2019.06

中国風険消息＜中国関連リスク情報＞ ＜2019 No.3＞

中国における日系企業のサイバーセキュリティへの対応

本稿は、上海菱威深信息技術有限公司（iVision 上海）副総経理の植木心氏に寄稿いただきました。

【要旨】
■中国ではサイバー攻撃に関する法整備や当局・企業の対策が進み被害件数自体が減少に転じる一方、従来の対策では防げない新たなサイバー攻撃による被害が増加している。
■日本本社でのサイバーセキュリティ対策と比べ、中国を含む海外拠点での対応は遅れており、この遅れが被害に繋がるケースがこの 1-2 年で増えている。
■これまでの「未然防止」を前提とした対策だけでは不十分な状況になりつつあり、今後は被害が発生することを前提とした複合的な対策が求められる。

1．中国におけるサイバーリスク対策に関する最新状況

中国では、永らくサイバーリスクに対するセキュリティ対策の水準が、欧米や日本と比べて低いといわれてきた。しかしながら、近年は、中国でも官主導によるサイバーセキュリティ対策が進展し、一定の効果を上げつつある。具体的な施策を下表に紹介する。

表１　中国当局による主なサイバーセキュリティ対策（弊社まとめ）

分類	項目	概要
法整備	公安部令 第 82 号	企業のインターネット利用履歴情報の管理（一定期間の保存）を義務化
	情報安全技術個人情報安全規範（GB/T 35273-2017）	組織や企業が収集した個人情報の取扱に関する規範
	サイバーセキュリティ法	個人情報や重要情報に対する管理のためのサイバーセキュリティ対策を企業等に義務化
当局による管理強化	WEB サイト登録の厳格化	WEB サイトの登録申請時の審査を厳格化
	IP アドレスの実名登録	IP アドレスの管理者の身分証明書提出の義務化
	政府系サイトの統廃合	不十分な管理が課題であった政府系 WEB サイトを統廃合、サイト数は直近 1 年で約 2.2 万→約 1.7 万に減少

特に、サイバーセキュリティ法が（要求する対応レベルや保護対象データの範囲等、詳細が不明な部分はあるものの）企業側の IT 管理に対する責任や罰則、つまりサイバー攻撃対策が不十分な企業にその管理を怠った責任を問うことを明確に打ち出した意義は大きい。こういった施策により、企業や組織が管理する WEB サイトのセキュリティ対策にも一定の進展が見られた。

当局は今後も法律を根拠に、企業・組織への指導・取り締まりを進めると思われるが、中国の法制度は、地域や時期（国家イベント前や関連事件の発生後等）により急に運用が厳格化されたり、運用ガイドラインにあたる法律の細則が短期間で発効されることがあるため、引き続き注視が必要である。（特にサイバーセキュリティ法関連は、米中貿易摩擦の影響を受ける可能性がある。）

上記のような対応の結果、2018 年には中国内のインターネット上のウイルスや不正アクセスが減少に転じており、サイバー攻撃による被害件数も減少傾向にあると考えられる（表 2）。

表 2　国家互聯網応急中心が検知したサイバーセキュリティインシデント数

インシデント分類	2017 年	2018 年	備考
ウイルス感染端末数	約 2,095 万件	約 616 万件	約 7 割減少
サイト改竄件数	約 6.3 万件	約 2.3 万件	約 6 割減少
セキュリティ脆弱性	約 16 万件	約 14 万件	約 1 割減少

データ出典：中国互聯網絡信息中心「第 43 次中国互聯網絡発展状況統計報告」

サイバー攻撃では、攻撃者は身元を偽装するために、対策が行われていない機器をウイルスに感染させる等してコントロールを奪い、その機器を起点として攻撃を行うことが一般的である。この攻撃に対する必要最低限の防御が、ウイルス対策ソフトの導入とソフトウェアのセキュリティ対策アップデートの実施であるが、こういった最低限の対策が進んでいることが伺える。

一方で、近年サイバーセキュリティ対策の担当者を悩ませているのは、上記のウイルス対策ソフトの導入やセキュリティ対策アップデートで防ぐことの出来ない未知の攻撃、いわゆる「ゼロデイ攻撃」や、なりすましメールによるウイルス感染や詐欺を誘導する「標的型メール」に対する被害の増加である。サイバーセキュリティについて必要最低限の対策が一巡する一方、対策がより困難なリスクにどう向き合っていくのかが問われるフェーズに入ったといえる。

