内部関係者による サイバー犯罪

なぜ悪意ある内部関係者から情報資産を積極的に保護する必要があるのか？

pwc

32%

外部の攻撃者によって引き起こされたインシデントよりも内部関係者による犯罪の方が高コストで被害が大きいと述べた回答者の割合

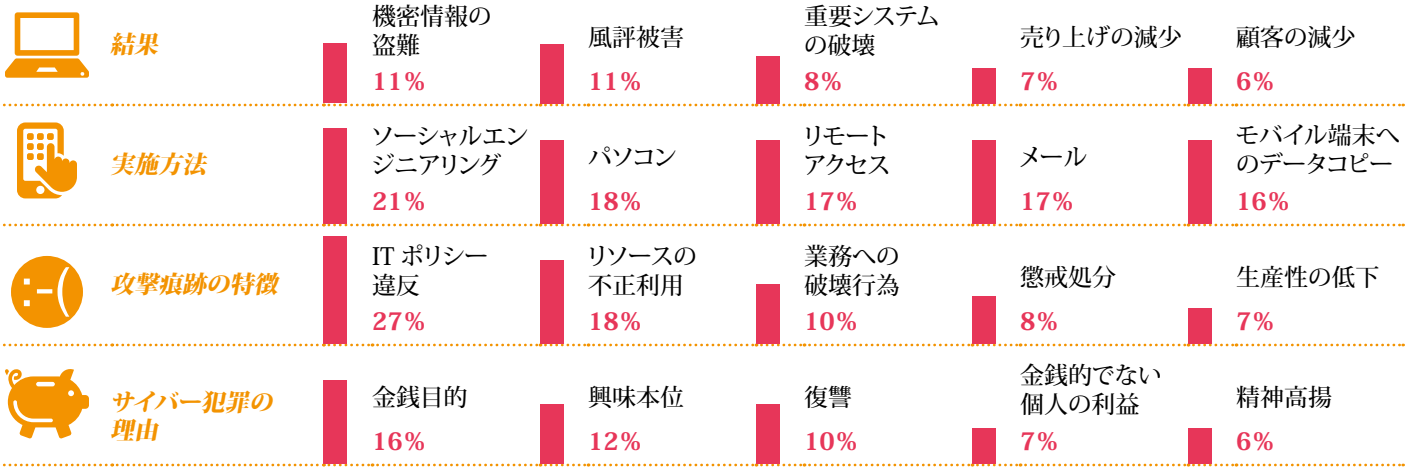
サイバー犯罪が世間を騒がせている昨今、主に報じられるのは外部の攻撃者によるインシデントだ。しかし上級幹部は、正規のアクセス権を持つ従業員やビジネスパートナーなどの内部関係者によるセキュリティ侵害の方が損害が大きいことを知っている。それにもかかわらず、大半の企業は内部関係者による脅威への対策を備えていない。

実態を数値で見てみよう。PwC の米国サイバー犯罪調査 2014 の回答者のほぼ 3 分の 1（32％）が、外部からの攻撃よりも内部犯罪の方がコストや損害が大きいと述べた。それにもかかわらず、内部の脅威に対応するための計画を作成している回答者は半数に満たない（49％）[1]。昨年中に内部関係者によるインシデントを検知したという回答が 28％に及ぶことを考えると、正式な内部犯行リスク管理戦略を策定せずにいる企業は見通しが甘いようだ。

内部関係者による犯行のほとんどは、現職または退職した従業員だ。信頼されているビジネスパートナーがサイバー犯罪に走ったり、そうとは知らずに犯罪者に手を貸したりすることもある。政府の請負業者が引き起こした大規模なデータ漏洩や、小売業でのセキュリティ侵害などがその最たる例である。特に警戒すべきは、正規のアクセス権を持つサードパーティーやビジネスパートナーだ。ほとんどの企業はサードパーティーのサイバーセキュリティ対策を十分に評価していないからだ。PwC の米国サイバー犯罪調査 2014 では、ビジネスを始める前にサードパーティーを評価するプロセスがあると述べた回答は 44％と半数に満たなかった。信頼しているベンダーやサプライヤーとの契約においてセキュリティに関する条項の交渉を行っているという回答も 31％と少ない。

