グローバル拠点を持つ日本企業における NISTサイバー・セキュリティー・フレームワーク適用のポイント

「事故前提社会」でのグローバル・セキュリティー・ガバナンスの確立に向けて

多くの日本企業が海外事業活動をさらに拡大させようとしている中、事業の存続を脅かすほどの被害を招くセキュリティー事故が国内外を問わず多数報告されています。このような背景の中、効率的かつ価値ある事業活動を進めるためには、グローバル拠点を含めた企業グループ全体としてセキュリティー・ガバナンスを整備し、セキュリティー・リスク管理体制を高度化することが必要不可欠です。本稿では、グローバルに拠点を持つ日本企業が、米国国立標準技術研究所（NIST）のサイバー・セキュリティー・フレームワークを適用する際のポイントについて解説します。

1.「事故前提社会」の到来

「増え続けるサイバー攻撃」といった見出しや情報漏洩に関わる事件・事故が毎日のように報道されています[1]。数年前までは、専門的な技術や知識を有した攻撃者によってサイバー攻撃が行われていましたが、現在では、サイバー攻撃を行うためのツールやウイルスを作成するための技術、攻撃対象システムの脆弱な点を見つける方法などを、インターネット上を少し検索するだけで簡単に手に入れられるようになりました。図らずも、誰もが気軽にサイバー攻撃を行える環境が整ってしまっていることが、サイバー攻撃の増加に拍車を掛けているとも言えます。

また、サイバー攻撃を行う側の動機も、従来とは異なるものが現れてきています。例えば、不倫や浮気を助長するSNSに対する抗議行動の手段[2]やテロ行為への報復手段[3]など、従来型の「いたずら」「能力の誇示」「金銭目的」「組織活動の妨害」だけではない新たな動機によるサイバー攻撃が今後ますます増えていくことが予想されます。

いつ、誰が、どのような動機によって、サイバー攻撃の被害に遭遇するか分からない昨今、まさに企業は「事故前提社会」への対応力を強化する必要があると実感します。事故前提社会とは、「内閣サイバーセキュリティセンター」（NISC）が、2009年2月に「第2次情報セキュリティ基本計画」[4]で打ち出したセキュリティーのキーワードで、「事故は発生するもの」として認識し、事前対策と事後対応の両面から対応力を強化する考え方です。

サイバー攻撃への対応を含めた情報セキュリティーの確保は、グローバル拠点を含めた企業グループ全体としての社会的責任です。企業はこの責任を果たすためにも、事故前提社会であることをふまえた合理的なセキュリティー対策を策定・実行し、その有効性を証明することが求められています。

本稿では、グローバル拠点を含めた企業グループ全体として、サイバー攻撃に対してどのように対策を取っていくべきなのか、どのようにグローバル拠点に対してガバナンスを効かせていくべきなのか、その方法論として注目されるサイバー・セキュリティー対策のフレームワークの効果的な適用方法について解説します。

2. サイバー・セキュリティー対策のフレームワーク「NIST-CSF」

日本においては、2015年1月にサイバーセキュリティ基本法が全面施行され、同年9月にはサイバーセキュリティ戦略が発表されるなど、政府としてサイバー・セキュリティーへ真摯に取り組む姿勢が示されました。しかし2015年11月時点ではまだ具体的なガイドラインは制定

されておらず、各行政機関や事業者などの自主的な取り組みに委ねられているという状況です。

そこで、欧米で標準的に活用されている、米国国立標準技術研究所(NIST)による「重要インフラのサイバーセキュリティを向上させるためのフレームワーク（以下、NIST-CSF)」[5][6]を適用してサイバー・セキュリティー対策を実施していくアプローチが、実効性のある取り組みとして注目されています。NIST-CSFは、サイバー・セキュリティー・リスクを管理するための「共通言語」を記しており、特にグローバルに拠点を持つ日本企業にとって、サイバー・セキュリティー対策の向上のみならず、グローバル・セキュリティー・ガバナンスの整備にも価値をもたらします。

●NIST-CSFの特徴と価値

2013年2月、米国で「重要インフラのサイバーセキュリティ強化に関する大統領令（第13636号）」が発表されました。これを受けて2014年2月にNISTが発表したのが、企業や組織のサイバー・セキュリティー・リスクに対する多様なベストプラクティス（あるべき姿）やアプローチを集約し、体系化・構造化したフレームワークNIST-CSFです。

これは、サイバー・セキュリティー・リスクに対する現状とあるべき姿とのギャップを明らかにし、サイバー・セキュリティー・リスクへの耐性や必要となる対策を検討し、対策レベルの底上げを図ることを目的としています。具体的には、サイバー・セキュリティー対策として実装すべき5つの機能（「特定」「防御」「検知」「対応」「復旧」）に分類され、22の下位カテゴリーが定義されています（**図1**）。

