NTTデータグループの
情報セキュリティ戦略と運用術

2008年12月17日

株式会社 ＮＴＴデータ
情報セキュリティ推進室長　山岡 正輝

情報セキュリティ対策の考え方

NTTデータグループの概要

NTTデータグループ

売上高	1兆744億円	(2008.3月期決算)
営業利益	959億円	(2008.3月期決算)
従業員数	23,080名	(2008.3末時点)
グループ会社数	135社	(2008.3末時点)

変える力を、ともに生み出す。
NTT DATAグループ

左:豊洲センタービル(本社)
右:豊洲センタービル アネックス

NTTデータの主な事業内容

システムインテグレーション事業
お客様の個別ニーズに合わせて，データ通信システムを開発し，その販売，賃貸，サービスの提供等を行う事業

ネットワークシステムサービス事業
市場のニーズに合わせて，インターネットに代表されるコンピュータネットワークを基盤として，種々の情報提供，情報処理等のサービスを提供する事業

その他
お客様の経営上の問題点に係る調査および分析，データ通信システムの在り方に係る企画および提案，メンテナンスおよびファシリティマネジメント等を行う事業

企業理念とブランドスローガン

企業理念

NTTデータグループは，情報技術で，新しい「しくみ」や「価値」を創造し，より豊かで調和のとれた社会の実現に貢献する．

企業コンセプト (～H17)

情報から活力をうみだすバリュー・クリエイター

ブランドスローガン (H20～)

変える力を、ともに生み出す。
NTT DATAグループ

ブランドプロミス

NTTデータグループは，変革を構想し実現するパートナーとして，お客様と，夢と感動を共有していきます．私たちは，ニーズへの先見性や深いお客様理解をもとに，新たなビジネスやサービス，そしてそれを支えるソリューションを構想し，社会やビジネスの更なる発展という夢を，お客様と共有します．そして，その変革を実現し，お客様と感動をともにすることこそ，私たちのゴールです．そのために，高度なシステム構築力や活用力を核に，様々なビジネスやサービスの連携など，IT領域にとどまらないサポートを行っていきます．

