米国における企業のサイバー攻撃対策の現状

中沢 潔
JETRO/IPA New York

1　サマリー

先月号（「米国におけるサイバー保険の現状」（https://www.ipa.go.jp/files/000062714.pdf））に続いて米国における企業のサイバー攻撃対策（全般）の現状を紹介したい。

近年、重要インフラや企業へのサイバー攻撃により、情報漏洩や企業活動の停止といった被害だけでなく、被害への対応ぶりにより社内体制に影響が及ぶ例も出ており、サイバー攻撃の防止だけでなく、サイバーリスクマネジメントの重要性も高まっている。

米国においては、被害防止の方法として、スタートアップ企業やベンチャー企業が様々な新たな製品、サービスを生み出している。また、サイバーレンジ（Cyber Range（演習場）において、模擬サイバー戦やセキュリティ製品、サービスの試験を行っている（日本でも、東京大学や NTT データでサイバーレンジへの取り組みが始まっている。）。

サイバーリスクマネジメントとしては、

- *企業の社内の体制整備*
  CISO、CSO などのサイバーセキュリティ責任者の設置、CSIRT（Computer Security Incident Response Team、シーサート）の設置等
- *内部不正対策*
  適切なアクセス権限の付与、人事・法務・財務・事業部門等との連携、社員のモニタリング等
- *情報共有組織への参加*
  Information Sharing and Analysis Center（ISAC、アイザック）等への参加

が重要視されている。また、一部のサイバーレンジでは、報道機関への対応、規制当局への報告等も含めたサイバー被害対応のシミュレーションが実施され、企業の幹部が限られた情報に基づき早期に判断を下す訓練が提供されている。

McAfee 社により、2018 年に向けて以下の 5 つの警告がなされている（併せて、2018 年 5 月に施行が予定されている EU の GDPR（General Data Protection Regulation）は、消費者のデータやユーザーが作り出すコンテンツの扱いについての基本的なルールを形成し得るとしている。）。

- *サイバー攻撃の攻撃側と防御側の間で敵対的機械学習による「兵器競争」が進む*
- *ランサムウェア攻撃が PC 乗っ取りから IoT、裕福層、企業破壊に広がる*
- *サーバーレスアプリケーションによりアプリ依存、データ転送等を狙った攻撃機会が増える*
- *コネクテッド家電により家庭が企業の店先となり消費者プライバシーがさらされる*
- *子供たちが作り出すデジタル・コンテンツを収集する企業は長期的に風評リスクを負う*

あらゆる対策を駆使し、世界全体でのサイバーセキュリティ認知度の向上、サイバー攻撃への対応能力（被害防止、リスクマネジメント）の向上、情報共有、人材教育・育成が重要であると考えられる（特に、米国はビジネスセクター－パブリックセクター間の人材流動が強みとの声がある。）。

2　近年のサイバー攻撃による被害

全世界のサイバー攻撃による被害額は、2016 年の 3 兆ドルから増加し、2021 年には 6 兆ドルに上るとみられている。サイバー攻撃は、全世界の違法薬物取引額を上回る巨額の犯罪分野となる。この脅威に対抗するため情報セキュリティの強化が進められ、2017 年の全世界の情報セキュリティ関連支出は 864 億ドルを超え、今後 5 年以内に 1 兆ドルに達すると予想されている[1]。その結果、サイバーセキュリティ関連の雇用は、2021 年には 3 倍以上に増加し 350 万人となる。全世界のインターネット利用者は、2017 年の 38 億人から 2022 年には 60 億人へ増加するが、それだけサイバー攻撃の潜在的な対象も増えることになる[2]。

近年は、図表 1 に挙げたような手法を通じて、感染した PC をロックしたり、データを暗号化したりすることで PC を使用不可能にして、その回復と引き換えに「身代金」を要求するランサムウェアが広範な被害を引きおこし、問題になっている。この猛威を振るっているランサムウェアの被害は、2015 年の 3 億 2500 万ドルから、2017 年には 15 倍の 50 億ドル超に増加した[3]。

図表 1：代表的なサイバー攻撃の手法

代表的なサイバー攻撃の手法	内容
ソーシャルエンジニアリング型マルウェア（Socially engineered malware）	何らかの方法でユーザーを騙して、トロイの木馬プログラムを実行させてハッキングする。もっともよくある手法で、最近はランサムウェアに使われることが多い。
フィッシング詐欺（Password phishing attacks）	正規のメールやウェブページを装い、ID やパスワード、クレジットカード番号といった個人情報をだまし取る。
パッチ未適用のソフトウェア（Unpatched software）	修正プログラムによるアップデートを適用していないソフトウェアを標的に、その脆弱性を攻撃する。
ソーシャルメディアを利用した攻撃（Social media threats）	SNS の友人申請などを通じ、SNS のアカウントをハッキングし、それを足がかりに使い回されているパスワードを悪用するなどの手段で、サイバー攻撃を行う。
ターゲット型攻撃（Advanced Persistent Threats、APT 攻撃）	特定の組織や個人を狙い、様々な手段を組み合わせて継続的に行われるサイバー攻撃で、国家機関などが諜報活動として行っているものが多い。

出典：CSOonline[4]などを基に作成

（1）　重要インフラへの攻撃

サイバー攻撃の脅威は依然深刻なものであり、世界各地で重要インフラが被害を受ける事例が頻繁に報じられている。近年の重要インフラへのサイバー攻撃の例を、図表 2 に示す。

[1] https://www.gartner.com/newsroom/id/3784965
なお、これは IoT や産業制御システム向けのセキュリティ対策費用を含まない予測値。この 2 つの分野の合計額は、2022 年に 430 億ドルに達するとみられている。
https://www.csoonline.com/article/3219165/it-careers/gartner-worldwide-information-security-spending-to-hit-93b-in-2018.html
[2] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html
[3] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html
[4] https://www.csoonline.com/article/2616316/data-protection/security-the-5-cyber-attacks-you-re-most-likely-to-face.html

図表 2:近年の重要インフラへのサイバー攻撃の例

発生時期	サイバー攻撃の内容
2015 年 12 月	ウクライナで大規模な停電が 6 時間にわたり発生し、影響は 22 万 5 千人に及んだ[5]。2016 年 12 月にも、同様にハッカーによるとみられる 1 時間の停電が、ウクライナの首都キエフで発生している[6]。
2016 年 11 月	サンフランシスコ市営鉄道の運賃システムなどの内部システムがランサムウェアによる攻撃を受け、2 日間停止。市営鉄道は、当時の時価で 7 万 3 千ドルのビットコインというハッカーからの支払要求に応じず、影響を受けなかった運行システムで運行を続け、システム復旧まで運賃を無料にするという対応を取った[7]。
2017 年 4 月	"Shawdow Brokers"を名乗る正体不明のハッカー集団が、Windows のバグをついて NSA(米国家安全保障局)のスパイツールを奪取したことを公表。このツールが、WannaCry や Petya といったランサムウェアにも寄与している。
2017 年 5 月	ランサムウェア WannaCry への感染が拡散し、英国の国民健康保険サービス(NHS)下の病院や施設で診察や治療に影響が生じ、数多くの被害が出た。
2017 年 6 月	新たなランサムウェア、Petya(NotPetya、Nyetya、Goldeneye などの名前でも呼ばれる)が広まり、Merck 社などの企業やウクライナの重要インフラ関連に大きな被害が出た。

出典:各種資料[8]を基に作成

こうしたサイバー攻撃の標的となる重要インフラは、今後さらに広範なものとなる可能性がある。例えば、インターネット接続している走行中の車もハッキングされる可能性がある。2015 年 7 月、Fiat Chrysler 社のインターネット接続エンターテイメントソフトウェア「Uconnect」を搭載した走行中の車両を、外部から無線通信を通じてハッキングし、車をコントロールすることができるという実証結果が報道された。セキュリティ研究者は、インターネットを通じて外部からこのソフトウェアの脆弱性を攻撃し、車のブレーキ、エンジン、ワイパーなどを自由に操ることができた。これを受けて、Fiat Chrysler 社は、対象となる約 140 万台のリコールを自主的に行うことになった[9]。

(2) 情報漏洩と被害額

過去 5 年間の大規模なデータ漏洩事例を図表 3 に示す。こうしたデータ漏洩は、企業の経営に深刻な影響を及ぼしている。例えば、これまでで史上最大規模の 30 億ユーザーのデータ流出となった Yahoo!の場合、このデータ漏洩に関する情報開示により 2017 年 2 月の Verizon への売却額は、3 億 5000 万ドル下がったと言われている[10]。また、米国大手量販店 Target 社では、2013 年 12 月のデータ漏洩により、2014 年に CEO と CIO が退任し、対応費用は 1 億 6200 万ドルに上ったと言われている[11]。さらに、2017 年 11 月、カーシェアリングサービスの Uber 社で、1 年ほど前に運転手とユーザーの 5700 万人の個人情報データがハッキングされ、そのデータ廃棄を求め、ハッカーに 10 万ドルを支払っていたことが明らかになった[12]。

[5] http://www.bbc.com/news/technology-35667989
https://wired.jp/2017/07/27/video-hackers-take-over-power-grid-computer/
[6] http://www.bbc.com/news/technology-38573074
[7] https://www.usatoday.com/story/tech/news/2016/11/28/san-francisco-metro-hack-meant-free-rides-saturday/94545998/
[8] https://www.wired.com/story/2017-biggest-hacks-so-far/
[9] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/index.html
[10] http://money.cnn.com/2017/02/21/technology/yahoo-verizon-deal/index.html?iid=EL
[11] https://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/
[12] https://www.newsday.com/business/uber-hack-1.15090158

