HITACHI
Inspire the Next

IronNet

ネットワーク脅威検知ソリューション

ご説明資料

株式会社 日立ソリューションズ・クリエイト

HITACHI
Inspire the Next

Contents

HITACHI
Inspire the Next

１．はじめに

1. はじめに

近年、**標的型サイバー攻撃による情報漏えい/情報破壊/不正侵入**などの事案が国内においても報道されています。

また、サイバー攻撃の高度化による運用負荷の増加、IoTなどのデジタルトランスフォーメーションなどによりセキュリティのカバーエリアが拡大して、**セキュリティ要員の負担増加、要員不足が深刻化**しています。

当社はそのような課題を解決するため、潜在的脅威の検知と集団防衛を支援するIronNet Cybersecurity, Inc.（以下、IronNet社）のセキュリティ製品「IronDefense®」「IronDome®」を活用した「ネットワーク脅威検知ソリューション」を提供します。

HITACHI
Inspire the Next

2. 情報セキュリティ10大脅威2021

2. 情報セキュリティ10大脅威2021

HITACHI
Inspire the Next

情報セキュリティ10大脅威2021では、「標的型攻撃による機密情報の窃取」「サプライチェーンの弱点を悪用した攻撃」「内部不正による情報漏えい」などがランクインしています。近年サイバー攻撃が巧妙化し、脅威がビジネスに与えるインパクトが大きくなっています。情報漏えいや、ランサムウェア被害などにより企業の事業継続が困難になり、膨大な対策費用が必要です。

被害事例

取引先を装ったメールの添付ファイルを開いたことで、PCがEmotetに感染。感染に気づかず当該PCからさらに組織内外へウイルスメールが送信され、他の従業員が当該メールの添付ファイルを開いたことで感染が広がり、業務停止、情報流出などに発展しました。

10大脅威(2021年)			
1位	ランサムウェアによる被害	6位	内部不正による情報漏えい
2位	標的型攻撃による機密情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止
3位	テレワーク等のニューノーマルな働き方を狙った攻撃	8位	インターネット上のサービスへの不正ログイン
4位	サプライチェーンの弱点を悪用した攻撃	9位	不注意による情報漏えい等の被害
5位	ビジネスメール詐欺による金銭被害	10位	脆弱性対策情報の公開に伴う悪用増加

出典：IPA 『情報セキュリティ −10大脅威2021-』から

3. サイバー攻撃による経営リスク

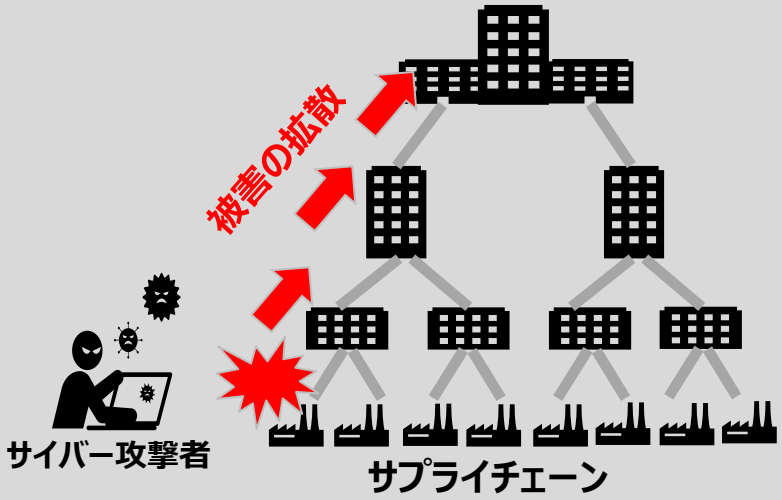
3. サイバー攻撃による経営リスク

HITACHI
Inspire the Next

標的型攻撃などのサイバー攻撃による経営リスク（課題）

- **事業の存続/機会損失**
- **損害賠償**
- **社会的な信用失墜**
- **サプライチェーンへの影響（サプライチェーン攻撃）**

などが挙げられ、これらは経営層にとって深刻な問題です。
経営層がリーダーシップをとってサイバーセキュリティ対策へ投資する必要があります。



セキュリティ事故の被害金額は
平均2,500万円※！
サプライチェーン攻撃では、被害が拡散し
さらに被害金額は拡大していきます。

企業横断（集団）でのセキュリティ対策への取り組みが必要です。

本ソリューションでは、既存のセキュリティ対策に加えて、さらにセキュリティ強化を行い、経営リスクを低減します。

※当社独自調査（2021年2月）
年商規模100億円以上の製造業勤務　かつ、「工場内ITセキュリティ」の現状や課題について、「多少～よく知っている」と回答したWebアンケート登録者1,000名に対し、調査を実施

HITACHI
Inspire the Next

4. ソリューション内容

４－１．ソリューションが解決する課題

４－２．ユースケース（今まで）

４－３．ユースケース（これから）

４－４．ソリューション導入による効果

4-1. ソリューションが解決する課題

HITACHI
Inspire the Next

お客さまのシステムにおいて、このようなお悩みはありませんか？

課題	解決
サイバー攻撃に気づくのが遅れて被害拡大の懸念がある。	ネットワーク通信を監視し、予兆検知による早期警戒と脅威の可視化を実現
巧妙化する脅威に対して、セキュリティ対策を手軽に導入したい。	FWやエンドポイントセキュリティの導入に比べて、 既存ネットワークへの影響なく、導入が可能 ※既存導入のセキュリティ対策製品と併用することで さらに高度なセキュリティ対策を実現
セキュリティ担当者の負荷が増加しているので、セキュリティ対策を支援してほしい。	予兆検知された脅威に対して、お客さまのセキュリティ担当者と連携して対策を支援
他社で見つかったセキュリティ関連の脅威に対して、いち早く対策したい。	業界やグループ企業などの間で脅威情報を共有することで、集団でセキュリティ対策が可能