情報から価値をうみだすバリュー・クリエイター

しくみの一例

アメダス（地域気象観測システム）
全国約1,300ヶ所の観測点で，降水量，風向・風速，気温等を自動的に観測するシステム

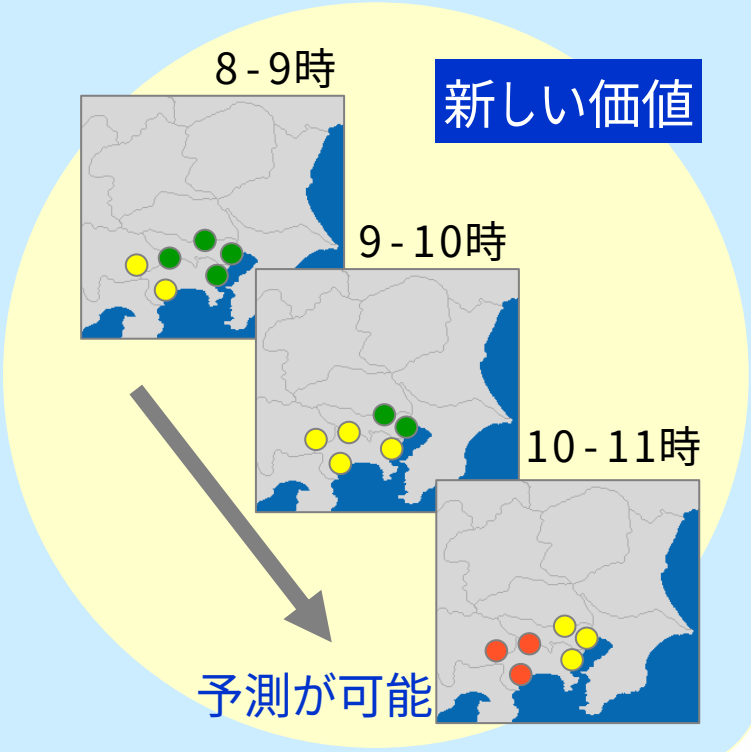
降水量

	8-9時	9-10時
小田原	3mm	3mm
横浜	0mm	3mm
東京	0mm	0mm

ひとつひとつの情報

地図上にプロットしてみる

時系列に並べてみる



新しい価値を創造するしくみをITでつくる

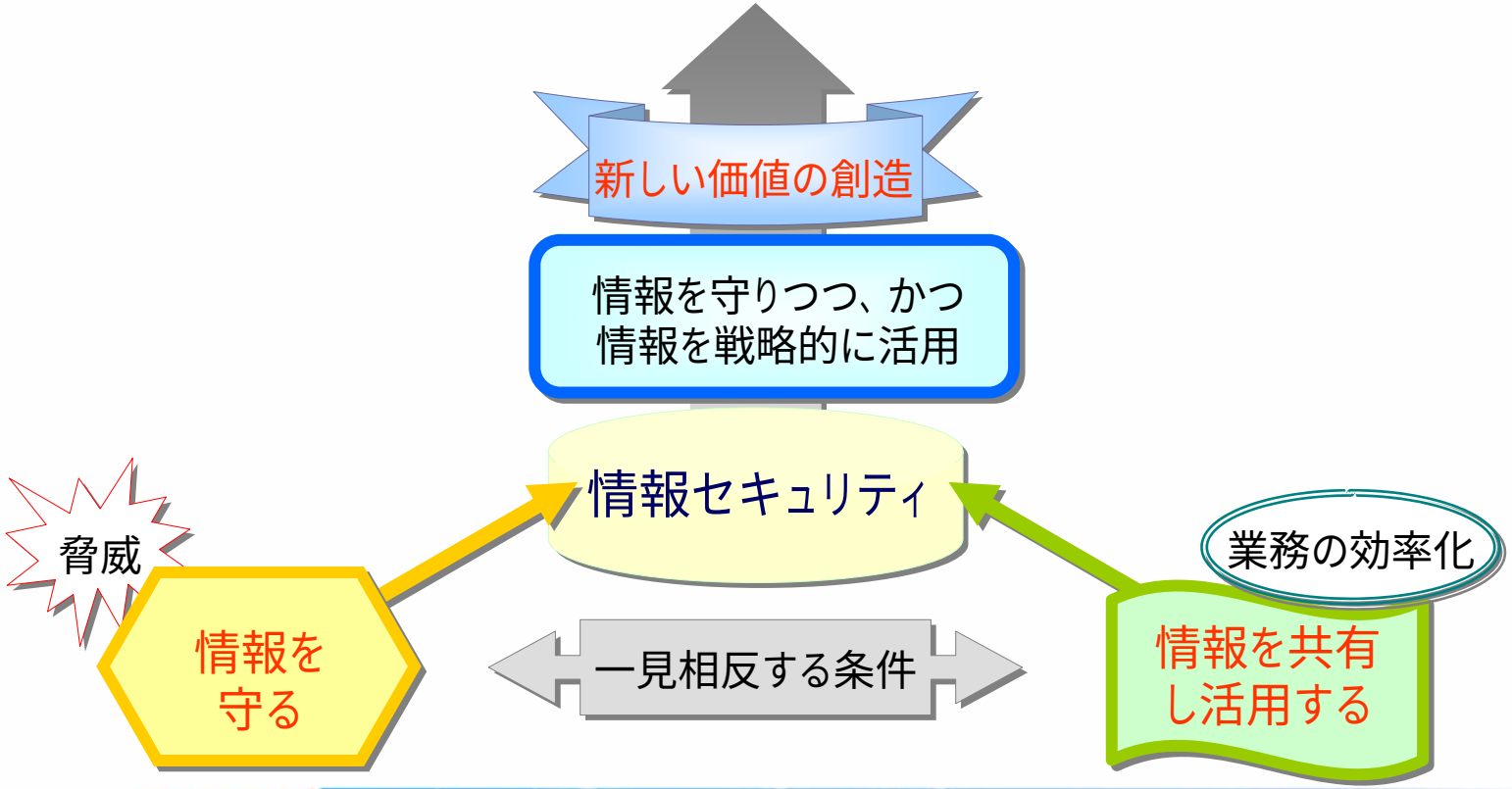
NTTデータにおける情報セキュリティ対策の考え方

情報セキュリティポリシーの目的

NTTデータの企業コンセプト「情報から活力をうみだすバリュー・クリエイター」に基づき，NTTデータグループの一員である当社において以下の実践を第一義の目的として制定するものである．