また、2016 年 4 月のパナマ文書公開、2017 年 11 月のパラダイス文書公開、2017 年 5 月の仏大統領決選投票直前のマクロン陣営からの大量メール流出など、データ流出は政界も揺るがす事態を引きおこしている[13]。

図表 3:過去 5 年間の大規模なデータ漏洩事例

データ漏洩元	漏洩発生時期	流出内容
US Office of Personnel Management (OPM)	2012～2014 年	現在および過去の 2200 万人の連邦職員個人情報
Target Stores	2013 年 12 月	1 億 1000 万人に上るクレジットカード・デビットカード情報や連絡先
Yahoo!	2013～14 年	30 億人のユーザーアカウント
eBay	2014 年 5 月	1 億 4500 万人のユーザー全員の氏名、住所、誕生日、パスワード
JP Morgan Chase	2014 年 7 月	7600 万世帯と 700 万の小企業のデータ
Home Depot	2014 年 9 月	5600 万人の顧客クレジットカード・デビットカード番号
Anthem	2015 年 2 月	現在および過去の顧客 7880 万人の個人情報
Adult Friend Finder	2016 年 10 月	4 億 1220 万人のアカウント
Equifax	2017 年 7 月	1 億 4300 万人の個人情報（ソーシャル・セキュリティ・ナンバー、誕生日、住所、運転免許番号）、このうち 20 万 9000 人のクレジットカードのデータ

出典：CSOonline[14]を基に作成

2017 年 6 月、プライバシー、データ保護、情報セキュリティポリシーについてリサーチを実施する米調査会社 Ponemon Institute[15]と IBM は、13 の国と地域の 410 社を対象とした情報漏洩のコストに関する 2017 年度レポートを発表した[16]。これによれば、データ漏洩インシデント対応の世界平均コストは、2016 年度から 10%減少し、362 万ドルであり、漏洩データ 1 件当たりに直すと平均 141 ドルだった。データ漏洩インシデントの全コストを地域別に見ると、欧州では昨年比で 26%の減少が見られたのに対し、米国ではコストが昨年比で 5%上昇し、データ漏洩インシデント 1 件のコストは 735 万ドルに上った。例えば、コンプライアンス失敗による費用は、欧州よりも 5 割以上多い。米国企業は、データ漏洩関連の通知にも平均で 69 万ドルを費やしている（これには、欧州は統一規制である一方、米国は全 50 州のうち 48 州が独自のデータ漏洩法を定めていることも影響した可能性がある。）。調査では、インシデント対応チーム（Incident Response (IR) team）を設置している企業では、インシデント対応コストが 3 年連続で減少し、漏洩データ 1 件当たり 19 ドル低いことが明らかになった。また、30 日以内にデータ漏洩を停止できる企業は、そうでない企業と比べてコストを 100 万ドル近く抑えることができている。EU では、2018 年 5 月に EU 一般データ保護規則[17]が施行されることからも、対応の迅速化は緊急の課題となっている。

この調査から得られた知見としては、他に以下の点がある。

- 産業別では、データ漏洩コストがもっとも高かったのは 7 年連続でヘルスケア産業であり、漏洩 1 データ当たりの費用は 380 ドルと、全業種平均 141 ドルの 2.5 倍以上に上った。

[13] https://www.wired.com/story/2017-biggest-hacks-so-far/
[14] https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html
[15] https://www.ponemon.org/
[16] https://www-03.ibm.com/security/uk-en/data-breach/
日本語版：https://www-935.ibm.com/services/jp/ja/it-services/business-continuity/impact-of-business-continuity-management/
[17] EU 一般データ保護規則（GDPR、General Data Protection Regulation）は、2018 年 5 月に施行される欧州の個人データ保護に関する新しい規則。EU 圏内の個人情報を扱う全世界の企業が対象となり、違反時に課せられる高額な制裁金からも注目されている。

- データ漏洩コストを増大させる最大の要因は、給与計算から顧客管理に至るまでの各種サービスプロバイダーなどのサードパーティー（外部企業）の関与であり、データ 1 件当たり 17 ドルコストが増加する。
- データ漏洩のコスト削減として有効だったのは、早期漏洩対応（1 件当たり 19 ドルの差）、暗号化の徹底（1 件当たり 16ドルの差）、研修（1 件当たり 12.5ドルの差）といった要素であった。
- IBM の Resiliency Orchestration ソリューションを使った場合、システム復旧を自動化しシステム管理を簡素化することで常時稼働が実現され、手動管理の 1 日当たり平均コスト 6101 ドルに比べ、Resiliency Orchestration を活用した場合の 1 日当たり平均コストは 4041ドルと 39%低かった。

なお、ここで考えている、データ漏洩により企業に生じるコストとしては、以下のようなものがある[18]。

- 直接経費：データ漏洩に対応するために生じる直接の経費（弁護士費用、直接相談口設置、途上与信監視、製品・サービスの割引が含まれる）
- 間接費用：直接現金で支出されるもの以外の、データ漏洩問題に対応するために割かれる時間、労力などの企業のリソースの経費（内部調査、通信、顧客喪失や顧客獲得率低下による損失推算額）
- 機会費用：データ漏洩が公表され、風評によりビジネスチャンスを失うことで生じる費用

（3） セクター別のサイバー攻撃被害

"IBM X-Force Threat Intelligence Index 2017"[19]では、2016 年のデータ漏洩のトレンドを示す 5 つのセクターとして、金融、情報通信、製造、小売、ヘルスケアを挙げている。これらのセクターへの攻撃で共通して多かったのは、SQL インジェクション（SQLi）[20]と OS コマンドインジェクション（OS CMDi）[21]であった。SQLi と OS CMDi に対する対策は進められているものの、手軽さからこれらの攻撃手法が良く利用されている。他方、セクター毎に保持する情報や使用するシステムが違うため、セクター毎に受ける攻撃の傾向にも違いがある。

- 金融セクターへの攻撃数はセクター別で、2015 年には 3 位であったが、2016 年にはもっとも攻撃を受けたセクターとなった。この増加は、SQLi と OS CMDi による攻撃が増加したことによる。SQLi や OS CMDi による攻撃が成功すれば、機微データの読み出し、改変、破壊が可能になる。金融機関のデータには、莫大な個人情報が含まれていることから、標的となりやすい。
- 情報通信セクターへの攻撃は 2016 年に増加したが、このセクターで一番多かったのは、バッファオーバーフロー攻撃[22]であり、51%がこの攻撃方法であった。
- 製造セクターでは、SQLi による攻撃が 71%以上と大半を占めた。このセクターは、コンプライアンス基準を満たしていない設計上脆弱なシステムが多いと認識されていることから、攻撃目標にされやすい。
- 小売セクターは、クレジットカードやソーシャル・セキュリティ・ナンバーといった個人情報を大量に抱えていることから標的にされることが多い。このセクターへの攻撃では、SQLi と OS CMDi による攻撃が半数を占めた。
- ヘルスケア・セクターへの攻撃では、SQLi と OS CMDi による攻撃が合計で 48%を占めた。ヘルスケア・セクターのデータは、サイバー犯罪者がもっとも求めているものであり、Dark Web[23]（ダ―ク・ウェブ）のアンダーグラウンド取引で広く流通している。

---

18 "2017 Cost of Data Breach Study, Global Overview" pp. 3, 7, 29

19 https://www.ibm.com/security/data-breach/threat-intelligence

20 Structured Query Language は「構造化照会言語」。多くの企業や組織のホームページやショッピングサイトでは、データベースを利用した Web アプリケーションが使われている。こうした Web アプリケーションが想定していない SQL 文を実行させることで脆弱性を突き、データベース接続を不正に操作する攻撃方法。

21 OS コマンドは「OS への命令文」。データの入力や操作を受け付ける Web サイトで、入力するパラメータに OS に対する命令文（コマンド）を紛れ込ませて不正に操作する攻撃方法。

22 実行中のプログラムメモリー内に攻撃プログラムを送り込み、データ構造体を改竄する攻撃。

23 Dark Web は秘密にされているものではなく、「インターネット上にオーバーレイネットワークで構築された Web サイトの集まり」であり、Dark Web 上のサイトへは専用ツールを使えば誰でもアクセスできるが、そのサイトを誰がどのサーバーで運営しているかを特定することは非常に困難。世界中の政府機関や法執行機関はソーシャルネットワークやバーチャルコミュニテ

また、”2016 Data Breach Investigations Report”[24] によれば、Web Apps.（ウェブアプリケーション）を通じた攻撃によるデータ漏洩が増加しており、特に金融分野での増加が著しいことが明らかになっている。その一方で、クライムウェア（犯罪行為を目的としたプログラム）によるデータ漏洩は減少している。

図表 4. サイバー攻撃のセクター別発生パターン

	クライムウェア	サイバースパイ	DoS 攻撃	盗品利用	その他のエラー	スキミング	POS システム	職権濫用	Web Apps.	その他
宿泊	0%	0%	0%	<1%	1%	<1%	95%	1%	1%	1%
教育	0%	7%	0%	17%	27%	0%	0%	3%	30%	17%
エンターテイメント	0%	0%	0%	3%	0%	0%	47%	0%	50%	0%
金融	1%	<1%	<1%	<1%	2%	9%	0%	4%	82%	2%
ヘルスケア	3%	3%	0%	19%	22%	0%	7%	32%	3%	11%
情報	1%	3%	0%	0%	25%	0%	<1%	11%	57%	4%
製造	3%	47%	0%	0%	0%	0%	3%	24%	21%	3%
学術研究，専門・技術サービス	4%	19%	0%	4%	15%	0%	0%	21%	13%	25%
官公庁	12%	16%	0%	9%	37%	0%	0%	13%	9%	4%
小売	1%	1%	0%	0%	<1%	3%	64%	2%	26%	4%