1 2014 US State of Cybercrime Survey, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

図 1：内部犯行の原因と結果*



*現職の従業員や退職者、派遣従業員および取引先

出典：2014 US State of Cybercrime Survey, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

なぜ内部関係者による脅威を警戒すべきなのか？

内部関係者による脅威主体は外部の攻撃者と違い、データやシステムへの正規のアクセス権を持っているため、セキュリティ管理策を破る必要がない。特定のタイプのシステムやデータへの正規のアクセス権を持たずとも、ネットワークにアクセスできれば、競合企業が欲しがる情報を入手することは可能だ。顧客リスト、価格設定、進行中の研究開発活動など、企業にとって重要な情報がどこにあるかを正確に知っていることもある。

従業員がアクセスできる知的財産や営業秘密は多くの場合、外部の脅威主体にとっては格好の標的だ。例えば最近、米国のある農業関連企業の従業員が、バイオエンジニアリングで生み出された貴重な種子のサンプルとその遺伝子配列を業者に売り、その業者は中国企業への転売を目論んでいたと伝えられている。ある米国企業は、情報漏洩による損害は 5 年分の研究、3000 万米ドルの収益に相当すると述べている[2]。従業員がこのような貴重な情報にアクセスできる場合、経済的利益の誘惑は大きな動機となり得る。

従業員は通常、善意を持って入社するが、その後の個人的な経済的問題や仕事への不満、人間関係の衝突、人員削減などの結果として、または競合企業でより高い地位を得るために善意は悪意へと変わる。例えば、ある石油ガス企業では、自分がまもなく解雇されることを知った従業員が企業のネットワークサーバーをシャットダウンして重要データを削除した。

その結果、30 日間は完全な通信ができず、データやアプリケーションへのアクセスが限られ、損失額は 100 万米ドル以上に上った[3]。

企業の思想、あるいは企業の不正行為が従業員の反感を生むこともある。2013 年に起こった政府に反感を募らせた防衛関係の請負業者が政府の監視データを大量に漏出させた事件を考えれば、その損害の甚大さがよくわかるだろう。問題のある従業員が犯罪に走る前には、勤務状況の乱れや業績の低下、欠勤の増加、同僚への言動の変化などの前兆が現れることが多い。

このような前兆が、外部の顧客やサードパーティー、外部の脅威主体の目に触れることもある。国家や犯罪組織などの外部の攻撃者は隙のある従業員を狙って味方に付け、内部からの手引きを得て機密データを盗み出す。狙われるのは、経済的に困窮している、あるいは転職先や金銭を求めていることが明らかな従業員だ。

同様に、退職した従業員も利用価値がある。2014 年、米国で 2 人のエンジニアが化学薬品メーカーに対する営業秘密の窃取および経済スパイの罪で有罪判決を受けた。エンジニアらはメーカーの元従業員から情報を買い、中国の国有企業に売っていた[4]。

2 FBI, *Chinese National Arrested for Conspiring to Steal Trade Secrets*, July 2, 2014

3 US Attorney's Office, *EnerVest Computer Attack Draws Four-Year Federal Sentence*, May 20, 2014

4 FBI, *Two Individuals and Company Found Guilty in Conspiracy to Sell Trade Secrets to Chinese Companies*, March 5, 2014

図 2：内部関係者による脅威の影響者、動機、行動

外部の影響者	動機	行動
 外国の政府諜報機関  犯罪組織  活動家  競合企業	• 個人的な経済的困窮または欲望 • 解雇通知（またはその恐れ） • 仕事への不満や復讐 • 職場での人間関係の衝突 • 金銭目当てでデータを盗み出す • 重要な運用システムにアクセスしてデータを奪い、金銭の見返りを求める • システムへのアクセス権を取得し資金を送金 • 思想上の理由から重要なシステムを停止させる • 不正行為を暴露	• 物理的に接近するのではなく、正規のアクセス権でシステムやデータにアクセス • 敷地外ではなく敷地内で犯罪に及ぶ • 営業時間外ではなく営業時間内に活動 • 業務用コンピューター、ネットワーク共有、外部メディアでファイルにエクスポート • ファイルを個人の電子メールに添付 • USB ストレージデバイスを使用 • 重要データを一括印刷 • 業務用コンピューターに不正ソフトウェアをインストール • 業績の低下、欠勤の増加 • 同僚への言動の変化

