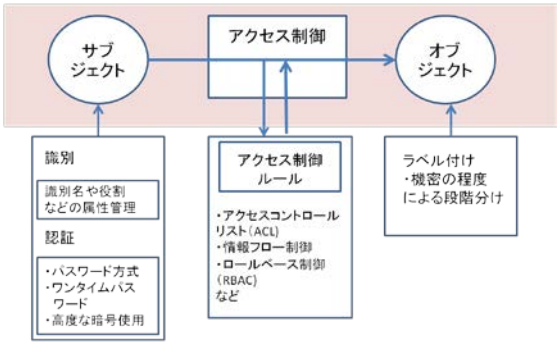


図 7　識別・認証，アクセス制御機能のモデル図

次に対象については，その機密の程度によるレベル分けを行う.これをラベル付けやクリアランスという.識別された主体と対象間のアクセスの許可・不許可を制御する機能が「アクセス制御」である.許可・不許可を規定するルールには，よく知られたものに，ファイルの識別子にアクセス可能な利用者 ID を関連づけるアクセスコントロールリスト方式，主体者にもラベルを付け，オブジェクトのラベル間の情報フローを制御する情報フロー制御方式，主体者に役割を付与し，その役割（主体者個人ではなく）とオブジェクトとのアクセスの制御するロールベース制御（RBAC）などがある.さらに，この機能が問題なく動作するためには，それを監査するためのログ収集機能と分析機能が必須である.なお，外部者による不正アクセスについても，原則としては同じモデルであるが，システムアーキテクチャ上，ネットワークのシステムが処理する主体となるため，選択できる機能には制限がある.たとえば，ファイアウォールではネットワークのアドレスである IP アドレスによって識別される送信元を認証する機能はない.

情報セキュリティにおける識別・認証，アクセス制御の各機能は，前述した営業秘密管理指針における判例から求められる全般的な傾向としての 3 点のうち，A と B の一部である「秘密であることの表示」を満たすと考えられる.ただし，情報セキュリティ対策として，これら機能を実装する際には，さらに，各機能における複数の方式のどれを選択するかを決定しなければならない.営業秘密管理指針には，機密情報の管理として，詳細な項目をチェックし，組織自身がその管理の程度を知ることができるように点数化するチェックシートが含まれている.ここに，「コンピュータ管理」の項目として，パスワード等という項目があり，パスワードを設定する，起動時に生体認証を必要とする，と例示されている.本シートでは，技術情報が電子情報として保管，活用されている状況についてのチェック項目がわずかであり，十分とは言えない.たとえば，パスワード方式の認証を実装する場合，パスワードの桁数，文字の種類をいかに選択するかがが安全性を決める.2013 年に航空会社で相次いで不正ログイン攻撃が発覚した事故では，これらのシステムはパスワードを数字 4 桁や 6 桁で運用していた.今や，4 桁や 6 桁のパスワードにより利用者を認証することで機密性を確保できる，と主張することは困難であると言える.

C　組織的管理に対する，情報セキュリティ対策は，3.1（1）で述べた「セキュリティガバナンス」「セキュリティマネジメント」の構築によって実現できる.しかし，多くの企業では，情報セキュリティと営業秘密保護を担当する部門は異なるため，それぞれの要件を満足することに終始してしまう危険をはらむ.効果的な保護のためには情報共有と相互理解を推進し，さらに横断的な体制を構築する必要がある.

3.3 営業秘密管理指針と情報セキュリティ対策

営業秘密が電子情報である場合は，情報セキュリティによる対策をするうえで，保護指針に散在する項目を集め補完し，セキュリティ機能として実現する必要がある.秘密指定，アクセス権者の指定，客観的認識可能性，分離保管などについては，3.2 で述べた識別・認証，アクセス制御のモデルにより，まず従業員を識別し，権限を付与する.ラベルが付与されたファイル等の営業秘密である機密情報に対して，アクセス制御のルールを設定し，権限のあるものだけが機密情報にアクセス可能とするメカニズムを実現すればよい.さらに，事後の追跡可能性のために，ログを収集する必要がある.他にも，電子情報を保護するためには，一般的な情報漏えい対策で述べたように，個人の情報機器及び記録媒体の業務利用及び持ち込みの制限や，ネットワーク利用のための安全管理，情報機器や記録媒体の持ち出しの保護，組織外部での業務における情報の保護などが必要である.これらの対策については，その実現するセキュリティレベルによって，複数の選択肢がある.リスク分析によってどのレベルを実現するかを決定することが重要である.