さらに詳細な対策として98のサブ・カテゴリーが定義され、このサブ・カテゴリーには、対策の内容を詳細に説明するリファレンスとして、複数のベストプラクティスがマッピングされています。

またNIST-CSFは、「サイバーセキュリティ対策は企業のリスク・レベルに応じた適切なものが実装されるべき」という論理に基づいているため、具体的な対策の詳細は記載されておらず、ISO/IEC 27001、COBIT 5、CCS-CSC、ISA-62443、NIST SP 800-53といった既存の複数のベストプラクティスを参照させる構造となっています。この構造により、企業はサイバー・セキュリティー・リスク管理のライフサイクルをハイレベルで捉えることが可能となります（**図2**）。

一方で、企業にとってはどのベストプラクティスや対策を選択すべきかが課題となります。すべてのベストプラクティスや対策を充足させるようなアプローチは、コストや工数超過の事態を招く可能性があり現実的ではありません。

では、自社にとって必要なベストプラクティスや対策をどのようにして絞り込み、技術面と管理面とのバランスが取れたサイバー・セキュリティー対策を実現していくべきなのか、グローバル拠点を持つ日本企業がNIST-CSFを効果的に活用するためのポイントを次に解説していきます。

3. 効果的なNIST-CSFの適用方法

日本企業において最も多く活用されているセキュリティー・フレームワークはISO/IEC27001（ISMS:情報セキュリティマネジメントシステム）であり[7]、2014

機能	カテゴリー
特定	資産管理
	ビジネス環境
	ガバナンス
	リスクアセスメント
	リスク管理戦略
防御	アクセス制御
	意識向上およびトレーニング
	データ・セキュリティー
	情報を保護するためのプロセスおよび手順
	保守
	保護技術
検知	異常とイベント
	セキュリティーの継続的なモニタリング
	検知プロセス
対応	対応計画の作成
	伝達
	分析
	低減
	改善
復旧	復旧計画の作成
	改善
	伝達

図1. NIST-CSFの機能とカテゴリー[6]

機能	カテゴリー	サブカテゴリー	リファレンス
特定	**資産管理** 組織が事業目的を達成することを可能にするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。	企業内の物理デバイスとシステムの一覧を作成している。	CCS CSC 1
			COBIT 5 BAI09.01, BAI09.02
			ISA 62443-2-1:2009 4.2.3.4
			ISA 62443-3-3:2013 SR 7.8
			ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
			NIST SP 800-53 Rev. 4 CM-8
		企業内のソフトウェア・プラットフォームとアプリケーションの一覧を作成している。	CCS CSC 2
			COBIT 5 BAI09.01, BAI09.02, BAI09.05
			ISA 62443-2-1:2009 4.2.3.4
			ISA 62443-3-3:2013 SR 7.8
			ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
			NIST SP 800-53 Rev. 4 CM-8
		企業内の通信とデータの流れの図を用意している。	CCS CSC 1
			COBIT 5 DSS05.02
			ISA 62443-2-1:2009 4.2.3.4
			ISO/IEC 27001:2013 A.13.2.1
			NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		外部情報システムの一覧を作成している。	COBIT 5 APO02.02
			ISO/IEC 27001:2013 A.11.2.6
			NIST SP 800-53 Rev. 4 AC-20, SA-9
		リソース（例：ハードウェア、デバイス、データ、ソフトウェア）を、分類、重要度、ビジネス上の価値に基づいて優先順位付けしている。	COBIT 5 APO03.03, APO03.04, BAI09.02
			ISA 62443-2-1:2009 4.2.3.6
			ISO/IEC 27001:2013 A.8.2.1
			NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		すべての従業員と第三者である利害関係者（例：供給業者、顧客、パートナー）に対して、サイバー・セキュリティー上の役割と責任を定めている。	COBIT 5 APO01.02, DSS06.03
			ISA 62443-2-1:2009 4.3.2.3.3
			ISO/IEC 27001:2013 A.6.1.1
			NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

図2. NIST-CSF「特定」のサブカテゴリーとリファレンス[6]

年時点でISMS認証を取得している日本企業はグローバル全体で最多の約3割を占めています[8]。

ISO/IEC27001は情報システムのみならず、紙や人の頭の中にある知識などを含め、組織にとって価値ある情報すべてを対象とした対策をやや広く示しているのに対し、NIST-CSFは情報システムをサイバー攻撃から保護するための対策をやや深く示しているという特徴があります。NIST-CSFを効果的に適用していくにあたっては、ISO/IEC27001とNIST-CSFとの差分を明らかにし、その差分に対してどのベストプラクティスを適用していくか検討を進めることが重要です。