企業はどのような行動をとるべきか

内部の犯罪を最小限に抑え、管理するには、内部関係者による脅威を管理するためのプログラムを開発し、実行する必要がある。しかもそれは、ビジネス、サイバーセキュリティ、データ保護のさまざまな戦略と連携し、全体として統合されたものでなければならない。

そのようなプログラムの基本的な構成要素は、企業と内部関係者にとって最も価値のあるものは何かを「識別」すること、内部関係者による脅威から「保護」すること、現れた脅威を「検知」すること、敵の活動と潜在的被害を抑えるために「対応」すること、そして環境を元に戻すために「復旧」することだ。

IT や情報セキュリティ、コーポレートセキュリティといった部門だけでは内部犯行リスクを管理することはできない。テクノロジーだけで内部関係者による脅威を未然に防ぐことも不可能だ。効果的な管理を行うには、IT、情報セキュリティ、コーポレートセキュリティ、人事、法務、監査などの部門の壁を越え、統制がとれたリスクベースの取り組みが必要だ。また、適切な部門の参加と、緻密なデータプライバシーポリシーも不可欠だ。

幸い、米国政府は、内部関係者による脅威を管理するためのプログラムをサイバーセキュリティ戦略に統合するなど、サイバーセキュリティに関する企業向けガイダンスの提供を急速に進めている。最近まで、統合セキュリティ戦略を作成するためのガイドラインは少なかった。変化のきっかけとなったのは、米国立標準技術研究所（NIST）が公開したサイバーセキュリティフレームワークだ。リスクベースのサイバーセキュリティのための一連のガイドラインである。NIST のサイバーセキュリティフレームワークは重要インフラ企業を対象としているが、リスクベースのセキュリティ向上を目標としていることから、あらゆる業界の企業に役立つと考えられる。このガイドラインに従うことで、受動的なコンプライアンスから、積極的なリスクベースの効果的なアプローチでサイバー脅威や脆弱性に立ち向かうよう戦略的な転換が可能になる[5]。

また、幹部や業界団体の間でのセキュリティに関する効果的な協力と情報共有、幅広いエンタープライズリスク管理の向上、法的リスクの低減、規制コンプライアンスの強化などの利点もある。いずれも機密データおよびシステムに対する内部関係者による脅威を管理するために不可欠だ。

5 PwC, *Why You Should Adopt the NIST Cybersecurity Framework*, May 2014

内部関係者による脅威を管理するためのプログラムの開発

内部関係者による脅威を管理するためのプログラムを開発するにあたっては、NIST フレームワークに従い、「識別」、「保護」、「検知」、「対応」、「復旧」を段階的に進めるとよいだろう。

内部関係者による脅威を管理するための優れたプログラムを開発するための段階的アプローチ

日　週　月

識別
システム、資産、データ、機能に対する内部犯行リスクを管理する方法の理解

保護
内部関係者による脅威を保護または阻止するための管理策または保護策

検知
内部関係者に関する事象についてリアルタイムのアラートを発するための継続的な監視

対応
識別した事象に対するインシデント対応

復旧
内部関係者によるインシデントが発生した後に環境や機能を復旧するための業務継続計画の作成／更新

重点領域

識別

- ガバナンス
- リスク管理
- 人事
- 物理的セキュリティ
- 倫理とコンプライアンス
- IT 資産およびユーザークレデンシャル管理
- 既存のセキュリティ監視テクノロジー

保護

- アクセス制御
- 認識向上とトレーニング
- 機密データの保管場所
- ポリシー

検知

- 対応計画
- 事象の分類
- 監視テクノロジー
- 脅威情報
- 営業秘密の移動
- コンピューターの利用

識別

NIST フレームワークの第 1 の要素である「識別」フェーズでは、内部犯行リスクの管理についての組織的理解を形成する。ビジネスにおける情報セキュリティ、重要なビジネス機能を支えるリソース、関連する内部犯行リスクを従業員が理解するためのプロセスに重点を置く。このような知識を持つことで、リスク管理戦略やビジネスニーズに一致するセキュリティ活動に優先的に注力することが可能になる。

