第371回NRIメディアフォーラム

生成AI時代、企業に求められる「試す勇気」

企業における情報セキュリティ実態調査2023

セキュリティコンサルタント　松本 彩花

NRIセキュアテクノロジーズ株式会社
DXセキュリティプラットフォーム事業本部
GRCプラットフォーム部

2024年3月7日

Envision the value,
Empower the change

01 調査概要

02 調査結果

1. セキュリティマネジメント
2. サプライチェーン
3. セキュリティ対策
4. 生成AI

03 総括

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

01. 調査概要

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

日本／アメリカ／オーストラリアの企業における情報セキュリティ実態調査

目的

- 日本／アメリカ／オーストラリアの企業における、情報セキュリティに対する取り組みを明らかにする
- 企業の情報システム／情報セキュリティ関連業務に携わる方に、有益な参考情報を提供する

調査期間

- 日本　：2023年8月1日～2023年9月29日
- アメリカ／オーストラリア　：2023年9月8日～2023年9月29日

調査方法

- Webによるアンケート

調査対象

- 企業の情報システム・情報セキュリティ担当者

回答数

- 日本　：1,657社
- アメリカ　：540社
- オーストラリア　：586社

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

回答企業の内訳

■ 従業員規模

■ 業種

Copyright (C) Nomura Research Institute, Ltd. All rights reserved.

4 つのテーマについて調査を実施｜エグゼクティブサマリ

セキュリティマネジメント

ソリューションの導入状況

JP n=1,657

前年度比 +8.9pt

	EDR※1	NDR※1	XDR※1
対応実施済み	27.8%	11.9%	6.5%
検討・検証中	34.3%	41.1%	36.6%

セキュリティ対策

DMARC 実施率

JP n=1,657

未対応・わからない率 約74%　検討中 約13%　実施済み※2 13%

生成AI

生成AIの導入状況

	導入済み	検討中	利用禁止／不要のため未導入
JP n=1,657	18.0%	30.6%	51.4%
US n=540	73.5%	24.3%	2.2%
AU n=586	66.2%	30.3%	3.4%

※1 E = Endpoint、N = Network、X = EXtended / DR = Detection and Response
※2 None (なにもしない)、Quarantine (検疫)、Reject (拒否)のいずれかを実施している回答割合

サプライチェーン

経済安全保障推進法に関連し、セキュリティの強化を意識している割合

JP n=1,657

39.6%

サプライチェーンのセキュリティ統制状況

JP n=1,657

国内関係会社に対して対策状況を把握している 47.1% ＞ 国内委託先に対して対策状況を把握している 35.6%

SBOM※3を利用中／検証中と回答した企業の割合

JP n=1,657	US n=540	AU n=586
3.2%	82.1%	77.4%

※3 Software Bill of Materials（ソフトウェア部品表）

Copyright (C) Nomura Research Institute, Ltd. All rights reserved.

02. 調査結果｜セキュリティマネジメント

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

セキュリティ対策の新しいソリューションの導入状況

- サイバー攻撃・被害の増加やテレワークの浸透などを背景にEDRの導入が進展
- EDRの導入が進むほど、運用の高度化および負荷軽減のためにXDRの注目が高まる

ソリューションの導入状況

JP　n=1,657

			導入済み、検証中または検討中	導入済み・利用している	検証している／していた	検討中・関心がある	未検討・関心がない	知らない
1位	EDR	遠隔での端末内潜伏脅威探索(スレットハンティング)とNW隔離、フォレンジック対応	62.0%	27.8%	10.6	23.7%	23.4%	14.6
2位	NDR	組織内のネットワーク上の通信内容の監視・脅威検出	53.0%	11.9	9.1	32.0%	28.3%	18.6
3位	CASB	クラウド利用の可視化・制御	44.6%	6.7	7.9	30.0%	32.7%	22.7%
4位	XDR	複数のセキュリティレイヤーにわたる一元的な脅威の検知、調査、対応	43.1%	6.5	8.2	28.4%	34.1%	22.8%
5位	IDaaS	クラウド型ID・アクセス管理	40.8%	8.3	7.4	25.1%	35.2%	24.0%
6位	SOAR	セキュリティアラート等への対応自動化	39.1%	5.3	5.2	28.6%	35.6%	25.3%
7位	UEBA	ユーザ行動に関わるログの統合分析とアラート	37.0%	8.4	5.2	23.4	35.7%	27.3%
8位	CSPM	クラウドセキュリティ態勢管理	31.3%	3.1	3.9	24.3	39.9%	28.8%
9位	SSPM	SaaSのセキュリティ態勢管理	29.1%	1.8	4.1	23.2	41.2%	29.8%
10位	TLPT	脅威ベースのペネトレーションテスト	27.3%	4.5	4.0	18.8	43.0%	29.7%
11位	VRM	ベンダーリスクの継続的な管理	22.3%	1.6	2.5	18.2	48.1%	29.6%

■導入済み・利用している　■検証している／していた　■検討中・関心がある　■未検討・関心がない　■知らない

Copyright (C) Nomura Research Institute, Ltd. All rights reserved.