本原稿執筆時点で，経済産業省の産業構造審議会における知的財産分科会，「営業秘密の保護・活用に関する小委員会」では，営業秘密管理指針における法的な保護について議論が始まっている.企業の営業秘密の多くが電子化されている現状で，事後に法的保護を受けることが可能な対策と，事前にあるべき防犯としての保護対策は，明らかに異なる.企業にとって侵害を受けた後の被害を考慮すれば，事前対策としての情報セキュリティ対策も必須である.しかし，営業秘密管理指針において，この区別が不明瞭であるため，企業においての運用に支障を起こすことが懸念されていた.既に述べたように，営業秘密管理指針に記載されている一般的な管理や高度な管理は，情報セキュリティの観点から一貫性が乏しいと言わざるをえない.したがって，サイバー攻撃や内部不正，情報技術の進展に伴う脅威の増大に対応可能な対策指針が必要であると考える.

4. 課題

近年のサイバー攻撃の状況と，内部不正についての現状，不正競争防止法における営業秘密の管理に求められる情報セキュリティ対策について述べた.

ⓒ 2014 Information Processing Society of Japan

現状の営業秘密管理における電子情報資産の保護に対しては，課題も多い.以下にそれぞれの課題について述べる.

（1） 企業におけるリスク分析

企業や組織において，サイバー攻撃や内部不正などの事故によって蒙る被害を想定し，算定する必要がある.しかし，被害額の算定や蓋然性表す確率は特に困難である.これらは，情報資産への資産価値の算定の困難さと，事故情報の収集が困難であるという背景がある.また，対策を講ずることによる効果算定も定量的な手法が確立されていない.

（2） 内部不正事故情報の共有

外部攻撃については，J-CSIP のように，情報共有の枠組みが確立されているが，内部不正による情報漏えいなどの事故情報は，組織外へ公表されることは少なく，内部で処理されがちである.米国では，CERT の内部脅威センターが長年にわたり情報収集しているが，国内にはそのような機関が存在していない.このため，過去の失敗事例を教訓として将来の対策に役立てることができない.

（3） 技術的課題

営業秘密を保護するために，情報セキュリティにおける組織・技術的な対策が有効であるが，さらに進展が望まれる技術について述べる.

(ア) 情報資産の流出後の技術的な保護

悪意のある攻撃者は，ログを削除するなど事後に追及されないよう行動することが多い.フォレンジックは，セキュリティ事故後にその痕跡を保全し，原因等を追究するための技術である.事故発生において，フォレンジックを容易に実行可能な状況をいかに整備するかについてさらに広く普及すべきである.また，ログを分析しセキュリティ事故発生を検知することや内部不正の事前の予兆を検知するなどの研究が取り組まれているが，実用化が望まれる.

(イ) 電子透かし技術

情報が流出しても，その情報内に秘密情報を隠して挿入しておくことで，後にその情報を所有していたことを主張可能な技術である.情報ハインディングの領域において研究が進められているが，今後の実用化が望まれる.

（4） 電子情報に対する営業秘密保護の具体化

営業秘密として認められる秘密管理性についての具体的な対策は，判例をもとにしているため，脅威が常に変動するような近年の高度な情報社会の現状を反映できない.このような脅威に対応できる組織・技術対策と，法的保護からの要件を対応づける指針等を策定できれば，実際に営業秘密保護を運用する企業・組織の助けになると考える.

5. おわりに

営業秘密保護について，情報セキュリティの観点から現状と対策，営業秘密保護との関連を述べた.ほとんどの企業の業務が電子化されている現状で，電子情報を守るための情報セキュリティの役割は大きい。しかしまた，情報化社会において情報資産を保護するために解決する課題も少なからずある． 課題解決を進め，企業や組織において技術対策と制度が良好に連携した対策実行を推進しいくことが必要である.

参考文献

1) 「ダークネットからライブネットへ-サイバーセキュリティ研究最前線」，NICT 情報通信セキュリティシンポジウム 2014 http://www2.nict.go.jp/nsri/plan/H26-symposium/files/2-2.pdf
2) 『JIS Q 27000：2014　情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語』日本規格協会, 2014
3) CERT インサイダー脅威センター: http://www.cert.org/insider-threat/
4) 『情報セキュリティ白書 2014』. IPA（2014.7）
5) サイバー情報共有イニシアティブ, IPA,2014,http://www.ipa.go.jp/security/J-CSIP/
6) PWC, CERT, CSO Magagine(2014). “2014 US State of Cybercrime Survey.”,2014.4 http://www.cert.org/insider-threat/research/cybersecurity-watch-survey.cfm.
7) 組織内部者の不正行為によるインシデント調査,IPA,2012.7 http://www.ipa.go.jp/security/fy23/reports/insider/index.html
8) 『JISQ27001 : 2014 情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-要求事項』日本規格協会,2014
9) 経済産業省(2013), 『営業秘密管理指針　2013.12』（2013.12）
10) コンピュータウイルス・不正アクセスの届出状況 2010 年 11 月分について，(独)情報処理推進機構，2010.11