出典："2016 Data Breach Investigations Report", Verizon[25]

3　サイバーセキュリティ製品・サービスの現状

（1）　サイバーセキュリティ業界概要

全世界のサイバーセキュリティ市場は、2004 年には 35 億ドルだったが、2017 年にはその約 35 倍の 1200 億ドルに達するとみられている。サイバーセキュリティ専門の調査会社 Cybersecurity Ventures は、全世界のサイバーセキュリティのための出費が 2017 年から 2021 年にかけて、年率 12～15%で成長し、1 兆ドルを突破するとみている。例えば、J.P. Morgan Chase & Co は、サイバーセキュリティの予算を 2 億 5000 万ドルから 5 億ドルに倍増した。Bank of America は、サイバー犯罪との戦いのための予算には糸目を付けないとしている。Microsoft 社は、引き続きサイバーセキュリティの研究開発に今後も年間 10 億ドルの予算を投じる予定である。また、米国政府もサイバーセキュリティに関する予算を、2016 年の 140 億ドルから 2017 年は 190 億ドルに増額する[26]。

また、世界規模のサイバーセキュリティ分野ベンチャーへの投資は 2012 年以降増加を続けており、2016 年の投資額は 2015 年の 38 億ドルから 6%減少したものの 428 件の案件があり、2017 年も投資額、案件数共に過去最高を記録する勢いである（図表 5）。

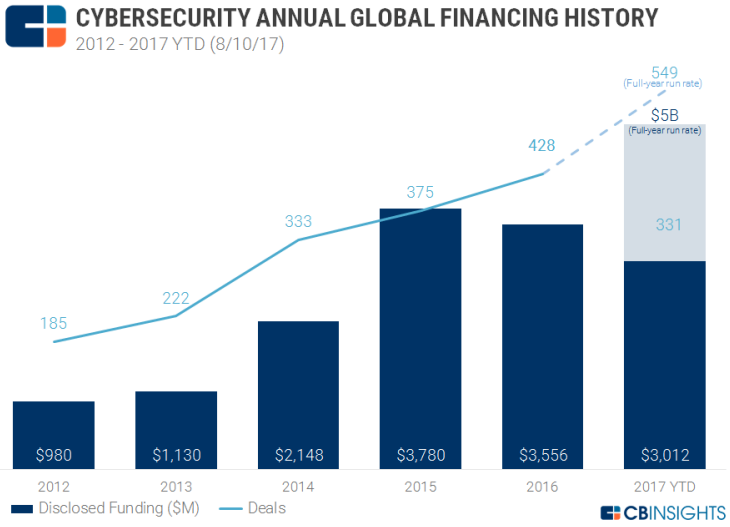
ィを監視しており、Dark Web はその匿名性から、過激派やテロ組織により思想普及や調整・連絡手段として利用されることがあり、先んじて情報を取得するための監視対象となっている。
https://inforium.nttdata.com/trend_keyword/266.html

[24] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

[25] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf pp.25

[26] https://cybersecurityventures.com/cybersecurity-market-report/

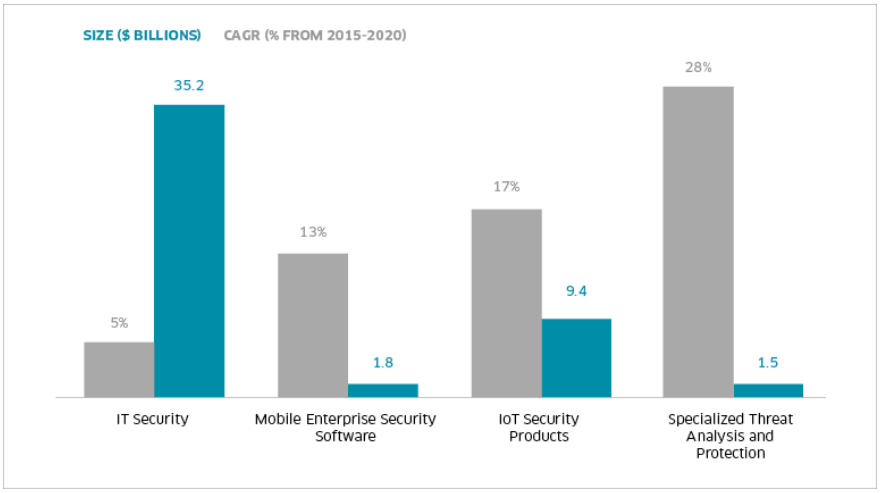
図表 5:全世界のサイバーセキュリティ企業資金調達額推移



出典:CB Insight[27]

従来のサイバーセキュリティ製品・サービスに比べてまだ市場規模は小さいが、今後は企業向けのモバイルセキュリティ・ソフトウェア、IoT セキュリティ製品、なかでも標的型サイバー攻撃向け特化型脅威対策(STAP:Specialized Threat Analysis and Protection)といった分野が、大きく成長するものと期待されている。

図表 6:サイバーセキュリティ製品分野別市場規模と年平均成長率
Market Size and Growth



出典:Bloomberg Intelligence (Anurag Rana – Senior Industry Analyst), Sept. 22nd, 2016 and IDC[28]

(2) セキュリティ対策ソフトウェアやサービスの動向

a. AI を活用したサイバーセキュリティ・ベンチャー企業

現在、サイバーセキュリティ分野で大きな注目を集めているのが AI の活用である。その背後には、サイバー攻撃が厳しさを増しているにもかかわらずサイバーセキュリティ人材が不足していること、これまではなかっ

[27] https://www.cbinsights.com/research/cybersecurity-deals-funding-acquisitions/
[28] http://business.nasdaq.com/marketinsite/2017/Cybersecurity-Investing-Update.html

たサイバー攻撃であるゼロデイ攻撃が増加していることという 2 つの理由がある。質の高い人材の数がボトルネックとなっている現状では、資金を投じようにも、人手が制約となっている限り、改善は進まない。また、ゼロデイ攻撃は、開発者が修正パッチを公開する前にソフトウェアの脆弱性を突くサイバー攻撃で、現状有効な対策がない。こうした問題を解決するために、AI の機械学習を活用して自動的なサイバーセキュリティ対応をしようとする取り組みが注目を集めている。

こうした SIEM（Security Information and Event Management）製品は、ログやイベントのデータをリアルタイムで解析し、セキュリティ情報をモニタリングすることができる。ガートナーでは、2017 年のサイバーセキュリティへの企業の支出は 984 億ドルと推算しているが、SIEM ソフトウェアはそのうち 24 億ドルを占めているにすぎないとしている。この分野の成長は緩やかで、2018 年に 26 億ドル、2021 年に 34 億ドルと見込んでいる。ガートナーでは、SIEM ソフトウェアは、主にコンプライアンス遵守が重視される大企業や公的機関での使用に留まっているからだとみている。これは、SIEM ソフトウェアを利用するには、年間 10 万ドル以上の利用料に加えて、これを保守管理する専門的な人材を雇う必要があるからである[29]。

図表 7：AI を活用したサイバーセキュリティ・ベンチャー企業の例

企業名	累積投資（百万ドル）	本拠地	設立年	概要
Tanium[30]	$295M	カリフォルニア州エミリービル	2007	組織内の膨大なエンドポイントの安全性をリアルタイムで管理するソリューションを提供する。
Cylance[31]	$177M	カリフォルニア州アーバイン	2012	AI アルゴリズムを活用し、マルウェアを予測・特定・阻止し、ゼロデイ攻撃の被害を抑える技術を開発。
LogRhythm[32]	$126M	英国メイデンヘッド	2003	サイバー攻撃情報と分析を提供し、サイバー攻撃に対して迅速な検出・対応・防衛ができるようにすることに加え、自動的にコンプライアンスを遵守し、防御を確固としたものにする。
SentinelOne[33]	$109M	カリフォルニア州パロアルト	2013	AI を活用し、行動検知と自動対応を組み合わせて、エンドポイントをサイバー攻撃から保護するプラットフォーム。
Darktrace[34]	$107M	英国ケンブリッジ	2013	高等数学を活用した二者間の行動分析を通じて、組織内の異常な動きを自動的に検出する。
Sift Science[35]	$54M	カリフォルニア州サンフランシスコ	2011	オンラインビジネス向けに、リアルタイム機械学習による不正防止を行う。
Exabeam[36]	$35M	カリフォルニア州サンメテオ	2013	既存のログデータを活用し、攻撃を優先付けし、効果的な対応を示唆し、高度なサイバー攻撃を迅速に検出するユーザー行動分析を提供する。

[29] https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html
[30] https://www.tanium.com/
[31] https://www.cylance.com/en_us/home.html
[32] https://logrhythm.com/
[33] https://www.sentinelone.com/
[34] https://www.darktrace.com/
[35] https://siftscience.com/
[36] www.exabeam.com

