NTT Com Security

Tetsuo Someya　Chief Business Development Officer and Chief Governance Officer

NTT Com Securityは，セキュリティ専業会社であるIntegralis（ドイツ）とSecode（スウェーデン）を母体に設立され，2013年6月，総合リスクマネジメントサービスWideAngleの提供を開始しました．今回は，企業を取り巻く情報セキュリティ環境を交えながら，弊社の事業を紹介します．

WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

設立背景

NTT Com Securityは，ドイツの株式市場に上場している，ドイツに本社を置く情報セキュリティサービスを提供する企業です．前身は，1988年に設立されたIntegralisと，1986年にスウェーデンで設立されたSecodeを母体とし，Integralisは2009年に，Secodeは2010年にNTTコミュニケーションズによる買収を経て，2011年に2社を統合，2013年10月に「NTT Com Security」に社名変更を行い，NTTコミュニケーションズグループのセキュリティ事業の中核を担う会社として再出発をしたところです（**図1**）．

会社設立以来，25年以上，セキュリティ分野のリーディングカンパニーとして，欧米エリアを中心に事業を拡大し，APAC（Asia Pacific）にも展開しています（**図2**）．

全世界の社員数は約870名で，うち500名以上はセキュリティ専門のコンサルタントや業界屈指のセキュリティアナリスト等のスキルを持った人材です．全世界15カ国に広がる本支社，世界7カ国に設置したグローバルリスクオペレーションセンタに，上述の社員のうち200名以上のセキュリティエンジニア並びにリスクアナリストを配置し，24時間365日，顧客企業のセキュリティ監視と，全世界のセキュリティ動向を観測しています．

セキュリティ市場の現状

通信技術の発達，BYOD（Bring Your Own Device）の普及，ビッグデータの活用がますます進む中にあって，セキュリティは避けては通れない

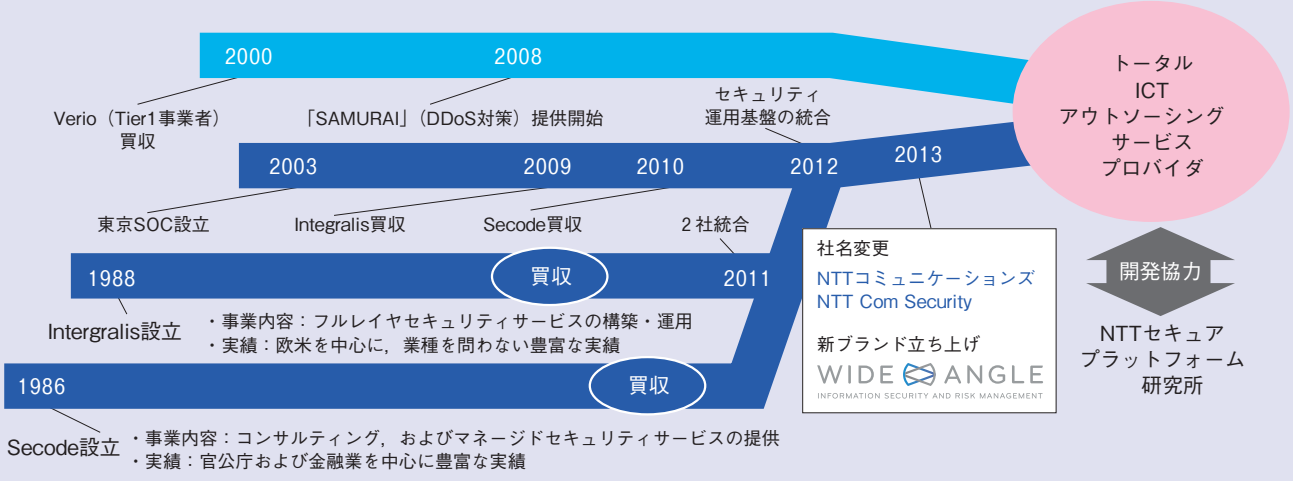

図1　NTT Com Securityの沿革

テーマです．日々，金融機関，政府系機関や軍事関連情報，電子商取引をねらった機密情報や金銭目的のハッキングは組織化，巧妙化しています．技術の発達の一方で，OpenSSL技術に見つかった重大なセキュリティ上の脆弱性（Heartbleed）や，広く利用されているオープンソースのWebアプリ作成用のフレームワークであるApache Struts 2の脆弱性により，Web上の多くの取引が情報漏洩の危険にさらされていたことが明るみに出たり，確定申告用のWebサイトが一時閉鎖に追い込まれたりするなど，日常的に利用しているサービスが脅威にさらされ，社会基盤に対する信頼が揺らぐ例は，枚挙に暇がありません．