・NTTデータグループの会社間で情報を積極的に共有，活用することにより，グループ各社が協働するシステム開発の場で創造性、生産性を高める

・情報資産を適切に取り扱い，情報セキュリティを確保する



Our Vision -Global IT Innovator-

Global IT Innovator
NTT DATA GROUP

＜全世界合計＞

拠点数：26都市⇒60都市
社員数：846名⇒4,800名

＜欧州圏＞
・日系ｸﾞﾛｰﾊﾞﾙ企業対応
・現地企業対応

拠点数：1都市⇒32都市
社員数：4名 ⇒ 2,848名

＜アジア圏＞
・日系ｸﾞﾛｰﾊﾞﾙ企業対応
・ｵﾌｼｮｱ開発拠点

拠点数：11都市⇒11都市
社員数：427名⇒1,256名

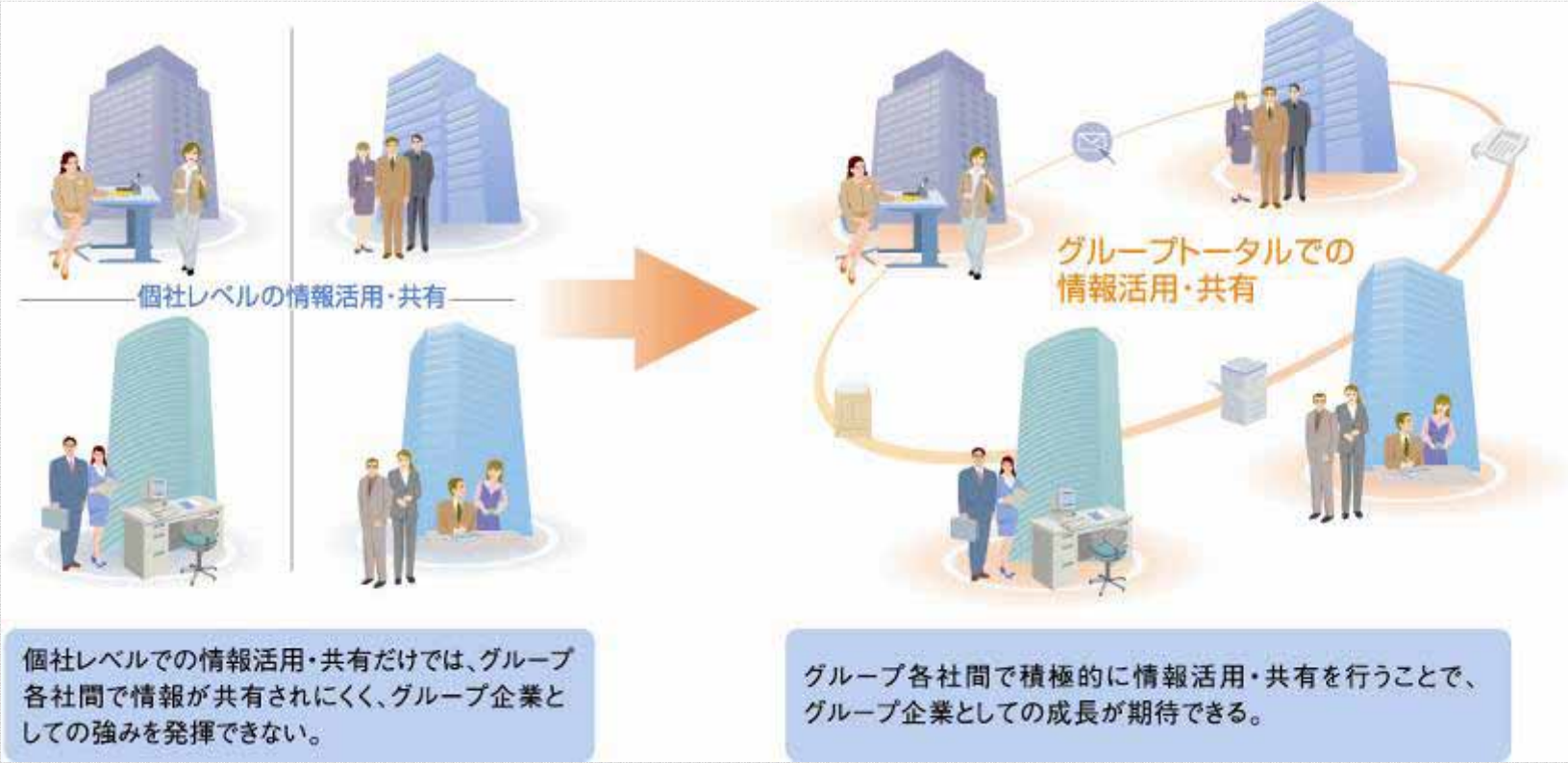
＜北米圏＞
・日系ｸﾞﾛｰﾊﾞﾙ企業対応
・現地企業対応

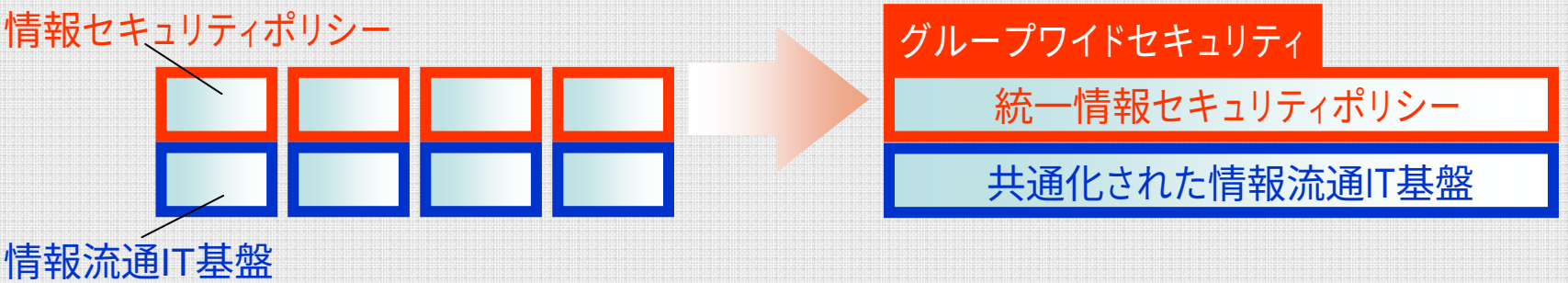
拠点数：14都市⇒17都市
社員数：415名⇒693名

21カ国60都市体制へ

※拠点数、社員数について・・・黒字：2007年3月末時点　青字：2008年10月1日時点

“グループワイドセキュリティ”という考え方





グループ統一の情報セキュリティポリシー

2001年スタート

SIをメインの事業とし，文化やビジョンも共通点が多いグループ会社

SSP（標準セキュリティポリシー）

NTTデータと情報の取り扱いルールが同一．SSPに準じたポリシーを持つ会社は，連名でSSP協定を締結．独自の監査機構を持つなど協力して情報セキュリティの維持・向上に取り組む．

2002年スタート

事業ドメインが異なるグループ会社や規模の小さなグループ会社

GSA（グループセキュリティ合意書）

規模の小さなグループ会社との情報流通を簡易に実現するため，必要な最低限のルールのみを規定．SSPに比べて自由度が高く，個社の独自のポリシーで対応が可能．

2008年スタート

GSP（NTTデータグループセキュリティポリシー）

グループ統一の情報流通基盤として，SSPのメリットである情報取り扱いルールの共通化と，GSAのメリットである多様なグループ会社への対応を取り入れた，統一的なグループセキュリティポリシー．