E8 Security[37]	$22M	カリフォルニア州レッドウッド	2013	長期間データ保持と遡及的解析のためのビッグデータ・プラットフォームを利用した解析ソフトウェアを提供している。
CyberX[38]	$11M	マサチューセッツ州フラミングハム	2012	ネットワークの挙動解析により、異常を検知する業務用インターネット・ネットワークを設計する。
Interset[39]	$10M	カナダ・オタワ	2015	製造業、ライフサイエンス、ハイテク分野、金融、政府関係、航空・防衛産業、証券仲介業といった業界の重要なデータを保護するための行動解析を提供する。
PatternEx[40]	$8M	カリフォルニア州サンノゼ	2013	企業内ネットワークでユーザーがサイバー攻撃をリアルタイムで予測・予防することができるよう、悪意のある挙動を特定するプラットフォームを提供する。
SecBI[41]	$5M	イスラエル	2014	外部からのサイバー攻撃に感染したユーザー、ドメインなどを含めてサイバー攻撃を明らかにする高度なサイバー攻撃検出システムを提供する。
Avata Intelligence[42]	$2.5M	カリフォルニア州ベニス	2013	サイバー攻撃を理解し対応するために、記述的、診断的、予測的、示唆的な解析を提供する。
Jask Labs[43]	$2M	カリフォルニア州サンフランシスコ	2015	AI と高度な解析を活用し、企業のデータと運営の安全性を保護する。

出典：各種資料[44]を基に作成

b. モバイル・IoT 関連のサイバーセキュリティ・ベンチャー企業

今後の成長が期待されるモバイル向けあるいは IoT 向けのサイバーセキュリティでも様々なソリューションが開発されている。特に、Wi-Fi デバイスは、過去の履歴をもとにアクセスポイントを探すことから、個人情報を容易に割り出せるといった危険性も指摘されており、セキュリティ対策が求められている[45]。

図表 8：モバイル・IoT 関連サイバーセキュリティ・ベンチャー企業

企業名	累積投資（百万ドル）	本拠地	設立年	概要
Mojo Networks[46]	$69M	カリフォルニア州マウンテンビュー	2002	Wi-Fi ネットワークのセキュリティおよびパフォーマンス管理のサービスを提供する。

[37] http://e8security.com/
[38] www.cyberx-labs.com
[39] https://interset.com/
[40] https://www.patternex.com/
[41] http://www.secbi.com/
[42] https://avataai.com/
[43] https://jask.ai/
[44] https://www.cbinsights.com/research/cybersecurity-artificial-intelligence/
[45] https://www.youtube.com/watch?v=fSErHToV8IU
[46] https://www.mojonetworks.com/

Bastille Networks[47]	$39M	カリフォルニア州サンフランシスコ	2014	IoT へのサイバー攻撃の検知と管理を行う。無線状態を検査し、予防対策を講じるソリューションを提供するスタートアップ企業。

出典：各種資料[48]を基に作成

c. その他のサイバーセキュリティ・ベンチャー企業

企業内のエンドポイント対策や、一貫性のあるポリシーを適用できるようにするクラウドアクセスセキュリティブローカー（CASB）など、社内のサイバーセキュリティ対策を一貫した形で管理できるようにする技術を提供するベンチャー企業が注目を集めている。また、企業内には多数の脆弱性が存在するため、これを検知するための侵入検査（penetration testing、または ethical hacking）や、脆弱性管理ソフトウェアにもニーズがある[49][50]。

図表 9：その他のサイバーセキュリティ・ベンチャー企業

企業名	累積投資（百万ドル）	本拠地	設立年	概要
Illmio[51]	$267.2M	カリフォルニア州サニーベール	2013	データセンターやクラウド上でサイバー攻撃の拡散を防ぐ適応的マイクロ・セグメンテーション技術を開発。
CrowdStrike[52]	$281M	カリフォルニア州サニーベール	2011	エンドポイント（ネットワークに接続された様々な端末）のセキュリティを保護するクラウドベースの SaaS を提供。
Netskope[53]	$231.4M	カリフォルニア州ロスアルト	2012	ユーザーと複数のクラウドプロバイダーの間に単一のコントロールポイントを設け、ここでクラウド利用の可視化や制御を行うことで、全体として一貫性のあるポリシーを適用できるようにするクラウドアクセスセキュリティブローカー（CASB）。
Wickr[54]	$82M	カリフォルニア州サンフランシスコ	2011	機密度の高いメッセージ、写真、動画、音声、ファイルなどをやり取りできる、その場限りでフリーのメッセージング App プラットフォーム。
HiTrust Alliance[55]	NPO	テキサス州フリスコ	2007	明らかになっている脆弱性を元にマルウェアの構成要素を検知する。
Attivo Networks[56]	$44M	カリフォルニア州フリーモント	2011	罠や仕掛けによりハッカーの攻撃情報を入手し対応策を講じる。
Kenna Security[57]	$25M	イリノイ州シカゴ	2009	企業のネットワークの脆弱性を検出して優先付けするサービスを SaaS として提供している。

[47] https://www.bastille.net/
[48] https://www.cbinsights.com/research/enterprise-cybersecurity-startups-funding/
[49] https://www.csoonline.com/article/3238128/hacking/what-is-penetration-testing-the-basics-and-requirements.html
[50] https://www.csoonline.com/article/3238080/vulnerabilities/what-is-vulnerability-management-processes-and-software-for-prioritizing-threats.html
[51] https://www.illumio.com/home
[52] https://www.crowdstrike.com/
[53] https://www.netskope.com/
[54] https://www.wickr.com/
[55] https://hitrustalliance.net/
[56] https://attivonetworks.com/
[57] https://www.kennasecurity.com/

SCYTHE[58]		バージニア州アーリントン	2017	同社の製品、CROSSBOW はサイバーセキュリティ検証プラットフォームであり、ネットワークへの侵入、ウィルス感染、フィッシング詐欺などのサイバー攻撃に対する対応をシミュレーションできる。
Bay Dynamics[59]	$31M	カリフォルニア州サンフランシスコ	2001	実際のネットワーク環境を考慮して、脆弱性の優先度を正確に調べることができる脆弱性管理ソフトウェア、Risk Fabric を提供している。
NSS Labs[60]	$27M	カリフォルニア州カールスバーグ	1991	実際のネットワークをミラーリングして、脆弱性を検証できるツール CAWS Continuous Security Validation Platform を提供している。

出典：各種情報[61][62]を基に作成

d. サイバーレンジの活用

高度なスキルを持つサイバーセキュリティ人材の不足は世界的な課題であり、人材育成の手段として大きな注目を集めているのが「サイバーレンジ（Cyber Range[63]）」である。サイバーレンジは、特別に設置された施設で、外部からのサイバー攻撃への対応を訓練するために模擬サイバー戦が行われる。サイバーレンジは、セキュリティ製品・サービスの試験に活用することもできる。

DARPA は、2009 年から 2012 年にかけて、National Cyber Range を開発した。その成果は、2012 年 10 月に DARPA から DOD へ Test Resources Management Center（TRMC）として引き渡された[64]。この開発を端緒として、現在は民間でも利用可能なサイバーレンジが各地に広まっている。
例：

- Michigan Cyber Range[65]
- Virginia Cyber Range[66]
- Palo Alto Networks（アムステルダム、シドニー、ワシントン D.C.、サンタクララ）[67]
- Baltimore Cyber Range[68]
- Cyberbit[69]

既に、日本でも、東京大学や NTT データでサイバーレンジへの取り組みが始まっている[70]。

例えば、大手金融機関 Wells Fargo は、サイバーレンジを活用して、セキュリティ対策の訓練を実施している。Wells Fargo の CISO、Rich Baich 氏は、米国海軍に 20 年以上にわたり勤務し、国家安全保障局（National Security Agency）海軍情報戦士官を務めてきた。現在は、金融セクターのサイバー攻撃対応を支援するために設立された、Financial Services Sector Coordinating Council[71]の議長も務めている。サイ

[58] https://www.scythe.io/
[59] https://baydynamics.com/
[60] https://www.nsslabs.com/
[61] https://www.cbinsights.com/research/enterprise-cybersecurity-startups-funding/
[62] https://www.csoonline.com/article/3238080/vulnerabilities/what-is-vulnerability-management-processes-and-software-for-prioritizing-threats.html
[63] Range は、「射撃場、ミサイル（ロケット）試射場」の意味（研究社 新英和中辞典）。
[64] https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf
https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2017/test/ChristensenPart1.pdf
[65] https://www.merit.edu/cyberrange/
[66] https://virginiacyberrange.org/
[67] https://www.paloaltonetworks.com/solutions/initiatives/cyberrange-overview
[68] https://www.baltimorecyberange.com/
[69] https://www.cyberbit.com/solutions/cyber-range/
[70] http://itpro.nikkeibp.co.jp/atcl/column/14/346926/072700589/
http://www.intellilink.co.jp/security/services/cyberrange.html
[71] https://www.fsscc.org/

バーレンジの運営には高額の費用がかかるため、中堅以下の金融機関ではサイバーレンジを保有して維持することが難しい。そこで、Baich 氏は、サイバーレンジの共同運用を提唱している[72]。

サイバーレンジのベンダーとしては、Cyberbit 社（イスラエル・Elbit Systems 社[73]の子会社）[74]、Raytheon 社[75]、Lockheed 社[76]、SimSpac 社[77]といった会社が代表的である。これらのサイバーレンジは企業内訓練だけでなく、教育にも使われ始めている。2017 年 7 月、バージニア州 Regent University は、Cyberbit のプラットフォームを導入したサイバーレンジ訓練施設、Institute for Cybersecurity を開設し、サイバーセキュリティ専門家の育成にあたろうとしている。これは、私大としては初の取り組みであり、学生だけではなく、企業や政府関連、軍関連も対象とした認定プログラムを提供する[78]。