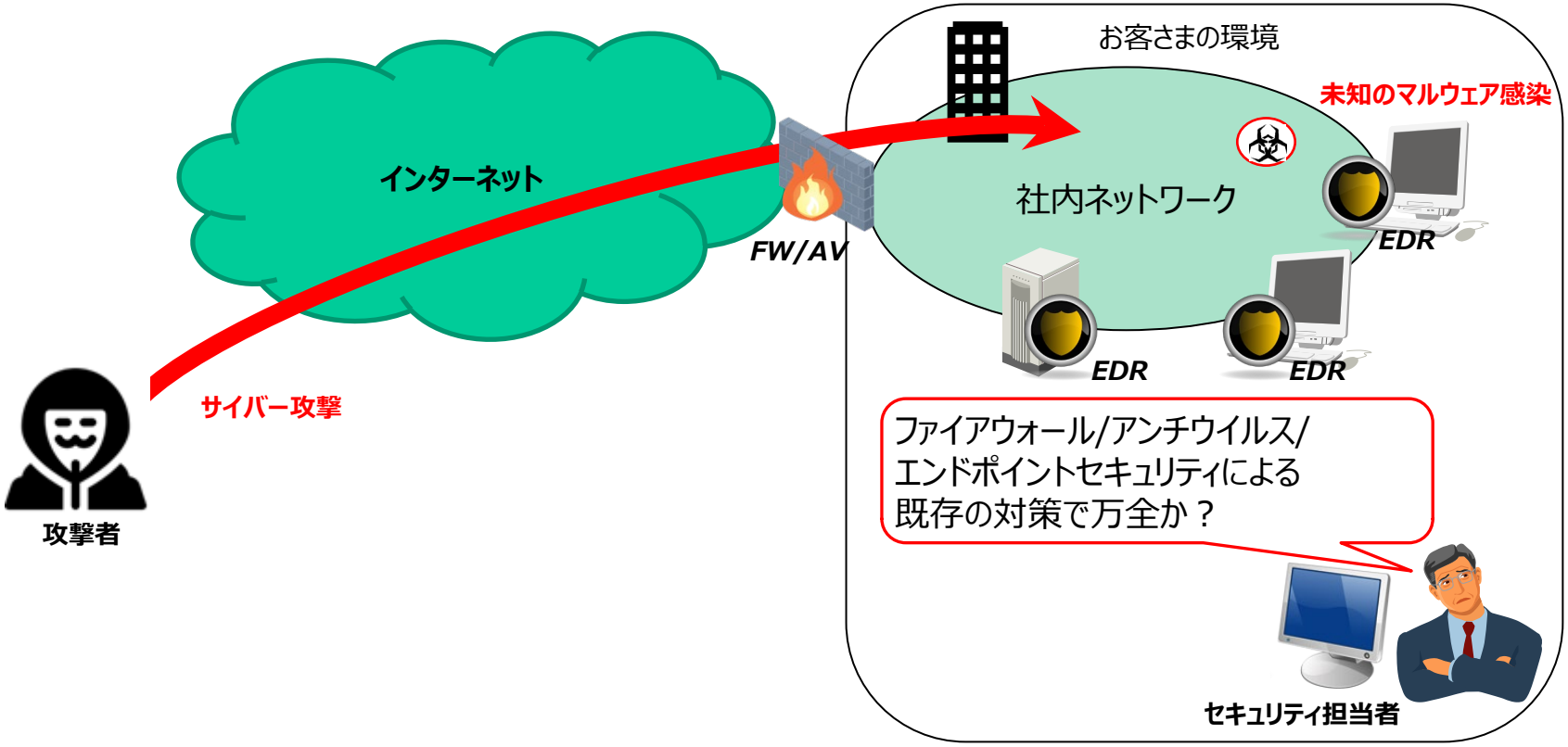
4-2. ユースケース（今まで）

HITACHI
Inspire the Next

従来

社内ネットワークのセキュリティ対策でFW/AVで入り口対策、EDR※を導入して脅威に備えているが、巧妙化するサイバー攻撃により侵入された脅威に対して、要員不足などにより既存対策では攻撃を受けていることに気づくのに時間がかかってしまう。これにより攻撃検知が遅れて、社内にウイルスがまん延、被害金額増大の危険性！

※EDR：Endpoint Detection and Response

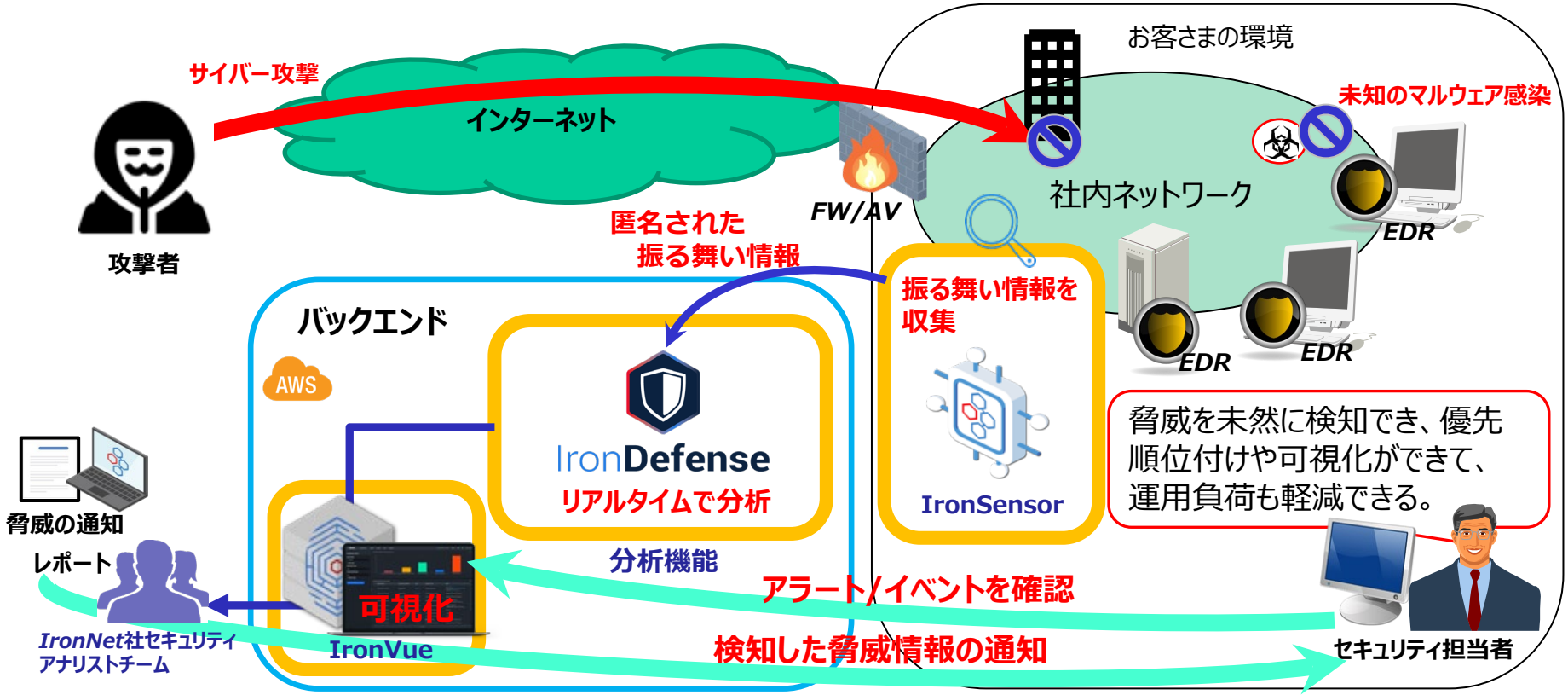


4-3. ユースケース（これから）

HITACHI
Inspire the Next

ネットワーク脅威検知ソリューションを適用①

社内ネットワークを「IronDefense® / IronSensor」で監視し、検知した脅威情報をリアルタイムで分析します。分析結果は優先順位付けし、セキュリティ担当者にIronVue（監視端末）で共有（可視化）されます。脅威を早期に把握でき、ネットワークの設定変更や社内への注意喚起を行うことで、被害に遭わないための対策を進められます。