共通化された情報流通IT基盤

GW-Net　NTTデータグループ各社をつなぐネットワークインフラで、情報共有サービスは全てGW-Net上で展開される。

G-EGG

NTTデータグループのイントラネットポータルサイト。グループ社員検索や、ニュースリリースなどを掲示している。

SWH

グループ各社の技術コンテンツ、技術情報・ノウハウを公開。

TeSS

技術的な問い合わせ窓口。受注活動やシステム構築時のアドバイス・ノウハウなどが共有されている。

POT

グループ各社間でのファイルのやり取りを行うサイト。アクセス権限の設定やバージョン管理が可能。

社員情報
ニュース配信

ソリューション
サービス情報

技術情報
Q&A

ファイル
交換

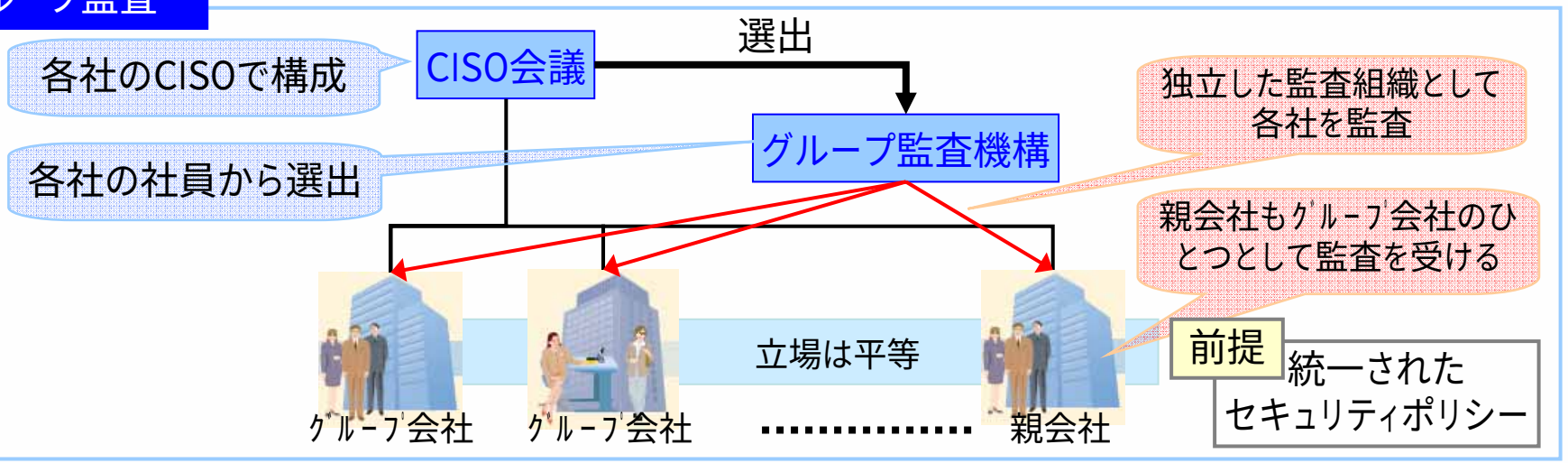
統一化された認証基盤

グループ監査体制　～親会社も監査をうける仕組み～

目的

企業グループ全体の情報セキュリティレベル向上

グループ監査



効果

親会社による監査ではなく，独立した監査機構による第三者監査が実現

監査機構に所属した社員が，他社のセキュリティ施策を知ることができる．
監査スキルも向上．

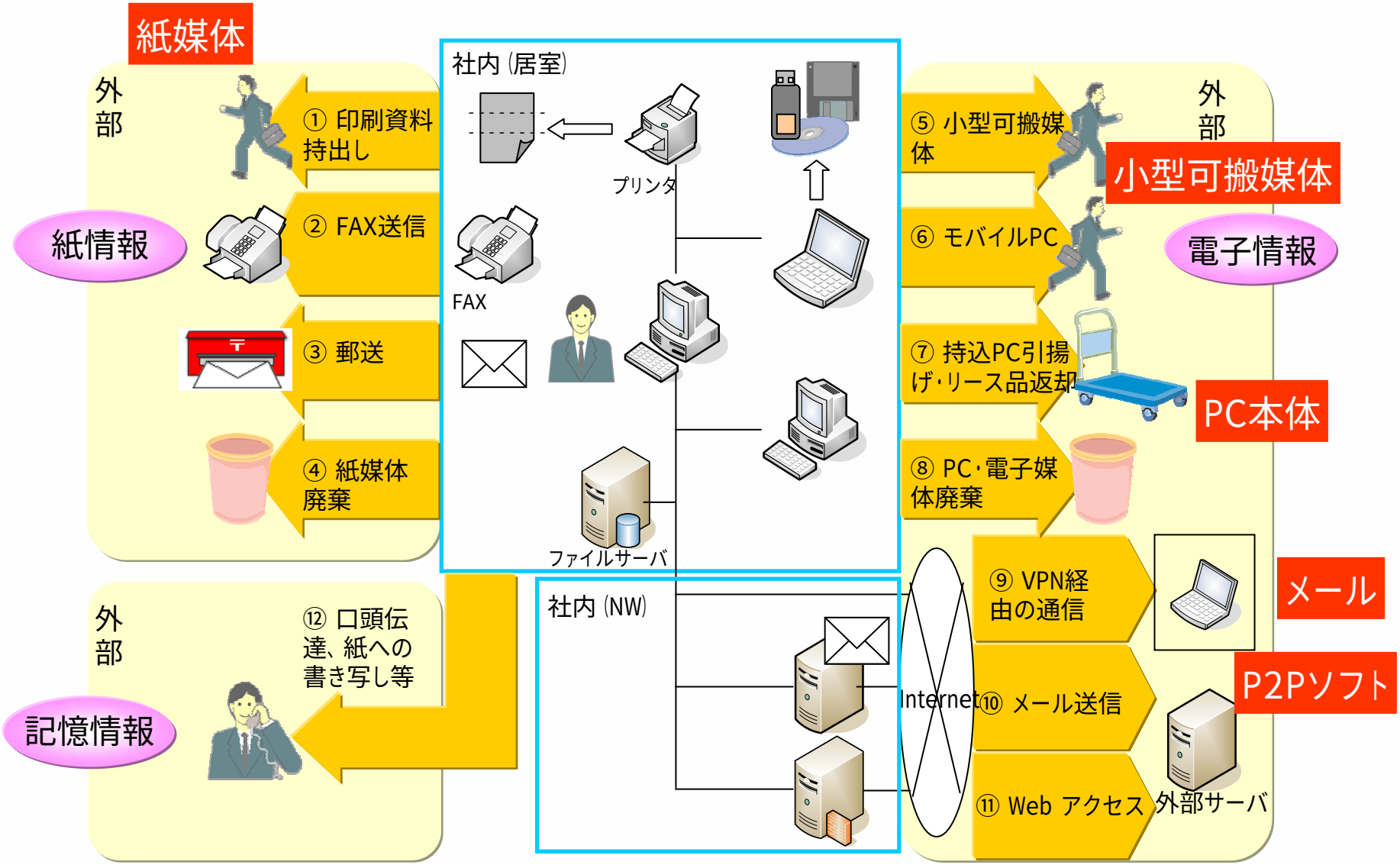
ｸﾞﾙｰﾌﾟ会社に対して，他社の情報ｾｷｭﾘﾃｨの実情を把握できる機会を与え，ﾍﾞｽﾄﾌﾟﾗｸﾃｨｽの自社展開が可能になるなど，ｸﾞﾙｰﾌﾟ全体の情報ｾｷｭﾘﾃｨﾚﾍﾞﾙが向上