ⓒ 2014 Information Processing Society of Japan

表４　営業秘密の管理のために実施することが望ましい秘密管理方法（抜粋）　出典：経済産業省　営業秘密管理指針

(1)秘密指定，アクセス権者の指定			情報セキュリティ機能
①情報の区分		営業秘密とその他の情報とを区分して管理し，営業秘密として区分した情報については，秘密であること及びその管理方法を指定・周知する. 取引先等から秘密情報の開示を受けている場合には，その秘密情報が自社の営業秘密に混入しないようにする	クリアランス，ラベル制御 (*注1)
②アクセス権者の指定		営業秘密ごとにアクセスできる権限を持つものをあらかじめ指定する. 営業秘密へのアクセス記録を残す	アクセス権限付与 ログ採取
一般的な管理		秘密の指定：営業秘密管理規程等の文書により，営業秘密を指定し，従業員に周知・ アクセス権者の指定：営業秘密にアクセス可能なもの(アクセス権者)を文章等で指定する.	―― ――
高度な管理		秘密の指定・アクセス権者の指定：情報の秘密性のレベルに応じた区分，区分ごとの管理，区分に応じたアクセス権者の限定 他社の営業秘密を不正取得していないことを証明するための措置：ペーパートレイル，クリーンルーム	クリアランス，コンパートメント，アクセス権限付与 コンパートメント，原本証明(*注2)
(2)物理的・技術的管理			
①基本的な考え方		営業秘密が記載・記録されている書面，記録媒体(USBメモリなど)等の管理にあたっては，媒体，保管庫，保管秘説等について，媒体に記載・記録されている情報が秘密であることを認識できる措置を講じ(客観的認識可能な表示)，かつ権限のない者がその媒体(または情報)にアクセスすることができない措置を講じることが重要である(分離保管)	媒体管理，物理セキュリティ(入退室管理)
②物理的管理	(ア)秘密表示，分離保管	営業秘密が記載・記録されている媒体であることを，権限を持ってアクセスした者が客観的に認識可能な状態にする.(以下略)	
		一般的な管理：媒体へのスタンプやシールで明確に表示，専用スペースの設置，媒体専用ファイル等への保管	クリアランス，ラベル付(*注1)，物理セキュリティ(注3)
		高度な管理：デジタル透かし情報を付加.秘密性のレベルを電子情報に組み込む.レベルに応じてパスワードの設定.電子情報ファイルを暗号化する.媒体等を専用の保管庫に保管する	ファイル暗号化，パスワードおよび鍵管理(*注4)
	(イ)媒体の保管，持ち出し，複製の制限，廃棄	営業秘密を記載・記録している媒体は，保管庫に施錠して保管する(保管).媒体については，持ち出しをできる限り制限する(持ち出し・複製の制限).複製についてもできる限り制限する.適切に回収する.復元不可能な措置を講じて廃棄する(回収廃棄).	物理セキュリティ 複製制御，回収，完全廃棄
		一般的な管理：施錠可能な保管庫に施錠して保管する.媒体の持ち出しや複写，複製を一律に禁止する.持ち出しを認める場合には，責任者の許可を必要とし，期間，場所を制限，鍵付きのカバン等に入れて自ら携行する.複写を認める場合は，責任者の許可が必要.適切な回収と，不要になった場合には廃棄する.	物理セキュリティ，持ち出し制御，複写，複製禁止，各制御における認可フローの整備，回収と廃棄
		高度な管理：(持ち出し)暗号化機能，生体認証機能等の機能を有した可搬記録媒体やノートパソコンを利用する.遠隔操作によるデータ消去機能を有するノートパソコンを利用する.記録媒体に含まれる情報全体を暗号化するソフトウエアを利用して暗号化する.記録媒体に情報を記録せず，外部から自社のサーバーに直接アクセスする.(ただし，条件あり) (複製)：コピー偽造防止用紙を使用する・電子情報を書類に印字出力するに際し，IC カードと複合機とを連動させることによって，利用者制限，枚数管理等を実施する.パソコンをシンクライアント化する (廃棄)：専門処理業者に依頼して，溶解処分する.シュレッダーにより書類を廃棄する際の廃棄期限チェック.記録媒体について，消去用ソフト，磁気賞与等により記録さ	可搬記録媒体に対するアクセス制御，暗号化，暗号鍵管理.シンクライアント，複製防止技術，印刷セキュリティ，完全消去機能