(1)差分の明確化と充足

サブ・カテゴリー・レベルで、NIST-CSFには存在しISO/IEC27001には存在しない項目は、5つの機能の中でも、特定（リスクアセスメント、リスク管理戦略）、検知（異常とイベント、セキュリティーの継続的なモニタリング）、対応（伝達）、復旧（改善、伝達）に多く存在しています（**図3**）。

これらの項目はサイバー・セキュリティー対策として必須要件であるため、該当するベストプラクティスや対策を参照しながら、どれをどのように適用していくか方針を検討し、まずは対策全体としての網羅性を確保することが重要です。

(2)技術的対策の強化

次に、サイバー・セキュリティーの脅威に対応するために、情報システムのどこを技術的に強化するべきかを検討します。NIST-CSFの5つの機能はサイバー攻撃の観点でまとめられており、特に、「防御」と「検知」については、情報システムの技術面に関わる対策が多数マッピングされています。これまでISO/IEC27001ベースで主に管理面でのセキュリティー対策を検討してきた企業は、NIST-CSFの「防御」と「検知」を確認することで、サイバー・セキュリティーにおける技術面での対策の漏れや強化すべき箇所を明確にすることができます。また技術面での対策はITセキュリティー・ソリューションと比較的容易に関係付けられるため、計画策定や予算編成の有意義なインプット情報として活用することも可能となります。

(3)グローバル・セキュリティー・ガバナンスのポイント

サイバー攻撃に対処するためには、「技術的対策」とともに「管理的対策」も重要です[9]。「技術的対策」の実装のみに目を奪われ、グローバル拠点に対する「管理的対策」、すなわちグローバル・セキュリティー・ガバナンスを効かせられていないことが、グローバルに拠点を持つ日本企業の多くが直面している共通の課題だと言えます。NIST-CSFでは、セキュリティー・ガバナンスに関わる対策には以下の3つの重要なポイントがあります。

①グローバル全体で標準化すべきサイバー・セキュリティー対策の範囲とレベルを確定する

②サイバー・セキュリティー対策を推進するための役割と責任を明確化する

③対策が実施されていることを確実にするためのモニタ

機能	カテゴリー	サブカテゴリー
特定	ビジネス環境	重要インフラとその産業分野における企業の位置付けを特定し、伝達している。
		企業のミッション、目標、活動に関して優先順位を定め、伝達している。
	ガバナンス	ガバナンスとリスク管理プロセスがサイバー・セキュリティー・リスクに対応している。
	リスクアセスメント	内外からの脅威を特定し、文書化している。
		ビジネスに対する潜在的な影響と、その可能性を特定している。
		リスクに対する対応を定め、優先順位付けしている。
	リスク管理戦略	リスク管理プロセスが自組織の利害関係者によって確立、管理され、承認されている。
		自組織のリスク許容度を決定し、明確にしている。
		企業によるリスク許容度の決定が、重要インフラにおける自組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。
防御	情報を保護するためのプロセスおよび手順	保護プロセスを継続的に改善している。
検知	異常とイベント	ネットワーク運用のベースラインと、ユーザとシステム間の予測されるデータの流れを特定し、管理している。
		イベントデータを複数の情報源やセンサーから収集し、相互に関連付けている。
		イベントがもたらす影響を特定している。
		インシデント警告の閾値を定めている。
	セキュリティーの継続的なモニタリング	発生する可能性のあるサイバー・セキュリティー・イベントを検知できるよう、ネットワークをモニタリングしている。
		発生する可能性のあるサイバー・セキュリティー・イベントを検知できるよう、物理環境をモニタリングしている。
		権限のない従業員、接続、デバイス、ソフトウェアのモニタリングを実施している。
対応	伝達	対応計画に従って、利害関係者との間で調整を行っている。
		サイバー・セキュリティーに関する状況認識を深めるために、外部利害関係者との間で任意の情報共有を行っている。
	改善	対応戦略を更新している。
復旧	改善	学んだ教訓を復旧計画に取り入れている。
		復旧戦略を更新している。
	伝達	広報活動を管理している。
		イベント発生後に評判を回復している。
		復旧活動について内部利害関係者と役員、そして経営陣に伝達している。

図3. NIST-CSFには存在し、ISO/IEC27001には存在しない25項目[6]