IBM はサイバーレンジのソフトウェア自体を販売してはいないが、2 億ドルを投じてサイバーレンジ施設をマサチューセッツ州ケンブリッジに 2016 年 11 月に開設した。ここに設置されたデータセンターは、Fortune500 企業級のもので、ヘルスケア、エネルギー、金融など様々なセクターの企業のシミュレーションが実施できるようになっている。これまでに顧客企業から約 800 名の幹部がここを訪れ、自社のインシデント対応力を試している。参加者の多くは金融業界である。参加者は、シミュレーションで迫真のシナリオを体験し、実際に起こるかもしれない報道・規制・法執行・技術的な問題への対応を迫られる。そして、情報が限られた中でも早期に判断を下し、被害を抑えることができるよう、経験を身に染み込ませるべく訓練を実施する。IBM はサイバーレンジ開発に当たり、米国空軍の協力も得ており、戦闘機パイロットの判断メソッドも訓練には取り入れられている。このサイバーレンジの利用自体は無料で、IBM はセキュリティ・ソリューションを販売している。さらに今後は、実害を及ぼさないように無害化されたマルウェアを用いて、事前の通知なしに実戦サイバー演習を実施することも検討されている[79]。

4 サイバーリスクマネジメントの現状

（1） 企業の社内体制

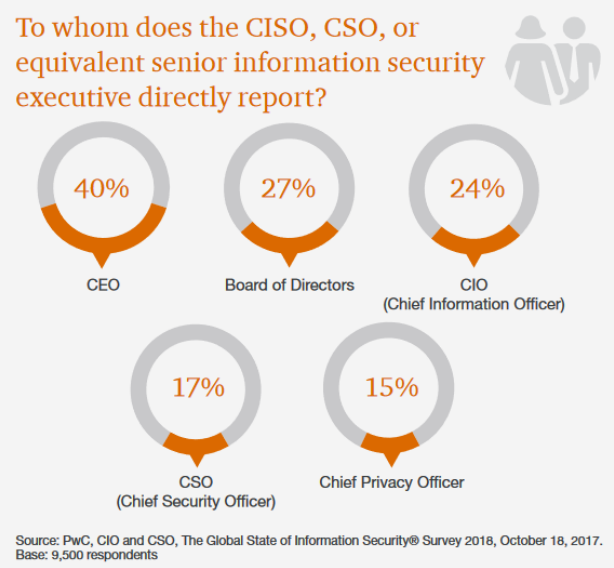
a. CISO、CSO などのサイバーセキュリティ責任者の設置

米国を中心に近年、Chief Information Security Officer（CISO）、あるいは Chief Security Officer（CSO）の役職を設置する企業が増えているが、CISO を設置している企業は 52%、CSO を設置している企業は 45%、セキュリティ専門の人員を配置している企業は 47%にとどまっている。CISO、CSO、あるいはこれらに相当する情報セキュリティ担当者のレポートラインも、CEO、役員会、CIO、CSO など様々である[8081]。ミッションもしばしば曖昧であり、活動への理解も得られにくいが、いったん被害が生じれば責任を問われるといったことから、CISO の在職期間は 18 ヶ月程度といわれ[82]、業界ではデータ漏洩などに伴う去就がしばしば報道されている[83]。

---

[72] https://www.americanbanker.com/news/how-wells-fargos-cyber-warriors-stay-battle-ready
[73] http://elbitsystems.com/
[74] https://www.cyberbit.com/solutions/cyber-range/
[75] https://www.raytheon.com/cyber/capabilities/range/
[76] https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-products.html
[77] https://simspace.com/products-overview/
[78] https://www.regent.edu/news-events/institute-cybersecurity-build-state-art-cyber-range-campus/?begin=now&utm_expid=140130747-105.xW4XajVAR9ecyKGxzrfU8g.1
[79] https://www.americanbanker.com/news/how-wells-fargos-cyber-warriors-stay-battle-ready
[80] https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society-against-cyber-shocks.pdf
"The Global State of Information Security® Survey 2018", PwC, 2017, pp.10
[81] この調査は、2017 年春、122 ヶ国の 9500 名以上の CEO、CFO、CIO、CSIO、CSO や、IT セキュリティ担当者からの回答を基に作成された。回答者の 38%は北米、29%が欧州、18%がアジア、14%が南米、1%が中東およびアフリカからである。
"The Global State of Information Security® Survey 2018", PwC, 2017, pp.16
[82] https://www.csoonline.com/article/3057243/security/these-cisos-explain-why-they-got-fired.html
[83] https://www.csoonline.com/article/3204008/it-careers/security-executives-on-the-move-and-in-the-news.html

図表 10：情報セキュリティ責任者のレポートライン



出典："The Global State of Information Security® Survey 2018"[84], PwC, 2017, pp.10

b. CSIRT の設置

Computer Security Incident Response Team (CSIRT、シーサート)は、サイバー攻撃への対応を目的とした専門チームである。CSIRT の対応範囲は、所属する企業、政府機関などによって様々だが、サイバー攻撃の報告・分析・対応が主な任務である。サイバー攻撃に対する対応を迅速に行うことが被害を最小限に食い止め費用を抑える鍵となることから、CSIRT を設置して備えておくことが重要になる。専従組織の場合もあれば、アドホックに活動している場合もある。規模も様々で、日本の JPCERT コーディネーションセンター（JPCERT/CC)[85]のように国全体を対象としたものから、企業向けのサービスとして提供されているものまで様々である[86]。日本では、JPCERT/CC 以外に、日本国内の CSIRT の連携や情報共有を目的とした日本シーサート協議会[87]が活動している。「企業の CISO や CSIRT に関する実態調査 2017－調査報告書－」（情報処理推進機構）の調査結果[88]によれば、米国企業の 90.1%、欧州企業の 78.0%、日本企業の 66.8%で、インシデント対応を担当する組織が設置されている（CSIRT あるいは他の名称の組織も含む。）。

また、米国の民間サイバーセキュリティ調査・訓練会社、SANS Institute[89]の 2017 年の調査[90]によれば、少なくとも 1 名のインシデント対応専任メンバーを持つ企業・団体は全体の 84%（2016 年度 76%）であり、サイバー攻撃に際して 1 名以上の専任メンバーが対応に当たる企業・団体は 55%（2016 年度 55%）だった。対応チームの規模内訳を次表に示す。なお、この調査は全世界を対象に実施されているが、総数は示されていない。回答者を業界別に見ると、サイバーセキュリティ業界が 17.3%、金融業界が 13.7%、テクノロジー関連が 12.3%、政府関連が 9.6%、製造業が 6.3%、通信および ISP が 5.8%、教育が 5.5%、ヘルスケアが 5.2%、小売が 3.8%、電力・ガス・水道が 3.0%であった。

図表 11：インシデント対応チームの規模内訳

	不明	無	1−2 名	3−5 名	6−10 名	11−20 名	20 名超

[84] https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society-against-cyber-shocks.pdf
[85] http://www.jpcert.or.jp/
[86] https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm?
[87] http://www.nca.gr.jp/
[88] https://www.ipa.go.jp/files/000058850.pdf pp.93
[89] https://www.sans.org/
[90] https://www.sans.org/reading-room/whitepapers/incident/show-on-2017-incident-response-survey-37815

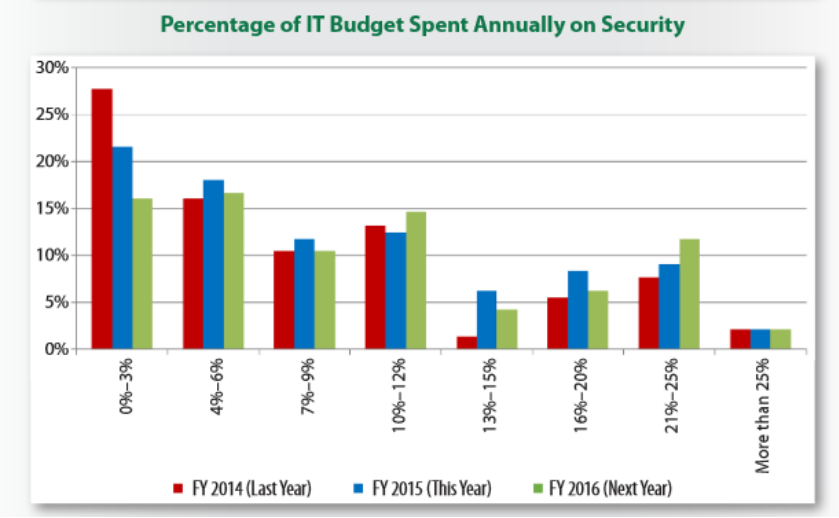
インシデント対応専門チーム	3.6%	11.7%	36.4%	25.9%	14.2%	4.5%	2.8%
内部兼務者（セキュリティ部署、IT リソース運営・管理部署）	5.3%	14.6%	27.9%	21.9%	13.8%	5.7%	7.3%
インシデント対応を含むアウトソーシング（MSSP[91]など）	13.4%	42.9%	18.6%	8.5%	4.9%	2.4%	4.0%
その他	5.3%	17.4%	2.0%	0.8%	0.0%	0.8%	0.0%

出典：”The Show Must Go On! The 2017 SANS Incident Response Survey[92]”, pp.14

c. 米国企業のサイバーセキュリティ予算

SANS Institute の調査によれば、サイバーセキュリティに割かれる予算は増加を続けており、特に内部の対応能力強化に目が向けられている[93]。そのなかでも、機微データの保護とコンプライアンス遵守への対応に力が注がれている。しかし、事の性質上、費用対効果を裏付けることが難しく、明確な指標がないのが実情である。この調査は 2015 年第 4 四半期に実施され、169 の回答を基にしたものであり、72%が米国からの回答であった。業種別の内訳は、金融が 25.4%、IT 関連 14.2%、政府機関 13.0%、教育機関 8.9%、ヘルスケア関連 7.7%であった。IT 予算に占めるセキュリティ関連費用の割合は、0%から 25%以上と様々であるが（図表 12）、組織の規模毎に中央値を取り比較したのが図表 13 である。