昨今の攻撃や，膨大なセキュリティ監視ログを基に，NTTグループでは，2014年3月にGlobal Threat Intelligence Report（GTIR）を発表しました（**図3**）．本レポートは，NTTグループのセキュリティ企業である，Solutionary, NTT Com Security, Dimension Data, NTTデータ，およびNTT研究所の協力を得て，NTT I^3（NTT Innovation Institute, Inc.：NTTアイキューブ）が作成・リリースをしたもので，全世界16拠点のSOC（Security Operation Center）での監視により得られた30億件を超える最新のセキュリティアタックからの情報と，幾兆件にもおよぶセキュリティ・ログデータからの分析を経て，攻撃者がどのような手口で情報資産をねらっているか，どのようにして身を守ることが有効であるかを検討するうえで，有用なレポートとなっています．

本レポートによれば，検知したセキュリティアタック全体の34%がボットネットによるもので，同15%がアノマリー，すなわち何らかの不自然で異常な通信によるものです（**図4**）．このことは約半分がユーザ内部の端末や利用者がこうしたアタックに意識的であれ無意識であれ加担してしまっていることを意味します．企業は自らの被害を防ぐと同時に，加害者となってしまうリスクに対しても，対策を講じていく必要があります．また，企業に勤める個人も，被害を企業や外部に与えてしまうことにより，大きな訴訟や賠償請求のリスクにさらされているといっても過言ではありません．

企業内のネットワークにおいて，システム管理者の端末がマルウェアに感染してしまうことによって，企業内ネットワークに，システム管理者自身がマルウェアをばら撒いてしまうケースなども発生しており，こうしたケースのほとんどが，多大な金銭的な損害を被っていることが調査資料では明らかにされており，GTIRでは1件のインシデント当りの損害を約11万USドルと試算しています．

こうしたマルウェアは，管理者や諸々のセキュリティ対策をかいくぐるように，日々進化を重ねています．同調査では，NTTグループが研究目的で設置したハニーポットで収集された新種のマルウェアの54%は，既存のアンチウイルスソフトウェアでは検知することができず，同様にサンドボックス環境で収集されたマルウェアの71%

図2　セキュリティ事業のグローバル展開状況

図3　Global Threat Intelligence Report

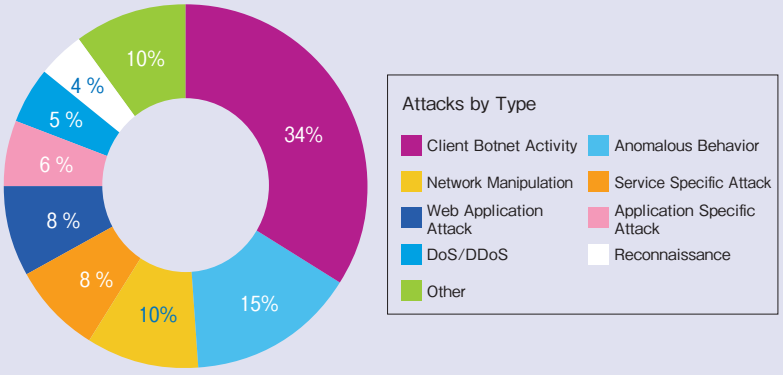

図４　セキュリティアタック手手法の割合

が，40におよぶ既存のウイルス対策では検知することができないという結果でした．

情報資産をねらった内外からの攻撃は日々新しいものが出てきており，セキュリティ機器や対策ソフトを導入するだけでは，身を守ることができません．外部からの攻撃のみならず，内部からの対策と，常に新しい攻撃手法に対応していくためのセキュリティ維持の仕組みが重要です．またエンドポイントのセキュリティのみならず，企業ネットワークないしクラウド全体でのマルウェア検知や，脆弱性，攻撃を把握する仕組みが備わっているかどうか，最新のセキュリティ動向に精通したリソースが備わっているか，サービスやセキュリティベンダを選定する際には，よく考慮に入れておくことが肝要です．

新サービスブランド「WideAngle」

NTT Com Securityが焦点を当てている市場は，主として，企業の情報セキュリティマネジメントであり，事業領域としては①プロフェッショナルサービス，②セキュリティ機器の販売・導入サポート，③マネージドセキュリティサービス（MSS）の３つです．

弊社は，海外では1986年から，日本国内の拠点としては2003年から東京のSOCにてセキュリティ事業を開始し，企業のネットワークセキュリティを監視し続けてきました．現在は，世界７拠点での顧客窓口の設置，日本，マレーシアでのセキュリティイベント管理およびデバイス変更管理，日本・スウェーデンでの高度セキュリティ分析および顧客企業ごとのリスク管理を，約200名体制で実施しています（**図５**）．