※　本施策は、平成18年より全グループ会社のうち26社にてスタートした

情報漏えいの脅威と対策，教育啓発

情報漏えいに対する脅威の洗い出し

社内から外部への情報持出し手段ごとに脅威と脆弱性を洗い出す



情報持出し手段に対する現状の対策と残存リスク

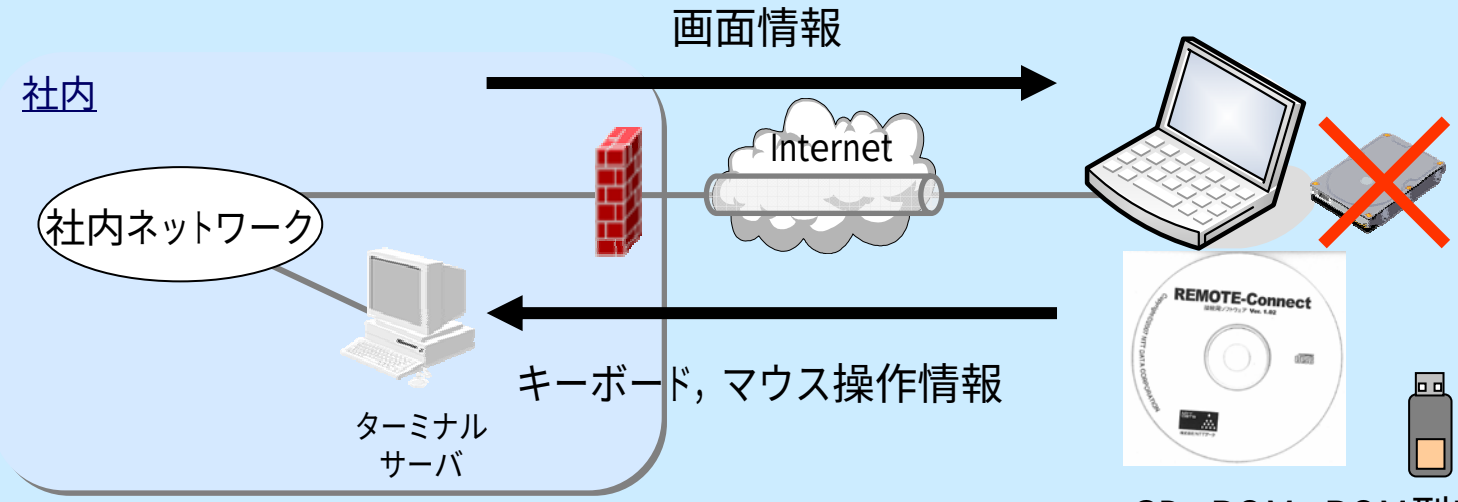
現状の対策と残存リスクの把握

No	区分	持出し手段	現状の主な対策（■: システム、●:ルール）	残存リスク
①	紙	印刷資料持出し	■TSFによる印刷時のログ取得	・印刷物の盗難/紛失
②		FAX送信	●送達確認	・誤送信
③		郵送	●機密性に応じて送達確認	・誤送信　・郵便事故
④		紙媒体廃棄	●機密性に応じて細断及び溶解処理	・ルール違反による漏洩
⑤	電子	小型可搬媒体	●原則使用禁止，例外使用のルール ■TSFによる小型可搬媒体への書込制限，ログ取得	・例外使用中の盗難/紛失
⑥		持出しPC	■シンクライアント化 ●HDD暗号化、BIOSパスワードの実施	・家族/第三者の無断利用 ・PCの盗難/紛失
⑦		持込PC引揚げ・リース品返却	●引揚げ・返却の際に、ツール等でHDDを完全消去	・ルール違反による漏洩
⑧		PC・電子媒体廃棄	●ツール等で完全消去を実行後、破壊	・ルール違反による漏洩
⑨		VPN経由の通信	■端末のシンクライアント化 ■TSFによる小型可搬媒体への書込制限、ログ取得 ●私物PC利用禁止	・VPN端末の盗難/紛失 ・家族/第三者の無断利用
⑩		メール送信	■メールフィルタリングソフトの導入 ■添付ファイルサイズ規制 ■メールアーカイブ、送信ログ取得 ■社外への送信権限取得制限 ●私用アドレスへの機密情報送付禁止	・権限所有者は自由にメール送信可能 ・誤送信
⑪		Web アクセス	■URLフィルタリング、アクセスログ取得 ■通信ポート制限 ■http 及び https 通信利用権限取得に上長承認必須	・権限所有者は自由に送信可能 ・Webサービスを利用した情報漏洩
⑫	記憶	口頭伝達、紙への書き写し等	-	・口頭などで可能な範囲の情報伝達

持ち出しPCのシンクライアント化

REMOTE - Connect

社外へ持ち出すPCを原則シンクライアントに限定しています



ハードディスクのないPCで，
CD-ROMまたはUSBメモリからLinuxを起動

PC紛失盗難による情報漏えいリスクが低減される

社外でも必要な情報にアクセスできる

情報を守る

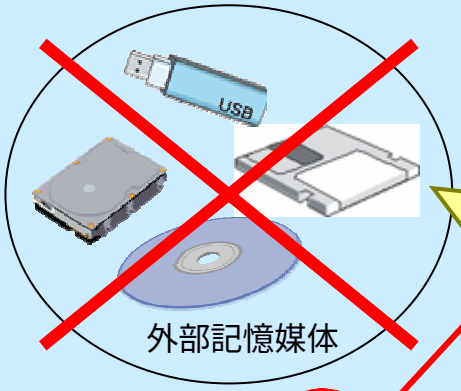
情報を守りつつ、かつ
情報を戦略的に活用

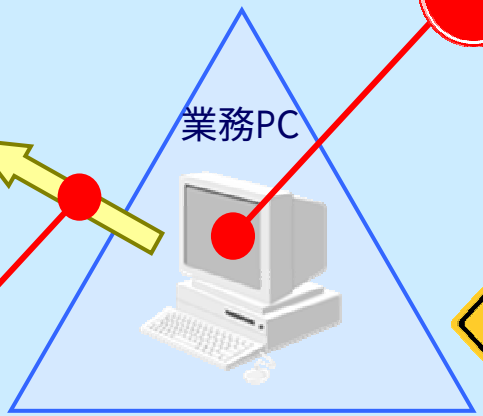
情報を共有し活用する

小型可搬媒体への書き込み禁止ツール

Total Security Fort

社内ネットワークに接続する全てのパソコンに、情報漏洩防止対策ソフトウェア
(Total Security Fort*) を適用しています





▼一部のソフトウェアの起動不可
・Norton Ghost
・P2Pソフト
・IM、Skypeでのファイル転送の不可
▼一部の通信デバイスの利用不可
・IrDA, Bluetooth の利用不可