リングを実施する

これらを踏まえ、企業がグローバル・セキュリティー・ガバナンスを確立させるための具体的なベスト・プラクティスとして、以下の2点が挙げられます。

●グループ会社との契約にグループ全体のセキュリティー標準の遵守を明記する

●グループ会社の経営者の業績評価指標にセキュリティーのKPIを含め、本社のガバナンスに従わない経営者に対する厳しいペナルティーを科す

グローバル・セキュリティー・ガバナンスを効かせるためには、サイバー・セキュリティー対策のどこまでをグローバルで共通化し、どこからを地域や事業ごとの裁量に任せるのか、その線引きと役割を明確化するとともに、監査などのモニタリングによるチェック機能を組み込むことが非常に重要になります。

(4)適用に向けた考慮点

ここまでNIST-CSFの効果的な適用方法について、いくつかポイントを解説してきました。NIST-CSFはサイバー・セキュリティー・リスクを管理し、改善するために活用するもので、既存のサイバー・セキュリティー対策の再考や、新たにサイバー・セキュリティー対策を検討する場合のツールとして有効です。検討範囲が広範で対策が大量にあること、対策をグローバル・レベルで一意の解釈となるように再考することなど、具体的な対策案を策定していくにはそれなりの時間を要することに注意が必要です。強化すべき領域やリスク・シナリオを確実に定めた上でNIST-CSFを適用することで、グローバル拠点を含めた組織全体のサイバー・セキュリティー対策のレベルを効果的に底上げすることが可能になります。

4. 終わりに

情報セキュリティー対策の必要性は感じているものの、「あまり多くのコストをかけたくないが、万が一事故を起こした場合の説明責任は果たしたい」というのが、多くの企業の本音ではないかと思われます。しかし、現代のサイバー攻撃は過去に例を見ないほど進化し巧妙さを増しています。特に2015年は国内企業、政府組織を標的とするサイバー攻撃が頻繁に発生し、十分なセキュリティー対策を行っていた企業や組織であっても、大規模な情報漏洩などを引き起こすリスクがあることが明らかになっています。セキュリティー・ガバナンスを確立した企業の多くは、その前に何らかのセキュリティー事故を経験しており、その事故を契機として、経営トップがリーダーシップを発揮して、セキュリティー・ガバナンスの確立に成功している事実があります[10]。

警察庁の「不正アクセス行為対策等の実態調査」によると、企業などが情報セキュリティー対策を実施する上での問題点として、「対策効果が見えない」「コストがかかりすぎる」「どこまで行えばよいのか基準が示されていない」の3つが、調査が開始された2001年以降、上位を独占し続けています[11]。そこで、企業が自社に合ったサイバー・セキュリティー対策をNIST-CSFを適用してコスト効率良く行っていくことで、最終的にはグローバル拠点をも含めた企業グループ全体としてのサイバー・セキュリティー・リスクの低減とグローバル・セキュリティー・ガバナンスの確立が期待できます。

[参考文献]

[1] Security NEXT:2015年11月のセキュリティニュース一覧, http://www.security-next.com/date/2015/11

[2] 日本経済新聞:不倫SNSの会員情報流出 米メディア報道, http://www.nikkei.com/article/DGXLASDG20H1D_Q5A820C1000000/ (2015年8月20日)

[3] ロイター:アノニマスがイスラム国にサイバー攻撃予告、パリ襲撃受け, http://jp.reuters.com/article/2015/11/17/france-shooting-anonymous-idJPKCN0T60AO20151117 (2015年11月16日)

[4] 内閣サイバーセキュリティセンター:第2次情報セキュリティ基本計画, http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf

[5] NIST:Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[6] IPA:重要インフラのサイバーセキュリティを向上させるためのフレームワーク, https://www.ipa.go.jp/files/000038957.pdf

[7] ISO:ISO/IEC 27001 - Information security management, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[8] pwc:プライスウォーターハウスクーパース、「グローバル情報セキュリティ調査®2016(日本版)」を発表, http://www.pwc.com/jp/ja/advisory/press-room/press-release/2015/information-security-survey151107.html

[9] 佐々木良一:ITリスクの考え方, 岩波新書(2008年)

[10] ITmedia エンタープライズ:情報セキュリティガバナンスの5力とは, http://www.itmedia.co.jp/im/articles/0604/04/news108.html

[11] 警察庁:不正アクセス行為対策等の実態調査 調査報告書, https://www.npa.go.jp/cyber/research/h26/h26countermeasures.pdf

日本アイ・ビー・エム株式会社
セキュリティー事業本部
コンサルティング・サービス
シニア・マネージング・コンサルタント

中島 大輔
Daisuke Nakajima

1991年日本IBM入社。流通・サービス業のお客様担当SEとして主にネットワーク分野の設計・構築を担当。2001年よりセキュリティー・コンサルタントとしてポリシー整備、リスク評価、ガバナンス構築等、多数のプロジェクトをリードしている。