図表 12：IT 予算に占めるセキュリティ関連費用の割合とその企業の割合



出典："IT Security Spending Trends（2016 年 2 月、SANS Institute）”[94]

[91] MSSP（managed security service provider）は、いわばサイバー警備会社で、セキュリティデバイスおよびシステムのモニタリングと管理のアウトソーシングを年中無休で引き受ける。一般的なサービスとしては、ファイアウォールの管理、サイバー侵入の検知、VPN（virtual private network）の提供、ウィルス対策などがある。
https://www.gartner.com/it-glossary/mssp-managed-security-service-provider
[92] https://www.sans.org/reading-room/whitepapers/incident/show-on-2017-incident-response-survey-37815
[93] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697
[94] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

図表 13:IT 予算に占めるセキュリティ関連費用と IT 予算に占める割合の中央値(規模別)

規模	従業員数、調査回答数	FY2014		FY2015		FY2016(予算)	
		予算額	比率	予算額	比率	予算額	比率
大	5000 人超(n=67)	$1M-$10M	4%-6%	$1M-$10M	4%-6%	$10M-$50M	7%-9%
中	500～5000 人(n=50)	$500K-$1M	4%-6%	$1M	4%-6%	$1M-$10M	7%-9%
小	500 人未満(n=52)	$100K-$500K	3%-4%	$100K-$500K	4%-6%	$100K-$500K	6%-7%

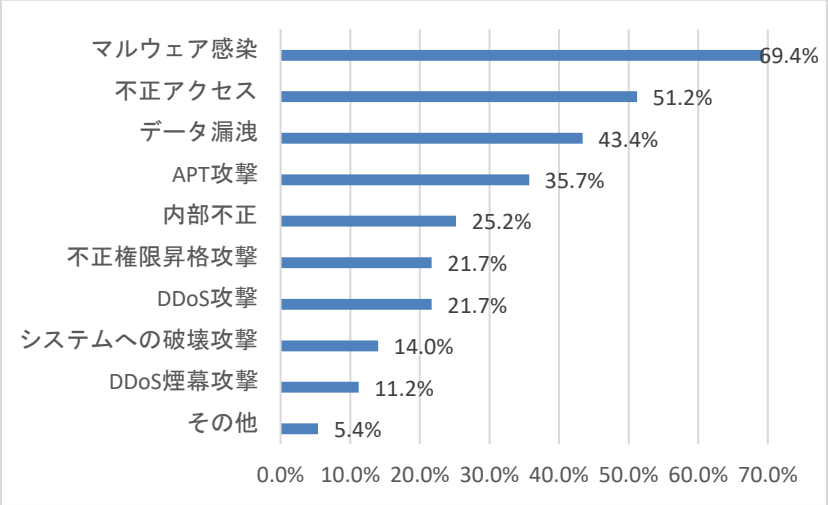
出典:"IT Security Spending Trends(2016 年 2 月、SANS Institute)[95]"から作成

(2) 内部不正対策

Crowd Research Partner 社の"Insider Threat 2018 Report"によれば、90%の組織では、内部不正に対して自組織が脆弱だと懸念している。そう感じるリスク要素として、過剰なアクセス権限を与えられているユーザーが多すぎること(37%)、機密情報にアクセスすることができるデバイスが増大していること(36%)、情報技術がますます複雑になっていること(35%)といった点が挙げられている[96]。

SANS Institute の調査によれば、2016 年のサイバー攻撃の原因は次表の通りであった。ここでは、マルウェア攻撃や DDoS 攻撃などの外部からの攻撃に交じって、内部不正が 25.2%と無視できない割合を占めていることが分かる。

図表 14:データ漏洩の原因[97]



出典:" Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey[98]"

[95] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697
[96] http://crowdresearchpartners.com/portfolio/insider-threat-report/
[97] 不正権限昇格攻撃(unauthorized privilege escalation Attack)とは、ソフトウェアの実行権限を昇格させてあらゆる攻撃を実行させる攻撃。
http://blogs.mcafee.jp/43-cc7b
DDoS 煙幕攻撃(DDoS diversion attack)とは、本格的な攻撃の煙幕として DDoS 攻撃を利用した攻撃。
https://www.arbornetworks.com/blog/insight/ddos-as-a-smokescreen-for-fraud-and-theft/
[98] https://www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047 pp.7

2017 年 6 月オランダのウェブ・ホスティング・プロバイダーVerelox 社は、元社員により全顧客データを削除され、ほとんどのサーバーの情報を消去され、数日間サービスの停止に追い込まれた。幸い重要なデータは失われておらず、数日後には復旧することができたが、こうした幸運なケースばかりとは限らない。アウトソーシング、在宅勤務やオフショア開発など、ビジネスと勤務形態が多様化し、インターネットへの依存度が高まるにつれ、企業内の情報漏洩の危険性は高まっており、把握は困難になっている。また、情報がクラウド上に保存されるようになり、情報保存のコストが低下したため、データが削除されずに残るようになっていることもリスクを高めている。そして、ダーク・ウェブでの個人情報取引が容易になっていることも懸念材料である。また、悪意がなくとも従業員の不注意からセキュリティの脆弱性が生じることもある[99]。

IBM の 2016 年の調査によれば、すべてのデータ漏洩の 60%はインサイダーによるもので、そのうち 75%は悪意によるもので、25%は過失によるものだった[100]。

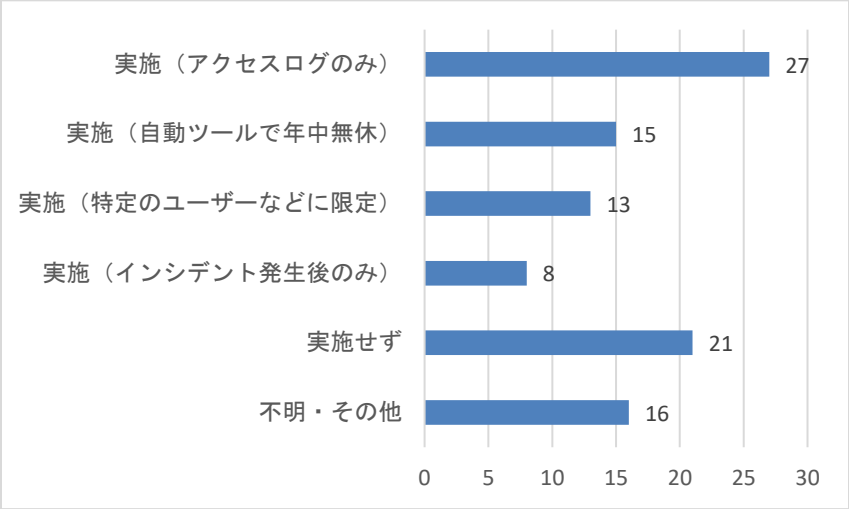
PwC の 2017 年の調査によれば、ハッカーなど外部からのインシデントは微減しているが、サードパーティー（サプライヤー、コンサルタント、コントラクターなど）と従業員によるインシデントは微増の傾向にある。サードパーティーと現在の従業員を合わせたインサイダーによるインシデントは全体の 30%を占めている。その他は、元従業員が 27%、外部のハッカーが 23%を占めている[101]。

また、Accenture の 2016 年の調査によれば、企業のセキュリティ担当者の 69%が、インサイダーによるデータ窃盗を過去 1 年以内に経験している。中でも、その割合は、アジア太平洋地域の企業では 77%、メディア・テクノロジー企業では 80%に上った[102]。

Haystax Technology, "Insider Attacks, Industry Survey[103]"によれば、内部不正による攻撃は、攻撃者がすでにアクセス権を持っている上に、クラウドの利用が増えているなどといった理由があるために、外部からの攻撃よりも検出が難しい。また、内部不正により生じた被害は、50 万ドル以上と推算する企業が 75%に上った。このため、内部不正に対するモニターを多くの企業が実施しており、内部ユーザーの行動を何らかの形でモニタリングしていない企業は 21%に過ぎない。そして、内部不正者に対する対策として、76%が境界防御（Perimeter Defense）[104]ツール、67%がデータベースおよびファイルのモニタリングツール、58%がセキュリティイベントダッシュボードを活用するなどの対策を取っている。内部不正に対する対策における課題としては、訓練や専門性の不足、予算の不足といった問題もあるが、部門・部署間の協力が不十分だとする声も多い。

[99] https://www.csoonline.com/article/3202770/access-control/how-to-spot-and-prevent-insider-threats.html
[100] https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/employees-commit-most-data-breaches.aspx
[101] https://www.pwc.com/us/en/cybersecurity/information-security-survey.html#insight4
https://www.idgenterprise.com/resource/research/2018-global-state-information-security-survey/
[102] https://www.accenture.com/t20160704T014005Z__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf “The State of Cybersecurity and Digital Trust 2016” Accenture and HfS Research、調査対象は 208 名の企業セキュリティ担当者
[103] https://haystax.com/blog/ebook/insider-attacks-industry-survey/
[104] 「境界防御」とは、”「情報」と「権限のない実体（個人、プロセスも含む）」とを分離する機能を持つセキュリティ境界を形成し、「権限のない実体」がもたらす脅威を防御する”という考え方。
http://www.itmedia.co.jp/enterprise/articles/0509/15/news002.html

図表 15：企業内ユーザーの行動モニタリング実施状況（%）



出典：Haystax Technology, "Insider Attacks, Industry Survey[105]"

多くの企業では、内部不正対策として力を入れているのは、アクセス制限・暗号化・ポリシーの徹底などを通じた抑止面であり（61%）、モニタリングや不正侵入検知・防御システム[106]などを活用した検出がそれに続き（49%）、SIEM[107]などを活用した解析（35%）もなされている。ハニーポット[108]といわれるおとりなどを用いている企業も 9%ある。