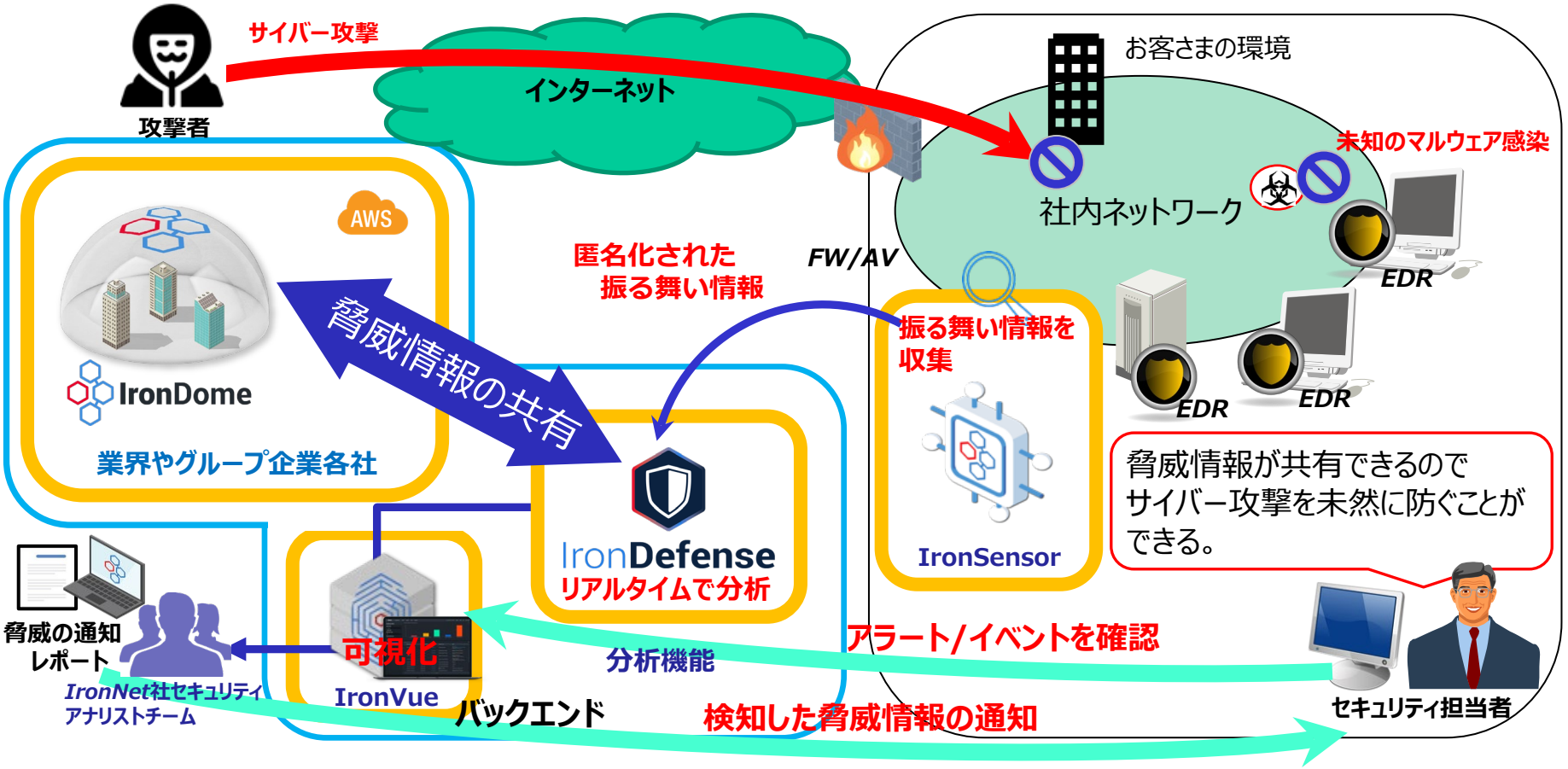


4-3. ユースケース（これから）

HITACHI
Inspire the Next

ネットワーク脅威検知ソリューションを適用②

業界やグループ企業間で「IronDome®」を形成し、脅威情報の共有を行うことで、サイバー攻撃が行われる前に、集団で効果的、かつ迅速にセキュリティ対策を実現します。



4-4. ソリューション導入による効果

HITACHI
Inspire the Next

既知の攻撃を知っており、攻撃されることが把握できている

導入前

・シグネチャ・ベースの検知（既知の脅威）
・ファイアウォール、エンドポイントでの対策
・未知の脅威発見の長期化（気づくのが遅れる）
・新しい脅威を分析する能力が不可欠

既知の攻撃や未知の攻撃に対して、攻撃されていることが把握できていない

ネットワークトラフィックの
振る舞い・挙動による対策

・侵入された脅威に対してネットワーク上の振る舞い・挙動から脅威の予測、検知が可能
・脅威レベルのスコアによる見える化
・AI※1/ML※2によるリアルタイムでの分析を行い、脅威の発見の早期化が可能
・脅威（振る舞い）情報の共有化で新しい脅威をより迅速に検知（IronDome®）
・セキュリティ対策人財に対して、負荷低減、サポート、レポートを提供

※1 AI：Artificial Intelligence　※2 ML：Machine Learning

HITACHI
Inspire the Next

5. ソリューション構成

5－1．ソリューションの提供形態

5－2．ソリューションメニュー

5－3．ソリューション導入費用例

5-1. ソリューションの提供形態

HITACHI
Inspire the Next

「ネットワーク脅威検知ソリューション」は、ネットワークの振る舞いから脅威を検知する**「IronDefense®」**と、集団で脅威を共有することができる**「IronDome®」**によって構成されています。

(1)IronDefense®はAWS上に構築され、脅威分析を行います。
お客さまの社内ネットワークには、センサー「IronSensor」を設置します。
ミラーポートに接続するため、既存ネットワークへの影響や構成変更はありません。
AWS上の機能「IronVue」を使用することで、お客さまにて脅威分析ができます。

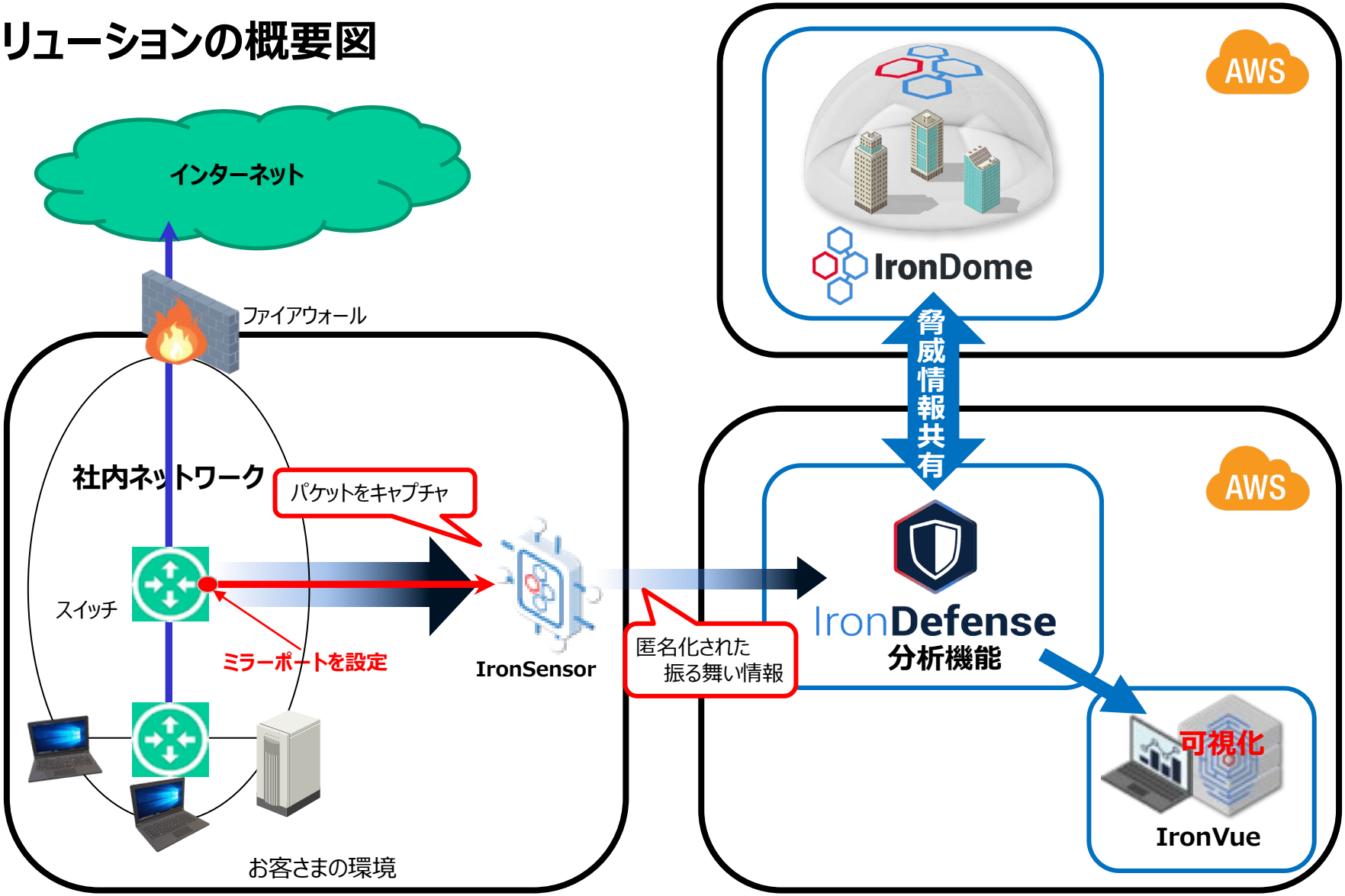
(2)IronDome®は、AWS上に構築されます。
IronDome®を形成することで企業間での脅威情報を共有できます。