そのためにまず必要なことは、上級幹部やビジネスリーダーが自社の高価値データおよびシステム（一般的には重要なビジネス機能を直接担っているもの）と内部関係者による脅威から資産を保護する担当者を把握し、合意を形成することだ。どの重要資産がどのような順に優先されるかという点で幹部や各部門リーダー、プロダクトマネージャーが合意することは非常に重要である。経営幹部への報告者として、意見をまとめて変革を指揮する力を持ち、内部犯行リスクの管理のための一連の役割と説明責任を負う上級リーダーの存在も必要だ。

自社の高価値データやシステムを把握する他、犯罪者の狙いを知ることも重要だ。例えば、外部脅威主体のプロファイルを使用して、攻撃を仕掛けてくる可能性のある敵を識別するとよいだろう。そのような敵は、請負業者やサプライヤーなどのサードパーティーを利用して情報を盗み出した過去を持つこともある。プロファイルは、攻撃の理由や方法、標的にされやすいシステムを知る手掛かりにもなる。外部の脅威を知ることには、外部の犯罪者が従業員や請負業者を狙いにくくする効果もある。

問うべきこと

システムが停止した場合に、ビジネスリスクが最も大きいのはどのシステムか？

情報が盗まれたり破損したりした場合に、深刻なビジネスリスクが生じるのはどのデータか？

高価値資産の保護策の優先順位はどうなっているか？

保護

高価値データを識別した後は、情報資産が社内のどこに保存され、誰がアクセスできるのかを特定する必要がある。全ての正規ユーザーを職務および地域別に識別する。

少し時間をとり精査し、ベンチマークを確立したうえで、悪意ある、または不審な行動をとっているユーザーがいるかどうかを判断するとよいだろう。

重要なのは、技術的および非技術的な内部犯行リスク指標を作ることだ。この指標の基盤として、内部関係者による脅威主体が機密データをどのように狙うか、内部関係者の活動の動かぬ証拠は何か、企業はどのように対応すべきかを理解しておく必要がある。技術的指標は、内部関係者がコンピューターやネットワークアクセスをどのように使用するか、また非技術的指標は内部関係者がどのような言動をとっているかに関連している。個人や職務に関連するリスク指標を識別することで、コンピューターやネットワークを監視するために必要なテクノロジーとその設定、人事、法務、倫理のポリシーの判断が容易になる。

特権アクセスが可能な従業員は違法行為に走りやすいことから、詳しい素行調査を行うことは多くの企業にとって有益だ。一般的に、徹底的な素行調査が必要なのは一部の従業員に対してのみである。個々の従業員のリスクを考慮する他、職務や職務に伴うアクセス権別に評価することも内部犯行リスクの予測と発見に役立つ。

また、内部関係者による脅威を管理するためのプログラムの基礎を固めるために、管理ツール、ポリシー、プロセス、従業員のトレーニングと意識向上、検知および監視ツールや分析など、さまざまな管理策や構成要素の評価も行うべきだ。意思決定に関するプロセスを見直してインシデント検知および対応を強化するとともに、経営陣による採用決定、契約評価のレビューも必要だ。同時に、効果的なサードパーティー管理を実現すれば、情報に基づいて効率的にリスクベースの意思決定を下すことが容易になり、さらなる脅威を回避できる。

内部関係者による脅威を管理するための効果的なプログラムの要となるものは、不審な行動やリスク指標を最初に察知することの多い従業員や管理職である。従って、「何か見つけたら報告する」という姿勢を社内に浸透させることで、内部関係者による脅威を検知しやすくし、時には思いとどまらせることができる。ほとんどの企業には既に情報セキュリティおよび倫理トレーニングプログラムがあり、予防措置や指標を効果的に伝える手段として機能している。このようなプログラムは個人の責任感や当事者意識を植え付け、インシデント防止に役立つ。