こうしたインサイダーによるデータ漏洩を防ぐためには、上に挙げたようなセキュリティ・テクノロジー製品・サービスを活用することもできるが、根本的には人に起因する問題である。そこで、以下のような対策が重要になる。

第 1 に、不要なアクセスを防止することである。自動的な管理により、退職した従業員などのアクセスを防止することもできる。ユーザーアカウント管理システムや権限管理手続きの欠如、ネットワークあるいはシステム管理者のアカウントの管理目的以外での使用、権限を付与されていないユーザーへの特別なアクセス許可、ユーザーアクセス権限付与に際しての文書化手続きの欠如、重複しないユーザー名やパスワードポリシー（定期的なパスワード変更など）の徹底不十分といった要因は、すべてセキュリティに対するリスクとなる[109]。

第 2 に、セキュリティ担当だけでなく、人事、法務などの関連部署が協力しあい、問題の対策に当たることである。社内の他部門の事情を把握することは、問題解決の糸口になる。Global Managing Director of Growth and Strategy at Accenture Security の Ryan LaSalle は、まずユーザーの業務を把握し、さらに重要データの所在とアクセス権限付与状況に基づいてリスクの特定と対策を講じた上で、人事・法務・事業部門と協力しあいモニタリングツールと業務の対象を明確にすることが重要だと述べている。セキュリティ部門が他部門と隔絶していると、どんなツールを利用していても、問題を把握することは困難である。

105 https://haystax.com/blog/ebook/insider-attacks-industry-survey/
106 https://it-trend.jp/ids-ips/article/explain
107 Security Information and Event Management の略称。ファイアウォールや IPS などのネットワーク機器、ソフトウェアやアプリケーションが出力するイベント情報を一元的に保管して管理し、脅威となる事象を把握するテクノロジー。
https://www.it-ex.com/focus/techinfo/prepare-cyberattack/detail/vol2.html
108 http://www.atmarkit.co.jp/fsecurity/special/13honey/honey01.html
109 https://www.itgovernance.co.uk/access-control-and-administrative-privilege

第 3 に、あくまで社内の人間が起こした問題だということを忘れないことである。個人的な問題などを把握していれば、事前の対策の可能性も出てくる。金銭的な問題や不満を抱える社員や、他社への転職予定の社員を把握すれば、モニタリングを行うといった対策を講じることもできる[110]。

カーネギーメロン大学の Software Engineering Institute[111]では、内部不正の問題に取り組んでいる。その成果を" Common Sense Guide to Mitigating Insider Threats[112]"としてまとめており、現在第 5 版が公開されている。ここでは、1,000 件以上の実例調査に基づいた内部不正への対策が述べられており、分析の成果は 20 のベストプラクティスとしてまとめられている。このガイドでは、これらのプラクティスの詳細、チェックリスト、関連する社内部署などについて、実践的なガイダンスが述べられている。そして、このプラクティスと、その他のセキュリティに関するガイド（National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4: Recommended Security Controls for Federal Information Systems and Organizations [113] 、CERT® Resilience Management Model [114] 、International Organization for Standardization (ISO) 27002[115]、NITTF Guidelines and Minimum Standards[116]）との対応も示されている。

図表 16：CERT Common Sense Guide ベストプラクティス

1	重要な情報資産を把握して保護する。
2	正式な内部不正対策プログラムを構築する。
3	情報ポリシーと統制を一貫して実施し、明確に文書化する。
4	疑わしい行動や破壊的な行動に対するモニターと対応を、雇用段階から開始する。
5	職場環境における問題を予見し管理する。
6	内部不正者とビジネスパートナーからの脅威を企業全体のリスクマネジメントの観点から考える。
7	ソーシャルメディアに関しては、特に注意が必要である。
8	内部による故意ではない負荷と過ちを最小化するべく、管理と作業を体系化する。
9	悪意の有無に拘わらず内部不正がありうることを、定期セキュリティ研修で全従業員に理解させる。
10	安全なパスワード、アカウント管理のポリシーおよび運用を徹底する。
11	権限を付与されたユーザーに対して、厳格なアクセス制限とモニタリングのポリシーを設定する。
12	従業員の行動をモニタリングし、複数のソースからのデータを関係づけるソリューションを導入する。
13	モバイルデバイスを含め、あらゆるエンドポイントからのリモートアクセスを、監視・制御する。
14	ネットワークおよび従業員の正常な挙動について基準を設ける。
15	業務と最小権限[117]を分離する。
16	特にアクセス制限とモニタリングに関し、すべてのクラウドサービスと明確な契約を定める。
17	システム変更コントロールを制度化する。
18	安全なバックアップと復旧プロセスを実行する。

110 https://www.csoonline.com/article/3202770/access-control/how-to-spot-and-prevent-insider-threats.html
111 https://www.cert.org/insider-threat/
112 https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738
113 https://nvd.nist.gov/800-53
114 https://www.cert.org/resilience/products-services/cert-rmm/
115 https://www.iso.org/standard/54533.html
116 https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf
117「最小権限の原則では、ユーザーにはジョブを実行するための最小限の権限を与えるべきであるとしています。特に組織のライフ・サイクルの初期、従業員が少数で作業を迅速に行う必要がある時期に、責任、役割、権限などを大胆に付与しすぎると、システムが大きく開放され不正使用を招きます。ユーザー権限を定期的にレビューして、現在のジョブの責任に対して妥当であることを確認する必要があります。」 Oracle® Linux セキュリティ・ガイド リリース 6、1.1.3 最小権限の原則の順守
https://docs.oracle.com/cd/E39368_01/b72804/ol_lpriv_sec.html

19	承認を受けずにデータを一括して持ち出すことを認めない。
20	明確な雇用打ち切り手続きを設定する。

出典:" Common Sense Guide to Mitigating Insider Threats" version 5, pp. xii [118]

こうした従業員のモニタリングは、行き過ぎれば従業員のプライバシーを侵害することになりかねない。EU では、2017 年 9 月 5 日、欧州人権裁判所(European Court of Human Rights)[119]が、企業が従業員の電子メールをモニタリングするには、事前の通告が必要であるとする判決を下した[120]。一方で、組織の利益に適った行動を奨励するポジティブなインセンティブも組み合わせて、バランスの取れた対応を考える必要もあるのではないかという考え方も提唱されている[121]。

(3) 米国における情報共有組織への参加

a. Information Sharing and Analysis Center(ISAC)

米国 Information Sharing and Analysis Center(ISAC、アイザック)は、重要インフラ所有者および運営者が、サイバー攻撃などの脅威から、施設・職員・顧客を守ることを支援するための業界別 NPO である。ISAC では、脅威に関する情報を収集・分析し、会員に広めると共に、リスクを緩和し、レジリエンシー[122]を向上させるツールを提供する。

ISAC のコンセプトは、1998 年 5 月 22 日の大統領決定指令第 63 号(Presidential Decision Directive-63、PDD-63)[123]によって導入され、以降、連邦政府は各重要インフラ関係セクターに対し、セクター毎にサイバー攻撃に関する情報やベストプラクティスを共有するための組織の設置を求めてきた。ISAC の設置は 1999 年から始まり、約 10 年でほとんどのセクターで団体が設立された。そして、セクター毎に重要情報の共有を図り、業界としての状況把握を進めてきた。ほとんどの ISAC では、休みなくいつでも警告とインシデントの発生やセクターの警戒レベル設定を通知できる体制を取っており、政府側よりも迅速な対応を取れる ISAC も多い[124]。例えば、2016 年に参加した Auto-ISAC のメンバーは、北米の軽自動車の 99%をカバーし、加盟メンバーは 3 大陸の 7 ヶ国に広がっている[125]。多くのセクターでは、90%を超える浸透度に達している[126]。

b. National Council of ISACs(NCI)

これら ISAC の間の連携を図るために、National Council of ISACs(NCI)が 2003 年に設置された。メンバーとなっているのは、以下の ISAC である。NCI は、セクター間の情報共有と、官民を交えて ISAC の対応戦略を進める場となっている。有事の際には、連邦政府関連機関との連携を即時に取れる態勢が敷かれている。

[118] https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738
[119] http://www.echr.coe.int/Pages/home.aspx?p=home
[120] http://www.echr.coe.int/Documents/Press_Q_A_Barbulescu_ENG.PDF
https://www.nytimes.com/2017/09/05/business/european-court-employers-workers-email.html
[121] https://www.sei.cmu.edu/podcasts/podcast_episode.cfm?episodeid=509052
[122] サイバー攻撃などの事業停止に追い込まれかねない事態に対し、影響を抑え、事業を継続する能力
[123] https://www.hsdl.org/?abstract&did=3544
[124] https://www.nationalisacs.org/about-isacs
[125] https://www.automotiveisac.com/
[126] http://ctin.us/site/isaos/

図表 17：National Council of ISACs メンバーISAC

Automotive ISAC	Aviation ISAC	Communications ISAC
Defense Industry base ISAC	Defense Security Information Exchange	Downstream Natural Gas ISAC
Electricity ISAC	Emergency Management and Response ISAC	Financial Services ISAC
Healthcare Ready	Information Technology ISAC	Maritime ISAC
Multi-State ISAC	National Health ISAC	Oil & Natural Gas ISAC
Real Estate ISAC	Research & Education Network ISAC	Retail Cyber Intelligence Sharing Center
Supply Chain ISAC	Surface Transportation, Public Transportation and Over-the-Road Bus ISAC	Water ISAC