弊社では、サイバーセキュリティ対策の対応レベルを以下の 5 つに分類している。

表 3　サイバーセキュリティ対策のレベル（弊社分類）

分類	概要	対策例
レベル 4	サイバー攻撃に対する監視、専門の対応体制の確保等を実施している状態	サイバー攻撃に対する監視（NOC/SOC）、常時情報収集・対策体制（CSIRT）の設置等
レベル 3	未知のリスクに対する対策を実施している状態	振る舞い検知型／サンドボックス型のウイルス対策ソフト・機器の導入、標的型メール対策ツール導入等
レベル 2	レベル 1 対策が徹底できている状態	レベル 1 対策状況のモニタリングや未対策機器・ソフトに対する対策運用の徹底等
レベル 1	既知のリスクに対する対策を実施している状態	パターンファイル型ウイルス対策ソフト、ファイアウォールの導入、各種ソフトのアップデート対応等
未対策	管理が不十分な状態	レベル 1 対策が徹底されていない状態、現状が把握されていない状態

レベル 1（既知のリスクへの対策を備えている状態）の対応が徹底されているか否かにより、敢えて「レベル 2」を設けている点が特徴である。日本では何らかの仕組みを導入する際に、この仕組みの運用が徹底されることが前提になる場合が多いが、海外では仕組みを導入したものの運用が徹底されず問題が生じるケースも多いからである。

中国の企業全体では、「未対策」の状態から急速にレベル 1～2 の段階に移行しつつあり、今後はレベル 3～4 の対策が求められるようになっている状況であると考えられる。

では中国の日系企業はどうだろうか。業種や規模にもよるが本邦では、概ねレベル 3～4 の対策を進めている企業が多いが、中国の日系企業では、まだレベル 1～2 の段階にとどまっている企業が多いのが実情であると思われる。

２．中国の日系企業におけるサイバーセキュリティ対策上の課題

本邦におけるサイバーセキュリティに関する脅威については、情報処理推進機構（IPA）が毎年情報公開を行っている（表 4）。

表４　情報セキュリティ 10 大脅威（2019 年）

順位	組織	前年順位
1 位	標的型攻撃による被害	1 位
2 位	ビジネスメール詐欺による被害	3 位
3 位	ランサムウェアによる被害	2 位
4 位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
5 位	内部不正による情報漏えい	8 位
6 位	サービス妨害攻撃によるサービスの停止	9 位
7 位	インターネットサービスからの個人情報の窃取	6 位
8 位	IoT 機器の脆弱性の顕在化	7 位
9 位	脆弱性対策情報の公開に伴う悪用増加	4 位
10 位	不注意による情報漏えい	12 位

データ出典：情報処理推進機構（IPA）

脅威のトレンドは毎年変化しており、昨年はビジネスメールの詐欺被害が新たにクローズアップされた。今年は仮想通貨のマイニングを目的としたサイバー攻撃が、仮想通貨市場の相場下落の影響により下火になる一方で、標的型攻撃や詐欺メールは引き続き重大な脅威となっている。

新たに 4 位に入ったサプライチェーンの弱点とは、自社の取引先等でサイバーセキュリティ対策が不十分であった場合に、ここから連鎖的なサイバーセキュリティの被害が発生するケースである。このような被害が今後拡大すると自社の IT ガバナンスの観点だけでなく、取引先への信用担保の観点でも対策が必要になったり、取引先からサイバーセキュリティ対策の実施を求められるようなケースも増えていく可能性がある。

日系企業の本社の多くでは、対策はレベル 3～4 まで進んでいるため、サイバー攻撃を受けた場合でもある程度はセキュリティ対策システム側で防御が出来るようになっている。例えば、ランサムウェアを含む不正な添付ファイルを含むメールが送付されてきたとしても、事前にシステム側で添付ファイルの内容をチェックし、そこに既知のリスク（悪意のあるコード、ウイルス等）や未知のリスク（サイバー攻撃が疑われるコード等）の可能性が見られる場合は削除する等の仕組みがこれに当たる。

一方、日系企業の海外拠点における対策はどうだろうか。日系企業の海外拠点のサイバーセキュリティ対策の実態を示す統計的なデータは多くないが、IT セキュリティ専門企業である NRI セキュア社が実施したセキュリティ診断サービスの結果より示唆が得られる。

表５　NRI セキュアによるセキュリティ診断結果（調査対象標本 923、うち海外 109）

公開が望ましくないサービスが存在した機器の割合	比率	備考
セキュリティ診断対象機器全体	24.9%	海外では機器の 2 台のうち 1 台にリスクが存在するという結果に
上記のうち、海外に存在する機器のみ	49.5%	