※(1)(2)ともサブスクリプションとして提供されます。

なお、AWS上で構築されるIronDefense® / IronDome®はメーカーによって提供・構築されるため、お客さまが構築する必要はありません。
※IronDefense® / IronDome®は、オンプレミスでの利用も個別対応可能です。

5-1. ソリューションの提供形態

ソリューションの概要図



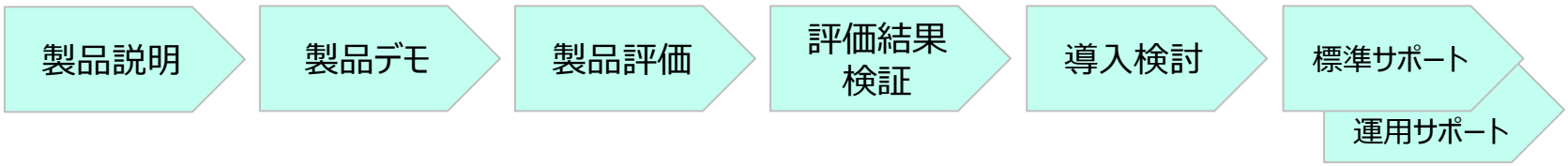
HITACHI
Inspire the Next

ソリューションメニュー

項目		内容
年間 サブスクリプション	運用サポート（標準契約） ※製品ライセンスに含む	・インシデント詳細調査支援（48インシデント/年）※メール対応 ・保守、お問い合わせ対応（当社営業日：9－17時） ・月次レポート（英語）
追加オプション		インシデント詳細調査の追加（２インシデント単位）
		IronVueの操作・運用方法トレーニング（２日間/回） ※トレーニングはIronNet社もしくは当社が実施
評価導入支援サポート（PoC）		導入を検討されているお客さまに、評価環境を準備し評価支援 ・IronDefense® 、IronSensor導入 ・操作・運用支援

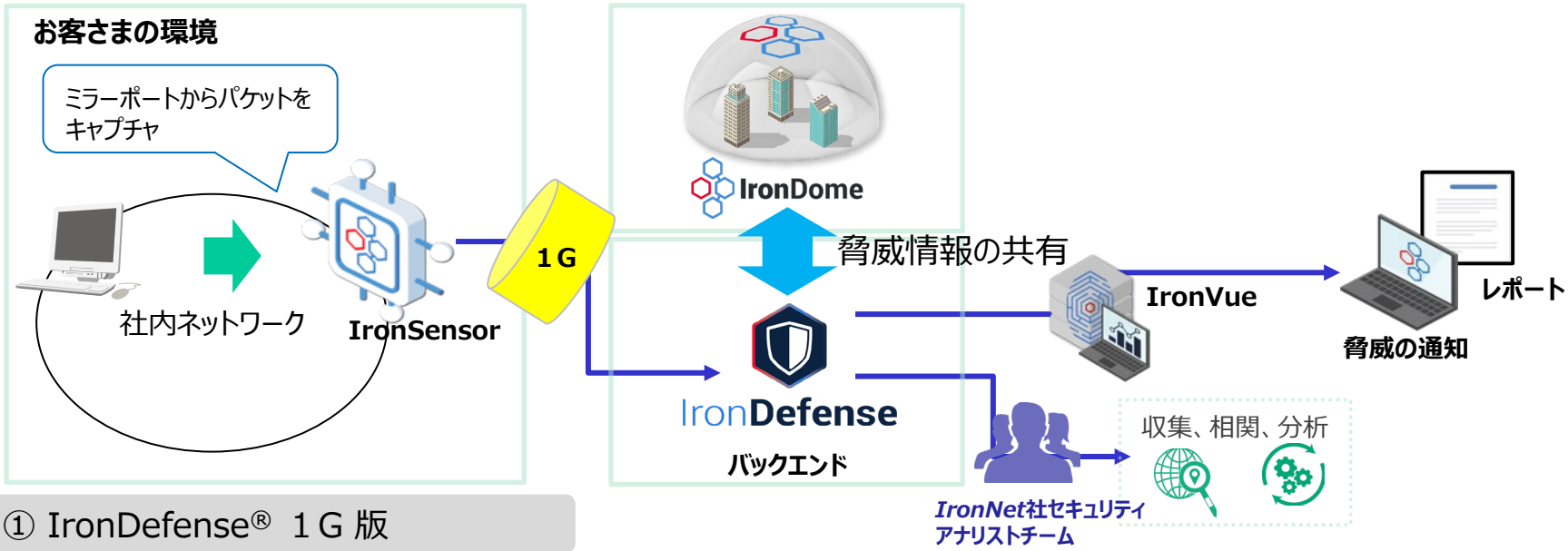
※上記運用サポートのメニュー内容は、IronDefense® Professional版（AWSプラットフォーム構成）の場合です。
その他のラインアップにつきましては、お問い合わせください。
※初期導入費用が別途必要です。

・提案～導入



5-3. ソリューション導入費用例

例えば、本ソリューションを活用してIronDefense® Professional １Gを1台導入した場合、導入費用（税抜）は以下のとおりです。
※IronDefense®はお客さま環境のデータ量により製品が１G/３G/５G/１０G/２０G版とあります。



① IronDefense® １G 版

#	コスト種別	内訳	標準価格
1	初期費用	・導入サービス：450万円 ※メーカーによるインストールサポート費用	450万円～
2	ランニング（年間）	・IronDefense® / IronDome®（サブスクリプション）：2,881.5万円 ・IronSensor（ハード サブスクリプション）：233.1万円	3,114.6万円/年

※価格には回線使用料は含んでおりません。

HITACHI
Inspire the Next

6. IronDefense® / IronDome® のご紹介

6－1. IronDefense® / IronDome® のご紹介

6－2. IronDefense® について

6－3. IronDome® について

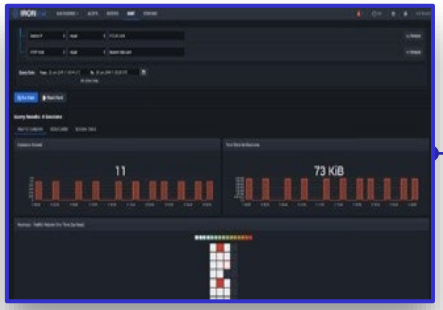
6－4. 運用サポートについて

6－5. ラインアップのご紹介

HITACHI
Inspire the Next

IronDefense® / IronDome® のご紹介

効率的なサイバー防衛では、挙動や振る舞いに基づく検知と集団によるセキュリティ対策を必要としています。
IronNet社は高度なサイバー脅威に対抗して企業、業界、そして国家規模間で集団的な防衛を行う最先端のサイバーディフェンスソリューションを提供します。