出典：NCI ホームページ[127]

c. Information Sharing and Analysis Organization（ISAO）

サイバー攻撃の脅威に備えるため、従来の重要インフラ分野に留まらず、一般の民間部門でも情報共有を広く進めるための組織が必要になっていることから、2015 年にオバマ政権は Executive Order（大統領令）13691[128]を発し、国土安全保障省（Department of Homeland Security、DHS）に対し、Information Sharing and Analysis Organization（ISAO）の推進を命じた[129]。

重要インフラ分野で設置された従来の ISAC は、いわばセクター別の ISAO であり、新たに設立される ISAO とも連携を進め、情報共有ネットワークの拡大を推進している[130]。ISAO は、非営利のコミュニティ、会員団体、顧客やパートナーとの情報共有を進める単一の企業であっても良い。

さらに、2015 年 10 月、国土安全保障省は、テキサス大学サンアントニオ校を中心に、非営利コンサルタント Logistics Management Institute（LMI）[131]と、小売業・消費者製品およびサービス業を対象としたサイバーセキュリティコミュニティである retail Cyber Intelligence Sharing Center（R-CISC）[132]の協力を得たチームを、非政府団体として Information Sharing and Analysis Organization Standards Organization（ISAO SO）に選定した。ISAO SO は、重要インフラ分野の所有者・運営者・既存情報共有組織、関連組織、官民の関係者と協力しあい、任意での合意形成プロセスを通じて、ISAO 設立・運営に関する任意での標準およびガイドライン設定に当たっている[133]。

その結果、2016 年度には、ISAO SO への登録 ISAO は 17、登録 ISAC は 24、その他の登録サイバー情報共有組織は 6、サイバー情報共有組織を持つ州は 13 に達した。Sports ISO は 2016 年リオデジャネイロ

127 https://www.nationalisacs.org/member-isacs
128 https://www.gpo.gov/fdsys/search/pagedetails.action?collectionCode=CFR&browsePath=Title+3%2FSubjgrp%2FOrder+13691&granuleId=CFR-2016-title3-vol1-eo13691&packageId=CFR-2016-title3-vol1&collapse=true&fromBrowse=true
129 https://www.dhs.gov/isao
130 https://www.dhs.gov/isao-faq
131 http://www.lmi.org/en/Home
132 https://r-cisc.org/
133 https://www.isao.org/about/

夏季オリンピックの運営に協力するなど、ISAO はサイバーセキュリティの推進に大きな成果を挙げている[134]。

しかし、企業や各種団体は、サイバーインシデントに関する情報共有に必ずしも積極的ではない。この状況を打開するために、2014 年には Cyber Information Sharing Tax Credit Act が Kirsten E. Gillibrand 上院議員（民主党、ニューヨーク州選出）によって提出された。これは、ISAO への参加に対して、税制優遇措置を与えるというものだったが、成立には至っていない[135]。また、2017 年 9 月に開催された Healthcare Security Forum[136]で、前国土安全保障庁官 Tom Ridge 氏は、金融セクターでは 9000 社が ISAO に参加していることを成功事例として挙げ、ヘルスケア業界では ISAC 参加メンバーが 200 に過ぎないことへの懸念を示し、業界としての ISAC への取り組みを求めた[137]。

5 今後の展望と日本への示唆

2017 年は、Equifax 社や Verizon 社といった企業へのハッキング、WannaCry の猛威といったデータ漏洩や新たなサイバー攻撃に見舞われた年だった。McAfee 社は、”McAfee Labs 2018 Threats Predictions Report”として、2018 年に向けて、以下の 5 点について警告している。併せて、2018 年 5 月に施行が予定されている EU の GDPR（General Data Protection Regulation）は、消費者のデータやユーザーが作り出すコンテンツの扱いについての基本的なルールを形成し得るとしている[138]。

- *サイバー攻撃の攻撃側と防御側の間で敵対的機械学習[139]による「兵器競争」が進む*
  競争に勝つには、人間の知性を結集させて、機器を活用した判断と組織化された反応を効果的に強化する必要がある。
- *ランサムウェア攻撃が PC 乗っ取りから IoT、裕福層、企業破壊に広がる*
  新たな様々なサイバー犯罪の「ビジネスモデル」が生み出されるとともにサイバー保険市場が拡大をするだろう。また、誰にでも簡単に使える疑似的なランサムウェアが国家、政治、ビジネスのライバルを叩きのめしたい者に売られていく。
- *サーバーレスアプリケーション[140]によりアプリ依存、データ転送等を狙った攻撃機会が増える*
  機能整備に必要なセキュリティプロセスが含まれ、拡張性が確保まれ、トラフィックが VPN（バーチャル・プライベート・ネットワーク）または暗号化により適切に守られることが必要である。
- *コネクテッド家電により家庭が企業の店先となり消費者プライバシーがさらされる*
  消費者はプライバシーに関する合意事項をほとんど読まないから、企業はデバイスやサービスが提供された後にそれを頻繁に変更しようとするだろう。法を破り、罰金を払い、それを繰り返して利益を上げていく企業に対する規制が求められるだろう。
- *子供たちが作り出すデジタル・コンテンツを収集する企業は長期的に風評リスクを負う*

---

[134] https://www.isao.org/wp-content/uploads/2017/01/isao-so-2016-year-in-review.pdf
[135] https://www.congress.gov/bill/113th-congress/senate-bill/2717
https://www.threatconnect.com/blog/isac-isao-financial-incentives-for-sharing-threat-intelligence-emerge/
[136] http://www.healthcaresecurityforum.com/boston/2017
[137] http://www.healthcareitnews.com/news/why-hospitals-should-join-isac-immediately
[138] https://www.businesswire.com/news/home/20171129005305/en/McAfee-Labs-Previews-Cybersecurity-Trends-2018
[139]スパムメールの検出や、アクセスログを利用したネットワークからの侵入検出に機械学習技術が利用されている。すると、送信や侵入を企てる敵対者 (adversary) は，意図的に入力パターンを変更して、検出を回避しようとする。こうした敵対的な環境下での利用を想定した機械学習の研究は、敵対的学習 (adversarial learning) や 敵対的環境下での機械学習 (machine learning in adversarial environments) と呼ばれる。
http://ibisforest.org/index.php?%E6%95%B5%E5%AF%BE%E7%9A%84%E5%AD%A6%E7%BF%92
[140] サーバーを自前で用意せず、マネージドサービスを活用してシステムを構築する Amazon Web Service に代表されるアーキテクチャー。
https://qiita.com/kotauchisunsun/items/7b39e698fd5cba97da15

2018 年、親たちは子供たちが作り出したデジタルコンテンツの著しい乱用に気づき、それが長期間続くと考えるだろう。アプリやサービスを提供する企業の多くが親たちの教育パートナーになることの価値を認識するだろう。

Global Cybersecurity Index 2017 によれば、国連加盟 193 ヵ国のうち、日本のサイバーセキュリティ対策状況は 11 位（12 番目）である（1 位シンガポール、2 位米国、3 位マレーシア）[141]。他方、2015 年の日本の民間部門の生産性は G7 の中で最低であり[142]、サイバーセキュリティの改善がこれを変え得るとの声もある[143]。

2017 年 10 月に慶應義塾大学で開催された Cyber3 Conference Tokyo 2017 では、東京 2020 オリンピック・パラリンピックを契機とした将来のサイバーセキュリティのあるべき姿に向けて、以下が提議されている。[144]。

- *Society5.0（IoT 等のテクノロジーでサイバー空間と物理空間が高度に融合される超スマート社会）を実現するためには、様々なデジタルトランスフォーメーションを推進するとともに、それに伴うセキュリティに係る組織的な対応を強化する必要がある。*
- *サイバーリスクが拡大しており、サイバー攻撃に企業単独で対応することには限界がある。特に中小企業ではサイバーセキュリティの専門家を採用することは難しいため、政府の積極的な支援のもと、産学官が一体となった対応を図る必要がある。*
- *更なる高度なサイバー攻撃を受ける可能性もあるため、攻撃者の動機・意図の分析結果に基づくプロアクティブな対抗策の検討・共有に向けた脅威情報管理の取組や事業継続計画（BCP）等を考慮した組織としてのレジリエンスを考える必要がある。*
- *サイバーセキュリティにはリーダーシップの発揮と情報共有の仕組が求められる。Cyber3 の議論を通して、今後の取組へ繋げていくことが重要である。*

加えて、『日本ではリスクゼロが良いとする文化があるが、サイバーセキュリティにおいては、ゼロリスクということはあり得ない。セキュリティインシデントを防ぐことは当然重要であるが、その後の対策展開、さらにその共有こそがより重要である。』との指摘がなされている[145]。

今回取り上げた様々な対策及びその他の対策を駆使し、世界全体でのサイバーセキュリティ認知度の向上、サイバー攻撃への対応能力（被害防止、リスクマネジメント）の向上、情報共有、人材教育・育成が重要であると考えられる（特に、米国はビジネスセクターーパブリックセクター間の人材流動が強みとの声がある。）。

※ 本レポートは、注記した参考資料等を利用して作成しているものであり、本レポートの内容に関しては、その有用性、正確性、知的財産権の不侵害等の一切について、執筆者及び執筆者が所属する組織が如何なる保証をするものでもありません。また、本レポートの読者が、本レポート内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。

141 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
142 http://www.oecd.org/newsroom/continued-slowdown-in-productivity-growth-weighs-down-on-living-standards.htm
143 http://ewn.co.za/2017/11/29/this-is-how-to-prepare-for-a-cyber-attack
144 http://www.npr-event.jp/cyber3/en/Cyber3-2017-FinalReport-JA.pdf
145 http://www.npr-event.jp/cyber3/en/Cyber3-2017-FinalReport-JA.pdf