ⓒ 2014 Information Processing Society of Japan

		れた情報を消去した後，物理的に破壊する.	
	（ウ）施設等の管理	営業秘密の保管場所を施錠する.営業秘密を補完している施設への入退出を制限する.	物理セキュリティ，入退室管理
		一般的な管理：秘密が保管されている場所を施錠する.業務時間外には警備員を配置する.警備システムを導入する （保管場所の区分・入退室管理）：秘密が保管されている場所をその他の場所と区切る.「関係者以外立ち入り禁止」等の表示を設置する.営業秘密を管理している施設への入退を制限する.営業秘密を管理している施設への入退出の記録を作成する	入退室制限，記録管理
		高度な管理：（保管場所の区分・入退室管理）：保管施設に入隊する際の認証システムとして，IC カード認証，生体認証，ワンタイムパスワードを利用する.上記に加え PIN 入力.保管施設に入退室する際の認証システムとしてアンチバスバック機能を採用する. （コンタミネーションの防止）：他社技術と自社技術を扱うものを区別し，部屋を分離し，関係者以外は相互に入出できないようにする.	生体認証による入退室管理等 コンパートメントによる管理
③技術的管理	電磁的に記録されているデータの取り扱いに関する各種ルールをマニュアル化あるいはシステム化しておくことが考えられる（マニュアル等の設定）.指定されたアクセス権者にのみアクセス可能な措置を講じる（アクセスおよびその管理者の特定・限定）.営業秘密を 保存するコンピュータやシステムを外部ネットワークから遮断するなど不正アクセスに対する措置を講じる（外部からの侵入に対する防御）.営業秘密のデータを復元不可能な措置を講じて消去・廃棄する（データの消去・廃棄）.		マニュアル化 識別・認証およびアクセス制御 不正アクセス防止，データ完全消去
	一般的な管理：（マニュアル等の設定）コンピュータ・ネットワークに接続する際のルールを確立する.データ複製，バックアップをする際の手順を文書等で明確化する. （アクセスおよびその管理者の特定・限定）：コンピュータの閲覧に関するパスワードを設定する.・パスワードの有効期限を設定する.同一または類似パスワードの再利用を制限する.情報セキュリティの管理者が退職した場合には，管理者パスワードの変更等を行う.パスワードに加え，ユーザ ID を設定する. （外部からの不正アクセス等に対する防御）：・営業秘密を保存・管理しているコンピュータはインターネットに接続しない.ファイアウォールを導入する.コンピュータにウイルス対策ソフトウエアを導入する		マニュアル化 パスワードによる識別，認証，アクセス制御，パスワードポリシーの策定，ネットワーク隔離，ウイルス対策，OS および AP アップデート、その他のセキュリティ対策
	高度な管理（アクセスおよびその管理者の特定・限定）：パソコンの起動またはサーバーにアクセスする際の認証システムとして，IC カード認証，生体認証等を利用する.上記認証システムに加え，PIN 入力を付与する （外部からの不正アクセス等に対する防御） ・IDS/IPS を設置する.サーバーにアクセスする際の認証システムとして，接続時認証及び通信情報の暗号化措置を講じる.閲覧専用機器も，インターネットに接続しない		IC カード認証（PIN＋PKI）（*注5），生体認証による認証，アクセス制御. IDS/IPS による不正アクセス対策，通信時認証および暗号化（SSL など）.
（3）人的管理： 略			教育，研修など
（4）営業秘密侵害に備えた証拠確保等に関する管理：略			ログ採取，ログの定期的な監査等

注1：クリアランス、コンパートメント制御、ラベル付与によるアクセス制御は高度なアクセス制御である。

注 2：原本証明については、本稿では扱っていないが、時刻認証や電子署名技術および公証などで実現できる

注 3：物理セキュリティとして、機密情報を保管する倉庫・場所に、それを明示することはセキュリティ上好ましくないという場合もある。

注 4：ただし、暗号化は、機密性を確保するものである。暗号鍵管理も必要となる。

注 5：管理指針における IC カード認証が、どのセキュリティ機能を用いているかが不明であるが、スマートカードと言われる暗号演算機能をもつカードとみなして、記載している。

ⓒ 2014 Information Processing Society of Japan