IronDefense®

洗練されたネットワーク振る舞い分析（NTA）プラットフォーム

IronDome®

業界を牽引する脅威の検知と集団防衛プラットフォーム

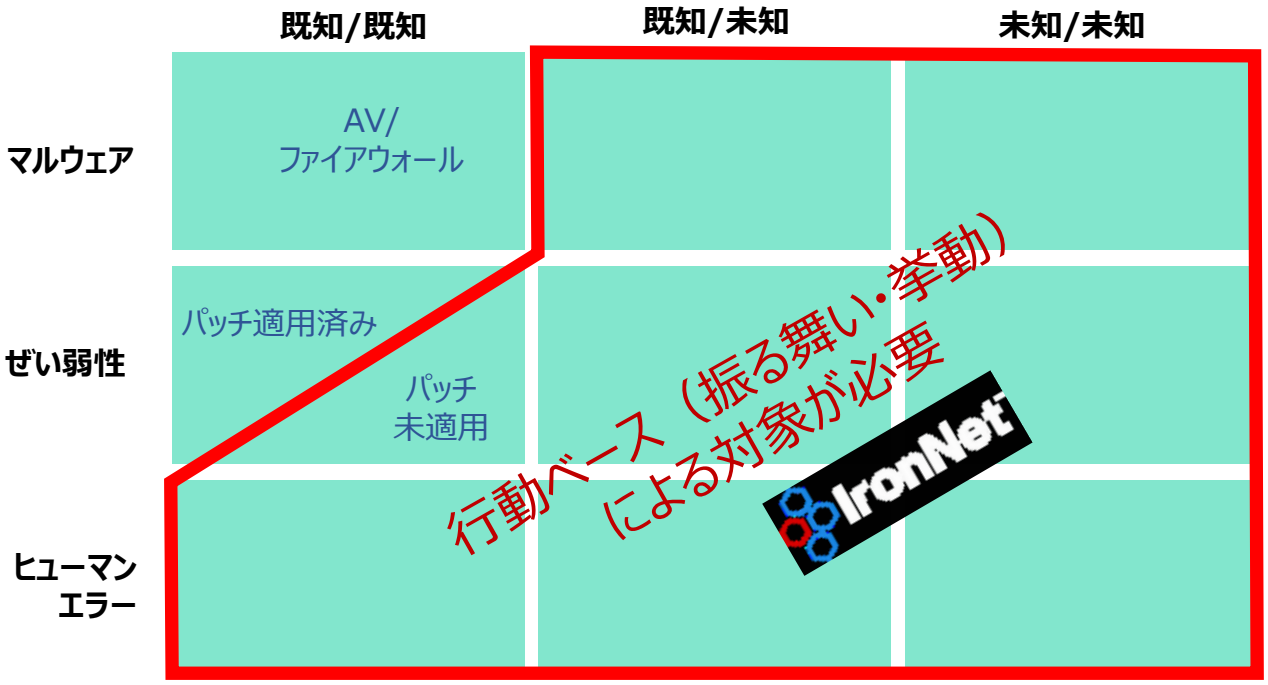
運用サポート

軍事レベルの経験に裏打ちされたサイバー運用チームと専門家たちにより運用される世界最高峰のセキュリティアナリストチーム

6-1. IronDefense® / IronDome® のご紹介

HITACHI
Inspire the Next

従来のシグネチャベースのセキュリティ製品と異なり「予兆検知」を特長とし、既存の情報分析では「警告」に至らない「潜在的な脅威」を事前に予知。優先順位を付けて対処を可能とするソリューションです。