セキュリティの専門人材

- 日本のCISO設置割合は約4割であるが、従業員規模が多いほどに割合は増加傾向
- 未設置の企業は、CISOとして一人だけを任命しようとせず、CISOをチームとして立ち上げ、時間をかけて整備・強化する発想が望まれる

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

02. 調査結果｜サプライチェーン

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

経済安全保障推進法への意識

- 日本企業の約 4 割が経済安全保障推進法を意識している
- 特定社会基盤事業者ほど、経済安全保障推進法への関心が高い

経済安全保障推進法に関連して、サイバーを含むセキュリティの強化を意識している割合

JP n=1,657

強く意識している／意識していると回答した割合 ※1

全体 39.6%（n=1,657社）

特定社会基盤事業者 ※2	特定社会基盤事業者を除く
88.2%（n=17社）※3	39.0%（n=1,640社）

※1 日本企業に対するアンケートは、2023/8/1-2023/9/29 の期間で実施

※2 経済安全保障推進法に基づき特定社会基盤事業者の対象として指定された210の事業者

※3 サンプル数が少ないので参考値

Copyright (C) Nomura Research Institute, Ltd. All rights reserved.

経済安全保障推進法を受けて強化した対策

- 経済安全保障推進法を受けた対策の1位は「委託先／取引先等の審査プロセス」
- 「不正なプログラム／機能の組み込み防止」の想定対策にはバラつきがあると推察

経済安全保障推進法を受けて、強化ないし新規導入したサプライチェーンリスク対策

※ 経済安全保障推進法に関連して、セキュリティの強化を強く意識している／意識していると回答した企業のみ対象

JP n=655

Copyright (C) Nomura Research Institute, Ltd. All rights reserved.

サプライチェーン統制状況

■ グループ会社数や従業員数が大きいほど、サプライチェーン統制が進んでいる

■ 委託先への統制は、対象数の多さやつながりの複雑さなどの難しい課題が存在する

国内関係会社／グループ会社の統制状況

JP n=1,657

国内パートナー／委託先の統制状況

JP n=1,657

■ セキュリティ対策状況が改善されていることを定期的に確認している
■ セキュリティ対策状況を把握し、自社の水準をみたすため改善を要求している
■ セキュリティ対策状況を把握している
■ セキュリティ対策状況を把握していない
■ 該当なし

Copyright (C) Nomura Research Institute, Ltd. All rights reserved.

サプライチェーンにおけるセキュリティ課題

■ 脅威の高まりや経済安保の流れで、サプライチェーン周辺の人材不足感は高まる

■ セキュリティ対応の初手は対象の把握だが、約3~4割の企業が課題と感じている

サプライチェーンに対するセキュリティ対応における課題

JP グループ会社規模別

※ 複数選択可
※ グループ会社数が0社の企業を除く
※ 他選択肢：取引先や委託先からセキュリティ対応の理解・協力を得られない／アンケートでセキュリティ対策状況を確認しているが、確認内容を更新できていない／その他（具体的に記載）

	1社～10社未満 n=989	10社～100社未満 n=322	100社以上 n=50
1位	33.6% セキュリティ対応のリソースが自社向けで手一杯	42.9% セキュリティ対応のリソースが自社向けで手一杯	36.0% サプライチェーンの対象数（拠点や取引先）が多い
2位	27.8% サプライチェーンとして管理すべき対象の全体像を把握できていない	36.3% サプライチェーンとして管理すべき対象の全体像を把握できていない	34.0% セキュリティ対応のリソースが自社向けで手一杯
3位	27.6% 特になし	32.0% サプライチェーンの対象数（拠点や取引先）が多い	32.0% サプライチェーンとして管理すべき対象の全体像を把握できていない
4位	26.8% 何から手をつければよいか分からない	31.7% サプライチェーン管理向けのセキュリティ予算を確保できない（本社・自社向けの対策予算がメイン）	26.0% サプライチェーン管理向けのセキュリティ予算を確保できない（本社・自社向けの対策予算がメイン）
5位	23.7% サプライチェーン管理向けのセキュリティ予算を確保できない (本社・自社向けの対策予算がメイン)	23.9% 何から手をつければよいか分からない	24.0% 特になし
6位	18.5% サプライチェーンの対象数（拠点や取引先）が多い	19.3% 特になし	20.0% アンケートでセキュリティ対策状況を確認しているが、実効性の観点で不安がある
7位	14.2% アンケートでセキュリティ対策状況を確認しているが、実効性の観点で不安がある	15.8% アンケートでセキュリティ対策状況を確認しているが、実効性の観点で不安がある	18.0% 何から手をつければよいか分からない