もちろん、テクノロジーも活用されている。この 15 年間で企業は数多くのサイバーおよび情報セキュリティソリューションに投資しており、その多くは他のツールとの連携により内部関係者による脅威の管理を強化できる。テクノロジーソリューションおよびプロセスには、ホストおよびネットワークベースの監視、データ消失防止、バックグラウンドチェック（素行調査）、フォレンジック調査、トレーニングプログラム、意思決定関連プロセスなどがある。これらのツールからは膨大な量の情報が生み出されるため、脅威分析ツールはリアルタイムアラートや主な脅威パターンを引き出すための手掛かりとして不可欠だ。

分析を行うことが、最終的にはセキュリティ活動および調査の優先付けと促進につながる。コンピューターおよびネットワークの監視と制御のための企業ポリシーを評価し更新することで、さらに厳密なリスク評価を行うことができる。

検知

コンピューターやネットワークを監視するための既存テクノロジーの強化と新規ツールの導入は、内部犯行リスクの管理と低減に大いに役立つ。

内部関係者によるインシデントを効果的に検知するには、異常な行動をすばやく察知し、潜在的影響を把握する必要がある。インシデント分析により、攻撃手法や標的の把握、事象データの集約と相関付けを行うことが必要だ。脆弱性スキャンを実行し、ユーザーのネットワークアクティビティを監視することも不可欠である。

各種テクノロジーを導入した後は、人事、倫理、コーポレートセキュリティなどの他部門からの非技術的リスク指標も取り込んだ脅威情報プラットホームとして全体を統合する。これらのテクノロジーや情報相関付けメカニズムの管理と監視を行うために、必要に応じて高度な技能を持つ専任チームを置くとよい。

さらに、次のようなポリシーの更新や調整が必要な場合もある。

- 従業員に行動が電子的手段で監視されていることを定期的に伝え、このポリシーへの署名での同意を得る。
- USB ストレージデバイスの使用とタイプ（外付けハードドライブ、小型ドライブ、暗号化、シリアルなど）を管理する。
- コンピューターの USB ポートを制御する。
- データベースへのアクセスと転送を制御する。
- 社内の機密文書のハードコピーの削除に関する管理策を実装する。
- 高価値データにアクセスできるユーザーのインターネットアクセスと電子資金の振替を厳格に制御する。

厳格なポリシーを実装して適用し、それらのポリシーについて従業員教育を行っている企業では、サイバー犯罪が起こりにくい環境が生まれる。

対応

社内の高価値データ、システム、活動を継続的に監視するには、専任チームが特権アクセスを利用可能なユーザーの活動を精査して相関関係を明確にする必要がある。

監視と相関関係定義とともに、コーポレートセキュリティ、倫理、人事部門から提供されたリスク指標を継続的に分析すべきだ。状況によっては、機密情報へのアクセスや役職に基づいてユーザーのリスク評価を行うことも必要だ。当該ユーザーについては、継続的な監視、定期的な素行調査、アクセス権の再認定も考慮するとよい。多くの内部関係者が悪意を持つようになるのは正規のアクセス権を与えられた後であることを忘れてはならない。

内部関係者によるインシデントの抑制と低減は、テスト済みの対応計画の有無にかかっている。

インシデントが検知された場合はこの計画をすぐに実行に移し、リーダーが従業員に行動指示を出す必要がある。

対応計画に従ってインシデントを分類し、検知システムからのアラートを分析する。その過程で、内部関係者に悪用される可能性があり、リスクとして文書化すべき新たな脆弱性が見つかることもある。

対応フェーズでは、入念に練られた内部関係者への介入計画と、不審な従業員の取り扱い方法が必要だ。リスク指標が決定的な証拠となるとは限らず、強引な手法によって火のない所に煙を立たせてしまうこともある。根拠のない申し立て、思慮に欠けた調査などが、従業員の士気の低下や関係悪化を招く恐れもある。このような行為は、内部関係者による脅威と同じかそれ以上の悪影響を及ぼす。

復旧

復旧フェーズにおいては、内部関係者による脅威を管理するためのプログラムが業務継続計画プロセスと緊密に連携している必要がある。これは特に従業員の回復力を確保し、脅威によって低下したさまざまな機能を復旧するためだ。NIST フレームワークをはじめとするリスク管理アプローチにおいては、5 つの段階全てにおいて計画と情報伝達を改善するために、情報共有、フィードバック、教訓の反映が重要であることが力説されている。