▼外部記憶媒体の利用不可
・フロッピー/MO
・USBメモリ/フラッシュメモリ
・CD-R/DVD-R
・外付けHDD　等

TSFの設定ポリシーを変更することで、例外的な処理 (暗号化出力を条件とした外部記憶媒体への出力等) も，申請承認プロセスをへて可能となる。

▼ログの収集
・ファイルサーバとのファイル入出力ログ
・印刷出力ログ
・インターネット(web)閲覧ログ
・ソフトウェア実行ログ
・ハードウェア変更ログ

不必要な小型可搬媒体への書き出しができない

書き出しを申請・承認できるワークフロー機能による一時的な書き出しが可能

情報を守る

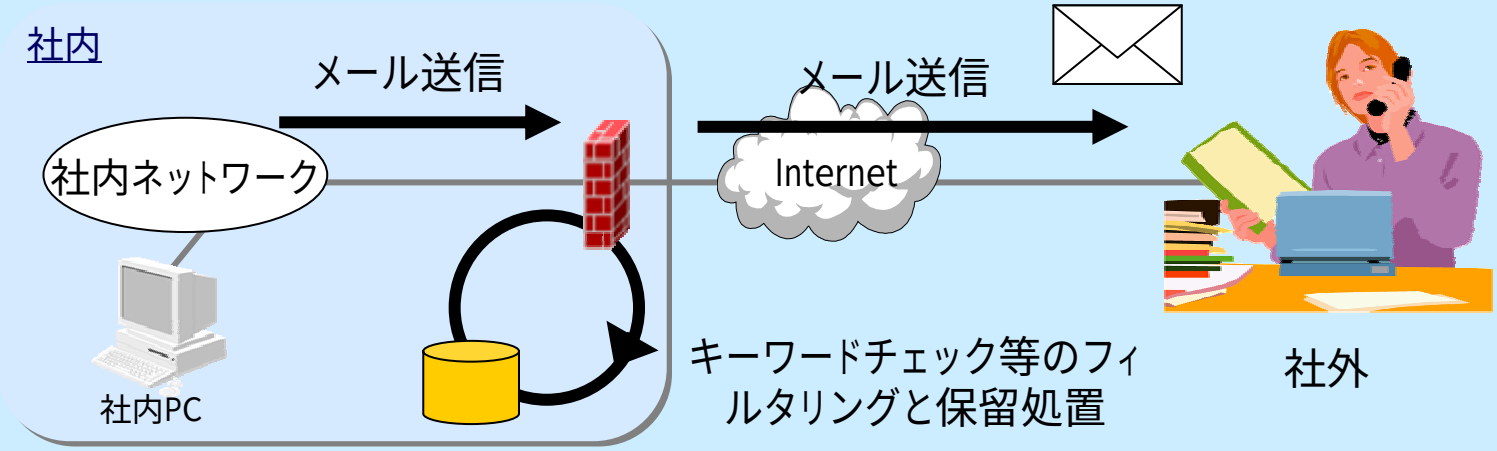
情報を守りつつ、かつ情報を戦略的に活用

情報を共有し活用する

メールによる持出しの規制

メールフィルタリング

社外に送信されるメールに対して，フィルタリングを実施しています．機密情報が含まれている場合，送信が一旦保留されます．



不必要な機密情報の社外送信が制限される

必要な場合には社外へもメール送信ができる

情報を守る

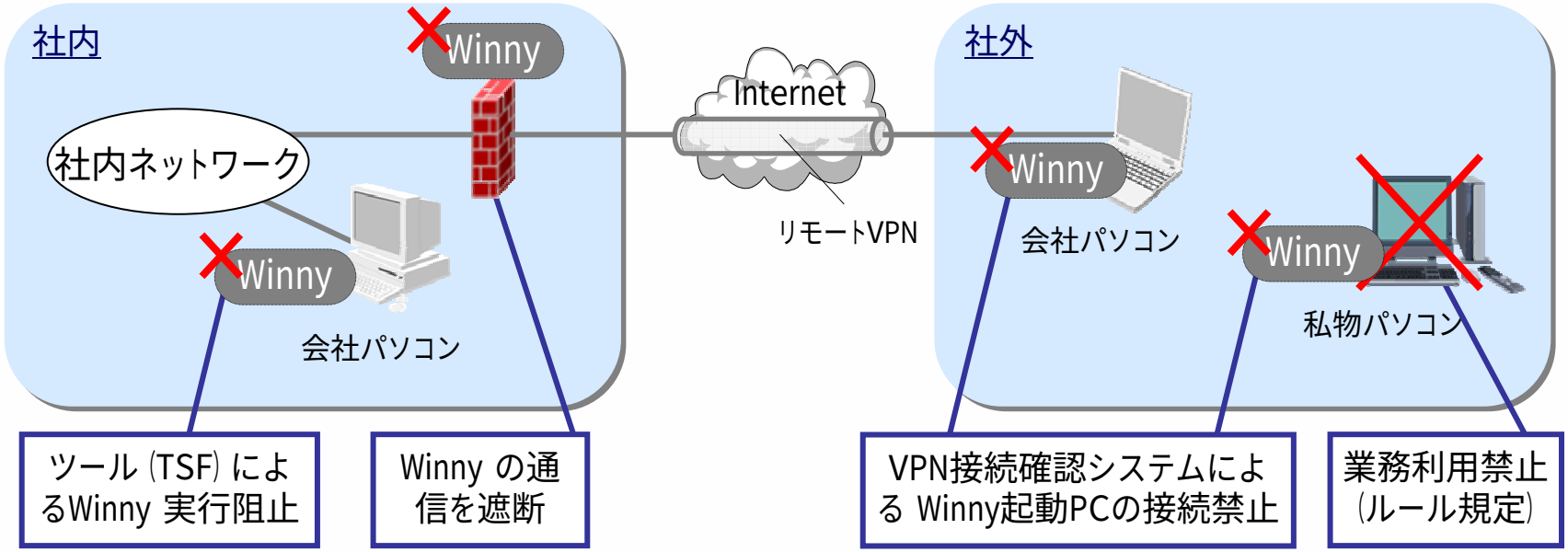
情報を守りつつ、かつ情報を戦略的に活用

情報を共有し活用する

P2Pソフトウェアへの対策

社内ネットワークとインターネットの出入口における通信制御や情報漏洩対策ソフトウェア（TSF）等の活用により、Winny などの P2Pソフトウェアの実行を禁止しています。

※ 技術的な対策だけでなく、Winny等のP2Pソフトウェアがインストールされている
PCの業務利用禁止について、全社員から誓約書を取得している。