MSSについては，日本向けに2012年６月から，Bizマネージドセキュリティサービスの提供を開始しており，2013年からは，新サービスブランド「WideAngle」として，サービス提供基盤を一新し，国内外のクラウドサービス，オンプレミス（企業の自社内のシステム）環境を問わず，シームレスに顧客システムにおける情報セキュリティサービスを提供し，Trusted Advisorとして顧客企業の情報セキュリティ基盤や運用を一手に担っています．MSSにおいては，前述の脆弱性や，ユーザ心理をねらった最新の標的型攻撃などの新たな脅威へも対応する，さまざまなレイヤにおけるトータルセキュリティアウトソーシングサービスを提供しており，2014年５月現在までに，約3000社の顧客企業に１万1000台以上のセキュリティ・デバイスのマネジメントを提供しています．

プロフェッショナルサービスの柱であるセキュリティコンサルティングは，25年で8000件以上の実績があります．会社設立以来積み上げてきたセキュリティコンサルティングの膨大な実績を元に，GEM（Global Enterprise Methodology）というグローバル統一の評価手法を確立，ノウハウを体系化し，顧客企業のセキュリティ対策レベルを定量化，顧客企業の業務や業界に応じて必要な最適な対策レベルと内容を把握，改善提案を行う新しいコンサルティングプログラムです．

情報セキュリティにおいては，攻撃の変化に応じて，常に守る側も最適化する必要があります．また，攻撃者は１回の攻撃で情報の搾取や詐欺行為をねらうのではなく，さまざまな事前準備と，事前の下見をしたうえで実行に移します．そうした予兆や事前の動きを察知することは，常にセキュリティ監視を行うマネージドサービスをおいてほかにはなく，対策を１回講じただけ，セキュリティ機器を導入しただけ，あるいはそうした検知システムのエンジンを利用するだけでは防ぎきれないのです．

ユーザ企業が自前でこうした対策

図5　セキュリティ監視運用体制

を，幾多の機器に対して目を光らせて，確実に脅威から身を守ることは大変に困難なことといえます．

NTT Com Securityが提供するWideAngleの新しいサービス基盤では，SIEM（Security Information and Event Management）エンジンを新たに開発するとともに，専門のリスクアナリストによるモニタリングと解析をサービスとして提供しています．また，あらゆるセキュリティ機器の状況が一元的に把握できるポータルを顧客企業に提供しています．

NTT Com Securityでは，こうした顧客企業や公的機関向けのトータルマネジメントサービスを提供するにあたり，NTT研究所，NTTデータ，Solutionaryとともに，NTTグループのセキュリティ技術に関する知見やノウハウを結集し，日々変化する脅威をいかにして突き止めるか，また，情報資産をいかにして守るか，安全に利活用することを可能とするかを研究し，スピーディに実際のサービスに取り入れています．

NTTグループのセキュリティソリューションへの取り組み

NTTグループでは，2013年に北米のSolutionaryを新たにセキュリティサービスプロバイダとして加え，NTT Com Security（旧Integralis，Secode），Dimension Dataの子会社Earthwave，そして北米研究開発拠点NTT I³とともに，グローバルのセキュリティ市場において，顧客企業からの高い評価をいただきながら，存在感を増してきています．

Gartner社が発表したMSSプロバイダのグローバルマーケットにおけるポジショニングを示す「Magic Quadrant for Global MSSPs」*において，NTTグループは2014年「Challenger」の評価を得ており，同象限の中でもっとも実行能力が高いベンダとしてポジショニングされています．

NTT Com Securityでは，高品質なMSSサービスの提供と，MSSサービスを支える多様な独自開発技術，グローバル標準化されたサービス提供体制やSOCの運用，グループ内における最新のセキュリティ動向や脅威についての情報交換網などが高く評価されていると確信しています．

今後はグループ企業間でのさらなる連携によるシナジー効果の発揮を目指し，ネットワークサービス，データセンタ，クラウドサービスなど，さまざまな領域のソリューション提供も併せて行っていきます．また，グループ一丸となって，一歩先を行く最先端のセキュリティソリューションを提供していきたいと考えています．

＊ Gartner, “Magic Quadrant for Global MSSPs” Kelly M. Kavanagh, 26 February 2014. ガートナーは，ガートナー・リサーチの発行物に掲載された特定のベンダ，製品またはサービスを推奨するものではありません．また，最高の評価を得たベンダのみを選択するようテクノロジの利用者に助言するものではありません．ガートナー・リサーチの発行物は，ガートナー・リサーチの見解を表したものであり，事実を表現したものではありません．ガートナーは，明示または黙示を問わず，本リサーチの商品性や特定目的への適合性を含め，一切の保証を行うものではありません．