HITACHI
Inspire the Next

IronDefense® 製品概要

ネットワークの振る舞いを分析

主要な機能

優れた振る舞い検知

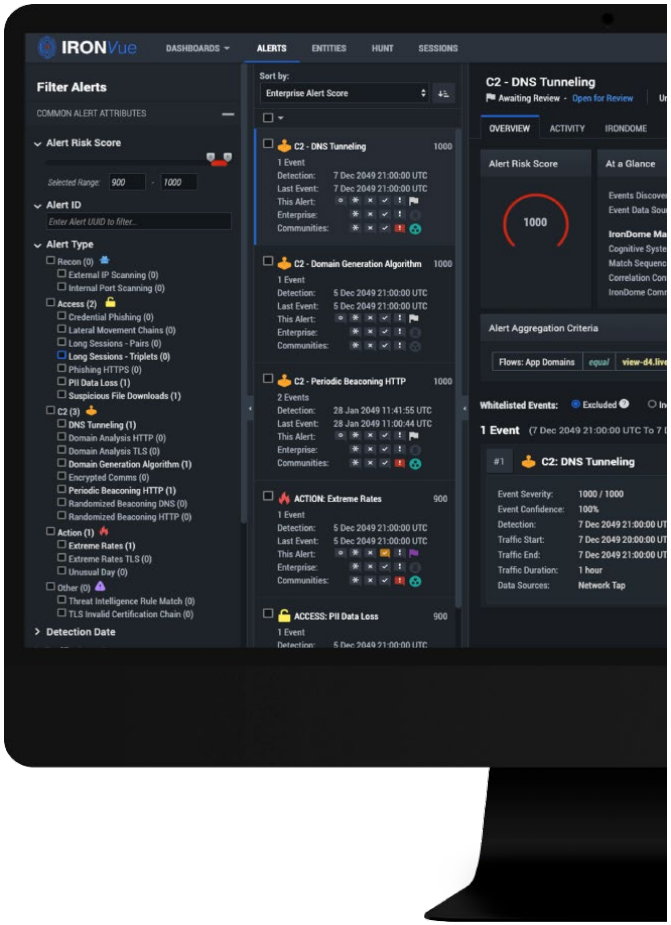
先進的な分析とAI/MLによる検知により、
手作業の分析を改善

エキスパートシステム

国家のトップサイバーディフェンダーたちが持つ判断
と経験に基づく知識を適用

統合されたサイバーハント

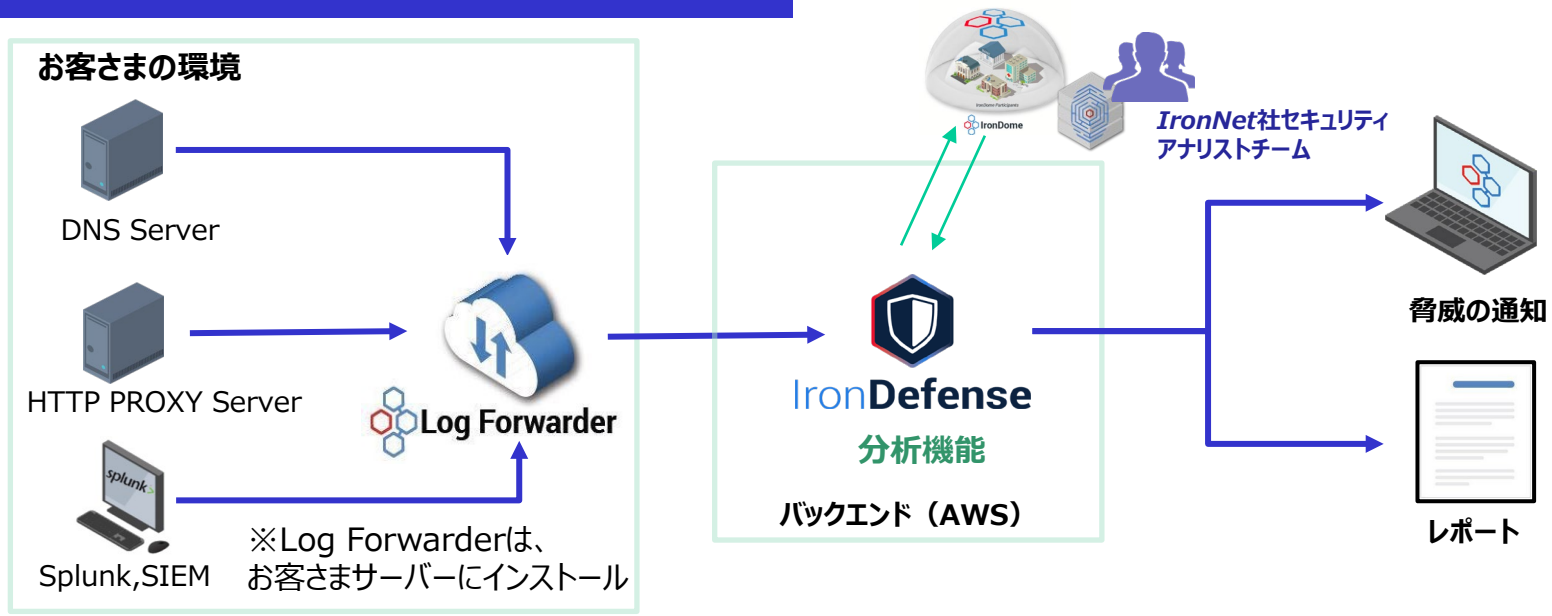
パケット単位の可視性により調査の速度と深さを
これまで以上に改善



6-2. IronDefense® について

HITACHI
Inspire the Next

IronDefense® Essential

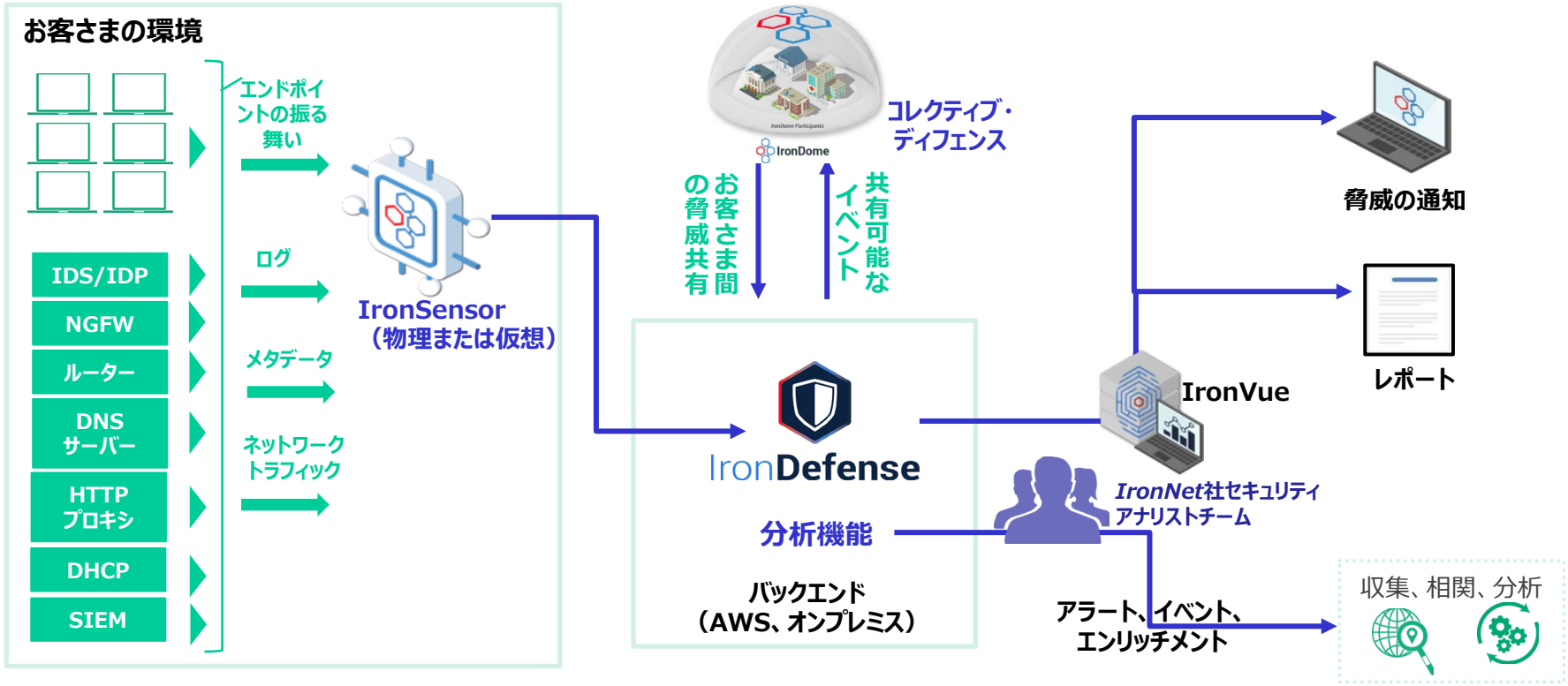


お客さま環境のDNS ServerおよびHTTP PROXY ServerのSyslogをLog ForwarderでAWS上のIronDefense®バックエンドに転送し分析を行います。
レポーティングにより脅威状況を把握。
エージェントの導入・配備の手間などが一切必要ありません（ログ転送の設定のみ）。
ログをIronNet社のエキスパートが監視、不正なサイトへのアクセスや資格情報搾取のフィッシングアクセスを検知するなど、セキュリティ事故への対応が迅速にできます。
お客さまは「脅威の通知」を受け取り、社内ユーザーにそのサイトへのアクセスの必要性を確認し、そのサイトへのアクセスをホワイト/ブラックリストでルールを掛けるなどの対策が進められます。

6-2. IronDefense® について

HITACHI
Inspire the Next

IronDefense® Professional / Enterprise



お客さま環境のネットワークトラフィックをキャプチャしてIronDefense®にて分析を行い、
優先度付けして警告し、脅威への対策を支援します。
IronDome®利用時には、脅威を共有してより迅速な脅威対策が可能です。
お客さまは、IronVueを用いて脅威の優先度の確認ができます。
エージェントの導入・配備の手間などが一切必要ありません。

6-3. IronDome® について

HITACHI
Inspire the Next

IronDome® （コレクティブ・ディフェンス）

主要な機能

企業のエコシステム間で脅威を可視化

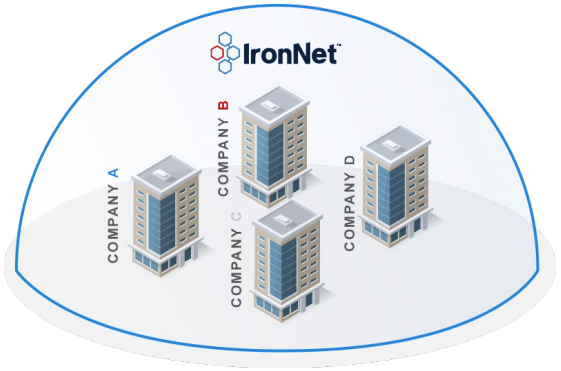
業界、グループ企業、大規模および小規模企業間でリアルタイムに脅威情報の共有を実現

IronDome®単位での検知と相関

IronDome®単位で洗練された振る舞い分析を実現し、隠れた脅威を検知し、予防

ディフェンダーたちと容易に協力

他の参加者達と調査と分析の結果を自動で共有



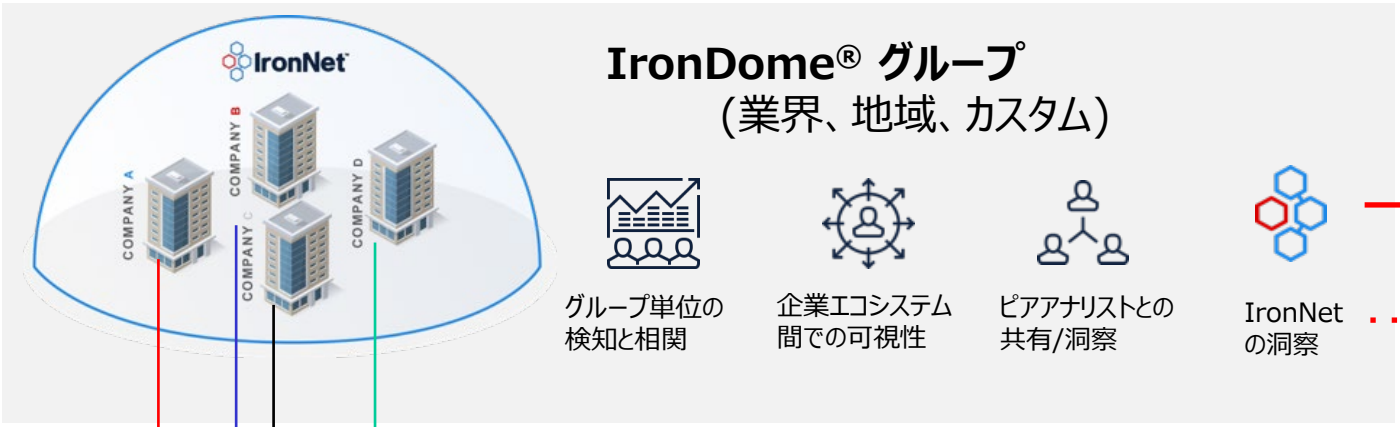
効果

- **より速く**
  - 脅威のアラートを即時に全ての企業に提供
- **より少ない資源で**
  - 各参加者の資源と投資からの利益を全員が享受
- **さらに効率よく**
  - 参加者の全てが攻撃の対策に成功