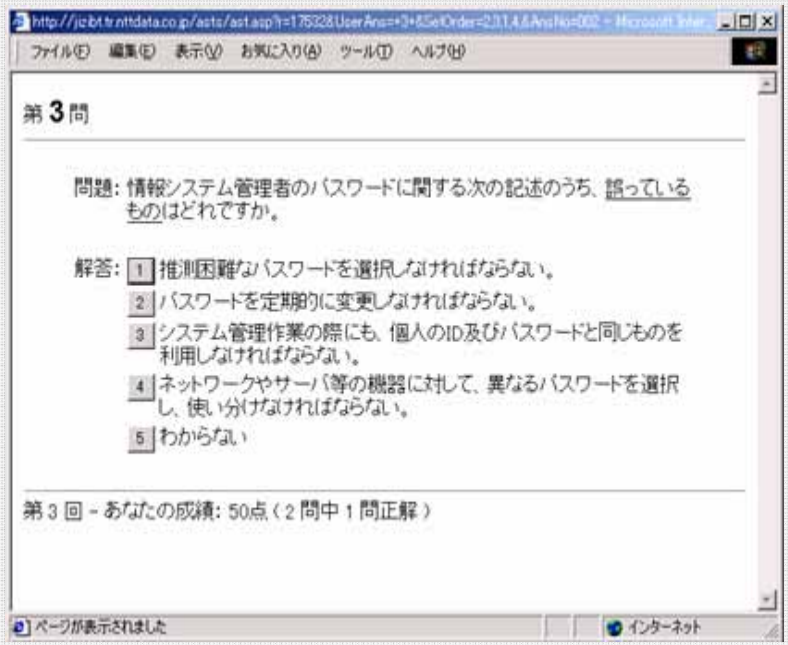


NTTデータの独自調査や外部のセキュリティ対応組織との連携など、Winnyネットワークの監視体制、及び、万が一 Winny等による情報漏洩事故が発生した場合の対応体制を整えている。

情報セキュリティ教育　～全社員教育～

情報セキュリティや個人情報保護に関して、社員が当然知っておかなければならない基本事項について、定期的･継続的に知識を授与･共有する教育活動を行っています。

情報セキュリティポリシーアセスメント



- 情報セキュリティポリシー等の社内規程の定着と実践意識の向上を目的とする。
- eラーニングによる教育を、全社員を対象に、2000年度より毎年実施している。
- 組織及び役職毎に実施状況を集計（自動表示）し、管理職等が実行管理を行う。

情報セキュリティ教育　～新入社員教育～

パソコンやメールの使い方，公共の場での注意など，社会人としてのマナーから教育しています．

入社時研修

会社のパソコンは私物パソコンとはちがいます！

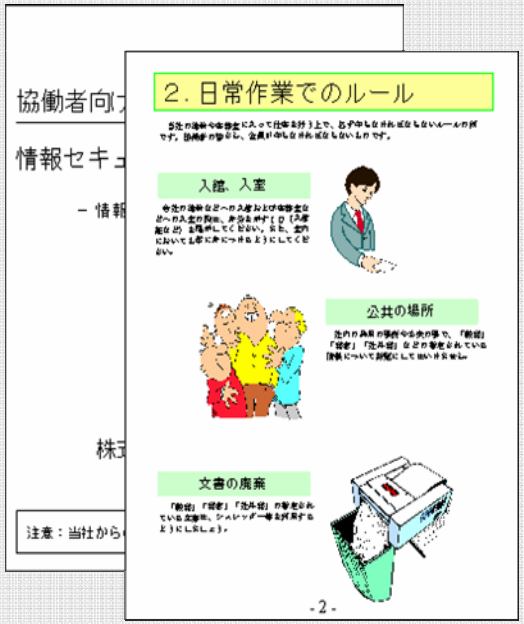
ちょっとした不注意が情報漏えい事故につながります！

業務に関する話題は，世間話とはちがいます！

情報セキュリティ教育　～協働者教育～

社員と協働する派遣社員等が、その業務の範囲内において果たすべき情報セキュリティ上の役割等について、教育・指導を行っています。

協働者向け情報セキュリティ教育



- 日常業務において、情報セキュリティポリシー等に則った適切な行動がとれるよう、新規契約時および定期的に指導する。
- 確認問題に合格しなければ、一部業務システムの利用を許可されない。