出典：NRI セキュア「サイバーセキュリティ傾向分析レポート 2018」

インターネットに接続されている機器では、外部からのウイルス等の侵入を防ぐためには、アクセス経路（ポート、サービス）の公開を制限するのが一般的だが、上記はこの対策状況の実施状況である。ポート管理が不十分な機器の割合が高いことがわかる。これは前述のレベル分類では、レベル 2 の状態にも達していないことになる。これだけを以て、サイバーセキュリティ対策全体のレベルが低

いとはいえないものの、日本国内と比べてこの管理が不十分である実態が垣間見える。つまり、日系企業においても日本本社と海外拠点ではサイバーセキュリティ対策のレベルが異なる、いわばギャップが存在することが多い。

近年、このギャップに起因するインシデントが多く発生しており、日本企業が対応を急ぐ重要課題のひとつになりつつある。実際の事例として、ある企業の日本本社と海外拠点が、同一のサイバー攻撃を同時に受け、日本本社ではセキュリティシステムによって被害を未然に防げた一方で、対策が遅れていた海外拠点では被害が発生したといったケースも散見される。

弊社でも、中国の日系企業より、標的型メールに関する問い合わせは多いときで月に数回受け付けており、ランサムウェアについては実際の被害に至ったケースも確認している。その多くのケースでは、レベル3以上の対策ができていれば被害発生を未然に防げた可能性が高い。未だ被害が発生していない企業でも被害が顕在化していないだけのケースもあり、決して他山の石とはいえない状況である。

３．中国の日系企業でサイバーセキュリティ対策が進まない理由

海外でのサイバーリスク対策を考える上で、そもそも日系企業の海外拠点におけるサイバーセキュリティ対策が進まない理由を理解しておく必要がある。

結論から言うと費用負担の問題が大きい。弊社も多くの日系企業に対して、現地でのサイバーセキュリティ対策のご支援をする中で、費用負担の問題に突き当たるケースを数多く見てきた。

まず、日本本社がいわゆる大企業である場合でも、海外拠点の一つひとつは従業員規模が数十人～数百人のいわゆる中小企業であるところが大多数である。しかも、中国においては地方政府の企業誘致の条件が、現地での法人登記が前提であるケースがほとんどであることから、一定規模以上の拠点は、日本本社の支店・支社ではなく独立した法人として登記しているケースも多い。こういった背景から、中国拠点は法人毎に予算を設定しているため、ITに関連する予算規模も中小企業レベルにとどまらざるを得ず、日本国内の小規模拠点の扱いとは大きく異なることになる。

この前提下でサイバーセキュリティ対策を実施するにあたり、次に突き当たる問題が「どこまでやらなければいけないのか？」という対策のレベル・領域の設定になる。仮に日本本社と同等の水準、ということになれば、費用が拠点単位で数千万円～1億円以上必要になる場合もある。また設備だけでなくセキュリティ対策を日常的に運用していく体制（要員）も必要になる。中小企業レベルの予算範囲内で実施するのは、かなりハードルが高い。海外拠点向けに、サイバーセキュリティ対策の対応基準の日本とは異なる独自の基準を作ればよいという考え方もあるが、これも実現できている企業も大変少ないのが実情である。なぜなら、日本側のシステム部門では、海外の実態が把握し切れていないため、海外向けの基準（どこまでやれば大丈夫なのか）を設定することが大変困難だからである。

では日本の本社から費用や要員を派遣するという意見も必ず出るが、インシデント発生後の一時的な対応ならまだしも継続的な対応体制となると、受益者負担の原則や移転価格税制等がハードルとなり、やはりこれも難しいという結論になるケースが多い。仮に、仕組みや要員の一部を日本側から提供することが出来たとしても、この費用負担が海外拠点に重くのしかかる、という構図は変わらない。

上記のように、日系企業の海外拠点がサイバーセキュリティ対策を進めるにあたっては、ハードルとなる背景・要素が多くあることを理解した上で、本社を含めて具体的な検討を進めていくことが肝要である。実際にこういった課題を踏まえて本格的な対応に着手する企業も増えてきている。

４．中国の日系企業におけるサイバーセキュリティ対策のポイント

最後に、中国の日系企業がサイバーセキュリティ対策を進めていく上での重要なポイントを以下に説明する。

(1) 複合的なサイバーセキュリティ対策の実施

中国の日系企業においても、前述した様々な制約下でも有効な対策を行っている企業も存在する。それらの企業に共通して見られる特長・傾向は以下のとおりである。

① 一定の予算確保
② 中国現地で対策を企画・検討・管理するための体制の確保
③ 中国向けに最適化したサイバーセキュリティ対策案の実施
④ 柔軟で複合的なサイバーセキュリティ対策