6-3. IronDome® について

HITACHI
Inspire the Next

IronDome® （コレクティブ・ディフェンス）



HITACHI
Inspire the Next

運用サポート

主要な能力

セキュリティ強化の支援

お客さまのセキュリティチームを継続的に支援し、より強力なセキュリティ対策を実現

サイバー運用センター

予兆検知した脅威情報は、お客さまのセキュリティチームと一体となり、またIronNet社のアナリストとも連携しながら、トリアージ、レスポンスなどの作業を実行

アドバイザリーサービス

お客さまのセキュリティチームを補完するアドバイザリーサービスによりお客さまの戦略とリスクの診断を支援

6-5. ラインアップのご紹介

HITACHI
Inspire the Next

		IronNet® Essential	IronDefense® Professional	IronDefense® Enterprise
		エントリーレベル ログのみのドームソリューション	基本的なサービスを備えた フルクラウドソリューション	信頼性の高い フルソリューション
ソリューション機能	コレクション	ログのみ	ログ、バーチャルもしくは物理センサー	ログ、バーチャルもしくは物理センサー
	バックエンド	クラウドのみ	クラウドのみ	クラウドもしくはオンプレミス
	IronVue®ユーザーインターフェイス	×	○	○
	ハンティング機能	×	○	○
	API統合	×	○	○
	アラートレイティングとコメント	×	○	○
カスタマーサクセス	インストールと実装	リモート	オンサイト	オンサイト
	チューニングとIronDefense®最適化	リモート	リモート	オンサイト
	ユーザートレーニング	リモート	リモート	オンサイト
	導入後の継続的なお客さま支援	○	○	○
提供サービス	イベント通知	毎日のDNSおよびHTTPアラート	すべてのアラート、リアルタイム	すべてのアラート、リアルタイム
	ルールの展開（新たな脅威の調査）	○	○	○
	レポーティング	マンスリーレポート（英語）	マンスリーレポート（英語）	マンスリーレポート（英語）
	インシデント対応	×	48インシデント/年間	60インシデント/年間
	ネットワーク防御のトレーニング および新機能のレビュー	×	×	4回/年間
技術サポート	製品テクニカルサポート	翌営業日の対応	翌営業日の対応	翌営業日の対応
製品トレーニング	基礎：2日間のトレーニング	×	1回/年間	4回/年間

HITACHI
Inspire the Next

7. ケーススタディ

7－1．ケーススタディ　（1）

7－2．ケーススタディ　（2）

7-1. ケーススタディ（1）

HITACHI
Inspire the Next

Emotetマルウェアの検知

脅威: DNS トンネリング攻撃がIronDefense®によって検知され、外部のドメインから隠れたデータの転送が疑われました。

IronNet®の導入効果

可視性の向上

- 振る舞い/挙動検知を通じて、IronNet社のエリートサイバー運用チームは疑わしいネットワークトラフィックの特徴を検知しました。

インパクトの低減

- エンドポイント分析によりDHSによって公共とプライベートセクターに影響があるものとして”最も費用がかかる破壊的なマルウェア”と言われたEmotetマルウェアの感染が確認されました。

改善された効果

- ファイアウォールは既知のDNSトンネリングを検知することができましたが、未検知の未知のマルウェアについてはわかっていませんでした。
- IronNet®だけが以前に未知の脅威を検知しており、お客さまのファイアウォールでそれを解決するべく更改が行われました。

7-2. ケーススタディ（2）

HITACHI
Inspire the Next

未承認のソフトウェアを検知

脅威: IronDefense®極めて重要なインフラのエンドポイント上で疑わしいネットワークの挙動を検知しました。

IronNet®の導入効果

可視性の向上

- 通常のネットワークトラフィックに対するベースラインを確立することで素早く検知および逸脱の評価と異常を検知することが必須であり、これによりマルウェアの存在を確認できる可能性があります。

インパクトの低減

- お客さまのSOC※へ以前は検知されなかった従業員の承認されていないソフトウェアダウンロードがアラートにより警告されました。

改善された効果

- Webサイトへのアクセスは許可されていましたが、従業員による未承認ソフトウェアのダウンロードが抑止できておらず、潜在的な脅威となっていました。
- 未承認のソフトウェアのダウンロードを検知、インストールを抑止できました。