情報セキュリティ教育　～啓発～

社員や協働者に対して「気づき」の機会を与え、情報セキュリティの重要性を認識することを目的とした啓発活動を行っています。

情報セキュリティ啓発ポスターの例

- 各職場の規模に応じて必要枚数配付
- 年間２～４種類を制作

月刊ニュースレター（SecurityToday）

- 社内のセキュリティ最新情報や注意喚起等
- 毎月発行（Webにてバックナンバー閲覧可）

情報セキュリティハンドブック

- 日常の基本動作についてまとめた読み物
- 小冊子の配布や、社内Webでの公開

情報セキュリティ教育　～啓発～

セキュリティ強化運動

あいさつ運動

ビルのエントランスで，腕章をつけた社員が，朝のあいさつ運動を展開しています．

情報セキュリティレッドカード

注意をうながす真っ赤なカードで，職場全体での運動を展開しています．

セキュアフライデー

毎週金曜日を、情報セキュリティ確保のために必要な行動を実践する日としています。これを、セキュアフライデーという名称で展開しています。

2008年11月～2009年3月の金曜日
「携帯電話情報削除デー」
携帯電話の紛失は、中に格納された機密情報の漏えいにつながります。携帯電話に蓄積されたメールや履歴は、週末に入る前に削除してしまいましょう。

情報セキュリティ教育　～脆弱性情報の共有～

NTTデータ内の専門チームがセキュリティ技術に関する脆弱性情報などを収集し、各自必要な最新情報の確認が無理なく行えるよう、随時全社に配信し、情報共有しています（Security News Flash サービス）。

～Security News Flash　Web画面イメージ図～

Security News Flash の特徴

①セキュリティの専門チームによる的確かつ迅速な情報収集及び情報共有が行われている（ほぼ毎日）。

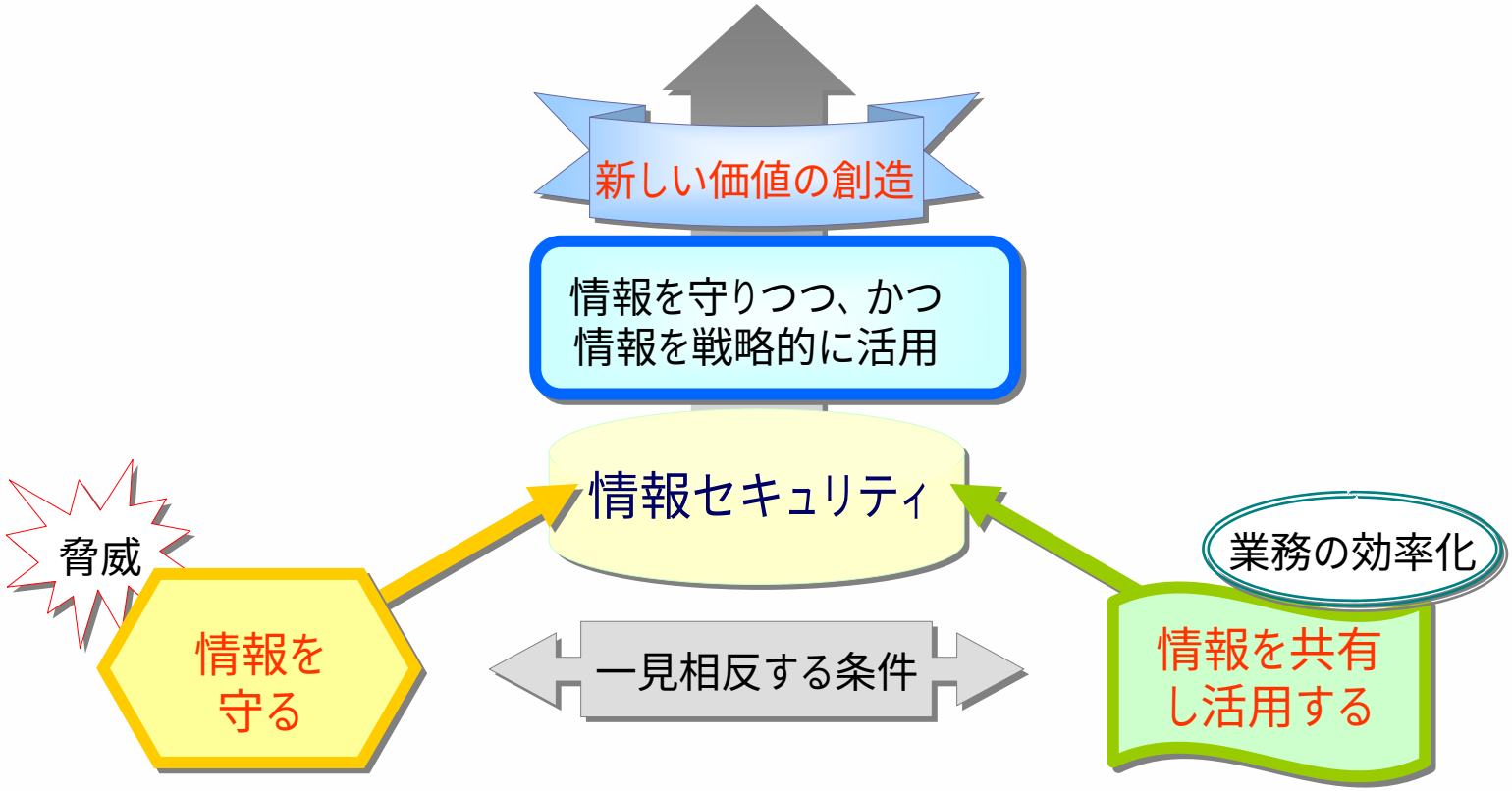
②Web画面または電子メールの２通りの閲覧方法がある。

③ニュース記事毎にリスクレベルが表示されているため、対処の実行判断や優先度を考える際に役に立つ。

④自分が興味を持つカテゴリに絞り込んで情報を取得することができる。

NTTデータグループが目指す方向

お客様に安心していただける情報セキュリティを
NTTデータグループ全体で実現する



“i”　：　information 「情報」 そして I 「わたし」

情報セキュリティへの取り組みの基本はひとりひとりの心構え

お問い合わせ先
NTTデータ　情報セキュリティ推進室
電話：050-5546-2545
E-Mail：grisec@kits.nttdata.co.jp