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

02. 調査結果｜セキュリティ対策

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

DMARC（ドメイン詐称対策）

解説

■ 偽装メール対策であるDMARCは、政府のセキュリティ統一基準に明記されたことをきっかけに注目が高まっている

DMARC (Domain-based Message Authentication, Reporting and Conformance)

DMARCポリシー

Reject（拒否）
DMARC認証に失敗したメールを拒否するよう求めるポリシー

Quarantine（検疫）
DMARC認証に失敗したメールを疑わしいメールとして扱うよう求めるポリシー

None（何もしない）
DMARC認証に失敗したメールでも受け入れ、監視のみするポリシー

- DMARCとは、メールに表示された送信元（ヘッダーFrom）ドメインから正規に送信されたメールであるかどうかを認証する、送信ドメイン認証技術であり、自社ドメインを偽装したメールから受信者を保護する。
- ヘッダーFromのドメインによってSPFまたは DKIMの認証に成功した場合、DMARCの認証成功となる。DMARCでは認証に失敗した場合のメールの扱いを、送信ドメイン所有者側がReject（拒否）、Quarantine（検疫）、None（何もしない）のいずれかに指定することができる。また、送信ドメイン所有者側はDMARCの判定結果についての情報をレポートとして受け取り、可視化することができます。
- 2023年度に改定された政府のセキュリティ統一基準に、偽装メール対策としてDMARCが明記されたことを理由に注目が高まっており、今後、日本でも導入が進むと予想される。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

DMARC・BIMIの実施状況

- 米豪のDMARC導入割合が高い理由は、国家機関でDMARC実施が義務付けられ、導入に関するガイドラインが公表されるなど、DMARC実施が推奨されていることが考えられる
- 日本ではDMARCの実施が求められる機会が増加しており、今後の導入が進むと予想
- DMARC対応の成熟には時間がかかるので、早期着手と中長期的な推進が望ましい
- BIMI導入には、DMARCポリシーがQuarantine／Rejectである必要。前提条件が整っていないため、必然的に日本ではBIMI対応も進んでいない

DMARCの実施・検討状況

BIMI※の実施・検討状況

※ Brand Indicators for Message Identification

Copyright (C) Nomura Research Institute, Ltd. All rights reserved.

02. 調査結果｜生成AI

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

生成AIの導入状況

- 日本ではルールを整備した上で、生成AIを導入する方針の企業が多い
- 日本と米豪では、新しい技術の導入とルール整備に対する優先度の違いがうかがえる

生成AIのルール整備と導入状況

Copyright (C) Nomura Research Institute, Ltd. All rights reserved.

生成AI利用に関するセキュリティルール

- 日本では、生成AI利用における機密情報入力に対する警戒が大きい
- 今後は、生成AIの利用状況の監視・分析を行うなどのシステム的な統制が必要

整備済み・整備予定の生成AIサービスの利用に関するセキュリティルール

※ セキュリティルールを整備・整備予定と回答した企業のみ対象　※ 複数選択可

Copyright (C)　Nomura Research Institute, Ltd. All rights reserved.

03. 総括

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

長年続くセキュリティ人材不足の影響が色濃くみられる

セキュリティマネジメント

テレワーク浸透等によるEDRの導入が進む
とともに、XDRへ注目が集まる

サプライチェーン

経済安全保障推進法を受けてサプライチェーン
リスクへの意識は高まっているが、
複雑さや人材不足など課題が多い

セキュリティ対策

日本でのDMARC実施は遅れているが、
Googleの「メール送信者のガイドライン」などの
影響を受け、普及が進むと予想

生成AI

日本では生成AIの導入に対して
慎重な方針の企業が多い

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

生成AIなどの新しい技術は、ネガティブリスクだけでなく、ポジティブリスクを捉えることが重要
「禁止」・「不要」と決めつけるのではなく、少しずつ試しながら取り入れる姿勢が望まれる

ネガティブリスクを気にしすぎて、成長機会を喪失

- 生成AIという新技術が台頭
- 機密情報の漏えいや法令違反などに過度に反応
- 最初から高い目標を設定することで「まずは禁止」「自社には不要」と判断してしまう
- 結果として、新技術の恩恵や従業員の成長を阻害

ポジティブリスクの姿勢で、新技術を試しながら前進

- 生成AIという新技術が台頭
- ポジティブとネガティブ、双方のリスクをバランスよく捉える
- アジャイルの発想で、小さな目標を立て、少しずつ試しながら経験や自信を養っていく（適度にリスクを取る）
- 結果として、組織の生成AIの経験値が増し、ビジネス活用へ

新技術を試しながら取り入れる文化・成功体験が浸透

提言 生成AI時代の企業リーダーには、新技術を自社の成長機会と捉え、ネガティブリスクとバランシングするアクションが必要

注）リスクとは発生が不確実な事象または状態、ポジティブリスクとはプラスに働くリスク（好機）を指す

Copyright (C) Nomura Research Institute, Ltd. All rights reserved.