※SOC： Security Operation Center

HITACHI
Inspire the Next

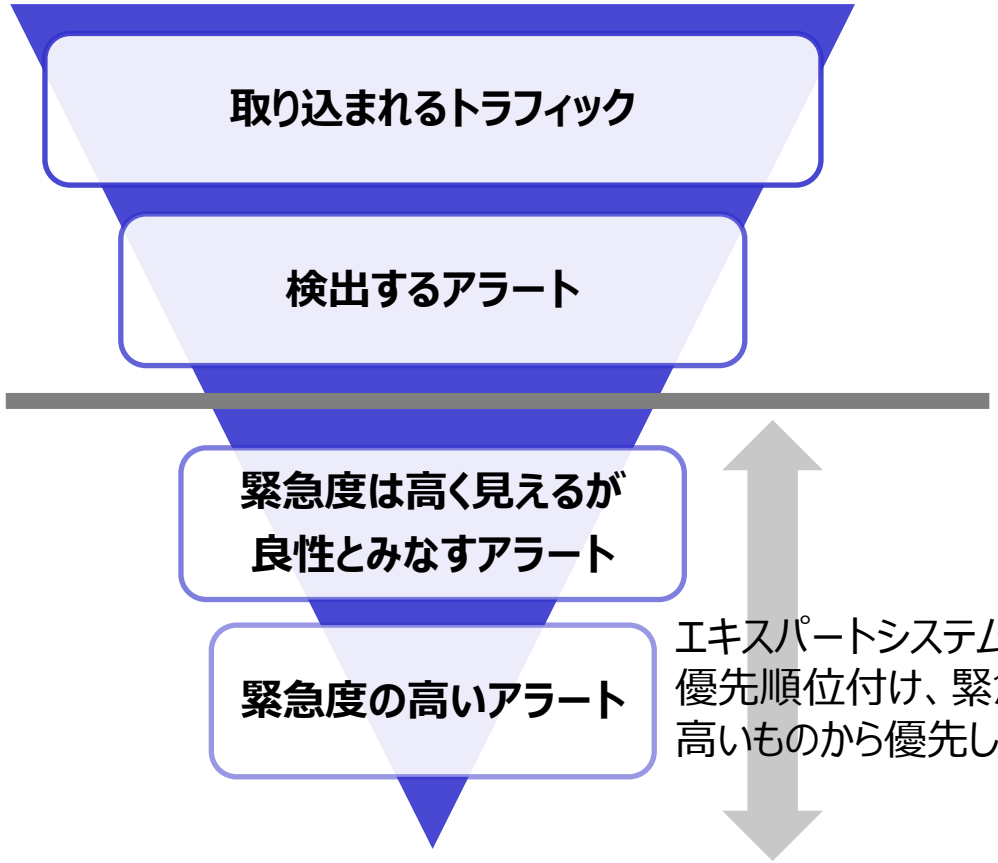
8. IronDefense®の機能検証（参考）

8. IronDefense®の機能検証（参考）

HITACHI
Inspire the Next

当社内で、IronNet社と共同で「Periodic Beaconing HTTP/HTTPS」および「Data Exfiltration」の疑似検証を実施

～脅威を検出して、エスカレーションされるまで～



エキスパートシステムにより優先順位付け、緊急度の高いものから優先して確認

1～1,000のスコアリングにより脅威を優先順位付けする

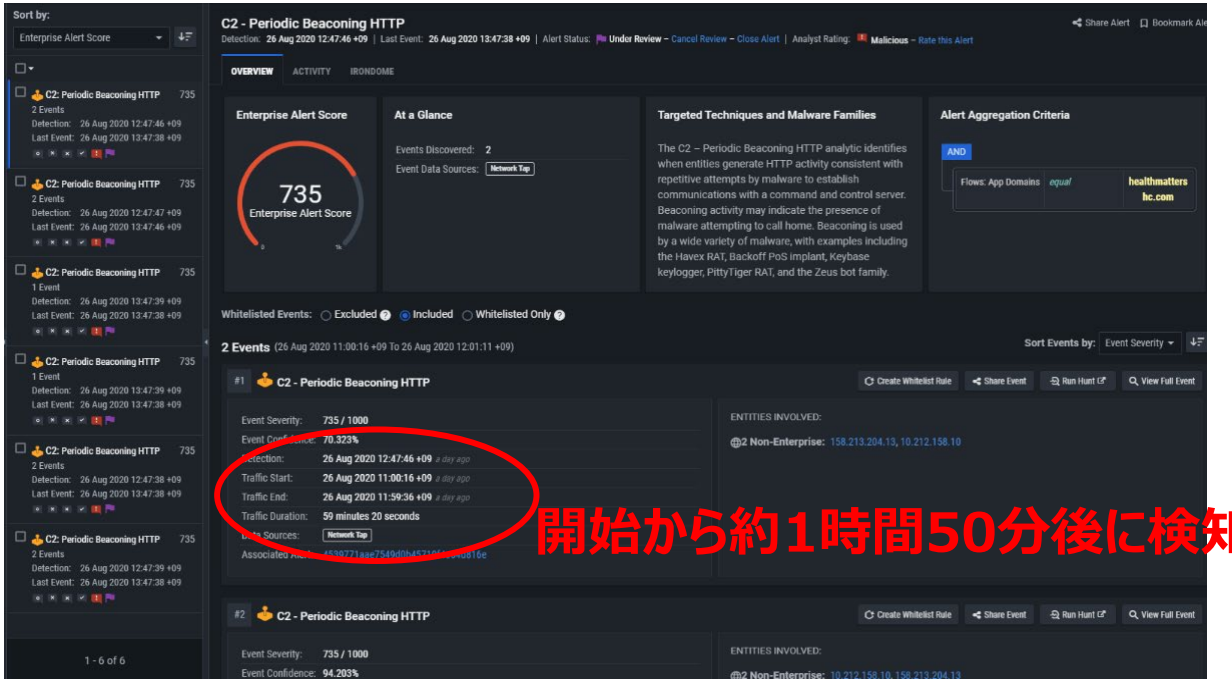
- 750以上あたりが重大な脅威の目安
- 600以下でも未知の脅威である可能性があり、スコアの幅は環境にもよるため、監視対象スコアは、検討が必要

8. IronDefense®の機能検証（参考）

HITACHI
Inspire the Next

①Periodic Beaconing

社内ネットワークからインターネットを介して社外サイトとのHTTP/HTTPS、一定周期/不定周期のBeaconingはすべて成功し、IronDefense®においてはトラフィック開始後約1時間50分後にすべて検知しました。警告スコア：735　検知例は以下の通り。



IronVue画面

8. IronDefense®の機能検証（参考）

HITACHI
Inspire the Next

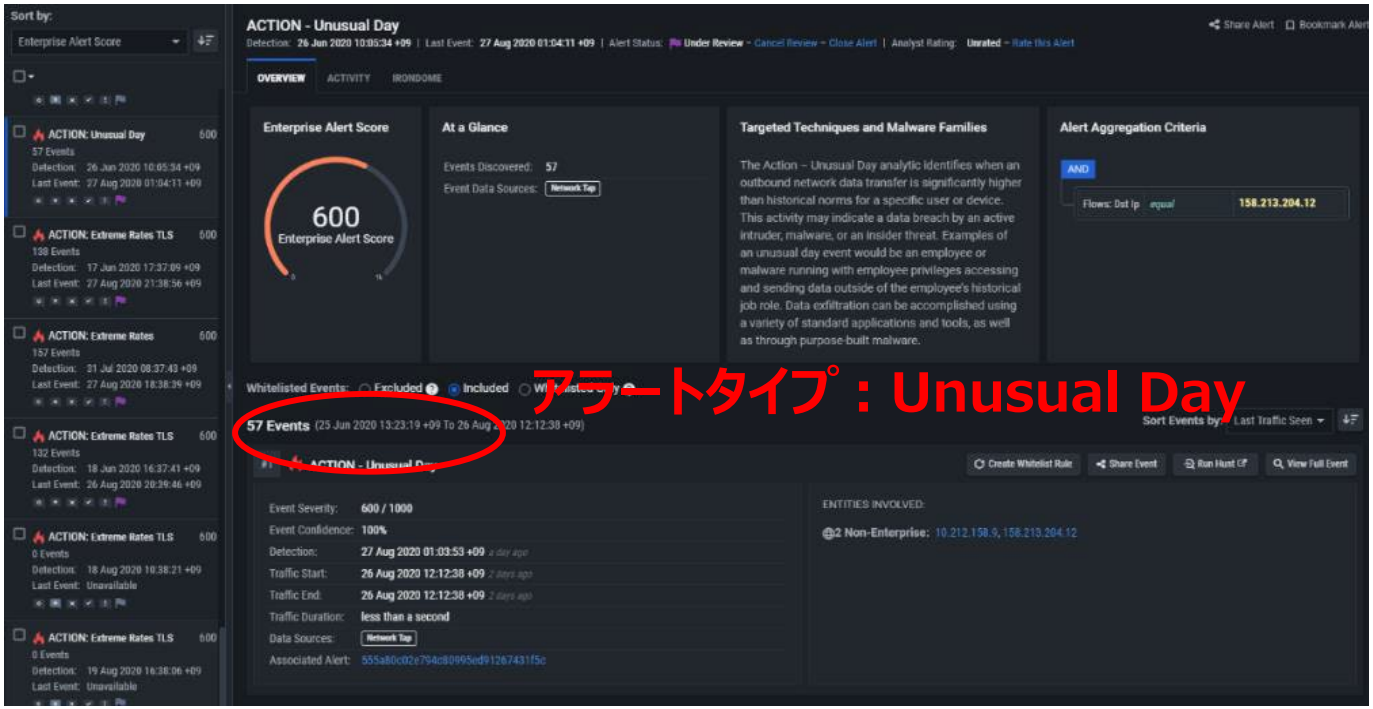
①Periodic Beaconing

社内ネットワークからインターネットを介して社外サイトとのHTTP/HTTPS、一定周期/不定周期のBeaconingはすべて成功し、IronDefense®においてはトラフィック開始後約1時間50分後にすべて検知しました。警告スコア：735　検知例は以下の通り。

IronVue画面

8. IronDefense®の機能検証（参考）

②Data Exfiltration
社内ネットワークからインターネットを介してクライアント側でPowerShellによるファイル送信は成功し、IronDefense®により検知に至った。実行：12:12。検知：翌日01:03
警告スコア：600　検知例は、以下の通り。



IronVue画面

Unusual Day 通常より多くのバイトを送信したエンティティを検知。
エンティティが通常よりも多くのトラフィックを送信しています。これは、マルウェアがデータを盗み出すか、内部関係者が従業員の職務外のリソースにアクセスし、その後大量のデータを送信することによって引き起こされる可能性があります。

お問い合わせ

HITACHI
Inspire the Next

株式会社 日立ソリューションズ・クリエイト

Webでのお問い合わせ

https://www.hitachi-solutions-create.co.jp/contact/solution.html

※該当のソリューションをお選びください

メールでのお問い合わせ

hsc-contact@mlc.hitachi-solutions.com

表示に関する注意事項

HITACHI
Inspire the Next

■他社商品名、商標などの引用に関する表示

- IronNet®、IronDome®、IronDefense®のロゴ及び製品名は米国法人IronNet Cybersecurity, Inc.の米国、日本またはその他の国における登録商標、または商標です。
- AWS、ロゴは、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2021年5月現在のものです。
サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。

■お問い合わせ情報について

お問い合わせ情報についてご相談・ご依頼いただいた内容は回答などのため、
当社の関連会社（日立ソリューションズグループ会社）および
株式会社日立製作所に提供（共同利用も含む）することがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。