既存の対応計画に教訓を反映させる必要がある。最新の計画と復旧活動を周知することで、従業員は内部関係者によるインシデントを真剣に受け止め、どのように対応すべきかを理解する。

また、復旧計画の中には、法執行機関へのインシデント報告も含めるべきだ。このプロセスを組み込んでいる企業は少ない。2014 年米国サイバー犯罪調査によると、内部関係者によるサイバー犯罪を検知した企業のうち法執行機関に報告した企業は 12%のみだった。

不正行為を働いても法的な追及を免れた人物は、次の職場でも同じような犯罪を繰り返す可能性がある。犯罪行為を報告しなければ、不正行為の公式記録が残らず、次の雇用主が採用前の身元調査でリスクを認識することが困難になる。

取締役会が検討すべきこと

内部関係者による脅威管理の責任者は誰か？

検知したセキュリティインシデントのうち内部関係者によるものはどれくらいか？

内部関係者によるインシデントによってどのような影響を受けるか？

内部関係者によるインシデントへの対応ポリシーはどの程度徹底されているか？

内部関係者による脅威に対応する部門はどこか？

従業員やサードパーティーの内部犯行リスクをどのように評価しているか？

従業員の悪意ある活動をどのように監視しているか？

ビジネスパートナーが自社のセキュリティ慣行を遵守しているかどうかをどのように監視しているか？

他社は内部関係者による脅威をどのような方法で管理、低減しているか？

従業員や利害関係者、政府機関に対し、内部管理プログラムの存在を知らせるべきか？

リスク管理に不可欠な要素

内部関係者による脅威を管理するためのプログラムが適切に設計され、効果的に実装されていても、内在するリスクを完全に排除することはできない。しかし、内部関係者が犯行に及ぶ確率を下げ、インシデントによる損害を低減することは可能だ。内部犯罪対応はハッカーや犯罪組織による大規模な攻撃よりも高コストになる傾向があるため、内部関係者による脅威を管理するためのプログラムがますます重要になっている。内部関係者は価値ある情報がどこにあり、どのようにアクセスすればよいかを熟知しているため、狙いが的確で被害が大きい。

内部関係者による脅威を管理するためのプログラムが真価を発揮するには、経営幹部や取締役会の支援と参加が不可欠だ。トップダウンの支援は法令遵守につながり、適切な保護策を配備することで内部のセキュリティ侵害によって生じる訴訟をできるだけ回避できる。

脅威が高まっている今日の環境において、全てのデータに最高水準の保護を施すことはもはや不可能だ。しかし、内部関係者による脅威を管理するためのプログラムを適切に設計して実装し、既存のセキュリティ慣習と融合させれば、内部リスクを効果的に検知して迅速に対応することが可能になる。サイバーセキュリティを効果的に管理するには、その実現が不可欠だ。

お問い合わせ先

プライスウォーターハウスクーパース株式会社

〒104-0061
東京都中央区銀座8−21−1　住友不動産汐留浜離宮ビル
03-3546-8480（代表）

松崎 真樹

パートナー
maki.matsuzaki@jp.pwc.com

山本 直樹

パートナー
naoki.n.yamamoto@jp.pwc.com

星澤 裕二

パートナー
yuji.hoshizawa@jp.pwc.com

www.pwc.com/jp

PwC Japan は、日本における PwC グローバルネットワークのメンバーファームおよびそれらの関連会社（PwC あらた監査法人、京都監査法人、プライスウォーターハウスクーパース株式会社、PwC 税理士法人、PwC 弁護士法人を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、ディールアドバイザリー、コンサルティング、税務、法務のサービスをクライアントに提供しています。
PwC は、世界 157 カ国に及ぶグローバルネットワークに 195,000 人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスの提供を通じて、企業・団体や個人の価値創造を支援しています。詳細は www.pwc.com/jp をご覧ください。

本報告書は、PwC メンバーファームが 2015 年 1 月に発行した『Managing insider threats』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/japan-knowledge/report.jhtml
オリジナル（英語版）はこちらからダウンロードできます。 http://www.pwc.com/us/en/increasing-it-effectiveness/publications/managing-insider-threats.jhtml
日本語版発刊月：2015 年 9 月　　管理番号：I201507-5