ご参考

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

経済安全保障推進法と「第2の柱」が求める要請事項

解説

■ 2022年5月公布の「経済安全保障推進法」には4つの柱があり、第2の柱である「特定社会基盤役務の安定的な提供の確保」に際して、事前審査が必要となる

経済安全保障推進法における4つの柱

- 第1の柱　重要物資の安定的な供給の確保に関する制度
- 第2の柱　特定社会基盤役務の安定的な提供の確保に関する制度
- 第3の柱　先端的な重要技術の開発支援に関する制度
- 第4の柱　特許出願の非公開に関する制度

▼ 公布（2022年5月18日）

▼ 施行（2022年8月1日）

1年6ヶ月以内 → ▼ 施行1 審査対象の指定（2023年11月17日）
→ 14業種から一定の規模を超える210事業者が指定

1年9ヶ月以内 → ▼ 施行2 審査・勧告・命令（2024年春頃）
→ 審査対象の指定から6ヶ月間の経過措置有

▼ 施行（2022年8月1日）

2年以内

第2の柱の要請事項

だれが	特定社会基盤事業者は、
どんな時に	特定社会基盤事業に関する役務の提供に際して、特定重要設備の導入及び重要維持管理等の委託を行う場合は、
なにを	事業所管大臣が行う**事前審査**を受けなければならない

事前審査の位置づけと考慮要素

事業所管大臣が、導入等計画書に関する特定重要設備が特定妨害行為の手段として使用される恐れが大きいかどうかを審査することを指す。

- 供給者・維持管理委託先が、**外部にある主体から強い影響**をうけているか
- リスクに関する評価を自ら行い、結果に応じた**リスク管理措置**を講じているか
- 構成設備に脆弱性を指摘された例、**維持管理に対して不適切性が指摘**された例、供給者・維持管理委託先が、国際的な基準、国内の**法令の不遵守が指摘**された例
- その他、**同盟国・同志国の制裁リスト**に含まれていないか

※内閣府『経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）』
https://www.cao.go.jp/keizai_anzen_hosho/を基にNRIセキュアが作成

Copyright (C)　Nomura Research Institute, Ltd. All rights reserved.

用語解説

用語	正式名称	解説
EDR	Endpoint Detection and Response	遠隔での端末内潜伏脅威探索(スレットハンティング)とNW隔離、フォレンジック対応を行う技術・製品
NDR	Network Detection and Response	組織内のネットワーク上の通信内容の監視・脅威検出を行う技術・製品
CASB	Cloud Access Security Broker	クラウド利用の可視化・制御を行う技術・製品
XDR	Extended detection and response	複数のセキュリティレイヤーにわたる一元的な脅威の検知、調査、対応を行う技術・製品
IDaaS	Identity as a Service	クラウド型ID・アクセス管理を行う技術・製品
SOAR	Security Orchestration, Automation and Response	セキュリティアラート等への対応自動化を行う技術・製品
UEBA	User and Entity Behavior Analytics	ユーザ行動に関わるログの統合分析とアラートを行う技術・製品
CSPM	Cloud Security Posture Management	クラウドセキュリティ態勢管理を行う技術・製品
SSPM	SaaS Security Posture Management	SaaSのセキュリティ態勢管理を行う技術・製品
TLPT	Threat Led Penetration Test	脅威ベースのペネトレーションテスト
VRM	Vendor Risk Management	ベンダーリスクの継続的な管理を行う技術・製品
CISO	Chief Information Security Officer	情報セキュリティ統括者
DMARC	Domain-based Message Authentication, Reporting and Conformance	メールに表示された送信元（ヘッダーFrom）ドメインから正規に送信されたメールであるかどうかを認証する、送信ドメイン認証技術
BIMI	Brand Indicators for Message Identification	DMARCで認証成功したメールにロゴを表示させる送信ドメイン認証技術
アジャイル	-	アジャイルおよびアジャイル開発とは、小さな単位で動くソフトウエアを作っていく考え方、あるいは、その方法論

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

Envision the value,
Empower the change