実効性のあるサイバーセキュリティ対策には、ある程度の予算が必要なことはいうまでもないが、重要なのは「体制」である。前述の対策レベルの分類でも触れたように、サイバーセキュリティ対策を確実に実施するためには、サイバーセキュリティ対策の仕組みを「備えた」だけでは不十分であり、このモニタリングと対応を確実に「実行」していくことが重要である。

この確実な実行のためには、ある水準以上の体制を現地に設置する必要がある。この体制をベースにサイバーセキュリティに関する規程・ガイドラインを策定し、現実的な対策を着実に実施していくことが重要となる。

次に、対策を実行していく上でどのレベルまで到達すればよいかという問題である。弊社でもお客様よりご相談をいただく機会は多いが、2、3年前であればまずレベル2を目標としていたが、この1、2年の現状を踏まえて見直す時期に来ていると考えている。

サイバー攻撃が巧妙化している状況下、また今後取引先への責任も求められる可能性を踏まえると、レベル2は最低限の条件であり、中国拠点でも段階的に未知のリスクへの対応、即ちレベル3～4の対応に取り組むべき時期になりつつあると感じる。

(2) 100%の未然防止は不可能な前提での対策

サイバーセキュリティ対策の基本は、他の組織や企業または個人で検知されたサイバーリスクに対して、同様の被害が発生しないための速やかな対応を行う「予防対策」である。Windowsのセキュリティアップデートや、ウイルス対策ソフトのパターンファイルの最新化等がこれに当たる。しかしながら、近年はこれらの対策だけでは予防できない種類のサイバー攻撃が急増している。これらの攻撃は、企業側が対策の準備を行うための時間的猶予が存在しない、という意味で「ゼロデイ攻撃」と呼ばれる。近年の標的型メールでは、添付ファイルを開封させてウイルスを仕込むタイプだけでなく、いわゆる「振り込め詐欺」の要素を持つ詐欺メール系の攻撃も急増している。「メールでの振り込め詐欺の被害になんてあう訳がない」と考える顧客企業も多いが、手口は巧妙化しており、実際の被害ケースを見ると、セキュリティ対策の専門家である弊社から見ても、見破るのが難しい巧妙なものが増えている。これら詐欺メールへの対策として、弊社でも疑似メール送付の訓練サービスのご提供等を行っている。被害の発生を減らす意味では大きな効果がある一方で、被害をゼロにすることは難しい。

このため、今後は実際に「被害が発生し得ること」を想定した対策も必要になってくる。具体的には、被害発生時の対応を予め整理しておくことや、データのバックアップ等の対応である。

特に、対策が過大にならないためには、データ（情報）の重要度による分類（本当に守るべきものを精査すること）を行うことが肝要である。また、未然防止が困難なサイバーリスクへの対応に

ついては、被害発生時に迅速な初動対応を行うための外部コンサルティングの活用や、金銭的被害を最小限に抑えるためのサイバーリスク保険の活用等を含めた複合的な対策も併せて検討し、費用対効果の高い対策を目指すことが求められる。

以　上

執筆：上海菱威深信息技術有限公司（iVision 上海）　副総経理　植木心

＜参考文献等＞

1) 中国互联网络信息中心（CNNIC）「第 43 次中国互联网络发展状况统计报告」
www.cac.gov.cn/2019-02/28/c_1124175677.htm
2) 国家计算机网络应急技术处理协调中心（CNCERT）「2018 年我国互联网网络安全态势综述」
www.cac.gov.cn/1124379080_15554834432651n.pdf
3) NRI セキュア　「サイバーセキュリティ傾向分析レポート 2018」
https://www.nri-secure.co.jp/report/2018/cstar2018.html
4) 独立行政法人　情報処理推進機構　「情報セキュリティ 10 大脅威 2019」
https://www.ipa.go.jp/security/vuln/10threats2019.html

＜執筆者略歴＞
◆ 植木 心 氏
学習院大学　経済学部卒
2001 年野村総合研究所(NRI)入社、
2008 年より iVision 上海に赴任
インフラ関連事業責任者、営業責任者を経て 2016 年より現職（副総経理）
専門は IT インフラの設計・構築、
海外拠点での IT マネジメント企画・推進、
システム導入コンサルティングなど